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。

■不正送金30億円！ 過去最多被害額を半年で超える勢い～金融庁発表

2023年10月30日

・金融庁は、メールやSMS、メッセージングツールなどを用いたフィッシングと見られる手口によってネットバンキングのアカウント情報を盗み取り、預金を不正送金する事案が多発しているとして注意喚起を発表しました。

・銀行を騙ったフィッシングメール／SMSなどでネットバンキング利用者を偽のWebサイトに誘導し、IDやパスワードなどを入力させることでアカウントを乗っ取り、口座内の預金を不正送金するという手口が使われているようです。

・発表によれば、被害額は2022年夏に急増し、その後一旦落ち着いたものの、今年2月以降再び増加。そのまま勢いは止まらず、8月4日時点における上半期の暫定被害額は過去最多の約30億円とのこと。上半期のみでこれまでの最多被害額約30億7000万円（2015年）に達している状況です。

最近は特にフィッシングメールによる手口が増加しています。フィッシングメールが届いた際は、あわてず、フィッシング対策協議会に報告しましょう。

■画像：2023年上半期までの不正送金発生状況（金融庁の発表より）

■出典：https://ascii.jp/elem/000/004/165/4165791/

■MyJCBをかたるフィッシング、件名「JCBカード株式会社からのご連絡 カードのご利用に関する重要な情報」などの不審なメールに注意

2023年10月25日

・MyJCBをかたるフィッシングの報告が増加しているとして、フィッシング対策協議会が情報を公開した。誘導先のフィッシングサイトは10月23日15時時点で稼働中であるため、引き続き注意が必要だ。

・誘導先のフィッシングサイトは、MyJCBのログイン画面を装っており、IDとパスワードの入力を求められる。

・フィッシング対策協議会は、「フィッシングサイトは本物のサイトの画面をコピーして作成されることが多く、見分けることは非常に困難」と指摘する。その上で、日頃から、サービスへログインする際はメールやSMSのリンクを利用するのでなく、公式アプリやウェブブラウザーのブックマークからアクセスするよう、注意を促している。

■画像：誘導先のフィッシングサイトの画面

■出典：
https://internet.watch.impress.co.jp/docs/news/1541470.html

フィッシングサイトを見極めるのは困難です。普段からログインの際は公式アプリやブックマークを利用するように心がけましょう。

■ライトオンのサーバーに不正アクセス。ランサムウェアによる被害。個人情報などの流出は現時点で確認されず

2023年10月27日

・ライトオンが、10月21日に業務上使用するサーバーに対してランサムウェアによる第三者からの外部攻撃を受けたことを発表した。

・サーバーに対しての外部攻撃は、同社のネットワークに対して不正にアクセスした上で、ランサムウェアを実行することにより、データの暗号化を行ったものと考えられている。同社は直ちに対策本部を設置のうえ、警察への通報および関係機関への相談を行いつつ、外部専門家を交えて原因の特定、被害情報の確認、情報流出の有無などの調査を継続しているという。外部攻撃が確認されてからは被害の拡大防止措置を実施し、外部専門家と連携をとり新たなセキュリティ対策を講じた上で、システムの保護と復旧に向けての作業に取り組んでいるとした。

・同社は今後も引き続き、警察および関係機関への相談を行いつつ、外部専門家を交えて原因や経路などの攻撃の詳細、情報流出の有無などの調査に全力で取り組んでいくとコメントした。

近年、不正アクセスを受けて被害に遭う事例が増えています。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：Right-on

■出典：
https://news.yahoo.co.jp/articles/531a5b12aa8873917aa58569d756e59dc698cfbf

■東京海上で顧客情報漏洩　生損保43社の契約情報も不正アクセス可能だったがその通知が遅れ、各社から怒りの声

2023年10月30日

・今年7月、同社の保険代理店で情報漏洩が発覚した。顧客情報を扱う代理店システムで、東京海上側が参照範囲の設定をミス。一部の代理店(勤務型代理店)が、本来閲覧できないはずの情報にアクセスできる状態になっていたという。

・一部代理店による不正アクセスの件数は2000～3000件程度とみられ、規模としてはさほど大きくなかったようだ。ただ悩ましかったのが、不正アクセスが可能になっていた10万件以上の顧客情報に、東京海上グループ以外のほかの生損保43社の契約情報も含まれていたことだった。

・東京海上は情報漏洩が発覚した7月に、監督官庁である金融庁へ不祥事案として報告した。しかし、生損保各社からは「通知を受けたのは9月に入ってから。調査をしていたのはわかるが、あまりにも遅すぎる」と対応の遅さに怒りの声が上がっている。

