MWS2022プレミーティング

インシデント現場の実情

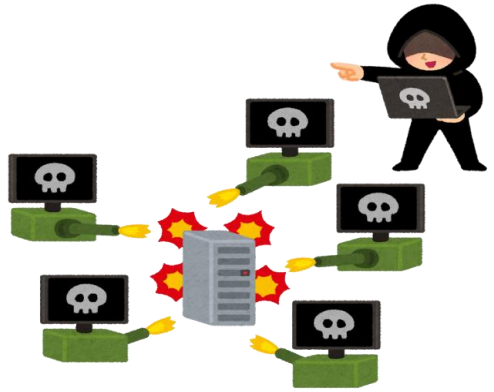
日立システムズ
折田 彰

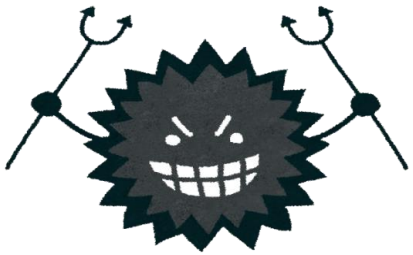
インシデント対応とは

セキュリティインシデント

事業運営を危うくする情報セキュリティを脅かす事象

- 不正アクセス
- マルウェア感染
- 情報漏洩
- DoS/DDoS攻撃
- など





インシデント対応支援

事業運営の影響を最小限に抑え、早期に通常状態に戻すこと

- 事実確認、状況整理
- 被害拡大防止
- 影響範囲の特定、原因調査
  （ログ解析、フォレンジック、マルウェア解析など）
- 再発防止と復旧

インシデント対応でよくある問題点

(1) 影響調査の未実施

- 影響範囲の調査が行われないケースが多い

- 被害が目に見えにくいインシデント
  - 単体システムへの不正侵入
  - システムの動作に影響を与えないマルウェアによる感染など

- 再発防止策だけを実施して復旧
  - パスワード変更、FW設定、Windowsアップデート、AVフルスキャン

- 後に横展開や内部に重要なデータが格納されいていたなどが発覚
  - 発生して数週間～数ヵ月後に急に調査が始まるが、既に大半の痕跡が消えている

(2) 保全の不備

発生当時の情報が保全されていない

- FW, Proxy などの通信ログが保全されていない
  - 通信量や設定によっては、数時間～数日しか残っていないケースあり
- 侵害されたアカウントや不審なアカウントの削除
  - アカウントのユーザフォルダも一式削除
- 検知したマルウェアや設置された怪しいファイルの削除
  - 隔離ではなくファイル削除

(3) 管理情報の更新不備

システムやネットワークなどの管理情報が更新されていない

- システム変更（合併・新拠点、DX、リモートワーク対応など）
  - IPアドレスの論理的、物理的な場所が特定できない(日本? 海外拠点?,データセンタ?)
  - どういったシステムなのか特定できない(サーバ?PC?VPN?など)
- 担当者(自組織担当者・委託業者など)の異動、契約更新・停止
  - 管理者が誰なのか
  - 自社管理、委託業者管理なのか
  - 運用契約、保守(ハードウェア、ソフトウェア)などの契約状況が不明

(4) セキュリティ対策の不備

基本的なセキュリティ対策を行っていれば防げていたインシデントが大半

- パスワード設定
  - 強度が弱い、各システムで同じパスワードを利用
- 放置された古い脆弱性
  - アップデート、パッチ未適用
  - 脆弱性のある古いソフトウェアやOSの使用
- セキュリティ設定の不備
  - FWの設定不備で許可されている（外向きは全て許可など）
  - AV 導入されていない、スキャン停止、シグネチャアップデートされていない