中小企業のための
実例で学ぶサイバーセキュリティリスク事例集

2026年　3月

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 Better Life with IT

はじめに

■中小企業の経営者・情報システム担当者の皆さま、および中小企業の支援に携わる関係機関の皆さまへ

本事例集は、「セキュリティ対策の必要性を十分に理解できているか不安」、「対策を進めたいものの、どこから取り組むべきか迷っている」企業の皆さまに向けて作成しました。

最近「サイバー攻撃」という言葉をよく耳にしますが、多くの方は「大企業の話で、中小企業には関係ない」と思いがちです。しかし、実際にはランサムウェアの被害のうち 約66%が中小企業 で発生しています。つまり、中小企業こそ「自分事」として捉える必要があります。

ところが、中小企業の被害事例や実際にどんな攻撃を受けているのかという情報は、まだあまり知られていません。そこで、経済産業省では126社を対象に調査※を行い、中小企業にどんな弱点があるのか、その弱点を狙われるとどんな被害が起きるのか、そしてどう対策すればよいのかを、できるだけわかりやすくまとめました。

本事例集を読むことで、自社の状況に置き換えて「何から始めればいいのか」「どこに注意すべきか」を具体的にイメージできるようになります。まずは「サイバー攻撃は他人事ではない」という現実を知り、なぜ対策が必要なのかを理解していただくことが目的です。そのうえで、対策のポイントも紹介しています。

※令和7年度に複数業界・規模の中小企業126社を対象にASM診断を実施。ASM診断は、インターネットから見える自社のIT資産 （サーバ、ネットワーク機器、IoT機器など）を把握し、攻撃されやすいポイントを特定する仕組み。

■本事例集の全体構成

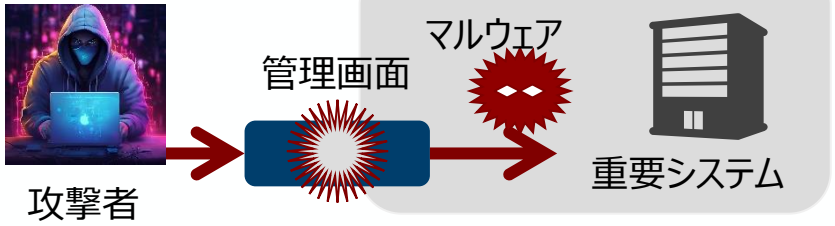
126社の調査結果を、脆弱性事例（20事例）、被害事例（5事例）、取組事例（5事例）に分類し、計30事例を紹介します。

脆弱性事例	被害事例	取組事例	コラム	業種別傾向分析
中小企業にどんな弱点があるのか、どう対策すればよいかを紹介	ヒアリングやアンケートで確認された過去のサイバー被害や同規模業種で起きた際の被害額を紹介	ヒアリングやアンケートで確認された好取組をまとめ、取組のポイントや期待される効果等を紹介	従業員教育やAI活用など最近の動向に合わせた注意事項を解説	業種別の傾向・課題・対策を解説

■事例の紹介

1 中小企業で実際に見つかった弱点を紹介

サーバの管理画面に弱点があり外部から侵入



2 中小企業のサイバー被害事例と被害額を紹介

想定被害額 **3,900万円**

初期対応費用、復旧費用、報告公表費用、弁護士訴訟費用、再発防止費用等

業務停止し**完全復旧まで2か月**要した

3 自社にあったレベルの対策が見つかる

すぐにできる対策

✓機器のIDとパスワードが**初期設定のまま**になっていないかチェック

より強固にする対策

✓トラブルが起きた時にどう対応するかの**手順書を整備**する

■本事例集の使い方

この資料は、次のような場面で活用できます。

対策アイデア・事例紹介として

他社の取組を参考に自社で出来る工夫を見つけるヒントになります。
一人情シスの工夫事例等も紹介しています。

被害リスクの説明として

中小企業でも起こり得る被害を知り、危機感を共有する助けに。
社内教育や勉強会の教材として、セキュリティ対策の必要性を伝える場面等で活用できます。

すぐ出来る対策集として

すぐに取り組める対策を見つけ、第一歩を踏み出すきっかけに。
すぐにできる対策とより強固にする対策に分けて紹介しています。

経営層への提案として

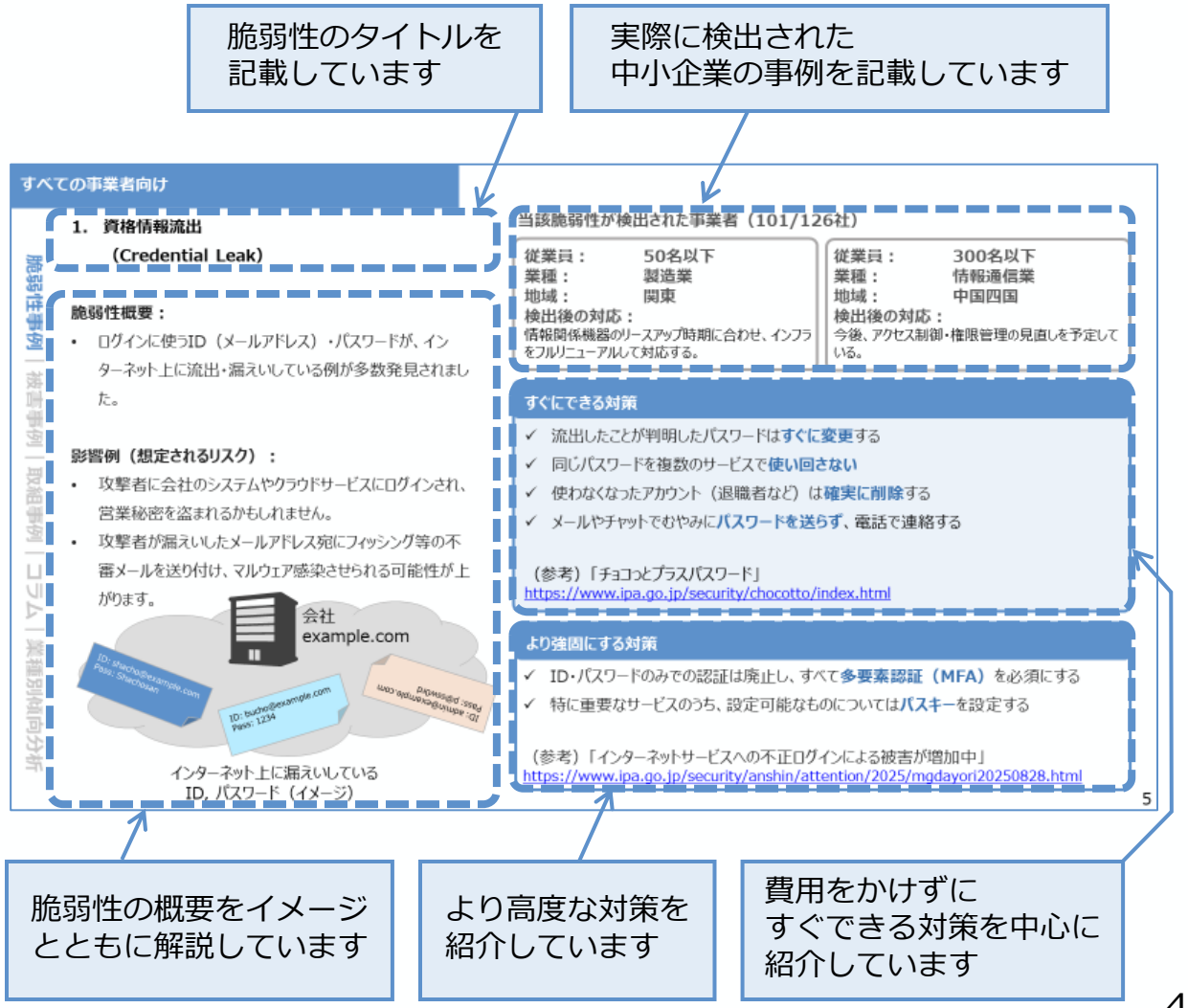
社長や経営層への相談や予算交渉の材料として必要性を訴え、予算確保の説得材料として活用できます。

上記のような使い方を通じて、この事例集は「読むだけで終わらない、実際に役立つ資料」となることを目指しています。
本書では、中小企業が直面しやすいリスクや対策を、“実際の声”としてまとめています。読み進めることで、自社に関係するポイントが自然と見つかる構成にしています。
この事例集が、皆さまのセキュリティ意識向上や日々の啓発活動の一助となりましたら幸いです。ぜひ、自社の現状確認や対策検討にお役立てください。

脆弱性事例の一覧　および　本事例の見方

- 本事業に参加した中小企業へのASM診断で実際に検出された脆弱性を紹介します。
- 脆弱性の概要や対策について紹介していますので、ご活用ください。

機密情報の漏えい	1.資格情報流出
	2.APIキー・クラウド認証情報流出
	3.リポジトリ・設定情報露出
ソフトウェアの脆弱性	4.リモートコード実行／ソフトウェア脆弱性
	5.Roundcubeウェブメールの脆弱性
	6.サポート切れソフトウェア
	7.暗号化ライブラリ脆弱性
不要な外部公開・露出	8.VPN／リモートアクセス露出
	9.FortiGate VPN／リモートアクセス露出
	10.管理パネル公開
	11.WordPress管理パネル公開
	12.管理・制御系プロトコルの外部公開
	13.機密サービスの外部公開
セキュリティ設定不備	14.DNS設定不備
	15.平文通信・暗号化不足
	16.証明書不備
	17.HTTPセキュリティヘッダ欠如
	18.Cookie属性不備
	19.メール認証レコード不備
	20.SPFメール認証レコード不備



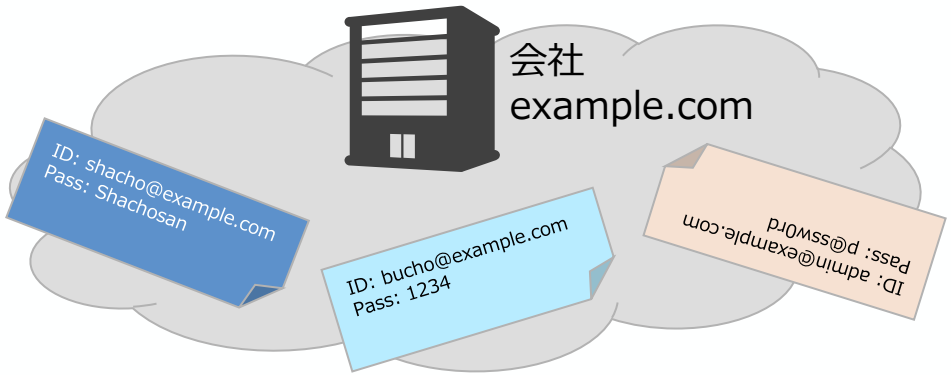
1. 資格情報流出（Credential Leak）

脆弱性概要：

- ログインに使うID（メールアドレス）・パスワードが、インターネット上に流出・漏えいしている例が多数発見されました。

影響例（想定されるリスク）：

- 攻撃者に会社のシステムやクラウドサービスにログインされ、営業秘密を盗まれるかもしれません。
- 攻撃者が漏えいしたメールアドレス宛にフィッシング等の不審メールを送り付け、マルウェア感染させられる可能性が上がります。



インターネット上に漏えいしている
ID, パスワード（イメージ）

当該脆弱性が検出された事業者（101/126社）

従業員：	50名以下
業種：	製造業
地域：	関東

検出後の対応：
情報関係機器のリースアップ時期に合わせ、インフラをフルリニューアルして対応する。

従業員：	300名以下
業種：	情報通信業
地域：	中国四国

検出後の対応：
今後、アクセス制御・権限管理の見直しを予定している。

すぐにできる対策

- ✓ 流出したことが判明したパスワードは**すぐに変更**する
- ✓ 同じパスワードを複数のサービスで**使い回さない**
- ✓ 使わなくなったアカウント（退職者など）は**確実に削除**する
- ✓ メールやチャットでむやみに**パスワードを送らず**、電話で連絡する

（参考）「チョコっとプラスパスワード」
https://www.ipa.go.jp/security/chocotto/index.html

より強固にする対策

- ✓ ID・パスワードのみでの認証は廃止し、すべて**多要素認証（MFA）**を必須にする
- ✓ 特に重要なサービスのうち、設定可能なものについては**パスキー**を設定する

（参考）「インターネットサービスへの不正ログインによる被害が増加中」
https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html

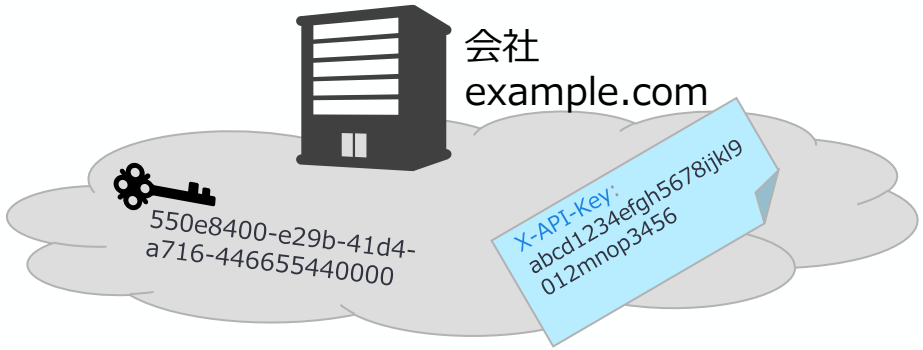
2. APIキー・クラウド認証情報流出（API Key Leak）

脆弱性概要：

- クラウドや外部サービスを使うためのAPIキー・認証情報（鍵）が、外部に流出しています。

影響例（想定されるリスク）：

- 攻撃者に流出した鍵を使用したクラウドサービスに不正アクセスされ、データの読み取り・コピーによる情報漏えい、改ざんされる可能性があります。
- 攻撃者にクラウドに侵入され、不正に仮想通貨マイニングなどをされた結果、高額請求が発生する可能性があります。



インターネット上に漏えいしている
APIキー・認証情報（イメージ）

当該脆弱性が検出された事業者（8/126社）

従業員：	20名未満
業種：	情報通信業
地域：	関東

検出後の対応：
検出結果を受け、念のためWebサイトにおけるGoogleマップの表示を見合わせた。

従業員：	50名以下
業種：	金融業・保険業
地域：	関東

検出後の対応：
外部サービスのアクセスに多要素認証を導入した。

すぐにできる対策

- ✓ 流出の可能性のあるキーを確認し、本来秘密にすべきシークレットが漏れていることが判明した場合は**すぐに無効化**し、新しいものを発行する
- ✓ 新しいキーを作成する際は**最低限の権限だけを付与**する
- ✓ 不審なAPI呼び出しがないか**利用ログを確認**する

（参考）「中小企業のためのクラウドサービス安全利用の手引き」
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000072150.pdf

