Contents

◆1◆合格へのアプローチ

◆2◆午前Ⅱ問題　レベル4の対策

本書は，2017 年春期から実施される新試験「情報処理安全確保支援士試験」に合格するための問題集です。この試験の前身として 2016 年秋期まで実施される「情報セキュリティスペシャリスト試験」の出題内容・形式を，新試験においても引き継ぐものと想定し，執筆・制作しております。

◆3◆午後Ⅰ・午後Ⅱ問題の対策

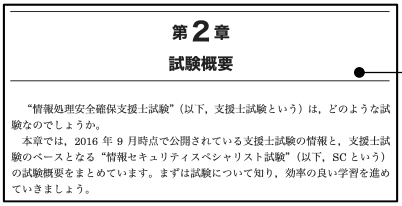
◆4◆巻末資料

第 1 章
ここが役立つ　本書の特長

本書は，
①プロが本試験を分析した結果に基づいて，予想した問題を掲載
②選び抜かれた良問を解くことで，効率良く合格を目指すことができる
問題集です。

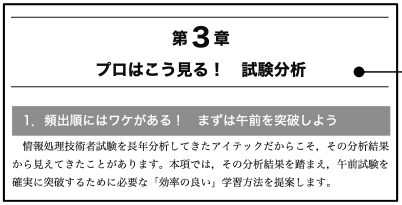
本書のいたるところに，学習者の皆様が効率良く学習を進められるような工夫を散りばめました。その一部をご紹介します。詳細は，各部・章をご覧ください。

1. 合格へのアプローチ　　合格に近づくための事前準備


第 2 章
試験概要

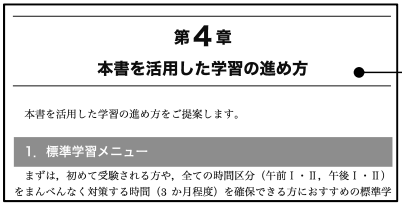
“情報処理安全確保支援士試験”（以下，支援士試験という）は，どのような試験なのでしょうか。
本章では，2016 年 9 月時点で公開されている支援士試験の情報と，支援士試験のベースとなる“情報セキュリティスペシャリスト試験”（以下，SC という）の試験概要をまとめています。まずは試験について知り，効率の良い学習を進めていきましょう。

試験概要
試験概要のうち，支援士試験学習者にとって必要な情報を紹介しています。


第 3 章
プロはこう見る！　試験分析

1. 頻出順にはワケがある！　まずは午前を突破しよう
情報処理技術者試験を長年分析してきたアイテックだからこそ，その分析結果から見えてきたことがあります。本項では，その分析結果を踏まえ，午前試験を確実に突破するために必要な「効率の良い」学習方法を提案します。

プロはこう見る！　試験分析
過去の本試験（SC）を徹底的に分析し，“なぜ本書の問題を解けば合格に近づくことができるのか”を説明しています。


第 4 章
本書を活用した学習の進め方

本書を活用した学習の進め方をご提案します。

1. 標準学習メニュー
まずは，初めて受験される方や，全ての時間区分（午前Ⅰ・Ⅱ，午後Ⅰ・Ⅱ）をまんべんなく対策する時間（3 か月程度）を確保できる方におすすめの標準学

