TOPIX

武蔵野銀行
サイバーセキュリティ対策セミナー

武蔵野銀行は「武蔵野銀行サイバーセキュリティ対策セミナー」を 12 月 3 日に開催した。本セミナーは、昨今、サイバー攻撃の手口巧妙化・悪質化、標的の多様化が進む一方、中小企業においては「専門的で難しく、何から対策すればよいかわからない」といった声を多く聞くことから、中小企業のサイバー攻撃に対する理解向上と具体的対策の実践へと繋げていただくため、情報提供をする機会として、武蔵野銀行において初めて実施した。

セミナーでは、埼玉県内を中心に、現地・オンラインあわせて約 300 社の経営者や経理担当者が参加し、埼玉県警察、トレンドマイクロ、ぶぎん地域経済研究所、武蔵野銀行の専門家が、それぞれの領域で知見を披露した。

埼玉県におけるサイバー犯罪の情勢、サポート詐欺・ランサムウェアの対処

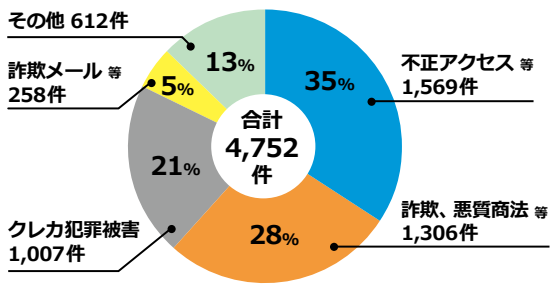
埼玉県警察　生活安全部　サイバー局
サイバー対策課　齊藤 隼人

埼玉県警察からは、①「埼玉県におけるサイバー犯罪の情勢」②「サポート詐欺」③「ランサムウェア」以上 3 点に関する、実情、手口、対策をご説明します。

①「埼玉県におけるサイバー犯罪の情勢」のパートでは、県内におけるサイバー犯罪の統計について説明します。

令和 7 年上半期におけるサイバー犯罪において、フィッシングに関連する不正アクセス被害等に関する相談は全体の約 33%（合計 4,752 件中 1,569 件）を占めました。

埼玉県のサイバー犯罪（令和 7 年上半期）



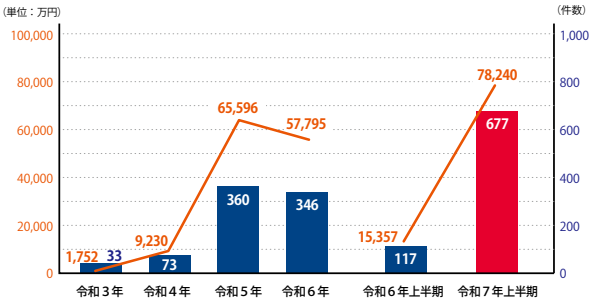
令和 7 年上半期のインターネットバンキングにおける不正送金被害は、認知件数が 677 件（前年同期比＋ 560 件）、被害額が約 7 億 8,240 万円（前年同期比＋約 6 億 2,883 万円）と、前年同時期と比較して被害件数、被害総額ともに急増しています。

ランサムウェア（身代金要求型ウイルス）も、令和 7 年、県内で 8 件発生しており、身近な県内においても脅威が潜んでいることがわかります。

②「サポート詐欺」のパートでは、実際の映像を用いて、手口をご説明します。

サポート詐欺は、インターネットの閲覧中に、突然「ウイルス感染した」等と偽の警告画面が表示され、パソコンから大きな警告音が鳴り、パソコンがウイルスに感染したと思わせ、その後パソコンを直す名目で、画面に表示されている犯人へと繋がる電話番号への架電を促します。犯人は対応しながら、