より強固にする対策

- ✓ APIキーを**定期的に変更**する
- ✓ AWS Secrets Managerなどの**「秘密情報を安全に保管するサービス」**を使う

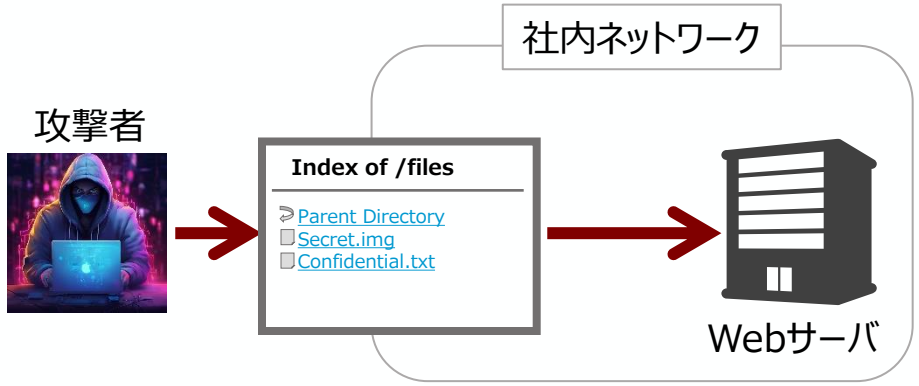
3. リポジトリ・設定情報露出（Repo / Config Exposure）

脆弱性概要：

- サーバ上のフォルダ構成、内部ファイルのパスなどがWebから確認できる状態になっています。

影響例（想定されるリスク）：

- 攻撃者にサーバのOS・ミドルウェア構成やディレクトリ構造を確認されることで、攻撃の足掛かりになるシステムの構造や弱点、侵入方法を見つけられ、既知の脆弱性と組み合わせて悪用されやすくなります。



Webサーバのフォルダ構成が見えてしまうと
攻撃者に手がかりを与える

当該脆弱性が検出された事業者（13/126社）

従業員：	100名以下
業種：	製造業
地域：	中国四国

検出後の対応：
フォルダ内のファイル一覧がブラウザに表示されないよう設定変更をベンダーに依頼中。

従業員：	20名未満
業種：	金融業・保険業
地域：	九州沖縄

検出後の対応：
内部ファイルパスがエラーメッセージで表示されないよう、設定変更をベンダーに相談中。

すぐにできる対策

- ✓ Webサーバを**フォルダ構成が表示されない設定**に変更する
  （ディレクトリリスティングを無効化する）
- ✓ アクセスが可能な**IPアドレスを限定**する
- ✓ Webサーバに**機密ファイルを置かない**
  （公開を想定していないファイルを、Web公開用のディレクトリ以下に置かない）

より強固にする対策

- ✓ 詳細な**エラー情報はサーバ側ログのみに出力**する設定にする
- ✓ エラー画面に余計な情報が表示されていないか**定期的な確認**を行う

（参考）「安全なウェブサイトの作り方」2.1 ウェブサーバに関する対策
https://www.ipa.go.jp/security/vuln/websecurity.html

4. リモートコード実行／ソフトウェア脆弱性（RCE / App Vuln）

脆弱性概要：

- OpenSSH（広く使われている暗号化プログラム）に、攻撃者がサーバの中で自由に悪意のあるプログラムを動かせてしまう脆弱性が発見されました。
- 多くのソフトウェアにおいて、常に新しい脆弱性が発見され、その都度メーカーにより修正されています。

影響例（想定されるリスク）：

- 攻撃者によりサーバが乗っ取られて、データを盗まれたり、書き換えられたり、ランサムウェアによるファイル暗号化、身代金要求が行われる可能性があります。

脆弱性を利用した攻撃例

当該脆弱性が検出された事業者（8/126社）

従業員：	300名以下
業種：	情報通信業
地域：	関東

検出後の対応：
OS・アプリケーションの更新（脆弱性修正プログラム適用含む）を実施した。

従業員：	50名以下
業種：	製造業
地域：	近畿

検出後の対応：
利用していないサービスの無効化・利用停止を実施した。

すぐにできる対策

- ✓ OSやソフトウェアのバージョンを一覧にして、**古いものを把握**する
  （MyJVNの活用もおすすめです。https://jvndb.jvn.jp/apis/myjvn/）
- ✓ OSやソフトウェアを常に**最新の状態**に保つ
- ✓ メーカーの「セキュリティ情報」を**定期的にチェック**する

（参考）「情報セキュリティ5か条」 No.1
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

より強固にする対策

- ✓ アップデートやパッチを当てる**頻度・手順を決めて**実行する
- ✓ 外部の専門家と連携して、**弱点を定期的に確認**する（脆弱性診断等）

（参考）「脆弱性診断内製化ガイド」
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2025/Vulnerability-assessment.html

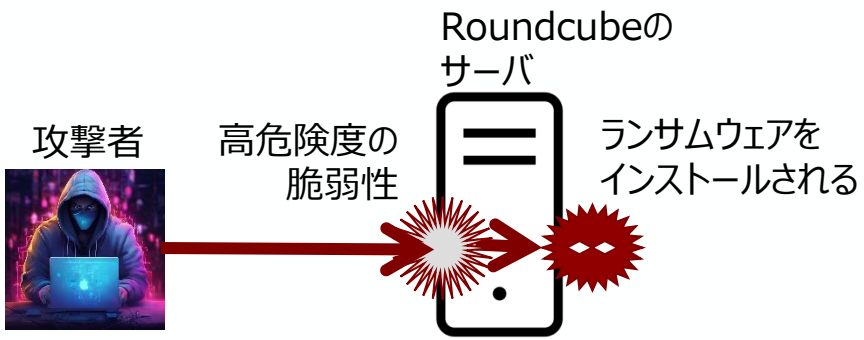
5. Roundcubeウェブメールの脆弱性

脆弱性概要：

- Roundcubeウェブメールに、サーバ上で特別なリクエストを送ることで自由に悪意のあるプログラムを動かせてしまう脆弱性が見つかっています。

影響例（想定されるリスク）：

- 攻撃者にメールアカウントだけではなく、サーバそのものを乗っ取られ、データを盗まれたり、書き換えられたり、ランサムウェアによるファイル暗号化、身代金要求が行われる可能性があります。



Roundcubeの脆弱性を利用した攻撃例

当該脆弱性が検出された事業者（1/126社）

従業員：	50名以下
業種：	金融業・保険業
地域：	近畿

すぐにできる対策

- ✓ Roundcubeが**最新バージョンにアップデート**されていることを確認する
- ✓ ベンダーの脆弱性情報を**定期的にチェック**する

（参考）「情報セキュリティ5か条」 No.1
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

より強固にする対策

- ✓ すべての管理者アカウントに**多要素認証（MFA）**の設定を行う
- ✓ ユーザアクセス許可が適切なものであるかどうかを**定期的にレビュー**する

（参考）「インターネットサービスへの不正ログインによる被害が増加中」
https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html

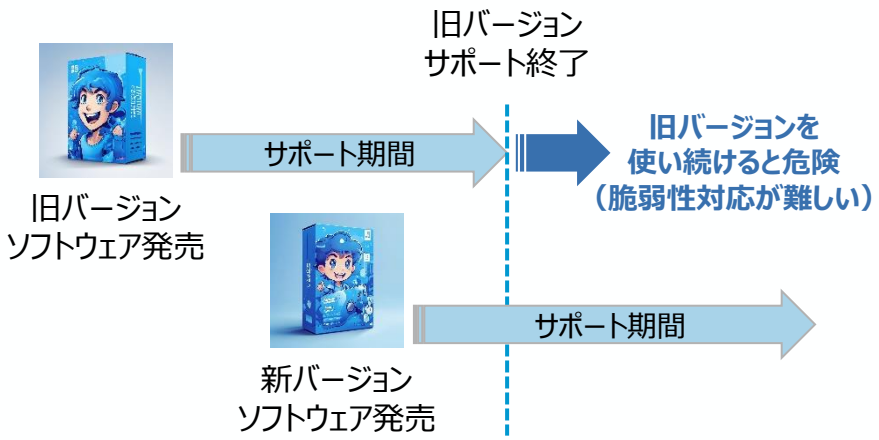
6. サポート切れソフトウェア（End-of-Life）

脆弱性概要：

- サポート期間が終了したソフトウェア（OSやアプリケーション）が使用されています。

影響例（想定されるリスク）：

- 今後新たに発見された脆弱性に対するセキュリティパッチ（修正ソフトウェア）が提供されず、新しい攻撃手法に対して無防備となり、攻撃者による侵入や情報漏えいを食い止められない可能性があります。



一般的なソフトウェアのサポート期間の例

当該脆弱性が検出された事業者（1/126社）

従業員： 20名未満
業種： 金融業・保険業
地域： 関東
検出後の対応：
セキュリティ更新（脆弱性修正）プログラム適用管理について課題を感じており、今後セキュリティ対策ツール・サービスの導入にて対応予定。

すぐにできる対策

- ✓ サポートが終わった、またはもうすぐ終わる**ソフトウェアを一覧にする**
  （MyJVNの活用もおすすめです。https://jvndb.jvn.jp/apis/myjvn/）
- ✓ 新しいバージョンや別ソフトウェアへの**移行計画を作る**
  新バージョン発売から旧バージョンサポート終了までの間に移行完了できるような計画を立てることが大切です

より強固にする対策

- ✓ やむを得ず古いシステムを使い続ける場合は**ネットワークを隔離**する
- ✓ 使用中のソフトウェアのサポート期間の把握を**ルール化、仕組み化**する

（参考）「Windows 10 のサポート終了に伴う注意喚起」
https://www.ipa.go.jp/security/security-alert/2024/win10_eos.html

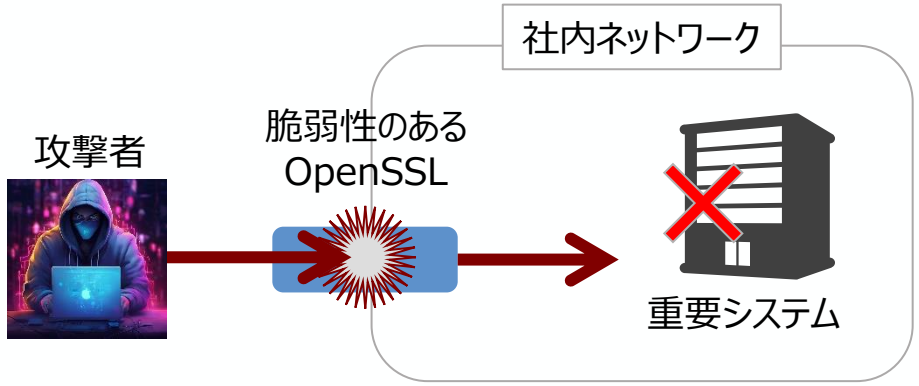
7. 暗号化ライブラリ脆弱性（Crypto Library Vuln）

脆弱性概要：

- OpenSSL（通信を暗号化するためのソフトウェア）に、攻撃者によってサーバ停止を引き起こすことができる脆弱性があります。

影響例（想定されるリスク）：

- 攻撃者が細工したメッセージを送信することにより、暗号化通信プログラムが異常停止し、サービスの停止が引き起こされる恐れがあります。



攻撃者が細工したメッセージによって
重要システムが異常停止させられる

当該脆弱性が検出された事業者（2/126社）

従業員：	300名以下
業種：	情報通信業
地域：	九州沖縄
検出後の対応：	OSの更新とあわせてOpenSSLのアップデートを行う予定。

従業員：	300名以下
業種：	卸売業・小売業
地域：	関東

すぐにできる対策

- ✓ OpenSSLが**最新バージョンにアップデート**されていることを確認する
- ✓ ベンダーの脆弱性情報を**定期的にチェック**する

（参考）「情報セキュリティ5か条」 No.1
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

より強固にする対策

- ✓ アップデートやパッチを当てる**頻度・手順を決めて**実行する
- ✓ 外部の専門家と連携して、弱点を**定期的に確認**する（脆弱性診断等）

（参考）「脆弱性診断内製化ガイド」
https://www.ipa.go.jp/jinzai/ics/core_human_resource/final_project/2025/Vulnerability-assessment.html

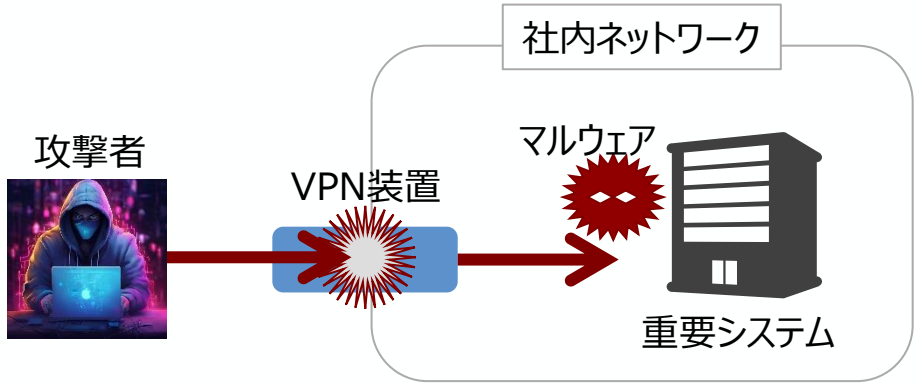
8. VPN／リモートアクセス露出（VPN Exposure）

脆弱性概要：

- 社外ネットワークから社内ネットワークへ入るためのVPN装置の存在が外部から確認できる状態になっています。

影響例（想定されるリスク）：

- 攻撃者がVPN装置の脆弱性を悪用して社内ネットワークに侵入し、多数のサーバやPCをまとめて乗っ取られ、ランサムウェアによるファイル暗号化、身代金要求を行う可能性があります。



VPN装置が攻撃者の侵入口となり、
重要システムにマルウェアを仕掛けられる原因となる

当該脆弱性が検出された事業者（10/126社）

従業員：	100名以下
業種：	情報通信業
地域：	中国四国

検出後の対応：
今後、アクセス制御・権限管理の見直しを予定している。

従業員：	300名以下
業種：	金融業・保険業
地域：	北海道東北

すぐにできる対策

- ✓ VPN機器のソフトウェアを**常に最新の状態**に保つ
- ✓ 初期ユーザ名や弱いパスワードは**使わない**
- ✓ 使っていないアカウントは**削除**する

（参考）「情報セキュリティ5か条」 No.1, No.3
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

より強固にする対策

- ✓ VPNのログインに**多要素認証（MFA）**を必須にする
- ✓ **ゼロトラスト**型のリモートアクセスへの移行を検討する

（参考）「インターネットサービスへの不正ログインによる被害が増加中」
https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html

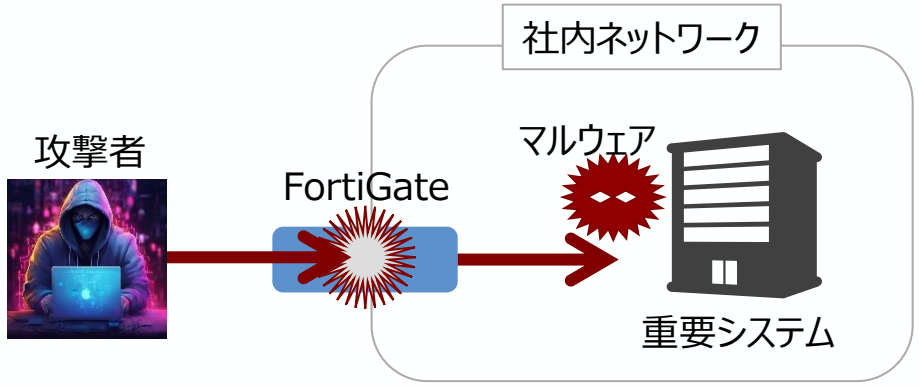
9. FortiGate VPN／リモートアクセス露出（VPN Exposure）

