SC：０６_実践技術

- NW APを参照
- セキュリティプロトコル
  - TLS
    - 最初のHelloメッセージ（Hello Request、Client Request、Server Hello）で、クライアントとサーバ間で使用する暗号アルゴリズムなどの情報を交換する
    - TLSから最初のやりとりからお互いFinishedメッセージ送信まではハンドシェイクプロトコル
      - マスタシークレットを作成し、それを基づいてセッション鍵を作って暗号化通信を行う
      - セッション鍵を使った暗号化通信を行うプロトコルをレコードプロトコルと呼ぶ
    - セキュリティ機能
      - 証明書による認証
        - CN（FQDN）が正しいかによりサーバ認証
        - クライアント証明書の提供でクライアント認証
      - 鍵交換
      - 暗号化通信
      - 改ざん検知 — HMACなど
    - 利用 — 証明書と秘密鍵が必要、証明書はCAより証明必要 — トランスポート層であり、TCP上で利用する — HTTPに限らず、SMTP、FTPなどTCPを用いるアプリケーションプロトコルではTLSを利用できる
    - SSL/TLSアクセラレータ — SSL / TLS専用ハードウェア
      - SSL/TLSサーバの負荷を減軽する
      - SSL/TLSを復号してから複数のサーバに負荷分散すること装置をSSL / TLSロードバランサといい
    - 常時SSL/TLS — 2021すべき
  - IPsec — ネットワーク層のIPベースのプロトコル
    - 通信流れ
      - SA（Security Association）
        - ISAKMP SA / IKE SA — Internet Security Association and Key Management Procotolは、制御用SA。TLSハンドシェイクプロトコルと同様に、通信に先立ち、データ交換を安全に行うために暗号化プロトコルや暗号鍵などの情報を交換する — フェーズ1：鍵交換
          - ISAKMP SA構築モード
            - メインモード — 基本モード、実装必須。通信相手の認証はIPアドレスを基に行うので、イニシエータ、レスポンダの両方でIPアドレスが固定である必要がある。IPsec対応ルータ同士の通信などでよく用いられる
            - アグレッシブモード — 実装必須ではない！簡略化されたモードです。イニシエータのIPアドレスは固定出なくても通信は可能、ルータとモバイルPCの通信などでよく用いられる
          - どちらのモードでも共通な処理流れ
            - パラメータ交換
            - 共通鍵の生成 — DH鍵交換アルゴリズムで互いに乱数を交換することで、暗号化に使用する共通鍵を安全に生成する
            - 認証 — 通信相手のルータやPCなどの機器を認証する。認証の方式には、事前共有鍵、ディジタル署名、公開鍵暗号などがある
        - IPsec SA — 通信データを送るためのSA、上り用と下り用でそれぞれ別のSAを生成、さらに、IPアドレスやポート番号、プロトコルが異なると別々のSAを生成する — フェーズ2：共通鍵での通信 — 通信モード
          - トランスポートモード
            - オリジナルIPヘッダとペイロードの間にセキュリティプロトコル（ESP / AH）を入れ
              - オリジナルIPヘッダ
              - AHまたはESP
              - IPペイロード
            - IPアドレスが付加されないので、PC同士などのエンドツーエンドでの通信に限られ
          - トンネルモード — 新しいIPヘッダが付け加え、IPsecゲートウェイでLAN内でのIPアドレスを隠蔽する場合などに用いられる
            - 新IPヘッダ
            - AHまたはESP
            - オリジナルIPヘッダ
            - IPペイロード
      - 用語
        - イニシエータ — 初めにIPsec通信を開始する機器
        - レスポンダ — 応答を返して通信進路を確立する機器
    - セキュリティプロトコル
      - ESP：Encapsulated Security Payload — データの暗号と認証 — トンネルモードでの範囲例
        - 新IPヘッダ
        - ESPヘッダ
        - オリジナルIPヘッダ
        - IPペイロード
        - ESPトレーラ
        - ESP認証データ
        - （ESPヘッダ～ESPトレーラ：認証範囲 / オリジナルIPヘッダ～ESPトレーラ：暗号範囲）
      - AH：Authentication Header — 認証 — トンネルモードの範囲例
