

徹底攻略

内容充実で応援価格！

[定価]
本体 **1,780**円
+税

情報セキュリティ マネジメント 教科書

株式会社わくわくスタディワールド
瀬戸美月／齋藤健一 著

平成 **29** 年度
(2017年度) **春期** **秋期**

わく☆すたAIが
出題範囲を徹底分析！

電子版無料
ダウンロード！※

2大特典

スマホで学べる
単語帳アプリ
「でる語句200」付き※

さらに

過去問解説3回 + 模擬問題 付き

インプレス

売上No.1
出題傾向を押さえた
**SG対策の
決定版！**

*1 大手取次調べ (2015年12～2016年10月発売の同試験参考書において)

*2 ダウンロード提供3回分含む。過去問解説のうち平成29年度春期については試験日以降の提供を予定しています

インプレス情報処理シリーズ購入者限定特典!!

●電子版の無料ダウンロード

本書の全文の電子版（PDFファイル）を無料でダウンロードいただけます。
加えて、本書に掲載していない過去問題＆解説もダウンロードできます。

▼本書でダウンロード提供している過去問題解説

- ・平成28年度春期試験（著者生解説原稿をPDF化）
- ・平成29年度春期試験（著者生解説原稿をPDF化）

※解説のみの提供になります。試験問題はIPAサイトにてご入手ください。

※平成29年度春期試験の解説PDFダウンロード提供開始は【2017年5月2週目】を予定しています。

その時期にあらためて下記ダウンロードURLをご確認ください。

電子版は、以下のURL からダウンロードいただけます。

ダウンロードURL： <http://book.impress.co.jp/books/1116101091>

※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、無料の読者会員システム「CLUB Impress」への登録が必要となります。

●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

出題が予想される200の語句を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、510ページを参照ください。

※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。

※ダウンロード期間は、いずれも本書発売より1年間です。

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/>

- ・本書は、情報セキュリティマネジメント試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つとめました。著者、株式会社インプレスは本書の内容に基づく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。
- ・本文中の製品名およびサービス名は、一般に各開発メーカーおよびサービス提供元の商標または登録商標です。なお、本文中には©および®、™は明記していません。

はじめに

「ウイルス対策ソフト、邪魔だから止めておいた」、「スマホのアップデートなんて、しないでいいよね」、「お金ないし、Windows XPのままにしよう」などなど、世の中には、情報セキュリティ的に危険な考えをもつ人であふれています。しかし、インターネットが進歩して誰もが接続できるようになった今、情報セキュリティの不備は大きな被害を及ぼすこともありますし、人に迷惑をかけることもあります。

情報セキュリティマネジメント試験は、情報処理技術者試験の中でも他の技術者向けの試験とは異なり、**ITを利用する人向けの試験区分**です。企業や一般生活でITを使う上で必要な情報セキュリティの知識を身に付け、まわりの人々を助ける立場、そんな人のための試験となります。これからの時代に必要とされる人材ということで新設された試験ですので、合格を目指して学習することで、今の世の中に必要な、大切なスキルを身に付けることができます。

情報セキュリティマネジメント試験は午前試験と午後試験に分かれており、午前試験では情報セキュリティを中心としたIT全般に関する知識、午後試験では実際に情報セキュリティに関する事例を基に、問題を解決する技能が問われます。情報セキュリティマネジメント試験を受験する場合には、これらの両方に対応することが大切です。

本書は、情報セキュリティマネジメント試験の**合格に必要な内容を1冊にまとめたもの**です。1～7章までは午前対策を中心とした知識を学習していきます。各單元ごとに午前演習問題も用意しましたので、知識の定着の確認にお役立てください。第8章は午後問題対策として、午後問題の演習で問題の解き方・考え方を学んでいきます。また、付録として、情報セキュリティマネジメント試験の全解答解説を用意いたしました。平成28年秋期の問題は巻末付録で、それ以前(平成28年春期)の問題はPDF(左ページのダウンロードURL参照)で用意いたしましたので、問題演習にご活用ください。

加えて、平成29年春期の試験後には、試験内容に関する解答・解説もPDFで提供する予定です。さらに深く理解できるように動画による解説も用意していますので(P.17参照)、あわせてご活用ください。

学習するときには、ポイントを暗記するだけより、周辺知識も合わせて勉強する方が記憶に残りやすく実力も付いていきます。すべてを暗記しようと頑張らなくてもいいので、気楽に読み進めていきましょう。辞書として使っていただくのも歓迎です。本書をお供にしながら、情報セキュリティマネジメント試験の合格に向かって進んでいってください。

最後に、本書の発刊にあたり、企画・編集など本書の完成までに様々な分野で多大なるご尽力をいただきましたインプレスの皆様、ソキウス・ジャパンの皆様に感謝いたします。また、一緒に仕事をしてくださった皆様、「わく☆すたセミナー」や企業研修での受講生の皆様のおかげで、本書を完成させることができました。皆様、本当に、ありがとうございました。

平成28年11月

わくわくスタディワールド 瀬戸 美月・齋藤 健一

CONTENTS

目次

はじめに.....	3
合格のポイント	10

第1章 情報セキュリティの基礎知識

1-1 情報セキュリティとは	20
1-1-1 情報セキュリティの目的と考え方	20
1-1-2 情報セキュリティの重要性	24
1-1-3 不正のメカニズム	26
1-1-4 演習問題	29
1-2 サイバー攻撃手法	31
1-2-1 サイバー攻撃手法	31
1-2-2 演習問題	40
1-3 情報セキュリティに関する技術	47
1-3-1 暗号化技術	47
1-3-2 認証技術	56
1-3-3 公開鍵基盤	67
1-3-4 演習問題	71

第2章 情報セキュリティ管理

2-1 情報セキュリティマネジメント	80
2-1-1 情報セキュリティ管理	80
2-1-2 情報セキュリティ諸規程	82
2-1-3 情報セキュリティマネジメントシステム	84
2-1-4 情報セキュリティ継続	89
2-1-5 演習問題	91

2-2 リスクマネジメント.....95

2-2-1 情報資産の調査・分類.....	95
2-2-2 リスクの種類.....	96
2-2-3 情報セキュリティリスクアセスメント.....	98
2-2-4 情報セキュリティリスク対応.....	101
2-2-5 演習問題.....	104

2-3 情報セキュリティに対する取組み.....108

2-3-1 情報セキュリティ組織・機関.....	108
2-3-2 セキュリティ評価.....	113
2-3-3 演習問題.....	118

第3章 情報セキュリティ対策**3-1 人的セキュリティ対策.....124**

3-1-1 人的セキュリティ対策.....	124
3-1-2 演習問題.....	129

3-2 技術的セキュリティ対策.....134

3-2-1 不正アクセス対策.....	134
3-2-2 マルウェア・不正プログラム対策.....	138
3-2-3 その他の技術的セキュリティ対策.....	140
3-2-4 セキュリティ製品・サービス.....	146
3-2-5 演習問題.....	148

3-3 物理的セキュリティ対策.....157

3-3-1 物理的セキュリティ対策.....	157
3-3-2 演習問題.....	161

3-4 セキュリティ実装技術.....163

3-4-1 セキュアプロトコル.....	163
3-4-2 ネットワークセキュリティ.....	165
3-4-3 データベースセキュリティ.....	169
3-4-4 アプリケーションセキュリティ.....	171
3-4-5 演習問題.....	173

第4章 法務

4-1 情報セキュリティ関連法規 178

4-1-1 サイバーセキュリティ基本法	178
4-1-2 不正アクセス禁止法	180
4-1-3 個人情報保護法	182
4-1-4 刑法	187
4-1-5 その他のセキュリティ関連法規・基準	189
4-1-6 演習問題	192

4-2 その他の法規・標準 200

4-2-1 知的財産権	200
4-2-2 労働関連・取引関連法規	202
4-2-3 その他の法律・ガイドライン・技術者倫理	206
4-2-4 標準化関連	208
4-2-5 演習問題	210

第5章 マネジメント

5-1 システム監査 216

5-1-1 システム監査	216
5-1-2 内部統制	222
5-1-3 演習問題	225

5-2 サービスマネジメント 231

5-2-1 サービスマネジメント	231
5-2-2 サービスの設計・移行	234
5-2-3 サービスマネジメントプロセス	235
5-2-4 サービスの運用	240
5-2-5 ファシリティマネジメント	243
5-2-6 演習問題	244

5-3 プロジェクトマネジメント..... 248

5-3-1	プロジェクトマネジメント	248
5-3-2	プロジェクト統合マネジメント	252
5-3-3	プロジェクトステークホルダマネジメント	253
5-3-4	プロジェクトスコープマネジメント	254
5-3-5	プロジェクト資源マネジメント	257
5-3-6	プロジェクトタイムマネジメント	258
5-3-7	プロジェクトコストマネジメント	261
5-3-8	プロジェクトリスクマネジメント	264
5-3-9	プロジェクト品質マネジメント	266
5-3-10	プロジェクト調達マネジメント	268
5-3-11	プロジェクトコミュニケーションマネジメント	269
5-3-12	演習問題	270

第6章 テクノロジ**6-1 ネットワーク..... 276**

6-1-1	ネットワーク方式	276
6-1-2	データ通信と制御	278
6-1-3	通信プロトコル	282
6-1-4	ネットワーク管理	289
6-1-5	ネットワーク応用	290
6-1-6	演習問題	294

6-2 データベース..... 298

6-2-1	データベース方式	298
6-2-2	データベース設計	300
6-2-3	データ操作	302
6-2-4	トランザクション処理	305
6-2-5	データベース応用	310
6-2-6	演習問題	312

6-3 システム構成要素..... 317

6-3-1	システムの構成	317
6-3-2	システムの評価指標	326
6-3-3	演習問題	329

第7章 ストラテジ

7-1 企業活動 334

7-1-1	経営・組織論	334
7-1-2	OR・IE	338
7-1-3	会計・財務	343
7-1-4	演習問題	349

7-2 システム戦略 353

7-2-1	情報システム戦略	353
7-2-2	業務プロセス	356
7-2-3	ソリューションビジネス	358
7-2-4	システム活用促進・評価	360
7-2-5	演習問題	361

7-3 システム企画 363

7-3-1	システム化計画	363
7-3-2	要件定義	365
7-3-3	調達計画・実施	367
7-3-4	演習問題	371

第8章 午後問題対策

8-1 午後問題の解き方 374

8-1-1	午後問題の解き方	374
-------	----------------	-----

8-2 午後問題の演習 393

8-2-1	内部不正防止のためのログのレビュー	393
8-2-2	標的型攻撃メールの脅威と対策	403
8-2-3	情報セキュリティ自己点検	416

付録 平成28年度秋期 情報セキュリティマネジメント試験

午前	問題	433
午前	解答と解説	447
午後	問題	459
午後	解答と解説	484

索引	496
「でる語句200」の使い方	510



生体認証の落とし穴	66
最適な対策と現実との兼ね合い	103
IPAの取組みを押さえておく	117



合格のポイント

情報セキュリティマネジメント試験とは

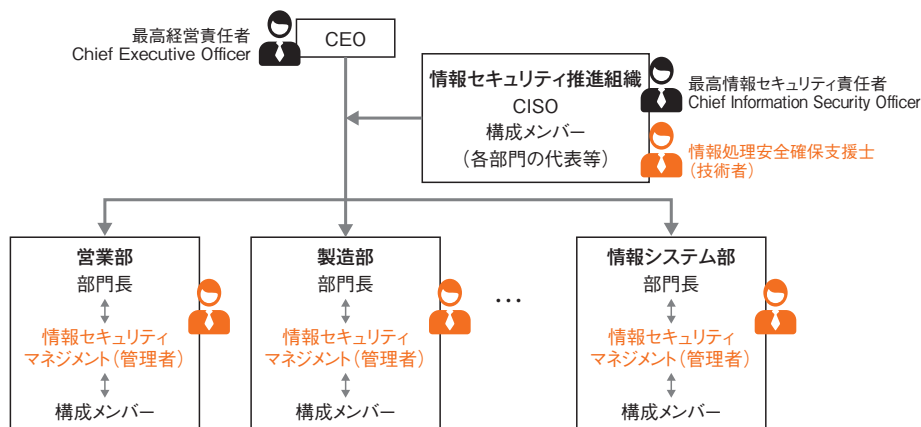
情報セキュリティマネジメント試験は、情報セキュリティの基本的な知識やスキルを問う試験です。

会社などの組織の情報セキュリティを確保するために設立された試験ですが、情報セキュリティ専門の部署ではなく、**情報セキュリティの利用部門において、情報セキュリティリーダーとして活躍する人を対象**としています。

利用部門の情報セキュリティマネジメントを行い、その部門における情報セキュリティ対策をリードしていく役割を担います。そのような人が、情報セキュリティやその周辺分野に関する知識やスキルを身につけるための試験が、情報セキュリティマネジメント試験なのです。

情報セキュリティマネジメント試験と 情報処理安全確保支援士試験の違い

平成29年度春期より開始される情報処理安全確保支援士試験は、情報セキュリティ専門家の国家資格である情報処理安全確保支援士として登録するための試験です。情報セキュリティマネジメント試験とは役割が異なり、会社組織での位置付けは、次のようになります。



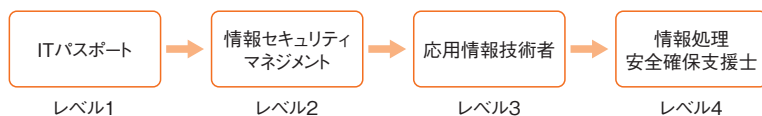
会社・組織での情報セキュリティの推進体制

情報セキュリティは組織全体で確保していくもので、組織全体を管理するのが情報セキュリティ推進組織です。CISO（Chief Information Security Officer：最高情報セキュリティ責任者）が全社を統括し、各部門に情報セキュリティのルールを守らせます。このときに、CISOの右腕となり、情報セキュリティのスペシャリストとして全社を統括するのが情報処理安全確保支援士となります。それに対し、利用部門の情報セキュリティリーダーは、それぞれの部門内の情報セキュリティマネジメントを推進します。情報セキュリティマネジメント試験は、この情報セキュリティリーダーのための試験です。

情報セキュリティマネジメント試験の活用方法

情報処理技術者試験での情報セキュリティマネジメント試験の位置づけは、入門資格であるITパスポート試験の上位の試験であり、ITを利用する人が対象です。IPA（独立行政法人情報処理推進機構）が発表する共通キャリア・スキルフレームワークではレベル2に相当し、これは技術者向けの試験である基本情報技術者試験と同等のレベルです。IT関連の技術者ではない利用者向けとしては、情報セキュリティマネジメント試験が一番上位の試験となっています。一般的な事務などの業務を行う人がこの試験に合格することによって、今の時代に役立つIT関連の知識をもっていることを証明できます。

また、先ほどの情報処理安全確保支援士は、共通キャリア・スキルフレームワークではレベル4に相当しますので、情報セキュリティマネジメント試験とは役割とレベルが大きく異なります。といっても同じ情報セキュリティに関する国家試験ですので、最終的に情報処理安全確保支援士を目指すにあたってのステップアップとしても、情報セキュリティマネジメント試験は活用できます。情報セキュリティのスペシャリストとしてステップアップしていく場合は、次のように試験を活用していくのが一般的です。



初心者から情報セキュリティのスペシャリストへのステップアップ手順

情報セキュリティマネジメント試験の形式と合格率

情報セキュリティマネジメント試験は、春期と秋期の年2回実施されます。次のような形式で、午前試験、午後試験に分けて実施されます。

	試験時間	出題形式	出題数・解答数	合格ライン
午前	9:30～11:00 (90分)	多岐選択式 (四肢択一)	出題数：50問 (全問解答)	60点／100点満点 (30問正解)
午後	12:30～14:00 (90分)	多岐選択式	出題数：3問 (全問解答)	60点／100点満点 (各問34点満点)

※午後は1問当たり34点の配点ですが、得点の上限は100点です。

以下に、過去2回の午前、午後での合格ラインを突破した割合(突破率)と、全体の合格率を示します。合格の条件は、午前、午後ともに合格ラインを突破することです。

○午前・午後の突破率と合格率

突破率	平成28年春	平成28年秋
午前	94.3%	78.9%
午後	90.8%	80.9%
全体	88.0%	80.4%

※情報処理技術者試験センター公表の統計情報を基に算出

午前の試験では知識を問うことによって、午後の試験では技能を問うことによって評価されます。基本的に難易度は、午前より午後の方が難しく、特に情報セキュリティマネジメントは考え方の理解が合否の一番のポイントになります。ただし、午前では情報セキュリティだけでなく情報技術全般に関する基本的な用語や内容が問われますので、全体的にしっかり学習しておくことが大切です。

■ 午前試験の傾向

情報セキュリティマネジメント試験の午前試験では50問が出題され、全問必須です。本書で学習するすべての分野から幅広く出題されます。

○午前の出題分野

分野	大分類	中分類	平成28年春	平成28年秋
テクノロジー系	技術要素	セキュリティ	29	30
		ネットワーク	2	1
		データベース	1	2
	コンピュータシステム	システム構成要素	1	1
マネジメント系	サービスマネジメント	システム監査	4	4
	プロジェクトマネジメント	サービスマネジメント	2	2
		プロジェクトマネジメント	1	1
ストラテジ系	企業と法務	法務	6	6
		企業活動	1	1
	システム戦略	システム戦略	2	1
		システム企画	1	1

重点分野は専門分野であるセキュリティ以外に**法務**が指定されています。さらに、傾向としては**システム監査**(情報セキュリティ監査を含む)の分野からの出題が多く、この3分野だけで50問中40問が出題されています。本書でいうと、セキュリティは第1～第3章、法務は第4章、システム監査は第5章の5-1に該当します。このように、本書では前半で解説している分野について特によく出題されますので、まずは先頭から順番に学習していくことが効率的です。

それに対し、テクノロジー系やストラテジ系などの他の分野は、ほぼ1問ずつの出題です。特にテクノロジー系に関しては、利用者向けの試験ということもあり、技術的に難しい内容は出題されません。全体的にざっくり学習して概要をつかむ程度で問題はないと考えられます。

午後試験の傾向

情報セキュリティスペシャリスト試験の午後試験では3問が出題され、全問必須です。会社などでの業務における事例を基に、情報セキュリティ対策を考えていきます。

過去2回の出題テーマとその概要は以下のとおりです。

○午後の出題分野

年度期	問	出題テーマ	概要
平成28年春	1	標的型攻撃メールの脅威と対策	販売代理店Y社での標的型攻撃メールによるマルウェア感染と、それをきっかけにした情報セキュリティ意識向上
	2	業務委託によるアクセス制御	通信販売業者A社がB社に業務委託する際のアクセス制御とその内容変更
	3	情報セキュリティ自己点検	投資コンサルティング会社R社海外営業部の情報セキュリティ監査をCSA（統制自己評価）により実施
平成28年秋	1	オンラインストレージサービスの利用	電気機器メーカーJ社でのオンラインストレージサービス利用時の情報公開事故について、原因調査と対策の検討
	2	情報機器の紛失	生命保険会社Z社でのノートPC入りかばんの置き忘れ事故についてのインシデント対応
	3	業務用PCでのWebサイト閲覧	健康食品製造会社P社での不審なアクセスについてのインシデント対応と全社的な改善

午後では、午前の知識を基に、実際に情報セキュリティマネジメントを行うことができるかどうかの技能が問われます。そのため、組織の事例を基に、問題点や対処法などについて出題されます。

各問とも文章が長文であり、的確に読みこなす必要があるため、**国語力も重要**となります。ただし、記述式ではなく多肢選択式なので、文章の記述は不要です。

用語の意味などの知識はあまり問われず、情報セキュリティの考え方にに基づき適切に対処する方法が問われます。用語の暗記だけでは通用しないのが午後試験ですので、一つ一つの用語について、実務での利用方法も合わせて丁寧に理解しておくことが合格のポイントになります。

合格のための勉強法

試験合格のために勉強計画を立てる上で最も大切なのは、**自分の現状を知ること**です。IT系の学習の場合、いわゆる机上の“お勉強”以外にも、日々の生活や仕事が学びにつながっていることはよくあります。そのため、自分がすでに知っていることの勉強は飛ばして、知らないことを中心に知識を身に付けることができれば、効率良く学習することが可能です。

情報セキュリティマネジメント試験の場合、大きく分けて次の三つの力が重要になってきます。

1. 情報技術全般(情報セキュリティ関連分野)の基礎的な知識
2. 情報セキュリティに関する基礎的な知識
3. 情報セキュリティマネジメントに関する技能(考え方の理解)

まず、1についてですが、基本的に、情報セキュリティマネジメント試験の受験はITパスポート試験合格レベルが前提なので、そこからのステップアップを考えます。ITパスポート試験での基礎の上に専門知識を積み重ねていきますので、ITパスポート試験の勉強をされていない方は、まずはそこからスタートするのが効率的です。ITパスポート試験はCBT(Computer Based Testing)方式で、他の情報処理技術者試験と異なり、いつでも受験可能ですので、情報セキュリティマネジメント試験の前に受験して、合格することも可能です。

2については、情報セキュリティに関する知識は、学習すれば確実に身に付きます。情報セキュリティマネジメントシステムなどのマネジメント方法や、暗号化・認証方式、アクセス制御などの技術的な内容を、参考書などでまんべんなく学習していくことが大切です。

3については、技能は知識の学習だけでは対応できませんので、実務や午後問題の演習などで体得していくことになります。考え方の理解がポイントで、机上の勉強以外にも、様々な実務や経験が助けになります。

情報セキュリティマネジメント試験の勉強法の王道は、**参考書を1冊しっかりマスターすること**です。知識を身に付けた後に、過去問題で問題演習を行うことで、今まで学習したことを定着させることができます。

本書では、各章ごとに午前の演習問題を掲載し、巻末には平成28年秋期の過去問題とその解答解説を掲載しています。さらに、平成28年春期の問題についても解答解説を用意しています(PDFで提供)。また、平成29年度春期の試験後には、最新の解答解説を掲載(PDFで提供)しますので、ご活用ください。

■ 本書の使い方

本書では、過去問題やシラバスの内容を分析し、試験に出てくる分野をまとめてあります。ですから、本書を全部読んで頭に入れていただければ、試験に合格するための知識は十分に身に付きます。そのときに、單元ごとにある演習問題を考えながら読み進んでいただくことで、知識が定着することの助けになります。

また、文章を読むのが苦手な方、特に、参考書を読み続けるのがつらいという方は、**無理に最初から全部読む必要はありません**。過去問題などで問題演習を行いながら、辞書として必要なことを調べるといった用途に使っていただいてもOKです。用語を調べつつ周辺の知識も身に付ければ、効率良く勉強していただけたと思います。

さらに、試験直前に少しでも勉強しておきたい方は、重要用語を赤字で示しておきましたので、それだけでも学習してみてください。ポイントを押さえて学習することで、より速く、必要な知識を学習することができます。ただし、重要ポイントだけを覚えるという学習方法は忘れやすい面もありますので、できれば、それ以外の部分も含めて読みながら学習していただくのがおすすめです。

また、第8章では、IPAが公表しているサンプル問題と過去問題を例に、午後問題の解き方を解説しています。学習してきたことの力試しに、出題の傾向の確認に、ぜひお役立てください。

■ 本書のフォローアップ

本書の訂正情報につきましては、インプレスのサイトをご参照ください。内容に関するご質問は、「お問い合わせフォーム」よりお問い合わせください。

●お問い合わせと訂正ページ

<http://book.impress.co.jp/books/1116101091>

上記のページで「お問い合わせフォーム」ボタンをクリックしますとフォーム画面に進みます。

また、情報セキュリティは変化の激しい技術ですし、日々新しい情報が公開されています。そのため、新情報などのフォローアップを下記のサイトで行っていきます。情報セキュリティ技術やネットワーク技術などの**動画解説**も併せて掲載し、順次更新していきますので、ぜひご活用ください。

徹底攻略情報セキュリティマネジメント教科書 書籍関連情報

<http://www.wakuwakustudyworld.co.jp/blog/sginfo/>

それでは、試験合格に向けて、楽しく勉強を進めていきましょう。

第 1 章

情報セキュリティの 基礎知識

情報セキュリティマネジメントを学ぶ際の基本は、情報セキュリティ全般の基礎知識についての学習です。

この章ではまず、情報セキュリティの考え方や概要を理解します。その後、現在行われている典型的なサイバー攻撃の手法について学びます。さらに、情報セキュリティに関する技術として、暗号化や認証、公開鍵基盤 (PKI) の基本的な内容を学習していきます。

1-1 情報セキュリティとは

- ◆ 1-1-1 情報セキュリティの目的と考え方
- ◆ 1-1-2 情報セキュリティの重要性
- ◆ 1-1-3 不正のメカニズム
- ◆ 1-1-4 演習問題

1-2 サイバー攻撃手法

- ◆ 1-2-1 サイバー攻撃手法
- ◆ 1-2-2 演習問題

1-3 情報セキュリティに関する技術

- ◆ 1-3-1 暗号化技術
- ◆ 1-3-2 認証技術
- ◆ 1-3-3 公開鍵基盤
- ◆ 1-3-4 演習問題

1-1 情報セキュリティとは

情報セキュリティマネジメントを学ぶ上では、情報セキュリティの基本を理解することが不可欠です。ここでは、情報セキュリティの基礎知識と、情報セキュリティマネジメントとの関連について学んでいきます。



勉強のコツ

情報セキュリティマネジメントでは、細かい知識よりも“考え方”を身に付けることが大切です。実際の事例を知ること、午後の問題演習を繰り返し行うことなどを通して、考え方をしっかり学んでいきましょう。

1-1-1 情報セキュリティの目的と考え方

情報セキュリティというと、「暗号化する」「ファイアウォールを設置する」など技術的な対策を思い浮かべがちですが、実は、情報セキュリティには経営寄りの考え方が不可欠です。

情報セキュリティとは

セキュリティとは、家の施錠や防犯カメラの設置なども含めた、安全を守る対策全般のことです。このうち情報セキュリティで取り上げられるのは、コンピュータの中のデータや顧客情報や技術情報など、情報に対するセキュリティです。“情報”は一般の防犯とは別の守りにくさがあるため、特別に取り扱う必要があるのです。

情報セキュリティは技術だけで確保できるものではありません。組織全体のマネジメントも含めて全体的に対策を考える必要があります。そのため、情報セキュリティ対策を行うときには、これから学習する情報セキュリティマネジメントについて理解することが不可欠となります。

情報セキュリティのポイント

セキュリティを考えたときのポイントは、**モレなく、全員で、当たり前を確認に行う**ことです。これが、情報セキュリティマネジメントの基本的な考え方となります。

情報セキュリティは、ファイアウォールの導入や暗号化といった技術的な対策だけでは確保できません。ファイアウォールで社内のネットワークを守っても、その社内の人間が機密データを窃取することは十分に考えられます。実際、情報セキュリティ犯

罪の多くは、社員などの内部関係者が主導したり協力したりすることで成立しています。

また、会社などの組織では、技術者だけでなく一般社員などITに詳しくない人も情報システムを利用します。暗号化するのを忘れたり、パスワードを書いた紙を見られるなど、個人のミスが情報漏えいにつながることもあります。そのため、組織の全員で、守るべきルール(情報セキュリティポリシー)などを決めて、**守るための仕組みをつくる**ことが重要です。



■ 情報セキュリティの目的と考え方

情報セキュリティマネジメントに関する要求事項を定めたJIS Q 27001 (ISO/IEC 27001)では、情報セキュリティを確保するためのシステムである情報セキュリティマネジメントシステム(ISMS)について次のように説明しています。

「ISMSの採用は、組織の戦略的決定である。組織のISMSの確立及び実施は、その組織のニーズ及び目的、セキュリティ要求事項、組織が用いているプロセス、並びに組織の規模及び構造によって影響を受ける。」

つまり、『**組織の戦略によって決定され、組織の状況によって変わる**』というのが情報セキュリティの考え方です。

用語

情報セキュリティの言葉の定義や基本的な考え方については、JIS (Japanese Industrial Standards: 日本工業規格)の様々な規格で定められています。情報セキュリティマネジメントに関しては、JIS Q 27001やJIS Q 27002に定義されており、これらの規格が情報セキュリティマネジメントの基準となります。

情報セキュリティの定義

情報セキュリティについては、JIS Q 27000 (ISO/IEC 27000) に、**情報の機密性、完全性及び可用性を維持すること**と定義されています。この三つの要素の正確な定義は次のとおりです。



囲み内は、JIS規格に記載されている厳密な定義です。少し言い回しが難しいですが、原文はこのように掲載されています。



機密性、完全性、可用性は、この三つの頭文字をとって**CIA**とも呼ばれます。単に情報を見られないこと(機密性)を考えるだけでなく、他の二つのポイントも考慮してバランスよく守ることが大切です。



企業活動の目的は、事業を継続して利益を出すことです。そのため、流出すると損失を出すおそれがあるものを保護し、利益を確保して事業を継続させるために、情報セキュリティを確保します。

そのときの視点として、情報を隠す機密性だけでなく完全性や可用性も見落とさないようにしようというのが、情報セキュリティの3要素(CIA)の考え方です。



ここでのエンティティとは、独立体、認証される1単位を指します。具体的には、認証される単位であるユーザや機器、グループなどのことです。



機密性、可用性はほぼ日本語で表現されますが、完全性だけは**インテグリティ**と英語で出てくることが多いので、押さえておきましょう。

①機密性 (Confidentiality)

認可されていない個人、エンティティまたはプロセスに対して、情報を使用させず、また、開示しない特性

②完全性 (Integrity : インテグリティ)

資産の正確さ及び完全さの特性

③可用性 (Availability)

認可されたエンティティが要求したときに、アクセス及び使用が可能である特性

機密性を維持するとは、許可した人以外には情報を見られないようにすることです。具体的には、暗号化や施錠などで情報を見られないように隠すことなどが機密性の対策です。

完全性を維持するとは、情報を書き換えられないようにすることです。具体的には、Webページが改ざんされないように、サーバへのアクセスを制限するなどが完全性の対策です。

可用性を維持するとは、情報をいつでも見られるようにすることです。具体的には、サーバが故障してデータが見られなくなることがないようにサーバを二重化するなどが可用性の対策です。

さらに、次の四つの特性も情報セキュリティの要素に含めることがあります。

④真正性 (Authenticity)

主体または資源が、主張どおりであることを確実にする特性

⑤責任追跡性 (Accountability)

あるエンティティの動作が、一意に追跡できる特性

⑥否認防止 (Non-Repudiation)

ある活動または事象が起きたことを、後になって否認されないように証明する能力

⑦信頼性 (Reliability)

意図した動作及び結果に一致する特性

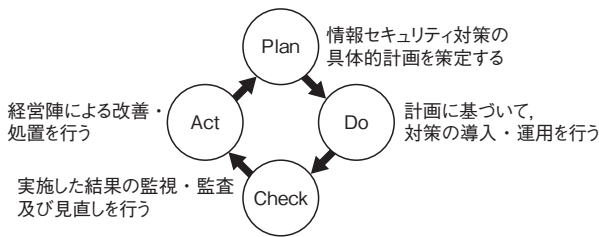
■ 情報セキュリティマネジメントシステム

情報セキュリティに取り組む上で大切なことは、情報を守るための対策をシステム化して継続的に改善していくことです。「がんばって守ろう!」というかけ声だけではどうがんばればいいのか分かりませんし、はじめから完璧に守れるわけではないので、徐々に改善していく必要があります。

組織の情報セキュリティの確保に体系的に取り組むことを情報セキュリティマネジメントといい、そのための仕組みを、**ISMS** (Information Security Management System: 情報セキュリティマネジメントシステム) といいます。ISMSでは、情報セキュリティ基本方針を基に、次のような**PDCAサイクル**を繰り返します。



ISMSの詳細な内容については、「2-1-3 情報セキュリティマネジメントシステム」で詳しく学習していきます。



ISMSのPDCAサイクル

ISMSの構築方法や要求事項などはJIS Q 27001 (ISO/IEC 27001) に示されており、これを基準にそれぞれの組織でISMSを構築していきます。

また、どのようにISMSを実践するかという実践規範はJIS Q 27002 (ISO/IEC 27002) に示されています。

▶▶ 覚えよう!

- ☐ 情報セキュリティとは、機密性、完全性、可用性を守ること
- ☐ 各組織で、情報セキュリティマネジメントシステムを構築し、PDCAサイクルを回す



発展

情報セキュリティで守るものは情報資産であり、その守り方は資産の金銭的価値などで決まります。

具体的には、すべての情報資産を最高レベルのセキュリティで守るのではなく、情報資産それぞれの価値に応じた最適な守り方をすることになります。すべての資産を守るのは難しいので、優先度を考えることも大切なセキュリティマネジメントです。



関連

情報資産の洗い出しについては、「2.2.1 情報資産の調査・分類」で詳しく解説します。

1-1-2 情報セキュリティの重要性

情報セキュリティマネジメントによって守るものは、情報資産です。情報資産ごとに、その脅威と脆弱性を洗い出し、どのように守るのかを決めていきます。

情報資産

企業の業務に必要な価値のあるものを資産といいますが、資産には、商品や不動産など形のあるものだけでなく、顧客情報や技術情報、人の知識や記憶などの**情報資産**も含まれます。



企業や自治体などの組織は、様々な情報資産を保持しています。どのような情報資産があるのかを洗い出して把握し、それぞれの資産に合わせた対策を考えることが大切です。

脅威

脅威とは、システムや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**です。インシデントとは、望まれていないセキュリティの現象(事象)で、組織の事業を危うくするおそれがあるものです。

脅威は、人為的(意図的、偶発的)なものと環境的なものに分類されます。具体的には、次のようなものがあります。

・人為的(意図的)な脅威

盗聴, 改ざん, 不正アクセス, 盗難, なりすまし, サービス不能, ウイルス感染など

・人為的(偶発的)な脅威

ケアレスミス, プログラムのバグ, 誤ったファイルの削除など

・環境的な脅威

地震, 洪水, 落雷, 火災, 台風など

■ 脆弱性

脆弱性とは, 脅威がつけ込むことができる, 資産がもつ弱点です。例えば, 施錠していない部屋にコンピュータを保管しているという脆弱性があることによって, 盗難などの脅威が起こる可能性が生じます。

■ リスク

リスクとは, ある脅威が脆弱性を利用して損害を与える可能性です。それぞれの情報資産について, その**脅威**を洗い出し, **脆弱性**を考慮することによってリスクの大きさを推定します。このことを, リスクアセスメントといいます。一般的に, 情報セキュリティリスクの大きさは, 次のような式で表されます。



用語

具体的な脅威や脆弱性, リスクの洗い出しや, リスク対応のために, **リスクアセスメント**を行います。詳しくは, 「2-2 リスクマネジメント」で改めて取り扱います。

情報セキュリティリスクの大きさ

＝情報資産の価値×脅威の大きさ×脆弱性の度合い

▶▶ 覚えよう!

- ☐ 情報資産とは, 企業の業務に必要な価値あるもの全般
- ☐ ある脅威が脆弱性を利用して損害を与える可能性がリスク

1-1-3 不正のメカニズム

不正行為は、機会、動機、正当化の不正のトライアングルが揃ったときに発生します。また、情報セキュリティの攻撃者の種類や動機には様々なものがあります。



発展

不正などの犯罪が起こらないようにするためには、以前は犯罪原因論といって、犯罪の原因をなくすことに重点をおく考え方が主流でした。現在では、犯罪機会論といって、犯罪を起こしにくくするように環境を整備する方向でも、犯罪予防が考えられています。

不正のメカニズム

米国の犯罪学者であるD.R.クレッシーが提唱している**不正のトライアングル理論**では、人が不正行為を実行するに至るまでには、次の三つの不正リスク（不正リスクの3要素）が揃う必要があると考えられています。

①機会

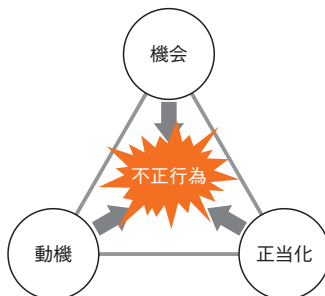
不正行為の実行が可能、または容易となる環境のことです。例えば、情報システム管理者にすべての権限が集中しており、チェックが働かないなどの状況が挙げられます。

②動機

不正行為を行うための事情のことです。例えば、借金がある、給料が不当に低いなどの状況が挙げられます。

③正当化

不正行為を行うための良心の呵責を乗り越える理由のことです。例えば、お金を盗むのではなく借りるだけ、と自分に言い訳をすることなどが挙げられます。



不正のトライアングル

不正のトライアングルを考慮して犯罪を予防する考え方の一つに、英国で提唱された状況的犯罪予防論があります。**状況的犯罪予防**では、次の五つの観点から、犯罪予防の手法を整理しています。

1. 物理的にやりにくい状況を作る
2. やると見つかる状況を作る
3. やっても割に合わない状況を作る
4. その気にさせない状況を作る
5. 言い訳を許さない状況を作る

■ 攻撃者の種類

情報セキュリティに関する攻撃者と一口にいても、様々な種類の人がいます。代表的な攻撃者の種類は、次のようなものです。

① スクリプトキディ

インターネット上で公開されている簡単なクラッキングツールを利用して不正アクセスを試みる攻撃者です。他人の台本どおりにしか攻撃しない幼稚な攻撃者という意味合いが込められています。



用語

クラッキングとは、ネットワークの不正利用全般のこと、システムの不正侵入や破壊・改ざんなどの悪用がそれに当たります。

② ボットハーダー

ボットを統制してボットネットとして利用することでサイバー攻撃などを実行する攻撃者のことです。



用語

ボットとは口ボットの略称で、もともとは人間が行っていた作業を代わりに実行するプログラムを指します。ボットネットとは、多数のボットが連携して構成されるネットワークです。

③ 内部関係者

従業員や業務委託先の社員など、組織の内部情報にアクセスできる権限を不正に利用して情報を持ち出したり改ざんしたりする攻撃者のことです。

④ 愉快犯

人や社会を恐怖に陥れて、その様子を観察して喜ぶことを目的にサイバー犯罪を行う攻撃者のことです。

⑤詐欺犯

フィッシング詐欺や本物そっくりのWebサイトなどで個人情報などを窃取するような詐欺を行う攻撃者のことです。

⑥故意犯

罪を犯す意志をもって犯罪を行う攻撃者が故意犯です。逆に、犯罪を行う意志がないのに注意義務を怠るなどの過失によって罪を犯してしまう攻撃者のことを過失犯といいます。

■ 攻撃の動機

情報セキュリティ攻撃の動機にも、様々なものが考えられます。代表的な攻撃の動機には、次のようなものがあります。

①金銭奪取

金銭的に不当な利益を得ることを目的に行われる攻撃です。個人情報など金銭につながる情報を得ることも含まれます。



ハッカーとは、コンピュータや電子回路などについて技術的に深い知識をもち、その技術を用いて技術的な課題を解決する人のことを指します。その行為をハッキングといいます。不正アクセスを行う場合には、ハッカーではなくクラッカーと言い換えることも多いです。

②ハクティビズム

ハクティビズムはハッカーの思想のことで、政治的・社会的な思想に基づき積極的にハッキングを行います。

③サイバーテロリズム

ネットワークを対象に行われるテロリズムです。人に危害を与える、社会機能に打撃を与える、といった深刻かつ悪質な攻撃のことを指します。

▶▶ 覚えよう！

- ☐ 不正は、機会・動機・正当化のトライアングルが揃うと起こる
- ☐ 攻撃者には、スクリプトキディ、ボットハーダー、内部関係者など、様々なパターンがある

1-1-4 演習問題

問1 “完全性”を脅かす攻撃

CHECK ▶ ☐☐☐

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2 スクリプトキディ

CHECK ▶ ☐☐☐

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。

問3 不正のトライアングル

CHECK ▶ ☐☐☐

“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、アカウントینگ |

■ 解答と解説

問1

(平成28年秋 情報セキュリティマネジメント試験 午前 問21)

《解答》ア

情報の“完全性”とは、資産の正確さ及び完全さを保護する特性です。Webページの改ざんは、Webページという資産の正確さを脅かす攻撃なので、アが正解です。

イ、エは“機密性”、ウは“可用性”を脅かす攻撃となります。

問2

(平成28年秋 情報セキュリティマネジメント試験 午前 問24)

《解答》イ

スクリプトキディとは、インターネット上で公開されている簡単なクラッキングツールを利用して不正アクセスを試みる攻撃者です。技術不足なので新しい攻撃手法を考え出すことはできませんが、公開された方法を利用することはできるので、イが正解です。

ア、ウはソーシャルエンジニアリングの行為です。エは故意犯の行為に該当します。

問3

(平成28年春 情報セキュリティマネジメント試験 午前 問9)

《解答》ア

“不正のトライアングル”理論では、不正行為は、機会、動機、正当化という3要素の不正リスクがそろったときに起きると言われています。したがって、アが正解です。

イ 情報セキュリティの3要素です。

ウ 3C分析の三つの視点です。

エ AAA (Authentication, Authorization, Accounting) と略される、三つの異なるセキュリティ機能の枠組みです。

1-2 サイバー攻撃手法

1

情報セキュリティ攻撃、いわゆるサイバー攻撃には様々な攻撃手法があります。代表的な手法を知っておくことは、情報セキュリティ対策に不可欠です。

1-2-1 サイバー攻撃手法

サイバー攻撃には様々なものがあり、日々進化しています。ここで、近年流行している代表的なサイバー攻撃を見ていきます。

■ パスワードに関する攻撃

パスワードを不正に取得してアクセスするための攻撃です。パスワードクラックともいいます。代表的な攻撃手法には、次のようなものがあります。

①ブルートフォース攻撃(総当たり攻撃)

適当な文字列を組み合わせる力任せにログインの試行を繰り返す攻撃です。

②辞書攻撃

辞書に出てくる用語を順に使用してログインを試みる攻撃です。

③スニффイング

盗聴することでパスワードを知る方法です。

④リプレイ攻撃

パスワードなどの認証情報を送信しているパケットを取得し、それを再度送信することでそのユーザになりすます攻撃です。パスワードが暗号化されていても使用できます。

⑤パスワードリスト攻撃

他のサイトで取得したパスワードのリストを利用して不正ログインを行う攻撃です。



サイバー攻撃の手法はどんどん進化しています。最新の情報は、IPA セキュリティセンターのWebサイト <http://www.ipa.go.jp/security/> に掲載されていますので、定期的に確認しておきましょう。



パスワードリスト攻撃は、例えば他のWebサイトで登録していたIDとパスワードで、TwitterやGoogleなどにログインしてみるという攻撃です。パスワードをサイト間で同じものにしてしまうと狙われやすくなります。対策としては、Webサイトごとに異なるパスワードにしておく方法が有効です。



レインボー攻撃に関するハッシュ値については、「1.3 情報セキュリティに関する技術」で詳しく取り扱います。詳しい内容はそちらを参考にしてください。

⑥レインボー攻撃

パスワードがハッシュ値で保管されている場合に、あらかじめパスワードとハッシュ値の組合せリスト(レインボーテーブル)を用意しておき、そのリストと突き合わせてパスワードを推測し不正ログインを行う攻撃です。

■マルウェアをインストールする攻撃

マルウェアとは、悪意のあるソフトウェアの総称です。不正ソフトウェアとも呼ばれ、ウイルスはマルウェアに含まれます。マルウェアがインストールされると、コンピュータに様々な影響を与えます。

主なマルウェアには、次のようなものがあります。

①rootkit

セキュリティ攻撃を成功させた後に、その痕跡を消して見つかりにくくするためのツールです。

②バックドア

正規の手続き(ログインなど)を行わずに利用できる通信経路です。

③キーロガー

キーボードの入力を監視し、それを記録するソフトウェアです。使い方次第で利用者の入力情報を盗むことが可能です。

④ウイルス(コンピュータウイルス)

自己伝染機能、潜伏機能、発病機能がある悪意のあるソフトウェアです。離れたところから遠隔操作を行うことができる遠隔操作ウイルスや、コンピュータ内部のデータを外部に流す暴露ウイルスなど、様々な形態のウイルスがあります。

⑤トロイの木馬

悪意のないプログラムと見せかけて、不正な動きをするソフトウェアです。自己伝染機能はありません。



マルウェア以外で情報を暴露させる手法に、利用者のWebブラウザの設定を変更して、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ブラウザハイジャックがあります。

⑥ ランサムウェア

システムへのアクセスを制限し、その制限を解除するための代金(身代金)を要求するソフトウェアです。

⑦ アドウェア

広告を目的とした無料のソフトウェアです。通常は無害ですが、中にはユーザに気づかれないように情報を収集するような悪意のあるマルウェアが存在します。

■ DoS 攻撃

DoS 攻撃 (Denial of Service attack: サービス不能攻撃) は、サーバなどのネットワーク機器に大量のパケットを送るなどしてサービスの提供を不能にする攻撃です。踏み台と呼ばれる複数のコンピュータから一斉に攻撃を行う **DDoS 攻撃** (Distributed DoS attack) もあります。



DoS 攻撃には、その手法により、SYN Flood 攻撃、Smurf 攻撃など様々な種類があります。対策を行う場合には、手法に応じて、該当するパケットを遮断するためにファイアウォールやIDSを利用するなど、いくつかの方法があります。

■ バッファオーバーフロー攻撃

バッファオーバーフロー (BOF) 攻撃は、バッファ (プログラムが一時的な情報を記憶しておくメモリ領域) の長さを超えるデータを送り込むことによって、バッファの後ろにある領域を破壊して動作不能にし、プログラムを上書きする攻撃です。

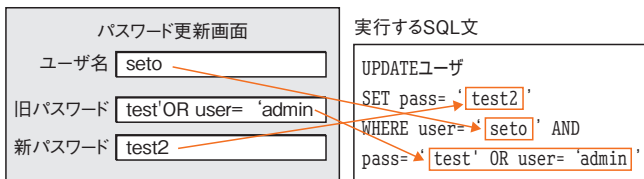
対策としては、入力文字列長をチェックする方法が一般的です。また、C 言語や C++ 言語など特定のプログラム言語でプログラムを作成したときに起こる攻撃なので、そのような言語を使わないという対策もあります。

■ SQL インジェクション

SQL インジェクションは、不正な SQL を投入することで、通常はアクセスできないデータにアクセスしたり更新したりする攻撃です。



SQL の詳細や具体的な使用方法については、「6-2-3 データ操作」で解説しています。



→ この攻撃が成功すると、adminユーザのパスワードも更新される



SQL インジェクション対策で利用するバインド機構とは、あらかじめSQL文をある程度まで用意しておいて、そこに入力された文字列を割り当てする方法です。具体的には、`preparedStatement("SELECT name FROM table WHERE code=?")`といったかたちであらかじめSQL文を作成しておき、「?」の部分に文字列を挿入します。この機能のことをプリペアドステートメント、「?」の部分プレースホルダといいます。



Cookie (HTTP Cookie) とは、WebサーバとWebブラウザとの間で情報をやり取りする仕組みです。ユーザを識別するなどの目的で使われます。

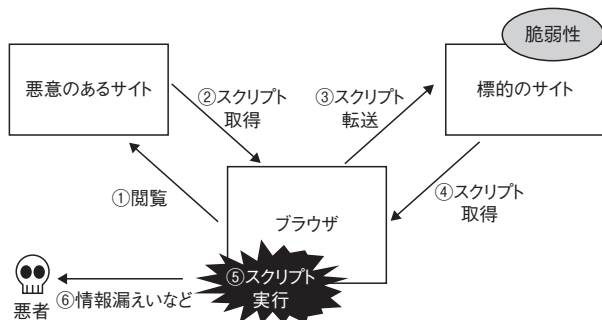


クロスサイトスクリプティングと同様に不正なスクリプトを実行させる攻撃には、Webサーバからの応答(レスポンス)を二つに分割させることによって、Webサーバのキャッシュを偽造するHTTPレスポンス分割攻撃や、WebブラウザのアクティブでないタブのWebページを偽のログインページに書き換えるタブナビングなどがあります。

SQL インジェクションでは、「」(シングルクォーテーション)などの制御文字をうまく組み入れることによって、意図しない操作を実行できます。対策としては、制御文字を置き換えるエスケープ処理や、事前にあらかじめSQL文を組み立てておくバインド機構などが有効です。

■ クロスサイトスクリプティング攻撃

クロスサイトスクリプティング (XSS : cross site scripting) 攻撃は、悪意のあるスクリプト(プログラム)を、標的となるサイトに埋め込む攻撃です。悪意のある人が用意したサイトにアクセスした人のブラウザを経由して、XSSの脆弱性のあるサイトに対してスクリプトが埋め込まれます。そのスクリプトをユーザが実行することによって、Cookie (クッキー) 情報などが漏えいするなどの被害が発生します。



クロスサイトスクリプティング攻撃

対処方法としては、スクリプトを実行できなくするために、制御文字をエスケープ処理する方法などがあります。

■ クロスサイトリクエストフォージェリ攻撃

クロスサイトリクエストフォージェリ (CSRF : Cross Site Request Forgeries) 攻撃は、Webサイトにログイン中のユーザのスクリプトを操ることで、Webサイトに被害を与える攻撃です。

XSSとの違いは、XSSではクライアント上でスクリプトを実行するのに対して、CSRFではサーバ上に不正な書き込みなどを行って被害を起こします。

■ ディレクトリトラバーサル

ディレクトリトラバーサルは、Webサイトのパス名(Webサーバ内のディレクトリやファイル名)に上位のディレクトリを示す記号(.. / や ..¥)を入れることで、公開が予定されていないファイルを指定する攻撃です。サーバ内の機密ファイルの情報の漏えいや、設定ファイルの改ざんなどに利用されるおそれがあります。

対策としては、パス名などを直接指定させない、アクセス権を必要最小限にするなどがあります。

■ セッションハイジャック

Webサーバに同じ人がアクセスしていることを確認するための情報として、セッションIDが利用されることがよくあります。別のユーザのセッションIDを不正に利用することで、そのユーザになりすましてアクセスする手口を、セッションハイジャックといいます。

対策としては、セッションIDを推測されにくいものにする、暗号化するなどの方法があります。



セッションIDは、Webサーバとクライアント(Webブラウザ)との間で情報をやり取りするときに使われるCookieの中に埋め込まれることが多いです。

そのため、暗号化した経路(SSLなど)を利用するときのみCookieを送るという設定も、セッションハイジャック対策として有効です。

■ OSコマンドインジェクション

コンピュータの基本ソフトウェアであるOS (Operating System) に対して、攻撃者からOSコマンドを受け取って実行してしまう攻撃を**OSコマンドインジェクション**といいます。Webサイトなどで、OSを実行する命令であるOSコマンドが実行できるような脆弱性がある場合に行われます。

■ 踏み台攻撃

関係のない第三者に、サーバなどを中継に利用されることで、迷惑メールを送る中継地点などとしてメールサーバが利用されるという攻撃です。外部ネットワークから別の外部ネットワークへの接続に利用されることを**第三者中継**といいます。第三者中継によって攻撃の拠点にされることを、**踏み台**にされるともいいます。

対策としては、第三者中継をサーバの設定で禁止する、メールサーバで認証を行うなどの方法があります。

■ IPスプーフィング

サーバなどで利用するIPアドレスを偽装して、他のサーバなどになります。DoS攻撃やDNSキャッシュポイズニング攻撃などと合わせて、攻撃者の身元を隠すためによく利用されます。

6 関連

DNSやIPの仕組みなど、ネットワーク関連の内容については、「6-1-3 通信プロトコル」で解説しています。ネットワークが苦手な方は、そちらでご確認ください。

■ DNSに関する攻撃

DNS (Domain Name System) とは、URL などにあるホスト名やドメイン名とIPアドレスを変換する名前解決のプロトコルです。DNSの名前解決の仕組みを悪用することで、様々な攻撃が可能となります。代表的なDNSに関する攻撃は、次のとおりです。

① DNSキャッシュポイズニング攻撃

DNSサーバのキャッシュに不正な情報を注入することで、不正なサイトへのアクセスを誘導する攻撃です。対策としては、DNSサーバをキャッシュサーバとコンテンツサーバの2台のサーバに分けて、キャッシュサーバでは外部からのアクセスを受け付けないようにする方法が有効です。

② DNSリフレクタ (DNS Reflector) 攻撃 (DNS amp 攻撃)

DNSの応答を利用したDoS攻撃です。IPスプーフィングを組み合わせて、DNSの応答が攻撃対象のサーバに集中するようにします。DNSアンプ (DNS amp) 攻撃ともいいます。

発展

ソーシャルエンジニアリングと技術を合わせた攻撃手法に、自動車などで移動しながら脆弱な無線LANアクセスポイントを探し出し、建物の外部から無線LANにアクセスするウォードラIVINGなどがあります。

■ ソーシャルエンジニアリング

人間の心理的、社会的な性質につけ込んで秘密情報を入手する手法のことです。コンピュータを操作している様子を後ろから肩越しに見てパスワードなどの情報を盗み見るショルダハッキングや、ゴミ箱をあさってパスワードの紙を見つけるスキベンジングなどの手法があります。

■ フィッシング

信頼できる機関を装い、偽のWebサイトに誘導する攻撃です。例えば、銀行を装って「本人情報の再確認が必要なので入力してください」などという偽装メールを送り、個人情報を入力させるといった手口があります。

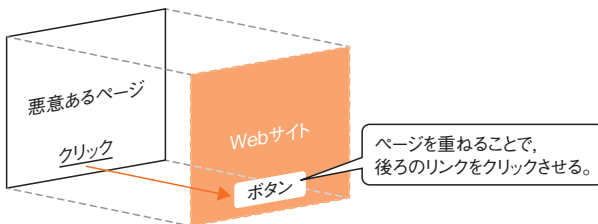
■ ドライブバイダウンロード攻撃

Webブラウザなどを通して、ユーザに気づかれずにソフトウェアなどをダウンロードさせる行為が**ドライブバイダウンロード**です。Webサイトを閲覧しただけでマルウェアに感染させられてしまいます。

ドライブバイダウンロード攻撃の事例としては、**ガンブラー**や広告配信サイトの改ざんなどがあります。ガンブラーでは、攻撃者がWebサイトを書き換えるための情報を盗み、正規のWebサイトを改ざんします。また、広告配信サイトの改ざんでは、広告配信サイトを運営する企業のサーバに侵入することで、Webサイトの中の広告の部分を改ざんします。

■ クリックジャッキング

クリックジャッキングとは、Webサイトのリンクやボタンなどの要素を隠蔽したり偽装したりしてクリックを誘い、利用者の意図しない動作をさせる手法です。クリックジャッキングでは、次のように二つの部品を重ねるイメージでWebサイトに細工をします。



クリックジャッキングのイメージ



クリックジャッキング攻撃でWebページを重ねるために利用されている仕組みは「フレーム」といいます。クリックジャッキング対策としては、このフレームの仕組みを無効化することや、同じサイト内の情報のみフレーム表示させるように設定変更する方法が有効です。このための仕組みに、HTTPのXFRAME-OPTIONヘッダがあります。

■ サイドチャネル攻撃

サイドチャネル攻撃は、暗号解読手法の一つで、暗号を処理している装置の動作などを観察・測定することによって機密情報を取得しようとする攻撃です。具体例としては、暗号の処理時間を計測するタイミング攻撃や、処理の実行中に放射させる電磁波を測定分析する電磁波解析攻撃などがあります。電磁波解析攻撃の一種に、漏えい電磁波を解読するテンペスト攻撃があります。

■ ゼロデイ攻撃

ゼロデイ攻撃は、ソフトウェアにセキュリティホール（脆弱性）が発見されたときに、その対処法や修正プログラムが提供されるまでの間にその脆弱性を攻撃することです。



TCPやUDP、ポート番号など、TCP/IP関連の内容については、「6-1-3 通信プロトコル」で解説しています。ネットワークの基本についてはそちらをご覧ください。

■ フットプリンティング

攻撃の準備として、ネットワーク上に存在している情報を収集することをフットプリンティングといいます。具体的には、サーバで使用しているOSやバージョン、ネットワーク構成情報などを取得し、攻撃者はこれらの情報を基にセキュリティ上の弱点を探し出します。代表的な手法としては、サーバのTCPやUDPのポート番号に対して順番にアクセスを行い、その返答を確認することでどのポートが有効であるかを確認する**ポートスキャン**があります。

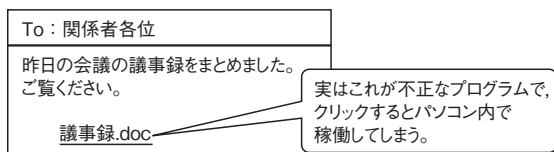
フットプリンティングの対策としては、公開情報を必要最小限にし、ログや不正侵入の検知ツールなどを利用して、攻撃者の足跡を検出する仕組みを整えることが挙げられます。

■ 標的型攻撃

特定の企業や組織を狙った攻撃です。標的とした企業の社員に向けて、関係者を装ってウイルスメールを送付するなどしてウイルスに感染させます。また、その感染させたPCからさらに攻撃の手を広げて、最終的に企業の機密情報を盗み出します。**APT**（Advanced Persistent Threat：先進的で執拗な脅威）と呼ばれることもあります。

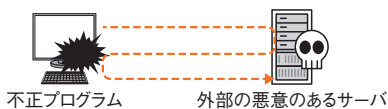
標的型攻撃の典型的な手法は、まず**標的型攻撃メール**を送り、

そのメールにマルウェアを添付して実行させます。このときのメールは通常の仕事関連のメールと同様の形式で送られてくるため、攻撃だと気づきにくいことが特徴です。



標的型攻撃メールの例

次に、そのマルウェアがパソコン内で稼働し、C&Cサーバと通信を行い、情報を外部に送ります。このときに、機密情報を含めた様々な情報が外部に漏えいします。



不正なプログラムが外部のC&Cサーバとやり取り

マルウェアを添付した標的型攻撃メールはウイルス対策ソフトで防げないことも多いため、攻撃を防ぐ入口対策だけでなく、感染後に被害を広げないための**出口対策**をしっかりと行うことが大切です。

出口対策とは、マルウェアに感染した後でその被害を外部に広げないための対策です。具体的には、ファイアウォールを使って内部から外部への通信を遮断する、プロキシサーバで外部のC&Cサーバとの通信を遮断などの方法があります。



用語

C & C (Command and Control) サーバとは、不正プログラムに対して指示を出し、情報を受け取るためのサーバです。



関連

ファイアウォールやプロキシサーバなどの機器については、「3-2 技術的セキュリティ対策」で改めて取り扱います。詳しい仕組みについては、そちらをご覧ください。

覚えよう！

- ☐ パスワードリスト攻撃は、他サイトのパスワードを利用
- ☐ 標的型攻撃は、出口対策が大事

1-2-2 演習問題

問1 機密情報の不正入手

CHECK ▶ ☐☐☐☐

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2 ランサムウェア

CHECK ▶ ☐☐☐☐

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に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

問3 クリックジャッキング攻撃

CHECK ▶ ☐☐☐☐

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、利用者が気付かない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4 ドライブバイダウンロード攻撃

CHECK ▶ ☐☐☐

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5 クロスサイトスクリプティング

CHECK ▶ ☐☐☐

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^{わな}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サーバに送り込まれ、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。

問6 バックドア

CHECK ▶ ☐☐☐

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7 APT

CHECK ▶ ☐☐☐

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て、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、複数の攻撃方法を組み合わせたマルウェアを継続的にばらまく。

問8 ポートスキャン

CHECK ▶ ☐☐☐

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9 パスワードリスト攻撃

CHECK ▶ ☐☐☐

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 想定し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10 ボットネットにおけるC&Cサーバ

CHECK ▶ ☐☐☐

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11 隠蔽機能をもつパッケージ

CHECK ▶ ☐☐☐

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

■ 解答と解説**問1**

(平成28年秋 情報セキュリティマネジメント試験 午前 問25)

《解答》ア

人間の心理的，社会的な性質につけ込んで秘密情報を入手する手法のことを「ソーシャルエンジニアリング」といいます。したがって，アが正解です。例としては，上司や重要顧客などを詐称してシステム管理者に電話をかけパスワードを聞き出す，ゴミ箱をあさってパスワードの紙を見つけるなどの手法があります。

イ コンピュータに入り込んで有害な動作を行うソフトウェアです。自己増殖機能はありません。

ウ 適切なセキュリティ対策が行われていないサーバに侵入し，そのサーバを経由して攻撃を行う手法です。

エ 適当な文字列を組み合わせる力任せにログインの試行を繰り返す攻撃です。

問2

(平成28年秋 情報セキュリティマネジメント試験 午前 問27)

《解答》エ

ランサムウェアとは，システムへのアクセスを制限し，その制限を解除するための代金(身代金)を要求するソフトウェアです。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のはランサムウェアに該当するので，エが正解です。

アは遠隔操作ウイルス，イはパスワードの暴露ウイルス，ウはキーロガーに該当します。

問3

(平成28年春 情報セキュリティマネジメント試験 午前 問22)

《解答》イ

クリックジャッキング攻撃とは，Webページのリンクやボタンなどを隠蔽・偽装してクリックを誘う攻撃です。透明化した標的サイトBを配置してWebサイトAの操作に見せかける攻撃はクリックジャッキング攻撃に該当するので，イが正解です。

アはHTTPレスポンス分割攻撃，ウはタブナビング攻撃，エはブラウザハイジャックに該当します。

問4

(平成28年春 情報セキュリティマネジメント試験 午前 問25)

《解答》ウ

ドライブバイダウンロード攻撃とは、Webサイトなどを通じて、利用者が気づかぬうちにソフトウェアをダウンロードさせる攻撃です。利用者のPCに不正プログラムが転送されるので、ウが正解です。

アはUSBメモリで感染するウイルス、イはランサムウェア、エはウォードライビングの説明です。

問5

(平成28年春 情報セキュリティマネジメント試験 午前 問21)

《解答》エ

クロスサイトスクリプティングとは、不正なスクリプトを実行させる攻撃です。罠を仕掛けられたWebページを利用者が閲覧し、リンクをクリックしたときに不正スクリプトが実行されるので、エが正解です。

アはSQLインジェクション、イはDoS攻撃(Denial of Service attack)、ウはバッファオーバーフローに該当します。

問6

(平成28年春 情報セキュリティマネジメント試験 午前 問27)

《解答》イ

バックドアとは、利用者に気づかれないようにシステムに秘密裏に仕込んだ遠隔操作のための窓口です。秘密裏に作成した利用者アカウントはバックドアに該当するので、イが正解です。

ア、ウ、エは有効なアカウントとして利用できず、バックドアとしては機能しません。

問7

(平成28年春 情報セキュリティマネジメント試験 午前 問19)

《解答》ウ

APT (Advanced Persistent Threat)はサイバー攻撃の一種で、標的型攻撃のうち高度で執拗な攻撃を指します。持続的標的型攻撃などと訳されることもあります。特定の目的をもち、標的となる組織に対して執拗に攻撃を繰り返すので、ウが正解です。

ア、イ 高度な攻撃ではないので誤りです。

エ APTは不特定多数への攻撃ではありません。

問8

(平成28年春 情報セキュリティマネジメント試験 午前 問29)

《解答》ア

ポートスキャンとは、利用可能なポートを探す行為です。ポート(番号)が分かると、そのポートを利用しているサービスが稼働しているかどうかを確認できるので、攻撃できそうなサービスがあるかどうかを調査することができます。したがって、アが正解です。

イはIDチェッカーなど、ウはスパイウェアなど、エはrootkitなどが利用されます。

問9

(平成28年秋 情報セキュリティマネジメント試験 午前 問26)

《解答》ウ

パスワードリスト攻撃とは、他のサイトで取得したパスワードのリストを利用して不正ログインを行う攻撃です。どこかのWebサイトから流出した利用者IDのパスワードのリストを用いて、他のWebサイトにログインを試みるので、ウが正解です。

アは辞書攻撃、イはレインボー攻撃、エはピクチャパスワードの盗聴に該当します。

問10

(平成28年秋 情報セキュリティマネジメント試験 午前 問12)

《解答》エ

ボットとは人間が行うようなことを代わりに行うプログラムで、ボットネットではボット同士が連携して動作を行います。C&C (Command and Control) サーバとは、ボットネットに対して指示を出し、情報を受け取るためのサーバです。ボットを感染させ、侵入して乗っ取ったコンピュータに対して、C&Cサーバが命令を出し、応答を受け取るので、エが正解です。

アはキャッシュサーバの役割です。イ、ウは、パスワードの盗聴を防ぐ仕組みです。

問11

(平成28年秋 情報セキュリティマネジメント試験 午前 問14)

《解答》イ

第三者がコンピュータに不正に侵入した後に利用するソフトウェアをまとめたパッケージは、rootkitです。したがって、イが正解です。

ア RFID (Radio Frequency Identification) は、電波を使った近距離の無線通信で情報をやりとりする仕組みです。

ウ TKIP (Temporal Key Integrity Protocol) は、無線LANで使われるセキュリティプロトコルで、システム運用中に動的に鍵を変更できます。

エ web beacon (ウェブビーコン) は、HTMLを利用した閲覧者を識別する仕組みです。

1-3 情報セキュリティに関する技術

1

情報セキュリティに関する技術で基本となるのは、暗号化技術と認証技術です。また、これらを応用した公開鍵基盤の技術は、社会的に利用されています。

1-3-1 暗号化技術

暗号化を行う仕組みには、共通鍵暗号方式と公開鍵暗号方式の2種類があります。また、ハッシュを組み合わせることによって、認証をはじめ様々なことを実現できます。

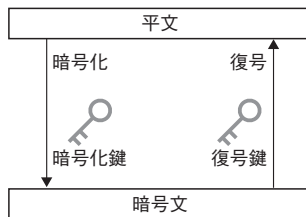


勉強のコツ

暗号化の仕組みは、セキュリティ技術を理解する上での基本中の基本です。確実に理解できるまで繰り返し学習することが大切です。

暗号化とは

暗号化とは、普通の文章(平文)^{ひらぶん}を読めない文章(暗号文)にすることです。ただし、誰も読めなくなったら役に立たないので、特定の人や機器だけは読めるようにする必要があります。読めなくすることを**暗号化**、元に戻すことを**復号**といいます。



暗号化と復号

暗号化と復号のために必要なのは、暗号化や復号の方法である**暗号化アルゴリズム**と、暗号化や復号を行うときに使う**鍵**です。暗号化するときの鍵は**暗号化鍵**、復号するときの鍵は**復号鍵**と呼ばれます。

暗号化の方式

暗号化の方式には、**共通鍵暗号方式**と**公開鍵暗号方式**の2種類があります。

① 共通鍵暗号方式

暗号化鍵と復号鍵が**同じ**暗号方式です。暗号方式の基本で、鍵は1種類しかないので秘密にしておく必要があります。そのため、**秘密鍵暗号方式**とも呼ばれます。

② 公開鍵暗号方式

暗号化鍵と復号鍵が**異なる**暗号方式です。鍵が2種類となり、暗号化を行うために**公開鍵**と**秘密鍵**の**キーペア**（鍵ペア）を作成します。公開鍵は他の人に公開し、秘密鍵は自分だけの秘密にしておきます。

続いて、それぞれの暗号方式について詳しく見ていきましょう。

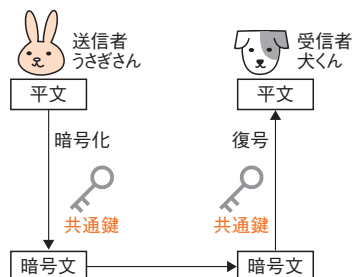


共通鍵暗号方式には様々なアルゴリズムがありますが、それぞれの暗号強度には大きな差があります。基本的な仕組みの理解だけでなく、どの暗号方式が推奨されているか、どの暗号方式に脆弱性が見つかっているかなど、運用面も押さえておくことが大切です。

共通鍵暗号方式

共通鍵暗号方式は、暗号化鍵と復号鍵が**共通**の方式です。その共通の鍵を**共通鍵**といい、通信相手とだけの秘密にしておく秘密鍵です。

共通鍵暗号方式での暗号化の流れは、次のようになります。



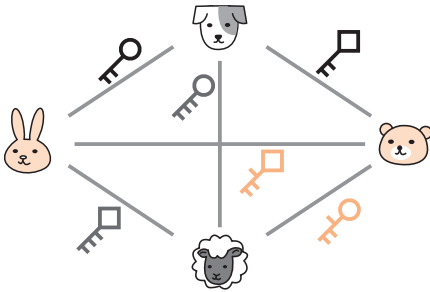
共通鍵暗号方式

うさぎさんが共通鍵を使って暗号化を行い、犬くんは受け取った暗号文を共通鍵で復号します。共通鍵を知られない限り、他の人は暗号文の内容を読むことはできません。

●共通鍵暗号方式の利点と問題点

共通鍵暗号方式の一番の利点は、公開鍵暗号方式と比べて暗号化と復号が速いということです。共通鍵での暗号化アルゴリズムでは排他的論理和を使うことが多く、処理は**単純で高速**です。そのため、データの暗号化を中心とした様々な分野で活用できます。

問題点は、暗号化する**経路の数だけ鍵が必要**であるため、人数が増えると管理が大変になることです。鍵を秘密にしておき、必要な人との間だけで共有するため、各人用の鍵を管理する必要があります。



組合せの数だけ鍵が必要

また、共通鍵は秘密鍵なので、第三者に知られては意味がありません。そのため、インターネット上で気軽にやり取りするわけにはいかず、**鍵の受け渡しに手間**がかかります。暗号化を行う前に、直接会うなど、インターネット以外の方法で鍵の受け渡しを行っておく必要があるため、使用を始めるまでが大変です。

●共通鍵暗号方式の種類

代表的な共通鍵暗号方式には、以下のものがあります。

① DES (Data Encryption Standard)

ブロックごとに暗号化する**ブロック暗号**の一種です。米国の旧国家暗号規格であり、56ビットの鍵を使います。しかし、鍵長が短すぎるため、近年では**安全性が低いとみなされています**。



関連

暗号化の方法には、ブロック暗号とストリーム暗号の2種類があります。ブロック暗号は、ブロックと呼ばれる固定長の長さに区切って暗号を行う方式で、全部の暗号化が終わってからデータを送信します。ストリーム暗号は、データを少しずつ暗号化していく方式で、暗号化が全部終わらないうちにデータ送信を行います。

② RC4 (Rivest's Cipher 4)

ビット単位で少しずつ暗号化を行っていくストリーム暗号の一種です。40～256ビットの鍵長可変です。処理が高速であり、無線LANの暗号化技術であるWEPなどで使用されています。近年では安全性が低いとみなされており、解読される危険性があります。

③ Triple DES (3DES)

DESを3回繰り返して暗号化を行う方式です。鍵長112ビットの2-key Triple DESと、鍵長168ビットの3-key Triple DESがあります。2-key Triple DESは安全性が低いとみなされており、使用する場合は3-key Triple DESが推奨されます。

④ AES (Advanced Encryption Standard)

米国立標準技術研究所(NIST)が規格化した新世代標準の方式で、DESの後継です。ブロック暗号で、鍵長は128ビット、192ビット、256ビットの三つが利用できます。排他的論理和の演算を繰り返し行いますが、その演算を行う数を段数(ラウンド数)といい、鍵長によって段数が決まります。

⑤ Camellia (カメリア)

NTTと三菱電機が共同で2000年に開発した共通鍵ブロック暗号です。ブロック長は128ビット、鍵長はAESと同じ128ビット、192ビット、256ビットの三つが利用できます。AESと同等の安全性を保ちつつ、ハードウェアでの消費電力を抑えつつ、高速な暗号化と復号を実現します。

⑥ KCipher-2 (ケーサイファー・ツー)

九州大学とKDDI研究所により共同開発されたストリーム暗号です。鍵長は128ビットです。AESなどと比べて7～10倍高速に暗号化／復号の処理をすることが可能です。



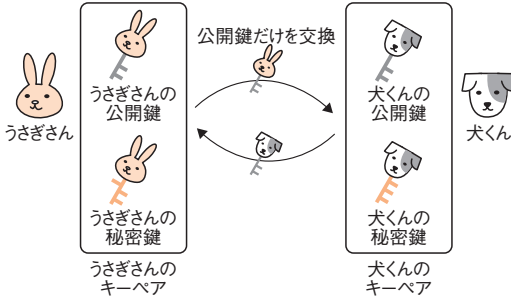
発展

CRYPTRECという団体が作成した「電子政府における調達のために参照すべき暗号のリスト」のうち、「電子政府推奨暗号リスト」に登録されているのは、次の四つです。

- 3-key Triple DES
 - AES
 - Camellia
 - KCipher-2
- これらが、政府が推奨する暗号です。

■ 公開鍵暗号方式

公開鍵暗号方式は、暗号化鍵と復号鍵が異なる方式です。使用する人ごとに**公開鍵**と**秘密鍵**のペア（キーペア）を作ります。そして、公開鍵は相手に渡して、秘密鍵は自分だけで保管しておきます。



鍵を二つずつ作り、互いに公開鍵だけを交換

公開鍵暗号方式のキーペアを用いることで、次の2種類の処理が可能になります。

1. 公開鍵で暗号化し、同じ人の**秘密鍵**で復号する
2. **秘密鍵**で暗号化し、同じ人の**公開鍵**で復号する



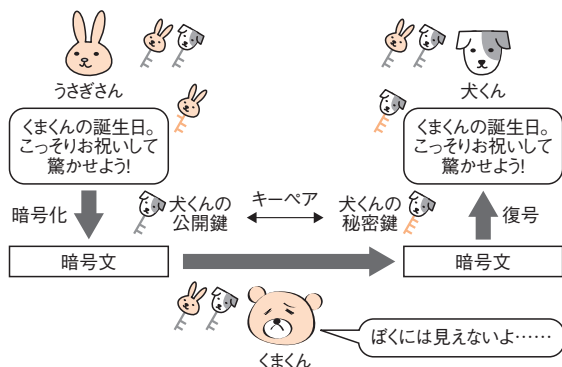
暗号化のアルゴリズムとしては公開鍵暗号方式の方が優れているのですが、計算が複雑で処理が遅いという欠点があります。そのため、データの暗号化にはあまり用いられません。しかし、共通鍵暗号方式は鍵の受け渡しが大変です。そのため、公開鍵暗号方式を用いた鍵共有の仕組みで共通鍵を作成するというのがよく行われています。

これらの性質を使い、公開鍵暗号方式では、守秘、鍵共有、署名を実現します。

公開鍵だけを交換すればいいので、安全に鍵交換ができるのが特徴です。鍵の種類も人数分×2を用意すればいいため、人数が増えてもそれほど鍵が増えません。

● 公開鍵暗号方式での守秘の実現

守秘の実現（暗号化）では、受信者が自分の秘密鍵で復号できるように、受信者の公開鍵で暗号化しておきます。送信者が相手（受信者）の公開鍵で暗号化すると、秘密鍵をもっている相手以外は読めなくなるので**守秘**が実現できます。



公開鍵暗号方式の暗号化



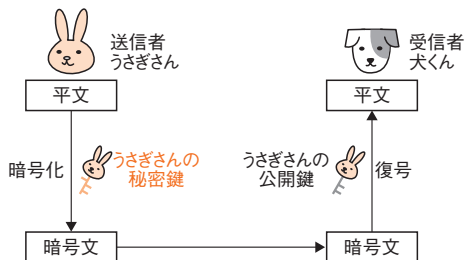
用語

署名とデジタル署名は、厳密には異なります。署名というときには、本人であることの証明の部分のみを指します。デジタル署名については後述しますが、ハッシュ関数を併用することによって改ざんの検出なども可能になっています。

また、共通鍵暗号方式で利用する鍵や鍵の種 (Seed) (鍵の基になる情報) を同じような方法で暗号化して送ることで**鍵共有**が実現できます。

●公開鍵暗号方式での署名

キーペアを逆に使い、送信者が自分の秘密鍵で暗号化することで、本人であることを証明できます。自分の**署名**を行い、真正性を実現することになるのです。



公開鍵暗号方式での署名の実現

●公開鍵暗号方式の種類

代表的な公開鍵暗号方式には、以下のものがあります。最も一般的に使用されているのは**RSA**です。

①RSA (Rivest Shamir Adleman)

大きい数での**素因数分解**の困難さを安全性の根拠とした方式です。公開鍵暗号方式で最もよく利用されています。鍵長1,024ビットのRSAは米国政府標準規格から外されており、鍵長2,048ビット以上の安全性証明の付いたRSAを使うことが推奨されています。



公開鍵暗号方式では、ほとんどの場合にはRSAが利用されています。公開鍵暗号方式の場合、アルゴリズムが複雑で、新しい暗号化方式を考えるのが大変なので、あまり新しい手法は出てきていないというのが現状です。

②DH 鍵交換 (Diffie-Hellman key exchange)

事前の秘密(秘密鍵などの秘密の情報)の共有なしに暗号鍵の共有を可能とする、**鍵共有**のための方式です。**離散対数問題**を安全性の根拠とした方式で、暗号鍵は共通鍵暗号方式の鍵として使用可能です。



離散対数問題とは、鍵の推測を難しくする数学的な性質です。例えば、素数 p と定数 g が与えられたとき $y = gx \bmod p$ ($\bmod$ は割り算の余り)を x から計算することは簡単ですが、 y から x を求めることは困難です。この性質が、公開鍵暗号方式に利用されています。

③DSA (Digital Signature Algorithm)

有限体上の**離散対数問題**を安全性の根拠とした署名アルゴリズムです。

④楕円曲線暗号 (Elliptic Curve Cryptography: ECC)

楕円曲線上の**離散対数問題**を安全性の根拠とした方式です。RSA暗号の後継として注目されています。署名アルゴリズムとして**ECDSA**があります。

■ハッシュ

ハッシュとは、一方向性の関数であるハッシュ関数を用いる方法です。データに対してハッシュ関数を用いてハッシュ値を求めます。ハッシュ値の長さは、データの長さによらず一定長となります。

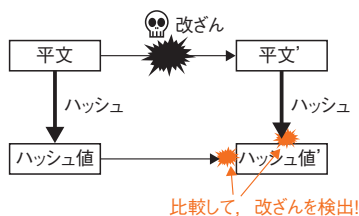
ハッシュは、暗号化(ハッシュ化)はできても元に戻せないという性質をもっているため、メッセージを復元させたくないときに役立ちます。

ハッシュの代表的な用途は、送りたいデータと合わせてハッ



ハッシュの利用で可能になるのは、改ざんを**検出**することです。厳密には、改ざんを**防止**することはできません。改ざんを防ぐことはできませんが、行われたときにハッシュ値を比較することによって改ざんに気づくことができます。

シュ値を送ることで**改ざんを検出**することです。改ざんとは、データを書き換えることです。元のデータが少しでも異なるとハッシュ値が変わってしまい、また、ハッシュ値が同じ別のデータを探すことも困難なため、改ざんを検出することが可能となります。



