

情報セキュリティ初級認定試験

《参考資料集》



I. 情報セキュリティ総論

1. 情報セキュリティの概要

(1) 情報セキュリティの7要素

JIS Q 27000:2014（情報技術—セキュリティ技術—情報セキュリティマネジメントシステム—用語）とJIS Q 13335-1:2006（情報技術—セキュリティ技術—情報通信技術セキュリティマネジメント—第1部：情報通信技術セキュリティマネジメントの概念及びモデル）との対応表を以下に示す。

用語	JIS Q 27000:2014	JIS Q 13335-1:2006
機密性	認可されていない個人、エンティティまたはプロセスに対して、情報を使用させず、また、開示しない特性。	認可されていない個人、エンティティまたはプロセスに対して、情報を使用不可または非公開にする特性。
完全性	正確さ及び完全さの特性。	資産の正確さ及び完全さを保護する特性。
可用性	認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。	認可されたエンティティが要求したときに、アクセス及び使用が可能である特性。
真正性	エンティティは、それが主張するとおりのものであるという特性。	ある主体または資源が、主張どおりであることを確実にする特性。真正性は、利用者、プロセス、システム、情報などのエンティティに対して適用する。
責任追跡性	※脚注 i	あるエンティティの動作が、その動作から動作主のエンティティまで一意に追跡できることを確実にする特性。
否認防止	主張された事象または処置の発生、及びそれを引き起こしたエンティティを証明する能力。	ある活動または事象が起きたことを、後になって否認されないように証明する能力。
信頼性	意図する行動と結果とが一貫しているという特性。	意図した動作及び結果に一致する特性。

※脚注 i : JIS Q 27000:2014「解説」より一部抜粋

責任追跡性、アカウンタビリティ (accountability) “accountability” については、引用元のJISで用いている用語との関係で、訳語を統一していない。JIS Q 27002との整合から、原則として“責任追跡性”と訳しているが、JIS Q 0073に合わせて“アカウンタビリティ”と訳している。“アカウンタビリティ”と訳した箇所では、情報セキュリティの分野における“責任追跡性”の意味ではなく、一般的な“責任”としての意味で使用されているため、訳し分けた。

(2) 情報セキュリティの関連用語の定義 (JIS Q 27000:2014)

①リスク

目的に対する不確かさの影響。

注記1 影響とは、期待されていることから、好ましい方向または好ましくない方向にかい（乖）離することをいう。

注記2 不確かさとは、事象、その結果またはその起こりやすさに関する、情報、理解または知識が、たとえ部分的にでも欠落している状態をいう。

注記3 リスクは、起こり得る事象、結果またはこれらの組合せについて述べることによって、その特徴を記述することが多い。

注記4 リスクは、ある事象（周辺状況の変化を含む）の結果とその発生の起こりやすさとの組合せとして表現されることが多い。

注記5 ISMSの文脈においては、情報セキュリティリスクは、情報セキュリティ目的に対する不確かさの影響として表現することがある。

注記6 情報セキュリティリスクは、脅威が情報資産のぜい弱性または情報資産グループのぜい弱性に付け込み、その結果、組織に損害を与える可能性に伴って生じる。

②ぜい弱性

一つ以上の脅威によって付け込まれる可能性のある、資産または管理策の弱点。

③脅威

システムまたは組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。

④情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象)、または予期しない単独もしくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。

(3) リスクマネジメントの関連用語の定義 (JIS Q 0073:2010)

① リスク

目的に対する不確かさの影響。

注記1 ※前述のJIS Q 27000:2014 注記1とほぼ同一の内容である。

注記2 目的は、例えば、財務、安全衛生、環境に関する到達目標など、異なった側面があり、戦略、組織全体、プロジェクト、製品、プロセスなど、異なったレベルで設定されることがある。

注記3 ※前述のJIS Q 27000:2014 注記3とほぼ同一の内容である。

注記4 ※前述のJIS Q 27000:2014 注記4とほぼ同一の内容である。

注記5 ※前述のJIS Q 27000:2014 注記2とほぼ同一の内容である。

② リスクアセスメント

リスク特定、リスク分析及びリスク評価のプロセス全体。

③ リスク特定

リスクを発見、認識及び記述するプロセス。

④ リスク分析

リスクの特質を理解し、リスクレベルを決定するプロセス。

⑤ リスク評価

リスク及び／またはその大きさが、受容可能かまたは許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス。

(4) リスク対応

リスク対応は、リスクコントロールとリスクファイナンス（リスクファイナンス）の手法に分類することもできるが、次の4つの手法に分類する場合もある。

① リスクの保有

特に対策を行わずに許容範囲として受容することであり、現状において実施すべきセキュリティ対策が見当たらない場合や、リスク対応の効果が得られない場合などにリスクを受容する。

② リスクの回避

リスクが発生する要因を排除することである。

③ リスクの移転

リスクを他社などに移転することである。

④ リスクの低減

ぜい弱性に対して対策を講じることにより、脅威の発生の可能性を下げることである。

(5) 脅威の分類

脅威の分類方法には、さまざまなものがある。

例えば、人為的脅威と環境的脅威に分類することができ、さらに人為的脅威を意図的脅威と偶発的脅威に分類することができる。

以下に、脅威の分類とその具体例を示す（JIS Q 13335-1:2006を参考に作成）。

人為的		環境的
意図的	偶発的	
・盗聴 ・情報の改ざん ・システムのハッキング ・悪意のあるコード ・盗難	・誤りやケアレスミス ・ファイルの削除 ・不正なルーティング ・物理的な事故	・地震 ・落雷 ・洪水 ・火災

2. 関連法規

(1) 刑法における、不正指令電磁的記録に関する罪

①不正指令電磁的記録作成・提供の罪

正当な目的がないのに、その使用者の意図とは無関係に勝手に実行されるようにする目的で、コンピュータウイルスやコンピュータウイルスのプログラム（ソースコード）を作成、提供する行為が該当する。この場合、3年以下の懲役または50万円以下の罰金に処せられる。

②不正指令電磁的記録供用の罪

正当な目的がないのに、コンピュータウイルスを、その使用者の意図とは無関係に勝手に実行される状態にした場合や、その状態にしようとした行為が該当する。この場合、3年以下の懲役または50万円以下の罰金に処せられる。

③不正指令電磁的記録取得・保管の罪

正当な目的がないのに、その使用者の意図とは無関係に勝手に実行されるようにする目的で、コンピュータウイルスやコンピュータウイルスのソースコードを取得、保管する行為が該当する。この場合、2年以下の懲役または30万円以下の罰金に処せられる。

(2) 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）の改正（平成24年）

①量刑の引き上げ

不正アクセス行為の禁止に違反した者は、1年以下の懲役または50万円以下の罰金から3年以下の懲役または100万円以下の罰金に改正された。

②準備行為の禁止

改正により、以下の準備行為が禁止となった。

- ・他人のID・パスワード等を不正に取得する行為（いわゆるフィッシング行為）
- ・不正に入手したID・パスワード等を他人に提供する行為
- ・他人のユーザID等を不正に保管する行為

