Contents

◆1◆合格へのアプローチ

◆2◆午前問題の対策

◆3◆午後問題の対策

◆4◆巻末資料

第 1 章

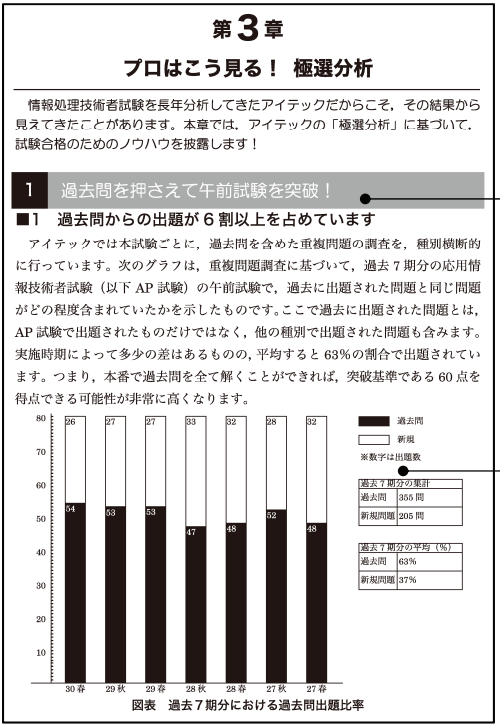
「極選分析 予想問題集」の特長・使い方

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，皆さま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，試験合格のためのノウハウを披露します！

1 過去問を押さえて午前試験を突破！

■1 過去問からの出題が 6 割以上を占めています

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，過去 7 期分の応用情報技術者試験（以下 AP 試験）の午前試験で，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。ここで過去に出題された問題とは，AP 試験で出題されたものだけではなく，他の種別で出題された問題も含みます。実施時期によって多少の差はあるものの，平均すると 63%の割合で出題されています。つまり，本番で過去問を全て解くことができれば，突破基準である 60 点を得点できる可能性が非常に高くなります。

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」，「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，午後それぞれに徹底的に分析しています。長年に渡る 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ています。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。

午後問題の分析表

過去 10 年間の本試験で出題された午後問題を，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。応用情報技術者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。

出題テーマ	出題回数	出題率（%）	H21 春	H21 秋	H22 春	H22 秋	H23 春	H23 秋	H24 春	H24 秋
① 攻撃手法，暗号化技術，認証技術など	5	26		○	○					
② ネットワークセキュリティ	4	21	○			○				
③ アプリケーションセキュリティ	2	11						○		
④ 情報セキュリティマネジメント	1	5							○	
⑤ 情報セキュリティ対策(マルウェア・不正アクセス対策)	7	37					○			○
① マーケティング	4	15	○			○				
② 事業・経営戦略，販売戦略，アウトソーシング戦略など	8	31				○	○	○	○	○

2　午前の演習問題と詳細解説

「◆2◆ 午前問題の対策」では，午前問題の過去問から，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が，午前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力を身に付けましょう。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。

演習問題

第 1 章

基礎理論

☆解答解説は p.55～

CHECK ☒☒☒

Q1　M/M/1 待ち行列モデルの条件

多数のクライアントが，LAN に接続された 1 台のプリンタを共同利用するときの印刷要求から印刷完了までの所要時間を，待ち行列理論を適用して見積もる

解答解説

A1　ィ

M/M/1 は，ケンドール記法の M/M/1(∞)で，(∞)を省略したものである。ケンドール記法では，「到着間隔の分布／サービス時間の分布／窓口の数（待ち行列の長さ）」のように表し，分布の M は指数分布を意味する。したがって，M/M/1(∞)は，到着間隔，サービス時間ともに指数分布（ランダムな状態）で，サービス窓口が一つのときの，待ち行列の長さに制限がない待ち行列モデルを表している。また，待ち行列は先入れ先出しであり，サービスが終了するまで待ち行列を離れ

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。

1章の掲載問題＆解答一覧

Q	難易度	問題区分	内　容	答	出題回数 全	出題回数 AP
1	☆☆☆☆	文	M/M/1 待ち行列モデルの条件	イ	6	3
2	☆☆☆☆	計	統合後の平均待ち時間を求める式	エ		2
3	☆☆☆	計	ハミング符号の誤りビット訂正	ア		5
4	☆☆☆	文	相関係数	ア		4
5	☆☆☆	計	負の整数の表現方法	エ		3
6	☆☆	考	集合	ア	5	5

