応用情報技術者

試験対策テキストⅡ【システムの利用と開発編】

無料体験入学者用

TAC

はじめに

応用情報技術者試験(AP)は2009年春期より実施された試験区分です。対象者像は,

「高度IT人材となるために必要な応用的知識・技能をもち,
高度IT人材としての方向性を確立した者」

とされています。基本情報技術者試験(FE)で求められる基本的な知識に加え,さらに専門的・詳細な内容を含めた応用的知識が問われることになります。

本書は応用情報技術者試験の出題範囲であるテクノロジ系,ストラテジ系,マネジメント系のうち,テクノロジ系の周辺技術要素であるヒューマンインタフェース,マルチメディア,データベース,ネットワーク,情報セキュリティ,そしてシステム開発に関する分野の知識を網羅しています。その上で,読者の皆さんが効率よく学習が行えるよう,基礎的な用語や考え方を分かりやすく解説するように心がけました。

本書により,読者のみなさんが応用情報技術者試験に合格されることを願ってやみません。

TAC情報処理講座

目　次

第４章

情報セキュリティ

学習テーマ　4－1

情報セキュリティマネジメント

(1)　情報セキュリティマネジメント

●情報セキュリティの定義

情報セキュリティマネジメントシステムの用語を定めた規格であるJIS Q 27000では，情報セキュリティを「情報の機密性，完全性及び可用性を維持すること」と定義している。これらの特性は，頭文字をとって情報のC.I.Aともいう。

表4.1　情報セキュリティのC.I.A

特性	意味
機密性（confidentiality）	認可されていない個人，エンティティ又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。
完全性（integrity）	正確さ及び完全さの特性。
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。

JIS Q 27000では情報セキュリティについて，「さらに，真正性，責任追跡性，否認防止，信頼性などの特性を維持することを含めることもある」と規定されている。これらの用語は，次のような意味をもつ。なお，ここでのエンティティ(実体)とは，情報を扱う組織，人，設備，ソフトウェアなどが該当する。

表4.2　各用語の意味

特性	意味
真正性	エンティティは，それが主張するとおりのものであるという特性
責任追跡性	あるエンティティの動作が，その動作から動作主のエンティティまで一意に追跡できることを確実にする特性
否認防止	主張された事象又は処置の発生，及びそれを引き起こしたエンティティ（利用者など）を証明する能力
信頼性	意図する行動と結果とが一貫しているという特性。

●JIS Q 27000シリーズ

情報セキュリティの，C.I.Aを維持するとともに継続的に改善する仕組みを，情報セキュリティマネジメントシステム(ISMS：Information Security Management System)という。JIS Q 27000シリーズはISO/IEC27000シリーズを基に策定された情報セキュリティマネジメントに関する規格群であり，次のような規格が制定されている。

JIS Q 27000：情報セキュリティマネジメントシステム－用語
JIS Q 27001：情報セキュリティマネジメントシステム－要求事項
JIS Q 27002：情報セキュリティ管理策の実践のための規範

JIS Q 27001に基づき，組織が構築した情報セキュリティマネジメントシステムの適合性を評価する制度を，ISMS適合評価制度という。

●情報セキュリティポリシ

情報セキュリティマネジメントシステムの構築においては，組織が情報セキュリティに取り組む際の方針を定める必要がある。これを情報セキュリティポリシまたは情報セキュリティ方針という。情報セキュリティポリシには多様な解釈があり，複数の文書で構成されることも多いが，情報セキュリティに関する企業の考え方や取組みを明文化したものを，情報セキュリティ基本方針という。情報セキュリティ基本方針は，企業の経営層が承認・宣言したものであり，社内外に広く公開すべきである。また，時勢や環境の変化に伴い，柔軟に変更していくことが望ましい。

