Ksisnetだより
発行:Ksisnet事務局
令和元年10月29日
Vol.68

「情報セキュリティ10大脅威2019」（組織に対する脅威）

3位　ランサムウェアによる被害

ＩPA（情報処理推進機構）から、「情報セキュリティ10大脅威2019」が公開されています。「組織」の視点からは、

「ランサムウェアによる被害」

が脅威の３位として選出されています。

ランサムウェアに感染すると、ＰＣやスマートフォンに保存されているファイルの暗号化や画面ロック等が行われ、解除と引き換えに金銭を要求されます。

順位	組織	昨年順位
１位	標的型攻撃による被害	１位
２位	ビジネスメール詐欺による被害	３位
３位	ランサムウェアによる被害	２位
４位	サプライチェーンの弱点を悪用した攻撃の高まり	NEW
５位	内部不正による情報漏えい	８位
６位	サービス妨害攻撃によるサービスの停止	９位
７位	インターネットサービスからの個人情報の窃取	６位
８位	ＩｏＴ機器の脆弱性の顕在化	７位
９位	脆弱性対策情報の公開に伴う悪用増加	４位
10位	不注意による情報漏えい	12位

「NEW」は初めてランクインした脅威

＜攻撃手口＞

○メールの添付ファイルやリンク

メールの添付ファイルやメール本文中のリンクを開かせることでランサムウェアに感染させます。

○ウェブサイトの閲覧

脆弱性等を悪用し、ランサムウェアをダウンロードさせるよう改ざんした正規のウェブサイトや、攻撃者が用意したウェブサイトを閲覧させることでランサムウェアに感染させます。

そのようなウェブサイトに誘導するために、メール等が利用される場合もあります。

○脆弱性の悪用

ＯＳの脆弱性を悪用し、アップデートしないままインターネットに接続しているＰＣをランサムウェアに感染させます。

○その他の手口

リモートデスクトッププロトコル（ＲＤＰ）等で遠隔からシステムに侵入しランサムウェアに感染させます。

＜事例＞

○病院の電子カルテシステムが感染

2018年10月、奈良県内の病院で感染し、電子カルテシステムが約２日間にわたり使用できなくなった。

感染原因は最新のセキュリティソフトがインストールされていなかったこととされており、バックアップ装置が適切に設定されていなかったため、データの一部は復元できなかった。

＜対策/対応＞

【経営者層】

○組織としての体制の確立

- 迅速かつ継続的に対応できる体制（CSIRT（※1））の構築
- 対策予算の確保と継続的な対策の実施

【システム管理者・従業員】

○被害の予防

- 受信メール、ウェブサイトの十分な確認
- サポートの切れたOSの利用停止、移行
- フィルタリングツールの活用
- ネットワーク分離
- 共有サーバのアクセス権最小化
- バックアップの取得

○被害を受けた後の対応

- CSIRTへ連絡
- バックアップからの復旧
- 復号ツールの活用
- 影響調査および原因の追究、対策の強化

（IPA『情報セキュリティ10大脅威2019』を基に作成）

CSIRT（※１）･･･企業や行政機関などの組織内に設置され、コンピュータシステムやインターネットなどのネットワークに保安上の問題や事故が生じた際に対応する専門チームのこと。

「情報セキュリティ10大脅威 2019」の詳細については、下記ウェブサイトで公開されています。
https://www.ipa.go.jp/security/vuln/10threats2019.html