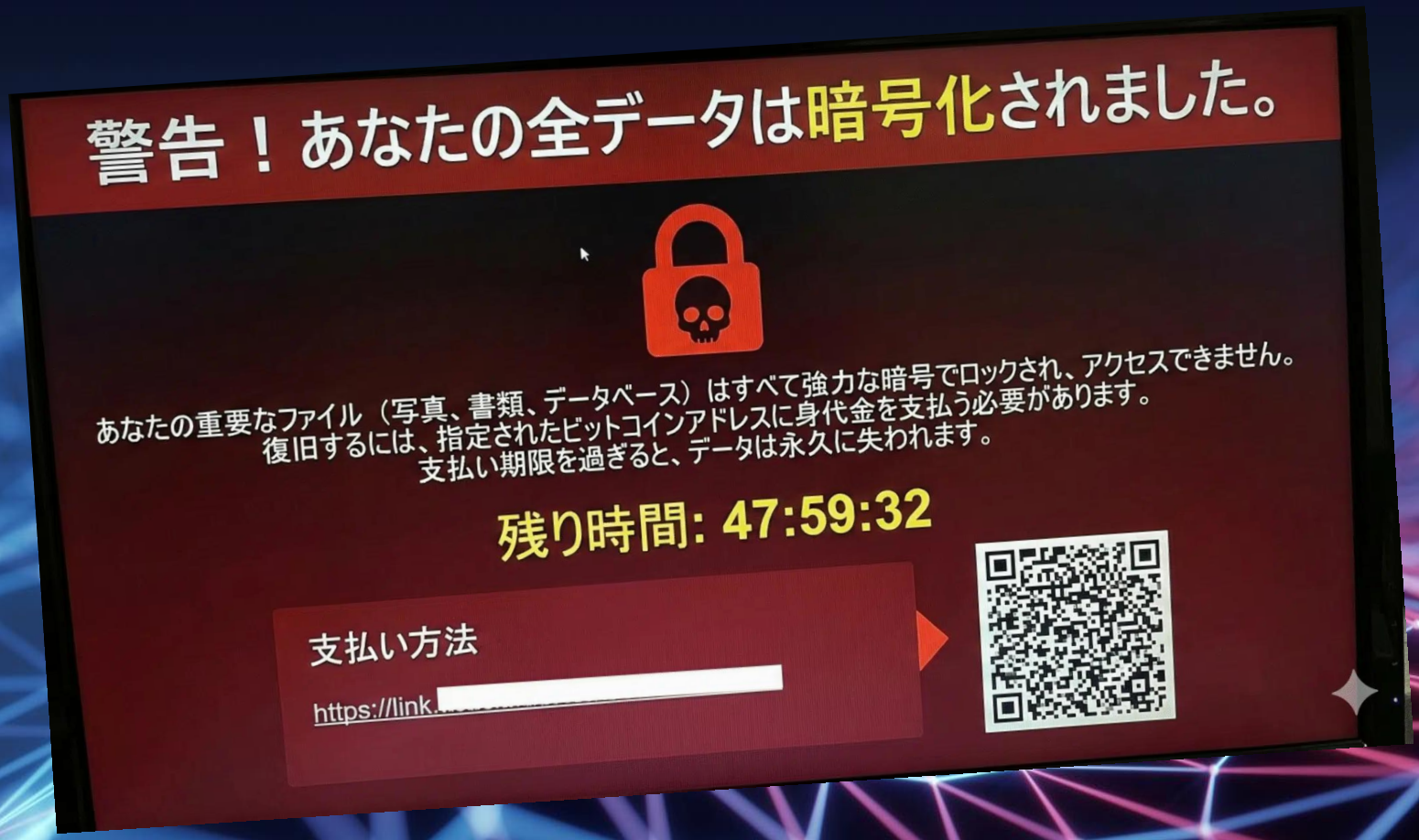


インターネットの脅威

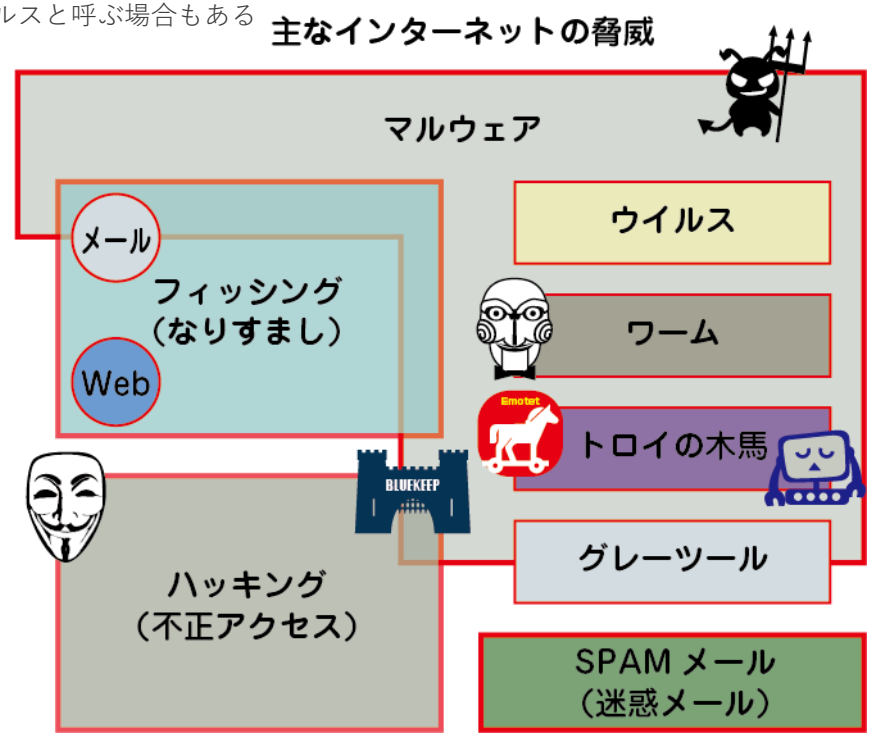
2026年最新情報

インターネットの脅威とは

- インターネットは、世界中と接続している公開されたネットワーク