●情報セキュリティインシデント

JIS Q 27000では，「情報セキュリティ方針への違反若しくは管理策の不具合の可能性，又はセキュリティに関係し得る未知の状況を示す，システム，サービス若しくはネットワークの状態に関連する事象」を情報セキュリティ事象と定義しており，「望まない単独若しくは一連の情報セキュリティ事象，又は予期しない単独若しくは一連の情報セキュリティ事象であって，事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの」を情報セキュリティインシデントと定義している。すなわち，情報セキュリティインシデントとは，サービスの停止や情報の漏えいなど，情報セキュリティを脅かす可能性が高い（または実際に脅かされた）出来事であり，単にインシデントともいう。

このインシデントの潜在的な原因を脅威といい，一つ以上の脅威によって付け込まれる可能性のある，資産又は管理策の弱点を脆弱性という。脅威には盗聴やシステムのクラッキング，誤り，地震などが該当する。脆弱性には，プログラムのセキュリティ上のバグ(セキュリティホール)，暗号化されていないデータ，施錠されていない入口などが該当する。

情報資産の脆弱性に対して脅威がつけ込むと，損害が発生する可能性が生じる。これをリスク又は情報セキュリティリスクという。情報セキュリティにおいてはリスクを適切に評価し，管理策を講じるリスクマネジメントが重要となる。

(2)　その他のセキュリティ規格・ガイドライン・関連組織

●ISO/IEC 15408

ISO/IEC 15408は，システム及び製品に関する情報技術セキュリティ評価基準を定めた国際標準であり，情報技術を利用した製品やシステムのセキュリティ機能が，評価基準に適合するかを評価するための規格である。日本ではJIS X 5070として標準化されており，コモンクライテリア(CC：Common Criteria)ともいう。この規格を評価基準とした制度にITセキュリティ評価及び認証制度がある。これは，情報技術に関連した製品のセキュリティ機能の適切性，確実性を第三者機関が評価し，その結果を公的に認証する。

●クラウドサービス利用のための情報セキュリティマネジメントガイドライン

JIS Q 27002では，第三者が提供するサービスの利用に関する管理策も定められているが，ITを所有せずにクラウドコンピューティングを全面的に利用するような組織に対しては十分といえない。そこで，クラウドサービスの利用者が情報セキュリティ対策を円滑に行えるように，JIS Q 27002の管理策を補完するために経済産業省によって作成された指針がクラウドサービス利用のための情報セキュリティマネジメントガイドラインである。

●JIS Q 27014

JIS Q 27014は，情報セキュリティガバナンスに関する規格である。情報セキュリティガバナンスを“組織の情報セキュリティ活動を指導し，管理するシステム”と定義し，その実現のための指針を記述している。組織が実施すべきプロセスとしては，以下のようなものがある。

・経営陣は統治のために“評価”，“指示”，“モニタ”及び“コミュニケーション”の各プロセスを実行する。
・さらに“保証”プロセスによって，ガバナンス及び達成レベルについての独立した客観的な意見が得られる

●リスクマネジメントに関する規格

リスクマネジメントに関する規格には，JIS Q 31000やJIS Q 0073がある。JIS Q 31000では，リスクマネジメントの原則及び指針を，JIS Q 0073ではリスクマネジメントの用語を定めており，JIS Q 27000シリーズはこれらの規格と整合するようになっている。

●サイバーセキュリティ経営ガイドライン

経済産業省とIPAが策定したサイバーセキュリティ経営ガイドラインは，企業の経営者を対象とした，サイバー攻撃から身を守る観点で認識すべき3つの原則や，情報セキュリティ対策を実施する上で責任者に指示すべき重要項目などを取りまとめたものである。

3つの原則には，サイバーセキュリティリスクを認識してリーダーシップによって対策を進めること，ビジネスパートナー及び委託先を含めたセキュリティ対策が必要なこと，関係者との適切なコミュニケーションが必要なことがある。

●中小企業の情報セキュリティ対策ガイドライン

中小企業では，情報セキュリティの重要性を理解していないことや，取り組む経済的余裕がないことも珍しくない。IPAが公表した中小企業の情報セキュリティ対策ガイドラインは，中小企業や小規模事業者を対象として，経営者が認識し実施すべき指針や，社内において対策を実践する際の手順や手法をまとめた文書である。当ガイドラインは，できるところから始め，ステップアップしていくことを目的としており，当ガイドラインに沿って中小企業などが情報セキュリティに取り組むことを自己宣言する制度を，SECURITY ACTIONという。