掲載問題＆解答一覧

章末には，掲載問題の難易度・区分・タイトル・解答・出題回数（全種別）出題回数（AP）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，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

「◆3◆ 午後問題の対策」では，これまで（平成 21 年春以降）に出題された午後問題をテーマごとに分類しました。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

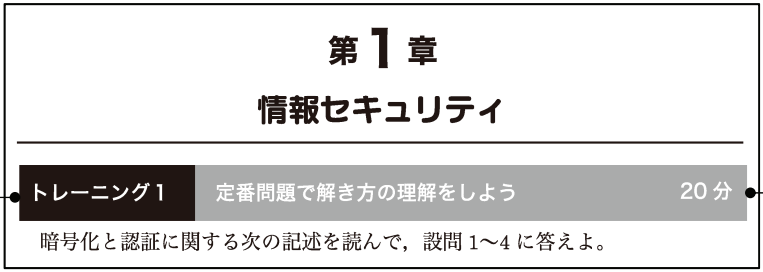
午後問題の問題リストを掲載しました。テーマごとにまとめた掲載問題について，「出題年度」，「試験区分」，「種別」，「時間区分」，「問題タイトル」，「解答目安時間」などを，問題を解く前に確認できます。苦手なテーマや知識分野の確認と克服に活用してください。

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 部								
第 1 章　情報セキュリティ								
1	2010 春	公開	AP	午後 I	9	暗号化と認証	20 分	
2	2014 春	公開	AP	午後 I	1	電子メールのセキュリティ対策	20 分	
3	2017 春	公開	AP	午後 I	1	サイバー攻撃への対策	20 分	
4	2012 秋	公開	AP	午後 I	9	リモートアクセスシステムの構築	20 分	
5	2015 秋	公開	AP	午後 I	1	セキュリティインシデント対応	20 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。



解答目安時間

問題を解くときには時間を測っておき，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。

各章のトレーニング 1 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 設問の特徴から以下のようにポイントを記しています。 「読み取り」：読んで答える（設問の内容から答える） 「読解」：読んだ上で基礎知識などを加味して答える 「解釈」：図表などの内容から結論を導き出す 「対比」：同じであるべきものを突き合わせて差異を見つける 「比較」：異なるものを比較して答える
注目！	問題を解くに当たって，追加で知っておくと役立つ知識
FAQ	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　テーマにあった問題で演習しよう　20分

電子メールのセキュリティ対策に関する次の記述を読んで，設問 1〜4 に答え

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をアップ！

解説 トレーニング1：暗号化と認証　(820391) ■公 10HAPP9

【解答例】

［設問1］ (a) 送信者 A の秘密鍵　(b) 送信者 A の公開鍵　(c) ハッシュ関数
(d) 共通鍵　(e) 公開鍵　(f) 有効期間
(g) PKI（又は，公開鍵基盤）

［設問2］ (h) オ　(i) ク　(j) イ　(k) キ

［設問3］ 暗号化だけでは，メッセージが改ざんされた場合，それを検出できないから。

［設問4］ 図 1 では，通信相手の認証はできるが，メッセージ認証ができない（又は，図 1 では，通信相手の認証はできるが，メッセージが改ざんされたときの検出ができない）。

【配点】

［設問1］	(a)〜(g)：1点×7
［設問2］	(h)〜(k)：1点×4

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。

第1章　情報セキュリティ　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 暗号化と認証	分 ／20分	点 ／16点	□OK □もう一度解く □試験直前に最終確認	分 ／20分	点 ／16点

