MLサイバー山梨 vol.2

企業を狙った標的型メールに注意

標的型攻撃とは、標的の知り合いや取引先を装い悪意のあるファイルを添付したり、悪意のあるサイトに誘導するためのリンク付きメールを送信、パソコンなどの端末をマルウェアに感染させようとする攻撃です。

標的型攻撃は、そのほとんどがターゲットを特定して行われ、銀行口座、仮想通貨、**企業の機密情報などを窃取する**目的で行われています。企業として大きな損害が出てしまう可能性が高いため注意が必要です。またマルウェア感染後、バックドアが設置され、内部に**何度も継続的に不正アクセスし情報を盗み出される**可能性もあります。

■「情報セキュリティ10大脅威 2019」

昨年順位	個人	順位	組織	昨年順位
1位 (*1)	クレジットカード情報の不正利用	1位	標的型攻撃による被害	1位
1位	フィッシングによる個人情報等の詐取	2位	ビジネスメール詐欺による被害	3位
4位	不正アプリによるスマートフォン利用者への被害	3位	ランサムウェアによる被害	2位

IPAの発表した情報セキュリティ10大脅威でも昨年に引き続き1位

サイバーセキュリティ対策

① 業務用端末のＯＳ、ソフトウェアを最新の状態にする
② セキュリティ対策ソフトを導入する
③ 職員や従業員のセキュリティ意識を高めることが重要
　IPAの「標的型攻撃メールの例と見分け方」参照
　<https://www.ipa.go.jp/files/000043331.pdf>
④ 特に重要な機密情報を保存する
　端末をネットワークから遮断する

山梨県警察本部 生活安全捜査課
サイバー犯罪対策室