情報技術者試験受験テキスト

技術要素

セキュリティ

令和２年４月発行

KMC学習所

txt0304　セキュリティ目次

txt0304　セキュリティ

txt03041　セキュリティとリスク管理

txt030411 情報セキュリティとＩＳＭＳ

①　情報セキュリティポリシ

ⓐ　情報セキュリティとは

情報セキュリティは各種のリスクから情報システムを保護することであり、種々の対策を施して安全を保障することである。保護の対象となる情報システムは、コンピュータ、通信施設、通信網、および蓄積または処理され、検索され、伝送されるデータ及び情報をいい、それらのデータ及び情報にはプログラムや仕様、保守・運用・使用手順を含む。

情報セキュリティを確保するためには、１つの組織体としてポリシ(方針)を設定し、これを徹底するために規定を明文化し、要員の継続的訓練を行う必要がある。

ⓑ　情報セキュリティポリシ

情報セキュリティポリシは、企業や公共団体などの組織において、情報資産の機密性、完全性、可用性を適切に確保・維持するための方針や基準を明文化したものである。

安全の保障を可能にするためには、セキュリティポリシを設定することが重要である。セキュリティマネジメントは、セキュリティ(安全)を組織的に計画し、実施し、その結果を計量評価し、次期の計画に反映させることである。

ⓒ　情報セキュリティポリシに盛り込むキーワード

㋐　情報は組織体における貴重な資産
㋑　情報の漏洩、改変、破壊の防止
㋒　作為、不作為に関係しない
㋓　効果的かつ経済的保護
㋔　組織体構成員全員の義務

②　情報セキュリティ確保の３条件

ⓐ　機密性

機密性はネットワーク上やコンピュータ内の情報を不適切な人間に見せないことである。

盗聴や傍受、不正アクセスあるいは不正放置などによって、その内容が他者に漏れたときに、持ち主にとって損失が発生する可能性がある。

機密性の喪失は不適切な利用者にネットワーク上やコンピュータ内の情報を見られたり、メールサーバ内のメールの内容を見られることである。通信路上で無線周波数を合わせ、プロトコルアナライザを利用して容易に傍受したり、ハードディスクやフロッピーディスクの内容を他人に成りすましたり、セキュリティホールを利用して不当に読み出したりする行為である。

ⓑ　完全性

完全性はネットワーク上やコンピュータ内の情報が常に完全な形で保たれ、不正によって改ざんされたり破壊されないことである。

完全性の喪失は、通信路上のデータ、ハードディスク内のデータ、フロッピーディスク内のデータの改ざんや破壊が行われたり、インターネット上の電子商取引において、金額情報の改ざんが行われたりすることである。長時間かけて蓄積、作成した情報源が破壊されると、その復旧に膨大な時間と金を必要としたり、時には復旧不能にもなる。交通システムに侵入され、制御情報を改ざんされると、生命の危険が生じかねない。

ⓒ　可用性

可用性はネットワークやコンピュータ内の情報や資源がいつでも利用でき、資格を与えられたユーザが情報システムを適時に使用できる保証である。ハードウェア、ソフトウェア、データベースなど情報システムに関する構成物のすべてに関係する。

可用性の喪失は、通信路やコンピュータパワー、コンピュータのディスクの不当な利用によって、ネットワークやコンピュータの機能、保存情報が使えなくなることである。

ⓓ　損失発生の原因と結果

自然災害は機器の故障、不具合、情報の破壊を生じさせる。人が引き起こす損失には物理的損失と論理的損失がある。物理的損失は機器の故障や記憶媒体が損傷を受けて壊れることである。論理的損失は情報の内容の破壊や改変、漏洩などによって生じる損失である。

原因＼結果		機器の故障	情報の破壊	情報の改変	情報の漏洩
自然災害		○	○		
人為的損失	不作為的	○	○	○	○
	作為的	○	○	○	○

③　リスクの定義

ⓐ　情報セキュリティにおけるリスク

期待される状態がある事象の発生によって変化し、期待される状態との間に差異が生じる可能性があるとき、この差異の発生の可能性をリスクと考える。

組織内で制定したセキュリティ標準や他の規制の標準と、現実の状態との差がリスクである。

すべてのリスクに対処することは、時間と費用がかかりすぎるので、リスク分析によって、損失額と発生確率を予測し、リスクの大きさに従って優先順位をつけて、対策を実施する。

ⓑ　リスクの発生要因

リスク発生の原因には脅威と脆弱性がある。

㋐　脅威

脅威は、顕在化すればシステムに損害を与える可能性のある要因である。地震や火災等の災害、機器の障害や誤操作、不正行為、景気変動などの外的要因が含まれる。

㋑　脆弱性

脆弱性は、脅威の顕在化を現実の損失あるいはその拡大に結びつけるシステムの脆さ、弱点である。ハード面、ソフト面におけるシステムの弱点、ネットワーク上の欠陥、バックアップ対策の不備、マニュアルの不整備などが含まれる。

㋒　損失の発生

情報システムに損失が生じるのは、そこに存在する脆弱性が脅威と結びついた時である。

④　リスク管理

ⓐ　リスク管理とは

情報システムを安全に運用するために、発生しうるリスクを事前に想定し、リスク分析して、対応策を検討することである。リスク対策は、リスクの発生を未然に防ぎ、リスクが発生したときの損害を最小にするために対応すべき施策である。

基本的な要素として、次のものがある。

㋐　リスクヘッジ

リスクヘッジは、セキュリティの考え方で、障害時に発生する損害規模をあらかじめ想定し、突発的なコスト流出などを事前に防ぐことである。

㋑　緊急事態計画

詳細は後述する。

ⓑ　リスクコントロールの手法

手法	内　　容
リスク回避	リスクの高い業務はあえて行わない。
リスク分離	資源の二重化など、リスク対象を分散させることによって、発生頻度や程度を分散させる。
リスク結合	リスク対象を結合し集中管理することで、管理精度を向上させる
損失予防	火災防止のための不燃材の使用など、リスク発生の確率を低減させる。
損失軽減	消火設備の設置など、リスク発生時の被害拡大を抑える。
リスク移転	リスクの発生時の責任を、契約書などで他者に転嫁する。

ⓒ　情報システムのリスク

㋐　大災害や故障の発生
㋑　システム内のデータやプログラムの更新障害
㋒　漏洩や破壊
㋓　ネットワークを介した不正アクセス
㋔　データの盗聴、改ざん

⑤　リスク分析と処理

ⓐ　リスク分析とは

守るべき情報資産に対して、損害をもたらす脅威や脆弱性を明らかにすることである。
情報システムを利用することに伴って、次の事項の検討が必要になる。

㋐　発生する可能性のあるリスクを洗い出し
㋑　その影響度合いを分析する

ⓑ　リスク分析の対象

情報セキュリティ対策を講じるためには、次の事項を把握・分析することが不可欠である。

㋐　情報システムの運用過程で発生する可能性のあるリスクの種類
㋑　リスクから守る必要のある資産の存在
㋒　リスクが顕在化した場合の影響範囲と影響度合

ⓒ　リスク対処の考え方

すべてのリスクに対処することは、時間と費用がかかりすぎるので、リスク分析によって、損失額と発生確率を予測し、リスクの大きさに従って優先順位をつけて、対策を実施する。

ⓓ　リスク分析の手順

㋐　発生が予想されるリスクを明確にする。
㋑　リスクの発生頻度と発生後との損失額を推定し、年間損失額を算出する。
㋒　リスクの発生機会を減らす対策と損失額を減らす対策の両面から、具体的リスク対策を策定する。
㋓　リスク対策を実施する。

ⓔ　分析手法

㋐　機密性、保全性、完全性、可用性に分類して重要性を考える定性的分析法
㋑　年間予想損失額を算出する定量的分析手法

ⓕ　リスク処理

リスク処理はリスク分析の結果を受けて行う対処のことである。リスクコントロールとリスクファイナンスがある。

㋐　リスクコントロール

リスクコントロールは、リスクの発生抑止、リスク発生時の損失の最小化を目的とする。

㋑　リスクファイナンス

リスクファイナンスは、リスクが顕在化して、損失が発生した場合を想定し、損失を補填するために必要な資金、および復旧回復に必要な資金を調達する方法である。

ⓖ　リスクファイナンス

リスクファイナンスには、次の２つがある。

㋐　リスク保有

リスクの保有は、リスクを内部的に留保しておく。

㋑　リスク移転

リスクの移転は、情報化保険などの契約を利用して外部に責任を転嫁する。

充実したセキュリティ対策を講じても、リスクの発生を０にすることはできない。リスクの発生を想定して、リスクファイナンスを対策の一部に組み入れておくことが重要となる。

⑥　緊急事態計画

ⓐ　緊急事態計画とは

緊急事態計画は、火災や地震などの災害発生時や大事故や大事件などの緊急事態に備えて、次の内容を決めておく計画である。

㋐　業務をどのように継続するか
㋑　システムをいかに早く復旧するか

ⓑ　計画内容

㋐　緊急時対応体制の整備、業務継続、復旧対策の側面などから対応を想定しておくことが重要である。
㋑　本部と連絡がとれない場合の権限委譲、責任分担を明確にしておく。
㋒　コンピュータベンダー、保守業者、資材調達先、取引業者などのサポート体制を確認しておき、あらかじめ緊急時応援を依頼しておく。
㋓　業務を継続する場合の優先順位や暫定措置、復旧時の優先業務の範囲、緊急暫定業務の範囲、システムを遠隔地でバックアップする機能や代替策を定めておく。
㋔　復旧処理の手順をマニュアル化しておく。

⑦　事業継続計画

ⓐ　事業継続計画とは

事業継続計画は、災害による影響度を認識し、災害発生時の事業継続を確実にするため、必要な対応策を策定することである。その策定・運用・訓練・継続的改善の取組みを事業継続マネジメントという。事故・災害時に対応する事業継続のリスクマネジメント手法であり、災害時重要業務が中断した場合における事業継続を追求する計画を指す。

ⓑ　取組みの手順

㋐　被災後、継続すべき重要業務の絞込み
㋑　重要業務についての復旧時間の設定
㋒　復旧について支障となる事項の抽出
㋓　支障となる事項への対策の策定

ⓒ　ビジネスインパクト分析

ビジネスインパクト分析は、不測の事態によって、業務が中断したりシステムが停止したり

した場合のビジネスへの影響度を分析することである。ビジネス影響度分析、事業影響度分析、ＢＩＡとも言う。

事業継続計画（ＢＣＰ）を策定する上で、必要不可欠なプロセスである。売上などの財務上の損失をはじめ、利用者への影響、風評被害、従業員のモチベーションの低下など、定量的および定性的な影響について時系列で整理していく。

分析を通じて、事業継続に重大な影響を及ぼすリソースを特定するとともに、優先的に対策を講じるべき重要な業務や、目標となる復旧時間、復旧レベルなどを決定していく。

⑧　ＩＳＭＳとその必要理由

ⓐ　ＩＳＭＳとは

ＩＳＭＳは企業や組織が自身の情報セキュリティを確保・維持するために、ルール（セキュリティポリシー）に基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのことである。ＩＳＭＳに求められる範囲は、ＩＳＯ／ＩＥＣ15408などが定めるような技術的な情報セキュリティ対策のレベルではなく、組織全体に渡ってセキュリティ管理体制を構築・監査し、リスクマネジメントを実施することである。

ＩＳＭＳの定義としてＪＩＰＤＥＣは、「ＩＳＭＳとは、個別の問題ごとの技術対策のほかに、組織のマネジメントとして自らのリスク評価により、必要なセキュリティレベルを定め、プランを持ち、資源配分してシステムを運用することである」、また、「組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し改善することがＩＳＭＳの要求する主なコンセプトである」と設定している。

ⓑ　情報資産

㋐　情報

❶　データベース：データベース、データファイル、アーカイブされたデータ

❷　システム文書：システム文書、事業計画、組織のもつ情報、個人情報、組織の機密事項

㋑　ソフトウェア

システムソフトウェア、アプリケーションソフトウェア、ユーティリティ、各種ＯＳ、各種ツール

㋒　物理的財産

ＰＣやサーバなどのコンピュータ装置、ルータやケーブルなどの通信装置、磁気媒体、ファクス、電話、電源装置、空調設備、書架など

㋓　サービス

組織の利用する通信サービス、照明・空調などの一般的ユーティリティなど

ⓒ　ＩＳＭＳのメリット

㋐　組織内部のメリット

❶　企業体質の強化

ＩＳＭＳを構築し、組織全体で運用することによって、継続的に情報セキュリティのマネジメントシステムを改善していくことが可能となる。内部牽制機能が働くことになる。

❷　責任区分の明確化

ＩＳＭＳの認証基準に組織の構成員の責任についての記述が有り、責任と権限について職務定義書に明確に定義する必要がある。情報セキュリティについての責任区分を文書で明確にしている。

❸　費用対効果を考えた資産管理

情報資産を分類し、守るべき保証の程度を明確化し、情報資産の重点管理の仕組みを構築することによって情報セキュリティに対する投資の無駄を省くことが可能になる。

❹　自社分析

自社のリスクアセスメントを適切な手法で行うことで、守るべき対象が明確になる。

❺　緊急事態への対応

事前に緊急事態を想定し、事業への影響度や復旧に要する費用などが明確にでき、緊急事態への管理体制を構築できる。緊急事態が発生した際、迅速に対応でき、被害を最小にとどめ、適切な予防処置を策定できる。

㋑　対外的なメリット

❶　取引先の信頼確保

顧客の重要情報を管理する組織、アウトソーシングを業とする組織、海外企業と取引している企業、他社と供給連鎖している企業などは信頼を確保するためにＩＳＭＳ認証を示すことが信頼を得るために効果的になる。

❷　セキュリティビジネスの展開

セキュリティシステム構築支援、情報セキュリティコンサルティングサービスを提供する企業はＩＳＭＳの認証により自ら情報セキュリティの仕組みを構築し運用していることを示すことがビジネスを有利に展開する。

❸　電子商取引への参加の条件

ＩＳＭＳを構築し運用することはシステムの可用性を組織全体で確保する仕組みを作ることになり、電子商取引における自社のサービスの質を高めることになる。

ⓓ　ＩＳＭＳの要求事項

㋐　一般要求事項

保護すべき情報資産、リスクマネジメントに対する組織の取り組み方法、管理目的、管理策の内容、保護すべき情報資産に要求される保証の度合いを明確にしたＩＳＭＳを確立し維持することが要求されている。

㋑　マネジメント枠組みの確立

組織にとって必要な管理目的及び管理策を文書化するために、情報セキュリティポリシーの策定、ＩＳＭＳの認証範囲の決定、リスク評価、リスクマネジメントの対象範囲の決定、ＩＳＭＳ認証基準の詳細管理策及び追加管理策の選択、適用宣言書の作成が要求され、定期的に必要に応じて見直すことが要求されている。

㋒　管理策の実施

選択した管理策を実施し､その実施手順について有効性を確認することが要求されている。

㋓　文書化

実施した作業の証拠と確立したマネジメント枠組みの要約を文書化して維持することが要求されている。

㋔　文書管理

❶　利用者が容易に利用でき、必要な部署において閲覧可能にする。
❷　容易に識別でき整頓された状態で維持する。
❸　定期的な見直しを行い、必要に応じて改訂する。
❹　策定や改訂の日付を明記し、更新履歴を管理する。
❺　新しい文書に置き換わるときは、不必要な文書は速やかに廃止する。
❻　管理を行うための責任体制や手順を維持する。定め

㋕　記録

要求事項に対する準拠状況を保証する必要な記録を特定し、その管理手順を定めて必要に応じて見直す。これらの記録の損傷などを防止するための措置を講じる。

ⓔ　詳細管理策

次の管理策の中から、リスクアセスメントおよびシステムの保証の度合い等にもとづき選択して実施する。なお、情報技術分野におけるめざましい技術、慣行の発展を考慮し、次に示す管理策だけでなく、よりよい管理策を取り入れるべきだとされている。

㋐　セキュリティポリシー
㋑　セキュリティ組織
㋒　情報資産の分類及び管理
㋓　人的セキュリティ
㋔　物理的及び環境的セキュリティ
㋕　通信及び運用管理
㋖　アクセス制御
㋗　システム開発及びメンテナンス
㋘　事業継続管理
㋙　準拠

⑨　情報セキュリティポリシーの運用

ⓐ　セキュリティ組織

㋐　情報セキュリティインフラストラクチャ

情報セキュリティ委員会は、組織の中心的役割を果たす組織で、情報セキュリティポリシーの決定機関である。委員会は経営陣により構成され、各種施策や改訂を検討、情報資産の取扱に関する責任、情報セキュリティポリシーの組織内への浸透を推進する。

情報セキュリティ事務局は、策定作業を担当する組織で、関連部門を横断的に調整する機能を持っている。

情報セキュリティ組織体制を構築する場合、情報資産に対する保護責任、特定の業務に対する実施責任、情報関連設備の導入に関する承認プロセス、専門家からの助言を公表する内部コミュニケーションプロセス、外部組織に対する外部コミュニケーションプロセス、情報セキュリティポリシーの導入や運用状況を監視するレビュープロセスの検討が必要になる。

㋑　第三者アクセスのセキュリティ

第三者に内部へのアクセスを許可する場合、評価されたリスクに基づいて必要な措置を講じ、セキュリティ要求事項を明記した正式な契約を締結する。

㋒　第三者への委託

情報システムの管理や制御を外部に委託する場合、セキュリティ要求事項を明記した正式な契約を締結する。

ⓑ　情報資産の分類・管理

情報資産の目録を作成、４つのカテゴリーに分類する。各情報資産のリスク評価を行い、その保護レベルと担当者の責任と権限を設定し、管理責任者を明確にする。

ⓒ　人的セキュリティ

㋐　職務定義及び採用におけるセキュリティ

従業員の情報システムの誤用、悪用などのリスクを低減する。職務定義書などの文書に従業員の層別にセキュリティ関する事項を含めた責任と権限を記述する。

採用する人員の能力を明確にし、必要に応じて採用時に機密保持の誓約書を提出させることも検討する。

㋑　ユーザの教育・訓練

セキュリティポリシーやセキュリティを守る手順について適切な訓練を受けること、訓練を定期的に行うことなど、教育計画をたて実行する。

㋒　セキュリティ事故及び誤動作への対処

セキュリティ事故の損害の最小化、事故の監視の徹底、事故発生時は脆弱性を改善する体制の確立、セキュリティ事故・システムへの脅威・脆弱性の発見時の報告ルートの明確化、日常的な記録の整備などの体制の整備が求められる。

ⓓ　物理的・環境的セキュリティ

㋐　セキュリティ区画

情報への許可されないアクセスや損傷の防止、新製品情報など機密情報の取扱等に対処できる物理的な境界を設け、セキュリティ区画への出入りに指紋認証、カード認証など必要な措置を講じる。

㋑　装置のセキュリティ

耐震構造のビルに設置すること、電源異常からの保護、傍受・損傷がないメンテナンス

㋒　一般管理策

重要な資料管理、パスワードの管理、長時間使用しないＰＣの電源停止、情報資産の持ち出し・移動時の認可プロセス

ⓔ　通信及び運用管理

㋐　運用手順及び責任

各手順の責任者を明確に記載、例外的な処理や不測の事態発生時の連絡先、システムの変更や設計・テスト・リリース等のステップの責任の明確化・運用手順の文書化

㋑　システム計画の作成及び受入

システムの利用状況を監視し、運用に支障ないように必要な容量を予測すること、受入テスト時に想定したデータ量で稼働率のテストを行うこと

㋒　不正ソフトウェアからの保護

ウィルス対策ソフトウェアの導入などを行い、システムの完全性を保持すること

㋓　情報システムの管理

バックアップの準備、障害発生原因を特定するための情報の取得、障害事象や対応手順の実施結果の記録

㋔　ネットワークの管理

ネットワーク管理者の責任の明確化、利用者の責任・手順の明確化

㋕　媒体の取扱及びセキュリティ

媒体の使用法、管理方法の文書化、重要なデータが記載された文書・媒体の管理方法、処分方法の文書化

㋖　組織間における情報及びソフトウェアの交換

組織間でやり取りする各種情報及びデータの保護のための管理策を決め、両者間で合意を取ること

ⓕ　アクセス制御

㋐　アクセス制御に関する事業の要求事項

開発要員、運用要員、管理職、一般従業員などのアクセス権限の明確化、許可されたアクセス以外は禁止すること

㋑ **ユーザアクセス管理**

一般ユーザへのアクセス権を与える正規の手続の確立、管理者による承認、定期的な調査の実施、特権ユーザに対しては特別な場合に限って最低限の要求事項に従って権限の付与

㋒ **ユーザの責任**

パスワードの取扱規程の設定、作業終了時の端末、サーバの終了処理の徹底

㋓ **ネットワークのアクセス制御**

個別のネットワーク使用のユーザ毎に許可されているオペレーションの明確化

㋔ **オペレーティングシステムのアクセス制御**

ＯＳレベルの本人の確認、ログオン手順の確立、ログオン時間の制限、ログオン失敗許容回数の制限、脅迫警報機能の準備

㋕ **アプリケーションシステムのアクセス制御の規定**

㋖ **システムアクセス及びシステム使用の監視**

㋗ **モバイルコンピューティング及び遠隔地勤務時の要求事項**

ⓖ　システム開発及びメンテナンス

㋐ **システムのセキュリティ要求事項**

システムの変更に際してリスクアセスメントを行い、要求事項の明確化、文書化を行う。

㋑ **アプリケーションシステムのセキュリティ**

システム設計段階に、入出力データの妥当性、適切なデータ量、メッセージの完全性などの確認の実行

㋒ **暗号による管理策**

メッセージの機密性、完全性の確保のための暗号化、暗号化に伴う管理体制の充実、本人確認、否認防止のための電子署名の活用など検討

㋓ **システムファイルのセキュリティ**

システムのライブラリ管理、システム変更テストのデータ量、試験データの終了時の速やかな削除など

㋔ **開発及びサポートプロセスにおけるセキュリティ**

システム変更の変更管理手順の設定、変更の記録、責任者の承認、変更ログの取得、プログラムの版数管理

ⓗ　事業継続管理

重大なシステム障害、災害から発生するリスクから業務手続を保護する事業継続計画を作成し管理する。計画には、計画を実行する前の手順、実行の判断をする責任者の明示、バックアップ機への移行手順、復帰手順、実施責任者の明確化、テストの実施、計画の見直し、更新要領などを設定する。

⑩　ＩＳＭＳの構築

ⓐ　構築のステップ

㋐　情報セキュリティポリシーの策定
㋑　適用範囲の決定
㋒　リスクアセスメントの実施
㋓　リスクマネジメント
㋔　管理策の選定
㋕　適用宣言書の作成

ⓑ　ＩＳＭＳの適用範囲

適用範囲の決定に当たっては、経営管理上の必要性、対外的な考慮からの必要性、組織へのアピールなどを考えて認証取得の範囲を決める。パイロット部門を選定し、運用が安定後、他部門への展開を行う。アウトソーシング業務への適用について検討や適用範囲の文書化、文書に組織、サイト、資産、技術などの明記も必要である。

ⓒ　リスクアセスメント

情報資産の洗い出し(名称、管理責任者、価値、利用者の範囲、保管形態、保管場所、保管期間、処分方法など)、情報資産のラベリング、リスクアセスメント(管理状況、存在する脅威、資産の脆弱性、事業への影響度、リスクの評価など)を順次実施する

リスク値は次の式を用いて計算する。

リスクの値＝情報資産の価値×脅威の値×脆弱性の値

情報資産の価値：機密性、完全性、可用性の観点から評価した結果の数値化

脅威の値：要求される保証度合い以下に引き下げる潜在的な要因

脆弱性の値：情報資産や人員の管理方法に起因する弱点

ⓓ　リスク管理

リスク許容、リスク低減、リスク移転、リスク回避の４ケースの観点から管理方法を検討し明確化する。

ⓔ　管理目的・監理策の選択

管理目的・管理策の選択・運用(時間的制約、費用対効果、技術上の制約、企業文化、地理的条件、関連法規制などを考慮)、教育(一般事項、情報セキュリティポリシーや関連文書、各人の役割・責任・権限、管理策実施上の手順など)、内部監査など

⑪　ＩＳＭＳ認証制度

ⓐ　ＩＳＭＳ適合性評価制度

㋐　ＩＳＭＳは、情報セキュリティを管理するための仕組みで、この仕組みの基準として用いるのが、国際規格ISO/IEC27001／日本工業規格 JIS Q 27001「情報セキュリティマネジメントシステムー要求事項」である。

㋑　構築されたＩＳＭＳが、ISO27001/JISQ27001に適合していることを、第三者が評価し、認定する制度がＩＳＭＳ適合性評価制度である。

㋒　ＩＳＭＳのマネジメントシステムの基盤部分は、品質管理マネジメントシステム（QMS）ISO9001や環境マネジメントシステム（EMS）ISO14001などと調和が図られており、ＩＳＭＳ（ISO/IEC 27001)、ＱＭＳ（ISO9001)、ＥＭＳ（ISO14001）をまとめて“三大マネジメントシステム”などと言われている。

ⓑ　認証取得のメリット

㋐　ＩＲの強化

取引先、金融機関、顧客などに対して自社の企業価値の評価を高めるのに役立つ。

㋑　ＳＩ認定企業、ＳＯ認定企業のメリット

ＳＩ登録企業やＳＯ認定企業がＩＳＭＳ認証取得によって取引先や顧客への信頼度を更に高めることになる。

㋒　自治体の入札条件

㋓　リスクマネジメントの強化

情報戦略策定能力、実行能力、情報リテラシー能力、情報リスクマネジメント能力が不可欠な企業の認証取得はＩＴガバナンスやリスク管理に関する優良企業のイメージを与える。

ⓒ　審査制度の概要

㋐　認証機関

認定機関は、審査する審査登録機関が審査するのにふさわしいかどうかを判断する組織である。ＩＳＭＳ認証制度の認証機関は財団法人日本情報処理開発協会(JIPDEC)である。

㋑　JIPDECの機能

❶　審査登録機関の認定、登録、公表

❷　審査員研修機関の認定、登録、公表

❸　審査員評価登録機関の管理運用

㋒　審査員の種類

ＩＳＭＳ審査員補、ＩＳＭＳ審査員、ＩＳＭＳ主任審査員の３種類がある。審査員になるためには情報技術分野で４年以上の実務経験を持ち、そのうち２年以上は情報セキュリティ関連分野の実務経験が必要である。ＩＳＭＳ審査員研修コースを終了し合格する必要がある。

㊓ 審査チームの編成

ⓓ 審査の流れ

㋐ 予備審査は事業者のオプションで実施し、ＩＳＭＳ認証基準に照らして、不足している点を明らかにする。
㋑ ステージ１の本審査はＩＳＭＳの整備状況について、文書を中心に審査する。
㋒ ステージ２の本審査はＩＳＭＳの運用状況について、インタビュー、記録の確認、現場視察を中心に審査する。
㋓ 審査結果の判定
㋔ 登録証の交付
㋕ サーベイランス審査は、認証取得後の定期検査で１年以内に最低１回受けることになる。認証取得後の運用状況、マネジメントシステムの変更点などが審査される。
㋖ 更新審査は本審査と同様にＩＳＭＳ認証基準の全項目について審査を行う。

ⓔ 審査のポイント

㋐ 不適合への対処(軽微な不適合、重大な不適合)
㋑ セキュリティポリシーの適切性
㋒ 情報資産の網羅性
㋓ リスク評価の妥当性、管理策の適切性
㋔ 関連法規制の把握と遵守状況
㋕ 外注先との契約内容
㋖ 人的セキュリティとユーザの教育
㋗ 文書管理、運用記録とその管理
㋘ 事業継続計画のテスト
㋙ 定期的なレビュー

例題演習

企業の情報セキュリティポリシの基本方針策定に関する記述のうち，適切なものはどれか。

ア　業種ごとに共通であり，各企業で独自のものを策定する必要性は低い。
イ　システム管理者が策定し，システム管理者以外に知られないよう注意を払う．
ウ　情報セキュリティに対する企業の考え方や取り組みを明文化する．
エ　ファイアウォールの設定内容を決定し．文書化する．

解答解説

セキュリティポリシに関する問題である。

安全の保障を可能にするためには、セキュリティに関するマネジメントの方針を設定することが重要である。セキュリティマネジメントとは、安全を組織的に計画し、実施し、その結果を計量評価し、次期の計画に反映させることである。

セキュリティ方針には、次の内容を盛り込む必要がある。

① 情報は組織体における貴重な資産　② 情報の漏洩、改変、破壊の防止

③ 作為、不作為に関係しない。　④ 効果的かつ経済的保護

⑤ 組織体構成員全員の義務

企業の情報セキュリティポリシは企業の考え方や取り組み方を明文化することであり、求める答えはウとなる。

例題演習

データの破壊やシステムの可用性が損なわれることで発生する損失に含まれる費用はどれか。

ア　業務形態の変更によるシステム再開発費用とデータベースの移行費用

イ　システム開発の実行可能性の検討にかかる費用

ウ　システムが復旧するまでの間，代替の手段にかかる費用

エ　新システムへの移行費用

解答解説

データの破壊や可用性が損ねた場合の損失費用の問題である。

データの破壊やシステムの可用性が損なわれた場合に発生する損失費用であるから、破壊したシステムが復旧するまでの間、代替の手段に費やした費用になる。求める答えはウとなる。

アは業務形態の変更に伴うシステムの再開発に必要な費用になる。

イはシステム計画時の実現可能性の検討にかかる費用である。

エはシステム開発後に新しいシステムに移行するために発生する費用である。

例題演習

情報セキュリティにおける“完全性”を脅かす攻撃はどれか。

ア　Ｗｅｂページの改ざん

イ　システム内に保管されているデータの不正コピー

ウ　システムを過負荷状態にするＤｏＳ攻撃

エ　通信内容の盗聴

解答解説

情報セキュリティの完全性に関する問題である。

完全性はネットワーク上やコンピュータ内の情報が常に完全な形で保たれ、不正によって改ざんされたり破壊されないことである。完全性の喪失は、通信路上のデータ、ハードディスク内のデータ、フロッピーディスク内のデータの改ざんや破壊が行われたり、インターネ

ット上の電子商取引において、金額情報の改ざんが行われたりすることである。長時間かけて蓄積、作成した情報源が破壊されると、その復旧に膨大な時間と金を必要としたり、時には復旧不能にもなる。交通システムに侵入され、制御情報を改ざんされると、生命の危険が生じかねない。

アは完全性、イ、エは機密性、ウは可用性である。求める答えはアとなる。

例題演習

コンピュータセキュリティ対策に関する記述のうち，適切なものはどれか。

ア　一時記憶領域に残っている機密データは，ジョブ終了時に確実に消去する。
イ　金利計算処理などで，端数を特定口座に振り込む，いわゆるサラミ技術に対しては，データにチェックディジットを付加する。
ウ　端末から入力された数値データの改ざんに対しては，仮想記憶額域のページ又はセグメント単位に割り付けられた記憶保護キーによって，保護のレベルを変える。
エ　ユーティリティプログラムを使用したデータ改ざんに対しては，そのユーティリティプログラムのバックアップをとっておき，元のプログラムと比較する。

解答解説

コンピュータセキュリティ対策に関する問題である。

アの記憶領域に残っている機密データはジョブ終了時に確実に消去することはセキュリティ対策として重要である。求める答えはアとなる。

イのデータにチェックディジットを付加することは入力データのチェックには役立つがサラミ技術などの犯罪の防止対策にはならない。

ウの内容の仮想記憶領域のページまたはセグメント単位に割り付けられた記憶保護キーの保護レベルの変更は、データの改ざんは実記憶域の主記憶で行われるためセキュリティ対策にはならない。

エの内容のユーティリティプログラムのバックアップをとっておき、元のプログラムとの変化が分かっても、データの改ざんを防止できることにはならない。

例題演習

インターネットＶＰＮのセキュリティに関する記述のうち，適切なものはどれか。

ア　ＩＰアドレスを悪用した不正アクセスや侵入の危険性はないので，ＩＰアドレスも含めたパケット全体の暗号化は必要ない。
イ　インターネットＶＰＮの仮想的なトンネルは特定ＬＡＮ間の専用通路であるから，通過するデータに対する盗聴防止の機能はない。
ウ　仮想的なネットワークを形成するものであり，ネットワークに参加する資格のない第三者による盗聴や改ざんを防御できない。
エ　ネットワークに参加する資格のある個々人を識別する能力はない。

解答解説

インターネットのＶＰＮに関する問題である。

ＶＰＮは、インターネットを専用線のように利用したネットワークで、通常の専用線と比較して、通信コストが安くなる。認証システムや暗号技術、トンネリング、ファイアウォールなどを利用することで、インターネット上を流れるデータを保護する。組織外のユーザがネットワーク上を流れるデータにはアクセスできない。トンネリングは、インターネットなどの公衆回線網上に、ある２点間を結ぶ閉じられた仮想的な直結通信回線を確立することであり、ネットワーク上に外部から遮断された見えない通り道を作るように見えることからトンネルと呼ばれるようになった。本来通信を行ないたいプロトコルで記述されたパケットを、別のプロトコルのパケットでカプセル化して、送り届けることにより通信を行なう。パケットのカプセル化とその解除はトンネルの両端の機器が自動的に行なうため、トンネルで結ばれた機器同士は途中の通信方式や経路を気にする必要はなく、あたかもトンネルの両端の機器が直結しているように見える。本社と支社のＬＡＮ間接続など、プライベートなネットワークをインターネットを経由して接続する際などに利用されることが多いため、実際のトンネリング機器やソフトウェアはパケットをカプセル化する際に暗号化を行ない、転送中に覗き見られたり改ざんされたりしないようにするセキュリティ機能を持っていることが多い。

アは､暗号技術と認証システムを活用して専用化を行っているので暗号技術は不可欠である。

イは、盗聴防止の機能はなくてもが、暗号化によってデータの解読が不能になるため、データの内容は保護されることになる。

ウは､暗号技術と認証システムを使用しているため第三者による盗聴や改ざんは防止できる。

エのネットワークに参加する資格の区別は組織単位であって、通常は、個人を識別する能力はない。求める答えはエとなる。

例題演習

リスクアセスメントに関する記述のうち，適切なものはどれか。

ア　以前に洗い出された全てのリスクへの対応が完了する前に，リスクアセスメントを実施することは避ける。

イ　将来の損失を防ぐことがリスクアセスメントの目的なので，過去のリスクアセスメントで利用されたデータを参照することは避ける。

ウ　損失額と発生確率の予測に基づくリスクの大きさに従うなどの方法で，対応の優先順位を付ける。

エ　リスクアセスメントはリスクが顕在化してから実施し，損失額に応じて対応の予算を決定する。

解答解説

リスクアセスメントに関する問題である。

リスクアセスメントは、リスク特定、リスク分析、リスク評価を網羅するプロセスである。

①　リスク特定　リスクを発見し、認識し、記述するプロセス

②　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

③　リスク評価　リスクとその大きさが受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

安全工学上は、リスクとは、人、環境、物に悪い影響をあたえる可能性と大きさ(の積)である。予測されるリスクの可能性と大きさ(予測値)と、許容されるリスクの可能性と大きさ(許容値)を比較し、予想値が許容値を上回った時リスク軽減の施策又はリスク回避の施策をとるという意思決定を行い、実際にその施策をとり、より安全な状態を実現するプロセスである。

アのリスクアセスメントは、わかっている現状のレベルでの分析、評価が必要で、それに基づいて将来のリスクを予測するプロセスを繰り返す必要がある。

イの過去のリスクアセスメントの利用は不可欠である。

ウの損失額と発生確率の予測に基づいて、対応の優先順位を付けるは適切である。求める答えはウとなる。

エのリスクが顕在化してからの分析、予測、評価は価値がない。

例題演習

リスク分析に関する記述のうち，適切なものはどれか。

ア　考えられるすべてのリスクに対処することは時間と費用がかかりすぎるので，損失額と発生確率を予測し，リスクの大きさに従って優先順位を付けるべきである。

イ　リスク分析によって評価されたリスクに対し，すべての対策が完了しないうちに，繰り返しリスク分析を実施することは避けるべきである。

ウ　リスク分析は，将来の損失を防ぐことが目的であるから，過去の類似プロジェクトで蓄積されたデータを参照することは避けるべきである。

エ　リスク分析は，リスクの発生による損失額を知ることが目的であり，その損失額に応じて対策の費用を決定すべきである。

解答解説

リスク分析に関する問題である。

リスク分析は、情報システムを利用することに伴って発生する可能性のあるリスクを洗い出し、その影響度合いを分析することである。

リスク分析の手順

①　発生が予想されるリスクを明確にする。

②　リスクの発生頻度と１回の発生ごとの損失額を推定し、それを基に年間の損失額を算出する。

③　リスクの発生機会を減らす対策と１回当たりの損失額を減らす対策の両面から、具体的リスク対策を策定する。

④　リスク対策を実施する。

アの損失額と発生確率を予測し、リスクの大きさに従って優先順位を付ける記述は適切である。求める答えはアとなる。

イは、リスクは人間の欲望の変化や技術の変化、産業組織の変化によって絶えず変動するため、リスク対策のすべてが完了しないうちに絶えずリスク分析を繰り返す必要がある。

ウの過去の類似プロジェクトのデータを分析に活用する。

エのリスク分析の目的は、リスクによる損失額を知ることではなく、リスクによって発生する損失を減らすことが目的である。

例題演習

リスク移転を説明したものはどれか。

ア　損失の発生率を低下させること
イ　保険に加入するなど資金面での対策を講じること
ウ　リスクの原因を除去すること
エ　リスクを扱いやすい単位に分解するか集約すること

解答解説

リスクの移転に関する問題である。

リスク移転はリスクコントロールの手法の一つであり、リスクの発生時の責任を契約書などで他社に転嫁することである。従って、保険に加入するなど資金面での対策を講じることになる。リスクコントロールの手法には、リスク回避、リスク分離、リスク結合、損失予防、損失軽減等がある。

アは損失予防、イはリスク移転、ウはリスク回避、エはリスク分離やリスク結合である。求める答えはイとなる。

例題演習

ネットワーク障害の原因を調べるために使用するＬＡＮアナライザの運用上の注意点はどれか。

ア　ＬＡＮアナライザにはネットワークを通過するパケットを表示できるものがあるので，盗聴などに悪用されないように注意する必要がある。
イ　障害発生に備えて，ネットワーク利用者にＬＡＮアナライザの保管場所と使用方法を周知しておく必要がある。
ウ　測定中は，本来通信すべきあて先のパケットを破棄してしまうので，測定対象外のコンピュータ利用を制限しておく必要がある。
エ　測定に当たって，ＬＡＮケーブルを一時的に切断する必要があるので，利用者に対して測定日を事前に知らせておく必要がある。

解答解説

ＬＡＮアナライザの運用上の注意点に関する問題である。

ＬＡＮアナライザは、ＬＡＮの故障診断、監視、問題解決などに使用する機器やソフトウェアである。パケットの衝突率、ネットワークのトラフィックの測定、各種プロトコルの解析したりする。また、ネットワークを通過するパケットを表示できるものがあるため、盗聴などに悪用されることがある。求める答えはアとなる。

例題演習

リスクが顕在化しても，その影響が小さいと想定されるので，損害の負担を受容するリスク対応はどれか。

ア　リスク移転　　イ　リスク回避
ウ　リスク低減　　エ　リスク保有

解答解説

リスクコントロールに関する問題である。

アのリスク移転は、特定のリスクに関する損失の負担を他者と分担することである。

イのリスク回避は、リスクのある状況に巻き込まれないようにする意思決定又はリスクのある状況から撤退する行動である。

ウのリスク低減は、特定のリスクに関する確からしさもしくは発生確率､好ましくない結果又はその両者を低減する行為である。

エのリスク保有は、特定のリスクに関する損失の負担を享受することである。求める答えはエとなる。

例題演習

ネットワークシステムのセキュリティ対策に関する記述のうち，適切なものはどれか。

ア　ＩＳＤＮ回線やパケット交換回線では，接続時に通知される相手の加入者番号によって相手確認を行うことができる。これをコールバックと呼ぶ。
イ　回線暗号化装置をＤＴＥ(通信制御装置や端末装置など)とＤＣＥ(モデムやＤＳＵなど)の間に設置して，伝送区間ごとに暗号化を行う方法では，既設のハードウェアやソフトウェアの一部に変更が必要になる。
ウ　閉域接続機能をもつ回線交換網を利用して，回線接続の範囲を特定の利用者グループに限定することは，外部からの不正アクセスの防止に有効である。
エ　無線ＬＡＮの使用は，ケーブルを介在させないので伝送途中の盗聴防止に有効である。

解答解説

ネットワークシステムのセキュリティ対策に関する問題である。

アのコールバックは、公衆回線を利用した通信で、接続要求側が接続先を呼び出し、回線を一端切断した後に接続先が接続要求側に折り返し接続して、通信回線を開く方法である。

イの回線暗号化装置の設置は暗号化アルゴリズムを使用して通信文を暗号文に変換するだけであり、通信上のハードウェアやソフトウェアの変更を必要としない。

ウの閉域接続機能をもつ回線交換網は外部からの不正アクセス防止に有効である。求める答えはウとなる。

エの無線ＬＡＮも盗聴される。

例題演習

情報システムのセキュリティコントロールを予防，検知，復旧の三つに分けた場合，復旧に該当するものはどれか。

ア　オペレータとプログラマの職務分離
イ　コンティンジェンシープラン
ウ　パスワードの利用
エ　メッセージ認証

解答解説

緊急事態計画に関する問題である。

緊急事態計画は火災や地震などの災害発生時や大事故や大事件などの緊急事態に備えて、業務をどのように継続するか、システムをいかに早く復旧するかを定めた計画書である。

アは、仕組みを考えるプログラマとその仕組みを操作するオペレータを分離しておくことによってセキュリティの予防となる。

イの緊急事態計画は、災害発生時の復旧対策であり、復旧である。求める答えはイとなる。

ウのパスワードの利用は不正アクセスの検知である。

エのメッセージ認証はメッセージ改ざんの検知である。

例題演習

企業内ネットワークやサーバにおいて，侵入者が通常のアクセス経路以外で侵入するために組み込むものはどれか。

ア　シンクライアントエージェント　　イ　ストリクトルーティング
ウ　バックドア　　エ　フォレンジック

解答解説

バックドアに関する問題である。

アのシンクライアントエージェントは､機能を絞ったクライアント用コンピュータのことで、サーバ側でアプリケーションソフトやファイルなどの資源を管理するシステムである。

イのストリクトルーティングは、送信元からあて先までに経由するルーターのＩＰアドレス・リストを送信元のルーターがすべて指定し,その順番通りにパケットを送信することである。

ウのバックドアは、ＩＤやパスワードを使って通信を制限したり、使用権を確認するコンピュータの機能を無許可で利用するために､コンピュータ内に設けられた通信接続の機能を指す。バックドアには、設計・開発段階で盛り込まれるものや稼動中のコンピュータに存在するセキュリティホールを使って送り込まれたソフトウェアである。求める答えはウである。

エのフォレンジックは、証拠として使えるように，コンピュータ内やネットワーク上にあるディジタル・データを収集・分析・保存することである。

例題演習

Ｗｅｂサーバが外部から侵入され、コンテンツが改ざんされた。その後の対応の順序のうち，適切なものはどれか。

①	**サーバ，IDS（Intrusion Detection System），ファイアウォールの各ログを解析し，不正アクセス手法，影響範囲，侵入経路を特定する。**
②	**システムを再構築し，最新のパッチやセキュリティ設定情報を適用する。**
③	**サーバをネットワークから切り離す。**
④	**ネットワークに接続後，しばらく監視する。**

ア　①→②→③→④　　イ　①→③→②→④

ウ　②→③→①→④　　エ　③→①→②→④

解答解説

コンテンツの改ざんが発生した場合の処理手順の問題である。

通常、次の手順で行う。

①　問題が発生した箇所、サーバをネットワークから切り離す。

②　問題内容をログを使用して分析し、不正アクセスの手法、影響範囲、進入経路を特定する。

③　システムを再構築する。

④　ネットワークに接続し、監視する。

答えは、③→①→②→④となり、求める答えはエとなる。

例題演習

ＷＡＦ(Web Application Firewall)を利用する目的はどれか。

ア　Ｗｅｂサーバ及びアプリケーションに起因する脆弱性への攻撃を遮断する。

イ　Ｗｅｂサーバ内でワームの侵入を検知し，ワームの自動駆除を行う。

ウ　Ｗｅｂサーバのコンテンツ開発の結合テスト時にアプリケーションの脆弱性や不整合を検知する。

エ　Ｗｅｂサーバのセキュリティホールを発見し，ＯＳのセキュリティパッチを適用する。

解答解説

ＷＡＦに関する問題である。

ＷＡＦは、従来のファイアウォールがネットワークレベルで管理していたことに対して、アプリケーションのレベルで管理を行う。プログラムに渡される入力内容などを直接に検査することによって、不正と見なされたアクセス要求を遮断するという仕組みが採用されている。クライアントの操作するＷｅｂブラウザとＷｅｂサーバを仲介するかたちで存在し、ブラウザとの直接的なやり取りをＷＡＦが受け持つ。ＳＱＬインジェクションやクロスサイトスクリプティング、強制ブラウジングといった要求に対して、「攻撃」と見なして拒絶することができる。

