情報通信の基礎知識

情報セキュリティ対策

東京デザインテクノロジーセンター専門学校　講師　石川敢也

Information Security Measures

- 情報セキュリティ対策
  - 個人や企業を脅かす情報セキュリティのリスクには、さまざまなものがある。必要な情報セキュリティ対策も多様である。
- 内容
  - CSIRT、CRYPTREC、プライバシーマーク制度
  - ファイアウォール、MACアドレスフィルタリング
  - VPN、ペネトレーションテスト、DMZ、 SSL／TLS
  - ディジタルフォレンジックス、認証局、デジタル署名
  - 共通鍵暗号方式、公開鍵暗号方式

Computer Security Incident Response Team

- CSIRT（シーサート）
  - 企業・組織内や政府機関に設置され、コンピュータセキュリティインシデントに関する報告を受け取り、調査し、対応活動を行う組織の総称。
- CRYPTREC（クリプトレック）
  Cryptography Research and Evaluation Committees
  - 電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。

CRYPTREC
Cryptography Research and Evaluation Committees

cryptrec.go.jp

Privacy Mark System

- プライバシーマーク制度
  - 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JIPDEC（日本情報経済社会推進協会）が評価・認定する制度。

- JAPHIC（ジャフィック）マーク制度
  - 個人情報保護法に適合した個人情報の適切な保護を促進する制度。個人情報について適切な保護措置を講ずる体制を整備し、運用している事業者を特定非営利活動法人日本個人・医療情報管理協会が認定する。

Firewall

- ファイアウォール
  - インターネットからの不正アクセスを防ぐことを目的として、インターネットと内部ネットワークの間に設置する仕組み。
- MACアドレスフィルタリング
  - 無線LANのセキュリティにおいて、アクセスポイントが接続要求を受け取ったときに、端末固有の情報（Media Access Control address）を基にアクセス制御を行う仕組み。

Virtual Private Network

- VPN（仮想プライベートネットワーク）
  - インターネットなどの共用のネットワークに接続された端末同士を、暗号化や認証によってセキュリティを確保して、あたかも専用線で結んだように利用できる技術。
  - 専用線ではなくインターネット経由で機密性を保つため、特殊な接続方法や暗号化を行っている。
  - インターネットを介しVPNを構成する「インターネットVPN」と、プロバイダが提供する閉域網を利用するタイプの2種類が主流である。
  - 後者はISPの専用IP網を利用する「IP-VPN」などがある。

– *Wikipediaより引用・抜粋・編集*

Penetration Test

- DMZ（DeMilitarized Zone）
  - 企業内ネットワークからも、外部ネットワークからも論理的に隔離された領域。
  - 外部からの不正アクセスによる被害が内部ネットワークに及ばないようにするための領域。
  - 本来は「非武装地帯」という意味。

- ペネトレーションテスト
  - 侵入テスト。実際にシステムに侵入を試みて検証するテスト。

Secure Socket Layer

- SSL／TLS（Transport Layer Security）
  - HTTP通信の暗号化を行うことによって、通信経路上での通信内容の漏えいを防ぐセキュアプロトコル。
  - 「SSL3.0」の次のバージョンから「TLS1.0」という名称になったが、一般にはSSLという名称が普及している。
- HTTPS(HTTP over SSL/TLS)
  - サーバとブラウザが安全に通信をするためにSSLを使って通信内容を暗号化するための仕組み。
  - メッセージを暗号化せずに送受信するHTTPと異なり、通信内容を暗号化し、改ざんの検出などを行う。

– *Wikipediaより引用・抜粋・編集*

Digital Forensics

- ディジタルフォレンジックス
  - 不正アクセスなどコンピュータに関する犯罪の法的な証拠を確保できるように、原因究明に必要な情報の保全、収集、分析をすること。
  - 関係する機器を押収して、証拠となるデータを抽出したり、サーバや通信機器などに蓄積された通信記録から、違法行為の証拠となる活動記録を割り出したり、消去された記憶装置を復元したりする技術・活動。
  - 「Forensics」は「科学捜査の」という意味。

