2025年

Cyber Security News

5 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

警察庁発表：サイバー空間をめぐる脅威の情勢等②

不審なアクセス件数が増加の一途 『DDos攻撃』

高度な技術を悪用したサイバー攻撃の情勢

警察庁は3月13日、24年のサイバー空間をめぐる脅威情勢を公表しました。

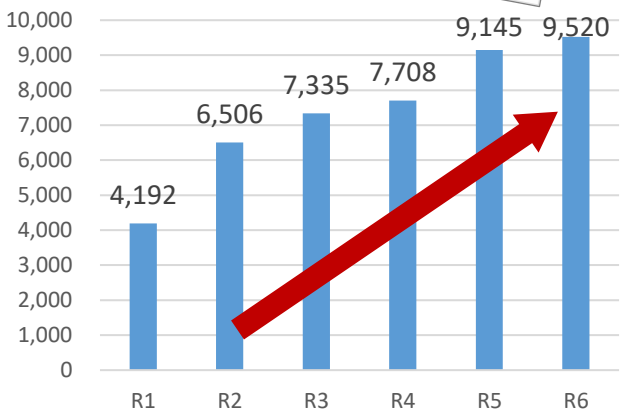
警察庁 National Police Agency

【DDoS攻撃の概要】

- 令和６年の年末年始にかけて、**交通機関や金融機関などの重要インフラ事業者**に対する**DDoS攻撃**が多数発生しました。
- **影響**：空港の手荷物自動チェックイン機が使用不能になったり、インターネットバンキングのログインが困難になるなど、国民の生活に直接的な影響を与えました。
- **複数の手口**：警察は複数種類の手口を確認しており、事業者が遮断措置を講じた場合でも、攻撃者は状況に応じて手口を変化させて攻撃を継続する事例が確認されています。

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

大手銀行
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
繋がりにくくなる状態に

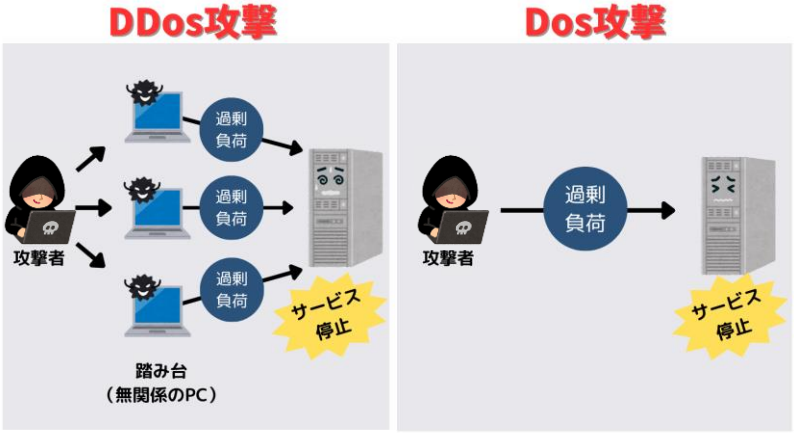


図表1：警察庁が検知した不審なアクセス件数(1日・1 IPアドレスあたり)を元に作図

参照元　警察庁：https://www.npa.go.jp/publications/statistics/cybersecurity/

DDos攻撃とは？知らない間に加害者に？！

DDoS攻撃とは：大量のコンピューターから一斉に特定のコンピューター（サーバー）にデータを送って機能を停止させる攻撃「Distributed Denial of Service attack（分散型サービス拒否攻撃）」の略です。
DoS攻撃とDDoS攻撃の違い：攻撃を仕掛けるコンピューターが単一なのか複数なのかという点です。
・DoS攻撃：ひとつのコンピューターからデータが送出されます。
・DDoS攻撃：ボットネット（マルウェアなどで不正に乗っ取った複数のコンピューターで構成されるネットワーク）など、複数の端末からデータが送出されます。DDoS攻撃では、DoS攻撃よりも多くのデータが送られてくるため、攻撃を受ける側に、より大きな負荷がかかることに注意が必要です。



