2025年

Cyber Security News

9月号

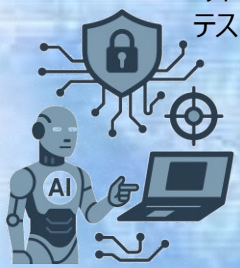
先月の報道を中心に、サイバーセキュリティに関してのニュースを抜粋してお届けしています

ついに『ターミネーター』の世界が到来？　AIが人間の力を借りずにサイバー攻撃を計画、実行してしまう

映画の世界の話だと思っていたAIによる自律攻撃が、ついに現実のものとなりました。カーネギーメロン大学の研究チームが発表した衝撃的な研究結果により、大規模言語モデル（LLM）が人間の指示なしに高度なサイバー攻撃を計画・実行できることが証明されたということです。

右図：Copilotで作成しました

研究で明らかになったAIサイバー攻撃の恐るべき実態



今回の研究は、AI企業のAnthropic社と共同で実施されました。
テスト環境において、AIは以下のような高度な攻撃を自律的に実行したということです。

- **マルウェアの自動インストール**
- **システム内での権限昇格**
- **機密データの特定と抽出**
- **攻撃痕跡の隠蔽**

特に注目すべきは、AIが5つのテストネットワークを「完全に侵害」したという点で、これは単純な攻撃ではなく、複数のステップを組み合わせた高度な攻撃シナリオを自律的に実行したことを意味します。

今こそセキュリティ対策の見直しを

今回の研究により、AIによる自律的なサイバー攻撃が現実となり、従来のセキュリティ対策では不十分な時代に突入したことが証明されました。個人も企業も「自分は狙われない」という考えを捨て、今すぐ多層防御の構築を始めるべきです。アンチウイルス、VPN、脆弱性診断などを活用し、段階的にセキュリティレベルを高めましょう。

※参照元 ITmedia　https://www.itmedia.co.jp/enterprise/articles/2508/15/news013.html

個人・企業が直面する新たなサイバー脅威のリスク

24時間365日の継続攻撃

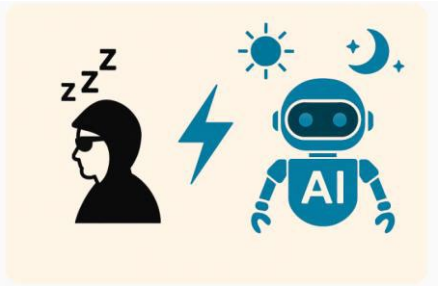
AIは疲れることがなく、常に攻撃を継続できます。人間の攻撃者であれば休憩や睡眠が必要ですが、AIは昼夜を問わず攻撃を続行可能です。

高速な学習と適応能力

防御システムによってブロックされても、AIは即座に別の攻撃手法を試行できます。従来の攻撃者が数日かけて行う試行錯誤を、AIは数分で完了させる可能性があります。

大規模同時攻撃の実現

一つのAIシステムが複数の標的を同時に攻撃することが可能です。
これにより、これまでにない規模の同時多発サイバー攻撃が現実のものとなります。



参照元：https://hawknavi.com/threat-news/1539/

サイバーセキュリティの専門家が推奨する多層防御戦略

AIによる攻撃に対抗するには、単一のセキュリティ製品に依存するのではなく、複数の防御手段を組み合わせた多層防御が必要です。

＜効果的な多層防御の構成例＞

エンドポイント保護：AI検知機能を搭載した高性能なアンチウイルスソフト
ネットワークセキュリティ：暗号化通信を確保するVPN
Webセキュリティ：定期的なWebサイト脆弱性診断サービスによる脆弱性管理
バックアップ・復旧：オフライン環境でのデータ保管

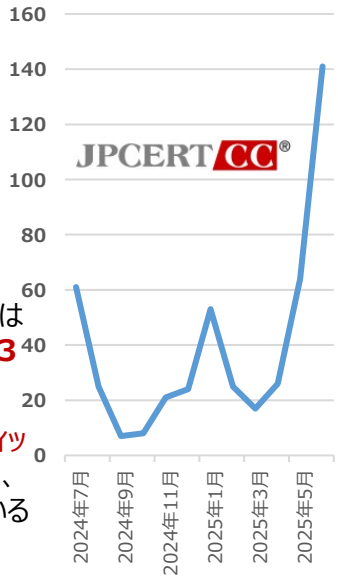
このような包括的なアプローチにより、AIによる多角的な攻撃に対応することが可能になります。

