SC：０１_情報セキュリティ

- 前提知識
  - AF、ES、OR、NW を参照ください
- 情報セキュリティとは
  - 目的と考え
    - 組織の規模が決定できる、組織のISMSの確立及び実施は、その組織のニーズ及び目的、セキュリティ要求事項、組織が いたっているプロセス、並びに組織の規模及び構造 によって影響を受ける
    - 要は「組織の規模によって決定され、組織の目 的によって変わる」
  - 定義
    - JIS Q 27000：情報の機密性、安全性及び可用性を維持する
    - 機密性：Confidentiality
      - 認可されていない個人、エンティティ及びプロセスに対して、情報を開示する、または、開示しない特性
      - 秘匿性、無認知
    - 完全性：Integrity：インテグリティ
      - 正確さ及び安全の特性
      - 改ざん防止、検証情報を書き換えられないようにする
    - 可用性：Availability
      - 認可されたエンティティが要求した時に、アクセス及び使用が可能である特性
      - こ最初、情報をいつでも見られるようにすること。
    - 真正性：Authenticity
      - エンティティは、それが主張通りであることを確保する特性
    - 責任説明性：Accountability
      - 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 (JIS X 5004)
    - 否認防止：Non-Repudiation
      - 主張された事象又は活動の発生、及びそれを引 き起こしたエンティティを証明する能力
    - 信頼性：Reliability
      - 意図する行動と結果とが一致している特性
  - マネジメントシステム
    - 組織の情報セキュリティの確保に体系的に取り組むこと
    - ISMS：Information Security Management System：情報 セキュリティマネジメントシステム
      - 基本方針：PDCAサイクル
        - Plan：情報セキュリティ対策の具体的計画を策定する
        - Do：計画を基づいて、対策の導入・運用を行う
        - Check：実施した結果の監視・検査及び内部監査を行う
        - Action：確認事による改善・是正を行う
- 情報セキュリティの種類と枠組み
  - 考え
    - 物理的セキュリティ対策：
      - 機器、設備、施設などの対策
      - 入口対策、出口対策、多重防御など
    - 人的セキュリティ対策：
      - 教育、訓練や契約などについていろんに対して行う対策
      - IPA：組織における内部不正防止ガイドライン
    - 物理的セキュリティ対策：
      - 建物や組織などを対象とした物理的な策
      - クリアスクリーン、クリアデスクなど
  - 方法
    - 予防：
      - あらかじめ対策を施す
      - 整理、点検など
    - 防止・抑制：
      - 事故が発生しないようにすること
      - バックアップなど
    - 検知・認識：
      - セキュリティ事故が起こったらすぐに気づけるようにすること
      - アクセスログ、IDS、SIEMの活用を組織 するためのインシデントマニュアルの導入など
    - 回復：
      - セキュリティ事故が発生しても迅速に対応できるようにする
      - BCPの策定など
  - 守るもの
    - 情報資産：
      - 業務に必要な資産のあるもの
      - 洗い出してレベル毎に分必要
      - 機密：
        - システム情報に関連性りを主な可能性がある インシデンプ ンの目的的活用設定する
        - 人為的（意図的）な脅威：
          - 盗難、改ざん、不正アクセス、盗聴、なりすまし、サービス不能、ウイルス感染など
        - 人為的（無意的）な脅威：
          - アクセミス、プログラムのバグ、誤ったファイルの削除など
        - 物理的な脅威：
          - 地震、洪水、雷撃、火災、台風など
      - 脆弱性：
        - 脆弱性が潜在的にとどけ ます。脆弱性が顕在化すると、情報セキュリティ対策が不能 となる。
      - リスク：
        - 発生確率が脆弱性を利用して損害を与える可能 性
        - リスクマネジメントとは潜在的な脅威を特定し、その脅威が顕在化した場合に、組織に対する影響を最小限にとどめるための活動のこと
        - 情報セキュリティ上のリスクの大きさ＝情報資産の価値＊脅威の大きさ＊脆弱性の度合い
    - 典型的な脅威や脆弱性
      - IPA セキュリティセンター：情報セキュリティ一覧表 https://www.ipa.go.jp/security/vuln/threat2020.html
      - OWASP TOP 10 https://www.owasp.org/www-project-top-ten/
- 不正な攻撃のメカニズム
  - 不正のトライアングル環境
    - 機会：
      - 不正行為が可能、または容易となる環境のこと。
      - 例：権限の集中
    - 動機：
      - 不正行為を行うための要因のこと
      - 例：借金、不心理
    - 正当化：
      - 不正行為を行うための自の応責を果り組える理由のこと
      - 例：言い訳、
    - 状況的犯罪予防
      - 物理的にやりにくい状況を作る
      - やると見つかる状況を作る
      - やっても割に合わない状況を作る
      - その恐ろさを伝える状況を作る
      - 言い訳を許さない状況を作る
  - 攻撃の種類
    - スクリプトキディ
      - ボットをお借りしてネットットとして利用することでマイバー攻撃などを実行する攻撃者
    - ボットハーダー
      - 組織の内部情報にアクセスする権限を不正利用して悪意を持ち込んり改ざんしようする攻撃者
    - 内部関係者
