

徹底攻略

ボリュームUPで応援価格!

[定価]
本体

1,480円
+税

情報セキュリティ マネジメント

過去問題集

平成29^[2017年]年度 **春期** | 五十嵐 聡 [著]



2大特典



情報処理試験指導歴25年の
現役ベテラン講師による詳細解説!

たくさん紙面
解ける!! 収録

5回分!

過去問 2回 + 模擬問題 3回

- 「問題」と「解説」が「見開き完結」で読みやすい!
- 「攻略のカギ」で重要ポイントがわかりやすい!

インプレス

目次

情報セキュリティマネジメント 攻略ガイド	3
-------------------------	---

情報セキュリティマネジメント 重要用語 334 選	8
------------------------------	---

情報セキュリティマネジメント試験

平成28年度 秋期	41
-----------	----

午前 問題	42
午後 問題	82

平成28年度 春期	111
-----------	-----

午前 問題	112
午後 問題	144

第1回 模擬試験	171
----------	-----

午前 問題	172
午後 問題	202

第2回 模擬試験	217
----------	-----

午前 問題	218
午後 問題	252

第3回 模擬試験	273
----------	-----

午前 問題	274
午後 問題	308

■ 問題文中で共通に使用される表記ルール	325
■ 解答一覧	326
■ 答案用紙	327
■ 索引	329
■ 単語帳アプリ「でる語句 200」の使い方	334

購入者限定特典のご案内

● スマホで学べる単語帳アプリ「でる語句 200」のダウンロード

巻頭記事「情報セキュリティマネジメント 重要用語」から、暗記に適した用語をピックアップしてまとめた、いつでもどこでも暗記できる単語帳アプリ「でる語句 200」を無料でダウンロードいただけます。手順については、334ページをご参照ください。

● 電子版の無料ダウンロード

- ・ 本文全文の電子版 (PDF ファイル。印刷不可) を無料でダウンロードいただけます。
- ・ 答案用紙の PDF (印刷可能) をダウンロードいただけます。
- ・ IPA が第 1 回試験開始前に、参考として公開したサンプル問題 (午前・午後) の解答・解説 PDF をダウンロードいただけます。
- ・ PDF のダウンロードについては、以下の URL をご確認ください。

ダウンロード URL :

<http://book.impress.co.jp/books/1116101092>

※ 画面の指示に従って操作してください。

※ ダウンロードには、無料の読者会員サービス「CLUB Impress」への登録が必要となります。

※ 本特典のご利用は、書籍をご購入いただいた方に限ります。

・ 本書は、情報セキュリティマネジメント試験の受験対策用の教材です。著者、株式会社インプレスは、本書の使用による情報セキュリティマネジメント試験への合格を保証するものではありません。

・ 本書の内容については正確な記述に努めました。著者、株式会社インプレスは本書の内容に基づきいかなる試験の結果にも一切責任を負いかねますので、あらかじめご了承ください。

・ 本書の試験問題は、独立行政法人 情報処理推進機構の情報処理技術者試験センターが公開している情報に基づいて作成しています。

攻略ガイド

情報セキュリティマネジメント試験の概要

情報セキュリティマネジメント試験は、経済産業省が創設し、平成28年4月からIPA（独立行政法人情報処理推進機構）が実施している国家資格です。近年増加しているサイバー攻撃や内部不正などの脅威に対抗するために、情報セキュリティ人材の育成と確保を目的としている試験で、4月（春期）と10月（秋期）の年2回実施されます。

この試験は、一般企業において必要とされる「情報セキュリティマネジメント人材」を対象としています。

◆情報セキュリティマネジメント人材

「情報セキュリティマネジメント人材とは、部門の情報資産に対して適切な情報管理を実施し、組織の情報セキュリティポリシーやルールを部門内のメンバーに周知して順守を促すなど、部門内で情報セキュリティマネジメントを推進する人材です。具体的には、部門内で不審メールを受信した場合には注意喚起を行い、速やかにCISO・情報システム部門に報告する、またサイバー攻撃の被害やインシデントが発生した場合には、企業内のインシデント対策チームであるCSIRTと連携し、情報共有を行うことで被害を最小限に抑える役割などを担うと考えられます」（<http://www.ipa.go.jp/about/press/20151016.html>より引用）

情報セキュリティマネジメント試験では、情報セキュリティマネジメント人材がもつべき知識やスキルを測ることを目的としています。特に、情報セキュリティマネジメントの計画、運用、評価、改善を通して、自らが所属する組織の情報セキュリティ管理体制を確立し、安全性を向上させるために必要な知識が重要視されます。

◆午前試験の概要

	試験時間	出題数（解答数）	出題形式	基準点
午前試験	90分 (9:30～11:00)	50問 (50問)	多岐選択式 (四肢択一)	60点 (100点満点)

午前試験では四肢択一（4つの選択肢から1つを選ぶ）の問題が50問出題されます。

◆ポイント

- ・90分の試験時間中に全問解答するには、1問に約1分48秒しか費やせません。後述するテクニックを用いて、解答時間を削減する必要があります。

◆午後試験の概要

	試験時間	出題数(解答数)	出題形式	基準点
午後試験	90分 (12:30～14:00)	3問 (3問)	多岐選択式	60点 (100点満点)

午後試験では、8～10ページの長文の問題が3問出題されます。全問必須です。

◆ポイント

- ・ 90分の試験時間中に全問解答するには、1問に30分しか費やせません。
- ・ 全問必須なので、得意分野の問題をあらかじめ特定しておき、試験が開始したらその問題だけを解くといったことができません。情報セキュリティ全般に関する知識と応用力が要求されます。

◆主な出題範囲 (IPA公表 情報セキュリティマネジメント試験要綱 重点分野のみ抜粋)

大分類	中分類	小分類	主な知識項目
技術要素 (セキュリティ)	セキュリティ	情報セキュリティ	機密性・完全性・可用性, 不正プログラム, 暗号方式, デジタル署名, 公開鍵基盤など
		情報セキュリティ管理	情報資産とリスクの概要, リスク対応, 情報セキュリティポリシーなど
		セキュリティ技術評価	PCI DSS, CVSSなど
		情報セキュリティ対策	情報セキュリティ対策, 不正プログラム対策, 不正アクセス対策, セキュリティ製品・サービスなど
		セキュリティ実装技術	セキュアプロトコル, ネットワークセキュリティなど
企業と法務 (法務)	法務	知的財産権	著作権法, 不正競争防止法など
		セキュリティ関連法規	不正アクセス禁止法, 個人情報保護法など
		労働関連・取引関連法規	労働基準法, 守秘義務など
		その他の法律・ガイドライン・技術者倫理	コンプライアンス, 情報倫理など
		標準化関連	JIS, ISO, IEEEなど

(https://www.jitec.ipa.go.jp/1_13download/youkou_ver2_0_sg_bassui.pdf を参考に作成)

◆平成28年度春期, 秋期試験における出題内容(午前)

大分類	中分類	小分類	出題内容
技術要素 (セキュリティ)	セキュリティ	情報セキュリティ	情報セキュリティの3要素, 不正のトライアングル, 2要素認証, C&Cサーバ, APT, クロスサイトスクリプティング, クリックジャッキング, ハッシュ関数, 認証局, ドライブバイダウンロード, パスワードリスト攻撃, バックドア, AES, ポートスキャン, 公開鍵暗号方式, ルートキット, スクリプトキディ, ソーシャルエンジニアリング, ランサムウェア, PKI

大分類	中分類	小分類	出題内容
技術要素 (セキュリティ)	セキュリティ	情報セキュリティ管理	CSIRT, クリアデスク, 情報セキュリティ監査, JIS Q 27001-リスク受容, リスク評価, 残留リスク, 情報セキュリティ方針, 特権的アクセス権, ICカード, リスク対応, JPCERT/CC, JVN, ベースラインアプローチ, MDM
		情報セキュリティ対策	情報漏えい対策, 組織における内部不正防止ガイドライン , アクセスログの取扱い, BYOD, IDS, WAF, マルウェア対策, 内部不正の防止, デジタルフォレンジックス, 磁気ディスクの廃棄, HDD パスワード, SIEM, ビヘイビア法, CAPTCHA, サイバーセキュリティ戦略
		セキュリティ実装技術	SPF, NTP
企業と法務 (法務)	法務	知的財産権	不正競争防止法
		セキュリティ関連法規	個人情報保護法, 電子計算機損壊等業務妨害, 電子計算機使用詐欺罪, 不正アクセス禁止法, 特定電子メール送信適正化法 , プロバイダ責任制限法, 特定個人情報の適正な取扱いに関するガイドライン
		労働関連・取引関連法規	請負契約, 準委任契約
		その他の法律・ガイドライン・技術者倫理	OECD プライバシーガイドライン
コンピュータシステム	システム構成要素	システムの評価指標	レスポンスタイム, クライアントサーバシステム
技術要素 (セキュリティ以外)	データベース	データベース設計	E-R図
		データベース応用	データウェアハウス
	ネットワーク	データ通信と制御	ルータ
		通信プロトコル	DHCP
		ネットワーク応用	プロキシサーバ
サービスマネジメント	サービスマネジメント	サービスマネジメント	SLA, 移行テスト, インシデント, バックアップ
		サービスマネジメントプロセス	RTO
	システム監査	システム監査	スプレッドシートの利用に係るコントロール, 従業員の守秘義務, 情報セキュリティ監査基準 , ISMSの内部監査, デジタルフォレンジックス, BCP
システム戦略	システム戦略	業務プロセス	BPO
		ソリューションビジネス	SaaS
	システム企画	システム化計画	企画プロセス
		調達計画・実施	RFP
企業と法務 (法務以外)	企業活動	経営・組織論	事業継続計画, コーポレートガバナンス, マトリックス組織
		OR・IE	積上げ棒グラフ

(太字は春期・秋期共に出題)

◆平成28年度春期, 秋期試験における出題内容(午後)

●28年度春期

問題	内容
問1	標的型攻撃メール, マルウェア, ウイルスメール, ソーシャルエンジニアリング
問2	業務委託, 利用者ID, ロール
問3	URL フィルタリング, リモート接続, アクセスログ, 最小権限の原則, チェックリスト, CSA

●28年度秋期

問題	内容
問1	オンラインストレージサービス, ファイル共有設定の問題点, 事故発生時の原因特定, 組織的・技術的対策
問2	情報機器の持出し, 紛失時の対応手順, HDDの暗号化, ノートPCの調査
問3	インシデントへの初動対応, 不正プログラム感染, 公開Webサイトの改ざん, アクセス権限の設定, リスクアセスメント

現時点で本試験はまだ2回しか実施されていないので, 今後どの内容が多く出題されるかは不明です。しかし, 情報処理試験では過去に出題された問題や用語が繰り返し出題される可能性が高いので, 今回出題された内容が再度出題されることを見越しておきましょう。

試験の位置付け・時間・出題形式

◆位置付け: 基本情報技術者試験と同じレベル2の試験

全問マークシート(多岐選択式) 午前・午後とも全問必須

ITを活用する者		情報処理技術者試験								情報処理安全確保支援士試験		
ITの安全な利活用を推進する者		情報処理技術者								情報処理安全確保支援士		
的知識・技能	ITの安全な利活用を推進するための基本	情報セキュリティマネジメント試験 (SG)	高度な知識・技能	システムアーキテクト試験 (ST)	プロジェクトマネージャ試験 (SA)	ネットワークスペシャリスト試験 (PM)	データベーススペシャリスト試験 (NW)	エンベデッドシステムスペシャリスト試験 (DB)	ITサービスマネージャ試験 (ES)	システム監査技術者試験 (SM)	安全な情報システムを設計、開発、運用するための情報セキュリティに関する知識・技能	情報処理安全確保支援士試験 (通称 情報セキュリティスペシャリスト試験) (SC)
	全ての社会人	ITパスポート試験 (IP)		応用的知識・技能	応用情報技術者試験 (AP)							
の共通の基礎知識	ITを活用するための		基本的知識・技能	基本情報技術者試験 (FE)								

(https://www.jitec.ipa.go.jp/1_13download/youkou_ver3_0.pdf より)

※ 情報セキュリティマネジメント試験の詳細はhttps://www.jitec.ipa.go.jp/1_04hanni_sukiru/_index_hanni_skill.htmlを参考にしてください

おすすめ学習法・試験のテクニック

◆過去問題の反復練習が合格のカギ

情報セキュリティマネジメント試験に限らず、情報処理技術者試験では過去問題の学習を何度も行う反復練習が効果的です。

◆午前試験では過去問題が出題される

午前試験では過去問題が高い頻度で出題されます。平成28年度秋期では、基本情報技術者試験から8問(16%)、応用情報技術者試験から12問(24%)、情報セキュリティアドミニストレータ試験などから4問(8%)、計24問(約48%)が出題されています。過去の各試験のセキュリティ関連の過去問を解いておくことで、本試験で見覚えのある問題が出題される可能性が高くなります。

◆攻略のカギ

自分の苦手な分野などを洗い出すために、解説欄の「攻略のカギ」を利用してください。午前の「攻略のカギ」には問題に関連する用語や要点、計算に関しては必要な計算式を、午後の「攻略のカギ」には問題を解くためのヒントを掲載しています。

◆間違えた問題は必ず復習する

間違えた問題は必ず復習して、次に解答するときは正解できるようにします。本書掲載の問題にはチェックボックスが付いています。チェックボックスに×印などをつけておき、解説をよく読んで間違えた理由を理解します。

- **解答群が全て単語の午前問題や、解答群から語句を選ぶ形式の午後の設問を間違えた場合：**正解の単語を記憶する。また、他の問題で正解以外の単語が出題されることもあるので、正解以外の単語もおろそかにせず、本書解説などで調べておくこと
- **解答群が文章の午前問題を間違えた場合：**正解の選択肢で説明されている内容と、出題されたテーマの単語とを結び付けて記憶する

◆繰り返し問題を解く

時間の許す限り、何回も繰り返して問題を解き、重要な語句や内容を覚えましょう。前述したように、午前試験では過去問題が出題される頻度が高いので、過去問題を何度も読むことで、問題(図表も含む)と正解のイメージをできるだけ多く頭に入れていくことが必要です。

午後試験では、問題文を全て熟読する必要はありません。問題文を流し読みして概要をつかんだら、先に設問に目を通し、各設問に対応する問題文の一部だけを参照することで、大部分の設問の正解そのものまたはそのヒントを得ることができます。

◆時間を計る

午前試験及び午後試験の時間は限られています。本試験で時間が足りなくなり、解ける問題に解答できなかったということがないように、実際の試験を受けていると想定して、時間を正確に測って問題を解く練習をしてみましょう。

情報セキュリティマネジメント重要用語334選

情報セキュリティマネジメント分野の問題を解く上で必要な関連用語を集めました。これらの用語を押さえつつ問題を解くことで、より実力アップが図れます。

アルファベット			JIS	29	SSH	25
AES	16	JIS Q 27001	21	SSID	23	
APT	13	JIS Q 27002	21	SSL/TLS	25	
BCP	39	JIS Q 27014	21	SSLアクセラレータ	24	
BIA	39	JIS Q 31000	19	TCP/IP	33	
BPR	38	JVN	21	TPM	27	
CAPTCHA	19	LAN	32	UPS	24	
CEO	39	LAN間接続装置	33	URLフィルタリング	23	
CIO	39	LTE	35	USBキー	25	
CISO	39	MAC	17	UTM	24	
Common Criteria	29	MACアドレス	34	VLAN	26	
Cookie	25	MACアドレス制限	23	VoIP	35	
CRL	18	MACアドレスフィルタリング	26	VPN	35	
CRYPTREC暗号リスト	16	MDM	24	WAF	24	
CSIRT	20	MIME	34	WAN	33	
CSRF	12	MTBF	31	WBS	36	
CVSS	21	MTTR	32	WEP	23	
DDoS攻撃	13	NAS	31	WPA2	23	
DES	16	NDA	29	XML	35	
DKIM	22	need-to-know	21	XMLデジタル署名	19	
DLP	24	NIDS	21			
DMZ	22	NIST	29	あ		
DNS	33	OCSF	19	アクセス制御	21	
DNS amp 攻撃	14	OP25B	23	アクティビティ	36	
DNSSEC	22	OSコマンドインジェクション	15	アローダイアグラム	37	
DoS攻撃	13	PCI DSS	21	暗号化技術	16	
EC	35	PDCA	36	インシデント	32	
EDI	35	PGP	16	インシデント管理	38	
EDoS攻撃	15	PKI	18	ウイルス	10	
FIPS 140-2	19	POP3	34	ウイルス作成罪	27	
FTP	34	RADIUS	33	ウイルス対策ソフト	24	
FTTH	33	RAID	31	ウォームスタンバイ	30	
HIDS	22	RASIS	24	請負契約	28	
HTML	35	RFI	39	運用テスト	37	
HTTP	34	RFP	39	営業活動によるキャッシュフロー	40	
HTTPS	34	RFQ	39	営業秘密	27	
HTTPヘッダインジェクション	15	RLO	14	エージェント方式	19	
ICMP flood攻撃	15	RPO	37	遠隔バックアップ	25	
IDS	21	RSA	16			
IEEE	29	RTO	37	か		
IEEE 802.1X	19	S/MIME	16	稼働率	32	
IMAP4	34	SaaSなどのサービスモデル	30	キーロガー	11	
IP-VPN	36	SAN	31	技術的脅威	10	
IPS	22	SEOボイズニング	15	危殆化	17	
IPsec	25	SIEM	24	キャッシュフロー計算書	40	
IPv4	34	SIP	36	キャッシュボイズニング	13	
IPv6	34	SLA	37	脅威	10	
IPスプーフィング	13	SMTP	34	共通鍵暗号方式	16	
IP電話	35	SMTP-AUTH	27	クライアントサービスシステム	30	
ISMS	20	smurf 攻撃	14	クラウドコンピューティング	30	
ISO/IEC 15408	29	SOC	21	クラウドサービス利用のための情報セキュリティマネジメントガイドライン	29	
ITIL	37	SPF	22	クラッキング	21	
ITガバナンス	38	SQL	32			
ITサービスマネジメント	37	SQLインジェクション	12			

クリアスクリーン.....	25	ゼロデイ攻撃.....	14	バレート図.....	39
クリアデスク.....	25	相互けん制.....	38	光ファイバ.....	33
クリックジャッキング.....	12	ソーシャルエンジニアリング.....	10	非機能要件.....	38
グローバルIPアドレス.....	33	損益計算書.....	40	ビッグデータ.....	32
クロスサイトスクリプティング.....	12	損益分岐点.....	40	否認防止.....	10
クロスサイトリクエストフォージェリ.....	12			ヒューマンエラー.....	31
刑法.....	27	た		標的型攻撃.....	13
ゲートウェイ.....	34	ターンアラウンドタイム.....	31	ファイアウォール.....	23
検疫ネットワーク.....	22	第三者中継.....	13	ファイル共有ソフト.....	11
減価償却.....	40	貸借対照表.....	40	フィッシング.....	13
広域イーサネット.....	36	ダイナミックパケットフィルタリング.....	26	フルプルーフ.....	31
公開鍵暗号方式.....	16	タイミング攻撃.....	14	フェールセーフ.....	31
公開鍵基盤.....	18	タイムスタンプ.....	18	フォールトトレラント.....	31
構成管理.....	38	対話型処理.....	30	不正アクセス禁止法.....	27
コールドスタンバイ.....	30	他人受入率.....	19	不正競争防止法.....	27
個人情報保護法.....	28	多要素認証.....	18	物理的脅威.....	10
コピーレフト.....	29	チャレンジレスポンス.....	17	プライバシーマーク.....	29
コンティンジェンシープラン.....	20	中間者攻撃.....	13	プライバシーポリシ.....	20
コンテンツフィルタ.....	23	調達計画・実施.....	39	プライベートIPアドレス.....	33
コンピュータ犯罪防止法.....	28	著作権法.....	27	ブラウザ.....	35
コンプライアンス.....	29	ディザスタリカバリ.....	37	ブラックリスト.....	26
		デジタル証明書.....	18	ブルートフォース.....	12
さ		デジタル署名.....	17	ブレーンストーミング.....	39
サービスレベル合意書.....	37	デジタルフォレンジックス.....	24	プロジェクト.....	36
サイドチャネル攻撃.....	14	ディレクトリトラバーサル.....	13	プロジェクトマネジメント.....	36
サイバー攻撃.....	11	データウェアハウス.....	32	プロバイダ責任制限法.....	28
サイバーセキュリティ.....	27	データマイニング.....	39	分散処理.....	30
サイバーセキュリティ基本法.....	27	テザリング.....	35	ペイジアンフィルタリング.....	26
サイバーテロ.....	12	デジュレスタンダード.....	30	ベースライン.....	37
財務活動によるキャッシュフロー.....	40	デファクトスタンダード.....	30	ベストエフォート.....	36
サブネット.....	34	デュアルシステム.....	30	ベネレーションテスト.....	21
サンドボックス.....	23	デュプレックスシステム.....	30	変更管理.....	38
残留リスク.....	20	デルファイ法.....	40	ポートスキャン.....	15
辞書攻撃.....	12	電子透かし.....	22	ホスト型IDS.....	22
システムの移行.....	37	テンペスト攻撃.....	15	ボット.....	11
集中処理.....	30	投資活動によるキャッシュフロー.....	40	ホットスタンバイ.....	30
瞬断.....	24	特定電子メール法.....	28	ポリモーフィック型ウイルス.....	11
情報資産.....	19	ドライブバイダウンロード.....	12	ホワイトハッカー.....	21
情報セキュリティ監査基準.....	38	トランスポートモード.....	25	ホワイトリスト.....	26
情報セキュリティ管理基準.....	38	トロイの木馬.....	11	本人拒否率.....	19
情報セキュリティポリシ.....	20	トンネリング.....	35		
情報のCIA.....	10	トンネルモード.....	25	ま	
情報漏えい.....	10			マークアップ言語.....	35
職務の分離.....	38	な		マクロウイルス.....	10
シンククライアントシステム.....	31	内部統制.....	38	マルウェア.....	10
シングルサインオン.....	18	ネットワーク型IDS.....	21	水飲み場型攻撃.....	13
真正性.....	10			ミラーリング.....	24
人的脅威.....	10	は		無線LAN.....	23
侵入検知システム.....	21	バージョンロールバック攻撃.....	15	迷惑メール.....	15
侵入防止システム.....	22	バイオメトリクス認証.....	18	メールボム.....	13
信頼性.....	10	排他制御.....	32	メタデータ.....	32
スイッチングハブ.....	33	ハイブリッド暗号.....	16	メッセージ認証.....	17
ステークホルダ.....	36	バグ.....	11	モラルハザード.....	20
スパイウェア.....	11	パケットフィルタリング.....	26	問題管理.....	38
スパムメール.....	11	派遣契約.....	29		
スループット.....	31	パスワードリスト攻撃.....	12	ら	
脆弱性.....	11	パスワードリマインダ.....	19	ランサムウェア.....	11
脆弱性情報データベース.....	21	バックアップ方式.....	32	ランニングコスト.....	32
生体認証.....	18	ハックティヴィズム.....	12	リース.....	40
責任追跡性.....	10	バックドア.....	11	リスク.....	20
セキュリティホール.....	11	ハッシュ関数.....	16	リバースプロキシ.....	26
セッションハイジャック.....	13	バッファオーバーフロー.....	27	リバースプロキシ方式.....	19

リピータ.....	33	ルートキット.....	11	ロック.....	32
リブレイ攻撃.....	13	レスポンスタイム.....	31		
利用者認証.....	18	レンタル.....	40	わ	
リリース及び展開管理.....	38	労働基準法.....	28	ワーム.....	11
ルータ.....	33	労働者派遣法.....	29	ワンタイムパスワード.....	18
ルーティング.....	33	ログ管理.....	21		

情報セキュリティ

情報のCIA

情報セキュリティを維持するために必要となる要素です。JIS Q 27001 (ISO/IEC 27001)などの主要な情報セキュリティの規格では、次の三つの要素を情報のCIA (または情報セキュリティの3要素)としています。

要素	概要
機密性 (Confidentiality)	不特定多数からデータにアクセスされないようにして、適切な権限をもつ者だけがアクセスできるようにする性質
完全性 (Integrity)	データの内容が不正に削除されたり改ざんされたりしないようにして、内容を矛盾なく保つようにする性質
可用性 (Availability)	適切な権限をもつ者が、必要なときにシステムやデータを利用できるようにする性質

真正性

情報セキュリティに関連する要素で、情報やその利用者が本物である(なりすましではない)という性質です。

責任追跡性

情報セキュリティに関連する要素で、事故や事件が発生したとき、情報システムに残されたログなどを参照して、その実行者を特定できる性質です。

否認防止

情報セキュリティに関連する要素で、処理を実行した人が、後からそれを否定できないようにする性質です。

信頼性

情報セキュリティに関連する要素で、情報システム及びその構成要素が意図したとおりに稼働している性質です。

脅威

情報システムに対して悪い影響を与える要因のことです。JIS Q 27001 で定義されています。

物理的脅威

脅威の一種で、重要な設備が格納されている建物に不正侵入され、物理的な破壊や盗難などの被害を受けることです。

技術的脅威

脅威の一種で、マルウェアなどに感染させられたり、サーバに不正アクセスされたりすることで、機密情報の漏えいや改ざんなどの被害を受けることです。

人的脅威

脅威の一種で、自社の従業員が意図的に情報を持ち出したり、または偶発的に操作ミスをしたりすることで、機密情報を盗んだり外部に漏えいさせたりすることです。

情報漏えい

自社が管理していた機密情報や顧客の個人情報などを、外部に漏えいさせることです。

ソーシャルエンジニアリング

不正なユーザが本人になりすまして、パスワードなどのセキュリティに関する情報をセキュリティ管理者などから不正に聞き出す行為です。

マルウェア

コンピュータに悪影響を与えることを目的として作成された不正なソフトウェアです。

ウイルス

マルウェアの一種で、攻撃対象のコンピュータ内のファイルなどに感染し、特定の日時になるまで潜伏した後、発病して不正な動作をするという特徴をもちます。

マクロウイルス

マクロとは、ワープロソフトや表計算ソフトなどの機能の一つで、一連の操作を呼び出して実行できるように、簡易なプログラムのような形式でまとめたものです。マクロは、ワープロソフトのファイルなどと一緒に保存されます。マクロウイルスは、マクロの仕組みを悪用したウイルスで、

ワープロソフトの文書ファイルや表計算ソフトのスプレッドシートなどに、通常のマクロと同様の形式で保存されます。マクロウイルスが感染した文書ファイルなどを開くと、ワープロソフトのテンプレート(文書の定型)などにマクロウイルスが感染します。その後に、別の文書ファイルを開いたり新規作成したりすると、そのファイルにもマクロウイルスが感染します。

ポリモーフィック型ウイルス

感染するごとにランダムに変化させた暗号化鍵を用いて、ウイルスのコードを暗号化することで自身の内容を常に変化させて、同一のパターンで検知されないようにするウイルスのことです。

ワーム

不正侵入や感染などの行為を単独で実行できるタイプのマルウェアです。ワームは、OSやアプリケーションソフトの脆弱性を突くなどの方法により、パソコンやサーバなどに侵入して、当該コンピュータ上で不正な行為を実行したり、同じネットワーク内の他のコンピュータに自身のコピーを送りつけて、さらに感染範囲を広げたりすることを行います。

ボット

マルウェアの一種で、攻撃対象のコンピュータに潜伏し、攻撃者が用意した外部のマルウェアから指令を受け取ると、情報を漏えいさせるなどの特定の行動をします。

スパムメール

広告宣伝などを目的として、受信者の意向に関係なく、不特定多数の利用者に無差別に送信されるメールのことです。

ファイル共有ソフト

インターネット上で、利用者間でファイルを共有するためのソフトウェアです。一部のマルウェアは、ファイル共有ソフトの脆弱性を突いて感染しようとするため、ファイル共有ソフトを不用意に使用すると、マルウェアに感染する危険性が高まります。

トロイの木馬

正当なプログラムを装ってインストールされ、秘密裏に不正行為を働くマルウェアのことです。

スパイウェア

通常の無害なソフトウェアに見せかけてコンピュータ内に

インストールされるマルウェアです。インストールされたスパイウェアは、秘密裏にコンピュータ内の個人情報やパスワードなどの情報を特定の外部サーバに送付したり、Web閲覧時にユーザの意図しない広告を勝手に表示したりするなどの処理を行います。

ランサムウェア

マルウェアの一種で、コンピュータに感染した上で内部のファイルを勝手に暗号化し、利用者を脅迫して元に戻すための代金を払わせようとしています。

キーロガー

コンピュータへのキー入力を記録し、その内容を外部に送信するソフトウェアです。キーロガーは、キーボードから入力された他人のパスワードを盗むために悪用されることがあります。

ルートキット

OSなどに秘密裏に組み込まれたバックドアなどの不正なプログラムを、隠蔽するための機能をまとめたツールのことです。

バックドア

攻撃者が、マルウェアに感染したPCに今後もアクセスできるようにするために、PC内に秘密裏に作られる攻撃用の侵入経路のことです。

脆弱性

情報システムや情報資産に存在する、脅威が顕在化する確率のことです。JIS Q 27001 で定義されています。

バグ

プログラムやシステムに内在している誤りのことです。

セキュリティホール

コンピュータやシステムに内在している、情報セキュリティ上の弱点のことです。マルウェアは、セキュリティホールを突くことでコンピュータなどへの攻撃を実行します。

サイバー攻撃

インターネットを経由して、インフラや政府機関などのシステム及びサーバなどを攻撃し、改ざんや破壊などの被害を与えることで、社会を混乱させようとする行為です。

ハックティビズム

情報技術を利用し、宗教的または政治的な目標を達成するという目的を持った人、または組織のことです。

サイバーテロ

サイバー攻撃と同様に、インフラや政府機関などのシステム及びサーバなどを攻撃し、社会を混乱させようとする行為です。

ブルートフォース

考えられる全ての種類の暗号化鍵またはパスワードを総当たりで作成して、それをもって暗号解読を試みたり、他人になりすましたりすることです。

辞書攻撃

辞書に掲載されている一般的な名詞などの単語(“apple”など)、及び単語の組合せなどの文字列をパスワードとして入力していき、標的ユーザのパスワードを推定しようとする攻撃方法です。

パスワードリスト攻撃

Webサービスや組織などから流出した、利用者IDとパスワードの組のリストを入手して、それを用いて他のWebサービスに不正ログインしようとする攻撃方法です。

SQLインジェクション

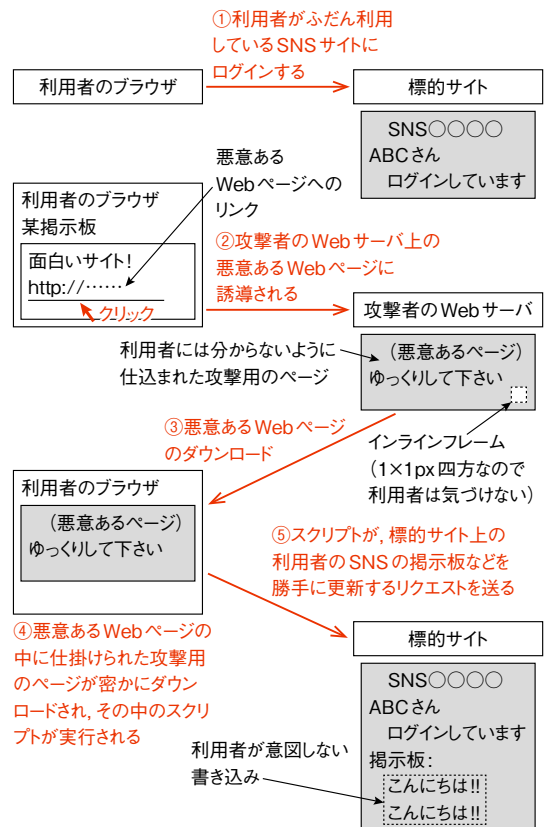
Webページ上の入力フォームに不正な文字列を入力し、入力フォームから受け取った値をもとにして生成されたSQL文を不正なものにして、Webアプリケーションを誤動作させたり、データベースの内容を削除したりする攻撃方法です。

クロスサイトスクリプティング

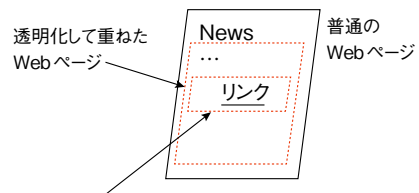
悪意を持ったスクリプト(JavaScriptなど)を利用者のブラウザに送り込み、利用者を標的サイトに誘導することで、標的サイト上で当該スクリプトを動作させ、利用者の個人情報盗み取る攻撃方法です。

CSRF (クロスサイトリクエストフォージェリ)

悪意あるスクリプトを含んだ攻撃用のページを密かにダウンロードして、そのスクリプトを自動的に実行するWebページを閲覧させるなどの方法で、利用者がログインしている状態の標的サイトに対して別のWebサイト上のページから不正なリクエストを送り、意図しない操作を行わせる攻撃方法です。



クリックジャッキング



透明化されたリンク(普通のWebページのリンクの上に設置されており、クリックすると、透明化したWebページ上で操作が実行される)

HTMLのiframeタグなどを用いることで、Webページの中に別のWebページを埋め込むことができます。当該レイヤを透明にすることで、一見問題がないように見えるWebページの上層に、別のWebサイトのWebページを透明化して密かに埋め込むことが可能になります。

このようなWebページ上で操作を行うと、利用者が気付かないうちに、別のWebサイトのWebページ上で不正な操作が行われます。このような攻撃をクリックジャッキングといいます。

ドライブバイダウンロード

攻撃用のWebページを閲覧した際に、利用者に気づかれることなく、秘密裏にマルウェアをダウンロードさせ、PCに感染させる攻撃のことです。

ディレクトリトラバーサル

ファイル名などをパラメタとして受け取るフォームの入力欄に、“../passwd”などといった不正なファイル名や相対パス名を入力することで、Webサーバに格納されている重要なファイルを表示させたり、削除させたりする攻撃手法のことで。

中間者攻撃

利用者Aと利用者Bがインターネット上で通信を行っているときに、攻撃者がAとB間に割り込んで、公開鍵などをすりかえるなどの方法で、やり取りされているデータを横取りしたり盗聴・改ざんしたりする攻撃手法のことで。

第三者中継

自社のメールサーバのセキュリティ対策が甘いため、外部から第三者宛てに送信するメールが転送可能な状態になっていることです。この状態では、悪意のユーザが発信したスパムメールなどの転送の肩代わりをさせられ、自社が不正行為に加担させられてしまいます。

IPスプーフィング

送信元IPアドレスを攻撃対象の組織内のIPアドレスに偽装したIPパケットを当該組織のネットワークに送付し、誤動作を起こさせたり、不正侵入を試みたりする攻撃手法です。

キャッシュポイズニング

DNSサーバなどに対して、ドメイン名などを改ざんした不正な情報を送り込み、そのサーバを参照したPCの利用者を、本来のWebサーバとは異なるWebサーバに誘導する攻撃手法のことで。

セッションハイジャック

Webサーバとブラウザの間で行われる継続的なやり取り(セッション)を維持するためのセッションIDを攻撃者が推測して、正当なブラウザになりすましてWebサーバに送り込み、ブラウザとWebサーバ間のセッションを乗っ取る攻撃方法のことで。

リプレイ攻撃

盗聴者が、正当な利用者のログインシーケンス(ログインするときに送受信されるパケットのやり取り)をそのまま記録してサーバに送信し、利用者になりすまそうとする攻撃方法のことで。

DoS攻撃

Denial of Service攻撃。DNSサーバなどを踏み台にして問合せを大量に行い、攻撃対象のサービスを妨害する攻撃手法のことで。

DDoS攻撃

Distributed Denial of Service攻撃。多数のホストにボットを感染させ、特定の日時になったときに全てのボットから攻撃対象のサーバに一齐に攻撃を仕掛けることで、攻撃対象のサービスを妨害する攻撃手法のことで。

メールボム

同じ宛先メールアドレスに大量の電子メールを送信することで、受信者の業務を妨害するなど、各種の被害を与えることです。

フィッシング

サイトの偽装や偽造電子メールの使用によって、ユーザを騙して個人情報などを不正に入手したりする行為です。具体的な方法は次のとおりです。

- ① 標的のサイトのWebページによく似せたWebページを作成する。
- ② 当該サイトの利用者に対して“本人確認の再確認が必要なのでこのURLにアクセスして入力してください”という主旨の、偽装した電子メールを送る。
- ③ そのメールに騙された利用者が、URLに示されたページにアクセスしてIDやパスワードを入力すると、入力したデータが詐取される。

標的型攻撃

特定の企業または個人を対象にした攻撃手法の総称です。対象に深く関連する人や組織(上司、同僚、得意先など)を送信元に偽装して、業務に関係する表題や内容の電子メールを送り付け、添付ファイルを開くよう促すなどの方法で、マルウェアに感染させようとしています。

APT

Advanced Persistent Threats。攻撃者が特定の組織を標的として、複数の手法を組み合わせで執拗に攻撃を繰り返す手法です。

水飲み場型攻撃

RSAセキュリティ社が2012年に公表した攻撃手法で、次のような手順をとります。

- ① 攻撃者は、攻撃対象の利用者がWebを利用する様子

を観察し、頻繁にアクセスするWebサイトを特定する。

- ② 攻撃者は、攻撃対象の利用者が頻繁にアクセスするWebサイトを改ざんして、攻撃用のコードを埋め込み、その利用者がアクセスしたときだけマルウェアをダウンロードするように設定する。

- ③ 攻撃対象の利用者が②のWebサイトにアクセスすると、攻撃が行われてマルウェアがダウンロードされる。

水飲み場型攻撃という名前は、攻撃者をライオン、攻撃対象の利用者が頻繁にアクセスするWebサイトを動物の水飲み場に例え、ライオンが水飲み場の近くで動物を待ち伏せすることから来ています。

ゼロデイ攻撃

新種のウイルスなど、対策が存在しなかったり、または公表されていないママルウェアによって行われる攻撃のことです。

RLO

文字の表示順を変えるUnicodeの制御文字を利用することで、ファイル名の拡張子を偽装することです。RLOを利用して、実行ファイル(拡張子がexe)を圧縮ファイル(拡張子がzip)などに見せかけて、マルウェアを実行させようとする手口が存在します。

例

dummydatapiz.exe ← マルウェアのファイル名

↑

この位置に、以降の文字の表示順を「左から右」から「右から左」に変えるUnicode制御文字を入れる

dummydataexe.zip ← というファイル名で表示される
(実体はマルウェア)

サイドチャネル攻撃

暗号化装置のソフトウェアやハードウェアをさまざまな方法で解析して、その消費電流などの物理量やエラーメッセージなどから暗号の解読を試みたり、機密情報を得たりする攻撃のことです。

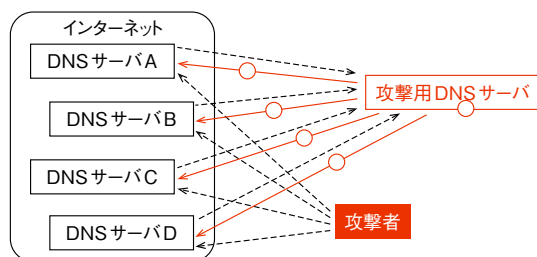
タイミング攻撃

サイドチャネル攻撃の一種で、複数の平文データを暗号化装置に与えて、それらを暗号化する処理時間の差異を観察することで、暗号化装置の演算アルゴリズムを推測しようとするものです。

DNS amp攻撃

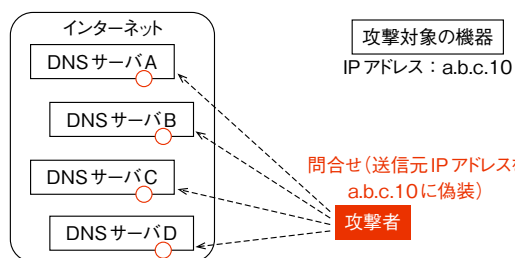
次のような攻撃手法のことです。

- ① 攻撃者は、攻撃用DNSサーバにデータ量の多いレコード(以下、攻撃用レコードという)を記録しておき、インターネット上の多数のDNSサーバに、攻撃用レコードへの問合せを行う。インターネット上の各DNSサーバは、攻撃用DNSサーバに攻撃用レコードを問い合わせ、攻撃用DNSサーバから受け取った攻撃用レコードをキャッシュする。

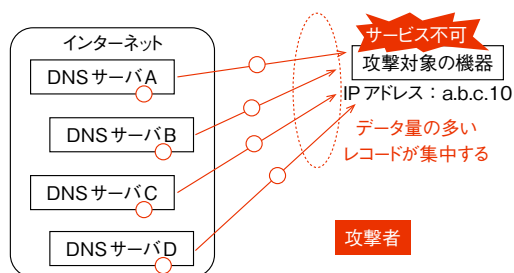


○：攻撃用レコード --->：問合せ →：DNSのレコードの応答

- ② 攻撃者は、①の全てのDNSサーバに対して、送信元IPアドレスを攻撃対象の機器のアドレスに偽造して、攻撃用レコードに関する問合せを行う。



- ③ ①の全てのDNSサーバは、攻撃対象の機器のIPアドレス宛てに攻撃用レコードを返答する。インターネット上の多数のDNSサーバから、攻撃対象の機器に対してデータ量の多いレコードが大量に送信されてくるので、攻撃対象の機器の負荷が増大し、サービスができなくなる。



smurf攻撃

ICMPの応答パケットを大量に発生させ、攻撃対象の通信負荷を大きくさせてサービスの停止などを狙う攻撃手法

のことです。攻撃対象のIPアドレスを送信元IPアドレスとして偽装したICMPの要求パケットを、攻撃対象の所属するネットワークの全コンピュータ宛てに、ブロードキャストで送信します。ICMP要求を受信した各コンピュータは、ICMPの応答パケットを攻撃対象に一斉に返送するので、通信負荷が大きくなってしまいます。

EDoS攻撃

Economic Denial of Service攻撃。経済的な損失を狙ったサービス妨害攻撃です。ファイル共有などの機能を提供しているクラウドサービスの中には、利用者から事業者のネットワークに対して与えられたトラフィックの量に応じて課金する、従量制の料金体系をとっているものもあります。そのようなサービスに対して、利用者のネットワークを経由して多数のアクセスを与えてリソースを大量に消費させることで、多額の料金を利用者に請求させます。

ICMP flood攻撃

pingコマンドを用いて、攻撃対象のサーバに対して大量の要求パケットを同時に発信し、当該サーバに至るまでの回線を過負荷にしてアクセスを妨害する攻撃手法です。

テンペスト攻撃

コンピュータやディスプレイなどから発せられる電磁波中の電磁的な信号を、測定用の機器を用いて観測し収集することで、操作中の画面の内容を再現したり、暗号化鍵や暗号化アルゴリズムなどの情報を不正に入手したりする攻撃方法のことです。

HTTPヘッダインジェクション

Webサーバは、次のようなテキスト形式の応答をブラウザに返します。

最初の改行のみの行の直前までがHTTPヘッダ

```
HTTP/1.1 200 OK (ステータスコード)
Date: ..... (レスポンスのデータが作成された日付)
...
Cache-Control: no-store, no-cache
```

(改行)
<html>
<head>
<title>●●ページへようこそ</title>
...

最初の改行のみの
行の直後からHTTP
ボディ(HTMLタグ
などが格納される)

HTTPヘッダインジェクションは、HTTPヘッダとHTTPボディが改行で区切られているというHTTPの仕組みを悪用して、HTTPレスポンスの中に不正なヘッダを仕込んだり、不正なHTMLタグなどを挿入したりする攻撃手法です。

OSコマンドインジェクション

Webページ上の入力欄にOSのコマンドライン(コマンドプロンプト)上で有効なコマンドを入力させ、Webサーバ上で不正な命令を実行させる攻撃方法です。例えば、UNIXやLinuxをOSとしているWebサーバで公開しているWebページの入力欄に、“……(正当なデータ); rm …”のような文字列を入力すると、正当なデータの処理の後に、“rm …”という、Webサーバ上のファイルを削除する命令が実行されてしまいます。

バージョンロールバック攻撃

SSL/TLSを実装する一部のソフトウェアでは、ブラウザとWebサーバとの間で使用する暗号化通信方式を決定するための通信(ハンドシェイクプロトコル)を行ったときに、通信経路に介在する攻撃者がその通信内容を改ざんして、暗号化通信方式の新しいバージョン(TLS1.0)ではなく古いバージョン(SSL2.0など)を使用するように強制することができます。SSL2.0などで使用する暗号化方式には暗号化鍵が短いなどの問題があるため、攻撃者はブラウザとWebサーバとの間で送受信される暗号化通信のパケットの内容を解読することができます。このような攻撃手法を、バージョンロールバック攻撃といいます。

SEOボイズニング

SEO(Search Engine Optimization、検索エンジン最適化)とは、自社のWebページのURLが検索サイトの検索結果の上位に表示されるように、Webページのタイトルや内容を改善することです。

SEOボイズニングとは、Web検索サイトの順位付けアルゴリズムを悪用して、キーワードで検索した結果の上位に悪意のあるサイトを表示させるために、そのサイトの内容を構成する手法のことです。

ポートスキャン

サーバなどの脆弱性を検出するときに用いる手法です。対象ホストに対して、宛先ポート番号を順次増加させながらアクセスしていき、対象ホストから正常な応答が返ってきたときに、そのポート番号のサービスが稼働している(対象ポートが開いている)と判断します。

迷惑メール

次のようなメールのことです。

- ① 広告宣伝などを目的として、受信者の意向に関係なく、不特定多数の利用者に無差別に送信されるメール(スパムメール)。

- ② フィッシングなどの攻撃または詐欺を目的として、不特定多数の利用者に送信されるメール。

CRYPTREC暗号リスト

CRYPTREC(Cryptography Research and Evaluation Committees)は、「電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト」のことで、CRYPTRECは、電子政府推奨暗号リストというリストを公開しています。このリストには、公的な機関によって客観的に評価され、安全性や実装性に優れると判断された暗号方式(DSA, AESなど)やハッシュ関数(SHA-1など)が掲載されています。

暗号化技術

特定のアルゴリズムに従って、データの置換・並べ替えなどの操作を行うことで、データの内容を解読不能にすることを暗号化といいます。暗号化されたデータを元の内容に戻すことを復号といいます。暗号化や復号を行うために用いられる情報を鍵といいます。鍵の作成や暗号化・復号の方法に関する技術を、暗号化技術といいます。

共通鍵暗号方式

暗号化と復号に同じ鍵(共通鍵)を用いる方式です。この方式では、ネットワークにN人の利用者がいるとき、ネットワーク全体では $(N-1)+(N-2)+\dots+2+1=N(N-1)/2$ 個の共通鍵が必要になります。

DES (Data Encryption Standard)

1977年に公表された共通鍵暗号方式で、56ビットの鍵を用いて暗号化を行います。現在は、鍵長が短く暗号を復号されやすい点で問題があり、後続の暗号方式であるAESを利用することが勧められています。

AES (Advanced Encryption Standard)

2001年に公表された共通鍵暗号方式で、128ビット、192ビットまたは256ビットの鍵を用いて暗号化を行います。

公開鍵暗号方式

一人の利用者に対してペア(対)で生成される「公開鍵」と「秘密鍵」の二つの鍵を、それぞれ暗号化や復号に用いる方式です。「公開鍵」はネットワーク上に公開して誰でも利用可能とし、「秘密鍵」は鍵の所有者が専有し、厳重に保管して他人には知られないようにします。利用者Aが利用者Bにデータを送るとき、AはBの公開鍵でデータを暗号化して送信し、それを受信したBは自身の秘密鍵でデー

タを復号します。

この方式では、ネットワークにN人の利用者がいるとき、ネットワーク全体では2N個の鍵が必要になります。

RSA

素因数分解の計算の困難さを利用した公開鍵暗号方式。鍵長は1,024ビット、2,048ビットまたは4,096ビット。

S/MIME

電子メールの暗号化方式規格。RSA securityにより提案され、IETFにより標準化されています。

- メッセージ本文を暗号化するために、共通鍵暗号方式の共通鍵を用いる。
- 共通鍵を送信者と受信者との間で安全に受け渡すことと、電子メールの改ざんを検出することを目的として、公開鍵暗号方式によるデジタル署名の仕組みを用いている。

PGP

共通鍵暗号技術と公開鍵暗号技術を併用した電子メールの暗号化・復号技術です。

- メッセージ本文を暗号化するために、メール送信の都度ランダムに生成した共通鍵暗号方式の共通鍵を用いる。
- 共通鍵を送信者と受信者との間で安全に受け渡すことを目的として、デジタル署名の仕組みを用いている。

ハイブリッド暗号

公開鍵暗号方式と共通鍵暗号方式とを組み合わせた暗号方式のことです。公開鍵暗号方式には暗号化・復号に必要な時間が長いという欠点があり、共通鍵暗号方式には鍵の個数が過大になるという欠点があります。データの送信の都度、共通鍵をランダムに生成し、その共通鍵を公開鍵暗号方式によって安全に相手に送信してから、データを共通鍵で暗号化して相手に送信することがハイブリッド暗号の例です。

ハッシュ関数

任意の長さのデータを入力すると、固定長のハッシュ値(メッセージダイジェストともいう)を出力する関数です。

【特徴】

- 出力されたハッシュ値から入力データの内容を推定(復元)することは困難。
- 入力データがわずかでも異なれば、ハッシュ値は著しく異なるものになる。

- 入力データの長さが異なっても、ハッシュ値は同じ長さになる。

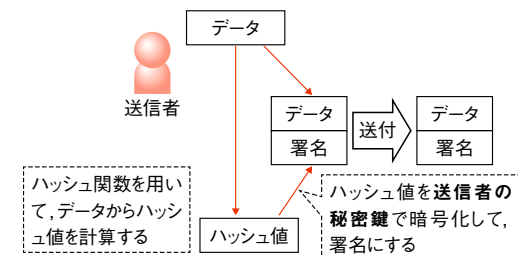
危殆化

安全でない状態になること、または安全が脅かされる状態になることです。暗号アルゴリズムの危殆化とは、パソコンなどの処理速度の向上によって暗号鍵の推定が容易にできるようになり、暗号の安全性が低下することを指します。

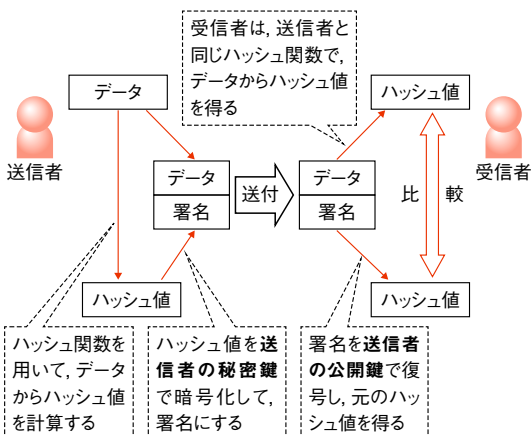
デジタル署名

通信相手に送付するデータの正当性を送信者が証明するための技術です。ハッシュ関数と公開鍵暗号方式を利用します。

- ① 送信者は、送付データ全体に対してハッシュ関数を用いて、ハッシュ値を求める。さらにそのハッシュ値を送信者の秘密鍵で暗号化して送信者の署名を作り、データと一緒に添付して受信者に送付する。



- ② 受信者は、送信者と同じハッシュ関数を用いてデータ本体からハッシュ値を生成する。さらに、送信者の署名を送信者の公開鍵で復号して、元のハッシュ値を入手する。この二つのハッシュ値が一致すれば、そのデータは送信者からのものであると確認できる。送信者以外は使用できない送信者の秘密鍵で送信者の署名が暗号化されているので、そのデータが確かに送信者本人の管理下にあったと証明できる。



メッセージ認証

デジタル署名と同様に、通信相手に送付するデータの正当性を送信者が証明するための技術です。共通鍵暗号方式を利用します。

送信者と受信者は同じ共通鍵を共有します。送信者はメッセージから共通鍵を用いてメッセージ認証符号(MAC: Message Authentication Code)を生成し、メッセージとともに送ります。受信者は、受け取ったメッセージからMACを生成して、送られてきたMACと一致することを確認します。

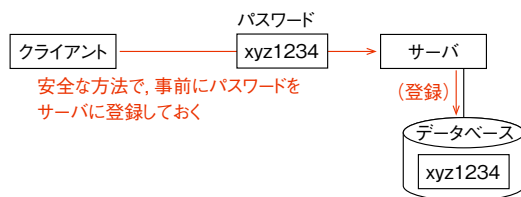
MAC

メッセージ認証において、送信者と受信者が共有する共通鍵を用いてメッセージから生成される認証用の符号です。

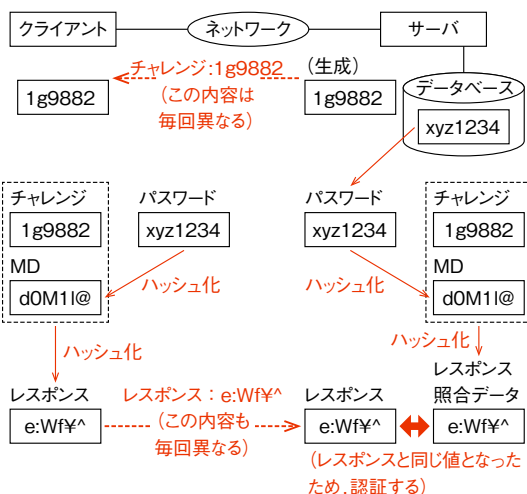
チャレンジレスポンス

次のような方法でクライアント(利用者)を認証する方式です。

- ① パスワードをサーバ側に事前に登録しておく



- ② クライアント-サーバ間で認証を行う



注記 MDはメッセージダイジェストの略である
また、利用者IDの送受は省略している

- サーバ(認証する側)は認証時に適当な長さのランダムな内容の電文(チャレンジ)を作成し、クライアント(認証される側)に送信する。
- クライアントは利用者のパスワードのメッセージダイジェストを計算し、送信されたチャレンジと合わせたものから、

さらにメッセージダイジェストを計算してレスポンスを生成する。

- クライアントは、利用者IDとともにレスポンスをサーバに返す。
- サーバは、クライアントから受け取った利用者IDで利用者情報を検索し、取り出したパスワードから計算したメッセージダイジェストとチャレンジとを合わせたものから、メッセージダイジェストを計算してレスポンス照合データを生成する。レスポンス照合データと、クライアントから受信したレスポンスが同じ値になれば、クライアントに送ったチャレンジが正しいパスワードのメッセージダイジェストと合わさって、レスポンスとして返送されてきたことが証明されるため、クライアントを認証する。

タイムスタンプ

文書の存在証明(ある時点よりも前に、文書が確かに存在していたことの証明)と原本保証性(文書が作成された時刻以降にその文書が変更・改ざんされていないこと)を証明するために、信頼できる第三者機関(タイムスタンプ機関)によって作成され、文書に添付されるデータのことで。

利用者認証

IDやパスワードなどを用いて利用者の本人性を証明し、情報システムなどの利用を可能とするための技術です。

多要素認証

複数の認証技術を併用することで、安全性を高める手法です。インターネットバンキングシステムで、パスワードだけではなく、トークンに表示されているワンタイムパスワードも一緒に入力しないと振込をできないようにすることが多要素認証の例です。他人にパスワードを知られても、トークンをもっていなければワンタイムパスワードを入力できないので、不正操作をされる危険性が減ります。

生体認証(バイオメトリクス認証)

生体認証(バイオメトリクス認証)とは、指紋、網膜、顔の形状などの、人間の身体的特徴から個人の識別を行う認証システムのことで。このシステムでは、認証を受けるユーザの指紋の形状などと、登録した本人の指紋の形状などを比較し、両者の類似の度合いが一定以上であれば、本人と識別します。

公開鍵基盤(PKI)

公開鍵暗号方式及びデジタル署名(電子署名)の仕組みを応用した、公開鍵の正当性を証明し、公開鍵とその利

用者を結び付けるための仕組みのことで。ある利用者がネットワーク上に公開している公開鍵が、本当にその利用者が作成して公開しているものか(本人性があるか)を証明するために、デジタル証明書が用いられます。信頼できる第三者機関(認証局)が利用者の本人確認をして、デジタル証明書を発行します。

デジタル証明書

利用者の公開鍵の本人性を証明するためのもので、公開鍵と認証局の署名が含まれます。

- 秘密鍵と公開鍵証明書の発行を受けた利用者は、秘密鍵は公開せず厳重に保管し、公開鍵証明書はネットワーク上に公開する。
- ある利用者の公開鍵証明書を入手した者は、デジタル署名の手続きと同様に、公開鍵証明書中の認証局の署名を認証局の公開鍵で復号する。
- 復号に成功すれば、その公開鍵証明書の署名は、認証局しか使用できない認証局の秘密鍵で暗号化されていたことが証明できる。すなわち、公開鍵証明書の利用者の本人性を認証局が確認しており、本人性が保証される。

CRL

Certificate Revocation List。有効期限内に無効になった(失効した)公開鍵証明書のシリアル番号を掲載したリストのことです。利用者が規約違反行為をするなどの理由で、デジタル証明書が無効となることがあります。相手から受け取ったデジタル証明書を使うとき、現在もそれが有効かを判定する必要があります。デジタル証明書とCRLとを付き合わせることで、有効かどうかを判断できます。

ワンタイムパスワード

毎回異なる認証データを送信することで、なりすましの危険性を低減する認証方式です。ワンタイムパスワードでは、ハッシュ関数の性質を利用して、毎回値が異なる使い捨てのパスワードを認証データとして用いています。

シングルサインオン

一度の利用者認証によって、複数のシステムやOSなどを利用可能とするための技術です。複数のシステムが存在し、それぞれのシステムについて異なったパスワードなどを用いて認証処理を経なければ、どのシステムも利用できないような状況では、「個々のシステムを利用する際に、その都度IDとパスワードの入力を求められる」ことになり、利用者にとって不便です。このような場合には、「一度利

用者認証に成功すれば、その後は全てのシステムやOSなどを、認証なしで利用できるようになる」という形態のシステムを導入することで、問題点を解決できます。

エージェント方式

シングルサインオンを利用する各システムに、エージェントというソフトウェアを組み込む方式です。利用者が一度入力した認証情報は、エージェントソフトによって認証情報を含んだクッキーというデータに加工され、各システム間で自動的に授受されます。その後、各システムにおいてクッキー内の情報が検証され、認証の成否が確認されます。

リバースプロキシ方式

シングルサインオンにおいて、認証用のサーバ(認証サーバ)を設置し、利用者の認証及び各システムへのアクセスを認証サーバに引き受けさせる方式です。認証の成功後は、認証サーバはプロキシ(代理)サーバとして機能し、利用者から各システムに送られた接続要求をいったん受け取ります。その後、認証サーバは利用者の代理として各システムに接続し、接続要求を送ります。そして、各システムから返却された業務処理の応答データなどを、利用者に戻します。

CAPTCHA

ゆがんだ文字など、人間なら認識できるがプログラムでは正常に認識できない画像データをサーバから送って、利用者にそれを読み取らせて入力させることによって、アカウントの作成や認証をする方式です。

パスワードリマインダ

利用者がパスワードを忘れた場合に、本人があらかじめ設定していた秘密の質問に答えることで、メールで送付する方法で利用者にパスワードを教えることです。

本人拒否率

生体認証において、正規の利用者本人を他人と誤認識して拒否してしまう確率です。判定しきい値を厳しくするほど上昇します。

他人受入率

生体認証において、他人を正規の利用者と誤認識して受け入れてしまう確率です。判定しきい値を厳しくするほど低下します。

IEEE 802.1X

無線LANの端末を認証するためのプロトコルです。アク

セスポイントなどの機器(認証装置またはオーセンティケータ)を経由して、無線LANの端末(クライアント)にインストールされたクライアントプログラム(サブリカント)と認証サーバとの間で認証情報がやり取りされます。認証を行うための利用者情報などは、認証サーバが管理します。

OCSP

Online Certificate Status Protocol。利用者が受け取ったデジタル証明書の失効状態を確認するためのプロトコルです。

デジタル証明書を受け取った利用者は、それを発行したCA(認証局)にOCSPメッセージを送信し、失効状態の問合せを行います。OCSPメッセージを受信したCAは、デジタル証明書の失効状態を確認して、利用者へ返答します。

FIPS 140-2

Federal Information Processing Standardization 140-2。暗号モジュール(暗号化を行うソフトウェアやハードウェア)に関するセキュリティ要件の仕様を定めている規格のことです。暗号モジュールのセキュリティレベルを、レベル1からレベル4までの4段階のレベルで規定しています。

XML デジタル署名

XML デジタル署名は、XML 文書の全体または一部の要素に対して付加できるデジタル署名の記述方法や署名アルゴリズムなどを定めたものです。署名を行うXML 文書中に署名用の要素(<signature>)を埋め込んだり、署名対象のXML 文書と別のファイルに署名用要素を用意したりすることが可能です。

XML デジタル署名では、従来のデジタル署名方法と比較して、文書(データ)の一部のエレメント(要素)にだけ署名することなどが可能です。

情報セキュリティ管理

情報資産

企業の業務に関連する顧客情報、財務情報、個人情報、製品情報などのデータと、それを保管・管理するためのシステム及び装置などのことです。

JIS Q 31000

リスクマネジメントの原則や組織のリスクマネジメントの取組みを継続的に改善することについて規定している規格です。

残留リスク

JIS Q 31000 で定義されている「リスク対応後に残るリスク」のことです。リスク対応においては、発生確率や被害額が大きいリスクに対しては適切な対策を施しますが、発生確率や被害額が非常に小さいリスクは、その被害額よりも対策費用の方が大きくなるがあるので、あえて対策をとらず許容することがあります。このようにして残したリスクが残留リスクです。

リスク

脅威が情報資産の脆弱性につけこみ、情報資産に損失などを与える可能性のことで、JIS Q 27001 で定義されています。

リスクマネジメント: リスクの防止、リスク発生時に被害を最小限にするための施策の制定、及びリスク発生により生じる費用に対する積み立てなどの措置を実施するなどの手法によってリスクを管理すること。

リスクアセスメント(リスク評価): 自社の事業に関する固有のリスクの発見と調査を行い、リスクの被害額や発生確率を評価することで、各リスクに適切に対処しようとする。

リスクマネジメントに関する用語

用語	概要
リスク分析	リスクの発生頻度や被害額などを判定し、重要なリスクと重要でないリスクとを区別し、各リスクについての対処方法などを決定すること。
リスク対策	リスクを防止するための各種手法。 ● リスクコントロール リスクが現実のものにならないようにするための、または現実化したリスクによってもたらされる被害を最小限にするための対策。 ● リスク回避: 事業から撤退するなどの方法で、リスクそのものを発生させなくすること ● リスク低減(軽減): リスクの発生確率や損失額を減らすこと ● リスクファイナンス リスクが発生することは不可避であると仮定し、リスクによる損失に備えて保険に加入したりすることで、リスクが現実化したときに生じる損失金額を少なくするための対策。 ● リスク移転(転嫁): 保険に加入したり、事業を外部に委託したりすることで、リスク発生時の影響、損失、責任の一部または全部を他者に肩代わりさせること ● リスク保有(受容): 軽微なリスクに対してはあえて対策を行わず、リスクが発生した場合の損失は自社で負担すること

モラルハザード

従業員の倫理観が著しく欠如した状態となり、社内の情

報を意図的に漏えいさせるなどの脅威を発生させたり、情報セキュリティに関する業務を怠ったりすることです。

コンティンジェンシープラン

「緊急時対応計画」または「不測事態対応計画」のことで、障害や事故などの事態が発生することを想定し、その対策を事前に定めた計画案のことです。

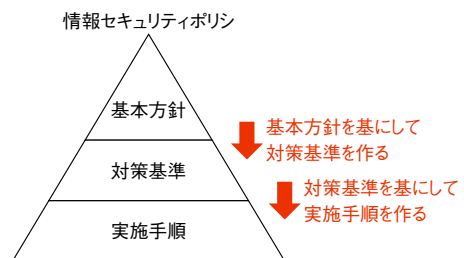
情報セキュリティポリシー

ISMS (情報セキュリティマネジメントシステム)を運用する際に必要となる、組織の情報セキュリティ維持体制を規定し、内外に公表するための文書です。

基本方針: 情報セキュリティポリシーの構成要素の最上位にある文書で、自社の情報セキュリティに対する基本的な考え方や姿勢を示す。

対策基準: 情報セキュリティ対策のために必要な組織の規則と、その適用範囲を示す。

実施手順: 対策基準で示した規則を遵守するために必要となる、具体的な業務手順を示す。



プライバシーポリシー

企業が個人情報を管理する際に必要となる、個人情報管理体制を規定し、内外に公表するための文書です。

ISMS

Information Security Management System, 情報セキュリティマネジメントシステム。情報システム上に存在する情報資産のセキュリティ管理体制のことです。ISMSを確立するとき、情報セキュリティポリシーを作成して遵守することが重要となります。

CSIRT

Computer Security Incident Response Team。インターネット上で各種の問題(特に、セキュリティに関する問題＝セキュリティインシデント)が発生していないかを監視し、発生した問題の報告を受け取ってその原因を調査したり、対策を想定したりする組織です。

SOC

Security Operation Center。CSIRTの一部として配置される組織で、ファイアウォールやIDSなどの装置を常時監視し、セキュリティインシデントの発生を検知した場合はCSIRTに報告して対処を依頼します。

ホワイトハッカー

情報セキュリティやコンピュータネットワークに関する高度な知識をもち、それを生かすことで、情報セキュリティの構築や攻撃からの防御など善良な活動をする人のことです。

JVN

Japan Vulnerability Notes。JPCERT/CCとIPAが共同で管理している、脆弱性情報データベースです。

脆弱性情報データベース

ソフトウェアなどに存在する脆弱性の一覧を集約し、公開しているデータベース。

JIS Q 27001

ISMS (情報セキュリティ管理システム)の国際標準規格であるISO/IEC 27001をJIS規格化したものです。情報の機密性、完全性、可用性の維持を管理するシステムが正常に機能しているかを監査対象としています。

JIS Q 27002

組織における情報セキュリティマネジメントの導入、実施、維持及び改善のための指針及び一般的原則を規定しているJIS規格です。

JIS Q 27014

情報セキュリティガバナンスについての概念及び原則に基づくガイダンスを提示しているJIS規格です。国際規格ISO/IEC 27014に対応しています。

セキュリティ技術評価

PCI DSS

Payment Card Industry Data Security Standard。クレジットカード情報などを保護することを目的として、VISAなどのクレジット会社が共同で策定した基準です。

CVSS

Common Vulnerability Scoring System, 共通脆弱性評価システム。米国のインフラストラクチャ諮問委員会

(NIAC, National Infrastructure Advisory Council) が2004年に原案を作成したシステムで、情報システムの脆弱性を汎用的な基準に基づいて評価するためのものです。

ペネトレーションテスト

対象の情報システムに対して実際に攻撃を行い、侵入を試みることによって、ファイアウォールや公開サーバなどに存在するセキュリティホールや脆弱性、及び設定ミスなどを発見するテスト手法のことです。このテストは、セキュリティのコンサルティングを行っている企業や専門家などに依頼した上で、外部から実施されます。

情報セキュリティ対策

need-to-know

情報セキュリティの維持に関する原則の一つで、情報を知ったり使用したりする必要がある人にだけアクセス権限を与え、そうでない人には与えないようにすることで、情報の漏えいなどを防止することです。

ログ管理

サーバやネットワーク機器などが取得するログ(アクセスしてきた利用者のIDや送信元IPアドレスなどを記録したデータ)を収集・分析して、不正アクセスなどの攻撃の検知に役立てることです。

アクセス制御

システムやデータにアクセスするための権限を利用者に設定し、適切なアクセス権限をもつ者だけアクセスを可能にし、そうでない者はアクセスできないように管理することです。

クラッキング

インターネットなどのネットワークを通じてサーバなどに不正に侵入し、データの改ざんや破壊を行うことです。

侵入検知システム (IDS)

Intrusion Detection System。内部ネットワークに対する外部(インターネットなど)からの攻撃を検知するためのシステムのことで。

NIDS (ネットワーク型IDS)

ネットワーク中のファイアウォールなどの重要な機器内に設定され、ネットワーク上を流れているパケットの内容を解析し、攻撃に使用されるタイプのパケットや、挙動の疑わ

しいパケットを判別し警告を発するタイプのIDSです。

HIDS (ホスト型IDS)

ネットワーク上の個々のコンピュータやサーバに設定され、自機器に到達したパケットの内容を解析し、攻撃に使用されるタイプのパケットを解析し警告するタイプのIDSです。

DMZ

外部に公開するWebサーバやメールサーバなどを組織内のLANに配置すると、外部からのIPパケットが社内LANに入り込むことになり、不正なIPパケットをクライアントPCや非公開のサーバなどに送りつけられるといった問題が起きます。そこで、外部に公開するサーバは、ファイアウォールにて内部LANや外部と分離した特別な領域に配置し、外部から一定の条件でアクセス可能とします。このようにして、公開サーバと非公開サーバ及びクライアントとを分離して配置することによって、セキュリティが向上します。この領域のことを、DMZ (DeMilitarized Zone＝非武装地帯)といえます。

侵入防止システム (IPS)

Intrusion Protection System。IDSの機能をもつとともに、攻撃を検知するとファイアウォールに指示を送信して攻撃元からのアクセスを遮断したり、サーバを停止させたりすることで、攻撃の被害を出さないように防御するシステムのことです。

検疫ネットワーク

マルウェアが社内ネットワークに蔓延することを防ぐために設置されるシステムです。PCが社内ネットワークに接続されたとき、最初は隔離用のLANに接続させてウイルス感染の有無を検査したり、セキュリティパッチが導入されているかを確認したりして、不備がある場合は必要な措置を行い、安全な状態にしてから社内ネットワークに接続させるようにします。

電子透かし

画像データなどに、利用者には分からない形式で著作権者(権利者)情報などを埋め込む技術のことです。例えば、画像データの画素の色情報のビットの値を少しずつ正規の値からずらし、差分の値を順番に組み合わせていくと、何らかの情報を表したビット列になっているようにします。

●ステガノグラフィ

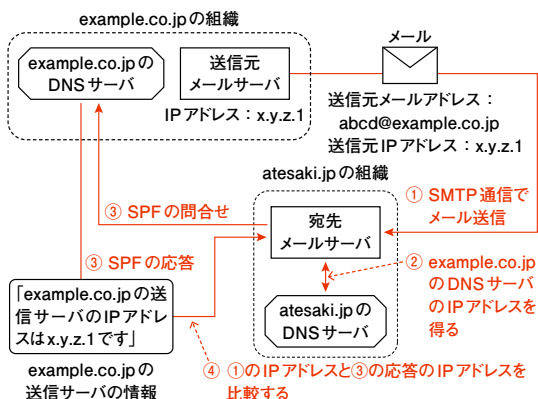
電子透かし技術を応用し、権利情報の代わりにメッセージを極秘に埋め込む技術のことです。

SPF

Sender Policy Framework。送信ドメイン認証の方法の一つです。送信ドメイン認証とは、メールの送信者の本人性を確認することです。

この方法では、メールサーバの組織が管理しているDNSサーバに、「自組織のメールサーバに対応するIPアドレスはこの値です」という主旨の情報を追記することで、自組織のメールサーバの正しいIPアドレスを他の組織のメールサーバから確認できるようにしています。

例えば、「abcd@example.co.jp」という送信元メールアドレスのメールを受信した①宛先メールサーバは、example.co.jpのDNSサーバのIPアドレスを、自組織のDNSサーバに問合せます②。その後、example.co.jpのDNSサーバに問合せた③送信サーバの情報を入手します④。その中に記載された送信サーバのIPアドレスと、送信元メールアドレスのIPアドレスとを比較して④、一致していれば正しいメールとして受信します。一致していなければ、他のIPアドレスのメールサーバから送信されてきたメールであるため、拒否します。



DNSSEC

DNS Security Extensions。DNSサーバから送信されてきたリソースレコードに公開鍵暗号方式のデジタル署名を付加することで、ドメイン名などの情報が改ざんされた場合に、それを検知できるようにするためのプロトコルです。DNSSECを用いることで、リソースレコードの送信者の正当性やデータの完全性を検証できます。

DKIM

DomainKeys Identified Mail。公開鍵暗号方式を応用して、電子メールの送信者認証及び改ざんの検出を可能とする技術です。送信側メールサーバは電子メールの内容のハッシュ値を求め、それを自ドメインの秘密鍵で暗号化してデジタル署名を作成します。送信側メールサーバは、

作成したデジタル署名を電子メールのヘッダに付与して、受信側メールサーバに送ります。

受信側メールサーバはDNSを検索して、送信側メールサーバが所属するドメインの公開鍵を入手し、それを用いてデジタル署名を復号することで、正当なメールサーバから電子メールが送信されてきたかどうかを検証できます。

OP25B

Outbound Port 25 Blocking。内部ネットワークのコンピュータから、外部のメールサーバのTCPポート番号25番への直接の通信を遮断することで、スパムメールの送信を防ぐことです。メール送信の際の宛先ポート番号が25番(SMTP)となることから、この行為では宛先ポート番号が25番のIPパケットを遮断(ブロック)します。

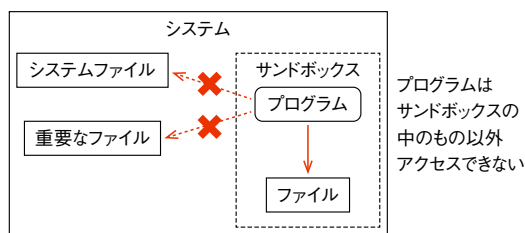
URL フィルタリング

組織内のPCからインターネット上のWebページを閲覧する際に、マルウェアに感染しているなど、不審な内容のWebページのURLをフィルタリング用の装置に登録しておき、当該Webページの閲覧を禁止することです。

コンテンツフィルタ

PCとインターネットとの間でやり取りされるWebページやメールなどの情報(コンテンツ)の内容を監視し、個人情報の流出が疑われるなど、問題がある場合は通信を遮断することです。

サンドボックス



情報セキュリティ対策技術の一つで、プログラムが実行できる機能やアクセスできるリソース(ファイルやハードウェアなど)を制限して、プログラムを動作させることです。プログラムのバグや不正な命令を組み込んだプログラムの実行などによって、システムファイルが破壊されるなどの被害を防ぐために有効です。

SSID

Service Set Identifier。ESS-IDともいいます。無線LANのアクセスポイントを識別するために、各クライアントに設定

される文字列のことです。各クライアントは、同じ値のESS-IDをもつアクセスポイントのみに接続することができます。

無線LAN

通信経路として無線電波を用いるLANのことです。PCなどの端末と、アクセスポイントから成ります。アクセスポイントは従来の有線LANのスイッチングハブやルータに該当します。

WEP (Wired Equivalent Privacy)

IEEE 802.11bなどの規格において用いられている無線LANの暗号化技術で、40ビットまたは104ビットの暗号化用の情報と、通信の都度ランダムに生成した24ビットの情報(IV, Initialization Vector)とを組み合わせ、暗号化鍵を生成する方法をとっています。この機能を有効にすることで、無線LANの通信データを暗号化することが可能となります。ただし、この暗号化技術は鍵の長さが短いなどの脆弱性があることが指摘されています。

MAC アドレス制限

MACアドレス制限とは、無線LANのセキュリティ機能の一つであり、指定したMACアドレスをもつ機器のみ、無線LANのアクセスポイントに接続することを可能とする機能です。

WPA2

Wi-Fi Protected Access2。鍵のビット数が少ないなどのWEPの脆弱性を改良するために作成された、無線LANの暗号規格やプロトコルなどの総称です。WPA2では、TKIP (Temporal Key Integrity Protocol)という鍵交換プロトコルや、IEEE 802.1Xという認証のためのプロトコルを利用しています。IEEE 802.1Xでは、複数のアクセスポイントが、1台のRADIUSサーバに対してユーザの情報を参照することで、ユーザ認証を行うことのできる仕組みを実装しています。WPA2では、通信中において動的に暗号鍵を更新することで、安全性を向上させています。

ファイアウォール

インターネットと社内LANとの間など、主要なネットワーク間に位置するネットワーク間接続装置で、ネットワーク間で送受信されるパケットの送信元、宛先、通信プロトコルまたは内容などを検査し、ルールに該当しない不審なパケットを破棄する役割をもちます。

WAF

Web Application Firewall。Webサーバとブラウザの間でやり取りされるデータの内容を監視し、Webアプリケーションプログラムの脆弱性を突く、XSS(クロスサイトスクリプティング)やSQLインジェクションなどの攻撃を防御するために用いられる、特別なファイアウォールのことです。

ウイルス対策ソフト

PCやサーバなどにインストールされ、ウイルス感染を防止するためのソフトウェアです。PCなどのファイルの内容を検査してウイルス感染の有無を検証し、感染していたファイルの削除や復元を行います。

DLP

Data Loss Prevention。情報システムから機密情報などが外部に流出することを防止すること、及びそのために導入・構築する装置やシステムのことです。

SIEM

Security Information and Event Management。ファイアウォールやサーバなどの各種機器から収集したログを分析して、セキュリティインシデントの発生を監視し、発生時は管理者に通知して迅速に対応するための仕組みのことです。

デジタルフォレンジックス

コンピュータ犯罪に対する科学的調査のことで、不正アクセスなどの犯罪に対する証拠(記録・ログなど)を立証するために必要なデータを保全して収集・分析すること、及びその後の訴訟などに備えることです。

UTM

Unified Threat Management, 統合脅威管理。ファイアウォール、IDS/IPS、ウイルス対策ソフト、及び各種フィルタリング機能といった情報セキュリティに関する各種製品の機能をまとめて保持している、統合的な管理用の機器を導入することで、情報セキュリティ対策コストの削減や情報の一元管理などを実現することです。

SSL アクセラレータ

SSL/TLSにおける暗号化・復号処理を、Webサーバの代わりに高速で実行する装置です。Webサーバの処理負荷を軽減することを目的として導入されます。

RASIS

コンピュータシステムの、5つの信頼性評価指標の総称です。

R=信頼性(Reliability):システムが故障せずに稼働し続ける度合いを示す指標。MTBF(平均故障間隔)で表される。

A=可用性(Availability):システムをいつでも通常どおりに利用できる度合いを示す指標。稼働率($MTBF / (MTBF + MTTR)$)で表される。

S=保守性(Serviceability):システムが、故障から可能な限り短い時間で復旧できる度合いを示す指標。MTTR(平均修理時間)で表される。

I=保全性(Integrity):障害が発生しても、データが破壊されず整合性を保った状態である度合いを示す指標。

S=機密性または安全性(Security):データが、外部からの不正アクセスなどによって盗まれたり、改ざんされたりすることがないように、データを保護する度合いを示す指標。

UPS

Uninterruptible Power Supply, 無停電電源装置。商用電源の一時的な停電や瞬断によって電流の供給が絶たれた場合に、コンピュータなどに一定時間安全に電流を供給するための装置です。UPSの内部にはバッテリーなどが存在し、コンセントから供給される電流が途絶えた場合にはバッテリーの電気を利用して即座に電流を供給することで、コンピュータの継続稼働を可能にしています。

瞬断

落雷などによって発電所などの施設が一時的に使用不可になると、電力会社は電源の供給ルートを切り替えるなどの措置によって電力の供給を継続させます。その際に、供給ルートを切り替えるために要したわずかな時間(数秒～数分)のみ、コンセントからの電力の供給が途切れることがあります。このような現象のことです。

MDM

Mobile Device Management。スマートフォンなどの携帯端末の情報セキュリティを管理するための機能及び管理体制のことです。管理者の許可なく携帯端末にソフトウェアをインストールすることを禁止したり、ウイルス対策ソフトのインストールやアップデートを強制したりすることです。

ミラーリング

同じデータを複数のディスクに冗長保存して安全性を高めるときに、メインのディスク装置と冗長ディスク装置の2

つを、常に同一の内容に保つことです。

遠隔バックアップ

遠隔地に用意したバックアップ用のサーバに、ネットワーク経由でバックアップデータを送信して保存させることで、バックアップを円滑に実行することです。

クリアデスク

JIS Q 27002で規定されている方針の一つで、離席時や帰宅時に、机の上の書類などを全て収納することで、機密情報が他人に知られないようにすることです。

クリアスクリーン

JIS Q 27002で規定されている方針の一つで、離席時にPCをログオフするか、スクリーンセーバなどで画面の内容を隠すことで、機密情報が他人に知られないようにすることです。

USBキー

USBにログイン用の情報を記録し、本人だけがPCを起動できるようにするための装置です。USBキーを装着していないとPCを起動できないので、USBキーをもっていない他人は勝手にPCを使用できなくなります。

セキュリティ実装技術

IPsec

インターネットなどの開かれたネットワーク上において、専用線と同様にセキュリティの確保された通信を行うための暗号化・認証プロトコルです。

トンネルモード

IPsecのうち、IPヘッダも含めたIPパケット全体を暗号化し、新たなIPヘッダを付加して受信側に送付する方法です。元の送信元・宛先IPアドレス自体を隠蔽できるため、安全性が高くなっています。しかし、もともとの送信元や宛先のIPアドレスは、暗号化によって経路上のルータなどからは読み取れなくなるため、発信ホストと受信ホストの間で暗号化したIPパケットを直接送受信することはできません。

トランスポートモード

IPsecのうち、IPパケットのデータ部のみを暗号化して送付する方法です。このモードでは、IPパケットのヘッダ部は暗号化されないため、もともとの発信側システムや受信側システムのIPアドレスをそのまま利用して通信を実行で

きます。そのため、発信ホストと受信ホストの間の全経路でデータが暗号化されます。

SSL/TLS

Secure Socket Layer/Transport Layer Security。Web上で安全なデータ送受信を行うためのプロトコルであり、共通鍵暗号方式と公開鍵暗号方式を組み合わせることで、通信相手との安全な鍵交換と暗号化を実現します。

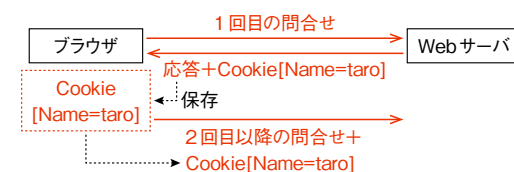
クライアントとWebサーバ間での、SSL/TLSの暗号化・データ送付の一般的な手順の概要を示すと、以下のとおりとなります。

- ①データの暗号化・復号に使用するための共通鍵を生成し、クライアントはその共通鍵を、Webサーバの公開鍵で暗号化してからWebサーバに送付する。
- ②Webサーバは、暗号化されて送付されてきた共通鍵を、Webサーバの秘密鍵で復号し、共通鍵を安全に入手する。
- ③以後、クライアントとWebサーバの間で共有できた共通鍵を用いて、データを暗号化して送受信する。なお、共通鍵を用いてデータの暗号化を行うのは、共通鍵の方が公開鍵よりも暗号化や復号に要する時間が短く、処理を高速に実行できるためである。

SSH

Secure Shell。リモートログイン(遠隔にあるコンピュータの操作)やリモートファイルコピーなどを、通信経路上のデータを暗号化した上で行えるツール及びプロトコルのことです。SSHには利用者認証機能も存在します。

Cookie



Nameの値がtaroであるという情報を、ブラウザに保存できる

Webサーバとブラウザとの間のセッション(データ送受信の順序及びその状態)の管理や、Webサーバに対するアクセスがどのPCからのものであるかを識別するために用いられるものです。CookieはWebサーバからブラウザに渡され、利用者のコンピュータのハードディスクに記録されます。そして、ブラウザからWebサーバへのアクセス時に必要に応じてWebサーバに送信され、利用されます。

パケットフィルタリング

ファイアウォールなどが行うパケット検証動作で、送信元IPアドレスなどの値を参照し、パケット送受信に関するルール(フィルタリングルール)に違反しているパケットを遮断することで、不正侵入などを防ぐことです。

ページアンフィルタリング

フィルタリングを行うソフトウェアが迷惑メールに含まれる特徴的な語句などを収集・解析して自己学習を行い、迷惑メールかどうかを統計的に解析して判定する、迷惑メール検知手法のことです。

ダイナミックパケットフィルタリング

次の方法で行うパケットフィルタリングのことです。

- ① 社内のPCを送信元、インターネット上のサーバを宛先とし、送信元ポート番号を任意の値、宛先ポート番号を特定のサービスのポート番号とする、サーバ上のサービスの利用を依頼するリクエストパケットだけをフィルタリングテーブルに掲載し、通過を許可する。

送信元 IPアドレス	宛先 IPアドレス	送信元 ポート番号	宛先 ポート番号
社内のPC	WebサーバA	任意	80

(WebサーバAはHTTP(ポート番号80)サービスを提供している)

- ② 次のようなフィルタリングテーブルを用意して、①のリクエストパケットに対応するレスポンスパケットの通過を常に許可していると、外部からの不正なパケットを侵入させてしまう可能性がある。

送信元 IPアドレス	宛先 IPアドレス	送信元 ポート番号	宛先 ポート番号
社内のPC	WebサーバA	任意	80
WebサーバA	社内のPC	80	任意

2行目のパケットを常に許可すると、社内のPCを宛先とし、送信元IPアドレスをWebサーバAのIPアドレスに偽装している、送信元ポート番号を80、宛先ポート番号を任意とした攻撃用のパケットの通過が許可されてしまう。

- ③ したがって、レスポンスパケットをフィルタリングテーブルに掲載しないようにしておき、リクエストパケットがファイアウォールを通過したとき、それに対応する適切なポート番号をもつレスポンスパケットだけ、一時的に通過を許可する。

例えば、社内のPCからWebサーバAに対して、送信元ポート番号を2000、宛先ポート番号を80とするリクエストパケットが送信されてファイアウォールで通過を許可したとき、次のような行を一定時間だけフィルタリ

ングテーブルに掲載し、WebサーバAから返ってくる正当なレスポンスパケットだけ通過を許可する。

送信元 IPアドレス	宛先 IPアドレス	送信元 ポート番号	宛先 ポート番号
社内のPC	WebサーバA	任意	80
WebサーバA	社内のPC	80	2000

(網掛け部分＝一定時間だけフィルタリングテーブルに掲載する行)

MACアドレスフィルタリング

ネットワーク上を流れるフレームの送信元MACアドレスを検査し、許可された送信元MACアドレスのフレームだけを通過させることで、不正な接続元からのアクセスを拒否することです。

ブラックリスト

WAFにおいて、攻撃用のスクリプトコードなどの問題のある通信データパターンを定義したものです。送信されてきたIPパケットがブラックリストに該当する場合、WAFはそのIPパケットを遮断するか、無害化します。

ホワイトリスト

WAFにおいて、問題のない正常な通信データパターンを定義したものです。

VLAN

PCやネットワーク機器が物理的に接続されている状況において、論理的にネットワークを分割できる機能のことです。

VLAN機能をもつスイッチは、自らがもつ各ポートを、それぞれ異なるネットワークに所属するように分割できます。スイッチによって分割されたポートに到達したフレームは、自分の所属するネットワーク以外のネットワークのポートには送付されなくなります。

リバースプロキシ

内部ネットワークやDMZ上に設置されるサーバで、外部(インターネット)から社内のWebサーバなどに向けて到達する要求をいったん受け取ったうえで、各要求を適切なサーバに割り振る機能をもっているサーバのことです。リバースプロキシには、Webサーバなどの静的コンテンツをキャッシュし、同一Webサーバ上の同じページへのアクセスが外部から何度も到達する場合、キャッシュしたデータを返すことによってWebサーバの負荷を低減させることで、アクセス性能を改善させる効果があります。また、リバースプロキシ上で強固なセキュリティ対策を実現する

ことで、外部からの不正アクセスから社内LAN上のWebサーバなどを防御できる効果を得ることもできます。

バッファオーバーフロー

メモリのスタック領域中に確保されていた配列に、その配列の大きさを超える長さのデータを書き込むことで、配列の直後に位置する別の変数または戻りアドレスの領域の内容を上書きし、不正なプログラムを実行させる攻撃手法のことです。

SMTP-AUTH

メール送信時にメールサーバ(SMTPサーバ)とユーザクライアント間でアカウントやパスワードを用いた利用者認証を行い、正式なパスワードによる認証が成功した場合だけ、ユーザにメールの送信を許可するためのプロトコルです。

TPM

Trusted Platform Module。鍵ペア(公開鍵及び秘密鍵)の生成、公開鍵暗号方式による暗号化や復号、共通鍵作成のために必要な乱数の生成、プラットフォームの完全性の検証などを行うことができる、セキュリティチップのことです。「プラットフォーム」とは、コンピュータを構成するOSやハードウェアなどをまとめたものです。TPMは、通常はコンピュータのマザーボードに埋め込まれています。

知的財産権

著作権法

著作物(思想または感情を創作的に表現したもの)を作成した人(著作者)が、自分の著作物を独占的に使用したりする権利(著作権)を定義している法律です。

日本の著作権法では、著作物の作成と同時に作者にその著作権が与えられるとしています(無方式主義)。また、プログラムを作成する際に利用するアルゴリズム(解法)、プログラム言語及び規約は、保護の対象にしません。プログラム自体は著作物として認められます。

不正競争防止法

「事業者間の公正な競争及びこれに関する国際約束の確実な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もって国民経済の健全な発展に寄与すること」を目的とした法律です。この法律では幾つかの行為を「不正競争」として定義し、不正競争によって営業上の利益を侵害された者などは、その侵害の停止などを請求する権利があると定めています。

営業秘密

不正競争防止法で保護されている対象で、「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」です。

セキュリティ関連法規

サイバーセキュリティ基本法

「サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること」を目的とした法律です。

サイバーセキュリティ

サイバーセキュリティ基本法における「サイバーセキュリティ」とは「**電子的方式、磁気的方式その他の知覚によっては認識することができない方式……により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置……が講じられ、その状態が適切に維持管理されていること**」をいいます。

不正アクセス禁止法

不正アクセス行為を禁止するための法律です。不正アクセス行為とは、特定電子計算機(コンピュータなど)の利用権限をもたない第三者が、他人のIDやパスワードを悪用して、アクセス制御機能による利用制限を免れて特定電子計算機を利用できる状態にする行為のことを指します。不正アクセス禁止法では、このような行為及びその助長行為を処罰の対象にしています。

刑法(ウイルス作成罪)

正式名称を不正指令電磁的記録に関する罪とする罪状で、刑法第168条の2で定義されています。

第168条の2 正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、3年以下の懲役又は50万円以下の罰金に処する。

一 人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録

二 前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録

個人情報保護法

個人情報の保護及び個人情報取扱事業者の義務などを定義している法律です。

個人情報：「この法律において「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう」（個人情報保護法第2条より引用）

個人情報取扱事業者：個人情報保護法では、「個人情報データベース等を事業の用に供している者」（個人情報保護法第2条より引用）を、個人情報取扱事業者と定義しています。個人情報取扱事業者は、個人情報の取得や利用などに関して、各種の義務を果たさなければなりません。

個人情報の利用目的による制限：個人情報取扱事業者は、個人情報の本人の同意をあらかじめ得ないまま、利用目的の範囲を超えて個人情報を取り扱ってはなりません。ただし、法令に基づく場合や人の生命などの保護のために必要であつて、かつ本人の同意を得ることが困難な場合などは、その限りではありません。

個人情報の取得・収集など：個人情報取扱事業者は、偽りその他不正の手段によって個人情報を取得してはなりません（個人情報保護法第17条より）。また、個人情報取扱事業者が個人情報を取得した場合は、「あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。」（個人情報保護法第18条より引用）と規定されています。

プロバイダ責任制限法

インターネット上で名誉毀損や他者の権利の侵害などが行われた場合に、その犯行者が契約しているプロバイダが負うべき責任（損害賠償の義務など）を規定している法律です（正式名称：特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律）。

特定電子メール法

特定電子メールの送信の適正化等に関する法律。広告宣伝などを目的として、利用者の許可なく送信される迷惑メールなどの送信を規制するための法律です。

特定電子メールは「電子メールの送信（国内にある電気通信設備（電気通信事業法第二条第二号に規定する電気通信設備をいう。以下同じ。）からの送信又は国内にある

電気通信設備への送信に限る。以下同じ。）をする者（営利を目的とする団体及び営業を営む場合における個人に限る。以下「送信者」という。）が自己又は他人の営業につき広告又は宣伝を行うための手段として送信をする電子メールをいう」

コンピュータ犯罪防止法

コンピュータ（電子計算機）に関連した犯罪を適切に処罰するため、1987年に改正された刑法の一部の条文と、そこに盛り込まれた各種罪状のことです。

電子計算機使用詐欺罪：刑法第246条の2に規定されている罪状で、他人の事務処理に使用する電子計算機に虚偽の情報などを与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、または財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得たり、又は他人にこれを得させたりする行為が該当します。

電磁的記録不正作出及び供用の罪：他人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務または事実の証明に関する電磁的記録を、コンピュータを利用して不正に作成した者は、5年以下の懲役または50万円以下の罰金に処すると定められています。

電子計算機損壊等業務妨害罪：他人が利用している業務用コンピュータに虚偽の指令やデータなどを入力して、コンピュータの使用目的に反する動作などをさせ、他人の業務を妨害する行為のことです。

労働関連・取引関連法規

労働基準法

労働に関する各種条件や罰則などについて規定した法律です。

第一条 労働条件は、労働者が人たるに値する生活を営むための必要を充たすべきものでなければならない。

2 この法律で定める労働条件の基準は最低のものであるから、労働関係の当事者は、この基準を理由として労働条件を低下させてはならないことはもとより、その向上を図るよう努めなければならない。

請負契約

注文者（委託元事業主）から委託された作業を請け負った請負人（委託先事業主）が作業の完成に責任をもち、納期までに必ず作業の成果物を引き渡すことを約束する契約形態です。

請負契約では、委託先事業主が雇用している従業者が、

委託先事業主の指揮命令の下で開発作業を行います。委託元事業主には、従業者に対する指揮命令の権限はありません。

派遣契約

派遣先事業主から依頼を受けた派遣元事業主が、雇用している労働者を派遣先事業主に派遣して、派遣先事業主の指揮命令の下で作業をさせる契約形態です。

労働者派遣法

派遣契約などについて定義している法律です。

第1条「労働力の需給の適正な調整を図るため労働者派遣事業の適正な運営の確保に関する措置を講ずるとともに、派遣労働者の保護等を図り、もって派遣労働者の雇用の安定その他福祉の増進に資することを目的とする」

コピーレフト

著作権(copyright)に対して、著作権を著作者が保持したままで、著作物の利用や改変、及び二次的著作物の作成などを誰でも自由に実行できるという考え方です。

NDA

Non-Disclosure Agreement, 秘密保持契約。公表していない新製品の情報などを取引先から提示されたりしたとき、それを勝手に公開したり不正に利用したりしないことを要求する契約です。

その他の法律・ガイドライン・技術者倫理

コンプライアンス

法令や社会規範(社会常識)、業界内での規則や企業倫理など、企業が守るべき各種の法律・規則・規範などを適切に遵守するため、それらに関するマニュアルなどを整備し、法令や社会規範を遵守した企業活動を行うことです。

クラウドサービス利用のための情報セキュリティマネジメントガイドライン

クラウドコンピューティングを利用したサービスに関して、経済産業省が2011年に公表したガイドラインです。序文は次のとおりです。

国内の組織の情報セキュリティには、国際的な規格(ISO/IEC 27002:2005)に準拠したJIS Q 27002:2006情報

技術—セキュリティ技術—情報セキュリティマネジメントの実践のための規範(以下「JIS Q 27002(実践のための規範)」という。)に基づく管理策の実施が推奨されており、実際に多く利用されている。……組織がITを所有せずに全面的にクラウドコンピューティングを利用する場合には、この管理策が求める事項だけでは組織の情報セキュリティを確保するためには不足があるのが実情である。

そのため、クラウド利用者の視点からJIS Q 27002(実践のための規範)の各管理策を再考し、クラウドコンピューティングを利用する組織においてこの規格に基づいた情報セキュリティ対策が円滑に行われることを目的として、このガイドラインを作成した。

標準化関連

ISO/IEC 15408 (Common Criteria)

情報システムのハードウェアやソフトウェアに関するセキュリティの保証レベルを評価するための国際規格です。この規格にはEAL(Evaluation Assurance Level, 評価保証レベル)という評価基準があり、セキュリティ評価の厳格さのレベルを示します。このEALにはEAL1(最も緩い)からEAL7(最も厳しい)まで存在します。

JIS

日本工業規格(Japanese Industrial Standards)。工業製品やコンピュータ技術などに関するわが国の国家標準です。

プライバシーマーク

個人情報保護マネジメントシステムに関する要求事項を定義した規格であるJIS Q 15001において、要求事項を満たしている事業者に与えられるマークです。このマークをWebサイトなどで使用することが許可されている事業者は、個人情報保護に関して一定の基準を満たしていると考えられます。

IEEE

The Institute of Electrical and Electronics Engineers, Inc. 米国の電気工学・電子工学学会で、IEEE 802シリーズなどの各種規格を公表しています。

NIST

National Institute of Standards and Technology, アメリカ国立標準技術研究所。米国の技術革新などのために、計測技術や情報処理技術などを促進させるための活動を

行っています。

デジュレスタンダード

JISなどの標準化団体が正式に制定・公表した技術標準(スタンダード)のことです。

デファクトスタンダード

標準化団体が定めた公的な規格ではなく、市場において広く利用された結果、事実上の技術標準となった各種規格のことです。TCP/IPなどが該当します。

システムの構成

集中処理

スーパーコンピュータなど、高性能のコンピュータが全ての処理を集中して実行するシステムのことで、

分散処理

複数のコンピュータに処理を分散させることで、高速化や負荷分散を図るシステムのことで、

機能分散: 複数の異なる機能を、それぞれ異なるコンピュータに分配することです。

負荷分散: 同じ機能の処理データを複数のコンピュータに配分し、同時並行的に処理させることで負荷分散を図ります。

対話型処理

ディスプレイに表示されるコンピュータからのメッセージを利用者が確認し、キーボードやマウスを用いて利用者が処理内容を入力していくことを繰り返して、あたかもコンピュータと人間が対話するようにして処理をすることです。

デュアルシステム

機器構成などが同一で、同一の処理を行うためのシステムを二つ用意し、両者に並行して処理を実行させる方式です。この方式では常にお互いの処理結果を照合して、システムに異常のないことを確認しています。障害発生時は、障害の発生したシステムを切り離して、正常なシステムのみで運転を継続します。

デュプレックスシステム

「運用系」と「待機系」の2つのシステムを持つ形態です。通常のシステム運用においては運用系を常時稼働させ、待機系は待機させたり停止させたりします。運用系に障害が発生して処理が不可能になったとき、待機系に切り替えて

処理を続行させます。

コールドスタンバイ

デュプレックスシステムの方式の一つで、システムの予備機(待機系)を通電せず、稼働させない状態で待機させておき、障害発生時には予備機の電源を入れて立ち上げ、切り替える方式です。

ホットスタンバイ

デュプレックスシステムの方式の一つで、システムの予備機(待機系)を、OS及び業務用プログラムが稼働した状態で待機させておき、運用系の状態を監視させます。待機系は運用系の障害を検知すると、運用系が行っていた処理を直ちに引き継ぎます。

ウォームスタンバイ

デュプレックスシステムの方式の一つで、OSのみが稼働した状態でシステムの予備機(待機系)を待機させておき、障害発生時には予備機の業務用プログラムを起動して、システムを切り替える方式です。

クライアントサーバシステム

処理要求をサーバに送信して処理を代行してもらう立場のコンピュータである「クライアント」と、クライアントから要求された処理を実行し、その結果をクライアントに返す「サーバ」の、2種類のコンピュータによって処理を行うシステムです。サーバが行う機能を「サービス」として扱っており、各サーバは自分の実行すべき機能を、サービスとして各クライアントに提供しています。

クラウドコンピューティング

ネットワーク上に存在する複数のサーバなどの資源を提供することで、スケラビリティ(拡張性)やアベイラビリティ(可用性)の高いサービスを利用できるようにすることです。サーバの一部に障害が発生しても、ネットワーク上の別のサーバを動的にシステムに組み込むことで、障害発生前と同じ構成でサービスを継続できるので、可用性が高くなります。また、使用するサーバの台数を増加したい場合も、ネットワーク上の別のサーバを追加するだけでシステムの規模を容易に拡張できるので、拡張性が高くなります。

SaaSなどのサービスモデル

NISTが制定した、クラウドコンピューティングに関するサービスモデルです。SaaS, PaaS, IaaSなどがあります。

サービスモデル	定義
IaaS (Infrastructure as a Service)	サービス事業者は、ハードウェアやネットワーク機器といったサービスのインフラだけを提供する。利用者は、OS及びアプリケーションソフトウェアを導入してシステムを運用する。利用者には、インフラの管理やコントロールを行う権限はないが、OSに関する設定を行ったり、セキュリティパッチを適用したりする権限がある。
PaaS (Platform as a Service)	サービス事業者は、インフラに加えてサーバ上で稼働するOSも提供する。利用者は、アプリケーションソフトウェアを導入してシステムを運用する。利用者には、インフラの管理やコントロールを行う権限はなく、OSに関する設定やセキュリティパッチ適用を行う権限もない(OSはサービス事業者が所有しているため)。
SaaS (Software as a Service)	サービス事業者は、インフラとOSに加えてアプリケーションソフトウェアも利用者に提供する。PaaSと同様に、利用者には、インフラの管理やコントロールを行う権限はなく、OSに関する設定を行ったり、セキュリティパッチを適用したりする権限もない。

シンククライアントシステム

データをサーバだけに保有させることで、端末からの情報漏えいを防ぐシステムのことで、利用者が使用する端末は、ハードディスクをもたないためデータを内部に保存できないシンククライアント端末とします。シンククライアント端末が社外で紛失したり盗まれたりしても、内部にはデータが存在しないので、機密情報が知られることはありません。

RAID

複数のディスクを用いて信頼性向上やアクセス速度の向上を図る技術です。RAIDでは、ミラーリングとディスクストライピングによって、信頼性やアクセス速度を向上させています。

ミラーリング: 同じデータを複数のディスクに冗長保存して安全性を高めること。

ディスクストライピング: データを複数のディスクに分散して保存し、並行アクセスによりアクセス時間を短縮すること。

NAS

Network Attached Storage。ネットワークに直接接続して使用可能なストレージ(記憶装置)です。磁気ディスクとコントローラ(NASゲートウェイ)からなり、コントローラ内には専用のOSなどが格納され、ネットワーク内からのファイルの参照・更新などの問合せに応答する働きをします。

SAN

Storage Area Network。コンピュータやサーバなどを接続しているLANとは別に、高速な専用ネットワークを用意して、ストレージを接続している構成のことで、

フォールトトレラント

何らかの障害が発生してシステムが部分的に故障しても、システムの稼働を停止せず、業務を継続できるように構成されたシステムのことで、

フェールセーフ

異常発生時にはシステムを停止させるか、人間系(オペレータなど)に処理の続行判断を委任するなどして、より安全な状態にシステムを導く方式のことで、

フルプルーフ

人間の過失などが原因でシステムが予期されない使い方をされても、信頼性や安全性を損なわないようにすることです。例えば、利用者が誤った操作をしても適切なエラーメッセージを表示して再入力を促し、システムに異常が起らないようにすることなどです。

ヒューマンエラー

勘違い、見間違いまたは操作ミスなど、人間特有の誤りによってシステムなどを誤動作させたり、適切な処理を実行できなくさせたりすることです。

システムの評価指標

レスポンスタイム

利用者がシステムへの入力を終了したときから、出力が開始されるまでの経過時間のことで、

ターンアラウンドタイム

利用者がシステムへの入力を開始したときから、結果の出力が終了するまでに経過した時間のことで、

スループット

単位時間内におけるジョブの処理件数のことで、

MTBF

Mean Time Between Failures。システムの稼働率を求めるときに利用する指標で、システムの稼働時間の合計を故障回数で割った値です。

MTTR

Mean Time To Repair。システムの稼働率を求めるときに利用する指標で、故障したシステムの修理に要した時間の合計を、故障回数で割った値です。

稼働率

システムが稼働している確率を表す指標です。右の式で求めます。

$$\frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

イニシャルコスト

システムを導入するときに要する初期費用(機器の購入費、ソフトウェアの開発費用など)です。

ランニングコスト

システムを正常に運用するために定常的に発生する費用(人件費、光熱費など)です。

データ操作

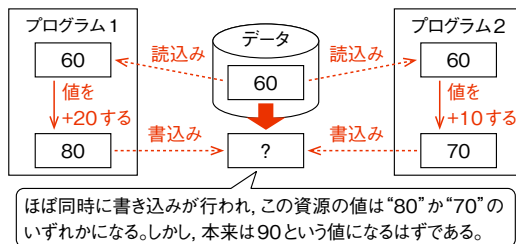
SQL

関係データベース管理システムのテーブル(表)に対して検索、挿入、更新または削除を行ったり、関係データベースやテーブルの属性を管理したりするために用いられるコマンド及び言語体系のことです。

トランザクション処理

排他制御

複数のプログラムが同じデータの参照や更新を同時に行うと、データの値に不整合が生じてしまうことがあります。このような事態を防ぐため、一つのプログラムがデータにアクセスしている間は、他のプログラムを待機させる必要があります。この制御を排他制御といいます。



ロック

データにアクセスしようとするプログラムが、同時に稼働している他のプログラムからのデータへのアクセス(読取り・書き込み)ができないように規制をかける操作のことです。

共有ロック:他のプログラムからの共有ロックは許容し、占有ロックは排除する。

占有ロック:他のプログラムからの共有ロック、占有ロックを排除する。

バックアップ方式

データのバックアップを取得する方式には次のようなものがあります。

フルバックアップ方式:データベースの全体をバックアップする方式です。

差分バックアップ方式:直前に実施したフルバックアップ後に更新されたファイルだけをバックアップの対象にする方式です。差分バックアップ方式の方が、バックアップの際に外部記憶媒体などに保存するファイル数が少ないので、処理時間はフルバックアップ方式よりも短くなります。障害復旧時には、前回のフルバックアップのほかに、障害発生時点までの差分バックアップのファイルもデータベースに復元しなければならないため、復旧にかかる時間は長くなります。

データベース応用

データウェアハウス

意思決定などの支援用に、目的別に蓄積・編成され統合化されたデータの集まりのことです。データウェアハウスに蓄積された、企業のさまざまな活動を介して得られた各種のデータは、過去の売上の傾向の分析などに使用されます。

メタデータ

「データのデータ」という意味の用語です。データの内容、容量及び存在位置などを、要約してデータとして記録するものです。

ビッグデータ

科学、商業などの各分野において、通常データベース管理システムでは管理することが困難になるほどの、大量のデータを管理・分析すること、及びそのために用意される膨大な量のデータの集合のことです。

ネットワーク方式

LAN

Local Area Network。企業や個人の敷地内など、比較的狭い範囲に構築されるネットワークのことです。

WAN

Wide Area Network。都市間、国と国との間など、広範囲にわたって専用回線や通信装置を敷設することで構築される大規模なネットワークのことです。

TCP/IP

インターネット上の機器がデータの送受信を行うときに用いる各種通信プロトコルの総称です。最上位(利用者に最も近い)のアプリケーション層、トランスポート層、インターネット層及び最下位のインタフェース層からなり、各層に複数のプロトコルが存在しています。

アプリケーション層	HTTP (80), HTTPS (443), SMTP (25), POP3 (110), IMAP4 (143), FTP (20, 21)	DNS (53), DHCP (67, 68), SNMP (161,162), NTP (123)
トランスポート層	TCP	UDP
インターネット層	IP, ICMP	
インタフェース層	PPP, CSMA/CD, CSMA/CA, ARP, RARP	

(括弧内はポート番号、試験センタ公表のシラバスに準拠)

ルーティング

ルータがパケットを中継するとき、宛先IPアドレスの値を参照して、適切な送信先を選択してパケットを転送することです。

グローバルIPアドレス

他の組織との間で通信を行うための、通常のIPアドレスのことです。各国のIPアドレスを管理している組織(日本ではJPNIC、日本ネットワークインフォメーションセンター)に申請して割当てを受ける必要があります。

プライベートIPアドレス

組織内の各コンピュータに対して、その組織内のみの通信で使用する限り、各コンピュータに任意の値を設定できるIPアドレスです。

DNS

Domain Name System。インターネット上の組織(ドメイン)を識別するための“example.com”のような名称をドメイン名、“www.example.com”のような特定のホストを一意に識別するために付けられたホスト名をFQDN (Fully Qualified Domain Name) といいます。ドメイン名やFQDNに対応するIPアドレスの問合せを受け付け、適切

なIPアドレスを返すためのシステムのことをDNS (Domain Name System)といいます。

RADIUS

ネットワーク上のサーバなどに対する利用者からのアクセスの認証と、利用者がサーバなどを利用した事実の記録、及びアカウント情報の管理などを、ネットワーク上の認証サーバで一元化して行うことを目的としたプロトコルです。RADIUSでは、クライアントは認証サーバ(RADIUSサーバ)にメッセージを送ることで認証要求を行います。認証要求を受け取った認証サーバは、パスワードを照合するなどの方法で認証の可否を確認し、認証可能な場合はクライアントに認証結果を返します。

データ通信と制御

光ファイバ

屈折率の異なる石英ガラスなどの素材を用いた通信ケーブルで、光を伝送するために用います。内側の屈折率の高い素材(コア)を外側の素材(クラッド)で覆い、コアだけが光を透過させるようにすることで、遠距離に光を伝送できるようにしています。

FTTH

Fiber To The Home。光ファイバ回線を一般家庭や企業の敷地内に引き込み、インターネット接続などのサービスを提供することです。

LAN 間接続装置

コンピュータやサーバをLANに接続したり、LANの大きさを拡張したりするために使用する装置です。リピータ、スイッチングハブ、ルータ及びゲートウェイなどがあります。

リピータ

TCP/IPのインタフェース層での中継を行い、伝送されてくるデータの信号波形を増幅・修正するための装置です。

スイッチングハブ

TCP/IPのインタフェース層での送信制御や通信の中継を行うための装置です。送られてきたフレームの宛先MACアドレスを参照し、その宛先MACアドレスをもつ機器が存在するポートだけにフレームを転送します。

ルータ

TCP/IPのインターネット層において、複数のLANを相互

接続する装置です。受信したIPパケットの宛先IPアドレスを参照して、適切な送信先に転送する機能(ルーティング機能)をもちます。

ゲートウェイ

TCP/IPのトランスポート層及びアプリケーション層において、複数のLANを相互接続する装置です。

通信プロトコル

サブネット

LAN全体を細分化して小規模なネットワークを複数作成する際に用いられる技術です。この技術によって分割した小規模なネットワークのことをサブネットと呼びます。

MACアドレス

機器に搭載されたNIC(Network Interface Card)を一意に識別するためのアドレスのことです。48ビットで構成されます。

MACアドレスは1バイトずつハイフンで区切った16進で表記します。

例 1A-B6-CC-00-10-FE

IPv4

TCP/IPにおいて、コンピュータやサーバなどの機器を全世界中で一意に識別するために付与されるアドレス及び関連するプロトコルの総称です。IPv4のIPアドレスは32ビット(4バイト)で表現され、1バイト＝8ビットずつピリオドで区切り、10進数で表記します。

IPv6

次世代のIPアドレス及び関連する通信プロトコルです。IPv6は128ビットの長さのIPアドレスをもち、ネットワーク部とホスト部という区分がなくなったことや、プラグアンドプレイ機能が追加されたことなどの特徴があります。また、IPv6ではアドレスを16進数で表記し、4文字(16ビット)ずつコロン“:”で区切る表記法を用いています。

IPv6アドレスの例:

2001:0db8:0000:0000:1111:1111:0001:000A

HTTP

Hypertext Transfer Protocol。インターネット上のWWWサービスにおいて、ブラウザがWebサーバ上のWebページや画像などを閲覧する際に用いられます。

HTTPS

HTTP over TLS。HTTPに暗号化・認証の機能をもたせたもので、パスワードやクレジットカード番号など、盗聴されてはならない情報をブラウザとWebサーバ間で送受信するために用いられます。

SMTP

Simple Mail Transfer Protocol。メールサーバ間でメールを送受信するときに使用されるプロトコルです。

POP3

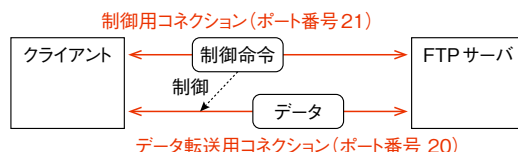
Post Office Protocol version3。メールサーバのメールボックスから、受信者のメールクライアントが電子メールを取り出すために用いられるプロトコルです。POP3では、メールボックスから電子メールをダウンロードして、メールボックス上のダウンロード済みメールを削除することが前提となっています。

IMAP4

Internet Message Access Protocol version4。受信者のメールクライアントが、メールサーバのメールボックスを参照して電子メールを確認するために用いられるプロトコルです。IMAP4ではメールボックスに電子メールを保存し続けることが前提です。

FTP

File Transfer Protocol。クライアント(PCなど)とサーバとの間でファイル転送を行うためのプロトコルです。



ネットワーク応用

MIME

Multipurpose Internet Mail Extensions。電子メールの伝送プロトコル(SMTP)上で画像や音声などの添付ファイルを送信できるようにした規格です。SMTPでは先頭ビットが0のASCII文字しか扱えず、先頭ビットが1のバイトが含まれる画像などのバイナリデータは送信できませんでした。MIMEでは、バイナリデータをASCII文字に変換(エンコード)するプロトコル(BASE64)を用いて、電子メール上でバイナリデータを送信できるようにしています。

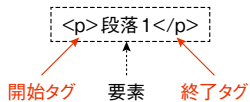
ブラウザ

WWWサービスにおいて、Webサーバ上で公開されているWebページや画像などを閲覧するために用いられるソフトウェアです。Microsoft社のInternet ExplorerやMozillaのFirefoxなどがあります。

マークアップ言語

Webページなどの文書データを作成するための言語で、文書内の要素(段落、箇条書きなど)をタグで表現します。

<タグの例>



HTML

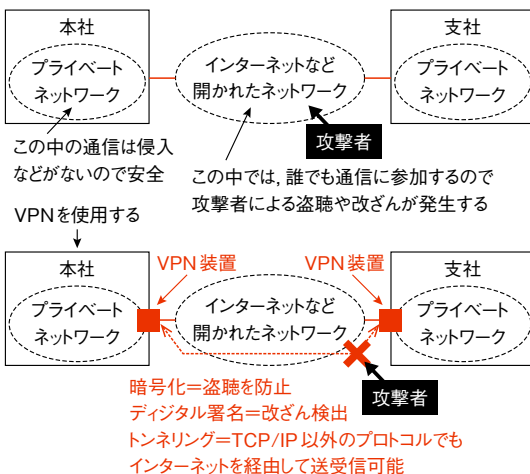
Hypertext Markup Language。Webページを作成するための言語です。あらかじめ決められたタグ(要素)しか使用できず、独自タグを定義することはできません。

XML

Extensible Markup Language。任意の名前の独自タグ(要素)を定義して使用することが可能です。要素の名前などの定義は、文書型定義(DTD)というファイルに記述し、XMLファイルは文書型定義ファイルを読み込んで、要素の名前や構成などを把握します。

VPN

インターネットなどの開かれたネットワーク上で、専用線と同等にセキュリティが確保された通信を行うことで、あたかもプライベートネットワークを利用しているかのようになるための技術のことです。トンネリングや暗号化技術などが用いられます。



トンネリング

あるプロトコルのパケット全体をデータとみなし、別のプロトコルのヘッダを付加して、別のプロトコルのパケットとして送受信すること。例えば、本社や支社のプライベートネットワークでTCP/IP以外のプロトコルを使っている場合、VPN装置がトンネリングすることで、TCP/IPのパケットとしてインターネット上で送受信することが可能になる。

EC

Electronic Commerce。インターネットなどのネットワークを利用して、商品の売買契約や取引などを行う商形態(電子商取引)のことです。ECには、「B to B (Business to Business)」、「B to C (Business to Consumer)」、「C to C (Consumer to Consumer)」の3つの取引形態があります。B to Bは企業間の取引、BtoCは企業と消費者間の取引、C to Cは消費者同士での取引を指します。

EDI

Electronic Data Interchange。電子商取引において使用される情報やその書式などを企業間で標準的なフォーマットとして統一し、ネットワーク経由でデータ交換を行う仕組みのことです。

IP電話

VoIPの技術を利用して、音声データなどをネットワーク上で送受信することで、利用者同士の会話などを実現する電話サービスのことで、

VoIP

Voice over Internet Protocol。アナログ音声をデジタルデータに符号化し、圧縮してデータサイズを縮小することでIPパケットに搭載して、IPネットワーク上で送受信する技術のことです。

LTE

Long Term Evolution。第3世代携帯電話(3G)の通信速度を向上させ、伝送遅延を軽減させた次世代の携帯電話通信規格です。通信速度は下りで100Mbps以上、上りで50Mbps以上となり、VoIP技術によって音声データを送受信します。

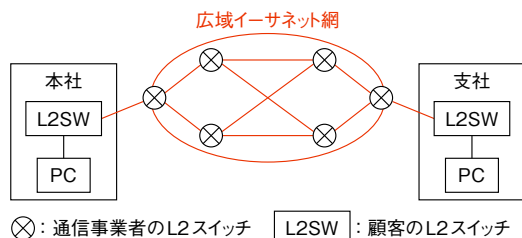
テザリング

携帯電話端末をモデムまたは無線LANのアクセスポイントのように用いて、PCやゲーム機などからインターネットに接続してデータ通信を行う機能のことです。

広域イーサネット

イーサネット技術を応用して作成されたWAN, 及びそれを用いて提供される接続サービスのことです。

通信事業者側のL2スイッチと、自社のL2スイッチなどを用いてイーサネット回線で接続することで、あたかも本社と支社とを直接イーサネット回線で接続したような状態で通信が可能になります。



IP-VPN

通信事業者が独自に開設している閉域通信網上で実現されるVPNです。MPLS (Multi Protocol Label Switching)を利用して、通信網上でパケットの高速通信を行います。

SIP

Session Initiation Protocol。マルチメディア通信のセッションの確立、変更及び切断を、2つのユーザエージェント間で実行するために利用される、汎用的なセッション管理用プロトコルです。VoIPにおいて通信相手とのセッション(論理的接続形態)を管理するために利用されます。

ベストエフォート

通信速度や可用性などを理論的な最大値に近づけるように提供者が最大限努力するものの、回線の混雑などの理由により、最大値未満の値になる可能性がある通信サービスのことです。

プロジェクトマネジメント

PDCA

プロジェクトを実行する際に、作業の結果を管理し、改善していくための仕組みのことです。Plan→Do→Check→Act→Plan→……の各フェーズを繰り返します。

Plan (計画): 計画を立案し、作業手順を決定する。

Do (実行): Planで決定した作業を実行する。

Check (点検): 作業の有効性などを定期的に点検し、改善点を見つけ出す。

Act (処置): Checkで発見された改善点の対策を立案し

たり、改善目標の設定を行ったりする。

プロジェクト

新しいシステムの開発など、特定の目標を実現するために立案する計画と、その計画をスケジュールどおりに実行することです。プロジェクトは日常の業務とは異なり、開始点と終了点を持ち、目標が実現された時点で終了するという有限性をもつことが特徴です。

プロジェクトマネジメント

プロジェクトの作業をスケジュールどおりに遂行させて目標を実現するために、作業内容、人員、費用、リスクなどを適切に管理することです。

プロジェクトステークホルダ マネジメント

ステークホルダ

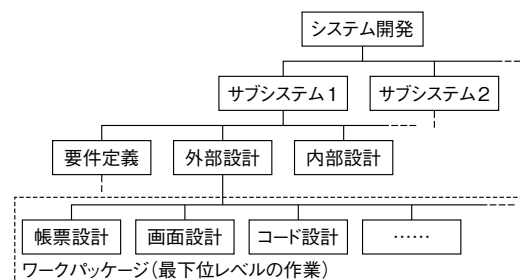
プロジェクトの利害関係者のことです。プロジェクトの成果物を使用して業務を行う利用部門や、プロジェクトに必要な資材などを供給する納入業者、及びプロジェクトの参加者などがステークホルダになります。また、プロジェクトによって利益を受ける者だけでなく、不利益を受ける者もステークホルダになります。

プロジェクトスコープマネジメント

WBS

Work Breakdown Structure。システム開発において必要な作業を、大きいものから小さいものへと細分化し、切り分けたものです。

<WBSの例>



アクティビティ

WBSのワークパッケージを、作業時間や作業者などを具体的に割り当てられるレベルにまで、さらに細分化した作業のことです。

ベースライン

プロジェクトマネジメントの計画プロセスにおいて決定し、顧客やプロジェクトマネージャから承認を受けたプロジェクトの実行計画のことです。プロジェクトの遂行中に機能の追加や変更が発生した場合は、ベースラインと実績の作業量とを比較することで、両者間の差異や作業の進捗を管理します。

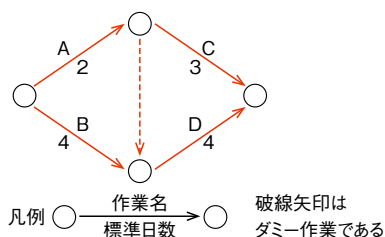
プロジェクトタイムマネジメント

アローダイアグラム

順序関係がある複数の作業の実行順序を、矢印と丸印からなるネットワーク図で表現したものです。

作業	標準日数	先行作業
A	2	—
B	4	—
C	3	A
D	4	A, B

＜アローダイアグラムの例＞



サービスマネジメント

サービスレベル合意書(SLA)

Service Level Agreement。各種サービスの品質について、そのサービスの利用者と提供者との間でなされた合意（契約内容なども含まれることがある）のことです。

サービスの設計・移行

システムの移行

旧式化したシステムの使用を停止して新しいシステムを開発・使用するために行う、システムの廃止、古い機器の撤去、新しいシステムの導入など、一連の業務のことです。

運用テスト

実業務において発生が予想される量の負荷を与えて、開発中のシステムが正常に動作するかを検証するテストのことです。

サービスマネジメントプロセス

ディザスタリカバリ

地震などの災害によって受けた被害をできるだけ早く回復させ、事業を早期に再開させようとすることです。

RTO

Recovery Time Objective。ディザスタリカバリで用いられる指標の一つで、災害発生時から業務が再開されるまでに要する時間のことです。

RPO

Recovery Point Objective。ディザスタリカバリで用いられる指標の一つで、災害発生時刻と、業務データを復元できた時点の時刻との差です。災害発生からどれだけ近い時刻まで業務の状態を復元できるかの指標です。例えば、障害発生時点から24時間前までの業務データの復旧を保証するとき、RPOは24時間になります。

ITIL

Information Technology Infrastructure Library。1989年に英国政府の中央コンピュータ電気通信局によって作成・公表された、ITサービスマネジメントにおけるベストプラクティスをまとめたものです。

ITサービスマネジメント

コンピュータを使用したサービスの実行状況を適切に管理し、障害から早急に復帰できるようにして、常に高品質なサービスを提供できるようにすることです。

ITILの最新版であるITILv3では、ITサービスの主要な活動（ITILv3コア）を、次に示す五つの段階に分類しています。

- ① サービスストラテジ(サービス戦略)：サービスの設計、開発などを適切かつ効率的に実行するための戦略を立てること。
- ② サービスデザイン(サービス設計)：サービスの設計や開発を実行すること。
- ③ サービストランジション(サービス移行)：既存のサービスから新しいサービスに移行すること。
- ④ サービスオペレーション(サービス運用)：システムを運用して顧客にサービスを提供すること。
- ⑤ 継続的サービス改善：①～④のいずれかの段階において発見された問題点を改善し、より良いITサービスを提供すること。

