第3章 本書の構成と使い方

(1) 本書の構成

本書は，学習者の皆様が，各分野の重要ポイントを確実に押さえ，試験合格に必要な知識を身に付けられるよう，次のような構成になっています。

●第２部　午前試験の対策　（第１章の例）

第1章 情報セキュリティ全般 ［重点分野］

- ◎ 学習のポイント …学習する上で重要なポイントの概要
- 1.1 情報セキュリティ
- 1.2 セキュリティ実装技術

1.1 / 1.2 の内容：

- ポイントの解説 …重要な知識事項を中心に解説
- 理解度チェック …「ポイントの学習」で学習した内容の復習
- 問題にチャレンジ …演習問題

※第１章～第４章まで，同じ構成になっています。

※第５章は関連分野のため，「学習のポイント」を省略しています。

分からない知識事項が出てきたら，午前のポイントへ ⇕ ポイントで学んだ知識を応用して，午後の演習問題へ

●第３部　午後試験の対策　（第２章の例）

第2章 情報セキュリティマネジメントの計画，情報セキュリティ要求事項に関すること

- ◎ 学習のポイント …学習する上で重要なポイントの概要
- 演習問題 …実力アップのための演習問題

※第３章も，同じ構成になっています。

※演習問題の解説は，第４部に掲載されています。

第1章 情報セキュリティ全般

［重点分野］

◎ 学習のポイント

午前問題で正解するためには，情報セキュリティに関する基本的な用語について，自分なりの言葉で説明できるように理解することを目標としましょう。

用語には「PKI（公開鍵基盤）」のような英字の略号が多く出てきます。略号のまま丸暗記するよりも，「Public Key Infrastructure（パブリックキーは公開鍵，インフラストラクチャは基盤）」と意味を含めてフルネームで覚えると理解しやすいでしょう。そのために，略号には原則としてフルスペルを付記しています。ただし，英単語のスペルを完全に覚える必要はありません。

ポイントの解説で取り上げる用語は，重要なものをピックアップしたものです。その他の用語については，「問題にチャレンジ」の午前問題を演習しながら整理しましょう。用語の理解は，午後対策としても役に立ちます。

(1) 情報セキュリティ　(→1.1)

情報セキュリティとは何か，情報資産・脅威・脆弱性といった基本的な概念と情報セキュリティの特性の意味を理解しましょう。情報資産のセキュリティを損なう様々な脅威に関する用語を整理しましょう。また，昨今，大きな問題となっている標的型攻撃の特徴や不正のメカニズムを理解しましょう。

情報セキュリティ技術については，IT を利活用する立場として，その目的を優先的に理解しましょう。暗号技術や認証技術では，共通鍵，秘密鍵，パスワードなどが秘密にすべき情報で，第三者に知られることのないように安全に管理することがポイントです。公開鍵やディジタル証明書は秘密の情報ではありません。

(2) セキュリティ実装技術　(→1.2)