（3）不正競争防止法における「営業秘密」

技術やノウハウ等の情報が「営業秘密」として不正競争防止法で保護されるためには、以下の3つの要件をすべて満たす必要がある。

①秘密管理性

秘密として管理されている情報であり、その情報に触れることができる者を制限することや、情報に触れた者にそれが秘密であると認識できることが必要である。

②有用性

有用な営業上または技術上の情報であることであり、有用性が認められるためには、その情報が客観的に有用であることが必要である。

③非公知性

公然と知られていないことであり、非公知性が認められるためには、保有者の管理下以外では一般に入手できないことが必要である。

（4）特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（プロバイダ責任制限法）

この法律は、特定電気通信による情報の流通によって権利の侵害があった場合について、特定電気通信役務提供者（プロバイダ、サーバの管理・運営者等）の損害賠償責任の制限及び発信者情報の開示を請求する権利等を定めるものである。

（5）特定電子メールの送信の適正化等に関する法律（特定電子メール法、迷惑メール防止法）

この法律は、宣伝・広告を目的とした電子メールのうち、受信者の同意のないものなどを規制するものであり、送信者の氏名及びメールアドレスの表示義務、架空電子メールアドレスへの送信禁止などが定められている。

平成20年の改正により、原則としてあらかじめ同意した者に対してのみ送信が認められる「オプトイン方式」が導入されるなど、迷惑メール対策への規制が強化された。

（6）著作権法における違法行為

以下のような行為は、著作権法における違法行為となる。

- ①販売または有料配信されている音楽や映像について、それが違法配信されたものであると知りながらダウンロードする行為
- ②DVDなどのコピー防止機能を解除して、自分のパソコンに取り込む（リッピング）行為
- ③DVDなどのコピー防止機能を解除するプログラムなどを作成・譲渡する行為
- ④個人的に利用する目的であっても、違法配信であることを知りながら、音楽や映像を録音または録画（ダウンロード）する行為
- ⑤個人的に利用する目的であっても、「海賊版」について、それが販売または有料配信されている音楽や映像であることと、違法配信されたものであることの両方を知りながら、自分のパソコンなどに録音または録画（ダウンロード）する行為

（７）個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（経済産業省）

「個人情報」及び「個人情報データベース等」に該当する事例として、以下のものが示されている。

①個人情報

事例１）本人の氏名

事例２）生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位または所属に関する情報について、それらと本人の氏名を組み合わせた情報

事例３）防犯カメラに記録された情報等本人が判別できる映像情報

事例４）特定の個人を識別できるメールアドレス情報（keizai_ichiro@meti.go.jp等のようにメールアドレスだけの情報の場合であっても、日本の政府機関である経済産業省に所属するケイザイチローのメールアドレスであることがわかるような場合等）

事例５）特定個人を識別できる情報が記述されていなくても、周知の情報を補って認識することにより特定の個人を識別できる情報

事例６）雇用管理情報（事業者が労働者等の雇用管理のために収集、保管、利用等する個人情報をいい、その限りにおいて、病歴、収入、家族関係等の機微に触れる情報を含む労働者個人に関するすべての情報が該当する）

事例７）個人情報を取得後に当該情報に付加された個人に関する情報（取得時に生存する特定の個人を識別することができなかったとしても、取得後、新たな情報が付加され、または照合された結果、生存する特定の個人を識別できた場合は、その時点で個人情報となる）

事例８）官報、電話帳、職員録等で公にされている情報（本人の氏名等）

なお、企業の財務情報等、法人等の団体そのものに関する情報（団体情報）や、記号や数字等の文字列だけから特定個人の情報であるか否かの区別がつかないメールアドレス情報については、「個人情報」に該当しないと示している。

②個人情報データベース等

事例1）電子メールソフトに保管されているメールアドレス帳（メールアドレスと氏名を組み合わせた情報を入力している場合）

事例2）ユーザIDとユーザが利用した取引についてのログ情報が保管されている電子ファイル（ユーザIDを個人情報と関連付けて管理している場合）

事例3）従業者が、名刺の情報を業務用パソコン（所有者を問わない）の表計算ソフト等を用いて入力・整理し、他の従業者等によっても検索できる状態にしている場合

事例4）人材派遣会社が登録カードを、氏名の五十音順に整理し、五十音順のインデックスを付してファイルしている場合

事例5）氏名、住所、企業別に分類整理されている市販の人名録

なお、従業者が、自己の名刺入れについて他人が自由に検索できる状況に置いていても、他人には容易に検索できない独自の分類方法により名刺を分類した状態である場合や、アンケートの戻りはがきが、氏名、住所等により分類整理されていない状態である場合は、「個人情報データベース等」に該当しないと示している。

③関連用語

・CPO（Chief Privacy Officer）

個人情報取扱事業者において、個人データの安全管理の実施及び運用に関する責任及び権限を有する者として任命される、個人情報保護管理者のことである。原則として、役員が任命される。

・管理委員会

個人情報取扱事業者において、CPOが責任者となり、社内の個人データの取扱いを監督する役割を果たす役割を担う。

④参考URL

個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン
http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf

3. 関連する認証制度

JIPDEC（一般財団法人日本情報経済社会推進協会）によって運用されている、プライバシーマーク制度及びISMS適合性評価制度の概要を、以下の表に示す。

	プライバシーマーク制度	ISMS適合性評価制度
目的 ※脚注 ii	消費者の目に見えるプライバシーマークで示すことによって、個人情報の保護に関する消費者の意識の向上を図ること。 適切な個人情報の取扱いを推進することによって、消費者の個人情報の保護意識の高まりにこたえ、社会的な信用を得るためのインセンティブを事業者に与えること。	わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としたものである。
認証取得単位	事業者全社単位	部門単位など
保護の対象	事業者が取扱う個人情報	組織が保護すべき情報資産
基準となる規格	JIS Q 15001:2006	JIS Q 27001:2014 ISO/IEC 27001:2014（国際規格）
維持・更新	有効期間は2年 更新審査は2年ごと	サーベイランス審査は通常1年ごと 再認証（更新）審査は3年ごと

※脚注 ii：以下の公式サイトより抜粋

ISMS <http://www.isms.jipdec.or.jp/about/index.html>

Pマーク http://privacymark.jp/privacy_mark/about/outline_and_purpose.html

Ⅱ. 情報資産に対する脅威と対策①

1. 物理的管理

(1) バイオメトリクス認証の方式

①指紋認証方式

読取り装置に直接触れて認証を行うため衛生面での課題があり、水分や傷などに左右される場合がある。技術の成熟度が高いこともあり、認証時のセンサー方式に感熱型や感圧式などの半導体式を採用した場合、他の方式と比較すると装置が小型で低コストでの導入が可能である。パソコンやスマートフォンなどでの認証に多く採用されている。

②静脈認証方式

装置に直接に触れずに認証が行えるため衛生的である。外見から認証情報が判断できず、認証情報は生涯変わらないことから、認証精度が高い。金融機関などでの認証に多く採用されている。

③虹彩認証方式

経年変化が少ないため認証精度は高いが、外見から認証情報を判断できる場合もあり、認証時には読取り装置の位置を調整する必要がある。

④顔認証方式

離れた場所からでも認証が可能であり、低解像度カメラの利用でも対応できる。しかし、環境に影響を受けやすく、顔の経年変化によって正しく認証されない場合もあり、その場合は認証情報の再登録が必要になる。

(2) 物理的セキュリティ関連用語

①セキュリティワイヤー

パソコンなどの機器を机などに固定するための器具であり、シリンダ錠やダイヤル錠などでロックする。これによって、パソコンなどの不正な持出しや盗難を防止することができるようになるだけでなく、製品によっては、使用していないポートを塞いで機器やケーブルの不正な接続などを防止することができるものもある。

