BASIC
Confertas Office

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
2023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
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。

■NISCにサイバー攻撃、メールデータ5千人分流出か　気象庁も被害

2023年8月5日

・政府の内閣サイバーセキュリティセンター（NISC）は4日、電子メールシステムがサイバー攻撃を受け、約5千人分の個人情報を含むメールのデータが外部に流出した可能性があると発表した。NISCと取引のある民間企業や協力組織が被害を受けた可能性があるという。

・発表によると、流出した可能性があるのは、昨年10月から今年6月までの間に、インターネットを経由してNISCとメールのやりとりをした個人や組織のメール。該当者約5千人には4日までにメールで通知した。政府の個人情報保護委員会には報告済みという。

・電子メールシステムを構成する機器に対する不正な通信の痕跡が6月13日に見つかり、調査していた。直近で発覚した機器の未知の欠陥（脆弱〈ぜいじゃく〉性）を悪用されたことが原因と考えられ、同じ被害が海外でも確認されているという。

不正アクセスを受けて被害に遭うという事例が近年、増加しています。各拠点のセキュリティ対策や従業員教育を徹底しましょう。

■画像：気象庁

■出典：https://www.asahi.com/articles/ASR8545P7R84ULZU009.html

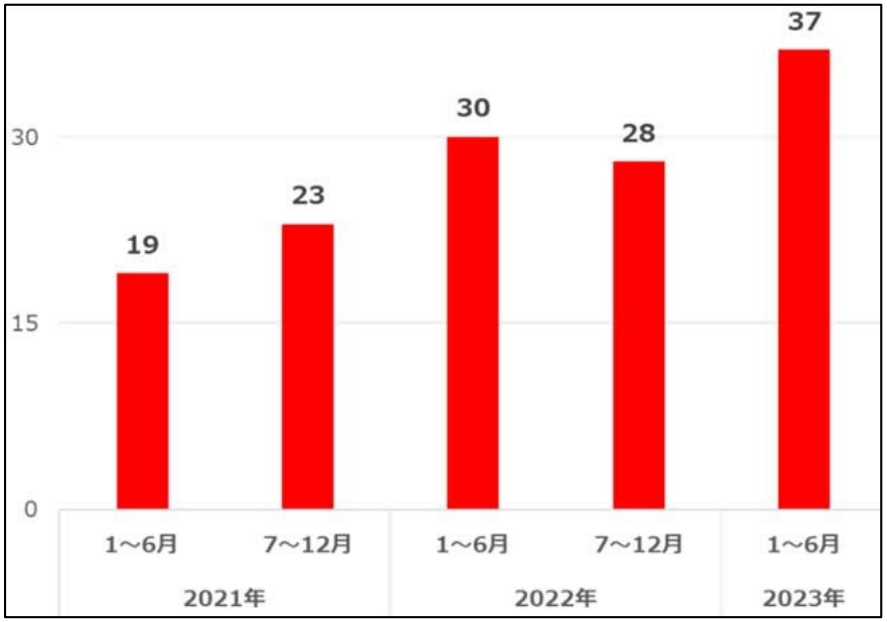
■国内のランサムウェア被害件数が最大に。VPNの脆弱性やアカウントリスト攻撃が発生原因

2023年8月24日

・トレンドマイクロは2023年8月24日、2023年上半期（1～6月）の国内法人のランサムウェア被害件数は2021年上半期以降で過去最大だったと発表した。海外拠点を含む、国内法人が公表したランサムウェア被害は37件で、2022年上半期と比べると2割強の増加になったという。

・ランサムウェア被害の発生原因だが、トレンドマイクロが公表されている10件の事例に着目したところ、VPNに代表されるネットワーク機器の脆弱性を利用した攻撃、もしくはリスト型アカウントハッキング（アカウントリスト攻撃）などの認証突破のいずれかだった。

・どちらにおいても攻撃者は、インターネット側から内部ネットワークへアクセスするための接点に存在する弱点を利用している。



■画像：国内組織が公表したランサムウェア被害件数推移

■出典：https://businessnetwork.jp/article/15941/

ランサムウェアの被害は増加傾向にあり、セキュリティ対策の重要性は増しています。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。

