最新セキュリティマネジメント（第12回）

サイバー攻撃情報の入手とその有効活用および提供

2022.05.24

経済産業省が策定した「セキュリティ経営ガイドライン」で、経営者が社内に対して指示すべきポイントとして示された「重要10項目」。今回は最後の10番目の項目、「情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供」について解説する。

情報の収集・提供・共有を推進

経済産業省と独立行政法人情報処理推進機構（IPA）が共同で策定した「サイバーセキュリティ経営ガイドライン Ver2.0」では、企業のIT活用を推進する上で経営者が認識すべきサイバーセキュリティに関する原則や、経営者がリーダーシップをもって取り組むべき項目がまとめられている。

サイバー攻撃の手法は多種多様で、その被害を防ぐための方法もさまざまだ。過去の事例を参考に企業が万全の対策を講じたとしても、攻撃者は新たな手法を考え、虎視眈々（たんたん）とわずかな隙を突いてくる。企業にとってセキュリティ対策は「ゴールのない取り組み」であり、これで絶対に安心というレベルに達することはないと考えておくべきだろう。

そこで重要になるのが「最新情報の入手」だ。サイバー攻撃に関する情報はメディアで報じられるニュースをはじめ顧客や取引先など、多くのチャンネルから収集できる。これを基に現在の対策を見直し、日々アップデートしていくことが重要なポイントとなる。また、自社が攻撃を経験した場合、その情報を外部に発信し共有することは業界、ひいては社会全体のセキュリティレベル向上につながる。今回は情報の入手と共有、そして提供の進め方について解説する。

正確な情報を素早く入手

わが国において、サイバーセキュリティに関する情報元として広く知られているのが、IPAや一般社団法人、JPCERTコーディネーションセンター（JPCERT/CC）が公開する「注意喚起情報」だ。両組織のWebサイトのトップページには新たに発見されたマルウエアをはじめ、ソフトウエアの脆弱性、アップデートなどの情報が掲載され、随時更新されている。必要な情報が素早く確認できるため、ここで収集した情報を自社の対策に生かすことは、最も効率的な方法といえる。

また、情報は入手するだけでなく、積極的に提供すればより役立つものとなる。サイバーセキュリティに関する報告を受け、調査・分析を行うCSIRT（Computer Security Incident Response Team：シーサート）間における情報共有や、日本コンピュータセキュリティインシデント対応チーム協議会（日本シーサート協議会）などのコミュニティー活動への参加による情報収集を通じて、自社のサイバーセキュリティ対策の強化を図るのは有効な方法だ。

情報はさまざまな方法で収集が可能だ。例えばセキュリティ関連企業のWebサイトには、自社で把握した新たなリスクに関する情報が掲載されているし、業界単位で事業に関係するセキュリティ情報をまとめているケースもある。

ただし、情報は「多ければ多いほどいい」というものではない。臆測や不正確な情報は役に立たないどころか、むしろ対策

の足を引っ張る障害になりかねないリスクとなる。情報の出どころを確認し、冷静に対応する姿勢が欠かせない。

情報共有の重要性を認識しよう… 続きを読む