特集

サイバー犯罪から会社と顧客を守るために

～あなたの会社のセキュリティ対策は大丈夫ですか？～

近年、情報通信技術の発展に伴い様々な脅威が現れ、攻撃者の手口は年々巧妙かつ悪質になっています。企業においては、ランサムウェア攻撃や標的型メール攻撃などのサイバー攻撃に加え、サプライチェーンに関連するリスクや内部不正といった脅威が顕在化しており、これらに対処するための適切なセキュリティ対策が求められています。今回は、福岡県警察本部サイバー犯罪対策課の協力のもと、中小企業の情報セキュリティ対策について紹介します。

本誌面は、以下資料を参考に作成しています。
・独立行政法人情報処理推進機構（IPA）「中小企業の情報セキュリティ対策ガイドライン」（https://www.ipa.go.jp/security/guide/sme/about.html）
・警察庁「令和６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」（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6/R06_cyber_jousei.pdf）

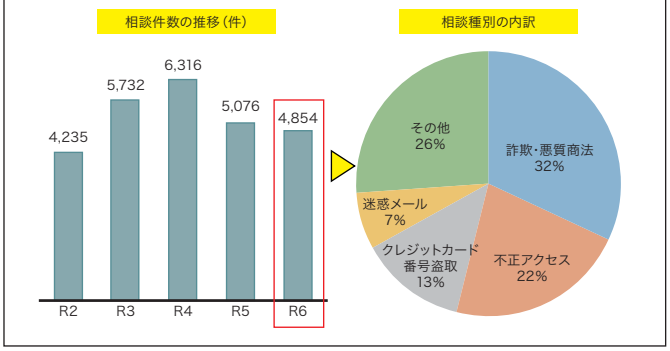
なぜ今、情報セキュリティが重要なのか

■サイバー犯罪に関する相談は高水準で推移

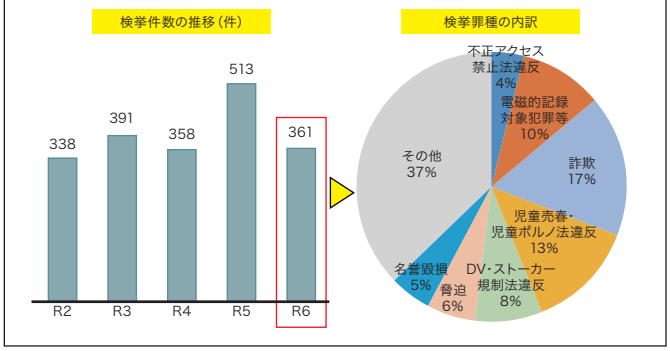
警察庁の「令和６年におけるサイバー空間をめぐる脅威の情勢等について」によると、サイバー犯罪の検挙件数は年々増加しています。また、サイバー攻撃の前兆ともなる不審なアクセスやランサムウェアの被害報告数も増加し、サイバー空間における脅威は年々深刻化しています。

福岡県警察本部サイバー犯罪対策課によると、**福岡県内のサイバー犯罪の相談受理件数も高水準で推移**しており、企業がランサム攻撃により情報漏洩や業務停止等といった深刻な被害を受けた事例も発生しています。

〈サイバー犯罪に関する相談受理状況（福岡）〉



〈サイバー犯罪の検挙状況（福岡）〉



■サイバー犯罪はどの企業にも起こりうるリスク

独立行政法人情報処理推進機構（IPA）が、2025年に発表した「組織」向け『情報セキュリティ10大脅威』では、「ランサム攻撃による被害（1位）」が10年連続でランクイン。その他、「サプライチェーンや委託先を狙った脅威（2位）」や「システムの脆弱性を突いた攻撃（3位）」などが選ばれました。様々な脅威がありますが「攻撃の糸口」は似通っています。**企業規模、業種に関わらず、どの企業にも起こりうるリスクであり、基本的な対策を行うことが重要です。**

