Contents

目次

■第１部　合格へのアプローチ

■第２部　午前Ⅱ問題　レベル４の対策

■第３部　午後Ⅰ・午後Ⅱ問題の対策

■第４部　巻末資料

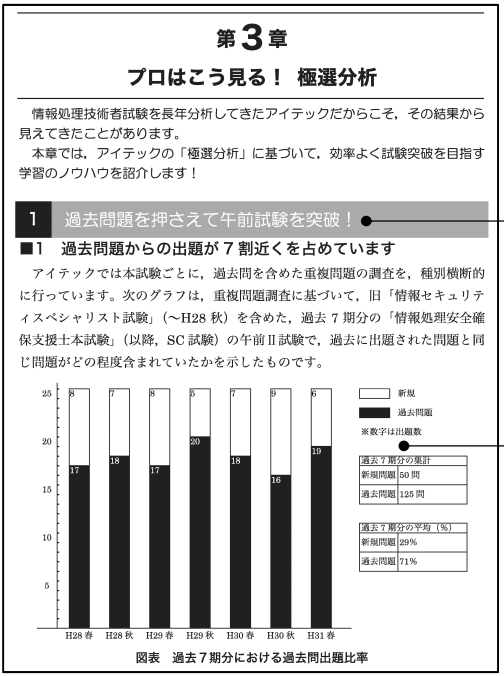
第 1 章
「極選分析 予想問題集」の特長・使い方

試験対策のプロ，アイテックが本試験問題を徹底的に分析し，試験に出やすい問題やテーマを予想しました。選び抜かれた過去問題，頻出テーマを詳細な解説付きで集中的に学ぶことで，必要な知識を効果的に身に付けることができます。

本書はアイテック独自の分析と詳細な解説を軸に，皆さんが効率よく学習を進められるよう，充実した内容，構成となっています。

1 試験対策のプロ，アイテックによる「極選分析」

第 3 章「プロはこう見る！ 極選分析」では，本試験問題の分析結果を，統計資料を交えてご紹介しています。アイテック独自の徹底した分析を通して，試験対策のツボを見つけましょう。



第3章

プロはこう見る！ 極選分析

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，その結果から見えてきたことがあります。

本章では，アイテックの「極選分析」に基づいて，効率よく試験突破を目指す学習のノウハウを紹介します！

1 過去問題を押さえて午前試験を突破！

■1 過去問題からの出題が 7 割近くを占めています

アイテックでは本試験ごとに，過去問を含めた重複問題の調査を，種別横断的に行っています。次のグラフは，重複問題調査に基づいて，旧「情報セキュリティスペシャリスト試験」（～H28 秋）を含めた，過去 7 期分の「情報処理安全確保支援士本試験」（以降，SC 試験）の午前Ⅱ試験で，過去に出題された問題と同じ問題がどの程度含まれていたかを示したものです。

図表 過去 7 期分における過去問出題比率

様々な観点から本試験を分析！

「過去問題」，「分野」，「頻出度」，「重点テーマ」などの観点から，本試験問題を午前，午後それぞれを徹底的に分析しています。37 年にわたる IT 教育の実績に基づいたプロの視点と，蓄積された膨大な試験問題の資料を元に，学ぶべき問題を選び出しました。

本試験問題の統計データ

アイテックでは，本試験ごとに出題された問題の統計資料を作成しています。第 3 章ではそれらを活用して，分析の根拠としてご紹介しました。演習問題と合わせて，効率的な学習方法を見つけ出しましょう。

			(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
			情報セキュリティ管理	暗号技術・認証技術・PKI	通信の制御と監視	Web システムのセキュリティ	セキュアプログラミング	電子メールのセキュリティ	DNS のセキュリティ	ネットワークのセキュリティ	認証基盤とアクセス制御	端末やサービスのセキュリティ
問題数			43	33	42	34	20	16	13	24	17	16
出題率（%）			38	29	37	30	18	14	11	21	15	14
H21 春	午後Ⅰ	問1			○			○	○			
		問2			○	○						
		問3		○		○	○					
		問4	○								○	
	午後Ⅱ	問1	○	○								
		問2	○									
H21 秋	午後Ⅰ	問1		○				○				○
		問2					○					
		問3	○	○								
		問4		○								○
	午後Ⅱ	問1									○	
		問2			○					○		