脆弱性概要：

- 社外ネットワークから社内ネットワークへ入るためのVPN装置として使われるFortinetデバイスのFortiManager（FGFM）プロトコルがインターネットに公開されています。

影響例（想定されるリスク）：

- 攻撃者が社内ネットワークに侵入し、多数のサーバやPCをまとめて乗っ取られ、ランサムウェアによるファイル暗号化、身代金要求が行われる可能性があります。



FortiGateが攻撃者の侵入口となり、
重要システムにマルウェアを仕掛けられる原因となる

当該脆弱性が検出された事業者（8/126社）

従業員：	100名以下
業種：	製造業
地域：	中国四国
検出後の対応：	脆弱性修正プログラムを適用し、VPN方式変更を業者に依頼中。

従業員：	50名以下
業種：	製造業
地域：	関東
検出後の対応：	情報インフラの刷新に向けた計画を策定中。

すぐにできる対策

- ✓ Fortinet製品のソフトウェアを脆弱性が修正された**最新版にバージョンアップ**する
- ✓ 初期ユーザ名や弱いパスワードは**使わない**
- ✓ 使っていないアカウントは**削除**する

（参考）「情報セキュリティ5か条」 No.1, No.3
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

より強固にする対策

- ✓ VPNのログインに**多要素認証（MFA）**を必須にする
- ✓ **ゼロトラスト**型のリモートアクセスへの移行を検討する

（参考）「インターネットサービスへの不正ログインによる被害が増加中」
https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html

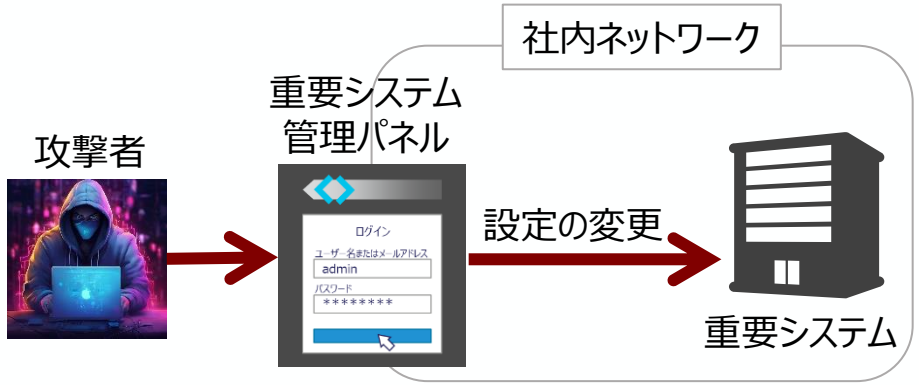
10. 管理パネル公開
（Admin Panel Exposure）

脆弱性概要：

- 重要システムの管理画面がインターネットから誰でも開ける状態で、攻撃者がログイン画面まで簡単にたどり着ける状態になっています。

影響例（想定されるリスク）：

- 攻撃者によってパスワードを総当たりで試されたり、既知の脆弱性を悪用されて、重要システムの設定を勝手に変えられたり、システムを乗っ取られるおそれがあります。



重要システムの管理パネルにアクセスされ
攻撃者に設定を変更される

当該脆弱性が検出された事業者（18/126社）

従業員：	300名以下
業種：	製造業
地域：	近畿

検出後の対応：
アクセス制御、権限管理の見直しを行った。

従業員：	50名以下
業種：	金融業・保険業
地域：	関東

検出後の対応：
日頃から経営層のセキュリティ意識が高く、検出結果を受けて多要素認証（MFA）の導入を行った。

すぐにできる対策

- ✓ 管理画面は**社内からのみアクセス**できるようにする
- ✓ 初期設定の**ID・パスワードは必ず変更**する
- ✓ 管理画面の**URLを推測しにくいものに変える**
- ✓ ソフトウェアを常に**最新版にバージョンアップ**する（別紙に参考URLがあります）

（参考）「情報セキュリティ5か条」 No.1, No.3
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

より強固にする対策

- ✓ 管理者アカウントに**多要素認証（MFA）**を必須にする
- ✓ 管理操作の**ログを残し、定期的にチェック**する

（参考）「インターネットサービスへの不正ログインによる被害が増加中」
https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html

11. WordPress管理パネル公開
（WordPress Admin Panel Exposure）

脆弱性概要：

- WordPressの管理画面がそのまま外部に公開されており、攻撃者がログイン画面に容易にアクセスできます。

影響例（想定されるリスク）：

- 攻撃者によってパスワードを総当たりで試され、侵入される可能性が高くなります。
- 攻撃者にWebサイトを書き換えられたり、マルウェアを仕込まれたりする可能性があります。

攻撃者にWordPressの管理パネルから侵入され
Webサイトを書き換えられる

当該脆弱性が検出された事業者（5/126社）

従業員：	20名未満
業種：	金融業・保険業
地域：	関東

検出後の対応：
検出結果を受け、WordPressの管理用URLの変更を行う予定。

従業員：	300名以下
業種：	情報通信業
地域：	関東

検出後の対応：
セキュリティ対策サービスの導入の予定があり、本脆弱性への対応もあわせて検討している。

すぐにできる対策

- ✓ 管理画面は**社内からのみアクセス**できるようにする
- ✓ 管理ユーザ名を**デフォルトの「admin」から変更する**
- ✓ 管理用URLを**デフォルトの「/wp-admin/」「/wp-login.php」から変更する**
- ✓ WordPressを常に**最新版にバージョンアップ**する（別紙に参考URLがあります）

（参考）「情報セキュリティ5か条」 No.1, No.3
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

より強固にする対策

- ✓ 管理者アカウントに**多要素認証（MFA）**を必須にする
- ✓ 管理操作の**ログを残し、定期的にチェック**する

（参考）「インターネットサービスへの不正ログインによる被害が増加中」
https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html

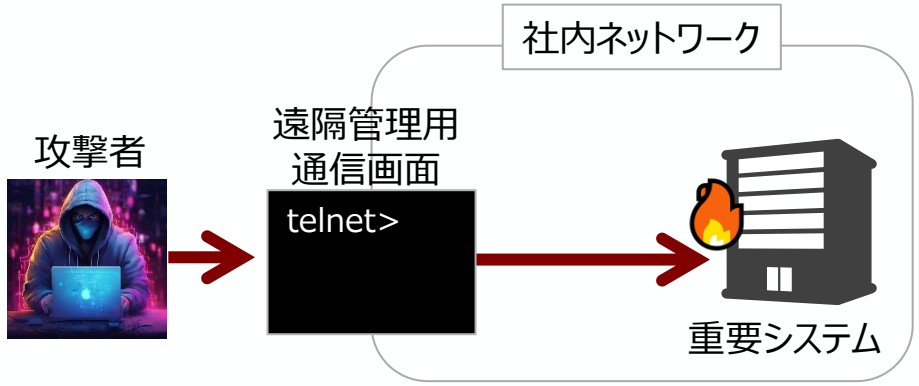
12. 管理・制御系プロトコルの外部公開（Management Protocol Exposure）

脆弱性概要：

- SSH、RDP、Telnet、SNMPなど、一般的に機器を遠隔管理・制御するために使う通信を、インターネットから直接行うことができる状態になっています。

影響例（想定されるリスク）：

- 攻撃者に社内ネットワークに関する詳細な情報を与えてしまい、パスワードを総当たりで試されたり、脆弱性を悪用されて、サーバやネットワーク機器を完全に乗っ取られるおそれがあります。



重要システムの遠隔管理用通信画面に
社外の攻撃者から直接アクセスされる

当該脆弱性が検出された事業者（2/126社）

従業員：	20名未満
業種：	金融業・保険業
地域：	関東

検出後の対応：
検出結果を受け、セキュリティ対策ツールの導入を検討中。

従業員：	300名以下
業種：	金融業・保険業
地域：	北海道東北

すぐにできる対策

- ✓ 使用していない場合※は**サービスを無効**にする
- ✓ 必要がない場合、外部からのアクセスを**ファイアウォールで遮断**する
- ✓ アクセスが可能な**IPアドレスを限定**する
- ✓ ソフトウェアを常に**最新版にバージョンアップ**する

※保守事業者がリモートメンテナンスのために使用している可能性もあるので注意してください

（参考）「情報セキュリティ5か条」 No.3
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

より強固にする対策

- ✓ VPNを経由しない**社外からのアクセスを拒否**する
- ✓ （SNMPの場合）**v3対応機器を使用**して認証・暗号の設定を行う

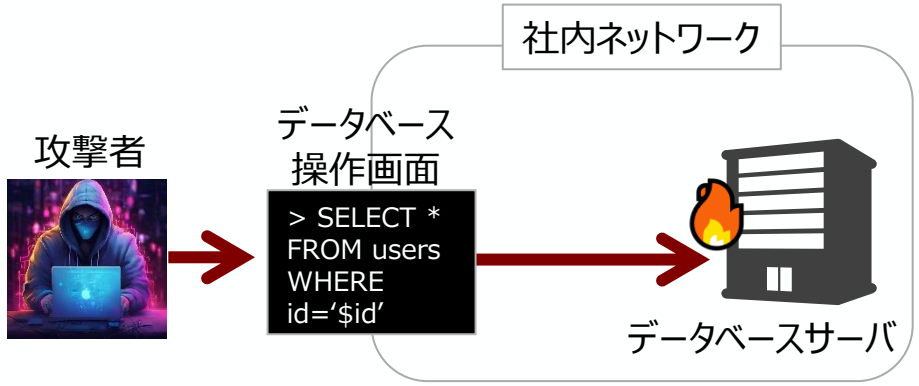
13. 機密サービスの外部公開
（Database / Service Exposure）

脆弱性概要：

- データベースサーバに対し、インターネットから直接アクセスできる状態になっています。

影響例（想定されるリスク）：

- 外部の攻撃者からデータベースサーバに直接アクセスされ、パスワードを総当たりで試されたり、脆弱性を悪用されて、機密情報を盗まれたり、書き換えられたりします。



機密情報のデータベースに
社外の攻撃者から直接アクセスされる

当該脆弱性が検出された事業者（8/126社）

従業員：	50名以下
業種：	製造業
地域：	近畿
検出後の対応：	検出結果を受け、利用していないデータベースサーバの停止を検討中。

従業員：	300名以下
業種：	製造業
地域：	近畿
検出後の対応：	データベースサーバのアプリケーションの更新を行い、脆弱性修正プログラムを適用した。

すぐにできる対策

- ✓ 必要がない場合、外部からのアクセスを**ファイアウォールで遮断**する
- ✓ データを暗号化するとともに、各ユーザに**必要最小限の権限**を与える
- ✓ 接続ログを有効にして、**攻撃者によるアクセスがないか定期的に確認**する
- ✓ ソフトウェアを常に**最新版にバージョンアップ**する

（参考）「情報セキュリティ5か条」 No.3
https://www.ipa.go.jp/security/sme/f55m8k0000001wb3-att/000055516.pdf

より強固にする対策

- ✓ データベースサーバを**社外から直接アクセスできないネットワークに配置**する
- ✓ 利用している**SQL文にSQLインジェクションなどの脆弱性がないことを確認**する

（参考）「安全なSQLの呼び出し方」
https://www.ipa.go.jp/security/vuln/websecurity.html

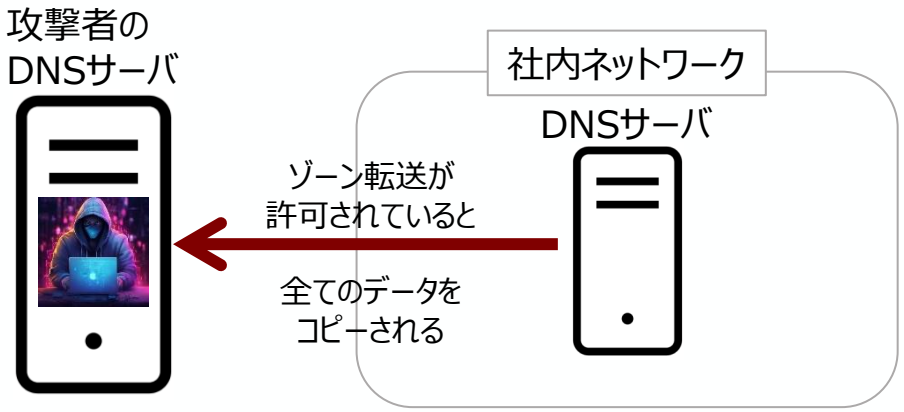
14. DNS設定不備
（DNS Misconfiguration）

脆弱性概要：

- DNS（ドメイン名とIPアドレスを対応させる仕組み）の設定ミスにより、内部情報が漏れたり悪用されやすい状態になっています。

影響例（想定されるリスク）：

- 攻撃者によって、IPアドレスやコンピュータホスト名を含む、詳細な社内ネットワークのデータを取得され、脆弱性を悪用した侵入の手がかりを与えてしまう可能性があります。



DNSサーバが持つ社内ネットワーク情報を
攻撃者から全て抜き取られてしまう

当該脆弱性が検出された事業者（3/126社）

従業員：	20名未満
業種：	金融業・保険業
地域：	九州沖縄

検出後の対応：
DNSの設定変更についてベンダーに相談中。

従業員：	300名以下
業種：	製造業
地域：	近畿

すぐにできる対策

✓ 必要のないIPアドレスからの
ゾーン転送（DNSの中身を丸ごと送信する機能）を拒否する設定にする
一般的には
プライマリサーバはセカンダリサーバのIPアドレスのゾーン転送要求のみ許可
セカンダリサーバは全てのIPアドレスからのゾーン転送要求を拒否　となります

より強固にする対策

✓ DNSサーバの設定不備と直接の関係はありませんが、**DNSSECを導入**することで、DNSに関係する典型的な攻撃（DNSキャッシュポイズニングなど）を防ぐことができます。

（参考）「安全なウェブサイトの作り方」2.2 DNS に関する対策
https://www.ipa.go.jp/security/vuln/websecurity.html

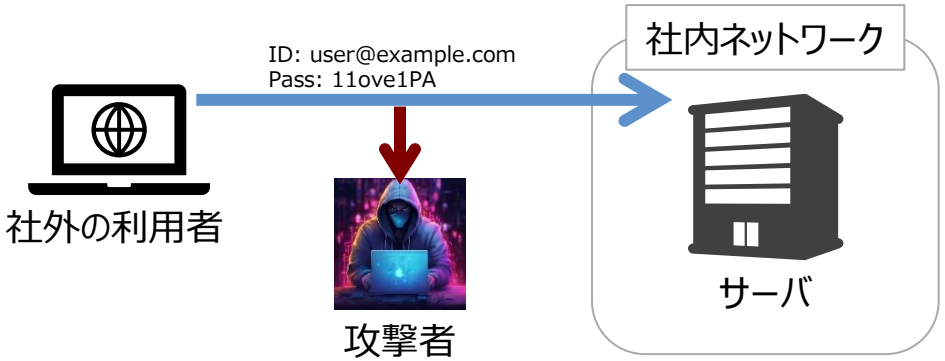
15. 平文通信・暗号化不足（Unencrypted Communication）

