応用情報技術者

科目B対策問題集

無料体験入学者用

Ver.1.1

TAC

はじめに

この問題集は, 弊社刊「応用情報技術者試験対策テキストⅠ・Ⅱ・Ⅲ」の各学習項目に対応させて作成された問題集です。応用情報技術者試験の科目Ｂ試験出題範囲である各分野(テクノロジ系, マネジメント系, ストラテジ系)の問題を，広く多数掲載しています。

本書は，過去の情報処理技術者試験において出題された午後試験(科目Ｂ試験の前身)の問題で構成されています。実際の応用情報技術者試験の出題形式に合わせ，テーマごとに問題を集めて掲載しています(出典は目次の後)。

試験に合格するためには，テキストによる知識のインプットだけではなく, 問題演習によるアウトプット(力試し)が非常に重要になります。問題を解き，間違えた問題のジャンルについては学習しなおして再度挑戦するという学習サイクルを身に付けましょう。

本書が，応用情報技術者試験の合格のお役に立てることを願ってやみません。

TAC情報処理講座

目　次

出典一覧

第1章　プログラミング

問1	令和3年秋期本試験	問3
問2	令和元年秋期本試験	問3
問3	令和2年本試験	問3
問4	令和5年秋期本試験	問3

第2章　システムアーキテクチャ

問1	令和3年秋期本試験	問4
問2	平成31年春期本試験	問4
問3	令和6年春期本試験	問4
問4	令和4年秋本試験	問4

第3章　データベース

問1	平成30年春期本試験	問6
問2	令和6年秋期本試験	問6
問3	令和5年秋期本試験	問6
問4	令和4年秋期本試験	問6

第4章　ネットワーク

問1	令和2年本試験	問5
問2	令和3年秋期本試験	問5
問3	令和5年春期本試験	問5
問4	令和6年春期本試験	問5

第5章　情報セキュリティ

問1	平成29年秋期本試験	問1
問2	令和6年秋期本試験	問1
問3	令和5年秋期本試験	問1
問4	令和5年春期本試験	問1
問5	令和4年秋期本試験	問1
問6	令和3年春期本試験	問1
問7	令和4年春期本試験	問1
問8	令和3年秋期本試験	問1

第6章　情報システム開発

問1	平成30年春期本試験	問8
問2	令和6年秋期本試験	問8
問3	平成29年春期本試験	問8
問4	令和5年秋期本試験	問8

第7章　組込みシステム開発

問1	平成31年春期本試験	問7
問2	令和3年春期本試験	問7
問3	令和5年秋期本試験	問7
問4	令和4年春期本試験	問7

第8章　プロジェクトマネジメント

問1	令和4年秋期本試験	問9
問2	令和元年秋期本試験	問9
問3	平成31年春期本試験	問9
問4	令和5年秋期本試験	問9

第9章　サービスマネジメント

問1	令和4年春期本試験	問10
問2	令和6年秋期本試験	問10
問3	平成30年秋期本試験	問10
問4	令和5年春期本試験	問10

第10章　システム監査

問1	令和2年本試験	問11
問2	令和6年春期本試験	問11
問3	令和4年度秋期本試験	問11
問4	平成29年春期本試験	問11

第11章　経営戦略

問1	令和3年度春期本試験	問2
問2	令和6年秋期本試験	問2
問3	令和4年度秋期本試験	問2
問4	令和元年度秋期本試験	問2

第５章　情報セキュリティ

問３　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，設問に答えよ。

K社は，IT製品の卸売会社であり，300社の販売店に製品を卸している。K社では，8 年前に従業員が，ある販売店向けの奨励金額が記載されたプロモーション企画書ファイルを添付した電子メール（以下，メールという）を，担当する全販売店の担当者宛てに誤送信するというセキュリティ事故が発生した。この事故を機に，メールの添付ファイルを，使い捨てのパスワード（以下，DPW という）によって復元可能な ZIP ファイルに変換する添付ファイル圧縮サーバを導入した。

添付ファイル圧縮サーバ導入後のメール送信手順を図１に示す。

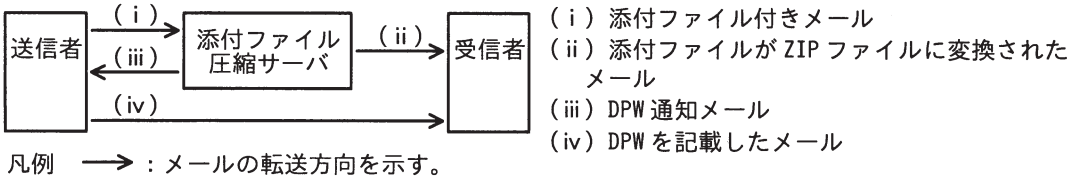

図１　添付ファイル圧縮サーバ導入後のメール送信手順

〔現在のメール運用の問題点と対策〕

K 社では，添付ファイル圧縮サーバを利用して，最初に DPW で復元可能な ZIP ファイルを添付したメール（以下，本文メールという）を送信し，その後，ZIP ファイルを復元するための DPW を記載したメール（以下，PW メールという）を送信することによって，メールのセキュリティを確保する方式（以下，この方式を PPAP という）を運用している。