②セキュリティキャビネット

従業員個々に付与しているIDカードで本人の認証を行うことにより、利用者の制限を行う。IDカードでの認証により、許可されるとキャビネットが解錠し、いつ・誰が・どの扉や引出しを開けたかの記録を残し、書類の持出しの管理を行う。また、閉め忘れや不正な解錠なども防止できる。

2. 人的管理の関連用語

(1) NDA (Non-disclosure agreement)

知り得た重要な情報を第三者に漏えいさせないことなどを約束させる目的で取り交わされるものであり、守秘義務契約や非開示契約などとも呼ばれる。

(2) ヒューマンエラー

誤入力や誤廃棄、開示の誤りなど、不注意による人為的なミスのことである。慣れていないツールを利用する場合や、作業結果の確認が容易にできない場合などに起こりやすい。

3. スマートフォンの盗難・紛失対策

- パスワードによる利用者認証を設定する。
- SIMカードの不正利用を防ぐため、PINコードによるロックを行う。
- キャリアで提供している、リモートからの強制ロックやデータ消去サービス、位置情報の確認サービスを利用する。
- リモートからの強制ロックや消去などの機能を持つ、専用のアプリケーションを利用する。
- 重要なデータは、本体やセットしているmicro SDカードには、安易に保存しない。
- 重要なデータは、本体やセットしているmicro SDカード以外の、別の媒体にバックアップを取る。
- 重要なデータを保存する場合、専用のアプリケーションを利用してデータの暗号化対策を行う。

4. バックアップサイト

(1) コールドサイト

必要最低限の機材と空調や無停電電源装置（UPS）などの設備環境のみの形態であり、災害発生時に必要な機材を搬入して設置・設定を行う形態である。

(2) ウォームサイト

稼働するための必要最低限のインフラ設備やシステムに関わるリソースが用意されていて、かつ、主要なシステムの稼働に必要な主要ハードウェアやソフトウェアの一式をあらかじめ保管してある形態であり、災害発生時にシステムを起動して運用を引き継ぐことが可能となる。

(3) ホットサイト

ITシステムに関わる機材が、すべて本運用とほぼ同じように設定されていて、データのバックアップを取りながら稼働状態で待機している形態であり、災害発生時に即時切替えが可能となる。

5. 事業継続

(1) BCP

事業継続計画のことである。自然災害などで企業が被災した場合、重要な事業を中断させない、もしくは中断しても可能な限り短期間で再開させ、中断に伴うシェアの低下や企業評価の低下などから企業を守るための方針や手続を示した計画のことである。

(2) BCM

事業継続管理のことである。自然災害や不測の事態によるさまざまなリスクに対して、迅速かつ効果的に対処し、事業活動の継続性を確保するための戦略的な運営管理手法である。緊急時における企業の事業継続に関して、事業継続計画の策定から導入・運用・見直しなどの継続的な改善活動を包括的に管理する。

6. 関連項目参考資料

(1) 事業継続ガイドライン ―あらゆる危機的事象を乗り越えるための戦略と対応― (内閣府)

企業・組織における、事業継続の取組みの必要性が示されている。実施が必要な事項、望ましい事項を記述することで、事業継続計画の策定・改善につながる事業継続マネジメントの普及促進を目指したものである。

<http://www.bousai.go.jp/kyoiku/kigyoku/pdf/guideline03.pdf>

(2) 情報システム安全対策基準（経済産業省）

情報システムの機密性、保全性及び可用性を確保することを目的として、自然災害、機器の障害、故意・過失等のリスクを未然に防止し、また、発生したときの影響の最小化及び回復の迅速化を図るため、情報システムの利用者が実施する対策項目を列挙したものである。

<http://www.meti.go.jp/policy/netsecurity/docs/regulations/esecu03j.pdf>

(3) 情報セキュリティ管理基準（経済産業省）

マネジメント基準と管理策基準から構成されている。

「マネジメント基準」では、情報セキュリティマネジメントの計画、実行、点検、処置に必要な実施事項を定めている。一方、「管理策基準」は、組織に情報セキュリティマネジメントの確立段階において、リスク対応方針に従って管理策を選択する際の選択肢を与えるものである。

なお、課題Ⅱのみならず、課題Ⅲでも参考となる。

http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard.pdf

Ⅲ. 情報資産に対する脅威と対策②

1. 不正プログラム（コンピュータウイルス）

（1）不正プログラムの種類

①ボット

感染したコンピュータを、インターネットを通じて外部から操るソフトウェアである。これに感染したコンピュータは、外部の指令サーバの配下でネットワークを形成し、その指示に従って、スパムメールの大量送信などの不正な活動を行う。このネットワークを、ボットネットという。

②ランサムウェア

正常に利用できないように、そのコンピュータのデータを人質にして、データの回復のための身代金を要求するソフトウェアである。データを暗号化して読み取れないようにし、身代金として代価を支払えば、復元するためのメッセージが送信されるといった手口がある。

③Hoax

デマウイルスのことであり、騒動を起こすことを目的として送信された、コンピュータウイルスに関するデマ情報のことである。

（2）不正プログラムへの対策

コンピュータウイルス対策基準（経済産業省）の「システムユーザ基準」において、次の事項が示されている。

a. ソフトウェア管理

- (1) ソフトウェアは、販売者又は配布責任者の連絡先及び更新情報が明確なものを入手すること。
- (2) オリジナルプログラムは、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。

b. 運用管理

- (1) 外部より入手したファイル及び共用するファイル媒体は、ウイルス検査後に利用すること。
- (2) ウイルス感染の被害が最小となるよう、システムの利用は、いったん初期状態にしてから行うこと。
- (3) ウイルス感染を早期に発見するため、システムの動作の変化に注意すること。
- (4) ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。

- (5) 不正アクセスによるウイルス被害を防止するため、パスワードは容易に推測されないように設定し、その秘密を保つこと。
- (6) 不正アクセスによるウイルス被害を防止するため、パスワードは随時変更すること。
- (7) 不正アクセスによるウイルス被害を防止するため、システムのユーザIDを共用しないこと。
- (8) 不正アクセスによるウイルス被害を防止するため、アクセス履歴を確認すること。
- (9) 不正アクセスによるウイルス被害を防止するため、機密情報を格納しているファイルを厳重に管理すること。
- (10) システムを悪用されないため、入力待ちの状態で放置しないこと。
- (11) ウイルス感染を防止するため、出所不明のソフトウェアは利用しないこと。
- (12) ウイルスの被害に備えるため、ファイルのバックアップを定期的に行い、一定期間保管すること。

c. 事後対応

- (1) ウイルスに感染した場合は、感染したシステムの使用を中止し、システム管理者に連絡して、指示に従うこと。
- (2) ウイルス被害の拡大を防止するため、システムの復旧は、システム管理者の指示に従うこと。
- (3) ウイルス被害の拡大を防止するため、感染したプログラムを含むフロッピーディスク等は破棄すること。

d. 監査

- (1) ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

※参考URL

①コンピュータウイルス対策基準

コンピュータウイルスに対する予防、発見、駆除、復旧等について実効性の高い対策をとりまとめたものである。

<http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm>

なお、この他、不正アクセスに関しては、次の基準が参考となる。

②コンピュータ不正アクセス対策基準（経済産業省）

不正アクセスによる被害の予防、発見、復旧、拡大及び再発防止について、企業等の組織及び個人が実行すべき対策をとりまとめたものである。

<http://www.meti.go.jp/policy/netsecurity/UAccessCMG.htm>

2. ネットワーク経由での攻撃の種類

(1) ドライブバイダウンロード攻撃

利用者の意図にかかわらず、Webサイト閲覧時にコンピュータウイルスなどを利用者のコンピュータに転送（ダウンロード）させて、不正プログラムの感染などを狙う攻撃であり、コンピュータのOSやアプリケーションなどに存在するぜい弱性を悪用して実行される。