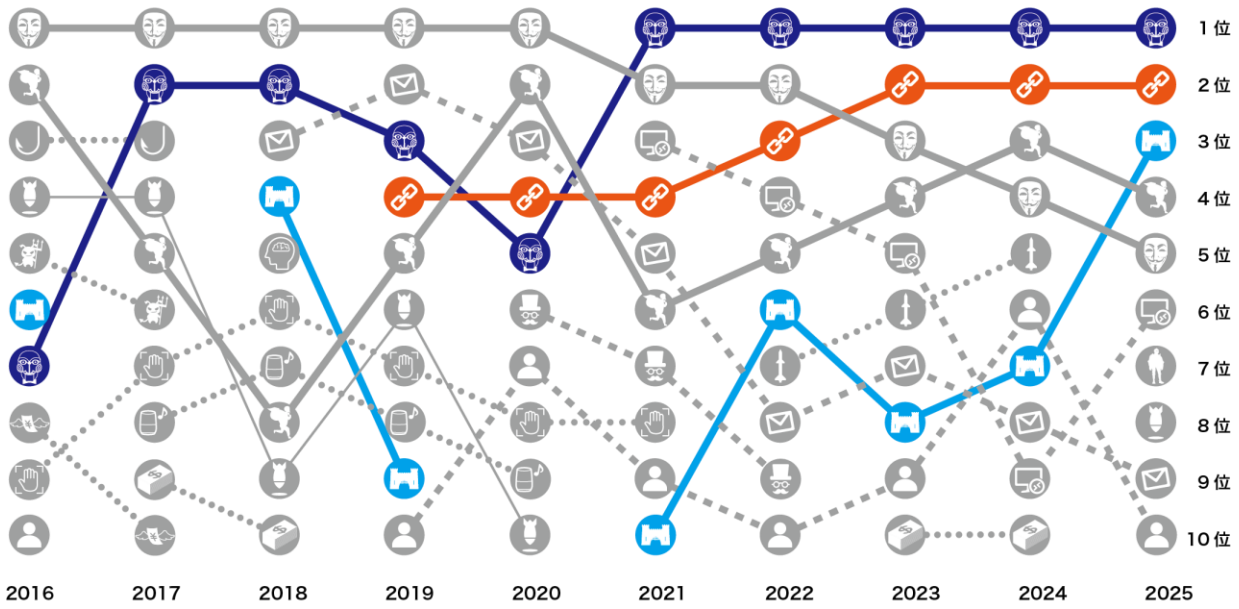
  リアルと同じく善人だけがいるわけではない
  インタネット上の悪意ある攻撃を「インターネットの脅威」と呼ぶ
  リアルと違い、距離や時間と言う概念がないので、誰でも被害に遭う危険性がある