インシデント

情報システムを利用したサービスが停止する原因となる出来事のことです。

インシデント管理

ITILのサービスオペレーションに含まれる活動(プロセス)で、発生したインシデントに対し、可能な限り迅速に通常のサービス運用を回復して、ビジネスへの悪影響を最小限に抑えることです。

問題管理

未知のインシデントの発生原因を究明し、それに対する解決策(是正措置)などを考案し、問題管理プロセスの後に実行される変更管理プロセスに当該解決策を提案することで、インシデントの発生を恒久的に防止することを目的とするプロセスです。

構成管理

構成管理データベースを用いて、ITサービス提供に必要な設備などを常に正しく把握し、他の各プロセスに効果的な情報を提供するプロセスです。

変更管理

問題管理プロセスから提出された変更要求の内容について、変更諮問委員会(CAB)が、変更に伴う影響を検証してインパクトや優先度の評価を行い、認可または却下を決定するプロセスです。

リリース及び展開管理

変更管理プロセスが認可した変更要求を実行し、システムを変更するプロセスです。

システム監査

情報セキュリティ監査基準

経済産業省が公表している、情報セキュリティ監査を監査人が行う際に利用すべき基準です。

情報セキュリティ監査の目的は、情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査人が独立かつ専門的な立場から検証又は評価して、もって保証を与えあるいは助言を行うことにある。

情報セキュリティ監査基準とは、情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを

目的とした監査人の行為規範である。

(情報セキュリティ監査基準より引用)

情報セキュリティ管理基準

経済産業省が公表している、組織体が効果的な情報セキュリティマネジメント体制を構築し、情報セキュリティに関するコントロールを適切に整備・運用するための実践規範です。

内部統制

内部統制

企業が自ら業務を適正に遂行していくために、従業員などを適切に管理する体制を構築して運用する仕組みのことです。

相互けん制(職務の分離)

内部統制によって不正などを検知するためには、ある従業員または部門が行った作業を、別の従業員または部門に検証させて作業の内容の正当性を確認させるなど、作業者と検証者とを分離し、相互にけん制させる必要があります。このような体制を相互けん制といいます。

ITガバナンス

ITを導入・活用する際の目的などを適切に設定し、企業が競争優位性を確立するために適切なIT戦略を策定することで、企業をあるべき方向に導いていくための組織能力や統率力のことです。

業務プロセス

BPR

Business Process Reengineering。生産性の向上や業務効率の改善などを実現するために、従来の組織形態や既存のビジネスルール、及び業務プロセスを抜本的に見直し、再構築することです。

要件定義

非機能要件

システムの使いやすさや処理性能・処理効率の高さ、処理時間の早さ、及び障害発生時の復旧時間の早さなど、要件定義の段階で定義される機能や要件(機能要件)とは直接の関係がない、システムの利用状況に関する各種の要素のことです。

調達計画・実施

RFP

Request For Proposal, 提案依頼書。システムを調達する側の企業(取得者)が, 発注する情報システムの概要や発注依頼事項, 調達条件及びサービスレベル要件などを明示し, ベンダに対して提案書の提出を依頼するための文書です。

RFI

Request For Information, 情報提供依頼書。取得者がRFPを作成するために必要な情報の提供を, ベンダに対して要請するための文書です。

RFQ

Request For Quotation, 見積依頼書。取得者からベンダに対して送付されるもので, 発注する情報システムの価格などの見積りの提出を依頼するための書類です。

経営・組織論

CIO

Chief Information Officer, 最高情報責任者。企業の経営戦略として情報資源を活用するための情報化戦略を, 立案・執行する情報統括役員のことです。

CEO

Chief Executive Officer, 最高経営責任者。企業の全業務を統括・執行する役員のことです。

CISO

Chief Information Security Officer, 最高情報セキュリティ責任者。企業の情報セキュリティ管理業務を統括・執行する役員のことです。

BCP

Business Continuity Plan。システムが地震や火災などの災害に見舞われても, 可能な限り早期にシステムを復旧させ, 業務を再開するために日ごろから立てておくべき計画のことです。ISO/IEC 27001では, ISMSを運用する際に, 災害発生後に重要な業務をできる限り早く復旧するために, 事業継続計画を策定して実施しなければならないとしています。

BIA

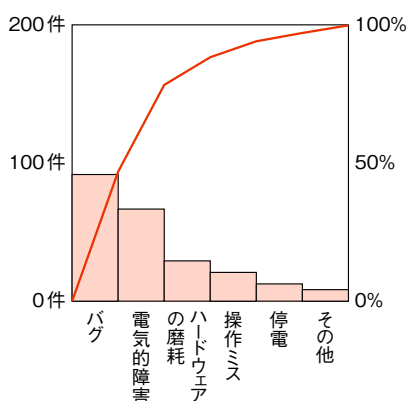
Business Impact Analysis, ビジネスインパクト分析。企業の主要な業務が障害によって停止させられたときの影響を分析し, 業務の優先度や目標復旧時間などを決定する段階のことです。

OR・IE

パレート図

各項目の値を表現する棒グラフと, 項目の値の累計値を表現する折れ線グラフを組み合わせた図法です。項目全体のうち, 重要な項目がどれであることを明確にするために用いられます。

＜パレート図の例＞



(原因ごとの障害の発生件数一覧)

データマイニング

通常業務において発生した大量のデータを蓄積し, それらを統計解析・ニューラルネットワークなどの統計的・数学的手法を用いて分析して, データの中に隠れた法則や因果関係などを算出する方法のことです。

ブレインストーミング

限られた時間内に, できるだけ多くのアイデアを得ることを目的とした会議の技法です。次の四つの原則に従い, 自由なアイデアを多数考え出すのが特徴です。

- ① 他人のアイデアを批判しない
- ② 自由奔放なアイデアを歓迎する
- ③ 質より量を重視する
- ④ 他人のアイデアに便乗したり, 複数のアイデアを合体させたりしたものも歓迎する

デルファイ法

統計的な予測方法では答えが得られにくい, 未来予測の

ような問題の最適解を求めるために用いられる予測技法のことです。

- ① 予測対象に従って、複数の専門家を選定し、アンケートを送付する。
- ② 専門家への質問に対する回答結果をフィードバックし、同じ専門家らに前回のアンケート結果を送付して意見の再考を促し、再度質問を行う。
- ③ ①から②を複数回繰り返して得た回答結果を統計的に処理し、確率分布とともに回答結果を示す。

会計・財務

損益計算書

会計期間中に発生した全ての収益と費用を記載し、収益から費用を減じて求めた利益(費用の額の方が大きい場合は、 $\text{収益} - \text{費用} = \text{利益}$ 、 $\text{費用} - \text{収益} = \text{損失}$ となる)を示した財務諸表のことです。

費用	収益
利益	

損益分岐点

収益と費用が一致し、利益がプラスマイナス0になるときの売上高のことです。

固定費：売上高の大小にかかわらず、常に一定の金額となる費用(広告費など)のこと。

変動費：売上高に比例して金額が増大する費用(売上原価など)のこと。

変動費率：売上高に対する変動費の額の割合($\text{変動費} \div \text{売上高}$)。

$\text{変動費率} = \text{変動費} \div \text{売上高}$

↓ 変形

$\text{変動費率} \times \text{売上高} = \text{変動費}$

損益分岐点では $\text{売上高} = \text{変動費} + \text{固定費}$ となります。

$\text{売上高} = \text{変動費} + \text{固定費} = \text{変動費率} \times \text{売上高} + \text{固定費}$

$\text{売上高} - \text{変動費率} \times \text{売上高} = \text{固定費}$

$\text{売上高} = \text{固定費} \div (1 - \text{変動費率})$

減価償却

企業の固定資産(建物や機材など)の価値を、每期償却(減らすこと)していき、その分だけ費用を計上することです。

固定資産は長期間にわたって使用するので、購入した年度だけ費用を計上し、以降の年においては費用を計上しないという方法では、その建物の利用期間と費用の計上期間が一致しないので不適切になります。よって、1,000万円の建物を購入したときは資産として1,000万円を計上

し、1年が経過するたびにその建物の価値を少しずつ減らして、その分だけの費用を計上していきます。

リース

コンピュータなどの機材の賃貸契約の一つで、リース会社が販売元から機材を一括で購入し、利用者に貸し出します。原則として利用者は中途解約ができません。

レンタル

コンピュータなどの機材の賃貸契約の一つで、リース会社が保有する機材を長期間にわたって提供し、不特定多数の利用者に貸し出して利益を得ることを目的としています。利用者は中途解約が可能です。

貸借対照表

特定の時点における、企業の所有する全ての資産、負債、及び純資産を表示するための財務諸表です。

資産	負債
	純資産

($\text{資産} = \text{負債(他人資本)} + \text{純資産(自己資本)}$ の関係となる)

キャッシュフロー計算書

会計期間中における、現金や現金同等物(キャッシュ)の出入りについて表すための財務諸表のことです。

営業活動によるキャッシュフロー

キャッシュフロー計算書の項目の一つで、税引前当期利益や減価償却費、売上債権の増減など、企業の本来の仕事(営業活動)を行う過程で得られたキャッシュ(収益など)や、消費されたキャッシュ(法人税等の支払など)の増減を示します。

投資活動によるキャッシュフロー

キャッシュフロー計算書の項目の一つで、有形固定資産(土地、建物、機械など)や無形固定資産(特許権、商標権など)の購入や売却といった投資活動に伴うキャッシュの増減が記載されます。

財務活動によるキャッシュフロー

キャッシュフロー計算書の項目の一つで、借入金の増減などの営業活動以外の活動、すなわち財務活動(借入金の支払いや自己資本の増加など)に関するキャッシュの増減が記載されます。

平成 **28** 年度 秋期

情報セキュリティ マネジメント

- 午前 問題 42
(全 50 問 試験時間：1 時間 30 分)
- 午後 問題 82
(全 3 問 試験時間：1 時間 30 分)

※ 327～328 ページに答案用紙がありますので、ご利用ください。

※ 「問題文中で共通に使用される表記ルール」については、325 ページを参照してください。

平成28年度 秋期 午前問題



問 1 ICカードとPINを用いた利用者認証における適切な運用はどれか。

- ア** ICカードによって個々の利用者が識別できるので、管理負荷を軽減するために全利用者に共通のPINを設定する。
- イ** ICカード紛失時には、新たなICカードを発行し、PINを再設定した後で、紛失したICカードの失効処理を行う。
- ウ** PINには、ICカードの表面に刻印してある数字情報を組み合わせたものを設定する。
- エ** PINは、ICカードの配送には同封せず、別経路で利用者に知らせる。



問 2 リスクの顕在化に備えて地震保険に加入するという対応は、JIS Q 31000:2010に示されているリスク対応のうち、どれに分類されるか。

- ア** ある機会を追求するために、そのリスクを取る又は増加させる。
- イ** 一つ以上の他者とそのリスクを共有する。
- ウ** リスク源を除去する。
- エ** リスクを生じさせる活動を開始又は継続しないと決定することによって、リスクを回避する。



問 3 JPCERT/CCの説明はどれか。

- ア** 工業標準化法に基づいて経済産業省に設置されている審議会であり、工業標準化全般に関する調査・審議を行っている。
- イ** 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトであり、総務省及び経済産業省が共同で運営する暗号技術検討会などで構成される。
- ウ** 特定の政府機関や企業から独立した組織であり、国内のコンピュータセキュリティインシデントに関する報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止策の検討や助言を行っている。
- エ** 内閣官房に設置され、我が国をサイバー攻撃から防衛するための司令塔機能を担う組織である。

解説

攻略のカギ

問 1 ICカードとPINの運用

ICカードは、利用者の情報を記録したICチップが埋め込まれているカードで、利用者認証に用いられます。**PIN** (Personal Identification Number) は、本人しか知らない本人確認のための番号で、利用者認証の際に入力されます。

ICカードを利用者に送るときに、PINが書かれた紙などを同封していると、

ICカードとPINの両方を第三者に盗まれる危険性が高くなるので、PINは別経路で利用者に知らせるのが適切です。正解は **エ** です。

- × **ア** 全ての利用者に共通のPINを設定すると、第三者が容易にPINを推測できるので、ICカードを盗むだけでなりすましが可能になります。
- × **イ** ICカード紛失時には、そのICカードの失効処理をただちに実行してから、新たなICカードの発行とPINの再設定を行います。
- × **ウ** ICカードの表面の数字情報などを用いてPINを設定すると、ICカードを入手した第三者が容易にPINを推測できるので、なりすましが可能になります。
- **エ** 正解です。

問2 JIS Q 31000:2010のリスク対応

JIS Q 31000:2010は、リスクマネジメントの原則及び指針を定義した規格です。組織の活動に含まれるリスクを特定し、分析し、適切に対応することでリスクを運用管理する際に、この規格が有効になります。

JIS Q 31000では、**リスク対応**が定義されています。

- ①「リスクを生じさせる活動を、開始または継続しないと決定することによって、リスクを回避すること」
- ②「ある機会を追求するために、リスクを取るまたは増加させること」
- ③「リスク源を除去すること」(リスク源=「それ自体又はほかとの組み合わせによって、リスクを生じさせる力を本来潜在的にもっている要素」)
- ④「起こりやすさを変えること」(起こりやすさ=「何かが起こる可能性」)
- ⑤「結果を変えること」(結果=「目的に影響を与える事象の結末」)
- ⑥「一つ以上の他者とリスクを共有すること」
- ⑦「情報に基づいた意思決定によって、リスクを保有すること」

リスクの顕在化に備えて地震保険に加入するという対応は、地震の発生時に自社の損失を保険会社に補填してもらうことになるので、「一つ以上の他者とリスクを共有する」(**イ**)という、⑥のリスク対応に分類されます。

問3 JPCERT/CC

JPCERT/CC(JPCERTコーディネーションセンター、Japan Computer Emergency Response Team Coordination Center)は、日本の一般社団法人です。情報セキュリティに関する情報を収集し、インターネットを介して発生した各種のインシデントの発生状況を把握して、その報告を受け付けたり、攻撃手法を分析したり、再発防止策の検討や助言などを行ったりしています(**ウ**)。特定の企業などから独立して、中立の組織として活動しています(<https://www.jpCERT.or.jp/faq.html>より)。「JPCERT/CCの活動は、特定の個人や組織の利益を保障することを目的としたものではありません」(https://www.jpCERT.or.jp/faq_service.htmlより)という理由から、独立性を保つ必要があるためです。

- × **ア** **JISC**(Japanese Industrial Standards Committee)の説明です。
- × **イ** **CRYPTREC**(CRYPTography Research and Evaluation Committees)の説明です。
- **ウ** 正解です。
- × **エ** 内閣サイバーセキュリティセンターの説明です。

攻略のカギ

ICカードの例 問1

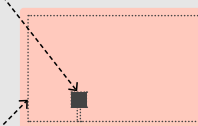
- 接触型(銀行のキャッシュカードなど)



ICモジュール
(ICカードリーダーと接触して情報を送受信する)

- 非接触型(SUICAなど)

ICチップ(カード内に埋め込まれている)



アンテナ(カード内に埋め込まれている。ICカードリーダー周辺の磁界に近付くとコイルとして働き、電流が発生して無線通信を行う)

リスク対応の種類 問2

リスクを防止するための方法には次のようなものがある。

- リスク回避
事業から撤退するなどの方法で、リスクそのものを発生させなくすること
 - リスク低減(軽減)
リスクの発生確率や損失額を減らすこと
 - リスク移転(転嫁)
保険に加入したり、事業を外部に委託したりすることで、リスク発生時の影響、損失、責任の一部または全部を他者に肩代わりさせること
 - リスク保有(受容)
軽微なリスクに対してはあえて対策を行わず、リスクが発生した場合の損失は自社で負担すること
- 各リスクに対して上記の対応策をとった後に、残存するリスクの発生確率または被害額のことを残留リスクという。

解答

問1 **エ** 問2 **イ**
問3 **ウ**



問4 JVN (Japan Vulnerability Notes) はどれか。

- ア 情報システムに存在する脆弱性の^{ぜい}深刻度を評価する手法
- イ 製品に存在する脆弱性に対して採番された識別子
- ウ 脆弱性対策情報などを提供するポータルサイト
- エ 組織内の情報セキュリティ問題を専門に扱うインシデント対応チーム



問5 ファイルサーバについて、情報セキュリティにおける“可用性”を高めるための管理策として、適切なものはどれか。

- ア ストレージを二重化し、耐障害性を向上させる。
- イ デジタル 証明書を利用し、利用者の本人確認を可能にする。
- ウ ファイルを暗号化し、情報漏えいを防ぐ。
- エ フォルダにアクセス権を設定し、部外者の不正アクセスを防止する。



問6 情報セキュリティ対策を検討する際の手法の一つであるベースラインアプローチの特徴はどれか。

- ア 基準とする望ましい対策と組織の現状における対策とのギャップを分析する。
- イ 現場担当者の経験や考え方によって検討結果が左右されやすい。
- ウ 情報資産ごとにリスクを分析する。
- エ 複数のアプローチを併用して分析作業の効率化や分析精度の向上を図る。

解説

問4 JVN

JVN (Japan Vulnerability Notes) は、「日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイト」です。



JVN (<https://jvn.jp/>)

攻略のカギ

JVNは、JPCERT/CCとIPA(独立行政法人情報処理推進機構)が共同で運営しています。脆弱性が確認されたソフトウェアの名称、バージョン、脆弱性への対策や回避などが掲載されます。

- × **ア** 共通脆弱性評価システム **CVSS** (Common Vulnerability Scoring System) の説明です。
- × **イ** 共通脆弱性識別子 **CVE** (Common Vulnerabilities and Exposures) の説明です。
- **ウ** 正解です。
- × **エ** **CSIRT** (Computer Security Incident Response Team) の説明です。

問5 可用性

情報セキュリティにおける“**可用性**”とは、必要なときに必要なデータを利用できるようにするという性質のことで、**情報セキュリティの3要素**の一つです。

情報セキュリティの3要素とは、情報セキュリティマネジメントシステムに関する規格である **JIS Q 27001** (ISO/IEC27001) で定義されている、“**機密性**”(不特定多数からデータにアクセスされないようにする)、“**完全性**”(データの内容を矛盾なく保つ)及び“**可用性**”のことです。

可用性を高めるための管理策としては、「ストレージを二重化し、耐障害性を向上させる」(**ア**)が適切です。

イ、**ウ**、**エ**は、機密性を高めるための管理策です。

問6 ベースラインアプローチ

ベースラインアプローチとは、ISMSにおけるリスク分析の手法の一つです。

ISMS(情報セキュリティマネジメントシステム)とは「マネジメントシステム全体の中で、事業リスクに対するアプローチに基づいて情報セキュリティの確立、導入、運用、監視、見直し、維持、改善を担う部分」と定義されています(ISMS認証基準より)。情報セキュリティを確立し維持するために社内を管理する仕組み(システム)のことです。

ISMSにおける**リスク分析**とは、情報システムに内在するリスクの発生頻度・被害額などを判定し、現実には発生すれば損失をもたらすリスクがシステムのどこにどのように潜在しているかを識別し、重要なリスクとそうでないリスクを見極め、各リスクについて対処するか否かを決定することです。

ベースラインアプローチでは、公表されている既存のセキュリティ対策基準や規格などを参考にして一定のセキュリティレベルを設定します。そのレベルと、現状の自社の対策レベルを比較してギャップを分析し、ギャップを埋めるために自組織が達成すべき大まかな対策基準を策定します。この対策基準を基にしてリスク分析を行ったり、リスクへの管理策を策定したりします。「基準とする望ましい対策」と、「組織の現状における対策」とのギャップを分析する、**ア**の記述が適切です。

- **ア** 正解です。
- × **イ** **非形式的アプローチ**の説明です。
- × **ウ** **詳細リスク分析**の説明です。
- × **エ** **組合せアプローチ**の説明です。

攻略のカギ

JIS Q 27001 問5

情報セキュリティマネジメントシステムの確立、実施、維持及び継続的改善の要求事項を提供しているJIS規格。

JIS Q 27002 問5

情報セキュリティマネジメントシステムの実施プロセスにおいて、管理策を選定する際に参考とするための規格

JIS Q 27000 問5

情報セキュリティマネジメントシステムに関する、JIS Q 27001や同27002などの規格(ISMSファミリ規格)で共通して用いる用語及び定義について規定している規格。

情報資産 問6

情報及び情報を管理するためのシステムのこと。特に、顧客情報や製品開発情報など、外部に漏えいすると自社の利益が損なわれたり、信用が失墜したりする情報が該当する。

解答

問4 **ウ** 問5 **ア**
問6 **ア**



問 7

組織の所属者全員に利用者IDが発行されるシステムがある。利用者IDの発行・削除は申請に基づき行われているが、申請漏れや申請内容のシステムへの反映漏れがある。資料A、Bの組合せのうち、資料Aと資料Bを突き合わせて確認することによって、退職者に発行されていた利用者IDの削除漏れが最も確実に発見できるものはどれか。

	資料 A	資料 B
ア	組織の現在の所属者の名簿	退職に伴う利用者 ID の削除申請書
イ	退職者の一覧	組織の現在の所属者の名簿
ウ	利用者 ID とそれが発行されている者の一覧	組織の現在の所属者の名簿
エ	利用者 ID とそれが発行されている者の一覧	退職に伴う利用者 ID の削除申請書

解説

問 7 削除漏れの発見

「利用者IDの発行・削除は申請に基づき行われているが、申請漏れや申請内容のシステムへの反映漏れがある」と説明されています。

所属者の名簿	システムに登録されている利用者IDと氏名
山田一郎 1000 …… 田川太郎 1001 …… 田中二郎 1002 …… 池田三郎 1005 …… 井上四郎 1008 …… 上田五郎 1010 ……	X0001 山田一郎 X0002 田川太郎 X0003 田中二郎 X0004 池田三郎 X0005 井上四郎 X0006 上田五郎

社員番号

上の6名の社員がいる組織を想定します。田川太郎と上田五郎が退職したことを考えます。田川太郎は利用者IDの削除申請書を提出したがシステムへの反映漏れとなり、上田五郎は利用者IDの削除申請を忘れたため申請漏れとなった場合に、利用者IDの削除漏れを発見できるかどうかを検証します。

● ア

組織の現在の所属者の名簿	退職に伴う利用者IDの削除申請書
山田一郎 1000 …… 田中二郎 1002 …… 池田三郎 1005 …… 井上四郎 1008 ……	削除申請書 田川太郎 (ID : X0002) 利用者IDの削除を

(全て紙媒体の情報であり、システム上の利用者IDを確認できない)

この方法では、組織の現在の所属者の名簿の内容を確認できますが、システムに登録されている利用者IDを参照できないので、どの利用者IDが削除されているかを確認できません。利用者IDの削除漏れを発見するのは困難です。



攻略のカギ

● イ

退職者の一覧

・田川太郎
・上田五郎

組織の現在の所属者の名簿

山田一郎 1000 ……
田中二郎 1002 ……
池田三郎 1005 ……
井上四郎 1008 ……

(全て紙媒体の情報であり、システム上の利用者IDを確認できない)

この方法では、**ア**と同様に組織の現在の所属者の名簿の内容を確認できますが、システムに登録されている利用者IDを参照できないので、どの利用者IDが削除されているかを確認できません。利用者IDの削除漏れを発見するのは困難です。

● ウ

利用者IDとそれが発行されている者の一覧

X0001 山田一郎
X0002 田川太郎
X0003 田中二郎
X0004 池田三郎
X0005 井上四郎
X0006 上田五郎

組織の現在の所属者の名簿

山田一郎 1000 ……
田中二郎 1002 ……
池田三郎 1005 ……
井上四郎 1008 ……

比較

(利用者ID X0002とX0006が削除漏れになっていることを確認できる)

この方法では、資料A(利用者IDとそれが発行されている者の一覧)と、資料B(組織の現在の所属者の名簿)を突き合わせることで、資料Aに存在している利用者IDが、資料Bに存在していない場合に、申請漏れまたは申請内容のシステムへの反映漏れによって、その利用者IDが削除漏れになってシステム上に残っていることを確認できます。正解です。

● エ

エの資料Bは「退職に伴う利用者IDの削除申請書」です。退職者が必ず利用者IDの削除申請をしている場合は、資料Bと資料Aを突き合わせることで、当該退職者の利用者IDがシステム上に残っているかどうかを検証できます。しかし、「申請漏れ」があると説明されているので、退職者が自分の利用者IDの削除申請をしないことがあります。

利用者IDとそれが発行されている者の一覧

X0001 山田一郎
X0002 田川太郎
X0003 田中二郎
X0004 池田三郎
X0005 井上四郎
X0006 上田五郎

退職に伴う利用者IDの削除申請書

削除申請書
田川太郎(ID : X0002)
利用者IDの削除を……

比較

(利用者IDがX0006の上田五郎も退職したが、申請漏れにより削除申請書が提出されていない)

(利用者ID X0002が一覧にあるので、当該利用者IDが削除漏れになったと判断する。)

しかし、利用者ID X0006が削除漏れになっていることは確認できない)

上の例では、利用者IDがX0002とX0006の2名が退職していますが、そのうちX0006の退職者が削除申請をしておらず、削除申請書が提出されていない状態です。資料Bの削除申請書を見ることで、X0002の利用者IDの削除漏れは確認できますが、X0006の利用者IDの削除漏れを確認できません。このような場合、資料Aと突き合わせようとしても、資料Bが存在しないため確認ができません。

解答

問7 ウ



問 8

JIS Q 27000におけるリスク評価はどれか。

- ア 対策を講じることによって、リスクを修正するプロセス
- イ リスクが受容可能か否かを決定するために、リスク分析の結果をリスク基準と比較するプロセス
- ウ リスクの特質を理解し、リスクレベルを決定するプロセス
- エ リスクの発見、認識及び記述を行うプロセス



問 9

JIS Q 31000:2010における残留リスクの定義はどれか。

- ア 監査手続を実施しても監査人が重要な不備を発見できないリスク
- イ 業務の性質や本来有する特性から生じるリスク
- ウ 利益を生む可能性に内在する損失発生の可能性として存在するリスク
- エ リスク対応後に残るリスク



問 10

情報セキュリティ意識向上のための教育の実施状況をJIS Q 27002に従ってレビューした。情報セキュリティを強化する観点から、改善が必要な状況はどれか。

- ア 従業員の受講記録を分析し、教育計画を見直していた。
- イ 従業員の職務内容や職制に応じた内容の教育を実施していた。
- ウ 出張中で受講できなかった従業員を対象に、追加の教育を実施していた。
- エ 正規従業員と同様の業務に従事している派遣従業員を除いて、教育を実施していた。

解説

問 8 JIS Q 27000のリスク評価

JIS Q 27000は、情報セキュリティマネジメントシステムに関する用語や定義について規定している規格です。この規格における**リスク評価**とは、「リスク及びその大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス」と定義されています。

リスク及びその大きさは、そのリスクの発生確率や、それによってもたらされる金銭的被害などを指します。例えば、個人情報の漏えいによって数千万円以上の損害賠償が発生するリスクがあり、個人情報管理を厳重にする対策の費用が年間10万円程度であるならば、対策を取ることで損失を減らせます。逆に、リスク対策に必要な費用に対して損害が非常に少ない場合、対策を取らずに済ませる(受容する)方が得になります。このように、リスクの損害と対策費用を照合して、リスクの重要性を評価すること(イ)が該当します。

- × ア JIS Q 27000における**リスク対応**の説明です。
- イ 正解です。
- × ウ JIS Q 27000における**リスク分析**の説明です。
- × エ JIS Q 27000における**リスク特定**の説明です。



攻略のカギ



リスク

問 8

脅威が情報資産の脆弱性につけこみ、情報資産に損失などを与える可能性のこと。

問9 JIS Q 31000の残留リスク

JIS Q 31000は、リスクマネジメントの原則や組織のリスクマネジメントの取組みを継続的に改善することについて規定している規格です。

JIS Q 31000では、**残留リスク**を「リスク対応後に残るリスク」と定義しています。リスク対応においては、発生確率や被害額が大きいリスクに対しては適切な対策を施しますが、発生確率や被害額が非常に小さいリスクは、その被害額よりも対策費用の方が大きくなることがあるので、あえて対策を取らず許容することがあります。このようにして残したリスクが残留リスクです。

- × **ア** 監査リスクの説明です。
- × **イ** 固有リスクの説明です。
- × **ウ** 投機的リスクの説明です。
- **エ** 正解です。

問10 JIS Q 27002による改善

JIS Q 27002は、情報セキュリティマネジメントシステムを実施するプロセスにおいて、管理策を選定するために用いられる規格です。

「改善が必要な状況」を問われているので、解答群のうち不適切なもの、または良くない状況が正解になります。正規従業員には教育・訓練を受けさせ、同様の業務を実行する派遣従業員などには受けさせないという管理策（**エ**）を採ると、教育を受けていない派遣従業員などが不正を実行したり、重大なミスを行ったりして情報が漏えいします。組織の全ての従業員に対して教育・訓練を実施するのが適切です。

なお、JIS Q 27002の「情報セキュリティの意識向上、教育及び訓練」の項では、「**組織の全ての従業員**……は、……適切な、意識向上のための教育及び訓練を受け、また、定めに従ってその更新を受けることが望ましい」としています。

- × **ア**、**イ** JIS Q 27002では「意識向上プログラムは、組織における従業員の役割……を考慮に入れて、計画することが望ましい」としています。従業員の受講記録を分析して教育計画を見直したり、従業員の職務内容などに応じた教育を実施したりすることは、この記述に従った適切な状況です。
- × **ウ** 出張中で受講できなかった従業員に追加の教育を実施するのは、「組織の全ての従業員に教育・訓練を受けさせるのが望ましい」という記述に従った適切な状況です。
- **エ** 正解です。

 攻略のカギ **リスクマネジメント 問9**

リスクの防止、リスク発生時に被害を最小限にするための施策の制定、及びリスク発生により生じる費用に対する積み立てなどの措置を実施するなどの手法によってリスクを管理すること。

解答

問8 **イ** 問9 **エ**
問10 **エ**



問 11 システム管理者に対する施策のうち、IPA “組織における内部不正防止ガイドライン” に照らして、内部不正防止の観点から適切なものはどれか。

- ア システム管理者間の会話・情報交換を制限する。
- イ システム管理者の操作履歴を本人以外が閲覧することを制限する。
- ウ システム管理者の長期休暇取得を制限する。
- エ 夜間・休日のシステム管理者の単独作業を制限する。



問 12 ボットネットにおけるC&Cサーバの役割はどれか。

- ア Webサイトのコンテンツをキャッシュし、本来のサーバに代わってコンテンツを利用者に配信することによって、ネットワークやサーバの負荷を軽減する。
- イ 遠隔地からインターネットを経由して社内ネットワークにアクセスする際に、CHAPなどのプロトコルを用いることによって、利用者認証時のパスワードの盗聴を防止する。
- ウ 遠隔地からインターネットを経由して社内ネットワークにアクセスする際に、チャレンジレスポンス方式を採用したワンタイムパスワードを用いることによって、利用者認証時のパスワードの盗聴を防止する。
- エ 侵入して乗っ取ったコンピュータに対して、他のコンピュータへの攻撃などの不正な操作をするよう、外部から命令を出したり応答を受け取ったりする。



問 13 会社や団体が、自組織の従業員に貸与するスマートフォンに対して、情報セキュリティポリシーに従った一元的な設定をしたり、業務アプリケーションを配信したりして、スマートフォンの利用状況などを一元管理する仕組みはどれか。

- ア BYOD (Bring Your Own Device)
- イ ECM (Enterprise Contents Management)
- ウ LTE (Long Term Evolution)
- エ MDM (Mobile Device Management)

解説

問 11 組織における内部不正防止ガイドライン

内部不正防止の観点から適切なものは、「夜間・休日のシステム管理者の単独作業を制限する」(エ)です。夜間などにシステム管理者が単独で作業できる状況では、他人の目がないので不正を実行しやすくなります。また、システム管理者の権限を利用してログを消去することで、不正の証拠を隠蔽可能です。

- × ア 通常業務の実行に支障が出てしまいます。
- × イ システム管理者の操作履歴を本人以外が閲覧することで、システム管理者は不正が他人に発覚するのを恐れて、犯行を控えるようになります。この閲覧を制限すると内部不正が発生しやすくなります。
- × ウ 内部不正防止との間には特に関連がありません。



攻略のカギ



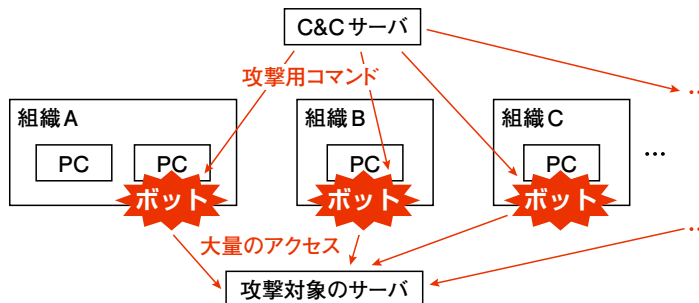
組織における内部不正防止ガイドライン 問 11

独立行政法人 情報処理推進機構 (IPA) が公表しているガイドラインで、組織における内部不正を防止するために実施する事項などをまとめたもの。このガイドラインでは、次の五つを基本原則としている。

- 犯行を難しくする (やりにくくする)
- 捕まるリスクを高める (やると見つかる)

○ **エ** 正解です。**問12 C&Cサーバ**

C&C (Command & Control) サーバとは、マルウェアに感染して攻撃者に乗っ取られた組織内のPCに対して、命令を送って挙動を制御することで、不正な処理を実行させる役割をもつサーバのことです。**エ**が正解です。

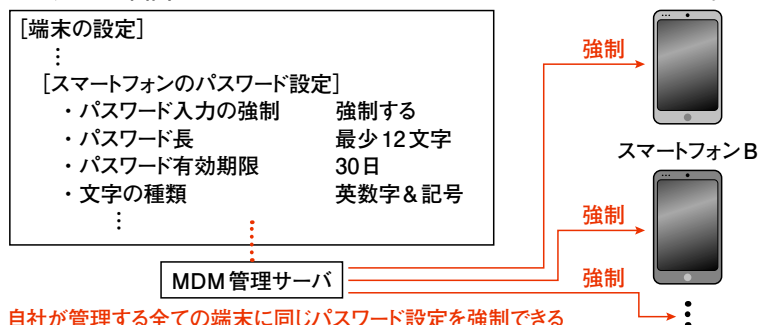


- × **ア** プロキシサーバの説明です。
 × **イ**, **ウ** リモートアクセスサーバの説明です。
 ○ **エ** 正解です。

問13 スマートフォンの一元管理

管理用の装置から複数のスマートフォンなどの端末を一元的に管理するのが、**MDM (Mobile Device Management, モバイルデバイス管理, エ)**です。

ブラウザ上の画面



自社が管理する全ての端末に同じパスワード設定を強制できる

全ての端末に対して、組織のセキュリティポリシーに従った同一のセキュリティ設定を施したり、同じ業務アプリケーションを配信したりすることで、会社などが自組織の従業員に貸与している端末の利用状況を管理できるとともに、端末を介した不正アクセスなどの危険性を少なくすることができます。

- × **ア** **BYOD (Bring Your Own Device)**とは、従業員が私的に保有する携帯電話やタブレットなどの情報端末を、社内に持ち込んだり出先で使ったりすることで、業務に利用することです。
 × **イ** **ECM (Enterprise Contents Management)**とは、組織が管理する情報を統括的に蓄積・管理するための技術及びシステムのことです。
 × **ウ** **LTE (Long Term Evolution)**は、第3世代携帯電話(3G)と第4世代携帯電話(4G)の間に位置する携帯電話の通信規格です。
 ○ **エ** 正解です。

攻略のカギ

- 犯行の見返りを減らす(割に合わない)
- 犯行の誘因を減らす(その気にさせない)
- 犯罪の弁明をさせない(言い訳させない)

操作ログ

問12

システムに対する操作、実行者の利用者ID、処理対象データ、操作時刻、結果(操作の成功又は失敗)などを記録したログファイル。不正アクセスの実行者を特定するなどの目的で使用する。

解答

問11 **エ** 問12 **エ**
 問13 **エ**

問 14 サーバにバックドアを作り、サーバ内での侵入の痕跡を隠蔽するなどの機能をもつ不正なプログラムやツールのパッケージはどれか。

ア RFID

イ rootkit

ウ TKIP

エ web beacon

問 15 SIEM (Security Information and Event Management) の機能として、最も適切なものはどれか。

ア 機密情報を自動的に特定し、機密情報の送信や出力など、社外への持出しに関連する操作を検知しブロックする。

イ サーバやネットワーク機器などのログデータを一括管理、分析して、セキュリティ上の脅威を発見し、通知する。

ウ 情報システムの利用を妨げる事象を管理者が登録し、各事象の解決・復旧までを管理する。

エ ネットワークへの侵入を試みるバケットを検知し、通知する。

解説

問 14 rootkit

OSなどに秘密裏に組み込まれたバックドアなどの不正なプログラムを、隠蔽するための機能をまとめたツールが、**rootkit** (ルートキット、イ) です。

①ソフトウェアがシステムディレクトリの内容を参照するためにOSのファイル機能呼び出す

②OSのファイル機能は、システムディレクトリの内容(不正プログラム含む)を全て出力する



ボットなどの不正プログラムは、コンピュータの利用者やウイルス対策ソフトなどによって発見され、駆除される可能性があります。よって、稼働している様子やファイル名を隠し、気づかれないようにします。その際にrootkitが利用されます。

× ア RFID (Radio Frequency IDentification) は、極小の集積回路とアンテナを組み合わせたRFタグに埋め込んだ情報を、電波などを用いて数センチ〜数m前後の近距離から、非接触形式で読み書きする技術、及びその技術を実現している電子機器のことです。DVDレンタルショップでRFIDのタグを商品に付与して、検品やレジでの会計作業を効率的に実行しています。

○ イ 正解です。

攻略のカギ

バックドア

問14

社内LANなどに不正侵入した攻撃者がサーバに設置する、不正プログラムやアカウント。攻撃者が攻撃対象のサーバなどに再び侵入しやすくするために用いられる。システム内に攻撃者が秘密裏に作成した利用者アカウントなどがバックドアに該当する。

攻撃者が実行する行為 問14

攻撃者がサーバなどに侵入する際に実行する、事前調査、権限取得、不正実行、後処理とは次のような行為。

●事前調査

ポートスキャンなどによって、攻撃対象のシステムに存在する脆弱性を調査する。

●権限取得

事前調査で特定した脆弱性を突いて、攻撃対象のシステムのアカウントの権限を取得し、不正アクセスができるようにする。

●不正実行

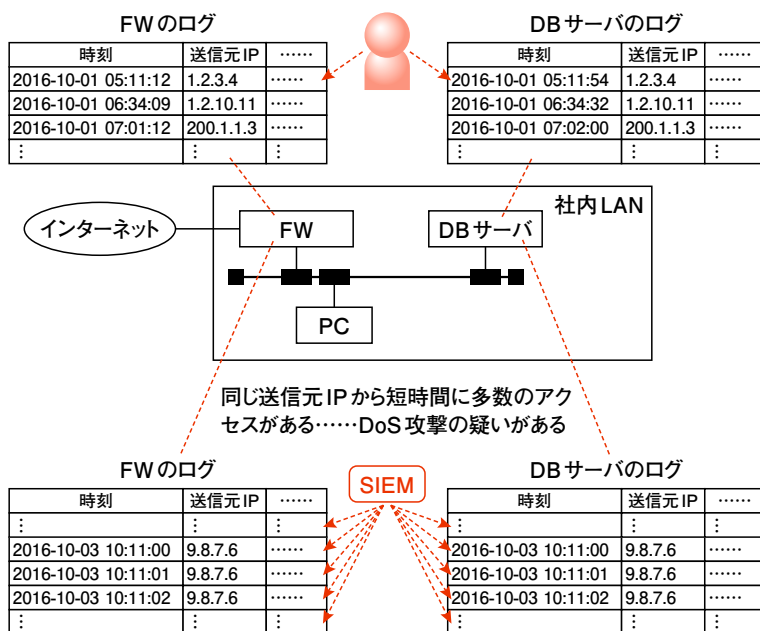
権限取得の段階で取得したアカウントでログインし、攻撃対象のシステム上の情報を盗み見たり、改ざんしたりするなどの不正行為を実行する。

- × **ウ** **TKIP** (Temporal Key Integrity Protocol) とは、無線LANの暗号化規格であるWPAにて用いられている、暗号化鍵を定期的に交換するためのプロトコルのことです。
- × **エ** **Web beacon**は、WebページやHTML形式のメールに埋め込まれる非常に小さな画像で、Webバグとも呼ばれています。

問15 SIEM

SIEM (Security Information and Event Management) とは、ファイアウォールやサーバなどの各種機器から収集したログを分析して、セキュリティインシデントの発生を監視し、発生時は管理者に通知して迅速に対応するための仕組み (**イ**) のことです。

人間では一度に複数のログをまとめて検証
できない……分析に時間が掛かりすぎる



SIEMのソフトウェアは処理能力が高く、一度に複数のログをまとめて検証して、不正アクセスなどの攻撃を見つけ出すことができる

機器が収集したログのデータ量は膨大になるので、セキュリティ管理者が人力で内容を分析するのは困難です。ログの内容をSIEMのソフトウェアが自動的に分析することで、セキュリティ管理者の負担を減らせます。社内の**CSIRT** (Computer Security Incident Response Team) がSIEMを利用してインシデントの発生を検知し、迅速に対策を取れるようにしています。CSIRTは、ネットワーク上での各種の問題 (不正アクセス、マルウェア、情報漏えいなど) を監視し、その報告を受け取って原因を調査したり、対策を検討したりする組織です。

- × **ア** **DLP** (Data Loss Prevention, Data Leak Protection) の説明です。
- **イ** 正解です。
- × **ウ** **インシデント管理プロセス**の説明です。
- × **エ** **IDS** (Intrusion Detection System) の説明です。

攻略のカギ

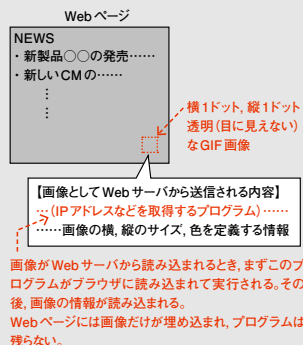
●後処理

不正侵入の痕跡を削除するために、ログの削除や改ざんなどを行う。また、攻撃対象のシステムに再度侵入しやすくするために、バックドアを仕掛けたりする。

Web beacon

問14

画像の横と縦のサイズが1×1で、透明な画像なので利用者は気付かない。画像がWebサーバから読み込まれるとき、Webページを閲覧したPCのIPアドレスなどを取得してサーバに送信するプログラムが密かに実行される。その後、画像の情報が読み込まれ、Webページに埋め込まれる。



解答

問14 **イ** 問15 **イ**



問 16 SPF (Sender Policy Framework) を利用する目的はどれか。

- ア HTTP 通信の経路上での中間者攻撃を検知する。
- イ LAN への PC の不正接続を検知する。
- ウ 内部ネットワークへの侵入を検知する。
- エ メール送信元のなりすましを検知する。



問 17 次の電子メールの環境を用いて、秘密情報を含むファイルを電子メールに添付して社外の宛先の利用者に送信したい。その際のファイルの添付方法、及びその添付方法を使う理由として、適切なものはどれか。

〔電子メールの環境〕

- ・電子メールは、Web ブラウザから利用できる電子メールシステム (Web メール) を用いて送信する。
- ・Web ブラウザと Webメールのサーバとの通信は HTTP over TLS (HTTPS) で行う。
- ・社外の宛先ドメインのメールサーバは SMTP と POP3 を使用している。
- ・IP 層以下は暗号化していない。

- ア Web ブラウザから Webメールのサーバまでの通信が暗号化されているので、ファイルは平文のままでメールに添付する。
- イ Web ブラウザから Webメールのサーバまでの通信は暗号化されるが、その後の通信が暗号化されないこともあるので、ファイルを暗号化してメールに添付する。
- ウ Web ブラウザから宛先の利用者がメールを受信する PC まで、全ての通信は暗号化されるので、ファイルは平文のままでメールに添付する。
- エ Webメールのサーバから宛先ドメインのメールサーバまでの通信は暗号化されないが、サーバ間の通信は Base64 形式でエンコードすれば盗聴できないので、ファイルは Base64 形式でエンコードしてメールに添付する。

解説



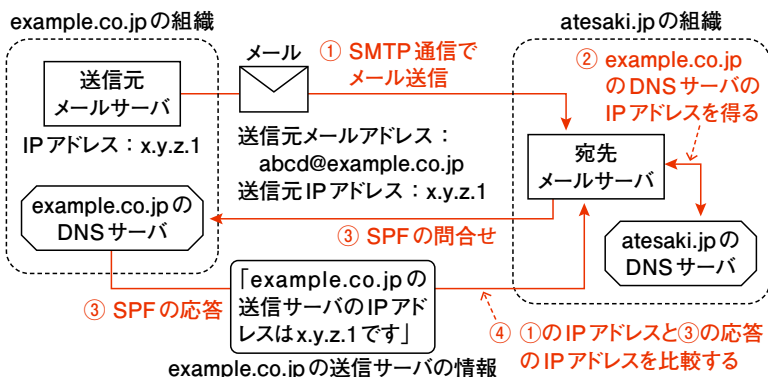
攻略のカギ

問 16 SPF

SPF (Sender Policy Framework) とは、送信ドメイン認証の方法の一つのことです。この方法では、メールサーバの組織が管理している DNS サーバに、「自組織のメールサーバに対応する IP アドレスはこの値です」という主旨の情報を追記することで、自組織のメールサーバの正しい IP アドレスを他の組織のメールサーバから確認できるようにしています。

例えば、「abcd@example.co.jp」という送信元メールアドレスのメールを受信した①宛先メールサーバは、example.co.jpのDNSサーバのIPアドレスを、自組織のDNSサーバに問合せます②。その後、example.co.jpのDNSサーバに問合せた③送信サーバの情報を入手します③。その中に記載された送信サーバのIPアドレスと、送信元メールサーバのIPアドレスとを比較して④、一致していれば正しいメールとして受信します。一致していなければ、他のIP

アドレスのメールサーバから送信されてきたメールであるため、拒否します。

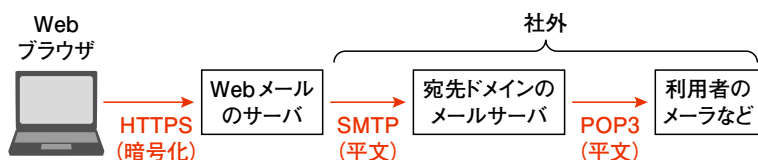


SPFを利用することで、メール送信のなりすましを検知することができます。**エ**が正解です。

- × **ア** 中間者攻撃を防ぐためには、認証局が発行したサーバ証明書などを用いて、送信相手を認証する必要があります。このような仕組みを用いているプロトコルには、**TLS** (Transport Layer Security) などがあります。
- × **イ** **検疫ネットワーク**の説明です。
- × **ウ** **IDS** (Intrusion Detection System) の説明です。
- **エ** 正解です。

問17 電子メールへの添付

〔電子メールの環境〕で説明されている環境を図にします。



Web ブラウザからWebメールのサーバまでの通信は、HTTPSで暗号化されています。この間の通信が盗聴されても、メールの添付ファイルを攻撃者に知られることはありません。しかし、Webメールのサーバが宛先ドメインのメールサーバにメールを送るときは、内容が暗号化されないSMTPが使用されます。また、社外の利用者がメールなどを使用して、宛先ドメインのメールサーバからメールをダウンロードしようとするときは、内容が暗号化されないPOP3が使用されます。これらの間の通信が盗聴されると、添付ファイルの情報が盗まれます。よって、ファイルを暗号化してからメールに添付する(**イ**)のが適切です。

- × **ア**, **ウ** ファイルを平文のままメールに添付すると、攻撃者に盗まれる可能性があります。
- **イ** 正解です。
- × **エ** **Base64**は、バイナリデータをSMTPで送信するときに、ASCII文字に変換する方式です。Base64のアルゴリズムは公開されていて誰でも利用できます。Base64でエンコード(ASCII文字に変換)したデータは、同じBase64によってデコード(元のデータに変換)できるので、ファイルをBase64形式でエンコードしても攻撃者にデコードされ、元のデータを知られます。

攻略のカギ



Base64

問17

8ビット符号で書かれたテキストやバイナリデータを7ビット符号に変換するために用いられる方式。7ビット符号しか送受信できない、SMTPなどのプロトコルにおいて利用される。

- ①変換対象のデータを6ビットのまとまりに区切る。なお、変換対象のデータのビット長が6の倍数でない場合は、変換対象のデータの末尾に0のビットをいくつか追加し、6の倍数にするようにする。
- ②①で区切ったまとまりを2進数値とみなし、その値に相当する7ビット符号の文字に変換する。変換した結果の文字数が4の倍数にならない場合は、末尾に"="を追加して文字数を4の倍数にする。

<例>

変換対象のデータ：

00001111 10101010 (2バイト=16ビット)

00001 111010 101000

↓ ↓ ↓
"D" "6" "o"

"D" "6" "o" "="

→変換後のデータ：D6o=

(追加)

解答

問16 **エ**問17 **イ**



問 18 ウイルス検出におけるビヘイビア法に分類されるものはどれか。

- ア あらかじめ検査対象に付加された、ウイルスに感染していないことを保証する情報と、検査対象から算出した情報とを比較する。
- イ 検査対象と安全な場所に保管してあるその原本とを比較する。
- ウ 検査対象のハッシュ値と既知のウイルスファイルのハッシュ値とを比較する。
- エ 検査対象をメモリ上の仮想環境下で実行して、その挙動を監視する。



問 19 インターネットと社内サーバの間にファイアウォールが設置されている環境で、時刻同期の通信プロトコルを用いて社内サーバがもつ時計をインターネット上の時刻サーバの正確な時刻に同期させる。このとき、ファイアウォールで許可すべき時刻サーバとの間の通信プロトコルはどれか。

- ア FTP (TCP, ポート番号 21)
- イ NTP (UDP, ポート番号 123)
- ウ SMTP (TCP, ポート番号 25)
- エ SNMP (TCP 及び UDP, ポート番号 161 及び 162)



問 20 人間には読み取ることが可能でも、プログラムでは読み取ることが難しいという差異を利用して、ゆがめたり一部を隠したりした画像から文字を判読して入力させることによって、プログラムによる自動入力を排除するための技術はどれか。

- | | |
|-----------|----------------|
| ア CAPTCHA | イ QRコード |
| ウ 短縮 URL | エ トラックバック ping |

解説

問 18 ビヘイビア法

ビヘイビア法とは、ウイルスの実際の感染や発病の際に発生する動作を監視し、検出する方法（**エ**）のことです。大部分のウイルスは、感染または発病時にシステムファイルなどに不正な書き込みを行ったり、コンピュータ内の情報を外部に不正に送信したりするような動作を行います。そのため、ウイルスに感染したコンピュータは、普段は使用しないポートを用いた通信を行ったり、多量のパケットを外部に送出したりするような行動を起こします。検査対象プログラムを動作させてその挙動を監視し、ウイルスによく見られる行動を検知して感染を検出するのが、ビヘイビア法の特徴です。

× **ア** チェックサム法／インテグリティチェック法の説明です。

× **イ**、**ウ** コンペア法の説明です。

○ **エ** 正解です。



攻略のカギ



ビヘイビア法

問 18

ビヘイビア＝behavior（英語の「ふるまい」「行為」の意）なので、この英語を覚えていれば方法を理解しやすい。



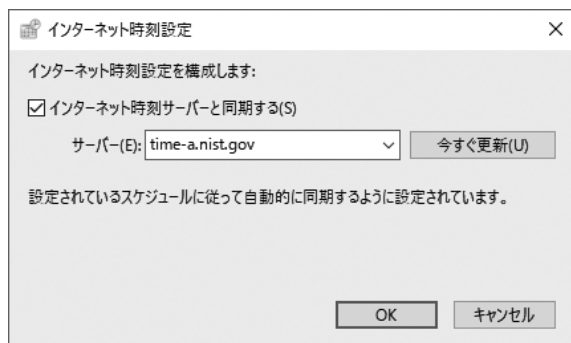
チェックサム法／インテグリティチェック法

問 18

チェックサム＝check sum（検査用の集計値＝検査用の情報）。インテグリティ＝完全性。デジタル署名によって検査対象が改ざんされていない（完全性が保たれている）ことを検査する。

問19 時刻同期の通信プロトコル

「時刻同期の通信プロトコル」を用いて、「社内サーバがもつ時計をインターネット上の時刻サーバの**正確な時刻に同期**させる」ことから、**NTP** (Network Time Protocol, **イ**) のパケットを社内とインターネットとの間でやり取りする必要があります。よって、ファイアウォールではNTPのパケットの通過を許可させます。



NTPは、複数ノード間の時刻の同期を図るためのプロトコルです。NTPサーバに対して現在の正しい時刻を問い合わせることで、時刻の同期を図ります。

- × **ア** **FTP** (File Transfer Protocol) は、サーバとクライアントとの間でファイル転送を行うためのプロトコルです。
- **イ** 正解です。
- × **ウ** **SMTP** (Simple Mail Transfer Protocol) は、メールサーバ間でメールの送受信をするためのプロトコルです。
- × **エ** **SNMP** (Simple Network Management Protocol) は、サーバなどのネットワーク機器の管理・監視を行うためのプロトコルです。

問20 CAPTCHA

インターネット上の掲示板やブログにコメントなどを投稿するとき、ゆがめられた文字が画像化されて表示され、それを読み取って正しい文字を入力するよう求められることがあります。このようなシステムや、ゆがめられた文字の画像のことを**CAPTCHA** (キャプチャ, **ア**) といいます。

CAPTCHAは、コメントなどを投稿しようとした者が人間であり、プログラムによる不正な自動入力でないことを確認するためのシステムです。人間はゆがんだ文字を読み取ることが可能ですが、プログラムでは読み取ることが困難なことを利用しています。



- **ア** 正解です。
- × **イ** **QRコード**は、日本企業が開発した2次元式のバーコードです。
- × **ウ** **短縮URL**は、Twitterなどの投稿可能文字数が限られたWebサービスにおいて、文字数が長いURLの代替として、文字数を短くしたURLを投稿するサービス、及びそのサービスで作成された短いURLです。
- × **エ** **トラフィックバックping**とは、ほかのブログの記事に関連する記事を新しく作成したときに、元となった記事を管理するサーバに宛てて送信するデータです。トラフィックバックpingを受信したサーバは、元となった記事のトラフィックバック欄に新しい記事のURLやその概要などを表示します。

攻略のカギ

コンペア法 問18

コンペア=compare (英語の「比較」)。検査対象と原本を「比較」する。

ポート番号 問19

パケットのTCPヘッダに含まれる番号で、サーバやPC上で稼働するサービス(プログラム)を識別するためのもの。0~65,535の値をとる。

短縮URL 問20

https://www.google.co.jp/search?q=%E3%82%A4%E3%83%B3%E3%83%86%E3%82%B0%E3%83%AA%E3%83%86%E3%82%A3%E3%83%81%E3%82%A7%E3%83%83%E3%82%AF%E6%B3%95&ie=utf-8&oe=utf-8&client=firefox-b&gfe_rd=cr&ei=Z3kiWMvbKpTR8gego5_gBgというURLを短縮化した結果は次のようになる (URX.NUというサービスを利用)。
<http://ur0.biz/zz6e>

解答

問18 **エ** 問19 **イ**
問20 **ア**

問21 情報の“完全性”を脅かす攻撃はどれか。

- ア Webページの改ざん
- イ システム内に保管されているデータの不正コピー
- ウ システムを過負荷状態にするDoS攻撃
- エ 通信内容の盗聴

問22 クロスサイトスクリプティングの手口はどれか。

- ア Webアプリケーションに用意された入力フィールドに、悪意のあるJavaScriptコードを含んだデータを入力する。
- イ インターネットなどのネットワークを通じてサーバに不正にアクセスしたり、データの改ざんや破壊を行ったりする。
- ウ 大量のデータをWebアプリケーションに送ることによって、用意されたバッファ領域をあふれさせる。
- エ パス名を推定することによって、本来は認証された後にしかアクセスが許可されていないページに直接ジャンプする。

解説

問21 完全性

JIS Q 27001 (ISO/IEC 27001)などの情報セキュリティの規格によって示される、情報セキュリティの3要素の一つである“**完全性**”とは、情報(データ)が正確かつ完全であること、言い換えれば、権限のないユーザから不正にデータを書き換え・改ざんされないことを指します。

よって、「Webページの改ざん(ア)」が、完全性を脅かす攻撃となります。

- ア 正解です。
- × イ システム内に保管されているデータが持ち出されると、データを参照する権限のない外部の者がデータを参照できるので、情報セキュリティの3要素の“機密性”が脅かされます。
- × ウ DoS攻撃によってシステムが過負荷状態にされると、システムの機能が利用できなくなり、情報セキュリティの3要素の“可用性”が脅かされます。
- × エ 通信内容が盗聴されると、通信内容を参照する権限のない攻撃者がデータを参照できるので、情報セキュリティの3要素の“機密性”が脅かされます。

問22 クロスサイトスクリプティング

クロスサイトスクリプティングとは、悪意あるスクリプトを含んだ不正なリンクを利用者のブラウザに送り込み、標的サイトにアクセスした利用者の個人情報やクッキーなどから盗み取る攻撃方法(ア)です。

攻略のカギ

情報のCIA 問21

情報セキュリティの3要素である機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability) の三つを、情報のCIAという。

- ①機密性 (Confidentiality)
情報にアクセスする権限のない者に、情報を不正に読まれないようにすること

【高める方法】

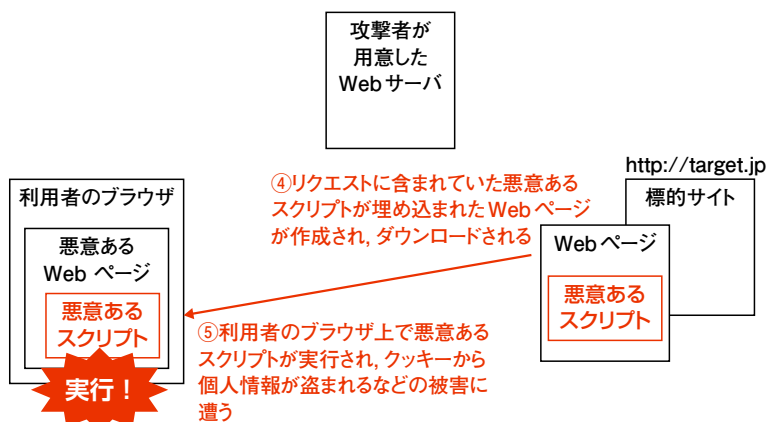
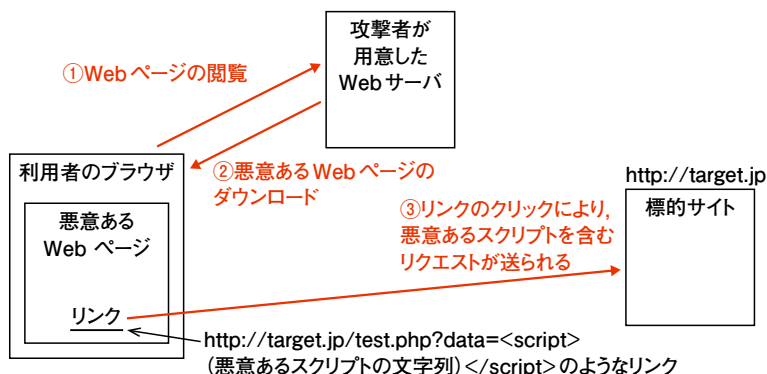
- ・ 情報を暗号化して第三者に読まれないようにする
- ・ 情報にアクセスする権限のある者だけに、参照・更新可能なアクセス権を与える

- ②完全性 (Integrity)

情報の内容が正確であり(矛盾していないこと)、改ざんなどがされないようにすること

【高める方法】

- ・ 情報へのアクセス権を適切な者だけに与えて、むやみに更新されないようにする



Web ブラウザから掲示板などの動的なサイトにアクセスする際に、次のような URL が用いられることがあります。

`http://target.jp/test.php?data=123456`

“?data=123456” は、サイト上の Web サーバプログラムに対してユーザが送信する情報を記載したものです。HTTP の GET リクエストを使用すると、URL の末尾にこのような形式でユーザからの送信情報が掲載される仕組みになっています。Web サーバプログラムは、このデータをもとに動的に Web ページを生成したり、検索処理を行ったりします。

ここで、上の“?”以降に、悪意あるスクリプトの文字列を記述した URL を作成して、他の Web ページにリンクとして貼ると、そのリンクをクリックした場合に、Web サーバプログラムに正常なデータの代わりに不正なスクリプトが与えられ、当該サイト上で生成されたページをブラウザが開き、その結果ブラウザ上で悪意のスクリプトが実行されてしまう可能性があります。

- **ア** 正解です。
- × **イ** サーバに対する不正アクセスの説明です。
- × **ウ** バッファオーバーフローの説明です。
- × **エ** ディレクトリトラバーサルの説明です。

攻略のカギ

③可用性 (Availability)

アクセス権限のある者が、いつでも情報にアクセスできるようにすること (障害などが発生しても情報にアクセスできるようにすること)

【高める方法】

- ・システムの機器を二重化して、一つの機器が故障しても残りをういて業務を継続する

スクリプト

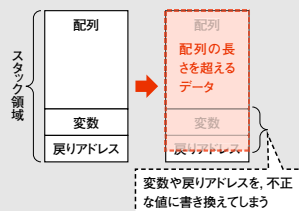
問22

文字で記述されたプログラム。HTMLなどに埋め込まれている。ブラウザがスクリプトを読み込むと、その内容が動的に解釈されて処理が実行される。

バッファオーバーフロー

問22

メモリのスタック領域中に確保されていた配列に、その大きさを超える長さのデータを書き込むことで、配列の直後に位置する戻りアドレスの領域の内容を上書きして、不正なプログラムを実行させる攻撃手法のこと。



ディレクトリトラバーサル

問22

Web ページ上のファイル名を入力する欄に、“../passwd”などの不正な文字列を入力して、本来はアクセスが許されないファイルを不正に閲覧する攻撃手法。

通常のアクセスで参照されるフォルダ `htdocs` の、一つ上“..”のフォルダ (ルート) の直下にある、ファイル “passwd” が閲覧されてしまう。

解答

問21 **ア** 問22 **ア**



問 23 内閣は、2015年9月にサイバーセキュリティ戦略を定め、その目的達成のための施策の立案及び実施に当たって、五つの基本原則に従うべきとした。その基本原則に含まれるものはどれか。

- ア** サイバー空間が一部の主体に占有されることがあってはならず、常に参加を求める者に開かれたものでなければならない。
- イ** サイバー空間上の脅威は、国を挙げて対処すべき課題であり、サイバー空間における秩序維持は国家が全て代替することが適切である。
- ウ** サイバー空間においては、安全確保のために、発信された情報を全て検閲すべきである。
- エ** サイバー空間においては、情報の自由な流通を尊重し、法令を含むルールや規範を適用してはならない。



問 24 スクリプトキディの典型的な行為に該当するものはどれか。

- ア** PCの利用者がWebサイトにアクセスし、利用者IDとパスワードを入力するところを後ろから盗み見して、メモをとる。
- イ** 技術不足なので新しい攻撃手法を考え出すことはできないが、公開された方法に従って不正アクセスを行う。
- ウ** 顧客になりすまして電話でシステム管理者にパスワードの再発行を依頼し、新しいパスワードを聞き出すための台本を作成する。
- エ** スクリプト言語を利用してプログラムを作成し、広告や勧誘などの迷惑メールを不特定多数に送信する。

解説

問23 サイバーセキュリティ戦略

サイバーセキュリティ戦略とは、サイバーセキュリティ基本法の第12条第1項の規定に基づいて、平成27年9月4日に閣議決定された戦略です。

この戦略では、目的達成のための施策の立案及び実施に当たって、次の**五つの基本原則**を規定しています。

●情報の自由な流通の確保

「新たな創意と発想の場としてのサイバー空間は、その内部における情報の自由な流通の確保がその発展の基盤である。このため、我が国は、**サイバー空間**においては、発信した情報が、その途中で不当に検閲されず、また、不正に改変されずに、意図した受信者へ届く世界が創られ、維持されるべきであるとする」

●法の支配

「連接融合情報社会においては、実空間と同様に、**サイバー空間**においても法の支配が貫徹されるべきである。……同様に、国際法を始めとする国際的なルールや規範についても、サイバー空間に適用され、国際的な法の支配が確立されるべきである。さらに、……国際社会の平和と安定のため、自由や民主主義といった普遍的価値にのっとった国際的なルールや規範作りが求められる」



攻略のカギ

 攻略のカギ

● 開放性

「サイバー空間が一部の主体に占有されることがあってはならず、常に参加を求める者に開かれたものでなければならない。…… また、少数の者の政治的利益のために、大多数の人々がサイバー空間の利用を否定されるようなことがあってはならない」

● 自律性

「インターネットは、長らく多様な参加主体による自律的なガバナンスにより発展を遂げてきた。サイバー空間上の脅威が、国を挙げて対処すべき課題となっても、サイバー空間における秩序維持を国家が全て代替することは不可能、かつ、不適切である。我が国は、サイバー空間の秩序と創造性の共存を実現していくことを目指す観点から、インターネットが育んだこの自律性を尊重し、…… 悪意ある行動を抑止していく自律的メカニズムの構築・運用を推進していく」

● 多様な主体の連携

「サイバー空間は、あらゆる階層で様々な主体が活動することにより構築される多次元的な世界である。このため、政府に限らず、重要インフラ事業者、企業、個人といったサイバー空間に関係する全てのステークホルダーが、サイバーセキュリティに係るビジョンを共有し、それぞれの役割や責務を果たし、また努力する必要がある。そして、政府はこれらのステークホルダーを適切な連携関係へと促す役割を担っている。こうした連携関係の構築に当たっては、サイバー攻撃が刻々と高度化していること等の事情を踏まえ、双方向的かつリアルタイムな情報共有等の措置によるダイナミックな対処策を実現していく」

基本原則に含まれるのは、「サイバー空間が一部の主体に占有されることがあってはならず、常に参加を求める者に開かれたものでなければならない」(ア)です。

○ **ア** 正解です。

× **イ** サイバー空間における秩序維持は「国家が全て代替することは不可能、かつ、不適切である」としているので誤りです。

× **ウ** 「我が国は、サイバー空間においては、発信した情報が、その途中で不当に検閲されず……」としているので誤りです。

× **エ** 「サイバー空間においても法の支配が貫徹されるべきである」としているので誤りです。

問24 スクリプトキディ

スクリプトキディとは、裏サイトなどで公開された攻撃方法を用いて、Webサイトに不正アクセスしようとする犯行者のことです。情報セキュリティに関する専門知識はほとんどなく、特別な技術ももっていないため、新しい攻撃方法を考え出すことはできず、Webサイトなどに掲載されている既存の方法を使って攻撃をします。**イ**が正解です。

× **ア** **ショルダハッキング**の説明です。

○ **イ** 正解です。

× **ウ** **ソーシャルエンジニアリング**の説明です。

× **エ** プログラムを利用して迷惑メールを不特定多数に送信する方法の説明です。

ショルダハッキング 問24

ノートPCやスマートフォンなどを操作している人の肩越しに画面をのぞきこむことで、情報を盗み見る攻撃。

解答

問23 **ア** 問24 **イ**



問 25 緊急事態を装って組織内部の人間からパスワードや機密情報を入手する不正な行為は、どれに分類されるか。

- ア** ソーシャルエンジニアリング
- イ** トロイの木馬
- ウ** 踏み台攻撃
- エ** ブルートフォース攻撃



問 26 パスワードリスト攻撃に該当するものはどれか。

- ア** 一般的な単語や人名からパスワードのリストを作成し、インターネットバンキングへのログインを試行する。
- イ** 想定され得るパスワードとそのハッシュ値との対のリストを用いて、入手したハッシュ値からパスワードを効率的に解析する。
- ウ** どこかのWebサイトから流出した利用者IDとパスワードのリストを用いて、他のWebサイトに対してログインを試行する。
- エ** ピクチャパスワードの入力を録画してリスト化しておき、それを利用することによってタブレット端末へのログインを試行する。



問 27 ランサムウェアに分類されるものはどれか。

- ア** 感染したPCが外部と通信できるようプログラムを起動し、遠隔操作を可能にするマルウェア
- イ** 感染したPCに保存されているパスワード情報を盗み出すマルウェア
- ウ** 感染したPCのキー操作を記録し、ネットバンキングの暗証番号を盗むマルウェア
- エ** 感染したPCのファイルを暗号化し、ファイルの復号と引換えに金銭を要求するマルウェア

解説

問 25 ソーシャルエンジニアリング

攻撃者が本人になりすまして、パスワードなどの情報を組織の内部の人間から聞き出そうとする行為を、**ソーシャルエンジニアリング** (**ア**) といいます。

ソーシャルエンジニアリングは、不注意や誤解・勘違いなどの、人間の心理的な盲点を突くため、システムの物理的・機械的な対策だけでは防止が困難な攻撃方法です。

- **ア** 正解です。
- × **イ** 正当なプログラムを装ってインストールされ、秘密裏に不正行為を働くソフトウェアのことです。
- × **ウ** 脆弱性のあるコンピュータに不正侵入した上で、そのコンピュータを乗っ取り、別のシステムなどに攻撃を仕掛ける方法です。不正侵入者が身元などを隠す際によく用いられます。
- × **エ** 全ての文字列を試すことで、パスワードを不正に入手したり、他人になりすましてログインしたりする方法のことです。



攻略のカギ



ソーシャルエンジニアリング

問 25

不正な利用者が、本人になりすまして「パスワードを忘れてしまったので教えてください」という主旨の電話をセキュリティ管理者にかけなどの方法で、パスワードなどのセキュリティに関する情報を不正に聞き出す行為のこと。

問26 パスワードリスト攻撃

パスワードリスト攻撃とは、Webサイトから流出した利用者IDとパスワードのリストを用いて、他のWebサイトに対してログインを試行する攻撃（ウ）です。多くの利用者は、複数のWebサービスに対してそれぞれ異なるパスワードでログインするのをわずらわしく感じて、同じ利用者IDとパスワードを使いまわす傾向があります。その結果、あるWebサービスのサイトから利用者IDとパスワードが流出すると、別のWebサービスにログインできる可能性が高くなります。パスワードリスト攻撃ではこの点を利用して、不正アクセスを試みます。

- × ア 辞書攻撃の説明です。
- × イ パスワードのハッシュ値を記録したリストを用いたパスワード解析手法の説明です。
- ウ 正解です。
- × エ **ピクチャパスワード**とは、画像の上でマウスカーソル又は指を線状に動かしたり円を描いたりするような動作（ジェスチャ）を記録し、そのジェスチャをパスワードとする認証方法です。マルウェアを端末に仕掛けて、ピクチャパスワードの入力を録画してリスト化し、それを利用してログインを試みる攻撃が存在します。

問27 ランサムウェア

ランサムウェアとはマルウェアの一種で、コンピュータに感染した上で内部のファイルを勝手に暗号化し、利用者を脅迫して元に戻すための代金を払わせようとしています。エが正解です。

- × ア 遠隔操作ウイルスの説明です。
- × イ スパイウェアの説明です。
- × ウ キーロガーの説明です。
- エ 正解です。

攻略のカギ

ピクチャパスワード 問26

図のような複数回のジェスチャ（操作）の組合せをパスワードとして登録する。



ランサムウェアの攻撃 問27

ランサムウェアは、次のような方法で感染し、PC内のデータを勝手に暗号化する。

- Webページに不正なスクリプトを仕込み、閲覧したPCの脆弱性を突いてランサムウェアをインストールする
- 有益なセキュリティソフトのように見せかけた広告を使って、利用者のインストールを促す

解答

問25 ア 問26 ウ
問27 エ



問 28 なりすましメールでなく、EC(電子商取引) サイトから届いたものであることを確認できる電子メールはどれか。

- ア 送信元メールアドレスがECサイトで利用されているアドレスである。
- イ 送信元メールアドレスのドメインがECサイトのものである。
- ウ デジタル署名の署名者のメールアドレスのドメインがECサイトのものであり、署名者のデジタル証明書の発行元が信頼できる組織のものである。
- エ 電子メール本文の末尾にテキスト形式で書かれた送信元の連絡先に関する署名のうち、送信元の組織を表す組織名がECサイトのものである。



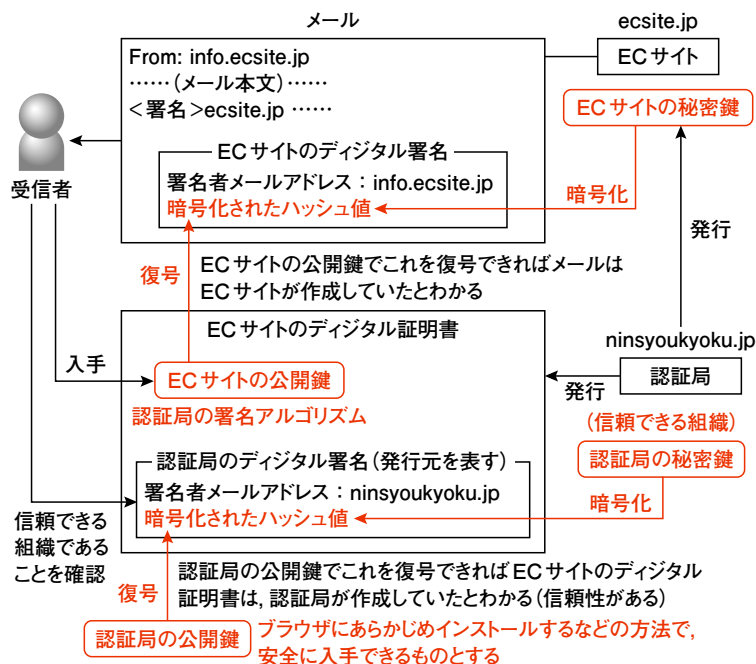
問 29 PKI(公開鍵基盤)における認証局が果たす役割はどれか。

- ア 共通鍵を生成する。
- イ 公開鍵を利用してデータの暗号化を行う。
- ウ 失効したデジタル証明書の一覧を発行する。
- エ データが改ざんされていないことを検証する。

解説

問 28 なりすましメール対策

メール本文や送信元メールアドレスの内容は偽装できます。本文中のテキストの署名に他人の名前や別の組織の名称を入れたり、送信元メールアドレスを他人のものに偽ったりすることで、なりすましが可能になります。



攻略のカギ

デジタル署名 問 28

公開鍵暗号方式とハッシュ関数を利用して、データの改ざんを検知したり、本人性を証明したりするための技術。

メールがなりすましでないことを確認するためには、メールに**デジタル署名**を施すのが適切です(図)。

電子メールがECサイトから届いたものと確認するためには、その電子メールのデジタル署名の署名者のメールアドレスのドメインがECサイトのものであり、かつ、署名者のデジタル証明書の発行元が信頼できる組織(認証局)であることを参照します。**ウ**が正解です。

× **ア**、**イ** 送信元メールアドレスは偽造できるので、このような電子メールをECサイトが送信してきたことを確認できません。

○ **ウ** 正解です。

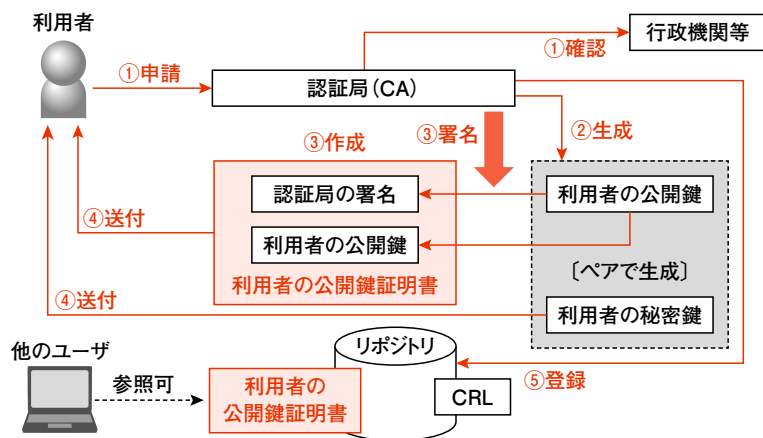
× **エ** 電子メール本文の末尾のテキスト形式の署名は、送信元メールアドレスと同様に偽造できるので、このような電子メールをECサイトが送信してきたことを確認できません。

問29 PKIの認証局

PKI(Public Key Infrastructure, 公開鍵基盤)とは、各種のセキュリティプロトコルや組織などを用いて、利用者の身元証明及び公開鍵の対応付けを行うシステムのことです。

公開鍵暗号方式では、誰でも公開鍵をネットワーク上に公開できるため、あるユーザになりすました攻撃者が、その公開鍵と偽って偽の公開鍵を公開する可能性があります。なりすましによって公開された偽の公開鍵を知らずに用いてしまい、攻撃者が作った偽のWebサイトに誘導されて、情報を不正に窃取される被害が起こります。よって、公開鍵を公開しているユーザの身元証明などが必要となってきました。そのために、PKIが利用されています。

PKIの概略図を示します。



公開鍵証明書には期限が設けられており、期限切れになると無効になります。また、インターネット上の他人の公開鍵証明書を、自分のものと偽って公開する攻撃者がいます。このような公開鍵証明書をCRLに掲載して、インターネット上のユーザに注意を促しています。認証局の果たす役割は、公開鍵証明書を発行することのほかに、CRLを発行すること(**フ**)などがあります。

× **ア** PKIでは共通鍵を生成しません。

× **イ** 公開鍵を利用するユーザの役割です。

○ **ウ** 正解です。

× **エ** データを受け取った人が、デジタル署名を利用して行うことです。

攻略のカギ

PKI(公開鍵基盤) 問29

公開鍵暗号方式及びデジタル署名の仕組みを応用した、公開鍵の正当性を証明して公開鍵とその利用者を結び付けるための仕組みのこと。

ある利用者がネットワーク上に公開している公開鍵が、本当にその利用者が作成して公開しているものか(本人性があるか)を証明するために、デジタル証明書(公開鍵証明書や電子証明書ともいう)が用いられる。

認証局 問29

公開鍵及び秘密鍵の利用を申請してきた者(利用者)に対して、公開鍵証明書を交付したり、公開鍵の本人性を保証したりする組織。ペリサイン社などが認証局として公開鍵証明書の交付を行っている。

解答

問28 **ウ** 問29 **ウ**

問 30 情報技術セキュリティ評価のための国際標準であり、コモンクライテリア (CC) と呼ばれるものはどれか。

ア ISO 9001

イ ISO 14004

ウ ISO/IEC 15408

エ ISO/IEC 27005

問 31 プロバイダ責任制限法において、損害賠償責任が制限されるプロバイダの行為に該当するものはどれか。ここで、“利用者”とはプロバイダに加入してサービスを利用している者とする。

ア 契約書に記載した利用者の個人情報を、本人の同意を得ずに関連会社に渡した。

イ 他のプロバイダに移転する利用者に対して、不当に高い違約金を請求した。

ウ 利用者の送信メールの内容を盗聴し、それを興味本位で他人に伝えた。

エ 利用者の電子掲示板への書込みが、他人の権利を侵害しているとは知らずに放置した。

問 32 刑法の電子計算機使用詐欺罪が適用される違法行為はどれか。

ア いわゆるねずみ講方式による取引形態のWebページを開設する。

イ インターネット上に、実際よりも良品と誤認させる商品カタログを掲載し、粗悪な商品を販売する。

ウ インターネットを経由して銀行のシステムに虚偽の情報を与え、不正な振込や送金をさせる。

エ 企業のWebページを不法な手段によって改変し、その企業の信用を傷つける情報を流す。

解説

問30 コモンクライテリア

米国のセキュリティ評価基準のCC (Common Criteria, コモンクライテリア) を基にした、IT製品のセキュリティ評価・認証基準に、ISO/IEC 15408 (ウ)があります。

ISO/IEC 15408では、「セキュリティ機能をもったIT製品/システム」が評価・認証対象となります。具体的には、OS、DBMS、ファイアウォールやルータ、ICカードなどです。これらのIT製品やシステムに実装されたセキュリティ機能が、攻撃に対して確実に対処できるかを客観的に評価する基準です。

× ア ISO 9001 は、品質マネジメントシステムに関する国際規格です。

× イ ISO 14004 は、環境マネジメントシステムに関する国際規格です。

○ ウ 正解です。

× エ ISO/IEC 27005 は、情報セキュリティリスクマネジメントの指針をまとめた国際規格です。

問31 プロバイダ責任制限法

プロバイダ責任制限法は、インターネット上で名誉毀損や他者の権利の侵害などが行われた場合に、その犯行者が契約しているプロバイダなどが負う責任

攻略のカギ

ISO 9001 問30

組織が品質マネジメントシステムを確立し、実施し、維持することや、その有効性を継続的に改善するために必要なプロセスを定義している。国内のJIS Q 9001が対応している。

ISO 14004 問30

環境マネジメントシステムを確立し、実施し、維持し、継続的に改善するための、共通の枠組みを規定している。国内のJIS Q 14004が対応している。

(損害賠償の義務など)を規定している法律です(正式名称:特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律)。この法律では、犯行者が契約しているプロバイダや、犯行者が書込みを行った掲示板の管理者などを「**特定電気通信役務提供者**」と定義しています。

プロバイダ責任制限法の第三条では、次のように規定しています。

「第三条 特定電気通信による情報の流通により他人の権利が侵害されたときは、当該特定電気通信の用に供される特定電気通信設備を用いる特定電気通信役務提供者(以下この項において「関係役務提供者」という。)は、これによって生じた損害については、**権利を侵害した情報の不特定の者に対する送信を防止する措置を講ずることが技術的に可能な場合であって、次の各号のいずれかに該当するときでなければ、賠償の責めに任じない。**ただし、当該関係役務提供者が当該権利を侵害した情報の発信者である場合は、この限りでない。

- 一 当該関係役務提供者が当該特定電気通信による情報の流通によって**他人の権利が侵害されていることを知っていたとき。**
- 二 当該関係役務提供者が、当該特定電気通信による情報の流通を知っていた場合であって、当該特定電気通信による情報の流通によって**他人の権利が侵害されていることを知ることができた**と認めるに足りる相当の理由があるとき」

以上から、犯行者の書込みを防止することが技術的に不可能であり、かつ、書込みによって他人の権利が侵害されたことを知らなかった場合は、プロバイダは損害賠償責任を負いません。**エ**が適切です。

- × **ア** 本人の同意を得ずに個人情報 را 他人に渡すと、個人情報保護法に違反する可能性があります。
- × **イ** このような行為は民法に違反する可能性があります。
- × **ウ** 盗聴した内容を他人に漏らすと、電気通信事業法や有線電気通信法などに違反します。
- **エ** 正解です。

問32 電子計算機使用詐欺罪

電子計算機使用詐欺罪は、刑法第246条の2に規定されている罪状です。

「人の〔他者の〕事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、十年以下の懲役に処する」(同法より引用)

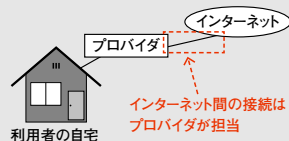
すなわち、この罪状では、他人の管理する電子計算機(コンピュータ)に虚偽の情報を与えて、不正な利益を得る行為を処罰の対象にしています。具体的には、銀行のシステムに虚偽の情報を流して不正な振込・送金をさせたりする、**ウ**のような行為です。

- × **ア** **無限連鎖講の防止に関する法律**(ねずみ講防止法)に違反する行為です。
- × **イ** **詐欺罪**に相当する行為です。
- **ウ** 正解です。
- × **エ** **信用毀損罪**に相当する行為です。

攻略のカギ

プロバイダ 問31

利用者の自宅から直接インターネットの回線に接続するのは困難なので、プロバイダが接続を代行している。



電子計算機使用詐欺罪の例 問32

2016年10月、有名銀行の元副支店長が外貨預金取引システムのデータ修正機能を不正に操作して、円とドルの交換レートを変更するなどの手口で口座上の金額を操作し、余剰分を自分の口座に入金していた。このような行為が電子計算機使用詐欺罪に該当する。

解答

問30 **ウ** 問31 **エ**
問32 **ウ**



問 33 “特定個人情報ファイル”の取扱いのうち、国の個人情報保護委員会が制定した“特定個人情報の適正な取扱いに関するガイドライン（事業者編）”で、認められているものはどれか。

- ア** 個人番号関係事務を行う必要がなくなり、かつ、法令による保存期間を経過した場合は、暗号化した上で保管する。
- イ** 事業者内の誰でも容易に参照できるよう、事務取扱担当者を限定せず従業員全員にアクセス権を設定する。
- ウ** 従業員の個人番号を含む源泉徴収票を、業務委託先の税理士に作成させる。
- エ** 従業員の個人番号を利用して営業成績を管理する。



問 34 広告宣伝の電子メールを送信する場合、特定電子メール法に照らして適切なものはどれか。

- ア** 送信の許諾を通知する手段を電子メールに表示していれば、同意を得ていない不特定多数の人に電子メールを送信することができる。
- イ** 送信の同意を得ていない不特定多数の人に電子メールを送信する場合は、電子メールの表題部分に未承諾広告であることを明示する。
- ウ** 取引関係にあるなどの一定の場合を除き、あらかじめ送信に同意した者だけに対して送信するオプトイン方式をとる。
- エ** メールアドレスを自動的に生成するプログラムを利用して電子メールを送信する場合は、送信者の氏名・連絡先を電子メールに明示する。

解説

問33 特定個人情報の適正な取扱いに関するガイドライン

特定個人情報保護委員会が平成26年に公開した“特定個人情報の適正な取扱いに関するガイドライン（事業者編）”（以下、ガイドラインという）は、**個人番号（マイナンバー）**を取り扱う事業者が、特定個人情報の適正な取扱いを確保するための具体的な指針を定めるものです。このガイドラインで定義している用語を表に示します。

ガイドラインでは、「事業者が、特定個人情報ファイルを作成することができるのは、個人番号関係事務又は個人番号利用事務を処理するために必要な範囲に限られている。法令に基づき行う従業員等の源泉徴収票作成事務、健康保険・厚生年金保険被保険者資格取得届作成事務等に限って、特定個人情報ファイルを作成することができるものであり、これらの場合を除き特定個人情報ファイルを作成してはならない」としています。また、「事業者から従業員等の源泉徴収票作成事務について委託を受けた**税理士等の受託者**についても、……個人番号関係事務を処理するために必要な範囲で特定個人情報ファイル（個人番号を含む源泉徴収票）を作成することができる」としています。適切な記述は**ウ**です。

× **ア** ガイドラインでは、「個人番号が記載された書類等については、……それらの事務を処理する必要がなくなった場合で、所管法令において定

攻略のカギ

特定個人情報の適正な取扱いに関するガイドラインで定義している用語 **問33**

用語	説明
特定個人情報	個人番号を含む個人情報のこと
個人情報データベース等	特定の個人情報について、コンピュータ等を用いて検索することができるように体系的に構成した個人情報を含む情報の集合物のこと
個人情報ファイル	個人情報データベース等であって、行政機関及び独立行政法人等以外の者が保有するもの
特定個人情報ファイル	個人番号を含む個人情報ファイルのこと

 攻略のカギ

められている保存期間を経過した場合には、個人番号をできるだけ速やかに廃棄又は削除しなければならない」としています。

- × **イ** ガイドラインでは、特定個人情報等を取り扱う事務に従事する従業者を「事務取扱担当者」としています。また、「事業者は、特定個人情報等の取扱いを検討するに当たって、……事務取扱担当者を明確にしておく必要がある」とし、「情報システムを使用して個人番号関係事務又は個人番号利用事務を行う場合、**事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う**」という安全管理措置を講じなければならないとしています。
- **ウ** 正解です。
- × **エ** ガイドラインでは、「事業者は、個人情報保護法とは異なり、本人の同意があったとしても、例外として認められる場合を除き……、**これらの事務以外で個人番号を利用してはならない**」としています。

問34 特定電子メール法

特定電子メールの送信の適正化等に関する法律（特定電子メール法）は、迷惑メールの送信の規制などを目的として制定された法律です。

特定電子メール法では、**特定電子メール**を次のように定義しています。

「電子メールの送信（国内にある電気通信設備（電気通信事業法第二条第二号に規定する電気通信設備をいう。以下同じ。）からの送信又は国内にある電気通信設備への送信に限る。以下同じ。）をする者（営利を目的とする団体及び営業を営む場合における個人に限る。以下「送信者」という。）が自己又は他人の営業につき広告又は宣伝を行うための手段として送信をする電子メールをいう」

また、特定電子メールの送信を次のように制限しています。

「第三条 送信者は、次に掲げる者以外の者に対し、特定電子メールの送信をしてはならない。

- 一 あらかじめ、特定電子メールの送信をするように求める旨又は送信をすることに同意する旨を送信者又は送信委託者（電子メールの送信を委託した者（営利を目的とする団体及び営業を営む場合における個人に限る。）をいう。以下同じ。）に対し通知した者
- 二 前号に掲げるもののほか、総務省令・内閣府令で定めるところにより自己の電子メールアドレスを送信者又は送信委託者に対し通知した者
- 三 前二号に掲げるもののほか、当該特定電子メールを手段とする広告又は宣伝に係る営業を営む者と取引関係にある者」

以上から、取引関係にあるなどの場合を除いて、あらかじめ送信に同意した者だけに対して送信できる方式（オプトイン方式）をとること（**ウ**）が適切です。

- × **ア** あらかじめ同意を得ていない不特定多数の人に特定電子メールを送信してはいけません。
- × **イ** 2008年の改正により、相手の承諾なしで特定電子メールを送信すること自体が禁止されたので、「未承諾広告※」と件名に明記しても承諾なしではメールを送信できなくなっています。
- **ウ** 正解です。
- × **エ** 自動生成されたものであり、かつ、利用者が存在しないメールアドレスのことを、架空電子メールアドレスといいます。特定電子メール法第六条では、架空電子メールアドレスを宛先とする電子メールを送信してはならないとしています。

解答

問33 **ウ**問34 **ウ**



問 35 不正アクセス禁止法による処罰の対象となる行為はどれか。

- ア 推測が容易であるために、悪意のある攻撃者に侵入される原因となった、パスワードの実例を、情報セキュリティに関するセミナーの資料に掲載した。
- イ ネットサーフィンを行ったところ、意図せずに他人の利用者IDとパスワードをダウンロードしてしまい、PC上に保管してしまった。
- ウ 標的とする人物の親族になりすまし、不正に現金を振り込ませる目的で、振込先の口座番号を指定した電子メールを送付した。
- エ 不正アクセスを行う目的で他人の利用者ID、パスワードを取得したが、これまでに不正アクセスは行っていない。



問 36 準委任契約の説明はどれか。

- ア 成果物の対価として報酬を得る契約
- イ 成果物を完成させる義務を負う契約
- ウ 善管注意義務を負って作業を受託する契約
- エ 発注者の指揮命令下で作業を行う契約



問 37 JIS Q 27001 に準拠してISMSを運用している場合、内部監査について順守すべき要求事項はどれか。

- ア 監査員にはISMS認証機関が認定する研修の修了者を含まなければならない。
- イ 監査責任者は代表取締役が任命しなければならない。
- ウ 監査範囲はJIS Q 27001に規定された管理策に限定しなければならない。
- エ 監査プログラムには前回までの監査結果を考慮しなければならない。

解説

問 35 不正アクセス禁止法

不正アクセス禁止法とは、不正アクセス行為を禁止するための法律です。不正アクセス行為とは、特定電子計算機（コンピュータなど）の利用権限をもたない第三者が、他人の利用者IDやパスワードを悪用して、アクセス制御機能による利用制限を免れて特定電子計算機の利用をできる状態にする行為のことを指します。不正アクセス禁止法では、このような行為及びその助長行為を処罰の対象にしています。

不正アクセス禁止法の第六条では「何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号（IDやパスワードなど）を保管してはならない」としています。不正アクセスをこれまでに行っていなくても、不正アクセスを行う目的で他人の利用者IDなどを取得した時点で処罰の対象になります。**エ**が正解です。

× **ア** 不正アクセス禁止法の第五条では、「何人も、業務その他正当な理由に



攻略の力



不正アクセス禁止法で禁止されている行為 問35

- ・他人のIDやパスワードを入力して不正にログインする（不正アクセス行為）。
- ・不正アクセス行為をする目的で、他人のIDやパスワードを取得する。
- ・利用者本人のIDやパスワードを、他人に提供する（業務その他正当な理由による場合を除く）。
- ・不正に取得された他人のIDやパスワードを、不正アクセス行為をする目的で保管する。

 攻略のカギ

よる場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用者権者以外の者に提供してはならない」としています。情報セキュリティ教育において、推測が容易なパスワードの実例を紹介するのは「業務その他正当な理由」に該当するので、パスワードの実例を資料に掲載しても問題はありません。

- × **イ** 他人の利用者IDやパスワードを、意図せず（不正アクセスを行う目的ではない）取得した場合は、第六条には違反しません。
- × **ウ** 口座番号を指定しているだけで、他人の利用者IDやパスワードにはアクセスしていないので、不正アクセス法の処罰対象にはなりません。
- **エ** 正解です。

問36 準委任契約

準委任契約とは、法律行為でない事務を委託する契約のことです。法律行為とは、法律上の権利・義務の発生、変更又は消失を引き起こす行為（売買契約の締結など）のことです。

準委任契約では、受託先は委託元からの依頼に従って、一定の注意を払って業務を行う義務（善管注意義務）を負います。また、委託元の求めに応じて作業内容の報告を行う義務があります。受託先の行為の結果として作成された成果物の内容については、受託先が責を負うことはありません。また、受託先には、仕事を完成して成果物を引き渡す責任もありません。

以上から、**ウ**が正解です。

- × **ア**、**イ** 請負契約の説明です。
- **ウ** 正解です。
- × **エ** 派遣契約の説明です。

問37 ISMS

JIS Q 27001では、この規格に準拠して**ISMS**（情報セキュリティマネジメントシステム）を運用している場合、内部監査について次のように定めています。

「組織は、……あらかじめ定めた間隔で内部監査を実施しなければならない」

「組織は、次に示す事項を行わなければならない」

「c) 頻度、方法、責任及び計画に関する要求事項及び報告を含む、監査プログラムの計画、確率、実施及び維持。**監査プログラムは、関連するプロセスの重要性及び前回までの監査の結果を考慮に入れなければならない**」(**エ**)

- × **ア** JIS Q 27001では、「監査プロセスの客観性及び公平性を確保する監査員を選定」しなければならないとされていますが、監査員にISMS認証機関が認定する研修の修了者を含まなければならないという規定はありません。
- × **イ** JIS Q 27001では、監査責任者の任命については特に規定がありません。
- × **ウ** JIS Q 27001では、「各監査について、監査基準及び監査範囲を明確にする」としていますが、監査範囲を限定しなければならないという規定はありません。
- **エ** 正解です。

委任契約

問36

法律行為を委託する契約のこと。弁護士に依頼して裁判の事務作業を代行してもらうことなどが該当する。

準委任契約

問36

法律行為でない事務を委託する契約のこと。コンサルタントに依頼して経営に関する助言を得たり、システム開発作業を他人に委託したりすることが該当する。

解答

問35 **エ**
問37 **エ**

問36 **ウ**

問 38 インシデントの調査やシステム監査にも利用できる、証拠を収集し保全する技法はどれか。

- ア コンティンジェンシープラン
ウ デジタルフォレンジックス

- イ サンプリング
エ ベンチマーキング

問 39 事業継続計画（BCP）について監査を実施した結果、適切な状況と判断されるものはどれか。

- ア 従業員の緊急連絡先リストを作成し、最新版に更新している。
イ 重要書類は複製せずに1か所で集中保管している。
ウ 全ての業務について、優先順位なしに同一水準のBCPを策定している。
エ 平時にはBCPを従業員に非公開としている。

問 40 “情報セキュリティ監査基準”に関する記述のうち、最も適切なものはどれか。

- ア “情報セキュリティ監査基準”は情報セキュリティマネジメントシステムの国際規格と同一の内容で策定され、更新されている。
イ 情報セキュリティ監査人は、他の専門家の支援を受けてはならないとしている。
ウ 情報セキュリティ監査の判断の尺度には、原則として、“情報セキュリティ管理基準”を用いることとしている。
エ 情報セキュリティ監査は高度な技術的専門性が求められるので、監査人に独立性は不要としている。

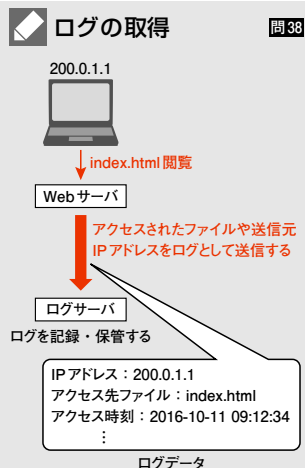
解説

問 38 証拠を収集し保全する技法

コンピュータ犯罪に対する科学的調査を、**デジタルフォレンジックス**（ウ）と呼びます。具体的には、不正アクセスなどの犯罪に対する証拠（記録・ログなど）を立証するために必要なデータを保全して収集・分析すること、及びその後の訴訟などに備えることです。デジタルフォレンジックスの手法を利用することで、情報システムのインシデントを発生させる原因を調べたり、システム監査において問題点の存在を証明する証拠を特定したりすることができます。

- × ア **コンティンジェンシープラン**とは、「緊急時対応計画」又は「不測事態対応計画」のことで、障害や事故などの事態が発生することを想定し、その対策を事前に定めた計画案のことです。
- × イ **サンプリング**とは、母集団（評価対象のデータ全体）から一部のデータを取り出して評価対象に選定することです。
- ウ 正解です。
- × エ **ベンチマーキング**とは、業務遂行のための最善の方法や、最も利益を上げている企業の手法を参考にして自社の経営方針を決定することです。

攻略のカギ



問39 BCP

情報システムが地震や火災などの災害や停電などの障害に見舞われても、可能な限り早期にシステムを復旧させ、業務を再開するために日ごろから立てておく計画のことを、**事業継続計画** (Business Continuity Plan, **BCP**) といいます。

システムに障害が発生したときに、従業員を招集して適切な対策をとれるようにするために、緊急連絡先リストを作成し、内容を定期的に更新しておくこと(ア)で、BCPの実効性が高くなります。

- **ア** 正解です。
- × **イ** 重要書類を1か所で集中保管すると、例えばその場所が火災に見舞われたときに、全ての重要書類が焼失する危険性が高くなります。重要書類を複数の箇所に分散して保管するなどの方法をとるのが適切です。
- × **ウ** BCPを策定する際には、重要性の高い業務を優先して回復できるようにするために、各業務を回復する優先順位を決定して、優先順位ごとに異なる水準のBCPを策定しておくのが適切です。
- × **エ** 平時にBCPを従業員に公開しないと、障害が発生してから初めてBCPの内容を知った従業員が、復旧のための適切な行動をとれないことがあります。平時からBCPを従業員に公開し、その内容に沿った訓練を定期的に行うことで、障害発生時に適切な行動をとれるようにするのが適切です。

問40 情報セキュリティ監査基準

経済産業省が公表している“**情報セキュリティ監査基準**”は、「情報セキュリティ監査業務の品質を確保し、有効かつ効率的に監査を実施することを目的とした監査人の行為規範」です。次の三つから成ります。

- **一般基準**：監査人としての適格性及び監査業務上の遵守事項を規定する基準
 - **実施基準**：監査手続の適用方法を中心に監査実施上の枠組みを規定する基準
 - **報告基準**：監査報告に係る留意事項と監査報告書の記載方式を規定する基準
- “情報セキュリティ監査基準”では、「情報セキュリティ監査は、**本監査基準の姉妹編である情報セキュリティ管理基準を監査上の判断の尺度として用い、監査対象が情報セキュリティ管理基準に準拠しているかどうかという視点で行われることを原則とする**」としています。**ウ**が正解です。

- × **ア** 情報セキュリティマネジメントシステムの国際規格はISO/IEC 27001です。“情報セキュリティ監査基準”は、この規格と同一の内容ではありません。
- × **イ** “情報セキュリティ監査基準”では、「情報セキュリティ監査人は、情報セキュリティ監査の目的達成上、必要かつ適切と判断される場合には、他の専門職による支援を考慮しなければならない」としています。
- **ウ** 正解です。
- × **エ** “情報セキュリティ監査基準”では、「情報セキュリティ監査人は、情報セキュリティ監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない」としています。

攻略のカギ

情報セキュリティ監査制度 問40

企業や政府などの情報セキュリティ対策が適切に実行され、情報セキュリティに係るリスクマネジメントが効果的に実施されているかどうかを、情報セキュリティ監査によって確認するための制度。この制度においては、経済産業省が公表している“情報セキュリティ監査基準”や“情報セキュリティ管理基準”が、情報セキュリティ監査の尺度として用いられる。

解答

問38 **ウ** 問39 **ア**
問40 **ウ**



問 41 システムの移行テストを実施する主要な目的はどれか。

- ア 確実性や効率性の観点で、既存システムから新システムへの切替え手順や切替えに伴う問題点を確認する。
- イ 既存システムの実データのコピーを利用して、新システムでも十分な性能が得られることを確認する。
- ウ 既存の他システムのプログラムと新たに開発したプログラムとのインタフェースの整合性を確認する。
- エ 新システムが、要求された全ての機能を満たしていることを確認する。



問 42 あるデータセンタでは、受発注管理システムの運用サービスを提供している。次の“受発注管理システムの運用中の事象”において、インシデントに該当するものはどれか。

〔受発注管理システムの運用中の事象〕

夜間バッチ処理において、注文トランザクションデータから注文書を出力するプログラムが異常終了した。異常終了を検知した運用担当者から連絡を受けた保守担当者は、緊急出社してサービスを回復し、後日、異常終了の原因となったプログラムの誤りを修正した。

- | | |
|--------------|--------------|
| ア 異常終了の検知 | イ プログラムの誤り |
| ウ プログラムの異常終了 | エ 保守担当者の緊急出社 |



問 43 メールサーバのディスクに障害が発生して多数の電子メールが消失した。消失した電子メールの復旧を試みたが、2週間ごとに行っている磁気テープへのフルバックアップしかなかったため、最後のフルバックアップ以降1週間分の電子メールが回復できなかった。そこで、今後は前日の状態までには復旧できるようにしたい。対応策として、適切なものはどれか。

- ア 2週間ごとの磁気テープへのフルバックアップに加え、毎日、磁気テープへの差分バックアップを行う。
- イ 電子メールを複数のディスクに分散して蓄積する。
- ウ バックアップ方法は今のままとして、メールサーバのディスクをミラーリングするようにし、信頼性を高める。
- エ 毎日、メールサーバのディスクにフルバックアップを行い、2週間ごとに、バックアップしたデータを磁気テープにコピーして保管する。

解説

問41 移行テスト

既存のシステムから新しいシステムへの移行を行う際には、一時的にシステムを停止するなどの措置が必要となります。そのため、システム移行の時刻を、



攻略のカギ

業務が実施されない深夜の時間帯に設定するなどの、入念な切換え手順を設定する必要があります。また、移行後にトラブルが発生して復旧不可能になった場合、暫定的に既存のシステムに戻す必要があります。

よって、切換え手順や切換えに伴う問題点について、安全性などの観点から確認する必要があります(ア)。そのために移行テストは実施されます。

- ア 正解です。
 ×イ 性能テストの説明です。
 ×ウ 結合テストの説明です。
 ×エ システムテストの説明です。

問42 インシデント

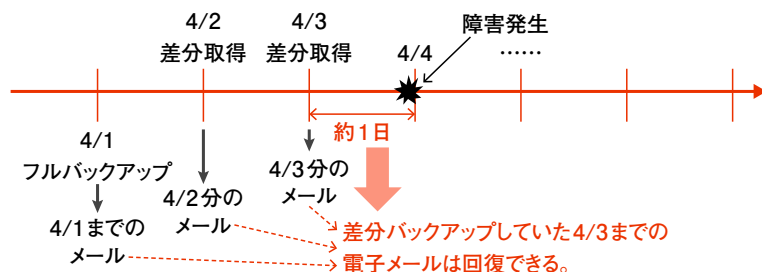
インシデントとは、情報システムを利用したサービスを停止させる**出来事(事象)**のことです。出来事の原因があっても、その出来事が実際に発生しない限りはインシデントになりません。

〔受発注管理システムの運用中の事象〕では「プログラムが異常終了」したことによって、注文書の出力ができなくなり、夜間バッチ処理のサービスが停止しています。したがって、ウの「プログラムの異常終了」がインシデントに該当します。

- ×ア インシデントの検知に該当します。
 ×イ インシデントを発生させた原因です。
 ○ウ 正解です。
 ×エ インシデントに対応するための従業員の行動です。

問43 バックアップ

バックアップをする直前に障害が発生した場合、最大でバックアップ間隔と同じ日数分のデータが失われます。前日の状態まで復旧できるようにするには、バックアップ間隔を1日にするために、差分バックアップを毎日とるようにします。このようにすると、最大で約1日分の電子メールしか失われなくなり、前日の状態までには復旧できます。



なお、メールサーバのディスクにバックアップデータを保存すると、ディスクの障害発生時にデータが失われます。よって、アの対応策が適切です。

- ア 正解です。
 ×イ メールサーバのディスクに障害が発生すると、その中に蓄積していた電子メールが失われます。
 ×ウ イと同様に、メールサーバのディスクに障害が発生すると、その中に蓄積していた電子メールが失われます。
 ×エ ディスクとは別の磁気テープなどにバックアップするのが適切です。

攻略のカギ

各種テスト手法 問41

- ・単体テスト
モジュール(単体のプログラム)の機能の正当性を検証するためのテスト。
- ・結合テスト
モジュール間またはサブシステム間のインタフェース(データのやり取り)の正当性について検証するためのテスト。
- ・システムテスト
結合テスト終了後に、全てのサブシステムを接続して、システム全体の動作の検証を行うためのテスト。
- ・運用テスト
システムを実際に運用する際に、システムに加わると想定される負荷などをシステムに与えて、システムが利用者の要求を満足し、運用に耐えられるかを検証するテスト。

フルバックアップ 問43

ハードディスク内の全てのファイルをバックアップする方式。

差分バックアップ 問43

前回のフルバックアップの後に、内容が変更されたファイルだけをバックアップする方式。

増分バックアップ 問43

直前のバックアップ(フル、差分、増分のいずれも該当)の後に、内容が変更されたファイルだけをバックアップする方式。

解答

問41 ア 問42 ウ
 問43 ア



問 44 プロジェクトに関わるステークホルダの説明のうち、適切なものはどれか。

- ア 組織の外部にいることはなく、組織の内部に属している。
- イ プロジェクトの成果が、自らの利益になる者と不利益になる者がいる。
- ウ プロジェクトへの関与が間接的なものにとどまることはなく、プロジェクトには直接参加する。
- エ プロジェクトマネージャのように、個人として特定できることが必要である。



問 45 クライアントサーバシステムを構築する。Webブラウザによってクライアント処理を行う場合、専用のアプリケーションによって行う場合と比較して、最も軽減される作業はどれか。

- ア クライアント環境の保守
- イ サーバが故障したときの復旧
- ウ データベースの構築
- エ ログインアカウントの作成と削除



問 46 E-R図に関する記述として、適切なものはどれか。

- ア 関係データベースの表として実装することを前提に表現する。
- イ 管理の対象をエンティティ及びエンティティ間のリレーションシップとして表現する。
- ウ データの生成から消滅に至るデータ操作を表現する。
- エ リレーションシップは、業務上の手順を表現する。

解説

問44 ステークホルダ

ステークホルダとは、プロジェクトの利害関係者のことです。システムの利用部門、必要な物資を供給する納入業者、及び参加者などがステークホルダになります。また、プロジェクトによって利益を受ける者だけでなく、不利益を受ける者も該当します。例えば、自社がプロジェクトの成果物を活用して市場シェアを広げることで、シェアを奪われて不利益を受ける競合他社も該当します。正解は **イ** です。

- × **ア** 外部業者などもステークホルダになるので誤りです。
- **イ** 正解です。
- × **ウ** プロジェクトに間接的に関与する者もステークホルダになります。
- × **エ** 外部業者など法人格をもつ組織もステークホルダになります。

問45 クライアントサーバシステム

クライアントサーバシステムにおいて、Webブラウザによってクライアント処理を行う場合、次ページの図のようになります。

この形態では、クライアント処理に変更が生じた場合、Webサーバに格納しているクライアント処理用のWebページやスクリプトを更新するだけで済み



攻略の力ギ



ステークホルダ
(steak holder)

問44

もともとは「賭け金を管理する人」を意味する用語。現在では「企業の経営活動などに関する利害関係者」という意味になっている。具体的には、顧客（消費者）、取引先、株主、従業員、公的機関など、企業活動の周辺に存在している、あらゆる利害関係者を指す。

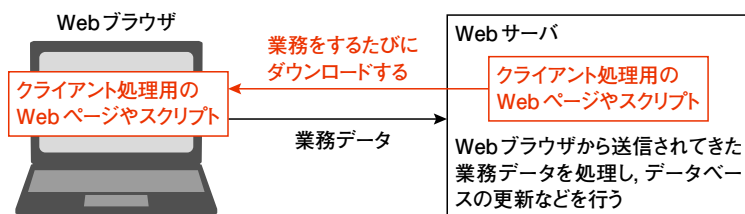


サーバ

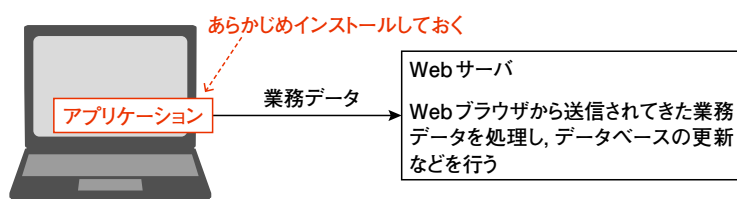
問45

他のコンピュータから依頼された作業を実行し、その結果を返す側コンピュータ。Webサーバ、メールサーバ、ファイルサーバなどが該当する。

ます。Webブラウザは、更新されたWebページなどを再読み込みするだけで、変更されたクライアント処理を利用できます。業務の変更のたびにソフトウェアを再インストールするなど、クライアント環境を更新する作業が不要なので、保守が容易になります。



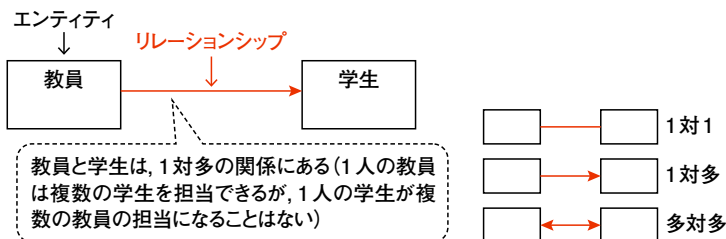
クライアントサーバシステムにおいて、専用のアプリケーションを用いる場合、利用者のPCにインストールする必要があります。



業務が変更されるとアプリケーションを再インストールしなければならない。
PCの台数が多くなると、再インストールに非常に多くの工数が掛かる

イ～エは、いずれもクライアント側の処理ではなくサーバ側で行う処理なので、Webブラウザによってクライアント処理を行う場合でも、工数は軽減されません。アが正解です。

問46 E-R図



E-R図は、システム化しようとする業務体系などを抽象化した上で、情報の中に存在する実体(エンティティ)と、実体間の関連(リレーションシップ)について表現する図法です。データベースシステムを実装する前に、データ同士の関連について定義するときによく用いられます。しかし、E-R図は、必ずデータベースへ実装されることを前提に作成されるわけではなく、データベースをもたないシステムの業務などを表現する図として作成されることもあります。

- × ア E-R図は、必ずしも関係データベースの表として実装することを前提に作成されるわけではありません。
- イ 正解です。
- × ウ データ操作は、DFDによって表現されます。
- × エ リレーションシップは実体間の関連であり、業務上の手順などの処理(プロセス)を表現するものではありません。業務上の手順は、DFDや流れ図などによって表現されます。

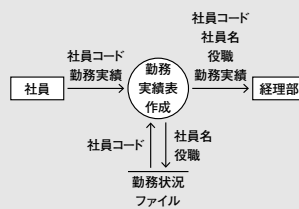
攻略のカギ

クライアント 問45

サーバに対して作業を依頼し、その結果を受け取る側(顧客)としてのコンピュータ。パソコンなどが該当する。

DFD (Data Flow Diagram) 問46

プロセス(処理)間のデータの流れを表現する図法。矢印(データの流れ)、丸印(プロセス)、長方形(データの源泉/吸収)、二重線(データを格納するファイルなど)の4つから構成される。



解答

問44 イ 問45 ア
問46 イ

問 47 IPアドレスの自動設定をするためにDHCPサーバが設置されたLAN環境の説明のうち、適切なものはどれか。

- ア DHCPによる自動設定を行うPCでは、IPアドレスは自動設定できるが、サブネットマスクやデフォルトゲートウェイアドレスは自動設定できない。
- イ DHCPによる自動設定を行うPCと、IPアドレスが固定のPCを混在させることはできない。
- ウ DHCPによる自動設定を行うPCに、DHCPサーバのアドレスを設定しておく必要はない。
- エ 一度IPアドレスを割り当てられたPCは、その後電源が切られた期間があっても必ず同じIPアドレスを割り当てられる。

問 48 BPOを説明したものはどれか。

- ア 災害や事故で被害を受けても、重要事業を中断させない、又は可能な限り中断期間を短くする仕組みを構築すること
- イ 社内業務のうちコアビジネスでない事業に関わる業務の一部又は全部を、外部の専門的な企業に委託すること
- ウ 製品を生産しようとするときに必要となる部品の数量や、調達する資材の所要量、時期を計算する生産管理手法のこと
- エ プロジェクトを、戦略との適合性や費用対効果、リスクといった観点から評価を行い、情報化投資のバランスを管理し、最適化を図ること

解説

攻略のカギ

問47 DHCP

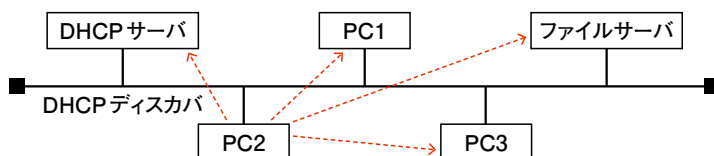
DHCPは、IPアドレスの自動割当を可能とするプロトコルです。DHCPにより、IPアドレス、サブネットマスク及びデフォルトゲートウェイの情報を、DHCPサーバから自動的に取得できます。PCがインターネットに接続する必要がなくなったときは、そのPCに割り当てていたIPアドレスを回収します。

DHCPでは、次の手順でDHCPサーバとDHCPクライアント(PC)との間でメッセージのやり取りが行われます。

① DHCPディスカバ(DHCP DISCOVER)のブロードキャスト

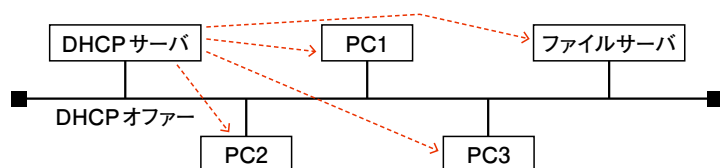
DHCPクライアントは、自分と同じネットワーク上のDHCPサーバを探すため、**DHCPディスカバ**というフレームをブロードキャストで送信する。この手順があるので、PCにはDHCPサーバのIPアドレスを登録しておく必要はない(ウ)。

(PC2がDHCPでIPアドレスを取得するとき)



②DHCPオファー(DHCP OFFER)のブロードキャスト

DHCPディスカバを受信したDHCPサーバは、割当て可能なIPアドレスなどをDHCPクライアントに通知するために、**DHCPオファー**というフレームを送信する。DHCPサーバでないPCやサーバはいずれもDHCPオファーを無視する。



③DHCPリクエスト(DHCP REQUEST)のブロードキャスト

DHCPクライアントは、受け取ったDHCPオファーに記録されているIPアドレスを使用するために、DHCPサーバに対して**DHCPリクエスト**を送信し、IPアドレス使用の許可を求める。この時点では、DHCPクライアントはまだIPアドレスの使用を許可されていないので、IPアドレスをもっていない状態である。よって、自分の送信元IPアドレスや相手の送信先IPアドレスを指定したパケットを送信することはできないので、宛先を指定しなくてよいブロードキャストフレームでDHCPリクエストを送信している。

④DHCPアック(DHCP ACK)のブロードキャスト

DHCPリクエストを受信したDHCPサーバは、DHCPクライアントに対してIPアドレスの利用を許可するメッセージ(DHCPアック)を送信する。

- × **ア** サブネットマスクなども自動設定できます。
- × **イ** DHCPで動的に割り当てるIPアドレスの範囲と、固定で割り当てるIPアドレスの範囲が重ならないようにすれば、混在させることが可能です。
- **ウ** 正解です。
- × **エ** PCの電源が切られて返却されたIPアドレスが、別のPCに割り当てられた場合、その後は異なるIPアドレスが割り当てられます。

問48 BPO

BPO(Business Process Outsourcing, ビジネスプロセスアウトソーシング)とは、自社の主要な事業に関する業務(コアビジネス)以外を外部に委託して、人材・労力・資金などの経営資源をコアビジネスに集中させることで、効率的に運営する手法のことです(**イ**)。BPOの例としては、総務や人事などの業務をアウトソーシングしたり、コールセンタ業務を外部委託したりすることなどが挙げられます。

- × **ア** **BCM**(Business Continuity Management)の説明です。
- **イ** 正解です。
- × **ウ** **MRP**(Materials Requirements Planning)の説明です。
- × **エ** IT投資の最適化に関する記述です。

攻略のカギ



MRP

問48

製品Xを製造するのに必要な中間製品と、それらを製造するのに必要な部品が次のように与えられているとする。

中間製品		必要な部品
α	2個	部品A 3個
		部品B 2個
β	1個	部品B 4個
		部品C 6個
γ	3個	部品A 2個
		部品C 7個

製品Xを1個製造する必要があるとき、

中間製品α、β、γの在庫が4個、1個、1個…γが2個不足
→部品Aが $2 \times 2 = 4$ 個、部品Cが $7 \times 2 = 14$ 個必要となる
部品A、B、Cの在庫が0個、1個、4個…部品Aが4個、部品Cが10個不足

→これらの部品を調達する

必要な中間製品や部品の個数を、システムが自動的に計算して発注を行うのがMRPの概要である。

解答

問47 **ウ**問48 **イ**



問 49 共通フレームによれば、企画プロセスにおいて明確にするものはどれか。

- ア 新しい業務の在り方や手順、入出力情報、業務上の責任と権限、業務上のルールや制約などの事項
- イ 業務要件を実現するために必要なシステムの機能、システムの開発方式、システムの運用手順、障害復旧時間などの事項
- ウ 経営・事業の目的及び目標を達成するために必要なシステムに関係する経営上のニーズ、システム化又はシステム改善を必要とする業務上の課題などの事項
- エ システムを構成するソフトウェアの機能及び能力、動作のための環境条件、外部インタフェース、運用及び保守の方法などの事項



問 50 マトリックス組織を説明したものはどれか。

- ア 業務遂行に必要な機能と利益責任を、製品別、顧客別又は地域別にもつことによって、自己完結的な経営活動が展開できる組織である。
- イ 構成員が、自己の専門とする職能部門と特定の事業を遂行する部門の両方に所属する組織である。
- ウ 購買・生産・販売・財務など、仕事の専門性によって機能分化された部門をもつ組織である。
- エ 特定の課題の下に各部門から専門家を集めて編成し、期間と目標を定めて活動する一時的かつ柔軟な組織である。

解説

問 49 共通フレーム

共通フレームは、ソフトウェアライフサイクルプロセスにおける作業全般にわたって使用される用語などを統一して、作業範囲や作業内容を明確にするための基準となります。

【企画プロセス】

現状：請求書を手書きで作成している

売り上げた商品の種類が多いと書くのが大変
時間が掛かり、効率が悪い

→コンピュータを使って作成できれば早いし効率的!