インターネットバンキング不正送金被害の推移（公表件数）



パソコンを直すふりをして金銭をだまし取るという手口です。サポート詐欺の画面上に表示された電話番号に絶対に電話しないでください。

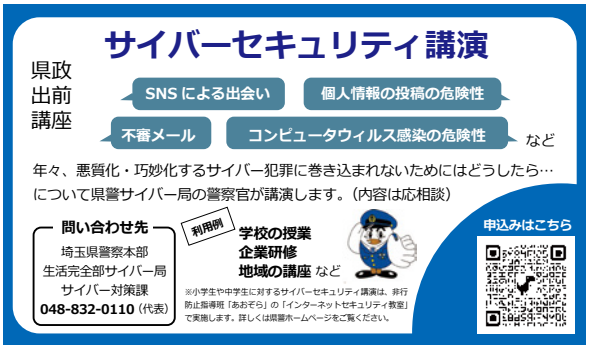
③「ランサムウェア」のパートでは、実際にランサムウェアに感染した場合の端末の様子や、対策について説明します。

ランサムウェアは、パソコンやサーバ内のデータを暗号化し、利用不可能な状態にしたうえで、そのデータを元に戻すことと引き換えに金銭などを要求する手口です。ランサムウェアに感染すれば、パソコン内の全ての情報が暗号化されることとなり、事業の継続は極めて難しくなります。また、復旧にも相当な時間を要します。

侵入経路は、VPN 機器やリモートデスクトップが多く、脆弱性や設定ミスが原因ですので、機器のアップデートやセキュリティパッチのこまめな適用が重要です。

また、社内での基本方針の策定やサイバーインシデント対応チーム「CSIRT（シーサート）」の態勢整備、オフラインバックアップを取得するといった対策などが有効であり、ぜひ実践してください。埼玉県警察では、サイバー犯罪に巻き込まれないための講演を受け付けていますので、企業の社員研修等でもご利用ください。土日祝日夜間なども事前に調整させていただければ可能です。内容については、SNS に関することなどご依頼に沿った内容でお話することが可能です。インターネットで申し込みすることができますのでお気軽に県警公式サイトからご応募ください。

https://www.police.pref.saitama.lg.jp/c0070/kurashi/cyber-koen.html



中小企業におけるサイバーセキュリティ対策の現状

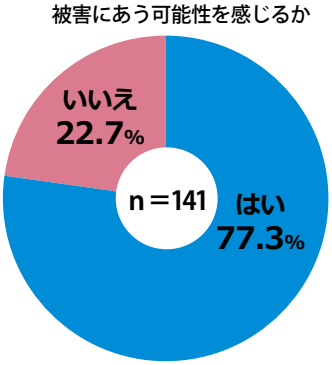
株式会社ぶぎん地域経済研究所
専務取締役　大西 浩一郎

当研究所では、2025 年 1 ～ 3 月期に県内企業の情報セキュリティ・リスクに対する認識やリスク管理に関するアンケート調査を行い、「埼玉県内企業の情報セキュリティの現状に関する調査」として取りまとめました。本日はそのエッセンスを説明します。

まず、「サイバーセキュリティ・リスクは遠い存在なのか」です。殆どの企業では、電子メールやホームページが使われていますので、社内システムはインターネット等を介して外部と繋がる可能性があります。過去 3 年のセキュリティ被害について尋ねると、「被害にあっていない」先は 6 割強止まり。残りの 4 割弱は「被害にあった」、「被害にあったかわからない」のいずれかです。被害にあった先では、現実に端末の修復・入れ替えや業務停止に迫られました。サイバーリスクはすぐそばにある脅威なのです。

しかし、「リスク認識とリスク管理の取組み姿勢」をみると、2 割以上が被害にはあわないと考えていました。理由は「情報セキュリティ対策を十分やっている」という過剰な自信や「規模が小さく標的にされない」といった誤解です。取組み姿勢についても、「最小限やっているつもり」と受け身、または「後回しにしがち」という先が多くを占めました。費用対効果が不明確なことが大きな理由です。