●CSIRT

CSIRT(Computer Security Incident Response Team)は，コンピュータセキュリティインシデントに対応するための組織である。企業などの組織内に設置される組織内CSIRTや，CSIRTをサービスとして提供する企業などがある。

●JPCERT/CC

JPCERT/CC(JPCERTコーディネーションセンター)は，日本国内のサイ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，再発防止のための対策の検討や助言などを，技術的な立場から行う特定の政府機関や企業から独立した組織であり，CSIRT間の調整なども行う。JPCERT/CCが公表する文書には，組織的なインシデント対応体制であるCSIRTの構築や運用を支援するためのCSIRTマテリアルや，インシデント発生時にCSIRTが行うべき解決までの一連の処理手順を表したインシデントハンドリングマニュアルなどがある。インシデントハンドリングマニュアルでは，次のような基本的な流れを提示している。

・検知／連絡受付　…　自組織での検知や外部からの連絡によるインシデント発生の認識
・トリアージ　…　インシデントの事実確認と対応の優先順位付け
・インシデントレスポンス　…　インシデントの分析や実際の対処
・報告／情報公開　…　プレスリリースや官公庁への報告など

また，IPAとJPCERT/CCは共同で，JVN(Japan Vulnerability Notes)を運営している。JVNは，日本で使用されているソフトウェアなどの脆弱性に関連する情報や，それに対する対策方法を提供することにより，情報セキュリティ対策に資することを目的としたポータルサイトである。

●J-CRATとJ-CSIP

サイバーレスキュー隊(J-CRAT：Cyber Rescue and Advice Team against targeted attack of Japan)は，IPAが発足させた，標的型サイバー攻撃の被害拡大防止のための支援体制である。標的型サイバー攻撃を受けた組織や個人から提供された情報を分析し，社会や産業に重大な被害を及ぼしかねない標的型サイバー攻撃の把握，被害の分析，対策の早期着手の支援を行う。

サイバー情報共有イニシアティブ(J-CSIP：initiative for Cyber Security Information sharing Partnership of Japan)は，IPAにサイバー攻撃などの情報を集約し，参加組織間で情報共有を行って高度なサイバー攻撃への対策につなげていく取組みである。

●CRYPTREC

CRYPTREC(CRYPTography Research and Evaluation Committees)とは，電子政府推奨暗号の安全性を評価・監視し，暗号技術の適切な実装法・運用法を調査・検討する組織である。電子政府における調達のために推奨すべき暗号リスト(CRYPTREC暗号リスト)を策定し，電子政府推奨暗号リスト，推奨候補暗号リスト，運用監視暗号リストを公開している。

●サイバーセキュリティ戦略本部とNISC

サイバーセキュリティ基本法は，サイバーセキュリティに関する基本理念や国及び地方公共団体の責務などを定めた法律である。電磁的方式によって記録・発信・伝送・受信される情報を対象としており，サイバーセキュリティに関する施策を総合的かつ効果的に推進するために，内閣にサイバーセキュリティ戦略本部を置くことを定めている。サイバーセキュリティ戦略本部は内閣官房長官を本部長とし，サイバーセキュリティ戦略の案の作成や，サイバーセキュリティ対策の基準の作成などを行う。また，内閣官房には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）が設置されている。NISCはサイバーセキュリティ政策に関する総合調整を行いつつ，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。