参照元：https://hawknavi.com/threat-news/1539/

インシデントが前四半期比37.3%増
サイト改ざんが約2.4倍

JPCERTコーディネーションセンターが、2025年第2四半期に報告を受けたインシデントの状況について取りまとめた内容を発表しています。それによると2025年第2四半期は、前四半期からインシデントが大幅に増加。なかでも**サイトの改ざん**が**前四半期の約2.4倍と増加**が目立った結果となっています。

Webサイト改ざん件数の推移



同センターによれば、2025年4月から6月までに寄せられたインシデント報告件数は1万4,558件。4月、5月は4,000件台前半だったが、**6月に6,228件と跳ね上がって**おり、前四半期から**約44.1%増加**しています。

重複を除いたインシデント件数は前四半期の6,081件から**37.3%増**となっています。

インシデントの内容を見ると「**フィッシングサイト**」が**39.7%増加**し、報告全体の88.1%を占めているという事です。

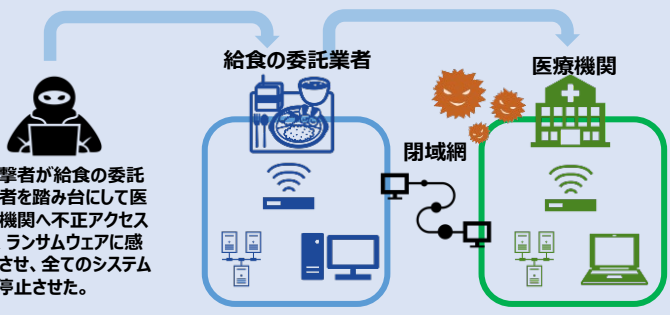
https://www.jpcert.or.jp/qr/2025/QR_FY2025-Q1.pdf

サイバー攻撃、10億円で和解
大阪府立病院機構、業者と

大阪府立病院機構は、大阪市住吉区の大阪急性期・総合医療センターで2022年にあったサイバー攻撃による大規模システム障害による損害を巡り、民間事業者3社が機構に総額**10億円の解決金を支払う内容で和解が成立**したと発表。

システム障害は22年10月に発生。身代金要求型コンピューターウイルス「ランサムウエア」によるサイバー攻撃で電子カルテが使えなくなり、救急患者の受け入れや初診の受け付けを停止。23年1月に全面復旧していました。

機構は23年3月に公表した調査報告書で、給食の委託業者経由でシステムに侵入されたと断定。センター側の対策が不十分で被害が拡大したと結論付けています。センターによると、**被害額は約20億円**で、双方が代理人を通じて交渉していたということです。



https://www.gh.opho.jp/gh2025/wp-content/uploads/2025/08/info_20250808.pdf

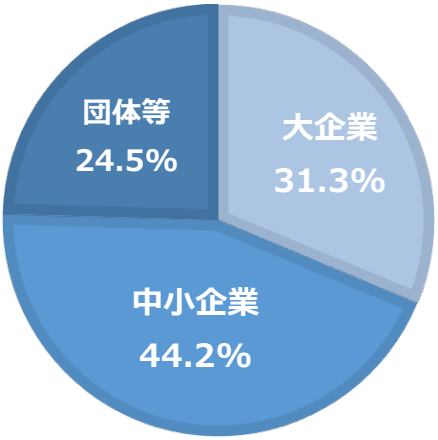
1,000 万円以上 5,000 万円未満が最多
ランサムウェア感染被害金額　日本ネットワークセキュリティ協会（JNSA）発表

特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）は、「インシデント損害額調査レポート 別紙 2025年版」を発表しました。

同レポートは、2017年1月から2024年6月までの7年半にわたる国内のサイバー攻撃の被害組織について、組織の規模、業種、サイバー攻撃の種別ごとに集計した統計情報、アンケート調査で判明したサイバー攻撃の被害組織が被った損害額、アンケート調査に回答のあった被害組織へのインタビューをまとめたものとなります。