こうした中、「リスク管理の実態」をみますと、従業員 100 人未満など規模の小さい先で不十分さが目立ちます。組織体制でいえば、総務部等が業

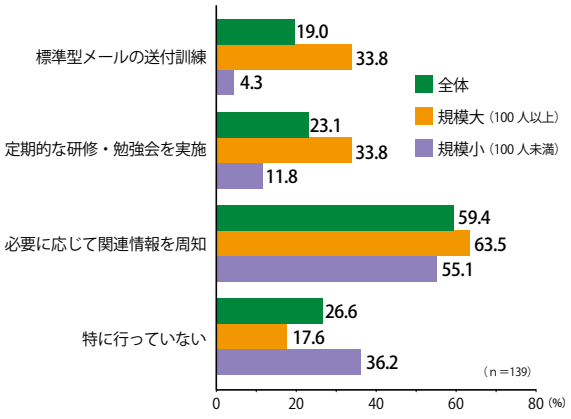


務の一環として情報セキュリティを担うケースが最多の 4 割弱ですが、「不明・キーパーソンもいない」先が全体の 1 割強、規模の小さい先の 2 割にのぼりました。また、対策ツール等をみると、EDR 製品（ウイルス感染時のシステムの不審な動きを検知）の導入は 1 割にとどまります。サポート期限切れの OS 使用も相応にみられました。

最後に、「従業員教育と今後の課題認識」です。従業員に対する情報セキュリティ教育は、リスク管理の有効性を高めるために不可欠ですが、定期的な研修・勉強会の実施も標的型メールの送付訓練も 2 割前後にとどまり、3 割弱の先では「特に行っていない」とのことでした。課題を質すと、「社内 IT 人材の不足」と「コストが過大、費用対効果」が半数を超えました。

このように、県内企業では、情報セキュリティに関するリスク認識、リスク管理体制の整備と実効性のいずれにおいても課題を抱えているように見受けられます。各社の自助努力と各方面からの手厚い支援が求められます。

従業員に対する情報セキュリティ教育



※複数回答のため、合計は 100% にならない。

とりあえず関連情報を集めたい

■ IPA 独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/sme/index.html

■ 埼玉県警察
https://www.police.pref.saitama.lg.jp/kurashi/cyber/index.html

県内の身近な窓口に相談したい

■ 公益財団法人 埼玉県産業振興公社 DX 推進支援グループ（埼玉県 DX 推進支援ネットワーク）
https://www.saitamadx.com/sodan/

「何を？どこから？始めていいかわからない」セキュリティ対策のご紹介

トレンドマイクロ株式会社
サイバーセキュリティ・イノベーション研究所
河田　芳希
コンシューマパートナービジネス開発本部
丸尾　周平

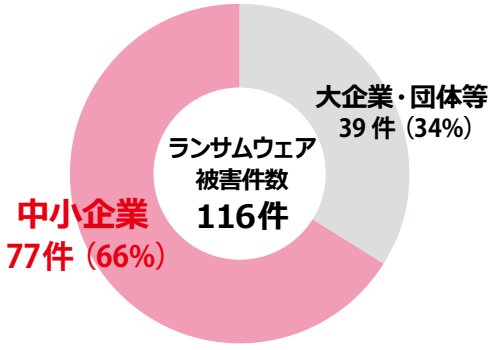
トレンドマイクロでは、「サイバーセキュリティは専門的で難しく、何から手を付けていいかわからない」といった方のために、最新の脅威である「①ランサムウェア」と「②サプライチェーン攻撃」の説明とその対策、電話を組み合わせたサイバー犯罪の対策として、自社商品の「③詐欺バスター」をご紹介させていただきます。

「①ランサムウェア」の被害は年々拡大しており、自社の調査によると 2022 年から 2023 年にかけて件数は 19% 増加。2023 年から 2024 年にかけて 22% 増加しています。

また、被害に遭っている企業の 66% が中小企業であり、50% が従業員 500 名以下の企業です。身代金を要求される点や、ニュースで取上げられる点から、「大企業が狙われやすい」と考える人もいるでしょう。詳細は「②サプライチェーン攻撃」で説明します。

