極選分析 応用情報技術者 予想問題集

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

ここが役立つ！　本書の特長

本書は，

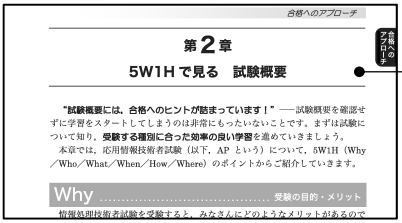
①プロが本試験を分析した結果に基づいて，予想した問題を掲載

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，学習者のみなさん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


合格へのアプローチ

第2章

5W1H で見る　試験概要

"試験概要には，合格へのヒントが詰まっています！"――試験概要を確認せずに学習をスタートしてしまうのは非常にもったいないことです。まずは試験について知り，**受験する種別に合った効率の良い学習**を進めていきましょう。

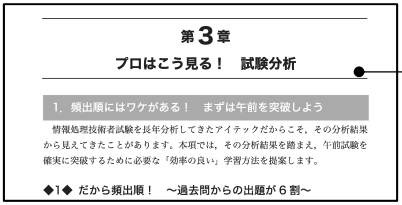
本章では，応用情報技術者試験（以下，AP という）について，5W1H（Why／Who,／What,／When,／How,／Where）のポイントからご紹介していきます。

Why …… 受験の目的・メリット

情報処理技術者試験を受験すると，みなさんにどのようなメリットがあるので

5W1H で見る　試験概要

試験概要のうち，AP 学習者にとって必要な情報を 5W1H の切り口で紹介しています。


第3章

プロはこう見る！　試験分析

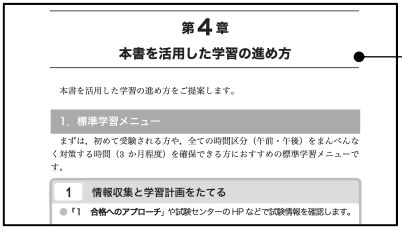
1．頻出順にはワケがある！　まずは午前を突破しよう

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。

◆1◆ だから頻出順！　～過去問からの出題が 6 割～

プロはこう見る！　試験分析

過去の本試験を徹底的に分析し，“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・午後）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習メニューです。

1　情報収集と学習計画をたてる

●「1　合格へのアプローチ」や試験センターの HP などで試験情報を確認します。

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. 午前問題の対策

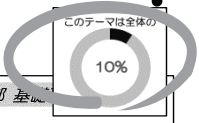
午前出題の６割を占める過去問題を頻出順に掲載

繰返し学習に役立つ“Check ボックス”

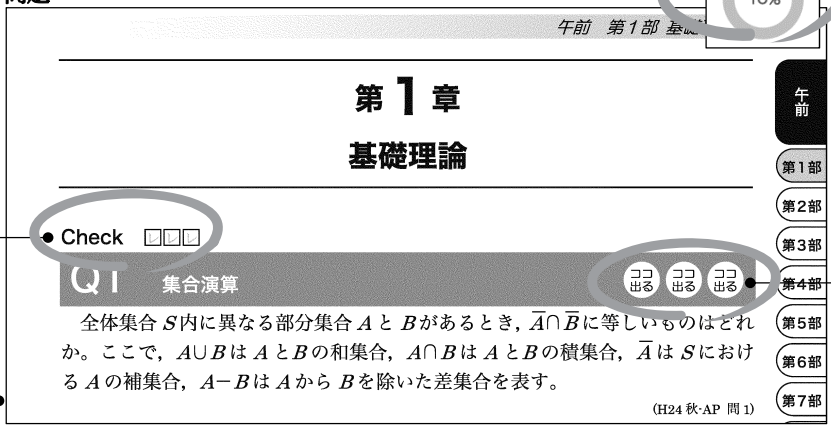
解いた問題にチェックを付けながら進めることで，後でどの問題を復習すればよいかの目安にもなります。

分野の出題割合

各分野の扉の円グラフは，午前問題におけるその分野の出題率を示しています。



問題



解答解説は章末に掲載

問題を解いたら，章末の解答・解説で理解を深めましょう。

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

A1 ア

差集合 $X-Y$ とは，X に含まれ，かつ Y に含まれない部分のことなので，$X-Y=X\cap\overline{Y}$ と表せる。この問題で問われている $\overline{A}-B$ は，$\overline{A}$（図 1）と B との差集合なので，$\overline{A}$ と $\overline{B}$（図 2）を使って $\overline{A}\cap\overline{B}$ と表すことができ，ベン図を使って表現すると図 3 のようになる。したがって，（ア）が正解である。

