東京海上日動

サイバーリスク対策

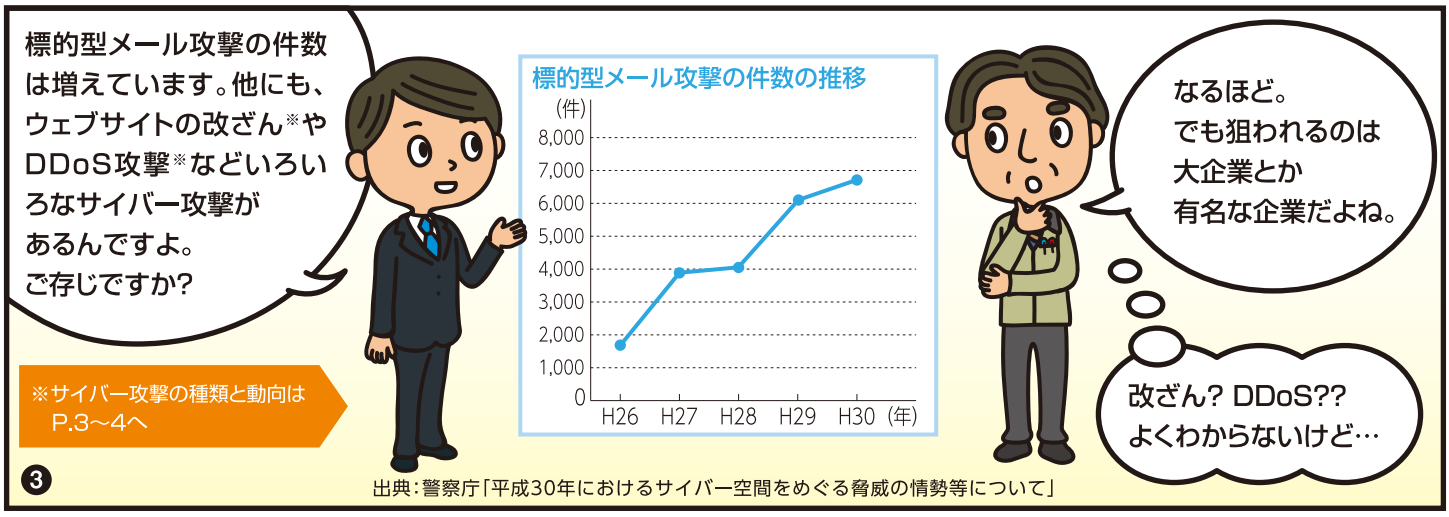
をお考えの皆さまへ

すべての企業が直面するサイバーリスク

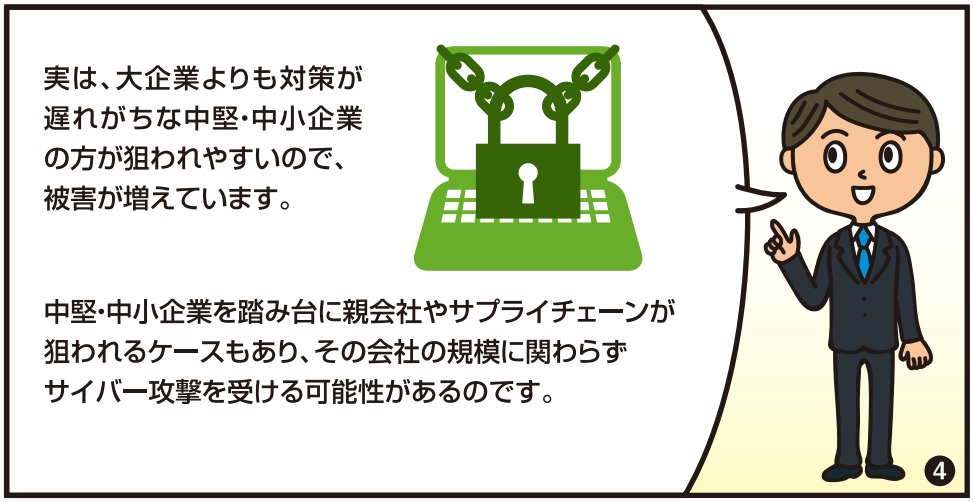
To Be a Good Company

あなたの会社も狙われている!?

