BASIC
Confertas Office

身を守るには
知ることから！

社内回覧用

情報セキュリティ被害の最新事例
2024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。

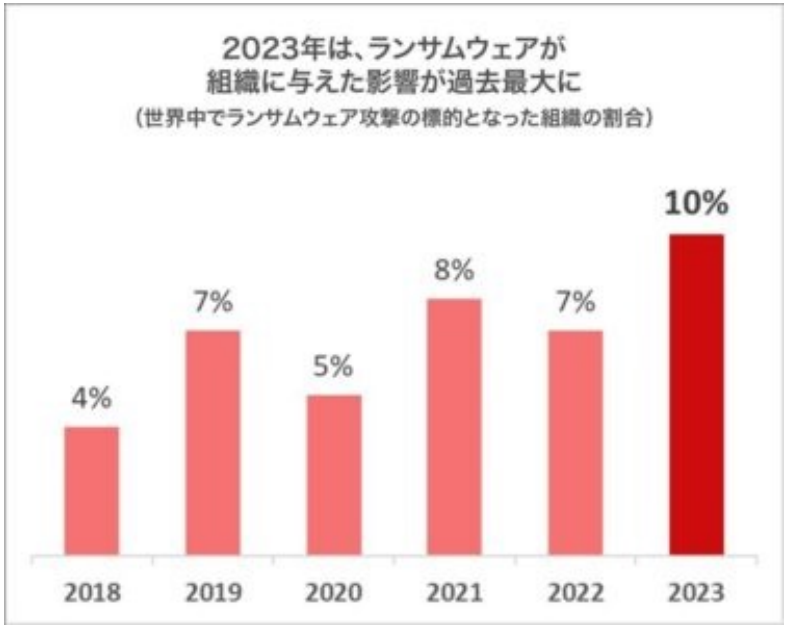
■ランサムウェア攻撃が前年比33%増、チェック・ポイントが2023年の脅威データを公開

2024年1月29日

・チェック・ポイント・ソフトウェア・テクノロジーズの脅威インテリジェンス部門であるチェック・ポイント・リサーチは2024年1月29日、2023年のサイバー脅威データを公開した。

・2023年を、大規模なランサムウェア攻撃によって世界中の組織が前例のない影響を受けた年と位置付けており、従来型のランサムウェアおよび、より大規模なランサムウェア攻撃 “メガランサムウェア”の両方が急激な増加を見せたという。

・攻撃手法も変化し、データ窃取に焦点を当て、暗号化ではなく盗んだデータを使った恐喝が増加。この進化は、組織のゼロデイ攻撃に対する防御の必要性を強調し、特に中小企業などサイバーセキュリティのリソースが限られている組織においてセキュリティ対策の強化が求められているとしている。



2023年に続き、2024年もランサムウェア攻撃の脅威が高まることが予想されます。セキュリティ対策の強化の重要性も高まるでしょう。

■画像：ランサムウェア攻撃の標的になった組織の割合

■出典：https://businessnetwork.jp/article/18567/

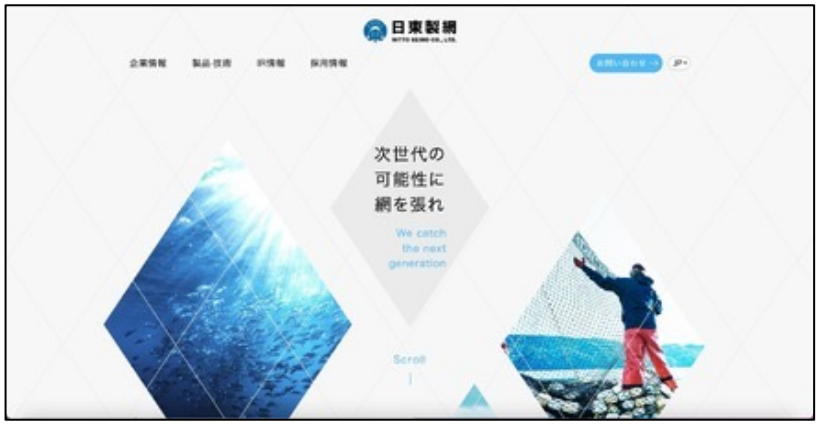
■日東製網にランサムウェア攻撃、情報流出の有無については調査中

2024年1月31日

・日東製網株式会社は1月19日、同社サーバのランサムウェア感染被害について発表した。これは1月16日午前8時頃に、外部から不正アクセスがあり、サーバに保存している各種業務データや業務用ソフトウェアが暗号化され、アクセス不能な状況となったこと等を同日に確認したというもの。