・「請求書発行システムを開発してほしい」

(経営上のニーズ(必要性))

・システム化方針の決定

「予算の都合からサーバは 1 台まで、ソフトウェアは自社開発することで業務に合わせる……」

・システム化計画の決定

「来年 3 月末までに開発完了させる」

→開発スケジュールを立てる

- ・システム化計画の基本要件の確認
- ・対象業務の内容の確認
- ・対象業務のシステム課題の定義 など



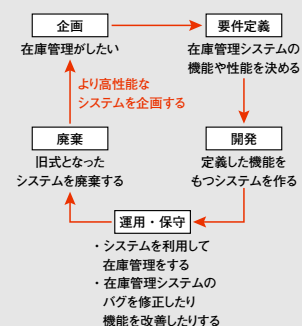
攻略のカギ



ソフトウェア ライフサイクル

問 49

企画、要件定義、開発、運用及び保守といった、ソフトウェア(システム)を企画し、開発し、それを運用していく過程での一連のプロセス(業務)の流れのこと。



【要件定義プロセス】

- ・業務要件とシステム要件を明確にする
 <システム要件> 請求書を印刷する機能をもたせる
 <業務要件> 印刷した請求書を封筒に入れ投函する
 (人手で行わなければならない作業)
- ・非機能要件(性能など)を決定する
 請求書は最大で1分に2枚印刷できるようにする
 ⋮



【開発プロセス】

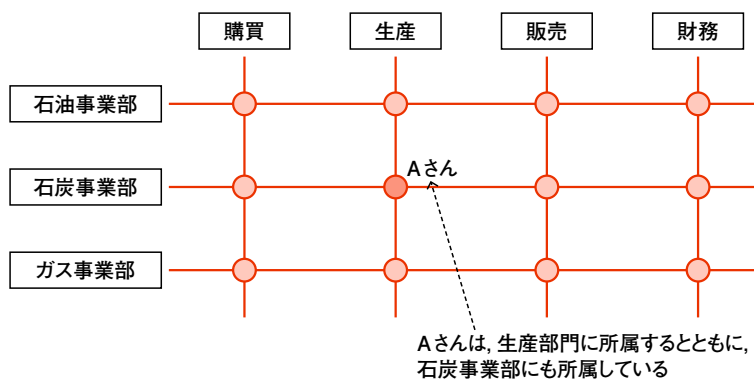
- ・開発手順の承認・作成
- ・システム設計
- ・プログラム設計
- ・プログラミング
- ・システムテスト・ユーザ受入れテスト
- ・システムの移行 ほか



共通フレームが規定しているソフトウェアライフサイクルプロセスの企画プロセスでは、事業で必要な機能や、システムに関する経営上のニーズなどをまとめ、情報システムを構築するためのシステム化方針を策定し、システムを実現するための計画(システム化計画)の立案が行われます。

システム化計画の立案では、システム化計画の基本要件の確認、対象業務(システム化する業務)の内容の確認、及び対象業務のシステム課題の定義などの作業が実行されます。以上から、ウの記述が適切です。他は要件定義プロセスで定義します。

問50 マトリックス組織



マトリックス組織とは、組織員が自己の専門とする職能部門と、特定の事業を遂行する部門の両方に所属する形態をとっている組織のことです(イ)。この組織は、職能制組織の特徴(命令の上意下達が生かされる)と事業部制組織の特徴(特定の事業に関して自己完結的な経営活動を展開できる)の両方を生かそうとすることを目的としています。

- × ア 事業部制組織の説明です。
- イ 正解です。
- × ウ 職能制組織の説明です。
- × エ プロジェクト組織の説明です。



事業部制組織

問50

利益責任と業務遂行に必要な機能を、製品別、顧客別または地域別にもつことにより、自己完結的な経営活動を展開できる組織構造。



職能制組織

問50

営業、経理、事務などの、企業において遂行される各種の活動の性質(職能)別に分類された組織構造。



プロジェクト組織

問50

新事業開発のために編成される組織構造。活動期間や目標を定め、独立した活動単位として活動する。

解答

問49 ウ

問50 イ

平成28年度 秋期 午後問題

問 1

オンラインストレージサービスの利用における情報セキュリティ対策に関する次の記述を読んで、設問1～4に答えよ。

J社は、従業員数150名の電気機器メーカーである。顧客企業から提示される仕様に基づいて電気製品を設計、製造している。

J社では、1年前に最高情報セキュリティ責任者（CISO）及び情報セキュリティ委員会を設置し、情報セキュリティポリシーを定め、情報セキュリティ関連規程を整備した。情報セキュリティ委員会の事務局は、情報システム課が担当している。また、各部の部長は、情報セキュリティ委員会の委員及び部における情報セキュリティ責任者を務め、自部の情報セキュリティを適切に確保し、維持、改善する役割を担っている。各情報セキュリティ責任者は、自部の情報セキュリティに関わる実務を担当する情報セキュリティリーダーを選任する。

J社では、社内ネットワークとインターネットの間にファイアウォールを設置している。また、社外のWebサイトの閲覧は、全てプロキシサーバ経由とし、業務上不要と思われるWebサイトへの接続をコンテンツフィルタで制限している。制限されているWebサイトへの接続が必要になった場合は、接続するPCを限定して、情報システム課が一時的に制限を解除している。J社では、DHCPは使っておらず、PCのIPアドレスは固定である。

〔オンラインストレージサービス〕

50名の従業員が所属する製造部では、製造の一部を協力会社であるB社に委託している。製造部からB社へは、従来、USBメモリを使用して製品製造に関係するファイルを提供していたが、USBメモリを管理する手間や、顧客企業からの急な仕様変更への対応が課題であった。製造部は、これらの課題を解決するために、顧客企業各社の了解も得た上で、2年前から、X社が提供するオンラインストレージサービス（以下、Xサービスという）をB社へのファイル提供に利用している。Xサービスはインターネット上で提供されている。サービス仕様（抜粋）を次に示す。

- ・専用のドメイン名をもち、インターネット上のどこからでもアクセスできる。
- ・スマートフォンやタブレットなど、PC以外の端末からでも利用できる。
- ・インターネット上における盗聴や改ざんへの対策として、サービスへの接続にHTTP over TLS (HTTPS) を使用している。
- ・利用アカウントのIDとして電子メールアドレス（以下、メールアドレスという）を登録し、パスワードを設定すれば、Webブラウザだけですぐに利用を始められる。
- ・利用アカウントごとに専用のフォルダが与えられ、ファイルの登録や、登録したファイルの閲覧、編集などの操作を行うことができる。フォルダ容量が10GBバイトまでは無料である。
- ・ファイルの登録時、又は登録後に、ファイル共有先を指定し、共有権限を付与することによって、指定した利用アカウントにファイルの操作を許可したり、インターネット上の誰にでもファイルの閲覧を許可したりすることができる。ファイルの共有設定には表1に示す4種類がある。

表1 Xサービスにおけるファイルの共有設定

番号	ファイル共有の有無	ファイル共有先	付与できる共有権限	設定内容
1	ファイル共有あり	指定した利用アカウント	編集権限	指定した利用アカウントに対して、ファイルの閲覧、編集、削除を許可する。
2			閲覧権限	指定した利用アカウントに対して、ファイルの閲覧を許可する。
3		パブリック ¹⁾	閲覧権限	利用アカウントがなくても、インターネットからのファイルの閲覧を可能にする。
4	ファイル共有なし	なし	権限なし	ファイルを登録した利用アカウント以外に、ファイル操作を許可しない。

注¹⁾ パブリックとは、インターネット利用者全般を意味する。

〔Xサービス利用規則〕

2年前、Xサービスの利用開始に当たって、製造部ではXサービス利用規則を作成し、部内に通知した。現在のXサービス利用規則を図1に示す。

なお、J社の社内規程では、スマートフォンやタブレットの業務利用は認めていない。かつ、PCを社外に持ち出して使用することも禁止している。

1. Xサービスを社外で業務利用することは禁止する。
2. Xサービスに登録するファイルは、B社に製造委託する製品の仕様とその関連情報に限定する。
3. メールアドレスをXサービス専用につけ、J社製造部が使用する利用アカウントのIDとして登録する。また、当該利用アカウントのパスワードは、製造部の情報セキュリティリーダーが設定し、製造部の従業員に通知する。
4. 当該利用アカウントのパスワードは半年ごとに更新し、秘密に管理する。
5. B社にファイルを提供する場合は、当該ファイルのファイル共有先としてB社の利用アカウントを指定し、“閲覧権限”を付与する。

図1 Xサービス利用規則（抜粋）

〔事故発生〕

1か月前、Q社からJ社に連絡が入った。Q社はJ社と取引関係はないが、Q社従業員がインターネット検索を行っていたところ、J社の社名が記載され、秘密情報と記されたファイルがXサービスで公開されているのを発見したので連絡したということであった。製造部の情報セキュリティリーダーであるS主任が調査したところ、J社がB社に提供するためにXサービスに登録している顧客企業の製品製造に関係するファイルの一つが公開されてしまっていることが判明した。問題のファイルは、ファイル共有先に「a1」が指定され、かつ、共有権限に「a2」が付与されていた。

S主任から報告を受けた製造部の情報セキュリティ責任者であるT部長は、CISOに一報を入れるとともに、①直ちにXサービスに登録している全てのファイルを削除し、Xサービスの利用を中止するように指示した。

今回の事故を重く見たCISOは、情報セキュリティ委員会を招集し、T部長に事故原因の調査と対策の検討を指示した。また、情報システム課のU課長には、製造部への支援を指示した。

〔原因調査〕

S主任は、T部長から指示を受けて事故原因の調査を開始し、Xサービスの情報セキュリティに影響する問題、つまり外部からの攻撃やシステム障害などが発生しなかったか、対象ファイルの共有設定を変更した者は誰かなどをX社に問い合わせた。X社からは、Xサービスの情報セキュリティに影響する問題は発生しておらず、また、操作の履歴情報を開示できるのは法令に基づいた開示請求があった場合に限り、と回答があった。

X社から調査協力を得ることができず、また、この時点で事件として警察に捜査を依頼することも難しいと思われたので、S主任はU課長と相談し、J社内の調査を進めることにした。U課長は②プロキシサーバを調査したが、不審な点は確認されず、また、製造部の全PCも調査したが問題点は見つけられなかったので、S主任は製造部の従業員全員に個別にヒアリングを行うことにした。

〔個別ヒアリング〕

S主任は、自分とT部長を除く製造部の従業員48名一人一人に対して、Xサービスの利用状況を確認した。ヒアリング結果を図2に示す。

- ・Xサービス利用規則については、全員がその存在を認識していた。
- ・Xサービスを利用したことがある者は48名中45名であった。残り3名はB社に關係する業務がなく、Xサービスの利用方法も知らなかった。
- ・Xサービスを利用したことがある45名の中に、ファイルを公開したという認識をもつ者はいなかったが、一部の者はファイルの共有設定に關係する“指定した利用アカウント”、“パブリック”、“編集権限”、“閲覧権限”といった用語の意味を正しくは理解していなかった。
- ・Xサービスをスマートフォンやタブレット、自宅のPCなどから利用している者はいなかった。

図2 ヒアリング結果(抜粋)

Xサービスでは、ファイル登録時点の共有設定は、ファイル共有先“なし”、共有権限“権限なし”が初期値である。B社にファイルを提供するには、ファイル登録時、又は登録後に共有設定を変更する必要がある。S主任は、ヒアリング結果のうち b という製造部の状況では、“B社にファイルを提供する際に、Xサービスのファイル共有設定を間違える”という事故が起きやすいと考えた。そこで、従業員がXサービスの利用を開始する時点でXサービス利用規則と利用方法についての十分な教育を行うとともに、③万一間違った共有設定がなされても第三者にファイルを読まれる可能性を下げる対策をXサービス利用規則の中に定めておくべきであったと反省した。

〔問題点の整理、対策の検討〕

S主任は、一連の調査結果をT部長に報告した。T部長は、Xサービスの利用中止によってB社への製造委託に支障を来していることから、Xサービスの利用を早期に再開できるようにS主任に検討を指示した。S主任は、製造部の従業員による共有設定の誤り防止を含めた対策をU課長と相談した。U課長は、XサービスをB社へのファイル提供に利用したこと自体が誤りであったとして、表2のように、Xサービスを業務で利用することの問題点とその理由を三つ指摘した。

表2 Xサービスを業務で利用することの問題点とその理由

番号	問題点	理由
1	c	今回の調査で判明したとおり、事故が発生した場合に原因を調べられないから。
2	従業員が自由にファイル共有を設定することができる。	個人向けサービスでは当然の機能であるが、従業員が自由にファイル共有を設定できると、 e 、 f の予防が困難であるから。
3	d	インターネット上で提供される社外のITサービスを業務で利用する場合は、なりすましのリスクを軽減するために2要素認証などの強固な対策が必要であると、情報セキュリティ関連規程に定めているから。

次は、U課長とS主任の会話である。

U課長：製造部の業務を考慮すると、USBメモリを使ったファイル提供に戻すことは難しいのではないかと思います。何か代替案を考えていますか。

S主任：同じオンラインストレージサービスでも、法人向けに有償で提供されているサービスには管理機能を強化しているものが多いので、そうしたサービスを使うことを考えたいと思います。

U課長：利用するサービス自体を切り替えることによって、問題点1～3の解決を図るということですね。

S主任：はい。ただし、現在のXサービス利用規則の内容では、④事故発生時の原因特定は困難です。適切な法人向けサービスに切り替えるとともに、利用規則も作り直すつもりです。

U課長：今回の事故によって、全社の情報セキュリティ対策がまだ十分でないことに気づきました。情報セキュリティ委員会の事務局として、情報セキュリティ委員会に対して追加の⑤組織的対策を行うように働きかけた上で、情報システム課としても⑥技術的対策を進め、情報セキュリティの改善に努めます。

S主任は、新しい利用規則をどのように作成すべきか、U課長とともに検討した。また、法人向けサービスの選定方法についてU課長から技術的なアドバイスを受けた。

その後、S主任は問題点1～3に対応したオンラインストレージサービスとして、W社の法人向けオンラインストレージサービス（以下、Wサービスという）を選定し、Xサービスからの切替えについて、T部長の承認を得た。T部長は、情報セキュリティ委員会の承認と顧客企業各社の了解を得た上でWサービスの利用規則を新たに定め、製造部従業員への周知など十分な準備を行い、Wサービスを使ってB社へのファイル提供を再開した。

設問1 〔事故発生〕について、(1)、(2)に答えよ。

- (1) 本文中の□ a1 □, □ a2 □に入れる字句の組合せはどれか。aに関する解答群のうち、適切なものを選び。

aに関する解答群

	a1	a2
ア	B社の利用アカウント	閲覧権限
イ	B社の利用アカウント	編集権限
ウ	Q社の利用アカウント	閲覧権限
エ	Q社の利用アカウント	編集権限
オ	パブリック	閲覧権限
カ	パブリック	編集権限

- (2) 本文中の下線①のように指示した理由はどれか。解答群のうち、最も適切なものを選び。

解答群

- ア J社が使用しているXサービスの利用アカウントのIDとパスワードが漏えいしたことが明らかであり、J社がXサービスに登録している全てのファイルに被害が及ぶおそれがあったから
- イ Xサービスがサイバー攻撃を受けたことが明らかであり、公開されたファイルの他にも、流出したファイルやマルウェア感染などの被害を受けたファイルが存在する可能性があったから
- ウ Xサービスよりも機能が豊富であり、かつ、不正アクセスやマルウェアへの対策も十分な信頼できるサービスに早急に移行することを決定したから
- エ 原因は不明だが、Xサービスに登録している全てのファイルが公開されたことが明らかであり、

J社としても早急に被害の拡大を防止する必要があったから

オ ファイルが公開された原因が不明であり、J社がXサービスに登録している他のファイルや、今後登録するファイルにも被害が及ぶおそれがあったから

カ ファイルがマルウェアに感染したことが明らかであり、J社がXサービスに登録している他のファイルや、今後登録するファイルにも被害が及ぶおそれがあったから

設問2 本文中の下線②について、次の(i)～(iii)のうち、調査を行う目的として適切なものだけを全て挙げた組合せを、解答群の中から選べ。

- (i) Xサービス以外のオンラインストレージサービスが利用されていなかったかを確認するため
- (ii) 情報システム課が一時的に制限を解除したWebサイトへの接続状況を確認するため
- (iii) 製造部のPC以外のJ社PCの中に、Xサービスに接続したのがあるかを確認するため

解答群

- | | | | |
|---------------|----------------------|---------------------------|---------------------|
| ア (i) | イ (i), (ii) | ウ (i), (ii), (iii) | エ (i), (iii) |
| オ (ii) | カ (ii), (iii) | キ (iii) | |

設問3 【個別ヒアリング】について、(1)、(2)に答えよ。

- (1) 本文中の□b□に入れる字句はどれか。解答群のうち、最も適切なものを選べ。

bに関する解答群

- ア** Xサービスの利用方法を知らない従業員が3名いた
- イ** Xサービスの利用規則の存在を従業員全員が認識していた
- ウ** Xサービスをスマートフォンやタブレット、自宅のPCなどから利用している従業員がいなかった
- エ** ファイルの共有設定に関係する用語の意味を正しくは理解していない従業員がいた

- (2) 本文中の下線③について、次の(i)～(iv)のうち、該当する対策だけを全て挙げた組合せを、解答群の中から選べ。

- (i) 登録するファイルに電子署名を付与する。
- (ii) 登録するファイルを暗号化する。
- (iii) ファイル登録後、B社だけに、登録したファイルのハッシュ値を連絡する。
- (iv) ファイル登録後、B社だけに連絡し、B社のダウンロードが完了次第直ちに削除する。

解答群

- | | | | |
|---------------------------|---------------------------|--------------------------|----------------------------|
| ア (i), (ii) | イ (i), (ii), (iii) | ウ (i), (ii), (iv) | エ (i), (iii) |
| オ (i), (iii), (iv) | カ (i), (iv) | キ (ii), (iii) | ク (ii), (iii), (iv) |
| ケ (ii), (iv) | コ (iii), (iv) | | |

設問4 【問題点の整理, 対策の検討】について、(1)～(4)に答えよ。

- (1) 表2中の□c□, □d□に入れる字句はどれか。解答群のうち、最も適切なものを選べ。

c, dに関する解答群

- ア** スマートフォンやタブレットから利用できる。
- イ** 操作の履歴情報が提供されない。
- ウ** 通信中の情報が暗号化されない。
- エ** 登録したファイルに対するウイルスチェック機能をもたない。
- オ** メールアドレスとパスワードだけで利用できる。

(2) 表2中の e, f に入れる字句はどれか。解答群のうち、最も適切なものを選び。

e, fに関する解答群

- | | | | |
|---|--|--|--|
| ア DDoS 攻撃 | イ 意図的な公開 | ウ クラッキング | エ 誤操作 |
| オ スパムメール | カ 中間者攻撃 | キ なりすまし | ク フィッシング |
| ケ 紛失 | | | |

(3) 本文中の下線④について、図1のどの項番が事故発生時の原因特定を困難にしているか。解答群のうち、最も適切なものを選び。

解答群

- | | | | | |
|---|---|---|---|---|
| ア 1 | イ 2 | ウ 3 | エ 4 | オ 5 |
|---|---|---|---|---|

(4) 本文中の下線⑤及び⑥について、次の(i)～(viii)のうち、今回の事故を受けて情報セキュリティ委員会と情報システム課が行うべき対策を三つ挙げた組合せはどれか。解答群のうち、最も適切なものを選び。

[情報セキュリティ委員会が行うべき組織的対策]

- (i) オンラインストレージサービス業者との秘密保持契約を見直し、情報流出の予防に関する条項を強化する。
- (ii) 業務に関係がないインターネット利用を禁止する旨を情報セキュリティ関連規程に定める。
- (iii) 社外のITサービスの導入について、全て情報セキュリティ委員会の承認を必要とすることを情報セキュリティ関連規程に定める。
- (iv) 情報システムの利用アカウントの共有を禁止する旨を情報セキュリティ関連規程に定める。

[情報システム課が行うべき技術的対策]

- (v) Xサービスの利用アカウントのIDに登録していたメールアドレスを廃止し、新たに選定する法人向けのオンラインストレージサービスの利用アカウントのIDとして登録する専用のメールアドレスを新たに用意する。
- (vi) 新たに選定する法人向けのオンラインストレージサービスに登録する全てのファイルを、定期的にバックアップする。
- (vii) 新たに選定する法人向けのオンラインストレージサービスに登録するファイルに電子署名を付与するために、電子証明書を準備する。
- (viii) オンラインストレージサービスは、情報セキュリティ委員会の承認を得たものだけ接続を許可するようにコンテンツフィルタを設定する。

解答群

- | | | | |
|---|---|---|--|
| ア (i), (ii), (vi) | イ (i), (iv), (viii) | ウ (i), (v), (viii) | エ (ii), (iii), (vii) |
| オ (ii), (iv), (vi) | カ (ii), (vi), (vii) | キ (iii), (iv), (viii) | ク (iii), (v), (vii) |
| ケ (iii), (vi), (viii) | コ (iv), (v), (vi) | | |

問 1

攻略のカギ

オンラインストレージサービスの利用中に発生したインシデントを題材として、ファイル共有設定の不備、利用者の知識不足に起因する事故、及びインターネット上のサービスを利用する際の組織的・技術的対策について問う問題です。

設問1 (1) J社とは無関係のQ社から事故の連絡が来たことが重要です。

(2) 〔事故発生〕で説明されている状況から、どのようなことが起こったのかを把握します。

設問2 冒頭の「社外のWebサイトの閲覧は、全てプロキシサーバ経由とし、……」という記述とJ社のIPアドレスの様態が解答の糸口になります。

設問3 (1) 「Xサービスのファイル共有設定を間違える」ことの原因に該当する、図2中のヒアリング結果が解答になります。

(2) インターネット上の第三者がファイルを閲覧できる状態にされても、その内容を読まれにくくするためには、第三者が内容を読めなくしたりすることが有効です。

設問4 (1) 空欄c, dの理由について、関連する内容を〔原因調査〕や〔オンラインストレージサービス〕の記述から読み取ります。

(2) 「従業員が自由にファイル共有を設定できる」ことによって、従業員の故意または過失によってファイル共有設定のミスが発生することが重要です。

(3) 同じアカウントを複数の従業員が使い回すという、アカウント管理における重大な問題が発生しているので、これを禁止する対策が適切です。

(4) (i) ～ (viii) の各対策によって、今回の事故の発生原因（サービスの提供元の姿勢、複数の従業員によるアカウントの共有）を防止できるかを確認します。

設問1 事故の状況

(1)

空欄a

〔事故発生〕の記述では、J社とは取引関係がないQ社から、インターネット上に秘密情報を発見したと連絡が来ています。Q社がXサービスの利用アカウントを使用しているという記述がないことや、「Q社従業員がインターネット検索を行っていたところ」という記述から、Xサービスを使用しておらず、利用アカウントももっていないQ社従業員が、J社のファイルを参照できる状態になっています。

表1から、利用アカウントがなくてもインターネットからファイルを閲覧できるのは、ファイル共有先が「パブリック」であり、共有権限が「閲覧権限」であるときだけです(図A)。

よって、空欄a1には「パブリック」、空欄a2には「閲覧権限」が入ります。空欄aには「オ」が適切です。

(2)

今回の事故が発見された時点で原因が既に判明しているのであれば、直ちに対策の検討をさせるのが適切です。しかし、下線①の直後で「今回の事故を重く見たCISOは……T部長に事故原因の調査と対策の検討を指示」しています。よって、発見の時点ではファイルが公開された原因が判明していません。これを踏まえて、ア～カが適切かを検証します。

ア 問題文冒頭から〔事故発生〕までには、J社が使用しているXサービスの利用アカウントのIDやパスワードが漏えいしたという記述はありません。「J社が使用しているXサービスの利用アカウントのIDやパスワードが漏えいしたことが明らか」と断

番号	ファイル共有の有無	ファイル共有先	付与できる共有権限	設定内容
1	ファイル共有あり	指定した利用アカウント	編集権限	指定した利用アカウントに対して、ファイルの閲覧、編集、削除を許可する。
2			閲覧権限	指定した利用アカウントに対して、ファイルの閲覧を許可する。
3		パブリック ¹⁾	閲覧権限	利用アカウントがなくても、インターネットからのファイルの閲覧を可能にする。
4	ファイル共有なし	なし	権限なし	ファイルを登録した利用アカウント以外に、ファイル操作を許可しない。

注¹⁾ パブリックとは、インターネット利用者全般を意味する。

図A

定することはできません。

イ アと同様に、【事故発生】の時点ではファイルが公開された原因が判明していないので、「Xサービスがサイバー攻撃を受けたことが明らか」とはいえませんが。

ウ本文中では、このような決定をしていません。

エ 今回の事故で公開されたファイルは一つだけであり「全てのファイルが公開されたことが明らか」とはいえませんが。

オ ファイルが公開された原因は不明です。今回の事故で公開されたファイルは一つだけですが、対策をとらないままにすると、同じ原因で今後他のファイルが公開される可能性があるため、Xサービスの利用を停止するのが適切です。

カ アと同様に、【事故発生】の時点ではファイルが公開された原因が判明していないので、「ファイルがマルウェアに感染したことが明らか」とはいえませんが。

以上から、**オ**が適切です。

設問2 アクセスの調査

冒頭で「社外のWebサイトの閲覧は、全てプロキシサーバ経由とし、業務上不要と思われるWebサイトへの接続をコンテンツフィルタで制限している」と説明されています。また、J社では「DHCPは使っておらず、PCのIPアドレスは固定」です。J社内のPCからXサービスを利用するとき、プロキシサーバを経由するので、接続元のPCのIPアドレスがプロキシサーバのログに記録されます。PCのIPアドレスは固定なので、同じPCからXサービスにアクセスするとき、接続元のPCのIPアドレスは常に同じになります。よって、プロキシサーバを調査することで、J社内のどのPCからXサービスにアクセスしたかを確認できます。

【原因調査】で「U課長は②プロキシサーバを調査したが、不審な点は確認されず、また、製造部の全PCも調査したが問題点は見つけられなかった」としています。下線②の調査をした後に製造部の全PCの調査をしているので、下線②の調査では製造部以外の社内のPCを調査していると考えられます。Xサービスは製造部しか使用しておらず、他の部からアクセスすることはないはずです。製造部のPC以外のJ社PCの中に、Xサービスに接続したものがあれば、そのPCを使用した社員が不正な操作をした可能性があります。すなわち、下線②の調査は(iii)を目的としています。**キ**が適切です。

(i) 業務上不要と思われるWebサイトへの接続は、プロキシサーバのコンテンツフィルタで制限されているので、J社内のPCがXサービス以外のオンラ

インストレージサービスに接続しようとしても拒否されます。今回の事故では、このような接続は行われていません。

(ii) 制限されているWebサイトに接続すること、今回のXサービス上の事故には特に関連がありません。

設問3 原因ととるべき対策

(1)

空欄b

空欄bの状況で「B社にファイルを提供する際に、Xサービスのファイル共有設定を間違える」という事故が起きやすいとしています。よって、空欄bは「Xサービスのファイル共有設定を間違える」ことの原因となります。図2で「一部の者はファイルの共有設定に係る“指定した利用アカウント”……」といった用語の意味を正しくは理解していなかった」とのヒアリング結果が示されています。このような従業員は、“パブリック”などの共有権限を、意味を正しく理解しないまま設定する可能性があります。その結果、サービスのファイル共有設定を間違えます。空欄bには**エ**の記述が適切です。

(2)

下線③は「万一間違った共有設定がなされても第三者にファイルを読まれる可能性を下げる」ための対策です。ファイルの共有設定が“パブリック”にされ、インターネット上の第三者がファイルを閲覧できる状態であっても、その内容を読まれにくいようにするのが適切です。

(i) 電子署名を付与することで、ファイルの作成者になりすましでないことを確認したり、改ざんを検知したりすることはできます。しかし、その内容は元のままなので、第三者にファイルを読まれる可能性を下げることはできません。

(ii) 登録するファイルを暗号化すれば、第三者がその内容を読むことは困難になります。適切な対策です。なお、(ii)には記述されていませんが、この対策ではファイルを暗号化するとともに、J社の製造部とB社だけに、暗号化や復号に必要な鍵を知らせておく必要があります。

(iii) 登録したファイルのハッシュ値をB社だけに連絡しても、ファイルが第三者に公開可能な状態になっていれば、Q社従業員が行ったように、インターネット検索によってファイルを読むことが可能になります。第三者にファイルを読まれる可能性を下げることはできません。

(iv) ファイル登録後、B社だけに連絡し、B社のダウンロードが完了次第直ちに削除することで、ファイルがXサービス上に存在する時間を可能な限り短くすることができるので、第三者にファイルを読まれる可能性は低くなります。適切な対策です。

以上から、**ケ** ((ii), (iv)) が適切です。

設問4 対策

(1)

空欄c

空欄cの理由は表2中で**図B⑥**の箇所のとおりです。**【原因調査】**において、X社から「操作の履歴情報を開示できるのは法令に基づいた開示請求があった場合に限る」と回答され、調査協力を得ることができなかったと説明されています。したがって、X社から操作の履歴情報の提供が得られなかったという問題点があります。空欄cには**イ**が入ります。

空欄d

空欄dの理由は表2中で**図B⑥**の箇所のとおりです。2要素認証とは、性質の異なる2つの認証手段を用いることです。利用者IDとパスワードの入力だけでなく、指紋などの生体認証も成功させないと、ログインを許可しないようにすることが2要素認証の例です。

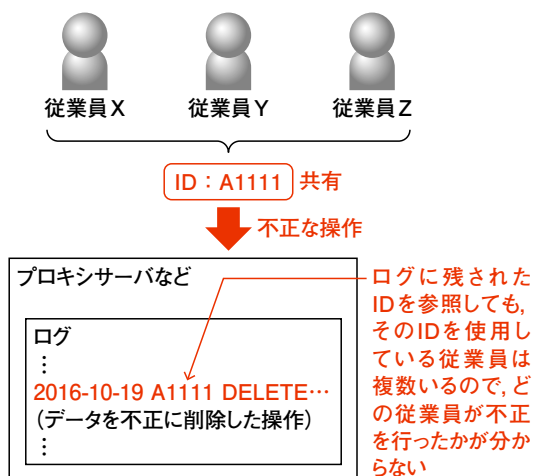
【オンラインストレージサービス】で、Xサービスは「利用アカウントのIDとして電子メールアドレス…」を登録し、パスワードを設定すれば、……すぐに利用を始められる」としており、IDとパスワードの入力だけでログインや利用ができる状況です。よって、Xサービスでは2要素認証が実現されていません。表2の番号3では、このような点を問題としています。空欄dには**オ**が入ります。

(2)

表2の番号2の理由で「従業員が自由にファイル共有を設定できる」ことで、空欄eや空欄fの予防が困難になると説明されています。従業員が自由にファイル共有を設定可能な状況では、設問3の(1)で示されているように、ファイル共有の知識に乏しい従業員が、誤った権限を設定する可能性があります。また、従業員が自由にファイル共有を設定できるので、ファイル共有のファイル共有先を意図的に「パブリック」にして、インターネット上に内容を公開するような不正行為をする危険性もあります。以上から、空欄e、fには「**意図的な公開**」(**イ**)、「**誤操作**」(**エ**)が順不同で入ります。

(3)

図1の利用規則のうち、3.では「メールアドレスをXサービス専用につけ、J社製造部が使用する利用アカウントのIDとして登録」しています。この利用<一つのIDを複数の従業員が共有する状態>



図C

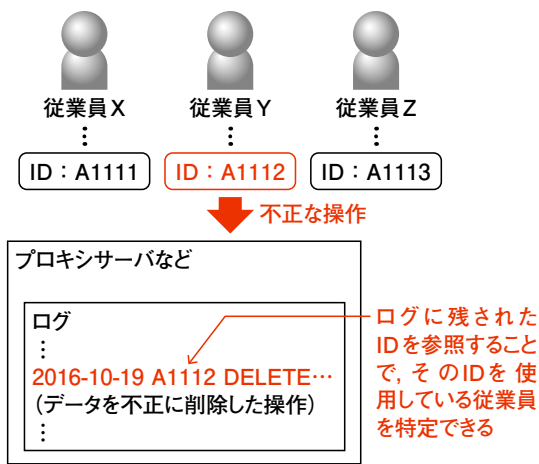
番号	問題点	理由
1	c	今回の調査で判明したとおり、 ⑤事故が発生した場合に原因を調べられないから。
2	従業員が自由にファイル共有を設定することができる。	個人向けサービスでは当然の機能であるが、従業員が自由にファイル共有を設定できると、 ④e 、 ④f の予防が困難であるから。
3	d	インターネット上で提供される社外のITサービスを業務で利用する場合は、 ⑥なりすましのリスクを軽減するために2要素認証などの強固な対策が必要であると、情報セキュリティ関連規程に定めているから。

図B

アカウントのパスワードを「製造部の従業員に通知」しているので、製造部の従業員全員が同じ利用者IDとパスワードを使い回していると分かります。このような利用形態では、そのIDを用いて不正行為が行われても、どの従業員が不正をしたかを特定できず、事故発生時の原因特定が難しくなります(図C)。

IDを共有させず、従業員ごとに1つのIDを割り当てて使うことで、不正行為が行われたときなどには操作したIDから従業員を特定できます(図D)。

<IDを共有させず、一つのIDを1人の従業員だけで使用させる状態>



図D

よって、「3」(ウ)が適切です。

(4)

- (i) Xサービスを提供しているX社とは、秘密保持契約を締結していません。また、Xサービスから切り替えたWサービスを提供しているW社とも、同様に秘密保持契約を締結していません。J社が契約の見直しをする必要はありません。
- (ii) 業務に関係がないインターネット利用を禁止しても、今回のような事故は防止できません。今回の事故は、B社にファイルを提供するという業務上必要な作業を、Xサービスを利用して行ったことで発生したためです。
- (iii) 今回の事故では、Xサービスの提供元のX社から操作の履歴情報を開示してもらえなかったのが、原因を特定できませんでした。ITサービスを導入するとき、事故の発生時に協力が得られるかといったことを考慮して、可能な限り協力的な提供元のITサービスを使用することで、今回のような事故の発生時に原因を特定しやすくなります。社外のITサービスを導入するとき、情報セキュリ

ティ委員会の承認を得るようにすることで、その提供元の事故発生時の協力姿勢、及び情報セキュリティへの取組みを適切に行っているかといったことを、サービスの利用前に検証できます。今回のような事故への対策として適切です。

- (iv) 情報システムの利用アカウントの共有を禁止することで、どの従業員が不正または誤操作を行ったかを把握できるので、事故発生時の原因特定につながります。今回のような事故への対策として適切です。
 - (v) この対策では、「利用アカウントのIDとして登録する専用のメールアドレス」を用意しているので、当該メールアドレスによる一つのIDだけを使用しています。よって、今回の事故においてIDを共有していたのと同じことをしています。このような対策では、事故発生時の原因特定が困難になります。
 - (vi) オンラインストレージサービスに登録する全てのファイルをバックアップすることで、同サービスの障害などによってファイルが消失しても、バックアップから復元することが可能です。しかし、これはファイルの可用性を維持するための対策であり、今回のような事故への対策にはなりません。
 - (vii) オンラインストレージサービスに登録するファイルに電子署名を付与することで、本人性の確認などには役立ちますが、今回のような事故への対策にはなりません。
 - (viii) オンラインストレージサービスは、情報セキュリティ委員会の承認を得たものだけ接続を許可するようにコンテンツフィルタを設定することで、安全なオンラインストレージサービスだけを使用させることができます。よって、情報セキュリティ対策が不十分である、不適切なオンラインストレージサービスの使用を禁止できます。今回のような事故への対策として適切です。
- 以上から、キ((iii)、(iv)、(viii))が適切です。

解答

- | | | | |
|-----|-----------|-----|-----------|
| 設問1 | (1) a : オ | 設問4 | (1) c : イ |
| | (2) オ | | d : オ |
| 設問2 | キ | | (2) e : イ |
| 設問3 | (1) b : エ | | f : エ |
| | (2) ケ | | (順不同) |
| | | | (3) ウ |
| | | | (4) キ |

問2

情報機器の紛失に関する次の記述を読んで、設問1、2に答えよ。

Z社は、従業員数2,000名の生命保険会社であり、東京に本社をもち、全国に支社が点在している。以下、本社及び各支社を拠点という。

Z社では、拠点の営業員が、会社貸与の持出し用ノートPC（以下、NPCという）を携帯して顧客を訪問し、商品説明資料、見積書、契約書の作成などを行っている。Z社の本社情報システム部は、NPCの情報セキュリティ対策とその持出し管理のために、表1に示すルールを定めている。

表1 NPCの情報セキュリティ対策とその持出し管理ルール

全 PC のための 情報セキュリティ 対策	・ 次の情報セキュリティ対策を行う。 (a) OS へのログインパスワード設定 (b) BIOS パスワードの設定 (c) CD 及び DVD からの起動禁止設定 (d) OS、ソフトウェアの最新化（脆弱性対応） (e) ウイルス対策ソフトのパターンファイル最新化及び定期的なフルスキャン (f) 5分間無操作でスクリーンをロックし、パスワード入力要求 (g) 外部記憶媒体の接続制限（Z社が従業員に貸与する USB メモリだけが接続可）
NPC のための情報 セキュリティ対策	・ (a)～(g)に加えて、次の情報セキュリティ対策を行う。 (h) ハードディスクドライブ（以下、HDD という）全体の暗号化 (i) クラウドサービスで提供される契約管理システム（以下、L システムという）を利用するためのクライアント証明書¹⁾のインストール ・ (h)、(i)の情報セキュリティ対策を施した NPC に“対策済 NPC”の文字列と有効期限日（最長6か月）を記載したシールを貼り付ける。
NPC による情報 の持出し管理	・ NPC に情報を保存して持ち出す場合は、本社情報システム部が運用する NPC 持出し申請システムを利用して、その都度、所属する部課の長の承認を得る。その際、持ち出すファイルのリストを NPC から出力し、NPC の資産管理番号と合わせて申請する。 ・ NPC の持出し頻度が高く、都度申請では支障が生じる場合には、部課の長は、最長1か月の“NPC 期間持出し”を承認することができる。

注¹⁾ L システムでは、クライアント認証とパスワード認証の組合せによる2要素認証の仕組みが提供されている。クライアント認証は公開鍵暗号方式を利用する。NPC 上のクライアント証明書と秘密鍵は、NPC の故障などに備えるためにエクスポート可能にしている。L システムの利用アカウントは本社情報システム部が管理している。L システムでは顧客情報を含む契約書を管理している。

Z社は、各拠点に情報セキュリティ管理責任者とその配下の情報セキュリティリーダを置いている。また、各拠点に配置された情報システム担当は、各拠点で利用するPCなどの情報機器の貸出し、表1に示した情報セキュリティ対策の設定と維持、持出し管理の実施指導、本社情報システム部と連携した情報システムの運用管理、利用支援などを行っている。

Z社の情報セキュリティ管理規程では、顧客情報を含めZ社が秘密として管理している情報（以下、秘密情報という）の漏えい及びその可能性がある情報セキュリティインシデント（以下、情報セキュリティインシデントをインシデントという）が発生した場合の対応手順を定めている。そのうち、従業員に貸与している情報機器の紛失・盗難が発生した場合の対応手順は図1のとおりである。

1. インシデントの発生

紛失・盗難の発生又はその可能性がある事象を発見した従業員は、直ちに、所属する部課（以下、当該部課という）の長に報告する。報告を受けた長は、直ちに、その時点で確認した事実関係を、当該部課がある拠点（以下、当該拠点という）の情報セキュリティ管理責任者に報告する。情報セキュリティ管理責任者は、情報機器への不正なアクセスのおそれ、秘密情報の紛失・漏えいの発生又はその可能性があると判断した場合には、インシデントの発生を宣言する。

2. 初動対応

情報セキュリティ管理責任者は、配下の情報セキュリティリーダーに対して、直ちに、初動対応の体制の編成及び初動対応の開始を指示する。情報セキュリティリーダーは、当該拠点の情報システム担当と協力して、インシデントの事実関係を整理し、情報機器に保存されていた情報の内容及び量、並びに暗号化、アクセス制御などの情報セキュリティ対策の実施状況を確認する。保存されていた情報に情報システムのアカウント情報が含まれる場合は、パスワードの変更やアカウントの停止を行うなど、インシデントの影響拡大を防止する措置をとる。情報セキュリティリーダーは、確認結果と防止措置を当該拠点の情報セキュリティ管理責任者に報告する。情報セキュリティリーダーは、必要に応じてインシデントの対応に当たるメンバを指名することができる。

以下省略（“3. 調査”，“4. 通知，報告及び公表”，“5. 復旧”，“6. 事後対応”が続く）。

図1 情報機器の紛失・盗難が発生した場合の対応手順（抜粋）

〔情報機器の紛失〕

R支社は、従業員数100名の支社であり、営業員が60名いる。R支社では、支社長が情報セキュリティ管理責任者を務め、各部課の長が情報セキュリティリーダーを務めている。

10月12日（水）10時30分頃、R支社の営業部1課のFさんが、客先からR支社に戻る途中、電車の網棚にかばんを置き忘れるという事象が発生した。かばんの中には、NPCが入っていた。

報告を受けたR支社長は、インシデントの発生を宣言し、営業部1課の情報セキュリティリーダーであるK課長に対して、直ちに初動対応を開始するよう指示した。また、R支社長の指示によって、K課長、各部の部長、及びR支社の情報システム担当として初動対応に当たるW主任が出席して、インシデント対策会議が開催されることとなった。

幸い、当日の15時頃にかばんとその中のNPCを回収することができた。しかし、紛失している間に、外部の者によってNPCを操作されたり、NPCから情報を窃取されたりした可能性は否定できない。K課長は、調査を継続しつつ、16時30分に開催予定のインシデント対策会議に向けてインシデント報告書案を作成することにした。

〔インシデント報告書案の作成〕

K課長は、まず、Fさんが置き忘れた情報機器（以下、紛失機器という）、紛失機器に保存されていた情報、及び紛失機器における情報セキュリティ対策の実施状況を表2のとおり整理した。

表2 インシデント報告書案(抜粋)

紛失機器	・ NPC (1 台) 資産管理番号: ZR00XXXX NPC 持出し申請システムにおいて、10 月 3 日に、1 か月間の NPC 期間持出しを承認した記録あり。 ・ 補足: 会社貸与のスマートフォンは紛失していない。 当日、会社貸与の USB メモリなどの外部記憶媒体は持ち出していない。
紛失機器に保存されていた情報の内容及び量	・ NPC 持出し申請システムにおいて、会社紹介資料、商品説明資料の持出し申請の記録あり。どちらも自社 Web サイトで社外に公開している資料。 ・ 持出し申請以後に保存した情報は調査中。
紛失機器における情報セキュリティ対策	・ 全 PC 及び NPC のための情報セキュリティ対策は、本社情報システム部が定める手順に従い正しく実施されていたことを、PC 管理ツールが NPC 紛失当日の朝に収集した情報を基に、W 主任が確認した。 なお、F さんのログインアカウントには情報セキュリティ対策を変更する権限はない。 ・ “対策済 NPC” シールは 7 月 25 日に発行されたものである。

続いて、K 課長は、インシデント報告書案の一部として、インシデント発生とその初動対応の経緯を図2のとおり整理した。

NPC の紛失から初動対応及び NPC の回収までの経緯		
(1) インシデントの発生及び報告		
09:45	F さん	訪問先を出る。
10:00	F さん	会社に戻るために、〇〇駅から××線に乗車。混んでいたため、立ったまま、かばんを目の前の網棚に置く。会社貸与のスマートフォンで電子メールを閲覧。
10:05	F さん	目の前の座席が空いたので、座る。かばんは網棚に置いたまま。
10:20	F さん	△△駅に到着。下車した後、網棚にかばんを置き忘れたことに気付く。
10:30	F さん	△△駅の係員にかばんの紛失を届ける。内容物は NPC、パンフレット、筆記用具など。その時点で、駅において該当する拾得物の届出はなし。
10:45	F さん	スマートフォンを使って、K 課長に、かばんの紛失を電話で連絡。 紛失した状況、かばんに NPC が入っていたこと、その NPC は持出しを承認されているが、紛失時にどのような情報を保存していたかは定かではないことを報告。
	K 課長	F さんに対し、警察に連絡するように指示。
10:55	K 課長	R 支社長に対し、第一報として、F さんからの報告内容を報告。
	R 支社長	インシデントの発生を宣言。K 課長に、直ちに体制を編成して初動対応を開始するように指示。
(2) 初動対応		
11:00	K 課長	関係者を召集して状況説明。初動対応を次のとおり開始。 (a) K 課長の実施内容 ・ 紛失物の捜索活動の支援 ・ 情報機器紛失時の状況など、事実関係の確認 ・ a (b) W 主任の実施内容 ・ 紛失機器の特定 ・ 紛失機器における b ・ c システムの特定 ・ 上記で特定したシステムにおいて F さんのアクセス権の無効化 ・ 上記で特定したシステムにおいて d

図2 インシデント発生とその初動対応の経緯

11:10	K 課長	R 支社長に電話で状況報告。
	R 支社長	対応の継続を指示するとともに、15:00 にインシデント対策会議を開催することを決定し、事実関係を整理するよう指示。
	W 主任	NPC 持出し申請システムにおける F さんの持出し申請記録を確認し、K 課長に連絡。
11:15	F さん	最寄りの警察署に、遺失届出書を提出。
11:20	W 主任	L システムにおいて F さんのアクセス権が無効化されたことを K 課長に報告。
11:45	F さん	R 支社に帰社。
	K 課長	事実関係を確認するために F さんにヒアリング。
	W 主任	
12:30	K 課長	この時点までに確認した事実関係と対応状況を R 支社長に報告。
(3) NPC の回収		
14:10	F さん	△△駅からかばんが見つかった旨の電話連絡を受ける。□□駅で、乗客が届けてくれていた。
	K 課長	R 支社長にインシデント対策会議延期を申し入れ、16:30 開始に決定。
14:50	F さん	□□駅でかばんとその中身を確認し、受領。
	K 課長	すぐに NPC を受け取る。
15:05	K 課長	R 支社長に電話で報告。

図2 インシデント発生とその初動対応の経緯(続き)

〔インシデントの影響及び対応〕

16時に、K課長はW主任に声を掛け、インシデント対策会議の事前確認のための打合せを行った。次はその時の会話である。

K 課長：Fさんは、NPCにはどのような情報が入っていたか定かではないと言っていました。契約書などの顧客情報は入っていたのでしょうか。

W 主任：NPCの持出し申請の時点では、顧客情報は含まれていませんでした。ただし、①持出しの承認の後でも、NPCに顧客情報を追加で保存できてしまいます。

K 課長：分かりました。②当社で定めた手順のうち、NPC紛失時にNPCの中の情報を盗まれるリスクを低減する手順は、施されていたでしょうか。

W 主任：はい。もちろんです。

K 課長：紛失時点で顧客情報がNPCに保存されていたかどうか、紛失後にNPCに誰かがアクセスしていたか、確認をお願いします。ところで、今、FさんはLシステムにアクセスができない状態ですね。

W 主任：はい。FさんのNPC内にあるクライアント証明書と秘密鍵が盗用される可能性を考慮した措置です。もし、Fさんの利用アカウントで認証に成功したとしたら、Fさんが担当する全ての顧客の情報にアクセスできてしまいます。

K 課長：すばやく対応してくれましたね。

W 主任：秘密鍵の漏えいの有無を調査するために、何者かがFさんの秘密鍵を使い、クライアント認証して e1 がLシステムの e2 のログ中にないか確認しました。確認したログの範囲では、不審な点はありませんでした。FさんがまたLシステムにアクセスできる状態にするために、f , アクセス権を有効にする予定です。

K 課長：FさんのNPCは、今後どのようになるのでしょうか。

W 主任：一時的にでも自社の管理を離れたことによって情報が盗まれたり、マルウェアが入れられたりした可能性があるので、g1。

K 課長：g2。

こうしてK課長はインシデント対策会議に臨み、インシデント報告書案に沿って事実関係、対応状況及び今後の調査予定を報告し、R支社長の了解を得た。

2日後、W主任から、NPC内に顧客情報は追加保存されていなかったこと、及びFさんがNPCを紛失していた間にNPCがアクセスされた痕跡はなかったことの報告があり、このインシデントは収束が宣言された。

設問1 【インシデント報告書案の作成】について、図2中の□a□～□d□に入れる字句はどれか。解答群のうち、適切なものを選び。

aに関する解答群

- ア** Fさんが紛失した情報の内容及び量の特定
- イ** Fさんが持ち出した情報の持出し方法の特定
- ウ** インシデントによる損害額の検討
- エ** インシデントの再発防止策の策定

bに関する解答群

- ア** “対策済NPC”シール発行記録の確認
- イ** Fさんの利用記録の確認
- ウ** 資産管理番号とFさんへの貸与記録の確認
- エ** 情報セキュリティ対策の実施状況の確認

cに関する解答群

- ア** Fさんがオフィスで使っている
- イ** Fさんが外出先からアクセスできる
- ウ** Fさんが顧客情報を保管している
- エ** Fさんが顧客訪問の際に画面を見せてもらったことがある

dに関する解答群

- ア** Fさんが当日訪問した顧客に関する顧客情報がダウンロードされていないかどうかに絞った確認
- イ** 社外から操作ログが改ざんされていないかどうかの確認
- ウ** 社外からパスワードリスト攻撃が行われていないかどうかの重点的な確認
- エ** 社外から不審なアクセスがないかどうかの幅広い確認

設問2 【インシデントの影響及び対応】について、(1)～(5)に答えよ。

- (1) 本文中の下線①について、どのような方法が考えられるか。次の(i)～(v)のうち、該当するものだけを全て挙げた組合せを、解答群の中から選べ。
- (i) 1か月間のNPC期間持出しの承認を得るとその期間中に、NPCを会社に持ち帰り、追加で保存できる。
 - (ii) NPCの持出しとは別に、会社貸与のUSBメモリに保存して持ち出すことによって、NPCに保存できる。
 - (iii) 外出先からLシステムにアクセスして、NPCにダウンロードして保存できる。
 - (iv) 外出先で、公衆無線LANに接続して、インターネット上で他社の公開Webサイトを閲覧し、NPCにダウンロードして保存できる。
 - (v) 顧客訪問先で、顧客から借りたUSBメモリからコピーして保存できる。

解答群

- | | | |
|---------------------------|--------------------------------------|--------------------------------|
| ア (i), (ii), (iii) | イ (i), (ii), (iii), (iv), (v) | ウ (i), (ii), (iii), (v) |
| エ (i), (iii) | オ (i), (iii), (v) | カ (i), (v) |
| キ (ii), (iii), (v) | ク (ii), (v) | ケ (iii), (iv), (v) |

コ (iii), (v)

- (2) 本文中の下線②について、表1に記載されている対策のうち、NPC紛失時に、NPC内のデータが読み取られるリスクを低減するための対策として最も効果的なものを、解答群の中から選べ。

解答群

ア (a) イ (b) ウ (c) エ (d) オ (e)
カ (f) キ (g) ク (h) ケ (i)

- (3) 本文中の , に入れる字句の組合せはどれか。eに関する解答群のうち、最も適切なものを選べ。

eに関する解答群

	e1	e2
ア	アクセスを試みた形跡	本日 00:00 から 11:20 まで
イ	アクセスを試みた形跡	本日 00:00 から 15:30 まで
ウ	情報をダウンロードした形跡	本日 00:00 から 11:20 まで
エ	情報をダウンロードした形跡	本日 00:00 から 15:30 まで

- (4) 本文中の に入れる適切な字句を、解答群の中から選べ。

fに関する解答群

ア FさんのLシステムの利用アカウントのパスワードを変更した後
イ Fさんの従来のクライアント証明書を失効させてから、新しい鍵ペアを生成しクライアント証明書を発行し直した後
ウ Fさんの秘密鍵のバックアップを取り寄せた後
エ 本社情報システム部でLシステムのログを保全した後

- (5) 本文中の , に入れる字句の組合せはどれか。gに関する解答群のうち、最も適切なものを選べ。

gに関する解答群

	g1	g2
ア	HDD を複製し、今日中には返却します	入念な調査をお願いします
イ	証拠保全をした上で調査しています	F さんには新しい NPC を手配しましょう
ウ	直ちに HDD を取り出し、データを消去した上で、破壊し、破棄します	情報漏えいがないように、確実にお願いします
エ	直ちに NPC を初期化して、OS から入れ直します	それなら安心ですね
オ	返却前に、F さんに NPC 中のファイルを確認してもらいましょう	私も立ち会います

問 2

攻略のカギ

インシデント発生時の各従業員の初動対応と、その後の対応を題材としています。社外に持ち出すPCへのセキュリティ対策の知識が問われています。

設問 1 空欄a, b: 図1の初動対応において、情報セキュリティリーダーの行動から解答を特定できます。空欄c: 特定したシステムにおいてFさんのアクセス権の無効化を実施していることが重要です。空欄d: 具体的な被害が発生していないことがヒントになります。

設問 2 (1) それぞれの方法で、顧客情報をダウンロードして保存できるかどうかを検証します。
(2) NPCが紛失して内部のデータが読み取られるリスクに対しては、そのデータを第三者が読み取りにくくすることが有効です。
(3) [インシデントの影響及び対応]で、「秘密鍵の漏えいの有無を調査」しており、不正アクセスの防御を目的としていないので、Fさんのアクセス権の無効化だけでは不十分です。
(4) 秘密鍵やパスワードなどが漏えいした場合の対策が必要になります。
(5) K課長とW主任の会話の後、W主任が2日間にわたってNPCの調査を継続している(NPCを破壊したりはしていない)ことから、解答を特定できます。

設問 1 インシデントの状況

空欄 a, b

図1では、インシデント発生時の初動対応において、情報セキュリティリーダーは次の行動をすると定めています(図A)。なお、次の行動は、「必要に応じてインシデントの対応に当たるメンバ」として指名された者が、情報セキュリティリーダーの代わりに行うことがあります。

- インシデントの事実関係の整理
- 情報機器に保存されていた情報の内容及び量の確認

- 情報機器への情報セキュリティ対策の実施状況の確認

図2の11:00の、(a)の囲みの部分で「インシデントの事実関係の整理」が行われています(図B)。「情報機器に保存されていた情報の内容及び量の確認」と「情報機器への情報セキュリティ対策の実施状況の確認」は、囲みより後の箇所で実施されています。(a)に関する解答群のうち、この二つのいずれかに該当するのはア(Fさんが持ち出した情報の内容及び量の特定)だけです。残りの「情報機器への情報セキュリティ

1. インシデントの発生

紛失・盗難の発生又はその可能性がある事象を発見した従業員は、直ちに、所属する部課(以下、当該部課という)の長に報告する。報告を受けた長は、直ちに、その時点で確認した事実関係を、当該部課がある拠点(以下、当該拠点という)の情報セキュリティ管理責任者に報告する。情報セキュリティ管理責任者は、情報機器への不正なアクセスのおそれ、秘密情報の紛失・漏えいの発生又はその可能性があるかと判断した場合には、インシデントの発生を宣言する。

2. 初動対応

情報セキュリティ管理責任者は、配下の情報セキュリティリーダーに対して、直ちに、初動対応の体制の編成及び初動対応の開始を指示する。情報セキュリティリーダーは、当該拠点の情報システム担当と協力して、インシデントの事実関係を整理し、情報機器に保存されていた情報の内容及び量、並びに暗号化、アクセス制御などの情報セキュリティ対策の実施状況を確認する。保存されていた情報に情報システムのアカウント情報が含まれる場合は、パスワードの変更やアカウントの停止を行うなど、インシデントの影響拡大を防止する措置をとる。情報セキュリティリーダーは、確認結果と防止措置を当該拠点の情報セキュリティ管理責任者に報告する。情報セキュリティリーダーは、必要に応じてインシデントの対応に当たるメンバを指名することができる。

以下省略(“3. 調査”, “4. 通知, 報告及び公表”, “5. 復旧”, “6. 事後対応”が続く)。

図A

(2) 初動対応		
11:00	K 課長	関係者を召集して状況説明。初動対応を次のとおり開始。 (a) K 課長の実施内容 - 紛失物の搜索活動の支援 - 情報機器紛失時の状況など、事実関係の確認 a (b) W 主任の実施内容 - 紛失機器の特定 - 紛失機器における b c システムの特定 - 上記で特定したシステムにおいて F さんのアクセス権の無効化 - 上記で特定したシステムにおいて d
11:10	K 課長	R 支社長 電話で状況確認

図 B

の内容及び量	持出し申請以後に保存した情報は調査中。
紛失機器における情報セキュリティ対策	・全 PC 及び NPC のための情報セキュリティ対策は、本社情報システム部が定める手順に従い正しく実施されていたことを、PC 管理ツールが NPC 紛失当日の朝に収集した情報を基に、W 主任が確認した。 なお、F さんのログインアカウントには情報セキュリティ対策を変更する権限はない。 ・“対策済 NPC” シールは 7 月 25 日に発行されたものである。

図 C

対策の実施状況の確認」は、インシデントの対応に当たるメンバである W 主任が、(b)以降で実施しています。表 2 の「紛失機器における情報セキュリティ対策」で「……NPCのための情報セキュリティ対策は、本社情報システム部が定める手順に従い正しく実施されていたことを、……W 主任が確認した」との記述(図 C)から、この確認を行ったのは W 主任と分かります。

空欄 b には **イ**(情報セキュリティ対策の実施状況の確認)が入ります。

空欄 c

「**c** システムの特定」をした後に、「上記で特定したシステムにおいて F さんのアクセス権の無効化」をしていることから、紛失した NPC を取得した者が、それを操作してシステムにアクセスできないようにして、インシデントの影響が社内のシステムに及ばないようにしています。よって、F さんが外出先からアクセスできるシステムの特定が行われています。空欄 c には **イ**(F さんが外出先からアクセスできる)が入ります。

空欄 d

インシデントにおいて具体的な攻撃が発生しているときは、個別の措置が必要になります。しかし、今回の

インシデントでは「外部の者によって NPC を操作されたり、NPC から情報が窃取されたりした可能性は否定できない」としています。インシデントが発覚した時点では、社内のシステムに対する具体的な攻撃、または情報の漏えいや改ざんなどは発生していません。この場合は、情報漏えいが本当に発生したのかを確認するために、社外からの不正アクセスについてあらゆる可能性を考え、広範に検証する必要があります。よって、**エ**(社外から不審なアクセスがないかどうかの幅広い確認)が適切です。

ア F さんが紛失した NPC は、10 月 3 日から 1 か月間の NPC 期間貸出しをしているので、紛失した日(10 月 12 日)までの間に別の顧客情報が保存されている可能性があります。また、NPC から L システムにアクセスして顧客情報をダウンロードできるので、当日訪問した顧客に関する顧客情報だけを確認するのではなく、それ以外の顧客情報が NPC に保存されたり、ダウンロードされたりしていないかを確認する必要があります。

イ L システムにアクセスして顧客情報を不正にダウンロードする攻撃が行われる可能性もあるので、この確認を行うだけでは不十分です。

ウ 他の攻撃が行われる可能性もあるので、この確認

を行うだけでは不十分です。

設問2 対策

(1)

- (i) Lシステムでは「顧客情報を含む契約書を管理」しています。NPC期間持出しの承認を得た後に、社内でNPCを操作してLシステムにアクセスするなどの方法で、顧客情報をダウンロードして保存できます。
- (ii) NPCには、Z社が従業員に貸与するUSBメモリだけを接続できます。このUSBメモリを介してNPCに顧客情報を保存できます。
- (iii) 外出先からLシステムにアクセスすることで、顧客情報をNPCにダウンロードできます。
- (iv) インターネット上で他社の公開Webサイトを閲覧して入手した情報は、Z社が管理している顧客情報ではなく、他社の公開情報です。このような情報を保存したNPCを紛失しても問題はありません。この方法では顧客情報を保存できません。
- (v) NPCには、Z社が従業員に貸与するUSBメモリしか接続できません。この方法では顧客情報を保存できません。

以上から、**ア** (i), (ii), (iii)) が正解です。

(2)

- (a), (b) OSへのログインパスワードやBIOSパスワードを設定することで、そのパスワードを知らない者はNPCを起動して操作できなくなります。しかし、NPCのハードディスクドライブ(HDD)を抜き取り、他のPCに接続することで、内部の情報を読み取ることが可能です。
- (c) CD及びDVDからの起動を禁止しても、HDDからOSを起動することでNPCを操作して情報を読み取ることが可能です。
- (d), (e) OSやソフトウェアを最新化することで、脆弱性を突く攻撃は防げます。しかし、紛失したNPCを外部の者に操作されて情報を盗まれることは防げません。また、ウイルス対策ソフトのパターンファイル最新化や定期的なフルスキャンによって、マルウェア感染のリスクを低下させることはできますが、外部の者にNPCを操作されることは防止できません。
- (f) この対策では、NPCの利用者が一時的に離れたときに、画面に映っている情報を盗み見られるリスクを減らせますが、紛失したNPCを外部の者に操作されて情報を読み取られることは防げません。

(g) この対策では、外部記憶媒体からマルウェアが感染することは防げます。しかし、紛失したNPCを外部の者に操作されて情報を読み取られることは防げません。

(h) HDD全体を暗号化することで、NPCが紛失して外部の者の手に渡っても、復号に必要な鍵を知らなければ、HDDの内容を読み取ることはできません。NPC内のデータが読み取られるリスクを少なくすることが可能です。

(i) この対策は、Lシステムにログインするためのものです。

以上から、最も効果的なものは、**ク** (h)) です。

(3)

空欄e

この問いは**ア**または**ウ**と誤りやすくなっています。図2では、11:20にFさんのアクセス権を無効化しているので、Lシステムへの不審なアクセスの有無の確認は11:20まで実行すればよく、それ以降は確認しなくてよいと考えがちです。しかし、**【インシデントの影響及び対応】**で、W主任は「**秘密鍵の漏えいの有無を調査するために**、何者かがFさんの秘密鍵を使い、クライアント認証して **e1** がLシステムの **e2** のログ中にないか確認」していることから、Fさんのアクセス権を無効化することだけでなく、秘密鍵が漏えいしたかどうかを検証する必要があります。

表1の注から、NPC上の秘密鍵は「NPCの故障などに備えるためにエクスポート可能」にしています。エクスポート可能とは、NPCに保存されている秘密鍵を、外部に取り出せるということです。NPCが紛失して外部の者の手に渡ったとき、紛失したNPCを入手した者が、その中の秘密鍵を他のPCなどにエクスポートして保存し、Lシステムへのアクセスを試みる考えられます。11:20にFさんのアクセス権が無効化されたとしても、それより後の時刻において、秘密鍵を入手した者がLシステムに不正アクセスを試みる可能性があります。このようなアクセスがあった場合、秘密鍵が外部に漏えいしたことが分かります。

以上から、秘密鍵の漏えいの有無を調査するには、本日の11:20以降においても、Lシステムに対する不審なアクセスがないかを検証する必要があります。よって、空欄e1には「**アクセスを試みた形跡**」、空欄e2には「**本日00:00から15:30まで**」が入ります。**✓**が適切です。

秘密鍵の漏えいの有無を調査するためには、Lシステムへのアクセスの形跡があったかどうかを確認するのが適切です。情報をダウンロードしたかどうかを確

認する必要はないので、**エ**は誤りです。

(4)

空欄f

漏えいした可能性がある秘密鍵を使用し続けると、外部の者がその秘密鍵を用いて、FさんになりすましてLシステムへのアクセスを試みるのを防げません。秘密鍵やパスワードなどが漏えいした可能性がある場合は、それを無効にして外部の者から不正に利用されないようにし、その後新しい秘密鍵などを発行して利用者に提供するのが適切です。空欄fには**イ**が入ります。

(5)

空欄g

K課長とW主任の会話の後に、「2日後、W主任から、NPC内に顧客情報は追加保存されていなかったこと、及びFさんがNPCを紛失していた間にNPCがアクセスされた痕跡はなかったことの報告があり、このインシデントは収束が宣言された」と説明されています。W主任は、Fさんが紛失したNPCの内容を確認して、顧客情報の追加保存がなかったことなどを調査し

たり、アクセスされた痕跡の有無を検証したりしています。この点から、WさんがNPCの内容を引き続き調査するという記述が空欄g1に入ります。これに該当するのは**イ**の「証拠保全をした上で調査しています」という記述だけです。他の解答群では、FさんにNPCを返却したり、HDDを破壊したり、NPCを初期化したり、またはFさんにNPCのファイルを点検させたりしているので不適切です。

W主任が調査している間は、FさんはNPCを使用できないので、新しいNPCを貸し出す必要があります。K課長は「Fさんには新しいNPCを手配しましょう」と発言しています。

以上から、空欄gに当てはまるのは**イ**です。

解答

- | | | |
|-----|--------------|-----------------|
| 設問1 | a: ア | (2) ク |
| | b: エ | (3) e: イ |
| | c: イ | (4) f: イ |
| | d: エ | (5) g: イ |
| 設問2 | (1) ア | |

問3

業務用PCでのWebサイト閲覧に関する次の記述を読んで、設問1～3に答えよ。

P社は、従業員数1,000名の消費者向け健康食品製造会社であり、経営方針として自社のブランドイメージを重視している。P社のマーケティング部では、社外向けWebサイトのコンテンツのうち、製品紹介情報、IR情報、CSR情報などの管理を行っている。マーケティング部には20名が在籍し、二つの課がある。マーケティング1課は、ブランドマーケティング戦略を担当している。マーケティング部では、情報セキュリティ責任者をA部長が、情報セキュリティリーダをマーケティング1課のB課長が務めている。

P社では全従業員が基盤情報システムを利用して日々の業務を行っている。基盤情報システムは、会社貸与の業務用PC(以下、PCという)、LAN及びインターネット接続から成るネットワークサービス、ディレクトリサービス、社内ファイル共有サービス、電子メールサービスなどから構成されている。P社従業員は、LANに接続された各自のPCから各サービスを利用している。また、LANからのプロキシサーバを経由しないインターネット接続はファイアウォールによって遮断されている。

P社には、基盤情報システム以外にも勤怠管理システム、交通費精算管理システム及び人事管理システムがある。P社従業員は、出勤時と退勤時に各自の磁気スライプカード型の従業員証をタイムレコーダに通すことになっており、出退勤時刻が勤怠管理システムに記録される。P社の課長以上の職位の者は、直属の部下について、勤怠管理システムを用いて出退勤時刻などの勤怠管理情報を、交通費精算管理システムを用いて交通費精算情報を、人事管理システムを用いて人事評価情報を確認できる。

基盤情報システム、勤怠管理システム、交通費精算管理システム及び人事管理システムは同じタイムサーバに基づいて時刻同期がなされている。それらの情報システム及び自社Webサイトの構築と運用管理は、情報システム部が行っている。

情報システム部のC部長が、P社の最高情報セキュリティ責任者(CISO)を務めている。情報システム部には運用管理課があり、基盤情報システムに対して図1に示す設定と運用管理を行っている。また、利用については図2に示すP社基盤情報システム利用規程(以下、利用規程という)を整備している。

1. 設定

- ・ PC 上のハードディスクドライブ（以下、HDD という）全体を暗号化
- ・ PC 上の Web ブラウザで、プロキシサーバを利用するように設定
- ・ 社内ファイル共有サービスでの共有フォルダの設定は、次のとおり
 - ディレクトリサービスを利用してアクセス権の設定を管理
 - アクセス権は、各利用部門からの申請に応じて設定単位を変更可能
 - アクセス権の設定単位は、次のいずれか一つを選択
 - 部単位：特定の部に属する従業員だけがアクセス可能
 - 課単位：特定の課に属する従業員だけがアクセス可能
 - 職位単位：特定の部に属する部長、課長、主任のいずれかの職位以上の従業員だけがアクセス可能
 - 従業員単位：特定の従業員だけがアクセス可能
 - デフォルトのアクセス権は、課単位

2. 運用管理

- ・ PC 上の OS、オフィスソフト、Web ブラウザ、ウイルス対策ソフトなどのソフトウェアのインストール、パッチ適用及びアップデートを一括で運用管理
- ・ 一括運用管理対象のソフトウェアのパッチ及びアップデートがベンダからリリースされた場合は、適用可否の確認を速やかに行い、適用が必要と判断したものを適用
- ・ PC の管理者権限は、PC 運用管理担当者だけに付与
- ・ 各利用部門からの情報システム利用に関する各種申請について、利用規程にのっとった承認を得たものだけを受理

図1 P社基盤情報システムにおける設定と運用管理（抜粋）

1. パスワードは、使用できる文字種（大小英字、数字、記号）全てを組み合わせ、8文字以上、かつ、他人に推測されにくいものとし、他人に知られないよう適切に管理すること。
2. 機密性が高い電子データには、暗号化を施し、適切なアクセス権を設定すること。
3. 各利用部門から情報システム部への情報システム利用に関する各種申請については、所属部門長及び情報セキュリティリーダーの承認を得ること。
なお、機密性が高い情報の取扱いに関連する申請内容については、CISOの承認を得ること。
4. 情報セキュリティインシデント（以下、インシデントという）の発生時には、その対応として第一に被害拡大防止に努め、第二に証拠保全に努めること。
なお、所属部門の情報セキュリティリーダー又は情報システム部からの指示があった場合には、その指示に従うこと。

図2 利用規程（抜粋）

〔インシデントの発見と初動対応〕

9月26日（月）10時、運用管理課のHさんが基盤情報システムを運用監視していたところ、9月23日（金）20時から25日（日）にかけての社内からインターネットへの通信量が前週の金曜日から日曜日にかけてのものと比較して大幅に増えていることを発見し、直ちに運用管理課のD課長に報告した。D課長は不審に思い、プロキシサーバのログを調査するようHさんに指示した。その結果、図3に示すことが判明した。

- ・ 大量の通信は、同一の社外IPアドレス（以下、アドレスYという）へのアクセスであった。
- ・ POSTメソッドから始まってCONNECTメソッドが連続したHTTP over TLS（HTTPS）通信であった。
- ・ 発信元はマーケティング1課に所属する入社2年目のEさんのPC（以下、E-PCという）であった。

プロキシサーバのログの調査結果

D課長はその旨をC部長に報告の上、B課長に連絡した。連絡を受けたB課長は利用規程にのっとり、①Eさんに初動対応を指示し、併せてA部長に報告した。

B課長は、自席のPCを利用してEさんの□a1□を調査した。Eさんは市場調査業務を担当しているので、P社の競合情報、消費者動向などについての様々なインターネット上のWebサイトを日々閲覧している。次に情報システム部の協力の下、B課長による調査結果とE-PCから□a2□へのアクセスログとを突き合わせたところ、大量の通信が記録されていた時刻の中には、Eさんが□a3□時刻が含まれていた。さらに、Eさんへの聞き取り調査を行ったところ、Eさんは、P社が入居するオフィスの法定点検に基づく停電時以外は離席、外出又は帰宅の際、E-PCにログインしたままにしていたことが判明した。これらのことから、今回の不審なアクセスは、Eさん自身によるものではないと推定された。

B課長とD課長による協議の結果、同日15時に、情報システム部による調査及び対応が開始された。情報システム部における調査の結果を図4に、各事象の発生日時を表1に示す。

- ・E-PCは、不正プログラムVに感染していた。
- ・不正プログラムVは、E-PCにインストールされていたソフトウェアZ（以下、ソフトZという）の脆弱性Mを突いて侵入するものであった。ソフトZは、インストールされて以来、パッチが適用されていなかった。
- ・E-PC上では、ウイルス対策ソフトが起動しないように管理者権限を用いて設定されていた。

図4 情報システム部における調査の結果（抜粋）

表1 各事象の発生日時

日付	時刻	事象
7月4日	11:00	Eさんが、業務の都合から、しばらくの間、E-PC上のウイルス対策ソフトが起動しないように設定してほしいとHさんに依頼
	11:30	Hさんが、E-PC上のウイルス対策ソフトが起動しないように管理者権限で設定
8月2日	15:00	ソフトZの開発元が脆弱性Mの対策パッチをリリース
8月4日	10:00	ウイルス対策ソフトの開発元が、不正プログラムVに対応するパターンファイルをリリース
9月23日	20:00	E-PCがアドレスYに向けた通信を開始
9月26日	10:00	Hさんが通信量の大幅増加を発見、D課長に報告 Hさんがプロキシサーバのログを調査開始
	13:30	Hさんがプロキシサーバのログの調査結果をD課長に報告 D課長がC部長に報告、B課長に連絡
	13:45	B課長がEさんに初動対応を指示、A部長に報告後、Eさんへの聞き取り調査などを開始
	14:30	B課長とD課長が協議
	15:00	②情報システム部が、次に示す調査及び対応を開始 ・社内からアドレスYへの通信を遮断 ・E-PCのHDD内のデータを証拠保全 ・E-PCからの大量の通信の原因の把握

注記 日付は全て同年のものである。

〔情報システム部による調査結果の中間報告〕

情報システム部によるE-PCの調査結果の中間報告が、9月27日（火）13時から行われた。次は、その時のD課長とB課長の会話である。

D課長：マーケティング部と情報システム部の間では、ソフトZに対するパッチ適用を含めた運用管理について何も取決めがない状態でした。マーケティング部からのソフトウェアインストール申請書には、パッチ適用などの運用管理についての依頼は記載されていませんでした。

B課長：すみません、依頼内容が不十分でしたね。

D課長：他にもこれらと同じようなことがあったら問題なので、引き続き調査をします。ところで、7月4

日から昨日までのログ中の通信先を解析したところ、ウイルス対策ソフトの開発元などによって悪意あるWebサイトと判断されたURL又はIPアドレスに該当するものではありませんでした。感染原因は、電子メールの添付ファイルやUSBメモリからと考えられますが、もし、感染原因がインターネット上のWebサイトへのアクセスだとしたら、Eさんがアクセスしたのは、閲覧するだけで不正プログラムに感染するように、企業の□b□の公開Webサイトが□c□されたものだったとも考えられます。

B課長：□b□のURLということであれば、悪意あるWebサイトだとは思わないので、防ぎようがないですね。Webサイトが□c□されたことによって、そのWebサイトの所有者たる企業は□d□となるだけでなく、Webサイト閲覧者に対しても不正プログラムによる被害が及ぶので、□e□の立場になってしまうおそれがあり、非常に怖いですね。③私自身の職務からも人ごとではないので、すぐに対策を検討しましょう。D課長、協力をお願いします。

〔課題の改善〕

内容が不明なデータがE-PCから社外に大量に送信されたことから、□f□が起きたおそれもあるとB課長は考えた。そこでEさんにヒアリングした。その結果、マーケティング2課へのヒアリングも必要と考えられたので、マーケティング2課のプレゼントキャンペーン担当を務めているG主任にもヒアリングを行った。それらの結果を図5に示す。

1. Eさんへのヒアリング結果

- ・マーケティング2課が8月に募集した、P社製品購入者向けプレゼントキャンペーンの匿名アンケート結果に関するファイル（以下、アンケートファイルという）を、9月8日（木）頃、社内共有フォルダN内で発見した。
- ・④いつか業務に役立つかもしれないと考え、アンケートファイルを社内共有フォルダNからE-PC内にコピーした。
- ・E-PC内には、暗号化されたアンケートファイルを復号したものはなかった。また、アンケートファイル以外には機密性が高い情報を含んだファイルはなかった。

2. G主任へのヒアリング結果

- ・アンケートファイルの暗号化には、マーケティング部内の共有パスワードを利用していた。
- ・アンケートファイルは、G主任を含めたマーケティング2課のプレゼントキャンペーン担当者3名が共同作業できるように、社内共有フォルダNに保存していた。
- ・アンケート結果には、P社製品の味や食感、健康食品としての有用性などへの批評や競合会社製品との比較による辛らつな意見が書かれていた。

図5 B課長による、Eさん及びG主任へのヒアリング結果

B課長は、A部長にこれまでの調査結果の報告を行うとともに、図6に示す項目の検討が必要であると進言した。

1. 調査結果から発見された、改善すべき課題

- 1-1 ソフトZの運用管理についてマーケティング部と情報システム部の間で取決めがなかった。
- 1-2 EさんとHさんの当事者間だけでE-PC上のウイルス対策ソフトの停止を決めていた。
- 1-3 HさんがE-PC上のウイルス対策ソフトを起動するように設定を戻すのを忘れていた。
- 1-4 Eさんが業務と直接関係ないマーケティング2課の管理下のアンケートファイルをE-PC上に保存していた。
- 1-5 アンケートファイルの暗号化のパスワードが、部内の共有パスワードであった。

2. 情報システム部の調査から□f□が発生したことが確になった場合の対処

- 2-1 P社所在地管轄の警察署や関係機関への届出又は報告
- 2-2 アンケートファイルの関係者へのおわびと説明、社外への公表

図6 検討が必要な項目

B課長は、社内関係者の協力を得て課題の改善を実施した。また、中間報告以降の情報システム部の調査結果から□f□が発生したおそれは低いことが分かった。

B課長は、改善すべき課題が図6の1-1から1-5の他にもないかの確認をA部長に提案し、了承を得た。

B課長は、改善すべき課題が他にもないか、□g□を実施した。その結果、他の課題が発見され、マーケティング部内で改善策の検討が開始された。

A部長は、マーケティング部内での他の課題の発見に至ったB課長の提案を高く評価した。発見された課題とその改善策をA部長がP社経営陣に報告したところ、これらの提案は、全社的な改善活動に発展した。

設問1 【インシデントの発見と初動対応】について、(1)～(3)に答えよ。

(1) 本文中の下線①について、次の(i)～(v)のうち、B課長がEさんに指示すべき初動対応だけを全て挙げた組合せを、解答群の中から選べ。

- (i) E-PCのHDD内のフォルダとファイルに対して何も操作をしない。
- (ii) E-PCの電源を強制切断し、かつ、電源ケーブルを電源コンセントから外す。
- (iii) E-PCをLANから切り離す。
- (iv) E-PCを再起動する。
- (v) E-PCを使ってEさんの基盤情報システムへのログインパスワードを変更する。

解答群

- | | | | |
|--------------------|---------------------------|-------------------------|----------------------|
| ア (i) | イ (i), (iii) | ウ (i), (iv), (v) | エ (ii), (iii) |
| オ (ii), (v) | カ (iii), (iv), (v) | キ (iii), (v) | ク (iv), (v) |

(2) 本文中の□a1□～□a3□に入れる字句の組合せはどれか。aに関する解答群のうち、最も適切なものを選べ。

aに関する解答群

	a1	a2	a3
ア	勤怠管理情報	インターネット	退勤していた
イ	勤怠管理情報	ディレクトリサービス	休暇を取得していた日の
ウ	交通費精算情報	社内ファイル共有サービス	外出していた
エ	交通費精算情報	ディレクトリサービス	出張していた日の
オ	人事評価情報	インターネット	無断欠勤していた日の
カ	人事評価情報	社内ファイル共有サービス	残業していた

(3) 表1中の下線②について、次の(i)～(v)のうち、該当する作業だけを全て挙げた組合せを、解答群の中から選べ。

- (i) E-PCのHDDを別のHDDにフルコピーし、その別のHDDを“秘密”とラベルに書いた資料保存用紙封筒に入れ、封印し、Eさんが管理するマーケティング部の鍵付きロッカーに保管
- (ii) E-PCのHDDを別のHDDにフルコピーした上で、最新のパターンファイルを搭載した別のPCに、その別のHDDを接続してフルスキャンを実施
- (iii) アドレスYへの通信をプロキシサーバで遮断し、ファイアウォールではインターネットへの通信のうち、プロキシサーバを経由しないものだけを許可
- (iv) 他の作業に先駆けて最初にE-PCにOS及びアプリケーションのクリーンインストールを実施した上で、E-PCをEさんに返却
- (v) プロキシサーバなどのネットワーク機器上のログとE-PC上のイベントログなどを時系列に沿って整理及び分析

解答群

- | | | | |
|----------------------------|--------------------------|----------------------|---------------------|
| ア (i) | イ (i), (iii), (v) | ウ (i), (iv) | エ (ii) |
| オ (ii), (iii), (iv) | カ (ii), (v) | キ (iii), (iv) | ク (iii), (v) |
| ケ (iv), (v) | | | |

設問2 【情報システム部による調査結果の中間報告】について、(1)、(2)に答えよ。

- (1) 本文中の□b□～□e□に入れる字句はどれか。解答群のうち、最も適当なものを選べ。

b, cに関する解答群

- | | | | |
|--------------|---------------|-------------|-------------|
| ア 改ざん | イ 偽装 | ウ 正規 | エ 設計 |
| オ 非正規 | カ ボット化 | | |

d, eに関する解答群

- | | | | |
|--------------|--------------|--------------|--------------|
| ア 加害者 | イ 首謀者 | ウ 助言者 | エ 扇動者 |
| オ 第三者 | カ 被害者 | | |

- (2) 本文中の下線③について、B課長とD課長はどのような対策を検討したか。解答群のうち、最も適当なものを選べ。

解答群

- ア** 自社Webサイトのアクセシビリティを見直し、自社Webサイトの閲覧者に対する利便性と安全性を確保することによって、自社のブランドイメージの向上を図る。
- イ** 自社Webサイトの改ざんを防ぐために、自社Webサーバを情報システム部に依頼して速やかに停止させ、自社Webサーバを社外のパブリッククラウド上に移行し、他者とのリスク共有(リスク移転)を図る。
- ウ** 自社Webサイトの脆弱性検査を定期的に実施して、問題があれば修正する。また、新たな脆弱性が発見された場合にも必要な対応をとる。
- エ** 自社Webサイトのトップページ上において、重要なお知らせとして、自社Webサイトにドライブバイダウンロードが仕掛けられた可能性があると公表し、自社Webサイトの閲覧者に対して注意を喚起する。

設問3 【課題の改善】について、(1)～(3)に答えよ。

- (1) 本文中及び図6中の□f□に入れる字句はどれか。解答群のうち、最も適切なものを選べ。

fに関する解答群

- | | | |
|-----------------------|---------------------|-----------------------|
| ア E-PCへのDDoS攻撃 | イ E-PCへの辞書攻撃 | ウ E-PCへの総当たり攻撃 |
| エ 情報改ざん | オ 情報破壊 | カ 情報漏えい |

- (2) 図5中の下線④について、社内共有フォルダNのアクセス権の設定単位はどのようなになっていたと考えられるか。解答群のうち、最も適切なものを選べ。

解答群

- | | | | |
|--------------|----------------|---------------|--------------|
| ア 課単位 | イ 従業員単位 | ウ 職位単位 | エ 部単位 |
|--------------|----------------|---------------|--------------|

- (3) 本文中の□g□に入れる字句はどれか。解答群のうち、最も適切なものを選べ。

gに関する解答群

- ア 情報システムのうち、マーケティング部内の従業員が利用しているものに対し、脆弱性検査
- イ マーケティング部内で取り扱っている全ての情報資産とその取扱い状況を可視化した上で、リスクアセスメント
- ウ マーケティング部内で取り扱っている全てのファイルの所在と所有者を洗い出し、各ファイルのアクセス権限の見直し
- エ マーケティング部における、E-PC以外でのウイルス対策ソフトを停止させたままのPC又はパッチ適用並びにアップデートが行われていないPCの有無の確認
- オ マーケティング部における、E-PC以外でのソフトZがインストールされたPCの有無と利用状況の確認

問3 攻略のカギ

マルウェアの感染への対策、Webサイトの改ざんなどへの迅速な対策、及び改善する必要がある課題の発見を題材としています。大部分の問いにおいては問題文中の記述をヒントとして解答を特定できます。

設問1 (1) マルウェアに感染したPCに対して、感染の拡大を防ぐとともに、感染の原因を特定するための適切な初動対応が必要になります。

(2) 今回の不審なアクセスの原因がEさん自身ではないことを推定するには、Eさんが不在の時間帯にもアクセスがあったかどうかを確認します。

(3) 各作業が、下線②の調査及び対応（通信の遮断、データの証拠保全、原因の把握）を行うのに適切かどうかを検討します。イベントログについての知識が必要です。

設問2 (1) D課長とB課長の会話から、各空欄の前後の記述をヒントとして解答を推測します。

(2) D課長とB課長は、企業のWebサイトが改ざんされたことに対して「すぐに対策を検討」しているので、これに適合する対策が正解になります。

設問3 (1) 内容が不明なデータ（暗号化されたもの）がE-PCから大量に送受信されているので、マルウェアが情報を暗号化して、密かに外部に流出させていると推定できます。

(2) Eさんが、自分が所属する課と異なる課のフォルダにアクセスしていることが重要です。

(3) B課長は、「改善すべき課題が図6の1-1から1-5の他にもないかの確認をA部長に提案」しているので、図6の1-1から1-5に該当するものを除外できます。

設問の解説に入る前に【プロキシサーバ】について解説します。

【プロキシサーバ】

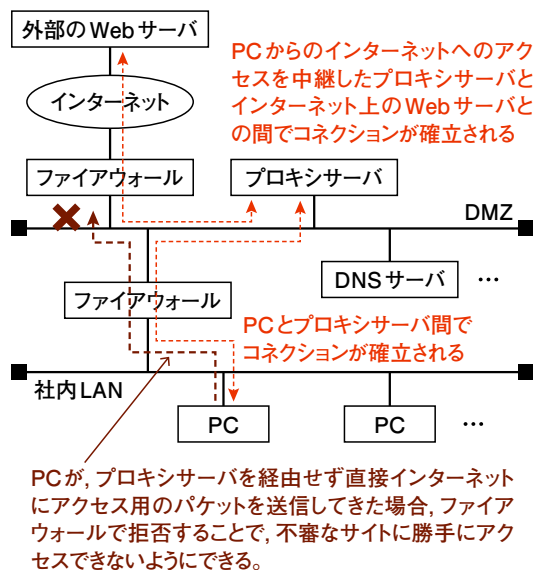
インターネット上のサーバに組織内のPCが直接アクセスすると、そのPCのIPアドレスなどが外部に知られて、不正アクセスなどの危険性が増加します。また、PCが直接インターネットにアクセスできる状況では、悪意のあるWebサイトに不用意にアクセスしてマルウェアに感染するなどの問題が発生します。

そこで、組織内に外部とのアクセスを中継するサーバを設置し、そこを経由して外部とアクセスする方法

をとります。このサーバをプロキシサーバといいます。（図A）

この方法によって、プロキシサーバのIPアドレスだけが外部に判明するため、安全性が高まります。また、プロキシサーバにはURLフィルタリング機能をもつものがあります。URLフィルタリング機能では、悪意のあるWebサイトのURLをブラックリストに登録してアクセスを禁止したり、アクセスを許可した安全なWebサイトのURLをホワイトリストに登録して、そのサイトへのアクセスだけを認めたりすることができます。

プロキシサーバには、一度アクセスしたWebコンテンツのキャッシュする機能があります。組織内のPC



図A

が一度アクセスしたWebページはプロキシサーバに保存されます。同じ組織内の別のPCが同じWebページにアクセスした場合、プロキシサーバに保存されているWebページの内容が返されます。これにより、表示時間の短縮を図れます。

設問1 初動対応

(1)

図3の内容から、E-PCからインターネットに向けて大量の通信が発生しています。このような現象は、PCに感染した不正プログラムが、社内の情報を盗んで外部の攻撃用サーバに送信したり、他のサーバに対して攻撃用のパケットを送信したりすることで発生します。E-PCは不正プログラムに感染した可能性があります。このような場合、次の初動対応をすることで、被害を最小限に食い止めるとともに、不正プログラムの種類の確認や証拠保全を図ります。

- 感染の疑いがあるPCをLANから切り離す
- 感染の疑いがあるPCの電源を切ったり、再起動したりせず、そのままにする

感染の疑いがあるPCをLANから切り離すことで、攻撃用のサーバに情報が渡らなくなります。また、感染の疑いがあるPCの電源を切ったり再起動したりすると、メモリ上の情報が失われ、稼働していた不正プログラムや、それがメモリ上に残っていた作業用のデータなどが消失します。感染の疑いがあるPCを後で調査するとき、メモリ上の情報が失われていると、稼働していた不正プログラムの種類や挙動などを突き

止めることができないことがあります。

以上から、B課長がEさんに指示する初動対応として適切なのは、**イ** ((i) と (iii)) です。

(2)

空欄a

【インシデントの発見と初動対応】でB課長が調査した結果、「今回の不審なアクセスは、Eさん自身によるものではない」と推定しています。こう考えるためには、EさんがE-PCを操作して大量のアクセスをしたのか、またはEさんが操作していないときにも大量のアクセスがあったのかを調べておく必要があります。Eさんが出勤して作業をしている期間だけ大量のアクセスがあった場合、前者の可能性が高くなります。Eさんが欠勤または退社している時間帯に大量のアクセスがあった場合、後者の可能性が高くなります。よって、Eさんの“**勤怠管理情報**” (空欄a1) を調査するのが適切です。

今回のインシデントでは、E-PCからインターネットへの大量のアクセスが発生しているので、E-PCから“**インターネット**” (空欄a2) へのアクセスログを入手し、Eさんの勤怠管理情報と突き合わせることで、上記の調査ができます。この調査によって、「今回の不審なアクセスは、Eさん自身によるものではない」と推定されたことから、Eさんが社内にはいない時刻においても大量の通信が記録されていると分かります。よって、空欄a3には“**退勤していた**”が入ります。

以上から、**ア**が適切です。

(3)

表1の9月26日15:00に、下線②の調査及び対応を実施しています。この調査及び対応は次のとおりです。

- 社内からアドレスYへの通信を遮断
 - E-PCのHDD内のデータを証拠保全
 - E-PCからの大量の通信の原因の把握
- (i) ~ (v) について、上記に該当するかを確認します。
- (ii) この作業を正解として選んでしまいがちなので、注意が必要です。この作業をすると、E-PCのHDD内のデータの証拠を保全できますが、E-PCからの大量の通信の原因の把握ができないままになります。(i)ではなく、次で説明する(ii)を行うことで、E-PCのHDD内のデータの証拠を保全するとともに、フルスキャンによってE-PCに感染した不正プログラムを突き止め、大量の通信の原因を把握するのが適切です。
- (iii) この作業によって、E-PCのHDD内のデータが保

全されます。また、E-PCに感染した不正プログラムを突き止め、大量の通信の原因を把握できます。

- (iii) この作業を正解として選んでしまいがちなので、注意が必要です。この作業によって、プロキシサーバを経由したアドレスYへの通信は遮断できますが、インターネットへの通信のうち、プロキシサーバを経由しないものがファイアウォールで許可されます。不正プログラムが、プロキシサーバを経由せず直接アドレスYへの通信をしてきた場合、許可されてしまいます。よって、社内からアドレスYへの通信を遮断することはできません。「アドレスYへの通信をプロキシサーバで遮断し、かつ、プロキシサーバを経由しない通信はファイアウォールで引き続き遮断する」のが適切な措置です。
- (iv) 他の作業に先駆けてE-PCのクリーンインストールを行うと、E-PCのHDD内のデータが保全されません。
- (v) プロキシサーバなどのネットワーク機器上のログには、通信の送信元や宛先などのデータが記録されます。また、PC上のイベントログには、アプリケーションを起動した時刻や参照されたファイル、及び操作内容などが記録されます。E-PC上のイベントログを確認することで、不正プログラムが稼働したことや、どの宛先に通信が行われたかなどを調査できます。

以上から、下線②の調査及び対応に該当する作業は **カ** ((ii), (v)) です。

設問2 原因

(1)

空欄b～e

D課長とB課長の会話中で「**空欄b**」のURLということであれば、**悪意あるWebサイトだとは思わないので、防ぎようがないですね**」と説明されていることから、利用者が悪意あるWebサイトとは思わないもの、すなわち企業や組織の正規のURLが用いられたと分かります。空欄bには「**正規**」(**ウ**)が入ります。

D課長が「**閲覧するだけで不正プログラムに感染するように、企業の正規の公開Webサイトが空欄c**された」と考えていることから、そのWebサイトには閲覧するだけで不正プログラムに感染する仕掛けが施されています。企業がこのような仕掛けをWebサイトに組み込むことはまずありません。よって、攻撃者がWebサイトの管理者権限を奪って、その一部を改ざんして上記の仕掛けを施したと考えられます。空欄cには「**改ざん**」(**ア**)が入ります。

B課長が「Webサイトが改ざんされたことによって、そのWebサイトの所有者たる企業は**空欄d**」となるだけでなく、Webサイト閲覧者に対しても不正プログラムによる被害が及ぶので、**空欄e**の立場になってしまう」と説明しています。Webサイトを攻撃者に改ざんされた企業は「**被害者**」(空欄d=**カ**)になりますが、そのWebサイトを放置して「閲覧者に対しても不正プログラムによる被害が及ぶ」ことで、その企業は閲覧者に不正プログラムの被害を与えた立場、すなわち「**加害者**」(空欄e=**ア**)になります。

(2)

下線③の直前で、D課長とB課長は企業のWebサイトが改ざんされたことを話し合い、それに対して「すぐに対策を検討」しています。よって、Webサイトの改ざんなどの攻撃を防止するための対策を取っていると分かります。解答群中でこの対策に該当するのは **ウ** だけです。自社Webサイトの脆弱性検査を定期的実施し、問題を修正することで、改ざんなどの攻撃を受ける可能性を減らせます。また、新たな脆弱性が発見された場合、セキュリティパッチをすぐに適用するなどの方法で、脆弱性を残さないようにすることが有効です。

ア 自社Webサイトのアクセシビリティを見直すことで自社Webサイトの閲覧者に対して利便性を確保できますが、脆弱性をなくさないと安全性を確保できません。

イ 自社Webサーバを社外のパブリッククラウド上に移行しても、Webサーバプログラムなどに脆弱性が残っている限り、改ざんを防げません。

エ 自社Webサイトの閲覧者に注意を喚起しているだけで、改ざんを防止することはできません。

設問3 影響と対策

(1)

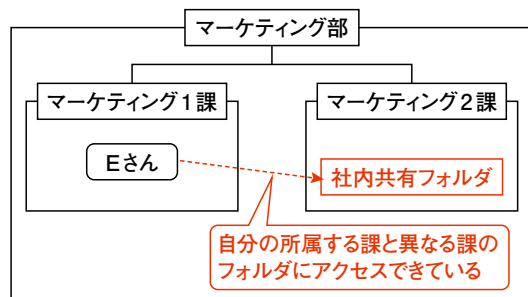
空欄f

【課題の改善】で「内容が不明なデータがE-PCから大量に送受信」されていると説明されています。不正プログラムが、社内のPCなどから取得した情報を暗号化して、外部の攻撃用サーバに送ることで、内容が不明なデータの送受信が発生します。よって、社内の情報が外部に漏えいしていると考えられます。空欄fには「**情報漏えい**」(**カ**)が入ります。

(2)

下線④では、Eさんは社内共有フォルダにアクセス

して、アンケートファイルをE-PC内にコピーしています。図3から、Eさんはマーケティング1課に所属します。社内共有フォルダはマーケティング2課に所属します。よって、Eさんは自分の所属する課とは異なる課のフォルダにアクセスできる状況です(図B)。社内共有フォルダのアクセス権が課単位の場合、マーケティング2課に所属する社員しかアクセスできないので、アクセス権は課単位ではありません。



部単位で見ると、Eさんはマーケティング部に所属している。社内共有フォルダも同じ部に所属している。同じ部内のフォルダにアクセスできるアクセス権が適切

図B

図5中にマーケティング部という記述があることから、マーケティング1課や同2課はマーケティング部に属しています。よって、Eさんはマーケティング部に所属しています。社内共有フォルダのアクセス権が部単位の場合、同部に所属している社員がアクセスできるので、下線④のような操作が可能になります。

なお、Eさんは「入社2年目」と説明されており、役職に関する記述がないので、役職は与えられていません。社内共有フォルダのアクセス権を職位単位にした場合は、Eさんはアクセスできません。また、社内共有フォルダのアクセス権を従業員単位にした場合は、Eさんしかアクセスできなくなります。図5のG主任へのヒアリング結果で「G主任を含めた……3名が共同作業できるように」していることから、アクセス権を従業員単位にするのは不適切です。

以上から、**エ**(部単位)が正解です。

(3)

空欄g

【課題の改善】で、B課長は図6に示す項目の検討を必要として、これらの課題の改善を実施しています。その後で、「B課長は、改善すべき課題が図6の1-1から1-5の他にもないかの確認をA部長に提案」して、了承を得ています。その上で、B課長は「改善すべき課題が他にもないか、gを実施」しています。空欄g

で行っていることは、図6の1-1から1-5までとは異なる課題を見つけようとしていることです。この点に着目して、解答群の記述を検証します。

ア 図1で、P社基盤情報システムとして「PC上のOS、オフィスソフト、Webブラウザ、ウイルス対策ソフト」などが挙げられています。情報システムのうち、マーケティング部内の従業員が利用しているものは、PCにインストールされているソフトウェアやウイルス対策ソフトです。その脆弱性検査をすることで、図6の1-1(脆弱性が発見されたソフトZを利用していたこと)の課題の改善につながります。図6中の課題に該当することなので、不適切です。

イ 図6の1-1～1-5では、ソフトウェアの脆弱性、ウイルス対策ソフトの停止、及びマーケティング部のアンケートファイルの取扱いに関してだけ、課題の改善を検討しています。冒頭の記述から、マーケティング部では顧客からのアンケートの情報だけでなく、「製品紹介情報、IR情報、CSR情報など」も管理しています。これらの情報資産の取扱い方法などについては、図6中で触れられていません。このような情報資産が不適切な取扱いをされていると、インシデントによって情報が外部に漏えいするリスクがあります。よって、マーケティング部が管理している、アンケートファイル以外の他の情報資産についても取扱い方法を明確にして、問題がないかを検証することで、図6中の課題とは異なる課題を見つけ出すことができます。

ウ マーケティング部内のフォルダのアクセス権は、図6の1-4に関連することです。図6中の課題に該当することなので、不適切です。

エ 図6の1-2に関連することです。図6中の課題に該当することなので、不適切です。

オ 図6の1-1に関連することです。図6中の課題に該当することなので、不適切です。

以上から、**イ**が適切です。

解答

設問1	(1) イ	e: ア
	(2) a: ア	(2) ウ
	(3) カ	設問3 (1) f: カ
設問2	(1) b: ウ	(2) エ
	c: ア	(3) g: イ
	d: カ	

平成 **28** 年度 春期

情報セキュリティ マネジメント

- 午前 問題 112
(全 50 問 試験時間：1 時間 30 分)
- 午後 問題 144
(全 3 問 試験時間：1 時間 30 分)

※ 327～328 ページに答案用紙がありますので、ご利用ください。

※ 「問題文中で共通に使用される表記ルール」については、325 ページを参照してください。

平成28年度 春期 午前問題



問 1 CSIRTの説明として、適切なものはどれか。

- ☒ **ア** IPアドレスの割当て方針の決定, DNSルートサーバの運用監視, DNS管理に関する調整などを世界規模で行う組織である。
- ☒ **イ** インターネットに関する技術文書を作成し, 標準化のための検討を行う組織である。
- ☒ **ウ** 企業内・組織内や政府機関に設置され, 情報セキュリティインシデントに関する報告を受け取り, 調査し, 対応活動を行う組織の総称である。
- ☒ **エ** 情報技術を利用し, 宗教的又は政治的な目標を達成するという目的をもった人や組織の総称である。



問 2 情報セキュリティ対策のクリアデスクに該当するものはどれか。

- ☒ **ア** PCのデスクトップ上のフォルダなどを整理する。
- ☒ **イ** PCを使用中に離席した場合, 一定時間経過すると, パスワードで画面ロックされたスクリーンセーバに切り替わる設定にしておく。
- ☒ **ウ** 帰宅時, 書類やノートPCを机の上に出したままにせず, 施錠できる机の引出しなどに保管する。
- ☒ **エ** 机の上に置いたノートPCを, セキュリティワイヤで机に固定する。



問 3 情報セキュリティに係るリスクマネジメントが効果的に実施されるよう, リスクアセスメントに基づいた適切なコントロールの整備, 運用状況を検証又は評価し, 保証又は助言を与えるものであり, 実施者に独立かつ専門的な立場が求められるものはどれか。

- | | |
|--|--|
| ☒ ア コントロールセルフアセスメント(CSA) | ☒ イ 情報セキュリティ監査 |
| ☒ ウ 情報セキュリティ対策ベンチマーク | ☒ エ デジタルフォレンジックス |

解説

問 1 CSIRT

CSIRT(Computer Security Incident Response Team)は, ネットワーク上での各種の問題(不正アクセス, マルウェア, 情報漏えいなど)を監視し, その報告を受け取って原因を調査したり, 対策を検討したりする組織です。CSIRTは企業内・組織内または公的機関内に設置されます。

- × ☒ **ア** **ICANN**(Internet Corporation for Assigned Names and Numbers)の説明です。
- × ☒ **イ** **IETF**(Internet Engineering Task Force)の説明です。
- ☒ **ウ** 正解です。



攻略のカギ



RFC

問1

Request For Comments。インターネットに関連する技術仕様を文書化したもので, IETFが公表している。RFC 1149などのように, 番号によって管理されている。

× **エ** ハックティヴィズム (hacktivism) の説明です。

問2 クリアデスク

情報セキュリティ対策の**クリアデスク**とは、外出時に机の上を片付けて何も残さないようにして、情報漏えいを防ぐことです。機密情報が記載された書類やノートPCなどは、施錠できる引出しなどに保管するのが望ましいとされます。机に残された書類を盗み見られたり、ノートPCを不正に操作されたりして機密情報が漏えいすることがあるので、クリアデスクによって机の上に何も残さないようにします。

- × **ア** PCのデスクトップを整理することは、情報セキュリティ対策にはなりません。
- × **イ** クリアスクリーンの説明です。
- **ウ** 正解です。
- × **エ** ノートPCの盗難防止策の説明です。

問3 情報セキュリティに係るリスクマネジメント

本問のような活動のことを**情報セキュリティ監査(制度)**(**イ**)といいます。情報セキュリティ監査とは、「情報セキュリティに係るリスクのマネジメントが効果的に実施されるように、リスクアセスメントに基づく適切なコントロールの整備、運用状況を、情報セキュリティ監査を行う主体が独立かつ専門的な立場から、国際的にも整合性のとれた基準に従って検証又は評価し、もって保証を与えあるいは助言を行う活動」のことです(経済産業省 情報セキュリティ監査制度のWebページより)。

情報セキュリティ監査を適切に実施するには、実施者が被監査部門から独立した立場にあり、かつ情報セキュリティに関する専門知識が必要とされます。

- × **ア** **コントロールセルフアセスメント**(CSA)とは、内部監査の手法の一つです。監査部または外部の監査人が監査を行うのではなく、業務内容に熟知している被監査部門の管理者及び担当者が、自身の活動を評価します。
- **イ** 正解です。
- × **ウ** **情報セキュリティ対策ベンチマーク**とは、独立行政法人 情報処理推進機構セキュリティセンターが公表している、組織の情報セキュリティマネジメントシステムの実施状況を評価するためのツールのことです。
- × **エ** **デジタルフォレンジックス**とは、コンピュータ犯罪(不正アクセスなど)に対する科学的調査のことで、犯罪を立証するために必要な情報を、各種の手段を用いて収集・分析することです。

攻略のカギ



TCP/IP

問1

インターネット上のコンピュータが通信を行うときに使用するプロトコルの総称。TCPはRFC 793、IPはRFC 791で規定された規格。利用者に最も近い層から順に、アプリケーション層、トランスポート層、インターネット層及びネットワークインタフェース層の4層を定義し、各層に複数のプロトコルが属している。



助言型監査

問3

システムに内在する問題点を把握し、その改善策(助言)を監査の依頼者に提示することを目的とする監査。



保証型監査

問3

システムの機密性などの特性を維持するための対策が適切に実行されており、システム監査人が調査した限り、システムに問題がないことを保証するための監査。

解答

問1 **ウ** 問2 **ウ**
問3 **イ**

**問 4**

ノートPCやスマートフォンなどのモバイル機器に重要情報を格納して持ち出すとき、機器の紛失による情報漏えい対策として有効なものはどれか。

- ア モバイル機器でのSNSの使用を制限する。
- イ モバイル機器内の情報をリモートから消去できるツールを導入する。
- ウ モバイル機器に通信を暗号化するツールを導入する。
- エ モバイル機器にのぞき見防止フィルムを貼付する。

**問 5**

JIS Q 27001において、リスクを受容するプロセスに求められるものはどれか。

- ア 受容するリスクについては、リスク所有者が承認すること
- イ 受容するリスクをモニタリングやレビューの対象外とすること
- ウ リスクの受容は、リスク分析前に行うこと
- エ リスクを受容するかどうかは、リスク対応後に決定すること

**問 6**

JIS Q 27001に基づく情報セキュリティ方針の取扱いとして、適切なものはどれか。

- ア 機密情報として厳格な管理を行う。
- イ 従業員及び関連する外部関係者に通知する。
- ウ 情報セキュリティ担当者各人が作成する。
- エ 制定後はレビューできないので、見直しの必要がない内容で作成する。

解説

問 4 モバイル機器の紛失による情報漏えい対策

モバイル機器を外部に持ち出すとき、紛失または盗難によって第三者に入手されると、重要情報が盗み見られる危険性があります。この危険性を低減するには、次のような対策が有効です。

- モバイル機器内の情報を暗号化し、特定のパスワードを入力しないと復号できないようにすることで、第三者が情報を読めないようにする
- モバイル機器内の情報を、リモートで操作できるツールを導入して、機器を紛失したときはすぐに情報を消去することで、第三者が情報を読めないようにする

よって、機器の紛失による情報漏えい対策として有効なものは **イ** です。

- × **ア** モバイル機器でのSNSの使用を制限すると、社員がモバイル機器からSNSを介して重要情報が流出するリスクが低減されます。しかし、紛失時に重要情報を盗み見られます。
- **イ** 正解です。
- × **ウ** モバイル機器と他の機器間の通信を暗号化しても、モバイル機器内の情報が暗号化されていなければ、紛失時に重要情報を盗み見られます。



攻略のカギ



リスク対応の種類 **問 4**

リスクを防止するための方法には次のようなものがある。

- リスク回避
事業から撤退するなどの方法で、リスクそのものを発生させなくすること
- リスク低減（軽減）
リスクの発生確率や損失額を減らすこと
- リスク移転（転嫁）
保険に加入したり、事業を外部に委託したりすることで、リスク発生時の影響、損失、責任の一部または全部を他者に肩代わりさせること
- リスク保有（受容）
軽微なリスクに対してはあえて対策を行わず、リスクが発生した場合の損失は自社で負担す

 攻略のカギ

ること

各リスクに対して上記の対応策をとった後に、残存するリスクの発生確率または被害額のことを残留リスクという。

- × **エ** モバイル機器にのぞき見防止フィルムを貼付すると、社員がモバイル機器を操作しているとき、他人に画面をのぞき見られるリスクは低減されます。しかし、紛失時には重要情報を盗み見られてしまいます。

問5 リスク受容

JIS Q 27001は、情報セキュリティマネジメントシステムの確立、実施、維持及び継続的改善の要求事項を提供している規格です。

情報セキュリティに関するリスクの中には、発生確率が非常に低かったり、被害額が非常に少なかったりするものがあります。このようなリスクの対策をとると費用が高額になることがあります。このようにして、対策をとらないままにするリスクのことを、**残留リスク**といいます。残留リスクを決めることを、リスクを**受容**するプロセスといいます。

JIS Q 27001の6.1.3情報セキュリティリスク対応の項では、情報セキュリティリスク対応計画を策定した後も残留しているリスクに対して、次のように定めています。

「情報セキュリティリスク対応計画及び残留している情報セキュリティリスクの受容について、リスク所有者の承認を得る」

以上から、**ア**が正解です。

- **ア** 正解です。
- × **イ** 情報セキュリティマネジメントシステムを運用するとき、受容するリスクも含めて、全てのリスクをモニタリング（監視）やレビューの対象とします。
- × **ウ** 先にリスク分析を行ってリスクの影響度を特定した後に、リスクを受容するプロセスを実行します。
- × **エ** リスクを受容するかどうかを先に決めてから、リスク対応を行います。

問6 JIS Q 27001

JIS Q 27001の5.2方針の項では、組織のトップマネジメント（経営陣）は、情報セキュリティ方針（情報セキュリティの目的やその設定のための枠組みを含む文書）を確立しなければならないとしています。この項では、情報セキュリティ方針を「組織内に伝達」し、「必要に応じて、利害関係者が入手可能」とするように定めています。よって、従業員や外部関係者などが内容を確認できるようにするのが適切です。

- × **ア** 情報セキュリティ方針は従業員や外部関係者なども入手できるようにします。
- **イ** 正解です。
- × **ウ** 情報セキュリティ方針は、経営陣が作成します。
- × **エ** 前掲の項では、情報セキュリティ方針は「ISMSへの継続的改善へのコミットメント」を含むとしています。コミットメントとは関与のことです。ISMSのプロセスを改善するとき、情報セキュリティ方針の内容も合わせて定期的に見直し、改善する必要があります。

解答

問4	イ	問5	ア
問6	イ		



問 7

IPA “組織における内部不正防止ガイドライン” にも記載されている, 組織の適切な情報セキュリティ対策はどれか。

- ア インターネット上のWebサイトへのアクセスに関しては, コンテンツフィルタ (URLフィルタ) を導入して, SNS, オンラインストレージ, 掲示板などへのアクセスを制限する。
- イ 業務の電子メールを, システム障害に備えて, 私用のメールアドレスに転送するよう設定させる。
- ウ 従業員がファイル共有ソフトを利用する際は, ウイルス対策ソフトの誤検知によってファイル共有ソフトの利用が妨げられないよう, ウイルス対策ソフトの機能を一時的に無効にする。
- エ 組織が使用を許可していないソフトウェアに関しては, 業務効率が向上するものに限定して, 従業員の判断でインストールさせる。



問 8

情報システムに対するアクセスのうち, JIS Q 27002 という特権的アクセス権を利用した行為はどれか。

- ア 許可を受けた営業担当者が, 社外から社内の営業システムにアクセスし, 業務を行う。
- イ 経営者が, 機密性の高い経営情報にアクセスし, 経営の意思決定に生かす。
- ウ システム管理者が業務システムのプログラムのバージョンアップを行う。
- エ 来訪者が, デモシステムにアクセスし, システム機能の確認を行う。



問 9

“不正のトライアングル” 理論において, 全てそろったときに不正が発生すると考えられている3要素はどれか。

- | | |
|---------------|--------------------|
| ア 機会, 動機, 正当化 | イ 機密性, 完全性, 可用性 |
| ウ 顧客, 競合, 自社 | エ 認証, 認可, アカウンティング |



問 10

利用者アクセスログの取扱いのうち, IPA “組織における内部不正防止ガイドライン” にも記載されており, 内部不正の早期発見及び事後対策の観点で適切なものはどれか。

- | | |
|-----------------------|---------------------|
| ア コストにかかわらずログを永久保存する。 | イ 利用者にログの管理権限を付与する。 |
| ウ 利用者にログの保存期間を周知する。 | エ ログを定期的に確認する。 |

解説

問 7 内部不正防止ガイドライン

“組織における内部不正防止ガイドライン” の「4-4 技術・運用管理」の項では, 次のような対策を提示しています。

「2. Webアクセスに関しては, コンテンツフィルタを導入して, SNS 及びアップローダー, 掲示板等へのアクセスを制限することが望まれます。(以下略)」

よって, **ア** の対策が適切です。



攻略のカギ



組織における内部不正防止ガイドライン 問 7

独立行政法人 情報処理推進機構 (IPA) が公表しているガイドラインで, 組織における内部不正を防止するために実施する事項などをまとめたもの。このガイドラインでは, 次の五つを基本原則としている。

- **ア** 正解です。
- × **イ** 同ガイドラインでは、「電子メールに関しては、業務のメールを個人のメールアドレスに転送する設定になっていないかを確認することが望まれます」としています。
- × **ウ** 同ガイドラインでは、ファイル共有ソフト等を社内のPCにインストールして利用することを禁止しています。
- × **エ** 同ガイドラインでは、利用者から新たに利用申請があったソフトウェアは、利用させてもよいか判断することが必要としています。

問8 特権的アクセス権

特権的アクセス権とは、コンピュータの設定を変更したり、アプリケーションプログラムをインストールしたりするなど、OSの全ての機能を利用できるアクセス権のことです。UNIXのroot権限などが特権的アクセス権に該当します。システム管理者が、業務システムのプログラムのバージョンアップを行うこと(**ウ**)は、特権的アクセス権を利用した行為に該当します。

ア、**イ**、**エ**はいずれもプログラムのインストール、更新、またはコンピュータの設定変更を行っていません。これらはシステムの機能や情報にアクセスしているだけなので、一般ユーザのアクセス権を使用した行為です。

問9 不正のトライアングル

- **ア** 正解です。
- × **イ** 機密性 (Confidentiality)、完全性 (Integrity)、可用性 (Availability) は**情報セキュリティの3要素**です。**CIA**ともいいます。
- × **ウ** 顧客 (Customer)、競合 (Competitor)、自社 (Company) は、**3C分析**で分析に用いる3要素です。
- × **エ** 認証 (Authentication)、認可 (Authorization)、アカウントニング (Accounting、課金) は、**情報システムの利用者識別と制御に関する3要素**で、**AAA**ともいいます。

問10 内部不正の早期発見

“組織における内部不正防止ガイドライン”の「4-5 証拠確保」の項では、情報システムにおけるログについて、次のようにすることが望ましいとしています。

「3. ログは定期的に確認します。多量なファイルへのアクセスや業務範囲外のファイルへのアクセス等の通常の業務と異なる事象が発見された者に対して、事象確認又は監視強化等の対策を行うことが望まれます。(以下略)」

以上から、**エ**(ログを定期的に確認する)が適切です。

- × **ア** ログを永久に保存しようとする、保存用の媒体を大量に購入するなど、コスト面での問題が発生します。
- × **イ** 利用者にログの管理権限を付与すると、利用者が不正アクセスを行った後にログを改ざんまたは削除することで、内部不正を隠ぺいできます。
- × **ウ** 保存期間を利用者に知らせると、その期間が過ぎるまで犯行が露呈しないように工作すればよいと考え、かえって内部犯行を誘発する可能性があります。
- **エ** 正解です。

攻略のカギ

- 犯行を難しくする(やりにくくする)
- 捕まるリスクを高める(やると見つかる)
- 犯行の見返りを減らす(割に合わない)
- 犯行の誘因を減らす(その気にさせない)
- 犯罪の弁明をさせない(言い訳させない)

特権的アクセスの例 問8

UNIXのroot権限や、Windowsの管理者 (Administrator) 権限のアカウントが特権的アクセス権の例。

不正のトライアングル 問9

犯罪学者のD.R. クレッシー氏が提唱した理論で、人が不正行為をする原因をまとめたもの。次の三つがそろったとき、不正行為が発生する。

①機会 (の認識)

「作業の実行者と承認者が同じ」、「承認者が作業内容を確認せずに承認している」など、不正行為を実行できるような客観的環境があること。

②動機

不正行為を実行しようとする主観的事情。例えば多額の借金があり、返済に追われていることなどが該当する。

③正当化

不正行為を正当化しようとする主観的事情。「他の人もやっている」、「自分は貧しいから他人から奪っても構わない」などの、都合のいい理由付けが該当する。

解答

問7 **ア** 問8 **ウ**
問9 **ア** 問10 **エ**



問 11 BYODの説明、及びその情報セキュリティリスクに関する記述のうち、適切なものはどれか。

- ア 従業員が企業から貸与された情報端末を、客先などへの移動中に業務に利用することであり、ショルダハッキングなどの情報セキュリティリスクが増大する。
- イ 従業員が企業から貸与された情報端末を、自宅に持ち帰って私的に利用することであり、機密情報の漏えいなどの情報セキュリティリスクが増大する。
- ウ 従業員が私的に保有する情報端末を、職場での休憩時間などに私的に利用することであり、セキュリティ意識の低下などに起因する情報セキュリティリスクが増大する。
- エ 従業員が私的に保有する情報端末を業務に利用することであり、セキュリティ設定の不備に起因するウイルス感染などの情報セキュリティリスクが増大する。



問 12 IDSの機能はどれか。

- ア PCにインストールされているソフトウェア製品が最新のバージョンであるかどうかを確認する。
- イ 検査対象の製品にテストデータを送り、製品の応答や挙動から脆弱性を検出する。
- ウ サーバやネットワークを監視し、セキュリティポリシーを侵害するような挙動を検知した場合に管理者へ通知する。
- エ 情報システムの運用管理状況などの情報セキュリティ対策状況と企業情報を入力し、組織の情報セキュリティへの取組状況を自己診断する。



問 13 クライアントとWebサーバの間において、クライアントがWebサーバに送信されたデータを検査して、SQLインジェクションなどの攻撃を遮断するためのものはどれか。

- | | |
|--------------|---------------|
| ア SSL-VPN 機能 | イ WAF |
| ウ クラスタ構成 | エ ロードバランシング機能 |

解説

問 11 BYOD

BYOD (Bring Your Own Device) とは、従業員が私的に保有する携帯電話やタブレットなどの情報端末を、社内や出先で業務に利用することです。社内で利用するPCや情報端末と比較して、私的に保有する情報端末はセキュリティの設定などを厳密に管理できないので、設定の不備に起因するウイルス感染や不正アクセスのリスクが増大します。

- × **ア、イ** 企業から貸与された情報端末を業務または私的に利用することで、セキュリティリスクは増大しますが、BYODには該当しません。
- × **ウ** 私的に保有する情報端末を私的に利用することは、BYODには該当しません。
- **エ** 正解です。



攻略の力ギ



ショルダハッキング 問 11

ノートPCやスマートフォンなどを操作している人の肩越しに画面をのぞきこむことで、情報を盗み見る攻撃。

問12 IDS

IDS (Intrusion Detection System : 侵入検知システム) は、外部 (インターネットなど) からの攻撃を検知するためのシステムです。

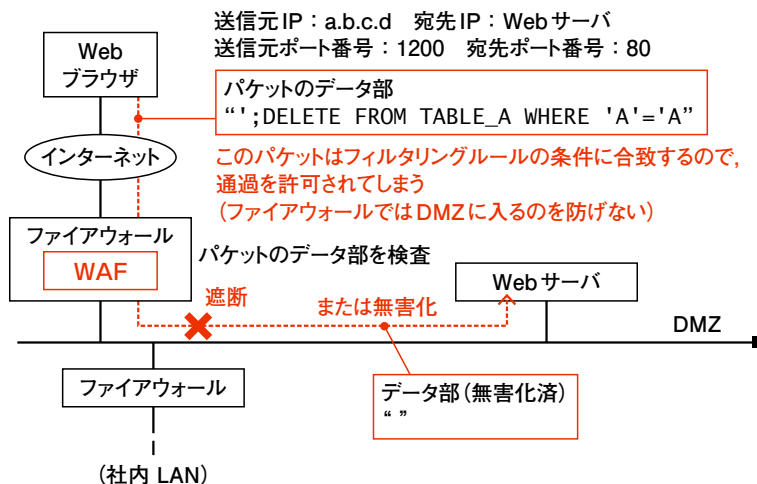
- × **ア** ソフトウェア製品のバージョン管理用ツールの説明です。
- × **イ** 脆弱性検出用ツールの説明です。
- **ウ** 正解です。
- × **エ** 情報セキュリティ対策ベンチマークの説明です。

問13 SQLインジェクションの遮断

ファイアウォールは、パケットのIPアドレスとポート番号を参照し、自身に設定されたフィルタリングルールと比較して、そのパケットの通過が許可されているかどうかを判断するための装置です。

ただし、SQLインジェクションなどの攻撃では、パケットのデータ部に攻撃用データが仕掛けられているので、フィルタリングルールで拒否することはできません。このような攻撃を防止するために、**WAF** (Web Application Firewall, **イ**) が用いられます。

WAFとは、Webサーバとブラウザの間でやり取りされるデータの内容を監視し、Webアプリケーションプログラムの脆弱性を突く攻撃を防御するために用いられるファイアウォールのことです。



- × **ア** **SSL-VPN**機能とは、セキュリティプロトコルSSL/TLSを利用して暗号化や認証を実施し、インターネット上でセキュリティが確保された通信を実現することです。
- **イ** 正解です。
- × **ウ** **クラスタ**構成とは、複数のサーバから構成されるシステムで、いずれかのサーバが故障しても他のサーバが処理を代行することで、可用性を向上させています。
- × **エ** **ロードバランシング**機能とは、複数のサーバに処理を振り分けて負荷を分散することです。

攻略のカギ

IDSの種類 問12

IDSには「NIDS (ネットワーク型IDS)」と「HIDS (ホスト型IDS)」の2つがある。

NIDS : ネットワーク中のファイアウォールなどの重要な機器内に配置する。ネットワーク上を流れているパケットの内容を解析し、攻撃に使用されるタイプのパケットや、挙動の疑わしいパケットを判別し警告を発する。

HIDS : ネットワーク上の個々のコンピュータやサーバに組み込む。自機器に到達したパケットの内容を解析し、攻撃に使用されるタイプのパケットを解析し警告する。

IPヘッダ 問13

パケットの一部で、送信元・宛先のIPアドレスといったパケットの送受信に関する情報が記載されている。

無害化 問13

パケットに含まれる攻撃用スクリプトコードなどの部分を削除して安全にすること。

クラスタ構成 問13

複数のサーバをまとめて一つのサーバのように扱う。1台のサーバに障害が発生しても、残りのサーバが処理を引き継ぐので、可用性が向上する。

ロードバランシング機能 問13

ロードバランサ (負荷分散装置) が、複数のサーバに処理を振り分ける機能。

解答

問11 **エ** 問12 **ウ**
問13 **イ**

平成
28
年度

春

午前



問 14 PCで行うマルウェア対策のうち、適切なものはどれか。

- ア PCにおけるウイルスの定期的な手動検査では、ウイルス対策ソフトの定義ファイルを最新化した日時以降に作成したファイルだけを対象にしてスキャンする。
- イ PCの脆弱性を突いたウイルス感染が起きないように、OS及びアプリケーションの修正パッチを適切に適用する。
- ウ 電子メールに添付されたウイルスに感染しないように、使用しないTCPポート宛ての通信を禁止する。
- エ ワームが侵入しないように、PCに動的グローバルIPアドレスを付与する。



問 15 システム管理者による内部不正を防止する対策として、適切なものはどれか。

- ア システム管理者が複数の場合にも、一つの管理者IDでログインして作業を行わせる。
- イ システム管理者には、特権が付与された管理者IDでログインして、特権を必要としない作業を含む全ての作業を行わせる。
- ウ システム管理者の作業を本人以外の者に監視させる。
- エ システム管理者の操作ログには、本人にだけアクセス権を与える。



問 16 デジタルフォレンジックスでハッシュ値を利用する目的として、適切なものはどれか。

- ア 一方向性関数によってパスワードを復元できないように変換して保存する。
- イ 改変されたデータを、証拠となり得るように復元する。
- ウ 証拠となり得るデータについて、原本と複製の同一性を証明する。
- エ パスワードの盗聴の有無を検証する。

解説

問 14 PCのマルウェア対策

マルウェアは、コンピュータウイルスやスパイウェアなど、PCに感染して不正行為を働くソフトウェアの総称です。マルウェアはOSやアプリケーションの脆弱性を突くことでPCに侵入し、感染を広げようとします。OSやアプリケーションソフトに最新の修正パッチ（追加プログラム）を適用していないと、脆弱性が残ったままになるのでマルウェアに感染しやすくなります。OSやアプリケーションソフトの修正パッチを適切に適用すること（イ）が有効な対策です。

- × ア ウイルス対策ソフトの定義ファイルを最新化する前に、既存のファイルがマルウェアに感染することもあるので、全てのファイルをスキャンの対象にします。
- イ 正解です。
- × ウ 使用しないTCPポート宛ての通信を禁止しても、電子メールに添付されたファイルは受信できます。



攻略のカギ



ポート番号

問 14

パケットのTCPヘッダに含まれる番号で、サーバやPC上で稼働するサービス（プログラム）を識別するためのもの。0～65,535の値をとる。

- × **エ** PCに動的グローバルIPアドレスを付与しても、ワームの侵入を防げません。

問15 システム管理者による内部不正

システム管理者は特権的アクセス権をもっているの、サーバなどに対する全ての操作が可能です。そこで、システム管理者の作業を別の人に監視させる(ウ)ことで内部不正を防止するのが適切です。

- × **ア** システム管理者が複数の場合、それぞれに異なる管理者IDでログインさせて、作業の実行者を特定できるようにします。
- × **イ** 特権を必要としない作業は、特権が付与された管理者IDではなく、一般権限だけが付与された一般ユーザのIDでログインして行わせます。
- **ウ** 正解です。
- × **エ** 本人にだけアクセス権を与えると改ざんなどの危険性が高くなるので、複数の人間にアクセス権を与えて監視させるのが適切です。

問16 デジタルフォレンジックスとハッシュ値

デジタルフォレンジックスとは、コンピュータ犯罪(不正アクセスなど)に対する科学的調査のことで、犯罪を立証するために必要な情報を、各種の手段を用いて収集・分析することです。

ハッシュ値は、データをハッシュ関数に与えることで出力される固定長のビット列です。次の特徴をもちます。

- 出力されたハッシュ値から入力データの内容を推定(復元)することは困難
- 入力データがわずかでも異なれば、ハッシュ値は著しく異なるものになる
- 入力データの長さが異なっても、ハッシュ値は同じ長さになる



デジタルフォレンジックスでは、原本のハッシュ値を求めて、複製とともに保存します。その後に原本または複製がわずかでも改ざんされると、ハッシュ値が異なるので、改ざんを検知できます。また、あるデータから出力したハッシュ値と、別のデータから出力したハッシュ値が一致していれば、両者の内容の一致が証明されます(同一性の証明, フ)。証拠として保存した複製と原本の同一性を証明するときに、ハッシュ値を利用します。

- × **ア** ハッシュ関数のような方向性関数でパスワードを変換して保存するのは、変換したパスワードを保存したファイルを盗み読まれても、パスワードの内容を知られないようにするためです。
- × **イ** デジタルフォレンジックスでは、改変される前のデータを証拠として使用します。
- **ウ** 正解です。
- × **エ** パスワードの盗聴の有無を検証するには、パスワードを保存したファイルのアクセスログを確認します。

攻略のカギ



ワーム

問14

不正侵入や感染などの行為を単独で実行できるマルウェアのことです。OSやアプリケーションソフトの脆弱性を突いてコンピュータに侵入します。そのコンピュータ上で不正な行為を実行したり、同じネットワーク内の他のコンピュータに自身のコピーを送りつけて、さらに感染範囲を広げたりします。



操作ログ

問15

システムに対する操作、実行者の利用者ID、処理対象データ、操作時刻、結果(操作の成功又は失敗)などを記録したログファイル。不正アクセスの実行者を特定するなどの目的で使用する。



