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3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。

■富士通、個人情報流出の恐れ - 複数のPCからマルウェアを検出

2024年3月19日

・富士通は3月15日、「個人情報を含む情報漏洩のおそれについて：富士通」において、社内の複数の業務PCからマルウェアを検出したと発表した。マルウェアにより、個人情報や顧客に関連する情報を不正に取得できる状態だったと説明している。

・富士通はマルウェアの存在の確認後、感染した業務PCを速やかに切り離し、その他の業務パソコンの監視を強化するなどの対策を講じたという。発表時点では、発見日時、侵害経路、マルウェアの詳細、被害規模とその内容などは、調査中として明らかにしていない。

・富士通は2021年に、機密データへの不正アクセスを経験しており、全社でセキュリティ対策強化と管理監督の徹底に取り組むとしていた。

FUJITSU

Japan 国・地域を変更 検索

産業別 サービス Fujitsu Uvance サステナビリティ テクノロジー 採用 企業情報

お知らせ > 個人情報を含む情報漏洩のおそれについて

シェア

お知らせ

2024年3月15日
富士通株式会社

個人情報を含む情報漏洩のおそれについて

当社の複数の業務パソコンでマルウェアの存在を確認し、社内調査の結果、個人情報やお客様に関する情報を含むファイルを不正に持ち出すことができる状態になっていたことが判明しました。

マルウェアの存在を確認後、速やかに影響のあった業務パソコンの切り離しを行うとともに、その他の業務パソコンの監視を強化する等の対策を講じております。また、マルウェアの侵入経緯や情報流出の有無等については現在も継続して調査を進めております。

なお、対象となる個人の方々やお客様については個別に報告を実施するとともに、個人情報が流出した可能性を想定し、個人情報保護委員会へも報告しております。現時点で個人情報やお客様に関する情報が悪用されたという報告は受けておりません。

関係者の皆様に多大なるご心配、ご迷惑をおかけしておりますことを、深くお詫び申し上げます。

以上

セキュリティ対策はどれだけ講じても、十分だということはありません。サイバー攻撃を未然に防げるよう、常に対策を強化していきましょう。

■画像：個人情報を含む情報漏洩のおそれについて：富士通

■出典：https://news.mynavi.jp/techplus/article/20240319-2909914/

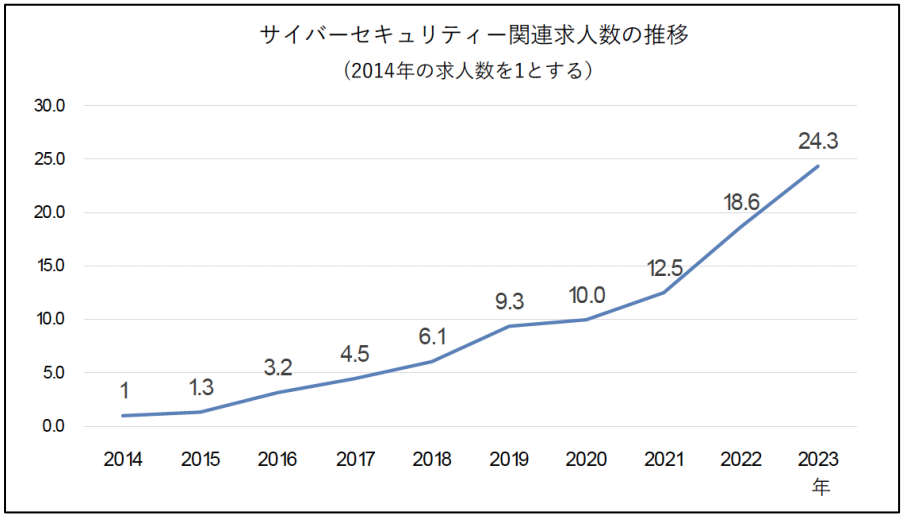
■リクルートがサイバーセキュリティーに関する求人と転職の動向を報告 -人材のニーズに転職者数が追いついていない現状