なお，（イ）～（エ）はベン図で表すと，すべて図 4 のようになる。

イ：$(\overline{A}\cup\overline{B})-(A\cap B)=S-(A\cap B)-(A\cap B)=S-(A\cap B)$　（エと同じ）

ウ：$(S-A)\cup(S-B)=S-(A\cap B)$　（分配の法則）（エと同じ）

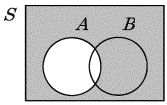


図 1　$\overline{A}$

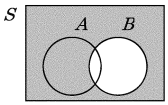
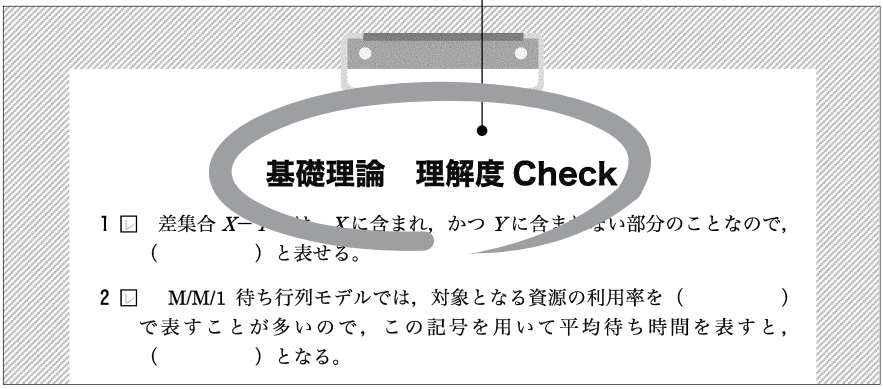


図 2　$\overline{B}$

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。



基礎理論　理解度 Check

1 □　差集合 $X-Y$ は，Xに含まれ，かつ Yに含まない部分のことなので，
（　　）と表せる。

2 □　M/M/1 待ち行列モデルでは，対象となる資源の利用率を（　　）で表すことが多いので，この記号を用いて平均待ち時間を表すと，
（　　）となる。

午前掲載問題＆解答一覧

Q	難易度	区分	内容	答	回数
1	★★	計	論理演算	ア	5
2	★★★	計	ハミング符号	ア	4
3	★★★★	文	M/M/1 待ち行列モデルの条件	イ	3
4	★★	計	定義式と等しい式	ア	
5	★★	考	パリティビットの付加で訂正できるビット数	ア	
6	★★★★	考	カルノー図と等価な論理式	エ	
7	★★★★	計	平均待ち時間が平均処理時間以上となる利用率	イ	
8	★★★	考	有限オートマトンの受理状態	ウ	
9	★★★★	考	含意を含む論理式	エ	
10	★★★	計	待ち行列モデルにおける回線利用率の計算	イ	

午前掲載問題＆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。
自身の苦手な問題の傾向を分析するのに使えます。

3．午後問題の対策

各テーマの定番問題・
演習問題で実力アップ

ー分析ー

午後問題のテーマと出題傾向

1．午後問題のテーマ

午後問題は，IPA 発表の「試験要綱」に基づき，次のカテゴリに分けられます。

設問番号	出題分野	出題テーマ
必須問1	情報セキュリティ	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，リスク分析，データベースセキュリティ，ネットワークセキュリティ，アプリケーションセキュリティ，物理的セキュリティ，アクセス管理，暗号・認証，PKI，ファイアウォール，マルウェア対策（コンピュータウイルス，ボット，スパイウェアほか），不正アクセス対策，個人情報保護
	経営戦略	マーケティング，経営分析，事業戦略・企業戦略，コーポレートファイナンス・事業価値評価，事業継続計画（BCP），会計・財務，リーダシップ論