「②サプライチェーン攻撃」とは、流通の流れから侵入し、ターゲット企業に攻撃を行う手口であり、直接大企業への侵入を狙うのではなく、サプライチェーン全体を侵入経路と捉え、セキュリティが甘い企業を侵入口として標的に達することを目的とします。したがって、中小企業こそセキュリ

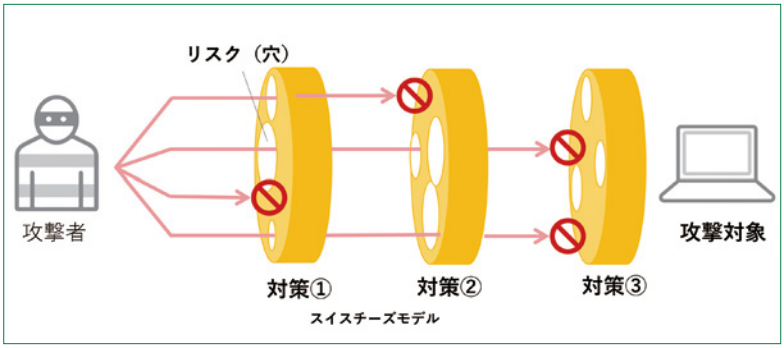
埼玉県のサイバー犯罪（令和 7 年上半期）

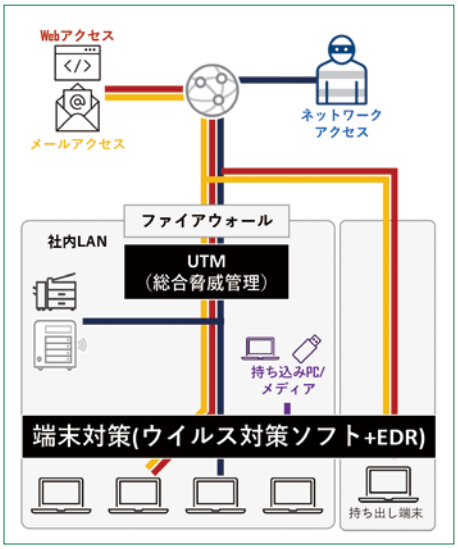


※警察庁「令和 7 年上半期におけるサイバー空間をめぐる脅威の情勢等について」

スイスチーズモデル

1種類で完結する完璧な対策は存在しない。それぞれの製品・機能には強み／弱みがあるため、複数の対策の重ね合わせによる対策（多重防御）が効果的であるという考え方





ティ対策を実施すべきです。

IPA「2024年度中小企業等実態調査結果」によれば、サイバーインシデントにより取引先に影響があった企業は7割という統計もあります。以上のことから、サイバーリスクはビジネスリスクに直結していると言えます。

では、中小企業はどのような対策を行えばよいのでしょうか。サイバー攻撃には様々な手口や侵入経路があるため、「スイスチーズモデル」と呼ばれる、複数製品、複数機能により多層的に防御することが大切です。

コストと手間を考えると、UTM（統合脅威管理）、EPP製品（ウイルス対策ソフト）、EDR（振舞検知）の導入がおすすめです。この3つを導入することで、「メール」「Webアクセス」「ネットワークアクセス」といった外部の脅威や、「メディア」「持込PC」といった内部の脅威にも総合的に対応できます。