しかし，現在運用している PPAP は，政府のある機関において中止するという方針が公表され，K 社の販売店や同業者の中でも PPAP の運用を止める動きが見られるようになった。

このような状況から，K 社の情報セキュリティ委員会は，自社の PPAP の運用上の問題点を検証することが必要であると判断して，情報セキュリティリーダーのL主任に，PPAP の運用上の問題点の洗い出しと，その改善策の検討を指示した。

L主任は，現在の PPAP の運用状況を調査して，次の二つの問題点を洗い出した。

(1)　①本文メールの宛先を確認せずに，本文メールと同じ宛先に対して PW メールを

送信している従業員が多い。

(2)　ほとんどの従業員が，PW メールを本文メールと同じメールシステムを使用して送信している。したがって，本文メールが通信経路上で何らかの手段によって盗聴された場合，PW メールも盗聴されるおそれがある。

問題点の(1)及び(2)は，ともに情報漏えいにつながるリスクがある。(1)の問題点を改善しても，(2)の問題点が残ることから，②L 主任は(2)の問題点の改善策を考えた。しかし，運用面の改善によってリスクは低減できるが，時間とともに情報漏えいに対する意識が薄れると，改善策が実施されなくなるおそれがある。そこで，L 主任は，より高度なセキュリティ対策を実施して，情報漏えいリスクを更に低減させる必要があると考え，安全なメールの送受信方式を調査した。

〔安全なメール送受信方式の検討〕

L 主任は，調査に当たって安全なメール送受信方式のための要件として，次の(ⅰ)～(ⅲ)を設定した。

(ⅰ)　メールの本文及び添付ファイル（以下，メール内容という）を暗号化できること

(ⅱ)　メール内容は，送信端末と受信端末との間の全ての区間で暗号化されていること

(ⅲ)　誤送信されたメールの受信者には，メール内容の復号が困難なこと

これら三つの要件を満たす技術について調査した結果，S/MIME（Secure/Multipurpose Internet Mail Extensions）が該当することが分かった。S/MIME は，K 社や販売店で使用している PC のメールソフトウェア（以下，メーラという）が対応しており導入しやすいと L 主任は考えた。

〔S/MIME の調査〕

まず，L 主任は S/MIME について調査した。調査によって分かった内容を次に示す。

・S/MIME は，メールに電子署名を付加したり，メール内容を暗号化したりすることによってメールの安全性を高める標準規格の一つである。

・メールに電子署名を付加することによって，メーラによる電子署名の検証で，送信者を騙(かた)ったなりすましや③メール内容の改ざんが検知できる。公開鍵暗号と共通鍵暗号とを利用してメール内容を暗号化することによって，通信経路での盗聴や誤送信による情報漏えいリスクを低減できる。

・S/MIME を使用して電子署名や暗号化を行うために，認証局（以下，CA という）が発行した電子証明書を取得してインストールするなどの事前作業が必要となる。

メールへの電子署名の付加及びメール内容の検証の手順を表 1 に，メール内容の暗号化と復号の手順を表 2 に示す。

表 1　メールへの電子署名の付加及びメール内容の検証の手順

送信側		受信側	
手順	処理内容	手順	処理内容
1.1	ハッシュ関数 h によってメール内容のハッシュ値 x を生成する。	1.4	電子署名を［ b ］で復号してハッシュ値 x を取り出す。
1.2	ハッシュ値 x を［ a ］で暗号化して電子署名を行う。	1.5	ハッシュ関数 h によってメール内容のハッシュ値 y を生成する。
1.3	送信者の電子証明書と電子署名付きのメールを送信する。	1.6	手順 1.4 で取り出したハッシュ値 x と手順 1.5 で生成したハッシュ値 y とを比較する。

表 2　メール内容の暗号化と復号の手順

送信側		受信側	
手順	処理内容	手順	処理内容
2.1	送信者及び受信者が使用する共通鍵を生成し，④共通鍵でメール内容を暗号化する。	2.4	［ d ］で共通鍵を復号する。
2.2	［ c ］で共通鍵を暗号化する。	2.5	共通鍵でメール内容を復号する。
2.3	暗号化したメール内容と暗号化した共通鍵を送信する。		

〔S/MIME 導入に当たっての実施事項の検討〕

次に，L 主任は，S/MIME 導入に当たって実施すべき事項について検討した。

メーラは，⑤受信したメールに添付されている電子証明書の正当性について検証する。問題を検出すると，エラーが発生したと警告されるので，エラー発生時の対応方

法をまとめておく必要がある。そのほかに，受信者自身で電子証明書の内容を確認することも，なりすましを発見するのに有効であるので，受信者自身に実施を求める事項もあわせて整理する。

メール内容の暗号化を行う場合は，事前に通信相手との間で電子証明書を交換しておかなければならない。そこで，S/MIME 導入に当たって，S/MIME の適切な運用のために従業員向けの S/MIME の利用手引きを作成して，利用方法を周知することにする。