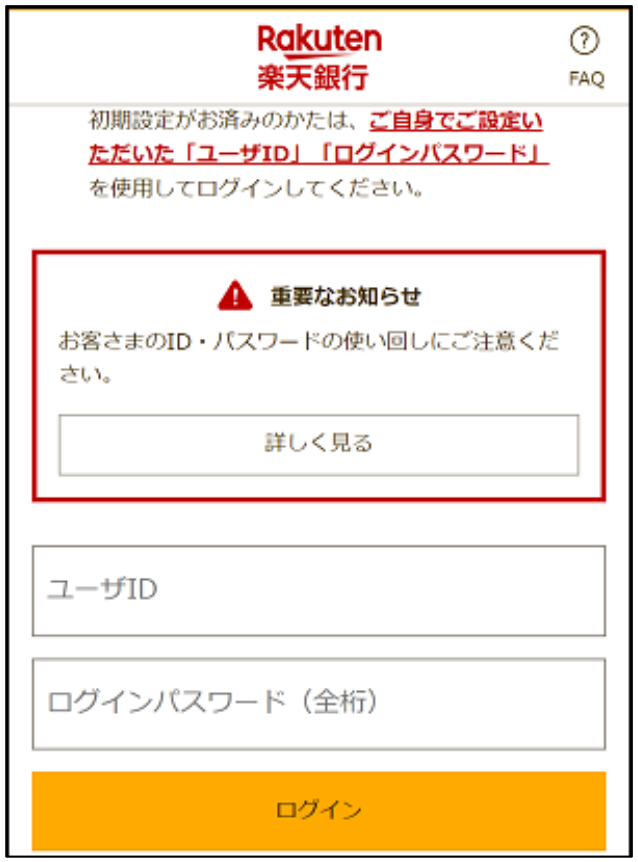
■楽天銀行をかたるフィッシング、件名「楽天銀行からのお知らせ［追加認証を一時制限しました］」などの不審なメールに注意

2023年8月2日

・楽天銀行をかたるフィッシングの報告が増えているとして、フィッシング対策協議会が情報を公開した。誘導先のフィッシングサイトは8月1日17時時点で稼働中であるため、引き続き注意が必要だ。

・フィッシング対策協議会は、「フィッシングサイトは本物のサイトの画面をコピーして作成されることが多く、見分けることは非常に困難」と指摘する。その上で、日頃から、サービスへログインする際はメールやSMSのリンクを利用するのでなく、公式アプリやウェブブラウザーのブックマークからアクセスするよう、注意を促している。

・楽天銀行でも注意喚起を実施、同行のログイン画面を装い、ユーザーIDとパスワードの入力を求める画面が発見されたとの情報があるとして、身に覚えのないメールやショートメールなどを受け取っても、画像やリンクを一切クリックせず、削除するようにと呼び掛けている。