ハッシュで改ざんを検出

ハッシュ関数において、ハッシュ値が一致する二つのメッセージを発見することの困難さを**衝突発見困難性**といい、ハッシュ関数の強度を示す指標となります。

●ハッシュ関数でできること

改ざん検出のほかにも、ハッシュ関数はいろいろな場面で使われます。後述する、パスワード認証を行うときのチャレンジレスポンス方式などでは、ハッシュ関数を用いることが多いです。

また、パスワードを保管するときには、パスワードをハッシュ関数で変換し、**ハッシュ値のみを保管**することが多いです。受け取ったパスワードをハッシュ関数で変換し、保管してあるハッシュ値と一致するかどうかを確かめます。ハッシュ値は、盗聴されても元のメッセージが復元できないので、**盗聴防止**に役立ちます。

●ハッシュ関数の種類

代表的なハッシュ関数には、以下のものがあります。

①MD5 (Message Digest Algorithm 5)

与えられた入力に対して**128ビット**のハッシュ値を出力するハッシュ関数です。理論的な弱点が見つかっています。

② SHA-1 (Secure Hash Algorithm 1)

NISTが規格化した、与えられた入力に対して160ビットのハッシュ値を出力するハッシュ関数です。脆弱性があり攻撃手法がすでに見つかっているので推奨はされません。しかし、すでに普及しているため、互換性維持のための継続利用は容認されています。

③ SHA-2 (Secure Hash Algorithm 2)

SHA-1の後継で、NISTが規格化したハッシュ関数です。それぞれ224ビット、256ビット、384ビット、512ビットのハッシュ値を出力するSHA-224、SHA-256、SHA-384、SHA-512の総称です。SHA-256以上は電子政府推奨暗号リストにも登録されており、推奨される方式です。

●ソルト

ソルトとは、パスワードをハッシュ値に変換する際に付加されるデータです。ハッシュ関数は、そのアルゴリズムは公開されているため、同じメッセージからは同じハッシュ値を求めることができます。そのため、ハッシュ値が同じデータを見つけることで元のメッセージが推測できてしまう可能性があります。ソルトは、この推測を防ぐためにメッセージに付加するデータです。

ソルトを付加することで、同じメッセージから異なるハッシュ値が求められることになり、メッセージの推測を困難にできます。そのため、レインボー攻撃の対策としてソルトを付加することが有効となります。

**関連**

レインボー攻撃については、「1-2-1 サイバー攻撃手法」で解説しています。

●HMAC

メッセージに秘密鍵を付加したものをハッシュ関数で変換した値を、HMAC (Hash-based Message Authentication Code) と呼びます。秘密鍵を加えることで、暗号的なハッシュ値となります。鍵付きハッシュ関数ともいわれます。内容認証など、メッセージの内容を認証する場合によく用いられます。

**関連**

内容認証については、「1-3-2 認証技術」で説明しています。

覚えよう！

- ☐ 公開鍵暗号方式は鍵が2種類で、公開鍵と秘密鍵のキーペアをつくる
- ☐ 共通鍵／公開鍵暗号方式とハッシュの組合せで、様々なセキュリティ対策ができる

1-3-2 認証技術

認証には、人の認証、物の認証など、様々な種類があります。知識、所持、生体の認証の3要素の中で2要素認証を行うことが大切です。

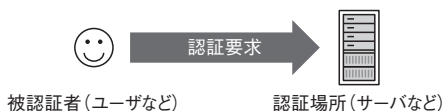
認証とは

認証とは、人や物などの対象についてその正当性を確認することです。**本人認証**(人の認証)をはじめ、物の認証、**メッセージ認証**(データの正当性確認)、**時刻認証**など、様々な認証があります。

認証の方法は、大きく分けて次の2種類です。

① Authentication (二者間認証)

認証される者(被認証者)について、認証が必要な場所(認証場所)で直接認証を行います。通常のサーバのログインなどのように、あらかじめ認証情報を認証場所で保持しておき、被認証者からの情報を基に認証の可否を決定します。



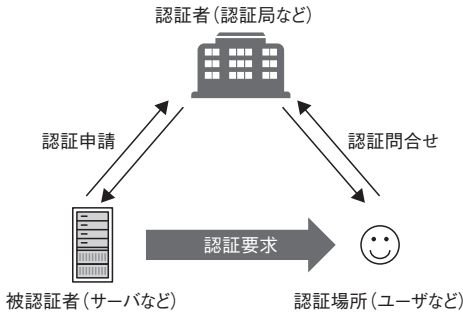
二者間認証 (Authentication)

② Certification (三者間認証)

被認証者と認証場所とは別に、認証する者(認証者)が存在し、認証者が認証を行う方法です。認証者が信頼できる機関である必要があり、PKI (Public Key Infrastructure : 公開鍵基盤)はこの仕組みを利用しています(次の図では、被認証者である「サーバ」が認証場所である「ユーザ」に対して、認証(サーバ認証)を求めています。このことにより、「サーバ」が正しいものであることを認証しています)。



PKIの詳細な内容については、「1-3-3 公開鍵基盤」で詳しく学習していきます。



三者間認証 (Certification)

■ 認証の3要素

認証を行うときに使用する要素 (内容) には大きく次の3種類があり、これを認証の3要素といいます。

1. **知識** ……ある情報をもっていることによる認証
例：パスワード、暗証番号など
2. **所持** ……ある物をもっていることによる認証
例：ICカード、電話番号、秘密鍵など
3. **生体** ……身体的特徴による認証
例：指紋、虹彩、静脈など

どの要素がすぐれているというものではなく、それぞれの認証には一長一短があります。例えば、パスワードは漏えいしたら他の人に使われますし、ICカードなどは盗難にあうおそれがあります。また、生体認証は他の人が代わりをすることは難しいですが、本人が認証を拒否されてしまうことがよくあります。

そのため、3要素のうちの2種類を組み合わせると**2要素認証 (多要素認証)**とすることが大切です。

■ パスワード認証

パスワード認証とは、ユーザ名 (ユーザID) とパスワードを組み合わせで行う認証です。パスワードは、そのままネットワーク上で送信すると盗聴されるおそれがあります。そのため、通信経路上のデータを盗聴されても不正にアクセスされないよう、



2要素認証は2段階認証とも呼ばれ、最近ではいろいろな場面で利用されています。

例えば、Googleの2段階認証では、パスワードに加え、携帯電話などに送られるコードの入力やスマートフォン上のアプリに回答することで認証します。これは、“知識”であるパスワードと、携帯電話などを“所持”していることによる2要素認証に該当します。



パスワードを忘れてしまったときに、利用者が事前に秘密の質問を設定し、それに答えることで認証を行う「パスワードリマインダ」という仕組みがあります。



パスワードをそのまま送るのは危険です。しかし、通常のメールの送受信などでは、パスワードの暗号化に対応していないことも多く、意識しないしているとパスワードを盗聴されるおそれがあります。自分が使用しているメールのパスワードがどのように送信されているのかをきちんと確認してみることは大切です。



パスワードの送信方法の説明などに、「パスワードを暗号化する」と書かれているのをよく目にしますが、厳密にはこのチャレンジレスポンス方式を使用している場合が多いです。パスワードを単純に暗号化しただけでは、暗号化したパケットごと再送信すれば認証できてしまい、リプレイ攻撃が可能になるため、あまり意味がありません。そのため、チャレンジレスポンス方式などが必要となってきます。

様々な対策が考えられています。

パスワードをネットワーク上で送信する方法には、次のようなものがあります。

①パスワードを平文で送信する方法

パスワードをそのままネットワーク上に流す方法です。盗聴される危険はありますが、メールの送受信など古くからある通信方法ではいまだに使われている場合も多いです。

②パスワードを判読できないようにして送信する方法

後述するチャレンジレスポンス方式などを用いて、パスワードを判読できないようにして送信する方法です。

③パスワードを毎回変更する方法

後述するワンタイムパスワード方式などを用いて、パスワードを毎回変える方法です。

④パスワードを送る経路を暗号化する方法

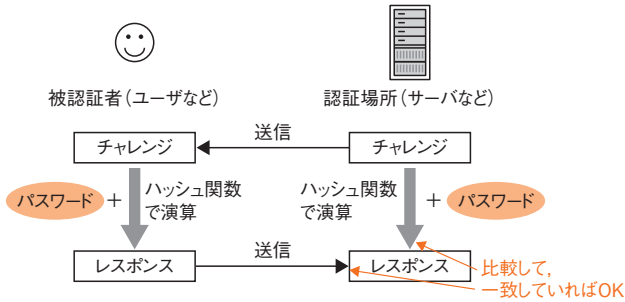
パスワードを送る通信経路を、SSLなどのプロトコルを用いて暗号化して送る方法です。

■チャレンジレスポンス方式

チャレンジレスポンス方式とは、認証場所（サーバなど）が毎回異なる情報（チャレンジ）を被認証者（ユーザなど）に送る認証方式です。チャレンジは、乱数や時刻などを使用して適当に決めます。被認証者は、チャレンジにパスワードを加えて演算した結果（レスポンス）を返します。認証場所では、チャレンジとレスポンスを比較して認証の可否を決めます。

演算には、ハッシュを用いる方法、公開鍵暗号方式を用いる方法、共通鍵暗号方式を用いる方法の3種類があります。最も一般的でよく利用されているのがハッシュを用いる方法で、PPPのCHAPや、APOP、EAP-MD5やEAP-TTLS、PEAPなど様々な認証方式で利用されています。

ハッシュを用いたチャレンジレスポンス方式では、次のような方法で、相手を認証します。



チャレンジレスポンス方式 (ハッシュを用いる方法)

■ ワンタイムパスワード

ユーザ名とパスワードは、一度盗聴されると何度でも不正利用される危険があります。それを避けるために、ネットワーク上を流れるパスワードを毎回変える手法が、**ワンタイムパスワード**です。ワンタイムパスワードの生成方法には以下のものがあります。

① セキュリティトークン

認証の助けとなるような物理的なデバイスのことを、セキュリティトークン、または単に**トークン**といいます。トークンの表示部に、認証サーバと時刻同期したワンタイムパスワードを表示するものが一般的です。

② S/Key

ハッシュ関数を利用して、ワンタイムパスワードを生成する方式です。乱数で作成した種 (Seed) を基に、ハッシュ関数で必要な回数の演算を行います。

■ パスワードの保管方法

サーバなどでファイルにそのままパスワードを保管していると、そのファイルが漏えいしたときにすべてのパスワードが見られてしまいます。それを防ぐため、パスワードの管理では、ハッシュ関数を用いてハッシュ値を求め、その**ハッシュ値のみを保管する**方法がよく用いられます。

ハッシュ値から元のパスワードを復元することはできないの

で、パスワードを忘れたりした場合には、**再度、新しいパスワードを設定**することになります。

なお、同じパスワードからは同じハッシュ値が求められます。これを異なる値にしてレインボーテーブルなどによる攻撃を防ぐために、パスワードに**ソルト**を加えてハッシュ値を生成する方法もよく用いられます。



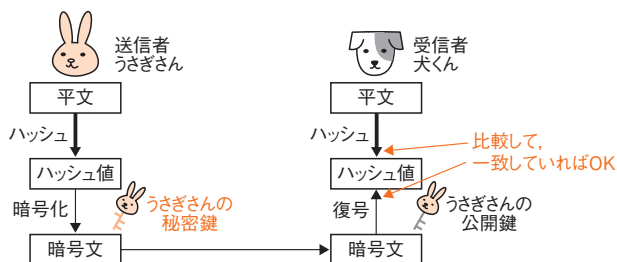
デジタル署名(デジタル署名)と同じような意味ですが、異なる使われ方をする用語に**電子署名**があります。デジタル署名は、公開鍵暗号方式を利用した認証と改ざん検知を行う仕組みです。それに対し、電子署名は国によって定義が異なります。日本では電子署名法で、「電子データの作成者を特定でき、電子データが改変されていないことが確認できるもの」を指すとされています。

つまり、電子署名はデジタル署名を含む、もう少し広義な概念として用いられています。

■ デジタル署名

公開鍵暗号方式は、暗号化以外にも使われます。本人の秘密鍵をもっていることが当の**本人であるという証明**になるのです。送信者の秘密鍵で暗号化し、それを受け取った受信者が送信者の公開鍵で復号することによって、確かに本人だということ(**真正性**)を確認できます。

さらに、先ほどのハッシュも組み合わせることで、データの**改ざんを検出**することもできます。この方法を**デジタル署名**といいます。



デジタル署名

● デジタル署名のアルゴリズム

デジタル署名に用いられるアルゴリズムには次のようなものがあります。最も一般的に用いられているものは、RSAです。

① RSA

公開鍵暗号方式のアルゴリズムであるRSAをデジタル署名に用いたものです。メッセージのエンコード(圧縮)を組み合わせたRSA-PSSがよく利用されています。

② DSA (Digital Signature Algorithm)

離散対数問題の困難性に基づくデジタル署名方式です。

③ ECDSA (Elliptic Curve Digital Signature Algorithm)

DSAについて、楕円曲線暗号を用いるようにしたものです。

● XML 署名

XML 署名は、デジタル署名のためのXML構文を規定する、W3C (World Wide Web Consortium)の勧告です。

XML 署名では、XML 文書全体に対する署名に限らず、文書の一部分への署名、複数のXML文書への署名、XML文書への複数人による署名に対応可能です。

```
<Signature>
  <SignedInfo>
    <SignatureMethod Algorithm="rsa-sha1">
    <Reference URI="参照するデータのURI" >
      <DigestMethod Algorithm="sha1">
      <DigestValue>ダイジェストの値</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>署名の値</SignatureValue>
  <KeyInfo>
    <KeyValue>公開鍵</KeyValue>
  </KeyInfo>
</Signature>
```

XMLのタグに、使用するアルゴリズムを記述します。

XML 署名の例

■ リスクベース認証

リスクベース認証とは、通常と異なる環境からログインをしようとする場合などに、通常の認証に加えて、合言葉などによる追加認証を行う認証方式です。ユーザの利便性をそれほど損わずに、第三者による不正利用が防止しやすくなります。

■ シングルサインオンの仕組み

シングルサインオン (Single Sign-On : **SSO**) とは、一度の認証で複数のサーバやアプリケーションを利用できる仕組みです。シングルサインオンの手法には、次のようなものがあります。

① エージェント型 (チケット型)

SSOを実現するサーバそれぞれに、エージェントと呼ばれるソフトをインストールします。ユーザは、まず認証サーバで認証を受け、許可されるとその証明に**チケット**を受け取ります。各サーバのエージェントは、チケットを確認することで認証済みであることを判断します。チケットには一般に、HTTPでの**クッキー** (Cookie) が用いられます。



HTTPについては、[6-1-3 通信プロトコル]を参照してください。

② リバースプロキシ型

ユーザからの要求をいったんリバースプロキシサーバがすべて受けて、中継を行う仕組みです。認証もリバースプロキシサーバで一元的に行い、アクセス制御を実施します。



認証連携型のサービスは、企業でのSSOという分野だけでなく、クラウドサービスでの認証で一般的に広がっています。GoogleやTwitterなどのIdPが発行するIDやパスワードを使って他のRPサービスを利用できる仕組みなどがあります。使用するプロトコルとしては、OAuthなどがあります。

③ 認証連携 (フェデレーション : Federation) 型

IDやパスワードを発行する事業者 (IdP: Identity Provider) と、IDを受け入れる事業者 (RP: Relying Party) の二つに役割を分担する手法です。

■ SAML

SAML (Security Assertion Markup Language) は、インターネット上で異なるWebサイト間での認証を実現するために、標準化団体OASISが考案したフレームワークです。

IDやパスワードなどの認証情報を安全に交換するための仕様で、XML (Extensible Markup Language) を用います。通信プロトコルには、HTTPやSOAPが用いられます。SSOを複数サイト間で実現するために利用されます。

■ ディレクトリサービス

ディレクトリサービスとは、ネットワーク上のユーザやマシンなどの様々な情報を一元管理するためのサービスです。ディレクトリサービスへのアクセスには、一般的に**LDAP** (Lightweight Directory Access Protocol) というプロトコルが用いられます。

SSOで使用するユーザ情報は、このディレクトリサービスを用いて一元管理されることも多いです。

■ CAPTCHA

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) は、ユーザ認証のときに合わせて行うテストで、利用者が**コンピュータでないことを確認**するために使われます。コンピュータには認識困難な画像で、人間は文字として認識できる情報を読み取らせることで、コンピュータで自動処理しているのではないことを確かめます。

■ 内容認証

内容認証(メッセージ認証)とは、送信されたデータの内容の完全性を確認することです。ハッシュ関数などを用いて二つのデータを比較することで、データが改ざんされていないかを確認します。

● MAC

MAC (Message Authentication Code: メッセージ認証コード) とは、メッセージ認証を行うときに、元のメッセージに送信者と受信者が共有する秘密鍵を加えて生成したコードです。MACを用いることで、データが改ざんされていないことに加えて、正しい送信者から送られたことを確認できます。

MACの生成にハッシュ関数を用いたものを**HMAC** (Hash-based Message Authentication Code) といいます。HMACの生成では、SHA-1、MD5など様々なハッシュ関数を利用することができます。ハッシュ計算時に**秘密鍵**の値を加えることで、ハッシュ値の改ざんを困難にします。

●送金内容認証

送金内容認証とは、金融機関などの取引で、送金内容に対してメッセージ認証を行う方式です。一般的には、トランザクション認証ともいわれます。利用者ごとに秘密鍵を用意し、金融機関と利用者との間で共有しておきます。実際に送金内容を送るときに、HMACなどを用いて計算を行い、送金内容が改ざんされていないかどうかを確認します。

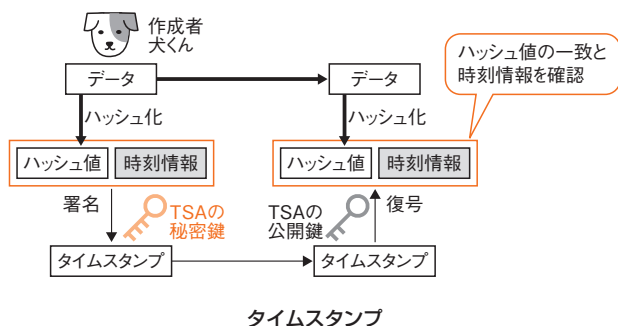


タイムスタンプの主な目的は、署名した本人が不正を働かないことを確認することです。そのため、内部統制などで法的証拠を集めるときによく使われます。

■時刻認証(タイムスタンプ)

契約書や領収書などの情報が電子化されると、それが改ざんされる危険が出てきます。PKIでのデジタル署名では、他人の改ざんは検出できますが、本人が改ざんした場合には対処できません。その対策として、メッセージに、ある出来事が発生した日時を表す情報を付加して**タイムスタンプ**を作成することで作成時刻を認証する時刻認証の仕組みがあります。タイムスタンプ技術ともいわれます。

具体的には、**TSA** (時刻認証局) が提供している**時刻認証**サービスを利用して書類のハッシュ値に時刻情報を付加し、TSAのデジタル署名を行ってタイムスタンプを作成します。これにより、本人が改ざんしたとしても、そのタイムスタンプを見ることで不正を判断できるようになります。



時刻認証によって証明できることは、次の二つです。

1. **存在性** …… そのデータがその時刻には存在していたこと
2. **完全性** …… その時刻の後には改ざんされていないこと

デジタル署名では、完全性は証明できても存在性に関しては証明できません。そのため、存在性の証明が必要なときに時刻認証を用いることになります。

■ ICカードによる認証

ICカードは、通常の磁気カードと異なり、情報の記録や演算をするためにIC(Integrated Circuit:集積回路)を組み込んだカードです。接触型と非接触型の2種類があります。PIN(Personal Identification Number:暗証番号)と合わせて用いることで、悪用されるのを防ぐことができます。

ICカードは、内部の情報を読み出そうとすると壊れるなどして情報を守ります。このような、物理的あるいは論理的に内部の情報を読み取られることに対する耐性のことを**耐タンパ性**といいます。



PINとは、情報システムが利用者の本人確認のために用いる秘密の番号のことです。パスワードと同じ役割をするものですが、クレジットカードの暗証番号など、数字のみの場合によく使われる用語です。

■ 生体認証

生体認証(**バイオメトリクス認証**)は、指や手のひらなどの体の一部や動作の癖などを利用して本人確認を行う認証手法です。忘れたり紛失したりすることがないため利便性が高いため、様々な場面で利用されています。

生体認証の代表的なものには、指紋を利用する**指紋認証**、手のひらを利用する**静脈認証**、目を利用する**虹彩(アイリス)認証**、顔で認証する**顔認証**、声で認証する**音声認証**などの身体的特徴をもとにした認証があります。また、それ以外にも**行動的特徴**を抽出して行う認証方法もあり、代表的なものに、**サイン(筆跡)**や**声紋**、**キーストローク**などがあります。

生体認証では、入力された特徴データと登録されている特徴データを照合して判定を行います。このとき、二つのデータが完全に一致することはほぼないので、あらかじめ設定されたしきい値以上の場合を一致とします。そのため、本人を拒否する可能性をなくすることができず、その確率を**本人拒否率**(FRR: False Rejection Rate)とします。また、誤って他人を受け入れることもあり、その確率を**他人受入率**(FAR: False Acceptance Rate)と呼びます。

覚 え よ う !

- ☐ デジタル署名は、ハッシュ値を送信者の秘密鍵で暗号化し、本人証明+改ざん検出
- ☐ 時刻認証では、存在性と完全性が確認できる



生体認証の落とし穴

生体認証は、認証の3要素のうちでは他人によるなりすましがされにくいと、最も強度が高いと考えられています。しかし、生体認証には、知識や所持の認証と比べて認証の精度が低く、「100%の認証はできない」という欠点があります。

例えば、生体認証の代表例である指紋認証では、「指紋を認識してくれないのでアクセスできない」ということがよくあります。筆者も以前、会社の入館が指紋認証だったことがあり、よく認証に失敗して苦勞していました。特に、冬に指が乾燥していると認証されないことが多く、ハンドクリームを持ち歩くようになりました。このように、生体認証の仕組みは完全ではないので、本人でも拒否されてしまうことがあります。

また、スパイ映画などでよく見られるような、指紋を偽造して入室するなど、難易度は高いですが可能です。

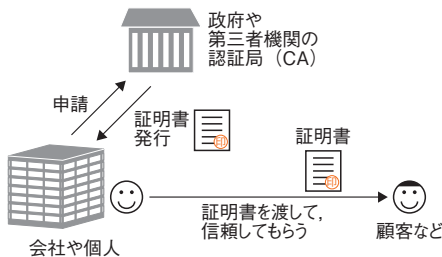
こうしたことから、生体認証は単独ではあまり使われません。パスワードと併用するなど、他の要素と組み合わせることが一般的です。生体認証でも2要素認証が大切になってくるのです。

1-3-3 公開鍵基盤

公開鍵基盤(PKI)は、公開鍵暗号方式を用いて社会的な信用を確保する仕組みです。

PKIの仕組み

PKI (Public Key Infrastructure : 公開鍵基盤)は、公開鍵暗号方式を利用した社会基盤(インフラ)です。政府や信頼できる第三者機関に設置した認証局(CA : Certificate Authority)に証明書を発行してもらい、身分を証明してもらうことで、個人や会社の信頼を確保します。



PKIの仕組み

CAの内部では、次のような役割をもつ機関を構築および運用しています。

- ・ **RA** (Registration Authority : 登録局)
証明書の登録を受け付け、証明書を発行してもよいかどうかの審査を行う機関
- ・ **IA** (Issuing Authority : 発行局)
実際に証明書を発行する機関。証明書にデジタル署名を行う

PKIのために、CAでは**デジタル証明書**を発行します。デジタル証明書は、CAがデジタル署名を行うことによって、申請した人や会社の公開鍵が正しいことを証明します。



公開鍵証明書は、パソコンで簡単に見ることができます。Internet Explorer や Chrome などの Web ブラウザで、https で始まる Web サイトを見ると、アドレスバーなどに鍵マークが表示されています。それをダブルクリック(ブラウザによりやり方は異なります)することで、Web サーバの証明書が表示されます。



デジタル証明書の例

GPKI

政府が主導する PKI は一般のものと区別し、政府認証基盤 (GPKI : Government Public Key Infrastructure) と呼ばれます。GPKI では、行政機関に対する住民や企業からの申請・届出などをインターネットを利用して実現することを目的としています。国税の電子申告・納税システムである e-Tax などでも利用されています。

プライベートCA

組織の中には、自営で CA を立ち上げ、公共の第三者機関ではなく自らがデジタル証明書を発行するところもあります。このような CA を **プライベートCA** といい、通常の第三者機関発行のものとは区別します。

デジタル証明書

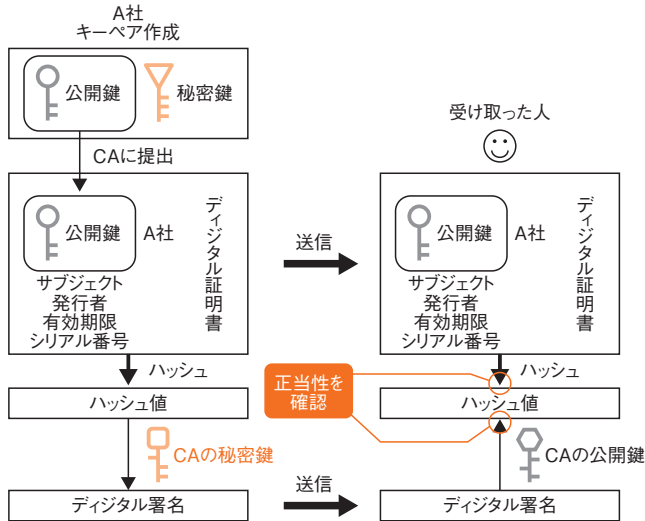
デジタル証明書は、作成したキーペアのうちの公開鍵を CA に提出し、その公開鍵に様々な情報を付加したのに対して、CA がデジタル署名を行ったものです。例えば、A 社という会社におけるデジタル証明書の作成と検証の流れは、次のようになります。



CA の公開鍵のうち信頼できる第三者機関のものは、あらかじめ Web ブラウザに登録されています。そのため、利用者は意識せずにサーバ証明書の正当性を確認することができます。しかし、プライベートCAの場合はそのままでは信頼されないため、CA の公開鍵を自分で Web ブラウザに登録する作業が必要です。



デジタル証明書は、公開鍵証明書、または単に証明書と呼ばれることもあります。これらの用語は区別せず使われることが多いです。



デジタル証明書の作成と検証の流れ (A社の例)

デジタル証明書を受け取った人は、CAの公開鍵を用いてデジタル署名を復元し、デジタル証明書のハッシュ値と照合して一致すると、デジタル証明書の正当性を確認できます。デジタル証明書の規格は、ITU-T X.509で定められています。

デジタル証明書のうち、サーバで使用する証明書を**サーバ証明書**、クライアントが使用する証明書を**クライアント証明書**とって区別することもよくあります。

■ CRL

デジタル証明書には有効期限がありますが、その有効期限内に秘密鍵が漏えいしたりセキュリティ事故が起こったりしてデジタル証明書の信頼性が損なわれることがあります。

そうした場合には、CAに申請し、**CRL** (Certificate Revocation List: 失効リスト) に登録してもらいます。これにより、そのデジタル証明書は無効であることを利用者に伝えることができます。CRLは、失効したデジタル証明書の**シリアル番号**と失効した日時を記したリストです。

用語

ITU-Tとは、ITU (International Telecommunication Union: 国際電気通信連合) の一部門で、主に通信分野の標準策定を担当する電気通信標準化部門 (Telecommunication Standardization Sector) です。標準技術をITU-T勧告として発表しています。勧告のうちXシリーズは、「データ網及びオープン・システム・コミュニケーション」に関する規定です。

用語

シリアル番号とは、デジタル証明書に割り振られた、一意な番号です。CRLは公開情報ですが、会社名などの情報は公開されず、シリアル番号のみを公開することで、最低限の情報で失効しているかどうかを確認できます。

■ VA

VA (Validation Authority : **検証局**)は、デジタル証明書のリストを集中的に管理し、証明書の有効性を確認することに特化した組織です。CAとは異なり、デジタル証明書の発行は行わず、CRLを集中管理して検証を行います。

■ OCSP

デジタル証明書の失効状態を取得するためのプロトコルにOCSP (Online Certificate Status Protocol)があります。CRLの代替として提案されており、主にHTTPを使ってやり取りされます。

OCSPのやり取りを行うサーバを**OCSPレスポнда**といいます。OCSPレスポндаは、クライアントから指定された証明書の有効状態について、「有効」「失効」「不明」のいずれかの応答を、署名を付けて返します。

■ EV SSL 証明書

EV (Extended Validation) SSL 証明書とは、発行者が審査に一定の基準を設けたデジタル証明書です。企業が物理的、法律的に存在していることを確認し、審査を行います。

EV SSL 証明書を導入したサイトを閲覧すると、ブラウザのアドレスバーが**緑色**になり、そのWebサイトの運営組織 (Organization Name) が表示されます。

▶▶ 覚えよう！

- ☐ デジタル証明書は、公開鍵に情報を付加したものにCAがデジタル署名する
- ☐ CRLは、有効期限内に失効した証明書のシリアル番号を記載したリスト

1-3-4 演習問題

問1 AES

CHECK ▶ ☐☐☐

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2 公開鍵暗号方式

CHECK ▶ ☐☐☐

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。

問3 2要素認証

CHECK ▶ ☐☐☐

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4 ハッシュ関数の特徴

CHECK ▶ ☐☐☐

デジタル署名などに用いるハッシュ関数の特徴はどれか。

- ア 同じメッセージダイジェストを出力する二つの異なるメッセージは容易に求められる。
- イ メッセージが異なっても、メッセージダイジェストは全て同じである。
- ウ メッセージダイジェストからメッセージを復元することは困難である。
- エ メッセージダイジェストの長さはメッセージの長さによって異なる。

問5 デジタル署名でできること

CHECK ▶ ☐☐☐

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。

問6 なりすましでないことを確認する方法

CHECK ▶ ☐☐☐

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7 利用者認証

CHECK ▶ ☐☐☐

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8 生体認証システム

CHECK ▶ ☐☐☐

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スなど別の手段と組み合わせる。
- 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 プログラムによる自動入力排除

CHECK ▶ ☐☐☐

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 |

問10 認証局の役割

CHECK ▶ ☐☐☐

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を暗号化する。
- 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。

問11 スマートフォンからの社内システムへのアクセス

CHECK ▶ ☐☐☐

社員が利用するスマートフォンにデジタル証明書を導入しておくことによって、当該スマートフォンから社内システムへアクセスがあったときに、社内システム側で確認できるようになることはどれか。

- ア 当該スマートフォンがウイルスに感染していないこと
- イ 当該スマートフォンが社内システムへのアクセスを許可されたデバイスであること
- ウ 当該スマートフォンのOSに最新のセキュリティパッチが適用済みであること
- エ 当該スマートフォンのアプリケーションが最新であること

問12 CAの役割

CHECK ▶ ☐☐☐

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。

■ 解答と解説

問1

(平成28年春 情報セキュリティマネジメント試験 午前 問28)

《解答》イ

暗号化アルゴリズムのAES (Advanced Encryption Standard) は、米国の新暗号規格として規格化された共通鍵暗号方式です。暗号化にはPCとサーバで共有された共通鍵を用いるので、イが正解です。

ア、ウ、エは、公開鍵暗号方式で利用する鍵です。

問2

(平成28年春 情報セキュリティマネジメント試験 午前 問30)

《解答》エ

AさんがBさんの公開鍵で暗号化した電子メールは、Bさんの公開鍵のキーペアであるBさんの秘密鍵でのみ復号できます。そのため、秘密鍵をもっているBさんだけが、自身の秘密鍵で電子メールを復号できるので、エが正解です。

問3

(平成28年春 情報セキュリティマネジメント試験 午前 問18)

《解答》ア

2要素認証とは、認証に用いる情報の種類である認証の3要素——「記憶」、「所持」、「生体」のうち2要素を用いて行う認証です。ICカード認証は所持の認証、指紋認証は生体の認証なので、この二つの組合せは2要素認証となるため、アが正解です。

イは二つとも所持の認証、ウは二つとも生体認証、エは二つとも記憶の認証です。

問4

(平成25年秋 基本情報技術者試験 午前 問38)

《解答》ウ

ハッシュ関数は一方向性の関数で、平文を変換してハッシュ値(ハッシュ、メッセージダイジェスト)を求めます。一方向性であるため、ハッシュ値から元の平文を復元することは困難です。したがって、ウが正解です。

ア 異なるメッセージから同じハッシュ値が出力される可能性は非常に低く、困難です。

イ メッセージが少しでも異なると、別のハッシュ値が出力されます。

エ ハッシュ値は一定の長さ(アルゴリズムにより異なる)です。

問5

(平成28年春 情報セキュリティマネジメント試験 午前 問23)

《解答》ウ

送信者Aが作成した文書ファイルのデジタル署名は、文書ファイルのハッシュ値に対して、送信者Aの署名生成鍵Yを用いて暗号化したものです。受信者Bでは、デジタル署名を署名検証鍵Xで復号し、文書ファイルのハッシュ値と照合することで、文書ファイルが改ざんされていないことと、デジタル署名が署名生成鍵Yによって生成されたことの両方が確認できます。したがって、ウが正解です。

アの改ざんの部位や、イのウイルスに感染していないこと、エの改ざんがどちらで行われたかなどは、デジタル署名では判定できません。

問6

(平成28年秋 情報セキュリティマネジメント試験 午前 問28)

《解答》ウ

ECサイトのデジタル署名が添付された電子メールでデジタル署名を検証することで、署名をした秘密鍵がECサイトのものであることを確認できます。また、ハッシュ値も合わせて確認でき、メールが改ざんされていないことも分かるので、メール内のドメインが正しいことも確認できます。したがって、ウが正解です。

ア、イのメールアドレスは偽装が可能です。また、署名も自由に設定できるので、エも偽装可能であり、相手が正しいことは確認できません。

問7

(平成28年秋 情報セキュリティマネジメント試験 午前 問1)

《解答》エ

PIN (Personal Identification Number) とは、ICカードに設定された暗証番号のことです。ICカード利用時にPINを入力することで、ICカードの正当な所有者であることを判定できます。ICカードを配送するときは、盗難や紛失による悪用防止のため、PINは別経路で利用者に知らせる必要があります。したがって、エが正解です。

ア ICカードに設定するPINは、ICカードごとに異なる値を設定します。

イ ICカード紛失時は、悪用防止のため、すぐに失効処理を行います。

ウ PINは暗証番号なので、予測されない値にします。

問8

(平成26年春 基本情報技術者試験 午前 問45)

《解答》エ

生体認証は、身体的な特徴による認証方式で、指紋、虹彩、静脈などを利用します。身体的特徴を各種センサー装置で読み取りますが、装置の設定によって、他人を本人として認識してしまう「他人受入率」や、本人を拒否してしまう「本人拒否率」が変わるため、装置を調整する必要があります。したがって、エが正解です。

ア SQL インジェクションやクロスサイトスクリプティングなどで考慮すべき点です。

イ ウイルス対策を行うときに考慮すべき点です。

ウ 証明書によるクライアント認証などを行うときに考慮すべき点です。

問9

(平成28年秋 情報セキュリティマネジメント試験 午前 問20)

《解答》ア

CAPTCHAとは、ユーザ認証のときに合わせて行うテストで、利用者がプログラムによる自動入力でないことを確認するために使われます。Completely Automated Public Turing test to tell Computers and Humans Apartの頭文字をとったものです。したがって、アが正解です。

イ 二次元バーコードの種類です。

ウ 長いURLを短いURLに変換したものです。リダイレクトという仕組みを利用して本来のサイトに接続します。

エ ブログの機能の一つで、双方向リンクである「トラックバック」の設置をリンク先に通知するために送信されるパケットのことです。

問10

(平成28年秋 情報セキュリティマネジメント試験 午前 問29)

《解答》ウ

PKIの認証局が果たす役割として、公開鍵証明書の発行があります。失効したデジタル証明書の一覧(CRL)の発行も行います。したがって、ウが正解です。

ア 暗号化通信で利用者が作成します。

イ 暗号化通信で利用者が暗号化します。

エ PKIにおいては受信者が検証します。

問11

(平成27年春 基本情報技術者試験 午前 問45)

《解答》イ

デジタル証明書は、第三者機関である認証局 (CA) が発行するもので、申請した人や会社の公開鍵が正しいことを、CA がデジタル署名を行うことによって証明します。

そのため、デジタル証明書を導入したスマートフォンで社内システムにアクセスすると、デジタル証明書のデジタル署名をCAの公開鍵で復号してデジタル証明書のハッシュ値と照合することで、CAが発行したデジタル証明書であることを確認できます。その結果、社内システム側では当該スマートフォンが、CAが発行したデジタル証明書をもっている、アクセスを許可されたデバイス (機器) であると確認できるのです。したがって、イが正解です。

- ア ウイルス対策ソフトの導入で確認できます。
- ウ OSのセキュリティパッチ適用機能で確認できます。
- エ アプリケーション配布サーバにアクセスして確認します。

問12

(平成28年春 情報セキュリティマネジメント試験 午前 問24)

《解答》イ

認証局 (CA : Certificate Authority) は、公開鍵に対するデジタル証明書を発行する機関です。したがって、イが正解です。

- ア 秘密鍵を共有するのは、共通鍵暗号方式です。
- ウ デジタル署名はCAが行い、CAが発行したデジタル証明書に付与されます。
- エ 公開鍵暗号ではパスワードは利用しません。

第2章

情報セキュリティ管理

情報セキュリティ管理は、情報セキュリティマネジメント試験の内容で中核となる分野です。

「情報セキュリティマネジメント」「リスクマネジメント」「情報セキュリティに対する取組み」の3分野について、情報セキュリティ管理のやり方・考え方を中心に学んでいきます。

「情報セキュリティマネジメント」ではISMSを中心とした情報セキュリティを確保する仕組みを、「リスクマネジメント」では、リスクを洗い出し、アセスメントする一連の流れを学習します。「情報セキュリティに対する取組み」では、国のセキュリティ組織や機関など、情報セキュリティを確保するために整えられている仕組みや取組みについて学びます。

2-1 情報セキュリティマネジメント

- ◆ 2-1-1 情報セキュリティ管理
- ◆ 2-1-2 情報セキュリティ諸規程
- ◆ 2-1-3 情報セキュリティ
マネジメントシステム
- ◆ 2-1-4 情報セキュリティ継続
- ◆ 2-1-5 演習問題

2-2 リスクマネジメント

- ◆ 2-2-1 情報資産の調査・分類
- ◆ 2-2-2 リスクの種類
- ◆ 2-2-3 情報セキュリティリスク
アセスメント
- ◆ 2-2-4 情報セキュリティリスク対応
- ◆ 2-2-5 演習問題

2-3 情報セキュリティに対する取組み

- ◆ 2-3-1 情報セキュリティ組織・機関
- ◆ 2-3-2 セキュリティ評価
- ◆ 2-3-3 演習問題

2-1 情報セキュリティマネジメント

情報セキュリティマネジメントとは、組織の情報セキュリティの確保に体系的に取り組むことです。情報セキュリティを管理し、緊急時にも適切に継続できるように対処します。



勉強のコツ

情報セキュリティマネジメント分野が、その言葉が示すように、情報セキュリティマネジメント試験では最重要ポイントです。

具体的なセキュリティ管理手法や、標準や法律などについても、しっかり押さえておきましょう。

2-1-1 情報セキュリティ管理

情報セキュリティ管理では、情報セキュリティポリシーに基づいて情報資産を洗い出し、情報セキュリティインシデントに対応します。

情報セキュリティポリシーに基づく情報の管理

情報セキュリティ対策においては、何をどのように守るのかを明確にしておく必要があります。そのために、企業や組織として意思統一された**情報セキュリティポリシー**を策定して明文化し、それに基づく管理を行います。

情報セキュリティポリシーは、情報の機密性や完全性、可用性を維持していくための組織の方針や行動指針をまとめたものです。策定する上ではまず、どのような情報(情報資産)を守るべきなのかを明らかにする必要があります。

情報資産の洗い出し

情報(Information)とは、状況を知るために獲得する知識のことで、その価値をもつものが**情報資産**(Information asset)です。企業や組織が保有する情報資産を漏れなく洗い出すことで、守るべきものを明確にします。

情報資産を洗い出す際の切り口には、次のようなものがあります。

- ・物理的資産 …………… 通信装置やコンピュータ、ハードディスクなどの記憶媒体など
- ・ソフトウェア資産 …… 業務やシステムのソフトウェア、開発ツールなど
- ・人的資産 …………… 経験や技能、資格など

- ・無形資産 ……………組織のイメージ，評判など
- ・サービス資産 ……………一般ユーティリティ（電源や空調，照明），
通信サービス，計算処理サービスなど
- ・直接的情報資産 ……………データベースやファイル，文書記録など

洗い出した情報資産は，**情報資産台帳**（情報資産目録）などにまとめられます。



情報資産台帳については、
[2-2-1 情報資産の調査・
分類]で説明します。

■ 情報セキュリティインシデントと情報セキュリティ事象

情報セキュリティインシデントとは，情報セキュリティを脅かす事件や事故のことです。単に**インシデント**と呼ぶこともあります。情報セキュリティ管理では，情報セキュリティインシデントが発生した場合の報告・管理体制が明確であり，関係者全員に周知・徹底されていることが重要です。

情報セキュリティ事象とは，情報セキュリティインシデントのほかに，情報セキュリティに関連するかもしれない状況のことです。情報セキュリティ事象が発生した場合は，適切な管理者に報告する必要があります。例えば，情報セキュリティポリシーに違反してウイルス対策ソフトを導入していないコンピュータがあったとします。これを放置しておくとうイルス感染などの情報セキュリティインシデントにつながるおそれがあるので，そのようなコンピュータを発見したら，情報セキュリティ事象として管理者に報告する義務があります。

■ 情報セキュリティマネジメントの監視及びレビュー

情報セキュリティマネジメントの仕組みを実装して管理策を策定しても，そのままでは実現されない，あるいは不備があるおそれがあるので，日常的に**監視**することが大切です。

また，情報セキュリティマネジメントは，環境の変化などに応じて見直す必要もあります。そのために，その管理策の有効性や継続性を計り，監視，監査，レビューなどを実施します。

▶▶ 覚えよう！

- ☐ 情報資産には，物理的資産，ソフトウェア資産，人的資産，無形資産などもある
- ☐ 情報セキュリティ事象の段階で，管理者に報告することも義務

2-1-2 情報セキュリティ諸規程

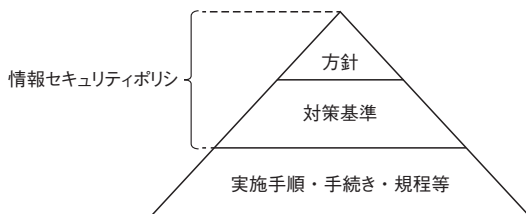
情報セキュリティを維持するためには、情報セキュリティポリシーだけでなく、文書管理規程や機密管理規程など、様々な規程を制定する必要があります。

6 関連

情報セキュリティポリシーは、あくまで方針と基準なので、細かい内容は決定されていません。そのため、実際に情報セキュリティマネジメントを行う際には、情報セキュリティ対策実施手順や規程類を用意し、詳細な手続きや手順を記述します。

情報セキュリティポリシーに従った組織運営

情報セキュリティポリシーに沿った組織運営を行うためには、明文化した文書を用意し、それに従って意思を統一する必要があります。一般的に、情報セキュリティポリシーに関する文書は次のように構成されています。



情報セキュリティポリシーの文書構成

上の二つの部分を情報セキュリティポリシーと呼ぶことが多いですが、特に定められているわけではありません。

情報セキュリティポリシーの構成

情報セキュリティポリシーとは、組織の情報資産を守るための方針や基準を明文化したもので、基本構成は次の二つです。

① 情報セキュリティ方針 (基本方針)

情報セキュリティに対する組織の基本的な考え方や方針を示すもので、経営陣によって承認されます。目的や対象範囲、管理体制や罰則などについて記述されており、全従業員及び関係者に通知して公表されます。秘密にしておくものではなく、正しく組織内に伝達することや、必要に応じて利害関係者が入手できるようにしておくことが求められています。

②情報セキュリティ対策基準

情報セキュリティ基本方針と、リスクアセスメントの結果に基づいて対策基準を決めます。適切な情報セキュリティレベルを維持・確保するための具体的な順守事項や基準を定めます。



関連

リスクアセスメントについては、「2-2-3 情報セキュリティリスクアセスメント」で解説します。

■ 規程類

規程は、情報セキュリティ対策基準で定めた決まりをどのように実施するかという具体的な手順について記述するものです。代表的な規程には次のようなものがあります。

- ・ 情報管理規程
- ・ 機密管理規程
- ・ 文書管理規程
- ・ マルウェア感染時の対応規程
- ・ 事故への対応規程
- ・ 情報セキュリティ教育の規程
- ・ 雇用契約
- ・ 職務規程
- ・ 罰則の規程
- ・ 対外説明の規程
- ・ 例外の規程
- ・ 規則更新の規程
- ・ 規程の承認手続き

■ 個人情報とプライバシーポリシー

個人情報とは、氏名、住所、メールアドレスなど、それ単体もしくは組み合わせることによって個人を特定できる情報のことです。

プライバシーポリシーとは、収集した個人情報をどう扱うのかを定めた規範のことです。**個人情報保護方針**ともいいます。Webサイトなどで明記されることが多いですが、セキュリティポリシーの一部として記載することもあります。

▶▶ 覚えよう！

- ☐ セキュリティポリシーは、基本方針と対策基準を合わせたもの
- ☐ 具体的な手順については、様々な規程類で明記する

2-1-3 情報セキュリティ マネジメントシステム

情報セキュリティマネジメントシステムは、組織の情報セキュリティを管理するための仕組みです。PDCAサイクルを繰り返し、管理・改善を行っていきます。

適用範囲

情報セキュリティマネジメントシステム（ISMS：Information Security Management System）を構築するときに最初に行うことは、組織の状況を理解し、ISMSの**適用範囲を定義すること**です。事業を継続していくために必要な、保護しなければならない重要な情報は何かを考え、守るべきものの範囲を決定します。

ISMSの適用範囲を決定するときには、事業的、組織的、物理的、ネットワーク的など様々な観点からその範囲を決定します。特に、どこまでを対象とするかという**境界を見定める**ことが大切です。

リーダーシップ

ISMSに関しては、**トップマネジメントのリーダーシップ**が必須です。トップマネジメントとは、企業を指揮、管理する首脳部であり、一般的には社長などの経営陣を指します。リーダーシップとは、組織の目標などに向かって集団活動を導いていくことで、その組織の状況に合わせて行います。リーダーシップには、仕事本位のリーダーシップ以外にも人間関係本位のリーダーシップがあり、組織の発達段階に応じて、そのスタイルを変化させていく必要があります。

情報セキュリティは経営の一環として全社で組織的に行うべきものなので、情報システム部などではなく、経営に関わる企業のトップがリーダーシップをとり、実現させていく必要があります。

トップマネジメントが、情報セキュリティに関連する役割に対して責任及び権限を割り当て、指揮を執り支援を行います。

計画

ISMSの計画を策定する際には、対処すべきリスクを決定する必要があります。そのために、**情報セキュリティリスクアセス**



情報セキュリティリスクアセスメントについては「2-2-3 情報セキュリティリスクアセスメント」で、情報セキュリティリスク対応については「2-2-4 情報セキュリティリスク対応」で詳しく取り上げます。

ントのプロセスを定め、それを運用します。また、その結果を考慮し、適切な**情報セキュリティリスク対応**を選択します。さらに、情報セキュリティの目的を明確にし、文書化しておきます。

■ 運用

情報セキュリティを守るためには、計画したことを継続して実施し、管理していかなければなりません。そのためには適切な運用が不可欠です。定期的に、または組織に重大な変化があった場合には、改めて情報セキュリティリスクアセスメント、リスク対応を実施し、新たなリスクに対応できるようにする必要があります。

■ パフォーマンス評価

ISMSの実施においては、それが有効かどうかを評価する必要があります。具体的には、**内部監査**を行い、ISMSが有効に実施され、維持されているかを確認します。また、トップマネジメントは、**マネジメントレビュー**を行い、ISMSが適切で有効であるかを定期的に確認する必要があります。

■ 改善(不適合及び是正処置、継続的改善)

パフォーマンス評価の結果、不適合が発生した場合には、それを改善する必要があります。その不適合に対する是正処置を実行し、その有効性をレビューします。

また、一度の処置で終わりにするのではなく、**継続的に改善**していく必要があります。

■ 管理目的及び管理策

JIS Q 27001:2014では、附属書Aとして**管理目的及び管理策**のリストが示されています。情報セキュリティのための方針や組織、人的資源のセキュリティ、アクセス制御や暗号、物理的及び環境的セキュリティなどについて、その目的や管理策がまとめられています。ISMSでは、これらのリストから、**必要なすべての管理策**を決定し、必要な管理策が見落とされていないことを検証します。

■ ISMS 適合性評価制度

ISMS 適合性評価制度とは、企業の ISMS が国際規格 (JIS Q 27001) に準拠していることを評価して認定する、日本情報経済社会推進協会 (JIPDEC) の評価制度です。

ISMS 適合性評価制度は、次の機関によって成り立っています。

- ・ 認証機関 …………… ISMS に適合しているか審査して登録する
- ・ 要員認証機関 …… ISMS 審査員の資格を付与する
- ・ 認定機関 …………… 上記の2機関がその業務を行う能力を備えているかをみる

■ ISMS 認証

ISMS 適合性評価制度の認証機関に申請し、審査の結果、認証されると、ISMS 認証を取得できます。ISMS 認証を取得すると、対外的に情報セキュリティの信頼性を証明でき、顧客や取引先からの信頼性の向上につながります。

また、官公庁の入札や電子商取引などの参加条件として提示されることもあります。

■ ISO/IEC 27000 シリーズ

ISO/IEC 27000 シリーズは、ISO (International Organization for Standardization : 国際標準化機構) と IEC (International Electrotechnical Commission : 国際電気標準会議) が共同で策定する情報セキュリティ規格群です。日本では、同じ番号で JIS Q 27000 シリーズとして規格化されています。

27000 シリーズでは、ISMS における情報セキュリティの管理・リスク・制御に対するベストプラクティスが表示されています。主な規格は、次のとおりです。

- ・ ISO/IEC 27000:2014 (翻訳 JIS Q 27000:2014)

情報技術—情報セキュリティマネジメントシステム—用語

ISMS のファミリー規格の概要や、使用される用語について定められています。

・ISO/IEC 27001:2013 (翻訳 JIS Q 27001:2014)

情報セキュリティマネジメントシステム—要求事項

組織がISMSを確立、導入、運用、監視、レビュー、維持し、継続的に改善するための**要求事項**を規定しています。BS(British Standards: 英国規格) 7799第2部を基に2006年に発行された第1版の改定第2版です。

・ISO/IEC 27002:2013 (翻訳 JIS Q 27002:2014)

情報技術—セキュリティ技術—情報セキュリティ管理策の実践のための規範

情報セキュリティ対策のベストプラクティスとして様々な**管理策**が記載されています。組織が、適用宣言書(情報セキュリティを守るという宣言。基本方針)の作成にあたってこれらの管理策も参照し、自社に合った管理策を構築できるようにするための規格です。

BS7799第1部を基にいったんISO/IEC17799:2005が発行され、2007年に規格番号が27002に変更され発行されています。

・ISO/IEC 27003:2010

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システムの実施の手引

ISMSを確立、導入、運用、監視、レビュー、維持及び改善するためのガイダンス規格です。

・ISO/IEC 27004:2009

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—測定

情報セキュリティの実施及び管理に使用すべきISMS、管理目的及び管理策の有効性を評価するための測定方法の開発及び使用に関するガイダンス規格です。

・ISO/IEC 27005:2011

情報技術—セキュリティ技術—情報セキュリティリスクマネジメント

情報セキュリティのリスクマネジメントのガイドラインです。



情報セキュリティに限らない一般的なリスクマネジメントについての規格には、ISO 31000:2009 (翻訳 JIS Q 31000:2010)があります。

・ISO/IEC 27006:2011 (翻訳 JIS Q 27006:2012)

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
システムの監査及び認証を行う機関に対する要求事項

情報セキュリティマネジメントシステムの認証機関のための要
求事項です。



和文で正式にJIS規格として発行されているISO/IEC 27000シリーズは、現在のところ次の四つです。

- ・JIS Q 27000:2014
- ・JIS Q 27001:2014
- ・JIS Q 27002:2014
- ・JIS Q 27006:2012

・ISO/IEC 27007:2011

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
システム監査のための指針

ISMS監査に関するガイドライン規格です。

・ISO/IEC 27014:2013

情報技術—ITガバナンス—

情報技術のガバナンスに関する規格です。

そのほかにも、次のように様々な規格があります。

・ISO/IEC 27010:2012

部門間及び組織間コミュニケーションのための情報セキュリ
ティマネジメントシステムに関する規格

・ISO/IEC 27011:2008

電気通信業界内の組織でのISO/IEC 27002に基づく情報セ
キュリティマネジメント導入を支援するガイドライン規格

▶▶ 覚えよう！

- ☐ ISMSでは、トップマネジメントのリーダーシップが大切
- ☐ JIS Q 27001が要求事項、JIS Q 27002が実践規範

2-1-4 情報セキュリティ継続

緊急時にも情報セキュリティを継続させていくためには、事前の対応計画の策定が不可欠です。組織全体の事業継続計画と整合性をとり、全社的に整合性のある計画を策定する必要があります。



関連

情報セキュリティに限らない全体的な対応計画のことを、事業継続計画(BCP: Business Continuity Planning)といいます。

2

緊急事態の区分

緊急時に適切に対応するためには、緊急の度合いに応じて**緊急事態の区分**を明らかにしておく必要があります。

例えば、緊急時の脅威によって、レベル1（影響を及ぼすおそれのない事象）、レベル2（影響を及ぼすおそれの低い事象）、レベル3（影響を及ぼすおそれの高い事象）などに区分しておくことで、実際に脅威が生じたときの対応を迅速化できます。

緊急時対応計画

緊急時対応計画(Contingency Plan: コンティンジェンシープラン)とは、サービスの中断や災害発生時に、システムを迅速かつ効率的に復旧させる計画です。

初期の対応計画では、初動で何を行うかなどを中心に計画します。完全な復旧を目指さず、暫定的に対応することもあります。

被害状況の調査手法なども定めておき、迅速に情報を集めて対応することが求められます。

復旧計画

緊急時対応の後に事業を完全に復旧させるための計画です。暫定的ではなく恒久的な復旧を目指します。特に、地震などの災害からの復旧の場合には、すぐに完全復旧を行うのは難しいので、暫定的な対応を行った後に順次、通常の状態へと復旧させていきます。

障害復旧

緊急時、または日常においても、システムに障害が発生したときにはその復旧を行います。日頃から、データのバックアップ対策を行っておき、復旧に備えておくことが大切です。

バックアップしたデータは、システムのすぐそばに置いておく方が通常時の復旧は早いですが、地震などの大災害時には、バックアップごと被災してしまうリスクがあります。そのため、バックアップデータは、**遠隔地に保管**しておき、大きな災害に備えることも大切です。

▶▶ 覚えよう！

- ☐ 災害時の対策には、緊急時の暫定的な対策と、その後の恒久的な対策がある
- ☐ 日頃から計画を立て、バックアップなどの準備を行っておくことが大切

2-1-5 演習問題

問1 情報セキュリティ方針

CHECK ▶ ☐☐☐

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。

問2 削除漏れが最も確実に発見できるもの

CHECK ▶ ☐☐☐

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

問3 ISMS適合性評価制度

CHECK ▶ ☐☐☐

ISMS適合性評価制度における情報セキュリティ基本方針に関する記述のうち、適切なものはどれか。

- ア 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。
- イ 情報セキュリティのための経営陣の方向性及び支持を規定する。
- 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4 情報セキュリティに関する文書

CHECK ▶ ☐☐☐

情報セキュリティ基本方針、又は情報セキュリティ基本方針と情報セキュリティ対策基準で構成されており、企業や組織の情報セキュリティに関する取組みを包括的に規定した文書として、最も適切なものはどれか。

- ア 情報セキュリティポリシー
- イ 情報セキュリティマネジメントシステム
- ウ ソーシャルエンジニアリング
- エ リスクアセスメント

■ 解答と解説

問1

(平成28年春 情報セキュリティマネジメント試験 午前 問6)

《解答》イ

JIS Q 27001の「5.2 方針」には、情報セキュリティ方針は、「組織内に伝達する」、「必要に応じて、利害関係者が入手可能である」の事項を満たさなければならないとあります。したがって、イが正解です。

- ア 情報セキュリティ方針は機密情報ではありません。
- ウ 情報セキュリティ方針はトップマネジメントがリーダーシップをとって確立します。
- エ 制定後に見直して改訂していく ISMSのプロセスを確立する必要があります。

問2

(平成28年秋 情報セキュリティマネジメント試験 午前 問7)

《解答》ウ

退職者の利用者IDの削除状況を把握するためには、現在の所属者の情報を基に、その内容と実際のシステムに残っている利用者IDを比較します。そのために、資料Aとして、現在のシステムでの「利用者IDとそれが発行されている者の一覧」を、資料Bとして「組織の現在の所属者の名簿」を用意します。資料Aと資料Bを突き合わせることで、利用者IDの削除漏れが確実に発見できます。したがって、ウが正解です。

- ア、エ 削除申請書は、申請漏れの可能性があるため、確実性の低い資料です。
- イ 退職者の一覧は、申請漏れの可能性や反映漏れの可能性があるため、確実性の低い資料です。

問3

(平成21年春 応用情報技術者試験 午前 問40)

《解答》イ

情報セキュリティ基本方針は、経営陣によって承認されるもので、情報セキュリティのための経営陣の方向性及び支持を規定します。したがって、イが正解です。

- ア 機密文書とするのではなく、全社員に公開し、必要なら外部関係者にも通知します。
- ウ 「変更してはならない」は誤りです。ISMSの一環として整備されるものなので、PDCAサイクルに則って定期的に改善する必要があります。
- エ 情報セキュリティ基本方針ではなく、情報セキュリティ対策実施手順、規程類のことです。

問4

(平成27年春 ITパスポート試験 午前 問47)

《解答》ア

情報セキュリティポリシーとは、組織の情報資産を守るための方針や基準を明文化したものです。情報セキュリティポリシーの基本構成は、「情報セキュリティ基本方針」と「情報セキュリティ対策基準」です。したがって、アが正解です。

イ 情報セキュリティマネジメントの仕組みのことです。

ウ 人間の心理的、社会的な性質につけ込んで秘密情報を入手する手法のことです。

エ リスク分析によって情報資産に対する脅威と脆弱性を洗い出し、そのリスクの大きさを算出することです。

2-2 リスクマネジメント

2

リスクマネジメントとは、リスクを基準として組織を指揮し管理することです。それぞれのリスクに対して評価を行い、リスク低減、リスク移転など、状況に応じた対策を講じます。

2-2-1 情報資産の調査・分類



勉強のコツ

リスクマネジメントでは、情報資産に優先度をつけ、リスクアセスメントを行います。

学習のポイントとなるのは、リスク分析の考え方と、リスク対応の種類です。

リスクマネジメントを行うためには、まず、どのような情報資産があるのかを調査し、それを分類する必要があります。情報資産は、情報資産台帳にまとめます。

情報資産の調査

リスクマネジメントの最初の段階ではまず、ISMSの適用範囲で用いられている情報資産について調査を行います。事業部門ごとに、インタビューや調査票による調査、現地での調査などを行い、漏れのないようにリスクを洗い出します。

また、過去のセキュリティ事件や事故、それによる損害額や対策費用なども考慮し、脅威と脆弱性を認識します。

情報資産の重要性による分類と管理

情報資産は、それぞれ単独で管理すると分析の負荷が大きくなるので、効率化を図るために分類し、グループ化します。情報資産のカテゴリや機能、保管形態などが一致するものを同じグループとし、グループごとに管理します。

情報資産台帳

情報資産とその機密性や重要性、分類されたグループなどをまとめたものを、**情報資産台帳**（情報資産目録）といいます。情報資産台帳は、情報資産を漏れなく記載するだけでなく、変化に応じて適切に更新していくことも大切です。

覚えよう！

- ☐ 情報資産はグループごとにまとめて管理
- ☐ 情報資産台帳に情報資産をまとめ、最新の状態に更新する



リスクマネジメントはセキュリティに限ったことではなく、プロジェクトマネジメントやITサービスマネジメントなど、様々な分野で実施されています。リスクマネジメント規格についてはJIS Q 31000で定義されており、これが一般的なリスクマネジメントの指針となります。

2-2-2 リスクの種類

リスクとは、もしそれが発生すれば情報資産に影響を与えるような事象です。財産に関するものだけでなく、信用や人的損失など様々なリスクが存在します。

■ リスク

リスクとは、まだ起こってはいないことですが、もしそれが発生すれば、情報資産に影響を与える事象や状態のことです。すでに起こったことは、リスクではなく**問題**として処理します。まだ起こっていない、起こるかどうかが不確実なことを、リスクとして洗い出します。

■ リスク源

リスク源(リスクソース)とは、リスクを生じさせる力をもっている要素のことです。リスク源を除去することは、有効なリスク対策となります。

■ リスク所有者

リスクを洗い出し、リスクとして特定したら、**リスク所有者**を決定する必要があります。リスク所有者とは、リスクの運用管理に権限をもつ人のことです。実質的には、情報資産を保有する組織の役員やスタッフが該当すると考えられます。

■ リスクの種類

組織を脅かすリスクには様々な種類があります。次のようなものが代表的なリスクの種類です。

- ・ **財産損失** …… 火災リスクや地震リスク、盗難リスクなど、会社の財産を失うリスク
- ・ **収入減少** …… 信用やブランドを失った結果、収入が減少するリスク
- ・ **責任損失** …… 製造物責任や知的財産権侵害などで賠償責任を負うリスク

- ・ 人的損失 …… 労働災害や新型インフルエンザなど、従業員に影響を与えるリスク

その他、外部サービス利用のリスク、サプライチェーンリスク、SNSによる情報発信のリスク、モラルハザード、オペレーショナルリスクなど、様々なリスクがあります。

■ リスク定量化

リスクは、その重要性を判断するため、金額などで定量化する必要があります。リスク定量化の手法としては、年間予想損失額の算出、得点法を用いた算出などがあります。



サプライチェーンリスクとは、委託先も含めたサプライチェーン全体のどこかで生じた事故・問題で影響を受けるリスクです。

モラルハザードとは、保険に加入していることにより、リスクを伴う行動が生じることです。

オペレーショナルリスクとは、通常の業務活動に関連するリスクの総称です。

▶▶▶ 覚えよう！

- ☐ まだ起こっていないことがリスク、起こってしまったら問題
- ☐ それぞれのリスクでリスク所有者を決める必要がある

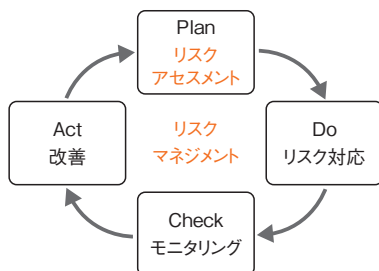
2-2-3 情報セキュリティ リスクアセスメント

情報セキュリティリスクアセスメントとは、リスク分析からリスク評価までのプロセスを指します。リスク分析のためには、様々な手法が提案されています。

リスクマネジメントとリスクアセスメントの違い

情報セキュリティリスクマネジメントでは、リスクに関して組織を指揮し、管理します。そこで行われるのが情報セキュリティリスクアセスメントや情報セキュリティリスク対応などです。

リスクマネジメントがPDCAサイクルの一連のプロセスであるのに対し、リスクアセスメントはPDCAサイクルのP（Plan）の部分に該当します。図にすると次のようになります。



リスクマネジメントとリスクアセスメント

リスク基準

情報セキュリティリスクアセスメントを実施するための基準を**リスク基準**といいます。リスクの重大性を評価するための目安とする条件で、リスクアセスメントの実施者によって評価結果に大きなブレが出ないように、あらかじめ設定しておく判断指標です。

リスクに対して対策を実施するかどうかを判断する基準は、**リスク受容基準**です。

■ リスクアセスメントのプロセス

リスクアセスメントとは、リスク特定、リスク分析、リスク評価を行うプロセス全体のことです。

① リスク特定

リスクを発見して認識し、それを記述します。

② リスク分析

特定したそれぞれのリスクに対し、情報資産に対する脅威と脆弱性を考えます。

リスクの**発生確率**を求め、実際にリスクが起こったときの**影響の大きさ**を考えます。影響の大きさは、単純に、“大”、“中”、“小”などの比較で表すことが多いですが、被害額や復旧にかかる費用などの**金額**で算出することもあります。

リスク分析の手法は、次の2種類に分けられます。

- ・ **定性的リスク分析** ……リスクの大きさを金額以外で分析する手法
- ・ **定量的リスク分析** ……**リスクの大きさを金額で分析する**手法

③ リスク評価

分析したリスクに対し、どのように対策を行うかを判断するのがリスク評価です。リスクが受容可能かどう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なります。

リスク分析の結果を基に、あらかじめ定められた評価基準などを用いてリスクを評価し、対策の優先度をつけていきます。

■ リスク選好とリスク忌避

リスク選好 (risk appetite) とは、リスクのある取引などを行うことです。リスク忌避 (risk aversion。「リスク回避」とも訳されます) とは、リスクを避けるためにその取引などを行わないことです。

■ リスクレベル

リスクレベルとは、リスクの優先度のことです。リスクには、リスクの重大度（重篤度^{じゅうとくと}）と発生の可能性という二つの度合いがあり、これらの組合せでリスクレベルを見積もります。リスクレベルは、次のようなリスクマトリックスで決定します。

リスクマトリックスによるリスクレベルの例

	重大度	重大	中程度	軽度
可能性				
高い		Ⅲ	Ⅲ	Ⅱ
可能性がある		Ⅲ	Ⅱ	Ⅰ
ほとんどない		Ⅱ	Ⅰ	Ⅰ

■ リスク分析の手法

リスク分析の代表的な手法には、次のようなものがあります。

① ベースラインアプローチ

既存の標準や基準をベースラインとして組織の対策基準を策定し、チェックしていく方法です。



詳細リスク分析の代表的な手法に、日本情報経済社会推進協会（JIPDEC：旧日本情報処理開発協会）が開発した **JRAM**（JIPDEC Risk Analysis Method）があります。

JIPDECでは2010年に、新たなリスクマネジメントシステムとして **JRMS2010**（JIPDEC Risk Management System 2010）を公表しました。

② 非形式的アプローチ

コンサルタントや担当者の経験、判断により行います。

③ 詳細リスク分析

情報資産に対し、資産価値、脅威、脆弱性、セキュリティ要件などを詳細に識別し、リスクを評価していく手法です。

④ 組合せアプローチ

複数のアプローチを併用する手法です。

▶▶ 覚えよう！

- ☐ リスクアセスメントではリスク特定、リスク分析、リスク評価を行う
- ☐ リスクを金額で分析するのが定量的リスク分析

2-2-4 情報セキュリティリスク対応

情報セキュリティリスクアセスメントの結果を基に、情報セキュリティリスク対応を決めていきます。

リスク対応の考え方

リスク対応の考え方には、大きく分けて**リスクコントロール**と**リスクファイナンス**(リスクファイナンス)があります。リスクコントロールは、技術的な対策など、なんらかの行動によって対応することですが、リスクファイナンスは資金面で対応することです。

また、リスクが起こったときにその被害を回避する、または軽減するように工夫することを**リスクヘッジ**といいます。

リスクが顕在化したときに備えて、情報化保険(IT保険)を利用する方法もあります。IT事業者向けの賠償責任保険や、個人情報漏えいに特化した保険などが用意されています。

リスク対応の方法

リスクを評価した後で、それぞれのリスクにどのように対応するかを決めていきます。リスクマネジメントの規格であるJIS Q 31000では、リスク対応の方法に次の四つを定義しています。



用語

リスクを扱いやすい単位に分割することをリスク分解、逆にリスクをまとめることをリスク集約といいます。

① リスクを取るまたは増加させる(リスクテイク)

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ます。方法としては次の三つがあります。

- ・ リスク源を除去する
- ・ 起こりやすさを変える
- ・ 結果を変える

一般的なリスクを減らすようなセキュリティ対策はこれに当たります。

② リスクの回避

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、リスクを回避します。例えば、メーリングリストのリスクが高いのでメーリングリストの運用をやめる、などです。

③ リスクの共有 (リスク移転, リスク分散)

一つ以上の他者とリスクを共有します。保険をかけるなどで、リスク発生時の費用負担を外部に転嫁するなどの方法があります。

④ リスクの保有 (リスク受容)

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を受け入れます。具体的な対策をしない対応です。

■ 残留リスク

リスク対応後に残るリスクを**残留リスク**といいます。あるリスクに対してリスク対応をした結果、残るリスクの大きさのことを指します。残留リスクを明確にし、そのリスクが許容範囲かどうかをリスク所有者が再度判断する必要があります。



リスク所有者(リスクオーナー)とは、JIS Q 27000では「リスクを運用管理することについて、アカウントビリティ及び権限をもつ人又は主体」と定義されています。リスクマネジメントの実行権限をもつ人や組織のことを指します。

■ リスク対応計画

リスク対応計画は、それぞれのリスクに対して、脅威を減少させるためのリスク対応の方法をいくつか策定するプロセスです。リスク対応計画を作成するときには、特定したリスクをまとめたリスク登録簿を用意します。そして、それぞれのリスクに対する戦略を考え、**リスク登録簿**を更新します。

■ リスクコミュニケーション

リスクコミュニケーションとは、リスクに関する正確な情報を企業の利害関係者(ステークホルダ)間で共有し、相互に意思疎通を図ることです。特に災害など、重大で意識の共有が必要なリスクについて行われます。

|| ▶▶ 覚えよう!