これらの検討結果を基に，L 主任は S/MIME の導入，導入に当たって実施すべき事項，導入までの間は PPAP の運用上の改善策を実施することなどを提案書にまとめ，情報セキュリティ委員会に提出した。提案内容が承認され S/MIME の導入が決定した。

設問1　〔現在のメール運用の問題点と対策〕について答えよ。

(1)　本文中の下線①によって発生するおそれのある，情報漏えいにつながる問題を，40 字以内で答えよ。

(2)　本文中の下線②について，盗聴による情報漏えいリスクを低減させる運用上の改善策を，30 字以内で答えよ。

設問2　〔S/MIME の調査〕について答えよ。

(1)　本文中の下線③が検知される手順はどれか。表 1，2 中の手順の番号で答えよ。

(2)　表 1，2 中の［　a　］～［　d　］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　CA の公開鍵　　イ　CA の秘密鍵　　ウ　受信者の公開鍵

エ　受信者の秘密鍵　　オ　送信者の公開鍵　　カ　送信者の秘密鍵

(3)　表 2 中の下線④について，メール内容の暗号化に公開鍵暗号ではなく共通鍵暗号を利用する理由を，20 字以内で答えよ。

設問3　本文中の下線⑤について，電子証明書の正当性の検証に必要となる鍵の種類を解答群の中から選び，記号で答えよ。

解答群

ア　CA の公開鍵　　イ　受信者の公開鍵　　ウ　送信者の公開鍵

問４　マルウェア対策に関する次の記述を読んで，設問に答えよ。

R 社は，全国に支店・営業所をもつ，従業員約 150 名の旅行代理店である。国内の宿泊と交通手段を旅行パッケージとして，法人と個人の双方に販売している。R 社は，旅行パッケージ利用者の個人情報を扱うので，個人情報保護法で定める個人情報取扱事業者である。

〔ランサムウェアによるインシデント発生〕

ある日，R 社従業員の S さんが新しい旅行パッケージの検討のために，R 社から S さんに支給されている PC（以下，PC-S という）を用いて業務を行っていたところ，PC-S に身の代金を要求するメッセージが表示された。S さんは連絡すべき窓口が分からず，数時間後に連絡が取れた上司からの指示によって，R 社の情報システム部に連絡した。連絡を受けた情報システム部の T さんは，PC がランサムウェアに感染したと考え，①PC-S に対して直ちに実施すべき対策を伝えるとともに，PC-S を情報システム部に提出するように S さんに指示した。

T さんは，セキュリティ対策支援サービスを提供している Z 社に，提出された PC-S 及び R 社 LAN の調査を依頼した。数日後に Z 社から受け取った調査結果の一部を次に示す。

・PC-S から，国内で流行しているランサムウェアが発見された。
・ランサムウェアが，取引先を装った電子メールの添付ファイルに含まれていて，S さんが当該ファイルを開いた結果，PC-S にインストールされた。
・PC-S 内の文書ファイルが暗号化されていて，復号できなかった。
・PC-S から，インターネットに向けて不審な通信が行われた痕跡はなかった。
・PC-S から，R 社 LAN 上の IP アドレスをスキャンした痕跡はなかった。
・ランサムウェアによる今回のインシデントは，表 1 に示すサイバーキルチェーンの攻撃の段階では［ a ］まで完了したと考えられる。

表1　サイバーキルチェーンの攻撃の段階

項番	攻撃の段階	代表的な攻撃の事例
1	偵察	インターネットなどから攻撃対象組織に関する情報を取得する。
2	武器化	マルウェアなどを作成する。
3	デリバリ	マルウェアを添付したなりすましメールを送付する。
4	エクスプロイト	ユーザーにマルウェアを実行させる。
5	インストール	攻撃対象組織のPCをマルウェアに感染させる。
6	C&C	マルウェアとC&Cサーバを通信させて攻撃対象組織のPCを遠隔操作する。
7	目的の実行	攻撃対象組織のPCで収集した組織の内部情報をもち出す。

〔セキュリティ管理に関する評価〕

Tさんは，情報システム部のU部長にZ社からの調査結果を伝え，PC-Sを初期化し，初期セットアップ後にSさんに返却することで，今回のインシデントへの対応を完了すると報告した。U部長は再発防止のために，R社のセキュリティ管理に関する評価をZ社に依頼するよう，Tさんに指示した。Tさんは，Z社にR社のセキュリティ管理の現状を説明し，評価を依頼した。

R社のセキュリティ管理に関する評価を実施したZ社は，ランサムウェア対策に加えて，特にインシデント対応と社員教育に関連した取組が不十分であると指摘した。Z社が指摘したR社のセキュリティ管理に関する課題の一部を表2に示す。

表2　R社のセキュリティ管理に関する課題（一部）

項番	種別	指摘内容
1	ランサムウェア対策	PC上でランサムウェアの実行を検知する対策がとられていない。
2	インシデント対応	インシデントの予兆を捉える仕組みが整備されていない。
3		インシデント発生時の対応手順が整備されていない。
4	社員教育	インシデント発生時の適切な対応手順が従業員に周知されていない。
5		標的型攻撃への対策が従業員に周知されていない。

