

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10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。**
自分事の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。

■ 任天堂、なりすましメールに改めて注意喚起 対応を誤ると不正ログインされる可能性も

2024年10月29日

- ・任天堂は10月29日、実在する同社のメールアドレスを装い、無関係の企業やサービスについて案内する不審なメールが確認されたとして注意喚起した。9月末に任天堂サポートの公式Xアカウントも同様の告知をしていた。
- ・万が一、リンク先のWebサイトを開き、ニンテンドーアカウントのメールアドレスやパスワードを入力してしまった場合は、ニンテンドーアカウントに不正ログインされるおそれもある。速やかにニンテンドーアカウントのWebサイトでパスワードを変更しなければならない。
- ・任天堂は、何度も不審なメールが届く場合はメールサービスを提供している事業者にご相談することを勧めている。

送信元のメールアドレスが同じため、なりすましメールであることに気づくことが難しいです。メールの内容が少しでも不審だと感じたら、URLを踏まないようにするといった意識を持ちましょう。



■ 画像：任天堂なりすましメールの注意喚起。

■ 出典：<https://www.itmedia.co.jp/news/articles/2410/29/news143.html>

■ シャープ、不正アクセスにより5836人の個人情報流出か

2024年10月30日

- ・シャープは30日、自社オンラインサイトの利用者5836人分の個人情報が出た可能性があると発表した。うち、クレジットカードの情報が流出した可能性がある利用者は4257人。シャープは7月、外部からの不正アクセスにより最大約10万人分の個人情報が出た可能性があると公表し、外部の専門機関による調査を続けていた。
- ・個人情報が流出したのはシャープの公式オンラインストア「ココロストア」と食材宅配サービス「ヘルシオデリ」の利用者。ココロストアで商品を購入する際にクレジットカードの番号などを入力した4257人にクレジットカードの情報が流出した可能性がある。
- ・シャープは「このたびの事態を厳粛に受け止め、セキュリティ対策および監視体制の強化を行い、再発防止に努める」とコメントした。



近年では、ネット通販を狙った不正アクセスが増加傾向にあります。クレジットカード情報や住所を入力するサイトの運営では、セキュリティ対策の重要性が非常に高いです。

■ 画像 : SHARP看板

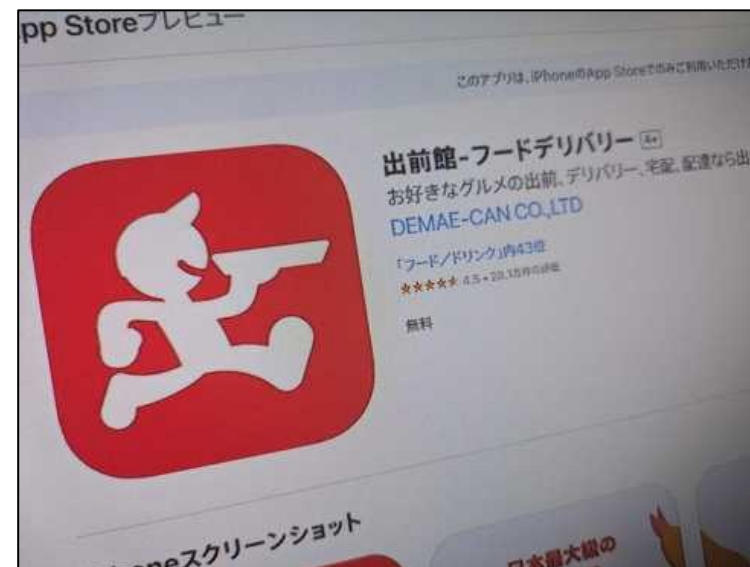
■ 出典 :

<https://www.nikkei.com/article/DGXZQOUF30BRD0Q4A031C2000000/>

■ 出前館のシステム障害、原因は“マルウェア感染” 確認作業で3日以上サービス停止 情報漏えいは現状なし

2024年10月29日

- ・フードデリバリーサービス「出前館」を提供する出前館社は10月29日、3日以上に渡ったシステム障害の原因が、マルウェア「RedTail」だったと発表した。RedTailはコンピューティングリソースを不正に利用して暗号資産をマイニングするマルウェアである。
- ・同社はその後マルウェアを削除したが、サービス再開に万全を期するため確認作業を行ったところ、3日以上のかかりかかったと説明している。29日午後6時30分時点で、出前館はサービスを再開しており、また個人情報の漏えいも確認していないという。



これはコンピュータの計算機能を不正に利用して暗号資産をマイニングするマルウェアの被害例です。被害に遭うと、コンピュータに高負荷がかかり、サービス提供に支障をきたすことがあります。

■ 画像：出前館アプリ

■ 出典：

https://www.itmedia.co.jp/news/articles/2410/29/news205.html#l_tm1636144_10297_2_w490.jpg