コンピュータ間の通信の規約をプロトコルといいます。セキュアプロトコルは，セキュリティの機能をもつプロトコルです。

セキュアプロトコルでは，Web システムで日常的に使われている SSL/TLS が重要です。

1.2 セキュリティ実装技術

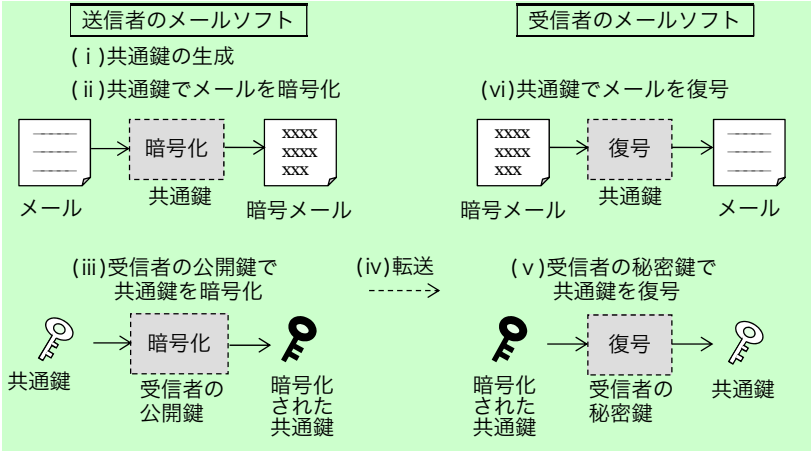
ポイントの解説

(1) セキュアプロトコル

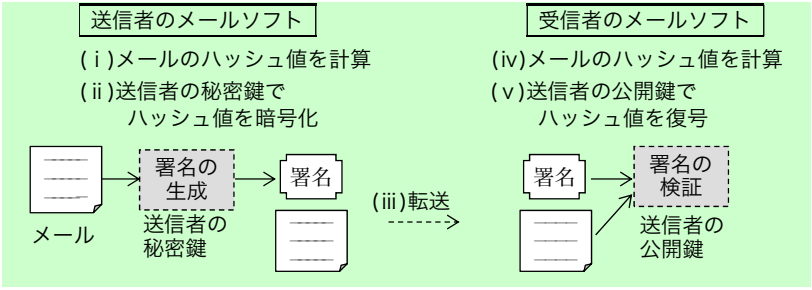
① S/MIME（Secure Multipurpose Internet Mail Extensions）

電子メールの暗号化と，ディジタル署名による送信者の認証と改ざんの検出を行う仕組みです。

・暗号メールの送信（共通鍵と受信者の公開鍵ペアを使用します）



・署名メールの送信（送信者の公開鍵ペアとハッシュ関数を使用します）



注記 署名の生成と検証の手順の詳細は，図表 1-9 を参照してください。

図表 1-12 S/MIME の仕組み

問題にチャレンジ

問１　サイバーセキュリティ基本法に関する記述として，**適切でないもの**はどれか。

(950051)

ア　国として，中小企業者が自発的に行うサイバーセキュリティに対する取組が促進されるための必要施策を講じる。

イ　この法律における“サイバーセキュリティ”は，音声や紙の書類など人が直接認識できる情報も対象にしている。

ウ　サイバーセキュリティ戦略の策定，その他サイバーセキュリティに関する施策の基本となる事項を定めている。

エ　サイバーセキュリティに関する施策の基本理念を定め，国及び地方公共団体の責務などを明らかにする。

【解き方のコツ】

サイバーセキュリティ基本法は平成 26 年 11 月に成立し，この法律における“サイバーセキュリティ”は，電子的方式や磁気的方式の他，人の知覚で認識することができない方式で記録された情報を対象として，必要な措置が講じられ，その状態が適切に維持管理されていることをいいます。したがって，(イ)の記述が適切ではありません。

（ア）は民間事業者及び教育研究機関等の自発的な取組の促進に関する記述（第 15 条），（ウ）と（エ）はサイバーセキュリティ基本法の目的に関する記述（第１条）です。

解答　イ

第1章 午後試験の概要と解法テクニック

1.1　午後試験の概要

(1)　午後の出題範囲と出題

午後の試験の具体的な出題範囲は図表 1-1 のとおりで，午前の出題範囲とは違う分類になっています。問題は出題範囲から 3 問出題されて，3 問全問に解答します。解答時間は 90 分ですので，1 問当たり平均して 30 分で解答することになります。

3 問出題されるそれぞれの問題は，出題範囲の中の一つのテーマに絞ったパターンと，一つの問題に複数のテーマが混在しているパターンが想定されます。1 回の試験で出題範囲の全ての内容が実際に出題されるとは限りませんが，3 問の出題によって出題範囲がおおよそカバーされると考えてください。そのため，特定のテーマに絞らずに，まんべんなく演習を行って準備をしましょう。

