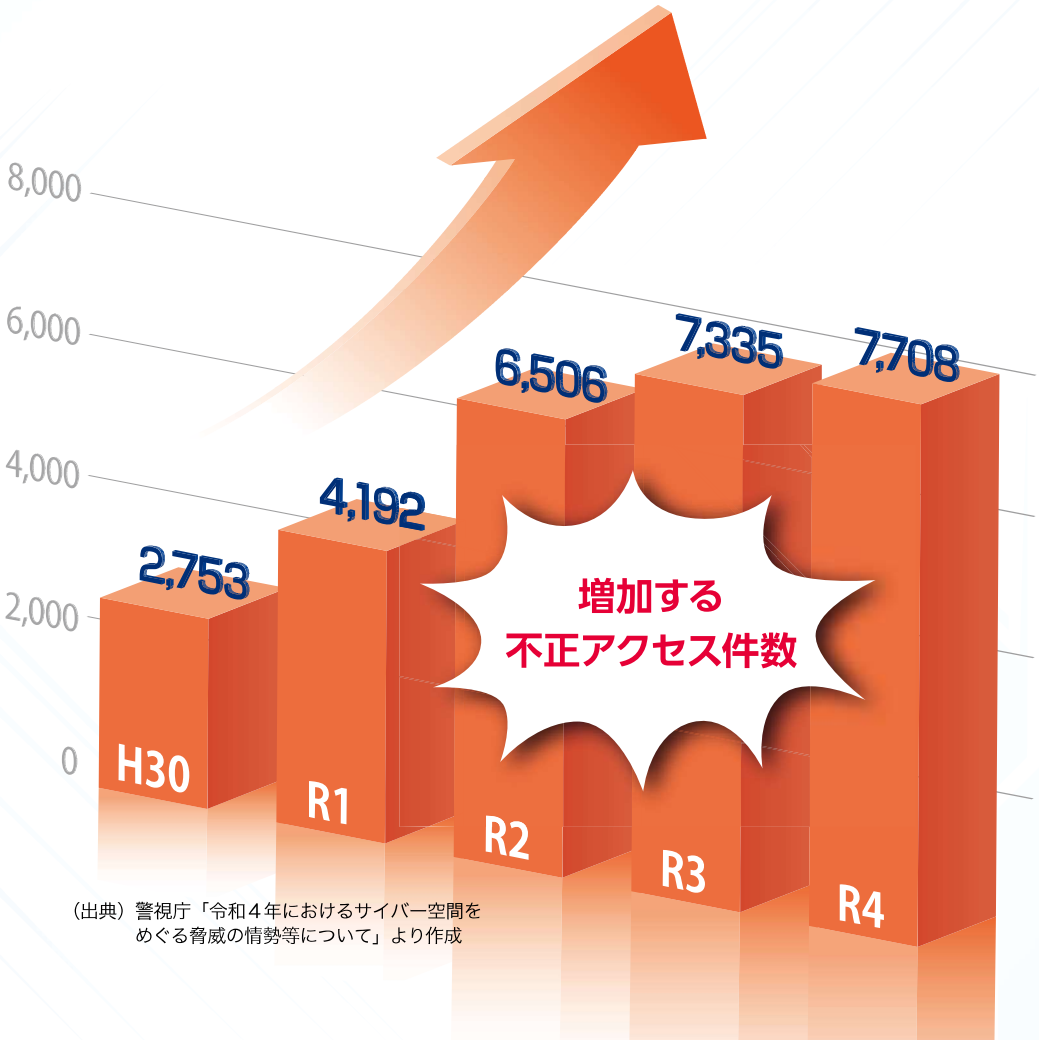
正しく恐れて備えよう！

中小企業が狙われる サイバー攻撃の実態とその対策

「商工会議所サイバーセキュリティお助け隊サービス」開始!!