■ KADOKAWAグループサイト復活 サイバー攻撃から4カ月半ぶり

2024年10月29日

- KADOKAWAグループは10月29日、グループポータルサイトを再開した。6月上旬に発生したランサムウェア攻撃の影響で停止してから、およそ4カ月半ぶりに復旧した。
- KADOKAWAグループは今年6月、第三者からランサムウェア攻撃を受け、社員の個人情報などが漏えい。「ニコニコ」のサービスなどが2カ月にわたって休止に追い込まれた他、書籍の出荷遅延や公式サイトへの停止などグループ全体で多岐にわたる影響が出た。
- 8月に発表した2025年3月期通期（24年4月1日～25年3月31日）連結業績予想では、書籍の出荷減やWebサービスの停止などによる売上高の84億円減少、営業利益64億円減少を見込む。また調査・復旧費用やニコニコのクリエイター補償費用などで36億円の特別損失の計上を予想している。

大規模サイバー攻撃によるシステム障害 — 業績への影響詳細

本事案により、通期業績における出版・IP創出とWebサービスで売上高▲84億円、営業利益▲64億円の減収減益影響。また、約36億円の特別損失が発生する見通し

(単位: 百万円)	通期業績への影響 (見通し)	うち1Q業績への影響 (実績)
売上高影響	▲8,400	▲2,600
出版・IP創出(国内紙書籍)	▲3,000	▲1,350
Webサービス	▲5,400	▲1,250
営業利益影響	▲6,400	▲1,900
出版・IP創出(国内紙書籍)	▲1,600	▲800
Webサービス	▲4,800	▲1,100
特別損失 <small>※ ニコニコビジネスクリエイター補償や調査・復旧作業等に 係るもの</small>	3,600	2,000

■ 画像：8月に発表した2025年3月期通期連結業績予想

■ 出典：https://www.itmedia.co.jp/news/articles/2410/29/news186.html

大規模なサイバー攻撃から、4ヶ月半の期間を経て、ポータルサイトが復旧しました。特別損失の計上予想からサイバー攻撃被害の深刻さが分かります。

■ 教育・研究部門へのサイバー攻撃数が前年比119%増

2024年10月24日

・2024年10月21日、チェック・ポイント・ソフトウェア・テクノロジーズは最新の「Global Threat Index」を発表。この期間、組織あたりの週平均サイバー攻撃数は1,876件に達し、前年同期比で75%の増加、前四半期と比べても15%の増加という数値が記録されている。

・特に攻撃のターゲットとなったのは教育・研究部門で、1週間あたり平均3,828件の攻撃を受け、前年比119%増という深刻な状況にあり、最も脆弱な業界として他業界と比べても際立った増加傾向が示されている。

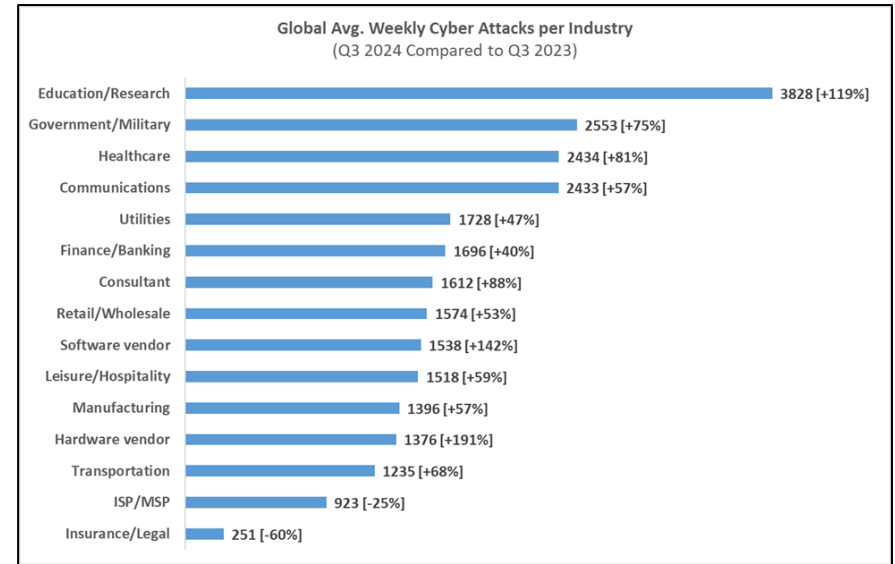
・チェック・ポイントは、今回の調査から以下のようなセキュリティ対策を推奨している。

○高度な脅威検出としてランサムウェア対策ツールの活用。

○定期的なデータバックアップとインシデント対応計画を練り、迅速な対応で影響を最小限に抑える。

○従業員の教育とフィッシング攻撃に対する意識向上を図る。

近年、サイバー攻撃は増加しており、セキュリティ対策の重要性は高まっています。対策が必要と感ずる場合は、すぐにセキュリティの専門家へ相談してみましょう。



■ 画像：世界の業種別ランサムウェア被害数

■ 出典：https://act1.co.jp/2024_10_23-1/

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、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いことが大切です。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。