この試験対策書では，「1.情報セキュリティマネジメントの計画，情報セキュリティ要求事項に関すること」を第 2 章，「2.情報セキュリティマネジメントの運用・継続的改善に関すること」を第 3 章で取り上げています。

(2)　午後試験の特徴と学習法

午前の試験と午後の試験の問題の違いは，出題目的（試験の目的）の違いにあります。試験センターの発表では，午前の試験は「知識を問うことによる評価」，午後の試験は「課題発見能力，抽象化能力，課題解決能力などの技能を問うことによる評価」としています。午後の試験は，午前の試験で学習した知識の応用を見るために，知識を適用する事例が午前の試験に比べて，具体的で現実に近いものになるという違いになります。

午後の試験で評価される応用能力の前提として基礎知識が必要であり，この基礎知識をまず理解するために，午前問題の重点分野（情報セキュリティと法務）の学習を行うことをお勧めします。

限られた時間の中で試験対策を行う場合，問題演習を中心にした学習が効率的です。しかし，午前問題の解説を読んで理解が不十分と感じたら，テキスト

第2章 情報セキュリティマネジメントの計画，情報セキュリティ要求事項に関すること

◎ 学習のポイント

この出題範囲の学習のポイントは，“情報セキュリティの基本をしっかりと理解する”ことです。基本とは，情報資産管理の考え方，リスクアセスメントの考え方，リスク対応策の考え方などです。具体的には，以下で出題範囲に沿って説明します。情報セキュリティマネジメントは，皆さんが所属する組織でも計画・構築されているはずです。午後問題の演習を通じて，そして，自分の組織の情報セキュリティマネジメントではどうなっているかを考えながら，情報セキュリティの基本を理解していきましょう。

【出題範囲に沿ったポイント解説】

(1)　情報資産管理の計画

情報セキュリティマネジメントの計画は，部門が所有する情報資産を特定する作業から始まります。情報資産の重要度の評価は，一般に，機密性，完全性，可用性の観点から行います。情報セキュリティ対策は，情報漏えい対策だけではありません。情報セキュリティの３要素（機密性，完全性，可用性）を理解して，重要度を評価する考え方を理解しましょう。

特定された情報資産は，情報資産台帳に登録し，管理責任者の任命や管理規程の作成を行って，受入れから利用を経て廃棄するまでのライフサイクルを通して適切に管理します。適切に管理するためには，重要度に基づいて情報資産を格付けし，格付けが分かるように適切にラベルを付けることがポイントです。格付けの呼び方は様々ですが，“極秘”“秘密”“社外秘”“公開”のようなレベルに分類します。

(2)　情報セキュリティリスクアセスメント及びリスク対応

リスクアセスメントでは，はじめにリスクを特定します。そのためには，情報資産を取り巻く脅威や脆弱性に，どのようなものがあるのかについての知識が必要です。典型的な脅威として，ウイルス攻撃を含む標的型サイバー攻撃と

演習問題 2-1

解答▸p.300

リスクマネジメントに関する次の記述を読んで，設問 1～4 に答えよ。

(950179)

A 社は，家具を製造・販売している企業で，創業 30 年目，資本金 1 億円，従業員約 400 人の企業である。ここ数年順調に売上を伸ばしてきている。このままいけば経営戦略にある将来の上場も問題ないと思えるほど順調である。そこで A 社は，今年から上場に向けた準備を始めるとともに，より安定した売上と利益を確保するために，インターネットを利用した新事業を開始する方針を打ち出した。

A 社には，自社で定期的に行っている消費者アンケートに答えてくれた人の個人情報がある。アンケートを開始して今年で 10 年目になることもあり，その数は数万件にも及ぶ。ただし，このアンケートは雑誌等に添付したはがきで収集しているので，全て“はがき”のまま金庫に保管されている。社長は，これだけの消費者の個人情報があれば，電子メールで新製品を案内したり，インターネットで通信販売をしたりできるのではないかと考えた。

