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4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。

■セガ子会社で、約4740件の個人情報漏えいの可能性 メールシステムに不正アクセス

2024年4月25日

・セガサミーホールディングス傘下で、玩具事業などを手掛けるセガフェイブ（東京都品川区）は4月24日、メールシステムが不正アクセスを受け、個人情報が外部に漏えいした可能性があると発表した。

・セガ フェイブのメールシステムのセキュリティを管理するセガサミーホールディングス（東京都品川区）が、4月4日に不正アクセスを検知した。不正アクセスを受けたアカウントが保有する情報に、取引先や従業員などの個人情報が含まれていることを4月9日に確認し、個人情報保護委員会へ報告したという。

・セガ フェイブは、対策として4月22日までに同社が保有する全てのアカウントのセキュリティを強化したといい、引き続き情報を精査する予定。あわせて、今回の件に関連する人に向けて相談窓口を設置する。

■画像：セガ フェイブ、不正アクセスによる個人情報漏えいの可能性に関するお詫びとお知らせ

■出典：
https://www.itmedia.co.jp/news/articles/2404/25/news178.html

企業のセキュリティー強化に伴い、攻撃者の手口も変化しています。被害を未然に防ぐ対策だけでなく、発生後即座に復旧するための対策も考えておく必要がありそうです。

■ ＨＯＹＡシステム障害おおむね復旧、眼鏡レンズ供給回復へ…サイバー攻撃が原因

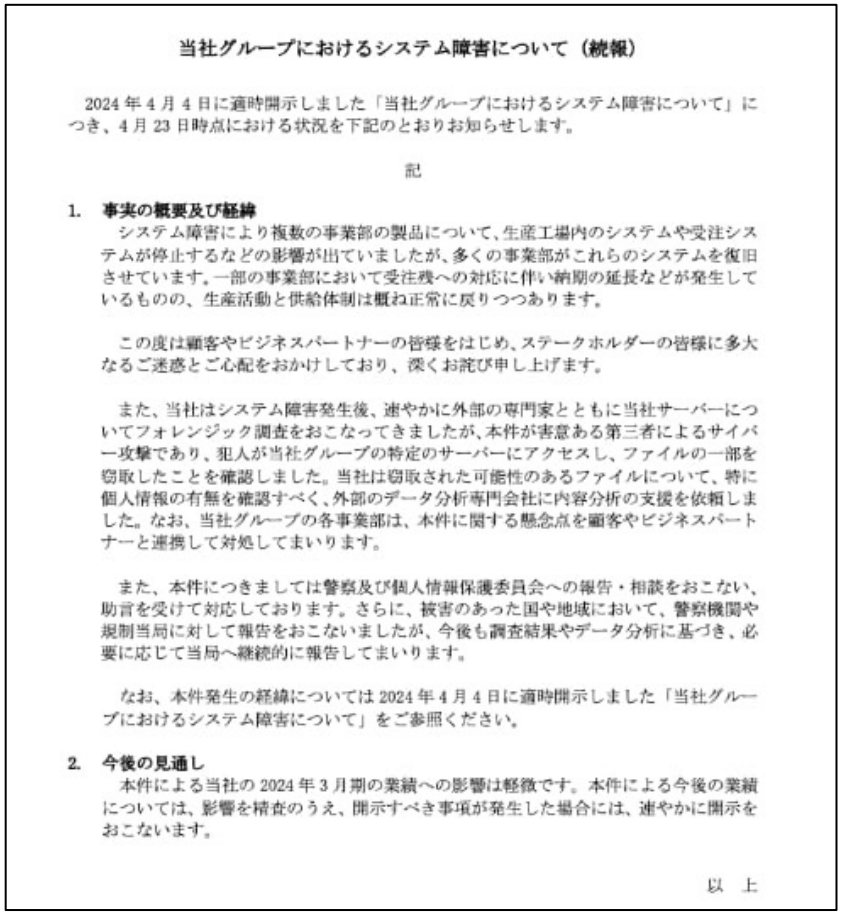
2024年4月23日

・光学機器大手ＨＯＹＡは２３日、３月末に発生したシステム障害がおおむね復旧したと発表した。ＨＯＹＡは眼鏡用レンズの国内市場でトップシェアを誇り、眼鏡店で販売停止などの影響が出ていた。

・システム障害は３月３０日に国内外の事業所で発覚し、工場や受注のシステムが停止した。眼鏡レンズの受注や出荷が滞り、ＪＩＮＳやＺｏｆｆなどでは、一部商品の販売を停止した。現在、多くの事業部でシステムが復旧し、レンズの供給は回復しつつあるが、一部残る納期の遅延について解消する時期は「明言できない」（広報）という。