- 脅威の種類
  - マルウェア（malicious software：悪意あるソフトウェア）
    - 機能により更に分類されるが、近年のマルウェアは複数の機能を持つ場合が多い
    - ウイルスはマルウェアの一種だが、マルウェア自体をウイルスと呼ぶ場合もある
  - フィッシング（なりすまし）
    - 他社を騙ったメールやWebサイトのこと
    - フィッシングメールからフィッシングサイトに誘導しユーザーの金融情報などを搾取する
    - サイト表示等は、本物と全く同一にできるため一般での判断は困難
  - ハッキング（不正アクセス）
    - ネット機器やPCの脆弱性（セキュリティホール）を突いた侵入
    - マルウェアの植え付けや情報収集などを行う
  - SPAM（スパム）メール
    - 受信者の意向を無視して一方的に繰り返し送り付けられる迷惑メール
    - 大半は広告や宣伝が目的



脅威の傾向

IPA 情報セキュリティ 10 大脅威 より集計



- ランサム攻撃による被害
- サプライチェーンや委託先を狙った攻撃
- システムの脆弱性を突いた攻撃
- 内部不正による情報漏えい等
- 機密情報等を狙った標的型攻撃
- リモートワーク等の環境や仕組みを狙った攻撃
- 地政学的リスクに起因するサイバー攻撃
- 分散型サービス妨害攻撃（DDoS 攻撃）
- ビジネスメール詐欺
- 不注意による情報漏えい等
- 犯罪のビジネス化（アンダーグラウンドサービス）
- 修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
- 予期せぬ IT 基盤の障害に伴う業務停止
- インターネット上のサービスへの不正ログイン
- IoT 機器の不正利用
- 脅威に対応するためのセキュリティ人材の不足
- ウェブサイトの改ざん
- ウェブサービスからの個人情報の窃取
- インターネットバンキングやクレジットカード情報の不正利用

