2025年

# Cyber Security News

2 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

## 2025年　日本国内のITトレンドは？

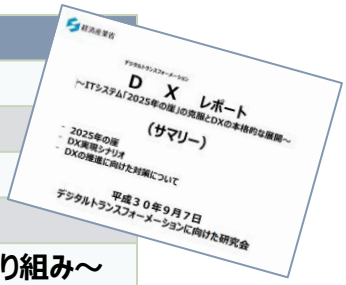

## 経済産業省が指摘した重大なリスク『2025年の崖』

**「2025年の崖」とは、2018年に発表され、企業がデジタルトランスフォーメーション（DX）を進めないと、2025年以降に年間最大12兆円の経済損失が発生する可能性があるという警告です。主な原因は、古いITシステムの老朽化や複雑化です。企業はDXを推進し、これらのシステムを見直す必要があります。**

経済産業省ウェブサイトより

### 情報セキュリティ監査人が選ぶ　情報セキュリティ10大トレンド（2025年予測）

| ランク | 項目 |
|---|---|
| 1 | 組織化、ビジネス化するランサムウェア攻撃 |
| 2 | 国際情勢の不安定化に伴い激化するサイバー攻撃 |
| 3 | 野放しになっていませんか？急速に普及するAI利活用 |
| 4 | AIの攻撃への悪用 |
| 5 | 急がれるサプライチェーンセキュリティ対応 ～上流から下流まで一体となって守る取り組み～ |
| 6 | クラウドサービスに起因した大規模障害によるビジネスリスク |
| 7 | サイバー人材不足が引き起こす経営リスクの増加 |
| 8 | 進まないDX化　～「2025年の崖」から転落するリスク～ |
| 9 | 急がれるサイバー安全保障への備え ～ 指定事業者の委託先も無縁ではいられない ～ |
| 10 | 急速なIDの集約化がもたらす被害拡大 |




出典：日本セキュリティ監査協会

セキュリティのプロが選ぶ！

# JNSA 2024セキュリティ 10大ニュース

| | | |
|---|---|---|
| 【第１位】 | 7月19日 | 「史上最大規模」の障害引き起こしたクラウドストライク<br>～影響受けた端末は850万台、損失は54億ドル～ |
| 【第２位】 | 11月29日 | 「能動的サイバー防御」法整備への提言まとまる<br>～セキュリティクリアランス制度も具体化、頑張れ日本！～ |
| 【第３位】 | ６月９日 | KADOKAWA「サイバー攻撃」が示した経営リスク<br>～ハッカー集団が闇サイトで犯行声明、36億円の特別損失を計上～ |
| 【第４位】 | 2月14日 | AIセーフティ・インスティテュート（AISI）を設立<br>～AI安全性評価法検討進む、一方セキュリティへの活用や悪用も進む～ |
| 【第５位】 | 1月1日 | 能登半島地震に乗じてSNS上に偽情報が拡散<br>～選挙でも増すSNSの存在感と問われる偽情報対策～ |
| 【第６位】 | 11月21日 | 偽のウイルス感染警告を表示させるサポート詐欺に注意<br>～IPAへの相談件数過去最高、金銭被害に加え個人情報流出の可能性も～ |
| 【第７位】 | 4月16日 | LINEヤフーの情報漏洩に2度目の行政指導、国家間問題へ<br>～親会社との資本関係の見直しを求める総務省に韓国政府らが懸念表明～ |
| 【第８位】 | ５月29日 | イセトーへのランサムウェア攻撃　全国多数の委託元が影響を受ける<br>～委託元の自治体や企業などから被害公表が相次ぐ～ |
| 【第９位】 | 5月1日 | 太陽光発電、サイバー攻撃の温床に　IoT経由で不正送金<br>～インターネットに直接つながるIoT機器の脆弱性、ハッカーが悪用～ |
| 【第10位】 | ７月５日 | JAXAにおいて発生した不正アクセスによる情報漏洩<br>～政府組織は高度なサイバー攻撃の標的としてより強固な対策を～ |

**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)が作成している10大ニュースで2024年を振り返ると！**

2024年の10大ニュースのトップはクラウドストライクが引き起こした史上最大規模の障害が選出されています。前向きのニュースとして能動的サイバー防御とAIセーフティ・インスティテュート（AISI)の設立がランクインし、KADOKAWAやイセトーのランサムウェア被害に太陽光発電やJAXAへのサイバー攻撃などに加えて、サポート詐欺やLINEへの行政指導のニュースが並び、選挙に影響を与えた偽情報やフェイクニュースは５位に入っています。