(2) ゼロデイ攻撃

セキュリティ上のぜい弱性が発見されたときに、開発者側からパッチなどのぜい弱性への対策が提供されるより前に、そのぜい弱性について攻撃を仕掛けるものである

(3) 標的型攻撃

主に電子メールを用いて特定の組織や個人を狙う手法であり、典型的な例として、メール受信者の仕事に関係する話題を含む件名や本文で興味をひき、不正プログラムが埋め込まれた添付ファイルを開かせることを促し、不正プログラムに感染させるといった手口がある。また、不正なWebページを用意しておき、メールに記載されたURLをクリックさせてそのページに誘導し、認証情報などを詐取する手口もある。

(4) リロード攻撃

Webブラウザの再読み込み機能を何度も連続して行うことにより大量のページ送信要求を送り、Webサーバに過大な負荷をかけて停止させるなどの攻撃である。WebブラウザでF5キーを連打あるいは押しっぱなしにすることで攻撃ができることから、F5攻撃とも呼ばれている。

3. 無線LANの関連用語

(1) WPA、WPA2

Wi-Fi Allianceにより規格化されている、無線LANクライアントとアクセスポイントとの接続に関する認証方式及び通信内容の暗号化方式を包含した規格である。認証により利用権限のない無線LANクライアントの接続などを防止し、暗号化により通信内容の窃取及び改ざんを防止する。

WPA2は、米国標準技術局が定めた暗号化標準のAESを採用しており、128～256ビットの変長鍵を利用した、強力な暗号化が可能となっている。

(2) MACアドレスフィルタリング

接続できる無線端末を制限する機能であり、端末ごとに固有のMACアドレスをルータなどに登録することにより、許可されている端末のみ接続できるようにするためのものである。

なお、MACアドレスとはネットワーク機器固有のアドレスのことである。

(3) ESS-ID

無線端末が接続できるアクセスポイントを識別するために使用するIDであり、混信を避けるために付けられるネットワーク名のようなものである。

4. その他の関連用語

(1) SSL

インターネットなどのネットワーク上でデータを暗号化して送受信する仕組みであり、クレジットカード番号や、個人に関する機密性の高い情報を取り扱うWebサイトなどで、これらの情報が傍受されることを防ぐために広く利用されている。

(2) ファイアウォール

外部ネットワークと内部ネットワークの境界に設置し、外部からの攻撃や不正なアクセスなどから、内部ネットワークやコンピュータを防御するためのソフトウェアやハードウェアのことである。内外の通信を中継・監視することにより、不正アクセスなどを防御する。

(3) バックドア

不正侵入や攻撃を受けたコンピュータに仕掛けられた、裏の侵入経路のことである。侵入者が侵入後に、そのシステムに再侵入するために仕掛けておくものである。

IV. コンピュータの一般知識

1. ソフトウェア関連用語

(1) オートフィル

オートフィルとは、「月」、「火」、「水」… や、「1月」「2月」「3月」…のように、日付や数値など、規則性のあるデータを連続して自動的に入力する、表計算ソフトに搭載されている機能である。

(2) シェアウェア

ソフトウェアの流通形態の一つであり、一定の試用期間は料金を支払わずに利用することができる。試用期間後も継続して使用する場合は、入金してユーザ登録を行う。

(3) 拡張子

プログラムやデータはそれぞれ決められたファイル形式で保存され、固有の識別文字が付加される。これを拡張子という。例えば、Word 2010で作成したファイルには「.docx」の拡張子が付加されるが、これはWord 2010独自のファイル形式であることを表すものである。

2. ハードウェア関連用語

(1) テンポラリファイル

ソフトウェアが作業中のデータの保存のために、一時的に自動生成するものであり、一般的に、このファイルはソフトウェア終了と同時に消去される。

(2) バッチファイル

複数の処理をまとめて行うときに使われる、起動するプログラムを順に列挙したものである。

(3) デバイスドライバ

プリンタやスキャナなどの周辺機器を動作させるためのソフトウェアであり、OSが周辺機器を制御するための橋渡しを行う。単にドライバとも呼ばれている。

(4) ホットプラグ

コンピュータの電源を切らずに機器やケーブルを装着することであり、USBやIEEE1394、PCカードなどのインタフェースが対応している。

(5) Bluetooth

携帯電話やPDA、ノートパソコンなどを、ケーブルを使わずに接続して音声データや文字データなどをやりとりする短距離無線通信技術である。

(6) IrDA

ノートパソコンやプリンタ、デジタルカメラなどの外部通信機能として利用されている、無線（赤外線）のインタフェースである。

3. ファイル形式の種類

(1) TXT

文字コードのみで構成されたファイル形式であり、ほとんどのOSやアプリケーションソフトが読み込みや書出しに対応しているため、異なるアプリケーションソフト間でのデータの受け渡しに利用されている。

(2) CSV

主に表計算ソフトやデータベースソフトのテキストデータの保存形式として使用されているファイル形式であり、異なるアプリケーションソフト間でのデータの受渡しに利用される。

(3) PDF

文字情報だけではなく、フォントや文字のサイズ、文字飾り、埋め込まれた画像などの情報が保存できるファイル形式であり、コンピュータの機種や環境、OSなどに依存せずに、オリジナルとほぼ同じ状態で文章や画像などの閲覧が可能である。

(4) GIF

256色以下のカラーやモノクロ画像を圧縮するファイル形式であり、JPEG形式とともにWebページの標準形式として多く利用されている。

(5) BMP

Windowsが標準でサポートしている画像ファイル形式であり、白黒からカラーまでの色数を指定できるが、ファイルサイズが大きいためネットワーク上でのやりとりには適していない。

(6) EXE

Windowsなどの環境で実行できるプログラムが収められた形式のファイルであり、一般的に、ダブルクリックすることによりそのプログラムが起動できるようになっている。

4. パソコンで用いられる単位

(1) bps

データ通信や回線などにおける情報の通信速度の単位であり、1秒間に送ることができるbit（ビット）数を表すものである。

(2) dpi

ディスプレイの表示性能やプリンタの印刷精度、スキャナの読取り精度などを表す際の指標として用いられる単位であり、1インチあたりのドット数を表すものである。

(3) pixel

画像を構成する最小の単位であり、色調・階調・透明度などの色情報を持つ点を意味するものである。

5. ネットワーク及びコンピュータ技術の名称とその概要

(1) CGI

アクセスカウンタなどの動的なWebページの作成に用いられている、WebサーバがWebブラウザからの要求に応じてプログラムを起動するための仕組みである。

(2) ユビキタスコンピューティング

生活や社会の至る所にコンピュータが存在し、コンピュータ同士が自律的に連携して動作することにより、人間の生活を支援する情報環境のことである。

(3) RFID

物体の識別に必要な情報などが記録されている小型の無線ICチップが埋め込まれていて、電波や電磁波で管理システムと情報を送受信する仕組みである。バーコードとは異なり、離れた位置から処理できるほか、複数のタグを同時に認識でき、バーコードと比較すると多くの情報を持つことが可能である。ICタグ、無線タグや電子荷札、電子タグなどとも呼ばれることもある。