- ☐ リスクファイナンスは、**金銭的に**リスクに対応すること
- ☐ リスク対応には、リスクテイク、回避、共有(移転)、保有(受容)の4種類がある



最適な対策と現実との兼ね合い

リスク対応では、すべてのリスクに対して完璧に対応できれば最高ですが、現実ではそんなことは不可能であることが多いです。情報セキュリティにかけられる予算は限られていますし、現実的に100%対応することが不可能なリスクも多くあります。また、装置や現場の状況によって、対応までに時間がかかることも多くあります。

例えば、過去に情報セキュリティマネジメント試験に出てきた制約には、次のようなものがあります。

- ・受注業務で、システムへの入力と承認は別の人が必要があるが、承認権限をもつのがN課長1人だけしかおらず、業務が停滞する恐れがある。

(平成28年春 午後 問2)

- ・セキュリティを守るためにはシステム改修が有効だが、ベンダに開発をお願いするので、半年は掛かる。

(平成28年春 午後 問3)

- ・ノートPCの持出しは、その都度申請する管理ルールだったが、持出頻度が高い場合には申請が大変なので、期間持出しを承認していた。

(平成28年秋 午後 問2)

実際の現場では、こういった組織ごとの状況に合わせて対応することが大切なので、情報セキュリティマネジメント試験でも、試験問題の状況に合わせて、適切に対応することが求められます。

「完璧な正解を求めるのではなく、現状に合わせた最適解を考える」ことを念頭に、セキュリティ対策や試験問題の解答を行っていきましょう。

2-2-5 演習問題

問1 リスク受容で求められるもの

CHECK ▶ ☐☐☐☐

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2 ベースラインアプローチ

CHECK ▶ ☐☐☐☐

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。

問3 残留リスク

CHECK ▶ ☐☐☐☐

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4 リスク対応**CHECK** ▶ ☐☐☐

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5 リスク評価**CHECK** ▶ ☐☐☐

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

■ 解答と解説**問1**

(平成28年春 情報セキュリティマネジメント試験 午前 問5)

《解答》ア

JIS Q 27001の「6.1.3 情報セキュリティリスク対応」には、「残留している情報セキュリティの受容について、リスク所有者の承認を得る」とあります。したがって、アが正解です。

イ 受容するリスクについても、モニタリングやレビューを行う必要があります。

ウ、エ リスクを受容するかどうかは、リスク分析後、リスク対応の前に決定します。

問2

(平成28年秋 情報セキュリティマネジメント試験 午前 問6)

《解答》ア

ベースラインアプローチとは、既存の標準や基準をベースラインとして組織の対策基準を策定し、チェックしていく方法です。基準とする望ましい対策をベースラインとして、現状とのギャップを分析するので、アが正解です。

イは非形式的アプローチ、ウは詳細リスク分析、エは組合せアプローチの特徴です。

問3

(平成28年秋 情報セキュリティマネジメント試験 午前 問9)

《解答》エ

JIS Q 31000:2010では、残留リスク(residual risk)は「リスク対応後に残るリスク」と定義されています。したがって、エが正解です。

ア 発見リスクの説明です。

イ 事業リスクの説明です。

ウ 投機的リスクの説明です。

問4

(平成28年秋 情報セキュリティマネジメント試験 午前 問2)

《解答》イ

リスク対応の方法には、リスクテイク、リスクの回避、リスクの共有、リスクの保有の四つがあります。地震保険に加入することは、一つ以上の他者とリスクを共有することなので、リスクの共有に該当します。したがって、イが正解です。

ア、ウはリスクテイク、エはリスクの回避に該当します。

問5

(平成28年秋 情報セキュリティマネジメント試験 午前 問8)

《解答》イ

JIS Q 27000 (情報技術—情報セキュリティマネジメントシステム—用語)では、リスク評価は、「リスク及び／又はその大きさが、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。したがって、イが正解です。

アはリスク対応、ウはリスク分析、エはリスク特定に該当します。

2

2-3 情報セキュリティに対する取組み

情報セキュリティに対する取組みは、組織内だけではなく組織間で連携して行うことが大切です。官公庁でも、様々な取組みが行われています。



勉強のコツ

情報セキュリティに対する取組みは国を挙げてのプロジェクトが多く、日々、その数は増え、進歩しています。単に覚えるだけでは、分量も多く大変なので、どのような機関が何のために行っているのか、その背景や組織との関連を合わせて学習すると、頭に入りやすくなります。

2-3-1 情報セキュリティ組織・機関

進化する情報セキュリティ攻撃から組織を守るためには、組織同士の連携が不可欠です。そのために、CSIRTなどの組織横断的な仕組みがあります。

情報セキュリティ委員会

組織の中における、情報セキュリティ管理責任者(CISO: Chief Information Security Officer)をはじめとした経営層の意思決定組織が、**情報セキュリティ委員会**です。情報セキュリティに関わる企業のビジョンを策定し、情報セキュリティポリシーの決定や承認などを行います。

情報セキュリティ関連組織

情報セキュリティ攻撃は年々進化しており、必要な対策も増えています。こうした状況では、1個人、1組織だけでの情報セキュリティ対策では多様な脅威を認識することができず、十分な対応が取れなくなります。そこで、社内外で連携して情報セキュリティ対策を行うために、SOCやCSIRTなどの組織横断的に連携する仕組みが必要となります。

セキュリティオペレーションセンター

セキュリティオペレーションセンター(SOC: Security Operation Center)とは、セキュリティ監視を行う拠点です。セキュリティ管理を行うIT企業が複数の顧客への対応を集中して行うためのSOCを用意し、顧客のセキュリティ機器を監視し、サイバー攻撃の検出やその対策を行っています。

CSIRT

CSIRT (Computer Security Incident Response Team) とは、主にセキュリティ対策のためにコンピュータやネットワークを監視し、問題が発生した際にはその原因の解析や調査を行う組織です。対応する業務により次のように類別されます。



関連

日本の組織内 CSIRT の連携を行うのは、日本シーサー
ト 協 議 会 (NCA : Nippon
CSIRT Association) です。
<http://www.nca.gr.jp/>
様々な企業が加盟していま
す。

2

・組織内 CSIRT (Internal CSIRT)

各企業や公共団体などで、組織ごとのインシデントに対応する組織です。

・国際連携 CSIRT (National CSIRT)

国や地域を代表するかたちで組織内 CSIRT を連携し、問合せ窓口となる組織です。

・コーディネーションセンター (Coordination Center)

他の CSIRT との情報連携や調整を行う組織です。日本のコーディネーションセンターには、**JPCERT/CC** (Japan Computer Emergency Response Team Coordination Center) があります。

IPA セキュリティセンター

IPA セキュリティセンターは、IPA (情報処理推進機構) 内に設置されているセキュリティセンターです。ここでは**情報セキュリティ早期警戒パートナーシップ**という制度を運用しており、コンピュータウイルス、不正アクセス、脆弱性などの届出を受け付けています。

不正アクセスを届け出るコンピュータ不正アクセス届出制度、脆弱性を届け出るソフトウェア等の脆弱性関連情報に関する届出制度などの提出先となっています。

また、情報セキュリティに関する様々な情報を発信しており、再発防止のための提言や、情報セキュリティに関する啓発活動を行っています。

脆弱性データベース

脆弱性の情報をデータベース化して一般に公開する取組みが、国内外でいくつか行われています。

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する

脆弱性対策情報ポータルサイトです。JPCERT/CCとIPAが共同で運営しています。

JVNでは、次の3種類の番号体系を用いて脆弱性識別番号を割り振り、脆弱性を特定しています。

- ・「JVN#」が先頭に付く8桁の番号

「情報セキュリティ早期警戒パートナーシップ」に基づいて調整・公表された脆弱性情報

- ・「JNVNU#」が先頭につく8桁の番号

上記以外の海外調整機関や海外製品開発者との連携案件

- ・「JVNTA#」が先頭に付く8桁の番号

調整の有無にかかわらず、必要に応じてJPCERT/CCが発行する注意喚起

■ 内閣サイバーセキュリティセンター

内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）とは、内閣官房に設置された組織です。

サイバーセキュリティ基本法に基づき、内閣に**サイバーセキュリティ戦略本部**が設置され、同時に内閣官房にNISCが設置されました。NISCでは、サイバーセキュリティ戦略の立案と実施の推進などを行っています。

内閣では、2015年9月にサイバーセキュリティ戦略を定め、公開しました。この戦略では、目標達成のための施策の立案及び実施にあたっては次の五つの基本原則に従うものとされています。

● サイバーセキュリティ戦略の基本原則

1. 情報の自由な流通の確保

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。

2. 法の支配

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。

3. 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、常に参加を求めるものに開かれたものでなければならない。

4. 自律性

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。

5. 多様な主体の連携

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。

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や運用法を調査・検討するプロジェクトです。CRYPTRECでは、「電子政府における調達のために参照すべき暗号のリスト」(**CRYPTREC 暗号リスト**)を公開しています。CRYPTREC 暗号リストには、次の3種類があります。



関連

CRYPTRECの具体的な内容については、CRYPTRECのWebページに詳しい記述があります。
<http://cryptrec.go.jp/index.html>
CRYPTREC暗号リストなどは、こちらを参考にしてください。

① 電子政府推奨暗号リスト

CRYPTRECにより安全性及び実装性能が確認された暗号技術で、市場における利用実績が十分であるか今後の普及が見込まれると判断され、利用を推奨するもののリストです。

② 推奨候補暗号リスト

CRYPTRECにより安全性及び実装性能が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリストです。

③ 運用監視暗号リスト

推奨すべき状態ではなくなった暗号技術のうち、互換性維持のために継続利用を容認するもののリストです。

■ ホワイトハッカー

コンピュータやネットワークに関する高い技術をもつハッカーと呼ばれる人のうち、その技術を善良な目的に生かす人をホワイトハッカーといいます。

サイバー犯罪に対処するためにも、ホワイトハッカーの育成は急務といわれています。

▶▶ 覚えよう！

- ☐ CSIRTはインシデント対応のチームで、組織内だけでなく組織外とも連携する
- ☐ NISCには、サイバーセキュリティ戦略本部が設置されている

2-3-2 セキュリティ評価

情報セキュリティ対策に役立つデータは、公共機関やセキュリティ関連企業などで、様々なものが公開されています。日々チェックし、セキュリティ管理に役立てることが大切です。

ISO/IEC 15408

情報セキュリティマネジメントではなくセキュリティ技術の評価する規格にISO/IEC 15408 (JIS規格ではJIS X 5070)があります。これは、IT関連製品や情報システムのセキュリティレベルを評価するための国際規格です。CC (Common Criteria : **コモンクライテリア**)とも呼ばれ、主に次のような概念を掲げています。

① ST (Security Target : セキュリティターゲット)

セキュリティ基本設計書のことです。製品やシステムの開発に際して、STを作成することは最も重要であると規定されています。利用者が自分の要求仕様を文書化したものです。

② EAL (Evaluation Assurance Level : 評価保証レベル)

製品の保証要件を示したもので、製品やシステムのセキュリティレベルを客観的に評価するための指標です。EAL1 (機能テストの保証) からEAL7 (形式的な設計の検証及びテストの保証) まであり、数値が高いほど保証の程度が厳密です。



共通の評価基準であるCCに加え、評価結果を理解し、比較するための評価方法「Common Methodology for Information Technology Security Evaluation」が開発されました。共通評価方法 (Common Evaluation Methodology) と略され、その頭文字をとって**CEM**と呼ばれます。ここには、評価機関がCCによる評価を行うための手法が記されています。

PCI DSS

PCI DSS (Payment Card Industry Data Security Standard : PCIデータセキュリティスタンダード) とは、**クレジットカード情報の安全な取扱いのために**、JCB、American Express、Discover、マスターカード、VISAの5社が共同で策定した、クレジットカード業界におけるグローバルセキュリティ基準です。

PCI DSSは、カード会員情報を格納及び処理するすべての組織を対象としており、安全なネットワークの構築や維持、カード会員データの保護などに関する具体的な要件が記述されています。



SCAPについては、IPAセキュリティセンターのWebサイトに詳しい説明があります。
<http://www.ipa.go.jp/security/vuln/SCAP.html>
それぞれの詳しい内容は、こちらを参考にしてください。

SCAP

IPAセキュリティセンターが開発した、情報セキュリティ対策の自動化と標準化を目指した技術仕様をSCAP (Security Content Automation Protocol: セキュリティ設定共通化手順) といいます。

現在、SCAPは次の六つの標準仕様から構成されています。

①脆弱性を識別するためのCVE

(Common Vulnerabilities and Exposures: 共通脆弱性識別子)

個別製品中の脆弱性を対象として、米国政府の支援を受けた非営利団体のMITRE社が採番している識別子です。脆弱性検査ツールやJVNなどの脆弱性対策情報提供サービスの多くがCVEを利用しています。

②セキュリティ設定を識別するためのCCE

(Common Configuration Enumeration: 共通セキュリティ設定一覧)

システム設定情報に対して共通の識別番号「CCE識別番号 (CCE-ID)」を付与し、セキュリティに関するシステム設定項目を識別します。識別番号を用いることで、脆弱性対策情報源やセキュリティツール間のデータ連携を実現します。

③製品を識別するためのCPE

(Common Platform Enumeration: 共通プラットフォーム一覧)

ハードウェア、ソフトウェアなど、情報システムを構成するものを識別するための共通の名称基準です。

④脆弱性の深刻度を評価するためのCVSS

(Common Vulnerability Scoring System: 共通脆弱性評価システム)

情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法です。CVSSを用いると、脆弱性の深刻度を同一の基準の下で定量的に比較できるようになります。また、ベンダー、セキュリティ専門家、管理者、ユーザ等の間で、脆弱性に関して共通の言葉で議論できるようになります。

CVSSでは、以下の三つの視点から評価を行います。

- ・ **基本評価基準** (Base Metrics)
脆弱性そのものの特性を評価する視点
- ・ **現状評価基準** (Temporal Metrics)
脆弱性の現在の深刻度を評価する視点
- ・ **環境評価基準** (Environmental Metrics)
製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する視点

⑤チェックリストを記述するためのXCCDF

(eXtensible Configuration Checklist Description Format : セキュリティ設定チェックリスト記述形式)

セキュリティチェックリストやベンチマークなどを記述するための仕様言語です。

⑥脆弱性やセキュリティ設定をチェックするためのOVAL

(Open Vulnerability and Assessment Language : セキュリティ検査言語)

コンピュータのセキュリティ設定状況を検査するための仕様です。

■ CWE

CWE (Common Weakness Enumeration : 共通脆弱性タイプ一覧) は、ソフトウェアにおけるセキュリティ上の弱点(脆弱性)の種類を識別するための共通の基準です。CWEでは多種多様な**脆弱性の種類**を脆弱性タイプとして分類し、それぞれにCWE識別子(CWE-ID)を付与して階層構造で体系化しています。脆弱性タイプは、下記の4種類に分類されます。

- ・ ビュー (View)
- ・ カテゴリ (Category)
- ・ 脆弱性 (Weakness)
- ・ 複合要因 (Compound Element)

脆弱性検査

システムを評価するために脆弱性を発見する検査のことを**脆弱性検査**といいます。脆弱性検査として、システムに実際に攻撃して侵入を試みる手法を**ペネトレーションテスト**といいます。

情報セキュリティ対策ベンチマーク

情報セキュリティ対策ベンチマークとは、IPAセキュリティセンターがWeb上で提供している、情報セキュリティ対策の状況を診断できる仕組みです。

- ・情報セキュリティ対策ベンチマーク

<http://www.ipa.go.jp/security/benchmark/>

Web上の質問に答えると、散布図、レーダーチャート、スコア(点数)などの診断結果が自動的に表示されます。点数だけでなく、自社の対策状況を他社の対策状況と比較することができます。

覚えよう！

- ☐ CVSSは共通脆弱性評価システムで3つの視点から評価
- ☐ CVEは脆弱性の識別子、CWEは脆弱性のタイプ



IPAの取組みを押さえておく

IPA（Information-technology Promotion Agency, Japan：独立法人情報処理推進機構）は、経済産業省所管の独立行政法人です。日本におけるIT国家戦略を技術面と人材面の両方から支えるために設立されました。

IPAの中には、人材を育成するため、今勉強している情報セキュリティマネジメント試験などの情報処理技術者試験を実施する試験センターも設置されています。また、情報セキュリティの技術面を支えるために、IPAセキュリティセンターを運営しています。

IPAセキュリティセンターでは、脆弱性対策情報（JVN）の提供やSCAPの開発など、情報セキュリティの啓発活動を行っています。同じIPA内で実施する試験なので、セキュリティセンターで実施していることは、一般に普及する前の最新情報も含めて情報セキュリティマネジメント試験で出題されることが予想されます。

IPAの情報を押さえることで、先手を打って情報セキュリティ対策を考えられるようになるという意識で、IPA公式の情報を押さえておくのがおすすめです。

書籍では紹介しきれない最新情報もいろいろ掲載されますので、ぜひ定期的に確認してみてください。

IPAセキュリティセンター

<http://www.ipa.go.jp/security/index.html>

2-3-3 演習問題

問1 CSIRT

CHECK ▶ ☐☐☐

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 JPCERT/CC

CHECK ▶ ☐☐☐

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、手口分析、再発防止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。

問3 JVN

CHECK ▶ ☐☐☐

JVN (Japan Vulnerability Notes) はどれか。

- ア 情報システムに存在する脆弱性の^{せい}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4 コモンクライテリア

CHECK ▶ ☐☐☐

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5 サイバーセキュリティ戦略の基本原則

CHECK ▶ ☐☐☐

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。

■ 解答と解説**問1**

(平成28年春 情報セキュリティマネジメント試験 午前 問1)

《解答》ウ

CSIRT (Computer Security Incident Response Team : シーサート) とは、コンピュータやネットワーク上の問題(主にセキュリティ問題)を監視し、問題が起きた場合にその原因の解析や調査を行う組織です。したがって、ウが正解です。

ア ICANN (Internet Corporation for Assigned Names and Numbers : アイキャン) の説明です。

イ IETF (The Internet Engineering Task Force) の説明です。

エ 共通思想集団の説明です。

問2

(平成28年秋 情報セキュリティマネジメント試験 午前 問3)

《解答》ウ

JPCERT/CC (Japan Computer Emergency Response Team Coordination Center) は、CSIRT (Computer Security Incident Response Team) のコーディネーションセンターで、日本において他のCSIRTとの情報連携や調整を行う組織です。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などを行っています。したがって、ウが正解です。

ア JISC (Japan Industrial Standards Committee : 日本工業標準調査会) の説明です。

イ CRYPTREC (Cryptography Research and Evaluation Committees) の説明です。

エ NISC (National center of Incident readiness and Strategy for Cybersecurity : 内閣サイバーセキュリティセンター) の説明です。

問3

(平成28年秋 情報セキュリティマネジメント試験 午前 問4)

《解答》ウ

JVN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する脆弱性対策情報ポータルサイトです。したがって、ウが正解です。

ア CVSS(Common Vulnerability Scoring System: 共通脆弱性評価システム) の説明です。

イ CVE (Common Vulnerabilities and Exposures : 共通脆弱性識別子) の説明です。

エ CSIRT (Computer Security Incident Response Team) 説明です。

問4

(平成28年秋 情報セキュリティマネジメント試験 午前 問30)

《解答》ウ

コモンクライテリアとは、IT関連製品や情報システムのセキュリティレベルを評価するための国際規格で、ISO/IEC 15408として定義されています。したがって、ウが正解です。

アは品質マネジメント、イは環境マネジメント、エは情報セキュリティのリスクマネジメントのための国際標準です。

問5

(平成28年秋 情報セキュリティマネジメント試験 午前 問23)

《解答》ア

サイバーセキュリティ戦略の五つの基本原則の三番目に「開放性」があり、「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、常に参加を求めるものに開かれたものでなければならない」と定められています。したがって、アが正解です。

- イ 基本原則「自律性」に、「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」と定められています。
- ウ 基本原則「情報の自由な流通の確保」に、「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」と定められています。
- エ 基本原則「法の支配」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」と定められています。

第3章

情報セキュリティ対策

情報セキュリティの脅威に関しては、リスクを認識して優先度を考えたあとに、必要に応じて適切に対策を行うことが大切です。

この章では、情報セキュリティ対策について、人的セキュリティ対策、技術的セキュリティ対策、物理的セキュリティ対策、及びセキュリティ実装技術の4分野に分けて学習していきます。

3-1 人的セキュリティ対策

- ◆ 3-1-1 人的セキュリティ対策
- ◆ 3-1-2 演習問題

3-2 技術的セキュリティ対策

- ◆ 3-2-1 不正アクセス対策
- ◆ 3-2-2 マルウェア・不正プログラム対策
- ◆ 3-2-3 その他の技術的セキュリティ対策
- ◆ 3-2-4 セキュリティ製品・サービス
- ◆ 3-2-5 演習問題

3-3 物理的セキュリティ対策

- ◆ 3-3-1 物理的セキュリティ対策
- ◆ 3-3-2 演習問題

3-4 セキュリティ実装技術

- ◆ 3-4-1 セキュアプロトコル
- ◆ 3-4-2 ネットワークセキュリティ
- ◆ 3-4-3 データベースセキュリティ
- ◆ 3-4-4 アプリケーションセキュリティ
- ◆ 3-4-5 演習問題

3-1 人的セキュリティ対策

綿密にポリシーや規程を作り上げて明文化しても、それを運用する人のセキュリティ意識が低ければ意味がありません。教育などの活動によって啓発していく必要があります。



勉強のコツ

人的セキュリティ対策は、実質的に効果があるように組織的な対策を考えていくことがポイントです。基本的な知識を身に付けた後は、午後問題の演習などで事例を学習していくことが効率的な試験対策となります。



関連

IPA セキュリティセンターが発行している「組織における内部不正防止ガイドライン」などは、下記のURLから確認できます。
<https://www.ipa.go.jp/security/fy24/reports/insider/>

3-1-1 人的セキュリティ対策

人的セキュリティ対策では、情報セキュリティの重要性や対策の方針を組織全体に浸透させていくことが大切です。そのためにガイドラインを作成し、啓発活動を行っていきます。

組織における内部不正対策

組織における内部不正を防止するためには、**内部不正対策の体制**を構築することが重要です。「組織における内部不正防止ガイドライン」によると、内部不正防止の基本原則は次の五つです。

1. 犯罪を難しくする（やりにくくする）
2. 捕まるリスクを高める（やると見つかる）
3. 犯罪の見返りを減らす（割に合わない）
4. 犯行の誘因を減らす（その気にさせない）
5. 犯罪の弁明をさせない（言い訳させない）

具体的な内部不正対策としては、次のようなことを実行していく必要があります。

①資産管理

それぞれの情報にアクセス権を指定し、アクセス管理を行います。また、機密情報には**秘密指定**を行い、外部に漏えいしないように管理します。

②情報機器や記憶媒体の持込、持出管理

持出可能なノートPCやスマートフォンなどの情報機器や、USBメモリ、CD-Rなどの記憶媒体について、持出しの承認、記録等の管理を行います。個人の情報機器や記憶媒体の業務利用

や持込みは制限します。また、持ち出すときに情報を暗号化するなどの対策を施す必要があります。

③業務委託時の確認

業務委託をする場合には、セキュリティ対策を事前に確認・合意してから契約し、委託先が契約どおりに情報セキュリティ対策を実施しているか**定期的に確認**する必要があります。

④証拠確保

アクセス履歴や操作履歴のログ・証跡を残します。システム管理者のログ・証跡もきちんと残し、**システム管理者以外の者が定期的に確認**する必要があります。

⑤雇用終了時の手続き

雇用終了時に、必要に応じて**秘密保持義務を課す誓約書の提出**を求めるなど、退職後の重要情報の漏えい等の不正行為が発生しないようにする必要があります。また、雇用終了時には情報資産をすべて返却し、**情報システムの利用者IDや権限を削除**しなければなりません。

⑥適正な労働環境及びコミュニケーションの推進

労働環境が悪く、コミュニケーションが十分に図れていないとストレスがたまり、内部不正が発生するおそれが高くなります。それを防ぐために、適正な労働環境と、適切にコミュニケーションが図れる環境を用意する必要があります。

⑦相互監視

単独作業では不正が発生しやすいため、**相互監視ができない環境での仕事を制限**します。具体的には、休日や深夜などの単独での作業を制限する必要があります。

■ 情報セキュリティ啓発

情報セキュリティ啓発とは、情報セキュリティに関する意識や知識を向上させるための取組みを周知徹底させていく活動のことです。情報セキュリティ啓発の主な内容は次のような活動になります。

①教育(情報セキュリティ教育)

策定した情報セキュリティポリシーの周知や、ソーシャルエンジニアリングに対する心構えなどについて、集合教育や各人への指導などによって教育していきます。教育の対象は、派遣従業員や取締役なども含めた、組織に関係する全関係者となります。また、教育は業務に従事する者に対して業務を最初に行う前に実施し、従事後も定期的に実施します。内容は、対象者の担当業務や役割、責任に応じて変更する必要があります。

②訓練

攻撃を受けた想定での実践や、手順に従って実際に対応するなどの訓練を行います。

③資料配付

情報セキュリティに関する必要な事項を資料にまとめ、配付します。

④メディア活用

動画やソーシャルメディア、eラーニングなど、様々なコンテンツを活用して啓発を行っていきます。

■ パスワード管理

パスワード管理の方法は、教育などで周知徹底させる必要があります。そのポイントは次のとおりです。

①質の良いパスワードを設定する

パスワードは、推測されにくく文字数の多いものを設定することが大切です。

②同じパスワードを使い回さない

システムごとに異なるパスワードを用意し、使い分けることが大切です。

③組合せでパスワードを管理する

パスワードを覚えられないときに紙に書いたりアプリで保管したりすると、それが漏えいした場合に被害にあう可能性があります。「アプリ+紙」など、複数の組合せでパスワードを管理すると、漏えいの危険性が下がります。

④パスワードをPCに保管しない

パスワードやIDはPCに保管せず、毎回入力するようにします。PCに記憶させて自動的に認証できるようにしないことが大切です。

■ 利用者アクセスの管理

利用者のアクセスを適切に制限するため、アカウント管理を行うことが重要です。通常の利用者権限だけでなく、特定のユーザのみに付与される、システムを変更することができる**特権的アクセス権**の管理も適正に行い、特権ユーザを1人1人識別できるようにしておく必要があります。

利用者にアクセス権を設定する際の最も大切な考え方は、**Need-to-know（最小権限）**の原則です。必要最小限のアクセス権を与え、業務に必要なない情報は見せないようにすることが大切です。例えば、業務でJavaScriptなどのプログラムを使用する必要がない場合にはJavaScriptを無効にすることなどが有効です。また、職位の高い人（部長など）にすべてのアクセス権を与えるなどの運用は、不正を行いやすくしてしまうので、職務に必要な最低限のアクセス権限を設定する必要があります。

■ ログ管理と監視

利用者のアクセスについては、ログ管理を行い、アクセスログを保管して、誰がいつアクセスしたのかを正確に管理する必要があります。ログを取得するだけでなく、ログを**監視**し、定期的にチェックすることが大切です。

また、ログを監視していることを周知するだけで、内部不正

の**抑止効果**があります。ログを監視していることは周知するが、具体的な監視方法は知らせないことが、不正を防止するために最も効果的です。

▶▶ 覚えよう！

- ☐ 情報セキュリティ啓発を行い、人の意識を変えていくことが大事
- ☐ 監視を行うことで不正の抑止効果が上がる

3-1-2 演習問題

問1 組織の適切な情報セキュリティ対策

CHECK ▶ ☐☐☐

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に設定させる。
- 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2 利用者アクセスログの取扱い

CHECK ▶ ☐☐☐

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。

問3 内部不正防止の施策**CHECK** ▶ ☐☐☐

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4 情報セキュリティ教育**CHECK** ▶ ☐☐☐

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。

問5 システム管理者による内部不正防止**CHECK** ▶ ☐☐☐

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6 特権的アクセス権

CHECK ▶ ☐☐☐

情報システムに対するアクセスのうち、JIS Q 27002で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。

■ 解答と解説**問1**

(平成28年春 情報セキュリティマネジメント試験 午前 問7)

《解答》ア

IPA「組織における内部不正ガイドライン」では、「4.4.技術・運用管理(12) ネットワーク利用のための安全管理」に、「組織のネットワーク利用では、PC等の情報機器から重要情報が漏えいしないように、ファイル共有ソフト及びソーシャル・ネットワーク・サービス(SNS)、外部のオンラインストレージ等の使用を制限して安全なネットワーク環境を整えなければならない」とあります。したがって、アが正解です。

イ 私用のメールアドレスなどの利用は制限すべきです。

ウ ウイルス対策ソフトは、常に有効にしておく必要があります。

エ 組織が使用を許可していないソフトウェアはインストールしてはいけません。

問2

(平成28年春 情報セキュリティマネジメント試験 午前 問10)

《解答》エ

IPA「組織における内部不正ガイドライン」では、「4.5.証拠確保(17) 情報システムにおけるログ・証跡の記録と保存」に、「内部不正の早期発見及び(27)の事後対策の影響範囲の観点から、重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を記録し、定めた期間に安全に保存することが望ましい」とあります((27)は「事後対策に求められる体制の整備」に関する記述です)。したがって、エが正解です。

ア ログの保管は定めた期間とします。

イ、ウ 内部不正を助長することになるので適切ではありません。

問3

(平成28年秋 情報セキュリティマネジメント試験 午前 問11)

《解答》エ

IPA「組織における内部不正防止ガイドライン」では、「4.8.職場環境(26) 職場環境におけるマネジメント」に、「組織内では、他の役職員が不在で相互監視ができない環境における単独作業を制限することが望ましい」とあります。単独作業は相互監視のできない環境であり、内部不正が発生する可能性が高くなるからです。したがって、エが正解です。

ア、ウ 「4.8.職場環境(25) 適正な労働環境及びコミュニケーションの推進」では、健全な労働環境や良好なコミュニケーションがとれる環境でないと、業務への悩みやストレスを抱えてしまい、内部不正が発生する可能性が増すことから、制限をしないことが推奨されます。

イ 「4.5.証拠確保(18) システム管理者のログ・証拠の確認」に、ログ・証拠を定期的にシステム管理者以外が確認しなければならないと記述されています。

問4

(平成28年秋 情報セキュリティマネジメント試験 午前 問10)

《解答》エ

JIS Q 27002:2014によると、「7.2.2 情報セキュリティの意識向上、教育及び訓練」の管理策に、「組織の全ての従業員、及び関係する場合には契約相手は、職務に関連する組織の方針及び手順についての、適切な、意識向上のための教育及び訓練を受け、また、定めて従ってその更新を受けることが望ましい」とあります。派遣従業員に関しても教育を実施する必要があるので、エは改善が必要な状況となります。

ア、イ、ウは、教育実施の観点から望ましい内容です。

問5

(平成28年春 情報セキュリティマネジメント試験 午前 問15)

《解答》ウ

内部不正を防止する対策としては、一人のシステム管理者に権限が集中しないように権限を分散し、相互に監視できるようにする必要があります。したがって、ウが正解です。

ア 複数の管理者IDを利用する必要があります。

イ 必要時のみ特権が付与された管理者IDを使う必要があります。

エ 操作ログのアクセス権限は本人に付与しません。

問6

(平成28年春 情報セキュリティマネジメント試験 午前 問8)

《解答》ウ

JIS Q 27002の「9.2.3 特権的アクセス権の管理」に、「各々のシステム又はプロセス(例えば、オペレーションシステム、データベース管理システム、各アプリケーション)に関連した特権的アクセス権」とあります。つまり、特権的アクセス権とは、システムを管理特権で操作するために必要な権限です。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際には特権的アクセス権が必要なので、ウが正解です。

ア、イは通常のアクセス権、エはゲスト用のアクセス権を利用した行為です。

3-2 技術的セキュリティ対策

技術的セキュリティ対策には、不正アクセス対策、マルウェア対策などをはじめ様々なものがあります。また、製品やサービスなどいろいろな用意されています。



勉強のコツ

技術的セキュリティ対策では、その技術でできるだけでなく“できないこと”も押さえておくことがポイントとなります。

例えば、ファイアウォール、IDS、IPSはそれぞれ役割もできることも異なりますが、その違いを押さえておくことが大切です。



関連

不正アクセス禁止法については、「4-1-2 不正アクセス禁止法」で詳しく取り上げています。

3-2-1 不正アクセス対策

不正アクセス対策のためには、ファイアウォール、IDS、IPSなど様々な機器があり、それぞれを状況に応じて使い分ける必要があります。

不正アクセス

不正アクセスとは、不正アクセス禁止法に定義された不正アクセス行為や不正アクセスを助長する行為のことです。ハッキングともいわれます。具体的には、OSやアプリケーションの脆弱性(**セキュリティホール**)を利用してコンピュータに侵入したり、バックドアを利用して侵入したりすることなどです。

不正アクセス対策には、不正なアクセスを制御するためのアクセス制御技術を利用します。

クラッキング

クラッキングとは、他人のコンピュータに侵入し、データの取得や改ざん、OSの破壊などの攻撃を目的としている行為です。不正アクセスとの違いは、侵入した後に攻撃を行うことを目的としているかどうかです。

クラッキング対策では、不正アクセス対策と同様のアクセス制御なども重要ですが、その後の攻撃に備えるための対策(出口対策など)を行う必要があります。

アクセス制御技術

アクセス制御技術とは、ネットワークにおけるアクセス権限を適切に管理し、アクセスを制御するための技術です。代表的なものに、ファイアウォールと、IDSやIPSなどの侵入検知システムがあります。

■ ファイアウォール

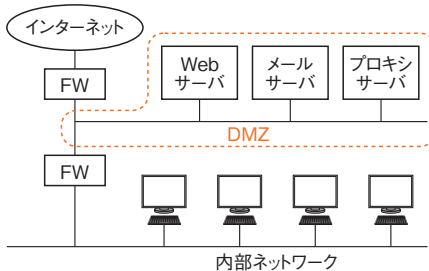
ファイアウォール (FW) とは、ネットワーク間に設置され、パケットを中継するか遮断するかを判断し、必要な通信のみを通過させる機能をもつものです。判断の基準となるのは、あらかじめ設定された ACL (Access Control List : アクセス制御リスト) です。

ファイアウォールの方式には主に、IPアドレスとポート番号を基にアクセス制御を行う**パケットフィルタリング型**と、HTTP、SMTPなどのアプリケーションプログラムごとに細かく中継可否を設定できる**アプリケーションゲートウェイ型**の2種類があります。

いずれの方式でも、インターネットから内部ネットワークへのアクセスは制御されます。しかし、完全に防御するだけでなく、外部に公開する必要がある Web サーバやメールサーバなどもあります。そこで、インターネットと内部ネットワークの間に、中間のネットワークとして**DMZ (非武装地帯 : DeMilitarized Zone)** が設置されるようになりました。



ファイアウォールなどのアクセス制御機器を理解するには、ネットワークの知識が不可欠です。詳しくは、「6-1 ネットワーク」で詳しく取り上げますので、そちらで学習してください。



DMZの設置

■ WAF

WAF (Web Application Firewall) は、Webアプリケーションの防御に特化したファイアウォールです。SQLインジェクションやクロスサイトスクリプティングなど、Webに特化した攻撃に対してきめ細かいアクセス制御を行います。

WAFの方式には、攻撃と判断できるパターンを登録しておき、それに該当する通信を遮断するブラックリスト方式と、正常と判断できるパターンを登録しておき、それに該当する通信のみを通過させるホワイトリスト方式の二つがあります。ホワイトリスト

はユーザが独自に設定しますが、ブラックリストは通常、WAFのベンダが提供し、適宜更新するため、ブラックリストの方が追加の運用コストがかかりません。

IDS

IDS (Intrusion Detection System:侵入検知システム)は、ネットワークやホストをリアルタイムで監視し、侵入や攻撃など不正なアクセスを検知したら管理者に通知するシステムです。

IDSには、ネットワークに接続されてネットワーク全般を監視するNIDS (ネットワーク型IDS)と、ホストにインストールされ特定のホストを監視するHIDS (ホスト型IDS)があります。それぞれの特徴は下表のとおりです。

IDSの種類とその特徴

種類	メリット	デメリット
NIDS	・ネットワーク全体を監視できる ・ホストに負荷がかからない	・暗号化されたパケットやファイルの改ざんなど、検知できない攻撃がある
HIDS	・ファイルの改ざんなど、きめ細かい監視ができる ・暗号化ファイルも復号して検査できる	・すべてのホストに導入する必要がある ・ホストに負荷がかかる

ファイアウォールとIDSの違いは、ファイアウォールでは、IPヘッダ、TCPヘッダやアプリケーションヘッダなどの限られた情報しかチェックできないのに対して、IDSでは検知する内容を自由に設定できることです。そのため、IDSでは、不正アクセスのパターンを集めたシグネチャを登録しておけば、それと照合することで不正アクセスを検出できます。また、IDSでは正常なパターンを登録しておき、それ以外を異常として検知するアノマリ検出も可能です。

IPS

IDSは侵入を検知するだけで防御はできないので、防御も行えるシステムとして用意されたのが、IPS (Intrusion Prevention System: 侵入防御システム)です。

IDSに比べて安全性は高まりますが、処理が遅くなるという欠点があります。

■ UTM

UTM (Unified Threat Management : 統合脅威管理) は、不正アクセスやウイルスなどの脅威からネットワークを全体的に保護するための管理手法です。

実際には、ファイアウォールやIPS、ウイルス対策ソフトや迷惑メールフィルタなど、セキュリティに必要な機能を1台にまとめた機器を指すことが多いです。

UTMを1台導入すればとりあえず一通りのセキュリティ対策ができるという利点がありますが、完全にすべての脅威を防御できるわけではありません。また、ウイルス対策やIPSなどは定期的に更新する必要があるので、適切に管理を続けないと役に立たなくなるおそれがあります。

▶▶ 覚えよう！

- ☐ Webに特化したファイアウォールがWAF
- ☐ IDSは攻撃を検知, IPSは防御

3-2-2 マルウェア・不正プログラム対策

マルウェア・不正プログラム対策では、感染を防ぐための入口対策だけでなく、感染した後に被害を広げないための出口対策も重要です。

関連

マルウェアの具体的な種類などについては、「1-2-1 サイバー攻撃手法」で取り上げています。攻撃の内容はこちらでご確認ください。

マルウェア・不正プログラム対策

マルウェアや不正プログラムの対策では、次の三つを**確実にすべてのコンピュータ**で行うことが重要です。マルウェアの感染はほとんど、この三つが正しく行われていないコンピュータで起きます。

①ウイルス対策ソフトの導入

コンピュータにウイルス対策ソフトを導入し、常に稼働させておきます。導入されていても削除する利用者がいるので、アクセス権限を設定し、管理者以外が削除できないようにすることも有効です。

②ウイルス定義ファイルの更新

ウイルス定義ファイル（パターンファイル）を常に更新し、最新の状態を維持しておきます。自動的にウイルス定義ファイルを最新版にアップデートする機能を有効にし、更新のし忘れのないようにすることも大切です。

③ソフトウェア脆弱性の修正

OSやアプリケーションの脆弱性が発見されたときには、それを修正するためのセキュリティパッチが公表されます。これらを適切に適用することが大切で、自動的に行う設定にしておくことも有効です。

入口対策と出口対策

標的型攻撃などと同様、マルウェアを完全に防ぐことはできません。そのため、ウイルス対策ソフトの導入、ウイルス定義ファイルの更新といった**入口対策**だけでなく、感染後にウイルスを外部に接続できないようにするための**出口対策**も大切です。

■ 検疫ネットワーク

検疫ネットワークとは、社外から持ち込んだり、持ち出して社外のネットワークに接続した後で社内のネットワークに接続したりするコンピュータに対してマルウェア対策を行う専用のネットワークです。

社内のネットワークに接続したコンピュータは、まず検疫ネットワークに接続され、ウイルス対策ソフトやウイルス定義ファイルなどが最新の状態であることを確認されます。最新でない場合は、最新版へのアップデートを行います。マルウェアに感染しておらず、ウイルス定義ファイルが最新版であることが確認できたコンピュータのみ、社内の業務を行う通常のネットワークに接続することが可能となります。

■ マルウェア検知後の対応

マルウェアを検知したときは、ウイルス対策ソフトの事業者が対策を発表している既知のマルウェアであれば、その対応手順に従って対処します。未知のマルウェアであれば、契約している情報セキュリティ事業者に報告するなどして対処を依頼します。

依頼を受けた事業者は、マルウェアの検体(マルウェアだと思われるソフトウェア)について、逆アセンブル(ソフトウェアからプログラムを復元すること)などの手法で新種ウイルスの動作を解明します。

|| ▶▶ 覚えよう！

- ☐ ウイルス対策ソフトは、すべてのコンピュータに漏れがないようインストールする
- ☐ 入口対策だけでなく、出口対策にも気を配る

3-2-3 その他の技術的セキュリティ対策

技術的セキュリティ対策には、これまで取り上げた対策以外に、秘匿化や脆弱性管理、メールやWebのセキュリティ対策など、様々なものがあります。

秘匿化

秘匿化とは、情報を秘密にし、必要な人以外は読めないようにすることです。具体的には、暗号化技術などでデータを変換し、特定の人以上では復号できないようにします。

秘匿化には、データそのものの暗号化に加え、ハードディスクの暗号化、データベースの暗号化など、情報をまとめて暗号化する方法も含まれます。

脆弱性管理

脆弱性(セキュリティホール)は、OSやアプリケーションにおいて随時発見され、修正プログラムを配布するなどの対策が施されています。そのため、企業などの組織では使用しているOSやアプリケーションに脆弱性が発見された場合に速やかに対処するための脆弱性管理の仕組みを作っておく必要があります。

具体的には、IPAセキュリティセンターなどで発表される脆弱性情報を日々チェックし、必要な場合にはOSのアップデートや脆弱性修正プログラムの適用を行います。

また、ソフトウェア製品において、開発者が認知していない脆弱性を検出する技術にファジングがあります。ファジングとは、検査対象のソフトウェア製品に、ファズ(Fuzz)と呼ばれる問題を引き起こしそうなデータを大量に送り込み、その応答や挙動を監視することで脆弱性を検出する検査手法です。

電子メールのセキュリティ

電子メールのセキュリティでは、SPAM(迷惑メール)を送らない、また、受け取らないことが重要です。そのためには、電子メールを送受信するときに認証する対策が有効です。それには次のような技術を利用します。

① SPF (Sender Policy Framework)

電子メールの認証技術の一つで、差出人のIPアドレスなどを基にメールのドメインの正当性を検証します。DNSサーバにSPFレコードとしてメールサーバのIPアドレスを登録しておき、送られたメールと比較します。

② DKIM (Domain Keys Identified Mail)

電子メールの認証技術の一つで、デジタル署名を用いて送信者の正当性を立証します。署名に使う公開鍵をDNSサーバに公開しておくことで、受信者は正当性を確認できます。

③ SMTP-AUTH

送信メールサーバで、ユーザ名とパスワードなどを用いてユーザを認証する方法です。

④ OP25B (Outbound Port 25 Blocking)

迷惑メールの送信に自社のネットワークを使われないようにするための対策です。直接、25番ポートでSMTP通信を行うことを防止します。

また、電子メールの誤送信対策としては、送信時に宛先メールアドレスを確認することや、それをメールのシステムで補助することが有効です。

■ DNSSEC

DNSSEC (DNS Security Extensions) は、DNS (Domain Name System) でのセキュリティに関する拡張仕様です。クライアントとサーバの両方がDNSSECに対応しており、該当するドメインの情報が登録されていれば、DNS応答レコードの偽造や改ざんなどを検出できます。

■ Webのセキュリティ

Webのセキュリティについては、WAFなど様々なものが利用され、アクセス制御が行われます。それ以外のWeb特有のセキュリティとしては、URLのリストを使用し、そのリストに当てはまる

ものを遮断、もしくは通過させるURLフィルタリングがあります。また、通信内容のキーワードなど、コンテンツの中身を基に遮断または通過させるコンテンツフィルタリングという手法もあります。

■ ハードディスク暗号化



ハードディスクドライブ (Hard Disk Drive: HDD) は、磁気ディスクを利用した補助記憶装置です。ハードディスクと略されることが一般的で、JIS規格でもハードディスクと定義されています。試験問題ではHDDと略号で記述されることも多く、また、ハードディスクに設定するパスワードは一般的にHDDパスワードと言われるため、両方とも知っておくと確実です。

ハードディスクは、ノートPCなどに内蔵されている場合でも、機密情報を扱う場合には適切な暗号化を行う必要があります。

ノートPCへのログイン時には、OSでのユーザIDやログインパスワードの認証がありますが、この認証だけでは、ハードディスクを単独で取り出されると、情報を直接確認することができてしまいます。また、OS起動時の認証であるBIOS (Basic Input/Output System) パスワードを設定することも可能で、OSが起動する前にアクセス制限をかけられますが、これもハードディスクを取り出された場合には効果がありません。

ハードディスクを暗号化する場合には、適切なHDDパスワードを設定し、パスワードを入力しないと復号できないように設定する必要があります。

■ スマートデバイスのセキュリティ

携帯端末、特にスマートデバイス (スマートフォンやタブレット) は高機能で携帯性にも優れており、ユーザに関する情報が大量に保存されています。近年では、その情報を狙った攻撃が増加しています。

スマートデバイスは、高機能でPCと同様の機能をもつと同時に、PCと同様の脆弱性もあります。ウイルスや不正なアプリケーションの導入などの脅威が大きいのですが、PCのようにウイルス対策が行われていないのが現状です。そのため、スマートデバイスを業務で活用する従業員がいる場合には、スマートデバイスに対するセキュリティ対策を新たに考える必要があります。

具体的な対策としては、次の六つが挙げられます。

- OSをアップデートする
- 改造行為を行わない
- 信頼できる場所からアプリケーションをインストールする

- Android 端末では、アプリケーションをインストールする前に、アプリケーションがアクセスする許可範囲を確認する
- セキュリティソフトを導入する
- 小さなPCと考え、PCと同様に管理する

■ 無線LANセキュリティ

無線LANは、有線LANと異なり電波を使ってデータをやり取りするので、盗聴が容易です。そのため、無線LANの利用にあたっては暗号化などでセキュリティを確保することが重要になります。まず、無線LANアクセスポイントを誰でも利用可能にすると、不正アクセスに使われる危険があるので、認証できないPCはアクセスを拒否する**ANY 接続拒否**を設定する必要があります。

無線LANの暗号化方式には、次のものがあります。

① WEP

無線LANでセキュリティを確保するための最も基本的な暗号方式がWEP (Wired Equivalent Privacy : 有線同等機密)です。暗号化アルゴリズムには、RC4が用いられます。暗号化鍵の長さは40ビットまたは104ビットで、これに毎回変更されるランダム値である24ビットのIV (Initialization Vector)を追加して、64ビットまたは128ビットとします。

なお、暗号解読者によって弱点が発見され解読が容易になったため、現在ではWEPの使用は推奨されていません。

② WPA

Wi-Fi Protected Access (WPA) は、無線LAN製品の普及を図る業界団体であるWi-Fi AllianceがWEPの脆弱性対策として策定した認証プログラムです。WPAではIVが48ビットになり、TKIP (Temporal Key Integrity Protocol) を利用して、システム運用中に動的に鍵を変更できます。

③ WPA2

WPAの改良版で、暗号化アルゴリズムとしてAES暗号ベースのAES-CCMP (AES Counter-mode with CBC-MAC Protocol) を使用します。

また、SSID (Service Set Identifier)、またはESSID (Extended SSID) は、無線LANアクセスポイントなどに設定されるネットワーク識別子なので、通常はネットワーク上でSSIDを通知します。

しかし、SSIDが明らかになると不正アクセスされやすくなるため、それを隠す**SSIDステルス**といった方法がとられることもあります。

■ クラウドサービスのセキュリティ

クラウドサービスとは、インターネットなどのネットワークを通じてアプリケーションやストレージなどを利用できるサービスです。

クラウドサービスは、独自に構築するシステムとは異なり、データをデータセンタなどの外部に保管するため、その特性に応じたセキュリティ対策が必要となります。

クラウドサービスを提供する事業者は、情報セキュリティ対策を行う必要があり、利用者はそれが適切に行われているかどうかを確認する必要があります。具体的には、次のようなことをチェックします。

- データセンタの物理的セキュリティ対策
- 不正アクセスや脆弱性、マルウェア対策
- アクセスログの取得
- バックアップの取得や障害対策
- 通信経路の暗号化やアクセス制御

■ 電子透かしとステガノグラフィ

電子透かしとは、画像や音楽などのデジタルコンテンツに情報を埋め込む技術です。電子透かしには、画像の合成など、見ただ目で判別可能なものもありますが、通常は知覚困難です。テキストやプログラムなどの情報を埋め込むことにより、著作権情報などを明らかにし、データの不正コピーや改ざんなどを防ぎます。

電子透かしの基になった技術に、データを隠蔽して情報をバインディング (結合) する技術である**ステガノグラフィ**があります。

■ デジタルフォレンジックス

デジタルフォレンジックスとは、法科学の一分野です。不正アクセスや機密情報の漏えいなどで法的な紛争が生じた際に、原因究明や捜査に必要なデータを収集・分析し、その法的な証拠性を明らかにする手段や技術の総称です。例えば、ログを法的な証拠として成立させるためには、ログが改ざんされないような工夫をする必要があります。

また、証拠としてのログは、時間が正確なことで、サーバ同士で時刻が同じになっていることが重要です。そのために、**NTP** (Network Time Protocol) を用いて時刻同期を行うことが有効です。

▶▶ 覚えよう！

- ☐ SPFはIPアドレス、DKIMはデジタル署名で電子メールを認証
- ☐ WPA2はWPAの改良版で、AESをベースとした手法で暗号化

3-2-4 ■ セキュリティ製品・サービス

セキュリティ対策に関連した製品やサービスとしては様々なものが開発・提供されています。

■ ウイルス対策ソフト

ウイルス対策ソフトは、ウイルスをはじめとするマルウェアを検出するためのソフトウェアです。ウイルス定義ファイル（パターンファイル）と呼ばれるファイルと比較することでウイルスを検出する**パターンマッチング**という手法が主流です。

パターンマッチング以外にも、ウイルスと疑われる異常な挙動（ふるまい）を検出する**ビヘイビア法**や、安全な場所に保管しておいた原本と比較し、ウイルス感染を検出する**コンペア法**などがあります。

また、パターンマッチングやコンペア法では、元のファイルではなく、ハッシュ値などを利用して簡便にチェックすることもあります。ハッシュ値やファイル容量などで簡便に変更をチェックするコンペア法を、特に**チェックサム法**ということもあります。

■ パーソナルファイアウォール

パーソナルファイアウォールは、PCなどのコンピュータ1台1台に導入する、ファイアウォール機能をもったソフトウェアです。ウイルス対策ソフトと同時に導入されることが多いです。

■ SSL アクセラレータ

SSL（TLSも含まます）では、鍵交換などを行うため様々な通信が発生します。そのため、SSLの通信が多くなるとサーバに負荷がかかり、サーバ遅延の原因になることもあります。そこで、SSL専用のハードウェアであるSSLアクセラレータを使ってSSLのサーバ負荷の軽減を図ることがあります。

■ DLP

機密情報を外部へ漏えいさせないための包括的な対策のことを**DLP**（Data Loss Prevention）といいます。機密情報と機密でない情報を自動的に区別し、機密情報だけを外部に漏えいさせ



SSLについては、「3-4-1 セキュアプロトコル」で改めて取り上げます。プロトコルの内容はこちらでご確認ください。

ないようにします。

DLPは、PCなどに入れるDLPエージェントと、集中管理を行うDLPサーバ、及びネットワーク上を流れるデータを監視するDLPアプライアンスの3種類の要素で構成されます。

■ SIEM

SIEM (Security Information and Event Management)とは、サーバやネットワーク機器などからログを集め、そのログ情報を分析し、異常があれば管理者に通知する、または対策方法を知らせる仕組みです。セキュリティインシデントにつながるおそれのあるものをリアルタイムで監視し、管理者が素早く検知、対応することを助けます。

■ MDM

個人のスマートデバイスを仕事で利用する**BYOD** (Bring Your Own Device)を導入するケースが増えてきています。この場合には、会社貸与のスマートデバイスよりも複雑な管理が必要となります。**MDM** (Mobile Device Management: モバイル端末管理)を適切に行い、全体的に管理することが大切です。

MDMでの管理は手動で行うこともありますが、MDMツールを用いて統合的に管理することも可能です。MDMツールには、端末の紛失・盗難時に操作をロックするリモートロック機能や、出荷時の状態に戻すリモートワイプ機能があります。

■ WORM

WORM (Write Once Read Many)は、書き込みが1回しかできない記憶媒体のことです。読み込みは何度でもできます。ログなど、改ざんされると困るデータの書き込みに利用されます。

▶▶ 覚えよう！

- ☐ **SIEM**はログ情報に基づいて、インシデントの予兆を発見して通知
- ☐ **MDM**はモバイルデバイスを統合的に管理

3-2-5 演習問題

問1 攻撃を遮断するためのもの

CHECK ▶ ☐☐☐

クライアントとWebサーバの間において、クライアントから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 |

問2 IDS

CHECK ▶ ☐☐☐

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^{ぜい}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3 可用性を高めるための管理策

CHECK ▶ ☐☐☐

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4 機器の紛失による情報漏えい対策**CHECK** ▶ ☐☐☐

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。

3

問5 マルウェア対策**CHECK** ▶ ☐☐☐

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6 ビヘイビア法**CHECK** ▶ ☐☐☐

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7 ファイアウォールで許可するプロトコル

CHECK ▶ ☐☐☐

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8 ハッシュ値を利用する目的

CHECK ▶ ☐☐☐

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。

問9 情報漏えいのリスク低減策

CHECK ▶ ☐☐☐

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10 SIEM

CHECK ▶ ☐☐☐

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パケットを検知し、通知する。

問11 スマートフォンのセキュリティ

CHECK ▶ ☐☐☐

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)

問12 BYOD

CHECK ▶ ☐☐☐

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。

■ 解答と解説

問1

(平成28年春 情報セキュリティマネジメント試験 午前 問13)

《解答》イ

Webサーバに送信されたHTTP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ファイアウォールをWAF(Web Application Firewall)といいます。したがって、イが正解です。

- ア SSL (Secure Sockets Layer) /TLS (Transport Layer Security) を使って通信を暗号化し、VPN (Virtual Private Network) を構築する機能です。
- ウ 複数のコンピュータを結合し、ひとまとまりのシステムにする機能です。
- エ 複数台のサーバを並列に稼働させて、負荷分散させる機能です。

問2

(平成28年春 情報セキュリティマネジメント試験 午前 問12)

《解答》ウ

IDS (Intrusion Detection System : 侵入検知システム) とは、サーバやネットワーク上で不正侵入を検知するシステムです。セキュリティポリシを侵害するような挙動を管理者へ通知するので、ウが正解です。

- ア JVN (Japan Vulnerability Notes) が提供する「MyJVN バージョンチェッカ」などが該当します。
- イ ファジングの説明です。
- エ 情報セキュリティ対策ベンチマークの説明です。

問3

(平成28年秋 情報セキュリティマネジメント試験 午前 問5)

《解答》ア

“可用性”とは、「認可されたエンティティが要求したときにアクセス及び使用が可能である特性」です。つまり、アクセスを可能とするために障害を起こりにくくする必要があります。ストレージを二重化することは、耐障害性を向上させ、可用性を高めるので、アが正解です。イは真正性、ウ、エは機密性を高めるための管理策です。

問4

(平成28年春 情報セキュリティマネジメント試験 午前 問4)

《解答》イ

モバイル機器を紛失したときに情報漏えいを防止するためには、モバイル機器内の情報をリモートから消去できる機能(リモートワイプ機能)をもったツールが有効です。したがって、イが正解となります。

アはSNS経由での情報漏えい、ウはモバイル通信時の情報漏えい、エはショルダハッキングなどによる情報漏えいへの対策として有効です。

問5

(平成28年春 情報セキュリティマネジメント試験 午前 問14)

《解答》イ

PCにおけるマルウェア対策では、ウイルス対策ソフトの導入だけでなく、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ことも大切です。したがって、イが正解です。

ア 定義ファイルが新しいと、以前の定義ファイルでは検出できなかったウイルスが検出される可能性があります。そのため、すべてのファイルをスキャンの対象とします。

ウ、エ このようなウイルス感染対策として、ポートの遮断や動的グローバルIPアドレスの付与などは意味がありません。

問6

(平成28年秋 情報セキュリティマネジメント試験 午前 問18)

《解答》エ

ビヘイビア法とは、ビヘイビア(ふるまい)を監視するための手法です。安全な仮想環境下などで実行し、その挙動を確認することで、ウイルスかどうかを判定します。したがって、エが正解です。

アはチェックサム法、イはコンペア法、ウはパターンマッチングに分類されます。

問7

(平成28年秋 情報セキュリティマネジメント試験 午前 問19)

《解答》イ

時刻サーバが使用している、時刻を同期させるプロトコルをNTP (Network Time Protocol) といいます。インターネット上の時刻サーバと社内サーバを同期させるためには、NTPをファイアウォールで許可して通過させる必要があります。NTPはトランスポート層のプロトコルとしてUDP (User Datagram Protocol) を用い、ポート番号123で通信するので、イが正解です。

アはファイル転送、ウはメール送信、エはネットワーク管理のための通信プロトコルです。

問8

(平成28年春 情報セキュリティマネジメント試験 午前 問16)

《解答》ウ

デジタルフォレンジックスでは、法的な証拠性を確保するため、ログなどのハッシュ値を取得します。改ざんを検出し、原本と複製の同一性を証明することができるので、ウが正解です。

ア パスワードをハッシュ化してファイルに保存するときのハッシュ値の利用目的です。

イ ハッシュ値から元のデータは復元できません。

エ 盗聴の有無は、ハッシュ値では判別できません。

問9

(平成28年春 情報セキュリティマネジメント試験 午前 問20)

《解答》ウ

HDD (Hard Disk Drive : ハードディスクドライブ) は、補助記憶装置の一種です。HDD自体を暗号化するためには、HDDパスワードを設定して暗号化し、HDDだけを抜き取られても情報を読めないようにしておく必要があります。したがって、ウが正解です。

ア、イ、エでは、HDDを抜き取られたときに情報漏えいのリスクがあります。

問10

(平成28年秋 情報セキュリティマネジメント試験 午前 問15)

《解答》イ

SIEMとは、サーバやネットワーク機器などからログを集め、そのログ情報を分析し、異常があれば管理者に通知する、または対策方法を知らせる仕組みです。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するので、イが正解です。

ア DLP (Data Loss Prevention) の機能です。

ウ CMDB (Configuration Management Database : 構成管理データベース) の機能です。

エ IDS (Intrusion Detection System : 侵入検知システム) の機能です。

問11

(平成28年秋 情報セキュリティマネジメント試験 午前 問13)

《解答》エ

会社や団体がスマートフォンに対して一元管理する仕組みのことをMDM (モバイル端末管理) といいます。したがって、エが正解です。

ア 個人所有のスマートフォンを業務で使用する取組みです。

イ 組織内の業務ドキュメントや文書の蓄積、管理、運用を統括的、包括的に行うための技術やシステムのことです。

ウ 携帯電話の通信規格の一つです。

問12

(平成28年春 情報セキュリティマネジメント試験 午前 問11)

《解答》エ

BYOD (Bring Your Own Device) とは、従業員が私物の情報端末を持ち込んで業務に利用することです。セキュリティ設定の不備による情報セキュリティリスクは増大するので、エが正解です。

ア、イは情報端末の持ち出しによるリスク、ウは情報端末の持ち込みによるリスクがあり、情報セキュリティリスクは増大しますが、BYODとは関係ありません。

3-3 物理的セキュリティ対策

物理的セキュリティでは、防犯対策や入退室管理などによって、情報資産を物理的に守ります。

3-3-1 物理的セキュリティ対策

物理的セキュリティとは、鍵をかける、データを遠隔地に運ぶなど、環境を物理的に変えることです。クリアデスクやクリアスクリーンといった対策があります。

RASIS

システムの信頼性を総合的に評価する基準として、RASISという概念があります。次の五つの評価項目を基に、信頼性を判断します。

① Reliability (信頼性)

故障や障害の発生しにくさ、安定性を表します。具体的な指標としては、MTBFやその逆数の故障率があります。

② Availability (可用性)

稼働している割合の多さ、稼働率を表します。具体的な指標としては、稼働率が用いられます。

③ Serviceability (保守性)

障害時のメンテナンスのしやすさ、復旧の速さを表します。具体的な指標としては、MTTRが用いられます。

④ Integrity (保全性・完全性)

障害時や過負荷時におけるデータの書換えや不整合、消失の起こりにくさを表します。一貫性を確保する能力です。

⑤ Security (機密性)

情報漏えいや不正侵入などの起こりにくさを表します。セキュ



勉強のコツ

物理的セキュリティ対策では、いわゆる“情報セキュリティ対策”とは思えないようなこともいろいろ考慮する必要があります。建物の設備やシステムの信頼性など、関連する周辺分野の知識もしっかり学習していきましょう。



関連

MTBF, MTTRについては、「6-3-2 システムの評価指標」で解説しています。詳しくはこちらをご覧ください。

リティ事故を防止する能力です。

RASISを意識してシステムの信頼性を上げることは、情報セキュリティの3要素である機密性、完全性、可用性を向上させることにつながります。

■ RAS技術

RASISのうち、信頼性、可用性、保守性を向上するための技術を**RAS技術**といいます。高信頼性を総合的に確保するためのもので、部品を故障しにくくすることで信頼性を上げ、万一の故障に備えて自動回復を行うことで保守性を上げ、自動回復に失敗した場合は故障場所を切り離すことで可用性を上げるなど、複数の技術を組み合わせて実現します。

■ 耐震耐火設備

データセンタなど、災害時にもシステムを停止させないような高信頼性が求められる施設では、耐震耐火設備をしっかりと設置する必要があります。建物には消化ガスによる消火設備を備え、重要機器には免震装置を取り付けるなど、災害対策を十分に施すことが大切です。



デュプレックスシステムなどの二重化技術の詳細は、「6.3.1 システムの構成」で詳しく学習します。

■ 二重化技術

一つの機器が故障しても、それが全体のシステム停止につながらないようにするために、二重化技術が重要になります。データを複製して二重化する**ミラーリング**や、バックアップ用のシステムを用意しておいて障害時に稼働する**デュプレックスシステム**など、様々な二重化技術を活用し、求められる可用性に対応できるようにすることが大切です。

■ 監視カメラ

設備の入口やサーバールームなどに監視カメラを設置し、映像を記録することによって、不正行為の証拠を確保することができます。また、監視カメラの設置を知らせることは、不正行為の抑止効果にもなります。

■ 施錠管理

重要な設備や書類が置いてある部屋を施錠することによって、情報へのアクセスを難しくすることができます。施錠した鍵の管理も厳密に行う必要があります。

■ 入退室管理

扱う情報のレベルに応じて、情報セキュリティ区域(安全区域)など、情報を守るための区域を特定します。その区域には認可された人だけが入室できるようなルールを設定し、そのための入退室管理を行います。

ICカードによる入退室では、機械的にログを取得し、入退室管理を行うことができます。それだけでなく、訪問者の入退室の日時・記録などを保管し、ログと照合することによって、より厳密な入退室管理が可能になります。

また、直前の入退室を行う人の後ろについて認証をすり抜ける**ピギーバック**が行われると、ログに残らなくなってしまいます。そのため、ルールで禁止し教育して伝える、対応する入室のない退室を検出してエラーとするなどの対策が必要です。

■ 遠隔地バックアップ

地震などの災害に備えて、バックアップしたデータは遠隔地に保管しておく必要があります。バックアップテープを**セキュリティ便**などの安全な輸送手段で遠隔地に運び、それを保管しておくことが有効です。また、遠隔地とネットワークで接続されており、十分な通信速度が確保できる場合には、ネットワーク経由での遠隔地バックアップも可能です。

■ クリアデスクとクリアスクリーン

盗難を防止するため、自席の机に置かれているノートPCなどを帰宅時にロッカーなどに保管して施錠する**クリアデスク**という対策があります。また、食事などで自席を離れるときに他の人がPCにアクセスできないようにスクリーンにロックなどをかける対策を**クリアスクリーン**といいます。

■ USBキー

USBキーを利用してPCにロックをかけることが可能です。USBキーを接続しているときにだけPCを利用できるようにすることで、PCを他人に操作される可能性を減らします。USBキーにPIN（暗証番号）を加えることも可能です。

■ 廃棄

PCなどを廃棄する場合には、その廃棄する機器から情報漏えいなどが起こらないようにすることが大切です。そのため、廃棄するハードディスクなどのメディアは物理的に破壊する、意味のないデータを上書きして元のデータを消すなどの対策が有効です。

▶▶ 覚えよう！

- ☐ RAS技術で、信頼性、可用性、保守性を上げる
- ☐ クリアデスクはPCをロッカーに保管、クリアスクリーンはスクリーンロック

3-3-2 演習問題

問1 クリアデスク

CHECK ▶ ☐☐☐

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2 廃棄する場合の情報漏えい対策

CHECK ▶ ☐☐☐

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3 機密ファイルの不正な持出し対策

CHECK ▶ ☐☐☐

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^{けん}を牽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

■ 解答と解説**問1**

(平成28年春 情報セキュリティマネジメント試験 午前 問2)

《解答》ウ

クリアデスクとは、情報セキュリティ対策での行動指針の一つで、自席の机の上に情報資産を放置しないことです。夜間などは施錠できる安全な場所に保管することが推奨されています。したがって、ウが正解です。

アはフォルダ管理、イはクリアスクリーン、エはセキュリティワイヤの説明です。

問2

(平成28年春 情報セキュリティマネジメント試験 午前 問17)

《解答》ウ

磁気ディスクを廃棄する場合には、ディスク内の情報を完全に消去する必要があります。そのためには、ランダムなビット列で、磁気ディスクの全領域を上書きすることで、ディスク内のデータの痕跡をなくし、完全に読めないようにすることが可能です。したがって、ウが正解です。

アの圧縮や、イのマスタブートレコードの消去、エのファイル名の変更などは、ディスクにデータが残るので、機密ファイルが読み取られる可能性があります。

問3

(平成26年秋 応用情報技術者試験 午前 問44)

《解答》ウ

システム管理者による機密ファイルの不正な持出しを牽制するためには、監視者を配置するなどして、システム管理者の行動を抑止することが有効です。したがって、ウが正解となります。

ア、イは不正アクセスやウイルス感染などへの対策です。エに関しては、バックアップを持ち出す可能性もあり、不正な持出しを助長するリスクがあります。

3-4 セキュリティ実装技術

3

セキュリティ実装技術には、ネットワーク関連、データベース関連、アプリケーション関連など、様々な種類のものがあります。技術を組み合わせて何層にも守ることが大切です。

3-4-1 セキュアプロトコル

セキュアプロトコルは、セキュリティを守るためのプロトコルです。TLS/SSLやIPsecを中心に、インターネットでは広く用いられています。

IPsec

IPパケット単位でデータの改ざん防止や秘匿機能を提供するプロトコルが**IPsec** (Security Architecture for Internet Protocol) です。

IPsecで使用されるプロトコルには、**AH** (Authentication Header), **ESP** (Encapsulated Security Payload), **IKE** (Internet Key Exchange protocol) などがあります。AHでは完全性確保と認証を、ESPではAHの機能に加えて暗号化をサポートします。また、IKEにより、共通鍵の鍵交換を行います。

TLS/SSL

SSL (Secure Sockets Layer) は、セキュリティを要求される通信のためのプロトコルです。SSL3.0を基に、**TLS** (Transport Layer Security) 1.0が考案されました。

提供する機能は、**認証**、**暗号化**、**改ざん検出**の三つです。最初に、通信相手を確認するために認証を行います。このとき、サーバがサーバ証明書をクライアントに送り、クライアントがその正当性を確認します。クライアントがクライアント証明書を送ってサーバが確認することもあります。

さらに、サーバ証明書の公開鍵を用いて、クライアントはデータの暗号化に使う共通鍵の種を、サーバの公開鍵で暗号化して送ります。その種を基にクライアントとサーバで共通鍵を生成し、



SSLが発展してTLSになっており、正確なバージョンとしては、SSL1.0、SSL2.0、SSL3.0、TLS1.0、TLS1.1、TLS1.2というかたちで順に進化しています。現在のブラウザなどではTLSが使われていることが多いのですが、SSLという名称が広く普及したので、あまり区別せず、TLSをSSLと呼ぶこともあります。

その共通鍵を用いて暗号化通信を行います。また、データレコードにハッシュ値を付加して送り、データの改ざんを検出します。

TLS/SSLは、次のように様々なプロトコルと組み合わせて使うことが可能です。

- **HTTPS (HTTP over TLS/SSL)**

Webページで使用するHTTP (HyperText Transfer Protocol) との組合せ

- **SMTPS (SMTP over TLS/SSL)**

電子メールの送信で使用するSMTP (Simple Mail Transfer Protocol) との組合せ

- **FTPS (FTP over TLS/SSL)**

ファイル転送で使用するFTP (File Transfer Protocol) との組合せ

■ S/MIME

S/MIME (Secure Multipurpose Internet Mail Extension) は、電子メールの**暗号化**と**デジタル署名**に関する標準規格です。認証局(CA)で正当性が確認できた公開鍵を用います。まず共通鍵を生成し、その共通鍵でメール本文を暗号化します。そして、その共通鍵を受信者の公開鍵で暗号化し、メールに添付します。このような暗号化方式のことを**ハイブリッド暗号**といいます。組み合わせることで、共通鍵で高速に暗号化でき、公開鍵で安全に鍵を配送できるようになります。また、デジタル署名を添付することで、データの真正性と完全性も確認できます。



SSHを利用したプログラムには、リモートホストでのファイルコピー用コマンドのrcpを暗号化するscpや、FTPを暗号化するsftpなどがあります。

■ SSH

SSH (Secure Shell) は、ネットワークを通じて別のコンピュータにログインしたり、ファイルを移動させたりするためのプロトコルです。公開鍵暗号方式によって共通鍵の交換を行うハイブリッド暗号を使用します。

▶▶ 覚えよう！

- ☐ TLS/SSLでは公開鍵で認証、共通鍵で暗号化、ハッシュで改ざん検出
- ☐ S/MIMEでは、共通鍵を公開鍵暗号方式で暗号化

3-4-2 ネットワークセキュリティ

ネットワークセキュリティでは、ファイアウォールやIDSなどの機器を使って、ネットワーク全体を監視します。機器を組み合わせ、全体的に守ることが大切です。

■ パケットフィルタリング

ファイアウォールやルータなどでは、ネットワーク上を通過する一つ一つのパケットについて、通すか通さないかの判断を行います。その仕組みのことをパケットフィルタリングといい、ネットワーク上でセキュリティを守るときの基本となります。

■ MACアドレスフィルタリング

MACアドレス(Media Access Control address)とは、同じLAN上でコンピュータを識別するためのアドレスです。特定のMACアドレスのみを通過させる仕組みをMACアドレスフィルタリングといい、無線LANのアクセスポイントなどで用いられています。

■ RADIUS

RADIUS(Remote Authentication Dial In User Service)は、認証と利用事実の記録を一つのサーバで一元管理する仕組みです。IEEE 802.1Xでの活用など、様々な場面で利用されています。

RADIUSはクライアントとサーバで動作します。RADIUSクライアントが認証情報をRADIUSサーバに送り、RADIUSサーバが認証の可否を決定して返答します。このとき、認証情報によって、どのサービスに接続可能かを合わせて確認します。

■ IEEE 802.1X

IEEE 802.1Xは、LAN接続で利用される認証規格です。無線LAN、有線LANにかかわらずポートごとに認証を行い、認証に成功した端末だけがLANに接続できます。IEEE 802.1Xで認証に使われるプロトコルは、EAP(Extensible Authentication Protocol: 拡張認証プロトコル)です。

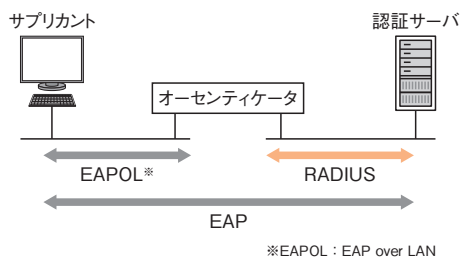
IEEE 802.1Xによる認証は、次のように構成されます。



関連

ファイアウォールやIDSについては、「3-2-1 不正アクセス対策」で説明しています。

また、VLANやMACアドレスなど、LAN関連のプロトコルについては、「6-1-2 データ通信と制御」で取り上げていますので、こちらに合わせて参考してみてください。



IEEE 802.1Xによる認証の構成

サブリカントは、IEEE 802.1Xでアクセスするコンピュータに含まれるソフトウェアです。オーセンティケーターとの間で認証情報をやり取りします。

オーセンティケーターは、無線LANアクセスポイントや認証スイッチなど、IEEE 802.1Xの機能を実装したネットワーク機器です。サブリカントから受け取った認証情報を基に、認証の可否を認証サーバに問い合わせます。

認証サーバは、認証情報を保存しているサーバです。オーセンティケーターからの問合せに対して認証情報を検証し、認証の可否を返答します。認証に成功したら、オーセンティケーターはスイッチのポート利用を許可します。

オーセンティケーターと認証サーバとの間でのやり取りには、RADIUSが使用されます。オーセンティケーターがRADIUSクライアントになり、RADIUSサーバである認証サーバに問合せを行います。

■ VLAN

VLAN (Virtual LAN) は、LANにおいて仮想的なネットワークを構築する技術です。例えば、物理的に同じスイッチに接続している機器を論理的に二つのネットワークに分割することができます。

VLANと、IEEE 802.1Xなどの認証の仕組みを組み合わせることで、**認証VLAN**を構築することができます。認証に成功したコンピュータのみを業務用のネットワークに接続させるなど、ネットワークを柔軟に変更することができます。物理的な接続を変えずにすむので、**検疫ネットワーク**などで用いられます。

■ セキュリティ監視

ネットワーク上でのセキュリティ監視には、**NIDS**（ネットワーク型侵入検知システム）などが用いられます。ファイアウォールなどでの一つ一つの packets だけでなく、総合的にネットワークを監視することで、DoS 攻撃など、様々な攻撃の予兆に気づくことができます。

■ プロキシサーバ

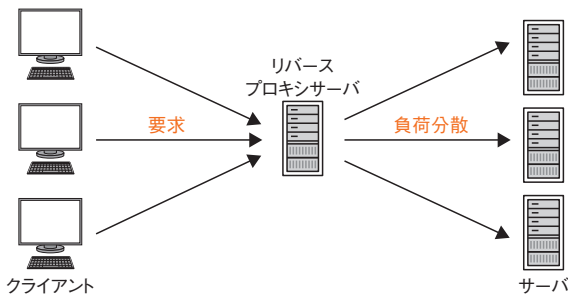
プロキシサーバとは、クライアント（PC など）の代わりにサーバに情報を中継するサーバです。複数の PC などから Web サーバなどへのアクセス要求を受け取り、それを中継して Web サーバなどに送ります。

プロキシサーバでは、Web サーバに一度問い合わせた情報を**キャッシュ**しておき、PC から同じ URL への要求があったときにそれを返答します。そのため、高速なアクセスが可能となります。

■ リバースプロキシ

プロキシサーバとは逆に、Web サーバなどの代替りのサーバ（**リバースプロキシサーバ**）が、クライアント（PC など）からサーバへのアクセス要求を代理で集中して受け付け、サーバに中継することを**リバースプロキシ**といいます。

リバースプロキシを利用することで、複数のサーバへ負荷を分散させることや、キャッシュによって負荷を低減させることが可能となります。



リバースプロキシサーバ

■ ハニーポット

ハニーポットは一種のおとり戦法で、不正アクセスを受けるために存在するシステムです。何か有益そうな場所を用意しておき、それにつられてやってきた者を観察し、不正アクセスのやり方を学習します。マルウェアなどを入手したり、不正アクセスの動向を調査したりするのに利用します。

▶▶ 覚えよう！

- ☐ サブリカントはPC、オーセンティケータはネットワーク機器
- ☐ リバースプロキシでは、サーバの代理で受け付けたアクセスを各サーバに分散させる

3-4-3 ■ データベースセキュリティ

データベースがもつセキュリティ機能を使うだけではデータを守り切れないことがあります。データベースセキュリティでは、他のセキュリティプロトコルや暗号化と組み合わせた対策が必要です。

■ データベース暗号化

データベースに格納されるデータ自体を暗号化します。これにより、DBMS (DataBase Management System: データベース管理システム) が格納されているストレージなどが盗難された場合でもデータを保護できます。

しかし、プログラムからアクセスされた場合には復号されるので、解読可能になります。SQL インジェクションなど、アプリケーションを中継した攻撃には対応できないので、注意が必要です。

■ データベースアクセス制御

DBMS へのログイン用のアカウントによって利用者認証を行います。ログイン用のアカウントには、ユーザだけでなくロール(役割)を設定し、ロールごとにアクセスを制御することが可能です。



関連

バックアップやロールフォワードについては、「6-2-4 トランザクション処理」で取り上げています。データベース関連の用語についてはこちらを参考にしてください。

■ データベースバックアップ

データの消失を防ぐためにも、データベースのバックアップは定期的に行う必要があります。しかし、バックアップから情報が漏えいする可能性もあるので、バックアップメディア(テープなど)は、施錠した部屋などで安全に保管します。

バックアップ復元後には、データベースの更新後ログなどを使用してロールフォワードを行うことで、最新に近い状態にまでデータを復元できます。

■ アクセスログの取得

Webサーバ上のプログラムからアクセスされる場合などには、複数のユーザが同じDBMSアカウントを使うので、利用者の記録が残らないことがあります。

DBMSのアクセスログにDBMSのアカウント情報が残ります

が、通常、WebアプリケーションではDBMSアカウントは共通なので、利用者を識別できません。そこで、Webサーバ側でアクセス制御を行います。ログに利用者情報を残すためには、Webサーバ側から利用者IDなどの情報を送ってもらう必要があります。

覚えてよう！

- ☐ データベースのデータは、暗号化することが可能
- ☐ バックアップは安全な場所に保管する

3-4-4 ■ アプリケーションセキュリティ

アプリケーションセキュリティは、アプリケーションに対する攻撃の種類に応じて個別に行う必要があります。そのために、主な攻撃とその対策を押さえておくことが重要です。

■ Webシステムのセキュリティ対策

Webアプリケーションの作成の仕方によって、Webシステムに脆弱性が生じてしまうことがあります。Webアプリケーション専用のファイアウォールであるWAFだけではすべての脆弱性に対応することが難しいので、それぞれのアプリケーションで脆弱性を作り込まないように工夫することが大切です。

■ セキュアプログラミング

アプリケーションに対しては、システム開発時に脆弱性を作り込まないようにするセキュアプログラミングが重要になります。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、多くのセキュリティ攻撃は、セキュアプログラミングをしっかりと行うことで避けられます。例えば、以下のようなことに気をつけてプログラムを組む必要があります。

- 入力値の内容チェックを行う
- SQL文の組み立ては、すべてバインド機構を利用する
- エラーをそのままブラウザに表示しない



関連

それぞれの攻撃については、「1-2-1 サイバー攻撃手法」で説明しています。

■ バッファオーバーフロー対策

バッファオーバーフロー (BOF) 対策としては、入力文字列長をチェックし、長い文字列の入力を受け付けないようにする対策が基本です。また、**カナリアコード**といって、メモリにあらかじめチェックデータを書き込んでおき、それが上書きされたときに通知する手法もあります。

■ クロスサイトスクリプティング対策

クロスサイトスクリプティング (XSS) 対策の基本は、スクリプトの実行を妨げることです。そのためには、スクリプトを検知し

てエスケープ処理(無効化)を行う方法があります。

また、他のWebサイトのプログラムを、アクセス権などの設定によって実行不可にする対策なども有効です。

■ SQLインジェクション対策

SQLインジェクションの場合には、**バインド機構**を利用し、制御文字を挿入できないようにする対策が有効です。しかし、すべてのSQL実行時にSQLインジェクション対策を行う必要があるため、セキュアプログラミングは漏れがないように行うことが重要です。

また、データベースにデータを挿入するときに制御文字の入ったデータを送り込む攻撃があります。この攻撃に対処するためには、すでにデータベースに読み込まれているデータに対してもバインド機構を利用し、制御文字を挿入できないようにする必要があります。

▶▶ 覚えよう！

- ☐ 脆弱性を作り込まないために、セキュアプログラミングが大切
- ☐ Webアプリケーション対策は、漏れがないように行うことが重要

3-4-5 演習問題

問1 電子メールのファイル添付方法

CHECK ▶ ☐☐☐

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。

問2 SSH

CHECK ▶ ☐☐☐

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3 無線LANセキュリティ

CHECK ▶ ☐☐☐

無線LANのセキュリティにおいて、アクセスポイントが接続要求を受け取ったときに、端末固有の情報を基にアクセス制御を行う仕組みはどれか。

- | | |
|---------|------------------|
| ア ESSID | イ MACアドレスフィルタリング |
| ウ WEP | エ WPA |

問4 LAN接続許可

CHECK ▶ ☐☐☐

レイヤ2スイッチや無線LANアクセスポイントで接続を許可する仕組みはどれか。

- | | |
|----------|-----------------|
| ア DHCP | イ Webシングルサインオン |
| ウ 認証VLAN | エ パーソナルファイアウォール |

問5 SPF

CHECK ▶ ☐☐☐

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6 SQLインジェクション攻撃

CHECK ▶ ☐☐☐

SQLインジェクション攻撃を防ぐ方法はどれか。

- ア 入力中の文字が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として解釈されないようにする。
- イ 入力にHTMLタグが含まれていたら、HTMLタグとして解釈されない他の文字列に置き換える。
- ウ 入力に、上位ディレクトリを指定する文字列(../)を含むときは受け付けない。
- エ 入力の全体の長さが制限を超えているときは受け付けない。

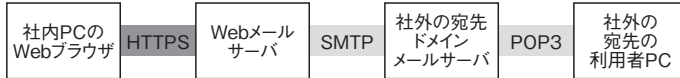
■ 解答と解説

問1

(平成28年秋 情報セキュリティマネジメント試験 午前 問17)

《解答》イ

設問の「電子メール環境」をまとめると、次の図のようにメールが送信されます。



このうち暗号化されているのは、HTTPS (HTTP over TLS) の部分だけで、SMTPとPOP3では平文でデータが送られます。そのため、秘密情報を含むファイルは暗号化してメールに添付する必要があります。したがって、イが正解です。

ア、ウ Webメールサーバ以降は暗号化されていないので、暗号化する必要があります。
エ Base64形式は、誰でもデコード(復元)できるので盗聴が可能です。

問2

(平成26年春 応用情報技術者試験 午前 問44)

《解答》エ

SSH (Secure Shell) は、リモートログインなどを行うプロトコルの TELNET などのセキュリティを強化したプロトコルです。リモートファイルコピー (RCP) などでも使用できます。データを暗号化して送信するので、通信経路での盗聴を防ぐことが可能です。したがって、エが正解です。

アはS/MIME、イはSET (Secure Electronic Transaction)、ウは暗号化メールソフトの説明です。

問3

(平成25年秋 ITパスポート試験 午前 問81)

《解答》イ

無線LANアクセスポイントが端末固有の情報を基に行うアクセス制御は、MACアドレスフィルタリングです。アクセスを許可する端末のMACアドレスをアクセスポイントに登録し、登録したMACアドレスからの通信以外を拒否します。したがって、イが正解です。

ア ESSID (Extended Service Set Identifier) は、無線LANアクセスポイントを識別する識別子です。

ウ WEP (Wired Equivalent Privacy: 有線同等機密) は暗号方式の一つです。脆弱性があり、現在では使用は推奨されていません。

- エ WPA (Wi-Fi Protected Access) は、WEPの脆弱性対策として策定された認証プログラムです。AES暗号をベースとした強固な暗号化を行います。

問4

(平成21年秋 情報セキュリティスペシャリスト試験 午前Ⅱ 問13)

《解答》ウ

レイヤ2スイッチや無線LANアクセスポイントなど、LANで接続を許可する仕組みのことを認証VLANといいます。したがって、ウが正解です。

ア DHCP (Dynamic Host Configuration Protocol) は、IPアドレスを自動的に割り当てる仕組みです。

イ Webシングルサインオンは、一度認証が成功したら複数のWebサーバにアクセスできる仕組みです。

エ パーソナルファイアウォールは、PCなどのコンピュータ1台1台に導入するファイアウォールです。

問5

(平成28年秋 情報セキュリティマネジメント試験 午前 問16)

《解答》エ

SPFは、送信ドメインを認証するための技術です。該当ドメインに対するメールサーバのIPアドレスをDNSサーバに登録しておき、受信したメールサーバがそのIPアドレスを検証することで、送信元のメールサーバが正規のサーバであることを確認します。メール送信のなりすましを検知することができるので、エが正解です。

アはHTTPS通信の利用、イはパーソナルファイアウォールの導入、ウはIDSなどの導入によって対処できます。

問6

(平成25年春 基本情報技術者試験 午前 問40)

《解答》ア

SQLインジェクションの対策としては、制御文字を通常の文字に置き換えるエスケープ処理やバインド機構を利用する方法があります。したがって、アが正解です。

イ クロスサイトスクリプティングやクロスサイトリクエストフォージェリなどの対策です。

ウ ディレクトリトラバーサル対策です。

エ バッファオーバーフロー対策です。

第4章

法務

情報セキュリティマネジメントを推進するにあたって、法律や標準などとの整合性を確認することはとても大切です。

この章では、情報セキュリティ関連法規と、その他の法規・標準について学んでいきます。

情報セキュリティ関連法規では、サイバーセキュリティ基本法や不正アクセス禁止法など、情報セキュリティに直接関係する法規について学習します。その他の法規・標準では、知的財産権や労働関連法規など、情報セキュリティと関係が深い法規や標準について学習していきます。

4-1 情報セキュリティ関連法規

- ◆ 4-1-1 サイバーセキュリティ基本法
- ◆ 4-1-2 不正アクセス禁止法
- ◆ 4-1-3 個人情報保護法
- ◆ 4-1-4 刑法
- ◆ 4-1-5 その他のセキュリティ関連法規・基準
- ◆ 4-1-6 演習問題

4-2 その他の法規・標準

- ◆ 4-2-1 知的財産権
- ◆ 4-2-2 労働関連・取引関連法規
- ◆ 4-2-3 その他の法律・ガイドライン・技術者倫理
- ◆ 4-2-4 標準化関連
- ◆ 4-2-5 演習問題

4-1 情報セキュリティ関連法規

情報セキュリティ関連法規には、不正アクセス禁止法や個人情報保護法をはじめ様々なものがあり、さらに新しい法規が追加され続けています。



勉強のコツ

情報セキュリティ関連の法規は、毎年のように新しいものが追加されています。今のようなものがあるのか、どのような法規が追加、変更されたのかをしっかりと押さえておきましょう。



発展

サイバーセキュリティ基本法は、2016年4月に改正法が参議院本会議で可決・成立しました。改正法では、国が行う不正な通信の監視、監査、原因究明調査等の対象範囲を拡大し、日本年金機構などの特殊法人・認可法人も対象としています。また、サイバーセキュリティ戦略本部の一部事務をIPAに委託することも定められています。

4-1-1 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では、国のサイバーセキュリティ対策の司令塔として、内閣にサイバーセキュリティ戦略本部を設置することが定められています。

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2014年に制定された法律で、国のサイバーセキュリティに関する施策を推進するにあたっての基本理念や国の責務などを定めたものです。

サイバーセキュリティとは何かを明らかにし、必要な施策を講じるための基本理念や基本的施策を定義しています。また、その司令塔として、内閣に**サイバーセキュリティ戦略本部**を設置することが定められています。国民には、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めることが求められています。