ハッシュ関数

問16

- **SHA-1**
 $2^{64}-1$ 以内の任意の長さをもつデータから、160ビット固定長のハッシュ値を生成するハッシュ関数。安全性に問題があると指摘されており、現在はSHA-2などの後続のハッシュ関数を用いることが推奨されている。
- **SHA-2**
 SHA-1の後継のハッシュ関数。SHA-224(ハッシュ値=224ビット固定長)、SHA-256(ハッシュ値=256ビット固定長)などの種類がある。
- **MD5**
 $2^{64}-1$ 以内の任意の長さをもつデータから、128ビット長のハッシュ値を生成する。



一方向性関数

問16

入力に対して出力を求めることは簡単にできるが、逆に出力から入力を求めることは非常に困難である関数のこと。

解答

問14 **イ** 問15 **ウ**
 問16 **ウ**

問 17 機密ファイルが格納されていて、正常に動作するPCの磁気ディスクを産業廃棄物処理業者に引き渡して廃棄する場合の情報漏えい対策のうち、適切なものはどれか。

- ア 異なる圧縮方式で、機密ファイルを複数回圧縮する。
- イ 専用の消去ツールで、磁気ディスクのマスタブートレコードを複数回消去する。
- ウ ランダムなビット列で、磁気ディスクの全領域を複数回上書きする。
- エ ランダムな文字列で、機密ファイルのファイル名を複数回変更する。

問 18 2要素認証に該当する組はどれか。

- ア ICカード認証, 指紋認証
- イ ICカード認証, ワンタイムパスワードを生成するハードウェアトークン
- ウ 虹彩認証, 静脈認証
- エ パスワード認証, パスワードリマインダ

問 19 APTの説明はどれか。

- ア 攻撃者はDoS攻撃及びDDoS攻撃を繰り返し組み合わせ、長期間にわたり特定組織の業務を妨害する。
- イ 攻撃者は興味本位で場当たりの、公開されている攻撃ツールや脆弱性検査ツール^{ぜい}を悪用した攻撃を繰り返す。
- ウ 攻撃者は特定の目的をもち、標的となる組織の防御策に応じて複数の手法を組み合わせ、気付かれないよう執拗^{よう}に攻撃を繰り返す。
- エ 攻撃者は不特定多数への感染を目的として、複数の攻撃を組み合わせたマルウェアを継続的にばらまく。

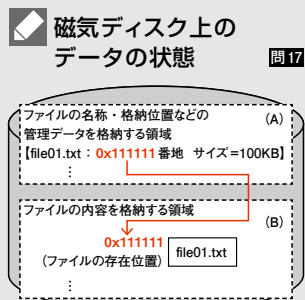
解説

問 17 磁気ディスクの廃棄

機密ファイルが格納されていて正常に動作するPCの磁気ディスクを、そのまま産業廃棄物処理業者に引き渡すと、その業者が磁気ディスクの内容を読み取って機密情報を知られる危険性があります。

廃棄する磁気ディスクの内容を読み取れないようにするためには、磁気ディスク全体に意味のない文字列を書き込み、元の内容を完全に消去する必要があります。ファイルを削除するだけでは、ファイルの名称や格納位置を示すデータが削除されるだけで、ファイルの内容は磁気ディスク上に残ります。なお、意味のない文字列を1回書き込んだだけでは、磁気ディスク上の元の内容の内容を示す磁気を完全に消去できないので、データ修復ツールを用いて復元されることがあります。書き込みを複数回行うことで、内容を完全に消去します(ウ)。

攻略のカギ



OSのファイル削除コマンドを使用しても、(A)の領域のデータが削除されるだけで、ファイルの内容そのもの(B)は磁気ディスク上に残る。

- × **ア** この方法では、複数回展開するだけで機密ファイルを読み取られてしまいます。
- × **イ** マスタブートレコードは、PCの電源を入れてOSが起動されるときに、読み取られる領域です。マスタブートレコードを複数回消去しても、機密ファイルは磁気ディスク上に残るので、廃棄したディスクを入手した業者などが内容を読み取れます。
- **ウ** 正解です。
- × **エ** ファイル名だけを変更しても機密ファイルの内容は残ります。

問18 2要素認証

2要素認証とは、異なる方式の認証手段を複数個組み合わせることです。**所持品による認証**（ICカード認証など）と、**知識による認証**（パスワード認証など）を組み合わせ、両方の認証に成功したときだけ入室を許可することが2要素認証の例です。

2要素認証に該当するのは**ア**です。所持品による認証（ICカード認証）と、**生体認証**（指紋認証）を組み合わせています。

- **ア** 正解です。
- × **イ** ICカード認証は所持品による認証です。ワンタイムパスワードを生成するハードウェアトークンは、そのトークンを持っている者だけが認証に成功するので、所持品による認証です。この組は同じ認証手段だけを含むので、2要素認証ではありません。
- × **ウ** この組は生体認証なので、2要素認証ではありません。
- × **エ** この組は知識による認証なので、2要素認証ではありません。

問19 APT

IPAが2010年に公表した「IPAテクニカルウォッチ：『新しいタイプの攻撃』に関するレポート」において、「この新しいサイバー攻撃は2010年の春頃から海外では**APT**（Advanced Persistent Threats）と呼ばれている」として、「脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定企業や個人をねらい、対応が難しく執拗な攻撃」を紹介しています。攻撃者が特定の組織を標的として、複数の手法を組み合わせ、執拗に攻撃を繰り返す手法がAPTです（**ウ**）。

- × **ア** 同じ種類の攻撃（DoS攻撃と類似したDDoS攻撃）だけを使っているので誤りです。
- × **イ** **スクリプトキディ**の説明です。
- **ウ** 正解です。
- × **エ** マルウェアを不特定多数に感染させるための攻撃の説明です。

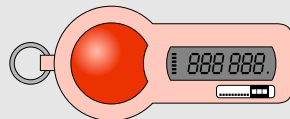
攻略のカギ

ブート 問17

PCのOSを起動すること。PCの電源を入れると、最初にIPL（Initial Program Loader）というプログラムがマザーボード上のROMからメモリに読み込まれ、マスタブートレコードに格納されたプログラム（ブートローダ）を実行する。ブートローダは、磁気ディスクに格納されたOSのプログラムを読み込み、起動する。

ハードウェアトークン 問18

一定時間が経過するとに値が変化する、ワンタイムパスワードの文字列が表示された小型の装置。ワンタイムパスワードの値はサーバと同期しており、この値を入力しないとログインが成功しないので、ハードウェアトークンをもっている者だけがログインできる。主に、インターネットバンキングサイトにログインするときに用いられる。



パスワードリマインダ 問18

利用者がパスワードを忘れた場合に、あらかじめ登録していた質問に正しく答えることで、利用者を認証して新しいパスワードを設定できるようにする機能。「お母さんの旧姓は」などの質問を選び、答えを事前に登録しておく。

ソーシャルエンジニアリング 問18

不正な利用者が、本人になりすまして「パスワードを忘れてしまったので教えてください」という主旨の電話をセキュリティ管理者にかけなどの方法で、パスワードなどのセキュリティに関する情報を不正に聞き出す行為のこと。

解答

問17 **ウ** 問18 **ア**
問19 **ウ**

問 20 利用者PCのHDDが暗号化されていないとき、攻撃者が利用者PCからHDDを抜き取り、攻撃者が用意したPCに接続してHDD内の情報を盗む攻撃によって発生する情報漏えいのリスクの低減策のうち、適切なものはどれか。

- ア HDDにインストールしたOSの利用者アカウントに対して、ログインパスワードを設定する。
- イ HDDに保存したファイルの読取り権限を、ファイルの所有者だけに付与する。
- ウ 利用者PC上でHDDパスワードを設定する。
- エ 利用者PCにBIOSパスワードを設定する。

問 21 クロスサイトスクリプティングに該当するものはどれか。

- ア Webアプリケーションのデータ操作言語の呼出し方に不備がある場合に、攻撃者が悪意をもって構成した文字列を入力することによって、データベースのデータの不正な取得、改ざん及び削除を可能とする。
- イ Webサイトに対して、他のサイトを介して大量のパケットを送り付け、そのネットワークトラフィックを異常に高めてサービスを提供不能にする。
- ウ 確保されているメモリ空間の下限又は上限を超えてデータの書込みと読出しを行うことによって、プログラムを異常終了させたりデータエリアに挿入された不正なコードを実行させたりする。
- エ 攻撃者が罠を仕掛けたWebページを利用者が閲覧し、当該ページ内のリンクをクリックしたときに、不正スクリプトを含む文字列が脆弱なWebサーバに送られ、レスポンスに埋め込まれた不正スクリプトの実行によって、情報漏えいをもたらす。

解説

問 20 HDDの抜き取りによる情報漏えい

利用者PCから抜き取ったHDDを、攻撃者が用意したPCに接続して情報を盗む攻撃に対しては、そのHDD内の情報にアクセスできないようにします。HDDへのアクセスを防ぐには、一般に次のような方法が有効です。

- ① BIOSパスワードを設定し、PCを起動できないようにする
- ② OSのログインパスワードを設定し、OSを使用できないようにする
- ③ ハードディスクを暗号化したり、パスワードを設定したりしてデータを読み取れないようにする

これらのうち、①と②によって利用者PCを起動させないようにすることができます。しかし、利用者PCから抜き取ったHDDを、攻撃者が用意したPCに接続して、攻撃者のPC上でOSを起動する場合、OSのログインパスワードやBIOSパスワードは使用されないで、情報を盗まれます。この場合は、③の方法が有効です。なお、利用者のHDDの暗号化はされていないことから、HDDにパスワードを設定することが有効になります。

ANSIが策定したATA規格に従ったHDDでは、HDDそのものにパスワードを設定して、パスワードを入力しない限りHDD内の情報を読み取れないようにすることが可能です。このパスワードをHDDパスワードといいます。攻撃者が上記の攻撃を実行しても、利用者PCのHDDパスワードを知らなければ情報を

攻略のカギ



BIOS

問 20

Basic Input/Output System。PCの電源を入れたときにROMから読み込まれて起動するソフトウェアで、ブートローダを読み込んでOSを起動させたり、ハードウェアの設定をしたりする機能をもつ。BIOSパスワードを設定すると、正しいパスワードを入力しない限りOSが起動しなくなる。



ANSI

問 20

American National Standards Institute (米国国家規格協会)。アメリカ合衆国における工業分野の標準化組織。ATAやTIA/EIA-568-B (LANケーブル結線の規格)などを公表している。

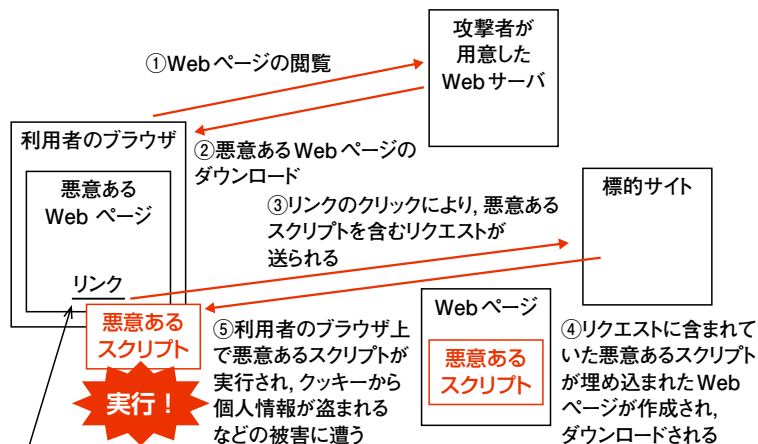
読み取れないので、リスクを低減できます。

- × **ア** HDDにインストールしたOSの利用者アカウントに対して、ログインパスワードを設定すると、それを知らない限りファイルを盗むことはできません。しかし、攻撃者が用意した別のPCに、そのHDDを外付けで接続すれば、OSを起動しなくてもHDD内のファイルにアクセスできるので情報が盗まれます。
- × **イ** 攻撃者が用意したPCのOSを起動し、管理者権限でログインすることで、ファイルの読取り権限をファイルの所有者以外にも付与できます。攻撃者のアカウントにファイルの読取り権限を付与すれば、情報が盗まれます。
- **ウ** 正解です。
- × **エ** 利用者PCにBIOSパスワードを設定すると、利用者以外は利用者PCのOSを起動できなくなります。しかし、攻撃者が用意した別のPCにHDDを接続すれば、OSを起動しなくてもHDD内のファイルにアクセスできるので、情報が盗まれます。

問21 クロスサイトスクリプティング

クロスサイトスクリプティングは次のような攻撃です。

- ① 攻撃者が用意したWebサーバ上のページを利用者が閲覧し、その中のリンクをクリックする
- ② 悪意あるWebページのダウンロード
- ③ リンクのクリックにより、悪意あるスクリプトを含むリクエストが送られる
- ④ リクエストに含まれていた悪意あるスクリプトが埋め込まれたWebページが作成され、ダウンロードされる
- ⑤ 利用者のブラウザ上で悪意あるスクリプトが実行され、クッキーから個人情報が盗まれるなどの被害に遭う



`http://(標的サイトのサーバ名)/***.htm?***=<script>(悪意あるスクリプトの文字列)</script>`のような内容のリンク

- × **ア** SQLインジェクションの説明です。
- × **イ** DoS攻撃の説明です。
- × **ウ** バッファオーバーフローの説明です。
- **エ** 正解です。

攻略のカギ



ATA

問20

Advanced Technology Attachment. 1989年にANSIが制定した、コンピュータにハードディスクを接続するための規格。



スクリプト

問21

文字で記述されたプログラム。HTMLなどに埋め込まれている。ブラウザがスクリプトを読み込むと、その内容が動的に解釈されて処理が実行される。

解答

問20 **ウ**

問21 **エ**



問22 クリックジャッキング攻撃に該当するものはどれか。

- ア Webアプリケーションの脆弱性を悪用し、Webサーバに不正なリクエストを送ってWebサーバからのレスポンスを二つに分割させることによって、利用者のWebブラウザのキャッシュを偽造する。
- イ WebサイトAのコンテンツ上に透明化した標的サイトBのコンテンツを配置し、WebサイトA上の操作に見せかけて標的サイトB上で操作させる。
- ウ Webブラウザのタブ表示機能を利用し、Webブラウザの非活性なタブの中身を、利用者が気づかぬうちに偽ログインページに書き換えて、それを操作させる。
- エ 利用者のWebブラウザの設定を変更することによって、利用者のWebページの閲覧履歴やパスワードなどの機密情報を盗み出す。



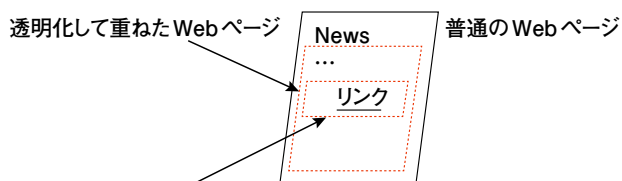
問23 送信者Aが文書ファイルと、その文書ファイルのデジタル署名を受信者Bに送信したとき、受信者Bができることはどれか。ここで、受信者Bは送信者Aの署名検証鍵Xを保有しており、受信者Bと第三者は送信者Aの署名生成鍵Yを知らないものとする。

- ア デジタル署名、文書ファイル及び署名検証鍵Xを比較することによって、文書ファイルに改ざんがあった場合、その部分を判別できる。
- イ 文書ファイルがウイルスに感染していないことを認証局に問い合わせて確認できる。
- ウ 文書ファイルが改ざんされていないこと、及びデジタル署名が署名生成鍵Yによって生成されたことを確認できる。
- エ 文書ファイルとデジタル署名のどちらかが改ざんされた場合、どちらが改ざんされたかを判別できる。

解説

問22 クリックジャッキング攻撃

クリックジャッキングは、Webページの上に透明なコンテンツを重ねてクリックを乗っ取る攻撃です。HTMLのiframeタグなどを用いることで、Webページの中に別のWebページをレイヤ(層)として表示することができます。さらに、当該レイヤを透明にすることで、一見問題がないように見えるWebページの前面に、別のWebページを透明化して密かに重ねることが可能です。このようなWebページ上で操作を行うと、利用者が気づかぬうちに、別のWebサイトで不正な操作が行われてしまいます(イ)。



透明化されたリンク(普通のWebページのリンクの上に設置されており、クリックすると、透明化したWebページ上で操作が実行される)



攻略のカギ



iframeタグ

問22

HTML文書のタグの一つで、あるWebページの中に別のWebページを埋め込んで表示するために用いられる。

- × **ア** HTTP Response Splitting Attackという攻撃手法の説明です。
- **イ** 正解です。
- × **ウ** Tabnabbing 攻撃の説明です。
- × **エ** 利用者のWebページの閲覧履歴やパスワードは、クロスサイトスクリプティングで盗むことが可能です。

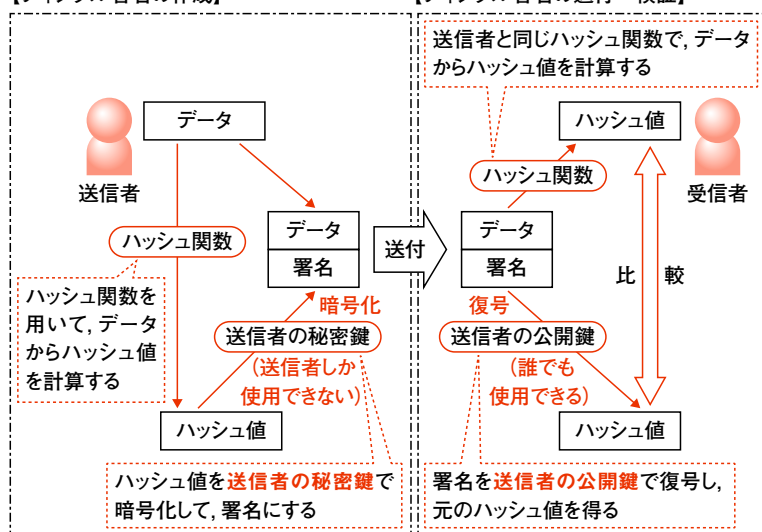
問23 デジタル署名

デジタル署名では、ファイルの送信者Aは自分の**署名生成鍵（秘密鍵）**を用いて、ファイルのハッシュ値を暗号化して、デジタル署名を生成します。送信者Aから送信されたファイルとデジタル署名を受信した受信者Bは、ファイルのハッシュ値を求めるとともに、送信者Aの**署名検証鍵（公開鍵）**でデジタル署名を復号して、送信者Aが生成していたハッシュ値を得ます。

上記の二つのハッシュ値が一致していれば、ファイルとデジタル署名の両方が改ざんされていないことと、署名生成鍵Yを利用してデジタル署名が生成されたことを確認できます。署名生成鍵Yで暗号化したファイルは、署名検証鍵Xでしか復号できないためです。

【デジタル署名の作成】

【デジタル署名の送付・検証】



- × **ア** デジタル署名では、改ざんがあったことは確認できますが、文書ファイルのどの部分が改ざんされたかは判別できません。
- × **イ** デジタル署名では、ウイルス感染の有無を認証局に問い合わせることはできません。
- **ウ** 正解です。
- × **エ** 文書ファイルとデジタル署名のどちらかが改ざんされたかは判別できません。

攻略のカギ

非活性なタブ 問22

複数のWebページをタブとして同時に開くことができるブラウザにおいて、現在閲覧していないタブのこと。

デジタル署名 問23

公開鍵暗号方式とハッシュ関数を利用して、データの改ざんを検知したり、本人性を証明したりするための技術。

認証局 問23

公開鍵及び秘密鍵の利用を申請してきた者（利用者）に対して、公開鍵証明書を交付したり、公開鍵の本人性を保証したりする組織。ペリサイン社などが認証局として公開鍵証明書の交付を行っている。

解答

問22 **イ** 問23 **ウ**



問24 公開鍵暗号を利用した電子商取引において、認証局（CA）の役割はどれか。

- ア 取引当事者間で共有する秘密鍵を管理する。
- イ 取引当事者の公開鍵に対するデジタル証明書を発行する。
- ウ 取引当事者のデジタル署名を管理する。
- エ 取引当事者のパスワードを管理する。



問25 ドライブバイダウンロード攻撃の説明はどれか。

- ア PCにUSBメモリが接続されたとき、USBメモリに保存されているプログラムを自動的に実行する機能を用いてウイルスを実行し、PCをウイルスに感染させる。
- イ PCに格納されているファイルを勝手に暗号化して、戻すためのパスワードを教えることと引換えに金銭を要求する。
- ウ Webサイトを閲覧したとき、利用者が気付かないうちに、利用者の意図にかかわらず、利用者のPCに不正プログラムが転送される。
- エ 不正にアクセスする目的で、建物の外部に漏れた無線LANの電波を傍受して、セキュリティの設定が脆弱な無線LANのアクセスポイントを見つけ出す。



問26 パスワードリスト攻撃の手口に該当するものはどれか。

- ア 辞書にある単語をパスワードに設定している利用者がいる状況に着目して、攻撃対象とする利用者IDを定め、英語の辞書にある単語をパスワードとして、ログインを試行する。
- イ 数字4桁のパスワードだけしか設定できないWebサイトに対して、パスワードを定め、文字を組み合わせた利用者IDを総当たりで、ログインを試行する。
- ウ パスワードの総文字数の上限が小さいWebサイトに対して、攻撃対象とする利用者IDを一つ定め、文字を組み合わせたパスワードを総当たりで、ログインを試行する。
- エ 複数サイトで同一の利用者IDとパスワードを使っている利用者がいる状況に着目して、不正に取得した他サイトの利用者IDとパスワードの一覧表を用いて、ログインを試行する。

解説

問24 認証局

利用者は、信頼できる第三者機関である認証局に対してデジタル証明書の申請を行います。認証局は、その利用者の正当性を戸籍謄本や会社の登記などによって確認し、正当な個人・団体であれば、デジタル証明書を発行します。デジタル証明書には「利用者の公開鍵」の他に、「認証局の秘密鍵」によって暗号化された「認証局の署名」が含まれています。

ある利用者のデジタル証明書を受け取った者は、デジタル証明書内の「認証局の署名」を「認証局の公開鍵」にて復号します。この手続きが成立すれば、そのデジタル証明書の署名は認証局しか使用できない「認証局の秘密鍵」によって暗号化されていたことが証明されます。すなわち、認証局によって、



攻略の力ギ



PKI（公開鍵基盤） 問24

公開鍵暗号方式及びデジタル署名の仕組みを応用した、公開鍵の正当性を証明して公開鍵とその利用者を結び付けるための仕組みのこと。

ある利用者がネットワーク上に公開している公開鍵が、本当にその利用者が作成して公開しているものか（本人性があるか）を証明するために、デジタル証明書（公開鍵証明書や電子証明書ともいう）が用いられる。

デジタル証明書及びそれに含まれる公開鍵の正当性が保証されることになります。

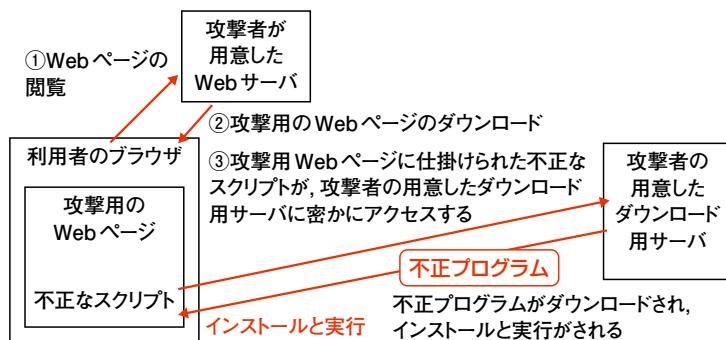
以上から、認証局の役割は、取引当事者（公開鍵の利用者）の公開鍵に対するデジタル証明書を発行すること（イ）です。

- × ア 秘密鍵は取引当事者が厳重に管理します。
- イ 正解です。
- × ウ デジタル署名は取引当事者自身で作成します。
- × エ パスワードは取引当事者自身が作成し管理します。

問25 ドライブバイダウンロード攻撃

ドライブバイダウンロード攻撃とは、次のような攻撃です。

攻撃用のWebページに不正なスクリプトを仕掛けて、利用者を誘ってWebブラウザで閲覧させます。Webブラウザ上で稼働した不正なスクリプトは、利用者の意図を確認しないまま、利用者のPCに密かに不正プログラムを転送して、インストールと実行をさせます。この不正プログラムは、PC内の機密情報を外部に流出させるなどの不正を働きます。



- × ア USBメモリのAutorun.infを悪用した攻撃です。
- × イ ランサムウェアの説明です。
- ウ 正解です。
- × エ ウォードライビング攻撃の説明です。

問26 パスワードリスト攻撃

パスワードリスト攻撃とは、Webサイトから流出した利用者IDとパスワードのリストを用いて、他のWebサービスに対してログインを試行する攻撃です。多くの利用者は、同じ利用者IDとパスワードを使い回す傾向があります。あるWebサービスから利用者IDとパスワードが流出すると、別のWebサービスに同じ利用者IDとパスワードでログインできる可能性が高くなります。パスワードリスト攻撃ではこの点を利用して、不正アクセスを試みます。

- × ア 辞書攻撃の説明です。
- × イ リバースブルートフォース攻撃の説明です。
- × ウ ブルートフォース攻撃の説明です。
- エ 正解です。

攻略のカギ

X.509証明書 問24

ITU-T (International Telecommunication Union Telecommunication Standardization Sector, 国際電気通信連合の電気通信標準化部門) が公表している、デジタル証明書の代表的なフォーマット。

X.509証明書の構成 (抜粋)

データ	説明
バージョン	証明書のバージョン
シリアル番号	証明書を一意に識別するために、認証局が付与した番号
有効期間	証明書の有効期間（開始日時及び終了日時）
主体者	証明書の発行を受けた者の情報
公開鍵アルゴリズム	証明書に含まれる公開鍵のアルゴリズム
公開鍵	主体者の公開鍵
証明書の署名	証明書のデジタル署名

(網掛けの範囲がデジタル署名の対象となる。認証局の秘密鍵で暗号化されている)

ランサムウェアの攻撃 問25

ランサムウェアは、次のような方法で感染し、PC内のデータを勝手に暗号化する。

- Webページに不正なスクリプトを仕込み、閲覧したPCの脆弱性を突いてランサムウェアをインストールする
- 有益なセキュリティソフトのように見せかけた広告を使って、利用者のインストールを促す

解答

問24 イ 問25 ウ
問26 エ

☐ **問 27** バックドアに該当するものはどれか。

- ☐ **ア** 攻撃を受けた結果、ロックアウトされた利用者アカウント
- ☐ **イ** システム内に攻撃者が秘密裏に作成した利用者アカウント
- ☐ **ウ** 退職などの理由で、システム管理者が無効にした利用者アカウント
- ☐ **エ** パスワードの有効期限が切れた利用者アカウント

☐ **問 28** PCとサーバとの間でIPsecによる暗号化通信を行う。ブロック暗号の暗号化アルゴリズムとしてAESを使うとき、用いるべき鍵はどれか。

- ☐ **ア** PCだけが所有する秘密鍵
- ☐ **イ** PCとサーバで共有された共通鍵
- ☐ **ウ** PCの公開鍵
- ☐ **エ** サーバの公開鍵

☐ **問 29** 攻撃者がシステムに侵入するときにポートスキャンを行う目的はどれか。

- ☐ **ア** 事前調査の段階で、攻撃できそうなサービスがあるかどうかを調査する。
- ☐ **イ** 権限取得の段階で、権限を奪取できそうなアカウントがあるかどうかを調査する。
- ☐ **ウ** 不正実行の段階で、攻撃者にとって有益な利用者情報があるかどうかを調査する。
- ☐ **エ** 後処理の段階で、システムログに攻撃の痕跡が残っていないかどうかを調査する。

☐ **問 30** AさんがBさんの公開鍵で暗号化した電子メールを、BさんとCさんに送信した結果のうち、適切なものはどれか。ここで、Aさん、Bさん、Cさんのそれぞれの公開鍵は3人全員がもち、それぞれの秘密鍵は本人だけがもっているものとする。

- ☐ **ア** 暗号化された電子メールを、Bさん、Cさんともに、Bさんの公開鍵で復号できる。
- ☐ **イ** 暗号化された電子メールを、Bさん、Cさんともに、自身の秘密鍵で復号できる。
- ☐ **ウ** 暗号化された電子メールを、Bさんだけが、Aさんの公開鍵で復号できる。
- ☐ **エ** 暗号化された電子メールを、Bさんだけが、自身の秘密鍵で復号できる。

解説

問27 バックドア

- × **ア** ロックアウトされた利用者アカウントを用いてシステムにログインすることはできません。
- **イ** 正解です。
- × **ウ** 無効にされた利用者アカウントを用いてシステムにログインすることはできません。
- × **エ** パスワードの有効期限が切れた利用者アカウントを用いてシステムにログインすることはできません。

攻略のカギ



バックドア

問27

社内LANなどに不正侵入した攻撃者がサーバに設置する、不正プログラムやアカウント。攻撃者が攻撃対象のサーバなどに再び侵入しやすくするために用いられる。システム内に攻撃者が秘密裏に作成した利用者アカウントなどがバックドアに該当する。

問28 IPsecの鍵

IPsecとは、IPパケットの暗号化及び認証に関する規格のことです。IPsecでは、IPパケットを暗号化するために、任意の暗号方式を選択して利用できます。

ブロック暗号は、データを一定のサイズに区切った単位（ブロック）ごとに暗号化を行う方式です。AES (Advanced Encryption Standard) は共通鍵暗号方式の一つで、ブロック暗号に属します。

AESを使うときは、PCとサーバが同じ共通鍵を共有し、PCが共通鍵で暗号化して送信したデータを、サーバが同じ共通鍵で復号できるようにします。**イ**が正解です。**ア**、**ウ**、**エ**は公開鍵暗号方式で用いられる鍵であり、AESでは使用できません。

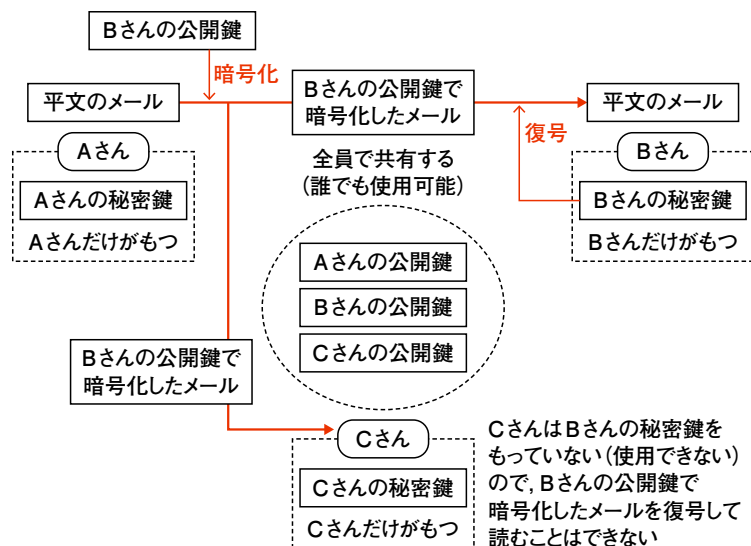
問29 ポートスキャン

ポートスキャンは、サーバの使用可能なサービスを調査するときに用いる攻撃です(**ア**)。対象ホストに対して、宛先ポート番号を順次増加させながらアクセスしていき、対象ホストから正常な応答が返ってきたときに、そのポート番号のサービスが稼働している(対象ポートが開いている)と判断します。

ポートスキャンは事前調査の段階で実施される行為です。権限取得、不正実行、後処理では実施されません。

問30 公開鍵暗号方式

公開鍵暗号方式では、利用者の公開鍵で暗号化したデータは、同じ利用者の秘密鍵でなければ復号できません。



AさんがBさんの公開鍵で暗号化した電子メールは、Bさんの秘密鍵でないと復号できません。よって、**エ**が適切です。

Bさんの公開鍵では電子メールを復号できないので**ア**は誤りです。CさんはBさんの秘密鍵を使用できないので、**イ**は誤りです。また、Aさんの公開鍵でも電子メールを復号できないので、**ウ**は誤りです。

攻略のカギ



IPsec

問28

インターネットなどの開かれたネットワーク上において、専用線と同様にセキュリティの確保された通信を行うための暗号化・認証プロトコル。OSI基本参照モデルのネットワーク層において暗号化などの処理を行う。



AES (Advanced Encryption Standard) 問28

共通鍵暗号方式の一つで、1977年に制定された共通鍵暗号方式であるDESの改善版として公募され、2000年に決定した方式。



攻撃者が実行する行為 問29

攻撃者がサーバなどに侵入する際に実行する、事前調査、権限取得、不正実行、後処理とは次のような行為。

- 事前調査
ポートスキャンなどによって、攻撃対象のシステムに存在する脆弱性を調査する。
- 権限取得
事前調査で特定した脆弱性を突いて、攻撃対象のシステムのアカウントの権限を取得し、不正アクセスができるようにする。
- 不正実行
権限取得の段階で取得したアカウントでログインし、攻撃対象のシステム上の情報を盗み見たり、改ざんしたりするなどの不正行為を実行する。
- 後処理
不正侵入の痕跡を削除するために、ログの削除や改ざんなどを行う。また、攻撃対象のシステムに再度侵入しやすくするために、バックドアを仕掛けたりする。

解答

問27 **イ** 問28 **イ**
問29 **ア** 問30 **エ**



問 31 “OECDプライバシーガイドライン”には8原則が定められている。その中の四つの原則についての説明のうち、適切なものはどれか。

	原則	説明
ア	安全保護の原則	個人データの収集には制限を設け、いかなる個人データも、適法かつ公正な手段によって、及び必要に応じてデータ主体に通知し、又は同意を得た上で収集すべきである。
イ	個人参加の原則	個人データの活用、取扱い、及びその方針については、公開された一般的な方針に基づかなければならない。
ウ	収集制限の原則	個人データの収集目的は収集時点よりも前に特定し、利用はその利用目的に矛盾しない方法で行い、利用目的を変更するに当たっては毎回その利用目的を特定すべきである。
エ	データ内容の原則	個人データは、利用目的に沿ったもので、かつ利用目的の達成に必要な範囲内で正確、完全、最新の内容に保つべきである。



問 32 個人情報に関する記述のうち、個人情報保護法に照らして適切なものはどれか。

- ア** 構成する文字列やドメイン名によって特定の個人を識別できるメールアドレスは、個人情報である。
- イ** 個人に対する業績評価は、特定の個人を識別できる情報が含まれていても、個人情報ではない。
- ウ** 新聞やインターネットなどで既に公表されている個人の氏名、性別及び生年月日は、個人情報ではない。
- エ** 法人の本店所在地、支店名、支店所在地、従業員数及び代表電話番号は、個人情報である。



問 33 刑法における“電子計算機損壊等業務妨害”に該当する行為はどれか。

- ア** 企業が運営するWebサイトに接続し、Webページを改ざんした。
- イ** 他社の商標に酷似したドメイン名を使用し、不正に利益を得た。
- ウ** 他人のWebサイトを無断で複製して、全く同じWebサイトを公開した。
- エ** 他人のキャッシュカードでATMを操作し、自分の口座に振り込んだ。

解説



攻略のカギ

問31 OECDプライバシーガイドライン

OECDプライバシーガイドラインは、1980年にOECD（経済協力開発機構）が公表した個人情報保護に関するガイドラインで、収集制限の原則などの8つの原則を定めています。

本問の解答群のうち、適切なのはデータ内容の原則 (**エ**) です。

- × **ア** この説明は収集制限の原則です。
- × **イ** この説明は公開の原則です。
- × **ウ** この説明は目的明確化の原則です。
- **エ** 正解です。

問32 個人情報保護法

個人情報保護法では、「個人情報」を次のように定義しています。

「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう
(同第2条より)

構成する文字列やドメイン名によって特定の個人を識別できるメールアドレスは、個人情報です。

- **ア** 正解です。
- × **イ** 個人に対する業績評価に、特定の個人を識別できる情報が含まれている場合は、個人情報です。
- × **ウ** 公開・非公開を問わず、特定の個人を識別できる情報は個人情報です。
- × **エ** 法人の本店所在地などは個人情報になりません。

問33 電子計算機損壊等業務妨害罪

電子計算機損壊等業務妨害罪は、刑法第234条の2で定義されている罪です。

人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、5年以下の懲役又は100万円以下の罰金に処する

人の業務に使用するコンピュータまたはデータを損壊したり、コンピュータに虚偽のデータを入力したりすることで、使用目的に反した動作をさせることが該当します。企業が運営するWebサイト上のWebページを改ざんすることも該当します。

- **ア** 正解です。
- × **イ** 商標法や不正競争防止法に違反する行為です。
- × **ウ** 著作権法に違反する行為です。
- × **エ** 電子計算機使用詐欺罪に該当する行為です。

攻略のカギ

OECDプライバシーガイドラインの8原則 問31

原則	説明
収集制限の原則	個人データの収集には制限を設ける。いかなる個人データも、適法かつ公正な手段によって、必要に応じてデータ主体に通知するか、または同意を得た上で収集しなければならない。
データ内容の原則	個人データは、その利用目的に沿ったものとする。かつ、利用目的に必要な範囲内で正確、完全、最新の内容に保つ。
目的明確化の原則	個人データの収集目的は、収集時よりも前の時点において明確化しなければならない。データの利用は、収集目的の達成または収集目的に矛盾してはならない。かつ、利用目的を変更する場合、毎回その利用目的を特定する。
利用制限の原則	個人データは、目的明確化の原則によって明確化された目的以外の目的のために、開示されたり利用されたりしてはならない。ただし、データ主体の同意があるか、法律の規定がある場合はその限りではない。
安全保護の原則	個人データは、紛失、不当なアクセス、破壊、使用、修正、開示などの危険に対して、合理的な安全保護措置により保護されなければならない。
公開の原則	個人データの活用、取扱い及びその方針については、公開された一般的な方針に基づくなくてはならない。
個人参加の原則	個人は、自分に関するデータを保有しているかどうかなどについて、データ管理者に確認する権利を有する。
責任の原則	データ管理者は、以上の各原則を実施するための措置に従う責任を有する。

解答

問31 **エ** 問32 **ア**
問33 **ア**



問 34 特定電子メール送信適正化法で規制される、いわゆる迷惑メール(スパムメール)はどれか。

- ア** ウイルスに感染していることを知らずに、職場全員に送信した業務連絡メール
- イ** 書籍に掲載された著者のメールアドレスへ、匿名で送信した批判メール
- ウ** 接客マナーへの不満から、その企業のお客様窓口に繰り返し送信したクレームメール
- エ** 送信することの承諾を得ていない不特定多数の人に送った広告メール



問 35 不正競争防止法によって保護される対象として規定されているものはどれか。

- ア** 自然法則を利用した技術的思想の創作のうち高度なものであって、プログラム等を含む物と物を生産する方法
- イ** 著作物を翻訳し、編曲し、若しくは変形し、又は脚色し、映画化し、その他翻案することによって創作した著作物
- ウ** 秘密として管理されている事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの
- エ** 法人等の発意に基づきその法人等の業務に従事する者が職務上作成するプログラム著作物



問 36 請負契約の下で、自己の雇用する労働者を契約先の事業所などで働かせる場合、適切なものはどれか。

- ア** 勤務時間、出退勤時刻などの労働条件は、契約先が定めて管理する。
- イ** 雇用主が自らの指揮命令の下に当該労働者を業務に従事させる。
- ウ** 当該労働者は、契約先で働く期間は、契約先との間にも雇用関係が生じる。
- エ** 当該労働者は、契約先の指揮命令によって業務に従事するが、雇用関係の変更はない。



問 37 スプレッドシートの利用に係るコントロールの監査において把握した、利用者による行為のうち、指摘事項に該当するものはどれか。

- ア** スプレッドシートに組み込まれたロジックの正確性を、検算によって確認していた。
- イ** スプレッドシートに組み込まれたロジックを、業務上の必要に応じて、随時、変更し上書き保存していた。
- ウ** スプレッドシートにパスワードを付した上で、アクセスコントロールが施されたサーバに保管していた。
- エ** スプレッドシートを所定のルールに従ってバックアップしていた。

問34 迷惑メール

特定電子メールの送信の適正化等に関する法律（以下、特定電子メール送信適正化法という）では、いわゆる**迷惑メール**に関して、次の用語を定義しています。

特定電子メール：「電子メールの送信……をする者（営利を目的とする団体及び営業を営む場合における個人に限る。以下「送信者」という。）が自己又は他人の営業につき広告又は宣伝を行うための手段として送信をする電子メール」

特定電子メールの送信を承諾している者に対して広告メールを送るのは問題がありません。しかし、特定電子メールの送信を承諾していない不特定多数の人に対して広告メールを送ることは、特定電子メール送信適正化法の第3条に違反します。このようなメールが、いわゆる迷惑メールです。正解は**エ**です。

ア～ウは、不特定多数には送られていません。

問35 不正競争防止法

- × **ア** 自然法則を利用した技術的思想の創作のうち高度なもののことを発明といいます。特許法では、発明を特許として保護対象にしています。
- × **イ** 著作権法が保護している二次的著作物の説明です。
- **ウ** 正解です。
- × **エ** 著作権法が保護しているプログラムの著作物の説明です。

問36 請負契約

請負契約では、労働者は雇用主（請負元）の指揮命令の下で、契約先（請負先）の指定する勤務先などにおいて作業を行います。労働者と契約先との間には、指揮命令関係はありません。よって、**イ**（雇用主が自らの指揮命令の下に当該労働者を業務に従事させる）が正解です。

- × **ア** 労働条件は、指揮命令権をもつ雇用主（請負元）が調整します。
- **イ** 正解です。
- × **ウ** 労働者と契約先との間には、契約先で働く期間において、特に雇用関係は生じません。
- × **エ** 請負契約では、労働者は契約先ではなく雇用主の指揮命令によって業務に従事します。

問37 スプレッドシートの利用の指摘事項

スプレッドシートに計算用のマクロなどを設定して、財務諸表の作成や会計処理などを行うことがあります。このとき、マクロのロジック（処理内容）を誰でも自由に変更できるようにすると、利用者がロジックを勝手に書き換えて売上高などの値を操作し、不正な会計処理を実行できます。

このような内部不正を発生させないために、スプレッドシートに組み込まれたロジックを、管理者など権限をもつ者以外は自由に変更できないようにする必要があります。スプレッドシートの利用に係るコントロールの監査において、**イ**の行為は指摘事項となります。**ア**、**ウ**、**エ**の行動は、いずれも会計処理の適切性確認や不正アクセスの防止などの適切な行動です。

不正競争防止法 問35

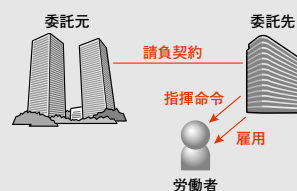
「事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もって国民経済の健全な発展に寄与する」（同法第1条より）ことを目的とした法律。幾つかの行為を「不正競争」として定義し、不正競争によって営業上の利益を侵害された者などは、その侵害の停止などを請求する権利があることを規定している。

営業秘密 問35

不正競争防止法が定義している「営業秘密」とは、同法で保護されている対象であり、「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」を指す。

請負契約における労働者と事業主間の関係

請負契約においては、「労働者」、「委託先事業主（発注者）」、「委託元事業主（受注者）」の3者間の関係は次の図のようになります。



スプレッドシート 問37

Excelなどの表計算ソフトのシートのこと。売上情報などの各種データの記録、集計、分析などをするために用いる。また、スプレッドシートに計算用のマクロを設定することで、定型的な集計処理などを簡単な操作で実行できる。

解答

問34 **エ** 問35 **ウ**
問36 **イ** 問37 **イ**

問 38 従業員の守秘義務について、“情報セキュリティ管理基準”に基づいて監査を行った。指摘事項に該当するものはどれか。

- ア 雇用の終了をもって守秘義務が解消されることが、雇用契約に定められている。
- イ 定められた勤務時間以外においても守秘義務を負うことが、雇用契約に定められている。
- ウ 定められた守秘義務を果たさなかった場合、相応の措置がとられることが、雇用契約に定められている。
- エ 定められた内容の守秘義務契約書に署名することが、雇用契約に定められている。

問 39 “情報セキュリティ監査基準”に基づいて情報セキュリティ監査を実施する場合、監査の対象、及びコンピュータを導入していない部署における監査実施の要否の組合せのうち、最も適切なものはどれか。

	監査の対象	コンピュータを導入していない部署における 監査実施の要否
ア	情報資産	必要
イ	情報資産	不要
ウ	情報システム	必要
エ	情報システム	不要

問 40 SLAに記載する内容として、適切なものはどれか。

- ア サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意事項
- イ サービス提供者が提供する全てのサービスの特徴、構成要素、料金
- ウ サービスデスクなどの内部グループとサービス提供者との間の合意事項
- エ 利用者から出されたITサービスに対する業務要件

解説

問 38 情報セキュリティ管理基準の指摘事項

“情報セキュリティ管理基準”の人的セキュリティの章では、従業員の雇用条件について以下のように規定しています。

「雇用条件には、情報セキュリティに対する従業員の責任について記述してあること」

「適切ならば、これらの責任を、雇用終了後の定められた期間継続すること」

情報セキュリティに対する従業員の責任とは、社内の機密情報を外部に漏らさないこと、すなわち守秘義務のことです。従業員の雇用を終了しても、これらの責任を一定期間継続することが、“情報セキュリティ管理基準”で規定されています。したがって、アの記述は指摘事項となります。

攻略のカギ

情報セキュリティ監査制度 問 38

企業や政府などの情報セキュリティ対策が適切に実行され、情報セキュリティに係るリスクマネジメントが効果的に実施されているかどうかを、情報セキュリティ監査によって確認するための制度。この制度においては、経済産業省が公表している“情報セキュリティ監査基準”や“情報セキュリティ管理基準”が、情報セキュリティ監査の尺度として用いられる。

- **ア** 正解です。
- × **イ** “情報セキュリティ管理基準”では、定められた勤務時間以外でも守秘責任を負うことを雇用契約に定めると規定しています。
- × **ウ** “情報セキュリティ管理基準”では、従業員がセキュリティ要求事項を無視した場合に採る措置についても雇用条件に含めることを規定しています。
- × **エ** “情報セキュリティ管理基準”では、従業員は雇用条件の一部として機密保持契約書又は守秘義務契約書に署名することを規定しています。

問39 情報セキュリティ監査の実施

“**情報セキュリティ監査基準**”では、監査人が監査上の判断の尺度として用いべき基準として、“情報セキュリティ管理基準”を使用すると定めています。“情報セキュリティ管理基準”では次のように定義しています。

「「情報セキュリティ管理基準」は、……組織体の業種及び規模等を問わず汎用的に適用できるように、情報資産を保護するための最適な実践慣行を帰納要約し、情報セキュリティに関するコントロールの目的、コントロールの項目を規定したものである。」

以上から、監査の対象は“情報資産”です。

情報セキュリティ管理基準は「組織体の業種及び規模等」を問うことなく適用できるので、コンピュータを導入していない部署に対しても情報セキュリティ監査を実施できます。また、例えばコンピュータを導入していない部署において、紙媒体の機密情報を管理している場合、その部署から情報が漏えいする危険性があります。コンピュータを導入していない部署においても、導入している部署と同じレベルの管理策が必要になるので、その実施状況を監査で検証するのが適切です。よって、コンピュータを導入していない部署における監査実施の要否は“必要”です。

両者から、**ア**が正解です。

問40 SLA

SLA (Service Level Agreement) とは、サービスの利用者と提供者との間で、その品質や提供時間などに関して締結された合意のことです。

よって、「サービス及びサービス目標を特定した、サービス提供者と顧客との間の合意事項」(**ア**)が、SLAに記載する内容として適切です。

- **ア** 正解です。
- × **イ** サービス提供者が提供する全てのサービスの特徴などは、顧客との合意事項ではありません。
- × **ウ** サービスデスクなどの内部グループとサービス提供者との間の合意事項は、社内規則などに記載するものです。
- × **エ** 利用者からの要件は、システムの設計時などにおいて考慮するものです。

攻略のカギ

情報セキュリティ管理基準 問38

組織体が効果的な情報セキュリティマネジメント体制を構築し、情報セキュリティに関するコントロールを適切に整備・運用するための実践規範。情報セキュリティ監査制度において、監査人が情報セキュリティ監査を行う際に用いられる。

情報資産 問39

情報及び情報を管理するためのシステムのこと。特に、顧客情報や製品開発情報など、外部に漏えいすると自社の利益が損なわれたり、信用が失墜したりする情報が該当する。

SLAの項目の例 問40

例えば、通信サービスの提供者（電気通信事業者など）と利用者との間で次の契約を結ぶとき、SLAには次のような項目が示される。

- 契約
提供者は利用者に対して、契約回線のデータ通信の遅延は常に**秒以下に抑えるようにサービスの品質を提供する。提供者の責によってその品質が満たされなかった場合は、当該月の利用料を減殺する
- SLAで示される項目
契約内容、遅延抑制の目標時間、品質が満たされなかった場合に減殺する利用料の額など

解答

問38 **ア** 問39 **ア**
問40 **ア**

☐ ☐ ☐ **問 41** 事業継続計画で用いられる用語であり、インシデントの発生後、次のいずれかの事項までに要する時間を表すものはどれか。

- (1) 製品又はサービスが再開される。
- (2) 事業活動が再開される。
- (3) 資源が復旧される。

ア MTBF

イ MTTR

ウ RPO

エ RTO

☐ ☐ ☐ **問 42** 過去5年間のシステム障害について、年ごとの種類別件数と総件数の推移を一つの図で表すのに最も適したものはどれか。

ア 積上げ棒グラフ

イ 二重円グラフ

ウ ポートフォリオ図

エ レーダチャート

☐ ☐ ☐ **問 43** コンピュータシステムに対して問合せの終わり又は要求の終わりを指示してから、利用者端末に最初の処理結果のメッセージが出始めるまでの経過時間を何と
いうか。

ア アクセスタイム

イ サイクルタイム

ウ ターンアラウンドタイム

エ レスポンスタイム

☐ ☐ ☐ **問 44** 企業の様々な活動を介して得られた大量のデータを整理・統合して蓄積しておく、意思決定支援などに利用するものはどれか。

ア データアドミニストレーション

イ データウェアハウス

ウ データディクショナリ

エ データマッピング

解説

問41 事業継続計画

RTO (Recovery Time Objective, **エ**) と RPO (Recovery Point Objective, **ウ**) は、ディザスタリカバリで用いられる指標です。RTO は、災害発生時から業務が再開されるまでに要する時間の指標です。

RPO は、災害発生からどれだけ近い時刻で業務の状態を復元できるかの指標です。災害発生時刻と、復元できた時点の時刻との時間差で表されます。

MTBF (Mean Time Between Failure, 平均故障間隔, **ア**) は、システムが故障から復旧した後、次に故障するまでに経過する時間の平均値です。

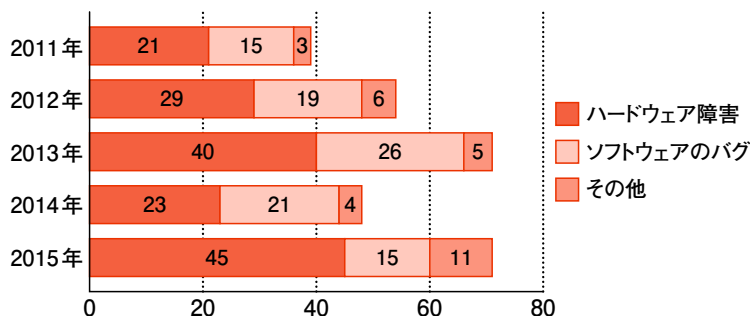
MTTR (Mean Time To Repair, 平均修理時間, **イ**) は、システムが故障してから復旧するまでに経過する時間の平均値です。

以上から、**エ** が (2) に該当するので正解です。

攻略のカギ

問42 種類別件数と総件数を表すグラフ

本問のように、各年の種類別件数と総件数をわかりやすく表示するためには、次のような**積上げ棒グラフ**が適切です。



- **ア** 正解です。
- × **イ** 二重円グラフは、売上高の内訳の比率など、構成比率に適しています。
- × **ウ** ポートフォリオ図は、二つの特性値を縦軸と横軸に取り、各データを二つの特性値に応じた位置に置いた図で、市場における製品の位置などを表現するのに適しています。
- × **エ** レーダチャートは、複数の特性間のバランスの把握に適しています。

問43 入力から結果までの経過時間

コンピュータシステムに問合せや入力の終わりを指示してから、最初の処理結果のメッセージ出力が開始されるまでの経過時間のことを、**レスポンスタイム**（応答時間）といいます。

- × **ア** アクセスタイムとは、データへのアクセスが開始してから完了するまでの経過時間のことです。
- × **イ** サイクルタイムとは、複数のデータを連続して処理しているときに、あるデータの処理を開始してから次のデータの処理が開始されるまでの経過時間のことです。
- × **ウ** ターンアラウンドタイムとは、ジョブの入力開始時から結果の出力終了時まで経過した時間のことです。
- **エ** 正解です。

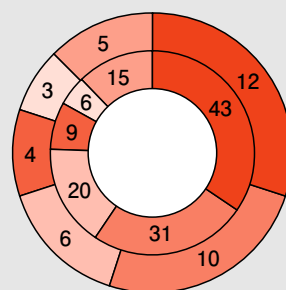
問44 意思決定のためにデータを蓄積するシステム

データウェアハウスの説明です。企業の様々な活動で得られたデータは、データウェアハウスに蓄積され、過去の売上傾向の分析に使用されます。

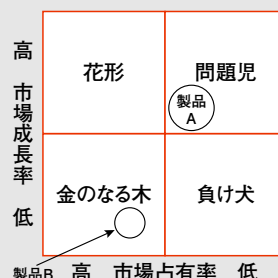
- × **ア** **データアドミニストレーション**とは、データベースに格納されたデータを適切に管理すること、及びそのための体制のことです。
- **イ** 正解です。
- × **ウ** **データディクショナリ**とは、ネットワーク内に存在する全てのデータについて、その存在箇所や使い方、及び定義などを記録するために設けられるものです。
- × **エ** **データマッピング**とは、複数のデータ間での関連付けを指す用語です。

攻略のカギ

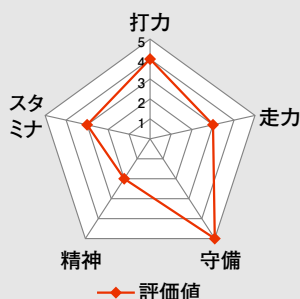
二重円グラフ 問42



ポートフォリオ図 問42



レーダチャート 問42



データウェアハウス 問44

売上動向などの分析のために、時系列に蓄積された日々の業務データから、さまざまな項目間の関連性を得るために使用されるシステムのこと。Oracleなどのデータベース管理システムを用いて構築される。

解答

- 問41 **エ** 問42 **ア**
問43 **エ** 問44 **イ**



問 45 ルータの機能に関する記述として、適切なものはどれか。

- ☐ ア LAN同士やLANとWANを接続して、ネットワーク層での中継処理を行う。
- ☐ イ データ伝送媒体上の信号を物理層で増幅して中継する。
- ☐ ウ データリンク層でネットワーク同士を接続する。
- ☐ エ 二つ以上のLANを接続し、LAN上のMACアドレスを参照して、その参照結果を基にデータフレームを他のLANに流すかどうかの判断を行う。



問 46 社内ネットワークからインターネットへのアクセスを中継し、Webコンテンツをキャッシュすることによってアクセスを高速にする仕組みで、セキュリティ確保にも利用されるものはどれか。

- ☐ ア DMZ
- ☐ イ IPマスカレード (NAPT)
- ☐ ウ ファイアウォール
- ☐ エ プロキシ



問 47 利用者が、インターネットを経由してサービスプロバイダのシステムに接続し、サービスプロバイダが提供するアプリケーションの必要な機能だけを必要なときにオンラインで利用するものはどれか。

- ☐ ア ERP
- ☐ イ SaaS
- ☐ ウ SCM
- ☐ エ XBRL

解説

問45 ルータ

ルータは、ネットワーク層での中継処理を行い、LAN同士またはLANとWANとを接続する機能をもつLAN間接続装置です。ルータは、受信したIPパケットの宛先IPアドレスを参照して、IPパケットを適切な宛先ネットワークに転送する処理（ルーティング）などを行います。

- **ア** 正解です。
- × **イ** **リピータ**の説明です。
- × **ウ** **ブリッジ**の説明です。
- × **エ** **スイッチングハブ**の説明です。

問46 Webのアクセスの中継

インターネット上のサーバに組織内のPCが直接アクセスすると、IPアドレスが外部に知られて、不正アクセスの危険性が増加します。このような場合に**プロキシサーバ**を利用します。プロキシサーバは、PCの代わりに外部のサーバにアクセスし、サーバから返ってきたレスポンスをPCに転送する装置です。

この方法ではプロキシサーバのIPアドレスしか外部に知られません。PCのIPアドレスは知られなくなり、安全性が高まります。



攻略のカギ



リピータ

問45

物理層での中継を行い、伝送されてくるデータの信号波形を増幅・修正するLAN間接続装置。



ブリッジ

問45

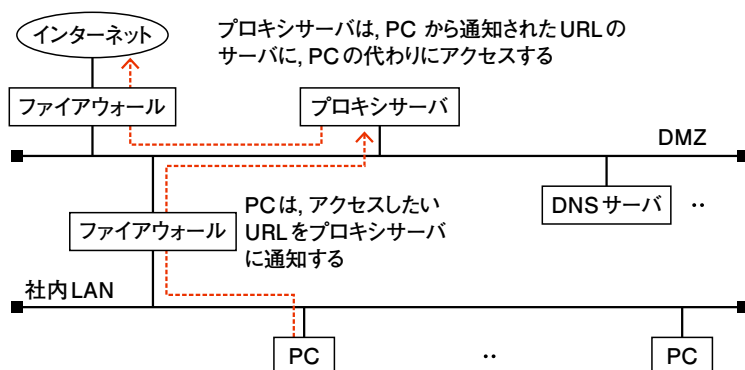
データリンク層でネットワーク同士を接続するLAN間接続装置。



スイッチングハブ

問45

二つ以上のLANを接続し、LAN上のMACアドレスを参照して、必要なLANのみにデータフレームを伝送するLAN間接続装置。



プロキシサーバには、一度アクセスしたWebコンテンツをキャッシュする機能があります。PCが一度アクセスしたWebページはプロキシサーバに保存されます。同じ組織の別のPCが同じWebページにアクセスした場合、プロキシサーバに保存されているWebページの内容が返されます。これによってWebコンテンツへのアクセスが高速化されます。

- × **ア** DMZ (DeMilitarized Zone = 非武装地帯) とは、インターネットに公開するサーバを配置するために用意する、内部LAN及びインターネットの両方から分離した特別な領域のことです。
- × **イ** IPマスカレード (NAPT) とは、プライベートIPアドレスとグローバルIPアドレスとを、多対1で変換するための仕組みのことです。
- × **ウ** ファイアウォールとは、インターネットと内部LAN、または内部LANとDMZとを分割するために設ける装置のことです。
- **エ** 正解です。

問47 アプリケーションをオンラインで利用する形態

サービス提供側 (プロバイダ) が用意したアプリケーションの機能を、インターネット経由で必要に応じて利用者側のPCにインストールさせ、オンラインで使用させるサービスのことを **SaaS** (Software as a Service) といいます。このサービスでは、利用者側がソフトウェアをPCにインストールする手間が省けるなどのメリットがあります。

- × **ア** **ERP** (Enterprise Resource Planning, 統合基幹業務システム) とは、企業の各種活動 (生産、製造、物流、販売、人事など) におけるプロセス (ビジネスプロセス) についての情報を一元管理し、迅速に利用することによって経営効率を最大限に向上させようとする活動のことです。
- **イ** 正解です。
- × **ウ** **SCM** (Supply Chain Management, サプライチェーンマネジメント) とは、製品の生産、受発注の管理、資材調達、在庫管理、物流などの一連の業務を、全体最適の視点から見直し、コンピュータを用いて管理する手法のことです。
- × **エ** **XBRL** (Extensible Business Reporting Language) とは、財務諸表や財務報告用の各種の情報などを、ソフトウェアやプラットフォームに依存せずに作成、流通、及び利用できるように標準化された、XMLベースの言語及び規約のことです。

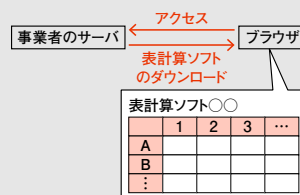
攻略のカギ

プロキシサーバによるセキュリティ確保 問46

インターネット上のサーバに組織内のPCが直接アクセスすると、IPアドレスが外部に知られて不正アクセスなどの危険性が増加する。プロキシサーバを設置して、外部とのアクセスをプロキシサーバ経由で行うようにすると、PCのIPアドレスは外部に知られなくなり、安全性が高まる。

SaaSの例 問47

ブラウザの画面上で表計算ソフトを利用できる。



PaaS (Platform as a Service) 問47

クラウドコンピューティングのサービスモデルの一つ。サービス事業者は、インフラに加えてサーバ上で稼働するOSも提供する。利用者は、アプリケーションソフトウェアを導入してシステムを運用する。

IaaS (Infrastructure as a Service) 問47

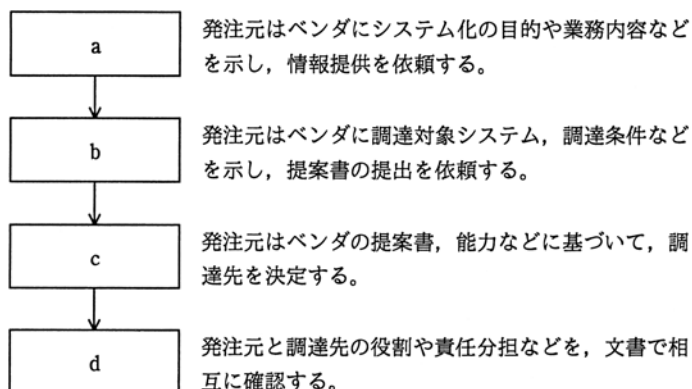
クラウドコンピューティングのサービスモデルの一つ。サービス事業者は、ハードウェアやネットワーク機器といったサービスのインフラだけを提供する。利用者は、OS及びアプリケーションソフトウェアを導入してシステムを運用する。

解答

問45 **ア** 問46 **エ**
問47 **イ**



問 48 図に示す手順で情報システムを調達する場合、bに入るものはどれか。



ア RFI

イ RFP

ウ 供給者の選定

エ 契約の締結



問 49 事業継続計画の策定に際し、リスクへの対応として適切なものはどれか。

ア 全リスクを網羅的に洗い出し、リスクがゼロとなるように策定する。

イ 想定するリスクのうち、許容できる損失を超えるものを優先的に対処する。

ウ 想定するリスクの全てについて、発生時の対応策をとることを目的とする。

エ 想定するリスクの優先度に差をつけずに検討する。



問 50 企業経営の透明性を確保するために、企業は誰のために経営を行っているか、トップマネジメントの構造はどうなっているか、組織内部に自浄能力をもっているかなどの視点で、企業活動を監督・監視する仕組みはどれか。

ア コアコンピタンス

イ コーポレートアイデンティティ

ウ コーポレートガバナンス

エ ステークホルダアナリシス

解説

問48 調達の手順

情報システムの発注元が、システム化の目的や業務内容などを示して、調達先に情報の提供を依頼するための書類を、**RFI** (Request For Information, 情報提供依頼書) といいます。aにはRFI (**ア**) が入ります。

調達先から情報を受け取った発注元が、発注する情報システムの概要や発注依頼事項、調達条件及びサービスレベル要件などを明示し、提案書の提出を依頼するために調達先に送付する文書を、**RFP** (Request For Proposal, 提案依頼書) といいます。bにはRFP (**イ**) が入ります。

発注元は、各調達先から送付されてきた提案書の内容などに基づいて、情報



攻略の力ギ



RFI (Request For Information, 情報提供依頼書) 問48

情報システムの発注をするために必要な情報の提供を受注者に対して要請するための文書。

システムの発注をする調達先（供給者）を選定します。この作業を**供給者の選定**といいます。cには供給者の選定（ウ）が入ります。

発注元は、選定した供給者との間で文書を取り交わして契約を締結し、両者の役割や情報システム開発における責任分担などを確認します。dには**契約の締結**（エ）が入ります。

以上から、イが正解です。

問49 事業継続計画

情報システムが地震や火災などの災害や停電などの障害に見舞われても、可能な限り早期にシステムを復旧させ、業務を再開するために日ごろから立ておく計画のことを、**事業継続計画**（Business Continuity Plan, BCP）といいます。

災害などが発生したとき、業務に及ぼす影響が少ない軽微なリスクに対応すると、業務の再開に多大な影響を及ぼす重大なリスクに対応するための人員や時間が確保できず、業務の再開が遅れます。損失が大きいものなど重大なリスクだけを優先的に対処し、そうでないものは対処しないか簡単な対処だけを行って、業務を早期に再開可能にするのが適切です。

- × ア リスクの中には、地震や台風など発生を抑止できないものがあり、全てのリスクをゼロにすることはできません。
- イ 正解です。
- × ウ 想定するリスクのうち、損失が大きいものを優先的に対処します。
- × エ 想定するリスクのうち、優先度の高いものほどより重点的に対策します。

問50 企業経営の正当性の維持

企業の経営管理が適切に行われているかを監視し、ステークホルダに対して企業活動の正当性を維持する行為、及びそのための仕組みのことを**コーポレートガバナンス**といいます。

コーポレートガバナンスは、企業の経営活動において粉飾決算などの不正行為が行われていないかを監督・監視して、企業の不祥事を防ごうとする目的で実施されます。

- × ア **コアカンピタンス**とは、競合他社にはまねのできない、企業独自のノウハウや技術などを核とし、それらに経営資源を集中して競争優位を確立することを目的とする経営手法のことです。
- × イ **コーポレートアイデンティティ**とは、企業の理念、特徴及び独自性などを、ロゴのデザインや広告のイメージ、及び企業が公開するメッセージによって、利用者にわかりやすく伝えて企業イメージを高めようとする戦略のことです。
- ウ 正解です。
- × エ **ステークホルダアナリシス**とは、自社の事業に関連する各ステークホルダの役割やニーズなどを分析することです。

攻略のカギ

RFP (Request for Proposal, 提案依頼書) 問48

発注する情報システムの概要や発注依頼事項、調達条件及びサービスレベル要件などを明示し、情報システムの提案書の提出を依頼するための文書。

RFQ (Request For Quotation, 見積依頼書) 問48

情報システムの取得者からベンダに対して送付されるもので、発注する情報システムの価格などの見積りの提出を依頼するための書類。

リスク 問49

脅威が情報資産の脆弱性につけこみ、情報資産に損失などを与える可能性のこと。

リスクマネジメント 問49

リスクの防止、リスク発生時に被害を最小限にするための施策の制定、及びリスク発生により生じる費用に対する積み立てなどの措置を実施するなどの手法によってリスクを管理すること。

ステークホルダ (stake holder) 問50

もともとは「賭け金を管理する人」を意味する用語。現在では「企業の経営活動などに関する利害関係者」という意味になっている。具体的には、顧客（消費者）、取引先、株主、従業員、公的機関など、企業活動の周辺に存在している、あらゆる利害関係者を指す。

解答

問48 イ 問49 イ
問50 ウ

平成28年度 春期 午後問題

問 1

標的型攻撃メールの脅威と対策に関する次の記述を読んで、設問1, 2に答えよ。

Y社は、事務用機器を主力商品とする販売代理店である。従業員数は1,200名であり、本社には営業部、情報システム部、総務部などがある。

〔PCのマルウェア感染〕

ある日、情報システム部は、Y社内の1台のPCが大量の不審なパケットを発信していることをネットワーク監視作業中に発見し、直ちに外部との接続を遮断した。

情報システム部による調査の結果、営業部に所属する若手従業員G君が、受信した電子メール（以下、電子メールをメールという）の添付ファイルを開封したことが原因で、G君のPCがマルウェアに感染し、大量のパケットを発信していたことが判明した。幸いにも、情報システム部の迅速な対処によって、顧客情報の漏えいなどの最悪の事態は防ぐことができた。

〔受信したメール〕

情報システム部のS主任は、営業部の情報セキュリティリーダーであるE課長に、今回の事態に関する調査結果を報告した。次は、その時の会話である。

S主任：G君が受信したメールは、いわゆる標的型攻撃メールと呼ばれるものです。標的型攻撃メールとは、の組織や個人を対象として、受信者のPCにマルウェアを送りつけ、情報を窃取することなどを目的とするメールであり、の組織や個人を対象として送られるウイルスメールとは異なるものです。

E課長：最近是国内でも標的型攻撃メールに起因する情報漏えい事故が多数発生しており、大手企業や官公庁以外もターゲットになり得るので、営業部の従業員には十分に注意するよう言っていたのだが。

S主任：標的型攻撃メールでは、注意していたつもりでも、気付かずにマルウェア感染が起こります。また、受信者が疑いをもたないように、メールの差出人を公的機関などに詐称したり、メールの件名や内容を受信者の業務に関連したものに偽装したりするといった、を利用します。

E課長：G君が受信したメールを具体的に説明してくれるかな。

S主任：メールの内容を図1に示します。この内容から、①受信者の疑いを低減させる手口や、受信者の動作を巧みに誘導する手口などが見受けられます。

S主任は、②標的型攻撃メールによく見られる注意すべき特徴のうち、G君が受信したメールに見られる特徴を説明した。

差出人：F <F@zz-freemail.co.jp> 送信日時：2016/03/18 10:22
宛先：info@y-sha.com
CC：
件名：Re: Re: 【至急】製品導入に関する問合せ
添付ファイル：  質問事項.exe

G様

お世話になっております。
先日、貴社の製品について問合せをしたX社のFです。
これまで、貴社の事務用機器に関する情報を提供していただき、
ありがとうございました。
弊社では、今回、貴社から提案していただいた製品について、
導入する方向で検討を進めております。
その中で、確認したい事項が幾つか出てきました。
つきましては、急なお願いで恐縮ですが、添付ファイルの質問内容をご確認の上、本日15時までに回答をいただけないでしょうか。
よろしくお願いいたします。

X社 調達部 F
E-mail: F@x-sha.co.jp
URL: http://www.x-sha.co.jp

図1 G君が受信したメールの内容

【ヒアリング】

S主任からの調査報告を受けたE課長は、G君に対して、このメールを受信した際の状況及び対応に関してヒアリングをした。また、Y社の情報セキュリティインシデント管理規程（以下、管理規程という）などにおいては対応しなかった理由をG君に確認した。

E課長がまとめたヒアリング結果を図2に、Y社の管理規程を図3に示す。

- ・X社は過去に取引がある会社であった。
- ・F氏と直接会ったことはなかったが、10日前から、製品の問合せが3回あり、メールでやり取りをしていた。
- ・メールの添付ファイルを開封した際は、見慣れないウィンドウが表示されただけでドキュメントは開くことができなかった。そこで、ファイルを再送してほしい旨を先方にメールで返信したが、15時までと急いでいた割にその後の返信が無く不審に思った。再度連絡しようと思っていたが、別件で多忙になり、確認ができなかった。
- ・その後、PCの処理速度が遅くなったり、見慣れないウィンドウが表示されたりするなどの不具合や不審な事象が発生していたが、その都度、PCを再起動するなどして解決を試みた。また、ウイルス対策ソフトが動作し、パターンファイルが最新になっていることを確認できたのでマルウェア感染はあり得ないだろうと考え、誰にも相談せず、報告もしなかった。
- ・以前に他の部のH君が、顧客から貸与されたUSBメモリをPCに接続してマルウェア感染が起きたことを上司に報告した際に、上司から大変厳しく叱責されたとH君本人から聞いていたので、マルウェア感染と確信できない限りは、報告したくないと思っていた。
- ・管理規程については、新入社員研修の際に一度見たことがある程度で、重要な規程とは思っていなかった。
- ・標的型攻撃メールについては、聞いたことはあったが理解はしていなかった。

図2 G君へのヒアリング結果

第1章 情報セキュリティインシデント（以下、インシデントという）の定義 ・インシデントとは次のことをいう。 “不正アクセス”，“マルウェア感染”，“情報の漏えい”，“情報の改ざん”，“情報の消失”，（省略） 第2章 インシデント検知時の報告及び対処 ・従業員は、インシデントを発見した際には、速やかに情報セキュリティリーダーに報告し、その指示に従うこと。 - なお、インシデントであるかどうか判断がつかない疑わしい事象も、自己判断せず同様に報告すること。 ・情報セキュリティリーダーは、インシデントを認知した場合には、その状況を確認し、情報セキュリティ責任者に速やかに報告するとともに、情報システム部と連携し、被害の拡大防止を図るための応急措置及び復旧に係る指示又は勧告を行うこと。 ・従業員は、各自の判断で復旧対応や解決を試みるのではなく、必ず情報セキュリティリーダーの指示又は勧告に従うこと。 第3章 インシデントの原因調査及び再発防止 ・情報セキュリティリーダーは、情報システム部と協力してインシデントの原因を調査するとともに、再発防止策を検討し、報告書にまとめて情報セキュリティ責任者に報告すること。 （省略）

図3 管理規定

〔情報セキュリティ意識向上に向けて〕

次は、ヒアリング実施後のE課長とS主任との会話である。

S主任：標的型攻撃メールによるマルウェア感染を完全に防ぐことは難しいので、被害を最小化するためには、メールの添付ファイルを開封した後に従業員が適切な対応を取ることが重要になります。

E課長：そうだね。③今回の初動対応における問題点は二つあったと思う。本来であれば、管理規程に基づき、疑わしい事象を発見した従業員は、に報告をしなければならない。また、報告に当たっては、報告することも重要だ。

S主任：おっしゃるとおりです。今回の問題点を解決するには、規程やルールは単に策定しただけでは不十分であり、それらが順守されるように, の2点を行うことが重要だと考えられます。

E課長：今回のような標的型攻撃メールなどへの対策に当たっては、従業員一人一人の情報セキュリティ意識を向上させる地道な活動が必要だと思う。まずは、④実際に攻撃を受けた場合にも一人一人が適切に対応できるかを定量的に測定し評価できるようにしていきたい。そのための全社的な取り組みも情報システム部で実施してもらえないだろうか。

S主任：承知いたしました。検討し実施したいと思います。

E課長からの提案もあって、Y社では、従業員の情報セキュリティ意識向上に着実に取り組むようになった。

設問1 〔受信したメール〕について、(1)～(4)に答えよ。

(1) 本文中の, に入れる字句はどれか。解答群のうち、最も適切なものを選び。

a, bに関する解答群

ア 海外

イ 国内

ウ 特定

エ 架空

オ 大企業

カ 不特定多数

ク 官界

ケ 中小企業

コ 民間

(2) 本文中の□ c □に入れる字句はどれか。解答群のうち、最も適切なものを選び。

cに関する解答群

- | | |
|------------------------|---------------------|
| ア AES | イ ゼロデイ攻撃 |
| ウ ソーシャルエンジニアリング | エ トロイの木馬 |
| オ ヒヤリハット | カ ブルートフォース攻撃 |

(3) 本文中の下線①について、今回の攻撃者が使った手口として考えられるものを二つ、解答群の中から選べ。

解答群

- ア** 製品を導入する方向で検討を進めているという趣旨を伝えた上で、質問の回答期限を指定することによって添付ファイルを開くよう誘導している。
- イ** メール本文にY社の従業員しか知り得ない情報を記載することによって疑いを低減している。
- ウ** メール本文に正当なURLを装ったリンクを記載した上で、そのURLリンクをクリックするよう指示し、誘導している。
- エ** メールやり取りを数回行うことによって疑いを低減している。

(4) 本文中の下線②について、次の(i)～(iii)のうち、G君が受信したメールに見られる特徴だけを全て挙げた組合せを、解答群の中から選べ。

- (i) 差出人のメールアドレスがY社の社内メールアドレスに詐称されている。
- (ii) 差出人のメールアドレスと、本文の末尾に記載された署名のメールアドレスが異なる。
- (iii) 実行形式ファイルが添付されている。

解答群

- | | | |
|---------------------|--------------------|---------------------------|
| ア (i) | イ (i), (ii) | ウ (i), (ii), (iii) |
| エ (i), (iii) | オ (ii) | カ (ii), (iii) |
| キ (iii) | | |

設問2 【情報セキュリティ意識向上に向けて】について、(1)～(5)に答えよ。

(1) 本文中の下線③について、次の(i)～(iv)のうち、今回の初動対応における問題点を二つ挙げた組合せを、解答群の中から選べ。

- (i) PCの不具合に気付いても直ちに再インストールなどの復旧対応を行わなかった点
- (ii) 問合せ対応を行うに当たって、X社との最近の取引記録を確認しなかった点
- (iii) 不審な事象が起きたにもかかわらず、情報セキュリティリーダーに報告しなかった点
- (iv) 不審な事象が起きたにもかかわらず、マルウェアには感染していないと自己判断した点

解答群

- | | | |
|----------------------|---------------------|----------------------|
| ア (i), (ii) | イ (i), (iii) | ウ (i), (iv) |
| エ (ii), (iii) | オ (ii), (iv) | カ (iii), (iv) |

(2) 本文中の□ d □に入れる字句はどれか。解答群のうち、最も適切なものを選び。

dに関する解答群

- ア** インシデントであると判断した後

- イ 原因調査後
- ウ 再発防止策を検討した後
- エ 速やか

(3) 本文中の「e」に入れる字句はどれか。解答群のうち、最も適切なものを選び。

eに関する解答群

- ア 誤った報告を行わないよう、事象をインターネットや書籍などで確認して、類似の事例が確認できたものを
- イ 判断に迷う事象であっても自己判断せずに
- ウ 部内の同僚と相談してから、報告するように勧められた事象を
- エ 報告事項がそろうのを待って、レポートにまとめたものを

(4) 本文中の「f1」、「f2」に入れる、次の(i)～(iv)の組合せはどれか。fに関する解答群のうち、最も適切なものを選び。

- (i) 管理規程の内容に関する従業員への周知
- (ii) 情報共有や報告が包み隠さず行われるような組織文化の醸成
- (iii) 情報セキュリティにおけるクラッキング手法の教育
- (iv) マルウェア感染時の迅速な復旧対応方法の指導

fに関する解答群

	f1	f2
ア	(i)	(ii)
イ	(i)	(iii)
ウ	(i)	(iv)
エ	(ii)	(iii)
オ	(ii)	(iv)
カ	(iii)	(iv)

(5) 本文中の下線④について、E課長の提案に応える取組みはどれか。解答群のうち、最も適切なものを選び。

解答群

- ア 標的型攻撃メールについて、従業員のPCがマルウェア感染しないために注意すべき事項を標語として作成して掲示する。
- イ 標的型攻撃メールへの対策を題材とするDVD上映会を年に2回開催し、従業員の出席率を確認する。
- ウ 標的型攻撃メールを起因とするインシデントについて、他社で発生した事例を月に1回、イントラネット上の掲示板で紹介する。
- エ 模擬の標的型攻撃メールを従業員に期間を空けて何回か送付し、添付ファイル開封後の報告完了率、報告完了までに要した時間などの変化を調査する。

標的型攻撃メールを用いた攻撃の手口や、情報セキュリティインシデント管理規程を遵守するための活動に関する応用力を問う問題です。標的型攻撃メールなどの攻撃手法に関する知識があると解答が容易になります。大部分の問いは、問題文中に記載されている記述を参考にすることで正解を特定できます。問2以降も同様ですが、問題文の内容を適切に読み込むことが重要です。

設問1 (1) 標的型攻撃メールとウイルスメールの知識が重要です。ただし、「標的」や「ウイルス」といった語句から、その特徴を推測することでも解答できます。単語を解答する形式の問いは、問題文中の用語から解答の単語を推定するテクニックが有効です。

(2) (1)と同様に、「ソーシャル」エンジニアリングという語句が重要です。

(3) 図1のG君が受信したメールの内容から攻撃者の手口を読み解けます。

(4) 図1のG君が受信したメールの内容を確認することで、同メールの特徴を確認します。

設問2 (1) 図3の事項と、G君の初期対応を比較することで問題点が判明します。

(2) 図3の情報セキュリティリーダに要求されている適切な報告及び対応方法がポイントです。

(3) 図3の従業員に要求されている適切な報告及び対応方法を確認します。

(4) 図2の上司の対応や、管理規程を社員に伝える方法に問題があります。

(5) E課長の「実際に攻撃を受けた場合にも…… 定量的に測定し評価」するという指示を満たせるものが適切です。

設問1 標的型攻撃メール

(1)

空欄a, b

標的型攻撃メールは、「標的」という語句から推測できるように、標的になり得る団体や個人を選別し、攻撃対象を絞り込んでからマルウェアを送付しています。すなわち、特定の組織または個人を攻撃の対象として、マルウェアを送り付けるために用いられるメールが、標的型攻撃メールに該当します。

標的型攻撃メールには、受信者が添付ファイルを開いてしまうように、攻撃対象者の業務に関連した内容を表題や文面に盛り込むなどの仕掛けが施されています。また、送信元メールアドレスを攻撃対象者の上司や知人などに詐称して、攻撃対象者の疑いを低減する仕掛けも施されています。

従来のウイルスメールは、「ウイルス」という語句から推測できるように、感染した人から別の人に感染して、次々と被害を拡散させることを目的としています。このとき、標的型攻撃メールのように特定の組織や個人だけを対象にすると、別の人に感染しにくくなるので被害が拡散されず、目的を達成できません。

よって、被害を拡散させるために、不特定多数の組織や個人を対象にします。できるだけ多くの組織または個人をマルウェアに感染させることを目的として、誰でもそのメールや添付ファイルに関心を持つような

表題または文面にすることが多いです。

以上から、空欄aには **キ** (特定)、空欄bには **ク** (不特定多数) が入ります。

(2)

空欄c

メールの差出人を公的機関などに詐称したり、メールの件名や内容を受信者の業務に関連したものに偽装したりすることは、次の特徴をもちます。

① ハッキングやソフトウェアの脆弱性への攻撃など、技術的な方法を用いてはいない

② 公的機関が国民から信頼されていることを悪用して、差出人を公的機関などに詐称することで、攻撃対象者の疑いを低減しようとする

③ 受信者の仕事上の人間関係や業務内容を悪用して、②と同様に攻撃対象者の疑いを低減しようとする

②や③の特徴では、公的機関の信頼性、人間関係、及び業務内容といった社会的 (social) な事項を悪用して、攻撃対象者を騙そうとしています。このような攻撃のことを、ソーシャルエンジニアリングといいます。

ソーシャルエンジニアリングは、不注意や誤解・勘違いなどの、人間の心理的な盲点を突くことで、パスワードや機密情報などを知らうとする攻撃です。空欄cには **ウ** が入ります。

ア AES (Advanced Encryption Standard) は、共通鍵暗号方式の一種です。

- イ** ゼロデイ攻撃とは、新種のウイルスなど、対策が公表されていないマルウェアによって行われる攻撃のことです。
- エ** トロイの木馬とは、データの破壊などの不正な機能を組み込んだプログラムを攻撃対象のユーザに送付するなどの方法で、利用者のPCに当該プログラムをインストールさせ、知らないうちに不正な機能を実行させる攻撃手法のことです。
- オ** ヒヤリハットとは、実際には重大な事故にはならなかったものの、一つ間違えば重大な事故になる可能性があった軽度な事故、または事故を誘発しうろ見間違いやミスのことです。
- カ** ブルートフォース攻撃（総当り攻撃）は、考えられる全ての種類のパスワードまたは暗号化鍵を総当りで作成して、それをもって不正なログインや暗号解読を試みる方式のことです。

(3), (4)

図1のG君が受信したメールの内容を参照すると、次のことが分かります。

- (A) 本文末尾の署名にはF@x-sha.co.jpというメールアドレスが記載されているが、差出人のメールアドレスはF@zz-freemail.co.jpとなっており、両者は異なっている。本日にX社のF氏が送信したメールであれば、差出人メールアドレスはF@x-sha.co.jpのようなX社のドメイン名（太字部分）が含まれるアドレスとなる。
- (B) 「[至急]」といった、早急にメールや添付ファイルを参照することを促す語句が表題に含まれている。また、「添付ファイルの質問内容をご確認の上、本日15時までに回答をいただけないでしょうか」といった、添付ファイルをすぐに開かせようとする語句が本文に含まれている。これらは、いずれも添付ファイルを開かせて、受信者のPCをマルウェアに感染させようとするためのものである。
- (C) 「弊社では、今回、貴社から提案していただいた製品について、導入する方向で……」といった記述がある。このような記述により、X社との取引を成功させようとG君（攻撃対象者）に思わせ、添付ファイルを開かせようとしている。
- (D) 添付されているファイルの拡張子が“exe”（実行形式ファイル）である。

また、図2のG君へのヒアリング結果で「F氏と直接会ったことはなかったが、10日前から、製品の問合せが3回あり、メールでやり取りしていた」と説明されており、G君のもとにF氏を名乗るメールが何回か届いています。このようにして、何回かメールのやり取り

をすることで、G君はF氏が実在しており、本人から正式な問合せを受けていると考えています。標的型攻撃メールでは、いきなりマルウェア付きの攻撃用メールを送りつけるのではなく、関係者を装った問合せなどのメールを最初に何回かやり取りして、攻撃対象者の疑いを低減してから攻撃用メールを送ることがあります。

下線①について、今回の攻撃者が使った手口に該当するのは、ア（上の(B)と(C)に該当）とエです。(3)の正解はア、エです。図1の本文には、Y社の従業員しか知りえない情報は記載されていないので、イは今回の攻撃者が使った手口ではありません。図1の本文にはURLのリンクをクリックするような指示や誘導の語句はないので、ウも今回の攻撃者が使った手口ではありません。

(4)の(i)～(iii)について考えます。差出人のメールアドレスは「F@zz-freemail.co.jp」であり、Y社の社内メールアドレスではありません(iは不適切)。上の(A)で説明したとおり、差出人のメールアドレスと署名のメールアドレスが異なります(iiは適切)。同(D)で説明したとおり、実行形式ファイルが添付されています(iiiは適切)。以上から、(4)はカの組合せが正解です。

設問2 セキュリティ意識向上

(1)

Y社の管理規程の第2章では、インシデントまたはその疑いがある事象を発見した従業員が行わなければならないこととして、次の事項が示されています。

- (I)「インシデントを発見した際には、速やかに情報セキュリティリーダーに報告し、その指示に従うこと」
- (II)「インシデントであるかどうか判断がつかない疑わしい事象も、自己判断せず同様に報告すること」
- (III)「従業員は、各自の判断で復旧対応や解決を試みるのではなく、必ず情報セキュリティリーダーの指示又は勧告に従うこと」

図2から、添付ファイルを開いたときに見慣れないウィンドウが表示されたりするなど、不審な事象を発見したにもかかわらず、G君は速やかに情報セキュリティリーダーに報告しておらず、(I)に違反しています。また、G君は「ウイルス対策ソフトが動作し、パターンファイルが最新になっていることを確認できたのでマルウェア感染はあり得ないだろうと」考えています。(II)では、インシデントであるかどうか判断がつかない疑わしい事象も、自己判断せず情報セキュリティリーダーに報告しなければならないとしています

が、G君は自己判断でマルウェアに感染していないと考えており、この事項に違反しています。

以上から、(iii)と(iv)が今回の初動対応における問題点です。**カ**の組合せが適切です。

なお、(i)は今回の初動対応における問題点ではありません。(Ⅲ)から、インシデント発見時において、従業員は各自の判断で復旧対応をしなければならないので、再インストールなどを行ってははいけません。G君が再インストールなどの復旧対応をしなかったのは適切な対応です。X社との最近の取引記録を確認するといったことはY社の管理規程に示されていないので、(ii)のようなことをしなくても問題はありません。

(2)

空欄d

(Ⅰ)で「インシデントを発見した際には、速やかに情報セキュリティリーダーに報告し、その指示に従うこと」と決められています。また、(Ⅱ)で「インシデントであるかどうか判断がつかない疑わしい事象も、自己判断せず同様に報告すること」とあることから、疑わしい事象を発見したときも、(Ⅰ)と同様に速やかに情報セキュリティリーダーに報告する義務があります。空欄dには「速やか」(**エ**)が入ります。ア～ウのようにすると、インシデントかどうかの判断、原因の調査または再発防止策を実施するので時間がかかり、速やかに報告できなくなります。

(3)

空欄e

(Ⅱ)で「インシデントであるかどうか判断がつかない疑わしい事象も、自己判断せず同様に報告すること」とあることから、報告に当たっては判断に迷う事象であっても自己判断せずに、必ず情報セキュリティリーダーに報告するのが適切です。空欄eには**イ**が入ります。

(4)

空欄f

図2から、次のような理由で、G君はマルウェア感染と確信できるまで報告をしていなかったとわかります。

以前に他の部のH君が、顧客から貸与されたUSBメモリをPCに接続してマルウェア感染が起きたことを上司に報告した際に、上司から大変厳しく叱責されたH君本人から聞いていたので、マルウェア感染と確信できない限りは、報告したくないと思っていた

インシデントを報告することで上司などから叱責

される状況では、従業員がインシデントやそれと疑わしい事象の報告を抑えるようになり、管理規程で決めている「速やかに報告すること」というルールが守られなくなります。このルールを従業員が遵守し、インシデントの発生が早期に報告されるようにするためには、(ii)の「情報共有や報告が包み隠さず行われるような組織文化の醸成」が必要になります。

図2から、G君は管理規程について「新入社員研修の際に一度見たことがある程度で、重要な規程とは思っていなかった」と考えています。管理規程の内容やその重要性が周知されていなかったため、インシデント発生の際にG君は管理規程を重要視せず、その結果、報告が遅れています。規程が遵守されるようにするためには、(ⅰ)のように、管理規程の内容などを従業員に対して十分に周知する必要があります。

以上から、**ア**の組合せが適切です。

(5)

下線④では、「実際に攻撃を受けた場合にも一人一人が適切に対応できるかを定量的に測定し評価できる」ようにしています。**ア**～**エ**がこの記述に該当するかどうかを考えます。

ア 標語を掲示しているだけで、実際に攻撃を受けたときに従業員がどのように対応するかを確認していないので、適切ではありません。

イ DVD上映会を年2回開催して出席率を確認しているだけで、実際に攻撃を受けたときに、従業員がDVDの内容のとおりに対応できたかを確認していないので、適切ではありません。

ウ 実際に攻撃を受けたときに従業員がどのように対応するかを確認していないので、適切ではありません。

エ 実際に攻撃を受けたときの従業員の対応を確認しています。また、添付ファイル開封後の報告完了率や、報告完了までに要した時間といった、定量的な特性を測定しています。この取組みはE課長の提案に応えられるものです。

以上から、**エ**が正解です。

解答

- | | | | |
|------------|------------------|------------|------------------|
| 設問1 | (1) a : キ | 設問2 | (1) カ |
| | b : ク | | (2) d : エ |
| | (2) c : ウ | | (3) e : イ |
| | (3) ア, エ | | (4) f : ア |
| | (4) カ | | (5) エ |

問2

業務委託におけるアクセス制御に関する次の記述を読んで、設問1、2に答えよ。

A社は従業員数200名の通信販売業者である。一般消費者向けに生活雑貨、ギフト商品などの販売を手掛けており、商品の種類ごとに販売課が編成されている。

〔Z販売課の業務〕

現在、Z販売課は、商品Zについて顧客から電子メール又はファックスによる注文及び問合せを受け、その対応を行っている。商品Zの販売に関わる要員（以下、商品Z関連要員という）は、販売責任者であるZ販売課N課長、及びその管理下に5名の担当者、並びに業務委託先の管理者であるB社運用課L課長、及びその管理下に8名の担当者の、計15名で構成されている。商品Z関連要員の業務を図1に示す。

1. 受注管理業務

顧客から届く注文を確認し、受注手続を行う。受注管理システム（以下、Jシステムという）を利用する。本業務は、A社のZ販売課の要員が担当する。

(1) 入力

担当者は、届いた注文（変更、キャンセルを含む）の内容を確認し、不備があれば顧客に問い合わせる。不備がなければその情報をJシステムに入力し、販売責任者に承認を依頼する。

(2) 承認

販売責任者は、注文の内容とJシステムへの入力結果を突き合わせて確認し、問題がなければ承認する。問題があれば差し戻す。

2. 問合せ対応業務

顧客からの問合せに対応する。問合せ管理システム（以下、Tシステムという）を利用する。本業務は、業務委託先であるB社の運用課の要員が担当する。

(1) 入力

担当者は、顧客から届いた問合せの内容を確認し、回答案をTシステムに入力して、管理者に承認を依頼する。

(2) 承認

管理者は、回答案を確認し、問題がなければ承認する。これによってTシステムから顧客に回答が返信される。問題があればコメントを付記して差し戻す。

補足：Jシステム及びTシステムはA社の情報システム部が運用している。

図1 商品Z関連要員の業務（概要）

B社は、自社内にA社からの受託業務専用のオペレーションルームをもち、そこからA社のTシステムにアクセスしている。B社は、A社からの受託業務に必要な

設備及び管理体制を整えており、A社が定める情報セキュリティ要件を満たしている。

〔Jシステム及びTシステムの操作権限〕

Z販売課では、Jシステム及びTシステムについて、次の利用方針を定めている。

〔方針1〕 1人の利用者に、一つの利用者IDを登録する。

〔方針2〕 一つの利用者IDは、1人の利用者だけが利用する。

〔方針3〕 ある利用者が入力した情報は、別の利用者が承認する。

〔方針4〕 販売責任者は、Z販売課の全業務の情報を閲覧できる。

Jシステム及びTシステムでは、業務上必要な操作権限を利用者に与えるためにシステム上の役割（以下、ロールという）を定義する機能が実装されている。ロールには、業務上必要な操作権限の組合せが付与される。利用者IDにロールを設定することによって、利用者の操作権限が決まる。一つの利用者IDにはロールを一つだけ設定する。システム利用部署の長は、所属する利用者の利用者IDに対するロール設定を

情報システム部に依頼する。情報システム部が受けた依頼はシステムに登録され、翌営業日の朝5時に自動的にシステムに反映される。

Jシステム及びTシステムにおいて、商品Z関連要員の利用者IDに設定されているロールの種類とその操作権限を表1に示す。

表1 ロールの種類とその操作権限

ロール ロールに付与されている 操作権限	Jシステム			Tシステム		
	閲覧	入力	承認	閲覧	入力	承認
A 社販売責任者	○		○	○		
A 社販売担当者	○	○		○		
B 社管理者				○		○
B 社 Tシステム担当者				○	○	

注記 ○は、操作権限が付与されていることを示す。

例えば、N課長の利用者IDには“A社販売責任者”というロールを設定して、Jシステムの閲覧及び承認並びにTシステムの閲覧の権限をもたせている。

〔受注管理業務の委託〕

Z販売課では、受注管理業務を担当するA社の従業員の作業量が受注増によって増えていることから、この業務の入力作業をB社に対して追加で委託することにした。追加の業務委託で必要となるJシステムの操作権限の見直しを、A社の販売課全体の情報セキュリティリーダを務める販売管理課のM主任が支援することになった。

M主任は、受注管理業務におけるA社とB社の役割分担について、Z販売課のN課長からヒアリングした内容を次のとおり整理した。

〔要求1〕 B社が入力した場合は、A社が承認する。

〔要求2〕 A社の担当者が入力した場合は、現状どおりにA社の販売責任者が承認する。

これに基づきM主任が作成した新しい操作権限案を表2に示す。

表2 新しい操作権限案

ロール ロールに付与される 操作権限	Jシステム			Tシステム		
	閲覧	入力	承認	閲覧	入力	承認
A 社販売責任者	○		○	○		
A 社販売担当者	○	○		○		
B 社管理者	◎	◎		○		○
B 社 Tシステム担当者				○	○	
B 社 Jシステム担当者	◎	◎				

注記1 ○は、付与される操作権限のうち、表1と同じものを示す。

注記2 ◎は、付与される操作権限のうち、表1に比べて新しく追加したものを示す。

次は、この操作権限案についてのM主任とN課長との会話である。

M主任：N課長の要求に従ってロールとその操作権限を見直してみました。

N課長：確かに、要求どおりだ。ただ、販売責任者は私だけなので業務が停滞することが心配だ。B社で入

力した情報はA社の担当者が承認すればよいので、“A社販売担当者”ロールに承認権限を追加できないだろうか。

M主任：承認権限を追加すると、①Jシステムで利用方針に違反してしまいます。

N課長：“A社販売担当者”ロールに承認権限を追加し、その上で、利用方針にも合うようにしたい。例えば a ことはできるだろうか。

M主任：それならば、利用方針は順守できそうです。ただ、システムの改修が必要ですね。また、②[要求2]を満たせません。別の案ですが、 b ようにシステム改修するのはどうでしょう。

N課長：確かに、それなら[要求2]も満たせる。早速、その方針で情報システム部にシステム改修の相談をしてくれないか。

M主任：承知しました。確認ですが、N課長は、出張などで承認手続きができなくなるようなケースはありませんか。

N課長：今のところ問題ない。ただ、③来年度から毎年2、3回、2週間ほどの海外出張に出る予定なので、誰かに代行してもらう必要が出てくる。この対応も検討したい。それと、B社のL課長からの話だが、一日の中でも問合せ数が少ない時間に、問合せ対応業務の担当者の一部が受注管理業務を応援できる運用を希望していたよ。あらかじめ担当者を任命して教育しておくそうだ。

M主任：承知しました。すぐにB社に詳細を確認して④必要な操作権限を与える方法を検討します。

M主任は、B社の管理者及びA社の情報システム部と調整して、N課長とともにJシステムの改修案、運用案を取りまとめた。

〔B社担当者の追加及び変更〕

A社情報システム部では、社内データベースに格納された情報を閲覧するための情報閲覧システム（以下、Dシステムという）を提供している。Dシステムで商品Z関連要員に付与されている閲覧権限を表3に示す。

なお、利用者IDは、Jシステム及びTシステムと共通である。

表3 商品Z関連要員に付与されている閲覧権限（抜粋）

情報の オーナー部署	情報	…	A社Z販売課の 要員	B社運用課の 要員
販売管理課	在庫情報	…	○	○
販売管理課	販売計画・実績情報	…	○	
サービス企画課	お客様情報	…	○	○
商品企画課	商品カタログ情報	…	○	○
商品企画課	問合せ履歴情報	…	○	○

注記 ○は、閲覧権限が付与されていることを示す。

A社では、Dシステムの閲覧権限の付与について、次の手続を定めている。

- (1) 各情報のオーナー部署の長が、閲覧権限を付与する対象者を決める。
- (2) 情報システム部は、情報のオーナー部署の長の決定に従ってDシステムの閲覧権限を設定する。
- (3) 利用部署の希望によって閲覧権限を付与する場合は、利用部署の長が、その情報のオーナー部署の長に申請して承認を得る。申請を承認した情報のオーナー部署の長は、情報システム部に対して閲覧権限の付与を依頼する。
- (4) 利用部署が、業務委託先要員への閲覧権限付与を希望する場合は、 c 。

次は、B社の担当者の追加及び変更に関する、M主任とN課長との会話である。

M主任：新しく追加されるB社Jシステム担当者に付与する閲覧権限について相談があります。□d□のリスクを低減するために、表3に示すDシステムの閲覧権限を見直して、必要最小限にした方がよいと思います。

N課長：Jシステム担当者の作業は、届いた注文の確認と入力だ。商品カタログ情報とお客様情報の閲覧だけだな。

M主任：では、N課長から□e□に対して、閲覧権限の付与を申請していただけますか。

N課長：新しいB社担当者の名簿はできているかな。

M主任：はい。B社から情報を受領しました。Jシステム担当者は3名です。

N課長：Tシステム担当者に変更はないかな。

M主任：あります。⑤来月中に1人が退任し1人が新規に着任すると聞きました。

引継ぎを兼ねて、おおよそ1週間は2人とも在籍してTシステムとDシステムを利用して業務を行う予定です。必要な権限を正しくシステムに登録するために、B社に担当者変更がある場合、原則2週間前に□f□から情報提供してもらうよう業務委託契約で定めています。後ほど、⑥正式に情報を受領します。

N課長：分かった。今回、業務委託の対象システムも人員も増えるので、改めて情報漏えい対策に力を入れていきたい。頼りにしているよ。

こうしてN課長とM主任は必要な準備を進め、新しい体制で業務を開始することができた。

設問1 [受注管理業務の委託]について、(1)～(6)に答えよ。

- (1) 本文中の下線①について、どの利用方針に違反するか。違反が考えられる利用方針だけを全て挙げた組合せを、解答群の中から選べ。

解答群

- | | | | | | |
|---|-------------|---|-------------|---|-------------|
| ア | [方針1] | イ | [方針1],[方針2] | ウ | [方針2] |
| エ | [方針2],[方針3] | オ | [方針3] | カ | [方針3],[方針4] |

- (2) 本文中の下線①について、この利用方針違反はどのリスクを高めると考えられるか。解答群のうち、最も適切なものを選べ。

解答群

- ア 正しく入力された注文が承認されず滞留してしまう。
- イ 正しく入力された注文の情報が窃取されてしまう。
- ウ 不正に入力された注文が差し戻されて滞留してしまう。
- エ 不正に入力された注文が承認されてしまう。

- (3) 本文中の□a□, □b□に入れる適切な字句を、解答群の中から選べ。

a, bに関する解答群

- ア “A社販売責任者”ロールを設定した利用者IDを二つに増やす
- イ “B社Jシステム担当者”ロール又は“B社管理者”ロールを使って入力された注文だけを承認できる権限を追加する
- ウ 自分が承認したい注文だけを検索できる機能を追加する
- エ 承認できる利用者IDを、入力者が指定する権限を追加する
- オ 他の利用者IDによって入力された注文だけを承認できる権限を追加する

- (4) 本文中の下線②について、なぜ□a□では「要求2」を満たせないのか。その理由を、解答群の中から選べ。ここで、□a□には正しい答えが入っているものとする。

解答群

- ア “A社販売責任者”ロールの利用者が、B社で入力された情報を承認できなくなるから。
- イ “A社販売責任者”ロールの利用者が、自分宛での承認依頼に気づくとは限らないから。
- ウ “A社販売担当者”ロールの利用者が複数人いるとき、1人が入力し、別の1人が承認することができるから。
- エ “B社管理者”ロールの利用者が承認権限をもっているから。

- (5) 本文中の下線③について、N課長が出張中に他の者が代行するための措置のうち、利用方針に合致するものを、解答群の中から選べ。

解答群

- ア “A社販売担当者”ロールを設定した利用者IDを一つ追加発行し、A社の担当者の1人が、代行者として利用する。
- イ A社の担当者の1人を代行者に任命し、“A社販売責任者”ロールの権限を追加で付与した新しいロールを作成して、代行者の利用者IDに設定する。
- ウ N課長が、出張の期間に限り、自分の利用者ID、パスワードを別の販売課の課長に貸す。
- エ N課長の上長に代行を依頼し、代行者の利用者IDをJシステム及びTシステムに登録して“A社販売責任者”ロールを設定する。

- (6) 本文中の下線④について、情報システム部に依頼して必要な操作権限を与える方法はどれか。解答群のうち、最も適切なものを選べ。ここで、応援に回すB社担当者をB社応援担当者という。

解答群

- ア “B社Jシステム担当者”ロールを設定した貸出し用の利用者IDを準備し、応援の都度、B社応援担当者にこの利用者IDを利用させる。
- イ “B社Tシステム担当者”ロールの権限と“B社Jシステム担当者”ロールの権限を併せ持つ新しいロールを定義し、B社応援担当者の利用者IDに設定しておく。
- ウ B社応援担当者の利用者IDに対して“B社管理者”のロールを設定しておく。
- エ 応援の都度、B社応援担当者の利用者IDに設定されたロールを“B社Jシステム担当者”に切り替えてもらう。

設問2 [B社担当者の追加及び変更]について、(1)～(4)に答えよ。

- (1) 本文中の□c□に入れる字句はどれか。解答群のうち、最も適切なものを選べ。

cに関する解答群

- ア 業務委託先の管理者が、利用部署の長に名簿を提出するとともに、情報のオーナー部署の長に申請する
- イ 業務委託先の従業員が、利用部署の長に申請し、利用部署の長が、情報のオーナー部署の長に申請する
- ウ 利用部署の長が、業務委託先から提出された申請書を情報のオーナー部署の長に転送する
- エ 利用部署の長が、業務委託先の管理者から提出された利用者の情報に基づき、情報のオーナー部署の長に申請する

(2) 本文中の□d～□fに入れる適切な字句を、解答群の中から選べ。

dに関する解答群

- ア 内部不正 イ 入力時のタイプミス ウ 病欠

e, fに関する解答群

- ア B社の管理者 イ 情報システム部 ウ 情報のオーナー部署の長

(3) 本文中の下線⑤について、対応するために必要な利用者ID管理の手続はどれか。解答群のうち、最も適切なものを選べ。

解答群

- ア 新任者がすぐに業務を開始できるよう、あらかじめ新任者用の利用者IDの登録を情報システム部に依頼しておく。退任者の利用者IDは削除しなくても支障はないのでそのまましておく。
イ 退任者が本当に業務を離れたことを確認してから、退任者の利用者IDを新任者用に割り当てるよう、情報システム部に依頼する。
ウ 引継ぎ開始に当たり、新任者の利用者IDを発行し、引継ぎ期間後、直ちに退任者の利用者IDを無効化するよう、情報システム部に依頼する。
エ 引継ぎ開始に当たり、直ちに退任者の利用者IDを無効化すると同時に、新任者の利用者IDを発行するよう、情報システム部に依頼する。

(4) 本文中の下線⑥について、今回の担当者変更のために受領する情報としては不要なものを、解答群の中から選べ。

解答群

- ア 新任者の閲覧希望情報 イ 新任者の着任予定日
ウ 退任者の退任予定日 エ 退任者の利用者ID

問2 攻略のカギ

アクセス権限の設定や、利用者IDの適切な利用方法に関する問題です。大部分の問いは問題文中の記述をヒントとして解答を特定できます。内部統制における作業者と承認者の分離の知識があると問題を理解しやすくなります。

設問1 (1) 入力権限と承認権限が同じロールで実行可能になることがポイントです。
(2) 作業者と承認者の分離ができなくなります。
(3) 承認権限を追加し、かつ作業者と承認者の分離を実現する必要があります。
(4) 承認権限を追加すると、A社販売責任者以外が承認を実行できるようになることが重要です。
(5) 各解答群の措置を「方針1」～「方針4」の内容と比較し、合致するかどうかを検討します。
(6) 利用者に利用者IDを割り振るルールや、利用者IDに設定するロールの切り替えの仕様を参照することで、不適切な解答群を特定できます。

設問2 (1) 手続(1)から、閲覧権限を付与する対象者を決定できる者を特定します。
(2) 空欄dのリスク低減のためのM主任の意見が重要です。
(3) 引継ぎ中の退任予定者や新任者の在籍期間及び業務の実行方法から想定できます。
(4) (3)と同様です。

設問の解説に入る前に【内部統制】について解説します。

【内部統制】

内部統制とは、組織が目的を達成するために、従業員などを適切に管理して自社の業務を適正に遂行しているかどうかを、合理的な方法で確認するための体制を構築・運用する仕組み、及びその仕組みにおいて行われる各種の作業のことです。

内部統制において内部不正を検知または防止するためには、ある従業員または部門が行った作業の内容を、別の従業員または部門に検証させ、正当性を確認させる措置が必要です。この措置のことを承認といいます。内部不正を検知・防止するために、作業者と承認者を分離することが有効です。作業者と承認者が同じ状況では、作業者の行った不正を検知する者がいないので、不正が意図的に隠ぺいされる可能性が高くなります。

設問1 委託業者の操作権限

(1)

方針3は、【内部統制】の項で説明した作業者と承認者の分離を目的としています。ある利用者が入力した情報を同じ利用者が承認できる状況では、不正な注文情報が入力されたとき、同じ利用者によって承認されてしまいます。

【受注管理業務の委託】でN課長が提案したように「A社販売担当者」ロールに承認権限を追加すると、「A社販売担当者」ロールがJシステムへの入力権限と承認権限の両方をもちます(図A)。

「A社販売担当者」ロールを設定された利用者は、Jシステムに入力した不正な注文を自分で承認できるようになります。この状況は、利用方針のうちの[方針3]に違反します。なお、N課長の提案では、1人の利用者

に複数の利用者IDを登録したり、一つの利用者IDを複数人の利用者で共用したり、販売責任者の閲覧権限を取り除いたりしていないので、[方針1]、[方針2]、[方針4]には違反しません。**オ**の組合せが正解です。

(2)

N課長が提案したように「A社販売担当者」ロールに承認権限を追加すると、不正な注文が承認されてしまうリスクが高まります。**エ**が正解です。N課長の提案では、A社販売責任者の承認権限を削除していません。よって、N課長は通常どおり承認を実行できます。**ア**、**ウ**は不適切です。また、表1、表2では各システムを利用しない者に対しては、そのシステムの閲覧権限を与えていないので、正しく入力された注文の情報は窃取されません。**イ**は不適切です。

(3)

空欄a

【受注管理業務の委託】でN課長が主張しているように、「A社販売担当者」ロールに承認権限を追加し、その上で、利用方針にも合うようにするためには、[方針3]に違反しないようにする必要があります。「A社販売担当者」ロールを設定された利用者が、Jシステムに入力した不正な注文を自分で承認できる状況では、[方針3]に違反します。しかし、あるA社販売担当者がシステムに入力した注文を、自分では承認できないようにして、別のA社販売担当者だけが承認できるようにすると、方針3が遵守されます。すなわち、「他の利用者IDによって入力された注文だけを承認できる権限を追加」するのが適切です。空欄aには**オ**が入ります。

空欄b

「A社販売担当者」ロールに対して、他の利用者IDによって入力された注文だけを承認できる権限を追加す

表2 新しい操作権限案

ロール \ ロールに付与される 操作権限	Jシステム			Tシステム		
	閲覧	入力	承認	閲覧	入力	承認
A社販売責任者	○		○	○		
A社販売担当者	○	○	○	○		
B社管理者	◎	◎		○		○
B社Tシステム担当者				○	○	
B社Jシステム担当者	◎	◎				

注記1 ○は、付与される操作権限のうち、表1と同じものを示す。

注記2 ◎は、付与される操作権限のうち、表1に比べて新しく追加したものを示す。

A社販売担当者が、Jシステムへの入力と承認の両方をもつことになる

図A

ると、あるA社販売担当者の注文入力を、別のA社販売担当者が承認できるので、[要求2]（A社の担当者が入力した場合は、現状どおりにA社の販売責任者が承認する）を満たせなくなります。N課長は「B社で入力した情報はA社の担当者が承認すればよい」としているので、B社管理者またはB社Jシステム担当者が入力した注文情報だけを承認できる権限を、A社販売担当者にもたせることが有効です。このようにすると、A社販売担当者は他のA社販売担当者が入力した注文情報を承認できなくなり、A社販売責任者だけが承認できるので、[要求2]を満たせます。また、B社で入力した情報はA社の担当者が承認できるようになり、N課長の負担が減るので業務が停滞なくなります。

以上から、空欄bには **イ**（「B社Jシステム担当者」ロール又は「B社管理者」ロールを使って入力された注文だけを承認できる権限を追加する）が入ります。

(4)

(3) 空欄bの解説で説明したとおり、空欄aのように「A社販売担当者」ロールに対して、他の利用者IDによって入力された注文だけを承認できる権限を追加すると、あるA社販売担当者の注文入力を、他のA社販売担当者が承認できるので、[要求2]を満たせなくなります。これに該当するのは **ウ** の記述です。**ウ** が正解です。

ア “A社販売責任者” ロールには承認権限があるので、B社で入力された情報を承認できます。[要求2]には違反しません。不適切な理由です。

イ 販売責任者が、自分宛での承認依頼があったことに気付かなかったとしても、承認作業が滞るだけで、販売責任者以外の者は販売担当者の注文入力を承認できず、[要求2]に違反しません。不適切な理由です。

エ “B社管理者” ロールには承認権限はありません。不適切な理由です。

(5)

ア～エ について、利用方針に合致するかどうかを確認します。

ア A社の担当者は“A社販売担当者”ロールを設定した利用者IDをもっています。A社の担当者の1人に、“A社販売責任者”ロールを設定した利用者IDを追加発行して利用させると、1人の利用者が複数の利用者IDを利用することになり、[方針1]に違反します。よって、利用方針には合致しません。

イ その担当者はJシステムの入力権限と承認権限の両方をもつので、[方針3]に違反します。よって、

利用方針には合致しません。

ウ N課長が自分の利用者IDやパスワードを別の販売課の課長に貸すと、別の販売課の課長は複数の利用者IDを同時に利用することになり、[方針1]に違反します。よって、利用方針には合致しません。

エ N課長の上長に代行を依頼し、代行者の利用者IDを各システムに登録して“A社販売責任者”ロールを設定することで、N課長が出張している間は、上長がN課長の業務を代行できます。また、**〔Z販売課の業務〕**で「商品Zの販売に関わる要員」は、N課長とその管理下の5名の担当者、並びにB社のL課長とその管理下の8名の担当者だけと説明されています。よって、これらの計15名だけがJシステムやTシステムの利用者IDをもっており、N課長の上長は当該利用者IDをもっていません。N課長が出張している間だけ上長に代行者の利用者IDを利用させても、[方針1]には違反しません。よって、利用方針に合致しています。

以上から、**エ** が正解です。

(6)

ア～エ について、適切な方法かどうかを確認します。

ア N課長は「一日の中でも問合せ数が少ない時間に、問合せ対応業務の担当者の一部が受注管理業務を応援できる運用を希望していた」と説明しています。問合せ対応業務の担当者は業務を実施するために、“B社Tシステム担当者”ロールを設定した利用者IDの登録を受けています。この担当者に、“B社Jシステム担当者”ロールを設定した貸出し用の利用者IDを利用させると、1人の利用者が複数の利用者IDを利用することになり、[方針1]に違反します。この方法は不適切です。

イ “B社Tシステム担当者”ロールの権限（Tシステムへの閲覧権限と入力権限）と、“B社Jシステム担当者”ロールの権限（Jシステムへの閲覧権限と入力権限）を併せ持つ新しいロールを定義し、B社応援担当者の利用者IDに設定しています。このようにすると、B社応援担当者は問合せ数の多い時にはTシステムの閲覧・入力を行うことで問合せに対応し、問合せ数が少ない時にはJシステムの閲覧・入力を行うことで受注管理業務を応援できるようになります。また、B社応援担当者が複数の利用者IDを利用することはないので、利用方針に違反しません。適切な方法です。

ウ B社応援担当者の利用者IDに“B社管理者”のロールを設定すると、B社応援担当者にとって不要な

Tシステムの承認権限が与えられてしまいます。また、Jシステムの閲覧・入力に関する権限がないので、受注管理業務を応援できません。この方法は不適切です。

Ⅰ この問いは **Ⅰ** の方法が適切と考えがちです。この方法によって、B社応援担当者が応援をしている間だけ、「B社Jシステム担当者」の権限で作業ができるので、受注管理業務を応援できるようになります。利用者IDに設定されているロールを即座に切り替えられる場合は、この方法でも問題はありません。

しかし、**〔Jシステム及びTシステムの操作権限〕**の記述から、「システム利用部署の長は、所属する利用者の利用者IDに対するロール設定を情報システム部に依頼する」と、その依頼は**「翌営業日の朝5時に自動的にシステムに反映される」**という運用形態になっています。B社応援担当者が応援に入れるようになって、その利用者IDのロールの設定を即座に切り替えることはできず、翌営業日の朝5時にしないと切り替えられません。よって、B社応援担当者が応援に入れる時間帯になっても、すぐにロールの設定が切り替わらないので、この方法は不適切です。

以上から、**Ⅱ** が正解です。

設問2 操作権限の変更

(1), (2)

空欄c, e

〔B社担当者の追加及び変更〕の会話で、B社Jシステム担当者に付与する閲覧権限に関して、M主任が「N課長から **〔e〕** に対して、閲覧権限の付与を申請していただけますか」と依頼しています。これに対してN課長は「新しいB社担当者の名簿はできているかな」と確認し、M主任が「B社から情報を受領しました」と言っています。これらの会話内容から、利用部署（Z販売課）が業務委託先要員（B社Jシステム担当者）への閲覧権限付与を希望する場合は、次のようにしています。

「B社（業務委託先）からZ販売課（利用部署）が閲覧権限付与希望者の情報を受領し、それを基にしてZ販売課（利用部署）の長（N課長）から、空欄eの者に対して閲覧権限の付与を申請する」

空欄cの前に空欄eの者について考えます。**〔B社担当者の追加及び変更〕**の手続(1)から、閲覧権限を付与する対象者を決められるのは、各情報のオーナー部署の長だけです。閲覧権限の付与の承認を得るには、そ

の対象者を決定できる者、すなわち情報のオーナー部署の長に申請しなければなりません。そのため、(3)の手続では、利用部署の長が情報のオーナー部署の長に申請して、閲覧権限の付与の承認を得ています。(4)の手続でも同様に行っていると考えられます。利用部署が業務委託先要員への閲覧権限付与を希望する場合に、N課長（利用部署の長）が閲覧権限の付与を申請する対象として適切なのは、「情報のオーナー部署の長」（空欄e = **〔f〕**）です。

利用部署（Z販売課）が業務委託先要員（B社Jシステム担当者）への閲覧権限付与を希望する場合は、次のようにするとわかります。

「B社（業務委託先）からZ販売課（利用部署）が閲覧権限付与希望者の情報を受領し、それを基にしてZ販売課（利用部署）の長（N課長）から、情報のオーナー部署の長に閲覧権限の付与を申請する」

(1)のcに関する解答群の中でこの記述に該当するのは **Ⅰ** です。

空欄d

〔B社担当者の追加及び変更〕の会話中でM主任が「**〔d〕**のリスクを低減するために、表3に示すDシステムの閲覧権限を見直して、必要最小限にした方がよいと思います」と説明しています。システムの閲覧などに関する権限を必要最小限にすることで、システム中の不要な情報が利用者に見られることがなくなるので、内部不正によって機密情報が漏えいするリスクを低減できます。以上から、空欄dには「**内部不正**」（**ア**）が入ります。

空欄f

B社の担当者が変更されたことはB社内で発生する事象なので、B社からA社に対して報告しないと、A社がそれを把握することができません。B社に担当者変更がある場合、B社の管理者からA社に報告してもらう必要があります。空欄fには「B社の管理者」（**ア**）が入ります。

(3)

〔B社担当者の追加及び変更〕の会話中でM主任が「引継ぎを兼ねて、おおよそ1週間は2人とも在籍してTシステムとDシステムを利用して業務を行う予定」と説明しています。**Ⅰ** のようにすると、退任予定者の利用者IDが引継ぎ開始と同時に無効になり、退任予定者が各システムを利用できないので不適切です。M主任の説明のようにするには、引継ぎの開始時に新任者の利用者IDを発行し、退任予定者の利用者IDも残しておくこ

とで、引継ぎ期間中は退任予定者と新任者が同時にTシステムとDシステムを利用できるようにします。引継ぎ期間の終了後に、不要になった退任者の利用者IDを直ちに無効化します。よって、**ウ**の手続きが適切です。

アや**イ**のようにすると、退任者の利用者IDが引継ぎ期間終了後も残るので、退任者が当該利用者IDを悪用して、各システムに不正にアクセスして情報を盗むなどの不正が実行される危険性があります。

(4)

(3)の解説で説明したように、引継ぎが始まってから1週間ほどは、退任予定者と新任者が同時にTシステムとDシステムを利用して業務を行います。新任者が着任して引継ぎが開始された日から新任者の利用者IDが必要になるので、その日に新任者の利用者IDを発行する必要があります。よって、新任者の着任予定日が必要です。

引継ぎ期間が終了した時点で、退任者の利用者IDは不要になるので削除します。よって、退任者の退任予

定日も必要な情報です。また、削除対象となる退任者の利用者IDも今回の担当者変更のために必要です。

新任者は退任予定者の業務を引き継ぐので、退任予定者と同じ業務を行い、同じ情報を閲覧します。退任予定者の利用者IDに付与されている閲覧権限を参照することで、新任者が今後閲覧する情報を特定できます。新任者の閲覧希望情報をB社から受領する必要はありません。

以上から、**ア**が正解です。

解答

- | | | | |
|------------|------------------|------------|------------------|
| 設問1 | (1) オ | 設問2 | (1) c : エ |
| | (2) エ | | (2) d : ア |
| | (3) a : オ | | e : ウ |
| | b : イ | | f : ア |
| | (4) ウ | | (3) ウ |
| | (5) エ | | (4) ア |
| | (6) イ | | |

問3

情報セキュリティ自己点検に関する次の記述を読んで、設問1～4に答えよ。

R社は従業員数600名の投資コンサルティング会社である。R社では顧客の個人情報（以下、顧客情報という）を取り扱っていることから、情報セキュリティの維持に注力している。

R社ネットワークではURLフィルタリングを導入しており、フリーメールサービスを提供するWebサイトやソフトウェアのダウンロードサイトへのアクセスを禁止している。また、従業員にノートPC又はデスクトップPCのどちらかを貸与しており、それらのPC（以下、貸与PCという）ではUSBメモリを使用できないようにしている。貸与PCのうち、ノートPCだけが、リモート接続サービスによる社内ネットワークへの接続を許可されている。

海外営業部の部員は10人で、顧客は500人弱である。各部員は、担当顧客に、電子メールや電話を使って営業を行っている。海外営業部は他の営業部のオフィスとは離れた海外営業部専用のオフィスで業務を行っている。海外営業部で使用している顧客管理システム（以下、Cシステムという）は、海外営業部だけが使用している。Cシステムでは、アクセスログを3か月分保存している。海外営業部の部員は、出張がなく、全員がデスクトップPCだけを使っている。

海外営業部では、情報システム部が運用管理を行っているファイルサーバを使用しており、各部員は顧客情報を含むファイルを当該ファイルサーバに一時的に保存する場合がある。その場合は、ファイルのアクセス権を各部員が最小権限の原則に基づいて設定することになっている。R社では、顧客情報を保護するために、次の2点を各担当者が定期的に確認することになっている。

- ・ファイルサーバに不要な顧客情報を保存していないか。
- ・ファイルのアクセス権は適切に設定されているか。

R社では、情報セキュリティ推進部が実施する情報セキュリティ教育があり、海外営業部では、新たに配属された部員だけが受講することになっている。教育終了後には試験があるが、1回では合格できず、再度教育と試験を受ける部員が時々いる。この教育資料は、世の中で新たなセキュリティ脅威が発見される都度、情報セキュリティ推進部で更新している。

〔海外営業部の簡易チェック〕

海外営業部のW氏は2か月前に情報セキュリティリーダに任命された。

海外営業部では、自部門の情報セキュリティを確保するために、独自の取組みとして、四半期に1回、海外営業部で作成した情報セキュリティ簡易チェックリスト(表1)を全部員に配布し、記入(以下、簡易チェックという)させている。表1のチェックリストは、5年前に作成されたものである。

表1 海外営業部の情報セキュリティ簡易チェックリスト

No.	チェック項目	OK/NG
ファイルサーバの顧客情報について		
1	業務上の必要がある人だけにアクセス権を付与している。 (全従業員にアクセス権が付与されている状態は不可)	
2	不要になった顧客情報は削除している。(3か月超の保存は不可)	
3	顧客情報は必要な属性だけ保存している。 (省略)	
9	離席時にはPCの画面をロックしている。	

注記 チェック項目のとおりの場合はOK、チェック項目とは異なる場合はNGを記入する。

W氏が全部員にこのチェックリストを記入してもらったところ、全部員が全てのチェック項目にOKを記入して報告してきた。W氏は、念のため、数人に実施状況を確認したが、いずれも確かに報告のとおりであった。チェックリストは作成から5年も経過しており、情報セキュリティ事故のニュースを最近よく目にするようになったことから、W氏は、表2のチェック項目の追加を部長に提案した。