(4) POSシステム

販売時点情報管理とも呼ばれ、商品販売時にバーコードなどから商品情報を読み取り、商品の販売情報を記録するシステムである。店頭での販売動向をコンピュータでチェックし、在庫管理、商品搬入などを統合的に管理することができる。また、緻密な在庫管理や受発注管理ができるだけでなく、複数の店舗の販売動向を比較するなど、他のデータと連携した分析や活用が容易になるというメリットがある。

(5) QRコード

縦と横の二方向に情報を記録させたマトリックス型二次元コードであり、主に日本で広く普及している。その用途として、URLの情報をこのコードで表したものをスマートフォンや携帯電話に搭載されている対応カメラで接写して情報を読み取り、該当するWebサイトへ直接アクセスさせることなどが挙げられる。チラシや名刺などの印刷物だけではなく、在庫管理や入場管理など幅広い場面で採用されている。

例題

(過去問題より抜粋)

I. 情報セキュリティの総論

問1. 以下の文章は、情報セキュリティに関するさまざまな知識を述べたものです。正しいものは○、誤っているものは×としなさい。

1. 情報セキュリティの要素の一つである「機密性」の具体例として、Webサーバのデータの改ざん・破壊が行われていないことや、機器の設定内容が不正に書き換えられていないことなどが挙げられる。

《解説》情報セキュリティの要素の一つである「機密性」の具体例として、特定の人にユーザIDやパスワードを付与したり、アクセス権限を制限してアクセスできる人や機器を特定することなどが挙げられる。

なお、Webサーバのデータの改ざん・破壊が行われていないことや、機器の設定内容が不正に書き換えられていないことは、「完全性」の具体例である。

2. JIS Q 27000:2014において、「リスク」を、目的に対する不確かさの影響と定義している。なお、ここでの「影響」とは、期待されていることから、好ましい方向または好ましくない方向に乖離することをいう。

《解説》JIS Q 27000:2014において、「リスク」を、目的に対する不確かさの影響と定義している。

なお、ここでの「影響」とは、期待されていることから、好ましい方向または好ましくない方向に乖離することをいう。

3. 正当な目的がないのに、その使用者の意図とは無関係に勝手に実行されるようにする目的で、コンピュータウイルスやコンピュータウイルスのソースコードを作成し、または提供する行為は、刑法における不正指令電磁的記録作成等の罪に該当する。

《解説》正当な目的がないのに、その使用者の意図とは無関係に勝手に実行されるようにする目的で、コンピュータウイルスやコンピュータウイルスのソースコードを作成し、または提供する行為は、刑法における不正指令電磁的記録作成等の罪に該当する。

《解答 1－× 2－○ 3－○》

問2. 以下のA～Cについて答えなさい。

A. 以下の文章を読み、()に入る最も適切なものを、それぞれ下の選択肢(ア～エ)から1つ選びなさい。

1. リスク対応の一つであるリスク移転とは、()、他にリスクを移転する手法である。

ア：リスクが発生したときのために保険をかけるなどにより

イ：例えば、水害などが頻繁に発生する場合、データセンターをそのリスクの低い安全な場所と思われる場所に移設するなどにより

ウ：許容できるリスクのレベルを超えるものの、現状において実施すべきセキュリティ対策が見当たらない場合にそれを受け入れて

エ：リスクを保有することによって得られる利益に対して、保有することによるリスクの方が極端に大きい場合

《解説》リスク対応の一つであるリスク移転とは、リスクが発生したときのために保険をかけるなどにより、他にリスクを移転する手法である。

なお、例えば、水害などが頻繁に発生する場合、データセンターをそのリスクの低い安全な場所と思われる場所に移設することは、リスク回避の事例である。また、許容できるリスクのレベルを超えるものの、現状において実施すべきセキュリティ対策が見当たらない場合にそれを受け入れるのは、リスク保有の手法である。

2. ()に沿って個人情報保護を実践している事業者を認定し、プライバシーマークを付与するプライバシーマーク制度を運用している。

ア：JIPDECでは、ISO 10015:2005

イ：経済産業省では、JIS Q 0073:2009

ウ：JIPDECでは、JIS Q 15001:2006

エ：経済産業省では、ISO 9004:2000

《解説》JIPDECでは、JIS Q 15001:2006に沿って個人情報保護を実践している事業者を認定し、プライバシーマークを付与するプライバシーマーク制度を運用している。

《解答》 1ーア 2ーウ》

B. 以下の文章は、情報セキュリティに関する事柄についての説明です。文中の（ ）に当てはまる最も適切なものを、選択肢（ア～エ）から1つ選びなさい。

3. 個人情報取扱事業者は、個人データの取扱いを総括する部署の設置、及び社内の個人データの取扱いを監督する「管理委員会」を設置する。なお、「管理委員会」は、（ア：CTO イ：CPO ウ：情報システムセキュリティ責任者 エ：個人情報保護監査人）が責任者となることが望ましい。

《解説》個人情報取扱事業者は、個人データの取扱いを総括する部署の設置、及び社内の個人データの取扱いを監督する「管理委員会」を設置する。なお、「管理委員会」は、**CPO**が責任者となることが望ましい。

CPO（Chief Privacy Officer）とは、個人データの安全管理の実施及び運用に関する責任及び権限を有する者であり、個人情報保護管理者とも呼ばれる。

C. 次の問いに対応するものを、各選択肢（ア～エ）から1つ選びなさい。

4. JIS Q 27000:2014における情報セキュリティの要素の定義として、誤っているものはどれか。

ア：「真正性」とは、正確さ及び完全さの特性である。

イ：「可用性」とは、認可されたエンティティが要求したときに、アクセス及び使用が可能である特性である。

ウ：「機密性」とは、認可されていない個人、エンティティまたはプロセスに対して、情報を使用させず、また、開示しない特性である。

エ：「否認防止」とは、主張された事象または処置の発生、及びそれを引き起こしたエンティティを証明する能力である。

《解説》JIS Q 27000:2014において、情報セキュリティの要素を、それぞれ次のように定義している。

ア：誤った記述である。

正確さ及び完全さの特性と定義されているのは、「完全性」である。

なお、「真正性」とは、エンティティは、それが主張するとおりのものであるという特性である。

イ：正しい記述である。

「可用性」とは、認可されたエンティティが要求したときに、アクセス及び使用が可能である特性である。

ウ：正しい記述である。

「機密性」とは、認可されていない個人、エンティティまたはプロセスに対して、情報を使用させず、また、開示しない特性である。

エ：正しい記述である。

「否認防止」とは、主張された事実または処置の発生、及びそれを引き起こしたエンティティを証明する能力である。

5. 情報セキュリティの関連法規に関する記述のうち、誤っているものはどれか。

- ア：民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（e-文書法）は、法令により、民間事業者に対して書面による保存が義務付けられている書類や帳票類を、電子データとして保存することを認める法律である。
- イ：特定電子メールの送信の適正化等に関する法律（特定電子メール法）は、宣伝や広告を目的とした電子メールのうち、受信者の同意のないものなどを規制する法律であり、送信者の氏名・メールアドレスの表示義務、架空電子メールアドレスへの送信禁止などが規定されている。
- ウ：コンピュータを使った情報解析のために、必要と認められる限度において、著作物を複製する行為は、著作権法に抵触しない。
- エ：特許法に規定される発明は、自然法則を利用した技術的思想の創作のうち高度のものであるため、コンピュータシステムを利用して生成する暗号は、同法において保護の対象とはならない。

《解説》

ア：正しい記述である。

民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律（e-文書法）は、法令により、民間事業者に対して書面による保存が義務付けられている書類や帳票類を、電子データとして保存することを認める法律である。