午後問題の分析表

過去 11 年間の本試験で出題された午後Ⅰ・Ⅱ問題を，テーマごとに分析し，出題年度と出題頻度を一覧で示しています。情報処理安全確保支援士試験の午後問題で出題されるテーマの大枠と重点的に出題されているテーマが分かります。

2　午前 II レベル４の演習問題と詳細解説

「第２部 午前Ⅱ問題レベル４の対策」では，「極選分析」に基づいて，午前Ⅱレベル４問題の過去問題（平成 21 年度春期以降）から，令和２年度春期の試験対策に効果的な問題を選び抜きました。アイテックの詳細な解答解説で午前Ⅱ試験を突破するための効率の良い学習に役立ちます。

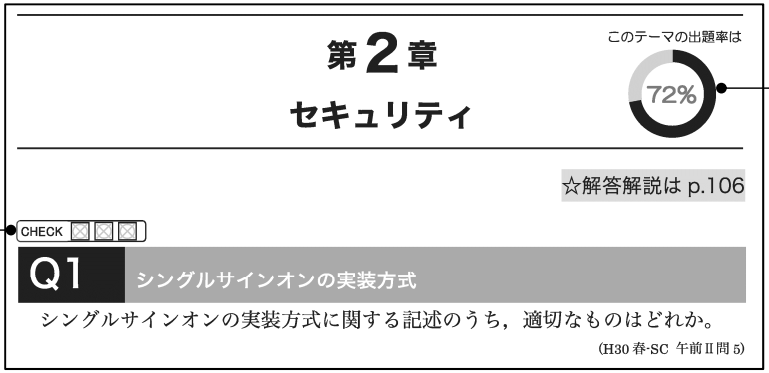
繰返し学習に便利な“CHECK ボックス”

午前問題は繰返し解いて，類似問題や午後試験への対策に役立つ知識を身に付けたいものです。CHECK ボックスを活用して，「使える」知識を増やしましょう！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問題全 25 問中，その分野の問題が何問出題されていたかの出題率を示しています。

演習問題



解答解説

A1　ェ

シングルサインオン（Single Sign On；SSO）とは，複数のシステムに対する利用者認証を，一元的な方法で行うための仕組みである。SSO を導入すると，利用者は一度の認証操作で複数のシステムを利用することが可能になる。

SSO の実装方式は，大別すると，エージェント方式とリバースプロキシ方式に分けられる。エージェント方式は，対象となる各サーバにエージェントと呼ばれる SSO 機

アイテックが誇る詳細な解答解説で理解を深めよう！

単に正解についての説明だけでなく，関連する技術やテーマ，正解以外の選択肢についても解説しているので，問われている内容についてより深く理解できます。

掲載問題＆解答一覧

Q	難易度	問題区分	内　容	答	出題回数	
					全	SC
1	☆☆☆	文	シングルサインオンの実装方式	エ	9	5
2	☆☆☆	文	TLS に関する記述	ウ		4
3	☆☆☆	文	ルートキットの特徴	ア		6
4	☆☆☆	考	SQL インジェクション対策	エ		6
5	☆☆☆	文	AES の特徴	ア		5
6	☆☆☆	文	ディジタル証明書	イ		5
7	☆☆☆	文	情報セキュリティリスクに関する記述	エ		5
8	☆☆☆	考	ファイアウォールの設定	ア	6	5

掲載問題＆解答一覧

章末には，掲載問題の難易度・問題区分・内容・解答・出題回数（全種別，SC）を一覧で掲載しています。出題回数が多い問題は定番問題ということで，重要な知識を問うていますので，ぜひ重点的に学習しておきましょう。