午後試験テーマ別出題分析表　（H21 春～H28 春）

設問番号	出題分野	出題テーマ	総出題回数	次回予想	H21 春	H21 秋	H22 春	H22 秋	H23 春	H23 秋	H24 春	H24 秋	H25 春	H25 秋	H26 春	H26 秋	H27 春	H27 秋	H28 春
必須問1	情報セキュリティ	① 攻撃手法，暗号化技術，認証技術など	3	23	○	○											○		
		② ネットワークセキュリティ	4	31	○			○							○	○			
		③ アプリケーションセキュリティ	2	15						○				○					
		④ 情報セキュリティマネジメント	1	8								○							
		⑤ 情報セキュリティ対策(マルウェア・不正アクセス対策)	3	23						○			○	○				○	○
	経営・情報戦略，戦略立案，コンサルティング技法	① マーケティング	3	15	○			○									○		
		② 事業・経営戦略，販売戦略，アウトソーシング戦略など	6	30				○	○	○	○	○2	○	○					
		③ 事業継続計画（BCP）	2	10						○									○
		④ 会計・財務，原価計算，キャッシュフロー分析	3	15		○2	○									○		○	
		⑤ 分析技法（バランススコアカード・SWOT 分析など）	3	15	○			○							○				
		⑥ その他(業務改善，ビジネスモデル，EA など)	3	15							○		○	○					

午後問題のテーマ

午後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

午後問題の出題テーマと，その中から重点的に出題されるテーマが分かります。

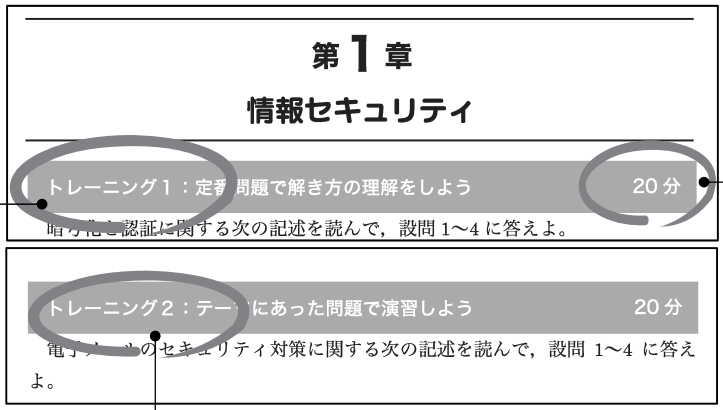
問題：トレーニング 1

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

トレーニング 1：定番問題で解き方の理解をしよう　20 分

暗号化と認証に関する次の記述を読んで，設問 1～4 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　20 分

電子データ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：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）

【配点】

［設問１］	(a)～(g)：１点×７
［設問２］	(h)～(k)：１点×４
［設問３］	３点
［設問４］	２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。

追加で知っておくと役立つ知識

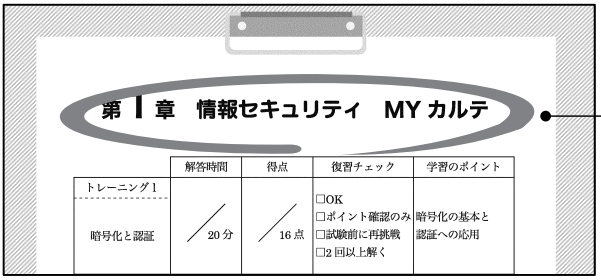
設問で問われている出題テーマ

［設問１］　出題テーマ　情報システム戦略の把握

情報システム戦略との整合性

注目！

企画プロセスでは，情報システム戦略や全体システム化計画を踏まえて，IT ストラジスト，プロジェクトマネージャ，システムアーキテクトなどが，システム開発を企画します。システム開発を企画する上で重要な点は，情報システム戦略との整合性です。



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
基礎理論

Check □□□

Q1 集合演算

ココ出る ココ出る ココ出る

全体集合 S 内に異なる部分集合 A と B があるとき，$\overline{A}\cap\overline{B}$ に等しいものはどれか。ここで，$A\cup B$ は A と B の和集合，$A\cap B$ は A と B の積集合，$\overline{A}$ は S における A の補集合，$A-B$ は A から B を除いた差集合を表す。

(H24 秋-AP 問 1)

ア $\overline{A}-B$　　イ $(\overline{A}\cup\overline{B})-(A\cap B)$

ウ $(S-A)\cup(S-B)$　　エ $S-(A\cap B)$

Check □□□

Q2 ハミング符号

ココ出る ココ出る ココ出る

ハミング符号とは，データに冗長ビットを付加して，1 ビットの誤りを訂正できるようにしたものである。ここでは，X_1，X_2，X_3，X_4 の 4 ビットから成るデータに，3 ビットの冗長ビット P_3，P_2，P_1 を付加したハミング符号 $X_1X_2X_3P_3X_4P_2P_1$ を考える。付加ビット P_1，P_2，P_3 は，それぞれ