■ ランサムウェア

2016年に10大脅威入りして以来、常に上位にいる脅威の雄

- 2025アサヒグループ
- 2025アスクル
- 2024KADOKAWA

■ サプライチェーン攻撃

セキュリティの強固な本陣へ直接侵入するのではなく、セキュリティの甘い取引先から侵入する手法

- 2025アサヒグループ
- 2025アスクル

■ 脆弱性攻撃

OS・アプリ・機器の未公開バグ（セキュリティホール）を突いた攻撃

- 2025アサヒグループ

生成AI登場による脅威の加速

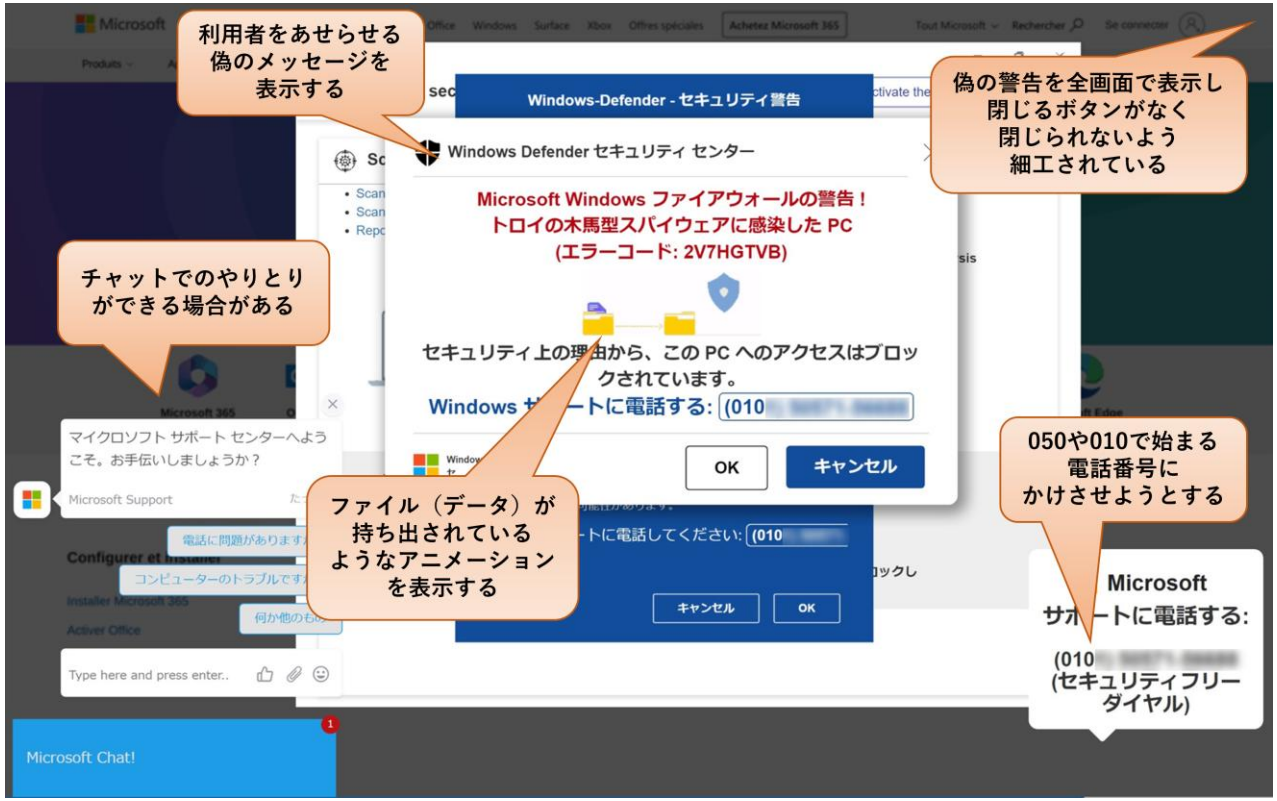
攻撃者御用達の生成AIを利用

- マルウェア開発スピードUP
  - PC/サーバーへの侵入速度最新記録27秒（2023年平均84分）
  - ゼロデイ攻撃**42%**増加

- 不自然さのないメール文章によるフィッシングメール生成
  - 業種や業務内容に即した自然な文章を短時間で大量に生成
  - Emotet（メールのアドレス帳やメール通信履歴を**窃取し悪用するマルウェア**）と生成AIにより、文章のトーンや専門用語、言い回しまで巧妙に再現

