身を守るには
知ることから！

情報セキュリティ被害の最新事例
2025年2月版

【大切なお願い】
会社を守るため、社長様、幹部様、従業員様、
パソコンやスマホを利用する**皆さまに回覧ください。**
自分事で実態を知ることが対策の第一歩です。

【この冊子の活用の仕方】
この冊子では、セキュリティの最新情報を月刊で
お伝えしています。被害事例を**自社に置き換えて、**
対策と意識向上にお役立てください。

BASIC Confertas Office

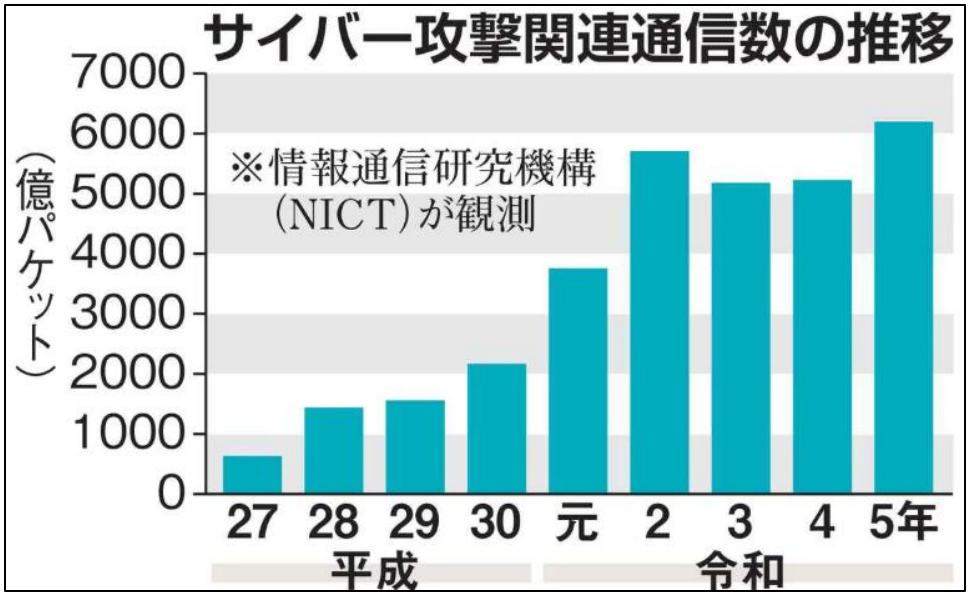
■日本へのサイバー攻撃関連通信数、8年で10倍に「14秒に1回」 各国で安全保障強化

2025年2月22日

・国立研究開発法人「情報通信研究機構」が観測した日本へのサイバー攻撃関連の通信数は、平成27年の年間約632億回から令和5年は同約6197億回とほぼ10倍に増加した。1つのIPアドレスにつき、約14秒に1回のサイバー攻撃を受けていることになる。

・警察庁の統計によると、令和6年の日本国内でのランサムウエアの被害件数は222件と高い水準で推移している。

・米英などの主要国は2010年代後半から、重要インフラ事業者による報告を義務化とともに、政府からの情報提供も義務付けているように、各国はサイバー安全保障の強化に力を入れている。



サイバー攻撃の脅威は増しており、それに伴いセキュリティも進化させていく必要があります。自社のセキュリティを常に見直し、更新していきましょう。

■画像：サイバー攻撃関連通信数の推移

■出典： https://www.sankei.com/article/20250222-2IC24RI7RFO5PII6D3IMKWDIP4/

■委託先がマルウェア感染、コード管理サービスから情報流出 - アイリッジ

2025年2月17日

・ノーコードでアプリを開発できる「APPBOX」を提供しているアイリッジは、同社で利用するソースコード管理サービス内の一部情報が流出したことを明らかにした。

・同社によれば、業務委託先で使用していた端末がマルウェアに感染しており、同社システムが侵害されたもの。ソースコード管理サービスに含まれる一部情報を第三者によって取得されたという。

