本スライドは、当日のセミナー資料の一部を抜粋したものです。

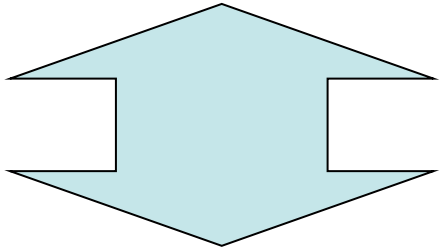
IoT・組込み機器のための脅威分析とセキュリティ・バイ・デザイン

2016/11/16

情報セキュリティ大学院大学
大久保 隆夫

セキュリティ・バイ・デザインとは

- ソフトウェアやシステム開発の課程で
  開発の早期段階(分析、設計)からセキュリティ
  を作りこむ



- 対義語？ セキュアプログラミング
  プログラミング工程での脆弱性排除

脅威分析とは

- 対象のソフトウェアやシステムに対する脅威を識別し、その影響を評価し、対策を策定する分析
- 「脅威」が、第三者の悪意に基づくため、このような(通常の開発にはない)分析が必要
- 分析工程における脅威分析
  =セキュリティ要求工学
- 設計工程における脅威分析

IoT、組込みにおける「安全」を考える

- ITと同様の考え方でできるものもある
  - Webサーバが組込まれた機器
    Webカメラ、ルータetc.
- 「セーフティ」を考慮しなければならないものも
  - 機械の無故障、人命の安全、事故防止etc.
  - 家電(エアコン、冷蔵庫)
  - 交通系(車、鉄道、航空)
  - 制御系(エレベータ等)

セーフティ分析とセキュリティ分析の相違

- 守る対象の観点
- 脅威の見つけ方
- リスク評価の手法
- 規格/標準の差異

規格/標準の問題

- 既存の一方の規格/標準で他方をカバーできるか？
  - セーフティ規格をセキュリティに応用
    →リスク評価における攻撃の扱いをどうするか
  - セキュリティ規格をセーフティに応用
    →安全性、ハザードの資産を拡張
- セキュリティ規格の問題
  CCの手法の業界への浸透が不十分