表2 W氏が作成した情報セキュリティ事故簡易チェックリスト追加項目案

No.	チェック項目	OK/NG
パスワードについて		
10	他人から容易に見えるところにパスワードを書いていない。	
電子メールの利用について		
11	不審な電子メールの添付ファイルを開いていない。	
情報セキュリティ事故への対応について		
12	情報セキュリティ事故が発生したときの連絡先を知っている。	
オフィスの情報セキュリティについて		
13	帰宅時は顧客情報を含む書類を施錠保管している。	

表2を見た部長は、①“部員がOKと記入してきたとしても、その結果が正しいか客観的に判断できないチェック項目がある”として、W氏に再検討するよう指示した。W氏は、次回の簡易チェックに向けて、チェック項目を見直すことにした。

〔監査部による情報セキュリティ監査〕

R社監査部は、1年に1回、CSA(Control Self Assessment：統制自己評価)方式による情報セキュリティ監査を実施している。CSAとは、監査部が被監査部門を直接評価するのではなく、被監査部門が、自部門の活動を評価することを指す。R社監査部では、被監査部門にCSAの実施を依頼し、その結果を活用して監査を実施している。

R社では、5年前、監査の方式を決定するに当たり、②監査部が各部門を直接監査する方式とCSA方式の利点、欠点を比較評価した。その結果、R社にとってはCSA方式の方がメリットが大きいと判断し、CSA方式を採用した。

R社の監査実施の手順を図1に示す。

1. 監査部が各部門に CSA シートを配布し、CSA の実施と結果の提出を依頼する。
2. 各部門は、CSA シートを用いて CSA を実施する。
3. 監査部が各部門から提出された CSA 結果を検証し、不明な点は当該部門に確認する。
4. “NG” の評価項目がある場合、及び改善が必要と監査部が判断した場合は、当該部門に改善計画の策定と提出を依頼する。

(改善が必要になった場合は次を行う。)

5. 改善が必要な部門は、改善計画を監査部に提出する。
6. 監査部は、提出された改善計画が適切か確認する。
7. 当該部門は、改善計画に基づき改善を実施する。
8. 改善後、当該部門は監査部に改善結果を報告する。
9. 監査部は改善された状況を確認し、適切であれば改善完了とする。

図1 R社の監査実施の手順

〔CSAの実施〕

海外営業部にも監査部からCSAを実施するよう依頼があり、W氏が海外営業部の評価を行うことになった。W氏は、監査部から送付されてきたCSAシートに従って、職場の状況を観察したり、部員にヒアリングしたりして評価を行った。評価結果を表3に示す。CSAシートの評価結果は次のルールに従って記入する。

- ・評価項目どおりに実施している場合：“OK”
- ・評価項目どおりに実施していないが、代替コントロールによって、“OK”の場合と同程度にリスクが低減されていると考える場合：“(OK)”(代替コントロールを具体的に評価根拠欄に記入する。)
- ・評価項目どおりに実施しておらず、かつ、代替コントロールによって評価項目に関するリスクが抑えられているわけではないと考える場合：“NG”
- ・評価項目に関するリスクがそもそも存在しない場合：“NA”

表3 CSAシート(海外営業部の評価結果)(抜粋)

No.	評価項目	評価結果	評価根拠
4	新たな脅威について全員が教育を受けている。		a
10	貸与 PC には会社が許可したソフトウェアだけがインストールされている。	OK	全部員に口頭で確認した。
11	リモート接続のためのパスワードを 90 日ごとに変更している。		b
19	ファイルサーバ上の顧客情報のアクセス権は最小権限の原則に基づいて設定されている。		c
25	業務用アプリケーションの利用者 ID の登録・変更・削除をルールどおり実施している。	OK	承認済みの利用者 ID 登録申請書を証跡として添付。
26	d	(OK)	少人数の専用オフィスであり、常に誰かが在席しているので、部外者が従業員に気付かれずに入ることは難しい。また、最終退出者はオフィスの出入口を施錠している。
29	業務用アプリケーションの利用者 ID 棚卸をルールどおり 3 か月に一度実施している。	OK	利用者 ID 棚卸記録を証跡として添付。

W氏が、CSA結果を監査部に提出したところ、監査部から電話があり、評価結果について質問を受けた。

最初の質問は、表3のNo.26の評価根拠欄についてであった。W氏は、記載内容が事実であることを説明したところ、それであれば監査部としての評価結果も“(OK)”にするとされた。

次の質問は、No.29の証跡として提出した利用者ID棚卸記録に、棚卸の際に不要と判断された利用者IDが5個あることについてであった。W氏が部内で事実を確認すると、いずれも棚卸の1か月以上前から、部員の退職又は異動で不要になっていた。これについてはW氏も改善が必要であると考え、③改善計画を策定して監査部に提出したところ、適切であるとの連絡があった。

〔新たな指摘についての改善計画〕

CSAの評価結果及びその後の事実確認に基づき、監査部から新たな指摘を受けた。それは、“Cシステムにおいて、利用者は自分の担当外の顧客情報に対してもアクセスが可能であり、最小権限の原則が守られておらず、社外への顧客情報の漏えいを防止できるようになっていない”というものであった。そこで、部長とW氏は改善計画について検討を行った。次は部長とW氏の会話である。

部長：新たな指摘に対応するために、が必要だね。

W氏：はい、そのために全部員に担当顧客を確認しますので、2週間ほど時間を下さい。

部長：分かった。その間のリスクを低減するために、を実施しておくというのはどうだろう。

W氏：はい、分かりました。他にも、万が一顧客情報の漏えいが発生してしまったときのことを考えると、も有効だと思います。

部長：それも実施しよう。他に、前から気になっていたのだが、部員が顧客情報を不適切に変更しないように、顧客情報の追加・修正・削除の権限についても考える必要があるね。

W氏：はどうでしょう。

部長：それでは業務が回らなくなるのではないかな。が、効率が良いのではないだろうか。

W氏：そうですね。しかし、ベンダに開発をお願いするので、半年は掛かります。対策が有効になるまで、負担は増えますが、を行うのはどうでしょうか。

部長：そうだな。ちょっと大変だが実施しよう。今までの話をまとめて監査部に報告しておいてくれ。

W氏：分かりました。

W氏が改善計画を監査部に提出したところ、監査部から、“内容に問題がないので、計画に基づいて監査を実施するように”と連絡がきた。

その後、W氏が再検討した簡易チェックリストは部長に承認され、使われることになった。また、情報セキュリティ監査結果に基づく改善も計画どおりに完了し、海外営業部の情報セキュリティレベルは大きく改善された。

設問1 本文中の下線①について、部長が再検討を指示したチェック項目はどれか。解答群のうち、最も適切なものを選べ。

解答群

☐ ア 10

☐ イ 11

☐ ウ 12

☐ エ 13

設問2 本文中の下線②について、CSA方式の利点を二つ、解答群の中から選べ。

解答群

☐ ア 関連法規への準拠性が担保できる。

☐ イ 業務内容の十分な理解に基づいて評価できる。

☐ ウ 証跡を提出する必要がない。

☐ エ 独立的な立場から公正に評価できる。

☐ オ 評価実施者に対する意識付けや教育として役立つ。

設問3 【CSAの実施】について、(1)～(5)に答えよ。

- (1) 表3中の□a□に入れる字句はどれか。解答群のうち、最も適切なものを選ぶ。

aに関する解答群

	評価結果	評価根拠
ア	OK	情報セキュリティ推進部の資料を使った教育が行われている。
イ	NG	新たなセキュリティ脅威に関する教育を受けていない部員がいる。
ウ	NG	教育後の試験を1回で合格できない部員がいた。
エ	NA	新たなセキュリティ脅威に対抗することはできないので教育は不要である。

- (2) 表3中の□b□に入れる字句はどれか。解答群のうち、最も適切なものを選ぶ。

bに関する解答群

	評価結果	評価根拠
ア	OK	会社のルールで決められている。
イ	NG	誰も1回も変更をしていない。
ウ	NG	リモート接続ができない。
エ	NA	部内ではリモート接続は誰も行わない。

- (3) 表3中の□c□に入れる字句はどれか。解答群のうち、最も適切なものを選ぶ。

cに関する解答群

	評価結果	評価根拠
ア	OK	簡易チェックで、アクセス権の付与状況について確認している。
イ	OK	簡易チェックで、アクセス権を適切に設定するルールが存在することを確認している。
ウ	NA	顧客情報をファイルサーバに保存することは禁止されている。
エ	NA	ファイルサーバは情報システム部が運用しているので、情報システム部が回答する。

- (4) 表3中の□d□に入れる字句はどれか。解答群のうち、最も適切なものを選ぶ。

dに関する解答群

- ア** PCを社外に持ち出す場合はあらかじめ許可を得ている。
- イ** 入退室管理システムが導入され、関係者だけ入室可能になっている。
- ウ** 必要な場所に監視カメラを設置して毎日24時間撮影し、映像を記録している。記録した映像の保存期間を1か月以上に行っている。
- エ** 部内で情報セキュリティ啓発活動をしている。

- (5) 本文中の下線③について、策定する改善計画の概要を、解答群の中から選べ。

解答群

- ア** Cシステムから出力された利用者IDの一覧を使って、3か月ごとに利用者IDの棚卸を実施する。
- イ** 部員の退職又は異動の際は、利用者IDの削除申請とCシステムからの削除を速やかに行うよう、管理職一人一人に周知する。
- ウ** 利用者ID棚卸の実施者を上位の役職者に変更する。
- エ** 利用者ID登録時、申請されたアクセス権限が業務上必要か確認する。

設問4 〔新たな指摘についての改善計画〕について、(1)、(2)に答えよ。

- (1) 本文中の **e1** ～ **e3** に入れる、次の〔対策1〕～〔対策3〕の組合せはどれか、eに関する解答群のうち、最も適切なものを選び。

〔対策1〕 アクセスログの保管期間を3年間に変更するという対策

〔対策2〕 営業部員に対し、担当顧客以外の顧客情報を閲覧しないように周知し、^{けん}牽制するという対策

〔対策3〕 担当する顧客の顧客情報だけにアクセスできるようにアクセス権を設定するという対策

eに関する解答群

	e1	e2	e3
ア	〔対策1〕	〔対策2〕	〔対策3〕
イ	〔対策1〕	〔対策3〕	〔対策2〕
ウ	〔対策2〕	〔対策1〕	〔対策3〕
エ	〔対策2〕	〔対策3〕	〔対策1〕
オ	〔対策3〕	〔対策1〕	〔対策2〕
カ	〔対策3〕	〔対策2〕	〔対策1〕

- (2) 本文中の **f1** ～ **f3** に入れる、次の〔対策4〕～〔対策6〕の組合せはどれか、fに関する解答群のうち、最も適切なものを選び。

〔対策4〕 顧客情報の追加・修正・削除の権限は管理職だけに付与するという対策

〔対策5〕 部員による顧客情報の追加・修正・削除は、システムのワークフロー機能を使って上長が承認することによって、データベースに反映されるようにするという対策

〔対策6〕 顧客情報の追加・修正・削除のログを上長が定期的に確認するという対策

fに関する解答群

	f1	f2	f3
ア	〔対策4〕	〔対策5〕	〔対策6〕
イ	〔対策4〕	〔対策6〕	〔対策5〕
ウ	〔対策5〕	〔対策4〕	〔対策6〕
エ	〔対策5〕	〔対策6〕	〔対策4〕
オ	〔対策6〕	〔対策4〕	〔対策5〕
カ	〔対策6〕	〔対策5〕	〔対策4〕

CSA (Control Self-Assessment, 統制自己評価) に関して, 自組織の情報セキュリティ上の問題点を適切に把握し, 問題を解決するための対応策 (コントロール) を想定する能力を確認する問題です。大部分の問いは問題文中の記述をヒントとして解答を特定できます。CSAの知識があると解答しやすくなりますが, 問題文中のCSAの説明から特徴を推測することも可能です。

設問 1 表2のNo.10～13のチェック項目について, その結果を証明するための内容が問題文に記載されているかどうか重要です。

設問 2 問題文中のCSAの説明から, そのメリットやデメリットを推測します。また, 表3の中で証拠を提出していることもポイントです。

設問 3 (1) 海外営業部の情報セキュリティ教育方法から, 新たな脅威に関する教育を全ての部員に実施できているかどうかを検討します。
(2) 海外営業部の部員が使用している機材の特徴から, リスクの存否を検証します。
(3) ファイルサーバ上に一時的に保存しているファイルに対する海外営業部のアクセス権付与方法が重要です。
(4) No.26の評価根拠の記述と, 海外営業部の入退室管理方法とを比較することで, 評価結果として適切な記述を想定します。
(5) 部員の退職・異動時に, その部員が使用していた利用者IDを「削除」するための措置が適切です。解答群中で利用者IDの削除を確実に実施しているものを特定します。

設問 4 (1) 各空欄の前後の記述と, [対策1] ～ [対策3] の内容とをそれぞれ比較し, 各空欄にあてはまる適切な内容を特定します。
(2) (1)と同様に, 各空欄の前後の記述を確認し, 各空欄にあてはまる適切な対策を特定します。

設問の解説に入る前に【CSA】について解説します。

【CSA】

CSAは内部監査の手法の一つです。監査部または外部の監査人が監査を行うのではなく, 業務内容に熟知している被監査部門の管理者及び担当者が, 自身の活動を評価することが特徴です。CSA方式の監査には, 監査部または外部の監査人が行う従来型の監査と比較して次のメリットやデメリットがあります。

【メリット】

- 業務内容に理解が深い管理者や担当者が監査を行うので, 従来型の監査と比べて現場の問題点を把握しやすい
- 監査を行う過程で, 業務に関する意識の向上や知識の習得を図ることができ, 教育効果が高い

【デメリット】

- 被監査部門が通常の業務と並行して監査を行うため, 負担が増える
- 監査の評価結果に独立性がなく, 客観性に乏しい

上記のメリットやデメリットは, 問題文中の「監査部が被監査部門を直接評価するのではなく, 被監査部門が, 自部門の活動を評価することを指す」という説

明からも推測できます。監査部が監査を行う方式では, 監査部が主体となるので被監査部門は受け身的になります。また, 外部の部署である監査部が行う監査では, 業務の実態を把握しづらくなります。CSA方式では, 被監査部門が自部門の活動を能動的に評価して問題点を把握していくので, 監査の進捗に応じて業務の意識向上などを図ることが可能です。

設問 1 チェックの客観性

表2のNo.10～13のチェック項目について, 結果を客観的に判断するための証拠となるものがあるかを確認します。

No.10: このチェック項目にOKと回答した部員のPCや机の周辺を視察して, パスワードを書いていないことを確認することで, 結果を客観的に判断できます。

No.11: このチェック項目にOKと回答した部員が, 実際には不審な電子メールの添付ファイルを開いていたとしても, その操作履歴はサーバのログなどに残りません。よって, 添付ファイルを開いていたことを証明できません。また, 添付ファイルを開かなかった場合も操作履歴は残らないので同様となります。証拠と

なるものがないので、結果を客観的に判断できません。
No.12：このチェック項目にOKと回答した部員にインタビューして、連絡先を本当に知っているかを確認することで、結果を客観的に判断できます。

No.13：このチェック項目にOKと回答した部員が帰宅した後、顧客情報を含む書類が施錠保管されているかを確認することで、結果を客観的に判断できます。

以上から、No.11のチェック項目は結果を客観的に判断できません。**イ**が正解です。

設問2 CSA方式の利点

解答群 **ア～オ** が、CSA方式の利点になるかどうかを確認します。

ア 関連法規への準拠性を担保するには、その法規で定められた適切な手順に従って、業務や監査を進める必要があります。本問のCSA方式の説明では、関連法規への準拠に関して特に説明がないので、関連法規への準拠性を担保することはできません。CSA方式の利点ではありません。

イ CSA方式では、被監査部門が自部門の活動を評価します。被監査部門は、常日頃から実施していて、その内容を熟知している自部門の業務を監査するので、十分な理解に基づいて業務内容を評価できます。これに対して、監査部が各部門を直接監査する方式では、被監査部門の業務内容を監査部が十分に理解しないまま監査が進められ、業務内容が適切に評価されない可能性があります。CSA方式の利点です。

ウ CSA方式と監査部が各部門を直接監査する方式の両方とも、業務内容を客観的に評価するためには、証拠（業務を適切に行ったことを証明するための書類やログなど）を用意する必要があります。表3のNo.25などで「承認済みの利用者ID登録申請書を証拠として添付」していることから、CSA方式では証拠を提出する必要があるとわかります。CSA方式の利点ではありません。

エ CSA方式では、被監査部門が自部門の活動を評価するので、独立した立場からの公正な評価にはなりません。これに対して、監査部が各部門を直接監査する方式では、独立的な立場から公正に評価できます。CSA方式の利点ではありません。

オ CSA方式では、被監査部門の部員が自部門の活動を評価します。部員が自部門の業務内容を評価する過程で、情報セキュリティを維持することに関する意識の向上や知識の習得を図ることができま

す。以上から、**イ**、**オ**の二つが正解です。

設問3 CSAシート

(1)

空欄a

海外営業部では、情報セキュリティ推進部が実施する情報セキュリティ教育を「新たに配属された部員だけが受講する」ことになっています。以前から海外営業部に所属している部員は、今後情報セキュリティ教育を受講する機会がありません。よって、以前から海外営業部に所属している部員は新たな脅威に関する教育を受けられません。空欄aの評価結果は“NG”です。評価根拠は“新たなセキュリティ脅威に関する教育を受けていない部員がいる”です。**イ**が正解です。なお、**ウ**は不適切です。教育後の試験を1回で合格できなくても、その部員が教育を受けたことには変わりがないので、「新たな脅威について教育を受けている」という評価項目の評価結果をNGにする根拠にはなりません。

(2)

空欄b

この問いは、海外営業部でパスワードを変更することに関する説明が問題文中にないので、**イ**と誤答する可能性があります。

R社では、ノートPCだけがリモート接続サービスによる社内ネットワークへの接続を許可されています。海外営業部の部員は全員がデスクトップPCだけを使っているため、リモート接続サービスを使用できません。したがって、リモート接続のためのパスワードを変更しないことによるリスクがもともと存在しません。**エ**（評価結果＝“NA”，評価根拠＝“部内ではリモート接続は誰も行わない”）が正解です。

(3)

空欄c

海外営業部では、ファイルサーバ上に一時的に保存しているファイルについて、そのアクセス権を最小権限の原則に基づいて設定することになっています。また、四半期に1回、表1のチェックリストを用いて、業務上の必要がある人だけにアクセス権を付与しているかをチェックしています。よって、空欄cの評価結果は“OK”です。評価根拠は“簡易チェックで、アクセス権の付与状況について確認している”となります。**ア**が正解です。

(4)

空欄d

表3のNo.26の評価根拠は「少人数の専用オフィスであり、常に誰かが在席しているので、部外者が従業員に気付かれずに入することは難しい。また、最終退出者はオフィスの出入り口を施錠している」です。この記述から、空欄dはオフィスへの入退室に関する評価項目です。これに該当するのは、イ、ウです。これらのうち、ウは「必要な場所に監視カメラを設置して毎日24時間撮影し、映像を記録している……」という、非常に厳重な入退室管理です。海外営業部ではこのような厳重な管理は行っていないので、空欄dをウと仮定すると、評価結果は「(OK)」ではなく「(NG)」になります。したがって、ウは不適切であり、イが適切です。海外営業部では入退室管理システムを導入していませんが、評価根拠に示す措置を行っているので、入退室管理システムの代わりとなる代替コントロールによって、関係者以外の者がオフィスに入ってくるというリスクを“OK”の場合と同程度に低減しています。イが正解です。

(5)

表3のNo.29について、棚卸の際に不要と判断された利用者IDが5個あることが監査部から指摘されています。部員の退職または異動で不要になった利用者IDを残しておく、それが悪用されてCシステム上の機密情報が不正に参照されたり、盗まれたりするリスクがあります。

海外営業部では、棚卸の1か月以上前の時点から、不要になった利用者IDがそのままになっています。この問題を改善するには、部員が退職したり異動したりしたとき、その部員が使用していた利用者IDを確実に削除します。そのために、利用者IDの削除申請やCシステムからの削除といった措置を、速やかに行うようにするのが適切です。削除措置を実行しているのはイだけなので、イが正解です。

なお、アの改善計画では3か月ごとに利用者IDの棚卸が行われます。棚卸の直後に部員の退職または異動が発生し、不要になった利用者IDが削除されないと、その時点から棚卸が約3か月間行われず、不要な利用者IDが次の棚卸の1か月以上前から残り続けます。この改善計画では監査部からの指摘に対応できません。また、カの改善計画では棚卸の実施者が上位の役職者に代わるだけで、不要な利用者IDを削除していません。エの改善計画では、利用者IDの登録時のアクセス権限が必要かを確認するだけで、不要な利用者IDを削除していません。

設問4 顧客情報の漏えい対策

(1)

空欄e

監査部からの新たな指摘は次のとおりです。

Cシステムにおいて、利用者は自分の担当外の顧客情報に対してもアクセスが可能であり、最小権限の原則が守られておらず、社外への顧客情報の漏えいを防止できるようになっていない

これに対応するには、Cシステムの利用者は自分の担当外の顧客情報に対してはアクセスできないようにする必要があります。そのために必要な対策は、[対策3]（担当する顧客の顧客情報だけにアクセスできるようにアクセス権を設定するという対策）です。空欄e1には“[対策3]”が入ります。

【新たな指摘についての改善計画】中の会話で、W氏は対策3を実施するために「2週間ほど時間を下さい」と言っており、[対策3]を実行するためには、ある程度の時間がかかります。その間に社外へ顧客情報が漏えいするリスクを低減するために、部長は空欄e2の対策を提案しています。空欄e2の対策として適切なのは[対策2]（営業部員に対し、担当顧客以外の顧客情報を閲覧しないように周知し、牽制するという対策）です。このような周知によって、営業部員が担当顧客以外の顧客情報にアクセスしないように牽制します。空欄e2には“[対策2]”が入ります。

上記の対策をとっても、万が一顧客情報の漏えいが発生してしまった場合は、顧客情報を漏えいさせた部員を特定して、業務規則に従って処分する必要があります。また、どの顧客の顧客情報が漏えいしたかを特定して、その顧客への謝罪などの対応も必要になります。この特定をするためには、Cシステムのアクセスログを参照して、漏えいした顧客情報やそれにアクセスした利用者IDを確認しなければなりません。現状では、Cシステムのアクセスログは3か月間しか保存されていません。顧客情報の漏えいが発生してから3か月以上経過してから漏えいが発覚した場合、利用者IDなどを特定できなくなります。よって、アクセスログの保管期間を長くして、顧客情報の漏えいが発覚するまでに経過した時間が長くても対応できるようにします。空欄e3に入る対策は“[対策1]”（アクセスログの保管期間を3年間に変更するという対策）です。

以上から、カの組合せが適切です。

(2)

空欄 f

【新たな指摘についての改善計画】中の会話で、部長が顧客情報の追加・修正・削除の権限について考えており、その直後に W 氏が空欄 f1 の対策を進めています。この対策に対して、部長は「それでは業務が回らなくなるのではないかな」と言っています。空欄 f1 の対策は、顧客情報の追加・修正・削除の権限に関する対策であり、かつ、この対策を実行すると業務に支障が出るとわかります。これに該当するのは【対策4】（顧客情報の追加・修正・削除の権限は管理職だけに付与するという対策）です。この対策によって、部員は顧客情報を不適切に変更できなくなります。しかし、海外営業部の顧客は約500人存在します。多数の顧客情報の追加・修正・削除に関する業務を管理職だけが担当すると、管理職本来の業務ができなくなる可能性があり、業務が回らなくなります。

よって、顧客情報の追加・修正・削除に関する業務を部員に担当させ、管理職は当該業務の内容を確認し、問題がなければ承認することが有効です。この措置により、管理職の負担はさほど増加しないので業務に支障は出ません。また、部員が顧客情報を不適切に変更

しようとしても、管理職が承認しないようにすることで変更を防止できます。空欄 f2 には“【対策5】”（部員による顧客情報の追加・修正・削除は、システムのワークフロー機能を使って上長が承認することによって、データベースに反映されるようにするという対策）が入ります。

【対策5】が有効になるまでの間に発生する、部員による顧客情報の不適切な変更に対しては、顧客情報の追加・修正・削除のログを上長が定期的に確認して、不適切な変更を発見して対応するのが有効です。空欄 f3 には“【対策6】”（顧客情報の追加・修正・削除のログを上長が定期的に確認するという対策）が入ります。

以上から、アの組合せが適切です。

解答

- | | | | |
|-----|----------|--------|----------|
| 設問1 | イ | (4) d: | イ |
| 設問2 | イ, オ | (5) | イ |
| 設問3 | (1) a: イ | 設問4 | (1) e: カ |
| | (2) b: エ | | (2) f: ア |
| | (3) c: ア | | |

第①回 模擬試験

情報セキュリティ マネジメント

- 午前 問題 172
(全 50 問 試験時間：1 時間 30 分)
- 午後 問題 202
(全 3 問 試験時間：1 時間 30 分)

本章で取り上げる問題文は、情報処理技術者の試験で過去に出題された問題の中から著者が精選して構成したものです。

第①回 模擬試験 午前 問題

☐ **問 1** JIS Q 27001 では、情報セキュリティは三つの特性を維持するものとして特徴付けられている。それらのうちの二つは機密性と完全性である。残りの一つはどれか。

- ☐ **ア** 安全性 ☐ **イ** 可用性 ☐ **ウ** 効率性 ☐ **エ** 保守性

☐ **問 2** 不正が発生する際には“不正のトライアングル”の3要素全てが存在すると考えられている。“不正のトライアングル”の構成要素の説明のうち、適切なものはどれか。

- ☐ **ア** “機会”とは、情報システムなどの技術や物理的な環境及び組織のルールなど、内部者による不正行為の実行を可能、又は容易にする環境の存在である。
☐ **イ** “情報と伝達”とは、必要な情報が識別、把握及び処理され、組織内外及び関係者相互に正しく伝えられるようにすることである。
☐ **ウ** “正当化”とは、ノルマによるプレッシャーなどのことである。
☐ **エ** “動機”とは、良心のかしゃくを乗り越える都合の良い解釈や他人への責任転嫁など、内部者が不正行為を自ら納得させるための自分勝手な理由付けである。

☐ **問 3** AESの暗号化方式を説明したものはどれか。

- ☐ **ア** 鍵長によって、段数が決まる。 ☐ **イ** 段数は、6回以内の範囲で選択できる。
☐ **ウ** データの暗号化、復号、暗号化の順に3回繰り返す。
☐ **エ** 同一の公開鍵を用いて暗号化を3回繰り返す。

☐ **問 4** 利用者認証に用いられるICカードの適切な運用はどれか。

- ☐ **ア** ICカードによって個々の利用者を識別できるので、管理負荷を軽減するために全利用者に共通なPINを設定する。
☐ **イ** ICカードの表面に刻印してある数字情報を組み合わせて、PINを設定する。
☐ **ウ** ICカード紛失時には、新たなICカードを発行し、PINを設定した後で、紛失したICカードの失効処理を行う。
☐ **エ** ICカードを配送する場合には、PINを同封せず、別経路で利用者に知らせる。

解説

問 1 情報セキュリティの3要素

JIS Q 27001 (ISO/IEC27001)などの情報セキュリティの規格によって示される「**情報セキュリティの3要素**」とは、「機密性」(不特定多数からデータにアクセスされないようにする)、「完全性」(データの内容を矛盾なく保つ)及

び「可用性」(必要なときにシステムやデータを利用できる)のことです。**イ**(可用性)が正解です。

問 2 不正のトライアングル

不正のトライアングルとは、犯罪学者のD.R. クレッシー氏が提唱した理論で、人が不正行為をする原因をまとめたものです。次の三つがそろったとき、不正行為が発生します。

機会(の認識)：「作業の実行者と承認者が同じ」など、不正行為を実行できるような客観的環境があることです。適切なアクセス権限が設定されておらず、機密情報を誰でも参照・コピーできるような環境も該当します。

動機：不正行為を実行しようとする主観的事情です。例えば多額の借金があり、返済に追われていることなどが該当します。また、厳しいノルマがあり、プレッシャーから業務内容を改ざんしようとする考えも動機の一つです。

正当化：不正行為を正当化しようとする主観的事情です。「他の人もやっている」、「自分は貧しいから他人から奪っても構わない」などの、都合のいい理由付けが該当します。

- **ア** 正解です。
- × **イ** “情報と伝達”は不正のトライアングルの要素ではありません。
- × **ウ** “正当化”ではなく、“動機”の説明です。
- × **エ** “動機”ではなく、“正当化”の説明です。

問 3 AES

AESは、NIST(米国商務省標準技術局)が制定した共通鍵暗号方式です。暗号化に使用する鍵(暗号化鍵)のビット長(鍵長)を、128ビット、192ビットまたは256ビットのうちのいずれかから選ぶことができます。暗号化対象のデータを切り出した各ブロックに対して、AESなどで利用される暗号化鍵を用いて暗号化を行う1回のステップを「**段**」と呼び、ステップを行う回数を**段数**と呼びます。AESでは、鍵長によって段数が決定されます。

- **ア** 正解です。
- × **イ** AESの段数は、10段、12段または14段のいずれかとなります。
- × **ウ** 暗号方式の一つである**3DES**(Triple DES)の説明です。
- × **エ** AESは公開鍵暗号方式ではないため、公開鍵を用いることはありません。

問 4 認証用ICカード

ICカードのみを認証時に使用する方式では、落としたICカードを拾われてしまうなどの理由で悪意の第三者が容易に認証を潜り抜けてしまう可能性があります。よって、認証時にはICカードの提示(または機器への挿入)後にユーザの暗証番号を入力させる方式にすることで、安全性が向上します。この暗証番号を**PIN**(Personal Identification Number)と呼びます。この方式をとる場合、ICカードを配送する際にPINを同封すると、ICカードを収めた封筒などを誤って別のユーザなどに届けてしまった場合に、ICカードとPINが同時に他人に知れ渡ってしまうため、問題があります。よって、**エ**のように、ICカードとは別ルートでPINを利用者に知らせるのが適切です。

- × **ア** 全利用者に共通なPINを設定するのでは、PINを使用する意味がありません。よって、誤りです。
- × **イ** ICカードの数字情報などからPINの内容が推測できる利用形態では、ICカードを拾った者がPINを推測してしまう危険性があります。よって、誤りです。
- × **ウ** 紛失時には、不正利用防止のため、紛失したICカードのアカウントを即座に失効させるのが適切です。
- **エ** 正解です。

○ 解答 ○

問 1 **イ**

問 2 **ア**

問 3 **ア**

問 4 **エ**



問 5

文書の内容を秘匿して送受信する場合の公開鍵暗号方式における鍵と暗号化アルゴリズムの取り扱いのうち、適切なものはどれか。

- ア 暗号化鍵と復号鍵は公開するが、暗号化アルゴリズムは秘密にしなければならない。
- イ 暗号化鍵は公開するが、復号鍵と暗号化アルゴリズムは秘密にしなければならない。
- ウ 暗号化鍵と暗号化アルゴリズムは公開するが、復号鍵は秘密にしなければならない。
- エ 復号鍵と暗号化アルゴリズムは公開するが、暗号化鍵は秘密にしなければならない。



問 6

送信者から電子メール本文とそのハッシュ値を受け取り、そのハッシュ値と、受信者が電子メール本文から求めたハッシュ値とを比較することで実現できることはどれか。ここで、受信者が送信者から受け取るハッシュ値は正しいものとする。

- ア 電子メールの送達の確認
- イ 電子メール本文の改ざんの有無の検出
- ウ 電子メール本文の盗聴の防止
- エ なりすましの防止



問 7

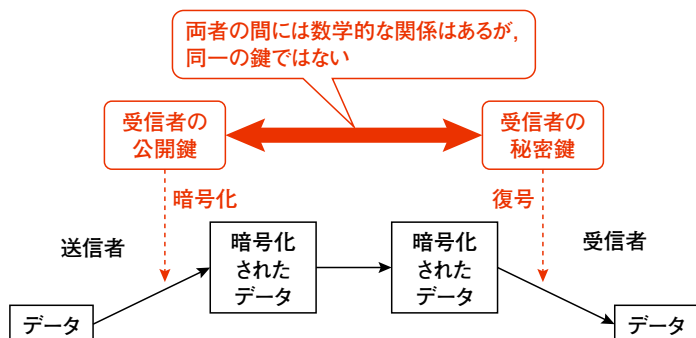
ディレクトリトラバーサル攻撃に該当するものはどれか。

- ア Webアプリケーションの入力データとしてデータベースへの命令文を構成するデータを入力し、想定外のSQL文を実行させる。
- イ Webサイトに利用者を誘導した上で、Webサイトの入力データ処理の欠陥を悪用し、利用者のブラウザで悪意のあるスクリプトを実行させる。
- ウ 管理者が意図していないパスでサーバ内のファイルを指定することによって、本来は許されないファイルを不正に閲覧する。
- エ セッションIDによってセッションが管理されるとき、ログイン中の利用者のセッションIDを不正に取得し、その利用者になりすましてサーバにアクセスする。

解説

問 5 公開鍵暗号方式

公開鍵暗号方式で暗号化や復号を行う場合、送信者は“受信者の公開鍵”（暗号化鍵）を用いて、データを暗号化して受信者に送信します。受信者は“受信者の秘密鍵”（復号鍵）を用いて、暗号化されたデータを復号します。



これらの鍵のうち、復号に用いる復号鍵(秘密鍵)は秘密にする必要がありますが、暗号化に用いる暗号化鍵は公開し、あらゆるユーザが使用できるようにしておく必要があります。正解はウです。

問 6 ハッシュ値

通信相手に送付するデータが、途中で改ざんされているかどうかを受信者が検出するために、ハッシュ関数を用いられます。

ハッシュ関数には、ハッシュ値を求めるデータの値がわずかでも変化すると、ハッシュ値の値が劇的に変化するという特徴があります。電子メール本文の内容が送信途中でわずかでも改ざんされると、送信者が最初に求めたハッシュ値と、受信者が受け取った電子メール本文から求めるハッシュ値が異なるので、ハッシュ値を比較することで改ざんを検出可能になります。

電子メールの送信者は、その本文のハッシュ値を求めて、本文に添付して受信者に送付します。電子メールの受信者は、送信者と同じハッシュ関数を用いて電子メール本文からハッシュ値を生成します。元のハッシュ値と生成したハッシュ値が一致すれば、そのデータは改ざんされていないことが確認できます。

- × ア 電子メールの送達を確認するのは、電子メールの受信者が送信者に返信することなどによって実現できます。ハッシュ値を電子メールに付加しても、電子メールがインターネット上で何らかの原因によって失われた場合には、受信者に電子メールが届かなくなるため、送達を確認できません。
- イ 正解です。
- × ウ 本問では電子メール本文が暗号化されていないため、本文の盗聴を防止することはできません。
- × エ なりすましを防止するためには、送信者のみが利用できるデータ(送信者の秘密鍵など)を用いて暗号化した情報を、電子メールに付加する必要があります。一般的なハッシュ関数は、ネットワーク上の全ての利用者が自由に利用できるため、ハッシュ関数を用いて電子メール本文から出力したハッシュ値を付加しても、なりすましを防止したり検出したりすることはできません。

問 7 ディレクトリトラバーサル攻撃

ディレクトリトラバーサル攻撃とは、Webサーバなどに存在しており、外部からのアクセスを想定していないディレクトリやファイルの名称を、外部から直接指定してアクセスすることで、本来は閲覧が許されないファイルを不正に閲覧する手法のことです。

大部分のブラウザのアドレス欄は、利用者が直接文字列を入力して、URLを指定することが可能です。悪意のある利用者はこれを悪用し、URLのファイル名やディレクトリ名を指定する箇所に、外部からのアクセスを想定していないサーバ上のディレクトリ名などを推測して直接入力し、機密性の高いファイルなどを不正に閲覧しようとすることができます。

- × ア データベース(サーバ)への命令文を構成するデータを入力して想定外のSQL文を構成しようとするのは、SQLインジェクションの説明です。
- × イ Webサイトの入力データ処理の欠陥を悪用し、利用者のブラウザ上で悪意のあるスクリプトを実行させるのは、XSS(クロスサイトスクリプティング)の説明です。
- ウ 正解です。
- × エ ログイン中の利用者のセッションIDを不正に取得し、その利用者になりすます行為は、セッションハイジャックです。

○ 解答 ○

問 5 ウ

問 6 イ

問 7 ウ



問 8 クロスサイトスクリプティングの手口はどれか。

- ア Webアプリケーションに用意された入力フィールドに、悪意のあるJavaScriptコードを含んだデータを入力する。
- イ インターネットなどのネットワークを通じてサーバに不正に侵入したり、データの改ざん・破壊を行ったりする。
- ウ 大量のデータをWebアプリケーションに送ることによって、用意されたバッファ領域をあふれさせる。
- エ パス名を推定することによって、本来は認証された後にしかアクセスできないページに直接ジャンプする。



問 9 DNSキャッシュポイズニングに分類される攻撃内容はどれか。

- ア DNSサーバのソフトウェアのバージョン情報を入手して、DNSサーバのセキュリティホールを特定する。
- イ PCが参照するDNSサーバに誤ったドメイン情報を注入して、偽装されたWebサーバにPCの利用者を誘導する。
- ウ 攻撃対象のサービスを妨害するために、攻撃者がDNSサーバを踏み台に利用して再帰的な問合せを大量に行う。
- エ 内部情報を入手するために、DNSサーバが保存するゾーン情報をまとめて転送させる。



問 10 バイオメトリクス認証には身体的特徴を抽出して認証する方式と行動的特徴を抽出して認証する方式がある。行動的特徴を用いているものはどれか。

- ア 血管の分岐点の分岐角度や分岐点間の長さから特徴を抽出して認証する。
- イ 署名するときの速度や筆圧から特徴を抽出して認証する。
- ウ どう孔から外側に向かって発生するカオス状のしわの特徴を抽出して認証する。
- エ 隆線によって形作られる紋様からマニューシャと呼ばれる特徴点を抽出して認証する。

解説

問 8 クロスサイトスクリプティング

ブラウザから掲示板などの動的なサイトにアクセスする際に、以下のようなURLが用いられることがあります。なお、以下のURLは架空のものです。

`http://*****.net/****.htm?data=123456`

“?data=…”は、当該サイトのCGI等に対してユーザが送信する情報を記載したものです。HTTPのGETリクエストを使用すると、URLの末尾にこのような形式でユーザからの送信情報が掲載される仕組みになっています。当該サイトのCGIは、このデータをもとに動的にWebページを生成したり、検索処理を行ったりする仕様となっています。

ここで、上の“?”以降に、正規のデータの代わりに悪意をもったスクリプトの文字列を記述したURLを作成して、他のWebページにリンクとして貼ると、そのリンクをクリックした場合に、CGIに正常なデータの代わりに不正なスクリプトが与えられ、当該サイト上で生成されたページをブラウザが開き、その結果ブラウザ上で悪意のスクリプトが実行

行されてしまう可能性があります。

クロスサイトスクリプティングとは、上記のような方法や、Webページの入力フィールドに悪意のあるJavaScriptコードを含んだデータを入力する方法などを用いて、悪意のスクリプトをユーザのブラウザに送り込み、標的サイトにアクセスしたユーザの個人情報をクッキーから盗み取るなどの手法を用いる攻撃方法です。

クロスサイトスクリプティングを防ぐには、入力されるデータの**サニタイジング**(データの文字列に含まれるスクリプトを無効化すること)などの措置が有効です。

○ **ア** 正解です。

× **イ** インターネットなどのネットワークを通じてサーバなどに不正に侵入し、データの改ざんや破壊を行うのは、クラッキング及び改ざん・破壊の手口の説明です。

× **ウ** 大量のデータをWebアプリケーションに送り、用意されたバッファ領域をあふれさせるのは、**バッファオーバーフロー攻撃**の説明です。

× **エ** 本来は認証された後にしかアクセスできないページに、パス名を推定することで直接ジャンプするのは、**パストラバース**の説明です。

問 9 DNS キャッシュポイズニング

DNS キャッシュポイズニングとは、DNSサーバに誤ったドメイン管理情報を送り込み、そのDNSサーバを参照してきたPCの利用者を、本来のWebサーバとは異なるWebサーバに誘導する攻撃手法のことです。この攻撃により、有名なWebサイトに偽装した不正なWebサイトに利用者を誘導して、個人情報を盗もうとするなどの手口が知られています。

× **ア** DNSサーバなどのソフトウェアのバージョン情報を入手し、当該サーバのセキュリティホールを特定する攻撃手法は、**バナーチェック**です。

○ **イ** 正解です。

× **ウ** DNSサーバなどを踏み台にして再帰的な問合せを大量に行い、攻撃対象のサービスを妨害する攻撃手法は、**DoS攻撃**です。

× **エ** DNSサーバの**ゾーン情報**とは、DNSサーバが管理するドメイン(組織)の名称や所在地、及び当該組織のネットワーク管理者のメールアドレスなどの情報のことです。DNSサーバのソフトウェアの設定を初期設定のままにしておくと、この情報を外部から問い合わせることが可能になり、自組織のゾーン情報が漏えいしてしまうことがあります。よって、ゾーン情報を「外向けのゾーン情報」と「内向けのゾーン情報」に分け、外部には「内向けのゾーン情報」を公開しないようにするのが、適切な運用方法です。なお、DNSサーバのゾーン情報を不正に入手しようとすることは、DNSキャッシュポイズニングとは関係のない記述です。

問 10 バイオメトリクス認証

バイオメトリクス認証には、指紋、虹彩、指の血管の形状などの身体的特徴を抽出して認証する方式と、筆跡、筆圧などの行動に関する各自の習性(癖)などの行動的特徴を抽出して認証する方式があります。**イ**は、「署名するときの速度や筆圧」など、各自の行動的特徴を抽出する方法の説明です。

アは指の血管、**ウ**は虹彩、**エ**は指紋の特徴を抽出する方法の説明です。これらはいずれも身体的特徴を抽出する方法の説明です。

○ 解答 ○

問 8 **ア**

問 9 **イ**

問 10 **イ**



問 11 情報システムのリスクマネジメント全体の説明として、最も適切なものはどれか。

- ア 事故や災害の発生を防止したり、それが万一発生した場合には損失を最小限にしたりする手段であり、回避、最適化、移転、保有などの手段がある。
- イ 情報システムの機能特性を損なう不安定要因やシステムに内在する脆弱性を識別して、企業活動に生じる損失を防止、軽減するとともに、合理的なコストでの対策を行う。
- ウ 情報システムの機能に障害が発生した際に、業務の中断や機密漏えいを、防止又は軽減する緊急時対策を行う。
- エ リスクを経済的な範囲で最小化するコントロールを設計するために必要な情報を提供する。



問 12 リスク対策をリスクコントロールとリスクファイナンスに分けた場合、リスクファイナンスに該当するものはどれか。

- ア システムが被害を受けた場合を想定して保険をかけた。
- イ システム被害につながるリスクの発生を抑える対策に資金を投入した。
- ウ システムを復旧するのに掛った費用を金融機関から借り入れた。
- エ リスクが顕在化した場合のシステム被害を小さくする対策に資金を投入した。



問 13 情報漏えいに関するリスク対応のうち、リスク回避に該当するものはどれか。

- ア 外部の者が侵入できないように、入退室をより厳重に管理する。
- イ 情報資産を外部のデータセンタに預託する。
- ウ 情報の重要性和対策費用を勘案し、あえて対策をとらない。
- エ データの安易な作成を禁止し、不要なデータを消去する。

解説

問11 リスクマネジメント

業務中に発生する偶発的または人為的な障害や事故(脅威)によって、情報システムや情報資産の脆弱性が突かれ、その結果システム上のデータやプログラムが破壊されたり、業務が長時間停止させられたりすることがあります。その結果、修復費用の発生や機会損失による利益の喪失などにより、多大な損失が発生することが往々にしてあります。

これらの「脅威が情報資産の脆弱性を利用して、情報資産への損失または損害を与える可能性」を、**リスク**と呼びます。

これらの、システムの脆弱性やそれに関するリスクを識別し、リスクによる損失の防止や軽減を目的として合理的なコストによる対策を行うことを、**リスクマネジメント**といいます。

× **ア** リスクマネジメント全体の記述ではありません。事故などの発生を防止したり、損失を最小限にしたりする方法には、リスク回避(リスクの発生確率を下げ、リスクに遭わないようにする)やリスク低減(リスクによる被害を減らす方策をとる)のほか、リスク保有(保険に加入するなどの方法で、リスクによる被害を補填できるようにし、自社でリスクを保有する)などがあります。

○ **イ** 正解です。

× **ウ** リスクマネジメント全体の記述ではありません。情報システムの障害発生時の緊急時の対策の計画のことを、**コンティンジェンシープラン(緊急時対応計画)**と呼びます。

- × **エ** リスクマネジメント全体の記述ではありません。リスクを経済的な範囲で最小化するための方法を、**リスクコントロール**といいます。

問12 リスクファイナンス

情報システム上の脅威、脆弱性、リスクとは次のようなものです。

脅威：情報システムに対して悪い影響を与える要因のこと

脆弱性：情報システムや情報資産に存在する、脅威が顕在化する確率のこと

リスク：脅威が情報資産の脆弱性につけこみ、情報資産に損失などを与える可能性のこと

なお、リスク評価によってリスクの大きさを判断した上で決める各種の対策として、リスクコントロールやリスクファイナンスがあります。

リスクコントロール：リスクが現実のものにならないようにするための、または現実化したリスクによってもたらされる被害を最小限にするための対策です。リスクコントロールには、リスク回避(リスクそのものをなくすこと、または発生確率を低下させること)、リスク集中(リスクをもつ情報資産を集中管理すること)、リスク分離(リスクをもつ情報資産を分離させ、全体のリスク発生確率などを低減させること)などがあります。

リスクファイナンス：リスクが発生することは不可避であると仮定し、リスクによる損失に備えてリスク対策の費用を事前に計上したり、積立金などを設けて損失を補填したり、保険に加入したりすることで、リスクが現実化したときに生じる損失金額を少なくするための対策です。リスクファイナンスには、リスク移転(保険に加入するなどの手段で資金面での対策を行い、リスク発生時の損失を他者に肩代わりさせること)やリスク保有(積立金などによって、損失を自社で負担すること)があります。

この説明に合致するのは解答群の **ア** の記述(システムが被害を受けた場合を想定して保険をかけた)のみです。他の解答群は、リスクの発生確率の軽減・回避や、システムの被害額の低減などを行っているため、リスクファイナンスではなく、リスクコントロールとなります。

問13 リスク回避

解答群の中で、**リスク回避**に相当するのは **エ** (データの安易な作成を禁止し、不要なデータを消去する) となります。不要なデータを消去することなどによってデータ自体をなくせば、データが漏えいする危険性そのものが消失するため、リスクそのものをなくすことになります。

- × **ア** 情報資産が保管されている重要な部屋などへの入退室をより厳重に管理することで、不正侵入などが行われる危険性が減るため、リスクの発生確率を減らすことになります。よって、**リスク低減**に相当します。
- × **イ** 情報資産を外部のデータセンタに預託することで、当該情報資産の管理を外部に任せることができます。また、当該情報資産に関するリスクの発生時には外部のデータセンタに損害賠償を請求することなどによって、リスク発生時の損失を他者に肩代わりさせることができます。よって、**リスク移転**に相当します。
- × **ウ** 発生確率が非常に低いリスクや、発生時の被害額が非常に少ない軽微なリスクに対して対策をとっても、対策費用の方が被害額よりも大きくなり、かえって損になることがあります。このような軽微なリスクに対しては、あえて対策をとらずに済ませることもあります。このように、発生時の被害額や対策費用などを勘案し、リスクへの対策をとらないことを、**リスク受容**といいます。

- **エ** 正解です。

○ 解答 ○

問11 **イ**

問12 **ア**

問13 **エ**



問 14 リスク分析に関する記述のうち、適切なものはどれか。

- ア** 考えられるすべてのリスクに対処することは時間と費用がかかりすぎるので、損失額と発生確率を予測し、リスクの大きさに従って優先順位を付けるべきである。
- イ** リスク分析によって評価されたリスクに対し、すべての対策が完了しないうちに、繰り返しリスク分析を実施することは避けるべきである。
- ウ** リスク分析は、将来の損失を防ぐことが目的であるから、過去の類似プロジェクトで蓄積されたデータを参照することは避けるべきである。
- エ** リスク分析は、リスクの発生によって被る実損失額を知ることが目的であり、その損失額に応じて対策の費用を決定すべきである。



問 15 CSIRTの説明として、適切なものはどれか。

- ア** IPアドレスの割当て方針の決定、DNSルートサーバの運用監視、DNS管理に関する調整などを世界規模で行う組織である。
- イ** インターネットに関する技術文書を作成し、標準化のための検討を行う組織である。
- ウ** 国レベルや企業・組織内に設置され、コンピュータセキュリティインシデントに関する報告を受け取り、調査し、対応活動を行う組織の総称である。
- エ** 情報技術を利用し、信教や政治的な目標を達成するという目的をもった人や組織の総称である。



問 16 基本評価基準、現状評価基準、環境評価基準の三つの基準でIT製品のセキュリティ脆弱性の深刻さを評価するものはどれか。

- ア** CVSS **イ** ISMS **ウ** PCI DSS **エ** PMS



問 17 情報システムへの脅威とセキュリティ対策の組合せのうち、適切なものはどれか。

	脅威	セキュリティ対策
ア	誤操作によるデータの論理的な破壊	ディスクアレイ
イ	地震と火災	コンピュータ内で複数の仮想化OSを利用したデータの二重化
ウ	伝送中のデータへの不正アクセス	HDLC手順のCRC
エ	メッセージの改ざん	公開鍵暗号方式を応用したデジタル署名

解説

問14 リスク分析

リスクには様々な種類が存在し、考えられる全てのリスクに対処するのは、時間的・費用的に無理となります。よって、各リスクの損失額や発生確率を予測し、リスクの大きさに従って優先順位をつけ、重大なリスクのみについて対処すべきです。

○ **ア** 正解です。

- × **イ** 社会状況の変化などによって、これまでは重大でなかったリスクが、重大なものに変化する可能性もあります。よって、リスクへの対策の途中であっても、繰り返しリスク分析を行うことが重要となります。
- × **ウ** 過去の類似プロジェクトで蓄積されたデータは、将来のプロジェクトのリスク分析に役立ちます。
- × **エ** リスク分析の際には、損失額だけではなく、リスクの発生確率なども考慮する必要があります。

問15 CSIRT

CSIRT (Computer Security Incident Response Team)は、インターネット上で各種の問題(特に、セキュリティに関する問題=セキュリティインシデント)が発生していないかを監視し、発生した問題の報告を受け取ってその原因を調査したり、対策を想定したりする組織です。CSIRTは国レベルまたは企業・組織内に設置されます。

- × **ア** **ICANN** (Internet Corporation for Assigned Names and Numbers)の説明です。
- × **イ** **IETF** (Internet Engineering Task Force)の説明です。
- **ウ** 正解です。
- × **エ** **ハックティヴィズム** (hacktivism)の説明です。

問16 脆弱性の評価基準

米国のインフラストラクチャ諮問委員会(NIAC)が2004年に原案を作成したシステムで、情報システムの脆弱性を汎用的な基準に基づいて評価するためのものに、**CVSS** (Common Vulnerability Scoring System, 共通脆弱性評価システム)があります。CVSSでは、基本評価基準(Base Metrics)、現状評価基準(Temporal Metrics)及び環境評価基準(Environmental Metrics)の三つを用いて、脆弱性を評価します。

- **ア** 正解です。
- × **イ** **ISMS** (Information Security Management System, 情報セキュリティマネジメントシステム)は、情報システム上に存在する情報資産のセキュリティ管理体制のことです。
- × **ウ** **PCI DSS** (Payment Card Industry Data Security Standard)は、クレジットカード情報などを保護することを目的として、VISAなどのクレジット会社が共同で策定した基準です。
- × **エ** **PMS** (Personal information protection Management Systems)は、個人情報マネジメントシステムです。

問17 脅威と対策

- × **ア** 誤操作によるデータの破壊に対しては、ディスクアレイは無効です。フールプルーフによって、システムの誤操作を防止するなどの措置が有効です。
- × **イ** データを二重化しても、二重化したデータが存在しているシステムが同一の建物内に存在している場合、地震などの災害でシステムが完全に破壊され、両方が同時に消滅してしまうことがあります。
- × **ウ** HDLCプロトコルのCRCは暗号化などの処理を行うものではなく、伝送誤りの検知を目的として付加されているものです。よって、伝送中のデータについてはCRCの有無にかかわらず不正アクセスによって盗聴されてしまうことになります。
- **エ** メッセージの改ざんについては、公開鍵暗号方式を応用した**デジタル署名**で対策を行います。デジタル署名において用いられている、メッセージに付加するハッシュ値の値を検証することにより、メッセージの改ざんを検知できるようになります。

○ 解答 ○

問14 **ア**

問15 **ウ**

問16 **ア**

問17 **エ**

問 18 情報漏えい対策に該当するものはどれか。

- ア 送信するデータにチェックサムを付加する。
- イ データが保存されるハードディスクをミラーリングする。
- ウ データのバックアップ媒体のコピーを遠隔地に保管する。
- エ ノート型PCのハードディスクの内容を暗号化する。

問 19 WAF (Web Application Firewall)を利用する目的はどれか。

- ア Webサーバ及びWebアプリケーションに起因する脆弱性^{ぜい}への攻撃を遮断する。
- イ Webサーバ内でワームの侵入を検知し、ワームの自動駆除を行う。
- ウ Webサーバのコンテンツ開発の結合テスト時にWebアプリケーションの脆弱性や不整合を検知する。
- エ Webサーバのセキュリティホールを発見し、OSのセキュリティパッチを適用する。

問 20 ウイルス対策ソフトのパターンマッチング方式を説明したものはどれか。

- ア 感染前のファイルと感染後のファイルを比較し、ファイルに変更が加わったかどうかを調べてウイルスを検出する。
- イ 既知ウイルスのシグネチャと比較して、ウイルスを検出する。
- ウ システム内でのウイルスに起因する異常現象を監視することによって、ウイルスを検出する。
- エ ファイルのチェックサムと照合して、ウイルスを検出する。

問 21 ネットワーク監視型侵入検知ツール(NIDS)の導入目的はどれか。

- ア 管理下のサイトへの不正侵入の試みを記録し、管理者に通知する。
- イ 攻撃が防御できないときの損害の大きさを判定する。
- ウ サイト上のファイルやシステム上の資源への不正アクセスであるかどうかを判定する。
- エ 時間をおいた攻撃の関連性とトラフィックを解析する。

解説

問18 情報漏えい対策

社内の情報がひそかに持ち出されたり、社外に持ち出して使用していたノートPCが盗まれたりすることで、情報の漏えいが発生します。これらの事象によって情報が外部に漏えいするのを防止するには、権限をもつ人だけに社内の情報にアクセスさせることや、ノートPCのハードディスクの内容を暗号化することなどが有効です。

- × ア チェックサムをつけることで、送信中にデータのビットに誤りが発生したときに、それを検知できます。この記述はデータの完全性が損なわれることへの対策です。
- × イ ハードディスクのミラーリングにより、ハードディスクが1台故障しても残りのハードディスクが稼働していればデータを利用することができます。この記述はデータの可用性が損なわれることへの対策です。
- × ウ イと同様に、データの可用性が損なわれることへの対策です。

○ **エ** 正解です。

問19 WAF

WAF (Web Application Firewall)とは、WebサーバとWebブラウザとの間でやり取りされるデータの内容を監視し、WebサーバプログラムやWebアプリケーションプログラムの脆弱性を突くことで行われる攻撃(SQLインジェクションなど)を防御するために用いられる、特別なファイアウォールのことです。

WAFは、WebサーバとWebブラウザの間に位置し、Webブラウザから送信されてきたパケットの内容を検査することによって、攻撃用のパケットを特定・遮断することができます。

○ **ア** 正解です。

× **イ** WAFでは、ワームの自動駆除などを行うことはできません。ワームの自動駆除などは、アンチウイルスソフトウェアが行う処理となります。

× **ウ** WAFでは、Webサーバのコンテンツ開発時に脆弱性などを検知することはできません。Webサーバが稼働を開始し、Webブラウザとの間で実際にパケットをやり取りする際に、WAFが機能することになります。

× **エ** WAFでは、Webサーバのセキュリティホールを発見することや、セキュリティパッチを適用することはできません。これらの処理は、Webサーバの管理者が行うべきことです。

問20 パターンマッチング方式

コンピュータウイルス対策ソフトの「**パターンマッチング**」方式とは、既に存在が知られている各種のウイルスに存在するウイルス特有の特別なプログラムコードなどを「シグネチャコード」としてパターンファイルなどに登録しておき、スキャンしたファイルにそのシグネチャコードが含まれていれば、ファイルにウイルスが感染している可能性が高いと判断する方法のことです。

× **ア** **コンペア法**の説明です。

○ **イ** 正解です。

× **ウ** **ビヘイビア法**の説明です。

× **エ** **チェックサム法**／**インテグリティチェック法**の説明です。

問21 NIDS

外部(インターネットなど)からの攻撃を検知するためのシステムを「**IDS** (Intrusion Detection System : 侵入検知システム)」といいます。IDSには「ネットワーク型IDS (NIDS)」と「ホスト型IDS (HIDS)」の2つがあります。

● **NIDS**: ネットワーク中のファイアウォール等の重要な機器内に設定され、ネットワーク上を流れているパケットの内容を解析し、攻撃に使用されるタイプのパケットや、挙動の疑わしいパケットを判別し警告を発する。

● **HIDS**: ネットワーク上の個々のコンピュータやサーバなどにインストールされ、自機器に到達したパケットの内容を解析し、攻撃に使用されるタイプのパケットを解析し警告する。

○ **ア** 正解です。

× **イ** NIDSは、損害の大きさの判定などを判定するために導入すべきものではありません。NIDSには、損害の大きさの判定などを行う機能はありません。

× **ウ** ファイルやシステム上の資源への不正アクセスを判定するためには、HIDSを導入するのが適しています。

× **エ** NIDSには、時間をおいた攻撃の関連性などを解析する機能はありません。

○ 解答 ○

問18 **エ**

問19 **ア**

問20 **イ**

問21 **ア**



問22 SQLインジェクション攻撃を防ぐ方法はどれか。

- ア 入力値から、上位ディレクトリを指定する文字(../)を取り除く。
- イ 入力値から、データベースへの問合せや操作において特別な意味をもつ文字を解釈されないよう保護する。
- ウ 入力値にHTMLタグが含まれていたなら、解釈、実行できないほかの文字列に置き換える。
- エ 入力値の全体の長さが制限を超えていたときは受け付けない。

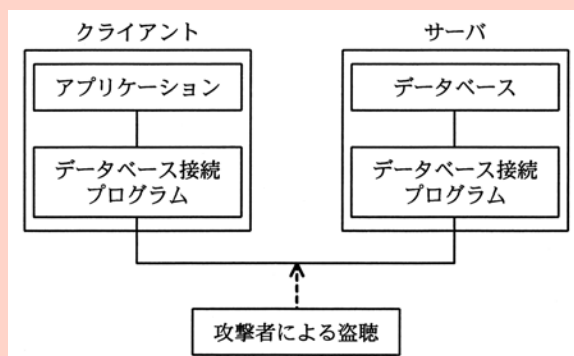


問23 不正利用を防止するためにメールサーバ(SMTPサーバ)で行う設定はどれか。

- ア ゾーン転送のアクセス元を制御する。
- イ 第三者中継を禁止する。
- ウ ディレクトリに存在するファイル名の表示を禁止する。
- エ 特定のディレクトリ以外でのCGIプログラムの実行を禁止する。



問24 図のように、クライアント上のアプリケーションがデータベース接続プログラム経由でサーバ上のデータベースのデータにアクセスする。データベース接続プログラム間で送受信されるデータが、通信経路上で盗聴されることに対する対策はどれか。



- ア クライアント側及びサーバ側にあるデータベース接続プログラム間の通信を暗号化する。
- イ サーバ側のデータベース接続プログラムにアクセスできるクライアントのIPアドレスを必要なものだけに制限する。
- ウ サーバ側のデータベース接続プログラムを起動・停止するときに必要なパスワードを設定する。
- エ データベース接続プログラムが通信に使用するポート番号をデータベース管理システムによって提供される初期値から変更する。

解説

問22 SQLインジェクション

SQLインジェクションとは、Webページ上の入力フォームに不正な文字列を入力し、その文字列から生成されたSQL文を不正なものにして、Webアプリケーションを誤動作させたり、データベースの内容を不正に閲覧または削

除したりする攻撃方法のことです。

一般的なDBMSでは、「;」(セミコロン)で区切って複数のSQL文を一括して実行できる仕様になっています。例えば、「SELECT～FROM～…; UPDATE～SET～…」というSQL文を作成すれば、SELECT文の実行後にUPDATE文も実行されます。

例として、検索したい名前の文字列(文字列Xとする)をWebページの入力フォームに入力させるWebアプリケーションシステムを考えます。このシステムのWebページから呼び出されるCGIの処理中では、

```
SELECT * FROM TABLE_A WHERE name like '文字列X'
```

のように、列nameの値が文字列Xと等しい行のみを検索するSQL文を作成します。この入力フォームに、例えば「';DELETE FROM TABLE_A WHERE 'A'='A」のような文字列が入力可能になっていると、以下のようなSQL文が作成されてしまいます。

```
SELECT * FROM TABLE_A WHERE name like '' ;DELETE FROM TABLE_A WHERE 'A'='A'
```

後半のDELETE文の条件('A'='A')は、TABLE_Aの内容にかかわらず常に成立します。よって、全ての行がWHERE以降の条件式に適合しているとみなされ、TABLE_Aの全部の行が削除されてしまうことになります。

この入力フォームでは、「'」のような、SQL文中で使用される「データベースの操作・問合せにおいて特別な意味をもつ」文字が入力可能であったため、問題が発生したことになります。よって、入力値から「'」「"」などの特別な文字(特殊文字)を取り除いたり、データ入力時に最初から特殊文字が入力されないように保護したりすることで、SQLインジェクションを防止することができます。

× **ア** この方法は、**ディレクトリトラバーサル攻撃**への対策です。

○ **イ** 正解です。

× **ウ** この方法は、**クロスサイトスクリプティング**への対策です。

× **エ** この方法は、**バッファオーバーフロー**への対策です。

問23 メールサーバの不正利用防止

一般には、SMTPサーバ(メールサーバ)は、自組織(自社)内のユーザ宛のメールの受信と、自社内のユーザが送信元となってインターネット上に送信するメール以外の転送を禁止し、無関係のメールを送受信または中継しないように設定します。これはSPAMメールなどの不正中継に利用されないようにするためです。

しかし、SMTPサーバのセキュリティ対策が甘く、外部から第三者あてに送信するメールを転送可能な設定にしておいたままにすると、悪意のユーザが発信したSPAMメールなどの不審なメールの転送の肩代わり(不正中継)をさせられ、自社が不正行為に加担させられてしまうだけでなく、「不正中継すら防げないようなセキュリティの甘い会社」とみなされ、社会的信用の低下を招いてしまいます。よって、第三者中継を禁止すること(**イ**)が最も適切な措置です。

アはDNSサーバのセキュリティ対策、**ウ**、**エ**はWebサーバのセキュリティ対策です。

問24 通信経路の盗聴対策

クライアントからサーバに送られる途中で、通信経路上にあるデータの盗聴を防ぐには、データベース接続プログラム間の通信を暗号化し、盗聴されても内容が判別できないようにすればよいことになります。サーバ上やクライアント上でパスワードなどの制限を施しても、データベース接続プログラム間の通信が平文のままであれば、盗聴によって内容が露呈してしまうため、不適切です。

よって、解答群**ア**の記述のみが適切であり、他の解答群はいずれも送受信されるデータの暗号化を施していないため、通信経路上での盗聴を防止することはできません。

○ 解答 ○

問22 **イ**

問23 **イ**

問24 **ア**



問25 Webサーバのコンテンツの改ざんを検知する方法のうち、最も有効なものはどれか。

- ☐ **ア** Webサーバのコンテンツの各ファイルの更新日を保管しておき、定期的にファイルの更新日と比較する。
- ☐ **イ** Webサーバのコンテンツの各ファイルのハッシュ値を保管しておき、定期的に各ファイルから生成したハッシュ値と比較する。
- ☐ **ウ** Webサーバのメモリ使用率を定期的に確認し、バッファオーバーフローが発生していないことを確認する。
- ☐ **エ** Webサーバへの通信を監視し、HTTP、HTTPS以外の通信がないことを確認する。



問26 A社は、B社と著作物の権利に関する特段の取決めをせず、A社の要求仕様に基づいて、販売管理システムのプログラム作成をB社に依頼した。この場合のプログラム著作権の原始的帰属はどれか。

- ☐ **ア** A社とB社が話し合って決定する。
- ☐ **イ** A社とB社の共有となる。
- ☐ **ウ** A社に帰属する。
- ☐ **エ** B社に帰属する。



問27 不正競争防止法で保護されるものはどれか。

- ☐ **ア** 特許権を取得した発明
- ☐ **イ** 頒布されている独自のシステム開発手順書
- ☐ **ウ** 秘密として管理している事業活動用の非公開の顧客名簿
- ☐ **エ** 秘密としての管理を行っていない、自社システムを開発するために重要な設計書

解説

問25 コンテンツの改ざんの検知

Webサーバのコンテンツなど、各種ファイルの改ざんを検知するには、ファイルをハッシュ関数に与えて生成したハッシュ値を保管しておき、ファイルから生成したハッシュ値と比較すること(イ)が有効です。

ハッシュ関数は、与えたデータの内容がわずかでも異なると、生成するハッシュ値が異なるという性質をもちます。Webサーバのコンテンツの各ファイルが改ざんされ、もともとの内容と異なる内容になった場合、改ざんされる前に取得していたハッシュ値とは異なるハッシュ値が生成されるようになるので、改ざんを検知できます。

- × **ア** Webサーバのコンテンツの各ファイルの更新日を保管していても、その更新日と同じ日に各ファイルが改ざんされた場合、保管していた更新日と改ざん後の各ファイルの更新日が一致するので、改ざんを検知できません。
- **イ** 正解です。
- × **ウ** Webサーバのメモリ使用率を確認することで、バッファオーバーフローによってWebサーバのアクセス権を攻撃者に奪われ、コンテンツの各ファイルが改ざんされたことを検知できる可能性があります。しかし、バッファオーバーフロー以外の攻撃手法でアクセス権を奪われ、各ファイルを改ざんされることもあるので、この

方法だけでは改ざんを検知するのは困難です。

- × **エ** HTTPまたはHTTPSを用いたアクセスによって、Webサーバのアクセス権を攻撃者に奪われることがあるので、この方法では改ざんを検知するのは困難です。

問26 著作権

著作権は、著作物(思想または感情を創作的に表現したもの)を作成した著作者が行使できる権利で、著作権法で定義されています。

著作権法では、著作物は「創作者」に帰属すると規定されています。よって、A社がB社に依頼してプログラムの著作物が作成された場合、発注側ではなく受注側(プログラムを実際に作成した側)に著作権が帰属します。

本問では、A社からB社に販売管理システムのプログラム作成が委託されています。A社においてシステムの要件定義までは行われていますが、この段階では著作物として認められる主体であるプログラム(ソースコードなども含む)は完成しておらず、設計からテストまでを行ってプログラム本体を実際に完成させたのはB社です。よって、著作物の権利に関する特段の取決めがない場合は、著作権はB社に帰属します。

以上から、**エ**が正解です。A社とB社が話し合って著作権の帰属する側がどちらかを決定したり、A社とB社で著作権を共有したり、創作者でないA社が著作権をもったりすることはありません。

問27 不正競争防止法

不正競争防止法は、「事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もって国民経済の健全な発展に寄与する」(同法第1条より)ことを目的とした法律です。この法律では幾つかの行為を「不正競争」として定義し、不正競争によって営業上の利益を侵害された者などは、その侵害の停止などを請求する権利があることを規定しています。

この不正競争の一つに、「窃取、詐欺、強迫その他の不正の手段により営業秘密を取得する行為……又は不正取得行為により取得した営業秘密を使用し、若しくは開示する行為」があります。この「営業秘密」とは、同法で保護されている対象であり、「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」を指します。よって、**ウ**が適切です。

- × **ア** 特許権を取得した発明は、特許権法の保護対象となります。
- × **イ**、**エ** 頒布されている開発手順書などは、その存在や内容が公然のため、営業秘密にはなりません。また、秘密としての管理を行っていない設計書なども営業秘密とは認められません。
- **ウ** 正解です。

○ 解答 ○

問 25 **イ**

問 26 **エ**

問 27 **ウ**



問 28 個人情報に関する記述のうち、個人情報保護法に照らして適切なものはどれか。

- ア 構成する文字列やドメイン名によって特定の個人を識別できるメールアドレスは、個人情報である。
- イ 個人に対する業績評価は、その個人を識別できる情報が含まれていても、個人情報ではない。
- ウ 新聞やインターネットなどで既に公表されている個人の氏名、性別および生年月日は、個人情報ではない。
- エ 法人の本店住所、支店名、支店住所、従業員数及び代表電話番号は、個人情報である。



問 29 サイバーセキュリティ基本法において、サイバーセキュリティの対象として規定されている情報の説明はどれか。

- ア 外交、国家安全に関する機密情報に限られる。
- イ 公共機関で処理される対象の手書きの書類に限られる。
- ウ 個人の属性を含むプライバシー情報に限られる。
- エ 電磁的方式によって、記録、発信、伝送、受信される情報に限られる。



問 30 労働者派遣法に基づいた労働者の派遣において、労働者派遣契約関係が存在するのはどの当事者の間か。

- ア 派遣先事業主と派遣労働者
- イ 派遣先責任者と派遣労働者
- ウ 派遣元事業主と派遣先事業主
- エ 派遣元事業主と派遣労働者



問 31 労働基準法において、36協定の説明はどれか。

- ア 業務遂行の手段、時間配分の決定などを大幅に労働者に委ねる業務に適用され、労働時間の算定は、労使協定で定めた労働時間の労働とみなす制度
- イ 業務の繁閑に応じた労働時間の配分などを行い、労使協定によって1か月以内の期間を平均して1週の法定労働時間を超えないようにする制度
- ウ 時間外労働、休日労働についての労使協定を書面で締結し、行政官庁に届け出ることによって、法定労働時間外の労働が認められる制度
- エ 労使協定によって1か月以内の一定期間の総労働時間を定め、1日の固定勤務時間以外では、労働者に始業・終業時刻の決定を委ねる制度

解説

問28 個人情報保護法

個人情報保護法では、「個人情報」を次のように定義しています。

この法律において「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)をいう
(同第2条より)

メールアドレスを構成する文字列などから特定の個人を識別できる場合、そのメールアドレスは上の定義によって個人情報となります。

- **ア** 正解です。
- × **イ** 個人を識別できる情報が含まれる業績評価は、個人情報となります。
- × **ウ** 公表されているか否かにかかわらず、個人を識別できる情報は個人情報となります。
- × **エ** 法人の住所や代表電話番号などから個人を識別することはできないので、個人情報ではありません。

問29 サイバーセキュリティ基本法

サイバーセキュリティ基本法は、「サイバーセキュリティに関する施策を総合的かつ効果的に推進し、もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、国際社会の平和及び安全の確保並びに我が国の安全保障に寄与すること」を目的とした法律です。

この法律の第2条では、「サイバーセキュリティ」を次のとおり定義しています。

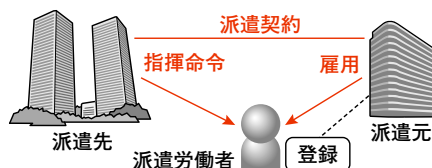
電子的方式、磁気的方式その他の知覚によっては認識することができない方式……により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置……が講じられ、その状態が適切に維持管理されていること

以上から、サイバーセキュリティの対象として規定されている情報は、電磁的方式によって記録、発信、伝送、受信される情報に限られます。正解は**エ**です。

問30 労働者派遣法

労働者派遣法では、「派遣労働者」、「派遣先事業主(企業)」、「派遣元事業主(企業)」の3者間の関係を図のように定めています。

派遣先事業主と派遣元事業主との間で「労働者派遣契約関係」が締結され、派遣先事業主の依頼に応じて、派遣元事業主が雇用している派遣労働者を派遣先事業主に派遣します。派遣労働者は、派遣先事業主の指揮命令下で業務を行います。正解は**ウ**です。



問31 労働基準法

労働基準法第三十二条では、一週間について40時間を超えて労働者を労働させてはならない(休憩時間を除く)ことや、一日について8時間を超えて労働させてはならない(同)ことを定めています。しかし、同法第三十六条に規定されている、使用者と労働組合間で取り交わした書面による労使協定があり、それを行政官庁に届け出ている場合は、第三十二条の時間を超えて労働させてもよいとしています。この協定のことを36協定といいます。

- × **ア** 裁量労働制の説明です。
- × **イ** 変形労働時間制の説明です。
- **ウ** 正解です。
- × **エ** フレックスタイム制の説明です。

○ 解答 ○

問28 **ア**

問29 **エ**

問30 **ウ**

問31 **ウ**



問 32 日本工業標準調査会を説明したものはどれか。

- ア** 経済産業省に設置されている審議会で、工業標準化法に基づいて工業標準化に関する調査・審議を行っており、JISの制定、改正などに関する審議を行っている。
- イ** 電気機械器具・材料などの標準化に関する事項を調査審議し、JEC規格の制定及び普及の事業を行っている。
- ウ** 電気・電子技術に関する非営利の団体であり、主な活動内容としては、書籍の発行、IEEEで始まる規格の標準化を行っている。
- エ** 電子情報技術産業の総合的な発展に資することを目的とした団体であり、JEITAで始まる標準規格の制定及び普及の事業を行っている。



問 33 システムの信頼性設計のうち、フルブーフを採用した設計はどれか。

- ア** オペレータが不注意による操作誤りを起こさないように、操作の確認などに配慮した設計
- イ** システムの一部に異常や故障が発生したとき、その影響が小さくなるような設計
- ウ** 障害の発生を予防できるように、機器の定期保守を組み入れた運用システムの設計
- エ** 装置を二重化し、一方が故障してもその装置を切り離してシステムの運用を継続できる設計



問 34 装置aとbのMTBFとMTTRが表のとおりであるとき、aとbを直列に接続したシステムの稼働率は幾らか。

単位 時間		
装置	MTBF	MTTR
a	80	20
b	180	20

- ア** 0.72
- イ** 0.80
- ウ** 0.85
- エ** 0.90



問 35 E-R図の説明のうち、適切なものはどれか。

- ア** エンティティタイプ間には、1対多、多対多などのリレーションシップがある。
- イ** エンティティタイプ間の関連は、参照側から被参照側へ方向の矢印線で表現する。
- ウ** エンティティタイプには属性をもたせないで、リレーションシップタイプに属性をもたせる。
- エ** エンティティタイプの中に関連先のエンティティ名を記述することによって、リレーションシップを表す。

解説

問32 日本工業標準調査会

- **ア** 正解です。
- × **イ** 一般社団法人電気学会電気規格調査会(JEC)の説明です。

- × **ウ** IEEE (The Institute of Electrical and Electronics Engineers)の説明です。
- × **エ** 社団法人 電子情報技術産業協会(JEITA)の説明です。

問33 フールプルーフ

フールプルーフとは、オペレータの操作誤りなどによってシステムが停止または誤動作することを防ぐために、入力の際に警告メッセージを出すなどの方法で、操作の確認などに配慮した設計のことをいいます。

- **ア** 正解です。
- × **イ** システムの一部に異常や故障が発生したとき、その影響が小さくなるようにする設計のことを、**フェールセーフ**といいます。
- × **ウ** 機器の定期保守を組み入れることで、障害の発生をあらかじめ予防できるようにする設計のことを、**フォールトアボイダンス**といいます。
- × **エ** 装置を二重化して、一方が故障してもその装置を切り離してシステムの運用を継続できるようにする設計のことを、**フォールトトレランス**といいます。

問34 稼働率

装置やシステムなどの**稼働率**は、 $MTBF \div (MTBF + MTTR)$ で求められます。

装置aの稼働率： $80 \div (80 + 20) = 0.8$

装置bの稼働率： $180 \div (180 + 20) = 0.9$

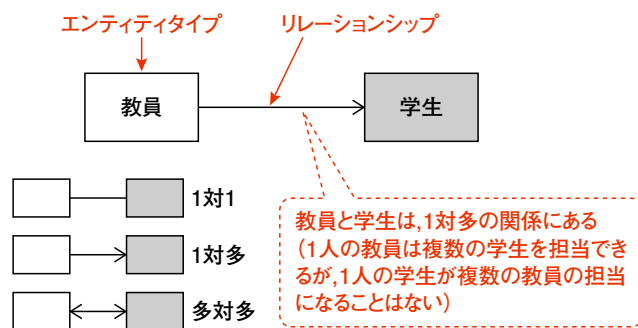
二つの装置を直列に接続したシステムの稼働率は、二つの装置の稼働率を乗じた値になります。よって、 $0.8 \times 0.9 = 0.72$ (**ア**)が正解です。

問35 E-R図

E-R図は、システム化しようとする業務体系などを抽象化した上で、情報の中に存在する実体(**エンティティタイプ**)と、実体間の関連(**リレーションシップ**)について表現する図法です。データベースシステムを実装する前に、データ同士の関連について定義するときによく用いられます。

エンティティタイプ間には、右の例に示したように、1対多、多対多などのリレーションシップがあります。

<例>



- **ア** 正解です。
- × **イ** エンティティタイプ間の関連を表すリレーションシップには、参照側、被参照側といった概念はありません。矢印線の矢じりは、1対多、多対多などの関連を表現するためのものです。
- × **ウ** エンティティタイプには実体が保持している属性をもたせません。リレーションシップタイプというものは、E-R図では表現されません。
- × **エ** リレーションシップは、矢印で表します。

○ 解答 ○

問 32 **ア**

問 33 **ア**

問 34 **ア**

問 35 **ア**



問36 関係データベースの操作の説明のうち、適切なものはどれか。

- ア 結合は、二つ以上の表を連結して、一つの表を生成することをいう。
- イ 射影は、表の中から条件に合致した行を取り出すことをいう。
- ウ 選択は、表の中から特定の列を取り出すことをいう。
- エ 挿入は、表に対して特定の列を挿入することをいう。



問37 TCP/IPのクラスBのIPアドレスをもつ一つのネットワークに、割り当てることができるホストアドレス数は幾つか。

- ア 1,022
- イ 4,094
- ウ 32,766
- エ 65,534



問38 電子メールの内容の機密性を高めるために用いられるプロトコルはどれか。

- ア IMAP4
- イ POP3
- ウ SMTP
- エ S/MIME



問39 プロジェクトスコープマネジメントにおいて、WBS作成のプロセスで行うことはどれか。

- ア 作業の工数を算定してコストを見積もる。
- イ 作業を階層的に細分化する。
- ウ 作業を順序付けして、スケジュールとして組み立てる。
- エ 成果物を生成するアクティビティを定義する。

解説

問36 関係データベース

関係データベースの表の操作には、選択・射影・結合などさまざまな種類があります。結合は、二つ以上の表を連結して、一つの表を生成する操作です。

- ア 正解です。
- × イ 射影は、表の中から特定の列を取り出す操作です。
- × ウ 選択は、表の中から条件に合致した行を取り出す操作です。
- × エ 挿入は、表に対して行を挿入することです。

問37 IPアドレス

IPアドレスは、TCP/IPを通信プロトコルとするネットワークにおいて、各機器に一意に付与すべきアドレスです。IPアドレスの長さは4バイト(32ビット)で、ネットワーク部(電話番号の市内局番までに相当する)と、ホスト部(電話番号の加入者番号部分)に分けられています。ネットワーク部の長さなどによって、IPアドレスはクラスA、クラスB、クラスC、クラスDに分類されています。

クラスA: 先頭1バイトがネットワーク部、残り3バイトがホスト部。ネットワーク部の先頭が“0”というビット列になる

クラスB: 先頭2バイトがネットワーク部, 残り2バイトがホスト部。ネットワーク部の先頭が“10”というビット列になる
クラスC: 先頭3バイトがネットワーク部, 残り1バイトがホスト部。ネットワーク部の先頭が“110”というビット列になる

クラスD: マルチキャスト通信(複数の端末に同時にデータを送信すること)のための, 特別なIPアドレス群。ネットワーク部の先頭が“1110”というビット列になる

なお, ホスト部のビット列が全て0, または全て1になっているものは, 特別な用途で使用するため, 個別の機器に割り当ててはできません。ホスト部の値のビットが全て0のものは, ネットワークそのものを表すアドレスです。ホスト部の値のビットが全て1のものは, ネットワークの全ての機器へのブロードキャストアドレスです。

以上から, クラスBではホスト部の長さが2バイトとなるため, $2^{16} = 65,536$ とおりのビットパターンをもつこととなります。しかし, ホスト部の値が全て0, 及び全て1の2とおりのパターンは使用できないため, $65,536 - 2 = 65,534$ (E)とおりのホストアドレスをもつこととなります。

問38 電子メールの機密性

電子メールの機密性を高めるために用いられる, 電子メールの暗号化プロトコルに, **S/MIME** (E) があります。S/MIMEは, MIME (Multipurpose Internet Mail Extensions, 電子メール上で, 画像などの添付ファイルを送信するための規格)の機能を拡張したものです。S/MIMEでは, 公開鍵暗号方式を用いてメールの暗号化・復号を行います。

ア, **イ** (IMAP4, POP3)はクライアントがメールサーバからメールを受信するためのプロトコルです。**ウ** (SMTP)は標準的な電子メール送受信用プロトコルです。

問39 プロジェクトスコープマネジメント

プロジェクトスコープマネジメントとは, システム開発のプロジェクトにおける作業を洗い出し, その名称や作業範囲などを決定して管理することです。プロジェクトスコープマネジメントにおいて, **WBS** (Work Breakdown Structure)の作成が行われます。WBSとは, システム開発のプロジェクト全体を細かい作業に分割し, 整理した図のことです。

WBSでは, まずプロジェクトを「企画プロセス」, 「要件定義プロセス」などといった大きな範囲の作業に分割し, それらの各作業をさらに細かい作業に分割することを繰り返していくことで, 詳細なレベルにまで作業を細分化します。WBS作成において細分化した最下位レベルの作業のことを, **ワークパッケージ**といいます。

- × **ア** **プロジェクトコストマネジメント**において実施される作業です。
- **イ** 正解です。
- × **ウ** **プロジェクトタイムマネジメント**において実施される作業です。
- × **エ** **アクティビティ**とは, ワークパッケージをさらに細分化した作業のことです。アクティビティの定義は, プロジェクトタイムマネジメントにおいて実施される作業です。

○ 解答 ○

問 36 **ア**

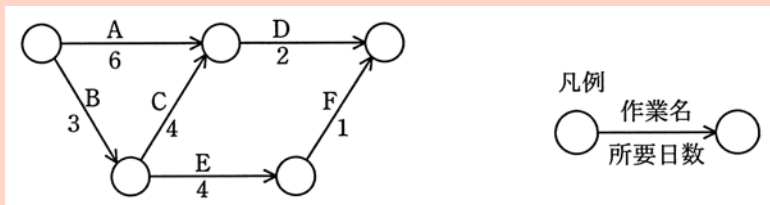
問 37 **エ**

問 38 **エ**

問 39 **イ**



問 40 図のアローダイアグラムにおいて、プロジェクト全体の期間を短縮するために、作業A～Eの幾つかを1日ずつ短縮する。プロジェクト全体を2日短縮できる作業の組合せはどれか。



ア A, C, E

イ A, D

ウ B, C, E

エ B, D



問 41 ITサービスマネジメントの管理プロセスはどれか。

ア サービスレベル管理

イ スケジュール管理

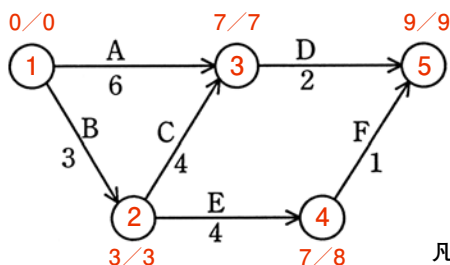
ウ 品質管理

エ リスク管理

解説

問40 アローダイアグラム

図のアローダイアグラムに、説明用の数字と最早結合点時刻及び最遅結合点時刻を付与したものを示します。



凡例：最早結合点時刻／最遅結合点時刻

● 最早結合点時刻

- ①：どの作業も実施されていないので0日目。
- ②：0日目(①)から作業Bが実施された時点なので $0+3=3$ 日かかる。
- ③：3日目(②)から作業Cが実施されるのに $3+4=7$ 日かかる。0日目(①)から作業Aが実施されるのに $0+6=6$ 日かかる。両方の作業が終わるのは7日目。
- ④：3日目(②)から作業Eが実施されるのに $3+4=7$ 日かかる。
- ⑤：7日目(③)から作業Dが実施されるのに $7+2=9$ 日かかる。7日目(④)から作業Fが実施されるのに $7+1=8$ 日かかる。両方の作業が終わるのは9日目。

● 最遅結合点時刻

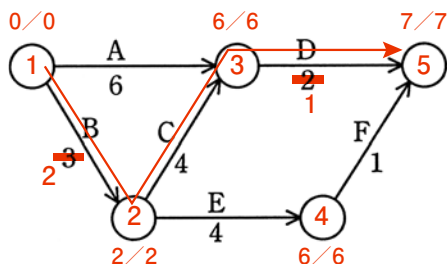
- ⑤：全ての作業が終わった時点なので、最遅結合点時刻は最早結合点時刻に一致する。9日。
- ④：⑤の最遅結合点時刻=9日目から作業Fの所要日数=1日を引くと8日目になる。8日目から作業Fを開始しても

プロジェクト全体は遅れないので、最遅結合点時刻は8日目。

- ③：⑤の最遅結合点時刻＝9日目から作業Dの所要日数＝2日を引くと7日目になる。7日目から作業Dを開始しないと作業Dの完了が9日目より遅くなり、プロジェクト全体が遅れる。よって、最遅結合点時刻は7日目。
- ②：④の最遅結合点時刻＝8日目から作業Eの所要日数＝4日を引くと4日目になる。また、③の最遅結合点時刻＝7日目から作業Cの所要日数＝4日を引くと3日目になる。3日目から作業Cを開始しないと後続の作業Dの開始も遅れ、プロジェクト全体が遅れる。よって、最遅結合点時刻は3日目。
- ①：③の最遅結合点時刻＝7日目から作業Aの所要日数＝6日を引くと1日目になる。また、②の最遅結合点時刻＝3日目から作業Bの所要日数＝3日を引くと0日目になる。0日目から作業Bを開始しないと後続の作業Cなどの開始も遅れ、プロジェクト全体が遅れる。よって、最遅結合点時刻は0日目。

上記の下線部分から、作業B、C、Dの三つのいずれかが遅れると、プロジェクト全体が遅れることがわかります。この三つの作業の流れ(①→②→③→⑤)がクリティカルパスです。クリティカルパス上の作業の所要日数を短縮することで、作業全体の終了時刻が早くなるので、プロジェクト全体を短縮できます。よって、作業B、C、Dのうち、二つの作業の所要日数を1日ずつ短縮することで、プロジェクト全体を2日短縮できます。**エ**の組合せ(B、D)が適切です。

(作業B、Dを1日ずつ短縮したときのアローダイアグラム)



ア～ウの組合せは、クリティカルパス上にない作業を1日短縮しているので、プロジェクト全体の期間を2日短縮させることはできません。

問41 ITサービスマネジメント

ITサービスマネジメントとは、顧客の要件(要求事項)を満たす高品質のITサービスの開発や提供を行うために、必要な業務プロセスを構築して運営管理することです。

ITサービスマネジメントのベストプラクティスとして、**ITIL** (Information Technology Infrastructure Library) がよく知られています。ITILとは、1989年に英国政府の中央コンピュータ電気通信局によって作成・公表された、ITサービスマネジメントにおけるベストプラクティスをまとめたものです。

ITILは、IT業務サービスの日々の運用手法をまとめた「サービスサポート」に関するプロセスと、中長期的なサービスの管理手法をまとめた「サービスデリバリー」に関するプロセスからなります。それらを以下に紹介します。

サービスサポートに関するプロセス：サービスデスク(機能)、インシデント管理、問題管理、構成管理、変更管理など

サービスデリバリーに関するプロセス：サービスレベル管理、可用性管理、ITサービス財務管理、キャパシティ管理、ITサービス継続性管理

以上から、**ア**が正解です。**ア**以外の管理プロセスは、システム開発プロジェクトにおける管理プロセスであり、ITサービスマネジメントには存在しません。

○ 解答 ○

問40 **エ**

問41 **ア**



問 42 システムの移行方式の一つである一斉移行方式の特徴はどれか。

- ア 新旧システム間を接続するアプリケーションが必要となる。
- イ 新旧システムを並行させて運用し、ある時点で新システムに移行する。
- ウ 新システムへの移行時のトラブルの影響が大きい。
- エ 並行して稼働させるための運用コストが発生する



問 43 システム監査人の独立性が保たれている状況はどれか。

- ア 営業部門の要員を監査チームのメンバに任命し、営業部門における個人情報保護対策について監査を行わせる。
- イ 監査法人からシステム監査人を採用して内部監査人に位置付け、社内の業務システム開発についての監査を行わせる。
- ウ システム部門の要員を監査部門に異動させ、システム部門に所属していたときに開発に参加したシステムの保守についての監査を担当させる。
- エ 社内の業務システム運用を委託しているITベンダの監査部門に依頼し、社内の業務システム運用についての外部監査を担当させる。



問 44 金融庁の“財務報告に係る内部統制の評価及び監査の基準”において、内部統制に関係を有する者の役割と責任の記述のうち、適切なものはどれか。

- ア 株主は、組織のすべての活動について最終的な責任を有する。
- イ 監査役は、内部統制の整備及び運用に係る基本方針を決定する。
- ウ 経営者は、取締役の職務の執行に対する監査の一環として、独立した立場から、内部統制の整備及び運用状況を監視、検証する役割と責任を有する。
- エ 内部監査人は、モニタリングの一環として、内部統制の整備及び運用状況を検討、評価し、必要に応じて、その改善を促す職務を担っている。

解説

問42 一斉移行方式

システムの移行方式のうちの、**一斉移行方式**に関する問題です。

一斉移行方式とは、古いシステムで使用していた機器やプログラムなどを、全ての拠点(本社・支社・店舗など)で一斉に新システムのものに入れ替える方式です。この方式では、移行に要する期間が短くなるため、移行に伴う運用や保守の負担は少なくなる(経済的効果が大きい)メリットがあります。しかし、以下のデメリットもあります。

- 全ての拠点が一斉に新システムに移行するため、移行後に旧システムに戻すことが難しくなる。
- 全ての拠点が一斉に新システムに移行するため、新システムに問題があり、旧システムに戻さなければならなくなった場合の影響範囲が、非常に大きくなる。
- 新システム移行時に発生したトラブルの影響範囲が大きくなる。

以上から、**ウ**の記述が適切です。

× **ア** 一斉移行方式では、新システムへの移行の時点で旧システムを廃止するため、新旧システムを同時に利用す

ることはありません。よって、新旧システム間を接続するアプリケーションなどは不要です。

- × **イ** **ア**と同様に、一斉移行方式では、新旧システムを同時に利用することはありません。
- **ウ** 正解です。
- × **エ** 一斉移行方式では、新旧システムを並行稼働させることはありません。

問43 システム監査人の独立性

経済産業省公表の「**システム監査基準**」では、システム監査人の独立性や客観性及び職業倫理について、以下のよう

に定義しています。

2.1 外観上の独立性

システム監査人は、システム監査を客観的に実施するために、監査対象から独立していなければならない。監査の目的によっては、被監査主体と身分上、密接な利害関係を有することがあってはならない。
(同基準より引用)

この記述から、監査対象の組織や部門に所属する人間をシステム監査人として選別するのは、システム監査基準の監査人の独立性の定義に照らして不適切となります。また、ある部門にかつて所属していて、当該部門の業務内容などに精通している要員を形式上別の部門に移動させてから、当該部門の監査をその要員に行わせることも、システム監査基準の監査人の独立性の定義に照らして不適切となります。よって、**ア**、**ウ**、**エ**は不適切な記述です。

- × **ア** 監査対象部門(営業部門)の要員が当該部門の監査を行っていることとなります。
- × **ウ** 実質的には監査対象部門(システム部門)の要員が当該部門の監査を行っていることとなります。
- × **エ** ITベンダの監査部門が、同システム運用についての監査を行っているため、監査対象業務を担当している部門(ITベンダの監査部門)が当該業務の監査を行っていることとなります。

以上から、**イ**の記述のみが適切です。

問44 財務報告に係る内部統制の評価及び監査の基準

「**財務報告に係る内部統制の評価及び監査の基準**」とは、金融庁が公表した「財務報告に係る内部統制の評価及び監査の基準並びに財務報告に係る内部統制の評価及び監査に関する実施基準の設定について(意見書)」という意見書に含まれている基準で、「経営者による財務報告に係る内部統制の評価及び報告の基準と監査人による財務報告に係る内部統制の監査の基準の前提となる内部統制の概念的な枠組み」などについて示しているものです。

この基準では、「モニタリングの一環として、内部統制の整備及び運用状況を検討、評価し、必要に応じてその改善を促す役割と責任を有している者」を、「**内部監査人**」と定義しています。よって、**エ**が正解です。

- × **ア** この基準では、組織の全ての活動について最終的な責任を有しており、その一環として、取締役会が決定した基本方針に基づき内部統制を整備及び運用する役割と責任がある者のことを、「**経営者**」と呼んでいます。「株主」については、この基準では特に定義していません。
- × **イ** この基準では、取締役及び執行役の職務の執行に対する監査の一環として、独立した立場から、内部統制の整備及び運用状況を監視、検証する役割と責任を有している者を、「**監査役**」または「**監査委員会**」と呼んでいます。監査役には、内部統制の整備及び運用に係る基本方針を決定する役割と責任はありません。内部統制の整備及び運用に係る基本方針を決定するのは、取締役会の役割です。
- × **ウ** この解答群は経営者ではなく、監査役または監査委員会の説明となります。
- **エ** 正解です。

○ 解答 ○

問 42 **ウ**

問 43 **イ**

問 44 **エ**



問45 BPRを説明したものはどれか。

- ア 企業全体の経営資源の配分を有効かつ総合的に計画して管理し、経営の効率向上を図ることである。
- イ 顧客視点から業務のプロセスを再設計し、情報技術を十分に活用して、企業の体質や構造を抜本的に変革することである。
- ウ 最強の競合相手又は先進企業と比較して、製品、サービス、オペレーションなどを定性的・定量的に把握することである。
- エ 利益をもたらすことのできる、他社より優越した自社独自のスキルや技術に経営資源を集中することである。



問46 SaaSを説明したものはどれか。

- ア インターネット経由でアプリケーションソフトウェアの機能を、利用者が必要なときだけ利用するサービスのこと
- イ 企業の経営資源を有効に活用するために、基幹業務を統合的に管理するためのソフトウェアパッケージのこと
- ウ 既存の組織やビジネスプロセスを抜本的に見直し、職務、業務フロー、管理機構、情報システムを再設計すること
- エ 発注者とサービス提供者との間で、サービスの品質の内容について合意した文書のこと



問47 共通フレーム2007によれば、企画プロセスで定義するものはどれか。

- ア 新しい業務の在り方や業務手順、入出力情報、業務を実施する上での責任と権限、業務上のルールや制約などの要求事項
- イ 業務要件を実現するために必要なシステムの機能や、システムの開発方式、システムの運用手順、障害復旧時間などの要求事項
- ウ 経営事業の目的、目標を達成するために必要なシステムに関係する経営上のニーズ、システム化、システム改善を必要とする業務上の課題などの要求事項
- エ 求められているシステムを実現するために必要なシステムの機能、能力、ライフサイクル、信頼性、安全性、セキュリティなどの要求事項

解説

問45 BPR

BPR (Business Process Reengineering)とは、企業活動に関する特定の目標を設定した上で、その目標を達成するために既存の組織やビジネスルール、及び業務プロセスなどを抜本的に見直し、各自の職務や組織構造、各種業務の流れ(業務フロー)、及び情報システムなどを改革し、業務の最適化を行うことです。BPRを行う際には、旧来の業務システムを情報化するなど、情報処理技術を用いた改善が行われることがあります。また、業務プロセスを見直す際には、企業の視点からではなく、製品やサービスを利用する顧客の視点から見直しを行い、自社の問題点などを客観的に確認することが多くなります。

- × **ア** 自社の経営資源の配分を有効かつ総合的に計画して管理し、経営効率を向上させようとするのは、**ERP** (Enterprise Resource Planning)の説明です。
- **イ** 正解です。
- × **ウ** 競合他社や先進企業のベストプラクティスを参考にして、自社の業務プロセスを抜本的に改善するのは、**ベンチマーキング**の説明です。
- × **エ** 競合他社にはまねのできない、企業独自のノウハウや技術などを核とし、それらに経営資源を集中することで競争優位を確立することを目的とする経営のことを、**コアコンピタンス経営**といいます。

問46 SaaS

SaaS (Software as a Service)とは、サービス提供側のサーバ上のアプリケーションソフトウェアの機能を、インターネットを経由して必要に応じて利用者側のブラウザなどにインストールさせ、当該機能を必要なときだけ利用者に提供するサービスのことです。このサービスでは、利用者側がソフトウェアをPCにインストールする手間が省けるなどのメリットがあります。

- **ア** 正解です。
- × **イ** **ERPパッケージ**の説明です。
- × **ウ** **BPR** (Business Process Re-engineering)の説明です。
- × **エ** **SLA** (Service Level Agreement)の説明です。

問47 共通フレーム2007

共通フレーム2007は、ソフトウェアライフサイクルプロセスの作業項目を可視化した規格です。ソフトウェアライフサイクルプロセスとは、企画、要件定義、開発、運用及び保守といった、ソフトウェア(システム)を企画し、開発し、それを運用していく過程で一連のプロセス(業務)をまとめたものです。

ソフトウェアライフサイクルプロセスの企画プロセスでは、経営事業の目的や目標達成のために必要な経営上のニーズ、システムの機能及び業務上の課題などの要求事項をまとめ、情報システムを構築するためのシステム化方針を策定し、システムを実現するための計画(システム化計画)を立案することが行われます。よって、**ウ**が正解です。

- × **ア** 要件定義プロセスにおいて定義される、業務要件の記述です。
- × **イ** 要件定義プロセスにおいて定義される、非機能要件の記述です。
- **ウ** 正解です。
- × **エ** 開発プロセスにおいて定義される、システム要件の記述です。

○ 解答 ○

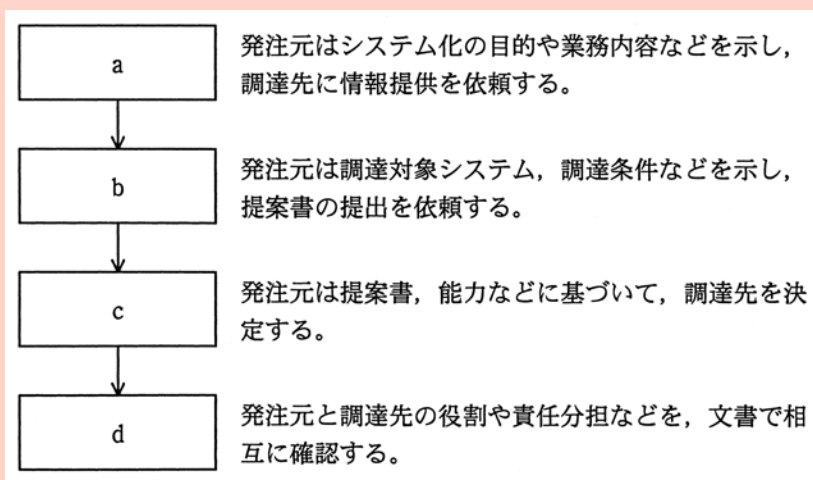
問45 **イ**

問46 **ア**

問47 **ウ**



問 48 図に示す手順で、情報システムを調達する場合、bに入るものはどれか。



- ア** RFI **イ** RFP **ウ** 供給者の選定 **エ** 契約の締結



問 49 ナレッジマネジメントを説明したものはどれか。

- ア** 企業内に散在している知識を共有化し、全体の問題解決力を高める経営を行う。
イ 迅速な意思決定のために、組織の階層をできるだけ少なくした平型の組織構造によって経営を行う。
ウ 優れた業績を上げている企業との比較分析から、自社の経営革新を行う。
エ 他社にまねのできない、企業独自のノウハウや技術などの強みを核とした経営を行う。



問 50 減価償却の方法として認められているものはどれか。

- ア** 移動平均法 **イ** 最終取得原価法 **ウ** 定率法 **エ** 持分法

解説

問48 情報システムの調達

情報システムの発注元が、システム化の目的や業務内容などを示して、調達先に情報の提供を依頼するための書類を、**RFI** (Request For Information, 情報提供依頼書)といいます。発注元が情報システムの発注を行う場合、最初にRFIを調達先に送付するのが一般的です。aにはRFI (**ア**)が入ります。

RFIを受け取った発注元が、発注する情報システムの概要や発注依頼事項、調達条件及びサービスレベル要件などを明示し、情報システムの提案書の提出を依頼するために、調達先に送付する文書を**RFP** (Request For Proposal, 提案依頼書)といいます。bにはRFP (**イ**)が入ります。

発注元は、各調達先から送付されてきた提案書の内容や能力などに基づいて、情報システムの発注をする調達先を選定します。この作業を供給者の選定といいます。cには供給者の選定 (**ウ**)が入ります。

発注元は、選定した調達先との間で文書を取り交わして契約を締結し、両者の役割や情報システム開発における責任分担などを、相互に確認します。dには契約の締結(エ)が入ります。

よって正解はイです。

問49 ナレッジマネジメント

ナレッジマネジメントとは、情報システムなどを活用して、組織の中の過去の経験から得られた知識を整理・管理し、社員に共有させて業務の効率化を図るための体制を作り、問題解決力を高める経営をすることをいいます。

- ア 正解です。
- × イ 迅速な意思決定のために、組織の階層をできるだけ少なくした平型の組織構造による経営を行うのは、**組織のフラット化**についての説明です。
- × ウ 優れた業績を上げている企業の経営方法を、自社の経営方法と比較するなどの方法で自社の経営革新を行うのは、**ベンチマーキング**の説明です。
- × エ 自社が確立してきた独自の技術や経営ノウハウなどを活用することで、競合他社にはまねのできない、企業独自のノウハウなどを核とした経営を行うのは、**コアコンピタンス経営**の説明です。

問50 減価償却

資産の減価償却を行う方法には、**定額法**(毎年一定の金額を減価償却費とする)と、**定率法**(毎年、資産が一定の前年比で価値が減少するようにする)の2つがあります。

定額法では、“(取得原価－残存価格)÷耐用年数”という式で求めた一定の金額を、減価償却費として毎年計上します。定率法では、“(取得原価－減価償却累計額)×耐用年数に応じた償却率”という式で求めた金額を、減価償却費として毎年計上します。

- × ア **移動平均法**とは、在庫単価の算出方法の一つです。移動平均法では、購入した都度、そのときの在庫金額と購入価格との合計額を、在庫数量と購入数量との合計数量で割ることで在庫単価を算出します。
- × イ **最終取得原価法**(最終仕入原価法)とは、在庫単価の算出方法の一つです。最終取得原価法は、期末(棚卸時点)に最も近い時期に仕入れた商品の単価を、全体の在庫単価とする方法です。
- ウ 正解です。
- × エ **持分法**とは、自社の子会社など、一定以上の議決権をもっている会社の経営成績などを、連結財務諸表に反映させる方法のことです。

○ 解答 ○

問 48 イ

問 49 ア

問 50 ウ

第①回 模擬試験 午後 問題

問 1 情報セキュリティにおけるリスクに関する次の記述を読んで、設問 1, 2 に答えよ。

E 君の所属する F 社では、自社の情報セキュリティにおけるリスクを数値化して管理することになり、基準を設定して所有する情報資産のリスク評価を行うことになった。E 君はこのうち、サーバ X 及びサーバ Y のリスク評価を担当した。

なお、ここでは、試行のための仮の基準と値を扱うが、それぞれに“仮”を表す文言は用いない。

〔リスクの値の算出〕

F 社では、機密性、完全性、可用性のそれぞれについて、情報資産のリスクの値を、次の式で算出する。

リスクの値 = 情報資産の価値 × 脅威 × ^{ぜい}脆弱性

〔情報資産の価値の評価基準〕

F 社では、機密性、完全性、可用性のそれぞれから見た情報資産の価値の評価基準と値を、表 1～3 のとおりに設定した。

表 1 機密性の評価基準と値

評価基準	値
社外に開示できる。	1
社内だけに開示できる。	2
部門内だけに開示できる。	3
必要最小限の関係者だけに開示できる。	4

表 2 完全性の評価基準と値

評価基準	値
情報の完全性が失われても、業務への影響はない。	1
情報の完全性が失われても、業務への影響は小さい。	2
情報の完全性が失われると、業務への影響は大きい。	3

表 3 可用性の評価基準と値

評価基準	値
定期メンテナンス以外で年間 24 時間までの利用停止は容認される。	1
定期メンテナンス以外で年間 5 時間までの利用停止は容認される。	2
定期メンテナンス以外で年間 1 時間までの利用停止は容認される。	3
定期メンテナンス以外で年間 10 分までの利用停止は容認される。	4
定期メンテナンス以外で年間 1 分までの利用停止は容認される。	5

〔脅威と脆弱性の判断基準〕

F 社では、脅威と脆弱性の判断基準と値を、それぞれ表 4, 5 のとおりに設定した。

表4 脅威の判断基準と値

判断基準	値
発生の可能性が低い。	1
発生の可能性が中程度である。	2
発生の可能性が高い。	3

表5 脆弱性の判断基準と値

判断基準	値
適切な管理と対策がなされている。	1
ある程度の管理と対策がなされている。	2
管理と対策が不十分である。	3

〔サーバX及びサーバY〕

サーバXでは、調達先一般情報のデータベースが稼働している。調達先一般情報とは、調達先コード、調達先の正式な名称、略称、住所、電話番号などである。

サーバYでは、取引情報のデータベースが稼働している。取引情報とは、調達先コード、購入品コード、単価、購入履歴などである。

E君は、サーバX及びサーバYの機密性、完全性、可用性のそれぞれから見た価値を評価するために、調達先一般情報と取引情報に関して、社内関連部門から聴取し、その内容を次のようにまとめた。

〔社内関連部門からの聴取内容〕

(1) 調達先一般情報

- ① 電話帳や各社のWebページで公開されている情報であるが、取引があることをF社の競合他社に知られたくない調達先もあるので、社外には公開できない。
- ② この情報は、調達先との間で行っているEDI（電子データ交換）では利用していないので、誤りがあっても調達業務に与える影響は小さい。
- ③ 社員が、電話番号の確認や、挨拶状の宛先ラベルの印字に利用しているが、サーバXが利用できない場合には、代替手段での入手が可能である。

(2) 取引情報

- ① 競合する調達先をはじめ、F社の同業他社に知られてはならない情報である。また、社内でも、他部門には開示できない情報である。
- ② 情報に誤りがあれば、調達や支払などの業務に与える影響は大きい。
- ③ 営業時間内の調達オンライン入力処理、及び夜間のバッチ処理で利用されており、これら进行处理するシステムは、メンテナンス以外では、年間4時間以上停止することは許されない。

〔脅威と脆弱性の状況〕

E君は、各サーバがさらされている脅威とその脅威に対するF社の脆弱性を調査し、表4及び表5の判断基準に基づいて評価した。そのうちの主なものを、表6に示す。

表6 サーバX及びサーバYの主な脅威と脆弱性の値

脅威		脆弱性	
種類	値	種類	値
ウイルス感染	3	ウイルス対策ソフト未導入	3
不正アクセス	3	アクセスコントロールの不備	2
故障	2	メンテナンス不足	3
なりすまし	2	パスワード管理の不備	2
盗聴	2	最新推奨暗号の未使用	1

〔受容可能なリスク水準〕

F社では、受容可能なリスク水準を、表7のとおりに設定した。情報資産について各リスクの値がこれらの値以下であれば、そのリスクを保有し、そうでなければ、リスク対応を行う。

表7 受容可能なリスク水準

機密性	13
完全性	15
可用性	10

〔サーバX及びサーバYのリスク評価〕

表1～5の基準、聴取内容及びサーバXとサーバYの状況から、E君は、サーバX及びサーバYに関するリスク評価を行った。F社では、評価に当たって、表1～3の評価基準では、該当する基準の値のうちで最も小さいものを選ぶことにしている。

評価結果の一部を表8に示す。

表8 サーバX及びサーバYのリスク評価（抜粋）

情報資産			脅威		脆弱性		リスク
名称	価値		内容	値	内容	値	値
	分類	値					
サーバ X	機密性		⋮				
			なりすまし		パスワード管理の不備		a
			⋮				
	完全性		ウイルス感染		ウイルス対策ソフト未導入		18
			不正アクセス		アクセスコントロールの不備		12
			なりすまし		パスワード管理の不備		8
			⋮				
可用性		⋮					
サーバ Y	機密性		⋮				
			不正アクセス		アクセスコントロールの不備		b
			⋮				
	完全性		ウイルス感染		ウイルス対策ソフト未導入		c
			⋮				
可用性	d	⋮					

注記 網掛けの部分は表示していない。“…”は表示の省略を示している。

設問 1 表8中の a ～ d に入れる正しい答えを、解答群の中から選べ。

a～cに関する解答群

- | | | | | |
|-------------|-------------|-------------|-------------|-------------|
| ア 4 | イ 6 | ウ 8 | エ 9 | オ 12 |
| カ 16 | キ 18 | ク 24 | ケ 27 | コ 36 |

dに関する解答群

- | | | | | |
|------------|------------|------------|------------|------------|
| ア 1 | イ 2 | ウ 3 | エ 4 | オ 5 |
|------------|------------|------------|------------|------------|

設問 2 表8のサーバXの完全性の破線で囲まれた部分に関し、F社の受容可能なリスク水準から判断されるリスク対応として適切なものを、解答群の中から選べ。

解答群

- ア** IDS (侵入検知システム)を導入する。
 イ ウイルス対策ソフトを導入する。
ウ 公開鍵暗号を利用する。
 エ 定期メンテナンスの回数を増やす。
オ パスワード管理を強化する。

解説

情報セキュリティにおけるリスクの受容または対応に関する問題です。問題文中のリスクの計算式や各種基準の説明を理解することで、リスクの値を容易に計算できます。

設問 1 リスク評価

空欄 a

サーバXでは調達先一般情報のデータベースが稼働しているので、調達先一般情報の機密性、完全性、可用性のそれぞれから見た価値を評価することで、サーバXの機密性、完全性、可用性の価値の値を求めることができます。

【社内関連部門からの聴取内容】から、調達先一般情報は「社外には公開できない」(すなわち、社内には公開できる)ので、表1の機密性の評価基準の「社内だけに開示できる」に該当します。よって、サーバXの機密性の値は2になります。表6から、脅威「なりすまし」の値は2です。これに対応する脆弱性「パスワード管理の不備」の値は2です。以上から、サーバXの機密性に関するなりすましのリスクの値 $=2 \times 2 \times 2 = 8$ (ウ)になります。

参考のために、サーバXの完全性に関する各脅威のリスクの値の求め方を確認します。【社内関連部門からの聴取内容】から、調達先一般情報は「誤りがあっても調達業務に与える影響は小さい」ので、表2の完全性の評価基準の「情報の完全性が失われても、業務への影響は小さい」に該当します。よって、サーバXの完全性の値は2になります。表6から、脅威「ウイルス感染」の値は3です。これに対応する脆弱性「ウイルス対策ソフト未導入」の値は3です。以上から、サーバXの完全性に関するウイルス感染のリスクの値 $=2 \times 3 \times 3 = 18$ になります。

同様に計算すると、サーバXの完全性に関する不正アクセスのリスクの値 $=2 \times 3 \times 2 = 12$ 、なりすましのリスクの値 $=2 \times 2 \times 2 = 8$ になります。

空欄 b

サーバYでは取引情報のデータベースが稼働しているので、取引情報の機密性、完全性、可用性のそれぞれから見た価値を評価することで、サーバYの機密性、完全性、可用性の価値の値を求めることができます。

【社内関連部門からの聴取内容】から、取引情報は「同業他社に知られてはならない」ものであり、かつ、社内でも「他部門には開示できない」ので、表1の機密性の評価基準の「部門内だけに開示できる」に該当します。よって、サーバYの機密性の値は3になります。表6から、脅威「不正アクセス」の値は3です。これに対応する脆弱性「アクセスコントロールの不備」の値は2です。以上から、サーバYの機密性に関する不正アクセスのリスクの値 $=3 \times 3 \times 2 = 18$ (キ)になります。

空欄 c

【社内関連部門からの聴取内容】から、取引情報に誤りがあると「調達や支払などの業務に与える影響は大きい」ので、表1の完全性の評価基準の「情報の完全性が失われると、業務への影響は大きい」に該当します。よって、サーバYの完全性の値は3になります。表6から、脅威「ウイルス感染」の値は3です。これに対応する脆弱性「ウイルス対策ソフト未導入」の値は3です。以上から、サーバYの完全性に関するウイルス感染のリスクの値 $=3 \times 3 \times 3 = 27$ (ケ)になります。

空欄 d

【社内関連部門からの聴取内容】から、営業時間内の調達オンライン入力処理などで取引情報が利用されており、これら进行处理するシステムは、メンテナンス以外では「年間4時間以上停止することは許されない」ので、サーバYの利用停止時間が4時間以上になることは容認されません。よって、表3の可用性の評価基準の「定期メンテナンス以外で年間5時間までの利用停止は容認される」には該当せず、その下の「定期メンテナンス以外で年間1時間までの利用停止は容認される」に該当します。し

たがって、サーバYの可用性の値は3(ウ)になります。

設問2 リスク対応

表7から、完全性に関する受容可能なリスク水準の値は15です。表8のうち、リスクの値がこの値より大きいのは、脅威“ウイルス感染”だけです。この脅威に対応する脆弱性である“ウイルス対策ソフト未導入”を解決してリスクの値を小さくするためには、イの「ウイルス対策ソフト

を導入する」というリスク対応を行うのが適切です。イ以外の対応ではウイルス対策ソフトの導入が行われないので、リスクの値を小さくすることはできません。

解答

設問1 a:ウ b:キ c:ケ d:ウ

設問2 イ

問2

ログ管理システムに関する次の記述を読んで、設問1～5に答えよ。

中堅の製造業であるB社では、他社で発生した情報漏えい事件を受けて、社内の業務システムへの不正アクセスを早期に検知するための仕組みを強化することになった。B社では、業務システムのアクセスログ(以下、ログという)を一元管理するために、ログ管理システムを構築することにした。ログ管理システムの対象になる業務システムは、図1のネットワーク構成図に示す、勤務管理システム、販売管理システム、生産管理システム及び品質管理システムの四つである。各管理システムには、1台のサーバが割り当てられている。

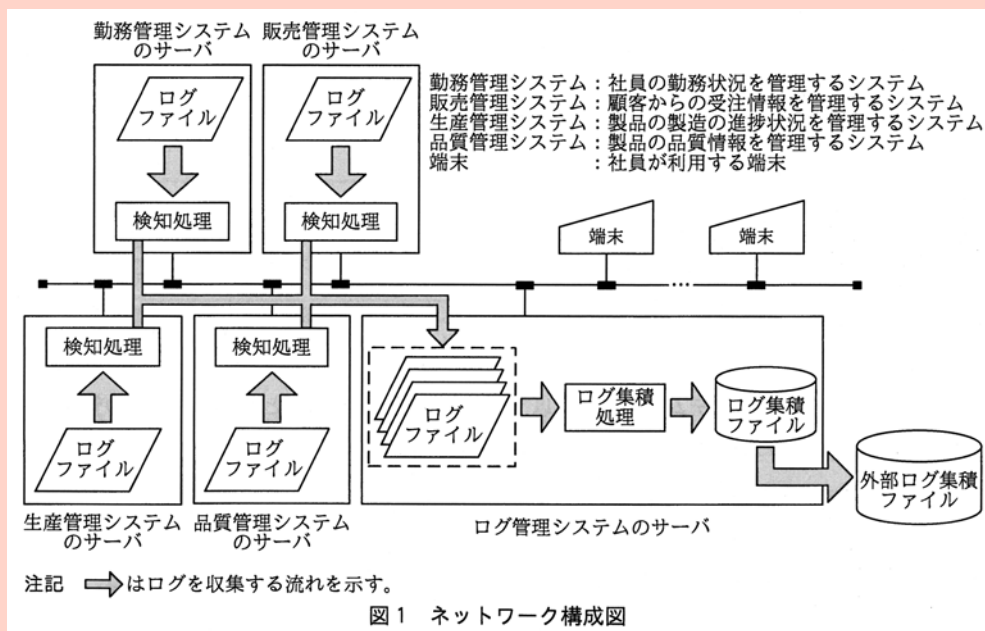


図1 ネットワーク構成図

〔業務システムの利用とログの説明(抜粋)〕

B社の社員は、固定のIPアドレスが設定されている端末から、一意に社員を特定できる社員IDで、業務システムのうちの一つにログインし、“参照”、“更新”、“ダウンロード”の操作を行う。社員が、業務システムにログインしたときに“参照”のログがログファイルに書き込まれる。また、ダウンロードの都度、そのデータ量を記録したログがログファイルに書き込まれる。一人の社員が、同時に複数の業務システムを使わないこと、及び、業務システム全体からデータを1日に5Mバイトを超えてダウンロードしないことを業務システムの利用規程で定めている。

〔ログ管理システムの概要(抜粋)〕

業務システムの各サーバ上のログファイルにログが書き込まれると、各業務システムに組み込まれている検知処理が、ログの書き込みを検知し、そのログをログ管理システムのサーバ上の業務システム別のログファイルに書き込む。書き込まれたログは、ログ管理システムのログ集積処理が、各業務システムのログを一元管理するログ集積ファイルに書き込む。ログには、業務システムを識別するための業務IDや、社員が実施した操作を示す、“参照”、“更新”、“ダウンロード”の操作種別などが含まれている。

〔ログ管理システムの要件(抜粋)〕

- (1) ログ集積ファイルを基に、いつ、誰が、どの端末からどの業務システムをどのように操作したかが追跡できる。
- (2) ログ管理システムのサーバ上のログファイルに書き込む処理は、ログ管理システムへのログインを必要とする。
- (3) ログ管理システムの管理者(以下、ログ管理者という)と業務システムの管理者(以下、業務システム管理者という)だけが、ログ集積ファイルを参照できる。
- (4) ログ管理者は、ログ集積ファイルをログ管理システムから外部の機器に出力することができる。
- (5) ログ管理システムから外部の機器に出力される外部ログ集積ファイルには、改ざんと漏えいを防止する対策を講じる。
- (6) 各サーバ間の通信には、公開鍵暗号方式を利用する。
- (7) ①ログ集積ファイルに書き込まれたログが一定条件を満たした際には、電子メールでログ管理者に通報する。

〔ログ管理システムの概要(抜粋)〕及び〔ログ管理システムの要件(抜粋)〕を基に、表1のログ管理システムの仕組み(抜粋)と、表2のログ管理システムへのアクセス権限表(抜粋)を作成した。

表1 ログ管理システムの仕組み(抜粋)

No.	要件	仕組み
1	ログ管理システムのログ集積ファイルを基に、いつ、誰が、どの端末からどの業務システムをどのように操作したかが追跡できる。	・業務システムに組み込まれた検知処理が、ログ管理システムのサーバ上のログファイルに書き込む。 ・ログファイルのログをログ集積ファイルに書き込む。 ・ a 。
2	ログ管理システムから外部の機器に出力される外部ログ集積ファイルには、改ざんと漏えいを防止する対策を講じる。	・ b 。 ・ c 。

表2 ログ管理システムへのアクセス権限表(抜粋)

	ログ管理システムへのログイン	ログファイルへのアクセス	ログ集積ファイルへのアクセス
ログ管理者	可		RE
業務システム管理者	可		R
検知処理	d1	d2	

注記 網掛けの部分は表示していない。

Rは参照、Eは外部へ出力、Wは書き込みを示す。

設問 1 表1中の ～ に入れる要件を満たす仕組みとして適切な答えを、解答群の中から選べ。

aに関する解答群

- ☐ ア 各業務システムの稼働状況を監視する
- ☐ イ 各業務システムの時刻を同期させる
- ☐ ウ 検知処理のログ管理システムへのアクセスを監視する
- ☐ エ ログ集積ファイルへのアクセスを監視する
- ☐ オ ログ集積ファイルを圧縮する

b, cに関する解答群

- ☐ ア 同一内容の複数個のログ集積ファイルを出力する
- ☐ イ ログ集積ファイルに電子署名を付加する
- ☐ ウ ログ集積ファイルの出力に当たっては、推測しにくい名称を付ける
- ☐ エ ログ集積ファイルのログ中の個人情報を削除する
- ☐ オ ログ集積ファイルを圧縮する
- ☐ カ ログ集積ファイルを暗号化する

設問 2 ログ管理システムの要件を満たすために、日時、操作種別以外で全てのログに共通して含むべき項目を全て挙げた適切な答えを、解答群の中から選べ。

解答群

- ☐ ア 業務ID, 社員ID
- ☐ イ 業務システムのサーバのIPアドレス, 業務ID
- ☐ ウ 業務システムのサーバのIPアドレス, 業務ID, 社員ID
- ☐ エ 端末のIPアドレス, 業務ID, 社員ID
- ☐ オ 端末のIPアドレス, 社員ID

設問 3 表2中の , に入れる適切な答えを、解答群の中から選べ。ここで、d1とd2に入れる答えは、解答群の中から組合せとして適切なものを選ぶものとする。

解答群

	d1	d2
☐ ア	可	RE
☐ イ	可	W
☐ ウ	不可	E
☐ エ	不可	RE
☐ オ	不可	RW
☐ カ	不可	W

設問 4 業務システムの検知処理はログ管理システムのサーバ上のログファイルへ書き込む。この通信を暗号化するために最低限必要な公開鍵の数として適切な答えを、解答群の中から選べ。

解答群

- ☐ ア 1
- ☐ イ 4
- ☐ ウ 8
- ☐ エ 12

設問 5 ログ集積ファイルを基に、業務システムへの不正アクセスを早期に検知するために、〔ログ管理システムの要件(抜粋)〕の下線①で言及している一定条件として適切な答えを、解答群の中から二つ選べ。ここで、解答群は、同じ社員IDのログに対する条件とする。

解答群

- ア 1日中“参照”のログだけが書き込まれたとき
- イ 1日の間に“更新”のログが1回以上、書き込まれたとき
- ウ ある業務システムの連続した“更新”のログの間に、別の業務システムのログが書き込まれたとき
- エ 同じ業務システムの“参照”と“更新”のログが連続して書き込まれたとき
- オ 業務システムからダウンロードされたデータ量が1日で5Mバイトを超えたとき
- カ 特定の業務システムの“参照”のログが15分間、書き込まれていないとき

