



あなたの会社は**感染防止対策**できてますか?!

今回は、コンピュータを扱う上で脅威となる「**マルウェア**」について説明します。



マルウェア (Malware) とは？

「Malicious (悪意のある)」と「Software (ソフトウェア)」を語源とする造語で、不正かつ有害なを行う意図で作成された、悪意のあるソフトウェアの総称です。

マルウェアの感染は、データの破壊だけでなく、会社の機密情報の流出に繋がることもあるので事前の対策が必要です。

マルウェアの一例

ウイルス

何らかのファイルに感染し、おかしい動作やファイルの破損等を実行するプログラムです。ファイルの一部を不正に上書きして感染し、感染したファイルを複製して増殖します。



ワーム

ワームは、自身が増殖して、ファイルの破損等を実行するプログラムです。感染して増殖する点ではウイルスと同じですが、ワームは、寄生するファイルを必要とせず増殖します。



トロイの木馬

無害のファイル等を装ってコンピュータ内部へ侵入し、攻撃者が意図した動作を侵入先で密かに実行させるプログラムです。

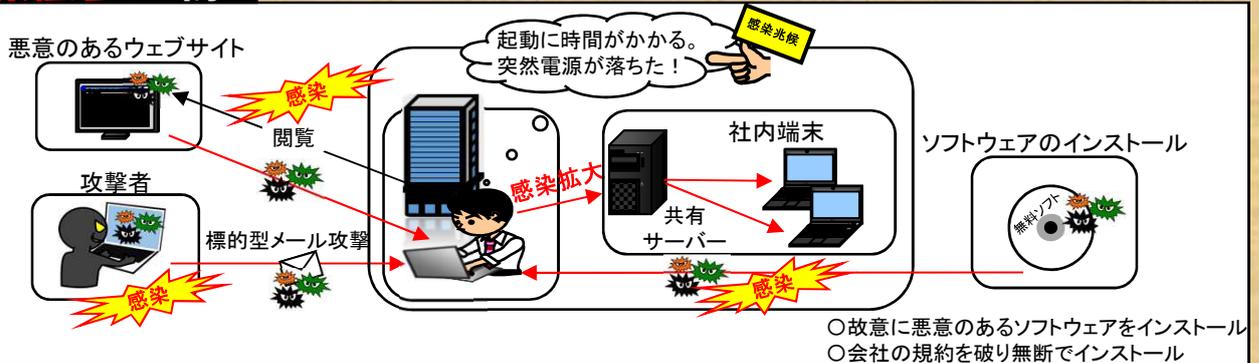


キーロガー

データの破壊・改ざんではなく情報収集を目的としており、キーボードの操作内容を記録させるプログラムです。パスワードが悪用されて、会社の機密情報が流出するおそれがあります。



感染経路の一例



☆SEAGULL通信からのアドバイス☆

マルウェアの感染防止対策において最も重要なのは、マルウェアが**「侵入する前に対策する」**ということです。

近年のマルウェアは、高度化・巧妙化しており、機密情報を抜き取るなどの悪意の目的を持ち、感染兆候の潜在化により、旧来のような「**あからさまな感染兆候**」がないこともあるので、気付いた時には被害に遭っている、又は被害に遭ったことにすら気が付かないという場合があります。

各事業者の情勢に応じて、「不審なメールを開封しない、怪しいサイトは閲覧しない、OSやソフトウェアを常に最新の状態にする、ファイアウォールを導入する」などの事前のセキュリティ対策を徹底しましょう。



▼ SEAGULL事務局 (外事課内) ▼

〒231-8403 横浜市中区海岸通2丁目4番 神奈川県警察本部

相談窓口 Email : seagull@police.pref.kanagawa.jp

