

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9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。

■「マイナポイント第2弾」申請期限迫る 詐欺メールなどに注意

2023年9月26日

- ・最大2万円分のポイントがつく「マイナポイント第2弾」の申請期限が今月末に迫るなか、総務省はポイントを申請させるように見せかけてクレジットカードの番号や個人情報をだまし取ろうとする詐欺メールや偽サイトなどに注意するよう呼びかけています。
- ・具体的にはポイントの申請を促すメールを送りつけて偽サイトに誘導し、クレジットカードの番号や、氏名・生年月日などの個人情報などをだまし取る手口や、総務省や市区町村の職員をかたって、申請のために手数料が必要だとして金をだまし取ろうとする電話などが確認されているということです。
- ・総務省は「少しでも不審に思ったら最寄りの警察署か、『マイナンバー総合フリーダイヤル』の0120-95-0178に相談してほしい」としています。



フィッシングメールを見極めることは困難です。少しでも不審に感じたら本文にあるような機関に相談してみましょう。

■画像：フィッシングサイトの例

■出典：
<https://www3.nhk.or.jp/shutoken-news/20230926/1000097546.html>

■ 警察庁とNISC、中国のサイバー攻撃グループ「BlackTech」に 米関係機関と共同で注意喚起

2023年9月29日

・警察庁と内閣サイバーセキュリティセンター（NISC）は9月27日、中国を背景とするサイバー攻撃グループ「BlackTech」（ブラックテック）に関する注意喚起を発表した。

・同注意喚起では、リスク低減の対処例として、次のことを挙げている。

- セキュリティパッチ管理の適切な実施
- 端末の保護（エンドポイント・プロテクションなど）
- ソフトウェアなどの適切な管理・運用、ネットワーク・セグメンテーション
- 本人認証の強化、多要素認証の実装
- アカウントなどの権限の適切な管理・運用

・あわせて、ネットワークの不審な通信を検知した際は、すみやかに所管省庁、警察、セキュリティ関係機関などに情報提供してほしいとしている。

サイバー攻撃が増加する中で、いつ被害に遭うかは分かりません。突然の攻撃にも対処できるよう、常にセキュリティ対策を万全な状態に保ちましょう。



■画像：警察庁ホームページ

■出典：
<https://internet.watch.impress.co.jp/docs/news/1535484.html>

■ マツダ、個人情報 10 万件超流出か サーバーに不正アクセス

2023年9月15日

- ・マツダは15日、社内システムのサーバーに外部から不正アクセスを受け、グループ会社を含む社員や取引先の担当者の氏名、電話番号など計10万4732件の個人情報が流出した可能性があるとして発表した。悪用は確認されておらず、顧客情報は含まれていないという。
- ・マツダは「関係者の皆さまに多大な迷惑と心配をかけ、深くおわびする」とコメントした。警察や政府の個人情報保護委員会に報告し、再発防止に取り組むとしている。
- ・7月24日に不正アクセスを検知し、すぐにサーバーをネットワークから切り離した。専門家の調査で、アカウント情報を管理するシステムに不正アクセスの形跡が確認され、個人情報が流出した可能性が判明した。



これは不正アクセスによって10万件もの個人情報が流出してしまった事例です。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：マツダのロゴ

■ 出典：<https://www.sankei.com/article/20230915-4F27MNCBONK3XDUBXLXBL2OUQA/photo/T634X2DWAVMZPFC5QKVDJO F771/>

■ サイバー攻撃「ランサムウェア」被害企業の9割 “業務に影響”

2023年9月21日

- データを勝手に暗号化して、身代金を要求する「ランサムウェア」と呼ばれるサイバー攻撃の被害が、ことしも全国で相次いでいて、被害に遭った企業などのうち9割以上で、業務への影響が出ていたことが警察庁の調べで分かりました。新たな手口も確認されていて、警察は、セキュリティーの強化を呼びかけています。
- 「ランサムウェア」は、企業などのコンピューターに侵入してデータを勝手に暗号化し、復元と引き換えに金銭や暗号資産を要求するサイバー攻撃の手口で、警察庁によりますと、ことし6月までの半年間の被害は全国で103件確認され、去年の同じ時期の114件からわずかに減ったものの、高い水準で推移しています。
- 最近では、データを暗号化せずに盗み取り「公開されたくなければ対価を支払え」と要求する「ノーウェアランサム」と呼ばれる新たな手口も確認されているということで、警察は企業などに対し、セキュリティーの強化を呼びかけています。



近年、ランサムウェア被害は未だに多く、ランサムウェアの新たな手口も確認されています。セキュリティー対策の強化に努めましょう。

■画像：NHK NEWS

■出典：
<https://www3.nhk.or.jp/news/html/20230921/k10014202091000.html>

■ PCウイルス感染で1212人の個人情報流出の可能性 三重県聴覚障害者支援センター

2023年9月29日

- 三重県聴覚障害者支援センターで、利用者など1200人余りの個人情報流出した可能性があることがわかりました。県によりますと今月12日、三重県聴覚障害者支援センターの女性職員がパソコンを使っていたところ、「トロイの木馬」と書かれたセキュリティ警告が表示されました。
- 警告に書かれた連絡先に電話し、オペレーターの指示に従い操作したところ、職員が気づかないまま遠隔操作が可能なソフトウェアがインストールされました。そして22日にパソコンが遠隔で操作されていることに気づき、ウイルスに感染していることがわかりました。
- 聴覚障害者や手話通訳者など1212人の個人情報流出した可能性があり、このうち399人は振込口座の情報が、58人はマイナンバーの情報が含まれているということです。



いつこのような悪質なソフトウェアの被害に遭うかは分かりません。少しでも怪しいと感じたら、周りの人に相談しましょう。

■ 画像：三重県聴覚障害者支援センター（名古屋テレビ）

■ 出典：
<https://news.yahoo.co.jp/articles/9a9804c769ee5bc2d724fb0702dd46fde3d22421>

■ 攻撃者を疑似体験し、セキュリティの重要性を学ぶボードゲーム - IPA

2023年9月15日

- ・情報処理推進機構（IPA）は、サイバー攻撃者の立場を疑似体験し、セキュリティ対策の重要性を学ぶことができるボードゲーム「Cyber Attacker Placement」を公開した。
- ・同作品は、サイバー攻撃の種類や多様性、脆弱性を放置することの危険性などをゲームを通じて学ぶことができるセキュリティを題材としたボードゲーム。教育性だけでなく、ゲーム性にも注力しつつ、制作したという。
- ・プレイヤーはハッカーグループに所属するハッカーの一員となり、組織幹部の席をめぐるほかの他メンバーと争うストーリーで、部下を動かしてターゲットに攻撃をしかけつつ、もっとも早くポイントを獲得して幹部になったプレイヤーが勝利となる。
マニュアルなどゲームで用いるツールはウェブサイトより無料でダウンロードできる。



これはゲーム感覚でセキュリティ対策の重要性を知ることができるボードゲームです。無料でダウンロードできるのでぜひ一度遊んでみてはいかがでしょうか？

■ 画像：ハッカー視点の獲得を目指したボードゲーム「Cyber Attacker Placement」

■ 出典：<https://www.security-next.com/149497>

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。

