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7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。

■京都のイセトー、ランサムウェア攻撃で約150万件の個人情報流出

・情報処理サービスなどを手掛けるイセトー（京都市）がランサムウエアに感染し、5日時点で少なくとも約150万件の個人情報が流出していることが分かった。

・愛知県豊田市は4日に、イセトーから約103万5000件の個人情報が流出したと報告を受けたと発表した。このほかにも5日までに徳島県が自動車税の納税者など約20万件（約14万5000人分）、和歌山市が住民税の納税者の個人情報など約15万件の流出があったと明らかにしている。

・徳島県によると、5月にランサムウェアに感染したと発表した当初はイセトーから「情報流出はない」と報告を受けていたが、6月に情報が流出した可能性が報告され、その後、ダークウェブ上に実際の個人情報が公開されたことで流出被害が明らかになった。

2024年7月5日

イセトーが自治体や企業から管理を受託した個人情報の流出が相次いでいる

徳島県	約20万件 (約14.5万人)
愛知県豊田市	約103.5万件 (最大延べ約42万人)
和歌山市	約15万件
クボタ	約6万人
京都商工会議所	延べ約4.2万件
公文教育研究会	約4700人

(注) 7月5日時点、日本経済新聞調べ

■画像：個人情報が流出したとされる自治体と企業

■出典：
https://www.nikkei.com/article/DGXZQOUF056CM0V00C24A7000000/

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。

■リクルート、従業員の氏名情報が漏洩　サイバー攻撃受け

2024年7月16日

・リクルートは16日、第三者によるサイバー攻撃で従業員などの氏名の情報が漏洩したと発表した。取引先顧客に関する情報の漏洩や従業員などの情報を使った二次被害などは確認されていないとしている。

・7月9日に不動産情報サイト「SUUMO」が一部エリアで提供している実証実験中の不動産会社向けサービスのサーバーに対し、第三者による不正アクセスを検知した。システムを停止して調査したところ、従業員などに関する情報漏洩があると判明した。

・当該サービスについて、「サーバーの再構築・再点検を実施しセキュリティー対策を一層強化する」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：サイバー攻撃で従業員などの氏名の情報が漏洩した
■出典： https://www.nikkei.com/article/DGXZQOUC168ZD0W4A710C2000000/

■りそな銀行を偽るフィッシング確認、注意を

2024年7月3日

・フィッシング対策協議会(Council of Anti-Phishing Japan)は7月2日、りそな銀行を偽るフィッシングの報告を受けているとして、注意を喚起した。

・パスワード入力間違いが連続したため一時的に制限を行っているなどの理由でサービスを制限したという旨のメールが送られ、制限を解除するために本人確認などが必要だとしてフィッシング詐欺サイトへのクリックを促される。

・この件に関して、りそな銀行も公式ホームページ等で注意喚起を行っている。

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：フィッシング対策協議会　Council of Anti-Phishing Japan｜ニュース｜緊急情報｜りそな銀行をかたるフィッシング (2024/07/02)