サイバー空間は人類の幸福に味方するのか、あるいはさらなる混乱をもたらすのかの分岐点は技術に依存するというよりもますます政治への依存度を高めています。その政治体制の確立がサイバー空間に依存するとなると、混乱にさらに拍車をかけることにもなりかねません。サイバー攻撃の被害が拡大の傾向にあることも気がかりで、これらの懸念払しょくへの手がかりを早く確実なものにしたい、そう感じさせる2024年のセキュリティ10大ニュースでした。

↓参照元：https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html

↑参照元：https://www.jnsa.org/active/news10/

## 日本のみを標的、先端技術情報窃取が目的か
## 中国系サイバー攻撃集団「ミラーフェース」

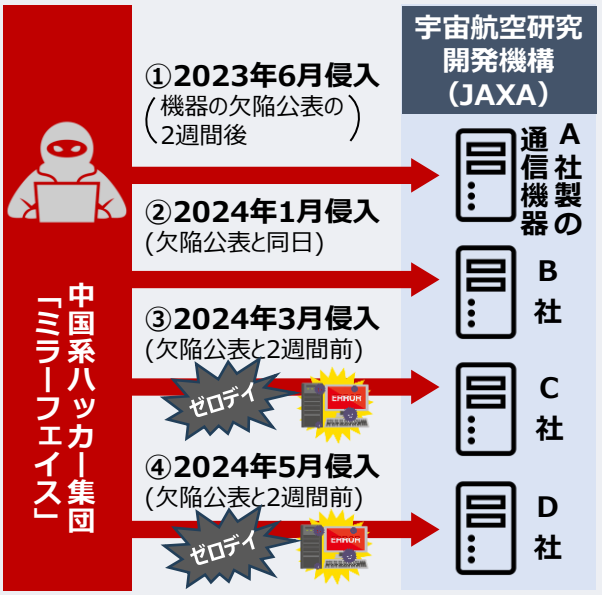
警察庁と内閣サイバーセキュリティセンター（NISC）は8日、中国系ハッカー集団「MirrorFace（ミラーフェイス）」によるサイバー攻撃が2019年以降に210件確認されたと明らかにしています。機密性が高い情報の窃取が目的とみられ、先端技術や安全保障に関連する企業・団体が標的とされました。

**ミラーフェイスによるサイバー攻撃の特徴**

| 攻撃時期 | 対象 | 手口 |
|---|---|---|
| 2019～23年ごろ | 安全保障、国際関係に関連する政府機関、政治家、マスコミなど | メールに添付したマルウェアに感染させる標的型メール攻撃 |
| 2023年ごろ～ | 半導体、情報通信、航空宇宙といった先端技術を持つ企業など | VPN機器などの脆弱性を悪用するネットワーク貫通型攻撃 |
| 2024年ごろ～ | 安全保障、国際関係に関連する政府機関、政治家、マスコミなど | メールに添付したマルウェアに感染させる標的型メール攻撃 |

※新聞各紙の情報より

## JAXAを狙った「ゼロデイ」サイバー攻撃



# 年6,000億回!? 日本へのサイバー攻撃 重要インフラ相次いで被害

2024年の年末から日本航空や三菱UFJ銀行、NTTドコモなどの企業が相次いでサイバー攻撃を受け、システムの不具合など大きな被害がでています。NICT（情報通信研究機構）によると日本は、1年間で6000億回のサイバー攻撃を受けています。なぜ、日本が標的になるのでしょうか。

**■航空・銀行・通信に相次ぐサイバー攻撃 誰が何の狙いで？**

2024年12月26日、JALでネットワーク障害が発生し、欠航や遅延、荷物のチェックインができなくなるなどの影響が出ました。DDoS（ディードス）攻撃とみられています。

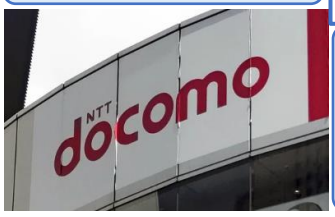
そして、三菱UFJ銀行、りそな銀行、みずほ銀行などの大手銀行で、年末にインターネットバンキングがつながりにくい状態になりましたが、これも、DDoS攻撃とみられています。

