情報セキュリティ設計と技術評価基準

情報社会とセキュリティ
2024 年度前期
佐賀大学理工学部 只木進一

情報システム設計

- 情報システム設計時にセキュリティも含めて設計
- 稼働後でセキュリティ対策をすると、脆弱性を持ち込む恐れ
- システムの機能、性能とそれ以外の要件

全体設計とセキュリティ設計

- 情報システム・サービスの設計時
  - 機能要件: ○○できること: システム・サービスの目的
  - 性能要件: ○人で同時使用できること。○秒以内に応答できること。
  - 機能性能以外の要件
    - セキュリティ要件: アクセス制限、認証、暗号化、攻撃対策、情報漏えい対策など
    - 保守、研修、データ移行、作業体制等
- 各要件がトレードオフ関係になることもある
- 設計時に、各要件の調整が必要

例: Web サービス

- Web サービスの目的を整理
  - 情報公開? 情報収集? 情報共有?
  - 利用人数
  - 認証の必要性
  - 認可の種類・権限管理
  - どこから利用する: 組織内、インターネット
- Web はもっとも狙われやすいことに留意
  - 新規サーバが立つと、大量のポートスキャンや攻撃が来る
  - セキュリティ対策を十分に行ってから、公開すべし

機密性、完全性、可用性のレベルを設定

- 機密性
  - 多要素認証で十分か? クライアント証明書が必要か
  - 利用者の本人確認の強度
  - 暗号化の強度
  - 証明書の必要性
  - 通信路を通る情報の確認
- 完全性
  - 改ざんへの対策
- 可用性
  - 停止することのリスク

Web サーバの構成要素への配慮

- OS: Linux, Windows Server, etc.
- Web サーバ本体: Apache, IIS, TomCat, etc.
- 関連ミドルウェア
  - プログラミング言語: Java, perl, php, python, javascript, etc.
  - データベース: postgresql, mySQL, SQL server, etc.
  - フレームワーク: Struts, Java Face, etc.
  - 認証: SAML、OAuth, etc.
  - コンテンツマネジメント: Word Press, etc.
- アプリケーション

- 安全なウェブサイトの運用管理に向けての 20 ヶ条 〜セキュリティ対策のチェックポイント〜
  https://www.ipa.go.jp/security/vuln/websitecheck.html
- 安全なウェブサイトの作り方
  https://www.ipa.go.jp/security/vuln/websecurity.html

質問

例えば、Web ページを公開した後に、セキュリティ要件、例えば、一部のページは認証が必要、一部のページはアクセス元を制限、などを追加することを考える。どのような、問題が発生するだろうか。

例: ネットワーク

- ネットワークの位置づけの整理
  - インターネットとの接続の有無 (方向も)
  - 接続機器の範囲
  - 内部で行われる業務が要求するセキュリティ強度
- 対策の整理
  - IDS などの境界の防御
  - 接続機器の認証
  - 接続機器の動作に対する監査
  - 内部への統一的認証の必要性

基準の必要性

- セキュリティ機器の導入時に、機能・性能を保証する
  - 暗号の強度
  - 認証・認可の強度
  - 不正読み取りへの耐性
- 契約時に、相手側の体制を確認する
  - 組織的な対応
  - 教育と監査
  - 点検と評価
- 組織のセキュリティレベルを標準化する
  - 組織内の最も弱いところが狙われる

国際標準: ISO/IEC 15408

アメリカ、カナダ、欧州で別々に策定されてきたものを、1999 年に統合

1. 概要及び一般モデル
   - セキュリティ要求仕様書
   - セキュリティターゲット: 脅威分析、対策方針等
2. セキュリティ機能要求事項
   - 通信や暗号などの機能要件
3. セキュリティ保証要求事項
   - 信頼性を保証するための要件
   - 開発、配布、テストなど

日本政府の調達でも要求する場合がある。

https://www.ipa.go.jp/security/jisec/about_cc.html

国内標準: ISMS

- 個別の問題毎の技術対策だけではない
- 組織のマネジメントとして自らのリスク評価
- 必要なセキュリティレベルの設定
- 計画的に資源配分してシステムを運用する