ヒューマンエラーを誘発させる「サポート詐欺」

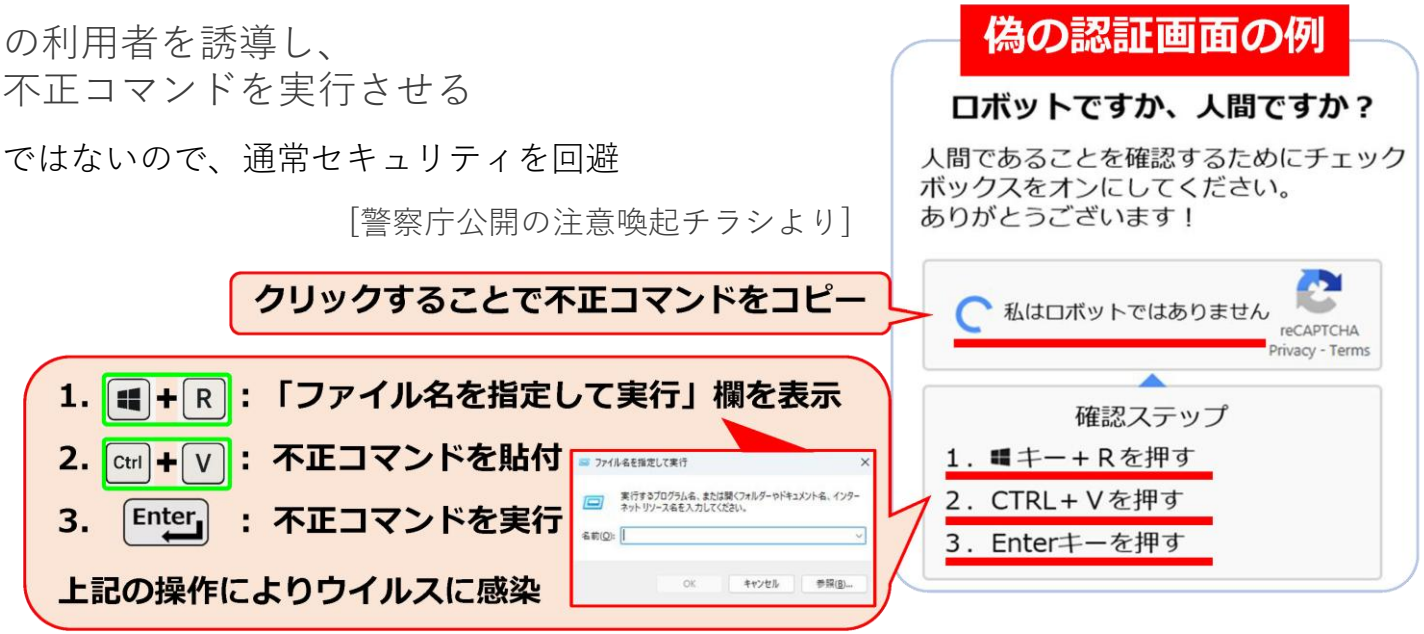
- ユーザーに自ら実行させ、マルウェアをインストール / 金銭や個人情報を騙し取る
- トラップサイトにアクセスすることで起動
  - マルウェアではないので、通常セキュリティを回避
  - アドレスを頻繁に変更してアンチフィッシングを回避
  - 大音量アラームでユーザーの恐怖心を煽る
  - 全画面表示で止めまれない
  - PCを強制終了しても起動時に再び表示するように細工



私はロボットではありません「CLICK FIX」

- パソコンなどの利用者を誘導し、
  利用者自身に不正コマンドを実行させる
  - マルウェアではないので、通常セキュリティを回避

[警察庁公開の注意喚起チラシより]