〔新事業の概要〕

現在，A 社では，インターネット上にホームページを公開している。Web サーバは自社に設置し，専用線でプロバイダ（以下，ISP という）に接続している。全体のシステム構成は次図のようになる。この環境を使って，消費者に対して自社製品を直接販売するサイトを構築することにした。

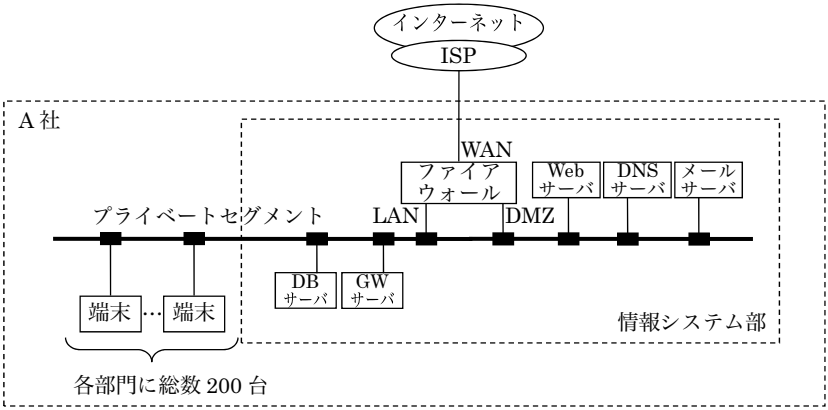


図　A 社のシステム構成

演習問題 3-4

業務委託におけるアクセス制御
（H28 春-SG 午後問 2）

【解答】

［設問１］　(1)　オ　　(2)　エ　　(3)　a－オ，b－イ
　　(4)　ウ　　(5)　エ　　(6)　イ

［設問２］　(1)　c－エ　　(2)　d－ア，e－ウ，f－ア　　(3)　ウ　　(4)　ア

【解説】

業務委託先の社員を含む利用者に対する情報システムのアクセス制御を題材として，情報セキュリティマネジメントの運用における，利用者のアクセス権管理と業務の外部委託における情報セキュリティの確保をテーマとした問題です。利用方針や業務部門の要求を満たすための操作権限の付与に関する考察問題が多く出題され，後半の設問２では，アクセスの管理に関わる申請手続の考察が出題されました。考察問題の数が多いため，30 分では解答時間が不足する可能性があり，問１で時間を貯金して，問２に割り当てるという時間管理になった受験者もいたと思われます。解答を特定する作業を根気よく繰り返すことが求められています。

また，この問題では，ロール（役割）に基づくアクセス制御が取り上げられています。このようなアクセス制御は，ロールベースアクセス制御（RBAC；Role Based Access Control）と呼ばれます。この方法では，利用者ごとに個人を識別するための利用者 ID が登録され，利用者 ID に対してロールが設定されます。そして，そのロールに対してアクセス権限（操作権限）が付与されます。同じアクセス権限をもつ利用者を同じロールに設定することによって，利用者の個人単位にアクセス権限を付与する作業を簡略化できる利点があります。しかし，ロールやロールに付与する権限，さらに利用者に設定するロールを適切に運用しないと，ある利用者に必要な権限が付与されなかったり，逆に必要以上の権限を付与してしまったりする不都合が発生します。そのため，この問題で出題されているように，適切な設定や運用が重要になります。

［設問１］

(1)　下線①の「J システムで利用方針に違反してしまいます」について，違反が考えられる利用方針だけを全て挙げた組合せを選ぶ問題です。まず，下線①を含む M 主任の発言に至る話の流れを整理すると次のようになります。

うか」と発言しています。このＮ課長の案を反映した操作権限は，次の表Ｃのようになります。

表Ｃ　Ｎ課長の案を反映した操作権限

ロールに付与される操作権限 / ロール	Ｊシステム		
	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	◎	◎	