外部ネットワークからの不正アクセスを防ぐためのソフトウェアあるいはハードウェアである。ファイアウォールの中でも、Ｗｅｂアプリケーションのやり取りを把握・管理することによって不正侵入を防御することのできるファイアウォールのことである。

Ｗｅｂサーバおよびアプリケーションに起因する脆弱性への攻撃を遮断する内容が適切である。求める答えはアとなる。

例題演習

クライアントとＷｅｂサーバの間において，クライアントからＷｅｂサーバに送信されたデータを検査して，ＳＱＬインジェクションなどの攻撃を遮断するためのものはどれか。

ア　ＳＳＬＶＰＮ機能　　イ　ＷＡＦ

ウ　クラスタ構成　　エ　ロードバランシング機能

解答解説

ＷＡＦに関する問題である。

ＷＡＦの特徴は、従来のファイアウォールがネットワークレベルで管理していたことに対して、アプリケーションのレベルで管理を行う。プログラムに渡される入力内容などを直接に検査することによって、不正と見なされたアクセス要求を遮断するという仕組みが採用されている。クライアントの操作するＷｅｂブラウザとＷｅｂサーバを仲介するかたちで存在し、ブラウザとの直接的なやり取りをＷＡＦが受け持つ。ＳＱＬインジェクションやクロスサイトスクリプティング、強制ブラウジングといった要求に対して、「攻撃」と見なして拒絶することができる。

アのＳＳＬ-ＶＰＮは、暗号化にＳＳＬを利用するＶＰＮ技術で、多くのＷｅｂブラウザやメールソフトは標準でＳＳＬに対応しているため、リモートアクセス用途などで手軽に導入できる。

イのＷＡＦは、外部ネットワークからの不正アクセスを防ぐためのソフトウェア（あるいはハードウェア）である。ファイアウォールの中でも、Ｗｅｂアプリケーションのやり取りを把握・管理することによって不正侵入を防御することのできるファイアウォールのことである。求める答えはイとなる。

ウのクラスタ構成は、複数のコンピュータを連結し、利用者や他のコンピュータに対して全体で１台のコンピュータであるかのように振舞うシステムまたは仕組みのことである。

エのロードバランシング機能は、並列に運用されている機器間での負荷がなるべく均等になるように処理を分散して割り当てることである。

例題演習

ＩＳＭＳプロセスのＰＤＣＡモデルにおいて，ＰＬＡＮで実施するものはどれか。

ア　運用状況の管理　　イ　改善策の実施

ウ　実施状況に対するレビュー　　エ　情報資産のリスクアセスメント

解答解説

ＩＳＭＳプロセスに関する問題である。

ＩＳＭＳは企業や組織が自身の情報セキュリティを確保・維持するために、ルール（セキュリティポリシー）に基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのことである。ＩＳＭＳに求められる範囲は、ISO/IEC15408などが定めるような技術的な情報セキュリティ対策のレベルではなく、組織全体に渡ってセキュリティ管理体制を構築・監査し、リスクマネジメントを実施することである。

ＩＳＭＳの定義としてJIPDECは、「ＩＳＭＳとは、個別の問題ごとの技術対策のほかに、組織のマネジメントとして自らのリスク評価により、必要なセキュリティレベルを定め、プランを持ち、資源配分してシステムを運用することである」、また、「組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し改善することがＩＳＭＳの要求する主なコンセプトである」と設定している。

ＰＤＣＡは業務の改善で計画－実施－確認－対応策の４フェーズを繰り返すことである。

リスクアセスメントとは、リスクの大きさを評価し、そのリスクが許容できるか否かを決定する全体的なプロセスのことである。具体的には、リスク分析により明確化されたリスク因子に基づき、リスク因子により組織の財務基盤にどのような悪影響を及ぼしうるかを評価し、それにより、どのリスク因子を優先的に対処していくかの優先順位決定し、リスク対処のコストパフォーマンスを上述の財務基盤への影響度も絡めて分析評価し検討する。

アの運用状況の管理はＤの実施、イの改善策の実施はＡの対応策、ウの実施状況のレビューはＣの確認、エの情報資産のリスクアセスメントはＰの計画である。求める答はエとなる。

例題演習

ＪＩＳＱ27001:2006におけるＩＳＭＳの確立に必要な事項①～③の順序関係のうち，適切なものはどれか。

① 適用宣言書の作成
② リスク対応のための管理目的及び管理策の選択
③ リスクの分析と評価

ア ①→②→③　　イ ①→③→②
ウ ②→③→①　　エ ③→②→①

解答解説

ＩＳＭＳの確立手順に関する問題である。

ＩＳＭＳは企業や組織が自身の情報セキュリティを確保・維持するために、セキュリティポリシーに基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みのことである。組織全体に渡ってセキュリティ管理体制を構築・監査し、リスクマネジメントを実施することである。JIPDECの定義は、「ＩＳＭＳとは、個別の問題ごとの技術対策のほかに、組織のマネジメントとして自らのリスク評価により、必要なセキュリティレベルを定め、プランを持ち、資源配分してシステムを運用することである」、また、「組織が保

護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し改善することがＩＳＭＳの要求する主なコンセプトである」と設定している。

ＩＳＭＳの確立の手順は、リスクの分析と評価、リスク対応のための管理目的および管理策の選択、適用宣言書作成の順序で進める。求める答えはエとなる。

例題演習

システム障害を想定した事業継続計画（ＢＣＰ）を策定する場合，ビジネスインパクト分析での実施事項はどれか。

ア　ＢＣＰの有効性を検証するためのテストを実施する。
イ　情報システム障害時の代替手順と復旧手順について関係者を集めて教育する。
ウ　情報システムに関する内外の環境の変化を踏まえてＢＣＰの内容を見直す。
エ　情報システムに許容される最大停止時間を決定する。

解答解説

事業継続計画の策定に関する問題である。

ビジネスインパクト分析は不測の事態によって、業務が中断したりシステムが停止したりした場合のビジネスへの影響度を分析することである。

アはＢＣＰの有効性の検証、イは復旧手順の関係者への教育、ウはＢＣＰの内容の見直しであり、エの許容される最大停止時間の決定は不測事態発生時のビジネスへの影響度の分析に関係する内容である。求める答えはエとなる。

例題演習

ＢＣＰの説明はどれか。

ア　企業の戦略を実現するために，財務，顧客，内部ビジネスプロセス，学習と成長の視点から戦略を検討したもの
イ　企業の目標を達成するために業務内容や業務の流れを可視化し，一定のサイクルをもって継続的に業務プロセスを改善するもの
ウ　業務効率の向上，業務コストの削減を目的に，業務プロセスを対象としてアウトソースを実施するもの
エ　事業中断の原因とリスクを想定し，未然に回避又は被害を受けても速やかに回復できるように方針や行動手順を規定したもの

解答解説

ＢＣＰに関する問題である。

ＢＣＰ（事業継続計画）は、企業がビジネスコンティニュイティに取り組むうえで基本となる計画のことである。災害や事故などの予期せぬ出来事の発生により、限られた経営資源で最低限の事業活動を継続、ないし目標復旧時間以内に再開できるようにするために、事前に策定される行動計画である。

アはＢＳＣ、イはＢＰＲ、ウはアウトソーシング、エはＢＣＰとなる。求める答えはエとなる。

例題演習

ＩＳＭＳ適合性評価制度の説明はどれか。

ア　ISO/IEC 15408 に基づき，ＩＴ関連製品のセキュリティ機能の適切性・確実性を評価する。
イ　JIS Q 15001に基づき，個人情報について適切な保護措置を講じる体制を整備している事業者などを認定する。
ウ　JIS Q 27001に基づき，組織が構築した情報セキュリティマネジメントシステムの適合性を評価する。
エ　電子政府推奨暗号リストに基づき，暗号モジュールが適切に保護されていることを認証する。

解答解説

ＩＳＭＳ適合性評価制度に関する問題である。

ＩＳＭＳは、情報セキュリティを管理するための仕組みで、この仕組みの基準として用いるのが、 国際規格ISO/IEC 27001／日本工業規格 JIS Q 27001「情報セキュリティマネジメントシステムー要求事項」であり、構築されたＩＳＭＳが、ISO27001/JISQ27001に適合していることを、第三者が評価し、認定する制度がＩＳＭＳ適合性評価制度である。ＩＳＭＳのマネジメントシステムの基盤部分は、品質管理マネジメントシステム(QMS)ISO9001や環境マネジメントシステム(EMS)ISO14001などと調和が図られており、ＩＳＭＳ(ISO/IEC 27001)、ＱＭＳ(ISO9001)、ＥＭＳ(ISO14001) をまとめて“三大マネジメントシステム”などと言われている。

アはＩＴセキュリティ評価及び認証制度(JISEC)、イはプライバシーマーク制度、ウはＩＳＭＳ適合性評価制度、エは暗号モジュール試験及び認証制度 (JCMVP)である。求める答えはウとなる。

例題演習

情報システムへの脅威とセキュリティ対策の組合せのうち，適切なものはどれか。

	脅威	セキュリティ対策
ア	誤操作によるデータの論理的な破壊	ディスクアレイ
イ	地震と火災	コンピュータ内で複数の仮想化 OS を利用したデータの二重化
ウ	伝送中のデータへの不正アクセス	HDLC 手順の CRC
エ	メッセージの改ざん	公開鍵暗号方式を応用したディジタル署名

解答解説

ＰＫＩに関する問題である。

ＰＫＩは公開鍵暗号を使ったセキュリティ技術基盤である。ネットワーク上での盗聴、改ざん、なりすましを防止し、安全な情報通信を可能にするためのデジタル署名技術や製品で構成される。だれでも入手できる公開鍵によって通信データを暗号化し、受信者だけが持つ秘密鍵で復号する。一方で、通信相手が間違いなく本人であることを確認するために、デジタル署名に用いる公開鍵の正当性を保証する認証局を設けて、電子証明書と公開鍵を発行管理して、通信相手の正当性を証明する。

公開鍵暗号化技術、ＳＳＬを組み込んだWWWサーバ／ブラウザ、Ｓ／ＭＩＭＥを使った暗号化電子メール、電子証明書を発行する認証局構築サーバなど、広範な仕組みや技術を統合することによってＰＫＩは実現できる。

アのディスクアレイはデータを複数のディスクに分散して格納し、並列アクセス処理の向上化と信頼性を実現する。システム障害、媒体障害の復旧には役立つが脅威を除くものではない。

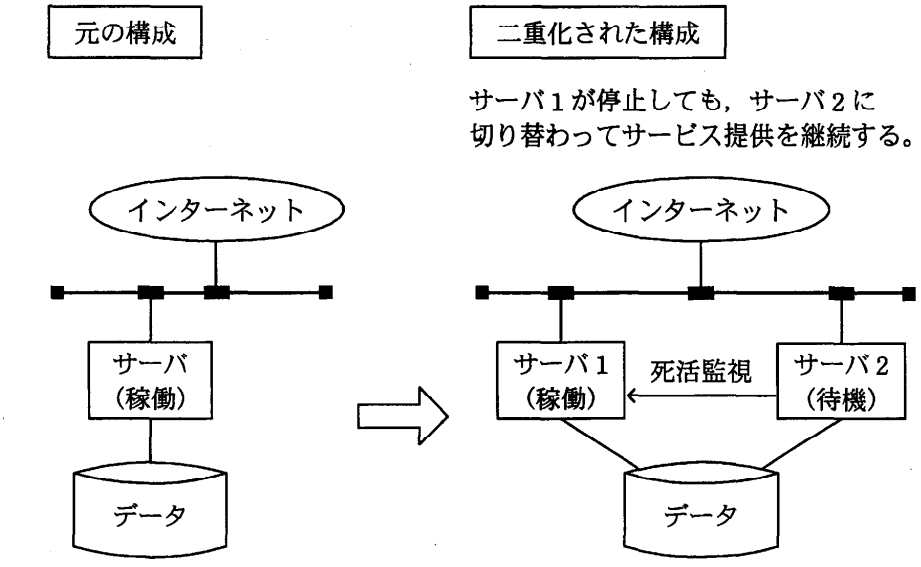
イの仮想化は１台のサーバコンピュータをあたかも複数台のコンピュータであるかのように論理的に分割するサーバ仮想化や、複数のディスクをあたかも１台のディスクであるかのように扱うストレージ仮想化などの技術である。地震や火災の対策にはならない。

ウのＣＲＣは伝送データの誤りの検出が可能であるが、不正アクセスの防止にはならない。

エの公開鍵暗号化方式を用いたデジタル署名は盗聴、改ざん、なりすましを防止し、安全な情報通信を可能にする。求める答えはエとなる。

例題演習

図のようなサーバ構成の二重化によって期待する効果はどれか。



ア　可用性の向上　　イ　完全性の向上

ウ　機密性の向上　　エ　責任追跡性の向上

解答解説

サーバの二重化の効果に関する問題である。

アの可用性の向上は、ネットワークやコンピュータ内の情報や資源がいつでも利用でき、資格を与えられたユーザが情報システムを適時に使用できる保証を高めることである。

イの完全性は、ネットワーク上やコンピュータ内の情報が常に完全な形で保たれ、不正によって改ざんされたり破壊されないことである。

ウの機密性はネットワーク上やコンピュータ内の情報を不適切な人間に見せないことである。

エの責任追跡性は、情報資産が改訂された履歴（ログ）などがたどれる状態を，責任追跡性が保たれているという。

サーバ構成の二重化は、信頼性の向上の手段であり、可用性の向上になる。求める答えはアとなる。

例題演習

経済産業省とＩＰＡが策定した”サイバーセキュリティ経営ガイドライン（Ｖｅｒ１．１）”が，自社のセキュリティ対策に加えて，実施状況を確認すべきとしている対策はどれか。

ア　自社が提供する商品及びサービスの個人利用者が行うセキュリティ対策
イ　自社に出資している株主が行うセキュリティ対策
ウ　自社のサプライチェーンのビジネスパートナが行うセキュリティ対策
エ　自社の事業所近隣の地域社会が行うセキュリティ対策

解答解説

サイバーセキュリティ経営ガイドラインに関する問題である。

経営者が留意すべき事項、セキュリティ責任者が指示すべき事項について、次の１０重要項目をまとめている。

① サイバーセキュリティリスクの認識、組織全体での対応の策定
② サイバーセキュリティリスク管理体制の構築
③ サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
④ サイバーセキュリティ対策フレームワーク構築と対策の開示
⑤ 系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施および状況把握
⑥ サイバーセキュリティ対策のための資源確保(予算、人材等)
⑦ ＩＴシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
⑧ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備
⑨ 緊急時の対応体制の整備、定期的かつ実践的な演習の実施
⑩ 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

以上の１０項目の内容は、自社のセキュリティ対策と系列企業やサプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施および状況把握に関するものである。

アはユーザ、イは株主、ウは系列企業やサプライチェーンのビジネスパートナー、エは地域社会である。求める答えはウとなる。

例題演習

ＢＹＯＤ(Bring Your Own Device)の説明はどれか。

ア　従業員が企業から貸与された情報端末を，客先などへの移動中に業務に利用することであり，ショルダハッキングなどのセキュリティリスクが増大する。
イ　従業員が企業から貸与された情報端末を，自宅に持ち帰って私的に利用することであり，機密情報の漏えいなどのセキュリティリスクが増大する。
ウ　従業員が私的に保有する情報端末を,職場での休憩時間などに私的に利用することであり，社内でのセキュリティ意識の低下などのセキュリティリスクが増大する。
エ　従業員が私的に保有する情報端末を業務に利用することであり，セキュリティ設定の不備に起因するウイルス感染などのセキュリティリスクが増大する。

解答解説

ＢＯＹＤに関する問題である。

ＢＯＹＤは、企業などで従業員が私物の情報端末などを持ち込んで業務で利用することである。私用で普段から使っているスマートフォンなどから企業の情報システムにアクセスし、必要な情報を閲覧したり入力したりすることなどを意味する。ＢＹＯＤを導入することで企業側は端末購入費や通信費の一部などのコストを削減することができ、社員側は同種の端末を２台持ちする必要がなくなり、普段から使い慣れた端末で仕事ができるというメリットがある。かかった経費は通信費の一部を会社が補助するといった運用が行われることが多い。

問題点は、端末の設定や導入するソフトウェアの種類などを企業側が完全にコントロールするのは難しい、情報漏洩・ウイルス感染などへの対策や、紛失・盗難時の対応などが複雑になる。業務中に利用できる機能やアクセスできるサイトを制限するといった対応も難しくなるなどがある。通信履歴や保存したデータなどをどこまで会社側が取得・把握するかといったプライバシーとの問題も発生する。

エの従業員が私的に保有する情報端末を業務に利用することであり、セキュリティ設定の不備に起因するウィルス感染などのセキュリティ対策が増大する内容が適切である。求める答えはエとなる。

例題演習

リスクアセスメントを構成するプロセスの組合せはどれか。

ア　リスク特定，リスク評価，リスク受容
イ　リスク特定，リスク分析，リスク評価
ウ　リスク分析，リスク対応，リスク受容
エ　リスク分析，リスク評価，リスク対応

解答解説

リスクアセスメントに関する問題である。

リスクアセスメントはリスク特定、リスク分析、リスク評価を網羅するプロセス全体を指す。リスク特定は、リスクを発見し、認識し、記述するプロセスである。リスク分析は、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である。リスク評価は、リスクが受容可能か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である。

リスクアセスメントはリスク管理プロセス内のサブプロセスである。安全工学上のリスクは、人、環境、物に悪い影響をあたえる可能性と大きさ(の積)である。予測されるリスクの可能性と大きさ(予測値)と、許容されるリスクの可能性と大きさ(許容値)を比較し、予想値が許容値を上回った時リスク軽減の施策又はリスク回避の施策をとるという意思決定を行い、実際にその施策をとり、より安全な状態を実現するプロセスをとることになる。このプロセス全体がリスク管理プロセスである。リスクアセスメントはリスク管理プロセス内の意思決定サブプロセスとなる。

リスクアセスメントを構成するプロセスの組み合わせは、リスク特定、リスク分析、リスク評価である。求める答えはイとなる。

例題演習

セキュリティバイデザインの説明はどれか。

ア　開発済みのシステムに対して，第三者の情報セキュリティ専門家が，脆弱性診断を行い，システムの品質及びセキュリティを高めることである。

イ　開発済みのシステムに対して，リスクアセスメントを行い，リスクアセスメント結果に基づいてシステムを改修することである。

ウ　システムの運用において，第三者による監査結果を基にシステムを改修することである。

エ　システムの企画・設計段階からセキュリティを確保する方策のことである。

解答解説

セキュリティバイデザインに関する問題である。

セキュア・バイ・デザインは、システムやソフトウェアの企画・設計、開発の段階からセキュリティ対策を組み込む考え方のことである。昨今のサイバー攻撃は企業等に大きな損失を与える可能性があることが認識されるようになり、運用時だけでなく、システムやソフトウェアの設計や開発段階で、セキュリティ対策を考慮する「セキュア・バイ・デザイン」の考え方に注目が集まっている。「セキュア・バイ・デザイン」を実現するための技術や手法には、プログラムの実行状態やソースコードを解析・検証する「プログラム解析」や、システムやアプリケーションなどの複数のコンポーネント間の通信プロトコルの正しさを検証する「プロトコル検証」といった様々なものがある。標的型攻撃などのように、特定のターゲットに対し、周到に、時間をかけて準備され、継続的に実行されるサイバー攻撃に対応していくためには、様々な観点からセキュリティを考え、対策を実施することが重要である。「セキュア・バイ・デザイン」はその対策の一つとして、システムの運用段階で実施される各種セキュリティ対策と併せて実施していく必要がある。求める答えはエとなる。

例題演習

会社や団体が，自組織の従業員に貸与するスマートフォンに対して，セキュリティポリシに従った一元的な設定をしたり，業務アプリケーションを配信したりして，スマートフォンの利用状況などを一元管理する仕組みはどれか。

ア　ＢＹＯＤ（Bring Your Own Device）
イ　ＥＣＭ（Enterprise Contents Management）
ウ　ＬＴＥ（Long Term Evolution）
エ　ＭＤＭ（Mobile Device Management）

解答解説

ＭＤＭに関する問題である。

アのＢＹＯＤは、企業などで従業員が私物の情報端末などを持ち込んで業務で利用することである。私用で普段から使っているスマートフォンなどから企業の情報システムにアクセスし、必要な情報を閲覧したり入力したりすることである。

イのＥＣＭは、企業や組織における情報の蓄積、管理、運用を統括的、包括的に行うための技術やシステムのことである。

ウのＬＴＥは、第３世代携帯電話のデータ通信を高速化した規格で。第４世代への橋渡しという意味で(第３．９世代)とも呼ばれる。

エのＭＤＭは、企業などで社員に支給するスマートフォンなどの携帯情報端末のシステム設定などを統合的・効率的に管理する手法である。また、それを実現するソフトウェアや情報システムなどのことである。求める答えはエとなる。

例題演習

JISQ27000:2014（情報セキュリティマネジメントシステム―用語）において，“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”と定義されているものはどれか。

ア　真正性　　イ　信頼性　　ウ　責任追跡性　　エ　否認防止

解答解説

真正性に関する問題である。

情報セキュリティの７特性である機密性、完全性、可用性、真正性、責任追跡性、否認防止、信頼性に関係する問題である。

アの真正性は、ある主体または資源が、主張通りであることを確実にする特性である。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。求める答えはアとなる。

イの信頼性は、意図した動作および結果に一致する特性である。

ウの責任追跡性は、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である。

エの否認防止は、ある活動または事象が起きたことを、後になって否認させないように証明

する能力である。

例題演習

機密ファイルが格納されていて，正常に動作するＰＣの磁気ディスクを産業廃棄物処理業者に引き渡して廃棄する場合の情報漏えい対策のうち，適切なものはどれか。

ア　異なる圧縮方式で，機密ファイルを複数回圧縮する。
イ　専用の消去ツールで，磁気ディスクのマスタブートレコードを複数回消去する。
ウ　特定のビット列で，磁気ディスクの全領域を複数回上書きする。
エ　ランダムな文字列で，機密ファイルのファイル名を複数回変更する。

解答解説

機密ファイルの廃棄処理に関する問題である。

データの利用に際しては、効率的な利用方法とセキュリティ保持が重要である。廃棄後のデータは管理されないため、重要情報が漏洩しやすい。不要になったデータの廃棄に当たっては、重要データの漏洩を防止するため、厳重なチェックが不可欠である。データの廃棄に当たっては、適切な方法の選択の他にも管理上、留意すべきことがある。特に、セキュリティ上の必要性とデータ保全の必要性を考慮することが重要である。

ＰＣの磁気ディスク上のデータの消去は、特定のビット列をディスクの全領域に上書き処理することによって読み出し不能にする。求める答えはウとなる。

アのデータの圧縮では、伸張の可能性があり、適切ではない。

イのマスタブートレコードを消去しても、静的に読み出すことが可能である。

エのファイル名を変更しても、ディスクから直接、データを読み出すことは可能である。

データ廃棄の方法として次の表に示す処理方法がある。

廃棄手段	内容、特徴、留意点
消磁、消去	磁気ディスクや磁気テープに保存された磁気データを消してから廃棄する 情報システムにおけるデータ廃棄の主要な方法である。 磁気ディスクの全領域を特定のビット列で複数回上書き処理する。
破壊	磁気媒体以外に保存されたデータの廃棄の際に用いる。 焼却が困難な媒体を使用している場合に有効である。
焼却、溶解	紙の上に記録されたデータを廃棄するのに最も適した方法である。 廃棄量が多くなるため、外部の専門業者に委託することが行われる。 セキュリティ上の問題が発生する恐れがあるため、書類の内容が見えない状態で外部に出す配慮が必要になる。
裁断	機密性の高い書類データを廃棄する際に用いられる方法である。 焼却と溶解の組合せが考えられる。

txt030412　コンピュータウィルス

①　ウィルス、ワーム、トロイの木馬

ⓐ　ウィルス

コンピュータウィルスはコンピュータのソフトウェアに密かに仕掛けられ、勝手にプログラムやデータを破壊したり書き換えたりしてしまう悪性のソフトウェアである。インターネット経由での感染が急増している。コンピュータウィルス対策基準では、自己伝染機能、潜伏機能、発病機能のうち、一つ以上の機能を有するプログラムと定義している。

ⓑ　ワーム

ワームはコンピュータウィルスの一種で、ネットワークを感染経路にして自己増殖し、システムに害を与える悪質なコンピュータプログラムである。ワーム自体は破壊を行わないが、増殖を繰り返していくことでコンピュータのＣＰＵの処理やディスクの容量などを占有し、システムに負荷をかけたり、停止させたりする。ワームなどを含む不正プログラム全体をウィルスと呼んでいる。

ⓒ　トロイの木馬

トロイの木馬はウイルスの一種で、パソコン・スマホに対し悪影響を与えるソフトウェアである。その特徴は、ギリシャ神話にならって偽装してひっそり攻撃を狙うウイルスといわれ、便利で悪意のないプログラムと見せかけて侵入し、感染したことを気づかせないように情報を盗んだりする。

ⓓ　トロイの木馬の種類

㋐　ダウンロード型

新しいウイルスをダウンロードするタイプのトロイの木馬で、感染するとパスワードを漏えいさせるもの、広告を表示するものなどがある。

㋑　クリッカ型

ブラウザの管理者設定を改変したり、勝手にウェブサイトへ接続させたりする種類で、勝手にブラウザを起動する能力があり、特定サイトのアクセス数を増やしたり、攻撃のターゲットとするサイトにＤｏＳ・ＤＤｏＳ攻撃を仕掛けたりする。

㋒　バックドアー型

攻撃者からの遠隔操作を可能にする危険なタイプで、感染した場合、不正アクセスの踏み台に利用される可能性が高く、遠隔操作により企業サイトなどのハッキングに悪用されると、犯罪者に間違えられる可能性があり、個人情報やクレジットカード番号などの重要情報が流出させられる危険がある。

㊓　**パスワード窃盗型**

感染したパソコン内のパスワード、ＩＰアドレスやコンピューターの詳細情報などを収集、攻撃者に対してメールなどで情報を送信して流出させるウイルスで、ＩＰアドレスなどの情報が盗まれ、支配権が奪われる場合もある。

㊔　**プロキシ型**

感染者のパソコンのネットワーク設定を改変してしまうウイルスで、感染者のＩＰを使ってＷＥＢサイト改ざんなどの犯罪行為をおこなうので、犯罪者に仕立てられる可能性がある。

㊕　**ドロッパー型**

さらなる悪意あるソフトを複数インストールさせるための実行役プログラムとしての役割を持っている。

㊖　**迷彩型ゼウス**

2014年に発見されたトロイの木馬の亜種で、画像データに偽装したウイルスである。現時点で日本国内において感染報告はないが、ドイツ・イタリアなどヨーロッパを中心に被害が拡大中である。今後、国内で亜種が発見される可能性もゼロではない。

ⓔ　トロイの木馬の感染症状

㋐　勝手にパソコンの電源が落ちる
㋑　セキュリティソフトが無効化される
㋒　タスクマネージャーで不自然にＣＰＵ使用率が変動する

ⓕ　トロイの木馬の感染時の被害

㋐　**各種サービスの個人情報を抜かれる**

会員制サービスのログインＩＤ・パスワードのほか、登録した個人情報を抜かれる可能性があり、通販サイトに不正ログインされ、クレジットカードが悪用されたり、ネットバンキングに不正ログインされ、預金が外部へ不正送金されたりする。

㋑　**ウイルス・スパムメールの送信元となる**

メールアカウントを乗っ取られると、アドレス帳の中身が盗まれるほか、迷惑メール送信元として悪用される場合がある。受信メールボックスに、送信失敗を伝える英語のメールを大量受信したり、メールを送ろうとしても、どこにも送れなくなったり、知り合いから「変なメールが届いた」と連絡がきたりする。

㋒　**ＷＥＢカメラやマイクで盗撮、盗聴される**

パソコンやスマホのＷＥＢカメラ・マイクを自由に操作され、盗撮・盗聴されてネット上に拡散されてしまう。

㋓　**キーボード入力した内容を監視される**

サイトのログイン情報ほか、機密情報を漏えいしてしまう可能性がある。

㋔　**不正な投稿をさせられる**

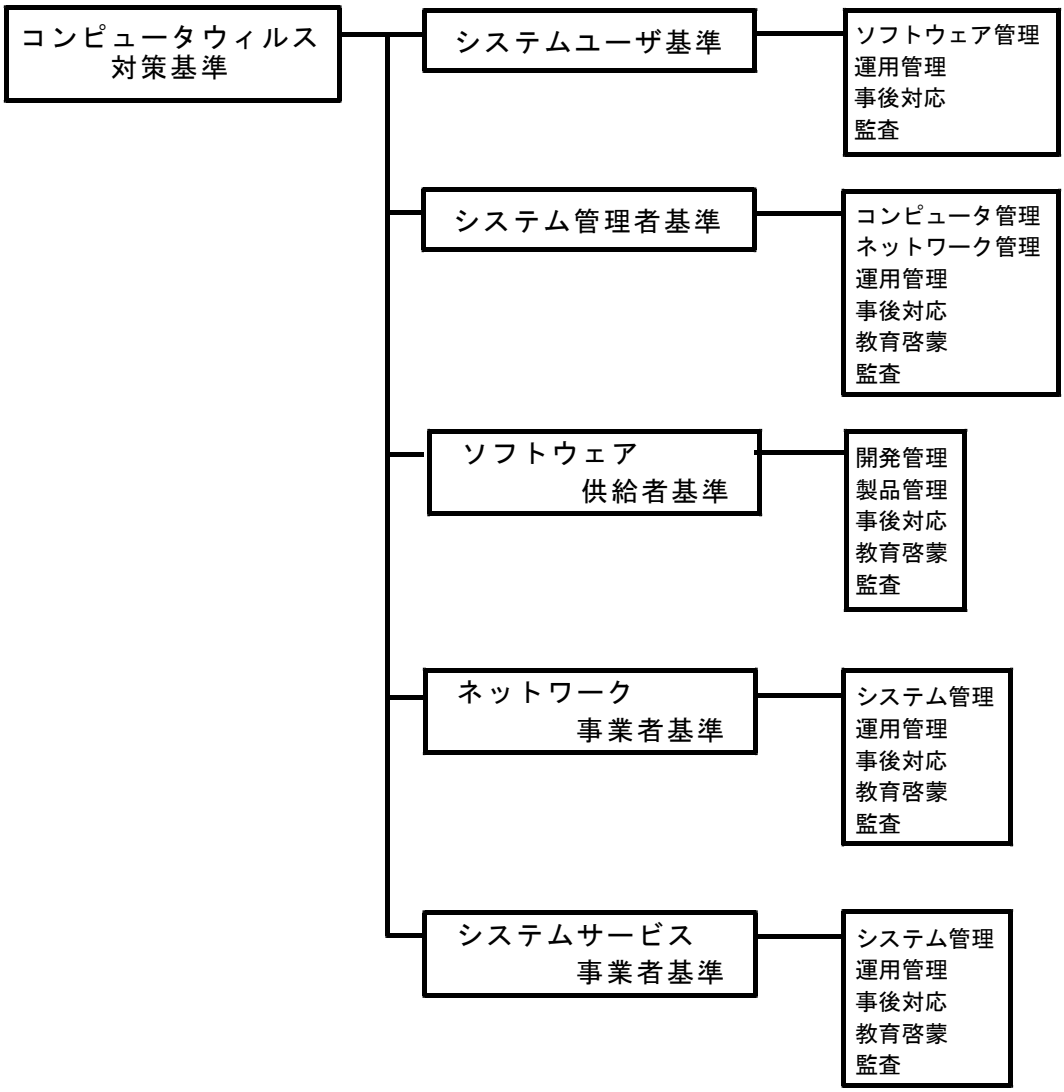
㋕　**不正アクセスの踏み台にされる**

②　コンピュータウィルス対策基準とウイルスの機能

ⓐ　「コンピュータウィルス対策基準」

コンピュータウィルス対策基準は、平成７年７月コンピュータウィルスの侵入を防ぐガイドラインとして告示、施行された。その後改訂されて、現在の基準は、システムユーザ基準が18項目、システム管理者基準が31項目、ソフトウェア供給者基準が21項目、ネットワーク事業者基準15項目、システムサービス事業者基準19項目、計104項目から構成されるている。

この対策基準は強制力はない。使用するコンピュータの種類や個々のソフトウェアの実態に即して適用すればよい。被害にあった際には、ＩＰＡに届け出る制度がある。



ⓑ　コンピュータウィルスの機能

ウィルスは第三者に危害を与える不正プログラムのうちでも、感染／潜伏／発病というルーチンを持つものである。プログラムファイルやデータの中に寄生し、パソコン通信やインターネットからダウンロードしたファイルや電子メール、フロッピーディスクなどを通じてシステムに侵入する。侵入したコンピュータウィルスは、一定の潜伏期間を経て、ある条件によ

って活性化し、様々な現象を引き起こす。最近の不正プログラムは、潜伏期間をおかずに発病するもの、発病の過程でシステム領域を破壊するもの、発病せずに感染活動を繰り返すものなど様々なものが登場している。

ⓒ　通産省の告示第429号よるウィルスの機能

㋐　自己伝染機能

自らの機能によって他のプログラムに自らのプログラムをコピーし、またはシステム機能を利用して自らのプログラムを他のシステムにコピーすることにより、他のシステムに伝染する機能である。

㋑　潜伏機能

発病するための特定時刻や一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能である。

㋒　発病機能

プログラムやデータ等のファイルの破壊を行ったり、設計者の意図しない動作をするなどの機能である。

③　侵入経路による分類

ⓐ　電子メール経由の感染

システム感染型は、フロッピーディスクを介してハードディスクのブートセクタに感染し、システムを起動するたびにメモリに読み込まれてしまうタイプである。ファイル感染型は、プログラムファイルに感染し､感染プログラムを起動するとメモリに読み込まれるタイプである。

ⓑ　外部媒体による感染

直接感染型ウィルスは、感染ファイルを実行すると、感染していないファイルを探してそのファイルに直接感染する。拡張子ＥＸＥ、ＣＯＭ、ＳＹＳ、ＤＬＬのファイルを感染対象とする。単純なファイル感染型ウィルスやマクロ型のウィルスの多くはこの形態で感染する。メモリ常駐型ウィルスは、活動開始からコンピュータの電源を切るまでメモリに常駐する。

常駐したウィルスは感染対象のファイルや領域を探して次々と感染する。割込機能に寄生し、対策システムの網をかいくぐって被害を与える。多くのファイル感染型ウィルスと一部のシステム領域感染型ウィルスに見られる形態である。駆除するには、コンピュータの電源を必ず切り、救済ディスクを使用して起動してから駆除を行う必要がある。

ⓒ　ダウンロードによる感染

追記感染型ウィルスは、感染対象のファイルの最後にウィルスプログラムを追加して感染する。感染したファイルはファイルサイズが大きくなる。上書き感染型ウィルスは、感染対

象のファイルにウィルスのプログラムコードを直接上書きして感染する。感染したファイルは破壊されてしまうため復旧にはバックアップファイルが必要になる。ウィルスコードが記述された部位によっては、どのような動きが起こるか特定できない場合がある。

④　感染ターゲットによる分類

ⓐ　ブートセクタ感染型

ハードディスクやフロッピ・ディスクの起動用プログラムを収める領域に感染する。ウィルスがブートセクタに感染すると、ＯＳが起動する前にメモリに読み込まれてＣＰＵが実行する。この状態でパソコンにディスクなどが挿入されると、ディスクも次々と感染する。

ⓑ　実行ファイル感染型

.comや.exeなどの実行ファイルに感染する。ユーザがウィルスに感染したプログラムを実行すると、パソコン内にある他の感染可能なプログラムファイルを加工し、ウィルスコードをコピーする。加工の仕方には、上書き感染型、追記感染型、隙間感染型の３パターンがある。

実行ファイルに感染すると同じような感染が、データファイルに対しても行われる。

ⓒ　スクリプト感染型

マイクロソフトの文書ファイルやＨＴＭＬファイルに感染する。ユーザがウィルス入りのデータを開くと、データファイルに対応するアプリケーションがデータファイルに書かれているスクリプトを実行し、ウィルスが起動し、自身のスクリプトを他のデータファイルにも追加していき感染を広める。

ⓓ　セキュリティホール攻撃型

プログラムのセキュリティ上の弱点を突いて感染する。セキュリティホールを攻撃するタイプのウィルスが狙うのは、ＯＳやプログラムのバグを利用する。

⑤　電子メールとセキュリティ

ⓐ　５つの危険

電子メールを使用する場合の５つの危険には次のものがある。

㋐　ウィルス
㋑　スパム
㋒　パスワード漏洩
㋓　盗聴

㋔　なりすまし

ⓑ　ウィルス

メール経由で感染するウィルスが潜む場所は、添付ファイルか、ＨＴＭＬメールの本文である。添付ファイルの場合は、実行ファイルか、文書ファイルのマクロやスプリプトに埋め込まれている。ＨＴＭＬメールでは、様々な色、文字、画像の中に埋め込まれている。ウィルス対策にはＯＳやメールソフトのバグをなくし、スクリプトの実行禁止、開く添付ファイルの限定、感染した場合にはウィルスメールを他のパソコンに送信しない対策んどが必要となる。

ⓒ　メールの添付ファイルの取り扱い

㋐　見知らぬ相手先から届いた添付ファイル付きのメールは厳重注意する
㋑　添付ファイルの見た目に惑わされない
㋒　知り合いから届いた変な添付ファイル付きのメールは疑ってかかる
㋓　メールの本文でまかなえるものをテキスト形式等のファイルで添付しない
㋔　各メーラー特有の添付ファイルの取り扱いに注意する

ⓓ　スパム

スパムは、受信者の意向を無視して、無差別かつ大量に一括してばらまかれる、各種ネットメディアにおけるメッセージのことで広告などを目的としたものがある。対策としてはメールソフトのフィルタの使用やプロバイダのフィルタリングサービスを使用する方法がある。

ⓔ　パスワード漏洩

パスワード漏洩の危険が高いのは外出先からのアクセスである。通信経路に信頼できない第三者が介在したり、無線ＬＡＮで簡単に傍受できる区間がある場合は漏洩しやすい。自宅や会社から契約プロバイダ間のアクセスなら問題は少ないが、途中に何社か経由すると危険度が高くなる。対策としてはパスワードの暗号化が必要になる。

ⓕ　盗聴となりすまし

ホテルや無線ＬＡＮサービス、海外からのアクセスは盗聴されている前提で対策を検討する必要がある。対策には暗号化技術の活用である。

なりすましは、送信者を偽る行為で、本人でない送信者が本人であると偽って発信する行為である。対策は電子署名を追加する処置があり、Ｓ／ＭＩＭＥやＰＧＰの仕組みを使用する。

⑥　セキュリティ・ホールへの攻撃

ⓐ　バッファ・オーバフロー

バッファオーバーフローは、プログラムで用意してあるバッファの大きさを越えるデータが入力されたり送り込まれることで、システムが誤動作を起こしたり、悪意のあるプログラムが実行できてしまう状態のことである。バッファオーバーフローは、想定以上のデータ長を受け入れないようにガードされていないプログラムで発生し、その脆弱性につけ込む。バッファオーバーフローを悪用して、ウィルスを混入したり、システムに侵入してファイルを削除したり、情報を盗んだりすることも可能となる。

ⓑ　ＳＱＬインジェクション

ＳＱＬインジェクションは、Ｗｅｂサイトで、データベースへの問い合わせや操作を行うプログラムにパラメータとしてＳＱＬ文の断片を与え、データベースを改ざんしたり不正に情報を入手する攻撃である。

Ｗｅｂアプリケーションではデータベースの操作にＳＱＬ言語を利用している。ユーザがフォームから送信した検索語などのパラメータを受け取り、これをＳＱＬ文に埋め込んでデータベースへの問い合わせや操作を行う。このとき、ＳＱＬ文として解釈できる文字列をパラメータに含めることで、プログラムが想定していないＳＱＬ文を合成し、不正にデータベースの内容を削除したり、本来アクセスできない情報を表示させたりすることができてしまう。

ⓒ　クロスサイト・リクフェスト・フォージェリ（ＣＳＲＦ）

ＣＳＲＦは、Ｗｅｂサイトの攻撃手法の一種で、悪意のあるスクリプトやＵＲＬにアクセスし、意図しないＷｅｂサイト上の操作を行わせる手法である。正規ユーザが本来想定されている操作を行ったかのようにリクエストを発生させる。ＣＳＲＦによる代表的な被害としては、掲示板への意図しない書き込みや、ショッピングサイトで買うつもりの無い商品を買ってしまうといったものがある。防ぐための対策としては、リクエストが正しい画面遷移を経て送信されているかをチェックしたり、リクエストを受け付ける前に確認画面をはさむといった方法がある。前者の方法では、画面を識別するために外部からは予測不可能な使い捨てＩＤを発行し画面遷移をチェックしたり、簡易にはリファラ情報を照合するなどの手法が用いられる。後者の方法では、確認画面で再度パスワードを入力させたり、ＣＡＰＴＣＨＡと呼ばれる画像として表示した文字をユーザに判読させ入力させるなどの手法が用いられる。

ⓓ　クロスサイト・スクリプティング（XSS）

クロスサイトスクリプティングはユーザのアクセス時に表示内容が生成される動的Ｗｅｂページの脆弱性を利用した攻撃方法のことである。動的Ｗｅｂページの表示内容生成処理の際、Ｗｅｂページに任意のスクリプトが紛れ込み、Ｗｅｂサイトを閲覧したユーザ環境で紛れ込んだスクリプトが実行されてしまう。

ⓔ　ディレクトリトラバーサル攻撃

ディレクトリトラバーサルは、ネットワーク上の脆弱性を利用した攻撃手法の一種で、「../」を利用してディレクトリを遡り、本来はアクセスが禁止されているディレクトリにアクセスする手法のことである。または、そのような脆弱性のことである。ネットワーク上でディレクトリのパスを指定する際、「一つ上の階層へ上る」ことを指示する「../」のパスを組み合わせて指定することで、公開されているディレクトリの上階層から、その併置されている非公開のディレクトリへアクセスできてしまう場合がある。このような操作によって、個人情報や機密情報を盗まれたり､悪意あるコードを書き込まれたりといった被害を被る危険性が生じる。

⑦　スパイウェア

ⓐ　スパイウェアの脅威

スパイウェアは、パソコン内にある個人情報やユーザーがどのようなサイトをよく見ているかの行動などを監視し、自動的に情報を外部に送信するソフトやプログラムのことである。スパイウェアは、マーケティング活動の１つとして用いられることが多い。自分が購入や閲覧した商品そのものやその類似商品についての広告がよく表示されるというケースは、そのユーザーの閲覧情報を基にポップアップ広告を出す仕組みが利用されている。一方で、スパイウェアがあるとは知らせずに、ソフトを使用させてユーザーの行動を監視したり、パソコンを経由して個人情報を盗むという悪質な使い方をするケースもある。インターネットバンキング利用時に利用者により入力される口座番号やログインＩＤ、パスワードなどの情報を盗み出して外部に送信するというものがある。

ⓑ　スパイウェア対策

スパイウェアの対策方法は、セキュリティソフトを最新の状態にアップデートし、パソコンのＯＳを最新にするということが基本となる。その他に、怪しいサイトをむやみに閲覧しない、怪しいメールに添付されているファイルを開かない、無料ソフトをダウンロードする際には使用許諾書などをしっかりと読みリスクを把握する、どうしてもソフトをダウンロードする際には信頼できるサイトからダウンロードするということがポイントになる。

⑧　フィッシング

ⓐ　フィッシングの手口

フィッシングは、金融機関などからの正規のメールやＷｅｂサイトを装い、暗証番号やクレジットカード番号などを詐取する詐欺である。メールの送信者名を金融機関の窓口などのアドレスにしたメールを無差別に送りつけ、本文には個人情報を入力するよう促す案内文とＷｅｂページへのリンクが載っている。リンクをクリックするとその金融機関の正規のＷｅｂサイト

と、個人情報入力用のポップアップウィンドウが表示される。メインウィンドウに表示されるサイトは「本物」で、ポップアップページは「偽者」である。本物を見て安心したユーザがポップアップに表示された入力フォームに暗証番号やパスワード、クレジットカード番号などの秘密を入力・送信すると、犯人に情報が送信される。

ⓑ　フィッシング対策

偽サイトを見抜く方法には次のものがある

㋐　アドレスバーに表示されたURLを確認する
㋑　ブラウザの「カギマーク」表示を確認する
㋒　URLが「https～」で始まっているか確認する
㋓　そのページの「ソース」を確認する

セキュリティソフトはウイルス対策だけでなく、さまざまな機能を駆使して総合的にセキュリティ対策を行う。フィッシング対策として、次のような機能がある。

㋐　迷惑メールを未然にブロック
㋑　リアルタイムでウイルスをブロック
㋒　個人情報を送信する際にブロック
㋓　個人情報保護ログで証拠を記録

⑨　ウィルス対策

ⓐ　ウィルス対策の７箇条

㋐　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こと
㋑　メールの添付ファイルは、開く前にウイルス検査を行うこと
㋒　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こと
㋓　アプリケーションのセキュリティ機能を活用すること
㋔　セキュリティパッチをあてること
㋕　ウイルス感染の兆候を見逃さないこと
㋖　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こと