U部長は，表2の課題の改善策を検討するようにTさんに指示した。Tさんが検討したセキュリティ管理に関する改善策の候補を表3に示す。

表3　Tさんが検討したセキュリティ管理に関する改善策の候補

項番	種別	改善策の候補
1	ランサムウェア対策	②PC上の不審な挙動を監視する仕組みを導入する。
2	インシデント対応	PCやサーバ機器，ネットワーク機器のログからインシデントの予兆を捉える仕組みを導入する。
3		PCやサーバ機器の資産目録を随時更新する。
4		新たな脅威を把握して対策の改善を行う。
5		インシデント発生時の対応体制や手順を検討して明文化する。
6		脆弱(ぜい)性情報の収集方法を確立する。
7	社員教育	インシデント発生時の対応手順を従業員に定着させる。
8		標的型攻撃への対策についての社員教育を行う。

〔インシデント対応に関する改善策の具体化〕

Tさんは，表3の改善策の候補を基に，インシデント対応に関する改善策の具体化を行った。Tさんが検討した，インシデント対応に関する改善策の具体化案を表4に示す。

表4　インシデント対応に関する改善策の具体化案

項番	改善策の具体化案	対応する表3の項番
1	R社社内に③インシデント対応を行う組織を構築する。	5
2	R社の情報機器のログを集約して分析する仕組みを整備する。	2
3	R社で使用している情報機器を把握して関連する脆弱性情報を収集する。	b，c
4	社内外の連絡体制を整理して文書化する。	d
5	④セキュリティインシデント事例を調査し，技術的な対策の改善を行う。	4

検討したインシデント対応に関する改善策の具体化案をU部長に説明したところ，表4の項番5のセキュリティインシデント事例について，特にマルウェア感染などによって個人情報が窃取された事例を中心に，Z社から支援を受けて調査するように指示を受けた。

〔社員教育に関する改善策の具体化〕

Tさんは，表3の改善策の候補を基に，社員教育に関する改善策の具体化を行った。Tさんが検討した，社員教育に関する改善策の具体化案を表5に示す。

表5　社員教育に関する改善策の具体化案

項番	改善策の具体化案	対応する表3の項番
1	標的型攻撃メールの見分け方と対応方法などに関する教育を定期的に実施する。	8
2	インシデント発生を想定した訓練を実施する。	7

R社では，標的型攻撃に対応する方法やインシデント発生時の対応手順が明確化されておらず，従業員に周知する活動も不足していた。そこで，標的型攻撃の内容とリスクや標的型攻撃メールへの対応，インシデント発生時の対応手順に関する研修を，新入社員が入社する4月に全従業員に対して定期的に行うことにした。

また，R社でのインシデント発生を想定した訓練の実施を検討した。図1に示す一連のインシデント対応フローのうち，⑤全従業員を対象に実施すべき対応と，経営者を対象に実施すべき対応を中心に，ランサムウェアによるインシデントへの対応を含めたシナリオを作成することにした。

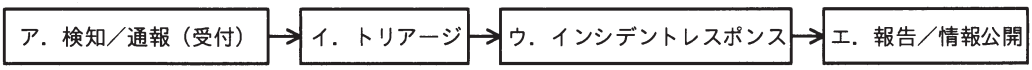

図1　一連のインシデント対応フロー

Tさんは，今回のインシデントの教訓を生かして，ランサムウェアに感染した際にPC内の重要な文書ファイルの喪失を防ぐために，取り外しできる記録媒体にバックアップを取得する対策を教育内容に含めた。検討した社員教育に関する改善策の具体化案をU部長に説明したところ，⑥バックアップを取得した記録媒体の保管方法について検討し，その内容を教育内容に含めるようにTさんに指示した。

