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
2024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。

■イズミにランサムウェア攻撃、仕入れ・新規開店に影響

2024年2月21日

・株式会社イズミは2月16日、同社グループへのランサムウェア攻撃について発表した。これは2月15日に同社グループの複数サーバがランサムウェアによって暗号化されたことを確認したというもの。個人情報の漏洩は確認されていない。

・同社ではアプリ・クレジットカード・通販サイト「ゆめオンライン」や配送サービスなどの利用を停止しているほか、店舗の仕入れも滞り、品薄の商品があるという。また、3月7日に予定されていた新規開店を未定とした。

・16日に政府の個人情報保護委員会に報告しており、5月1日の完全復旧を目指し、外部専門家や警察と連携の上、原因追求とシステム保護に取り組むという。

ランサムウェアの被害に遭ってしまうと、業務遂行に支障や遅れが発生してしまいます。対策が必要と感じる場合は専門家に相談してみましょう。

■画像：イズミ本社

■出典：
https://www.nikkei.com/article/DGXZQOCC215VA0R20C24A2000000/

■情報セキュリティ10大脅威2024発表、組織向け1位は「ランサムウェアによる被害」

2024年2月15日

・独立行政法人 情報処理推進機構（IPA）は、「情報セキュリティ10大脅威2024」を公開した。2023年に発生した情報セキュリティの事故・事件に対して、選考会での投票から、「個人」「組織」の立場でそれぞれ上位10件を選出している。

・「組織」向け脅威の1位は「ランサムウェアによる被害」、2位は「サプライチェーンの弱点を悪用した攻撃」であり、前年と同順位だった。3位の「内部不正による情報漏えいなどの被害」、6位の「不注意による情報漏えいなどの被害」は前年から順位を上げており、要注意だとしている。

・内容は同じであっても被害者を騙す手口は更新され、最新の社会情勢に便乗するものが多い。今後は生成AIのような新技術が攻撃に採り入れられると考えられ、最新の動向に留意が必要だ。

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	ランサムウェアによる被害	2016年	9年連続9回目	1
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目	2
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目	4
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目	3
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目	6
6	不注意による情報漏えい等の被害	2016年	6年連続7回目	9
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目	8
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目	7
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目	5
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目	10

情報セキュリティの脅威は様々なものがあります。内容ごとにどのような対策がとる必要があるか、今一度確認してみましょう。

■画像：IPA 情報処理推進機構

■出典：
https://www.ipa.go.jp/pressrelease/2023/press20240124.html

■セキュリティを無効化するマルウェアが333%増加 防御回避は“常識”になっている

2024年2月15日

・Picus Securityは2024年2月13日（現地時間）、年次セキュリティレポート「Picus Red Report 2024」を公開した。

・レポートの中で、セキュリティ機能を標的にしたマルウェアが333%増加し、「Hunter-killer」と呼ばれるセキュリティを無効化するマルウェアが顕著に増加していることを報告した。1年前、「マルウェアがセキュリティの無効化を試みること」は比較的稀なことだったが、現在はマルウェアサンプルの4分の1にみられ、事実上全てのランサムウェアグループによって使用されているという。

・同社は、サイバー攻撃によってセキュリティツールが無効化または再構成されたかどうかを検出するのは非常に難しく、多層防御のアプローチで、複数のセキュリティ制御を使用する必要があると指摘している。