ⓑ　ワクチンプログラム

ワクチンプログラムはコンピュータウィルスを検知・駆除するためのユーティリティソフトウェアである。検知・駆除するだけであり、破壊されたデータの修復をすることができない。発見されたウイルス定義情報を登録したパターンファイルをもとに、ディスクやファイル内に潜むウイルスを検出する。

最近のウィルス被害は、電子メールの添付文書ファイルに付いたマクロウィルスによるものが増加している。マクロウィルスは、電子メールを受け取ると自動的にウィルスもコンピュータの中に入ってくる。このため、予防やウィルス駆除の機能を持つワクチンプログラムが重要性を増してきている。

ⓒ　ワクチンプログラムの基本機能

㋐　ウィルス検査機能：既知ウィルスの検出
㋑　ファイルの変更チェック機能：未知ウィルスの検出
㋒　修復機能：発見したウィルスの駆除
㋓　百科事典機能：発見したウィルスの詳細調査

ⓓ　ウィルス駆除のための管理体制

ワクチンプログラムは新しいウィルスが次々に現れており、古いワクチンプログラムでは十分に対応できないため、パターンファイルを常に最新の状態にしておく必要がある。ウイルスに感染した場合、直ちに、ネットワークから切り離し、駆除すると共に、情報処理振興事業協会(ＩＰＡ)に届ける。企業のシステム管理者は、運用面のルールを整備し、最新のワクチンプログラムを提供する体制を整える。データのバックアップ、被害時の報告制度、感染ファイルの除去対策などの管理体制の整備が必要になる。

市販されているウィルス対策のソフトウェアとして、Norton AntiVirus、VirusScan、ウィルスバスターなどがある。

⑩　ワクチンプログラムの検知の仕組み

ⓐ　コンペア法（比較法）

㋐　コンペア法は、新規に受け取ったファイルがウイルスをもっているか発見するのではく、ウイルス感染していなかった既存のファイルが、その後、感染したかどうかを発見する手段である。
㋑　ウイルス感染以前のファイルと現在のファイルを比較して、異なっていればウイルスに感染したのではないかと疑う方法である。
㋒　仕組みは簡単であるが、ウイルス感染以前のファイルを保管しておく必要があり、比較するファイルが多くなると長時間かかることになる。そこで、あらかじめ感染の恐れのあるファイルや重要なファイルを指定しておく。

ⓑ　チェックサム法

㋐　コンペア法をさらに簡便にしたもので、感染以前のファイルの容量やハッシュ値を記録しておき、それらが変化していたら感染したと疑う方法である。
㋑　以前のファイルの内部に立ち入らないので短時間でスキャンできる。ウイルス作者が容量を変化させない方法やハッシュ値を変更させる手段などを知っているのと、厳格な検出ができなくなる。
㋒　コンペア法やチェックサム法だけでウイルス感染を決めつけることはできないが、さらに他の方法で検査するための対象ファイルを絞り込むことができる。通常のウイルス対策ソフトで、これらの方法だけをもつのは稀です。

ⓒ　パターンマッチング法

㋐　パターンマッチング法は、ウイルス対策ソフトの基本になっている方法で、既発見ウイルスの特徴パターンをデータベース化した定義ファイルを用いて、対象となるファイルに同一または類似したシグニチャが存在したら、ウイルスに感染しているとする方法である。
㋑　効率的に高い検出率が得られることから広く利用されている。
㋒　定義ファイルに登録されていないパターンを持つウイルスは検出できない。
㋓　定義ファイルを更新せずに古いまま使っていると、最新のウイルスは検出できないことになる。定義ファイルを最新版に保つために、多くのウイルス対策ソフトでは、自動的にオンライン更新する機能をもっている。

ⓓ　ビヘイビアブロッキング法（ジェネリック法）

㋐　未知のパターンをもつウイルスを発見する方法である。
㋑　実行しているプログラムをリアルタイムに監視し、不正な動作をする命令をモニタリングし、その命令がコールされると、その実行をブロッキングする。
㋒　正規のプログラムでもＯＳへのシステムコールやファイル更新などを行うため、正常な指令なのかウイルスなのかを見極めることが重要で、そのためのルールを定義したデータベースの整備と維持更新が必要になる。

ⓔ　ヒューリスティック法

㋐　ヒューリスティック法は、ウイルス対策ソフトに任せるのではなく、対策担当者が疑わしいと判断したプログラムを安全な環境で検査する方法である。それを支援すつツールがある。人間とツールが協力することからヒューリスティックという。
㋑　対象ファイルを分析することにより、実行動作を予測し、不正動作であるかどうかを確認する静的ヒューリスティックと、安全な環境を設定し、その環境で実際に動作させて検査する動的ヒューリスティックがある。

⑪　代表的なウィルス・犯罪手口

ⓐ　サラミ法

サラミ法は多数の資源からわずかずつ資産を搾取する方法である。預金システムの利息の端数処理プログラムを操作して、切り捨て額を犯人の口座に振り込ませる。プログラムの操作にはトロイの木馬を応用する。

ⓑ　論理爆弾、電子メール爆弾

㋐　論理爆弾

論理爆弾は通常のプログラムに未承認のプログラムを組み込んで、特定の条件の発生や特定のデータの入力を起爆剤として、コンピュータに不正行為を実行させる。未承認コードの挿入にはトロイの木馬を応用する。

㋑　電子メール爆弾

電子メール爆弾は特定の相手に対して大量あるいは容量の大きな電子メールを短時間に送信する。メールシステムの障害につながる。

ⓒ　マクロウィルス

マクロウィルスは表計算やワープロなどのマクロ言語で記述された文書データに潜み、電子メールを介して送信相手に感染するタイプのウイルスである。感染経路は電子メールの添付ファイルが利用され、文書を開いたときに自動的に実行されることで、他の文書ファイルに感染する。文書ファイルを開く前に、アプリケーションソフトのマクロ言語を使用しない設定にしておくことで、マクロウィルスの感染を防止できる。米国で発見されたメリッサが有名である。

ⓓ　メリッサ

メリッサは感染した電子メールを受け取ったユーザが、メールに添付されたWord文書を開き、自動的にマクロが実行されると直ちに感染し、同時に発病する。感染したパソコンに電子メールソフトのOutlook がインストールされていると、アドレス帳に登録された上から５０件の宛先にメリッサが添付された電子メールを送信する。

ⓔ　トラップドア、ミケランジェロ

トラップドアは大規模なアプリケーションやオペレーティングシステムの開発では、コードの途中にトラップドアと呼ぶ中断部分を設けて保守を容易にする。このトラップドアが削除されずに残されていると、未承認プログラムの挿入などに悪用する。

ミケランジェロはミケランジェロの誕生日にシステムを初期化するウイルスである。

ⓕ　クッキーモンスタ、タッピング

クッキーモンスタは特定のプログラムの動作を止めるウイルスであり、タッピングはネット

ワーク上の電文を不正に盗み取る行為である。

ⓖ　クリッパー、カスケード

クリッパーは記憶容量を食いつぶすウイルスであり、カスケードは画面の表示文字を下方に落とすウイルスである。

ⓗ　ランサムウエア

インターネット利用者のパソコンに感染し、ファイルを開けない状態にした後、復旧させる代わりに金銭を要求するウイルスである。

ⓘ　ボット

ボットはコンピュータを外部から遠隔操作するためのバックドア型不正プログラムの一種である。特徴はボットネットワークを構成することで、ボットネットワークは、攻撃者がＣ＆Ｃサーバから一括して複数のボット感染環境を遠隔操作できる仕組みである。

ⓙ　アカウントリスト攻撃

アカウントリスト攻撃はオンラインサービスへの不正ログインを狙った不正アクセス攻撃の一種で、不正ログインのためにＩＤとパスワードがセットとなったアカウント情報リストを利用することを示し、従来からある不正ログイン攻撃手法であるブルートフォース攻撃や辞書攻撃と区別するための呼称である。

ⓚ　ＵＳＢワーム

ＵＳＢワームとは、ＵＳＢメモリ、メモリカードなどＵＳＢ接続のリムーバブルメディアを媒介として増殖、拡散する不正プログラムである。特徴はWindowsの正規機能であるオートランと呼ばれる機能を悪用し、リムーバブルメディアの使用時にＵＳＢワームが自動的に実行される仕組みを実現する。感染システム上で使用されたリムーバブルメディアや全ドライブに、ワーム本体のコピーと自動実行のためのオートラン設定ファイルautorun.infを作成し、感染したリムーバブルメディアを他のコンピュータに接続すると、Windowsのオートラン機能によりワームが自動実行される。

①　ＤＮＳキャッシュポイズニング

ＤＮＳキャッシュポイズニングは、ＤＮＳがＷｅｂへのアクセスやメールの送受信などの際に、接続相手のＩＰアドレスを調べたりする仕組みに対して、ＤＮＳが偽の応答を返すようにしてしまう攻撃手法である。インターネットの利用者が、この攻撃により偽の応答をするようにされたＤＮＳを介してＷｅｂにアクセスすると、気づかないうちにフィッシングサイトに誘導されてしまう。

ⓜ　ブルートフォース攻撃、パスワードリスト攻撃

㋐　ブルートフォース攻撃

ブルートフォース攻撃は、暗号解読手法の一つで、考えられる全ての鍵をリストアップし、片っ端から解読を試みる方式である。暗号文の一部を復号プログラムにしたがって変換し、意味のある文章になるか調べる。どのような形態の暗号に対しても攻撃できるが、鍵の長さが増えると考えられる鍵のパターンの数は幾何級数的に増大するため、効率の悪い攻撃手法である。

㋑　パスワードリスト攻撃

パスワードリスト攻撃は、ネットサービスやコンピュータシステムの利用者アカウントの乗っ取りを試みる攻撃手法の一つで、別のサービスやシステムから流出したアカウント情報を用いてログインを試みる手法である。

ⓝ　ゼロディ攻撃

ゼロディ攻撃は、ソフトウェアにセキュリティ上の脆弱性(セキュリティホール)が発見されたときに、問題の存在自体が広く公表される前にその脆弱性を悪用して行われる攻撃である。

例題演習

ある会社の資材担当者が電子メールを取引先へインターネットで送信したところ，取引先から不明なファイルが添付されているとの連絡が入った。資材担当者はファイルを添付した覚えがなく，電子メールソフトのマニュアルを見ても，添付されるとは記載されていないファイルであった。この場合，資材担当者の取るべき行動のうち，適切なものはどれか。

ア　送信履歴の添付ファイルを開き，確認する。画面上に見覚えのない画面が表示された場合，送信履歴から送信メールを削除する。

イ　どのような内容が送信されたのか，添付ファイルを開いて確認してくれるように送信先に依頼する。

ウ　パソコンにデータ破壊などの異常が発生していなければ，問題なしと判断し，そのままにする。

エ　連絡を受けた時点で，取引先には，添付ファイルを開かないように依頼し，すぐに自社のセキュリティ対策担当部署に調査を依頼する。

解答解説

電子メールの添付ファイルの処理に関する問題である。

コンピュータウィルスは第三者のコンピュータシステムに侵入して正常な動作を妨げることを目的として作成されたプログラムである。電子メールの添付ファイルを開くだけで感染することがある。不審なメールは開かない、添付ファイルは自動的に開く設定にしないなどの対策が必要である。

アの履歴不明の添付ファイルを開くことは問題である。適切な動作ではない。

イの送信先にフィルを開くことを依頼するのも問題がある。開くと感染する可能性がある。

ウの現状問題がないという理由で、そのまま放置するのも問題である。ある時期に発病する可能性がある。

エの添付ファイルを開かないように連絡し、セキュリティ担当者に調査を依頼するのが適切である。求める答えはエとなる。

例題演習

通商産業省の“コンピュータウイルス対策基準”によるコンピュータウイルスの対策として，適切なものはどれか。

ア　ウイルスに感染した直後の対応として，一般利用者が最初にすべきことは，ウイルスの種類を解明し，特定することである。

イ　ウイルスに感染した媒体は，原則として廃棄する。どうしても廃棄できない重要なファイルがある場合だけ，ワクチンによるウイルスの駆除を試みる。

ウ　常に最新バージョンのワクチンプログラムを導入し，定期的にウイルスをチェックすることによって，ウイルスの感染を完全に防ぐことができる。

エ　バックアップファイルへのウイルス感染を防ぐには，バックアップ用の媒体として，ライトプロテクトを施せるものでは不十分であり，ライトワンスのものを用いる必要がある。

解答解説

コンピュータウィルス対策に関する問題である。

アの感染直後の一般利用者のウィルスの種別の解明は、対象の種類が多く登録されていない新種のウィルスもあり、簡単にはできない作業である。最初の作業としては正しくない。

イの感染媒体の破棄、ワクチンによるウィルスの除去の試みは正しい。ただし、ウィルスが除去できるとは限らないため、その場合には媒体の破棄になる。求める答えはイとなる。

ウの最新バージョンのワクチンを使用しても、ウィルスの感染を完全に除去することは困難である。

エのバックアップファイルへのウィルス感染の防止は、バックアップファイルに感染データやプログラムなどを書き込まなければよいから、ライトプロテクトで十分である。

例題演習

電子メール送信時に送信者に対して宛先アドレスの確認を求めるのが有効であるセキュリティ対策はどれか。

ア　ＯＰ２５Ｂによるスパム対策

イ　ＳＰＦによるスパム対策

ウ　電子メールの誤送信対策

エ　電子メールの不正中継対策

解答解説

電子メールの宛先アドレス確認に関する問題である。

アのＯＰ２５Ｂは、ネットワークの境界にあるルータなどの機器で、ネットワーク内から外部のコンピュータのＴＣＰポート25番への通信を禁止することである。これによって、電子メールが送信不能になる。

イのＳＰＦは、メールの送信元アドレスの偽装を防止する技術である。ドメインと無関係なメールサーバを利用して送信元を偽ったメールを送信しようとすると、受信側でそのことを検出して自動的に受け取りを拒否することができる。

ウの誤送信対策としては、電子メールの送信者が送信時に、宛先アドレスの確認を行うことは有効である。求める答えはウとなる。

エの不正中継は、メールサーバを運用しているサイトで受取先のサーバとは全く関係のないメールが第三者によって送り付けられ、これを受取ったサーバが本来必要のないメール配送処理をさせられてしまう現象である。 送信者に宛先アドレスの確認を求めても意味がない。

例題演習

コンピュータウィルスに関する記述のうち、適切なものはどれか。

ア　ウィルスの潜伏しているプログラムファイルがコンピュータ内に存在している場合であっても、コンピュータ利用者が意図的にファイルを起動しない限り感染しない。

イ　ウィルスは、主記憶装置を物理的に破壊したり、コンピュータ利用者の意図しない動作を引き起こしたりする。

ウ　ウィルスを検出・駆除するためのエンジンや定義ファイルなどが、最新のものに更新されているコンピュータでは感染しない。

エ　駆除作業では、ウィルスに感染していないＯＳ起動ディスクを使用することによって、ブートセクタからの感染を回避することができる。

解答解説

コンピュータウィルスに関する問題である。

ウィルスにはシステム感染型とファイル感染型がある。システム感染型はフロッピーディスクを介してハードディスクのブートセクタに感染し、システムを起動するたびにメモリに読み込まれてしまうタイプである。ファイル感染型はプログラムファイルに感染し、感染プログラムを起動するとメモリに読み込まれるタイプである。

アのファイルの起動と感染の関係では、一定の潜伏期間を経過すると発病するものもあり、ファイルが起動されなければ感染しないとは言えない。

イのウィルスは主記憶を物理的に破壊することはない。物理的に破壊するは誤りである。

ウの新しいワクチンでも有効でないウィルスが存在する。

エの感染していないＯＳの起動ディスクを使用すると、ブートセクタからの感染は防止することができる。求める答えはエとなる。

例題演習

“コンピュータウイルス対策基準”において，コンピュータウイルスは三つの機能のうち少なくとも一つを有するものと定義されている。この機能の組合せとして，正しいものはどれか。

ア　自己伝染機能，潜伏機能，増殖機能
イ　自己伝染機能，潜伏機能，発病機能
ウ　自己伝染機能，増殖機能，マクロ機能
エ　自己伝染機能，発病機能，マクロ機能

解答解説

コンピュータウィルス対策基準の３つの機能の組み合わせに関する問題である。

コンピュータウィルスの３つの機能は次の内容である。

① 自己伝染機能：自らの機能によって他のプログラムに自らのプログラムをコピーし、またはシステム機能を利用して自らのプログラムを他のシステムにコピーすることにより、他のシステムに伝染する機能。

② 潜伏機能：発病するための特定時刻や一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能。

③ 発病機能：プログラムやデータ等のファイルの破壊を行ったり、設計者の意図しない動作をするなどの機能。

コンピュータウィルス対策基準で定義されている３機能は、自己伝染機能、潜伏機能、発病機能であり、求める答えはイである。

例題演習

不正プログラムのワームに関する記述として、適切なものはどれか。

ア　アプリケーションソフト専用のマクロ言語で記述されている。
イ　ある指定の期日や条件を満たしたときに機能が働き、データファイルなどを破壊する。
ウ　ネットワーク経由でコンピュータ間を自己複製しながら移動する。
エ　他のプログラムに感染し、ネットワークを利用せずに単独で増殖する。

解答解説

ワームに関する問題である。

ワームはコンピュータウィルスの一種で、ネットワークを感染経路にして自己増殖し、システムに害を与える悪質なコンピュータプログラムである。ワーム自体は破壊を行わないが、増殖を繰り返していくことでコンピュータのＣＰＵの処理やディスクの容量などを占有し、システムに負荷をかけたり、停止させたりする。

ウのネットワーク経由でコンピュータ間を自己複製しながら移動するが適切な記述である。求める答えはウとなる。

アはマクロウィルス、イは時限爆弾や論理爆弾、エは狭義のウィルスであり、ファイル感染型やカーネル感染型が相当する。

例題演習

コンピュータウィルス対策で用いられるウイルス定義ファイルに関する記述のうち，適切なものはどれか。

ア　ウイルス対策ソフトに含まれているファイルであり，ウイルスに感染したファイルを修復するために使用する。
イ　既知ウイルスのシグネチャコードを記録したファイルであり，ウイルス対策ソフトがウイルス検出時に使用する。
ウ　既知ウイルスのプログラムコードを記録したファイルであり，ウイルスを再現し，動作を監視するために使用する。
エ　復旧のためのファイルであり，ウイルスによってデータファイルが破壊されたときに使用する。

解答解説

ウィルス定義ファイルに関する問題である。

ウィルス定義ファイルは、コンピュータウイルスに感染したファイルや、ネットワーク上で自己複製を繰り返すワームプログラムの特徴を収録したファイルで、ワクチンソフトがコンピュータウイルスやワームを検出するのに使う。「パターンファイル」などとも呼ばれる。ワクチンソフトはウイルス定義ファイル内に収録された各ウイルスのパターンと検査対象のファイルを照合し、パターンとの一致が見られるとそのファイルがウイルスに感染していると判断する。次々と現れる新種のウイルスに対応するため、各ワクチンソフトメーカーは頻繁に自社ソフト向けの新しいウイルス定義ファイルをインターネットなどで配布している。

アの修復するためのファイルではなく、検出するためのファイルである。

イの記述内容が適切である。求める答えはイとなる。

ウのウィルスを再現し、動作を監視するために使用するは誤りである。

エの復旧のためのファイルは誤りである。

例題演習

コンピュータウイルス対策に関する記述のうち，適切なものはどれか。

ア　ウイルスに感染したディスクは論理フォーマッティングを行い，感染ファイルごとにウイルスを消去すべきである。
イ　書換え可能媒体からソフトウエアをインストールするときには，書込み禁止処置をせずにインストールすべきである。
ウ　ソフトウェアをインストールするときには，コンピュータ自体がウイルスに感染していないことを確認してからインストールすべきである。
エ　マルチユーザシステムでもウイルス対策は個人の問題なので,責任者を置かなくてもよい。

解答解説

コンピュータウィルス対策に関する問題である。

コンピュータウイルスは感染する場所によって大別できる。プログラムファイルに感染するものをプログラムファイル感染型、ハードディスクの起動を管理する部分に感染するものをブートセクター感染型、アプリケーションが持つマクロ機能を悪用しデータファイルに感染するものをマクロ感染型と呼ぶ。プログラムファイルとブートセクターのどちらにも感染する複合感染型もある。特に最近は電子メールの普及でデータファイルをやり取りする機会が増え、マクロ感染型による被害が急増している。ウイルスの感染経路は電子メールを使ったファイルのやり取りが大半を占める。添付ファイルを開くことによって感染し、さらに感染したパソコンのアドレス帳を読み出して、勝手にウイルスに感染したファイルを電子メールで送るものも多い。インターネットなどからダウンロードしたプログラムやフロッピーディスクなどのリムーバブルメディアの受け渡しの場合もある。感染予防としては、ウイルスの発見や駆除を行うウイルス対策ソフトが不可欠である。また、ダウンロードしたファイルや電子メールの添付ファイルは開く前にこまめにチェックする、外部から持ち込んだハードディスクなどは初期化してから使う、不特定多数の人とのハードウエアやフロッピーディスクの共用を避けるといった注意も必要である。

アの論理フォーマットではウィルスを消去することが出来ない。

イは書き込み禁止処理を行ってからインストールする方が好ましい取扱である。

ウのソフトウェアをインストールする場合はコンピュータ自身がウィルスに感染していないかどうかを確認してから実行する記述は適切な内容である。求める答えはウとなる。

エのウィルス対策は管理責任者を設置して講じるべきである。

例題演習

ウイルスの調査手法に関する記述のうち，適切なものはどれか。

ア　逆アセンブルは,バイナリコードの新種ウイルスの動作を解明するのに有効な手法である。

イ　パターンマッチングでウイルスを検知する方式は，暗号化された文書中のマクロウイルスの動作を解明するのに有効な手法である。

ウ　ファイルのハッシュ値を基にウイルスを検知する方式は，未知のウイルスがどのウイルスの亜種かを特定するのに確実な手法である。

エ　不正な動作からウイルスを検知する方式は,ウイルス名を特定するのに確実な手法である。

解答解説

ウィルスの調査法に関する問題である。

アのバイナリファイルを逆アセンブルしてアセンブラ言語のプログラムにすることはウイルスの動作を解明に有効である。求める答えはアとなる。

イのパターンマッチングは既知のウイルスやその亜種の検出に効な手法である。

ウのファイルのハッシュ値を確認することでウイルスに感染しているかどうかを確認することができる。

エの不正な動作からウイルスを検知する方式は、振る舞いから未知のウイルスを検出することが可能である。ビヘイビア法は検査対象のプログラムを実行してその振る舞いを監視するウイルス検出方法の1つであり、ウイルス対策ソフトの既知のウイルスパターンに存在しない未

知のウイルスを検出するために用いられる。

例題演習

プログラムの一部をひそかに入れ替えて、本来の仕様どおりに機能させながら、データの不正コピー、悪用、改ざんなどの不正を意図的に実行させる方法はどれか。

ア　サラミ法　　イ　スーパザップ法
ウ　タッピング　　エ　トロイの木馬

解答解説

コンピュータウィルスに関する問題である。

アのサラミ法は、多数の資源からわずかの資産をさく取するウィルスの１種である。預金システムの利息の端数処理プログラムを操作して、切り捨て額を犯人の口座に振り込ませる犯罪に用いる。

イのスーパザップ法は、緊急事態に対処するためにシステムが備えている、あらゆる資源を回避してプログラムやファイルにアクセスして変更できるようにする機能を悪用する。

ウのタッピングは、ネットワーク上の電文を不正に盗み取る行為である。

エのトロイの木馬は、プログラムコードの中に本来の処理に影響を与えないように未承認コードを隠しておき、不正行為を実行させる仕組みのウィルスの１種である。求める答えはエとなる。

例題演習

コンピュータウィルスを発見したときの適切な対処はどれか。

ア　ウイルス感染時の動作特性からウイルス名を特定するために，動作の再現性を確認する。
イ　短時間のうちに広範囲に感染するワームが発見されても，オンライン業務システムとして稼働中の場合は，そのままの状態でウイルス対策を進める。
ウ　ネットワークを経由してほかのコンピュータに感染する可能性があるので，まず感染したコンピュータをネットワークから切り離す。
エ　メモリ上にウイルスプログラムが展開されている可能性があるので，まずコンピュータの電源を切る。

解答解説

コンピュータウィルス対策に関する問題である。

ウィルス対策の８箇条

①　最新のワクチンソフトを活用すること
②　ウィルス対策に備えてデータのバックアップを行うこと
③　ウィルス感染の可能性が考えられる場合、ウィルス検査を行うこと
④　コンピュータウィルスを発見した場合、感染したコンピュータをネットワークから直ちに切り離す。

⑤　メールの添付ファイルはウィルス検査後開くこと
⑥　ウィルス感染の可能性のあるファイルを扱うときは、マクロ機能の実行は行わないこと
⑦　外部から持ち込まれたフロッピーディスクおよびダウンロードしたファイルはウィルス検査後使用すること
⑧　コンピュータの共同利用時の管理を徹底すること

アの処理は、感染したコンピュータをネットワークから切り離し後、行う。

イのオンライン状態のままでは、他のコンピュータに感染する危険性がある。

ウのネットワークからの切り離しは直ちに行う処置であり、適切である。求める答えはウとなる。

エのコンピュータの電源を切っても、ウィルスの除去にはならない。

例題演習

データの破壊，改ざんなどの不正な機能をプログラムの一部に組み込んだものを送ってインストールさせ，実行させるものはどれか。

ア　ＤｏＳ攻撃　　イ　辞書攻撃
ウ　トロイの木馬　　エ　バッファオーバフロー攻撃

解答解説

コンピュータウィルスに関する問題である。

アのＤｏＳ攻撃は、サーバなどのネットワークを構成する機器に対して攻撃を行い、サービスの提供を不能な状態にすることである

イの辞書攻撃は、クラッカーが特定のコンピュータに施されたパスワードを調べたり、スパム送信者が送信先のメールアドレスを決める際に用いる手法である。

ウのトロイの木馬は、プログラムコードの中に本来の処理に影響を与えないように未承認コードを隠しておき、データの破壊、改ざんなどの不正行為を実行させるウィルスである。求める答えはウとなる。

エはバッファー領域をオーバフローさせる攻撃である。

例題演習

ソーシャルエンジエアリングに分類される手ロはどれか。

ア　ウイルス感染で自動作成されたバックドアからシステムに侵入する。
イ　システム管理者などを装い，利用者に問い合わせてパスワードを取得する。
ウ　総当たり攻撃ツールを用いてパスワードを解析する。
エ　バッファオーバフローなどのソフトウエアの脆弱性を利用してシステムに侵入する。

解答解説

ソーシャルエンジニアリングに関する問題である。

ソーシャルエンジニアリングは、ネットワークシステムへの不正侵入を達成するために、必

要なＩＤやパスワードを、物理的手段によって獲得する行為を指す。代表的な例として、侵入した企業・組織の従業員になりすましてパスワードを聞き出したり、盗み聞きしたりする行為が挙げられる。ほかにも廃棄された紙ゴミから企業・組織に関する重要情報を読み取るなどの行為もあり、電話に出た子どもに対して、両親に関する個人情報を聞き出す事例などがある。

システム管理者などを装い、利用者に問い合わせてパスワードを取得する行為はソーシャルエンジニアリングである。求める答えはイとなる。

アはバックドア、イはソーシャルエンジニアリング、ウはフルートフォース攻撃、エはセキュリティフォールである。

例題演習

手順に示すセキュリティ攻撃はどれか。

〔手順〕

（1） 攻撃者が金融機関の偽のＷｅｂサイトを用意する。

（2） 金融機関の社員を装って，偽のＷｅｂサイトへ誘導するＵＲＬを本文中に含めた電子メールを送信する。

（3） 電子メールの受信者が，その電子メールを信用して本文中のＵＲＬをクリックすると，偽のＷｅｂサイトに誘導される。

（4） 偽のＷｅｂサイトと気付かずに認証情報を入力すると，その情報が攻撃者に渡る。

ア　ＤＤｏＳ攻撃　　イ　フィッシング

ウ　ポット　　エ　メールヘッダインジェクション

解答解説

フィッシングに関する問題である。

アのＤＤｏＳ攻撃は、第三者のマシンに攻撃プログラムを仕掛けて踏み台にし、その踏み台とした多数のマシンから標的とするマシンに大量のパケットを同時に送信する攻撃である。

イのフィッシングは、金融機関などからの正規のメールやWebサイトを装い、暗証番号やクレジットカード番号などを搾取する詐欺の一種である。求める答えはイとなる。

ウのポットは、ハニーポットといい、ハッカーやクラッカーに対して、あたかも“本物のシステム”であるかのように見せかけるおとりのような仕組みである。

エのメールヘッダインジェクションは､問い合わせフォームなどのメールを送信する画面で、メールの内容を改ざんし、迷惑メールの送信などに悪用する脆弱性である。

例題演習

コンピュータシステムを利用する上でウィルスという新しい災害が出現し、これに対する予防や検知、事後対策等が講じられている。対策に利用されているものは次のうちのどれか。

ア　クリッパー　　イ　カスケード

ウ　ミケランジェロ　　エ　ワクチン

解答解説

ウィルスの予防対策に用いられるワクチンに関する問題である。

アのクリッパーは記憶容量を食いつぶすウィルスである。

イのカスケードは画面の表示文字を下方に落とすウィルスである。

ウのミケランジェロはミケランジェロの誕生日に初期化するウィルスである。

エのワクチンはウィルスの検出・駆除対策に利用される。求める答えはエとなる。

例題演習

フィッシングの手口に該当するものはどれか。

ア　Ｗｅｂページに入力した内容をそのまま表示する部分がある場合，ページ内に悪意のスクリプトを埋め込み，ユーザとサーバに被害を与える。

イ　ウイルスに感染したコンピュータを，インターネットなどのネットワークを通じて外部から操る。

ウ　コンピュータ利用者のＩＰアドレスやＷｅｂの閲覧履歴などの個人情報を，ひそかに収集して外部へ送信する。

エ　電子メールを発信して受信者を誘導し，実在する会社などを装った偽のＷｅｂサイトにアクセスさせ，個人情報をだまし取る。

解答解説

フィッシングに関する問題である。

フィッシングは、金融機関などからの正規のメールやWebサイトを装い、暗証番号やクレジットカード番号などを搾取する詐欺の一種である。

アはクロスサイトスクリプティング、イはマルウェア、ウはスパイウェア、エはフィッシングである。求める答えはエとなる。

例題演習

コンピュータ犯罪の代表的な手口に関する記述のうち,適切なものはどれか。

ア　サラミ法とは、多数の資産から、全体への影響が無視できる程度にわずかずつ詐取する方法である。

イ　スキャビンジング(ごみ箱あさり)とは、電話機や端末を使用してコンピュータネットワークからデータを盗用する方法である。

ウ　盗聴とは、音声の伝送を行っている電話回線への不正アクセスに用いられる犯罪手口のことであり、コンピュータデータを対象としない。

エ　トロイの木馬とは、プログラム実行後のコンピュータ内部、又はその周囲に残っている情報をひそかに入手する方法である。

解答解説

コンピュータ犯罪の手口に関する問題である。

アのサラミ法は、コンピュータ犯罪の手口の一つで、開発担当のプログラマが、利子の金額を計算する際に切り捨てられる端数(日本なら1円未満の金額)を特定の休眠口座に集めるようにプログラムを細工しておき、ある程度金額がまとまった時点で自分の口座に移し換えて詐取する方法である。サラミを少しずつ切り取る様子に例えて、この名前が付けられた。

イのスキャピンジングは、プログラム実行後のコンピュータ内部に残っている情報やデータを密かに入手して悪用する手段である。

ウの盗聴は、ネットワークを介して送受信しているデータを不正に傍受することで、クレジット・カード番号や銀行口座番号など金銭に関係する情報、コンピュータ・システムへのログインに必要なIDとパスワードなどの情報が盗聴の対象となることが多い。

エのトロイの木馬は、プログラムコードの中に本来の処理に影響を与えないように未承認コードを隠しておき、データの破壊、改ざんなどの不正行為を実行させるウィルスで、ファイルを削除してしまう機能を持ったプログラムを作る。利用者がプログラムを起動すると、ファイルが勝手に削除されてしまう。

アはサラミ法、イは盗聴、ウはトロイの木馬、エはスキャビンジングの内容を示している。求める答えはアとなる。

例題演習

コンピュータ犯罪の手口の一つであるサラミ法はどれか。

ア　回線の一部に秘密にアクセスして他人のパスワードやＩＤを盗み出してデータを盗用する方法である。
イ　ネットワークを介して送受信されている音声やデータを不正に傍受する方法である。
ウ　不正行為が表面化しない程度に，多数の資産から少しずつ詐取する方法である。
エ　プログラム実行後のコンピュータ内部又はその周囲に残っている情報をひそかに探索して，必要情報を入手する方法である。

解答解説

サラミ法に関する問題である。

サラミ法は、多数の資源からわずかずつ資産を搾取する方法である。預金システムの利息の端数処理プログラムを操作して、切り捨て額を犯人の口座に振り込ませる。プログラムの操作にはトロイの木馬を応用する。

アはなりすまし、イは盗聴、ウはサラミ法、エはスカビンジングである。求める答えはウとなる。

例題演習

コンピュータやネットワークのセキュリティ上の脆弱性を発見するために，システムを実際に攻撃して侵入を試みる手法はどれか。

ア　ウォークスルー　　イ　ソフトウェアインスペクション
ウ　ペネトレーションテスト　　エ　リグレッションテスト

解答解説

ペネスレーションテストに関する問題である。

ペネスレーションテストは、ネットワーク接続された情報システムが外部からの攻撃に対して安全かどうか、実際に攻撃手法を試しながら安全性の検証を行う。不正に侵入できるかどうかだけでなく、ＤｏＳ攻撃にどれくらい耐えられるかを調べたり、侵入された際にそこを踏み台にして他のネットワークを攻撃できるかどうかなどを調べる場合もある。

アのウォークスルー、イのソフトウェアインスペクションはシステム開発でのデザインレビューの方法の一つである。

ウのペネストレーションテストは、コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つで、システムを実際に攻撃して侵入を試みる手法である。求める答えはウとなる。

エのリグレッションテストは、情報システムの一部に修正を加えたときに、修正部分が他に悪影響を与えてないかどうかを確認するテストである。

例題演習

ＳＱＬインジェクションの説明はどれか。

ア　Ｗｅｂアプリケーションに問題があるとき，データベースに悪意のある問合せや操作を行う命令文を入力して，データベースのデータを改ざんしたり不正に取得したりする攻撃

イ　悪意のあるスクリプトを埋め込んだＷｅｂページを訪問者に閲覧させて，別のＷｅｂサイトで，その訪問者が意図しない操作を行わせる攻撃

ウ　市販されているＤＢＭＳの脆弱性を利用することによって，宿主となるデータベースサーバを探して自己伝染を繰り返し，インターネットのトラフィックを急増させる攻撃

エ　訪問者の入力データをそのまま画面に表示するＷｅｂサイトに対して，悪意のあるスクリプトを埋め込んだ入力データを送ることによって，訪問者のブラウザで実行させる攻撃

解答解説

ＳＱＬインジェクションに関する問題である。

ＳＱＬインジェクションは、Ｗｅｂサイトで、データベースへの問い合わせや操作を行うプログラムにパラメータとしてＳＱＬ文の断片を与えることにより、データベースを改ざんしたり不正に情報を入手する攻撃である。

Ｗｅｂアプリケーションではデータベースの操作にＳＱＬ言語を利用している。ユーザがフォームから送信した検索語などのパラメータを受け取り、これをＳＱＬ文に埋め込んでデータベースへの問い合わせや操作を行う。このとき、ＳＱＬ文として解釈できる文字列をパラメータに含めることで、プログラムが想定していないＳＱＬ文を合成し、不正にデータベースの内容を削除したり、本来アクセスできない情報を表示させたりすることができてしまう場合がある。

アはＳＱＬインジェクション、イはクロスサイトリクエストフォージェリ、ウはワームの一種のＳＱＬ Slammer、エはクロスサイトスクリプティングである。求める答えはアとなる。

例題演習

ＳＱＬインジェクション攻撃を防ぐ方法はどれか。

ア　入力中の文字がデータベースへの問合せや操作において，特別な意味をもつ文字として解釈されないようにする。
イ　入力にＨＴＭＬタグが含まれていたら，ＨＴＭＬタグとして解釈されない他の文字列に置き換える。
ウ　入力に，上位ディレクトリを指定する文字列(‥／)を含むときは受け付けない。
エ　入力の全体の長さが制限を超えているときは受け付けない。

解答解説

ＳＱＬインジェクション攻撃に関する問題である。

ＳＱＬインジェクションは、Ｗｅｂサイトで、データベースへの問い合わせや操作を行うプログラムにパラメータとしてＳＱＬ文の断片を与えることにより、データベースを改ざんしたり不正に情報を入手する攻撃である。

Ｗｅｂアプリケーションではデータベースの操作にＳＱＬ言語を利用している。ユーザがフォームから送信した検索語などのパラメータを受け取り、これをＳＱＬ文に埋め込んでデータベースへの問い合わせや操作を行う。この時、ＳＱＬ文として解釈できる文字列をパラメータに含めることで、プログラムが想定していないＳＱＬ文を合成し、不正にデータベースの内容を削除したり､本来アクセスできない情報を表示させたりすることができてしまう場合がある。

開発・導入したＷｅｂアプリケーション、またはデータベース上のストアドプロシージャ等を改修し、意図しないＳＱＬ文を受け入れないようにする必要がある。即ち、入力中の文字がデータベースへの問合せや操作において、特別な意味をもつ文字として解釈されないようにする必要がある。求める答えはアとなる。

例題演習

最近、増加しているマクロウィルスに関する記述として、正しいものはどれか。

ア　感染したアプリケーションを実行すると、マクロウィルスは主記憶にロードされ、その間に実行したほかのアプリケーションのプログラムファイルに感染する。
イ　感染したフロッピーディスクからシステムを起動するとマクロウィルスは主記憶にロードされ、ほかのフロッピーディスクのブートセクタに感染する。
ウ　感染した文書ファイルを開いた後に､別に開いたり新規作成した文書ファイルに感染する。
エ　マクロがウィルスに感染しているかどうかが容易に判断できるので、文書ファイルを開く時点で感染を防止できる。

解答解説

マクロウィルスに関する問題である。

マクロウィルスは表計算やワープロなどのマクロ言語で記述された文書データに潜み、電子メールを介して送信相手に感染するタイプのコンピュータウィルスである。マクロウィルスの

１種であるメリッサは、感染した電子メールを受け取ったユーザが、メールに添付されたワード文書を開き、自動的にマクロが実行されると直ちに感染し、同時に発病する。求める答えはウとなる。

アはファイル感染型、イはブートセクタ感染型であり、マクロウィルスではない。

エの感染が容易に判断できるは誤りであり、文書を開き、マクロを実行した段階で発病するため通常の手段では簡単に把握することができない。

例題演習

コンピュータウィルス対策ソフトのパターンマッチング方式を説明したものはどれか。

ア　感染前のファイルと感染後のファイルを比較し，ファイルに変更が加わったかどうかを調べてウイルスを検出する。
イ　既知ウイルスのシグネチャコードと比較して，ウイルスを検出する。
ウ　システム内でのウイルスに起因する異常現象を監視することによって，ウイルスを検出する。
エ　フアイルのチェックサムと照合して，ウイルスを検出する。

解答解説

コンピュータウィルス対策ソフトに関する問題である。

ウィルス対策ソフトはコンピュータウィルスを発見するために使用されるファイルである。パターンファイルに蓄積されているウィルスの情報を利用してファイルをチェックする。パターンファイルにないウィルスは発見できない可能性が高い。ウィルスに感染しないためにはパターンファイルを常に最新の状態にしておく必要がある。

アの感染前後のファイルを比較しても変化は分かるがウィルスに感染したかどうかを判断することはできない。パターンファイルとの比較が必要である。

イの既存ウィルスのシグネチャコードと比較するとウィルスを検出できる。求める答はイとなる。

ウのウィルスに起因する異常現象を絶えず監視することができない。新しいウィルスによる異常現象を特定する事ができない。

エのファイルとの照合はパターンファイルと行うのであって、チェックサムと照合してもウィルを検出することはできない。

例題演習

緊急事態を装う不正な手段によって組織内部の人間からパスワードや機密情報を入手する行為は，どれに分類されるか。

ア　ソーシャルエンジニアリング　　イ　トロイの木馬
ウ　パスワードクラック　　エ　踏み台攻撃

解答解説

ソーシャルエンジニアリングに関する問題である。

アのソーシャルエンジニアリングは技術的な手段によらずに巧みな話術やゴミ箱を漁るといった方法で顧客や従業員のパスワードや機密情報などを不正に取得する行為をいう。求める答はアとなる。

イのトロイの木馬はプログラムコードの中に、本来の処理に影響を与えないように未承認のコードを隠しておき、不正行為を実行させる。コンピュータの全ファイルを破壊したり、パスワードを盗み出したりする。

ウのパスワードクラックは他人のパスワードを解析し、探り当てることである。人名や誕生日、意味のある単語をパスワードに使うのは避け、数字や記号を混在させることで、被害に遭う可能性を減らすことができる。

エの踏み台攻撃はセキュリティ対策の甘いサイトに不正侵入し、他サイトの攻撃の中継サイトとして利用することである。

例題演習

ディレクトリトラバーサル攻撃に該当するものはどれか。

ア　攻撃者が，Ｗｅｂアプリケーションの入力データとしてデータベースへの命令文を構成するデータを入力し，管理者の意図していないＳＱＬ文を実行させる。

イ　攻撃者が，パス名を使ってファイルを指定し，管理者の意図していないファイルを不正に閲覧する。

ウ　攻撃者が，利用者をＷｅｂサイトに誘導した上で，ＷｅｂアプリケーションによるＨＴＭＬ出力のエスケープ処理の欠陥を悪用し，利用者のＷｅｂブラウザで悪意のあるスクリプトを実行させる。

エ　セッションＩＤによってセッションが管理されるとき，攻撃者がログイン中の利用者のセッションＩＤを不正に取得し，その利用者になりすましてサーバにアクセスする。

解答解説

ディレクトリトラバーサル攻撃に関する問題である。

ディレクトリトラバーサルは、ネットワーク上の脆弱性を利用した攻撃手法の一種で、「../」を利用してディレクトリを遡り、本来はアクセスが禁止されているディレクトリにアクセスする手法のことである。または、そのような脆弱性のことである。ネットワーク上でディレクトリのパスを指定する際、「一つ上の階層へ上る」ことを指示する「../」のパスを組み合わせて指定することで、公開されているディレクトリの上階層から、その併置されている非公開のディレクトリへアクセスできてしまう場合がある。このような操作によって、個人情報や機密情報を盗まれたり､悪意あるコードを書き込まれたりといった被害を被る危険性が生じる。

アはＳＱＬインジェクション、イはディレクトリトラバーサル攻撃、ウはクロスサイトスクリプティング、エはセションハイジャックである。求める答えはイとなる。

例題演習

ＤＮＳキャッシュポイズニングに分類される攻撃内容はどれか。

ア　ＤＮＳサーバのソフトウェアのバージョン情報を入手して，ＤＮＳサーバのセキュリティホールを特定する。
イ　ＰＣが参照するＤＮＳサーバに誤ったドメイン情報を注入して，偽装されたＷｅｂサーバにＰＣの利用者を誘導する。
ウ　攻撃対象のサービスを妨害するために，攻撃者がＤＮＳサーバを踏み台に利用して再帰的な問合せを大量に行う。
エ　内部情報を入手するために，ＤＮＳサーバが保存するゾーン情報をまとめて転送させる。

解答解説

ＤＮＳキャッシュポイズニング攻撃に関する問題である。

ＤＮＳはドメイン名とＩＰアドレスの対応を検索するサーバであるが、この処理を効率化するためにキャッシュを利用する。過去に行った内容と同じ問い合わせをする場合、他のネームサーバへ問い合わせることなく、キャッシュとして保持している情報を利用してクライアントに返答する。

ＤＮＳキャッシュポイズニング攻撃は、ＤＮＳのこの機能を悪用し、キャッシュサーバに偽のＤＮＳ情報をキャッシュとして蓄積させ、攻撃を受けたキャッシュサーバを利用するユーザーに対して、以下のような影響を与える。

①　ホスト名とＩＰアドレスの対応を変更し有害サイトへ誘導する。
②　Ｗｅｂメールの内容を盗聴する、改ざんする。
③　ｓｐａｍを送信する。
⑤　ＤＮＳを使用不能にして、各種サービスやアプリケーションを動作不能にする。

アはポストスキャン、イはＤＮＳキャッシュポイズニング、ウはＤＮＳリフレクション、エはゾーン転送を悪用した登録情報の収集である。求める答えはイとなる。

例題演習

情報漏えい対策に該当するものはどれか。

ア　送信するデータにチェックサムを付加する。
イ　データが保存されるハードディスクをミラーリングする。
ウ　データのバックアップ媒体のコピーを遠隔地に保管する。
エ　ノート型ＰＣのハードディスクの内容を暗号化する。

