

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



INDEX

Mission

Mission 2

Mission 3

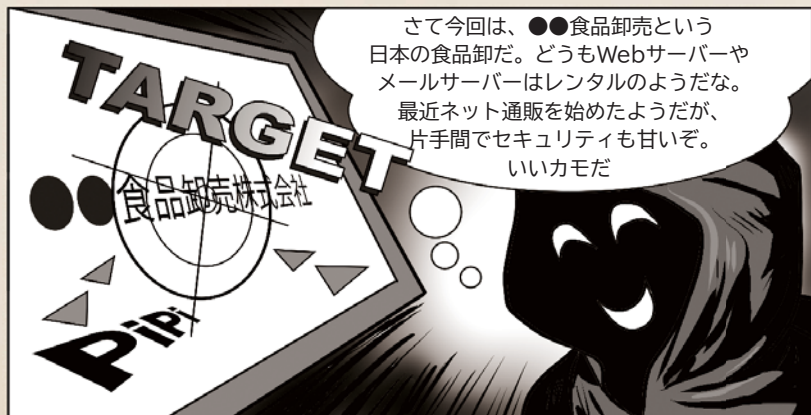
Mission 4

Mission 5

info

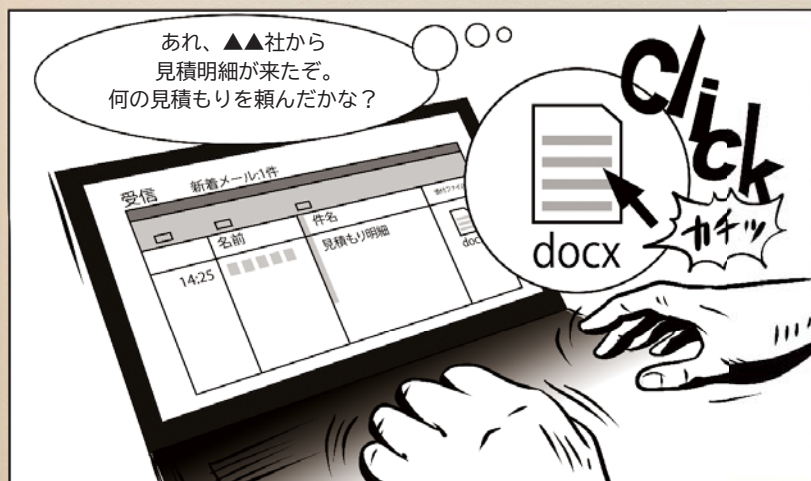


サイバー攻撃前夜





攻撃発生その瞬間



INDEX

Mission 1

Mission 2

Mission 3

Mission 4

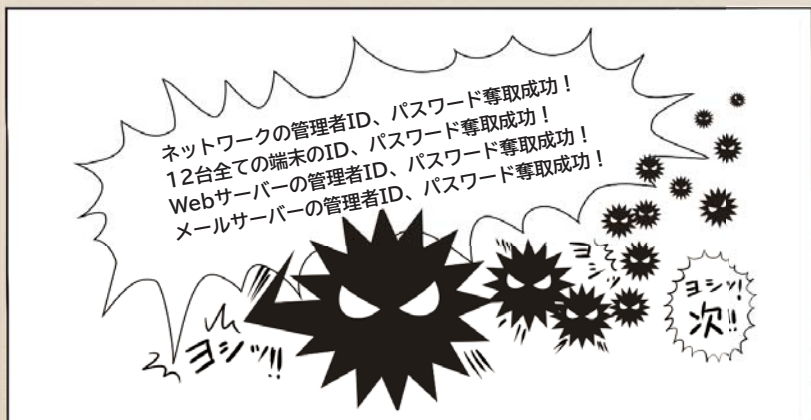
Mission 5

Info



サイバー攻撃直後

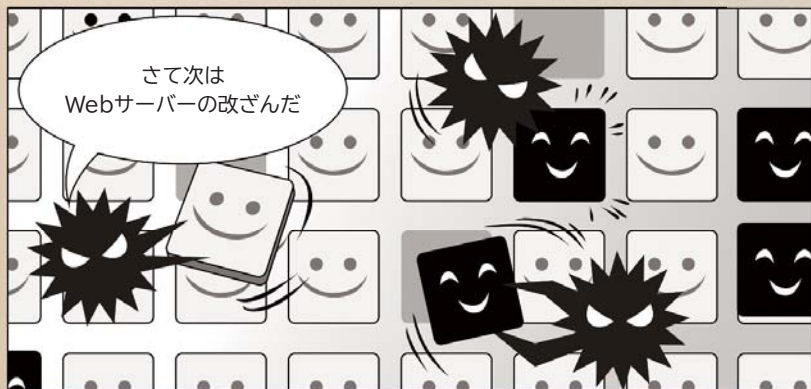
よし、標的型メールを開いたぞ。
さあ、活動開始だ





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



INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

Info



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





サイバー攻撃の発覚



さあ、あなたならどうしますか?

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

Info

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





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?

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

Info

ACTION
1

ネットワークからの切断

いや、それでは
メールも送れなくなって
業務が中断してしまう

ネットワークから
切断して感染を駆除する作業
を進めます

このままでは、どんどん感染
を拡大させてしまいますよ

ACTION
2

感染ウイルス・不正プログラムの駆除

一応、感染ウイルス
と不正プログラムは
駆除しました

また、各端末のウイ
ルス対策ソフトは最
新版に更新しました

ええー！

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
最新の状態で

データは必ずウイルス対策
ソフトで複数チェック

しかし、これだけ
では安全とはいえません。
感染した端末は全て
初期化します

ACTION
3

各機関への連絡・関係先への報告



再発防止策の作成



さあ、あなたならどうしますか？



INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

Info

ACTION
1

物理的および環境的セキュリティを再検討する

何をやらなければ
いけないのでしょ
うか



まずは、個別のウイルス
対策だけでなくネットワーク
全体の統合セキュリティ機器を
導入したり、アクセス管理の設
定を行ったりなど基本的なこと
を確実にやっていきましょう

ACTION
2

社員教育など人的セキュリティを強化する

今回の攻撃ではウイルス
対策ソフトの自動更新を停止して
最新版にしなかったり、安易に添
付ファイルを開いてしまったりなど、
社員のITスキル不足も原因の1つ
です。社員教育も必要ですね



分かりました

それと多少なりとも
サイバーセキュリ
ティのことが分かる
人材を育成すること
も必要です





復旧回復



セキュリティ対策を軽く
見ていたために、結果的には
費用が高くなりました。



さあ、あなたならどうしますか？

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

Info

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。