～他人事ではないサイバーリスク対策～

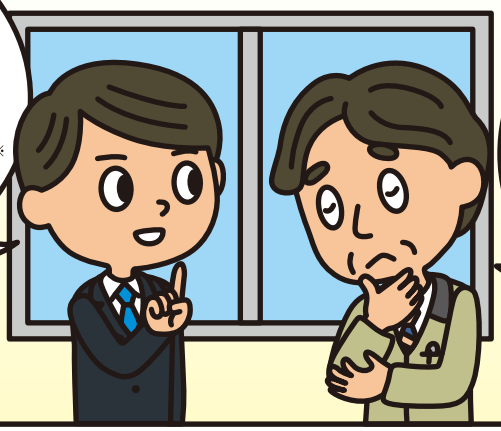


出典：警察庁「平成30年におけるサイバー空間をめぐる脅威の情勢等について」

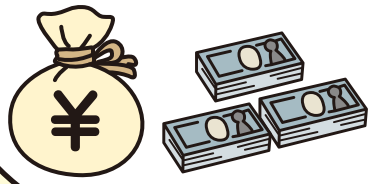


お詫びの費用だけではないですよ。
調査・復旧の費用や、賠償に関わる費用のほか、IT機器が停止することによる利益損害も発生する可能性があります。※

※サイバー攻撃による事故が発生した場合の影響は、P.5〜6へ



ずいぶんお金がかかりそうだね。
対策を考えたほうがいいかな?



❻

対策には、組織的対策・人的対策・物理的対策・技術的対策などがあります。
取り組むべき対策については、経済産業省による「サイバーセキュリティ経営ガイドライン」の中で、重要10項目がまとめられています。

サイバーセキュリティ対策

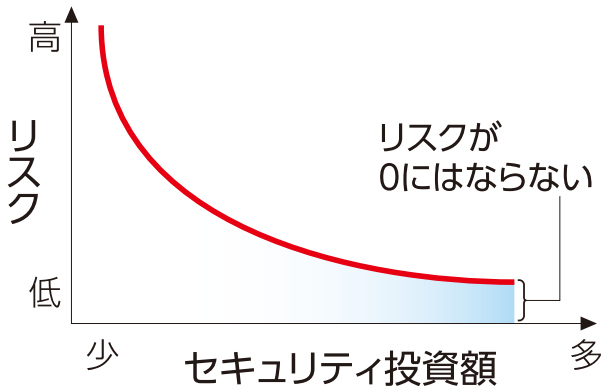
- ■ 組織的対策
- ■ 人的対策
- ■ 物理的対策
- ■ 技術的対策

詳しくはP.7へ

❼

❽

リスクとセキュリティ投資額の関係



一方、企業がどれだけ対策をしても、攻撃する側も日々巧妙化しているため、リスクはなくならないのです。

え!?
そうなの??

それでも発生してしまう不正アクセスなどの可能性に気づいたら、すぐに調査・対応をすることが重要ですが、可能性の段階で調査費用を支出するという判断は難しいですよね。
そんなとき、保険の活用も有効な手段の1つですよ!

❾

なるほど。じゃあ、IT担当者と一緒にもっと詳しい話を聞きたいな。

詳しくは東京海上日動にお問い合わせください

❿

サイバー攻撃の種類と動向

標的型メール攻撃

「標的型メール攻撃」とは、特定の組織や情報を狙って、業務を装ったメールを送り、メールの添付ファイルやリンク先に埋め込まれたウイルスに感染させること。

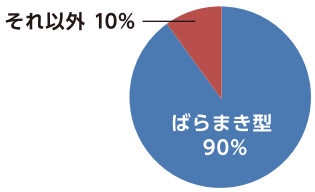
＜影響の例＞ ●機密情報・個人情報などの情報漏えい ●アカウントの乗っ取り ●ランサムウェア感染