解答解説

情報漏洩に関する問題である。

情報漏洩は、内部の機密情報などが外部に漏れてしまうことである。パソコンなどに情報を保存し、情報漏洩対策を怠ると漏洩する恐れがある。漏洩の原因となるのは、スパイウェアなどのインストール、クラッキング、パソコンや記憶媒体などの紛失、電子メールの一斉送信が

ある。

アのチェックサムは誤りの検出機能、イのミラーリングは信頼性向上、ウの遠隔地保管はバックアップ機能、エの暗号化は漏洩対策である。求める答えはエとなる。

例題演習

虚偽のデータや不正プログラム等を入力して、自分の預金口座に振り込み、入金させたり、偽造や変造したりプリペイドカードを使って不正な利益を得る行為に適用される犯罪はどれか。

ア　詐欺罪　　イ　電磁的記録不正作出罪
ウ　電子計算機損壊等業務妨害罪　　エ　電子計算機使用詐欺罪

解答解説

電子計算機使用詐欺罪に関する問題である。

アは通常の詐欺罪である。計算機と関係ない犯罪にも適用される。

イの電磁的記録不正作出罪は人の事務処理を誤らせる目的で、権利、義務、または事実証明に関する電磁的記録を不正に作出した者は処罰されることになっている。

ウの電子計算機損壊等業務妨害罪は、コンピュータの損壊や動作障害などコンピュータ業務を妨害した者は処罰される。

エの電子計算機使用詐欺罪は虚偽のデータや不正のプログラムなどを入力して、自分の預金口座に振り込み入金をさせたり、偽造や変造したプリペイドカードを使って不正な利益を得る行為などを詐欺罪として処罰する。求める答えはエとなる。

例題演習

クライアントＰＣで行うマルウェア対策のうち，適切なものはどれか。

ア　ＰＣにおけるウイルスの定期的な手動検査では，ウイルス対策ソフトの定義ファイルを最新化した日時以降に作成したファイルだけを対象にしてスキャンする。
イ　ウイルスがＰＣの脆弱性を突いて感染しないように，ＯＳ及びアプリケーションの修正パッチを適切に適用する。
ウ　電子メールに添付されたウイルスに感染しないように，使用しないＴＣＰポート宛ての通信を禁止する。
エ　ワームが侵入しないように，クライアントＰＣに動的グローバルＩＰアドレスを付与する。

解答解説

マルウェア対策に関する問題である。

マルウェアは、コンピュータウイルス、ワーム、スパイウェアなどの悪意のこもったソフトウェアのことである。遠隔地のコンピュータに侵入したり攻撃したりするソフトウェアや、コンピュータウイルスのようにコンピュータに侵入して他のコンピュータへの感染活動や破壊活動を行ったり、情報を外部に漏洩させたりする有害なソフトウェアである。

マルウェア対策としては、パターンファイルを最新の状態に保つ、最新のソフトウェアを使用する、自動･リアルタイムスキャンをオンに設定しておく、ウイルス対策ソフトは、全社共通のものを使用するなどが重要である。

ＯＳやブラウザ、メールソフトなどのソフトウェアは、セキュリティホールを修正したり、セキュリティ上の問題を解決したり、ソフトウェアの不具合を解消したりするための修正プログラムが、インターネット経由で各メーカから提供されいる。これらの修正プログラムを定期的に適用して、ソフトウェアを最新の状態に保つ必要がある。

ウィルスがＰＣの脆弱性を突いて感染しないように、ＯＳやアプリケーションの修正パッチを適切に適用する内容が適切である。求める答えはイとなる。

例題演習

ウイルス検出におけるビヘイビア法に分類されるものはどれか。

ア　あらかじめ検査対象に付加された，ウイルスに感染していないことを保証する情報と，検査対象から算出した情報とを比較する。
イ　検査対象と安全な場所に保管してあるその原本とを比較する。
ウ　検査対象のハッジュ値と既知のウイルスファイルのハッジュ値とを比較する。
エ　検査対象をメモリ上の仮想環境下で実行して，その挙動を監視する。

解答解説

ビヘイビア法に関する問題である。

アンチウイルスソフトなどがウイルスの存在を検知する手法の一つで、実行中のプログラムの振る舞いを監視して、不審な処理が行われていないかを調べる方式である。仮想的な実行環境を用意してプログラムを実行し、異常な行動を起こさないか調べる方式と、実際の環境で実行されているプログラムを監視して異常な行動が観測されたら即座に実行を打ち切る方式がある。ウイルス定義ファイルを用いたパターンマッチング法では検知できない新しいウイルスや、ヒューリスティック法での検知が難しいミューテーション型(ポリモーフィック型)などにも対応することができる。

アはチェックサム法、イはコンペア法、ウはハッシュ値比較法、エはビヘイビア法である。求める答えはエとなる。

例題演習

ワームの検知方式の一つとして，検査対象のファイルからSHA-256を使ってハッシュ値を求め，既知のワーム検体ファイルのハッシュ値のデータベースと照合することによって，検知できるものはどれか。

ア　ワーム検体と同一のワーム
イ　ワーム検体と特徴あるコード列が同じワーム
ウ　ワーム検体とファイルサイズが同じワーム
エ　ワーム検体の亜種に当たるワーム

解答解説

ワームの検知方針に関する問題である。

ＳＨＡ-256とは、任意長の原文から固定長の特徴的な値であるハッシュ値を求める計算手順で、最長で２の64乗ビットまでの原文から、256ビットのハッシュ値を算出することができる。2001年に米国家安全保障局（NSA）が開発し、米国立標準技術研究所（NIST）がハッシュ関数の国家標準の一つとして採用した。SHA-224、SHA-256、SHA-384、SHA-512をまとめて「SHA-2」と通称することがある。

ワームの検知方式は、検知対象ファイルからＳＨＡ-256を使用してハッシュ値を求めたものとデータベース化されているワーム検体ファイルのハッシュ値を比較する方法である。従って、検出できるワームはワーム検体と同一のワームとなる。求める答えはアとなる。

例題演習

スパイウェアに該当するものはどれか。

ア　Ｗｅｂサイトへの不正な入力を排除するために，Ｗｅｂサイトの入力フォームの入力データから，ＨＴＭＬタグ，JavaScript，ＳＱＬ文などを検出し，それらを他の文字列に置き換えるプログラム

イ　サーバへの侵入口となり得る脆弱なポートを探すために，攻撃者のＰＣからサーバのＴＣＰポートに順番にアクセスするプログラム

ウ　利用者の意図に反してＰＣにインストールされ，利用者の個人情報やアクセス履歴などの情報を収集するプログラム

エ　利用者のパスワードを調べるために，サーバにアクセスし，辞書に載っている単語を総当たりで試すプログラム

解答解説

スパイウェアに関する問題である。

スパイウェアは、パソコンを使うユーザの行動や個人情報などを収集したり、マイクロプロセッサの空き時間を借用して計算を行ったりするアプリケーションソフトである。得られたデータはマーケティング会社など、スパイウェアの作成元に送られる。

アはサニタイジング、イはポートスキャンツール、ウはスパイウェア、エは辞書攻撃を行うパスワードクラックツールである。求める答えはウとなる。

例題演習

別のサービスやシステムから流出したアカウント認証情報を用いて，アカウント認証情報を使い回している利用者のアカウントを乗っ取る攻撃はどれか。

ア　パスワードリスト攻撃　　イ　ブルートフォース攻撃

ウ　リバースブルートフォース攻撃　　エ　レインボー攻撃

解答解説

パスワードリスト攻撃に関する問題である。

アのパスワードリスト攻撃は、ネットサービスやコンピュータシステムの利用者アカウントの乗っ取りを試みる攻撃手法の一つで、別のサービスやシステムから流出したアカウント情報を用いてログインを試みる手法である。脆弱なサービスやシステムが攻撃者の侵入を受け、利用者のアカウント名とパスワードのリスト一覧の情報が流出すると、その情報を利用して別のシステムへの攻撃を試みるのがパスワードリスト攻撃で、同じアカウント名とパスワードを使っている利用者のアカウントでログインし、利用者になりすまして不正に操作することができてしまう。求める答えはアとなる。

イのブルートフォース攻撃は、暗号やパスワードを解読、解析するための手法のひとつで、特定のユーザＩＤに対して考えられる全ての暗号鍵を自動化されたプログラムによってひたすら入力し、復号化プログラムによって、暗号が意味のある文字列になるかどうかを試行錯誤しながら調べて行く方法である。

ウのリバースブルートフォース攻撃は、不正ログインを目的とするアカウント突破手法で、特定のパスワードに対して、ユーザーＩＤに使用され得る文字列の組み合わせを用いて総当り的にログインを試みる手法のことである。

エのレインボー攻撃は､想定されうるパスワードとそのハッシュ値との対のリストを用いて、入手したハッシュ値からパスワードを効率的に解析する手法である。

例題演習

攻撃者が用意したサーバXのＩＰアドレスが，Ａ社ＷｅｂサーバのＦＱＤＮに対応するＩＰアドレスとして，Ｂ社ＤＮＳキャッシュサーバに記憶された。この攻撃によって，意図せずサーバXに誘導されてしまう利用者はどれか。ここで，Ａ社，Ｂ社の各従業員は自社のＤＮＳキャッシュサーバを利用して名前解決を行う。

ア　Ａ社ＷｅｂサーバにアクセスしようとするＡ社従業員
イ　Ａ社ＷｅｂサーバにアクセスしようとするＢ社従業員
ウ　Ｂ社ＷｅｂサーバにアクセスしようとするＡ社従業員
エ　Ｂ社ＷｅｂサーバにアクセスしようとするＢ社従業員

解答解説

ＤＮＳキャッシュポイズニングに関する問題である。

ＤＮＳキャッシュポイズニングは、ＤＮＳがＷｅｂへのアクセスやメールの送受信などの際に、接続相手のＩＰアドレスを調べたりする仕組みに対して、ＤＮＳが偽の応答を返すようにしてしまう攻撃手法である。インターネットの利用者が、この攻撃により偽の応答をするようにされたＤＮＳを介してＷｅｂにアクセスすると、気づかないうちにフィッシングサイトに誘導されてしまう。

ＤＮＳキャッシュサーバは、利用者からの任意のドメイン名の名前解決の問い合わせを受け付け、当該ドメイン名を管理するＤＮＳサーバへの問い合わせを代理で行い、結果を利用者に返答するコンピュータやソフトウェアである。この問題の仕組みではＡ、Ｂ各社の従業員は自

社のＤＮＳキャッシュサーバを利用して名前解決を行う。

攻撃者はＡ社のＷｅｂサーバのドメイン名に対応するＩＰアドレスをＢ社のＤＮＳキャッシュサーバに記憶させたので、Ｂ社のＤＮＳキャッシュサーバにアクセスし、Ａ社のＩＰアドレスを得ようとする従業員が偽アドレスに誘導されることになる。Ｂ社のＤＮＳキャッシュサーバにアクセスするのはＢ社の従業員である。従って、Ａ社ＷｅｂサーバにアクセスしようとするＢ社の従業がサーバＸに誘導される。求める答えはイとなる。

例題演習

共通鍵暗号の鍵を見つけ出そうとする，ブルートフォース攻撃に該当するものはどれか。

ア　一組みの平文と暗号文が与えられたとき,全ての鍵候補を一つずつ試して鍵を見つけ出す。
イ　平文と暗号文と鍵の関係を表す代数式を手掛かりにして鍵を見つけ出す。
ウ　平文の一部分の情報と，暗号文の一部分の情報との間の統計的相関を手掛かりにして鍵を見　つけ出す。
エ　平文を一定量変化させたときの暗号文の変化から鍵を見つけ出す。

解答解説

ブルートフォース攻撃に関する問題である。

ブルートフォース攻撃は、暗号解読手法の一つで、考えられる全ての鍵をリストアップし、片っ端から解読を試みる方式である。暗号文の一部を復号プログラムにしたがって変換し、意味のある文章になるか調べる。どのような形態の暗号に対しても攻撃できるが、鍵の長さが増えると考えられる鍵のパターンの数は幾何級数的に増大するため､効率の悪い攻撃手法である。

アはブルートフォース攻撃、イは線形解読法、ウは関連鍵攻撃、エは差分解読法である。求める答えはアとなる。

例題演習

ポットネットにおいてＣ＆Ｃサーバが果たす役割はどれか。

ア　遠隔操作が可能なマルウェアに，情報収集及び攻撃活動を指示する。
イ　電子商取引事業者などに，偽のディジタル証明書の発行を命令する。
ウ　不正なＷｅｂコンテンツのテキスト，画像及びレイアウト情報を一元的に管理する。
エ　踏み台となる複数のサーバからの通信を制御し遮断する。

解答解説

ボットネットに関する問題である。

ボットネットは、パソコンやスマートフォンを第三者の指示通りに動くロボットにしてしまう悪意のあるプログラムであり、そのボットをいくつも集めてネットワーク化したものがボットネットである。Ｃ＆Ｃサーバーは、マルウェアに感染したボットネットに指令を送り、制御の中心となるサーバーである。

Ｃ＆Ｃサーバの役割は、ボットネットの遠隔操作が可能なマルウェアに情報収集及び攻撃活

動を指示するであり、求める答えはアとなる。

例題演習

マルウェアについて，トロイの木馬とワームを比較したとき，ワームの特徴はどれか。

ア　勝手にファイルを暗号化して正常に読めなくする。
イ　単独のプログラムとして不正な動作を行う。
ウ　特定の条件になるまで活動をせずに待機する。
エ　ネットワークやリムーバブルメディアを媒介として自ら感染を広げる。

解答解説

ワームとトロイの木馬に関する問題である。

ワームはコンピュータウィルスの一種で、ネットワークやＵＳＢメモリなどを感染経路にして自己増殖し、システムに害を与える悪質なプログラムである。ワーム自体は破壊を行わないが、増殖を繰り返していくことでＣＰＵの処理やディスクの容量などを占有し、システムに負荷をかけたり、停止させたりする。トロイの木馬はプログラムコードの中に本来の処理に影響を与えないように未承認コードを隠しておき、データの破壊、改ざんなどの不正行為を実行させるウィルスで、ファイルを削除してしまう機能を持ったプログラムを作る。利用者がプログラムを起動すると、ファイルが勝手に削除されてしまう。

アはランサムウェアの特徴、イはマルウェアの特徴、ウはトロイの木馬の特徴、エはワームの特徴である。求める答えはエとなる。

例題演習

ドライブバイダウンロード攻撃に該当するものはどれか。

ア　ＰＣ内のマルウェアを遠隔操作して，ＰＣのハードディスクドライブを丸ごと暗号化する。
イ　外部ネットワークからファイアウォールの設定の誤りを突いて侵入し，内部ネットワークにあるサーバのシステムドライブにルートキットを仕掛ける。
ウ　公開Ｗｅｂサイトにおいて，スクリプトをＷｅｂページ中の入力フィールドに入力し，Ｗｅｂサーバがアクセスするデータベース内のデータを不正にダウンロードする。
エ　利用者が公開Ｗｅｂサイトを閲覧したときに，その利用者の意図にかかわらず，ＰＣにマルウェアをダウンロードさせて感染させる。

解答解説

ドライブバイダウンロード攻撃に関する問題である。

ドライブバイダウンロード攻撃は、Ｗｅｂブラウザを通じてユーザーに気づかせないようにソフトウェア部品をダウンロードさせることで、スパイウェアやマルウェア、コンピュータウィルスなどが侵入・攻撃を行う場合の経路として用いられる。ユーザーがＷｅｂサイトを閲覧しただけで自動的にスパイウェアやマルウェアがダウンロードされてしまったり、ダウンロードが実行されてもユーザーは気づくことができなかったりというに特徴がある。また、企業の

Ｗｅｂサイトが改ざんされ、ドライブバイダウンロードが埋め込まれてユーザーを脅かした例もある。ドライブバイダウンロードによる攻撃は主にＷｅｂブラウザやＯＳの脆弱性を突くようにして行われる。そのため、ドライブバイダウンロードによる攻撃を回避するためには、ウィルス対策ソフトやファイアーウォールの導入などを並んで、ＷｅｂブラウザやＯＳのセキュリティパッチを更新して常に最新の状態に保つといった事柄が主要な施策となる。

アはランサムウェア、イはルートキット攻撃、ウはＳＱＬインジェクション、エはドライブバイダウンロードである。求める答えはエとなる。

例題演習

ＳＰＦ(Sender Policy Framework)の仕組みはどれか。

ア　電子メールを受信するサーバが，電子メールに付与されているディジタル署名を使って，送信元ドメインの詐称がないことを確認する。

イ　電子メールを受信するサーバが，電子メールの送信元のドメイン情報と，電子メールを送信したサーバのＩＰアドレスから，ドメインの詐称がないことを確認する。

ウ　電子メールを送信するサーバが，送信する電子メールの送信者の上司からの承認が得られるまで，一時的に電子メールの送信を保留する。

エ　電子メールを送信するサーバが，電子メールの宛先のドメインや送信者のメールアドレスを問わず，全ての電子メールをアーカイブする。

解答解説

ＳＰＦの仕組みに関する問題である。

ＳＰＦは電子メールの送信元ドメインが詐称されていないかを検査するための仕組みである。メール送信に使用されるＳＭＴＰは差出人のメールアドレスを自由に設定することが可能で、「なりすましメール」を簡単に送ることができる。ＳＰＦはこうしたメールアドレスにおけるなりすましを防ぐための技術の一つで、ＤＮＳを利用する。ドメインをＳＰＦに対応させるために、そのドメインのゾーンデータにＳＰＦレコードという情報を追加し、ＳＰＦレコードにそのドメイン名を送信元としてメールを送ってもよいサーバのＩＰアドレス等を記述する。一方、ＳＰＦに対応したメール受信サーバは、メールの受信時にそのメールの送信元となっているドメインのＳＰＦレコードをＤＮＳで問い合わせる。送信元のサーバがＳＰＦレコード中で許可されていない場合は送信ドメインの詐称が行われたと判断して、受信を拒否するなどの処理を行う。ＳＰＦは送信元サーバのＩＰアドレスとＤＮＳを利用して、あらかじめ想定された送信元以外からのなりすましメールを検出できるようにする機構である。

アのディジタル証明書を利用したものではない。

イの送信元のドメイン情報と送信したサーバのＩＰアドレスを利用して確認する仕組みはＳＰＦである。求める答えはイとなる。

ウの送信者の上司の承認による確認ではない。

エのＳＰＦはすべての電子メールをアーカイブすることではない。

txt03042　セキュリティ技術と管理

txt030421　暗号化技術とアクセス制御

①　暗号化

ⓐ　暗号化とは

暗号化は文章に対して変換を施し、第三者には何が書かれているか分からない状態にすることである。変換する前の文を平文(ひらぶん)、変換された状態の文書を暗号文という。暗号にはコードとサイファーがある。

コードはあるまとまりのある語や句を他のもので置き換えることである。当事者同士が理解でき、第三者に理解できないものならば何でもよい。サイファーは通信文の文字を１対１に置き換えるものである。暗号というとサイファーだけを指す場合が多い。

ⓑ　古代の暗号化

暗号は古来より主に軍事目的に利用されており、基本的なアイデアは、古代ギリシャ・ローマ時代からすでに存在していた。ギリシャ時代にはスキュタレーと呼ばれる指揮棒に文書を巻き付けて、文章内の文字の位置を置き換える方式の暗号化が用いられた。

シーザ暗号は文字を何文字かずらしたものに置き換える方式である。ＡをＣ、ＢをＤに置き換えることで、ＡＢＣをＣＤＥと表す。文書内の文字の位置を置き換える置換や他の文字との置き換えである換字というアルゴリズムは現代においても暗号を構成する基本要素になっている。

これらの暗号はアルゴリズムおよび暗号化・復号の鍵は、共に秘密にしておく必要があった。

ⓒ　20世紀の暗号化

1977年にアメリカ合衆国商務省標準局によって、商業用の標準暗号ＤＥＳが制定された。このとき、暗号アルゴリズムが仕様として公開され、暗号アルゴリズムは必ずしも秘匿されるものではなくなった。アルゴリズムが公開されていても、解読不可能な強度を持つことが暗号アルゴリズムに対して要求されるようになった。鍵を秘密にしておく暗号化方式を、秘密鍵暗号、または共通鍵暗号と呼ぶ。

1976年に公開鍵暗号の概念が発表された。暗号アルゴリズム、鍵の一部を公開しても解読は不可能という画期的な概念である。この方式を公開鍵暗号方式という。1978年に大きな数の素因数分解の困難性に基づいたＲＳＡ方式が発表され、1982年に離散対数問題の困難性に基づいたＥＬＧamal暗号が考案され、1985年に楕円曲線上の離散対数問題の困難性に基づいた楕円曲線暗号が考案されている。公開鍵暗号方式の出現によって、古典暗号では第三者に対する情報の秘匿に限られていた暗号の利用目的は、相手認証、メッセージ認証という認証機能を持ち合わせるようになり、大きく広がった。

② インターネットの脅威

ⓐ 盗聴

盗聴は、通信内容を第三者に知られたり、盗まれたりしてしまうことである。通信内容が第三者に漏れてしまう危険性があると、社外秘の文書やプライベートな情報などを安心して通信できなくなる。

ⓑ 改ざん

改ざんは、通信内容を書き換えられてしまうことである。送信者から受信者に送ったデータを第三者が途中で横取りし、内容を一部変更して受信者に向けて送り出すことである。契約書をやり取りする途中で契約金額を書き換えられるようなことが起こるネットワークでは、安心してビジネスに利用できなくなる。

ⓒ なりすまし

なりすましは、通信の相手に正体を偽ることである。対面して話を行うときには相手が本人であることを確認できるが、ネットワークでは不可能である。通信相手が本人であることを確認できなければ、インターネットをビジネスに使用できなくなる。

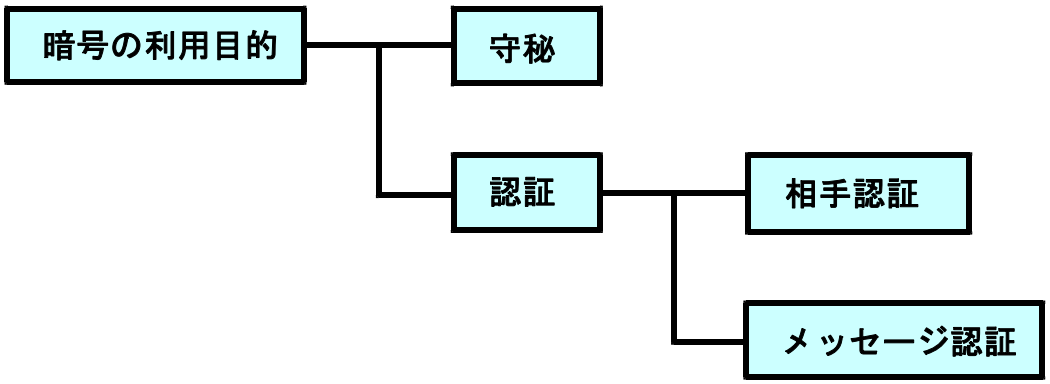
ⓓ 否認

否認は、通信した事実やその内容を否定することである。イクターネットを通じて契約した事実や契約した内容がその後に否定されたり、修正されると、インターネットを使用して契約行為をすることができなくなる。

③ 暗号化の利用目的

ⓐ 暗号化の目的

守秘、認証、アクセス管理の３つの目的がある。



ⓑ　守秘

二者間での情報秘密の共有、第三者に対する情報秘匿、第三者の傍受・盗聴に対する安全性確保をはかるものである。

ⓒ　認証

㋐　相手認証

相手認証は本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。単純な方式ではパスワードを使用する。第三者のなりすましに対する対策である。

㋑　メッセージ認証

メッセージ認証はデータの完全性と否認防止がある。データの完全性は通信途上で内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は送ったことを否定できないことの保証であり、受信側は受け取ったことを否定できないことの保証である。「言った／言わない」ということを避けるための手段で、当事者の不正に対する対策である。

ⓓ　アクセス管理

アクセス管理は正当な利用者のみアクセスでき、不正なアクセスができないことである。

④　暗号の原理

ⓐ　換字暗号と転置暗号

暗号化で文字をずらせる換字暗号や文字の順序を変える転置暗号が基本的な暗号変換であり、ずらせる文字数などが鍵となる。非常に長い乱数鍵との排他的論理和で暗号化／復号するバーナム暗号もある。

元データ	１００１０１１１１１０００１０１		
元データ	１００１０１１１	１１０００１０１	転置処理
転置後データ	０１１１１００１	０１０１１１００	
元データ	０１１１１００１	０１０１１１００	換字処理
暗号鍵	１１００１００１	１１００１００１	
暗号データ	１００１０００１	１００１０１０１	

ⓑ　ＸＯＲ演算

ＸＯＲ演算は、排他的論理和の演算であり、２つの入力のどちらか片方が真でもう片方が偽の時には結果が真となり、両方とも真あるいは両方とも偽の時は偽となる論理演算である。この考え方は、次のストリーム暗号やパーナム暗号、換字処理に活用されている。

ⓒ　ストリーム暗号

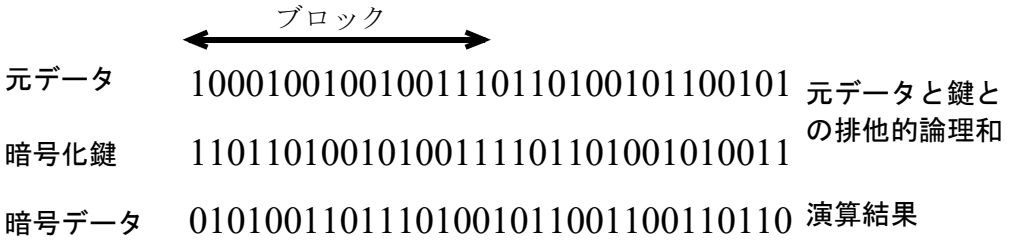
共通鍵暗号はストリーム暗号とブロック暗号の２種類に分類される。ストリーム暗号は、ブロックに区切らず１ビット単位あるいは１バイト単位で逐次暗号化する方式である。任意長の鍵ストリーム列を生成させ、これと入力の平文を演算させる方式である。１ビットや１バイト単位でデータを暗号化できるので、ＳＳＬや無線ＬＡＮなど、ネットワークのトラフィックを暗号化するために利用されている。

暗号化したデータを伝送する場合、ブロック暗号ではブロック全体が揃わないと復号できないが、ストリーム暗号は受信したデータを即座に復号化できる。ブロック暗号がデータ量をブロック長の整数倍に調整するのに対し、ストリーム暗号は平文の量と暗号化後のデータ量が常に一致するという特性がある。応答性が重視される通信用途で用いられることが多い。

ⓓ　ブロック暗号

ブロック暗号は与えられたデータ(平文)を６４ビットや１２８ビットなどあらかじめ定められた固定長のブロックに区切り、この単位ごとに暗号化していく方式である。ブロックごとに分割された平文を内部でさらに分割、転置し、暗号鍵との加算を繰り返していくことで、暗号化を行う。鍵の長さ(鍵長)が大きいほど複雑な暗号を作成できる。ブロック長及び鍵長は固定長のものと、可変長のものがあるが、処理のし易さから固定長のものを採用したものが多い。復号もブロック単位に処理される。

軍事用途で使われることが多かったストリーム暗号に比べて、ブロック暗号は企業など民間で開発されたものが多く、さまざまな種類のものが存在する。代表的なブロック暗号としては米国政府の標準として採用されているＤＥＳ、ＤＥＳを３回かけてさらに安全性を向上させたTriple-ＤＥＳ、ＳＳＬなどＷｅｂの暗号化に利用されているＲＣ５、メール用の暗号PGPで採用されているＩＤＥＡ、ＤＥＳの次世代版として期待されているＡＥＳなどがある。



ⓔ　一方向性関数

一方向性関数は、計算すること自体は比較的容易だが、計算結果から元の情報を逆算することは極めて困難であるような関数のことである。数学的に記述すると、関数ｆが任意のｘについてｙ＝ｆ(ｘ)の計算は簡単であるが、ｙ＝ｆ(ｘ)となるｙが与えられたとき、ｆの逆関数ｇを用いてｘ＝ｇ(ｙ)を導き出すのは事実上不可能である場合に、関数ｆは一方向性関数と呼ばれる。一方向性関数は、暗号理論などで用いられる概念でり、素因数分解問題の困難性を用いたものが代表的名ものである。一方向性関数を利用した暗号は、相手に暗号化鍵を教える際に、他人に漏れても直ちに暗号を解読されるという事態にならないという考えに基づいている。

この考え方は公開鍵暗号方式に利用され、ハッシュ関数として活用されている。

ⓕ　ハッシュ関数

ハッシュ関数は、長い文章やデータを固定長のビット列に圧縮する一方向性の関数で、圧縮された値をハッシュ値と呼ぶ。ハッシュ関数は一方向性のため、ハッシュ値から元のデータを復元することはできない。従って、ハッシュ値にディジタル署名を付して、本人性と文書の真正性の証明に利用したり、証拠の保全・開示に広く利用される。

ⓖ　デジタルフォレックス

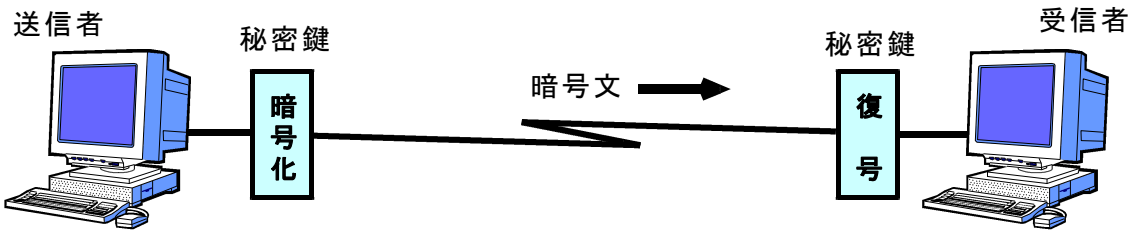
デジタルフォレンジックは、犯罪捜査や法的紛争などで、電子機器に残る記録を収集・分析し、その法的な証拠性を明らかにする手段や技術のことである。対象となるのはパソコンやサーバ、ネットワーク機器、携帯電話、情報家電など、デジタルデータを扱う機器全般である。

関係先の機器を押収して記憶装置から事件の証拠となるデータを抽出したり、サーバや通信機器などに蓄積された通信記録から違法行為の証拠となる活動記録を割り出したり、破壊・消去された記憶装置を復元して証拠となるデータを割り出したりといった技術、コピーや消去、改ざんが容易であるというデジタルデータの性質に対応して、データが捏造されたものかどうかを検証する技術、記録の段階でデータが改ざんできないよう工夫したり、ハッシュ値やデジタル署名などで同一性を保全する技術などの活動が該当する。

デジタルフォレンジックは、不正アクセスや機密情報漏洩など、コンピュータや通信ネットワークに直接関係する犯罪における捜査手法として注目されたが、社会へのＩＴの普及・浸透に伴って、一般の刑事事件などでも捜査や立証に活用されるようになってきている。

⑤　秘密鍵方式

ⓐ　秘密鍵方式とは



秘密鍵方式は送信元の暗号化と受信先の復号を同じ共通鍵で行う方式で、送信者と受信者が共に共通鍵を秘密にもっている暗号化方式である。アルゴリズムは公開されている。代表的なものに米国の標準化暗号方式のＤＥＳがあったが、技術進歩により安全性が低下したため、新たな共通鍵ブロック暗号を世界から公募した結果、ベルギーの研究者が設計したラインダールがＡＥＳとして採用された。ＡＥＳはブロック暗号で、ブロック長は１２８ビット、鍵長は１２８ビット、１９２ビット、２５６ビットの３つが利用できる方式である。

ⓑ　ＤＥＳ暗号

ＤＥＳ暗号は、暗号化と復号に同じ暗号鍵を用いる共通鍵暗号(秘密鍵暗号)の一つで、データを６４ビット単位に区切って処理するブロック暗号である。鍵長は５６ビットだが、パリティチェック用の８ビットを加えた６４ビットを鍵データとして管理する。

ＤＥＳでは変換処理を行った結果に再度同じ処理を行うという繰り返し(ラウンド)を１６回行うが、それぞれのラウンドでは元の鍵から一定の計算により生成した異なる鍵データを用いる。最初にデータを３２ビットずつ半分(Ｌ,Ｒ)に分割し、一回のラウンドでは半分(Ｒ)を変換して残りの半分(Ｌ)と合成する処理を行う。次のラウンドでは前回の合成結果を新たなＲ、変換に用いた半分(Ｒ)を新たなＬとして同じ処理を行う。このような処理方式はファイステル構造と呼ばれ、暗号化と復号が同じアルゴリズムになる(適用する鍵データを変えるだけでよい)ことからＤＥＳ以外にも様々な暗号方式に広まった。

ⓒ　ＡＥＳ暗号

ＡＥＳ暗号は、ＤＥＳの後継として米国の国立標準技術研究所によって制定された新しい暗号化規格である。ＤＥＳの後継となる共通鍵方式の暗号化規格が公募された時、世界中から21の方式が提案された。それらの暗号方式の中から、暗号強度や安全性、ハードウエアやソフトウエアでの実装のしやすさや性能（速度)、計算に必要なハードウエアリソースや必要な電力、鍵長やブロック長などに対する柔軟性、知的財産的な評価など、さまざまな視点から評価・検討された。最終的にラインダール暗号化方式が選ばれた。ラインダールは鍵長やブロック長が可変の共通鍵方式のブロック暗号である。提案されたラインダーではいくつかの鍵長やブロック長が選べたが、最終的には、鍵長１２８、１９２、２５６ビット、ブロック長１２８ビットのパラメーターだけを使うことになり、これが正式なＡＥＳ規格となった。

ＡＥＳには鍵長に応じてＡＥＳ１２８、ＡＥＳ１９２、ＡＥＳ２５６の３種類のバリエーションがある。鍵長を長くすれば、それだけ安全性が増すと考えられるが、その分計算量が増えるのでどれを使うかはケースバイケースである。現在の所は、ＡＥＳ１２８で十分と考えられている。

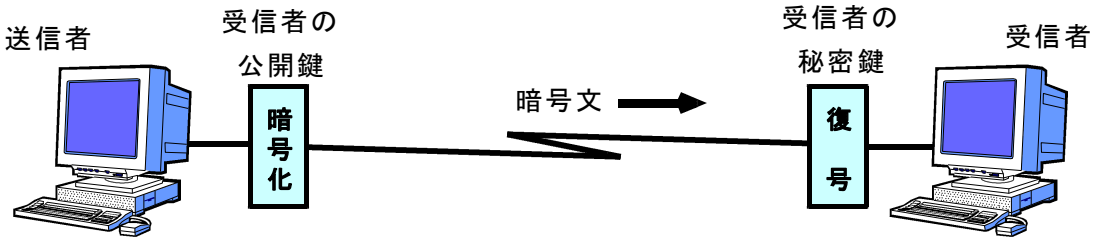
⑥　公開鍵方式

ⓐ　公開鍵方式とは

公開鍵暗号方式は通信文を送信する場合、送信元で公開鍵により暗号化し、受信先で専用の秘密鍵で復号する方式である。暗号化する鍵と復号する鍵が異なり、片方の鍵を公開し、もう一方の鍵は秘密にした暗号化方式である。代表的なものにＲＳＡ方式がある。

公開鍵から秘密鍵を発見することは不可能であり、公開鍵を管理する必要がない。秘密鍵は自分だけが持てばよいので、鍵管理が簡単で安全度が高い。論理が複雑なため処理時間が長くなり、処理速度は共通鍵方式よりも遅い。公開鍵暗号を守秘に使う場合、送信者は受信者の公開鍵を用いて暗号化し、暗号文を送る。受信者は自分だけが知っている秘密鍵を用いて復号し、元の平文を得ることができる。

鍵の配布やデジタル署名に利用される。



ⓑ　ＩＦ型、ＤＬ型、ＥＣ型

公開鍵暗号は、ＩＦ型、ＤＬ型、ＥＣ型に分類できる。ＩＦ型は、素因数分解の困難性に基づくものである。ＤＬ型は、素数の剰余類群における離散対数問題に基づくものである。ＥＣ型は、楕円曲線上の離散対数問題に基づくものである。

ⓒ　ＲＳＡ暗号

ＲＳＡ暗号は、代表的な公開鍵暗号の１つで、整数論の定理であるオイラーの定理と２つの素数を使って公開鍵暗号の仕掛けを実現しており、大きな数の素因数分解が困難であることを、安全性の根拠としている。インターネットを活用した情報交換では、その相手が不特定多数かつ広範囲となることから、鍵の管理が容易かつ相互運用性に優れた方式が必要になる。ＲＳＡ暗号はその性質を満たしており、ＰＫＩやＳＳＬ、ＴＬＳなど、さまざまな場面で活用されている。

通常の公開鍵暗号方式は、公開鍵を用いて暗号化を行い、秘密鍵を用いて復号を行うが、ＲＳＡ暗号はその構造上、通常の公開鍵暗号方式とは逆に、秘密鍵を利用して暗号化を行い、公開鍵を用いて復号を行うことも可能である。このような性質を電子署名に応用することは十分可能だが、秘密鍵と公開鍵の役割を逆転させたＲＳＡ暗号を、そのまま署名として利用する場合、利用の仕方によっては安全性が損なわれる。このため、ＲＳＡ暗号を電子署名用途に用いる場合には、安全性が証明されているＲＳＡ-ＰＳＳなどの既存の方式を用いるべきである。

⑦　ネットワークへの不正侵入

ⓐ　インターネット社会の特性

㋐　ネットワーク上で個人はＩＤとパスワードによって識別される。他人のＩＤとパスワードを使用してなりすますことも可能である。
㋑　不特定多数の人に情報を伝達したり、逆に電子メールを受け取ることもできる。
㋒　時間的、地理的な制約がなく、広範囲なコミュニケーションが可能である。
㋓　ネットワーク上では物理的な場所は必要がない。
㋔　電子データは瞬時に抹消できる。

ⓑ　不正侵入とは

不正侵入は権限のないものがコンピュータシステムへ侵入する行為のことである。他人のＩＤやパスワード、システム上の弱点を悪用して不正にサーバにアクセスする。侵入されると、機密情報を盗まれたり、データを改ざん・消去されたり、別のコンピュータへの不正侵入の踏み台になったりする。ネットワークの利用の広範囲化と高度化に伴って、セキュリティが重要視されるようになり、ネットワークへの不正侵入が問題になっている。侵入検知ツールは不正な侵入を見つけた場合、管理者にアラームを発し、アクセスの遮断やシステムの復旧、侵入者の作業を記録するバックトレースを行う。

ⓒ　代表的なネットワークへの不正侵入の方法

㋐　他人へのなりすましの侵入

相手認証をパスワードで行う方式では、他人のパスワードを使用すると簡単になりすましによる侵入が可能となる。パスワードの類推、ソシアルエンジニアリング手法の利用によるシステム管理者へのなりすましによりパスワードの入手が可能になる。

㋑　セキュリティホールを利用した侵入

開発時のテストに利用した機能が残存した場合、管理者権限を使用して遠隔からプログラムの立ち上げが可能になる。セキュリティホールはプログラムの不具合によるセキュリティ上の弱点である。

㋒　外部からの攻撃

大量のデータを攻撃対象のサーバに送り込んで、正当な利用者にシステムを使わせなくする方法である。システムの機能を停止させてしまう。

ⓓ　不正アクセス対処法

㋐　パスワードを簡単に類推できないものにする。
㋑　ＩＤカードとパスワードを同時に使用する。
㋒　サーバプログラムをセキュリティホール対策済みのものを使用する。
㋓　ファイアウォールを設置する。
㋔　セキュリティ監視により、不正アクセスの兆候を早期に把握し、予防する。
㋕　暗号化によりデータを保護する。

⑧　アクセス管理

ⓐ　アクセス管理とは

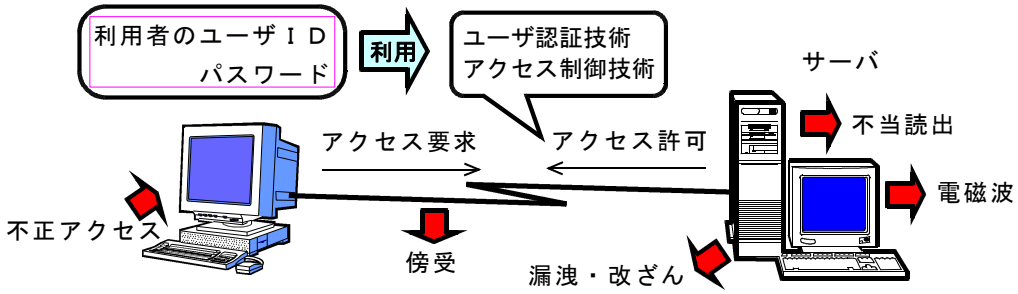
アクセス管理はファイルやネットワークなどへのアクセスに関して、ユーザごとにアクセス権を与え、アクセス状況を管理することである。暗号化と並んで、情報への不当なアクセス

を防止する直接的な対策である。システムの不正利用のリスクやユーザの誤操作によって発生するデータ消失などのリスクを防ぐために実施する。

アクセス管理を適切に行うためには、ユーザ認証技術、アクセス制御技術の二つの技術が必要である。ユーザ認証技術は、名乗ったユーザが本人であることを証明する本人確認技術である。アクセス制御は共有資源の利用を管理・制御する機能であり、アクセス制御技術は、それぞれのユーザがあらかじめ許可された権利以上のアクセスを防止する技術である。

ⓑ　アクセス権

アクセス権は、ユーザがコンピュータのファイルやネットワークなどの共有資源を利用するための権利のことであり、アクセスの禁止や読み取りの許可、書換・削除の許可など、ユーザごとに権利の設定を行う。アクセス制御は他人への成りすまし対策やセキュリティホール対策には無力である。



⑨　アクセス制御技術

ⓐ　アクセスのブロックする部位による分類

㋐　サブネットワークの入り口でのブロック

ファイアウォール技術で特定のネットワークへの不当な侵入を防止する。企業情報ネットワークとインターネットを接続し、その間で選択的にデータのやり取りを行う。

㋑　コンピュータの入り口でのブロック

不当な相手がコンピュータに入れなくするためのものである。相手からかかってきた通信を最初に一度切ってから、コールバックする方式である。

㋒　ファイルの入り口でのブロック

ファイルにアクセスできなくするためのものである。ファイル取り扱いの権利を設定し、その設定により権利のない主体の不正アクセスを制御することができる。

ⓑ　アクセスマトリックス

ユーザがあるファイルに対するアクセス要求を出すと、ＯＳはアクセスマトリックスを参照してそのアクセスが許されているか否かを調べる。許されているならばそのアクセスを実行させ、許されていないならばそのアクセスを行えないようにする。

ⓒ　アクセスマトリックスの設定・変更のやり方

㋐　任意アクセス制御

ユーザにアクセスマトリックスの任意の設定・変更を許す。

㋑　強制アクセス制御

ユーザにアクセスマトリックスの変更を許さない。システムが最初に決定したセキュリティ方針を守らせる。アクセスマトリックスを改ざんされにくいので、セキュリティレベルは高い。あらかじめ正しくアクセスマトリックスができていることが不可欠である。

⑩　オレンジブック

ⓐ　オレンジブックとは

オレンジブックはアクセス制御の機能レベルなどに関連するセキュリティの要求レベルを規準化したものである。米国の軍や政府が民間から製品を調達するために使用している。

ⓑ　セキュリティレベル

Ｄクラスは、セキュリティ機能がないシステムである。Ｃクラスは、任意アクセス制御の機能があるものが対応し、Ｃ１は正規のユーザかどうかが区別できるものであり、Ｃ２は個々のユーザを区別し、アクセス制御が個々のユーザに対して可能なものである。通常のオフィスで使用するシステムはＣクラスである。Ｂクラスは、強制アクセス制御が可能なものである。Ｂ１、Ｂ２、Ｂ３の３クラスからなり、後のものほどセキュリティレベルが高い。Ａクラスは、最もセキュリティレベルが高く、セキュリティ方針とシステムの設計が合致していることを数学的に証明する必要がある。

⑪　ユーザ管理

ⓐ　ユーザ管理とは

ユーザ管理は情報システムの利用者をユーザＩＤなどの識別子を用いて、ユーザの資源利用の実態把握やユーザの不当アクセス防止などの管理を行うことである。ユーザ管理を利用して、ユーザごとにファイルなどの共有資源へのアクセス権を設定し、管理する。障害時に影響されるユーザの迅速な把握、的確な情報提供を行うユーザ支援もユーザ管理の重要な一面である。

ユーザ管理を実施することにより、情報処理システムの信頼性、安全性、効率性および有用性を高め、設備計画の方向性の明確化、セキュリティ面の強化、障害対策の迅速化などの効果が期待される。

ⓑ　ユーザ管理の目的

㋐　資源利用の把握に活用し、合わせて発生する費用の配賦に使用する。
㋑　資源の将来的な設備増強など設備計画に活用する。
㋒　障害発生時に影響の及ぶユーザへ迅速な連絡に活用する。
㋓　利用権を持たない利用者を制限し、情報処理システムの安全性や、信頼性、性能維持の確保に利用する。
㋔　ユーザ支援の一貫として、情報処理システム広報作業など効率性向上のために利用する。

