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
# 2023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。

# ■「PayPayカード」かたる詐欺メールは本物と見わけつかず… 判断に迷ったらURLをクリックしないで

2023年7月24日

・PayPayカード株式会社は「【ご注意ください】PayPayカードをかたる不審なメール」と題したお知らせを掲載。「PayPayカードをかたる不審なメールが確認されております」とし、「当社に限らず、大手通販会社や宅配業者など実在する企業やサービス・ウェブサイトを装って、不審なメールやSMSなどで、個人情報をだまし取るフィッシング詐欺などの不正行為が増えております。不審なメールを受信した場合には、送られてきたメールそのものを開かずに削除してください。フィッシングメールかどうかの判断が難しい場合には、メール内のリンクはクリックしないようお願いいたします」と注意喚起した。

・また、同社は「フィッシング詐欺の被害に遭わないための対策」もあわせて紹介。「不審なメールは、開かずに削除する」「会員メニュ―でご利用明細を確認する」など、被害に遭わないための対策を案内し、不審なメールが届いた際には念のため利用明細を確認するように呼びかけている。


**フィッシングメールを見極めるのは困難です。少しでも怪しいと感じた場合には、メール内のリンクはクリックしないようにしましょう。**

■画像：フィッシングサイトの例

■出典：https://otona-life.com/2023/07/24/184032/

BASIC
Confertas Office

## ■日本コンクリート工業へのランサムウェア攻撃 サーバ11台が復号不可能に

2023年7月13日

・日本コンクリート工業は、ランサムウェアによるサイバー攻撃を受けた問題で、被害状況などの調査結果を公表した。サーバ11台で暗号化被害が確認されており、定時株主総会において決算報告ができないなど影響が出ている。

・情報流出の痕跡は見つかっておらず、攻撃に用いられたランサムウェアに関しても、複数のセキュリティベンダーによってデータの持ち出しを行わないことが確認されていることなども踏まえ、データの外部流出はないものと結論づけた。

・一方、業務システムの大部分が暗号化されており、被害に遭ったファイルの復号は不可能と判断。完全復旧を断念し、被害を免れたシステムを利用しつつ、以前より計画していた新システムへの移行を進める。


**不正アクセスによるランサムウェア攻撃は、近年増加しています。今一度、社内のセキュリティ対策について見直しや強化を検討してみてるのも大切ですね。**

■画像：日本コンクリート工業ホームページ

■出典：https://www.security-next.com/147820/2

BASIC
Confertas Office

## ■ 生成AI「ChatGPT」を装う偽の広告やアプリが出回る Googleの検索結果から詐欺サイトに誘導する手口も

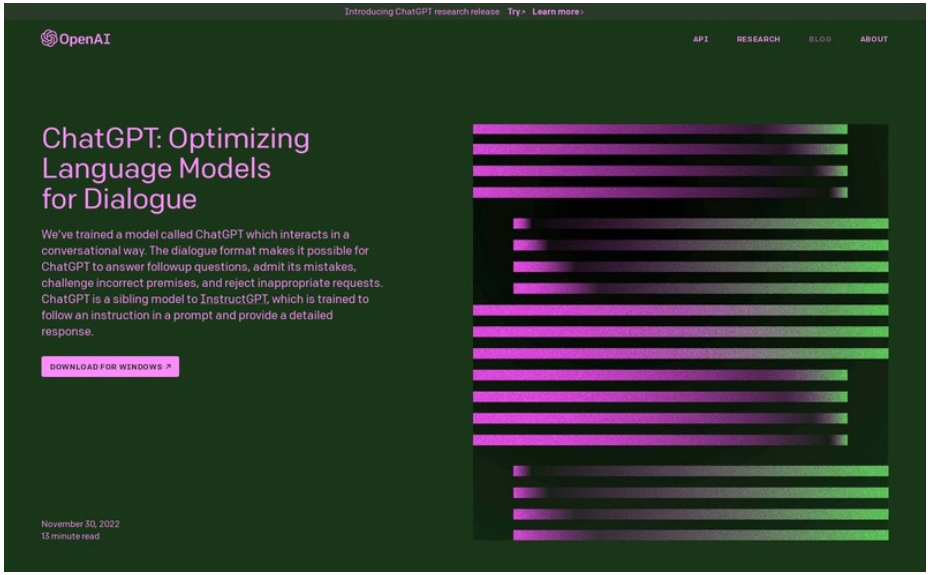
2023年7月21日

・サイバーセキュリティ企業のパロアルトネットワークスによると、Android向けにChatGPTに関する2種類の偽アプリがGoogle Playで発見されたそうです。

・同じくサイバーセキュリティ企業のカスペルスキーによると、ChatGPTの公式サイトそっくりのウェブサイトからマルウェアをダウンロードさせる詐欺サイトの存在が確認されました。正規サイトでは「Try ChatGPT」と表示されているボタンが「Download for Windows」となっており、クリックするとインストーラーがダウンロードされ、実行するとトロイの木馬がPCにインストールされます。

・トロイの木馬がインストールされると、ウェブブラウザーで保存されたアカウントの認証情報のほか、FacebookやTikTok、Googleのアカウントや Cookieを盗み出します。カスペルスキーによると、企業アカウントを見つけ出し、広告ツールの利用履歴や残高の情報を取得するようです。

