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12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。

サイバー攻撃最新事例

■ ＪＡＬにサイバー攻撃、一部の国内線に３０分以上の遅れ …ＤＤｏＳ攻撃か

2024年12月26日

・２６日午前７時２４分頃、日本航空が外部からサイバー攻撃を受け、社外システムとの通信に不具合が発生した。

・攻撃で障害の起きたルーターを特定し、１時間半後に一時的に遮断したが、国内各空港での搭乗に伴う荷物の預かりなどに支障が生じた。

・捜査関係者によると、同社は２６日朝、大量のデータを送りつけて通信機能をまひさせる「ＤＤｏＳ（ディードス）攻撃」を受けたと警視庁に相談した。

・影響範囲は特定できており、システムの復旧状況を確認しているという。安全運航に影響はないとしている。

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：サイバー攻撃を受けてネットワーク機器に不具合があることを伝えるJALのホームページ

■出典： https://www.yomiuri.co.jp/national/20241226-OYT1T50041/

■三井住友海上、顧客情報１２万件流出か　ランサムウエア被害

2024年12月25日

・三井住友海上火災保険は２５日、業務委託先の東京損保鑑定（東京）のサーバーがランサムウエア被害で、流出した可能性のある顧客情報が約１２万件に上ると発表した。

・同じく業務を委託する東京海上日動火災保険や損害保険ジャパンも顧客情報が漏えいした疑いがあり、各社は実態把握を急いでいる。

・三井住友海上で流出した可能性があるのは保険契約者の名前や住所、証券番号といった顧客情報。同社は「深くおわびしたい」と陳謝した。ただ、顧客情報の不正使用は現時点で確認されていないとしている。

サイバー攻撃を防御し、迅速に復旧するためには事前の準備が非常に重要です。自社のセキュリティ対策を改善していきましょう。

■画像：三井住友海上火災保険の看板

■出典:https://www.jiji.com/jc/article?k=2024122500623&g=eco

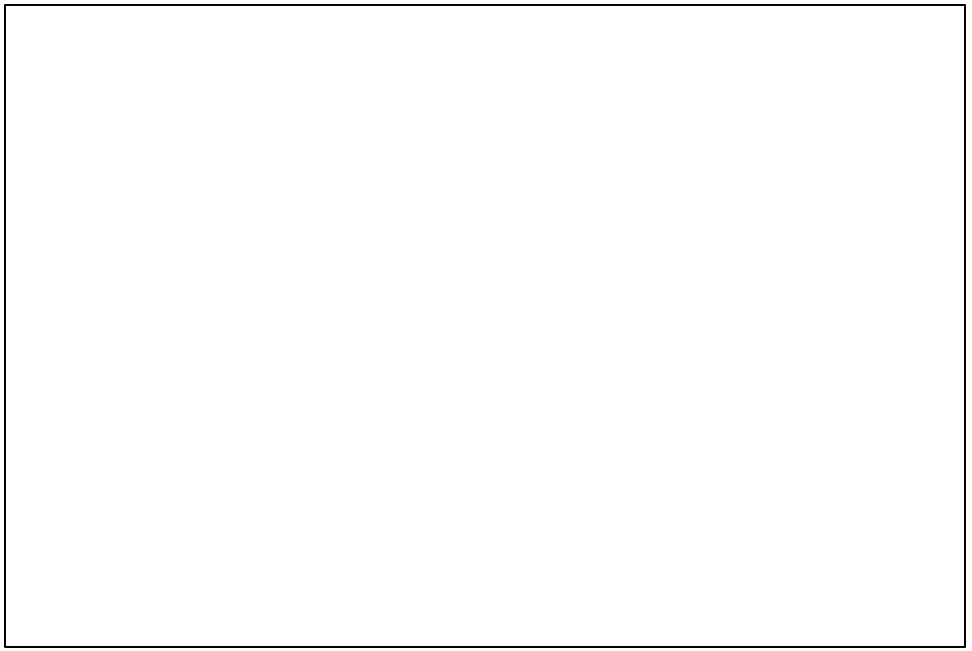
■サイゼリヤ、不正アクセスにより個人情報6万件流出か

2024年12月12日

・外食大手サイゼリヤは12月10日、同社のサーバーへの不正アクセスにより、個人情報の一部が漏えいしたと発表した。

・原因は、10月5日以降に発生したランサムウェア攻撃により、一部サーバーがマルウェアに感染。第三者が不正アクセスできる状態となっていたことだとされている。

・流出件数は、取引先企業の関係者（約2200件）のほか、従業員、元従業員およびその家族（約5万9000件）など計約6万1000件。店舗利用客の個人情報の漏えいはない。



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：サイゼリヤのニュースリリース
■出典：https://ascii.jp/elem/000/004/240/4240626/

■「キッザニア東京」来場予約者2.5万人の個人情報流出 不正アクセス受け

2024年12月9日

・職場体験テーマパーク「キッザニア」を運営するKCJ GROUPは12月6日、Webサイトが第三者による不正アクセスを受け、「キッザニア東京」（東京都江東区）への来場を予約した一部ユーザーの氏名や住所など2万4644件が流出したと発表した。

・流出したのは、氏名と住所、メールアドレス、電話番号。2024年10月17日以前にキッザニア東京を予約する際に登録された一部という。

・10月16日、同社が運営するWebサイトへの不正アクセスを検知し、17日に個人情報流出のおそれがあることが判明。情報流出の遮断措置を行った。

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：ニュースリリースより

■出典：
https://www.itmedia.co.jp/news/articles/2412/09/news145.html

■ PayPayの初売り・お年玉キャンペーンかたるフィッシングに注意

2024年12月5日

・フィッシング対策協議会は12月4日、PayPayによる「初売りキャンペーン」や「お年玉キャンペーン」をかたるフィッシング詐欺の報告が増えているとして、注意を呼び掛けた。

・メールではキャンペーンの参加にはログインが必要だとして偽サイトへ誘導、個人情報やクレジットカード情報などの入力を促される。

・4日午後1時半時点で偽サイトは稼働中。フィッシング対策協議会は、サイトに情報を入力しないよう注意喚起している。

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。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：偽メールの本文（一例）
■出典：
https://www.itmedia.co.jp/news/articles/2412/05/news142.html

サイバー攻撃最新事例

■7割の企業がサイバー攻撃経験、累計被害平均1.7億円

2024年12月17日

・サイバーセキュリティー大手のトレンドマイクロにより、日本国内の従業員規模500人以上の企業の経営らを対象に行われる、サイバー攻撃の実態調査の結果が発表された。

・調査の結果、70.9%が過去3年間にサイバー攻撃を経験したと回答し、被害コストが大きかったのはビジネスメール詐欺が18.3%と最も多かった。続いて、ランサムウエアが13.0%となった。

・サイバー攻撃の被害を受けた企業の累計被害額は平均約1億7100万円で、昨年度の調査から約4600万円増加した。
特にランサムウエア攻撃の累計被害額は平均2億2000万円(昨年度比4400万円増)となっている。

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3年間のサイバー攻撃による累計被害額

■出典： https://dempa-digital.com/article/617033?type=gallery

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。