⑫　ユーザＩＤ

ⓐ　ユーザＩＤの付け方

㋐　英数字の組合せで構成されたものが一般的である。
㋑　個人単位のユーザに付与する。ユーザがどのような利用者であるかも体系づける。
㋒　先頭に利用者の作業内容を示す英字を付ける。
㋓　ユーザＩＤによるアクセス権を設定する。

ⓑ　ユーザＩＤの発行・停止

ユーザＩＤの発行・停止はシステム運用管理者によって管理される。ユーザＩＤは、ユーザからの申請に基づき、ＩＤを初期パスワードとセットで発行する。同時に、ユーザのアクセス権も要件に応じて設定される。ユーザは、システム管理者が発行した初期パスワードを独自のパスワードに変更する。

ⓒ　設定・発行・停止時の作業

㋐　ユーザＩＤ発行時のユーザ要件の確認
㋑　人事異動による利用制限の見直し
㋒　退職に伴う利用停止
㋓　定期的な利用状況の確認
㋔　ユーザへの使用指導

ⓓ　ユーザＩＤ発行時の確認項目

㋐　申請者の会社名・所属・氏名・連絡先・プロジェクト名
㋑　利用時間帯
㋒　利用目的

㊓　利用資源、使用量

ⓔ　承認・却下の決定

運用担当者が受付し、システム運用管理者が内容を確認し、承認・却下などを決定する。

ⓕ　ＩＤ発行の可否を決定する審査のポイント

㋐　申請者が以前にも登録申請を行っていないか。(二重登録の禁止)。
㋑　申請者が以前に不正使用などによるＩＤ抹消などの措置を受けていないか。
㋒　利用目的と利用資源が適合しているか(不要箇所へのアクセス禁止)
㋓　利用目的、ＩＤ利用者(責任者)が明確になっているか。
㋔　プロジェクト、組織単位で複数のＩＤ申請を提出した場合、複数申請の理由、利用方法、管理者が明確になっているか。

ⓖ　ユーザＩＤの管理

システム管理者は発行後もユーザＩＤの管理が必要となる。定期的にユーザＩＤの有効性管理を実施する必要がある。過去に情報処理システムを利用していたユーザが過去使用していたユーザＩＤを利用してアクセスすることが考えられる。

ユーザＩＤの管理内容は次の通りである。

㋐　ユーザＩＤの利用期限の設定

利用期限を設定し、期限切れの場合は再度利用申請を行わせる規定を設ける。１年間程度の有効期限を設定し定期更新と併せて更新申請を受け付ける。

㋑　一定期間未使用ユーザのアクセス権停止

一定期間、一度も情報処理システムへアクセスしていないユーザに利用停止措置を行う。利用停止措置を受けたユーザは新たにユーザＩＤの利用承認を受けることとする。

㋒　認証エラーの回数によるアクセス権停止

ユーザが情報処理システムを利用する場合、ユーザＩＤの他にパスワードを入力し、ユーザ認証を行う。このとき何度もパスワードを間違えるということは、ユーザ以外の人間による不正アクセスと考えられるので、一定回数以上の認証エラーの検出をしたユーザＩＤへは停止措置を行う。この保護対策は銀行などの現金自動支払機(ＣＤ)システムなどで利用されている。

⑬　パスワード

ⓐ　パスワードとは

パスワードはコンピュータで利用者の認証を行うために利用される数字や文字列である。利

用制限を行っているコンピュータや共有資源では、ユーザＩＤとパスワードによって利用者であることを認証する。ユーザＩＤの保有者自身が実際にアクセスしているかどうかを確認するために利用する。正当な利用者以外にパスワードを漏洩したり、推測しやすいパスワードを設定すると、悪意ある第三者による不正利用の恐れがある。パスワードの発行はユーザＩＤの発行手続きと同様な方法をとる。

ⓑ　パスワード設定上の留意点

㋐　パスワード入力の際にパスワード自体の表示や印字を抑止する。
㋑　パスワードの有効期限を設定する。
㋒　利用者が自分のパスワードをいつでも自由に変更できるようにする。
㋓　パスワードを暗号化してファイル上に格納する。
㋔　パスワードを保存するパスワードファイルのアクセスを制限する。
㋕　高度パスワードを適用し、類推できるようなパスワードの使用を制限する。
㋖　初期パスワードの設定をする。
㋗　初期パスワードは、初回だけ仮パスワードで情報処理システムへアクセスを許し、ファイルアクセス前にユーザ側で正式のパスワードに変更しなければならない方法にする。

⑭　ユーザＩＤとパスワードの管理機能

ⓐ　セキュリティ監視

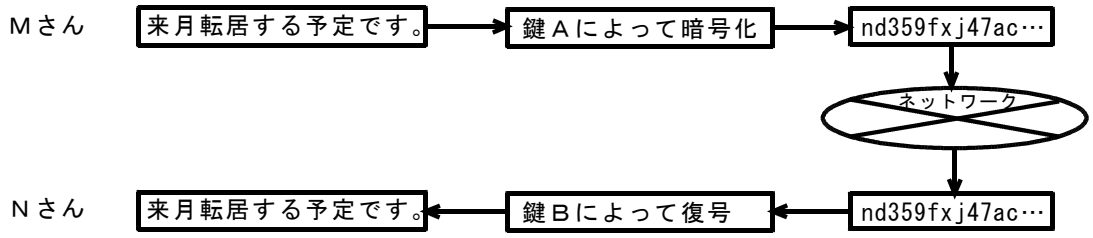
ユーザＩＤとパスワードの管理の機能を利用して、システム運用管理者はユーザの認証などセキュリティ監視を強化する。ユーザＩＤとパスワードのセキュリティ管理プログラムを作成し、管理する仕組みを作り上げることが必要となる。

ⓑ　セキュリティ管理プログラムの機能

㋐　ユーザＩＤの登録／削除機能
㋑　ユーザＩＤに対する認証情報の管理機能
　　ユーザ名、所属部署、連絡先、有効期限など
㋒　ユーザＩＤに対する認証チェック機能
㋓　パスワードの登録／変更機能
㋔　パスワードに対する認証チェック機能
㋕　最終アクセス日時の管理機能

例題演習

公開鍵暗号方式を用いて、図のようにMさんからNさんに他人に秘密にしておきたい文章を送るとき、暗号化と復号に用いる鍵として、適切な組合せはどれか。



	鍵A	鍵B
ア	Mさんの秘密鍵	Mさんの公開鍵
イ	Nさんの公開鍵	Nさんの秘密鍵
ウ	共通の公開鍵	Nさんの秘密鍵
エ	共通の秘密鍵	共通の公開鍵

解答解説

公開鍵暗号方式の鍵に関する問題である。

公開鍵暗号方式は送信元は受信先(Nさん)の公開鍵を利用して暗号化し、受信先は(Nさん)秘密鍵を利用して復号する。求める答えはイである。

例題演習

暗号方式に関する記述のうち、正しいものはどれか。

ア　公開かぎ暗号方式では、暗号かぎを通信相手へ秘密裡に配信する必要がある。

イ　公開かぎ暗号方式では、秘密かぎ暗号方式よりも後で考案され、数学的に巧みな理論を応用しているので、秘密かぎ暗号方式に比べ復号処理が単純で高速なものとなっている。

ウ　秘密かぎ暗号方式のかぎを通信の開始時に公開かぎ暗号方式を使って送り、データの暗号化をそのかぎで行うという方法が実用化されている。

エ　秘密かぎ暗号方式は、多数の相手との通信の際、同一の暗号かぎを用いても安全である。

解答解説

暗号方式に関する問題である。

アの公開鍵暗号方式は送信者は受信者の公開鍵を利用して暗号化し、受信者は自分の秘密鍵で復号する。暗号鍵は公開されている。秘密時に配信する必要はない。

イの公開鍵暗号方式は秘密鍵暗号方式と比べて処理方法が複雑なため処理速度も速くはない。単純で高速であるは誤りである。

ウの内容は秘密鍵暗号化方式の鍵管理の方法として実用化されており正しい。求める答えはウとなる。

エの同一の秘密鍵を多数の通信相手に使用すると秘密鍵でなくなるため安全でない。

例題演習

通信の“傍受や盗聴”の被害を避ける対策として，正しいものはどれか。

ア　暗号化　　イ　デジタル署名
ウ　ファイアウオール　　エ　メッセージ認証

解答解説

傍受や盗聴と暗号化に関する問題である。

傍受・盗聴は、通信回線上を転送されているデータを相手に知られないように入手する犯罪の１つである。高度な技術と機器が必要であり、探知は難しい。

アの暗号化は、傍受や盗聴されても直ちに内容が把握されることにならないため、被害を避ける対策としては効果がある。求める答えはアとなる。

イのデジタル署名は、発信者の認証である。

ウのファイアフォールは、システムへの不正アクセスの防止である。

エのメッセージ認証は、通信上での情報の改変やエラーの検査のために有効な手段であり、傍受や盗聴防止には役立たない。

例題演習

公開かぎ暗号方式の暗号化かぎと復号かぎの関係として，適切なものはどれか。

	暗号化鍵と復号鍵の関係	暗号化鍵	復号鍵
ア	暗号化鍵≠復号鍵	公開	公開
イ	暗号化鍵≠復号鍵	公開	秘密
ウ	暗号化鍵＝復号鍵	秘密	公開
エ	暗号化鍵＝復号鍵	秘密	秘密

解答解説

公開鍵暗号方式の鍵に関する問題である。

公開鍵暗号方式は暗号化鍵と復号鍵は等しくなく、暗号化鍵は公開で、復号鍵は秘密であり、求める答はイとなる。

例題演習

Ｘさんは，Ｙさんにインターネットを使って電子メールを送ろうとしている。電子メールの内容は秘密にする必要があるので，公開かぎ暗号方式を使って暗号化して，送信したい。電子メールの内容を暗号化するのに使用するかぎとして，適切なものはどれか。

ア　Ｘさんの公開かぎ　　イ　Ｘさんの秘密かぎ
ウ　Ｙさんの公開かぎ　　エ　Ｙさんの秘密かぎ

解答解説

電子メールの公開鍵暗号化方式による暗号化の問題である。

送信者はＸさん、受信者はＹさんであるから、Ｘさんが使用する鍵はＹさんの公開鍵である。求める答えはウとなる。

例題演習

公開かぎ暗号方式で，送信者が受信者に暗号文を送る場合の手順はどれか。

ア　送信者は自分の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。
イ　送信者は自分の秘密かぎで暗号化し，受信者は送信者の公開かぎで復号する。
ウ　送信者は受信者の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。
エ　送信者は受信者の秘密かぎで暗号化し，受信者は自分の公開かぎで復号する。

解答解説

公開鍵暗号方式に関する問題である。

送信者は受信者の公開鍵で暗号化し、受信者は自分の秘密鍵で復号する。求める答えはウとなる。

アの暗号化は送信者の自分の公開鍵が誤りで、受信者の公開鍵である。

イの暗号化は送信者の秘密鍵ではなく、受信者の公開鍵で行い、復号は受信者の秘密鍵になる。

エの暗号化は受信者の秘密鍵ではなく、受信者の公開鍵で行い、復号は自分の秘密鍵で行う。

例題演習

代表的な暗号方式の一つであるＤＥＳについて、正しいものはどれか。

ア　アルゴリズムが公開されている共通鍵方式である。
イ　暗号化鍵だけを公開し、復号鍵を秘密にする方式である。
ウ　処理に時間がかかるが、認証機能に優れインターネットでの利用に適した方式である。
エ　米国政府の標準方式で、盗聴者はもちろん、作成者も暗号文を平文に戻すことはできない安全性の高い方式である。

解答解説

ＤＥＳの暗号化方式に関する問題である。

アのアルゴリズムが公開されている秘密の共通鍵暗号方式である。ＤＥＳの内容であり、求める答えはアである。

イの暗号化鍵を公開し復号鍵を秘密にするのは公開鍵暗号方式であり、ＲＳＡ方式である。

ウの処理に時間がかかり認証機能に優れているのは公開鍵暗号化方式のＲＳＡ方式である。

エの暗号文は必ず解読が可能なものであり、平文に戻すことができないは誤りである。ＤＥＳ方式は鍵の管理が的確に行われると安全性の高い方式である。

例題演習

文書の内容を秘匿して送受信する場合の公開鍵暗号方式における鍵の取扱いのうち，適切なものはどれか。

ア　暗号化鍵と復号鍵は公開してもよいが，暗号化のアルゴリズムは秘密にしなければならない。
イ　暗号化鍵は公開してもよいが，暗号化のアルゴリズムは秘密にしなければならない。
ウ　暗号化鍵は秘密にしなければならないが，復号鍵は公開する。
エ　復号鍵は秘密にしなければならないが，暗号化鍵は公開する。

解答解説

公開鍵暗号方式に関する問題である。
アは、暗号化鍵、暗号化アルゴリズムは公開であり、復号鍵が秘密である。
イは、暗号化アルゴリズムも公開でよい。
ウは、暗号化鍵は公開で、復号鍵が秘密である。
エの復号鍵は秘密、暗号化鍵は公開は適切である。求める答えはエとなる。

例題演習

暗号に関する記述のうち, 適切なものはどれか。.

ア　ＤＥＳは, 公開かぎ暗号方式の一種である。
イ　ＲＳＡは, 素因数分解の計算の複雑さを利用した公開かぎ暗号方式の一種である。
ウ　公開かぎ暗号方式の難点は, かぎの管理が煩雑になることである。
エ　公開かぎ暗号方式は, 暗号化と復号とに異なるかぎを用い, 受信者の復号かぎを公開する方式である。

解答解説

暗号に関する問題である。
アのＤＥＳは秘密鍵暗号方式であり、公開鍵暗号方式ではない。
イのＲＳＡは素因数分解を利用した公開鍵暗号方式である。求める答えはイとなる。
ウの鍵の管理が問題になるのは秘密鍵暗号方式であり、公開鍵暗号方式ではない。
エの公開する鍵は受信者の暗号化鍵であり、復号鍵ではない。

例題演習

暗号化方式の名称に関する記述のうち，共通かぎ方式に分類されるものはどれか。

ア　ＤＥＳ　　イ　ＲＳＡ　　ウ　エルガマル暗号　　エ　だ円曲線暗号

解答解説

共通鍵暗号化方式の名称に関する問題である。

アのＤＥＳは米国の商務省標準局によって制定された共通鍵暗号方式である。求める答えはアとなる。

イのＲＳＡは大きな数の素因数分解の困難性を利用したもので、公開鍵暗号方式である。

ウのエルガマル暗号は離散対数問題の困難性を利用したもので、公開鍵暗号方式である。

エの楕円曲線暗号は楕円曲線上の離散対数問題の困難性を利用したもので、公開鍵暗号方式である。

例題演習

平文を公開かぎ暗号方式を用いて暗号化するときの“かぎ”に関する記述として，正しいものはどれか。

ア　暗号文を受信した時に，暗号化かぎから計算によって復号かぎを算出する。
イ　事前に，暗号化かぎから計算によって復号かぎを算出しておく。
ウ　受信側は，暗号化かぎを知っている。
エ　送信側は，暗号化かぎから算出した復号かぎを，暗号化されたメッセージ本文とは別に受信側へ渡す。

解答解説

公開鍵暗号方式の暗号化鍵に関する問題である。

アの復号鍵を暗号化鍵から計算によって求めることができるのなら、暗号化鍵が公開されているからもともと暗号化の意味がなくなる。

イの復号鍵を事前に暗号化鍵から計算によって求めることができるなら、暗号化鍵が公開されていることから、暗号化の意味がなくなる。

ウの受信側が暗号化の鍵を知っていることは、受信側しか知らなければ公開鍵で暗号化しても暗号化の意味があることになる。求める答えはウとなる。

エの暗号鍵から算出した復号鍵を受信側に渡しても、暗号鍵が公開されているから、暗号化の意味がなくなる。

例題演習

ある商店が、顧客からネットワークを通じて注文を受けるために、公開鍵暗号方式を利用して、注文の内容が第三者に分からないようにした。商店、顧客それぞれが利用する鍵の適切な組合せはどれか。

	商店	顧客
ア	公開鍵	秘密鍵
イ	公開鍵	公開鍵と秘密鍵
ウ	秘密鍵	公開鍵
エ	秘密鍵	公開鍵と秘密鍵

解答解説

公開鍵暗号方式に関する問題である。

顧客から注文内容の秘密を商店が守ることであり、商店の関係者以外に秘密にしなければならないため、商店は秘密鍵、顧客は公開鍵を使用する必要がある。求める答えはウとなる。

例題演習

平文を４文字ずつのブロックに分け、それぞれのブロック内の文字の位置を、１番目を３番目に、２番目を１番目に、３番目を４番目に、４番目を２番目に置き換える転置式暗号がある。このとき、平文“ＤＥＥＲＤＩＤＤＲＥＡＭＤＥＥＰ”の暗号文として、正しいものはどれか。

ア　ＤＩＤＤＤＥＥＰＤＥＥＲＲＥＡＭ
イ　ＥＤＲＥＤＤＤＩＡＲＭＥＥＤＰＥ
ウ　ＥＲＤＥＩＤＤＤＥＭＲＡＥＰＤＥ
エ　ＩＤＤＤＥＰＤＥＥＲＤＥＥＭＲＡ

解答解説

暗号文に関する問題である。

ＤＥＥＲ→ＥＲＤＥ　ＤＩＤＤ→ＩＤＤＤ　ＲＥＡＭ→ＥＭＲＡ　ＤＥＥＰ→ＥＰＤＥ

従って、ＥＲＤＥＩＤＤＤＥＭＲＡＥＰＤＥとなり、求める答えはウである。

例題演習

共通かぎ方式の暗号として，ビット列のデータにかぎとの排他的論理和(Å)を適用する方式がある。排他的論理和とは，次のとおりの結果になる演算である。

０Å０＝０　０Å１＝１　１Å０＝１　１Å１＝０

例えば，１１００というデータに対して，１０１０というかぎを使って暗号化すると，暗号データは０１１０となり，同じかぎとの排他的論理和をとることによって復号もできる。

データ	1	1	0	0
かぎ	1	0	1	0
暗号データ	0	1	1	0

↓暗号化　↑復号

１０１０というかぎを使って００１０という暗号データを得た。元のデータはどれか。

ア　００１０　　イ　１０００　　ウ　１０１０　　エ　１１００

解答解説

排他的論理和の論理演算によって暗号化する問題である。

元のデータとかぎの１０１０との排他的論理和が００１０となる元のデータを求めればよいことになる。答は１０００となり、求める答えはイとなる。

例題演習

暗号化に関する記述のうち，正しいものはどれか。

ア　ＤＥＳは公開かぎ暗号方式，ＲＳＡは秘密かぎ暗号方式の代表例である。
イ　公開かぎ暗号方式では，必ず暗号化かぎを秘密にして，復号かぎを公開する。
ウ　デジタル署名に利用するには，公開かぎ暗号方式よりも秘密かぎ暗号方式の方がよい。
エ　秘密かぎ暗号方式では，暗号化かぎと復号かぎは同じである。

解答解説

暗号化に関する問題である。
アのＤＥＳは、秘密鍵暗号方式であり、ＲＳＡは公開鍵暗号方式である。
イの公開鍵暗号方式では暗号化鍵を公開する。復号鍵の公開ではない。
ウのデジタル署名に利用するのは公開鍵暗号方式である。秘密鍵方式ではない。
エの秘密鍵暗号方式は暗号化の鍵と復号の鍵は同じである。求める答えはエとなる。

例題演習

公開鍵暗号方式に関する記述として，適切なものはどれか。

ア　ＡＥＳなどの暗号方式がある。
イ　ＲＳＡや楕円曲線暗号などの暗号方式がある。
ウ　暗号化鍵と復号鍵が同一である。
エ　共通鍵の配送が必要である。

解答解説

公開鍵暗号方式に関する問題である。
ア、ウ、エの内容は秘密鍵暗号方式であり、イの内容が公開鍵暗号方式である。求める答えはイとなる。

例題演習

公開かぎ暗号方式の用法に関する記述のうち，送信者が間違いなく本人であることを受信者が確認できるのはどれか。

ア　送信者は自分の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。
イ　送信者は自分の秘密かぎで暗号化し，受信者は送信者の公開かぎで復号する。
ウ　送信者は受信者の公開かぎで暗号化し，受信者は自分の秘密かぎで復号する。
エ　送信者は受信者の秘密かぎで暗号化し，受信者は自分の公開かぎで復号する。

解答解説

デジタル署名に関する問題である。
公開かぎ暗号方式で、送信者を保証する方式は、送信者が自分の秘密かぎで暗号化し、受信

者が送信者の公開かぎで復号する場合である。求める答えはイとなる。

例題演習

シーザ暗号はアルファベットをＮ文字分ずらす暗号方式である。例えば、ａｂｃｄをＮ＝２で暗号化するとｃｄｅｆとなる。シーザ暗号で暗号化された結果得られた文ｇｅｗｌを復号したところｃａｓｈであることが分かった。Ｎの値で正しいものはどれか。

ア　２　　イ　３　　ウ　４　　エ　５

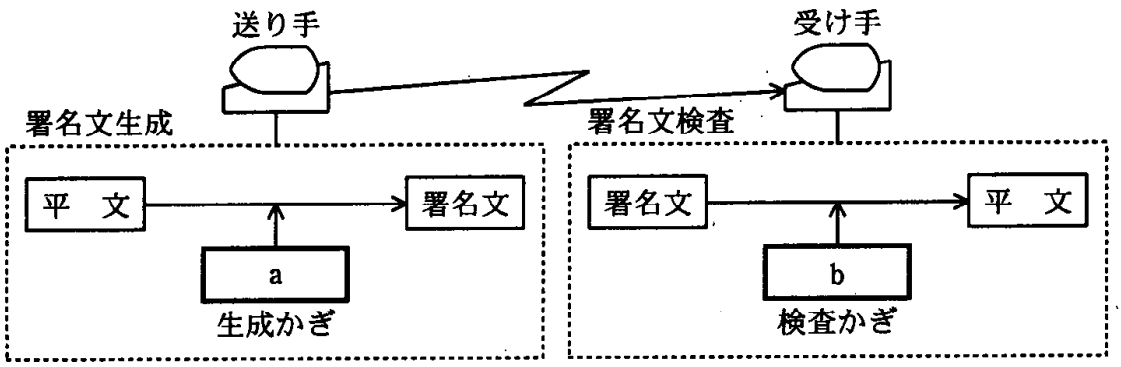
解答解説

シーザ暗号に関する問題である。

ｃ→ｇ、ａ→ｅ、ｓ→ｗ、ｈ→ｌであるからＮ＝４である。求める答えはウである。

例題演習

図は，公開かぎ暗号方式による電子署名の構成を示している。ａ，ｂに該当する適切な組合せはどれか。



	a	b
ア	受け手の公開鍵	受け手の秘密鍵
イ	送り手の公開鍵	送り手の秘密鍵
ウ	送り手の秘密鍵	受け手の公開鍵
エ	送り手の秘密鍵	送り手の公開鍵

解答解説

電子署名に関する問題である。

電子署名は送信元は送り手の秘密鍵を用いて署名文(暗号文)にし、受信先は送り手の公開鍵を用いて平文にする。通常、平文を署名文に変換することを復号、署名文を平文に変換することを暗号化という。

ａは送り手の秘密鍵、ｂは送り手の公開鍵であり、求める答えはエである。

例題演習

公開鍵暗号方式に関する記述のうち，適切なものはどれか。

ア　ＡＥＳは，ＮＩＳＴが公募した公開鍵暗号方式である。
イ　ＲＳＡは，素因数分解の計算の困難さを利用した公開鍵暗号方式である。
ウ　公開鍵暗号方式に参加する利用者の数が増えると鍵の配送が煩雑になる。
エ　通信文の内容の秘匿に公開鍵暗号方式を使用する場合は，受信者の復号鍵を公開する。

解答解説

公開鍵暗号方式に関する問題である。

公開鍵暗号方式は通信文を送信する場合、送信元で公開鍵により暗号化し、受信先で専用の秘密鍵で復号する方式である。暗号化する鍵と復号する鍵が異なり、片方の鍵を公開し、もう一方の鍵は秘密にした暗号化方式である。代表的なものにＲＳＡ方式がある。公開鍵から秘密鍵を発見することは不可能であり、公開鍵を管理する必要がない。秘密鍵は自分だけが持てばよいので、鍵管理が簡単で安全度が高い。論理が複雑なため処理時間が長くなり、処理速度は共通鍵方式よりも遅い。公開鍵暗号を守秘に使う場合、送信者は受信者の公開鍵を用いて暗号化し、暗号文を送る。受信者は自分だけが知っている秘密鍵を用いて復号し、元の平文を得ることができる。鍵の配布やデジタル署名に利用される。

アのＡＥＳは共通鍵暗号方式である。

イのＲＳＡは素因数分解の計算の困難さを利用した公開鍵暗号方式である。求める答はイとなる。

ウの公開鍵暗号方式の利用者が増加しても、鍵は公開されているので煩雑にはならない。

エの公開するのは受信者の暗号化鍵である。

例題演習

電子メールの送信者が正当な相手かどうかを確認するために，公開かぎ暗号方式を用いたディジタル署名を利用する場合，必要となるかぎの組合せはどれか。

ア　受信者の公開かぎと受信者の秘密かぎ
イ　受信者の公開かぎと送信者の秘密かぎ
ウ　送信者の公開かぎと受倍者の秘密かぎ
エ　送信者の公開かぎと送信者の秘密かぎ

解答解説

デジタル署名に関する問題である。

デジタル署名は電子メールの送信者が間違いなく本人であることや、文書やデータが改ざんされていないことを確認するための方法である。文書の送信者が文書をハッシングと呼ばれる手法でダイジェストという短いコードに変換し、このダイジェストを送信者の秘密鍵で暗号化したものがデジタル署名となり、これを元の文書とともに受信者に送付する。受信者はデジタル署名を送信者の公開鍵で復号し、ダイジェストを作成する。送信者のダイジェストと受信者

が再作成したダイジェストが一致すれば、送信者本人からのメールであることを確認できる仕組みである。

アは受信者の公開鍵と秘密鍵であり、誤りである。

イは受信者の公開鍵が誤りである。

ウは受信者の秘密鍵が誤りである。

エの送信者の秘密鍵と公開鍵が正しい。求める答えはエとなる。

例題演習

非常に大きな数の素因数分解が困難なことを利用した公開鍵暗号方式はどれか。

ア　ＡＥＳ　　イ　ＤＳＡ　　ウ　ＩＤＥＡ　　エ　ＲＳＡ

解答解説

公開鍵暗号方式に関する問題である。

アのＡＥＳは、アメリカ合衆国の新暗号規格（Advanced Encryption Standard）として規格化された共通鍵暗号方式である。

イのＤＳＡは、離散対数問題に基づく公開鍵暗号を応用して開発された、デジタル署名方式の一つである。

ウのＩＤＥＡは、ＰＧＰやＳＳＨなどで使用される秘密鍵暗号方式である。

エのＲＳＡは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つである。求める答えはエとなる。

例題演習

デジタル署名の説明として、最も適切なものはどれか。

ア　受信者が署名鍵を使って暗号文を元の平文に戻す。

イ　送信者が、送信する平文の意味を関係者以外に分からないようにする。

ウ　送信者は平文に冗長性を付加し、暗号化する。受信者は復号したとき、予め定められた冗長性が入っていれば正しいメッセージと判断する。

エ　送信者は平文に署名鍵を使って署名することによって、受信者が送信者を確認できるようにする。

解答解説

デジタル署名に関する問題である。

署名が意味があるのは署名者しか署名できないからである。署名の内容を暗号化する場合に署名者しか暗号化の方法が判らないようにする必要がある。デジタル署名は公開鍵暗号方式を利用して署名者が秘密鍵をもち、署名を受信する人が署名者の公開鍵でメッセージを平文に復号するので、信頼性と公開性の上で意味のあるものになる。

アの受信者が署名鍵で平文に戻しても、多くの人が署名鍵を持つことになると署名の意味がなくなってしまうことになる。

イの送信者が署名の意味を関係者以外に分からないようにすると、関係者以外は署名の内容を把握することができない。関係者のみが知るための手段が問題になる。

ウの平文の冗長性のみで署名が可能になるならば暗号化の意味がない。もともと暗号化は冗長性を加えて意味不明のメッセージに一定のルールによって行う手段であり、他人がそれを実行できないところに価値がある。署名の信頼度を高める技術が問題になる。

エは公開鍵暗号方式の仕組みであり、正しい。求める答えはエとなる。

例題演習

ディジタル署名に用いる鍵の種別に関する組合せのうち，適切なものはどれか。

	ディジタル署名の作成に用いる鍵	ディジタル署名の検証に用いる鍵
ア	共通鍵	秘密鍵
イ	公開鍵	秘密鍵
ウ	秘密鍵	共通鍵
エ	秘密鍵	公開鍵

解答解説

ディジタル署名の鍵に関する問題である。

ディジタル署名の作成には発信者の秘密鍵を使用し、ディジタル署名の検証には発信者の公開鍵を使用する。求める答えはエとなる。

例題演習

ディジタル署名などに用いるハッシュ関数の特徴はどれか。

ア　同じメッセージダイジェストを出力する二つの異なるメッセージは容易に求められる。
イ　メッセージが異なっていても，メッセージダイジェストは全て同じである。
ウ　メッセージダイジェストからメッセージを復元することは困難である。
エ　メッセージダイジェストの長さはメッセージの長さによって異なる。

解答解説

ディジタル署名に用いるハッシュ関数の特徴に関する問題である。

ドキュメントや数字などの文字列の羅列から一定長のデータに要約するための関数・手順のことをハッシュ関数という。通信回線を通じてデータを送受信する際に、経路の両端でデータのハッシュ値を求めて両者を比較すれば、データが通信途中で改ざんされていないか調べることができる。１方向関数による生成であるので、ハッシュ値を変更しないまま元データを改ざんすることはできないため、認証と完全性検査に用いられる。

メッセージダイジェストからメッセージを復元することは困難である。求める答えはウとなる。

例題演習

ディジタル署名を利用する主な目的は二つある。一つは，受信者がメッセージの発信者を確認することである。もう一つの目的はどれか。

ア　受信者が，発信者のＩＤを確認すること
イ　受信者が，秘密かぎを返送してよいかどうかを確認すること
ウ　署名が行われた後で，メッセージに変更が加えられていないかどうかを確認すること
エ　送信の途中で，メッセージが不当に解読されていないことを確認すること

解答解説

認証に関する問題である。

認証には、相手認証とメッセージ認証がある。

相手認証は、本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。単純な方式ではパスワードを使用する。第三者のなりすましに対する対策である。

メッセージ認証には、データの完全性と否認防止がある。データの完全性は、通信途上で、内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は、送ったことを否定できないことの保証であり、受信側は、受け取ったことを否定できないことの保証である。

相手認証以外の目的であるから、メッセージ認証である。ウの署名が行われた後で、メッセージに変更が加えられていないかどうかを確認することである。求める答えはウとなる。

ア、イは相手認証、ウはメッセージ認証である。

エは盗聴であり、認証では対応できない。

例題演習

インターネットで公開されているソフトウェアにディジタル署名を添付する目的はどれか。

ア　ソフトウェアの作成者が保守責任者であることを告知する。
イ　ソフトウェアの使用を特定の利用者に制限する。
ウ　ソフトウェアの著作権者が署名者であることを明示する。
エ　ソフトウェアの内容が改ざんされていないことを保証する。

解答解説

ディジタル署名に関する問題である。

ディジタル署名が使用される認証には、相手認証とメッセージ認証がある。相手認証は、本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。メッセージ認証は、データの完全性と否認防止がある。データの完全性は、通信途上で内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は送ったことを否定できないことの保証であり、受信側は受け取ったことを否定できないことの保証である。

ディジタル署名は、ソフトウェアの作成者を認証するものであり、署名後変更されていない

ことを証明するものである。従って、インターネットで公開されているソフトウェアの署名はデータの完全性を保証するものである。求める答えはエとなる。

例題演習

通信販売の電子商取引では，受発注における改ざん，なりすまし，否認によって販売業者又は利用者に被害が及ぶ危険性がある。この三つの防止に適用できるセキュリティ技術はどれか。

ア　ウィルスチェック　　イ　ジャンクメールフィルタ
ウ　ディジタル署名　　エ　フアイアウォール

解答解説

ディジタル署名に関する問題である。

アのウィルスチェックは、コンピュータウィルスを発見・駆除するための処理である。

イのジャンクメールフィルタは、迷惑メールを仕分けし、取り除くフィルタである。

ウのデジタル署名は、受発注情報の改ざん、なりすまし、否認の防止に役立つ。求める答えはウとなる。

エのファイアフォールは、システムへの不正アクセスの防止である。

例題演習

暗号を利用したデジタル署名に関する記述のうち、正しいものはどれか。

ア　発信者は自分の公開鍵でメッセージを暗号化することによってデジタル署名を行い、受信者は自分の公開鍵で復号し確認する。
イ　発信者は自分の公開鍵でメッセージを暗号化することによってデジタル署名を行い、受信者は自分の秘密鍵で復号し確認する。
ウ　発信者は相手の秘密鍵でメッセージを暗号化することによってデジタル署名を行った上で、自分の公開鍵でさらに暗号化する。
エ　発信者は自分の秘密鍵でメッセージを暗号化することによってデジタル署名を行った上で、相手の公開鍵でさらに暗号化する。

解答解説

デジタル署名に関する問題である。

デジタル署名は、電子メールの送信者が間違いなく本人であることや、文書やデータが改ざんされていないことを確認するための方法である。

デジタル署名は秘密鍵と公開鍵を組み合わせた個人認証システムである。

送信元の秘密鍵を用いて復号し、受信先で送信元の公開鍵を用いて暗号化し、元の平文としての署名を得る。文書の送信者が文書をハッシングと呼ばれる手法でダイジェストという短いコードに変換し、このダイジェストを送信者の秘密鍵で暗号化したものがデジタル署名となり、これを文書とともに受信者に送付する。受信者はデジタル署名を送信者の公開鍵で復号し、ダイジェストを作成する。送信者のダイジェストと受信者が再作成したダイジェストが一致すれ

ば、送信者本人からのメールであることを確認できる仕組みである。

発信者は自分の秘密鍵でメッセージを暗号化することによってデジタル署名を行った上で、相手の公開鍵でさらに暗号化することになる。求める答えはエとなる。

例題演習

電子メールを暗号化するために使用される方式はどれか。

ア　ＢＡＳＥ６４　　イ　ＧＺＩＰ
ウ　ＰＮＧ　　エ　Ｓ／ＭＩＭＥ

解答解説

Ｓ／ＭＩＭＥに関する問題である。

アのＢＡＳＥ６４は、電子メールに画像などのバイナリデータを添付する際に、中身を文字列データに置換する方式の一つである。

イのＧＺＩＰは、ファイル圧縮形式の一つである。

ウのＰＮＧは、画像フォーマットの一つである。

エのＳ／ＭＩＭＥは、電子メールを暗号化するための方式である。求める答えはエとなる。

例題演習

ディジタル証明書をもつＡ氏が，Ｂ商店に対して電子メールを使って商品の注文を行うときに，Ａ氏は自分の秘密鍵を用いてディジタル署名を行い，Ｂ商店はＡ氏の公開鍵を用いて署名を確認する。この事法によって確認できることはどれか。ここで，Ａ氏の秘密鍵はＡ氏だけが使用できるものとする。

ア　Ａ氏からＢ商店に送られた注文の内容は，第三者に漏れない。
イ　Ａ氏から発信された注文は，Ｂ商店に届く。
ウ　Ｂ商店に届いたものは，Ａ氏からの注文である。
エ　Ｂ商店は，Ａ氏に商品を売ることの許可が得られる。

解答解説

ディジタル署名に関する問題である。

デジタル署名は、個人認証システムと通信文の暗号化システムの組み合わせで実現するシステムである。送信側は送信元の秘密鍵を用いて署名を復号し、署名を含んだ通信文を受信先の公開鍵で暗号化し伝送する。受信側では、その通信文を受信側の秘密鍵で復号し平文を得て、送信元の公開鍵を用いて暗号化することによって送信者のデジタル署名を得ることができる。メッセージの受信者が、そのメッセージは正当な送信者が署名したものであり、途中で改変されていないことを確認できるシステムである。送信者はメッセージのデータに、秘密鍵で作成した署名データを付けて送信する。受信者は公開鍵を使って署名を確認する。

アの第三者に情報が漏れるかどうかはディジタル署名では確認できない。

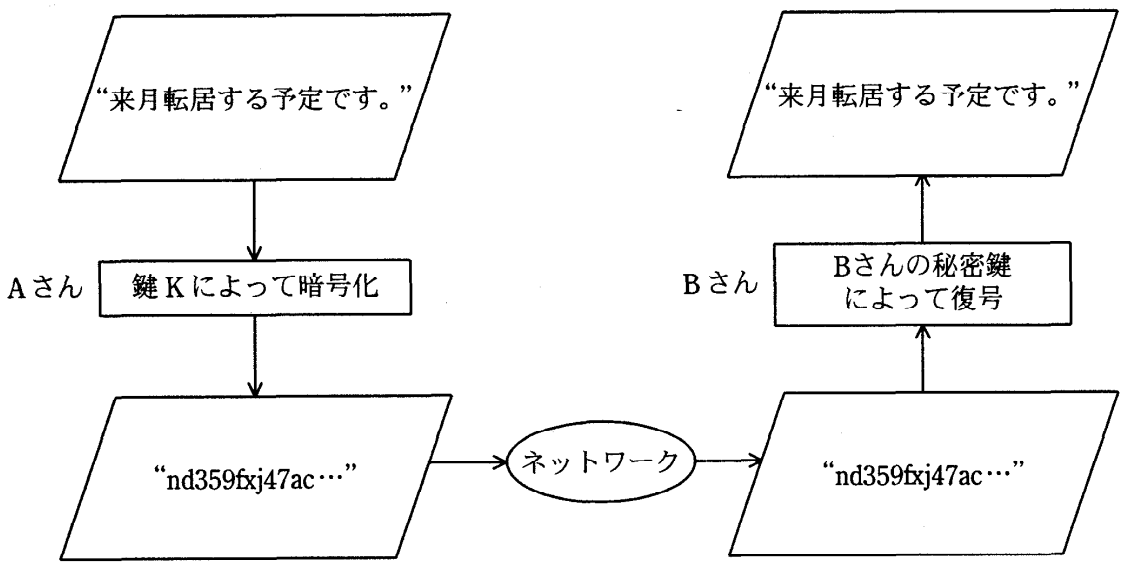
イの発信された注文がＢ商店についてかどうかは確認できない。

ウの発信者がＡさんであることは確認できる。求める答はウとなる。

エのＡ氏に商品を売ることの許可は確認できない。

例題演習

公開鍵暗号方式を用いて，図のようにＡさんからＢさんへ，他人に秘密にしておきたい文章を送るとき，暗号化に用いる鍵Ｋとして，適切なものはどれか。



ア　Ａさんの公開鍵　　イ　Ａさんの秘密鍵

ウ　Ｂさんの公開鍵　　エ　共通の秘密鍵

解答解説

公開鍵暗号方式に関する問題である。

ＡからＢに通信文を送信する時に、暗号化に使用する鍵は受信者Ｂの公開鍵である。ＡはＢの公開鍵で暗号化し、ＢはＢの秘密鍵で復号する。求める答えはウとなる。

例題演習

デジタル署名に関する記述のうち，適切なものはどれか。

ア　発信者は相手の公開かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。

イ　発信者は相手の秘密かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。

ウ　発信者は自分の公開かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。

エ　発信者は自分の秘密かぎでメッセージのハッシュ値を暗号化することによってデジタル署名を生成する。

解答解説

デジタル署名のメッセージの暗号化の方法に関する問題である。

発信者は自分の秘密鍵でメッセージのハッシュ値を暗号化する方法で行う。求める答えはエとなる。

アは相手の公開鍵でなく、自分の秘密鍵である。

イは相手の秘密鍵でなく、自分の秘密鍵である。

ウは自分の公開鍵でなく、自分の秘密鍵である。

例題演習

ディジタル署名付きのメッセージをメールで受信した。受信したメッセージのディジタル署名を検証することによって，確認できることはどれか。

ア　メールが，不正中継されていないこと
イ　メールが，漏えいしていないこと
ウ　メッセージが，改ざんされていないこと
エ　メッセージが，特定の日時に再送信されていないこと

解答解説

ディジタル署名に関する問題である。

ディジタル署名が使用される認証には、相手認証とメッセージ認証がある。相手認証は、本人確認ともいわれ、相手が確かに本当の相手であることを確認する手段である。メッセージ認証は、データの完全性と否認防止がある。データの完全性は、通信途上で内容が改ざんされていないことを検査し、保証する手段であり、第三者の不正に対する対策である。否認防止は、送信側は送ったことを否定できないことの保証であり、受信側は受け取ったことを否定できないことの保証である。

ディジタル署名は、ソフトウェアの作成者を認証するものであり、署名後変更されていないことを証明するものである。従って、インターネットで公開されているソフトウェアの署名はデータの完全性を保証するものであり、メッセージが改ざんされていないことを保証する。求める答えはウとなる。

例題演習

ネットワークを使用するシステムで，暗号化技術を利用しても実現できないものはどれか。

ア　いったん受信したメッセージを，後で送信元から送信した覚えはないといって否定されることを防止する。
イ　受信メッセージが，正当な送出者からのものであることを確認する。
ウ　データの第三者への漏えいを防止する。
エ　メッセージが途中で失われることを防止する。

解答解説

暗号化技術の利用目的に関する問題である。

アの否認防止はメッセージ認証によって実現できる。公開鍵暗号方式の利用である。

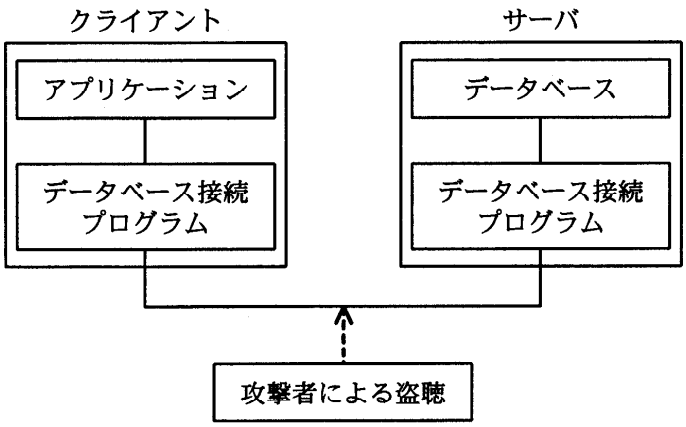
イの相手認証は公開鍵暗号方式を利用すれば実現する。

ウの守秘は暗号化によって実現できる。

エの通信途中での喪失は防止することができない。途中で情報が失われても、内容が理解できないとか理解に時間がかかる場合には対策を講じることが可能になる。そのために暗号化は意味のあることになる。求める答えはエとなる

例題演習

図のように，クライアント上のアプリケーションがデータベース接続プログラム経由でサーバ上のデータベースのデータにアクセスする。データベース接続プログラム間で送受信されるデータが，通信経路上で盗聴されることに対する対策はどれか。



ア　クライアント側及びサーバ側にあるデータベース接続プログラム間の通信を暗号化する。

イ　サーバ側のデータベース接続プログラムにアクセスできるクライアントのＩＰアドレスを必要なものだけに制限する。

ウ　サーバ側のデータベース接続プログラムを起動・停止するときに必要なパスワードを設定する。

エ　データベース接続プログラムが通信に使用するポート番号をデータベース管理システムによって提供される初期値から変更する。

解答解説

盗聴防止対策に関する問題である。

盗聴は電話回線上の通話や通信ネットワーク上で送受信されるデータを不正に傍受することである。ログインに必要なＩＤとパスワード、クレジットカード番号、銀行口座番号などが対象になる。電話盗聴、室内盗聴、電子盗聴などがある。盗聴を防止する手段は暗号化がある。

アの通信の暗号化は盗聴防止に効果がある。求める答えはアとなる。

イのＩＰアドレスの制限、ウのパスワードの設定、エのポート番号の変更などはアクセス制御の役割は果たすが盗聴防止には役立たない。

例題演習

電子メールに用いられるＳ／ＭＩＭＥの機能はどれか。

ア　内容の圧縮　　イ　内容の暗号化と署名
ウ　内容の開封通知　　エ　内容の再送

解答解説

Ｓ／ＭＩＭＥに関する問題である。

Ｓ／ＭＩＭＥは電子メールの暗号化と電子署名に関する規格である。インターネット電子メールの標準仕様であるＭＩＭＥを拡張したプロトコルである。なりすまし、盗聴、改ざんといった電子メールに関する不正行為を防ぐための機能を提供している。Ｓ／ＭＩＭＥではＰＫＩを用いるため、認証局で発行する公開鍵証明書を用いて電子署名の正当性を保証している。

