txt030412　ＩＳＭＳ

①　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

②　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。

③　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

④　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。

㋓　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

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

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。

ＰＤＣＡは業務の改善工程において、計画－実施－確認－対応策の４つのフェーズを繰り返し実行し、業務改善を進めていく方法である。

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

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

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

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

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

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。