

第1章 IT（情報技術）に潜む危険 ～まとめ編～

1. ITの落とし穴

要点

ITの利便性の影にマイナス面もあります。どのような実例がありますか？
インターネットに潜む危険にはどのようなものがありますか？

解説

要 点	参照ページ	解 説
ITの利便性の影にマイナス面もあります。どのような実例がありますか？	2～5	情報セキュリティ読本では、次の実例が紹介されています。 <ul style="list-style-type: none">・個人情報の漏えい・キーロガー・常時接続の落とし穴・危ない無線LAN
インターネットに潜む危険にはどのようなものがありますか？	6～8	インターネットサーフィンに伴う危険として次のようなものがあります。 <ul style="list-style-type: none">・トロイの木馬のダウンロード・不正なプログラムのダウンロード・不正な会員料金や通信料金の請求 メール利用に伴う危険として次のようなものがあります。 <ul style="list-style-type: none">・スパムメール・身に覚えの無い料金を請求する詐欺メール・フィッシングメール

第 1 章 IT (情報技術) に潜む危険 ~ 演習編 ~

問題 1

次の文章は、IT の利便性の影に潜む危険について述べたものです。正しいものを 1 つ選択してください。

- (1) インターネットカフェとは異なり、自宅のパソコンはキーロガーを仕込まれないので安全性が高い。
- (2) 常時接続をしても、ADSL 接続であれば侵入されることはない。
- (3) 情報漏えいは人為的な問題なので、システムのセキュリティ設定とは関連がない。
- (4) ID やパスワードのずさんな管理が、個人情報の漏えいにつながることもある。
- (5) オフィスビルなど壁の厚いビルは電波を通さないので、無線 LAN も比較的安全だ。

問題 2

次の文章は、インターネットに潜む危険について述べたものです。正しくないものを 1 つ選択してください。

- (1) Web ページを閲覧するだけでは、ファイルはダウンロードされない。
- (2) 有用なプログラムに見えるソフトウェアでも、トロイの木馬の可能性もあるので、無闇なダウンロードは避ける。
- (3) Web ページやメールに記載されている URL は、必要がない限りクリックしない。
- (4) 身に覚えのない請求メールは返信せずに無視するのが賢明だ。
- (5) 実在の会社からのメールを装い、罠の Web サイトにユーザを導き、パスワードやクレジットカード番号等を入力させようとするフィッシングメールというものがある。

解答

問題番号	正解	参照先ページ番号
1	4	p.2 ~ 5
2	1	p.6 ~ 8 解説：Web ページに仕掛けられた仕組みにより、自動的にウイルスファイルなどの不正プログラムがダウンロードされることがあります。

第2章 今日のセキュリティリスク ～まとめ編～

1. 情報セキュリティ

要点

情報セキュリティの基本概念とは？

維持すべき3要素とは？

脅威、リスク、インシデントの相互関係は？

解説

要 点	参照ページ	解 説
情報セキュリティの基本概念とは？	10	正当な権利をもつ個人や組織が、情報や情報システムを意図通りに制御できること。
維持すべき3要素とは？	10	情報の機密性、完全性、可用性。
脅威、リスク、インシデントの相互関係は？	11	脅威: 情報の機密性・完全性・可用性を阻害する要因。外部からの要因と内在する要因がある。 リスク: 脅威によって情報資産が損なわれる可能性。 インシデント: 実際に情報資産が損なわれてしまった状態。

2. 高水準で推移するウイルス被害

要点

ウイルスの最近の傾向は？

解説

要 点	参照ページ	解 説
ウイルスの最近の傾向は？	13	ウイルスメールを大量に送信したり、セキュリティホールを悪用するなど、巧妙化および悪質化が進んでいます。

3. 外部からの侵入（不正アクセス）

要点

システムへの侵入はどのように行われますか？

不正行為にはどのような種類がありますか？（具体的に）

解説

要 点	参照ページ	解 説
システムへの侵入はどのように行われるか？	15～16	事前調査、権限取得、不正実行、後処理の段階を経て行われます。
不正行為にはどのような種類がありますか？（具体的に）	17	盗聴、改ざん、なりすまし、破壊、コンピュータ不正使用、不正プログラムの埋め込み、踏み台など。

4. サーバへの攻撃（サービス妨害）

要点

サーバへの攻撃にはどのようなものがありますか？

DoS 攻撃とは？（簡単に説明しよう）

解説

要 点	参照ページ	解 説
サーバへの攻撃(サービス妨害)にはどのようなものがあるか？	18～20	<ul style="list-style-type: none">・ DoS 攻撃（サービス妨害攻撃） 詳細は p.18・ DDoS 攻撃（分散 DoS 攻撃） 詳細は p.19・ メール攻撃 詳細は p.20
DoS 攻撃とは？（簡単に説明しよう）	18	<ul style="list-style-type: none">・ サーバに過大な負荷をかけ、パフォーマンスの低下やサービス停止に追い込む攻撃です。・ Ping の悪用など、さまざまな攻撃手法があります。・ DoS 攻撃を行うコードを仕込むウイルスも登場しています。

5. 情報システムのセキュリティホール

要点

脆弱性とは?

脆弱性にはどのようなものがありますか?

脆弱性を放置するとなぜいけないのでしょうか?

解説

要 点	参照ページ	解 説
脆弱性とは?	21	<p>情報システムのセキュリティ上の欠陥で、セキュリティホールとも言います。このような欠陥があると、それが弱点となり、外部からの攻撃を受ける可能性があります。</p> <p>情報セキュリティの基本概念で述べた脅威の中で、脆弱性は内在する要因の 1 つです(p.12 図 2.2 参照)。</p>
脆弱性はどこに存在するか?	21 ~ 24	脆弱性は、さまざまなハードウェア、ソフトウェア(OS、メールソフト、Web ブラウザ、CGI、ASP など)に存在する可能性があります。
脆弱性にはどのようなものがあるか?	22	脆弱性は数多く発見され、報告されています。例えば、かつてマイクロソフト社の IE(Internet Explorer)という Web ブラウザの脆弱性で、「不適切な MIME ヘッダが原因で、Internet Explorer が電子メールの添付ファイルを実行する(MS01-020)」というものが報告されました。これは、簡単に言うと、メール本文を見る、またはプレビューするだけで、添付ファイルが実行されてしまう、という脆弱性です。
脆弱性を放置するとなぜいけないのか?	21 ~ 24	<ul style="list-style-type: none">・ バッファオーバーフロー攻撃、クロスサイトスクリプティング攻撃など、脆弱性を悪用する攻撃を受けることがあります。・ 脆弱性を利用して感染を広げるウイルスに感染することがあります。

