経済産業省

中小企業が取り組むべきセキュリティ対策のいろは

経済産業省　商務情報政策局

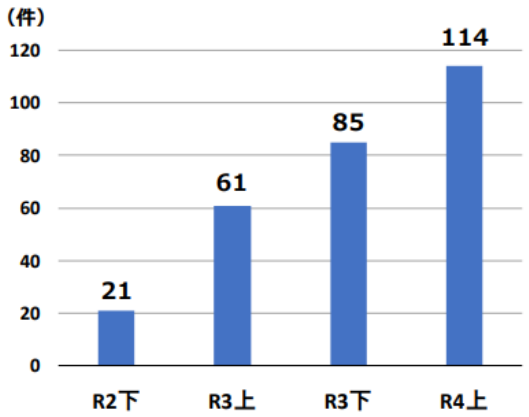
サイバーセキュリティ課

企画官　星 代介

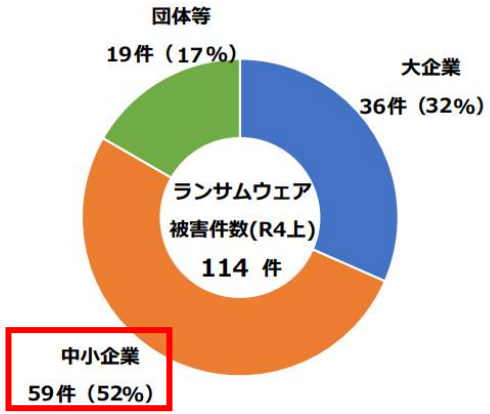
中小企業に対するサイバー攻撃の顕在化

- 近年、大企業を標的としたサイバー攻撃のみならず、サプライチェーン全体の中で対策が相対的に遅れている中小企業（※）を対象とするサイバー攻撃により、**中小企業自身**及びその取引先である大企業等への**被害が顕在化**している。
  ※昨年実施した調査によると、**中小企業のうち、直近３年間で情報セキュリティ対策投資について、「全く行っていない」と回答した企業が33%存在。**

- 企業等における**サイバー被害（ランサムウェア被害）**の警察庁への報告件数は**右肩上がりに増加中**。
- 被害件数(114件)の内訳は、大企業が36件（32%）に対して、**中小企業は59件（52%）と過半数超**。



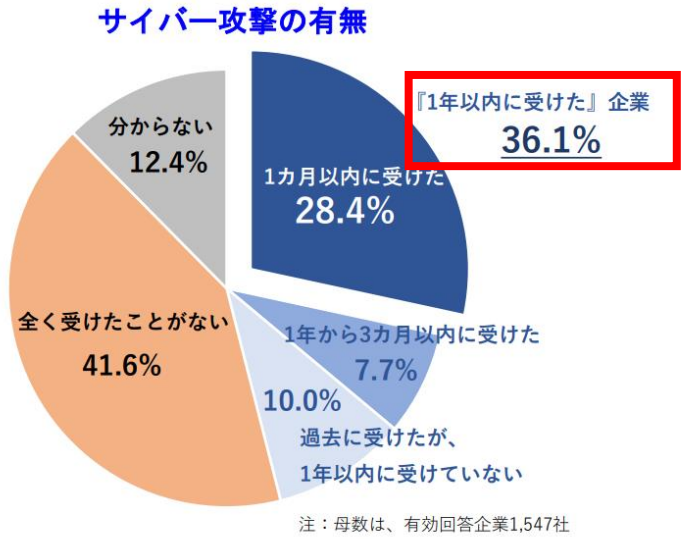
企業・団体等における
ランサムウェア被害の報告件数



ランサムウェア被害企業等の
規模別件数

警察庁「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（令和4年4月7日）」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