（出典）警視庁「令和４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」より作成

現代社会では、デジタル技術の発達によって、利便性の高い様々なサービスが提供されている。また、ビジネスの場においては、こうした技術・サービスを活用することで、ビジネスプロセスの変革やイノベーティブなサービスの創生、商品の高付加価値化など様々な効果が期待できる。デジタル技術が発達する一方、サイバー攻撃の脅威は年々増大している。サイバー攻撃による情報漏洩やシステムの停止など、深刻な影響が懸念される現代のビジネスにおいて、サイバーセキュリティはますます重要性を増している。

特に、中小企業は、サイバー攻撃の被害に遭いやすく、対策を怠ることで深刻な被害を被る可能性がある。そこで本特集では、中小企業が抱えるサイバー攻撃の実態や、対策のポイントを解説する。

協力：東京海上日動火災保険株式会社・大阪商工会議所

実は身近なサイバー攻撃!?

「うちみたいな小さな会社が狙われるわけがない」は嘘!?
中小企業は狙われている

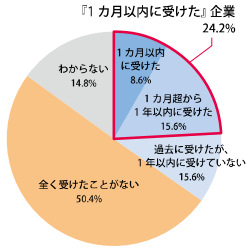
サイバー攻撃とは、インターネットやコンピュータネットワークを通じて、コンピュータシステムやデータ、個人情報、金融情報などに不正アクセスしたり、破壊・改ざん・盗用したりする行為を指す。また、サイバー攻撃には「標的型攻撃」と「ランダム攻撃」というものがあり、「ランダム攻撃」では個人や企業の規模に関係なく、全ての端末がターゲットとなる。

特に、最近のサイバー攻撃は、セキュリティが強固な大企業を直接狙うのではなく、セキュリティ対策が不十分な中小企業をターゲットにすることが多く、ターゲットにした中小企業から取引先情報を抜き取ったうえで、その取引先に攻撃を行うこともあり、知らず知らずのうちに自社が加害者になってしまうこともある。

多岐にわたるサイバー攻撃
ランサムウェアは事業停止リスク

サイバー攻撃の手法は、ウイルスを用いてシステムやデータを破壊・改ざん・盗難するマルウェア攻撃や、実在する人物になりすまして信頼性のある電子メールを送りつけることで機密情報を盗難する標的型攻撃メールなど、多岐にわたるが、近年は、ウイルスの一種であるランサムウェアによる感染被害が拡大している。

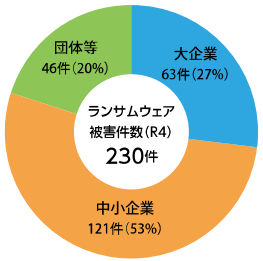
ランサムウェアとは、PCやサーバーが感染すると端末等に保存されているデータを暗号化し、使用できない状態にするもの。その復旧と引き換えに金銭を要求されるほか、端末やサーバーの暗号化でシステムが停止してしまい、事業継続が脅かされる恐れがある。復旧に時間がかかる場合は大きな経済的損失につながるうえ、重要な情報が窃取されることで社会的信用を失う恐れもある。



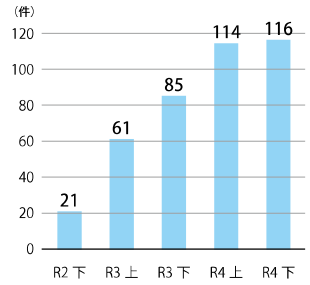
(出典)(株)帝国データバンク「特別企画:サイバー攻撃に関する実態アンケート(2022年10月)」より作成

令和4年度のランサムウェア被害件数は230件
その被害の半分が中小企業

ランサムウェア被害内訳



ランサムウェア推移



企業・団体等におけるランサムウェア被害として、令和4年に都道府県警察から警察庁に報告のあった件数は230件であり、令和2年下半期以降、右肩上がりでの増加となった。
被害(230件)の内訳を企業・団体等の規模別にみると、大企業は63件、中小企業は121件であり、その規模を問わず、被害が発生した。
(出典)警視庁「令和4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」より作成

狙われる中小企業

中小企業にどんな攻撃が?

