S-1
「標的型攻撃と インシデントレスポンス」

文京学院大学
浜　正樹

基本概念

「インシデント」とは

- 組織が定めるセキュリティポリシーやコンピュータの利用規定に対する違反行為
- インシデント例
  - 不正アクセス、Webサイト改竄、DoS、情報窃取、コンピュータ侵入

「標的型攻撃」とは

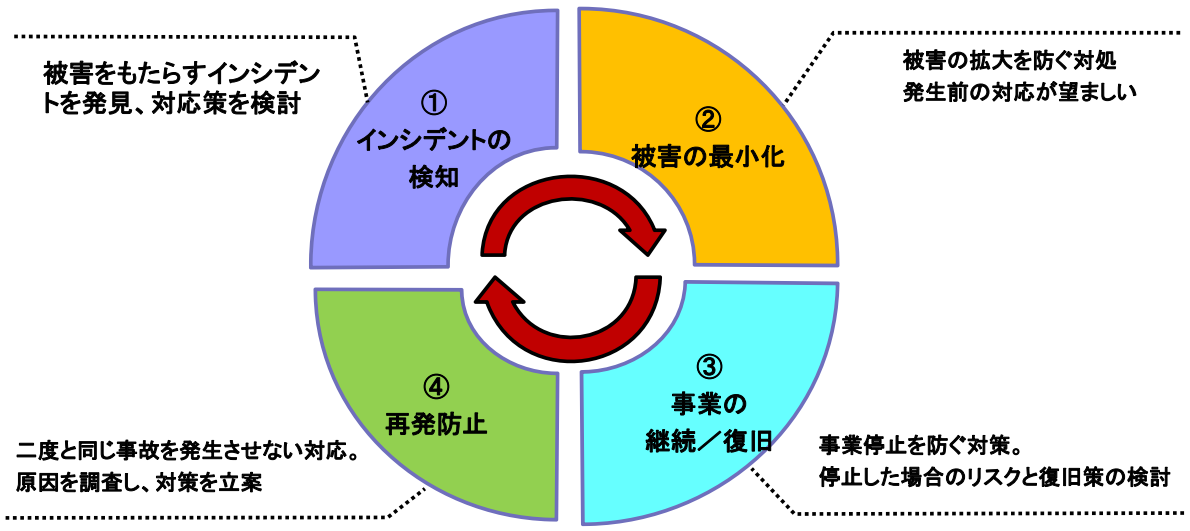
- 特定の組織・個人の所有する機密情報の搾取を目的とするインシデントの1種
- 目的を達するまで、長期に亘って・何度でも攻撃する点が特徴

標的型攻撃に対する
インシデントレスポンス

インシデントレスポンスの目標

- 標的型攻撃の確認
- 正確な情報収集の促進
- 対応戦略決定のための要因収集

インシデント対応サイクル



引用： 日経ネットワーク 2014.07 P46

方法論 [1]

1. 準備
2. 標的型攻撃の検出
3. 初期対応
4. 対応戦略の策定
5. 被害システムの複製
6. 被害・痕跡調査

方法論 [2]

7. セキュリティ対策の実施
8. ネットワーク監視
9. 復旧
10. 報告書の作成

初期対応の目的

- 被害の概要を把握
- 対応戦略決定のための要因収集
- 被害拡大の防止

初期対応における確認事項

- 標的型攻撃の痕跡
- 被害を受けたシステム
- 関係しているユーザー
- 業務継続に与える影響

対応戦略の策定

- 攻撃者の活動監視
- 被害システムの分離
- システム復旧
- 漏洩情報の割り出し

対応戦略の決定

- 継続調査と被害システムの分離
- 専門機関への依頼
- 経営陣からの承認受諾

総合演習について

総合演習（演習方法）

- 標的型攻撃インシデントを想定
- グループワーク
  - テクニカルコース受講者2名とマネジメントコース受講者2名
- 検知から被害の拡大防止までを検討

総合演習（内容）

- 標的型攻撃の確認（テクニカルコース）
- 対応手順の確認と報告（マネジメントコース）
- 対応戦略決定のためのディスカッション