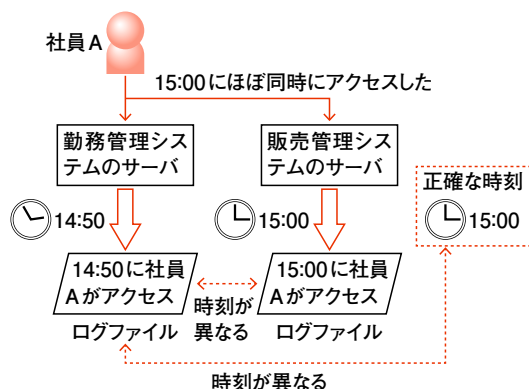
解説

業務システムのアクセスログ(以下、ログという)の管理を題材としている問題です。

設問の解説に入る前に【サーバの時刻同期】【デジタル署名】について解説します。

【サーバの時刻同期】

ログを管理する際には、複数のサーバの時刻を同期させることが重要になります。サーバの時刻が異なっていると次のようになるので、本問の「一人の社員が、同時に複数の業務システムを使わない」という利用規程に違反しているかどうかを検知できません。



上の図は、勤務管理システムのサーバの時刻が正確な時刻から10分遅れている状態で、社員Aが勤務管理システムと販売管理システムにアクセスしたときの状況です。

勤務管理システムのサーバの時刻が遅れているので、社員がアクセスした正確な時刻をログに残すことができなくなります。また、社員Aが二つのシステムに同時

にアクセスしたにもかかわらず、勤務管理システムへのアクセスの10分後に販売管理システムにアクセスしたように、ログファイルに記録されます。後に管理者がログファイルを参照しても、社員Aが二つのシステムに同時にアクセスしたことを確認できません。

以上のような問題以外にも、サーバの時刻がずれていると、同じ社員が行った操作の記録が、ログファイル中で時系列順に並ばなくなるなどの問題があります。よって、ログを記録する場合には、全てのサーバの時刻を同期させるのが適切な措置です。

【デジタル署名】

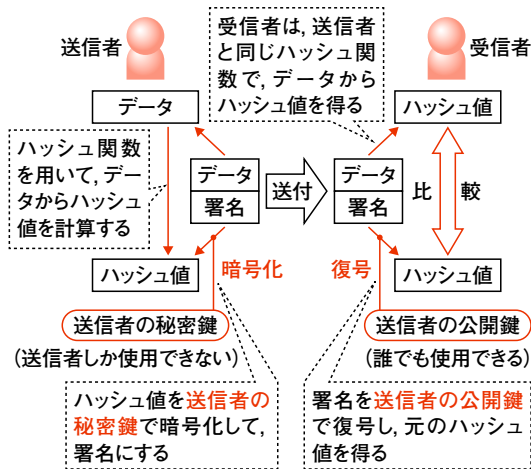
デジタル署名は、公開鍵暗号方式を応用して、利用者認証やなりすましの防止、及び改ざんの検知を実行するための技術です。電子署名ともいいます。

受信者は、送信者と同じハッシュ関数を用いてデータ本体からハッシュ値を生成します。また、送信者の署名を送信者の公開鍵で復号して、元のハッシュ値を入手します。この二つのハッシュ値が一致すれば、送信者本人がデータを送ってきたことを確認できます。送信者以外は使用できない送信者の秘密鍵で送信者の署名が暗号化されているので、そのデータが確かに送信者本人の管理下にあったと証明できるからです。

ハッシュ関数には、入力するデータの内容がわずかでも異なると、出力されるハッシュ値の内容が大きく異なるという性質があります。送信されたデータが送信経路上で改ざんされた場合、改ざんされる前のデータから作成されたハッシュ値と、改ざんされた後のデータ本体から作成されたハッシュ値が異なるので、改ざんが

あったことを検知できます。

● デジタル署名の作成・送信・検証



設問 1 ログ管理システムの仕組み

空欄 a

表 1 の No. 1 の要件は、「…… ログ集積ファイルを基に、いつ、誰が、どの端末からどの業務システムをどのように操作したかが追跡できる」ことです。この要件を満たすためには、ログ集積ファイルに書き込まれたログの中に、

- いつ(日時)
- 誰が(一意に社員を特定できる社員 ID)
- どの端末から(端末を識別できる固定の IP アドレス)
- どの業務システムを(業務システムを識別する業務 ID)
- どのように操作したか(“参照”, “更新”, “ダウンロード” の操作種別)

を特定するための情報が必要です。したがって、上記の括弧内の情報がログに含むべき項目です。

ただし、【サーバの時刻同期】で説明したように、サーバの時刻が異なっていると、社員がアクセスした日時と異なる日時がログに記録されるので、社員がアクセスした正確な時刻を確認できなくなります。よって、**各業務システムの時刻を同期させる**(㊦)ことが、要件を満たす仕組みとして適切です。

空欄 b, c

表 1 の No. 2 の要件は、「…… 外部ログ集積ファイルには、改ざんと漏えいを防止する対策を講じる」ことです。この要件を満たすためには、外部ログ集積ファイルの改ざんを検知するための電子署名(デジタル署名)

と、外部ログ集積ファイルが攻撃者に盗まれても、その内容を読み取られないようにするための暗号化が必要です。**ログ集積ファイルに電子署名を付加する**(㊦)と、**ログ集積ファイルを暗号化する**(㊧)が正解です。

設問 2 ログに含むべき項目

設問 1 空欄 a の解説から、ログ管理システムの要件を満たすためにログに含むべき項目は、日時、社員 ID、端末の IP アドレス、業務 ID、及び操作種別です。「日時、操作種別以外」を解答するので、**端末の IP アドレス、業務 ID、社員 ID**(㊦)が正解です。

設問 3 ログのアクセス権限

空欄 d1

業務システムの検知処理では、ログ管理システムのサーバ上のログファイルにログを書き込みます。〔ログ管理システムの要件(抜粋)〕の(2)から、ログ管理システムのサーバ上のログファイルに書き込む処理は、ログ管理システムへのログインを必要とするので、検知処理はログ管理システムへのログインを可能にしなければなりません。空欄 d1 には「可」が入ります。

空欄 d2

業務システムの検知処理では、ログ管理システムのサーバ上のログファイルにログを書き込む必要があるため、表 2 の検知処理の「ログファイルへのアクセス」を「W」にするのが適切です。

以上から、㊦の組合せが正解です。

設問 4 暗号化

公開鍵暗号方式を利用して暗号化を行う場合、データの送信者は、受信者の公開鍵を用いてデータを暗号化します。受信者の公開鍵で暗号化したデータは、受信者の公開鍵では復号できないので、他の人が受信者の公開鍵を使っても、暗号化されたデータを復号して内容を盗聴することは不可能です。よって、ネットワーク上に受信者の公開鍵を一つだけ用意しておけば、他の全ての人は受信者に対して暗号化したデータを安全に送信できます。

業務システムの検知処理をログのデータの送信者、ログ管理システムのサーバを受信者と考えれば、両者間の通信を暗号化するためには、ログ管理システムのサー

バの公開鍵を一つだけ用意しておけばよくなります。

アが正解です。

設問5 不正アクセスの検知

業務システムの利用規程では、次の事項を定めています。

① 一人の社員が、同時に複数の業務システムを使わないこと

② 業務システム全体からデータを1日に5Mバイトを超えてダウンロードしないこと

ログ集積ファイルに記録されたログの内容から、①、②の事項に違反したかどうかを検知するためには、次のようにするのが適切です。

①について：一人の社員が同時に複数の業務システムを使うと、ある業務システムへの操作がログに記録されると同時に、別の業務システムへの操作がログに記録されるので、ある業務システムの連続した「更新」のログの

間に、別の業務システムのログが書き込まれます。よって、**ウ**の条件からこの不正アクセスを検知できます。

②について：〔業務システムの利用とログの説明(抜粋)〕で「ダウンロードの都度、そのデータ量を記録したログがログファイルに書き込まれる」と説明されているので、一人の社員が、業務システムからダウンロードしたデータ量が1日で5Mバイトを超えると、そのデータ量がログファイルに書き込まれます。よって、**オ**の条件からこの不正アクセスを検知できます。

以上から、**ウ**、**オ**が正解です。

° 解答 °

設問1 a:**イ** b:**イ** c:**カ**(b, c順不同)

設問2 **エ** 設問3 **イ** 設問4 **ア**

設問5 **ウ**, **オ**

問3

セキュリティ事故の対応に関する次の記述を読んで、設問1～4に答えよ。

自転車用品の中堅通信販売会社のD社では、顧客からの注文を郵便及び電話で受け付けていた。顧客へのサービスの拡大を目的として、インターネットを利用した会員制のサービスを開始することとした。

会社の紹介だけを掲載していた従来のWebサイトを改修し、Webサイトでの会員情報の登録及び修正、会員に対するWebサイトでの商品の販売並びに会員向けのメールマガジン送付の登録を行う。

なお、Webサイトでの商品の販売における決済手段はクレジットカードだけとする。

改修後のWebサイトは、D社のDMZ上に設置されたWebサーバと、社内LAN内に設置されたデータベースサーバで構成される。データベースサーバのデータは平文で保存しており、会員情報の登録及び修正、商品の販売並びに会員向けのメールマガジン送付の登録を行う際には、SSLによってネットワーク経路の暗号化を行う。

〔会員情報の登録〕

D社では、Webサイトで取得する個人情報の利用目的を、注文の受付、決済、商品の配送、及びメールマガジンの送付に限定し、会員登録の希望者に対し、登録時に利用目的を通知して同意を得ることとした。同意を得た会員に対しては、会員情報として次の情報を登録してもらうこととした。

【全員に登録してもらう情報】

利用者ID、パスワード、メールアドレス、メールマガジン送付の有無

【任意に登録してもらう情報】

性別、生年月日

【商品を購入する会員に登録してもらう情報】

氏名、配送先住所、電話番号、クレジットカードの発行会社名、

〔セキュリティ事故の発生〕

複数の会員から、“D社のサービスに登録したメールアドレス宛てに迷惑メールが大量に送られてくるようになった”との連絡がお客様相談窓口に入った。さらに、連絡があった会員のうち数名については、迷惑メールの宛先メールアドレスはD社以外のサービスでは利用していないことが分かった。

この報告を受けてD社の情報システム部のY部長は、会員情報が漏えいしている可能性がある判断した。また、会員情報として登録されているクレジットカード情報が漏えいしていることも考えられると判断した。そこで、情報システム部のWebサイト担当者Z氏に対し、Webサイトを停止して調査するよう指示した。

Z氏の調査の結果、D社のWebサイトにおいて、会員が利用者IDとパスワードの入力を行うログインの処理に不備があり、外部からSQLインジェクション攻撃を受けていたことが判明した。

〔セキュリティ事故への対応〕

Z氏は、一般的なWebサイトにおけるセキュリティ事故に関して考えられる対策と対応を調査し、今回のセキュリティ事故において会員とWebサイトに対して必要と思われる対策と対応を表1にまとめて、Y部長に報告した。

表1 セキュリティ事故の対策と対応の概要

対象	対策と対応
会員	① 全ての会員に対する謝罪 ② 事故の公表と被害状況の説明 ③ 会員への事故対応の依頼
Web サイト	④ 被害状況の把握及び原因の特定 ⑤ SQLインジェクション攻撃を防ぐためのWebサイトの改修 ⑥ Webサイトへのアクセスの常時監視 ⑦ ネットワークを介した攻撃によるネットワークアクセス負荷上昇に対応するためのネットワーク回線の二重化

Y部長は、表1の⑦は実施を見合わせ、Z氏に①～⑥の実施を急がせるとともに、更なる情報セキュリティ対策の実施を指示した。

設問 1 今回受けたSQLインジェクション攻撃に関する記述として適切な答えを、解答群の中から選べ。

解答群

- ア** 攻撃者がDNSに登録されたドメインの情報を改ざんすることによって、利用者をフィッシングサイトに誘導し、そこで入手した利用者IDとパスワードを用いて、データベースを不正に操作した。
- イ** 攻撃者が、D社のWebサイトの入力項目に対し、命令文を送り込むことによって、データベースを不正に操作した。
- ウ** 攻撃者がD社のデータベースの管理ツールを入手し、管理ツール経由で直接D社のデータベースを不正に操作した。
- エ** 攻撃者がネットワーク上で情報の盗聴を行い、D社のデータベースの管理者のIDとパスワードを入手し、データベースを不正に操作した。

設問 2 表1中の③に関して、今回のセキュリティ事故の対応として適切な答えを、解答群の中から選べ。

解答群

- ア** 安易なパスワードの設定を防止するために、パスワードは英字、数字、記号が混在する8文字以上のものにするよう会員に依頼する。
- イ** 攻撃を受けた場合の被害を抑えるために、メールマガジン購読だけを利用する会員の会員情報を格納したデータベースと商品の購入を行う会員の会員情報を格納したデータベースとを分離し、商品の購入を行う会員だけには、利用者ID及びパスワードの変更を依頼する。
- ウ** 個人情報の目的外利用を避けるために、D社が取得する個人情報の利用目的に事故の対応を追加し、同意を会員に依頼する。
- エ** クレジットカード情報が漏れいしている場合の不正利用を防止するために、登録されたクレジットカードの停止及び番号変更の手続を会員に依頼する。

設問 3 表1中の⑦に関して、Y部長が実施を見合わせた理由として適切な答えを、解答群の中から選べ。

解答群

- ア** Webサーバの増設が必要となる。
- イ** 稼働中のサービスの停止が必要であり、事業への影響が大きい。
- ウ** 今回のSQLインジェクション攻撃を防ぐ対策にならない。
- エ** セキュリティ事故発生時に攻撃者の侵入経路の特定に時間が掛かる。

設問 4 Y部長は、Z氏に事故の再発防止のために更なる情報セキュリティ対策の実施を指示した。次の記述中の **a** ～ **c** に入れる適切な答えを、解答群の中から選べ。

〔SQLインジェクション攻撃への追加対策〕

SQLインジェクション攻撃は、システム開発の際にセキュリティを考慮した設計及び実装を行うことで回避できる。例えば、**a** ことで、アプリケーション開発時に脆弱性が作り込まれる可能性を減らすこととする。

〔会員情報に対するその他のセキュリティ対策〕

会員情報を格納したデータベースサーバへの不正アクセス対策として、**b** こととする。また、情報漏えいが発生した場合の原因の分析や犯人の追跡を行うための証拠の確保には、**c** を行うこととする。

aに関する解答群

- ア** 開発担当者と運用担当者の職務を分離する
- イ** 開発用の端末と通常利用の端末を分離する
- ウ** 瑕疵の発生に備えた保険に加入する
- エ** 機密保持に関する誓約書を作成する
- オ** セキュアプログラミングのルールを作成する
- カ** 負荷分散装置を設置する

bに関する解答群

- ア Webサーバとデータベースサーバの時刻を同期させる
- イ 会員情報を暗号化する
- ウ 社内からのインターネット利用時にフィルタリングを実施する
- エ 共有IDを利用する
- オ データベースサーバをRAID構成にする

cに関する解答群

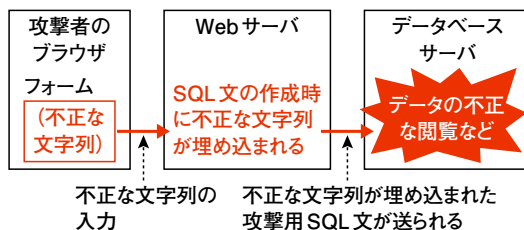
- ア アクセスログやエラーログの保管
- イ 外部記憶媒体の利用禁止を明文化
- ウ 業界団体との連携によるセキュリティ事故情報の共有
- エ 担当する業務に応じた情報セキュリティ教育の実施
- オ 内部不正に対する罰則の強化

解説

Webサービスに対する攻撃手法やセキュリティ事故への対応をテーマとした問題です。

設問1 SQLインジェクション

SQLインジェクションとは、Webページ上の入力フォームの項目に不正な文字列を入力し、その文字列から生成されたSQLの命令文を不正なものにして、Webアプリケーションを誤動作させたり、データベースの内容を不正に閲覧または削除したりする攻撃方法のことです。



一般的なDBMSでは、「;」（セミコロン）で区切って複数のSQL文を一括して実行できる仕様になっています。例えば、「SELECT～FROM～…; UPDATE～SET～…」というSQL文を作成すれば、SELECT文の実行後にUPDATE文も実行されます。したがって、SELECT文の後にDELETE文を実行させるようなSQL文を不正に作成すれば、特定のテーブルのレコードが全て削除されてしまいます。

例として、検索したい名前の文字列（文字列Xとする）をWebページの入力フォームに入力させるWebアプリ

ケーションシステムを考えます。このシステムのWebページから呼び出されるCGIの処理中では、

```
SELECT * FROM TABLE_A WHERE name  
like '文字列X'
```

のように、列nameの値が文字列Xと等しい行のみを検索するSQL文を作成します。この入力フォームに、例えば「';DELETE FROM TABLE_A WHERE 'A'='A)」のような文字列が入力可能になっていると、以下のようなSQL文が作成されてしまいます。

```
SELECT * FROM TABLE_A WHERE name  
like ''';DELETE FROM TABLE_A WHERE  
'A'='A'
```

後半のDELETE文の条件（'A'='A'）は、TABLE_Aの内容にかかわらず常に成立します。よって、全ての行がWHERE以降の条件式に適合しているとみなされ、TABLE_Aの全部の行が削除されてしまうことになります。

この入力フォームでは、「'」のような、SQL文中で使われる「データベースの操作・問合せにおいて特別な意味をもつ」文字が入力可能であったため、問題が発生したことになります。よって、入力値から「'」、「"」などの特別な文字を取り除く（エスケープ処理をする）ことで、SQLインジェクションは防止できます。

また、バインド機構の使用によっても、SQLインジェクションを防止できます。バインド機構とは、変数部分に仮の文字列（静的プレースホルダ）をあてはめて作成された「SQL文の雛形」をあらかじめ用意しておき、Webページから変数（データ）が入力された際には、その変

数にエスケープ処理を施して得られた変数(バインド変数)を、SQL文の雛形にあてはめて実行する方式です。変数は自動的にエスケープ処理されてあてはめられるため、安全にSQL文を実行できます。

解答群の中でSQLインジェクション攻撃に関する記述として適切なものは**イ**です。**ア**は、DNSキャッシュポイズニングという攻撃手法の説明です。SQLインジェクション攻撃では、データベースの管理ツールなどを入手しなくても攻撃が可能なので、**ウ**の記述は不適切です。また、D社のWebサイトでは、会員情報の登録などにおいてSSLでネットワーク経路の暗号化を行っているため、攻撃者がネットワーク上で情報の盗聴を行っても、IDなどの情報を入手することは困難です。**エ**の記述は不適切です。

設問2 セキュリティ事故後の対応

【会員情報の登録】の説明から、商品を購入する会員には、クレジットカードの発行会社名、クレジットカード番号などの、クレジットカード情報をD社のWebサイトに登録してもらっています。また、【セキュリティ事故の発生】において、IDやパスワードなどの他にクレジットカード情報が漏えいした可能性があると説明されています。攻撃者が、D社のWebサイトを攻撃して入手したクレジットカード情報を悪用して、D社の会員のクレジットカードで不正に購入を行うことで、会員が金銭的な損害を被る可能性があります。

よって、登録されたクレジットカードの停止や番号変更の手続きを会員に依頼してもらい、損害の発生を防止する必要があるため、**エ**が適切です。

- × **ア** 会員がパスワードを英字、数字、記号が混在するものにしても、そのパスワードがSQLインジェクション攻撃によって盗まれた場合、攻撃者がパスワードを悪用できるので、今回のセキュリティ事故の対応として不適切です。
- × **イ** メールマガジン購読だけを利用する会員の会員情報を格納したデータベースと、商品の購入を行う会員の会員情報を格納したデータベースとを分離しても、両方のデータベースに対してSQLインジェクション攻撃を仕掛けられれば、全ての会員の会員情報を盗まれるので意味がありません。
- × **ウ** 今回のセキュリティ事故では、SQLインジェクション攻撃を防げなかったことが問題であり、個

人情報の利用に不備があったわけではないので、このような対応をとっても事故の再発防止などには繋がりません。

○ **エ** 正解です。

設問3 アクセス負荷対策

ネットワーク回線を二重化することで、DoS (Denial of Service) 攻撃などの、ネットワークアクセスの負荷を上昇させる種の攻撃を防ぐことができます。しかし、今回のセキュリティ事故の原因になったSQLインジェクション攻撃では、ネットワークアクセスの負荷を増加させることはないため、ネットワーク回線の二重化は有効な対策にはなりません。よって、**ウ**が正解です。

- × **ア** ネットワーク回線を二重化する際にWebサーバを増設するとは説明されていないので、Webサーバの増設は不要です。
- × **イ** 既存のネットワーク回線を用いてサービスを提供している間に、追加するネットワーク回線の導入や設置などを行えば、サービスを継続したままネットワーク回線を二重化することが可能なので、不適切な記述です。

○ **ウ** 正解です。

- × **エ** セキュリティ事故発生時に攻撃者の侵入経路の特定をするためには、アクセスログを取得する必要があります。ネットワーク回線の二重化と侵入経路の特定とは特に関連はありません。

設問4 セキュリティ事故防止

空欄a

「**a**」ことで、アプリケーション開発時に脆弱性が作り込まれる可能性を減らすことができる」と説明されているので、空欄aにはアプリケーション開発に関連する字句が入ります。解答群のうち、アプリケーション開発に関連するのは**オ**(セキュアプログラミングのルールを作成する)です。セキュアプログラミングのルールを作成して開発を行うことで、SQLインジェクション攻撃を防ぐためにバインド機構を利用するなど、アプリケーションのプログラムを適切な方法で作成できるようになります。**オ**以外の記述では、アプリケーション開発時に脆弱性が作り込まれる可能性を減らすことは困難です。

空欄b

会員情報を格納したデータベースサーバが攻撃を受

けて、会員情報が盗まれた場合にも被害を最小にするためには、格納された会員情報を暗号化し、攻撃者が会員情報を判読できないようにするのが適切です。よって、**イ**が正解です。**イ**以外の対策を用いても、データベースサーバが外部からの攻撃を受けて会員情報が盗まれることには対応できません。

空欄 c

情報漏えいが発生した場合の原因の分析や犯人の追跡を行うためには、サーバ上やネットワーク機器上でアクセスログやエラーログを採取し、Webサーバなどにアクセスしてきたコンピュータの送信元IPアドレスや、

不正アクセスの疑いがあるアクセスを行ってエラーを発生させた会員のIDなどの情報を取得して、不正アクセスの証拠を確保するのが適切です。**ア**が正解です。**ア**以外の対策では、不正アクセスの送信元の情報を採取できないので、誤りです。

解答

設問 1 **イ** 設問 2 **エ** 設問 3 **ウ**
設問 4 a: **オ** b: **イ** c: **ア**

第②回 模擬試験

情報セキュリティ マネジメント

- 午前 問題 218
(全 50 問 試験時間：1 時間 30 分)
- 午後 問題 252
(全 3 問 試験時間：1 時間 30 分)

本章で取り上げる問題文は、情報処理技術者の試験で過去に出題された問題の中から著者が精選して構成したものです。

第2回 模擬試験 午前 問題

☐
☐
☐

問 1 完全性を脅かす攻撃はどれか。

- ア Web ページの改ざん
- イ システム内に保管されているデータの持出しを目的とした不正コピー
- ウ システムの過負荷状態をねらうDoS 攻撃
- エ 通信内容の盗聴

☐
☐
☐

問 2 JIS Q 27002における情報資産に対する脅威の説明はどれか。

- ア 情報資産に害をもたらすおそれのある事象の原因
- イ 情報資産に内在して、リスクを顕在化させる弱点
- ウ リスク対策に費用をかけないでリスクを許容する選択
- エ リスク対策を適用しても解消しきれずに残存するリスク

☐
☐
☐

問 3 米国NISTが採用したAES (Advanced Encryption Standard)における鍵長の条件はどれか。

- ア 128, 192, 256ビットから選択する。
- イ 256ビット未満で任意に指定する。
- ウ 暗号化処理単位のプロック長より32ビット大きくする。
- エ 暗号化処理単位のプロック長より32ビット小さくする。

☐
☐
☐

問 4 100人の送受信者が共通鍵暗号方式で、それぞれ秘密に通信を行うときに必要な共通鍵の総数は幾つか。

- ア 200
- イ 4,950
- ウ 9,900
- エ 10,000

解説

問 1 完全性

JIS Q 27001 (ISO/IEC27001)などの情報セキュリティの規格によって示される「情報セキュリティの3要素」の一つである「完全性」とは、情報(データ)が正確かつ完全であること、言い換えれば、権限のないユーザから不正にデータを書き換え・改ざんされないことを指します。

- ア 正解です。
- × イ システム内のデータの持出しによって、権限のない利用者などにデータが不正に公開されることになるため、機密性が損なわれることになります。よって、この攻撃は機密性を脅かす攻撃となります。
- × ウ システムにDoS 攻撃がかけられてシステムが停止した場合、利用したいときにシステムが利用できなくな

るため、可用性が損なわれることになります。よって、この攻撃は**可用性**を脅かす攻撃となります。

- × **エ** 通信内容の盗聴によって、権限のない利用者や悪意の第三者などに通信内容のデータが不正に公開されることになるため、機密性が損なわれることになります。よって、この攻撃は**機密性**を脅かす攻撃となります。

問 2 脅威

JIS Q 27002とは、組織における情報セキュリティマネジメントの導入、実施、維持及び改善のための指針及び一般的原則を規定しているJIS規格のことです。

JIS Q 27002では、「システム又は組織に損害を与える可能性があるインシデントの潜在的な原因」を、「**脅威**」と定義しています。インシデントとは、望まない単独もしくは一連の情報セキュリティ事象、または予期しない単独もしくは一連の情報セキュリティ事象のことです。すなわち、脅威とは「(システムや組織中の)情報資産に害をもたらすおそれのある事象の原因」のことです。

- **ア** 正解です。
- × **イ** 情報資産に内在してリスクを顕在化させる弱点のことを、**脆弱性**といいます。
- × **ウ** リスク対策に費用をかけないでリスクを許容する選択のことを、**リスク保有**といいます。
- × **エ** リスク対策を適用しても解消できず、残ってしまうリスクのことを、**残留リスク**といいます。

問 3 AES

AESは、NIST(米国商務省標準技術局)が制定した共通鍵暗号方式です。1977年に制定された共通鍵暗号方式であるDESの改善版として公募され、2000年に決定した方式です。この暗号方式では暗号化に使用する鍵(暗号化鍵)のビット長(鍵長)を、128ビット、192ビットまたは256ビットのうちのいずれかから選ぶことができます。

- **ア** 正解です。
- × **イ** AESでは、任意の鍵長を選択することはできません。
- × **ウ、エ** 暗号化処理単位のブロック長と鍵長には、特に関係がありません。

問 4 共通鍵暗号方式

暗号化などに用いられる鍵の方式のうち、**共通鍵暗号方式**では、相異なるn人の相手とそれぞれ秘密の通信を行いたい場合、自分と各相手との間で共有する共通鍵もn個必要となります。

例えば、4人の送受信者がいると仮定します(A、B、C、Dとする)。また、以下の説明では送受信者XとYとの間で使用する共通鍵を“XY_k”と呼びます。

Aが他の3人と秘密の通信を行いたい場合、AB_k、AC_k、AD_kの3つが必要となります。また、Bが他の3人と秘密の通信を行いたい場合、Aに対する鍵はAB_kを使用すればよいので新たに用意する必要はありません。残りのC、Dに対して、それぞれBC_k、BD_kが必要となります。Cが他の3人と秘密の通信を行いたい場合、A、Bに対する鍵はそれぞれAC_k、BC_kを使用すればよいので新たに用意する必要はなく、Dに対するCD_kのみが必要です。

よって、4人の送受信者がいる場合は、3(AB_k、AC_k、AD_k)+2(BC_k、BD_k)+1(CD_k)=6個の共通鍵を要します。

同様に考えると、5人の送受信者がいる場合は4+3+2+1=10個、10人の送受信者がいる場合は9+8+7+...+2+1=45個、...となるため、n人の送受信者がいる場合は $(n-1)+(n-2)+(n-3)+\dots+2+1=\frac{n(n-1)}{2}$ 個の共通鍵を必要とします。すなわち、この式にn=100を代入すると、 $\frac{100 \times 99}{2}=4,950$ (**イ**)となります。

○ 解答 ○

問 1 **ア**

問 2 **ア**

問 3 **ア**

問 4 **イ**



問 5

公開鍵暗号方式の用法によって、送信者が間違いなく本人であることを受信者が確認できる鍵の組合せはどれか。

- ア 送信者は自分の公開鍵で暗号化し、受信者は自分の秘密鍵で復号する。
- イ 送信者は自分の秘密鍵で暗号化し、受信者は送信者の公開鍵で復号する。
- ウ 送信者は受信者の公開鍵で暗号化し、受信者は自分の秘密鍵で復号する。
- エ 送信者は受信者の秘密鍵で暗号化し、受信者は自分の公開鍵で復号する。



問 6

公開鍵暗号方式によるデジタル署名のプロセスとハッシュ値の使用方法に関する記述のうち、適切なものはどれか。

- ア 受信者は、送信者の公開鍵で復号してハッシュ値を取り出し、元のメッセージをハッシュ変換して求めたハッシュ値と比較する。
- イ 送信者はハッシュ値を自分の公開鍵で暗号化して、元のメッセージと共に受信者に送る。
- ウ デジタル署名の対象とする元のメッセージは、それを変換したハッシュ値から復元できる。
- エ 元のメッセージ全体に対して公開鍵で暗号化を行い、ハッシュ値を用いて復号する。



問 7

企業内情報ネットワークやサーバにおいて、通常のアクセス経路以外で、侵入者が不正な行為に利用するために設置するものはどれか。

- | | |
|---------------|---------------|
| ア VoIP ゲートウェイ | イ ストリクトルーティング |
| ウ バックドア | エ フォレンジック |

解説

問 5 デジタル署名と公開鍵暗号方式

受信者が送信者を認証(確認)できるようにするため、及び改ざんの検知を行うために、**デジタル署名**が用いられます。デジタル署名は、**公開鍵暗号方式**の技術に応用したものです。

送信者は、送付データ全体に対してハッシュ関数を用いて、ハッシュ値を求めます。さらにそのハッシュ値を「送信者の秘密鍵」で暗号化し、これを「送信者の署名」としてデータと一緒に添付し、受信者に送付します。

受信者は、送信者と同じハッシュ関数を用いてデータ本体からハッシュ値を生成します。さらに、「送信者の署名」を「送信者の公開鍵」で復号して、元のハッシュ値を入手します。二つのハッシュ値が一致すれば、確かにそのデータは送信者からのものであると確認できます。送信者以外は知らない(使用できない)「送信者の秘密鍵」で「送信者の署名」の暗号化が行われているということは、そのデータが正しい送信者によって送信されたことと証明できるためです。

したがって、送信者が自分の秘密鍵で暗号化を行い、受信者が送信者の公開鍵で復号するという方法(イ)のみが適切となります。

- × ア 送信者の公開鍵は、送信者だけでなく誰でも自由に利用可能なため、送信者が自分の公開鍵を用いてデータを暗号化しても、そのデータの送信者が本人であることを確認できません。
- イ 正解です。
- × ウ 受信者の公開鍵は、受信者だけでなく誰でも自由に利用可能なため、送信者が受信者の公開鍵を用いてデータを暗号化しても、そのデータの送信者が本人であることを確認できません。

- × **エ** 受信者の秘密鍵は受信者が秘匿して管理しているため、送信者が受信者の秘密鍵を利用することはできません。

問 6 デジタル署名とハッシュ値

通信相手に送付するデータの正当性の証明と送信者の本人確認(なりすましの防止)のために、デジタル署名が用いられます。

データの送信者は、送付データ全体に対して**ハッシュ関数**を用いて**ハッシュ値**を求めます。さらにそのハッシュ値を「送信者の秘密鍵」で暗号化し、これを「送信者の署名」としてデータと一緒に添付し、受信者に送付します。

受信者は、送信者と同じハッシュ関数を用いてデータ本体からハッシュ値を生成します。さらに、「送信者の署名」を「送信者の公開鍵」で復号して、元のハッシュ値を入手します。二つのハッシュ値が一致すれば、そのデータは送信者からのものであると確認できます。送信者以外は使用できない「送信者の秘密鍵」で「送信者の署名」の暗号化が行われているということは、そのデータが確かに送信者の管理下にあったと証明できるためです。

なお、ハッシュ関数の性質より、ハッシュ値から元のデータを復元することはできないようになっています。

- **ア** 正解です。
- × **イ** デジタル署名の手続きでは、送信者はハッシュ値を自分の秘密鍵で暗号化するため、誤りです。
- × **ウ** デジタル署名を付ける元となったメッセージを、ハッシュ値から復元することはできません。
- × **エ** 元のメッセージを公開鍵で暗号化した場合は、公開鍵に対応する秘密鍵で復号することになります。ハッシュ値は、データの復号には利用できません。

問 7 不正なアクセス経路

サーバや企業内LANなどに侵入した不正侵入者が、後に再度侵入を試みたり、サーバ内の情報を後から盗んだりするために設置しておく不正なプログラムなどのことを、**バックドア**(**ウ**)といいます。バックドアは、正規のアクセス経路と異なる別の経路として設けられます。

- × **ア** **VoIPゲートウェイ**とは、VoIPによる通信において、パケット間隔のタイミング、音声の符号化・圧縮、インタフェース変換などの機能を司る装置のことです。
- × **イ** **ストリクトルーティング**とは、パケットの転送経路を最初のルータから最後のルータまで厳密に指定することです。
- **ウ** 正解です。
- × **エ** **フォレンジック**(デジタルフォレンジックス)とは、コンピュータ犯罪(不正アクセスなど)に対する科学的調査のことで、不正アクセスなどに関する証拠(記録・ログ)を立証するために必要な情報を、各種の手段をもって収集・分析すること(もしくはその手法のこと)です。

○ 解答 ○

問 5 **イ**

問 6 **ア**

問 7 **ウ**



問 8

生体認証システムを導入するときに考慮すべき点として、最も適切なものはどれか。

- ア システムを誤作動させるデータを無害化する機能をもつライブラリを使用する。
- イ パターンファイルの頻繁な更新だけでなく、ヒューリスティックなど別の手段を組み合わせる。
- ウ 本人のデジタル証明書を信頼できる第三者機関に発行してもらう。
- エ 本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する。



問 9

シングルサインオンの説明のうち、適切なものはどれか。

- ア クッキーを使ったシングルサインオンでは、サーバごとの認証情報を含んだクッキーをクライアントで生成し、各サーバ上で保存・管理する。
- イ クッキーを使ったシングルサインオンでは、認証対象の各サーバをそれぞれ異なるインターネットドメインにする必要がある。
- ウ リバースプロキシを使ったシングルサインオンでは、認証対象の各Webサーバをそれぞれ異なるインターネットドメインにする必要がある。
- エ リバースプロキシを使ったシングルサインオンでは、ユーザ認証においてパスワードの代わりにデジタル証明書を用いることができる。



問 10

公開鍵暗号方式を採用した電子商取引において、認証局(CA)の役割はどれか。

- ア 取引当事者の公開鍵に対するデジタル証明書を発行する。
- イ 取引当事者のデジタル署名を管理する。
- ウ 取引当事者のパスワードを管理する。
- エ 取引当事者の秘密鍵に対するデジタル証明書を発行する。

解説

問 8 生体認証

生体認証(バイオメトリクス認証)とは、指紋、網膜、顔の形状などの、人間の身体的特徴から個人の識別を行う認証システムのことです。このシステムでは、認証を受けるユーザの指紋の形状などと、登録した本人の指紋の形状などを比較し、両者の類似の度合いが一定以上であれば、本人と識別します。この度合いを「判定しきい値」と呼びます。

生体認証では、FRR(本人拒否率)とFAR(他人受入率)という2つのパラメタが重要となります。FRRは、正規のユーザ本人を他人と誤認識して拒否してしまう確率のことで、判定しきい値を厳しくするほど上昇します。FARは、他人を正規のユーザと誤認識して受け入れてしまう確率のことで、判定しきい値を緩くするほど上昇します。

生体認証システム導入時に考慮すべき点は、このFRRとFARの双方の値の許容上限値や下限値を勘案して、システムの判定しきい値を調節することです。

- × ア システムを誤作動させるデータを無害化するのは、サニタイジングの説明です。
- × イ パターンファイルだけでなく、ヒューリスティックなどの別の手段を組み合わせるのは、コンピュータウイルスを検出する手法の説明です。
- × ウ 生体認証システムでは、デジタル証明書などは不要となります。

○ **エ** 正解です。

問 9 シングルサインオン

シングルサインオンは、一度の利用者認証によって、複数のシステムやOSなどを利用可能とするための技術です。

現在、シングルサインオンの実現方式としては、「エージェント方式(エージェント型)」と「リバースプロキシ方式(プロキシ型)」などがあります。

エージェント方式：シングルサインオンを利用する各システムに、エージェントというソフトウェアを組み込む方式です。利用者が一度入力した認証情報は、エージェントソフトによって認証情報を含んだクッキーというデータに加工され、各システム間で自動的に授受されます。その後、各システムにおいてクッキー内の情報が検証され、認証の成否が確認されます。

リバースプロキシ方式：認証用のサーバ(認証サーバ)を設置し、利用者の認証及び各システムへのアクセスを認証サーバに引き受けさせる方式です。認証の成功後は、認証サーバはプロキシ(代理)サーバとして機能し、利用者から各システムに送られた接続要求をいったん受け取ります。その後、認証サーバは利用者の代理として各システムに接続し、接続要求を送ります。そして、各システムから返却された業務処理の応答データなどを、利用者に返します。

このリバースプロキシ方式では、ユーザ認証においてパスワードの代わりに、利用者が取得していたデジタル証明書を用いることもできます。よって、**エ**の記述が適切です。

- × **ア** クッキーを使ったシングルサインオンでは、認証情報を含んだクッキーをWebサーバが生成して、クライアントに送信する方法をとります。クライアントがクッキーを生成することはありません。
- × **イ** クッキーの技術的仕様により、あるWebサーバが生成したクッキーを、異なるインターネットドメイン上に存在する別のWebサーバへの認証に用いることはできなくなっています。クッキーを使ったシングルサインオンでは、認証対象のサーバを、同じインターネットドメインに配置することになります。
- × **ウ** リバースプロキシを使ったシングルサインオンでは、認証対象のWebサーバをそれぞれ異なるインターネットドメインに配置する必要はありません。

○ **エ** 正解です。

問 10 認証局

電子商取引の利用者がネットワーク上に公開している公開鍵が、本当にその利用者が作成して公開しているものかを証明するために、**電子証明書**(デジタル証明書)が用いられます。利用者は、信頼できる第三者機関である**認証局(CA)**に対して電子証明書の申請を行います。

認証局は、その利用者の正当性を戸籍謄本や会社の登記などによって確認し、その利用者が正当な個人・団体であれば、その利用者に対して電子証明書を発行します。電子証明書には「利用者の公開鍵」の他に、「認証局の秘密鍵」によってデジタル署名された「暗号化された認証局の署名」が含まれています。

○ **ア** 正解です。

- × **イ** 取引当事者のデジタル署名は、取引当事者自身が作成すべきものです。認証局は、デジタル署名の管理などにはかかわることはありません。
- × **ウ** 取引当事者のパスワードは、取引当事者自身が作成・管理すべきものです。
- × **エ** 取引当事者の秘密鍵は、取引当事者以外の者は使用できないように、取引当事者自身が厳重に管理すべきものです。認証局は、秘密鍵の作成などにかかわることはありません。

○ 解答 ○

問 8 **エ**

問 9 **エ**

問 10 **ア**



問 11 リスク移転を説明したものはどれか。

- ア** 損失の発生率を低下させること
- イ** 保険に加入するなど資金面での対策を講じること
- ウ** リスクの原因を除去すること
- エ** リスクを扱いやすい単位に分解するか集約すること



問 12 情報システムのリスク分析に関する記述のうち、適切なものはどれか。

- ア** リスクには、投機的リスクと純粹リスクとがある。情報セキュリティのためのリスク分析で対象とするのは、投機的リスクである。
- イ** リスクの予想損失額は、損害予防のために投入されるコスト、復旧に要するコスト、及びほかの手段で業務を継続するための代替コストの合計で表される。
- ウ** リスク分析では、現実に発生すれば損失をもたらすリスクが、情報システムのどこに、どのように潜在しているかを識別し、その影響の大きさを測定する。
- エ** リスクを金額で測定するリスク評価額は、損害が現実のものになった場合の1回当たりの平均予想損失額で表される。



問 13 ISMSプロセスのPDCAモデルにおいて、PLANで実施するものはどれか。

- | | |
|-----------------------|-------------------------|
| ア 運用状況の管理 | イ 改善策の実施 |
| ウ 実施状況に対するレビュー | エ 情報資産のリスクアセスメント |

解説

問11 リスク移転

情報システム上の脅威、脆弱性、リスクとは次のようなものです。

脅威：情報システムに対して悪い影響を与える要因のこと

脆弱性：情報システムや情報資産に存在する、脅威が顕在化する確率のこと

リスク：脅威が情報資産の脆弱性につけこみ、情報資産に損失などを与える可能性のこと

なお、リスク評価によってリスクの大きさを判断した上で決める各種の対策として、リスクコントロールやリスクファイナンスがあります。

リスクコントロール：リスクが現実のものにならないようにするための、または現実化したリスクによってもたらされる被害を最小限にするための対策です。リスクコントロールには、**リスク回避**(リスクそのものをなくすこと、または発生確率を低下させること)、**リスク集中**(リスクをもつ情報資産を集中管理すること)、**リスク分離**(リスクをもつ情報資産を分離させ、全体のリスク発生確率などを低減させること)などがあります。

リスクファイナンス：リスクが現実化したときに生じる損失金額を少なくするための対策です。リスクファイナンスには、**リスク移転**(保険に加入するなどの手段で資金面での対策を行い、リスク発生時の損失を他者に肩代わりさせること)や**リスク保有**(積立金などによって、損失を自社で負担すること)があります。

リスク移転として適切な記述は、保険に加入するなどの方法で資金面での対策を行う、**イ**となります。

× **ア** 損失の発生率を低下させるのは、リスク回避となります。

- **イ** 正解です。
- × **ウ** リスクの原因を除去するのは、リスク回避となります。
- × **エ** リスクを扱いやすい単位に分割したり集約したりするのは、リスクコントロールの一種である、リスク分離やリスク集中となります。

問12 リスク分析

リスク分析とは、情報システムのリスク、すなわち「現実には発生する可能性のある、様々な災害(地震・火災などの天災や、盗難・個人情報の漏えいなどの人災)などの出来事」について、情報システムのどこに、どのようにそれらのリスクが潜んでいるかを識別し、その可能性の大きさや被害額などを測定することを指します。

- × **ア** **純粋リスク**とは、発生することによってネガティブな結果だけが生じるリスク(災害など)のことです。**投機的リスク**とは、新製品の開発など、成功すればポジティブな結果(利益)を、失敗すればネガティブな結果(損失)をもたらす行為に関するリスクのことです。情報セキュリティのためのリスク分析では、純粋リスクを取り扱います。
- × **イ** 予想損失額には、災害そのものがもたらす損失額などのコストも含まれます。
- **ウ** 正解です。
- × **エ** リスク評価額は、損害の1回当たりの平均予想損失額に、その損害の平均発生回数(回/年)を乗じたものです。

問13 ISMSプロセス

ISMSとは、「情報セキュリティマネジメントシステム」のことで、「マネジメントシステム全体の中で、事業リスクに対するアプローチに基づいて情報セキュリティの確立、導入、運用、監視、見直し、維持、改善を担う部分」と定義されています(ISMS認証基準 Ver.2.0より)。わかりやすく解釈すると、情報セキュリティを確立し維持するために社内を管理する仕組み(システム)のことです。

ISMSプロセスとは、ISMSを確立し、維持し、運用中のISMSに問題がないかなどを検査し、問題などがある場合は見直しを行い、システムを刷新する……というプロセスの繰返しのことを指します。セキュリティに関する法律や技術、また社会情勢などは日々変化し続けているため、ISMSを一度作成すれば以後永久に同じシステムのままで運用し続けられるということはありません。常にISMSの検証と見直しが必要とされます。

ISMSのプロセスは、PDCAサイクル(Plan(立案・確立)→Do(セキュリティ対策の実施・管理)→Check(ISMSの検証)→Act(ISMSの見直し))で構成されます。Actフェーズ(見直し)の後にISMSは適切に更新され(Planフェーズ)、新しいISMSによるセキュリティ対策が実施され(Doフェーズ)…という手順の繰返しによって、ISMSは更新され、維持されていきます。

上記のPlanフェーズでは、情報セキュリティ方針の策定や情報セキュリティに関する各種目標の設定、及び情報資産のリスクの把握(リスクアセスメント)などが行われます。

- × **ア** 運用状況の管理は、Doフェーズで実施されます。
- × **イ** 改善策の実施(すなわちISMSの見直し)は、Actフェーズで実施されます。
- × **ウ** 実施状況に対するレビュー(すなわちISMSの検証)は、Checkフェーズで実施されます。
- **エ** 正解です。

○ 解答 ○

問11 **イ**

問12 **ウ**

問13 **エ**

☐ **問 14** ISMS適合性評価制度における情報セキュリティポリシーに関する記述のうち、適切なものはどれか。

- ☐ **ア** 基本方針は、事業の特徴、組織、その所在地、資産及び技術を考慮して策定する。
- ☐ **イ** 重要な基本方針を定めた機密文書であり、社内の関係者以外の目に触れないようにする。
- ☐ **ウ** セキュリティの基本方針を述べたものであり、ビジネス環境や技術が変化しても変更してはならない。
- ☐ **エ** 特定のシステムについてリスク分析を行い、そのセキュリティ対策とシステム運用の詳細を記述したものである。

☐ **問 15** ISMSにおけるリスク分析の方法の一つであるベースラインアプローチはどれか。

- ☐ **ア** 公表されている基準などに基づいて一定のセキュリティレベルを設定し、実施している管理策とのギャップ分析を行った上で、リスクを評価する。
- ☐ **イ** 情報資産を洗い出し、それぞれの情報資産に対して資産価値、脅威、脆弱性^{ぜい}及びセキュリティ要件を識別し、リスクを評価する。
- ☐ **ウ** 複数のリスク分析方法の長所を生かして組み合わせ、作業効率や分析精度の向上を図る。
- ☐ **エ** リスク分析を行う組織や担当者^{担当者}の判断によって、リスクを評価する。

☐ **問 16** PCIデータセキュリティ基準(PCI DSS Version 2.0)の要件のうち、詳細要件の選択肢として、WAFの導入を含むものはどれか。

- ☐ **ア** 要件1: カード会員データを保護するために、ファイアウォールをインストールして構成を維持すること
- ☐ **イ** 要件3: 保存されるカード会員データを保護すること
- ☐ **ウ** 要件6: 安全性の高いシステムとアプリケーションを開発し、保守すること
- ☐ **エ** 要件7: カード会員データへのアクセスを、業務上必要な範囲内に制限すること

☐ **問 17** セキュリティ対策の“予防”に該当するものはどれか。

- ☐ **ア** アクセスログをチェックし、不正なアクセスがないかどうかを監視する。
- ☐ **イ** コンティンジェンシープランを策定し、訓練を実施する。
- ☐ **ウ** 重要ファイルのバックアップ処理を定期的に行う。
- ☐ **エ** セキュリティに関する社内教育を実施し、個人の意識を高める。

解説

問14 ISMS適合性評価制度

ISMS適合性評価制度は、組織の情報セキュリティマネジメントシステムが適切であるかどうかを評価するための制度です。この制度において、組織の情報セキュリティ維持体制などを規定し、内外に公表するための文書が「情報セ

セキュリティポリシー」です。情報セキュリティポリシーの「基本方針」は、組織の「情報セキュリティの維持に対する取り組み」についての具体的な内容等を定義していく上で、基本となるべき重要なものです。「基本方針」は、組織の規模・業務内容、事業の特徴、技術力などの様々な状況を考慮した上で作成し(ア)、外部に公表します。

- ア 正解です。
- × イ 「基本方針」は機密文書ではありません。外部に公開すべきものです。
- × ウ ビジネス環境の変化やセキュリティ技術の進歩、また新たに発見された不正アクセスの手法などに対応するため、セキュリティを確保するための方法などは日々進歩させる必要があります。よって、その基礎となる情報セキュリティポリシーの「基本方針」も、時勢の変化に合わせて変化させていきます。
- × エ 「基本方針」は、特定のシステムのみではなく、組織の業務全般に対する規範となります。

問15 ISMSにおけるリスク分析

ISMSにおけるリスク分析とは、情報システムに内在するリスクの発生頻度・被害額などを判定し、現実には発生すれば損失をもたらすリスクがシステムのどこにどのように潜在しているかを識別し、重要なリスクとそうでないリスクを見極め、各リスクについて対処するか否かを決定することです。

ベースラインアプローチとは、公表されている既存のセキュリティ対策基準や規格などを参考にして一定のセキュリティレベルを設定し、そのレベルを基にして自組織が達成すべき大まかな対策基準を策定し、当該対策基準を基にしてリスク分析を行ったり、リスクへの管理策を策定したりする方法のことです。

- ア 正解です。
- × イ ISMSにおけるリスク分析のうちの詳細リスク分析です。
- × ウ ISMSにおけるリスク分析のうちの組み合わせアプローチです。
- × エ ISMSにおけるリスク分析のうちの非形式的アプローチです。

問16 PCIデータセキュリティ基準

PCIデータセキュリティ基準(PCI DSS: Payment Card Industry Data Security Standard)は、クレジットカード情報などを保護することを目的として、VISAなどのクレジットカード会社が共同で策定した基準です。

PCI DSSの要件6(安全性の高いシステムとアプリケーションを開発し、保守すること)の6.6の項では、一般公開されているWebアプリケーションについて、「Webベースの攻撃を検知及び回避するために、一般公開されているWebアプリケーションの手前に、Webアプリケーションファイアウォール(WAF)がインストールされていることを確認する」としています。以上から、ウが正解です。

問17 予防

情報セキュリティ対策の「予防」とは、ハードウェア・ソフトウェアの安全性の強化や、ユーザに対する教育訓練により不正アクセスなどを未然に防止し、被害をはじめから生じさせない施策のことです。

- × ア セキュリティ対策の「監視」に関する記述です。
- × イ 障害発生時の対応に関する記述です。コンティンジェンシープランとは、「緊急時対応計画」または「不測事態対応計画」のことで、障害や事故等の事態が発生することを想定し、その対策を事前に定めた案のことです。
- × ウ セキュリティ対策の「回復」に関する記述です。
- エ 正解です。

○ 解答 ○

問14 ア

問15 ア

問16 ウ

問17 エ



問 18 社内のセキュリティポリシーで、利用者の事故に備えて秘密鍵を復元できること、及びセキュリティ管理者の不正防止のための仕組みを確立することが決められている。電子メールで公開鍵暗号方式を使用し、鍵の生成はセキュリティ部門が一括して行っている場合、秘密鍵の適切な保管方法はどれか。

- ア** 1人のセキュリティ管理者が、秘密鍵を暗号化して保管する。
- イ** 暗号化された秘密鍵の一つ一つを分割し、複数のセキュリティ管理者が分担して保管する。
- ウ** セキュリティ部門には、秘密鍵を一切残さず、利用者本人だけが保管する。
- エ** 秘密鍵の一覧表を作成して、セキュリティ部門内に限り参照できるように保管する。



問 19 ペネトレーションテストで確認する対象はどれか。

- ア** 使用している暗号方式の強度
- イ** 対象プログラムの様々な入力に対する出力結果と仕様上の出力との一致
- ウ** ファイアウォールが単位時間当たりに処理できるセッション数
- エ** ファイアウォールや公開サーバに対するセキュリティホールや設定ミスの有無



問 20 コンピュータウイルスの検出、機能の解明、又は種類の特定をする手法について、適切な記述はどれか。

- ア** 暗号化された文書中のマクロウイルスを検出するにはパターンマッチング方式が有効である。
- イ** 逆アセンブルは、バイナリタイプの新種ウイルスの機能を解明するのに有効な手法である。
- ウ** 不正な動作を識別してウイルスを検知する方式は、ウイルス名を特定するのに最も有効である。
- エ** ワームは既存のファイルに感染するタイプのウイルスであり、その感染の有無の検出にはファイルの大きさの変化を調べるのが有効である。



問 21 テンペスト技術の説明とその対策として、適切なものはどれか。

- ア** ディスプレイなどの機器から放射される電磁波を傍受し、内容を観察する技術であり、電磁波遮断が施された部屋に機器を設置することによって対抗する。
- イ** データ通信の途中でパケットを横取りし、内容を改ざんする技術であり、デジタル署名による改ざん検知の仕組みを実装することによって対抗する。
- ウ** マクロウイルスに対して使われる技術であり、ウイルス対策ソフトを導入し、最新の定義ファイルを適用することによって対抗する。
- エ** 無線LANの信号から通信内容を傍受し、解析する技術であり、通信パケットを暗号化することによって対抗する。

解説

問18 秘密鍵の保管方法

× **ア** この方式では、秘密鍵の管理が単独の管理者のみに任されるため、危険です。また、このセキュリティ管理者

のPCが故障すると、全ての秘密鍵が失われる可能性もあります。

- **イ** 正解です。
- × **ウ** この方式は、利用者のPCが故障するなどの、「秘密鍵が利用できなくなる事態」に対処できません。
- × **エ** 秘密鍵を暗号化せずに一覧表にしているので、セキュリティ部門の人員全てが参照できてしまい、危険です。

問19 ペネトレーションテスト

ペネトレーションテストとは、テスト対象の情報システムに対して実際に攻撃を行い、侵入を試みることによって、セキュリティホールや脆弱性、及び設定ミスなどを発見するテスト手法のことです。

- × **ア** 暗号方式の強度は、このテストでは検証しません。
- × **イ** 入力に対する出力結果の検証などは、ブラックボックステストで行います。
- × **ウ** ファイアウォールが単位時間内に処理できるセッション数などは、耐久テストなどで検証されます。
- **エ** 正解です。

問20 コンピュータウイルスの機能の解明

コンピュータウイルスの機能を解明するために、**逆アセンブル**が用いられます。逆アセンブルは、機械語で記述されたバイナリタイプのプログラムを解析して、当該プログラムのソースコードや仕様などを導き出す方法です。この方法により、バイナリタイプの新種のウイルスのプログラムのコードから、当該ウイルスの仕様や機能などを解明できます。

- × **ア** 暗号化された文書の中にマクロウイルスが潜んでいる場合、そのウイルスのコードなども暗号化されるため、アンチウイルスソフトウェアに登録されたウイルスのコードの特徴と、暗号化されたマクロウイルスのコードの特徴が異なることになり、パターンマッチング方式では検出できない可能性が高くなります。
- **イ** 正解です。
- × **ウ** 多くのウイルスは、その動作(感染時に、他のファイルに自らをコピーすることなど)などが類似しているという性質があります。したがって、ウイルスの不正な動作を識別しても、その動作またはその動作に近い動作を行うウイルスが多数存在している可能性があり、個別のウイルスの名称を特定できないことがあります。
- × **エ** ワームは、既存のファイルに感染することではなく、単独で動作可能なプログラムとなります。よって、ファイルの大きさの変化を調べても、そのファイルにワームが感染したかどうかを判定することは不可能です。

問21 テンペスト技術

テンペスト技術(攻撃)とは、コンピュータやディスプレイなどから発せられる電磁波中の電磁的な信号を、測定用の機器を用いて観測し収集することで、操作中の画面の内容を再現したり、暗号化鍵や暗号化アルゴリズムなどの情報を不正に入手したりする攻撃方法です。この攻撃を防ぐためには、ネットワークケーブルなども含めた機器のシールド化(金属などによって電磁波が漏れないように囲うこと)や、電磁波遮断が施された部屋にコンピュータなどを設置することが有効です。

- **ア** 正解です。
- × **イ** テンペスト技術では、データ通信の途中でパケットを横取りして改ざんすることはありません。この記述は、パケットの改ざんとその対処方法の説明です。
- × **ウ** この記述は、マクロウイルスの特徴とその対処方法の説明です。
- × **エ** この記述は、無線LANの盗聴とその対処方法の説明です。

○ 解答 ○

問18 **イ**

問19 **エ**

問20 **イ**

問21 **ア**



問 22 サーバへのログイン時に用いるパスワードを不正に取得しようとする攻撃とその対策の組合せのうち、適切なものはどれか。

	辞書攻撃	スニффイング	ブルートフォース攻撃
ア	パスワードを平文で送信しない。	ログインの試行回数に制限を設ける。	ランダムな値でパスワードを設定する。
イ	ランダムな値でパスワードを設定する。	パスワードを平文で送信しない。	ログインの試行回数に制限を設ける。
ウ	ランダムな値でパスワードを設定する。	ログインの試行回数に制限を設ける。	パスワードを平文で送信しない。
エ	ログインの試行回数に制限を設ける。	ランダムな値でパスワードを設定する。	パスワードを平文で送信しない。



問 23 TLSについて説明したものはどれか。

- ア 相手が秘密鍵をもっているかどうかを検証するために、乱数を送付し、署名してもらう認証
- イ トランスポート層において、アプリケーションとは独立に暗号化及びデジタル署名を施すことを可能にした規約
- ウ 複数のLANやコンピュータシステムを、インターネットや共用回線を用いて仮想的に同一ネットワークとして安全に接続する技術
- エ ルータ間の通信の秘匿性、相手認証、パケットごとの改ざん防止を提供するためのプロトコル



問 24 クロスサイトスクリプティングによる攻撃へのセキュリティ対策はどれか。

- ア OSのセキュリティパッチを適用することによって、Webサーバへの侵入を防止する。
- イ Webアプリケーションで、クライアントに入力データを再表示する場合、情報内のスクリプトを無効にする処理を行う。
- ウ WebサーバにSNMPプログラムを常駐稼働させることによって、攻撃を検知する。
- エ 許容範囲を超えた大きさのデータの書込みを禁止し、Webサーバへの侵入を防止する。

解説

問22 パスワードの不正取得

パスワードの不正取得を試みる攻撃方法をまとめます。

辞書攻撃：辞書に掲載されている一般的な名詞などの単語(“apple”など)、及び単語の組合せなどの文字列をパスワードとして入力していき、標的ユーザのパスワードを推定しようとする攻撃方法です。人間の心理として、よく使用するパスワードは、できるだけ覚えやすい一般的な単語を使用しがちです。辞書攻撃を防ぐためには、無意味文字列(意味のないランダムな文字列)をパスワードとして用いることが有効です。

スニッフイング：スニッフイングとは、ネットワーク上のパケットを盗聴する行為です。この行為により、パケットに含まれるパスワードを読み取り、不正取得する攻撃方法が知られています。

スニффイングを防ぐためには、パスワードを平文で送受信せず、暗号化してからネットワーク上に送出すべきです。

ブルートフォース攻撃(総当り攻撃):ブルートフォース攻撃(総当り攻撃)は、考えられる全ての種類のパスワード(または暗号化鍵など)を総当りで作成して、それをもって不正なログインや暗号解読を試みる方式のことです。

ブルートフォース攻撃を防ぐには、パスワードの長さ(文字数)をできるだけ長くしたり、暗号化・復号に使用する鍵のビット長を可能な限り長くしたりすることが有効です。また、何回かパスワードを入力ミスした場合、一定時間そのアカウントからのログインを禁止したり、アカウントを停止したりする対策も有効です。

以上より、**イ**の組合せが適切です。

問23 SSL/TLS

SSLは、クライアントとWebサーバ間の情報の暗号化を行い、取引情報や個人情報などの機密性の求められる情報をインターネット上に安全に送出するためのものです。このSSLがIETFによって暗号化・認証形式として扱われるようになり、**TLS**(Transport Layer Security)という名前では呼ばれるようになりました。

SSL/TLSにおいては、トランスポート層において、上位層のアプリケーションとは独立に暗号化やデジタル署名を実行するためのプロトコルが用意されています。

- × **ア** この認証方法を、**チャレンジレスポンス**といいます。
- **イ** 正解です。
- × **ウ** 複数のLANなどを、インターネットなどを用いて仮想的に同一のネットワークとするのは、**VPN**(Virtual Private Network)です。
- × **エ** ルータ間の通信の秘匿性や改ざん防止を提供するためのプロトコルとしては、IPsecなどがあります。

問24 クロスサイトスクリプティング

ブラウザから掲示板などの動的なサイトにアクセスする際に、以下のようなURLが用いられることがあります。なお、以下のURLは架空のものです。

`http://*****.net/****.htm?data=123456`

“?data=…”は、当該サイトのCGIなどに対してユーザが送信する情報を記載したものです。当該サイトのCGIは、このデータを基に動的にWebページを生成したり、検索処理を行ったりする仕様となっています。

ここで、上の“?”以降に、正規のデータの代わりに悪意をもったスクリプトの文字列を記述したURLを作成して、他のWebページにリンクとして貼ると、そのリンクをクリックした場合に、CGIに正常なデータの代わりに不正なスクリプトが与えられ、ブラウザ上で悪意のスクリプトが実行されてしまう可能性があります。**クロスサイトスクリプティング**とは、この方法を用いて、悪意をもったスクリプト(JavaScriptなど)をユーザのブラウザに送り込み、標的サイトにアクセスしたユーザの個人情報をクッキーから盗み取るなどの手法を用いる攻撃方法です。

クロスサイトスクリプティングを防ぐには、入力されるデータのサニタイジング(データの文字列に含まれるスクリプトを無効化すること)などの措置が適切です。

- × **ア** WebサーバのOSのセキュリティパッチをあてていても、クロスサイトスクリプティングを防止することはできません。クロスサイトスクリプティングでは、不正なスクリプトがブラウザ上で実行されるためです。
- **イ** 正解です。
- × **ウ** **ア**と同様に、SNMPプログラムを常駐させることなどによってWebサーバのセキュリティを向上させても、クロスサイトスクリプティングを防止することはできません。
- × **エ** 許容範囲を超えた大きさのデータの書き込みを禁止するのは、バッファオーバーフローへの対策です。

○ 解答 ○

問22 **イ**

問23 **イ**

問24 **イ**



問 25 パケットフィルタリング型ファイアウォールがルール一覧のアクションに基づいてパケットを制御する場合、パケットAに対する処理はどれか。ここで、ファイアウォールでの処理は番号の順に行い、一つのルールが適合した場合には残りのルールを無効とする。

ルール一覧

番号	送信元 アドレス	送信先 アドレス	プロトコル	送信元 ポート	送信先 ポート	アクション
1	10.1.2.3	*	*	*	*	通過禁止
2	*	10.2.3.*	TCP	*	25	通過許可
3	*	10.1.*	TCP	*	25	通過許可
4	*	*	*	*	*	通過禁止

注 * は任意のパターンを表す。

パケット A

送信元 アドレス	送信先 アドレス	プロトコル	送信元 ポート	送信先 ポート
10.1.2.3	10.2.3.4	TCP	2100	25

- ア** 番号1によって、通過が禁止される。 **イ** 番号2によって、通過が許可される。
ウ 番号3によって、通過が許可される。 **エ** 番号4によって、通過が禁止される。



問 26 インタラクティブ送信における著作権に関する記述のうち、適切なものはどれか。

- ア** サーバに蓄積された情報を、著作権者の許諾なしに送信可能な状態にするだけでは権利侵害とならない。
イ 著作権者の許諾なしに公衆に情報を送信する行為は、サーバに情報を蓄積するか否かにかかわらず権利侵害となる。
ウ 著作権者の許諾なしに送信された情報を、第三者が正常に受信できた場合に限り、権利侵害となる。
エ 著作権者の送信権は有線の場合に限って発生するものであり、無線の場合は権利侵害の対象とならない。

解説

問25 パケットフィルタリング型ファイアウォール

パケットフィルタリング方式では、IPパケットのヘッダ中の情報(送信元・宛先IPアドレスや、ICMP・TCP・UDPなどの上位プロトコルの区別など)や、TCPセグメントのヘッダの情報(送信元・宛先ポート番号など)を参照し、条件に適しないパケットやセグメントを通過させない方法をとることで、不審なIPパケットの侵入などを防ぎます。

問題文の「ルール一覧」の表の各行の記述を分析します。

番号1の行：この行では、送信元アドレスが「10.1.2.3」というIPアドレスであるもの(他の条件は"*"(=任意)となっているため、特に評価しない)について、「通過禁止」というアクションをとります。すなわち、送信元アドレスが「10.1.2.3」というIPアドレスのIPパケットは、通過が禁止されます。

番号2の行：この行では、送信先アドレスが「10.2.3.*」(= 10.2.3.1～10.2.3.254の範囲のIPアドレス)で、トランスポート層プロトコルがTCPであり、かつ送信先ポート番号が25であるものについて、「通過許可」というアクションをとります。

番号3の行：この行では、送信先アドレスが「10.1.*」(= 10.1.0.1～10.1.255.254の範囲のIPアドレス)で、トランスポート層プロトコルがTCPであり、かつ送信先ポート番号が25であるものについて、「通過許可」というアクションをとります。

番号4の行：この行では、全ての条件が"*"(=任意)となっているものについて「通過禁止」というアクションをとります。すなわち、あらゆるIPパケットは、通過が禁止されます。

「ファイアウォールでの処理は、ルール一覧に示す番号の1から順に」行われるため、番号1, 2, 3, 4の順で以上のルールは評価されます。よって、番号4などより番号1の方が先に評価されます。問題文のパケットは送信元アドレスが「10.1.2.3」であるため、番号1の条件に一致し、通過が禁止されます。正解は **ア** です。

問26 インタラクティブ送信における著作権

著作物を著作者に無断で複製したり、配布・公表などを行ったりすると、一般的には**著作権**の侵害になります。また、インターネット上のWebサーバなどの各種のサーバに、他人の著作物を許諾なしにアップロードする行為も、一般的には「**公衆送信権**」の侵害となります。

例えば、著作物などを画像や文字などのファイルにしてホームページに掲載するということは、Webサーバ内にそのファイルを置くということであり、この時点でそれらのファイルは「外部からリンクされれば(参照されれば)、誰でも参照可能となる状態」になります。このような状態を「**送信可能化**」状態といいます。

著作物を送信可能化状態にするか否かを選ぶ権利も、作者の「公衆送信権」の範囲に含まれます。よって、たとえ誰からも参照されていない(リンクされていない)状態でも、ホームページに掲載した時点で権利侵害になりえます。そのほか、サーバに入力される情報(TV放送など)をサーバに蓄積させずに自動公衆送信する場合なども権利侵害になります。

以上から、**イ**の記述が適切です。

- × **ア** 前述のとおり、「送信可能な状態に」するだけで、権利侵害となりえます。
- **イ** 正解です。
- × **ウ** 第三者が正常に受信できるか否かは、公衆送信権の侵害とは関係ありません。
- × **エ** 有線・無線といった媒体やメディアの違いは、公衆送信権の侵害とは関係ありません。

○ 解答 ○

問 25 **ア**

問 26 **イ**



問27 トレードシークレット(営業秘密)に関する記述のうち、適切なものはどれか。

- ア 特許は技術情報を公開した上で保護されるが、トレードシークレットは秘密として管理されていることを条件として保護される。
- イ トレードシークレットとは、企業秘密として管理されている専門技術情報を指し、販売マニュアル、取引先リストなどは含まれない。
- ウ トレードシークレットは、産業財産権の一つに分類される権利であり、特許権、実用新案権と並ぶものである。
- エ 不正競争防止法では、トレードシークレットに関する不正な行為に対して“差止請求権”を認めているが、“損害賠償請求権”は認めていない。



問28 開発した製品で利用している新規技術に関して特許の出願を行った。日本において特許権の取得が可能なものはどれか。

- ア 学会で技術内容を発表した日から11か月目に出願した。
- イ 顧客と守秘義務の確認を取った上で技術内容を説明した後、製品発表前に出願した。
- ウ 製品に使用した暗号の生成式を出願した。
- エ 製品を販売した後に出願した。

解説

問27 トレードシークレット

特許法では、自然法則を利用した発明のうち高度なものを特許として定義しています。また、特許法では特許の発明者が、一定の期間当該特許を独占的に利用できる権利(特許権)を定めています。ある発明が特許として認められるためには、特許庁への出願を行う必要があります。その際に、当該発明の技術情報が公開されることになります。

不正競争防止法は、「事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もって国民経済の健全な発展に寄与する」(同法第1条より)ことを目的とした法律です。この法律では幾つかの行為を「不正競争」として定義し、不正競争によって営業上の利益を侵害された者などは、その侵害の停止などを請求する権利があることを規定しています。

この不正競争の一つに、「窃取、詐欺、強迫その他の不正の手段により営業秘密を取得する行為……又は不正取得行為により取得した営業秘密を使用し、若しくは開示する行為」があります。この「**営業秘密(トレードシークレット)**」とは、同法で保護されている対象であり、「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」を指します。よって、**ア**が適切です。

- **ア** 正解です。
- × **イ** 秘密として保護されていれば、販売マニュアルなどの事業活動に有用な情報もトレードシークレットとなります。
- × **ウ** トレードシークレットは、「技術上又は営業上の情報」であり、権利ではありません。よって、特許権などと並ぶものとはいえません。
- × **エ** 不正競争防止法では、トレードシークレットに関する不正な行為(盗用など)を受けることで営業上の利益を侵害された者、もしくは営業上の利益を侵害されるおそれがある者について、不正行為の差止を請求する権利(差止請求権)や、侵害された利益の賠償を請求する権利(損害賠償請求権)を認めています。

問28 特許権

特許権とは、産業上利用できる発明(自然法則を利用した技術的思想の創作のうち高度のもの)を行った人が、その発明を独占排他的に使用できる権利のことです。この権利を取得するためには、特許庁への出願及び審査が必要となります。

特許法では、特許の要件について以下のように規定しています。

第二十九条 産業上利用することができる発明をした者は、次に掲げる発明を除き、その発明について特許を受けることができる。

- 一 特許出願前に日本国内又は外国において公然知られた発明
 - 二 特許出願前に日本国内又は外国において公然実施をされた発明
 - 三 特許出願前に日本国内又は外国において、頒布された刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明
- (特許法第二十九条より引用)

すなわち、特許の技術が組み込まれた製品を出願前に販売することなどによって、出願前に公然と知られることになった発明については、出願しても特許として認められない(特許権が取得できない)ことになります。なお、この第一項及び第二項の規定には例外があります。

第三十条 特許を受ける権利を有する者が試験を行い、刊行物に発表し、電気通信回線を通じて発表し、又は特許庁長官が指定する学術団体が開催する研究集会において文書をもつて発表することにより、第二十九条第一項各号の一に該当するに至った発明は、その該当するに至った日から六月以内にその者がした特許出願に係る発明についての同条第一項及び第二項の規定の適用については、同条第一項各号の一に該当するに至らなかったものとみなす。

(特許法第三十条より引用)

すなわち、技術内容を学会などに発表して「公然知られた」状態になった発明を、発表から6か月以内に出願した場合には、第二十九条の「公然知られた発明」には相当しないため、特許権を取得することができます。

解答群のうち、特許権の取得が可能なものは **イ** のみとなります。この記述では、顧客と守秘義務の確認を取った上で技術内容の説明をしています。このように、守秘義務を結んだ上で一部の限られた人または組織のみに技術内容の説明をした発明については、「公然知られた」ものとはみなされないため、前述の第二十九条の条件には該当せず、特許権の取得が可能となります。

- × **ア** 学会で技術内容を発表してから11か月目に出願した場合、先の「6か月以内」の条件を満たしていないため、この発明は公然知られたものとみなされます。よって、前述の第二十九条の条件に該当してしまうため、特許権の取得は不可能となります。
- **イ** 正解です。
- × **ウ** 特許法では、特許を取得できる「発明」を、「自然法則を利用した技術的思想の創作のうち高度のもの(同法第二条より引用)」と定義しています。よって、単なる計算式(暗号の生成式など)やアルゴリズムといった自然法則を利用していないものは、特許として認められません。
- × **エ** 製品の販売後に出願しているため、この発明は公然知られたものとみなされます。よって、前述の第二十九条の条件に該当してしまうため、特許権の取得は不可能となります。

○ 解答 ○

問27 **ア**

問28 **イ**

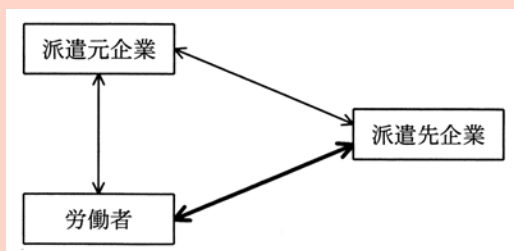


問 29 特段の措置をとらずになされた個人情報取扱事業者の行為のうち、個人情報保護法に照らして適法な行為はどれか。

- ア** 開催したセミナーで回収した、商品企画立案を目的としたアンケートに記載された参加者の氏名及び住所を、自社の販売促進セミナー案内用ダイレクトメール発送先住所録に登録した。
- イ** 開設しているWebサイトの問合せページで自社製品販売促進ダイレクトメール送付可否欄に可と記入した依頼者の氏名及び住所を、自社の製品販売促進用ダイレクトメール発送先住所録に登録した。
- ウ** 自社が主催した市場動向に関する勉強会の参加者リストの内容を、自社の子会社の製品販売促進用メールマガジン発送先アドレスリストに登録した。
- エ** 従業員が参加した同窓会で配布された同窓生名簿に記載されている、同窓生の氏名及び電話番号を、自社製品販売促進用コールセンタのアウトバウンド用電話番号リストに登録した。



問 30 労働者派遣事業法に基づく、派遣先企業と労働者との関係(図の太線部分)はどれか。



- ア** 請負契約関係
- イ** 雇用関係
- ウ** 指揮命令関係
- エ** 労働者派遣契約関係



問 31 ソフトウェア製品を輸出する場合、“外国為替及び外国貿易法(外為法)”による規制を考慮する必要があるものはどれか。

- ア** 暗号化技術に関連するソフトウェア
- イ** 会計処理専用ソフトウェア
- ウ** 販売店の店頭で購入可能なソフトウェア
- エ** 輸出地域の商取引法を考慮しないで作成されたソフトウェア

解説

問29 個人情報保護法

個人情報保護法の概要を示します。

個人情報保護法では、「個人情報」を次のように定義しています。

この法律において「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう
(個人情報保護法第2条より引用)

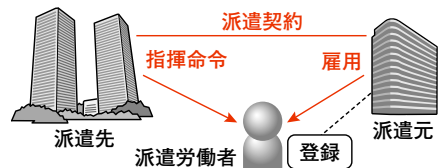
個人情報保護法では、「個人情報データベース等を事業の用に供している者」(個人情報保護法第2条より引用)を、**個人情報取扱事業者**と定義しています。個人情報取扱事業者は、個人情報の取得や利用などに関して、各種の義務を果たさなければなりません。

個人情報取扱事業者が、利用目的を公表せずに個人情報を収集したり、利用目的の範囲を超えて個人情報を取り扱ったりすることはできません。**ア**のように、商品企画立案を利用目的としたアンケートに記載された個人情報を、販売促進セミナー案内用ダイレクトメール発送先住所録に登録するのは適法ではありません。公表した利用目的(商品企画立案)とは異なる目的(販売促進セミナー案内用ダイレクトメール発送)のために個人情報が利用されるためです。**ウ**、**エ**も、公表した利用目的と異なる目的に利用するためのリストに個人情報を登録しているので、適法ではありません。**イ**の記述は、公表した利用目的と同じ目的のリスト(住所録)に個人情報を登録しているので、適法です。

問30 労働者派遣事業法

労働者派遣法では、「派遣労働者」、「派遣先事業主(企業)」、「派遣元事業主(企業)」の3者間の関係を図のように定めています。

派遣先事業主と派遣元事業主との間で「労働者派遣契約関係」が締結され、派遣先事業主の依頼に応じて、派遣元事業主が雇用している派遣労働者を派遣先事業主に派遣します。派遣労働者は、派遣先事業主の指揮命令下で業務を行います。



以上から、派遣先企業(派遣先事業主)と派遣労働者(労働者)の間には、指揮命令関係(**ウ**)が築かれることとなります。**ウ**が正解です。

なお、請負契約と派遣契約は契約の形態が異なるため、派遣事業においていずれかの業者や労働者の間に請負契約関係(**ア**)が生じることはありません。

問31 外為法

外国為替及び外国貿易法(外為法)とは、外国為替や外国貿易などの対外取引に対して、必要最小限の管理または調整を行うことにより、対外取引の正常な発展や、日本国の経済の健全な発展に寄与することを目的としている法律です。

この法律では、「国際的な平和及び安全の維持を妨げることとなると認められるものとして政令で定める特定の地域を仕向地とする特定の種類の貨物の輸出をしようとする者は、政令で定めるところにより、経済産業大臣の許可を受けなければならない」(同法四十八条より引用)と規定されています。外為法に関連した政令である**輸出貿易管理令**では、核兵器などに転用可能な部品や技術、もしくは毒物や兵器などの製造に転用可能な貨物などを外国に輸出しようとする者は、経済産業大臣の許可を得なければならないとしています。暗号装置またはその部分品も、輸出の際には同様に経済産業大臣の許可が必要です。暗号技術に関連するソフトウェアは、この規制に相当する可能性があるため、**ア**の記述が適切です。

他の解答群については、いずれも外為法や輸出貿易管理令において規制されていないため、解答として不適切となります。

○ 解答 ○

問 29 **イ**

問 30 **ウ**

問 31 **ア**



問32 企業経営における、コンプライアンス強化の説明はどれか。

- ☐ **ア** 企業存続の危機につながりかねない、経営者や従業員による不法行為の発生を抑制する。
- ☐ **イ** 競合他社に対する差別化の源泉となる経営資源を保有し、競争力を強化する。
- ☐ **ウ** 経営者の権力行使をけん制し、健全な経営を行うことができる仕組みを作る。
- ☐ **エ** 顧客、株主、従業員などの利害関係者の満足度を向上させ、企業の継続した発展を図る。



問33 フェールセーフの考え方として、適切なものはどれか。

- ☐ **ア** システムに障害が発生したときでも、常に安全側にシステムを制御する。
- ☐ **イ** システムの機能に異常が発生したときに、すぐにシステムを停止しないで機能を縮退させて運用を継続する。
- ☐ **ウ** システムを構成する要素のうち、信頼性に大きく影響するものを複数備え、システムの信頼性を高める。
- ☐ **エ** 不特定多数の人が操作しても、誤動作が起こりにくいように設計する。



問34 東京～大阪及び東京～名古屋がそれぞれ独立した通信回線で接続されている。東京～大阪の稼働率は0.9、東京～名古屋の稼働率は0.8である。東京～大阪の稼働率を0.95以上に改善するために、大阪～名古屋にバックアップ回線を新設することを計画している。新設される回線の稼働率は最低限幾ら必要か。

- ☐ **ア** 0.167 ☐ **イ** 0.205 ☐ **ウ** 0.559 ☐ **エ** 0.625

解説

問32 コンプライアンス

“**コンプライアンス**”とは、「法令遵守」という意味です。コンプライアンス経営とは、法令や社会規範(社会常識)、業界内での規則や企業倫理など、企業が守るべき各種の法律・規則・規範などを適切に遵守するため、それらに関するマニュアルなどを整備し、法令や社会規範を遵守した企業活動を行うことを指します。

コンプライアンスを強化することにより、経営者や従業員が企業倫理や法律などを適切に遵守し、法律や規範などに違反することが少なくなることから、不法行為の発生を抑制できます。

- **ア** 正解です。
- × **イ** 競合他社に対する差別化の源泉となる、他社にはまねのできない経営資源やノウハウなどを保有することで競争力を強化することを、**コアコンピタンス**といいます。この記述は、コアコンピタンスを重視した経営に関する記述です。
- × **ウ** 経営者の権力行使をけん制する仕組みを作るのは、**コーポレートガバナンス**に関する説明です。コーポレートガバナンスとは、経営者によって企業の経営管理が適切に行われているかを監視し、ステークホルダに対して企業活動の正当性を維持する行為、及びそのための仕組みのことです。また、この記述は、株主総会によって不正行為を行う経営者を罷免できることなどにも関連しています。
- × **エ** 顧客、株主、従業員などの企業に関する利害関係者の満足度を向上させることで企業の継続した発展を図るのは、ステークホルダを重視した企業経営に関する説明です。

問33 フェールセーフ

システムに異常が発生した場合の対処方法として、フェールセーフとフェールソフトがあります。

フェールセーフ：異常発生時にはシステムを停止させるか、人間系(オペレータ等)に処理の続行判断を委任し、必ず「より安全な状態」にシステムを導く方式。一般的には、システムを停止させることが多い。

フェールソフト：異常発生時にはシステムの機能を縮退(減少・制限)させた上で、異常の影響のない機器などを活用して、性能を低下させてでも可能な限り処理を継続する方式。

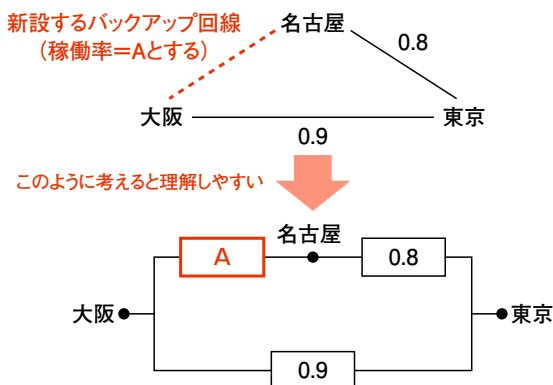
フェールセーフの説明に該当するのは、解答群 **ア** の記述(常に安全側にシステムを制御する)です。

- **ア** 正解です。
- × **イ** 異常発生時にシステムの機能を縮小させて運転を継続するのは、フェールソフトの説明です。
- × **ウ** 信頼性に大きく影響する要素を複数用意し、システムの信頼性を高めるのは、**フォールトトレランス**の説明です。
- × **エ** 不特定多数の人が操作しても誤操作が起こりにくように設計するのは、**フールプルーフ**の説明です。

問34 稼働率

問題文の説明から、東京－大阪間と東京－名古屋間に独立した通信回線が存在していることがわかります。大阪－名古屋間にバックアップ回線を新設すると、東京－大阪間は以下の2つの経路で結ばれることが理解できます。

- 東京－大阪の経路
- 東京－名古屋経由－大阪の経路



新設されるバックアップ回線の稼働率をAとおき、この2つの経路の稼働率を求めます。

東京－大阪の経路の稼働率：0.9

東京－名古屋経由－大阪の経路の稼働率：0.8×A=0.8A

東京－大阪間は、この2つの経路による並列構成の通信回線によって結ばれていると考えられるので、全体の稼働率は以下の式で計算できます。

$$\text{全体の稼働率} : 1 - (1 - 0.9) \times (1 - 0.8A) = 1 - 0.1 \times (1 - 0.8A) = 1 - 0.1 + 0.08A = 0.9 + 0.08A$$

この値が0.95以上になるために必要なAの値は、

$$0.95 = 0.9 + 0.08A$$

$$\rightarrow 0.05 = 0.08A$$

$$\therefore A = \frac{0.05}{0.08} = 0.625 \text{ (エ)}$$

となります。

○ 解答 ○

問 32 **ア**

問 33 **ア**

問 34 **エ**



問 35 SQLの構文として、正しいものはどれか。

- ア** SELECT 注文日, AVG (数量)
FROM 注文明細
- イ** SELECT 注文日, AVG (数量)
FROM 注文明細
GROUP BY 注文日
- ウ** SELECT 注文日, AVG (SUM (数量))
FROM 注文明細
GROUP BY 注文日
- エ** SELECT 注文日
FROM 注文明細
WHERE SUM (数量) > 1000
GROUP BY 注文日



問 36 データマイニングの説明として、適切なものはどれか。

- ア** 大量のデータを分析し、単なる検索だけでは発見できない隠れた規則や相関関係を導き出すこと
- イ** データウェアハウスに格納されたデータの一部を、特定の用途や部門用に切り出して、データベースに格納すること
- ウ** データ処理の対象となる情報を基に規定した、データの構造、意味及び操作の枠組みのこと
- エ** 複数の属性項目をデータベースに格納し、異なる属性項目の組合せによる様々な分析を短時間で行うこと



問 37 LAN同士を接続する装置に関する記述のうち、ルータについて述べたものはどれか。

- ア** データリンク層で接続する装置
- イ** ネットワーク層で接続する装置
- ウ** ネットワーク層よりも上位の層で接続する装置
- エ** 物理層で接続する装置

解説

問35 SQLの集計関数

SELECT文において、SUM関数やAVG関数などの**集計関数**を使用して列の値の合計や平均を求める場合、一般的には**イ**のようにGROUP BY句を用います。この文は、正しい構文のSQL文です。

GROUP BY句を用いない場合は、表の全ての行が一つのグループとして1行にまとめられ、合計などが集計されます。その際は、集計関数以外の値(表の列の値など)を、出力することができません。よって、**ア**のようなSQL文は誤りとなります。

ウの文ではSUM関数の結果をAVG関数に与えていますが、このようなこともSQLの文法的に誤りとなります。また、エの文では、WHERE句において“SUM(数量) > 1000”という比較を行っていますが、WHERE句においては集計関数の値を比較対象にすることはできません。よって、これらの文も誤りとなります。

問36 データマイニング

データマイニングは、通常業務において発生した大量のデータを蓄積し、それらを統計解析・ニューラルネットワークなどの数学的手法を用いて分析して、単なる検索だけでは判明しない隠れた法則や因果関係を算出する方法のことです。

- ア 正解です。
- × イ データウェアハウスのデータを、特定の目的用に切り出すのは、データウェアハウスの検索機能の説明です。
- × ウ データ処理の対象となる情報を基に規定したデータの構造や意味、及び枠組みは、データベースのスキーマとなります。
- × エ データウェアハウスによるデータの分析の説明です。

問37 ルータ

ルータは、OSI基本参照モデルのネットワーク層において、複数のネットワークを相互接続する装置です。受信したIPパケットのあて先IPアドレスを参照して、適切な送信先に転送する機能(ルーティング機能)をもっています。

- × ア OSI基本参照モデルのデータリンク層で接続を行うのは、ブリッジやスイッチングハブとなります。
- イ 正解です。
- × ウ OSI基本参照モデルのネットワーク層よりも上位の層で接続を行うのは、ゲートウェイとなります。
- × エ OSI基本参照モデルの物理層で接続を行うのは、リピータとなります。

○ 解答 ○

問 35 イ

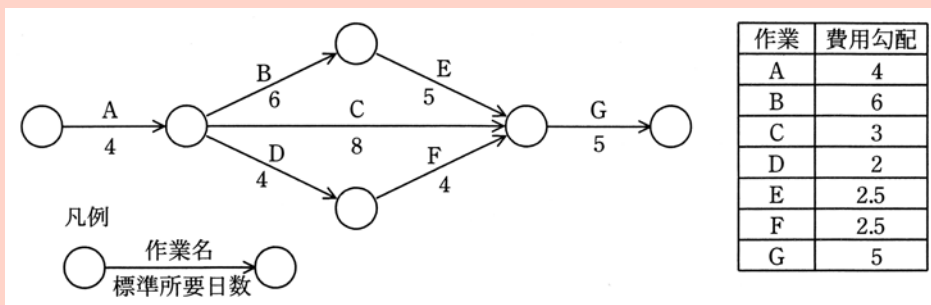
問 36 ア

問 37 イ

問38 IPアドレス 10.1.2.146, サブネットマスク 255.255.255.240 のホストが属するサブネットワークはどれか。

- ア 10.1.2.132/26 イ 10.1.2.132/28 ウ 10.1.2.144/26 エ 10.1.2.144/28

問39 あるプロジェクトでは、図に示すとおり作業を実施する計画であったが、作業Aで1日の遅れが生じた。各作業の費用勾配を表の値とするとき、当初の予定日数で終了するために発生する追加費用を最も少なくするには、どの作業を短縮すべきか。ここで、費用勾配は(特急費用-標準費用) / (標準所要日数-特急所要日数)で求めている。



- ア B イ C ウ D エ E

解説

問38 IPアドレスとサブネット

IPアドレスは、インターネット上の通信プロトコル(TCP/IP)において、コンピュータやサーバなどの機器を全世界中で一意に識別するために付与されるアドレスです。

IPアドレスは32ビット(4バイト)で表現され、32ビット中の上位ビットを「**ネットワーク部**」、残りの下位ビットを「**ホスト部**」と呼びます。

ネットワーク部は特定の組織・団体などを区別するために与えられているもので、電話番号の「市外局番」と「市内局番」にあたります。ホスト部は、組織・団体内の各機器を一意に識別するために与えられるもので、電話番号のうちの加入者番号にあたります。例えば「03-xxxx-……」という電話番号なら、「03」の部分を見るだけで「東京23区内の番号」であると判明するのと同様に、IPアドレスのネットワーク部によって、そのIPアドレスをもつ機器がどの組織や団体に所属しているかを判別することが可能になります。

比較的大規模のLAN環境では、LAN全体を一つのネットワークとするより、LAN全体を細分化して小規模なネットワーク(**サブネット**または**サブネットワーク**)を複数作成し、サブネット内のPCは同じサブネット内の他のPCとだけ通信可能な状態にした方が、有効な場合があります。

ネットワーク内にサブネットを構築するには、IPアドレスのホスト部のうちの一部を、サブネットを区別するための別のアドレスとして扱うことになります。

IPアドレスのうち、ホスト部の上位の数ビットをサブネット識別のためのアドレス「**サブネット部**」とします。サブネットに分割されたネットワークを利用する場合、ネットワーク部とサブネット部をひとまとめにして、サブネットを区別します。

【サブネット分割しないネットワーク】

IP アドレス：

ネットワーク部	ホスト部
---------	------

【サブネット分割したネットワーク】

IP アドレス：

ネットワーク部	サブネット部	ホスト部
---------	--------	------

このサブネット部のビット数により、ネットワークを細分化できる個数(サブネットの個数)が決定します。

IPアドレスの上位何ビットまでが、サブネットを区別するための「ネットワーク部とサブネット部」であるかを表現するには、**サブネットマスク**を用います。サブネットマスクは、「ネットワーク部とサブネット部」がIPアドレスの左から何ビット目までを占めているかを表し、「ネットワーク部とサブネット部」にあたる部分を“1”のビットで、ホスト部に当たる部分を“0”のビットで記載します。

本問に示された、255.255.255.240というサブネットマスクを用いる場合、以下のようになります。

255 . 255 . 255 . 240
 ↓(2進数に直す)
 1111 1111 . 1111 1111 . 1111 1111 . 1111 0000
 ネットワーク部とサブネット部 ホスト部

このサブネットマスクと、IPアドレス(10.1.2.146=00001010.00000001.00000010.10010010)とのAND(論理積)を取った値が、ホストの属するサブネットのネットワークアドレスになります。よって、

```

1111 1111 . 1111 1111 . 1111 1111 . 1111 0000
0000 1010 . 0000 0001 . 0000 0010 . 1001 0010
-----
= 0000 1010 . 0000 0001 . 0000 0010 . 1001 0000
= 10.1.2.144

```

10.1.2.144という値が、PCのネットワークアドレスになります。また、IPアドレスを表記する際には、そのサブネットマスクの1のビットが左(最上位ビット)から数えて何ビット目まで存在しているかを数えて、その値をIPアドレスの末尾に“/”で区切って表記します。例えば、本問に示された255.255.255.240というサブネットマスクでは、1のビットが左から数えて28ビット目まで存在しているため、“10.1.2.144/28”(E)という表記となります。

問39 クリティカルパス

問題文のPERT図より、最後の作業Gは、作業E、C、Fの全てが終了しなければ開始できません。

各作業の終了日時は次のとおりです。

作業E=4+6+5=15日

作業C=4+8=12日

作業F=4+4+4=12日

作業Eの終了日時が最も遅いので、作業Gは15日目から開始できます。**クリティカルパス**はA→B→E→Gとなり、この箇所の作業日数の増減が、全体の完了日数に影響します。

作業Aが1日遅れた場合、クリティカルパス上の他の作業のうちの一つの作業日数を1日縮める(早める)ことが可能なら、全体の完了日数の遅れは1-1=0でプラスマイナス0となり、遅れは生じません。問題文の表より、作業B、E、Gのうち、費用勾配が最も少ないものはE(E)なので、この作業を短縮するのが最も適切です。

○ 解 答 ○

問 38 E

問 39 E



問 40 入力、出力などを基に複雑さを加味してシステム規模を見積もる方法であり、開発工数の見積りにも使われるものはどれか。

- ア COCOMO
- イ 標準タスク法
- ウ ファンクションポイント法
- エ プットナム(Putnum)モデル



問 41 SLAの説明はどれか。

- ア 開発から保守までのソフトウェアライフサイクルプロセス
- イ サービスの品質に関する利用者と提供者間の合意
- ウ システムの運用手法を体系化したフレームワーク
- エ 製品ベンダの品質マネジメントシステムに関する国際規格



問 42 ITIL v2において、日々のITサービス運営手法を示したサービスサポートに分類されている5プロセスと1機能を一覧表にまとめたとき、表中のaに該当するプロセスはどれか。

種別	名称	概要
プロセス	インシデント管理	発生したインシデントに対し、可能な限り迅速に通常のサービス運用を回復して、ビジネスへの悪影響を最小限に抑える。
	a	インシデントや問題の根本原因を特定し、事業に対する悪影響を最小限に抑制し、また再発を防止する。
	構成管理	構成管理データベースを用いて IT サービス提供に必要な構成アイテム (CI) を常に正しく把握し、各プロセスに効果的な情報を提供する。
	変更管理	変更要求 (RFC) の内容について、変更に伴う影響を検証してインパクトや優先度の評価を行い、認可又は却下を決定する。
	リリース管理	承認の得られたコンポーネントを、正しい場所に、適切な時期にリリースする。
機能	サービスデスク	IT サービスを利用する顧客と IT サービスを提供する組織との間の一元的な窓口として活動する。

- ア ITサービス継続性管理
- イ 可用性管理
- ウ サービスレベル管理
- エ 問題管理

解説

問40 システム規模の見積もり

本問の記述は、**ファンクションポイント法**の説明です。

- × **ア COCOMO** (constructive cost model)は、1981年にベームによって提唱されたシステム開発の期間や工数の見積りモデルです。ソフトウェアの規模(プログラムコードの行数)を入力係数とし、設計要員の能力などの補正係数を乗じて、工数や生産性を算出してコストを見積もります。

- × **イ** **標準タスク法**とは、WBSに基づいて切り分けた成果物や処理(作業)単位に工数を見積もり、ボトムアップ的に工数を積み上げていくことでシステム全体の工数を見積もる手法のことです。
- **ウ** 正解です。
- × **エ** **プットナム(Putnum)モデル**とは、仮説を立てることによってプロジェクトの開発工数を予測し、総開発工数を見積もる手法のことです。

問41 SLA

SLA (Service Level Agreement)とは、各種のサービスの品質について、そのサービスの利用者と提供者との間でなされた合意や契約内容のことです。例えば、通信サービスの提供者と利用者の間で、「提供者は利用者に対して、契約回線のデータ通信の遅延は常に10秒以下に抑えるような品質のサービスを提供する。提供者の責によってその品質が満たされなかった場合、当該月の利用料を減殺する」などの契約を結ぶ場合、その契約内容や遅延抑制の目標時間、要求水準を満たせなかった場合の違約金の金額などが、SLAの項目として示されることになります。

- × **ア** **ソフトウェアライフサイクルプロセス**は、SLCP-JCF 2007(共通フレーム)などの規格によって規定されているものです。
- **イ** 正解です。
- × **ウ** システムの運用手法を体系化したフレームワークには、**ITIL**などがあります。
- × **エ** 製品ベンダの品質マネジメントシステムに関する国際規格は、**ISO 9001**となります。

問42 ITIL

ITILとは、1989年に英国政府によって作成・公表された、ITサービスマネジメント(顧客の要件を満たす高品質のITサービスの開発・提供などに必要なプロセスを構築すること)におけるベストプラクティスをまとめたものです。このITILでは、IT業務サービスの運用における実業務に即した知識やノウハウがまとめられています。

ITILは、IT業務サービスの日々の運用手法をまとめた「**サービスサポート**」に関するプロセスと、中長期的なサービスの管理手法をまとめた「**サービスデリバリー**」に関するプロセスからなります。

サービスサポートに関するプロセス：サービスデスク、インシデント管理、問題管理、構成管理、変更管理、リリース管理

サービスデリバリーに関するプロセス：サービスレベル管理、可用性管理、ITサービス財務管理、キャパシティ管理、ITサービス継続性管理など

サービスサポートのプロセスのうちのインシデント管理プロセスとは、情報システムの稼働中に発生した障害(インシデント)から早期に復旧したり、障害を引き起こしかねない事象に適切に対処したりすることで、可能な限りシステムを継続して稼働させようとするためのプロセスのことです。ここでインシデントの発生が確認されると、サービスサポートの**問題管理**プロセスに、インシデントの情報などが伝達されます。問題管理プロセスにおいては、インシデントの影響を最小限に抑制するために、発生したシステムのエラーの根本原因の特定が行われます。

問題管理プロセスにおいてエラーの根本原因が特定されると、当該エラーを修正するための依頼が、**変更管理**プロセスに提出されます。この際に、**RFC** (変更要求, Request For Change)という文書が、提出されます。RFCは、システム上のハードウェアやソフトウェアなどの変更を要求する理由や変更内容などをまとめた書類です。変更管理プロセスでは、提出されたRFCを確認して、変更要求が理に合ったものである場合、システムの変更を行います。

以上から、インシデントなどの根本原因を特定し、インシデントの影響を最小限に抑制するためのプロセス(空欄a)は、問題管理(**エ**)となります。なお、**ア～ウ**は、サービスデリバリーに関するプロセスとなります。

○ 解答 ○

問 40 **ウ**

問 41 **イ**

問 42 **エ**



問 43 監査において発見した問題に対するシステム監査人の責任として、適切なものはどれか。

- ア** 発見した問題を監査依頼者に報告する。
- イ** 発見した問題をシステムの利用部門に通報する。
- ウ** 発見した問題を被監査部門に是正するよう命じる。
- エ** 発見した問題を自らは正する。



問 44 データ入力の変換を発見し、修正するのに有効な内部統制手続はどれか。

- ア** ドキュメンテーションの完備
- イ** 取引記録と入力データの照合
- ウ** 入力時のフィールド検査
- エ** バックアップリカバリ手順の確立



問 45 エンタープライズアーキテクチャを説明したものはどれか。

- ア** 今まで開発してきた業務システムをビジネス価値とソリューション品質の2軸で分析し、業務システムごとの改善の方向を決定する。
- イ** 既存の業務と情報システムの全体像及び将来の目標を明示することによって、ITガバナンスを強化し、経営の視点からIT投資効果を高める。
- ウ** 財務、顧客、業務プロセス、学習・成長の四つの視点から評価指標を設定し、IT投資による組織全体への効果を的確に管理する。
- エ** 情報システムの開発・保守とその組織運営の現状を調査し、ソフトウェアプロセスの成熟度を評価して、プロセス改善の方向を決定する。

解説

問43 システム監査人

システム監査人は、被監査部門の上長などの監査依頼者からの依頼を受け、被監査部門(組織体)の情報システムなどの状況を客観的に監査し、その結果判明した情報システムの改善点や問題点などを監査報告書にまとめて監査依頼者に提出し、改善の勧告や助言を行う責任をもちます。なお、システム監査人は、発見した問題を自らは正したり、問題の是正を被監査部門に命令したりする権限はもっていません。システム監査によって発見された問題の是正は、被監査部門の行うべき業務となります。

- **ア** 正解です。
- × **イ** システム監査人が発見した問題は、システムの利用部門ではなく、監査依頼者に報告されることになります。システムの利用部門に問題を通報するのは、不適切な行為です。
- × **ウ** システム監査によって発見された問題の是正は、被監査部門の行うべき仕事となります。システム監査人は、発見した問題の是正を被監査部門に命令するといった権限はもっていません。
- × **エ** システム監査によって発見された問題の是正は、被監査部門の行うべき仕事となります。システム監査人は、発見した問題を自らは正する権限はもっていません。

問44 データ入力重複

データ入力重複を発見するためには、システムに入力されたデータと、取引記録(帳票など)のデータとを比較・照合し、取引記録に存在しないデータがシステムに入力されていたり、取引記録の同じデータが2回以上システムに入力されたりしていないかを確認し、データの重複がある場合には修正することが適切な措置となります。したがって、イの記述が正解となります。

- × ア ドキュメンテーションの完備により、データ入力のマニュアルなどが充実することになります。しかし、データ入力のマニュアルなどが充実しても、入力者のミスなどによってデータ入力重複が発生することがあるため、ドキュメンテーションの完備を行うだけでなく、システムに入力されたデータの参照を行う必要があります。
- イ 正解です。
- × ウ 入力時のフィールド検査により、誤った値のデータが入力されようとしたときに、それをチェックして再入力を促すことができます。しかし、正しい値の同じデータが2回以上連続して入力され、入力データが重複した場合には、入力時のフィールド検査では重複を発見できません。
- × エ バックアップリカバリ手順を確立しても、システムのデータをバックアップして残すことができるだけであり、システムに入力されたデータの重複を発見することはできません。

問45 エンタープライズアーキテクチャ

エンタープライズアーキテクチャ(Enterprise Architecture)とは、組織の業務や情報システムを、政策・業務体系、データ体系、適用処理体系及び技術体系という4つの体系で分析して、業務や情報システムの最適化などを進めたり、全体最適化の観点から業務の問題点などを見直したりすることで、ITガバナンスを強化して経営の視点からIT投資効果を高めようとする技法のことです。

- × ア ビジネス価値とソリューション品質の2軸で業務システムを分析するのは、一般的なシステム分析・改善手法であり、具体的な名称はありません。
- イ 正解です。
- × ウ 財務、顧客、業務プロセス、学習・成長の4つの視点から評価指標を設定する技法は、バランススコアカードとなります。
- × エ ソフトウェアプロセスの成熟度を評価してプロセス改善の方向を決定する技法は、CMMI(Capability Maturity Model Integration)となります。

○ 解答 ○

問43 ア

問44 イ

問45 イ



問 46 業務プロセスのモデリング表記法として用いられ、複数のモデル図法を体系化したものはどれか。

- ア** DFD **イ** E-R図 **ウ** UML **エ** 状態遷移図

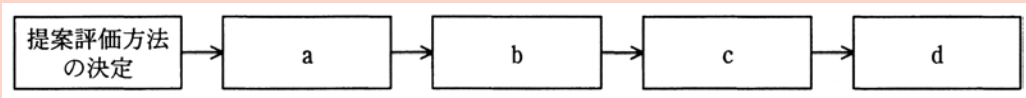


問 47 共通フレーム2007によれば、非機能要件に該当するものはどれか。

- ア** 新しい業務の在り方をまとめた上で、業務上実現すべき要件
イ 業務の手順や入出力情報、ルールや制約などの要件
ウ 業務要件を実現するために必要なシステムの機能に関する要件
エ ソフトウェアの信頼性、効率性など品質に関する要件



問 48 “提案評価方法の決定”に始まる調達プロセスを、調達先の選定、調達の実施、提案依頼書(RFP)の発行、提案評価に分類して順番に並べたとき、cに入るものはどれか。



- ア** 調達先の選定 **イ** 調達の実施
ウ 提案依頼書(RFP)の発行 **エ** 提案評価

解説

問46 業務プロセスのモデリング表記法

業務プロセスのモデリング表記法として用いられ、複数のモデル図法を体系化しているのは、**UML**です。UMLには、業務プロセスやシステムの構成などを表現するためのユースケース図、クラス図、シーケンス図、ステートチャート図などの各種のモデル図法が存在しています。

- × **ア** **DFD**は、データの流れを表すための図法です。
× **イ** **E-R図**は、エンティティ(実体)とリレーションシップ(関連)を表すための図法です。
○ **ウ** 正解です。
× **エ** **状態遷移図**は、ある状態から別の状態に遷移する条件や遷移後の状態などを表すための図法です。

問47 共通フレームの非機能要件

ソフトウェアライフサイクルプロセスの作業項目を可視化した規格として、システム開発と取引のための共通フレームがあります。ソフトウェアライフサイクルプロセスとは、企画、要件定義、開発、運用及び保守といった、ソフトウェア(システム)を企画し、開発し、それを運用していく過程で一連のプロセス(業務)をまとめたものです。

共通フレームは、ソフトウェアライフサイクルプロセスにおける作業全般にわたって使用される用語などを統一して、作業範囲や作業内容を明確にするための基準となります。共通フレームは、委託側と請負側とで共有する「システム開発作業全般にわたった共通の枠組み・共通の物差し」といわれることが多いようです。共通フレームによって、シ

システムの購入者・供給者双方が、明確な基準によって取引を実行できます。

共通フレームの要件定義プロセスでは、業務内容や業務特性などの、業務上実現すべき要件(業務要件)を実現するために必要な、システムの機能要件(システムのデータの流れや、システムの処理の内容、入出力情報など)を定義するとともに、システムの機能要件以外の要件(非機能要件)を定義すると規定しています。

非機能要件とは、システムの使いやすさや処理性能・処理効率の高さ、処理時間の早さ、及び障害発生時の復旧時間の早さなど、要件定義の段階で定義される機能などとは直接の関係がない、システムの利用状況に関する各種の要素のことです。非機能要件の例としては、品質要件(機能性、信頼性、効率性などの要素)があります。

以上から、解答群エの記述が適切です。

- × ア 業務上実現すべき要件は、システムの機能要件となります。
- × イ 業務の手順や入出力情報などは、システムの機能要件となります。
- × ウ 「システムの機能に関する要件」との記述から、システムの機能要件となります。
- エ 正解です。

問48 調達プロセス

システムの取得者が、複数のベンダからシステムの調達先を選定する際のプロセス(調達プロセス)は、おおよそ以下のような順序となります。

1. 提案評価方法の決定

複数のベンダのうち、どのベンダにシステムを発注するかを選定するための評価方法や評価において用いるべき基準(システムの価格、調達先の経営状態など)を、最初に決定します。

2. 提案依頼書(RFP)の発行(ウ)

RFP(Request For Proposal, 提案依頼書)とは、情報システムの取得者からベンダに対して送付されるもので、発注する情報システムの概要や発注依頼事項、調達条件及びサービスレベル要件などを明示し、情報システムの提案書の提出を依頼するための文書です。RFPを受け取った各ベンダは、取得者に対して情報システムの提案書を提出します。

3. 提案評価(エ)

取得者は、各ベンダから提出された情報システムの提案書の内容を、1.の段階において決めていた提案評価方法に従って評価します。

4. 調達先の選定(ア)

取得者は、3.の段階にて最も高い評価を得た提案書を提出してきたベンダを、調達先として選定します。

5. 調達の実施(調達先との契約締結)(イ)

取得者は、4.の段階にて調達先として選定したベンダとの間で契約を結び、システムを発注します。

以上から、本問の図のcの段階に入るのは、「調達先の選定(ア)」です。

○ 解答 ○

問 46 ウ

問 47 エ

問 48 ア

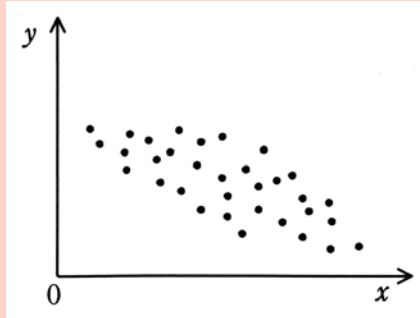


問 49 プロジェクトを準独立的な事業として遂行し、その成果に対して全面的な責任を負う起業家としての権限と責任を与えられる組織構造はどれか。

- ☐ ア 事業部制組織
- ☐ イ 社内ベンチャ組織
- ☐ ウ 職能別組織
- ☐ エ マトリックス組織



問 50 図は、製品の製造上のある要因の値 x と品質特性の値 y との関係をプロットしたものである。この図から読み取れることはどれか。



- ☐ ア x から y を推定するためには、2次回帰係数の計算が必要である。
- ☐ イ x から y を推定するための回帰式は、 y から x を推定する回帰式と同じである。
- ☐ ウ x と y の相関係数は正である。
- ☐ エ x と y の相関係数は負である。

解説

問49 準独立的な事業

新たなプロジェクトを準独立的な事業として社内で遂行するために、選抜した人員から構成された新しい事業部を社内につくったり、子会社を設立したりすることを、**社内ベンチャ**といいます。社内ベンチャを実現するために、プロジェクトの成果に対して全面的な責任を負う起業家としての権限と責任を与えられる組織構造のことを、社内ベンチャ組織といいます。

- × ☐ **事業部制組織**とは、利益責任と業務遂行に必要な機能を事業部別にもつことで、自己完結的な経営活動を展開できる組織構造のことです。
- ☐ **正解です。**
- × ☐ **職能制(職能別)組織**とは、企業における各種の活動の性質(職能)別に分類された組織構造のことです。
- × ☐ **マトリックス組織**とは、自分の専門の職能部門と、特定のプロジェクトを遂行する部門の両方に、組織の人員が所属する形態の組織構造のことです。

問50 散布図

散布図は、2つのデータの間に相関関係が存在するかを調べるために用いられます。**相関関係**とは、「あるデータ x の値が増減するとき、別のデータ y の値もそれに応じて増減する」という関係のことです。データ x とデータ y の間

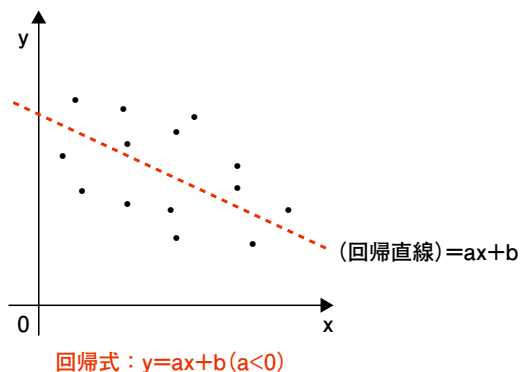
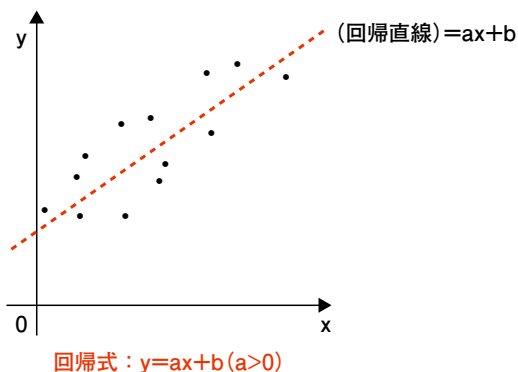
に相関関係がある場合、両者の間には何らかのつながりがあるとみなせる可能性があります。

散布図では、データ x 及び y を横軸・縦軸にとり、 x と y の値を点としてプロットしていきます。プロットした結果の点の集合が右上がりになっていれば、「**正の相関**」があるということになります。逆に、点の集合が左上がりになっていれば、「**負の相関**」があるということになります。

正の相関または負の相関を表すために、**相関係数**という指標が用いられます。二つのデータの間の相関係数は、最小自乗法などの方法によって計算することができます。相関係数が正の値であれば正の相関、負の値であれば負の相関が、二つのデータ間に存在することになります。

この問題では、点の集合が左上がりになっているため、 x と y の間には「負の相関」があると考えられます。よって、 x と y の相関係数は負となります(**エ**)。

× **ア** 2次回帰係数とは、“ $y=ax^2+b$ ”のように、 x と y の間の関係が2次式で表されるような、複雑な関係を示している二つのデータ間の関係を式で表現するために用いられるものです。本問の散布図は、以下のような1次式の回帰式で表される関係になっているため、2次回帰係数を用いる必要はありません。



× **イ** x から y を推定するための回帰式と、 y から x を推定するための回帰式は、一般的には異なる式になります。例えば、 x から y を推定するための回帰式を“ $y=2x$ ”とすると、 y から x を求めるための回帰式は“ $x=y/2$ ”となり、両式は異なることになります。

× **ウ** x と y の間の相関係数は、正ではなく負になります。

○ **エ** 正解です。

○ 解答 ○

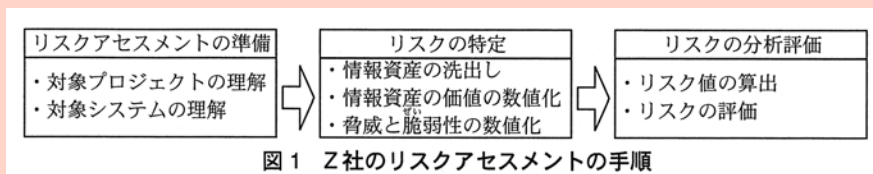
問 49 **イ**

問 50 **エ**

第2回 模擬試験 午後 問題

問 1 情報資産についてのリスクアセスメントに関する次の記述を読んで、設問1～3に答えよ。

Z社は、従業員数が500の中堅SIベンダである。Z社では、プロジェクト開始前に、プロジェクトで扱う情報資産について、図1に示す自社で定めた手順に従って、リスクアセスメントを実施している。このたび、新規に受注したプロジェクトYに対して、リスクアセスメントを実施することになった。



〔プロジェクトYの説明(抜粋)〕

- (1) 顧客が利用する購買システムを開発する。
- (2) 開発で利用するテストデータは顧客から提供される。
- (3) 顧客のテストデータを格納した顧客のUSBメモリを、プロジェクトメンバが顧客から受け取って自社に持ち帰り、顧客のテストデータを開発用サーバに複写後、USBメモリから削除する。
- (4) Z社から顧客の事務所を訪問するのに、電車で1時間30分ほど要する。
- (5) 開発用PCでプログラムを開発し、適宜、開発用サーバにアップロードする。

〔Z社の開発環境(抜粋)〕

- (1) プログラムの開発には、開発用サーバと開発用PCを利用する。
- (2) 開発用サーバは、施錠されたサーバールームに設置されている。
- (3) 開発用サーバは、アクセス管理がされており、プロジェクトメンバとシステム管理者だけがアクセスできる。
- (4) 開発用PCは、プロジェクト開始時にシステム部から各プロジェクトメンバに貸与され、プロジェクト終了時に返却される。

〔Z社の開発標準(抜粋)〕

- (1) 開発時、プロジェクトメンバは顧客のテストデータのうち必要なものだけを、開発用サーバから自分の開発用PCにダウンロードし、不要になったら削除する。
- (2) プロジェクト終了時に、プロジェクトマネージャは開発用サーバの顧客のテストデータを削除し、全ての開発用PCから顧客のテストデータが削除されていることを確認する。

〔Z社のリスク値算出方法〕

Z社では、各情報資産のリスク値を、次の式で算出する。

$$\text{リスク値} = \text{情報資産の価値} \times \text{脅威} \times \text{脆弱性}$$

ここで、“情報資産の価値”とは情報資産が損なわれたときの影響の大きさを意味し、機密性(以下、Cと

いう)、完全性(以下、Iという)、可用性(以下、Aという)の観点に対して、影響の大きさをそれぞれ1～3の値で評価する。“脅威”は、発生の可能性の大きさを1～3の値で評価する。“脆弱性”は、脅威が発生した場合に被害が顕在化する度合いの大きさを1～3の値で評価する。ここで、各1～3の値は大きい場合を3、小さい場合を1とする。

C, I, A ごとに算出したリスク値が全て12以下ならばリスクを受容し、そうでないならば追加のリスク対策を実施することとしている。

〔リスクの特定〕

① 情報資産の洗出し

プロジェクトYで扱う情報資産の洗出しを行った。その結果を、表1に示す。

表1 情報資産の洗出し結果

No.	情報資産	作成又は取得	保管場所	廃棄
⋮				
3	開発用サーバ上の開発中のプログラム	プロジェクトメンバが開発用サーバにアップロードする	開発用サーバ	プロジェクト終了時に削除する
4	顧客のテストデータ	顧客の USB メモリで受領して、開発用サーバに複写する	顧客の USB メモリ、開発用サーバ及び開発用 PC	
⋮				

注記 網掛けの部分は表示していない。“…”は表示の省略を示している。

② 情報資産の価値の数値化

表1の各情報資産に対して、C, I, Aのそれぞれについてその価値を評価した値と評価理由を、表2に示す。

表2 情報資産の価値と評価理由

No.	情報資産	C	I	A	価値の評価理由
⋮					
3	開発用サーバ上の開発中のプログラム	3	3	3	(i) 開発中のプログラムが利用できない場合、プロジェクトの進捗に影響を与える (ii) 社外に漏れた場合、顧客からの信頼を失う (iii) 版管理が行われない場合、不整合によって、プロジェクトの進捗に影響を与える
4	顧客のテストデータ	3	2	1	
⋮					

注記 網掛けの部分は表示していない。“…”は表示の省略を示している。

③ 脅威の数値化

表2の情報資産のうち、情報資産No.4(顧客のテストデータ)について、脅威の内容と脅威の値を、表3に示す。

表3 情報資産 No.4 の脅威の内容と値

No.	脅威 ID	脅威の内容	値
4	T1	顧客のテストデータを格納した顧客の USB メモリを自社に持ち帰る途中で紛失する	3
	T2	開発用サーバが外部から不正アクセスされて顧客のテストデータが盗み出される	1
	T3	ウイルス感染によって顧客のテストデータの破壊又は漏えいが発生する	2
	T4	開発用サーバに複写後、顧客の USB メモリから顧客のテストデータが漏えいする	3
	T5	テスト終了後、不要になった顧客のテストデータが開発用 PC から漏えいする	2
	T6	プロジェクトメンバ又はシステム管理者が顧客のテストデータを開発用サーバから取り出してサーバールームから持ち出す	1
	T7	開発用サーバから顧客のテストデータが滅失する	1

④ 脅威に対する脆弱性の数値化

表3の各脅威に対する脆弱性の低減策と脆弱性の値を、表4に示す。脆弱性の値は、システム、規則又は運用で、二つ以上対策済みなら1、一つだけなら2、未対策は3とする。

表4 表3の脅威に対する脆弱性の低減策と値

脅威 ID	脆弱性 ID	脆弱性の低減策	値
T1	Z1	・顧客の USB メモリに顧客のテストデータを保存するときに暗号化してもらう	2
T2	Z2	・脆弱性に対する対策なし	3
T3	Z3	・開発用サーバと開発用 PC にウイルス対策ソフトを導入し、ウイルス定義ファイルを自動更新する ・顧客の USB メモリをウイルスチェックした後に顧客のテストデータを開発用サーバに複写する	1
T4	Z4	・顧客の USB メモリから顧客のテストデータが削除されていることをプロジェクトマネージャが確認する	2
T5	Z5	・開発用 PC から顧客のテストデータが削除されていることをプロジェクトマネージャが確認する	2
T6	Z6	・社員証による入退室管理を行う ・サーバールームに監視カメラを設置する	1
T7	Z7	・脆弱性に対する対策なし	3

〔リスクの分析評価〕

表2～4を基に情報資産 No.4 (顧客のテストデータ) のリスクの分析評価を行い、リスク値を算出した結果を、表5に示す。

表5 情報資産 No.4 のリスク値

No.	情報資産の価値			脅威		脆弱性		リスク値			
	C	I	A	脅威 ID	値	脆弱性 ID	値	リスク値 ID	C	I	A
4	3	2	1	T1	3	Z1	2	R1	18	12	6
				T2	1	Z2	3	R2	9	6	3
				T3	2	Z3	1	R3			
				T4	3	Z4	2	R4			
				T5	2	Z5	2	R5			
				T6	1	Z6	1	R6			
				T7	1	Z7	3	R7			

注記 網掛けの部分は表示していない。

プロジェクトYのプロジェクトマネージャは、リスクの分析評価の結果からリスク対応計画を作成した。その後、リスク対策を実施した。

設問1 表2中の(ii), (iii)は、C, I, Aのいずれかの観点から“情報資産の価値”を評価した際の評価理由である。(ii), (iii)に対応するC, I, Aの組合せとして適切な答えを、解答群の中から選べ。

解答群

	(ii)	(iii)
ア	A	C
イ	A	I
ウ	C	A
エ	C	I
オ	I	A
カ	I	C

設問2 情報資産No.4(顧客のテストデータ)に対するリスクの分析評価の結果、追加のリスク対策が必要になる脅威の数として正しい答えを、解答群の中から選べ。

解答群

ア 1 **イ** 2 **ウ** 3 **エ** 4

設問3 社内でのセキュリティ事故の発生と対策に関する次の記述中の **a** , **b** に入れる適切な答えを、解答群の中から選べ。

プロジェクトYの終了後、新たに発足したプロジェクトXで利用している開発用PCに、プロジェクトYの顧客のテストデータが格納されている、とシステム部に連絡があった。調査した結果、このPCは、プロジェクトYで利用していた開発用PCであり、システム部に返却された後に、システム部からプロジェクトXに貸与されたものであることが判明した。そこで、Z社では、顧客のテストデータの漏えいというリスクに対処するために、 **a** , **b** という対策を追加することにした。

解答群

- ア 開発用サーバのアクセスログをシステム部が定期的に確認する
- イ 顧客のテストデータを開発用PCにダウンロードして利用する場合は、管理台帳にダウンロード日、削除日、実施者を記入する
- ウ 顧客のテストデータを開発用PCに保存する際に、警告メッセージが表示されるようにする
- エ プロジェクトごとに新たに開発用サーバを用意する
- オ プロジェクトメンバが開発用サーバ上の顧客のテストデータにアクセスする権限を参照だけに設定する
- カ 返却された開発用PCは、システム部が全データを完全消去する工程を追加する

解説

情報セキュリティのリスクアセスメントに関する問題です。

設問の解説に入る前に【リスクアセスメント】について解説します。

【リスクアセスメント】

リスクアセスメントとは、情報システムの開発などの各種プロジェクトに関連する情報資産を洗い出し、その価値を数値化するとともに、各情報資産にまつわる脅威（情報システムや情報資産に対して悪い影響を与える出来事が発生する可能性）の大きさと、脆弱性（情報システムや情報資産に対して脅威が発生したときに、被害が顕在化する度合い）の大きさを数値化して、それらを基にして情報資産のリスク値を算出することです。

リスクアセスメントを実施するとき、一般的には情報資産のリスク値を、本問の計算式と同様に次の式で算出します。

リスク値＝情報資産の価値×脅威×脆弱性

情報資産の価値、脅威、及び脆弱性の値が大きいほど、リスク値も大きくなります。リスク値が大きい情報資産は、価値が大きいため喪失や漏えいによる損害額が大きくなり、脅威が大きいため喪失や漏えいなどが発生する確率が高く、また脆弱性が大きいため被害が顕在化する度合いが大きくなります。したがって、リスク値が大きい情報資産については、追加のリスク対策を実施するなどの措置をとることで、脅威や脆弱性の大きさを小さくする必要があります。

設問 1 情報セキュリティの三要素

JIS Q 27001 などの主要な情報セキュリティの規

格では、次の三つの要素を情報セキュリティの三要素としています。

要素	概要
機密性 (Confidentiality)	不特定多数からデータにアクセスされないようにして、適切な権限をもつ者だけがアクセスできるようにする性質
完全性 (Integrity)	データの内容が不正に削除されたり改ざんされたりしないようにして、内容を矛盾なく保つようにする性質
可用性 (Availability)	適切な権限をもつ者が、必要ときにシステムやデータを利用できるようにする性質

以上の三つを情報のCIAということがあります。

表2の下線(ii)の記述は「社外に漏れた場合、顧客からの信頼を失う」です。開発中のプログラムが社外に漏れることで、適切な権限をもつ者（Z社のプロジェクトメンバとシステム管理者）以外の者がその内容にアクセスされるので、機密性(C)が失われることになります。この記述は、「C」の観点から情報資産の価値を評価した際の評価理由です。