ここで実際に中小企業が受けたサイバー攻撃の事例を見てみよう。

A社
金属製品製造業/従業員10~20人
- ラトビア共和国から管理者パスワードでログインされ、パソコンが遠隔操作されていた。
- 同社にはラトビアに営業所も現地工場も取引先もなく、社員の出張経験も無し。同国に関係するITサービス利用も無い。

B社
土木工事業/従業員70~80人
- コンピュータウイルスを配布するとして世界的にもブラックリストに掲載されている悪性サイトと社内端末が、深夜を含め頻繁に通信をしており、コンピュータウイルスをダウンロードした可能性が強い。

C社
建築材料卸売業/従業員30~40人
- DDoS攻撃(多数の外部端末から大量の情報を送りつける攻撃で、ウェブサイトがアクセスしにくくなること、またはサーバーダウンにつながる)を受けていた。

D社
医療用器具製造業/従業員80~90人
- 「GhOstRAT」(感染コンピュータをコントロールする為に利用されるコンピュータウイルス)による悪性サーバーからの指令等の通信が検知された。

E社
製造業/従業員100~150人
- ランサムウェア被害に遭い復旧のために2000万円の被害が出た。

※出典:大阪商工会議所・神戸大学・東京海上日動火災保険㈱による「中小企業を狙ったサイバー攻撃の実態を調査・分析する実証事業」(2018年)/大阪商工会議所での相談事例(2020年7月)

2021年 社会的に影響が大きかったサイバーセキュリティ10大脅威ランキング

	サイバーセキュリティの脅威	想定される被害
1位	**ランサムウェアによる被害** ウイルスの一種で、PC やサーバーが感染すると、端末のロックやデータの暗号化が行われる	・データを復旧と引き換えに金銭を要求される ・重要情報を窃取し、金銭を支払わなければ情報を公開すると脅迫される ・システムの停止によって事業継続が脅かされる
2位	**標的型攻撃による機密情報の窃取** 特定の企業に狙いを定め、ウイルスメールの送信や不正アクセス等を行い、機密情報を窃取する	・窃取された機密情報が悪用された場合、企業の事業継続に重大な影響を及ぼす ・データ削除やシステム破壊により企業等の活動が妨害される
3位	**サプライチェーンの弱点を悪用した攻撃** セキュリティ対策の強固な企業を直接攻撃せずに、サプライチェーンの中でセキュリティ対策が手薄な関連企業を最初の標的とし、そこを踏み台として本命の標的である企業を攻撃する	・機密情報の漏えいや信用の失墜等、様々な被害が発生する ・取引相手にも損害を与えてしまうことで、取引相手を失ったり、損害賠償を求められるおそれがある
4位	**テレワーク等のニューノーマルな働き方を狙った攻撃** 私有端末や自宅のネットワークを利用、初めて使うソフトウェアを導入等、業務環境の急激な変化を狙った攻撃が行われる	・業務環境に脆弱性があると、ウェブ会議ののぞき見、テレワーク用端末へのウイルス感染、感染した端末から社内システムへの不正アクセスのおそれがある
5位	**内部不正による情報漏えい** 勤務する従業員や元従業員等の企業関係者による機密情報の持ち出しや悪用等の不正行為	・漏えいした情報の重要性や機密性、漏えいの規模によっては、組織の社会的信用の失墜や、顧客等に対する損害賠償や補填による経済的損失が発生する ・不正に取得した情報を他組織に持ち込んだ場合、その組織も損害賠償等の対象になるおそれがある。
6位	**脆弱性対策情報の公開に伴う悪用増加** ソフトウェアや機器類の脆弱性対策情報の公開を悪用され、当該製品に対する脆弱性対策を講じていないシステムを狙う攻撃が行われる	・情報漏えいや改ざん、ウイルス感染等の被害の発生
7位	**修正プログラムの公開前を狙う攻撃(ゼロデイ攻撃)** ソフトウェアの脆弱性が発見され、脆弱性の修正プログラムや回避策が公開される前にサイバー攻撃が行われる	・情報漏えいや改ざん、ウイルス感染等の被害の発生
8位	**ビジネスメール詐欺による金銭被害** 取引先や自社の経営者等を装い、巧妙な作られた偽のメールを送信し、従業員を騙して送金取引に関わる資金を詐取する	・攻撃者が用意した口座へ送金させる金銭的な被害をもたらす ・金銭の被害は高額になる傾向がある
9位	**予期せぬIT 基盤の障害に伴う業務停止** 企業や業務システム等で利用するサーバーやインターネット上のサービス等に予期せぬ障害が発生する	・提供するサービスの利用者がそのサービスを利用できなくなるなど、業務の停止につながる ・長時間停止した場合、利益減少や競争力の弱体化等につながる
10位	**不注意による情報漏えい等の被害** 企業の規程の不備や情報を扱う従業員に対する情報リテラシー教育の不足、不注意・ミスによって引き起こされる情報漏えい	・漏えいした情報が悪用されると詐欺被害等の二次被害に繋がるおそれがある。 ・社会的信用の失墜やそれに伴う経済的損失が発生する可能性がある。