技術の進化に伴い、サイバー攻撃の手口は更新されています。セキュリティ対策もそれに応じて対応していくことが重要です。いま一度対策を見直してみましょう。

■画像：Picus SecurityのWebサイト

■出典：https://www.picussecurity.com/

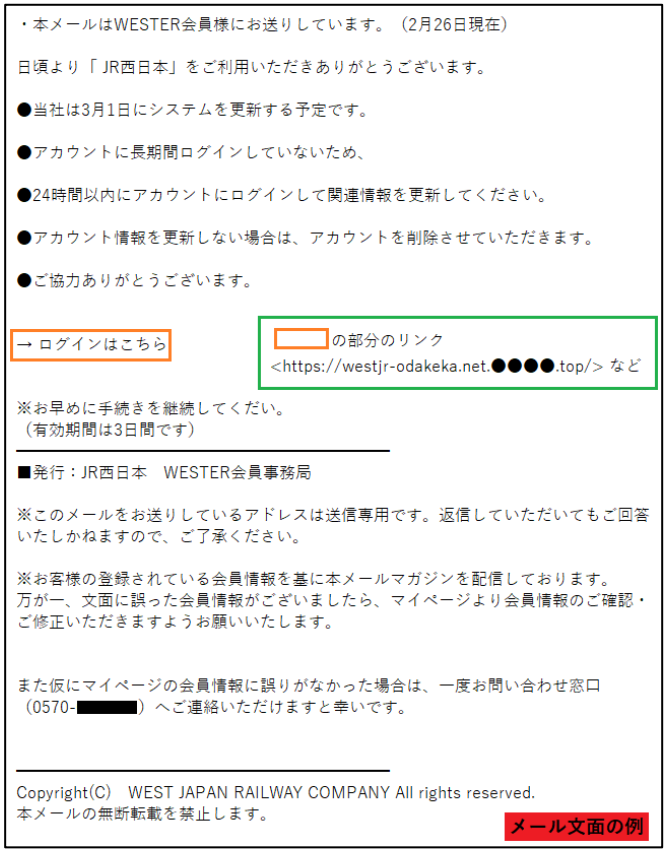
■JR西日本をかたるフィッシング確認、注意を

2024年2月27日

・フィッシング対策協議会は2月27日JR西日本を偽るフィッシングの報告を受けているとして、注意を呼び掛けた。

・「長期間ログインしていないため24時間以内にログインして情報を更新する必要がある」といった旨のメールが送られてくる。リンク先に情報を入力することにより、アカウント情報の窃取、個人情報の窃取、クレジットカード情報の窃取などが行われる。

・フィッシング詐欺に使われているWebサイトは一見しただけで判別することが難しい。そのため、メールやメッセージに含まれているリンクではなく、公式アプリやWebブラウザーに登録したブックマークなどからアクセスすることや、迷惑メールフィルターが有効になっているか確認することが望まれる。



・本メールはWESTER会員様にお送りしています。（2月26日現在）

日頃より「JR西日本」をご利用いただきありがとうございます。

●当社は3月1日にシステムを更新する予定です。

●アカウントに長期間ログインしていないため、

●24時間以内にアカウントにログインして関連情報を更新してください。

●アカウント情報を更新しない場合は、アカウントを削除させていただきます。

●ご協力ありがとうございます。

→ ログインはこちら

[　　]の部分のリンク
<https://westjr-odakeka.net.●●●●.top/> など

※お早めに手続きを継続してください。
（有効期間は3日間です）

■発行：JR西日本　WESTER会員事務局

※このメールをお送りしているアドレスは送信専用です。返信していただいてもご回答いたしかねますので、ご了承ください。

※お客様の登録されている会員情報を基に本メールマガジンを配信しております。
万が一、文面に誤った会員情報がございましたら、マイページより会員情報のご確認・ご修正いただきますようお願いいたします。

また仮にマイページの会員情報に誤りがなかった場合は、一度お問い合わせ窓口
（0570-[redacted]）へご連絡いただけますと幸いです。

Copyright(C)　WEST JAPAN RAILWAY COMPANY All rights reserved.
本メールの無断転載を禁止します。

メール文面の例

■画像：メール・SMSの文面例

■出典：https://www.antiphishing.jp/news/alert/westjr_20240227.html

フィッシングは気を付けていても、「ついうっかり」で被害に遭う危険性が高いです。日頃から、正規のアプリや正規のWebサイトにアクセスする習慣をつけて、被害を防止しましょう。

