

急増し高度化・巧妙化する標的型メール攻撃

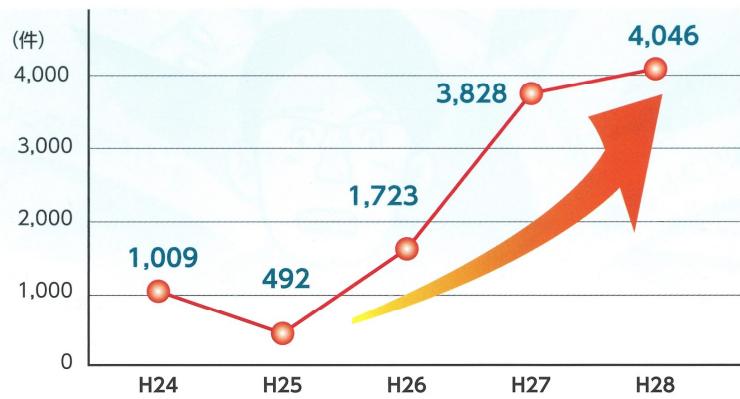
サイバー攻撃に気付かず被害拡大…!?

中小企業にとっても、ITの利活用は、業務の効率化による収益性向上だけでなく、新しい製品やサービスを創造し、企業価値や国際競争力を高めていくための必須条件となっています。

一方で、企業が有する個人情報や重要な技術情報等を狙うサイバー攻撃は年々

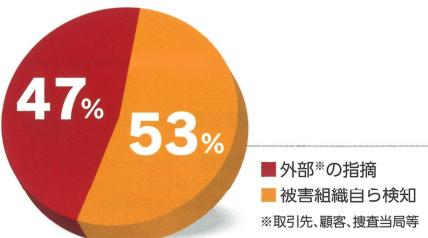
増加の傾向にあります。また特定の組織を狙う標的型攻撃を中心としてその手口や攻撃手法は高度化・巧妙化しており、組織は攻撃を受けたことに気付かず、攻撃の発覚経緯の約47%は外部からの指摘によるものといわれています。

標的型メール攻撃の件数の推移



出典：平成28年中におけるサイバー空間をめぐる脅威の情勢等について 2017年3月23日（警察庁）

セキュリティ侵害の発覚経緯



出典：サイバーセキュリティ経営ガイドラインVer2.0 2017年11月（経済産業省、独立行政法人情報処理推進機構）



標的型メール攻撃とは

あたかも通常の業務や依頼であるかのように見せかけるメールを送り、添付ファイルを開封させたり、所定のサイトに誘導することにより、PCをマルウェア^(※)感染させる攻撃。

(※) マルウェア=悪意のあるソフトウェアの総称
(例：ウイルス、ランサムウェア等)

近年の標的型メール攻撃の特徴

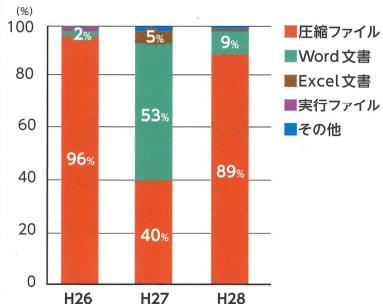
攻撃対象の組織や職員について調査し、周到な準備を行った上で攻撃を実行

- 大多数が非公開メールアドレスに対する攻撃（SNSからも情報収集）
- あたかも業務で普段やり取りしているメールを装うため、件名や文面に業界用語や日常よく使われる表現を使用

人の心理を突いてくる
アプローチ手法を実行

- 送信元メールアドレスは全体の99%が偽装（2017年 警察庁調査）
- 社内の人間や取引先になりすまし、添付ファイルを開かざるを得ない内容
- 心当たりはなくとも興味をそそられる内容

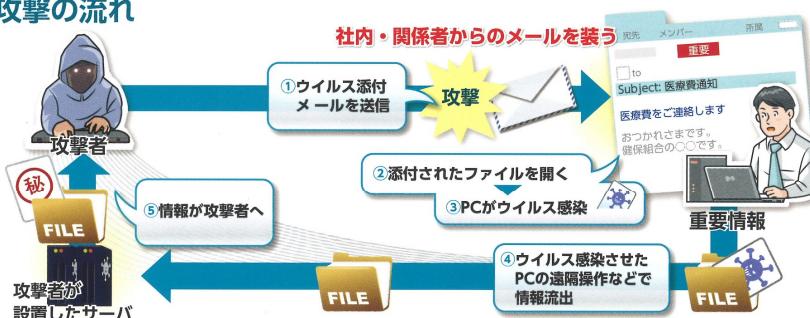
標的型メールに添付されたファイル形式の割合



出典：平成28年中ににおけるサイバー空間をめぐる
脅威の情勢等について 2017年3月23日（警察庁）



攻撃の流れ



事例 標的型メール攻撃の文例

宛先: info@info-test.com
件名: 貴社への就職を希望しております
添付: [履歴書.exe](#)

宛先: info@info-test.com
件名: 【5%OFF】あと3日！全国500店舗で使えるランチクーポン

全国500店舗で使えるランチクーポンを期間限定で配信！

今すぐ詳細を見る
<http://lunch500.com/coupon/XXXXXXX/>

宛先: info@info-test.com
件名: 【重要】Windowsの脆弱性暫定回避策実施のお願い

昨日、Windowsに極めて深刻な脆弱性が発見されました。
今回の脆弱性は、リモートからPC端末を乗っ取ることができてしまう可能性のあるものです。
現時点ではセキュリティパッチが提供されておりませんが、暫定回避策が公表されていますので、下記URLの手順に従って各自で至急対策を実施ください。

<暫定回避策手順>
<http://windows.security/techXXXXXXX/>

宛先: info@info-test.com
件名: ミーティング議事録を送付します
添付: [20171211_MTG議事録.zip](#)

標的型メール攻撃は、「人」が思わずメールの添付ファイルを開いてしまうことやURLリンクにアクセスしてしまうことを前提に作られています。

