特集

ますます必要性が高まる 中小企業の情報セキュリティ対策

独立行政法人情報処理推進機構

ICTの活用により経営効率が向上した反面、機密情報の漏えいや金銭的損失など、情報セキュリティに関する被害が多発しています。一方で、中小企業は経営者の情報セキュリティに対する消極的な姿勢や予算の問題などにより、対策があまり進んでいないのが現状です。そこで情報セキュリティ被害の現況や効果的な対応策を、中小企業の情報セキュリティ対策のスペシャリストである、独立行政法人情報処理推進機構の江島 将和氏にうかがいました。

セキュリティセンター
セキュリティ普及開発・振興部
普及啓発グループ　グループリーダー
江島 将和氏

被害届の約6割は中小企業 特にランサムウェアを警戒

近年、サイバー攻撃やコンピューターウイルスなどによる情報セキュリティ被害が深刻化しています。独立行政法人情報処理推進機構（以下、IPA）が毎年公開している「情報セキュリティ10大脅威2024」（図1参照）では、社会的に影響の大きい事案として、4年連続で「ランサムウェアによる被害」が1位に選ばれました。狙われた会社だけでなく、顧客やサプライチェーン※1にまで影響を及ぼしかねないランサムウェアの手口はますます巧妙になり、被害金額も高額化していると警鐘を鳴らしています。

「ランサムウェアとは、身代金を意味するランサムとソフトウェア（ウイルス）を組み合わせた造語で、感染させることでデータを暗号化し、使用不能にして復旧と引き換えに金銭を要求するウイルスの一種です。国内でも最近、大規模な被害のニュースが話題を集めました」（江島氏）

大企業の被害が大きく報道される一方で、2023年上半期に警察庁に提出されたランサムウェアによる被害届の約6割は、中小企業からのものだったと江島氏は言います。

「ランサムウェアの被害を受けやすいのは、実は大企業ではなく情報セキュリティ対策が比較的脆弱な中小企業です。世界的な自動車メーカーが被害を受けた件も、実際に攻撃を受けたのは自動車メーカーに部品を納める会社の子会社でした。同件は、子会社を経由して親会社のシステムがランサムウェアに感染し、部品の生産が停止したことで、結果的に自動車メーカーの国内全工場の稼働が停止する事態にまで発展しました。また、ある大病院では、給食委託事業者のシステムから侵入され、そこからネットワークをたどって病院のシステムが攻撃を受け、電子カルテなどがランサムウェアに感染、暗号化されてしまい、病院はほぼ機能不全状態に陥りました」（江島氏）

被害が深刻化する一方で 変化が見られない危機意識

被害の深刻さが顕著になる一方で、ここ数年中小企業の危機意識や対策にはあまり変化が見られないと、江島氏は指摘します。

「IPAが公開している『2021年度 中小企業における情報セキュリティ対策に関する実態調査』によると、中小企業の3割以上が、直近3年間で情報セキュリティ対策への投資をしていないと回答しています。その理由として、コスト面、費用対効果の見える化をしにくいなどの意見が寄せられましたが、中でも40%以上の企業が『必要性を感じていない』と答えています。2020年度の1年間で情報セキュリティの被害に遭遇したか否かの設問では、84.3%が『被害にあっていない』と答えた一方で、2019年にIPAが中小企業1,000社の協力を得て、各社のシステムにセンサーを設置し、外部からの攻撃調査を行った結果では驚くべきことに、全社のセンサーから何らかのサイバー攻撃の痕跡が発見されました。この結果から、実際に情報セキュリティ被害を受けている企業数は、データ以上に多いのではないかと推測しています。実態調査で『被害にあっていない』と回答した84.3%の企業の中にもサイバー攻撃に気づいていないだけの企業がある可能性は否定できません」（江島氏）

【図1：情報セキュリティ10大脅威2024】

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏えいなどの被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	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
10	犯罪のビジネス化（アンダーグラウンドサービス）

基本的な5か条の対応で 被害の大半は防げる!

情報セキュリティ対策の必要性は認識しても、多くの中小企業にとって、いきなり精巧かつ高予算の対策を施すのは難易度が高いと思われます。そこで江島氏は、できるところから始められる対策として、IPAが提案する「情報セキュリティ5か条」（図2参照）を実行してほしいと語ります。

「第1に、OSやソフトウエアは常に最新の状態に保ってください。サイバー攻撃の被害の多くは、アップデートを行わずセキュリティが脆弱化したシステムが受けています。2番目にウイルス対策ソフトは必ず導入してください。あるいは最近のOSはセキュリティ機能が標準搭載されていますので、活用すると良いでしょう。第3にパスワードの強化を実施しましょう。現在のものより長く、複雑なものに変更してください。また同じパスワードを、複数のサービス間で使い回さないようにしましょう。第4は共有設定の見直しです。設定のミス、従業員の異動や退職後の削除を疎かにすることで、無関係な人に情報を覗き見られるトラブルが増えています。そして最後に、攻撃の手口の最新情報を知ってください。危険を敏感に察知できる知識は、情報セキュリティ被害を防ぐ第一歩です。攻撃者の手口は年々巧妙かつ悪質になっています。しかし、この5か条を実施することで、大半の情報セキュリティ被害は未然に防げると思います」（江島氏）