・侵害されたシステムにおいて同社の顧客企業が提供するアプリの利用者に関する個人情報は管理しておらず、個人情報の流出については否定した。
今回の問題を受けて、同社は業務委託先を含めて情報管理のフローやセキュリティ体制について強化し、再発の防止を図るとしている。

他社で起きたサイバー攻撃が、自社に起こる可能性は高いです。どのような攻撃が行われたのか、情報を集めることも重要です。

■画像：アイリッジのHP(https://iridge.jp/)

■出典：https://www.security-next.com/167280

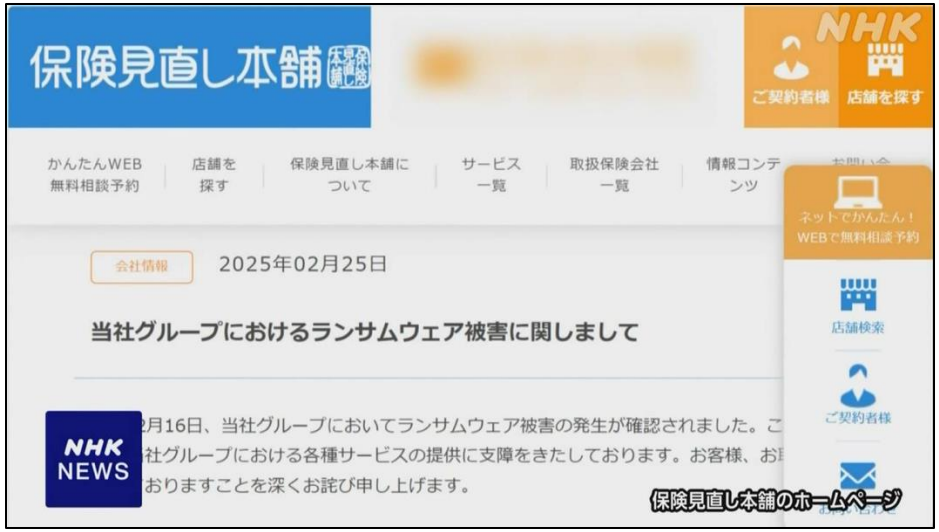
■保険見直し本舗 サイバー攻撃でシステム障害 臨時休業し点検

2025年2月25日

・大手保険代理店の「保険見直し本舗」を運営する会社は、身代金要求型のコンピューターウイルスによるサイバー攻撃を受け、社内のシステムに障害が起きたと発表した。顧客の情報が漏えいしていないか調べるとともに全国の250店舗余りを臨時休業し、点検を進めている。

・「保険見直し本舗」の運営会社によりますと、2月16日に社内のシステムに障害が発生し、調査したところ身代金要求型の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を受けたことが確認された。

・会社は、顧客情報の漏えいは今の時点では確認されていないものの、漏えいの可能性はあるとして詳しく調査しており、運営する保険代理店など全国の258店舗を25日から2月28日まで臨時休業している。