権限追加

そして，この案に対してＭ主任が，下線①のように「Ｊシステムの利用方針に違反してしまいます」と返答しています。話の流れを整理できたところで，利用方針への違反の有無について順に検討すると，次のようになります。

［方針１］表Ｃの操作権限によるＪシステムの利用においても，「１人の利用者に，一つの利用者ＩＤを登録する」ことは実現できるので，利用方針に違反しません。

［方針２］方針１と同様に，「一つの利用者ＩＤは，１人の利用者だけが利用する」ことを実現できるので，利用方針に違反しません。

［方針３］表Ｃの操作権限では，“Ａ社販売担当者”ロールには，“入力”と“承認”の権限が付与されるため，自分で入力した情報を自分で承認することができてしまいます。そのため，「ある利用者が入力した情報は，別の利用者が承認する」という利用方針に違反します。

［方針４］“Ａ社販売責任者”ロールには，表Ｃにおいても閲覧権限が付与されているので，「販売責任者は，Ｚ販売課の全業務の情報を閲覧できる」という利用方針には違反していません。

以上の検討から，Ｎ課長の案が違反している利用方針は，［方針３］だけなので，（オ）が正解です。

(2)　下線①の「Ｊシステムで利用方針に違反してしまいます」について，この利用方針違反が高めると考えられるリスクを選ぶ問題です。利用方針違反は，(1)の解説のとおり，［方針３］の「ある利用者が入力した情報は，別の利用者が承認する」という方針に対するもので，このことによるリスクは，“Ａ

付録3 学習記録用問題リスト

●第 2 部　午前試験の対策　問題にチャレンジ

問番号	内容	1 回目		2 回目	
		正解・不正解	やり直し	正解・不正解	やり直し
1.1 情報セキュリティ					
問 1	BYOD の説明	○・×	必要・不要	○・×	必要・不要
問 2	脅威によって直接的に引き起こされた事象	○・×	必要・不要	○・×	必要・不要
問 3	不正のトライアングルの構成要素	○・×	必要・不要	○・×	必要・不要
問 4	APT の説明	○・×	必要・不要	○・×	必要・不要
問 5	スパイウェアに該当するもの	○・×	必要・不要	○・×	必要・不要
問 6	セキュリティ攻撃	○・×	必要・不要	○・×	必要・不要
問 7	水飲み場型攻撃の手口	○・×	必要・不要	○・×	必要・不要
問 8	パスワードリスト攻撃の手口	○・×	必要・不要	○・×	必要・不要
問 9	ディレクトリトラバーサル攻撃	○・×	必要・不要	○・×	必要・不要
問 10	SQL インジェクション攻撃の説明	○・×	必要・不要	○・×	必要・不要
問 11	クリックジャッキング攻撃	○・×	必要・不要	○・×	必要・不要
問 12	標的型攻撃メールの特徴	○・×	必要・不要	○・×	必要・不要
問 13	公開鍵暗号方式の暗号アルゴリズム	○・×	必要・不要	○・×	必要・不要
問 14	ディジタル署名でできること	○・×	必要・不要	○・×	必要・不要
問 15	ハッシュ関数の特徴	○・×	必要・不要	○・×	必要・不要
問 16	2 要素認証	○・×	必要・不要	○・×	必要・不要
問 17	PKI（公開鍵基盤）の認証局が果たす役割	○・×	必要・不要	○・×	必要・不要
問 18	生体の行動的特徴による認証	○・×	必要・不要	○・×	必要・不要
1.2 セキュリティ実装技術					
問 1	電子メールを暗号化するための方式	○・×	必要・不要	○・×	必要・不要
問 2	SSL で使用する鍵の種類	○・×	必要・不要	○・×	必要・不要
問 3	パケットフィルタリング型ファイアウォール	○・×	必要・不要	○・×	必要・不要
問 4	無線 LAN における接続制限	○・×	必要・不要	○・×	必要・不要
問 5	暗号化や認証機能をもつ遠隔操作プロトコル	○・×	必要・不要	○・×	必要・不要

索　引