2024年3月15日

・株式会社リクルートは3月15日、『リクルートエージェント』におけるサイバーセキュリティーに関する求人と転職の動向について報告を行った。

・サイバーセキュリティー関連の求人数はサイバー攻撃への懸念の高まりから右肩上がりで推移している。特に2018年から2019年、2020年以降で求人の伸びが大きくなっており、背景として、オリンピックやコロナの影響が考えられている。

・転職者数の伸びは2014年比で3.62倍だった。近年は急増しているものの、求人数の急激な伸び幅と比べると小さく、企業のサイバーセキュリティー関連人材へのニーズに、転職者数が追いついていない状況が表れている。



セキュリティー強化には、スキルや知識をもった人材の確保が重要です。新たに人を雇うのだけではなく、従業員への教育も有効な手段だと考えられます。

■画像：サイバーセキュリティー関連求人の推移

■出典：
https://www.recruit.co.jp/newsroom/pressrelease/assets/20240315_work_01.pdf

BASIC Confertas Office

■「フィッシング」の手口などによる不正送金の被害額が過去最多に

2024年3月14日

・警視庁は3月14日、「令和５年におけるサイバー空間をめぐる脅威の情勢等について」を公表した。資料の中で、サイバー空間の脅威の情勢を示す指標、事例を示すとともに、安全・安心の確保に向けた警察の主な施策等を取りまとめている。

・主にフィッシングによるとみられるインターネットバンキングでの不正送金被害額は、去年1年間で約87億円にのぼり、過去最多となった。また、日本クレジット協会によると、去年1月から9月までのクレジットカードの不正利用の被害額は約400億円で、これも過去最多となった。

・警察庁は極めて深刻な情勢だとして、官民連携によるセキュリティーを強化や、不正な金の流れの監視の強化など対策を進めている。

サイバー攻撃の手口は日々更新されており、それに応じてセキュリティ対策の見直しが必要です。具体的にどのような事例が起こっているか知っておくことも重要だと考えられます。

■画像：警視庁　ホームページ

■出典：
https://news.yahoo.co.jp/articles/0b9153aa8a4b586c3cd952a9bc133d7fe879c848

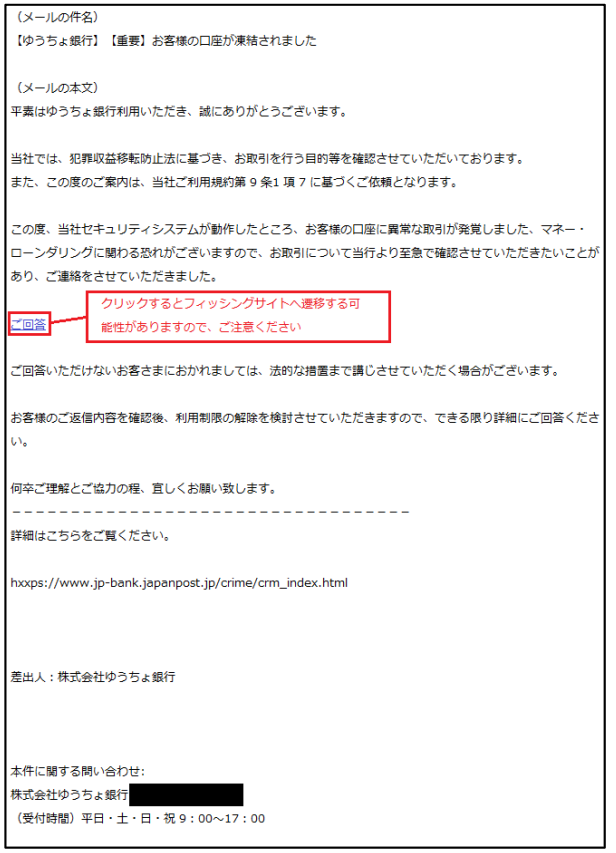
■ゆうちょ銀行がフィッシング詐欺に注意喚起、アプリの利用など推奨

2024年3月28日

・フィッシング対策協議会は、ゆうちょ銀行を騙ったフィッシング詐欺が報告されていると発表した。

・これは、“あなたの口座がセキュリティシステムに引っ掛かったので利用制限した。至急確認したいので回答せよ”という主旨のメールを送りつけて偽Webサイトに誘導し、アカウントやキャッシュカードにまつわる情報を入力させて盗み取るというもの。

