情報セキュリティ技術史から浮かび上がる制御系システムの課題

What CS could learn from the history of information security?

2009-2-19

JPCERT/CC
宮地 利雄

本日のアジェンダ

- 情報セキュリティと「攻撃」
- 情報セキュリティの「歴史」
- 「オープン化」と情報セキュリティ
- 情報セキュリティ対策の歴史からの「学び」
- セキュアな制御システムに向けて

情報セキュリティとは

情報セキュリティとは、情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。

- 機密性(Confidentiality):　認可されていない個人、エンティティ(団体等)又はプロセスに対して、情報を使用不可又は非公開にする特性
- 完全性(Integrity):　資産の正確さ及び完全さを保護する特性
- 可用性(Availability):　認可されたエンティティ(団体等)が要求したときに、アクセス及び使用が可能である特性

出典:　ISO/IEC27001:情報技術−セキュリティ技術−情報セキュリティマネジメントシステム−要求事項の「用語及び定義」より

情報セキュリティに対する脅威

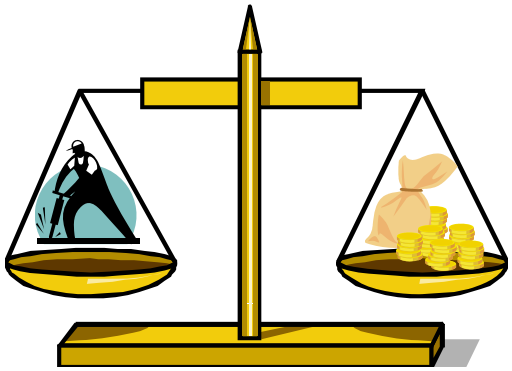
脅威： 情報セキュリティのCIAを擾乱する要因

- 偶発的で異常な入力または操作
- 攻撃 ＝ 故意(悪意)による異常な入力または操作

セキュリティの議論の前提
(Cf. 安全性)

攻撃者にとっての損得勘定：動機がありコスト＜メリットならば攻撃

攻撃のコスト：
- 投入費用
- 手間かず
- 懲罰の痛み



攻撃のメリット：
- 注目(愉快犯)
- 相手の損害(報復)
- 金銭的な利益

情報セキュリティの歴史概観

暦年	時代	トピックス
1980年代以前	暗号技術の時代	• DES暗号FIPS制定(1976～1977年) • RSA暗号の発明(1977年)
1990年代	ネットワーク・セキュリティの時代	• モーリス・ワーム(1988年) • 「カッコーはコンピュータに卵を産む」(1991年) • CheckPoint社(ファイアウォール)創立(1993年) • JPCERT/CC開設(1996年)
2000～2005年	ネットワーク・ウィルスの時代 (情報セキュリティ管理)	• コンピュータウイルス対策基準制定(1990年) • Nimdaウイルス(2001年) • Blasterワーム(2003年) • Sasserワーム(2004年) • BS7799-1をISO/IEC 17799に採用(2000年) • 日本政府がNISCを設置(2005年)
2005～2010年	ウェブ・セキュリティの時代	• SQLインジェクション攻撃が広まる(2005年～) • 「ぼくはまちちゃん」騒動(2005年)
2010年～		

