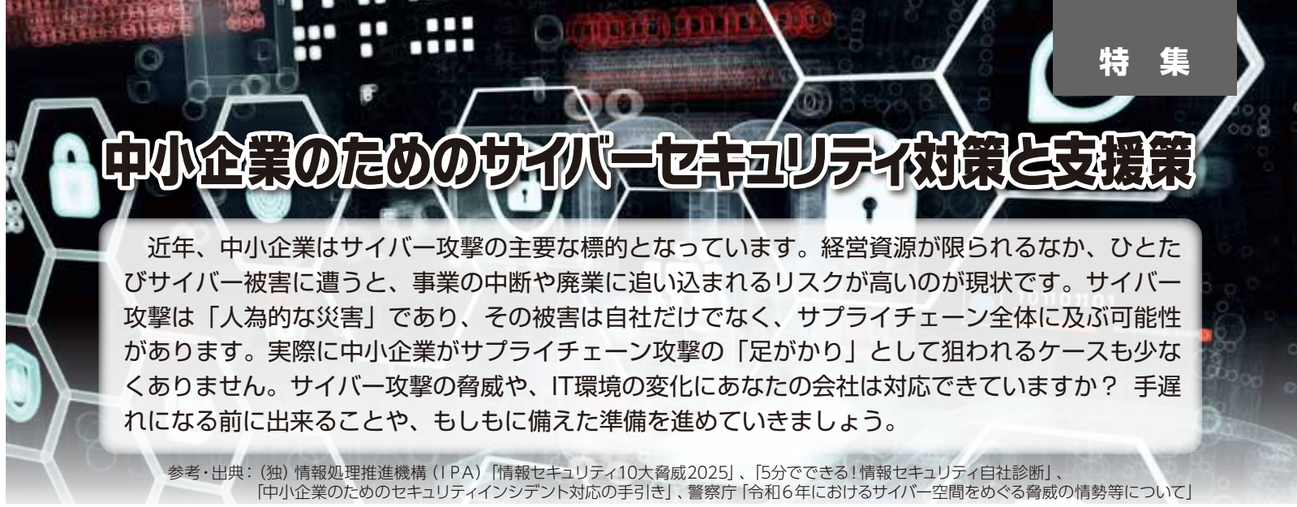


特　集

中小企業のためのサイバーセキュリティ対策と支援策

近年、中小企業はサイバー攻撃の主要な標的となっています。経営資源が限られるなか、ひとたびサイバー被害に遭うと、事業の中断や廃業に追い込まれるリスクが高いのが現状です。サイバー攻撃は「人為的な災害」であり、その被害は自社だけでなく、サプライチェーン全体に及ぶ可能性があります。実際に中小企業がサプライチェーン攻撃の「足がかり」として狙われるケースも少なくありません。サイバー攻撃の脅威や、IT環境の変化にあなたの会社は対応できていますか？ 手遅れになる前に出来ることや、もしもに備えた準備を進めていきましょう。

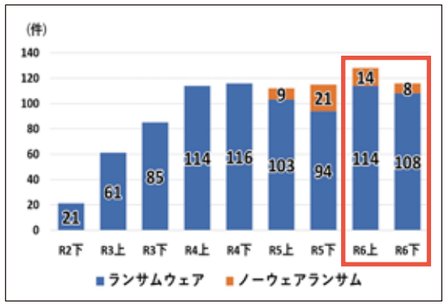
参考・出典：(独) 情報処理推進機構（ＩＰＡ）「情報セキュリティ10大脅威2025」、「5分でできる！情報セキュリティ自社診断」、「中小企業のためのセキュリティインシデント対応の手引き」、警察庁「令和６年におけるサイバー空間をめぐる脅威の情勢等について」