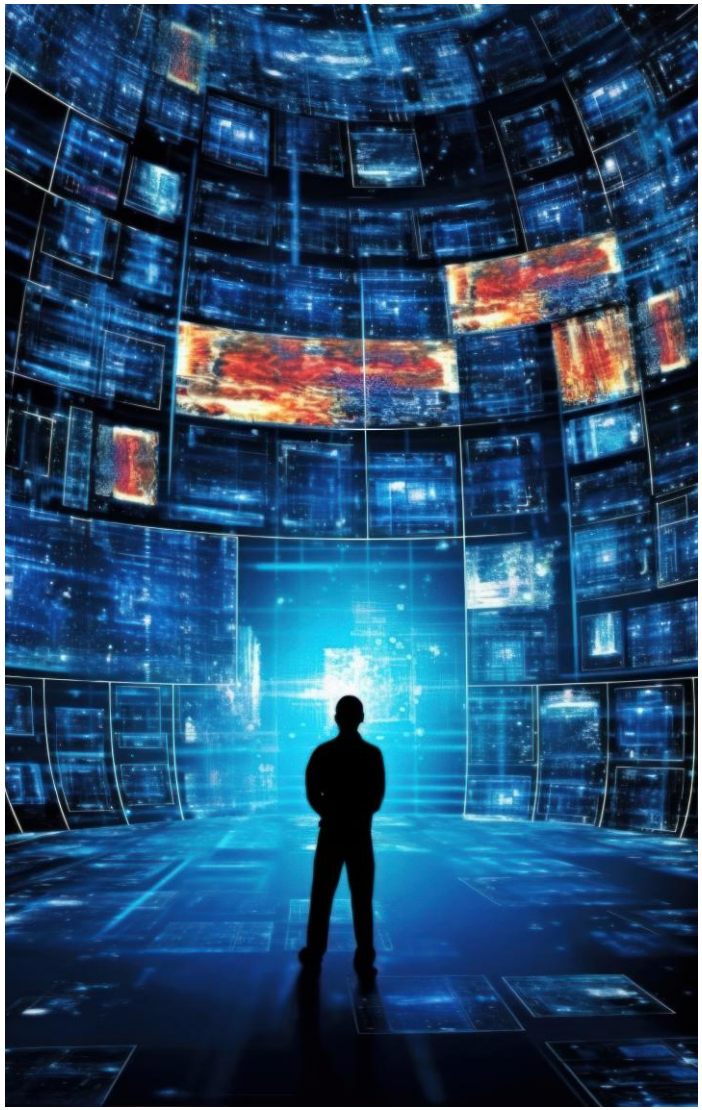


社長名を騙りLINEグループへ誘導する「CEO詐欺」

- 会社の社長や役員の実名を騙り、従業員をLINEグループへ誘導して現金を振り込ませる
- 東京都内だけでも、わずか数週間で約1億4000万円の被害

最新マルウェア情報

- 「ファイルレス」マルウェア
  - 記憶媒体でなく、PCメモリ上に感染
  - アンチマルウェアソフトのフルスキャンでも検知が困難
- 「BIOS感染」マルウェア（Boot kit）
  - OS起動前のBIOSに感染し、アンチマルウェアソフトに正常と誤認識させる
  - OSを初期化（再インストール）しても完全に削除できない
- 「PC内生成」マルウェア
  - セキュリティに検知されないようにマルウェアをパーツとして収集、PC内でマルウェア生成
  - PC内のAIモデルを悪用し、そのPCのセキュリティをかいくぐるためのカスタム攻撃スクリプトを生成する（例：ランサムウェア「PromptLock」）



サイバーセキュリティ最前線

- 境界線セキュリティから「ゼロトラスト（何も信用しない）」セキュリティへ
  - 感染を考慮した多層防御セキュリティの構築（IPA推奨）
    - 入口対策としてのUTM 設置は企業として、当然
    - 自社のシステム環境を考慮したゼロトラスト製品の導入

- セキュリティ意識の向上

  セキュリティ機器・ツールをすり抜ける攻撃を回避する
    - ヒューマンエラーに誘導する攻撃に対する意識を持つ
    - 自身の名前が記載されていないメールは疑う
    - 既知の取引先、同僚、サービスでもメールアドレスを確認する