第2章 今日のセキュリティリスク ～演習編～

問題 1

情報セキュリティとして維持すべき3要素は何ですか。正しいものを1つ選択してください。

- (1) 情報の脅威、リスク、インシデント。
- (2) 情報の機密性、完全性、流動性。
- (3) 情報の利用性、将来性、互換性。
- (4) 情報の機密性、完全性、可用性。
- (5) そのような3要素はなく、機密性のみ維持すればよい。

問題 2

次の文章は、ウイルス被害の最新の傾向について述べたものです。正しいものを1つ選択してください。

- (1) ワクチンソフトの普及によって、巧妙なウイルスが減り、単純なウイルスが増えている。
- (2) 届出件数は1999年から急増し、特にマクロウイルスの被害が大きい。
- (3) 全体の数は増加傾向にあるが、セキュリティホール悪用型は減少している。
- (4) 届出件数は1999年から急増し、特にブートセクタ感染型の被害が大きい。
- (5) ウイルスメールを大量に送信したり、セキュリティホールを悪用するなど、巧妙化および悪質化が進んでいる。

問題 3

次の文章は、システムへの侵入について述べたものです。正しくないものを1つ選択してください。

- (1) 侵入された場合の被害として最も注意すべきは個人情報の漏えいであり、その他の被害についてはあまり注意を払う必要は無い。
- (2) 侵入の前に、ポートスキャンなどによって、システム情報を収集することがある。
- (3) 侵入されると、クレジットカードやID・パスワードなどの情報が盗まれることがある。
- (4) 侵入の後に、次回の侵入を容易にするために、バックドアを作成することがある。
- (5) 侵入されると、踏み台にされて、気づかぬうちに攻撃に加担していることがある。

問題 4

次の文章は、DoS攻撃/DDoS攻撃について述べたものです。正しいものを1つ選択してください。

- (1) DDoS攻撃のためには、多数のコンピュータに攻撃プログラムを仕込む必要があるが、攻撃者とは無関係の個人のコンピュータが利用されることはまず無い。

- (2) DoS 攻撃はデータの破壊が目的なので、クライアントよりもサーバが狙われやすい。
- (3) DoS 攻撃は、サーバに侵入し機密データを盗み出したり、データを改ざんする攻撃である。
- (4) DoS 攻撃は、サーバに過大な負荷をかけ、パフォーマンスの低下やサービスの停止に追い込む攻撃である。
- (5) サーバに脆弱性があると DoS 攻撃を受けてしまうので、脆弱性を解消することが必要だ。

問題 5

次の文章は、脆弱性について述べたものです。正しくないものを 1 つ選択してください。

- (1) 脆弱性は、情報システムのセキュリティ上の欠陥で、セキュリティホールとも言う。
- (2) 脆弱性は、さまざまなハードウェアやソフトウェアに存在する可能性がある。
- (3) OS、メールソフト、Web ブラウザの脆弱性は数多く報告されているが、ワードやエクセルなどの文書作成用アプリケーションソフトには脆弱性は報告されていない。
- (4) 脆弱性を放置すると、バッファオーバーフロー攻撃やクロスサイトスクリプティング攻撃などを受けることがある。
- (5) 脆弱性を放置すると、脆弱性を利用して感染を広げるウイルスに感染するおそれがある。

解答

問題番号	正解	参照先ページ番号
1	4	p.10
2	5	p.13
3	1	p.15 ~ 17 解説：個人情報の漏えい防止には、確かに最大限の注意を払うべきですが、システムに侵入された場合、ファイルの改ざんや消去など他にも様々な被害を受けることがありますので、そのような被害を受けないよう、対策を行う必要があります。
4	4	p.18 ~ 19 解説：DDoS 攻撃では、攻撃者に無関係のコンピュータが利用されることがよくあります。また、DoS/DDoS 攻撃では、Web サーバなどが狙われやすいのですが、それは Web 閲覧ができないように（サービスの提供ができないように）するという目的で行われます。
5	3	p.21 ~ 24

第3章 ウイルス被害とその対策 ～まとめ編～

1. ウイルスの定義と症状

要点

ウイルスとは?

ウイルスに感染するとどうなるのか?

解説

要 点	参照ページ	解 説
ウイルスとは?	26	<p>簡単に言うと「コンピュータに対して、数々の悪さをする不正プログラム」です。感染の仕方や発症の様子などが、人に病気をもたらす生物界のウイルスに似ているため、このように(ウイルスまたはコンピュータウイルス)と呼ばれています。</p> <p>経済産業省告示「コンピュータウイルス対策基準」によると、「第三者のプログラムやデータベースに対して、意図的に何らかの被害を及ぼすように作られた不正プログラムで、(1)自己伝染機能 (2)潜伏機能 (3)発病機能 の3つのうち一つ以上の機能をもつもの」。</p>
ウイルスに感染するとどうなるのか?	26～30	<p>ウイルスに感染すると、様々な被害が起こります。最近のウイルスは感染しても見た目にわかる症状を表さないものがほとんどです。したがって、気付かない間にウイルスメールを撒き散らすなど、いつの間にか加害者になっていることが多いのです。</p> <p>ウイルスに感染すると、知らないうちに大量のウイルスメールを送信したり、情報漏えいを引き起こしてしまったり、踏み台として攻撃に加担していることがあります。これらは、自分が気づかないうちに起きていることが多いので、そのようなことにならないよう、しっかりウイルス対策を行う必要があります。</p>

2. ウイルス感染の原因

要点

ウイルス感染につながる操作にはどのようなものがあるか？

解説

要 点	参照ページ	解 説
ウイルス感染につながる操作にはどのようなものがあるか？	31 ~ 34	ウイルス感染につながる操作には次のものがあります。 (1) メールの添付ファイルやインターネット経由（Web や P2P）などで入手したファイルを開く (2)メールの開封やプレビュー (3) Web ページの閲覧 また、自分では何の操作もしないのに、(4)インターネットへ接続しているだけで、感染することがあります。 (2)、(3)、(4)は、脆弱性の悪用による感染です。脆弱性を解消すれば基本的には防ぐことができます。

