情報ネットワークⅡ（情213）
【第2回】
情報セキュリティ概論
（教科書：第1章）

担当教員：長田智和

E-Mail: nagayan@ie.u-ryukyu.ac.jp

URL: http://n-lab.info/

（講義日：2017年10月12日）

第１章：情報セキュリティ概論

1.1 情報セキュリティとは

- 世界的なインターネットの普及
  - 2013年時点で27億人以上（日本は人口の8割以上）
- ITの普及によるネガティブな側面
  - 障害、事故、事件への配慮が必要
  - 「機密性」「完全性」「可用性」の確保・維持
  - 不測の事態が発生した時に、速やかに元の状態に復旧する仕組みが必要
  - 企業などで情報資産のセキュリティを確保・維持する必要性 → 情報セキュリティの目的

1.1 情報セキュリティとは

- 1.1.1 情報セキュリティの分類
  - 物理セキュリティと論理セキュリティ
  - 物理セキュリティ：建物や設備。インフラ周り。
  - 論理セキュリティ：物理セキュリティ以外。さらにシステムセキュリティと人的セキュリティに分類される。
  - ITシステムにおけるセキュリティは「システム開発者」「システム運用者」「エンドユーザー」など観点によって異なる。
- （教科書p.3の図1.1を参照）

1.1 情報セキュリティとは

- 1.1.2 情報セキュリティが満たすべき3つの性質
  - 機密性：情報資産へのアクセスを許可された者だけに制限すること。暗号化や認証、アクセス制限で実現。
  - 完全性：情報資産が棄損や改竄されないこと。ハッシュ関数やデジタル署名、改竄検知機構（パリティチェック）、バックアップなどで実現。
  - 可用性：情報資産やITシステムなどにアクセスする際、正常にサービスを利用できる状態に維持すること。システムの多重化などで実現。
- （教科書p.4の図1.2を参照）

1.1 情報セキュリティとは

- 脅威への具体的なセキュリティ対策
  - 予防：ファイアウォールの導入、OSやアプリケーションのバージョンアップ、セキュリティパッチの適用など。
  - 抑止：人的管理では、情報セキュリティポリシーの周知・教育・実施状況の監査、技術観点では、ITシステムのリアルタイムモニタリングなど。
  - 検知：ウィルス対策ソフトの導入、ログの監視など。
  - 回復：データのバックアップ、復旧手順書の作成など。
- （教科書p.6の表1.1を参照）

1.1 情報セキュリティとは

- 情報セキュリティリスクへの対処
  - リスクの低減：システムの脆弱性に対して対策を講じること。（前述の予防や抑止に相当）
  - リスクの保有（受容）：リスクの影響が少ない場合は、敢えてそのリスクを許容すること。
  - リスクの回避：リスクの要因自体を排除すること。
  - リスクの移転：リスクの要因を別の組織に移すこと。
- （教科書p.7の図1.3を参照）

1.1 情報セキュリティとは

- 1.1.3 脅威の範囲とインパクト
  - 個人情報の漏えいによる影響
    - 記憶メディア、紙媒体の流出、ファイル共有ソフトによる流出、マルウェアによる流出など
  - Webサービスへの攻撃による影響
    - Webサイトの脆弱性を悪用する攻撃による情報漏洩、閲覧者PCに対するマルウェア感染、サービス運用妨害など。
    - 動的なWebサイトはDBと連携しており、DB内の個人情報が漏洩すると影響は非常に大きなものとなる。
  - PCのワーム感染による影響
    - 2003年ごろに広まった「Blaster」は、感染したPCの動作を不安定にするだけではなく、他のPCに感染を広げた。
- （教科書p.9の図1.4を参照）

1.1 情報セキュリティとは

- 1.1.4 情報セキュリティの変遷
  - インターネットの登場
  - コンピュータウィルスの登場
  - Webの登場
  - 米国による暗号技術の輸出制限
  - 進化する攻撃手法
- （教科書p.10の表1.2を参照）

1.2 セキュリティを構成する要素

- 1.2.1 暗号化技術
  - 共通鍵暗号方式：秘密を共有したい2者間で同じ鍵を使う方式。現在は、AES（Advanced Encryption Standard）の利用が推奨されている。
  - 公開鍵暗号方式：暗号化する鍵と復号する鍵が異なる方式。RSA（開発者3名の頭文字）方式が一般的。
  - ハイブリッド暗号化方式：共通鍵暗号方式と公開鍵暗号方式の欠点を補い合う方式。
- （教科書p.15-16の図1.5-1.6を参照）

1.2 セキュリティを構成する要素

- 1.2.2 デジタル署名
  - 公開鍵暗号方式をデジタル署名として用いて、発信者の真正性を確保する。
  - 印鑑を押した書類と同等に扱われる。
  - デジタル署名されたデータは完全なコピーが可能であるため、原本性は保証できない。
- （教科書p.17の図1.7を参照）

1.2 セキュリティを構成する要素

- PKI（Public Key Infrastructure）
  - 公開鍵暗号方式における公開鍵の所有者を結びつける手段。
  - 信頼できる機関が公開鍵の真正性を保証する。
- （教科書p.17の図1.8を参照）

1.2 セキュリティを構成する要素

- 1.2.3 セキュリティプロトコル
  - 真正性、機密性、完全性を確保する通信技術
  - サイトの真正性 → PKI証明書と公開鍵で認証
  - 通信データ完全性 → メッセージ認証コードで確認
  - Webのセキュリティプロトコル標準

    → SSL/TLS（Secure Socket Layer/Transport Layer Security）
- 1.2.4 認証
  - ITシステムが利用者を特定する技術
  - ID&パスワード認証、虹彩や指紋認証など
  - 複数システムの認証プロセスを統合するID連携

1.2 セキュリティを構成する要素

- 1.2.5 バッファオーバーフロー対策
  - CやC++で書かれたプログラムに存在する典型的な脆弱性。プログラマが想定したメモリサイズ以上のデータが書き込まれ、そのデータには不正なプログラムが含まれており、それが実行されてしまう。
- 1.2.6 アクセス制御
  - 認証によって特定された主体に対して、許可された操作しかできないようにするメカニズム。
  - 任意アクセス制御、強制アクセス制御、ロールベースアクセス制御
- （教科書p.19-20の図1.9-1.10を参照）

1.2 セキュリティを構成する要素

- 1.2.7 ファイアウォール
  - 外部・内部ネットワークを区別し、それらを行きかう通信を主にIPパケットレベルで制御し内部ネットワークの安全を維持する仕組み。
- 1.2.8 Webにおけるセキュリティ対策
  - 大半のインターネットサービスはWeb技術を利用
  - Web技術はDBと連携している場合が殆ど
  - SQLインジェクション等の脆弱性攻撃でDBから情報を盗み取られたり改竄されたりする恐れがある。

1.3 昨今のセキュリティに関する脅威

- 標的型攻撃に関わる脅威
- 災害に関わる脅威
- 共通思想集団に関わる脅威
- クライアントソフトウェアの脆弱性に関わる脅威
- Webサイトに関する脅威
- スマートフォンに関わる脅威
- 公開鍵証明書に関わる脅威
- 内部からの攻撃・情報漏洩に関わる脅威
- アカウント情報に関わる脅威
- 利用者情報に関わる脅威

【次回予告】
第3回
暗号化技術（1）
（第2章）

また来週！