セキュリティが大きな問題になったのは1990年頃から

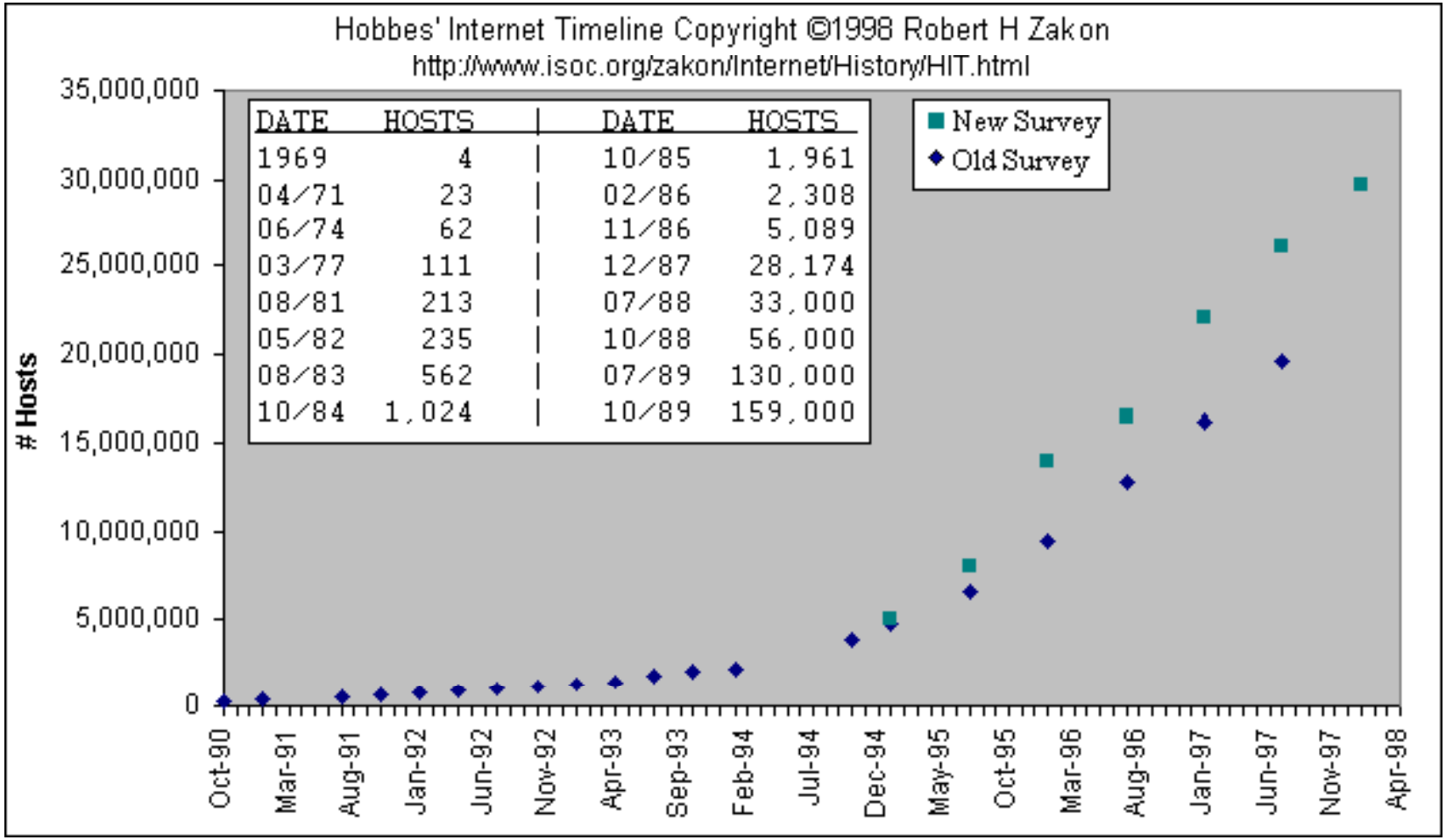
セキュリティ問題が浮上した時代的な背景

- 主要なセキュリティ概念は1980年代以前に既に登場していた
  例：コンピュータ・ウイルス，ファイアウォール，IDS(侵入検知システム)
  ⇒セキュリティ問題が浮上する背景

- セキュリティ問題が浮上した背景
  - 1990年代：　ネ・オ・ダ・マの時代　（**オープン化の進展**）
  - 2000年代：　個人用パソコンの普及
  - 2005年以降：　ウェブ技術の複雑化やDB連携