情報セキュリティ問題は、これからより複雑化していくでしょう。しかも、被害は自社のみに留まらず、顧客やサプライチェーンにまで波及するだけに、ある日突然経営に関わる緊急事態が発生したとしても不思議ではありません。それだけに情報セキュリティ対策は、経営陣が率先して「情報セキュリティ5か条」に取り組み、会社全体の意識を改革する必要があると言えそうです。

【図2：「情報セキュリティ5か条」と対応のポイント】

1 OSやソフトウェアは常に最新の状態にしよう！

OSやソフトウェアのセキュリティ上の問題点を放置していると、それを悪用したウイルスに感染してしまう危険性があります。OSやソフトウェアの製造元は、セキュリティ上の問題を発見した場合、修正プログラムを提供しますので、この修正プログラムを取得して実行することで対応します。

対応のポイント
- ■サポートが終了したOSやソフトウェアは使用しない
- ■OSやソフトウェアが最新かチェックし、OSやソフトウェアの修正プログラム（Windows Updateなど）を実行（アップデート）する
- ■パソコンやルーターのファームウェア※2についても最新かチェックし、最新版に更新（アップデート）する
  ※OS、ソフトウェア、ファームウェアのチェックは定期的に行い、可能であれば、自動アップデートを有効にして更新漏れのリスクを減らす。

2 ウイルス対策ソフトを導入しよう！

ウイルス対策を怠ったデバイス（パソコンやスマホなど）は、ウイルスの攻撃に対して無防備で、感染すると、情報漏えいや不正利用などのリスクが高まります。デバイスからネットワーク経由で、企業のサーバーなどにも感染が広がり、企業の情報漏えいやシステムダウンなどの被害拡大も招きます。

対応のポイント
- ■OSに標準でセキュリティ機能が搭載されている場合※3は、それを使用するのも有効
- ■OS標準セキュリティ機能よりも多くの機能を持ったウイルス対策ソフト製品を導入することが、より望ましい（その場合は評価や信頼性の高い製品を選ぶと良い）
- ■ソフトを導入した場合は、ウイルス定義ファイル（パターンファイル）※4が自動更新されるように設定する

3 パスワードを強化しよう！

パスワードの管理が不適切だと不正ログインの被害に遭う恐れがあります。また、単純で短いパスワードを設定している場合、総当たり攻撃で解明されてしまう可能性が高まるため、パスワードは長く、複雑に、使い回さないようにします。

対応のポイント
- ■大文字・小文字・数字・記号を混ぜて長く複雑なパスワードを設定する
- ■パスワードを使い回さない
- ■二段階認証（パスワード+別の認証を組み合わせる方式）が使える場合は有効化する

4 共有設定を見直そう！

データ保管などのクラウドサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。共有設定が適切に行われていないと、本来アクセスすべきでない社員や外部者が、重要な情報を参照・更新できてしまうリスクが生じます。

対応のポイント
- ■情報の重要度に応じて共有設定、漏えいしてはならない情報は最小限の人のみアクセスできるように設定する
- ■セキュリティ部門担当だけでなく、全社員に共有設定の重要性を周知する
- ■社員の異動や退職時の見直しに加え、定期的に共有設定を見直す

5 脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウイルス付きのメールを送る巧妙な手口が増えています。巧妙になればなるほど、その手口を知らないことには自己防衛が難しくなり、知識不足が、個人情報流出や企業全体に影響するウイルス感染など重大なリスクを増大させます。

対応のポイント
- ■サイバー攻撃の情報を獲得・周知することの重要性を認識する（体制確立）
- ■IPAサイトの「重要なセキュリティ情報」（https://www.ipa.go.jp/security/security-alert/）などで最新情報を日々チェックする
- ■導入しているクラウドサービスなどの提供企業が発信するセキュリティ情報に注意する

（IPA「情報セキュリティ5か条」を基に作成）

※1 サプライチェーン：原材料・部品などの調達から販売によりエンドユーザーに製品が届くまでの一連の流れ。
※2 ファームウェア：パソコン、スマートフォン、通信機器、ゲーム機、デジタル家電など、さまざまなデバイスに組み込まれたハードウェアを動かすためのソフトウェア。
※3 Windows 8 以降はMicrosoft Defender（旧Windows Defender）というセキュリティ対策機能がOSに標準搭載されている。
※4 ウイルス定義ファイル（パターンファイル）：セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル。

IPA

●組織概要
法　人　名：独立行政法人情報処理推進機構
創　　立：2004年（平成16年）
所　在　地：東京都文京区本駒込2丁目28番8号 文京グリーンコートセンターオフィス（総合受付13階）
理　事　長：齊藤 裕
政府出資金：199億9,569万1,983円
事業内容：「サイバーセキュリティの確保」「デジタル基盤の提供」「デジタル人材の育成」を事業の三本柱として、デジタル技術の利用促進により豊かな暮らしを実現し、グローバルコミュニティのメンバーとして、直面する課題の解決に貢献している
URL：https://www.ipa.go.jp/index.html

Webで読もう ユーザ協会 D10040