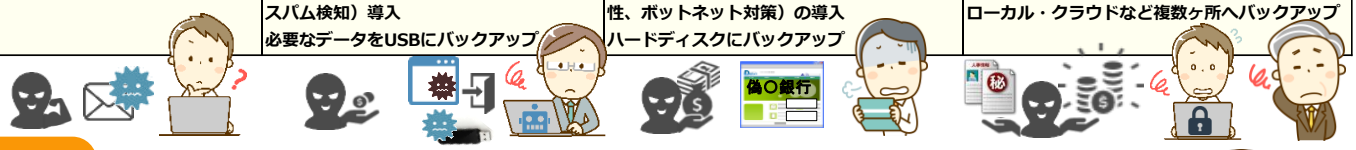
ASAMA あさまセキュリティニュースレター
Security Newsletter
2023年9月12日
Vol.100

今も昔も基本的な対策は一緒！

日本では、35年前の1988年に初めてコンピューターウイルス感染したといわれています
攻撃者の目的のほとんどが金銭ですが、昨今は金銭被害に業務停止＝組織の存続に関わってきています。
日々様々なコンピューターウイルスが出現、常時サイバー攻撃が行われていますが、
基本的な対策は今も昔も変わりません。現状を確認し基本的な対策ができているか確認しましょう

	2000年代	～ 2010年代前半	～ 2010年代後半	～ 2023年・・・
目的	能力の誇示、金銭	金銭、スパイ行為、主義・主張	金銭（組織化）、スパイ行為、主義・主張、システムダウンによる社会的混乱	
攻撃手法	インターネット経由 メール添付型ウイルス 感染PCから他の社内PCへ拡散 スパイウェア（偽の不具合画面）	メールプレビューでもウイルス感染 改ざんされたホームページ閲覧で感染 USBメモリ経由で次々感染 ボット（遠隔操作や入力情報の搾取）	フィッシングメール フィッシングサイト（不正送金） メールサーバ乗っ取り ランサムウェア（ファイル暗号化） Emotet（取引先へ被害拡大）	VPN脆弱性を悪用、多重脅迫型ランサムウェア 多種多様なフィッシング、サポート詐欺 ウイルスチェックを避ける攻撃　PPAPで送信 IoT機器、クラウドサービスの脆弱性から、 情報搾取、情報の売買やデータ流出の脅迫
被害	パソコンの不具合 情報漏えい 他組織へDDoS攻撃 スパムメール発信源	情報漏えい フィッシング詐欺被害 USBメモリ経由で取引先へウイルス拡散 ボットによる他組織へ攻撃（踏み台）	不正送金（2023年再度被害急増中） 取引先（サプライチェーン攻撃）二次被害 情報漏洩お詫び費用 ランサムウェア感染で業務停止、復旧費用	様々なネットワーク機器を悪用、乗っ取り、 他組織への攻撃、データ流出、データ暗号化、 脅迫（搾取データの公開）、高額な金銭被害、 システム停止など、事業継続困難、経営危機
対策	脅威を知る・アップデート・組織で対策 ウイルス対策ソフトの導入	脅威を知る・アップデート・組織で対策 検知力の高いウイルス対策ソフトの導入 UTM（ファイアウォール・ウイルス・スパム検知）導入 必要なデータをUSBにバックアップ	脅威を知る・アップデート・組織で対策 ふるまい検知等、検知力の高いウイルス対策ソフトの導入、多機能UTM（不正侵入、脆弱性、ボットネット対策）の導入 ハードディスクにバックアップ	脅威を知る・アップデート・組織で対策 多層防御型ウイルス対策ソフト、UTMの導入 被害にあった場合を想定した対策 ローカル・クラウドなど複数ヶ所へバックアップ



POINT

昔はコンピューターウイルスに感染するとパソコンがおかしくなり気づきやすかったのですが、今は感染していることに気づかない、いつどこから感染したかわからない、被害が目に見えてから気づくという事が多いため、基本的な対策を全員で行い、組織として抜け漏れを防ぐ対策を

サイバー攻撃のパターン

- **インターネット経由**　正規ホームページを改ざんし、ユーザーがアクセスするとウイルスがダウンロードされる
  フィッシングサイトで入手した情報で、様々なサービスに不正アクセスを試みデータ搾取
- **メール経由**　差出人を偽装、巧妙な文面で本文のURL（フィッシングサイトや不正なサイト）をクリックさせる
  添付ファイルを開かせ、不正なプログラムをダウンロード・インストールさせる
  ウイルスチェックを回避するためにパスワード付きZIPで送る
  メールサーバ容量がいっぱいです等の偽メールで、メールサーバを乗っ取り、ウイルス・スパム発信元として悪用、取引先とやり取り（ビジネスメール詐欺）
- **脆弱性の悪用**　パソコンやソフトの脆弱性のみならず、ウイルス対策ソフトでカバーできない、ルータやネットワークカメラ、NAS、無線機器等、インターネットに接続できる機器の脆弱性を悪用し、ランサムウェア攻撃、不正サイトへ誘導、情報盗み見、他組織への攻撃などを行う

対策

- **フィッシングメールは本物と見分けにくいため、最新の情報を確認**　・・・　参考URL　迷惑メール相談センター
  https://www.dekyo.or.jp/soudan/index.html
- **不審なメール、WEB閲覧中の警告表示など、社内で情報を共有・確認を**
- **利用するソフトやデバイスは必要最小限にし、OS、ソフト、ファームウェアなど定期的にアップデートを**
- **サポート切れのパソコンやソフト、古いネットワーク機器は使用をやめ、定期的に見直しを**
- **フリーWiFiや、公衆WiFiのビジネス利用は避けましょう。デバイスやサービスは公私を分けての利用を**
- **バックアップは必ず取りましょう。社内ネットワーク以外の場所（クラウドなど）へのバックアップの検討を**

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