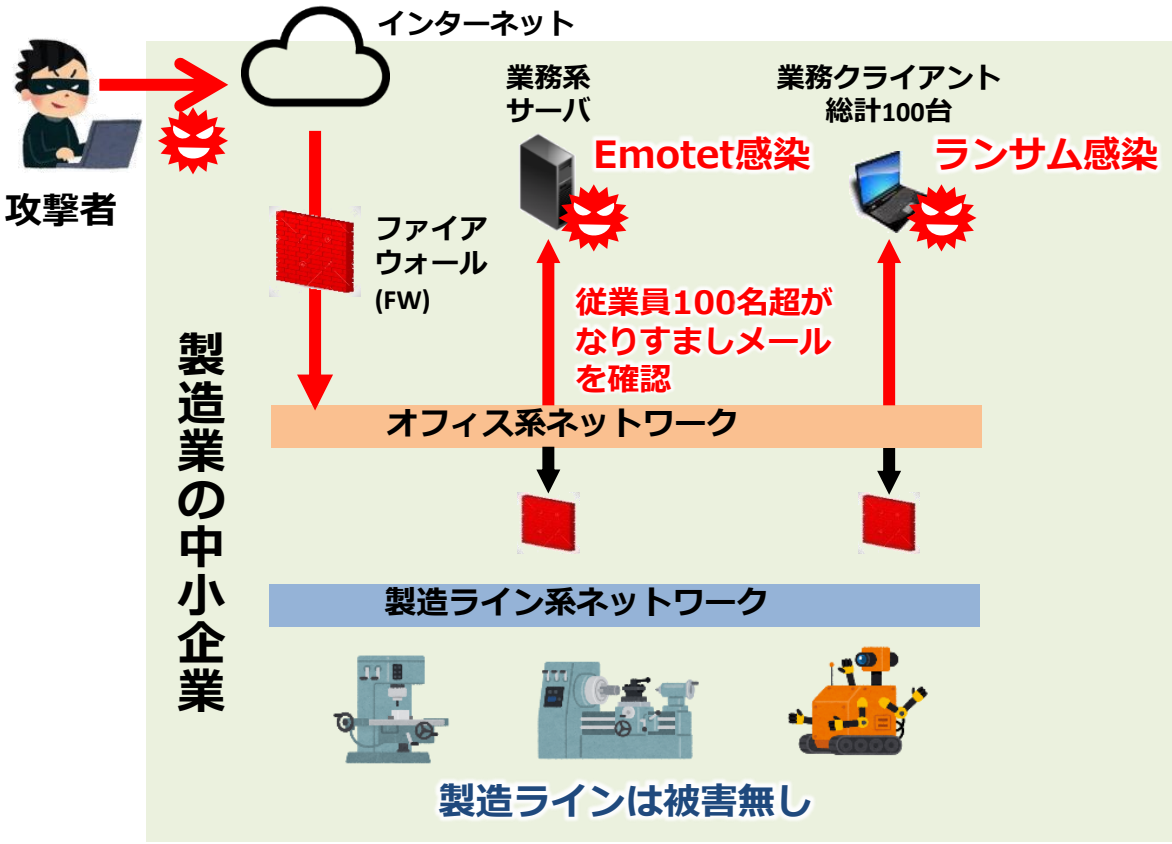
中小企業の約36%が1年以内にサイバー攻撃の被害



帝国データバンク「サイバー攻撃が多くなっています1 カ月以内に攻撃を受けた企業、約 3 割に！」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf

中小企業におけるサイバー攻撃の事例

- 重要インフラに関連する製造業の中小企業（従業員約200名規模）で、Emotetとランサムウェアに感染。Emotetに感染したメールアカウントは約100名分。原因は、受信メールの添付ファイルを自動実行する環境で開封したことであった。
- サイバーインシデントの初動対応体制や手順、セキュリティポリシーが整備されておらず、業務停止の判断等が困難な状況に陥った。
- 結果として、製造ラインの業務停止はなかったが、取引先へは、製造ラインに被害が無いことを証明する必要があり、影響範囲の特定を行うためフォレンジック調査費だけで500万円程度かかった。



対処時の問題点

- 業務停止の判断基準が整備されておらず、数日間判断が出来ないまま時間が経過。
- インシデント時の初動対応体制の役割分担が不明確であり、適切な人員確保もできず。
- 重要インフラを取り扱う業種で、影響範囲の把握が急務だったが自社内では調べきれず。

業務影響/被害額

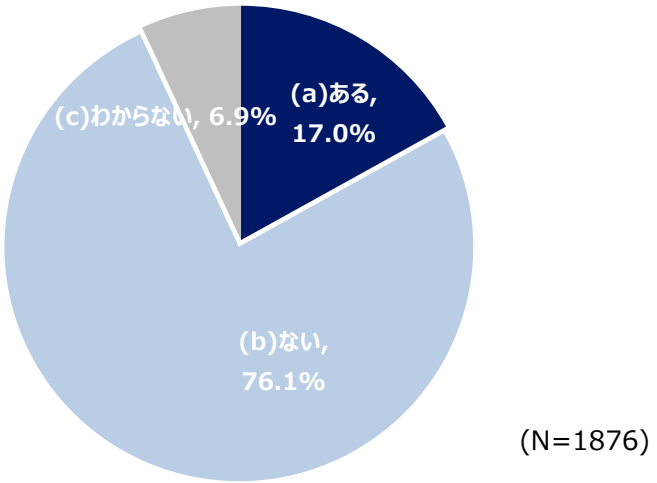
- 製造ラインに影響はなかったものの、結果を取引先に報告する必要あり。
- フォレンジック調査費だけで500万円程度を支出。高額な緊急支出に。
- 原因の判明だけでも10営業日程度を要した。
- 設計データなど最重要データが一部消失した。
- 取引先から問合せと苦情が殺到し、数週間にわたって業務がひっ迫した。

なぜ中小企業でもセキュリティ対策が必要なのか

- 大企業等を直接標的とせず、弱いところを狙って**サプライチェーン経由で攻撃を行うなどサイバー攻撃が巧妙化**。**取引先等を経由したサイバー攻撃被害**の経験がある。
- **取引先に対するサイバー攻撃により、大企業の操業が停止するケース**も発生。
- サイバー攻撃の対処を怠った場合の中小企業の**被害想定額**が**5000万円**近くなる事案も。

取引先等を経由したサイバー攻撃被害の経験

➢ 過去に取引先等がサイバー攻撃の被害を受け、それが自社に及んだ経験がありますか（仕入・外注・委託先等の取引先）



(N=1876)