本書を活用した学習の進め方
標準的な学習メニューに加え，ケース別の学習メニューも提案しています。

2. 午前Ⅱ問題　レベル 4 の対策

午前Ⅱ出題の大半を占める
レベル 4 問題を頻出順に掲載

→「レベル 4」などの技術レベルに関する詳細な説明は，「プロはこう見る！　試験分析」へ

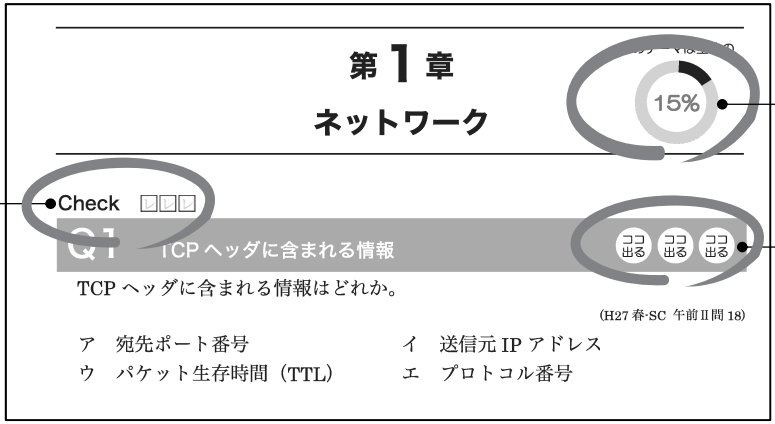
繰返し学習に役立つ“Check ボックス”

解いた問題にチェックを付けながら進めることで，後でどの問題を復習すればよいかの目安にもなります。

分野の出題割合

章冒頭の円グラフは，午前Ⅱ問題におけるその分野の出題率を示しています。

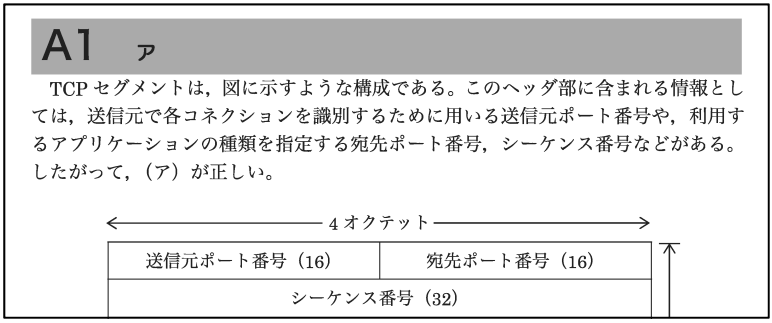
問題



頻出度を表す“ココ出るマーク”

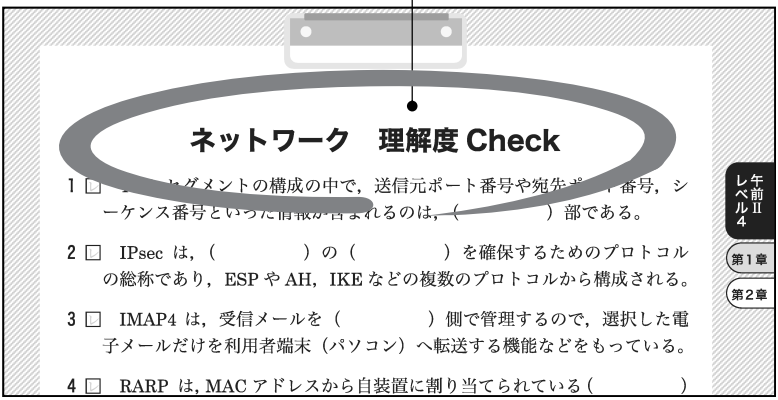
マークの数で，どの問題がよく出題されるのかがひと目で分かります。

解答解説



理解度 Check

章末の振り返りとして，理解度を確認します。理解度 Check の問題は，章内で解いてきた問題と対応しているので，復習に最適です。



ネットワーク　理解度 Check

1 □ セグメントの構成の中で，送信元ポート番号や宛先ポート番号，シーケンス番号といった情報が含まれるのは，（　　）部である。

2 □ IPsec は，（　　）の（　　）を確保するためのプロトコルの総称であり，ESP や AH，IKE などの複数のプロトコルから構成される。

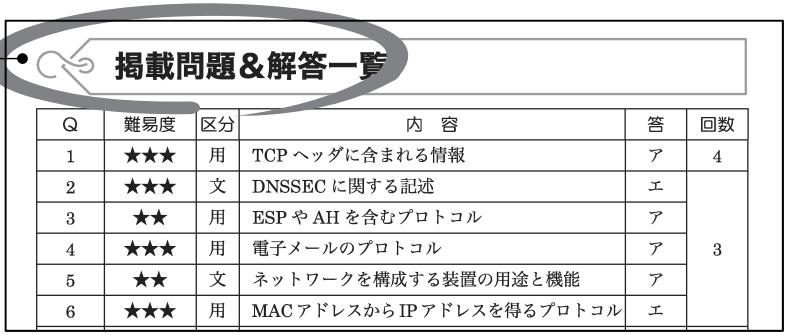
3 □ IMAP4 は，受信メールを（　　）側で管理するので，選択した電子メールだけを利用者端末（パソコン）へ転送する機能などをもっている。