        - 新IPヘッダ
        - AHヘッダ
        - オリジナルIPヘッダ
        - IPペイロード
        - （認証範囲）
    - NAT — NATトラバーサル技術が必要
      - IPsecでは、IPアドレスが認証範囲に含まれるため、NAT認証エラーになり。
      - IPsecはIPペイロードを全て暗号化され、その中のTCPヘッダ、UDPヘッダも含まれるため、ポート番号を使用するNAPTを使用もできない
  - VPN
    - IPsec-VPN — ネットワーク層のプロトコルなので、トランスポート層以上のプロトコルに制約がなく、TCPやUDPなどの様々なアプリケーションを利用することができる
    - SSL-VPN
      - トランスポート層のプロトコル、TCPに限られる — UDPを利用するIP電話のRTP、一部ゲームなどができない
      - 方式
        - SSL-VPNレイヤ2フォワード方式 — ソフトイーサネットなど擬似的なLANカードを利用してVPNトンネルを作る
        - ポートフォワード方式 — ファイアウォールを通過できないアプリケーションのポート番号番号を、通過できるアプリケーションのポート番号に変換して通信する
    - その他
      - PP2P-VPN
      - L2TP-VPN（IPsec）
      - GRE-VPN（IPsec
      - （PP2P-VPN・L2TP-VPN：データリンク層 / GRE-VPN：ネットワーク層）
      - トンネリングを行うだけで暗号化機能がない — 必要に応じてIPsecと組合わせで利用
  - IEEE 802.1X
    - 認証プロトコル、無線LAN、有線LANに拘らずポートごとに認証を行う、認証に成功した端末だけがLANに接続できる
      - 構成 — EAP
        - EAPOL
          - サプリカント — 認証を要求する側（クライアント側）の機器やソフトウェアのこと。また、クライアント側で認証のやり取りを実行するソフトウェアのこと。
          - オーセンティケータ — 無線LAN APや認証スイッチなど、IEEE802.1Xの機能を実施したブリッジ
        - RADIUS
          - オーセンティケータ — サプリカントから受け取った認証情報を元に、認証可否を認証サーバに問い合わせ
          - 認証サーバ — 認証情報を検証し、可否を返答する
      - プロトコル
        - EAP — 拡張認証プロトコル、PPPを拡張した認証プロトコル。クライアント認証とサーバ認証をサポートしている
          - EAP-MD5 — 認証にユーザ名とパスワードを使い、パスワードは平文で送るのではなく、CHAPと同様に8種関数MD5を利用して送り、サーバ認証はしない
          - EAP-PEAP — サーバから送られて北サーバのディジタル証明書が正当なものかどうかを検証する、その後、その証明書の公開鍵を使ってクライアントとサーバ間に暗号化された通信路を作り、そこでユーザ名とパスワードやキートークンなどの認証情報をやりとり — Microsoft社に開発され、サプリカントがWindows標準でOSに内蔵
          - EAP-TLS — サーバ、クライアントのディジタル証明書を相互検証を行う
          - EAP-TTLS（Tunneled TLS） — サーバ認証はサーバのディジタル証明書、クライアントはTLS経路を構築後、ユーザ名とパスワードによるクライアント認証を行う
          - EAP-LEAP — Cisco社が自社製品用に開発した独自使用の双方向認証プロトコルです。ディジタル証明書を利用せず、双方向でチャレンジレスポンス方式のパスワード認証を行う — 類似のCisco社から開発され双方向認証もＩＤ / PWのやつがEAP-FASTもあり
          - EAP-OTP — 認証にOTPを利用する方式
        - EALOL：EAP over LAN — EAPパケットをEthernetフレームのデータ部分に入れてやりとりのプロトコル — サプリカントと認証サーバ途中のオーセンティケータの間でイーサネットを使用している場合で利用
        - RADIUS — 認証と利用事実の記録（アカウンティング）を一つのサーバで一元管理する仕組み。元々はダイヤルアップ接続のためのプロトコル、IEEE802.1Xでの活用など、様々な場面で利用する
    - とVLAN — IEEE 802.1Xでは、認証状況（成功、失敗とも）によって、割り当てるVLANをポートごとに決める — ウィルス対策が施されていないPCを隔離する検疫ネットワークなどでは、このようなVLANにIEEE 802.1X認証方式を利用している
  - SSH：Secure Shell
    - 暗号方式 — 共通鍵暗号方式の共通鍵を公開鍵暗号するによって暗号化して送るハイブリッド暗号