攻撃の動向

警察庁の統計データでは、2018年の標的型メール攻撃件数6,740件(P.1参照)のうち、ばらまき型攻撃※が全体の90%を占める。

※同じ文面や不正プログラムが10ケ所以上に送付された攻撃

ばらまき型とそれ以外の標的型メール攻撃の割合



出典：警察庁「平成30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」をもとに弊社作成

Check!
ばらまき型攻撃は、無差別に送信されるため企業規模を問わず標的となります。

対策例

- メールフィルタリングソフト・アンチマルウェアソフトの導入
- OSを最新の状態にアップデートする
- 従業員教育（不審なメールを開かない・開いたらすぐに報告する）

ランサムウェア

「ランサムウェア」とは、パソコンに保存しているファイルやハードディスク等が暗号化されるなど使用不能となり、パソコンの画面上で元に戻すことと引き換えに「身代金」を要求される、身代金要求型ウイルス。

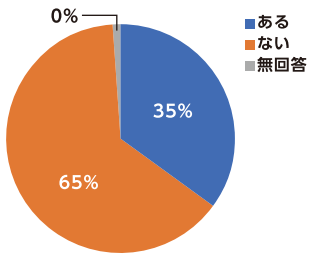
＜影響の例＞ ●重要データの消失 ●業務の停止

攻撃の動向

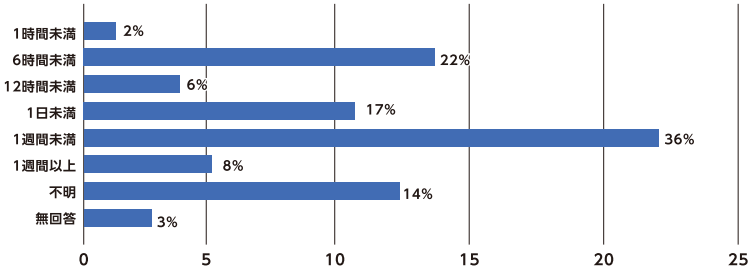
JPCERT コーディネーションセンターのアンケート調査によると、35%の組織がランサムウェアの被害にあったことがあると回答。復旧までにかかった時間は、1日～1週間未満が一番多く、1週間以上かかったケースもある。

Check!
個人情報を保有しているかどうかにかかわらず、ランサムウェアの標的になります。

ランサムウェアの感染被害の有無



業務が復旧するまでにかかった時間



出典：JPCERT コーディネーションセンター「ランサムウエアの脅威動向および被害実態調査報告書」(https://www.jpcert.or.jp/research/Ransom-survey.pdf)

対策例

- 標的型メール攻撃への対策
- 従業員教育（不審なサイトを閲覧しない）
- ランサムウェアの感染に備えて定期的に重要データのバックアップを取る

Point
バックアップは外部媒体に保存し、パソコンから切り離しておきましょう。

ウェブサイトの改ざん

「ウェブサイトの改ざん」とは、第三者により、ウェブサイトの内容が書き換えられる、またはウェブサイトにウイルス等を埋め込まれること。

＜影響の例＞ ●個人情報・クレジットカード情報などの漏えい ●閲覧者のパソコンへのウイルス感染
●ECサイトの一時閉鎖による販売減

攻撃の動向

業種	中小企業の事故事例
衣料品通信販売	オンラインショップが不正アクセスを受け、不正なプログラムを設置されたことにより、クレジットカード入力画面の情報が流出。 ＜原因＞ウェブアプリケーションの脆弱性
雑貨通信販売	オンラインショップが不正アクセスにより一部改ざんされ、顧客のクレジットカード情報（クレジットカードの名義・番号・有効期限・セキュリティコードなど）が流出。 ＜原因＞システムの脆弱性
専門機器通信販売	オンラインショップが不正アクセスを受け、顧客のクレジットカード情報（クレジットカードの名義・番号・有効期限・セキュリティコードなど）が流出。 ＜原因＞ウェブアプリケーションの脆弱性

出典:各社ウェブサイトをもとに弊社作成

対策例

- WAF（ウェブアプリケーションファイアウォール）の導入
- CSM（コンテンツマネジメントシステム）のアップデート
- ウェブアプリケーション診断、プラットフォーム診断などのセキュリティ診断の実施

Check!
ウェブサイトの改ざんは大企業と比べてセキュリティの弱い中小企業においても、被害事例が多く発生しています。

DDoS攻撃

「DDoS攻撃」とは、「Distributed Denial of Service attack」の略。
複数のコンピューターから大量のアクセスを集中させることにより、相手のサーバーやネットワークをダウンさせる。
（1台のコンピューターから攻撃が行われる場合は、DoS攻撃という）