3　各テーマの定番問題・演習問題で実力アップ

「第３部 午後Ⅰ・午後Ⅱ問題の対策」では，「極選分析」に基づいて，これまで（平成 21 年度春期以降）に出題された午後Ⅰ・午後Ⅱ問題をテーマ毎に分類しました。各テーマに沿って選ばれた定番問題と演習問題を解いて，午後試験突破に必要な解法力を養いましょう。

掲載問題リスト

午後Ⅰ・Ⅱ演習問題の問題リストを掲載しました。テーマごとにまとめた掲載問題について，「出題年度」，「試験区分」，「種別」，「時間区分」，「問題タイトル」，「解答目安時間」などを，問題を解く前に確認できます。苦手なテーマや知識分野の確認と克服に活用してください。

●問題リスト

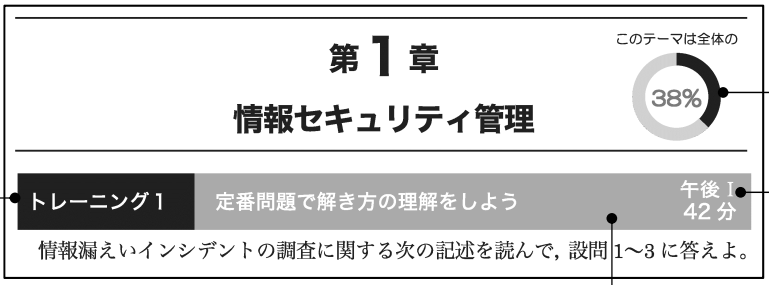
トレーニング	年度	試験区分	種別	時間区分	問NO	問題タイトル	解答目安時間	CHECK!
第1章　情報セキュリティ管理								
1	2015春	本試	SC	午後Ⅰ	2	情報漏えいインシデントの調査	42分	
2	2013秋	公開	SC	午後Ⅰ	3	社内における脅威	42分	
3	2017春	本試	SC	午後Ⅱ	1	マルウェアの解析	105分	
第2章　暗号技術・認証技術・PKI								
1	2014秋	本試	SC	午後Ⅰ	2	代理店販売システム	42分	
2	2017春	公開	SC	午後Ⅰ	1	暗号アルゴリズム	42分	
3	2017秋	本試	SC	午後Ⅱ	2	データ暗号化の設計	105分	

トレーニング1は定番問題！

各章のトレーニング1には定番問題を掲載しました。定番問題では，各テーマの解法力を養うために必要な基礎的な知識や考え方を身に付けることを目指しましょう。

テーマの出題割合

章冒頭の円グラフは，平成21年度以降に実施された午後Ⅰ・Ⅱ試験で，そのテーマの問題が何問出題されていたかの統計を元に出題率を示しています。



トレンド問題

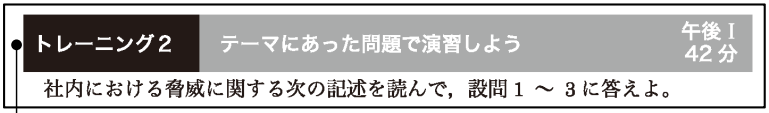
特に近年，急激に普及が進む技術やそれに関わる脅威をテーマとして取り上げた問題を，「トレンド問題」として，このアイコンを付けて示しています。情報セキュリティ分野では常に最新の技術動向に関する知識・技能が求められますので，トレンド問題は要CHECKです！