4 □ RARP は，MAC アドレスから自装置に割り当てられている（　　）

午前Ⅱレベル4

第1章

第2章



掲載問題＆解答一覧

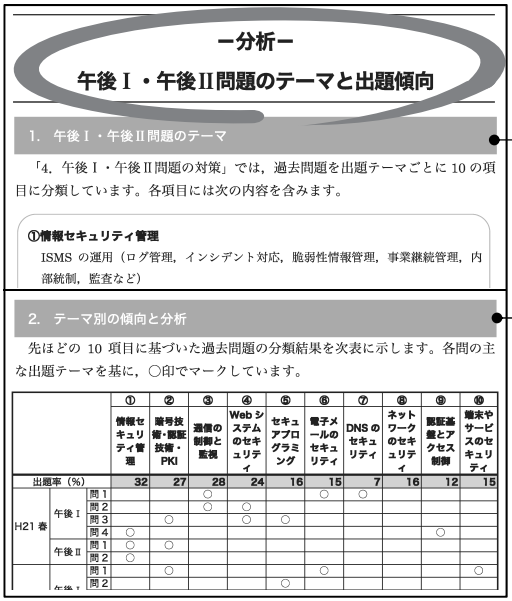
Q	難易度	区分	内　容	答	回数
1	★★★	用	TCP ヘッダに含まれる情報	ア	4
2	★★★	文	DNSSEC に関する記述	エ	
3	★★	用	ESP や AH を含むプロトコル	ア	
4	★★★	用	電子メールのプロトコル	ア	3
5	★★	文	ネットワークを構成する装置の用途と機能	ア	
6	★★★	用	MAC アドレスから IP アドレスを得るプロトコル	エ	

掲載問題＆解答一覧

章末には，掲載問題の難易度・区分・内容・解答・出題回数を一覧で掲載しています。

3．午後Ⅰ・午後Ⅱ問題の対策

各テーマの定番問題・演習問題で実力アップ



ー分析ー

午後Ⅰ・午後Ⅱ問題のテーマと出題傾向

1．午後Ⅰ・午後Ⅱ問題のテーマ

「4．午後Ⅰ・午後Ⅱ問題の対策」では，過去問題を出題テーマごとに 10 の項目に分類しています。各項目には次の内容を含みます。

①情報セキュリティ管理
ISMS の運用（ログ管理，インシデント対応，脆弱性情報管理，事業継続管理，内部統制，監査など）

2．テーマ別の傾向と分析

先ほどの 10 項目に基づいた過去問題の分類結果を次表に示します。各問の主な出題テーマを基に，○印でマークしています。

			① 情報セキュリティ管理	② 暗号技術・認証技術・PKI	③ 通信の制御と監視	④ Web システムのセキュリティ	⑤ セキュアプログラミング	⑥ 電子メールのセキュリティ	⑦ DNS のセキュリティ	⑧ ネットワークのセキュリティ	⑨ 認証基盤とアクセス制御	⑩ 脆弱やサービスのセキュリティ
出題率（%）			32	27	28	24	16	15	7	16	12	15
H21 春	午後Ⅰ	問1			○			○	○			
		問2			○	○						
		問3		○		○	○					
		問4	○								○	
	午後Ⅱ	問1	○	○								
		問2	○									
		問1		○				○				○
		問2					○					

