2024年

Cyber Security NEWS 10月号

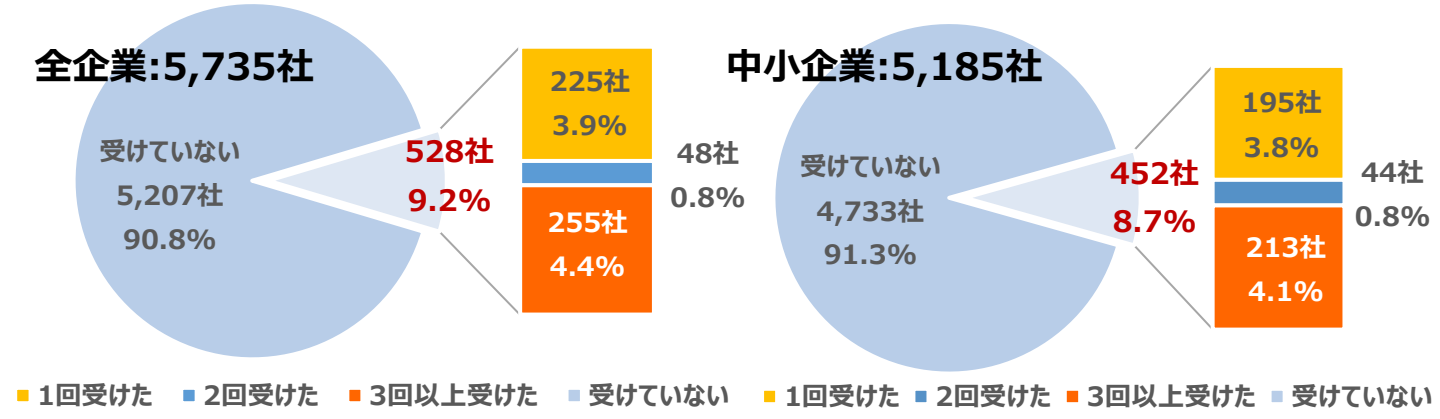
先月の報道を中心に、サイバーセキュリティに関してのニュースを抜粋してお届けしています

2020年以降で「不正アクセスを受けた」企業は約1割

課題は「従業員の意識改革・リテラシー向上」

2024年8月「不正アクセスと情報セキュリティ対策に対するアンケート」調査結果

2020年以降で、不正アクセスを受けたことがありますか？



不正アクセスによる情報流出が頻発しており、他人事では済まされない状況です。東京商工リサーチが2024年8月1日～13日に行った調査結果を発表し、528社が「2020年以降に不正アクセスを受けた」と回答したことが分かりました。このうち、不正アクセスを2回以上受けた企業は303社。規模別に見ると、不正アクセスを1回以上受けた企業の比率は**中小企業で8.7%**、大企業では13.8%だったということです。