・調査の結果、システム障害の原因は第三者によるサイバー攻撃だった。また、特定のサーバーに不正アクセスされ、ファイルの一部を盗み取られたこともわかった。盗まれたファイルに個人情報が含まれていないか、確認を続けている。

サイバー攻撃では、被害をうけた会社だけでなく、関連している多くの会社が影響を受けます。自社のセキュリティ対策を常に確認しておきましょう。



当社グループにおけるシステム障害について（続報）

2024年4月4日に適時開示しました「当社グループにおけるシステム障害について」につき、4月23日時点における状況を下記のとおりお知らせします。

記

1. 事実の概要及び経緯

システム障害により複数の事業部の製品について、生産工場内のシステムや受注システムが停止するなどの影響が出ていましたが、多くの事業部がこれらのシステムを復旧させています。一部の事業部において受注残への対応に伴い納期の延長などが発生しているものの、生産活動と供給体制は概ね正常に戻りつつあります。

この度は顧客やビジネスパートナーの皆様をはじめ、ステークホルダーの皆様に多大なるご迷惑とご心配をおかけしており、深くお詫び申し上げます。

また、当社はシステム障害発生後、速やかに外部の専門家とともに当社サーバーについてフォレンジック調査をおこなってきましたが、本件が害意ある第三者によるサイバー攻撃であり、犯人が当社グループの特定のサーバーにアクセスし、ファイルの一部を窃取したことを確認しました。当社は窃取された可能性のあるファイルについて、特に個人情報の有無を確認すべく、外部のデータ分析専門会社に内容分析の支援を依頼しました。なお、当社グループの各事業部は、本件に関する懸念点を顧客やビジネスパートナーと連携して対処してまいります。

また、本件につきましては警察及び個人情報保護委員会への報告・相談をおこない、助言を受けて対応しております。さらに、被害のあった国や地域において、警察機関や規制当局に対して報告をおこないましたが、今後も調査結果やデータ分析に基づき、必要に応じて当局へ継続的に報告してまいります。

なお、本件発生の経緯については2024年4月4日に適時開示しました「当社グループにおけるシステム障害について」をご参照ください。

2. 今後の見通し

本件による当社の2024年3月期の業績への影響は軽微です。本件による今後の業績については、影響を精査のうえ、開示すべき事項が発生した場合には、速やかに開示をおこないます。

以　上

■画像：HOYAの発表（全文）

■出典：https://www.yomiuri.co.jp/economy/20240423-OYT1T50137/

■「サポート詐欺」で情報漏えいか　雇用支援の独立行政法人が発表、委託プランナーのPCが遠隔操作状態に

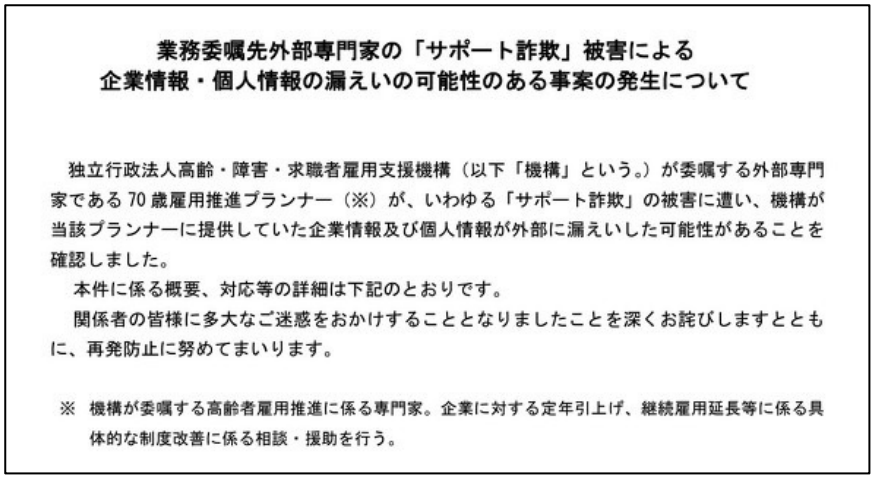
2024年4月30日

・高齢者、障害者などに対して総合的な雇用支援を実施する高齢・障害・求職者雇用支援機構（JEED）は4月26日、591件の企業、個人情報が漏えいした可能性があると発表した。JEEDが業務を委嘱する専門家がサポート詐欺に遭ったためとしている。

・JEEDによると、3月11日に自身のPCを利用していた当該プランナーがサポート詐欺に遭遇。偽のセキュリティ警告に記載されたサポート窓口に電話し、指示に従った結果、約3時間にわたってPCが第三者にリモート接続されていた状態だったという。当該プランナーはJEEDが求めるセキュリティ対策を講じていなかった。

・ JEEDは2023年度中に全てのプランナーなどに対して、求める情報セキュリティ対策が順守されているか確認を行い、改めて注意喚起と研修を実施した。24年度以降も同様の確認や研修を実施することで、再発防止に努めるとしている。