サイバーセキュリティとは

サイバーセキュリティ基本法の第二条では、サイバーセキュリティを次のように定義しています。

「電磁的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」

つまり、サイバー攻撃に対する防御行為全般をサイバーセキュリティといいます。

■ サイバーセキュリティ戦略本部

内閣サイバーセキュリティセンター（NISC：National center of Incident readiness and Strategy for Cybersecurity）内に設置された**サイバーセキュリティ戦略本部**は、国のサイバーセキュリティ対策の司令塔です。IT 総合戦略本部や国家安全保障会議などと連携して、国全体の安全を保障するための活動を行います。地方公共団体や各省庁への勧告なども行います。

▶▶ 覚えよう！

- ☐ サイバーセキュリティ基本法は、国がサイバー攻撃に対して司令塔となるための法律
- ☐ サイバーセキュリティ戦略本部が、国の司令塔としてサイバーセキュリティ対策を行う

4-1-2 ■ 不正アクセス禁止法

不正アクセス禁止法は、不正アクセスを規制する法律です。実際の被害を与えなくても、不正なアクセスを行うだけで犯罪となります。

■ 不正アクセス禁止法

不正アクセス行為の禁止等に関する法律(不正アクセス禁止法)は、インターネットなどでの不正アクセスを規制する法律です。ネットワークへの侵入、アクセス制御のための情報提供などを処罰の対象としています。

不正アクセス禁止法では、被害がなくても不正アクセスをしただけ、またはそれを助けただけの助長行為も処罰の対象になります。さらに、不正アクセスを行わなくても、その目的で利用者IDやパスワードの情報を集めただけで、不正に保管する行為として処罰の対象となります。

■ アクセス制御機能

不正アクセス禁止法では、第一条に「アクセス制御機能により実現される電気通信に関する秩序の維持」とあり、アクセス制御機能を用いて利用者のアクセスを制限することが推奨されています。不正アクセス禁止法の処罰の対象となるのは、アクセス制御を超えて権限のないコンピュータ資源にアクセスすることです。

■ 不正アクセス行為

不正アクセス行為は、アクセス権限のないコンピュータ資源にアクセスすることですが、具体的には次のようなことが想定されています。

- 他人のIDやパスワードを盗用または不正使用し、その人になりすまして認証を行うこと
- 認証サーバの脆弱性(セキュリティホール)などを突いた攻撃で、認証を行わずにコンピュータ資源にアクセスできるようになること

- 目標の端末にアクセスするため、その端末のネットワークのゲートウェイの認証を不正に突破し、目標の端末にアクセスすること

不正アクセス行為を助長する行為

実際の不正アクセス行為だけでなく、不正アクセスを助長する行為も処罰の対象となります。具体的には、IDやパスワードなどの認証情報を、端末利用者や管理者以外の人に漏らすなどの行為が助長行為とされています。ただし、情報セキュリティ教育を行う、注意喚起するなど正当な理由がある場合には、処罰の対象とはなりません。

覚えよう！

- ☐ 不正アクセスは、アクセス制御機能を超えて行うアクセス
- ☐ 不正アクセスは、自分でやらず助長しただけでも犯罪

4-1-3 個人情報保護法

個人情報保護法は、個人情報を守るための法律です。個人情報保護マネジメントの考え方にに基づき、目的外利用の禁止や、個人情報保護マネジメントシステムの運用などについて定められています。

個人情報保護マネジメント

個人情報とは、氏名、住所、メールアドレスなど、それ単体もしくは組み合わせることによって生存している個人を特定できる情報のことです。対象となる個人が死亡していたり、法人の場合には個人情報とはなりません。

個人情報保護の基本的な考え方は、個人情報は本人の財産なので、それが勝手に別の人の手に渡ったり（**第三者提供**）、間違った方法（**目的外利用**）で使われたり、内容を勝手に変えられたりしないように適切に管理する必要があるということです。

そのためには、個人情報を守るためのシステムである **PMS** (Personal information protection Management Systems：個人情報保護マネジメントシステム)を構築し、ISMSと同様に維持管理していく必要があります。

個人情報保護に関するガイドラインは、**JIS Q 15001**として定められています。

JIS Q 15001

JIS Q 15001は、PMSを事業者が構築し、適切にマネジメントしていくための仕組み作りについて定めている標準規格です。国際規格であるISO/IEC 15001が基となっており、最新版は2006年に改正されたJIS Q 15001:2006です。JIS Q 15001では、主に次のことが要求されています。

- **個人情報保護方針**の策定と公表
- 個人情報の特定とリスク分析
- 個人情報の利用目的の明確化
- 内部規程を定め、個人情報を適切に管理すること
(PDCAサイクルの運用)



PMSは、改訂前の規格であるJIS Q 15001:1999までは、CP (コンプライアンス・プログラム：Compliance Program)と呼ばれていました。そのため、古い専門書や参考書などではこの言葉で説明されていることも多いです。

- 本人の同意を得て、開示・訂正・苦情などに対応すること

個人情報保護方針とは、個人情報保護に関する取組みについて文書化したもので、企業のWebページなどで公開されています。

■ OECD プライバシーガイドライン

国際的なプライバシーに関する原則としては、OECD(Organization for Economic Co-operation and Development：経済協力開発機構)が発表した、OECD プライバシーガイドラインがあります。プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告として出されています。

このガイドラインには、個人情報保護に関する次の8原則(OECD8原則)が定められています。

1. 収集制限の原則

個人情報の収集は適法かつ公正な手段によらなければならない。本人の認識や同意が必要。

2. データ内容の原則

個人情報は、必要な範囲内で、正確で完全で最新のものでなければならない。

3. 目的明確化の原則

収集目的は、収集時に特定されていなければならない。

4. 利用制限の原則

収集目的を超えて開示、提供、利用されてはならない。

5. 安全保護の原則

紛失、改ざんなどのリスクに対して安全対策が必要。

6. 公開の原則

個人情報の取り扱いについて基本方針を公開する。

7. 個人参加の原則

本人の求めに応じて、回答を行わなければならない。

8. 責任の原則

管理者は、1～7のルールに準拠する責任をもつ。

■ 個人情報保護法

個人情報を守るために2003年に成立した法律が、個人情報の保護に関する法律（個人情報保護法）です。

5,000件以上の個人情報をデータベース等として保持し、事業に用いている事業者は**個人情報事業者**とされ、以下のことを守る義務があります。

- 利用目的の特定
- 利用目的の制限（**目的外利用**の禁止）
- 適正な取得
- 取得に際しての利用目的の通知
- 本人の権利（開示・訂正・苦情など）への対応（窓口での苦情処理）



プライバシーマーク制度については、以下のWebサイトに詳しく解説されています。

<https://privacymark.jp/>
 こちらには、「JIS Q 15001:2006をベースにした個人情報保護マネジメントシステム実施のためのガイドライン【第2版】」など、個人情報を守る仕組みを作るための有益な情報がいろいろ公開されています。

■ プライバシーマーク

JIS Q 15001の要求を満たし、個人情報保護に関して適切な処理を行っていると認定される事業者には、プライバシーマークの利用が認められます。



プライバシーマーク

プライバシーマーク制度の認定は、ISMS適合性評価制度と同様、JIPDEC（日本情報経済社会推進協会）が行っています。

■ マイナンバー法

行政手続における特定の個人を識別するための番号の利用等に関する法律（**マイナンバー法**）とは、国民1人1人に**マイナンバー**（個人番号）を割り振り、社会保障や納税に関する情報を一元的に管理するマイナンバー制度を導入するための法律です。

各種法定書類にマイナンバーが必要となるので、企業の従業

員や個人事業主などは、関係する機関にマイナンバーを提示する必要があります。

■ 特定個人情報の適正な取扱いに関するガイドライン

特定個人情報とは、マイナンバーやマイナンバーに対応する符号をその内容に含む個人情報のことです。マイナンバーに対応する符号とは、マイナンバーに対応し、マイナンバーに代わって用いられる番号や記号などで、住民票コード以外のものを指します。

特定個人情報の適正な取扱いに関するガイドラインは、特定個人情報保護委員会が策定したもので、(事業者編)と(行政機関等・地方公共団体等編)の2種類があり、特定個人情報を扱う際の注意点などがまとめられています。

ガイドラインでは、マイナンバーの利用目的を特定し、源泉徴収票などの**特定の業務以外でのマイナンバーの利用を制限**しています。また、必要がない場合にマイナンバーを請求することが制限されており、委託する場合にも業務が限られ、監督責任が生じます。さらに、不要になって**一定の保管期間を過ぎた場合には速やかに廃棄**することなどが定められています。

■ プライバシー対策の三つの柱

個々の組織やプロジェクトが個人情報保護対策を検討する前提となる、個人情報保護に関する法律やガイドライン、指令等を**プライバシーフレームワーク**といいます。

このフレームワークを規範として、組織での個人情報保護がどのように運用されているか、プライバシー要件を満たしているかについて、組織の判断を支援するシステムが**プライバシー影響評価**(PIA: Privacy Impact Assessment)です。

また、技術面からのプライバシー強化策は、**プライバシーアーキテクチャ**と呼ばれます。

これら三つが**プライバシー対策の三つの柱**として運用され、個々の組織やプロジェクトでカスタマイズされます。



特定個人情報の適正な取扱いに関するガイドラインは、個人情報保護委員会のホームページに公開されています。

<http://www.ppc.go.jp/legal/policy/>

Q&Aなども公開されており、具体的な手続きについての回答も行われています。

■ 匿名化手法

匿名化とは、個人情報を活用する際、その個人を特定できないようにするために、属性に対して削除、加工などを行うことです。匿名化の手法としては、基のデータから一定の割合・個数でランダムに抽出するサンプリングや、同じ保護属性の組合せをもつレコードが少なくともk個存在するように属性の一般化やレコードの削除を行うk-匿名化などがあります。

▶▶ 覚えよう！

- ☐ 個人情報保護法では、利用目的の特定と、窓口の設置などを義務化
- ☐ PMSは、個人情報を保護する体制を作るマネジメントシステム

4-1-4 刑法

刑法の改正で、コンピュータ犯罪に関する条文が追加されました。電磁的記録に関する犯罪行為、詐欺行為などに加え、ウィルスの作成・提供行為なども対象とされています。

■ コンピュータ犯罪防止法

刑法では、1987年の改正から、コンピュータ犯罪も処罰の対象となりました。そのときに制定された刑法を**コンピュータ犯罪防止法**といいます。コンピュータ犯罪防止法では、電子計算機損壊等業務妨害罪や電子計算機使用詐欺罪など、様々な犯罪が定義されています。

① 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、人の業務に使用する電子計算機(コンピュータ)を破壊するなどして業務を妨害することを処罰する法律です。企業が運営するWebページを改ざんする、またはその改ざんによって企業の信用を傷つける情報を流すなどで、業務の遂行を妨害した場合に適用されます。

また、実際に被害が発生せず、**未遂に終わった場合**にも罰せられます。

② 電子計算機使用詐欺罪

電子計算機使用詐欺罪は、電磁的記録を用いて財産上不法の利益を得る犯罪を処罰する法律です。虚偽の内容や不正な内容を作成する**不実の電磁的記録の作出**と、内容が虚偽の電磁的記録を他人のコンピュータで使用する**電磁的記録の供用**の2種類の類型が定められています。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送ることで、不正な振込や送金を実現させることなどが該当します。

③ 電磁的記録不正作出及び供用罪

電磁的記録不正作出及び供用罪は、人の事務処理を誤らせる目的で、その事務処理に関連する電磁的記録を不正に作るという罪です。

④ 支払用カード電磁的記録不正作出等罪

支払用カード電磁的記録不正作出等罪は、人の財産上の事務処理を誤らせる目的で、その事務処理に関連する電磁的記録を不正に作るという罪です。代金・料金の支払用のカード(クレジットカードやプリペイドカードなど)や、預金等のカード(キャッシュカードなど)を不正に作ると、この法律により罰せられます。



ウイルス作成罪は、正当な理由なく故意にウイルスを作成、提供した場合が対象です。

そのため、ウイルス感染を知らずに広めてしまった場合や、ウイルスの報告のために送付することなどは対象外となります。

⑤ 不正指令電磁的記録に関する罪(ウイルス作成罪)

2011年に改正された刑法で新たに追加された不正指令電磁的記録に関する罪(ウイルス作成罪)は、マルウェアなど、不正な指示を与える電磁的記録の作成および提供を正当な理由がないのに故意に行うことを処罰する法律です。

ウイルスの作成については、他人の業務を妨害した場合には、もともと電子計算機損壊等業務妨害罪として処罰の対象となっています。しかし、ウイルスの作成自体が、コンピュータ・ネットワークの安全性に対する公衆の信頼を損なうものと考えられるため、社会一般の信頼を保護するための法律として、ウイルス作成罪が新設されました。

▶▶ 覚えよう!

- ☐ 電子計算機損壊等業務妨害罪は、未遂でも処罰の対象となる
- ☐ ウィルス作成罪は、ウィルスを作成するだけで処罰の対象となる

4-1-5 ■ その他のセキュリティ関連法規・基準

情報セキュリティ関連では、その他にも様々な法規があります。また、情報セキュリティに関連する基準は、様々な省庁から公表されています。

■ その他のセキュリティ関連法規

これまで取り上げてきた法規の他に、次のようなセキュリティ関連法規があります。

① 電子署名及び認証業務等に関する法律 (電子署名法)

インターネットを活用した商取引などでは、ネットワークを通じて社会経済活動を行います。そのために、相手を信頼できるかどうか確認する必要があり、PKI（公開鍵基盤）が構築されました。そのPKIを支え、電子署名に法的な効力をもたせる法律に**電子署名及び認証業務等に関する法律 (電子署名法)**があります。電子署名法により、電子署名に押印と同じ効力が認められるようになりました。電子署名で使う**電子証明書**を発行できる機関は**認定認証事業者**と呼ばれ、国の認定を受ける必要があります。

② プロバイダ責任制限法

Webサイトの利用やインターネット上での商取引の普及、拡大に伴い、サイト上の掲示板などでの誹謗中傷、個人情報の不正な公開などが増えてきました。こういった行為に対し、プロバイダが負う損害賠償責任の範囲や、情報発信者の情報の開示を請求する権利を定めた法律が**プロバイダ責任制限法**です。正式名称は、「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」といいます。ここで定義されている特定電気通信役務提供者には、プロバイダだけでなく、Webサイトの運営者なども含まれます。

プロバイダ責任制限法では、他人の権利を侵害した書込みがなされたとき、プロバイダがそれを知らなかった場合には責任は問われないとされています。



スパムメールとは、受信者の意向を無視して、無差別かつ大量に送りつけるメールのことです。日本では迷惑メールと呼ばれることも多く、これら二つはほぼ同じものとして扱われます。



情報セキュリティに関する基準のうち経済産業省が公表しているものは、以下のWebページにまとめられています。

http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm

情報セキュリティに関するものだけでなく、システム監査などに関するものも、こちらに掲載されています。

③ 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：特定電子メール送信適正化法)

広告などの迷惑メールを規制する法律です。俗に迷惑メール防止法と呼ばれることもあり、スパムメール (迷惑メール) を規制するための内容となっています。

送信者のメールの配信は原則自由で、受け取りたくない場合には受信拒否を通知するという仕組みをオプトアウトといいます。これに対し、受信者があらかじめメール送信の許可を送信者に与えることでメールを送ることが可能となる仕組みをオプトインといいます。

2008年に改定された特定電子メール法では、メール送信の方式がオプトアウトから**オプトイン方式**に変更され、あらかじめ許可を得た場合以外のメールの配信が禁止されました。

■ 情報セキュリティに関する基準

情報セキュリティに関する基準は、経済産業省などがガイドライン・基準として公開しています。主に以下のようなものがあります。

① コンピュータウイルス対策基準

コンピュータウイルスに対する予防、発見、駆除、復旧のために実効性の高い対策をとりまとめた基準です。

② コンピュータ不正アクセス対策基準

コンピュータ不正アクセスによる被害の予防、発見、復旧や拡大、再発防止のために、企業などの組織や個人が実行すべき対策をとりまとめた基準です。

③ ソフトウェア等脆弱性関連情報取扱基準

ソフトウェアの脆弱性関連情報等の取扱いにおいて、関係者に推奨する行為を定めた基準です。脆弱性の情報を適切に流通させ、対策の促進を図ることを目的としています。

■ 政府機関の情報セキュリティ対策のための統一基準

政府機関の情報セキュリティ対策のための統一基準は、政府機関の情報セキュリティ対策を統一するために定められた基準で、内閣サイバーセキュリティセンターが発表しています。

■ スマートフォン安全安心強化戦略

スマートフォンを安心かつ安全に利用する環境について総務省が取りまとめた提言です。利用者情報の適切な取扱い、利用者からの苦情・相談に業界全体で取り組むこと、青少年がSNSを利用するための対応「スマートユースイニシアティブ」などについてまとめられています。

■ ソーシャルメディアガイドライン

ソーシャルメディアガイドラインとは、ソーシャルメディアの利用に際し、企業や学校などが提唱するガイドラインです。SNS利用ポリシともいわれます。総務省では、スマートユースイニシアティブに合わせて、学校などでソーシャルメディアガイドラインを作成することを推奨しています。

▶▶ 覚えよう！

- ☐ 電子署名法では、電子署名に印鑑と同じような効力を認める
- ☐ 特定電子メール法はオプトイン方式で、許可を得ていない相手への送信は不可

4-1-6 演習問題

問1 個人情報保護法

CHECK ▶ ☐☐☐

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2 OECD プライバシーガイドライン

CHECK ▶ ☐☐☐

“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3 特定個人情報の適正な取扱い**CHECK** ▶ ☐☐☐

“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4 不正アクセス禁止法**CHECK** ▶ ☐☐☐

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5 特定電子メール送信適正化法(特定電子メール法)

CHECK ▶ ☐☐☐

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6 特定電子メール法

CHECK ▶ ☐☐☐

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。

問7 電子計算機損壊等業務妨害

CHECK ▶ ☐☐☐

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。

問8 電子計算機使用詐欺罪**CHECK** ▶ ☐☐☐

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ページを不正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。

問9 プロバイダ責任制限法**CHECK** ▶ ☐☐☐

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。

解答と解説

問1

(平成28年春 情報セキュリティマネジメント試験 午前 問32)

《解答》ア

個人情報保護法で定義されている個人情報は、生存する個人の情報であって、特定の個人を識別できる情報を含むものです。メールアドレスは、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場合は個人情報となります。したがって、アが正解です。

イ 特定の個人を識別できる情報が含まれていれば個人情報です。

ウ 既に公表されているものでも、個人情報に該当します。

エ 法人に関する情報は個人情報とはなりません。

問2

(平成28年春 情報セキュリティマネジメント試験 午前 問31)

《解答》エ

OECD プライバシーガイドラインの8原則には「データ内容の原則」があり、データ内容の正確性、完全性、最新性を確保することが定められています。したがって、エが正解です。

アは「収集制限の原則」、イは「公開の原則」、ウは「目的明確化の原則」の説明となります。

問3

(平成28年秋 情報セキュリティマネジメント試験 午前 問33)

《解答》ウ

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)”では、第4-1- (2)「特定個人情報ファイルの作成の制限」に、「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、「個人番号関係事務実施者」に該当する」とあります。つまり、税理士に業務委託して源泉徴収票作成事務を行わせることは認められているので、ウが正解です。

ア 第4-3- (3)「収集・保管制限」に、「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」とあるので、保管してはいけません。

イ 別添の「特定個人情報に関する安全管理措置」の2「講ずべき安全管理措置の内容」では、「F 技術的安全管理措置」の「a アクセス制御」に、「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」とあるので、事務取扱担当者を限定し、アクセス権を制限する必要があります。

エ 第4-1- (1)「個人番号の利用制限」に、「事業者が個人番号を利用するのは、主として、源泉徴収票及び社会保障の書類類に従業員等の個人番号を記載して行政機関等及び健康保険組合等に提出する場合である」とあり、例外的な場合を除いて、これら以外の

目的で利用することは禁じられています。そのため、営業成績の管理などには利用できません。

問4

(平成28年秋 情報セキュリティマネジメント試験 午前 問35)

《解答》エ

不正アクセス禁止法では、第六条に「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を保管してはならない」とあり、他人の識別符号を不正に保管する行為の禁止を明記しています。そのため、不正アクセスを行っていないくても、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場合には処罰の対象となります。したがって、エが正解です。

- ア パスワードの実例を教えることは不正アクセス行為を助長する行為とみなされることもありますが、情報セキュリティの啓発という正当な理由があるので処罰の対象とはなりません。
- イ 不正アクセスを行う目的で保管していないので、処罰の対象ではありません。
- ウ 人を欺いて詐欺を働く行為は、不正アクセス禁止法ではなく刑法の詐欺罪(第二百四十六条)での処罰の対象となります。

問5

(平成28年春 情報セキュリティマネジメント試験 午前 問34)

《解答》エ

特定電子メール送信適正化法(特定電子メール法)で規制される特定電子メールとは、営業や広告宣伝の手段として送信する電子メールであり、あらかじめ特定電子メールを受信することを許可した人以外へのメール送信は禁じられています(オプトイン方式)。したがって、送信することの承諾を得ていない不特定多数の人に送る広告メールは、特定電子メール送信適正化法では禁止されており、迷惑メールに該当します。したがって、エが正解です。

- ア ウイルスに感染していることを知らずに送信した場合は罪にはなりません。
- イ、ウ 特定の相手に送るメールは特定電子メールではないので、特定電子メール送信適正化法では規制されません。

問6

(平成28年秋 情報セキュリティマネジメント試験 午前 問34)

《解答》ウ

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)では、第三条(特定電子メールの送信の制限)において、「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することに同意する旨を送信者又は送信委託者に対し通知した者」への特定電子メールの送信を許可しています。これをオプトイン方式というので、ウが正解です。

ア 第三条での許可される送信者にはあてはまらず、特定電子メールの送信は禁止されています。

イ 2008年12月の特定電子メール法改正によって、未承諾広告であることを明記しても、相手の承諾なしに広告メールを送ることは禁止となりました。

エ 第六条(架空電子メールアドレスによる送信の禁止)で、プログラムによって自動的に生成される架空のメールアドレスの使用は禁止されています。

問7

(平成28年春 情報セキュリティマネジメント試験 午前 問33)

《解答》ア

“電子計算機損壊等業務妨害”とは、人の業務に使用する電子計算機を損壊するなどの方法によって、電子計算機に使用目的に沿うべき動作をさせず、または使用目的に反する動作をさせて、人の業務を妨害することです。Webページの改ざんは業務妨害に該当するので、アが正解です。

イは不正競争防止法(ドメイン名の不正取得)違反、ウは著作権侵害、エは窃盗罪に該当します。

問8

(平成28年秋 情報セキュリティマネジメント試験 午前 問32)

《解答》ウ

刑法の第二百四十六条の二(電子計算機使用詐欺)には、「人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」とあります。

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ことは、虚偽の電磁的記録での不法の利益となるので、ウが正解です。

- ア 特定商取引法「連鎖販売取引」第三十四条(禁止行為)が適用されます。
- イ 特定商取引法「通信販売」第十二条(誇大広告等の禁止)が適用されます。
- エ 刑法の第二百三十四条の二(電子計算機損壊等業務妨害)が適用されます。

問9

(平成28年秋 情報セキュリティマネジメント試験 午前 問31)

《解答》エ

プロバイダ責任制限法(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)では、第三条(損害賠償責任の制限)で、「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」に該当しない場合には、賠償の責めに任じないとされています。そのため、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なかった場合には、放置していても損害賠償責任が制限されます。したがって、エが正解です。

- ア 個人情報保護法の第十六条(利用目的による制限)が適用されます。
- イ 消費者契約法の第九条(消費者が支払う損害賠償の額を予定する条項等の無効)が適用されます。
- ウ 電波法の第五十九条(秘密の保護)、または有線電気通信法の第九条(有線電気通信の秘密の保護)が適用されます。

4-2

その他の法規・標準

情報セキュリティ関連以外にも、情報資産を守るための法規・標準には、知的財産権や労働関連の法律をはじめとする様々なものがあります。



勉強のコツ

法律は、基本的には暗記分野なので、知っていれば解答はできますが、その法律の意義や背景について理解していると、覚えやすく、実務にも役立ちます。

4-2-1 知的財産権

知的財産権は、ソフトウェアなどの知的財産を守るための権利です。知的財産の開発者の利益を守り、市場で適正な利潤を得られるようにするために法律が整備されています。

■ 知的財産権

知的財産権とは、知的財産に関する様々な法令により定められた権利です。文化的な創作の権利には、**著作権**や**著作隣接権**があります。また、産業上の創作の権利には、**特許権**や**実用新案権**、**意匠権**、**産業財産権**などがあります。営業上の創作の権利には、**商標権**や**営業秘密**などがあります。



関連

2015年10月、TPP（環太平洋戦略的経済連携協定）交渉が大筋合意されました。その内容をもとに、著作権改正法案が2016年3月に国会に提出されました。法案には、著作権の存続期間を死後70年に延長、著作権等侵害罪の一部非親告罪化などの改正項目もあります。

2016年11月現在、国会で審議中ですので、今後の動向を確認しておきましょう。

■ 著作権法

著作権の保護対象は著作物で、思想または感情を創作的に表現したものであって、文芸、学術、美術または音楽の範囲に属するものです。コンピュータプログラムやデータベースは著作物に含まれますが、アルゴリズムなどアイデアだけのものや、工業製品などは除かれます。

著作権は産業財産権と違い、**無方式主義**、つまり出願や登録といった手続は不要です。そのため、権利侵害が認められれば処罰されます。また著作権の存続期間は、著作者の**死後50年**です。コンピュータプログラムの場合には、**私的使用のための複製**は認められています。

また、2012年に改正された著作権法では、**違法ダウンロード行為**に対する罰則が加えられました。また、**コピープロテクト外**しなど、複製を防ぐ技術に対して、それを回避してコピーすることも違法とされています。

■ 産業財産権法

産業財産権には、**特許権**、**実用新案権**、**意匠権**、**商標権**の四つがあります。特許法では、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る**発明**を保護します。特許は発明しただけでは保護されず、特許権の審査請求を行い、審査を通過しなければなりません。特許の要件は、産業上の利用可能性、新規性、進歩性があり、先願（最初に出願）の発明であることなどです。

発明のうち高度でないものは、実用新案法の対象になります。また、意匠（デザイン）に関するものは意匠法の対象で、商標に関するものは商標法の対象になります。

■ 不正競争防止法

不正競争防止法は、事業者間の不正な競争を防止し、公正な競争を確保するための法律です。営業秘密（トレードシークレット）に係る不正行為では、不正な手段によって営業秘密を取得し使用する、第三者に開示するなどの行為は禁じられています。**営業秘密**として保護を受けるためには、次の三つを満たす必要があります。

1. **秘密管理性**（秘密として管理されていること）
2. **有用性**（有用であること）
3. **非公知性**（公然と知られていないこと）

また、他人の著名な商品にただ乗りする**著名表示冒用行為**や、他人の商品などと同一・類似のドメイン名を使用するなどの**ドメイン名に係る不正行為**なども、不正競争防止法で禁止されています。

▶▶ 覚えよう！

- ☐ 改定著作権法では、違法ダウンロード行為やコピープロテクト外しもダメ
- ☐ 営業秘密は秘密管理性、有用性、非公知性を満たす必要がある

4-2-2 ■ 労働関連・取引関連法規

労働関連法規は、労働者の生活・福祉の向上を目的とする法律です。労働基準法や労働者派遣法などがあります。取引関連法規は会社の取引に関する法律で、下請法、民法、商法などがあります。

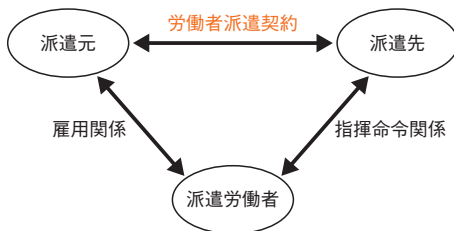
■ 労働基準法

労働基準法では、労働者を保護するため、就業規則や労働時間などを規定しています。労働時間については、1日の法定労働時間の上限は**8時間**、1週間では**40時間**と定められています。

また、労働基準法では、時間外労働(残業)、休日労働は基本的に認められていません。労働者と使用者(経営者)の間で労使協定を結び、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ようになります。この協定は、労働基準法第36条を根拠とすることから**36協定**^{サブロク}と呼ばれます。

■ 労働者派遣法

労働者を派遣する場合、労働者、派遣元、派遣先の三者で関係を結びます。具体的には、以下の図のようになります。



労働者派遣法の概念

雇用関係があるのは、派遣元と派遣労働者の間で、指揮命令は派遣先から派遣労働者に対して行います。

■ その他の労働関連の法規

その他の労働関連の法律としては、男女雇用機会均等法や公益通報者保護法、労働安全衛生法などがあります。

男女雇用機会均等法では、性別による、配置、昇進、降格、教育訓練などへの差別的扱いを禁止します。

公益通報者保護法では、内部告発を行った労働者を保護するため、内部告発者に対する解雇や減給などの不利益な扱いを無効にします。

労働安全衛生法では、労働災害を防止し、労働者の安全と健康の確保や快適な職場環境の形成を促進することが定められています。

■ 下請法

下請法とは、下請取引の公正化や、下請事業者の利益を保護するための法律です。プログラムなどの情報成果物に対しては、情報成果物作成委託が行われます。

■ 企業間の取引にかかわる契約

企業間の取引にかかわる契約にはいろいろな形態がありますが、典型契約として代表的なものに、請負契約と委任契約があります。

請負契約とは、ある仕事を完成することを約束する契約で、労働者への指揮命令は請け負った企業（請負先）が行います。請負元の企業が具体的な指揮命令を行うことは、偽装請負と判断されます。

委任契約は、法律行為を行うことを委託する契約です。法律行為以外を委託する場合は**準委任契約**といいます。

■ ソフトウェア開発契約

ソフトウェア開発においては、**請負契約**や**準委任契約**がよく用いられます。請負契約では、契約した仕事を**完成させる責任**があるのに対して、準委任契約では、**善管注意義務**（善良な管理者としての注意義務）はありますが**完成責任**はありません。

また経済産業省では、産業構造・市場取引を可視化する取組みとして**情報システム・モデル取引・契約書**をとりまとめ、公開



善管注意義務とは、業務を行う人の階層や地位、職業などに応じて、社会通念上、客観的・一般的に要求される注意を払う義務です。

しています。それに関連し、JISA（一般社団法人情報サービス産業協会）がソフトウェア開発委託基本モデル契約を公表しています。

■ インターネットを利用した取引

インターネットを利用した取引に関する法律には、特定商取引法や電子消費者契約法などがあります。

特定商取引法は、訪問販売や通信販売などを規制する法律です。**電子消費者契約法**は、電子商取引などによる消費者の操作ミスを救済するための法律です。

また、インターネットにおける新しい著作権ルールの普及を目指すプロジェクトに、著作権者が自分で著作物の再利用を許可するためにライセンスを策定するクリエイティブ・コモンズというプロジェクトがあります。**クリエイティブ・コモンズ・ライセンス**には、著作権がある状態と、著作権が消滅して放棄された状態であるパブリックドメインの中間に位置するものまで、様々なレベルのライセンスがあります。

■ ソフトウェア使用許諾契約(ライセンス契約)

ソフトウェアの知的財産権の所有者が第三者にソフトウェアの利用許諾を与える際に取り決める契約が、**ソフトウェア使用許諾契約**(ライセンス契約)です。許諾する条件により、ボリュームライセンス契約、サイトライセンス契約、シュリンクラップ契約など、様々な形態があります。



市販のパッケージなどでは、購入したソフトウェアの入ったCD (DVD)・ROMの包装を破った時点で使用許諾契約が成立するとするシュリンクラップ契約があります。

■ オープンソースライセンスリング

オープンソースソフトウェア (Open Source Software : OSS) のライセンスでは、ソフトウェアの原作者がどのようなライセンスを採用するかは自由です。そのためライセンスは多様で、次のような考え方があります。

① コピーレフト

著作権を保持したまま、二次的著作物も含めて、すべての人が著作物を利用・改変・再頒布できなければならないという考え方です。

②デュアルライセンス

一つのソフトウェアを異なる2種類以上のライセンスで配布する形態です。利用者は、そのうちの一つのライセンスを選びます。

③GPL (General Public License)

OSSのライセンス体系の一つで、コピーレフトの考え方に基づきます。GPLのソフトを再頒布する場合にはGPLのライセンスを踏襲する必要があります。

④BSD (Berkeley Software Distribution) ライセンス

OSSのライセンス体系の一つで、GPLに比べて制限の少ないライセンスです。無保証であることの明記と、著作権及びライセンス条文を表示する以外は自由です。



デュアルライセンスでは、フリーライセンス／商用ライセンスなどのかたちで、複数のライセンスから条件に応じてライセンスを選びます。例えば、元のソースコードを改変して公開したくない場合には商用ライセンス、公開する場合にはフリーライセンス、というように使い分けます。

▶▶ 覚えよう！

- ☐ 派遣契約では命令指揮は派遣先、請負契約では請負元自身で完成責任を負う
- ☐ 36協定を結ばないと、残業を行わせることはできない

4-2-3 その他の法律・ガイドライン・技術者倫理

これまで取り上げてきた法律やガイドラインの他にも、IT関連の法律には様々なものがあります。また、法律を守るだけでなく、情報倫理・技術者倫理について考えることも大切です。

その他のIT関連の法律

IT関連の法律としては、次のものがあります。

① IT基本法

高度情報通信ネットワーク社会形成基本法（IT基本法）は、日本が世界最高水準のIT国家になることを目指して制定された法律です。高度情報通信ネットワークの整備や、行政の情報化などが掲げられています。

② e-文書法

e-文書法とは、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」と「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律の施行に伴う関係法律の整備等に関する法律」の総称で、電子文書法ともいいます。

商法や税法で保管が義務づけられている文書について、電磁的記録（電子化された文書ファイル）での保存が認められるようになりました。

③ 電子帳簿保存法

電子帳簿保存法とは、国税関係の帳簿書類を電子保存するための法律で、2015年9月に改正されました。原本が紙である国税書類も、スキャナを使用して作成した電子データで保存できるようになりました。

■ コンプライアンス

コンプライアンスは法令遵守と翻訳される概念で、法令や規則などのルールや社会的規範を守ることです。

企業のコンプライアンスのことを企業コンプライアンスと呼び、区別することもあります。

■ CSR

CSR (Corporate Social Responsibility：企業の社会的責任) とは、企業が利益を追求するだけでなく、社会へ与える影響にも責任をもち、利害関係者(ステークホルダ)からの要求に対し適切な意思決定をすることです。

■ 情報倫理・技術者倫理

情報倫理とは、ITを利用するときの行動規範です。ITに特有な倫理としては、利用者の情報倫理や技術者の職業倫理(技術者倫理)などがあります。

利用者の情報倫理としては、SNSなどで他人を誹謗・中傷しない、プライバシーを侵害しない、反社会的な情報を流さない、などが挙げられます。また、セキュリティ対策を行い、マルウェア感染や第三者攻撃の踏み台にされないようにすることも大切です。

技術者倫理としては、IT関連だけでなくIT化の対象業務関連も含むコンプライアンスを遵守する必要があります。また、経営者がコンプライアンスポリシー、セキュリティポリシー、プライバシーポリシーなどを作成して、組織の内外に宣言することも重要となります。さらに、技術者自身が自律的に職業倫理を守るような組織文化を作り出すことが大切です。

▶▶ 覚えよう！

- ☐ 電子帳簿保存法では、スキャナで取り込んだ紙の文書も使用可能
- ☐ 情報倫理とは、ITを利用するときの行動規範

4-2-4 ■ 標準化関連

標準や規格などには、標準化団体が決めるデジュレスタンダードと、事実上の標準であるデファクトスタンダードの2種類があります。

■ 日本工業規格 (JIS)

JIS (Japanese Industrial Standards: 日本工業規格) は、日本の国家標準の一つで、工業標準です。工業標準化法に基づき、**JISC** (Japanese Industrial Standards Committee: 日本工業標準調査会) の答申を受けて主務大臣が制定します。情報処理についてはJIS X部門が、管理システムについてはJIS Q部門が行っています。

■ 国際規格 (IS)

IS (International Standards: 国際規格) は、**ISO** (International Organization for Standardization: 国際標準化機構) で制定された世界の標準です。ISOは各国の代表的な標準化機関から成り、電気及び電子技術分野を除く工業製品の国際標準の策定を目的としています。

■ その他の標準

ISOでは電気及び電子技術分野を取り扱いませんが、その分野を補う国際規格としては、**ITU** (International Telecommunication Union: 国際電気通信連合) や**IEC** (International Electrotechnical Commission: 国際電気標準会議)、**IEEE** (Institute of Electrical and Electronics Engineers: 電気電子学会) などがあります。IEEEの規格としては、イーサネットに関するIEEE 802や、Fire Wireに関するIEEE 1394などが有名です。

任意団体では、インターネットの標準を定める**IETF** (Internet Engineering Task Force: インターネット技術タスクフォース) があります。RFC (Request For Comments) を公開し、プロトコルやファイルフォーマットを主に扱います。

また、日本のJISに対応する米国の標準化組織にANSI (American National Standards Institute: 米国規格協会) があり、ASCIIの

文字コード規格や、C言語の規格などを定めています。

■ デジュレスタンダードとデファクトスタンダード

JISやISなどの標準化団体によって定められた標準規格のことをデジュレスタンダード (de jure standard) といいます。

それに対し、公的に標準化されていなくても事実上の規格、基準となっているものをデファクトスタンダード (de facto standard: 事実上の標準) といいます。オブジェクト指向のOMG (Object Management Group) や、Webの標準を定めるW3C (World Wide Web Consortium) などがその例です。

|| ▶▶ 覚えよう!

- ☐ 国際標準化団体がIS, 日本の標準化団体がJIS, 米国はANSI
- ☐ デファクトスタンダードは、公式に標準化されていない事実上の標準

4-2-5 演習問題

問1 著作権法によるソフトウェア保護

CHECK ▶ ☐☐☐

著作権法によるソフトウェアの保護範囲に関する記述のうち、適切なものはどれか。

- ア アプリケーションプログラムは著作権法によって保護されるが、OSなどの基本プログラムは権利の対価がハードウェアの料金に含まれるので、保護されない。
- イ アルゴリズムやプログラム言語は、著作権法によって保護される。
- ウ アルゴリズムを記述した文書は著作権法で保護されるが、そのアルゴリズムを用いて作成されたプログラムは保護されない。
- エ ソースプログラムとオブジェクトプログラムの両方とも著作権法によって保護される。

問2 不正競争防止法

CHECK ▶ ☐☐☐

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3 請負契約**CHECK** ▶ ☐☐☐

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。

4**問4 準委任契約****CHECK** ▶ ☐☐☐

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5 コンプライアンスの確立**CHECK** ▶ ☐☐☐

企業の活動a～dのうち、コンプライアンスの確立に関するものだけを全て挙げたものはどれか。

- a 芸術や文化活動を支援する。
- b 従業員に対して行動規範の教育を行う。
- c 地球の砂漠化防止の取組みを行う。
- d 内部通報の仕組みを作る。

ア a, b イ a, c ウ b, d エ c, d

問6 日本工業標準調査会

CHECK ▶ ☐☐☐

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、特にJISの制定、改正などに関する審議を行っている。
- イ 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、学会活動、書籍の発行、IEEE規格の標準化を行っている。
- ウ 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。
- 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規格の制定及び普及の事業を行っている。

■ 解答と解説

問1

(平成26年秋 基本情報技術者試験 午前 問79)

《解答》 **エ**

著作権が保護する対象は著作物です。著作物とは、思想または感情を創作的に表現したものであり、文芸、学術、美術または音楽の範囲に属するものです。コンピュータプログラムやデータベースは著作物に含まれますが、アルゴリズムなどアイデアだけのものや工業製品などは除かれます。したがって、**エ**が正解です。

ア OSはコンピュータプログラムなので、著作権で保護されます。

イ アルゴリズムは著作権で保護されません。

ウ プログラムは著作権で保護されます。

4

問2

(平成28年春 情報セキュリティマネジメント試験 午前 問35)

《解答》 **ウ**

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るものには営業秘密があります。営業秘密とは、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であるため、**ウ**が正解です。

アは特許法で保護される発明、イ、エは著作権法で保護される著作物です。

問3

(平成28年春 情報セキュリティマネジメント試験 午前 問36)

《解答》 **イ**

請負契約とは、請負人が仕事の完成を約束する契約です。請負の場合は、労働者の作業場所が契約先の事務所であっても、請負人の雇用主は自らの指揮命令の下に労働者を業務に従事させる必要があります。したがって、**イ**が正解です。

ア、エ 労働者派遣契約の下で行われる必要があります。

ウ 請負契約、労働者派遣契約のいずれにおいても、雇用関係の変更はありません。

問4

(平成28年秋 情報セキュリティマネジメント試験 午前 問36)

《解答》ウ

準委任契約では、仕事の完成は約束されず、業務を実施して報告する善管注意義務があります。業務分析や要件定義、コンサルティングなどでよく行われる契約です。したがって、ウが正解です。

ア、イ 請負契約の説明です。

エ 派遣契約、出向契約の説明です。

問5

(平成27年春 ITパスポート試験 午前 問22)

《解答》ウ

コンプライアンスは法令遵守と翻訳される概念で、法令や規則などのルールや社会的規範を守ることです。企業のコンプライアンスのことを企業コンプライアンスと呼び、区別することもあります。これに該当するのが、b、dです。したがって、ウが正解です。

a、cは、CSR (Corporate Social Responsibility：企業の社会的責任)に該当します。

問6

(平成27年春 基本情報技術者試験 午前 問80)

《解答》ア

日本工業標準調査会 (Japanese Industrial Standards Committee：JISC) は、工業標準化法に基づき、JIS (Japanese Industrial Standards：日本工業規格) を制定する審議を行います。したがって、アが正解です。

イ IEEE (Institute of Electrical and Electronics Engineers：電気電子学会) の説明です。

ウ 電気規格調査会 (Japanese Electrotechnical Committee：JEC) の説明です。

エ 一般社団法人電子情報技術産業協会 (Japan Electronics and Information Technology Industries Association：JEITA) の説明です。

第5章

マネジメント

マネジメント分野は、組織の情報セキュリティを考えるとときに重要となる分野です。情報セキュリティマネジメント試験では、午前問題で主に出題されます。

この章では、マネジメント系の分野であるシステム監査、サービスマネジメント、プロジェクトマネジメントの3分野について学びます。それぞれの考え方と、情報セキュリティとの関連を押さえておくことがポイントです。

5-1 システム監査

- ◆ 5-1-1 システム監査
- ◆ 5-1-2 内部統制
- ◆ 5-1-3 演習問題

5-2 サービスマネジメント

- ◆ 5-2-1 サービスマネジメント
- ◆ 5-2-2 サービスの設計・移行
- ◆ 5-2-3 サービスマネジメントプロセス
- ◆ 5-2-4 サービスの運用
- ◆ 5-2-5 ファシリティマネジメント
- ◆ 5-2-6 演習問題

5-3 プロジェクトマネジメント

- ◆ 5-3-1 プロジェクトマネジメント
- ◆ 5-3-2 プロジェクト統合マネジメント
- ◆ 5-3-3 プロジェクトステークホルダマネジメント
- ◆ 5-3-4 プロジェクトスコープマネジメント
- ◆ 5-3-5 プロジェクト資源マネジメント
- ◆ 5-3-6 プロジェクトタイムマネジメント
- ◆ 5-3-7 プロジェクトコストマネジメント
- ◆ 5-3-8 プロジェクトリスクマネジメント
- ◆ 5-3-9 プロジェクト品質マネジメント
- ◆ 5-3-10 プロジェクト調達マネジメント
- ◆ 5-3-11 プロジェクトコミュニケーションマネジメント
- ◆ 5-3-12 演習問題

5-1 システム監査

システム監査とは、組織の情報システムが適正に運用・活用されているか評価することです。システム監査基準やシステム管理基準などの基準に従って、情報システムの監査を行います。



頻出ポイント

システム監査(情報セキュリティ監査も含む)の分野は、情報セキュリティマネジメント試験では頻出で、この分野だけで午前に毎回4問程度出題されています。重点的に学習することをおすすめする分野です。



勉強のコツ

システム監査基準に出てくるシステム監査の考え方や手順について、主に問われます。監査の独立性や専門性などの考え方と、監査調書や監査証跡、指摘事項など、用語は正確に押さえておきましょう。



関連

システム監査基準、システム管理基準については後述します。

5-1-1 システム監査

システム監査では、対象の組織体(企業や行政機関など)が情報システムにまつわるリスクを適切にコントロールし、整備・運用しているかどうかをチェックします。

監査業務の種類

監査とは、ある対象に対し、順守すべき法令や基準に照らし合わせ、業務や成果物がそれに則っているかについて証拠を収集し、評価を行って利害関係者に伝達することです。

監査の業務には、その対象によって、システム監査、会計監査、情報セキュリティ監査、個人情報保護監査、コンプライアンス監査など、様々なものがあります。

また、組織外の独立した第三者が行う**外部監査**と、その組織の内部で行われる**内部監査**の2種類に分けられます。

さらに、基準に照らし合わせて適切であることを保証する**保証型監査**と、問題点を検出して改善提案を行う**助言型監査**という分け方もあります。

システム監査の目的

システム監査では、情報システムに関して監査を行います。対象の組織体(企業や行政機関など)が情報システムに関連するリスクを適切にコントロールし、整備・運用しているかをチェックします。監査を受けた組織体は、監査の結果を基に、情報システムの**安全性**、**信頼性**、**効率性**、**有効性**をさらに高め、経営方針や戦略目標の実現に取り組むことができますようになります。

■ システム監査人の要件

システム監査を行う人をシステム監査人といいます。システム監査人の要件で最も大切なものは**独立性**です。内部監査の場合でも、システム監査は社内の独立した部署で行われます。システム監査人は監査対象から独立していなければなりません。身分上独立している**外観上の独立性**だけでなく、公正かつ客観的に監査判断ができるよう**精神上的の独立性**も求められます。

また、システム監査人は、**職業倫理と誠実性**、そして**専門能力**をもって職務を実施する必要があります。

■ システム監査の手順

システム監査は、①監査計画の策定、②予備調査、③本調査、④評価・結論の手順で実施します。

① 監査計画

システム監査人は、実施するシステム監査の目的を有効かつ効率的に達成するために、監査手続の内容、時期及び範囲などについて適切な監査計画を立案します。監査計画は、事情に応じて修正できるよう、弾力的に運用します。

② 予備調査

監査手続は、十分な監査証拠を入手するための手続です。システム監査の調査は、予備調査と本調査の二つに分けて行います。予備調査では、正確なシステム監査を実施するために、管理者へのヒアリングや資料の確認などで、監査対象の実態を概略的に調査します。

③ 本調査

予備調査の結果を基に、監査対象の実態を調査します。システム監査人は適切かつ慎重に**監査手続**を実施し、監査結果を裏付けるのに十分かつ適切な**監査証拠**を入手します。

監査手続としては、ヒアリング、現場調査、資料の入手、内容確認、質問票やアンケートなどがよく使われます。



システム監査では独立性が重視されるので、現在関係がある会社に依頼することは避ける必要があります。まったく独立して監査を行う企業を探すための資料としては、**システム監査企業台帳**があります。経済産業省が公表しており、こちらを参考に、システム監査を行う企業を探すことができます。

<http://www.meti.go.jp/policy/netsecurity/sys-kansa/>

④ 評価・結論

監査手続の結果とその関連資料をまとめて**監査調書**として作成します。監査調書は、監査結果の裏付けとなるため、監査の結論に至った過程が分かるように記録し、保存します。

■ システム監査の報告

システム監査人は、実施した監査についての**監査報告書**を作成し、監査の依頼者（組織体の長）に提出します。監査報告書には、実施した監査の対象や概要、保証意見または助言意見、制約などを記載します。また、監査を実施した結果において発見された**指摘事項**と、その改善を進言する**改善勧告**について明瞭に記載します。参考資料として、システム監査時にまとめた監査調書や監査証拠なども添付します。

■ システム監査終了後の任務

システム監査人は、監査報告書の記載事項について責任を負います。そして、監査の結果に基づいて改善できるよう、監査報告に基づく改善指導（**フォローアップ**）を行います。また、システム監査の実施結果の妥当性を評価するシステム監査の**品質評価**も行うことがあります。

■ システム監査技法

システム監査の技法としては、一般的な資料の閲覧・収集、ドキュメントレビュー（査閲）、チェックリスト、質問書・調査票、インタビューなどのほかに次のような方法があります。

① 統計的サンプリング法

母集団からサンプルを抽出し、そのサンプルを分析して母集団の性質を統計的に推測します。

② 監査モジュール法

監査対象のプログラムに監査用のモジュールを組み込んで、プログラム実行時の監査データを抽出します。

③ITF (Integrated Test Facility) 法

稼働中のシステムにテスト用の架空口座 (ID) を設置し、システムの動作を検証します。実際のトランザクションとして架空口座のトランザクションを実行し、システムの正確性をチェックします。

④コンピュータ支援監査技法 (CAAT : Computer Assisted Audit Techniques)

監査のツールとしてコンピュータを利用する監査技法の総称です。③のITF法もCAATの一例であり、テストデータ法など様々な技法があります。

■ 監査証跡とコントロール

監査証跡とは、監査対象システムの入力から出力に至る過程を追跡できる一連の仕組みと記録です。情報システムの**可監査性**を保つために、ログやトレースの情報を取得できるように設計しておきます。監査証跡は、情報システムに対して、**信頼性**、**安全性**、**効率性**のコントロールが適切に行われていることを実証するために用いられます。

監査におけるコントロールとは、**統制を行うための手続**です。コントロールの具体例としては、画面上で入力した値が一定の規則に従っているかどうかを確認する**エディットバリデーションチェック**や、数値情報の合計値を確認することでデータに漏れや重複がないかを確認する**コントロールトータルチェック**などがあります。

■ システム監査の基準

システム監査を行う際の基準としては、システム監査基準とシステム管理基準があります。

①システム監査基準

システム監査人のための行動規範です。一般基準、実施基準、報告基準から構成されています。



可監査性とは、処理の正当性などを効果的に監査できるように情報システムが設計・運用されていることです。監査ができるような情報システムにしておくことで、適正にコントロールされているか確認できます。



トレースとは、プログラムの実行過程を辿ることです。監査におけるトレースは、実際に実行されたデータや実行状況などを詳細に記録したものとなります。



システム監査基準／管理基準、情報セキュリティ監査基準／管理基準などの原本は、経済産業省のホームページ (下記) に掲載されています。
http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm

②システム管理基準

システム監査基準に従って監査を行う場合に、監査人が判断の尺度として用いる基準です。

情報戦略、企画業務、開発業務、運用業務、保守業務、共通業務について全287項目から構成されています。

■情報セキュリティの監査

情報セキュリティに関する監査を行うためには、システム監査と同様に監査を実施し、評価・フォローアップを行います。さらに、情報セキュリティ特有の監査として、JIS Q 27001やJIS Q 27002などの情報セキュリティマネジメントシステムの基準をもとに、監査項目を定めていきます。

情報セキュリティ監査を行うにあたって利用する主な基準には、次のものがあります。

①情報セキュリティ監査基準

情報セキュリティ監査人のための行動規範です。システム監査基準の情報セキュリティバージョンといえます。**情報資産**を保護し、情報セキュリティのリスクマネジメントが効果的に実施されるように、情報セキュリティ監査人が**独立かつ専門的な立場**から検証や評価を行います。

また、場合によっては**他の専門家の支援**を仰ぐことも定義されており、適切な監査体制を築いて、情報セキュリティ監査人の責任で監査を行います。

②情報セキュリティ管理基準

情報セキュリティ監査基準に従って監査を行う場合に、監査人が判断の尺度として用いる基準です。平成28年度改正版は**JIS Q 27001とJIS Q 27002を基に策定**されており、情報セキュリティマネジメント体制の構築と、適切な管理策の整備と運用を行うための基準となっています。

そのため、情報セキュリティ管理基準は、マネジメント基準と管理策基準から構成されており、情報セキュリティマネジメントの確立から具体的な管理策の整備まで、幅広くカバーしています。



関連

情報セキュリティ管理基準は、「ISMS適合性評価制度」で用いられる適合性評価の尺度と整合するように配慮されています。

しかし、以前の平成20年度改正版ではISO/IEC 27001:2005及びISO/IEC 27002:2005に基づいており、平成26年にJIS Q 27001:2014及びJIS Q 27002:2014にに合わせて改正されたISMS適合性評価制度の文書とはずれが生じていました。

平成28年度改正版で、JIS Q 27001:2014及びJIS Q 27002:2014に合わせて改正されたため、再びISMS適合性評価制度と整合するようになりました。

■ 監査関連法規・標準

その他、システム監査に関連する標準や法規としては、主に以下のものがあります。

①個人情報保護関連法規

個人情報保護に関する法律や、プライバシーマーク制度で使われるJIS Q 15001などのガイドラインは、個人情報保護に関する監査に利用されます。

②知的財産権関連法規

システム監査では権利侵害行為を指摘する必要があるため、著作権法、特許法、不正競争防止法などの知的財産権に関する法律を参考にします。

③労働関連法規

システム監査では法律に照らして労働環境における問題点を指摘する必要があるため、労働基準法、労働者派遣法、男女雇用機会均等法などの労働に関する法律を参考にします。

④法定監査関連法規

システム監査は、会計監査などの法定監査との連携を図りながら実施する必要があるため、株式会社の監査等に関する商法の特例に関する法律や金融商品取引法、商法など法定監査に関わる法律も参考にします。

■ コンプライアンス監査

コンプライアンス監査は、組織のコンプライアンスに関する監査です。組織の行動指針や倫理、透明性などについて監査を行います。権利侵害行為への指摘、労働環境における問題点の指摘などを行います。

▶▶ 覚えよう！

- ☐ システム監査人は外観上と精神上的の独立性が大事
- ☐ 監査証跡は信頼性、安全性、効率性をコントロールする

5-1-2 内部統制

内部統制とは、健全かつ効率的な組織運営のための体制を、企業などが自ら構築し運用する仕組みです。内部監査と密接な関係があります。

内部統制

内部統制のフレームワークの世界標準は、米国のトレッドウェイ委員会組織委員会(COSO: the Committee of Sponsoring Organization of the Treadway Commission)が公表した**COSO フレームワーク**です。日本では、金融庁の企業会計審議会・内部統制部会が、「財務報告に係る内部統制の評価及び監査の基準」及び「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」を制定し、日本における内部統制の実務の基本的な枠組みを定めています。この基準によると、内部統制の意義は次の四つの目的を達成することです。

【四つの目的】

●業務の有効性及び効率性

事業活動の目的の達成のため、業務の有効性及び効率性を高めること

●財務報告の信頼性

財務諸表及び財務諸表に重要な影響を及ぼす可能性のある情報の信頼性を確保すること

●事業活動に関する法令等の遵守

事業活動に関わる法令その他の規範の遵守を促進すること

●資産の保全

資産の取得、使用及び処分が正当な手続及び承認の下に行われるよう、資産の保全を図ること

そして、内部統制の目的を達成するために、次の六つの基本要素が定められています。

【六つの基本的要素】

●統制環境

組織の気風を決定する倫理観や経営者の姿勢、経営戦略など、他の基本的要素に影響を及ぼす基盤です。

●リスクの評価と対応

リスクを洗い出し、評価し、対応する一連のプロセスです。

●統制活動

経営者の命令や指示が適切に実行されることを確保するための要素です。**職務の分掌**や**相互牽制**(職務の分離)の方針や手続が含まれます。

●情報と伝達

必要な情報が識別、把握、処理され、組織内外の関係者に正しく伝えられることを確保するための要素です。

●モニタリング

内部統制が有効に機能していることを継続的に評価するプロセスです。

●ITへの対応

組織の目標を達成するために適切な方針や手続を定め、それを踏まえて組織の内外のITに適切に対応することです。IT環境への対応とITの利用及び統制から構成されます。COSOフレームワークにはない、**日本独自の追加要素**です。



職務の分掌とは、業務を実行する人とそれを承認する人を分けるなど、業務を1人で完了できないようにすることです。

相互牽制とは、複数の人間が互いに牽制し合って誤りや不正を防ぐ仕組みです。

■ITガバナンス

ITガバナンスとは、企業などが競争力を高めることを目的として情報システム戦略を策定し、戦略実行を統制する仕組みを確立するための組織的な仕組みです。より一般的なコーポレートガバナンス(企業統治)は、企業価値を最大化し、企業理念を実現するために企業の経営を監視し、規律する仕組みです。そのため的手段として、内部統制やコンプライアンス(法令遵守)が実施されます。

ITガバナンスのベストプラクティス集(フレームワーク)には **COBIT** (Control Objectives for Information and related Technology) があります。

■ 順守状況の評価・改善

内部統制では、自社内外の行動規範の順守状況を継続的に評価することが大切です。内部統制の有効性について、業務運営の中で業務を運用している人自身が、その有効性について評価を行う **CSA** (Control Self Assessment : 統制自己評価) という手法があります。CSAを行うことで、管理部門としては評価の負荷軽減となります。また、業務を行う人自身も、どのようなリスクがあるか、どのように対応すべきかなどについて自分のこととして考えることができます。

▶▶ 覚えよう！

- ☐ 内部統制は、企業自らが構築し運用する仕組み
- ☐ ITガバナンスは、IT戦略をあるべき方向に導く組織能力

5-1-3 演習問題

問1 スプレッドシートに係るコントロールの監査

CHECK ▶ ☐☐☐

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2 BCPについての監査

CHECK ▶ ☐☐☐

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3 情報セキュリティに係る保証又は助言を与えるもの

CHECK ▶ ☐☐☐

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

問4 情報セキュリティ管理基準に基づく監査

CHECK ▶ ☐☐☐

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5 情報セキュリティ監査基準の対象

CHECK ▶ ☐☐☐

“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可否の組み合わせのうち、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 監査実施の可否
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6 情報セキュリティ監査基準

CHECK ▶ ☐☐☐

“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”が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。

問7 証拠を収集し保全する技法

CHECK ▶ ☐☐☐

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 イ サンプルング
- ウ デジタルフォレンジックス エ ベンチマーキング

問8 ISMS運用の内部監査

CHECK ▶ ☐☐☐

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。

問9 データの完全性

CHECK ▶ ☐☐☐

内部統制の観点から、組織内の相互牽制^{けんせい}の仕組みで、データのインテグリティが確保できる体制はどれか。

- ア 業務ニーズにそった効率の良いデータ入力システムを実現するため、情報システム部門がデータ入力システムを開発してデータ入力する。
- イ 情報システム部門の担当者は、その経験を生かし、システム開発においてデータの整合性が保てるように、長期間、同一部署に配置する。
- ウ 情報システム部門の要員が他部門に異動する場合は、関連する資料をもたせ、システムトラブルなどの緊急時に戦力となるようにする。
- エ 情報システム部門は、データを入力する利用部門からの独立を保ち、利用部門がデータの正確性を維持できるようにする。

解答と解説

問1

(平成28年春 情報セキュリティマネジメント試験 午前 問37)

《解答》イ

スプレッドシートの利用に係るコントロール(統制)に関しては、スプレッドシート統制として、金融商品取引法で企業に要求される内部統制として定められています。具体的な基準は、経済産業省の「システム管理基準 追補版(財務報告に係るIT統制ガイダンス)」として公開されています。

<http://www.meti.go.jp/policy/netsecurity/docs/regulations/ITGovernanceGuideline.pdf>

この指針では、スプレッドシートに対するアクセス制御や検証、変更管理について定義されています。スプレッドシートに組み込まれたロジックを随時変更し上書き保存することは、不正が見逃されるリスクがあるので不適切であり、指摘事項に該当します。したがって、イが正解です。

アの正確性確認や、ウのアクセスコントロール、エのバックアップは適切な対処なので、指摘事項には該当しません。

問2

(平成28年秋 情報セキュリティマネジメント試験 午前 問39)

《解答》ア

事業継続計画(BCP:Business Continuity Planning)は、災害発生時に最小時間でITサービスを復旧させ、事業を継続させるための計画です。緊急時に迅速に連絡を行うためには緊急連絡先リストは不可欠なので、最新版に更新しておく必要があります。したがって、アが正解です。

イ 重要書類は災害時の紛失を想定して、遠隔地に複製を管理しておく必要があります。

ウ 緊急時には、優先度に応じて対応の優先順位を決める必要があります。

エ BCPは普段から公開し、従業員に周知徹底しておく必要があります。

問3

(平成28年春 情報セキュリティマネジメント試験 午前 問3)

《解答》イ

情報セキュリティの整備、運用状況などについて、独立かつ専門的な立場の人が検証、評価し、保証又は助言を与えるものは、情報セキュリティ監査です。したがって、イが正解です。

ア 実際に運用している人自身が、その有効性について評価・分析を行う手法です。

ウ 組織の情報セキュリティ対策自己診断テストで、IPAセキュリティセンターが公開しています(<http://www.ipa.go.jp/security/benchmark/>)。

- エ 犯罪捜査や法的紛争などのために、コンピュータなどのデジタル記録を収集・分析し、法的な証拠とするものです。

問4

(平成28年春 情報セキュリティマネジメント試験 午前 問38)

《解答》ア

“情報セキュリティ管理基準”(平成28年改正版)の「7.3 雇用の終了又は変更」に、「雇用終了以降の一定期間継続する、秘密保持契約及び雇用条件に規定された責任」との記述があります。雇用の終了をもって守秘義務が解消されるわけではないので、アは指摘事項に該当します。

イ、ウ、エは情報セキュリティ管理基準に基づいた適切な雇用契約なので、指摘事項には該当しません。

5

問5

(平成28年春 情報セキュリティマネジメント試験 午前 問39)

《解答》ア

経済産業省が公表している“情報セキュリティ監査基準 実施基準ガイドライン”には、『情報セキュリティ管理基準』は、情報資産を保護するため』という記述があります。また、情報資産とは、財務情報、人事情報、顧客情報、技術情報などの目に見えない資産です。そのため、コンピュータだけでなく、紙や人の記憶なども含まれるので、コンピュータを導入していない部署でも監査を実施する必要があります。

したがって、アのように、監査の対象は「情報資産」、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可否は「必要」となります。

問6

(平成28年秋 情報セキュリティマネジメント試験 午前 問40)

《解答》ウ

“情報セキュリティ監査基準”は、情報セキュリティ監査人のための行動規範です。具体的な判断の尺度には、原則として“情報セキュリティ管理基準”を用います。したがって、ウが正解です。

ア “情報セキュリティ管理基準”は、ISO/IEC 27001などの国際規格を基に策定されています。

イ 監査人が必要と認めた場合には、他の専門家の支援を仰ぐことを考慮すべきであると定められています。

エ 監査対象から独立していなければならないと規定されています。

問7

(平成28年秋 情報セキュリティマネジメント試験 午前 問38)

《解答》ウ

証拠を収集し保全する技法には、デジタルフォレンジックスがあり、ログを法的な証拠として保全します。インシデントの調査やシステム監査にも利用できるもので、ウが正解です。

ア 緊急時対応計画のことで、災害発生時などに活用します。

イ 監査技法の一つである統計的サンプリング法で使われる、母集団からサンプルを抽出する手法です。

エ 経営を抜本的に改革するために、同じ分野の優良事例などとパフォーマンスを比較・分析し、自社の問題点を明確にして変革を実現する方法です。

問8

(平成28年秋 情報セキュリティマネジメント試験 午前 問37)

《解答》エ

JIS Q 27001では、「9.2 内部監査」のc)に、「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」とあります。したがって、エが正解です。

ア ISMS認証を行う外部監査では必要ですが、内部監査では不要です。

イ 任命についての規定はありませんが、監査結果を管理層に報告する必要はあります。

ウ ISMSに適合しているかなど、管理策以外にも監査範囲です。

問9

(平成22年春 基本情報技術者試験 午前 問60)

《解答》エ

相互牽制とは、複数の人間が互いにチェックしあう仕組みで、複数の部門で独立して、データのインテグリティを確保します。情報システム部門だけでなく、独立した利用部門がデータの正確性を確認することは、データのインテグリティを確保する相互牽制として有効です。したがって、エが正解となります。

その他の選択肢は情報システム部のみの体制となっており、他からのチェックが働かないので、適切ではありません。

5-2 サービスマネジメント

ITのサービスマネジメントは、システムの運用や保守などをITサービスとしてとらえて体系化し、これを効果的に提供するための統合されたプロセスアプローチです。

5-2-1 サービスマネジメント

サービスマネジメントでは、サービスをただ実施するだけでなく、顧客にとっての価値を創造することが重要です。

■ サービスマネジメントの目的と考え方

ITILではサービスマネジメントを「顧客に対し、サービスの形で価値を提供する組織の専門能力の集まり」と定義しています。

システムの運用や保守などをITサービスとしてとらえて体系化し、適切なサービス品質で、サービス価値を提供します。また、顧客満足度を考え、サービス提供者だけでなく、ユーザの順守事項も決定します。

■ サービスマネジメント構築手法

ITサービスマネジメントでは、計画(Plan)、実行(Do)、点検(Check)、処置(Act)のPDCAマネジメントサイクルによってサービスマネジメントの目的を達成します。そのために、ITサービス全体をマネジメントする仕組みとして**ITSMS** (IT Service Management System : ITサービスマネジメントシステム)を構築します。

ITサービスマネジメントシステムの構築手法には以下のものがあります。

①ベンチマーキング

業務やプロセスのベストプラクティスを探し出して分析し、それを指標(ベンチマーク)にして現状の業務のやり方を評価し、変革に役立てる手法です。現状とベストプラクティスの差異を分析することを**ギャップ分析**といいます。



勉強のコツ

ITILのマネジメント手法を中心に、システム運用管理手法全般についての方法論を押さえておきましょう。知識としては、ITILのサービスマネジメントプロセスのそれぞれの管理について出題されますので、一度しっかりそれぞれのプロセスを押さえておくことで確実です。

②リスクアセスメント

ITサービスにかかわるリスクを洗い出し、リスクの大きさや、許容できるリスクかどうかということと、対策の優先順位などを評価します。

③CSFとKPIの定義

ITサービスマネジメントが成功したかどうかを、あいまいにせず確実に評価するため、**CSF** (Critical Success factor：重要成功要因)を定義します。そして、そのCSFが実現できたかどうかを確認する指標として、**KPI** (Key Performance Indicator：重要業績評価指標)を設定します。

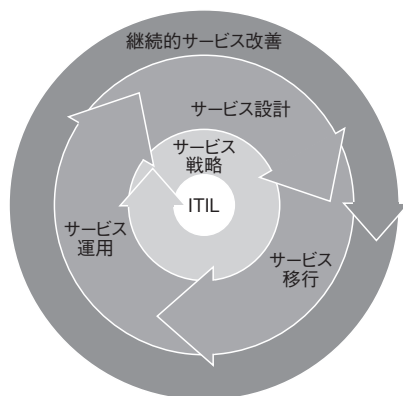
■ITIL

ITIL (Information Technology Infrastructure Library) は、ITサービスマネジメントのベストプラクティスをまとめたフレームワークで、現在、デファクトスタンダードとして世界中で活用されています。ITILを基にした規格が**JIS Q 20000** (ISO/IEC 20000)です。JIS Q 20000は、ITSMSの構築にあたって適用する運用管理手順でもあります。ITILがベストプラクティスとして、「このようにすればよい」という手法を示すのに対して、JIS Q 20000は**ITSMS適合性評価制度**として、ITSMSが適切に運用されていることを認定するために使用します。

ITILでは、サービスライフサイクルからサービスマネジメントにアプローチしています。サービスライフサイクルは、サービスマネジメントの構造や、様々なライフサイクル要素の関連などについての組織モデルです。サービスライフサイクルには5段階あり、それぞれの関係は、次のようになっています。

1. サービス戦略 ITサービスの指針を定義する段階
2. サービス設計 適切なITサービスを設計及び開発する段階
3. サービス移行 サービスの実現を計画立案及び管理する段階
4. サービス運用 サービスの提供とサポートに必要な活動をする段階

5. 継続的サービス改善 …… IT サービスの有効性と効率性を 継続的に改善する段階



ITILにおけるサービスライフサイクル

SLA

SLA (Service Level Agreement：サービスレベル合意)とは、サービスの提供者と委託者との間で、提供するサービスの内容と範囲、品質に対する要求事項を明確にし、さらにそれが達成できなかった場合のルールも含めて合意しておくことです。サービス時間、応答時間、サービス及びプロセスのパフォーマンスなどの目標を設定します。

要求事項を明文化した文書や契約書もSLAと呼ばれ、ITILでは、サービス設計のサービスレベル管理プロセスで文書化されます。サービスレベルを管理することを、SLM (Service Level Management：サービスレベル管理)といいます。



関連

SLMについては、[5-2-3 サービスマネジメントプロセス]で詳しく説明します。

覚えよう！

- ☐ ITILはベストプラクティス、JIS Q 20000は評価の基準
- ☐ SLAは、サービスの提供者と委託者の間であらかじめ合意すること

5-2-2 サービスの設計・移行

サービスの設計では、適切なITサービスを設計し開発します。サービスの移行では、新規サービスやサービスの変更を行います。

サービスの設計

サービスの設計は、経営戦略で定められた事業のニーズを満たすために行われます。SLAなどで定められた、具体的な数値を満たすために必要なサービスの設計を行います。ITILのサービス設計に関するプロセスには、サービスカタログ管理、サービスレベル管理、キャパシティ管理、可用性管理、ITサービス継続性管理、情報セキュリティ管理、供給者管理があります。

サービスの移行

サービスを移行するためには、新しいシステムの稼働環境を用意し、導入・移行を行う必要があります。ITILのサービス移行に関するプロセスには、移行の計画立案及びサポート、変更管理、サービス資産管理及び構成管理、リリース管理及び展開管理、サービスの妥当性確認及びテスト、評価、サービスナレッジ管理があります。システムを稼働環境に導入するためには、資産の引継ぎ、稼働環境の準備、実施計画の作成などが必要です。また、導入時にはシステム移行テストを行う必要があり、システム移行テスト計画を作成し、旧サービスから新サービスへの移行に関するテストを実施します。

システムの移行方式

システムの移行方式には、全システムを一度に移行する**単純移行方式**や、特定の一部(パイロットシステム)だけを先行して移行する**パイロット移行方式**、新旧環境での並行運用を行う**並行運用移行方式**などがあります。システムの移行時には、問題発生時に元に戻せることが大切です。

覚えてよう！

- ☐ サービスの移行時には、運用テストなどのテストが必要
- ☐ パイロット移行方式では、限定した部分で先行して移行する

5-2-3 ■ サービスマネジメントプロセス

サービスマネジメントプロセスは、JIS Q 20000では、サービス提供プロセス、関係プロセス、解決プロセス、統合的制御プロセスの四つに分類できます。各プロセスにはそれぞれ必要な管理が定められています。ここではそのポイントを示します。

■ サービス提供プロセス

サービスを提供するときに利用されるプロセスです。次の六つの管理を行います。

① サービスレベル管理

サービスレベル管理 (SLM : Service Level Management) の最終目標は、現在のすべてのITサービスに対して合意されたレベルを達成すること、そして将来のサービスが、合意された達成可能なサービス目標を満たすように提供されることです。提供しているITサービスのリストである**サービスカタログ**を提示します。

SLMでは、サービスの利用者とサービスの提供者との間でSLAを締結し、PDCAマネジメントサイクルでレビューを行い、サービスの維持、向上を図ります。

② サービスの報告

効果的なコミュニケーションを促進し、十分な情報に基づいて意思決定を行うために、適時に信頼できる報告書を作成します。サービス目標に対するパフォーマンスや、傾向情報をまとめます。

③ サービス継続及び可用性管理

サービス継続及び可用性管理では、ITサービスの継続性と可用性の両方を管理します。顧客と合意したサービス継続をあらゆる状況の下で満たすことを確実にするための活動がITサービス継続性管理です。サービス継続に関する要求事項は、事業計画やSLA、リスクアセスメントに基づいて決定します。ITサービス継続性管理では、災害のインパクトを定量化するためにビ

ビジネスインパクト分析 (BIA: Business Impact Analysis) や、サービス継続性に関するリスク分析 (RA: Risk Analysis) を行います。

また、災害発生時に最小時間でITサービスを復旧させ、事業を継続させるために**事業継続計画 (BCP: Business Continuity Planning)**を策定し、事業継続管理 (BCM: Business Continuity Management) を実施します。

すべてのサービスで提供されるサービス可用性のレベルが、費用対効果に優れた方法であり、合意されたビジネスニーズに合致するように実行するためのプロセスがサービス可用性管理です。可用性管理は、次の四つの側面をモニタ、測定、分析、報告します。

●サービス可用性管理の四つの観点

- **可用性** …………… 必要なときに合意された機能を実行する能力
- **信頼性** …………… 合意された機能を中断なしに実行する能力
- **保守性** …………… 障害の後、迅速に通常の稼働状態に戻す能力
- **サービス性** …… 外部プロバイダが契約条件を満たす能力

④サービスの予算業務及び会計業務

サービス提供にかかる費用を計画・管理する予算業務を行います。ITサービスのコストを明確にし、事業を行う者がその内容を確実に理解するようにします。サービスの内容を考慮した会計機能により、サービスに直接的に寄与するコストである直接費と、直接的には確認できない間接費を求めます。そして、サービスごとに必要なコストを算出し、基本的にはサービスの受益者 (利用者) が負担するように課金を行います。サービスを実施するコストだけでなく、ランニングコストなどの必要な経費を含めた総保有コストである**TCO (Total Cost of Ownership)**を意識することが大切です。

⑤キャパシティ管理

容量、能力などシステムのキャパシティを管理し、最適なコストで合意された需要を満たすために、サービス提供者が十分な能力を備えることを確実にする一連の活動がキャパシティ管理です。キャパシティ管理は最初にサービスの設計で扱われ、キャ

パシティ目標を設定します。サービスがSLAの目標値を満たすように、サービスをモニタし、パフォーマンスを測定します。具体的には、CPU使用率、メモリ使用率、ファイル使用量、ネットワーク利用率などを**管理指標**として測定し、それぞれのリソースのしきい値を設定します。

⑥情報セキュリティ管理

情報資産の機密性、完全性、可用性を保つように、情報セキュリティを管理します。**ISMS**を構築し、情報セキュリティマネジメントの規格に基づき、情報を適切に管理します。

■関係プロセス

サービス提供にかかわる、他の組織の関係者を適切に管理するためのプロセスです。次の二つの管理を行います。

①事業関係管理

サービス提供者と顧客との間の良好な関係を確立するための活動を行います。苦情の処理や顧客満足度の測定・分析・レビューなどを行います。

②供給者管理

サービス提供者が委託などにおいて、さらにサービスマネジメントプロセスの導入や移行のために供給者(サプライヤ)を用いる場合には、その供給者の管理が必要です。運用を委託する場合には、運用レベルを保証するために**OLA** (Operation Level Agreement: 運用レベル合意書)を作成し、契約を行います。

■解決プロセス

インシデントとは、中断・障害、損失、緊急事態、危機になり得るまたはそれらを引き起こし得る状況で、**問題**とは、その根本原因です。解決プロセスとは、インシデントと問題を適切に解決するためのプロセスです。次の二つの管理を行います。

①インシデント及びサービス要求管理

顧客へのサービスを迅速に回復し、提供を続けるために、イ

ンシデントへの対応、またはサービス要求への対応を行います。

インシデントが起こったときに、できる限り迅速に通常の状態を再開させるためのプロセスが**インシデント管理**です。インシデントとは、ITサービスの計画外の中断、品質の低下のことです。インシデントについてはまず記録、**識別（分類）**し、優先度付けを行います。インシデントが発生したときに早急に行われる、サービスへの影響を低減または除去する方法のことを、**回避策（ワークアラウンド）**といいます。また、重大なインシデントに発展する前段階である**ヒヤリハット**についても管理します。

②問題管理

一つまたは複数のインシデントの**根本原因**のことを問題といいます。その問題を突き止めて、登録し管理するのが**問題管理**です。問題管理では、根本原因を見つけて診断するために調査を行います。根本原因を突き止めて対応することによって、インシデントの再発を防止する予防処置を確立します。

■ 統合的制御プロセス

ITサービスや機器などの構成要素を明確にして管理するためのプロセスです。次の三つの管理を行います。

①構成管理

構成管理は、サービスや製品を構成するすべての**CI**（Configuration Item：構成品目）を識別し、維持管理することです。構成管理では、大規模で複雑なITサービスとインフラを管理するため、**CMS**（Configuration Management System：構成管理システム）を構築して一元管理します。CMSで使われるデータベースを**構成管理データベース**（**CMDB**：Configuration Management Database）といい、プロジェクト情報やツール、イベントなど様々な情報を一元管理します。

また、ソフトウェアなどの**資産管理**も行う必要があります。ソフトウェアのライセンス証書などのエビデンスを保管し、法的に問題なく、かつムダのないように余分な資産を除去し、ライセンス管理を行います。

②変更管理

変更管理は、サービスやコンポーネント、文書の変更を安全かつ効率的に行うための管理です。事業部やIT部門などからの **RFC** (Request for Change: 変更要求) を受け取り、対応します。すべての変更はもれなくCMDBに記録し、反映させる必要があります。

ITサービスに変更を加える要因には、単純なオペレーションだけでなく事業戦略やビジネスプロセスの変更など、様々なものがあります。そのため、顧客やユーザ、開発者、システム管理者、サービスデスクなどの様々な立場の利害関係者が定期的に集まり、変更をアセスメントする **CAB** (Change Advisory Board: **変更諮問委員会**) が開かれます。

③リリース及び展開管理

変更管理プロセスで承認された変更内容を、ITサービスの本番環境に正しく反映させる作業(リリース作業)を行うのがリリース管理及び展開管理です。リリース管理では、本番環境にリリースした確定版のすべてのソフトウェアのソースコードや手順書、マニュアルなどのCI(構成品目)を1か所にまとめて管理します。まとめておく書庫のことを **DML** (Definitive Media Library: 確定版メディアライブラリ) といいます。

覚 え よ う !

