今月の特集

中小企業のセキュリティ対策
サイト構築ガイドラインを公開

サイバー攻撃で情報漏えいが多発

近年、ECサイトへのサイバー攻撃により個人情報やクレジットカード情報が漏えいする事件が多数発生している。特に中小企業が構築・運用するサイトのセキュリティ対策に課題が多く見られることから、経済産業省と独立行政法人情報処理推進機構（IPA）では2022年度に中小企業のECサイトにおける実態把握を目的とした調査や脆弱（ぜいじゃく）性診断を行った。

最近サイバー被害を受けたECサイト運営事業者20社を対象としたヒアリング調査では、１社当たりの顧客情報の平均漏えい件数は約3,800件、そのうち事故対応費用を支出した19社では、事故対応費用の平均額が約2,400万円に上ったことが分かった。また、20社のうち75％がECサイト構築プログラムやCMS（コンテンツマネジメントシステム）などの脆弱性を放置または最新版へのアップデートを怠っていたことや、90％が保守など運用時のセキュリティ対策を実施していなかったことが分かった。

こうした状況を踏まえ、経済産業省とIPAは、ECサイトの構築・運用に必要なセキュリティ対策とその実践方法を取りまとめた「ECサイト構築・運用セキュリティガイドライン」を作成し、３月16日に公開した。

実行すべき対策を明示

本ガイドラインの最大の特長は、経営者がECサイトにおけるセキュリティ対策の基本を認識できるよう、第１部としてまず経営者向けのメッセージを図表やイラストを用いて伝えていることにある。ECサイトのサイバー被害が経営に及ぼす影響やセキュリティ対策の重要性をデータで示した上で、セキュリティ確保のために経営者が実行すべきセキュリティ対策の基本を７項目で明示した。IPAの「中小企業の情報セキュリティ対策ガイドライン」に記載されている七つの重要項目に基づき、必要な予算と人材の確保や、脆弱性対策のための日常的なセキュリティ運用、緊急時の体制整備などを示し、実務担当者に適切な指示を出せるようにしている。

また、第２部として実務者向けに、ECサイトの構築時、運用時それぞれにおけるセキュリティ対策要件を示し、さらに付録としてチェックリストの形で利用可能にしたことも特長である。

構築時のセキュリティ対策要件は14、運用時のセキュリティ対策要件は七つの要件で構成され、要件ごとに「必須」「必要」「推奨」と３段階の区分が記載されている。

例えば、構築時には「ECサイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する」「管理者画面や管理用ソフトウエアへ接続する端末のセキュリティ対策を実施する」、運用時には「サイバーおよび管理端末等で利用しているソフトウエアをセキュリティパッチ（脆弱性を解消するためのプログラム）等により最新の状態にする」「ECサイトへの脆弱性診断を定期的およびカスタマイズを行った際に行い、見つかった脆弱性を対策する」などを必須項目として示し、それぞれ詳しく解説している。

本ガイドラインの詳細については、IPAのウェブサイトで確認してほしい。

（独立行政法人情報処理推進機構・江島将和）

ECサイト構築・運用セキュリティガイドラインはこちら

貴社のネットワークに「勝手口」はありませんか？

サイバーセキュリティお助け隊で連携を結んでいる大阪商工会議所では、立命館大学との共同研究調査として、**会社に設置されているVPN機器等のグローバルIPアドレスを元に、ランサムウェア等に侵入される可能性をチェックする「脆弱性診断」を期間限定で無償実施**しております。グローバルIPアドレスを利用されている場合は、いずれの企業・団体も対象。診断実施後、メールにて結果を報告させていただきます。詳細やお申込みは右記QRよりご覧ください。（大阪商工会議所のサイトに繋がります。）

募集期間	2023年６月30日（金）まで
必要なもの	**グローバルIPアドレスをご提供ください** ○VPN機器（Fortigate、SonicWall、F5、Beat、Pulse Secure等）を運用されている企業様、また、ITベンダーにリモートでメンテナンスしてもらっている企業様は、グローバルIPアドレスを保持しておられるケースが多いです。
調査結果	後日メール送付
費用	無償