脆弱性概要：

- 暗号化されていない通信を使っていて、ユーザ名、パスワード、通信内容などが攻撃者から容易に確認できる状態になっています。

影響例（想定されるリスク）：

- 攻撃者により個人情報を通信経路上で盗み見られる、送受信者の間に入ってなりすましされるなどのリスクがあります。
- ID・パスワードや機密情報がネットワーク上で盗み取られると、不正ログインや情報漏えいにつながります。



通信経路が暗号化されていないと
攻撃者に重要情報を盗み見られる

当該脆弱性が検出された事業者（120/126社）

従業員：	300名以下
業種：	情報通信業
地域：	関東

検出後の対応：
Email, HTTP, FTPの通信が暗号化されるように設定を変更した。

従業員：	20名未満
業種：	情報通信業
地域：	関東

検出後の対応：
Email, HTTP, FTPの通信が暗号化されるように設定を変更した。

すぐにできる対策

- ✓ Webブラウザにおいて**暗号化されていない通信をさせない**設定にする
  （「常に安全な接続を使用する」設定をオンにする）
- ✓ Webサイト全体を**HTTPS(暗号化HTTP)**にする

（参考）「TLS暗号設定ガイドライン」
https://www.ipa.go.jp/security/crypto/guideline/ssl_crypt_config.html

より強固にする対策

- ✓ メール送受信を行うサーバに対し、**暗号化通信を行うための適切な設定**を行う
- ✓ FTPサービスにおいて**FTPS(暗号化FTP)**を設定する

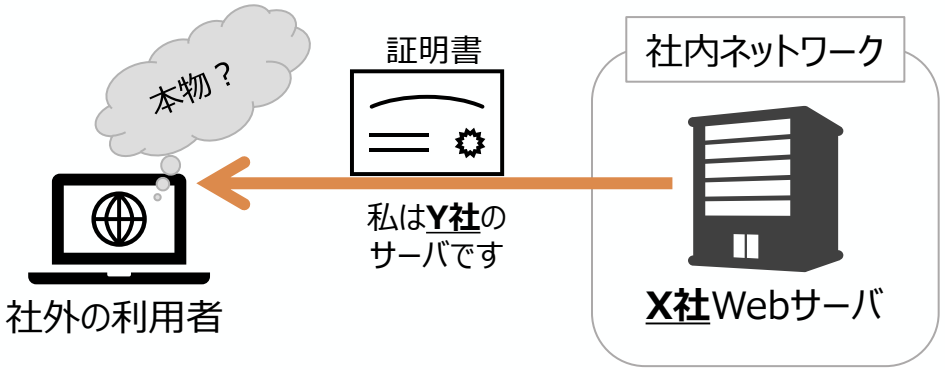
16. 証明書不備
（Certificate Misconfiguration）

脆弱性概要：

- Webサーバで使用している電子証明書に、期限切れ、サイト名との不一致などの不備がある、あるいは自己署名証明書（オレオレ証明書）が利用されており、ブラウザから「安全ではない」と警告される状態になっています。

影響例（想定されるリスク）：

- 自社のWebサーバが正規のものであることを証明できないため、アクセスしてきた利用者が、攻撃者が設置したフィッシングサイトに誘導されるリスクが高くなります。



不備がある証明書では
Webサーバが本物であることを証明できない

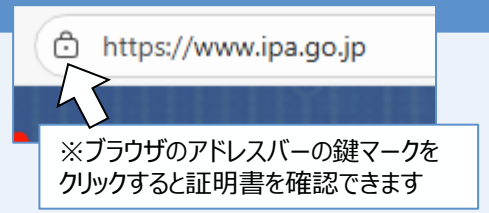
当該脆弱性が検出された事業者（106/126社）

従業員：	20名未満
業種：	金融業・保険業
地域：	九州沖縄

検出後の対応：
電子証明書の設定変更についてベンダーに相談中。

従業員：	100名以下
業種：	製造業
地域：	北海道東北

すぐにできる対策



- ✓ ブラウザの警告を無視しないよう**社内に周知**する
- ✓ 証明書が有効期限内であることを確認※し、期限切れ・期限間近の**証明書を更新**する
- ✓ 証明書の**CN/SAN（ドメイン名）の設定が正しいことを確認**する

（参考）「安全なウェブサイトの作り方」2.4 フィッシング詐欺を助長しないための対策
https://www.ipa.go.jp/security/vuln/websecurity.html

より強固にする対策

- ✓ 社内の電子証明書の一覧をまとめ、**期限を管理する体制**をととのえる
- ✓ 重要サービスに対しては**より信頼性の高い証明書（OV/EV）**を使う

17. HTTPセキュリティヘッダ欠如（Security Header Missing）

脆弱性概要：

- X-Frame-OptionsやContent-Security-Policyなど、Webサイトのセキュリティを強化するためのセキュリティヘッダが設定されていません。

影響例（想定されるリスク）：

- 攻撃者によってデータを盗み取られたり、フィッシング画面を表示され、マルウェアをインストールさせられる可能性が高くなります。

HTTPセキュリティヘッダが設定されていないと
マルウェアを送り込まれる可能性が高まる

当該脆弱性が検出された事業者（124/126社）

従業員：	20名未満
業種：	情報通信業
地域：	関東
検出後の対応：	自社でHTTPセキュリティヘッダの設定を行った。

従業員：	50名以下
業種：	金融業・保険業
地域：	北海道東北
検出後の対応：	専門業者に依頼してHTTPセキュリティヘッダの設定を行った。

すぐにできる対策

✓ HTTPセキュリティヘッダの**設定を追加**してセキュリティを向上する

Strict-Transport-Security	例：HTTPS（暗号化）通信をさせる
Content-Security-Policy	例：外部サイトの画像読込を防ぐ
X-Frame-Options Header	例：フレームを読み込ませない
X-Content-Type-Options	例： MIMEタイプの推測をとめる

（参考）「安全なウェブサイトの作り方」2.3 ネットワーク盗聴への対策
https://www.ipa.go.jp/security/vuln/websecurity.html

より強固にする対策

✓ セキュリティヘッダの**標準ルールを作り、管理する全てのWebサーバに適用**する

✓ 外部の専門家と連携して、**弱点を定期的に確認**する（脆弱性診断等）

（参考）「TLS暗号設定ガイドライン」
7.4.1 HTTP Strict Transport Security（HSTS）の設定有効化
https://www.ipa.go.jp/security/crypto/guideline/gmcbt80000005ufv-att/ipa-cryptrec-gl-3001-3.1.1.pdf

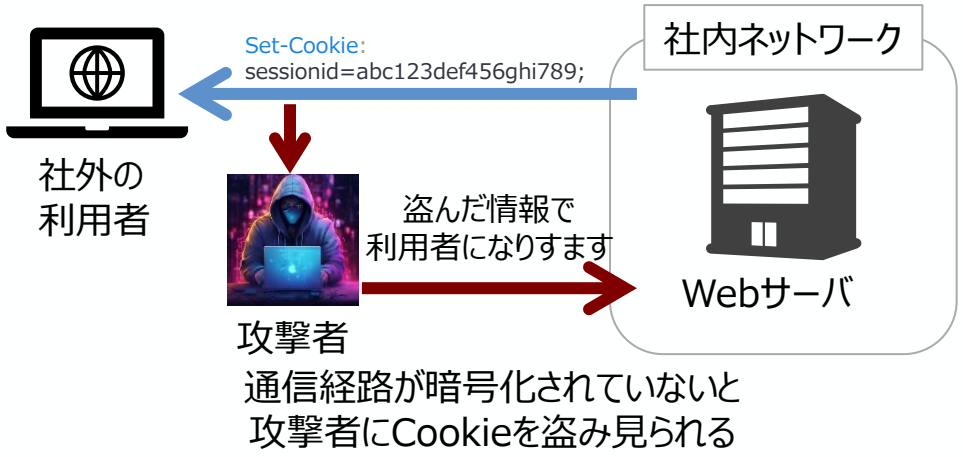
18. Cookie属性不備
（Cookie Attribute Weakness）

脆弱性概要：

- Webサイトへのログイン状態を保存する際に使われるCookieの設定がデータを盗まれやすい状態になっています。

影響例（想定されるリスク）：

- Cookieは、一度Webサイトにアクセスして IDとパスワードを入力してログインしたユーザを記録し、しばらくの間はIDとパスワードを入力せずに再アクセスできる機能に使われています。Cookieの設定に不備があると、攻撃者がログイン中のユーザになりすまして不正な操作をする危険があります。



当該脆弱性が検出された事業者（61/126社）

従業員：	20名未満
業種：	情報通信業
地域：	中国四国
検出後の対応：	セキュリティ対策ツール、サービスの導入とあわせて対応を行った。

従業員：	300名以下
業種：	情報通信業
地域：	関東
検出後の対応：	アクセス制御・権限管理とあわせて対応を行った。

すぐにできる対策

✓ セッションCookie（ログイン状態を保存する）の**設定を見直す**

Secure	暗号化通信をさせる
HttpOnly	JavaScriptなどからアクセスさせない
SameSite	別サイトからCookie情報を読み取らせない

（参考）「安全なウェブサイトの作り方」
1.4 セッション管理の不備, 1.5 クロスサイト・スクリプティング
https://www.ipa.go.jp/security/vuln/websecurity.html

より強固にする対策

✓ 不審なログインを検知して**セッションを強制終了**する仕組みを入れる

（参考）「TLS暗号設定ガイドライン」【コラム①】常時HTTPS化に伴う留意点
https://www.ipa.go.jp/security/crypto/guideline/gmcbt80000005ufv-att/ipa-cryptrec-gl-3001-3.1.1.pdf

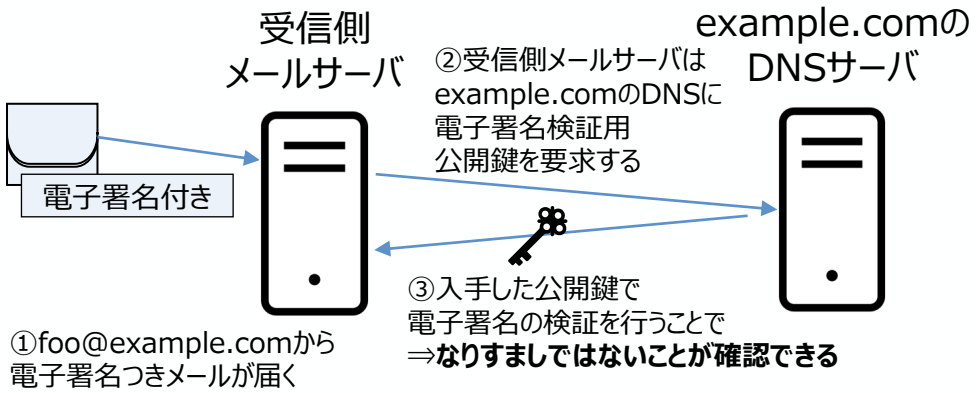
19. メール認証レコード不備（Email Auth Misconfiguration）

脆弱性概要：

- DKIM・DMARCなど、メールのなりすましを防ぐ設定が不十分で、受信者が偽メールを見分けにくい状態になっています。

影響例（想定されるリスク）：

- 自社ドメインを名乗るフィッシングメールが出回り、顧客がだまされる可能性が高くなることで、自社の評判が落ちる可能性があります。



DKIMによる署名検証の流れ

当該脆弱性が検出された事業者（112/126社）

従業員：	300名以下
業種：	製造業
地域：	関東
検出後の対応：	セキュリティ対策ツール、サービスの導入とあわせて対応を行う予定。

従業員：	50名以下
業種：	金融業・保険業
地域：	北海道東北
検出後の対応：	専門業者に確認して対応を行った。

すぐにできる対策

- ✓ DNSに**DKIMレコードを設定**する（適切な公開鍵を設定する）
- ✓ DNSに**DMARCレコードを設定**する
  （まずは影響が少ない「none」設定として、DMARCレポートの分析から始める）

より強固にする対策

- ✓ DMARC**レポートを分析**し、なりすまし送信元を特定・対処する
- ✓ DMARCの**設定を少しずつ厳格化**し、自社を騙る迷惑メールを顧客に受信させないようにする(none（何もしない）→quarantine（隔離）→reject（拒否）の順)

（参考）迷惑メール対策推進協議会「送信ドメイン認証技術導入マニュアル」
https://www.dekyo.or.jp/soudan/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf

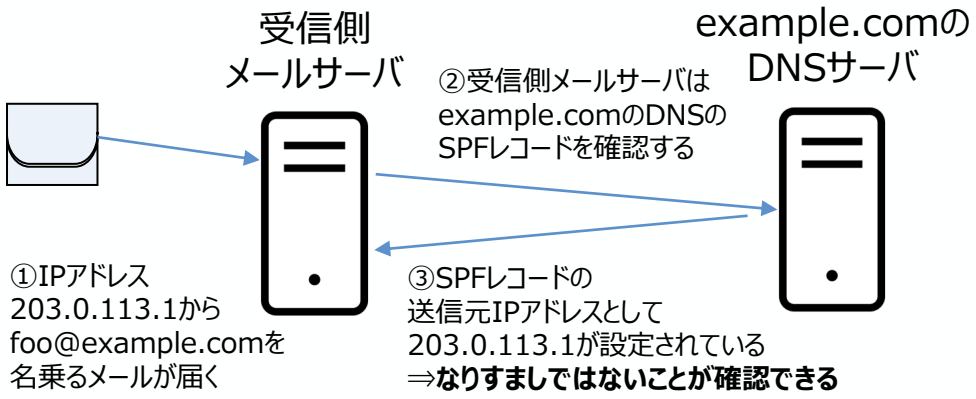
20. SPFメール認証レコード不備
（SPF Email Auth Misconfiguration）

脆弱性概要：

- SPFレコードがセキュリティ的に緩い設定になっていて、自社ドメインを騙る不正な送信元からのメールを受信者が「偽物」と判断しづらい状態になっています。

影響例（想定されるリスク）：

- 自社ドメインを名乗るフィッシングメールが出回り、顧客がだまされる可能性が高くなり、自社の評判が落ちる可能性があります。



SPFによる送信元IPアドレス確認の流れ

当該脆弱性が検出された事業者（104/126社）

従業員：	50名以下
業種：	製造業
地域：	関東

検出後の対応：
情報インフラの刷新とあわせて対応を行う予定。

従業員：	50名以下
業種：	金融業・保険業
地域：	北海道東北

検出後の対応：
専門業者に確認して対応を行った。

すぐにできる対策

✓ SPFレコードの**設定を厳格化**し、送信元IPアドレスを適切に設定する
　-all　ここに書いた送信元以外は正規の送信元ではない。拒否してよい
　　（最もセキュリティ的に望ましい設定）
　この設定を行うことで、受信者はどこから送信されたメールが本物かを確認し、なりすましメールを削除することが容易になります。

より強固にする対策

✓ SPFだけでなく、**DKIM・DMARCも合わせて運用**する
✓ DMARCレポートを確認し、送信元の設定を**継続的に見直す**

（参考）迷惑メール対策推進協議会「送信ドメイン認証技術導入マニュアル」
https://www.dekyo.or.jp/soudan/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf

- 本事業に参加した中小企業での被害事例を紹介します。　※本事例はモデルケースとして積算したものでありシナリオや被害額等には、一部想定を含みます
- 被害に至った原因、被害額、推奨する対策について紹介していますので、ご活用ください。

1．VPN装置の脆弱性悪用によるランサムウェア感染･ファイル暗号化
想定被害額　：　４，６００万円
2．クラウド設定ミスによる情報漏えい
想定被害額　：　５，３００万円
3．Webサイト改ざんによるフィッシング誘導
想定被害額　：　２，４２０万円
4．取引先を装う標的型メールでの侵入
想定被害額　：　２，３５０万円
5. 社長メールアカウント乗っ取りによる送金詐欺
想定被害額　：　８２０万円

費目	概要
費用損害	インシデント対応に必要な原因調査、フォレンジック、復旧作業、外部専門家（弁護士･コンサル）の費用、システム再構築、顧客通知やコールセンター設置費用などが含まれる。
賠償損害	インシデントにより第三者に与えた損害について、法的責任に基づき支払う金銭。個人情報漏えいによる慰謝料、取引先の業務停止に伴う損害賠償、集団訴訟の和解金などが典型例となる。
利益損害	インシデントがなければ得られたはずの利益が失われた損害。システム停止による売上減少、顧客離反による将来収益の減少、ブランド毀損に伴う取引縮小など、機会損失が挙げられる。

1．VPN装置の脆弱性悪用によるランサムウェア感染・ファイル暗号化

項目	概要	
組織情報	製造業（中国四国）	従業員数：80名
	売上規模：約10億円	端末台数：80台
体制	情報システム担当2名(他業務と兼任)	
実施していたセキュリティ対策	• ウイルス対策ソフトの導入 • オンラインバックアップの整備 • その他、年間100万円程度のセキュリティ予算	
被害経緯	• 攻撃者にVPN装置の脆弱性を悪用され、ランサムウェアに感染し、業務データが暗号化された • ウイルス対策ソフトの監視が及ばない経路で攻撃を受けた	
被害内容	**業務停止** ランサムウェア感染により設計データ・経理データが暗号化し業務が停止した **データ復旧困難** クラウドに保存したバックアップデータも暗号化され、データ復旧困難となった ⇒**一部業務が停止し、納期遅延が発生！**	
攻撃要因	• リモートワーク用VPN装置の脆弱性更新漏れ	
被害後に実施したこと	• VPN機器のファームウェア更新・設定見直し • クラウドの認証見直し • オフラインバックアップ、インシデント対応計画の整備 • セキュリティに関する定期的な教育の実施	

想定被害額（被害額の計算明細は別紙の参考資料参照） **4,600万円**

- 初期対応費用（緊急対応、記録データの調査等）・・・約3,050万円
- 復旧費用（データ復旧、サーバ再構築等）・・・約350万円
- 報告公表費用（外部コンサルタント起用等）・・・約300万円
- 弁護士訴訟費用（弁護士への相談費用等）・・・約150万円
- 再発防止費用（新しい安全対策等）・・・約750万円

※その他、利益損害・賠償請求等の費用もかかる可能性があります

すぐにできる対策

✓ VPN装置やネットワーク機器の**ファームウェア・OSを定期的に更新**する

✓ バックアップから**復旧するための手順書**を作成する

（参考）IPA「日常における情報セキュリティ対策」
3.定期的なバックアップの実施
https://www.ipa.go.jp/security/anshin/measures/everyday.html

より強固にする対策

✓ 多重化したバックアップからの復旧訓練行う

✓ 多要素認証導入し、認証強度を高める

（参考）IPA「不正ログイン対策特集ページ」
3.「多要素認証」の設定について
https://www.ipa.go.jp/security/anshin/measures/account_security.html

2．クラウド設定ミスによる情報漏えい

項目	概要	
組織情報	情報通信業（中国四国）	従業員数：100名
	売上規模：約10億円	端末台数：150台
体制	情報システム担当10名	
実施していたセキュリティ対策	• ウイルス対策ソフト・EDRの導入及びログの収集・監視 • インシデント対応計画の策定、データのバックアップ • その他、年間500万円程度のセキュリティ予算	
被害経緯	• クラウドストレージがインターネットから誰でも閲覧可能な状態になっており、外部から顧客リスト等をダウンロードされた	
被害内容	**情報漏えい** 顧客リストや取引条件が外部からダウンロードされた **信頼低下・取引停止** 取引先からの信頼が低下し、一部顧客との取引停止が発生した ⇒**情報漏えいによる信頼低下・一部顧客との取引停止！**	
攻撃要因	• クラウドストレージのアクセス権限誤設定	
被害後に実施したこと	• 個人情報保護委員会への報告、本人への通知 • クラウドストレージのアクセス権限の全社点検・再設定 • アクセス権限に関する権限設計・管理手順の文書化 • アクセスログの定期監査・自動通知設定	

想定被害額（被害額の計算明細は別紙の参考資料参照） **5,300万円**

- 初期対応費用（クラウドストレージ調査等）・・・約200万円
- 弁護士訴訟費用（弁護士への相談費用等）・・・約100万円
- 利益損害（一部顧客の取引停止）・・・約5,000万円(売上の5%)

※信頼失墜による新規受注の減少も発生する可能性があります
※その他、賠償請求等の費用もかかる可能性があります

すぐにできる対策

✓ クラウドサービスの**アクセス権限設定を定期的に確認・棚卸し**する
✓ アクセス権限管理手順の文書化

（参考）IPA「中小企業のためのクラウドサービス安全利用の手引き」
https://www.ipa.go.jp/security/sme/f55m8k0000001wpl-att/outline_guidance_cloud.pdf

より強固にする対策

✓ アクセス権限や公開設定の自動監査・異常検知ツールを導入し、設定ミスや不正アクセスを迅速に検知・通知する
✓ 重要データの分類・ラベリングを徹底し、機密度に応じたアクセス制御・暗号化を行う

3．Webサイト改ざんによるフィッシング誘導

項目	概要	
組織情報	金融・保険業（関東）	従業員数：50名
	売上規模：約4億円	端末台数：60台
体制	営業担当1名が情報システム管理を兼任	
実施していたセキュリティ対策	• ウイルス対策ソフト・UTMの導入 • インシデント対応計画の策定、データのバックアップ • その他、年間150万円程度のセキュリティ予算	
被害経緯	• 自社ウェブサイトが改ざんされ、当該ページに入力された顧客のクレジットカード情報が外部に漏えいした • 導入していたセキュリティ対策ではウェブサイトの改ざんを検知できなかった	
被害内容	**情報改ざん** 自社ウェブサイトがフィッシングサイトに改ざんされた **信頼低下・取引停止** 顧客が自社サイトに入力したクレジットカード情報が外部に漏えいした ⇒**情報改ざんにより顧客情報が漏えい！**	
攻撃要因	• ウェブサイト更新管理システムの追加機能未更新	
被害後に実施したこと	• ウェブサイト更新管理システムの追加機能更新 • ウェブアプリケーション診断の実施 • システムにログインするためのID・パスワード強化 • 顧客への状況説明及び注意喚起	

想定被害額（被害額の計算明細は別紙の参考資料参照） **2,420万円**

- 初期対応費用（緊急対応、記録データの調査等）・・・約200万円
- 報告公表費用（記録データの復旧等）　・・・約20万円
- 弁護士訴訟費用（弁護士への相談費用等）・・・約100万円
- 再発防止費用（ウェブアプリケーション診断）・・・約100万円
- 利益損害（一部顧客との取引停止）・・・約2,000万円(売上の5%)

※その他、賠償請求等の費用もかかる可能性があります

すぐにできる対策

✓ウェブサイトを作るソフトや追加機能は、こまめに**最新の状態に更新**する

✓**強固なパスワードを設定**するとともに、使っていないアカウントは都度確認し、消去する

（参考）IPA「安全なウェブサイトの作り方」
https://www.ipa.go.jp/security/vuln/websecurity/index.html

より強固にする対策

✓ウェブサイト更新管理システムに多要素認証を導入する

✓ウェブサイト改ざん検知サービスを導入する

✓ウェブサイト更新管理システムを自動で更新するように設定する

✓ウェブサイト管理業務を外部に委託する

4．取引先を装う標的型メールでの侵入

項目	概要	
組織情報	金融業・保険業	従業員数：20名
	売上規模：非公開	端末台数：20台
体制	IT部門で開発、運用、セキュリティを担当	
実施していたセキュリティ対策	• ウイルス対策ソフト、侵入検知ソフトの導入 • PC利用ログ取得及び定期的なログチェック • その他、年間50万円程度のセキュリティ予算	
被害経緯	• 従業員が取引先を装ったメールの添付ファイルを開き、端末がマルウェアに感染。社内ネットワークに感染が広がった • 導入していたマルウェア対策ソフトでは検知できない新型のマルウェアが使用されていた	
被害内容	**業務停止** 基幹システムが停止し、業務を継続することが困難となった **情報漏えい** マルウェアの影響により、顧客(契約者)の情報が外部へ流出した ⇒**復旧・調査のため数週間の業務遅延！**	
攻撃要因	• 標的型メール攻撃に関する教育不足	
被害後に実施したこと	• 不審なメールの添付ファイルを開いてしまったときの対応手順の策定 • 社員に怪しいメールや危険な操作を避けるための研修	

想定被害額（被害額の計算明細は別紙の参考資料参照） **2,350万円**

- 初期対応費用（緊急対応、記録データの調査等）・・・約1,200万円
- 復旧費用（データ復旧、サーバ再構築等）・・・約150万円
- 報告公表費用（外部コンサルタント起用等）・・・約300万円
- 弁護士訴訟費用（弁護士への相談費用等）・・・約100万円
- 再発防止費用（新しい安全対策等）・・・約600万円

※その他、利益損害・賠償請求等の費用もかかる可能性があります

すぐにできる対策

✓ 不審なメールのURLクリックや添付ファイル開封をしてしまったときの対応手順を策定する

（参考）IPA「日常における情報セキュリティ対策」
2-2.4.不審なメールに注意
https://www.ipa.go.jp/security/anshin/measures/everyday.html

より強固にする対策

✓ 取引先と連携してメールの送信元認証を導入し、サプライチェーン全体として**不審なメールを受信しない・迷惑メールへ振り分ける仕組み**を整える

✓ **標的型メールを模擬した訓練**を実施し、体験を通じて不審なメールへの対処能力を向上させる

5．社長メールアカウント乗っ取りによる送金詐欺

項目	概要	
組織情報	製造業（関東）	従業員数：30名
	売上規模：約10億円	端末台数：40台
体制	情報システム担当2名(他業務と兼任)	
実施していたセキュリティ対策	• ウイルス対策ソフト、EDRの導入 • PC利用ログ取得及び定期的なログチェック • その他、年間500万円程度のセキュリティ予算	
被害経緯	• 社長が登録していた外部サービスから情報が漏えいし、メールアドレスとパスワードの組み合わせが流出した • 流出したパスワードは社長のクラウドメールのものと同一であり、攻撃者は社長アカウントへのログインに成功した	
被害内容	**アカウント乗っ取り** 社長のメールアカウントが攻撃者に乗っ取られ、ビジネスメール詐欺が発生した **資金流出** 社長を騙るメールに経理担当が騙され、攻撃者の口座へ500万円送金した ⇒**社長アカウントを使用した詐欺により、会社資金が流出！**	
攻撃要因	• 社長及び経理担当のITリテラシー不足	
被害後に実施したこと	• 全社員メールアカウントのパスワード変更・強化 • 全社員へのフィッシング・なりすましメール対応教育の実施	

想定被害額（被害額の計算明細は別紙の参考資料参照） **820万円**

- 初期対応費用（緊急対応、記録データの調査等）・・・約200万円
- 弁護士訴訟費用（弁護士への相談費用等）・・・約100万円
- 再発防止費用（新しい安全対策等）・・・約20万円
- 資金流出（攻撃者への送金）・・・約500万円

※その他、利益損害・賠償請求等の費用もかかる可能性があります

すぐにできる対策

✓ 全社員に対し**フィッシング・なりすましメール対応教育**を実施する

✓ 不審なメールや普段と異なる指示を受けた際の**報告要領**を明確にする

（参考）IPA「ビジネスメール詐欺（BEC）対策」
https://www.ipa.go.jp/security/bec/index.html

より強固にする対策

✓ クラウドメールに**多要素認証を導入**する

✓ **パスワード管理ツールを導入**し、パスワードを強化し、使い回しを防止する

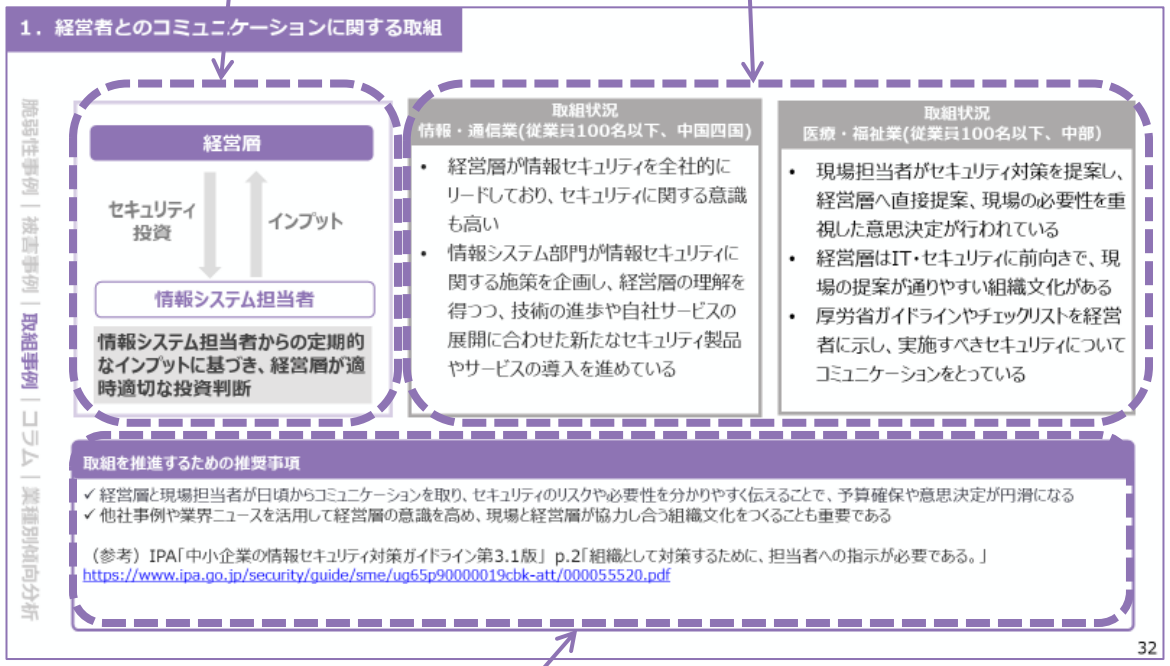
✓ **SIEMを導入**することにより、通信を包括的に監視し、異常があれば自動でアラートを出す仕組みを整備する

