EY Japan プリンシパル　杉山 一郎氏

パーソナルデータ新潮流（4）

「万が一」への対応急げ

今年秋のラグビーワールドカップ、来年夏の東京五輪・パラリンピックと大型イベントが続く。関係者の大きな懸念の一つがサイバーセキュリティーだ。背景として、ここ数年の実害を伴ったサイバー攻撃の増加が挙げられる。

サイバー攻撃の実態を調査した複数のリポートが、攻撃などによる侵害に気づくまで100日以上かかった組織が多いと報告している。また、個人情報が流出した場合の被害額についても楽観視できない数字が出ている。これらのリポート以外にも数多くの報道から「サイバー攻撃は気づきにくく甚大な被害をもたらす可能性がある」ことは想像できるであろう。

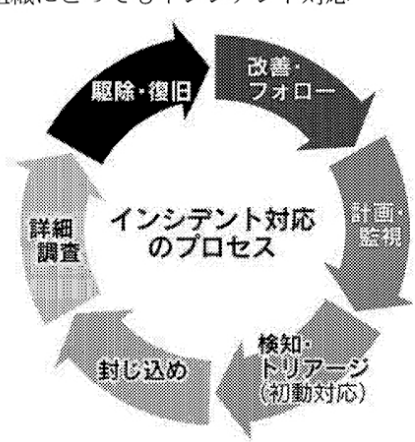
一方、欧州連合（ＥＵ）の一般データ保護規則（ＧＤＰＲ）などで、インシデント（事故につながる恐れのある事態）発生時の迅速な報告・通知義務や対応計画の策定が義務付けられる傾向にある。日本でも個人情報保護法上の責任として報告・通知・対応の努力義務が課せられており、重要インフラだけでなく個人情報を取り扱う組織にとってもインシデント対応態勢の構築が急務となっている。

インシデント対応の手順は計画の策定に始まり、攻撃などの監視、攻撃の検知、トリアージ（初動対応）、詳細調査と続く。

これらのうち、トリアージや調査が、データ保護のための技術的対策やデータ移転の規制の影響により思うように実施できない状況が起きている。例えば、データ保護対策でインシデント対応に必要なデータを保全（証拠確保）できない、あるいはログなどが暗号化されて調査できないといった問題はかなり前から生じている。

また、内部犯行による情報流出が疑われる場合、法人貸与のモバイルデバイスなどにも調査の範囲が及ぶことがあるが、パソコンよりもセキュリティーが厳しくデータの保全が困難で、より一層のプライバシー配慮が要求される。このほかにもビジネスチャットやグループウエアなど様々なデータがクラウドに保存される傾向にあり、それらの保全も容易ではなく、様々な課題が生じている。

企業はこれらの課題に対し、事前にサイバー攻撃へのリスク分析・データマッピング・重要データの保護手段および緊急時の解除手続きの確認・準拠法令などとのギャップを分析し、インシデント対応計画を作成、改善することを優先的に行うべき対応と考える。



すぎやま・いちろう　ＥＹＪａｐａｎで不正調査などを専門とする組織のテクノロジーチームの日本地域リーダー。サイバーインシデント対応やデジタル証拠を保全・分析するデジタルフォレンジックを活用した係争支援に従事。

掲載日　2019年07月10日　日経産業新聞　014ページ