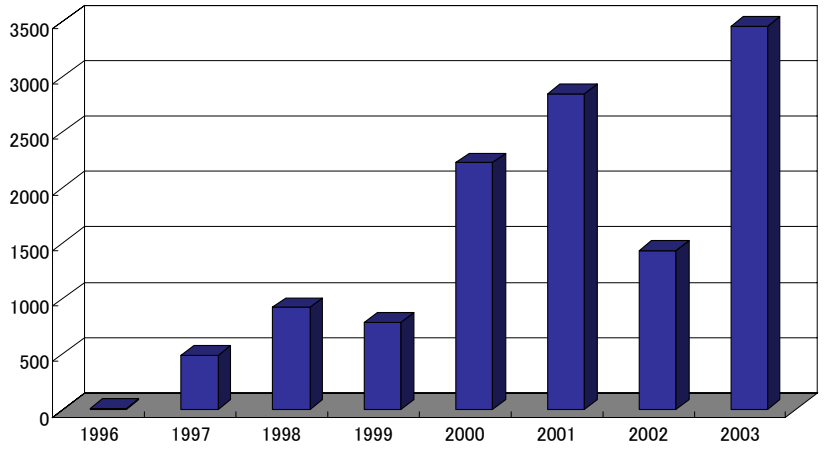
脆弱性の基礎知識

JPCERT/CC
JPNIC
(株)インターネットイニシアティブ
歌代和正

JPCERT/CC

- Japan Computer Emergency Response Team Coordination Center
  - 緊急事態への対応
  - コンピュータセキュリティインシデントに関する調整、対応の協調、連携など
- 1996年10月設立の民間の非営利団体
  - 1992年頃からの非公式な活動が母体
- 2003年3月有限責任中間法人化
- 脆弱性関連情報取り扱い指定機関
- FIRST メンバー
  - National IRT としての認知
  - 国内他組織参加の促進,



セミナー内容
脆弱性の基礎知識

10月4日

1. Webの脆弱性
2. 脆弱性キーワードを読み解く
3. Buffer Overflowのケーススタディとデモンストレーション

10月5日

1. 脆弱性情報流通体制
2. プロトコルの脆弱性
3. プロトコルの脆弱性の実例

ソフトウェア等脆弱性関連情報取扱基準

脆弱性

ソフトウエア等において、コンヒ･ュータウイルス、コンヒ･ュータ不正アクセス等の攻撃によりその機能や性能を損なう原因となり得る安全性上の問題箇所。

ウェフ･アフ･リケーションにあっては、ウェフ･サイト運営者がアクセス制御機能により保護すべき情報等に誰もがアクセスできるよ うな、安全性か･欠如している状態を含む。

Microsoft TechNet

- セキュリティの脆弱性とは、製品の適切な使用による場合でも、攻撃者によるユーザーシステムに対する特権の不正行使、操作の制限、システム上のデータの損傷、および許可されていない信頼の偽装を防止不能にする、製品に含まれる問題である。
  http://www.microsoft.com/japan/technet/archive/community/columns/security/essays/vulnrbl.mspx

IT用語辞典

- 脆弱性
  - コンピュータやネットワークなどの情報システムにおいて、第三者が保安上の脅威となる行為(システムの乗っ取りや機密情報の漏洩など)に利用できる可能性のあるシステム上の欠陥や仕様上の問題点。
  - システムの脆弱性となるのはハードウェアの欠陥やソフトウェアのバグが多いが、こうした明白な欠陥だけが脆弱性になるわけではなく、開発者が予想しなかった利用形態や設計段階での見落としなど、形式的には欠陥とはならない潜在的な問題点が脆弱性として後から認知されることも多い。(後略)
    (http://e-words.jp/)

GMITS: Guidelines for the Management of IT Security

（情報セキュリティ事典より）

- 資産 (asset)
  - 組織に対して価値を持つもの
- 影響 (impact)
  - 好ましくない事故の結果
- リスクマネジメント (risk management)
  - 資産に影響を及ぼす不確かな事象を識別、制御、除去、または低減する総合的なプロセス
- セーフガード (safeguard)
  - リスクを低減する具体策、手順、またはメカニズム
- 脅威 (threat)
  - システムまたは組織に危害を与える好ましくない事故の潜在的な原因
- 脆弱性 (vulnerability)
  - 脅威によって影響を受ける資産または資産グループの弱さ
    (*保護されていないネットワーク接続、訓練や教育されていないユーザ、災害を受けやすい地域にあるなどの資産に対する弱点*)

