

覚えておきたい情報セキュリティ&ネットワークのキホン(第2回)

情報セキュリティ事故はどうすれば防げるのか？実際の事故から対策を学ぶ

2022.03.25



企業を円滑に経営していく上で、サイバー攻撃や情報漏えい、不正アクセスやウイルス感染といった情報セキュリティ事故への対策は欠かせないものとなっています。

本記事では過去の情報セキュリティ事故について紹介しながら、事故を未然に防ぐために必要なことを整理します。

情報セキュリティ事故の企業への影響

情報セキュリティ事故が起きた場合、企業の経営にさまざまな影響が懸念されます。例えばサイバー攻撃を受け、社内のネットワークに障害が発生した場合、業務に多大な支障を来します。顧客リストなどの機密情報が漏えいすれば、被害は自社にとどまらず、取引先や顧客などへも広がってしまう恐れがあります。

情報セキュリティ事故の種類

情報セキュリティ事故には、どのようなものがあるのでしょうか？ 独立行政法人情報処理推進機構(IPA)が毎年公開している「情報セキュリティ10大脅威」では、実際に発生した事故を踏まえて、組織への影響が大きかった情報セキュリティ脅威として以下を挙げています。

「情報セキュリティ10大脅威 2022」

※独立行政法人情報処理推進機構(IPA)が2021年に発生した脅威候補を選定したもののから投票で決定(「前回」の順位は独立行政法人情報処理推進機構(IPA)が2020年での脅威候補の順位)

- 1位 ランサムウェアによる被害(前回1位)
- 2位 標的型攻撃による機密情報の窃取(前回2位)
- 3位 サプライチェーンの弱点を悪用した攻撃(前回4位)
- 4位 テレワークなどのニューノーマルな働き方を狙った攻撃(前回3位)
- 5位 内部不正による情報漏えい(前回6位)
- 6位 脆弱性対策情報の公開に伴う悪用増加(前回10位)
- 7位 修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)(前回ランク外)
- 8位 ビジネスメール詐欺による金銭被害(前回5位)
- 9位 予期せぬIT基盤の障害に伴う業務停止(前回7位)
- 10位 不注意による情報漏えいなどの被害(前回9位)

2年連続で3位以内となっているのが「ランサムウェアによる被害(前回1位)」と「標的型攻撃による機密情報の窃取(前回2位)」です。

「ランサムウェア」は、マルウェア(ウイルス)の一種で、感染したパソコンやスマートフォンなどの端末をロックしたり、ファイル

を暗号化したりして、解除と引き換えに身代金(ランサム)を要求するサイバー攻撃です。「標的型攻撃」は、企業や個人に対してサイバー攻撃を仕掛け、情報の奪取・金銭の要求などを行います。

さらに、昨今の新たな脅威として「サプライチェーンの弱点を悪用した攻撃」「テレワークなどのニューノーマルな働き方を狙った攻撃」が挙げられます。前者はターゲットとなる大企業のサプライチェーンの中で、情報セキュリティ対策が甘い企業を踏み台にして、攻撃をかける手法です。後者は、コロナ禍によって急速にテレワークが普及したことで、情報セキュリティ対策が不十分な自宅のネットワーク機器や公衆無線LANの脆弱性を狙った攻撃です。

情報セキュリティ事故の事例

サイバー攻撃は日々、高度化巧妙化しています。情報セキュリティ事故を起こさないためには、実際にどのような手口で発生した情報セキュリティ事故があるのかを把握しておくことが肝要です。ここ数年で報道された事故の事例を紹介します。

マルウェア「Emotet」による情報漏えい

マルウェアによる事故の事例として、2019年頃から大流行した「Emotet」が挙げられます。Emotetはメールに添付されたファイルからパソコンに感染すると、そのパソコンのメールの内容やメールアドレス、パスワードなどを盗み取り、別のユーザーへのなりすましメールや不正ファイル転送などを繰り返します。そのため取引先や顧客などにも被害が拡大します。

2020年には、東京都の企業が運営する通信販売サイトにおいてEmotetの被害が確認され、最大2800件の消費者のメール情報流出が報告されています。あるガス会社では、取引先のパソコンが感染したことで被害を受けました。情報ネットワークでつながる外部の企業に被害が広がった事例です。

従業員の管理ミスによる情報漏えい

ある外食産業に携わる従業員が、帰宅途中に立ち寄った小売店で顧客情報およそ7万件が入ったノートパソコンを紛失。すぐに警察や現場の小売店に連絡を取りましたが、発見には至りませんでした。ある協同組合では、Webサイト更新作業中のミスによって顧客情報およそ2万件を記載した資料が外部から閲覧できる状態になりました。資料はその後、約2カ月半に渡って閲覧可能な状態が続きました。

情報セキュリティ事故の対応策—情報セキュリティを強化する仕組みの導入… 続きを読む