サイバーセキュリティ最前線

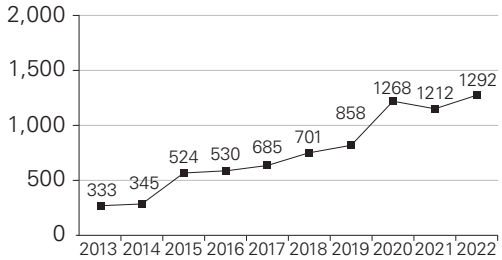
最先端のソリューションを駆使して無数の「脆弱性」を乗り越える

多くのセキュリティ侵害の原因となっている「脆弱性」。これはセキュリティ上の「弱点」を示す用語で、一般的にはコンピューターのプログラムのセキュリティ上の欠陥（バグ）を意味する。そこで、今号では脆弱性に関するリスクの現状と対策について紹介したい。

なくなることがない「脆弱性」

「脆弱性」をついたセキュリティ事件が相ついでいる。たとえば、大阪急性期・総合医療センターへのサイバー攻撃では、同センターの納入業者の通信機器システムに脆弱性が見出された。また、2022年3月に森永製菓が公表した個人情報漏えいに関しても、脆弱性が悪用された可能性が報告されている。

マイクロソフト製品の脆弱性の総数（2022年までの10年間）



では、世の中に脆弱性はどの程度、存在するのか。企業などで広く利用されているマイクロソフト製品の場合、22年の1年間に公表された脆弱性の総件数は1292件（この10年で最多）で、製品分類別ではパソコン用のWindows（513件）が最多となっている。その背景には近年、マイクロソフト製品の売り上げが増加していること、クラウド向けなどの新製品群が加わったことなどがあるが、とくにパソコン用のWindowsについては専門家らによると「セキュリティが重視されていなかった時代のプログラムコードが再利用されている部分がある」とのことなので、引きつづき注意を払いたい。

ソリューションの活用が肝心

マイクロソフトの公表内容によると、脆弱性の7種の影響分類のうち「リモートコード実行（遠隔から送り込まれた悪意のあるプログラムコードが実行されること）」と「権限昇格（システムなどの権限が取得されてしまうこと）」がもっとも多く、とくに22年は「権限昇格」が3年連続で最多の55㌫を占め、長年、もっとも多かった「リモートコード実行」はここ数年はほぼ横ばいで、全体の24㌫だった。

もっとも、メーカー側も脆弱性が認識されると、修正プログラムの提供などを行うが、修正プログラムの適用にはいくつかのハードルがある。まず、脆弱性の存在を把握するには、脆弱性情報に日常的に気を配り、その修正プログラムがシステムに支障をきたさないかを確認しなければならない。また、脆弱性への対応はあらたなものが公表されるたびに必要であり、ともすれば延々と対応に追われてしまいかねない。

このように、ユーザーの努力だけではタイムリーな対応が難しい脆弱性に関するリスクだが、㈱ブロード（東京都千代田区）ではこの課題に対応できるセキュリティソリューションを提案している。たとえば、Windowsパソコンのエンドポイントを保護する「HP Sure Click Enterprise（HP SCE）」は仮想化技術を生かしてPC上に別のパソコンを稼働させる仕組みになっており、仮に脆弱性を悪用するマルウェアが動いても本体には何ら影響が出ないという。

また、マイクロソフトの重要な脆弱性の75㌫は「ユーザーが管理者権限を持っていなければ、その影響が大幅に軽減される」といわれているが、その点についてはBeyondTrust社製の特権管理ソリューションが効果を発揮する。実際、このソリューションを活用すれば、標準ユーザーのままでも不便なく管理者権限が必要な操作を実行できるようになるそうなので、気になる方は一度、ブロードに問い合わせてみてはどうだろうか。