3. 巧妙化するウイルスの手口

要点

感染を広げる手口にはどのようなものがあるか？

解説

要 点	参照ページ	解 説
ウイルスが感染を広げる手口にはどのようなものがあるか？	35 ~ 38	ウイルス付きのメールを受け取っても、ユーザがそのまま（開かず、プレビューもせず）廃棄してしまえば、ウイルスに感染することはまずありません。ウイルスに感染させるためには、ユーザにメールを開かせたり、添付ファイルをダブルクリックさせるなど、何らかの操作（=感染のきっかけ）をさせることが必要です。 そのため、ウイルスはさまざまな工夫を凝らして、ユーザの操作を引き出します。その手口は、年々巧妙化しています。例えば次のような手口があります。 (1)送信者を詐称する（知合いや管理者などから来たメー

		<p>ルにみせかける)。</p> <p>(2)ユーザの気を引くファイル名をウイルスファイルにつける。</p> <p>(3)二重拡張子をつけたり、アイコンを偽装して実行形式のファイルであることを隠す。</p> <p>(4)ワクチンソフトを停止してウイルスが検出されないようにする。</p> <p>また、感染したパソコンから大量のウイルスメールを送信するウイルスが多くなっていますが、そのため、感染被害が拡大します。</p>
--	--	--

4. ウイルスの感染予防と駆除

要点

ウイルス対策7箇条とは?

添付ファイルの取り扱い(5つの心得)とは?

感染してしまった場合の対処手順は??

解説

要 点	参照ページ	解 説
ウイルス対策7箇条とは?	41 ~ 43	<p>(1)最新のウイルス定義ファイルに更新しワクチンソフトを活用する。</p> <p>(2)添付ファイルを開く前にウイルス検査を行う。</p> <p>(3)ダウンロードしたファイルは、使用する前にウイルス検査を行う。</p> <p>(4)アプリケーションのセキュリティ機能を活用する。</p> <p>(5)セキュリティパッチをあてる。</p> <p>(6)ウイルス感染の兆候を見逃さない。</p> <p>(7)ウイルス感染被害からの復旧のためデータのバックアップを行う。</p>
添付ファイルの取り扱い(5つの心得)とは?	44 ~ 45	<p>(1)見知らぬ相手から届いた添付ファイル付きメールは削除する。</p> <p>(2)添付ファイルの見た目に惑わされない。</p> <p>(3)知人からのメールでも、添付ファイル付きは疑う。</p>

		(4)やたらにファイルを添付しない。 (5)メールソフトの添付ファイルの扱い方を理解する。
感染してしまった場合の対処手順は?	45 ~ 46	(1)コンピュータの使用を停止、ネットワークへの接続を遮断し、システム管理者の指示を仰ぐ。 (2)最新のワクチンソフトで検査し、ウイルス名を特定。 (3)ウイルスに合った適切な駆除を行う。 (4)データが破壊された場合は、バックアップから復旧。 (5)最新のワクチンソフトでもう一度検査。 (6)再発防止の対策を講じる。

5. モラルが問われる感染対策

要点

ウイルス対策でモラルが問われるとは?

解説

要 点	参照ページ	解 説
ウイルス対策でモラルが問われるのは?	48	対策を怠ると、自分が被害に遭うだけでなく、感染を広げることにより、間接的な加害者になってしまうためです。

第3章 ウイルス被害とその対策 ～演習編～

問題 1

次の文章は、ウイルスに感染したときの被害について述べたものです。正しいものを 1 つ選択してください。

- (1) 最近のウイルスは大きな被害を与えるものが多いので、通常どおりコンピュータが使えるときはウイルス感染を疑う必要はない。
- (2) インターネットを停止させてしまうようなウイルスはまだ発見されていない。
- (3) ウイルス感染に気づかないでいると、DoS 攻撃の踏み台として使用されることがある。
- (4) ウイルス感染によって情報が漏えいすることはないが、キーロガーを仕込まれることがあるので注意が必要だ。
- (5) フィッシング詐欺とウイルス感染は関連性がないと考えられる。

問題 2

次の文章は、ウイルス感染の原因について述べたものです。正しいものを 1 つ選択してください。

- (1) ウイルスはネットワーク経由で感染するので、スタンドアロンのコンピュータ(ネットワークに接続されていないコンピュータ)は安全である。
- (2) メールによる感染だけでなく、Web ページを見るだけでウイルスに感染することもある。
- (3) ウイルスは添付ファイルに潜んでいるので、メールを読むだけで、添付ファイルに触らなければウイルスに感染することはない。
- (4) 共有フォルダにパスワードを設定すると、ウイルスが入り込めないので安全である。
- (5) ウイルスに感染するのはセキュリティホールがあるからで、セキュリティホールをすべてふさげばウイルス感染を完全に防げる。

問題 3

次の文章は、巧妙化するウイルス感染の手口について述べたものです。正しくないものを 1 つ選択してください。

- (1) ウイルスは、セキュリティホール悪用型、ネットワーク感染型、マクロ感染型の 3 つのタイプに分類できる。
- (2) ウイルス自身が、送信者名を詐称してウイルスメールを大量に送信することがある。
- (3) 人の気を引くようなファイル名が付けられるケースがある。
- (4) 二重拡張子を使用したり、アイコンを偽装して、普通のファイルや別のプログラムを装うことがある。
- (5) ワクチンソフトを停止させてしまうようなウイルスも見つかっている。

問題 4

次の文章は、ウイルスの感染予防と駆除について述べたものです。正しくないものを 1 つ選択してください。

- (1) ワクチンソフトをインストールし、常に最新の定義ファイルに更新する。
- (2) メール添付ファイルは、開く前に必ずウイルス検査を実施する。
- (3) Web ブラウザのセキュリティレベルは中以上に設定するなど、アプリケーションのセキュリティ機能を活用する。
- (4) 添付ファイルの使用はできるだけ控え、Winny などの P2P ファイル交換ソフトを利用する。
- (5) セキュリティパッチをあて、セキュリティホールをふさぐ。

問題 5

次の文章は、ウイルス対策について述べたものです。正しいものを 1 つ選択してください。

- (1) ウイルスに感染したと思われるときは、すぐにコンピュータを停止、ネットワークへの接続を遮断し、システム管理者の指示を仰ぐ。
- (2) ワクチンソフトをインストールしていればウイルス対策は万全である。
- (3) ウイルス感染後、最も安全で確実な復旧方法は、ワクチンソフトを使用してシステムを修復する方法である。
- (4) ウイルスはデータファイルには感染しないので、データのバックアップは不要である。
- (5) インターネットサービスプロバイダ (ISP) のメールチェックサービスを利用すれば、ウイルスに感染することはない。