※出典：IPA「情報セキュリティ10大脅威 2025 組織編（2025年２月）」
（https://www.ipa.go.jp/security/10threats/index.html）

〈情報セキュリティ10大脅威 2025（2025年２月発表）〉

順位	「組織」向け脅威
1位	ランサム攻撃による被害　10年連続ランクイン
2位	サプライチェーンや委託先を狙った攻撃
3位	システムの脆弱性を突いた攻撃
4位	内部不正による情報漏えい等
5位	機密情報等を狙った標的型攻撃
6位	リモートワーク等の環境や仕組みを狙った攻撃
7位	地政学的リスクに起因するサイバー攻撃
8位	分散型サービス妨害攻撃（DDoS攻撃）
9位	ビジネスメール詐欺
10位	不注意による情報漏えい等

実際にサイバー被害を受けるとどうなるの？　～ランサム攻撃を受けた場合～

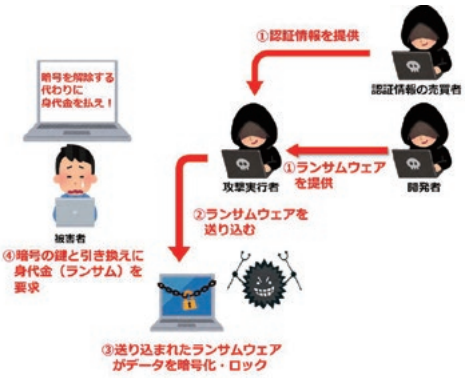
■そもそもランサム攻撃とは？

「ランサムウェア」と呼ばれるコンピュータウイルスに感染すると、**パソコンやサーバに保存しているデータが暗号化され使用できなくなり、データを復号する対価として金銭（身代金＝ランサム）を要求されます。**さらに、データを盗み取った上、「対価を支払わなければデータを公開する」などと脅迫するダブルエクストーション（二重恐喝）という手口も発生しています。

侵入例

- **ソフトウェアの脆弱性を狙う攻撃**（古いOS、未更新のソフトウェアの使用）
- **感染したUSB、外部メディアの使用**
- **悪意のあるメールの添付ファイル開封、Webサイトの閲覧**
- **取引先、委託先等のサプライチェーン経由**

〈ランサム攻撃の流れ〉



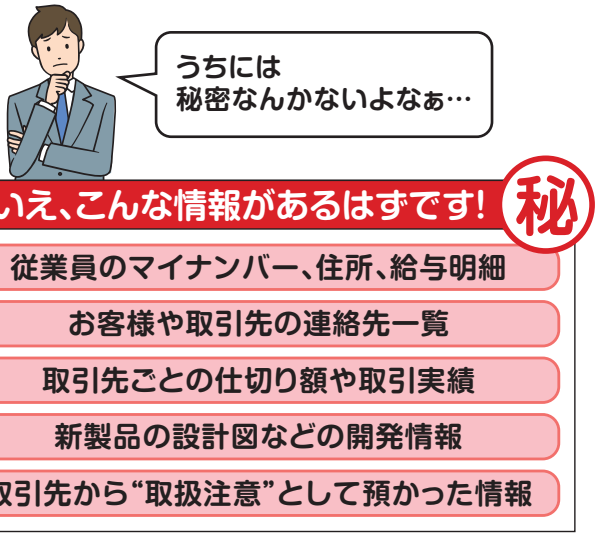
■中小企業が標的に、長期化・高額化する被害

令和6年にランサムウェアの被害を受けた企業・団体のうち、約6割が中小企業であり、**対策が比較的手薄な中小企業への被害が増加**しています。被害に遭った場合、**復旧までに2か月以上掛かるケースや、調査・復旧費用が1億円を超えるケース**も確認されるなど、事業への影響が深刻化（復旧までの長期化、被害額の高額化）する傾向にあります。

