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1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

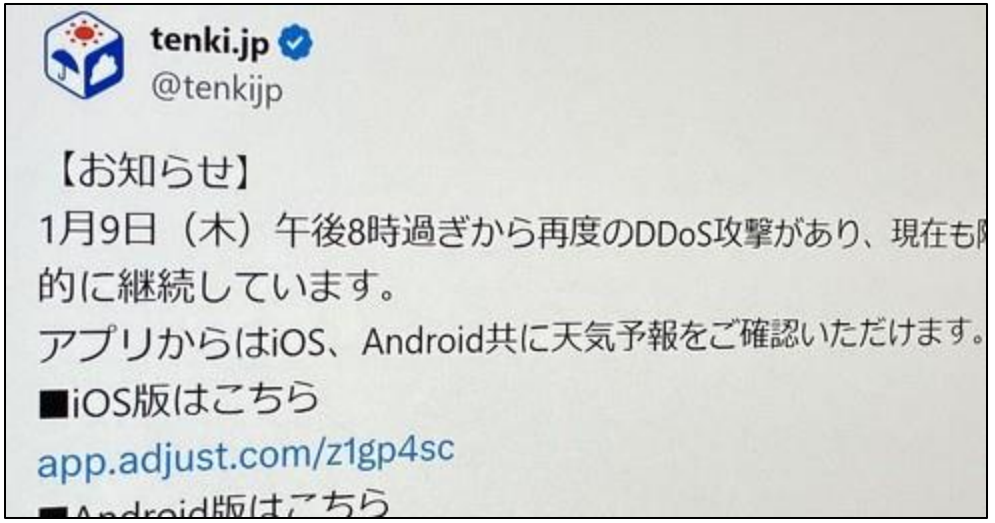
■「tenki.jp」にまたDDoS攻撃、Web版で障害 日本気象協会はアプリや公式Xの利用を呼びかけ

2025年1月10日

・日本気象協会は1月10日、天気予報メディア「tenki.jp」Web版にアクセスしづらくなっていると発表した。

・9日午後8時過ぎからDDoS攻撃を受けており、10日午前11時30分時点で、障害復旧のめどは立っていない。tenki.jpのアプリ版や公式Xには影響は出ておらず、そちらの利用を呼びかけている。

・tenki.jpを巡っては、5日にDDos攻撃を受け、Web版・アプリ版に一時つながりにくい状況が発生していた。その後、9日午前7時ごろから再度DDos攻撃を受け、tenki.jpのWeb版で同様の障害が発生。同日午後4時30分ごろに復旧したとしていた。