■出典：https://news.mynavi.jp/techplus/article/20240703-2978320/

■国内企業のランサムウェアへの備えは不十分、備えた準備の中で最も多い「バックアップからの復旧体制」でも4割弱

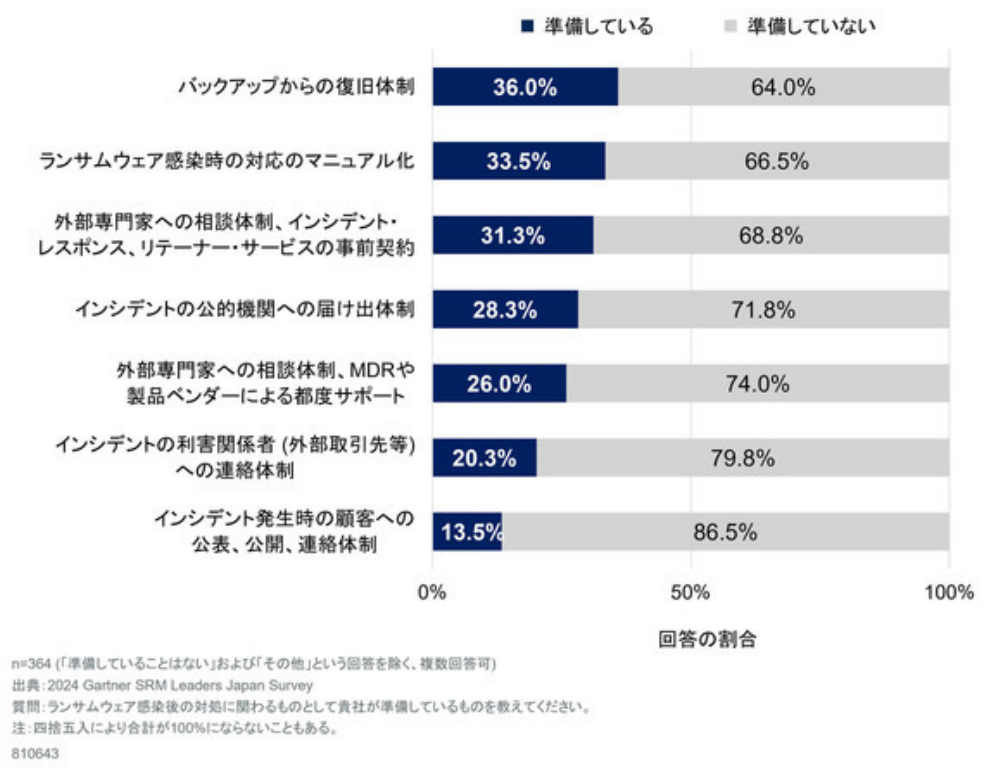
2024年7月2日

・ガートナージャパンは2024年7月1日、国内のランサムウェア対策状況に関する調査結果を発表した。

・ランサムウェア感染に対する企業の対策・準備状況について聞いたところ、最も多かった項目は「バックアップからの復旧体制」（36.0%）だった。「ランサムウェア感染時の対応のマニュアル化」（33.5%）が次に続いた。

・同社のシニアプリンシパルアナリストの鈴木弘之氏は、この結果から企業はランサムウェアの感染を前提とした、感染後の対処を準備している現状が読み取れると、最も多い「バックアップからの復旧体制の対策」でも４割弱の割合であるため、備えが十分とは言えないとしている。

ランサムウェアの攻撃を防御し、迅速に復旧するためには事前の準備が非常に重要です。自社のランサムウェア対策を改善していきましょう。



■画像：ランサムウェア感染に備えた準備の実態

■出典：https://www.gartner.co.jp/ja/newsroom/press-releases/pr-20240701

■フィッシング報告が前月比1.3倍、過去最多を更新 - 1日平均約5000件

2024年7月5日

・フィッシング対策協議会によれば、6月に報告を受けたフィッシング攻撃は14万9714件。3万8269件となった1月から増加傾向が続いており、過去最多となった前月をさらに約3割上回った。1日あたり約4990.5件の報告が寄せられている。

・フィッシングサイトに悪用されたURLは2万3420件。前月の1万8991件を大きく上回った。1日あたりに換算すると約780.7件となる

・フィッシングメールに受信者の氏名を宛名に記載するなど、外部流出したデータを悪用したと見られるケースが確認されているとして注意を呼びかけている。

■画像：フィッシング報告やURL件数の推移

■出典：https://www.security-next.com/147585

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。

BASIC Confertas Office

■チェック・ポイント・リサーチ、サイバー攻撃の頻度が過去2年間で最大となっていることを確認

2024年7月25日

・チェック・ポイント・リサーチは、2024年第２四半期のサイバー攻撃の傾向に関するデータを発表した。

・サイバー攻撃は世界的に増加を続けている。2024年第2四半期における企業への週平均攻撃数は、2023年第2四半期に比べ30%増加し、2024年第1四半期から25%増加した。全世界で、1組織当たり週平均1,636件もの攻撃が確認されている。

・同社は、世界的なサイバー攻撃の急増、特にランサムウェア攻撃の劇的な増加は、企業がセキュリティ体制を強化することの必要性を示しているとし、進化するサイバー攻撃に対して効果的な対策をとることが重要であるとしている。

地域	1組織当たりの週平均攻撃数	前年比
アフリカ	2960	+37%
ラテンアメリカ	2667	+53%
アジア太平洋地域	2510	+23%
ヨーロッパ	1367	+35%
北アメリカ	1188	+17%
日本	**1389**	**+29%**

■画像：地域別のサイバー攻撃分析

■出典：
https://prtimes.jp/main/html/rd/p/000000311.000021207.html

定期的なシステムのアップデートや従業員のセキュリティ意識の向上、セキュリティの脆弱性診断など様々なセキュリティ対策に積極的に取り組んでいきましょう。

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。