表2の下線(iii)の記述を可用性(A)と考え、ウと誤答することがあるので注意が必要です。この記述は「版管理が行われない場合、不整合によって、プロジェクトの進捗に影響を与える」です。開発中のプログラムの版（バージョン）の管理を適切に実行しないと、古いバージョンのプログラムを新しいバージョンのプログラムに上書きしてしまい、プログラムが最新の状態にならなくなるという不整合が発生します。すなわち、この不整合によってプログラムの内容に矛盾が発生するので、完全性(I)が失われることになります。この記述は、「I」の観点

表A

情報資産の脅威			脅威の値	脆弱性の値	リスク値			
C	I	A			リスク値ID	C	I	A
3	2	1	2	1	R3	3×2×1=6	2×2×1=4	1×2×1=2
			3	2	R4	3×3×2=18	2×3×2=12	1×3×2=6
			2	2	R5	3×2×2=12	2×2×2=8	1×2×2=4
			1	1	R6	3×1×1=3	2×1×1=2	1×1×1=1
			1	3	R7	3×1×3=9	2×1×3=6	1×1×3=3

から情報資産の価値を評価した際の評価理由です。また、(i)の記述が「開発中のプログラムが利用できない場合、……」なので、開発中のプログラムというデータを必要なときに利用できないことになり、可用性が失われます。(i)が可用性(A)なので、残りの(ii)と(iii)は機密性が完全性のいずれかと予測できることから、(iii)を可用性と考えるという誤りを犯さないようにしましょう。

以上から、**E**の組合せが正解です。

設問2 リスク分析評価

情報資産No.4のC、I及びAのリスク値R1とR2を求めます。

- R1 (対応する脅威ID=T1, 脆弱性ID=Z1)

C: 情報資産No.4の価値(C)=3, 脅威の値=3, 脆弱性の値=2

$3 \times 3 \times 2 = 18$ (12を超えている)

I: 情報資産No.4の価値(I)=2, 脅威の値=3, 脆弱性の値=2

$2 \times 3 \times 2 = 12$

A: 情報資産No.4の価値(A)=1, 脅威の値=3, 脆弱性の値=2

$1 \times 3 \times 2 = 6$

- R2 (対応する脅威ID=T2, 脆弱性ID=Z2)

C: 情報資産No.4の価値(C)=3, 脅威の値=1, 脆弱性の値=3

$3 \times 1 \times 3 = 9$

I: 情報資産No.4の価値(I)=2, 脅威の値=1, 脆弱性の値=3

$2 \times 1 \times 3 = 6$

A: 情報資産No.4の価値(A)=1, 脅威の値=1, 脆弱性の値=3

$1 \times 1 \times 3 = 3$

以上から、**表5**のリスク値のうち網掛けになっていない部分の値を確認しました。他のリスク値(R3～R6)

についても同様に計算した結果を、**表A**に示します。表Aの太字部分は、算出したリスク値が12を超えている部分です。

以上から、リスク値IDがR1のCのリスク値が18、リスク値IDがR4のCのリスク値が18となっているので、この二つのリスクに対応する二つの脅威(T1, T4)に対して、追加のリスク対策が必要になります。正解は**E**(2)です。

設問3 セキュリティ事故への対策

空欄a, b

「開発用PCに、プロジェクトYの顧客のテストデータが格納されている」、「このPCは、プロジェクトYで利用していた開発用PCであり、システム部に返却された後に、システム部からプロジェクトXに貸与された」との記述から、プロジェクトYで利用していた開発用PCに保存していた顧客のテストデータを削除するのを忘れていたと判明します。Z社の開発標準の(1)では、不要になったテストデータをプロジェクトメンバが開発用PCから削除することを規定し、(2)ではプロジェクト終了時にプロジェクトマネージャが開発用PCからテストデータが削除されていることを確認すると規定しています。これらの規定が守られておらず、不要になった顧客のテストデータが開発用PCに残っていたため、設問3のセキュリティ事故が発生しました。

以上から、開発用PCに保存していた顧客のテストデータを確実に削除するための対策をとる必要があります。解答群の中で、開発用PCに保存した顧客のテストデータに関する対策は、**E**(顧客のテストデータを開発用PCにダウンロードして利用する場合は、管理台帳にダウンロード日、削除日、実施者を記入する)と**カ**(返却された開発用PCは、システム部が全データを完全消去する工程を追加する)だけです。**E**の対策により、顧客のテストデータを削除する日が管理台帳に記載されるので、そ

れを参照することで指定した日に顧客のテストデータを削除することを励行できます。また、**力**の対策により、システム部に返却された開発用PCの全データは必ず完全消去されるので、顧客のテストデータが削除されずに残ることはなくなります。

以上から、空欄a, bには**イ**と**カ**が順不同で入ります。なお、**ア**, **エ**, **オ**は開発用PCではなく開発用サーバに関する対策です。これらの対策をとっても、開発用PCに保存された顧客のテストデータの削除忘れを防止することはできません。また、**ウ**の対策では、顧客の

テストデータを保存するときに警告メッセージを表示するだけなので、プロジェクトメンバがそれを読み流してしまえば、顧客のテストデータを開発用PCに保存したり、削除せずに残したりすることができます。よって、開発用PCに保存された顧客のテストデータの削除忘れを防止することはできません。

° 解答 °

設問 1 **エ** 設問 2 **イ**
設問 3 a: **イ** b: **カ** (a, b 順不同)

問 2

ICカードを利用した入退室管理システムに関する次の記述を読んで、設問1～5に答えよ。

J社は、中規模のSIベンダであり、外部の協力が必要なシステム開発のときには、プロジェクトごとに協力会社と契約している。J社には、開発室と執務室があり、開発室には執務室を通して入退室する。各室の出入口の内側と外側にICカード読取り装置が設置されており、社員と、協力会社社員（以下、協力社員という）の入退室は、入退室管理システムで管理されている。社員及び協力社員は入退室時に、ICカードを読取り装置にかざし、入室時には更にパスワードを入力することによって、出入口の扉が開錠される。また、扉が閉められると、自動的に施錠される。

J社の入退室管理システムのセキュリティ要件は、次のとおりである。

〔J社の入退室管理システムのセキュリティ要件〕

- (1) 社員及び協力社員は、プロジェクトに参画している期間中だけ開発室に入室可能とする。
- (2) ICカードには、①耐タンパ性をもつものを使用し、ICカードIDだけを情報としてもつ。
- (3) ②入退室管理システムは入退室のログを収集する。
- (4) 入退室のログから、開発室又は執務室への入退室ごとの出入りした社員又は協力社員、日時、出入口が特定できる。
- (5) パスワードは8桁の数字(00000000～99999999)とする。
- (6) 有効期間中は、ICカードとパスワードによって開発室や執務室への入室ができる。
- (7) 入室時又はパスワードの変更時に、3回連続してパスワードを誤って入力した場合、開発室や執務室への入室はできなくなる。

なお、J社では、社員や協力社員が、同時に複数のプロジェクトに参画することはない。

〔入退室管理システムの説明〕

入退室管理システムが管理する、利用者情報のうち主なものを表1に、入退室情報のうち主なものを表2に示す。

表1 主な利用者情報

利用者情報	説明
利用者 ID	社員の場合は社員番号を設定し、協力社員の場合は契約時に個人ごとに付与される契約番号を設定する。
IC カード ID	IC カードを識別する一意の ID
IC カードの状態	“仮パスワード”、“有効”、“返却”、“一時利用停止”のいずれかである。IC カードを発給したときは、“仮パスワード”を設定する。3 回連続してパスワードを誤って入力した場合、“一時利用停止”になる。
入室許可の状態	“開発室許可”、“執務室だけ許可”、“入室不可”のいずれかである。
有効期間の終了日	社員の場合は、退職予定の年月日を設定しておく。協力社員の場合は契約期間に基づいて契約終了予定の年月日を設定しておく。
(上記以外の利用者情報) 氏名、有効期間の開始日、利用者区分、プロジェクト番号、パスワードなど	

表2 主な入退室情報

入退室情報	説明
IC カード利用日時	出入口で IC カードをかざした年月日時分秒
IC カード読取り装置識別番号	出入口に設置している IC カード読取り装置を識別する一意の番号
IC カード ID	出入口でかざした IC カードの ID

〔入退室管理システムの運用の説明〕

セキュリティ管理者は、入室申請の受付、入退室管理システムへの利用者情報の設定、ICカードの発給を担当する。

(1) 社員に対する運用は、次のとおりである。

- (a) 社員の入社時に、入退室管理システムの運用ルールを説明した後、ICカードを発給し、パスワードを仮パスワードから変更させる。これで社員の執務室への入室が可能となる。
- (b) プロジェクトの開始時及び終了時に、プロジェクトマネージャ(以下、PMという)からの申請を受けて、開発室へのプロジェクトメンバの“入室許可の状態”の設定を変更する。
- (c) 退職時には、ICカードを返却させるとともに、“有効期間の終了日”に退職日を、“ICカードの状態”に“返却”を設定する。

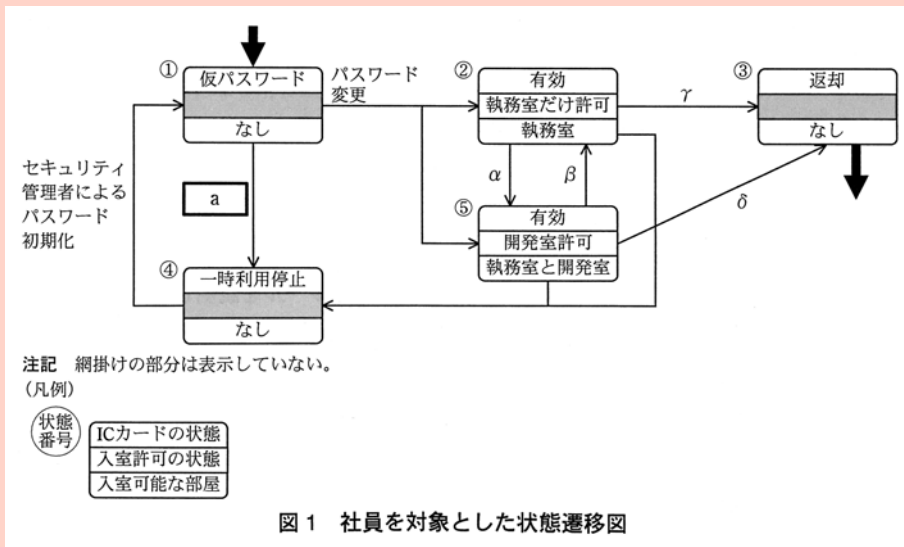
(2) 協力社員に対する運用は、次のとおりである。

- (a) プロジェクト開始時に、PMからの申請を受けて、当該協力社員の利用者情報を登録すると同時に“入室許可の状態”を設定し、PMに協力社員用のICカードを発給する。ICカードを受領したPMは入退室管理システムの運用ルールを協力社員に説明した後、ICカードを配布してパスワードを仮パスワードから変更させる。
- (b) 契約の終了時は、協力社員に配布していたICカードの返却をPM経由で受けて、“有効期間の終了日”に契約の終了日を、“ICカードの状態”に“返却”を設定する。

(3) 利用者情報の削除処理は、次のとおりである。

- (a) “有効期間の終了日”を過ぎ、かつ、“ICカードの状態”が“返却”の利用者情報は、週末のバッチ処理でバックアップメディアに保存した上で、入退室管理システムから削除する。
- (b) 返却されたICカードは、後日再利用する。

入退室管理システムで管理する, 社員を対象にした“ICカードの状態”, “入室許可の状態”及び“入室可能な部屋”の関係を表す状態遷移図を, 図1に示す。



設問1 【J社の入退室管理システムのセキュリティ要件】の説明中の下線①のICカードの説明として正しい答えを, 解答群の中から選べ。

解答群

- ☐ ア 一部が破損しても利用できるICカード
- ☐ イ 外部から強い衝撃があっても変形しないICカード
- ☐ ウ 内部情報に外部から不正にアクセスできないICカード
- ☐ エ 返却後に, 再利用できるICカード

設問2 【J社の入退室管理システムのセキュリティ要件】の説明中の下線②のログとして収集するのが適切な情報を, 解答群の中から選べ。

解答群

- ☐ ア ICカード読取り装置識別番号, ICカードID, 利用者ID
- ☐ イ ICカード利用日時, ICカードID, 利用者ID
- ☐ ウ ICカード利用日時, ICカード読取り装置識別番号, ICカードID, 利用者ID
- ☐ エ ICカード利用日時, ICカード読取り装置識別番号, 入室許可の状態

設問3 図1の a に入れる正しい答えを, 解答群の中から選べ。

解答群

- ☐ ア 3回連続してパスワードを誤入力
- ☐ イ 社員の入社
- ☐ ウ 入退室管理システムの異常
- ☐ エ プロジェクトの終了

設問4 図1を基に、最少の変更で、協力社員を対象にした状態遷移図を作成するとした場合、協力社員が契約を終了して遷移する矢印として適切な答えを、解答群の中から選べ。

解答群

ア a

イ β

ウ γ

エ δ

設問5 J社では内部監査時に、開発室及び執務室の入退室に関する調査を行ったところ、入退室管理システムのログに、入室履歴のない退室履歴や退室履歴のない入室履歴が見つかった。そこで、更に調査した結果、直前に入退室した者がいるとき、扉が施錠される前に、自分のICカードを使わずに入退室する者がいることが分かった。そこで、入退室時には自分のICカードを必ず読取り装置にかざさせる対策として、教育を実施するとともに入退室管理システムで管理する現在の状態遷移を変更することにした。図1の状態番号のうち、入室履歴又は退室履歴のない者がICカードをかざして退室又は入室しようとした際に、遷移する先として適切な状態番号を、解答群の中から選べ。

解答群

ア ①

イ ②

ウ ③

エ ④

オ ⑤

解説

ICカードの運用に関する問題です。設問1では耐タンパ性の知識が必要になります。

設問1 耐タンパ性

耐タンパ性(tamper resistant)とは、ICカード内の情報の不正読取に対抗するための保護機能のことです。具体的には、ICカード内部のチップを保護膜で厳重に包み、保護膜をはがしてチップを読み取ろうとするとチップ自体が破壊されるような仕組みにしておくという技術などが考案されています。ウが正解です。

設問2 収集すべき情報

〔J社の入退室管理システムのセキュリティ要件〕の(3)で入退室のログを収集すると説明されています。続く(4)では、「入退室のログから、開発室又は執務室への入退室ごとの出入りした社員又は協力社員、日時、出入口が特定できる」と説明されています。よって、入退室のログとして収集するのが適切な情報は、次の3種類です。

- ① 出入りした社員または協力社員：社員または協力社員を特定するための利用者ID(表1参照)
- ② 出入りした日時：ICカードをかざして出入りした日時、すなわちICカード利用日時(表2参照)

③ 出入口：表2から、各出入口に設置しているICカード読取り装置はICカード読取り装置識別番号で識別されているので、この番号を収集することで社員などが出入りした出入口を特定できる。

以上の三つを含んでいるのはウだけです。よって、ウが正解です。

設問3 ICカードの一時利用停止

空欄a

〔J社の入退室管理システムのセキュリティ要件〕の(7)で「入室時又はパスワードの変更時に、3回連続してパスワードを誤って入力した場合、開発室や執務室への入室はできなくなる」と説明されています。表1から、3回連続してパスワードを誤って入力すると、ICカードの状態が「一時利用停止」になり、その結果、社員などは入室ができなくなります。

ICカードを発給された社員がパスワードを仮パスワードから変更するとき(〔入退室管理システムの運用の説明〕(1)(a))に、パスワードを3回連続して誤った場合、ICカードの状態が「仮パスワード」から「一時利用停止」になります。したがって、空欄aには「3回連続してパスワードを誤入力」(ア)が入ります。

設問4 協力社員のICカード

【入退室管理システムの運用の説明】(1)(社員に対する運用)と、同(2)(協力社員に対する運用)を比較すると、両者はほとんど同じ運用形態になっています。両者の主な相違点は、社員に対する運用では退職時にICカードの返却などを行い、協力社員に対する運用では契約の終了時にICカードの返却などを行うことです。ICカードの返却などを行うタイミングを考慮しなければ、図1の社員を対象とした状態遷移図は、協力社員を対象とした状態遷移図として利用することができます。

【J社の入退室管理システムのセキュリティ要件】の(1)で「社員及び協力社員は、プロジェクトに参画している期間中だけ開発室に入室可能」としているので、プロジェクトに参画している協力社員のICカードの「入室許可の状態」は「開発室許可」になっています。したがって、プロジェクトに参画している協力社員の契約が終了したとき、図1の⑤の状態になっています。この状態から、契約の終了によってICカードの返却が行われ、図1の

③の状態に遷移するので、 δ の矢印が適切です。正解は **エ** です。

設問5 不正な入退室

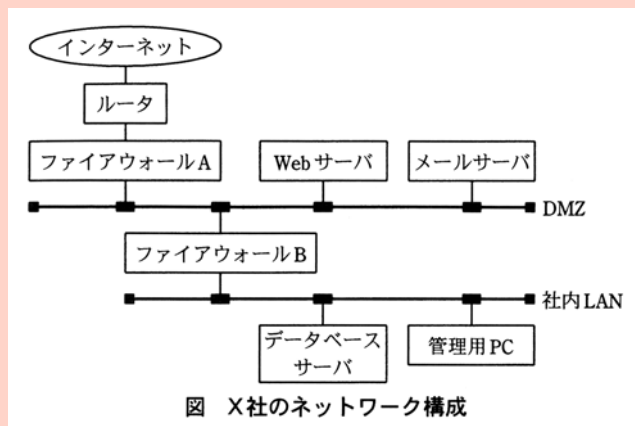
入室履歴または退室履歴のない者がICカードをかざして退室または入室しようとした場合、その者は設問5で説明されている不正な入退室方法を使ったと特定できます。この者がICカードをかざして退室または入室しようとしたとき、ICカードの状態を図1の④(「一時利用停止」)にして、ICカードによる入退室を一時的にできないようにすることで、不正に入退室した者にペナルティを与え、自分のICカードを必ずかざさせるように教育することが適切です。**エ** が正解です。

解答

設問1 **ウ** 設問2 **ウ** 設問3 a: **ア**
設問4 **エ** 設問5 **エ**

問3 パケットフィルタリングに関する次の記述を読んで、設問1, 2に答えよ。

X社では、図に示すネットワークを構築し、インターネットへのWebサイトの公開と電子メール(以下、メールという)の送受信を行っている。



X社のネットワークは二つのファイアウォールによって、DMZ及び社内LANの二つのセグメントに分けられている。Webサーバ、メールサーバ及びデータベースサーバ(以下、DBサーバという)は、それぞれ次の役割を果たしている。

(1) Webサーバ

Webサイトとして、自社の情報をインターネットに公開する。Webサーバ上では、社外との取引情報を処理するプログラムが動作する。このプログラムが利用するデータはDBサーバ上に格納される。

(2) メールサーバ

社外とのメールの送受信を行う。また、取引先に対してメールを自動配信するプログラムが動作する。メール配信のためのデータはDBサーバ上に格納される。

(3) DBサーバ

Webサーバ及びメールサーバで利用するデータを格納する。

社内LANに接続された管理用PCからは、SSHを使った各サーバへのログイン操作と、メールサーバを介した外部とのメール送受信が可能である。管理用PCから自社Webサーバの参照はできるが、社外Webサイトの利用は許可されていない。

ネットワーク上で使われるプロトコルとポート番号を表1に示す。

表1 プロトコルとポート番号

サービス	プロトコル	ポート番号
Web	HTTP	80
メール転送	SMTP	25
セキュアシェル（遠隔ログイン）	SSH	22
メール受信	POP3	110
DBアクセス	DB専用	1999

設問 1

次の記述中の ～ に入れる正しい答えを、解答群の中から選べ。解答は重複して選んでもよい。

インターネットとDMZをつなぐファイアウォールAのパケットフィルタリングの設定を表2に示す。また、DMZと社内LANをつなぐファイアウォールBのパケットフィルタリングの設定を表3に示す。

フィルタリングの設定ルールは、送信元のIPアドレス、あて先のIPアドレス及び接続先ポート番号を指定して通信の許可／拒否を制御する。設定は上の行のルールから調べて、最初に条件が合致した行の動作を実行する。また、応答パケットについては動的フィルタリング機能によって自動的に許可されるので設定は不要なものとする。

表2 ファイアウォールAのフィルタリングの設定

条件			動作
送信元	あて先	ポート番号	
任意	Webサーバ	80	許可
任意	メールサーバ	25	許可
a	任意	b	許可
任意	任意	任意	拒否

表3 ファイアウォールBのフィルタリングの設定

条件			動作
送信元	あて先	ポート番号	
Webサーバ	DBサーバ	1999	許可
メールサーバ	DBサーバ	1999	許可
管理用PC	c	d	許可
管理用PC	メールサーバ	22	許可
管理用PC	メールサーバ	25	許可
管理用PC	Webサーバ	80	許可
管理用PC	Webサーバ	22	許可
任意	任意	任意	拒否

a, cに関する解答群

ア DBサーバ イ Webサーバ ウ 管理用PC エ メールサーバ オ 任意

b, dに関する解答群

ア 22 イ 25 ウ 80 エ 110 オ 1999

設問2 X社のネットワークでは、ファイアウォールによるパケットフィルタリングによって、インターネット接続に伴うセキュリティ上のリスクを低減しているが、パケットフィルタリングは、全ての脅威に対する防御とはならない。パケットフィルタリングによって防ぐことができるセキュリティ上のリスクとして、正しい答えを解答群の中から二つ選べ。

解答群

- ア Webサイトとやり取りされるデータの盗聴や改ざん
- イ WebサイトへのSQLインジェクション攻撃
- ウ インターネットからDMZ内のサーバへの許可されていないポートでの接続
- エ インターネットから社内LANへの不正アクセスによる攻撃
- オ メールによる社内からのファイル流出

解説

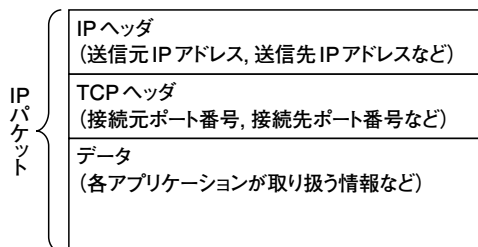
ファイアウォールによるパケットフィルタリング、DMZ、SQLインジェクションなどのインターネットセキュリティに関する知識が必要とされる問題です。

設問の解説に入る前に【IPパケットの構成】【DMZ (DeMilitarized Zone)】【ファイアウォール】【パケットフィルタリング】【動的パケットフィルタリング】【SMTPとPOP3】【SQLインジェクション】【SSH】について解説します。

【IPパケットの構成】

インターネットで使用されている通信プロトコル(規

約)であるTCP/IPでは、データをIPパケットという単位にして送受信を行います。一般的なIPパケットの構成は図Aのようになります。



図A

IPヘッダ部分には、データの送信元・あて先の各コンピュータを特定するために必要な情報が格納されます。送信元IPアドレスにはIPパケットを送信するコンピュータのIPアドレスが、あて先IPアドレスにはIPパケットを受信するコンピュータ(あて先のコンピュータ)のIPアドレスがそれぞれ記録されます。

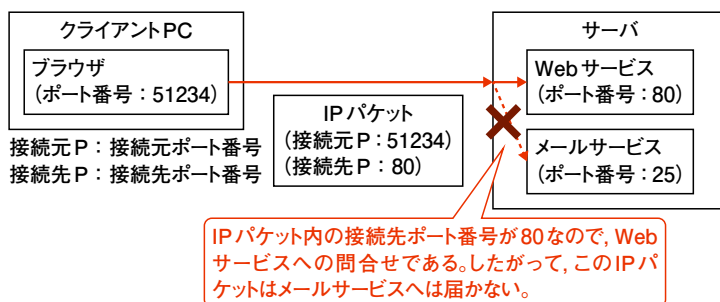
このIPアドレスによって、ネットワーク上の送信元・あて先の各コンピュータ自体は特定可能になります。しかし、コンピュータやサーバ上で動作しているアプリケーションやネットワークサービスが複数存在している場合は、IPアドレスだけではどのサービスにIPパケットが受け渡されるのか特定できないため、IPアドレス以外の情報を用いて、「このIPパケットはこのサービスに対して渡してほしい」との指定を行います。

この情報に相当するのが、TCPヘッダ内のポート番号です。ポート番号とは、コンピュータ上で動作するサービス(プロトコル)を区別するために、各サービスに対して付与される番号です。メールの送受信(SMTP)などの、サーバ上で稼働する主要なサービスについては、ポート番号が固定的に割り振られています。例えば、ブラウザからの要求に対してWebサーバがHTMLのページなどを返却するHTTP(WWW)サービスに対しては80番、メールの送受信に関するSMTPサービスに対しては25番、という値が割り当てられています。

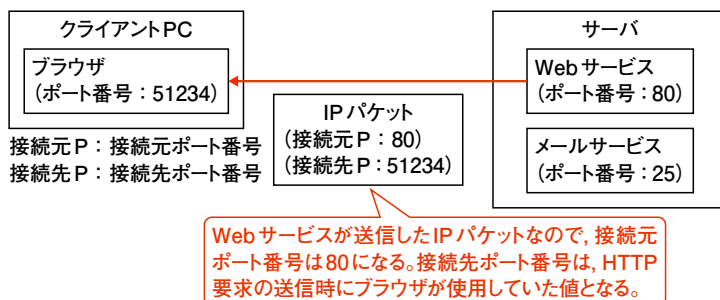
ポート番号は0~65535まで存在しますが、1023以下の各番号は特定のプロトコルに固定的に割り当てられているため、メーカーやユーザ独自の通信プロトコルなどに勝手に割り当ててはできません。この1023までのポート番号を「ウェルノウン(well-known)ポート番号」といいます。

TCPヘッダ部分には、IPパケットのデータを取り扱う各アプリケーションソフトや各サービスを区別するために、接続元及び接続先(あて先)ポート番号が記録されます。接続元ポート番号には、送信元のコンピュータ上でIPパケットを送信したプログラム(サービス)のポート番号が、接続先ポート番号には、あて先のコンピュータ上でIPパケットを受信するプログラム(サービス)のポート番号が、それぞれ記録されます。

図Bは、あるクライアントPC上で起動しているブラウザから、サーバへ向けてHTTP要求のIPパケットを送っている状況を示しています。このサーバ上では、Webサービスとメールサービスが同時に稼働しているものとします。IPパケットの接続先ポート番号が80(HTTP)のため、このHTTP要求のパケットは確実にWebサービスの方に渡され、Webサービスと関係のないメールサービスへ渡されることはありません。なお、ブラウザなどのクライアントPC上で動作するプログラムがWebサーバなどに対してHTTP要求などを送信する際には、



図B



図C

ウェルノウンポート番号以外の接続元ポート番号を、通信の都度任意に選んで使用します。

このWebサービスが、図BのHTTPのアクセス要求に対する応答パケットをブラウザに返却するときは、そのIPパケットの接続元及び接続先ポート番号は、図Cのようになります。

【DMZ (DeMilitarized Zone)】

外部に公開するWebサーバやメールサーバなどを社内(組織内)のLANに配置すると、外部からのIPパケットが社内LANに入り込むことになり、悪意のデータや不正操作などのIPパケットをクライアントPCや非公開のサーバなどに送りつけられるなどの問題が起こります。そこで、外部に公開するサーバは、本問の図に示されているようなファイアウォールに囲まれた領域に配置し、外部(インターネット)から一定の条件でのみアクセス可能とします。このように、公開サーバと非公開サーバ及びクライアント(管理用PCなど)とを分離して配置することによって、公開サーバに対してのみ外部からのアクセスを限定的に許可し、非公開サーバ及びクライアントに対しては外部からのアクセスを許可しないようにすることができると、セキュリティが向上します。この領域を、DMZ (DeMilitarized Zone＝非武装地帯)といいます。

【ファイアウォール】

ファイアウォールとは、インターネットなどの外部ネットワークからの不正アクセスを防ぐために、外部と内部ネットワークとの間に設置される機器、及びその機器によって行われるセキュリティ向上のための仕組みのことです。

インターネットから、悪意のある利用者からの不正なパケットなどが社内の非公開サーバやクライアントPCなどに送りつけられることを防止するために、インターネットから社内に入ってきたIPパケットを検査して通過または遮断(破棄)を選択することが、セキュリティを保つ上で一般的な措置となります。このような、次に説明するパケットフィルタリングや動的パケットフィルタリングといった処理を行うのがファイアウォールの役割です。

【パケットフィルタリング】

ファイアウォールでは、外部からの社内の機器などへの不正アクセスを防止するため、ファイアウォールを通過するIPパケット内の送信元及び宛先IPアドレスや

ポート番号を検査して、IPアドレスなどの値によってIPパケットの通過または遮断(破棄)を選択することができます。このような処理をパケットフィルタリングといいます。

パケットフィルタリングに用いられるのが、本問の表2、表3のようなフィルタリングの設定表です。ファイアウォールはIPパケットを受信すると、フィルタリングの設定表を参照し、IPパケットのIPアドレスやポート番号の値が表の特定の行の条件に一致した場合に、その行で指定されている動作(許可または拒否)を行います。

パケットフィルタリングを行う際に重要なことは、インターネットや公衆通信網などの、外部から社内に送信されてくるIPパケットについて、特に注意しなければならないということです。悪意の第三者は、インターネット上に存在するコンピュータから社内のクライアントPCなどに向けて不正なパケットを送信する攻撃を仕掛けてくることが多いため、社外から社内へのパケットを可能な限り排除するようにフィルタリングの設定を行うのが、セキュリティを保つ上で適切な方法となります。

【動的パケットフィルタリング】

社内LAN上のPCとインターネット上の任意のWebサーバとの間で、HTTPの要求のIPパケット及びその応答のIPパケットの通過を許可し、それ以外のアクセスは全て拒否することを考えます。この場合、ファイアウォールのフィルタリング設定表を表Aのように設定します。

しかし、表Aのようにフィルタリング設定表を設定すると、問題が起こることがあります。インターネット上のWebサーバからPCに返却されるHTTP応答のIPパケットは、接続元ポート番号が80となっています。また接続先ポート番号は、HTTP要求のIPパケットの送信時に、ブラウザによって任意に選ばれた番号になります。2行目の条件は、このようなパケットの通過を許可するために設けられたものです。

しかし、このようなパケットの通過を常に許可するようにしておくと、「接続先ポート番号＝任意、接続元ポート番号＝80で、インターネット上の任意のコンピュータから社内LAN上のPCへ送信されたパケット」として作成した不正なパケットがファイアウォールに送りつけられた場合、それは2行目の条件に合致してしまうため遮断されず、社内LANの内部に侵入してしまいます。動的パケットフィルタリング機能は、このような問題に対処するために利用されています。

表Bは、動的パケットフィルタリング機能を利用する

表A

送信元IPアドレス	あて先IPアドレス	接続元ポート番号	接続先ポート番号	動作
社内LAN上のPC	任意	任意	80	許可
任意	社内LAN上のPC	80	任意	許可
任意	任意	任意	任意	拒否

表B

番号	送信元IPアドレス	あて先IPアドレス	接続元ポート番号	接続先ポート番号	動作
10	社内LAN上のPC	任意	任意	80	許可
20	任意	任意	任意	任意	拒否

表C

番号	送信元IPアドレス	あて先IPアドレス	接続元ポート番号	接続先ポート番号	動作
10	社内LAN上のPC	任意	任意	80	許可
15	y.y.y.y	x.x.x.x	80	1024	許可
20	任意	任意	任意	任意	拒否

際に用いられるフィルタリング設定表の例です。このフィルタリング設定表では、PCからインターネット上の任意のWebサーバに送信されるHTTPの要求パケットのみの通過を許可し、それ以外のパケットは常に全て拒否しています。

ここで、社内LAN上のあるPC (IPアドレス=x.x.x.xとする)から、接続元ポート番号=1024、接続先ポート番号=80としたHTTP要求のIPパケットが、インターネット上のIPアドレスy.y.y.yのWebサーバに向けて送信されると、ファイアウォールは自身のフィルタリング設定表に、一時的に表Cのような行を追加します。

表Cの行番号15の行は、送信されたHTTP要求のIPパケットに対応する応答パケットを、社内LANに取り込むために一時的に設けられた条件です。この条件では、送信元やあて先のIPアドレスが具体的に指定されているため、IPアドレスがy.y.y.yのWebサーバだけが社内LANに応答パケットを送ることが可能になり、それ以外の不審なコンピュータが接続元ポート番号などを偽造したIPパケットを送りつけてきても、行番号15の条件に合致しないため拒否されます。したがって、前述のような問題を防ぐことができます。本問の表2、表3のフィルタリング設定表も、本解説の表Bと同様に動的フィルタリング機能を用いることを前提としているため、応答パケットの設定は不要となります。

なお、PCとWebサーバとのHTTPによるデータのやり取りが終了した後は、両者の間でパケットが送受信されなくなるため、行番号15の行の条件は不要となり

削除されます。

【SMTPとPOP3】

電子メールの送信や受信を行う際には、SMTPやPOP3というプロトコルが利用されます。SMTPとPOP3の特徴を以下に示します。

SMTP: 送信側メールクライアントから受信側メールサーバにメールを送信する際、及び送信側メールサーバから受信側メールサーバにメールを転送する際に用いられる、メール送信用プロトコルである。送信側が使用した送信元メールアドレスが実在しないものであっても、特にチェックせずに送信される。

POP3(POP version 3): 受信側メールサーバのメールボックスに格納されているメールを、そのメールの受信者がメールクライアントを用いて受け取る際に使用される、メール受信用プロトコルである。メールの受信前に、パスワードを用いて受信者の認証を行う。

本問の状況において、社内LANの管理用PCから外部にメールを送信するときと、外部から管理用PCの利用者のメールアドレスあてに送信されたメールを受信するときは、それぞれ以下のようにアクセスが行われることになります。

- 社内LANの管理用PCから外部にメールを送信するとき
 - (a) 管理用PCからDMZ内のメールサーバに対して、メール送信のためのSMTP要求のアクセスが行われ、DMZ内のメールサーバにメールが送信

される。DMZ内のメールサーバは、当該メールをいったん受信する。

(b) DMZ内のメールサーバは、(a)で受信したメールを、そのあて先メールアドレスを参照して適切な外部のメールサーバに送る。その結果、DMZ内のメールサーバから、外部のメールサーバに対してメール送信のためのSMTP要求のアクセスが行われることになる。

- 外部から管理用PCの利用者のメールアドレスあてに送信されたメールを受信するとき

(c) 外部のメールサーバからDMZ内のメールサーバに対して、管理用PCの利用者のメールアドレスあてのメールを送信するためのSMTP要求のアクセスが行われ、DMZ内のメールサーバにメールが送信される。DMZ内のメールサーバは当該メールを受信し、管理用PCの利用者のメールボックスに保管する。

(d) 管理用PCの利用者は、メールクライアントを立ち上げ、(c)でDMZ内のメールサーバが保管した自分あてのメールの受信を行う。このとき、管理用PCからDMZ内のメールサーバに対して、メール受信のためのPOP3要求のアクセスが行われ、管理用PCはDMZ内のメールサーバから利用者あてのメールを受信する。

【SQLインジェクション】

SQLインジェクションとは、Webページ上の入力フォームに不正な文字列を入力し、その文字列から生成されたSQL文を不正なものにして、Webサーバ上で稼働するWebアプリケーションを誤動作させたり、データベースの内容を不正に閲覧または削除したりする攻撃方法のことです。

一般的なDBMSでは、「;」(セミコロン)で区切って複数のSQL文を一括して実行できる仕様になっています。例えば、「SELECT～FROM～…; UPDATE～SET～…」というSQL文を作成すれば、SELECT文の実行後にUPDATE文も実行されます。したがって、SELECT文の後にDELETE文を実行させるようなSQL文を不正に作成してデータベースサーバ上で実行させれば、データベース上の特定のテーブルのレコードが全て削除されてしまうことになります。SQLインジェクションでは、このような不正なSQL文を生成するための文字列を、攻撃者のブラウザからWebページ上の入力フォームに入力し、その内容をIPパケットとしてWebサーバに送

りつけることによって攻撃を行います。

SQLインジェクションによる攻撃が行われたときは、不正なSQL文を作成するためにブラウザから入力された不正な文字列は、IPパケットのデータ部分に格納され、攻撃者のブラウザからWebサーバに送信されます。前述のパケットフィルタリングでは、IPパケットのIPヘッダやTCPヘッダに存在しているIPアドレスやポート番号を確認して、IPパケットの通過の許可や拒否を行うことは可能です。しかし、パケットフィルタリングではIPパケットのデータ部分の内容は参照されないため、SQLインジェクションによって不正な文字列がブラウザから入力されても、そのような入力が行われたIPパケットをパケットフィルタリングによって検知したり、通過を拒否したりすることはできません。

よって、パケットフィルタリングではSQLインジェクションを防止することはできません。これは、設問2の解答を得る上で重要なことです。

【SSH】

SSH(Secure SHell)とは、リモートからの遠隔操作(遠隔地のサーバなどのコンピュータにログインして操作を行うこと)の機能を持ち、かつ暗号化機能や認証機能も備えているプロトコルのことです。このプロトコルにおいては、ログイン時に入力されるIDやパスワードなども含めて通信内容が暗号化されるため、ログイン時に入力するパスワードなどを盗まれる可能性が低くなります。

設問 1 パケットフィルタリングの設定

空欄 a, b

本問の表2のフィルタリングの設定表と同様の表を表Dに示します。なお、本問の表2では省略されている接続元のポート番号を、表Dでは記載しています。

表Dの「条件」の各項目と、本問の表2の「条件」の各項目との対応を示します。

- 送信元IP: 本問の表2の「送信元」に相当
- あて先IP: 本問の表2の「あて先」に相当
- 接続元ポート番号: 新たに追加したもの
- 接続先ポート番号: 本問の表2の「ポート番号」に相当

表Dの各行(A)～(D)について検証します。

- (A)

この行では、送信元IPが任意となっていることから、

表D

	条件				動作
	送信元IP	あて先IP	接続元ポート番号	接続先ポート番号	
(A)	任意	Webサーバ	>1023	80	許可
(B)	任意	メールサーバ	>1023	25	許可
(C)	a	任意	>1023	b	許可
(D)	任意	任意	任意	任意	拒否

(“>1023”は「1023よりも大きい任意のポート番号」を表す。以下同じ)

表E

	条件				動作
	送信元IP	あて先IP	接続元ポート番号	接続先ポート番号	
(A)	任意	Webサーバ	>1023	80	許可
(B)	任意	メールサーバ	>1023	25	許可
(C)	メールサーバ	任意	>1023	25	許可
(D)	任意	任意	任意	任意	拒否

インターネット上の任意のコンピュータを送信元として送られてくるIPパケットを通過させることになります。また、あて先IPがWebサーバ、接続先ポート番号が80(HTTP)となっていることから、インターネット上の任意のコンピュータのブラウザなどからDMZ内のWebサーバに対して送信されるHTTP要求のIPパケットを、この行の条件によって通過させていると推定できます。

【IPパケットの構成】の説明にて示したとおり、ブラウザなどのプログラムがサーバに対してHTTP要求などを送信する際には、接続元ポート番号はウェルノウンポート番号よりも大きい任意のポート番号が選ばれます。よって、(A)の行の接続元ポート番号は“>1023”となります。(B)などの行の接続元ポート番号も同様となります。

● (B)

この行では、送信元IPが任意となっていることから、インターネット上の任意のコンピュータを送信元として送られてくるIPパケットを通過させることになります。また、あて先IPがメールサーバ、接続先ポート番号が25(SMTP)となっていることから、インターネット上の任意のメールサーバなどから、DMZ内のメールサーバに対して送信されるSMTP要求(メール送信)のIPパケットを、この行の条件によって通過させていると推定できます。以上から、この行では【SMTPとPOP3】の(c)で示した、「外部(インターネット)のメールサーバからDMZ内のメールサーバに対して、管理用PCの利用者のメールアドレスあてのメールを送信するためのSMTP要求のアクセスが行われ、DMZ内のメールサー

バにメールが送信される」ときのIPパケットを通過させていると考えられます。

● (C)

(B)の行の条件によって、インターネットからDMZ内のメールサーバに送信されるメールを通過させることは可能となります。しかし、本問では「メールサーバを介した外部とのメール送受信」を可能としているため、外部からDMZ内のメールサーバにメールを送信できるようにするだけでなく、DMZ内のメールサーバから外部にメールを送信できるようにしなければなりません。

そのためには、メールサーバを送信元とし、接続先ポート番号を25(SMTP)とする条件の行が、表Dに必要となります。(C)の行が、そのための役割を担っていると理解できます。この行は、【SMTPとPOP3】の(b)で示した、DMZ内のメールサーバから外部のメールサーバに対して行われる、メール送信のためのSMTP要求のアクセスをファイアウォールAで通過させるために用意されたものです。

なお、外部のメールサーバのIPアドレスを固定的に指定することはできません(どのような値のIPアドレスも、外部のメールサーバのあて先IPアドレスになりうるため)。よって、(C)の行のあて先IPは「任意」となります。

以上から、表Dの空欄aには「メールサーバ」(E)、空欄bには「25」(F)という語句が入ることになります(表E)。

● (D)

この行では、任意の送信元から任意のあて先に対し

表F

	条件				動作
	送信元IP	あて先IP	接続元ポート番号	接続先ポート番号	
(A)	Webサーバ	DBサーバ	>1023	1999	許可
(B)	メールサーバ	DBサーバ	>1023	1999	許可
(C)	管理用PC	c	>1023	d	許可
(D)	管理用PC	メールサーバ	>1023	22	許可
(E)	管理用PC	メールサーバ	>1023	25	許可
(F)	管理用PC	Webサーバ	>1023	80	許可
(G)	管理用PC	Webサーバ	>1023	22	許可
(H)	任意	任意	任意	任意	拒否

て送信されてきた任意のサービス(接続先ポート番号)のIPパケットを拒否しています。(A)～(C)までの条件にあてはまらなかったIPパケットは、この行の条件にあてはまり、拒否されます。よって、例えばDMZ内のメールサーバやWebサーバに対して、外部からSSHを用いて不正にログイン操作しようとするために、接続先ポート番号22(SSH)のIPパケットが送信されてきても、このIPパケットは(D)の条件にあてはまり、ファイアウォールAによって拒否され接続は失敗します。このように、フィルタリング設定表に(D)のような行を設けることで、DMZ内のサーバ上のサービスのうち、外部に公開していないサービスに対して、外部から不正に接続しようとするために送信されてくる不正なパケットなどを拒否できます。

空欄c, d

本問の表3のフィルタリングの設定表と同様の表を表Fに示します。表Fの「条件」の各項目と、本問の表3の「条件」の各項目との対応は、本解説の表Dと同様になります。

表Fの各行(A), (B), 及び(D)～(H)について検証します。

● (A)

この行は、DMZ内のWebサーバの「社外との取引情報を処理するプログラム」が、社内LAN内のDBサーバにアクセスしてデータを入手するために送信するIPパケット(DBアクセスのポート番号=1999のため、接続先ポート番号=1999となる)を、通過させるためのものです。

● (B)

この行は、DMZ内のメールサーバの「取引先に対してメールを自動配信するプログラム」が、社内LAN内のDBサーバにアクセスしてメール配信のためのデータ

を入手する際に送信するIPパケットを、通過させるためのものです。

● (D)

送信元IP=管理用PC、あて先IP=メールサーバ、接続先ポート番号=22のため、SSH(ポート番号=22)によって、社内LAN内の管理用PCからDMZ内のメールサーバにログイン操作するために送信されてくるIPパケットを通過させるためのものです。

● (E)

送信元IP=管理用PC、あて先IP=メールサーバ、接続先ポート番号=25のため、SMTP(ポート番号=25)によって、社内LAN内の管理用PCからDMZ内のメールサーバにメールを送信するために送られてくるIPパケットを通過させるためのものです。すなわち、【SMTPとPOP3】の(a)に示した処理を行うためのものです。

● (F)

送信元IP=管理用PC、あて先IP=Webサーバ、接続先ポート番号=80のため、HTTP(ポート番号=80)によって、社内LAN内の管理用PCからDMZ内のWebサーバの参照を行うために送られてくるIPパケットを通過させるためのものです。

● (G)

送信元IP=管理用PC、あて先IP=Webサーバ、接続先ポート番号=22のため、SSH(ポート番号=22)によって、社内LAN内の管理用PCからDMZ内のWebサーバにログイン操作するために送信されてくるIPパケットを通過させるためのものです。

● (H)

表Dの(D)と同様に、この行では、任意の送信元から任意のあて先に対して送信されてきた任意のサービスのIPパケットを拒否しています。(A)～(G)までの条件にあてはまらなかったIPパケットは、この行の条件にあ

てはまり、拒否されます。よって、例えば社内LAN内の管理用PCに対して、外部からSSHで不正にログイン操作しようとするために、接続先ポート番号22 (SSH)のIPパケットが送信されてきても、このIPパケットは(H)の条件にあてはまり、ファイアウォールBによって拒否され接続は失敗します。また、SSH以外の任意の接続先ポート番号によるアクセスや、管理用PC以外の社内LAN内の任意の機器へ外部から送信されたIPパケットも同様に拒否されます。

このように、フィルタリング設定表に(H)のような行を設けることで、社内LAN内のコンピュータに対して、外部から不正にアクセスするために送信されてくる不正なパケットなどを拒否できます。

以上から、本問で説明されている通信のうち、

- WebサーバからDBサーバのデータを利用するための通信
- メールサーバからDBサーバのデータを利用するための通信
- 管理用PCからSSHを使ってメールサーバにログイン操作するための通信
- 管理用PCからメールサーバにメールを送信するための通信
- 管理用PCからSSHを使ってWebサーバにログイン操作するための通信
- 管理用PCからWebサーバを参照するための通信

については、表Fの(A)、(B)及び(D)～(H)によって許可できることが分かります。しかし、【SMTPとPOP3】の(d)に示された、管理用PCの利用者が自分あてのメールを受信するための「管理用PCからDMZ内のメールサーバに対して行われる、メール受信のためのPOP3要求のアクセス」については、表Fの(A)、(B)及び(D)～(H)によっては許可できていません。よって、空欄c、dが含まれる(C)の条件によって、当該アクセスの通過が許可されることになります。

以上から、管理用PCを送信元とし、DMZ内のメールサーバをあて先とするアクセスを許可するため、空欄c(あて先)＝「メールサーバ」(イ)となります。また、POP3(ポート番号＝110)要求のアクセスを許可するため、空欄d(接続先ポート番号)＝「110」(イ)となります。

設問2 パケットフィルタリングで防げるリスク

解答群ア～オについて、順に検証します。

● ア

X社では、DMZ内のWebサーバを用いてWebサイトを構築しています。よって、「Webサイトとやり取りされるデータ」とは、外部(インターネット)上のコンピュータなどとX社のWebサーバとの間のデータのやり取りを指します。これらの情報を暗号化したり、デジタル署名などの技術によって改ざん検知の措置をとったりしているとの記述は存在しないため、外部とWebサーバ間のデータは平文のまま送受信されていると考えられます。

このような場合、X社内のファイアウォールにおいて、パケットフィルタリングによってX社のDMZや社内LANにおいてIPパケットを検査していても、IPパケット中の情報の盗聴や改ざんがX社の管轄外のインターネット上で行われた場合は、それを防ぐことはできません。

よって、このリスクはパケットフィルタリングによって防ぐことはできません。

● イ

【SQLインジェクション】の説明に示したとおり、SQLインジェクション攻撃において不正なSQL文を作成するために入力された不正な文字列は、IPパケットのデータ部分に格納され、攻撃者のブラウザからWebサーバに送信されます。パケットフィルタリングでは、IPパケットのデータ部分の内容は参照されないため、SQLインジェクションによって不正な文字列がブラウザから入力されても、そのような入力が行われたIPパケットをパケットフィルタリングによって検知したり、通過を拒否したりすることはできません。よって、パケットフィルタリングではSQLインジェクションを防止することはできません。

● ウ

設問1の空欄a、bの解説において、「DMZ内のサーバ上のサービスのうち、外部に公開していないサービスに対して、外部から不正に接続しようとするために送信されてくる不正なパケットなどを拒否」できると判明しています。よって、本問の表2のフィルタリングの設定によって、DMZ内のメールサーバなどへの、外部に公開していない(接続を許可していない)サービス、すなわち接続を許可していない接続先ポート番号のIPパケットを拒否することができます。したがって、「インターネットからDMZ内のサーバへの許可されていないポートでの接続」を防ぐことができます。

● エ

設問1の空欄c、dの解説において、「社内LAN内のコンピュータに対して、外部から不正にアクセスするた

めに送信されてくる不正なパケットなどを拒否」できると判明しています。よって、本問の表3のフィルタリングの設定によって、社内LAN内の管理用PCなどへの、外部からの不正アクセスのIPパケットを拒否することができます。したがって、「インターネットから社内LANへの不正アクセスによる攻撃」を防ぐことができます。

● オ

本問の表2及び表3の設定から、社内LANの管理用PCからインターネットにメールを送信することは可能であると理解できます。よって、例えば管理用PCの利用者が、個人情報などの重要な情報が記載されたファイルなどを、メールの添付ファイルとしてインターネット上の取引先などに誤って送信してしまうと、そのメールはフィルタリングによっては遮断されず、そのまま社

外に送出され、情報が漏えいしてしまうことになります。

イの解説と同様に、パケットフィルタリングではIPアドレスやポート番号のみがチェック対象となり、IPパケットのデータ部分の内容は検査されないため、メール本文や添付ファイルなどの内容がチェックされることはありません。

よって、このリスクはパケットフィルタリングによって防ぐことはできません。

以上から、ウ、エの二つが解答となります。

○ 解答 ○

設問 1 a: エ b: イ c: エ d: エ

設問 2 ウ, エ

第③回 模擬試験

情報セキュリティ マネジメント

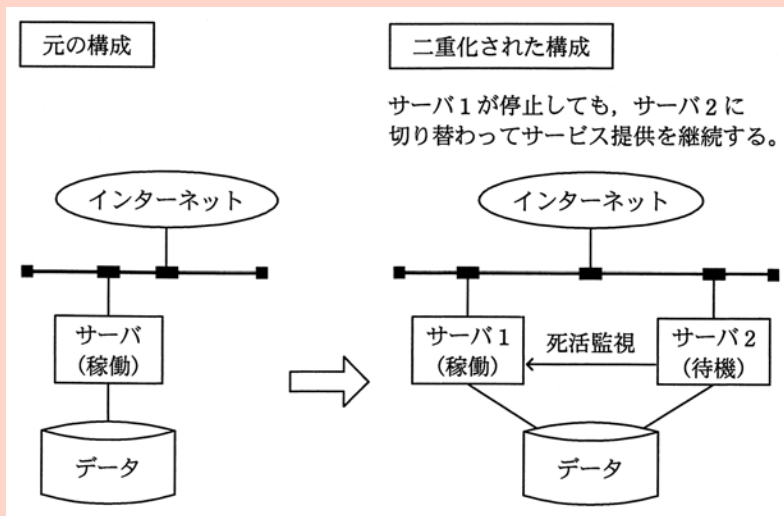
- 午前 問題 274
(全 50 問 試験時間：1 時間 30 分)
- 午後 問題 308
(全 3 問 試験時間：1 時間 30 分)

本章で取り上げる問題文は、情報処理技術者の試験で過去に出題された問題の中から著者が精選して構成したものです。

第③回 模擬試験 午前 問題

問 1

図のようなサーバ構成の二重化によって期待する効果はどれか。



- ☐ ア 可用性の向上 ☐ イ 完全性の向上 ☐ ウ 機密性の向上 ☐ エ 責任追跡性の向上

問 2

ポリモーフィック型ウイルスの説明として、適切なものはどれか。

- ☐ ア インターネットを介して、攻撃者がPCを遠隔操作する。
☐ イ 感染するごとにウイルスのコードを異なる鍵で暗号化し、ウイルス自身を変化させて同一のパターンで検知されないようにする。
☐ ウ 複数のOSで利用できるプログラム言語でウイルスを作成することによって、複数のOS上でウイルスが動作する。
☐ エ ルートキットを利用してウイルスに感染していないように見せかけることによって、ウイルスを隠蔽する。

問 3

フィールド 1 に入力された値が変数 \$jouken1 に、フィールド 2 に入力された値が変数 \$jouken2 に代入され、次の SQL 文によって表 TABLE_A を検索して結果を表示する Web アプリケーションがある。

```
SELECT * FROM TABLE_A
WHERE jouken1='$jouken1' AND jouken2='$jouken2'
```

悪意のある利用者が、SQL インジェクションによって TABLE_A の全レコードの削除を試みるとき、それぞれのフィールドに入力する文字列はどれか。

	フィールド1	フィールド2
ア	*	'DELETE FROM TABLE_A WHERE 'A'='A'
イ	*	DELETE FROM TABLE_A WHERE 'A'='A'
ウ	(何も入力しない)	' ;DELETE FROM TABLE_A WHERE 'A'='A'
エ	(何も入力しない)	DELETE FROM TABLE_A WHERE 'A'='A'

解説

問 1 二重化された構成

図のようにしてサーバ構成を二重化することで、サーバ1が故障などの原因で停止しても、サーバ2を稼働させてサービス提供を継続できます。その結果、**可用性**が向上します。

- **ア** 正解です。
- × **イ** **完全性**は、データの内容が正確であり、改ざんなどが行われていないという性質です。図では、デジタル署名による改ざんの検知などの対策は採っていないため、完全性の向上は期待できません。
- × **ウ** **機密性**は、アクセス権限のない者にはデータを開示しないという性質です。図では、データの暗号化などの機密性を向上させるための対策は採っていないため、機密性の向上は期待できません。
- × **エ** **責任追跡性**は、ある操作を行った主体を特定できるという性質です。図では、システムを操作した人のIDを記録するなどの責任追跡性を向上させるための対策は採っていないため、責任追跡性の向上は期待できません。

問 2 ポリモーフィック型ウイルス

ポリモーフィック型ウイルスとは、感染するごとにランダムに変化させた暗号化鍵を用いて、ウイルスのコードを暗号化することで自身の内容を常に変化させて、同一のパターンで検知されないようにするウイルスのことです。

- × **ア** 遠隔操作型ウイルスの説明です。
- **イ** 正解です。
- × **ウ** Javaなどの複数のOSで利用できるプログラム言語で作成したウイルスの説明です。
- × **エ** ルートキットによってウイルスを隠蔽する方法の説明です。

問 3 SQLインジェクション

SQLインジェクションは、Webページ上の入力フォームに不正な文字列を入力し、入力フォームから受け取った値をもとにして生成されたSQL文を不正なものにして、Webアプリケーションを誤動作させたり、データベースの内容を削除したりする攻撃方法です。

一般的なDBMSでは、「;」(セミコロン)で区切って複数のSQL文を一括して実行できる仕様になっています。本問では、SELECT文の後にDELETE文を実行させ、TABLE_Aのレコードを全て削除させようとしています。

フィールド2のセミコロンが含まれているのは**ウ**のみです。以下のようなSQL文が作成されます。

```
SELECT * FROM TABLE_A WHERE jouken1=' '
AND jouken2='';DELETE FROM TABLE_A WHERE 'A'='A'
```

○ 解答 ○

問 1 **ア**問 2 **イ**問 3 **ウ**



問 4 Webアプリケーションの脆弱性を悪用する攻撃手法のうち、Perlのsystem関数やPHPのexec関数など外部プログラムの呼出しを可能にするための関数を利用し、不正にシェルスクリプトや実行形式のファイルを実行させるものは、どれに分類されるか。

- | | |
|----------------------------|-------------------------|
| ア HTTPヘッダインジェクション | イ OSコマンドインジェクション |
| ウ クロスサイトリクエストフォージェリ | エ セッションハイジャック |



問 5 企業のDMZ上で1台のDNSサーバをインターネット公開用と社内用で共用している。このDNSサーバが、DNSキャッシュポイズニングの被害を受けた結果、引き起こされ得る現象はどれか。

- ア** DNSサーバで設定された自社の公開WebサーバのFQDN情報が書き換えられ、外部からの参照者が、本来とは異なるWebサーバに誘導される。
- イ** DNSサーバのメモリ上にワームが常駐し、DNS参照元に対して不正プログラムを送り込む。
- ウ** 社内の利用者が、インターネット上の特定のWebサーバを参照する場合に、本来とは異なるWebサーバに誘導される。
- エ** 電子メールの不正中継対策をした自社のメールサーバが、不正中継の踏み台にされる。



問 6 暗号方式に関する説明のうち、適切なものはどれか。

- ア** 共通鍵暗号方式で相手ごとに秘密の通信をする場合、通信相手が多くなるに従って、鍵管理の手間が増える。
- イ** 共通鍵暗号方式を用いて通信を暗号化するときには、送信者と受信者で異なる鍵を用いるが、通信相手にその鍵を知らせる必要はない。
- ウ** 公開鍵暗号方式で通信文を暗号化して内容を秘密にした通信をするときには、復号鍵を公開することによって、鍵管理の手間を減らす。
- エ** 公開鍵方式では、署名に用いる鍵を公開しておく必要がある。

解説

問 4 外部プログラム呼び出しの脆弱性

Perlのsystem関数などを用いて、「不正にシェルスクリプトや実行形式のファイル」を実行させるとの説明から、この攻撃は**OSコマンドインジェクション**です。**イ**が正解です。

OSコマンドインジェクションとは、Webページ上の入力欄にOSのコマンドライン(コマンドプロンプト)上で有効なコマンドを入力させ、Webサーバ上で不正な命令を実行させる攻撃方法です。例えば、UNIXやLinuxをOSとしているWebサーバで公開しているWebページの入力欄に、“……(正当なデータ); rm …”のような文字列を入力すると、正当なデータの処理の後に、“rm …”という、Webサーバ上のファイルを削除する命令が実行されてしまいます。

Perlのsystem関数やPHPのexec関数は、OSのコマンドなどの外部プログラムを呼び出す関数です。OSコマンドインジェクションでは、これらを利用して不正にシェルスクリプトなどを実行させようとする場合があります。

× **ア** **HTTPヘッダインジェクション**とは、HTTPヘッダの部分に不正な改行文字を含めることで、不正なHTTPヘッダを作成してWebサーバプログラムを誤動作させようとする攻撃手法のことです。

- × **ウ** クロスサイトリクエストフォージェリ(Cross Site Request Forgeries)とは、悪意のあるスクリプトを埋め込んだWebページのリンクを訪問者にクリックさせるなどの方法で、別のWebサイト上で訪問者が意図しない操作を行わせる攻撃のことです。
- × **エ** Webサーバとブラウザの間で行われる継続的なやり取りをセッションと呼びます。セッションを維持するために、WebサーバはセッションIDという値をブラウザと交換し合い、その値が適切である限り、正当な利用者(ブラウザ)と適切にやり取りを行っているかと判断します。このセッションIDが固定値である場合など、その値が容易に推測できるような状況では、悪意のあるユーザがセッションIDの値を推測した上で、推測したセッションIDを正当なブラウザになりすましてWebサーバに送り込み、ブラウザとWebサーバ間のセッションを乗っ取ってしまうことが可能です。この攻撃方法を、**セッションハイジャック**と呼びます。

問 5 DNS キャッシュポイズニング

DNS キャッシュポイズニングとは、DNSサーバに誤ったFQDN情報を送り込み、そのDNSサーバを参照してきたPCの利用者を、本来のWebサーバとは異なるWebサーバに誘導する攻撃手法のことです。FQDN情報とは、Webサーバなどのインターネット上の正式名称であるFQDN(Fully Qualified Domain Name、完全修飾ドメイン名)とIPアドレスの対応を示している情報のことです。

DNSキャッシュポイズニングによって、企業の社内の利用者(以下、利用者という)が、以下のような被害に遭う危険性があります。なお、以下の記述のFQDNやIPアドレスは全て架空のもです。

- ① 利用者が使用しているブラウザが、自社のDNSサーバに、“www.x-sya.co.jp”というFQDNをもつインターネット上のWebサーバのIPアドレスを問い合わせる。
 - ② 自社のDNSサーバは、当該WebサーバのFQDNやIPアドレスを管理する外部のDNSサーバに、当該WebサーバのIPアドレスを問い合わせる。
 - ③ 外部のDNSサーバは、②の問合せに対して応答を返す。しかし、このときにインターネット上の攻撃者が、この応答に見せかけた偽の情報を、先に自社のDNSサーバに返してきた場合、自社のDNSサーバは偽の情報を正当な応答として受信してしまう。その結果、自社のDNSサーバに偽の情報がキャッシュされてしまう。
 - ④ 自社のDNSサーバは、利用者が使用しているブラウザに偽の情報を答えてしまう。その結果、利用者は本来と異なるWebサーバに誘導されてしまう。
- × **ア** 自社が管理しているサーバのFQDN情報については、社外のDNSサーバに問合せが行われることはないため、DNSキャッシュポイズニングによって差し替えられることはありません。
 - × **イ** DNSキャッシュポイズニングでは、ワームなどの不正なプログラムが用いられることはありません。
 - **ウ** 正解です。
 - × **エ** DNSキャッシュポイズニングでは、電子メールの不正中継などが行われることはありません。

問 6 共通鍵暗号方式と公開鍵暗号方式

共通鍵暗号方式は、暗号化と復号に同一の鍵を使用します(**イ**は誤り)。この暗号方式で通信の秘匿性を守るためには、通信相手ごとに異なった鍵を用意しなければならないため、通信相手が多くなるに従って鍵管理の手間が増え、管理が困難になります(**ア**が正解)。

公開鍵暗号方式は、データの暗号化に必要な鍵と復号に必要な鍵を共通にするのではなく、異なる2つの鍵(公開鍵と秘密鍵)を用いるのが特徴です。公開鍵暗号方式では暗号化鍵を公開し復号鍵を秘密にします。**ウ**は誤りです。署名に用いる鍵は復号鍵であり、公開しないため、**エ**は誤りです。

○ 解 答 ○

問 4 **イ**

問 5 **ウ**

問 6 **ア**

**問 7**

公開鍵暗号を使って n 人が相互に通信する場合、全体で何個の異なる鍵が必要になるか。ここで、一組の公開鍵と秘密鍵は2個と数える。

- ア** $n+1$ **イ** $2n$ **ウ** $n(n-1)/2$ **エ** $\log_2 n$

**問 8**

暗号アルゴリズムの危^{たい}殆化を説明したものはどれか。

- ア** 外国の輸出規制によって、十分な強度をもつ暗号アルゴリズムを実践した製品が利用できなくなること
イ 鍵の不適切な管理によって、鍵が漏えいする危険性が増すこと
ウ 計算能力の向上などによって、鍵の推定が可能になり、暗号の安全性が低下すること
エ 最高性能のコンピュータを用い、膨大な時間とコストを掛けて暗号強度をより確実なものにすること

**問 9**

暗号解読のための攻撃法のうち、ブルートフォース攻撃はどれか。

- ア** 与えられた一組の平文と暗号文に対し、総当たりで鍵を割り出す。
イ 暗号化関数の統計的な偏りを線形関数によって近似して解読する。
ウ 暗号化装置の動作を電磁波から解析することによって解読する。
エ 異なる二つの平文とそれぞれの暗号文の差分を観測して鍵を割り出す。

**問 10**

公開鍵暗号方式によるデジタル署名の手続とハッシュ値の使用法のうち、適切なものはどれか。

- ア** 受信者は、送信者の公開鍵で署名を復号してハッシュ値を取り出し、元のメッセージを変換して求めたハッシュ値と比較する。
イ 送信者はハッシュ値を自分の公開鍵で暗号化して、元のメッセージとともに受信者に送る。
ウ デジタル署名を付ける元となったメッセージをハッシュ値から復元する。
エ 元のメッセージ全体に対して公開鍵で暗号化を行い、ハッシュ値を用いて復号する。

解説**問 7 公開鍵暗号方式の鍵数**

公開鍵暗号方式では、対になって生成される「公開鍵」と「秘密鍵」の2つの鍵を用います。「公開鍵」はネットワーク上に公開して誰でも利用可能とし、「秘密鍵」は鍵の所有者のみが使用します。ネットワーク上のユーザは、自分の「公開鍵」と「秘密鍵」さえあれば、他のユーザからそれぞれ暗号化されたデータを送信してもらうことが可能です。また、自分から相手にデータを暗号化して送付したい場合、その相手が公開している公開鍵さえ存在すればよいことになります。共通鍵暗号方式のように、他のユーザー一人一人に対して異なる鍵を用意しなくてよいことが、公開鍵暗号方式の利点の一つです。

よって、ユーザ数= n とすると、ユーザー一人が「公開鍵」と「秘密鍵」の2つをもつため、全体では $2n$ 個(**イ**)の鍵が必要になります。

問 8 暗号アルゴリズムの危殆化

危殆化とは、安全でない状態になること、または安全が脅かされる状態になることです。暗号アルゴリズムの危殆化とは、パソコンなどの計算能力や処理速度の向上によって暗号鍵の推定が容易にできるようになり、暗号の安全性が低下することを指します。例えば、DES方式の鍵長は56ビットのため、 $2^{56}=72,057,594,037,927,936$ とおりの鍵を全て試せば鍵を推定できます。以前はこれだけの鍵を試すのに多大な時間がかかっていましたが、現在はパソコンなどの性能が飛躍的に向上しており、短い時間で鍵の推定ができてしまいます。正解は **ウ** です。暗号アルゴリズムの危殆化によって、DES方式は使用を推奨されなくなっています。

問 9 ブルートフォース攻撃

ブルートフォース攻撃(総当たり攻撃)は、考えられる全ての種類のパスワード(または暗号化鍵など)を総当たりで作成して、それをもって不正なログインや暗号解読を試みる方式のことです。例えば、0～9までの数字とA～Zの英大文字のみが使用でき、長さが3文字以内に限られる形式では、36種類の文字を最大でも3つしか使用できないので $36^3=46,656$ となり、最大で46,656種類のパスワードしか存在しないことになります。よって、手作業またはツールなどで約46,000強の種類のパスワードを全て入力していけば、正当なユーザでなくともいずれ不正にログインが可能になります。

ブルートフォース攻撃を防ぐには、パスワードの長さ(文字数)をできるだけ長くしたり、暗号化・復号に使用する鍵のビット長を可能な限り長くしたりすることが有効です。また、何回かパスワードを入力ミスした場合、一定時間そのアカウントからのログインを禁止したり、アカウントを停止したりする対策も有効です。

- **ア** 正解です。
- × **イ** 線形解読法の説明です。
- × **ウ** サイドチャネル攻撃の説明です。
- × **エ** 差分解読法の説明です。

問10 デジタル署名

通信相手に送付するデータの正当性の証明と送信者の本人確認(なりすましの防止)のために、**メッセージ認証(デジタル署名)**が用いられます。

データの送信者は、送付データ全体に対して**ハッシュ関数**を用いて**ハッシュ値**を求めます。さらにそのハッシュ値を「送信者の秘密鍵」で暗号化し、これを「送信者の署名」としてデータと一緒に添付し、受信者に送付します。

受信者は、送信者と同じハッシュ関数を用いてデータ本体からハッシュ値を生成します。さらに、「送信者の署名」を「送信者の公開鍵」で復号して、元のハッシュ値を入手します。二つのハッシュ値が一致すれば、そのデータは送信者からのものであると確認できます。送信者以外は使用できない「送信者の秘密鍵」で「送信者の署名」の暗号化が行われているということは、そのデータが確かに送信者の管理下にあったと証明できるためです。

なお、ハッシュ関数の性質より、ハッシュ値から元のデータを復元することはできないようになっています。

- **ア** 正解です。
- × **イ** デジタル署名の手続きでは、送信者はハッシュ値を自分の秘密鍵で暗号化するため、誤りです。
- × **ウ** デジタル署名を付ける元となったメッセージを、ハッシュ値から復元することはできません。
- × **エ** 元のメッセージを公開鍵で暗号化した場合は、公開鍵に対応する秘密鍵で復号することになります。ハッシュ値は、データの復号には利用できません。

○ 解答 ○

問 7 **イ**

問 8 **ウ**

問 9 **ア**

問 10 **ア**

☐ **問 11** パスワードに使用できる文字の種類を M 、パスワードの文字数を n とするとき、設定できるパスワードの理論的な総数を求める数式はどれか。

- ☐ **ア** M^n ☐ **イ** $\frac{M!}{(M-n)!}$ ☐ **ウ** $\frac{M!}{n!(M-n)!}$ ☐ **エ** $\frac{(M+n-1)!}{n!(M-1)!}$

☐ **問 12** 人間には読み取ることが可能でも、プログラムでは読み取ることが難しいという差異を利用して、ゆがめたり一部を隠したり画像から文字を判断させ入力させることで、人間以外による自動入力を排除する技術はどれか。

- ☐ **ア** CAPTCHA ☐ **イ** QRコード ☐ **ウ** 短縮 URL ☐ **エ** トラックバック ping

☐ **問 13** 所有者と公開鍵の対応付けをするのに必要な方式、システム、プロトコル及びポリシーの集合によって実現されるものはどれか。

- ☐ **ア** IPsec ☐ **イ** PKI ☐ **ウ** ゼロ知識証明 ☐ **エ** ハイブリッド暗号

☐ **問 14** 特定の認証局が発行した CRL (Certificate Revocation List) に関する記述のうち、適切なものはどれか。

- ☐ **ア** CRL には、失効したデジタル証明書に対応する秘密鍵が登録されている。
☐ **イ** CRL には、有効期限内のデジタル証明書のうち破棄されているデジタル証明書と破棄された日時の対応が提示される。
☐ **ウ** CRL は、鍵の漏えい、破棄申請の状況をリアルタイムに反映するプロトコルである。
☐ **エ** 有効期限切れで失効したデジタル証明書は、所有者が新たなデジタル証明書を取得するまでの間、CRL に登録される。

解説

問11 パスワードの総数

けた数=1 のとき：パスワードとして設定できる文字列=M 個

けた数=2 のとき：パスワードとして設定できる文字列=M×M 個=M² 個

けた数=3 のとき：パスワードとして設定できる文字列=M×M×M 個=M³ 個

⋮

けた数=X のとき：パスワードとして設定できる文字列=M^X 個

よって、文字の種類=M 個、けた数=n とすると、Mⁿ 個(**ア**)のパスワードが設定できます。

問12 CAPTCHA

インターネット上の掲示板やブログにコメントなどを投稿するとき、ゆがめられた文字が画像化されて表示され、それを読み取って正しい文字を入力するよう求められることがあります。このようなシステムや、ゆがめられた文字の

画像のことを**CAPTCHA**(キャプチャ)といいます。CAPTCHAは、コメントなどを投稿しようとした者が人間であり、プログラムによる不正な自動入力でないことを確認するためのシステムです。人間はゆがんだ文字を読み取ることが可能ですが、プログラムでは読み取ることが困難なことを利用しています。

- **ア** 正解です。
- × **イ** **QRコード**は、日本企業が開発した2次元式のバーコードです。
- × **ウ** **短縮URL**は、Twitterなどの投稿可能文字数が限られたWebサービスにおいて、文字数が長いURLの代替として、文字数を短くしたURLを投稿するサービス、及びそのサービスで作成された短いURLです。
- × **エ** **トラッキングping**とは、ほかのブログの記事に関連する記事を新しく作成したときに、元となった記事を管理するサーバに宛てて送信するデータです。トラッキングpingを受信したサーバは、元となった記事のトラッキング欄に新しい記事のURLやその概要などを表示します。

問13 公開鍵と所有者の対応付け

公開鍵暗号方式では、送信者はネットワーク上に受信者が公開している公開鍵を用いて暗号化を行い、暗号化したデータを受信者に送信します。受信者は、自分の秘密鍵(公開鍵と対になっている)を用いて、データを復号します。

この方式では、誰でも公開鍵をネットワーク上に公開できるため、あるユーザAになりすました悪意のユーザが、ユーザAの公開鍵と偽って「偽の公開鍵」を公開することを防ぐことはできません。よって、なりすましによって公開された偽の公開鍵を知らずに用いてしまい、悪意のユーザが作った偽のWebサイトに誘導されて、情報を不正に窃取されるという被害が起こりうるため、公開鍵を公開しているユーザの身元証明と、ユーザ(公開鍵の所有者)と公開鍵との対応付けをするためのプロトコルなどが必要となってきています。

これらのプロトコルやシステムなどを用いて実現されるユーザの身元証明及び公開鍵の対応付けを行うシステムを、**PKI**(Public Key Infrastructure, 公開鍵基盤, **イ**)と呼びます。PKIは、広義では“公開鍵暗号を用いた技術・製品全般”を示し、以下に示すプロトコルなどから構築されます。

- RSAなどの公開鍵暗号方式そのもの
- 公開鍵所有者の身元証明のためのデジタル署名、デジタル証明書、及びデジタル証明書を発行する認証局(CA)
- クライアント・サーバ間の相互認証技術のプロトコル(SSL)、及びSSLに対応するWebサーバ/ブラウザ

問14 CRL

CRL(Certificate Revocation List)とは、有効期限内に無効となった(破棄された)公開鍵証明書のシリアル番号と、破棄された日時との対応をリスト化したものです。公開鍵証明書とCRLとを付き合わせることで、有効かどうかを判断するために使用されます。

- × **ア** CRLに秘密鍵が登録されることはありません。
- **イ** 正解です。
- × **ウ** CRLはプロトコルではありません。
- × **エ** 有効期限切れで無効になった公開鍵証明書は今後永久に使用できなくなるので、所有者が新しい公開鍵証明書を取得しても、CRLに残り続けます。

○ 解答 ○

問11 **ア**

問12 **ア**

問13 **イ**

問14 **イ**



問 15 TR X 0036-1 : 2001 (ITセキュリティマネジメントのガイドライン—第1部：ITセキュリティの概念及びモデル)では、情報資産に対する脅威の例を表のように分類している。表のbに入るものはどれか。

脅威の分類		脅威の例
a	b	盗聴，情報の改ざん
	c	誤り及び手落ち，物理的な事故
d		地震，落雷

- ア** 意図的 **イ** 環境 **ウ** 偶発的 **エ** 人間



問 16 リスク対策の一つであるリスクファイナンスに該当するものはどれか。

- ア** システムが被害を受けた場合を想定して保険をかけておく。
イ システム被害につながるリスクの発生を抑える対策に資金を投入する。
ウ システムを復旧するのに掛かった費用を金融機関から借り入れる。
エ リスクが顕在化した場合のシステム被害を小さくする対策に資金を投入する。



問 17 CRYPTRECの活動内容はどれか。

- ア** 客観的な評価によって安全性及び実装性に優れると判断された暗号技術のリストを決定する。
イ 情報セキュリティ政策に係る基本戦略の立案，官民における統一的，横断的な情報セキュリティ対策の推進に係る企画などを行う。
ウ 組織の情報セキュリティマネジメントシステムについて評価し認証する制度を運用する。
エ 認証機関から貸与された暗号モジュール試験報告書作成支援ツールを用いて暗号モジュールの安全性についての評価試験を行う。



問 18 システム運用管理者による機密ファイルの不正な持出しを制するための対策はどれか。

- ア** 運用管理者のPCの定期的なウイルス検査
イ 運用管理者のPCへのクライアントファイアウォールの導入
ウ 監視者の配置
エ 機密ファイルのバックアップ

解説

問15 脅威

ISO/IEC TR 13335 (GMITS, The Guidelines for the management of IT Security, ITセキュリティマネジメントのガイドライン)は、情報セキュリティマネジメントに関する概要や手法などを列挙している規格です。JIS

TR X 0036 は、この規格の日本語訳となります。

JIS TR X 0036 では、情報資産に対する**脅威**の例を、**意図的脅威**、**偶発的脅威**及び**環境的(環境)脅威**として分類しています。意図的脅威は、悪意のある人間が意図的に行う、盗聴や改ざんなどの脅威となります。偶発的脅威は、悪意のない人間が不注意や勘違いなどの原因によって引き起こしてしまう、誤りや手落ちなどを指します。環境的脅威は、人間の意志によらない自然災害(地震、落雷など)による脅威を指します。

よって、本問の図のbには「意図的」(**ア**)という語句が入ります。なお、cには「偶発的」、dには「環境的(環境)」, aには「人為的」または「人間」という語句が入ります。

問16 リスクファイナンス

リスクファイナンスとは、リスクが発生することは不可避であると仮定し、リスクによる損失に備えてリスク対策の費用を事前に計上したり、積立金などを設けて損失を補填したり、保険に加入したりすることを指します。すなわち、リスクに対処して被害を少なくするのではなく、リスクからの被害を保険などで補填する考えのことです。

この説明に合致するのは解答群の**ア**のみです。他の解答群はリスクの発生確率の軽減・回避や、システムの被害額の低減などを行っているので、リスクファイナンスではありません。

問17 CRYPTREC

CRYPTREC (Cryptography Research and Evaluation Committees)は、「電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト」のことです。CRYPTRECは、**電子政府推奨暗号リスト**というリストを公開しています。このリストには、公的な機関によって客観的に評価され、安全性や実装性に優れると判断された暗号方式(DSA, AESなど)やハッシュ関数(SHA-1 など)が掲載されています。

- **ア** 正解です。
- × **イ** 情報セキュリティ政策会議の説明です。
- × **ウ** ISMS適合性評価制度の説明です。
- × **エ** CMVP (Cryptographic Module Validation Program, 暗号モジュール評価プログラム)の説明です。

問18 システム運用管理者による不正な持出し

管理者以外の一般の従業員は機密ファイルなどにアクセスする権限はないので、不正な持出しをすることは困難です。それに対してシステム運用管理者は、運用業務を円滑に実行するために、機密ファイルなどにアクセスできる権限をもっています。したがって、システム運用管理者による機密ファイル不正持出しが発生する可能性があります。ただし、システム運用管理者から機密ファイルなどにアクセスできる権限を奪うと、システム運用管理者が業務を遂行できなくなり、問題があります。

上のような不正行為を牽制するには、監視者を置いてシステム運用管理者の作業内容を定期的に監視し、不正行為をしないようにさせるのが適切です。

- × **ア**, **イ** PCの定期的なウイルス検査やクライアントファイアウォールの導入では、PCにウイルスが感染したり、不正プログラムからの攻撃を防止したりできますが、システム運用管理者の故意による不正行為は防止できません。
- **ウ** 正解です。
- × **エ** 機密ファイルをバックアップしても、システム運用管理者の故意による不正行為は防止できません。

○ 解答 ○

問15 **ア**

問16 **ア**

問17 **ア**

問18 **ウ**



問 19 認証局が侵入され、攻撃者によって不正なWebサイト用のデジタル証明書が複数発行されたおそれがある。どのデジタル証明書が不正に発行されたものかわからない場合、誤って不正に発行されたデジタル証明書を用いたWebサイトにアクセスしないために利用者側で実施すべき対策はどれか。

- ア** Webサイトのデジタル証明書の有効期限が過ぎている場合だけアクセスを中止する。
- イ** Webサイトへのアクセスログを確認し、ドメインがWhoisデータベースに登録されていない場合だけアクセスする。
- ウ** 当該認証局のCP (Certificate Policy)の内容を確認し、セキュリティを考慮している内容である場合だけアクセスする。
- エ** ブラウザで当該認証局を信頼していない状態に設定し、Webサイトのデジタル証明書に関するエラーが出た場合はアクセスを中止する。



問 20 コンピュータフォレンジクス(Computer Forensics)を説明したものはどれか。

- ア** 画像や音楽などのデジタルコンテンツに著作権者などの情報を埋め込む。
- イ** コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つであり、システムを実際に攻撃して侵入を試みる。
- ウ** 証拠となりうるデータを保全し、その後の訴訟などに備える。
- エ** ネットワークの管理者や利用者などから、巧みな話術や盗み聞き、盗み見などの手段によって、パスワードなどのセキュリティ上重要な情報を入手する。



問 21 セキュリティ上、脆弱性^{ぜい}のあるホストやシステムをあえて公開し、受けた攻撃の内容を観察するためのものはどれか。

- | | |
|-----------------|----------------------|
| ア IDS | イ インシデントレスポンス |
| ウ スパイウェア | エ ハニーポット |

解説

問19 認証局への侵入

認証局は、Webサイトの正当性を証明するためのデジタル証明書を発行する組織です。認証局が侵入され、攻撃者によって不正なデジタル証明書が発行されると、攻撃者が用意した偽のWebサイトにアクセスしようとしたとき、そのサイトが用いている不正なデジタル証明書を参照することで、偽のWebサイトを正当なものと誤認してしまう危険性があります。

このような場合は、不正なデジタル証明書を用いているWebサイトにアクセスしないのが適切な対策です。ただし、どのデジタル証明書が不正に発行されたかわからないので、攻撃を受けた認証局が発行しているデジタル証明書は全て不正なものとみなしてアクセスを避けるべきです。ブラウザのセキュリティ設定を変更して、当該認証局を「信頼しない」状態にすると、その認証局が発行したデジタル証明書を用いたサイトにアクセスしようとしたときに警告やエラーが表示されます。その場合はアクセスを中止することで、不正なデジタル証明書を参照する危険性は減ります。

- × **ア** 有効期限が過ぎていなくても、攻撃者が発行した不正なデジタル証明書を参照するのは危険です。
- × **イ** ドメインがWhoisデータベースに登録されていることと、そのドメインのWebサイトのデジタル証明書の正当性とは関係がありません。
- × **ウ** **CP** (Certificate Policy)は、認証局の責任やセキュリティ運用方針などを示す文書です。当該認証局はすでに攻撃者の攻撃を受けているので、CPでセキュリティを考慮していると公表していても、実際の運用ではセキュリティに問題があったと考えるのが妥当です。CPを参照することには意味がありません。
- **エ** 正解です。

問20 コンピュータフォレンジクス

コンピュータフォレンジクス(デジタルフォレンジクス)とは、不正アクセスなどのコンピュータ犯罪に対する科学的調査のことで、不正アクセスなどに関する証拠(記録・ログなど)を立証するために必要なデータを保全して収集・分析すること、及びその後の訴訟などに備えることです。

- × **ア** **ステガノグラフィ**の説明です。
- × **イ** **ペネトレーションテスト**の説明です。
- **ウ** 正解です。
- × **エ** **ソーシャルエンジニアリング**の説明です。

問21 故意の脆弱性公開による観察

脆弱性のあるコンピュータやルータ、もしくはシステムなどを外部に公開し、クラッカーなどに当該コンピュータなどを攻撃させ、攻撃内容を観察するために設けるものを**ハニーポット**といいます。ハニーポットは、不正侵入の手口などを解析するために利用されるものであり、適切に用いれば自社の情報セキュリティの向上などを図ることができます。

- × **ア** **IDS**とは、内部ネットワークに対する外部(インターネットなど)からの攻撃を検知するためのシステムのことです。
- × **イ** **インシデントレスポンス**とは、発生したインシデント(セキュリティが侵害された事象、またはセキュリティが侵害されそうになった事象)への対処のことです。
- × **ウ** **スパイウェア**とは、通常の無害なソフトウェアに見せかけてコンピュータ内にインストールされる不正プログラムです。インストールされたスパイウェアは、秘密裏にコンピュータ内の個人情報やパスワードなどの情報を特定の外部サーバに送付したり、Web閲覧時にユーザの意図しない広告を勝手に表示したりするなどの処理を行います。
- **エ** 正解です。

○ 解答 ○

問 19 **エ**

問 20 **ウ**

問 21 **エ**



問22 SSL/TLSの利用に関する記述のうち、適切なものはどれか。

- ア SSL/TLSで使用する個人認証用のデジタル証明書は、ICカードなどに格納できるので、格納場所を特定のPCに限定する必要はない。
- イ SSL/TLSは特定利用者間の通信のために開発されたプロトコルであり、Webサーバ提供者への事前の利用者登録が不可欠である。
- ウ デジタル証明書にはIPアドレスが組み込まれているので、SSL/TLSを利用するWebサーバのIPアドレスを変更する場合は、デジタル証明書を再度取得する必要がある。
- エ 日本国内では、SSL/TLSで使用する共通鍵の長さは、128ビット未満に制限されている。



問23 SSHの説明はどれか。

- ア MIMEを拡張した電子メールの暗号化とデジタル署名に関する標準
- イ オンラインショッピングで安全にクレジット決済を行うための仕様
- ウ 対称暗号技術と非対称暗号技術を併用した電子メールの暗号化、復号の機能をもつ電子メールソフト
- エ リモートログインやリモートファイルコピーのセキュリティを強化したツール及びプロトコル



問24 無線LANのセキュリティ技術に関する記述のうち、適切なものはどれか。

- ア ESS-ID及びWEPを使ってアクセスポイントと通信するには、クライアントにEAP(Extensible Authentication Protocol)を実装する必要がある。
- イ WEPの暗号化鍵の長さは128ビットと256ビットがあり、どちらを利用するかによって処理速度とセキュリティ強度に差が生じる。
- ウ アクセスポイントにMACアドレスを登録して認証する場合、ローミング時にESS-IDを照合しない。
- エ 無線LANの複数のアクセスポイントが、1台のRADIUSサーバと連携してユーザ認証を行うことができる。

解説

問22 SSL/TLS

SSL/TLSの個人認証用デジタル証明書は、数百バイト前後の容量です。この性質により、USBメモリなどに記録して持ち運べるため、特定の機器に固定することなく使用できます。

- ア 正解です。
- × イ 特定ユーザ間だけではなく、不特定多数のユーザとの認証・暗号化機能を、公開鍵暗号方式で実現しています。
- × ウ 証明書に必須の項目は、認証局(CA)の情報などです。IPアドレスは証明書に必須の項目でなく、オプションとして記載可能な項目です。
- × エ SSL/TLSで使用する共通鍵の長さは、128ビット、256ビットなど各種存在し、日本国内では使用できる鍵の長さが制限されるなどということはありません。

問23 SSH

SSH (Secure Shell)は、リモートログインやリモートファイルコピーなどを、通信経路上のデータを暗号化した上で行うことができるツール及びプロトコルのことです。リモートログインを行うツール及びプロトコルとして Telnet が古くから使用されていますが、Telnetは通信経路上のデータが暗号化されないため、パスワードなどが平文のまままで送信されてしまう危険性があります。この危険性に対応するため、SSHなどが用いられます。

- × ア MIMEを拡張した電子メールの暗号化・デジタル署名の技術は、S/MIMEです。
- × イ オンラインショッピングで安全にクレジット決済を行うための仕様は、SETです。
- × ウ 対称暗号技術と非対称暗号技術を併用する電子メールの暗号化・復号ツールには、PGP (Pretty Good Privacy)などがあります。
- エ 正解です。

問24 無線LANのセキュリティ

無線LANに関する各種のセキュリティ技術を説明します。

WEP: WEP (Wired Equivalent Privacy)は、IEEE 802.11bなどの規格において用いられている無線LANの暗号化技術で、40ビットまたは104ビットの暗号化用の情報と、通信の都度ランダムに生成した24ビットの情報(IV, Initialization Vector)とを組み合わせ、暗号化鍵を生成する方法をとっています。この機能を有効にすることで、無線LANの通信データを暗号化することが可能となります。ただし、この暗号化技術は鍵の長さが短いなどの、脆弱性があることが指摘されています。

ESS-ID: ESS-IDとは、無線LANのアクセスポイントを識別するために、各クライアントに設定される文字列のことです。各クライアントは、同じ値のESS-IDをもつアクセスポイントのみに接続することができます。

MACアドレス制限: MACアドレス制限とは、無線LANのセキュリティ機能の一つであり、指定したMACアドレスをもつ機器のみ、無線LANのアクセスポイントに接続することを可能とする機能です。

WPA: WPA (Wi-Fi Protected Access)とは、鍵のビット数が少ないなどのWEPの脆弱性を改良するために作成された、無線LANの暗号規格やプロトコルなどの総称です。WPAでは、TKIP (Temporal Key Integrity Protocol) という鍵交換プロトコルや、IEEE 802.1Xという認証のためのプロトコルを利用しています。IEEE 802.1Xでは、複数のアクセスポイントが、1台のRADIUSサーバに対してユーザの情報を参照することで、ユーザ認証を行うことのできる仕組みを実装しています。

WPAの説明から、無線LANの複数のアクセスポイントは、1台のRADIUSサーバと連携してユーザ認証を行うことができるとわかります。よって、エが正解です。

- × ア EAP (Extensible Authentication Protocol)は、ユーザ認証プロトコルの一つです。このプロトコルは、WPAの認証プロトコルであるIEEE 802.1xにおいて、ユーザの認証を行うために採用されています。WPAを用いず、ESS-IDとWEPを用いてアクセスポイントと通信するときは、EAPをクライアントに実装させる必要はありません。
- × イ WEPの暗号化鍵の長さは40ビットまたは104ビットとなります。
- × ウ 無線LANのローミング機能とは、携帯電話などのローミング機能と同様のもので、異なるアクセスポイントのエリアに移動しても、端末がそのまま通信を継続できるようにする機能のことです。MACアドレス制限を用いる場合でも、ローミング時には端末とアクセスポイントとの間でESS-IDの照合が実行されます。
- エ 正解です。

○ 解答 ○

問 22 ア

問 23 エ

問 24 エ



問25 安全なWebアプリケーションの作り方について、攻撃と対策の適切な組合せはどれか。

	攻撃	対策
ア	SQLインジェクション	SQL文の組立てに静的プレースホルダを使用する。
イ	クロスサイトスクリプティング	任意の外部サイトのスタイルシートを取り込むようにする。
ウ	クロスサイトリクエストフォージェリ	リクエストにGETメソッドを使用する。
エ	セッションハイジャック	利用者ごとに固定のセッションIDを使用する。

解説

問25 安全なWebアプリケーション

Webアプリケーションに関する各種の脅威をまとめます。

● SQLインジェクション(ア)

SQLインジェクションとは、Webページ上の入力フォームに不正な文字列を入力し、その文字列から生成されたSQL文を不正なものにして、Webアプリケーションを誤動作させたり、データベースの内容を不正に閲覧または削除したりする攻撃方法のことです。

例として、検索したい名前の文字列(文字列Xとする)をWebページの入力フォームに入力させるWebアプリケーションシステムを考えます。このシステムのWebページから呼び出されるCGIの処理中では、

```
SELECT * FROM TABLE_A WHERE name like '文字列X'
```

のように、列nameの値が文字列Xと等しい行のみを検索するSQL文を作成します。この入力フォームに、例えば「';DELETE FROM TABLE_A WHERE 'A'='A」のような文字列が入力可能になっていると、以下のようなSQL文が作成されてしまい、TABLE_Aの全部の行が削除されてしまうことになります。

```
SELECT * FROM TABLE_A WHERE name like ''';DELETE FROM TABLE_A WHERE 'A'='A'
```

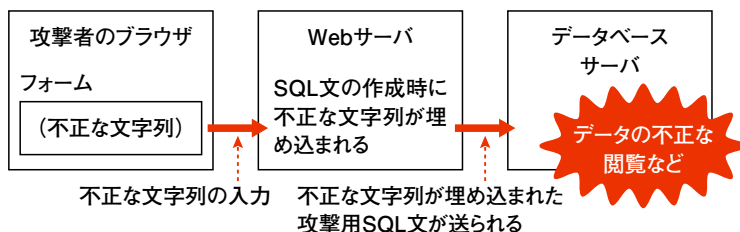
この入力フォームでは、「'」のような、SQL文中で使用される「データベースの操作・問合せにおいて特別な意味をもつ」文字が入力可能であったため、問題が発生したことになります。よって、入力値から「'」、「"」などの特別な文字を取り除く(エスケープ処理をする)ことで、SQLインジェクションは防止できます。

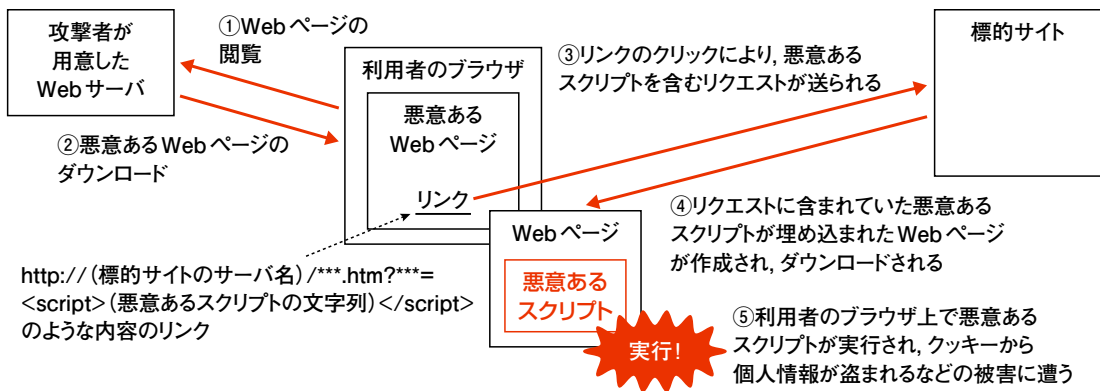
また、**バインド機構**の使用によっても、SQLインジェクションを防止できます。バインド機構とは、変数部分に仮の文字列(**静的プレースホルダ**)をあてはめて作成された「SQL文の雛形」をあらかじめ用意しておき、Webページから変数(データ)が入力された際には、その変数にエスケープ処理を施して得られた変数(**バインド変数**)を、SQL文の雛形にあてはめて実行する方式です。

● クロスサイトスクリプティング(イ)

クロスサイトスクリプティングとは、悪意あるスクリプトを含んだ不正なリンクを利用者のブラウザに送り込み、標的サイトにアクセスした利用者の個人情報をクッキーから盗み取るなどの手法を用いる攻撃方法です。

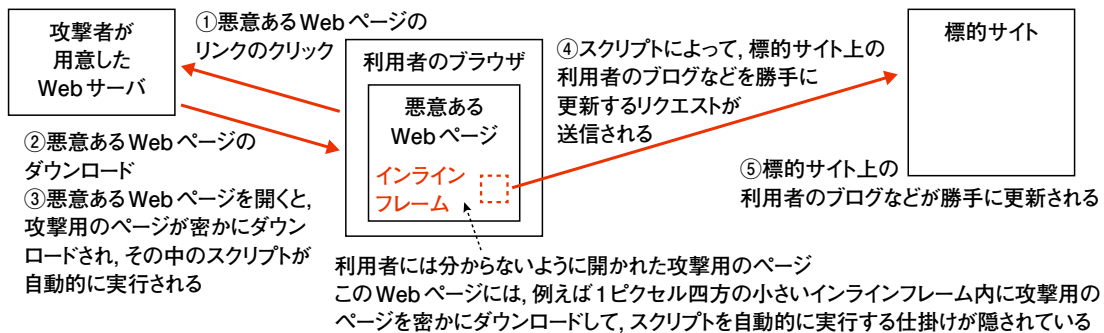
クロスサイトスクリプティングを防ぐには、CGIに入力されるデータのサニタイジングなどの措置が適切です。任意の外部サイトのスタイルシートを取り込むようにしても、クロスサイトスクリプティングを防ぐことはできません。





● クロスサイトリクエストフォージェリ(ア)

悪意あるスクリプトを含んだ攻撃用のページを密かにダウンロードして、そのスクリプトを自動的に実行するようなWeb ページを利用者のブラウザで開かせるなどの方法で、標的サイトに対して別のWeb サイト上のページから不正なリクエスト(処理要求)を送信して、標的サイト上で意図しない操作を行わせる攻撃のことです。



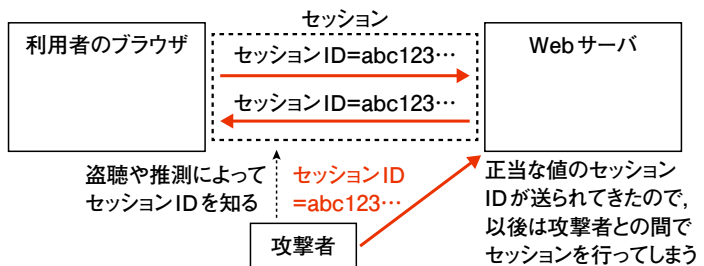
クロスサイトリクエストフォージェリを防止するには、他のサイト上のWeb ページから送信されてきたリクエストを、自分のサイトでは受け付けられないようにすることが有効です。リクエストにGET メソッドを使用しても、クロスサイトリクエストフォージェリを防止することはできません。

● セッションハイジャック(エ)

Web サーバとブラウザの間で行われる継続的なやり取りをセッションと呼びます。セッションを維持するために、Web サーバはセッションIDという値をブラウザと交換し合い、その値が適切である限り、正当な利用者(ブラウザ)と適切にやり取りを行っていると判断します。

このセッションIDが固定値である場合など、その値が容易に推測できるような状況では、悪意のあるユーザがセッションIDの値を推測した上で、正当なブラウザになりすましてWeb サーバ間のセッションを乗っ取ってしまうことが可能です。この攻撃方法を、セッションハイジャックと呼びます。

セッションハイジャックを防止するには、セッションIDの値を推測困難なものとし、暗号化してデータの送受信を行うなどの措置が適切です。以上より、アの組合せが適切です。



○ 解答 ○

問 25 ア



問26 Webページの著作権に関する記述のうち、適切なものはどれか。

- ア 営利目的でなく趣味として、個人が開設しているWebページに他人の著作物を無断掲載しても、私的使用であるから著作権の侵害とはならない。
- イ 作成したプログラムをインターネット上でフリーウェアとして公開した場合、配布されたプログラムは、著作権法による保護の対象とはならない。
- ウ 試用期間中のシェアウェアを使用して作成したデータを、試用期間終了後もWebページに掲載することは、著作権の侵害に当たる。
- エ 特定の分野ごとにWebページのURLを収集し、独自の解釈を付けたリンク集は、著作権法で保護される。



問27 不正競争防止法において、営業秘密となる要件は、“秘密として管理されていること”、“事業活動に有用な技術上又は営業上の情報であること”ともう一つはどれか。

- ア 営業譲渡が可能なこと
- イ 期間が10年を超えないこと
- ウ 公然と知られていないこと
- エ 特許出願していること



問28 企業のWebサイトに接続してWebページを改ざんし、システムの使用目的に反する動作をさせて業務を妨害する行為を処罰の対象とする法律はどれか。

- ア 刑法
- イ 特定商取引法
- ウ 不正競争防止法
- エ プロバイダ責任制限法

解説

問26 著作権

著作権とは、著作物を創作した者(著作者)に与えられる権利です。**著作権法**では、「思想または感情を創作的に表現したもの」を著作物と定義しています。著作物の題号は、一般的な語句の組合せで構成された比較的短い字句となり、思想または感情を創作的に表現していないとみなされるので、著作物とは認められません。同様に、WebページのURLも著作権法における著作物と認められません。しかし、URLに独自の解釈を付けたリンク集は、その解釈に著作者の思想が反映されているので著作物に該当します。

- × **ア** 個人が開設しているWebページであっても、公開しているWebページに他人の著作物を無断掲載する行為は、著作権の侵害となります。
- × **イ** フリーウェアのプログラムは、著作者の許可を取らなくても無料で利用可能です。しかし、フリーウェアのプログラムであっても、著作者の著作権が放棄されているわけではありません。
- × **ウ** シェアウェアを使用して作成したデータの著作権は、シェアウェアの著作者ではなく、そのデータを作成した人自身が有します。よって、シェアウェアの試用期間が過ぎて使用資格が消失しても、データの作成者は引き続き著作権を有することになり、Webページ上に掲載しても問題はありません。
- **エ** 正解です。

問27 不正競争防止法

不正競争防止法は、「事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もって国民経済の健全な発展に寄与する」(同法第1条より)ことを目的とした法律です。この法律では幾つかの行為を「不正競争」として定義し、不正競争によって営業上の利益を侵害された者などは、その侵害の停止などを請求する権利があることを規定しています。

この不正競争の一つに、「窃取、詐欺、強迫その他の不正の手段により営業秘密を取得する行為……又は不正取得行為により取得した営業秘密を使用し、若しくは開示する行為」があります。この「**営業秘密**」とは、同法で保護されている対象であり、「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」を指します。よって、**ウ**が適切です。

- × **ア** 営業譲渡が可能か否かについては、営業秘密の要件とは無関係です。
- × **イ** 期間については、営業秘密の要件とは無関係です。
- **ウ** 正解です。
- × **エ** 特許出願をしているかどうかについては、営業秘密の要件とは無関係です。

問28 Webページの改ざんと法律

企業のWebページを改ざんしてシステムの利用目的に反する動作をさせ、業務を妨害する行為は、刑法第234条の2で規定されている**電子計算機損壊等業務妨害罪**に該当します。

第二百三十四条の二 人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する

- **ア** 正解です。
- × **イ** **特定商取引法**は、特定商取引(訪問販売や通信販売など)を公正にし、購入者が受けることのある損害の防止を図ることにより、購入者等の利益を保護することを目的とした法律です。
- × **ウ** **不正競争防止法**は、「事業者間の公正な競争及びこれに関する国際約束の的確な実施を確保するため、不正競争の防止及び不正競争に係る損害賠償に関する措置等を講じ、もって国民経済の健全な発展に寄与する」(同法第1条より)ことを目的とした法律です。
- × **エ** **プロバイダ責任制限法**(正式名称：特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律)は、インターネット上で著作権などの権利侵害があった場合に、権利侵害を行った者がインターネットに接続するために契約していたプロバイダが負うべき責任(損害賠償の義務や、当該人物の住所氏名の公表の義務など)を規定している法律です。

○ 解答 ○

問 26 **エ**問 27 **ウ**問 28 **ア**



問 29 電子署名法に規定されているものはどれか。

- ア 電子署名技術は公開鍵暗号技術によるものと規定されている。
- イ 電子署名には、電磁的記録以外であって、コンピュータ処理の対象とならないものも含まれる。
- ウ 電子署名には、民事訴訟法における押印と同様の効力が認められている。
- エ 電子署名の認証業務を行うことができるのは、政府が運営する認証局に限られる。



問 30 プロジェクトマネージャのP氏は、A社から受託予定のソフトウェア開発を行うために、X社から一時的な要員派遣を受けることを検討している。労働者派遣法に照らして適切なものはどれか。

- ア 厳しいスケジュールが見込まれることから、派遣労働者個人への担保責任を負わせる契約案をX社に提示した。
- イ 前回のプロジェクトの成功に大きく貢献したX社のY氏の参加を指名した。
- ウ 派遣される要員のスキルを適切に判断しようと考え、事前にX社の派遣候補者を面接した。
- エ 派遣者への業務指示など、派遣に伴う各種業務をP氏が直接行うことをX社に伝えた。



問 31 請負契約の下で、自己の雇用する労働者を契約先の事業所などで働かせる場合、適切なものはどれか。

- ア 勤務時間、出退勤時刻などの労働条件は、契約先が調整する。
- イ 雇用主が自らの指揮命令の下に当該労働者を業務に従事させる。
- ウ 当該労働者は、契約先で働く期間は、契約先との間にも雇用関係が生じる。
- エ 当該労働者は、契約先の指示によって配置変更が行える。



問 32 シュリンクラップ契約において、ソフトウェアの使用許諾契約が成立するのはどの時点か。

- ア 購入したソフトウェアの代金を支払った時点
- イ ソフトウェアの入ったCD-ROMを受け取った時点
- ウ ソフトウェアの入ったCD-ROMの包装を破った時点
- エ ソフトウェアをPCにインストールした時点

解説

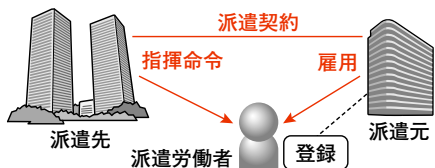
問29 電子署名法

電子署名法の第三条では、「電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。」（同法第三条から引用）と規定しています。これにより、電子署名が「真正に成立したもの」とみなされるため、民事訴訟法による押印や手書きの署名などと同様の効力が、電子署名にも認められることになります。

- × **ア** 電子署名法では、電子署名を実現するための技術を、公開鍵暗号技術に限ってはいません。よって、誤りです。
- × **イ** 電子署名法では、電磁的記録(電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるもの(同法第二条より))に対して行われるもののみを、電子署名と定義しています。よって、誤りです。
- **ウ** 正解です。
- × **エ** 電子署名法では、電子署名の認証業務(特定認証業務)を行おうとする業者は、主務大臣への認定を受ける必要があると規定しています。特定認証業務の遂行は、政府が運営する認証局に限られているわけではありません。

問30 労働者派遣法

労働者派遣法では、「派遣労働者」、「派遣先事業主(企業)」、「派遣元事業主(企業)」の3者間の関係を右の図のように定めています。



- 派遣先事業主と派遣元事業主との間で「労働者派遣契約関係」が締結され、派遣先事業主の依頼に応じて、派遣元事業主が雇用している派遣労働者を派遣先事業主に派遣します。派遣労働者は、派遣先事業主の指揮命令下で業務を行います。よって、派遣者への業務の指示などをP氏が直接行うこと(**エ**)は、適切な行為です。
- × **ア** 派遣労働者は、派遣先事業主の「指揮命令下で」業務を行います。よって、派遣労働者のミスなどによって担当業務が期間内に完了しなかったなどの責は、その派遣労働者に指揮命令を与えていた派遣先事業主が負うこととなります。派遣元事業主や派遣労働者には何の責もないため、契約案に瑕疵担保責任などを盛り込むことは不適切です。
 - × **イ、ウ** 派遣先事業主が、派遣労働者を事前を選別したり、特定の派遣労働者の指名を行ったりすることなどは認められていません。
 - **エ** 正解です。

問31 請負契約

請負契約では、労働者は雇用主(請負元)の指揮命令の下で、契約先(請負先)の指定する勤務先などにおいて作業を行います。労働者と契約先との間には、指揮命令関係はありません。よって、**イ**(雇用主が自らの指揮命令の下に当該労働者を業務に従事させる)が正解です。

- × **ア** 勤務時間などの労働条件は、指揮命令権をもつ雇用主(請負元)が調整します。
- **イ** 正解です。
- × **ウ** 労働者と契約先との間には、契約先で働く期間において、特に雇用関係は生じません。
- × **エ** 契約先には、労働者の配置変更を行う権限はありません。

問32 シュリンクラップ契約

シュリンクラップ契約は、ソフトウェアの入ったCD-ROMなどのメディアの包装を破った時点で、ソフトウェアの使用許諾契約が成立します。よって、**ウ**のみが正解です。購入したソフトウェアの代金を支払った時点またはソフトウェアの入ったCD-ROMを受け取った時点では、ソフトウェアの使用許諾契約は成立しません。代金を支払っていても、包装を破っていない場合は返品などが可能です。ソフトウェアをPCにインストールするためには、メディアの包装を破る必要があるため、ソフトウェアをPCにインストールする時点よりも前にソフトウェアの使用許諾契約が成立しています。

○ 解答 ○

問 29 **ウ**

問 30 **エ**

問 31 **イ**

問 32 **ウ**

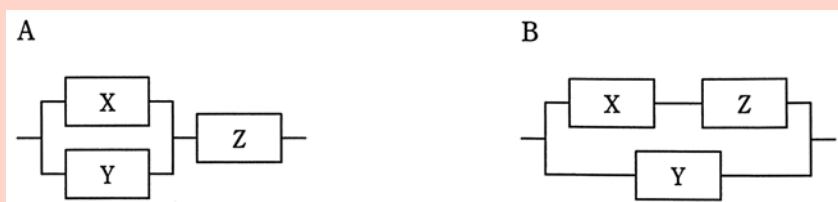


問33 システムの信頼性向上技術に関する記述のうち、適切なものはどれか。

- ア 故障が発生したときに、あらかじめ指定されている安全な状態にシステムを保つことを、フェールソフトという。
- イ 故障が発生したときに、あらかじめ指定されている縮小した範囲のサービスを提供することを、フォールトマスキングという。
- ウ 故障が発生したときに、その影響が誤りとなって外部に出ないように訂正することを、フェールセーフという。
- エ 故障が発生したときに対処するのではなく、品質管理などを通じてシステム構成要素の信頼性を高めることを、フォールトアボイダンスという。



問34 3台の装置X～Zを接続したシステムA, Bの稼働率について、適切なものはどれか。ここで、3台の装置の稼働率は、いずれも0より大きく1より小さいものとする。



- ア 各装置の稼働率の値によって、AとBの稼働率のどちらが高いかは変化する。
- イ 常にAとBの稼働率は等しい。
- ウ 常にAの稼働率が高い。
- エ 常にBの稼働率が高い。

解説

問33 故障への対処方法

システムに故障や異常が発生した場合の各種の対処方法を説明します。

フェールセーフ：異常発生時にはシステムを停止させるか、人間系(オペレータなど)に処理の続行判断を委任し、必ずより安全な状態にシステムを導く方式です。

フェールソフト：異常発生時にはシステムの機能を縮退させた上で、異常の影響のない機器を活用して、性能が低下しても処理をできる限り継続する方式です。

フォールトトレランス：信頼性に大きく影響する機器などを複数備えて故障に対処するなどの方法で、システムの信頼性を高める方式です。

フォールトアボイダンス：製品の品質管理などを通じて、システムを構成するハードウェアなどの要素の信頼性自体を向上させ、始めから故障が起こらないようにすることでシステムの信頼性を高める方式です。

フォールトマスキング：システムを構成する重要な要素を二重化し、一つの要素が故障しても自動的にもう一つの要素に切り替えるなどの機能をシステムに設けることで、内部で故障が発生してもその影響が外部に出ないようにして、故障を利用者に気づかせないままシステムを稼働させ続ける考え方です。

以上から、**エ**の記述のみが適切です。**ア**はフェールソフトではなくフェールセーフの説明です。**イ**はフォールトマスキングではなくフェールソフトの説明です。**ウ**はフェールセーフではなくフォールトマスキングの説明です。

問34 稼働率

各装置X, Y, Zの稼働率を、それぞれx, y, zとおきます。このときのシステムAの稼働率を求めます。

● システムAの稼働率

(1) 装置Xと装置Yが並列になっている箇所の稼働率

$$= 1 - (1 - x) \times (1 - y)$$

$$= 1 - (1 - x - y + xy)$$

$$= x + y - xy$$

(2) 装置Zの稼働率

$$= z$$

(3) 全体の稼働率

システムAは、装置Xと装置Yが並列になっている箇所と、装置Zとの直列構成となるため、

$$(x + y - xy) \times z$$

$$= xz + yz - xyz$$

となります。

● システムBの稼働率

(1) 装置Xと装置Zが直列になっている箇所の稼働率

$$= xz$$

(2) 全体の稼働率

システムBは、装置Xと装置Zが直列になっている箇所と、装置Yとの並列構成となるため、

$$= 1 - (1 - xz) \times (1 - y)$$

$$= 1 - (1 - xz - y + xyz)$$

$$= xz + y - xyz$$

となります。

ここで、システムBの稼働率からシステムAの稼働率を引くと、

$$xz + y - xyz - (xz + yz - xyz)$$

$$= xz + y - xyz - xz - yz + xyz$$

$$= y - yz = y(1 - z)$$

となります。

問題文から、各装置の稼働率はいずれも0より大きく1より小さいため、この式のyは0以上となり、正の値となります。また、(1 - z)も0より大きく1より小さい正の値となります。以上から、y(1 - z)は必ず正の値となります。

よって、システムBの稼働率からシステムAの稼働率を引いた値が必ず正になるため、システムBの稼働率の方がシステムAの稼働率よりも常に大きい値となります。したがって、「常にBの稼働率が高い」(**エ**)が正解です。

○ 解答 ○

問33 **エ**

問34 **エ**



問35 “プログラマは全て社員であり、社員の約10%を占める。社員は社員番号と氏名をもち、職種がプログラマである場合は、使用できるプログラム言語を一つ以上もつ。”という状況を記録するデータベース設計案として、適切なものはどれか。ここで、実線の下線は主キーを、破線の下線は外部キーを表す。

- ア** 社員(社員番号, 氏名, 職種, プログラム言語)
- イ** 社員(社員番号, 氏名, プログラム言語)
- ウ** 社員(社員番号, 氏名)
プログラマ(社員番号, プログラム言語)
- エ** 社員(社員番号, 氏名)
プログラマ(社員番号, プログラム言語)



問36 埋込みSQLにおいて、問合せによって得られた導出表を1行ずつ親プログラムに引き渡す操作がある。この操作と関係の深い字句はどれか。

- ア** CURSOR **イ** ORDER BY **ウ** UNION **エ** UNIQUE



問37 DHCPの説明として、適切なものはどれか。

- ア** IPアドレスの設定を自動化するためのプロトコルである。
- イ** ディレクトリサービスにアクセスするためのプロトコルである。
- ウ** 電子メールを転送するためのプロトコルである。
- エ** プライベートIPアドレスをグローバルIPアドレスに変換するためのプロトコルである。

解説

問35 データベース設計

社員の10%がプログラマであり、社員は社員番号と氏名をもち、プログラマの社員は使用できるプログラム言語を一つ以上もつという状況で、**ア**のような“社員”表を用いると、右のように情報が記録されます。

この表では、プログラマでない社員のプログラム言語がNULLになります。また、プログラマの社員は使用できるプログラム言語を一つ以上もつので、複数のプログラム言語をもっているプログラマの社員の情報を記録

すると、主キーである社員番号が重複する行が現れてしまいます。主キーの重複は許されないなので、このような形式の表は不適切です。**イ**の表も同様になります。

社員の10%だけがプログラマなので、残りの90%の社員はプログラマではありません。**ア**や**イ**の形式の表を用いると、大部分の社員の行のプログラム言語の列の値がNULLになり、情報の格納効率が悪くなります。よって、社員の情報として社員番号と氏名だけを記録する“社員”表と、プログラマの社員番号及びプログラム言語だけを記録する“プログラマ”表の二つを用いることで、大部分の社員については社員番号と氏名だけを記録し、プログラマの社員

“社員”表

社員番号	氏名	職種	プログラム言語
1001	〇〇一郎	営業	NULL
1002	××二郎	経理	NULL
1003	△△三郎	プログラマ	C言語
1003	△△三郎	プログラマ	Java
1003	△△三郎	プログラマ	Perl

だけは、社員番号や氏名に加えてプログラム言語も記録できるようにするのが適切です。

さきほどの表の情報を“社員”表と“プログラマ”表に分けた結果は右のとおりです。

複数のプログラム言語をもっているプログラマの社員の情報を記録すると、“プログラマ”表に同じ社員番号をもつ行が複数現れるので、**ウ**のように社員番号だけでは主キーにはなりません。社員番号とプログラム言語の組が主キーになります。また、“プログラマ”表の社員番号は“社員”表の主キーなので、外部キーになります。

以上から、**エ**が正解です。

“社員”表

社員番号	氏名
1001	〇〇一郎
1002	××二郎
1003	△△三郎

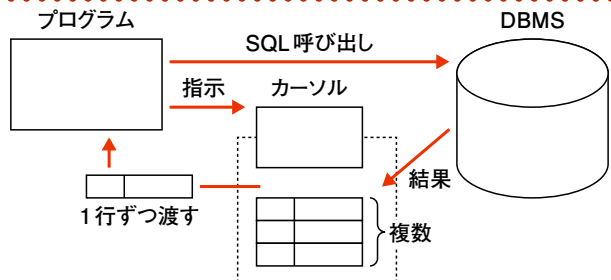
“プログラマ”表

社員番号	プログラム言語
1003	C言語
1003	Java
1003	Perl

問36 データベースの実行結果の受け渡し

一般的な業務プログラム中からのSQL呼出しによってDBMSの表を検索する場合、SELECT文を実行すると、ほとんどの場合DBMSから複数の行(レコード)が結果としてまとめて返されます。

よって、DBMSとプログラム言語との間で実行結果を受け渡すための機能として、**カーソル**が用いられます。カーソルは、SELECT文の実行結果としてDBMSから返された複数の行を一時的に格納しておき、プログラムからデータ読み込みの指定があるたびに、結果の行を1行ずつプログラムに渡します。このカーソルの作成のために“DECLARE CURSOR”文を使用します。よって、**ア**のCURSOR句が正解です。



○ **ア** 正解です。

× **イ** **ORDER BY** 句は、SELECT文の実行結果を特定の列の値の昇順または降順に整列するために用います。

× **ウ** **UNION** 句は、複数のSELECT文の実行結果を一つにまとめるために用います。

× **エ** **UNIQUE** 句は、特定の列にユニーク制約(値が一意でなければならないこと)を設定するために用います。

問37 DHCP

クライアントに固定的にIPアドレスを付与する方式では、IPアドレスの管理が煩雑になったり、ネットワークの構成変更時にクライアントのIPアドレスの設定変更のための工数が膨大になったりするという問題があります。

TCP/IPのプロトコルの一つである**DHCP**では、クライアントは起動時にDHCPサーバに接続して、その時点で空いているIPアドレスの割当てを動的に受け取ります。クライアントの電源が切れたときは、そのクライアントに与えられていたIPアドレスは回収され、別のクライアントから使用可能になります。

○ **ア** 正解です。

× **イ** ディレクトリサービスにアクセスするためのプロトコルには、**LDAP** (Lightweight Directory Access Protocol) などがあります。

× **ウ** 電子メールを転送するためのプロトコルは、**SMTP** (Simple Mail Transfer Protocol) です。

× **エ** プライベートIPアドレスをグローバルIPアドレスに変換するためのプロトコルは存在しません。なお、プライベートIPアドレスをグローバルIPアドレスに変換するための技術として、**NAT** (Network Address Translation) があります。

○ 解答 ○

問 35 **エ**

問 36 **ア**

問 37 **ア**

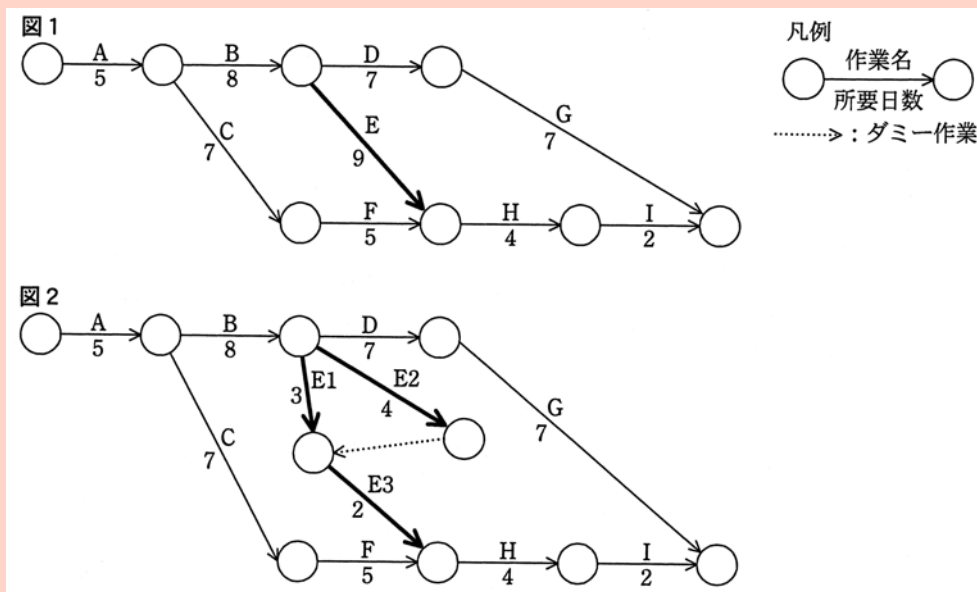


問38 クラスCのIPアドレスを分割して、10個の同じ大きさのサブネットを使用したい。ホスト数が最も多くなるように分割した場合のサブネットマスクはどれか。

- ア 255.255.255.192 イ 255.255.255.224 ウ 255.255.255.240 エ 255.255.255.248



問39 ファストトラッキング技法を用いてスケジュールの短縮を行う。当初の計画は図1のとおりである。作業Eを作業E1, E2, E3に分けて、図2のように計画を変更すると、スケジュールは全体で何日短縮できるか。



- ア 1 イ 2 ウ 3 エ 4

解説

問38 サブネットマスク

IPアドレスは、インターネットの通信プロトコル(TCP/IP)において、コンピュータ等を全世界中で一意に識別するために付与されるアドレスです。IPアドレスは32ビット(4バイト)で表現され、32ビット中の上位ビットを「ネットワーク部」、残りの下位ビットを「ホスト部」と呼びます。

比較的大規模のLAN環境では、LAN全体を一つのネットワークとするより、LAN全体を細分化して小規模なネットワーク(サブネットワーク、又はサブネットと呼びます)を複数作成し、サブネット内のPCは同じサブネット内の他のPCとだけ通信可能にするという形態にした方が有効な場合があります。

IPアドレスのうち、ホスト部の上位の数ビットをサブネット識別のためのアドレス「サブネット部」とします。サブネットに分割されたネットワークは、ネットワーク部とサブネット部をひとまとめにして、サブネットを区別します。

このサブネット部のビット数により、ネットワークを細分化できる個数(サブネットの個数)が決定します。例えばサブネット部を3ビット確保した場合、 $2^3=8$ 個の異なるビット列を得られるので、サブネットの個数は8個です。

そのためには、IPアドレスの上位何ビットまでが、サブネットを区別するための「ネットワーク部とサブネット部」であるかを表現するには、サブネットマスクを用います。サブネットマスクは、「ネットワーク部とサブネット部」がIPア

ドレスの左から何ビット目までを占めているかを“1”のビットで表し、ホスト部に当たる部分を“0”のビットで記載します。

例えば、クラスC(ネットワーク部=24ビット、ホスト部=8ビット)のIPアドレスをもつネットワークを5個のサブネットに分割する場合、サブネット部は3ビットあれば十分です。よって、右の図のようになります。

問題文では、「10個の同じ大きさのサブネット」を使用するので、サブネット部は4ビット($2^4 - 2 = 14$)以上あればよいことになります。ただし、ホスト部のビット数を最も大きくして、ホスト数が最も多くなるように分割するには、サブネット部のビット数を必要最低限の4ビットのみにします。

クラスC(ネットワーク部=24ビット)のIPアドレスにおいてサブネット部に4ビット設定した場合、サブネットマスクの値は以下のようになります。

$$1111\ 1111\ .\ 1111\ 1111\ .\ 1111\ 1111\ .\ 1111\ 0000 = 255.255.255.240$$

【サブネット分割しないネットワーク】

IPアドレス：

ネットワーク部	ホスト部
---------	------



【サブネット分割したネットワーク】

IPアドレス：

ネットワーク部	サブネット部	ホスト部
---------	--------	------

ネットワーク部	サブネット部	ホスト部
---------	--------	------

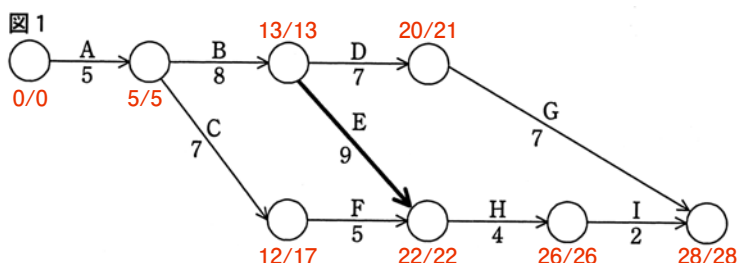
1111 1111 . 1111 1111 1111 . 111 00000
 ↓ (10進数に)
 255 . 255 . 255 . 224 と表す

問39 ファストトラッキング技法

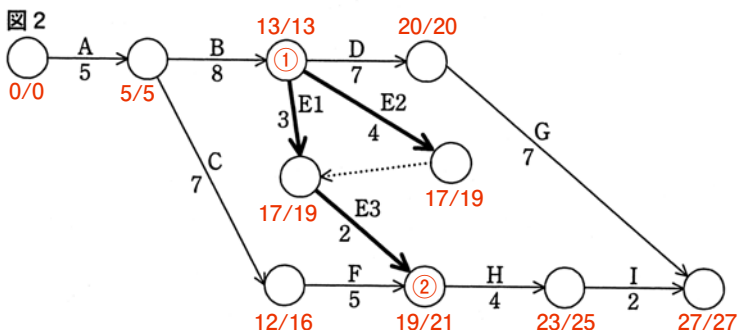
ファストトラッキング技法とは、アローダイアグラム中の作業のうち、前倒しが可能なものを前倒ししたり、大きな作業を小さな複数の作業に分割して並行実行したりして、スケジュールの短縮を図ることです。

