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5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

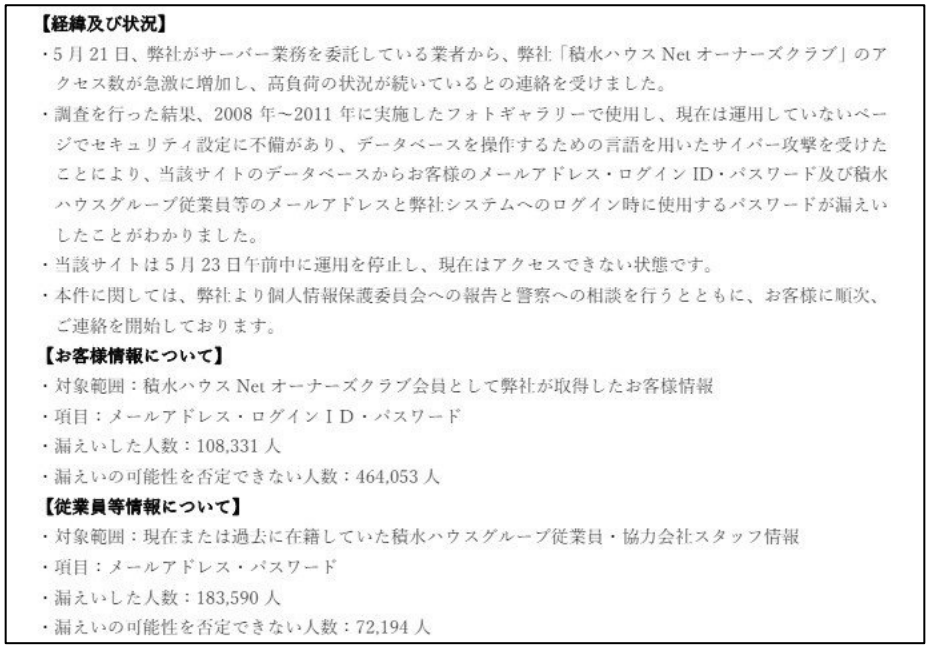
■積水ハウスにサイバー攻撃　約30万件の情報漏えい、パスワードもさらに流出疑いも50万件超

2024年5月24日

・積水ハウスは5月24日、住宅オーナー向けの会員制サイト「積水ハウス Net オーナーズクラブ」で情報漏えいがあったと発表した。会員・従業員のメールアドレスやパスワードなど30万件近くが漏えいした他、これとは別に50万件超の情報が漏えいした可能性も否定できないという。

・2008年から11年にかけて運用、現在は使用していないWebページのセキュリティ設定に不備があり、漏えいにつながったという。調査により、データベースを操作するための言語を用いたサイバー攻撃を受けたことが分かった。

・積水ハウス Net オーナーズクラブは23日午前に停止。今後は個人情報保護委員会への報告や警察への相談と並行して、顧客への説明を進めるという。



【経緯及び状況】
・5 月 21 日、弊社がサーバー業務を委託している業者から、弊社「積水ハウス Net オーナーズクラブ」のアクセス数が急激に増加し、高負荷の状況が続いているとの連絡を受けました。
・調査を行った結果、2008 年～2011 年に実施したフォトギャラリーで使用し、現在は運用していないページでセキュリティ設定に不備があり、データベースを操作するための言語を用いたサイバー攻撃を受けたことにより、当該サイトのデータベースからお客様のメールアドレス・ログイン ID・パスワード及び積水ハウスグループ従業員等のメールアドレスと弊社システムへのログイン時に使用するパスワードが漏えいしたことがわかりました。
・当該サイトは 5 月 23 日午前中に運用を停止し、現在はアクセスできない状態です。
・本件に関しては、弊社より個人情報保護委員会への報告と警察への相談を行うとともに、お客様に順次、ご連絡を開始しております。
【お客様情報について】
・対象範囲：積水ハウス Net オーナーズクラブ会員として弊社が取得したお客様情報
・項目：メールアドレス・ログイン ＩＤ・パスワード
・漏えいした人数：108,331 人
・漏えいの可能性を否定できない人数：464,053 人
【従業員等情報について】
・対象範囲：現在または過去に在籍していた積水ハウスグループ従業員・協力会社スタッフ情報
・項目：メールアドレス・パスワード
・漏えいした人数：183,590 人
・漏えいの可能性を否定できない人数：72,194 人

