2025年

Cyber Security News

3 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

IPA 情報セキュリティ10大脅威2025 公表

IPAは情報セキュリティ対策の普及を目的として2006年から、前年に発生した情報セキュリティ事故や攻撃の状況等から脅威を選出し、上位10位を公表しています。
「情報セキュリティ10大脅威 2025」は、2024年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです。

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）	前年順位
1	ランサムウェア攻撃による被害	2016年	10年連続10回目	1
2	サプライチェーンや委託先を狙った攻撃	2019年	7年連続7回目	2
3	システムの脆弱性を突いた攻撃	2016年	5年連続8回目	5、7
4	内部不正による情報漏えい等	2016年	10年連続10回目	3
5	機密情報等を狙った標的型攻撃	2016年	10年連続10回目	4
6	リモートワーク等の環境や仕組みを狙った攻撃	2021年	5年連続5回目	9
7	地政学的リスクに起因するサイバー攻撃	2025年	初選出	圏外
8	分散型サービス妨害攻撃（DDoS攻撃）	2016年	5年ぶり6回目	圏外
9	ビジネスメール詐欺	2018年	8年連続8回目	8
10	不注意による情報漏えい等	2016年	7年連続8回目	6

参照元　IPA　情報処理推進機構：https://www.ipa.go.jp/security/10threats/10threats2025.html

半数以上が業務停止　日本企業が直面するランサムウェア危機

現代の脅威に対するセキュリティアーキテクチャなどを提供するセキュリティベンダーのIllumio社（米）は、ランサムウェアの脅威に関するグローバル調査レポート「The Global Cost of Ransomware Study」を発表しました。

同レポートによると、ランサムウェア攻撃を受けた**日本企業の51%が業務停止**に陥り、**48%が顧客を失い**、**45%が雇用削減**を余儀なくされています。また、**35%が大幅な減収を経験**していることが判明しています。

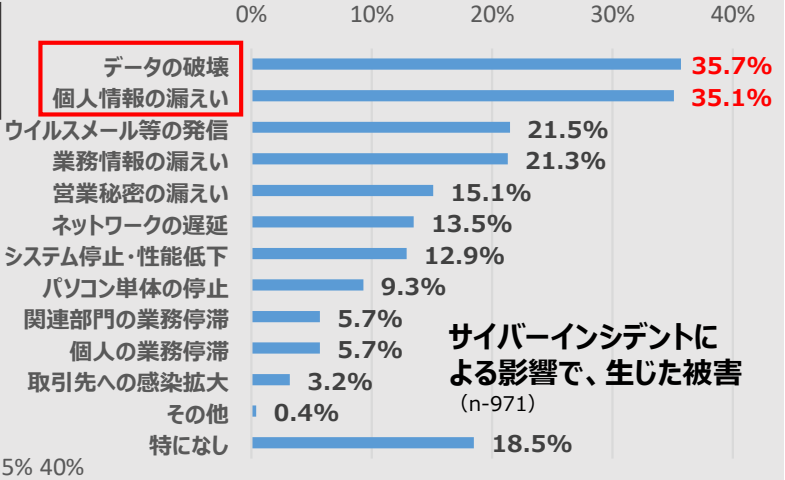
さらに、ランサムウェア攻撃を受けた**日本企業の70%が、（警察などの）法執行機関への報告をしていません**でした。報告しなかった主な理由は、事件を公表したくない（38%）、支払い期限が迫っている（37%）、報復を恐れている（29%）などが挙げられています。

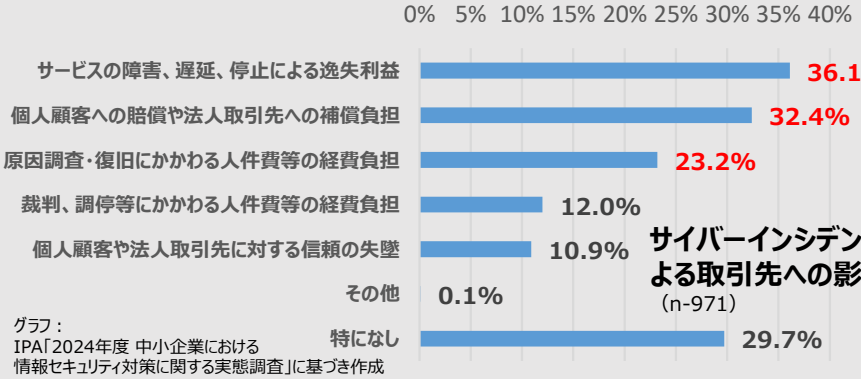
参照元　https://www.illumio.com/ja/news/cost-of-ransomware-study

