サイバーセキュリティ最前線

政府による「能動的サイバー防御」実現へ 問われるユーザー自身のセキュリティ対応力

サイバー攻撃を未然に防ぐための「能動的サイバー防御法案」が4月8日、衆院本会議で可決した。そこで、今号ではこの法案が日本の事業者に与えるインパクトや今後の展開について解説したい。

「能動的サイバー防御」とは、サイバー被害を防ぐために、事前に攻撃の主体を特定し排除することを意味する。この取り組みを法的に実現しようというのが「能動的サイバー防御法案」。政府が防衛や国民生活にかかわる水道、電気、ガスなどの重要インフラへのサイバー攻撃を検知した段階で、能動的に遮断することができるという法律なのだ。この法案は「政府が通信の中身を把握することにつながるのでは」という議論もあって、なかなか成立しなかった経緯がある。今回も衆院審議で野党は憲法21条が保障する「通信の秘密」の制約につながるとの懸念を示したほか、政府が集める情報の範囲をめぐっても議論になった。法案では「外外通信」(国外から発信され、日本を経由して国外で受信)など海外が絡むものにかぎるとしているが、平将明サイバー安保相は国内の企業や個人同士の「内内通信」への将来的な拡大を否定しなかった。こうしたさまざまな懸念についての議論を経て、法案には与野党6党派の共同提出で国民の権利と自由を「不当に制限するようなことがあってはならない」と明記する修正が加えられた。立憲民主党、日本維新の会、国民民主党はこの微修正だけで賛成にまわったわけだが、それだけ野党側もサイバー攻撃の脅威を強く認識しているということだろう。この点についてセキュリティ専門会社の㈱ブロードは「現在のサイバー攻撃はきわめて深刻であり、今回の法案の対象である重要インフラ分野以外でも攻撃を受けるリスクは変わらない点に気をつけたい」と話す。

もちろん、これでひと安心かとはいかない。これまで以上に管理者側にセキュリティ対応が求められることになる。たんなるITセキュリティの脆弱性管理にとどまらず、運用中の「特定重要電子計算機」に対する包括的な管理が必要となるのだ。ただ「現時点で法案に記されているのはシステムを導入する際の届け出やサイバー攻撃を受けた際の報告などの枠組みだけ」とブロード。「どのようなセキュリティ対策や管理をどの水準で実施すべきかは今後、ガイドラインなどで示されるのではないか」という。そもそも、運用しているシステムの種類によってセキュリティ対策が一様でないため、当面、具体的な実装内容までは示しにくいと思われる。防衛産業の分野で使用されている米国NIST(米国立標準技術研究所)の基準をベースにしたガイドラインが持ち込まれた前例があるが、同様に海外の既存の基準を参考に早期導入をはかることも考えられる。

いずれにしても、今後は、政府がサイバーセキュリティ対策を本格的に主導していくことになるのは間違いない。そうなれば、重要インフラ事業者だけでなく、いずれはその取引業者やグローバルビジネスを展開している製造業など、他業種にも波及していくことが考えられる。であればこの際、ブロードのようなセキュリティ専門の企業に相談してみてはどうか。ブロードはこれまでも欧米の先進的なセキュリティ情報やソリューションを日本に紹介・提案してきた実績があり、その知見とネットワークは大いに役に立つはず。海外のケーススタディを参考にしながら、事業者ごとに柔軟な提案ができるのが強みだ。この法案成立を機に自社のセキュリティにどのような影響をおよぼすのかを把握することが大事であり、備えあれば憂いなし、中長期的な視点で適切なセキュリティ対策を講じてほしい。