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6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。

■KADOKAWA、犯罪集団のサイバー攻撃による情報流出を認める

2024年6月28日

・サイバー攻撃による大規模システム障害が起きている出版大手KADOKAWAは28日、サイバー攻撃を仕掛けた組織が公開した情報について、同社が保有する情報が外部に流出したものだと確認した。

・KADOKAWAを襲ったサイバー攻撃にはランサムウェアが使われた。サーバー内のデータが暗号化され、事業に大きな影響が出ている。

・「BlackSuit（ブラックスーツ）」を自称するサイバー犯罪集団は27日、発信元の特定が難しい「ダークウェブ」上に犯行声明を出していた。データの公開中止などと引き換えに身代金の支払いを求めており、支払わなければ7月1日に全データを公開すると通告している

■画像：出版大手「ＫＡＤＯＫＡＷＡ」本社前に設置された社名碑

■出典： https://www.asahi.com/articles/ASS6X3JP2S6XUCVL02TM.html

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。

■リクルートにサイバー攻撃 「Ａｉｒペイ」など主要サービスに一時障害

2024年6月25日

・リクルートは２５日、電子決済サービス「Ａｉｒ（エア）ペイ」など、主要サービスが一時使えなくなるシステム障害が前日発生し、自社サーバーに対する外部からのサイバー攻撃が原因だったと明らかにした。情報漏洩などは確認されていないとしている。

・リクルートによると、２４日午後４時１０分ごろ、不動産情報サイト「ＳＵＵＭＯ（スーモ）」でアクセスしづらい状況を確認した。午後７時半以降、国内のほぼ全てのサービスで障害が起き、午後１０時ごろ解消したという。リクルートは「現状把握とサービスの安定稼働を最優先に、全社を挙げて調査と対応を進める」とコメントした。

サイバー攻撃を受けたとき、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。

■画像：リクルート本社ビル

■出典：https://www.sankei.com/article/20240625-5DFK46HGUFNMFP6L6RE5KQECFY/

■九電グループの給湯器販売会社にランサム攻撃 約10万4千件の個人情報漏えいか

2024年6月5日

・九州電力グループで電気温水器の販売などを手がけるキューヘンは6月3日、第三者によるランサムウェア攻撃を受けたと発表した。また、約10万4000件の個人情報が漏えいした可能性があることも分かった。

・被害状況は調査中だが、3日の時点で社内情報の一部が暗号化されていることを確認した。緊急対応として、影響を受けた可能性があるPCの停止、PCとデータ保存領域のネットワークからの切り離しなどを実施したという。

・九州電力も5日付でプレスリリースを出し、グループ会社への不正アクセスがあったこと、個人情報が漏えいした可能性のある顧客には、個別に連絡していくことを明らかにした。

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。

■画像：キューヘンのプレスリリース（第2報）
■出典：https://www.itmedia.co.jp/news/articles/2406/05/news193.html

BASIC Confertas Office

■森永製菓、職員など4882件の情報漏えいの可能性 社内システムのIDやハッシュ化パスワードなど

2024年6月19日

・森永製菓は6月18日、同社のサーバ機器が外部からの不正アクセスを受け、同社とグループ会社の役職員などの4882件の個人情報が外部へ流出したおそれがあると発表した。

・漏えいしたおそれがあるのは、同社とグループ会社の役職員、委託業務従事者の個人情報（退職者、元従業者の一部も含む）4882件。
氏名と会社名、部署名などの所属、社用メールアドレス、社内システムのログインID、ハッシュ化したパスワードが含まれていた。

・侵入経路は特定・遮断しており、不正使用などの二次被害は確認していないとしている。

お知らせ

不正アクセスによる役職員等の個人情報漏えいのおそれのお知らせとお詫び

2024年06月18日

印刷

森永製菓株式会社のサーバー機器が外部からの不正アクセスを受け、当社およびグループ会社の役職員等の一部の個人情報が外部へ流出したおそれがあることが判明しました。関係者の皆さまに多大なご迷惑とご心配をおかけすることになり深くお詫び申し上げます。
なお、既に侵入経路を特定・遮断しており、現時点で不正使用などの二次被害は確認されていません。

【漏えいのおそれのある個人情報】
当社及びグループ会社の役職員、委託業務従事者（退職者、元従業者の一部を含む）の個人情報　4,882件
・氏名　・所属（会社名、部署名等）　・メールアドレス（ドメイン名：@morinaga.co.jp/@morinaga.com）
・社内システムログインID　・読み取り不可能なようにランダムな文字列に変換（ハッシュ化）されたパスワード
※お客様の個人情報は含まれておりません。

2024年4月9日、当社サーバーで不審な動作を認知後、すみやかに個人情報保護委員会へ報告いたしました。現在、外部の専門機関による調査を進めており、個人情報が外部に流出した明確な証拠は見つかっていませんが、漏えいの可能性を完全に否定することが困難な状況であることから、漏えいのおそれのある対象の方に対し郵送またはメール等で個別に連絡いたします。