      - 人や社会を対象に騙れて、その様子を観察して盗ることを目的にサイバー攻撃を行う攻撃者
    - 情弱型
      - フィッシング詐欺やSNSやそしりのWeb サイトなどで個人情報などを窃盗することを目的とするフ攻撃者
    - 詐欺型
      - ランサムウェアを用いてPCを使えなくさせるWebサイトなどで個人情報などを窃盗することを目的とするフ攻撃者
    - 純愛型
      - 自分を慕う相手を利用して脅迫をする攻撃者
      - 相川一直矢犯
  - 攻撃の動機
    - 金銭目的
    - ハクティビズム
      - ハクティビズムとはハッカー思想のことで、政治的・社会的な目的に基づき実施されるハッキングを行う
      - ネットワークを対象に行われるテロリズム、人に危害を与える、社会機能に打撃を与える、といった活動が一環実は攻撃を指す
    - サイバーテロリズム
  - ハッカー
    - ホワイトハッカー：Whitehacker
    - クラッカー：Cracker
  - 攻撃の技術モデル
    - サイバーキルチェーン
      - 偵察：
        - インターネットなどから組織や人物を調査し、対象組織に対する情報を集る
      - 武器化：
        - エクスプロイトやマルウェアを作成
      - デリバリ：
        - なりすましメール（添付やリンク）などで武器を配送
      - エクスプロイト：
        - 武器を実行する
      - インストール：
        - 標的がマルウェアに感染する
      - C&C：
        - 遠隔操作して、指令サーバとマルウェアをテクニカルコードさせることでやられるルートを実行する
      - 目的の実行：
        - 探し出した情報を加工した末と、情報を持ち出す
    - ATT&CK：Adversarial Tactics、Techniques、and Common Knowledge
      - MITRE社が開発され、攻撃者の攻撃手法、戦術を分析して作成
      - されたセキュリティのフレームワークです
- SC：０１_情報セキュリティ
  - 情報セキュリティ組織・機関
    - 機能インテリジェンス
      - 機能に対応するために専門家によって収集・整理されている情報
    - セキュリティ情報共有団体
      - STIX：Structured Threat Information eXpression：脅威情報構造化記述形式
        - XML仕様
        - サイバー攻撃活動：Campaigns
        - 攻撃者：Threat_Actors
        - 攻撃手法：TTPs
        - 脅知指標：Indicators
        - 観測事象：Observables
        - インシデント：Incidents
        - 対処措置：Courses_Of_Action
        - 攻撃対象：Exploit_Targets
      - TAXII：Trusted Automated eXchange of Indicator Information：脅知指標情報交換仕様
        - 脅威情報を、サービス対象、利用目的、情報の種類毎にまとめて、安全に交換するための仕様
        - 主な機能：サーバ対応、利用目的、メッセージ性、コンテンツ対応
      - 情報セキュリティ管理責任者：CISO：Chief Information Security Officer）をはじめとする組織の最高次官級
      - セキュリティオペレーションセンター：SOC：Security Operation Center
      - セキュリティ事中監視拠点
      - ISAC：Information Sharing and Analysis Center
        - 同じ業界の関連事業所でセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めるための組織
        - 電力ISAC、金融ISACなどがある
      - CSIRT：Computer Security Incident Response Team
        - セキュリティ対策 ためのコンピュータネットワークを監視し、問題が発生した際はその原因の解析や対策を行う組織
        - 組織内CSIRT：Internal CSIRT
          - 各企業やSI利用ないなどに、組織ごとのインシデントに対応する組織
            - インシデント発生時
              - 検知・連絡受付
              - システムの異常発知や、外部組織や組織内からの通知によってインシデントを発見する
              - トリアージ：triage
              - インシデントハンドリング
              - インシデントを解決するための、インシデント対応の優先順位付けを行う
            - インシデント発生時以外
              - 事後作業後報告以と ラインシンマネジメントを実施
              - インシデントレスポンス
              - CSIRTが対応不へ者と利用してインシデントを適切に対応する
        - 国際連携CSIRT：National CSIRT
          - 国中規模毎で異ずる形で組織内CSIRTを連携し、問題を協じるる組織
        - コーデ ネーションセンター：Coordination Center
          - 他のCSIRTと の情報連携や調整を行う組織
          - 日本：JPCERT/CC（Japan Computer Emergency Response Team Coordination Center）
        - 米国：アメリカ&リーランド州に本部が設置、 日本支部にも置る
        - CNAPP Top 10
          - Web アプリケーションのセキュリティに関する重要中最脆弱性について、識別するために資料 ＿＿＿