ネット上に公開されているすべてのWebページでサイバー攻撃を受ける可能性があります。個人情報を保護するために、自社でのセキュリティ対策を徹底しましょう。

■画像：漏えいした、もしくはその可能性がある情報の内訳

■出典：
https://www.itmedia.co.jp/news/articles/2405/24/news180.html

BASIC Confertas Office

■北洲のサーバに不正アクセス、攻撃者が一部ファイルを開いた可能性を確認

2024年5月28日

・株式会社北洲は5月21日、3月15日に公表した同社サーバへの第三者による不正アクセス攻撃について、調査結果を発表した。

・同社では3月11日午前1時頃に、サーバへの不正アクセスを確認し、不正アクセスのあったサーバ、ファイルの特定や不正アクセスの原因調査、復旧作業を併行して進めていた。調査の結果、社内データが外部に持ち出された可能性は極めて低いと判断しているが、一方で攻撃者によって開かれた可能性のあるファイルが一部あることが確認された。

・同社では再発防止策として、管理体制見直し・社員教育の再徹底とセキュリティシステムの強化を実施するとのこと。

■画像：リリース（当社サーバへの不正アクセスに関するお知らせと調査結果のご報告）

不正アクセス攻撃を受けた後には、迅速かつ的確な対応が求められます。起きてしまった場合の対応について考えておく必要があるかもしれません。

■出典：https://scan.netsecurity.ne.jp/article/2024/05/28/51062.html

■株式会社ネクストレベルに不正アクセス　個人情報など約50万件漏えいか

2024年5月28日

・短期人材派遣サービスを提供する株式会社ネクストレベルは5月24日、不正アクセスにより個人情報など50万件近くが漏洩した可能性があると発表した。

・事態が発覚したのは2023年7月14日。第三者から1部のユーザーの個人情報が漏洩しているとの報告があり、調査した結果、事業者側に提供していた管理画面からデータベースに不正アクセスがあり、個人情報が漏洩していたことが分かったという。

・ 発覚後、直ちに事業者側のアカウントの停止等、必要な緊急対策を実施し、また、システム会社と連携の上、セキュリティ向上のためのアップデートを行い、同様の事態が発生しないよう改善措置を行ったという。

個人情報の流出といった不正アクセスの被害にあってしまうと、システムの復旧からお客様への対応まで多くの作業と時間を要します。被害に合わないよう最大限の対策をしましょう。

■本件の概要

・発覚の経緯

2023年7月14日、第三者から、一部のワーカー様の個人情報が漏えいしているとの情報提供がありました。

当社が直ちに外部のシステム専門家と連携しつつ、調査を実施したところ、当社が管理運営する「ネクストレベル」のプラットフォーム加盟企業に付与していた管理画面から、ワーカーデータベースに対する不正なアクセスにより、一部のワーカー様の個人情報が抜き取られるという事態が発生していたことが発覚いたしました。

・対象となる情報の内容と件数

内容：当社が管理運営する「ネクストレベル」に登録・エントリーされているワーカー様のID、氏名、性別、生年月日、住所、電話番号、メールアドレス、口座情報、勤務経歴及び勤務条件、資格、緊急連絡先、当社システム上に保存されていた身分証明書写真データにアクセスするためのリンクURL（既に変更・セキュリティ措置済）。なお、当社はマイナンバーを取得しておりませんので、漏えい情報にマイナンバーは含まれません。

件数：496,119件

■画像：インシデントの概要
■出典：https://www.itmedia.co.jp/news/articles/2405/28/news155.html

■イオンカードをかたるフィッシング、件名「【イオンカード】お客様のカードご利用明細の内容をお知らせいたします」などの不審なメールに注意

2024年5月9日

・イオンカードをかたるフィッシングの報告を受けたとして、フィッシング対策協議会が情報を公開した。

・メール本文は、カードの利用確認をするためとして、リンクへのアクセスを促している。誘導先のフィッシングサイトは、イオンカードの公式サイト（暮らしのマネーサイト）を装っており、イオンスクエアメンバーIDとパスワードの入力を求められる。入力すると、氏名、生年月日、クレジットカード情報の入力画面が表示される。さらに続けると、SMS認証番号を送信したとして、その番号の入力を促される。