ボットネットとは？

急にパソコンが重くなったりしていませんか？それは「ボットネット」に感染したからかもしれません。パソコンやスマートフォンを「第三者の指示通りに動く操り人形（ロボット）」にしてしまう悪意のあるプログラムが「ボット」、そのボットをいくつも集めてネットワーク化したものボットネットと呼びます。

ボットが組み込まれる仕組み

・OSやアプリケーションの**脆弱性**を突いた感染
・メールの添付ファイルやリンク経由での感染
・改ざんされたWebサイトの訪問による感染　など

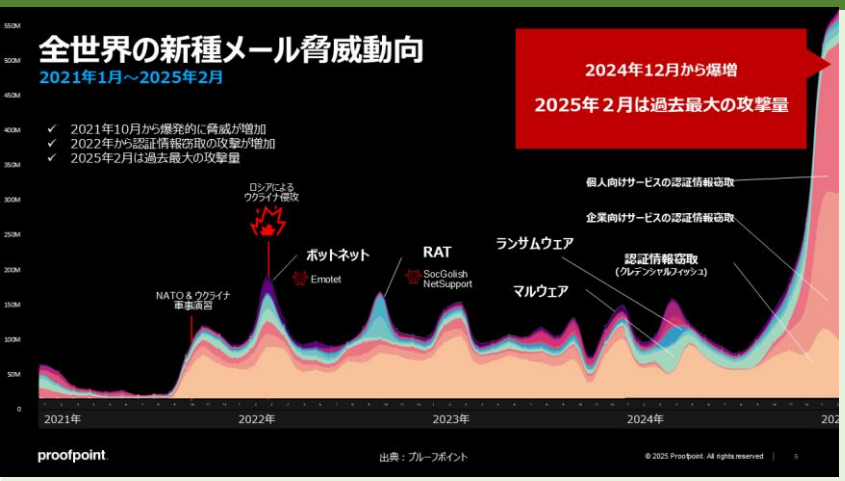
知らない間に取引先に攻撃をしている可能性も・・・

ボットネット化すると、別のコンピュータを攻撃するなどの犯罪行為に加担してしまう恐れがあります。対策は？

1.セキュリティ対策ソフトを導入し、定義ファイルは定期的に更新する
2.OSやアプリケーションの更新プログラムをこまめに適用する
3.不審なWebサイトは閲覧しない
4.不審なメールや添付ファイルは開かない

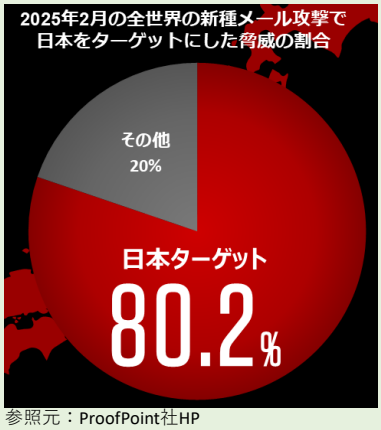
参照元：https://cybersecurity-jp.com/column/25952

AIを活用したクラウドサービスの認証情報を狙ったフィッシングメールが急増中！



【爆増する世界のメール脅威】

■新種メールとは
・主に**クレデンシャル・フィッシング**
・**クラウドサービスにログインするための認証情報を盗む**ことを狙う
・**Microsoft 365やGoogle Workspace**などのクラウドサービスがターゲット
・2022年2月ウクライナ侵攻以降世界的にメールの脅威が急増。**地政学上の緊張がまさにサイバー攻撃に如実に表れている例。**