保険見直し本舗のホームページ

不正アクセスを受けた際は、少しでも被害の拡大を防ぐための早急な対応が必要です。普段から不正アクセスを受けてからの手順を考えておくと良いかもしれません。

■画像：保険見直し本舗のホームページ

■出典：
https://www3.nhk.or.jp/news/html/20250225/k10014733041000.html

BASIC Confertas Office

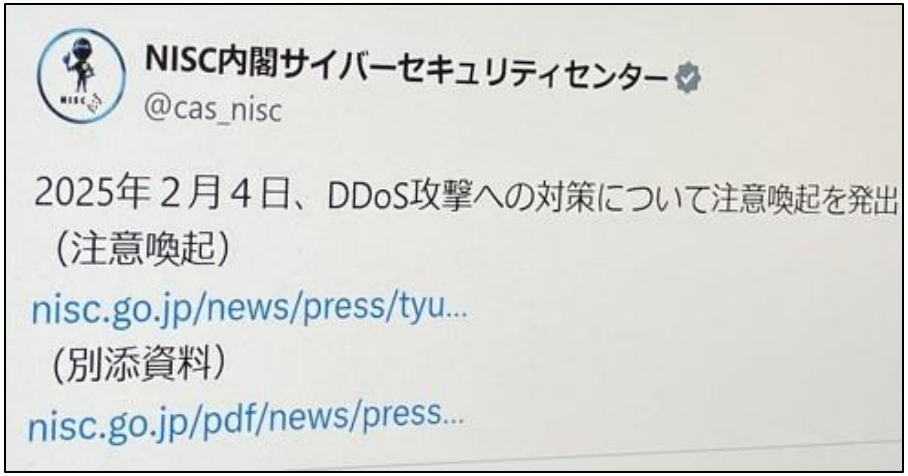
■日本企業を狙う、相次ぐDDoS攻撃に国が注意喚起

2025年2月4日

・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～25年1月にかけてDDoS攻撃が相次いでいることを受け、各事業者に注意を呼びかけた。

・NISCは、DDoS被害を抑えるための対策の1つとして、海外に割り当てられたIPアドレスからの通信の遮断を挙げる。マルウェアに感染している端末が多い国やドメインからの通信を拒否することで、攻撃の影響を緩和できるとしている。

・また、DDoS攻撃の影響を排除・低減するための対策装置やサービスとして、Webアプリに特化したファイアウォール「WAF」や、不正アクセスを検知・防止するシステム「IPS」／「IDS」などを導入することも有効という。



サイバー攻撃を防ぐ方法には様々なものがあります。様々な対策装置やサービスの特性を知り、いくつか組み合わせて対策を講じることは、セキュリティを高める有効な方法です。

■画像：日本企業を狙う、相次ぐDDoS攻撃に国が注意喚起

■出典:https://www.itmedia.co.jp/news/articles/2502/04/news120.html

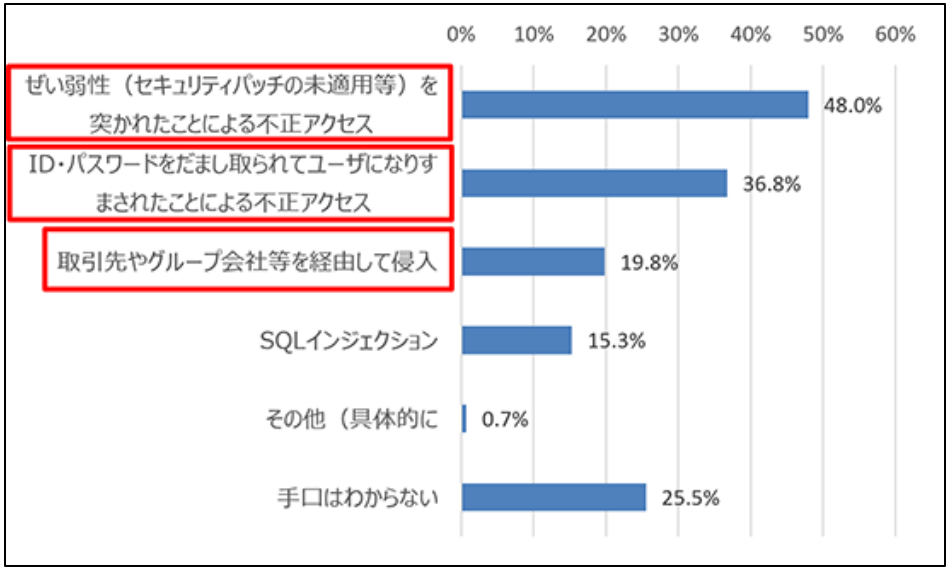
■「2024年度中小企業等実態調査結果」速報版を公開

2025年2月14日

・独立行政法人情報処理推進機構（IPA）は2月14日、「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」の速報版を発表した。

・サイバー攻撃の手口では、「脆弱性を突かれた」との回答が48.0%、次いで、「ID・パスワードをだまし取られた」との回答が36.8%であった。「取引先やグループ会社等を経由して侵入」との回答も19.8%あり、サプライチェーン上のセキュリティリスクが読み取れる。