・イオンカードでは不審なメールを受信しても開封しないよう、注意喚起を行っている。

■画像：誘導先のフィッシングサイトの画面（フィッシング対策協議会の緊急情報より）

■出典：
https://internet.watch.impress.co.jp/docs/news/1590126.html

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。

BASIC Confertas Office

■企業のメールセキュリティへに関するアンケート調査結果を発表 大企業の34.7%がサイバー攻撃の被害経験あり

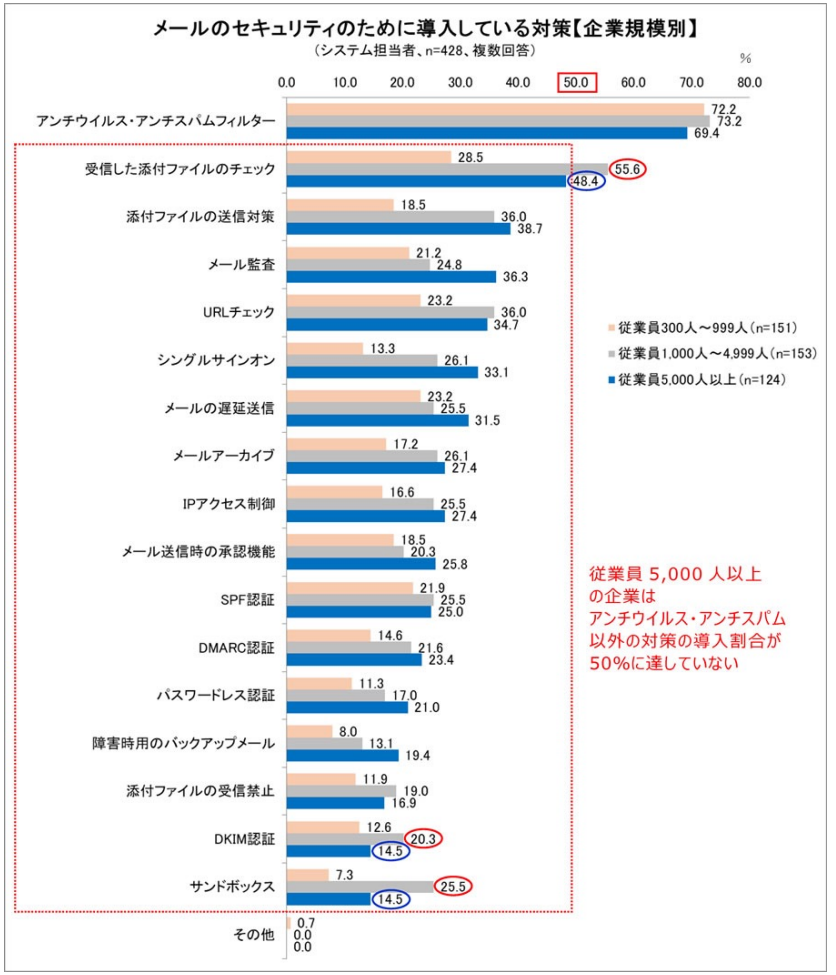
2024年5月22日

・サイバーセキュリティ株式会社が、「企業のメールセキュリティへの取り組みに関するアンケート調査」の結果を発表した。

・過去３年間にサイバー攻撃の被害にあった割合は、従業員5,000人以上の企業では34.7%と1/3を超えることが分かった。被害のうち、「データが暗号化され身代金を要求された」割合は21.6%だった。また、従業員5,000人以上の企業のメールのセキュリティ対策の導入割合は、「アンチウイルス・アンチスパムフィルター」「受信した添付ファイルのチェック」以外の対策は10～40%の普及割合にとどまった。

・ITRのシニア・アナリスト 入谷光浩氏は「業種や規模を問わず、どの企業もランサムウェア攻撃を受ける可能性があり、適切なサイバーセキュリティ対策が不可欠となります。」とコメントしている。

