サイバーセキュリティ最前線

# 「情報セキュリティ10大脅威」から最新のソリューションで自社を守る!!

**このほど、独立行政法人情報処理推進機構（ＩＰＡ）が「情報セキュリティ10大脅威 ２０２４」を公表した。個人向けと組織向けにそれぞれ10種類の脅威が選出されたが、今号では1位と2位になった脅威と前年から順位を上げた脅威をチェックしてみたい。**

**「情報セキュリティ 10大脅威 2024」に掲載された組織向け脅威**

| 順位 | 組織向け脅威 | 前年順位 | 前年比 |
|---|---|---|---|
| 1 | ランサムウェアによる被害 | 1位 | - |
| 2 | サプライチェーンの弱点を悪用した攻撃 | 2位 | - |
| 3 | 内部不正による情報漏えい等の被害 | 4位 | ↑ |
| 4 | 標的型攻撃による機密情報の窃取 | 3位 | ↓ |
| 5 | 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃） | 6位 | ↑ |
| 6 | 不注意による情報漏えい等の被害 | 9位 | ↑ |
| 7 | 脆弱性対策情報の公開に伴う悪用増加 | 8位 | ↑ |
| 8 | ビジネスメール詐欺による金銭被害 | 7位 | ↓ |
| 9 | テレワーク等のニューノーマルな働き方を狙った攻撃 | 5位 | ↓ |
| 10 | 犯罪のビジネス化（アンダーグラウンドサービス） | 10位 | - |

1位の「ランサムウェア」の厄介な点は、手口やプログラムが年々進化しつづけていること。ランサムウェアといえばユーザーのデータを暗号化して使えなくして、それを解除する「キー」を売りつけたり、詐取した情報を開示すると脅迫したりするのが一般的だったが、最近は最初から詐取した情報を公開し、脅迫するノーウェアランサムが増加しているという。2位の「サプライチェーンの弱点を悪用した攻撃」については、昨年、企業・組織の子会社や納入業者、業務委託先などが入口となったセキュリティ侵害の事例が多かったとし、その反省から納入業者が一定のセキュリティ基準を満たすようになってきているようだ。

前年から順位が上がったものに「内部不正による情報漏えい等の被害」がある。これは従業員ら内部の者による情報の搾取のこと。また「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」と「脆弱性対策情報の公開に伴う悪用増加」も順位を上げている。これらはいずれも、コンピュータ機器に「セキュリティ上のバグ」として存在する脆弱性を狙ったものだ。

ではこれら5つの脅威に対し、ユーザー、企業はどのように対応すべきだろうか。長年にわたってサイバーセキュリティに取り組んでいる㈱ブロード（東京都千代田区）によると、ランサムウェアに関しては「HP Sure Click Enterprise（ＨＰ ＳＣＥ）」が有効とのこと。「外部由来のファイルを『仮想のパソコン』で開くことで、たとえ未知のマルウェアがどのような動作をしたとしても、ＰＣ本体に一切影響を与えない」という。

「サプライチェーンの弱点を悪用した攻撃」に関しては、ＨＰ ＳＣＥのシリーズ製品にあたる「HP Sure Access」というソリューションが効果的。このソリューションを導入すれば、サプライチェーン内のセキュリティ対策が弱い接続元のＰＣがマルウェアに感染したとしても、「仮想のパソコン」が作動、サーバーのデータを守ることができるという。ついで「内部不正による情報漏えい等の被害」については「アクセス管理」を強化するしかない、という。ブロードでは「この分野の世界的なリーダー格のVanguard社やBeyondTrust社と協業関係にあり、幅広い対応策を提案できる」とのことなので、相談してみるといいだろう。

そして「修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）」と「脆弱性対策情報の公開に伴う悪用増加」に関しては、「RidgeBot」が有効だ。RidgeSecurity社が開発したこのツールは、最新のハッキング情報とＡＩの技術を融合した仕組みになっており、自動的にペネトレーションテスト（侵入テスト）を実施し、侵入経路を特定し、対策の優先度を含む診断結果を得ることができる。

自社の懸念事項とあわせて、ぜひこれらのソリューションをチェックしてみてほしい。