目　　次

第３部　午後問題のテーマ別対策と必要知識

Part 1　第1章　Chapter 1

情報処理安全確保支援士制度と試験

1. 情報処理安全確保支援士制度の創設と試験

経済産業省は，2016 年 10 月 21 日から，サイバーセキュリティ分野において初の国家資格となる情報処理安全確保支援士制度を開始しました。

それに伴い，独立行政法人 情報処理推進機構（IPA）が，2016 年 10 月 24 日に，情報処理安全確保支援士の概要，登録，登録手続き，講習について公表しました。

これによって，第 1 回目の情報処理安全確保支援士試験が情報処理安全確保支援士制度の中で，2017 年 4 月に実施されました。2016 年 10 月を最後に廃止となった情報セキュリティスペシャリスト試験を引き継ぐ形です。

IPA のホームページには次のように紹介されています。

> 情報処理安全確保支援士試験の出題内容・範囲は，これまでの情報セキュリティスペシャリスト試験（SC）と変わりません。
>
> 情報処理安全確保支援士試験の合格者は，これまでのSC合格者と同様に，情報セキュリティに関する知識・技能を有する者として，経済産業大臣から合格証書が交付されます。
>
> 次に，情報処理安全確保支援士試験の合格者は，登録することによって，独占的に「情報処理安全確保支援士」の資格名称を使用することができます。
>
> （詳細は，国家資格「情報処理安全確保支援士」 参照）

まず，ここで情報処理安全確保支援士制度とはどのようなものなのかを解説し，その次に，本書を利用して合格を目指していただく情報処理安全確保支援士試験について解説します。

1. 国家資格「情報処理安全確保支援士」について

ここでは，情報処理安全確保支援士試験が実施されることになった背景と情報処理安全確保支援士制度の概要を，IPA のホームページなどから抜粋して掲載します。

1-1　情報処理安全確保支援士とは

(1)　概要

サイバー攻撃の急激な増加により，企業などにおけるサイバーセキュリティ対策の重要性が高まる一方，サイバーセキュリティ対策を担う実践的な能力を有する人材は不足しています。そこで，サイバーセキュリティに関する実践的な知識・技能を有する専門人材の育成と確保を目指して，国家資格「情報処理安全確保支援士」制度が創設されました。

「情報処理安全確保支援士（登録セキスペ）」はサイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し，サイバーセキュリティ対策の調査・分析・評価やその結果に基づく指導・助言を行います。

登録のメリット：

- 国家資格「情報処理安全確保支援士」の資格名称を使用することができます。
- 情報セキュリティに関する高度な知識・技能を保有する証になります。
- 毎年の講習受講により，情報セキュリティに関する最新知識や実践的な能力を維持できます。

情報処理安全確保支援士の通称名とロゴマーク：

情報処理安全確保支援士が社会全体で活用され，企業等におけるセキュリティ対策を進めるため，法律上の名称に加え，通称名とロゴマークを設けます。

法律名：情報処理安全確保支援士
通称名：登録セキスペ（登録情報セキュリティスペシャリスト）
英語名：RISS（Registered Information Security Specialist）
ロゴマーク：