    - 認証方式 — 代表
      - パスワード認証 — 推奨しない
        - 総当たり
        - 使い回し
        - スクリプト
      - 公開鍵認証 — 使い回しと鍵管理
      - ワンタイムパスワード認証 — ほかの認証方式と組み合わせて、SSH→TOKENより別のサービス（メッセーじゃなど）
    - 関連プロトコル
      - SCP：Secure Copy Procotol — リモートホストでのファイルコピー
      - SFTP：SSH File Transfer Procotol — FTPを暗号化する
  - 無線LAN
    - SSID / ESSID
      - APを識別するID。ESSIDは複数同様なSSIDのAPの組合せ利用の呼び方
      - BSSID — LANの中にAPの物理アドレス（デフォルトは48ビットのMACを利用）
    - 暗号化
      - WEP：Wired Equivalent Privacy：有線同等機密 — RC4（40bit/104bitの鍵長さ + 24bitのIV）
      - WPA：WiFi Prototed Access — 無線LAN製品の普及を図る業界団体であるWiFi Allianceが策定した — IV：48bit、TKIPを利用して、システム運用中に動的に鍵を変動する
      - WPA2 — 改良版、暗号化アルゴリズムとしてAES-CCMP（AES Counter-mode with CBC-MAC Protocol）を利用している
      - WPA3 — 暗号強度を192ビットに上げるなど改善があり
- アプリケーションセキュリティ
  - Web
    - アクセス制御
      - URLフィルタリングや
      - コンテンツフィルタリング
    - HTTPヘッダ
      - STS(Strict-Tranport-Security) — HSTS — Http Strict Transport Security：一度あるWebサイトにアクセスすると、次回から当該Webサイトには全てHTTPSによってアクセスするというHSTSポリシの利用をWebブラウザに強制する仕組み
      - Cookie
        - Secure
        - HttpOnly — HTMLテキスト内のスクリプトからアクセスすることを禁じ
        - DomainやPath — パスなら最後の/を省略しないで
        - Max-Age — 保存する最大有効期限（普通はローカルセッションの利用）
      - X-Frame-Options
      - X-XSS-Protection — 既存サイトに適用には慎重、良いデザインが必要
    - 認証
      - フォーム認証 — フォーム上の何らかの入力データにより暗号化を実施、一般的にはパスワード
      - ベーシック認証 — IDとパスワードのBase64を設定ので傍受盗聴解析可能
      - ダイジェスト認証 — IDとパスワードをハッシュ関数であるmd5を利用して解析されにくく
  - メール
    - 本体暗号化
      - S / MIME — ディジタル署名を行う標準規格、認証局（CA）で正当性が確認できた公開鍵を用いる
        - 生成した共通鍵でメールを暗号化、受信者の公開鍵で共通鍵を暗号化して送付
        - ディジタル署名を添付することで、データの真正性と完全性も確認できる
      - PGP — 認証局がなく、「信頼の輪」の理念の基づいて、自分の友人が信頼している人の公開鍵を信頼するという形式。小規模なコミュニティ向き
    - 経路暗号化
      - メール送受信に使われるSMTPやPOP3、IMAP4などのプロトコルには暗号化機能はない — SSL・TLSと組み合わせ
        - SMTPS
        - POP3S
        - IMAP4S
      - Webメールなどでは通常HTTPS暗号
    - 認証
      - SPF — Sender Policy Framework — 送信者認証：差出人のIPアドレスなど元にメールのドメインの正当性をDNSのTXTレコードより検証する
      - DKIM — Domain Keys Identified Mail — 受信者認証、ディジタル署名を用いて送信者の正当性を検証。署名に使う公開鍵をDNSサーバに公開して置くことで、暗号技術を組み合わせて受信者の正当性を検証できる
      - SMTP-AUTH — 送信メールサーバーで、メール送信時にユーザ名とパスワードなどを用いてユーザを認証する方法
      - POP before SMTP — SMTPにはユーザ認証機能がないので、先にPOPより認証
      - OP25B — OutBound Port 25 Blocking — 迷惑メールの送信に自社のネットワークを使われないようにするために、25番ポートで直接、SMTP通信を行うこと防止