Check!
セキュリティの弱いコンピューターやIoT機器などがマルウェアに感染した場合、DDoS攻撃の踏み台として悪用されてしまうため、気づかないうちに自社が加害者となってしまう可能性があります。

内部不正

「内部不正」とは、役職員・退職者・委託先職員など内部者の不正によるインシデント。故意によるものだけでなく、うっかりミスによる不正も含まれる。

盗難・紛失

「盗難・紛失」とは、モバイル端末（ノートパソコンやタブレットなど）・外部記憶媒体（USBやCD-ROMなど）の盗難や紛失による情報漏えい。

もしサイバー攻撃による事故が起こったら…

中堅企業編

製造業A社の場合

会社概要

年間売上高:95億円
従業員:400名

事故内容

工場の生産ラインを管理するパソコンがランサムウェアに感染。(システムバックアップと事業継続計画(BCP)があったため、24時間で復旧できたケース)

想定される被害・影響

- 工場の生産停止:24時間
- 逸失利益:5,000万円
- 調査・復旧費用:500万円
  (フォレンジック※を行った場合)
- 納品遅れによる信用の低下

合計 5,500万円

対応の流れ(例)

ランサムウェア感染発覚 → 初動対応 感染拡大防止 → 顧客への連絡・対応 / 調査・復旧 → 再発防止 → 生産再開

小売業B社の場合

会社概要

年間売上高:360億円
従業員:200名
売上高の10%がウェブサイト経由の販売

事故内容

ウェブサイトが改ざんされ、マルウェアを埋め込まれた。

想定される被害・影響

- ウェブサイト閉鎖:10日間
- 調査・復旧費用:500万円
  (フォレンジック※を行った場合)
- 逸失利益:5,000万円
- 営業継続費用:170万円
- ウェブサイト閲覧数の減少

合計 5,670万円

対応の流れ(例)

ウェブサイト改ざんが発覚 → 初動対応 状況確認 → ウェブサイト閉鎖 → 調査 → 顧客への連絡・対応 → 再発防止 → ウェブサイト再開

教育業C社の場合

会社概要

年間売上高:75億円
従業員:300名

事故内容

標的型メール攻撃により、会員情報2万件が漏えいした。
(住所・氏名・電話番号・メールアドレス・成績等)

想定される被害・影響

- 調査・復旧費用:600万円
  (フォレンジック※を行った場合)
- 訴訟費用および損害賠償費用:60万円
- お詫び対応費用(お見舞金等):1,400万円
- コールセンター設置費用:160万円
- 新聞(全国紙)へのお詫び掲載費用:900万円
- 風評による会員数の減少

合計 3,120万円

対応の流れ(例)

標的型メールによる不正アクセス → 初動対応 被害状況確認 → 公表、顧客への連絡・対応 / 調査・復旧 → 再発防止

●被害および金額はあくまで想定です。個社の状況、事故の内容、対応業者等により変わります。
●記載の金額以外に、再発防止費用や風評による売上減少など、その他の費用や損失が発生する可能性があります。
●個人情報漏えい時のお見舞金は、1人あたり500円+諸経費としています。

もし、サイバー攻撃による事故が起こったら、どのような被害・影響が想定されるのでしょうか？
中堅企業と中小企業に分けて、具体的な例をみてみましょう。

中小企業編

食品製造業D社の場合

会社概要

年間売上高：2億円
従業員：30名

事故内容

工場の生産ラインを管理するパソコンがランサムウェアに感染。

想定される被害・影響

- 生産停止：48時間
- 逸失利益：340万円
- 調査・復旧費用：300万円
  （フォレンジック※を行った場合）
- 納品遅れによる信用の低下

合計 640万円

対応の流れ（例）

ランサムウェア感染発覚 → 初動対応 感染拡大防止 → 顧客への連絡・対応 / 調査・復旧 → 再発防止 → 生産再開

小売業E社の場合

会社概要

年間売上高：2億円
従業員：10名
売上高の80％がウェブサイト経由の販売

事故内容

ウェブサイトへの不正アクセスにより、顧客情報1,000件が流出。
（住所・氏名・電話番号・クレジットカード番号・セキュリティコード・有効期限）

想定される被害・影響

- ウェブサイト閉鎖：20日間
- 調査・復旧費用：300万円
  （フォレンジック※を行った場合）
- 逸失利益：680万円
- 営業継続費用：70万円
- お客様対応の人件費：40万円
- お詫び対応費用（お見舞金等）：70万円
- ウェブサイト閲覧数の減少