ランサムウェアによる攻撃は、すべての企業が受ける可能性があります。攻撃を受けても感染を未然に防げるよう、新たなセキュリティの導入も検討していきましょう。



■画像：企業のメール環境とセキュリティ対策の実態調査2024
■出典： https://www.cybersolutions.co.jp/news/20240522/

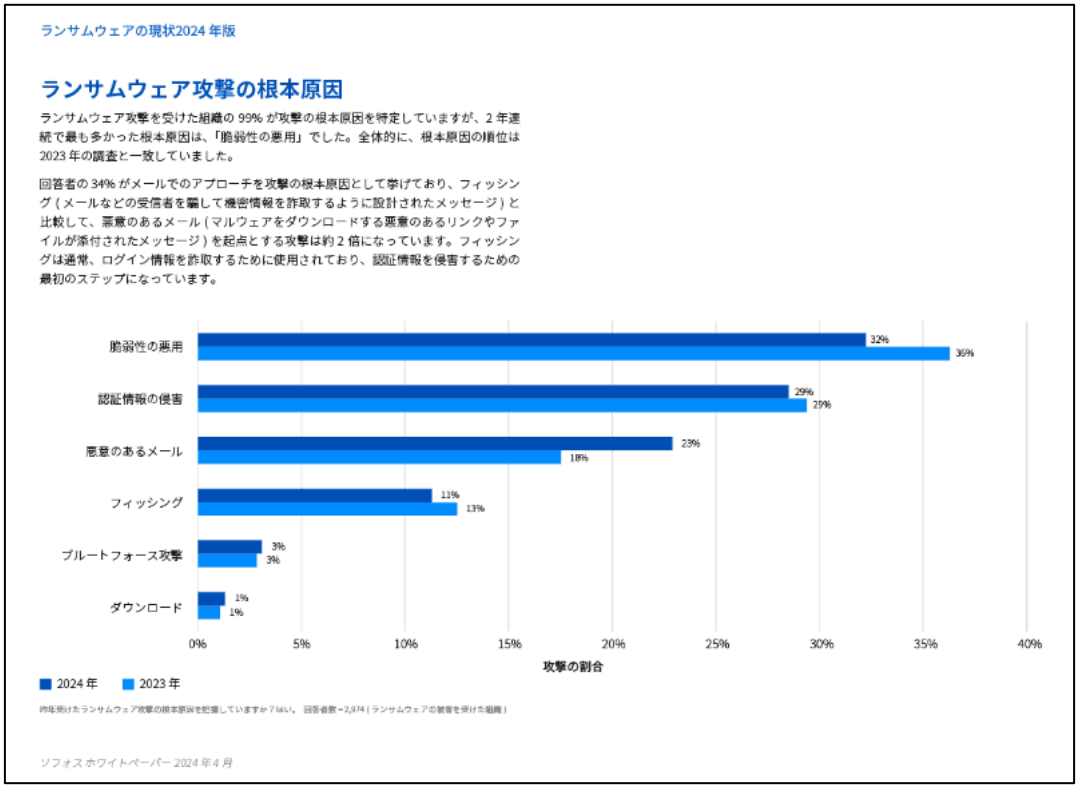
■ランサムウェア攻撃の根本原因、最多は「脆弱性の悪用」～ソフォスが調査結果を発表

2024年5月10日

・ソフォス株式会社は5月9日、年次調査レポート「ランサムウェアの現状 2024年版」を公開した。

・調査の中でランサムウェア攻撃を受けた組織の99%が攻撃の根本原因を特定しており、最も多かったものは「脆弱性の悪用」で32%、次が「認証情報の侵害」で29%、続いて「悪意のあるメール」が23%だった。

・脆弱性が悪用されて攻撃を受けた場合は、認証情報が侵害されて攻撃が開始された場合よりも、バックアップが侵害される割合や、データが暗号化される割合、身代金を支払う割合が高くなっており、深刻な影響を受ける傾向があるという。また、平均復旧コストが高く、復旧完了までに要する期間が長くなる傾向もあるという。



■画像：ランサムウェア攻撃の根本原因

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。

■出典：https://internet.watch.impress.co.jp/docs/news/1590189.html

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。