解答

問題番号	正解	参照先ページ番号
1	3	p.26 ~ 29
2	2	p.31 ~ 34
3	1	p.35 ~ 40 解説：(1)ウイルスは、これら 3 つのタイプの他にも、メール機能悪用型、ファイル感染型など様々なものがあります。
4	4	p.41 ~ 43 解説：(4)Winny などの P2P ファイル交換ソフト経由で感染するウイルスもありますので、注意が必要です。
5	1	p.45 ~ 47

第4章 実際のセキュリティ対策 ～まとめ編～

1. 個人レベルのセキュリティ対策

要点

- セキュリティホールの解消
- Web ブラウザのセキュリティレベルの設定
- ネットサーフィンの危険についての認識と対策
- メールソフトのセキュリティレベルの設定
- メールの暗号化とデジタル署名の利用
- 不審な添付ファイル、迷惑メールの取り扱いに対する注意
- 常時接続に伴う脅威の認識と対策

解説

要 点	参照ページ	解 説
セキュリティホールの解消	50	セキュリティホールの解消は、情報セキュリティ対策の第一歩です。 Windowsを使用している場合はWindows Updateを活用します。
Web ブラウザのセキュリティ設定	50	Web ブラウザにはセキュリティを設定する機能があります。標準設定のまま使用せず、不要なサービスや機能は積極的にオフにします。
ネットサーフィンの危険についての認識と対策	52～53	・安易なダウンロードやファイルの実行(ダブルクリック)はできるだけ避けるようにします。 不審なサイトにはアクセスしないことが肝要です。 クレジットカード番号などの個人情報を無闇に入力しないように気をつけます。特に、フィッシングには注意しましょう。個人情報を入力する場合は、必ずSSL通信であることを確認しましょう。
メールソフトのセキュリティの設定	52～53	メールソフトにもセキュリティを設定する機能があります。 標準設定のまま使用せず、不要なサービスや機能は積極的にオフにします。
メールの暗号化とデ	54	メールの暗号化とデジタル署名を使用することで、なり

デジタル署名の利用		すまし、改ざん、盗聴を防止できます。
不審な添付ファイル、迷惑メールの取り扱いに対する注意	54	<p>以下の基本方針を遵守します。</p> <ul style="list-style-type: none"> ・ 不審なメールの添付ファイル = 基本的に開かない ・ 迷惑メール = そのまま捨てる ・ 身に覚えのない請求メール等 = 専門家に相談、警察に届ける。 ・ デマメール、チェーンメール = 無視して、転送しない
常時接続に伴う脅威の認識と対策	54 ~ 55	<p>常時アクセス環境は、不正アクセスを受けやすいのでそれなりの対策が必要です。</p> <p>例えば、ルータの packets フィルタリングの機能を利用したり、パーソナルファイアウォールで対策を講じることが必要です。</p>

2. 企業レベルのセキュリティ対策

要点

計画フェーズ
 構築フェーズ
 運用フェーズ
 分析・見直しフェーズ
 個人情報保護対策
 セキュリティ事故への対処
 終わりのないプロセス

解説

要 点	参照ページ	解 説
対策の手順	56	<p>組織における情報セキュリティ対策は次のようなフェーズ（段階）により行います。</p> <ul style="list-style-type: none"> ・計画フェーズ ・構築フェーズ ・運用フェーズ ・分析・見直しフェーズ <p>セキュリティレベルの維持向上には、上記フェーズを継続して繰り返すことが肝要です。</p>
計画フェーズ	57～58	<p>セキュリティポリシーを策定する</p> <p>セキュリティポリシーとは、組織として一貫したセキュリティ対策を行うために、組織のセキュリティ方針と対策の基準を示したものです。基本方針、対策基準、実施手順の3階層で構成されます。</p> <p>対策事項を立案し、手順書を整備する</p> <p>対策基準とは、情報資産を脅威から守る方法を具体的に定めたものです。</p> <p>実施手順は、対策基準を実際の行動に移す際の手順書（マニュアルのようなもの）で、例えば次のようなものがあります。</p> <ul style="list-style-type: none"> ・最初に設定する内容とその手順 ・定期的実施する対策の手順 ・インシデント発生時の対策と手順
構築フェーズ	58～59	<p>情報セキュリティ対策の基本となる次のような設定を行います。</p>

		<ul style="list-style-type: none"> ・ファイアウォールの構築と設定 ・ソフトウェアの脆弱性をふさぐ ・レベルに応じたアクセス制御 <p>設定時は次の点に注意します。</p> <ul style="list-style-type: none"> ・デフォルト設定は非常に危険なので使用しない。 ・不要なサービスを停止する。
運用フェーズ	59～60	<p>運用時のポイントには、次のようなものがあります。</p> <ul style="list-style-type: none"> ・脆弱性情報を定期的にチェックする ・公開されたパッチを速やかに適用する ・セキュリティ教育を行う ・異動/退職社員のフォローをする
分析・見直しフェーズ	61	<p>ポリシーに基づいて、セキュリティ対策の実施状況を測定・評価する情報セキュリティ監査など、自社の対策状況のチェックや見直しを行い、改善すべきことがあれば、速やかに改善作業を行います。</p>
個人情報保護対策	61～62	<p>2005年4月から個人情報保護法が本格施行されたため、個人情報保護対策がますます重要になります。個人情報保護の基本5原則は次のとおりです。</p> <ul style="list-style-type: none"> ・利用目的による制限 ・適正な方法による取得 ・内容の正確性確保 ・安全管理措置の実施 ・透明性の確保
セキュリティ事故への対処	62～63	<p>セキュリティポリシーに則ったインシデント対応が必要です。インシデント対応を行うためには、事前に計画を定め、インシデント発生時の手順の確認や訓練が必要です。特に注意すべき点は次のとおりです。</p> <ul style="list-style-type: none"> ・被害状況を調査し、二次災害を防ぐ ・原因を特定し、再発防止策を徹底する ・実施した対応の記録、各種届出(必要な場合)を行う ・対応窓口を設置し、正確な情報を提供する
終わりのないプロセス	63	<p>セキュリティ対策は、一度、導入すればそれで終わり、というのではなく、運用、見直し、フィードバックを繰り返すプロセスが大事です。セキュリティ対策は、技術面、管理面両方を漏れなく行うことが必要です。</p>