2-3　情報処理安全確保支援士試験の対象者像

情報処理安全確保支援士試験の対象者像，業務と役割，期待する技術水準及びレベル対応を次に示します。

情報処理安全確保支援士試験
（SC：Registered Information Security Specialist Examination）

対象者像	サイバーセキュリティに関する専門的な知識・技能を活用して企業や組織における安全な情報システムの企画・設計・開発・運用を支援し，また，サイバーセキュリティ対策の調査・分析・評価を行い，その結果に基づき必要な指導・助言を行う者
業務と役割	セキュリティ機能の企画・要件定義・開発・運用・保守を推進又は支援する業務，若しくはセキュアな情報システム基盤を整備する業務に従事し，次の役割を主導的に果たすとともに，下位者を指導する。 ①　情報システムの脅威・脆弱性を分析，評価し，これらを適切に回避，防止するセキュリティ機能の企画・要件定義・開発を推進又は支援する。 ②　情報システム又はセキュリティ機能の開発プロジェクトにおいて，情報システムへの脅威を分析し，プロジェクト管理を適切に支援する。 ③　セキュリティ侵犯への対処やセキュリティパッチの適用作業など情報システム運用プロセスにおけるセキュリティ管理作業を技術的な側面から支援する。 ④　情報セキュリティポリシの作成，利用者教育などに関して，情報セキュリティ管理部門を支援する。
期待する技術水準	情報セキュリティ技術の専門家として，他の専門家と協力しながら情報セキュリティ技術を適用して，セキュアな情報システムを企画・要件定義・開発・運用・保守するため，次の知識・実践能力が要求される。 ①　情報システム又は情報システム基盤のリスク分析を行い，情報セキュリティポリシに準拠して具体的な情報セキュリティ要件を抽出できる。 ②　情報セキュリティ対策のうち，技術的な対策について基本的な技術と複数の特定の領域における応用技術をもち，これらの技術を対象システムに適用するとともに，その効果を評価できる。 ③　情報セキュリティ対策のうち，物理的・管理的な対策について基本的な知識と適用場面に関する技術をもつとともに，情報セキュリティマネジメントの基本的な考え方を理解し，これを適用するケースについて具体的な知識をもち，評価できる。 ④　情報技術のうち，ネットワーク，データベース，システム開発環境について基本的な知識をもち，情報システムの機密性，責任追跡性などを確保するために必要な暗号，認証，フィルタリング，ロギングなどの要素技術を選択できる。 ⑤　情報システム開発における工程管理，品質管理について基本的な知識と具体的な適用事例の知識，経験をもつ。 ⑥　情報セキュリティポリシに関する基本的な知識をもち，ポリシ策定，利用者教育などに関して，情報セキュリティ管理部門を支援できる。 ⑦　情報セキュリティ関連の法的要求事項などに関する基本的な知識をもち，これらを適用できる。
レベル対応	共通キャリア・スキルフレームワークの 人材像：テクニカルスペシャリストのレベル4の前提要件

図表 1-1-5　情報処理安全確保支援士の対象者像

4.　午後Ⅰ・午後Ⅱ対策

最後は本書のメインでもある午後対策です。

(1)　試験の“量”を把握する

午後Ⅰ試験は記述式です。試験時間は 90 分で，3 問出題される中から 2 問を選択し解答します。問題の形式は次のとおりです(極端な例外は除いています)。

基本情報	試験時間		90 分
	解答数／出題数		2 問／3 問
	1 問当たりの解答時間		45 分
問題 1 問 当たりの分量	ページ数		5〜7 ページ（20，24 ページ冊子）
	設問数		2 問〜5 問
	小問数		6 問〜12 問
		用語の穴埋めもしくは選択問題 （要求記述文字数 10 文字以下のみ）	1 個〜9 個
		記述式解答文字数の範囲	20 字／問〜50 字／問が中心， 60 文字／問以上もある
		記述式解答文字数の合計 （要求記述文字数 10 文字以下除く）	150 文字〜250 文字が多い

図表 1-2-7　午後Ⅰ問題形式

一方，午後Ⅱ試験の試験時間は 120 分で，2 問出題される中から 1 問を選択し解答します。

基本情報	試験時間		120 分
	解答数／出題数		1 問／2 問
問題 1 問 当たりの分量	ページ数		11〜14 ページ（24〜32 ページ冊子）
	設問数		3 問〜6 問
	小問数		8 問〜15 問
		用語の穴埋めもしくは選択問題 （要求記述文字数 10 文字以下のみ）	4 個〜6 個
		記述式解答文字数の範囲	30 字／問〜50 字／問が中心， 60 文字／問以上もある
		記述式解答文字数の合計 （要求記述文字数 10 文字以下除く）	300 文字〜400 文字が多い

