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8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

■伊藤忠テクノソリューションズの委託先がランサムウェア攻撃の被害にファイル共有サービスに不正なアクセス

2024年8月14日

・伊藤忠テクノソリューションズは8月13日、委託先企業がランサムウェア攻撃を受け、何者かがファイル共有サービスに不正アクセスしたと発表した。

・ファイル共有サービスは委託先が業務で使っていたもので、顧客を含めた取引先情報や個人情報が含まれていた。情報は閲覧されたか持ち出された可能性もあるという。現在、侵入の経緯や情報漏えいの有無について詳細を調査中。

・影響のあったPCはネットワークから遮断。不正アクセスのあったファイル共有サービスもアクセスを制限した。個人情報保護委員会にも報告し、情報を閲覧・持ち出された可能性がある顧客にも個別に連絡済み。今後、調査で判明した内容を基に、再発防止策を整備するという

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：同社公式サイトから引用

■出典：https://www.itmedia.co.jp/news/articles/2408/14/news111.html

■三菱電機子会社にサイバー攻撃　従業員らの個人情報が流出の可能性

2024年8月5日

・三菱電機子会社で掃除機や炊飯器などを手がける三菱電機ホーム機器（本社・埼玉県深谷市）は5日、サイバー攻撃を受けて従業員ら3893人の個人情報が流出した可能性があると発表した。情報の悪用は確認されていないという。

・情報システムサーバーへの不正アクセスを確認したのは4月17日。従業員、元従業員、採用に応募した人の氏名、住所、電話番号、メールアドレスが流出した可能性があるという。

・また、家電製品の顧客約231万人についても、別のサーバーで保管していた同様の個人情報が閲覧された可能性があるという。こちらは閲覧時間が短く、流出の可能性はないとしている。

サイバー攻撃によって従業員の個人情報が漏洩してしまうこともあります。きちんと社内の情報を守れるよう、常にセキュリティの状態を確認しましょう。

■画像：三菱電機本社＝東京都千代田区
■出典：https://www.asahi.com/articles/ASS852TNFS85ULFA01XM.html

■「マネーフォワード」ユーザーのアカウントが乗っ取られ、不審なメールの大量送信に悪用される。注意呼び掛け

2024年8月16日

・株式会社マネーフォワードは、同社のサービス「マネーフォワード クラウド請求書」を悪用して不特定多数へのメールが大量送信される事象が発生したとして、8月8日付で注意喚起を行った。

・ユーザーのアカウントが第三者に乗っ取られるなどして、同サービスの機能が不正に利用されたという。同社ではアカウント不正利用のモニタリングを強化し、8月13日までに12件のアカウントでの不正利用を確認。さらに不正利用が疑われるアカウントを含め、計75件のアカウントを利用停止する措置をとった。

・同社メールアカウントからの不審なメールに注意を呼び掛けるとともに、「マネーフォワード ID」を保有するユーザーに対してアカウント管理の再確認を呼び掛けている。

■画像：マネーフォワードが8月8日付で出した注意喚起のお知らせ。その後、8月13日に情報が更新されている

■出典：https://internet.watch.impress.co.jp/docs/news/1616440.html

サイバー攻撃によりアカウントが悪用されることで、自社がサイバー攻撃に加担してしまうこともあります。自社が加害者にならないためにもセキュリティ対策を講じていきましょう。

■SMBCかたるフィッシングメールに注意　QRコードで偽サイトに誘導

2024年8月28日

・三井住友銀行をかたるフィッシングメールが増加しているとして、フィッシング対策協議会が8月28日に注意を呼び掛けた。メールに記載したQRコードからフィッシングサイトに誘導する手口の報告が増えているという。

・「カードの利用明細を確認するため、以下のQRコードをスキャンしてほしい」などとし、コード経由でフィッシングサイトに誘導。ID・パスワードやカード情報などの入力を求めるという。

・フィッシングサイトは28日午前10時時点で稼働中。フィッシング対策協議会は「一般的にメールに記載したQRコードからログインを促すメールは不正メールの可能性が高い」とし、個人情報などを入力しないよう注意を呼び掛けている。

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。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：メールの文面（フィッシング対策協議会の発表より）

