4/16 配布プリント： 第１章　要点

- 1.1.1　情報技術への依存の高まり
  - ○ 問　：2018年の時点でインターネットの利用者数はどの程度か。
  - ○ 回答：39億人

  - ○ 問　：2025年には、インターネットに接続されるデバイス数は何台になると予想されているか。
  - ○ 回答：416億台

- 1.1.2　情報セキュリティの考え方
  - ○ 問　：セキュリティにおける「非対称な関係性」とはどのようなものか。
  - ○ 回答：守り手はあらゆる攻撃手段を考慮し守る必要があるのに対し，攻撃者は攻撃可能な脆弱性を1つ見つければその目的を達成できるため，守り手側の負担が大きくなり，不利であること．

  - ○ 問　：p.4の「アタックサーフェス」とはどのような意味か。また、図1.8の例のアタックサーフェスの要素となるものを列挙せよ。
  - ○ 回答：アタックサーフェスとは，攻撃対象となる脆弱性が存在しうる領域のことで，例としてはあげられる．

- 1.1.3　情報セキュリティの定義
  - ○ 問　：情報セキュリティのCIAを意味する3要素の名称を挙げ、それぞれの意味を1〜2行で概説せよ。
  - ○ 回答：
    機密性（Confidentiality）： 許可されたユーザーのみが情報にアクセスできるようにし，情報の漏洩を防ぐこと．
    完全性（Integrity）： 情報が正確であり，許可されていない変更や破損がない状態を維持すること．
    可用性（Availability）： 必要なときに情報やシステムへアクセスできる状態を確保すること．

- 1.1.4　情報セキュリティの分類
  - ○ 問　：物理的セキュリティとはどのような概念か概説せよ。
  - ○ 回答：おもに建物や設備などを対象としたセキュリティのこと．防災，防犯，電源，データバックアップ，通信回線などの，ITインフラ周りのセキュリティが対象となる．また，環境的セキュリティとも呼ばれる．

  - ○ 問　：人的セキュリティとはどのような概念か概説せよ。
  - ○ 回答：人的管理に関するセキュリティのこと．人的セキュリティまたは，組織的セキュリティともよばれる．情報セキュリティポリシーの「策定・運用・チェック・見直し」といった，組織運営におけるITシステムの運用上で必要なセキュリティを指す．

  - ○ 問　：技術的セキュリティとはどのような概念か概説せよ。
  - ○ 回答：おもにITシステムに関するセキュリティのことで，論理セキュリティやシステムセキュリティとも呼ばれる．さらに，ネットワークセキュリティやホストセキュリティに分類することができ，技術的セキュリティは暗号化技術，認証技術，アクセス制御技術などから構成される．

  - ○ 問　：CSIRTとはどのようなものか概説せよ。
  - ○ 回答：Computer Security Incident Response．シーサートとよみ，コンピュータセキュリティに関する事故に対応するチームの事．

- 1.1.5　脅威とリスクについて

○ 問　：次の表を完成させよ。
○ 回答：

脅威の種類	脅かされる性質	内容例
情報漏洩	**機密性**	機密情報が外部に漏れてしまった。
マルウェア感染	**機密性・完全性**	コンピュータウイルスに感染してしまった。
破壊	完全性・可用性	データが破壊されて利用できなくなった。
不正アクセス	機密性・完全性	システムに不正に侵入されてしまった.
サービス停止	可用性	操作ミスでシステムが停止してしまった。
改ざん	完全性	データベースが不正に変更されてしまった.

-

○ 問　：リスク評価とはどのような概念か概説せよ。
○ 回答：リスクの大きさが受容可能か，または許容可能かを決定するために，リスク分析の結果をリスク基準と比較するプロセス.

○ 問　：リスクアセスメントとはどのような概念か概説せよ。
○ 回答：リスク特定，リスク分析，およびリスク評価のプロセス全体.

- 1.1.6　情報セキュリティにおけるリスクの例
  ○ 問　：「委託先任せ」はどのようなリスクを生じさせるか概説せよ。
  ○ 回答：構築・運用を外部に委託している自社のシステムにおいて，任せっぱなしにしているとなにかインシデントが生じた際に，委託しているとはいえ自社のシステムでインシデントが生じている以上「知らなかった」では済まされず，責任が問われるリスクが生じる.

  ○ 問　：「アクセス制御不備」はどのようなリスクを生じさせるか概説せよ。
  ○ 回答：簡単にシステム構成を変更することができるクラウドサービスなどにおいては，アクセス制御の設定も簡単に変更できてしまうため，本来は公開されるべきではない情報が公開されてしまうリスクが生じる.

  ○ 問　：「OSS」とはどのような意味か概説せよ。
  ○ 回答："OpenSourceSoftware"の略でアプリケーションのソースコードを公開しているソフトウェアのこと．複製・改変・再頒布を認めているものの，著作権は放棄していないことがあるため注意が必要.

  ○ 問　：「バックドア」とはどのようなものか概説せよ。
  ○ 回答：システムの正規アクセスの認証を不正にバイパスし，任意のタイミングで対象システムに不正侵入できる経路のこと.

  ○ 問　：「情報の持ち出し」にはどのようなリスクがあるか概説せよ。
  ○ 回答：企業側で十分な管理をせずにリモートワークや業務委託を行ってしまうと，社外秘情報が外部に漏洩するリスクがある.