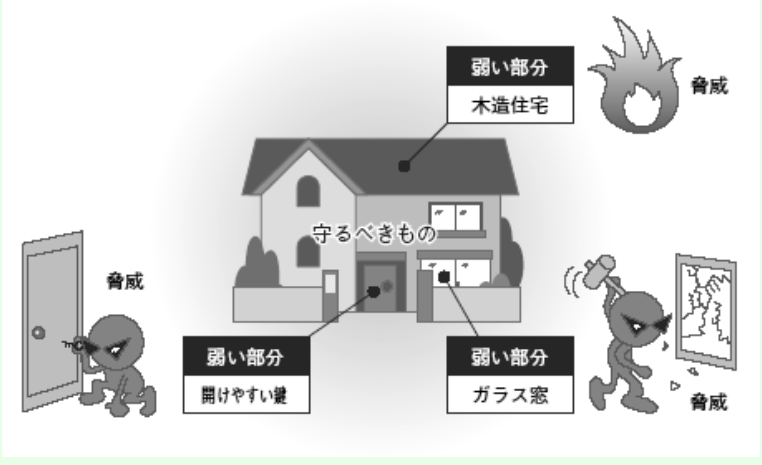
図表 1-2-8　午後Ⅱ問題形式

1　情報セキュリティの概念

情報セキュリティの全体像を理解する

セキュリティは，通常，図に見られるように，次の三つの要素が存在するときに必要になると言われています。

① 守るべきものの存在
② それを脅かす存在（脅威）
③ その脅威が突いてくる弱い部分の存在



図表 2-1-1　セキュリティを考えるときの三つの要素のイメージ（例）

図表 2-1-1 は，一般的なセキュリティの概念になりますが，企業が情報セキュリティを考えるとき，この三つの要素は，それぞれ次のような名称で呼ばれます。まずは，この三つの名称を覚えるところからスタートしましょう。

4　脅威

情報を詐取したり，改ざんや破壊したりする目的で，システムに対する攻撃が行われます。マルウェア，不正アクセス，盗聴，なりすまし，サービス不能攻撃，アプリケーションへの攻撃など。個々の攻撃手法には，独特の名称が付けられているので，それを覚えていきましょう。

(1)　マルウェア（malware）

悪意のコード（malicious code），又は悪意のソフトウェア（malicious software）の総称。コンピュータウイルス（ワーム，トロイの木馬，ボット等）に加えて，バックドアやルートキット，キーロガーなどの攻撃ツール，スパイウェアなども含んだ概念になります。

代表的なマルウェア		概要
ウイルス		自己伝染機能，潜伏機能，発病機能のいずれか一つ以上を有するもの（経済産業省：コンピュータウイルス基準より）。
	ワーム	ネットワークを通じてほかのコンピュータに拡散することを目的とした不正プログラム。
	トロイの木馬	増殖が主目的ではなく，ひっそりと常駐し，特定の日時や外部からの指示で破壊活動を開始する。
	ボット	コンピュータウイルスやワームの一種。語源はロボット。ボットを仕掛けた攻撃者は，遠隔操作によって，その端末から迷惑メールを送信したり，他のコンピュータを攻撃したりする。同一の指令サーバ配下のボットで形成されたネットワークをボットネットという。
攻撃ツール	バックドア	裏口。ハッキング成功時に，次回からアクセスや操作をしやすいように常駐させておくプログラムなど。
	ルートキット（rootkit）	様々なハッキングツールをまとめてキット状にしたもの。不正プログラムそのものや，バックドアの設置，ログの改ざんなど，標的サーバに不正侵入した後に使うツールなどをまとめたもの。
	キーロガー	打鍵したキーの使用を記録するソフト。
スパイウェア		利用者のコンピュータ内部の情報（環境設定情報，アクセス履歴など）を外部に自動的に通知する目的で常駐するプログラム（ソフトウェア）。

暗記事項

暗記事項をまとめました。しっかりと暗記してください。

問題	解答
1．情報セキュリティの概念	
三大要素（3）	① 情報資産 ② 脅威 ③ 脆弱性
情報セキュリティ確保の手順（4）	① 基本方針，情報セキュリティ委員会設置 ② 情報セキュリティポリシの作成 ③ セキュリティ教育，周知活動 ④ 定期的に評価・監査，必要に応じて見直し
情報セキュリティ対策（4）	① 抑止効果を狙う ② 予防的対策 ③ 事後対策（検知，復旧） ④ 再発防止策
情報セキュリティの三要素（3）	① Confidentiality；機密性 ② Integrity；完全性 ③ Availability；可用性
2．情報セキュリティマネジメント	
制度（6）	① 情報セキュリティマネジメント試験（新設） ② ISMS 適合性評価制度 ③ システム監査制度 ④ 情報セキュリティ監査制度 ⑤ プライバシーマーク制度 ⑥ 内部統制制度
情報セキュリティの推進体制（3）	① 情報セキュリティ推進組織 ② CISO ③ 情報セキュリティ管理者
ISMS 構築手順（10）	① ISMS の適用範囲を定義 ② ISMS の基本方針を定義 ③ リスクアセスメントの取組方法を定義 ④ リスク特定 ⑤ リスク分析・リスク評価 ⑥ リスク対応 ⑦ 管理目的と管理策を選択 ⑧ 残留リスクの承認 ⑨ ISMS の導入・運用を許可 ⑩ 適用宣言書を作成