      - DMARC — Domain-based Message Authentication, Reporting & Conformance — DNSのTXTレコードにより、メール受信側のポリシーを送信側に表明する方法
    - 迷惑メール対策
      - 迷惑メールフィルタ — 正常なメールを迷惑メールと判断してしまうフォールスポジティブに注意要 — 迷惑メールの学習手法には、統計的に迷惑メールの確率を演算するベイジアンフィルタリングがよく用いられる
      - オープンリレー（第三者中継）の防止
      - 送信ドメイン認証
  - DNS
    - コンテンツサーバとキャッシュサーバを分けることが最も重要
      - キャッシュサーバは、クライアントからの再帰的な問い合わせに応答するので、この仕組みが攻撃に利用されやすいので、内部用キャッシュサーバを公開しないことが望まれる — DNS amp攻撃とDNSキャッシュポイズニング攻撃に対して有効
      - DNSコンテンツサーバ — 自分で管理している情報を教えてあげるのがお仕事のDNSサーバ
      - DNSキャッシュサーバ — 他のDNSサーバさんに答えを教えてもらいを行くDNSサーバ — ネットワーク利用の普通に「DNSサーバ」と言った場合は、DNSキャッシュサーバを指すことも多い
      - （主に概念上区別するための用語です、ほぼ同一製品で二つ機能を実現できるが、分けてキャッシュサーバが非公開が一般推奨）
    - DNSSEC — クライアントとサーバの両方がDNSSECに対応しており、該当するドメインの情報が登録されていれば、DNS応答レコードの偽造や改ざんなどを検出できる — 具体的には、DNS応答レコードのハッシュ値にDNSサーバの秘密鍵を用いてディジタル署名を生成する、受け取った側がDNSサーバの公開鍵で復号することで、DNSレコードの完全性と真正性を確認できる
    - ゾーン転送の保護 — DNSでは、オリジナルの情報はプライムDNSサーバに保持されており、この情報をセカンダリDNSサーバにコピーする。この時使われる手法をゾーン転送と言い — ゾーン転送は通信相手が限られているので、特定の通信相手飲みに制限することが望ましい。TLS暗号化も可能です
  - 脆弱性対策
    - 対策
      - 根本的解決
      - 保険的解決 — 目の前にある攻撃手法に着目した、取り急ぎ特定の攻撃のみを防ぐ
    - クラウドサービス — 責任区分があり、提供してくれても確認要
      - データセンタの物理的セキュリティ
      - 不正アクセスや脆弱性、マルウェア対策
      - アクセスログの取得
      - バックアップの取得や障害対策
      - 通信経路の暗号化やアクセス制御
    - 電子透過し — 画像や音楽などのディジタルコンテンツに情報を埋め込む技術
      - 画像の合成など、見た目で判別可能なものもあるが、通常は知覚困難です
      - ステガノグラフィ — データを隠蔽して情報をバインディング（結合）する技術であるステガのグラフィックがあり
  - 証拠保全技術
    - 時刻同期（NTP）
    - SIEM — Security Information and Event Management — サーバやネットワーク機器などからログを集め、そのログ情報を分析し、異常があれば管理者に通知する、または対策方法を知らせる仕組み
    - WORM — Write Once Read Many — 書き込みが一回しかできない記憶媒体、改ざん防止（媒体丸ごとに改ざんは防止不可）
    - ブロックチェーン — 仮想通貨などで用いられる分散型台帳技術、ログごとのハッシュ値を連続でチェーンのように繋げることで、ログの完全性と順番を保障することができる
- ハードウェアセキュリティ
  - ハードディスク暗号化
  - スマートデバイスのセキュリティ
    - OSをアップデートする
    - 改造行為を行わない
    - 信頼できる場所からアプリケーションのインストール
    - Android端末では、APインストール前に、APがアクセスする許可範囲を確認する
    - セキュリティソフトを導入する
    - 小さいなPCと考え、PCと同様に管理する
  - ハードウェアトークン — インターネットバンキングサービスなどを利用するときに用いられる認証用専用機器 — 所持
  - 耐タンパ性 — ソフトウェアやハードウェアが備える、内部構造や記憶しているデータなどの解析の困難さのこと — 解析しようとすると、それを検知してシステム自体を破壊するなどの方法で、耐タンパ性を確保
  - TPM — Trusted Platform Module — ハードウェアに耐タンパ性を持つセキュリティチープです。内部でRSAの鍵ペアを生成することができる — 秘密鍵はTPMの外部に取り出す事ができないため、秘密鍵の漏えいを防ぐことが可能 — チープ内での暗号化・復号、ディジタル署名の生成・検証、プラットフォームの完全性検証を行う