- 1.1.7　セキュリティ対策の基本的な考え方
  ○ 問　：リスクへの対処方法を4つ挙げよ。
  ○ 回答：リスクの低減・リスクの保有・リスクの回避・リスクの移転

- ○ 問　：上記の4つの対処方法について、リスクの発生可能性が高い場合に採用すべき方法から発声可能性の低い場合に採用すべき方法の順に列挙せよ。ただし一部同順になってよい。
- ○ 回答：リスクの回避，リスクの低減，リスクの保有・リスクの移転

- ○ 問　：リスクへの対応策として「回復」「検知」「予防」「抑止」があるとき、対応すべき順番に沿って並び替えよ。
- ○ 回答：予防，抑止，検知，回復

- ○ 問　： Attributionとはどのような概念か概説せよ。
- ○ 回答：サイバー攻撃を実施した攻撃者の帰属を特定すること．

- 1.1.8　セキュリティ対策の標準・ガイドライン
  - ○ 問　：ISO/IEC27001は国際規格か。
  - ○ 回答：○

  - ○ 問　：JIS Q 27001は国際規格か。
  - ○ 回答：×

  - ○ 問　：CISOとはどのような役職か。
  - ○ 回答：情報セキュリティ管理最高責任者．企業の経営理念や経営方針を反映し，企業活動におけるITシステムのセキュリティ対策を行うほか，セキュリティ関連規定の策定などセキュリティに関する事柄を幅広く統括する．

- 1.1.9　インシデントレスポンス
  - ○ 問　：インシデントとはどのような概念か概説せよ。
  - ○ 回答：システム運用や情報資産管理において，セキュリティに関連する事故・事象．

  - ○ インシデントレスポンスの典型的な対応の4段階をそれぞれ概説せよ。
  - ○ 回答：
    準備：インシデントに対応するチームを設置しツール等リソースの用意を行ったり，リスク評価・管理策を実施しインシデント発生の確立を低減する．
    検知と分析：インシデントを検知して保護対象組織に警告し，攻撃・漏洩の分析を行い対処法を検討・文書化する
    封じ込め・根絶・復旧：インシデント発生時のインパクトを推定し被害拡大の封じ込めを行い最終的な復旧をめざす．
    インシデント後の対応：適切にインシデントを処理したのち，報告書を作成し事件の原因・被害，将来事件を防止するために行うべき対策を詳細に記録する．

- 1.2.1　脆弱性とは
  - ○ 問　：脆弱性とはどのような概念か概説せよ。
  - ○ 回答：1つ以上の脅威によって付け込まれる可能性のある資産または管理策の弱点．

  - ○ 問　：エクスプロイトコードとはどのようなものか概説せよ。
  - ○ 回答：コンピューターウイルスに感染した際に，攻撃者が脆弱性を悪用してシステムの制御を奪うことや，権限を取得することなどの機能をコード化したもの．ウイルスの機能の一部であるペイロード部を実行させる役割がある．

  - ○ 問　：脆弱性と露出の違いを概説せよ。
  - ○ 回答：脆弱性は攻撃に直結するが，露出は被害につながる欠陥であり攻撃には直結しない．

- 1.2.2　脆弱性情報データベース

- ○ 問　：JVNとはなにか概説せよ。
- ○ 回答：JPCERT/CCとIPAが共同で管理する脆弱性情報データベース.

- 1.2.3　NVDに関連する用語
  - ○ 問　：CVEとは何か概説せよ。
  - ○ 回答：CVE識別子を用いてソフトウェアにおける脆弱性を識別するシステム

  - ○ 問　：CVEの例として、「CVE-2024-26023」はどのような脆弱性か、web検索して回答せよ。
  - ○ 回答：CVE-2024-26023 は BUFFALO 製無線 LAN ルータの管理 Web インタフェースに存在する OS コマンドインジェクションであり，ログイン済みの攻撃者が任意の OS コマンドを実行できる脆弱性.

  - ○ 問　：CVSSとは何か概説せよ。
  - ○ 回答：脆弱性の深刻度や影響度合いを評価するスコアシステム.

- 1.2.4　ゼロデイ攻撃
  - ○ 問：　ゼロデイ攻撃とは何か概説せよ。
  - ○ 回答：脆弱性が発見され修正プログラムが提供されるより前に，攻撃者がその脆弱性を独自に入手し悪用する攻撃.

- 1.4　情報セキュリティの変遷
  - ○ 問　：セキュリティを脅かす攻撃者の種類が歴史を経てどのように増えたか概説せよ。
  - ○ 回答：1990年まではインターネットは一般的ではなくインシデントも愉快犯やいたずらのレベルだったが，1990年から2009年にかけてはインターネットの商業利用が始まり，金銭的損失を伴う犯罪や現代に通じるインシデントも増えた．また2010年以降は国家や非国家組織の利益増大のため，情報技術を用いた行為が散見されるようになり，犯罪行為に加え，よりインパクトの大きい国家的・組織的な攻撃が行われるようになった.

  - ○ 問　：ワームとはどのようなマルウェアか概説せよ。
  - ○ 回答：ネットワークを介して，自己複製ながら拡散するマルウェア．脆弱性をついたり，共有サービスを悪用して次々にほかの機器へコピーされていく．ワームの例としてはCodeRed,Nimdaなどがある.

  - ○ 問　：ボットネット、C&Cサーバ、DDoS攻撃の3つの用語を使い、それぞれの関係性を説明する文を作れ。
  - ○ 回答：攻撃者はC&Cサーバからボットネットに一斉攻撃の指令を送信し，DDoS攻撃を実現する.

  - ○ 問　：Stuxnetとは、どこを狙ったもので、どのような感染経路を使っていたか概説せよ。
  - ○ 回答：Stuxnetは核開発を強行していたとされるイランの核施設の遠心分離機を狙ったもので，ネットワーク経由だけでなく感染したPCに接続したUSBメモリ経由でも感染し拡散するようになっていた.