JIPDEC(日本情報経済社会推進協会) が認証を実施

CRYPTREC暗号リスト: 電子政府推奨暗号リスト

- 電子政府における調達のために参照すべき暗号のリスト
- https://www.cryptrec.go.jp/list.html

ISMAP: 政府情報システムのためのセキュリティ評価制度

- 政府が求めるセキュリティ要求を満たしているクラウドサービス
- https://www.ismap.go.jp/

質問

重要情報を扱うシステムの構築を発注する際に、発注先の情報セキュリティ対策の状況を知る必要があるのはなぜでしょう。

セキュリティポリシーの必要性

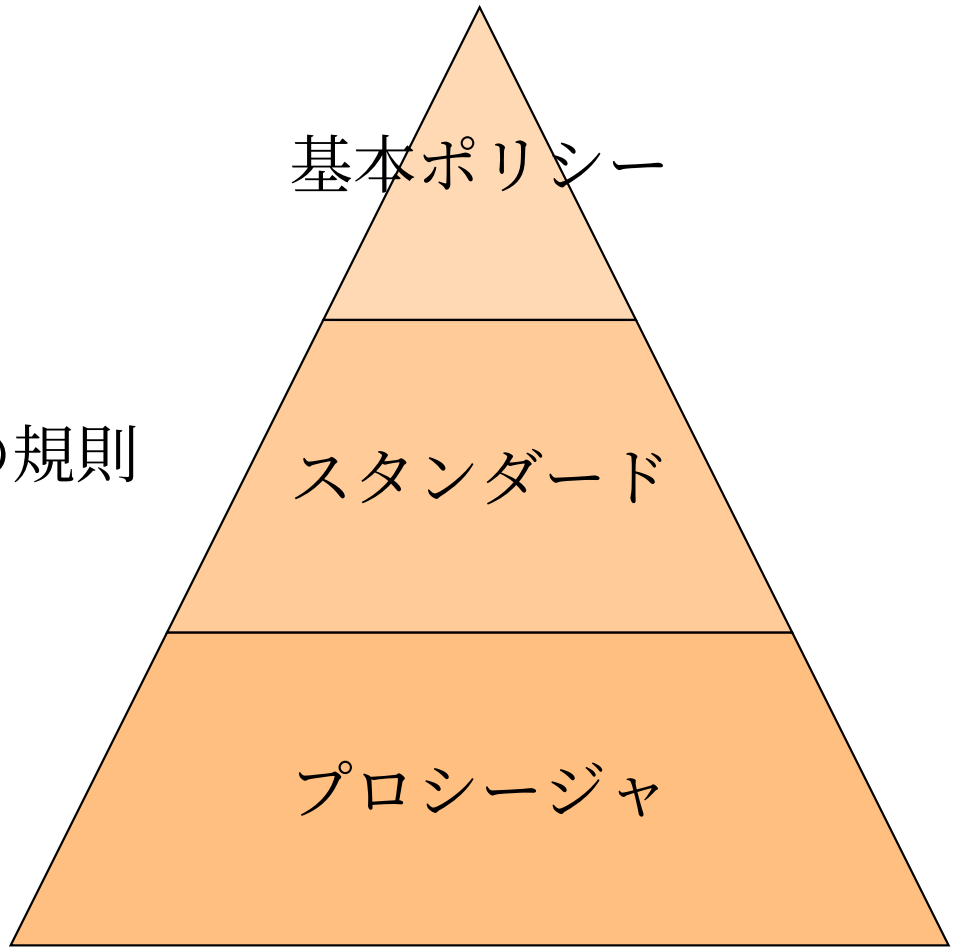
- 90 年代までの電子計算機に対する対策
  - 計算機室に対する入退室管理
  - 文書管理規定
- インターネット時代には不十分
  - 物理的対策
  - 技術的対策
  - 人的対策
- 組織として、セキュリティに対する意思を示す必要

セキュリティポリシー

- 情報資産をどのように保護するかの方針
- 目的
  情報システムの企画、開発、運用、利用の指針を組織のメンバーに伝達し、遵守させる
- 対象
  - 情報そのもの
  - 情報システム、ネットワーク
  - 情報の作成・加工、保管、運搬、出力などの過程
  - 設計や企画書などの紙の書類も含む

セキュリティポリシーの階層

- 基本ポリシー
  組織の基本方針
- スタンダード
  情報管理やシステム運用の規則
- プロシージャ
  より、詳細な手順



セキュリティポリシーに関する国内基準など

発行元	名称
FSA	金融機関等におけるセキュリティポリシー策定のための手引書
旧通商産業省	情報システム安全対策基準 コンピュータ不正アクセス対策基準 コンピュータウィルス対策基準 ソフトウェア管理ガイドライン システム監査基準
警察庁	情報システム安全対策指針
IPA	情報処理技術者スキル標準
内閣サイバーセキュリティセンター	政府機関の情報セキュリティ対策のための統一基準
国立情報学研究所	高等教育機関の情報セキュリティ対策のためのサンプル規程集

政府機関等の情報セキュリティ対策のための統一基準

1. 総則
2. 情報セキュリティ対策の基本的枠組み
3. 情報の取扱い
4. 外部委託、クラウド利用
5. 情報システムのライフサイクル
6. 情報システムのセキュリティ要件
7. 情報システムの構成要素
8. 情報システムの利用

https://www.nisc.go.jp/policy/group/general/kijun.html

課題

「政府機関等の情報セキュリティ対策のための統一基準」のうち、「1.2 情報の格付の区分・取扱制限」を読みなさい。