(出典)独立行政法人情報処理推進機構セキュリティセンター(IPA)「情報セキュリティ 10 大脅威 2022」より作成

中小企業のサイバーセキュリティ対策

まずはできるところから！

中小企業にとってサイバー攻撃は身近な脅威である。その手口は年々巧妙かつ悪質になっているが、対策には共通する部分がある。適切な対策を行い、自社のみならず取引先に被害を拡大させないためにもサイバーセキュリティ対策を実践してみよう。できるところから始めて、段階的にステップアップし、サイバーセキュリティ対策のレベルを上げていただきたい。

情報セキュリティ基本方針を策定 組織的な取り組みを開始しよう

企業がサイバーセキュリティ対策に取り組むうえで、情報セキュリティ基本方針を策定し、組織内で周知徹底することは重要である。情報セキュリティに関する方針を明記することで、組織内の全ての関係者の意識向上と基本方針に基づいた行動が期待できる。

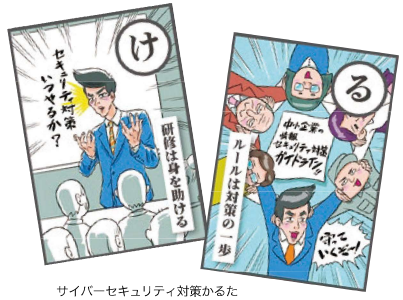
また、情報セキュリティ基本方針の策定により、情報セキュリティに真剣に取り組んでいる姿勢を顧客やパートナーに示すことができる。信頼性のあるセキュリティ対策は、顧客やパートナーにとって重要な要素であり、基本方針の存在は信頼関係の構築に寄与する。

情報セキュリティ基本方針の記載項目例

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善

など

情報セキュリティ基本方針のサンプルはこちら



サイバーセキュリティ対策かるた
[協力]独立行政法人情報処理推進機構

5分でできる情報セキュリティ自社診断 対策の実施状況を把握しよう

情報セキュリティ対策に取り組むうえで、自社の実施状況を把握することも大切である。セキュリティ対策の実施状況を把握することは、セキュリティ上の脆弱性などのリスク把握やサイバーセキュリティに関する法的要件・規制を遵守しているかの確認につながり、さらなるセキュリティ対策強化のきっかけにもなる。

IPAでは、情報セキュリティ診断ツールを提供している。まずは入門編として「5分でできる！情報セキュリティ自社診断」を実施いただき、自社のセキュリティ対策の実施状況を把握いただきたい。

自社診断の結果、点数に応じて次のステップが示され、問題があった項目については、解説編で対策を立てるうえでの考え方や具体的な対策例を確認することができる。

サイバーセキュリティ対策かるた
[協力]独立行政法人情報処理推進機構

5分でできる！セキュリティ自社診断はこちら

必ず実行!!

