サイバーセキュリティ最前線

セキュリティ認証だけでは自社を守れない!?

APIを狙う最新の攻撃にも要注意!!

近年、大手企業の間で、取引先をセキュリティリスクの観点から評価・選別する動きが加速している。NECは調達先1800社超にセキュリティチェックシートによる点検を実施し、数百社には訪問やリモートによる確認も行った。楽天グループも個人データを扱う外部委託先に対し、事前のセキュリティチェックを必須としている。はたして、そういったセキュリティ認証やチェックのみで、複雑化するサイバー攻撃から自社を守ることはできるのだろうか。

認証の取得だけでは不十分

現在、セキュリティの信頼度を示すうえで一般的に活用されているのは、外部スコアリングサービスによるリスク格付け、ISO/IEC 27001やプライバシーマークといった認証制度だ。経済産業省も2025年4月には「サプライチェーン強化に向けたセキュリティ対策評価制度」の中間とりまとめを公表し、2026年度の制度化を目指しているという。

ただ、セキュリティ専門企業の㈱ブロード（東京都千代田区）は「サイバーセキュリティの分野では『コンプライアンスと実効性は別』と考えるべき」と指摘。事実、米国小売大手のTarget社はセキュリティ監査を通過していたにもかかわらず、委託業者経由の侵入で甚大な被害を被っている。国内でもそうした事案が発生している。24年にランサムウェア被害を公表した印刷会社（㈱イセトー）は、ISO/IEC 27001、ISO/IEC 27017、プライバシーマークを取得していたが、それでもサイバー被害を受け、その取引先である大手企業や自治体も情報漏洩の発生を公表せざるを得ない状況に陥った。こうした状況を踏まえ、前出のブロードは「認証の取得は組織管理や従業員の意識づけにはプラスだが、実際のセキュリティ対策の実効性やリスクの高さをかならずしも反映するわけではない。形式的な基準だけに依存するのではなく、実効性をともなった対策が必要だ」と強調する。

「API＝セキュリティ」の重要性

では、具体的にどのような対策が必要になるのか。たとえば、取引先や外部委託先を含むサプライチェーン全体を守るためには「攻撃者視点に立ったセキュリティ検証や端末レベルでの安全確保、さらにはAPIといった企業間連携によるリスクへの対応が欠かせない」とブロード。なかでも、最近話題になっているのが「APIセキュリティ」だ。これはアプリケーション・プログラミング・インターフェースの略で、異なるソフトやプログラムなどを連携させる仕組みのこと。たとえば、スマートフォンでネットショッピングをすると、表面上はひとつのサービスで完結しているように見えるが、実はその裏側では決済サービス、配送サービス、在庫管理システムなど、複数の企業のシステムがリアルタイムでデータ連携をしている。この連携を支えているのがAPIであり、まさに現代の経済活動を支える〝情報の窓口〟となっている。

しかし、利便性が高い反面、APIは攻撃者に狙われやすいという側面がある。現に最近、世界的に多くの企業がAPIを経由した不正アクセスによって、顧客情報の漏洩などの被害に遭っている。24年には米国のクラウド型データ基盤サービス「Snowflake」を利用する企業群が標的となり、認証情報などの情報が盗まれ、その弱点が狙われてしまったという。日本ではまだそれほど注目されていないが、海外ではすでに大きなテーマになっているのだ。

こうした状況を踏まえ、ブロードでは、AIを活用して攻撃者の視点で脆弱性を自動検証する「RidgeBot」や感染端末からでも安全に重要サーバーへアクセスさせる「HP Sure Access／Sure Click」、さらにAPIの安全性の検証に特化した最新ソリューションなどを積極的に提案している。具体的な対策を検討する際には問い合わせてみてはどうか。