午後Ⅰ・午後Ⅱ問題のテーマ

午後Ⅰ・午後Ⅱ問題の出題テーマが分かります。どんなテーマが出題されるか大枠で理解しましょう。

テーマ別の傾向と分析

重点的に出題されるテーマが分かります。

テーマの出題割合

平成 21 年以降に実施された SC 本試験で，このテーマの問題が出題された割合を示しています。

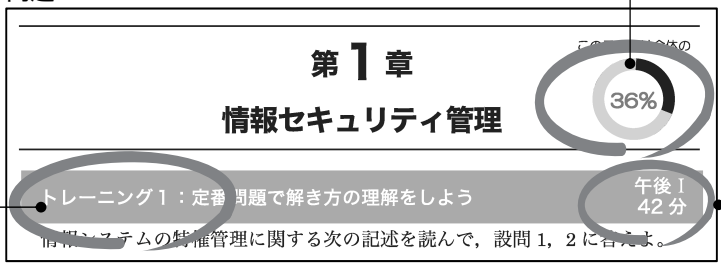
問題：トレーニング 1

定番問題で解き方のコツを身に付けます。

解答目安時間

解答の目安時間を設定しています。

問題



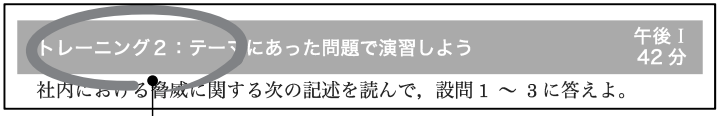
第 1 章

情報セキュリティ管理

36%

トレーニング 1：定番問題で解き方の理解をしよう　午後Ⅰ 42 分

情報システムの特権管理に関する次の記述を読んで，設問 1，2 に答えよ。



トレーニング 2：テーマにあった問題で演習しよう　午後Ⅰ 42 分

社内における脅威に関する次の記述を読んで，設問 1 ～ 3 に答えよ。

問題：トレーニング 2

テーマに合った良問の演習問題で，合格力をアップさせます。

解答解説

解説　トレーニング１：情報システムの特権管理　(H21 春-SC 午後 I 問 4)

【解答例】

［設問１］　(1) イ
(2) a：特権 ID の共用
(3) b：ログのレビュー

［設問２］　(1) ア
(2) c：syslog
(3) d：ログサーバの特権 ID 使用者とほかのサーバの特権 ID 使用者を分離

【配点】（アイテックで設問ごとに予想）

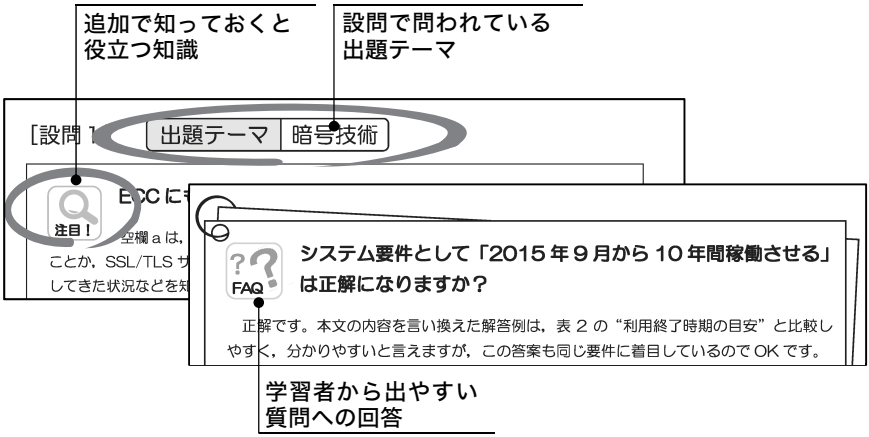
［設問１］	(1) 2 点，(2) 3 点，(3) 3 点
［設問２］	(1) 2 点，(2) 2 点，(3) 8 点，(4) 6 点， (5) 下線④：6 点，下線⑤：6 点 (6) 確認する内容：6 点，立証しようとしていること：6 点