・また、不正アクセスによる被害内容については、「自社Webサイトのサービス停止、または機能が低下させられた」、「業務サーバのサービス停止、または機能が低下させられた」「自社Webサイトの改ざん」の順に多く、特定のシステムに限らず被害を受けている状況が分かった。



■画像：不正アクセスの手口（n=419）
■出典：
https://www.ipa.go.jp/pressrelease/2024/press20250214.html#topics_02

サイバー攻撃の手口、受ける被害は様々です。様々な手口で行われる不正アクセスを防げるよう、セキュリティを常に更新しましょう。

■フィッシング詐欺メールの報告件数 去年170万件余 過去最多に

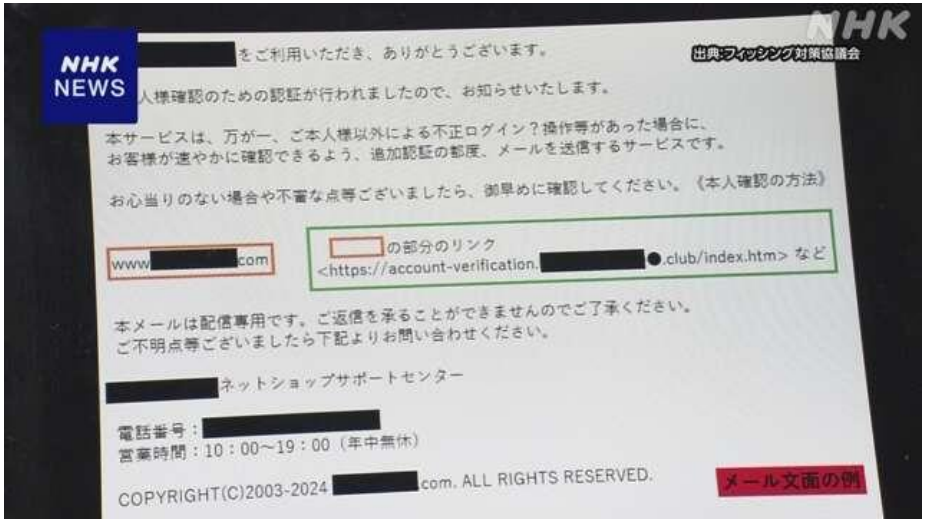
2025年2月3日

・「フィッシング詐欺」のメールの報告件数が、去年は170万件余りに上り、過去最多となった。民間の事業者で作るフィッシング対策協議会によりますと、去年に報告されたフィッシング詐欺のメールの件数はおよそ171万8000件で、前の年より52万件余り増え、過去最多となった。

・メールの内訳は、クレジットカード会社をかたるものが36%、通販サイトが24%、電力やガス、水道事業者が8%、金融機関が6%などとなっている。報告件数は5年前と比べて30倍以上に増加していて、犯罪グループが、自動化したシステムなどを使って、大規模にメールを送信しているとみられている。

・協議会は、公式アプリやブックマークした正規サイトからアクセスするなど、確認を徹底するように注意を呼びかけています。

フィッシングサイトは大抵、本物のサイトをコピーして作られているので人の目で判断するのは危険です。アクセスブロックを強化すると共に、日頃からブックマークや公式アプリを利用するように心がけましょう。



■画像：フィッシング対策協議会

■出典：
https://www3.nhk.or.jp/news/html/20250203/k10014710551000.html

情報セキュリティ対策は、実績豊富で信頼できる企業をお選びください。

最近は、ランサムウェアや情報漏えいなど、経営に関わるサイバー攻撃の被害も増加し、ひとつの社会問題となっています。私たちは、「サイバー攻撃の脅威からお客様を守りたい」そして、「今後もお客様と一緒に永く成長していきたい」と強く思っています。

情報セキュリティは、社内ネットワークに関わる重要な部分であり、信頼できる会社と付き合うことが大切です。私たちは、お客様に正確な情報と知識、安心の技術サポートを提供できる体制を整えていますので、ぜひご安心ください。