第4章 実際のセキュリティ対策 ～演習編～

問題 1

次の文章は、個人レベルのセキュリティ対策について述べたものです。正しいものを1つ選択してください。

- (1) JavaScript、ActiveX コントロールなどは Web を活用するための優れた技術なので、これらの機能を常に有効（オン）にしておくことが推奨されている。
- (2) Web ブラウザのセキュリティを変更すると操作に支障がでることもあるので、Web ブラウザはできるだけデフォルト設定で使うことが望ましい。
- (3) ネットサーフィンを安全に楽しみたいときは、事前にワクチンソフトをインストールしておけばよい。
- (4) セキュリティホールがあると、ウイルス感染や不正アクセスを受ける原因となるので、セキュリティホールをふさぐことが情報セキュリティ対策の第一歩となる。
- (5) 迷惑メールやデマメールを受け取ったときは、二度と送信しないよう、送信者に抗議すべきである。

問題 2

次の文章は、ネットサーフィンと常時接続について述べたものです。正しくないものを1つ選択してください。

- (1) トロイの木馬やキーロガーは実行ファイル（拡張子が .exe のものなど）に含まれているので、実行ファイル以外ならダウンロードしてもかまわない。
- (2) 罾を仕掛けてユーザを待ち受けている Web サイトもあるので、不審なサイトにはできるだけアクセスしない方がよい。
- (3) クレジットカード番号などの個人情報を入力するときは SSL 接続されている（鍵がつながったアイコンがブラウザに表示される）ことを確認するようにしたい。
- (4) 常時接続のセキュリティ対策として、パケットフィルタリングやパーソナルファイアウォールを使用することが望ましい。
- (5) P2P アプリケーションやオンラインチャットでウイルスを送り込まれることがある。

問題 3

次の文章は、セキュリティポリシーの策定段階について述べたものです。正しくないものを1つ選択してください。

- (1) セキュリティポリシーの策定にあたっては、基本方針、対策基準、実施手順という3つの層に分けて考えるとよい。
- (2) 基本方針は頻繁に更新する性質のものではない。
- (3) セキュリティポリシー策定にあたっては、どの情報資産を守るかを決め、その情報資産に対するリスク分析を行う。
- (4) セキュリティポリシーの策定はセキュリティ技術をよく知っているシステム管理者に任

せておけばよい。

- (6) セキュリティポリシーの承認と宣言は、情報セキュリティの最高責任者である組織体の長が行う。

問題 4

次の文章は、企業レベルのセキュリティ対策について述べたものです。正しくないものを 1 つ選択してください。

- (1) アクセス制御は重要なので、構成員ごとにアクセス権を設定し、アクセスできる範囲や操作権限などを制御することが必要である。
- (2) 脆弱性対策は一度だけのものではなく、定期的なチェックとパッチの適用が肝要である。
- (3) 情報セキュリティ対策がポリシーどおりに実施されていることをチェックする情報セキュリティ監査は、外部の監査法人に依頼して実行する必要がある。
- (4) 従業員へのセキュリティ教育を行うなど、定めたセキュリティポリシーが遵守されるよう務めるべきである。
- (5) 退職した社員の ID・パスワードの削除は、退職後すぐに行うべきである。

問題 5

次の文章は、セキュリティ事故への対処について述べたものです。正しいものを 1 つ選択してください。

- (1) 被害の状況や範囲を調査し、二次災害がないと判断できれば報告の必要はなく、通常業務に戻ってよい。
- (2) 再発防止よりも原因究明に全力を注ぐことが重要だ。
- (3) インシデントは特別な事態なので、ポリシーを超えた臨機応変の対応が求められる。
- (4) インシデントに関する正確な情報を把握することは必須だが、外部への発表は対策が完了し、沈静化してからの方が望ましい。
- (5) 事故の発生はやむを得ないにしても、その後の対応姿勢によっては企業の倫理観まで問われることもあるので、インシデント対応の重要性を再確認したい。

解答

問題番号	正解	参照先ページ番号
1	4	p.50 ~ 55 解説：(1) JavaScript、ActiveX コントロールなどにより、Web 上のコンテンツの魅力を高めることができますが、これらの機能を有効（オン）にしていると、不正プログラムの自動ダウンロードなどの攻撃を受け

		ることがありますので、Web ブラウザのセキュリティの設定には、注意を払う必要があります。
2	1	p.50 ~ 55
3	4	p.57
4	3	p.57 ~ 61 解説：(3)外部の監査法人だけでなく、内部の監査部門に依頼することも可能です。
5	5	p.62 ~ 63

第5章 もっと知りたいセキュリティ技術 ~まとめ編~

1. アカウント、ID、パスワード

要点

- パスワードの重要性
- パスワードクラッキング
- パスワードを保護するための対策
- さまざまな認証方式

解説

要 点	参照ページ	解 説
パスワードの重要性	66	ID によって誰であることを識別し、パスワードによって本人であることを確認します。 パスワードが漏れいした瞬間からシステムやネットワークが脅威にさらされます。
パスワードクラッキング	66 ~ 67	攻撃者は、ソーシャルエンジニアリング、推測、不正ツールを使用した解析、盗聴、フィッシングなど様々な方法によりパスワードの入手を試みます。
パスワードを保護するための対策	67 ~ 68	次のような対策があります。 <ul style="list-style-type: none">・強度が高い(推測しにくい)パスワードを使用する・定期的にパスワードを変更する・絶対に人に教えない 参考： たかがパスワード、されどパスワード http://www.ipa.go.jp/security/crack_report/20020606/0205.html#spe1
さまざまな認証方式	68	<ul style="list-style-type: none">・本人しか知らない情報を入力(パスワードなど)・本人固有の持ち物(ワンタイムパスワード、スマートカードなど)・身体的特徴(バイオメトリクス)

2. ポートと脆弱性

要点

ポートとは何か

ポートと脆弱性

解説

要 点	参照ページ	解 説
ポートとは何か	69	インターネットで特定のサービスを通信させるための識別番号です。 提供するサービス(プロトコル)ごとに、使用するポートが決められているものがあります。 (例) <ul style="list-style-type: none">・WWW プロトコル (HTTP) : ポート 80 番・メール送信プロトコル (SMTP) : ポート 25 番・メール受信プロトコル (POP3) : ポート 110 番
ポートと脆弱性	70	使用しないポートは閉じるのが原則です。 (ポートを閉じる = サービスは停止する) 特定のサービスに脆弱性が発見されることがあります。その場合は、メーカーからセキュリティパッチが出たら、できるだけ早くパッチを適用するのが自衛策となります。

3. ファイアウォール

要点

ファイアウォールとは?