■画像：東京海上

■出典：
https://finance.yahoo.co.jp/news/detail/803290a1b91c32f2659cbadfcfc196a49902b3e9

**不正アクセスが発覚した後の対応が遅れてしまった事例です。
いつでも対処できるように万全の体制を保ちましょう。**

■CEOの7割「サイバー攻撃への対応力に懸念」セキュリティ意識と実態にギャップ　アクセンチュア調査

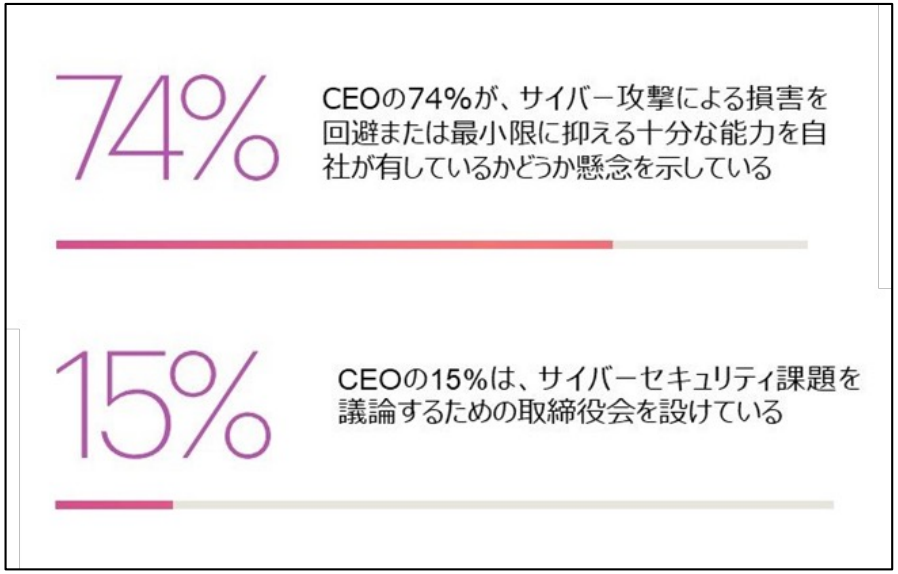
2023年10月30日

・企業のCEOのうち7割超は、自社のサイバーセキュリティに懸念を持っている――アクセンチュアは10月27日、こんな調査結果を発表した。サイバー攻撃による損害を回避するか最小限に抑えるために、自社が十分な能力を有しているかCEO1000人に聞いたところ、74%が対応力に懸念があると答えたという。

・一方で「サイバーセキュリティの課題を討議する取締役会の有無」を聞いたところ、実施しているのは15%だった。CEOによるサイバーセキュリティへの関与を聞いたところ、90%が「セキュリティは経営ではなく技術的な問題であり、CEOではなくCIOやCISOの職掌範囲」と答えた。

・アクセンチュアは一連の回答に対し「絶えず進化し、終わりの見えない脅威の状況は、サイバー攻撃がビジネスに与える影響に対するCEOの意識の高まりと、それを軽減する自信のなさの間に大きなギャップを生み出している」と指摘した。

セキュリティ対策の重要性は高くなってきています。対策が必要と感じる場合は、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：アクセンチュアの調査結果

■出典：
https://www.itmedia.co.jp/news/articles/2310/30/news160.html

■サイバー攻撃への対策を考えるセミナー　名古屋

2023年10月3日

・相次いでいる企業を狙ったサイバー攻撃への対策について理解を深めてもらおうと、中部経済連合会が、企業の経営者などを対象にしたセミナーを１０月３日、名古屋市で開きました。

・セミナーでは、独立行政法人ＩＰＡ＝情報処理推進機構の専門家が講師を務め、最近では企業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を要求する「ランサムウェア」の手口が大きな脅威になっていると指摘しました。

・続いて、東海地方にある自動車部品メーカーや、電力会社の情報セキュリティーの担当者も参加したトークセッションが開かれ、最低限やるべき対策として、社内のパソコンなどサイバー攻撃のリスクがある端末の管理を徹底することや、仮に攻撃を受けても被害を最小化できるよう、重要なデータのアクセスはあらかじめ制限しておくことなどをあげていました。

セキュリティ対策には従業員の教育も不可欠です。少しずつ知識を身に着けサイバーセキュリティをより強固にしていきましょう。

■画像：サイバー攻撃への対策を考えるセミナー（NHK NEWS）

■出典：https://www3.nhk.or.jp/tokai-news/20231003/3000032046.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。