設問1　〔ランサムウェアによるインシデント発生〕について答えよ。

(1)　本文中の下線①について，PC-Sに対して直ちに実施すべき対策を解答群の中から選び，記号で答えよ。

解答群

ア　怪しいファイルを削除する。　イ　業務アプリケーションを終了する。

ウ　ネットワークから切り離す。　エ　表示されたメッセージに従う。

(2) 本文中の［ a ］に入れる適切な攻撃の段階を表1の中から選び，表1の項番で答えよ。

設問2 〔セキュリティ管理に関する評価〕について答えよ。

(1) 表2中の項番3の課題に対応する改善策の候補を表3の中から選び，表3の項番で答えよ。

(2) 表3中の下線②について，PC上の不審な挙動を監視する仕組みの略称を解答群の中から選び，記号で答えよ。

解答群

ア APT　　イ EDR　　ウ UTM　　エ WAF

設問3 〔インシデント対応に関する改善策の具体化〕について答えよ。

(1) 表4中の下線③について，インシデント対応を行う組織の略称を解答群の中から選び，記号で答えよ。

解答群

ア CASB　　イ CSIRT　　ウ MITM　　エ RADIUS

(2) 表4中の［ b ］～［ d ］に入れる適切な表3の項番を答えよ。

(3) 表4中の下線④について，調査すべき内容を解答群の中から全て選び，記号で答えよ。

解答群

ア 使用された攻撃手法　　イ 被害によって被った損害金額

ウ 被害を受けた機器の種類　　エ 被害を受けた組織の業種

設問4 〔社員教育に関する改善策の具体化〕について答えよ。

(1) 本文中の下線⑤について，全従業員を対象に訓練を実施すべき対応を図1の中から選び，図1の記号で答えよ。

(2) 本文中の下線⑥について，記録媒体の適切な保管方法を20字以内で答えよ。

第５章　情報セキュリティ　解答・解説

問3

解答

設問		解答例	備考
設問1	(1)	本文メールを誤送信すると，DPWも誤送信した相手に届いてしまう。	
	(2)	DPWを，電話や携帯メールなど異なった手段で伝える。	
設問2	(1)	1.6	
	(2)	a カ　b オ　c ウ　d エ	
	(3)	暗号化と復号の処理速度が速いから	
設問3		ア	

解説

本問で取り上げられているPPAPとは，「Password付きZIPファイルを送ります Passwordを送ります Angoka（暗号化）Protocol（プロトコル）」の略称であり，1通目で「暗号化ZIPファイル」を，2通目で「復号に必要なパスワード」をそれぞれ別のメールで送信する方式を指す。この方式は本質的にメールの安全性（機密性）を向上させないだけでなく，暗号化されていることによってメールサーバでのウイルスチェックも妨げるなどの弊害の方が大きく問題視されているため，利用しないことを推奨するために命名された。

設問1

(1)

下線①では本文メールとPWメールについて述べているので，本文メールとPWメールに関する説明を整理すると次のようになる。

1. 使い捨てのパスワード（DPW）で復元可能なZIPファイルをメールに添付して送る（本文メール）。
2. DPWを記載したメールを本文メールとは別のメールで送る（PWメール）。

さらに下線①では，「本文メールの宛先を確認せずに，本文メールと同じ宛先に対してPWメールを送信している従業員が多い」と述べている。このような運用方法で宛先を間違えて送信した場合，本文メール（DPWで復元可能なZIPファイル）とPWメール（DPW）の両方が同じ宛先（誤送信先）に到着することになり，受信者は，DPWを用いて，ZIPファイルを復元できてしまう。ここでは，「発生する恐れのある，情報漏えいにつながる問題」が問われているので，

本文メールを誤送信すると，DPWも誤送信した相手に届いてしまう。

のように解答すればよい。

(2)

下線②で述べられた(2)の問題点とは,「ほとんどの従業員が，PWメールを本文メールと同じメールシステムを使用して送信している。したがって，本文メールが通信経路上で何らかの手段によって盗聴された場合,PWメールも盗聴されるおそれがある」というものである。盗聴者が両方のメールを盗聴するということは，メールの通信経路が同じであり，どちらも盗聴者を経由することを意味する。この対策としては本文メールとPWメールが異なる通信経路となるよう別の通信手段を用いればよい。これを制限字数内にまとめ，

DPWを，電話や携帯メールなど異なった手段で伝える。

のように解答すればよい。

設問2

解説の前に，電子署名(デジタル署名)の付与と検証の流れを整理しておく。本問における電子署名の付与と検証は，次のような手順で行う。

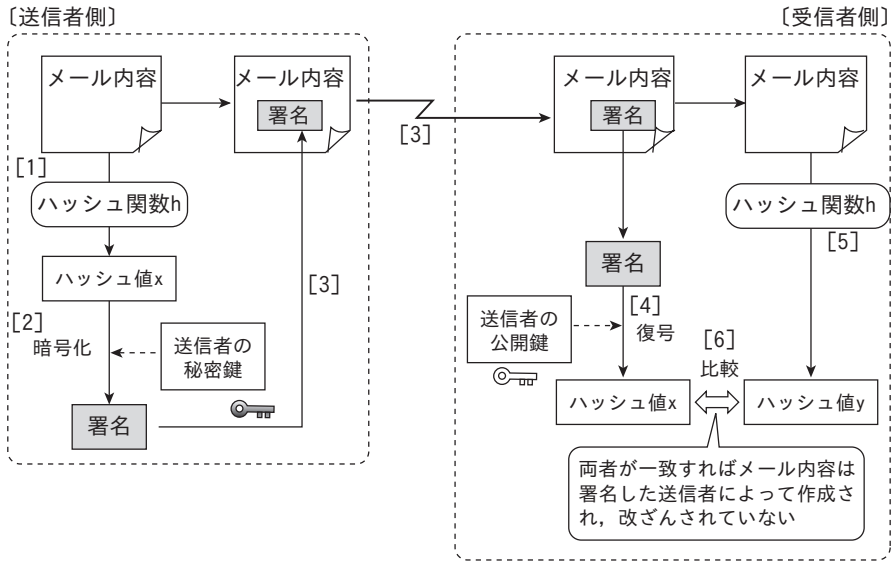

図2　電子署名

・署名の付与

[1]　ハッシュ関数hを用いて，メール内容からハッシュ値xを生成する。

[2]　ハッシュ値xを送信者の秘密鍵で暗号化し，電子署名を生成する。

[3]　メール内容に電子署名を付加して送信する（必要に応じてデジタル署名の検証に利用する公開鍵を含んだ電子証明書も送信する)。

・署名の検証

[4]　電子署名を送信者の公開鍵で復号し，ハッシュ値xを取り出す。

[5]　ハッシュ関数hを用いて，受信したメール内容からハッシュ値yを生成する。

[6]　ハッシュ値xとハッシュ値yを比較する。

(1)