情報セキュリティ5か条

01 OSやソフトウェアは常に最新の状態にしよう！

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よう。

対策例
- WindowsUpdate、(WindowsOSの場合)、ソフトウェア・アップデート(macOSの場合)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。

02 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）は常に最新の状態にしよう。

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。

03 パスワードを強化しよう！

パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しよう。

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。

サイバーセキュリティ対策かるた
[協力]独立行政法人情報処理推進機構

04 共有設定を見直そう！

組織外の人物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よう。

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。

05 脅威や攻撃の手口を知ろう！

年々巧妙化する脅威や攻撃の手口について最新の情報を確認し、対策をとろう。

対策例
- IPA（独立行政法人 情報処理推進機構）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。

IPA(独立行政法人情報処理推進機構)HPはこちら

最新情報をチェックするために

サイバーセキュリティ情報発信サイトTokio Cyber Port 誕生

企業のサイバーセキュリティに関する情報を発信する総合情報ポータルサイト「Tokio Cyber Port」が東京海上日動火災保険(株)により開設された。企業のサイバーリスク対策に役立つ①ニュース・コラム②「無料セキュリティサービス」③「トラブル発生時の電話相談」「お役立ち情報」を無料で提供している。

「Tokio Cyber Port」HPはこちら

デジタルツールを活用した企業の成長に向けて

デジタル技術が進化し、利便性の高い様々なサービスが普及する中、中小企業にとって、サイバーセキュリティ対策は非常に重要な経営課題である。自分事としてセキュリティ対策に取り組むことで、自社の情報資産や顧客情報を保護するだけでなく、他社への被害拡大を防ぎ、ビジネスリスクを低減することができる。

中小企業は予算や人材といった経営資源を割り当てることが難しいという制約がある。一方、中小企業は経営者が意思決定を迅速に行うことができ、従業員とのコミュニケーションも容易であるなど、変化に応じた柔軟な対応が出来るという強みがある。こうした強みを活かして柔軟で継続的なサイバーセキュリティ対策に取り組むことで、企業の信頼性向上や事業継続性の確保、デジタル技術を活用した新しい取り組みなど、自社の成長につなげていただきたい。

サイバーリスクを回避する！「商工会議所サイバーセキュリティお助け隊サービス」

前橋商工会議所では5月1日より「サイバーセキュリティお助け隊サービス」を開始しました。本サービスは、独立行政法人情報処理推進機構（IPA）が定めるセキュリティサービス基準を満たした中小企業特化型サイバーセキュリティ対策サービスです。

群馬県内商工会議所（高崎を除く）の会員であれば月額6,600円（税込）で、①統合脅威管理（UTM）装置のレンタル②24時間365日の監視③定期報告④相談窓口⑤インシデント発生時のIT事業者駆け付けサービスをオールインワンのパッケージで提供するものです。初期費用なし・長期契約なし（1年更新）で事業所のサイバーセキュリティ対策が可能です。

詳細は今月に同封しております「サイバーセキュリティお助け隊チラシ」もしくは前橋商工会議所ホームページをご覧ください。

リスクを転嫁する！「スケールメリットを活かした商工会議所の保険制度」

リスクを回避する取り組みは必要ですが、全てのサイバーリスクを100%回避することはできません。万が一の被害を想定し、対応できる備えが必要です。前橋商工会議所ではビジネス総合保険制度や情報漏えい賠償責任保険制度～サイバーリスク補償型～などの制度をご用意しております。全国商工会議所のスケールメリットにより、低廉な保険料でご加入いただけますので、合わせてご検討ください。

お問い合わせ　前橋商工会議所　総務部　TEL：027-234-5111

商工会議所サイバーセキュリティお助け隊サービス　ホームページ

商工会議所会員向け保険制度ホームページ