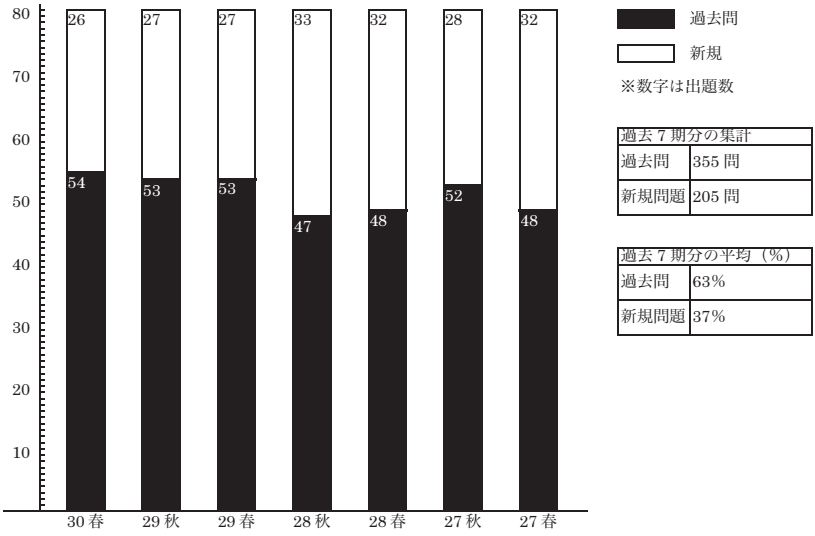
第3章
プロはこう見る！ 極選分析

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，試験合格のためのノウハウを披露します！

1　過去問を押さえて午前試験を突破！

■1　過去問からの出題が 6 割以上を占めています

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，過去 7 期分の応用情報技術者試験（以下 AP 試験）の午前試験で，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。ここで過去に出題された問題とは，AP 試験で出題されたものだけではなく，他の種別で出題された問題も含みます。実施時期によって多少の差はあるものの，平均すると 63%の割合で出題されています。つまり，本番で過去問を全て解くことができれば，突破基準である 60 点を得点できる可能性が非常に高くなります。



過去 7 期分の集計	
過去問	355 問
新規問題	205 問

過去 7 期分の平均（%）	
過去問	63%
新規問題	37%

図表　過去 7 期分における過去問出題比率

書籍をご購入いただいた方限定!

ダウンロードコンテンツ

②学習に役立つコンテンツ

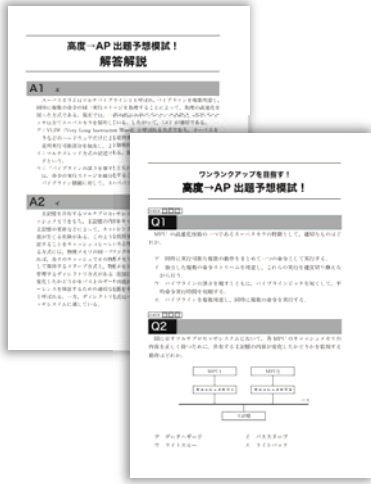
◎「ワンランクアップを目指す！
高度→ＡＰ出題予想模試！」
（PDF ファイル）

「第３章　プロはこう見る！ 極選分析」でご紹介したとおり，AP 試験の午前問題では，高度系種別の過去問題が出題されることもあります。

そこで，高度系の過去問題で，今後 AP 試験に流用される可能性が高い問題を予想し，問題・解説を提供しています。出題問題の分野は，本試験の出題比率に準拠していますので（※），模擬試験形式での演習も可能です。

本書掲載の AP の過去問を一通り解いた後は，得点力アップのために，こちらにもチャレンジしてみましょう。

※ 高度試験で出題されない，基礎理論，アルゴリズム，ヒューマンインタフェース，マルチメディアの分野の問題は掲載していません。



第3章
データベース

☆解答解説は p.186〜

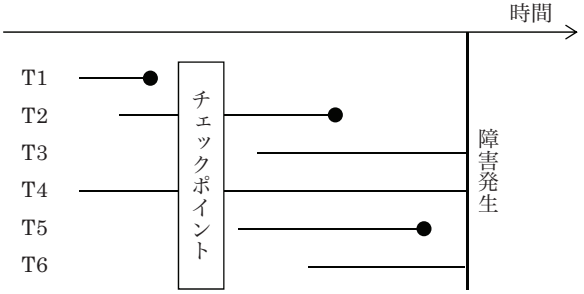
CHECK ☒☒☒

Q1 障害発生後の DBMS 再立上げ復帰方法

DBMS をシステム障害発生後に再立上げするとき，ロールフォワードすべきトランザクションとロールバックすべきトランザクションの組合せとして，適切なものはどれか。ここで，トランザクションの中で実行される処理内容は次のとおりとする。

(H28 秋-AP 問 30)

トランザクション	データベースに対する Read 回数と Write 回数
T1，T2	Read 10，Write 20
T3，T4	Read 100
T5，T6	Read 20，Write 10