参照元　東京商工リサーチ社：https://www.tsr-net.co.jp/data/detail/1198865_1527.html

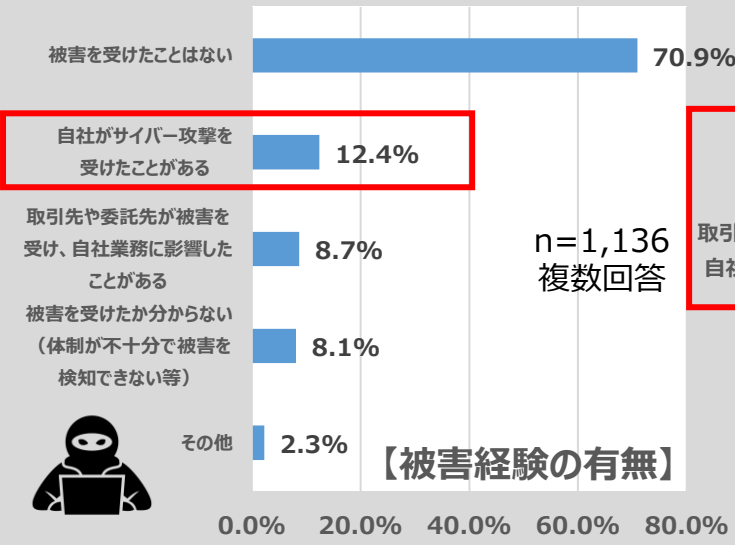
１割でサイバー被害　標的型攻撃メールが多数　東京商工会議所調査

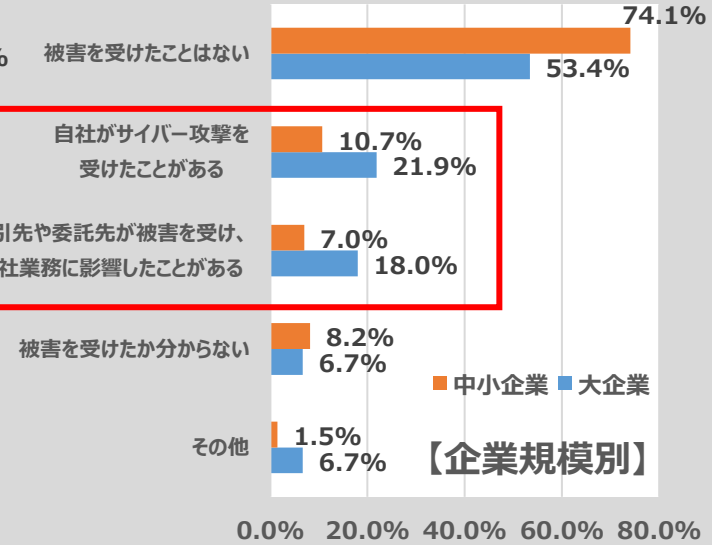
企業の１割がサイバー攻撃の被害を受けた経験がある――こんな実態にあることが、東京商工会議所が会員企業に実施した調査で明らかになっています。サイバー攻撃の被害経験を複数回答で聞いた結果、**12.4%が「受けたことがある」**と答えています。**「取引先や委託先が被害を受け、自社の業務に影響した」は8.7%、「体制が不十分で被害を検知できず、攻撃を受けたかどうか分からない」は8.1%**となっています。

具体的な被害内容（企業の声）

調査期間：2024年6月3日～6月19日
調査対象：東京商工会議所会員企業 17,472件

- **不正アクセスによるHP改ざん・破壊/標的型攻撃メールが複数端末に届いたが、被害なし。**
- **委託先の利用システムが攻撃を受け、２か月程度物流・経理業務が紙でのやり取りとなった。**
- **委託先の不正アクセスにより、メールの一部が第三者に不正転送された。**



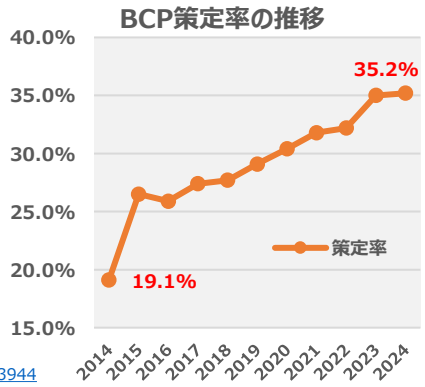


参照元：東京商工会議所 https://www.tokyo-cci.or.jp/page.jsp?id=1203944

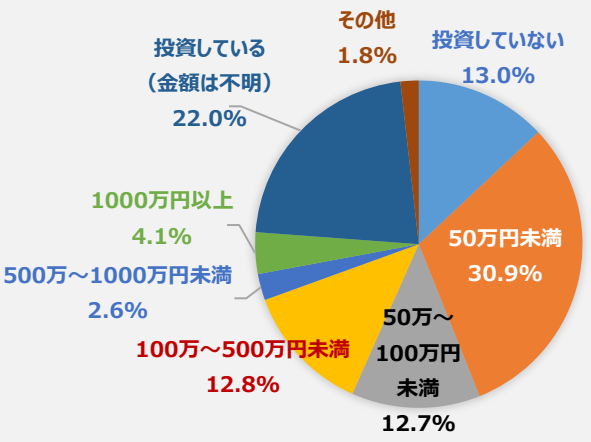
企業情報セキュリティー対策、無投資が1割

水害や地震といった自然災害やサイバー攻撃などに対する企業の備えについて、東京商工会議所が会員企業を調査したところ、**回答企業の1割が情報セキュリティー上のリスクに対し投資していない**ことが明らかになっています。更に、**年間50万円未満と回答した企業も合わせると4割**に上る結果となっています。

調査ではまず事業継続計画（BCP）の策定状況を聞き、**大企業の73･7%、中小企業の28･2%が策定済み**であると回答。全体では35･2%が策定済みで、前回2023年の調査よりも0･2ポイント上昇したということです。