Part 3　第2章　Chapter 2

PKI

PKI をメインテーマにした問題はそれほど多くはありません。しかし，設問単位ではコンスタントに出題されていましたし，問題文にキーワードが登場するケースも多く，「本当に，よく見かけるな」という印象があります。PKI が普及してきたことの現れでしょう。実際の開発現場でも，普通に“SSL”，“https”，“ディジタル証明書(公開鍵証明書，電子証明書)”という用語を用いますよね。

したがって，(メインテーマでの出題や，設問単位での出題，キーワードのみの出現などすべてを含めて)問題文に出現する可能性はとても高いと考えて，早い段階でしっかりと学習しておきましょう。問題を解くときに PKI 関連の用語に即座に反応できるようになれば，問題文を短時間で正確に理解することができますからね。

●学習目標　(次の知識が，瞬時に“アウトプット”できるようになる)

(1)　ディジタル証明書（概要）
(2)　PKI の運用環境（CA，RA，IA）
(3)　PKI の仕組み（一連の手順，CSR，CP/CPS）
(4)　ディジタル証明書のチェック方法
(5)　SSL の仕組み
(6)　HSTS（HTTP Strict Transport Security）
(7)　PKCS（Public-Key Cryptography Standards）

1．過去の出題内容を確認

出現率	75%

PKIは暗号技術などと同じようにセキュリティのインフラなので，午後問題にメインで出題されることは少ないですが，ごくごく普通に使われているので，逆に，しっかりとした知識が必要になるテーマになります。

そんなPKIの過去問題ですが，一番軸になる問題は，旧SC試験のH21年春午後Ⅱ問1だと考えています。この問題のキーワードは，「CP/CPS」，「自営CA」，「商用CA」，「ルートCA」，「CSR」，「鍵管理のアプライアンス製品」などです。

他には，H23年秋午後Ⅰ問3でプロキシ経由のWebアクセスをテーマにした問題が出題されています。このときのキーワードは「プロキシによるSSLの内容検査」，「コモンネーム」ですね。古くは，SU試験開始直後のH13年，H14年に出題されています。H13年午後Ⅰ問3「電子商取引の情報セキュリティ対策」では基礎的な問題が，H14年午後Ⅰ問2「認証システム」では，公開鍵証明書（ディジタル証明書）の更新のタイミングなどが問われています。

全出題実績

試験＼期		平成29年春
SC (注1)	午後Ⅰ	△ − △
	午後Ⅱ	○ △ ＼

試験＼期		平成21年春	平成21年秋	平成22年春	平成22年秋	平成23年春	平成23年秋	平成24年春	平成24年秋	平成25年春	平成25年秋
SC (注2)	午後Ⅰ	− − − −	○ − △ −	− − ○ −	△ − ○ −	− − − −	− − ◎ −	− − − −	○ − − ○	− − − −	− − − −
	午後Ⅱ	◎ − ＼	− △ ＼	− − ＼	− − ＼	− △ ＼	△ △ ＼	− − ＼	○ − ＼	− − ＼	− △ ＼

試験＼期		平成26年春	平成26年秋	平成27年春	平成27年秋	平成28年春	平成28年秋
SC (注2)	午後Ⅰ	− − ○	− ◎ −	○ − −	− − − −	− △ ◎	△ − △
	午後Ⅱ	− − ＼	△ ○ ＼	− ○ ＼	○ − ＼	− − ＼	○ ○ ＼