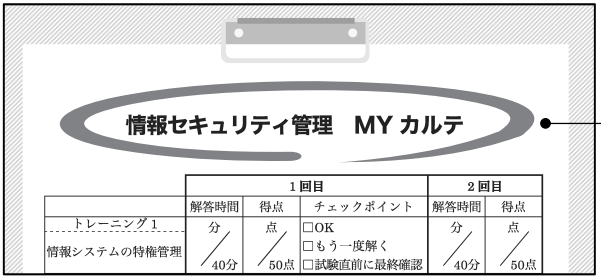
配点表

配点表（本試験問題については，アイテックの予想配点）を活用すれば，自分の実力を把握できます。

アイコン

トレーニング１の解説には，次のアイコンで，より詳しく説明をしています。





MY カルテ

章末の MY カルテに，解答時間，得点，チェックポイントなどを記録しておけば，後からの復習に役立ちます。

第1章 ネットワーク

このテーマは全体の15%

☆解答解説は p.41

Check □□□

Q1 TCP ヘッダに含まれる情報

ココ出る ココ出る ココ出る

TCP ヘッダに含まれる情報はどれか。

(H27 春-SC 午前Ⅱ問 18)

ア　宛先ポート番号　　イ　送信元 IP アドレス
ウ　パケット生存時間（TTL）　　エ　プロトコル番号

Check □□□

Q2 DNSSEC に関する記述

ココ出る ココ出る

DNSSEC に関する記述として，適切なものはどれか。

(H26 秋-SC 午前Ⅱ問 18)

ア　DNS サーバへの DoS 攻撃を防止できる。
イ　IPsec による暗号化通信が前提となっている。
ウ　代表的な DNS サーバの実装である BIND の代替として使用する。
エ　ディジタル署名によって DNS 応答の正当性を確認できる。

Check □□□

Q3 ESP や AH を含むプロトコル

ココ出る ココ出る

インターネット VPN を実現するために用いられる技術であり，ESP（Encapsulating Security Payload）や AH（Authentication Header）などのプロトコルを含むものはどれか。

(H26 春-SC 午前Ⅱ問 20)

ア　IPsec　　イ　MPLS　　ウ　PPP　　エ　SSL

解答解説

A1　ア

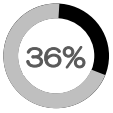
TCP セグメントは，図に示すような構成である。このヘッダ部に含まれる情報としては，送信元で各コネクションを識別するために用いる送信元ポート番号や，利用するアプリケーションの種類を指定する宛先ポート番号，シーケンス番号などがある。したがって，（ア）が正しい。

なお，送信元 IP アドレス，パケット生存時間（TTL；Time To Live），プロトコル番号は IP ヘッダに含まれる情報である。

A2　エ

DNS（Domain Name System）サーバは，その役割からキャッシュサーバとコンテンツサーバ（権威 DNS サーバ）に分類される。クライアントが DNS 問合せを行う際には，キャッシュサーバに問い合わせるが，キャッシュサーバが問合せのあった名前情報をキャッシュに保存していない場合には，コンテンツサーバに問い合わせて，名前情報を得るようにしている。しかし，正規のコンテンツサーバから応答が返される前に，悪意の第三者が偽の応答パケット（問合せパケットがもつ条件と一致するもの）を送信すれば，それを正規のコンテンツサーバからの応答と見なして，キャッシュに保存してしまう。すると，クライアントは，キャッシュサーバから偽の IP アドレスを受け取ることになり，偽のサーバに誘導されてしまうという危険性がある。そこで，DNSSEC では，ディジタル署名を添付して正規のコンテンツサーバからの応答である

第1章 情報セキュリティ管理

このテーマは全体の


トレーニング1：定番問題で解き方の理解をしよう

午後Ⅰ 42分

情報システムの特権管理に関する次の記述を読んで，設問1，2に答えよ。

(H21春-SC 午後Ⅰ問4)

E社は，従業員数2,000名の上場している運輸会社である。E社の情報システム部では80台のサーバを管理しており，複数種のOSと，複数のDBMS及びアプリケーション（以下，APという）が稼働している。