いつ、どこからサーバーが不正に侵入されるか分かりません。即座に侵入を感知し、経路を遮断できるよう対策をすすめていきましょう。

■画像：森永製菓のホームページ

■出典：https://www.itmedia.co.jp/news/articles/2406/19/news136.html

■5月のフィッシング報告、前月比34.6%増 - 過去3番目の規模に

2024年6月24日

・5月のフィッシング報告数は前月から急増し、14万件超となる過去3番目に多い件数となった。「Amazon」をかたるケースが3割以上を占めている。

・フィッシング対策協議会によると、同月に寄せられたフィッシング攻撃の報告は14万3680件。前月の10万6757件から34.6%増加した。1日あたり約4634.8件の報告が寄せられている。

・フィッシングで悪用が確認された具体的なブランドを見ると、報告の約31.1%が「Amazon」を偽装したものだった。1000件以上の報告が寄せられたブランドは16件。これらをあわせると全体の約94.0%を占めた。

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。

■画像：フィッシング報告とURL件数の推移

■出典：https://www.security-next.com/158751

■これまでにサイバー攻撃を経験した企業は29.3%【サイバーソリューションズ調べ】

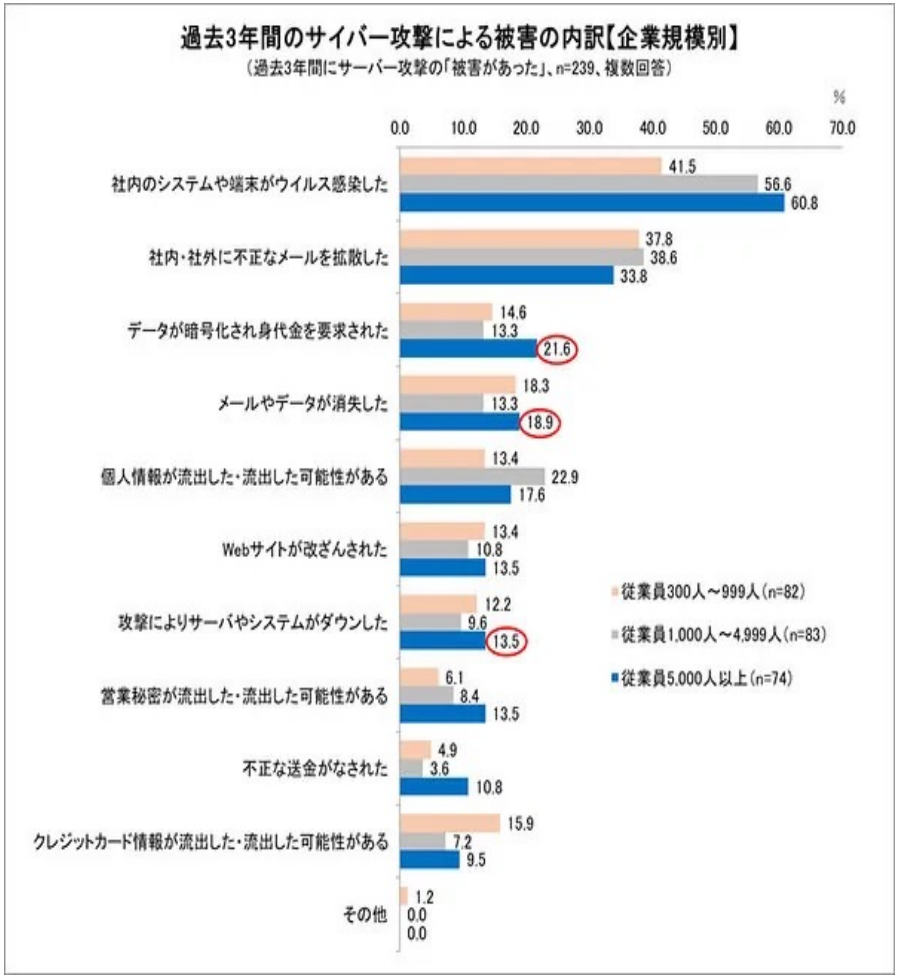
2024年6月27日

・サイバーソリューションズは、「企業のメールセキュリティへの取り組み」に関する調査結果を発表した。従業員300名以上の企業に勤務する1,035人が回答している。

・過去3年間でサイバー被害にあった企業は29.3%だった。企業規模で見ると、300人～999人では24.7%。1,000人～4,999人では30.6%。5,000人以上では34.7%だった。企業規模が大きいほど被害にあった割合が高かった。

・具体的な被害内容を見ると、従業員5,000人以上の企業でもっとも多く発生した被害は、「社内のシステムや端末がウイルス感染した」60.8%、「社内・社外に不正なメールを拡散した」33.8%が上位。また中小規模企業より「データが暗号化され身代金を要求された」「メールやデータが消失した」が高い傾向も見られた。

サイバー攻撃は、すべての企業が受ける可能性があります。攻撃を受けても被害を受けなくて済むよう、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：「企業のメールセキュリティへの取り組み」に関する調査
■出典： https:

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。