情報セキュリティ対策は経営者の責務

情報セキュリティ対策を怠ると企業は様々な不利益を被ります。例えば、顧客情報や取引先の設計データが漏洩した場合、企業としての社会的信用は失墜し、業務停止による売上減少だけでなく、損害賠償や契約解除といった二次被害が発生することもあります。

情報セキュリティ対策は、顧客・取引先・従業員・株主などに対する経営者としての責任を果たすためにも重要です。顧客や従業員の個人情報や商品の開発情報などを守るためにも、まずは**自社で起こりうる情報セキュリティ上の事故とは何か、どの業務にそのような心配があるか、自社の経営において最も懸念される事態は何か**等を具体的に思い描くことが経営者が情報セキュリティ対策を認識する第一歩です。



〈情報セキュリティ対策を怠ることで企業が被る主な不利益〉

金銭の損失	情報漏洩で取引先や顧客等から損害賠償請求を受けるケースや、不正送金等で直接的な損失が発生するケースも。
顧客の損失	社会的評価や信用が低下し顧客離れが発生。サプライチェーン企業の場合は受注停止に追い込まれることも。
事業の停止	生産活動の遅れや営業機会の損失が発生し業務が停滞。事業停止や取引先への影響も。
従業員への影響	対策の不備を悪用した内部不正が容易に行える職場環境は、従業員のモラル低下を招く要因に。

まずはできるところから情報セキュリティ対策を始めましょう！

独立行政法人情報処理推進機構（IPA）は、サイバー空間の脅威への基本的な対策として、「情報セキュリティ5か条」を示しています。まずはこの基本の5か条から実践してみましょう！

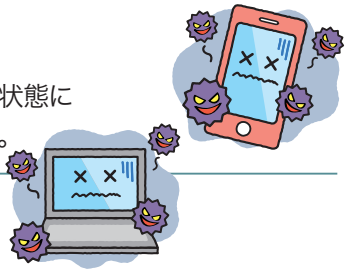
※参考：IPA「情報セキュリティ5か条」（https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055516.pdf）

①OSやソフトは常に最新の状態にしよう！

パソコンやスマートフォンのOSやソフトはもちろんのこと、ルータなどの通信機器や、スマート家電、ネットワークカメラなどのIoT機器のファームウェアも更新しましょう。

対策例
- WindowsUpdate（Windows OSの場合）、ソフトウェア・アップデート（macOSの場合）などベンダの提供するサービスを実行する。
- Adobe Reader、ブラウザなど利用中のソフトウェアを最新版にする。
- テレワークで利用するパソコン等のソフトウェアやルーター等のファームウェアを最新版にする。

②ウイルス対策ソフトを導入しよう！



ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）を常に最新の状態に保つことで、ウイルスの感染を防ぎ、会社のシステムや機密情報を守ることができます。

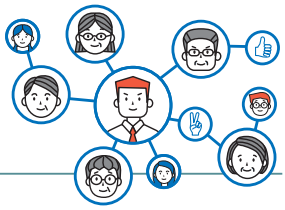
対策例
- ウイルス定義ファイルが自動更新されるように設定する。
- 統合型のセキュリティ対策ソフトの導入を検討する。
- OSに標準搭載されているセキュリティ機能を有効活用する。

③パスワードを強化しよう！

パスワードは初期設定のまま使用せず、「長く」、「複雑に」、「使い回さないこと」を心がけましょう。また、アカウント管理を徹底しましょう。

対策例
- パスワードは最低でも10文字以上にし、大文字・小文字・数字・記号含めて複雑に、個人情報や簡単な英単語は使わず、推測できないようにする。
- 同じID・パスワードを複数サービス間で使い回さない。
- テレワークでVPNやクラウドサービスを利用する際は、強固なパスワードを設定し、可能な場合は多段階認証や多要素認証を利用する。

