標的型攻撃を想定した対策のあり方

2015年10月2日

株式会社 日本HP
佐藤慶浩

自己紹介

佐藤　慶浩（さとう　よしひろ）

株式会社 日本HP　チーフ・プライバシー・オフィサー

元　内閣参事官補佐・情報セキュリティ指導専門官（民間併任）

（内閣官房　情報セキュリティセンター）

【社外の活動】

IT総合戦略本部パーソナルデータ検討会技術検討ワーキンググループ　構成員

経済産業省 個人情報保護ガイドライン検討委員会　委員

厚生労働省医療等分野における番号制度の活用等に関する研究会　構成員

杉並区　住基ネット運用監視委員会　委員長

世田谷区　情報公開・個人情報保護審議会　構成員

経済産業省 IT融合フォーラム パーソナルデータワーキンググループ　元構成員

JIPDEC　プライバシーマーク運営要領改正委員会　元委員

JIPDEC　ISMS適合性評価制度技術専門部会　委員

ISO/IEC JTC1/SC27 WG5 プライバシー小委員会　元主査、現エキスパート

情報ネットワーク法学会　元・副理事長

デジタル・フォレンジック研究会　理事

【その他】

http://yosihiro.com/profile/

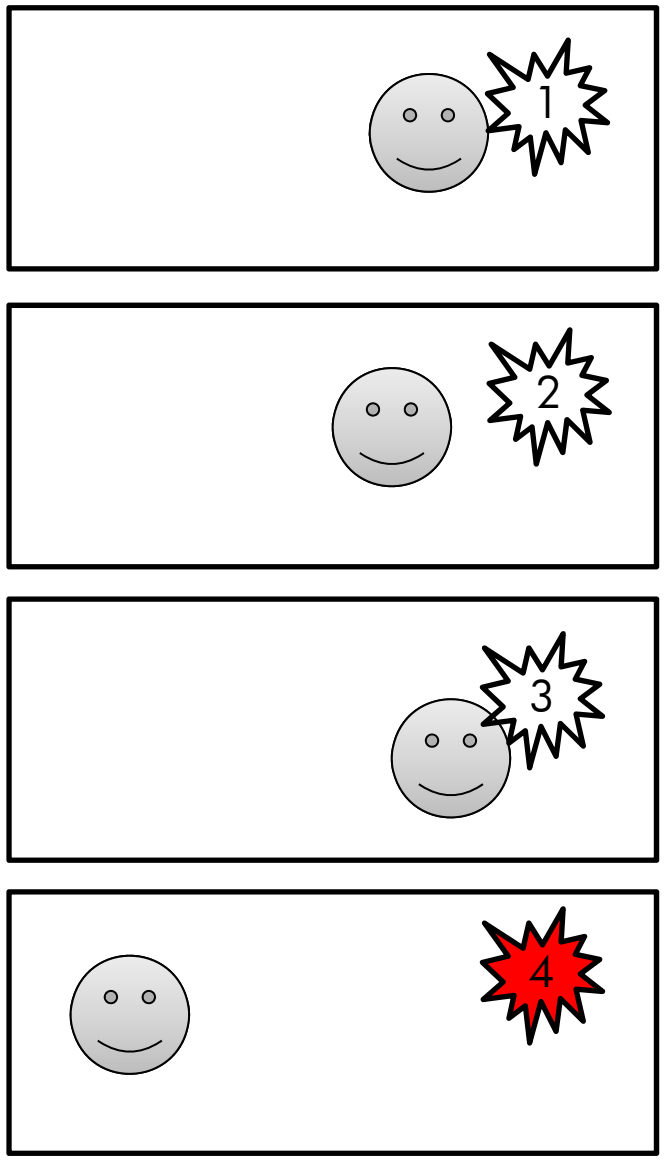
目次

無差別攻撃と標的型攻撃との違い

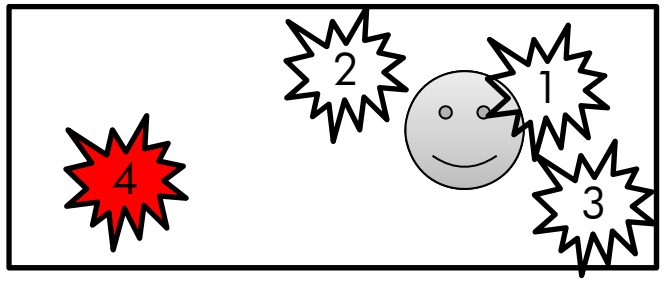