Ｓ／ＭＩＭＥの機能は内容の暗号化と署名である。求める答えはイとなる。

例題演習

コンピュータシステムに対する利用者の利用資格の正当性チェックと利用状況の把握を行う目的で，利用者に付与される情報を表す用語として，適切なものはどれか。

ア　ＩＰアドレス　　イ　アクセス権
ウ　パスワード　　エ　ユーザＩＤ

解答解説

利用資格の正当性チェックと利用状況の把握に関する問題である。

ユーザＩＤはユーザの識別子で、そのユーザがそのシステムを使う権利があるかどうかを判断するのに利用する。ユーザＩＤとパスワードの差異の認識が重要である。

アのＩＰアドレスはＴＣＰ／ＩＰで通信する場合に通信元や通信先を識別するためのアドレスである。

イのアクセス権はデータやプログラムを読み書きし、それを利用することを認めた権利である。

ウのパスワードは正当なユーザかどうかを確認するための合い言葉である。

エのユーザＩＤはコンピュータの利用時にユーザを認識するために、個々のユーザに与えられた番号であり、英字と数字が用いられる。システムへのアクセス権を判断するのに利用したり、使用実績の把握に用いる。求める答えはエとなる。

例題演習

ＰＣからサーバに対し，ＩＰｖ６を利用した通信を行う場合，ネットワーク層で暗号化を行うのに利用するものはどれか。

ア　ＩＰsec　　イ　ＰＰＰ　　ウ　ＳＳＨ　　エ　ＳＳＬ

解答解説

ＩＰsecに関する問題である。

ＩＰsecは、暗号技術を用いて、ＩＰパケット単位でデータの改竄防止や秘匿機能を提供するプロトコルである。ＩＰsecはネットワーク層のプロトコルを保護するので、暗号化がサポートされていない上位層やアプリケーションでもセキュリティの確保が可能になる。ＩＰｖ４ではオプションとして使用することができるが、次世代のＩＰｖ６では標準で実装される。

アのＩＰsecは、ネットワーク層でＩＰによる通信を暗号化するためのプロトコルである。求める答えはアとなる。

イのＰＰＰは、２地点間で回線をつなぎリンクを確立するためのプロトコルである。パソコンからプロバイダのルータまでの間を電話回線でつなぐ場合に利用する。

ウのＳＳＨは、暗号や認証の技術を利用して、安全にリモートコンピュータと通信するためのプロトコルで、ＰＯＰ３やＦＴＰなどネットワーク上に平文のパスワードが流れてしまう既存のプロトコルを安全に使用する技術として広く利用される。

エのＳＳＬは、Ｗｅｂブラウザと Ｗｅｂサーバ間の通信を暗号化して安全にデータをやり取りするためのプロトコルである。

例題演習

“コンピュータ不正アクセス対策基準”に適合しているものはどれか。

ア　監視効率を向上させるためにすべてのネットワークを相互接続する。
イ　業務上必要な場合は，利用者ＩＤを個人間で共有して使用できる。
ウ　システム管理者が，すべての権限をもつ利用者ＩＤを常に使用できる。
エ　組織のセキュリティ方針を文書化し，定期的に研修を開催する。

解答解説

コンピュータ不正アクセス対策基準に関する問題である。

コンピュータ不正アクセス対策基準は、コンピュータ不正アクセスによる被害の予防、発見及び復旧並びに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。システムユーザ基準、システム管理者基準、ネットワークサービス事業者基準及びハードウェア・ソフトウェア供給者基準から構成される。この基準で考えられている「不正アクセス」とは、システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うことである。「システムユーザ」が実施すべき対策として、パスワード及びユーザＩＤ管理、情報管理、コンピュータ管理、事後対応、教育及び情報収集、監査ついてまとめられている。

アの監視効率向上のため単純にネットワーク相互接続したり、ファイルを共有することは、セキュリティ上問題がある。

イの利用者ユーザＩＤは個人単位に設定するのが原則であり、共有は問題がある。

ウのシステム管理者が全ての権限をもつ利用者ＩＤを常に使用するのは不適合である。システム管理者が不正を働く危険性がある。

エのセキュリティ方針の文書化、定期的な研修は適合している。求める答えはエとなる。

例題演習

手順に示す電子メールの送受信によって得られるセキュリティ上の効果はどれか。

〔手順〕

（1）送信者は，電子メールの本文を共通鍵暗号方式で暗号化し(暗号文)，その共通鍵を受信者の公開鍵を用いて公開鍵暗号方式で暗号化する(共通鍵の暗号化データ)。

（2）送信者は，暗号文と共通鍵の暗号化データを電子メールで送信する。

（3）受信者は，受信した電子メールから取り出した共通鍵の暗号化データを，自分の秘密鍵を用いて公開鍵暗号方式で復号し，得た共通鍵で暗号文を復号する。

ア　送信者による電子メールの送達確認

イ　送信者のなりすましの検出

ウ　電子メールの本文の改ざんの有無の検出

エ　電子メールの本文の内容の漏えいの防止

解答解説

通信文の共通鍵を用いた暗号化方式の問題である。

通信文は共通鍵方式で暗号化し、共通鍵の送信を受信者の公開鍵を用いて暗号化し、受信者は自分の秘密鍵で共通鍵を得て、その共通鍵を使用して通信文を平文に復号する。

セキュリティ上の効果は電子メールの本文の内容の漏洩の防止である。求める答えはエとなる。

例題演習

インターネット利用時のセキュリティ確保に関する記述のうち，適切なものはどれか。

ア　インターネットを経由してデータベースサーバを利用する場合，データベースへの不正アクセスやデータの改ざんを防止する対策も必要となる。

イ　インターネットを利用して電子メールを送る場合，暗号化を行えば，電子メールの到達確認ができる。

ウ　インターネットを利用するには，利用者認証システムに登録する必要がある。

エ　社内電子メールシステムをインターネットで社外と接続しても，ファイアウォールを導入すれば，社内からの重要情報の流出は自動的に防止できる。

解答解説

インターネットのセキュリティに関する問題である。

アのデータベースサーバを利用する場合に不正アクセスの防止やデータの改ざん対策が必要になる。求める答えはアとなる。

イの暗号化は、第三者へ内容が漏洩しないようにするために、ある一定の規則に従ってデータを変換することである。暗号化は電子メールの到達確認とは異なる。

ウの利用者認証システムは、ネットワーク経由でコンピュータにアクセスしてくるユーザーが登録済みか否かを信頼できる方法で確認するソフトウエアである。中心部分は認証サー

バと呼ぶソフトウエアで、ユーザーの名前やパスワードなどを一括管理する。インターネットを利用するためには必ずしも必要としない。個人ユーザがプロバイダーと契約してインターネットを利用する場合には、プロバイダーのシステムを経由するために認証が必要になるだけである。

エのファイアウォールは、インターネットとＬＡＮとの間に置くことでデータ通信を管理し、外部からの攻撃や不正アクセスから内部ネットワークを守る仕組みである。ファイアウォールを設置しても社内からの重要情報の流出を自動的に防止できない。

例題演習

セキュリティ技術に関する記述のうち、適切なものはどれか。

ア　地震や火災に対しては、フォールトトレラント方式のコンピュータによるシステムの二重化が有効である。

イ　データの物理的な盗聴や破壊に対しては、ディスクアレイシステムやファイアフォールが有効である。

ウ　伝送中のデータへの不正アクセスに対して、ＨＤＬＣプロトコルのＣＲＣ方式が有効である。

エ　メッセージの改ざんやなりすましによる不正アクセスに対しては、公開鍵暗号方式を応用したディジタル署名が有効である。

解答解説

セキュリティ技術に関する問題である。

アのフォルトトレラント技術は、システムの一部に障害が起きても全体を停止させずに稼働を続け、その間に復旧を図る考え方である。この技術は地震や火災に対しては意味がない。

イの盗聴は、電話回線上の通話や通信ネットワーク上で送受信されているデータを不正に傍受することであり、ファイアフォールやディスクアレイシステムで防ぐことはできない。

ウのＣＲＣ方式は、バーストエラーやランダムエラーなどの通信上の誤りを検出する方式であり、データの不正アクセス防止の対策にはならない。

エのメッセージの改ざんやなりすまし防止にディジタル署名は効果的である。求める答えはエとなる。

例題演習

公衆回線を利用しているコンピュータシステムで、セキュリティの面から適切な運用方法はどれか。

ア　あらかじめ定められたパスワードの変更を禁止する。

イ　接続要求があった場合、特定の電話番号にコールバックして接続する。

ウ　パスワードはユーザが確認できるように、ログイン時に端末に表示する。

エ　パスワードをあらかじめ定めた回数間違えて入力した場合、パスワードを通知する。

解答解説

ユーザ認証の問題である。

パスワードは正当なユーザを確認するための合い言葉であり、設定上次のことに留意する。

① パスワード入力の際にパスワード自体の表示や印字を抑止する。

② パスワードの有効期限を設定する。

③ パスワードを暗号化してファイル上に格納する。

④ パスワードを保存するパスワードファイルのアクセスを制限する。

⑤ 高度パスワードを適用し、類推できるようなパスワードの使用を制限する。

⑥ 初期パスワードの設定をする。

⑦ 初期パスワードは初回だけ仮パスワードでシステムへアクセスを許し、ファイルアクセス前にユーザ側で正式のパスワードに変更しなければならない方法にする。

アのパスワードの変更は、有効期限を設定し、絶えず変更する必要がある。変更を禁止するのは誤りである。

イのコールバックは本人であるかどうかの認証方法の一つて、折り返し電話をすることで本人確認をする方法である。求める答えはイとなる。

ウのユーザがパスワードを確認できるように端末に表示するのは誤りで、パスワードの表示や印字は行ってはならない。

エの一定回数間違ったからといって、親切に相手に通知するのは誤りである。

例題演習

ユーティリティプログラムの不正な実行によるデータの改ざんや破壊を防止する上で，効果的な管理手段として，最も適切なものはどれか。

ア　システムログの採取
イ　ソースプログラムと実行プログラムの比較
ウ　データのバックアップ
エ　ファイルへのアクセス権限の設定

解答解説

データの改ざんや破壊防止に関する問題である。

災害や情報セキュリティのシステム的対策として次のことが考えられる。

① システム・回線の多重化等のフォルトトレラント技術、

② バックアップ技術、無停電電源などの信頼性技術、

③ 暗号、ユーザ認定、アクセス制御などの情報セキュリティ技術

データの改ざんや破壊を防止する最も効果的な方法はセキュリティ技術であり、ファイルへのアクセス権限の設定が効果的である。

ア、ウの内容は障害発生時の回復処理には必要であるが、改ざんや破壊防止には役立たない。

イは改ざんの検出には役立つが防止にはならない。

エのファイルへのアクセス権限の設定はデータの改ざんや破壊防止に効果的である。求める答えはエとなる。

例題演習

あるコンピュータのログイン時に入力するパスワードの文字数は５文字である。英字の大文字２６字と数字が使えるものとする。一つのパスワードが使用できるかどうかを試みるのに０．５秒かかるとした場合、すべてのパスワードの組合せを試すためにはどの程度の期間を必要とするか。

ア　１０日　　イ　１０週間　　ウ　６か月　　エ　１年

解答解説

パスワードの文字数と種類の数、その調査に必要な時間を求める問題である。

パスワードの文字数は５文字で、使用できる文字は英字２６文字、数字１０文字の計３６文字である。これらの文字でできるパターンの種別は36^5＝６０４６６１７６となる。

一つのパスーワードの調査に０．５秒必要であるから、全部のパスワードの検査には次の時間がかかることになる。

３０２３３０８８(秒)→８３９７(時間)→３５０(日)→１(年)

求める答えはエとなる。

例題演習

ユーザＩＤの管理について、最も適切なものはどれか。

ア　同じプロジェクトに参加している利用者は、みな同じユーザＩＤを用いる。
イ　複数のユーザＩＤをもつ利用者は、すべてのＩＤに対して同じパスワードを設定する。
ウ　ユーザＩＤに権限を設定する場合は、必要最小限なものにする。
エ　ユーザＩＤの抹消は、廃止の届出後、十分な期間をおいてから行う。

解答解説

ユーザＩＤ管理に関する問題である。

あるコンピュータをユーザーが使う時に、コンピュータはユーザーＩＤを使って、そのユーザーがそのコンピュータを使う権利があるかどうかを識別する。ＩＤは各ユーザーの識別子であり、このＩＤを管理することをユーザＩＤ管理という。

ユーザ管理の主な目的は次の通りである。

① 資源利用の把握に活用し、合わせて発生する費用の配賦に使用する。
② 資源の将来的な設備増強など設備計画に活用する。
③ 障害発生時に影響の及ぶユーザへ迅速な連絡に活用する。
④ 利用権を持たない利用者を制限し、情報処理システムの安全性や、信頼性、性能維持の確保に利用する。
⑤ ユーザ支援の一貫として、情報処理システム広報作業など効率性向上のために利用する。

ユーザＩＤの付け方は次の通りである。

① 英数字の組合せで構成されたものが一般的である。

② 個人単位のユーザに付与する。ユーザがどのような利用者であるかも体系づける。

③ 先頭に利用者の作業内容を示す英字を付ける。

④ ユーザＩＤによるアクセス権を設定する。

アのプロジェクトで皆同じユーザＩＤを用いるのは間違いで、個人単位に付与する。個人の識別子を用いて、ユーザの資源利用の実態把握と不当アクセス防止などの管理を行う。

イの同一人が複数のＩＤカードをもつのは管理上不合理になる。アクセス権の設定などのユーザＩＤに付与する権限か不明確になる。

ウのユーザＩＤの権限を設定する場合に権限は必要最小限のものにし、利用目的、利用期限を明確にする。求める答えはウとなる。

エのユーザＩＤの抹消は利用目的が完了した時点で直ちに抹消する必要がある。

例題演習

データベースの不正利用を防止する方法として有効なものはどれか。

ア　アクセス権の設定　　イ　一貫性維持の制御

ウ　データのカプセル化　　エ　ファイルの二重化

解答解説

データベースの不正利用防止の方法に関する問題である。

アのアクセス権の設定は正当な利用者のみにアクセスを許可するものであるから、不正な利用者のアクセスを防止することができる。求める答えはアとなる。

イの一貫性維持の制御は状態の変化が正しく反映されるとか矛盾を発生させない性質であり、複数のデータベースで論理矛盾を発生させないように、矛盾が発生する恐れがある場合には、すべてのデータベースを元の状態に戻すことによって回避する方法である。不正利用者のアクセス防止にはならない。

ウのデータのカプセル化は、データとその操作法を一体にすることによって独立性を保つことは可能になるが不正アクセスの防止にはならない。

エのファイルの二重化は故障時の停止を防止でき信頼性の向上にはなるが、不正利用者のアクセス防止にはならない。

例題演習

利用者認証に用いられるＩＣカードの適切な運用はどれか。

ア　ＩＣカードによって個々の利用者を識別できるので，管理負荷を軽減するために全利用者に共通なＰＩＮを設定する。

イ　ＩＣカードの表面に刻印してある数字情報を組み合わせて，ＰＩＮを設定する。

ウ　ＩＣカード紛失時には，新たなＩＣカードを発行し，ＰＩＮを設定した後で，紛失したＩＣカードの失効処理を行う。

エ　ＩＣカードを配送する場合には，ＰＩＮを同封せず，別経路で利用者に知らせる。

解答解説

ＩＣカードの暗証番号に関する問題である。

利用者認証を行うには、ＩＣカードのユーザＩＤとそのカードを使用しているのが本人であることを確認する暗証番号が必要である。ＰＩＮコードは、クレジットカードやキャッシュカードの利用に際し持ち主の本人確認のために使われる秘密の識別番号である。カードを提示した人物が所有者本人であることを確認するために照合される番号で、他人に知られると成りすまして悪用される恐れがあるため、秘密にして暗誦しなければならない。銀行のキャッシュカードなど、多くの場合に４桁の番号が使われる。

アの共通な暗証番号の設定では本人確認は不可能である。

イのＩＣカードの表面に印字している数字情報を組み合わせて暗証番号を作成すると、第三者が推測可能な番号となり、本人確認の機能にはならない。

ウの失効処理の順序が逆である。

エのＩＣカードを配送する場合には暗証番号は同封しない。暗証番号の配送が必要な場合は別経路で配送する。求める答えはエとなる。

例題演習

パスワードに使用する文字の種類をM，パスワードのけた数をｎとするとき，設定できるパスワードの個数Ｐを求める数式はどれか。

ア　$P=M^n$

イ　$P=\dfrac{M!}{(M-n)!}$

ウ　$P=\{\dfrac{M!}{(M-n)!}\}\times\dfrac{1}{n!}$

エ　$P=\{\dfrac{(M+n-1)!}{(M-1)!}\}\times\dfrac{1}{n!}$

解答解説

パスワードに使用する文字の種類を問題にしている。

パスワードに使用する文字の種類をM、パスワードの桁数をｎとするとき、設定できるパスワードの個数は、場合の数の計算で求めると、各桁にM通りの文字が使用できるため、M^nとなる。求める答えはアである。

例題演習

Ｗｅｂビーコンに該当するものはどれか。

ア　ＰＣとＷｅｂサーバ自体の両方に被害を及ぼす悪意のあるスクリプトによる不正な手口

イ　Ｗｅｂサイトからダウンロードされ ＰＣ上で画像ファイルを消去するウイルス

ウ　Ｗｅｂサイトで用いるアプリケーションプログラムに潜在する誤り

エ　Ｗｅｂページなどに小さい画像を埋め込み，利用者のアクセス動向などの情報を収集する仕組み

解答解説

Ｗｅｂビーコンに関する問題である。

Ｗｅｂビーコンは、Ｗｅｂページに埋め込まれた情報収集用の極めて小さい画像のことで、利用者のアクセス動向などを収集するために用いられる。大手サイトを中心に利用されている。求める答えはエとなる。

例題演習

ディレクトリに，読取り，更新，配下のファイル作成のアクセス権を設定できるＯＳがある。この３種類のアクセス権は，それぞれに１ビットを使って許可，不許可を設定する。この３ビットを８進数表現０～７の数字で設定するとき，次の試行結果から考えて，適切な記述はどれか。

〔試行結果〕

① ０を設定したら，一切のアクセスができなくなってしまった。

② ３を設定したら，読取りと更新はできたが，作成ができなかった。

③ ７を設定したら，すべてのアクセスができるようになった。

ア ２を設定すると，読取りと作成ができる。

イ ４を設定すると，作成だけができる。

ウ ５を設定すると，更新だけができる。

エ ６を設定すると，読取りと更新ができる。

解答解説

アクセス権設定に関する問題である。

３ビットで読取り、更新、作成のアクセス権を設定する。

① ０００はすべてのアクセス権を許可しない。

② ０１１は読取り、更新ができ、作成ができない。

③ １１１はすべてのアクセスが可能になる。

④ 以上の内容からアクセス権の設定は、作成・読取り・更新、または作成・更新・読取りになる。

アは、０１０となり、作成はできない。

イは、１００となり、作成だけができる。求める答えはイとなる。

ウは、１０１となり、作成と更新、または作成と読取りになる。

エは、１１０となり、作成と更新、または作成と読取りになる。

例題演習

公開鍵暗号方式の暗号アルゴリズムはどれか。

ア ＡＥＳ　　イ KCipher-2　　ウ ＲＳＡ　　エ ＳＨＡ-２５６

解答解説

公開鍵暗号方式に関する問題である。

アのＡＥＳは、アメリカ合衆国の新暗号規格（Advanced Encryption Standard）として規格化された共通鍵暗号方式である。

イのKCipher-２は、九州大学とＫＤＤＩ研究所により共同開発されたストリーム暗号で、共通鍵暗号方式ある。

ウのＲＳＡは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つである。求める答えはウとなる。

エのＳＨＡ-２５６は、任意長の原文から固定長の特徴的な値であるハッシュ値を求める計算手順である。

例題演習

利用者情報を管理するデータベース(利用者データベース)がある。利用者データベースを検索し，検索結果を表示するアプリケーションに与えるデータベースのアクセス権限として，セキュリティ管理上適切なものはどれか。ここで，権限の範囲は次のとおりとする。

〔権限の範囲〕

参照権限：　利用者データベースのレコードの参照が可能

更新権限：　利用者データベースへのレコードの登録，変更，削除が可能

管理者権限：利用者データベースのテーブルの参照，登録，変更，削除が可能

ア　管理者権限　　イ　更新権限

ウ　参照権限　　エ　参照権限と更新権限

解答解説

権限の範囲に関する問題である。

アプリケーションは、利用者が必要としている情報をデータベースから検索して、その結果を表示する処理であるから、権限のうち登録や変更、削除などは必要でない。アプリケーションに必要な権限は参照権限であり、更新権限、管理者権限は必要がない。求める答えはウとなる。

例題演習

複数の業務システムがある場合のアクセス管理の方法として，最も適切なものはどれか。

ア　業務の担当変更に迅速に対応するために，業務グループごとに共通の利用者ＩＤを使用する。

イ　人事異動が頻繁に発生する場合には，年初にまとめてアクセス権限の変更を行う。

ウ　新入社員の名簿に基づいて，あらかじめ全業務システムに全員の利用者登録を実施しておく。

エ　利用者の職位権限にかかわらず，業務システムごとに適切なアクセス権限の設定を行う。

解答解説

アクセス管理に関する問題である。

アクセス管理はファイルやネットワークなどへのアクセスに関して、ユーザごとにアクセス権を与え、アクセス状況を管理することである。アクセス権は、ユーザがコンピュータのファイルやネットワークなどの共有資源を利用するための権利のことであり、アクセスの禁止や読み取りの許可、書換・削除の許可など、ユーザごとに権利の設定を行う。

ユーザ管理は情報システムの利用者をユーザＩＤなどの識別子を用いて、ユーザの資源利用の実態把握やユーザの不当アクセス防止などの管理を行うことである。ユーザ管理を利用して、ユーザごとにファイルなどの共有資源へのアクセス権を設定し、管理する。

アの利用者ＩＤは利用者個人に対して発行するものであって、原則として業務グループごとに共通のＩＤを使用しない。

イのアクセス権の設定は人事異動など必要が発生する度に変更し、年初にまとめて発行してはならない。

ウの利用者ＩＤの発行は本人の申請に基づいて､担当の業務に関連して発行するものであり、あらかじめ登録しておくものではない。

エの利用者の職務権限に関係なく､業務システムごとにアクセス権を設定するは適切である。求める答えはエとなる。

例題演習

キーロガーの悪用例はどれか。

ア　通信を行う２者間の経路上に割り込み，両者が交換する情報を収集し，改ざんする。
イ　ネットバンキング利用時に，利用者が入力したパスワードを収集する。
ウ　プラウザでの動画閲覧時に，利用者の意図しない広告を勝手に表示する。
エ　プラウザの起動時に，利用者がインストールしていないツールバーを勝手に表示する。

解答解説

キーロガーに関する問題である。

キーロガーは、キーボードからの入力を監視して記録するソフトである。もともとデバッグなどに利用するツールだったが、複数の人間が利用するパソコンに仕掛けてパスワードやクレジットカード番号などを収集するなど、悪用されることがある。

イのネットバンキング利用時に、利用者が入力したパスワードを収集する。

アはプロキシサーバを悪用した中間者攻撃、イはキーロガーの悪用例、ウはアドウェアの悪用例、エはブラウザのアドオン悪用例である。求める答えはイとなる。

例題演習

コンピュータシステムにおけるパスワード運用管理方法として、適切なものはどれか。

ア　トラブル処理を迅速化するために、ユーザＩＤとパスワードの一覧表を作成し、管理者しか分からないように隠す。

イ　利用者が自分のパスワードをいつでも自由に変更できるようにする。

ウ　利用者管理作業を簡素化するために、現在使用されていないユーザＩＤとパスワードを再利用する。

エ　利用者登録申請書が届く前に、新任者の人事異動速報を見てユーザＩＤと仮のパスワードを登録する。

解答解説

パスワード運用方法に関する問題である。

パスワードは利用者の認証を行うために利用する数字や文字列である。利用制限をかけているコンピュータや共有資源では、ユーザＩＤとパスワードによって利用者であることを認証する。

パスワードは次の特徴をもっている。

①　正当な利用者以外に漏らしてはならない

②　推測しやすいパスワードを設定すると、悪意ある第三者による不正利用の恐れがある。

③　パスワードは数字や文字・記号を混在させた推測しづらいものを使用する。

④　パスワードは有効期限を設定し、適宜変更する。

⑤　パスワードは暗号化してファイルに格納する。

アの内容は、パスワードは本来、本人のみが認識でき変更できるものでなければならないため、管理者と言えども他人のユーザＩＤとパスワードの一覧表を作成し、いつでも確認できるようにすることは誤りである。

イの利用者がいつでも変更できるようにすることはパスワードの運用管理方法として適切である。求める答えはイとなる。

ウの現在利用されていないユーザＩＤとパスワードの再利用は、不正アクセスや情報処理システムの破壊などのトラブルの原因になる。従って、使用停止処理を必ず行う必要がある。

エの利用者登録申請書が到着する前に、ユーザＩＤや仮のパスワードを登録することは間違いである。

txt030422　認証システムとファイアウォール

①　認証方式の基本原理

ⓐ　平文認証

平文認証は、通信する相手同士が既知の情報をネットワーク経由でやり取りして相手を確認する認証方式である。通常、ＩＤとパスワードが利用される。ネットワークにログインする場合、ＩＤとパスワードを組み合わせてネットワークに送信し、あらかじめ登録されているＩＤとパスワードを比較して一致すれば認証する。

この方式の問題点は、通信路で盗聴されると正しく認証が行われなくなることである。パスワードを暗号化しても暗号化されたパスワードが盗聴され、利用されるケースが発生すると、正しく認証されなくなる。。

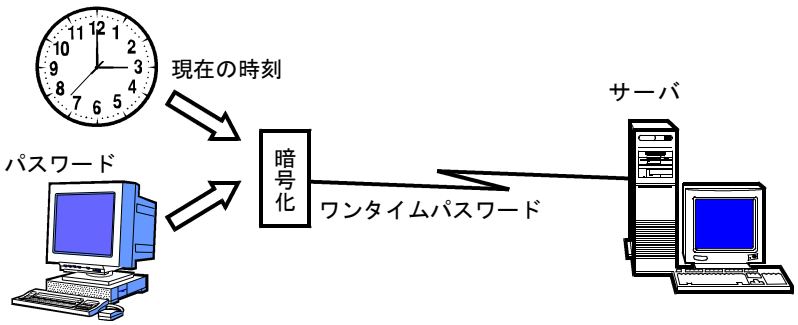
ⓑ　チャレンジ・レスポンス認証

チャレンジ・レスポンス認証は、パスワード自体を送信せずに認証する方法である。通信前に通信者間でパスワードを利用した計算方法を決めておき、双方が同じ計算を行った結果が一致すると相手が本物であると認証する。通信前に取り決める計算方法をハッシュ関数という。

ＡＢ両者間で通信する場合、ＡがＢにアクセスしてくると、ＢはＡに適当な数値をチャレンジとして送信する。受信したＡは、Ｂから送信されたチャレンジとＡのパスワードを使ってＡＢ間のハッシュ関数を利用して数値を求め、この数値をレスポンスとして、ＡのＩＤと共にＢに送信する。これを受信したＢは、ＡのＩＤからＡのパスワードを引き出し、Ｂが送信したチャレンジと組み合わせて同じハッシュ関数を用いて数値を計算する。この計算した数値とＡから送信されたレスポンスを比較して一致すると認証成功となる。

よく利用されるハッシュ関数には、ＭＤ４、ＭＤ５、ＳＨＡ-１などがある。

ⓒ　ワンタイムパスワード

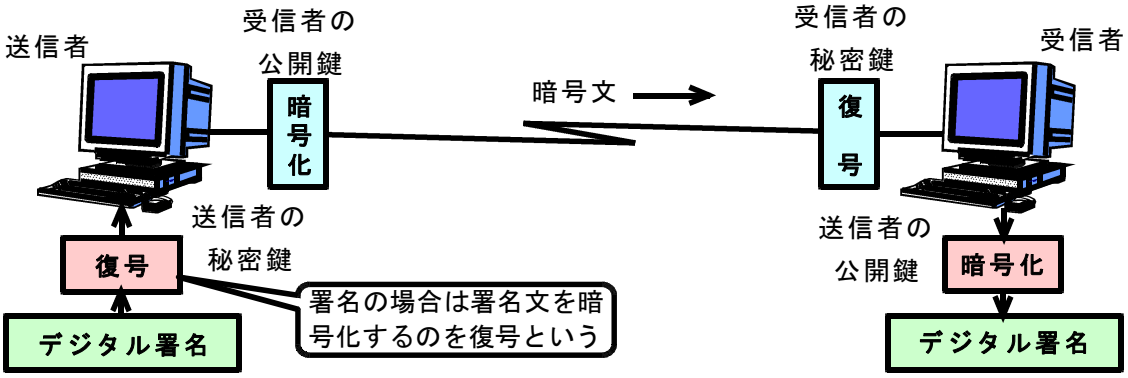


クライアントとサーバ間で暗号鍵を共有し、パスワードを送る場合、毎回暗号化された同じデータで通信すると、そのデータを盗聴し、正当なユーザと偽ってサービスを要求すると、サーバは正当なユーザと認証してしまう。不正者は正しいパスワードを知らないまま正当な

ユーザになりすますことができる。これをリプレイアタックと呼ぶ。

リプレイアタックを考慮すると、認証のためのデータは毎回異なるものにする必要がある。パスワードと現在時刻を組み合わせて情報を暗号化し、時刻が変化すると、認証に用いるデータも変化する方式を利用する。この方式をワンタイムパスワードという。パスワードを使い捨てにする方式である。

ⓓ　デジタル署名



デジタル署名は個人認証システムと通信文の暗号化システムの組み合わせで実現するシステムである。送信側は送信元の秘密鍵を用いて署名を復号し、署名を含んだ通信文を受信先の公開鍵で暗号化し伝送する。受信側では、その通信文を受信側の秘密鍵で復号し平文を得て、送信元の公開鍵を用いて暗号化することによって送信者のデジタル署名を得ることができる。

デジタル署名システムは、メッセージの受信者が、そのメッセージは正当な送信者が署名したものであり、途中で改変されていないことを確認できるシステムである。送信者はメッセージのデータに、秘密鍵で作成した署名データを付けて送信する。受信者は公開鍵を使って署名を確認する。

このシステムでは、署名の暗号化を「復号」といい、署名の復号を「暗号化」という。

ⓔ　デジタル署名実現の条件

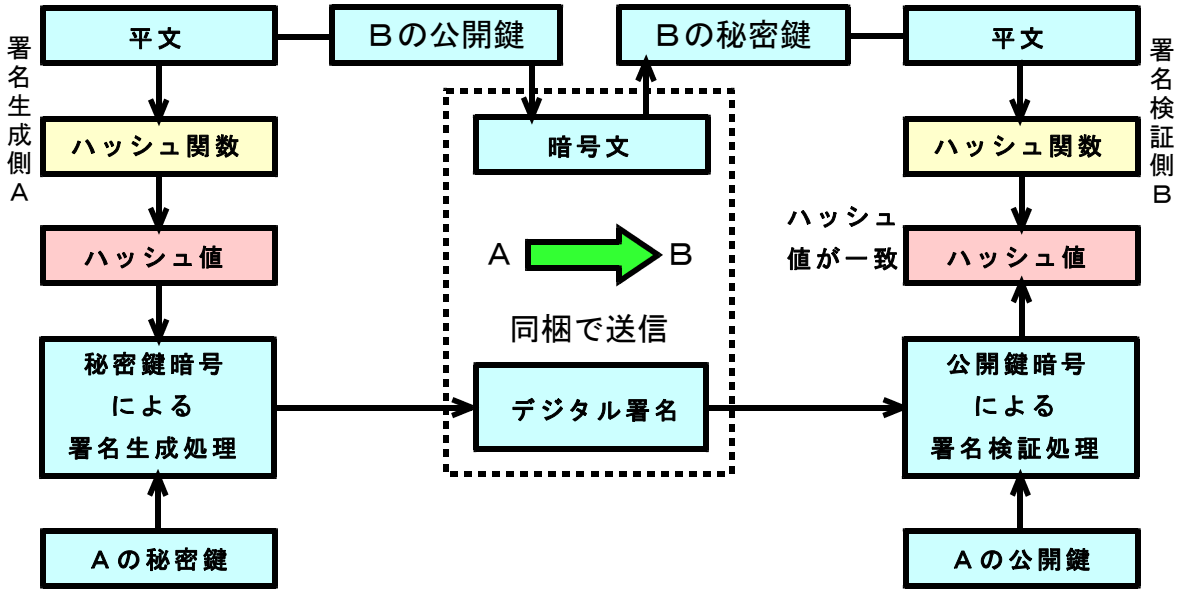
㋐　Ａを確認するには、署名者Ａだけが署名でき、Ａ以外は署名できない条件が必要である。
㋑　Ａ以外のＡの関係者がだれもがＡの署名であることを確認できる必要がある。

ⓕ　公開鍵暗号方式の基本原理

デジタル署名実現の条件は、次の公開鍵暗号方式の基本原理を活用すると可能になる。

㋐　「Ａだけができる」に対して、Ａだけが持っているＡの秘密鍵による処理で可能である。
㋑　「誰でもできる」に対して、みんなが持っているＡの公開鍵による処理で可能である。

ⓖ　ハッシュ値とハッシュ関数



デジタル署名はメッセージに署名して初めて意味のあるものになる。しかし、長いメッセージにデジタル署名することは効率的でない。そこで、長いデータに署名する代わりに、そのデータのハッシュ値に署名することによって効率的になる。長いデータを攪乱し、一定の長さのハッシュ値に圧縮する操作に利用される数学的処理法がハッシュ関数である。

安全なハッシュ関数の条件は、ハッシュ値から入力を推定することが困難であり、異なるデータのハッシュ値が一致する確率が極めて小さいということである。標準的に用いられている関数としては、ＭＤ５、ＭＡＳＨ、ＳＨＡ－１などがある。

ⓗ　ハッシュを活用したデジタル署名の手順

㋐　送信者は送信するデータを作成する。

㋑　作成したデータを基にハッシュ関数を使ってハッシュ値を算出する。

㋒　公開鍵暗号方式を利用してハッシュ値を送信者の秘密鍵を使って暗号化する。

㋓　㋐で作成したデータと㋒で作成した「送信者の秘密鍵で暗号化したハッシュ値」を合わせて受信者に送付する。

㋔　受信者は，受信データを基に，送信者が使ったものと同じハッシュ関数を使ってハッシュ値を算出する。

㋕　送信者が送ってきた「送信者の秘密鍵で暗号化されたハッシュ値」を，あらかじめ入手していた送信者の公開鍵で復号する。

㋖　㋔で算出したハッシュ値と，㋕で復号したハッシュ値を比較する。両者が一致すれば，「伝送経路上でデータが改ざんされていない」，「送信者が正しい」という点を確認できる。

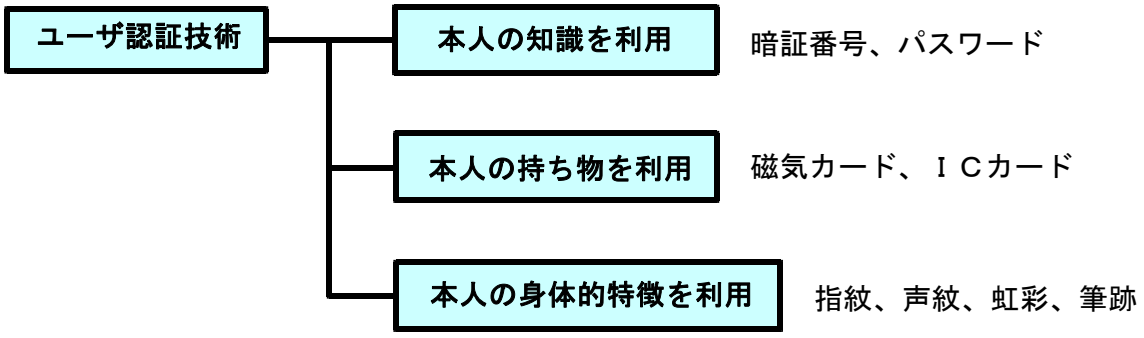
②　ユーザ認証技術

ⓐ　ユーザ認証

認証は正当性を検証する作業のことであり、ユーザ名とパスワードの組み合わせを使って、コンピュータを利用しようとしている人にその権利があるかどうかや、その人が名乗っている本人かどうかなどを確認することである。パソコンへのアクセスやコンピュータルームへの立ち入り時などに実施される。

ユーザ認証は、利用者を識別してユーザごとに異なるサービスを提供するために利用する。認証の際に用いられる情報が他人に発覚すると不正利用が行われてしまう恐れがあり、金銭移動を伴うサービスなど、特に認証データの機密性が要求される場合には、認証データを暗号化するなど、漏洩防止に細心の注意が要求される。なりすまし防止のための本人確認を行なう認証については、認証サービスを行なう企業から入手したデジタル証明書が用いられている。

ⓑ　ユーザ認証技術の分類



㋐　本人の知識を利用するもの

暗証番号、パスワードなどがある。現状のコンピュータシステムではパスワードを用いるものが中心である。

㋑　本人の持ち物を利用するもの

磁気カード、ＩＣカードなどがある。ＩＣカードは安全性の高い手段であるが、値段が高い欠点がある。電子商取引が普及すると、中心的手段の一つになる。

㋒　本人の身体的特徴を利用するもの

指紋、声紋、虹彩、網膜パターン、筆跡、ＤＮＡなどがある。指紋と虹彩を使う方法が有望である。価格とユーザ認証の確実性に課題がある。

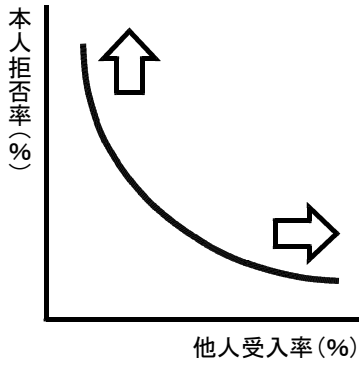
ⓒ　生体認証

生体認証は人間の身体的特徴や行動的特徴の情報を用いて行う個人認証である。

ＦＲＲ(本人拒否)は本人同士のデータの照合で不一致と判定されることことである。ＦＡＲ(他人受入)は本人と他人のデータの照合で一致と判定されることである。

ＦＲＲとＦＡＲは相関関係にあり、片方の比率を上げるともう片方の比率が下がる。安全性を重視すると、ＦＡＲを小さくする必要があるが、その場合ＦＲＲが上がり、使い勝手に影響

がでる。逆に利便性を重視するためにＦＲＲを下げると、ＦＡＲが上がってしまい、安全性が低下してしまう特徴がある。



ⓓ　ユーザ認証技術選択の条件

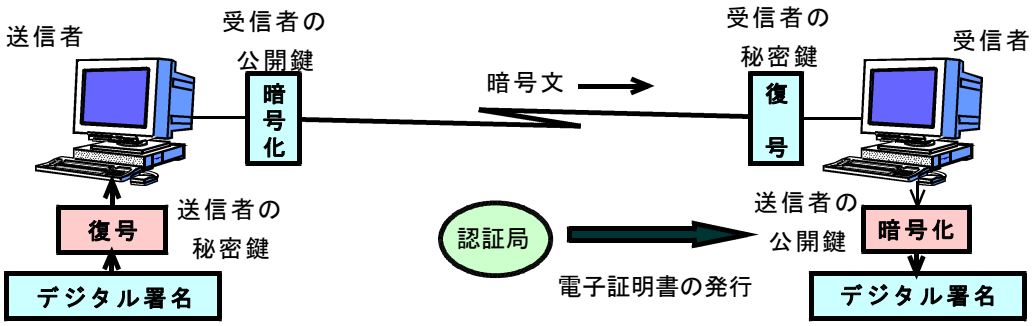
どの方法を採用するかは、ユーザ認証の確実性と実現のためのコストを考慮して決める。安全性を高めるためには、いくつかの対策技術を組み合わせて用いることが大切であり、パスワードとＩＣカードの組合せや更に指紋情報を組み合わせる方法などが考えられる。

ⓔ　リモートユーザ認証とは

分散システムでは、ネットワークを経由して離れた場所にあるサーバにアクセスするときユーザの認証を行う必要がある。この場合の認証がリモートユーザ認証である。リモート環境でユーザ認証を行う場合、パスワードの情報が誰かに見られたり、その情報を記録し再送する脅威にさらされる。

③　電子認証システム

ⓐ　電子認証システムとは



電子認証システムは、デジタル署名技術と認証局、電子証明書を用いて、取引者間の相互認証を実現する仕組みである。商取引における取引相手の確認やデータ改ざんの有無の確認はメッセージ認証やデジタル署名の技術を利用して実現できる。署名の検証者は署名者の正しい公

開鍵を用いることによって可能となる。デジタル署名を使用するシステムでは各ユーザとそのユーザの公開鍵との対比関係が第三者機関によって保証されていなければならない。

ⓑ　認証局（ＣＡ）とは

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。

④　公開鍵基盤（ＰＫＩ）

ⓐ　ＰＫＩとは

公開鍵暗号を利用した証明書の作成、管理、格納、配布、破棄のために必要なハードウェア、ソフトウェア、人、ポリシー、プロトコルによって提供される基盤をＰＫＩという。ＰＫＩはインターネット上で、公開鍵を使って安全に情報をやりとりするための環境である。公開鍵の正当性を保証する機関であるＣＡが発行した公開鍵とその所有者を関連づけるデジタル証明書、公開鍵技術、暗号通信技術など、広範な仕組みや技術を統合することでＰＫＩは実現される。

ⓑ　ＰＫＩに基づく認証の手順

㋐　署名者は、自分の秘密鍵を使用して送信データにデジタル署名を行う。
㋑　署名者は、署名付きデータと自分の電子証明書とを組にして検証者に送る。
㋒　検証者は、安全な手段で入手した認証局の公開鍵を使用して、受け取った電子証明書の正当性を確認する。
㋓　検証者は、署名者から受け取った署名付きデータに施されたデジタル署名の検証を行う。

⑤　ファイアウォールの機能

ⓐ　ファイアウォールとは

ファイアウォールはインターネットと内部ネットワークの接点である境界に設置される。ファイアウォールは、アクセス制御を実現するために流出入情報の一元管理を実施し、外部からの不正侵入を阻止すると共に、不正侵入の影響範囲の局所化や限定化を実現する。

内部ネットワークのセキュリティポリシーに従って、ある通信データの通過は許可するが、他の通信データの通過は拒否するというアクセス制御である。外界のネットワークであるインターネットからの不正な侵入を防止する技術であるが、組織の内部ネットワークにおいて

も、部署間などで異なる機密情報を取り扱うときにアクセス制御することで、不正なアクセスを防止することができる。

ⓑ　設置場所による種類

㋐　外部ファイアウォール

外部ネットワークからの不正な侵入を阻止すると共に、内部ネットワークからの不用意な情報の流出を防止する。外部ネットワークと内部ネットワークの接続点に設置する。

㋑　内部ファイアウォール

内部ネットワークにサブネットワークが複数存在する場合に、各サブネットワークでのセキュリティポリシーの違いにより、サブネットワーク間での情報の流通を種類などにより制御する。内部ネットワークのサブネットワーク間の接続点に設置する。

ⓒ　ファイアウォールの機能要件

㋐　アクセス制御

外部ネットワークと内部ネットワークの間で転送されるデータや利用ユーザ、コンピュータなどのアクセス対象資源の制限を実施する。

㋑　認証

利用を試みるユーザやコンピュータが、正当なアクセスが認められているユーザやコンピュータであるかを検証する。

㋒　暗号化

パスワードや転送データの暗号化を実施する。インターネットにおいてファイアウォール間で転送データを暗号化し、安全に通信することにより専用線のように使用する。これを仮想プライベートネットワークという。

㋓　監視

ネットワーク上のトラフィック量の監視やコンピュータやルータなどの通信機器の使用状況の監視、現在のアクセスログなどのリアルタイム状況の監視などを行う。

㋔　監査

アクセス制御を実施したコンピュータの稼働環境や稼働状況を定期的に監査する。アクセス制御が正当に実施されていたかの監査を行う。

⑥　静的フィルタリングの機能

ⓐ　静的フィルタリング条件

静的フィルタリングは、次の情報を基に条件を静的に作成し、その条件に基づいてパケットの「通過」／「遮断」を実行する。

㋐　送信元IPアドレス
㋑　宛先IPアドレス
㋒　プロトコルの種類（ＴＣＰ,ＵＤＰ，ＩＣＭＰなど）
㋓　送信元ポート番号
㋔　宛先ポート番号
㋕　パケットが流れる方向

ⓑ　フィルタリングテーブルの処理内容

パケットを「通過」させるのか「遮断」するのかを決める条件の集まりをフィルタリングテーブルと呼ぶ。

フィルタリングテーブルの一例を次に示す。

番号	向き	プロトコル	送信元ＩＰアドレス	宛先ＩＰアドレス	送信元ポート番号	宛先ポート番号	処理
①	→(内→外)	ＴＣＰ	192.168.1.＊	＊.＊.＊.＊	＊	80	通過
②	←(内→外)	ＴＣＰ	＊	192.168.1.＊	80	＊	通過
③	＊	＊	＊	＊	＊	＊	遮断