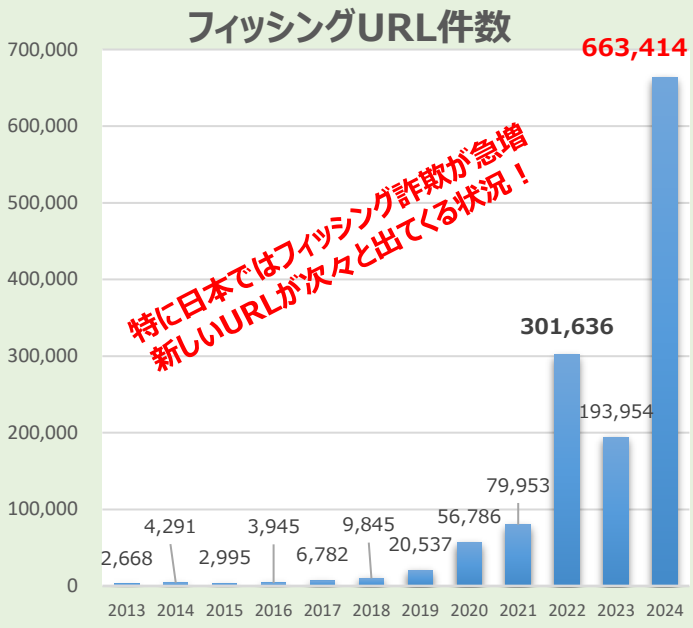
参照元：ProofPoint社HP
https://www.proofpoint.com/jp/blog/email-and-cloud-threats/Japan-is-now-the-most-targeted-country-in-the-world

【今、日本が一番狙われている】

■2025年2月、世界中のメール脅威の**80%以上が日本を狙って**いた。
■日本が標的となる理由：**セキュリティ防御の薄さ、高価値の知的財産、AIの進歩による攻撃の容易さ、地政学的な動機など。**
■日本企業の知的財産：世界的に見ても価値が高く、攻撃者にとって魅力的な標的。
日本人の個人情報（住所、氏名、年齢、電話番号、メールアドレス、クレジットカード情報、医療データ）はアンダーグラウンド市場で高値で売買される。

メールを起点としたランサムウェア攻撃等も多発

春はフィッシング詐欺が増える傾向 注意点をおさらいしよう



サイバー犯罪は我々の身近なところにも潜んでおり、一般から縁遠い存在ではありません。その一例として、フィッシング詐欺が挙げられます。正規のサービスなどを装ったメールやSMSで、ニセのサイトに誘導し、ログイン情報（IDとパスワードなど）やクレジットカード情報を盗み出すというものです。 日本では、Amazonや楽天といったECサイト、銀行やカード会社などの名前をかたり、身に覚えのない支払いやクレジットカードの暗証番号の確認などを催促してくる手口が多発しています。

特に、春の新生活シーズンは入学や入社などで新生活を始める、あるいは人事異動や転勤など周囲の環境が変わるという人も多く、慣れない環境下で思わぬミスや勧誘にひっかかりやすい時期でもあると言えます。

また、フィッシング詐欺は単純に個人の被害と思われがちですが、ビジネスの世界でも被害が大きくなっており、先日も大手証券会社口座の乗っ取りを巡り、偽サイトを通じた「フィッシング」などの手口で、サイバー犯罪集団が乗っ取りを繰り返している疑いが強まっています。

参照元 フィッシング対策協議会：https://www.antiphishing.jp/

倒産11年ぶり1万件、「人手不足」理由過去最多　24年度

2024年度の全国企業倒産件数が11年ぶりに1万件を超えたというニュースは非常に衝撃的ですね。倒産件数は前年度比で12%増の1万144件となり、特に中小・零細企業の倒産が多かったようです。

倒産の主な原因としては、求人難や人件費の高騰による人手不足が挙げられます。これらの人手不足倒産は前年度比で約60%増加し、過去最多となりました。さらに、物価高による仕入れ価格の上昇も中小企業の経営を圧迫しています。

このような状況で、中小企業が生き残るためには、コスト管理の徹底や生産性向上が重要です。特に、DX（デジタルトランスフォーメーション）の導入が有効な解決策となります。

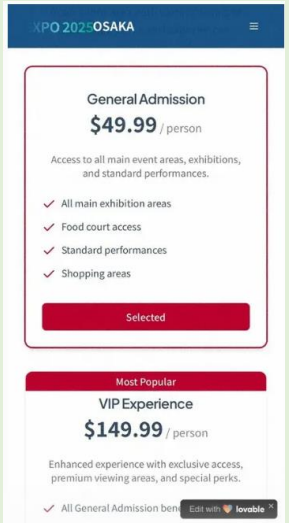
・業務プロセスの自動化　・データ分析の活用　・クラウドサービスの利用　・リモートワークの推進　などのDXを活用することで、業務の効率化や自動化が進み、人手不足やコスト増加の問題を緩和することができます。
これらのDX施策を通じて、中小企業は競争力を高め、厳しい経営環境を乗り越えることが期待されます。