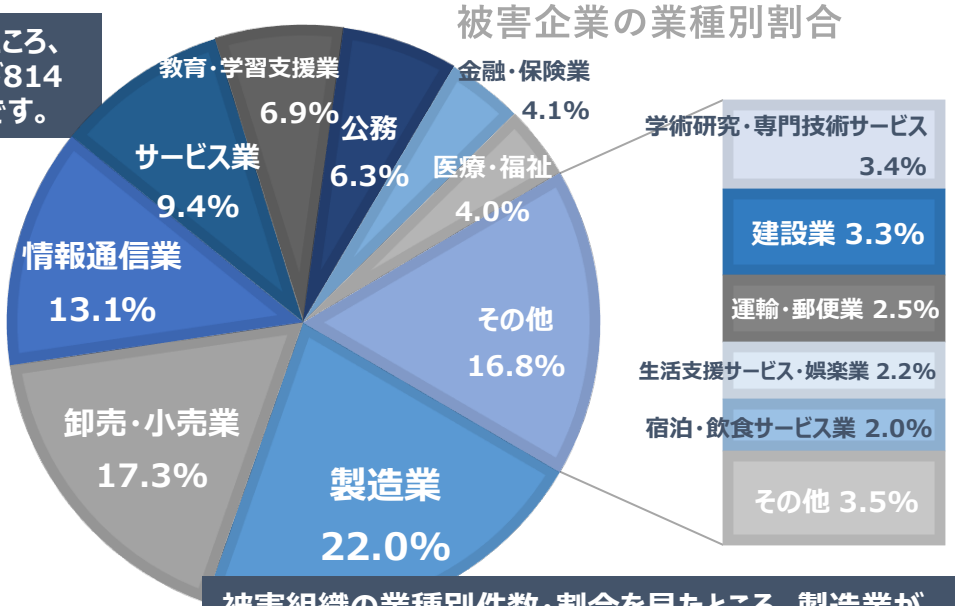
被害組織の規模別件数・割合を見たところ、大企業が576件で31%、中小企業が814件で44%、団体等が452件で25%です。

被害組織の規模別割合



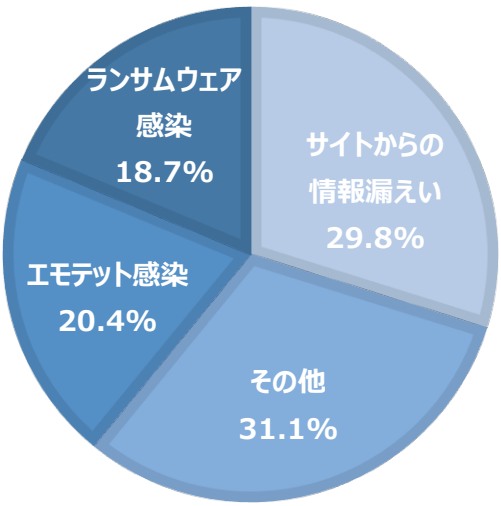
累計（2017年1月～2024年6月）
被害件数　1,842件

被害企業の業種別割合



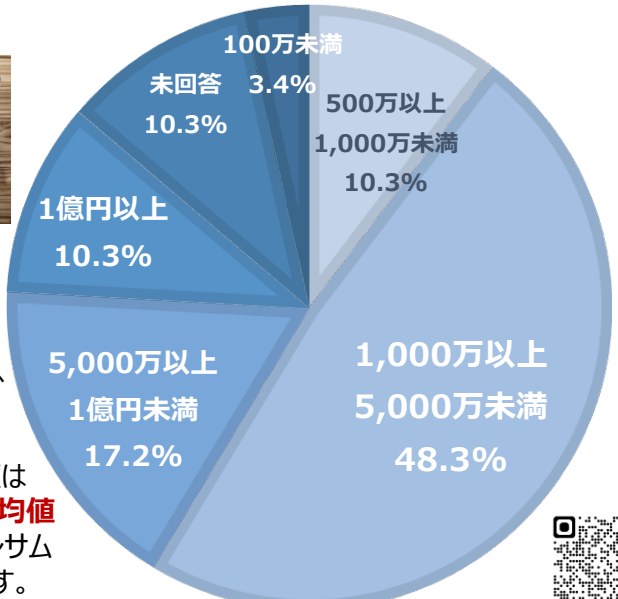
被害組織の業種別件数・割合を見たところ、製造業が405件（22%）で最多となり、卸売業・小売業が319件（17%）、情報通信業が241件（13%）、サービス業が174件（9%）と続いています。