（※）令和３年度サイバー・フィジカル・セキュリティ対策促進事業
（企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査）

中小企業であった特徴的な実例

古いOSの使用

・Windows XPでしか動作しないソフトウェア利用のために、**マルウェア対策ソフト未導入のWindows XP端末を使用**。

・社内プリンタ使用のために、社内LANに接続したことで、意図せずにインターネット接続状態になり、マルウェアに感染。

・検知・駆除できていなかった場合の**想定被害額は5,500万円**。

私物端末の利用

・社員の**私物iPhoneが会社のWi-Fiに無断で接続**されていたことが判明。

・私物iPhoneは、過去にマルウェアやランサムウェアの配布に利用されている攻撃者のサーバーと通信していた。

・検知・駆除できていなかった場合の**想定被害額は4,925万円**。

ウイルス対策ソフトを入れていれば大丈夫…？

セキュリティ対策は、何から始めたらいいの？

- できるところから初めて**段階的にステップアップ**
- 社として、IPA「情報セキュリティ５か条」を実践する。＝**SECURITY　ACTION１つ星宣言**
- 次に、IPA「５分でできる！情報セキュリティ自社診断」をやる。**＝SECURITY　ACTION２つ星宣言**
- **「サイバーセキュリティお助け隊サービス」の活用**を含む、さらなるセキュリティ対策の実施
- **IPA「中小企業の情報セキュリティ対策ガイドライン」**を参照。

（出典）中小企業庁 「中小企業の情報セキュリティ」 https://www.chusho.meti.go.jp/keiei/gijut/security.htm

中小企業向けセキュリティ対策ツール

● 中小企業の情報セキュリティ対策ガイドライン（第3版 2019年3月）

–中小企業が情報セキュリティ対策に取り組む際の経営者が認識し実施すべき指針、社内において対策を実践する際の手順や手法をまとめたもの。

–第3版より、付録６として、クラウドサービスを安全に利用するための留意事項やチェック項目を記載した手引きを追加。

中小企業の情報セキュリティ対策ガイドライン

経営者向けの解説

経営者が認識すべき３原則と実施すべき重要７項目を解説

実践者向けの解説

企業のレベルに合わせて**段階的にステップアップ**できるような構成で解説

付録6:クラウドサービス安全利用の手引き

【クラウドサービス導入時の考慮ポイントの例】

- ✓ クラウドで扱う情報と業務の重要性（情報漏洩、改ざん、サービス停止した際の影響等）
- ✓ 自社・事業者間でのセキュリティルール・水準の整合性（データアップデート時の暗号化やパスワード強度の警告等）
- ✓ 利用者の範囲、権限の管理（利用目的に合わせ利用者、権限を設定等）
- ✓ クラウド事業者・サービスの安全・信頼性（セキュリティ対策の開示状況等）　等

● 「SECURITY ACTION」

中小企業自らが、セキュリティ対策に取り組むことを自己宣言する制度。20万者を超える中小企業が宣言（2022年6月末）。

★一つ星

情報セキュリティ５か条に取り組む

★★二つ星

情報セキュリティ自社診断を実施し、基本方針を策定

● サイバーセキュリティお助け隊サービス

相談窓口、システムの異常の監視、緊急時の対応支援、簡易サイバー保険など中小企業のサイバーセキュリティ対策に不可欠な各種サービス内容を要件としてまとめた基準を満たすワンパッケージサービス。（2022年８月時点で18サービス）

サイバーセキュリティ お助け隊

IT導入補助金に「セキュリティ推進枠」創設

サイバーセキュリティお助け隊サービス

- 2019年度・2020年度実証事業で得られた知見に基づき、実証参加事業者がサービスを開発。
- サービス普及に向け、2021年度よりサービスブランドを設立。2022年８月時点で18サービスが登録。サービス審査登録制度の運営とともに、中小企業の意識啓発・サプライチェーンによる普及などの施策と一体となった普及施策の展開を開始。

中小企業のサイバーセキュリティ対策に不可欠な各種サービス

サイバーセキュリティお助け隊サービスウェブページ
https://www.ipa.go.jp/security/otasuketai-pr/

- EDR・UTM等による異常監視
- 緊急時の対応支援・駆付けサービス
- 相談窓口
- 簡易サイバー保険
- 簡単な導入・運用

中小企業でも導入・維持できる価格でワンパッケージで提供

お助け隊サービス審査登録制度：
一定の基準を満たすサービスにお助け隊マークの商標利用権を付与

お助け隊サービスA
お助け隊サービスB
お助け隊サービスC

サービス提供 → 中小企業 → 自社の信頼性をアピール → 取引先（大企業等）

お助け隊サービス利用の推奨等の中小企業の取組支援

サイバーセキュリティお助け隊

SC3(サプライチェーン・サイバーセキュリティ・コンソーシアム)

→SC3（業種別業界団体が参加）で利用推奨を行うことで、より多くの中小企業がお助け隊サービスを活用し、万が一の際に早急に正しい対処が行える状態を目指す。