サイバー攻撃は、被害にあった企業だけでなく、それに関わる多くの人に影響を与えます。
被害を未然に防げるよう、常にセキュリティ対策を万全な状態にしておきましょう。

■画像：「tenki.jp」にまたDDoS攻撃、Web版で障害

■出典：
https://www.itmedia.co.jp/news/articles/2501/10/news137.html

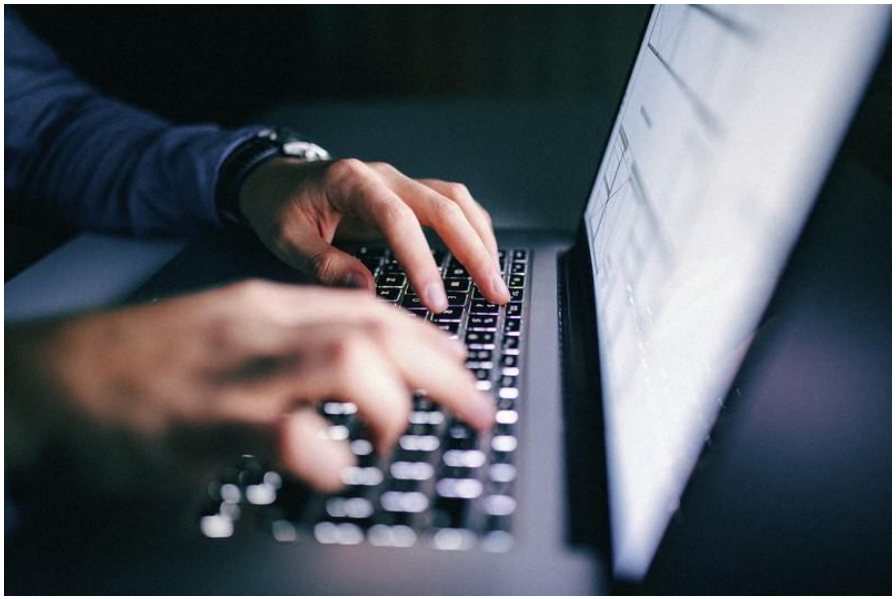
■同一の不正プログラム使い攻撃か　日航など国内46事業者に

2025年1月10日

・日航や三菱UFJ銀行などが、大量のデータを送り付けてサーバーに負荷をかける「DDoS攻撃」を相次いで受けたとされる問題で、同一の不正プログラムが使われたとみられることが9日、セキュリティー会社「トレンドマイクロ」への取材で分かった。

・昨年12月末の日航の被害以降、このプログラムによる攻撃を受けたのは省庁を含む国内の46事業者に上ることも確認された。

・同社が日航の被害を受け調査したところ、特定のボットネットで各事業者のIPアドレスに攻撃の指令が出されていたのを確認した。米国や欧州などでも攻撃の形跡があった。インターネットに接続されたカメラや家電などを、大量に遠隔操作して攻撃していた。



■画像：イメージ

■出典:https://news.livedoor.com/article/detail/27915355/

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。

■ カシオ、個人情報含む内部資料の一部流出を確認 ランサムウェア攻撃の調査で

2025年1月7日

・カシオ計算機は1月7日、昨年10月に公表したランサムウェア攻撃についての調査結果を発表した。8479人分の個人情報を含む内部資料の一部流出を確認した。

・流出が確認された個人情報は、カシオの従業員情報6456人分、取引先の代表者や窓口担当者、カシオの採用面接を受けた人など1931人分、そして配送設置を伴う製品を購入したユーザー情報が91人分。クレジットカード情報などは含まれていない。

・再発防止策として、1）海外拠点を含むグループ全体のITセキュリティの強化を継続的に実施、2）情報管理体制の見直しを行い、ルール徹底のために社内教育を強化することを挙げた。

サイバー攻撃によって、流出する情報の範囲は計り知れません。個人情報を守れるよう、常にセキュリティの状態を確認しましょう。

■画像：カシオ計算機のWebサイト
■出典：https://www.itmedia.co.jp/news/articles/2501/07/news179.html

■サンリオに不正アクセス　ピューロランドのチケット購入などが不可能に　情報漏えいについては調査中

2025年1月22日

・サンリオエンターテイメントは1月22日、会社のネットワークに第三者からの不正アクセスがあったと発表した。不正アクセスを確認したのは21日で、これが原因でネットワークトラブルが発生。サンリオピューロランドの公式Webサイトの一部機能などが利用できない状態になっている。

・22日時点では、サンリオピューロランド公式Webサイト内のマイページ機能や来場予約の取得、公式eパスポートチケットの購入などができない状態だ。他にも、サンリオエンターテイメントのコーポレートサイトもアクセス不能になっている。

・現時点で個人情報の漏えいなどがあったかは不明。同社は現在調査を進めているという

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：サンリオエンターテイメントに不正アクセス

■出典：
https://www.itmedia.co.jp/news/articles/2501/22/news184.html

BASIC Confertas Office

■9割が「セキュリティは十分対策している」と回答も、6割がインシデントを経験、～ドリーム・アーツが大企業の経営層・情シスを対象に調査

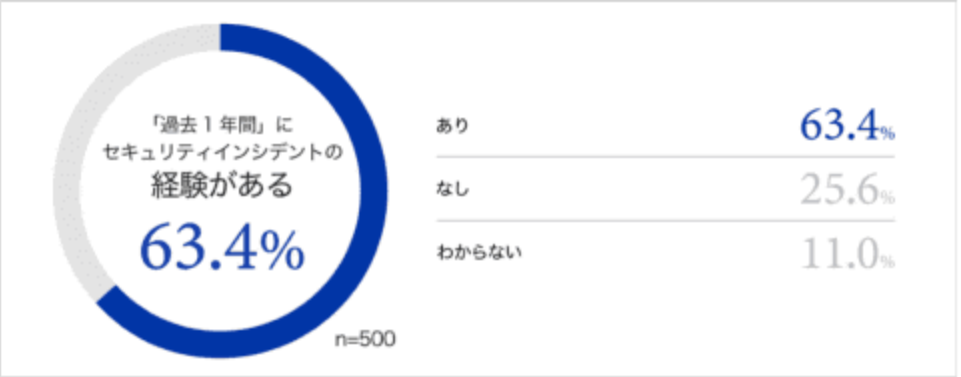
2025年1月10日

・株式会社ドリーム・アーツは1月9日、従業員数1000人以上の大企業を対象とした「情報セキュリティ」に関する調査を行い、その結果を発表した。

・調査から、91.0%の回答者が「十分なセキュリティ対策ができている」と回答しており、63.4%の回答者が過去1年間でセキュリティインシデントの経験があることが分かった。