メーラによる電子署名の検証でメール内容の改ざんを検知するためには，電子署名を復号して得られたハッシュ値と受信したメール内容から得られたハッシュ値を比較すればよい。両者が一致すれば受信したメールの内容に改ざんはないと判断でき，一致しない場合は改ざんが行われたことを検知できる。表1中でハッシュ値を比較している処理は，

1.6

である。

(2)

aについて

電子署名は，メール内容を作成した送信者のみが付加できるものでなくてはならない。このためには，送信者がハッシュ値xを，

送信者の秘密鍵　（カ）

で暗号化して電子署名を生成すればよい。

bについて

電子署名を検証する際は，暗号化に用いた送信者の秘密鍵と対になる鍵を用いて電子署名を復号する。すなわち，受信者が電子署名を，

送信者の公開鍵　　（オ）

で復号し，ハッシュ値xを取り出せばよい。

cについて

S/MIMEでは，メール内容を暗号化する際は共通鍵暗号を利用する。共通鍵暗号では，共通鍵そのものが盗聴されるとメール内容が復号されてしまうので，共通鍵を暗号化する必要がある。暗号化した共通鍵は，受信者のみが復号できるようにすればよいので，送信者は共通鍵を，

受信者の公開鍵　（ウ）

で暗号化すればよい。

dについて

元の共通鍵を得るためには，これと対になる鍵で復号すればよい。よって，受信者は暗号化された共通鍵を，

受信者の秘密鍵　（エ）

で復号すればよい。

(3)

ここではメール内容の暗号化に，公開鍵暗号ではなく共通鍵暗号を用いる理由が問われているので，まずは共通鍵暗号と公開鍵暗号の特徴を整理する。共通鍵暗号と公開鍵暗号の特徴を比較すると，次のようになる。

表3　共通鍵暗号と公開鍵暗号の比較

	共通鍵暗号	公開鍵暗号
暗号化や復号に要する時間	短い	長い
鍵の安全な配送	困難	容易

公開鍵暗号では，自分の公開鍵（実際には電子証明書の形式）を通信相手に配送すればよい。この公開鍵が盗聴されても暗号文が解読されることはないので，鍵を安全に配送できる。一方，共通鍵暗号では共通鍵を配送する必要がある。この共通鍵が盗聴されると暗号文も復号されてしまうので，メールなどで共通鍵を配送することは安全とはいえない。また，公開鍵暗号には暗号化や復号に要する時間が長いという特徴もある。このため，メール内容のようなデータまで公開鍵暗号で暗号化すると処理に時間がかかり，利便性が損なわれてしまう。そこで，メール内容などのデータは高速な共通鍵暗号で暗号化し，データ量の小さな鍵は安全な公開鍵暗号で暗号化することにより，両者の長所を活かすことができる。共通鍵暗号と公開鍵暗号を組み合わせた方式を，ハイブリッド暗号ともいう。以上より，

　暗号化と復号の処理速度が速いから

のように共通鍵暗号の長所を解答すればよい。

設問3

下線⑤で述べられた電子証明書は，公開鍵や公開鍵の所有者情報に対してCA（認証局）が電子署名を付加したデータである。電子証明書が正当であることが確認できれば，その証明書に含まれる公開鍵や所有者情報も正当であり，なりすまされてないと判断できる。

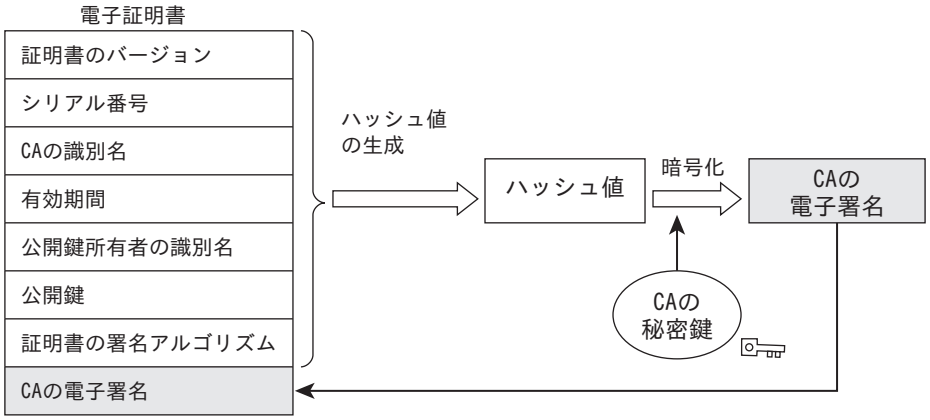

図3　電子証明書の構成

電子証明書の正当性を検証するためには，電子証明書に付加された電子署名が正しいかを検証すればよい。電子証明書を発行するCAが電子署名を付加するためには，CAの秘密鍵を用いる。よって，正当性を検証するためには，それと対になる

