

# ☆情報セキュリティ10大脅威 2020☆

「情報セキュリティ10大脅威 2020」は、2019年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約140名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。

※IPA: 情報処理推進機構

昨年 順位	個人	順位	組織	昨年 順位
<b>NEW</b>	スマホ決済の不正利用	<b>1位</b>	標的型攻撃による機密情報の窃取	1位
2位	フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい	5位
1位	クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害	2位
7位	インターネットバンキングの不正利用	4位	サプライチェーンの弱点を悪用した攻撃	4位
4位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害	3位
3位	不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止	16位
5位	ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい（規則は遵守）	10位
8位	インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取	7位
6位	偽警告によるインターネット詐欺	9位	IoT機器の不正利用	8位
12位	インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止	6位

個人では金銭絡みの脅威が、組織では情報取得絡みの脅威が上位を占めています。サイバー攻撃の目的も、直接ウイルス感染させた端末だけではなく、その関係者（取引先）を攻撃するための準備として行われるケースもあり、自分の端末には取られても困る情報は無い、という認識でセキュリティ意識が低いと大変な目に遭うかもしれません。

## BSS通信

～2020年03月号～

もうすぐ東日本大震災から9年が経とうとしています。あらためて、防災への意識や備えは大丈夫なのか？と思っていた矢先に、先月から新型コロナウイルスが猛威を振るい、日本全国への感染拡大が危惧されております。この疾患やウイルスの特徴は徐々にわかってきているとはいえ、まだまだ説明されていない点が多いので、常に情報をチェックすることが重要です。ただし、デマも流れやすいので、きちんとした情報源を抑えておきましょう。（今月は、両面ともに情報セキュリティの題材です。）

## ⚠️ 新型コロナウイルスを題材した攻撃メール(エモテット)に要注意 ⚠️

2020年1月30日に日本経済産業省の独立行政法人IPAより、最新のエモテットの事例が発表されました。

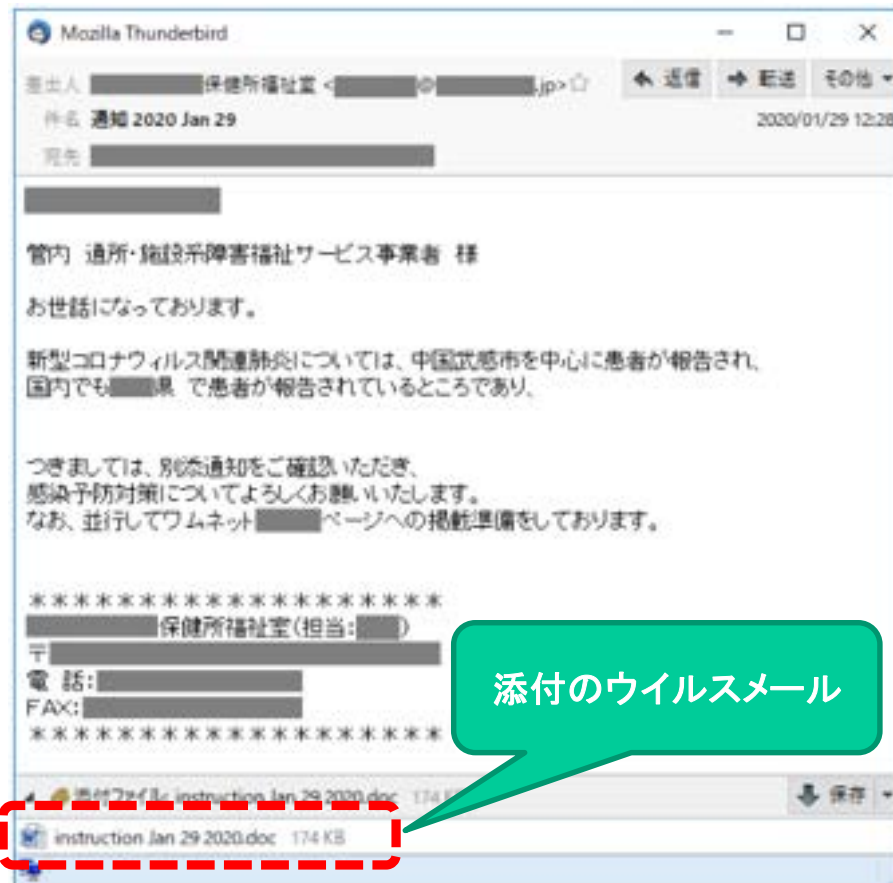
内容は、「新型コロナウイルス対策について」のメールです。メールには、悪意のあるプログラムが仕込まれたWordが添付されていました。

ニュースでも話題になっている新型コロナウイルス。本文を読んで興味を持ち、送信者を気にせずに関いてしまうケースがあります。

実在する企業、団体であっても取引・関係性がない場合はメールを開かないようにしてください。

運用面では「関係のないメールは破棄する運用徹底」「端末のセキュリティプログラム(WindowsUpdateなど)の定期更新」「Wordマクロの自動実行の無効化」ソフト・ハード面では「ウイルス対策ソフト導入」「UTM導入、セキュリティHUB導入」といった多層防御の仕組みでウイルスの侵入を防ぐ、外部への情報漏えいを防げる仕組みが大事になってます。

今一度、職場の環境を見直してみてもいいでしょうか？



サイバー攻撃は日々巧妙化されており「取引企業を語ったメール」や「実在する企業・サービスを謳ったメール」など、人が判断するには限界の部分があります。その部分はセキュリティ対策の専門家に託すのも1つの選択ではないでしょうか？

お問い合わせ

株式会社ビー・エス・サイトー

TEL:018-865-7400

FAX:018-865-7401