学習テーマ　4－2
リスク管理

●リスクマネジメント

組織におけるリスクを特定し，リスクの除去や最小化といった管理を行う一連の活動をリスクマネジメントという。リスクマネジメントは，次のようなプロセスで構成される。

表4.3　リスクマネジメント

リスクマネジメント			リスクを管理する一連の活動
	リスクアセスメント		リスク分析からリスク評価にいたるプロセス
		リスク特定	リスク因子(脅威と脆弱性の組合せ)を特定
		リスク分析	リスク発生する可能性と影響度を分析
		リスク評価	リスクの重大さをリスク評価基準と比較する
	リスク対応		リスクに対する対策を選択･実施する
	リスク受容		リスク対応後の残留リスクを受容
	リスクコミュニケーション		リスクに関する情報の共有

●リスクアセスメント

JIS Q 27001では，ISMSの適用範囲内における情報の機密性，完全性及び可用性の喪失に伴うリスクを特定するために，情報セキュリティリスクアセスメントのプロセスを適用することが求められている。リスクアセスメントとは，リスク特定，リスク分析，リスク評価から構成されるプロセス全体のことである。

リスクアセスメントを実施するにあたり，リスク基準などを設定する必要がある。リスク基準とは，リスクの重大性を評価するための目安とする条件であり，組織の目的，外部状況及び内部状況に基づいて決定する。リスクアセスメントの分析手法には，次のようなものがある。

表4.4　リスクアセスメントの分析手法

ベースラインアプローチ	確保すべき一定のセキュリティ水準(ベースライン)をあらかじめ決めておき，対象となるシステムに一律に適用する手法。省力化が期待できるが，セキュリティ対応策が不十分または過剰になるおそれがある。
詳細リスク分析	資産ごとにリスク識別を実施する手法。脅威や脆弱性からリスクを評価し，対応策を選択する。適切な対応策が期待できるが，労力は大きくなる。
組合せアプローチ	ベースラインアプローチと詳細リスク分析を組み合わせ，双方の弱点を相互に補完する手法。
非形式的アプローチ	現場担当者がもつ知識や経験，判断に基づく手法。省力化が期待でき，適切な対応策が期待できるが，客観性に欠ける場合がある。

・リスク特定

リスク特定は，リスクを発見・認識及び記述するプロセスであり，リスクの原因となる脅威や脆弱性，起こり得る結果等を特定する。このために，過去のデータや専門家の意見，ステークホルダ(利害関係者)のニーズなどを含むことがある。

・リスク分析

リスク分析は，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である。リスクレベルは，JIS Q 27000において「結果とその起こりやすさの組合せとして表現される，リスクの大きさ」と定義されており，次のように考えることもできる。

リスクレベル ＝ 資産価値 × 脅威 × 脆弱性

・リスク評価

リスク評価は，リスクレベルが受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であり，この結果を受けてリスクの優先順位付けを行う。

●リスク対応

リスク対応はリスクを修正するプロセスである。このための手法には，次のようなものがある。

表4.5　リスクを変更するための方策

方策	内容	例
リスク低減	適切な管理策(コントロール)を採用することにより，リスクが発生する可能性やリスクが発生した場合の影響度を低減する。	セキュリティ技術の導入， 入口の施錠， スプリンクラの設置　など
リスク回避	リスクと資産価値を比較した結果，コストに見合う利益が得られない場合など，資産ごと回避する。	業務の廃止， 資産の廃棄　など
リスク移転	資産の運用やセキュリティ対策の委託，情報化保険など，リスクを他者に移転する。	ハウジングサービスの利用， 情報化保険の加入　など
リスク受容	識別されており，受容可能なリスクを意識的，客観的に受容する。リスクが顕在化したときは，その損害を受け入れる。	会社が損失額を負担する など

このうち，リスク低減では，適切な管理策を適用することによって，リスクが発生する可能性やリスクが発生した場合の影響度を低減させる。したがって，管理策適用後のリスクレベルは，管理策の適用前よりも小さくなる。これが受容できるリスク基準の範囲内であれば，残留リスクとして受容することになる。残留リスクとは，リスク対応後に残ったリスクのことであり，特定されていないリスクが含まれている場合もある。リスクの対応計画や残留しているリスクの受容については，リスク所有者(リスクの運用管理についてアカウンタビリティ及び権限をもつ者)の承認を得る。