- ☐ インシデント管理はとりえず復旧、問題管理で根本的原因を解明
- ☐ 変更管理では、RFCを作成し、それをCABで検討する

5-2-4 サービスの運用

サービスの運用では、システム運用管理者の役割が重要になってきます。通常時の運用と障害時の運用の両方を考える必要があります。

システム運用管理者の役割

システム運用管理者の役割は、業務を行うユーザに対してITサービスを提供し、業務に役立ててもらうことです。従来は依頼があったときに対応するリアクティブ(受動的)な運用が主でしたが、最近は自発的に貢献する**プロアクティブ**(能動的)な取り組みが推奨されます。

システム運用管理者が運用以外の業務にもプロアクティブに関わっていくことで、より良いITサービスを提供できるようになります。

サービスの運用

サービスの運用では、システムの運用管理を行います。運用オペレーションでは、システムの監視や操作、状況連絡を行い、作業指示書や操作ログを記録します。

スケジュール設計

通常時の運用では、日次処理、週次処理、月次処理など、段階別に運用内容を決定しておく必要があります。運用ジョブに対しても、プロジェクトマネジメントの場合と同様に、先行ジョブとの関連を考え、ジョブネットワーク(ジョブのつながり方)を考慮してスケジュール設計を行います。

障害時運用設計

障害時には、待機系の切替え、データの回復などを行います。その手法はあらかじめ設計しておく必要があります。**BCP**(Business Continuity Planning: 事業継続計画)を策定し、**RTO**(Recovery Time Objective: 目標復旧時間)、**RPO**(Recovery Point Objective: リカバリポイント目標)を決めておきます。RPOとは、障害時にどの時点までのデータを復旧できるように

するかという目標です。

災害などによる致命的なシステム障害から情報システムを復旧させることや、そういった障害復旧に備えるための復旧措置のことを**ディザスタリカバリ** (災害復旧) と呼びます。

また、障害が起ると企業に重大な影響を及ぼすため、24時間365日常に稼働し続ける必要があるシステムを**ミッションクリティカルシステム**といいます。ミッションクリティカルシステムでは、システム障害が起こっても停止しないように待機系を複数用意するなど、万全の対策が求められます。

■ システム運用の評価項目

システムが運用要件を満たしているかどうかを定期的に評価することは重要です。様々な視点からの評価項目が設定されます。例として、次のようなものがあります。

- ・機能性評価指標 要求機能の実現度
- ・使用性評価指標 特定の利用の実現度
- ・性能指標 応答時間、処理時間
- ・資源の利用状況に関する指標 資源の利用状況
- ・信頼性評価指標 システム故障の頻度、
障害件数、回復時間、
稼働率

その他、安全性とセキュリティ、運用者の作業負担、利用者のシステム使用性なども評価項目として考えられます。

■ サービスデスク(ヘルプデスク)

サービスデスクとは、様々なサービスやイベントに関わるスタッフを擁する機能です。利用者にとっては、問題が起こったときに連絡する**単一窓口 (SPOC: Single Point Of Contact)** となり、利用者からの問合せに対応します。

サービスデスクで問合せの内容をすぐに解決できない場合には、**エスカレーション**を行います。

また、サービスデスクには次のように様々な形態があります。



用語

エスカレーションは、問合せに対応できないときにほかの担当者(通常は上位担当者)に連絡してその内容を引き継ぐことです。サービスデスクが受け付けたインシデントをほかのサポートグループに送ることを**機能的エスカレーション**、上位のITマネージャに連絡することを**階層的エスカレーション**といいます。

● サービスデスクの形態

・ ローカルサービスデスク

組織の拠点が複数箇所に分散している場合に、それぞれの拠点に要員を置き対応する

・ フォロー・ザ・サン

分散した二つ以上のサービスデスクを組み合わせ、24時間体制でサービスを提供する

・ 中央サービスデスク

中央で一括してサービスの提供を行う

・ バーチャルサービスデスク

サービスデスクが物理的に分散していても、サポートツールなどを利用することで、中央で集中して対応しているように見える

▶▶ 覚えよう！

- ☐ BCP（事業継続計画）では、RPO（リカバリポイント目標）やRTOを設定する
- ☐ サービスデスクは単一窓口（SPOC）で、他の部署にエスカレーションする

5-2-5 ■ ファシリティマネジメント

ファシリティマネジメントでは、経営の視点から業務用不動産を総合的にマネジメントします。

■ ファシリティマネジメント

ファシリティマネジメントとは、経営の視点から業務用不動産（土地や建物や設備など）を保有、運用し、維持するための総合的な管理手法です。単なる施設管理ではなく、施設を適切に使っていくためのあらゆるマネジメントを含みます。

■ 施設管理・設備管理

データセンタなどの施設や、コンピュータ、ネットワークなどの設備を管理し、コストの削減を図り、快適性、安全性などを確保します。

また、電源・空調設備などの管理を行います。停電時に数分間電力を供給し、システムを安定して停止させることができる **UPS** (Uninterruptible Power Supply：無停電電源装置) や、停電時に自力で電力を供給できるようにする **自家発電装置** などを利用した電源管理を行います。さらに、PCなどにワイヤを取り付ける **セキュリティワイヤ** の利用などにより、物理的なセキュリティを確保します。

■ 環境側面

環境側面では、地球環境に配慮したIT製品やIT基盤、環境保護や資源の有効活用につながるIT利用を推進することが大切です。この思想のことを **グリーンIT** といいます。

▶▶ 覚えよう！

- ☐ ファシリティマネジメントでは設備を管理する
- ☐ 停電時はUPSで数分間電力を提供し、その後は自家発電装置が必要

5-2-6 演習問題

問1 SLA

CHECK ▶ ☐☐☐

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

問2 事業継続計画の復旧時間

CHECK ▶ ☐☐☐

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3 事業継続計画のリスク対応

CHECK ▶ ☐☐☐

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4 インシデントに該当するもの

CHECK ▶ ☐☐☐

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

5

問5 システムの移行テストを実施する目的

CHECK ▶ ☐☐☐

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6 過電圧被害への対応

CHECK ▶ ☐☐☐

落雷によって発生する過電圧の被害から情報システムを守るための手段として、有効なものはどれか。

ア サージ保護デバイス (SPD) を介して通信ケーブルとコンピュータを接続する。

イ 自家発電装置を設置する。

ウ 通信線を経路の異なる2系統とする。

エ 電源設備の制御回路をデジタル化する。

■ 解答と解説**問1**

(平成28年春 情報セキュリティマネジメント試験 午前 問40)

《解答》 **ア**

SLA (Service Level Agreement : サービスレベル合意) とは、サービス提供者が顧客に対して、どの程度のレベルのサービスが提供できるかという合意です。サービス及びサービス目標を特定した合意事項なので、**ア**が正解です。

イはサービス料金などの明示事項、ウは内部グループの合意、エはITサービスの要件に関する内容です。

問2

(平成28年春 情報セキュリティマネジメント試験 午前 問41)

《解答》 **エ**

事業継続計画で用いられる用語で、インシデントの発生後、復旧までにかかる時間のことをRTO (Recovery Time Objective : 目標復旧時間) といいます。したがって、**エ**が正解です。

アは平均故障間隔、**イ**は平均修理時間のことで、稼働率の計算に用いられます。**ウ**は目標復旧地点 (Recovery Point Objective) のことで、インシデントで損壊・消失したデータをどの時点まで復旧させる必要があるのかを示す指標です。

問3

(平成28年春 情報セキュリティマネジメント試験 午前 問49)

《解答》 **イ**

事業継続計画の策定においては、緊急時の資源配分が大切です。そのため、リスクに優先度をつけ、許容できる損失を超えるものから優先的に対処することが必要となります。したがって、**イ**が正解です。

ア、**ウ**のように全てのリスクに対応することや、**エ**のように優先度に差をつけずに検討することは、限られた資源で事業継続を行うという観点から、適切ではありません。

問4

(平成28年秋 情報セキュリティマネジメント試験 午前 問42)

《解答》ウ

インシデントとは、中断・阻害、損失、緊急事態、危機になり得る、またはそれらを引き起こし得る状況です。プログラムの異常終了は、システムの中断を引き起こす状況なので、インシデントに該当します。したがって、ウが正解です。

ア インシデントの検知に該当します。

イ 問題(インシデントの根本原因)に該当します。

エ インシデント対応に該当します。

問5

(平成28年秋 情報セキュリティマネジメント試験 午前 問41)

《解答》ア

5

システムの移行テストとは、既存システムから新システムへの移行を行うためのテストです。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ので、アが正解です。

イ システムテストなどで行う性能テストの目的です。

ウ 結合テストを実施する目的です。

エ 単体テスト(ソフトウェアテスト)を実施する目的です。

問6

(平成25年春 基本情報技術者試験 午前 問56)

《解答》ア

落雷によって発生する過電圧(サージ)の被害から情報システムを守るためには、サージ防護デバイス(Surge Protective Device : SPD)を設置することが有効です。したがって、アが正解です。

イ 停電の対策です。

ウ 通信経路の信頼性向上の対策です。

エ 電源設備の小型化・高効率化を目的とした手段です。

5-3 プロジェクトマネジメント

プロジェクトマネジメントでは、毎回異なるプロジェクトを無事完了させるために、プロジェクトマネージャが様々な行動を行う必要があります。そのときに活用できる方法論がPMBOKにまとめられています。



勉強のコツ

プロジェクトマネジメントのベストプラクティス集であるPMBOKには、実際の現場での経験則が詰まっています。そのため、プロジェクトのチームで働いた経験があれば、理解しやすい分野です。

PMBOKに出てくる様々なプロジェクトマネジメントの手法についての知識が主な出題ポイントなので、用語を中心に理解しておきましょう。

動画

プロジェクトマネジメント分野についての動画を以下で公開しています。

<http://www.wakuwakuacademy.net/itcommon/5>
プロジェクトマネジメントの考え方やリスクマネジメントなどについて詳しく解説しています。

本書の補足として、よろしければご利用ください。

5-3-1 プロジェクトマネジメント

プロジェクトマネジメントでは、プロジェクトの目標を達成するために、計画し(Plan)、計画どおりに作業を進め(Do)、計画と実績の差異を検証し(Check)、差異の原因に対する処置を行う(Act)、PDCAマネジメントサイクルで管理します。

■ プロジェクトとは

プロジェクトとは、**目標達成のために行う有期の活動**です。つまり、定常的な業務と異なり、そのプロジェクトならではの独自性をもち、ゴールがあります。そして、明確な始まりと終わりがあることもプロジェクトの特徴です。プロジェクトが終わりになるのは、プロジェクト目標が**達成**されたときか、プロジェクトが**中止**されたときです。

■ プロジェクトマネジメント

プロジェクトマネジメントとは、プロジェクトの要求事項を満たすため、知識、スキル、ツール及び技法をプロジェクト活動に適用することです。具体的には、**テーラリング**(プロジェクトの設計)を実施し、プロジェクトの環境を考慮してプロジェクトの体制を決定し、プロセスごとに適切なツールや技法を決めます。

プロジェクトでは、**ステークホルダ**(利害関係者)のニーズと期待に応えつつ、競合する要求のバランスをとります。また、プロジェクトの進行中には、変更管理、問題発見、問題報告、対策立案、文書化といった自己管理も行う必要があります。

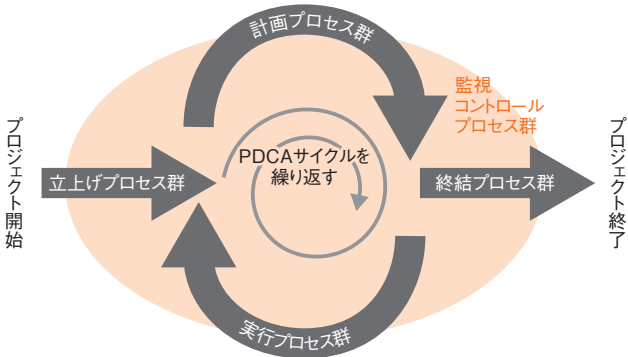
PMBOK

プロジェクトマネジメントの専門家が、「実務でこうすればプロジェクト成功の可能性が高くなる」という方法論やスキルなどを集めて作成された標準が**PMBOK** (Project Management Body of Knowledge：プロジェクトマネジメント知識体系)です。PMBOKでは、次のような五つのプロセス群が定義されています。

プロジェクトマネジメントの五つのプロセス群

プロセス群	内容
立上げプロセス群	プロジェクトの認可を得て、新しいフェーズを明確に定める
計画プロセス群	プロジェクトのスコップを定義し、目標を洗練し、一連の行動を規定する
実行プロセス群	プロジェクトの作業を実行する
監視コントロール・プロセス群	プロジェクトの進捗やパフォーマンスを追跡し、統制し、変更を開始する
終結プロセス群	プロジェクトを公式に完結し、すべてのアクティビティを終了する

各プロセス群は次のような相互関係にあります。



各プロセス群の相互関係

プロジェクトマネジメントに必要な知識は、次の十の知識エリアに分けられます。



プロジェクトマネジメントを行うためには、プロジェクトマネジメントの知識以外にも必要とされる知識がたくさんあります。人間関係のスキルやマネジメント分野の知識などはその代表例です。PMBOKは、それらの知識は必要であるという前提で、プロジェクトマネジメントに関する**知識だけ**がまとめられたものです。

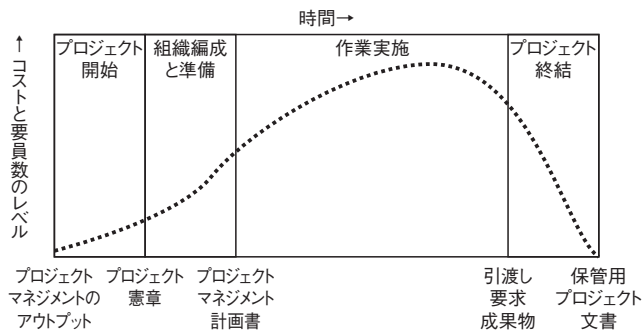
- 1. プロジェクト統合マネジメント
- 2. プロジェクトステークホルダマネジメント
- 3. プロジェクトスコープマネジメント
- 4. プロジェクト資源マネジメント
- 5. プロジェクトタイムマネジメント
- 6. プロジェクトコストマネジメント
- 7. プロジェクトリスクマネジメント
- 8. プロジェクト品質マネジメント
- 9. プロジェクト調達マネジメント
- 10. プロジェクトコミュニケーションマネジメント

以上の知識エリアについては、次項以降で詳しく見ていきます。

■プロジェクトライフサイクル

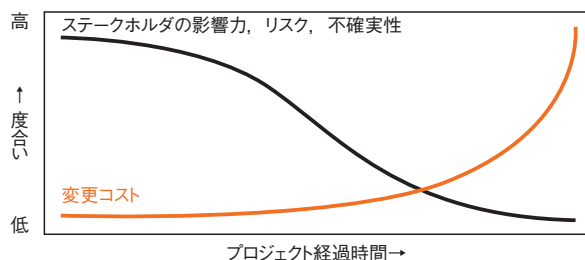
プロジェクトライフサイクルとは、プロジェクトのフェーズの集合です。プロジェクトの規模や複雑さは様々ですが、ライフサイクルはプロジェクト開始、組織編成と準備、作業実施、プロジェクト終結の4段階で表現することができます。

プロジェクトライフサイクルにおける典型的なコストと要員数は、プロジェクト開始時に少なく、作業を実行するにつれて頂点に達し、プロジェクトが終了に近づくときと急激に落ち込む、次の図のように推移します。



プロジェクトライフサイクルにおけるコストと要員数の推移

また、ステークホルダの影響力、リスク、不確実性は、プロジェクト開始時に最大であり、プロジェクトが進むにつれて徐々に低下します。変更コストは、プロジェクトが終了に近づくにつれて図のように大幅に増加していきます。



ステークホルダの関わり方と変更コストの推移

▶▶ 覚えよう！

- ☐ プロジェクトは目標を達成するために実施する有期の活動
- ☐ プロジェクトの必要人員は、作業実施時が最も多い

5-3-2 ■ プロジェクト統合マネジメント

プロジェクト統合マネジメントでは、プロジェクトマネジメント活動の各エリアを統合的に管理、調整します。

■ プロジェクト統合マネジメントのプロセス

プロジェクト統合マネジメントでは、プロジェクト全体像の把握と管理を行い、プロジェクトの定義や統一、調整など、必要なプロセスを実施します。個々のプロセスは相互に関係しているので、その中で競合する目標と代替案などのトレードオフを行い、相互依存関係のマネジメントを実施します。

プロジェクト統合マネジメントのプロセスには、プロジェクト憲章作成、プロジェクトマネジメント計画書作成、プロジェクト実行の指揮・マネジメント、プロジェクト作業の監視・コントロール、統合変更管理、プロジェクトやフェーズの終結があります。



トレードオフとは、一方を追求すれば他方を犠牲にせざるを得ないという状態または関係です。プロジェクトマネジメントでは、このようなトレードオフを調整することが求められます。

■ プロジェクト憲章

プロジェクト憲章は、プロジェクトやフェーズを公式に認可する文書です。立上げプロセス群の中で実行される、ステークホルダのニーズと期待を満足させる初期の要求事項を文書化するプロセスが、プロジェクト憲章作成です。

プロジェクト憲章には、以下のような内容が記述されます。

- ・プロジェクトの目的や妥当性
- ・測定可能なプロジェクト目標とその成功基準
- ・予算、スケジュールなどの概要

■ プロジェクトやフェーズの終結

プロジェクトやフェーズを公式に終了するためにすべてのプロジェクトマネジメントプロセス群のすべてのアクティビティを完結するプロセスが、プロジェクトやフェーズの終結です。プロジェクトマネージャは、すべての作業が完了し、その目標を達成したことを確認します。

▶▶ 覚えよう！

- プロジェクト憲章でプロジェクトは正式に認可される

5-3-3 ■ プロジェクトステークホルダ マネジメント

プロジェクトステークホルダマネジメントでは、プロジェクトに影響を受けるか、あるいは影響を及ぼす個人、グループまたは組織を明らかにします。

■ ステークホルダ

ステークホルダとは、プロジェクトに積極的に関与しているか、またはプロジェクトの実行や完了によって利益にプラスまたはマイナスの影響を受ける個人や組織です。具体的には、顧客やユーザ、スポンサー、プロジェクトチームのメンバ、メンバが所属する組織、商品の納入を行う業者などです。

■ プロジェクトステークホルダマネジメントのプロセス

プロジェクトステークホルダマネジメントに含まれるプロセスには、ステークホルダマネジメント計画、ステークホルダエンゲージメントマネジメント、ステークホルダエンゲージメントコントロールがあります。エンゲージメントとは、ステークホルダの関係や関わりの度合いを、強すぎもせず弱すぎもしない適切なものとするような活動です。

■ ステークホルダ登録簿

ステークホルダを適切に管理するため、ステークホルダの利害や環境に関する情報を文書化します。**ステークホルダ登録簿**を作成し、ステークホルダの氏名や評価情報などを記載します。



PMBOKでは、従来はプロジェクトコミュニケーションマネジメントの一部としてステークホルダマネジメントを定義していました。しかし、ステークホルダマネジメント活動はプロジェクトを円滑に進める上で非常に重要であるという判断から、最新版のPMBOK 第5版では、新たに独立した知識エリアとして定義されました。

|| ▶▶ 覚えよう！

- ☐ ステークホルダには、顧客やメンバ、関係組織など、様々な人がいて、利害関係が対立する
- ☐ ステークホルダとプロジェクトとの関係が適度な距離になるよう管理する

5-3-4 ■ 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は、プロジェクトに必要な作業を過不足なく含めることを目的に行われます。

■ プロジェクトスコープ

プロジェクトスコープとは、プロジェクトの範囲であり、必要なプロダクトやサービスを生み出すために行わなければならない作業です。プロジェクトスコープマネジメントでは、計画された作業の基準値であるベースラインを決め、それを実績と比較することによって、プロジェクトが順調かどうかを判断します。

■ プロジェクトスコープマネジメントのプロセス

プロジェクトスコープマネジメントに含まれるプロセスには、スコープマネジメント計画、要求事項収集、スコープ定義、WBS作成、スコープ妥当性確認、スコープコントロールがあります。

■ プロジェクトスコープ記述書

プロジェクトスコープマネジメントでは、スコープ定義において、専門家の判断やプロダクト分析、ワークショップなどの結果を参考にしながらスコープを定義します。定義したスコープは、プロジェクトスコープ記述書に、プロジェクトの要求成果物、成果物受入れ基準、プロジェクトからの除外事項などの項目を含めて記述します。

■ スコープコントロール

プロジェクトスコープマネジメントでは、プロジェクトスコープに従って、スコープの変更や、予定と異なるスコープになることを最小限に押さえるためにコントロールする必要があります。プロジェクトのスコープは、時間の経過とともに拡大していく傾向があり、そうなった状態を**スコープクリープ**といいます。スコープクリープが起こればプロジェクトの成功が危うくなるため、プロジェクトマネージャは、起こらないようにしっかりスコープコントロールを行う必要があります。

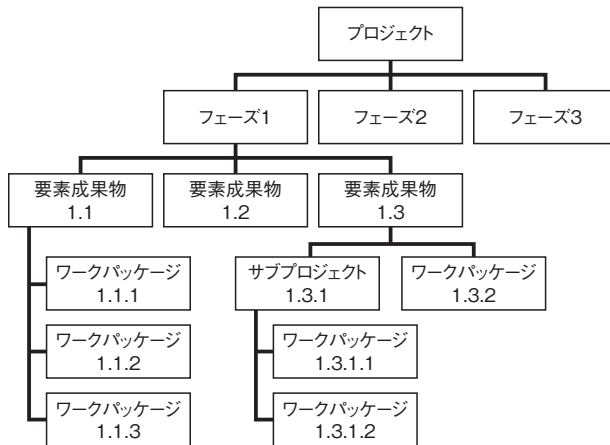
■ WBS

WBS (Work Breakdown Structure)は、成果物を中心に、プロジェクトチームが実行する作業を階層的に要素分解したものです。WBSを使うと、プロジェクトのスコープ全体を系統立ててまとめて定義することができます。

WBSでは、上位のWBSレベルから下位のWBSレベルへと、より詳細な構成要素に分解します。最も詳細に分解した最下位のWBSを**ワークパッケージ**といいます。ワークパッケージには、実際に行う作業である**アクティビティ**を割り当てます。

WBSの構造は、プロジェクトライフサイクルのフェーズを要素分解の第1レベルに置く方法、主要な成果物を第1レベルに置く方法、組織単位・契約単位で分ける方法などがあり、いろいろな形態で利用することができます。

WBSの構造は次の図のようになります。



WBSの構造

WBSは毎回一から作るのではなく、これまでのプロジェクトで作成されたWBSを参考にするすることで、より効率的にプロジェクトを運営できます。過去のプロジェクトの実績に基づき、典型的な作業の階層構造や作業項目をまとめたひな形を**WBSテンプレート**といいます。WBSテンプレートを作ることで、中長期的

にスケジュール作成の効率と精度を高めることができます。

■ WBS辞書

WBS辞書は、WBS作成プロセスにおいて生成する文書であり、WBSを補完します。各WBS要素に対応する作業の詳細な記述や、技術的な文書の詳細な記述を行います。

|| ▶▶ 覚えよう！

- ☐ スコープはプロジェクトに必要なものを過不足なく定義
- ☐ WBSの最下位の要素はワークパッケージ

5-3-5 ■ プロジェクト資源マネジメント

プロジェクト資源マネジメントは、プロジェクトチームのメンバーが各々の役割と責任を全うすることでチームとして機能し、プロジェクトの目標を達成することを目的に行われます。

■ プロジェクト資源マネジメントのプロセス

プロジェクト資源マネジメントのプロセスには、人的資源マネジメント計画作成、プロジェクトチーム編成、プロジェクトチーム育成、プロジェクトチームマネジメントがあります。

■ プロジェクト資源マネジメント

プロジェクト資源マネジメントでは、プロジェクトチームの管理を行います。プロジェクトチームの要員として、プロジェクトマネージャやプロジェクトメンバーを決定し、プロジェクトマネジメントチームで管理を行います。機器、備品、資材、ソフトウェア、ハードウェア、外部人材の管理なども行います。

■ PMO

PMO (Project Management Office : プロジェクトマネジメントオフィス)とは、組織の個々のプロジェクトマネジメントの支援を横断的に行う部門のことです。プロジェクト間の要員調整などを行います。

■ 教育技法

プロジェクトの人材育成では、知識中心ではなく、より実践的な教育技法が用いられます。代表的なものに、日常業務の中で先輩や上司が個別指導する **OJT** (On the Job Training) や、具体的な事例を取り上げて詳細に分析し、解決策を見出していく **ケーススタディ**、その応用で、制限時間内で多くの問題を処理させる **インバケット** などがあります。

▶▶ 覚えよう！

- ☐ PMOでは、個々のプロジェクトマネジメントの支援を横断的に行う
- ☐ インバケットは、一定時間に数多くの案件を処理する

5-3-6 ■ プロジェクトタイムマネジメント

プロジェクトタイムマネジメントでは、プロジェクトを所定の時期に完了させることを目的とします。プロジェクトだけでなく、プロジェクトに関わる要員それぞれの進捗管理も重要です。

■ プロジェクトタイムマネジメント

プロジェクトタイムマネジメントに含まれるプロセスには、スケジュールマネジメント計画、アクティビティ定義、アクティビティ順序設定、アクティビティ資源見積り、アクティビティ所要期間見積り、スケジュール作成、スケジュールコントロールがあります。

■ アクティビティ

プロジェクトのWBSで定義されたワークパッケージを、より小さく、よりマネジメントしやすい単位に要素分解したものが**アクティビティ**です。チームメンバーや専門家などと協力してアクティビティを分解し、必要なすべてのアクティビティを網羅した**アクティビティリスト**を作成します。そして、すべて**マイルストーン**を特定し、マイルストーンリストを作成します。さらに、アクティビティの順序関係をまとめ、プロジェクトのスケジュールを**アローダイアグラム**で表現します。

■ スケジュールの作成方法

アクティビティごとに、資源がいつどれだけ必要になるか、作業量や期間はどの程度かを見積もり、スケジュールを作成します。スケジュール作成の代表的な手法には以下のものがあります。



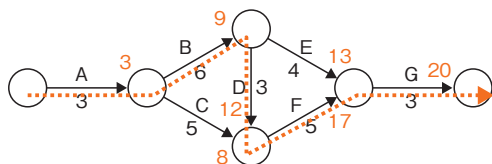
クリティカルパス法とよく似た手法に**PERT** (Program Evaluation and Review Technique) があります。PERTでは、三点見積りという、時間見積りを確率的に行う方法を用いて、全体スケジュールの所要期間を計算します。PMBOKでは、三点見積りはアクティビティ所要時間見積り手法として紹介されています。

① クリティカルパス法

アクティビティ（作業）の順序関係を表した**アローダイアグラム**から、プロジェクト完了までにかかる最長の経路である**クリティカルパス**を計算し、それを基準にそれぞれのアクティビティがプロジェクト完了を延期せずにいられる余裕がどれだけあるか(**トータルフロート**)を計算します。

具体的には、最初にスケジュール・ネットワークの経路の往

路時間計算(フォワードパス)を求め、作業期間の合計が最も大きい経路をクリティカルパスとし、その期間をプロジェクト全体の所要時間とします。そして、その所要時間から逆算して復路時間計算(バックワードパス)を行います。フォワードパスにより、すべてのアクティビティの最早開始日と最早終了日を、バックワードパスにより最遅開始日と最遅終了日を求めることができます。



アローダイアグラムの例(点線はクリティカルパス)

②クリティカルチェーン法

クリティカルパス法では、資源（人員など）に関する制限を考慮せずに計算していました。しかし実際には資源に限度があるので、その資源に合わせてクリティカルパスを修正する手法がクリティカルチェーン法です。

③スケジュール短縮手法

作成したスケジュールの予定が目標の期限に間に合わない場合にスケジュールを短縮させる方法に、クラッシングとファストトラッキングがあります。**クラッシング**とは、コストとスケジュールのトレードオフを分析し、最小の追加コストで最大の期間短縮を実現する手法を決定することです。**ファストトラッキング**は、順を追って実行するフェーズやアクティビティを並行して実行するというスケジュール短縮手法です。

■ スケジュールコントロール

スケジュールコントロールでは、プロジェクトの進捗を更新するためにプロジェクトの状況を監視し、スケジュールに対する変更をマネジメントします。スケジュール作成で行われたクリティカルパス法などの分析により、基本となるスケジュールであるス

ケジュールベースラインを決定します。それを基に差異分析を行い、スケジュールを調整します。

■ ガントチャート

ガントチャートは、作業の進捗状況を表す図です。プロジェクト管理などにおいて工程管理に用いられます。縦軸でWBSのそれぞれの要素を表し、横棒で実施される期間や実施状況を色分けなどして表します。ガントチャートは、次のような一種の棒グラフのかたちで示されます。

アクティビティ	開始	終了	1	2	3	4	5	6	7	8	9
要件定義	1月	1月									
概要設計	2月	3月									
詳細設計	4月	5月									
プログラミング	6月	8月									
テスト	7月	9月									

ガントチャートの例

覚 え よ う !

- ☐ クリティカルパスは日程に余裕のない経路
- ☐ ガントチャートは進捗管理に利用される図

5-3-7 プロジェクトコストマネジメント

プロジェクトコストマネジメントは、プロジェクトを決められた予算内で完了させることを目的に行われます。プロジェクトだけでなく、プロジェクトに関わる要員それぞれのコスト管理も重要です。

プロジェクトコストマネジメント

プロジェクトコストマネジメントでは、プロジェクトのそれぞれのアクティビティで見積もられたコストを集計し、パフォーマンスを測定するためのコストベースラインを決定します。様々な資源費用や要員の人件費なども考慮に入れる必要があります。

プロジェクトコストマネジメントのプロセス

プロジェクトコストマネジメントに含まれるプロセスには、コストマネジメント計画、コスト見積り、予算設定、コストコントロールがあります。

コスト見積手法

代表的なコスト見積手法には、次のものがあります。

① ファンクションポイント法 (FP法)

ソフトウェアの機能(ファンクション)を基本にして、その処理内容の複雑さからファンクションポイントを算出します。帳票、画面、ファイルなどのソフトウェアの機能を洗い出し、その数を見積もります。その後、機能を次の5種類のファンクションタイプに分け、それぞれの難易度を容易・普通・複雑の3段階で評価して点数化し、それを合計して基準値とします。

ファンクションの評価基準の例

ファンクション	ファンクションタイプ	容易	普通	複雑
トランザクション ファンクション	外部入力 (EI)	3	4	6
	外部出力 (EO)	4	5	7
	外部参照 (EQ)	3	4	6
データファンクション	内部論理ファイル (ILF)	7	10	15
	外部インタフェースファイル (EIF)	5	7	10

次に、システム特性に対してその複雑さを14の項目で0～5の6段階で評価し、それを合計して調整値を求めます。基準値と調整値を基に、以下の式でファンクションポイントを算出します。

$$\text{ファンクションポイント} = \text{基準値} \times (0.65 + \text{調整値} / 100)$$

ファンクションポイント法は、プログラミングに入る前にユーザ要件が決まり、必要な機能が見えてきた段階で見積りが行えるという特徴があります。

② LOC法

LOC (Lines Of Code) 法は、ソースコードの行数でプログラムの規模を見積もる方法です。オンライン系とバッチ系に分けて機能を洗い出します。従来からある方法ですが、担当者によって見積り規模に大きな偏差が出ることから、客観的に計算できるファンクションポイント法が普及してきました。

③ COCOMO

COCOMO (Constructive Cost Model) は、ソフトウェアで予想されるソースコードの行数に、エンジニアの能力や要求の信頼性などによる補正係数を掛け合わせ、開発に必要な工数、期間などを算出する手法です。現在は、ファンクションポイントなどの概念を取り入れて発展させたCOCOMO IIが提唱されています。

■ EVM

アーンドバリューマネジメント (EVM: Earned Value Management) は、予算とスケジュールの両方の観点からプロジェクトの遂行を定量的に評価するプロジェクトマネジメントの技法です。PMBOKでは、コストコントロールの技法として使われています。

アーンドバリューマネジメントでは、次の三つの値を用いて測定し、監視します。

① PV (Planned Value : 計画値)

遂行すべき作業に割り当てられた予算です。計画から求められます。

② EV (Earned Value : 出来高)

実施した作業の価値です。完了済の作業に対して当初割り当てられていた予算を算出します。

③ AC (Actual Cost : 実コスト)

実施した作業のために実際に発生したコストです。実測値から求められます。

これらの三つの値を使って、次のような差異や効率指数を計算することができます。

• SV (Schedule Variance : スケジュール差異)

$SV = EV - PV$ で、進捗の遅れをコストで表します。

SVが+ならスケジュールは進んでおり、-なら遅れています。

• CV (Cost Variance : コスト差異)

$CV = EV - AC$ で、コストの超過を表します。

CVが+ならコストは黒字、-なら赤字です。

• SPI (Schedule Performance Index : スケジュール効率指数)

$SPI = EV \div PV$ で、進捗状況を指数で表します。

$SPI > 1$ なら進んでおり、 $SPI < 1$ なら遅れています。

• CPI (Cost Performance Index : コスト効率指数)

$CPI = EV \div AC$ で、コストの効率を指数で表します。

$CPI > 1$ なら黒字、 $CPI < 1$ ならコスト超過です。

覚 え よ う !

- ☐ 帳票や画面など機能を基に見積もるファンクションポイント法
- ☐ EVMは進捗とコストの両方を定量的に評価する

5-3-8 ■ プロジェクトリスクマネジメント

プロジェクトリスクマネジメントでは、プロジェクトに関するリスクについてマネジメントの計画、特定、分析、対応、監視・コントロール等を実施します。

■ プロジェクトリスクマネジメントのプロセス

プロジェクトリスクマネジメントに含まれるプロセスには、リスクマネジメント計画、リスク特定、定性的リスク分析、定量的リスク分析、リスク対応計画、リスクコントロールがあります。

■ リスク特定

リスクとは、もしそれが発生すれば、プロジェクト目標に影響を与える不確実な事象あるいは状態のことです。常に将来において起こるものが対象になります。すでに起こっていて明らかなものは課題（または問題点）と呼ばれ、リスクとは区別して管理します。リスク特定では、可能性のあるリスクを洗い出します。

リスクの情報収集方法としては、参加者が自由にアイデアを出すブレインストーミングや、専門家の間でアンケートを使用して質問を繰り返すことで合意を形成するデルファイ法、根本原因分析などが挙げられます。

■ リスク分析

リスク分析では、リスクの発生確率とその影響度を策定し、プロジェクトへの影響を分析します。大まかにリスクの優先順位付けを行う定性的リスク分析と、リスクの影響を数量的に分析する定量的リスク分析があります。

■ リスク対応

リスク対応では、リスク分析の結果を基に、プロジェクト目標に対する好機を高め、脅威を減少させるための選択肢と方法を策定します。

●プラスのリスクもしくは好機に対する戦略

- ・活用 …… 好機が確実に到来するようにする
- ・共有 …… 能力の高い第三者に好機の実行権を与える
- ・強化 …… 好機の発生確率や影響力を増加させる
- ・受容 …… 特に何もしないが、実現したときには利益を享受する

●マイナスのリスクもしくは脅威に対する戦略

- ・回避 …… 脅威を完全に取り除くために、プロジェクトマネジメント計画を変更する
- ・転嫁 …… 脅威によるマイナスの影響や責任の一部または全部を第三者に移転する。保険、担保など
- ・軽減 …… リスク事象の発生確率や影響度を減少させる
- ・受容 …… 脅威に対して特別な対応をしないが状況に応じて次のような対策をとる
能動的な受容：脅威の発生に備えて時間や資金に予備を設けるなど
受動的な受容：何もせず起きたときに対応する



関連

リスク対応については、「2-2-4 情報セキュリティリスク対応」でも取り上げています。
プロジェクトのリスクと情報セキュリティリスクの一番の違いは、プロジェクトではプラスのリスクが考えられるのに対して、情報セキュリティではマイナスのリスク(脅威)しか考えられないことです。

▶▶ 覚えよう！

- ☐ リスクは、まだ起こっていないもの。起こったら課題
- ☐ リスクを第三者に移すのは転嫁、代替策は回避

5-3-9 プロジェクト品質マネジメント

プロジェクト品質マネジメントでは、プロジェクトのニーズを満足させることを目的とします。プロジェクトでは、必要に応じて行われる継続的プロセス改善活動とともに、方針、手順を通して品質マネジメントを実施します。

プロジェクト品質マネジメントのプロセス

プロジェクト品質マネジメントに含まれるプロセスには、品質マネジメント計画、品質保証、品質コントロールがあります。それぞれのプロセスでは、以下のことを行います。

①品質マネジメント計画(品質計画)

品質要求事項や品質標準を定め、プロジェクトでそれを順守するための方法を文書化します。

②品質保証

適切な品質標準と運用基準の適用を確実に行うために、品質の要求事項と品質管理測定の結果を監査します。

③品質コントロール(品質管理)

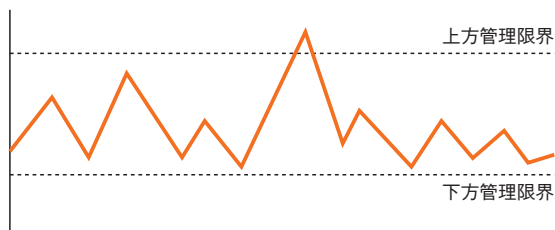
パフォーマンスを査定し、必要な変更を提案するために品質を監視するシステムなどの実行結果を監視し、記録します。QC七つ道具や新QC七つ道具などを駆使します。**障害報告書**などを作成し、障害が起こったという事実とその内容を管理します。

品質マネジメントの手法

代表的な品質マネジメントの手法には、以下のものがあります。

①管理図

管理図は、プロセスが安定しているかどうか、またはパフォーマンスが予測どおりであるかどうかを判断するための図です。許容される上方管理限界と下方管理限界を設定します。



管理図の例

②ベンチマーク

実施中または計画中のプロジェクトを類似性の高いプロジェクトと比べることによって、ベストプラクティスを特定したり、改善策を考えたり、測定基準を設けたりすることです。

③レビュー，テスト

ウォークスルー，インスペクションなどのレビューや，段階的なテストは，品質を向上させるための大切な手法です。

④品質の指標

JIS X 25010 (ISO/IEC 25010) で定められているソフトウェア品質特性の指標は，ソフトウェア開発時の品質の指標としてよく用いられます。

覚 え よ う !

- ☐ 品質保証は，品質を確実にするための体系的な活動
- ☐ 品質マネジメント計画では，手順を定めて文書化する

5-3-10 プロジェクト調達マネジメント

プロジェクト調達マネジメントの目的は、作業の実行に必要な資源やサービスを外部から購入、取得するために必要な契約やその管理を適切に行うことです。

プロジェクト調達マネジメントのプロセス

プロジェクト調達マネジメントのプロセスに含まれるものには、調達マネジメント計画、調達実行、調達コントロール、調達終結があります。外部資源の活用方法を考え、購入者、サプライヤを決定していきます。

それぞれのプロセスでは、以下のことを行います。

① 調達マネジメント計画

プロジェクト調達の意思決定を文書化し、取り組み方を明確にして、納入候補を特定します。

② 調達実行

納入候補から回答を得て、納入者（**サプライヤ**）を選定し、契約を締結します。

③ 調達コントロール

調達先との関係をマネジメントし、契約のパフォーマンスを監視して、必要に応じて変更と是正を行います。

④ 調達終結

プロジェクトにおける個々の調達を完結します。

覚 え よ う !

☐ 調達マネジメントでは、必要な資源やサービスを外部から取得する

5-3-11 ■ プロジェクトコミュニケーション マネジメント

プロジェクトコミュニケーションマネジメントは、プロジェクト情報の生成、収集、配布、保管、検索、最終的な廃棄を適宜、適切かつ確実に行うためのプロセスから構成されます。人と情報を結び付ける役割を果たすことが目的です。

■ プロジェクトコミュニケーションマネジメントのプロセス

プロジェクトコミュニケーションマネジメントのプロセスには、コミュニケーションマネジメント計画、コミュニケーションマネジメント、コミュニケーションコントロールがあります。コミュニケーションマネジメント計画書を作成し、ステークホルダのコミュニケーションに関するニーズに応えるための仕組みを構築します。

■ 情報配布の方法

情報配布の形態としては、相手の行動にかかわらず情報を提供する**プッシュ型**と、相手の行動に応じて情報を提供する**プル型**があります。また、相手の応答を受け取るフィードバック型もあります。

代表的な配布手段には、電子メールやボイスメール、テレビ会議や紙面などがあります。

▶▶ 覚えよう！

- ☐ 相手の行動に応じて情報を提供するのがプル型

5-3-12 演習問題

問1 ステークホルダ

CHECK ▶ ☐☐☐

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 組織の外部にすることはなく、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と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2 プロジェクトスコープマネジメント

CHECK ▶ ☐☐☐

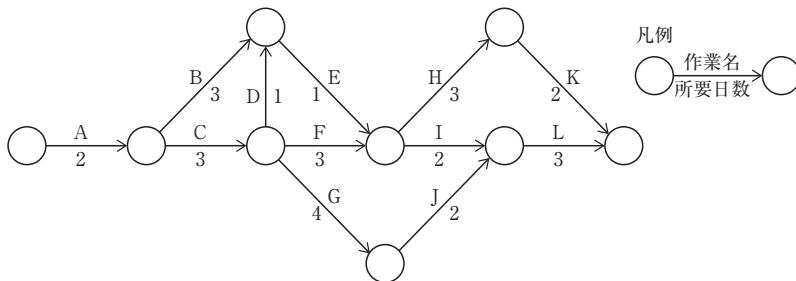
プロジェクトスコープマネジメントにおいて、WBS作成のプロセスで行うことはどれか。

- 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 成果物を生成するためのアクティビティを定義する。

問3 クリティカルパス

CHECK ▶ ☐☐☐

図に示すプロジェクト活動のクリティカルパスはどれか。



ア A → B → E → I → L

イ A → C → D → E → H → K

ウ A → C → F → I → L

エ A → C → G → J → L

問4 システム障害を表す図

CHECK ▶ ☐☐☐

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
ウ ポートフォリオ図

- イ 二重円グラフ
エ レーダチャート

問5 ファンクションポイント法

CHECK ▶ ☐☐☐

ある新規システムの開発規模を見積もったところ、500FP（ファンクションポイント）であった。このシステムを構築するプロジェクトには、開発工数の他にシステムの導入や開発者教育の工数が10人月必要である。また、プロジェクト管理に、開発と導入・教育を合わせた工数の10%を要する。このプロジェクトに要する全工数は何人月か。ここで、開発の生産性は1人月当たり10FPとする。

ア 51

イ 60

ウ 65

エ 66

問6 プロジェクトリスクマネジメント

CHECK ▶ ☐☐☐

PMBOKによれば、プロジェクトのリスクマネジメントにおいて、脅威に対して適用できる対応戦略と好機に対して適用できる対応戦略がある。脅威に対して適用できる対応戦略はどれか。

ア 活用

イ 強化

ウ 共有

エ 受容

■ 解答と解説**問1**

(平成28年秋 情報セキュリティマネジメント試験 午前 問44)

《解答》 **イ**

ステークホルダとは、プロジェクトに積極的に関与しているか、またはプロジェクトの実行や完了によって利益にプラスまたはマイナスの影響を受ける個人や組織です。プロジェクトの成果が利益(プラス)になる者だけでなく、不利益(マイナス)になる者も含まれるので、イが正解です。

- ア 組織の外部に属していることもあります。
- ウ 間接的な関与を行う者も含まれます。
- エ 個人として特定する必要はなく、組織や顧客なども含まれます。

問2

(平成27年春 基本情報技術者試験 午前 問53)

《解答》 **イ**

WBS (Work Breakdown Structure) は、成果物を中心に、プロジェクトチームが実行する作業を階層的に要素分解したものです。WBSを使うと、プロジェクトのスコープ全体を系統立ててまとめて定義することができます。したがって、イが正解です。

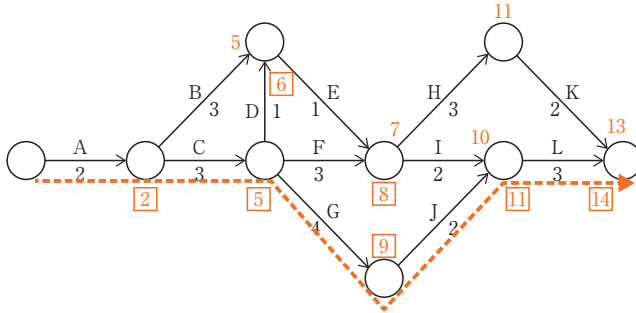
- ア プロジェクトコストマネジメントで行うコスト見積りです。
- ウ プロジェクトタイムマネジメントで行うスケジュール作成です。
- エ アクティビティは、プロジェクトのWBSで定義されたワークパッケージを要素分解したもので、プロジェクトタイムマネジメントで定義します。

問3

(平成26年春 基本情報技術者試験 午前 問53)

《解答》エ

フォワードパスを求め、クリティカルパスとそれぞれの作業の最早終了日を出すと、次図の色文字で示したようになります(□で囲ったものが作業時間の合計が最も大きい経路です)。



したがって、エが正解です。

問4

(平成28年春 情報セキュリティマネジメント試験 午前 問42)

《解答》ア

過去5年間のシステム障害を種類別件数ごとに積み重ねて棒グラフで示し、年ごとの種類別件数と総件数の推移をまとめて表すためには、積上げ棒グラフを利用するのが適当です。したがって、アが正解となります。

イ 二重円グラフは、二つの推移の比較に適しています。

ウ ポートフォリオ図は、全体の割合の確認に適しています。

エ レーダチャートは、分野ごとの偏りなどを表すのに適しています。

問5

(平成26年春 基本情報技術者試験 午前 問54)

《解答》エ

全工数の人月は、

- ・ 開発規模から計算された人月
- ・ システムの導入や開発者教育の工数
- ・ 上記二つを加算した工数のプロジェクト管理の人月

を加算したものになります。

開発規模の人月を計算すると、 $500\text{FP} \div 10\text{FP} = 50$ 人月になります。システムの導入や開発者教育の工数は10人月となるので、加算して $50 + 10 = 60$ 人月です。プロジェクト開発の工数は全体の10%なので、 $60 \times 0.1 = 6$ 人月になります。

以上を加算すると、 $60 + 6 = 66$ 人月となります。したがって、エが正解です。

問6

(平成26年秋 基本情報技術者試験 午前 問55)

《解答》エ

リスク対応では、リスク分析の結果を基に、プロジェクト目標に対する好機を高め、脅威を減少させるための選択肢と方法を策定します。マイナスのリスクもしくは脅威に対する戦略としては、「回避」「転嫁」「軽減」「受容」の四つがあります。したがって、エが正解です。

その他の選択肢は、プラスのリスクもしくは好機に対する戦略です。

第6章

テクノロジー

テクノロジー系の関連分野について知っておくことは、情報セキュリティを理解する上でとても大切です。

この章では、ネットワーク、データベース、システム構成要素の3分野について、その概要を学習していきます。

ネットワークは、サイバー攻撃やファイアウォールなどのセキュリティ機器を理解する上で基本となる知識です。

データベースは、SQLインジェクションをはじめとしたサイバー攻撃やデータへのアクセス制御などを理解する上で大切な分野です。

6-1 ネットワーク

- ◆ 6-1-1 ネットワーク方式
- ◆ 6-1-2 データ通信と制御
- ◆ 6-1-3 通信プロトコル
- ◆ 6-1-4 ネットワーク管理
- ◆ 6-1-5 ネットワーク応用
- ◆ 6-1-6 演習問題

6-2 データベース

- ◆ 6-2-1 データベース方式

6-2-2 データベース設計

- ◆ 6-2-3 データ操作
- ◆ 6-2-4 トランザクション処理
- ◆ 6-2-5 データベース応用
- ◆ 6-2-6 演習問題

6-3 システム構成要素

- ◆ 6-3-1 システムの構成
- ◆ 6-3-2 システムの評価指標
- ◆ 6-3-3 演習問題

6-1 ネットワーク

情報セキュリティは、もともとネットワーク利用の分野から発展していきました。情報セキュリティを理解するためには、ネットワークの基礎知識が不可欠です。



勉強のコツ

ネットワークの知識は、情報セキュリティ技術を理解する上での基本となります。特にTCP/IPやLANなどについて、重点を置いて学習していきましょう。

動画

テクノロジー(技術要素)の分野についての動画を以下で公開しています。

<http://www.wakuwakuacademy.net/itcommon/3>
本書では記載しきれなかった基本的な内容や、正規化の手法などの手順について詳しく解説しています。本書の補足として、よろしければご利用ください。



用語

電気通信事業者とは、NTTやKDDIなど、公共の場所にネットワークを構築することを許可された事業者です。

6-1-1 ネットワーク方式

ネットワークの種類には、大きく分けてLANとWANがあります。インターネット技術では、TCP/IP技術を中心に様々な方式があります。

通信ネットワークの役割

初期の通信ネットワークは、管理者が特定のコンピュータ同士を接続しただけのものでした。このようなネットワークを私的(プライベート)なネットワークといいます。それが徐々に、プライベートなネットワーク同士を接続する公共(パブリック)のネットワークへと移行していきました。その一番大きなものが、世界中のネットワークが接続されたインターネットです。

ネットワーク社会とICT

ネットワークで世界中がつながり、情報が世界中に広がる現在の社会は、ネットワーク社会、または情報社会と呼ばれています。ネットワーク社会で使われる情報・通信技術の総称をICT(Information and Communication Technology)といい、ネットワークを利用したITの活用はますます重要になってきています。

ネットワークの種類と特徴

LAN(Local Area Network)は、一つの施設内で用いられるネットワークです。WAN(Wide Area Network)は、広い範囲を結ぶネットワークです。といっても二つの違いは広さではなく、管理する人によって区別されます。ユーザが主体となって運営・管理するのがLAN、電気通信事業者が提供するサービスで構成されるのがWANです。

電気通信事業者が提供するサービスには、FTTH(Fiber To

The Home)や携帯電話接続サービスなど、様々なものがあります。それに加えて、インターネットサービスプロバイダが提供するインターネット接続サービスを利用することで、インターネットに接続できるようになります。

■ インターネット技術

プロトコルとは、コンピュータとコンピュータがネットワークを利用して通信するために決められた約束ごとです。プロトコルをきちんと決めておくことによって、メーカーやCPU、OSなどが異なるコンピュータ同士でも、同じプロトコルを使えば互いに通信することができます。

インターネットの標準であるプロトコルは**TCP/IPプロトコル群**(Transmission Control Protocol/Internet Protocol)といい、インターネットのデファクトスタンダードとして世界中で最も広く使われています。



用語

TCP/IPプロトコル群の詳細は、「6-1-3 通信プロトコル」で改めて取り上げます。

6

■ クライアントとサーバ

ITサービスを実際に提供する機器のことを**サーバ**といいます。そして、ITサービスを利用するためにユーザが使用するPCなどの機器が**クライアント**です。サーバでは、クライアントからのリクエスト(問合せ)を受け、必要なレスポンス(応答)を返します。

▶▶ 覚えよう!

- ☐ LANは施設内に自分で設置，WANは電気通信事業者が用意
- ☐ ITサービスを提供する機器がサーバ，ユーザが利用するのがクライアント

6-1-2 データ通信と制御

ここでは、LANやWANでの伝送方式や仕組みについて学びます。プロトコルは、階層化させることで処理の変更に対応しやすくなります。

パケット交換と回線交換

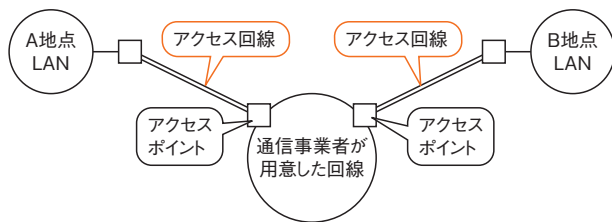
データを送るときに、大きなデータをそのまま送ると、ネットワークに負荷がかかる上、時間もかかります。そのため、コンピュータネットワーク上では、大きなデータをパケットと呼ばれる小さな単位に分割して送信する**パケット交換**という手法がよく用いられます。

それに対し、通信回線を専用で用意する専用線では、電話回線のように通信ごとに専用の回線を接続して、連続してデータを流し続ける**回線交換**という方法を利用します。

WANでの伝送方式

電気通信事業者は、全国にWANの回線を張り巡らせています。しかし、その回線は、特定の場所に設置されているアクセスポイントまで行かないと利用できません。そのため、会社のLANをその回線に接続するために、アクセスポイントまで別の回線を利用する必要があります。

そのときに利用する回線をアクセス回線といいます。例えば、A地点とB地点のLANを、通信事業者が用意した回線を用いて接続する場合は、次図のように利用します。



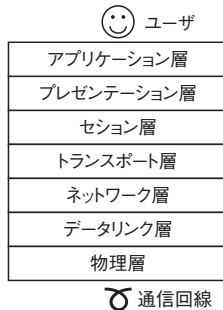
WANでの回線の利用方法

ネットワーク接続では、LAN内での接続、LAN－WAN接続、WAN内での接続など、様々な接続を行いながら通信を行います。

■ OSI基本参照モデル

一つのプロトコルにすべての機能を詰め込んでしまうと、処理が変わったときに変更するのが大変なので、プロトコルを階層化させて役割を分けておきます。

ネットワーク階層化の考え方として最も有名なものが、OSI (Open Systems Interconnection) 基本参照モデルです。コンピュータのもつべき通信機能を、次の七つの階層に分けて定義しています。



OSI基本参照モデル

ユーザが作成したデータは、通信に使用するアプリケーションに送られます。それがアプリケーション層です。その後、順にプレゼンテーション層、セッション層……と送られ、最終的に物理層に到達し、電気信号として通信回線に流されます。

それぞれの層の機能や役割は、以下のとおりです。

第7層 アプリケーション層

通信に使うアプリケーション（サービス）そのものです。

第6層 プレゼンテーション層

データの表現方法を変換します。例えば、画像ファイルをテキスト形式に変換したり、データを圧縮したりします。

第5層 セッション層

通信するプログラム間で会話をを行います。セッションの開始や終了を管理したり、同期をとったりします。

第4層 トランスポート層

コンピュータ内でどの通信プログラム(サービス)と通信するのかを管理します。また、通信の信頼性を確保します。

第3層 ネットワーク層

ネットワーク上でデータが始点から終点まで配送されるように管理します。ルーティングを行い、データを転送します。

第2層 データリンク層

ネットワーク上でデータが隣の通信機器まで配送されるように管理します。通信機器間で信号の受渡しを行います。

第1層 物理層

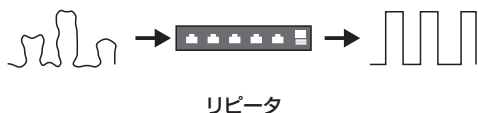
物理的な接続を管理します。電気信号の変換を行います。

LAN間接続装置

OSI基本参照モデルでは階層ごとに機能や役割が違うので、ネットワークに接続するときに必要な装置も異なります。それぞれの階層で必要な機器は以下のとおりです。

①リピータ(第1層 物理層)

電気信号を増幅して整形する装置です。リピータの機能で複数の回線に中継するリピータハブ(L1スイッチ)が一般的です。すべてのパケットを中継するので、接続数が多くなってくるとパケットの衝突が発生し、ネットワークが遅くなります。



リピータ

②ブリッジ(スイッチングハブ)(第2層 データリンク層)

データリンク層の情報(MACアドレス)に基づき、通信を中継するかどうかを決める装置です。ブリッジの機能で複数の回線に中継する**レイヤ2 (L2) スイッチ**がよく用いられます。リピータに加えて、アドレス学習機能とフィルタリング機能を備えてい

ます。送信元のMACアドレスをアドレステーブルに学習し、宛先のMACアドレスがアドレステーブルにある場合に、そのポートのみにデータを送信します。

③ルータ (第3層 ネットワーク層)

ネットワーク層の情報(IPアドレス)に基づき、通信の中継先を決める装置です。ルーティングテーブルによって中継先を決める動作を**ルーティング**といいます。スイッチングハブの機能にルーティングの機能を加えた**レイヤ3 (L3) スイッチ**もあります。

④ゲートウェイ (第4～7層 トランスポート層以上)

トランスポート層以上でデータを中継する必要がある場合に用います。例えば、PCの代理としてインターネットにパケットを中継するプロキシサーバや、電話の音声をデジタルデータに変換して送出するVoIPゲートウェイなどは、ゲートウェイの一種です。

■ スイッチの機能

スイッチ(レイヤ2スイッチ, レイヤ3スイッチ)には、有線／無線にかかわらず次のような機能をもつ機器があり、信頼性やセキュリティを向上させています。

①VLAN (Virtual LAN : 仮想LAN)

一つのスイッチに接続されているPCを、論理的に複数のネットワークに分ける仕組みです。部署ごとに接続するVLANを分ける、または、ウイルス対策は専用のVLAN (検疫VLAN)に隔離して行うなどの使い方があります。

②認証スイッチ

スイッチのポート一つ一つで認証を行い、アクセス制御を行うスイッチです。よく用いられる規格はIEEE 802.1Xです。

▶▶ 覚えよう！

- ☐ OSI基本参照モデルは、通信機能を七つの階層に分けて定義したもの
- ☐ リピータは物理層、ブリッジはデータリンク層、ルータはネットワーク層

6-1-3 通信プロトコル

通信プロトコルで一番用いられているのは、TCP/IP プロトコル群です。それぞれの階層で様々なプロトコルが利用されています。

TCP/IP プロトコル群

インターネットや多くの商用ネットワークで使われるプロトコルをまとめたインターネットプロトコル群です。最初に定義された最も重要な二つのプロトコルであるTCP (Transmission Control Protocol) とIP (Internet Protocol) にちなんで、TCP/IP プロトコル群と呼ばれます。次の4階層にまとめられますが、OSI 基本参照モデルの7階層と切り口は同じです。

TCP/IPプロトコル	OSI基本参照モデル
アプリケーション層	アプリケーション層
	プレゼンテーション層
	セッション層
トランスポート層	トランスポート層
インターネット層	ネットワーク層
ネットワークインタフェース層	データリンク層
	物理層

TCP/IP プロトコルと OSI 基本参照モデル

ネットワークインタフェース層のプロトコル

ネットワークインタフェース層(物理層、データリンク層)の代表的な規格に、WANで使用されるPPP (Point-to-Point Protocol) や、主にLANで使用されるイーサネットがあります。

PPPは、2点間を接続してデータ通信を行うためのプロトコルで、ダイヤルアップネットワークで使用されてきました。通信相手の認証や、IPアドレスの取得などを行います。

イーサネットは、MACアドレス(Media Access Control address)によって通信相手を決めます。MACアドレスは、各通信機器に固定で設定されているハードウェアアドレスであり、同じネットワーク内で通信相手を識別するために使用されます。

■ インターネット層のプロトコル

インターネット層のプロトコルの中心は、**IP** (Internet Protocol) です。IPの役割は、パケットを目的のホスト(通信機器)まで届けることです。IPアドレスによって、世界中のインターネットに接続されている機器の中から相手を見つけ、パケットを送ります。また、エラー通知や情報通知を行う**ICMP** (Internet Control Message Protocol) がIPをサポートします。

IPアドレスは、**ネットワークアドレス+ホストアドレス**で構成されます。IPv4 (IP version 4) アドレスは合計で32ビットで表現されます。同じネットワークであれば同じネットワークアドレスが割り当てられ、そのネットワーク内で一意のホストアドレスが割り当てられます。

ネットワークアドレスの長さはクラスを基準に定められます。クラスは、次の表のようにIPアドレスの範囲から設定されます。

クラスとIPアドレス

クラス	IPアドレスの範囲	ネットワーク アドレス	ホスト アドレス
クラスA	0.0.0.0 ~ 127.255.255.255	8ビット	24ビット
クラスB	128.0.0.0 ~ 191.255.255.255	16ビット	16ビット
クラスC	192.0.0.0 ~ 223.255.255.255	24ビット	8ビット
クラスD	224.0.0.0 ~ 239.255.255.255	IP マルチキャスト用	

ただ、近年では、クラスを固定してネットワークアドレスを割り当てるとIPアドレスが足りなくなるため、クラスに依存せずにネットワークアドレスを割り当てる**CIDR** (Classless Inter-Domain Routing) という技術が用いられるようになってきました。IPアドレスをCIDRで表記する場合は、ネットワークアドレス(サブネットアドレス)が占める範囲のビット数を“/”(スラッシュ)の後に付記します。

例えば、200.200.200.1/28なら、先頭から28ビットがネットワークアドレス、残りの4ビットがホストアドレスであることを示します。

また、これと同じことを**サブネットマスク**を用いて表現することもあります。サブネットマスクは、ネットワークアドレスの部分を1、ホストアドレスの部分を0で示したアドレス表記なので、



ICMPを使う代表的なプログラムに**ping**があります。特定のIPアドレスに向けてpingを実行することで、相手のホストが動いているかどうかを確認します。



ホストとは、ネットワークに接続されたコンピュータです。PCだけでなくサーバなどもホストに含まれます。

CIDRでの/28は255.255.255.240となります。以下の図で確認してください。

IPアドレス	200	.200	.200	.1	
2進数	11001000	11001000	11001000	00000001	
サブネットマスク	255	.255	.255	.240	
2進数	11111111	11111111	11111111	11110000	

なお、ホストアドレスのすべてのビットが0のIPアドレス（ネットワークアドレス）と、すべてのビットが1のIPアドレス（ブロードキャストアドレス）は、普通のIPアドレスとしては使用できません。

また、他のインターネット層のプロトコルとしては、**ARP** (Address Resolution Protocol) があります。ARPは、IPアドレスからMACアドレスを求めるためのプロトコルです。宛先ホストのIPアドレスを手がかりに、次に送るべき機器のMACアドレスを調べます。

■ トランスポート層のプロトコル

トランスポート層の主なプロトコルは、**TCP** (Transmission Control Protocol) と **UDP** (User Datagram Protocol) の二つです。

どちらも**ポート番号**を使って、同じIPアドレスのコンピュータ内でサービス（プログラム）を区別します。

TCPでは、信頼性を確保するために、必ず1対1で通信し、3段階でコネクションを確立します。また、シーケンス（処理の流れ）をチェックして、パケットの再送管理やフロー制御などを行います。機能が多い分、速度が下がるので、信頼性よりリアルタイム性が要求される場合にはUDPを使います。

■ アプリケーション層のプロトコル

アプリケーション層は、通信を行うアプリケーション特有のプロトコルを扱う層です。通信の用途によっていろいろなプロトコルが用意されています。以下に代表的なものを挙げます。



ARPには、ルータなどの機器が代理でARPの応答を行うプロキシARPや、IPアドレスの重複を確認するためにARP要求を出してみるGratuitous ARPなど、様々な応用例があります。また、セキュリティ攻撃としても、ARPを偽装するARPスプーフィング攻撃などがあります。

① HTTP (HyperText Transfer Protocol)

WebブラウザとWebサーバとの間で、HTML (HyperText Markup Language) などのコンテンツの送受信を行うプロトコルです。暗号化プロトコルであるTLSと組み合わせ、HTTPS(HTTP over TLS)として利用されることも多いです。



用語

HTML (HyperText Markup Language) は、Web ページを記述するための言語です。タグをつけて文章に装飾を行うことで、いろいろな機能を追加することができます。

② SMTP (Simple Mail Transfer Protocol)

インターネットでメールを転送するプロトコルです。

③ POP (Post Office Protocol)

ユーザがメールサーバから自分のメールを取り出すときに使います。メールをクライアントにダウンロードします。

④ IMAP (Internet Message Access Protocol)

メールサーバ上のメールにアクセスして操作するためのプロトコルです。メールをサーバ上に保存したまま管理します。

⑤ DNS (Domain Name System)

インターネット上のホスト名・ドメイン名とIPアドレスを対応付けて管理します。分散データベースシステムで、ルートサーバから階層的にデータを管理しています。ゾーン情報(元となるDNSレコード)をもつプライマリサーバと、その完全なコピーとなるセカンダリサーバとの間でゾーン転送を行い、データの同期を実行します。

⑥ FTP (File Transfer Protocol)

ネットワーク上でファイルの転送を行うプロトコルです。

⑦ DHCP (Dynamic Host Configuration Protocol)

コンピュータがネットワークに接続するときに必要なIPアドレスなどの情報を自動的に割り当てるプロトコルです。



用語

DHCP では、IP アドレスだけでなく、サブネットマスクやデフォルトゲートウェイ、DNS サーバについても設定を行います。デフォルトゲートウェイは、外部に接続する場合に最初にデータを転送するルータのことです。

⑧ NTP (Network Time Protocol)

ネットワーク上の機器を正しい時刻に同期させるためのプロトコルです。GPSや標準電波などに接続されたインターネット上の

NTPサーバと通信して正確な時刻を取得し、その時刻でネットワーク内のすべての機器の時刻を同期させます。

■ IPアドレスとMACアドレス

IPアドレスとMACアドレスはそれぞれ、OSI基本参照モデルのネットワーク層とデータリンク層のアドレスです。そのため、IPアドレスはエンドツーエンド、つまり通信の最初から最後までを管理するので、送信元IPアドレスと宛先IPアドレスは、基本的に通信の途中では変わりません。

一方、MACアドレスは、リンクバイリンク、つまり、一つのリンク（ネットワーク）ごとに宛先が変わります。送信元の端末から最初のルータまで、ルータから次のルータまで、最後のルータからサーバまで、というように、送信元MACアドレスと宛先MACアドレスの値はネットワークを越えるたびに毎回変わります。



自分自身と通信するときのアドレスとして、**ループバックアドレス**があります。ループバックアドレスには127で始まるIPアドレスが使用できますが、通常は127.0.0.1を使用します。

■ アドレス変換

IPアドレスは、基本的にはエンドツーエンドで変わらないものですが、近年はIPv4のアドレス枯渇問題により、IPアドレスを節約するためにアドレスを変換することが一般的になりました。具体的には、社内LANなど、内部でしか使用できないアドレスとしては**プライベートIPアドレス**を使用し、外部と接続するときにはグローバルIPアドレスを使用します。プライベートIPアドレスの範囲は、以下のように決まっています。

プライベートIPアドレスのクラスと範囲

クラス	範囲
クラスA	10.0.0.0 ~ 10.255.255.255
クラスB	172.16.0.0 ~ 172.31.255.255
クラスC	192.168.0.0 ~ 192.168.255.255

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には、次のような仕組みを利用します。

① NAT (Network Address Translation)

プライベートIPアドレスをグローバルIPアドレスに1対1で対応させます。あらかじめ決められたIPアドレス同士を対応させ

る静的NATのほかに、接続ごとに動的に対応させる動的NATも可能です。同時接続できるのは、IPアドレスの数と同じ数の端末のみです。

②NAPT (Network Address Port Translation)

IPアドレスだけでなくポート番号も合わせて変換する方法です。一つのIPアドレスに対して異なるポート番号を用いることで、1対多の通信が可能になります。**IPマスカレード**と呼ばれることもあります。

③プロキシサーバ

アドレス変換のほかに、外部へのアクセスを1台のプロキシサーバで代行する方法があります。クライアントの代理で外部に接続する通常の**プロキシサーバ**のほかに、サーバの代理でクライアントからサーバへのアクセスを受け付ける**リバースプロキシサーバ**があります。

■ IPv6

現在普及しているIPアドレスは、IPv4 (Internet Protocol version 4) です。インターネットの普及に伴いIPv4アドレスは枯渇しかかっており、それを根本的に解決するための策としてIPv6 (Internet Protocol version 6) が開発されました。

IPv6ではIPアドレスを128ビットで表現するので、十分なアドレス空間が用意されています。IPv6の特徴としては、以下のものがあります。

①IPアドレスの自動設定

DHCPサーバがなくても、IPアドレスを自動設定できます。

②ルータの負荷軽減

IPv4では可変だったヘッダの長さがIPv6では固定長になり、ルータは余分なヘッダを読み込んだりエラー検出を行ったりする必要がなくなったので処理を高速化できます。



関連

IPアドレスは、IPv4では最大で 2^{32} (約42億)個でしたが、IPv6では最大で 2^{128} (約340澗)個まで対応できます。澗(かん)とは、 10^{36} のことで、1兆倍の1兆倍の1兆倍にあたり、事実上無限大と考えていいほど大きい数字です。

③セキュリティの強化

IPsecのサポートが必須であるため、セキュリティが確保され、ユーザ認証やパケット暗号化が可能になりました。

④3種類のアドレス

一つのインタフェースに割り当てられるユニキャストアドレスのほかに、複数のノードに割り当てられるマルチキャストアドレスや、複数のノードのうち、ネットワーク上で最も近い一つだけと通信するエニーキャストアドレスの三つのタイプのアドレスを設定できます。



ノードとは、ルータやサーバなどの通信機器のことです。PCなどのホストも含め、ネットワークでの中継点や終点になる機器が含まれます。

▶▶ 覚えよう！

- ☐ MACアドレスはリンクバイリンク、IPアドレスはエンドツーエンド
- ☐ メール送信はSMTP、受信はPOPとIMAP

6-1-4 ネットワーク管理

ネットワークは、導入した後も、障害が発生したり、PCの台数が増えて性能が落ちたりするなどいろいろな変化があるので、適切な管理が重要になります。

■ ネットワーク運用管理

ネットワークの運用においては、以下のような管理が行われます。

①構成管理

ネットワークの構成情報を維持し、変更を記録します。ネットワーク構成図を作成し、そのバージョンを管理します。

②障害管理

障害の検出、切り分け、障害原因の特定、復旧措置などを管理します。障害時の記録をとって稼働統計を行い、対応を管理して次に役立てます。

③性能管理

ネットワークのトラフィック量や転送時間を管理します。トラフィックを監視して不具合がないかチェックするほか、構成変更による負荷分散なども管理します。

▶▶ 覚えよう！

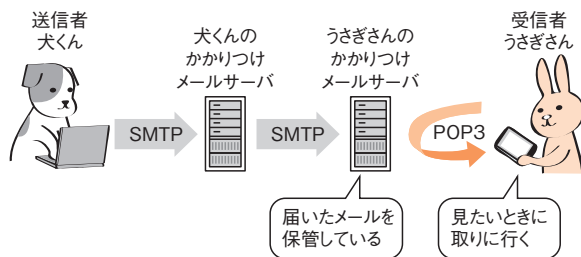
- ☐ 障害管理では、障害の検出、切り分け、原因の特定、復旧措置を行う

6-1-5 ネットワーク応用

ネットワークは日々進化しており、新しい通信サービスもどんどん増えてきています。

インターネット——電子メール

メールを送るためのプロトコルとして最初に登場したのは **SMTP** です。しかし SMTP は、送信側と受信側、両方の機器に電源が入っていることを前提に転送を行うプロトコルなので、通常の PC などでは送受信が円滑に行われません。そのため、電源を落とさないメールサーバのメールボックスにメールを保管しておき、必要に応じてメールクライアント（メールソフト）からアクセスしてメールを受信する **POP3** や **IMAP** などが登場しました。



メール通信の流れ

メールサーバは、上の図のようなリレー方式でメールを中継して送信していきます。また、一度に複数の相手にメールを送る**同報メール**も可能です。

メールの宛先は、通常の宛先である To のほかに、CC (Carbon Copy) で別の人にそのメールのコピーを送ることができます。また、BCC (Blind Carbon Copy) で、宛先に知らせずにメールのコピーを送ることも可能です。あらかじめ登録されたリストに送る**メーリングリスト**という方法もあります。

メールのデータ形式には、画像や動画、プログラムなど様々な種類のバイナリデータを送れるようにするための **MIME** (Multipurpose Internet Mail Extensions) があります。

■ インターネット——Web

Webとは、インターネット上で情報を公開・閲覧するシステムです。Webを利用するには、Webブラウザを用いて、Webサーバで動作しているWebアプリケーションソフトウェアと通信を行います。このときにやり取りされるデータは、マークアップ言語 (HTML, XML) で記述されており、ハイパリンクを用いてWebページ間の関連を表します。

インターネット上でのデータやサービスがある場所を示す識別子をURL (Uniform Resource Locator) といいます。URLには、インターネット上で区別するための名前であるドメイン名などが含まれており、これをDNS (Domain Name System) という仕組みでIPアドレスに変換し、通信を行います。

また、Webアプリケーションソフトウェアでは、通信しているユーザの情報を続けて管理するために、クッキー (Cookie) が使用されます。



用語

マークアップ言語とは、視覚表現や文章構造などを記述するための言語で、タグなどを用いて文章の形式を表します。タグを用いて表すものの代表としてハイパリンクがあり、別の文書 (URL) への参照を記述し、文章同士を結びつけることができます。

■ インターネット——ファイル転送

ファイル転送で用いられる最も基本的なプロトコルはFTPです。FTPでは、FTPサーバとFTPクライアントとの間で制御用とデータ転送用の二つのTCPコネクションを利用し、ファイルのアップロードやダウンロードを行います。

また、インターネット上にファイル保管場所としてストレージを用意したオンラインストレージのサービスも普及しています。

■ イン트라ネット／エクストラネット

イントラネットとは企業内ネットワークのことで、インターネットなどの技術を用いることで利便性を高め、アクセス制限をかけることで安全性を高めたものです。VPN (Virtual Private Network) やプライベートIPアドレスなどを利用し、セキュリティを確保しています。

複数のイントラネットを相互接続したネットワークのことをエクストラネットといいます。

インターネット回線上にIPsecなどを用いて作成する、セキュリティを確保したネットワークのことをインターネットVPNといいます。

インターネットを介した企業間の取引では、**EC**(Electronic Commerce：電子商取引)、**EDI**(Electronic Data Interchange：電子データ交換)などを実施し、Webを通して注文データのやり取りなどを行います。

■ 通信サービス

電気通信事業者が提供する通信サービスには、大きく分けて、回線を単独利用する専用回線と、回線を複数で共有する交換回線の2種類があります。さらに、交換回線には、回線の切替えを行い1対1での通信を実現する回線交換と、パケットを通信経路に流すことによって複数人で回線を共有する蓄積交換があります。

また、通信サービスには、回線速度を保証する**ギャランティ**型と、通信速度を保証せず、できる限り高速での通信を実現する**ベストエフォート**型の2種類があります。

主な通信サービスには、次のようなものがあります。

①専用回線(専用線)

接続形態が必ず1対1の専用のネットワークです。高いセキュリティや接続の安定性を確保したい場合に利用します。回線を独占して使えるので、ギャランティ型のサービスとなります。

②電話回線

電話回線は公衆電話網などの公衆回線を利用し、通話を行うサービスです。通常の固定電話の他に、携帯電話、PHSなどの移動体通信サービスも含まれます。回線自体は共有ですが、通信ごとに1対1で回線を接続するので、基本的にギャランティ型のサービスとなります。

③IP-VPN

通信事業者が提供する専用のIPネットワークでVPN(Virtual Private Network)を構築します。インターネット回線を利用するインターネットVPNはベストエフォート型ですが、IP-VPNでは通信事業者との契約や設定によって、ギャランティ型の通信も実現できます。

④ 広域 Ethernet

通信事業者が提供する専用のイーサネット接続サービスです。VLANを用い、他の顧客と通信を分離します。通信事業者との契約によって、ギャランティ型の速度保証も可能です。

⑤ FTTH (Fiber To The Home)

高速の光ファイバを建物内に直接引き込みます。回線の終端にはONU (Optical Network Unit)を用いて、光と電気信号を変換します。基本的にベストエフォート型で、通信速度は、同じ回線を利用している他の人の通信によって変わってきます。

■ モバイル通信

移動体通信規格 (LTE: Long Term Evolution など) を基に、様々なモバイル通信サービスが提供されています。スマートフォンなどをネットワークの中継機器のように用いて、他のコンピュータなどをインターネットに提供することを**テザリング**といいます。

また、LTE回線で音声通信を行う VoLTE (Voice over LTE) サービスが近年開始されました。

■ IP 電話

IP 電話は、電話網に^{ボイプ}**VoIP** (Voice over Internet Protocol) 技術を利用する電話サービスです。インターネットやイントラネット上で電話を利用することができます。VoIPでは、音声を符号化してパケットに変換し、IPネットワーク上でリアルタイム伝送を行います。

|| ▶▶ 覚えよう！

- ☐ SMTPでメール送信、POP3やIMAPでメール受信
- ☐ ベストエフォートで、速度を保証せずに通信するサービスがある

6-1-6 演習問題

問1 転送時間の計算

CHECK ▶ ☐☐☐

10Mバイトのデータを100,000ビット／秒の回線を使って転送するとき、転送時間は何秒か。ここで、回線の伝送効率を50%とし、1Mバイト=10⁶バイトとする。

- ア 200 イ 400 ウ 800 エ 1,600

問2 NAPT

CHECK ▶ ☐☐☐

PCが、NAPT（IPマスカレード）機能を有効にしているルータを経由してインターネットに接続されているとき、PCからインターネットに送出されるパケットのTCPとIPのヘッダのうち、ルータを経由する際に書き換えられるものはどれか。

- ア 宛先のIPアドレスと宛先のポート番号
イ 宛先のIPアドレスと送信元のIPアドレス
ウ 送信元のポート番号と宛先のポート番号
エ 送信元のポート番号と送信元のIPアドレス

問3 ルータの機能

CHECK ▶ ☐☐☐

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4 IPv4**CHECK** ▶ ☐☐☐

IPv4のグローバルIPアドレスはどれか。

- | | |
|-------------------|------------------|
| ア 118.151.146.138 | イ 127.158.32.134 |
| ウ 172.22.151.43 | エ 192.168.38.158 |

問5 Webアクセスを高速化する仕組み**CHECK** ▶ ☐☐☐

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 プロキシサーバ |

6**問6 DHCPサーバが設置されたLAN環境****CHECK** ▶ ☐☐☐

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。

解答と解説

問1

(平成27年春 基本情報技術者試験 午前 問31)

《解答》 **エ**

転送時間は、データ量を回線速度で割ることで求められます。計算時には、「単位を合わせる」「ビット・バイト換算を行う」点に注意が必要です。計算式は次のとおりです。

$$\begin{aligned}\text{転送時間} &= (10 \times 10^6 \times 8[\text{ビット}]) \div (100,000 \times 0.5[\text{伝送効率}][\text{ビット/秒}]) \\ &= 1,600\text{秒}\end{aligned}$$

したがって、**エ**が正解です。

問2

(平成26年秋 応用情報技術者試験 午前 問32)

《解答》 **エ**

NAPT (Network Address Port Translation : IPマスカレード)では、ルータを経由してインターネットに接続するとき、送信元のIPアドレスだけでなく、送信元のポート番号も同時に変換します。したがって、**エ**が正解です。

NAPTは、内部のIPアドレスを隠蔽して外部に知らせないことと、一つのIPアドレスで複数のPCが接続できることを目的としているため、ア、イ、ウのように、宛先のIPアドレスやポート番号の変換は行いません。

問3

(平成28年春 情報セキュリティマネジメント試験 午前 問45)

《解答》 **ア**

ルータは、ネットワーク層で中継を行う装置で、LAN同士、LANとWAN間など、様々なネットワークを相互接続します。したがって、**ア**が正解です。

イはリピータ、ウ、エはブリッジ(スイッチングハブ、レイヤ2スイッチ)に関する記述です。

問4

(平成27年春 基本情報技術者試験 午前 問36)

《解答》 **ア**

IPv4のIPアドレスは、グローバルIPアドレスとプライベートIPアドレスに分けられます。選択肢のうち、グローバルIPアドレスはアのみです。したがって、**ア**が正解です。

イ ループバックアドレスです。

ウ クラスBのプライベートIPアドレスです。

エ クラスCのプライベートIPアドレスです。

問5

(平成28年春 情報セキュリティマネジメント試験 午前 問46)

《解答》エ

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するサーバで、Web コンテンツをキャッシュする機能をもつものをプロキシサーバといいます。したがって、エが正解です。

- ア DMZはネットワークにおける非武装地帯 (DeMilitarized Zone) で、ファイアウォールによって内部ネットワークとインターネットの両方から隔離し、外部からの接続を直接受け付けるネットワークです。
- イ IP マスカレード (NAPT : Network Address Port Translation) は、IP アドレスとポート番号を用いて IP アドレス変換を行うものです。
- ウ ファイアウォールは、ネットワーク上で通過させるべきではない通信を遮断するための装置です。

問6

(平成28年秋 情報セキュリティマネジメント試験 午前 問47)

《解答》ウ

DHCPサーバは、IPアドレスの他にネットマスクやデフォルトゲートウェイアドレスなども自動設定するサーバです。PCは、DHCPサーバのアドレスを知らなくても、ブロードキャストパケット (LAN全体に送るパケット) を送ることで、DHCPサーバがそのパケットを受け取って情報を返答します。あらかじめDHCPサーバのアドレスを設定しておく必要はないので、ウが正解です。

- ア サブネットマスクやデフォルトゲートウェイアドレスも自動設定できます。
- イ PCへのIPアドレスの固定設定は、DHCPによる自動割当てのIPアドレスと重複しなければ設定可能です。
- エ IPアドレスは毎回自動で割り当てられるので、電源が切られた後に再度割当てを行うと、異なるIPアドレスになることもあります。

6-2 データベース

データベースとは、もともとは「データの基地」という意味で、データを1か所に集めて管理しやすくしたものです。データベースを運用・管理するためのシステムがデータベース管理システム(DBMS)です。



勉強のコツ

データベースについては、基本的な用語やトランザクション管理を中心に押さえておきましょう。

情報セキュリティとの関連では、DBMSのセキュリティ機能やSQLインジェクションなどの攻撃を理解するためのSQLがポイントです。

6-2-1 ■ データベース方式

データベースの方式には様々なものがありますが、現在は関係データベースが主流です。DBMSではメタデータ管理、クエリ処理、トランザクション管理などを行います。

■ データベースの種類と特徴

データベースには、大きく分けて以下の4種類があります。

①階層型データベース

データを階層型の親子関係で表現します。最も古くからある手法であり、データ同士の関係はポインタで表します。

②ネットワーク型データベース

階層型で表現できない、子が複数の親をもつ状態を表現します。

③関係データベース(リレーショナルデータベース：RDB)

テーブル間の関連でデータを表現するデータベースです。数学の理論を基にしているので、上記の2種類とは考え方がまったく異なります。現在のデータベースの主流です。

④オブジェクト指向データベース

オブジェクト指向という開発手法に対応したデータベースです。データと操作を一体化して扱います。

■ DBMS (データベース管理システム)

DBMS (DataBase Management System : データベース管理システム) は、データを一つにまとめて管理することでデータの整合性を保ち、データを安全に保管することを目的としたシステムです。そのために、DBMSは次の三つの機能を備えています。

① メタデータ管理

データとその特性 (**メタデータ**) を管理します。メタデータは、DBMS 中にある **データディクショナリ** に格納されます。

② 問合せ (クエリ) 処理

データベースに対する問合せ (クエリ) を処理します。問合せはSQLで記述されます。

③ トランザクション管理

複数のトランザクションの同時実行を管理します。そのために排他制御や障害回復などを行います。

④ セキュリティ機能

データのセキュリティを確保します。データが失われないようにする**保全機能**や、暗号化などでデータを秘匿化する**データ機密保護機能**、必要な人のみがデータを操作できるようにする**アクセス制限機能**など、様々なセキュリティ機能があります。



用語

メタデータとは、データの属性など、そのデータが何を示すかを表すものです。例えば、商品番号、商品名などの属性情報や、日付や数値などのデータ形式などの情報がメタデータです。



関連

SQL については、「6-2-3 データ操作」で詳しく説明しています。



関連

トランザクションについては、「6-2-4 トランザクション処理」で詳しく説明しています。

6

▶▶ 覚えよう!