イ：正しい記述である。

特定電子メールの送信の適正化等に関する法律（特定電子メール法）は、宣伝や広告を目的とした電子メールのうち、受信者の同意のないものなどを規制する法律であり、送信者の氏名・メールアドレスの表示義務、架空電子メールアドレスへの送信禁止などが規定されている。

ウ：正しい記述である。

コンピュータを使った情報解析のために、必要と認められる限度において、著作物を複製する行為は、著作権法に抵触しない。

エ：誤った記述である。

特許法に規定される発明は、自然法則を利用した技術的思想の創作のうち高度のものである。なお、コンピュータシステムを利用して生成する暗号は、コンピュータという自然法則にもとづいて動作するアルゴリズムを利用していることから、同法において保護の対象となる。

Ⅱ．情報資産に対する脅威と対策①

問1．以下の文章は、情報セキュリティに関するさまざまな知識を述べたものです。正しいものは○、誤っているものは×としなさい。

- 1．バックアップシステムの運用方式の一つであるコールドサイトは、システム障害や大規模自然災害などが発生した際に備え、本運用とほぼ同じシステムを導入し、常時データの複製などを行いながら稼動状態で待機させる形態である。

《解説》バックアップシステムの運用方式の一つであるコールドサイトは、システム障害や大規模自然災害などが発生した際に備え、必要最低限の機材と空調や電源などの設備環境のみの形態であり、災害発生時に必要な機材を搬入して設置・設定を行う形態である。
なお、本運用とほぼ同じシステムを導入し、常時データの複製などを行いながら稼動状態で待機させる形態は、ホットサイトである。

- 2．非開示契約とは、知り得た重要な情報を第三者に漏えいさせないことなどを約束させる目的で取り交わされるものであり、SLAや守秘義務契約などとも呼ばれる。

《解説》非開示契約とは、知り得た重要な情報を第三者に漏えいさせないことなどを約束させる目的で取り交わされるものであり、NDA（Non-disclosure agreement）や守秘義務契約などとも呼ばれる。

- 3．BCMとは、緊急時における企業の事業継続に関して、事業継続計画の策定から導入・運用・見直しなどの継続的な改善活動を包括的に管理することであり、事業継続管理とも呼ばれる。

《解説》BCM（Business Continuity Management）とは、緊急時における企業の事業継続に関して、事業継続計画の策定から導入・運用・見直しなどの継続的な改善活動を包括的に管理することであり、事業継続管理とも呼ばれる。

《解答 1－× 2－× 3－○》

問2. 以下のA～Cについて答えなさい。

A. 以下の文章は、情報セキュリティに関する事柄についての説明です。文中の（ ）に当てはまる最も適切なものを、各選択肢（ア～エ）から1つ選びなさい。

1. 脅威を環境的脅威と人為的脅威に分類し、さらに、人為的脅威を意図的脅威と偶発的脅威に分類した場合、（ア：改ざん イ：のぞき見 ウ：記録媒体の劣化 エ：人的リソース不足）や誤った上書きは、偶発的脅威に分類される。

《解説》脅威を環境的脅威と人為的脅威に分類し、さらに、人為的脅威を意図的脅威と偶発的脅威に分類した場合、人的リソース不足や誤った上書きは、偶発的脅威に分類される。

なお、改ざんやのぞき見は意図的脅威、記録媒体の劣化は環境的脅威に分類される。

2. バイオメトリクス認証方式の一つである（ア：虹彩 イ：静脈 ウ：指紋 エ：掌形）認証方式は、認証情報の登録不可能な人は少なく、非接触での認証が可能であるため、衛生的である。また、乾燥や湿気などの外的要因による認証情報の読取りに関する影響は低く、認証情報は、外見で判断することができず偽造が困難である。

《解説》バイオメトリクス認証方式の一つである静脈認証方式は、認証情報の登録不可能な人は少なく、非接触での認証が可能であるため、衛生的である。また、乾燥や湿気などの外的要因による認証情報の読取りに関する影響は低く、認証情報は、外見で判断することができず偽造が困難である。

B. 以下の文章を読み、（ ）に入る最も適切なものを、下の選択肢（ア～エ）から1つ選びなさい。

3. 内閣府の「事業継続ガイドライン」において、BCP策定や維持・更新、事業継続を実現するための予算・資源の確保、事前対策の実施、取組みを浸透させるための教育・訓練の実施、点検、継続的な改善などを行う（ ）を、BCMと呼ぶと示している。

ア：サプライチェーンに関する管理計画

イ：平常時からのマネジメント活動

ウ：緊急時に招集する事業継続に関する組織委員会

エ：緊急時に検討すべき対応策

《解説》内閣府の「事業継続ガイドライン」において、BCP策定や維持・更新、事業継続を実現するための予算・資源の確保、事前対策の実施、取組みを浸透させるための教育・訓練の実施、点検、継続的な改善などを行う平常時からのマネジメント活動を、BCMと呼ぶと示している。

なお、BCP（Business Continuity Plan）は事業継続計画、BCM（Business Continuity Management）は事業継続管理を指すものである。

C. 次の問いに対応するものを、各選択肢（ア～エ）から1つ選びなさい。

4. 経済産業省の「情報システム安全対策基準」における「設置基準」に関する記述のうち、誤っているものはどれか。

- ア：建物は、落雷の被害を受ける恐れのない場所に設けること。また、建物及び室は、電界及び磁界の被害を受ける恐れのない場所に設けること。
- イ：外部及び共用部分に面する窓は、防災措置を講ずること。また、外部より容易に接近しうる窓は、防犯措置を講ずること。
- ウ：建物は、建築基準法に規定する耐震構造とすること。また、建物及び室の窓ガラスは、破損、飛散及び落下防止の措置を講ずること。
- エ：情報システムは、設置位置に応じた移動、転倒及び振動防止の措置を講ずること。災害時にバックアップするための情報システムを設置する場合は、近隣の別棟に設置すること。