BASIC Confertas Office

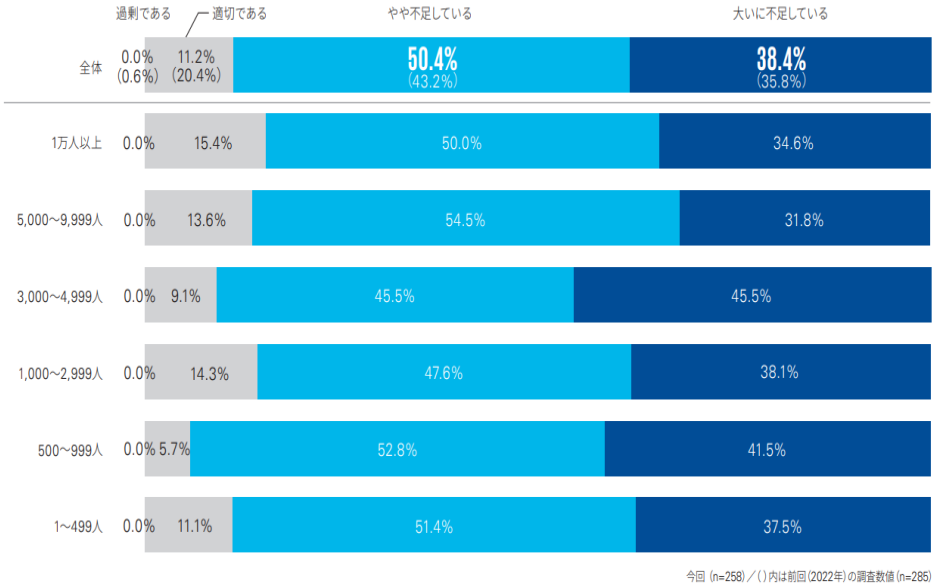
■KPMGが2023年の調査レポートを公開 約9割が「セキュリティ人材不足」

2024年2月28日

・KPMGコンサルティングは、国内企業のサイバーセキュリティの調査結果をまとめた「サイバーセキュリティサーベイ2023」を発表した。調査は、国内の上場企業・売上高400億円以上の未上場企業を対象に、サイバー攻撃の実態やセキュリティ管理態勢など複数の側面から企業のセキュリティ対策を評価している。

・調査の中で、88.8%が「サイバーセキュリティ人材が不足している」と答えた。従業員規模に関わらず、人材不足の割合は前回調査から増加しており、人材不足の深刻化が浮き彫りになった。

・自社の人材育成だけでなく、外部の専門家やサービスを利用する、自動化ツールを導入する等、予算も考慮した上で、様々な対策を組み合わせ、人材不足に対処する必要がある。



■画像：サイバーセキュリティ人材の状況

■出典：https://assets.kpmg.com/content/dam/kpmg/jp/pdf/2024/jp-cyber-security-survey2023.pdf

サイバー攻撃が高度化され、セキュリティの重要性が増すにつれ人手不足は深刻化しています。様々な対策を組み合わせ、効率的なセキュリティ管理体制を構築しましょう。

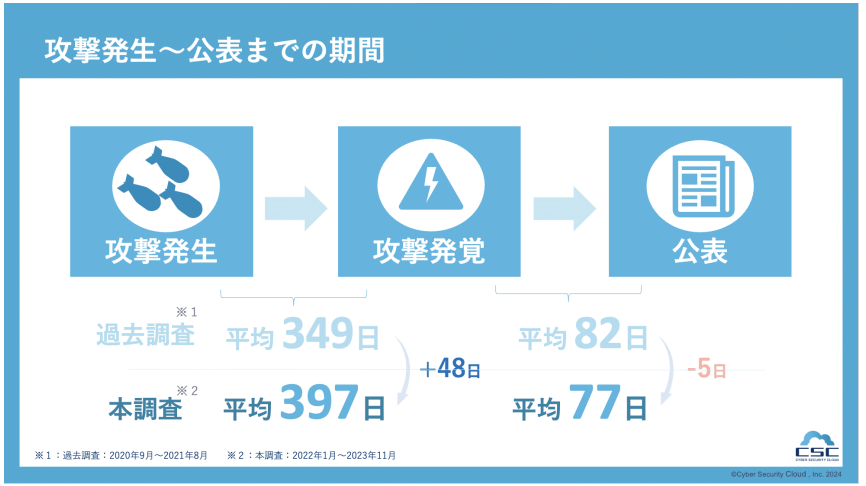
■サイバー攻撃に関する日数の調査レポート公開
攻撃発生～発覚まで、かかる期間は平均で1年以上！

2024年2月21日

・サイバーセキュリティクラウド（CSC）は、「サイバー攻撃の発生から発覚・公表までの日数に関する調査レポート」を発表した。2022年1月1日から2023年11月30日までに公表された、不正アクセスに関する個人情報流出事案をもとに調べている。

・法人や団体がサイバー攻撃を受けた「攻撃発生」から、攻撃に気づいた「攻撃発覚」までにかかる日数は、平均で397日となった。これは、過去調査（2020年9月～2021年8月）から48日長期化している。長期化の要因として、攻撃が未知の脆弱性（Zero-Day）を利用しているため、脆弱性が検出されにくいことが挙げられている。

・「攻撃発覚」の長期化は、攻撃者が長期間にわたってシステム内に潜伏し、企業の貴重なデータにアクセスし続けることを意味しており、企業はサイバーセキュリティの体制を強化していく必要がある。



■画像：「攻撃発生」～「攻撃発覚」～「公表」までの平均日数

■出典：https://www.cscloud.co.jp/news/press/202402216761/

サイバー攻撃を発見し、対応するには多くの時間を必要とします。サイバー攻撃被害を未然に防げるよう、セキュリティ体制を強化しましょう。

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。