- ☐ 関係データベースは、テーブルとテーブル間の関連でデータを表現
- ☐ DBMS には、セキュリティ機能として、保全機能やデータ機密保護機能などがある

6-2-2 データベース設計

データベース設計では、データ分析を行い、正規化します。また、データの関係を表すのにE-R図を使用します。

データ分析

データベース設計では、どのようなデータがあるのかを洗い出し、データ分析を行います。データ分析では、正規化を行います。正規化とは、正しい規則に従ってテーブルを分割することです。

正規化の目的は、データの重複を排除し、データの整合性を保つことです。テーブルの構造など、データに関連する情報は、データディクショナリに格納されます。

E-R図

データ分析を行った後のテーブル間の関連は、E-R図(Entity-Relationship Diagram)で表します。E-R図は、実体(エンティティ)と関連(リレーションシップ)を表す図です。関連では、対応関係(カーディナリティ)を記述しますが、対応関係には次の4種類があります。



実務的には、E-R図のエンティティは関係データベースのテーブルに対応します。リレーションシップは、外部キーなどを用いてテーブルに設定します。

① 1対1の関連



一つのデータに一つのデータが対応します。先生と生徒なら、家庭教師のようなマンツーマンの関係です。

② 1対多の関連



一つのデータに複数のデータが対応します。先生と生徒なら、学校の担任のように先生1人で複数の生徒を教える関係です。

③ 多対1の関連



複数のデータに一つのデータが対応します。先生と生徒なら、複数の先生が1人の生徒に質問する面接のような関係です。

④ 多対多の関連



複数のデータに複数のデータが対応します。先生と生徒なら、学校のように複数の先生が複数の生徒を教える関係です。

覚えてよう！

- ☐ 正規化を行うことで、データの重複をなくし、整合性を確保する
- ☐ E-R図は、エンティティ間の関係をリレーションシップで表した図

6-2-3 データ操作

データ操作を行う言語はいろいろありますが、関係データベースの操作を行うのはSQLです。SQLには、SQL-DDLとSQL-DML、SQL-DCLがあります。

SQL

SQLは、関係データベースを記述するための言語です。次の3種類に大別できます。

- データ定義言語 (SQL-DDL : SQL Data Definition Language)
- データ操作言語 (SQL-DML : SQL Data Manipulation Language)
- データ制御言語 (SQL-DCL : SQL Data Control Language)

データ定義言語 (SQL-DDL)

データ定義言語は、データベースの構造などを定義する言語です。CREATE文で新たなテーブルやビューなどを作成します。

例えば、見せるための表である**ビュー**を作成するときには、次のようなかたちで基のテーブルからビューを作成します。

```
CREATE VIEW ビュー名 AS SELECT * FROM テーブル名
```

データ操作言語

データ操作言語は、データの表示、挿入、更新、削除を行うための言語です。データ操作言語のうち最もよく使われるのは、検索して表示するためのSELECT文です。SELECT文の文法は決まっており、次の書式となります。



発展

ビューを定義して、基になるテーブルから必要なデータを抜き出し、ビューだけにアクセスを許可することで、データに細かくアクセス制御を行うことが可能になります。

```

SELECT * | [ALL | DISTINCT] <列名1> [, <列名2>, ... ]
FROM <表名1> [, <表名2>, ... , ]
      [JOIN <表名2> ON <結合条件>]
[WHERE <検索条件> (AND <検索条件2> ...)]
[GROUP BY グループ化する列の位置 (または列名)]
[HAVING グループ化した後の行を抽出する条件]
[ORDER BY 整列の元となる列 [ ASC | DESC ] ]

```

・[]で示した内容はオプションです。「|」はORを示し、いずれかを選択します。

SELECT文の書式

SELECT文の最初に、表示する列名を記述します。このとき、行の重複を許さない場合には**DISTINCT**を用います。

FROM句では、使用するテーブルを記述します。二つ以上のテーブルの結合は、FROM句で**JOIN**句を使い、結合するときに使用する列を記述します。

WHERE句は、行を選択する条件を記述します。

GROUP BY句は、グループ化、つまり指定された列の値が同じ複数の行を一つにまとめるものです。グループ化すると複数の行が一つになるので、基の行のデータは取り出せなくなります。

グループ化後の選択条件は、**HAVING**句に記述します。

ORDER BY句は、指定された列を使って整列します。

SELECT文以外のSQL-DMLは更新系SQLとも呼ばれ、INSERT文、UPDATE文、DELETE文の3種類があります。INSERT文ではデータを挿入、UPDATE文ではデータを更新、DELETE文ではデータを削除します。

■ データ制御言語(SQL-DCL : GRANTなど)

データベースを制御するための言語です。トランザクションの開始や終了、アクセス権限の制御などに用います。

データベースに作成される表やビューなどは、すべての人に公開する場合もありますが、アクセスを制限して特定のユーザのみに公開する場合もあります。その際にデータベースのアクセス権限を設定するSQLが、**GRANT**文です。

例えば、商品表に対して、うさぎさんにSELECT権限を付与する場合には、次のように記述します。

```
GRANT SELECT ON 商品 TO うさぎ
```

■ ストアドプロシージャ

ストアドプロシージャとは、データベースへの問合せ(SQL)を一連の処理としてまとめ、DBMSに保存したものです。使用するときには、プロシージャ名で呼び出すと、一連の処理を実行してくれます。

データベースの処理での通信回数が少なくなるため、速度の向上につながります。また、通信経路上に流すデータが少なくなるため、セキュリティの向上にもつながります。

▶▶ 覚えよう！

- ☐ SELECT 列 FROM 表 WHERE 条件 GROUP BY グループ化 ORDER BY 整列
- ☐ ストアドプロシージャでは、一連の処理をまとめて実行

6-2-4 ■ トランザクション処理

データベースのデータが失われたり改ざんされたりしないように、トランザクションを適切に管理する必要があります。また、性能を向上させるための工夫も行います。

■ トランザクション管理

トランザクションとは、分けることのできない一連の処理単位です。例えば銀行の処理なら、Aさんの口座からBさんの口座に振り込む場合、次のような一連の処理が発生します。

Aさんの口座の残高を減らす → Bさんの口座の残高を増やす

これらを途中で終わらせるわけにはいかないので、二つの処理をまとめてトランザクションとします。

トランザクション管理では、トランザクションを適切に管理するために排他制御を行い、障害が発生した際には回復処理を行います。

■ 排他制御

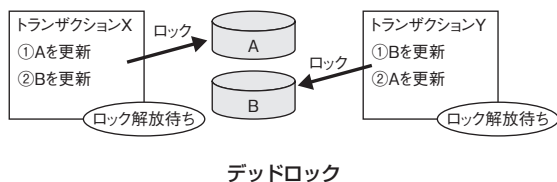
二つのトランザクションを同時に実行し、同じデータを更新してしまいデータに矛盾が生じることがあります。それを防ぐためには、排他制御(同時実行制御)を行い、一度に一つのトランザクションしかデータの更新が行えないようにする必要があります。そのための方法に**ロック**があります。参照・更新するデータにロックをかけ、使用が終わったときにロックを解除します。ロックの種類には以下のものがあります。

① 共有ロック／占有ロック

データを参照するだけの場合には、複数のトランザクションで同時に実行しても問題ありません。そのために**共有ロック**をかけて、データの参照は自由に行えるようにします。データを更新する場合には、ほかのトランザクションに見えないように**占有ロック**(専有ロック、排他ロック)をかけ、参照もできないようにします。

②デッドロック

二つのトランザクションで複数のデータを参照するとき、ロックのために互いのデータが使用可能になるのを待ち続けて、互いに動けない状態になることが**デッドロック**です。



デッドロックが起こらないようにするためには、複数のトランザクションにおいてデータの呼出し順序を同じにする方法が効果的です。

障害回復処理

データベースの障害には、大きく分けて次の三つがあります。

- トランザクション障害
- ソフトウェア (電源) 障害
- ハードウェア (媒体) 障害

トランザクション障害とは、デッドロックのような、トランザクションに不具合が起こる障害です。トランザクション障害ではDBMSは正常に動いており、データの不具合はないため、DBMSの状態を元に戻すロールバック命令などを実行することだけで対処できます。

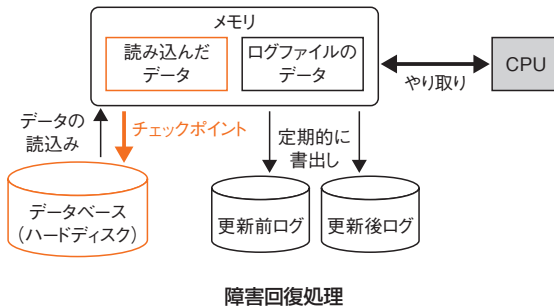
ソフトウェア障害とは、ソフトウェアの実行中止などで、DBMSのデータに不具合が起こる障害です。ハードウェア障害とは、ハードディスクの故障などでデータが損傷するような障害で、バックアップデータを用いて復元する必要があります。ただし、バックアップ後に更新されたデータやソフトウェア障害時のデータの復元には、次に挙げるログファイルが使われます。

■ ログファイルによる障害回復処理

データベース障害に備えるために、データベース用のハードディスクとは別のディスクにログファイルを用意します。用意するログファイルは、**更新前ログ**と**更新後ログ**の二つです。データベースを更新したらその都度、更新する前のデータを更新前ログに、更新した後のデータを更新後ログに記述します。

トランザクションがコミットしたら、その情報もログファイルに書き込みます。これは、データベースの内容は実際にはメモリ上でのみ更新されており、ハードディスク上のデータは不定期にしか更新されないためです。

メモリからハードディスク上のデータベースに書き込みを行うポイントが、**チェックポイント**です。チェックポイント後のデータは、障害が発生してメモリ上のデータが消えると失われてしまいます。そのためにログファイルを用意しておき、障害発生に備えます。

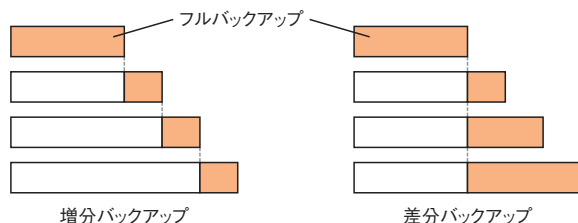


データベースに障害が発生したときにトランザクションのコミットが完了していた場合には、**更新後ログ**を使って、チェックポイント後のデータを復元させます。この動作を**ロールフォワード**と呼びます。

また、コミットが完了しないうちに障害が発生したときには、ハードディスクに書き込まれていた実行途中のデータをトランザクションの実行前の状態に戻す必要があります。そのためには、**更新前ログ**を用いて復元させます。この動作を**ロールバック**といいます。

■ バックアップによる障害回復処理

障害回復にバックアップは不可欠です。バックアップを取得する際、バックアップ対象をすべて取得することを**フルバックアップ**といいます。それに対し、前回のフルバックアップとの増分や差分のみを取得することを**増分バックアップ**、**差分バックアップ**といいます。増分バックアップでは、前回のフルバックアップまたは増分バックアップ以後に変更された部分だけをバックアップします。差分バックアップでは、前回のフルバックアップ以後に変更された部分だけをバックアップします。図で示すと次のとおりです。



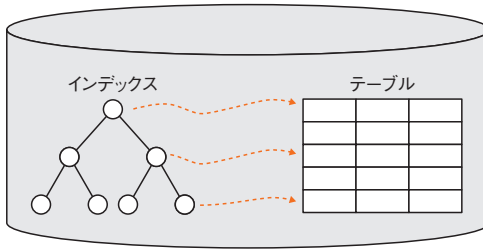
増分バックアップと差分バックアップ

フルバックアップを取得する周期が短い方が、復旧にかかる時間は短くなります。また、増分バックアップでは、1回のバックアップにかかる時間は短くて済みますが、復旧時にはすべての増分バックアップを順番に使用する必要があるため、復旧に時間がかかります。

また、ウイルス感染などのために、直前のバックアップ以外で復旧しなければならない場合があります。そのため、バックアップの**世代管理**を行い、最新のバックアップ以外も保管しておくことが大切です。

■ データベースの性能向上

データベースの性能を向上させる方法として一般的なのが**インデックス**です。インデックスとは、検索速度を上げるために設定する索引であり、基のテーブルとは別に、キーとデータの場所(ポインタ)の組を一緒に格納します。



インデックス

インデックスはテーブルを更新するたびに更新する必要があるため、インデックスを設定すると、かえって処理速度が遅くなることがあります。

覚 え よ う !

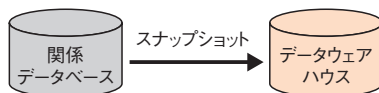
- ☐ トランザクションの排他制御のためにロックを使用する
- ☐ 更新前ログでロールバック，更新後ログでロールフォワード

6-2-5 ■ データベース応用

データベースでは、日々の業務を行うだけではなく、そのデータを分析する必要があります。そのため、データウェアハウスを構築します。

■ データウェアハウス

データベースに記録されたデータを分析するために、関係データベースなどのデータのスナップショット(ある時点のデータベースの内容)を取り、別のデータベースに移します。そのとき、多次元データとして再構成することで、いろいろな次元(分析軸)での分析を可能にします。この、多次元データの集まりが**データウェアハウス**です。



データウェアハウス

データウェアハウスの基本操作には、以下のものがあります。

①スライシング

多次元のデータを2次元の表に切り取る操作です。

②ダイシング

データの分析軸を変更し、視点を変える操作です。

③ドリリング

分析の深さを詳細にしたり、また、集計したりして変更する操作です。例えば、年月での分析を年単位にすることをドリルアップ、日単位にすることをドリルダウンといいます。ロールアップ、ロールダウンともいいます。

データウェアハウスなどに、統計学、パターン認識、人工知能などのデータ解析手法を適用することで新しい知見を取り出す技術のことを**データマイニング**といいます。

■ ビッグデータ

ビッグデータとは、通常のDBMS（関係データベースなど）で取り扱うことが困難な大きさのデータの集まりのことです。単にデータ量が多いだけでなく、様々な種類があり、構造化できないデータや定型的でないデータなども含まれます。

ビッグデータを扱うための技術には、グリッド・コンピューティング、データマイニング、超並列コンピュータなどがあります。

また、ビッグデータは通常の関係データベースでSQLを使用する処理に向いていません。そのため、様々な新しいデータベースが考案されており、それらのDBMSを総称して**NoSQL**と呼びます。

ビッグデータを扱うためには高度な技術スキルや統計スキルが必要とされるため、データサイエンティストと呼ばれる人材の育成も課題の一つです。



用語

グリッド・コンピューティングとは、インターネットなどの広域ネットワークにある計算資源を結び付け、一つの複合的なシステムとして使用する仕組みです。

▶▶ 覚えよう！

- ☐ 視点を変えるのがダイジニング、掘り下げるのがドリリング
- ☐ ビッグデータの処理には、NoSQLを使用することもある

6-2-6 演習問題

問1 E-R図

CHECK ▶ ☐☐☐

E-R図に関する記述のうち、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。

問2 RDBMSのビュー

CHECK ▶ ☐☐☐

関係データベース管理システム(RDBMS)におけるビューに関する記述のうち、適切なものはどれか。

- ア ビューとは、名前を付けた導出表のことである。
- イ ビューに対して、ビューを定義することはできない。
- ウ ビューの定義を行ってから、必要があれば、その基底表を定義する。
- エ ビューは一つの基底表に対して一つだけ定義できる。

問3 バックアップ方法**CHECK** ▶ ☐☐☐

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バイス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。

6

問4 同時実行制御**CHECK** ▶ ☐☐☐

トランザクションの同時実行制御に用いられるロックの動作に関する記述のうち、適切なものはどれか。

- ア 共有ロック獲得済の資源に対して、別のトランザクションからの新たな共有ロックの獲得を認める。
- イ 共有ロック獲得済の資源に対して、別のトランザクションからの新たな専有ロックの獲得を認める。
- ウ 専有ロック獲得済の資源に対して、別のトランザクションからの新たな共有ロックの獲得を認める。
- エ 専有ロック獲得済の資源に対して、別のトランザクションからの新たな専有ロックの獲得を認める。

問5 DBMSのログファイル

CHECK ▶ ☐☐☐

DBMSにおけるログファイルの説明として、適切なものはどれか。

- ア システムダウンが発生したときにデータベースの回復処理時間を短縮するため、主記憶上の更新データを定期的にディスクに書き出したものである。
- イ ディスク障害があってもシステムをすぐに復旧させるため、常に同一データのコピーを別ディスクや別サイトのデータベースに書き出したものである。
- ウ ディスク障害からデータベースを回復するため、データベースの内容をディスク単位で複写したものである。
- エ データベースの回復処理のため、データの更新前後の値を書き出してデータベースの更新記録を取ったものである。

問6 大量データの整理・統合

CHECK ▶ ☐☐☐

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き、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 |

■ 解答と解説

問1

(平成28年秋 情報セキュリティマネジメント試験 午前 問46)

《解答》イ

E-R図とは、実体(エンティティ)と関連(リレーションシップ)を表す図です。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ので、イが正解です。

ア 関係データベースに限らず表現できます。

ウ DFD (Data Flow Diagram)で表現します。

エ リレーションシップは、エンティティ間のデータの関連を表します。

問2

(平成24年春 基本情報技術者試験 午前 問29)

《解答》ア

ビューは、見せるための表です。導出表ともいいます。基の表から必要なデータを選択し、表示します。見せるだけなので、更新された場合は基の表に変更が加わります。すべてのビューが更新可能ではなく、基の行が特定できる必要があります。したがって、アが正解です。

イ ビューに対して、ビューを定義することもできます。

ウ 基底表とは、ビューが参照する基の表のことです。基底表を先に定義する必要があります。

エ 一つの基底表に対して複数定義できます。

問3

(平成28年秋 情報セキュリティマネジメント試験 午前 問43)

《解答》ア

差分バックアップでは、前回のフルバックアップ以降に変更されたファイルだけをバックアップします。フルバックアップに加えて、毎日差分バックアップを取得しておくことで、前日までのデータを復旧できるようになります。したがって、アが正解です。

イ、ウ 一つのディスクだけで障害が起こったときにはデータ消失を回避できますが、複数ディスクの障害時には、これまでと同様に、フルバックアップ時までしか回復できません。

エ メールサーバのディスクに障害が起こった場合には、これまでと同様、磁気テープにコピーした情報までしか復旧できません。

問4

(平成26年秋 基本情報技術者試験 午前 問30)

《解答》ア

ロックのかけ方には、共有ロックと専有ロックの2種類があります。共有ロック獲得済の資源へは、別のトランザクションから新たな共有ロックの獲得は認められますが、専有ロックは認められません。専有ロックの場合、新たな共有ロック、専有ロックのいずれも認められません。したがって、アが正解です。

問5

(平成24年春 基本情報技術者試験 午前 問32)

《解答》エ

DBMSでは、障害時に備えて、データの変更内容を記録したログを用意しておき、障害回復処理に役立てます。ログには、更新前ログと更新後ログの2種類があります。したがって、エが正解です。

- ア チェックポイントの説明です。
- イ レプリケーションの説明です。
- ウ バックアップの説明です。

問6

(平成28年春 情報セキュリティマネジメント試験 午前 問44)

《解答》イ

大量のデータを整理・統合して蓄積したデータベースのことを、データウェアハウスといいます。したがって、イが正解です。

- ア データを統合的に管理することです。
- ウ データの定義情報やユーザ、アクセス権限などを管理するものです。
- エ 異なるデータ間での関連づけを行うことです。

6-3 システム構成要素

システム構成要素では、システム、つまり複数のコンピュータやサーバ、プリンタなどが集まったときの全体の構成について学びます。

6-3-1 システムの構成

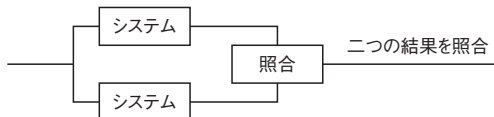
複数台のコンピュータを接続してシステムを構成するには、複数台のサーバを用意して並列に動かすなど、いろいろな工夫が必要になります。

■ システム構成の基本

システム構成の基本は、2台のシステムを接続するデュアルシステムとデュプレックスシステムです。3台、4台と増やす場合も、この考え方が基礎になります。

①デュアルシステム

二つのシステムを用意し、並列して同じ処理を走らせて、結果を比較する方式です。結果を比較することで高い信頼性が得られます。また、一つのシステムに障害が発生しても、もう一つのシステムで処理を続行することができます。



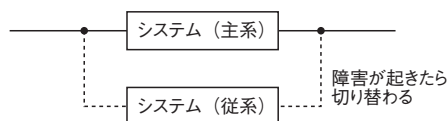
②デュプレックスシステム

二つのシステムを用意しますが、普段は一つのシステムのみ稼働させて、もう一方は待機させておきます。このとき、稼働させるシステムを主系（現用系）、待機させるシステムを従系（待機系）と呼びます。



勉強のコツ

システム構成要素の分野は計算問題が多く、稼働率の計算が一番のポイントになります。直列・並列システム、またその組合せについて、計算練習を行っておきましょう。



デュプレックスシステムのイメージ

デュプレックスシステムには、従系の待機のさせ方によって次の三つのスタンバイ方式があります。



ホット、ウォーム、コールドという言葉は、システムの待機系以外でもよく使われます。

災害時の対応で、別の場所に情報処理施設(ディザスタリカバリサイト)を用意しておくときの形態に、ホットサイト、ウォームサイト、コールドサイトという呼び方を用います。

●ホットスタンバイ

従系のシステムを常に稼働可能な状態で待機させておきます。具体的には、サーバを立ち上げておき、アプリケーションやOSなどもすべて主系のシステムと同じように稼働させておきます。そのため、主系に障害が発生した場合には、すぐに従系への切替えが可能です。故障が起こったときに自動的に従系に切り替えて処理を継続することをフェールオーバーといいます。

●ウォームスタンバイ

従系のシステムを本番と同じような状態で用意してありますが、すぐに稼働はできない状態で待機させておきます。具体的には、サーバは立ち上がっているものの、アプリケーションは稼働していないか別の作業を行っているかで、切替えに少し時間がかかります。

●コールドスタンバイ

従系のシステムを、機器の用意だけをして稼働しないで待機させておきます。具体的には、電源を入れずに予備機だけを用意しておいて、障害が発生したら電源を入れて稼働し、主系の代わりになるように準備します。主系から従系への切替えに最も時間がかかる方法です。

■システムの処理形態／利用形態

システムの形式は、処理形態や利用形態などでも様々なものがあります。例えば、処理を一つのサーバに集中させる**集中処理**の他に、処理を複数のサーバに分散させる**分散処理**があります。

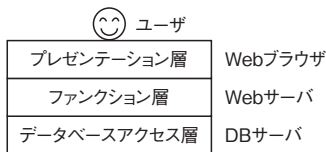
さらに、利用形態によって、処理をまとめて一度に行う**バッチ処理**や、すぐに処理を行う**リアルタイム処理**に分けられます。リアルタイム処理では、対話型処理を行うこともできます。

■ 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とは、クライアントとサーバでそれぞれ役割分担して、協力して処理を行うシステムです。3層クライアントサーバシステムでは、その役割を次の三つに分けています。それぞれの役割をクライアントとサーバのどちらが行うかは、システムの形態によって異なります。

- ・ **プレゼンテーション層**
ユーザインタフェースを受けもつ層
- ・ **ファンクション層** (アプリケーション層／ロジック層)
メインの処理やビジネスロジックを受けもつ層
- ・ **データベースアクセス層**
データ管理を受けもつ層

例えば、一般的なWebシステムの場合には、三つの役割を次のように分担します。



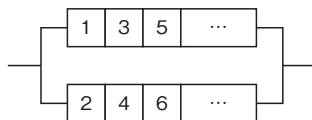
3層クライアントサーバシステム

■ RAID

システムの構成要素には、記憶装置の障害に備える仕組みが必要です。RAID (Redundant Arrays of Inexpensive ^{レイド}Disks) は、複数台のハードディスクを接続して全体で一つの記憶装置として扱う仕組みです。その方法はいくつかありますが、複数台のディスクを組み合わせることによって信頼性や性能が上がります。RAIDの代表的な種類としては、以下のものがあります。

① RAID0

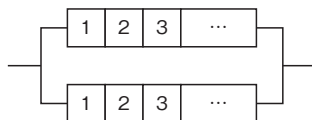
複数台のハードディスクにデータを分散することで高速化したものです。これを**ストライピング**と呼びます。性能は上がりますが、信頼性は1台のディスクに比べて低下します。



ストライピングのイメージ

② RAID1

複数台のハードディスクに同時に同じデータを書き込みます。これを**ミラーリング**と呼びます。2台のディスクがあっても一方は完全なバックアップです。そのため、信頼性は上がりますが、性能は特に上がりません。



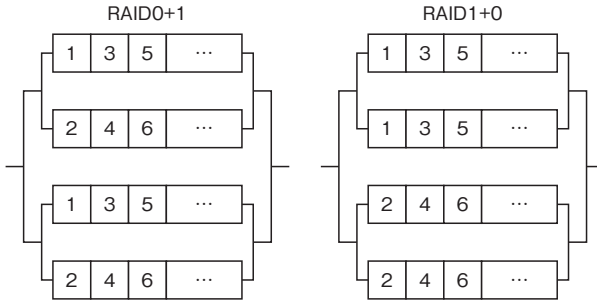
ミラーリングのイメージ



このように、二つのRAIDを組み合わせる方法はよく使われます。RAID0+1, RAID1+0以外にも、RAID0+5, RAID1+5, RAID5+5, RAID0+6など、RAID5, RAID6と組み合わせるものもあります。

③ RAID0+1, RAID1+0

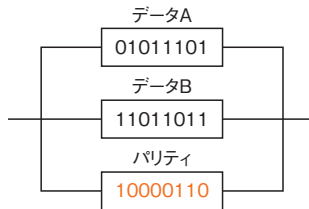
RAID0, RAID1はそれぞれ、性能(速度)、信頼性のどちらか一方しか向上しません。そこで、この二つを組み合わせる性能と信頼性の両方を向上させる技術として、RAID0+1, RAID1+0が考えられました。RAID0+1は、ストライピングされたディスクをミラーリングし、RAID1+0は、ミラーリングされたディスクをストライピングします。最低でもディスクが4台必要です。



RAID0+1, RAID1+0のイメージ

④ RAID3, RAID4

複数台のディスクのうち1台を誤り訂正用の**パリティディスク**にし、誤りが発生した場合に復元します。次の図のように、パリティディスクにはほかのディスクの偶数パリティを計算したものを格納しておきます。



パリティディスクの役割

この状態でデータBのディスクが故障した場合、データAとパリティディスクから偶数パリティを計算することで、データBが復元できます。データAのディスクが故障した場合も同様に、データBとパリティディスクから偶数パリティでデータAが復元できます。これをビットごとに行う方式がRAID3、ブロックごとにまとめて行う方式がRAID4です。

⑤ RAID5

RAID4のパリティディスクは誤り訂正専用のディスクであり、通常時は使いません。しかし、データを分散させた方がアクセス効率は上がるので、パリティをブロックごとに分散し、通常時にもすべてのディスクを使うようにした方式がRAID5です。



発展

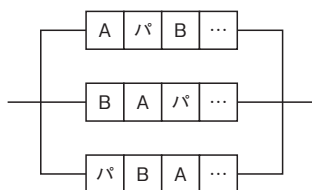
RAID3, RAID4 は、RAID5 と信頼性が同等で性能の面で劣るため、RAID5が用いられる場合がほとんどです。

また、RAID5はRAID1に比べてもディスクの使用効率が高いので、非常によく用いられるRAID方式です。



発展

RAID3, RAID4, RAID5 では、最低でもディスクが3台必要です。RAID6ではパリティディスクに2台割り当てるため、ディスクは最低でも4台必要になります。



パリティをブロックごとに分散

⑥ RAID6

RAID5では、1台のディスクが故障してもほかのディスクの排他的論理和を計算することで復元できます。しかし、ディスクは同時に2台壊れることもあります。そこで、冗長データを2種類作成することで、2台のディスクが故障しても支障がないようにした方式が**RAID6**です。

■ 信頼性設計

システム全体の信頼性を設計するときには、システム一つ一つを見る場合とは違った、全体の視点というものがになってきます。代表的な信頼性設計の手法には、次のものがあります。

① フォールトトレランス

システムの一部で障害が起こっても、全体でカバーして機能停止を防ぐという設計手法です。

② フォールトアボイダンス

個々の機器の障害が起こる確率を下げて、全体として信頼性を上げるという考え方です。

③ フェールセーフ

システムに障害が発生したとき、安全側に制御する方法です。信号が故障したときにはとりあえず赤を点灯させるなど、障害が新たな障害を生まないように制御します。処理を停止させることもあります。

④フェールソフト

システムに障害が発生したとき、障害が起こった部分を切り離すなどして最低限のシステムの稼働を続ける方法です。このとき、機能を限定的にして稼働を続ける操作をフォールバック (縮退運転) といいます。

⑤フォールトマスキング

機器などに故障が発生したとき、その影響が外部に出ないようにする方法です。具体的には、装置の冗長化などによって、1台が故障しても全体に影響がないようにするなどします。

⑥フールプルーフ

ヒューマンエラー (利用者が行う間違った操作) が起こっても危険な状況にならないようにするか、そもそも間違った操作ができないようにする設計手法です。具体的には、画面上で押してはいけないボタンは押せないようにするなどの方法があります。

■ いろいろなシステム構成

基本的なシステムのほかにも、近年ではいろいろなシステム構成が見られます。ここに代表的なものを示します。

①クラスタ

複数のコンピュータを結合してひとまとまりにしたシステムです。クラスタリングともいいます。負荷分散 (ロードバランス) や、HPC (High-Performance Computing: 高性能計算) の手法としてよく使われます。

②シンクライアント

ユーザが使うクライアントの端末には必要最小限の処理を行わせ、ほとんどの処理をサーバ側で行う方式です。

③ピアツーピア

端末同士で対等に通信を行う方式です。P2Pともいわれます。クライアントサーバ方式と異なり、サーバを介さずクライアント同士で直接アクセスするのが特徴です。



発展

シンクライアントが導入されるのは、性能上の理由だけではなくではありません。データがクライアント上に残らないことが情報漏えいの防止につながるため、セキュリティの観点から導入する企業が増えています。



発展

ピアツーピアは、サーバへのアクセス集中が起こらないため処理を拡大しやすく、IP電話や動画配信サービスなどで応用されています。Skypeなどでも採用されています。

④分散処理システム

複数のプログラムが並列的に複数台のコンピュータで実行され、それらが通信しあって一つの処理を行うシステムです。分散処理システムでは複数の場所で処理を行います。利便性の面では、利用者にその場所を意識させず、どこにあるプログラムも同じ操作で利用できることが大切です。これをアクセス透過性といいます。

■ストレージ

ストレージは、ハードディスクやCD-Rなど、データやプログラムを記録するための装置のことです。従来は、サーバに直接、外部接続装置や内蔵装置として接続するのが一般的でしたが、近年ではネットワークを通じて、コンピュータとは別の場所にあるストレージと接続することも多くなっています。

ストレージを接続する方法には、次の3種類があります。

①DAS (Direct Attached Storage)

サーバにストレージを直接接続する従来の方法です。SANやNASが出てきたことで、DASと位置づけるようになりました。

②SAN (Storage Area Network)

サーバとストレージを接続するために専用のネットワークを使用する方法です。ファイバチャネルやIPネットワークを使って、あたかも内蔵されたストレージのように使用することができます。

③^{ナス}NAS (Network Attached Storage)

ファイルを格納するサーバをネットワークに直接接続することで、外部からファイルを利用できるようにする方法です。



ファイバチャネル(FC: Fibre Channel)とは、主にストレージネットワーク用に使用される、ギガビット級のネットワークを構築する技術の一つです。機器の接続に光ファイバや同軸ケーブルを用います。

DASに比べると、SANもNASもストレージを複数のサーバやクライアントで共有できるので、ストレージの資源を効率的に活用することができます。また、物理的なストレージ数を減らせるため、バックアップなども取りやすくなります。

SANとNASの大きな違いは、サーバから見たとき、SANで接続されたストレージは内蔵のディスクのように利用できるのに

対し、NASでは外部のネットワークにあるサーバに接続するように見えることです。

▶▶ 覚えよう！

- ☐ フェールセーフは安全に落とすこと、フェールソフトは処理を継続すること
- ☐ SANは専用のネットワーク、NASはファイルサーバ

6-3-2 システムの評価指標

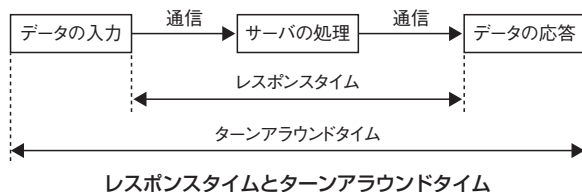
システムの性能や信頼性、経済性などについて総合的に評価するための指標のことを、システムの評価指標といいます。

■ システムの性能特性と評価

システムの性能を評価する性能指標や手法には、次のようなものがあります。

① レスポンスタイム (応答時間)

システムにデータを入力し終わってから、データの応答が開始されるまでの時間です。「速く返す」ことを表す指標です。また、データの入力が始まってから、応答が完全に終わるまでの時間を**ターンアラウンドタイム**と呼びます。



② スループット

単位時間あたりにシステムが処理できる処理数です。「数多く返す」ことを表す指標です。Webシステムの応答性能を求めるときにはレスポンスタイムが、処理性能を求めるときにはスループットがよく用いられます。

③ ベンチマーク

システムの処理速度を計測するための指標です。特定のプログラムを実行し、その実行結果を基に性能を比較します。有名なベンチマークとしては、TPC (Transaction Processing Performance Council: トランザクション処理性能評議会) が作成している **TPC-C** (オンライントランザクション処理のベンチマーク) があります。ほかに、SPEC (Standard Performance Evaluation Corporation: 標準性能評価法人) が作成している

SPECint（整数演算を評価）、SPECfp（浮動小数点演算を評価）があります。

④モニタリング

システムを実際に稼働させて、その性能を測定する手法です。システムの性能改善時に用いられます。

■信頼性指標

信頼性指標は、システムの信頼性を表す指標です。代表的なものを以下に挙げます。

①MTBF（Mean Time Between Failure：平均故障間隔）

故障が復旧してから次の故障までにかかる時間の平均です。連続稼働できる時間の平均値にもなります。

②MTTR（Mean Time To Repair：平均復旧時間）

故障したシステムの復旧にかかる時間の平均です。

③稼働率

ある特定の時間にシステムが稼働している確率です。次の式で計算されます。

$$\text{稼働率} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}$$

④故障率

故障率という言葉は2通りの意味で使われます。

一つ目は稼働率の反対で、ある特定の時間にシステムが稼働していない確率です。不稼働率とも呼ばれるもので、以下の式で計算されます。

$$\text{故障率} = (1 - \text{稼働率})$$

二つ目は、単位時間内にどの程度の確率で故障するかを表したものです。こちらはMTBFを使用し、以下の式で計算されます。

$$\text{故障率} = \frac{1}{\text{MTBF}}$$

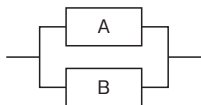
信頼性計算

信頼性，特に稼働率の計算については，複雑なものがたくさん出題されます。基本的な計算方法を押さえておきましょう。

①並列システム

機器を並列に並べたシステムは，どれか一つが稼働していれば全体で稼働していることになるので，稼働率が向上します。

下の図のようなA，B二つの機器がある並列システムで，それぞれの稼働率がa，bだとします。このシステムは，A，Bのいずれも動かないとき以外は動くので，Aの不稼働率 $(1-a)$ とBの不稼働率 $(1-b)$ を用いて，稼働率は $1 - (1-a)(1-b)$ となります。



②直列システム

機器を直列に並べたシステムは，すべて稼働していなければ全体で稼働しないので，稼働率が低下します。

下の図のようなA，B二つの機器がある直列システムで，それぞれの稼働率がa，bだとします。このシステムは，A，Bのどちらも動くときだけ稼働するので，稼働率は $a \times b$ となります。



システムの経済性の評価

システムの経済性を評価するときには，システムを導入するときの初期コスト（**インシャルコスト**）だけでなく，運用コスト（**ランニングコスト**）も考えることが大切です。

ランニングコストも含めた，システムに必要な総コストのことを**TCO**（Total Cost of Ownership）といいます。TCOを意識し，システムの経済性を考えることが大切です。

覚えよう！

- ☐ 応答性能はレスポンスタイムで，処理性能はスループットで測定
- ☐ 並列処理の稼働率は $1 - (1-a)(1-b)$ ，直列処理の稼働率は $a \times b$

6-3-3 演習問題

問1 最も軽減される作業

CHECK ▶ ☐☐☐

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2 ストアドプロシージャ

CHECK ▶ ☐☐☐

クライアントサーバシステムにおいて、クライアント側からストアドプロシージャを利用したときの利点として、適切なものはどれか。

- ア クライアントとサーバの間の通信量を削減できる。
- イ サーバ内でのデータベースファイルへのアクセス量を削減できる。
- ウ サーバのメモリ使用量を削減できる。
- エ データベースファイルの格納領域を削減できる。

問3 フェールセーフ

CHECK ▶ ☐☐☐

フェールセーフ設計の考え方に該当するものはどれか。

- ア 作業範囲に人間が入ったことを検知するセンサが故障したとシステムが判断した場合、ロボットアームを強制的に停止させる。
- イ 数字入力フィールドに数字以外のものが入力された場合、システムから警告メッセージを出力して正しい入力を要求する。
- ウ 専用回線に障害が発生した場合、すぐに公衆回線に切り替え、システムの処理能力が低下しても処理を続行する。
- エ データ収集システムでデータ転送処理に障害が発生した場合、データ入力処理だけを行い、障害復旧時にまとめて転送する。

問4 スループット

CHECK ▶ ☐☐☐

スループットに関する記述のうち、適切なものはどれか。

- ア ジョブの終了と次のジョブの開始との間にオペレータが介入することによってシステムに遊休時間が生じて、スループットには影響を及ぼさない。
- イ スループットはCPU性能の指標であり、入出力の速度、オーバヘッド時間などによって影響を受けない。
- ウ 多重プログラミングはターンアラウンドタイムの短縮に貢献するが、スループットの向上には役立たない。
- エ プリンタへの出力を一時的に磁気ディスク装置に保存するスプーリングは、スループットの向上に役立つ。

問5 メッセージが出始めるまでの経過時間

CHECK ▶ ☐☐☐

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6 TCO

CHECK ▶ ☐☐☐

システムの費用を表すTCO（総所有費用）の意味として、適切なものはどれか。

- ア 業務システムの開発に関わる費用の総額
- イ システム導入から運用及び維持・管理までを含めた費用の総額
- ウ システム導入時の費用の総額
- エ 通信・ネットワークに関わるシステムの運用費用の総額

■ 解答と解説

問1

(平成28年秋 情報セキュリティマネジメント試験 午前 問45)

《解答》ア

Webブラウザは、クライアントのPCには最初から入っており、専用のアプリケーションのようにクライアント1台1台に導入する必要がありません。そのため、クライアント環境の保守が大幅に軽減されます。したがって、アが正解となります。

イ サーバ環境は変わらないので、作業は変わりません。

ウ データベース環境は変わらないので、作業は変わりません。

エ Webブラウザのシステムでもログインは必要なので、作業は変わりません。

問2

(平成27年春 基本情報技術者試験 午前 問27)

《解答》ア

ストアドプロシージャは、データベースの一連の処理をまとめたもので、アプリケーションから命令を発行して呼び出します。あらかじめ“SP_処理”のような名前で一連の処理を登録しておき、その名前で呼び出すことによって処理を実行でき、通信量の削減が可能です。したがって、アが正解です。

イ、ウ、エは、ストアドプロシージャを利用しても削減できません。

問3

(平成26年春 基本情報技術者試験 午前 問15)

《解答》ア

フェールセーフとは、システムに障害が発生したときに安全側に制御する方法です。信号が故障したときにはとりあえず赤を点灯させるなど、障害が新たな障害を生まないように制御します。処理を強制的に停止させることもあります。したがって、アが正解です。

イ フールプルーフの説明です。

ウ、エ フェールソフトの説明です。

問4

(平成26年春 基本情報技術者試験 午前 問14)

《解答》エ

スループットとは、単位時間あたりにシステムが処理できる処理数です。「数多く返す」ことを表す指標です。Webシステムの応答性能を求めるときにはレスポンスタイムが、処理性能を求めるときにはスループットがよく用いられます。

スプーリングは、メモリやディスク装置などのバッファに出力内容を保存し、出力装置が処理を受け付けられるようになったら出力を行う方法です。印刷時の印刷スプーリングが一般的な例となります。したがって、エが正解です。

ア 遊休時間が生じることで、スループットに影響が出ます。

イ 入出力の速度、オーバヘッド時間に影響を受けます。

ウ 多重プログラミングは、ターンアラウンドタイムの短縮に貢献すると同時に、スループットの向上にも役立ちます。

問5

(平成28年春 情報セキュリティマネジメント試験 午前 問43)

《解答》エ

コンピュータシステムに対して指示してから、最初の処理結果が出始めるまでの時間をレスポンスタイム(エ)、最後の処理を受け取るまでの時間をターンアラウンドタイム(ウ)といます。したがって、エが正解です。

アのアクセスタイム(アクセス時間)は、CPUが記憶装置にデータの書き込みを行うのに必要な時間、イのサイクルタイムは、繰り返し処理で一連のサイクルを実施するのにかかる時間です。

問6

(平成27年春 基本情報技術者試験 午前 問58)

《解答》イ

TCO (Total Cost of Ownership) は、運用管理などのランニングコストを含めたすべてのコストです。したがって、イが正解です。

アやウのように、導入や開発に要する費用だけでなく、それらすべてを含めたコストになります。エは運用管理の総額ですが、それだけでなく、すべてのコストの合計がTCOです。

第7章

ストラテジ

ストラテジ系の内容は、企業の経営やシステム開発など、情報セキュリティを守る上で必要な環境を考えるのに役立ちます。

この章では、ストラテジ系の分野である、企業活動、システム戦略、システム企画の3分野について学びます。

企業活動では、組織論や会計など、企業で行う活動について学びます。
システム戦略・システム企画では、情報システムの導入に関する知識を、利用者・経営者の立場から学びます。

7-1 企業活動

- ◆ 7-1-1 経営・組織論
- ◆ 7-1-2 OR・IE
- ◆ 7-1-3 会計・財務
- ◆ 7-1-4 演習問題

7-2 システム戦略

- ◆ 7-2-1 情報システム戦略
- ◆ 7-2-2 業務プロセス

◆ 7-2-3 ソリューションビジネス

- ◆ 7-2-4 システム活用促進・評価
- ◆ 7-2-5 演習問題

7-3 システム企画

- ◆ 7-3-1 システム化計画
- ◆ 7-3-2 要件定義
- ◆ 7-3-3 調達計画・実施
- ◆ 7-3-4 演習問題

7-1 企業活動

企業は、部品や材料など必要なものを調達し、それを消費者のニーズに合ったものに変えて提供します。そのためには資金や人員が必要になるので、資金調達をしたり従業員を雇用したりします。こういった活動が企業活動です。



勉強のコツ

会計・財務の分野がポイントとなります。利益の計算、経営分析の方法など、会計・財務の基本を押さえておきましょう。
用語はほかの分野と重なる部分も多いので、復習も兼ねて知識を身に付けていきましょう。

動画

ストラテジ(経営戦略)の分野についての動画を以下で公開しています。
<http://www.wakuwakuacademy.net/itcommon/8PPMや競争地位別戦略など、経営戦略分野の定番用語について詳しく解説しています。>
本書の補足として、よろしければご利用ください。



発展

一つの取引しか行わない期間のある企業の場合は、収支を精算して終わりになります。しかし、ゴーイングコンサーンを前提にすると企業に終わりはないので、収支の算出は、一定期間ごとに意図的に行う必要があります。それが会計期間です。

7-1-1 経営・組織論

企業は、企業理念の下、その会社の目的を実現するために企業活動を行います。その際に大切になる経営資源には、ヒト・モノ・カネ・情報の四つがあり、これを管理するのが経営管理です。

企業経営

企業は営利活動を行う組織ですが、単に利益を追求するだけでなく、企業理念をもち、CSR (Corporate Social Responsibility : 企業の社会的責任) を果たすことも重要です。また、地球環境に配慮したIT活用を行うグリーンITの思想も大切です。

法人化された企業を会社と呼びますが、現在、日本で設立できる会社の形態は、合資会社、合名会社、合同会社(LLC : Limited Liability Company)、株式会社の4種類です。株式会社では、市場で株式の売買を行えるよう、株式公開(IPO : Initial Public Offering)ができます。

企業の特徴

企業が将来にわたって無期限に事業を継続することを前提とした考え方が**ゴーイングコンサーン**(継続的事業体)です。そして、企業の特長や個性を明確に提示し、共通したロゴやメッセージなどを発信することで社会に向けたイメージを形成していくことをコーポレートアイデンティティといいます。また、企業は一般投資家や株主、債権者などに情報を開示する必要があります。その投資家向け広報がIR (Investor Relations)です。

そして、企業は1社だけで活動するのではなく、様々な利害関係者との相互作用で成り立っています。そのため、企業に対す

る利害関係者の視点から、企業経営の社会性や政治性を確保する必要があります。この考え方を**コーポレートガバナンス**といい、企業の経営者が適切にマネジメントを行っているかをチェックします。

■ ヒューマンリソースマネジメント

経営管理においては、**ヒューマンリソースマネジメント** (HRM: Human Resource Management: 人的資源管理) が非常に重要です。HRMには、人事管理や労務管理だけでなく、組織の設計や教育・訓練、報酬体系の設計、福利厚生など様々な内容が総合的に含まれます。

従来は能力主義だった人事制度は徐々に、具体的な成果を基準とする成果主義に変わってきました。成果主義ではMBO (Management by Objectives: 目標管理制度) などが導入され、評価の公平性や透明性を上げています。

さらに、従業員の**コンピテンシ**に重点を置き、コンピテンシの高い人材を採用する、またコンピテンシで従業員を評価するといった概念の導入も進んでいます。

■ 行動科学

企業組織での人間行動に影響する理論として、**マズローの欲求段階説**があります。これは、人間の欲求を低次のものから挙げると、

1. 生理的欲求
2. 安全欲求
3. 所属と愛の欲求
4. 承認欲求
5. 自己実現欲求

の五つであり、低次の欲求が満たされるとより高次の欲求へと段階的に移動するという考え方です。

また、別の側面からの理論に**XY理論**があります。

X理論とは、「人間は本来ナメケモノなので、放っておくと仕事をしない。だから命令や懲罰で管理する必要がある」という考え方です。

Y理論は、「人間は本来進んで働きたがる生き物であり、自己



コンピテンシとは、高い業務成果を生み出す顕在化された個人の行動特性です。職種別に高い業績を上げている個人の行動特性(例えば「ムードメーカー」「論理思考」など)を分析し、その行動特性を評価基準として従業員を評価します。



CEO、CIO という呼び方は米国由来のもので、日本では法的な効力はもちません。日本では、最高責任者は**代表取締役**となります。

実現のために自ら行動する」という考え方です。低次の欲求が満たされている現代では、Y理論に基づいた経営手法が望ましいとされています。

■ 経営者の職能

経営者の職能のうち、すべての業務を統括する役員のことを**CEO** (Chief Executive Officer：最高経営責任者)といいます。また、情報を統括する役員は**CIO** (Chief Information Officer：最高情報責任者)です。情報セキュリティ関係の役職としては、**CISO** (Chief Information Security Officer：最高情報セキュリティ責任者)、**CPO** (Chief Privacy Officer：最高個人情報保護責任者)があります。

■ 経営組織

経営組織の構造には、経営者、部長、課長、平社員といった**階層型組織**や、人事、営業、システムなどの職能で分ける**職能別組織**、製品やサービスごとに事業部を分ける**事業部制組織**などがあります。また、職能別組織と事業部制組織を合わせた**マトリックス組織**という形態もあります。さらに、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一時的に活動する**プロジェクト組織**という形態もあります。

■ 経営環境の変化

社会環境の変化により、仕事だけを一生懸命するのではなく、**ワークライフバランス**に考慮した勤務形態を実現する必要性が出てきました。そのために、本拠地から離れた場所に設置し遠隔勤務を可能とするサテライトオフィスや、自宅でビジネスを行う**SOHO** (Small Office Home Office) といった形態が発展してきました。

また、国際化により、ステークホルダ(利害関係者)に対して、経営や財務の状況など各種の情報を公開する**ディスクロージャ**や、企業が株主から委託された資金を適正な使途に配分し、その結果を説明する責任があるとする**アカウンタビリティ**も重視されるようになっていきます。そして投資家も、単に利益を追求するのではなく、経営陣に対してCSRに配慮した経営を求めていく



ワークライフバランスとは、1人1人が仕事上の責任を果たすとともに、家庭や地域生活などにおいても多様な生き方を実現できるようにするという考え方です。仕事と生活を調和させ、仕事のために他の私生活を犠牲にしないようにする必要があります。

SRI (Socially Responsible Investment : 社会的責任投資) を行う必要があります。また、地球環境と調和した企業経営を行う環境経営という考え方もあります。

▶▶ 覚えよう！

- ☐ 企業の経営を監視する仕組みがコーポレートガバナンス
- ☐ SRIでは、CSRに配慮した企業に投資する

7-1-2 OR・IE

企業経営では、オペレーションズリサーチ (OR) やインダストリアルエンジニアリング (IE) の手法が用いられます。

OR・IE

オペレーションズリサーチ (OR: Operations Research) とは、数学的・統計的モデルやアルゴリズムなどを利用して、様々な計画に対して最も効率的な方法を決定する技法です。

インダストリアルエンジニアリング (IE: Industrial Engineering) とは、企業が経営資源をより効率的・効果的に運用できるよう、作業手順や工程、管理方法などを分析・評価して、改善策を現場に適用できるようにする技術です。生産工学、経営工学などと訳されます。

以降で、OR・IEの代表的な手法を見ていきます。

線形計画法

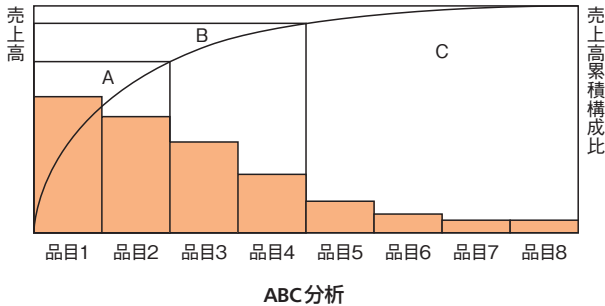
ORの手法の一つに線形計画法 (LP: Linear Programming) があります。線形計画法とは、いくつかの一次式を満たす変数の中で、ある一次式を最大化または最小化する値を求める方法です。

在庫管理

在庫管理の考え方には、一定期間ごとに発注を行う**定期発注方式**と、一定量の発注を行う**定量発注方式**の2種類があります。

在庫は、もっているだけで在庫費用がかかります。そのため、定期発注方式の場合は、発注費用と在庫費用を最小化する**EOQ** (Economic Ordering Quantity: 経済的発注量)、または発注ロットサイズを考えることが重要です。定量発注方式の場合には、在庫がこの数を切ったら発注するという発注点を考えることが大切になります。

また、どの商品を在庫としてもつか、集中して管理するかということも在庫管理では重要です。**ABC分析**では、商品を売上高が多い順にA, B, Cの三つに分類し、能率的に管理を行います。品目、売上高、売上高累積構成比をグラフにすると、おおよそ次のようになります。



■ ゲーム理論

ゲーム理論とは、ある特定の条件下において、互いに影響を与え合う複数のプレイヤーの間での意思決定の考え方を研究するものです。ビジネスの分野でも、競争相手がいる場合にはゲーム理論を応用できる場面はいろいろあります。ゲーム理論では、ゲームを支配するルールを決め、その行動戦略がいくつかあり、プレイヤーがそれを選択する、という枠組みの中でどう意思決定すると利得(利益などの効用)を最大化できるかを考えます。

戦略の例として、毎回同じ行為をする**純粋戦略**と、毎回異なった行為をする**混合戦略**があります。意思決定を行う際の判断基準には、最悪の場合の利得を最大とする**マクシミン原理**、最良の場合の利得を最大とする**マクシマックス原理**があります。また、各プレイヤーが自己の利得を最大化することを考え、どのプレイヤーも戦略変更によってより高い利得を得ることができなくなった戦略の組合せのことを**ナッシュ均衡**といいます。

■ 検査手法

検査を行うときに、あるロットのすべての物品を調べるのではなく、抜取検査として少数の標本を抜き取り(**サンプリング**)、それを調べることがあります。しかし、単純に不良品がn個以下のロットを合格とすると、抜き取り方によって品質にばらつきが出てしまうので、そのロットの合格確率を統計的に求めます。

このとき、横軸にロットの不良率、縦軸にロットの合格確率をとった曲線を**OC** (Operating Characteristic : 検査特性) 曲線といいます。OC曲線を見れば、ある不良率をもったロットがどの程度の確率で合格するのかを判断できます。

品質管理手法

品質管理手法において、主に定量分析に用いられるものがQC七つ道具、主に定性分析に用いられるのが新QC七つ道具です。それぞれの構成を以下に示します。

【QC七つ道具】

①層別

母集団をいくつかの層に分割することです。

②ヒストグラム

データの分布状況を把握するのに用いる図です。データの範囲を適当な間隔に分割し、度数分布表を棒グラフ化します。



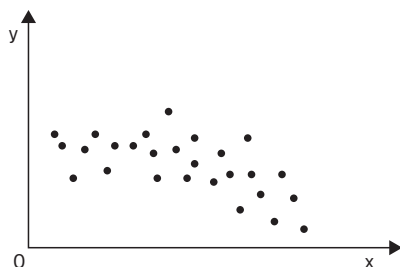
パレート図では、出現頻度の順に層別を比較します。ABC分析では、品目ごとに売上高を比較します。扱うものは違いますが、重要なものを見つけ出して重点を置くという考え方は同じです。

③パレート図

項目別に層別して、出現頻度の高い順に並べるとともに、累積和を示して、累積比率を折れ線グラフで表す図です。前述したABC分析とほぼ同様の図になります。

④散布図

二つの特性を横軸と縦軸とし、観測値をプロット(配置)します。相関関係や異常点を探るのに用いられます。



散布図の例

点の散らばり方に直線的な関係があるときには、 x と y の間に相関があるといわれます。右肩上がりのときは**正の相関**、右肩下がりのときは**負の相関**です。統計分析によって相関係数を求めることもあります。正の相関のときには相関係数は正、負の

相関のときには相関係数は負になります。

⑤特性要因図

ある特性をもたらす一連の原因を階層的に整理する手法です。矢印の先に結果を記入して、因果関係を図示します。

⑥チェックシート

事実を区分して、詳しく定量的にチェックするためにデータをまとめてグラフ化する手法です。

⑦管理図

連続した量や数値などのデータを時系列に並べ、異常かどうかの判断基準を管理限界線として引いて管理する図です。

【新QC七つ道具】

①親和図法

多くの散乱した情報から、言葉の意味合いを整理して問題を確定する手法です。

②連関図法

問題が複雑にからみ合っているときに、問題の因果関係を明確にすることで原因を特定する手法です。

③系統図法

目的と手段を多段階に展開する手法です。

④マトリックス図法

目的とその手段など、二つの関係を行と列の二次元に表し、行と列の交差点に二つの関係の程度を記述します。複数の関連を多角的に整理する手法です。

⑤マトリックスデータ解析法

問題に関係する特性値間の相関関係を手がかりに総合特性を見つけ、個体間の違いを明確にする手法です。

⑥ PDPC (Process Decision Program Chart) 法

プロセス決定計画図と訳され、計画を実行する上で、事前に考えられる様々な結果を予測し、プロセスをできるだけ望ましい方向に導く手法です。

⑦ アローダイアグラム法

クリティカルパス法やPERTで使われている図です。

■ 分析手法

ORやIEで利用される分析手法には様々なものがあります。代表的な分析手法は以下のとおりです。

① 回帰分析

相互関係がある二つの変数の間の関係を統計的な手法で推測します。

② パレート分析

複数の事象などを、現れる頻度によって分類し、管理効率を高める手法です。パレート図を作成して行います。

③ クラスタ分析

対象の集合を似たようなグループに分け、その特徴となる要因を分析する手法です。

④ モンテカルロ法

乱数を用いてシミュレーションや数値演算を行うことで答えを求める手法です。

⑤ デルファイ法

専門家の間でアンケートを使用して質問を繰り返すことで合意を得る方法です。

▶▶ 覚えよう！

- ☐ ABC分析、パレート図では、重要なものに重点を置く
- ☐ 最良の場合の利益を最大にするマクシマックス、最悪の場合の利益を最大にするマクシミン

7-1-3 会計・財務

企業の財政状態や利益を計算するための方法が会計(アカウンティング)です。そして、企業の資金の流れに関する活動が財務(ファイナンス)です。企業会計には、法律に定められた情報公開の仕組みである財務会計と、企業活動の見直しや経営計画の策定に使われる管理会計があります。

■ 売上と利益の関係

企業活動では、売上高=利益となるわけではありません。売上を上げるために様々な費用がかかっているからです。売上を上げるためにかかる費用を**売上原価(原価)**といい、**固定費**と**変動費**に分けられます。固定費は、売上高にかかわらず固定でかかる費用です。変動費は、売上高によって変動する費用で、変動費率として割合を示されることもあります。

また、**売上高-売上原価=売上総利益(粗利益)**です。

利益(売上総利益または営業利益)が0となる点のことを**損益分岐点**といいます。

■ 決算の仕組み

決算とは、一定期間の収支を計算し、利益(または損失)を算出することです。そのために**財務諸表**を作成します。半年ごとの決算を中間決算、3か月ごとの決算を四半期決算といいます。会計基準には日本独自のものもありますが、国際的な会計基準に**IFRS**(International Financial Reporting Standards: 国際財務報告基準)があります。

■ 財務諸表

企業が作成を義務づけられている財務諸表の代表的なものに、**貸借対照表**と**損益計算書**があります。また、上場企業では**キャッシュフロー計算書**も求められます。それぞれの概要は次のとおりです。

①貸借対照表

貸借対照表では、ある時点における企業の財政状態を表します。バランスシート (Balance Sheet : **B/S**) ともいいます。その名のとおり、会社の資産と負債、純資産 (資本) の関係が**資産＝負債＋純資産**となり、完全に等しくなります。

資産	負債
	純資産 (資本)

貸借対照表の構成

②損益計算書

損益計算書では、一定期間における企業の経営成績を表します。利益 (Profit) と損失 (Loss) を表すことから、**P/L**ともいいます。損益計算書では、次のような計算を行います。

売上高	－売上原価	= 売上総利益
さらに	－販売費及び一般管理費	= 営業利益
さらに	＋営業外収益－営業外費用	= 経常利益
さらに	＋特別収益－特別損失	= 税引前当期純利益
さらに	－法人税、住民税及び事業税	= 当期純利益

③キャッシュフロー計算書

キャッシュフロー計算書では、一定期間のキャッシュの増減を表します。具体的には、**営業活動**によるキャッシュフロー、**投資活動**によるキャッシュフロー、**財務活動**によるキャッシュフローの三つに分けて表示されます。

なお、キャッシュフロー計算書の「現金及び現金同等物の期末残高」は、貸借対照表 (期末) の「現金及び預金」の合計額と一致します。

■ 資産管理

資産管理では、在庫や固定資産をどのように管理するかを決めておくことが大切です。棚卸資産評価を行うときには、在庫の取得原価を求める方法を決めます。方法としては、先に取得したものから順に吐き出される**先入先出法**、合計金額を総数で割って平均を求める**総平均法**、仕入れのたびに購入金額と受入数量の合計から単価の平均を計算する**移動平均法**などがあります。

また、設備などの固定資産は、購入した年の経費とするのではなく、利用する期間にわたって費用配分する**減価償却**という考え方があります。減価償却の主な方法には、毎年均等額を減価償却費として計上する**定額法**や、毎年期末残高に一定の割合を掛けて求めた額を減価償却費として計上する**定率法**などがあります。減価償却を行うごとに、固定資産の価値(帳簿価額)は減価償却費の分だけ減少します。固定資産を購入する代わりに、リースやレンタルなどの方法で資産を借りることで、減価償却をせず、かかった費用をすべて経費にすることが可能です。

■ 経営分析

経営分析とは、財務諸表の数値を用いて計算・分析し、企業の収益性や効率性などを評価・判定することです。企業内部の経営者や管理者が行う内部分析は、企業の現状の把握や経営戦略立案に役立っています。企業外部のステークホルダーが行う外部分析は、投資などに役立っています。

経営分析の手法には、**収益性分析**、**安全性分析**、**生産性分析**などがあります。それぞれの分析で用いられる主な指標は、次のとおりです。

1. 収益性指標

企業の収益獲得能力に関する指標です。利益を絶対額ではなく比率として見ることで、企業規模に関係なく比較できます。主な収益性指標には、以下のものがあります。

① ROI (Return on Investment : 投資利益率)

$$\text{ROI} = \frac{\text{利益}}{\text{投資資本}} \times 100 [\%]$$

投資した資本に対して、どれだけの利益を獲得したかを表します。上の式で求められますが、資本の概念、利益の概念によって、利益や投資資本の金額は変わってきます。

② ROA (Return On Assets : 総資産利益率)

$$\text{ROA} = \frac{\text{事業利益}}{\text{総資本}} \times 100 [\%]$$

事業利益とは、営業利益＋受取利息・配当金です。

③ ROE (Return On Equity : 自己資本利益率)

$$\text{ROE} = \frac{\text{当期純利益}}{\text{自己資本}} \times 100 [\%]$$

株主が自ら出資した資本でどれだけの利益を獲得したかを示す指標です。

④ 売上高総利益率(粗利益率)

$$\text{売上高総利益率} = \frac{\text{売上総利益}}{\text{売上高}} \times 100 [\%]$$

売上総利益は粗利ともいいます。企業が提供しているサービスそのものの収益性です。

⑤ 総資本回転率

$$\text{総資本回転率} = \frac{\text{売上高}}{\text{総資本}}$$

総資本をどの程度効率的に使うて売上高を獲得しているかを表す指標です。

2. 安全性指標

企業の支払能力や財務面での安全性に関する指標です。代表的な安全性指標には、以下のものがあります。

①流動比率

$$\text{流動比率} = \frac{\text{流動資産}}{\text{流動負債}} \times 100 [\%]$$

1年以内に現金化できる流動資産がどれくらいあるかを示す指標で、**200%以上**が望ましく、少なくとも**100%以上**あることが必要とされています。

②当座比率

$$\text{当座比率} = \frac{\text{当座資産}}{\text{流動負債}} \times 100 [\%]$$

流動資産を当座資産に置き換え、支払能力をより厳格に評価します。流動比率と当座比率の差が大きいと、将来の資金繰りの悪化が懸念されます。

③固定比率

$$\text{固定比率} = \frac{\text{固定資産}}{\text{自己資本}} \times 100 [\%]$$

固定資産が、負債ではなく自己資本によってどれだけカバーされているかを示します。固定比率は低い方がより安全で、**100%以下**が安全な水準となります。

④固定長期適合率

$$\text{固定長期適合率} = \frac{\text{固定資産}}{\text{自己資本} + \text{固定負債}} \times 100 [\%]$$

固定資産が長期資本によってどれだけカバーされているかを示します。固定長期適合率は**100%以下**であることが必要です。

⑤自己資本比率

$$\text{自己資本比率} = \frac{\text{自己資本}}{\text{総資本}} \times 100 [\%]$$

総資本(負債+自己資本)に占める自己資本の割合です。高い方がより安全です。

3. 生産性指標

企業のインプット(経営資源, 投入量)をどれだけアウトプット(産出量)に変換できたかを表す指標です。主な指標は以下です。

①労働生産性

$$\text{労働生産性} = \frac{\text{付加価値額}}{\text{従業員数}}$$

従業員1人当たりの付加価値(円/人)です。

②資本生産性(設備生産性)

$$\text{資本生産性} = \frac{\text{付加価値額}}{\text{有形固定資産} - \text{建設仮勘定}}$$

資本(生産設備)の投資効率です。

▶▶ 覚えよう!