**急激に普及して知名度が高まったサービスには、詐欺サイトや偽アプリが大量に作られます。利用の際は十分に注意しましょう。**




■画像：ChatGPTを装ったマルウェア配布サイト

■出典：
https://news.yahoo.co.jp/articles/9ae53370316701c3244855b73a538f03545e2a2e

# ■サイバー攻撃で通信内容流出 富士通に行政指導

2023年7月1日

・総務省によりますと、富士通が法人向けに提供しているインターネット回線サービスで、去年3月から11月にかけてネットワーク機器に不正なプログラムが仕掛けられ、サービスを利用している顧客企業およそ1700社分のメールなどの通信の内容が外部に流出しました。

・これについて総務省は、富士通に対して6月30日付けで行政指導を行い、「通信の秘密」の保護や再発防止策の徹底などを求めました。

・総務省によりますと、富士通社内の管理体制がずさんで、セキュリティーに関する経営層の積極的な関与も見られなかったほか、警察から指摘を受けるまでおよそ8か月にわたって会社側がこうした事態に気付いていなかったということで、こうした実態を重く見たとしています。


**近年、不正アクセスが増加するにつれて、セキュリティ対策の重要性も高まってきています。対策が必要と感じる場合には専門家に相談してみましょう。**

■画像：富士通

■出典：
https://www3.nhk.or.jp/news/html/20230630/k10014114571000.html

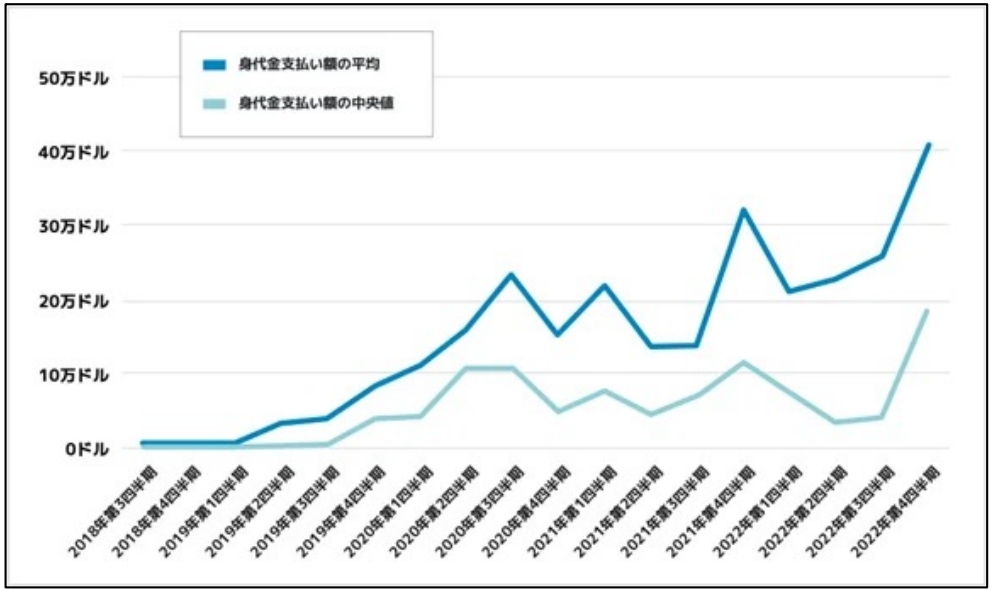
# ■OpenText、サイバーセキュリティ脅威レポート(日本語版)を発表 多層防御によるセキュリティアプローチの必要性を強調

2023年7月18日

・OpenTextは本日、最新の脅威とリスクを調査した「2023年 OpenText Cybersecurity脅威レポート(日本語版)」を発表しました。

・脅威アクターによる攻撃は、年々巧妙化され、進化しています。昨年の顕著な傾向として、マルウェアやフィッシングサイトをホストするURLの位置情報を隠蔽する手法が大幅に増加したことが挙げられます。プロキシやジオロケーションマスクサービスの背後に隠された悪意のあるURLの割合は、前年比36%増加しました。

・オンライン上のサイバーセキュリティの脅威は、驚くべき速さで出現し続けています。悪質なウェブサイトが日々出現する一方で、正しいサイトが不正な目的のために侵害され、利用されることもあります。このような問題は相互に絡み合って脅威を増加させるため、サイバーレジリエンスの導入がこれまで以上に重要となってきています。




**悪質な攻撃は年々巧妙になっていき、さらに数も多くなっています。自分の身を守るためにも一人一人が知識を得ることが大切です。少しずつ知識をつけていきましょう。**

■画像：ランサムウェア被害の平均身代金支払額の推移

■出典：https://prtimes.jp/main/html/rd/p/000000010.000048361.html

# ■名古屋港にサイバー攻撃か　システム障害、搬出入中止

2023年7月5日

・名古屋港運協会（名古屋市）は5日、名古屋港内のコンテナターミナルを管理するシステムで障害が発生したと発表した。トレーラーによるコンテナの搬出入作業を終日中止した。同協会はシステムの復旧を進め、6日午前8時半からの作業再開を目指している。

・協会によると4日午前6時半ごろ、名古屋港統一ターミナルシステムに障害が発生した。ランサムウエア（身代金要求型ウイルス）に感染しており、外部からのサイバー攻撃が原因とみられる。4日朝、ランサムウエア「ロックビット」の感染を疑わせる英語のメッセージが印刷されていたのを確認したという。


**ランサムウェアの攻撃によって業務に支障が出てしまった事例です。被害に遭う前に、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：トレーラーの出入りもなくなった名古屋港のコンテナ埠頭

■出典：
https://www.nikkei.com/article/DGXZQOFD053RH0V00C23A7000000/

# 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。