TOP SECRET

MISSION 5

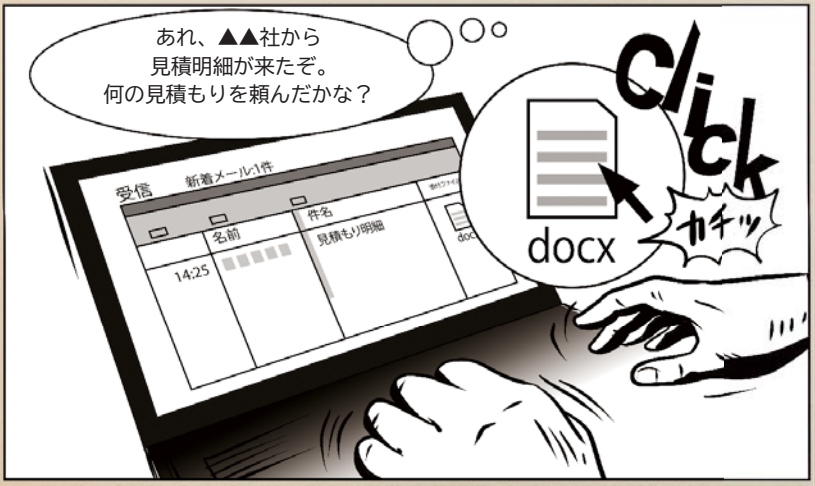
やってみよう! サイバー攻撃対策シミュレーション

SCENE 01

サイバー攻撃前夜

SCENE 02

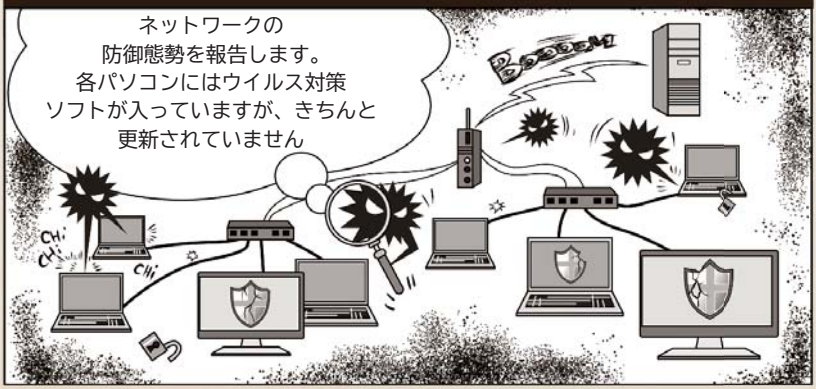
攻撃発生その瞬間

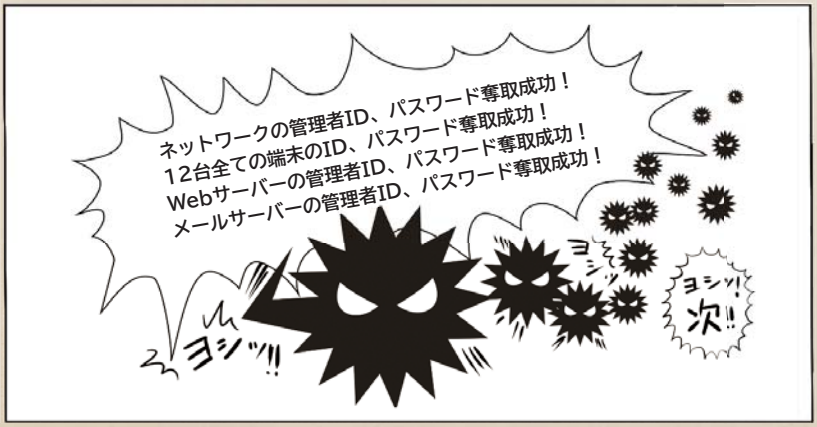


SCENE 03

サイバー攻撃直後

よおし、標的型メールを開いたぞ。
さあ、活動開始だ

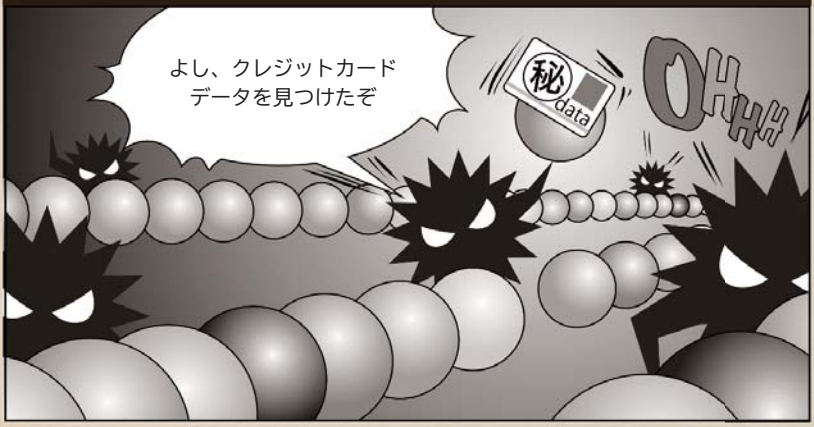


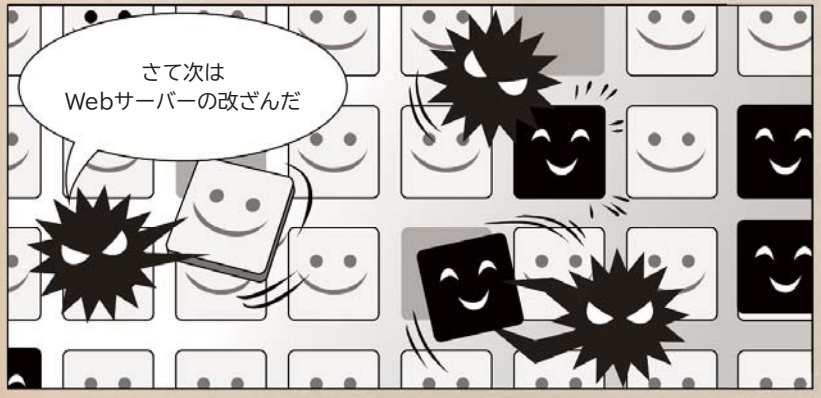


SCENE 04

潜入拡大

クレジットカードの個人情報を取得。クレジットカードを自由に使うためにセキュリティコードなどを盗み取る





SCENE 05

顧客への被害の拡大
取引先への被害の拡大

フィッシングサイトでセキュリティコード情報を窃取。
取得した個人情報を使ってキャッシングで現金を引き出す

●●食品卸売株式会社からの請求明細のメールを装い、
標的型メールの攻撃

SCENE 06

サイバー攻撃の発覚

さあ、あなたならどうしますか？

ACTION 1 原因と被害範囲の調査を自社で実施できるかどうかを判断する