インストールされたそれぞれのOS，DBMS，APに対して，システム管理特権が付与された利用者ID（以下，特権IDという）が一つずつ登録されており，情報システム部内のシステム管理チームに所属するシステム管理者10名がすべての特権IDとパスワードを共用している。例えば，OS，DBMS，APがそれぞれ一つずつ稼働しているサーバでは，OSに一つ，DBMSに一つ，APに一つの特権IDが登録されており，システム管理者10名がこれらの特権IDを共用している。特権IDの使用は，基本的にはネットワーク経由で行われているが，コンソールからでないと行えない特定の作業については，サーバが保管されているラック内に設置されたコンソールから行われている。

E社は，システム運用の安全性を確認するために，セキュリティ専門会社のF社に，サーバの設定や運用に関するセキュリティ診断を依頼した。診断の結果，情報システムの特権ID管理が十分でないとの指摘を受けたことから，経営陣は情報システム部に対して特権IDの管理を改善するように指示した。

〔特権ID管理の要件〕

F社による指摘は，“特権IDの使用において，内部者の不正使用を防止及び発見する仕組みが構築されていない”というものであった。システム管理チームのN課長とM君は，この指摘に基づき，必要な管理要件を明確にすることにした。

N課長：M君，現状の特権ID管理において必要な管理要件とは具体的に何だろう。

「ログサーバのログに対してアクセス権限を設定」は正解になりますか？

残念ですが不正解です。「アクセス権限を設定する」だけでは，「ほかのサーバ管理者による故意のログ削除を防止」という効果に直接結びつきません。ほかのサーバ管理者がログにアクセスできないことが明確に分かるように，ログ管理サーバ専用のIDによって職務を分離することまでの説明が必要です。

(4) 下線③を含む記述は，N課長の「これらの条件だけでは，本人に割り当てられている特権IDを使用したときにしか検出できないな。特権IDをもっていない人が特権IDを使用しようとする行為があったときにも検出できるようにしてくれないか」という発言の中にある。特権IDをもっていない人が特権IDを使用した場合には，不正行為にあたるので，アラートを発生させる必要がある。また，アラートの発生条件としては，一般に特権IDのパスワード認証に失敗したことが契機となる。したがって，解答としては「特権IDの認証が失敗したとき」などのように答えるとよい。

(5) 下線④は，「アラートを設定していることはシステム管理者に周知」である。一般に，アラートを設定していることをシステム管理者に周知するということは，システム管理者による不正行為の実行を抑止させるという効果を持つ。したがって，下線④のセキュリティ上の目的としては「システム管理者による不正行為の実行を抑止する」旨を解答すればよい。

下線⑤は，「具体的なアラートの発生条件は伝えない」である。つまり，具体的なアラートの発生条件をすべて明示してしまうと，そのアラートの発生条件にかからないように，不正行為が行われてしまうというリスクを抱えることになってしまう。したがって，下線⑤のセキュリティ上の目的としては「アラートが発生しないような不正使用方法を発見されないようにする」旨の解答を導くことができる。

ログ管理の定番問題

注目！

アラートやログ監視の周知とその程度に関する設問で，定期的に出題されています。

(6) 下線⑥は，N課長の「データベース（以下，DBという）では当社の財務にかかわる重要なデータが管理されているから，財務報告の信頼性を担保するためにも，特権IDを使用してDBを操作したログを取得して保存することは重要なんだ」と

情報セキュリティ管理　MY カルテ

	1 回目			2 回目	
	解答時間	得点	チェックポイント	解答時間	得点
トレーニング 1 情報システムの特権管理	分 ／ 42分	点 ／ 50点	□OK □もう一度解く □試験直前に最終確認	分 ／ 42分	点 ／ 50点
トレーニング 2 社内における脅威	分 ／ 42分	点 ／ 50点	□OK □もう一度解く □試験直前に最終確認	分 ／ 42分	点 ／ 50点
トレーニング 3 Web システムのインシデント対応	分 ／ 105分	点 ／ 100点	□OK □もう一度解く □試験直前に最終確認	分 ／ 105分	点 ／ 100点