－ IT用語辞典 e-Wordsより引用・抜粋・編集

One-time Password

- ワンタイムパスワード
  - 認証のために一度しか使えないパスワード。
  - 利用者は、トークンと呼ばれる装置などを用いて、
    生成された使い捨てのパスワードで認証を受ける仕組み。
- シングルサインオン（Single Sign-On）
  - 一度の認証で、複数のサーバやアプリケーションなどを
    利用できる仕組み。
- コールバック（Call Back）
  - アクセス権を確認するために、回線をいったん切り、
    システム側から再発信して通信を開始する方法。

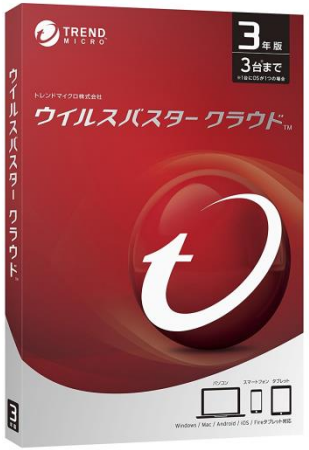
Biometrics Authentication

- 生体認証／バイオメトリクス認証
  - 指紋や声紋など、身体的な特徴を利用する認証の仕組み。
- 静脈パターン認証（Vein Authentication）
  - 掌や指先の静脈パターンを利用する認証の仕組み。
- 虹彩認証（Iris Recognition）
  - 角膜と水晶体の間にある薄い膜によって本人確認を行う認証の仕組み。

- 「ピースで指紋が盗まれる」という事件は本当？

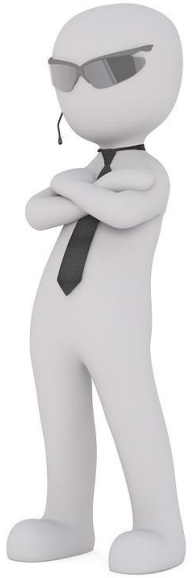
Anti-Virus Software

- ウイルス対策ソフト
  - マルウェアを検出したり除去したりするソフトウェア。
  - パーソナルファイアウォール、スパイウェア対策、迷惑メール対策などの機能を統合したソフトウェアもある。
- パターンマッチング方式
  - ウイルス定義ファイル（パターンファイル）を用いて、PCに存在するファイルと照合し、一致すればマルウェアとして検出する手法。
  - 導入後もウイルス定義ファイルの更新を継続して行う必要がある。



Common Key Cryptography

- 暗号化／復号
  - 暗号化は通信文の内容を秘匿するための変換方法。
  - 暗号文を平文に戻すことを復号という。



- 共通鍵暗号方式
  - 暗号化と復号で同じ鍵を使用する暗号方式。
  - 通信相手ごとに異なる共通鍵が必要。
  - 処理時間は、公開鍵暗号方式よりも短い。
- AES（Advanced Encryption Standard）
  - 次世代暗号方式として規格された共通鍵暗号方式。

Public Key Cryptography

- 公開鍵暗号方式
  - 暗号化と復号に異なる鍵を使用する暗号方式。
  - 暗号化鍵(公開鍵)は、誰もが使用できるように公開し、復号鍵(秘密鍵)は受信者が厳重に管理する必要がある。
- RSA(Rivest Shamir Adleman)
  - 公開鍵暗号のひとつ。桁数が大きい数の素因数分解が困難であることを利用している。
- ハイブリッド暗号方式
  - 公開鍵暗号方式における鍵管理の利便性と、共通鍵暗号方式の速い処理速度を組み合わせた方式。

Digital Signature

- ディジタル署名
  - 公開鍵暗号技術を応用して、文書の正当性を保証するために付けられる暗号化された署名情報。
  - 発信元の正当性と改ざんの有無が確認できる。

- 認証局（CA、Certification Authority）
  - 公開鍵暗号方式を用いたデータ通信において、利用者の公開鍵の正当性を保証するためのディジタル証明書を発行する第三者機関。

お疲れさまでした！