$X_1\oplus X_3\oplus X_4\oplus P_1=0$

$X_1\oplus X_2\oplus X_4\oplus P_2=0$

$X_1\oplus X_2\oplus X_3\oplus P_3=0$

となるように決める。ここで，$\oplus$ は排他的論理和を表す。

ハミング符号 1110011 には 1 ビットの誤りが存在する。誤りビットを訂正したハミング符号はどれか。

(H25 春-AP 問 4)

ア 0110011　　イ 1010011　　ウ 1100011　　エ 1110111

解答解説

A1　ア

差集合 $X-Y$とは，Xに含まれ，かつ Yに含まれない部分のことなので，$X-Y=X \cap \overline{Y}$と表せる。この問題で問われている$\overline{A}-B$は，$\overline{A}$（図 1）と Bとの差集合なので，$\overline{A}$と $\overline{B}$（図 2）を使って$\overline{A} \cap \overline{B}$と表すことができ，ベン図を使って表現すると図 3 のようになる。したがって，（ア）が正解である。

なお，（イ）～（エ）はベン図で表すと，すべて図 4 のようになる。

イ：$(\overline{A} \cup \overline{B})-(A \cap B)=S-(A \cap B)-(A \cap B)=S-(A \cap B)$　（エと同じ）

ウ：$(S-A) \cup (S-B)=S-(A \cap B)$　（分配の法則）（エと同じ）

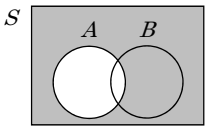


図 1　$\overline{A}$

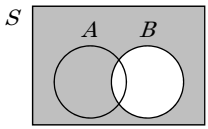


図 2　$\overline{B}$

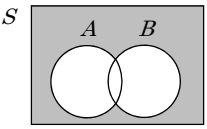


図 3　$\overline{A} \cap \overline{B}$

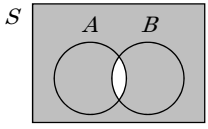


図 4　S－(A∩B)

A2　ア

ハミング符号 1110011 から，情報ビット，冗長ビットは次のようになる。

$X_1=1$，$X_2=1$，$X_3=1$，$X_4=0$，$P_1=1$，$P_2=1$，$P_3=0$

これらを与えられた式に当てはめる。

$X_1 \oplus X_3 \oplus X_4 \oplus P_1 = 1 \oplus 1 \oplus 0 \oplus 1 = 1$

$X_1 \oplus X_2 \oplus X_4 \oplus P_2 = 1 \oplus 1 \oplus 0 \oplus 1 = 1$

$X_1 \oplus X_2 \oplus X_3 \oplus P_3 = 1 \oplus 1 \oplus 1 \oplus 0 = 1$

誤りがなければ，全ての式が 0 になるが，誤りビットを含んでいる式は 1 になる。したがって，三つの式ともに誤りビットを含んでいることを示している。この三つの式に共通して含まれているのは X_1だけであるから，誤りは X_1であることが分かる。これを訂正すると，正しいハミング符号は，0110011 となり，（ア）が正解となる。

基礎理論　理解度 Check

1 □ 差集合 $X-Y$ とは，X に含まれ，かつ Y に含まれない部分のことなので，（　　）と表せる。

2 □ M/M/1 待ち行列モデルでは，対象となる資源の利用率を（　　）で表すことが多いので，この記号を用いて平均待ち時間を表すと，（　　）となる。

3 □ 入力した値だけではなく，それ以前の状態にも影響されて動作する機械を（　　）という。更に，有限の状態をもち，（　　）と（　　）から，（　　）と次の状態を決めて動作するオートマトンを有限オートマトンという。

4 □ 逆ポーランド表記法で表現された数式は，数式を左から順に参照し，演算数なら（　　）※にプッシュする。また，演算子なら（　　）※のトップにある二つの演算数を（　　）して演算し，結果を（　　）※にプッシュするという簡単な方法で処理できる。

※の空欄には同じ値が入る。

5 □ 二つの対応する特性 x，y をもつデータについて相関関係を調べるとき，（　　）を用いることが多いが，相関係数が 1 に近いときは二つの関係には（　　）があるという。

6 □ アナログ信号をパルス信号に変換して伝送する方式を（　　）伝送方式という。

7 □ 桁落ちによる誤差とは，値のほぼ等しい二つの数値の差を求めたときに，有効桁数が（　　）ことによって発生する誤差である。

【解答】
1. $X \cap \overline{Y}$（→Q1） 2. ρ，ρ／(1－ρ)×T(平均処理時間)（→Q7） 3. オートマトン，現在の状態，入力値，出力値（→Q8）4. スタック※，ポップ（→Q12）5. 散布図，正の相関（→Q13）6. PCM（→Q14）7. 減る（→Q18）