ファイアウォールの構成

パケットフィルタリング、アプリケーションゲートウェイ、プライベートアドレス
ネットワークアドレス変換技術 (NAT)

DMZ

ファイアウォールの落とし穴

パーソナルファイアウォール

解説

要 点	参照ページ	解 説
ファイアウォールとは?	71	インターネットなどの外部ネットワークと内部ネットワーク (LAN) などのネットワークの境界線上に設置し、アクセス制御などにより、保護したいネットワークを守る装置です。 ファイアウォールの主な機能 ・外部との出入り口を絞る ・内部ネットワーク (LAN) を外部に見せない ・外部からの不正なアクセスを排除する ・必要なアクセスだけを通過させる
ファイアウォールの構成	71	ネットワークの規模や目的に応じてさまざまな構成が可能です。 基本的な構成は P.72 の図 5.3 を参照して下さい。
パケットフィルタリング、アプリケーションゲートウェイ、プライベートアドレス	71 ~ 74	パケットフィルタリング パケットの情報に基づいて、通過させるパケットと通過させないパケットを選別します。通常は、通過を許可するパケットだけを指定し、あとは全て禁止とします。 アプリケーションゲートウェイ アプリケーションプロトコルに基づいてアクセスを制御します。 プライベートアドレス インターネットに接続する各機器ごとに、一意に割り当てられた IP アドレスを「グローバル IP アドレス」といいます。「グローバル IP アドレス」に対し、組織や

		<p>会社内の閉じられた空間で独自に割り当てられた IP アドレスを「プライベート IP アドレス」といいます。</p>
ネットワークアドレス変換技術 (NAT)	74	<p>内部のプライベート IP アドレスをグローバル IP アドレスに変換する技術です。</p> <p>NAT の利点</p> <ul style="list-style-type: none"> ・限られたグローバルアドレスの有効活用 ・内部情報を隠す ・外部からの直接的なアクセスを防ぐ
DMZ	74 ~ 75	<p>DMZ: DeMilitarized Zone: 非武装地帯。</p> <p>外部のインターネットと内部の LAN の間に設けた緩衝地帯です。通常公開サーバなどが設置されます。</p>
ファイアウォールの落とし穴	75 ~ 76	<p>ファイアウォールも万全ではありません。</p> <p>ファイアウォールを過信せず、必要に応じてできる限りのセキュリティ対策を行なうことが肝要です。</p>
パーソナルファイアウォール	76 ~ 77	<p>インターネットに常時接続する個人ユーザにとって、効果的なセキュリティ対策となります。</p> <p>Windows XP には簡易ファイアウォール機能がありますが、機能は限られています。また、さまざまなパーソナルファイアウォール製品が発売されています。</p> <p>個人ユーザもファイアウォール機能を積極的に活用しましょう。</p>

4. 暗号化とデジタル署名

要点

共通鍵暗号方式
 公開鍵暗号方式
 共通鍵方式と公開鍵方式の組み合わせ
 認証機関
 デジタル署名
 WWW での暗号化 (SSL)
 暗号化メール

解説

要 点	参照ページ	解 説
共通鍵暗号方式	79 ~ 80	<p>暗号化とは、万一、データの盗聴や漏えいが発生しても、第三者には内容が推測できない形にしておくことです。暗号化と復号に使用する鍵によって、暗号化方式が分けられます。</p> <ul style="list-style-type: none"> ・ 共通鍵暗号方式 ・ 公開鍵暗号方式 <p>共通鍵暗号方式では、暗号化と復号に同じ鍵を使用します。この鍵を共通鍵と呼びます。 (共通鍵暗号方式の例) DES、トリプル DES、RC4、RC5、AES など</p>
公開鍵暗号方式	80 ~ 82	<p>秘密鍵と公開鍵の 2 本の鍵 (ペア) を使用します。暗号化通信では、公開鍵を使用して暗号化し、秘密鍵を使用して復号します。 (公開鍵暗号方式の例) RSA、Diffie-Hellman など</p>
共通鍵方式と公開鍵方式の組み合わせとは？	82	<p>共通鍵暗号方式 最初の鍵の受け渡しが弱点 公開鍵暗号方式 暗号化と復号の処理速度が遅いという弱点 2 つを組み合わせることの利点 最初に、公開鍵暗号方式で共通鍵を送り、以降は共通鍵を使用して暗号化/復号することにより、弱点を克服します。</p>

認証機関	82 ~ 84	なりすましを防ぐために、第三の機関を設け、公開鍵の正当性を証明します。これを認証局と呼びます。
デジタル署名	84 ~ 85	送信者が本人であり、送信した内容が改ざんされていないことを検証する仕組みです。 秘密鍵を使用して署名する 対応する公開鍵で復号できるので、秘密鍵を持っている本人であることが証明されます。 ハッシュ関数によるメッセージダイジェストで改ざんを検証します。
WWW での暗号化 (SSL)	86	HTTP プロトコルでは、データがそのまま (平文で) 流れてしまい、内容を盗み見られるという危険があります。そのため、SSL によってデータを暗号化して送受信します。 SSL で接続されている時は、閉じた鍵マークがブラウザ上に表示されます。
暗号化メール	86 ~ 88	メールを暗号化してやり取りすることにより、メールの安全性を高める仕組みです。 盗聴の防止、改ざんの検証、なりすましの防止が可能になります。 メールの暗号化方式としては、PGP、S/MIME などがあります。

第5章 もっと知りたいセキュリティ技術 ~ 演習編 ~

問題 1

次の文章は、パスワードの安全性について述べたものです。正しいものを 1 つ選択してください。

- (1) パスワードは自分のデータを守るものなので、大切なデータが含まれていないシステムでは、簡単なパスワードで十分である。
- (2) パスワードは、同じものを使い続けるよりも、定期的に変えた方が安全性が高まる。
- (3) 最初に交付されたパスワードはランダムに生成されたものなので、安全性が高い。
- (4) パスワードを頻繁に変えると忘れてしまうことがあるので、推測しにくいパスワードを最初に設定して、それを使い続けるとよい。
- (5) ソーシャルエンジニアリングとは、パスワードクラッキングツールを使ってパスワードを解析する攻撃手法である。

問題 2

次の文章は、ポートについて述べたものです。正しくないものを 1 つ選択してください。

- (1) ポートとはインターネットにおいて特定のサービスを通信させるための識別番号である。
- (2) ポートを開くことにより、そのポートを介してサービスを提供できる。
- (3) 特定のプロトコルごとに、使用するポート番号があらかじめ決められているものもある。
- (4) 提供するサービスに脆弱性がある場合は、ポートの割り当て変更が最も有効である。
- (5) 使用しないポートを閉じておくことは、セキュリティ対策の原則である。