解答目安時間

問題を解くときにかかった時間を確認しておき，解答目安時間と比べてみましょう。この時間より多くかかる場合には，本試験で最後まで答えきれない可能性があります。

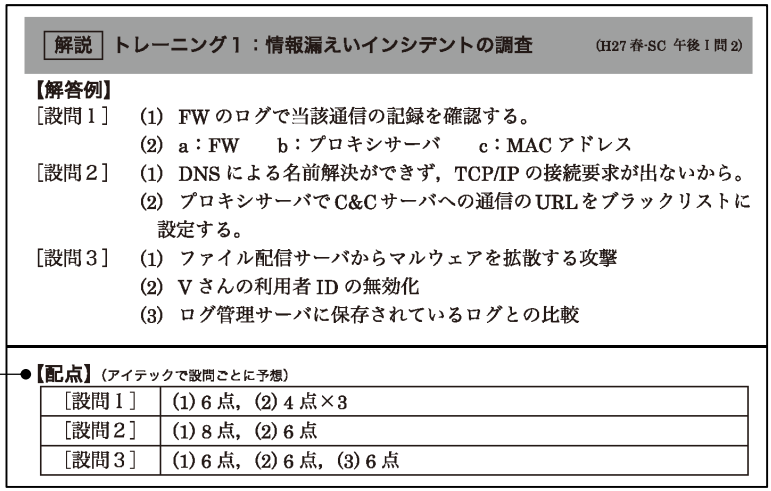
各章の解説では，次のアイコンを使って，テーマに関係する，より詳しい説明を加えています。

アイコン	説明
ココが要点	各設問で問われている知識／内容
	問題を解くに当たって，追加で知っておくと役立つ知識
	学習者から多く寄せられた質問への回答



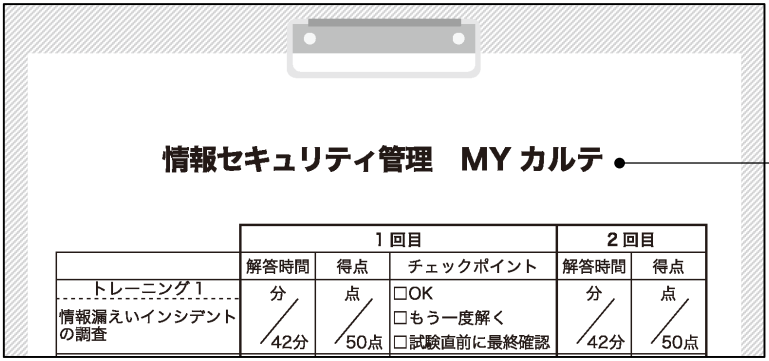
トレーニング２以降は演習問題！

テーマに合った良問を解いて，合格に必要な解法力アップ！



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，現在の自分の実力を把握できます。

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，復習時に役立ちます。



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 情報漏えいインシデントの調査	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

本試験

過去問題の出典	H31春	H30秋	H30春	H29秋	H29春	H28秋	H28春
H30秋	0						
H30春	0	0					
H29秋	**8**	0	1				
H29春	0	**9**	0	0			
H28秋	0	2	**11**	0	0		
H28春	2	2	2	**11**	0	0	
H27秋	3	1	2	2	**8**	0	0
H27春	2	0	0	0	2	**8**	0
H26秋	1	0	1	1	5	2	**9**
H26春	1	0	1	1	0	3	1
H25秋	0	0	1	0	0	3	2
H25春	0	1	0	0	1	1	1
H24秋	0	0	0	0	0	0	1
H24春	0	0	0	0	0	1	2
H23秋	0	0	0	0	0	0	0
H23春	0	0	0	1	1	0	1
H22秋	1	0	0	1	0	0	0
H22春	0	0	0	0	0	0	0
H21秋	0	0	0	0	0	0	0
H21春	0	1	0	0	0	0	0

※数字は出題数

図表　過去7期分における過去問題の出典年度

過去問として多く出題されている期に注目してみると，期ごとに多少の差はありますが，おおむね表の太枠で囲まれている箇所，つまり3期前から特に多く出題されている傾向を読み取ることができます。これはSC試験で顕著な傾向です。

今後もこの傾向が続くとするならば，過去問演習においても，該当年度の過去問を押さえておくことが効率的であることになります。本書掲載の「午前Ⅱ試験レベル4対策」問題では，この点も反映した問題選択を行っています。

■5　頻出問題に注目！

実は過去問の中には何度も出題されている問題があります。この何度も出ている問題は良問あるいは定番と呼ばれ，該当分野の中で受験者に確実に身に付けておいてほしい知識が問われます。そのため，今後も出題される可能性が高い問題といえるでしょう。そこで，本書では出題傾向や実際の出題回数などをさらに分析し，出た回数が多い（頻出）順で掲載しています。今後も出題される可能性が高い良問を解くことで，効率良く学習することができます。

書籍をご購入いただいた方限定!