④共有設定を見直そう！



共有範囲は最小限としているか、アカウントは共有することなく適切に付与しているかなど、設定を見直しましょう。

対策例
- ウェブサービス、ネットワーク接続の複合機・カメラ、ハードディスク（NAS）などの共有範囲を限定する。
- 従業員の異動や退職時には速やかに設定を変更（削除）する。
- テレワークで使用するパソコン等は他者と共有しない。共有せざるを得ない場合は、別途ユーザーアカウントを作成する。
- 外出先でフリー Wi-Fiを使うときにはパソコンのファイル共有をオフにする。

⑤脅威や攻撃の手口を知ろう！

情報セキュリティに対する脅威や攻撃の手口については、IPAなどのセキュリティ専門機関や警察が発信する情報を確認し、適切な対策をとりましょう。

企業規模に関わらず、必ず実行すべき基本的な対策です。今一度、自社の対策状況のご確認をお願いします。

～警察からのお願い～

サイバー犯罪の被害は警察へ通報を

お問い合わせ
福岡県警察本部サイバー犯罪対策課
TEL:092-641-4141

警察では寄せられた情報を分析し、捜査を行うほか、被害企業における対策に必要な情報の提供・助言、他の企業への被害拡大を防止するための注意喚起等の被害防止のための取組みを行っています。

■速やかな通報・相談

サイバー犯罪の被害に遭った際は、最寄りの警察署へ通報・相談してください。
また「サイバー事案に関する相談窓口」もご活用ください。

■警察との連絡体制の確保等

・被害発生時のマニュアル等に警察の連絡先を記載する。
・被害の発生を想定した事業継続計画（BCP）を策定する。初動対応における警察との連携を記載する。
・策定した計画に基づき、可能な範囲で訓練を行う。

■初動対応における警察との連携

・侵入経路や侵害範囲特定のため、外部接続機器を中心としたログの保全に努めてください。
・必要に応じて、被害端末に関する情報（データの暗号化の有無）やネットワークの構成図等をを伺いますので情報提供にご協力をお願いします。

Q 通報したら被害を公表させられるのでは？（信用の毀損・風評被害が心配）

警察から被害の公表を求めることはなく、保秘を徹底します！通報して必要な捜査を行うこと、つまり「社会的責任を果たすこと」が、顧客や取引先等に対する説明責任を負う上で重要な要素となります。

Q 通報すると警察対応で時間を取られ復旧作業が遅れそう。

警察は、被害組織の復旧作業や業務継続に最大限配慮し対応します。

商工会議所が提供するサービスをご紹介

■YOKA-DIGIデジタル化相談窓口

セキュリティ対策に関するご相談も受け付けています。

日　時 毎月第2・第4木曜日 10:00～16:00
場　所 当所 経営相談窓口（当所ビル2階）
対　象 福岡市内の事業者または当所会員
内　容 自社の課題の把握・整理、デジタル化ツールの検討、その他デジタル化・DXに関するご相談
※特定の商品・サービスの操作方法等のサポートを行うものではありません。

1社1時間　事前予約制

電話予約 TEL:092-441-2161（平日 9:00～17:00）

WEB予約

■デジタル化優待サービス

当所会員を対象に、デジタル化に役立つツールやサービスを優待をつけて提供しています。セキュリティに関するツールもありますので、YOKA-DIGIウェブサイトよりぜひご確認ください。

詳細はこちら

■サイバー保険制度

■お問い合わせ / 会員組織・共済グループ　TEL：092-441-2845

本制度は、外部からのサイバー攻撃（不正アクセスやウイルス感染等）や情報漏えい、またはその恐れが生じた場合に、事業者が負う法律上の賠償責任・争訟費用や、事故発生時の各種対応費用（事故調査から再発防止策策定までの費用など）を補償するものです。商工会議所のスケールメリットを活かした割安な保険料でご提供していますので、お気軽にご相談ください。

詳細はこちら

本誌面に関するお問い合わせ / 企画広報グループ　TEL：092-441-1112