・ゆうちょ銀行は、このような偽メールやSMSにより誘導されたサイトに、お客さま番号・ログインパスワード・カナ氏名・電話番号・生年月日・メールアドレス・キャッシュカード暗証番号等の情報を絶対に入力しないよう呼びかけを行っている。



（メールの件名）
【ゆうちょ銀行】【重要】お客様の口座が凍結されました

（メールの本文）
平素はゆうちょ銀行利用いただき、誠にありがとうございます。

当社では、犯罪収益移転防止法に基づき、お取引を行う目的等を確認させていただいております。
また、この度のご案内は、当社ご利用規約第９条1 項７に基づくご依頼となります。

この度、当社セキュリティシステムが動作したところ、お客様の口座に異常な取引が発覚しました、マネー・ローンダリングに関わる恐れがございますので、お取引について当行より至急で確認させていただきたいことがあり、ご連絡をさせていただきました。

ご回答

クリックするとフィッシングサイトへ遷移する可能性がありますので、ご注意ください

ご回答いただけないお客さまにおかれましては、法的な措置まで講じさせていただく場合がございます。

お客様のご返信内容を確認後、利用制限の解除を検討させていただきますので、できる限り詳細にご回答ください。

何卒ご理解とご協力の程、宜しくお願い致します。

詳細はこちらをご覧ください。

hxxps://www.jp-bank.japanpost.jp/crime/crm_index.html

差出人：株式会社ゆうちょ銀行

本件に関する問い合わせ:
株式会社ゆうちょ銀行[redacted]
（受付時間）平日・土・日・祝９：00～17：00

■画像：ゆうちょ銀行を装うフィッシングサイト画面の一部

■出典：https://ascii.jp/elem/000/004/191/4191164/

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。

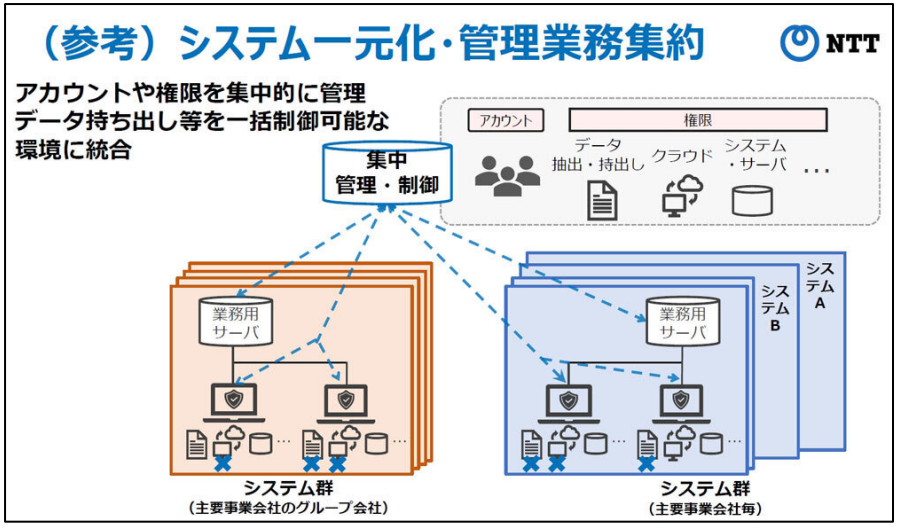
■NTT、内部不正などによる情報漏えいの対策を発表 --総費用は約300億円

2024年3月8日

・　NTT（持株会社）は3月8日、2023年にNTT西日本グループ企業の業務委託で発生した内部不正による情報漏えい事件を踏まえて、対策を発表した。約300億円を投じ、「緊急対策」と「本格対策」の2段階で施策を進めていく。

