

INDEX

Mission 1

Mission 2

Mission 3

Mission 4

Mission 5

Info

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





サイバー攻撃前夜



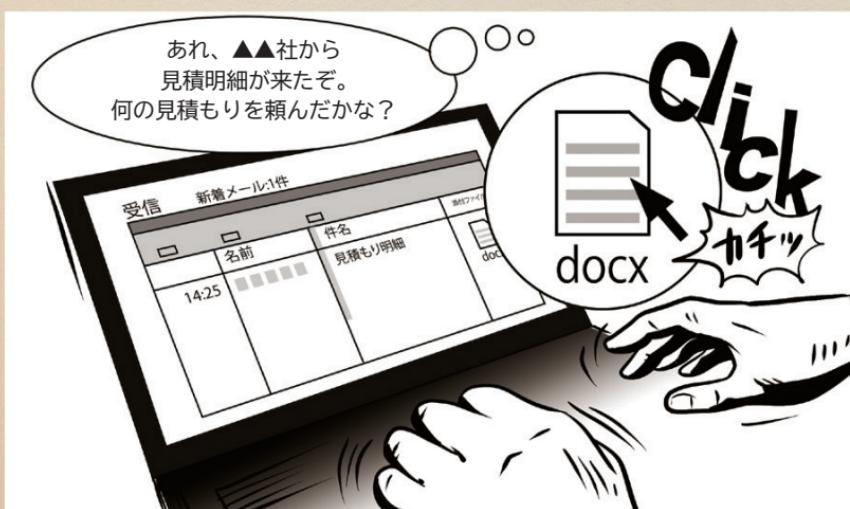


攻撃発生その瞬間

まずは、この会社の取引先をかたって標的型メールを送ってみるか。
件名とファイル名は「見積明細」でいこう



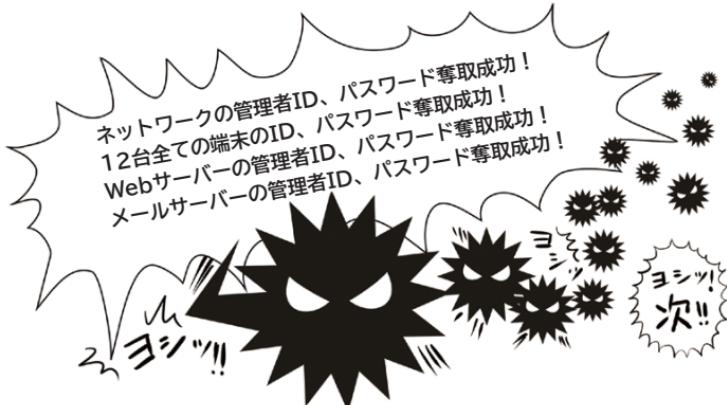
あれ、▲▲社から
見積明細が来たぞ。
何の見積もりを頼んだかな？



**SCENE
03**

サイバー攻撃直後

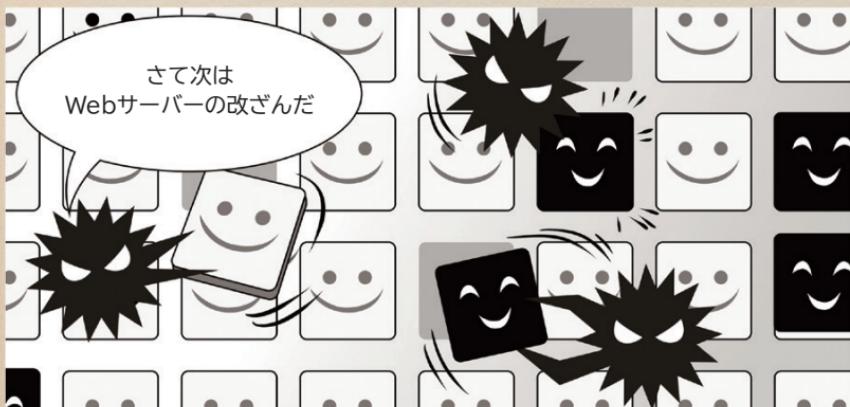
よおし、標的型メールを開いたぞ。
さあ、活動開始だ





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





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

**ACTION
2**

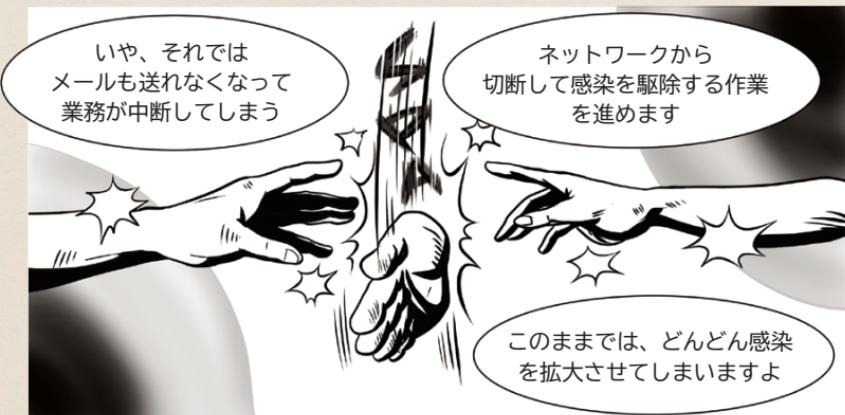
原因と被害範囲の調査を依頼する





原因が判明 ウイルス感染が原因



**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

ええー！

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

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？



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

管理者

まずは、個別のウイルス
対策だけではなくネットワーク
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

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

分かりました



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

毎回ログイン
しなければならないが、
安全のために仕方がないね

**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。



大切なのは社内意識の向上！ ～感染を狙うメールに注意～





経営者にとってメールの安全な運用は他人事ではない!

コンピューターウィルスやマルウェアは、以下のような経路から感染する。

- ・USB機器からの感染
- ・ファイル共有、アプリからの感染
- ・ウェブ閲覧からの感染 など

これらは、システム設定などにより使用を禁止することで回避できる。しかし、ビジネスツールであるメールを一切禁止することは現実的ではない。加えて、メールを悪用した攻撃の中には人の心理的な隙や行動ミスをついた、システム設定だけでは対応が難しい手口も存在する。

メールを発端とするサイバー攻撃の中には、企業の事業継続に多大な影響を与えるものもある。自社がそのような当事者にならないためにも、定期的な勉強会や訓練を実施するほか、経営者自身も率先して参加するなど、社内全体で危機意識を共有し、個々のリテラシー向上を図っていくことが何より大切だろう。