　CAの公開鍵

が必要になる。

問4

解答

設問		解答例	備考
設問1	(1)	ウ	
	(2)	a　5	
設問2	(1)	5	
	(2)	イ	
設問3	(1)	イ	
	(2)	b　3　c　6　d　5	(b, cは順不同)
	(3)	ア，ウ	
設問4	(1)	ア	
	(2)	PCから切り離して保管する。	

解説

設問1

(1)

ランサムウェアは，PCに内蔵または外部接続された補助記憶装置(磁気ディスク装置やSSDなど)，ネットワークを介してアクセス可能な記憶装置(ファイルサーバなど)に保存されているデータを暗号化し，暗号化の解除と引き替えに金銭を要求するマルウェアである。金銭を支払っても暗号化が解除される保証はなく，ファイルを流出させると脅迫して更なる金銭を要求するものもある。このような特徴を踏まえると，ランサムウェアに代表されるマルウェアへの感染が疑われる場合は，PCを早急にネットワークから切り離し，ネットワーク上のデータや機器に被害が拡大しないようにすることが重要である。

よって，ランサムウェアに感染したと考えたPC-Sに対して，直ちに実施すべき対策は，

ネットワークから切り離す　(ウ)

である。

(2)

空欄aの前では,「ランサムウェアによる今回のインシデント」と述べられていることから，まずはランサムウェアによるインシデントの内容を整理する。〔ランサムウェアによるインシデント発生〕では,「ランサムウェアが，取引先を装った電子メールの添付ファイルに含まれていて，Sさんが当該ファイルを開いた結果，PC-Sにインストールされた」と述べられていることから，表1の項番5(インストール)までは完了していると判断できる。

続いて，その次の段階である項番6についても検討する。C&C(Command and Control)サーバとは,マルウェアに対して指示を出すために攻撃者が用意したサーバであり,インターネット上に設置されている。「PC-Sから，インターネットに向けて不審な通信が行われた痕跡は

なかった」という調査結果を考慮すると，項番6の段階は完了していないと判断できる。

よって，空欄に入れるべき項番は，

5

となる。

設問2

(1)

表2中の項番3の課題は，「インシデント発生時の対応手順が整備されていない」となっているので，インシデント発生時の対応手順を確立するような改善策を表3中から選べばよい。表3中で，インシデント対応に関する改善策は項番2～6であり，インシデント対応手順を事前に策定しておくことに関連している改善策の項番は，

5

である。インシデント発生時の対応手順は，事前に策定してインシデント対応手順書などとして明文化するとともに，関連する組織に周知しておくことが大切である。

(2)

本文中の下線②では，「PC上の不審な挙動を監視する仕組み」と述べられている。PC上の不審な挙動を監視するためには，その仕組みが当該のPC上で稼働していなければならない。解答群のうち，PC上で稼働する仕組みに該当するのは，

EDR(Endpoint Detection and Response)（イ）

である。

エンドポイントとは，PCやタブレットといったネットワークの末端に位置する機器のことである。EDRは，このようなエンドポイントとなる機器にインストールし，当該機器の挙動を監視することにより，マルウェアの活動や不審な通信などを検出する。異常を検出した場合は，管理サーバなどへ通知する機能ももつ。

APT(Advanced Persistent Threat)：標的型攻撃に使われる手法の一つで，攻撃していることを感づかれないよう，執拗かつ長期に渡って攻撃を継続する手法である。一般的には，電子メールにマルウェアを添付して送信し，これにPCを感染させることが，最初の段階である。その後，PCを乗っ取って，徐々にシステムの中枢部へ攻撃を広げる。

UTM(Unified Threat Management)：統合脅威管理のことである。ウイルス対策やファイアウォール，侵入検知システム(IDS)などを統合して運用するシステムや，そのためのソフトウェアを指すこともある。

WAF(Web Application Firewall)：Webアプリケーションへの攻撃(SQLインジェクション，クロスサイトスクリプティングなど)に特化したファイアウォールである。

設問3

(1)

インシデントが発生した際に，インシデント対応を行う組織(部署や対応チームなど)のことを，

CSIRT(Computer Security Incident Response Team)

という。CSIRTには，組織内に設置されるものだけでなく，CSIRTをサービスとして提供する企業もある。セキュリティインシデントが発生すると，CSIRTはトリアージ(深刻度や緊急度などから優先度を設定)を行うと共に，必要に応じて外部の組織とも連携しながら解決に向けた活動を行う。また，通常時は，インシデント情報の収集やインシデントが発生した際の影響分析といったインシデントの発生に備えた活動なども行う。