中小企業の7割で サイバー攻撃被害が取引先にも影響

経済産業省は**独立行政法人情報処理推進機構（IPA）**を通じて実施した**「2024年度中小企業における情報セキュリティ対策の実態調査報告書」**の速報版を2月14日に公表しています。

調査結果によると、2023年度にサイバーインシデントの被害を受けたと回答した企業975社のうち、サイバーインシデントによる影響として**「データの破壊」と回答したのは35.7%**、**「個人情報の漏えい」と回答したのは35.1%**となっています。





グラフ：
IPA「2024年度 中小企業における情報セキュリティ対策に関する実態調査」に基づき作成

また、取引先への影響については**「取引先にサービスの停止や遅延による逸失利益」が36.1%**、**「個人顧客への賠償や法人取引先への補償負担」が32.4%**、**「原因調査・復旧に関わる人件費等の経費負担」23.2%**となっています。

中小企業の6割が「情報セキュリティ対策投資をしていない」

直近過去3期の**情報セキュリティ対策投資額**（IT機器や社員への教育等も含む）について尋ねたところ、**「情報セキュリティ対策投資をしていない」企業は62.6%**で、**2016年**度調査の**55.2%**、**2021年**度調査の**33.1%**からさらに増加していることが判明しています。

「サイバードミノ」を防ぎ、取引先の信頼を得るセキュリティ対策が急務

過去3年間にサイバー攻撃の被害に遭った**中小企業のうち**、「特になし」と回答した29.7%を除くと**約7割が取引先にも影響が及んだ**と回答しており、いわゆる**「サイバードミノ」**が起きているという実態が明らかな結果となりました。

一方で、普段からセキュリティ対策投資を行っている中小企業の約5割が、取引先との取引につながったと実感しているという実態も判明しています。

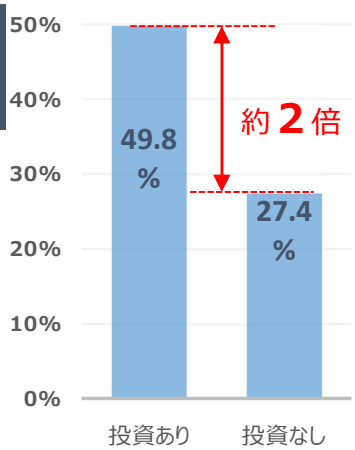
参照元　独立行政法人情報処理推進機構（IPA）
https://www.ipa.go.jp/pressrelease/2024/press20250214.html

取引先は、あなたのセキュリティ対策を見ています!

普段からセキュリティ対策投資を行っていると、そうでない場合の2倍近くの取引につながっています。

要請されたサイバーセキュリティ対策を実施したことが取引につながったと考える企業の割合⇒

過去3年間で対策投資を行った企業の半数が、発注元からの要請でサイバーセキュリティ対策を行ったことで取引につながったと回答しているのに対し、投資を行っていない企業では3割弱に留まっています。



グラフ：
IPA「2024年度 中小企業における情報セキュリティ対策に関する実態調査」に基づき作成

参照元：　経済産業省
https://www.meti.go.jp/press/2024/02/20250219001/20250219001.html

年末年始に相次いだDDoS攻撃を受け、内閣サイバーセキュリティセンターが注意喚起を実施

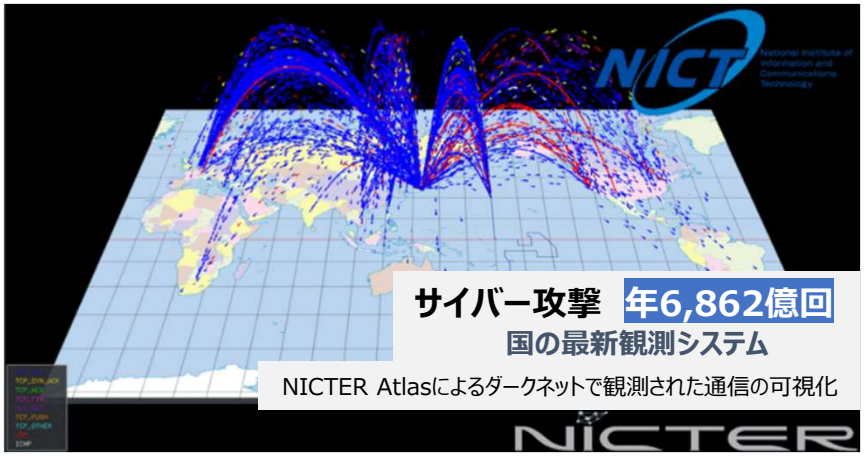
内閣サイバーセキュリティセンター　（NISC）は2月4日、2024年12月から2025年1月の年末年始にかけ、DDoS攻撃が相次いで発生していることから、各事業者に向け、適切なセキュリティ対策を講じるよう注意喚起を実施しています。