社内のセキュリティ強化には従業員への教育も欠かせません。情報セキュリティについて共通認識をもっておきましょう。



業務委嘱先外部専門家の「サポート詐欺」被害による
企業情報・個人情報の漏えいの可能性のある事案の発生について

独立行政法人高齢・障害・求職者雇用支援機構（以下「機構」という。）が委嘱する外部専門家である 70 歳雇用推進プランナー（※）が、いわゆる「サポート詐欺」の被害に遭い、機構が当該プランナーに提供していた企業情報及び個人情報が外部に漏えいした可能性があることを確認しました。

本件に係る概要、対応等の詳細は下記のとおりです。

関係者の皆様に多大なご迷惑をおかけすることとなりましたことを深くお詫びしますとともに、再発防止に努めてまいります。

※ 機構が委嘱する高齢者雇用推進に係る専門家。企業に対する定年引上げ、継続雇用延長等に係る具体的な制度改善に係る相談・援助を行う。

■画像：JEEDが保有する591件の企業、個人情報が漏えいした可能性がある
■出典：https://www.itmedia.co.jp/news/articles/2404/30/news159.html

■東京ガスをかたるフィッシング、件名「【東京ガス】ご請求料金確定のお知らせ」などの不審なメールに注意

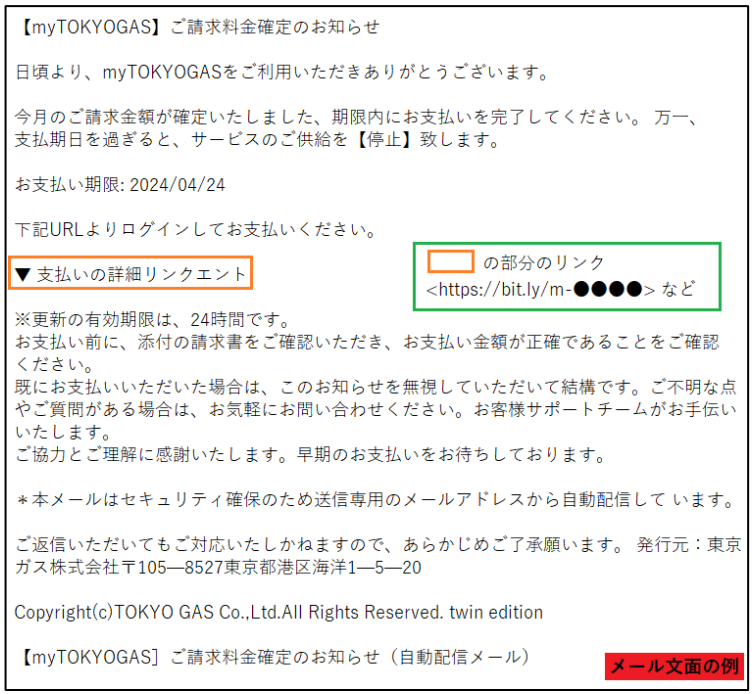
2024年4月25日

・東京ガスをかたるフィッシングの報告を受けたとして、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4月24日9時時点で稼働中であり、引き続き注意が必要だ。

・メール本文は、ガス料金が未払いのため支払うよう、リンクへのアクセスを促している。誘導先のフィッシングサイトは、東京電力の会員向けサービス「myTOKYOGAS」を装っており、クレジットカード情報、携帯電話番号やメールアドレスの入力を求められる。

・東京ガスは、悪質な訪問や電話とともにフィッシングの注意喚起を実施しており、不審と思われるSMSやメールが届いた場合、開封せずに削除するよう呼びかけている。

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。


【myTOKYOGAS】ご請求料金確定のお知らせ

日頃より、myTOKYOGASをご利用いただきありがとうございます。

今月のご請求金額が確定いたしました、期限内にお支払いを完了してください。 万一、支払期日を過ぎると、サービスのご供給を【停止】致します。

お支払い期限: 2024/04/24

下記URLよりログインしてお支払いください。

▼ 支払いの詳細リンクエント

□ の部分のリンク
<https://bit.ly/m-●●●●> など

※更新の有効期限は、24時間です。
お支払い前に、添付の請求書をご確認いただき、お支払い金額が正確であることをご確認ください。
既にお支払いいただいた場合は、このお知らせを無視していただいて結構です。ご不明な点やご質問がある場合は、お気軽にお問い合わせください。お客様サポートチームがお手伝いいたします。
ご協力とご理解に感謝いたします。早期のお支払いをお待ちしております。