㋐　テーブル番号①の処理

テーブル番号①では、Ｗｅｂサーバへの送信はＨＴＴＰプロトコルで行われ、トランスポート層のプロトコルにＴＣＰが用いられる。Ｗｅｂサーバはポート番号８０でＷｅｂアクセスを待ち受けているので、ＬＡＮ→Ｗｅｂサーバ方向にフィルタリングを行い、処理の条件に合致するパケットは通過となる。従って、送信元がＬＡＮ側のＩＰアドレスのＰＣから、Ｗｅｂサーバ宛てのパケットを通過させるように指定していることになる。

㋑　テーブル番号②の処理

テーブル番号②では、Ｗｅｂサーバからの戻りのパケットに対してフィルタリングを行っている。送信元がＷｅｂサーバで、ＬＡＮ側のＰＣ宛てのパケットを通過させるように設定している。

㋒　テーブル番号③の処理

テーブル番号③では、全ての項目が「*」となっている。処理が遮断であるから、全ての送信元から全ての宛先までの通信を遮断することになる。全ての通信がこの条件に合致する場合に遮断される処理になる。

㋓　フィルタリングテーブルの処理内容

このフィルタリングテーブルで処理する場合、番号①、番号②の条件では、ＬＡＮ側のＰＣとＷｅｂサーバ間の通信を通過させ、Ｗｅｂ以外の通信が全て条件③に合致することとなり遮断されるため、結果として、ＬＡＮ側のＰＣとＷｅｂサーバ間のＨＴＴＰの通信だけがファイアウォールを通過することとなる。

ⓒ　フィルタリング条件の指定とセキュリティ

㋐　遮断するパケットだけを条件で指定し、条件に一致しない通信を通過させる。

この方法は､あらかじめ予想される攻撃を事前にフィルタリング条件として定義するため、条件に一致しないパケットは全て通過してしまうことになる。危険な攻撃手法は無数にあるので、漏れなく全てを定義するのは困難である。フィルタリング条件に漏れがあると不正なパケットが侵入してしまうことになるので、随時、ファイアウォールの条件の見直し、フィルタリングの条件に漏れがないかをを確認する必要がある。

㋑　通過させるパケットだけを条件で指定し、条件に一致しない通信を遮断する。

この方法は、あらかじめ通したいパケットを定義する。定義されていない通信は全て遮断されるので、㋐よりもセキュリティを確保することができる。定義漏れがあったとしても、遮断されることになるので安全である。従って、多くのファイアウォール機能が搭載された製品のデフォルトのフィルタリングの設定は、条件に一致しない通信を全て遮断するようになっている。

⑦　動的フィルタリングの機能

ⓐ　静的フィルタリングの限界

静的フィルタリングは、通過させたい通信のために、行きと戻りのパケットを通過させる穴が開けた状態になってしまう。そこから、クラッカーやウイルスなどから侵入されるリスクが残ってしまう。、送信元のＴＣＰの８０番のポート番号を通すように穴をあけていた場合、クラッカーが送信元ポートを偽装して、不正なパケットを送りつけてくると、ファイアウォールは正規のパケットとして通過させてしまう。パケットフィルタリングは、通過するパケットのＩＰヘッダとＴＣＰヘッダの一部だけをチェックして通過させるかどうかを判断するため、パケットのデータ部分にウイルスやスパムウェアを仕込まれるとパケットフィルタリングをすり抜ける。静的フィルタリングの弱点は、内側から外側へパケットが流れていないときも、戻りのパケットのためにを穴を開けておくということである。

ⓑ　動的フィルタリング機能

次に動的フィルタリングテーブルの例を示す。

番号	向き	プロトコル	送信元ＩＰアドレス	宛先ＩＰアドレス	送信元ポート番号	宛先ポート番号	処理
①	→(内→外)	ＴＣＰ	192.168.1.＊	＊.＊.＊.＊	＊	80	通過
②	←(外→内)	ＴＣＰ	10.0.0.1	192.168.1.1	80	1024	通過
③	＊	＊	＊	＊	＊	＊	遮断

セキュリティを確保するには、通過させたいときにだけ穴を開けたいところなのですが、静的フィルタリングではそれができない。そこで、静的フィルタリングの弱点を解消するために考えられたのが動的フィルタリングである。

ＰＣからＷｅｂサーバへの通信前のフィルタリングテーブルは、条件①、③のみであり、条件②は存在しない。そこで、内部のＰＣがＷｅｂサーバへの通信を開始すると、ファイアウォールが、Ｗｅｂサーバへのアクセスを検知し、この条件がトリガとなり、戻りのパケットのために条件②がフィルタリングテーブルに追加される。

追加された条件②は、送信元のＩＰアドレスが、「10.0.0.1」、宛先ＩＰアドレスが、「192.168.1.1」、宛先ポート番号が「1024」となっており、静的フィルタリングの条件よりも厳密な条件になる。このように、動的フィルタリングでは、条件②を動的に作成するため、ファイアウォールに開ける穴がピンポイントで小さくなるので、想定外のパケットを通過させてしまうリスクが低くなる。Ｗｅｂサーバからの通信は、追加された条件②に一致するため、ファイアウォールを通過する。Ｗｅｂサーバからの通信がなくなると条件②が削除されて条件③となり、外側のＷｅｂサーバから内側のＰＣへ穴を閉じることになる。

⑧　各種ファイアウォール

ⓐ　ネットワーク層型ファイアウォール

インターネットプロトコルのＩＰ層でアクセス制御を実現し、経路制御とパケットフィルタリングの機能を使用する。次の機能がある。

㋐　経路制御

ＩＰ層のデータ転送では、データ転送を行うコンピュータは相手のコンピュータの経路情報を知らなければならない。外部ネットワークと直接データ転送を行う内部ネットワークのコンピュータについては、その経路情報のみを外部ネットワークに対して教え、直接データ転送しないコンピュータについては経路情報を教えない。内部ネットワークのコンピュータへの外部からの不正なアクセスを制御する。

㋑　パケットフィルタリング制御

パケットフィルタリングは、送信元ＩＰアドレス／宛先ＩＰアドレス、送信元ポート番号／宛先ポート番号、接続を開始する方向性、プロトコルに基づき、転送バケットを通過させるかさせないかのアクセス制御を実現することである。パケットフィルタリングによって、あらかじめ設定されていない不正なパケットの流出入を防止する。ルータなどの経路情報を有する装置を利用する。

ⓑ　トランスポート層型ファイアウォール

インターネットプロトコルのＴＣＰ／ＵＤＰ層でアクセス制御を実現し、トランスポートゲートウェアの機能を使用する。データの中継をトランスポート層で実現するため、この中継を行う際にアクセス制御を実施する。アクセス制御の対象は、送信元ＩＰアドレス／宛先

ＩＰアドレスや送信元ポート番号／宛先ポート番号である。

ⓒ　アプリケーション層型ファイアウォール

インターネットプロトコルのアプリケーション層でアクセス制御を実現する。プログラム中継型とユーザログイン型がある。

㋐　プログラム中継型

アクセス制御の対象は、アプリケーションに依存しないＩＰアドレス、ポート番号はもちろんのこと、アプリケーションのプロトコルやデータ構造に依存したユーザ認証や、利用可能なコマンドの選択などのアプリケーション固有のアクセス制御を行う。アプリケーション毎にアプリケーションプロトコルを中継するゲートウェイの新設が必要になる。きめ細かなアクセス制御と利用状況などのプロトコルに基づくログを取得する。

㋑　ユーザログイン型

ファイアウォールにtelnetなどの遠隔端末プログラムを用いてログインし、ファイアウォールに搭載されているプログラムを使用して、外部ネットワークへのアクセスを実現する。特別なプログラムを用意する必要がなく構築そのものは容易である。外部ネットワークにアクセスする際には、常にログインを実施しなければならないために手間がかかり、操作性がよくない。

⑨　仮想プライベートネットワーク

ⓐ　仮想プライベートネットワーク（ＶＰＮ）

ＶＰＮはインターネットをあたかも専用線のように使い､不正な第三者からの脅威に対して、安全な私的なネットワークを構築する。認証システムや暗号技術、トンネリング、ファイアウォールなどを利用することで、インターネット上を流れるデータを保護する。ファイアウォールを基本的な構成要素として使用する。送信ＩＰパケットをファイアウォールにおいて暗号化し、暗号化したデータをファイアウォール間のパケットとして送信する。

通常の専用線と比較して、通信コストが安くなる。組織外のユーザがネットワーク上を流れるデータにはアクセスできない。ネットワークへの参加資格は、組織単位であり、個人を識別する能力はない。トランスポート型とトランスポート／アプリケーション型がある。

ⓑ　ネットワーク層型ＶＰＮ

ネットワーク層に実装したケートウェイを利用して、暗号化通信路を実現する。

通信手順

㋐　送信元はＩＰパケットを送信側ＶＰＮゲートウェイに送る。

㋑　送信側ＶＰＮゲートウェイは、ＩＰパケットを受け取り暗号化する。

㋒　受信側ＶＰＮゲートウェイ宛のＩＰパケット内に、暗号化されたＩＰパケットをカプセ

ル化する。

㋓　受信側ＶＰＮゲートウェイに送信する。

㋔　受信側ＶＰＮゲートウェイは、受信したＩＰパケットのカプセル化を解く。

㋕　暗号化された送信元ＩＰパケットを復号し、送信先に送信する。

ＩＰパケットを別のＩＰパケットにカプセル化する技術をトンネリング技術と呼ぶ。

ⓒ　トランスポート／アプリケーション層型ＶＰＮ

クライアントの通信モジュールとゲートウェイプログラムを用いて、トランスポート層またはアプリケーション層においてアプリケーションの通信データを暗号化することによって実施する。セションの開始時に、ファイアウォールの機器ないしは機器を使用しているユーザの認証を実施することによってアクセス制御を行う。

ⓓ　トンネリング

トンネリングはインターネットなどの公衆回線網上にある２点間を結ぶ閉じられた仮想的な直結通信回線を確立することである。ネットワーク上に外部から遮断された見えない通り道を作るように見えることからトンネルと呼ばれるようになった。

本来通信を行ないたいプロトコルで記述されたパケットを、別のプロトコルのパケットでカプセル化して、送り届けることにより通信を行なう。パケットのカプセル化とその解除はトンネルの両端の機器が自動的に行なうため、トンネルで結ばれた機器同士は途中の通信方式や経路を気にする必要はなく、あたかもトンネルの両端の機器が直結しているように見える。本社と支社のＬＡＮ間接続など、プライベートなネットワークをインターネットを経由して接続する際などに利用される。トンネリング機器やソフトウェアはパケットをカプセル化する際に暗号化を行ない、転送中に覗き見られたり改ざんされたりしないようにするセキュリティ機能を持っていることが多い。

⑩　ＰＰＴＰとＩＰｓｅｃ

ⓐ　ＰＰＴＰ

ＰＰＴＰは、ＰＰＰを拡張したトンネリング・プロトコルである。 ＰＰＴＰ自体は認証や暗号化の機能を有していないが、ＭＳ-ＣＨＡＰによる認証とＲＣ４による暗号化を組み合わたものが、Windowsなどのマイクロソフト製オペレーティングシステムに標準搭載され、ＶＰＮのために利用されている。

ⓑ　ＩＰｓｅｃ

ＩＰｓｅｃは、いくつかの要素技術の組み合わせとして実現され、通信相手を確認して成りすましを防止したり通信途上での改竄を防止するＡＨ､伝送するデータの暗号化を行うＥＳＰ、

公開鍵暗号を用いて安全に暗号鍵の交換・共有を行うＩＫＥなどが利用される。

ＩＰのレベルで送受信内容を暗号化するため、より上位のトランスポート層やアプリケーション層のプロトコルが暗号化に対応していなくても安全に情報をやり取りできるが、ＳＳＬ/ＴＬＳなどと異なり、上位のプロトコルやソフトウェアから通信がＩＰｓｅｃで暗号化されているかどうかを知ることはできない。

ＩＰsecでは二つの動作モードが用意されており、ＩＰヘッダ部分はそのままで、送受信するデータ本体部分のみを暗号化する「トランスポートモード」と、元のＩＰヘッダを暗号化して新しいＩＰヘッダを付け加えることによりパケット全体を暗号化する「トンネルモード」がある。トンネルモードは末端のパソコンなどがＩＰsecに対応していなくても通信経路上のルータなどが対応していれば異なるネットワーク間を暗号化して接続することができるため、ＶＰＮの構築などに利用される。

ⓒ　ＥＳＰ、ＡＨ、ＩＫＥ

ＥＳＰは、ＩＰsecによる暗号化通信で送受信されるペイロード(通信内容)を暗号化して付加情報を付け足したものである。ＩＰパケットのヘッダ部に続くペイロード部を暗号化したもので、暗号化されたデータ本体に一定の形式で暗号化方式や鍵についての情報、認証データなどが付与された構造になっている。

ＡＨは、ＩＰsecの仕様の一部で、送信元の認証や改ざん防止を実現するための仕組みである。ＩＰパケットの中でヘッダの直後に挿入されるデータで、通信内容や秘密鍵などから一定の計算によって割り出したハッシュ値を含み、これにより送信元の偽証や通信内容の改ざんを防止する。ＥＳＰと異なり通信内容の暗号化は行わず、データ本体は平文で送受信される。

ＩＫＥは、ＩＰsecで暗号化通信を行うのに先立って、暗号鍵を交換するために利用される通信プロトコルである。その場限りの暗号化通信を行って、ＩＰsecに必要な暗号化アルゴリズムの決定と暗号鍵の共有を行う。Diffie-Hellman鍵交換と呼ばれる手順によって暗号鍵を交換し、ＩＫＥ限定の暗号化通信を行う。その際にＩＰsecでの通信に必要な各種の情報の交換などの手続きが行われ、ＩＰsecによる通信を開始する。ＩＫＥの通信を盗み見られても、それ自体が暗号化されているため、ＩＰsecの通信を解読される恐れはない。

⑪　ＩＤＳとＩＰＳ

ⓐ　ＩＤＳの役割と仕組み

ＩＤＳは、サーバやネットワークの外部との通信を監視し、攻撃や侵入の試みなど不正なアクセスを検知して管理者にメールなどで通報するシステムである。

防御の対象から、ネットワーク型ＩＤＳ(ＮＩＤＳ)とホスト型ＩＤＳ(ＨＩＤＳ)に大別される。ＮＩＤＳはネットワークを流れる通信をリアルタイムに監視し、不正の兆しのある通信を発見すると記録をとって管理者に知らせる。必ずしもネットワーク境界に設置する必要はなく、プロミスキャスモード(ステルスモード)と呼ばれる特殊な通信モードでネットワーク上のすべての通信を捕捉するようになっている製品が多い。汎用のサーバ機で動作するソフトウェアと

して実装された製品と、専用の通信機器(アプライアンス)として提供される製品がある。対象の個々のコンピュータにソフトウェアの導入や設定の変更などを行う必要がなく、ネットワーク上のすべてのコンピュータに対する攻撃を一台でまとめて監視できる。

ＨＩＤＳは、サーバに常駐して動作するソフトウェアで、そのサーバと他のコンピュータの通信を監視して、攻撃の徴候とみなされるアクセスを検知するとサーバの管理者に知らせる。ソフトウェアの動作状況などをＯＳレベルで詳細に解析することができ、ネットワーク型では検知が難しい攻撃にも対処できる場合がある。ただし、ＨＩＤＳが動作しているコンピュータしか監視できず、コンピュータごとに個別に導入・設定が必要となる。

ⓑ　ＩＤＳの検知手法

㋐　シグネチャ検知方式

シグネチャ検知(不正検出)方式は、既知の攻撃手法について特徴的なパターンを登録したデータベースを用意し、パターンに一致するデータを含むパケットが見つかると攻撃の徴候として検出する手法である。誤検知の可能性は低いが未知の手法による攻撃は見過ごしてしまう場合もある。

㋑　アノマリ検知方式

アノマリ検知(異常検出)方式は、普段とは大きく異なる事態や通常はありえない行動などを検知する手法である。いつもと異なる使い方などをすると攻撃と誤認識してしまうこともあるが、未知の手法による攻撃にもある程度対応できる長所がある。

ⓒ　ＩＰＳ(侵入防止システム)

ＩＰＳは、通信を監視して異常を検知すると管理者に知らせ、アクセスを遮断する等の防御措置を取る機能を持ったシステムである。ネットワークやサーバを監視し、外部から不正アクセスがあると管理者に通知してくれる。設定された条件に従って単純にパケットを選別するファイアウォールとは違って、ネットワークを通過するパケットをリアルタイムに監視し、ポートスキャンやセキュリティホールに対する攻撃、ブルートフォースなどパスワードに対する攻撃などを検知すると管理者に報告する。侵入検知サービス自体は不正アクセスを防御するわけではないが、不正アクセスや未遂の記録をとることによって効率的にネットワークのセキュリティを強化することが可能になる。

⑫　その他ファイアウォール、暗号化プロトコル

ⓐ　ＤＭＺ

ＤＭＺは、インターネットなどの信頼できないネットワークと社内ネットワークなどの信頼できるネットワークの中間に置かれるセグメントのことである。社内ネットワークをインターネットに接続する際に、Ｗｅｂサーバやメールサーバなどインターネットに公開しなければならないサーバは、ＤＭＺセグメントに設置する。ＤＭＺセグメントは、ファイアウォールで囲

まれたセグメントとして存在し、インターネットからの不正なアクセスから保護されるとともに、内部ネットワークへの被害の拡散を防止する。最近では内部犯行による被害の増加から、内部ネットワークからの不正なアクセスを防ぐという目的で使用する場合もある。

ⓑ　ＷＡＦ

ＷＡＦは､外部ネットワークからの不正アクセスを防ぐためのファイアーウォールの中でも、Ｗｅｂアプリケーションのやり取りを把握・管理することによって不正侵入を防御することのできるファイアウォールである。ＷＡＦの特徴としては、従来のファイヤーウォールがネットワークレベルで管理していたことに対して、ＷＡＦはアプリケーションのレベルで管理を行うことである｡ＷＡＦでは､プログラムに渡される入力内容などを直接に検査することによって、不正と見なされたアクセス要求を遮断するという仕組みが採用されている。クライアントの操作するＷｅｂブラウザとＷｅｂサーバを仲介するかたちで存在し、ブラウザとの直接的なやり取りをＷＡＦが受け持つ。それによってＳＱＬインジェクションやクロスサイトスクリプティング、強制ブラウジングといった要求に対して、「攻撃」と見なして拒絶することができる。

ⓒ　ＨＴＴＰＳ

ＨＴＴＰＳは、ＨＴＴＰにＳＳＬやＴＬＳで暗号化機能を加えたプロトコルで、サーバの認証、通信内容の暗号化、改竄検出などを行い、なりすましや盗聴などの攻撃を防ぐことができる。ＷｅｂブラウザとＷｅｂサーバの間の通信を暗号化して、ウェブサーバーとクライアントの間の通信を傍受から守ったり、通信経路上での第三者のなりすましを防止したりする。クレジットカードの番号や個人情報をやりとりするショッピングサイトなどで用いられる。

ⓓ　ＳＳＬ－ＶＰＮ

ＳＳＬ-ＶＰＮは、暗号化にＳＳＬ技術を使用したリモートアクセスＶＰＮのことである。リモートアクセスＶＰＮには、ＩＰｓｅｃによるリモートアクセスＶＰＮと、ＳＳＬによるリモートアクセスＶＰＮの大きく分けて２つがある。ＩＰｓｅｃによるリモートアクセスＶＰＮの場合、クライアントＰＣに必ずＶＰＮクライアントのソフトウェアをインストールする必要があるのに対して、ＳＳＬによるリモートアクセスＶＰＮの場合はＷｅｂブラウザさえあれば通信可能である。多くのＷｅｂブラウザやメールソフトは標準でＳＳＬに対応しているため、リモートアクセス用途などで手軽に導入できる。

ⓔ　ＳＭＴＰ－ＡＵＴＨ

ＳＭＴＰ-ＡＵＴＨは、メールの送信や転送に用いるプロトコルであるＳＭＴＰの拡張仕様の一つで、メールの発送時に、メールサーバが送信依頼をしてきた相手が正規の利用者かどうかを確認する方法を規定したものである。利用者の手元のメールクライアントからネットワーク管理者の運用するＳＭＴＰサーバへメールの送信依頼を行う際に認証過程を導入し、クライアント側にアカウント名やパスワードを申告させて確かに正規の利用者であることを確認してから送信を受け付けるようにする。

⑬　検疫ネットワーク

ⓐ　検疫ネットワークとは

検疫ネットワークとは、社外から持ち込んだパソコンや携帯情報端末などを接続し、ウイルスなどに感染していないか検査する専用のネットワークである。

コンピュータウイルスなどの中には、ネットワークに接続するとすぐに別のコンピュータへの侵入や感染を試みるものがあるため、社内の業務用のネットワークから隔離された検疫ネットワークに一旦接続し、不審な点がないか調査する。ウイルス対策ソフトなどにより問題が見つかった場合は、ウイルスの駆除などを行い、業務用ネットワークへの接続を許可する。

検疫ネットワーク製品によっては、ウイルス感染だけでなく、ＯＳのバージョンが最新か、既知の保安上の脆弱性が放置されていないかなども調べ、ソフトウェアの更新を行ったりする機能を持っているものもある。

ⓑ　アクセス先を振り分ける機能

㋐　ＤＨＣＰサーバー方式

ＤＨＣＰサーバー方式は、アクセス先の切り替えにＤＨＣＰサーバーを使用する。検査を受けていないパソコンと検査に合格したパソコンに異なるネットワークアドレスを割り振ることで、検査に合格したパソコンだけが社内ＬＡＮに接続できるようになる。

㋑　認証スィッチ方式

認証スィッチ方式は、ユーザーを認証する機能を持ったＬＡＮスィッチを使用する方法である。認証の結果によって、そのパソコンがアクセスできるＬＡＮスィッチのポートなどを変更して、パソコンが接続できるネットワークの範囲を切り替える。

㋒　パーソナル・ファイアウォール方式

パーソナル・ファイアウォール方式は、パソコンにインストールするパーソナル・ファイアフォール・ソフトとそれらを遠隔制御する検疫サーバーからなる。パソコンを社内ＬＡＮに接続すると、検疫ネットワークにアクセスし、パーソナル・ファイアウォール・ソフトエージェント機能が動作し、最新のセキュリティ情報に合致しているかを調べ、合致していると社内ＬＡＮに切り替える。

例題演習

認証局（ＣＡ）の役割に関する記述のうち、適切なものはどれか。

ア　相手の担保能力を確認する。
イ　公開鍵暗号方式を用いて、データの暗号化を行う。
ウ　転送すべきデータのダイジェスト版を作成し、電子署名として提供する。
エ　ユーザの公開鍵の正当性を保証する証明書を発行する。

解答解説

ＣＡに関する問題である。

ＣＡはインターネットのメールやWWWページなどにデジタル署名するときに付与する電子印鑑証明書を発行するシステムである。求める答えはエである。

例題演習

ＰＫＩ（公開鍵基盤）の認証局が果たす役割はどれか。

ア　共通鍵を生成する。
イ　公開鍵を利用しデータの暗号化を行う。
ウ　失効したディジタル証明書の一覧を発行する。
エ　データが改ざんされていないことを検証する。

解答解説

認証局の役割に関する問題である。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。

認証局の主な役割には次のものがある。

①　申請者の公開鍵にディジタル署名を付したディジタル証明書を発行する
②　ＣＲＬ(証明書失効リスト)を発行する
③　ＣＰＳ(認証局運用規定)を公開する
④　ディジタル証明書を検証するための認証局の公開鍵を公開する
⑤　認証局の秘密鍵を厳重に管理する

失効した(効力をなくした)ディジタル証明書の一覧を発行する内容が適切である。求める答えはウとなる。

例題演習

パスワードを用いて利用者を認証する方法のうち，適切なものはどれか。

ア　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。
イ　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して比較する。
ウ　パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。
エ　パスワードをハッシュ値に変換して登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して比較する。

解答解説

パスワードを用いた利用者認証に関する問題である。

利用者認証は、相手が本当の相手であることを確認する手段であり、単純な方式では、利用者ＩＤとパスワードを組み合わせて利用する。その際、パスワードの盗難防止の目的で、パスワードをハッシュ値に変化して使用する。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止を図る。

アの利用者ＩＤをハッシュ関数で変換して登録し、認証時に入力されたパスワードをハッシュ関数で変換して比較しても利用者認証にはならない。

イの利用者ＩＤをハッシュ関数で変換して登録し、認証時に入力された利用者ＩＤをハッシュ関数で変換しても、本人の確認は不十分である。

ウのパスワードをハッシュ関数で変換して登録し、認証時に入力されたパスワードをハッシュ関数で変換し、比較すると本人の確認は可能である。求める答えはウとなる。

エのパスワードをハッシュ関数で変換して登録し、認証時に入力された利用者ＩＤをハッシュ関数で変換しても、本人の確認は不十分である。

例題演習

入力パスワードと登録パスワードを用いて利用者を認証する方法において，パスワードファイルへの不正アクセスによる登録パスワードの盗用防止策はどれか。

ア　パスワードに対応する利用者ＩＤのハッシュ値を登録しておき，認証時に入力された利用者ＩＤをハッシュ関数で変換して参照した登録パスワードと入力パスワードを比較する。

イ　パスワードをそのまま登録したファイルを圧縮しておき，認証時に復元して，入力されたパスワードと比較する。

ウ　パスワードをそのまま登録しておき，認証時に入力されたパスワードと登録内容をともにハッシュ関数で変換して比較する。

エ　パスワードをハッシュ値に変換して登録しておき，認証時に入力されたパスワードをハッシュ関数で変換して比較する。

解答解説

パスワードの盗難防止に関する問題である。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止を図る。

アの利用者ＩＤをハッシュ関数で変換して、登録パスワードをそのまま保管していると、盗

難時には、パスワードがそのまま使用されることになる。

イのパスワードファイルを圧縮して保管していても、復元すればパスワードを知ることができるため無意味である。

ウのパスワードをそのまま登録していると、ファイルの盗難時にパスワードの内容がそのまま相手に知られてしまう。

エのパスワードをハッシュ関数を使用して、ハッシュ値を求めていると、ファイルを盗まれても直ちに内容が相手に分かることがない。

例題演習

送信者からメール本文とそのハッシュ値を受け取り，そのハッシュ値と，受信者がメール本文から求めたハッシュ値とを比較して実現できることはどれか。ここで，送信者からのハッシュ値は保護されているものとする。

ア　改ざんの有無の検出　　イ　盗聴の防止

ウ　なりすましの防止　　エ　メールの送達の確認

解答解説

メッセージ認証に関する問題である。

認証には相手認証とメッセージ認証がある。相手認証はある人が他の人に自分が確かに本人であると納得させる事をいう。本人固有の情報(名前、所属、住所、電話番号)を伝えたり、指紋、虹彩等のバイオメトリクス情報を伝えたり、パスワードを入力したり、合言葉を認証者に言ったり、ＩＣカードを認証機械に通すことによって行われる。メッセージ認証はメッセージの同一性の保証であり、コンピュータウイルス、不正侵入等を使った破壊行為によりメッセージが変更されていない事を保証する為の手続きである。メッセージmに対しそのハッシュ値Ｘ＝Ｈ(m)を計算し、Ｘを安全なな場所に保管する。mが改竄されて別のメッセージMになっていた場合、Ｘ≠Ｈ(Ｍ)なのでメッセージが改竄された事が分かる。

アの改ざんの有無を検出するはメッセージ認証である。メール本文をハッシュ値と比較するのはメッセージ認証の方法である。求める答えはアとなる。

イの盗聴は電話回線上の通話や通信ネットワーク上で送受信されているデータを不正に傍受することである。

ウのなりすましは他者のユーザＩＤやパスワード、ＩＰアドレスなどを使用して、他者であるふりをしてシステムに進入して不正行為を行うことである。

エのメールの送達確認はメールが目的の相手に無事送られたかどうかを確認することである。

例題演習

無線ＬＡＮやＶＰＮ接続などで利用され，利用者を認証するためのシステムはどれか。

ア　ＤＥＳ　　イ　ＤＮＳ　　ウ　ＩＤＳ　　エ　RADIUS

解答解説

RADIUSに関する問題である。

RADIUSは、ネットワーク資源の利用の可否の認証と利用の事実の記録を、ネットワーク上のサーバコンピュータに一元化することを目的とした、ＩＰ上のプロトコルである。常時接続方式のインターネット接続サービス、無線ＬＡＮ、ＶＬＡＮ、コンテンツ提供サービスなどのサービス提供者側設備において、認証とアカウンティングを実現するプロトコルとして幅広く利用されている。

アのＤＥＳは、米国の商務省が標準暗号化方式として制定した共通鍵暗号方式である。

イのＤＮＳは、インターネットに接続されたコンピュータのドメイン名とＩＰアドレスの対応付けや、両者を置き換える機能などを提供する仕組みである。

ウのＩＤＳは、ネットワークやコンピュータに対する不正行為を検出し、知らせるためのシステムである。

エのRADIUSは、無線ＬＡＮやＶＰＮ等で利用され、利用者を認証するシステムである。求める答えはエとなる。

例題演習

公開かぎ暗号方式を採用した電子商取引において，取引当事者から独立した第三者機関である認証局(ＣＡ)が作成するものはどれか。

ア　取引当事者の公開かぎに対する電子証明書
イ　取引当事者のディジタル署名
ウ　取引当事者のパスワード
エ　取引当事者の秘密かぎに対する電子証明書

解答解説

認証局に関する問題である。

電子商取引(ＥＣ)は、コンピュータとネットワークを利用して企業間の商取引や企業と消費者の直接取引を行う。ＥＣを実現するために各企業はインターネットを活用したプライベートのポータルサイトを構築したり､業界共通のパブリックなポータルサイトに接続するなどして、顧客からのアクセス機会を増やすことを行う。

電子認証システムは、デジタル署名技術と認証局、電子証明書を用いることにより、取引者間の相互認証を実現する仕組みである。電子証明書は、インターネットを利用する電子決済などのために、利用者の正当性を保証する証明書で、この証明書は第３者の認証機関が発行する。電子証明書の技術は、公開鍵暗号方式を利用し、公開鍵のデータが正当であることを証明するために、認証機関はこのデータにデジタル署名をする。デジタル署名を使用するシステムでは、各ユーザとそのユーザの公開鍵との対比関係が第三者機関によって保証されていなければならない。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認後に正しいユーザであることを保証する所有者の識別情報や公開鍵などを記載した電子証明書を発行する。

認証局が発行するのは、取引当事者の公開かぎに対する電子証明書である。求める答えはアとなる。

例題演習

二つの通信主体X，Y間で，次の手順で情報をやり取りしたときの認証に関する記述のうち，正しいものはどれか。

手順１：Yは任意の情報を織り込んだ文字列(チャレンジコード)をXへ送信する。

手順２：Xは，あらかじめX，Y間で定めたルールに基づき，受け取った文字列から新たな文字列(レスポンスコード)を生成しYへ返送する。

手順３：Yは返送されてきたレスポンスコードが正しいことを確認する。

ア　XがYを認証し，YがXを認証する。

イ　XがYを認証する。

ウ　Xがチャレンジコードを認証する。

エ　YがXを認証する。

解答解説

X、Yの２者間での認証に関する通信の問題である。

YがチャレンジコードをXに送信し、Xはレスポンスコードを返信し、Yが確認する仕組みであるから、YがXを認証することになる。求める答えはエとなる。

例題演習

ＥＣ(電子商取引)における認証の役割に関する記述のうち、最も適切なものはどれか。

ア　受信側で、送信者の正当性を証明することである。

イ　送信側及び受信側で、トランザクションの内容が正しいことを証明することである。

ウ　第三者機関によって、トランザクションの内容が正しいことを証明することである。

エ　第三者機関によって、取引相手の正当性を証明することである。

解答解説

電子商取引における認証の役割に関する問題である。

電子認証システムは、デジタル署名技術と認証局(ＣＡ)、電子証明書を用いることにより、取引者間の相互認証を実現する仕組みである。

電子証明書は、インターネットを利用する電子決済などのために、利用者の正当性を保証する証明書で、この証明書は第３者の認証機関が発行する。電子証明書の技術としては公開鍵暗号方式を利用するのが一般的である。公開鍵のデータが正当であることを証明するために、認証機関はこのデータにデジタル署名をする。

商取引における取引相手の確認やデータ改ざんの有無の確認は、メッセージ認証やデジタル署名の技術を利用することによって実現できる。署名の検証者は署名者の正しい公開鍵を用いることによって可能となる。デジタル署名を使用するシステムでは、各ユーザとそのユーザの

公開鍵との対比関係が第三者機関によって保証されていなければならない。

エの第三者機関によって、取引相手の正当性の証明が電子証明書で、求める答えはエとなる。

例題演習

手順に示す処理を実施したとき，メッセージの改ざんの検知の他に，受信者Ｂがセキュリティ上できることはどれか。

〔手順〕

送信者Ａの処理

（1） メッセージから，ハッシュ関数を使ってダイジェストを生成する。

（2） 秘密に保持していた自分の署名生成鍵を用いて，（1）で生成したダイジェストからメッセージの署名を生成する。

（3） メッセージと，（2）で生成したデータを受信者Ｂに送信する。

受信者Ｂの処理

（4） 受信したメッセージから，ハッシュ関数を使ってダイジェストを生成する。

（5） 受信したデータ，（4）で生成したダイジェスト及び送信者Ａの署名検証鍵を用いて，署名を検証する。

ア　メッセージが送信者Ａからのものであることの確認

イ　メッセージの改ざん部位の特定

ウ　メッセージの盗聴の検知

エ　メッセージの漏えいの防止

解答解説

ハッシュ関数を使用した認証システムの問題である。

ハッシュ関数は、あるデータが与えられた場合にそのデータを代表する数値を得る操作、または、その様な数値を得るための関数のことである。ハッシュ関数から得られた数値のことをハッシュ値または単にハッシュという。通信における暗号化やユーザ認証、ディジタル署名などでは、不可逆的な関数で処理を行い、ハッシュ値から原文を再現することができないようにする。これを利用することによって、改ざん防止やパスワードの盗難防止、メッセージ送信者の確認などを図る。

メッセージが送信者Ａからのものであることを確認するとなり、求める答えはアとなる。

例題演習

メッセージ認証符号におけるメッセージダイジェストの利用目的はどれか。

ア　メッセージが改ざんされていないことを確認する。

イ　メッセージの暗号化方式を確認する。

ウ　メッセージの概要を確認する。

エ　メッセージの秘匿性を確保する。

解答解説

メッセージダイジェストに関する問題である。

メッセージダイジェストは、元のメッセージから任意の長さのメッセージを演算処理して特徴的なパターンを生成し、データ通信のメッセージが正しいことを証明する技術である。インターネットの標準技術であるＭＤ５（Message Digest Algorithm 5）では、一方向ハッシュ関数を使った演算により、元のデータの長さに関係なく128ビットのデータを生成する。

メッセージ認証は、受信したメッセージが途中で改ざんされていないかを確認することである。ハッシュ関数の一種であるメッセージダイジェスト関数を用いて求めるメッセージダイジェストを比較して改ざんの有無を確認する。送信メッセージのメッセージダイジェストと受信メッセージのメッセージダイジェストが異なる場合、伝送途中で改ざんがあったと判断する。

メッセージダイジェストは電子署名の基礎技術であり、電子署名ではダイジェストデータをさらに暗号化する。通信回線を通じてデータを送受信する際に、経路の両端でデータのハッシュ値を求めて両者を比較すれば、データが通信途中で改ざんされていないか調べることができる。求める答えはアとなる。

例題演習

セキュリティプロトコルＳＳＬの特徴はどれか。

ア　ＳＳＬはＷｅｂサーバだけで使用されるセキュリティ対策用のプロトコルで，ネットワーク層に位置するものである。

イ　ＳＳＬを利用するＷｅｂサーバでは，そのＦＱＤＮをディジタル証明書に組み込む。

ウ　個人認証用のディジタル証明書は，ＰＣごとに固有のものを作成する必要がある。

エ　日本国内では，政府機関に限り１２８ビットの共通鍵長のディジタル証明書を取得申請できる。

解答解説

ＳＳＬに関する問題である。

ＳＳＬは、インターネット上で情報を暗号化して送受信するプロトコル。現在インターネットで広く使われているWWWやＦＴＰなどのデータを暗号化し、プライバシーに関わる情報やクレジットカード番号、企業秘密などを安全に送受信することができる。

ＦＱＤＮは、インターネットやイントラネットなどのＴＣＰ／ＩＰネットワーク上で、ドメイン名・サブドメイン名・ホスト名を省略せずにすべて指定した記述形式のことである。

アのＳＳＬはＷｅｂだけで使用されるプロトコルではない。

イは適切な記述である。求める答えはイとなる。

ウのディジタル証明書は、各ユーザからの電子証明書の発行依頼を受け、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。ＰＣ単位ではない。

エのディジタル証明書は、共通鍵ではなく公開鍵暗号方式を使用する。

例題演習

インターネット経由で、WWWサーバにアクセスして商取引をしたい。このWWWサーバの提供者が、商取引上、信頼できる相手であるかどうかを判断するのに有効な情報を与えてくれる仕組みはどれか。

ア　ＩＰパケットフィルタリング　　イ　ＩＰポート番号
ウ　ＳＳＬ　　エ　クッキーヘッダ

解答解説

商取引に関係する認証の問題である。

アのＩＰパケットフィルタリングは、ルーター、ゲートウエイ、ファイア・ウオールなどで、パケットのあて先アドレス、あるいは送信元アドレスとあて先アドレスの組み合わせを調べて、通過させて良いパケットと阻止すべきパケットを区別すること及びその機能である。パケット・フィルタリングは、余分なトラフィックが生じることの抑制と、セキュリティ機能を実現するための方法である。

イのＩＰポート番号はパソコンと周辺機器を接続するインターフェースのコネクタ部分の番号で、ポート番号を通してＩＰパケットは入出力される。ファイアウォールなどで利用される。

ウのＳＳＬは、WWWのブラウザやサーバ間でサーバの認証に利用されたり、通信データを暗号化したりする技術である。求める答えはウである。

エのクッキーヘッダは、WWWサーバーがユーザーを識別・管理するための仕組みである。

例題演習

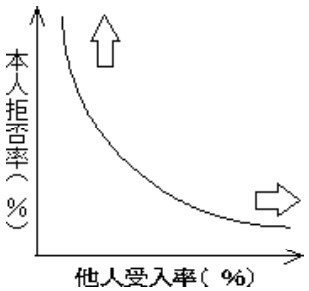
バイオメトリクス認証システムの判定しきい値を変化させるとき，ＦＲＲ(本人拒否率)とＦＡＲ(他人受入率)との関係はどれか。

ア　ＦＲＲとＦＡＲは独立している。
イ　ＦＲＲを減少させると，ＦＡＲは減少する。
ウ　ＦＲＲを減少させると，ＦＡＲは増大する。
エ　ＦＲＲを増大させると，ＦＡＲは増大する。

解答解説

バイオメトリック認証に関する問題である。

ＦＲＲ(本人拒否)は本人同士のデータの照合で不一致と判定されることことである。ＦＡＲ(他人受入)は本人と他人のデータの照合で一致と判定されることである。ＦＲＲとＦＡＲは相関関係にあり、片方の比率を上げるともう片方の比率が下がる。安全性を重視すると、ＦＡＲを小さくする必要があるが、その場合ＦＲＲが上がり、使い勝手に影響がでる。逆に利便性を重視するためにＦＲＲを下げると、ＦＡＲが上がってしまい、安全性が低下してしまう特徴がある。



アのＦＲＲとＦＡＲは相関関係にある。
イのＦＲＲを減少するとＦＡＲが増大する。
ウのＦＲＲを減少するとＦＡＲが増大する内容は適切である。求める答えはウとなる。
エのＦＲＲを増大するとＦＡＲは減少する。

例題演習

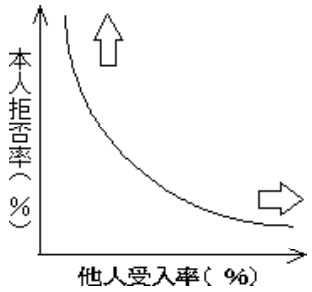
生体認証システムを導入するときに考慮すべき点として，最も適切なものはどれか。

ア　システムを誤作動させるデータを無害化する機能をもつライブラリを使用する。
イ　パターンファイルの頻繁な更新だけでなく，ヒューリスティックなど別の手段を組み合わせる。
ウ　本人のディジタル証明書を信頼できる第三者機関に発行してもらう。
エ　本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する。

解答解説

生体認証システムに関する問題である。

ＦＲＲ(本人拒否)は本人同士のデータの照合で不一致と判定されることことである。ＦＡＲ(他人受入)は本人と他人のデータの照合で一致と判定されることである。



ＦＲＲとＦＡＲは相関関係にあり、片方の比率を上げるともう片方の比率が下がる。安全性を重視すると、ＦＡＲを小さくする必要があるが、その場合ＦＲＲが上がり、使い勝手に影響がでる。逆に利便性を重視するためにＦＲＲを下げると、ＦＡＲが上がってしまい、安全性が低下してしまう特徴がある。

生体認証システムを導入する場合、本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する必要がある。求める答えはエとなる。

例題演習

バイオメトリクス認証には身体的特徴を抽出して認証する方式と行動的特徴を抽出して認証する方式がある。行動的特徴を用いているものはどれか。

ア　血管の分岐点の分岐角度や分岐点間の長さから特徴を抽出して認証する。
イ　署名するときの速度や筆圧から特徴を抽出して認証する。
ウ　どう孔から外側に向かって発生するカオス状のしわの特徴を抽出して認証する。
エ　隆線によって形作られる紋様からマニューシヤと呼ばれる特徴点を抽出して認証する。

解答解説

バイオメトリクス認証の問題である。

身体的特徴を利用しているのは、アの血管の分岐点の分岐角度や分岐点間の長さの特徴を用

いるもの、ウの瞳孔から外側に向かって発生するカオス状のしわの特徴を用いるもの、エの隆線によって形作られる紋様からマニューシャと呼ばれる特徴点を抽出して認証するものがある。

行動的特徴を用いるものには、署名するときの速度や筆圧から特徴を抽出して認証するものがある。求める答えはイとなる。

例題演習

ＳＳＬ／ＴＬＳを利用することによって実現できるものはどれか。

ア　クライアントサーバ間の通信の処理時間を短縮する。
イ　クライアントサーバ間の通信を暗号化する。
ウ　ブラウザとＷｅｂサーバの通信の証跡を確保する。
エ　メールソフトからＷｅｂサーバへのＳＭＴＰ接続を可能にする。

解答解説

ＳＳＬ／ＴＬＳに関する問題である。

ＳＳＬ／ＴＬＳはウェブブラウザとサーバ間の通信を暗号化して安全にデータをやり取りするプロトコルである。

クライアントサーバ間の通信を暗号化するが正しい答である。求める答はイとなる。

例題演習

ＨＴＴＰＳ(HTTP over SSL/TLS)の機能を用いて実現できるものはどれか。

ア　ＳＱＬインジエクションによるＷｅｂサーバへの攻撃を防ぐ。
イ　ＴＣＰポート８０番と４４３番以外の通信を遮断する。
ウ　Ｗｅｂサーバとブラウザの間の通信を暗号化する。
エ　Ｗｅｂサーバへの不正なアクセスをネットワーク層でのパケットフィルタリングによって制限する。

解答解説

ＨＴＴＰＳに関する問題である。

ＨＴＴＰＳは、ＳＳＬ／ＴＬＳプロトコルを用いて、サーバの認証、通信内容の暗号化、改竄検出などを行い、なりすましや盗聴などの攻撃を防ぐことができる。ＷｅｂブラウザとＷｅｂサーバの間の通信を暗号化して、盗聴や改竄を防ぐ。

アのＳＱＬインジェクションは、ＳＱＬ文を利用して、ＤＢの改ざんや不正に情報を入手することである。

イのＴＣＰポート８０は、ＨＴＴＰを利用してアプリケーションにデータを渡す場合に利用するポートで、ＨＴＴＰＳはそれ以外のデータ通信を遮断することではない。

ウのサーバとブラウザ間の通信の暗号化は適切な内容である。求める答えはウとなる。

エのパケットフィルタリングは、ネットワーク層型ファイアウォールの機能である。

例題演習

ＨＴＴＰＳを用いて実現できるものはどれか。

ア　Ｗｅｂサーバ上のファイルの改ざん検知
イ　クライアント上のウイルス検査
ウ　クライアントに対する侵入検知
エ　電子証明書によるサーバ認証

解答解説

ＨＴＴＰＳに関する問題である。

ＨＴＴＰＳは、ＳＳＬ／ＴＬＳプロトコルを用いて、サーバの認証、通信内容の暗号化、改竄検出などを行い、なりすましや盗聴などの攻撃を防ぐことができる。ＷｅｂブラウザとＷｅｂサーバの間の通信を暗号化して、盗聴や改竄を防ぐ。

アのサーバ上のファイルの改ざんの検知ではない。

イのウィルス検査の役割はない。

ウのクライアントへの侵入検知はしない。

エの電子証明書を用いてサーバ認証に使用する。求める答えはエとなる。

例題演習

１台のファイアウォールによって，外部セグメント，ＤＭＺ，内部ネットワークの三つのセグメントに分割されたネットワークがある。このネットワークにおいて，Ｗｅｂサーバと，重要なデータをもつＤＢサーバから成るシステムを使って，利用者向けのサービスをインターネットに公開する場合，インターネットからの不正アクセスから重要なデータを保護するためのサーバの設置方法のうち，最も適切なものはどれか。ここで，ファイアウォールでは，外部セグメントとＤＭＺ間及びＤＭＺと内部ネットワーク間の通信は特定のプロトコルだけを許可し，外部セグメントと内部ネットワーク間の通信は許可しないものとする。

