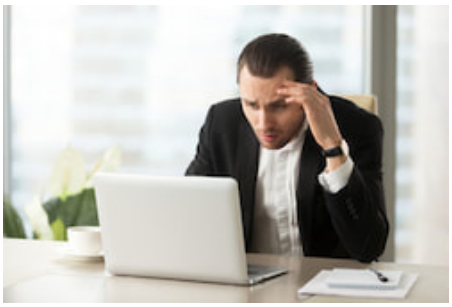
覚えておきたい情報セキュリティ&ネットワークのキホン（第2回）

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 ランサムウエアによる被害（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「ランサムウエアによる被害（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。

「ランサムウエア」は、マルウエア（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。

マルウエア「Emotet」による情報漏えい

マルウエ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ー情報セキュリティを強化する仕組みの導入

Emotetの被害から考える対策

Emotetに代表されるマルウエアの被害を防ぐためには、不審なメールや添付ファイルは開かないことが重要です。サイバー攻撃による被害の多くはマルウエアが原因であり、マルウエア感染のきっかけはメールの添付ファイルや悪意のあるWebサイトへのアクセスなどさまざまですが、Emotetはメールの添付ファイルが主流となっています。

差出人が詐称されていたり、本文にビジネス文面と酷似した内容が書かれているため、受信者はウイルスと見分けがつかずファイルを開いたり、Webサイトを訪問したりしてしまうのです。特定企業にビジネス文面を偽装してメールを配信する標的型攻撃も同様です。

対策としては、メール文面の日本語が不自然ではないか、添付ファイルやURLにおかしな点はないかなど、従業員が不審なメールに気付ける教育をしていくことが重要です。

システム面での対策も必須です。アンチウイルスソフト（Anti-Virus Software）などのマルウエア対策製品をパソコンにインストールすれば自動でアラートを表示し、マルウエアへの感染を防ぐことができます。ランサムウエアへの対策としては、データを定期的にバックアップする仕組みも有効です。

最近ではサイバー攻撃による個人情報の流出や業務妨害に備えるための「サイバー保険」というサービスも登場しています。

従業員の管理ミスから考える対策

従業員の管理ミスによるパソコンの紛失は、テレワークが普及した昨今、あらゆる企業で起こり得る事例です。対策としては、指紋認証システムや顔認証システムなど、本人しか持ち得ない属性を認証キーとして利用する手法があります。

さらに、暗号化ツールを使い、機密情報や個人情報などの重要データは暗号キーがないと解読できないようにすれば、仮にデータが外部へ流出したとしても、その内容の漏えいは防ぐことができます。このほかにも、ノートパソコンを遠隔操作で

きるようにしておき、端末を紛失した際はパスワードを複雑なものに変更し、社内ネットワークへのアクセスを遮断するといった措置が考えられます。

情報漏えいに対応する6つのステップ

これまで説明してきたような情報セキュリティ対策を十分に実施したとしても、巧妙なサイバー攻撃の手口やヒューマンエラー、悪意のある内部不正などによって、情報漏えいが発生する可能性はあります。その際は、下記の6つのステップによって速やかに対応することが重要となります。

ステップ1：情報漏えいの兆候や事実の発見・報告

情報漏えいの事実が確認された場合は、速やかに責任者に報告し、迅速に対応するための体制作りを行います。漏えいの兆候を察知した段階であっても、責任者へ報告を行うことが重要です。

不正アクセスなどにより、社内ネットワークやシステムから情報が漏えいした可能性がある場合は、従業員の不用意な操作により、不正アクセスの証拠が消去されないように注意します。

ステップ2：初動対応

初動対応で行うべきは次の2つの対応です。
・対策本部を設置し、対応方針を決定
・情報漏えいによる二次被害の防止措置

被害が拡大する可能性がある場合には、情報の隔離・ネットワークの遮断・サービスの停止などの措置を取ります。

ステップ3：調査

情報漏えいに対して適切な対応を行うためには、事実関係を調査して情報を整理し、事実を裏付ける情報や証拠を確保する必要があります。この調査は、十分な情報が得られるまで、以降のステップにおいても並行して継続します。

ステップ4：通知・報告・公表など

調査結果によって漏えいの詳細が把握できた後は、関係者へ次のように通知・報告・公表を行う必要があります。
・漏えいした情報の本人や取引先など
漏えいした個人情報の本人には、特別な理由がない限り通知します。
・監督官庁や警察、IPA（独立行政法人情報処理推進機構）など
紛失・盗難・不正アクセス・内部犯行・脅迫など犯罪性がある場合は、届け出ます。
・Webサイトやマスコミなど
すべての関係者に対して個別通知が困難な場合や、広く一般に影響が及ぶと考えられる場合は、自社Webサイトでの情報公開や記者発表などにより公表します。

ステップ5：抑制措置と復旧

情報漏えいによる被害拡大の防止と復旧の措置を行います。加えて、再発防止に向けて具体的な取り組みを行い、停止したサービスやアカウントを復旧します。

ステップ6：事後対応

調査報告書を経営陣に提示し、被害者に対する損害の補償などを行います。そして被害の具合を総合的に判断して、従業員の責任などを見極め、必要であれば処分を実施します。さらに、再び同じことが起こらないよう、抜本的な再発防止策を検討する必要があります。

この上記に挙げた6つのステップは「フォレンジック調査」という手法を用いることで、迅速に行うことができます。フォレンジック調査とは、スマートフォンやパソコンなどの電子機器に残されている履歴やログ情報などを解析・調査することで、ウイルス感染調査や社内不正調査に活用される調査方法です。

フォレンジック調査による対策を行うことで、以下のような対策を講じることが可能です。

(1)情報漏えい発覚時の初動対応
(2)情報漏えいの被害調査や原因特定
(3)原因や被害をまとめた、法的効力を持つレポートの作成

(4) 被害の抑制とデータや業務の復旧支援
(5) 再発防止策の提案・コンサルティング

前述した6つのステップと内容は似ていますが、フォレンジック調査は外部企業に委託できます。このサービスを利用することで「万が一の事態」に速やかに対応することが可能となります。

まとめ

企業経営には顧客、取引先、社会との「信頼」の2文字が欠かせません。しかし、ひとたび情報セキュリティ事故が起きてしまえば、その信頼はいとも簡単に崩れてしまいます。ビジネスを円滑に進めるためには、社内外のさまざまなリスクや脅威に対して、過去の事故事例も参考にしながら、備えておくことが重要です。

※掲載している情報は、記事執筆時点のものです