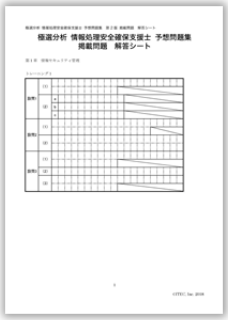
ダウンロード／Web コンテンツ

①学習前に準備しておきたいコンテンツ

◎「午後問題解答シート」（PDF ファイル）

本書の「第３部　午後Ⅰ・午後Ⅱ問題の対策」に掲載している午後問題の解答シートをご用意いたしました。実際に解答を書き込みながら，問題を解いてみましょう。

午後問題の解答は手書きで記入します。この「午後問題解答シート」を利用して，制限時間内に解答を書き込む感覚を身に付けてください。本番で焦ることのないよう，バッチリ対策しましょう。



ご利用方法

① https://www.itec.co.jp/support/download/book/sc_gokusen3.zip に Web ブラウザからアクセスしてください。

② ダウンロードしたファイルをパスワード「■■■■■■■■■■■■■■」で解凍してご利用ください。

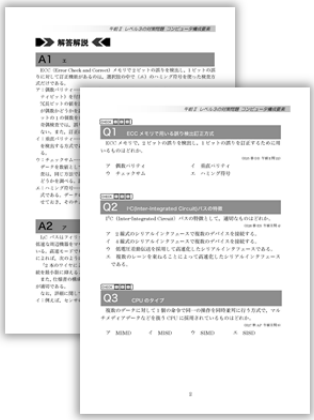
※こちらのダウンロード期限は，2021 年 10 月末です。

②学習に役立つコンテンツ

◎「午前Ⅱ　レベル３の対策問題」（PDF ファイル）

午前Ⅱ試験はレベル４を押さえることが最優先。ですが，レベル３の問題の対策もしておけば，より万全の態勢で午前試験突破を目指せます。

本コンテンツでは SC 試験のレベル３として出題される「データベース」，「システム開発技術」，「ソフトウェア開発管理技術」，「サービスマネジメント」，「システム監査」の５分野の演習用問題を PDF ファイルにてご用意しております。



◎「どこでも極選午前Ⅰ演習問題」
（Web コンテンツ）

午前Ⅰ対策用の Web コンテンツ「どこでも極選午前Ⅰ演習問題」をご用意しました。スマートフォンや PC で繰り返し問題演習ができる Web コンテンツです。

全 110 問の中から本試験での大分野ごとの出題率に合わせて 30 問が出題されます。移動中のスキマ時間にも，手軽に本番を想定した学習ができるコンテンツになっています。

ご利用方法

① https://questant.jp/q/sc_gokusen3 に Web ブラウザからアクセスしてください。

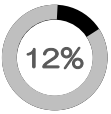
② 本書に関する簡単なアンケートにご協力ください。
アンケートのご回答後，「午前Ⅱ　レベル３の対策問題」，「どこでも極選午前Ⅰ演習問題」のダウンロードページに移動します。

③ ダウンロードした zip ファイルをパスワード「■■■■■■■■■■■■■■■■■■■■」で解凍してご利用ください。

・毎年，4 月末，10 月末までに弊社アンケートにご回答いただいた方の中から抽選で 20 名様に，図書カード 1,000 円分をプレゼントしております。ご当選された方には，ご登録いただいたメールアドレスにご連絡させていただきます。当選者の発表は，当選者へのご連絡をもって代えさせていただきます。
・ご入力いただきましたメールアドレスは，当選した場合の当選通知，賞品お届けのためのご連絡，賞品の発送のみに利用いたします。
・こちらのダウンロード期限は 2021 年 10 月末です。