オープン化とは：
1. 仕様が公開された技術の採用
2. 標準的なモジュール(実現)の採用
3. 広域汎用ネットワークの利用

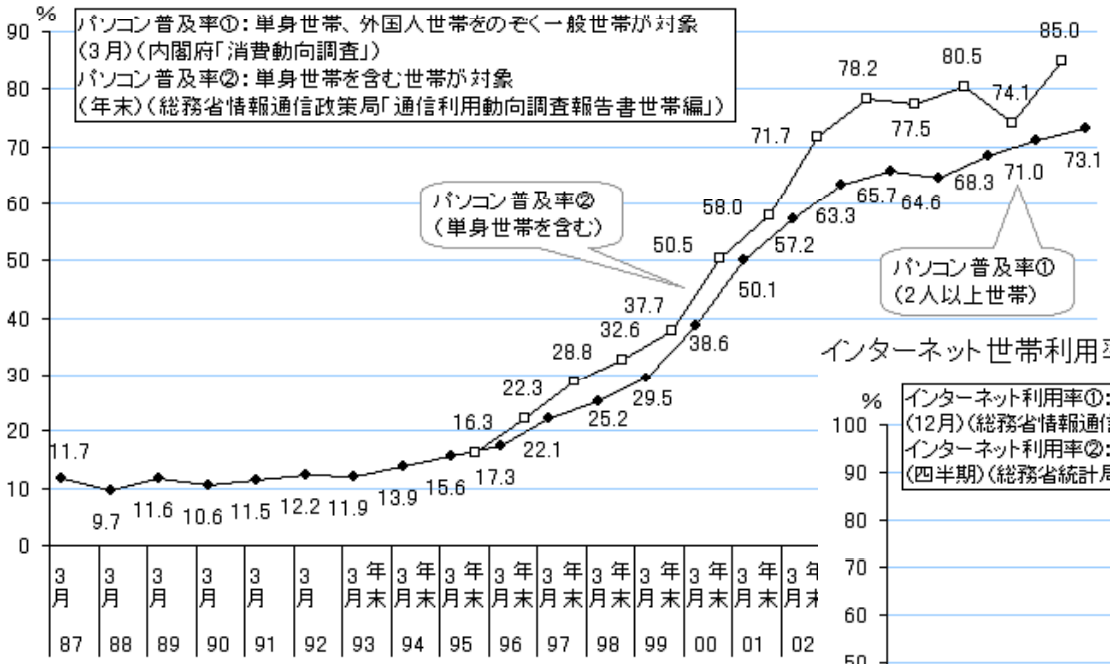
[参考] インターネットの普及



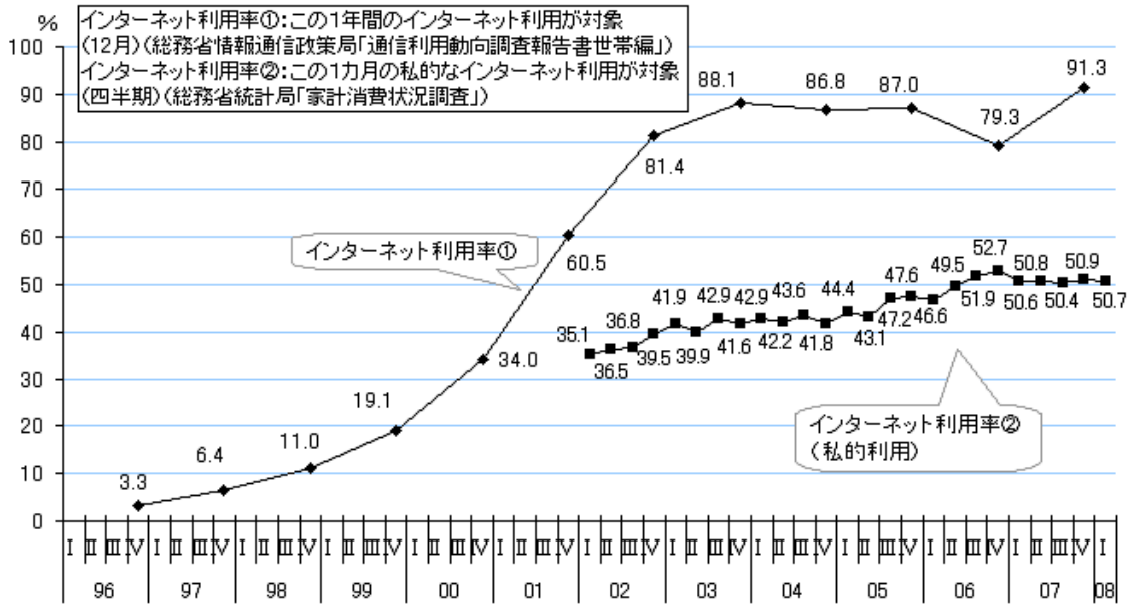
DATE	HOSTS	DATE	HOSTS
1969	4	10/85	1,961
04/71	23	02/86	2,308
06/74	62	11/86	5,089
03/77	111	12/87	28,174
08/81	213	07/88	33,000
05/82	235	10/88	56,000
08/83	562	07/89	130,000
10/84	1,024	10/89	159,000

[参考] パソコンとネットワークの国内普及

パソコン世帯普及率



インターネット世帯利用率の推移



オープン化が始まった制御システム

- 制御システムもオープン化へ
- オープン化への歩み

ちょうど情報処理における
1990年代と類似した
状況では？

セキュリティの時代への
夜明け前後

- 応用領域により緩急多様
  - ビル管理や生産管理の分野は急
  - 電力関連は緩
- グローバル競争と関連して進行
  - 製品/提供システムとしての競争力
  - オープン化を使いこなすことを通じた競争力

オープン化の光と陰

オープン化

- 公開された仕様
- 標準的モジュール
- 広域汎用ネットワーク

光

- 複数ベンダーからBest of Breed製品を調達できる
- 顧客や調達先などパートナー企業との接続性の向上
- 高度な機能を低価格で実現できる
- 類似システムでの海外展開も容易
- 通信回線費用低減