- ☐ 売上高-売上原価が売上総利益, 管理費を引くと営業利益
- ☐ 固定長期適合率=固定資産÷(自己資本+固定負債)×100

7-1-4 演習問題

問1 CIOの役割

CHECK ▶ ☐☐☐

CIOが経営から求められる役割はどれか。

- ア 企業経営のための財務戦略の立案と遂行
- イ 企業の研究開発方針の立案と実施
- ウ 企業の法令遵守の体制の構築と運用
- エ ビジネス価値を最大化させるITサービス活用の促進

問2 企業活動を監督・監視する仕組み

CHECK ▶ ☐☐☐

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 |

問3 マトリックス組織

CHECK ▶ ☐☐☐

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。

問4 予測技法

CHECK ▶ ☐☐☐

他の技法では答えが得られにくい、未来予測のような問題に多く用いられ、(1)～(3)の手順に従って行われる予測技法はどれか。

- (1) 複数の専門家を回答者として選定する。
- (2) 質問に対する回答結果を集約してフィードバックし、再度質問を行う。
- (3) 回答結果を統計的に処理し、分布とともに回答結果を示す。

- ア クロスセクション法

ウ 親和図法
- イ シナリオライティング法

エ デルファイ法

問5 損益分岐点

CHECK ▶ ☐☐☐

表は、ある企業の損益計算書である。損益分岐点は何百万円か。

単位 百万円		
項 目	内 訳	金額
売上高		700
売上原価	変動費 100	300
	固定費 200	
売上総利益		400
販売費・一般管理費	変動費 40	340
	固定費 300	
営業利益		60

- ア 250

イ 490
- ウ 500

エ 625

問6 財務諸表

CHECK ▶ ☐☐☐

財務諸表のうち、一定時点における企業の資産、負債及び純資産を表示し、企業の財政状態を明らかにするものはどれか。

- ア 株主資本等変動計算書

ウ 損益計算書
- イ キャッシュフロー計算書

エ 貸借対照表

■ 解答と解説

問1

(平成25年春 基本情報技術者試験 午前 問74)

《解答》 **エ**

CIO (Chief Information Officer : 最高情報責任者) は経営から、ビジネス価値を最大化させるITサービス活用の推進を求められます。したがって、**エ**が正解です。

ア CFO (Chief Financial Officer : 最高財務責任者) に求められる役割です。

イ CTO (Chief Technology Officer : 最高技術責任者) に求められる役割です。

ウ CLO (Chief Legal Officer : 最高法務責任者) に求められる役割です。

問2

(平成28年春 情報セキュリティマネジメント試験 午前 問50)

《解答》 **ウ**

企業経営の透明性を確保するために、企業活動を監督・監視する仕組みのことをコーポレートガバナンスといいます。したがって、**ウ**が正解です。

ア 企業の活動分野のうち、競合他社を圧倒的に上回るレベルの能力のことです。

イ 企業戦略の一つで、企業文化の特性や独自性を統一されたデザインやメッセージで発信することです。

エ ある変革を実行に移すとき、そのステークホルダ(利害関係者)を洗い出し、対策を考えることです。

問3

(平成28年秋 情報セキュリティマネジメント試験 午前 問50)

《解答》 **イ**

マトリックス組織とは、職能別組織と事業部制組織を合わせた組織構造で、構成員は、自己の専門とする職能部門と、特定の事業を遂行する事業部門の両方に所属します。したがって、**イ**が正解です。

ア 事業部制組織の説明です。

ウ 職能別組織の説明です。

エ プロジェクト組織の説明です。

問4

(平成26年春 基本情報技術者試験 午前 問70)

《解答》エ

デルファイ法とは、専門家の間でアンケートを使用して質問を繰り返すことで合意を形成する技法です。したがって、エが正解です。

ア 複数の因子の相互関係をある一時点で切って横断的に分析する手法です。

イ 特定の事象の未来予測を物語風に描写する手法です。

ウ 多くの散乱した情報から、言葉の意味合いを整理して問題を確定する手法です。

問5

(平成26年春 基本情報技術者試験 午前 問78)

《解答》エ

損益分岐点とは、利益が0となる点(売上高)のことです。固定費は、売上高にかかわらず固定で掛かる費用、変動費は、売上高によって変動する費用です。変動費については「変動費÷売上高」の計算で変動費率を求められます。

表の値から、変動費は $100 + 40 = 140$ [百万円] なので、変動費率は $140 \div 700 = 0.2$ となります。損益分岐点の売上高を x とすると、次の式で求められます。

$$x - (x \times 0.2 + 200 + 300) = 0, \quad 0.8x = 500, \quad x = 625 \text{ [百万円]}$$

したがって、エが正解です。

問6

(平成25年春 基本情報技術者試験 午前 問77)

《解答》エ

貸借対照表では、一定時点における企業の財政状態を表します。バランスシート (Balance Sheet : B/S) ともいいます。その名のとおり、会社の資産と負債、純資産(資本)の関係が資産=負債+純資産となり、完全に等しくなります。したがって、エが正解です。

ア 株主資本等変動計算書とは、貸借対照表の純資産の部の一会計期間における変動額のうち、主として、株主に帰属する部分である株主資本の各項目の変動事由を報告するために作成されます。

イ キャッシュフロー計算書では、一定期間のキャッシュの増減を表します。

ウ 損益計算書では、一定期間における企業の経営成績を表します。利益 (Profit) と損失 (Loss) を表すことから、P/Lともいいます。

7-2 システム戦略

システム戦略の分野では、経営戦略のうち情報システムに関わる戦略と、組織の業務に関わる情報システムについて学びます。

7-2-1 情報システム戦略

情報システム戦略の目的は、経営戦略を実現させることです。そのため、経営戦略に沿って効果的な情報システム戦略を策定することが重要になります。

情報システム戦略の策定

情報システム戦略の策定では、経営陣の1人であるCIO（Chief Information Officer：最高情報責任者）が中心となり、経営戦略に基づいて全体システム化計画や情報化投資計画を策定します。このとき、自社の状況を知るために、経済産業省が提案した、IT活用度を測る「物差し」であるIT経営力指標を利用することもあります。

全体システム化計画

全体システム化計画では、組織のシステム化全体についての計画を立てます。最初に全体最適化方針を決め、それに基づいて全体最適化計画を立てます。

情報化投資計画

情報化投資計画では、情報化への投資に関する予算を適切に配分します。経営戦略との整合性を考慮して策定することと、投資対効果の算出方法を明確にすることが求められます。情報システムの全体的な業績や個別のプロジェクトの業績を財務的な観点から評価し、ITの投資効果をマネジメントするIT投資マネジメントの観点も大切です。



勉強のコツ

エンタープライズアーキテクチャなどの全体最適化と、SaaS、PaaSなどのクラウドコンピューティングが出題の中心です。経営戦略に沿って全体最適化を行い、情報システムを構築していくという考え方をしっかり押さえておきましょう。

■ 全体最適化方針

全体最適化方針は、組織全体としてどのようにシステム化に取り組むべきかを示す指針です。全体最適化目標を制定し、ITガバナンスの方針を明確にします。To-Beモデルといわれる、情報システムのあるべき姿を明確にした業務モデルを作成します。

■ 全体最適化計画

全体最適化計画は、全体最適化方針に基づき、事業者の各部署において個別に作られたルールや情報システムを統合化し、効率性や有効性を向上させるための計画です。

全体最適化計画では、コンプライアンスを考慮し、情報化投資の方針及び確保すべき経営資源を明確にしてシステムのあるべき姿を定義することなどが求められています。

組織体制としては、情報システムの全体最適化を実現するために**情報システム化委員会**を設置し、**情報化推進体制**を整えます。情報システム化委員会では、情報システムに関する活動全般についてモニタリングを実施し、必要に応じて**是正措置**をとります。また、技術情報の動向に対応するため、**技術採用指針**を明確にすることも大切です。

■ システム化計画

全体システム化計画に従って、個別システム化計画を立案します。企業の戦略性を向上させ、企業全体または事業活動の統合管理を実現するシステムには次のようなものがあります。

① ERP (Enterprise Resource Planning)

ERPは企業資源計画などと訳されます。企業全体の経営資源を統合的に管理して経営の効率化を図るための手法で、これを実現するためのソフトウェアをERPパッケージと呼びます。

② SCM (Supply Chain Management)

SCM (サプライチェーンマネジメント) は、原材料の調達から最終消費者への販売に至るまでの調達→生産→物流→販売の一連のプロセスを、企業の枠を超えて統合的にマネジメントするシステムです。一連のプロセスで在庫、売行き、販売・生産計画

などの情報を共有することで、余分な在庫の削減が可能となり、ムダな物流が減少します。

③ CRM (Customer Relationship Management)

CRMは顧客関係管理などと訳されます。顧客との関係を構築することで顧客満足度を向上させる経営手法です。これを実現するためのシステムがCRMシステムで、詳細な顧客情報の管理や分析、問合せやクレームへの対応などを一貫して管理することが可能になります。

④ SFA (Sales Force Automation)

営業支援のための情報システムです。商談の進捗管理や営業部内の情報共有などを行います。CRMの一環として扱われることも多くなっています。

⑤ KMS (Knowledge Management System)

ナレッジマネジメントを行うためのシステムです。ナレッジマネジメントとは、個人のもつ暗黙知を形式知に変換することにより知識の共有化を図り、より高いレベルの知識を生み出すという考え方です。フレームワークとしてSECIモデルがあり、①共同化 (Socialization)、②表出化 (Externalization)、③結合化 (Combination)、④内面化 (Internalization) の4段階のプロセスが定義されています。

⑥ シェアドサービス

関連する複数の会社が共通して持っている部門 (経理や総務など) をそれぞれ社内から切り離して共同の新会社を設立し、そこで業務を請け負うという形態です。

▶▶ 覚えよう！

- ☐ 全体最適化計画では情報システム化委員会を設立
- ☐ 情報システム戦略は、経営戦略を基に策定

7-2-2 業務プロセス

業務プロセスの改善と問題解決においては、既存の組織構造や業務プロセスを見直し、効率化を図ります。それとともに、情報技術を活用して、業務・システムを最適化します。

業務プロセスの改善手法

業務プロセスの改善手法には、以下のものがあります。

① ビジネスプロセスマネジメント

BPM (Business Process Management) は、業務分析、業務設計、業務の実行、モニタリング、評価のサイクルを繰り返し、継続的なプロセス改善を遂行する経営手法です。

② ビジネスプロセスリエンジニアリング

BPR (Business Process Reengineering) とは、顧客の満足度を高めることを主な目的とし、最新の情報技術を用いて業務プロセスを抜本的に改革することです。品質・コスト・スピードの三つの面から改善し、競争優位性を確保します。

③ ビジネスプロセスアウトソーシング

BPO (Business Process Outsourcing) とは、企業などが自社の業務の一部または全部を、外部の専門業者に一括して委託することです。業務を外に出すことで、経営資源をコアコンピタンスに集中できます。海外の事業者や子会社に開発をアウトソーシングするオフショア開発も一般的です。

④ 業務プロセスの可視化

業務プロセスを可視化するための手法には様々なものがあります。業務流れ図 (WFA: Work Flow Architecture) やBP図 (BPD: Business Process Diagram), E-R図 (ERD: Entity Relationship Diagram) などの手法を用います。また、データの流れを記述するためのDFD (Data Flow Diagram) の手法を用いることもあります。これらによって業務プロセスを把握、分析して問題点を発見し、業務改善の提案を行います。

■ 業務プロセスの改善と問題解決

業務プロセス改善のためのその他の手法としては、システム化による業務効率化が挙げられます。ワークフローシステムを導入し、承認手続きを電子化して、決済処理の効率化を図ることなどによりITを有効活用できます。

また、コミュニケーションのためにシステムを利用することもあります。**SNS** (Social Networking Service)の利用や、業務における電子メール利用方法の改善なども有効です。

▶▶ 覚えよう！

- ☐ BPRは抜本的に改革，BPOは業務をアウトソーシング

7-2-3 ソリューションビジネス

ソリューションビジネスとは、顧客の経営課題をITと付加サービスを通して解決する仕組みです。最新のITを活用して、顧客の経営課題を解決するサービスを提供します。

ソリューションビジネスの種類とサービス形態

ソリューションビジネスでは、顧客の経営課題を解決するサービスを提案するので、業種別、業務別、課題別など様々なサービスがあります。代表的なソリューションサービスの形態としては、クラウドコンピューティングやアウトソーシングサービス、ホスティングサービス、ERPパッケージ、CRMソリューションなどが挙げられます。

クラウドコンピューティング

クラウドコンピューティングとは、ソフトウェアやデータなどを、インターネットなどのネットワークを通じて、サービスというかたちで必要に応じて提供する方式です。

ソフトウェア機能をサービスと見立て、そのサービスをネットワーク上で連携させてシステムを構築する手法にSOA（Service Oriented Architecture：サービス指向アーキテクチャ）があります。この方法により、ユーザの要求に合わせてサービスを提供することができます。

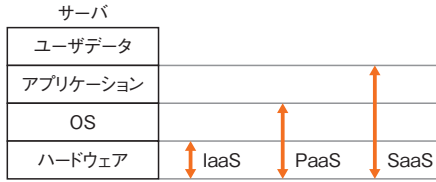
クラウドコンピューティングの形態には、次のようなものがあります。



SaaS, PaaS, IaaS は、クラウドコンピューティングの構成要素にどこまでクラウド側のサービスを利用するかという観点で分類したものです。その他のサービスには、端末のデスクトップ環境をネットワーク越しに提供する **DaaS** (Desktop as a Service) があります。また、SaaSを別の観点から呼んだものとして、**ASP** (Application Service Provider) があります。

- **SaaS** (Software as a Service)
ソフトウェア（アプリケーション）をサービスとして提供する
- **PaaS** (Platform as a Service)
OSやミドルウェアなどの基盤（プラットフォーム）を提供する
- **IaaS** (Infrastructure as a Service)
ハードウェアやネットワークなどのインフラを提供する

図にすると、次のようなかたちになります。



SaaS, PaaS, IaaSで提供される構成要素

▶▶ 覚えよう！

- ☐ SaaSはソフトウェア, PaaSはプラットフォーム, IaaSはインフラを提供
- ☐ 既存の業務をパッケージの業務モデルに合わせる方が効率的

7-2-4 システム活用促進・評価

情報システムを有効に活用し、経営に生かすために、情報システムの構築時から活用促進活動を継続的にを行います。

データ活用

情報システムに蓄積されたデータを分析し、今後の事業戦略に活用します。データマイニング、ナレッジマネジメントなどの手法があります。



データマイニングについては「6-2-5 データベース応用」、ナレッジマネジメントについては「7-2-1 情報システム戦略」を参照してください。

情報システム利用実態の評価・検証

情報システムの投資対効果を分析し、システムの利用実態を調査して評価します。評価指標としては、投資利益率(ROI: Return On Investment)や利用者満足度があります。

普及啓発

PCやインターネットなどの利用においては、使いこなせる人と使いこなせない人に生じる格差(デジタルディバイド)ができてしまいがちです。そのため、情報システムを活用するためには、各人に合わせた教育・訓練の実施などで、全社員のコンピュータリテラシ(コンピュータを活用する能力)を向上させるための普及啓発活動を行う必要があります。また、人材育成計画を立て、講習会などを開いて利用方法を説明します。



システムライフサイクルとは、システムの設計や構築、運用などの一連のシステム利用の流れのことです。使用が終わったシステムを廃棄するところまでがシステムライフサイクルとなります。

情報システム廃棄

システムライフサイクルの最後には、情報システムを廃棄する必要があります。廃棄の際は、システムを最終の状態にし、起動不能にする、解体する、データを消去するなどの作業を行います。このとき、単純にデータを消すだけではディスク上に残ることがあるので、無意味なデータを上書きするなどの作業が必要です。

覚えよう！

- ☐ 情報システムの評価に投資対効果分析を行う
- ☐ 廃棄時には、データの消去を、データを上書きすることで行う

7-2-5 演習問題

問1 BPO

CHECK ▶ ☐☐☐

BPOの説明はどれか。

- 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

問2 必要な機能だけオンラインで利用するもの

CHECK ▶ ☐☐☐

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と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

問3 ナレッジマネジメント

CHECK ▶ ☐☐☐

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フラット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 他社にはまねのできない、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。

■ 解答と解説**問1**

(平成28年秋 情報セキュリティマネジメント試験 午前 問48)

《解答》 **イ**

BPO (Business Process Outsourcing) とは、企業などが自社の業務の一部または全部を、外部の専門業者に一括して委託することです。社内業務のうちコアビジネスでない事業を委託するので、**イ**が正解です。

ア BCP (Business Continuity Planning) の説明です。

ウ MRP (Material Requirement Planning) の説明です。

エ プロジェクトマネジメントの説明です。

問2

(平成28年春 情報セキュリティマネジメント試験 午前 問47)

《解答》 **イ**

インターネット経由で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(サービス)を利用する仕組みを、SaaS (Software as a Service)といいます。したがって、**イ**が正解です。

ア 統合基幹業務システム (Enterprise Resource Planning) で、企業の資源を統合的に管理するものです。

ウ サプライチェーンマネジメント (Supply Chain Management) で、業界の流れを統合的に見直し、プロセス全体の効率化を図るものです。

エ 拡張可能な事業報告言語 (eXtensible Business Reporting Language) で、XMLをベースにしたビジネスレポートなどを電子文書化するときに使う規格です。

問3

(平成27年春 基本情報技術者試験 午前 問70)

《解答》 **ア**

ナレッジマネジメントとは、個人のもつ暗黙知を形式知に変換することにより知識の共有化を図り、より高いレベルの知識を生み出すという考え方です。したがって、**ア**が正解です。

イ フラット型組織の説明です。

ウ ベンチマーキングの説明です。

エ コアコンピタンス経営の説明です。

7-3 システム企画

システム企画で扱う内容は、システム化計画、要件定義、調達計画・実施です。システムの開発者ではなくシステムを発注する側の視点で、システム化を考えます。

7-3-1 システム化計画

システム化構想とシステム化計画では、要求事項を集めて合意し、システム化の方針を決め、システムの実施計画を策定します。

■ システム化構想の立案

システム化構想の立案では、経営要求・課題の確認、現行業務・システムの調査分析、情報技術動向の調査分析、対象となる業務の明確化、業務の新全体像の作成、システム化構想の文書化と承認、システム化推進体制の確立など、様々なことを行います。

経営層や各部門などいろいろな方向からシステムに関係する要求事項が集められ、合意をとります。

■ システム化計画の立案

システム化計画の立案での目的は、システムを実現するための実施計画を得ることです。全体システム化計画、個別システム化計画を行うことによって全体最適化を図ります。また、システムの目的や適用範囲、開発範囲を決め、業務モデルを作成します。サービスレベルと品質に対する基本方針や開発プロジェクト体制も策定します。

システム化計画における検討事項には次のものがあります。

① 全体開発スケジュールの作成

対象となったシステムを必要に応じてサブシステムに分割し、サブシステムごとに優先順位を付けます。また、要員、納期、コスト、整合性などを考え、各サブシステムについて開発スケジュールの大枠を作成します。



勉強のコツ

システムを開発する側の視点ではなく、発注する側の企業の視点で、システム開発について知っておくべき内容をまとめています。RFI、RFPなど、調達に関する用語を学ぶことがポイントです。

②要員教育計画

業務・システムに関する教育訓練について、教育訓練体制やスケジュールなどの基本的な要件を明確にします。

③投資の意思決定

経済性計算の手法を利用してより正確な投資の価値を算出し、投資の意思決定を行います。

④開発投資対効果 (IT 投資効果)

システム実現時の定量的、定性的な効果予測を行います。また、期間・体制などの大枠を予測し、費用を見積もります。このとき、IT投資のバランスやシステムライフサイクルを意識します。

⑤情報システム導入リスク分析

導入に伴うリスクの種類や大きさを分析します。リスク分析の対象を決定し、リスクの発生頻度・影響・範囲などを特定し、リスクの種類に応じた損害内容と損害額を算出します。その後、リスクに応じてリスク対策を行います。

▶▶ 覚えよう！

- ☐ システム化構想では、多方面から分析して要求事項を集める
- ☐ システム化計画では、全体の大枠の計画を立てる

7-3-2 要件定義

システムへの要求を洗い出して分析することを要求分析といいます。要求分析の結果をまとめて明確にし、定義するのが要件定義です。

要求分析

要求分析は、要求項目の洗出し、要求項目の分析、ユーザニーズ調査、前提条件や制約条件の整理という手順で行います。このときに、利害関係者から提示されたユーザのニーズや要望を識別し、要求仕様書に整理します。

要件定義

要件定義の目的は、システムや業務全体の枠組みやシステム化の範囲と機能を明らかにすることです。共通フレーム2013の要件定義プロセスでは、プロセス開始の準備、利害関係者の識別、要件の識別、要件の評価、要件の合意、要件の記録の六つのアクティビティが定義されています。

① 要件定義で明確化する内容

要件定義で明確化する内容には、大きく分けて機能要件と非機能要件があります。機能要件は、業務要件を実現するために必要なシステムの機能です。非機能要件とは、機能として明確にされない要件です。また、情報・データ要件や移行要件など、システムに関連する様々な要件についても定義します。

② 要件定義の手法

要件定義の手法には、構造化分析手法やデータ中心分析手法、オブジェクト指向分析手法などがあります。プロセス仕様を明らかにしてDFDなどを記述するのが構造化分析手法です。データ中心分析手法では、E-R図を記述してデータの全体像を把握します。オブジェクト指向分析手法ではUMLを利用します。

③利害関係者への要件の確認

要件定義者は、定義された要件の実現可能性を十分に検討した上で、ステークホルダに要件の合意と承認を得ます。

■非機能要件

非機能要件とは、システム要件のうち、機能要件以外の要件です。その要件に対する要求を非機能要求といいます。機能要求に比べて非機能要求は顧客の意識に上がってこないことが多いため、要求分析時に見落とされやすく、トラブルの原因になりがちです。そのため、意識して非機能要求を洗い出す必要があります。

IPAで公開している「非機能要求グレード」には、以下の六つのカテゴリがあります。

- **可用性**……………システムを継続的に利用可能にするための要求
- **性能・拡張性**……………システムの性能と将来のシステム拡張に関する要求
- **運用・保守性**……………システムの運用と保守のサービスに関する要求
- **移行性**……………現行システム資産の移行に関する要求
- **セキュリティ**……………構築する情報システムの安全性の確保に関する要求
- **システム環境・エコロジー** ……システムの設置環境やエコロジーに関する要求

▶▶ 覚えよう！

- ☐ 要件定義プロセスでは、利害関係者の要求をまとめ合意をとる
- ☐ 非機能要求には、可用性や性能・拡張性、セキュリティなどが含まれる

7-3-3 調達計画・実施

ここでの調達には、開発するシステムに必要な製品やサービスの購入だけでなく、組織内部や外部委託によるシステム開発なども含まれます。開発するシステムの用途、規模、取組方針、前提や制約条件に応じた調達方法を考える必要があります。

調達

調達とは、品物やサービス、労働力などを用意することです。外部資源の利用を行い、必要なものを調達します。情報システムの場合、SI（System Integrator：システムインテグレータ）事業者にアウトソーシングすることも考えられます。

調達を行ったシステム資産及びソフトウェア資産については、ライセンス管理や構成管理などを適切に行い、管理する必要があります。

調達計画

調達計画の策定では、調達の対象、調達の条件、調達の要求事項などを定義します。また、要件定義を踏まえ、既存の製品またはサービスの購入、組織内部でのシステム開発、外部委託によるシステム開発などから調達方法を選択します。

このとき、社内で実施することと社外に委託することを決める内外作基準を作成します。

調達の方法

調達の代表的な方法には、**企画競争入札**や**一般競争入札**があります。企画競争入札では、事業テーマについて企画書などの提出を求め、提案内容を審査します。それに対し、一般競争入札では、提案の内容だけでなく価格も合わせて審査します。

一般競争入札では、技術点や価格点などそれぞれの点数を合計して総合点で入札者を決定する**総合評価落札方式**が用いられます。

■ 情報提供依頼書 (RFI)

調達にあたっては、ベンダ企業に対し、システム化の目的や業務内容を示し、RFP（次項参照）を作成するための情報の提供を依頼する **RFI**（Request For Information：情報提供依頼書）を作成します。ベンダ企業は、RFIに基づいて情報を提供します。

■ 提案依頼書 (RFP)

ベンダ企業に対し、調達対象システム、提案依頼事項、調達条件などを示した **RFP**（Request For Proposal：提案依頼書）を提示し、提案書・見積書の提出を依頼します。RFPには、システムの対象範囲やモデル、サービス要件、目標スケジュール、契約条件、ベンダの経営要件、ベンダのプロジェクト体制要件、ベンダの技術及び実績評価などを含みます。

■ 提案書・見積書

ベンダ企業では、提案依頼書を基にシステム構成、開発手法などを検討し、提案書や見積書を作成して発注元に提案します。このとき、見積りを依頼するために **RFQ**（Request For Quotation：見積依頼書）を作成することもあります。

■ 調達選定

調達先の選定にあたっては、提案評価基準や要求事項適合度の重み付けを行う選定手順を確立する必要があります。このとき、コストや工期だけでなく法令遵守（コンプライアンス）や内部統制などの観点からも比較評価して選定することが大切です。

また、**CSR**（Corporate Social Responsibility：企業の社会的責任）も意識する必要があります。CSRを意識した調達を **CSR調達**といいます。

さらに、製品やサービスなどを調達する際、購入前に必要性を考慮し、環境への負担が少ないものから優先的に選択する **グリーン調達**（グリーン購入）の観点も重要です。



CSRについては、「4-2-3 その他の法律・ガイドライン・技術者倫理」で説明していますので参照してください。

■ 契約締結

契約締結時には、受入システム、費用、受入時期、発注元とベンダ企業の役割分担などを明記する必要があります。また、JISAが発表するソフトウェア開発委託モデル契約、情報システム・モデル取引・契約書などを基に契約書を作成します。必要に応じて、知的財産権利用許諾契約も行います。

■ ファブレス

ファブレスとは、ファブ(fabrication facility：工場)を所有せずに製造活動を行う企業のことです。具体的には、製品の企画設計や開発は行いますが、製造は自社工場で行わず、EMS (Electronics Manufacturing Service：電子機器の受託生産サービス)などを行う企業などに委託します。製品は、**OEM** (Original Equipment Manufacturer：相手先ブランド名製造)での供給を受けるかたちで、自社ブランドとして発売します。

ファブレスが主流になっている業種には半導体産業があります。その他、コンピュータ、食品、玩具、造船業界など様々な業種で見られるようになっています。

■ 調達リスク分析

調達にあたっては、内部統制、法令遵守、CSR調達、グリーン調達などの観点によるリスク管理が必要です。リスクを分析および評価して、対策を立てる必要があります。また、調達のリスクには、信用リスク、事務リスク、風評リスクなど様々なものがあるので、リスクの内容に合わせて個々に対策を考える必要があります。

■ 契約の形態

契約締結のとき、情報システムの取引において業務を委託するかたちで行われる契約には、**請負契約**と**準委任契約**の2種類があります。**請負契約**では、頼んだ仕事を完成させる責任がベンダ企業にあるのに対し、**準委任契約**では、完成責任は発注者側にあり、ベンダ企業には仕事の完成ではなく業務の実施が求められます。



JISA (Japan Information Technology Services Industry Association：情報サービス産業協会)では、情報サービス産業に関連するソフトウェア開発委託モデル契約、情報システム・モデル取引・契約書などのサンプルを公開しています。
<http://www.jisa.or.jp/>

さらに、**派遣契約**と**出向契約**もあります。この二つは業務の委託ではなく、労働力の提供に関する契約で、指揮命令は発注者側が行います。両者の違いは、労働条件（残業するかどうかなど）を受注者（派遣会社など）が決めるのが派遣契約、発注者（出向先企業など）が決めるのが出向契約です。

▶▶ 覚えよう！

- ☐ RFIで情報をもらって、RFPで提案書を提出する
- ☐ 完成させるのが請負契約、業務を行うのが準委任契約

7-3-4 演習問題

問1 企画プロセスで定義するもの

CHECK ▶ ☐☐☐

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2 非機能要件

CHECK ▶ ☐☐☐

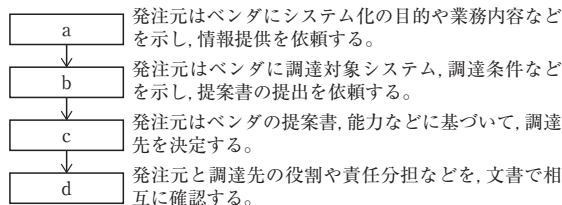
非機能要件の定義で行う作業はどれか。

- ア 業務を構成する機能間の情報(データ)の流れを明確にする。
- イ システム開発で用いるプログラム言語に合わせた開発基準、標準を作成する。
- ウ システム機能として実現する範囲を定義する。
- エ 他システムとの情報授受などのインタフェースを明確にする。

問3 情報システムの調達

CHECK ▶ ☐☐☐

図に示す手順で情報システムを調達するとき、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

■ 解答と解説**問1**

(平成28年秋 情報セキュリティマネジメント試験 午前 問49)

《解答》 **ウ**

企画プロセスでは、システムが関与するシステム化構想の立案、システム化計画の立案などを行います。システム化構想の立案プロセスでは、経営上のニーズや業務上の課題などの事項を明確にします。したがって、**ウ**が正解です。

ア 合意プロセスで明確にします。

イ システム開発プロセス、保守プロセスで明確にします。

エ ソフトウェア構成管理プロセスで明確にします。

問2

(平成26年秋 基本情報技術者試験 午前 問65)

《解答》 **イ**

非機能要件とは、システム要件のうち、機能要件以外の要件です。開発基準、標準などは、システムの運用・保守性を上げるためのもので、非機能要件に該当します。したがって、**イ**が正解です。

ア DFD (Data Flow Diagram) などで行う、機能要件の定義です。

ウ システム要件の定義で行います。

エ ソフトウェア要件定義で行います。

問3

(平成28年春 情報セキュリティマネジメント試験 午前 問48)

《解答》 **イ**

情報システムを調達するときには、まず発注元はベンダに情報提供を依頼するRFI(Request For Information)を示します(a)。続いて、その情報を基に、発注元がベンダに提案書を依頼するRFP (Request For Proposal)を示します(b)。その後、RFPなどを参考に、供給者の選定を行います(c)。最後に、選定した調達先と役割や責任分担などを決め、契約の締結を行います(d)。したがって、bに入るものはRFPとなるので、**イ**が正解です。

第8章

午後問題対策

情報セキュリティマネジメント試験の午後問題は、長文の問題文を読解し、問題の原因や解決策を考えていく内容です。午後問題は3問出題され、全問必須なので、午後問題の解き方を学習し、どのような問題にも対応できるようにしておくことが大切です。

この章では、過去問題を例に、午後問題の解き方を学習していきます。さらに、いくつかの午後問題で問題演習を行い、合格するために必要な、午後問題を解く実力を身につけていきます。

8-1 午後問題の解き方

◆ 8-1-1 午後問題の解き方

8-2 午後問題の演習

◆ 8-2-1 内部不正防止のためのログのレビュー

◆ 8-2-2 標的型攻撃メールの脅威と対策

◆ 8-2-3 情報セキュリティ自己点検

8-1 午後問題の解き方

午後問題は長文なので、読みこなして正確に解いていく必要があります。解き方を理解し、どのようにすれば合格点が取れるのかを知っておくことが大切です。

8-1-1 午後問題の解き方

午後問題では、長文の問題文を把握する必要があるのですが、そのためには、少しずつ確実に読み解いていきます。

問題文(平成28年春 午後 問2)

ここでは、平成28年春 情報セキュリティマネジメント試験 午後 問2を読み解きます。テーマは、業務委託におけるアクセス制御です。

まず、最初の段落を見ていきましょう。

問 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(以下、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。

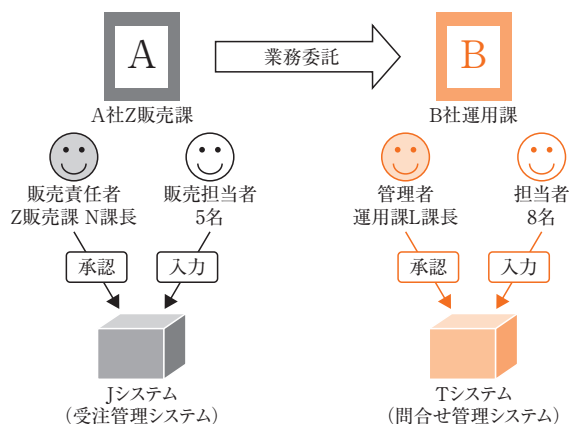
補足：Jシステム及びTシステムはA社の情報システム部が運用している。

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。

最初の段落〔Z販売課の業務〕は、今回の舞台となる通信販売業者A社のZ販売課と、その委託先となるB社運用課の業務についての説明です。なんとなく読み飛ばしがちなのですが、業務委託のアクセス制御を考える上では、その業務の状況を正確に把握することが不可欠です。

ここに書いてあることを、A社、B社という組織とJシステム、Tシステムというシステムを中心に整理すると、次の図のようになります。



実際に図まで書き起こす必要はありませんが、この対応関係をチェックしておくことが次につながります。

それでは、次の段落を見ていきましょう。

〔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	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。

〔Jシステム及びTシステムの操作権限〕について、表1のように操作権限を整理します。この部分を解く上で知っておく必要がある用語としては、「ロール」があります。

ロールはシステム上の役割であり、複数の人が関わる場合でも、「A社販売担当者」などのロールでまとめることで、操作権限を一度に割り当てることが可能となります。

また、問題文を読みながら、**情報セキュリティ対策**としてふさわしいか、この会社で特徴的なところがあるかをチェックします。チェックするためには、あらかじめ情報セキュリティマネジメントやセキュリティ対策などを学習し、ISMSでの一般的なセキュリティ対策手法について知っておく必要があります。

JシステムとTシステムの利用方針は、[方針1][方針2]から、利用者と利用者IDは1対1に対応していることが分かります。これは、利用者アクセスの管理として必要なルールです。

また、[方針3]には、入力と承認を別の人が行うことが記されています。これは、責務の分離を考えており、適切な対策です。



ロールについては「3-4-5 データベースセキュリティ」を参照してください。

さらに、[方針4]に「販売責任者は、Z販売課の全業務の情報を閲覧できる」とあり、販売責任者の権限が強いことが分かります。

この段落で特徴的なのは、「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」という部分です。これは、システム権限の変更が必要となすにすぐに行われず、1日1回しか変更できないことを示しています。迅速にロール設定ができないことを、ここで読み取っておく必要があるのです。

それでは、次の段落を確認していきましょう。

〔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				○	○	
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]を満たしません。別の案ですが、b ようにシステムを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もしておくそう。

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。

今までの委託に加えて、Jシステムでの入力作業を新たに追加で業務委託します。そのため、A社とB社の役割分担を再度見直します。

新しく付与される操作権限は、表2より、「B社管理者」のJシステムの閲覧、入力の権限と、追加されたロール「B社Jシステム担当者」のJシステムの閲覧、入力の権限です。

ここでのポイントは、A社販売責任者はN課長だけなので、Jシステムの承認業務が滞る可能性です。単純にA社販売担当者に承認させることにすると、今までの方針や要求の条件を満たせないで、適切な権限変更を行う必要が出てきます。

続いて、最後の段落を確認していきましょう。

[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、次の手順を定めている。

- (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来月中旬に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。

[B社担当者の追加及び変更]に関する内容です。新たに業務委託したJシステム入力作業を担当するJシステム担当者に対して、Dシステムに対する閲覧権限を設定します。

アクセス権限を考えるとときに大切なのは、リスクを最小限にするために、アクセス権限は必要最小限にするという **Need-to-know (最小権限)** の原則です。この考え方を基に、必要なアクセス権限を設定していきます。

また、適切に変更するための手続や、N課長(A社販売責任者、システム利用部署の長)の役割について問題文から読み取り、整理していく必要があります。適切なロールや権限の変更方法について、A社システムでの対処を考えていきます。

問題文は以上ですが、設問に移る前に、問題の全体像を整理しておきます。

今までの段落の概要と、設問の関係は次のようになります。

段落	概要	設問
[Z販売課の業務]	業務とJシステム、Tシステムの利用者	
[Jシステム及びTシステムの操作権限]	利用方針[方針1]～[方針4] JシステムとTシステムの操作権限	
[受注管理業務の委託]	追加委託の要求1、2と新しい操作権限案	設問1
[B社担当者の追加及び変更]	Dシステムへの閲覧権限の付与	設問2

最初の二つの段落の内容を基に、設問1では[受注管理業務の委託]、設問2では[B社担当者の追加及び変更]について問われています。

設問1

設問1から確認していきましょう。

設問1 [受注管理業務の委託]について、(1) ～ (6)に答えよ。

設問1では、[受注管理業務の委託]について問われています。業務の入力作業をB社に追加で委託するにあたり、新しい操作権限案(表2)を考え、それについて検討していきます。

(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]

ウ [方針2]

オ [方針3]
- イ [方針1], [方針2]

エ [方針2], [方針3]

カ [方針3], [方針4]

(1) では、本文中の下線①「Jシステムで利用方針に違反」について、承認権限を追加することでどの利用方針に違反するかを

考えます。具体的には、[Jシステム及びTシステムの操作権限]の四つの方針について、表2の操作権限で違反が生じるかを考えます。

[方針1], [方針2]

今回の変更はロールとロールに付与される操作権限のみなので、利用者IDの付与には影響はありません。したがって、違反とはなりません。

[方針3]

Jシステムでは、今まではA社販売担当者が入力、A社販売責任者が承認というように権限を分けていたので、「ある利用者が入力した情報は、別の利用者が承認する」という利用方針は満たされていました。しかし、“A社販売担当者”ロールに承認権限を追加すると、A社販売担当者が入力と承認の両方を行えることになるので、利用方針に違反します。

[方針4]

A社販売責任者に対しての権限には変更はないので、問題ありません。

したがって、違反が考えられる利用方針は[方針3]のみなので、オが正解です。

- (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び。

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。

(2)では、[方針3]の利用方針違反が高めるリスクについて問われています。

A社販売担当者が入力と承認の両方を行えるようになると、1

人で注文を入力して承認することが可能となってしまいます。すると、不正に入力された注文がチェックされずに承認されてしまうことが起こります。

したがって、エが正解です。

アの承認されず滞留することや、ウの差し戻されることは、[方針3]の利用方針違反とは関係ありません。また、イの注文情報の窃取は、閲覧権限があれば可能なので、承認権限とは関係ありません。

(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

(3)は空欄a, bの穴埋め問題です。文章の流れに沿って、解答群から二つの案を選び出していきます。

“A社販売担当者”ロールに承認権限を追加した上で、利用方針にも合うものを考えます。なお、下線②より、空欄aの条件は「要求2」を満たさないものであり、これを満たすものが空欄bに入ります。

利用方針[方針3]に合うように、入力と承認の利用者を分けるためには、オの「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」を追加する方法が有効です。しかし、この方法ではA社の販売担当者同士でも別人なら承認が可能となり、[要求2]の「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」を満たせません。

“A社販売担当者”ロールで承認できる注文を、イのように“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

力された注文だけに限ると、[方針3]の入力と承認の利用者を分けるという条件を満たせると同時に、[要求2]を満たすことができます。

したがって、空欄aがオ、空欄bがイとなります。

アは、販売責任者が2人になるということなので、システムだけでは解決できません。ウ、エは、今回の委託業務の変更とは関係ありません。

- (4) 本文中の下線②について、なぜ 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、 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、自分宛て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。

8

(4)では、空欄a(オ)の方法では[要求2]を満たせない理由が問われています。

(3)で説明したとおり、「他の利用者IDによって入力された注文だけを承認」という制限だけでは、“A社販売担当者”ロールの利用者が複数人いるとき、2人で協力して入力、承認を行うことが可能となります。つまり、1人が入力し、別の1人が承認することができるため、[要求2]にあるA社の販売責任者の承認が不要となります。したがって、ウが正解です。

ア、エのようなB社に関する権限については問題ありません。イの承認依頼に気づくかということは、権限の話とは関係ありません。

- (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社販売責任者”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。

(5)では、下線③の「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」について、代行者をどうするかを考えます。

利用方針の[方針3]より、入力と承認は別の人が行う必要がありますが、アのように、“A社販売責任者”ロールをA社の担当者に割り当ててしまうと、この方針が満たせなくなります。

同様に、イでもA社の担当者に入力と承認の両方の権限が割り当てられるので、[方針3]が満たせません。

ウのように、N課長の利用者IDやパスワードを別の人が運用することは、[方針2]の「一つの利用者IDは、1人の利用者だけが利用する」に違反します。

エのように、N課長の上長なら、A社販売担当者ではないので、入力と承認の権限が重なることはありません。そのため、上長の利用者IDに“A社販売責任者”ロールを設定して代行してもらうことに問題はありません。

したがって、利用方針に合致するのはエとなります。

- (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。

(6)では、本文中の下線④にある、B社の担当者の一部が応援できるように「必要な操作権限を与える方法」を考えます。

B社Tシステム担当者は、通常はTシステムを担当していますが、問合せ数が少ない時間帯に、応援としてJシステムも利用することになりました。そこで、B社応援担当者に新しいロールを定義し、そのロールに“B社Tシステム担当者”と“B社Jシステム担当者”の両方の権限をもたせる必要があります。したがって、イの新しいロールの定義が正解となります。

ア、エのような、応援の都度、切り替えて行う運用は、[Jシステム及びTシステムの操作権限]に、利用者IDに対するロール設定は「翌営業日の朝5時に自動的にシステムに反映」とあり、必要に応じた即時の対応ができないことから適切ではありません。ウの“B社管理者”ロールはTシステムへの入力ができないため、業務に支障が出ます。

設問2

続いて、設問2を見ていきます。

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。

設問2は、[B社担当者の追加及び変更]についての問題です。
B社担当者の追加や変更を行う場合に必要手続きや運用について問われています。

(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

(1)は、空欄cの穴埋め問題です。利用部署が、業務委託先要員への閲覧権限の付与を希望する場合の申請方法について問われています。

[B社担当者の追加及び変更](3)に、「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」とあります。また、業務委託先要員の監督責任は利用部署にあるので、業務委託先の管理者から利用者の情報を入手し、確認する必要があります。そのため、利用部署が業務委託先要員への閲覧権限の付与を希望する場合は、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いて、情報のオーナー部署の長に申請する必要があります。したがって、エが正解です。

アのように、業務委託先の管理者と情報のオーナー部署が直接

やり取りすることはありません。また、業務を依頼するのは利用部署なので、イやウのように、業務委託先から申請を行うこともありません。

(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

(2) は、空欄 d ～ f の穴埋め問題です。それぞれ見ていきます。

空欄 d

D システムの閲覧権限を見直して必要最小限にすることは、B 社 J システム担当者からの情報漏えいを防ぐことに当たり、これにより内部不正のリスクが低減されます。したがって空欄 d は **アの内部不正** となります。

空欄 e

閲覧権限の付与に関しては、[B 社担当者の追加及び変更] (4) の空欄 c の解答より、利用部署の長が情報のオーナー部署の長に申請する必要があります。ここでは、利用部署の長である N 課長は、情報のオーナー部署の長に対して申請するので、空欄 e は **ウの情報のオーナー部署の長** となります。

空欄 f

B 社の担当者変更に関しては、[B 社担当者の追加及び変更] (4) の空欄 c の解答より、利用者の情報を業務委託先の管理者から提供してもらう必要があります。業務委託先は B 社なので、情報提供は B 社の管理者が行います。したがって、空欄 f は **アの B**

社の管理者となります。

- (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び。

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にしておく。
- 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、直ちに退任予定者の利用者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。

(3)では、本文中の下線⑤「来月中に1人が退任し1人が新規に着任する」ことに対応するために必要な利用者ID管理の手続を考えます。

[Jシステム及びTシステムの操作権限]の利用方針のうち、[方針1]と[方針2]を満たすためには、退任者と新任者それぞれに利用者IDを割り当てます。また、引継ぎ期間は同時にTシステムとDシステムを利用するので、この業務に支障が出ないようにし、なおかつ必要最小限の権限となるようにする必要があります。そのためには、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を無効化することが有効です。したがって、ウが正解となります。

ア 退任者の利用者IDは、不要になったら直ちに無効化する必要があります。

イ 利用者IDの引継ぎは、利用方針[方針2]に反します。

エ 引継ぎ開始時に退任予定者の利用者IDを無効化すると、引継ぎ業務に支障が出てしまいます。

- (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 |

(4)では、本文中の下線⑥について、担当者変更のために受領する情報として不要なものを考えます。

(3)の利用者ID管理の手続を行うためには、無効化する退任者の利用者IDと、新任者の着任予定日、退任者の退任予定日は必要となります。しかし、新任者の閲覧希望情報については、閲覧する情報は業務を引き継ぐだけなので退任者と変わらず、またどの情報を閲覧させるのかを決めるのは利用部署の長(今回はN課長)なので、申請を受け取る必要はありません。したがって、不要なものは**アの新任者の閲覧希望情報**となります。

イ、ウ、エは、担当者変更のために必須となる情報です。

この問題は以上です。長い文章ですが、段落に分けて全体像を見ながら、一つ一つていねいに読み解いていけば確実に解答を導くことができます。他の問題も同様に解くことができるので、演習を重ね、合格できる実力を身につけていきましょう。

解答

- 設問1 (1) オ (2) エ (3) a オ b イ
 (4) ウ (5) エ (6) イ
- 設問2 (1) エ (2) d ア e ウ f ア
 (3) ウ (4) ア

採点講評

問2は、業務の一部を外部委託する状況での情報システムにおけるロールベースアクセス制御(RBAC)について出題した。

設問1は、情報システムの利用方針と業務上の要求事項の両面を踏まえ、ロールに設定する適切な操作権限を検討するという設問であり、(5)、(6)の正答率が低かった。承認手続の代行、他業務の応援といった状況においても、情報システムの利用方針及び運用上の制約を満たすことが重要である点を、是非理解しておいてほしい。

設問2では、社内情報の閲覧権限の付与に関する外部委託先との手続、担当者変更の際の利用者ID管理を問うた。(3)の正答率が高かった。業務の引継ぎという状況での適切な権限設定は、よく理解されていた。

情報システムの利用に関する内部不正を防止し、情報セキュリティを維持するために、情報セキュリティリーダには、業務で日常起こり得る変化に対して適切な権限設定を検討する役割を期待したい。

8-2 午後問題の演習

午後問題は、問題を実際に解いて慣れることが、合格への一番の近道です。過去問題やサンプル問題を例に、しっかり問題演習を行っていきましょう。

8-2-1 内部不正防止のためのログのレビュー

問 内部不正防止のためのログのレビューに関する次の記述を読んで、設問1～6に答えよ。

A社は、高級化粧品を個人に販売しており、従業員は100人である。A社は総務部、情報システム部、購買部、営業部から成り、営業部には60人の従業員が属している。営業部は企画課、営業1課～4課から構成される。営業部のIT環境は次のとおりである。

- ・営業部員は全員A社所有のノートPCを使用している。
- ・社内ネットワークに接続された、スキャナ用の共用PCが1台設置されている。
- ・営業部員は、社外から社内のシステムを使用する際には、ノートPCをインターネット経由でA社のVPNサーバに接続して使用している。

なお、A社では、インターネットの使用を広く認めており、Webメールやファイル共有サービスなどを含め、サービスの使用を制限していない。

A社では、顧客情報などの機密情報の漏えいを防ぐ目的で、退職後も一定期間有効な損害賠償条項を含む機密保持契約を全従業員と締結している。

A社では、営業部員が表計算ソフトを使用してノートPCで顧客情報を管理していたが、顧客管理パッケージ(以下、Bシステムという)を社内を導入し、そこで集約して管理することを決定した。Bシステムに関する方針は次のとおり定めた。

- ・Bシステムの主管部門は営業部である。
- ・Bシステムを使用するのは営業部だけである。
- ・見込み客の登録から販売後のフォローアップまでを一貫してBシステムによって管理する。
- ・Bシステムの導入及び運用はA社の情報システム部が行う。
- ・Bシステムは2か月後から使用開始する。

- ・表計算ソフトを使用して管理していた顧客情報はBシステムに移行後、ノートPCから削除する。

情報システム部は、Bシステムに関して、利用者IDの管理、データのバックアップ取得、ログの記録などに関する要件について営業部との間で合意した。Bシステムは顧客情報を取り扱うシステムなので、内部不正による顧客情報の漏えいを防止するため、採取するログの保存方法や、レビュー方法（誰がいつ、どのように）についてC君が検討を開始した。

〔ログのレビュー方法の検討〕

営業部の企画課に所属するC君は、営業部の情報セキュリティリーダーを兼ねている。C君はBシステムのログの仕様を確認しようと思い、情報システム部担当者のD君にログの仕様の調査を依頼した。そこでD君は、Bシステムのログのサンプルを提示した(表1)。ログイン及びログアウトのログはサーバXで、それ以外のログはサーバYで記録されるが、表1は、情報システム部でツールを用いてそれらのログを同じ形式に整え、表計算ソフトを使用して時系列順に並び替えたもの（以下、加工済みログという）とのことであった。

表1 Bシステムの加工済みログ(抜粋)

日時	利用者のIPアドレス	利用者ID	操作	顧客ID
2015/03/10 15:30:10	10.0.0.5	1013	LOGIN	0
2015/03/10 15:40:03	10.0.0.5	1013	READ	10023
2015/03/10 15:40:10	10.0.0.5	1013	READ	10025
2015/03/10 15:40:15	10.0.0.5	1013	READ	10102
2015/03/10 15:45:20	10.0.0.5	1013	UPDATE	10102
2015/03/10 15:50:16	10.0.0.5	1013	DELETE	10023
2015/03/10 16:03:10	10.0.0.8	1002	LOGIN	0
2015/03/10 16:15:03	10.0.0.8	1002	READ	10105
2015/03/10 16:16:10	10.0.0.8	1002	READ	10321
2015/03/10 16:16:15	10.0.0.8	1002	READ	10222
2015/03/10 16:20:12	10.0.0.5	1013	LOGOUT	0
2015/03/10 16:25:19	10.0.0.8	1002	LOGOUT	0

注記 顧客IDの0は、顧客情報に関係しない操作であることを意味する。

D君は、Bシステムでは、次の対策を実施することをC君に説明した。

- ・加工済みログの順番が、実際に営業部員がBシステムに対して実施した操作の順番どおりになるよう、aを行う。
- ・ログが故意に消されてしまうことがないようにbを行う。

営業部では、顧客ごとに担当営業を決めているが、担当営業が休みの際のサポートなどが必要なので、Bシステムでは、全営業部員が全顧客情報にアクセスできるようにする。

最近、同業他社で、従業員が、共有ファイルサーバにある全ての顧客情報をUSBメモリにコピーして持ち出し、転職先で使ったという事件が発生した。そこで営業部長は、C君に図1の要件を伝え、対策の検討を指示した。

- ・顧客情報への業務目的外のアクセスをログのレビューによって検出したい。ログのレビュー手順は、まずログの内容を確認し、もし業務目的外と思われる顧客情報へのアクセスログがあった場合は、遅滞なく営業部長に報告の上、そのログが示す操作を行った営業部員がなぜその操作を行ったかを適切な方法で確認する。
- ・万が一問題が発生したときに備えて、後からでもどの営業部員がどの顧客情報にアクセスしたか特定できるようにしておきたい。

図1 営業部長が伝えた要件

営業部長は、①リスクを更に低減させるために、営業部員が退職する際に新たな手続を実施することとした。

②C君は、営業部長が伝えた要件を基に、どのような立場の人がどの程度の頻度でレビューをすべきかを検討した。③さらにC君は、ログの長期的な保存方法についても検討を行った。C君が、検討結果を営業部長に説明したところ、営業部長もこれに同意した。

情報システム部によるBシステムの導入完了後、各営業部員は、表計算ソフトを使用して管理していた顧客情報をBシステムに移行し、ノートPCから削除した。移行完了後、営業部ではBシステムの使用を開始した。

〔ログのレビュー開始〕

Bシステムの使用を開始して1か月が経過し、ログのレビューが開始された。Bシステムには約4,000人の顧客情報が保管されている。ログの生成件数を考えると、30日間で100人分以上の顧客情報にアクセスした営業部員のログに限定してレビューを行うべきだということになった。そこで、④C君は、過去30日間に発生したREADのログからレビュー対象のログを抽出する条件を示してD君にログの抽出を依頼した。抽出されたログを見たC君は、ある営業部員が1,000人分の顧客情

報にアクセスしたことを示すログを発見した。そこで、C君はすぐに営業部長に報告し、その営業部員の上長の課長に確認した。その結果、その課長の指示でダイレクトメールを送付していたことが分かり、問題はないことが確認できた。

営業部長とC君で相談した結果、レビューを行う人、及び頻度は検討結果のとおりとし、抽出条件に基づいて抽出したログだけをレビュー対象とすることとした。営業部長は、ログをレビューするに当たり、次のことを指示した。

- ・全ての営業部員に対し、ログをレビューすることを伝えること。ただし、ログのレビューを回避されないように、抽出条件を営業部員には伝えないこと。
- ・ログがレビューされていることを営業部員に印象付けるために、ログに記録されているアクセスについて定期的に必ず営業部員にアクセスの目的を確認すること。

〔課題の発見とリスクの更なる低減〕

C君は、職場内でBシステムが適切に使用されているかどうかを観察していたところ、いくつかの事象が目にとまり、このままでは、⑤ログのレビューを適切に実施したとしても、図1の要件が実現できないことに気付いた。そこでC君は、営業部長に相談の上、各課長に改善を依頼した。

Bシステムの使用開始から1年間が経過した。ログのレビューによって営業部全体の情報セキュリティ意識が高まり、営業部長のC君に対する評価は大きく高まった。

設問1 本文中の a と b に入れる組合せとして正しい答えを、解答群の中から選べ。

a, bに関する解答群

	a	b
ア	サーバの時刻同期	ログのWORMメディアへの記録
イ	サーバの時刻同期	ログの暗号化
ウ	ログのWORMメディアへの記録	サーバの時刻同期
エ	ログのWORMメディアへの記録	ログの暗号化
オ	ログの暗号化	サーバの時刻同期

注記 WORM : Write Once Read Many

設問2 本文中の下線①で実施することになった手続はどれか。解答群のうち、最も適切なものを選べ。

解答群

- ア 退職する営業部員が担当していた顧客情報を、他の営業部員に引き継ぐ。
- イ 退職する営業部員が担当していた顧客情報を、Bシステムから完全に消去する。
- ウ 退職する営業部員に、その営業部員と締結した機密保持契約書を見せ、その営業部員がアクセスした顧客情報がログに記録されていることを説明する。
- エ 退職する営業部員のPCのハードディスクは再利用せず、完全に物理破壊する。

設問3 本文中の下線②における、C君の検討結果はどれか。解答群のうち、最も適切なものを選べ。

解答群

- ア 営業部の各課長が、情報システム部担当者の依頼があった都度、ログをレビューする。
- イ 営業部の各課長が、毎週、ログをレビューする。
- ウ 情報システム部担当者が、営業部長が指定した頻度でログをレビューする。
- エ 情報システム部担当者が、毎週、ログをレビューする。

設問4 本文中の下線③においてC君が検討したログの保存方法はどれか。解答群のうち、最も適切なものを選べ。

解答群

- ア 情報システム部が全てのログを10年間保存する。
- イ 情報システム部が営業部員ごとにログを仕分けして、各営業部員が自分の分を保存する。
- ウ レビュー後のログは保存せず、情報システム部担当者が速やかに削除する。
- エ レビューで不審であると判断したログだけを情報システム部が10年間保存する。

設問5 本文中の下線④でC君がD君に出した抽出条件を、解答群の中から選べ。

解答群

- ア アクセスしたユニークな顧客ID数が100以上の営業部員のログ
- イ アクセスしたユニークな顧客ID数が100以上の日のログ
- ウ ログ件数が100以上の営業部員のログ
- エ ログ件数が100以上の日のログ

設問6 C君が観察した次の(i)～(iv)の事象のうち、本文中の下線⑤の原因となるものを全て挙げた組合せを、解答群の中から選べ。

- (i) Bシステムで表示した顧客情報をコピーし、表計算ソフトにペーストした上でA社の共有ファイルサーバに置いて共有している。
- (ii) Bシステムの使用申請をしてから、営業部長が承認するまでに2週間掛かっている。
- (iii) ある営業部員が共用PCからBシステムにログインし、ログインしたままそのPCで他の営業部員がBシステムを使っている。
- (iv) ある営業部員が頻繁にBシステムにログイン、ログアウトを繰り返している。

解答群

- | | | |
|--------------|-------------------|---------------------|
| ア (i), (ii) | イ (i), (ii), (iv) | ウ (i), (iii) |
| エ (i), (iv) | オ (ii), (iii) | カ (ii), (iii), (iv) |
| キ (ii), (iv) | ク (iii), (iv) | |

(情報セキュリティマネジメント試験 サンプル問題)

■ 解答

設問1 ア 設問2 ウ 設問3 イ
 設問4 ア 設問5 ア 設問6 ウ

出題趣旨

情報セキュリティにおいて、権限をもった者による内部不正を防止することは一般に困難である。内部不正が行われていたことを発見する手段として、記録したログのレビューを適切に実施することが有効な選択肢となり得る。しかし、レビューのプロセスが適切に設計されていないと機能しない。具体的には、レビュー実施者、レビュー頻度、レビュー対象となるログの抽出条件などを適切に設計する必要がある。そして、レビューに当たっては、業務をよく理解したユーザ部門が主体的に関与することが重要である。

本問では、営業部門が保有する顧客情報へのアクセスログのレビューを題材として、ログのレビューがどのような目的で行われるかを理解した上で、プロセスが適切であるか判断する能力と、ログのレビューを適切に運用する能力を問う。

■ 解説

利用部門である営業部の情報セキュリティリダーとして活動するC君が、ログのレビューを行うことで営業部全体の情報セキュリティ意識を高め、営業部長からの評価を大きく高めるという内容の事例が問題として出題されています。ログのレビューでは、レビューを行うことを通知することによって不正行為を抑止する効果があり、それを組織的、効果的に実現する方法について問われています。

設問1

空欄a, bに関する穴埋め選択問題です。ログの取得に関する基礎知識が問われています。

空欄a

加工済みログの順番が、実際に営業部員がBシステムに対して実施した操作の順番どおりになるようにするために行うべきことについて問われています。

〔ログのレビュー方法の検討〕に、加工済みログは、「ログイン及びログアウトのログはサーバXで、それ以外のログはサーバYで記録されるが、表1は、情報システム部でツールを用いてそれらのログを同じ形式に整え、表計算ソフトを使用して時系列順に並び替えたもの」とあります。サーバXとサーバYのログを合わせて、時系列順が

狂わないようにするためには、サーバXとサーバYで同じ時刻に合わせておく必要があります。

そのための方法に時刻同期があり、NTP (Network Time Protocol) などを用いて、サーバの時刻を同期させることができます。

したがって、空欄aは**サーバの時刻同期**となります。

空欄b

ログが故意に消されてしまうことがないようにするためには何を行うかを問われています。

ログは、通常のハードディスクなどのメディアに記録していると、不正アクセスなどによって消去される危険性があります。これを防ぐためには、一度書き込んだら変更ができないWORM (Write Once Read Many) メディアにログを記録することで、ログの書き換えが不可能になります。

したがって、空欄bは**ログのWORMメディアへの記録**となります。

以上から、空欄a, bの適切な組合せは**A**です。

設問2

本文中の下線①「リスクを更に低減させるために、営業部員が退職する際に新たな手続を実施」について、実施することになった手続を考えます。

〔ログのレビュー方法の検討〕に、「Bシステムでは、全営業部員が全顧客情報にアクセスできるようにする」とあるので、顧客情報は全営業部員で共有しており、引継ぎなどは必要ないことが分かります。しかし、全顧客情報にアクセスできるということは、退職する社員が全顧客情報を持ち出すリスクがあるということなので、それを防ぐための方策が必要です。

機密保持契約書には、退職する場合、退職日以降も一定期間の機密保持を約束させる契約を入れておくのが一般的です。そして、ログに記録を残しておくことによって、機密情報を持ち出したかどうかの証拠を確認することができます。これを退職する営業部員に説明することによって、顧客情報の持ち出しなどの不正行為を抑止できます。

したがって、新たに実施することになった手続は、ウの「退職する営業部員に、その営業部員と締結した機密保持契約書を見せ、その営業部員がアクセスした顧客情報がログに記録されていることを説明する」ことです。

解答群のその他の手続は、もともと全顧客情報に全営業部員がアクセスできるようになっているため、意味がありません。

設問3

本文中の下線②の「C君は、営業部長が伝えた要件を基に、どのような立場の人がどの程度の頻度でレビューをすべきかを検討した」について、C君の検討結果を問われています。

営業部長が伝えた要件は、図1にあるとおり、「業務目的外のアクセスをログのレビューによって検出」することです。この「業務目的外かどうか」の判断は、情報システム部担当者などの部外者にはできません。実際、[ログのレビュー開始]で、情報システム部担当者のD君が抽出したログをC君が見て確認していますが、この二人では、不審なアクセスを見つけるだけで、業務目的外かどうかを判断できていません。結局、[ログのレビュー開始]では、「営業部員の上長の課長に確認した」とあり、判断ができる最適な人物は営業部の課長であることが読み取れます。したがって、レビューを行う立場の人は、営業部の各課長であることが分かります。

また、レビューの頻度については、図1に「遅滞なく営業部長に報告」などとあり、業務目的外のアクセスは速やかに発見させることが求められています。このとき、情報システム部担当者の依頼など、不定期な頻度でレビューを行うと、時期によっては業務目的外のアクセスに長い間気づかないというリスクがあります。したがって、毎週など頻度を決めて定期的にログをレビューすることが適切です。

以上から、C君の検討結果は、イの「営業部の各課長が、毎週、ログをレビューする」となります。

ア 依頼のあった都度では、時期によって発見が遅れるリスクがあります。

ウ、エ 情報システム部担当者では、業務目的外のアクセスかどうかの判断ができません。

設問4

本文中の下線③「さらにC君は、ログの長期的な保存方法についても検討を行った」について、C君が検討したログの保存方法を問われています。

ログを証拠として保管する際には、不審なアクセスと判断できるものだけを保存しておくことでは証拠として役立たないことがあります。一見して不審なアクセスではないものが不正の証拠となることもあるからです。人間の判断は万全ではありませんし、証拠として万全を期するためには、ログを仕分けせず、全てのログを保存する必要があります。保管期間については、十分に長い期間が必要なので、10年程度が適当です。したがって、ログの保存方法は、アの「情報システム部が全てのログを10年間保存する」となります。

イの各営業部員が自分の分を保存する方法は、営業部員が自分の不正アクセスの証拠を消すことが可能なため、適切ではありません。

ウのようにログを保存しないこと、またはエのように不審なログだけを保存するこ

とは、証拠保全の観点から適切ではありません。

設問5

本文中の下線④「C君は、過去30日間に発生したREADのログからレビュー対象のログを抽出する条件」について、C君がD君に示した抽出条件が問われています。

〔ログのレビュー開始〕より、レビューを行うべきログは、「30日間で100人以上の顧客情報にアクセスした営業部員のログ」です。100人以上なので、同じ顧客IDに複数回アクセスした場合はカウントせず、ユニークな顧客ID数が100以上の営業部員のログを抽出することで条件を満たすことができます。したがって、抽出条件はアの「アクセスしたユニークな顧客ID数が100以上の営業部員のログ」となります。

イの「日」のログは、営業部には60人の従業員がおり、それらの部員が別々にアクセスするので、ユニークな顧客ID数が100以上となっても不自然ではなく、抽出条件とはなりません。

ウ、エのログ件数では、同じ顧客情報に複数回アクセスすることが十分考えられるので、抽出条件として適当ではありません。

設問6

本文中の下線⑤「ログのレビューを適切に実施したとしても、図1の要件が実現できない」ことについて、その原因となるものを、(i)～(iv)の事象から選んでいきます。

- (i) 顧客情報をコピーし、表計算ソフトにペーストした上で共有ファイルサーバに置くと、そのコピーした顧客情報へのアクセスについてはログが残りません。そのため、図1のログのレビューによる検出ができなくなる原因となります。
- (ii) Bシステムの使用申請をしてから、営業部長が承認するまでに2週間掛かっているのは、可用性という意味では問題があります。しかし、その期間は営業部員がアクセスできないというだけなので、図1の要件には影響はありません。
- (iii) ある営業部員がログインした共用PCから、別の営業部員がBシステムを使用すると、ログには最初の営業部員のアクセスとして残ります。そうすると、図1のログのレビューで、業務目的外のアクセスかどうかの判断を誤ってしまうおそれがあるので、検出ができなくなる原因となります。
- (iv) ログイン、ログアウトを頻繁に繰り返すのは、システムに負荷がかかり、可用性の部分では問題がある可能性はあります。しかし、ログにはログイン、ログアウトも含めてすべて記録されるので、レビューでの検出には影響はありません。

したがって、下線⑤の原因となるものは(i),(iii)となり、ウが正解です。

8-2-2 標的型攻撃メールの脅威と対策

問 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、a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、b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、c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）どおりに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無かったが、10日前から、製品の間合せが3回あり、メールでやり取りをしていた。
- ・ メールへ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 管理規程

〔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べ。

a, bに関する解答群

- | | | |
|------|---------|--------|
| ア 海外 | イ 架空 | ウ 官界 |
| エ 国内 | オ 大企業 | カ 中小企業 |
| キ 特定 | ク 不特定多数 | ケ 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べ。

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べ。

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 報告事項がそろそろのを待って、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트라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。

■ 解答

設問1 (1) a キ b ク

(2) ウ (3) ア, エ (4) カ

設問2 (1) カ (2) エ (3) イ (4) ア (5) エ

採点講評

問1は、標的型攻撃メールによるマルウェア感染の脅威、従業員の情報セキュリティ意識向上策について出題した。全体として、正答率は高かった。標的型攻撃は近年大きな話題になっており、理解が進んでいたと思われる。

設問1では、標的型攻撃の特徴、受信者に添付ファイルを開封させる手口について問うた。(4)は、正答率が高かった。標的型攻撃メールの特徴について、よく理解されていた。

設問2では、標的型攻撃メールによる被害を最小化するための、規程、体制、組織文化における課題と対応について問うた。また、情報セキュリティ意識を向上させるための活動であるサイバー演習の効果を上げるための工夫について問うた。(4)は、G君の行動の背景を分析することがポイントとなるが、正答率は平均的で、おおむね理解されていた。

標的型攻撃のように、技術的対策だけでは防ぎきれない脅威に対して、情報セキュリティリーダーには、関連規程の順守状況の改善、情報セキュリティの円滑な運用に加えて、職場の情報セキュリティ文化を醸成するという役割も期待したい。

■ 解説

標的型攻撃メールの脅威と対策に関する問題です。インシデントの発生から、対応の問題、課題と対策と、標的型攻撃メール対応の典型的な流れについて問われています。

設問1

〔受信したメール〕についての問題です。標的型攻撃メールの特徴や、その見分け方などが問われています。

(1)

空欄a, bの穴埋め問題です。標的型攻撃メールの特徴を問われています。標的型攻撃メールとは、**特定の**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、情報を搾取することなどを目的とするメールであり、**不特定多数**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。したがって、空欄aはキ、

空欄bはクが正解です。

(2)

空欄cの穴埋め問題です。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手法のことをソーシャルエンジニアリングといいます。したがって、空欄cはウが正解です。

(3)

本文中の下線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」に該当するものを問われています。そのため、図1のG君が受信したメールの内容を見ていきます。

まず、件名に「Re: Re:」が付加されています。「Re:」は、メールを返信するときに付加される文字列で、これが二つ付加されていることで、複数回メールのやり取りを行っていることが分かります。つまり、複数回やり取りすることで、返信するに値する相手であると認識させ、問合せ者に対する疑いを低減しています。また、図2のG君へのヒアリング結果にも、「製品の問合せが3回あり」とあり、複数回のやり取りが裏付けられます。

次に、メール本文6行目に「導入する方向で検討を進めております。」とあり、取引先になる可能性の高い優良顧客であることを示唆しています。この文面は、G君に対して、丁寧に対応することを迫るものです。さらに、メール本文の下から2行目で「本日15時までに回答を」と期限を指定しています。件名の「【至急】」でも緊急性を表現し、すぐに添付ファイルを開いて確認しなければならない動機付けになっています。

したがって、ア、エが正解です。

イ Y社の従業員しか知り得ない情報は記載されていません。

ウ 正当なURLを装ったリンクは記載されていません。

(4)

本文中の下線②「G君が受信したメールに見られる特徴」について、具体的な特徴を問われています。(i)～(iii)の内容を見ていきます。

・(i)

差出人のメールアドレスは「F@zz-freemail.co.jp」となっており、Y社の社内メールアドレスに詐称はされていないので誤りです。

・(ii)

署名のメールアドレスは「F@x-sha.co.jp」であり、差出人のメールアドレスと異なり

ます。

・(iii)

拡張子が「.exe」の実行形式ファイルが添付されています。

したがって、(ii)と(iii)が特徴に該当するので、力が正解です。

設問2

〔情報セキュリティ意識向上に向けて〕について、問題点や適切な対応を問われています。

(1)

本文中の下線③「今回の初動対応における問題点」を問われています。(i)～(iv)の内容を確認し、今回の問題点を挙げていきます。

・(i)

図3「管理規程」の第2章に「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」とあり、直ちに復旧対応を行う必要はありません。したがって、これは問題点ではありません。

・(ii)

図2「G君へのヒアリング結果」の1行目に「X社は過去に取引がある会社であった」とあることから、取引記録を確認していることが分かります。したがって、これは誤りです。

・(iii)

図3「管理規程」の第2章に「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」とあります。しかし、G君へのヒアリング結果によると、図2の下から7行目に「誰にも相談せず、報告もしなかった」、下から4行目に「報告したくないと思っていた」とあり、報告しなかったことが分かります。したがって、これは問題点です。

・(iv)

図3「管理規程」の第2章に「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」とあります。しかし、G君へのヒアリング結果によると、図2の下から7行目に「マルウェア感染はあり得ないだろうと考え」、下から4行目に「マルウェア感染と確信できない限りは」とあり、自己判断により疑わしい事象を報告しなかったことが分かります。したがって、これも問題点となります。

以上から、(iii)、(iv)が問題点に該当するので、力が正解です。

(2)

空欄dの穴埋め問題です。図3「管理規程」の第2章に、「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」とあります。したがって、エが正解です。

(3)

空欄eの穴埋め問題です。図3「管理規程」の第2章に、「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**」とあります。したがって、イが正解です。

(4)

空欄f1、f2の穴埋め問題です。規程やルールを策定しただけでは順守されないという現状があったため、それを改善し実際に順守させるために行うことについて問われています。(i)～(iv)について、順守させるために有効な対策かどうかを考えていきます。

・(i)

図2「G君へのヒアリング結果」の下から3行目に「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」とあります。そのため、重要な規程であるということと、その内容を従業員へ周知させることは重要です。

・(ii)

図2「G君へのヒアリング結果」の下から6行目に「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」とあります。このように情報の伝達がされない組織は問題なので、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です。

・(iii)

情報セキュリティにおけるクラッキング手法などは、情報セキュリティの専門家が、セキュリティ対応を考えるために学ぶものです。一般の従業員に対して教育する必要はありません。

・(iv)

マルウェア感染時の復旧対応は、情報セキュリティリーダーの指示の下に行います。そのため、あらかじめ一般の従業員が知っておく必要はなく、また、自己判断を助長することになるため危険でもあります。したがって、適切ではありません。

以上から、適切なものは(i), (ii)なので、アが正解です。

(5)

本文中の下線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」取組みとして適切なものを答える問題です。標的型攻撃メールは、設問1 (2)の解答より、「ソーシャルエンジニアリング」を利用します。そのため、アの標語の掲示や、イのDVD上映会、ウの事例教育などを行っても、標的型攻撃メールを業務に関連するメールであると認識してしまう可能性があり、一人一人が適切に対応できるかは未知数です。また、実際に対応できるかどうかは、これらの対策では測定できません。

実際に攻撃を受けた場合の対応を定量的に測定し評価するためには、模擬の標的型攻撃メールを従業員に送付し、その対応を確認する方法があります。従業員に向けた標的型攻撃メールを、期間を空けて何回か送信し、その対応を確認します。従業員がインシデントであると認識し報告した件数、報告までに要した時間の測定や、添付ファイルの開封率の変化を調査することで、定量的に評価できるようになります。したがって、エが正解です。

8-2-3 情報セキュリティ自己点検

問 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となっている。

- ・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ーに任命された。

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)”にすると言われた。

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、計画に基づいて改善を実施するように”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び。

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ある。
- 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び。

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び。

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び。

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び。

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か月以上にしている。
- 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べ。
- [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] 営業部門に対し、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
- [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べ。

[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]

(平成28年春 情報セキュリティマネジメント試験 午後 問3)

■ 解答

設問1 イ

設問2 イ, オ

設問3 (1) イ (2) エ (3) ア (4) イ (5) イ

設問4 (1) カ (2) ア

採点講評

問3では、監査部による監査とは別に、情報システムの利用部門が主体となって行う情報セキュリティ自己点検(本問では、簡易チェック及びCSA)によってコントロールを評価する取組みについて出題した。

設問1は、正答率が低かった。チェック項目として、客観的に判断できる基準を明確に設定することが重要であることを理解しておいてほしい。

設問2では監査におけるCSA方式の利点を問うたが、正答率は平均的で、おおむね理解されていた。

設問3は、(3)の正答率が低かった。ルールどおりに運用されていることを確認したかどうかという点が、評価する際のポイントであることを理解しておいてほしい。

設問4は、正答率が高かった。改善計画の策定において複数の対策を比較し検討する際には、根本的対策、暫定的対策、注意喚起などの選択肢から適切に選択することが重要だが、よく理解されていた。

情報セキュリティ自己点検は、情報システムの利用部門の情報セキュリティを効率的に維持する上で有効である。情報セキュリティリーダーには、このような活動を推進する役割を期待したい。

■ 解説

情報セキュリティ自己点検に関する問題です。海外営業部において、監査部がCSA(Control Self Assessment: 統制自己評価)による情報セキュリティ監査を実施します。標的型攻撃メールやISMSなどについての基礎知識と、問題文の正確な理解が必要な問題です。

設問1

本文中の下線①の「結果が正しいか客観的に判断できないチェック項目」について問われています。

表2のチェック項目のうち、No.11の「不審な電子メールの添付ファイル」の「不審」については、本人の判断です。標的型攻撃メールは、疑われないように巧妙に送りつけ

てくるので、不審だと判断できないことが多くあります。したがって、客観的に判断できないチェック項目は、イの11です。

No.10（パスワードを書いていない）、No.12（連絡先を知っている）、No.13（施錠保管している）は、実際に知っているか、行っているかでチェックできるので、客観的な判断が可能です。

設問2

本文中の下線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」について、CSA方式の利点を問われています。

CSA方式は自己評価を行う方式なので、業務を行っている本人が評価します。そのため、業務内容は十分理解しており、その理解に基づいて評価することができます。また、評価を自分で行うことで、セキュリティについて何をすべきかを学習することができます。これは、評価実施者に対する意識付けや教育として役立ちます。以上から、イ、オが正解です。

アの準拠性の担保やエの独立的な立場は、監査部が各部門を直接評価する方式の利点です。ウの証跡は、どちらの監査方式でも必要となります。

設問3

〔CSAの実施〕についての問題です。表3のCSAシートについて、空欄a～dの穴埋めを行い、改善計画を考えます。R社海外営業部の現状を正確に読み取ることがポイントです。

(1)

表3の空欄a、No.4の評価項目に対する穴埋め問題です。

全員が教育を受けているかどうかについては、本文中に「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」とあります。これは、配属時の教育の後に発見された新たなセキュリティ脅威については、情報セキュリティ教育を受けていないということです。

したがって、評価結果は“NG”，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”が適切であり、イが正解です。

(2)

表3の空欄b、No.11の評価項目に対する穴埋め問題です。

リモート接続のためのパスワードの変更については、本文中に「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」とあり、また「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」とあります。これは、海外営業部にはリモート接続サービスの接続が許可されているPCはないということです。

したがって、評価結果は“NA”，評価根拠は“部内ではリモート接続は誰も行わない”が適切であり、エが正解です。

(3)

表3の空欄c, No.19の評価項目に対する穴埋め問題です。

ファイルサーバ上の顧客情報のアクセス権が最小権限の原則に基づいて設定されているかについては、表1の簡易チェックリストのNo.1に「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」とあるので、最小権限で設定されているかを簡易チェックしています。これは、自己判断で全部員に確認しているということです。

したがって、評価結果は“OK”，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”が適切であり、アが正解です。

(4)

表3の空欄d, No.26の評価項目を答える穴埋め問題です。

No.26の評価根拠に、「部外者が従業員に気付かれずに入ることは難しい」、「出入口を施錠」とあるので、入退室に関することであることが分かります。また、評価結果が“(OK)”であることから、この入退室管理の方法が代替コントロールであることが分かります。そのため、本来行うべき情報セキュリティ対策は、入退室管理システムなどで厳密に入退室管理を行うような方法であることが考えられます。

したがって、評価項目は“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”が適切であり、イが正解です。

(5)

本文中の下線③「改善計画の策定」について、その概要が問われています。

改善が必要な内容としては、〔CSAの実施〕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」、「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」とあります。つまり、退職又は異動の際に速やかに利用者IDが削除されていないことが問題であり、それを改善するには、システムからの削除を速やかに行う対策が必要です。

したがって正解は、イの「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」となります。

設問4

〔新たな指摘についての改善計画〕についての問題です。最小権限の原則を守り、社外への顧客情報の漏えいを防止するための対策を考えていきます。

(1)

本文中の空欄e1～e3に入る対策を考えていきます。

空欄e1

新たな指摘に対応するための対策であり、全部員に担当顧客を確認してから行う根本対策です。Cシステムにおいて最小権限の原則を守らせるためには、システムで制御することが最も効果的です。具体的には、[対策3]の「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」が有効です。したがって、空欄e1は[対策3]となります。

空欄e2

暫定的な対策で、空欄e1の対策に掛かる2週間のリスクを低減するための対策です。最小権限の原則を守らせるためにシステム以外で制御するには、規則を周知徹底させて、運用的に行う方法があります。具体的には、[対策2]の「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」が有効です。したがって、空欄e2は[対策2]となります。

空欄e3

万が一顧客情報の漏えいが発生してしまったときのための対策です。顧客情報の漏えいが発生した場合には、アクセスログなどから、その漏えい元を特定することが肝心です。しかし、本文中に「Cシステムでは、アクセスログを3か月分保存している」とあり、3か月より前に発生した情報漏えいは追跡できないことになります。これには、[対策1]の「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」が有効です。したがって、空欄e3は[対策1]となります。

これらを組み合わせると、正解は力となります。

(2)

本文中の空欄f1～f3に入る対策を考えていきます。

空欄f1

顧客情報の追加・修正・削除の権限についての対策で、厳密なので業務が回らないような対策です。部員が顧客情報を不適切に変更しないようにするには、管理職だけが追加・修正・削除を行うことが最も確実ですが、業務は非効率となります。具体的には、[対策4]の「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」が該当します。したがって、空欄f1は[対策4]となります。

空欄 f2

空欄 f1 よりも効率的な対策ですが、ベンダに開発を依頼するので半年は掛かる対策です。顧客情報を追加・修正・削除したとき、それが不適切でないことを確認するには、上長が承認を行うことが確実です。具体的には、[対策5]の「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」が該当します。したがって、空欄 f2 は[対策5]となります。

空欄 f3

空欄 f2 の対策が有効になるまでの暫定的な対策です。上長の承認がシステムのワークフロー機能で行えない場合には、それを手動で行う必要があります。具体的には、[対策6]の「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」です。したがって、空欄 f3 は[対策6]となります。

これらを組み合わせると、正解はアとなります。

付録

平成28年度秋期 情報セキュリティマネジメント試験

◆ 午前 問題

試験時間：1 時間 30 分

問題番号：問 1 ～ 問 50

選択方法：全問必須

◆ 午前 解答と解説

◆ 午後 問題

試験時間：1 時間 30 分

問題番号：問 1 ～ 問 3

選択方法：全問必須

◆ 午後 解答と解説

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

Q

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。

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。

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

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。

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 Content Management)
- ウ LTE (Long Term Evolution)
- エ MDM (Mobile Device Management)

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パケットを検知し、通知する。

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。

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 |

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ないページに直接ジャンプする。

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。

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 想定し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に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

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を暗号化する。
- 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。

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き込みが、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ページを不正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。

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。

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。

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
- イ サンプルング
- ウ デジタルフォレンジックス
- 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”が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。

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ので、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バイス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。

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 組織の外部にすることはなく、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ととまることがなく、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図に関する記述のうち、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。

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の説明はどれか。

- 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

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。

A

午前 解答と解説

問1

《解答》エ

PIN(Personal Identification Number)とは、ICカードに設定された暗証番号のことです。ICカード利用時にPINを入力することで、ICカードの正当な所有者であることを判定できます。ICカードを配送するときは、盗難や紛失による悪用防止のため、PINは別経路で利用者に知らせる必要があります。したがって、エが正解です。

ア ICカードに設定するPINは、ICカードごとに異なる値にします。

イ ICカード紛失時は、悪用防止のため、すぐに失効処理を行います。

ウ PINは暗証番号なので、予測されない値にします。

問2

《解答》イ

リスク対応には、リスクテイク、リスクの回避、リスクの共有、リスクの保有の四つの方法があります。地震保険に加入することは、リスクを一つ以上の他者と共有することになるので、リスクの共有に該当します。したがって、イが正解です。

ア、ウはリスクテイク、エはリスクの回避に該当します。

問3

《解答》ウ

JPCERT/CC (Japan Computer Emergency Response Team Coordination Center)は、CSIRT (Computer Security Incident Response Team)のコーディネーションセンターで、日本において他のCSIRTとの情報連携や調整を行う組織です。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などを行っています。したがって、ウが正解です。

ア JISC (Japan Industrial Standards Committee : 日本工業標準調査会)の説明です。

イ CRYPTREC (Cryptography Research and Evaluation Committees)の説明です。

エ NISC (National center of Incident readiness and Strategy for Cybersecurity:内閣サイバーセキュリティセンター)の説明です。

問4

《解答》ウ

JVN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する脆弱性対策情報ポータルサイトです。したがって、ウが正解です。

ア CVSS (Common Vulnerability Scoring System : 共通脆弱性評価システム)の説明です。

イ CVE (Common Vulnerabilities and Exposures : 共通脆弱性識別子)の説明です。

エ CSIRT (Computer Security Incident Response Team)の説明です。

問5

《解答》ア

“可用性”とは、「認可されたエンティティが要求したときに、アクセス及び使用が可能である特性」です。つまり、アクセスを可能とするために障害を起こりにくくする必要があります。ストレージを二重化することは、耐障害性を向上させ、可用性を高めるので、アが正解です。

イは真正性、ウ、エは機密性を高めるための管理策です。

問6

《解答》ア

ベースラインアプローチとは、既存の標準や基準をベースラインとして組織の対策基準を策定し、チェックしていく方法です。基準とする望ましい対策をベースラインとして、現状とのギャップを分析するので、アが正解です。

イは非形式的アプローチ、ウは詳細リスク分析、エは組合せアプローチの特徴です。

問7

《解答》ウ

退職者の利用者IDの削除状況を把握するためには、現在の所属者の情報を基に、その内容と実際のシステムに残っている利用者IDを比較します。そのために、資料Aとして、現在のシステムでの「利用者IDとそれが発行されている者の一覧」を、資料Bとして「組織の現在の所属者の名簿」を用意します。資料Aと資料Bを突き合わせることで、利用者IDの削除漏れが確実に発見できます。したがって、ウが正解です。

ア、エ 削除申請書は、申請漏れの可能性があるため、確実性の低い資料です。

イ 退職者の一覧は、申請漏れの可能性や反映漏れの可能性があるため、確実性の低い資料です。

問8

《解答》イ

JIS Q 27000（情報技術－情報セキュリティマネジメントシステム－用語）では、リスク評価は、「リスク及び／又はその大きさが、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。したがって、イが正解です。

アはリスク対応、ウはリスク分析、エはリスク特定に該当します。

問9

《解答》エ

JIS Q 31000:2010では、残留リスク(residual risk)は「リスク対応後に残るリスク」と定義されています。したがって、エが正解です。

ア 発見リスクの説明です。

イ 事業リスクの説明です。

ウ 投機的リスクの説明です。

問10

《解答》エ

JIS Q 27002:2014では、「7.2.2 情報セキュリティの意識向上, 教育及び訓練」の管理策に、「組織の全ての従業員, 及び関係する場合には契約相手は, 職務に関連する組織の方針及び手順についての, 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」とあります。派遣従業員に関しても教育を実施する必要があるので, エは改善が必要な状況となります。

ア, イ, ウは, 教育実施の観点から望ましい内容です。

問11

《解答》エ

IPA「組織における内部不正防止ガイドライン」では、「4.8.職場環境 (26) 職場環境におけるマネジメント」に、「組織内では, 他の役職員が不在で相互監視ができない環境における単独作業を制限することが望ましい」とあります。単独作業は相互監視のできない環境であり, 内部不正が発生する可能性が高くなるからです。したがって, エが正解です。

ア, ウ 「4.8.職場環境 (25) 適正な労働環境及びコミュニケーションの推進」では, 健全な労働環境や良好なコミュニケーションがとれる環境でないと, 業務への悩みやストレスを抱えてしまい, 内部不正が発生する可能性が増すことから, 制限をしないことが推奨されます。

イ 「4.5.証拠確保 (18) システム管理者のログ・証跡の確認」に, ログ・証跡を定期的にシステム管理者以外が確認しなければならないと記述されています。

問12

《解答》エ

ボットとは, 人間が行うようなことを代わりに行うプログラムで, ボットネットでは, ボット同士が連携して動作を行います。C & C (Command and Control) サーバとは, ボットネットに対して指示を出し, 情報を受け取るためのサーバです。ボットを感染させ, 侵入して乗っ取ったコンピュータに対して, C & Cサーバが命令を出し, 応答を受け取るので, エが正解です。

アはキャッシュサーバの役割です。イ, ウは, パスワードの盗聴を防ぐ仕組みです。

問13

《解答》エ

会社や団体がスマートフォンに対して一元管理する仕組みのことをMDM (モバイル端末管理) といいます。したがって, エが正解です。

ア 個人所有のスマートフォンを業務で使用する取組みです。

イ 組織内の業務ドキュメントや文書の蓄積, 管理, 運用を統括的, 包括的に行うための技術やシステムのことです。

ウ 携帯電話の通信規格の一つです。

問14

《解答》イ

第三者がコンピュータに不正に侵入した後に利用するソフトウェアをまとめたパッケージは rootkit です。したがって、イが正解です。

ア RFID (Radio Frequency Identification) は、電波を使った近距離の無線通信で情報をやりとりする仕組みです。

ウ TKIP (Temporal Key Integrity Protocol) は、無線LANで使われるセキュリティプロトコルで、システム運用中に動的に鍵を変更できます。

エ web beacon (ウェブビーコン) は、HTMLを利用した閲覧者を識別する仕組みです。

問15

《解答》イ

SIEMとは、サーバやネットワーク機器などからログを集め、そのログ情報を分析し、異常があれば管理者に通知する、または対策方法を知らせる仕組みです。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するので、イが正解です。

ア DLP (Data Loss Prevention) の機能です。

ウ CMDB (Configuration Management Database : 構成管理データベース) の機能です。

エ IDS (Intrusion Detection System : 侵入検知システム) の機能です。

問16

《解答》エ

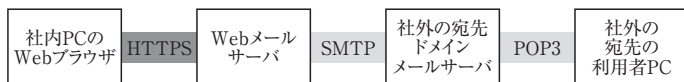
SPFは、送信ドメインを認証するための技術です。該当ドメインに対するメールサーバのIPアドレスをDNSサーバに登録しておき、受信したメールサーバがそのIPアドレスを検証することで、送信元のメールサーバが正規のサーバであることを確認します。メール送信元のなりすましを検知することができるので、エが正解です。

アはHTTPS通信の利用、イはパーソナルファイアウォールの導入、ウはIDSなどの導入によって対処できます。

問17

《解答》イ

この〔電子メール環境〕をまとめると、次の図のようにメールが送信されます。



このうち暗号化されているのは、HTTPS (HTTP over TLS) の部分だけで、SMTPとPOP3では平文でデータが送られます。そのため、秘密情報を含むファイルは暗号化してメールに添付する必要があります。したがって、イが正解です。

ア、ウ Webメールサーバ以降は暗号化されていないので、暗号化する必要があります。

エ Base64形式は、誰でもデコード(復元)できるので盗聴可能です。

問18

《解答》エ

ビヘイビア法とは、ビヘイビア(ふるまい)を監視するための手法です。安全な仮想環境下などで実行し、その挙動を確認することで、ウイルスかどうかを判定します。したがって、エが正解です。
アはチェックサム法、イはコンペア法、ウはパターンマッチングに分類されます。