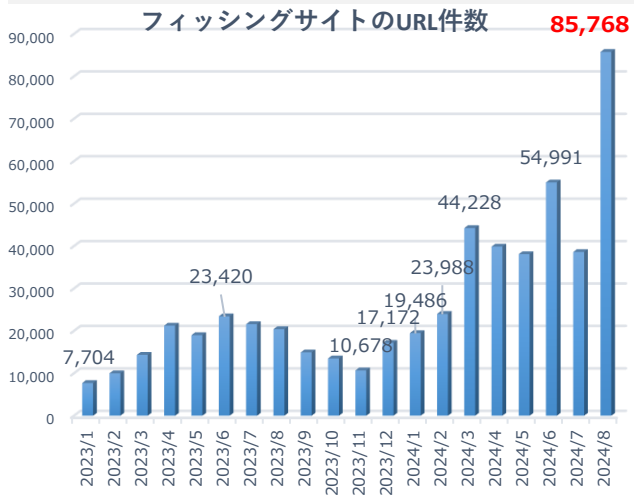
参照元：東京商工会議所
https://www.tokyo-cci.or.jp/page.jsp?id=1203944



フィッシングの悪用URLが前月比2.2倍ー過去最多を更新

フィッシング対策協議会によれば、フィッシングサイトに悪用されたURLは8万5768件。**前月の約2.2倍へと急増**し、**過去最多を更新**しました。1日あたり約2766.7件のURLが見つかっている計算になります。大量にフィッシングメールをばらまく手口において、URLのサブドメインにランダムの文字列を用いるケースが目立ち、その影響でURL数が急増したということです。

悪用URL件数については、今年**8月までの集計結果が既に**過去最悪だった2022年の1年間の件数を**上回り**、急増している状況が顕著に表れていると共に、これまで以上の注意が必要です。



参照元：フィッシング対策協議会
https://www.antiphishing.jp/report/monthly/202408.html

サイバー攻撃者の標的はバックアップ

2024ランサムウェアトレンド　アジア太平洋・日本版エグゼクティブサマリによりますと、「サイバー対策チームがクリアで復元可能なバックアップ」を実現すべく取り組んでいるのと同様に、「サイバー攻撃者も企業が自社のデータを復元できないようにするため」に取り組んでおり、残念なことに、あまりにも多くの攻撃において、攻撃者が相手の防御をすり抜けることに成功しているといいます。
データによると、身代金を支払わずに回復できた組織はわずか16%で、平均では43%のバックアップがサイバー攻撃の影響を受けているとしています。
各府警・県警のセミナーでもバックアップから復元できるかどうか普段からチェックが必要と訴えています。
2024ランサムウェアトレンド アジア太平洋・日本版エグゼクティブサマリ
参照元：https://www.veeam.com/jp/resources/wp-2024-ransomware-trends-executive-summary-apj.html

ランサムウェアの一般的な攻撃手法

- フィッシングや、機器の脆弱性を突くなどの方法で、内部ネットワークに侵入
- 多数の検知機能を回避しながら、ネットワーク経由で範囲を拡大
- ネットワークにあるサーバーや端末から重要と思われる情報を入手
- バックアップデータをまず暗号化（復旧手段を潰す）
- システム全体の暗号化と高額な身代金を要求

委託先を狙った？

自治体の業務を受託する企業や労働組合の業務を受託する企業、物流業務を受託する企業など、国内では数か月の間に相次いでランサムウェア攻撃により、大規模な個人情報の流出被害に遭っています。また、委託元への被害も広がる一方です。こうした被害報告や報道をきっかけに、ランサムウェアに対する警戒が改めて高まっています。

今年上半期のサイバー攻撃を試みた“不審アクセス”は過去最多更新　警察庁

大手出版社が不正アクセスによって36億円の損失を出すなどサイバー犯罪による被害が深刻化するなか、今年上半期の不審なアクセス数が過去最多を更新しています。
警察庁によりますと、今年上半期にサイバー攻撃を試みたとみられる不審なアクセスは1つのIPアドレスに対して一日あたり9,825件でした。
去年の同時期の8,219件を超え、増加の一途をたどっています。
また、銀行などを装ってクレジットカードの番号やパスワードを入手する**「フィッシング」による被害は63万3089件**に上り、それらに関わる不正送金による**被害額は24億4000万円**となっています。