第1章 ネットワーク

このテーマの出題率は



☆解答解説は p.61

CHECK ☒☒☒

Q1 呼量の計算

180 台の電話機のトラフィックを調べたところ，電話機 1 台当たりの呼の発生頻度（発着呼の合計）は 3 分に 1 回，平均回線保留時間は 80 秒であった。このときの呼量は何アーランか。

(H29 秋-NW 午前Ⅱ問 2)

ア　4　　イ　12　　ウ　45　　エ　80

CHECK ☒☒☒

Q2 TCP ヘッダに含まれる情報

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 ☒☒☒

Q3 ホストアドレス

ネットワークに接続されているホストの IP アドレスが 198.51.100.90 で，サブネットマスクが 255.255.255.224 のとき，ホストアドレスはどれか。

(H29 秋-SC 午前Ⅱ問 20)

ア　10　　イ　26　　ウ　90　　エ　212

解答解説

A1　エ

呼量（アーラン）は，呼数×平均回線保留時間で求められる。本問では，電話機が180台，呼の発生頻度が3分（180秒）に1回で，平均回線保留時間が80秒であることから，その呼量Aは，

A＝180(台)×(1／180(秒))×80(秒)
　＝80(アーラン)

となる。したがって，（エ）が正しい。

A2　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。

第1章
情報セキュリティ管理

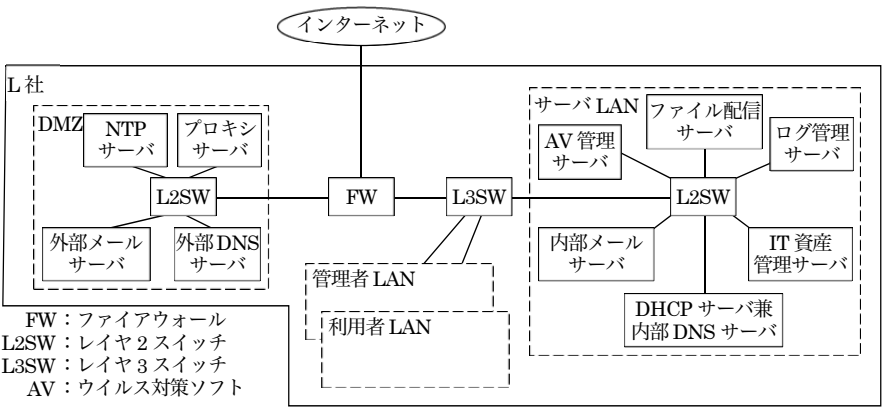
このテーマは全体の


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

情報漏えいインシデントの調査に関する次の記述を読んで，設問1～3に答えよ。

(H27春-SC 午後Ⅰ問2)

L社は，従業員数700名のシステムインテグレータである。L社のネットワーク構成を図1に，主なサーバとその概要を表1に示す。



注記1　L3SWのデフォルトゲートウェイは，FWに設定されている。
注記2　L社のPCは，利用者LAN又は管理者LANに接続されている。

図1　L社のネットワーク構成（概要）

表1　主なサーバとその概要

サーバ名称	概要
プロキシサーバ	・プロキシ認証機能を使用し，利用者IDとパスワードで認証する。 ・ブラックリスト型のURLフィルタリング機能をもつ。
AV管理サーバ	・各PC及び各サーバ上で稼働しているAVは，ウイルス定義ファイルをAV管理サーバから自動的に取得するよう設定されている。
ファイル配信サーバ	・パッチの自動配信及びパッチの強制適用に利用されている。
ログ管理サーバ	・図1中のネットワーク機器及びサーバのログをsyslogで受信し，直近3か月分を保存する。 ・syslog受信に必要なポート以外は全て閉じ，リモートからアクセスできないようにしている。

解答解説

解説　トレーニング1：情報漏えいインシデントの調査　(H27春-SC 午後Ⅰ問2)

【解答例】

［設問1］　(1) FWのログで当該通信の記録を確認する。
(2) a：FW　　b：プロキシサーバ　　c：MACアドレス

［設問2］　(1) DNSによる名前解決ができず，TCP/IPの接続要求が出ないから。
(2) プロキシサーバでC&Cサーバへの通信のURLをブラックリストに設定する。