CASB(Cloud Access Security Broker)：クラウドサービス利用時に求められる脆弱性対策のこと,または,そのような対策を行うためのソフトウェアのことである。CASBでは,シャドーIT対策，データ漏えい防止対策(DLP：Data Loss Prevention)，マルウェア対策，リスクの可視化などを行う。

MITM(Man In The Middle)：中間者攻撃のことである。通信当事者間に入り込み，双方の通信当事者になりすまして，通信の盗聴や，情報の改ざんなどを行う。

RADIUS(Remote Authentication Dial-In User Service)：社外から社内へのアクセスなどのリモートアクセス時の利用者認証を行うための仕組みである。

(2)

空欄b～dを含む表4は，表3のセキュリティ管理に関する改善策のうち，インシデント対応に関する具体化案である。よって,空欄b～dを含む各項番の「改善の具体化案」を参照し，関連するものを表3の種別が“インシデント対応”となっている項番2～6の中から探せばよい。

b，cについて

表4の項番3では，改善策の具体化案として,「R社で使用している情報機器を把握して関連する脆弱性情報を収集する」と述べられている。これを，

①R社で使用している情報機器を把握

②脆弱性情報を収集

の2点に分解して考える。

①については，使用している情報機器を把握することにより，どのような情報機器があるのかを管理する一覧表のようなものが作成されると考えられる。これに該当するものを表3の中から探すと，項番3でPCやサーバといった情報資産の一覧である“資産目録”を随時更新することが述べられている。

②については,脆弱性情報の収集に関連するものを表3の中から探す。すると,項番6で「脆弱性情報の収集方法を確立する」と述べられている。各機器の脆弱性情報がどこでどのように公開されているかを確認するとともに，それを収集する方法や頻度などを確立することにより，脆弱性情報を適切に収集できる。

以上より，

3，6

を解答すればよい。

dについて

項番4では,改善策の具体化案が「社内外の連絡体制を整理して文書化する」となっている。表3から体制に関するものを探すと，項番5で「インシデント発生時の対応体制や手順を検討して明文化する」とある。インシデント発生時の対応体制を明文化するためには，インシデント発生時にはどのような組織・人と連絡をとればよいかを整理し，文書化すればよいはずなので，

5

を解答すればよい。

(3)

下線④では，「技術的な対策の改善を行う」と述べられている。技術的な対策の改善を行うためには，セキュリティインシデントについての技術的な事柄を調査する必要がある。選択肢の中で，技術的な事柄を述べているものは，

使用された攻撃手法　（ア）

と

被害を受けた機器の種類　（ウ）

である。「損害金額」や「組織の業種」などの情報は，技術的な事柄ではないので，技術的な対策を改善するうえでは有用とはいえない。

設問4

(1)

設問では，全従業員を対象に訓練を実施すべき対応を，図1の記号で答えるよう要求されている。図1で示されたインシデント対応フローは，JPCERT/CCが公開しているインシデントハンドリングマニュアルに沿ったものとなっている。

検知／通報（受付）は，発生したインシデントを検知し，受け付ける活動である。インシデントは，大きく分けて二つの方法で検知される。一つは，保守作業中に発見する，セキュリティ機器からの警告などによって検知するといった，自組織内で検知する方法である。もう一つは，他の組織（被害者やセキュリティベンダなど），自組織の従業員，サービス利用者などからの通報を受けて検知する方法である。後者については，実際に機器を利用している利用者，すなわち，全従業員が通報を行う可能性がある。表3の項番7では，社員教育に関する改善策として，「インシデント発生時の対応手順を従業員に定着させる」と書かれていることからも，実際の利用者が，検知／報告を行うと判断できる。

トリアージは，発生したインシデントの緊急度を考慮して，対応の優先順位を定めることである。トリアージは，実際にインシデント対応を行う組織であるCSIRTなどが行う。

インシデントレスポンスは，トリアージの結果を受けてインシデントに対応することである。トリアージと同様に，CSIRTなどの組織が行う。

インシデント対応と並行して，必要に応じて顧客や関係者，メディアなどに対する情報公開や，監督官庁などに対する報告などを行う。この活動は，経営陣やその対応を行う部署などが行うので，全従業員が行うわけではない。

以上より，全従業員を対象に訓練を実施すべき対応は，

検知／報告（受付）（ア）

である。

(2)

下線⑥の前では，「ランサムウェアに感染した際にPC内の重要な文書ファイルの喪失を防ぐために，取り外しできる記録媒体にバックアップを取得する」と述べられている。設問1(1)の解説で述べたように，ランサムウェアは，PCに内蔵または外部接続された補助記憶装置（磁気ディスク装置やSSDなど），ネットワークを介してアクセス可能な記憶装置（ファイルサーバなど）に保存されているデータを暗号化する。よって，取得したバックアップが格納されている「取り外しできる記録媒体」をPCに接続したままにしておくと，取得したバックアップもランサムウェアによって暗号化されてしまう。よって，バックアップを取得した記録媒体は，

PCから切り離して保管する

必要がある。このことを答えればよい。