カード会社から不正利用の確認の連絡が来た そこにあったQRコードに罠が！

「不正利用を監視している」という連絡そのものが罠だった

フィッシング対策協議会は、「メールに記載したQRコードから誘導する」フィッシングの報告が増えているとして、注意を呼びかけています。
それによれば、メールの本文は、カードの利用確認をするために本人確認が必要などとして、記載されたQRコードをスキャンしてサイトへアクセスするよう促す文面になっているといいます。
しかし、そこから誘導された先はフィッシングサイトになっていて、三井住友カードの会員向けウェブサイトが装われ、IDとパスワードの入力を求められるという。
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です。フィッシング対策協議会に寄せられた報告は三井住友カードをかたっていますが、別の企業・団体をかたる、これ以外の件名も使われているなどの可能性もあり、注意が必要です。

https://www.antiphishing.jp/news/alert/qr_20240828.html

メール本文内に二次元コードが記載されたフィッシングメール
画像はフィッシング対策協議会より

CLOSE

オンラインセミナーのご案内

インターネット環境があれば自席で受講できます。

防犯設備士が解説 事後からリアルタイムへ

監視カメラヒストリーからみる映像DX

- **開催日　：10月24日（木）（21日 17:30申込締切）**
- **開催時間　：14:00～15:00**
- **定　員　：300名**
- **対　象　：経営層・現場部門の責任者**
- **お申込み：下記URLより事前登録願います**
  URL：https://canon.jp/business/event

セミナー紹介動画！
https://youtu.be/vPXNiEPxvX0

毎日のようにニュースなどで流れる監視カメラの映像。
みなさまもご覧になることが多いと思います。
また、製造業におけるロボットの目や流通・店舗における映像によるマーケティング利用など単純な監視・防犯から映像DXのインプットデバイスとしての役割としてカメラは大きく変化してきています。
この度のオンラインセミナーでは、監視カメラの導入価値の変遷をカメラの歴史とともに解説するとともに、カメラを利用した映像DXの現状と今後についてご紹介いたします。
みなさまの業務に少しでも役立つことができれば幸甚に存じます。

≪講師PROFILE≫

キヤノンマーケティングジャパン株式会社
ソリューション事業推進本部　ＮＶＳ営業推進課
防犯整備士　牧　啓之

キヤノンMJ　セミナー　検索

IPAが注意喚起！ サポート詐欺の対処法が効かない 画面全体に偽メッセージが表示され操作不能になる手口

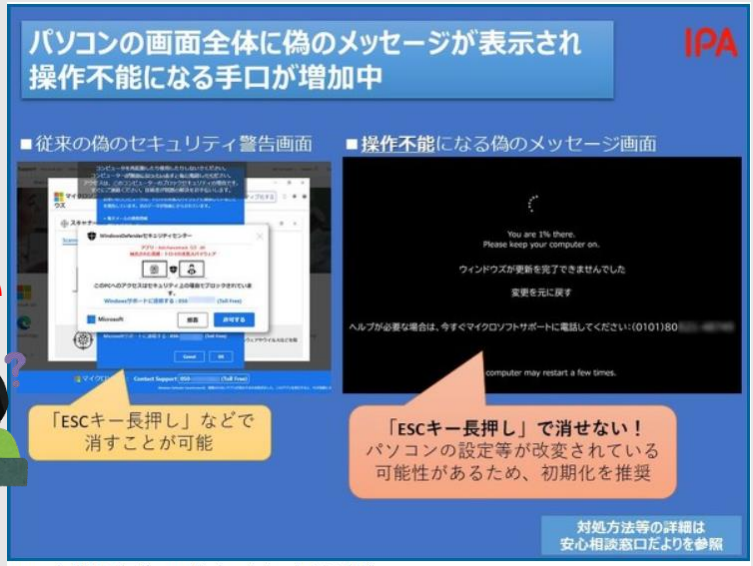
CAUTION

情報処理推進機構（IPA）はPCを使用中、画面全体に米Microsoftをかたる偽メッセージが表示され、キーボードやマウスの操作を受け付けなくなる上、再起動しても改善しない事象に関する相談が相次いでいるとして、注意を呼び掛けています。いわゆるサポート詐欺に似ていて、目的も同様とみられますが、これまでサポート詐欺で通用した対処法が使えないということです。 なお、実際に遭遇した場合の対処法として、

- **偽メッセージに書かれた連絡先には電話をかけない**
- **PCを直ぐにネットワークから切断する**
- **数分間、様子をみる**
- **Ctrl+Alt+Deleteキーで反応をみる**
- **パソコンの電源ボタンを長押しして電源を切る**

電源を切ったあとは、パソコンを安全な状態に復旧するため、パソコンの初期化をお勧めするとしています。

https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20240917.html



IPAの呼び掛け（画像はIPA公式Xアカウントから引用）