2．テーマ別の傾向と分析

本書に掲載する予想問題の選定に当たって，平成 21 年春期から平成 28 年春期までの本試験の出題実績を集計，分析し，出題実績が多いテーマが類似する問題を選定しました。オリジナル問題，本試験問題からも選定をすることで，出題頻度の高いテーマの問題を幅広くカバーしています。

午後試験テーマ別出題分析表　（H21 春～H28 春）

設問番号	出題分野	出題テーマ	出題回数	出題率（%）	年度															
					H21		H22		H23		H24		H25		H26		H27		H28	
					春	秋	春	秋	春	秋	春	秋	春	秋	春	秋	春	秋	春	
必須問1	情報セキュリティ	① 攻撃手法，暗号化技術，認証技術など	3	23		○	○										○			
		② ネットワークセキュリティ	4	31	○			○							○	○				
		③ アプリケーションセキュリティ	2	15						○				○						
		④ 情報セキュリティマネジメント	1	8							○									
		⑤ 情報セキュリティ対策(マルウェア･不正アクセス対策)	3	23					○			○	○					○	○	
選択問2～問11	経営・情報戦略，戦略立案，コンサルティング技法	① マーケティング	3	15	○			○									○			
		② 事業・経営戦略，販売戦略，アウトソーシング戦略など	6	30				○	○	○	○2	○	○	○						
		③ 事業継続計画（BCP）	2	10					○											○
		④ 会計・財務，原価計算，キャッシュフロー分析	3	15		○2	○									○		○		
		⑤ 分析技法（バランススコアカード･SWOT 分析など）	3	15	○		○								○					
		⑥ その他(業務改善，ビジネスモデル，EA など)	3	15						○		○	○							
	プログラミング	① 探索アルゴリズム	3	21	○							○						○		
		② 文字列照合・圧縮アルゴリズム	2	14		○					○									
		③ その他アルゴリズム（ソート，再帰など）	5	36				○		○					○	○	○			○
		④ データ構造	3	21			○						○	○						
		⑤ プログラム・マークアップ言語	1	7					○											
	システムアーキテクチャ	① 信頼性・性能(復旧対策)，キャパシティプランニング	8	53	○	○		○				○	○		○	○				○
		② 仮想化技術	3	20						○				○			○			
		③ 要件定義・要求分析，提案依頼書など	3	20					○		○							○		
		④ 待ち行列モデル，負荷分散など	1	7			○													
	ネットワーク	① プロトコルとインタフェース	5	36	○								○	○	○	○				
		② ネットワーク方式（インターネット技術，有線・無線 LAN など）	5	36				○	○	○							○			○
		③ 通信トラフィック，負荷分散など	2	14							○	○						○		
		④ ネットワーク応用（VPN,モバイル通信，エクストラネットなど）	2	14		○	○													
	データベース	① データベース言語（SQL），データベース操作	10	67	○		○	○	○	○	○		○	○			○			○
		② 正規化・スキーマ設計，データベース設計	2	17		○						○						○		
		③ トランザクション処理（排他制御など）	2	17											○	○				

第1章
情報セキュリティ

トレーニング1：定番問題で解き方の理解をしよう　20分

暗号化と認証に関する次の記述を読んで，設問1〜4に答えよ。

(820391)

X社では，インターネット経由で取引先と電子メールやデータ（以下，メッセージという）の交換を行っている。インターネット経由でメッセージの交換を行う場合，メッセージの本文を暗号化するだけではセキュリティ面で安全とは言えない。例えば，メッセージの交換相手の認証も行う必要がある。なお，相手の認証を行うにあたって，暗号化と復号を同一の鍵（共通鍵）で行う秘密鍵方式ではなく，暗号化と復号を各個人が所有する秘密鍵と公開鍵とで行う公開鍵方式の暗号化アルゴリズムを採用している。公開鍵方式を使って受信者Bが送信者Aの認証を行う場合の手順を図1に示す。

