FireEye

すべての始まりは ONE

101通に1

通が悪意のあるEメール[1]

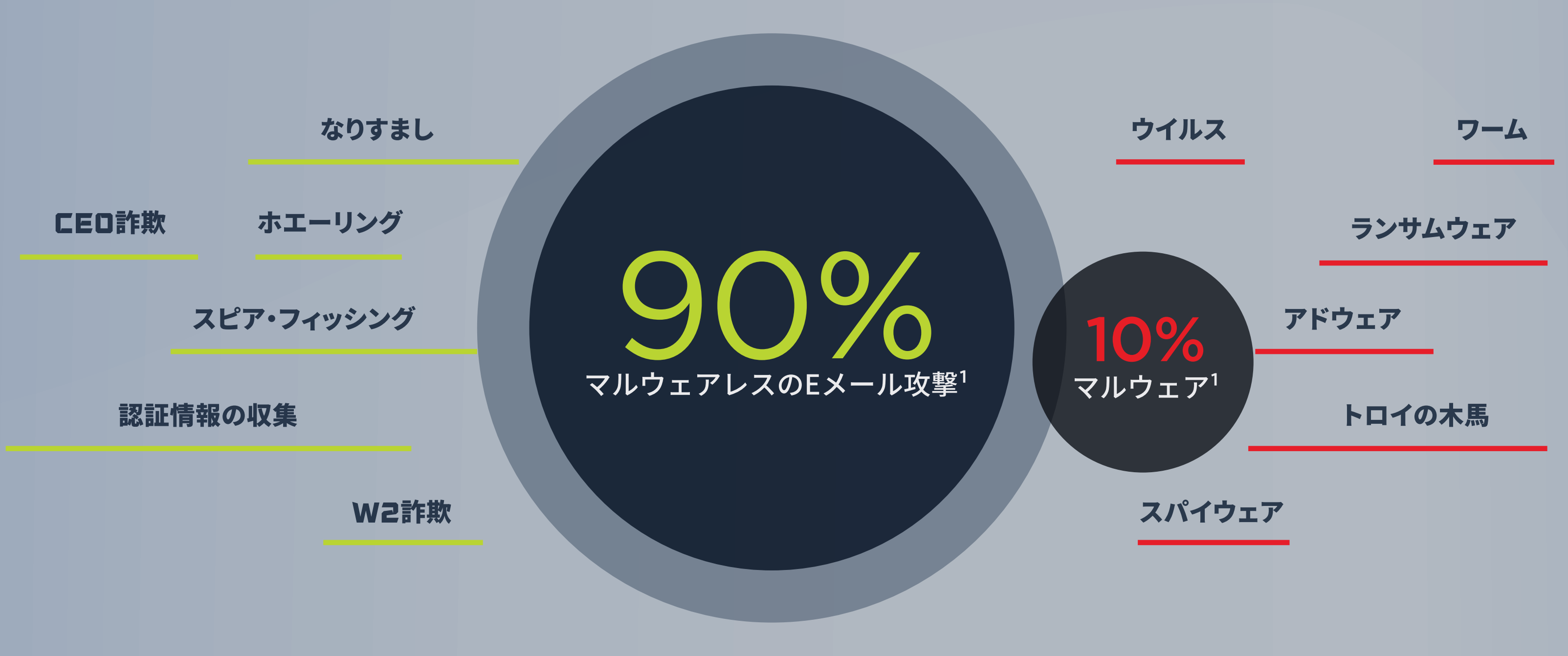
サイバー犯罪の91%は Eメール[2]から始まります。組織への侵入に必要なのはたった1通のEメールです。

Eメールはサイバー攻撃で最も一般的な攻撃経路です。
FireEyeは、Eメール・トラフィックのサンプルを分析して、サイバー犯罪者の攻撃トレンドを特定し、大切なお客様企業を守るためのEメール・セキュリティ・ソリューションを強化しました。

---

[1] FireEye Email Threat Report, September 2018
[2] Radicati Group Email Statistics Report, 2017–2021

