

セキュリティ技術評価

情報セキュリティについて

- "完璧な対策"は無理だが、ある程度の対策は(世間体的にも)必要
- どのレベルまで対策をすれば良いか？を示すために様々な企画や制度が制定されている

ISO/IEC 15408

- セキュリティ技術を評価する規格
(JIS規格ではJIS X 5070)
- CC (Common Criteria) コモンクライテリア
とも呼ばれ、次のような概念を掲げている

①ST (Security Target)

- セキュリティ基本設計書
- 利用者が自分の要求仕様を文書化したもの

②EAL (Evaluation Assurance Level)

- 製品の保証要件を示したもの
- 製品やシステムのセキュリティレベルを客観的に評価するための指標
- EAL1 (機能テストの保証)からEAL7 (形式的な設計の検証及びテストの保証)までであり、数値が高いほど保証の程度が厳密

JISEC

(ITセキュリティ評価および認証制度)

- Japan Information Technology Security Evaluation and Certification Scheme
- IT関連製品のセキュリティ機能の適切性・確実性をISO/IEC 15408に基づいて評価， 認証する制度
- 第三者機関 (評価機関)が評価し， IPA (情報処理推進機構)が認証する

JCMVP

(暗号モジュール試験及び認証制度)

- 暗号化機能, ハッシュ機能, 署名機能などのセキュリティ機能を実装したハードウェアやソフトウェアなどから構成される暗号モジュールが, セキュリティ機能や内部の重要情報を適切に保護していることについて評価, 認証する.
- 製品認証制度の一つとしてIPAによって運用

PCI DSS

- クレカ情報の安全な取り扱いのために
JCB, American Express, Discover, マスターカード, VISAの5社が共同策定したクレカ業界の
グローバルセキュリティ基準
- カード会員情報を格納及び処理する全組織を対象としており、安全なネットワークの構築や維持、カード会員データの保護などに関する要件を具体的に定めている。

SCAP

- IPAセキュリティセンターが開発した，情報セキュリティ対策の自動化と標準化を目指した技術仕様のこと
- 以下の6つの標準仕様から構成されている

①脆弱性を識別するためのCVE (共通脆弱性識別子)

- 個別製品中の脆弱性を対象として， 米政府の支援を受けた非営利団体のMITRE社が採番している識別子
- 脆弱性検査ツールやJVNなどの脆弱性対策情報提供サービスの多くがCVEを利用

②セキュリティ設定を識別するためのCCE(共通セキュリティ設定一覧)

- システム設定情報に対して共通の識別番号「CCE識別番号 (CCE-ID)」を付与，セキュリティに関するシステム設定項目を識別する.
- 識別番号を用いることで脆弱性対策情報源やセキュリティツール間のデータ連携を実現する.

③製品を識別するためのCPE (共通プラットフォーム一覧)

- ハードウェア, ソフトウェアなど, 情報システムを構成するための共通の名称基準

④脆弱性の深刻度を評価するためのCVSS(共通脆弱性評価システム)

- 情報システムの脆弱性に対するオープンで包括的、汎用的な評価手法
- 脆弱性の深刻度を同一の基準の下で定量比較できるようになる
- ベンダー，セキュリティ専門家，ユーザなどの間で，脆弱性に関して共通の言葉で議論できるようになる

④補足 CVSSの3つの視点

- 基本評価基準 (Base Metrics)
脆弱性そのものの特性を評価する視点
- 現状評価基準 (Temporal Metrics)
脆弱性の現在の深刻度を評価する視点
- 環境評価基準 (Environmental Metrics)
製品利用者の利用環境も含め、最終的な脆弱性の深刻度を評価する視点

⑤チェックリストを記述するためのXCCDF (セキュリティ設定チェックリスト記述形式)

- セキュリティチェックリストやベンチマークなどを記述するための仕様言語

⑥脆弱性やチェックリスト設定を チェックするためのOVAL (セキュリティ検査言語)

- コンピュータのセキュリティ設定状況を検査するための仕様

CWE (共通脆弱性タイプ一覧)

- ソフトウェアにおけるセキュリティ上の弱点の種類を識別するための共通の基準
- 多種多様な脆弱性の種類を脆弱性タイプとして4種類に分類し, CWE識別子 (CWE-ID)を付与して階層構造で体系化

View, Category, Weakness(脆弱性),

Compound Element(複合要因)

脆弱性検査

- システムを評価するために脆弱性を発見する検査のこと
- ペネトレーションテスト
 - システムに実際に攻撃して侵入を試みる手法