「③詐欺バスター」を導入することで、不審な電話番号への受発信を検知でき、ボイスフィッシングやサポート詐欺に有効です。無料版もあり、ぜひご検討ください。

最後に、社内リテラシーの強化、すなわち「人の脆弱性」への対策も併せて重要です。技術的な対策だけでなく、社内教育などを含めた総合的な対策が必要であると思います。

インターネット取引時の注意点とお客さまへのお願い

株式会社武蔵野銀行 事務統括部
システム統括室　川畑　直貴

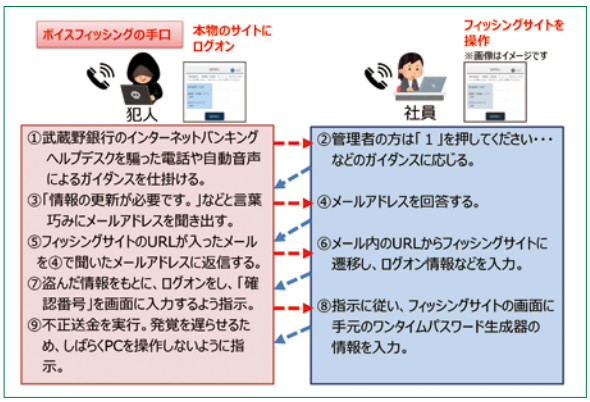
弊行から、インターネットバンキングサービスを中心に、企業の皆さまにおいて金融犯罪から身を守るために、「①ボイスフィッシングの手口」、「②気をつけていただきたいこと」「③実施していただきたいセキュリティ対策」について説明します。

まず、3月に当行、11・12月に複数の金融機関で発生した「①ボイスフィッシング」について説明します。この手口は、銀行や銀行のヘルプデスクを騙った電話や自動音声により、「情報の更新が必要です。」などと犯人が不安をあおり、手続きと称しメールアドレスを聞き出し、当該アドレスにフィッシングメールを送付します。偽サイトに誘導された顧客がID、パスワード、ワンタイムパスワード等を入力してしまうと不正送金がされるというものです。

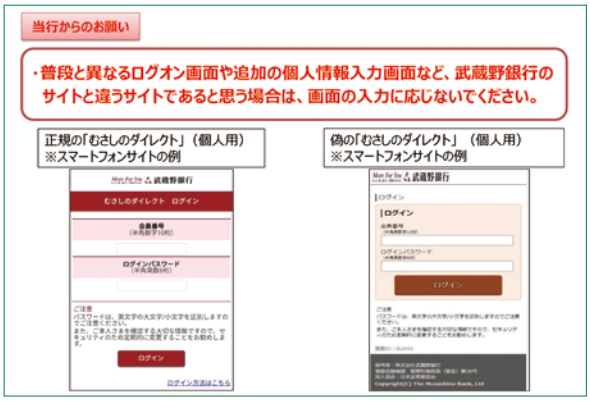
当行において、法人向けのインターネットバンキングにおいては普段振込をしていない先への当日の即時振込を停止しており、皆さまにはご不便をおかけしております。皆さまのご資産を守るための対応でございますので、ご理解とご協力をお願いします。

さて、「②気をつけていただきたいこと」について説明します。先ほどお話ししたような不審な電話や

インターネットでの不正送金における最新の手口



お客さまに気をつけていただきたいこと



メールなどが来た時に、大切な３つの標語をお伝えします。「不審な電話に出ない」、「不審なメールを開かない」「ID・パスワードを教えない」この３点が非常に重要となりますので、ぜひ覚えてください。

次に、普段と異なるログオン画面や追加の個人情報の入力画面など、武蔵野銀行のサイトと違うサイトであると思う場合は、画面の入力に応じないでください。武蔵野銀行が過去に観測したフィッシングサイトでは、色味、ロゴ、レイアウトなど、正規のサイトと比較して異なっているものもありました。万が一このようなフィッシングサイトを開いてしまった場合は、すぐに閉じ、ウイルススキャンを実施してください。

平時から実施していただきたいセキュリティ対策として、PC での利用の場合は当行推奨のセキュリティソフト「Phish Wall プレミアム」をインストールしてください。OS、ブラウザ、ソフトウェアの最新化や定期的な口座の異動確認もお願いします。

もし、不審な電話やメールが実際に来た場合は、当行のインターネットヘルプデスクがございますので、そちらにお問い合わせください。最後に、当行ではＩＴ人材紹介やセキュリティに関するご資金、サイバー保険などのご相談ができますので、ぜひお取引店舗や担当者までお問い合わせください。

日時：2025 年 12 月 3 日（水）14：00 ～ 16：00
会場：武蔵野銀行本店 4 階大会議室