《解説》経済産業省の「情報システム安全対策基準」における「設置基準」では、次のような具体策を示している。

ア：正しい記述である。

建物は、落雷の被害を受ける恐れのない場所に設けること。また、建物及び室は、電界及び磁界の被害を受ける恐れのない場所に設けること。

イ：正しい記述である。

外部及び共用部分に面する窓は、防災措置を講ずること。また、外部より容易に接近しうる窓は、防犯措置を講ずること。

ウ：正しい記述である。

建物は、建築基準法に規定する耐震構造とすること。また、建物及び室の窓ガラスは、破損、飛散及び落下防止の措置を講ずること。

エ：誤った記述である。

情報システムは、設置位置に応じた移動、転倒及び振動防止の措置を講ずること。災害時にバックアップするための情報システムを設置する場合は、遠隔地に設置すること。

《解答 1－エ 2－イ 3－イ 4－エ》

5. 経済産業省の「情報セキュリティ管理基準」における「情報の分類」に関する記述のうち、誤っているものはどれか。

ア：情報を共有または制限する業務上の必要、及びこのような必要から起こる業務上の影響を考慮し、情報の分類及び関連する保護管理策を策定する。

イ：分類の指針には、あらかじめ決められたアクセス制御方針に従った最初の分類及び時間が経ってからの再分類に関する取扱いを含める。

ウ：資産の利用者の個々の判断で資産の分類を定め、定期的にそれをレビューし、それを最新の状態で、かつ、適切なレベルで維持することを確実にする仕組みを整備する。

エ：分類項目の数及びそれらの利用で得られる効用（経済性または実用性など）を考慮し、情報を分類する。

《解説》経済産業省の「情報セキュリティ管理基準」における「情報の分類」では、次のような具体策を示している。

ア：正しい記述である。

情報を共有または制限する業務上の必要、及びこのような必要から起こる業務上の影響を考慮し、情報の分類及び関連する保護管理策を策定する。

イ：正しい記述である。

分類の指針には、あらかじめ決められたアクセス制御方針に従った最初の分類及び時間が経ってからの再分類に関する取扱いを含める。

ウ：誤った記述である。

資産の管理責任者の責任で、資産の分類を定め、定期的にそれをレビューし、それを最新の状態で、かつ、適切なレベルで維持することを確実にする仕組みを整備する。

エ：正しい記述である。

分類項目の数及びそれらの利用で得られる効用（経済性または実用性など）を考慮し、情報を分類する。

Ⅲ. 情報資産に対する脅威と対策②

問1. 以下の文章は、情報セキュリティに関するさまざまな知識を述べたものです。正しいものは○、誤っているものは×としないさい。

1. HOAXとは、ネットワークを通じて他のコンピュータに伝染することを目的とした不正プログラムであり、電子メールの添付ファイルとして自動的に自分自身のコピーを拡散させるものや、ネットワークを利用して次々に感染していくものなどがある。

《解説》ネットワークを通じて他のコンピュータに伝染することを目的とした不正プログラムはワームであり、電子メールの添付ファイルとして自動的に自分自身のコピーを拡散させるものや、ネットワークを利用して次々に感染していくものなどがある。

なお、HOAXとは、デマウィルスのことであり、騒動を起こすことを目的として送信された、コンピュータウィルスに関するデマ情報のことである。

2. SSLとは、インターネットなどのネットワーク上でデータを暗号化して送受信する仕組みであり、クレジットカード番号や、個人に関する機密性の高い情報を取り扱うWebサイトなどで、これらの情報が傍受されることを防ぐために広く利用されている。

《解説》SSLとは、インターネットなどのネットワーク上でデータを暗号化して送受信する仕組みであり、クレジットカード番号や、個人に関する機密性の高い情報を取り扱うWebサイトなどで、これらの情報が傍受されることを防ぐために広く利用されている。

3. DoS攻撃またはDDoS攻撃とは、大量のパケットをサーバに送りつけて、サーバが他の処理を実行できないような状態にして、正規のユーザからのアクセスを受け付けられないようにする攻撃である。その手法としてSYNフラッド攻撃や反射攻撃、オンライン攻撃、ゼロデイ攻撃などがある。

《解説》DoS攻撃またはDDoS攻撃とは、大量のパケットをサーバに送りつけて、サーバが他の処理を実行できないような状態にして、正規のユーザからのアクセスを受け付けられないようにする攻撃である。その手法としてSYNフラッド攻撃やLAND、TEAR DROP、Ping of Deathなどがある。

なお、オンライン攻撃とは、動作しているコンピュータにユーザIDとパスワードを順に送っていき、認証に成功するかどうかを調べる手法のことである。また、ゼロデイ攻撃とは、セキュリティ上のぜい弱性が発見されたときに、開発者側からパッチなどのぜい弱性への対策が提供される前から、そのぜい弱性について攻撃を仕掛けるものである。

《解答》 1－× 2－○ 3－×》

問2. 以下のA～Cについて答えなさい。

A. 以下の文章は、情報セキュリティに関する事柄についての説明です。文中の（ ）に当てはまる最も適切なものを、各選択肢（ア～エ）から1つ選びなさい。

1. （ア：ゼロデイアタック イ：リプレイアタック ウ：ドライブバイダウンロード攻撃 エ：LAND攻撃）とは、Webサイト閲覧時に、利用者の意図にかかわらずコンピュータウイルスなどをダウンロードさせて、不正プログラムの感染などを狙う攻撃であり、コンピュータのOSやアプリケーションなどに存在するぜい弱性を悪用して実行される。

《解説》 ドライブバイダウンロード攻撃とは、Webサイト閲覧時に、利用者の意図にかかわらずコンピュータウイルスなどをダウンロードさせて、不正プログラムの感染などを狙う攻撃であり、コンピュータのOSやアプリケーションなどに存在するぜい弱性を悪用して実行される。

なお、ゼロデイアタックとは、セキュリティ上のぜい弱性が発見されたときに、開発者側からパッチなどのぜい弱性への対策が提供される前から、そのぜい弱性を突いて攻撃を仕掛けるものである。

2. 無線LANの有効な情報セキュリティの方式として、Wi-Fi Allianceにより規格化されている（ア：WPA2 イ：WEP ウ：DSA エ：RSA）があり、米国標準技術局が定めたAESを採用しており、128～256ビットの可変長かぎを利用した強力な暗号化が可能となっている。

《解説》無線LANの有効な情報セキュリティの方式として、Wi-Fi Allianceにより規格化されているWPA2があり、米国標準技術局が定めたAESを採用しており、128～256ビットの可変長かぎを利用した強力な暗号化が可能となっている。

なお、WEPとは、無線LANで使用される暗号化技術の一つであり、暗号化アルゴリズムにはRC4を採用していて、アクセスポイントごとに決められている共通かぎとパケットごとにランダムな24bitのIVを使う。ただし、IVの長さが十分ではなく、ある程度の時間があれば暗号の解読が可能になってしまうという問題点がある。

《解答》 1ーウ 2ーア》

B. 次の問いに対応するものを、選択肢（ア～エ）から1つ選びなさい。

3. 以下の文章は、不正プログラムに関する説明です。該当する名称は、次のうちどれか。

システムのセキュリティを回避するように設計されたプログラムであり、多くの場合、有益なソフトウェアだとユーザに信じ込ませ、実行するように仕向ける。ファイルやディスク内容を破壊したり、プログラムのソースコードのコピーを利用して侵入のための裏口を開けるなどの、セキュリティ侵害を行うものがある。なお、感染機能は持っていないため、感染増殖することはない。

ア：ランサムウェア イ：ボット ウ：トロイの木馬 エ：コードレッド

《解説》以下の内容に該当する不正プログラムの名称は、トロイの木馬である。

システムのセキュリティを回避するように設計されたプログラムであり、多くの場合、有益なソフトウェアだとユーザに信じ込ませ、実行するように仕向ける。ファイルやディスク内容を破壊したり、プログラムのソースコードのコピーを利用して侵入のための裏口を開けるなどの、セキュリティ侵害を行うものがある。なお、感染機能は持っていないため、感染増殖することはない。

なお、ボットとは、インターネットを通じてコンピュータを外部から操る不正なプログラムであり、これに感染したコンピュータは、自らネットワークを通じて外部の指令サーバと通信を行い、外部からの指示により、迷惑メールの大量送信や、特定サイトへの一斉攻撃などを行う。