―― はコミットされていないトランザクションを示す。
――● はコミットされたトランザクションを示す。

	ロールフォワード	ロールバック
ア	T2，T5	T6
イ	T2，T5	T3，T6
ウ	T1，T2，T5	T6
エ	T1，T2，T5	T3，T6

解答解説

A1 ア

データベースの障害が発生した場合，再立上げするとき，データの整合性が取れた状態に復旧する必要がある。このために，ロールフォワード（前進復帰）とロールバック（後退復帰）という方法が使用される。そして，システム障害時の回復時間を短縮する目的で，主記憶上にあるデータベースの更新内容をディスクに書き込むチェックポイント法を併用するのが一般的である。システム障害時に障害発生時刻から最新のチェックポイントまで戻れば，それ以前はディスクへの書込みが終了しているからである。なお，チェックポイントとは，データベースの更新性能を向上させるために，更新内容をバッファ上に記録しておき，周期的に一括して書き込む手法，及び，そのタイミングのことであり，最新のチェックポイントまでは，データベースの更新内容が確定されている。

ロールフォワードでは，障害発生以前にコミットされたトランザクションに対して，その処理を完了させるために，チェックポイント時点の情報とログファイルの更新後情報を使って，データベースの内容を更新する。問題の図のトランザクションでは，T2 と T5 が対象になる。一方，ロールバックでは，障害発生時にコミットされていないトランザクションに対し，ログファイルの更新前情報を使って，データベースの内容をトランザクションの実行前の状態に戻す。図のトランザクションでは，T3，T4，T6 が該当する。しかし，問題の表からトランザクションの中で実行される処理内容を確認すると，T3 と T4 はデータベースに対して Read しか行っていない。つまり，データベースの内容を更新していないので，ロールバックの対象にはならない。したがって，（ア）が適切な組合せである。

なお，T1 はチェックポイント前にコミットされているので，回復処理の対象にはならない。

A2 エ

データマイニングとは，大量に蓄積された生データから特徴のあるパターンを見つけ出し，そのパターンから有用となる一定の規則（ルール）を導き出す発見的手法である。そして，その発見のためにニューラルネットワークや統計解析などの手法が使用されるので，（エ）が適切である。なお，ニューラルネットワークとは，動物の神経細胞（ニューロン）の機能の一部の特性をモデル化し，コンピュータ上で表現したものである。

ア：一般のデータウェアハウスについての説明である。

イ：分析者すなわちエンドユーザの目的別に切り出されたデータ，つまりデータ

5章の掲載問題＆解答一覧

Q	難易度	問題区分	内　容	答	出題回数	
					全	AP
1	☆☆	計	パスワードの総数を求める数式	ア	9	5
2	☆☆	文	暗号方式の説明	ア	8	3
3	☆☆	文	暗号方式に関する記述	イ	7	2
4	☆☆☆	計	公開鍵暗号方式の鍵の総数	イ		4
5	☆☆	文	ディジタル署名における署名鍵の用い方と目的	ウ		1
6	☆☆	文	公開鍵暗号方式	イ		3
7	☆☆☆	文	ISMS適合性評価制度の情報セキュリティ基本方針	ウ	6	5
8	☆☆☆☆	文	シングルサインオンの説明	エ		1
9	☆☆☆	文	DNS キャッシュポイズニング攻撃で起こる現象	エ	5	3
10	☆☆☆	文	認証局の公開鍵を利用する目的	ウ		2
11	☆☆☆	文	ブルートフォース攻撃に該当するもの	イ		2
12	☆☆	用	ハッシュ値のディジタル署名	エ		2
13	☆☆☆	用	JIS Q 27001 の情報セキュリティ特性	イ		1
14	☆☆	用	人為的な機密情報の不正入手行為	ア		2
15	☆☆☆	文	パケットフィルタリング型ファイアウォールで防げるもの	ア	4	3
16	☆☆☆	文	クロスサイトスクリプティングの手口	ア		2
17	☆☆☆	文	CRL に関する記述	イ		1
18	☆☆☆	用	暗号化や認証機能をもつ遠隔操作プロトコル	ウ		2
19	☆☆☆	文	チャレンジレスポンス認証方式	エ		2
20	☆☆☆	用	共通鍵暗号方式の説明	ア		1
21	☆☆☆	文	DNS キャッシュポイズニング	イ		2
22	☆☆	用	素因数分解の困難性を利用した公開鍵暗号方式	エ		1
23	☆☆☆☆	文	LAN アナライザの運用時の留意点	イ		2
24	☆☆	文	電子商取引における認証局の役割	ア		1
25	☆☆☆	文	SAML の説明	エ		3
26	☆☆	文	コンピュータ犯罪手口のサラミ法	ウ		1
27	☆☆☆	文	電子メールの内容を暗号化するのに使用するかぎ	ウ		1

