txt030411 情報セキュリティ

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、リスクヘッジと緊急事態計画がある。

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。

ⓑ　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。

④　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。

㊓　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。

㊔　復旧処理の手順をマニュアル化しておく。

⑤　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。

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

セキュリティ方針に関する問題である。

アは、企業毎に独自の考え方や取り組み方を設定することが重要である。

イは、システム管理者が設定し、全従業員に徹底させる必要がある。

ウの企業の考え方や取り組み方を明文化する内容が適切である。求める答えはウとなる。

エのファイアウォールは内部と外部のネットワークの関所で、設定時にセキュリティ方針の考えを利用する。セキュリティ方針は組織の活動の仕組みを記述したものである。

例題演習

情報システムのセキュリティを考えるときに，インテグリティ(integrity)，機密性(confidentiality)とともに考慮すべき要素の一つであり，情報システムを，定められた方法でいつでも利用できることを意味するものはどれか。

ア　安全性　　イ　一貫性　　ウ　可用性　　エ　信頼性

解答解説

セキュリティの可用性に関する問題である。

アの安全性は、自然災害、不正アクセスや破壊行為からシステムを保護することである。

イの一貫性は、データ入力やデータの内容、プログラムロジックが正確性、完結性を維持していることである。

ウの可用性は、資格を与えられたユーザが情報システムを適時に使用することの保障である。情報システムを定められた方法でいつでも利用できることを意味する。求める答えはウとなる。

エの信頼性は、システムの品質を高め、エラーや事故の発生を未然に防止し、発生時には最小限にくい止め、迅速に回復することができることである。

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

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

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

災害を想定した事業継続計画(ＢＣＰ)を策定する場合に行う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　許容される最大停止時間を決定する。

ウ　代替手順や復旧手順について関係者を集めて教育する。

エ　内外の環境の変化を踏まえＢＣＰの内容を見直す。

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、ウは復旧手順の関係者への教育、エはＢＣＰの内容の見直しで

ある。求める答えはイとなる。

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。

リスク特定はリスクを発見し、認識し、記述するプロセス、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、リスク評価は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である。予測されるリスクの可能性と予測値と、許容されるリスクの可能性と許容値を比較し、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。

リスク管理は、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。

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

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、リスクの発生時の責任を契約書などで他社に転嫁するために、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。

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

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。

アの発生の可能性があるリスク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ことはリスク分析の作業である。求める答えはアとなる。

イのリスクは人間の欲望の変化や技術の変化、産業組織の変化などによって絶えず変動するため、リスク対策が完了しないうちにも、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。

予測されるリスクの可能性と予測値と、許容されるリスクの可能性と許容値を比較し、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意思決定を行い、施策を実施し、安全な状態を実現するプロセスをとる。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。