ASAMA あさまセキュリティニュースレター
Security Newsletter
2024年2月16日
Vol.105

情報セキュリティ10大脅威2024 [組織]

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
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	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

出典　IPA　情報セキュリティ10大脅威 2024 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

POINT

IPA　情報セキュリティ10大脅威 2024が発表されました
サイバー攻撃のニュースも目にする機会も急増しています。インターネットにつながっている以上、脅威は常にあると考え、セキュリティ対策は個人の判断任せではなく、組織としてどう対策するかが重要です。新入社員や人事異動等、組織の変更を迎える時期、セキュリティ対策の確認と見直しを！

攻撃パターン

ランサムウェアの特長をまとめてみると
・**犯罪のビジネス化**で、簡単に攻撃が可能
・**テレワーク**でも利用されるVPNの**脆弱性**を悪用した攻撃によるランサムウェア被害が急増
・病院や大手企業を**標的**とする場合、セキュリティ対策が強固でない**サプライチェーン**経由で攻撃
↑
このように、甚大な被害をもたらすランサムウェアは、10大脅威にあげられるキーワードがいくつも含まれており、組織全体で対策+取引先に対してもリスク評価を行うケースも増えています

さらに2024年は、**AIや機械学習を悪用した攻撃**が活発化し、**取引先になりすましたメール、添付ファイル、URLリンク経由の不正プログラム**など、**セキュリティ対策でも検知されず**に各個人に届く可能性が増えるでしょう

対策

組織の社員全員・・・日頃から怪しいと思ったら開かず確認、報告と情報共有、インシデント時の対応方法の確認

組織全体の対策・・・アップデートを怠らない、古い機器やソフトでサポートが切れたものは見直しを
万が一のバックアップがあるか、定期的にとれているか確認を

人為的ミスの対応・・・セキュリティ対策をしていても不注意等での人為的ミスによる情報流出も増えています
機密情報の整理、情報持ち出しのルール、権限の見直し、公私を分け個人利用デバイス、クラウドサービス、USBメモリ等の利用制限なども検討を

浅間商事株式会社　〒110-0005　東京都台東区上野7-15-70 浅間第一ビル　0120-830-414