［設問3］　(1) ファイル配信サーバからマルウェアを拡散する攻撃
(2) Vさんの利用者IDの無効化
(3) ログ管理サーバに保存されているログとの比較

【配点】

［設問1］	(1) 6点，(2) 4点×3
［設問2］	(1) 8点，(2) 6点
［設問3］	(1) 6点，(2) 6点，(3) 6点

【解説】

マルウェア攻撃によるインシデントの調査をテーマとして，設問1ではC&Cサーバへのバックドア通信に関する調査，設問2ではバックドア通信の考察や遮断方法，設問3では内部拡大攻撃の考察や対策の問題が出題されている。プロキシサーバやMACアドレス，DNSの仕組みなどのネットワーク分野の基本的な技術知識が必要となるが，ほとんどの設問は問題文中の複数の記述を結び付けると解答を導くことができる。制限時間の中で，解答に必要な記述をどれだけ的確に読み取れるかがポイントになるといえる。

［設問1］　**ココ**が要点　マルウェアの活動に関する通信ログの調査

(1) この設問では，下線①について，確認の具体的な方法が問われている。なお，下線①を含む記述は，「M部長から指示を受け，Nさんが確認したところ，送信元IPアドレスは間違いなくL社のものであった。また，このIPアドレスから当該C&Cサーバへの通信が発生していたことも確認できた」である。

当該C&Cサーバへの通信の送信元IPアドレスがL社のものなので，L社のどのIPアドレスが使用されているかを確認するとよい。表2の前に「FWはステートフルパケットインスペクション型であり，NAPT機能を使用している。また，許可した通信，拒否した通信ともにログを取得するように設定し，取得したログは全てログ管理サーバに送信している」と記述されている。FWでNAPT（Network Address

Port Translation）機能によって，送信元の IP アドレスとポート番号を変換しているので，L 社から外部（インターネット側）に出て行く送信元 IP アドレスは，全て FW のものになる。そして，FW で許可した通信，拒否した通信ともにログを取得しているので，FW のログを調査すれば，FW の IP アドレスから当該 C&C サーバへの通信が発生しているかどうかを確認できる。したがって，解答としては「FW のログで当該通信の記録を確認する」旨を答えるとよい。

①「ログ管理サーバのログで C&C サーバへの通信記録を確認する」は正解になりますか？

②「ログ管理サーバの FW が許可したログで当該通信を確認する」は正解になりますか？

①この答案自体は間違ってはいませんが，これは“ゆるい”答案なので正解にならなかったと考えます。設問では「確認の具体的な方法」が問われています。具体的に述べる設問において対象を絞り込めるケースでは，試験センターの解答例は絞り込んだ内容になっていることがほとんどです。そのため，L 社に割り当てられたグローバル IP アドレスが記録されるログは FW のログだけなので，対象を絞り込んで「FW のログ」と解答するのが確実です。ログ管理サーバには，FW のログの他に各サーバのアクセスログや操作ログなどが保持されているのため，「ログ管理サーバのログ」は“ゆるい”答案です。さらにゆるい答案は，単に「ログ」です。これまで正解にすると，何でも正解になってしまいます。

②正解になります。「FW のログ」という要点を含んでいるからです。「許可した」を追加した点も妥当なので OK です。

“NAT”や“NAPT”はマーキングしながら本文を読む。

この設問では，「プロキシサーバのログを確認する」という間違いが多いです。「FW が NAPT 機能を使用している」という本文の記述を読み落とさないことがポイントです。

(2) 空欄 a ～ c は，図 3（C&C サーバへの通信の送信元の調査結果）の記述の中にある。

空欄 a は，図 3 の 1. の「提供された送信元 IP アドレスは，L 社のネットワーク構成から分かるように，［ a ］のものであった」などの記述の中にある。提供された IP アドレスとは，〔情報漏えいインシデント〕に記述されているセキュリテ