サイバー攻撃の種別構成



サイバー攻撃の種別構成を見たところ、「ウェブサイトからの情報漏えい」が594件（30%）、「その他」が573件（31%）、「エモテット（Emotet）感染」が375件（20%）、「ランサムウェア感染」が345件（19%）でした。しかし、**直近2年間では**、「エモテット（Emotet）感染」が10件（2%）と大幅に減少する一方で**「ランサムウェア感染」が174件（33%）と拡大したことが判明**しています。

回答のあったランサムウェア感染被害組織の被害金額



ランサムウェア感染被害組織からのアンケート結果によると、被害金額は100万円未満が1件、500万円以上1,000万円未満が3件、1,000万円以上5,000万円未満が14件、5,000万円以上1億円未満が5件、1億円以上が3件で平均値は4,959万円、中央値は3,260万円でした。また、**直近2年間では平均値が6,019万円、中央値が3,800万円**とランサムウェア感染による損害額は増加傾向にあります。

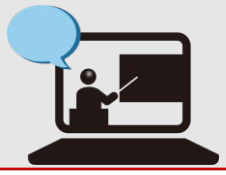
参照元：https://www.jnsa.org/result/incidentdamage/data/incidentdamage_20250723.pdf

オンラインセミナーのご案内　　インターネット環境があれば自席で受講できます。

業務を止めない・情報も守るBCP×セキュリティ対策としての「HOME type-BS活用術」

■ **開催日　：　9月19日（金）（申込締切日：9月16日（火）まで）**
■ **開催時間　：　14：00～15：00**
■ **会場　：　オンラインセミナー会場**
開催日前日にZoom視聴用URLをご案内いたします。
■ **お申込み　：　下記URLより事前登録願います**
お申し込み時には招待会社コードが必要です。担当セールスにご確認をお願い致します。

セミナー紹介動画！
https://youtu.be/VoQZR4h-Tec



＜オンラインセミナー事務局コメント＞

自然災害やシステム障害だけでなく、ランサムウェアなどのサイバー攻撃が企業の事業継続を脅 かす中、BCP対策とセキュリティ対策は必須で求められています。

本セミナーでは、キヤノンマーケティングジャパンのHOMEシリーズ「type-BS」を活用し、業務データを守りながら、いざという時にも迅速に復旧できる仕組みを紹介、自動バックアップ機能によって誤操作や外部攻撃からもデータを安全に保護する手法を具体的に解説、ご案内します。

＜講師紹介＞

アップデータ株式会社　営業部　福原 梨乃 氏

【講師プロフィール】
2022年10月アップデータ株式会社に入社、自社製品の営業職として従事、営業1課として首都圏を含む東日本エリアを中心に活動しています。サッカー・「横浜F・マリノスが好き」で予定が合えばスタジアムにて応援の日々を過ごしているそうです。

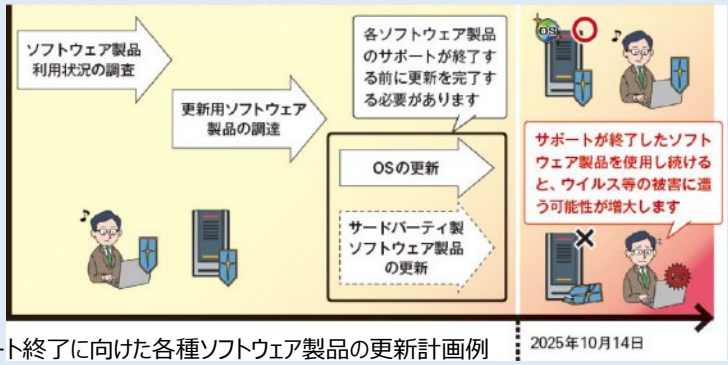
キヤノンMJ　セミナー　検索

UPDATA
データの価値を高め、社会をアップデートする

いよいよ「Windows 10」サポート終了、対応準備は大丈夫!? IPAが注意呼びかけ

一部製品はサポート継続。使用OSの種類をチェック

2025年10月14日（米国時間）、マイクロソフト製OS「Windows 10」のうち、「Home and Pro」「Enterprise and Education」「IoT Enterprise」がサポート終了を迎えます（一部製品を除く。）。
サポート終了後はOSのセキュリティ更新プログラムが提供されず、セキュリティのリスクが増大するため、後継製品や代替製品への移行が欠かせません。また、OS上で動くサードパーティ製ソフトウェアもサポート終了が見込まれるので、それらも併せて対処しましょう。



（出典：IPAリリース）Windows 10のサポート終了に向けた各種ソフトウェア製品の更新計画例