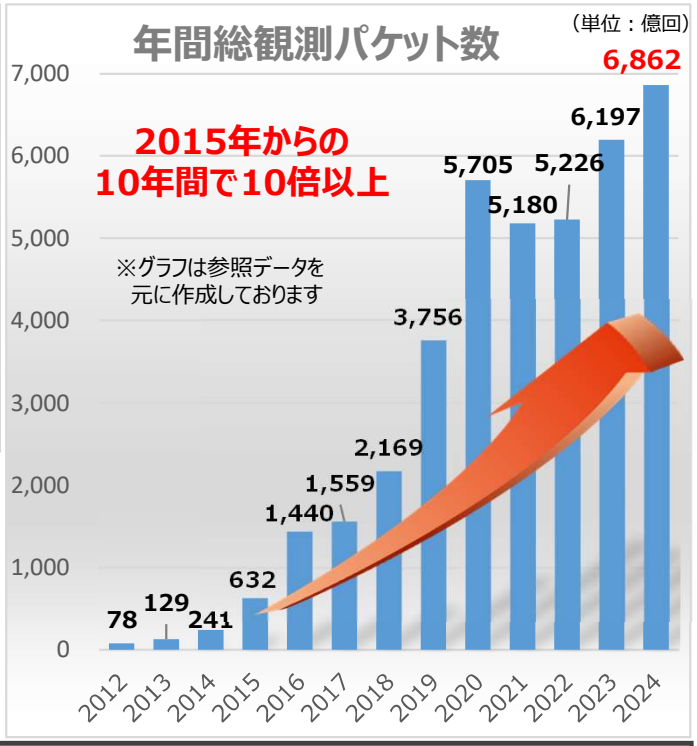
NISCでは、費用がかかる対策もあるが、まずは機器やシステムの設定見直し、ソフトウェアの更新など、身近な対策から進めてほしいとしています。

参照元　内閣サイバーセキュリティセンター（NISC）
https://www.nisc.go.jp/pdf/news/press/20250204_ddos.pdf

狙われるニッポン… サイバー攻撃年間6,800億回！11%増加

ネット社会でますます脅威となるサイバー攻撃。国立研究開発法人情報通信研究機構（NICT） サイバーセキュリティネクサスは、NICTER観測レポート2024を公開しました。それによると、NICTERプロジェクトの大規模サイバー攻撃観測網で2024年に観測されたサイバー攻撃関連通信は、**2023年と比べて11%**増加しています。日本を狙ったサイバー攻撃は増え続け、１ IPアドレス当たり約243万パケットが1年間に届いた計算になります。





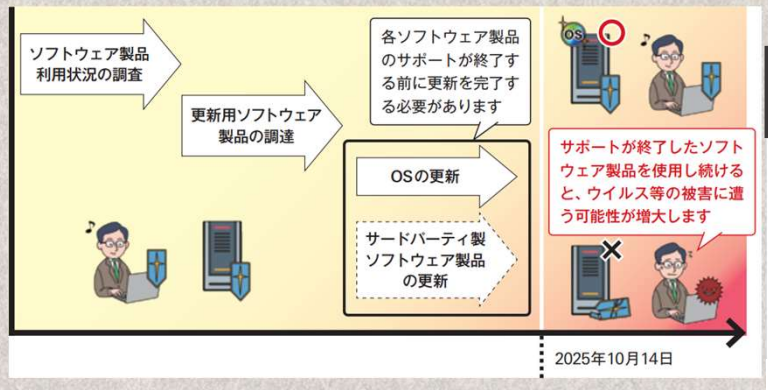
NICTERのダークネット観測網（約29万IPアドレス）において2024年に観測されたサイバー攻撃関連通信は、合計6,862億パケットに上り、2024年もインターネット上のIoT機器や脆弱性を狙った調査が活発に行われていることが分かります。**日本国内では、1日当たり**約730～11,500ホストが**IoTボットに感染**していることが確認され、平均すると**1日当たり約2,600台**のIoT機器**が感染している状況**です。

参照元：https://www.nict.go.jp/press/2025/02/13-1.html

IPA（独立行政法人 情報処理推進機構）から「Windows 10 のサポート終了に伴う注意喚起」がアナウンスされました

2025年10月、**Windows 10のサポートが終了**します。
サポート終了後はセキュリティ更新プログラムの提供がなくなり、セキュリティリスクが高まるため、同ソフトウェア製品の利用者は、サポートが継続している後継製品、または代替製品への移行などの対応が望まれます。
また、OSだけでなく、対象OS上で稼働するアプリケーションもサポートが順次終了していくため、あわせて対策が必要となります。

