サイバーセキュリティ最前線

省庁がガイドラインやルールにペネトレーションテストの必要性を明記!!

日本は長年にわたって、ITセキュリティにおけるルールやペナルティなどが欧米主要国と比べて未整備だと指摘されつづけてきた。ところが最近、行政機関によるガイドラインやルールが急速に整備されつつある。本誌6月号で報じた防衛産業サイバーセキュリティ基準はその先行例といえる。そこで、今号ではこうした流れを概観しつつ、事業者が講じるべき対策を紹介したい。

関連事業者への波及も

2024年6月28日、金融庁が「金融分野におけるサイバーセキュリティに関するガイドライン（案）」を公開した。従来、金融庁は監督する業種ごとに「主要行等（都市銀）向け」「中小・地域金融機関向け」「保険会社向け」とそれぞれ監督指針を出してきたが、今後はサイバーセキュリティに関する部分を一本化していくという。つまり、たとえば「漁協系統信用事業における総合的な監督指針」も「主要行等向けの総合的な監督指針」と同一の「金融分野におけるサイバーセキュリティに関するガイドライン」を参照しなければならなくなるというわけだ。今後は業種や規模によらず、かなり高度なサイバーセキュリティが求められることになるだろう。

こうした点について、長年にわたってITセキュリティに取り組む㈱ブロード（東京都千代田区）は「金融庁のガイドラインにかぎらず、たとえば国土交通省所管の主要インフラ（航空、空港、鉄道、水道、物流、港湾など）での情報セキュリティのガイドラインなど、多様な産業でセキュリティ対策に関する要件はより具体的になりつつある。将来的には、本誌6月号で紹介した防衛産業サイバー基準と同様に取引業者などにも影響が広がっていくことも考えられる」と指摘する。

「RidgeBot」の活用を

事業者にとっては厳しい状況だが、この動きはけっして理不尽な対応ではない。現にブロード社では「国内でサイバー被害を受けた企業や組織の発表をチェックしていくと、ランサムウェアのようなマルウェアの感染のほか、明らかに『不正アクセス』とわかる事案やIT機器への不正アクセスや情報漏洩といった事件が頻発していることがわかる」としている。現に、今年5月には大手ハウジングメーカーが過去に使用されていたウエブページのセキュリティ設定の不備で顧客情報を漏洩させてしまったという。

実際、各省庁のガイドランドではこういったリスクにも対応しはじめている。先述の金融庁のガイドラインでは「脆弱性診断やペネトレーションテストの重要性が強調されており、従来よりも具体的な実施方法まで記載されている」とブロード社のセキュリティ担当者。ちなみに、脆弱性とはネットワークやシステム上に存在するセキュリティ上の不具合（バグ）で、プログラムの不良であることもあれば、セキュリティ上の好ましくない設定漏れやミスも含む。だが「マイクロソフト社の製品だけでも年間に約1200件もの脆弱性が公開されるため、膨大にある脆弱性をすべて確認して対応することは非効率で現実的ではない」（ブロード社）そうだ。

こうしたなか、注目を集めているのがペネトレーションテストだ。「実際の攻撃を模倣してアクセスし、事前にリスクを発見する」のがこのテストの目的。そしてさらに、最初に見つけた脆弱性を足掛かりに別の脆弱性を発見するなど、より現実的な侵入経路を特定していく。これでリスクヘッジは万全。そのうえ、ブロード社がイチオシのペネトレーションテストツール「RidgeBot」（Ridge Security社）はまさに完璧、これを使えば「最新の攻撃手法をAIの力で瞬時に検出し、継続的な検査によってその脆弱性を認識することができる」という。

日本全体がセキュリティ対策の向上に動くなか、こういった先端ツールの導入はもはや急務、企業の信頼性の向上にもつながる。ぜひとも前向きに検討してほしいものだ。