図1のアローダイアグラムの全ての作業を完了するのに要する時間は28日です(右図参照)。このアローダイアグラムのクリティカルパスはA→B→E→H→Iです。

図1の作業Eを作業E1、E2、E3に分けて、図2のように計画を変更したとき、全ての作業を完了するのに要する時間は27日です(右図参照)。このアローダイアグラムのクリティカルパスはA→B→D→Gです。右図の①から②に至るまでの時間が、変更前の9日から6日に変更されたため、①からE1、E3、H、Iを経由する経路の日数よりも、①からD、Gを経由する経路の日数の方が長くなり、クリティカルパスが変更されることに注意が必要です。アが正解です。



凡例 x/y : x=最早結合点時刻, y=最遅結合点時刻



○ 解答 ○

問 38 ア

問 39 ア

問40 プロジェクト要員がインフルエンザに感染することを予防するために、“ワクチン接種”費用をプロジェクトで負担し、また“アルコール製剤”をプロジェクトルームの入り口やトイレに配備する。このリスク対応策は、どのリスク対応戦略に該当するか。ここで、リスク対応戦略の分類はPMBOKに従うものとする。

ア 回避

イ 軽減

ウ 受容

エ 転嫁

問41 (1)～(4) はある障害の発生から本格的な対応までの一連の活動である。(1)～(4) の各活動とそれに対応するITILv3の管理プロセスの組合せのうち、適切なものはどれか。

- (1) 利用者からサービスデスクに“特定の入力操作が拒否される”という連絡があったので、別の入力操作による回避方法を利用者に伝えた。
- (2) 原因を開発チームで追及した結果、アプリケーションプログラムに不具合があることが分かった。
- (3) 原因となったアプリケーションプログラムの不具合を改修する必要があるのかどうか、改修した場合に不具合箇所以外に影響が出る心配はないかどうかについて、関係者を集めて確認し、改修することを決定した。
- (4) 改修したアプリケーションプログラムの稼働環境への適用については、利用者へ周知、適用手順及び失敗時の切戻し手順の確認など、十分に事前準備を行った。

	(1)	(2)	(3)	(4)
ア	インシデント管理	問題管理	変更管理	リリース管理及び展開管理
イ	インシデント管理	問題管理	リリース管理及び展開管理	変更管理
ウ	問題管理	インシデント管理	変更管理	リリース管理及び展開管理
エ	問題管理	インシデント管理	リリース管理及び展開管理	変更管理

解説

問40 リスクマネジメント

業務中に発生する偶発的または人為的な障害・事故によって、業務システム上のデータやプログラムが破壊されたり、業務が長時間停止させられたりすることがあります。その結果、修復費用の発生や機会損失による利益の喪失などにより、多大な損失が発生することが往々にしてあります。

これらの「損失の発生する可能性」を**リスク**と呼びます。リスクの防止、リスク発生時に被害を最小限にするための施策の制定、及びリスク発生によって生じる費用に対する積み立て措置を講じるなどの手法によってリスクを管理することを、**リスクマネジメント**といいます。

なお、PMBOKでは損失が発生する事象だけでなく、自社に利益をもたらす事象もリスクと定義しています。損失が発生する事象をマイナスのリスク、利益をもたらす事象をプラスのリスクといいます。

PMBOKで規定されている、プロジェクトのリスクマネジメントにおけるリスク対応戦略を示します。

● マイナスのリスクに対するリスク対応戦略

- ・**リスク回避**：リスクそのものを発生させなくすること
- ・**リスク転嫁**：保険に加入するなどの手段で資金面での対策を行い、リスク発生時の影響、損失、責任の一部また

は全部を他者に肩代わりさせること

・**リスク軽減**: リスクの発生確率や被害額を低減させること

● **プラスのリスクに対するリスク対応戦略**

・**リスク強化**: リスクの発生確率や利益額を上げて、利益を得やすくすること

・**リスク共有**: 第三者とリスクを共有し、利益を得やすくすること

・**リスク活用**: プラスのリスクが確実に発生するようにすること

● **プラスのリスク、マイナスのリスク両方に対するリスク対応戦略**

・**リスク受容**: 軽微なリスクに対してはあえて対策を行わず、リスクが発生した場合の損失は自社で負担すること

プロジェクト要員がインフルエンザに感染することを予防するためにワクチン予防接種費用を負担したり、アルコール製剤を配備したりすることで、プロジェクト要員のインフルエンザ感染確率を下げるすることができます。しかし、予防接種を受けなかったり手洗いを励行しなかったりしたプロジェクト要員がインフルエンザに感染する可能性が残るので、感染のリスクを完全に排除することはできません。このリスク対応戦略はリスク軽減(イ)です。

問41 ITIL

ITILの各種管理プロセスを示します。

インシデント管理: 日常的に発生する障害の発生時に、業務処理をできる限り早期に再開できるようにシステムを早急に回復させ、障害による事業活動への影響を最小限にすることを目的としている業務プロセスのことです。ハードウェアの故障などの日常的に発生する障害のことを、**インシデント**と呼びます。

インシデント管理では、インシデントが発生した原因を究明するなどの措置は行わず、とりあえず現在発生しているインシデントからシステムを早期に復旧させ、システムを利用できるようにします。

問題管理: 未知のインシデントの発生原因を究明し、それに対する解決策(是正措置)などを考案し、問題管理プロセスの後に実行されるプロセスに当該解決策を提案することで、インシデントの発生を恒久的に防止することを目的としているプロセスのことです。

このプロセスでは、システムの稼働状況などの情報からインシデントの原因を求め、同様のインシデントが今後発生しないようにするために、システムの運用手順を変更したりソフトウェアのバグを取り除いたりするなどの変更要求を、**RFC** (Request For Change)という書類にまとめて変更管理プロセスに提案します。

変更管理: 問題管理プロセスから提案されたRFCに記載されている、問題の解決策としてのシステムの変更要求を検討し、当該要求が実現可能かつ妥当なものであれば、RFCに従ってシステムの変更を行うプロセスのことです。

リリース管理及び展開管理: 変更管理によって実行されたシステムの変更を、正しい場所に、適切な時期にリリース(適用)するとともに、利用者への周知や失敗時の切戻し手順の確認などの事前準備を行うためのプロセスのことです。

本問の(1)～(4)の活動について考えます。(1)は“特定の入力操作が拒否される”というインシデントに対して、その原因の究明などは後回しにして、とりあえず他の入力操作をしてシステムを利用できるようにしているため、インシデント管理です。(2)は前述のインシデントの原因を究明しているため、問題管理です。(3)はインシデントの原因(アプリケーションプログラムの不具合)を改修する必要があるかどうかを検討しているため、変更管理です。(4)は変更管理によって実行されたシステムの変更を適用しようとしているため、リリース管理及び展開管理です。

以上から、正解はアです。

○ 解答 ○

問40 イ

問41 ア



問 42 電源の瞬断時に電力を供給したり、停電時にシステムを終了させるのに必要な時間の電力を供給したりすることを目的とした装置はどれか。

ア AVR

イ CVCF

ウ UPS

エ 自家発電装置



問 43 情報セキュリティに関する従業員の責任について、“情報セキュリティ管理基準”に基づいて監査を行った。指摘事項に該当するものはどれか。

ア 雇用の終了をもって守秘責任が解消されることが、雇用契約に定められている。

イ 定められた勤務時間以外においても守秘責任を負うことが、雇用契約に定められている。

ウ 定められた守秘責任を果たさなかった場合、相応の措置がとられることが、雇用契約に定められている。

エ 定められた内容の守秘義務契約書に署名することが、雇用契約に定められている。



問 44 営業債権管理業務に関する内部統制のうち、適切なものはどれか。

ア 売掛金回収条件の設定は、営業部門ではなく、審査部門が行っている。

イ 売掛金の消込み入力と承認処理は、販売を担当した営業部門が行っている。

ウ 顧客ごとの与信限度の決定は、審査部門ではなく、営業部門の責任者が行っている。

エ 値引き又は割戻しの処理は、取引先の実態を熟知している営業部門の担当者が行っている。

解説

問42 電力断時の電力供給

落雷などによって発電所などの施設が一時的に使用不可になると、電力会社は電源の供給ルートを切り替えるなどの措置によって電力の供給を継続させます。その際に、供給ルートを切り替えるために要したわずかな時間(数秒～数分)のみ、コンセントからの電力の供給が途切れることがあります。このような現象を「**瞬断**」といいます。

瞬断は、電灯などの単純な機器にとっては特に問題のない現象ですが、コンピュータにとっては重大な問題を引き起こす恐れがあります。一瞬でも電流の供給が途切れると、コンピュータは停止してしまいます。そのため、磁気ディスク装置などに書き込みを行っている最中に瞬断が発生すると、最悪の場合、磁気ディスクの故障でコンピュータの起動ができなくなるなどの障害の原因になります。

UPS (Uninterruptible Power Supply, 無停電電源装置)は、商用電源の一時的な停電や瞬断によって電流の供給が絶たれた場合に、コンピュータなどに一定時間安全に電流を供給するための装置です。UPSの内部にはバッテリーなどが存在し、コンセントから供給される電流が途絶えた場合にはバッテリーの電気を利用して即座に電流を供給することで、コンピュータの継続稼働を可能にしています。

× **ア AVR** (Automatic Voltage Regulator, 自動電圧調整器)は、入力電圧が変化しても出力電圧を常に一定に保つ装置です。

× **イ CVCF** (Constant Voltage Constant Frequency, 定電圧定周波数装置)は、非常用電源として用いられます。CVCFは、電力供給の停止を検知してから発電開始まで数秒から数分程度の時間が掛かるため、瞬断発生時に即座に電力を供給できません。

○ **ウ** 正解です。

× **エ** 自家発電装置は、ガソリンエンジンなどを用いて電力を供給する発電装置です。

問43 情報セキュリティ管理基準

企業や政府などの情報セキュリティ対策が適切に実行され、情報セキュリティに係るリスクマネジメントが効果的に実施されているかどうかを、情報セキュリティ監査によって確認するための制度のことを**情報セキュリティ監査制度**といいます。この制度においては、経済産業省が公表している**情報セキュリティ監査基準**や**情報セキュリティ管理基準**が、情報セキュリティ監査の尺度として用いられます。

情報セキュリティ管理基準は、組織体が効果的な情報セキュリティマネジメント体制を構築し、情報セキュリティに関するコントロールを適切に整備・運用するための実践規範です。情報セキュリティ管理基準の「4 人的セキュリティ」の章では、従業員の雇用条件について以下のように規定しています。

- 4.1.4 雇用条件には、情報セキュリティに対する従業員の責任について記述してあること
4.1.4.1 適切ならば、これらの責任を、雇用終了後の定められた期間継続すること

「情報セキュリティに対する従業員の責任」とは、社内の機密情報を外部に漏らさないこと、すなわち守秘責任などのことです。従業員の雇用を終了しても、これらの責任を一定期間継続することが、情報セキュリティ管理基準で規定されています。したがって、雇用の終了をもって守秘責任が解消されるという**ア**の記述は情報セキュリティ管理基準に反しており、指摘事項となります。

- **ア** 正解です。
× **イ** 情報セキュリティ管理基準では、「4.1.4.6 雇用条件には、通常の勤務場所及び勤務時間からは外れた状況においても、これらの責任が適用されることの記述があること」と規定しています。よって、定められた勤務時間以外でも守秘責任を負うことを雇用契約に定めることは、特に問題はありません。
× **ウ** 情報セキュリティ管理基準では、「4.1.4.2 従業員がセキュリティ要求事項を無視した場合に採る措置についても雇用条件に含めること」と規定しています。よって、セキュリティ要求事項で定められた守秘責任を果たさなかった場合、相応の措置が取られることを雇用契約に定めることは、特に問題はありません。
× **エ** 情報セキュリティ管理基準では、「4.1.3 従業員は、雇用条件の一部として、機密保持契約書又は守秘義務契約書に署名すること」と規定しています。よって、定められた内容の守秘義務契約書に署名することを雇用契約に定めることは、特に問題はありません。

問44 内部統制

内部統制とは、組織が目的を達成するために、従業員などを適切に管理して自社の業務を適正に遂行しているかどうかを、合理的な方法で確認するための体制を構築・運用する仕組み(マネジメントシステム)、及びその仕組みにおいて行われる各種の作業(マネジメントプロセス)のことです。

内部統制によって不正などを検知するためには、ある従業員または部門が行った作業を、別の従業員または部門に検証させて作業の内容の正当性を確認させるなど、作者者と検証者とを分離する措置をとることが必要となります。

よって、解答群**ア**のように、売掛金回収条件の設定などは、売掛金を回収する部門(営業部門)ではなく、別の部門(審査部門など)に行わせるべきです。売掛金回収条件の設定を営業部門に任せると、本来は回収していない売掛金を回収したように見せかけることができるような不正な条件が営業部門によって設定され、営業部門が回収できなかった売掛金が、回収されたように粉飾されてしまう危険性があります。

解答群**イ**～**エ**については、各作業の作業(営業部門)がチェックも行っているため、不適切となります。

○ 解答 ○

問 42 **ウ**

問 43 **ア**

問 44 **ア**



問 45 エンタープライズアーキテクチャにおいて、業務と情報システムの理想を表すモデルはどれか。

- ☐ ア EA 参照モデル ☐ イ To-Beモデル ☐ ウ ザックマンモデル ☐ エ データモデル



問 46 IT投資効果の評価に用いられる手法のうち、ROIによるものはどれか。

- ☐ ア 一定期間のキャッシュフローを、時間的変化に割引率を設定して現在価値に換算した上で、キャッシュフローの合計値を求め、その大小で評価する。
- ☐ イ キャッシュフロー上で初年度の投資によるキャッシュアウトフローが何年後に回収できるかによって評価する。
- ☐ ウ 金銭価値の時間的変化を考慮して、現在価値に換算されたキャッシュフローの一定期間の合計値がゼロとなるような割引率を求め、その大小で評価する。
- ☐ エ 投資額を分母に、投資による収益を分子とした比率を算出し、投資に値するかどうかを評価する。



問 47 業務要件定義において、業務フローを記述する際に、処理の分岐や並行処理、処理の同期などを表現できる図はどれか。

- ☐ ア アクティビティ図 ☐ イ クラス図 ☐ ウ 状態遷移図 ☐ エ ユースケース図

解説

問45 エンタープライズアーキテクチャ

エンタープライズアーキテクチャ(Enterprise Architecture, EA)とは、組織の業務や情報システムを、政策・業務体系(ビジネスアーキテクチャ)、データ体系(データアーキテクチャ)、適用処理体系(アプリケーションアーキテクチャ)及び技術体系(テクノロジーアーキテクチャ)という4つの統合的な手法でモデル化して分析することで、業務や情報システムの最適化などを進めたり、全体最適化の観点から業務の問題点などを見直して改善を行ったりする技法のことです。

EAでは、現状の業務をモデル化するとともに、情報システムを導入することによって現状の業務の改善を行った結果としての理想のモデルを導き出して、現状と理想との比較を行うことがあります。現状の業務をモデル化したものを“**As-Isモデル**”，理想のモデルを“**To-Beモデル**”といいます。よって、**イ**が正解です。

× **ア** **EA参照モデル**とは、エンタープライズアーキテクチャを構築する際に用いられる業務プロセスやデータ形式などの雛形のことです。EA参照モデルには、業績測定参照モデル、政策・業務参照モデル、データ参照モデル、サービスコンポーネント参照モデル、技術参照モデルの五つがあります。

○ **イ** 正解です。

× **ウ** EAによって業務分析を行い、業務内容を分類・体系化するための枠組みとして、**ザックマンフレームワーク**が知られています。ザックマンフレームワークでは、業務に関係する株主・幹部社員・プログラマなどの各種の従業者の視点を縦軸にとり、5W1H(What, How, Where, Who, When, Why)を横軸にとった形式のマトリックス図を用いて、現状の業務内容などを従業者の視点別及び5W1H別に分類しています。このフレームワークに関連する業務モデルが、**ザックマンモデル**となります。

- × **エ** データモデルとは、データとデータ間の関連などをモデル化すること、及びその方法でデータなどをモデル化して表現したもののことです。

問46 ROI

ROI (Return On Investment, 投資利益率または投資回収率)とは、事業への投資によって得られた利益が、投資額に占める割合を指します。ROIは、情報戦略の投資対効果を評価する際に用いられます。ROIが高いほど、投資に対して得られた利益が大きくなり、投資対効果が大きくなります。

ROIは、次の式で求められます。

$$\text{ROI} = \frac{\text{投資による収益}}{\text{投資額}} \times 100 (\%)$$

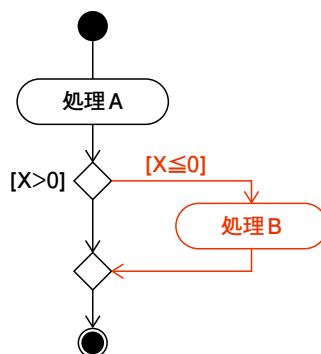
- × **ア** 正味現在価値法の説明です。
 × **イ** 回収期間法の説明です。
 × **ウ** 内部利益率法の説明です。
 ○ **エ** 正解です。

問47 業務要件定義

業務要件定義において用いられるアクティビティ図とは、処理の流れを具体的に明記するために用いられる図で、従来のシステム設計にて多用される、フローチャートに似た構成になっています。

アクティビティ図では、矢印を用いて処理の流れを示します。角丸四角形の記号は実行する処理を、ひし形の記号は条件分岐を示します。処理は黒丸印の記号から開始し、二重線黒丸の記号に到達することで終了します。アクティビティ図では、単独の処理の流れの他に、複数のプロセスの並行処理を記述することも可能です。

右図は、簡単なアクティビティ図の例です。この図では、開始後に「処理A」という処理が実行され、その直後にXの値によって条件分岐が実行されます。Xの値が0以下であれば処理Bが実行され、終了します。Xが0より大きければ、処理Bが実行されないままですでに終了します。



アクティビティ図は、ビジネスプロセスにおける各種の処理の流れを記述することができ、また、複数のプロセスが並行して動作するときの処理(並行処理)を表現できるという特徴があります。

- **ア** 正解です。
 × **イ** クラス図は、クラス間の相互関係などを表現できる図です。
 × **ウ** 状態遷移図は、システムの状態と別の状態への遷移条件を表現できる図です。
 × **エ** ユースケース図は、システムが利用者などに提供する機能を表現できる図です。

○ 解答 ○

問 45 **イ**

問 46 **エ**

問 47 **ア**

問48 情報システムの調達の際に作成されるRFIの説明はどれか。

- ア 調達者から供給者候補に対して、システム化の目的や業務内容などを示し、情報の提供を依頼すること
- イ 調達者から供給者候補に対して、対象システムや調達条件などを示し、提案書の提出を依頼すること
- ウ 調達者から供給者に対して、契約内容で取り決めた内容に関して、変更を要請すること
- エ 調達者から供給者に対して、双方の役割分担などを確認し、契約の締結を要請すること

問49 分析対象としている問題に数多くの要因が関係し、それらが相互に絡み合っているとき、原因と結果、目的と手段といった関係を追及していくことによって、因果関係を明らかにし、解決の糸口をつかむための図はどれか。

- ア アローダイアグラム イ パレート図 ウ マトリックス図 エ 連関図

問50 最大利益が見込める新製品の設定価格はどれか。ここで、いずれの場合にも、次の費用が発生するものとする。

固定費：1,000,000円

変動費：600円／個

設定価格（円）	予測需要（個）
1,000	80,000
1,200	70,000
1,400	60,000
1,600	50,000

- ア 1,000 イ 1,200 ウ 1,400 エ 1,600

解説

問48 RFI

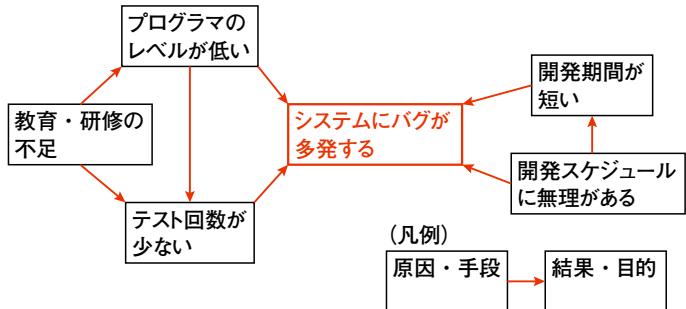
RFI (Request For Information, 情報提供依頼書)とは、調達しようとする情報システムの機能などを調達者が理解するために、供給者候補に対して情報の提供を要請するための文書です。RFIで提供を依頼する情報は、現在の状況において利用可能な技術や製品、及び供給者が同種のシステムを開発した実績などです。

- ア 正解です。
- × イ RFP (Request For Proposal, 提案依頼書)の説明です。
- × ウ RFC (Request For Change, 変更要求書)の説明です。
- × エ SOW (Statement Of Work, 作業範囲記述書)の説明です。

問49 因果関係の分析

分析対象とする問題の要因について、それらの原因と結果、目的と手段が複雑に絡み合っているときに、その関係を図示することで因果関係を明らかにし、理解の助けとするための図法に、新QC七つ道具の一つである**連関図**があります。

<連関図の例>



- × **ア** **アローダイアグラム**は、作業を矢印、作業の開始点や終了点を丸印で表す図で、スケジュールの日数やクリティカルパスを求めるために用いられます。
- × **イ** **パレート図**は、折れ線グラフと棒グラフを組み合わせた図で、複数の項目の中から重要な項目を見いだすために用いられます。
- × **ウ** **マトリックス図**は、行と列をもつ図で、PPM分析などで用いられます。
- **エ** 正解です。

問50 価格設定

各設定価格における利益を求めます。

ア 設定価格=1,000円

売上高=80,000(個)×1,000(円/個)=80,000,000円
 変動費=80,000(個)×600(円/個)=48,000,000円
 固定費=1,000,000円
 利益=80,000,000-48,000,000-1,000,000=31,000,000円

イ 設定価格=1,200円

売上高=70,000(個)×1,200(円/個)=84,000,000円
 変動費=70,000(個)×600(円/個)=42,000,000円
 固定費=1,000,000円
 利益=84,000,000-42,000,000-1,000,000=41,000,000円

ウ 設定価格=1,400円

売上高=60,000(個)×1,400(円/個)=84,000,000円
 変動費=60,000(個)×600(円/個)=36,000,000円
 固定費=1,000,000円
 利益=84,000,000-36,000,000-1,000,000=47,000,000円

エ 設定価格=1,600円

売上高=50,000(個)×1,600(円/個)=80,000,000円
 変動費=50,000(個)×600(円/個)=30,000,000円
 固定費=1,000,000円
 利益=80,000,000-30,000,000-1,000,000=49,000,000円
 以上から、**エ**の利益が最大になります。

○ 解答 ○

問 48 **ア**

問 49 **エ**

問 50 **エ**

第③回 模擬試験 午後 問題

問 1 Webアプリケーションのセキュリティ対策に関する次の記述を読んで、設問1～4に答えよ。

W社は、インターネット上で日用雑貨品の会員制通信販売システムを運営する会社である。この通信販売システム(以下、本システムという)は、商品検索、注文、会員管理、会員掲示板などの機能を提供する。本システムの機能を利用するには、あらかじめ会員管理機能を使って、会員登録しなければならない。図1は、会員掲示板機能を使った会員掲示板画面の例である。

Figure 1 shows two examples of the Member Bulletin Board screen. The top panel, labeled 'No.20', contains the following information: Date (日付) 2011-xx-xx, Name (氏名) O川O子, ID: xxxxxxxx, and a Subject (件名) field. Below the subject field are two buttons: '登録' (Register) and 'キャンセル' (Cancel). The bottom panel, labeled 'No.19', contains the following information: Date (日付) 2011-xx-xx, Name (氏名) O山O男, ID: yyyyyyyy, and a Subject (件名) field with the text 'Re: OOについて' followed by a row of 16 circles.

図1 会員掲示板画面の例

ある日、会員情報が知らぬ間に書き換わっていたり、覚えの無い商品が届いたりしたとのクレームが複数の会員から寄せられた。情報システム部門で本システムを調べたところ、クレームに該当する登録情報の変更処理や商品の注文処理が確認された。

情報システム部門の責任者であるA部長は、セキュリティ事故が発生したと判断して、本システムの利用を直ちに停止し、外部のセキュリティ専門会社の支援を受けながら対策をとることを指示した。

後日、外部のセキュリティ専門会社から、今回のセキュリティ事故に関する調査報告書が届けられた。調査報告書に記載された内容は、次のとおりである。

〔セキュリティ事故の経過〕

- (1) 会員Xは、本システムのトップ画面から、会員ログインページへのボタンを押した。
- (2) 本システムは、ログイン画面を表示した。
- (3) 会員Xは、ログイン画面で、自身のアカウント名とパスワードを入力した。
- (4) 本システムは、アカウント名とパスワードを確認して、セッションIDを発行し、cookieを利用して会員のブラウザに戻した。
- (5) 会員Xは、会員メニュー画面で、会員掲示板機能を選択した。
- (6) 本システムは、会員掲示板画面を表示した。
- (7) 会員Xが、特定の会員掲示板ページを参照したときに、悪意のあるコードが自動的に実行され、会員Xの登録情報を書き換える処理と、注文処理が行われた。

〔想定される原因〕

- (1) 会員掲示板ページを出力する処理に問題があり、この問題を悪用した<script>タグを用いた悪意のあるコードが、会員掲示板ページに埋め込まれた形跡があった。
- (2) ログインした会員が、この悪意のあるコードが埋め込まれた会員掲示板ページを参照すると、そのコードが自動的に実行され、会員の登録情報を書き換える処理や特定の商品の注文処理が行われるようになっていた。

〔原因から想定される脅威〕

- (1) 登録情報や会員掲示板情報に対して、ログインした会員が予期しない処理を勝手に実行させられることによって起こる情報の改ざん
- (2) ログインした会員が予期しない注文処理を勝手に実行させられることによって起こるサービスの悪用

〔対策の提言〕

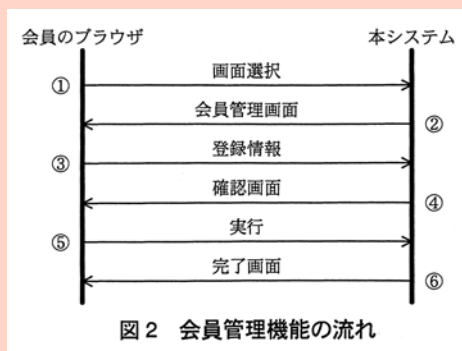
- (1) 入力された文字列は、そのままではなく、エスケープ処理を適切に施してからブラウザに表示する。入力データに“<”、“>”、“&”などのHTMLの特別な記号文字が存在した場合、その記号文字が有する特別な働きを無効にする文字や文字列に置き換える。例えば、“>”は“>”、“<”は“<”、“&”は“&”とする。これによって、タグの文字列“<script>”は、文字列“<script>”に置き換わる。
- (2) 特に、会員情報の登録処理や注文処理のような重要な処理を実行するページには、 メソッドでアクセスするようにし、そのhiddenパラメタに秘密情報（ページトークン）が挿入されるように、前のページを自動生成する。実行ページでは、その値が正しい場合だけ処理を行う。もし メソッドの代わりに メソッドでアクセスすると、秘密情報をURLに付加して送信することになるので、ここでは利用を避けるべきである。また、HTMLフォームで <form> タグを用いる場合、メソッド属性の指定を省略すると メソッドと解釈されるので、適切に指定する必要がある。

今回のように、ログインした会員だけが、予期しない処理を実行させられてしまうセキュリティ攻撃は、クロスサイトリクエストフォージェリーと呼ばれている。

この攻撃が成功する主たる要因は、会員の正しい要求と悪意のあるコードの要求を区別できないことである。

この後、A部長は、外部のセキュリティ専門会社の提言に従い、今回のセキュリティ攻撃の根本的な原因を解消すべく、本システムの改善を行うことにした。

提言された対策(1)を本システムの全てのプログラムに適用し、その上で重要な処理を行う注文機能と会員管理機能に対して、提言された対策(2)を適用した。会員登録時における本システムと会員のブラウザとの間の情報の流れは、図2のとおりである。



設問 1 本文中の a , b に入れる適切な字句を解答群の中から選び、記号で答えよ。

解答群

- | | | | |
|---|---|--|--|
| ア GET | イ HEAD | ウ OPTION | エ POST |
| オ PUT | カ RESET | | |

設問 2 [対策の提言](1)について、今回の場合、<script> タグを用いたコードにエスケープ処理を適切に施す目的は何か。解答群の中から選び、記号で答えよ。

解答群

- | |
|--|
| ア hidden パラメタに秘密情報を挿入するため |
| イ 悪意のあるコードを実行させないため |
| ウ セッションIDをcookieに保存するため |
| エ ブラウザと本システム間の通信全体を暗号化するため |

設問 3 図2において、秘密情報(ページトークン)を送受信する適切な箇所の組合せを解答群の中から選び、記号で答えよ。

解答群

- | | | | |
|---|---|--|--|
| ア ①, ②, ③ | イ ②, ③, ④ | ウ ③, ④ | エ ④, ⑤ |
| オ ⑤ | カ ⑤, ⑥ | | |

設問 4 今回のセキュリティ攻撃を防ぐ対策として[対策の提言](1), (2)を実施した上で、この攻撃を検出する対策をとることにした。この攻撃を検出するために有効な対策として適切なものを解答群の中から選び、記号で答えよ。

解答群

- | |
|---|
| ア 悪意のあるコードを埋め込まれた特定の会員掲示板ページを直ちに削除する。 |
| イ 会員情報の登録や変更、注文処理などの重要な処理を行うページでは、HTTPSによって、途中経路を暗号化する。 |
| ウ 会員情報の登録や変更、注文処理などの重要な処理については、必ずログを記録する。 |
| エ 本システムで利用するセッションIDとして会員ごとに一意の固定値を割り当て、常にそれを利用する。 |

解説

Webアプリケーションのセキュリティ対策を主題としています。

設問の解説に入る前に【クロスサイトリクエストフォージェリー】【HTTPのメソッド】について解説します。

【クロスサイトリクエストフォージェリー】

悪意のあるスクリプトを埋め込んだWebページのリンクを利用者にクリックさせるなどの方法で、Webサイト上で利用者が意図しない操作を行わせる攻撃のことを、クロスサイトリクエストフォージェリー(Cross Site Request Forgeries, 以下CSRFとする)といいます。

本問の本システムでは、次のような方法でCSRFが実行されています。

- ① 会員掲示板ページを出力する処理に問題があり、<script>タグを用いた悪意のあるコードを、会員掲示板ページに埋め込むことが可能だった。
- ② ①の脆弱性に気付いた悪意のある会員が、<script>タグを用いた悪意のあるコードを含む文字列を、会員掲示板の特定のページに書き込んだ。このコードには、会員が当該ページをブラウザで開くと、本システムに密かにアクセスしてその会員の登録情報を書き換える処理と、特定の商品の注文処理を行う処理

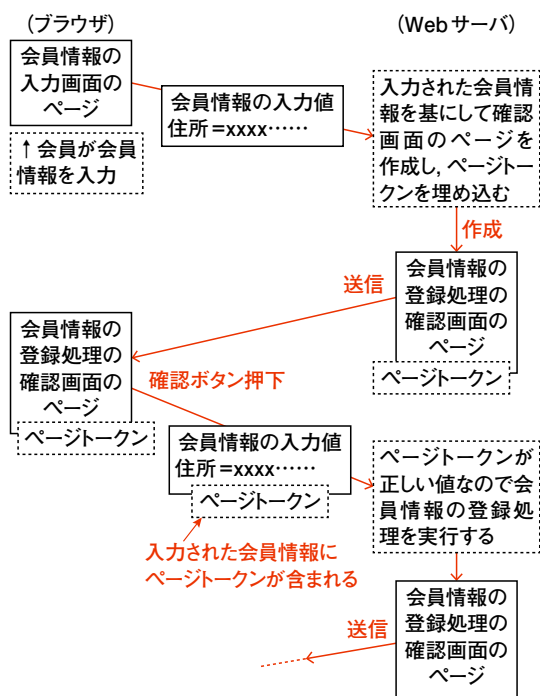
が実装されていた。

- ③ ②の後に別の会員が当該ページを参照したため、悪意のあるコードがその会員のブラウザ上で実行され、登録情報の書換えや特定の商品の注文がその会員の知らないうちに行われた。

● CSRFを防止する方法

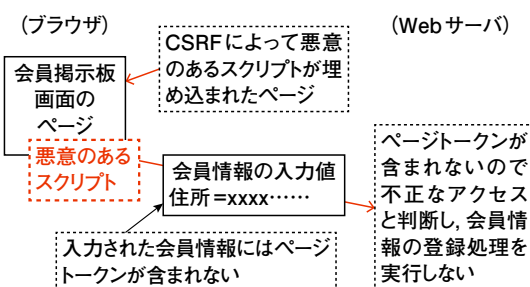
会員情報の登録処理などの重要な処理を行うためのページにアクセスして処理を実行する際には、その前のページに秘密情報(ページトークン)を埋め込んでおき、正しい値のページトークンが埋め込まれたページからアクセスされたときだけ、処理を行うのが適切です。

<正しい処理>



上の図では、会員情報の登録処理を実行する前に開かれる、会員情報の登録処理の確認画面のページがWebサーバ上で作成され、会員のブラウザに送信されています。このページには、Webサーバが作成した秘密情報であるページトークンが含まれます。このページの内容を確認した利用者が確認ボタンを押すと、ページ中の会員情報の入力値などとともに、ページトークンが含まれた入力データがWebサーバに送られます。送信されてきたデータに含まれているページトークンが正しい値なので、Webサーバは会員情報の登録処理を実行し、その結果である会員情報の登録処理の完了画面をブラウザに送信します。

<CSRFによる不正な処理>



CSRFが実行された場合、CSRFによって悪意のあるスクリプトが埋め込まれた会員掲示板画面のページなどが利用者のブラウザ上で表示されます。この悪意のあるスクリプトが、利用者の意図しない方法でWebサーバに会員情報の入力値などを送信し、Webサーバ上で会員情報の登録処理を実行させようとしたときは、送信されたデータにページトークンが含まれないので、Webサーバは会員情報の登録処理を実行しません。

【HTTPのメソッド】

Web販売システムなどでは、Webページの入力欄から利用者の住所などを入力して、商品の購入を行うことがあります。この入力欄は、次のようなHTMLのタグで構成されます。

<HTMLのタグ>

```
...
<form action="http://...../buy.cgi" .....
method="POST">
    住所:<input type="text" .....
    name="zyuusyo">
</form>
...
```

form要素は、複数の入力欄などをまとめた入力フォームを表す要素です。input要素は、文字列の入力欄やラジオボタンなどの、値を入力する項目を表す要素です。form要素のmethod属性は、入力された値をWebサーバ上のCGIプログラムに渡すときに使用する、HTTPのメソッドを指定するために用いられます。メソッドとは、ブラウザがWebサーバなどに問合せやデータを送信するときに用いられる方法のことです。

method属性を「method="POST"」とした場合はPOSTメソッドが、「method="GET"」とした場合はGETメソッドが用いられます。

● GETメソッド

Webページの入力欄に入力した情報をGETメソッド

で送信すると、Webページにアクセスするときに指定されたURLのクエリストリングに、入力した情報が記載されます。その例を示します。

http://…….co.jp/search?q=%E6%83%85%E5%A0%B1%E5%87%A6%E7%90%86+JITEC& (以下略)
(クエリストリング)

このURLは、ある検索エンジンの検索語句入力欄に、“情報処理 JITEC”という語句を入力して検索を行ったときに、ブラウザのアドレス欄に表示されたものです。URLの“?”記号よりも後の部分がクエリストリングです。クエリストリング中の“q=%E6%83%85%E5%A0%B1%E5%87%A6%E7%90%86+JITEC”という部分は、日本語の語句である“情報処理”をエンコードした文字列“%E6%83%85%E5%A0%B1%E5%87%A6%E7%90%86”と、英字のみで構成される語句“JITEC”の文字列を示しています。

GETメソッドを利用すると、利用者が入力した住所などの文字列がクエリストリングに記載されてしまいます。クエリストリングの内容は他人から容易に参照されます。前述のページトークンなども、GETメソッドを利用するとクエリストリングに記載されます。したがって、攻撃者はクエリストリング中のページトークンを盗み、CSRFで作成した悪意のあるスクリプトを埋め込んだページにページトークンも一緒に埋め込むことで、CSRFの攻撃を成功させることができます。

● POSTメソッド

Webページの入力欄に入力した情報をPOSTメソッドで送信すると、クエリストリングには入力した情報が記載されなくなり、代わりに利用者が送信したHTTPリクエストのヘッダ部分に情報が記載されます。この部分の情報を他人が参照するのは困難なため、攻撃者がページトークンを盗むことは難しくなります。会員情報の登録処理などの重要な処理を実行するページにはPOSTメソッドでアクセスするようにして、利用者が送信したページトークンを盗まれないようにします。

設問 1 HTTPのメソッド

空欄 a, b

【クロスサイトリクエストフォージェリー】及び【HTTPのメソッド】の解説から、会員情報の登録処理などの重要な処理を実行するページには“POST”メソッドでアクセスするようにします。もしPOSTメソッドの代わりに“GET”メソッドでアクセスすると、URLのクエリストリン

グにページトークンが含まれてしまうので、利用してはいけません。

以上から、空欄aには **イ**、空欄bには **ア**が入ります。

- × **イ** HEADメソッドは、Webサーバに対してHTTPのヘッダ部分だけを返し、ボディ部分(Webページ本体の部分)を返さないように依頼するメソッドです。
- × **ウ**, **カ** HTTPには、OPTIONメソッドやRESETメソッドは存在しません。
- × **オ** PUTメソッドは、ブラウザからファイルを送信してWebサーバ上に保存させるためのメソッドです。

設問 2 HTMLのエスケープ

<script>タグを用いたコードにエスケープ処理を施すと、HTMLにおいてタグを構成するための文字である“<”や“>”が別の文字に変換されるので、ブラウザは当該コードの部分の文字列を、HTMLのタグやスクリプトではなくただの文字列と判断し、そのまま表示する処理だけを行います。そのため、<script>タグが無効になるので悪意のあるコードが実行されなくなり、CSRFを防ぐことができます。

以上から、“悪意のあるコードを実行させないため” **イ** が正解です。

- × **ア** <script>タグの内容は、hiddenパラメタの内容とは関係がありません。
- × **ウ** セッションIDを保存するcookieは、HTMLのタグ内ではなくHTTPヘッダ内に存在します。
- × **エ** “<”や“>”だけを別の文字に変換しても、他の文字は特に変換せずそのままにしているので、通信全体が暗号化されることはありません。

設問 3 ページトークンの送信

図2から、会員情報の登録が実際に実行されるのは⑤の「実行」です。その前の③の「登録情報」では、会員情報を登録するための入力データが本システムに送信されますが、本システムは④「確認画面」を会員のブラウザに送信し、入力した情報が正しいかどうかを会員に確認させています。③の「登録情報」の時点では、会員情報の登録はまだ行われていません。よって、⑤の「実行」の直前の、④の「確認画面」にページトークンを埋め込んで本システムから会員のブラウザに送信し、⑤でペー

ジトークンを含むデータを会員のブラウザから本システムに送信させることで、前述の対策(2)の措置を行っていると分かります。したがって、秘密情報(ページトークン)を送受信する箇所は“④、⑤”(エ)です。

設問4 セキュリティ攻撃の検出

本問のCSRFに限らず、システムに対する攻撃を検出するためには、システムの入力や出力のログを記録し、ログの内容を定期的にチェックすることで不正なアクセスなどの有無を確認することが適切です。よって、ウが正解です。

× ア この対策は、CSRFによって悪意のあるコードが埋め込まれたページを削除しているの、CSRFが行われた後の回復措置です。CSRFの検出ではありません。

× イ HTTPSで途中経路を暗号化することで、利用者のブラウザと本システムとの間の通信内容を攻撃者が盗聴することは防止できますが、会員情報の登録などの処理が不正に実行されるのを防ぐことはできません。

× エ セッションIDとして会員ごとに一意の固定値を割り当てると、各会員が使用するセッションIDを攻撃者が容易に特定できるようになり、そのセッションIDの値を悪用して他人になりますますことができるため、問題があります。

解答

設問1 a:エ b:ア

設問2 イ 設問3 エ 設問4 ウ

問2

ネットワークやWebアプリケーションプログラムのセキュリティに関する次の記述を読んで、設問1～3に答えよ。

X社は、中堅の機械部品メーカーである。X社では、部品製造に関わる特許情報や顧客情報を取り扱うので、社内のネットワークセキュリティを強化している。社内のネットワークの内部セグメントには、内部メールサーバ、内部Webサーバ、ファイルサーバなど社内業務を支援する各種サーバが配置されている。また、DMZには、インターネット向けのメール転送サーバ、DNSサーバ、Webサーバ、プロキシサーバが配置されている。Webサーバでは、製品情報や特定顧客向けの部品情報の検索システムを社外に提供しており、内部Webサーバやファイルサーバでは、特許情報や顧客情報の検索システムを社内に提供している。X社のネットワーク構成を図1に示す。

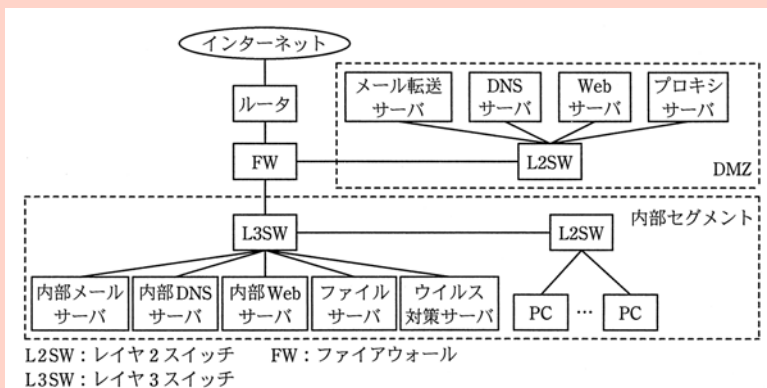


図1 X社のネットワーク構成

先日、同業他社の社外向けWebサイトが外部からの攻撃を受けるというセキュリティインシデントが発生したことを聞いた情報システム部のY部長は、特にFWに関するネットワークセキュリティの強化を検討するように部下のZさんに指示した。

X社の社内ネットワークのセキュリティ要件を図2に示す。

1. 共通事項
 - 1.1 社内の通信機器やサーバがインターネットと通信する場合には、FWなどの装置を用いてアクセス制御を行うこと。
 - 1.2 業務上必要がない通信は全て禁止すること。
 - 1.3 インターネットに公開する社内のサーバは必要最小限にとどめること。
2. Web
 - 2.1 社内のPCから社外WebサイトへのHTTP通信（HTTPSを含む。以下同じ）は、プロキシサーバ経由で行うこと。
 - 2.2 社外から社内へのHTTP通信は、インターネットからWebサーバへのHTTP通信だけを許可すること。
 - 2.3 Webアプリケーションプログラムの脆弱性を悪用した攻撃を防ぐために、インターネットからWebサーバにアクセスする通信は、あらかじめ定められた一連の手続のHTTP通信だけを許可すること。
3. 電子メール
 - 3.1 社内のPC間のメール通信は、内部メールサーバを介して行うこと。
 - 3.2 内部セグメントとDMZの間のメール通信は、内部メールサーバとメール転送サーバの間だけを許可すること。
 - 3.3 社内と社外の間のメール通信は、メール転送サーバとインターネットの間だけを許可すること。
4. DNS
(以下省略)

図2 X社の社内ネットワークのセキュリティ要件（抜粋）

Zさんは、FWによるIPアドレスやポート番号を用いたパケットフィルタリングだけでは外部からの攻撃を十分に防ぐことができないと考えた。そこで、より高度なセキュリティ製品の追加導入を検討するために、IDS、IPSやWAFの基本的な機能について調査した。調査の結果、IDSは、X社の外部からの ことができ、IPSは、X社の外部からの ことができ、一方、WAFは、 ことができるということが分かった。

この結果から、Zさんは、次の二つの案を考えた。

案1：社内ネットワークのルータとFWの間にネットワーク型のIPSを導入する。

案2：セキュリティ強化の対象とするサーバにWAFを導入する。

今回、 を目的とする場合には案1を、 を目的とする場合には案2を選択することがそれぞれ有効であると分かった。

特に案2のWAFは、ブラックリストやホワイトリストの情報を有効に活用することで、社内ネットワークのセキュリティ要件2.3を満たすことができる。

Zさんは、それぞれの案について、費用面や運用面での課題の比較検討も行い、結果を取りまとめてY部長に報告した。これを受けてY部長は、案2を採用することを決め、具体的な実施策を検討するようにZさんに指示した。

設問 1 本文中の下線において、FWでは防げない攻撃を解答群の中から全て選び、記号で答えよ。

解答群

- ア** DNSサーバを狙った、外部からの不正アクセス攻撃
- イ** WebサーバのWebアプリケーションプログラムの脆弱性を悪用した攻撃
- ウ** 内部Webサーバを狙った、外部からの不正アクセス攻撃
- エ** ファイルサーバを狙った、外部からの不正アクセス攻撃
- オ** プロキシサーバを狙った、外部からのポートスキャンを悪用した攻撃

設問 2 本文中の a ～ c に入れる最も適切な字句を解答群の中から選び、記号で答えよ。

解答群

- ア** IPパケットの中身を暗号化して盗聴や改ざんを防止する
- イ** IPパケットの中身を調べて不正な挙動を検出し遮断する
- ウ** IPパケットの中身を調べて不正な挙動を検出する
- エ** Webアプリケーションプログラムとのやり取りに特化した監視や防御をする
- オ** Webアプリケーションプログラムとのやり取りを暗号化して盗聴や改ざんを防止する
- カ** 電子メールに対してウイルスチェックを行う

設問 3 本文中の d , e に入れる最も適切な字句を解答群の中から選び、記号で答えよ。

解答群

- ア** PCに対するウイルス感染チェック
- イ** WebサーバのWebアプリケーションプログラムの脆弱性を悪用した攻撃の検出や防御
- ウ** 外部からの不正アクセス攻撃の検出や防御をX社の社内ネットワーク全体に対して行うこと
- エ** 内部からの不正アクセス攻撃の検出や防御をX社の社内ネットワーク全体に対して行うこと
- オ** 内部メールサーバに対する不正アクセス攻撃の検出や防御

解説

ネットワークセキュリティを題材として、IDSやIPSなどの各種技術への知識や理解を問う問題です。

設問の解説に入る前に【IDSとIPS】【WAF (Web Application Firewall)】について解説します。

【IDSとIPS】

● IDS (Intrusion Detection System, 侵入検知システム)

外部から社内ネットワークに対して行われる不正侵入などの攻撃を検出し、管理者に警告を発するシステムです。検出や警告を行うだけで、攻撃の防止はしません。外部から送信されてきたIPアドレスの、ヘッダ部分だけでなくボディ部分に格納されているデータ(中身)を調

べて、不正な挙動の原因となる文字列などがあるかどうかを検査します。

● IPS (Intrusion Protection System, 侵入防止(防御)システム)

IDSの機能をもつとともに、攻撃を検知するとファイアウォールに指示を送信して攻撃元からのアクセスを遮断したり、サーバを停止させたりすることで、攻撃を防御するシステムです。IDSと同様に、外部から送信されてきたIPアドレスのボディ部分のデータを調べます。

● IDS, IPSの侵入検知方法

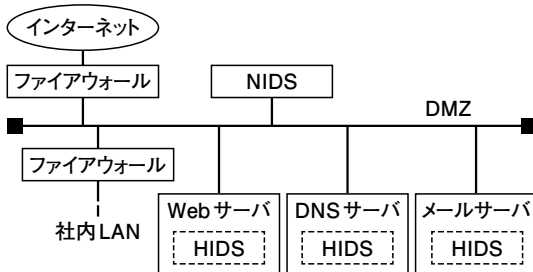
IDSやIPSが攻撃用のパケットを検知する方法を次の表に示します。

| 名称 | 特徴 |
|--------|---|
| シグネチャ型 | シグネチャを用いて攻撃パケットの検知を行う方法。
・シグネチャ…侵入検知用のルールや、攻撃パケットに含まれるパターンを記録しているファイル
【デメリット】シグネチャに記録されていない新種の攻撃手法は検知できない |
| アノマリ型 | 通常時と比較して大量のパケットが送受信されるなど、異常な挙動があったときに攻撃が発生したとみなす方法。
【メリット】新種の攻撃手法を検知できることがある
【デメリット】通常の業務において大量のデータを送受信したときに、攻撃がなくても攻撃されたとみなす可能性がある |

● IDSなどの形式

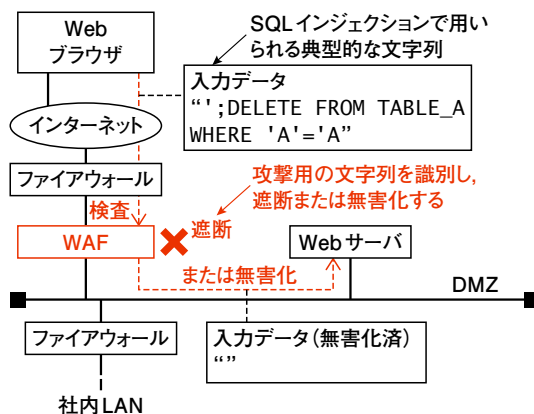
IDSなどは、設置場所によって次の二つの形式に分類できます。

| 名称 | 特徴 |
|----------------|---|
| ネットワーク型 (NIDS) | 社内LANなどのネットワークに設置される。
ネットワーク全体に対する攻撃を検知できる。 |
| ホスト型 (HIDS) | サーバなどの機器にインストールされる。
その機器だけに対する攻撃を検知できる。 |



【WAF (Web Application Firewall)】

WAFは、Webサーバ上で稼働するWebアプリケーションプログラムと、Webブラウザとの間でやり取りされるデータの内容を監視して、Webアプリケーションプログラムの脆弱性を突く攻撃(SQLインジェクションなど)を防御するために用いられる、特別なファイアウォールです。



● ホワイトリスト

正常系のルール(正常なアクセス対象だけをリストに登録するルール)に従って、社内のサーバなどにアクセスしてもよい正常な送信元のIPアドレスや、適切なアクセス手順などを登録したリストのことです。ホワイトリストを用いているWAFでは、ホワイトリストに掲載されていない送信元からのアクセスを禁止し、掲載されている送信元からのアクセスだけを許可します。また、ホワイトリストに掲載されているアクセス手順に従ったアクセスだけを許可し、他のアクセスを禁止します。

● ブラックリスト

社内のサーバなどにアクセスしてはならない不正な送信元のIPアドレスや、不適切なアクセス手順などを登録したリストのことです。

設問 1 FWで防げない攻撃

各解答群の攻撃がFWで防げるかどうかを検証します。

● ア

DNSサーバは「インターネット向け」なので、インターネットからのX社のドメイン名などの問合せを受け付けています。よって、インターネット上の任意の送信元IPアドレスから、DNSのポート番号(53)を宛先ポート番号とするアクセスは、FWによって通過を許可しなければなりません。インターネットからX社のDMZ上のDNSサーバに、通常のDNSのアクセスを装って、不正アクセスのパケットを送りつけるような攻撃が行われたとき、FWはそれを通過させてしまうので、この攻撃を防ぐことはできません。

● イ

Webサーバは「インターネット向け」なので、インターネットからX社のWebページをHTTPまたは

HTTPSで参照しようとするアクセスを受け付けています。よって、インターネット上の任意の送信元IPアドレスから、HTTPやHTTPSのポート番号(80, 443)を宛先ポート番号とするアクセスは、FWによって通過を許可しなければなりません。

インターネットからX社のDMZ上のWebサーバに、通常のHTTPなどのアクセスを装って、SQLインジェクションなどWebサーバのアプリケーションプログラムの脆弱性を悪用した攻撃用のパケットが送られたとき、FWはそれを通過させてしまいます。このパケットのボディ部分には攻撃用の不正な文字列などが格納されていますが、FWのパケットフィルタリング機能ではパケットのヘッダ部分のIPアドレスやポート番号だけを参照して通過の拒否または許可を判断し、ボディ部分は参照しないので、送られてきたパケットが攻撃用のものかどうかを判定することはできません。この攻撃を防ぐことはできません。

● **ウ, エ**

図2の1.~3.から、インターネット(社外)から社内へ向けて送られてくる通信のうち、FWで許可されるものは次のとおりです。他の通信は全てFWによって通過を拒否されます。

- ① インターネットからWebサーバへのHTTP通信(2.2)
- ② メール転送サーバとインターネットとの間のメール通信(3.3)

よって、インターネットから内部セグメントの内部Webサーバやファイルサーバへの通信は全てFWで拒否されるので、これらの攻撃はFWで防ぐことができます。

● **オ**

図2の2.1から、社内のPCから社外WebサイトへのHTTP通信は、プロキシサーバ経由で行われます。よって、プロキシサーバから社外WebサイトへのHTTP通

信はFWで許可されます。また、このHTTP通信の戻りパケットも、ダイナミックパケットフィルタリングによってFWで許可されます。その他のポート番号の通信はFWによって通過を拒否されるので、外部からプロキシサーバを狙ったポートスキャン用のパケットが送信されてきても、FWで防ぐことができます。

以上から、**ア, イ**の二つが正解です。

設問2 IDS, IPS, WAF

空欄 a, b

IDS及びIPSの解説から、IDSは不正な挙動の検出を行い、IPSは不正な挙動の検出と防御(遮断)を行うので、空欄aには**ウ**(IPパケットの中身を調べて不正な挙動を検出する)、bには**イ**(IPパケットの中身を調べて不正な挙動を検出し遮断する)が入ります。

空欄 c

WAFの解説から、WAFはWebアプリケーションプログラムとのやり取りに特化した監視や防御をするので、**エ**が正解です。

設問3 セグメントごとの対策

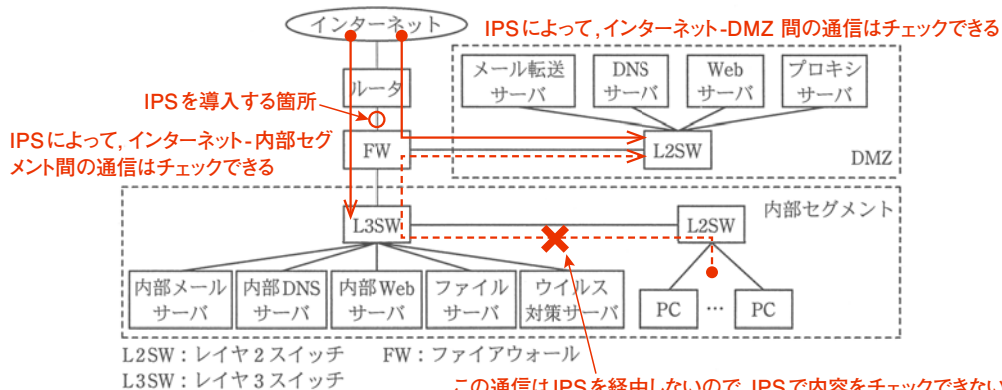
空欄 d

案1では、IPSをルータとFWの間に導入しているので、下の図に示す通信の内容を検証して、不正な挙動を検出し遮断することができます。

下の図から、外部からの不正アクセスの検出や防御を、DMZ及び内部セグメントに対して行えるので、**ウ**が正解です。

× **ア** PCに対するウイルス感染チェックは、IPSなどではなくウイルス対策プログラムが行います。

× **エ** 下の図から、内部からDMZ上のサーバに対す



る攻撃が行われても、その通信はIPSを経由しないので検出などはできません。

- × **オ** インターネットから内部メールサーバに対する不正アクセスは、FWで既に防止できています。内部セグメント上のPCなどから内部メールサーバに対する不正アクセスが行われても、IPSでは検出できません。

空欄 e

WAFを導入することで、Webアプリケーションプログラムとのやり取りに特化した監視や防御が可能になる

ので、“WebサーバのWebアプリケーションプログラムの脆弱性を悪用した攻撃の検出や防御”ができるようになります。**イ**が正解です。

° 解答 °

設問 1 **ア, イ**

設問 2 **a:ウ b:イ c:エ**

設問 3 **d:ウ e:イ**

問 3

ソーシャルネットワーキングサービスのセキュリティに関する次の記述を読んで、設問 1～3に答えよ。

P社は、ソーシャルネットワーキングサービスの運営会社である。P社のサービス(以下、P-SNSという)は、約30,000人の会員が利用している。PCやスマートフォンのWebブラウザから簡単に日記や写真を登録できることが人気で、会員数を伸ばしつつある。

〔P-SNSの利用方法〕

P-SNSの利用には、会員登録が必要である。利用を希望するユーザは、会員情報として希望するアカウント名とパスワード、電子メールアドレス、ニックネーム、プロフィール情報(氏名、誕生日、年齢、性別、居住地)を入力し会員登録を行う。会員登録をすると、P-SNS内にマイページが作成される。

会員登録後は、アカウント名とパスワードを用いてP-SNSにログインし、日記や写真を登録して、マイページを更新する。

P-SNSでは、マイページ内の日記や写真について、情報の公開範囲の設定が可能であり、P-SNS内に無制限に公開するか、特定の会員だけに公開するかを設定できる。ただし、日記や写真以外の情報については、公開範囲の設定ができず、P-SNS内に無制限に公開される。

日記と写真をP-SNS内に無制限に公開する設定にした場合、他の会員がPCのWebブラウザからアクセスしたときに見えるP-SNSのマイページのイメージを図1に示す。

| “ニックネーム”のページ | | | “アカウント名” | |
|--|----|----|-------------|--|
| 日記 | | | プロフィール | |
| XX月XX日
XXXXXXXXXXXXXX
XXXXXXXXXXXXXX | 写真 | 写真 | 氏名: XXXXXX | |
| | 写真 | 写真 | 誕生日: XX月XX日 | |
| XX月XX日
XXXXXXXXXXXXXX
XXXXXXXXXXXXXX | 写真 | 写真 | 年齢: XX歳 | |
| | 写真 | 写真 | 性別: XX | |
| | 写真 | 写真 | 居住地: XXX | |

注記 “ニックネーム”と“アカウント名”は、会員登録時に入力したニックネームとアカウント名に置き換えられる。

図1 P-SNSのマイページのイメージ

〔P-SNSのアカウント名とパスワードの設定ポリシー〕

P-SNSでは、アカウント名とパスワードの設定ポリシーを図2のように定めており、設定ポリシーを満たさないアカウント名とパスワードは設定できないように、会員登録時やパスワード変更時に入力チェックが行われる。

アカウント名の設定ポリシー

- ・アカウント名長は、6文字以上32文字以下
- ・利用可能な文字は、半角英数字
- ・他の会員と重複したアカウント名の設定は不可

パスワードの設定ポリシー

- ・パスワード長は、6文字以上32文字以下
- ・利用可能な文字は、半角英数字、記号文字
- ・英大文字、英小文字、数字のうち少なくとも2種を組み合わせた文字列

図2 アカウント名とパスワードの設定ポリシー

〔不正ログインの発覚〕

ある日、会員のQさんからP社に、“情報の公開範囲の設定が勝手に変更され、日記や写真が無制限に公開されている”とのクレームが入った。

そこで、P社カスタマサポート担当のR君が、Qさんのアカウントの利用状況調査を行うことになった。まず、R君がアクセスログからログイン状況を調査したところ、クレームの前日に、Qさんのアカウントでログインを試みるアクセスが100回あったことを確認した。そのうち、99回はパスワード誤りによってログインが拒否されており、最後の1回でログインが成功していた。また、Qさんへのヒアリングから、Qさん自身はこの日にログインしていないことが分かった。そこで、R君は、Qさんのアカウントが第三者による不正ログインに使用されたと判断し、Qさんのアカウントの利用を停止し、P-SNSの全会員に不正ログインの事件発生について注意喚起の案内を行った。

次にR君は、Qさんへのヒアリングから、設定されていたパスワードが氏名と誕生日を組み合わせた単純なものであったことが判明したので、今回の攻撃は **a** である可能性が高いと判断した。また、アカウント名とパスワードの組合せが第三者に知られたことから、**b** に備えて、P-SNSと同じパスワードを設定している他のサービスについてもパスワードを変更するように、Qさんにアドバイスした。

〔不正ログインに対する調査〕

R君は、Qさん以外の会員のアカウントに対する不正ログインについても調査を行った。その結果、Qさんの場合と同様の100回程度のログイン試行の記録が幾つか見つかった。

R君は、P-SNSのマイページには、①公開範囲の設定ができない情報の中にこれらの攻撃の足掛かりとなるものがあり、不正ログインにつながるリスクが高いと考えた。

〔不正ログイン対策の検討〕

R君は、不正ログイン対策として、次の三つの対策を検討した。

対策1：アカウント名とパスワードの設定ポリシーを見直して、悪意をもった第三者がP-SNSに不正ログインしにくくする。

対策2：パスワード誤りによってログインが一定の回数拒否された場合、アカウントの利用を自動的に停止する機能を追加する。

対策3：悪意をもった第三者がP-SNSに不正ログインできないように、アカウント名とパスワードによる認証に加え、Cookieによる認証を追加する。

対策3を採用した場合の、会員登録から初回ログインまでの手順を図3に示す。

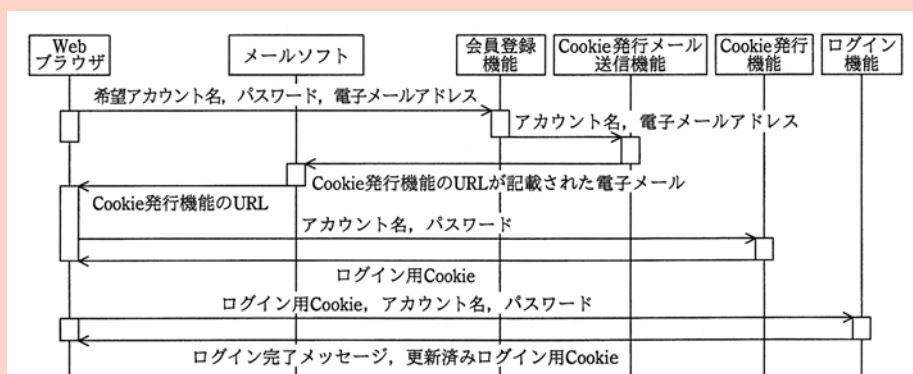


図3 対策3を採用した場合の会員登録から初回ログインまでの手順

ユーザがWebブラウザを用いて会員登録機能から会員登録を行うと、Cookie発行機能のURLが記載された電子メール（以下、メールという）がCookie発行メール送信機能から送信される。ユーザは、メールソフトを用いてメールを受信し、メール内に記載されたURLからCookie発行機能にWebブラウザを用いてアクセスする。ユーザがアカウント名とパスワードを入力し認証が完了すると、ログイン用Cookieが発行される。Cookie発行機能のURLは、登録した会員一人一人にメールを送信する都度、異なるものが発行され、メールの送信から1時間だけ有効である。また、発行されたログイン用Cookieの有効期間は半年間とし、ログインするたびに有効期間がその日から半年間に更新される。

会員がP-SNSにログインするときには、会員が入力するアカウント名とパスワードとともにログイン用Cookieがログイン機能へ送信される。ログイン機能では、送信されたログイン用Cookieがその会員に発行されたログイン用Cookieと異なる場合にはアクセスを拒否する。

会員が利用端末を変更したい場合やCookieの有効期間が過ぎた場合には、Cookie発行メール送信機能に対して、Cookie発行機能のURLが記載されたメールの送信を要求する。その後、会員登録時と同様にログイン用Cookieを入手する。

なお、P-SNSの通信は暗号化し、悪意をもった第三者が盗聴しても必要な情報を入手できないようにする。

その後R君は、アカウントへの不正ログインの足掛かりとなった情報を全会員のマイページから削除するとともに、Cookieによる認証機能の導入を行った。

設問 1 本文中の a , b に入れる適切な字句を解答群の中から選び、記号で答えよ。

aに関する解答群

- ア DoS攻撃
- ウ 標的型攻撃

- イ サイドチャネル攻撃
- エ 類推攻撃

bに関する解答群

- ア ゼロデイ攻撃
- ウ パスワードリスト攻撃

- イ 総当たり攻撃
- エ フィッシング攻撃

設問 2 本文中の下線①について、攻撃の足掛かりとなる情報とは何か。解答群の中から選び、記号で答えよ。

解答群

- | | |
|--------------------|-------------|
| ア アカウント名 | イ 写真 |
| ウ 電子メールアドレス | エ 日記 |

設問 3 〔不正ログイン対策の検討〕について、(1)～(3)に答えよ。

(1) 対策1について、Qさんのアカウントへの攻撃手法に対する対策として有効ではないものを、解答群の中から選び、記号で答えよ。

解答群

- | |
|---|
| ア 英和辞典にある英単語の利用禁止 |
| イ パスワード中に会員情報として登録した文字列を含めることの禁止 |
| ウ パスワードに記号文字を含めることの必須化 |
| エ 半年以上ログイン実績がないアカウントの利用停止 |

(2) アカウント名とパスワードによる認証がユーザを認証するのに対し、Cookieによる認証は何を認証するものか。解答群の中から選び、記号で答えよ。

解答群

- | | |
|------------------|------------------|
| ア Webサーバ | イ Webブラウザ |
| ウ 会員の利用端末 | エ メールソフト |

(3) 図3の手順を用いることで、会員登録時に入力した情報の有効性を確認できる。どの情報の有効性を確認できるか。解答群の中から選び、記号で答えよ。

解答群

- | | | | |
|--------------------|--------------|-------------|-------------|
| ア アカウント名 | イ 居住地 | ウ 氏名 | エ 性別 |
| オ 電子メールアドレス | カ 年齢 | | |

解説

ソーシャルネットワーキングサービス(以下、SNSという)へのログインに関する攻撃手法や、Cookieを用いた安全なログイン方法など、SNSに関するセキュリティ全般の知識を問う問題です。

設問の解説に入る前に【パスワードを推測しようとする攻撃】【Cookie】について解説します。

【パスワードを推測しようとする攻撃】

SNSにログインする際に用いたりするパスワードを推測しようとする攻撃には次のようなものがあります。

● 類推攻撃

パスワードを推測しようとする対象者の個人情報や嗜好などの文字列を入力する攻撃手法のことです。対象者

の氏名、アカウント名、生年月日、電話番号、趣味、好きな著名人などの文字列をパスワードとして入力します。

● ブルートフォース攻撃

考えられる全ての文字の組み合わせをパスワードとして入力していくことで、パスワードを推測する攻撃手法のことです。

● 辞書攻撃

英和辞典などの辞書に載っている一般的な単語や人名などをパスワードとして入力していくことで、パスワードを推測する攻撃手法のことです。

● パスワードリスト攻撃

多くの人は、複数のSNSやその他Webサービスを利用するに当たって、同じアカウント名や同じパスワー

ドを使いまわす傾向があります。利用者があるSNSで
使用しているアカウント名とパスワードが攻撃者に知ら
れると、その人が他のSNSで使用するアカウントに対
しても、同じパスワードを用いてログインしようとする
攻撃が行われ、被害が拡大します。あるWebサービス
において流出したアカウント名とパスワードの組をまと
めたリスト(パスワードリスト)を、他のWebサービスな
どへの攻撃に利用する手法を、パスワードリスト攻撃と
いいます。

【Cookie】

Cookie(クッキー)は、Webサーバとブラウザとの間
のセッションを管理したり、Webサーバにアクセスして
きたクライアントを識別したりするために用いられるも
ののです。

CookieはHTTP Header(ヘッダ)に格納されていま
す。クライアントを識別したWebサーバは、Cookieを
作成してHTTPレスポンス内のHTTPヘッダに格納し、
ブラウザに渡します。そして、ブラウザからWebサーバ
にアクセスするときに、必要に応じてCookieがHTTP
リクエストに格納されてWebサーバに渡されます。

<Cookieの例>

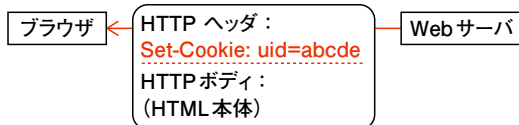
WebサーバからのHTTPレスポンス中のHTTPヘッダ

```
HTTP/1.1 200 OK
:
Set-Cookie: uid=abcde
:
```



利用者のブラウザが動作しているPCに保存されたCookie

```
uid=abcde
```



uid=abcde というデータを Cookie として保存

図 A

設問 1 パスワードを推測する攻撃手法

空欄 a

Qさんへのヒアリングから、設定されていたパスワ
ードが氏名と誕生日を組み合わせたものであったことが
判明しています。このような文字列を入力したパスワ
ードを推測する攻撃手法は、類推攻撃(Ⅰ)です。

- × **ア** DoS (Denial of Service) 攻撃とは、大量のパ
ケットを送りつけるなどの方法で、攻撃対象の
サーバなどの処理効率を低下させたり、機能を
停止させたりする攻撃手法のことです。
- × **イ** サイドチャネル攻撃とは、暗号化装置のソフト
ウェアやハードウェアをさまざまな方法で解析
して、暗号の解読を試みる攻撃のことです。
- × **ウ** 標的型攻撃とは、特定の組織または個人を対象
として、その組織または個人の関係者になりす
まして、業務に関係する字句を含むメールを送
信し、添付ファイルを開かせるなどの手口で、マ
ルウェアに感染させようとする攻撃手法です。

空欄 b

Qさんのアカウント名とパスワードが第三者に知られ
たので、【パスワードを推測しようとする攻撃】で説明し
たパスワードリスト攻撃が、P-SNS以外のサービスに
対して実行される危険性があります。空欄 bには「**パス
ワードリスト攻撃**」(Ⅱ)が入ります。

- × **ア** ゼロデイ攻撃手法は、新種のウイルスなど、対
策が公表されていない不正プログラムによって
行われる攻撃です。
- × **イ** 総当たり攻撃は、ブルートフォース攻撃の別名
です。
- × **エ** フィッシング攻撃は、サイトの偽装や偽造電子
メールの使用によって、ユーザを騙して個人情報
などを不正に入手したりする攻撃です。

設問 2 攻撃の足掛かりとなる情報

「公開範囲の設定ができない情報」と下線①にありま
す。解答群のうち、日記と写真は公開範囲の設定ができ
ますが、アカウント名は設定ができないので、他の会員
から常に見られます。また、電子メールアドレスは図 1
には存在しないので、他の会員が参照することはできま
せん。以上から、「**アカウント名**」(Ⅲ)が正解です。攻撃
者は、マイページ内のアカウント名を足掛かりとして各
種のパスワードを類推して、当該アカウントに不正にロ
グインしようとします。

設問 3 不正ログイン対策

(1)

各解答群の記述を確認します。

- **ア** について

英和辞典にある英単語をパスワードとして利用禁止にすることで、【パスワードを推測しようとする攻撃】の辞書攻撃でパスワードを推測されることはなくなります。Qさんのアカウントへの攻撃手法に対する有効な対策です。

● **イ**について

会員情報として登録した文字列(本名, 生年月日など)の文字列をパスワードに含めることを禁止すると、【パスワードを推測しようとする攻撃】の類推攻撃でパスワードを推測されることはなくなります。Qさんのアカウントへの攻撃手法に対する有効な対策です。

● **ウ**について

辞書に載っている単語には, “*”や”@”などの記号文字が含まれることはありません。パスワードに記号文字を含めることを必須化すると, 辞書攻撃や類推攻撃ではパスワードを推測できなくなり, 安全性が向上します。Qさんのアカウントへの攻撃手法に対する有効

な対策です。

● **エ**について

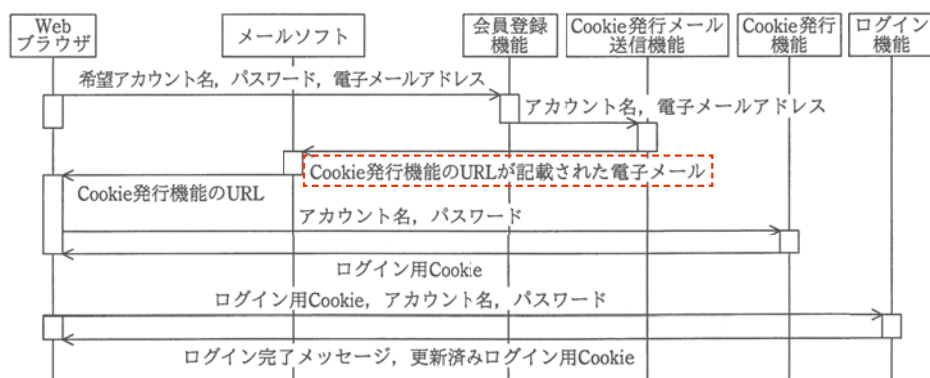
あるアカウントがログインしなくなってから半年以内に類推攻撃などが行われ, 不正ログインされる場合があります。そのため, 半年以上ログイン実績がないアカウントを利用停止にする対策は, 有効ではありません。

以上から, **エ**が正解です。

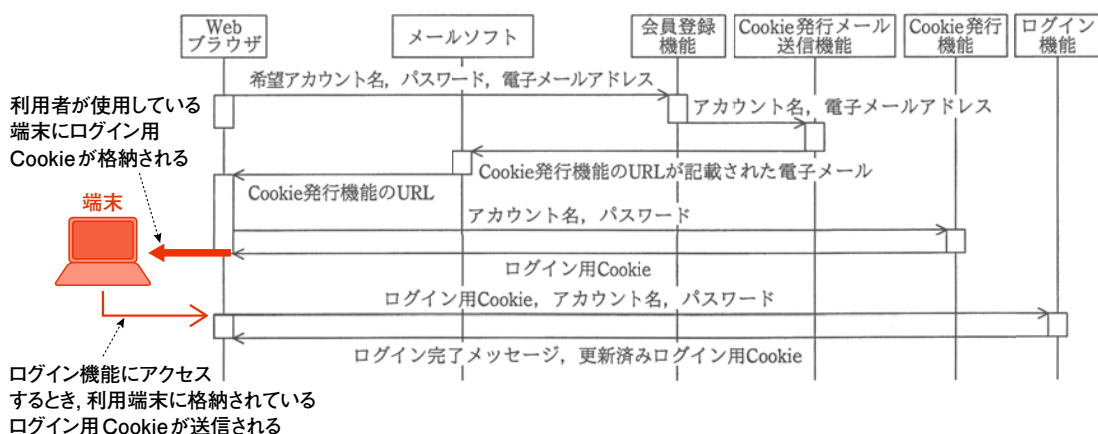
(2)

WebブラウザからWebサーバにアクセスすると, そのWebブラウザが稼働しているコンピュータにCookieが格納されます。アカウント名とパスワードによる認証は, それらを知っているユーザを認証するのに対し, Cookieによる認証は, Cookieをもっているコンピュータそのものを認証します。

Cookieによる認証を追加すると, ユーザが希望アカウント名などを入力して会員登録をしたとき, Cookie発



図B



図C

行機能のURLが記載された電子メールがユーザ宛てに送られます(図B)。

ユーザは、このメール内に記載されたURLからWebブラウザを用いてCookie発行機能にアクセスします。当該URLのページでアカウント名とパスワードを入力すると、ログイン用Cookieが発行されて、会員の利用端末に保存されます(図C)。

Webブラウザがログイン機能にアクセスすると、端末に格納されているログイン用Cookieが送信されます。このログイン用Cookieによって、アクセス時に使用されたWebブラウザを認証することができます。設問文に「何を認証するものか」という表記があることから、「Webブラウザ」(イ)が適切です。

(3)

【P-SNSの利用方法】から、会員登録時に入力する情報はアカウント名、パスワード、電子メールアドレス、プロフィール情報です。図3の手順を用いると、入力した

電子メールアドレス宛てに、Cookie発行機能のURLが記載されたメールが送信されます。会員が入力した電子メールアドレスが正しければ、そのメールアドレスに届いたメールを読んで、会員はログイン作業を完了させることができます。入力時のミスによって存在しない電子メールアドレスを入力した場合は、このメールが会員に届かず、ログイン作業を完了できません。

すなわち、会員登録時に入力された情報のうち、電子メールアドレスの有効性を確認することができます。よって、「電子メールアドレス」(オ)が正解です。

解答

設問1 a: エ b: ウ

設問2 ア

設問3 (1) エ (2) イ (3) オ

■問題文中で共通に使用される表記ルール

各問題文中に注記がない限り、次の表記ルールが適用されているものとする。

| 試験問題での表記 | 規格・標準の名称 |
|---------------|--------------------|
| JIS Q 9001 | JIS Q 9001:2015 |
| JIS Q 14001 | JIS Q 14001:2015 |
| JIS Q 15001 | JIS Q 15001:2006 |
| JIS Q 20000-1 | JIS Q 20000-1:2012 |
| JIS Q 20000-2 | JIS Q 20000-2:2013 |
| JIS Q 27000 | JIS Q 27000:2014 |
| JIS Q 27001 | JIS Q 27001:2014 |
| JIS Q 27002 | JIS Q 27002:2014 |
| JIS X 0160 | JIS X 0160:2012 |
| ISO 21500 | ISO 21500:2012 |
| ITIL | ITIL 2011 edition |
| PMBOK | PMBOK ガイド 第5版 |
| 共通フレーム | 共通フレーム 2013 |

解答一覧

平成28年度 秋期

●午前問題

| | | | | | | | | | | | | | | | | | | | |
|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| 問1 | 正 | 問2 | イ | 問3 | ウ | 問4 | ウ | 問5 | ア | 問6 | ア | 問7 | ウ | 問8 | イ | 問9 | 正 | 問10 | 正 |
| 問11 | 正 | 問12 | 正 | 問13 | 正 | 問14 | イ | 問15 | イ | 問16 | 正 | 問17 | イ | 問18 | 正 | 問19 | イ | 問20 | ア |
| 問21 | ア | 問22 | ア | 問23 | ア | 問24 | イ | 問25 | ア | 問26 | ウ | 問27 | 正 | 問28 | ウ | 問29 | ウ | 問30 | ウ |
| 問31 | 正 | 問32 | ウ | 問33 | ウ | 問34 | ウ | 問35 | 正 | 問36 | ウ | 問37 | 正 | 問38 | ウ | 問39 | ア | 問40 | ウ |
| 問41 | ア | 問42 | ウ | 問43 | ア | 問44 | イ | 問45 | ア | 問46 | イ | 問47 | ウ | 問48 | イ | 問49 | ウ | 問50 | イ |

●午後問題

| | | | | | | |
|----|-----|-----------------------------------|-----------|-----------------------------|-----|--------------|
| 問1 | 設問1 | (1)a: ア (2)ア | 設問2 | キ | 設問3 | (1)b: 正 (2)ケ |
| | 設問4 | (1)c: イ d: ア (2)e: イ f: 正 (順不同) | (3)ウ (4)キ | | | |
| 問2 | 設問1 | a: ア b: 正 c: イ d: 正 | | | | |
| | 設問2 | (1)ア (2)ウ (3)e: イ (4)f: イ (5)g: イ | | | | |
| 問3 | 設問1 | (1)イ (2)a: ア (3)カ | 設問2 | (1)b: ウ c: ア d: カ e: ア (2)ウ | | |
| | 設問3 | (1)f: カ (2)正 (3)g: イ | | | | |

平成28年度 春期

●午前問題

| | | | | | | | | | | | | | | | | | | | |
|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| 問1 | ウ | 問2 | ウ | 問3 | イ | 問4 | イ | 問5 | ア | 問6 | イ | 問7 | ア | 問8 | ウ | 問9 | ア | 問10 | 正 |
| 問11 | 正 | 問12 | ウ | 問13 | イ | 問14 | イ | 問15 | ウ | 問16 | ウ | 問17 | ウ | 問18 | ア | 問19 | ウ | 問20 | ウ |
| 問21 | 正 | 問22 | イ | 問23 | ウ | 問24 | イ | 問25 | ウ | 問26 | 正 | 問27 | イ | 問28 | イ | 問29 | ア | 問30 | 正 |
| 問31 | 正 | 問32 | ア | 問33 | ア | 問34 | 正 | 問35 | ウ | 問36 | イ | 問37 | イ | 問38 | ア | 問39 | ア | 問40 | ア |
| 問41 | 正 | 問42 | ア | 問43 | 正 | 問44 | イ | 問45 | ア | 問46 | 正 | 問47 | イ | 問48 | イ | 問49 | イ | 問50 | ウ |

●午後問題

| | | | | | | |
|----|-----|---------------------------------------|-----|------|-----|--------------------------------------|
| 問1 | 設問1 | (1)a: キ b: ク (2)c: ウ (3)ア, 正 (4)カ | | | | |
| | 設問2 | (1)カ (2)d: 正 (3)e: イ (4)f: ア (5)正 | | | | |
| 問2 | 設問1 | (1)ア (2)正 (3)a: ア b: イ (4)ウ (5)正 (6)イ | | | | |
| | 設問2 | (1)c: 正 (2)d: ア e: ウ f: ア (3)ウ (4)ア | | | | |
| 問3 | 設問1 | イ | 設問2 | イ, ア | 設問3 | (1)a: イ (2)b: 正 (3)c: ア (4)d: イ (5)イ |
| | 設問4 | (1)e: カ (2)f: ア | | | | |

第1回 模擬試験

●午前問題

| | | | | | | | | | | | | | | | | | | | |
|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| 問1 | イ | 問2 | ア | 問3 | ア | 問4 | 正 | 問5 | ウ | 問6 | イ | 問7 | ウ | 問8 | ア | 問9 | イ | 問10 | イ |
| 問11 | イ | 問12 | ア | 問13 | 正 | 問14 | ア | 問15 | ウ | 問16 | ア | 問17 | 正 | 問18 | 正 | 問19 | ア | 問20 | イ |
| 問21 | ア | 問22 | イ | 問23 | イ | 問24 | ア | 問25 | イ | 問26 | 正 | 問27 | ウ | 問28 | ア | 問29 | 正 | 問30 | ウ |
| 問31 | ウ | 問32 | ア | 問33 | ア | 問34 | ア | 問35 | ア | 問36 | ア | 問37 | 正 | 問38 | 正 | 問39 | イ | 問40 | 正 |
| 問41 | ア | 問42 | ウ | 問43 | イ | 問44 | 正 | 問45 | イ | 問46 | ア | 問47 | ウ | 問48 | イ | 問49 | ア | 問50 | ウ |

●午後問題

| | | | | | | |
|----|-----|--------------------------|-----|---|-----|------|
| 問1 | 設問1 | a: ウ b: キ c: ケ d: ウ | 設問2 | イ | | |
| 問2 | 設問1 | a: イ b: イ c: カ (b, c順不同) | 設問2 | 正 | | |
| | 設問3 | イ | 設問4 | ア | 設問5 | ウ, ア |
| 問3 | 設問1 | イ | 設問2 | 正 | 設問3 | ウ |
| | 設問4 | a: ア b: イ c: ア | | | | |

第2回 模擬試験

●午前問題

| | | | | | | | | | | | | | | | | | | | |
|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| 問1 | ア | 問2 | ア | 問3 | ア | 問4 | イ | 問5 | イ | 問6 | ア | 問7 | ウ | 問8 | エ | 問9 | エ | 問10 | ア |
| 問11 | イ | 問12 | ウ | 問13 | エ | 問14 | ア | 問15 | ア | 問16 | ウ | 問17 | エ | 問18 | イ | 問19 | エ | 問20 | イ |
| 問21 | ア | 問22 | イ | 問23 | イ | 問24 | イ | 問25 | ア | 問26 | イ | 問27 | ア | 問28 | イ | 問29 | イ | 問30 | ウ |
| 問31 | ア | 問32 | ア | 問33 | ア | 問34 | エ | 問35 | イ | 問36 | ア | 問37 | イ | 問38 | エ | 問39 | エ | 問40 | ウ |
| 問41 | イ | 問42 | エ | 問43 | ア | 問44 | イ | 問45 | イ | 問46 | ウ | 問47 | エ | 問48 | ア | 問49 | イ | 問50 | エ |

●午後問題

| | | | | | | | | | | |
|----|-----|-----|-----|-----|-----|--------------------|-----|---|-----|------|
| 問1 | 設問1 | エ | 設問2 | イ | 設問3 | a:イ b:カ (a, b 順不同) | | | | |
| 問2 | 設問1 | ウ | 設問2 | ウ | 設問3 | a:ア | 設問4 | エ | 設問5 | エ |
| 問3 | 設問1 | a:エ | b:イ | c:エ | d:エ | 設問2 | | | | ウ, エ |

第3回 模擬試験

●午前問題

| | | | | | | | | | | | | | | | | | | | |
|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|-----|---|
| 問1 | ア | 問2 | イ | 問3 | ウ | 問4 | イ | 問5 | ウ | 問6 | ア | 問7 | イ | 問8 | ウ | 問9 | ア | 問10 | ア |
| 問11 | ア | 問12 | ア | 問13 | イ | 問14 | イ | 問15 | ア | 問16 | ア | 問17 | ア | 問18 | ウ | 問19 | エ | 問20 | ウ |
| 問21 | エ | 問22 | ア | 問23 | エ | 問24 | エ | 問25 | ア | 問26 | エ | 問27 | ウ | 問28 | ア | 問29 | ウ | 問30 | エ |
| 問31 | イ | 問32 | ウ | 問33 | エ | 問34 | エ | 問35 | エ | 問36 | ア | 問37 | ア | 問38 | ウ | 問39 | ア | 問40 | イ |
| 問41 | ア | 問42 | ウ | 問43 | ア | 問44 | ア | 問45 | イ | 問46 | エ | 問47 | ア | 問48 | ア | 問49 | エ | 問50 | エ |

●午後問題

| | | | | | | | | | |
|----|-----|------|-----|-----|-----|-----|----------------|-----|-----|
| 問1 | 設問1 | a:エ | b:ア | 設問2 | イ | 設問3 | エ | 設問4 | ウ |
| 問2 | 設問1 | ア, イ | 設問2 | a:ウ | b:イ | c:エ | 設問3 | d:ウ | e:イ |
| 問3 | 設問1 | a:エ | b:ウ | 設問2 | ア | 設問3 | (1)エ (2)イ (3)オ | | |

答案用紙

※本ページをコピー、またはPDFを【ダウンロード→印刷】してご利用ください。ダウンロードについては2ページをご確認ください。

| | | | | | | | |
|----------|---|--------|---|---|---|---|---|
| マークの記入方法 |  | 悪いマーク例 |  |  |  |  |  |
|----------|---|--------|---|---|---|---|---|

●午前問題 (共通)

| 解答欄 | | | | | | | | | |
|-----|---|---|---|---|-----|---|---|---|---|
| 問1 | ア | イ | ウ | エ | 問11 | ア | イ | ウ | エ |
| 問2 | ア | イ | ウ | エ | 問12 | ア | イ | ウ | エ |
| 問3 | ア | イ | ウ | エ | 問13 | ア | イ | ウ | エ |
| 問4 | ア | イ | ウ | エ | 問14 | ア | イ | ウ | エ |
| 問5 | ア | イ | ウ | エ | 問15 | ア | イ | ウ | エ |
| 問6 | ア | イ | ウ | エ | 問16 | ア | イ | ウ | エ |
| 問7 | ア | イ | ウ | エ | 問17 | ア | イ | ウ | エ |
| 問8 | ア | イ | ウ | エ | 問18 | ア | イ | ウ | エ |
| 問9 | ア | イ | ウ | エ | 問19 | ア | イ | ウ | エ |
| 問10 | ア | イ | ウ | エ | 問20 | ア | イ | ウ | エ |
| 問21 | ア | イ | ウ | エ | 問31 | ア | イ | ウ | エ |
| 問22 | ア | イ | ウ | エ | 問32 | ア | イ | ウ | エ |
| 問23 | ア | イ | ウ | エ | 問33 | ア | イ | ウ | エ |
| 問24 | ア | イ | ウ | エ | 問34 | ア | イ | ウ | エ |
| 問25 | ア | イ | ウ | エ | 問35 | ア | イ | ウ | エ |
| 問26 | ア | イ | ウ | エ | 問36 | ア | イ | ウ | エ |
| 問27 | ア | イ | ウ | エ | 問37 | ア | イ | ウ | エ |
| 問28 | ア | イ | ウ | エ | 問38 | ア | イ | ウ | エ |
| 問29 | ア | イ | ウ | エ | 問39 | ア | イ | ウ | エ |
| 問30 | ア | イ | ウ | エ | 問40 | ア | イ | ウ | エ |
| 問41 | ア | イ | ウ | エ | 問50 | ア | イ | ウ | エ |

平成28年度 秋期

●午後問題

| 解答欄 | | | | | | | | | |
|-----|-----|-------|-------|-------|-------|-------|-------|-----|--|
| 問1 | 設問1 | (1) a | (2) | 設問2 | | 設問3 | (1) b | (2) | |
| | 設問4 | (1) c | d | (2) e | f | (3) | (4) | | |
| 問2 | 設問1 | a | b | c | d | | | | |
| | 設問2 | (1) | (2) | (3) e | (4) f | (5) g | | | |
| 問3 | 設問1 | (1) | (2) a | (3) | | | | | |
| | 設問2 | (1) b | c | d | e | (2) | | | |
| | 設問3 | (1) f | (2) | (3) g | | | | | |

平成28年度 春期

●午後問題

| 解答欄 | | | | | | | | | | | | | | | |
|-----|-----|--------------------|-----|---|-------|--------------------|-----|-------|-----|-------|-----|-------|-----|-----|--|
| 問1 | 設問1 | (1) a b | | | (2) c | | (3) | | (4) | | | | | | |
| | 設問2 | (1) | | (2) d | | (3) e | | (4) f | | (5) | | | | | |
| 問2 | 設問1 | (1) | | (2) | | (3) a b | | | (4) | | (5) | | (6) | | |
| | 設問2 | (1) c | | (2) d e f | | | | (3) | | (4) | | | | | |
| 問3 | 設問1 | | 設問2 | , | 設問3 | (1) a | | (2) b | | (3) c | | (4) d | | (5) | |
| | 設問4 | (1) e | | (2) f | | | | | | | | | | | |

第1回 模擬試験

●午後問題

| 解答欄 | | | | | | | | | | | | |
|-----|-----|---|-----|---|-----|-----|-----|-----|---|-----|--|-------|
| 問 1 | 設問1 | a | b | c | d | 設問2 | | | | | | |
| 問 2 | 設問1 | a | b | c | | 設問2 | | 設問3 | | 設問4 | | 設問5 , |
| 問 3 | 設問1 | | 設問2 | | 設問3 | | 設問4 | a | b | c | | |

第2回 模擬試験

●午後問題

| 解答欄 | | | | | | | | | |
|-----|------|---|------|---|------|----------------|------|---|------|
| 問 1 | 設問 1 | | 設問 2 | | 設問 3 | a b | | | |
| 問 2 | 設問 1 | | 設問 2 | | 設問 3 | a | 設問 4 | | 設問 5 |
| 問 3 | 設問 1 | a | b | c | d | 設問 2 | | , | |

第3回 模擬試験

●午後問題

| 解答欄 | | | | | | | | | |
|-----|-----|---|-----|-----|---|-----|-----|-----|-----|
| 問1 | 設問1 | a | b | 設問2 | | 設問3 | | 設問4 | |
| 問2 | 設問1 | , | 設問2 | a | b | c | 設問3 | d | e |
| 問3 | 設問1 | a | b | 設問2 | | 設問3 | (1) | (2) | (3) |

索引

数字

| | |
|--------|-----|
| 2次回帰係数 | 251 |
| 2要素認証 | 123 |
| 3DES | 173 |

英字

| | |
|-------------|--------------------|
| AES | 131, 149, 173, 219 |
| ANSI | 124 |
| APT | 123 |
| As-Isモデル | 304 |
| ATA | 125 |
| Autorun.inf | 129 |
| AVR | 302 |
| Base64 | 55 |
| BCM | 79 |
| BCP | 73, 143 |
| BIOS | 124 |
| BIOSパスワード | 124 |
| BPO | 79 |
| BPR | 198 |
| BYOD | 51, 118 |
| C&Cサーバ | 51 |
| CA | 223, 281 |
| CAPTCHA | 57, 281 |
| CC | 66 |
| CMMI | 247 |
| CMVP | 283 |
| COCOMO | 244 |
| Cookie | 322 |
| CP | 285 |
| CRL | 65, 281 |
| CRYPTREC | 43, 283 |
| CSA | 113, 167 |
| CSIRT | 45, 53, 112, 181 |
| CSRF | 310 |
| CVCF | 302 |
| CVE | 45 |
| CVSS | 45, 181 |
| DFD | 77, 248 |
| DHCP | 78, 297 |
| DHCPアック | 79 |
| DHCPオファー | 79 |
| DHCPディスカバ | 78 |
| DHCPリクエスト | 79 |
| DLP | 53 |

| | |
|--------------------------------|-------------------|
| DMZ | 141, 266 |
| DNSキャッシュポイズニング | 177, 277 |
| DoS | 125 |
| DoS攻撃 | 177, 322 |
| E-R図 | 77, 191, 248 |
| EA | 304 |
| EAP | 287 |
| EA参照モデル | 304 |
| ECM | 51 |
| ERP | 141, 199 |
| ESS-ID | 287 |
| FAR | 222 |
| FP | 200 |
| FQDN | 277 |
| FRR | 222 |
| FTP | 57 |
| GETメソッド | 311 |
| GMITS | 282 |
| GROUP BY句 | 240 |
| HDDパスワード | 124 |
| HIDS | 119, 183 |
| HTTP Response Splitting Attack | 127 |
| HTTPのメソッド | 311 |
| HTTPヘッダインジェクション | 276 |
| IaaS | 141 |
| ICANN | 112, 181 |
| ICカード | 42 |
| IDS | 53, 119, 183, 285 |
| IEEE | 191 |
| IEEE 802.1X | 287 |
| IETF | 112, 181 |
| iframe | 126 |
| IMAP4 | 193 |
| IP | 113 |
| IPL | 123 |
| IPS | 315 |
| IPsec | 131 |
| IPアドレス | 192, 242, 298 |
| IPパケット | 264 |
| IPヘッダ | 119, 264 |
| IPマスカレード | 141 |
| ISMS | 45, 181, 225, 226 |
| ISMSにおけるリスク分析 | 227 |
| ISMSプロセス | 225 |

| | |
|------------------|------------------|
| ISO/IEC 15408 | 66 |
| ISO/IEC 27005 | 66 |
| ISO/IEC TR 13335 | 282 |
| ISO 14004 | 66 |
| ISO 9001 | 66, 245 |
| ITIL | 195, 245, 301 |
| ITU-T | 129 |
| ITサービスマネジメント | 195 |
| IV | 287 |
| JEC | 190 |
| JEITA | 191 |
| JISC | 43 |
| JIS Q 27000 | 45, 48 |
| JIS Q 27001 | 45, 58, 115, 218 |
| JIS Q 27002 | 45, 49, 219 |
| JIS Q 31000 | 49 |
| JIS Q 31000:2010 | 43 |
| JIS TR X 0036 | 283 |
| JPCERT/CC | 43 |
| JVN | 44 |
| LDAP | 297 |
| LTE | 51 |
| MACアドレス制限 | 287 |
| MD5 | 121 |
| MDM | 51 |
| MRP | 79 |
| MTBF | 138 |
| MTTR | 138 |
| NAPT | 141 |
| NAT | 297 |
| NIDS | 119, 183 |
| NTP | 57 |
| OECDプライバシーガイドライン | 132 |
| ORDER BY句 | 297 |
| OSコマンドインジェクション | 276 |
| PaaS | 141 |
| PCI DSS | 181, 227 |
| PCIデータセキュリティ基準 | 227 |
| PDCAサイクル | 225 |
| PGP | 287 |
| PIN | 42, 173 |
| PKI | 65, 128, 281 |
| PMS | 181 |
| POP3 | 193, 267 |
| POSTメソッド | 312 |

| | |
|-------------|--------------------|
| QRコード | 57, 281 |
| RFC | 112, 245, 301, 306 |
| RFI | 142, 200, 306 |
| RFID | 52 |
| RFP | 143, 249, 306 |
| RFQ | 143 |
| ROI | 305 |
| rootkit | 52 |
| RPO | 138 |
| RTO | 138 |
| S/MIME | 193, 287 |
| SaaS | 141, 199 |
| SCM | 141 |
| SET | 287 |
| SHA-1 | 121 |
| SHA-2 | 121 |
| SIEM | 53 |
| SLA | 137, 199, 245 |
| SMTP | 57, 193, 267, 297 |
| SNMP | 57 |
| SOW | 306 |
| SPF | 54 |
| SQLインジェクション | 184, 214, 268, 288 |
| SSH | 268, 287 |
| SSL | 231, 286 |
| SSL-VPN | 119 |
| Tabnabbing | 127 |
| TCP/IP | 113 |
| TCPヘッダ | 265 |
| Telnet | 287 |
| TKIP | 53, 287 |
| TLS | 55, 231, 286 |
| To-Beモデル | 304 |
| UML | 248 |
| UNION句 | 297 |
| UNIQUE句 | 297 |
| UPS | 302 |
| VoIPゲートウェイ | 221 |
| VPN | 231 |
| WAF | 119, 183, 227, 316 |
| WBS | 193 |
| Web beacon | 53 |
| WEP | 287 |
| WPA | 287 |
| X.509証明書 | 129 |
| XBRL | 141 |

あ行

| | |
|-----------------|--------------------|
| アクセスタイム | 139 |
| アクティビティ | 193 |
| アクティビティ図 | 305 |
| 後処理 | 131 |
| アノマリ型 | 316 |
| アプリケーションアーキテクチャ | 304 |
| アローダイアグラム | 307 |
| 暗号化 | 100 |
| 暗号化鍵 | 174 |
| 暗号モジュール評価プログラム | 283 |
| 移行テスト | 75 |
| 一方向性関数 | 121 |
| 一斉移行方式 | 196 |
| 五つの基本原則 | 60 |
| 一般基準 | 73 |
| 移動平均法 | 201 |
| 意図的脅威 | 283 |
| 委任契約 | 71 |
| インシデント | 75, 301 |
| インシデント管理 | 301 |
| インシデント管理プロセス | 53 |
| インシデントレスポンス | 285 |
| インテグリティチェック法 | 56, 183 |
| ウェルノウンポート | 265 |
| ウォードライビング | 129 |
| 請負契約 | 71, 135, 293 |
| 運用テスト | 75 |
| 営業秘密 | 135, 187, 234, 291 |
| エージェント方式 | 223 |
| 遠隔操作ウイルス | 63 |
| エンタープライズアーキテクチャ | 247, 304 |
| エンティティ | 77 |
| エンティティタイプ | 191 |
| 応答時間 | 139 |
| オンラインストレージサービス | 82 |

か行

| | |
|-------------|-------------------|
| カーソル | 297 |
| 外国為替及び外国貿易法 | 237 |
| 回収期間法 | 305 |
| 外為法 | 237 |
| 回復 | 227 |
| 開放性 | 61 |
| 架空電子メールアドレス | 69 |
| 稼働率 | 191, 239, 295 |
| 可用性 | 45, 205, 256, 275 |
| 環境的脅威 | 283 |

| | |
|-------------------|--------------------|
| 関係データベース | 192 |
| 監査委員会 | 197 |
| 監査役 | 197 |
| 監査リスク | 49 |
| 監視 | 227 |
| 完全性 | 58, 172, 205, 218 |
| キーロガー | 63 |
| 機会 | 117 |
| 機会の認識 | 173 |
| 危殆化 | 279 |
| 基本方針 | 227 |
| 機密性 | 45, 172, 205, 218 |
| 逆アセンブル | 229 |
| キャプチャ | 281 |
| 脅威 | 179, 219, 224, 283 |
| 供給者の選定 | 143 |
| 共通鍵暗号方式 | 219, 277 |
| 共通フレーム | 80, 248 |
| 共通フレーム2007 | 199 |
| 業務フロー | 198 |
| 業務要件 | 199, 249 |
| 業務要件定義 | 305 |
| 緊急時対応計画 | 178 |
| 偶発的脅威 | 283 |
| クエリストリング | 312 |
| クッキー | 322 |
| 組合セアプローチ | 45 |
| クライアント | 77 |
| クライアントサーバシステム | 76 |
| クラスA | 192 |
| クラスB | 193 |
| クラスC | 193 |
| クラスD | 193 |
| クラス図 | 305 |
| クラスタ | 119 |
| クリアスクリーン | 113 |
| クリアデスク | 113 |
| クリックジャッキング | 126 |
| クリティカルパス | 195, 243 |
| クロスサイトスクリプティング | 58, 176, 231, 288 |
| クロスサイトリクエストフォージェリ | 277, 289, 310 |
| 経営者 | 197 |
| 契約の締結 | 143 |
| ゲートウェイ | 241 |
| 結合テスト | 75 |
| 検疫ネットワーク | 55 |
| 減価償却 | 201 |

| | |
|-----------------|--------------------|
| 権限取得 | 131 |
| コアコンピタンス | 143, 238 |
| コアコンピタンス経営 | 199, 201 |
| 公開鍵 | 127, 174, 278 |
| 公開鍵暗号 | 65, 131 |
| 公開鍵暗号方式 | 174, 210, 220, 277 |
| 公開鍵基盤 | 65, 128, 281 |
| 公開鍵証明書 | 128 |
| 公衆送信権 | 233 |
| コーポレートアイデンティティ | 143 |
| コーポレートガバナンス | 143, 238 |
| 個人情報 | 133 |
| 個人情報取扱事業者 | 237 |
| 個人情報保護法 | 133, 188, 236 |
| 個人番号 | 68 |
| コモンクライテリア | 66 |
| 固有リスク | 49 |
| コンティンジェンシープラン | 72, 178, 227 |
| コントロールセルフアセスメント | 113 |
| コンピュータフォレンジクス | 285 |
| コンプライアンス | 238 |
| コンベア法 | 57, 183 |

さ行

| | |
|---------------------------|--------------|
| サーバ | 76 |
| サービス | 265 |
| サービスサポート | 195, 245 |
| サービスデリバリー | 195, 245 |
| サイクルタイム | 139 |
| 最終取得原価法 | 201 |
| サイドチャネル攻撃 | 279, 322 |
| サイバーセキュリティ基本法 | 189 |
| サイバーセキュリティ戦略 | 60 |
| 財務報告に係る内部統制の評価及び
監査の基準 | 197 |
| 裁量労働制 | 189 |
| 詐欺罪 | 67 |
| ザックマンフレームワーク | 304 |
| ザックマンモデル | 304 |
| サニタイジング | 177, 222 |
| サブネット | 242, 298 |
| サブネット部 | 242, 298 |
| サブネットマスク | 243, 298 |
| 差分解読法 | 279 |
| 差分バックアップ | 75 |
| 散布図 | 250 |
| サンプリング | 72 |
| 残留リスク | 49, 115, 219 |

| | |
|------------------|---------------|
| 自家発電装置 | 303 |
| 磁気ディスク | 122 |
| 事業継続計画 | 73, 143 |
| 事業部制組織 | 81, 250 |
| シグネチャ型 | 316 |
| シグネチャコード | 183 |
| 時刻同期 | 209 |
| 辞書攻撃 | 63, 230, 321 |
| システム監査基準 | 197 |
| システム監査人 | 246 |
| システムテスト | 75 |
| 事前調査 | 131 |
| 実施基準 | 73 |
| 射影 | 192 |
| 社内ベンチャ | 250 |
| 集計関数 | 240 |
| シュリンクラップ契約 | 293 |
| 準委任契約 | 71 |
| 純粹リスク | 225 |
| 瞬断 | 302 |
| 詳細リスク分析 | 45, 227 |
| 状態遷移図 | 248, 305 |
| 商標法 | 133 |
| 情報資産 | 45, 137 |
| 情報セキュリティ監査基準 | 73, 136, 303 |
| 情報セキュリティ監査制度 | 113, 136, 303 |
| 情報セキュリティ管理基準 | 137, 303 |
| 情報セキュリティ政策会議 | 283 |
| 情報セキュリティ対策ベンチマーク | 113, 119 |
| 情報セキュリティの3要素 | 45, 172, 218 |
| 情報セキュリティポリシ | 226 |
| 情報のCIA | 58, 256 |
| 情報の自由な流通の確保 | 60 |
| 正味現在価値法 | 305 |
| 職能制組織 | 81, 250 |
| 助言型監査 | 113 |
| 所持品による認証 | 123 |
| 署名検証鍵 | 127 |
| 署名生成鍵 | 127 |
| ショルダハッキング | 61, 118 |
| 自律性 | 61 |
| シングルサインオン | 223 |
| 信用毀損罪 | 67 |
| スイッチングハブ | 140, 241 |
| スクリプト | 59, 125 |
| スクリプトキディ | 61, 123 |

| | |
|--------------------|-------------------|
| ステークホルダ | 76, 143 |
| ステークホルダアナリシス | 143 |
| ステガノグラフィ | 285 |
| ストリクトルーティング | 221 |
| スニッフィング | 230 |
| スパイウェア | 63, 285 |
| スプレッドシート | 135 |
| 脆弱性 | 179, 219, 224 |
| 生体認証 | 123, 222 |
| 静的プレースホルダ | 214, 288 |
| 正当化 | 117, 173 |
| 性能テスト | 75 |
| 正の相関 | 251 |
| 責任追跡性 | 275 |
| セッションハイジャック | 175, 277, 289 |
| 接続先ポート番号 | 265 |
| 接続元ポート番号 | 265 |
| ゼロデイ攻撃 | 150, 322 |
| 善管注意義務 | 71 |
| 線形解読法 | 279 |
| 選択 | 192 |
| 総当たり攻撃 | 150, 231, 279 |
| 相関関係 | 250 |
| 相関係数 | 251 |
| 操作ログ | 51, 121 |
| 送信可能化 | 233 |
| 挿入 | 192 |
| 増分バックアップ | 75 |
| ソーシャルエンジニアリング | 62, 123, 149, 285 |
| ゾーン情報 | 177 |
| 組織における内部不正防止ガイドライン | 50, 116 |
| 組織のフラット化 | 201 |
| ソフトウェアライフサイクル | 80 |
| ソフトウェアライフサイクルプロセス | 199, 245, 248 |

た行

| | |
|-------------|---------|
| ターンアラウンドタイム | 139 |
| 耐タンパ性 | 261 |
| 他人受入率 | 222 |
| 多様な主体の連携 | 61 |
| 短縮URL | 57, 281 |
| 段数 | 173 |
| 単体テスト | 75 |
| チェックサム | 182 |
| チェックサム法 | 56, 183 |
| 知識による認証 | 123 |

| | |
|-------------------------|-------------------|
| チャレンジレスポンス | 231 |
| 調達プロセス | 249 |
| 著作権 | 187, 233, 290 |
| 著作権法 | 133, 187, 290 |
| 積上げ棒グラフ | 139 |
| 定額法 | 201 |
| デジタル証明書 | 64, 128, 223, 286 |
| デジタル署名 | 64, 127, 209, 220 |
| デジタルフォレンジックス | 72, 121, 221, 285 |
| 定率法 | 201 |
| ディレクトリトラバーサル | 59 |
| ディレクトリトラバーサル攻撃 | 175 |
| データアーキテクチャ | 304 |
| データアドミニストレーション | 139 |
| データウェアハウス | 139, 241 |
| データディクショナリ | 139 |
| データマイニング | 241 |
| データマッピング | 139 |
| データモデル | 305 |
| テクノロジーアーキテクチャ | 304 |
| 展開管理 | 301 |
| 電子計算機使用詐欺罪 | 67, 133 |
| 電子計算機損壊等業務妨害罪 | 133, 291 |
| 電子証明書 | 128, 223 |
| 電子署名法 | 292 |
| 電子政府推奨暗号リスト | 283 |
| テンベスト攻撃 | 229 |
| 同一性の証明 | 121 |
| 動機 | 117, 173 |
| 投機的リスク | 49, 225 |
| 統制自己評価 | 167 |
| 動的パケットフィルタリング | 266 |
| 特定個人情報の適正な取扱いに関するガイドライン | 68 |
| 特定商取引法 | 291 |
| 特定電気通信役務提供者 | 67 |
| 特定電子メール | 69, 135 |
| 特定電子メールの送信の適正化等に関する法律 | 69, 135 |
| 特定電子メール法 | 69 |
| 特定認証業務 | 293 |
| 特許権 | 235 |
| 特許法 | 234 |
| 特権的アクセス権 | 117 |
| ドライブバイダウンロード | 129 |
| トラックバックping | 57, 281 |
| トレードシークレット | 234 |

| | |
|--------|-----|
| トロイの木馬 | 150 |
|--------|-----|

な行

| | |
|------------------|------------------------|
| 内閣サイバーセキュリティセンター | 43 |
| 内部監査人 | 197 |
| 内部統制 | 158, 303 |
| 内部利益率法 | 305 |
| ナレッジマネジメント | 201 |
| 二重円グラフ | 139 |
| 認証局 | 65, 127, 223, 281, 284 |
| ねずみ講防止法 | 67 |
| ネットワーク型 | 119, 316 |
| ネットワーク部 | 192, 242, 298 |

は行

| | |
|-------------|--------------------|
| ハードウェアトークン | 123 |
| バイオメトリクス認証 | 177, 222 |
| バインド機構 | 214, 288 |
| バインド変数 | 288 |
| パケットフィルタリング | 232, 266 |
| 派遣契約 | 71 |
| パストラバース | 177 |
| パスワードリスト攻撃 | 63, 129, 321 |
| パスワードリマインダ | 123 |
| パターンマッチング | 183 |
| バックアップ | 75 |
| ハックティヴィズム | 113, 181 |
| バックドア | 52, 130, 221 |
| ハッシュ関数 | 121, 175, 186 |
| ハッシュ値 | 175, 186, 221, 279 |
| パッチ | 120 |
| バッファオーバーフロー | 59, 125, 177 |
| 発明 | 235 |
| バナーチェック | 177 |
| ハニーポット | 285 |
| バランススコアカード | 247 |
| パレート図 | 307 |
| 判定しきい値 | 222 |
| 非活性化タブ | 127 |
| 非機能要件 | 199, 249 |
| ピクチャパスワード | 63 |
| 非形式的アプローチ | 45, 227 |
| ビジネスアーキテクチャ | 304 |
| ビヘイビア法 | 56, 183 |
| 秘密鍵 | 127, 174, 278 |
| ヒヤリハット | 150 |
| 標準タスク法 | 245 |
| 標的型攻撃 | 322 |
| 標的型攻撃メール | 149 |

| | |
|------------------|--------------------|
| 品質要件 | 249 |
| ファイアウォール | 141, 266 |
| ファストトラッキング技法 | 299 |
| ファンクションポイント法 | 244 |
| フィッシング攻撃 | 322 |
| ブート | 123 |
| ブートルoader | 123 |
| フルブルーフ | 191, 239 |
| フェールセーフ | 191, 239, 294 |
| フェールソフト | 239, 294 |
| フォールトアボイダンス | 191, 294 |
| フォールトトレランス | 191 |
| フォールトトレラント | 239, 294 |
| フォールトマスキング | 294 |
| フォレンジック | 221 |
| 復号鍵 | 174 |
| 不正アクセス禁止法 | 70 |
| 不正競争防止法 | 135, 187, 234, 291 |
| 不正実行 | 131 |
| 不正のトライアングル | 117, 173 |
| プットナムモデル | 245 |
| 負の相関 | 251 |
| ブラックリスト | 316, 316 |
| ブリッジ | 140, 241 |
| ブルートフォース | 231, 279, 321 |
| フルバックアップ | 75 |
| フレックスタイム制 | 189 |
| ブロードキャストアドレス | 193 |
| プロキシサーバ | 51, 107, 140 |
| プロジェクトコストマネジメント | 193 |
| プロジェクトスコープマネジメント | 193 |
| プロジェクト組織 | 81 |
| プロジェクトタイムマネジメント | 193 |
| プロセス | 77 |
| プロトコル | 265 |
| プロバイダ | 66 |
| プロバイダ責任制限法 | 66, 291 |
| ページトークン | 311 |
| ベースラインアプローチ | 45, 227 |
| ベネトレーションテスト | 229, 285 |
| 変形労働時間制 | 189 |
| 変更管理 | 245, 301 |
| ベンチマーキング | 72, 199, 201 |
| 報告基準 | 73 |
| 法の支配 | 60 |
| ポートスキャン | 131 |
| ポート番号 | 57, 120, 265 |
| ポートフォリオ図 | 139 |

| | |
|---------------|---------------|
| 保証型監査 | 113 |
| ホスト型 | 119, 316 |
| ホスト部 | 192, 242, 298 |
| ポリモーフィック型ウイルス | 275 |
| ホワイトリスト | 316 |
| 本人拒否率 | 222 |

ま行

| | |
|----------------|----------|
| マイナンバー | 68 |
| マスタブートレコード | 123 |
| マトリックス図 | 307 |
| マトリックス組織 | 81, 250 |
| マルウェア | 120 |
| ミラーリング | 182 |
| 無害化 | 119 |
| 無限連鎖講の防止に関する法律 | 67 |
| 迷惑メール | 135 |
| メッセージ認証 | 279 |
| 持分法 | 201 |
| 問題管理 | 245, 301 |

や行

| | |
|---------|-----|
| ユースケース図 | 305 |
|---------|-----|

| | |
|---------|-----|
| 輸出貿易管理令 | 237 |
| 予防 | 227 |

ら行

| | |
|-----------|-------------------|
| ランサムウェア | 63, 129 |
| リスク | 48, 143, 178, 224 |
| リスクアセスメント | 256 |
| リスク移転 | 43, 114, 179, 224 |
| リスク回避 | 43, 114, 179, 224 |
| リスク活用 | 301 |
| リスク強化 | 301 |
| リスク共有 | 301 |
| リスク軽減 | 43, 114, 301 |
| リスクコントロール | 179, 224 |
| リスク集中 | 224 |
| リスク受容 | 43, 114, 179, 301 |
| リスク対応 | 43, 48 |
| リスク低減 | 43, 114, 179 |
| リスク転嫁 | 43, 114, 300 |
| リスク特定 | 48 |
| リスク評価 | 48 |
| リスクファイナンス | 179, 224, 283 |
| リスク分析 | 45, 48, 225 |

| | |
|----------------|-------------------|
| リスク分離 | 224 |
| リスク保有 | 43, 114, 219, 224 |
| リスクマネジメント | 49, 143, 178, 300 |
| リバースブルートフォース攻撃 | 129 |
| リバースプロキシ方式 | 223 |
| リピータ | 140, 241 |
| リモートアクセスサーバ | 51 |
| リリース管理 | 301 |
| リレーションシップ | 77, 191 |
| 類推攻撃 | 321 |
| ルータ | 140, 241 |
| ルートキット | 52, 275 |
| レーダチャート | 139 |
| レスポンスタイム | 139 |
| 労働基準法 | 189 |
| 労働者派遣法 | 189, 237, 293 |
| ロードバランサ | 119 |
| ロードバランシング | 119 |
| ローミング | 287 |

わ行

| | |
|----------|-----|
| ワークパッケージ | 193 |
| ワーム | 121 |

スマホで学べる単語帳アプリ（無料）

「でる語句 200」の使い方

注意!! 「でる語句 200」は、株式会社ビズリーチのスマートフォンアプリ「^{ズノフ}zukunft」で動作します。単語帳を無料で利用するには、お手持ちのスマートフォン（iPhone / Android）への「zukunft」のインストールと、「zukunft」を利用するためのユーザー登録が必要になります。

<対応 OS>

Android 版：

Android 4.0 以上

iPhone 版：

iOS 7.0 以降（iPad/iPod touch でも利用可）

「でる語句 200」とは

「でる語句 200」とは、「試験によくでる語句 厳選 200 語」の略で、スマートフォンで使える単語帳アプリです。情報処理技術者試験の専門家が、各試験の特性と出題頻度を徹底分析し、合格に必要なキーワード・用語を厳選して、200 語にまとめました。通勤・通学などのすき間学習や、試験直前の最終チェックなどにご活用ください。「でる語句 200」の利用には「zukunft」のインストール（導入手順 1）と、本書用の単語帳の登録（導入手順 2）が必要になります。下記の手順を参照して操作を行ってください。なお、すでに「zukunft」をお使いの方は、導入手順 2 から行なってください。

導入手順 1 ▶ スマートフォンに「zukunft」をインストールする

ここでは、iPhone の画面で説明を進めますが、Android でもほぼ同じ手順での操作になります。

1 お使いのスマートフォンで「App Store」（iPhone / iPad※ の場合）または「Google Play」（Android の場合）を起動してから「zukunft」を検索し、インストールしてください。

※ iPad の場合、画面左上のメニューを「iPhone のみ」に切り替えると zuknow が表示されます。



初めて起動するとアプリの機能紹介が始まるので「次へ」をタップして読み進め、「zukunft をはじめる」をタップするとこの画面が出る。Facebook アカウント、Twitter アカウント、メールアドレスの 3 種類の登録方法があるので、任意の方法を選択し、画面の指示に従ってユーザー登録を進める。[ユーザー登録せずに試す] を選ぶと「でる語句 200」が利用できないので、必ずいずれかの方法で登録する

登録が終わると「おすすめ設定」画面が表示されるので、画面の指示に従って選択していく。なにも選択しないと先に進めないのので 1 つ以上選択する

「ブッシュクイズ」画面が表示されるので、「送信確認画面へ」をタップする。「学習」画面が表示され、アプリが使えるようになる。「おすすめ設定」で選択した単語帳がすでに登録されている

導入手順 2 ▶ 本書専用の単語帳「でる語句 200」を登録する

1 「zukunft」の QR コード読み取り機能呼び出します。



画面下部にある「学習」をタップしたあと画面左上の「…」をタップする

「その他」画面が表示されるので、「アプリ設定」をタップする

「設定」画面が表示されるので、「QR コード」をタップする

【Android での手順】画面左上の「zukunft」マークをタップ⇒「設定とヘルプ」をタップ⇒「QR コード」をタップ

2 QRコードを読み込んで、単語帳を登録してください。



「QRコード」画面が表示されるので、「QRコード読み取り」をタップする。「カメラへのアクセスを求めています」が表示された場合は「OK」をタップする



カメラが起動するので、このQRコードを読み取る。読み取りが成功すると自動的に画面が切り替わる



単語帳の詳細画面が表示されるので、「追加する」をタップすると「でる語句200」の登録が完了する

※ Android の場合、QRコードが読み取りにくいことがあります。zuknow を一旦終了し、別の QRコード読み取りアプリを使うと、読み取ることができます。

「でる語句 200」を使った学習方法の例

1 「zuknow」を起動したら、画面下部にある「学習」をタップし、単語帳一覧にある「でる語句 200」を選んで学習画面を開いてください。



単語カードを使った暗記学習と、クイズ形式での暗記確認ができる

2 「カードで暗記する」をタップすると、単語カードを使った暗記学習ができます。



[?] をタップすると単語の意味が表示される。カードを左右にスワイプすると、前後の単語カードに移動できる。画面左上の[<] をタップすると 1 の画面に戻る

3 「クイズで確認する」をタップすると、クイズ形式による暗記確認ができます。



画面の上部に表示された単語の意味を、下部に表示されている4つの選択肢から選んで解答する

アプリの詳しい機能説明や操作方法

「zuknow」はたくさんの機能が搭載されています。機能紹介や使い方の詳細は、アプリ内の「ヘルプ」を参照してください。

「学習」画面で [...] ⇒ 「ヘルプ」の順にタップすると「ヘルプ」画面を表示できる。「スタートアップガイド」をタップすると、詳しい操作方法の解説が参照できる



「zuknow」の公式サイトでは、さらに様々な情報が掲載されているので、パソコンなどでアクセスしてご参照ください。

<http://www.zuknow.net/>

通知について

クイズの通知が1日に3回、アプリから届きます。この通知は、画面下部の「学習記録」⇒画面右上の歯車マークをタップして表示される画面の「プッシュクイズ」のスイッチをOFFにすることで止めることができます。

■注意事項■

- ・ zuknow は、株式会社ビズリーチが提供するサービスです。zuknow に関する質問・問い合わせなどは株式会社ビズリーチへお問い合わせください。
- ・ 本アプリに関するトラブルについて、株式会社インプレスは一切責任を負いかねますので、あらかじめご承知ください。
- ・ 単語帳「でる語句 200」の内容は、著作権法により保護されています。株式会社インプレスの許可を得ず、転載・複製・複製などはできません。

本書のご感想をぜひお寄せください

<http://book.impress.co.jp/books/1116101092>

「読者アンケートに答える」をクリックしてアンケートにぜひご協力ください。はじめての方は「CLUB Impress (クラブインプレス)」にご登録いただく必要があります。アンケート回答者の中から、抽選で商品券(1万円分)や図書カード(1,000円分)などを毎月プレゼント。当選は賞品の発送をもって代えさせていただきます。

読者登録
サービス

CLUB
IMPRESSIONS

登録カンタン
費用も無料!

アンケート回答で本書の読者登録が完了します

著者紹介

五十嵐 聡 (いがらし さとし)

1964年横浜市生まれ。60社を超えるIT系メーカーやソフトウェア企業などですべての区分をこなせる情報処理技術者試験対策などの講師として25,000名以上の指導実績がある。各研修先では、その指導力とキャラクターから常に高合格率を誇っている。

「情報処理試験用語集 (インプレス)」 「ITパスポートパーフェクトラーニング過去問題集 (技術評論社)」 など著書は60冊を超える。

STAFF

| | |
|--------|-------------|
| 編集 | 片元 論 |
| DTP | 株式会社トップスタジオ |
| 表紙デザイン | 馬見塚意匠室 |
| 編集長 | 玉巻秀雄 |

• 本書の内容に関するご質問は、書名・ISBN (このページの下に記載)・お名前・電話番号と、該当するページや具体的な質問内容、お使いの動作環境などを明記のうえ、インプレスカスタマーセンターまでメールまたは封書にてお問い合わせください。電話やFAX等のご質問には対応しておりません。なお、本書の範囲を超える質問に関しましてはお答えできませんのでご了承ください。

• 落丁・乱丁本はお手数ですがインプレスカスタマーセンターまでお送りください。送料弊社負担にてお取り替えさせていただきます。但し、古書店で購入されたものについてはお取り替えできません。

• 読者の窓口
インプレスカスタマーセンター
〒101-0051 東京都千代田区神田
神保町一丁目105番地
TEL 03-6837-5016 / FAX 03-6837-5023
info@impress.co.jp

• 書店／販売店のご注文窓口
株式会社インプレス 受注センター
TEL 048-449-8040
FAX 048-449-8041

徹底攻略 情報セキュリティマネジメント 過去問題集 平成29年度春期

2016年12月1日 初版発行

著 者 五十嵐 聡

発行人 土田米一

編集人 高橋隆志

発行所 株式会社インプレス

〒101-0051 東京都千代田区神田神保町一丁目105番地

TEL 03-6837-4635 (出版営業統括部)

ホームページ <http://book.impress.co.jp/>

本書は著作権法上の保護を受けています。本書の一部あるいは全部について、株式会社インプレスから文書による許諾を得ずに、いかなる方法においても無断で複写、複製することは禁じられています。

Copyright © 2016 Satoshi Igarashi, All rights reserved.

印刷所 日経印刷株式会社

ISBN978-4-295-00041-9

Printed in Japan

インプレスの書籍ホームページ

書籍の新刊や正誤表など最新情報を随時更新しております。

<http://book.impress.co.jp/>