サイバー攻撃の手法



マルウェアレス攻撃
信頼できる差出人や企業になりすまし、ユーザーをだまして企業情報や資産を提供させます。こうした攻撃では通常、偽のログイン・ページ、不正なリンク、偽のリクエストなどが使われます。

マルウェア攻撃
Eメールに不正なファイルを添付して、ユーザーのコンピュータへのアクセスを試みます。マルウェアは、PDFやDOCなど様々なファイルに埋め込まれます。

65%
フィッシング詐欺の増加（2017年）[1]

125億ドル以上
CEO詐欺攻撃による企業の損失[1]

46%
ランサムウェア攻撃のうち、きっかけがEメールだったもの[1]

2017年のランサムウェアによる被害額は**50億ドル（約5,600億円）**[2]

---

[1] FireEye Email Threat Report, September 2018
[2] Cybersecurity Ventures, 2017

脅威の排除

FIREEYEが疑わしいメールを阻止する方法

1. コネクション・レベル
不自然なEメール・トラフィックを検知してブロック
- ブロック・リスト
- 侵害されたIPアドレス
- 不正なドメイン

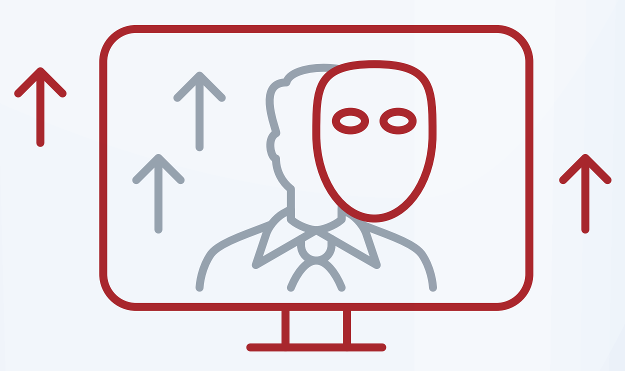
2. コンテンツ・レベル
高度な攻撃を検知してブロック
- 高度なURLセキュリティ対策
- URLの検査
- なりすましの検知

---

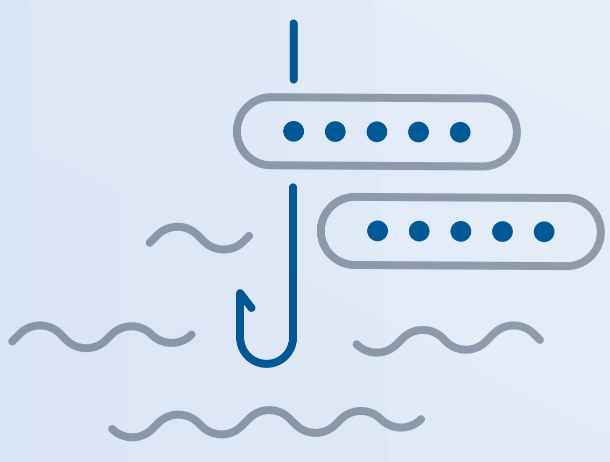
* FireEye Email Threat Report, September 2018

攻撃の変化

マルウェアレス技術を用いて攻撃を行うサイバー犯罪者が増えています。なりすまし攻撃も増加の一途をたどり、よく知る人の名前を詐称する、あるいは受信者のドメインのタイポスクワッティングを利用するなどの方法で攻撃が行われています。



マルウェアの検知に重点を置いたEメール・セキュリティ・ソリューションを導入していても、**サイバー犯罪者は攻撃方法を適応させていき、**組織はCEO詐欺のようなマルウェアレス攻撃にさらされることになります。



フィッシング攻撃の増加
2017年にフィッシング攻撃は65%増加しました。休暇シーズン中だけで30%の増加でした。

モバイル脅威
携帯電話でメールの確認をする人が増えています。ほとんどの場合、携帯メールには差出人の名前のみが表示され、アドレスは表示されません。そのため、攻撃者がユーザーをだまして、知人からのメールであると簡単に思い込ませることができます。

詳細は、**www.FireEye.jp/email-tactics**からFireEyeのレポートをご覧ください。

FireEye