・。緊急対策では、国内グループ各社への説明や、内部不正による情報漏えいを防ぐためなどに設けていた25項目のルールについて、報告が実施された。本格対策では、システム面や技術面のみならず労務、法務、監査なども含む包括的な施策を行うとする。

・NTTグループCISO（最高情報セキュリティ責任者）の横浜信一氏は「持株会社からグループ各社に指示するだけではなく、各社トップがけん引して現場への対策を実行していくことが重要になる」と話した。



セキュリティー対策はシステムや技術によるものだけでなく、労務、法務、監査など様々な視点から考える必要があります。自社の対策を、一度見直してみても良いかもしれません。

■画像：システム面における対策の一例（NTTの報道向け資料より）

■出典： https://japan.zdnet.com/article/35216276/

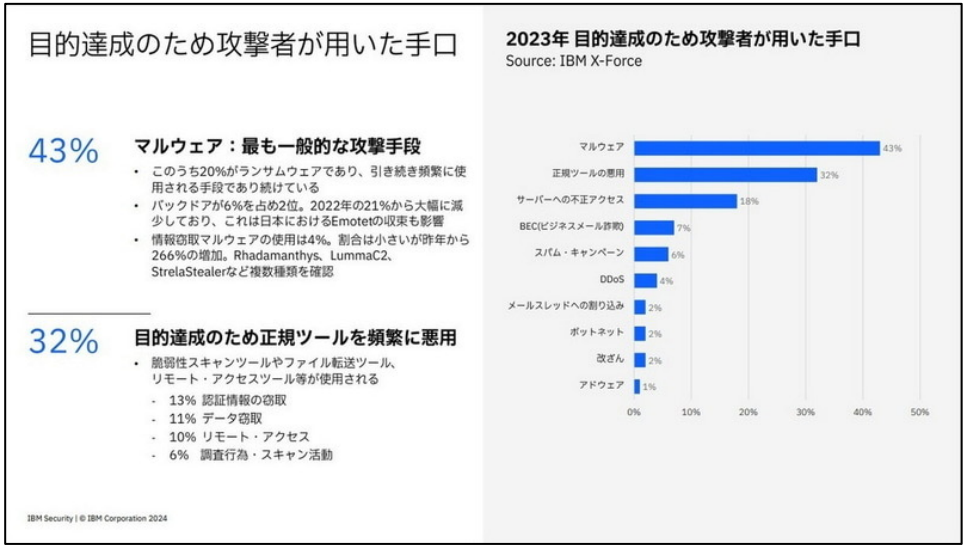
■正規アカウントを悪用するインシデントが増加傾向に――、IBM調査

2024年3月26日

・日本IBM株式会社は25日、「IBM X-Force脅威インテリジェンス・インデックス2024」の日本語版を公開した。同レポートでは、過去1年間に世界で発生したサイバー脅威の事例や攻撃パターンを分析し、傾向や特徴がまとめられている。

・正規アカウントを狙った攻撃活動が活発になっており、正規アカウントを悪用する事例が世界で71%増加しているという。初期侵入経路について、正規アカウントを不正利用するケース事例が昨年の16%から大幅に増加し、30%であった。背景として、ダークウェブで正規アカウントが入手しやすくなったことが考えられている。

・対策について、「インシデントの発生をゼロにすることは困難なため、その確率を低下させ、インシデントが発生しても即座に業務復旧できるよう準備することが重要だ」と述べられている。



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。

■画像：メタバース上で危機対応について学ぶ研修

■出典：
https://news.yahoo.co.jp/articles/00a61419f7e52c957ff75f4bddced5686187e9e3

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。