・星の数は難易度を表しています。（例：☆ 易 ＜ 難 ☆☆☆☆）
・区分は，問題を計＝計算，用＝用語，文＝文章，考＝考察として，出題タイプ別に分類しています。
・出題回数のうち，「全」は，全種別における過去出題回数を，「AP」は，AP 試験（旧 SW 試験含む）の出題回数を示します。

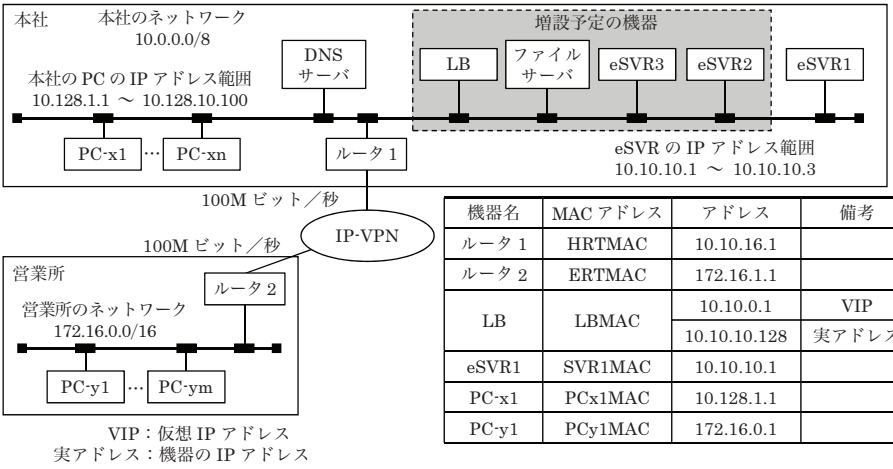
第4章
ネットワーク

トレーニング1　定番問題で解き方の理解をしよう　20分

ネットワークシステムの増強に関する次の記述を読んで，設問1〜3に答えよ。

(822486)

H社では，社員の業務スキル向上のために，PCのブラウザからHTTPによって利用できるeラーニングシステム（以下，eシステムという）を導入して，一部の部署で利用してきた。その結果，eシステムによる学習効果が高いことが分かったので，研修コースを拡充して全社に展開することにした。この全社展開によってeシステムの利用者数が大幅に増加することになるので，これまで1台であったeシステムのサーバ（以下，eSVRという）を複数台にして，負荷分散装置（以下，LBという）でアクセスを振り分ける構成に変更することにした。H社のネットワーク構成を，図1に示す。なお，本社と営業所のネットワークのIPアドレスは，［　a　］を設定せず，それぞれクラスAとクラスBを用いている。



機器名	MACアドレス	アドレス	備考
ルータ1	HRTMAC	10.10.16.1	
ルータ2	ERTMAC	172.16.1.1	
LB	LBMAC	10.10.0.1	VIP
		10.10.10.128	実アドレス
eSVR1	SVR1MAC	10.10.10.1	
PC-x1	PCx1MAC	10.128.1.1	
PC-y1	PCy1MAC	172.16.0.1	

注記　LBの実アドレスは，ソースNAT機能を使用する場合に限り使用される。

図1　H社のネットワーク構成（抜粋）

解答解説

解説 トレーニング１：ネットワークシステムの増強

(822486)
■公 18HAPP5

【解答例】

［設問１］ a：ク　b：ウ　c：オ　d：キ

［設問２］ (1) ウ
(2) 三つのホスト名に対して，それぞれのサーバの IP アドレスを設定する。

［設問３］ (1) e：HRTMAC　f：LBMAC　g：SVR1MAC　h：172.16.0.1
(2) 変更前：ルータ１
変更後：LB

【配点】

［設問１］	(a)～(d)：１点×４
［設問２］	(1) ２点，(2) ３点
［設問３］	(1) (e)～(h)：２点×４，(2) ３点（完答）※但しいずれか一方のみ正解は，１点