標的型攻撃に代表される企業ネットワークに対する外部からの攻撃や、Webアプリケーションの改ざん、不正アクセスなどのサイバー攻撃の発生時に、本格的な調査（フォレンジック〈法的〉調査、ウイルスの不正プログラムの解析、ログの分析など）、復旧支援と再発防止策のアドバイスを支援するセキュリティ会社があります。

ACTION 2 原因と被害範囲の調査を依頼する

SCENE 07

原因が判明 ウイルス感染が原因

さあ、あなたならどうしますか？

ACTION 1 ネットワークからの切断

ACTION 2 感染ウイルス・不正プログラムの駆除

- OSは最新バージョン自動更新をチェック
- アプリケーションも最新の状態に
- データは必ずウイルス対策ソフトで複数チェック

ACTION 3 各機関への連絡・関係先への報告

SCENE 08

再発防止策の作成

さあ、あなたならどうしますか？

ACTION 1 物理的および環境的セキュリティを再検討する

ACTION 2 社員教育など人的セキュリティを強化する

SCENE 09

復旧回復

さあ、あなたならどうしますか？

ACTION 1 情報漏えいについての発表

ACTION 2 再発防止の恒久的対策

ACTION 3 不審なログオンや通信の監視

不自然な通信をしているプログラムがないか、外部から不正なログオンが行われていないか、監視します。