C. 次の問いに対応するものを、各選択肢（ア～エ）から1つ選びなさい。

4. 経済産業省の「コンピュータウイルス対策基準」の「システムユーザ基準」に関する記述のうち、誤っているものはどれか。

ア：ソフトウェア管理において、ソフトウェアは、販売者または配布責任者の連絡先及び更新情報が明確なものを入手すること。

イ：運用管理において、ウイルス感染を早期に発見するため、複数のワクチンを利用した方法で集中的に、かつ断続的にウイルス検査を行うこと。

ウ：運用管理において、不正アクセスによるウイルス被害を防止するため、機密情報を格納しているファイルを厳重に管理すること。

エ：事後対応において、ウイルスに感染した場合は、感染したシステムの使用を中止し、システム管理者に連絡して、指示に従うこと。

《解説》経済産業省の「コンピュータウイルス対策基準」の「システムユーザ基準」では、次のような具体策を示している。

ア：正しい記述である。

ソフトウェア管理において、ソフトウェアは、販売者または配布責任者の連絡先及び更新情報が明確なものを入手すること。

イ：誤った記述である。

運用管理において、ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。

ウ：正しい記述である。

運用管理において、不正アクセスによるウイルス被害を防止するため、機密情報を格納しているファイルを厳重に管理すること。

エ：正しい記述である。

事後対応において、ウイルスに感染した場合は、感染したシステムの使用を中止し、システム管理者に連絡して、指示に従うこと。

5. 経済産業省の「コンピュータ不正アクセス対策基準」における「システムユーザ基準」に関する記述のうち、誤っているものはどれか。

- ア：他人のパスワードを知った場合は、速やかにシステム管理者に通知すること。また、ユーザIDを利用しなくなった場合は、速やかにシステム管理者に届け出ること。
- イ：コンピュータ及び通信機器を維持、保守するために必要なファイルは、盗用、改ざん、削除等されないように厳重に管理すること。
- ウ：コンピュータ、通信機器及びソフトウェアの導入、更新、撤去等を行う場合は、自己の判断により行い、かつ、自己の責任のもとで行うこと。
- エ：コンピュータを入力待ち状態で放置しないこと。また、コンピュータが無断で利用された形跡がないか、利用履歴等を随時確認すること。

《解説》経済産業省の「コンピュータ不正アクセス対策基準」における「システムユーザ基準」では、次のような具体策を示している。

ア：正しい記述である。

他人のパスワードを知った場合は、速やかにシステム管理者に通知すること。また、ユーザIDを利用しなくなった場合は、速やかにシステム管理者に届け出ること。

イ：正しい記述である。

コンピュータ及び通信機器を維持、保守するために必要なファイルは、盗用、改ざん、削除等されないように厳重に管理すること。

ウ：誤った記述である。

コンピュータ、通信機器及びソフトウェアの導入、更新、撤去等を行う場合は、システム管理者の指導の下で行うこと。

エ：正しい記述である。

コンピュータを入力待ち状態で放置しないこと。また、コンピュータが無断で利用された形跡がないか、利用履歴等を随時確認すること。

Ⅳ. コンピュータの一般知識

問1. 以下の文章を読み、正しいものには○、誤っているものには×で答えなさい。

1. MIDIファイルとは、文字コードのみで構成されたファイルであり、ほとんどのOSやアプリケーションソフトが読み込みや書き出しに対応しているため、異なるアプリケーションソフト間でのデータの受け渡しに利用されている。

《解説》TXTファイルとは、文字コードのみで構成されたファイルであり、ほとんどのOSやアプリケーションソフトが読み込みや書き出しに対応しているため、異なるアプリケーションソフト間でのデータの受け渡しに利用されている。

2. bpsとは、データ通信や回線などにおける情報の通信速度の単位であり、1秒間に送ることができるbit（ビット）数を表すものである。

《解説》bpsとは、データ通信や回線などにおける情報の通信速度の単位であり、1秒間に送ることができるbit（ビット）数を表すものである。

3. プログラムやデータはそれぞれ決められたファイル形式で保存され、固有の識別文字が付加される。これを拡張子という。例えば、Word 2010で作成したファイルには「.docx」の拡張子が付加されるが、これはWord 2010独自のファイル形式であることを表すものである。

《解説》プログラムやデータはそれぞれ決められたファイル形式で保存され、固有の識別文字が付加される。これを拡張子という。例えば、Word 2010で作成したファイルには「.docx」の拡張子が付加されるが、これはWord 2010独自のファイル形式であることを表すものである。

《解答 1－× 2－○ 3－○》

問2. 次の問いに対応するものを、各選択肢（ア～エ）から1つ選びなさい。

1. 複数の処理をまとめて行うときに使われる、起動するプログラムを順に列挙したものは、次のうちどれか。

ア：バッチファイル

イ：イメージファイル

ウ：テンポラリファイル

エ：パターンファイル

《解説》複数の処理をまとめて行うときに使われる、起動するプログラムを順に列挙したものは、バッチファイルである。

なお、テンポラリファイルとは、ソフトウェアが作業中のデータの保存のために、一時的に自動生成するものであり、一般的に、このファイルはソフトウェア終了と同時に消去される。

2. 動画像の符号化方式を策定する組織及びその符号化方式の名称は、次のうちどれか。

ア：PICT

イ：EXE

ウ：MPEG

エ：JPEG

《解説》動画像の符号化方式を策定する組織及びその符号化方式の名称は、MPEGである。

なお、EXEは、Windowsなどの環境で実行できるプログラムが収められたファイル形式であり、JPEGは、静止画像の圧縮方式を策定する組織及びその圧縮方式の名称である。

3. マウスやキーボードなどの周辺機器を動作させるためのソフトウェアのことで、OSが周辺機器を制御するための橋渡しを行うものは、次のうちどれか。

ア：ウィジェット

イ：ファームウェア

ウ：デバイスドライバ

エ：テンポラリファイル

《解説》マウスやキーボードなどの周辺機器を動作させるためのソフトウェアはデバイスドライバであり、OSが周辺機器を制御するための橋渡しを行う。

なお、テンポラリファイルとは、作業中のデータの保存のためにソフトウェアが一時的に自動生成するファイルである。

《解答》 1ーア 2ーウ 3ーウ

4. Windowsなどの環境で実行できるプログラムが収められたファイルの形式は、次のうちどれか。

ア : EXE

イ : CSV

ウ : SGML

エ : BMP

《解説》Windowsなどの環境で実行できるプログラムが収められたファイルの形式は、**EXE**である。

なお、CSVは、主に表計算ソフトやデータベースソフトのテキストデータの保存形式として使用されているファイル形式であり、SGMLは、文書の内容を構造化して記述するマークアップ言語である。また、BMPは、Windowsが標準でサポートしている画像ファイル形式であり、白黒からカラーまでの色数を指定できるが、ファイルサイズが大きいためインターネット上でのやりとりには適していない。

5. 以下の文章は、入出力インタフェースに関する説明です。該当する用語は、次のうちどれか。

最大で63台の機器をダイジーチェーン接続やツリー接続することができるインタフェース規格であり、パソコンと周辺機器だけではなく、家電製品との接続も可能である。また、機器を動作中に抜き差しするホットプラグにも対応しており、接続ケーブルによる電源の供給も可能になっている。FireWireやi. Link、DV端子とも呼ばれている。

ア : RS-232C

イ : IrDA

ウ : IEEE 1394

エ : セントロニクス

《解説》以下の入出力インタフェースに関する内容に該当するのは、**IEEE 1394**である。

最大で63台の機器をダイジーチェーン接続やツリー接続することができるインタフェース規格であり、パソコンと周辺機器だけではなく、家電製品との接続も可能である。また、機器を動作中に抜き差しするホットプラグにも対応しており、接続ケーブルによる電源の供給も可能になっている。FireWireやi. Link、DV端子とも呼ばれている。

なお、RS-232Cとは、パソコン本体とプリンタ、モデムなどの周辺機器の接続に利用されるインタフェースであり、IrDAとは、ノートパソコンやプリンタ、デジタルカメラなどの外部通信機能として利用されている、無線（赤外線）のインタフェースである。