問19

《解答》イ

時刻サーバが使用している、時刻を同期させるプロトコルをNTP (Network Time Protocol) といいます。インターネット上の時刻サーバと社内サーバを同期させるためには、NTPをファイアウォールで許可して通過させる必要があります。NTPはトランスポート層のプロトコルとしてUDP (User Datagram Protocol) を使い、ポート番号123で通信するので、イが正解です。
アはファイル転送、ウはメール送信、エはネットワーク管理のための通信プロトコルです。

問20

《解答》ア

CAPTCHAとは、ユーザ認証のときに合わせて行うテストで、利用者がコンピュータでないことを確認するために使われます。Completely Automated Public Turing test to tell Computers and Humans Apartの頭文字をとったものです。したがって、アが正解です。
イ 二次元バーコードの種類です。
ウ 長いURLを短いURLに変換したものです。リダイレクトという仕組みを利用して本来のサイトに接続します。
エ ブログの機能の一つで、双方向リンクである「トラックバック」の設置をリンク先に通知するために送信されるパケットのことです。

問21

《解答》ア

情報の“完全性”とは、資産の正確さ及び完全さを保護する特性です。Webページの改ざんは、Webページという資産の正確さを脅かす攻撃なので、アが正解です。
イ、エは“機密性”、ウは“可用性”を脅かす攻撃となります。

問22

《解答》ア

クロスサイトスクリプティングとは、悪意のあるスクリプトを、標的となるサイトに埋め込む攻撃です。Webアプリケーションに用意された入力フィールドに、JavaScriptコードを入力することで実現できるので、アが正解です。
イは不正アクセスを行う攻撃全般、ウはバッファオーバーフロー、エはディレクトリトラバーサルの手口となります。

問23

《解答》ア

サイバーセキュリティ戦略の五つの基本原則の三番目に「開放性」があり、「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、常に参加を求めるものに開かれたものでなければならない」と定められています。したがって、アが正解です。

イ 基本原則「自律性」に、「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」と定められています。

ウ 基本原則「情報の自由な流通の確保」に、「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」と定められています。

エ 基本原則「法の支配」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」と定められています。

問24

《解答》イ

スクリプトキディとは、インターネット上で公開されている簡単なクラッキングツールを利用して不正アクセスを試みる攻撃者です。技術不足なので新しい攻撃手法を考え出すことはできませんが、公開された方法を利用することはできるので、イが正解です。

ア、ウはソーシャルエンジニアリングの行為です。エは故意犯の行為に該当します。

問25

《解答》ア

人間の心理的、社会的な性質につけ込んで秘密情報を入手する手法のことを「ソーシャルエンジニアリング」といいます。したがって、アが正解です。例としては、上司や重要顧客などを詐称してシステム管理者に電話をかけパスワードを聞き出す、ゴミ箱をあさってパスワードの紙を見つけるなどの手法があります。

イ コンピュータに入り込んで有害な動作を行うソフトウェアです。自己増殖機能はありません。

ウ 適切なセキュリティ対策が行われていないサーバに侵入し、そのサーバを経由して攻撃を行う手法です。

エ 適当な文字列を組み合わせる力任せにログインの試行を繰り返す攻撃です。

問26

《解答》ウ

パスワードリスト攻撃とは、他のサイトで取得したパスワードのリストを利用して不正ログインを行う攻撃です。どこかのWebサイトから流出した利用者IDのパスワードのリストを用いて、他のWebサイトにログインを試みるので、ウが正解です。

アは辞書攻撃、イはレインボー攻撃、エはピクチャパスワードの盗聴に該当します。

問27

《解答》エ

ランサムウェアとは、システムへのアクセスを制限し、その制限を解除するための代金（身代金）を要求するソフトウェアです。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のはランサムウェアに該当するので、エが正解です。

アは遠隔操作ウイルス、イはパスワードの暴露ウイルス、ウはキーロガーに該当します。

問28

《解答》ウ

ECサイトのデジタル署名が添付された電子メールでデジタル署名を検証することで、署名をした秘密鍵がECサイトのものであることを確認できます。また、ハッシュ値も合わせて確認でき、メールが改ざんされていないことも分かるので、メール内のドメインが正しいことも確認できます。したがって、ウが正解です。

ア、イのメールアドレスは偽装が可能です。また、署名も自由に設定できるので、エも偽装可能であり、相手が正しいことは確認できません。

問29

《解答》ウ

PKIの認証局が果たす役割として、公開鍵証明書が発行があります。また、失効したデジタル証明書の一覧(CRL)の発行も行います。したがって、ウが正解です。

ア 暗号化通信で利用者が作成します。

イ 暗号化通信で利用者が暗号化します。

エ PKIにおいては受信者が検証します。

問30

《解答》ウ

コモンクライテリアとは、IT関連製品や情報システムのセキュリティレベルを評価するための国際規格で、ISO/IEC 15408として定義されています。したがって、ウが正解です。

アは品質マネジメント、イは環境マネジメント、エは情報セキュリティのリスクマネジメントのための国際標準です。

問31

《解答》エ

プロバイダ責任制限法(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)では、第三条(損害賠償責任の制限)で、「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」に該当しない場合には、賠償の責めに任じないとされています。そのため、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なかった場合には、放置していても損害賠償責任が制限されます。したがって、エが正解です。

ア 個人情報保護法の第十六条(利用目的による制限)が適用されます。

イ 消費者契約法の第九条(消費者が支払う損害賠償の額を予定する条項等の無効)が適用されます。

ウ 電波法の第五十九条(秘密の保護)、または有線電気通信法の第九条(有線電気通信の秘密の保護)が適用されます。

問32

《解答》ウ

刑法の第二百四十六条の二(電子計算機使用詐欺)には、「人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」とあります。

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ことは、虚偽の電磁的記録での不法の利益となるので、ウが正解です。

ア 特定商取引法「連鎖販売取引」第三十四条(禁止行為)が適用されます。

イ 特定商取引法「通信販売」第十二条(誇大広告等の禁止)が適用されます。

エ 刑法の第二百三十四条の二(電子計算機損壊等業務妨害)が適用されます。

問33

《解答》ウ

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)”では、第4-1・(2)「特定個人情報ファイルの作成の制限」に、「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、「個人番号関係事務実施者」に該当する」とあります。つまり、税理士に業務委託して源泉徴収票作成事務を行わせることは認められているので、ウが正解です。

ア 第4-3・(3)「収集・保管制限」に、「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」とあるので、保管してはいけません。

イ 別添の「特定個人情報に関する安全管理措置」の2「講ずべき安全管理措置の内容」では、「F 技術的安全管理措置」の「a アクセス制御」に、「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」とあるので、事務取扱担当者を限定し、アクセス権を制限する必要があります。

エ 第4-1・(1)「個人番号の利用制限」に、「事業者が個人番号を利用するのは、主として、源泉徴収票及び社会保障の書類に従業員等の個人番号を記載して行政機関等及び健康保険組合等に提出する場合である」とあり、例外的な場合を除いて、これら以外の目的で利用することは禁じられています。そのため、営業成績の管理などには利用できません。

問34

《解答》ウ

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)では、第三条(特定電子メールの送信の制限)において、「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することに同意する旨を送信者又は送信委託者に対し通知した者」への特定電子メールの送信を許可しています。この方式をオプトイン方式というので、ウが正解です。

ア 第三条での許可される送信者には当てはまらず、特定電子メールの送信は禁止されています。

イ 2008年12月の特定電子メール法改正によって、未承諾広告であることを明記しても、相手の承諾なしに広告メールを送ることは禁止となりました。

エ 第六条(架空電子メールアドレスによる送信の禁止)で、プログラムによって自動的に生成される架空のメールアドレスの使用は禁止されています。

問35

《解答》エ

不正アクセス禁止法では、第六条に「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を保管してはならない」とあり、他人の識別符号を不正に保管する行為の禁止を明記しています。そのため、不正アクセスを行ってなくても、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場合には処罰の対象となります。したがって、エが正解です。

ア パスワードの実例を教えることは不正アクセス行為を助長する行為とみなされることもあり
ますが、情報セキュリティの啓発という正当な理由があるので処罰の対象とはなりません。

イ 不正アクセスを行う目的で保管していないので、処罰の対象ではありません。

ウ 人を欺いて詐欺を働く行為は、不正アクセス禁止法ではなく刑法の詐欺罪(第二百四十六条)での処罰の対象となります。

問36

《解答》ウ

準委任契約では、仕事の完成は約束されず、業務を実施して報告する善管注意義務があります。業務分析や要件定義、コンサルティングなどでよく行われる契約です。したがって、ウが正解です。

ア、イ 請負契約の説明です。

エ 派遣契約、出向契約の説明です。

問37

《解答》エ

JIS Q 27001では、「9.2 内部監査」のc)に、「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」とあります。したがって、エが正解です。

ア ISMS認証を行う外部監査では必要ですが、内部監査では不要です。

イ 任命についての規定はありませんが、監査結果を管理層に報告する必要はあります。

ウ ISMSに適合しているかなど、管理策以外にも監査範囲です。

問38

《解答》ウ

証拠を収集し保全する技法には、デジタルフォレンジックスがあり、ログを法的な証拠として保全します。インシデントの調査やシステム監査にも利用できるもので、ウが正解です。

ア 緊急時対応計画のことで、災害発生時に活用します。

イ 監査の技法の一つである統計的サンプリング法で使われる、母集団からサンプルを抽出する手法です。

エ 経営を抜本的に改革するために、同じ分野の優良事例などとパフォーマンスを比較・分析し、自社の問題点を明確にして変革を実現する方法です。

問39

《解答》ア

事業継続計画(BCP: Business Continuity Planning)は、災害発生時に最小時間でITサービスを復旧させ、事業を継続させるための計画です。緊急時に迅速に連絡を行うためには緊急連絡先リストは不可欠で、最新版に更新しておく必要があります。したがって、アが正解です。

イ 重要書類は災害時の紛失を想定して、遠隔地に複製を保管しておく必要があります。

ウ 緊急時には、優先度に応じて対応の優先順位を決める必要があります。

エ BCPは普段から公開し、従業員に周知徹底しておく必要があります。

問40

《解答》ウ

“情報セキュリティ監査基準”は、情報セキュリティ監査人のための行動規範です。具体的な判断の尺度には、原則として“情報セキュリティ管理基準”を用います。したがって、ウが正解です。

ア “情報セキュリティ管理基準”は、ISO/IEC 27001などの国際規格を基に策定されています。

イ 監査人が必要と認めた場合には、他の専門家の支援を仰ぐことを考慮すべきであると定められています。

エ 監査対象から独立していなければならないと規定されています。

問41

《解答》ア

システムの移行テストとは、既存システムから新システムへの移行を行うためのテストです。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ので、アが正解です。

イ システムテストなどで行う性能テストの目的です。

ウ 結合テストを実施する目的です。

エ 単体テスト(ソフトウェアテスト)を実施する目的です。

問42

《解答》ウ

インシデントとは、中断・阻害、損失、緊急事態、危機になり得る、またはそれらを引き起こし得る状況です。プログラムの異常終了は、システムの中断を引き起こす状況なので、インシデントに該当します。したがって、ウが正解です。

ア インシデントの検知に該当します。

イ 問題(インシデントの根本原因)に該当します。

エ インシデント対応に該当します。

問43

《解答》ア

差分バックアップでは、前回のフルバックアップ以降に変更されたファイルだけをバックアップします。フルバックアップに加えて、毎日、差分バックアップを取得しておくことで、前日までのデータを復旧できるようになります。したがって、アが正解です。

イ、ウ 一つのディスクだけで障害が起こったときにはデータ消失を回避できますが、複数ディスクの障害時には、これまでと同様に、フルバックアップ時までしか回復できません。

エ メールサーバのディスクに障害が起こった場合には、これまでと同様、磁気テープにコピーした情報までしか復旧できません。

問44

《解答》イ

ステークホルダとは、プロジェクトに積極的に関与しているか、またはプロジェクトの実行や完了によって利益にプラスまたはマイナスの影響を受ける個人や組織です。プロジェクトの成果が利益(プラス)になる者だけでなく、不利益(マイナス)になる者も含まれるので、イが正解です。

ア 組織の外部に属していることもあります。

ウ 間接的な関与を行う者も含まれます。

エ 個人として特定する必要はなく、組織や顧客なども含まれます。

問45

《解答》ア

Webブラウザは、クライアントのPCには最初から入っており、専用のアプリケーションのようにクライアント1台1台に導入する必要がありません。そのため、クライアント環境の保守が大幅に軽減されます。したがって、アが正解となります。

イ サーバ環境は変わらないので、作業は変わりません。

ウ データベース環境は変わらないので、作業は変わりません。

エ Webブラウザのシステムでもログインは必要なので、作業は変わりません。

問46

《解答》イ

E-R図とは、実体(エンティティ)と関連(リレーションシップ)を表す図です。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ので、イが正解です。

ア 関係データベースに限らず表現できます。

ウ DFD (Data Flow Diagram)で表現します。

エ リレーションシップは、エンティティ間のデータの関連を表します。

問47

《解答》ウ

DHCPサーバは、IPアドレスの他にネットマスクやデフォルトゲートウェイアドレスなども自動設定するサーバです。PCは、DHCPサーバのアドレスを知らなくても、ブロードキャストパケット(LAN全体に送るパケット)を送ることで、DHCPサーバがそのパケットを受け取って情報を返答します。あらかじめDHCPサーバのアドレスを設定しておく必要はないので、ウが正解です。

ア サブネットマスクやデフォルトゲートウェイアドレスも自動設定できます。

イ PCへのIPアドレスの固定設定は、DHCPによる自動割当てのIPアドレスと重複しなければ設定可能です。

エ IPアドレスは毎回自動で割り当てられるので、電源が切られた後に再度割当てを行うと、異なるIPアドレスになることもあります。

問48

《解答》イ

BPO (Business Process Outsourcing) とは、企業などが自社の業務の一部または全部を、外部の専門業者に一括して委託することです。社内業務のうちコアビジネスでない事業を委託するので、イが正解です。

ア BCP (Business Continuity Planning) の説明です。

ウ MRP (Material Requirement Planning) の説明です。

エ プロジェクトマネジメントの説明です。

問49

《解答》ウ

企画プロセスでは、システムが関与するシステム化構想の立案、システム化計画の立案などを行います。システム化構想の立案プロセスでは、経営上のニーズや業務上の課題などの事項を明確にします。したがって、ウが正解です。

ア 合意プロセスで明確にします。

イ システム開発プロセス、保守プロセスで明確にします。

エ ソフトウェア構成管理プロセスで明確にします。

問50

《解答》イ

マトリックス組織とは、職能別組織と事業部制組織を合わせた組織構造で、構成員は、自己の専門とする職能部門と、特定の事業を遂行する事業部門の両方に所属します。したがって、イが正解です。

ア 事業部制組織の説明です。

ウ 職能別組織の説明です。

エ プロジェクト組織の説明です。

Q

午後 問題

全問が必須問題です。必ず解答してください。

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。サービスの仕様(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10G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社に関係する業務がなく、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関係する“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と思いますが、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がきました。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、適切なものを選べ。

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べ。

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サービスに登録され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も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び。

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памメール | カ 中間者攻撃 |
| キ なりすまし | コ 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^{ぜいりょ}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ーを置いている。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。

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して判断した場合には、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・盗難発生時の対応手順（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	・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 W主任	事実関係を確認するためにFさんにヒアリング。
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

〔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、施されていたのでしょうか。

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、最も適切なものを選べ。

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 e1 , e2 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 f 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 g1 , g2 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の中のファイルを点検してもらいましょう	私も立ち会います

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、交通費清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ト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、交通費清算管理システムを用いて交通費清算情報を、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、交通費清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
 - ー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
 - ーアクセス権は、各利用部門からの申請に応じて設定単位を変更可能
 - ー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
 - ー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、適用要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。

図3 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いく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か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おびと説明、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び。

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	交通費清算情報	社内ファイル共有サービス	外出していた
エ	交通費清算情報	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、最も適切なものを選び。

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 ポット化 |

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、最も適切なものを選び。

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

A**午後 解答と解説****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****《解答》**

- 設問1 (1) a オ (2) オ
 設問2 キ
 設問3 (1) b エ (2) ケ
 設問4 (1) c イ d オ
 (2) e イ f エ ※eとfは順不同
 (3) ウ (4) キ

《解説》

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問題です。事故発生から、原因調査、個別ヒアリング、問題点の整理・対策の検討と、インシデント対応の典型的な流れが問題となっています。

設問1

「事故発生」についての問題です。「表1 Xサービスにおけるファイルの共有設定」から事故の原因を読み解きます。

(1)

Xサービスに登録している情報がインターネット上で公開されてしまった場合のファイルの共有設定について考えます。

ファイルの共有設定は「表1 Xサービスにおけるファイルの共有設定」に示す4種類であり、登録した利用アカウントと指定した利用アカウント以外のインターネット利用者全般が閲覧できてしまう設定は、番号3（ファイル共有先：パブリック、付与できる共有権限：閲覧権限）のみになります。

したがって、空欄a1はパブリック、空欄a2は閲覧権限となるので、**オ**が正解です。

(2)

本文中の下線①「直ちにXサービスに登録している全てのサービスを削除し、Xサービスの利用を中止するように指示した」について、この対応が必要な理由を問われています。

Xサービス利用については、「図1 Xサービスの利用規則（抜粋）」のように利用規則が定められています。しかし、ファイルの一つがインターネット上で公開されてしまったという事故があり、その原因が不明であることから、公開されてしまったファイル以外にも公開されているファイルが存在する可能性や、今後登録するファイルが公開される可能性が考えられます。このような被害

を広げるリスクを回避するには、Xサービスに登録しているファイルを削除し、利用を中止する必要があります。したがって、オが正解です。

設問2

〔原因調査〕についての問題です。本文中の下線②「プロキシサーバを調査した」について、調査を行う目的が問われています。

〔オンラインストレージサービス〕に、Xサービスは、「サービスへの接続にHTTP over TLS (HTTPS)を使用している」、「Webブラウザだけでなく利用を始められる」とあります。ここから、XサービスはWebサイトの閲覧を行う通信であることが分かります。

また、本文の最初の段落に、J社の「社外のWebサイトの閲覧は、全てプロキシサーバ経由とし」とあります。これは、Xサービス利用者はJ社のプロキシサーバを必ず通るということなので、プロキシサーバを調査することで、原因を見つけられる可能性があります。

これらを踏まえ、調査を行う目的として、(i)～(iii)について内容を確認していきます。

・(i)

今回インターネット上で公開されたのはXサービスに登録したファイルなので、その他のサービスが利用されたかを確認するのは適切ではありません。

・(ii)

Xサービスは業務上必要であり、接続が制限されていないので、一時的に制限を解除したWebサイトには含まれません。

・(iii)

Xサービスは、図1の利用規則に従い、製造部のみで利用されると定められています。そのため、製造部以外でXサービスが利用された形跡がないかどうかを確認する必要があります。これはプロキシサーバへのアクセス状況を調べることで確認できます。

したがって、(iii)のみが適切なので、キが正解です。

設問3

〔個別ヒアリング〕についての問題です。製造部の従業員に個別ヒアリングした結果「図2 ヒアリング結果(抜粋)」を基に、J社製造部の現状と行うべき対策について考えていきます。

(1)

本文中の空欄bに関する穴埋め問題です。

Xサービスにファイルを登録した後は、初期値設定(ファイル共有先“なし”、共有権限“権限なし”)から適切なファイル共有設定・共有権限に変更する必要があります。つまり、今回の事故の原因としては、この二つの設定を正しく行っていない場合が考えられます。図2を見ると、「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係る“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」とあり、ファイルを公開したという意識がなく操作していた従業員がいる可能性が考えられます。したがって、エが正解です。

ア 利用方法を知らない従業員は、利用していなければ問題ありません。

イ 利用規則の存在を全員が知っていることは望ましいことです。

ウ スマートフォンなどでの利用は禁じられており、そのような従業員がいなかったことは望ましいことです。

(2)

本文中の下線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」について、該当する対策を選びます。

第三者にファイルを読まれる可能性を下げるためには、ファイルを取得されても読まれないようにする対策と、ファイルを取得できる可能性を下げる対策の二つが考えられます。

まず、ファイルを取得されても読まれないようにするためには、情報の暗号化を行うことが有効です。また、ファイルを取得できる可能性を下げるためには、情報がJ社からB社へ伝わった後に速やかに削除することが有効です。この内容に当てはまるのは、(ii)、(iv)であり、ケが正解です。

(i)の電子署名は、改ざん検出や情報作成者の特定に利用でき、(iii)のハッシュ値は、改ざん検出に利用できますが、どちらも今回の目的には関係ありません。

設問4

〔問題点の整理、対策の検討〕についての問題です。一連の事故に関して、表2に問題点を整理し、新しいオンラインストレージサービスへの変更を検討します。

(1)

表2中の空欄c、dに対する穴埋め問題です。

空欄c

番号1の問題点について考えます。番号1の理由に「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」とあります。〔原因調査〕に、Xサービスでは、「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」という記述があります。つまり、通常の場合には操作の履歴情報が提供されないのので、必要に応じて操作履歴を調べることができません。したがって、空欄cはイが正解です。

空欄d

番号3の問題点について考えます。番号3の理由に「2要素認証などの強固な対策が必要である」とあります。2要素認証とは、「知識、保持、生体」の認証のうち二つの要素を使用した認証方法です。Xサービスは、メールアドレスとパスワードだけで利用できるため、1要素(知識のみ)しか使用していません。したがって、空欄dはオが正解です。

(2)

表2中の空欄e、fに対する穴埋め問題です。

番号2の問題点に「従業員が自由にファイル共有を設定することができる」とあり、さらに図2に、「共有設定に係する“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」とあります。これは、“誤操作”で不適切な設定をし

てしまう可能性があることを示します。また、自由にファイル共有を設定することができると、組織内の不正行為により“意図的な公開”をされることも考えられます。

したがって、空欄e、fはイ、エが正解です(順不同)。

(3)

本文中の下線④「事故発生時の原因特定は困難です」について、図1から、その理由となっているものを特定します。

図1の3に、「メールアドレスをXサービス専用の一つ設け、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」とあります。これは、J社製造部でアカウントを共有することなので、事故発生時に原因となる従業員を特定することができなくなります。したがって、ウの3が正解です。

1の社外での業務利用禁止や、2のファイルの内容制限、4のパスワード更新は必要であり、問題はありません。また、5のファイル権限変更の方法は適切です。

(4)

本文中の下線⑤「組織的対策」と下線⑥「技術的対策」として行うべき対策を合わせて三つ選びます。それぞれの対策について、適切かどうかを確認していきます。

[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は、通常、自由な秘密保持契約はできません。

・(ii)

業務に関係がないWebサイトは、すでにコンテンツフィルタで制限されています。

・(iii)

今回、製造部独自に行ったXサービスの利用で問題が起こったため、情報セキュリティ委員会の承認を求めるような変更は適切です。

・(iv)

利用アカウントの共有については、(3)の解答のとおり、事故発生時の原因特定が困難となるため、禁止することは適切です。

[情報システム課が行うべき技術的対策]

・(v)

利用アカウントの共有は禁止される予定なので、新たなサービスでの専用の利用アカウントは不要です。

・(vi)

オンラインストレージサービスの利用目的は、他社とのファイル共有のみなので、バックアップは必要ありません。

・(vii)

委託先であるB社とファイルをやり取りするだけなので、電子署名で真正性や完全性を確認する必要はありません。

・(viii)

オンラインストレージサービスを自由に利用できるようにすると、不適切に使用される可能性があるため、コンテンツフィルタで制限することは適切です。

したがって、適切な対策は、(iii)、(iv)、(viii)の三つとなり、キが正解です。

問2

情報機器の紛失

《解答》

設問1	a ア	b エ	c イ	d エ	
設問2	(1) ア	(2) ク	(3) e イ	(4) f イ	(5) g イ

《解説》

情報機器の紛失に関する問題です。電車にNPC（ノートPC）を置き忘れるというインシデントに対して、インシデント報告書を作成し、影響を調査して対応します。Z社の情報セキュリティ対策の基準や役割分担を整理して読み取る必要がある問題です。

設問1

〔インシデント報告書案の作成〕についての問題です。「図2 インシデント発生とその初動対応の経緯」をまとめ、空欄a～dを埋めていきます。

空欄a

11:00の初動対応(a) K課長の実施内容について、図2に記述がないものを考えます。

〔情報機器の紛失〕の記述より、K課長は営業部1課の情報セキュリティリーダーです。「図1 情報機器の紛失・盗難発生時の対応手順(抜粋)」の「2. 初動対応」によると、「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」ことが必要です。このうち、図2に記載されておらず、情報セキュリティリーダーが対応可能なものとしては、FさんのNPCに保存されていた情報の内容及び量があります。

したがって、空欄aはAの「Fさんが紛失した情報の内容及び量の特定」が正解となります。

空欄b

11:00の初動対応(b) W主任の実施内容について、図2に記述がないものを考えます。

〔情報機器の紛失〕の記述より、W主任はR支社の情報システム担当として初動対応に当たります。

本文中に、「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」とあり、情報システム

担当の役割に“情報セキュリティ対策の設定と維持”があることが分かります。空欄aでも取り上げた図1の「2. 初動対応」に、情報セキュリティリーダーが当該拠点の情報システム担当と協力して行うことに、「情報セキュリティ対策の実施状況を確認」とあるので、情報システム担当は、担当していた紛失機器における情報セキュリティ対策の実施状況を確認する必要があります。

したがって、空欄bはエの“情報セキュリティ対策の実施状況の確認”が正解となります。

空欄c

空欄bと同様に、初動対応でW主任が行うことのうち、システムの特定にかかわることを考えます。

「表1 NPCの情報セキュリティ対策と持出し管理ルール」より、Z社のNPCでの認証には、OSやBIOSなどのパスワード認証に加え、クライアント証明書によるクライアント認証が設定され、2要素認証の仕組みが提供されています。クライアント認証では、NPC上にクライアント証明書と秘密鍵をインストールするため、今回紛失したNPCにはFさん用の設定として、Fさんのクライアント証明書と秘密鍵はインストールされていると考えられます。つまり、紛失したNPCには情報システムのアカウント情報としてFさんの秘密鍵が含まれるため、パスワードが破られるとLシステムに侵入可能です。

図1の「2. 初動対応」に、「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」とあります。そのため、Fさんが外出先からアクセスできるシステムを特定し、Fさんのアクセス権を無効化する必要があります。

したがって、空欄cはイの“Fさんが外出先からアクセスできる”が正解となります。

空欄d

空欄cの説明でも述べたように、今回紛失したFさんのNPCでは、パスワードが特定されると、社外からZ社のシステムへアクセスすることが可能となります。アクセスを試行するために辞書攻撃やパスワードリスト攻撃が使われるかもしれませんが、アクセスに成功した場合にはシステムの内容が改ざんされてしまうかもしれません。そのため、状況を絞って確認するのではなく、社外からの不審なアクセスについて幅広く確認する必要があります。したがって、空欄dはエの“社外から不審なアクセスがないかどうかの幅広い確認”が正解です。

設問2

【インシデントの影響及び対応】についての問題です。インシデントの影響範囲を確認し、対応方法を検討します。ISMSでの適切な情報セキュリティ対策に合わせた最善の対策を考えることが大切です。

(1)

本文中の下線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」について、具体的な保存方法が問われています。(i)～(v)の中で追加する方法として可能なものを検討していきます。

・(i)

NPC期間持出しの承認を得る場合には、表1に「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」とあり、何度もNPCを持ち出して会社に持ち帰ることが想定されています。つまり、NPCを会社に持ち帰ることは可能で、そのときに追加で顧客情報を保存することができます。

・(ii)

表1の「全PCのための情報セキュリティ対策」(g)に、外部記憶媒体の接続制限がありますが、Z社が従業員に貸与するUSBメモリは接続可能です。そのため、会社貸与のUSBメモリに顧客情報を保存して持ち出すことによって、NPCに保存できます。

・(iii)

表1の「NPCのための情報セキュリティ対策」(i)に、Lシステムを利用するためにはクライアント証明書が必要とありますが、持ち出すNPCにはインストールされているので、外出先からでもLシステムへのアクセスが可能です。そのため、外出先からLシステムにアクセスして顧客情報をダウンロードして保存することができます。

・(iv)

外出先でNPCを用いて他社の公開Webサイトを閲覧することは可能です。しかし、公開情報には顧客情報は特に含まれていないので、今回の保存方法には該当しません。

・(v)

(ii)でも述べましたが、Z社のNPCには外部記憶媒体の接続制限があります。そのため、顧客から借りたUSBメモリからの情報はコピーできません。

したがって、保存可能な方法は(i)、(ii)、(iii)となり、アが正解です。

(2)

本文中の下線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」について、表1から最も効果的な対策を確認します。

表1の(a)～(i)のうち、(a)、(b)、(f)、(i)は、NPCへのアクセスを制御するための対策です。アクセス制御により、NPC内の情報を盗まれるリスクはいくらか減少しますが、直接の対策ではありません。

また、(c)、(d)、(e)、(g)は、マルウェアの感染防止や脆弱性対策なので、直接の対策とはなりません。

(h)のHDD全体の暗号化は、HDDが抜き取られても情報漏えいを防止できるということで、NPCの中の情報を盗まれるリスクを低減する対策となります。

したがって、最も効果的なものは(h)となり、クが正解です。

(3)

空欄e1、e2の穴埋め問題です。秘密鍵の漏えいの有無を調査するための方法について問われています。

空欄e1

Fさんの秘密鍵が漏えいした場合、2要素認証のうちの一つであるクライアント認証が成功します。その後、Lシステムにアクセスするためには、パスワード認証にも成功する必要があります。辞書攻撃やパスワードリスト攻撃などを行うためには何度もアクセスを試みるので、アクセスを試みた形跡があれば、秘密鍵が漏えいしていると考えられます。したがって空欄e1は、**アクセスを試みた形跡**となります。

空欄e2

Lシステムへアクセスされる可能性がある時間帯について考えます。図2より、11:20にFさんのアクセス権は無効化されています。しかし、NPCが無事回収できたのは14:50で、その間に不正アクセスを試みられた可能性があります。そのため、11:20以降のログも確認する必要があります。15時頃にはNPCを回収しているので、確実に戻ってきたと判断できる15:30まで確認できれば万全です。したがって空欄e2は、**本日00:00から15:30まで**となります(開始時刻については、選択肢ですべて00:00からとなっているので、考慮の必要はありません)。

組み合わせると、イが正解となります。

(4)

空欄fの穴埋め問題です。Fさんのアクセス権を有効にするための手順を考えます。

表1の注¹⁾に、「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」とあります。つまり、FさんがNPCを紛失している間に、何者かがNPCにアクセスし、秘密鍵をエクスポートして取り出した可能性は否定しきれません。そのため、Fさんの従来のクライアント証明書を利用するのは危険なので、失効させる必要があります。その場合には、Fさんには新しいクライアント証明書を発行し直す必要があり、新しい鍵ペアを生成します。

したがって、空欄fはイとなります。

(5)

空欄g1、g2の組合せ穴埋め問題です。FさんのNPCの対処方法について、適切なものを解答群から考えていきます。

ア HDDを複製しての調査は、マルウェアの感染などを確認する場合には有効です。しかし、FさんのNPCをそのまま返却することは、マルウェアに感染していた場合に被害が広がるので不適切です。

イ 証拠保全と、Fさんに新しいNPCを手配することは、調査と安全なPCの使用が両立できるので、コストはかかりますが最も適切です。

ウ HDDの破棄は、証拠を保全して調査する必要があることに対しては不適切です。

エ NPCの初期化は、証拠が消えてしまうので不適切です。

オ Fさんの点検だけでは、不審なファイルを見つけるのには不十分です。Fさんは専門家ではないため、システムファイルなどが変更されていても分からないと考えるのが妥当です。

したがって、最も適切なものはイです。

問3

業務用PCでのWebサイト閲覧

《解答》

- 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) エ (3) g イ

《解説》

業務用PCでのWebサイト閲覧に関する問題です。不正プログラムによる不審なWebアクセスについて、その挙動をインシデントとして発見し、初動対応及び調査、改善を行います。

設問1

〔インシデントの発見と初動対応〕についての問題です。行うべき初動対応について検討していきます。

(1)

本文中の下線①「Eさんに初動対応を指示」について、指示すべき初動対応を(i)～(v)からすべて選択します。優先順位としては、「図2 利用規程(抜粋)」の4に「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」とあるので、この二つを優先して考えます。

・(i)

E-PCのHDD内のフォルダとファイルに対しては、証拠を保全して後で調査できるようにする必要がありますので、何も操作をしないことは適切です。

・(ii)

PCの電源を強制切断することは、PCの故障の原因にもなります。また、メモリ上の証拠が失われるので、証拠保全の観点から適切ではありません。

・(iii)

E-PCをLANから切り離すことは、マルウェアの感染など、被害拡大を防止するために必要です。

・(iv)

PCを再起動するとメモリ上の証拠が失われるので、証拠保全の観点から適切ではありません。

・(v)

E-PCを使って基盤情報システムにアクセスすることは、マルウェアの感染など、被害拡大の可能性があるので、適切ではありません。

したがって、指示すべき初動対応は(i)、(iii)の二つとなり、イが正解です。

(2)

空欄a1～a3の組合せに関する穴埋め問題です。今回の問題の調査に必要な情報について考えていきます。

〔インシデントの発見と初動対応〕において、不審なアクセスは、「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」が前週に比べて大幅に増えていたことから発見されています。つまり、通常は休日である時間帯のアクセスです。

本文中の空欄a1～a3が含まれるB課長の調査では、Eさんは、「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」ことが判明しています。そのため、E-PCは休日にアクセスが可能な状態であったことが読み取れます。さらに、「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」とあるので、休日のアクセスは、Eさん以外の人が行った不正アクセスであると考えられます。

ここで、Eさんではないと推定するためには、大量の通信が記録されていた時刻にEさんがアクセスしていないことを確認する必要があります。Eさんの勤務時刻を確認するためには、勤怠管理情報を参照し、大量通信時にEさんが退勤していたかどうかを確認することが有効です。また、今回の不審なアクセスは、社内からインターネットへの通信なので、アクセスログはインターネットへのアクセスに絞って突き合わせる必要があります。

したがって、空欄a1は「勤怠管理情報」、空欄a2は「インターネット」、空欄a3は「退勤していた」となるので、組み合わせるとAが正解となります。

(3)

表1中の下線②「情報システム部が、次に示す調査及び対応を開始」の三つの調査について、該当する作業を考えます。

一つ目の「社内からアドレスYへの通信を遮断」については、プロキシサーバでアドレスYへの通信を遮断することが適切です。しかし、(iii)のように、ファイアウォールでプロキシサーバを経由しないものを許可してしまうと、ファイアウォールを通らない不正アクセスが可能となってしまうので、誤りとなります。

二つ目の「E-PCのHDD内のデータを証拠保全」については、(ii)のようにE-PCのHDDを別のHDDにフルコピーすることで証拠保全が可能です。また、HDDに対してフルスキャンを行うことは、マルウェアなどの検出に有効なので適切です。しかし、(i)のように封印して保管してしまうと、証拠から原因を特定できなくなるので不適切です。また、(iv)のようにE-PCをクリーンインストールすると、証拠も消去されてしまうので不適切です。

三つ目の「E-PCからの大量の通信の原因の把握」については、(v)のようにネットワーク機器やPC上のログを突き合わせて整理・分析することで可能です。

したがって、該当する作業は(ii)、(v)となり、力が正解です。

設問2

〔情報システム部による調査結果の中間報告〕についての問題です。調査結果を基に、EさんがアクセスしたWebサイトを推定し、対策を検討します。

(1)

空欄b～eに関する穴埋め問題です。EさんがアクセスしたWebサイトについて、アクセスした可能性とその状況について考えます。

空欄b, c

インターネット上のEさんがアクセスした可能性があるWebサイトについて考えます。〔情報システム部による調査結果の中間報告〕のD課長の発言に、「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」とあり、Eさんが悪意あるWebサイトにアクセスした形跡はありません。その場合に考えられるのは、正規のWebサイトの改ざんにより、閲覧するだけで不正プログラムに感染するようなスクリプトなどを埋め込まれた可能性です。したがって、空欄bはウの正規、空欄cはアの改ざんが正解となります。

空欄d, e

空欄b, cのように、正規のWebサイトが改ざんされた場合の状況について考えます。Webサイトの所有者たる企業は、改ざんというサイバー攻撃を受けており、被害者です。しかし、Webサイト閲覧者に不正プログラムによる被害を与える場合には、加害者の立場になります。したがって、空欄dはカの被害者、空欄eはアの加害者が正解です。

(2)

本文中の下線③のB課長の発言「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」について、B課長とD課長が協力して検討した対策を考えます。

空欄d, eで検討したような、Webサイト閲覧者に対して加害者になる可能性を減少させるためには、改ざんされないように、自社Webサイトの脆弱性を減少させる必要があります。その方法として、自社Webサイトの脆弱性検査を定期的を実施して、問題があれば修正することは有効です。また、新たな脆弱性が発見された場合にも、その都度適切な対応をとる必要があります。したがって、正解はウとなります。

ア アクセシビリティの見直しは、安全性の向上にはつながりません。

イ Webサーバをパブリッククラウドに移行してもデータはそのままなので、脆弱性の軽減にはつながりません。

エ ドライブバイダウンロード攻撃は、今回検討した、閲覧するだけで不正プログラムに感染するようなスクリプトを実行させる攻撃ですが、現時点で自社Webサイトに仕掛けられているわけではないので誤りです。

設問3

〔課題の改善〕についての問題です。今回の不正アクセスによる影響や、適切な対応策について検討します。

(1)

本文中及び図6の空欄fに対する穴埋め問題です。

内容が不明なデータがE-PCから大量に送信されたことから考えられるセキュリティ被害は、情報漏えいです。したがって空欄fはカとなります。その他の攻撃は、E-PCからではなくE-PCへの攻撃なので、今回の状況には当てはまりません。

(2)

図5中の下線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」について、社内共有フォルダNのアクセス権の設定単位を考えます。

「図3 プロキシサーバのログの調査結果」に、Eさんは「マーケティング1課に所属」とあります。また、「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」の「1. Eさんへのヒアリング結果」より、Eさんは社内共有フォルダNにアクセスし、ファイルを発見しています。しかし、「2. G主任へのヒアリング結果」に、「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、社内フォルダNに保存」とあるように、本来、アンケートファイルはマーケティング2課のみで使うものでした。EさんとG主任は課が違うため、アクセス権の設定単位は課単位ではなく、部単位であったと考えられます。また、Eさんは役職者ではないため、職位単位も考えられません。

したがって、エの部単位が正解となります。

(3)

本文中の空欄gに対する穴埋め問題です。B課長が、改善すべき課題が他にもないかを知るために実施するものです。

今まで見落としていたものを検討するためには、全ての情報資産を全体的に確認する必要があります。このとき、情報セキュリティマネジメントを考慮すると、リスクアセスメントを実施し、全ての情報資産とその取扱い状況を確認することが最適です。したがって空欄gは、イが正解となります。

アの脆弱性検査、エのウイルス対策ソフト、オのソフトZのインストールは、図1より、全社的に運用管理されるものなので、マーケティング部のみで検討できるものではありません。

ウのアクセス権限についても、アクセス権の設定単位によっては、マーケティング部だけでは管理できないもの（例えば職位単位のものなど）があるので、B課長の権限の範囲では実現できません。

INDEX

索引

数字

2段階認証	57
2要素認証	57
3DES	50
3-key Triple DES	50
36協定	202

A

ABC分析	338
AC	263
ACL	135
AES	50
AES-CCMP	143
AH	163
ANSI	208
ANY接続拒否	143
APT	38
ARP	284
ASCII	208
ASP	358
Authentication	56
Availability	157

B

B/S	344
BCM	236
BCP	89, 236, 240
BIA	236
BIOS	142
BPM	356
BPO	356
BPR	356
BP図	356
BSD	205
BYOD	147

C

CA	67
CAAT	219

CAB	239
Camellia	50
CAPTCHA	63
CC	113
CCE	114
C&Cサーバ	39
CEM	113
CEO	336
Certification	56
CIA	22
CIDR	283
CIO	336, 353
CISO	108, 336
CMDB	238
CMS	238
COBIT	223
COCOMO	262
Cookie	34, 62, 291
COSOフレームワーク	222
CPE	114
CPI	263
CPO	336
CRL	69
CRM	355
CRYPTREC	50, 111
CRYPTREC暗号リスト	111
CSA	224
CSF	232
CSIRT	109
CSR	207, 334, 368
CSRF攻撃	34
CSR調達	368
CV	263
CVE	114
CVSS	114
CWE	115
CWE-ID	115
CWE識別子	115

D

DaaS	358
DAS	324
DBMS	169, 299
DDoS攻撃	33
DELETE文	303
DES	49
DFD	356, 365
DHCP	285
DH鍵交換	53
DISTINCT	303
DKIM	141
DLP	146
DML	239
DMZ	135
DNS	36, 141, 285, 291
DNS amp攻撃	36
DNSSEC	141
DNSキャッシュポイズニング攻撃	36
DNSリフレクタ攻撃	36
DoS攻撃	33
DSA	53, 61

E

EAL	113
EAP	165
EC	292
ECC	53
ECDSA	53, 61
EDI	292
EMS	369
EOQ	338
ERP	354
E-R図	300, 356
ESP	163
ESSID	144
EV	263
EVM	262

EV SSL証明書 70
e-文書法 206

F

FAR 65
FP法 261
FROM句 303
FRR 65
FTP 285, 291
FTPS 164
FTTH 293
FW 135

G

GPKI 68
GPL 205
GRANT文 303
GROUP BY句 303

H

HAVING句 303
HDD 142
HIDS 136
HMAC 55, 63
HRM 335
HTML 285
HTTP 285
HTTPS 164, 285
HTTPレスポンス分割攻撃 34

I

IA 67
IaaS 358
ICMP 283
ICT 276
ICカード 65, 159
Identity Provider 62
IdP 62
IDS 136
IE 338
IEC 86, 208
IEEE 208
IEEE 802.1X 165
IETF 208

IFRS 343
IKE 163
IMAP 285, 290
INSERT文 303
Integrity 157
IP 282, 283
IPAセキュリティセンター 109
IPO 334
IPS 136
IPsec 163, 288
IPv4 283, 287
IPv6 287
IP-VPN 292
IPアドレス 286
IPスプーフィング 36
IP電話 293
IPマスカレード 287
IR 334
IS 208
ISMS 23, 84, 237
ISMS適合性評価制度 86
ISO 86, 208
ISO 31000 87
ISO/IEC 15408 113
ISO/IEC 27000 86
ISO/IEC 27000シリーズ 86
ISO/IEC 27001 23, 87
ISO/IEC 27002 23, 87
ISO/IEC 27003 87
ISO/IEC 27004 87
ISO/IEC 27005 87
ISO/IEC 27006 88
ISO/IEC 27007 88
ISO/IEC 27014 88
ITF法 219
ITIL 232
ITSMS 231
ITSMS適合性評価制度 232
ITU 208
ITU-T 69
ITU-T X.509 69
ITガバナンス 223
IT基本法 206

ITサービスマネジメントシステム 231
IT投資効果 364
IT投資マネジメント 353
IT保険 101
IV 143

J

JIPDEC 86, 100, 184
JIS 21, 208
JISA 204
JISC 208
JIS Q 15001 182
JIS Q 20000 232
JIS Q 27000 86
JIS Q 27001 23, 85, 87, 220
JIS Q 27002 23, 87, 220
JIS Q 27006 88
JIS Q 31000 87, 96
JIS X 5070 113
JIS X 25010 267
JOIN句 303
JPCERT/CC 109
JRAM 100
JRMS2010 100
JVN 109

K

KCipher-2 50
KMS 355
KPI 232
k-匿名化 186

L

L2スイッチ 280
L3スイッチ 281
LAN 276
LAN間接続装置 280
LDAP 63
LLC 334
LOC法 262
LP 338
LTE 293

M

MAC	63
MACアドレス	165, 282, 286
MACアドレスフィルタリング	165
MD5	54
MDM	147
MIME	290
MTBF	327
MTTR	327

N

NAPT	287
NAS	324
NAT	286
Need-to-knowの原則	127
NIDS	136, 167
NISC	110
NIST	50
NoSQL	311
NTP	145, 285

O

OCSP	70
OCSPレスポンス	70
OC曲線	339
OECD	183
OECD8原則	183
OECDプライバシーガイドライン	183
OEM	369
OJT	257
OLA	237
OMG	209
OP25B	141
OR	338
ORDER BY句	303
OSI基本参照モデル	279
OSコマンドインジェクション	35
OSのアップデート	140
OVAL	115

P

P/L	344
PaaS	358

PCI DSS	113
PDCAサイクル	23
PDPC法	342
PERT	258
PIA	185
PIN	65, 160
PKI	56, 67, 189
PMBOK	249
PMO	257
PMS	182
POP	285
POP3	290
PPP	282
PV	263

Q

QC七つ道具	340
--------	-----

R

RA	67, 236
RADIUS	165
RAID	319
RASIS	157
RAS技術	158
RC4	50
RDB	298
Reliability	157
Relying Party	62
RFC	208, 239
RFI	368
RFP	368
RFQ	368
Rivest's Cipher 4	50
ROA	346
ROE	346
ROI	346, 360
rootkit	32
RP	62
RPO	240
RSA	53, 60
RSA-PSS	60
RTO	240

S

S/Key	59
S/MIME	164
SaaS	358
SAML	62
SAN	324
SCAP	114
SCM	354
Security	157
SELECT文	303
Serviceability	157
SFA	355
SHA-1	55
SHA-2	55
SHA-256	55
SHA-384	55
SHA-512	55
SI	367
SIEM	147
SLA	233
SLM	233, 235
SMTP	285, 290
SMTP-AUTH	141
SMTPS	164
Smurf攻撃	33
SNS	357
SOC	108
SOHO	336
SPEC	326
SPF	141
SPI	263
SPOC	241
SQL	302
SQL-DCL	302
SQL-DDL	302
SQL-DML	302
SQLインジェクション	33
SQLインジェクション対策	172
SRI	337
SSH	164
SSID	144
SSIDステルス	144
SSL	163
SSLアクセラレータ	146

SSO 62
 ST 113
 SV 263
 SYN Flood攻撃 33

T

TCO 236, 328
 TCP 282, 284
 TCP/IPプロトコル群 277, 282
 TKIP 143
 TLS 163, 285
 TLS/SSL 163
 TPC-C 326
 Triple DES 50
 TSA 64

U

UDP 284
 UPDATE文 303
 UPS 243
 URL 291
 URLフィルタリング 142
 USBキー 160
 UTM 137

V

VA 70
 VLAN 166, 281
 VoIP 293
 VoLTE 293
 VPN 291

W

W3C 209
 WAF 135
 WAN 276
 WBS 255
 WBS辞書 256
 WBSテンプレート 255
 Web 291
 Webアプリケーションソフトウェア
 291
 Webサーバ 291
 Webのセキュリティ 141

Webブラウザ 291
 WEP 50, 143
 WHERE句 303
 WORM 147
 WPA 143
 WPA2 143

X

XCCDF 115
 XML署名 61
 XSS攻撃 34
 XY理論 335

あ

アードバリューマネジメント
 262
 アイリス認証 65
 アカウンタビリティ 336
 アクセス制御技術 134
 アクセス制御機能 180
 アクセス制御リスト 135
 アクセスログ 169
 アクティビティ 255, 258
 アクティビティリスト 258
 アドウェア 33
 アドレス変換 286
 アプリケーションゲートウェイ型
 135
 アプリケーションセキュリティ
 171
 アプリケーション層 279, 284
 粗利益 343
 粗利益率 346
 アローダイアグラム 258
 アローダイアグラム法 342
 暗号化 47
 暗号化アルゴリズム 47
 暗号化鍵 47
 暗号化技術 47
 暗号文 47

暗証番号 65
 安全性指標 347
 安全性分析 345

い

イーサネット 282
 意匠権 201
 一般競争入札 367
 移動体通信規格 293
 イニシャルコスト 328
 委任契約 203
 違法ダウンロード行為 200
 入口対策 39, 138
 インシデント 24, 81, 237
 インシデント及びサービス要求管理
 237
 インシデント管理 238
 インスペクション 267
 インターネット 276, 290
 インターネットVPN 291
 インターネット層 283
 インダストリアルエンジニアリング
 338
 インテグリティ 22
 インデックス 308, 309
 イントラネット 291
 インバスケット 257

う

ウイルス 32
 ウイルス作成罪 188
 ウイルス対策ソフト 138, 146
 ウイルス定義ファイル 138
 ウォークスルー 267
 ウォードライビング 36
 ウォームスタンバイ 318
 請負契約 203, 369
 売上原価 343
 売上総利益 343, 344
 売上高総利益率 346
 運用監視暗号リスト 111
 運用レベル合意書 237

え

営業秘密 201
 営業利益 344
 エージェント型 62
 エクストラネット 291

エスカレーション	241
エスケープ処理	34
エディットバリデーションチェック	
.....	219
エニーキャストアドレス	288
遠隔操作ウイルス	32
遠隔地バックアップ	159
エンティティ	22, 300

お

応答時間	326
オーセンティケータ	166
オープンソースライセンス	
.....	204
オブジェクト指向データベース	
.....	298
オプトアウト	190
オプトイン	190
オプトイン方式	190
オペレーショナルリスク	97
オペレーションズリサーチ	338
音声認証	65
オンラインストレージ	291

か

カーディナリティ	300
回帰分析	342
解決プロセス	237
改ざん	54
改善勧告	218
回線交換	278
階層型組織	336
階層型データベース	298
開発投資対効果	364
外部監査	216
顔認証	65
可監査性	219
鍵	47
鍵共有	52
鍵長	49
鍵付きハッシュ関数	55
拡張認証プロトコル	165
確定版メディアライブラリ	239
過失犯	28

仮想LAN	281
稼働統計	289
稼働率	327
カナリアコード	171
株式会社	334
株式公開	334
可用性	22, 157
環境評価基準	115
環境的な脅威	25
関係データベース	298
関係プロセス	237
監査	216
監査計画	217
監査証拠	217
監査証跡	219
監査調査	218
監査手続	217
監査報告書	218
監査モジュール法	218
監視カメラ	158
完全性	22, 157
ガントチャート	260
ガンブラー	37
管理図	266, 341
管理目的及び管理策	85

き

キーペア	48, 51
キーロガー	32
機会	26
企画競争入札	367
企業経営	334
企業の社会的責任	
.....	207, 334, 368
技術採用指針	354
技術者倫理	207
機能的評価指標	241
基本評価基準	115
機密性	22, 157
キャッシュフロー計算書	
.....	343, 344
ギャップ分析	231
キャパシティ管理	236
ギャランティ型	292

脅威	24
教育技法	257
供給者管理	237
共通鍵	48
共通鍵暗号方式	48
共通脆弱性識別子	114
共通脆弱性タイプ一覧	115
共通脆弱性評価システム	114
共通セキュリティ設定一覧	114
共通プラットフォーム一覧	114
業務流れ図	356
業務プロセス	356
共有ロック	305
緊急時対応計画	89
緊急事態の区分	89
金銭奪取	28

く

クエリ	299
クッキー	34, 62, 291
組合せアプローチ	100
クライアント	277
クライアントサーバシステム	319
クライアント証明書	69
クラウドコンピューティング	358
クラウドサービス	144
クラウドサービスのセキュリティ	
.....	144
クラスタ	323
クラスタ分析	342
クラッカー	28
クラッキング	27, 134
クラッシング	259
クリアスクリーン	159
クリアデスク	159
グリーンIT	243
グリーン調達	368
クリエイティブ・コモンズ	204
クリエイティブ・コモンズ・	
.....	204
ライセンス	204
クリックジャッキング	37
グリッド・コンピューティング	
.....	311
クリティカルチェーン法	259

クリティカルパス	258
クリティカルパス法	258
グローバルIPアドレス	286
クロスサイトスクリプティング攻撃	34
クロスサイトスクリプティング対策	171
クロスサイトリクエストフォージェリ 攻撃	34

け

経営分析	345
計画値	263
経済協力開発機構	183
経常利益	344
系統図法	341
刑法	187
ケーススタディ	257
ゲートウェイ	281
ゲーム理論	339
決算	343
検疫ネットワーク	139, 166
原価	343
減価償却	345
検査手法	339
検証局	70
現状評価基準	115

こ

コアコンピタンス	356
故意犯	28
広域Ethernet	293
公益通報者保護法	203
公開鍵	48, 51
公開鍵基盤	56, 67, 189
公開鍵証明書	68
虹彩認証	65
合資会社	334
更新後ログ	307
更新前ログ	307
構成管理	238, 289
構成管理システム	238
構成管理データベース	238
構成品目	239

合同会社	334
行動科学	335
行動の特徴	65
合名会社	334
ゴーイングコンサーン	334
コーディネーションセンター	109
コーポレートアイデンティティ	334
コーポレートガバナンス	335
コールドスタンバイ	318
国際連携CSIRT	109
国際規格	208
国際財務報告基準	343
国際電気通信連合	69, 208
国際電気標準会議	86, 208
国際標準化機構	86, 208
故障率	327
個人情報	83
個人情報事業者	184
個人情報保護法	182, 184
個人情報保護方針	83, 182
個人情報保護マネジメント	182
個人情報保護マネジメントシステム	182
個人番号	184
コスト効率指数	263
コスト差異	263
コスト見積手法	261
固定長期適合率	347
固定費	343
固定比率	347
コピープロテクト外し	200
コピーレフト	204
コモンライテリア	113
混合戦略	339
コンティンジェンシープラン	89
コントロールトータルチェック	219
コンピテンシ	335
コンピュータウイルス	32
コンピュータウイルス対策基準	190
コンピュータ支援監査技法	219
コンピュータ犯罪防止法	187

コンピュータ不正アクセス対策基準	190
コンピュータリテラシ	360
コンプライアンス	207
コンプライアンス監査	221
コンペ法	146

さ

サーバ	277
サーバ証明書	69
サービス可用性管理	236
サービス継続	235
サービス継続及び可用性管理	235
サービス資産	81
サービス提供プロセス	235
サービスデスク	241
サービスの移行	234
サービスの運用	240
サービスの設計	234
サービスの報告	235
サービスの予算業務及び会計業務	236
サービス不能攻撃	33
サービスマネジメント	231
サービスマネジメントプロセス	235
サービス目標	235
サービスライフサイクル	232
サービスレベル管理	233, 235
サービスレベル合意	233
最高経営責任者	336
最高個人情報保護責任者	336
最高情報責任者	336, 353
最高情報セキュリティ責任者	336
在庫管理	338
財産損失	96
最小権限の原則	127
サイドチャネル攻撃	38
サイバー攻撃	31
サイバーセキュリティ	178
サイバーセキュリティ基本法	178
サイバーセキュリティ戦略の 基本原則	110

サイバーセキュリティ戦略本部 110, 178, 179	システム監査技法 218	情報資産目録 95
サイバーテロリズム 28	システム監査人 217	情報システム化委員会 354
財務諸表 343	システム管理基準 220	情報システム戦略 353
サイン 65	システム構成 317	情報システム導入リスク分析 364
先入先出法 345	システムの移行方式 234	情報システム・モデル取引・契約書 203
詐欺犯 28	システムライフサイクル 360	情報社会 276
サテライトオフィス 336	下請法 203	情報セキュリティ 20
サブネットアドレス 283	失効リスト 69	情報セキュリティ委員会 108
サブネットマスク 283	実コスト 263	情報セキュリティインシデント 81
サプライチェーンマネジメント 354	実用新案権 201	情報セキュリティ監査基準 220
サプライチェーンリスク 97	指摘事項 218	情報セキュリティ管理 80, 237
サプライヤ 268	支払用カード電磁的記録 不正作出等罪 188	情報セキュリティ管理基準 220
サブリカント 166	資本生産性 348	情報セキュリティ管理責任者 108
差分バックアップ 308	指紋認証 65	情報セキュリティ教育 126
産業財産権 201	社会的責任投資 337	情報セキュリティ啓発 126
三者間認証 56	収益性指標 346	情報セキュリティ事象 81
散布図 340	収益性分析 345	情報セキュリティ早期警戒 パートナーシップ 109
サンプリング 186, 339	集中処理 318	情報セキュリティ対策基準 83
残留リスク 102	収入減少 96	情報セキュリティ対策ベンチマーク 116
し		
シェアドサービス 355	重要業績評価指標 232	情報セキュリティ方針 82
自家発電装置 243	重要成功要因 232	情報セキュリティ方針 82
事業関係管理 237	縮退運転 323	情報セキュリティポリシー 80, 82
事業継続管理 236	出向契約 370	情報セキュリティマネジメント 80
事業継続計画 89, 236, 240	守秘 51	情報セキュリティマネジメント システム 23, 84
事業部制組織 336	準委任契約 203, 369	情報セキュリティリスク 25
時刻認証 56, 64	純粹戦略 339	情報セキュリティリスクアセスメント 84, 98
時刻認証局 64	障害回復処理 306	情報セキュリティリスク対応 85, 101
時刻認証サービス 64	障害管理 289	情報提供依頼書 368
自己資本比率 348	障害時運用設計 240	情報配布 269
自己資本利益率 346	障害復旧 89	情報倫理 207
資産管理 345	障害報告書 266	静脈認証 65
資源の利用状況に関する指標 241	状況的犯罪予防 27	職能別組織 336
辞書攻撃 31	詳細リスク分析 100	職務の分掌 223
システムインテグレータ 367	使用性評価指標 241	助言型監査 216
システム運用管理者 240	衝突発見困難性 54	所持 57
システム化計画 354, 363	商標権 200, 201	助長行為 180
システム化構想 363	情報 80	署名 52
システム監査 216, 219	情報化推進体制 354	ショルダハッキング 36
システム監査企業台帳 217	情報化投資計画 353	シリアル番号 69
システム監査基準 219	情報化保険 101	
	情報サービス産業協会 204	
	情報資産 24, 80, 95, 220	
	情報資産台帳 81, 95	

新QC七つ道具	341
人為的な脅威	25
シンクライアント	323
シングルサインオン	62
真正性	22, 60
人的資産	80
人的セキュリティ対策	124
人的損失	97
侵入検知システム	136
侵入防御システム	136
信頼性	23, 157
信頼性計算	328
信頼性設計	322
信頼性評価指標	241
親和図法	341

す

推奨候補暗号リスト	111
スイッチ	281
スイッチングハブ	280
スキャベンジング	36
スクリプトキディ	27
スケジュール効率指数	263
スケジュールコントロール	259
スケジュール差異	263
スケジュール設計	240
スケジュール短縮手法	259
スコープクリーブ	254
スコープコントロール	254
ステークホルダ	102, 248, 253
ステークホルダ登録簿	253
ステガノグラフィ	144
ストアドプロシージャ	304
ストライビング	320
ストリーム暗号	49, 50
ストレージ	324
スナップショット	310
スニッフィング	31
スパムメール	190
スマートデバイス	142
スマートデバイスのセキュリティ	142
スマートフォン安全安心強化戦略	191

スマートユースイニシアティブ	191
スライシング	310
スループット	326

せ

正規化	300
生産性指標	348
生産性分析	345
脆弱性	25
脆弱性管理	140
脆弱性検査	116
脆弱性修正プログラム	140
脆弱性データベース	109
生体	57
生体認証	65
正当化	26
性能管理	289
性能指標	241
信頼性指標	327
製品を識別するためのCPE	114
政府機関の情報セキュリティ	
対策のための統一基準	191
政府認証基盤	68
責任損失	96
責任追跡性	22
セキュアプログラミング	171
セキュアプロトコル	163
セキュリティオペレーションセンター	108
セキュリティ検査言語	115
セキュリティ設定共通化手順	114
セキュリティ設定チェックリスト	
記述形式	115
セキュリティターゲット	113
セキュリティトークン	59
セキュリティ便	159
セキュリティホール	
	38, 134, 140
セキュリティワイヤ	243
施錠管理	159
セッション層	280
世代管理	308
セッションID	35

セッションハイジャック	35
設備生産性	348
ゼロデイ攻撃	38
善管注意義務	203
線形計画法	338
先進的で執拗な脅威	38
全体開発スケジュール	363
全体最適化方針	354
全体最適化計画	354
全体システム化計画	353
占有ロック	305
専用回線	292
専用線	292

そ

素因数分解	53
総当たり攻撃	31
送金内容認証	64
総合評価落札方式	367
相互監視	125
総資産利益率	346
総資本回転率	346
増分バックアップ	308
層別	340
総保有コスト	236
ソーシャルエンジニアリング	36
ソーシャルメディアガイドライン	
	191
経営組織	336
組織内CSIRT	109
組織における内部不正防止	
ガイドライン	124
ソフトウェア開発委託	
基本モデル契約	204
ソフトウェア開発契約	203
ソフトウェア資産	80
ソフトウェア障害	306
ソフトウェア使用許諾契約	204
ソフトウェア脆弱性	138
ソフトウェア等脆弱性関連情報	
取扱基準	190
ソリューションビジネス	358
ソルト	55, 60
損益計算書	343, 344

損益分岐点…………… 343

た

ターンアラウンドタイム…………… 326
 第三者中継…………… 35
 第三者提供…………… 182
 貸借対照表…………… 343, 344
 ダイシング…………… 310
 耐震耐火設備…………… 158
 耐タンパ性…………… 65
 タイムスタンプ…………… 64
 楕円曲線暗号…………… 53
 他人受入率…………… 65
 タブナビング…………… 34
 多要素認証…………… 57
 単一窓口…………… 241
 男女雇用機会均等法…………… 203
 段数…………… 50

ち

チェックサム法…………… 146
 チェックシート…………… 341
 チェックポイント…………… 307
 チケット…………… 62
 チケット型…………… 62
 知識…………… 57
 知的財産権…………… 200
 チャレンジ…………… 58
 チャレンジレスポンス方式…………… 58
 中央サービスデスク…………… 242
 調達…………… 367
 調達コントロール…………… 268
 調達実行…………… 268
 調達終結…………… 268
 調達マネジメント計画…………… 268
 調達リスク分析…………… 369
 直接的情報資産…………… 81
 直列システム…………… 328
 著作権…………… 200
 著作権法…………… 200
 著作権隣接権…………… 200
 著名表示冒用行為…………… 201

つ

通信サービス…………… 292
 通信ネットワーク…………… 276
 通信プロトコル…………… 282

て

提案依頼書…………… 368
 定額法…………… 345
 定期発注方式…………… 338
 ディザスタリカバリ…………… 241
 ディザスタリカバリサイト…………… 318
 デジタル証明書…………… 67, 68
 デジタル署名…………… 60
 デジタルディバイド…………… 360
 デジタルフォレンジックス…………… 145
 ディスクロージャ…………… 336
 定性的リスク分析…………… 99
 定率法…………… 345
 定量的リスク分析…………… 99
 定量発注方式…………… 338
 ディレクトリサービス…………… 63
 ディレクトリトラバーサル…………… 35
 データウェアハウス…………… 310
 データサイエンティスト…………… 311
 データ制御言語…………… 303
 データ操作言語…………… 302
 データ定義言語…………… 302
 データディクショナリ…………… 299, 300
 データ分析…………… 300
 データベース…………… 298
 データベースアクセス制御…………… 169
 データベースアクセス層…………… 319
 データベース暗号化…………… 169
 データベース管理システム…………… 299
 データベースセキュリティ…………… 169
 データベースバックアップ…………… 169
 データマイニング…………… 310, 311, 360
 データリンク層…………… 280
 テーラリング…………… 248
 出来高…………… 263
 出口対策…………… 39, 138
 テザリング…………… 293
 デジュレスタンドアード…………… 209
 テッドロック…………… 306

デファクトスタンダード…………… 209
 デフォルトゲートウェイ…………… 285
 デュアルシステム…………… 317
 デュアルライセンス…………… 205
 デュプレックスシステム…………… 158, 317
 デルファイ法…………… 342
 電気通信事業者…………… 276
 電気電子学会…………… 208
 電子計算機使用詐欺罪…………… 187
 電子計算機損壊等業務妨害罪…………… 187, 188
 電子商取引…………… 292
 電子消費者契約法…………… 204
 電子証明書…………… 189
 電子署名及び認証業務等に関する法律…………… 189
 電子署名法…………… 189
 電子透かし…………… 144
 電子政府推奨暗号リスト…………… 50, 111
 電子帳簿保存法…………… 206
 電子データ交換…………… 292
 電磁的記録…………… 206
 電磁的記録不正作出及び供用罪…………… 187
 電磁的記録の供用…………… 187
 電磁波解析攻撃…………… 38
 電子メール…………… 290
 電子メールのセキュリティ…………… 140
 テンベスト攻撃…………… 38
 電話回線…………… 292

と

動機…………… 26
 統計的サンプリング法…………… 218
 統合脅威管理…………… 137
 統合的制御プロセス…………… 238
 当座比率…………… 347
 投資の意思決定…………… 364
 投資利益率…………… 360
 統制自己評価…………… 224
 登録局…………… 67
 トークン…………… 59
 トータルフロート…………… 258
 特性要因図…………… 341

特定個人情報の適正な取扱いに 関するガイドライン	185
特定電気通信役務提供者	189
特定商取引法	204
特定電子メール送信適正化法	190
特定電子メールの送信の適正化等に 関する法律	190
特定電子メール法	190
匿名化	186
特許権	200, 201
特権的アクセス権	127
トップマネジメント	84
ドメイン名に係る不正行為	201
ドライブバイダウンロード攻撃	37
トランザクション	299
トランザクション管理	305
トランザクション障害	306
トランスポート層	280, 284
ドリリング	310
トレース	219
トレードオフ	252
トレードシークレット	201
トロイの木馬	32

な

内外作基準	367
内閣サイバーセキュリティセンター	110, 191
内部関係者	27
内部監査	85, 216
内部不正対策	124
内部統制	222
内容認証	55, 63
ナッシュ均衡	339
ナレッジマネジメント	355, 360

に

二者間認証	56
二重化技術	158
日本工業規格	21, 208
日本工業標準調査会	208
日本シーサート協議会	109
日本情報経済社会推進協会	100, 184

入退室管理	159
認証	56
認証VLAN	166
認証機関	86
認証局	67
認証サーバ	166
認証スイッチ	281
認証の3要素	57
認証連携型	62
認定機関	86
認定認証事業者	189

ね

ネットワーク	276
ネットワークアドレス	283, 284
ネットワークインタフェース層	282
ネットワーク型IDS	136
ネットワーク型侵入検知システム	167
ネットワーク型データベース	298
ネットワーク管理	289
ネットワーク社会	276
ネットワークセキュリティ	165
ネットワーク層	280

の

ノード	288
-----	-----

は

パーソナルファイアウォール	146
バーチャルサービスデスク	242
ハードウェア障害	306
ハードディスク	142
ハードディスク暗号化	142
バイオメトリクス認証	65
廃棄	160
排他制御	305
ハイブリッド暗号	164
パイロット移行方式	234
パイロットシステム	234
バインド機構	34, 172
ハクティビズム	28
暴露ウイルス	32

バケット交換	278
バケットフィルタリング	165
バケットフィルタリング型	135
派遣契約	370
パスワード	58
パスワード管理	126
パスワード認証	57
パスワードリスト攻撃	31
パスワードリマインダ	58
パターンファイル	138
パターンマッチング	146
ハッカー	28
ハッキング	28
バックアップ	89, 159, 308
バックドア	32
バックワードパス	259
発行局	67
ハッシュ	53, 58
ハッシュ関数	54
ハッシュ値	54
バッチ処理	319
バッファ	33
バッファオーバフロー攻撃	33
バッファオーバフロー対策	171
発明	201
ハニーポット	168
バランスシート	344
パリティディスク	321
バレー図	340
バレー図分析	342

ひ

ピアツーピア	323
ヒギーバック	159
非機能要求グレード	366
非機能要件	366
非形式的アプローチ	100
非公知性	201
秘密保持義務	125
ビジネスインパクト分析	235
ビジネスプロセスアウトソーシング	356
ビジネスプロセスマネジメント	356

- ビジネスプロセスリエンジニアリング 356
 ヒストグラム 340
 ビッグデータ 311
 秘匿化 140
 否認防止 23
 非武装地帯 135
 ビヘイビア法 146
 秘密鍵 48, 51
 秘密鍵暗号方式 48
 秘密管理性 201
 秘密指定 124
 ヒヤリハット 238
 ヒューマンエラー 323
 ヒューマンリソースマネジメント 335
 評価保証レベル 113
 標的型攻撃 38
 標的型攻撃メール 38
 平文 47
 品質管理 266
 品質管理手法 340
 品質計画 266
 品質コントロール 266
 品質評価 218
 品質保証 266
 品質マネジメント 266
 品質マネジメント計画 266
- ふ**
- ファイアウォール 135
 ファイバチャネル 324
 ファイル転送 291
 ファシリティマネジメント 243
 ファジング 140
 ファストトラッキング 259
 ファブレス 369
 ファンクション 261
 ファンクション層 319
 ファンクションポイント 262
 ファンクションポイント法 261
 フィッシング 37
 フールブルーフ 323
 フェールオーバー 318
 フェールセーフ 322
 フェールソフト 323
 フェデレーション型 62
 フォールトアポイダンス 322
 フォールトトレランス 322
 フォールトマスキング 323
 フォールバック 323
 フォローアップ 218
 フォロー・ザ・サン 242
 フォワードパス 259
 不稼働率 327
 負荷分散 323
 復号 47
 復号鍵 47
 不実の電磁的記録の作出 187
 不正アクセス 134
 不正アクセス禁止法 180
 不正アクセス行為 180
 不正アクセス対策 134
 不正競争防止法 201
 不正指令電磁的記録に関する罪 188
 不正のトライアングル 26
 不正のメカニズム 26
 復旧計画 89
 プッシュ型 269
 フットプリンティング 38
 物理層 280
 物理的資産 80
 踏み台 33, 35
 踏み台攻撃 35
 ブライバシーアーキテクチャ 185
 ブライバシー影響評価 185
 ブライバシーフレームワーク 185
 ブライバシーマーク 184
 ブライバシポリシ 83
 ブライベートCA 68
 ブライベートIPアドレス 286, 291
 ブラウザハイジャック 32
 ブリッジ 280
 プリバードステートメント 34
 ブルートフォース攻撃 31
 ブル型 269
 フルバックアップ 308
 ブレースホルダ 34
 フレーム 37
 プレーンストーミング 264
 プレゼンテーション層 279, 319
 プロアクティブ 240
 ブロードキャストアドレス 284
 プロキシサーバ 167, 287
 プロジェクト 248
 プロジェクト憲章 252
 プロジェクトコストマネジメント 261
 プロジェクトコミュニケーション
 マネジメント 269
 プロジェクト資源マネジメント 257
 プロジェクトスコープ 254
 プロジェクトスコープ記述書 254
 プロジェクトスコープマネジメント 254
 プロジェクトステークホルダ
 マネジメント 253
 プロジェクトタイムマネジメント 258
 プロジェクト調達マネジメント 268
 プロジェクト統合マネジメント 252
 プロジェクト品質マネジメント 266
 プロジェクトマネジメント 248
 プロジェクトマネジメントオフィス 257
 プロジェクトマネジメント知識体系 249
 プロジェクトライフサイクル 250
 プロジェクトリスクマネジメント 264
 ブロック暗号 49
 プロトコル 277
 プロバイダ責任制限法 189
 分散処理 318
 分散処理システム 324
 分析手法 342

へ

平均故障間隔	327
平均復旧時間	327
米国規格協会	208
米国立標準技術研究所	50
並列システム	328
ベースラインアプローチ	100
ベストエフォート型	292
ペネトレーションテスト	116
ヘルプデスク	241
変更管理	239
変更諮問委員会	239
変更要求	239
ベンチマーキング	231
ベンチマーク	231, 267, 326
変動費	343

ほ

ポートスキャン	38
ポート番号	284
保守性	157
保全性	157
保証型監査	216
ホスト	283
ホストアドレス	283
ホスト型IDS	136
ポット	27
ホットスタンバイ	318
ポットネット	27
ポットハーダー	27
ホワイトハッカー	112
本調査	217
本人拒否率	65
本人認証	56

ま

マークアップ言語	291
マイナンバー	184
マイナンバー制度	184
マイナンバー法	184
マイルストーン	258
マクシマックス原理	339
マクシミン原理	339
マズローの欲求段階説	335

マトリックス図法	341
マトリックス組織	336
マトリックスデータ解析法	341
マネジメントレビュー	85
マルウェア	32
マルウェア・不正プログラム対策	138
マルチキャストアドレス	288

み

ミッションクリティカルシステム	241
見積依頼書	368
ミラーリング	158, 320

む

無形資産	81
無線LAN	143
無線LANアクセスポイント	143
無線LANセキュリティ	143
無停電電源装置	243
無方式主義	200

め

迷惑メール	190
メールクライアント	290
メールサーバ	290
メールボックス	290
メタデータ	299
メッセージ認証	56, 63
メッセージ認証コード	63

も

目的外利用	182, 184
目標復旧時間	240
モニタリング	327
モバイル端末管理	147
モバイル通信	293
モラルハザード	97
問題	96, 237
問題管理	238
モンテカルロ法	342

ゆ

有用性	201
愉快犯	27
ユニキャストアドレス	288

よ

要員教育計画	364
要員認証機関	86
要求分析	365
要件定義	365
予備調査	217

ら

ライセンス契約	204
ランサムウェア	33
ランニングコスト	328

り

リアルタイム処理	319
リーダシップ	84
投資利税率	346
利害関係者	102
リカバリポイント目標	240
リクエスト	277
離散対数問題	53
リスク	25, 96, 264
リスクアセスメント	99, 232
リスク移転	102
リスクオーナー	102
リスク回避	99
リスク基準	98
リスク忌避	99
リスク源	96
リスクコミュニケーション	102
リスクコントロール	101
リスク集約	101
リスク受容	102
リスク受容基準	98
リスク所有者	102
リスク選好	99
リスクソース	96
リスク対応	101, 264
リスク対応計画	102
リスクテイク	101

リスク定量化……………97
 リスク登録簿……………102
 リスク特定……………99, 264
 リスクの回避……………101
 リスクの共有……………102
 リスクの保有……………102
 リスク評価……………99
 リスクファイナンス……………101
 リスクファイナンス……………101
 リスク分解……………101
 リスク分散……………102
 リスク分析……………99, 236, 264
 リスクベース認証……………61
 リスクヘッジ……………101
 リスクマトリックス……………100
 リスクマネジメント……………95
 リスクレベル……………100
 リバースプロキシ……………167
 リバースプロキシ型……………62
 リバースプロキシサーバ…62, 287
 リピータ……………280

リブレイ攻撃……………31
 リモートワイプ機能……………147
 流動比率……………347
 リリース及び展開管理……………239
 リレーショナルデータベース…298
 リレーションシップ……………300

る

ルータ……………281
 ルーティング……………281
 ループバックアドレス……………286

れ

レイヤ2スイッチ……………280
 レイヤ3スイッチ……………281
 レインボー攻撃……………32, 55
 レインボーテーブル……………32
 レスポンス……………58, 277
 レスポンスタイム……………326
 連関図法……………341

ろ

労働安全衛生法……………203
 労働基準法……………202
 労働者派遣法……………202
 労働生産性……………348
 ローカルサービスデスク……………242
 ロードバランス……………323
 ロールバック……………307
 ロールフォワード……………307
 ログ……………127
 ログ監視……………127
 ログ管理……………127
 ログファイル……………307
 ロック……………305

わ

ワークアラウンド……………238
 ワークパッケージ……………255
 ワークライフバランス……………336
 ワンタイムパスワード……………59

STAFF

編集

水橋明美（株式会社ソキウス・ジャパン）

片元諭

制作

波多江宏之

イラスト

ケイコモス

本文デザイン

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

■著者

株式会社わくわくスタディワールド

IT分野を中心に、楽しく効果的に学んで合格する方法を提案し、そのための教材やセミナーを提供する会社。わくわくする学びをテーマに、企業研修やオープンセミナーなどで、単なる試験対策にとどまらない学びを提供中。また、IT系を中心としたブログ「わく☆すたブログ」や、動画を中心にIT全般の知識を学ぶサイト「わくわくアカデミー」など、様々なサイトを展開。

ホームページ: <http://www.wakuwakustudyworld.co.jp>

わく☆すたブログ: <http://www.wakuwakustudyworld.co.jp/blog>

わくわくアカデミー: <http://www.wakuwakuacademy.net>

瀬戸 美月（せと みづき）

株式会社わくわくスタディワールド代表取締役。

独立系ソフトウェア開発会社、IT系ベンチャー企業でシステム開発、Webサービス立ち上げなどに従事した後独立。企業研修やセミナー、勉強会などで、数多くの受験生を15年以上指導。

保有資格は、情報処理技術者試験全区分制覇（旧15区分+α）、高等学校教諭一種免許状（情報）他多数。著書は、『徹底攻略 応用情報技術者教科書』『徹底攻略 ネットワークスペシャリスト教科書』『徹底攻略 データベーススペシャリスト教科書』（以上、インプレス）、『新 読む講義シリーズ 8 システムの構成と方式』（以上、アイテック）他多数。

齋藤 健一（さいとう けんいち）

株式会社わくわくスタディワールド取締役。

食品会社の経営情報企画部で、情報システム導入やセキュリティ管理を10数年にわたり主導。独立後はセキュリティを中心とした指導にあたる傍ら、IT関連や情報処理技術者試験などの動画を中心とした教材作成に携わる。

保有資格は、情報セキュリティスペシャリスト、情報セキュリティアドミニストレータ、ネットワークスペシャリスト他多数。著書は、『インターネット・ネットワーク入門』『徹底解説データベーススペシャリスト過去問題』（以上、アイテック）『基本情報技術者過去問題集』（以上、エクスメディア）他。

わく☆すたAI

わくわくスタディワールド社内で開発されたAI（人工知能）。情報処理技術者試験の問題を中心に、現在いろいろなことを学習中。今回は、機械学習（クラスタリング）で、出題傾向の分析を中心に活躍。近い将来、参考書を自分で全部書けるようになることが目標。

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「zuknow」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「zuknow」のインストールと、「zuknow」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）

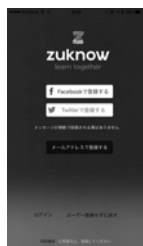
「でる語句 200」とは

「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「zuknow」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「zuknow」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「zuknow」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「zuknow」を検索し、インストールしてください。
- 2 インストールしたアプリを起動して、画面の指示に従い、初回のユーザー登録手続きを進めてください。



※ 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、「zuknow 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(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もので必ず 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 「zuknow」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

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

「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biz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biz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。

徹底攻略 情報セキュリティマネジメント教科書

平成 29 年度 【購入者限定特典】

2016 年 12 月 21 日 初版発行

著 者 株式会社わくわくスタディワールド 瀬戸美月／齋藤健一

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（ソフトウェア及びプログラムを含む）、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 Mizuki Seto/Kenichi Saito. All rights reserved.