試験＼春期		平成18年	平成19年	平成20年
SV	午後Ⅰ	− △ ○ ○	− − − ○	− − △ −
	午後Ⅱ	− ○ ＼	− − ＼	− △ ＼

試験＼秋期		平成13年	平成14年	平成15年	平成16年	平成17年	平成18年	平成19年	平成20年
SU (SS)	午後Ⅰ	− − ◎ −	− ◎ ○ −	− − − −	− − − −	− − − ◎	− − − −	○ − − −	− − − ○
	午後Ⅱ	− − ＼	− − ＼	− − ＼	− − ＼	○ − ＼	− − ＼	− − ＼	− ○ ＼

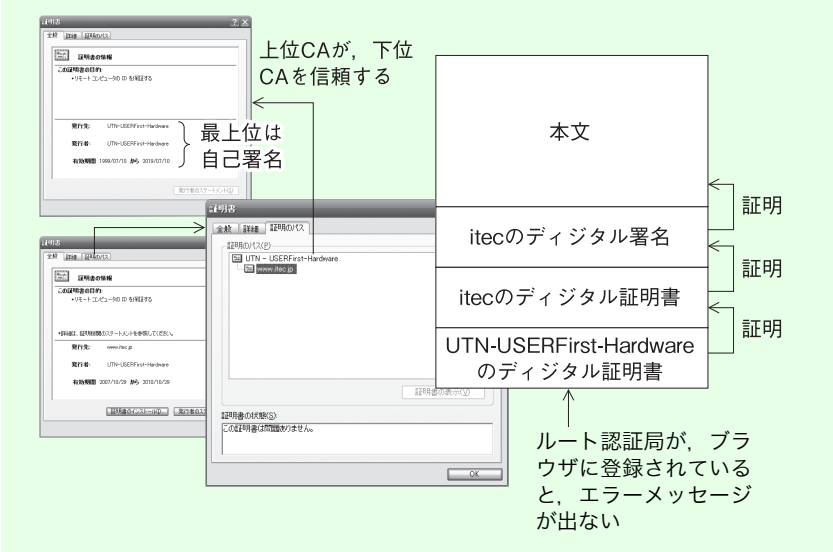
※1.記号の意味(◎＝メインテーマとして出題，○＝設問単位の出題，△＝問題文に登場，−＝無関係)
※2.各期内の欄は，左から順に問1，問2，問3，問4を表しています。
※3.(注1)は情報処理安全確保支援士試験，(注2)は情報セキュリティスペシャリスト試験です。

てもバッチ処理になってしまいます。その弱点を解消し，オンラインでリアルタイムに失効情報の確認を行う仕組みが，OCSP を使う方法です。この仕組みを利用するには，OCSP レスポンダ（OCSP サーバ）を立てて，そこに事前に CRL を取り込んでおかなければなりませんが，ディジタル証明書の確認を行うアプリケーションは，OCSP レスポンダに証明書番号でその都度問合せをかけ，失効していないかどうかを確認できるので，バッチ処理によるタイムラグは比較的ましになります。

④　ルート認証局，ルート証明書の検証

ディジタル証明書は，CA（認証局）さえ立ち上げれば，すなわち CA サーバを設置すれば，誰でも容易に運用することが可能です。しかし，それでは，ときに信頼に値しないことになるでしょう。

そこで，ディジタル証明書を階層管理し，上位の認証局が下位の認証局のディジタル証明書の正当性を証明する仕組みにしています（図表 3-2-6）。そして，階層構造の最上位にある CA を特に，ルート認証局，ルート CA，ルート証明機関などといいます。このルート CA をどのレベルにするかは，必要となる信頼度によって決めることになっています。なお，ルート認証局自体の正当性は自己署名で行います。



図表 3-2-6　IE の「証明書のパス」

6．演習問題

(H28秋-SC 午後Ⅱ問1)

IC カードを用いた認証システムに関する次の記述を読んで，設問 1～4 に答えよ。

D 社は，全国でマンションの開発・メンテナンスを手掛ける中堅の不動産デベロッパである。D 社は各地域を担当する四つの子会社をもち，各子会社はそれぞれ複数の事業部門をもつ。D 社及び子会社（以下，D 社グループという）は，積極的に人材交流を行い，人材育成及び人材活用を推進している。D 社グループの構成を表 1 に示す。