合計 1,160万円

対応の流れ（例）

顧客情報流出発覚 → 初動対応 状況確認 → ウェブサイト閉鎖 → 公表、顧客への連絡・対応 / 調査・復旧 → 再発防止 → ウェブサイト再開

※フォレンジックとは

Q.
「フォレンジック」って聞いたことがあるんだけど、具体的にどんなことをするの？
外部への委託が必要なのかな？

A.
フォレンジックとは、パソコンやネットワークのログなどの記録から法的証拠を収集・保全することです。サイバー攻撃を受けた際に、原因や感染範囲を調査するために実施します。
専用のツールや解析の技術が必要であるため、外部へ委託することが多いです。
フォレンジックを実施することで、二次被害の拡大防止や再発防止につながります。

フォレンジックの流れ（外部委託をした場合の例）

証拠保全	ハードディスクなどを専用の保全機器を用いて完全複製し、改ざんされていないことを確認
復元	専用ツールを用いて、パスワード解析・データ復元を実施
解析	専門人材が、解析ソフトを用いて、マルウェア検体の抽出や感染時刻・感染後の挙動などを解析
報告	調査結果を整理し、レポートを作成

サイバーセキュリティ対策の全体像

組織的対策

■サイバーセキュリティ対応方針
■守るべき情報資産の特定
■リスクに応じた対応計画

回避	ウェブサイトの閉鎖など
低減	マルウェア対策ソフト導入など
移転	保険の活用など
保有	影響力が小さいリスクは許容する

■リスク管理体制の構築
■緊急時対応体制整備
（定期的な演習）

人的対策

■社内規定・罰則規定の周知
■セキュリティ教育（従業員・管理職・経営層・IT担当）
■標的型メール訓練
■インシデント発生時の対応・報告要領の周知

物理的対策

■入退出の制限　■入退出ログの管理　■盗難防止

技術的対策

■アクセス制御・アクセス権限の管理
■ファイアウォールの設置
■アクセスログ・認証ログ等の取得
■通信の暗号化
■セキュリティ製品の導入（IPS/IDS、EDRなど）

※カテゴリーごとの対策例を記載しています。

「サイバーセキュリティ経営ガイドライン」とは

経済産業省と独立行政法人情報処理推進機構により、経営者のリーダーシップの下でサイバーセキュリティ対策を推進するためのガイドラインとして、2015年12月に策定され、2017年11月にはVer2.0に改訂されました。
また、解説書や中小企業向けのガイドラインも公開されています。

経営者が認識するべき3原則

1. 経営者のリーダーシップ
2. ビジネスパートナー・委託先を含めたセキュリティ対策
3. 関係者との平時からのコミュニケーション・情報共有

サイバーセキュリティ経営の重要10項目

経営者のリーダーシップ

■サイバーセキュリティリスクの管理体制構築
①リスク認識・対応方針策定　②管理体制の構築
③予算・人材の確保

■サイバーセキュリティリスクの特定と対策の実装
④リスク把握・対応計画策定　⑤リスク対応の仕組み構築
⑥セキュリティ対策のPDCAサイクル

■インシデント発生に備えた体制構築
⑦インシデント発生時の緊急対応体制の整備
⑧インシデントによる被害に備えた復旧体制の整備

サプライチェーンセキュリティ対策

⑨ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

関係者とのコミュニケーション

⑩情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

出典：経済産業省 独立行政法人情報処理推進機構「サイバーセキュリティ経営ガイドラインVer2.0」をもとに弊社作成

東京海上日動火災保険株式会社
本店　東京都千代田区丸の内1-2-1　〒100-8050　TEL.03-3212-6211（代表）
http://www.tokiomarine-nichido.co.jp/

お問い合わせ先