陰

- 攻撃法を編み出すための参考情報の入手が容易化
- 一撃により影響を受ける範囲が拡大
- 遠隔からの攻撃が可能に
- 潜在的な攻撃者数が増加

攻撃者のコストが減りメリットが大きくなる

オープン化されたセキュリティ対策

隠すことだけに終始しない対策

- 標準化された
  セキュリティ機能仕様
  - 暗号アルゴリズム
  - セキュリティ・プロトコル
- 標準的な
  セキュリティ・モジュールの活用
- 標準的な
  セキュリティ・アーキテクチャー

- 標準化された
  セキュリティ管理方法
- 標準化された
  インシデント管理方法
- オープンで責任ある情報共有
  - セキュリティ情報の開示
  - 情報共有コミュニティへの参加

セキュリティに関するアカウンタビリティ(説明責任)

止め難いオープン化への流れとその影響

始まったオープン化への流れは止め難い

(1990年代前半に言われたこと)

- メイン・フレームは不滅！
  UNIXサーバが取って替わるはずがない
- ブラウザはお遊びツール！
  ビジネス利用とは無縁

制御システムのオープン化の今後は？

オープン化の影響

- 基盤コンポーネントの低価格化
  (価格競争により提供者減少)
- 独立機能の高度化
- 製品からサービスへの移行
  (高度化された機能に関して)

◆提供ベンダーの事業構造変化
- 得意分野への集中
- サービス事業化

◆ベンダー～利用者の関係変化

製品・サービス市場への影響

- セキュリティは無料で製品に付属されたものでは必ずしもなくなる
  - 要求を明確化して調達
  - セキュリティに対する対価を調達側が負担
- セキュリティ専業ベンダーを活用する可能性
  - セキュリティ・コンサルティングや侵入事故解析などのプロフェッショナル・サービス
  - セキュリティ監視などにおけるアウト・ソーシング

情報セキュリティ対策の歴史 (1/2)

JPCERT CC®

1980年代～

まず⇒ 保護機構の導入 (コンピュータ・セキュリティ)

- 認証，権限管理
- ファイアウォール，VPN
- 侵入検知システム(IDS)
- ログ(セキュリティ情報)管理システム

1990年代～

次いで⇒ セキュリティ教育(人間(ヒューマン)セキュリティ)

- 利用者の教育
  - セキュリティ問題に対する気づき (awareness)
  - 保護機構の基本的な理解と利用法
- 開発者の教育

情報セキュリティ対策の歴史 (2/2)

JPCERT CC®

2000年～

その後⇒ 組織としてのセキュリティ対策

- 情報セキュリティ・ポリシー
- 情報セキュリティ管理システム
  (ISMS: Information Security Management System)
- セキュリティ組織体制
  - CISO (Chief Information Security Officer)
  - インシデント対応体制

2005年～

その後さらに⇒ 情報セキュリティ・ガバナンス

- 企業経営の一つの側面としての情報セキュリティ
- 情報セキュリティ監査

セキュリティ対策の歴史からの学び

1. いずれが欠けても成らないセキュリティ対策の３本柱
   - 物的(システム面での)対策
   - 教育 (一人ひとりを強くする)
   - 組織としての対策 (組織的な対応力)

2. 矛に合わせた盾の準備を
   - 完璧なセキュリティ対策(盾)はあり得ない;
     過度な対策は費用がかかり過ぎる
   - 矛(脅威)をにらみながら盾(対策)を用意

3. 情報共有できる仲間作りの重要性
   - 一朝一夕に形成できない信頼

セキュアな制御システムの実現に向けて

JPCERT CC®

■ 情報処理におけるセキュリティ対策の知見の活用
- 基本概念
- 教育や組織面での対策

■ 制御システムに固有な要件の整理と解決策の探索
- 比較的長いシステム更改サイクル
- サービス継続性に関する要件
- 処理能力が限られたコンポーネントの存在

■ 制御システムのセキュリティについて情報共有できるコミュニティ作り

セキュアな制御システムに向けたJPCERT/CCの取組み

制御システム運用者に対して

- 制御システムに係る情報発信
  - 注意喚起情報の提供
  - WAISEなどによる
    特定分野向けの情報提供

制御システム提供者に対して

- 制御システム用製品の
  脆弱性関連情報の取扱い
  - 制御システムに合わせた取扱方法の検討
  - 海外の取扱い組織との連携
- 制御システム提供者のための
  セキュリティ情報共有に向けた
  コミュニティ形成の支援

JPCERT コーディネーションセンター
Email: office@jpcert.or.jp
TEL: 03-3518-4600
URL: http://www.jpcert.or.jp/