- 本事業に参加した中小企業での取組事例を紹介します。
- 同じような悩みを抱える中小企業における解決方法や課題感を共有し、自社の課題解決にご活用ください。

1．経営者とのコミュニケーションに関する取組
情シス担当からの定期的なインプットに基づき、経営層が適時適切な投資判断
2．取引先からのセキュリティ要求に関する取組
多種多様なセキュリティチェックシートへの回答を求められ、対応に負担が発生
3．業務効率化・データのバックアップに関する取組
業務データをクラウドに保管することにより、業務効率化を推進
4．インシデント対応体制整備に関する取組
サイバーインシデント対応計画の作成により、 インシデント発生時にも迅速に対応する体制を整備
5．リソース・専門性の確保に関する取組
保険やベンダーへの業務委託により、自社で不足するリソース・専門性を確保

取組事例のイメージを図で表現しています

参加企業における取組事例を紹介しています



取組を推進するための推奨事項を記載しています
参考となるリンクがある場合にはURLも記載しています

1．経営者とのコミュニケーションに関する取組

情報システム担当者からの定期的なインプットに基づき、経営層が適時適切な投資判断

取組状況
情報・通信業(従業員100名以下、中国四国)

- 経営層が情報セキュリティを全社的にリードしており、セキュリティに関する意識も高い
- 情報システム部門が情報セキュリティに関する施策を企画し、経営層の理解を得つつ、技術の進歩や自社サービスの展開に合わせた新たなセキュリティ製品やサービスの導入を進めている

取組状況
医療・福祉業(従業員100名以下、中部)

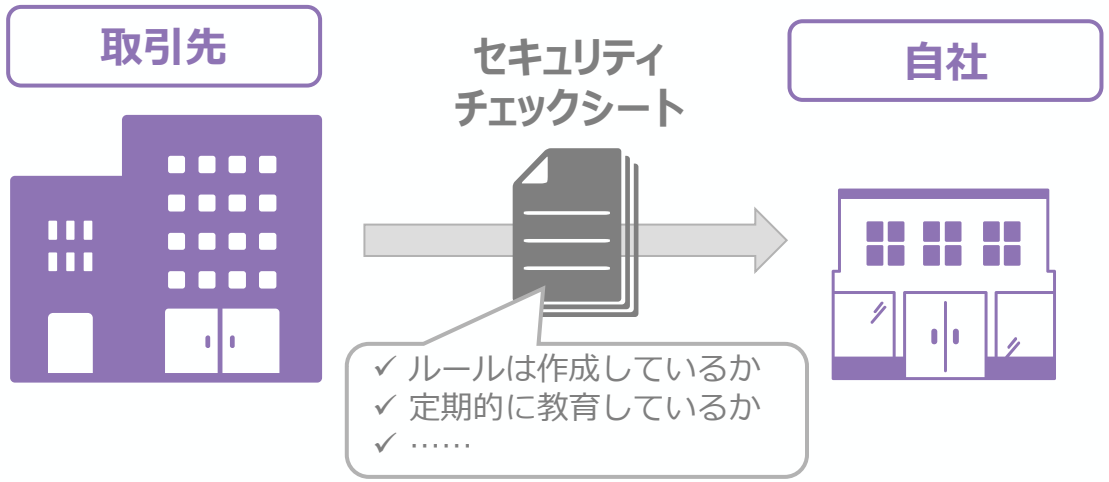
- 現場担当者がセキュリティ対策を提案し、経営層へ直接提案、現場の必要性を重視した意思決定が行われている
- 経営層はIT・セキュリティに前向きで、現場の提案が通りやすい組織文化がある
- 厚労省ガイドラインやチェックリストを経営者に示し、実施すべきセキュリティについてコミュニケーションをとっている

取組を推進するための推奨事項

✓ 経営層と現場担当者が日頃からコミュニケーションを取り、セキュリティのリスクや必要性を分かりやすく伝えることで、予算確保や意思決定が円滑になる
✓ 他社事例や業界ニュースを活用して経営層の意識を高め、現場と経営層が協力し合う組織文化をつくることも重要である

（参考）IPA「中小企業の情報セキュリティ対策ガイドライン第3.1版」p.2「組織として対策するために、担当者への指示が必要である。」
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/000055520.pdf

2．取引先からのセキュリティ要求に関する取組



多種多様なセキュリティチェックシートへの回答を求められ、対応に負担が発生

課題
製造業（従業員50名以下、関東）

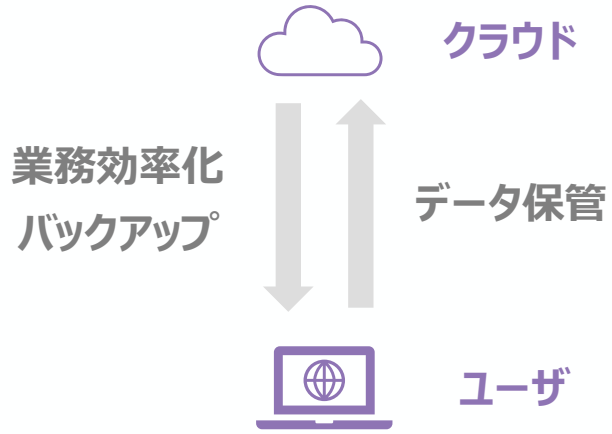
- 取引先からセキュリティチェックシートの記入や脆弱性管理の要請が多く寄せられている
- チェックシートの内容が実態や自社の規模に合わないものが多い。大企業向けの項目もあり、中小企業としては対応が難しい部分も多い
- 取引先ごとに異なるフォーマットや記載内容に対応する必要があり、負担が大きい
- セキュリティチェックシートの内容が明確な評価基準に基づいていないため、経営層への説明にも苦慮している

取組を推進するための推奨事項

✓ 取引先からのセキュリティチェックシートや要請内容をよく確認し、自社の実態や規模に合わない場合は、無理にすべてを満たそうとせず、できる範囲や現状について取引先とコミュニケーションを図る
✓ 業界団体や公的機関が発信する標準的な評価基準やガイドラインを参考に、自社の対応方針を整理しておく

（参考）経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）を活用する中小企業向け支援策について」
https://www.meti.go.jp/policy/netsecurity/sme-guide.html

3．業務効率化・データのバックアップに関する取組



業務データをクラウドに保管することにより、業務効率化を推進

取組状況
製造業（従業員20名以下、近畿）

- 重要データのバックアップ体制として、大部分をクラウドに移行し、サーバ室にも一部データを保管するハイブリッド運用を実施している
- クラウド活用により、リモートワークや多拠点間でのデータ共有が容易となり、業務の柔軟性・効率性が向上した

取組状況
製造業（従業員50名以下、近畿）

- グループウェアをクラウドサービスへ移行し、メール・クラウドストレージ等を一元管理している
- クラウド活用によりリモートワークや業務効率化、バックアップの自動化を実現した
- 業務データは全てクラウド上に保存し、PC本体にデータを残さないルールを徹底している

取組を推進するための推奨事項

✓ クラウド活用は、業務効率化・バックアップ・セキュリティ強化に効果的である
✓ 導入時は利便性と安全性のバランスを意識し、アクセス権限や多要素認証などの基本的なセキュリティ設定が重要である
✓ クラウドの利用については、被害事例１および被害事例２も参照されたい

（参考）IPA「中小企業のためのクラウドサービス安全利用の手引き」
https://www.ipa.go.jp/security/sme/f55m8k0000001wpl-att/outline_guidance_cloud.pdf

4．インシデント対応体制整備に関する取組

サイバーインシデント対応計画の作成により、インシデント発生時にも迅速に対応する体制を整備

取組状況
金融・保険業（従業員50名以下、関東）

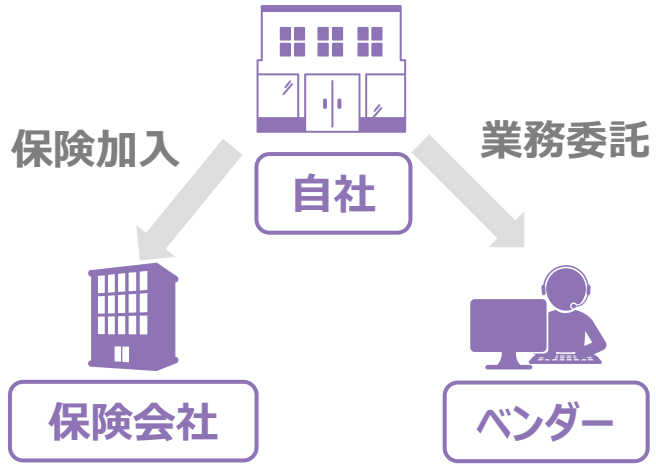
- 営業担当がシステム管理の業務を兼任しており、いわゆる「一人情シス」という状況だが、インシデント発生時の対応計画を策定し、社員に連絡フロー（誰に連絡するか）や対応手順（どのように対応するか）を周知している
- インシデント対応については、すべてを自社で完結させるのではなく、必要な機能については外部業者の協力を得る形としている

取組を推進するための推奨事項

✓インシデント対応計画を社内で作成し、初動対応（連絡先、対応手順）を明確にして全社員に周知する
✓外部業者と契約している場合は、インシデント発生時の連絡体制や対応範囲を確認し、連携方法を明文化しておく
✓作成したインシデント対応計画について、机上演習を行って実効性を向上させる

（参考）IPA「セキュリティインシデント対応の手引き」
https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/security-incident.pdf

5．リソース・専門性の確保に関する取組



保険やベンダーへの業務委託により、自社で不足するリソース・専門性を確保

取組状況
医療・福祉業（従業員100名以下、関東）

- サイバー保険に加入し、インシデント発生時の金銭的リスクに備えている
- セキュリティ分野の知識が必要となる場合は無理せず外部専門家やベンダーの力を借りる方針をとっている
- IT・セキュリティ運用は組織内に専任者がおらず、ベンダーへ運用や保守を外部委託し、最小限の工数で運用

取組状況
製造業（従業員100名以下、中国四国）

- インシデントを経験したことから、サイバー保険に速やかに加入し、リスク対応体制を強化した
- セキュリティ専任人員が不足しているため、外部の業者やベンダーの力を活用している
- ベンダーとの保守契約はないが、必要に応じて対応（脆弱性対応など）を依頼している

取組を推進するための推奨事項

✓サイバー保険への加入は、インシデント発生時の金銭的リスクや復旧費用をカバーする有効な手段である
✓必要なセキュリティ人材を確保できない場合は、ベンダーや外部専門家のサービス・支援を積極的に活用し、事業に必要なセキュリティ水準を確保することが重要

（参考）「サイバーセキュリティお助け隊サービス」の活用により、インシデント発生時の駆け付け支援、簡易的なサイバー保険を利用可能
https://www.meti.go.jp/policy/netsecurity/otasuketai.html

- その他、本事業に参加した中小企業での工夫を紹介します。
- 参考とする際は、いずれも自社の実態を踏まえ、適切な手法を検討のうえで、課題解決にご活用ください。

従業員教育に関する事例

✓ IPAが作成しているサイバーセキュリティ動画を、**年1～2回全社員に視聴**させ、さらに**社内ルール違反者には社長から直接指導**することで、教育とトップダウンの抑止を組み合わせている。

✓ **標的型攻撃メール訓練を年1回**程度、営業担当者向けに実施し、あわせて**「メール添付禁止＋専用アプリでのデータ共有」というルール**で誤送信・マルウェア感染リスクを下げている。

✓ 公的資料を**生成AIで自社向けに再構成**し、年2回の社員教育資料として配布することで、**教材作成の負荷を下げつつ最新情報を取り入れ**ている。

✓ **eラーニング教材と受講管理ツール**を使い、全社員に定期的なセキュリティ教育を行うとともに、**社内外のインシデント事例を全社発信して危機意識を共有**している。

✓ ITリテラシーの低い職員層には、ホワイトリスト型Webフィルタリングなど**技術的対策と組み合わせつつ、定期的な不審メール対応教育**を続けている。

（参考）IPA「映像で知る情報セキュリティ」映像コンテンツ一覧
https://www.ipa.go.jp/security/videos/list.html

AI活用の事例と留意点

✓ **ASM診断レポートを生成AIに要約させる**事例
- ◆ 機密情報・個人情報を含む内容をそのまま外部サービスに入力しない（**ASM診断レポートは自社の脆弱性が記載**）
- ◆ AIが生成した内容に誤りや過度な単純化がないか確認すること
- ◆ **セキュリティポリシーや秘密保持契約に反しないか確認**すること

✓ **公開している資料・動画を生成AIで自社向けに再構成・要約して社内教育資料に転用**する事例
- ◆ 著作権・利用規約を確認し、**許容される範囲で利用**すること
- ◆ AIが要約・再構成する過程で、重要な注意点や免責事項が抜け落ちていないかを確認すること
- ◆ **自社の実態に合う**よう、人手で内容を調整すること

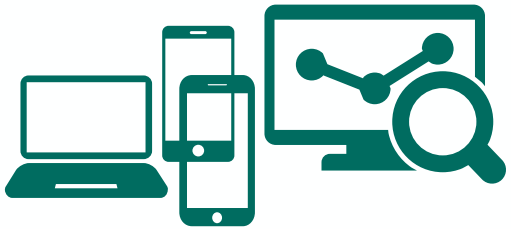
✓ **セキュリティポリシーや規程、インシデント対応計画などをまず生成AIにドラフトさせる**事例
- ◆ そのまま採用せず、必ず**担当部門（情報システム部門、法務、コンプライアンス等）がレビュー**・修正すること
- ◆ 自社の業種・規模・法令・ガイドライン（例：個人情報保護法、業界規制等）への適合性を人間が判断すること
- ◆ それらしい文書であっても、**実際の運用体制やリソースに照らして実現可能かを検証**すること

未把握IT資産に関する事例

✓ クラウド移行時に止めたつもりのバックアップDBや旧サーバが残りやすい。**ASM診断結果と照合しながら一つずつ潰す運用**を入れておくと取りこぼしを防げる。

✓ サブドメインやテスト環境は担当者異動・退職で放置されやすい。新規ドメイン／サブドメイン発行時に**「申請書＋台帳登録」を必須にし、廃止時の手順（DNS削除まで）を明文化**しておくことが重要。

✓ 使われていないSaaSアカウントは、ダークウェブ流出やなりすましの入口になりやすい。人事異動・退職のたびに**「アカウント棚卸しチェックリスト」で一括停止する運用**を組み込むとよい。



※本事業参加企業126社のうち、53社（製造・建設業）から得られた情報を元にしています。

製造・建設業における傾向

技術的対策は比較的進んでいる層が多い

- FW、UTM、ウイルス対策、VPN、多要素認証、バックアップ、EDR/WAFなどを導入している企業が多い

組織面は「兼務情シス」が標準

- 担当は「情報システム部（他業務と兼任）」が多く、経営者自身が担当するケースも一部あり

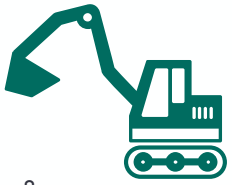
インシデント経験率が比較的高く、行動に結びつきやすい

- ウイルス感染、情報漏えい、Web改ざん、不正アクセスなどを経験した企業が一定数あり

経営層の関心は二極化

- 経営者がIT・DXを強く推進するケースと、「最低限でよい」とするケースが混在
- アンケートでは「どちらかといえば高い」が多い一方、「どちらかといえば低い」も製造業で散見される