・同社はこれらの結果を踏まえ、特に経営層の7割が自社のセキュリティ対策が万全だと考えている点について指摘。情報漏洩やインシデントが実際に発生していない限り、そのリスクを過小評価してしまう傾向があると、調査レポートにおいて分析している。

サイバー攻撃は常に進化しており、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：過去1年間のセキュリティインシデント経験の有無

役職	十分対策している	おおむね十分だが改善の余地はある	対策はしているが十分ではない	全く対策できていない	必要性を感じていない
非管理職（社会人1～3年未満）	35.3%	41.2%	23.5%	0.0%	0.0%
非管理職（3年以上）	54.9%	35.6%	8.2%	0.0%	1.3%
中間管理職（係長、課長、次長クラス）	42.5%	48.1%	8.5%	0.0%	0.9%
管理職（部長クラス）	53.2%	41.5%	5.3%	0.0%	0.0%
経営層（取締役以上）	68.0%	24.0%	8.0%	0.0%	0.0%

■画像：「重要な情報」に対する情報セキュリティ対策状況（役職別）

■出典：
https://internet.watch.impress.co.jp/docs/news/1653524.html

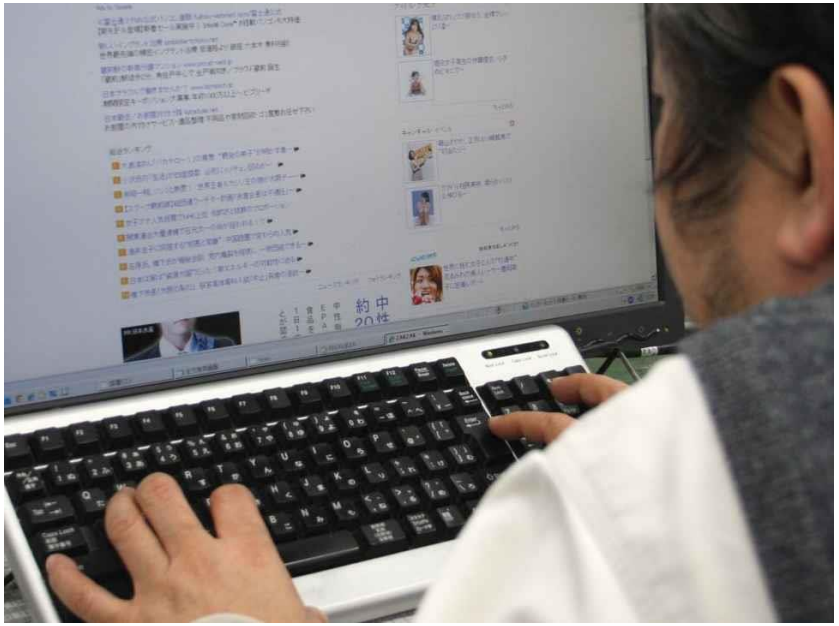
■昨年の「フィッシング」が過去最多　148万件超　民間監視団体まとめ

2025年1月11日

・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、過去最多となることが11日、民間監視団体のフィッシング対策協議会のまとめで分かった。1月から11月までの累計件数は148万5746件だった。

・協議会は犯罪者が自動送信システムを使っている可能性を指摘。セキュリティー企業は文面作成に生成人工知能（AI）を悪用している恐れがあるとみている。

・協議会の担当者は同じ文面のメールが同時間に何万通も送信される例があるとし「人手でこれほど大量に送ることは難しい」と分析した。



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：パソコンを操作する男性

■出典： https://www.sankei.com/article/20250111-62JDLODSOVKJTJ766MOSR2QYSY/photo/HXCYKJ6VIVDMNJZZAWJUBJXJNU/

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。