ISO/IEC 15408

（情報セキュリティ事典より）

① 所有者（owner)―情報資産の持ち主

② 対策（countermeasures)―リスクを低減するための手段

③ 脆弱性（vulnerabilities)―・・資産の中や周辺環境、管理体制、精度などに内在し、損失を発生しやすくさせたり、拡大させる要因

④ 脅威エージェント（threat agents)―資産を悪用したり、損害を与えようとするもの

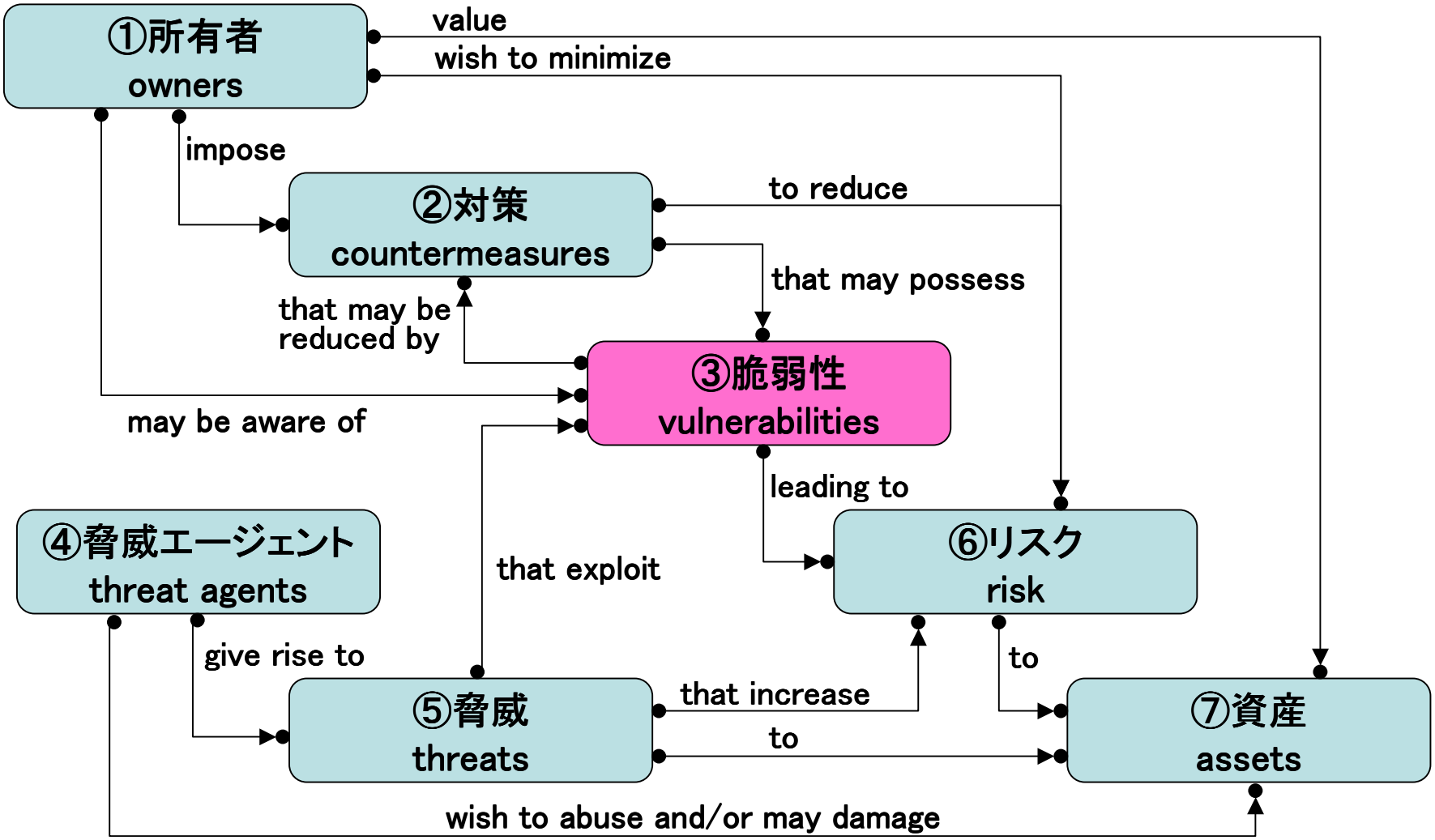
⑤ 脅威（threats)―損失を発生させる直接の原因

⑥ リスク（risk)―脅威と対策が与えられた環境において、脆弱性をつかれたり、脅威が有害になる可能性

⑦ 資産（assets)―情報システムやそのサービス、あるいは情報そのもの

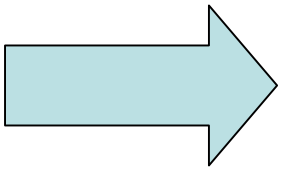
ISO/IEC 15408

（情報セキュリティ事典より）

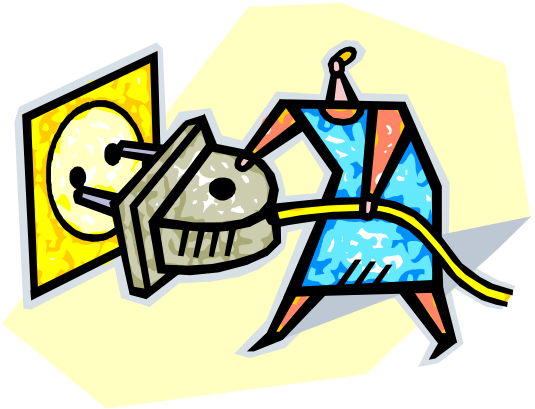


脆弱性に対する見方

- 利用者の視点
  - 同じ脆弱性でも資産、脅威、リスク等の環境によって捉え方は大きく異なる



③脆弱性
vulnerabilities



脆弱性に対する見方

③脆弱性
vulnerabilities

- 提供者の視点
  - 様々な利用者による多様な利用形態を想定する必要がある

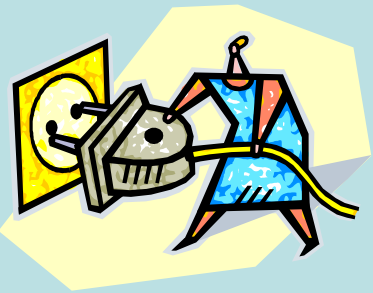
脆弱性に対する見方

社会としての脆弱性

総合的な環境としての脆弱性

システムの脆弱性

製品の脆弱性



システムの脆弱性

製品の脆弱性

システムの脆弱性

製品の脆弱性