無差別攻撃の特性と対策

標的型攻撃の特性と対策

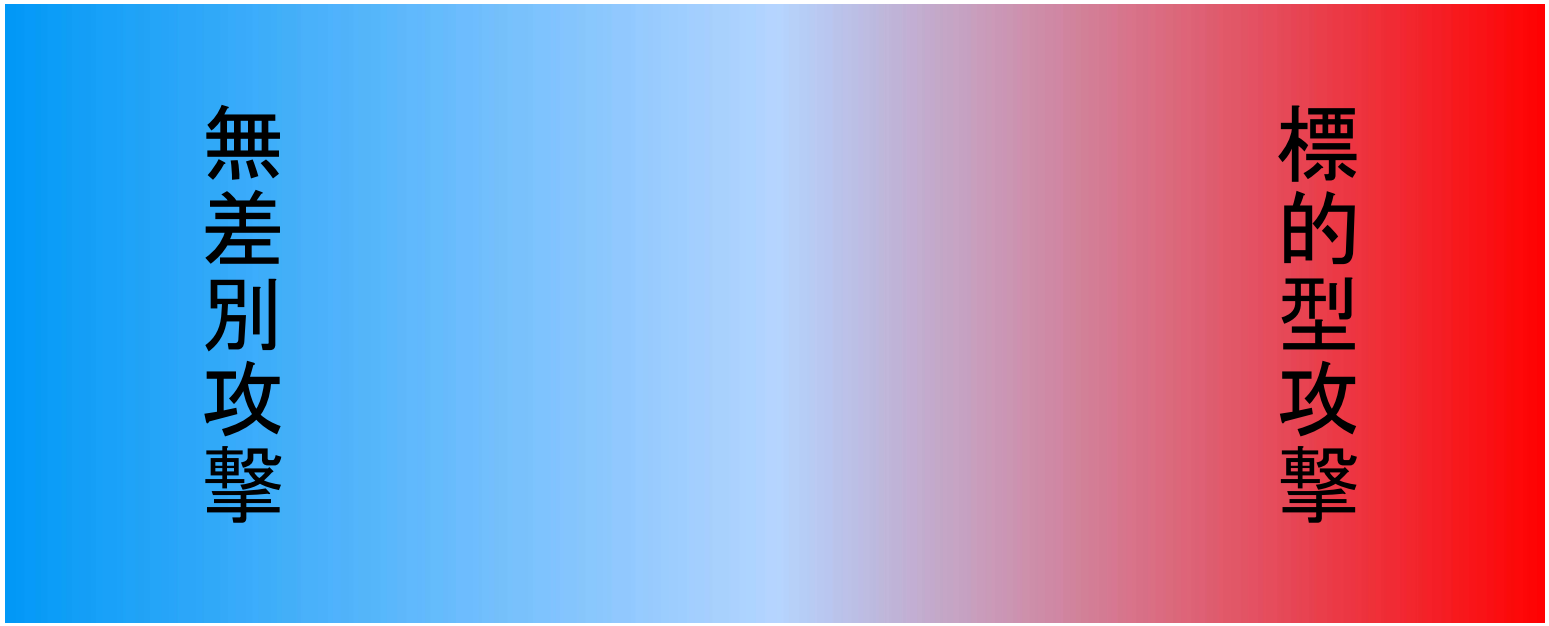
無差別攻撃



標的型攻撃



無差別攻撃と標的型攻撃との違い



無差別・・・・・特定分野・・・・・特定組織
多数・・・・・・・十～百・・・・・・１箇所
１回・・・・・・・・・・・・・・・・・・・・・・・際限なし
０秒・・・・・・・・・・・・・・・・・・・・・・・３７ヶ月

無差別攻撃の特性と対策

特性

成功事例の多い攻撃を選択する

無差別に共通の攻撃をする

その対策を怠っている組織で攻撃を成功させる

攻撃に失敗すれば別の組織への攻撃に移る

対策＝ワクチン接種方式

一般的にすべきとされる対策を実施する

他組織での事故から対策を学び実施する

標的型攻撃の特性と対策

特性

標的組織の環境と対策を調査する

標的組織の脆弱性を推定して環境に応じた攻撃をする

攻撃に失敗すれば別の脆弱性を探って、成功するまで標的を繰り返し攻撃する

標的型攻撃の特性と対策

対策＝基礎体力向上方式

攻撃させない
　　→ゲームホイッスルは敵が持っている
　　→止まない雨はある
攻撃を成功させない
　　→マルウェア検出の限界
　　→被害未遂なら、攻撃は止まない
攻撃が成功しても被害を少ない環境にする
　　→攻撃の検出は困難
　　→アノマリ・アクセスの検出
　　→従事者による不正行為の被害防止