■出典：
https://www.itmedia.co.jp/news/articles/2408/28/news115.html

■【セキュリティ関係者 1000人にアンケートを実施】約38%がセキュリティインシデントを経験、企業のセキュリティ対策の現状と課題

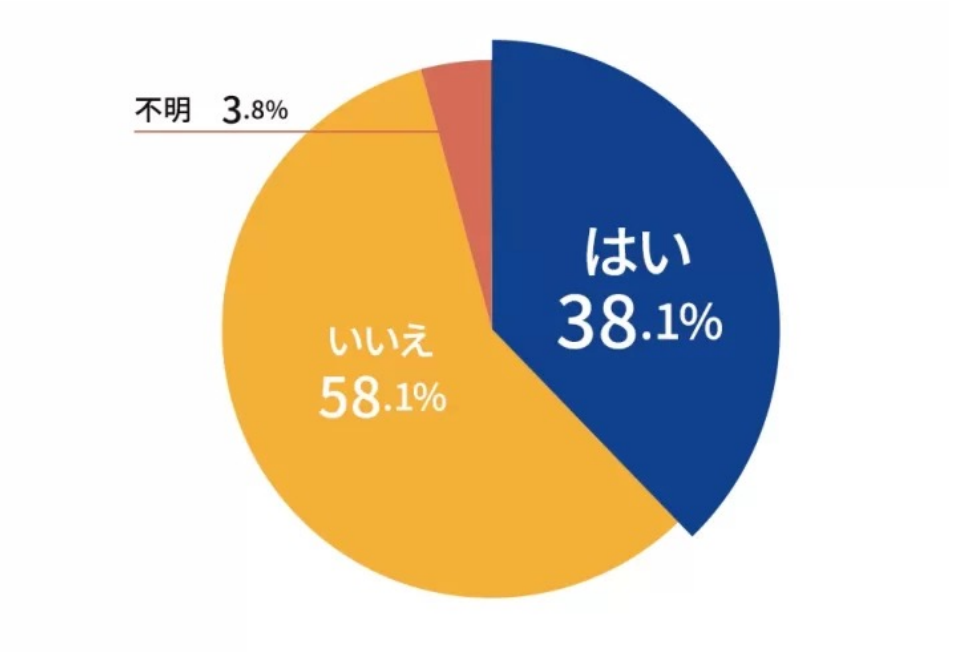
2024年8月7日

・株式会社スリーシェイクは、1045名のセキュリティ関連業務に従事する方を対象に、「企業のセキュリティ対策の現状と課題」についてアンケート調査を行った。

・過去1年間におけるセキュリティインシデント（データ漏洩、サイバー攻撃など）の発生状況を調査した結果、回答者の約38.1%がセキュリティインシデントを経験していることが明らかになった。

・サイバーセキュリティ対策の充実度については、61.6%が「おおむね十分だが、改善の余地はある」と回答した。多くの企業が基本的なセキュリティ対策を実施しているが、新しい技術や変化する脅威に対し、継続的な改善していく必要を感じていることが分かった。

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：過去1年間にセキュリティインシデントの経験があるか

■出典：https://www.securify.jp/news/research-202405/

■フィッシング報告が過去最多を更新 - 悪用URLは減少

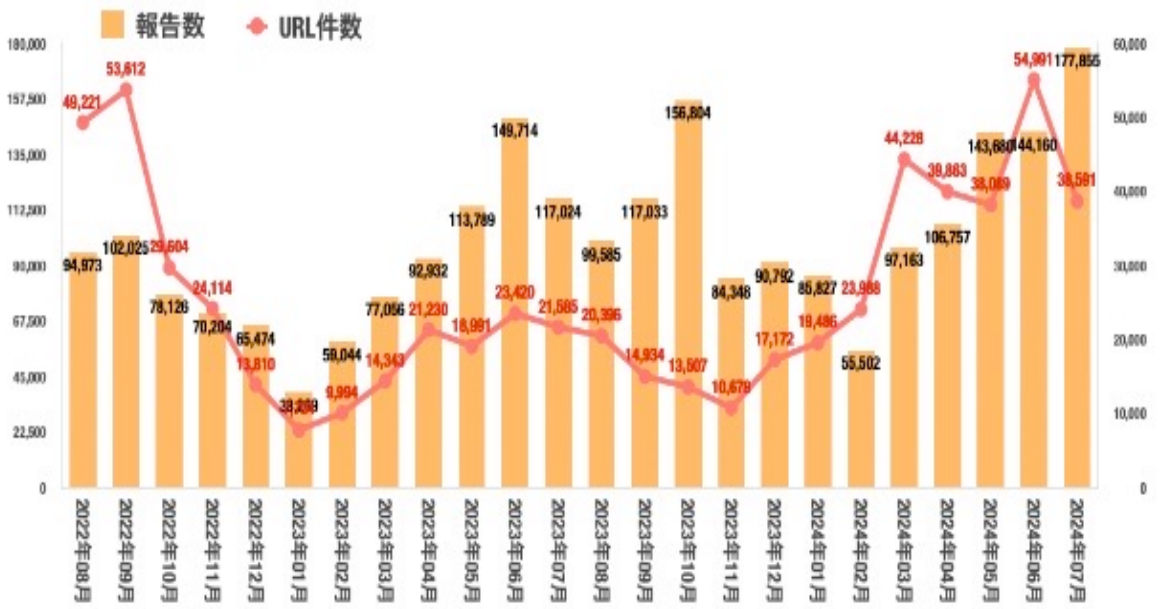
・フィッシング対策協議会によれば、7月に寄せられたフィッシング攻撃の報告は17万7855件。前月から23.4%増加した。これまで最多だった2023年10月の15万6804件を大きく上回り、過去最多となった。

・報告が大きく増加する一方、フィッシングサイトに悪用されたURLは、前月の5万4991件から約29.8%減少し、3万8591件となった。1日あたりに換算すると約1244.9件となる。

・フィッシングサイトのURLを見ると、約35.8%が1000回以上の報告があるドメインを含むため、ドメイン名を用いたフィルタに一定の効果はあるものの、約19.3%は報告回数が10回以下のドメインであり、URLフィルタ以外の対策の必要性について強調している。

ドメインの判別技術を用いた受信拒否をすり抜けてくるものもあります。対策しているからと安心せず、常に注意することが重要です。

2024年8月23日



■画像：フィッシング報告やURL件数の推移

■出典：https://www.security-next.com/161061

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。