■画像：誘導先のフィッシングサイトの画面

■出典：
https://internet.watch.impress.co.jp/docs/news/1521010.html

フィッシングメールを見分けることは困難です。ログインの際は公式アプリやウェブブラウザのブックマークからのアクセスを日ごろから意識してみましょう。

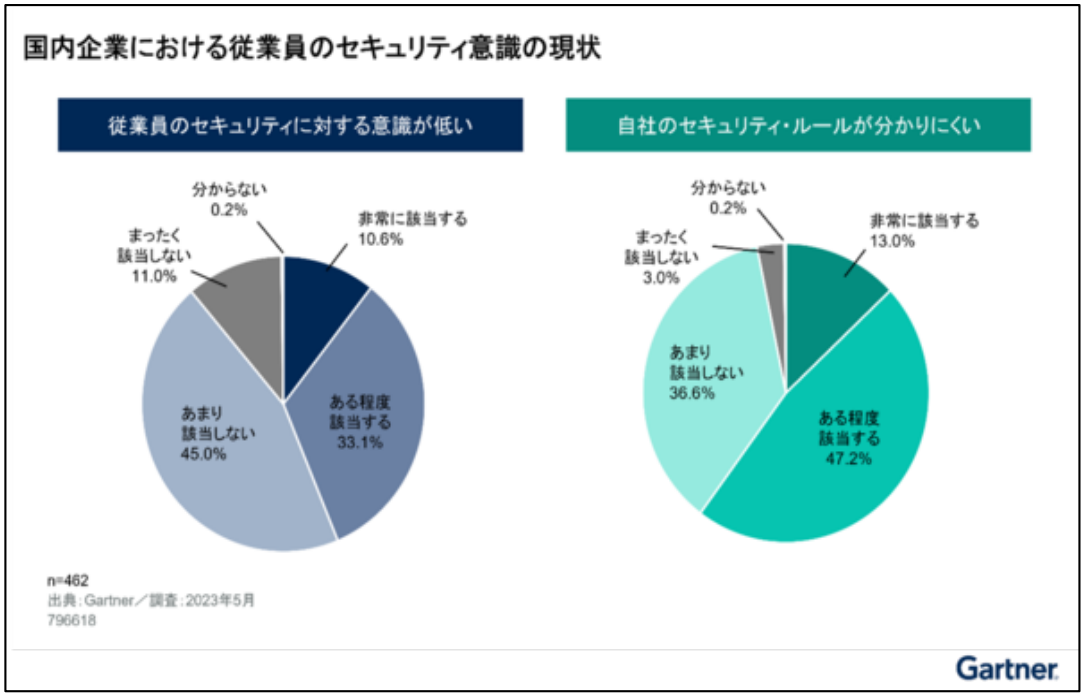
■4割を超える国内企業が「従業員のセキュリティ意識が低い」と回答

2023年8月10日

・ガートナージャパンは、国内企業に所属する従業員のセキュリティ意識を調査した。2023年5月に従業員300人以上の国内企業を対象に調査した。

・4割を超える企業が「自社の従業員のセキュリティ意識は低い」と回答した。「従業員のセキュリティに対する意識が低い」という項目に対して「非常に該当する」との回答が10.6%、「ある程度該当する」との回答が33.1%、合わせて43.7%に達した。

・この結果を受けて同社は「ルールを実践すべき従業員のセキュリティ意識が低いことは、セキュリティの取り組みを推進する企業にとっては大きな問題。従業員のセキュリティリテラシーの向上は喫緊の課題」と指摘する。



セキュリティ対策において従業員の協力は必要不可欠です。従業員の教育を徹底し、セキュリティ対策をより強固なものにしていきましょう。

■画像：国内企業における従業員のセキュリティ意識の現状

■出典：https://it.impress.co.jp/articles/-/25220

■倉敷帆布　クレジットカード情報など4万人分超の個人情報を漏洩か

2023年8月18日

・かばんや雑貨などの製造・販売を手掛ける倉敷帆布は、8655件のクレジットカード情報を含む4万人分を超える個人情報が漏洩した可能性があると発表しました。

・クレジットカードの情報が漏れた可能性があるのは、2021年3月24日から2023年4月17日の間にオンラインストアでクレジット決済を利用した8655人分です。

・倉敷帆布は、対象者には電子メールなどで個別に連絡するとしていて、問題発覚以降オンラインストアは閉鎖しています。

・また、7月13日に児島警察署に被害を報告していて「今後セキュリティの見直しを行い万全の体制でサイトを再開します」としています。

いつサイバー攻撃の被害に遭うかは分かりません。突然の攻撃にも対処できるよう、常にセキュリティ対策を万全な状態に保ちましょう。

■画像：倉敷帆布のホームページ

■出典：
https://news.yahoo.co.jp/articles/f73a8798b80e3f24b2e76ef3a8acf803f13a18a0

BASIC Confertas Office

■経済安保の強化へ２３の技術を「特定重要」に追加…偽情報探知するＡＩやサイバー防御

2023年8月1日

・政府は、経済安全保障の強化に向け、官民の研究機関に財政支援をして育成する「特定重要技術」について、新たに２３の先端技術を追加する方針を固めた。ＡＩ（人工知能）を活用した偽情報の探知技術や、重大なサイバー攻撃を未然に防ぐ「能動的サイバー防御」の関連技術などが柱だ。

・２３の技術を盛り込んだ「第２次研究開発ビジョン（構想）」案は８月１日、政府の有識者会議に提示される予定だ。

・偽情報対策では、膨大なネット上のやり取りの中から、偽情報を見つけ出すＡＩの開発を進める。ＳＮＳを中心に、誤った日本の政府方針や災害情報、選挙情報など、悪意を持って拡散されるフェイクニュースを素早く探知することが想定されている。

「特定重要技術」に追加される主な技術

サイバー	▶ AI（人工知能）を活用し、偽情報を探知する技術 ▶（能動的サイバー防御を念頭に置いた）サイバー空間の状況把握・防御技術
海洋	▶ 海中作業の無人化・効率化を可能とする海中無線通信技術
宇宙・航空	▶ 人工衛星の寿命を延長するための燃料補給技術
バイオ	▶ 有事に備えた止血製剤製造技術

日々、技術が進歩する中で新しい技術の強みや弱点を知ることは大切なことです。ぜひ新技術について日常的に調べてみましょう。

■画像：特定重要技術に追加される主な技術

■出典：https://www.yomiuri.co.jp/politics/20230801-OYT1T50078/

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。