**・JAL（'24/12/26）**
**ネットワーク障害で欠航や遅延、荷物のチェックインができなくなるなどの影響**
**⇒DDoS攻撃とみられる**



**・大手銀行でも**
**三菱UFJ銀行(12/26)**
**りそな銀行(12/28)**
**みずほ銀行(12/31)などで**
**インターネットバンキングがつながりにくくなる状態に**
**⇒DDoS攻撃とみられる**

**NTTドコモ（'25/1/2）**
**DDoS攻撃を受け**
**情報ポータルサイトなど一部のサービスへアクセスしづらい状況に**

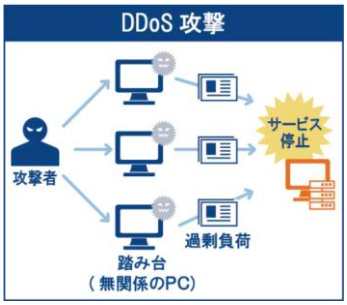




**日本気象協会（'25/1/9）**
**DDoS攻撃を受け**
**天気予報メディア「tenki.jp」のWeb版がアクセスしづらい状態に**
**1/5と1/15にも、サイバー攻撃被害に**

2025年に入っても、NTTドコモがDDoS攻撃を受け、情報ポータルサイトなど一部のサービスにアクセスしづらい状況が発生しました。

また、日本気象協会が運営する天気予報メディア「tenki.jp」のWeb版もアクセスしづらい状況になり、**原因はDDoS攻撃**ということです。




※今回も、無関係なPCやルーターを経由した攻撃の可能性が指摘されており、巻き込まれないために、自社のシステム管理が重要です

## 台湾政府機関へのサイバー攻撃、1日平均240万回　中国の関与指摘

[1月6日 ロイター] 台湾の国家安全局は５日、台湾政府機関に対する昨年のサイバー攻撃が１日平均240万回と、前年の平均120万回から倍増したとの報告書をまとめ、大半が中国のサイバー部隊による攻撃だったとしています。

報告書によると、中国によるサイバー攻撃の一部は台湾周辺での**中国の軍事演習に合わせて行われ**、台湾の**交通機関や金融機関**のウェブサイトへのアクセスを妨害する**ＤＤｏＳ攻撃**などを仕掛けたということです。

参照元　https://jp.reuters.com/world/taiwan/EWZJ6C6WXVIPNABUSGTUELCE6U-2025-01-06/

## 台湾有事 サイバー攻撃シミュレーション

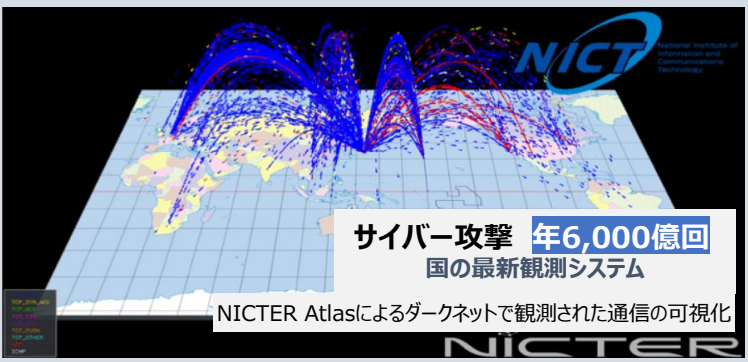
日本のシンクタンクが主催する「台湾海峡危機政策シミュレーション」で中国が台湾進攻した際、最悪の場合に想定されること

**サイバー攻撃が激化すると**
- **政府や報道機関：ウェブサイトが停止**
- **病院：電子カルテのシステムが停止**
- **携帯電話：通信障害が発生**
- **金融機関：オンライン決済が利用不可**
- **放送局：放送システムが破壊**

**実際に、この数年で重要インフラが様々なサイバー攻撃を受けて一時的に止まってしまったケースは多数あり、一部は有事を想定した攻撃の可能性も考えられます**

## 止まらない被害拡大　日本が標的に！

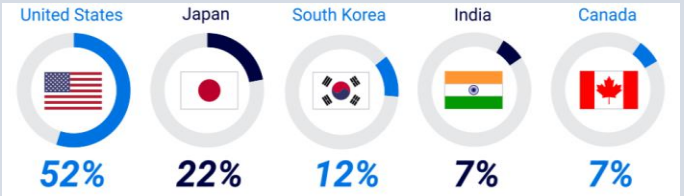
日本へのサイバー攻撃は、1年間で約6000億回と言われています。
これは、情報通信分野の研究開発を行う国立の研究機関、NICTが観測した2023年の日本へのサイバー攻撃の数です。