＊本メールはセキュリティ確保のため送信専用のメールアドレスから自動配信して います。

ご返信いただいてもご対応いたしかねますので、あらかじめご了承願います。 発行元：東京ガス株式会社〒105―8527東京都港区海洋1―5―20

Copyright(c)TOKYO GAS Co.,Ltd.All Rights Reserved. twin edition

【myTOKYOGAS】ご請求料金確定のお知らせ（自動配信メール）

メール文面の例

■画像：メール文面の例（フィッシング対策協議会の緊急情報より）

■出典：
https://internet.watch.impress.co.jp/docs/news/1587070.html#20240424tokyogas02_l.png

■復旧失敗確率 3 分の 2、ランサムウェア身代金支払い ～ JIPDEC、ITR 調査

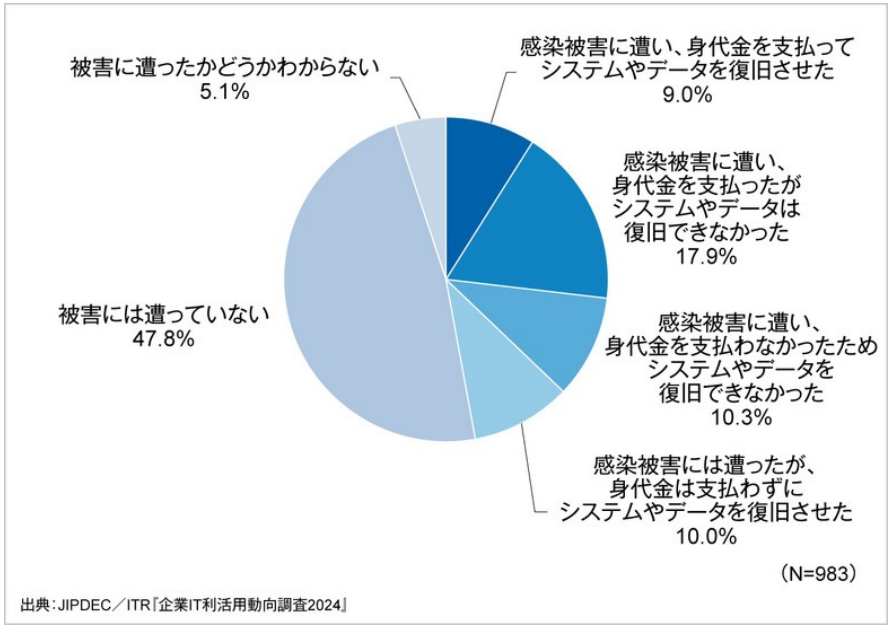
2024年4月5日

・一般財団法人日本情報経済社会推進協会（JIPDEC）と株式会社アイ・ティ・アール（ITR）は3月15日、「企業IT利活用動向調査2024」の結果を発表した。

・同調査で、ランサムウェアの感染被害の経験について尋ねたところ、感染経験があったのは47.1%であった。
このうち「感染被害に遭い、身代金を支払ってシステムやデータを復旧させた」が9.0%、「感染被害に遭い、身代金を支払ったがシステムやデータは復旧できなかった」が17.9%であり、身代金を支払った企業の3分の2は復旧できなかったことが判明した。

・ITRのシニア・アナリスト 入谷光浩氏は「業種や規模を問わず、どの企業もランサムウェア攻撃を受ける可能性があり、適切なサイバーセキュリティ対策が不可欠となります。」とコメントしている。

ランサムウェアによる攻撃は、すべての企業が受ける可能性があります。攻撃を受けても感染を未然に防げるよう、セキュリティの見直しを行いましょう。



■画像：企業IT利活用動向調査2024

■出典： https://scan.netsecurity.ne.jp/article/2024/04/05/50823.html

■企業のサイバー対応力、5段階で格付け　経産省案を提示

2024年4月5日

・経済産業省は5日、企業のサイバー対策を5段階で格付けする制度を2025年度に始める政策案を公表した。背景としてサプライチェーンを狙うサイバー攻撃が増えたことがある。

・5段階のうちレベル1～3は、ソフトウエアの定期更新や情報の管理体制の整備など、最低限の対策を求めており、企業が自社の対策状況を確認し、レベルを自ら宣言する形としている。

・レベル4～5は供給網で重要な役割を担う企業向けで、サイバー攻撃時の早期復旧策を設けているかといった、複数の要素が基準になる見込みである。外部の認証団体から対応状況に関する第三者認証を受ける必要がある。

・格付けを通じて企業はセキュリティーレベルの高い取引先を選びやすくなり、供給網全体のサイバー対策の強化につながる。経産省は格付けの取得を、公共調達や補助金支給などの要件にする方針だ。

■画像：経済産業省＝東京都千代田区

■出典：
https://www.nikkei.com/article/DGXZQOUA0586S0V00C24A4000000/

セキュリティ対策を講じることは当然になっており、今後はより質の高い対策を行うことが求められると考えられます。自社での対策を強化していきましょう。

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。