【解説】

本問は，サーバに対する負荷分散の方法を IP アドレスの観点から考えるものである。具体的には，TCP/IP 通信の基本動作，MAC アドレスと IP アドレスとの関係，LB による処理の振分けで発生する問題などが問われている。正解を導くためには，ネットワークに関する基本的な知識をベースにしながら，論理的に矛盾がないように考えていくことが必要である。

［設問１］ **ココ**が要点 TCP/IP 通信に関する基本用語の知識

空欄 a は，「本社と営業所のネットワークの IP アドレスは，［ a ］を設定せず，それぞれクラス A とクラス B を用いている」という記述の中にある。図１の H 社のネットワーク構成（抜粋）を見ると，本社のネットワークには“10.0.0.0/8”が，営業所のネットワークには“172.16.0.0/16”が割り当てられている。“/8”，“/16”は，CIDR（Classless Inter-Domain Routing）表記であり，ネットワークアドレス部がそれぞれ８ビット，16 ビットであることを示す。ネットワークアドレス部が８ビット，16 ビットということは，本社，営業所のネットワークアドレスは，サブネットに分割せずにクラス A，クラス B のままで使用していることになる。したがって，空欄 a にはサブネット（ク）が入る。

CIDR の Classless（クラスレス）が意味するもの

CIDR の C は Classless なので，CIDR は A，B，C のクラス分けをしない，もしくはクラスの概念のない IP アドレスと覚えてしまいがちです。そうすると，“/8”や“/16”などクラスを意味する表記に違和感をもってしまいます。サブネットは，インターネット上で一つとして扱われるネットワークを内部的に複数のネットワークに分割したものですから，分割した個々のネットワークを識別する情報（サブネットアドレス部）だけでなく，インターネット上でネットワークを識別する情報（ネットワークアドレス部）ももっています。クラスがないわけではなく，先頭から 8，16，24 ビットにとらわれずにネットワークを識別するものと理解しておきましょう。そうすれば，“/8”は先頭からの 8 ビットでそのネットワークを識別することができる IP アドレスであり，クラス A，“/20”は 8 で割り切れないのでサブネットをもつネットワークの IP アドレスと解釈することができます。

サブネットアドレス部とサブネットアドレスの違いを教えてください

CIDR は，その IP アドレスのどこまでがサブネットアドレスかを示すための表記です。“/”の後ろの数字がサブネットアドレスの長さを示しています。下図は，サブネットアドレスを使った IP アドレスの構成です。この図の「組織内ネットワークでの中継」に該当する部分がサブネットアドレスで，分割された個々のネットワークを表します。

サブネットアドレス部は，本来のホストアドレス部の一部で，サブネットを識別するための情報です。例えば，A 社のネットワークには，内部的に技術部と営業部の二つのネットワークがあるとします。この場合，技術部の端末の IP アドレスでは，ネットワークアドレス部が A 社，サブネットアドレス部が技術部を表します。そして，サブネットアドレスは A 社＋技術部となり，技術部のネットワークを表します。同様に，営業部の端末では，ネットワークアドレス部は A 社ですが，サブネットアドレス部は営業部，サブネットアドレスは A 社＋営業部となり，営業部のネットワークを表します。

第 1 章　情報セキュリティ　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 暗号化と認証	分 ／ 20分	点 ／ 16点	□OK □もう一度解く □試験直前に最終確認	分 ／ 20分	点 ／ 16点
トレーニング 2 電子メールのセキュリティ対策	分 ／ 20分	点 ／ 16点	□OK □もう一度解く □試験直前に最終確認	分 ／ 20分	点 ／ 16点
トレーニング 3 サイバー攻撃への対策	分 ／ 20分	点 ／ 20点	□OK □もう一度解く □試験直前に最終確認	分 ／ 20分	点 ／ 20点
トレーニング 4 リモートアクセスシステムの構築	分 ／ 20分	点 ／ 16点	□OK □もう一度解く □試験直前に最終確認	分 ／ 20分	点 ／ 16点
トレーニング 5 セキュリティインシデント対応	分 ／ 20分	点 ／ 20点	□OK □もう一度解く □試験直前に最終確認	分 ／ 20分	点 ／ 20点