主な課題



「どこまでやれば十分か」が不明確

- 「どの程度の対策が適切か」の基準がなく、EDR・WAF導入後もログ分析や運用の深度が不足しがち
- アンケートでは「費用対効果が不明」「対象範囲の特定ができない」が製造業でも高頻度で挙がる

サプライチェーン要求と自社実態のギャップ

- チェックシート対応はしているが、自社の基準がないまま「言われたからやる」状態の企業が多い
- ヒアリングでも、「フォーマットがバラバラで負担」「実態にそぐわない項目が多い」と指摘

有効な対策

- **サプライチェーン評価制度の活用**
- サイバーセキュリティお助け隊サービスなどパッケージでお任せできる**外部ベンダーの活用**

※本事業参加企業126社のうち、26社（情報通信業）から得られた情報を元にしています。

情報通信業における傾向

技術・運用ともに全体として高水準

- アンケートでは、技術的対策項目（ログ収集・監視、異常通信検知、EDR、脆弱性診断など）に複数チェック
- ISMS/ISO27017取得、NIST準拠、クラウド前提設計など、マネジメントシステムまで整備している企業も

経営層の関心が高く、技術バックグラウンドを持つ役員がいる

- アンケートでも情報通信業は「経営層の関心度：高い／どちらかといえば高い」が多い
- ヒアリングでも、技術部門トップの役員がセキュリティポリシー策定・投資判断を主導している事例

取引先からの高度な要求に日常的にさらされている

- チェックシート、脆弱性管理要請、NIST SP800-53レベルの要求など、大手顧客からの要請が厳しい
- アンケートの「取引先から脆弱性管理を求められたことがある」に「はい」と答える割合が高い業種の一つ

主な課題

外部委託先の選定基準が高く、「任せられる先がない」

- 海外法制リスクを理由に国内法人に限定し、自社技術力の高さもあって「委託できる業者がいない」と回答
- アンケートで「依頼/委託できる業者がいない」が挙がるが、その背景は「要求水準が高すぎる」側面も

マネジメント負荷の増大

- 技術的には対応済みでも、記録・レビュー・文書化といったマネジメント要求が増え続け、人的負荷が課題

有効な対策

- 高度な事業者向けの標準テンプレート（NIST/ISOに沿ったチェックシート、運用記録フォーマット）を整備し、取引先要求との整合を取りやすくする

※本事業参加企業126社のうち、20社（金融・保険業）から得られた情報を元にしています。

金融・保険業における傾向

クラウド＋ログ管理で統制を図る企業が多い

- アンケートでも、「ログ収集・監視」「アクセス制御・権限管理」を実施している割合が比較的高い

サプライチェーン管理への意識が高い

- 取引先にチェックシートを送付し、アンケートでも「外部委託先やサプライチェーンの管理」を実施していると回答する比率が高い業種の一つ

インシデント経験は限定的だが、危機感は一定程度ある

- 情報漏えい経験があるケースもあるが、全体としては「過去に大きなインシデントはない」企業が多い
- それでも不審メール開封などの“ヒヤリハット”を契機に教育や対策を強化している

主な課題

兼務情シス＋専門人材不足

- 営業兼務でシステム担当をしている事例が多く、「セキュリティに工数を割けるのは全体の2割程度」との声
- アンケートでも「専門人材不在」「時間が取れない」が金融・保険業で繰り返し挙がる

経営層への翻訳・説得がボトルネック

- 専門用語をかみ砕く工夫をしているが、これは裏を返せば「そのままでは伝わらない」ことを意味する
- アンケートでも、「理解はしたが実施しない」層の理由として「費用対効果が不明」「優先度が低い」が目立つ

有効な対策

- ASM結果やログ情報を「想定被害額」「信用失墜」「顧客影響」といった経営指標に翻訳したレポートが有効
- 兼務情シスを前提に、「診断＋設定変更代行＋運用モニタリング」を一体提供する外部サービスの活用

※本事業参加企業126社のうち、8社（医療・福祉業）から得られた情報を元にしています。

医療・福祉業における傾向

入口対策・物理対策は一定レベルで実施

- UTM（FortiGate等）導入、電子カルテのクローズドネットワーク運用、USBポート無効化など
- アンケートでも「ファイアウォール・境界防御」「バックアップ」「アクセス制御・権限管理」の実施率は高い

インシデント経験はあるが、被害は軽微と認識されがち

- 不審メール開封によるウイルス感染などを経験しているが、「大きな被害はなかった」と整理
- そのため、「今後の投資優先度」を上げる決定打にはなっていない

経営層の関心は中程度～低め

- アンケートでは「どちらかといえば高い」～「どちらかといえば低い」が多い
- ヒアリングでも、「患者サービス等の目に見える投資と比べるとセキュリティの優先度は下がる」との声

主な課題

「説明責任」レベルで止まりがち

- 「何もしていないと言われないための最低限対策」としてUTM等を導入しているが、実際の防御効果や運用の深度は不明なまま、ベンダー任せになっているケースがある
- アンケートでも「費用対効果が不明」「経営層関与が薄い」が医療・福祉で顕著

人材・教育の二重の不足

- 専任IT・セキュリティ人材がほぼおらず、「ベンダー任せ＋最低限の職員教育」が標準
- 職員のITリテラシー差が大きく、教育は「不審メールを開かない」などの基礎に集中せざるを得ない

有効な対策

- ベンダー任せを前提に、「何をベンダーに求めるべきか」「契約で確認すべきポイント」をまとめる

※本事業参加企業126社のうち、19社（卸売・小売業）から得られた情報を元にしています。

卸売・小売業における傾向

クラウド活用が多い

- クラウド活用が比較的進んでおり、「PCにデータを置かない」「クラウドに集約する」設計を志向する企業が多い

基本的な技術対策は導入済み

- ウイルス対策ソフト、ファイアウォール、バックアップといった基本的な技術対策は導入済みが標準
- 一方で、EDR・ログ監視・異常通信検知など一段進んだ対策は未導入の企業が多い

兼務情シスが主流

- 情報システム専任部門は少なく、経営者や営業・総務が「兼務情シス」として担当する体制が一般的
- セキュリティポリシーやインシデント対応計画は未整備～簡易版にとどまりやすい

主な課題

クラウドへの過信

- クラウドを使っていること自体が「安全」と誤解されやすく、多要素認証やIP制限、共有設定などクラウド側のセキュリティ設定が甘くなりがち

兼務体制の限界

- アンケートでも「専門人材不在」「時間が取れない」「費用対効果が不明」が対策停滞の理由として多く、兼務体制の限界がボトルネックになっている

有効な対策

- クラウド前提のミニマムセットを明確にする
- 経営層向けには、「ECサイト停止時の売上損失」「顧客情報流出時のレビュー炎上・信用失墜」といった卸売・小売特有の影響シナリオを示し、ASMの想定被害額や同業他社事例と組み合わせて投資判断の材料にする

（参考）１．VPN装置の脆弱性悪用によるランサムウェア感染・ファイル暗号化

想定被害額計算明細（被害事例１）

※本明細は費用損害のみで、利益損害・賠償損害・詐欺被害額等は含みません

費目	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
費用損害	初期対応費用 原因調査費用	ファスト・フォレンジック費用 （影響範囲調査）	PC	300,000	円	80	台	1	回	24,000,000	感染経路・影響範囲特定のため全数を対象とする
			物理サーバ	750,000	円	2	台	1	回	1,500,000	感染経路・影響範囲特定のため全数を対象とする
		フォレンジック費用（PC）	証拠保全	100,000	円	1	台	1	回	100,000	感染源と考えられるPC1台を対象とする
			データ復旧・復元	50,000	円	1	台	1	回	50,000	感染源と考えられるPC1台を対象とする
			データ解析	1,000,000	円	1	台	1	回	1,000,000	感染源と考えられるPC1台を対象とする
			報告書作成	350,000	円	1	冊	1	回	350,000	感染源と考えられるPC1台を対象とする
		フォレンジック費用（サーバ）	証拠保全	150,000	円	1	台	1	回	150,000	サーバ1台を対象とする
			データ復旧・復元	0	円	0	台	0	回	0	データ復旧は不可と想定
			データ解析	1,400,000	円	1	台	1	回	1,400,000	サーバ1台を対象とする
			報告書作成	350,000	円	1	冊	1	回	350,000	サーバ1台を対象とする
		攻撃痕跡分析	マルウェア検体分析	1,250,000	円	1	検体	1	回	1,250,000	マルウェア1検体を解析とする
		生産管理システム影響調査		100,000	円	1	業者	1	調査	100,000	保守ベンダーの訪問費用として計上
		制御設備影響調査		100,000	円	1	業者	1	調査	100,000	保守ベンダーの訪問費用として計上
		小計								30,350,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	復旧費用	クリーンインストール	PC	50,000	円	20	台	1	回	1,000,000	PC全80台中、20台が感染していたとする
		サーバ復旧	サーバ	100,000	円	2	台	1	回	200,000	2台のサーバが感染していたとする
		データリカバリー	PC	50,000	円	20	台	1	回	1,000,000	PC全80台中、20台が感染していたとする
			サーバ	100,000	円	2	台	1	回	200,000	2台のサーバが感染していたとする
		PCレンタル		10,000	円	20	台	1	カ月	200,000	感染PCをクリーンアップするまでの代替
		生産管理システム復旧費用		1,000,000	円	1	業者	1	訪問	1,000,000	保守ベンダーが1週間滞在し復旧を行ったと仮定
		小計								3,600,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	対応費用	外部コンサルタント起用		3,000,000	円	1	人	1	カ月	3,000,000	危機管理とインシデントハンドリングのコンサルティングを起用
		小計								3,000,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	弁護士 訴訟費用	弁護士への相談費用		1,000,000	円	1	人	1	依頼	1,000,000	法律相談費用のほか各種雑費も含めて100万円と仮定
		着手金・成功報酬		500,000	円	1	人	1	依頼	500,000	納期遅延・約定不履行に対する賠償請求の交渉
		小計								1,500,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	再発防止費用	セキュリティサービス導入	EDR導入	13,200	円	82	台	1	年契約	1,082,400	スケールメリット考慮せず、PC80台＋サーバ2台
		情報セキュリティ管理体制見直し	セキュリティ規程見直し	3,000,000	円	1	社	1	回	3,000,000	ISMS準拠の情報セキュリティ規程見直しコンサルティング
			インシデントマニュアル策定	3,000,000	円	1	社	1	回	3,000,000	インシデント対応マニュアルの新規策定コンサルティング
		従業員教育	eラーニングによる研修	5,280	円	80	人	1	回	422,400	eラーニング費用
		小計								7,504,800	
	費用損害計									45,954,800	

（参考）２．クラウド設定ミスによる情報漏えい

想定被害額計算明細（被害事例２）

※本明細は費用損害のみで、利益損害・賠償損害・詐欺被害額等は含みません

費目	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
費用損害	初期対応費用 原因調査費用	ファスト・フォレンジック費用 （影響範囲調査）	PC	300,000	円	0	台	0	回	0	対象なし
			物理サーバ	750,000	円	0	台	0	回	0	対象なし
		フォレンジック費用（PC）	証拠保全	100,000	円	0	台	0	回	0	対象なし
			データ復旧・復元	50,000	円	0	台	0	回	0	対象なし
			データ解析	1,000,000	円	0	台	0	回	0	対象なし
			報告書作成	350,000	円	0	冊	0	回	0	対象なし
		フォレンジック費用（サーバ）	証拠保全	150,000	円	1	台	1	回	150,000	クラウドストレージを対象とする
			データ復旧・復元	0	円	0	台	0	回	0	対象なし
			データ解析	1,400,000	円	1	台	1	回	1,400,000	クラウドストレージを対象とする
			報告書作成	350,000	円	1	冊	1	回	350,000	クラウドストレージを対象とする
		攻撃痕跡分析	マルウェア検体分析	1,250,000	円	0	検体	0	回	0	対象なし
		生産管理システム影響調査		100,000	円	0	業者	0	調査	0	対象なし
		制御設備影響調査		100,000	円	0	業者	0	調査	0	対象なし
		小計								1,900,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	復旧費用	クリーンインストール	PC	50,000	円	0	台	0	回	0	対象なし
		サーバ復旧	サーバ	100,000	円	0	台	0	回	0	対象なし
		データリカバリー	PC	50,000	円	0	台	0	回	0	対象なし
			サーバ	100,000	円	0	台	0	回	0	対象なし
		PCレンタル		10,000	円	0	台	0	カ月	0	対象なし
		生産管理システム復旧費用		1,000,000	円	0	業者	0	訪問	0	対象なし
		小計								0	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	対応費用	外部コンサルタント起用		3,000,000	円	0	人	0	カ月	0	対象なし
		小計								0	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	弁護士 訴訟費用	弁護士への相談費用		1,000,000	円	1	人	1	依頼	1,000,000	法律相談費用のほか各種雑費も含めて100万円と仮定
		着手金・成功報酬		0	円	0	人	0	依頼	0	対象なし
		小計								1,000,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	再発防止費用	セキュリティサービス導入	EDR導入	13,200	円	0	台	0	年契約	0	対象なし
		情報セキュリティ管理体制見直し	セキュリティ規程見直し	3,000,000	円	0	社	0	回	0	対象なし
			インシデントマニュアル策定	3,000,000	円	0	社	0	回	0	対象なし
		従業員教育	eラーニングによる研修	5,280	円	0	人	0	回	0	対象なし
		小計								0	
	費用損害計									2,900,000	

（参考）３．Webサイト改ざんによるフィッシング誘導

想定被害額計算明細（被害事例３）

※本明細は費用損害のみで、利益損害・賠償損害・詐欺被害額等は含みません

費目	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
費用損害	初期対応費用 原因調査費用	ファスト・フォレンジック費用 （影響範囲調査）	PC	300,000	円	0	台	0	回	0	対象なし
			物理サーバ	750,000	円	0	台	0	回	0	対象なし
		フォレンジック費用（PC）	証拠保全	100,000	円	0	台	0	回	0	対象なし
			データ復旧・復元	50,000	円	0	台	0	回	0	対象なし
			データ解析	1,000,000	円	0	台	0	回	0	対象なし
			報告書作成	350,000	円	0	冊	0	回	0	対象なし
		フォレンジック費用（サーバ）	証拠保全	150,000	円	1	台	1	回	150,000	サーバ1台を対象とする
			データ復旧・復元	0	円	0	台	0	回	0	対象なし
			データ解析	1,400,000	円	1	台	1	回	1,400,000	サーバ1台を対象とする
			報告書作成	350,000	円	1	冊	1	回	350,000	サーバ1台を対象とする
		攻撃痕跡分析	マルウェア検体分析	1,250,000	円	0	検体	0	回	0	対象なし
		生産管理システム影響調査		100,000	円	0	業者	0	調査	0	対象なし
		制御設備影響調査		100,000	円	0	業者	0	調査	0	対象なし
		小計								1,900,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	復旧費用	クリーンインストール	PC	50,000	円	0	台	0	回	0	対象なし
		サーバ復旧	サーバ	100,000	円	1	台	1	回	100,000	サーバ1台を対象とする
		データリカバリー	PC	50,000	円	0	台	0	回	0	対象なし
			サーバ	100,000	円	1	台	1	回	100,000	サーバ1台を対象とする
		PCレンタル		10,000	円	0	台	0	カ月	0	対象なし
		生産管理システム復旧費用		1,000,000	円	0	業者	0	訪問	0	対象なし
		小計								200,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	対応費用	外部コンサルタント起用		3,000,000	円	0	人	0	カ月	0	対象なし
		小計								0	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	弁護士 訴訟費用	弁護士への相談費用		1,000,000	円	1	人	1	依頼	1,000,000	法律相談費用のほか各種雑費も含めて100万円と仮定
		着手金・成功報酬		0	円	0	人	0	依頼	0	対象なし
		小計								1,000,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	再発防止費用	ウェブアプリケーション診断		1,000,000	円	1	サービス	1	回	1,000,000	対象のサイトに対しウェブアプリケーション診断を実施
		情報セキュリティ管理体制見直し	セキュリティ規程見直し	3,000,000	円	0	社	0	回	0	対象なし
			インシデントマニュアル策定	3,000,000	円	0	社	0	回	0	対象なし
		従業員教育	eラーニングによる研修	5,280	円	0	人	0	回	0	対象なし
		小計								1,000,000	
	費用損害計									4,100,000	