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



図：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
（IPA NEWS vol.71 3月号より）

サポートが終了したOSをアップデートしなかった場合

Windows OSや ExcelやWordなどのMicrosoft Office製品は使用者が多いため、サイバー攻撃者の標的となりやすい傾向があります。サポート期間終了後に新たな脆弱性が発見されても、更新プログラムは原則として配布されなくなります。更新プログラムが適用できない古いOSや古いMicrosoft Officeを使い続けることでマルウェアの感染の危険性が高まります。

※IPA「Windows 10 のサポート終了に伴う注意喚起」より
https://www.ipa.go.jp/security/security-alert/2024/win10_eos.html

ランサムウェア攻撃グループ「8base」構成員とみられる ロシア人被疑者4人を検挙、警察庁が発表

警察庁は2月12日、ランサムウェア攻撃グループ「8base」を主導していたとみられるロシア人被疑者4人が検挙されたことを発表しています。

8baseは、主に中小企業を狙った攻撃を行うとされ、日本での事例では、日本生命や公文教育研究会(KUMON)、徳島県、和歌山市など複数の企業や自治体の業務を受託し、ランサムウェア被害に遭ったイセトーや太陽工業、株式会社ISEKI Japan北海道カンパニー（旧：ヰセキ北海道）を攻撃したグループであると指摘されています。

参照元 https://www.npa.go.jp/news/release/2025/20250212001.html

個人情報保護委員会、中国AI「DeepSeek」利用に注意喚起　林官房長官も「留意を」

個人情報保護委員会は2月3日、**中国のAIベンチャー**が開発した**生成AI「DeepSeek」**のプライバシーポリシーに書かれている内容について説明し、**注意喚起**しました。これを受け、４日の会見で林官房長官も「こうした情報提供に留意してほしい」としています。

DeepSeekをめぐっては、その性能が注目を集める一方で、個人情報などが中国政府へ流出する危険性が指摘されており、国内でも複数の企業や自治体が利用を禁じています。

参照元　個人情報保護委員会
https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/

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。

Windows 10からの移行計画
Windows 11導入で実現するこれからのPC環境

- **開催日　：　3月21日（金）（申込締切日：3月18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**
  URL：https://canon.jp/business/event
  お申し込み時には招待会社コード「DM0001」をご使用ください。

セミナー紹介動画！
https://www.youtube.com/watch?v=3PF1I6TT_rY

キヤノンMJ　セミナー　検索

申し込みQRコード

Windows 10のサポート終了に伴うWindows 11への移行の重要性と、ビジネスPCの移行についてのポイントを紹介します。

- 移行にあたっての課題やメリットの整理
- 生成AIの活用：Microsoft Copilotなどの生成AIが業務の効率化や生産性向上に役立つ
- 管理：　クラウドを利用した効率的かつ品質の高いPCの管理

是非この機会にご参加ください。

中小・ベンチャー　働き方改革　ITソリューション　セキュリティ

登壇者：　日本マイクロソフト マスタートレーナー
赤井 誠 氏

大阪・関西万博で想定されるサイバー攻撃の脅威

OSAKA, KANSAI, JAPAN EXPO 2025

ぜんぶのいのちと、
ワクワクする未来へ。

2025年は、**大阪・関西万博**が開かれ、関西や大阪が世界的に有名になり、名前を売ろうとするグループが、サイバー攻撃を仕掛ける可能性が高まると懸念されています。

【想定されるサイバー攻撃の脅威】
①DDos攻撃
②ランサムウェア
③偽情報（フィッシング、悪質ECサイト）

既に、万博の公式アカウントを装う偽アカウントが確認されたと発表されています。

（参考）大阪・関西万博（博覧会協会）の公式サイトより

7位ランクインした『地政学的リスクに起因するサイバー攻撃』も関連？！

地政学的リスクとは、**国家間の政治的・経済的な緊張や対立が原因で発生するサイバー攻撃のこと**です。近年の戦争等がこれらのリスクとなります。大規模な国際イベントである大阪・関西万博にとっても重要な懸念事項です。万博のようなイベントは、多くの国や企業が参加し、注目を集めるため、サイバー攻撃の標的になりやすいです。

【具体的な対策例】
①DDos攻撃対策：ファイアウォールやルーターの設定など
②機密情報の保護：多層防御の導入、バックアップ体制の見直しなど
③偽情報対策：ファクトチェック機関の活用　など

ファクトチェックとは？
SNSやウェブ上で拡散される情報の真偽を検証し、結果を公開します。

【参考】日本ファクトチェックセンター（JFC）
https://www.factcheckcenter.jp/