中小企業を狙うサイバー攻撃の脅威と現状

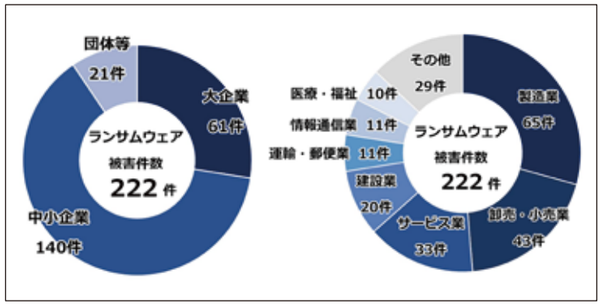
独立行政法人情報処理推進機構（ＩＰＡ）が発表した「情報セキュリティ10大脅威　２０２５」によると、組織や企業に対しての脅威として、上位から①ランサム攻撃、②サプライチェーンや委託先を狙った攻撃、③システムの脆弱性を突いた攻撃、④内部不正による情報漏えい等、⑤機密情報等を狙った標的型攻撃などが上位を占めました。

この中でも近年、被害が増加しているのが「ランサムウェア」による被害です。

ランサムウェアの被害件数
（警察庁サイバー警察局の令和6年調査より）



ランサムウェアの被害の内訳（業種・規模）
（警察庁サイバー警察局の令和6年調査より）



ランサムウェアとは、感染するとパソコン等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復元する対価（金銭や暗号資産）を要求する不正プログラムです。

２０２４年には、大手出版社の「ＫＡＤＯＫＡＷＡ」が大規模な被害に受け、サービス停止や情報流出が発生しました。その原因は、フィッシング攻撃によって従業員のアカウント情報が盗まれたことだとされています。

ニュース等の報道は大企業が中心ですが、実際には中小企業の方が被害件数は多く、その多くの原因は簡易すぎるＩＤ・パスワードや不要アカウントの放置など、基本的対策の不足が目立ちます。

被害防止には、強固なパスワード設定と定期的な変更、不要アカウントや権限の削除、社員へのフィッシング対策教育、システムやソフトウェアの最新化など基本の徹底が欠かせません。今からできる「基本の見直し」を始めましょう。

まずはここから！ 押さえておきたい、セキュリティ対策

サイバー攻撃には、様々なパターンが存在しますが、攻撃の「糸口」は似通っており、基本的な対策の重要性は長年変わっていません。まずは、ＩＰＡが提唱する「情報セキュリティ５か条」の実践から始めましょう。これらは一度やれば良いものではなく、継続的な実施が欠かせないため、運用ルールとして社内に定着させることも重要です。

押さえておきたい情報セキュリティ５か条

① OSやソフトウェアは常に最新の状態にする

OSやソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があります。お使いのOSやソフトウェアには、修正プログラムを適用する、または最新版を利用するようにしましょう。

対策例

- ●Windows　Update(Windowsの場合)、ソフトウェア・アップデート(macの場合)などベンダー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(機械を制御するソフトウェア)を最新版にする。

【Windows10のサポートは10月14日まで！】

情報セキュリティ対策に役立つツール「MyJVNバージョンチェッカ」

パソコンにインストールされているソフトウェア製品（ウェブブラウザや動画再生ソフトなど）のバージョンが最新であるかを簡単な操作でチェックできるツールです。MicrosoftのWindows Updateと併せて、ソフトウェア製品のバージョンアップを行う習慣を身に付けましょう。

MyJVNバージョンチェッカのダウンロードサイトはこちら

② ウイルス対策ソフトを導入し、適切に利用する

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。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）は常に最新の状態になるようにしましょう。

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。
- ●テレワークで利用するパソコン等の端末にウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にする。

③ 強固なパスワードを使用する

パスワードが推測や解析されたり、ウェブサービスから流出したID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。

対策例

- ●パスワードは１０文字以上で「できるだけ長く」、大文字、小文字、数字、記号含めて「複雑に」、名前、電話番号、誕生日、簡単な英単語などは使わず、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 共有設定を見直す

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。

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り、対策に活かす

取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

対策例

- ●IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る。
- ●利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する。
- ●テレワークでは管理者が従業員に適宜注意喚起し、従業員はセキュリティの懸念は速やかに報告する。