不正行為の類型と対策

許可されていない者による不正行為（通称：外部犯）

悪意あり

– 無許可の行為
  •技術面：アクセス制御による防御・多重の防御

許可された者による不正行為（通称：内部犯）

悪意なし

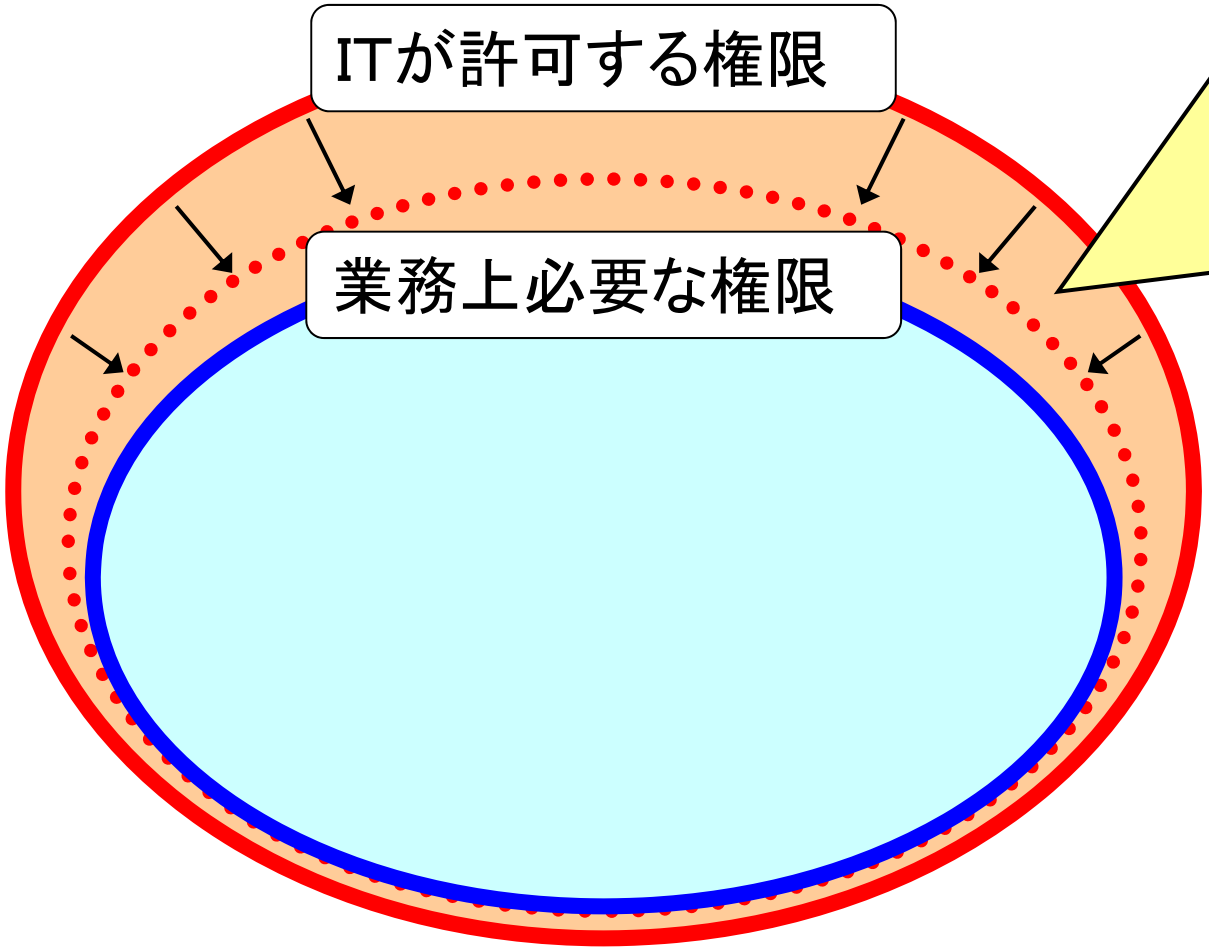
– 誤操作・過失
  •誤操作を軽減する設計
  •啓発、教育、訓練

悪意なし　悪意あり

– 権限の悪用
  •運用面：許可する権限の最少化
  •技術面：監視による抑止効果
  •技術面：アノマリ・アクセス（非通常行動）の検出

不正行為の類型：権限の悪用

許可する権限の最小化



不必要な権限
↓
最小化
5W1H
誰が
いつ
どこで
何を
どんな目的で
どのように

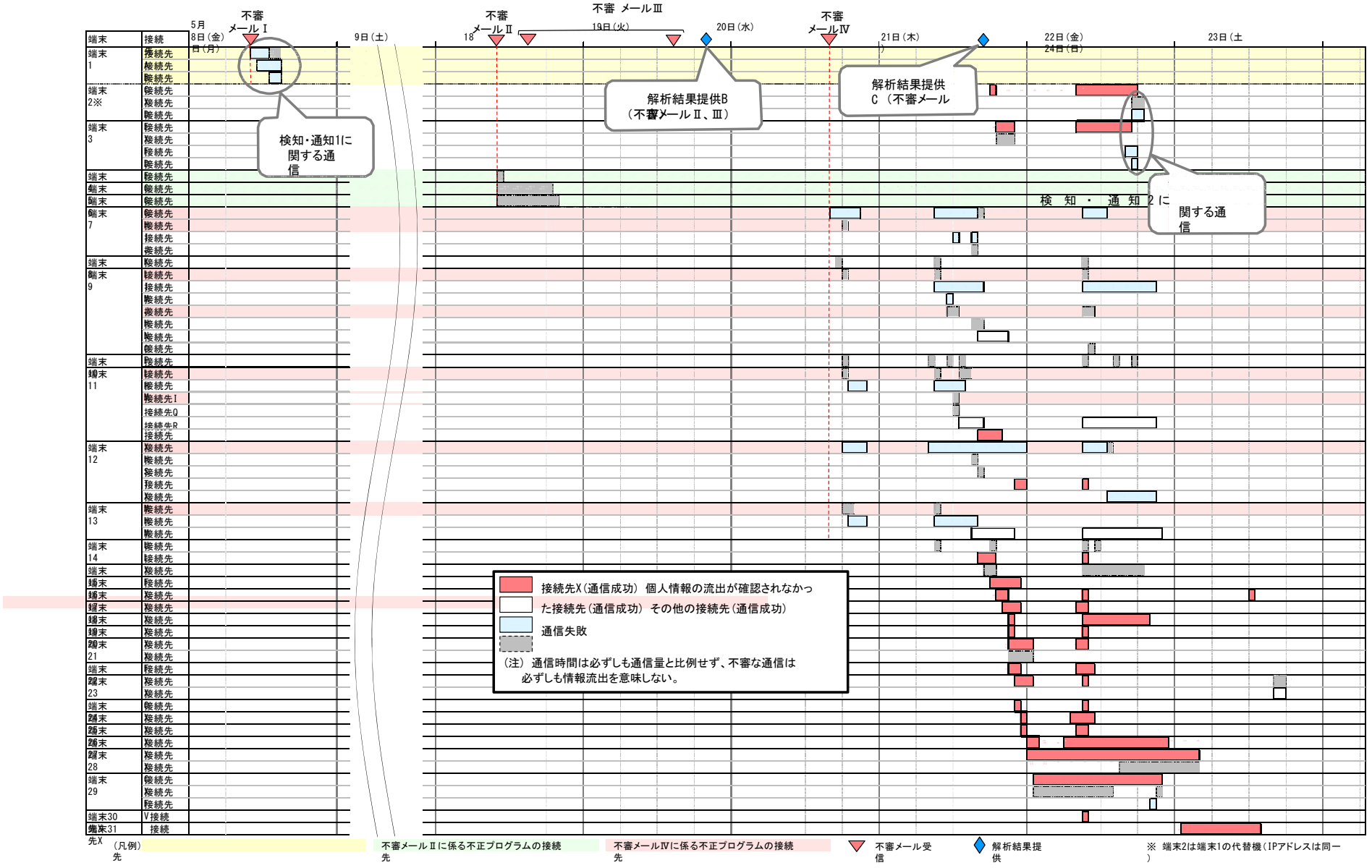


図 2 感染端末と不審な通信

標的型攻撃の特性と対策

対策＝基礎体力向上方式

攻撃させない

→ゲームホイッスルは敵が持っている

→止まない雨はある

攻撃を成功させない

→マルウェア検出の限界

→被害未遂なら、攻撃は止まない

攻撃が成功しても被害を少ない環境にする

→攻撃の検出は困難

→アノマリ・アクセスの検出

→従事者による不正行為の被害防止

→事務処理：情報/基幹系の整理・定型処理化

→管理作業：RBA(Run Book Automation)

標的型攻撃を想定した対策のあり方

対無差別攻撃

ワクチン接種方式による　ー流行、外的、CISO

網羅性のある多層防御によるセキュリティ対策

対標的型攻撃

基礎体力向上方式による　ー免疫力、内的、CIO

業務計画に基づく堅牢なITシステムの構築

　アノマリ監視は障害監視、リソース予測などの観点としても動機付けるのがよい