Ksisnetだより
発行:Ksisnet事務局
令和元年7月29日
Vol.65

「情報セキュリティ10大脅威2019」（組織）
1位　標的型攻撃による被害

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、昨年に引き続き、
「標的型攻撃による被害」
が脅威の１位として選出されています。
攻撃者（犯人）はメールの添付ファイルや悪意のあるウェブサイトを利用し、組織のＰＣを感染させた後、組織内部へ潜入し、組織内部の侵害範囲を拡大しながら重要情報や個人情報を窃取します。

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
添付ファイルやメール本文のリンク先にウイルスを仕込み、開かせることで組織のＰＣをウイルスに感染させます。本文や件名、添付ファイル名は業務に関連するような内容に偽装され、実在する組織の差出人名が使われる場合もあります。
また複数回のメールのやりとりで油断させ、添付ファイルを開かせる等、不審を抱かないような巧妙な騙しのテクニックが使われます。

○ウェブサイトの閲覧
標的の組織が閲覧するウェブサイトを調査し、ウェブサイトからウイルスに感染させるように改ざんします。標的となる組織の従業員が改ざんされたウェブサイトを閲覧することでウイルスに感染します。

○不正アクセス
組織が利用するメールのクラウドサービスやウェブサーバーへ不正アクセスし、認証情報等を窃取します。そして窃取した情報を利用し、社内システムの利用等に用いる正規のアクセス経路で組織内部へ潜入し、組織内部のＰＣやサーバーをウイルスに感染させます。

＜脅威＞

○メール等によりPCをウイルスに感染させ組織内部へ潜入
○長期にわたって侵害範囲を徐々に広げる
○組織の機密情報を窃取

＜傾向＞

○悪意のあるCSVファイルが添付されたメールを観測
（Excelの起動時にプログラムを実行する機能を悪用）

○MS Office製品の文書ファイルを悪用した手口も観測
ファイルの拡張子は「.wiz」「.iqy」「.slk」等（WordやExcelの起動時にプログラムを実行する機能を悪用）

（IPA「『情報セキュリティ10大脅威2019』を決定」を基に作成）

「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

対策／対応

【経営者層】
- **組織としての体制の確立**
  - ①迅速かつ継続的に対応できる体制の構築
  - ②対策予算の確保と継続的な対策の実施
  - ③セキュリティポリシーの策定

【セキュリティ担当者】
- **被害の予防／対応力の向上**
  - ①情報の管理とルール策定
  - ②サイバー攻撃に関する継続的な情報収集と情報共有
  - ③セキュリティ教育の実施
  - ④インシデント発生時の訓練の実施
  - ⑤統合運用管理ツール等によるセキュリティ対策状況の把握
  - ⑥取引先のセキュリティ対策実施状況の確認
- **被害を受けた後の対応**
  - ①組織内の体制（CSIRT（※１）等）の運用
  - ②影響調査および原因の追究,対策の強化

【システム管理者】
- **被害の予防（BCP（※２）対策含む）**
  - ①セキュアなシステム設計
  - ②重要サーバーの要塞化（アクセス制御、暗号化等）
  - ③ネットワーク分離
  - ④バックアップの取得
- **被害の早期検知**
  - ①ネットワーク監視、防御
  - ②エンドポイントの監視、防御
- **被害を受けた後の対応**
  - ①バックアップから復旧

【従業員・職員】
- **情報リテラシーの向上**
  - ①セキュリティ教育の受講
- **被害の予防**
  - ①「情報セキュリティ対策の基本」（※３）を実施
- **被害を受けた後の対応**
  - ①CSIRTへの連絡

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。
BCP（※２）･･･企業が自然災害などの緊急事態に遭遇した場合において、業務中断に伴うリスクを最低限にするために、平素から事業継続について戦略的に準備しておく計画のこと。

「情報セキュリティ対策の基本」（※３）

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

参考　ＩＰＡ（情報処理推進機構）