サイバーセキュリティ最前線

情報漏洩に対する課徴金の議論が噴出!!
一足はやく万全のセキュリティ体制を

2024年12月、個人情報保護委員会が開催した有識者会議では、個人情報の漏洩を招いたセキュリティ事案への不十分な対応について、課徴金を設ける必要性が議論された。その内容を紐解きながら、現在、求められているセキュリティソリューションについて紹介したい。

対策を怠った際の罰則が世界中で徐々に浸透中

今回、議論された課徴金の対象となるのは、個人情報保護法にもとづく違法な第三者への提供や漏洩で、適用されるかどうかは、事業者が講じるべき対策を怠っていたかどうかが判断のポイントになるという。つまり、攻撃を受けた際の対策が不十分で、結果的に個人情報が漏洩した場合、罰則対象となる可能性が出てくるかもしれないということだ。ちなみに、課徴金を設ける理由としては①現行制度の抑止力強化②被害拡大の防止③公平性の確保（適切にコストを負担する事業者とのバランス）④国際的動向との整合性があげられている。

こうした動向について、長年にわたってセキュリティに取り組み、欧米などのセキュリティ情勢にも詳しい㈱ブロード（東京都千代田区）は「すでにEUや米国では個人情報漏洩に対する制裁金制度が導入されているし、英国や韓国、さらには中国でも同様の法制度が整備されている」という。「被害を受けたのにペナルティを科せられるのは納得がいかない」という声も聞くが「サイバー犯罪の収益が犯罪集団や敵対国の資金源になっている現実を踏まえて『対策を怠った場合の罰則もやむなし』という考え方が世界中で浸透しはじめている」と指摘する。

複雑化する攻撃に適切なソリューションを

現在、サイバー攻撃のなかで情報漏洩につながる懸念がもっとも高いのはランサムウェアと呼ばれるマルウェアだが、最近は「データを暗号化して使えなくし、脅迫する」という従来パターンだけでなく、「詐取したデータを外部に晒すと脅迫する手口」も増えているという。こうした攻撃側の変化に逐次、対応していくには、膨大な人的・資金的コストが必要になるだろう。

そこでブロードでは、各企業の対策や課題をヒアリングし、優先して取り組むべきリスクへの対策はもちろん、業務や管理の効率向上との両立が可能なソリューションを取り扱い、適切なものを提案するようにしているという。

まず「喫緊の課題を明確にするため、侵害経路を特定するペネトレーションテスト（侵入テスト）を提案したい」と話す。ブロードが提案する「RidgeBot」であれば「組み込まれた先端的なAIで、任意のタイミングでこのペネトレーションテストを実施できるようになる」という。この種のテストはどうしても特殊なスキルが求められるため専門業者に依頼せざるを得なくなるが、RidgeBotを活用すればその必要がなくなるという。

さらに、「HP SCE」を導入するのもオススメだ、と。パソコン上の「仮想のパソコン」で侵入者を隔離して点検することができるからだ。メールやダウンロードなどによって侵入されるリスクから社内のパソコンやシステムを守ってくれるのだ。これまでのセキュリティは無害なものを有害とする「誤検知」が多く、担当者がそのつど対応してきたが、その必要がない点もユーザーに愛用されている点だ。もうひとつガードを固めておきたいのなら、ユーザーの使用権限を必要な範囲に絞れるBeyondTrust社製の特権管理ソリューション群を導入することだ。サイバー攻撃が横展開することを防ぐこともできるというスグレモノだ。そのほか、万が一、ランサムウェアなどの影響でシステムが停止したとしても、アプリケーションの継続利用を可能にする「Neverfail」を導入していれば、業務を安心して継続できるという。課徴金の議論がすすむなか、先手必勝、一足先にこういった二重、三重の対策が肝心ではないか。