問題 3

次の文章は、ファイアウォールについて述べたものです。正しいものを 1 つ選択してください。

- (1) ファイアウォールはデフォルト設定で使うことが推奨されている。
- (2) ファイアウォールを正しく設定することにより、DoS 攻撃を効果的に防止できる。
- (3) ファイアウォールは、パケットフィルタリング、アプリケーションゲートウェイ、NAT などの機能があり、外部からの不正アクセスを防ぐ装置であるが、過信は禁物である。
- (4) インターネットからアクセスされる Web サーバを持たない組織では、ファイアウォールを設置する必要はない。
- (5) ファイアウォールはインターネットと社内 LAN を遮断するものなので、個人ユーザにはあまり役に立たない。

問題 4

次の文章は、IP アドレスとネットワークアドレス変換技術について述べたものです。正しくないものを1つ選択してください。

- (1) グローバル IP アドレスは、インターネットに接続する機器に一意に割り当てられた IP アドレスである。
- (2) プライベート IP アドレスは、組織や会社内の閉じられた空間で独自に割り当てられた IP アドレスである。
- (3) ネットワークアドレス変換技術は、内部のプライベート IP アドレスをグローバル IP アドレスに変換する技術である。
- (4) ネットワークアドレス変換技術を使用すると、プライベートアドレスが割り当てられた複数のコンピュータで1つのグローバルアドレスを共有できる。
- (5) ネットワークアドレス変換技術を使用すると、プライベートアドレスのままでインターネットにアクセスするので、限られたグローバルアドレスを有効活用できる。

問題 5

次の文章は、暗号化について述べたものです。正しいものを1つ選択してください。

- (1) 共通鍵暗号方式には、暗号化と復号の処理速度が、公開鍵暗号方式に比べて遅いという弱点がある。
- (2) 暗号化することにより、データの盗聴や漏えいが起きた場合でも、暗号が解読されない限り、内容が第三者に明らかになることはない。
- (3) 公開鍵暗号方式では、秘密鍵で暗号化し、公開鍵で復号することにより、データの機密性が確保される。
- (4) HTTP プロトコルでは、データを暗号化して送信するので、データの機密性が確保される。
- (5) 暗号技術の使用により、盗聴やなりすましを防止できるが、改ざん対策はできない。

解答

問題番号	正解	参照先ページ番号
1	2	p.66～68 解説：ソーシャルエンジニアリングについては、p.67 表 5.1「本人から入手する方法」の「説明」を参照して下さい。
2	4	p.69～70 解説：提供するサービスに脆弱性がある場合は、メーカーより提供されるセキュリティパッチを適用するのが一般的な対策となります。場合によってはポートの割り当て変

		更(80 番以外で WEB サービスを提供するなど)も行われますが、これが最も有効というわけではありません。
3	3	p.71 ~ 77 解説：(1)デフォルト設定とは、出荷時またはインストール後の初期状態の設定であり、デフォルト設定で使うことは、セキュリティ上問題があります。
4	5	p.73 ~ 74
5	2	p.79 ~ 84 解説：(4)データを暗号化して送信するのは、HTTPS プロトコルです。 (5)暗号技術の使用により、盗聴やなりすましを防止でき、改ざんを検出することができます。

第6章 情報セキュリティ関連の法規と制度 ～まとめ編～

1. 情報セキュリティの国際標準

要点

情報セキュリティマネジメントの国際標準 ISO/IEC 17799

セキュリティ製品の評価認証のための国際標準 ISO/IEC 15408

OECD セキュリティガイドライン

解説

要 点	参照ページ	解 説
ISO/IEC 17799	90	情報セキュリティマネジメントの国際標準。 情報セキュリティを守るためのベストプラクティスが記述されています。 BS7799 から ISMS 認証基準までの流れは、P90.の図 6.1 を参照して下さい。
ISO/IEC 15408	91	セキュリティ製品の評価認証のための国際標準。 機能要件（製品やシステムが備えるべき IT セキュリティに必要な機能）と保証要件（セキュリティ機能が確実に実現されていることを保証するための要件）の集大成。 日本では、ISO/IEC15408 に基づいて「IT セキュリティ評価及び認証制度」が運用されています。
OECD セキュリティガイドライン	92	1992 年、OECD（経済協力開発機構）により制定されました。OECD 加盟国が尊重すべき情報セキュリティの基本方針を制定したもので、5 年ごとに見直しが行なわれます。2002 年には大幅な見直しが行われ、全面改訂されました。

2. 情報セキュリティに関する法律

要点

刑法

不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）

電子署名及び認証業務に関する法律（電子署名法）

個人情報の保護に関する法律（個人情報保護法）

解説

要 点	参照ページ	解 説
刑法	93	1987年の改正で、コンピュータ犯罪を防止するため、次のものが犯罪として規定され、コンピュータの破壊やデータの改ざんが罰せられるようになりました。 <ul style="list-style-type: none">・電子計算機損壊等業務妨害罪・電磁的記録不正作出及び供用罪・電子計算機使用詐欺罪
不正アクセス禁止法	93	電気通信回線を通じて行われる不正アクセス犯罪を防止するために制定されました。この法律に則り、不正にアクセスする行為と不正アクセスを助長する行為が処罰の対象となります。
電子署名法	93～94	電子署名(デジタル署名)に署名や押印と同じ効力を持たせることを目的として制定されました。電子署名と電子証明書を規定し、さらに、認証業務や認証事業者についても規定しています。
個人情報保護法	94	個人の権利を保護するために、個人情報を取り扱う事業者の守るべき義務を規定するために制定されました。2005年4月には全面的に施行されました。本人の了解なしに個人情報の流用、売買、譲渡することを規制しています。「適正な方法による個人情報の取得」、「個人情報の収集目的の範囲内での利用」、「情報漏えいを防ぐためのセキュリティ対策の実施」などを規定しています。

3. 知的財産を守る法律

要点

著作権法
不正競争防止法

解説

要 点	参照ページ	解 説
著作権法	95	創作性のある思想や表現などの著作物や著作者を保護することが目的で制定されました。 著作権は、著作者人格権と著作財産権に分けられます。 著作者人格権 ・公表権、氏名表示権、同一性保持権 著作財産権 ・複製権、上演権、公衆送信権、口述権など
不正競争防止法	95	トレードシークレット(企業秘密)を保護することが目的の法律です。 第三者がトレードシークレットを不正に入手したり、不正使用することに対し、差止請求権、損害賠償請求権が認められました。