・同社では1月17日に全社対策本部を設置し、外部専門家の助言を受けながら、原因特定や被害情報の確認、情報流出の有無などの調査を行い、復旧への対応を進めている。

・同社では引き続き、外部専門家及びシステム関係機関等と連携のうえで早期復旧に向け作業を進めるとともに、通常の業務遂行が可能となるよう対応を進めるとのこと。



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：日東製網　ホームページ

■出典：https://s.netsecurity.ne.jp/article/2024/01/29/50517.html

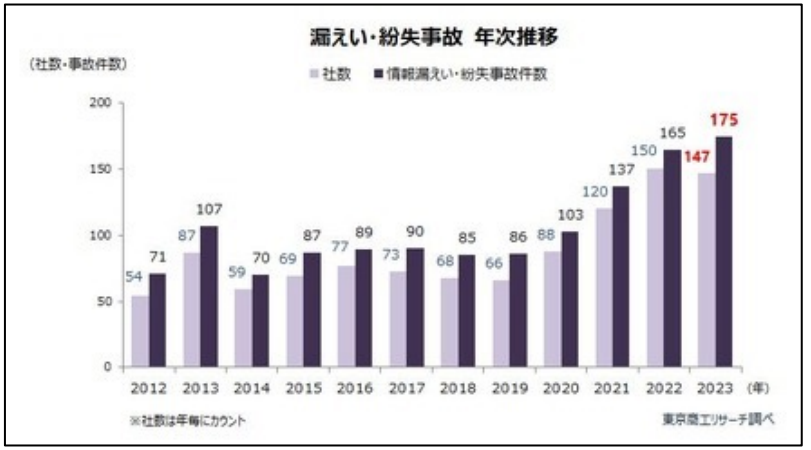
■2023年の「個人情報漏えい・紛失事故」が歴代最多。件数175件、流出・紛失情報も最多の4,090万人分

2024年1月19日

・2023年に上場企業とその子会社が公表した個人情報の漏えい・紛失事故は、175件だった。漏えいした個人情報は前年（592万7,057人分）の約7倍の4,090万8,718人分と大幅に増えた。

・事故件数は2012年から2023年までで累計1,265件に達した。漏えい・紛失した可能性のある個人情報は累計1億6,662万人分に達し、日本人の人口を優に超えている。

・社内で抱える個人情報を守るためには、巧妙化するサイバー犯罪に対するセキュリティ強化が不可欠である。同時に、不正防止を目的としたガバナンスの徹底も求められ、個人情報の取り扱いルールの厳格化を通じた従業員の意識付けも重要になっている。



デジタル化が進む中で、個人情報の漏えいも年々増加しています。今一度、不正アクセスの対策と個人情報取り扱いルールの見直しをしてみましょう。

■画像：漏えい・紛失事故　年次推移

■出典：https://www.tsr-net.co.jp/data/detail/1198311_1527.html

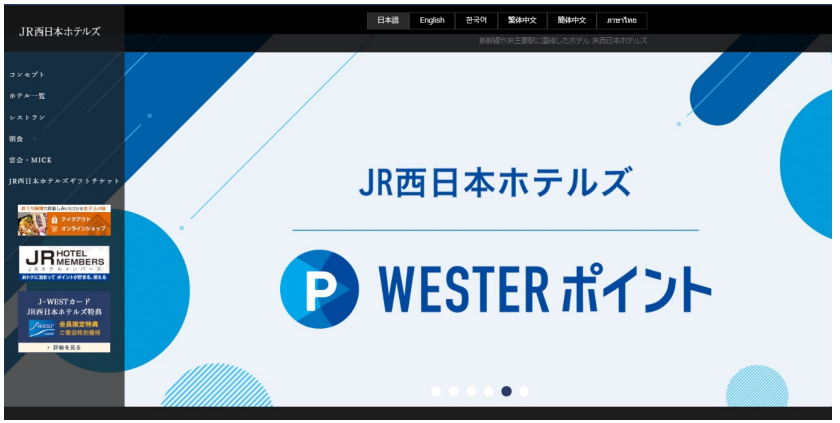
■メールアドレスが不正アクセスによる乗っ取り被害、フィッシングの踏み台に - JR西日本ホテルズ

2024年1月15日

・JR西日本ホテルズは、同社が運営する梅小路ポテル京都において、メールアカウントが不正アクセスを受け、フィッシングメールが送信されたことを明らかにした。同ホテルによれば、2023年12月17日から翌18日にかけてメール送信サーバが不正アクセスを受けたもの。

・同ホテルが運用するメールアカウント1件より不特定多数のメールアドレスに対し、フィッシングメールが送信された。同社ではアカウントのパスワードを変更。フィッシングメールの送信は停止している。2023年12月3日から同月18日にかけて受信したメールを第三者に閲覧された可能性もあるとして調査を行ったが、メール受信サーバに対するアクセスの痕跡なく、受信メールの流出については否定している。