ア　ＷｅｂサーバとＤＢサーバをＤＭＺに設置する。
イ　ＷｅｂサーバとＤＢサーバを内部ネットワークに設置する。
ウ　ＷｅｂサーバをＤＭＺに，ＤＢサーバを内部ネットワークに設置する。
エ　Ｗｅｂサーバを外部セグメントに，ＤＢサーバをＤＭＺに設置する。

解答解説

ＤＭＺを使用したサーバ設置法に関する問題である。

ＤＭＺは、インタネットなどの外部ネットワークと社内ネットワークの中間につくられるネットワーク上のセグメントで、外部ネットワークからも内部ネットワークからもファイアウォールなどによって隔離されている。社内ネットワークをインターネットに接続する際に、Ｗｅｂサーバやメールサーバなどインターネットに公開しなければならないサーバは、ＤＭＺセグメントに設置しセキュリティ強化を図ることができる。外部に公開するＷｅｂサーバは、常にリスクに晒されているため、Ｗｅｂサーバーを社内ネットワークに置くとリモートハッキング

やマルウェアなどを組み込まれたりした場合、社内ネットワークに接続されているその他のサーバやパソコンがすべて被害を受ける可能性がある。ＤＭＺ内に公開用のＷｅｂサーバを設置して、社内ネットワークと隔離することで、不正侵入された後のマルウェアの感染拡大を防ぐことができ、業務システムなどへの侵入による機密情報の漏洩を防止することが可能になる。

ＤＭＺの構成は、２台のファイアウォールを設置して、インターネット／ファイアウォール／ＤＭＺ／ファイアウォール／社内ネットワークとする方法がセキュリティ強度を高くすることになるが、ファイアウォール1台だけで構成する方法も可能で、１台のファイアウォールが外部セグメントとＤＭＺの間、およびＤＭＺと内部セグメントとの間を特定の通信プロトコルで通信許可の処理を行い対応する。

ＷｅｂサーバはＤＭＺに、データベースサーバは内部セグメントに設置する。求める答えはウとなる。

例題演習

ネットワークを通してデータ交換を行う場合，ユーザを認証する方法として，適切なものはどれか。

ア　受信データが改ざんされていないかどうかを調べる。
イ　送信データを暗号化する。
ウ　データを発信しているコンピュータを特定する。
エ　パスワードの一致を調べる。

解答解説

ユーザ認証に関する問題である。

アの受信データの改ざんの調査を行っても、ユーザ認証にはならない。

イの送信データの暗号化はデータの守秘は守れるが、ユーザ認証にはならない。

ウのデータを発信するコンピュータを特定しても、ユーザを特定することはできない。ユーザ認証にはならない。

エのパスワードはユーザ特有のものであり、ユーザ認証になる。求める答えはエとなる。

例題演習

画像などのディジタルコンテンツが，不正にコピーされて転売されたものであるかを判別できる対策はどれか。

ア　タイムスタンプ　　イ　電子透かし
ウ　電子保存　　エ　配達証明

解答解説

電子透かしに関する問題である。

アのタイムスタンプは、ファイルなどの電子データにおいて、その作成や更新などが行われた日時を示す情報である。

イの電子透かしは、音声や画像などの電子化されたコンテンツに対して、品質を落とさず利用者に分からない方法で著作権情報を記録する仕組みである。求める答えはイとなる。

ウの電子保存は、情報を電子媒体に保存することである。

エの配達証明は、一般書留とした郵便物や荷物を配達した事実を証明するサービスである。

例題演習

Ｗｅｂサーバのコンテンツの改ざんを検知する方法のうち，最も有効なものはどれか。

ア　Ｗｅｂサーバのコンテンツの各ファイルの更新日を保管しておき，定期的に各ファイルの更新日と比較する。

イ　Ｗｅｂサーバのコンテンツの各ファイルのハッシュ値を保管しておき，定期的に各ファイルから生成したハッシュ値と比較する。

ウ　Ｗｅｂサーバのメモリ使用率を定期的に確認し，バッファオーバフローが発生していないことを確認する。

エ　Ｗｅｂサーバへの通信を監視し，ＨＴＴＰ，ＨＴＴＰＳ以外の通信がないことを確認する。

解答解説

コンテンツの改ざんに関する問題である。

何らかの理由でファイルが破損していないか、オリジナルから変更されていないかをチェックする場合には、ファイルの「ハッシュ値」を比較する方法が広く使われている。フリーソフトウェアやシェアウェアでは、配布サイト上にＭＤ５やＳＨＡ１方式によるハッシュ値を掲載し、ダウンロード中にファイルが破損するなどの理由でオリジナルと違ってしまっていないかを確認できるようにしているサイトも多い。求める答えはイとなる。

例題演習

ファイアウォールのパケットフィルタリング機能に関する記述のうち,適切なものはどれか。

ア　インターネットから受け取ったパケットに改ざんがある場合は修正し，改ざんが修正できない場合には，ログを取って内部ネットワークへの通過を阻止する。

イ　インターネットから受け取ったパケットのヘッダ部分及びデータ部分に，改ざんがあるかどうかをチェックし，改ざんがあった場合にはそのパケットを除去する。

ウ　動的に割り振られたＴＣＰポート番号をもったパケットを，受信側で固定値のＴＣＰポート番号をもったパケットに変更して，内部ネットワークへの通過を許可する。

エ　特定のＴＣＰポート番号をもったパケットだけに，インターネットから内部ネットワークへの通過を許可する。

解答解説

ファイアウォールに関する問題である。

パケットフィルタリングは、送信元ＩＰアドレス／宛先ＩＰアドレス、送信元ポート番号／宛先ポート番号、接続を開始する方向性、プロトコルに基づき、転送パケットを通過させ

るかさせないかのアクセス制御を実現することである。パケットフィルタリングによって、あらかじめ設定されていない不正なパケットの流出入を防止する。ルータなどの経路情報を有する装置を利用する。

特定のＴＣＰポート番号をもったパケットだけに、インターネットから内部ネットワークへの通過を許可する。求める答えはエとなる。

例題演習

パケットフィルタリング型ファイアウォールがルール一覧に基づいてパケットを制御する場合，パケットＡに対する制御はどれか。ここで，ファイアウォールでは，ルール一覧に示す番号の１から順にルールの適用判断を行い，一つのルールが適用されたときには残りのルールは適用しない。

〔ルール一覧〕

番号	送信元アドレス	宛先アドレス	プロトコル	送信元ポート番号	宛先ポート番号	動作
1	10.1.2.3	*	*	*	*	通過禁止
2	*	10.2.3.*	TCP	*	25	通過許可
3	*	10.1.*	TCP	*	25	通過許可
4	*	*	*	*	*	通過禁止

注記　＊は任意のパターンを表す。

〔パケットA〕

送信元アドレス	宛先アドレス	プロトコル	送信元ポート番号	宛先ポート番号
10.1.2.3	10.2.3.4	TCP	2100	25

ア　番号１によって，通過を禁止する。
イ　番号２によって，通過を許可する。
ウ　番号３によって，通過を許可する。
エ　番号４によって，通過を禁止する。

解答解説

パケットフィルタリング型ファイアウォールに関する問題である。

ファイアウォールのルールは次のように適用される。

①　番号１で、送信元アドレスをチェックし、一致すれば通過禁止にする。

②　番号２で、宛先アドレス、プロトコル、宛先ポート番号をチェックし、一致すれば通過許可する。

③　番号３で、宛先アドレス、プロトコル、宛先ポート番号をチェックし、一致すれば通過許可する。

④　番号１～３で、ルールが適用されなかったものは、通過禁止にする。

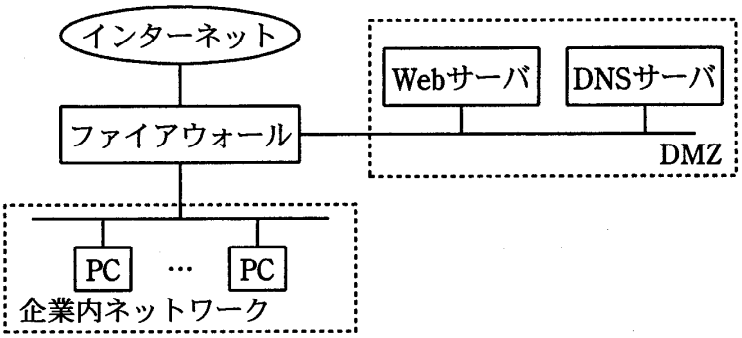
パケットＡは、ルール番号１の送信元アドレスで一致するため、番号１によって通過を禁止

する。求める答えはアとなる。

例題演習

図に示すネットワーク構成で，Ｗｅｂページの閲覧だけを社外に提供する。攻撃を防止するためにファイアウォールのＩＰパケットフィルタリングを設定する場合，フィルタリングルールでインターネットからＤＭＺへのパケットの通過を禁止できないプロトコルはどれか。

ア　ＦＴＰ
イ　ＨＴＴＰ
ウ　ＳＭＴＰ
エ　ＳＮＭＰ



解答解説

ＨＴＴＰプロトコルに関する問題である。

アのＦＴＰは、ファイル転送プロトコルである。ファイルを転送する場合、ユーザアカウントとパスワードを用いてユーザ認証を行い、認証後に転送を利用できる。

イのＨＴＴＰは、ＨＴＭＬで記述されたファイルを転送するプロトコルである。WWWクライアントとWWWサーバ間で、クライアントからのコンテンツ転送要求に応じて、サーバに格納されているＨＴＭＬファイル、画像、音声、動画像などのコンテンツを転送し、表示する。Ｗｅｂページの閲覧が目的であるからインターネットからの通過を禁止できない。

ウのＳＭＴＰは、インターネット上で電子メールを送信または転送するためのプロトコルである。ＴＣＰのポート番号２５を利用して行う。ユーザの確認、メールボックスの有無、容量の不足などをチェックしながら通信が行われる。

エのＳＮＭＰは、ＴＣＰ／ＩＰのネットワーク管理プロトコルで、ルータやハブなどのネットワーク機器のネットワーク管理情報を管理システムに送る場合の標準プロトコルである。ネットワーク情報の収集に必要なパケットのみを通過させる。

例題演習

ワームの検知方式の一つとして，検査対象のファイルからSHA-256を使ってハッシュ値を求め，既知のワーム検体ファイルのハッシュ値のデータベースと照合することによって，検知できるものはどれか。

ア　ワーム検体と同一のワーム
イ　ワーム検体と特徴あるコード列が同じワーム
ウ　ワーム検体とファイルサイズが同じワーム
エ　ワーム検体の亜種に当たるワーム

解答解説

ワームの検知方針に関する問題である。

ＳＨＡ-256とは、任意長の原文から固定長の特徴的な値であるハッシュ値を求める計算手順で、最長で２の64乗ビットまでの原文から、256ビットのハッシュ値を算出することができる。2001年に米国家安全保障局（NSA）が開発し、米国立標準技術研究所（NIST）がハッシュ関数の国家標準の一つとして採用した。SHA-224、SHA-256、SHA-384、SHA-512をまとめて「SHA-2」と通称することがある。

ワームの検知方式は、検知対象ファイルからＳＨＡ-256を使用してハッシュ値を求めたものとデータベース化されているワーム検体ファイルのハッシュ値を比較する方法である。従って、検出できるワームはワーム検体と同一のワームとなる。求める答えはアとなる。

例題演習

認証デバイスに関する記述のうち，適切なものはどれか。

ア　ＩＥＥＥ８０２．１Ｘでは，ディジタル証明書や利用者ＩＤ，パスワードを格納するＵＳＢキーは，２００ｋバイト以上のメモリを内蔵することを規定している。

イ　安定した大容量の電力を必要とする高度な処理には，接触型ＩＣカードよりも非接触型ＩＣカードの方が適している。

ウ　虹彩認証では，成人には虹彩の経年変化がないので，認証デバイスでのパターン更新がほとんど不要である。

エ　静電容量方式の指紋認証デバイスでは，ＬＥＤ照明を設置した室内において正常に認証できなくなる可能性がある。

解答解説

認証デバイスに関する問題である。

アのＩＥＥＥ８０２．１Ｘ(ＥＡＰ-ＴＬＳ)は、無線ＬＡＮなどで利用される認証プロトコルの１つである。ネットワークのセキュリティを高めるＥＡＰ(Extensible Authentication Protocol)に対応し、サーバ／クライアントの双方で電子証明書を利用する方式のためセキュリティが、より強化される。また、電子証明書の保管にＵＳＢ認証トークン、指紋認証トークンなどを用いることで、さらにセキュリティレベルを強化することができる。

イの確実な通信を行える接触型は主に、より堅牢なセキュリティが求められる決済や認証の分野で使われている。非接触型とは、カード内部にアンテナの役目を果たすコイルが内蔵されており、端末のリーダ／ライタから発生している磁界にカードをかざすと無線通信でデータのやりとりができる。鉄道改札や入退室管理など、より利便性を求められるジャンルで活用されている。

ウの虹彩認証は、眼球の黒目に現れる皺のパターンを識別して本人確認を行う認証方式であり、人体の特徴を利用するバイオメトリクス認証(生体認証)の一つである。カメラで眼の部分を撮影し、コンピュータで虹彩のパターンを抽出して認証する。非接触式であるため衛生的で、心理的抵抗が少ない。顔や声のように年をとっても変化することがなく、指紋のような偽造も難しい。認証率も高く、処理するデータ量も少なくて済むという。求める答えはウとなる。

エの静電容量方式の指紋認証デバイスはＬＥＤ照明の下でも正常に認証でき、活用されている。

例題演習

ＰＣへの侵入に成功したマルウェアがインターネット上の指令サーバと通信を行う場合に，宛先ポートとしてＴＣＰポート番号８０が多く使用される理由はどれか。

ア　ＤＮＳのゾーン転送に使用されるので，通信がファイアウォールで許可されている可能性が高い。
イ　ＷｅｂサイトのＨＴＴＰＳ通信での閲覧に使用されることから，侵入検知システムで検知される可能性が低い。
ウ　Ｗｅｂサイトの閲覧に使用されることから，通信がファイアウォールで許可されている可能性が高い。
エ　ドメイン名の名前解決に使用されるので，侵入検知システムで検知される可能性が低い。

解答解説

ＷｅｂサーバとのＨＴＴＰ通信に関する問題である。

ＨＴＴＰ通信では、ＴＣＰのポート番号８０を使用して、Ｗｅｂサーバとの通信を行う。ＰＣに侵入したマルウェアは、業務上のＷｅｂ閲覧と同じ条件でサーバへのアクセスを行い、侵入を図る。

アのＤＮＳサーバのポート番号は５３、イのＨＴＴＰＳは４４３、ウのＨＴＴＰは８０、エのドメイン名の名前解決に使用されるのはＵＤＰの５３である。求める答えはウとなる。

例題演習

ネットワーク障害の原因を調べるために，ミラーポートを用意して，ＬＡＮアナライザを使用できるようにしておくときに留意することはどれか。

ア　ＬＡＮアナライザがパケットを破棄してしまうので，測定中は測定対象外のコンピュータの利用を制限しておく必要がある。
イ　ＬＡＮアナライザはネットワークを通過するパケットを表示できるので，盗聴などに悪用されないように注意する必要がある。
ウ　障害発生に備えて，ネットワーク利用者に対してＬＡＮアナライザの保管場所と使用方法を周知しておく必要がある。
エ　測定に当たって，ＬＡＮケーブルを一時的に切断する必要があるので，ネットワーク利用者に対して測定日を事前に知らせておく必要がある。

解答解説

ＬＡＮアナライザに関する問題である。

ＬＡＮアナライザは、通信回線を流れるパケットを捕獲して中身を表示するソフトウェアやハードウェアの総称である。ネットワークを流れるデータの通信量やその変化を調べたり、障

害発生時に原因を調査するのに使われる。ＬＡＮアナライザには専用のハードウェアをネットワークに接続して解析するタイプの製品もあるが、多くの製品はソフトウェアで提供されており、コンピュータのネットワークカードが受信したパケットを解析する。ネットワークカードは、パケットの宛先などを読んで自分に関係がなければこれを破棄するが、プロミスキャスモードと呼ばれる特殊な設定にすることで、自分の属するセグメントを流れるすべてのパケットを受信することができる。ＬＡＮアナライザはこれを解析して、パケットの中身を表示したり各種の統計を取ったりすることができる。通信量を記録して時間帯や曜日による変化を表示したり、パケットの送信元や宛先、プロトコルの種類などによる統計を表示することができる。

ＬＡＮアナライザは通信内容を送信者や受信者に気付かれずに閲覧することができるため、暗号化されていないパスワードやクレジットカード番号など、秘密にしたい通信内容の盗聴に悪用される場合がある。外部からの侵入者がこっそりＬＡＮアナライザを仕掛けて、定期的に結果を報告させていたという事例もある。

ＬＡＮアナライザは、ネットワークを通過するパケットを表示できるので、盗聴などに悪用されないように注意する必要がある。求める答えはイとなる。

例題演習

ディジタル署名における署名鍵の用い方と，ディジタル署名を行う目的のうち，適切なものはどれか。

ア　受信者が署名鍵を使って，暗号文を元のメッセージに戻すことができるようにする。
イ　送信者が固定文字列を付加したメッセージを署名鍵を使って暗号化することによって，受信者がメッセージの改ざん部位を特定できるようにする。
ウ　送信者が署名鍵を使って署名を作成し，それをメッセージに付加することによって，受信者が送信者を確認できるようにする。
エ　送信者が署名鍵を使ってメッセージを暗号化することによって，メッセージの内容を関係者以外に分からないようにする。

解答解説

ディジタル署名に関する問題である。

デジタル署名は、個人認証システムと通信文の暗号化システムの組み合わせで実現するシステムである。送信側は送信元の秘密鍵を用いて署名を復号し、署名を含んだ通信文を受信先の公開鍵で暗号化し伝送する。受信側では、その通信文を受信側の秘密鍵で復号し平文を得て、送信元の公開鍵を用いて暗号化することによって送信者のデジタル署名を得ることができる。メッセージの受信者が、そのメッセージは正当な送信者が署名したものであり、途中で改変されていないことを確認できるシステムである。送信者はメッセージのデータに、秘密鍵で作成した署名データを付けて送信する。受信者は公開鍵を使って署名を確認する。

送信者が署名鍵を使って署名を作成し、それをメッセージに付加することによって、受信者が送信者を確認できるようになる。求める答えはウとなる。

アの署名鍵はメッセージダイジェストを暗号化するのに使用する。

イのメッセージダイジェクトの復号に使われるのは送信者の公開鍵であり、ディジタル署名

には改ざん部位を特定する機能はない。

エのディジタル署名はメッセージ本文の暗号化を目的としない。

例題演習

２要素認証に該当するものはどれか。

ア　２本の指の指紋で認証する。
イ　虹彩とパスワードで認証する。
ウ　異なる２種類の特殊文字を混ぜたパスワードで認証する。
エ　異なる二つのパスワードで認証する。

解答解説

２要素認証に関する問題である。

２要素認証は、ユーザが知っているもの（ID・パスワード）とユーザが持っているもの（複製できない、もしくは複製しづらい機器）を組み合わせてセキュリティレベルを高める方法である。２つの要素が揃っていないと認証を完了することができないため、たとえＩＤ・パスワードが漏えいしてしまっても、もう1つの要素がない限りはログインすることができない仕組みである。

アの２本の指の指紋は、ユーザがもっているものの組合せであり、不適である。

イの虹彩とパスワードは、ユーザがもっているものと知っているものの組合せであるから、２要素認識となる。求める答えはイとなる。

ウの２種類のパスワードは、ユーザが知っているものの組合せであり、不適である。

エの異なる２つのパスワードは、ユーザが知っているものの組合せであり、不適である。

例題演習

社員が利用するスマートフォンにディジタル証明書を導入しておくことによって，当該スマートフォンから社内システムへアクセスがあったときに，社内システム側で確認できるようになることはどれか。

ア　当該スマートフォンがウイルスに感染していないこと
イ　当該スマートフォンが社内システムへのアクセスを許可されたデバイスであること
ウ　当該スマートフォンのＯＳに最新のセキュリティパッチが適用済みであること
エ　当該スマートフォンのアプリケーションが最新であること

解答解説

スマートフォーンのディジタル証明書に関する問題である。

デジタル署名は個人認証システムと通信文の暗号化システムの組み合わせで実現するシステムである。送信側は送信元の秘密鍵を用いて署名を復号し、署名を含んだ通信文を受信先の公開鍵で暗号化し伝送する。受信側では、その通信文を受信側の秘密鍵で復号し平文を得て、送信元の公開鍵を用いて暗号化することによって送信者のデジタル署名を得ることができる。メ

ッセージの受信者が、そのメッセージは正当な送信者が署名したものであり、途中で改変されていないことを確認できるシステムである。

ディジタル証明書が導入されたスマートフォーンは社内システムへのアクセスが許可されたデハイスであること認証している。求める答えはイとなる。

例題演習

Ｗｅｂサーバの検査におけるポートスキャナの利用目的はどれか。

ア　Ｗｅｂサーバで稼働しているサービスを列挙して，不要なサービスが稼働していないことを確認する。

イ　Ｗｅｂサーバの利用者ＩＤの管理状況を運用者に確認して，情報セキュリティポリシとの相違を調べる。

ウ　Ｗｅｂサーバへのアクセス履歴を解析して，不正利用を検出する。

エ　正規の利用者ＩＤでログインし，Ｗｅｂサーバのコンテンツを直接確認して，コンテンツの脆弱性を検出する。

解答解説

ポートスキャナの利用目的に関する問題である。

ポートスキャンは攻撃の前段階の調査として行われるもので、当該コンピュータの各ポートへ接続開始を要請するデータを送り、どのような反応を返すかを確かめる。これにより、アクセスを受け付けているポートが何番か、どのようなソフトウェアが使用されているか、ソフトウェアの設定がどのようになっているかなどを外部からある程度知ることができ、攻撃に利用可能な設定の不備やソフトウェアの脆弱性などがないかを調べることができる。

ポートスキャンは攻撃者が攻撃対象に対して行う場合のほかに、コンピュータやネットワークの管理者などが自らが管理・運用するコンピュータにセキュリティ上の問題がないか調べるために実行することもある。従って、ポートスキャナーの利用目的は、使用したいポートが通信可能であること、あるいは、使用していないポートが通信不能であることをなどをネットワークの管理者が確認することであり、自分の管理するシステムに弱点がないかどうか調べるためにポートスキャナを利用する。

アはポートスキャナーによる検査、イは利用者ＩＤの管理状況の確認、ウはアクセスログの解析、エはＷｅｂアプリケーション脆弱性診断サービスである。求める答えはアとなる。

例題演習

ディジタルフォレンジックスでハッジュ値を利用する目的として，適切なものはどれか。

ア　一方向性関数によってパスワードを復元できないように変換して保存する。

イ　改変されたデータを，証拠となり得るように復元する。

ウ　証拠となり得るデータについて，原本と複製の同一性を証明する。

エ　パスワードの盗聴の有無を検証する。

解答解説

デジタルフォレンジックスに関する問題である。

デジタルフォレンジックは、犯罪捜査や法的紛争などで、コンピュータなどの電子機器に残る記録を収集・分析し、その法的な証拠性を明らかにする手段や技術のことである。

対象となるのはパソコンやサーバ、ネットワーク機器、携帯電話、情報家電など、デジタルデータを扱う機器全般である。事件の関係先の機器を押収して記憶装置から証拠となるデータを抽出したり、サーバや通信機器などに蓄積された通信記録から違法行為の証拠となる活動記録を割り出したり、破壊・消去された記憶装置を復元して証拠となるデータを割り出したりといった技術・活動が該当する。また、コピーや消去、改ざんが容易であるというデジタルデータの性質に対応して、データが捏造されたものかどうかを検証する技術や、記録の段階でデータが改ざんできないよう工夫したり、ハッシュ値やデジタル署名などで同一性を保全する技術なども含まれる。

不正アクセスや機密情報漏洩など、コンピュータや通信ネットワークに直接関係する犯罪における捜査手法として注目されたが、社会へのＩＴの普及・浸透に伴って、一般の刑事事件などでも捜査や立証に活用されるようになってきている。

ハッシュ関数は、長い文章やデータを固定長のビット列に圧縮する一方向性の関数で、圧縮された値をハッシュ値と呼ぶ。ハッシュ関数は一方向性のため、ハッシュ値から元のデータを復元することはできない。従って、ハッシュ値にディジタル署名を付して、本人性と文書の真正性の証明に利用したり、証拠の保全・開示に広く利用される。

アのパスワードをハッシュ値に変換する説明は、ハッシュ値の機能の説明であり、ディジタルフォレンジックスにハッシュ値を利用する目的ではない。

イは､ハッシュ関数は一方向性のためハッシュ値から元のデータを復元することはできない。

ウのディジタルフォレンジックスにハッシュ値を利用し、原本と複製の同一性の証明する内容は、ハッシュ値を利用する目的である。求める答えはウとなる。

エのハッシュ値に盗聴の有無を検知する仕組みはない。

例題演習

企業内ネットワークやサーバに侵入するために攻撃者が組み込むものはどれか。

ア　シンクライアントエージェント　　イ　ストリクトルーテイング
ウ　ディジタルフォレンジックス　　エ　バックドア

解答解説

バックドアに関する問題である。

バックドアは、クラッカーにより侵入を受けたサーバに設けられた、不正侵入を行なうための裏口である。クラッカーはコンピュータへの侵入に成功すると、次回も侵入できるように、管理者に気づかれないようこっそりと侵入経路を確保する。これがバックドアである。バックドアが設置されていると、管理者が不正侵入に気づいて侵入路をふさいでも、クラッカーは前回侵入時に設置したバックドアから再び不正侵入を行なうことができる。

アのシンクライアントエージェントは、シンクライアントからの要求に応じて、処理を代理

して行うサーバ側のコンピュータである。

イのストリクトルーティングは、ＲＦＣ２５４３の規則で動作するプロキシサーバである。

ウのディジタルフォレンジックスは、不正アクセスなどコンピュータに関する犯罪行われたときに、原因究明や法的な証拠性を明らかにするための手段や技術の総称である。

エのバックドアは、クラッカーにより侵入を受けたサーバに設けられた、不正侵入を行なうための裏口である。求める答えはエとなる。

例題演習

社内ネットワークとインターネットの接続点にパケットフィルタリング型ファイアウォールを設置して，社内ネットワーク上のＰＣからインターネット上のＷｅｂサーバの８０番ポートにアクセスできるようにするとき,フィルタリングで許可するルールの適切な組合せはどれか。

ア

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	80	1024 以上
Web サーバ	PC	80	1024 以上

イ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	80	1024 以上
Web サーバ	PC	1024 以上	80

ウ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	1024 以上	80
Web サーバ	PC	80	1024 以上

エ

送信元	宛先	送信元 ポート番号	宛先 ポート番号
PC	Web サーバ	1024 以上	80
Web サーバ	PC	1024 以上	80

解答解説

パケットフィルタリングに関する問題である。

通信を行う場合、通信前にポート番号を決める必要がある。通常、ポート番号はアプリケーションごとに標準で決められた番号があり、０～１０２３の番号が割り当てられている。イン

ターネット上のＷｅｂサーバと通信を行う場合はサーバ側のポート番号は８０を用いる。

この問題では、社内のＰＣからインターネット上のＷｅｂサーバにアクセスする場合であるから、Ｗｅｂサーバでのポート番号は８０、ＰＣのポート番号は１０２４以上を用いる。

ＰＣからの発信は、送信元はＰＣ、あて先はＷｅｂサーバ、送信元ポート番号１０２４以上、あて先ポート番号８０であり、サーバからの応答は、送信元はＷｅｂサーバ、あて先はＰＣ、送信元ポート番号８０、あて先ポート番号１０２４以上となる。求める答えはウとなる。

例題演習

Ｗｅｂシステムのパスワードを忘れたときの利用者認証において合い言葉を使用する場合，合い言葉が一致した後の処理のうち，セキュリティ上最も適切なものはどれか。

ア　あらかじめ登録された利用者のメールアドレス宛てに，現パスワードを送信する。

イ　あらかじめ登録された利用者のメールアドレス宛てに，パスワード再登録用ページへアクセスするための，推測困難なＵＲＬを送信する。

ウ　新たにメールアドレスを入力させ，そのメールアドレス宛てに，現パスワードを送信する。

エ　新たにメールアドレスを入力させ，そのメールアドレス宛てに，パスワード再登録用ページへアクセスするための，推測困難なＵＲＬを送信する。

解答解説

パスワードリマインダに関する問題である。

パスワードリマインダはユーザがパスワードを忘れた際の救済措置である。本人しか知らない秘密情報をユーザに登録してもらい、パスワード忘れの際には、その情報をユーザ認証の代用とすることで、パスワードを再発行する仕組みである。パスワードリマインダは、認証の機会が増えることでセキュリティが弱くなるため、できればパスワードリマインダを設けない方がよい。

パスワード再設定/再発行手順

パスワードリマインダの「合言葉」が一致したら、パスワード再設定に次の手順を踏むことが推奨されている。

① パスワードリマインダのＷｅｂページ上で１回限り有効なキーをユーザに発行する。

② １回限り有効な別のキーを含むＵＲＬを、ユーザがあらかじめ登録している電子メールアドレス宛送信する。

③ ユーザにそのＵＲＬのＷｅｂページにアクセスしてもらい、先ほどのキーを入力してもらう。

④ キーが照合できたらパスワードの再設定あるいは再発行を行う。

⑤ 一定回数以上照合に失敗したら２つのキーは無効にする。

アの場合、暗号化されていないと盗聴されてパスワードが盗まれる。

イの場合の一時的なパスワード再設定ページへのＵＲＬを送るのが安全な方法であり、キーが照合できたらパスワードの再設定あるいは再発行を行う。求める答えはイとなる。

ウ、エの場合、攻撃者が任意のメールアドレスを指定できてしまうため危険である。

例題演習

公開鍵暗号を利用した電子商取引において，認証局（ＣＡ）の役割はどれか。

ア　取引当事者間で共有する秘密鍵を管理する。
イ　取引当事者の公開鍵に対するディジタル証明書を発行する。
ウ　取引当事者のディジタル署名を管理する。
エ　取引当事者のパスワードを管理する。

解答解説

認証局の役割に関する問題である。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。

取引当事者の公開鍵に対するディジタル証明書を発行する。求める答えはイとなる。

例題演習

サーバにバックドアを作り，サーバ内での侵入の痕跡を隠蔽するなどの機能をもつ不正なプログラムやツールのパッケージはどれか。

ア　ＲＦＩＤ　　イ　rootkit
ウ　ＴＲＩＰ　　エ　webbeacon

解答解説

rootkitに関する問題である。

rootkitは、クラッカーが遠隔地のコンピュータに不正に侵入した後に利用するソフトウェアをまとめたパッケージである。セキュリティホールなどを利用して他人のコンピュータに不正侵入を行った攻撃者は、侵入を隠蔽するためのログの改ざんツール、侵入口が塞がれても再び侵入できるようにする裏口（バックドア）ツール、侵入に気付かれないための改ざんされたシステムコマンド群などをインストールする。これらを素早く導入するため、一連のソフトを使いやすいパッケージにまとめたものがrootkitで、いくつかの種類がある。これらのソフトのほかにも、ネットワークを盗聴するスニッファツールや、侵入したコンピュータを踏み台にして他のコンピュータを攻撃するための攻撃ツールなどがパッケージされたものもある。

サーバにバックドアを作り，サーバ内で侵入の痕跡を隠蔽するなどの機能がパッケージ化された不正なプログラムやツールはrootkitである。求める答えはイとなる。

アのＲＦＩＤは、微小な無線チップにより人やモノを識別・管理する仕組みである。

ウのＴＫＩＰは、無線ＬＡＮの暗号化に用いられるＷＰＡで採用された暗号化方式である。

エのweb beaconは、Webページに埋め込まれた情報収集用の極めて小さい画像のことである。

例題演習

ＰＫＩにおける認証局が，信頼できる第三者機関として果たす役割はどれか。

ア　利用者からの要求に対して正確な時刻を返答し，時刻合わせを可能にする。
イ　利用者から要求された電子メールの本文に対して，ディジタル署名を付与する。
ウ　利用者やサーバの公開鍵を証明するディジタル証明書を発行する。
エ　利用者やサーバの秘密鍵を証明するディジタル証明書を発行する。

解答解説

認証局の役割に関する問題である。

認証局は公開鍵とその所有者を対応づけるために電子証明書を発行する機関である。認証局では、各ユーザからの電子証明書の発行依頼を受けると、そのユーザの本人確認を行った後に、正しいユーザである場合にのみ電子証明書を発行する。電子証明書には所有者の識別情報や公開鍵などが記載されている。

認証局の主な役割には次のものがある。

①　申請者の公開鍵にディジタル署名を付したディジタル証明書を発行する
②　ＣＲＬ(証明書失効リスト)を発行する
③　ＣＰＳ(認証局運用規定)を公開する
④　ディジタル証明書を検証するための認証局の公開鍵を公開する
⑤　認証局の秘密鍵を厳重に管理する

ウの利用者やサーバの公開鍵を証明するディジタル証明書を発行する。求める答えはウとなる。

アはＮＴＰ、イ、エは公開鍵を証明するディジタル証明である。

例題演習

ＷＡＦの説明はどれか。

ア　Ｗｅｂサイトに対するアクセス内容を監視し，攻撃とみなされるパターンを検知したときに当該アクセスを遮断する。
イ　Ｗｉ-Ｆｉアライアンスが認定した無線ＬＡＮの暗号化方式の規格であり，ＡＥＳ暗号に対応している。
ウ　様々なシステムの動作ログを一元的に蓄積，管理し，セキュリティ上の脅威となる事象をいち早く検知，分析する。
エ　ファイアウォール機能を有し，ウイルス対策，侵入検知などを連携させ，複数のセキュリティ機能を統合的に管理する。

解答解説

ＷＡＦに関する問題である。

ＷＡＦは、外部ネットワークからの不正アクセスを防ぐためのソフトウェアあるいはハードウェアであるファイアウォールの中でも、Ｗｅｂアプリケーションのやり取りを把握・管理す

ることによって不正侵入を防御することのできるファイアウォールである。

ＷＡＦの特徴は、従来のファイアウォールがネットワークレベルで管理していたことに対して、アプリケーションのレベルで管理を行う。プログラムに渡される入力内容などを直接に検査することによって、不正と見なされたアクセス要求を遮断するという仕組みが採用されている。クライアントの操作するＷｅｂブラウザとＷｅｂサーバを仲介するかたちで存在し、ブラウザとの直接的なやり取りをＷＡＦが受け持つ。ＳＱＬインジェクションやクロスサイトスクリプティング、強制ブラウジングといった要求に対して、「攻撃」と見なして拒絶することができる。

アはＷＡＦ、イはＷＰＡ２、ウは総合ログ管理システム、エはＵＴＭである。求める答えはアとなる。

例題演習

攻撃者が用意したサーバＸのＩＰアドレスが，Ａ社ＷｅｂサーバのＦＱＤＮに対応するＩＰアドレスとして，Ｂ社ＤＮＳキャッシュサーバに記憶された。この攻撃によって，意図せずサーバＸに誘導されてしまう利用者はどれか。ここで，Ａ社，Ｂ社の各従業員は自社のＤＮＳキャッシュサーバを利用して名前解決を行う。

ア　Ａ社ＷｅｂサーバにアクセスしようとするＡ社従業員
イ　Ａ社ＷｅｂサーバにアクセスしようとするＢ社従業員
ウ　Ｂ社ＷｅｂサーバにアクセスしようとするＡ社従業員
エ　Ｂ社ＷｅｂサーバにアクセスしようとするＢ社従業員

解答解説

ＤＮＳキャッシュポイズニングに関する問題である。

ＤＮＳキャッシュポイズニングは、ＤＮＳがＷｅｂへのアクセスやメールの送受信などの際に、接続相手のＩＰアドレスを調べたりする仕組みに対して、ＤＮＳが偽の応答を返すようにしてしまう攻撃手法である。インターネットの利用者が、この攻撃により偽の応答をするようにされたＤＮＳを介してＷｅｂにアクセスすると、気づかないうちにフィッシングサイトに誘導されてしまう。

ＤＮＳキャッシュサーバは、利用者からの任意のドメイン名の名前解決の問い合わせを受け付け、当該ドメイン名を管理するＤＮＳサーバへの問い合わせを代理で行い、結果を利用者に返答するコンピュータやソフトウェアである。この問題の仕組みではＡ、Ｂ各社の従業員は自社のＤＮＳキャッシュサーバを利用して名前解決を行う。

攻撃者はＡ社のＷｅｂサーバのドメイン名に対応するＩＰアドレスをＢ社のＤＮＳキャッシュサーバに記憶させたので、Ｂ社のＤＮＳキャッシュサーバにアクセスし、Ａ社のＩＰアドレスを得ようとする従業員が偽アドレスに誘導されることになる。Ｂ社のＤＮＳキャッシュサーバにアクセスするのはＢ社の従業員である。従って、Ａ社Ｗｅｂサーバにアクセスしようとするイ社の従業がサーバＸに誘導される。求める答えはイとなる。

例題演習

情報セキュリティにおけるタイムスタンプサービスの説明はどれか。

ア　公式の記録において使われる全世界共通の日時情報を，暗号化通信を用いて安全に表示するＷｅｂサービス
イ　指紋，声紋，静脈パターン，網膜，虹彩などの生体情報を，認証システムに登録した日時を用いて認証するサービス
ウ　電子データが，ある日時に確かに存在していたこと，及びその日時以降に改ざんされていないことを証明するサービス
エ　ネットワーク上のＰＣやサーバの時計を合わせるための日時情報を途中で改ざんされないように通知するサービス

解答解説

タイムスタンプサービスに関する問題である。

タイムスタンプは、タイムスタンプに刻印されている時刻以前にその電子文書が存在していたこと（存在証明）と、その時刻以降、当該文書が改ざんされていないこと（非改ざん証明）を証明するものである。

アは標準時配信サービス、イはバイオメトリックス認証、ウはタイムスタンプサービス、エはＮＴＰである。求める答えはウとなる。

例題演習

攻撃者がシステムに侵入するときにポートスキャンを行う目的はどれか。

ア　後処理の段階において，システムログに攻撃の痕跡が残っていないかどうかを調査する。
イ　権限取得の段階において，権限を奪取できそうなアカウントがあるかどうかを調査する。
ウ　事前調査の段階において，攻撃できそうなサービスがあるかどうかを調査する。
エ　不正実行の段階において，攻撃者にとって有益な利用者情報があるかどうかを調査する。

解答解説

ポストスキャンに関する問題である。

ポートスキャンは攻撃の前段階の調査として行われるもので、当該コンピュータの各ポートへ接続開始を要請するデータを送り、どのような反応を返すかを確かめる。これにより、アクセスを受け付けているポートが何番か、どのようなソフトウェアが使用されているか、ソフトウェアの設定がどのようになっているかなどを外部からある程度知ることができ、攻撃に利用可能な設定の不備やソフトウェアの脆弱性などがないかを調べることができる。ポートスキャンは攻撃者が攻撃対象に対して行う場合のほかに、コンピュータやネットワークの管理者などが自らが管理・運用するコンピュータにセキュリティ上の問題がないか調べるために実行することもある。

事前調査の段階において、攻撃できそうなサービスがあるかどうかを調査することである。求める答えはウとなる。

アの後処理段階、イの権限取得段階、エの不正実行段階は適切でない。

例題演習

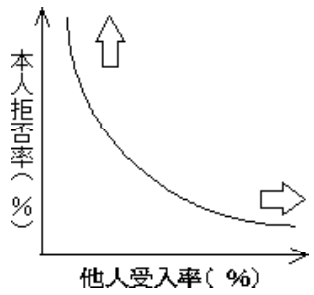
生体認証システムを導入するときに考慮すべき点として，最も適切なものはどれか。

ア　本人のディジタル証明書を，信頼できる第三者機関に発行してもらう。
イ　本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する。
ウ　マルウェア定義ファイルの更新が頻繁な製品を利用することによって，本人を誤って拒否する確率の低下を防ぐ。
エ　容易に推測できないような知識量と本人が覚えられる知識量とのバランスが，認証に必要な知識量の設定として重要となる。

解答解説

生体認証システムに関する問題である。

ＦＲＲ(本人拒否)は本人同士のデータの照合で不一致と判定されることことである。ＦＡＲ(他人受入)は本人と他人のデータの照合で一致と判定されることである。



ＦＲＲとＦＡＲは相関関係にあり、片方の比率を上げるともう片方の比率が下がる。安全性を重視すると、ＦＡＲを小さくする必要があるが、その場合ＦＲＲが上がり、使い勝手に影響がでる。逆に利便性を重視するためにＦＲＲを下げると、ＦＡＲが上がってしまい、安全性が低下してしまう特徴がある。

生体認証システムを導入する場合、本人を誤って拒否する確率と他人を誤って許可する確率の双方を勘案して装置を調整する必要がある。求める答えはイとなる。

例題演習

ＣＳＩＲＴの説明として，適切なものはどれか。

ア　ＩＰアドレスの割当て方針の決定，ＤＮＳルートサーバの運用監視，ＤＮＳ管理に関する調整などを世界規模で行う組織である。
イ　インターネットに関する技術文書を作成し，標準化のための検討を行う組織である。
ウ　企業内・組織内や政府機関に設置され，情報セキュリティインシデントに関する報告を受け取り，調査し，対応活動を行う組織の総称である。
エ　情報技術を利用し，宗教的又は政治的な目標を達成するという目的をもつ者や組織の総称である。

解答解説

ＣＳＩＲＴに関する問題である。

ＣＳＩＲＴ(シーサート)は、コンピュータセキュリティにかかるインシデントに対処するた

めの組織の総称で、インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をしいる。シーサートの活動は、目的、立場、活動範囲、法的規制などの違いからそれぞれ独自で活動を行ってきた。 しかし、コンピュータセキュリティインシデントの攻撃が巧妙かつ複雑になり、迅速な対応には、単独のシーサートでは困難な状況になってきている。日本国内の企業事情を巧みに利用した攻撃手法などによるコンピュータセキュリティインシデントや、対応ノウハウの蓄積が難しい標的型攻撃などの存在があり、インターネットの発達、ビジネスにおけるＩＴへの依存度の高まりから、コンピュータセキュリティインシデントの発生リスクも大幅に高まり、攻撃が単なる愉快犯から、経済的利益を目的とした犯行へと移り変わっており、その手法も高度化、複雑化し、問題の把握がより難しくなる傾向にある。これらに適切に対処するためには、同じような状況や課題を持つシーサート同士による緊密な連携と、インシデント関連情報、脆弱性情報、攻撃予兆情報などを互いに収集し、積極的に共有する必要があり、互いに協調し、高いレベルでの緊密な連携体制の実現を目指し、共通の問題を解決する場を設けることを目的とした日本シーサート協議会が設立された。

アはＩＣＡＮＮ、イはＩＥＴＦ、ウはＣＳＩＲＴ、エはハクティビストである。求める答えはウとなる。

例題演習

社内ネットワークとインターネットの接続点に，ステートフルインスペクション機能をもたない，静的なパケットフィルタリング型のファイアウォールを設置している。このネットワーク構成において，社内のＰＣからインターネット上のＳＭＴＰサーバに電子メールを送信できるようにするとき，ファイアウォールで通過を許可するＴＣＰパケットのポート番号の組合せはどれか。ここで，ＳＭＴＰ通信には，デフォルトのポート番号を使うものとする。

	送信元	宛先	送信元 ポート番号	宛先 ポート番号
ア	PC	SMTP サーバ	25	1024 以上
	SMTP サーバ	PC	1024 以上	25
イ	PC	SMTP サーバ	110	1024 以上
	SMTP サーバ	PC	1024 以上	110
ウ	PC	SMTP サーバ	1024 以上	25
	SMTP サーバ	PC	25	1024 以上
エ	PC	SMTP サーバ	1024 以上	110
	SMTP サーバ	PC	110	1024 以上

解答解説

パケットフィルタリングに関する問題である。

通信を行う場合、通信前にポート番号を決める必要がある。通常、ポート番号はアプリケーションごとに標準で決められた番号があり、０～１０２３の番号が割り当てられている。インターネット上のＳＭＴＰサーバと通信を行う場合はサーバ側のポート番号は２５を用いる。

この問題では、社内のＰＣからインターネット上のＳＭＴＰサーバにアクセスする場合であるから、ＳＭＴＰサーバでのポート番号は２５、ＰＣのポート番号は１０２４以上を用いる。

ＰＣからの発信は、送信元はＰＣ、あて先はＳＭＴＰサーバ、送信元ポート番号１０２４以上、あて先ポート番号２５であり、サーバからの応答は、送信元はＳＭＴＰサーバ、あて先はＰＣ、送信元ポート番号２５、あて先ポート番号１０２４以上となる。求める答えはウとなる。