表 1　D 社グループの構成

会社名	役割
D 社	持株会社であり，D 社グループの戦略立案を担当する。グループ人事部門，グループ財務部門，研究部門などが，それぞれ D 社グループ全体の業務を担当する。
E 社	D 社の子会社であり，東日本地域の事業を担当する。
F 社	D 社の子会社であり，西日本地域の事業を担当する。
G 社	D 社の子会社であり，南日本地域の事業を担当する。
H 社	D 社の子会社であり，北日本地域の事業を担当する。

D 社グループの従業員（以下，グループ従業員という）には，D 社グループ内で一意となる番号（以下，グループ従業員番号という）が付与されている。また，オフィスや現場事務所の入室及び退室時に必要となる専用の IC カード（以下，入退室カードという）が貸与されている。D 社グループ各社にはそれぞれ IT 部門がある。D 社グループの全ての入退室カードは，D 社の IT 部門が管理している。各社の IT 部門は，自社従業員が利用する PC 及びネットワークを管理しており，D 社の IT 部門は，それらに加えて人事，経理などのバックオフィス系のシステムを管理している。

各事業部門は，それぞれ専用の Web システム（以下，事業用システムという）を多数運用している。D 社の子会社が実施するプロジェクトに参加する D 社グループ及び取引先のプロジェクトメンバには，必要に応じて事業用システムのアカウントが付与される。事業用システムは，今後も新しいシステムの導入や既存システムの更新が見込まれている。

〔IT 部門の統合〕

D 社では，IT による業務効率向上，コスト削減及び情報セキュリティ強化を目的に，D 社グループ各社の IT 部門を統合し，D 社内にシステム部を創設することにし

〔解答用紙〕

コピーして活用してください。また，アイテックホームページ https://www.itec.co.jp/ からダウンロードすることもできます（P.76 参照）。

設問1	(1)	a					b					c								
		k					l													
	(2)																			
	(3)	d					e					f								
	(4)																			
	(5)	g					h					i								
		j																		
設問2	(1)	①																		
		②																		
	(2)																			
	(3)	改善すべき不備																		
		失効事由の値																		

〔解説〕

本問では，認証カードの方式設計として，認証技術の基本知識，ディジタル署名の検証方法，認証対象者の不適切な行為などが問われています。また，認証カードの運用設計として，認証カードを発行する条件や，失効情報を公開するための条件の考察の他，認証局階層とサーバ証明書に関する記述式の設問が設定されています。さらに，取引先の従業者へ認証カードを貸与する場合における利点や，認証カードの管理方法などが問われています。用語の穴埋め問題については，解答群の中から選択する方法に変更されたので，記述式の設問に落ち着いて取り組むことができるでしょう。全体の難易度を評価すると，少し易しいレベルと考えられます。

［設問1］

(1) 空欄a，bは，Nさんの「パスワードを用いる利用者認証では，ログインする人の［ a ］を確認していました。認証カードを利用する利用者認証では，認証カードの［ b ］を確認することになりますね」という発言の中にあります。一般に，利用者認証としては，記憶認証，所持認証，生体認証（属性認証とも呼ぶ）という方法が用いられます。これらのうち，パスワードを用いる方法は，利用者の記憶に頼るものなので，記憶認証に当たります。したがって，空欄aには記憶（ウ）が入ります。また，認証カードを利用する方法は，利用者が認証カードを持っているかどうかを確かめる方法なので，所持認証に当たる。したがって，空欄bには所持（オ）が入ります。

空欄cは，R主任の「加えて，認証カードの利用時にPINを入力させることで，2種類の方法を組み合わせた［ c ］認証にすることができる」という発言の中にあります。認証カードの利用時にPIN（Personal Identification Number）を入力させるという方法は，認証カードを保持していることと，PINを記憶しているという二つの要素によって利用者認証を行います。このように複数の要素を組み合わせて認証する方法は，一般に多要素認証，又は複数要素認証と呼ばれています。したがって，空欄cには複数要素（ス）が入ります。

空欄k，lは，R主任の「1点目は，認証が成立するためには，鍵が［ k ］していないことが必要であることだ。事業用システムは，利用者証明書の失効情報を確認しなければならない。認証カードの紛失時などの場合，認証局は速やかに当該利用者証明書についての失効情報を提供する。失効情報は，CRLの配布により，又は［ l ］を使って提供されることが多い」とい