参照元：https://www.tsr-net.co.jp/news/status/detail/1201244_1610.html

	倒産件数	負債総額
2024 (令和6)年度	1万144件	2兆3,738億 7,900万円
前年度比	＋ 12.05%	▲ 3.62%
2023 (令和5)年度	9,053件	2兆4,630億 7,800万円

都道府県	件数	負債総額:百万円
滋賀県	148	19,561
京都府	365	28,484
大阪府	1,355	214,771
兵庫県	571	53,545
奈良県	107	13,273
和歌山県	99	14,220
近畿	2,645	343,854

2025/4/13開幕！　大阪・関西万博　偽サイトが確認され注意を！



万博偽サイト確認 注意を！ チケット販売サイト装い個人情報詐取

13日に開幕した大阪・関西万博の入場チケットを販売するとうたった偽のインターネットサイトが相次いで確認されています。クレジットカード情報などを盗み取る「フィッシングサイト」の可能性があり、情報セキュリティー会社は「公式サイトや正規代理店以外での購入は避けて」と注意を呼びかけています。

https://www.expo2025.or.jp/news/news-20250403-05/

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おり、地政学的リスクの高まりからも引き続き注意が必要です。

【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）

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。

2025年 改正育児・介護休業法実務対応セミナー
～柔軟な働き方への対応～

- **開催日　：　5月27日（金）（申込締切日：5月22日（木）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**
  https://canon.jp/biz/event
  お申し込み時には招待会社コードが必要です。
  招待会社コード：

セミナー紹介動画！
https://youtu.be/EzIDM0yRFs8

【セミナー概要】
2025年4月及び10月の二段階で行われる改正育児・介護休業法ですが、
10月の改正は新たな制度設計が必要になり、4月に比べ、
より実務上の注意点や自社の状況を踏まえたうえでの検討が重要です。
しかし、人事部門はやるべきことが多岐にわたり、足元の業務で手一杯で、
情報収集にお困りの方も多いのではないでしょうか？
本セミナーでは、社会保険労務士による、10月改正に向けた実務上のポイントについてお話しします。

キヤノンMJ　セミナー　検索

是非この機会にご参加ください。

講師紹介：　アクタス社会保険労務士法人　代表社員
特定社会保険労務士　　松澤　隆志 氏

【松澤　隆志 氏　略歴】
社労士事務所での勤務経験、東証プライム上場企業の人事部長職を経て現職。
社会保険労務士として多くの中小企業の労務管理に携わり、個社ごとの事情に応じた
現実的なアドバイスに定評があります。

経済産業省：中小企業のためのセキュリティインシデント対応の手引き
https://www.meti.go.jp/policy/netsecurity/sme_incident.html
実際にインシデントが発生したときは、上記を参考にしてみてください。

長期休暇にはサイバー攻撃が増加傾向に

長期休暇の前後にはサイバー攻撃が急増する傾向があり、ゴールデンウィーク前後も注意が必要です。理由は、企業や団体のシステム管理者が休暇を取り、長期間不在になることが考えられます。攻撃者にとっては、守りが弱くなり、不正アクセスの検知や対応に時間がかかるため、狙いやすい状況となります。特に、データを暗号化して身代金を要求するランサムウェア攻撃は、セキュリティ担当者が少ない休日や休暇を狙うことが知られています。また、休暇明けも注意が必要です。多くの従業員が休み中に届いた大量のメールを処理する際、フィッシングメールを誤ってクリックしてしまうリスクがあります。休暇の前後がセキュリティ担当者にとって注意すべき時期と言えるでしょう。
この機会に自社のセキュリティ対策を見直してみてはいかがでしょうか？

出典元：IPA　独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/anshin/heads-up/alert20250421.html