世界の中で、日本はサイバー攻撃の標的になっています。

参照元　https://news.tv-asahi.co.jp/news_economy/articles/900016342.html

**新たなウイルスなどが検出された数が多い国トップ5**




## 日本が世界で2番目の「標的国」

セキュリティソフトなどを扱う会社・ブラックベリージャパンの調査によると、2024年の4～6月、日本は、新たなウイルスなどが検出された数が世界で2番目に多かったということです。

↑　2024年第2四半期BlackBerry社グローバル脅威インテリジェンス レポート
https://www.blackberry.com/ja/jp/solutions/threat-intelligence/2023/threat-report

**「日本には盗みたくなる機密情報や、お金に換えやすい重要な情報が多く、管理が行き届いていないシステムも増えて、攻撃されるスキができてしまっている」とも指摘されています。**

参照元　https://news.tv-asahi.co.jp/news_economy/articles/900016342.html

**※報道・公表された情報から、一部を抜粋しております。**

ビジネストレンドウェビナーのご案内

インターネット環境があれば
自席で受講していただけます。

# 大阪・関西万博目前！
# サイバー攻撃のターゲットは中小企業へ
## ～エンドポイントセキュリティ最前線～

■ **開催日時 ： 第1回 2025年2月26日（水）14:00-14:45**
**第2回 2025年2月27日（木）14:00-14:45**

■ **定　員　　： 先着 200名 様（各回）**

■ **形　式　　： Zoomオンライン配信**

※第１回/第２回とも内容は同じです。

講師 :キヤノンマーケティングジャパン株式会社
セキュリティソリューション事業推進部　友納　源

大阪・関西万博目前となり、世界から日本へのサイバー攻撃増加が予測され、セキュリティ対策強化の必要性が高まっている状況にあります。中小企業はセキュリティ対策の脆弱性等の理由から、サイバー攻撃の対象となりやすく、早急なセキュリティ対策が求められています。
本セミナーでは、なぜ中小企業が標的になるのか、どのような被害が発生しているのかなど、理由や被害内容を交えて解説します。さらに、対策の基本として、エンドポイントセキュリティに焦点を当て、最新機能や話題のMDR、また多層防御の考え方等もご紹介いたします。

**【第1回】**
**‘25年2月26日(水)**
**① 14:00 – 14:45**

**申込URL↓↓↓**

https://zoom.us/webinar/register/WN_yuiMTKejSgiuyUQeIQEPNQ

**【第2回】**
**‘25年2月27日(木)**
**① 14:00 – 14:45**

**申込URL↓↓↓**

https://zoom.us/webinar/register/WN_6HcSB4PIQ0ytDOO2hpgF2Q

## 大規模サイバー攻撃と爆破予告に備え、京都府警が京都競馬場で訓練

4月に開幕する大阪・関西万博を前に、大規模サイバー攻撃を想定して、京都府警は京都競馬場の駐車場で訓練を実施するなど、緊張感も高まりつつあります。

訓練を行う警護車列＝京都市伏見区

参照元：https://www.itmedia.co.jp/news/articles/2501/09/news170.html

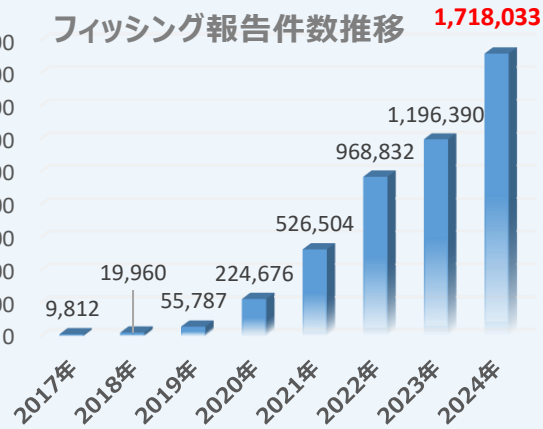
OSAKA, KANSAI, JAPAN EXPO 2025

ぜんぶのいのちと、
ワクワクする未来へ。

## フィッシング報告、過去最多を大幅更新

フィッシング対策協議会の発表によると、偽サイトに誘導してクレジットカード情報を盗む「フィッシング」を狙い、金融機関などを装って送り付けられたメールやショートメッセージサービス（ＳＭＳ）の報告件数が2024年、統計を取り始めた‘05年以降で最多だった2023年を大幅に上回り、**過去最多**となることが分かりました。

生成ＡＩで作成したメールが増えたとも言われており、一層の警戒が必要な状況となっています。




参照元：https://www.antiphishing.jp/report/monthly/202412.html