・同社は、同ホテルを発信元とする不審なメールを受信していた場合は、返信したり、URLを開かないよう注意を呼びかけている。



■画像：JR西日本ホテルズ　ホームページ

■出典：https://www.security-next.com/152498

不正アクセスによって会社のサーバーが迷惑メールの送信に悪用されてしまうという事例が多くあります。不正アクセスを受けないためのセキュリティ対策が大切です。

■メルカリがフィッシング詐欺に注意喚起、アプリの利用など推奨

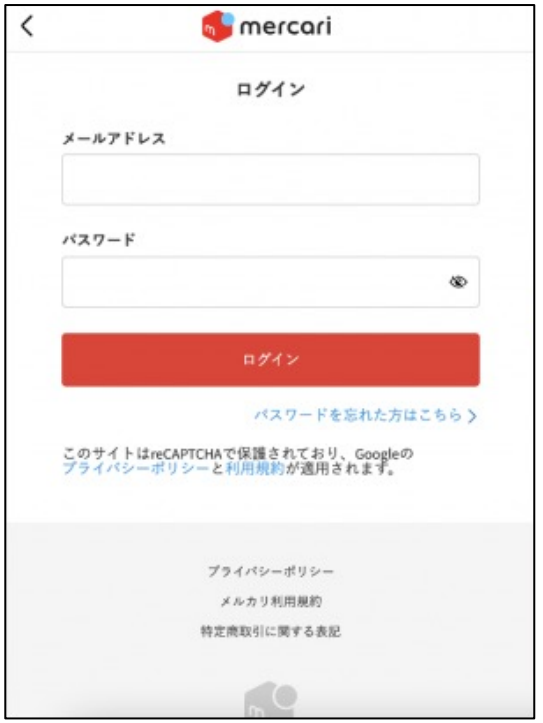
2024年1月30日

・株式会社メルカリは1月25日、同社と郵便局が連携した配送サービス「メルカリびより」サイトにおいて、「メルカリ・メルペイを装ったWebサイトによるフィッシング詐欺について」とする注意喚起を発表した。

・注意喚起によると、現在メルカリグループのサービスを装ったフィッシングサイトが確認されており、フィッシングサイトでアカウント情報やパスワード、二段階認証番号、カード情報などの個人情報を入力してしまうと、メルカリやメルペイのサービスを不正利用されたり、同じパスワードを使っている他社のWebサイトへログインされる可能性があるとしている。

・メルカリのフィッシングサイトは、本物をコピーして作られているため、画面を見ただけで偽物と見破ることは困難。いつもと違う経路でメルカリのログイン画面が表示されたら決してログイン情報を入力せず、まずは疑い、ブックマークや公式アプリなどのいつもと同じ方法でメルカリにアクセスするよう呼びかけている。

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。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：メルカリを装うフィッシングサイト画面の一部

■出典：https://scan.netsecurity.ne.jp/article/2024/01/30/50523.html

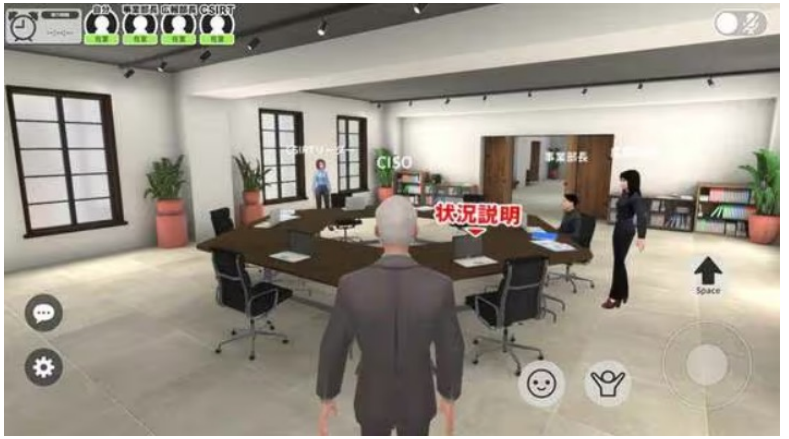
■「サイバー攻撃」メタバースで"訓練"受ける効用 大日本印刷、実践的なシナリオで研修を展開

2024年1月5日

・サイバー攻撃の被害に遭う企業が増える中、大日本印刷はメタバース上でサイバー攻撃を想定した訓練を行うことのできる研修プログラムの提供を2023年11月から開始した。

・企業の経営層を対象として、サイバー攻撃を受けた際に関係者が連携して対応しなければならない状況をメタバース上に再現したもので、4人1組で危機対応について学ぶ。シナリオについては、サイバーセキュリティの第一人者であるサイバーディフェンス研究所専務理事の名和利男氏の知見をもとに、過去の事案とその対応を反映させた実践的なシナリオを採用している。

・演習後にはフィードバックもあり、自社の課題や改善点を洗い出すのはもちろんだが、関係者でサイバー攻撃に対する共通認識を持つことが重要だという。



セキュリティ対策には従業員の教育が欠かせません。サイバー攻撃を受けてしまった時の対応について、考えてみるのもいいかもしれませんね。

■画像：メタバース上で危機対応について学ぶ研修

■出典：https://toyokeizai.net/articles/-/722745

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。