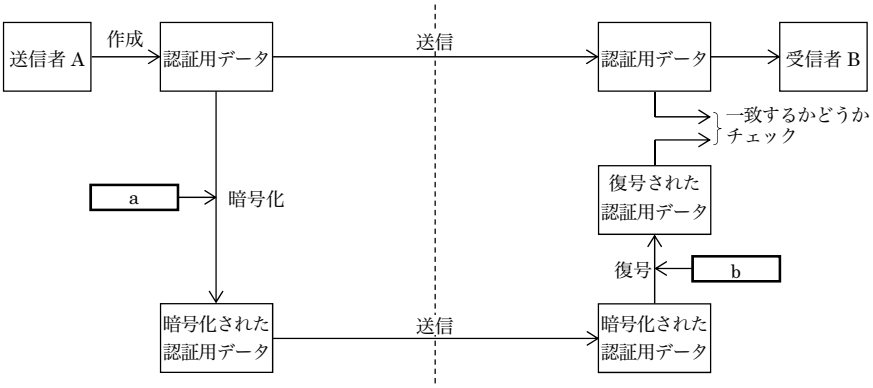


図1　公開鍵方式による認証の手順

図1の手順を応用して認証を可能にしたメッセージ送受信の手順を図2に示す。図2の［　a　］，［　b　］には，それぞれ図1の［　a　］，［　b　］と同じ字句が入る。

解答解説

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
［設問3］	3点
［設問4］	2点

【解説】

公開鍵暗号方式を使ってディジタル署名を実現するときの基本的な仕組みや，共通鍵暗号方式と公開鍵暗号方式に関する技術的な知識を問う問題である。暗号化については，情報セキュリティ分野で最もよく出題される内容なので，しっかり理解しておく必要がある。特に，公開鍵暗号方式は，情報セキュリティの根幹となるPKI（Public Key Infrastructure；公開鍵基盤）を実現するために利用されているので，その仕組みについて十分に理解しておくとよいでしょう。

［設問1］　出題テーマ｜公開鍵暗号方式

問題文の記述内容と図を見比べながら，“暗号化”，“復号”，“生成”というキーワードに着目して考えていきます。また，公開鍵暗号方式の場合，送信者，受信者ともに公開鍵，秘密鍵をもっている可能性があるので，どちらのものなのかを区別する必要があります。

図1は，公開鍵暗号方式を使って受信者Bが送信者Aの認証を行う手順を示したものである。送信者Aが認証用データを暗号化するためには，確かにA自身が行ったこ

とを証明する必要があるので，A しか所有していない秘密鍵を使用する。このため，空欄 a には“送信者 A の秘密鍵”が入る。公開鍵暗号方式において，秘密鍵で暗号化したものを復号するときには，秘密鍵に対応する公開鍵でしか復号できない。このため，空欄 b には“送信者 A の公開鍵”が入る。

公開鍵と共通鍵の違い

公開鍵暗号方式に関する学習の導入では，共通鍵暗号方式との違いに注目して，受信者の公開鍵で暗号化して送り，受信者は自身の秘密鍵で復号するという説明がほとんどです。このために，認証では鍵の使い方が逆になることに，疑問を感じる方が多いようです。公開鍵は暗号用，秘密鍵は復号用という理解ではなく，一方の鍵で暗号化した内容を，もう一方の鍵で復号できるのが公開鍵暗号方式であるというように理解しましょう。

暗号文による通信では，第三者に復号されて中身を知られてしまうことが問題なので，受信者だけにしか復号できないように，復号のために受信者の秘密鍵を使います。一方，認証の目的は，本人だけにしかできないことを示すことですから，本人しか持っていない秘密鍵で暗号化して，本人であることを示します。

空欄 c は，問題文の(2)の「認証を行うために，A と B とで共有している [c] を用いて，A はメッセージダイジェストを生成し，……」という記述の中にある。メッセージダイジェスト（ハッシュ値）を生成するには，一般にハッシュ関数が使用される。したがって，空欄 c には“ハッシュ関数”が入る。

ハッシュ関数の種類の違いを教えてください

以前は，ハッシュ関数としては MD5（Message Digest Algorithm 5）や SHA-1（Secure Hash Algorithm 1）がよく利用されていました。MD5 は，任意のメッセージを圧縮し 128 ビットのハッシュ値を生成し，SHA-1 は 160 ビットのハッシュ値を生成します。しかし，これらのハッシュ関数に対する脆弱性が指摘されるようになったので，最近では SHA-2（Secure Hash Algorithm 2）の利用が推奨されています。なお，SHA-2 では 256 ビットのほか，384 ビット，512 ビットなどのハッシュ値を生成することができます。

空欄 d は，(1)に「送信者 A は，メッセージ本文を，A と受信者 B が共有している共通鍵を使って，秘密鍵方式で暗号化して B へ送る」，(3)に「更に，メッセージ本文を共通鍵で復号し，……」と記述されている。したがって，空欄 d には“共通鍵”が