「セキュリティの基礎
ーセキュリティとは」

琉球大学　工学部工学科　特別講義　2限目

「2日間でわかるITの基礎」

2017年8月15日

株式会社エス･キュー･シー
倉田　克徳

SQC
System Quality Certification

目次

- 概要

1. セキュリティポリシー
2. デバイスのセキュリティ
3. サーバー・インフラのセキュリティ
4. その他のセキュリティ
5. セキュリティの現状
6. サイバー空間は第4の戦場
7. まとめ

SQC
System Quality Certification

1. セキュリティポリシー

- セキュリティポリシー
  - どのような情報資産をどのような脅威から、どのようにして守るかについての基本的な考え方(JIS Q 27002:セキュリティ方針)
  - 具体的な組織、体制、運用等が記載された規定
  - 継続的に改善をしていかなければならない
- 情報セキュリティ3要素
  - 機密性の確保→情報資産を限られた人だけが使用できる状態にしておくこと
  - 完全性の確保→情報資産が正当な権利を持たない人により変更されていないことを確実にしておくこと
  - 可用性の確保→情報資産を必要なときに使用できること

2. デバイスのセキュリティ

- コンテネクティッド・デバイス（IoTデバイス）
  - ソフトウェアセキュリティ
    - NIST（米国立標準技術研究所）の規定→暗号化キーの保護、デバイス認証の実行、ソフトウェアの検証→信頼されているコンポーネント(root of trust)
  - ハードウェアのセキュリティ
    - 暗号化→デジタル署名（フィンガープリント）、公開鍵基盤（PKI）

SQC System Quality Certification

3. サーバー・インフラのセキュリティ

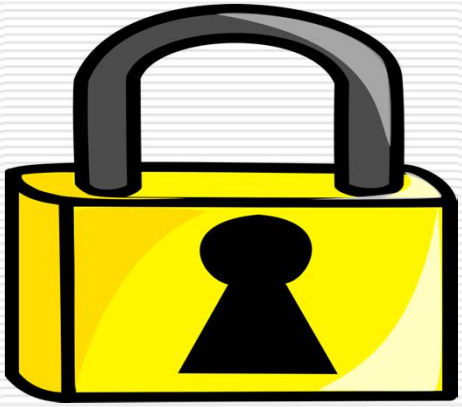
- ネットワーク機器
  - ファイアウォール、その他あらゆるネットワーク機器のセキュリティ対応
- 各種サーバー
  - プログラマブルなセキュリティ対応
    - セキュアのプログラミング→IPA：公開Webサイトの運用におけるセキュリティ対策　参照
  - システム運用でのセキュリティ対応
    - セキュリティパッチの適用、そのた運用面でのセキュリティ対策

4. その他のセキュリティ

- 一番の弱点は「人」
  - 法令遵守（コンポライアンス）
- 悪意を持った「人」が一番の弱点で有り、恐怖

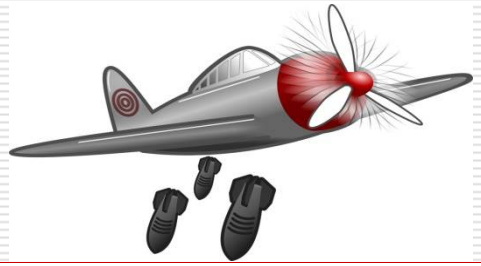
5. セキュリティの現状

- ハッカー、クラッカーのタイプ
  - 通常のハッカー、クラッカー
  - ホワイト・ハッカー、クラッカー
- 対処法と政府の対応
  - 対処法→基本的には追いかけっこ
  - セキュリティ技術者育成、要請（IPA）
  - セキュリティ・キャンプ、セキュリティ・コンテスト
    - 若手のセキュリティ技術者育成、技術研鑽



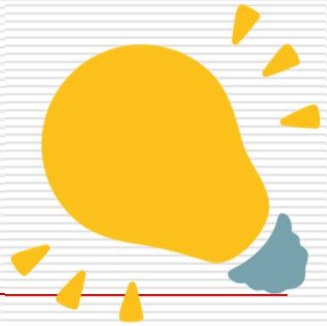
6. サイバー空間は第4の戦場

- 世界中からのハッキング・クラッキング
- 日本政府関連情報、防衛情報
  - 事例：三菱重工、「標的型メール」（内閣府実在人物名、メールアドレスも本人のもの）、添付ファイル名「原発のリスク整理」、目的：原発を攻撃するする方法を探る
  - その他企業、川崎重工、IHI等、自衛隊関連情報も対象として多い



SQC System Quality Certification

7. まとめ



- 考えられるセキュリティ対策は必ず講じておく
  - 可能な限り対策を講じても、セキュリティは破られる
  - 最終的には可能な限りの対策を講じたという責任
- セキュリティの最終的な原因は「人」
  - 悪意を持った「人」→ハッカー、クラッカー
  - 善意を持った「人」→ホワイトハッカー
- 守るべき情報資産
  - 国家国益に関する情報から、個人情報まで
  - 他人の情報は蜜の味→のぞき見、悪用