4. 迷惑メール関連法

要点

迷惑メール関連法

解説

要 点	参照ページ	解 説
迷惑メール関連法	96	2002年7月1日に施行された次の2つの法律を迷惑メール関連法といいます。 ・特定商取引に関する法律の改正 ・特定電子メールの送信の適正化等に関する法律 迷惑メール(スパムメール)の規制が目的です。

5. 情報セキュリティ関連制度

要点

ISMS 適合性評価制度

IT セキュリティ評価及び認証制度

プライバシーマーク制度

情報セキュリティ監査制度

コンピュータウイルス及び不正アクセスに関する届出制度

脆弱性関連情報に関する届出制度

解説

要 点	参照ページ	解 説
ISMS 適合性評価制度	97	組織の情報セキュリティマネジメントシステム（ISMS）が基準に適合しているかどうかを第三者機関が客観的に評価する制度です。
IT セキュリティ評価 及び認証制度	97	ISO/IEC 15408 に基づき、セキュリティ製品やシステムを評価・認証する制度です。 認証機関として IPA が指定されています。
プライバシーマーク 制度	97	個人情報保護の取り組みが適切であると認められた事業者に、それを認定するプライバシーマークの使用を許可する制度です。「個人情報保護に関するコンプライアンス・プログラムの要求事項 JIS Q 15001」に適合しているかどうかを認定します。
情報セキュリティ監 査制度	97～98	監査人が、組織の情報セキュリティ対策の状況を客観的に検証・評価し、保証及び助言を行う制度です。 情報セキュリティ監査を実施する際に準拠する基準として、情報セキュリティ管理基準と情報セキュリティ監査基準が策定されています。 情報セキュリティ監査を行う主体（企業等）を登録する情報セキュリティ監査企業台帳が創設されました。
コンピュータウイルス 及び不正アクセス に関する届出制度	98	経済産業省制定のコンピュータウイルス対策基準およびコンピュータ不正アクセス対策基準に基づき、コンピュータウイルスや不正アクセスの届出を受け付ける制度です。 届出を受け付ける機関として IPA が指定されています。

脆弱性関連情報に関する届出制度	98	経済産業省制定のソフトウェア等脆弱性関連情報取扱基準に基づく、ソフトウェア製品や Web アプリケーションの脆弱性に関する情報の届出を受け付ける制度です。 届出の受付機関として IPA が、調整機関として JPCERT/CC が指定されています。
-----------------	----	--

第6章 情報セキュリティ関連の法規と制度 ～演習編～

問題 1

次の文章は、情報セキュリティの国際標準について述べたものです。正しいものを 1 つ選択してください。

- (1) ISO/IEC 17799 は脆弱性情報の取り扱いを定めた国際標準である。
- (2) ISO/IEC 15408 は ISO/IEC 17799 から派生し、保証要件を含むよう拡張したものである。
- (3) ISO/IEC 15408 は、セキュリティ製品やシステムが適切に設計され、正しく実装されているかどうかを評価するための国際標準である。
- (4) ISO/IEC 15408 では、必要な機能要件をどこまで保証するのかを示す 5 段階の評価レベル (EAL) が定義されている。
- (5) OECD 情報セキュリティガイドラインは OECD 加盟国が尊重すべき情報セキュリティの基本方針で、毎年更新されている。

問題 2

次の文章は、情報セキュリティに関する法律について述べたものです。正しいものを 1 つ選択してください。

- (1) 1987 年の刑法改正で、個人情報の漏えいが刑法での罪に問われることになった。
- (2) 不正アクセス禁止法では、直接侵入は処罰できるが、踏み台などの間接攻撃は処罰できない。
- (3) 電子署名法の目的は、電子署名に署名や押印と同じ効力を持たせることである。
- (4) 個人情報保護法により、監督官庁への届出がない限り、事業者は個人情報を扱うことができなくなった。
- (5) 個人情報保護法は、2005 年 4 月からの本格施行により、法規制の対象が個人ユーザにも広がられた。

問題 3

次の文章は、知的財産を守る法律について述べたものです。正しいものを 1 つ選択してください。

- (1) 著作権法の目的は、「創作性」のある思想や表現などの著作物や著作者を保護することである。
- (2) 著作権法によって、プログラムやアルゴリズムなども著作物として保護される。
- (3) プログラムの不正コピーは著作財産権の侵害だが、CD の音源から作成した MP3 データはコピーではないので、著作財産権の侵害にはあたらない。
- (4) 不正競争防止法の目的は、著作権や商標権を持つ企業の重要な情報を保護することである。
- (5) 一般に広く知られているノウハウは著作権法の対象とはならないので、不正競争防止法で保護される。

問題 4

次の文章は、迷惑メール防止法について述べたものです。正しくないものを 1 つ選択してください。

- (1) 迷惑メールを規制する法律として、「不正アクセス禁止法」がある。
- (2) 迷惑メールを規制する法律として、「特定商取引に関する法律の改正」がある。
- (3) 迷惑メールを規制する法律として、「特定電子メールの送信の適正化等に関する法律」がある。
- (4) 迷惑メールを規制する法律により、宣伝や勧誘のメールを送る場合は、「未承諾広告」という表示や、送信者の氏名、名称、住所などを表示することが義務付けられた。
- (5) 迷惑メールを規制する法律では、架空電子メールアドレスへの送信は禁止されている。

問題 5

次の文章は、情報セキュリティ関連制度について述べたものです。正しくないものを 1 つ選択してください。

- (1) ISMS 適合性評価制度は、組織の情報セキュリティマネジメントシステムが基準に適合しているかどうかを第三者機関が客観的に評価する制度である。
- (2) IT セキュリティ評価及び認証制度では、認証機関として IPA が指定されている。
- (3) コンピュータウイルスや不正アクセスの届出を受け付ける機関として、IPA が指定されている。
- (4) 情報セキュリティ監査は、個人情報を取り扱う業者に年 1 回の情報セキュリティ監査を義務づけた制度である。
- (5) 脆弱性関連情報に関する届出制度では、調整機関として JPCERT/CC が指定されている。

解答

問題番号	正解	参照先ページ番号
1	3	p.90 ~ 92
2	3	p.93 ~ 94
3	1	p.95
4	1	p.96
5	4	p.97 ~ 98