（参考）４．取引先を装う標的型メールでの侵入

想定被害額計算明細（被害事例４）

※本明細は費用損害のみで、利益損害・賠償損害・詐欺被害額等は含みません

費目	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
費用損害	初期対応費用 原因調査費用	ファスト・フォレンジック費用 （影響範囲調査）	PC	300,000	円	20	台	1	回	6,000,000	感染経路・影響範囲特定のため全台を対象とする
			物理サーバ	750,000	円	2	台	1	回	1,500,000	感染経路・影響範囲特定のため全台を対象とする
		フォレンジック費用（PC）	証拠保全	100,000	円	1	台	1	回	100,000	感染源と考えられるPC1台を対象とする
			データ復旧・復元	50,000	円	1	台	1	回	50,000	感染源と考えられるPC1台を対象とする
			データ解析	1,000,000	円	1	台	1	回	1,000,000	感染源と考えられるPC1台を対象とする
			報告書作成	350,000	円	1	冊	1	回	350,000	感染源と考えられるPC1台を対象とする
		フォレンジック費用（サーバ）	証拠保全	150,000	円	1	台	1	回	150,000	サーバ1台を対象とする
			データ復旧・復元	0	円	0	台	0	回	0	対象なし
			データ解析	1,400,000	円	1	台	1	回	1,400,000	サーバ1台を対象とする
			報告書作成	350,000	円	1	冊	1	回	350,000	サーバ1台を対象とする
		攻撃痕跡分析	マルウェア検体分析	1,250,000	円	1	検体	1	回	1,250,000	マルウェア1検体を解析とする
		生産管理システム影響調査		100,000	円	0	業者	0	調査	0	対象なし
		制御設備影響調査		100,000	円	0	業者	0	調査	0	対象なし
		小計								12,150,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	復旧費用	クリーンインストール	PC	50,000	円	10	台	1	回	500,000	PC全20台中、10台が感染していたとする
		サーバ復旧	サーバ	100,000	円	1	台	1	回	100,000	1台のサーバが感染していたとする
		データリカバリー	PC	50,000	円	10	台	1	回	500,000	PC全20台中、10台が感染していたとする
			サーバ	100,000	円	1	台	1	回	100,000	1台のサーバが感染していたとする
		PCレンタル		10,000	円	10	台	1	カ月	100,000	感染PCをクリーンアップするまでの代替、最少契約単位は1か月とする
		生産管理システム復旧費用		1,000,000	円	0	業者	0	訪問	0	対象なし
		小計								1,300,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	対応費用	外部コンサルタント起用		3,000,000	円	1	人	1	カ月	3,000,000	危機管理とインシデントハンドリングのコンサルティングを起用
		小計								3,000,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	弁護士 訴訟費用	弁護士への相談費用		1,000,000	円	1	人	1	依頼	1,000,000	法律相談費用のほか各種雑費も含めて100万円と仮定
		着手金・成功報酬		0	円	0	人	0	依頼	0	対象なし
		小計								1,000,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	再発防止費用	セキュリティサービス導入	EDR導入	13,200	円	0	台	0	年契約	0	対象なし
		情報セキュリティ管理体制見直し	セキュリティ規程見直し	3,000,000	円	1	社	1	回	3,000,000	ISMS準拠の情報セキュリティ規程見直しコンサルティング
			インシデントマニュアル策定	3,000,000	円	1	社	1	回	3,000,000	インシデント対応マニュアルの新規策定コンサルティング
		従業員教育	eラーニングによる研修	5,280	円	20	人	1	回	105,600	eラーニング費用
		小計								6,105,600	
	費用損害計									23,555,600	

（参考）５．社長メールアカウント乗っ取りによる送金詐欺

想定被害額計算明細（被害事例５）

※本明細は費用損害のみで、利益損害・賠償損害・詐欺被害額等は含みません

費目	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
費用損害	初期対応費用 原因調査費用	ファスト・フォレンジック費用 （影響範囲調査）	PC	300,000	円	0	台	0	回	0	対象なし
			物理サーバ	750,000	円	0	台	0	回	0	対象なし
		フォレンジック費用（PC）	証拠保全	100,000	円	0	台	0	回	0	対象なし
			データ復旧・復元	50,000	円	0	台	0	回	0	対象なし
			データ解析	1,000,000	円	0	台	0	回	0	対象なし
			報告書作成	350,000	円	0	冊	0	回	0	対象なし
		フォレンジック費用（サーバ）	証拠保全	150,000	円	1	台	1	回	150,000	クラウドメールを対象とする
			データ復旧・復元	0	円	0	台	0	回	0	対象なし
			データ解析	1,400,000	円	1	台	1	回	1,400,000	クラウドメールを対象とする
			報告書作成	350,000	円	1	冊	1	回	350,000	クラウドメールを対象とする
		攻撃痕跡分析	マルウェア検体分析	1,250,000	円	0	検体	0	回	0	対象なし
		生産管理システム影響調査		100,000	円	0	業者	0	調査	0	対象なし
		制御設備影響調査		100,000	円	0	業者	0	調査	0	対象なし
		小計								1,900,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	復旧費用	クリーンインストール	PC	50,000	円	0	台	0	回	0	対象なし
		サーバ復旧	サーバ	100,000	円	0	台	0	回	0	対象なし
		データリカバリー	PC	50,000	円	0	台	0	回	0	対象なし
			サーバ	100,000	円	0	台	0	回	0	対象なし
		PCレンタル		10,000	円	0	台	0	カ月	0	対象なし
		生産管理システム復旧費用		1,000,000	円	0	業者	0	訪問	0	対象なし
		小計								0	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	対応費用	外部コンサルタント起用		3,000,000	円	0	人	0	カ月	0	対象なし
		小計								0	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	弁護士 訴訟費用	弁護士への相談費用		1,000,000	円	1	人	1	依頼	1,000,000	法律相談費用のほか各種雑費も含めて100万円と仮定
		着手金・成功報酬		0	円	0	人	0	依頼	0	対象なし
		小計								1,000,000	
	大項目	中項目	小項目	単価	単位	数	単位	頻度	単位	想定損失額（円）	積算根拠
	再発防止費用	セキュリティサービス導入	EDR導入	13,200	円	0	台	0	年契約	0	対象なし
		情報セキュリティ管理体制見直し	セキュリティ規程見直し	3,000,000	円	0	社	0	回	0	対象なし
			インシデントマニュアル策定	3,000,000	円	0	社	0	回	0	対象なし
		従業員教育	eラーニングによる研修	5,280	円	30	人	1	回	158,400	eラーニング費用
		小計								158,400	
	費用損害計									3,058,400	

用語集

管理パネル（管理画面）	システムの設定を変更したり、ユーザを管理したりするための画面。
クラウドサービス	自社にサーバを置かず、インターネット経由で他社のサーバやソフトを利用するサービス（例：オンラインストレージ、クラウドメールなど）。
サプライチェーン	自社と取引先・委託先などを含めた「モノやサービスが届くまでのつながり」で、その中の一社が攻撃されると他社にも影響が及ぶ。
自己署名証明書	自分で作った証明書。信頼性が低く、ブラウザで警告が出やすい。
セキュリティインシデント	ウイルス感染や情報漏えいなど、セキュリティ上の事故やそのおそれがある出来事。
セキュリティチェックシート	取引先が「どの程度セキュリティ対策をしているか」を確認するために、質問項目を一覧にした書類。
セキュリティポリシー	会社として「情報をどう守るか」を定めた社内ルールや文書の総称。
ゼロトラスト	「社内だから安全」という前提をやめ、すべてのアクセスを毎回確認・認証する考え方・仕組み。
バックアップ	データが消えたり壊れたりしたときに備えて、別の場所にコピーを保存しておくこと。
パスキー	ID・パスワードの代わりに、スマホやPCの生体認証（指紋・顔など）でログインできる新しい仕組み。
平文通信	暗号化されていない通信。途中で見られると、内容がそのまま読めてしまう。
ファイアウォール	不正な通信をブロックする「ネットワークの門番」のような装置やソフト。
フィッシング	本物そっくりのメールやWebサイトで利用者をだまし、ID・パスワードやカード情報を盗み取る手口。
標的型メール攻撃	特定の会社や人をねらって、それらしく見えるメールを送りつけ、添付ファイルやURLを開かせて侵入を試みる攻撃。
マルウェア	ウイルスやランサムウェアなど、コンピュータに害を与える目的で作られた不正なソフトの総称。
ランサムウェア	PCやサーバ内のデータを勝手に暗号化し、「元に戻してほしければ身代金を払え」と要求するマルウェア。
ログ	誰が・いつ・どこから・何をしたか、といったシステムの動きを記録したデータ。
脆弱性（ぜいじゃくせい）	ソフトやシステムの設計ミス・設定ミスなどによる「弱点」で、攻撃者に悪用される可能性がある部分。

用語集

APIキー	外部サービスやクラウドとプログラム同士でやり取りする際に使う「合言葉」のような文字列。
AWS（Amazon Web Services）	Amazonが提供する代表的なクラウドサービス群で、サーバやストレージなどをインターネット経由で利用できる。
ASM（Attack Surface Management）	組織がインターネット上に公開している資産（ドメイン、IP、クラウド環境、APIなど）を継続的に洗い出し、攻撃者視点で脆弱な入口を特定・管理する仕組み。
BCP（Business Continuity Plan）	災害やサイバー攻撃が起きたときに、事業を止めない・早く再開するための計画。
CMS（Content Management System）	専門知識がなくても、Webサイトの文章や画像を更新できる仕組み（例：WordPressなど）。
Cookie（クッキー）	Webサイトが、利用者のブラウザに保存する小さなデータ。ログイン状態の維持などに使われる。
DMARC	なりすましメールを見分けるために、受信側がSPFやDKIMの結果をもとに「受信するか拒否するか」を判断する仕組み。
DNS	「example.com」のような名前と、実際のIPアドレスを結びつけるインターネットの住所録のような仕組み。
DNSSEC	DNSの情報が書き換えられていないかを確認するための仕組みで、偽の名前解決を防ぐ。
DKIM	メールに電子署名を付けて、「このメールは本当にこのドメインから送られたものか」を確認できる仕組み。
EDR（Endpoint Detection and Response）	PCやサーバ上の不審な動きを検知し、調査・対処まで行う高度なセキュリティソフト。
FTP / FTPS	ファイルをサーバとやり取りするための仕組みで、FTPSはその通信を暗号化したもの。
HTTPS	Webサイトとの通信を暗号化する仕組みで、アドレスが「https://」から始まる安全な通信方式。
IPアドレス	インターネット上で機器を識別するための番号で、ネット上の「住所」にあたるもの。
ISMS / ISO 27001	情報セキュリティを管理する仕組みを整えていることを示す国際規格と、その認証制度。

用語集

MFA （Multi Factor Authentication） ：多要素認証	パスワードに加え、スマホの認証コードや生体認証など複数の要素を組み合わせてログインする仕組み。
NIST	アメリカの標準化機関で、サイバーセキュリティのフレームワークやガイドラインを公開している。
OS （オペレーティングシステム）	WindowsやLinuxなど、PCやサーバを動かす基本ソフト。
RCE （リモートコード実行）	攻撃者が遠隔から、サーバやPCの中で任意のプログラムを実行できてしまう危険な脆弱性。
SaaS	インターネット経由でソフトウェアを利用するサービス形態（例：クラウドメール、オンライン会計ソフトなど）。
SIEM	さまざまな機器のログを集めて分析し、怪しい動きをまとめて検知するための仕組み・製品。
SLA	クラウドや外部サービスの「稼働率」「サポート範囲」などを定めた、サービス品質に関する取り決め。
SOC （Security Operation Center）	24時間体制などでログを監視し、サイバー攻撃の兆候を見つけて対応する専門チーム（またはそのサービス）。
SPF	「このドメインのメールは、このサーバからしか送られない」と宣言することで、なりすましメールを見分けやすくする仕組み。
TLS / SSL	インターネット通信を暗号化するための技術。HTTPSなどで使われている。
UTM（統合脅威管理）	ファイアウォール、ウイルス対策、不正侵入防止など複数の機能を1台にまとめたセキュリティ機器。
VPN （Virtual Private Network）	インターネットを通じて、社外から社内ネットワークに安全に接続するための仮想的な専用回線の仕組み。
WAF （Web Application Firewall）	Webサイトへの不正なアクセスや攻撃（SQLインジェクションなど）を検知・遮断するための防御装置。
Webフィルタリング	危険なWebサイトや業務に関係ないサイトへのアクセスを制限する仕組み。
WordPress	多くの企業サイトやブログで使われている代表的なCMS（Webサイト管理ソフト）。

講演などで使う事例を選ぶ際のポイント

Step1：講演の目的に応じて分類を選ぶ		Step２：同じ分類の中から事例を選ぶ
脆弱性の仕組みを わかりやすく説明したい	脆弱性事例	✓ ４ページに記載の脆弱性のグルーピングを参考に ✓ 講演の参加者層にあわせて業界・規模・地域を参考に ✓ 説明したい技術要素にあわせて
危機感や必要性を 伝えたい	被害事例	✓ 業界・規模・地域の近いケースを参考に ✓ 想定被害額を参考に ✓ 攻撃要因や対策など訴えたい内容にあわせて
改善・成功ポイント を示したい	取組事例	✓ 同規模の企業が取り組んだ内容を参考に ✓ 講演の参加者層が共感できる内容にあわせて ✓ 訴えたい取組にあわせて
補助的な情報を 補いたい	コラム・業界別傾向分析	✓ 講演の補足として講演内容にあわせて ✓ 講演の参加者層にあわせて ✓ 注意喚起や全体整理に役立つ内容にあわせて

注意事項

本PDFをそのまま抜粋いただきご使用いただくことが可能です。ぜひご活用いただけますと幸いです。
その際の引用元については、以下のようにご指定ください。
「出典：IPA「中小企業のための実例で学ぶサイバーセキュリティリスク事例集」より抜粋」
原則、PPTでの公開は行っておりませんので、ご理解いただきたくよろしくお願いいたします。

本事例集の、「活用時の注意事項」と「想定活用法」

■活用時の注意事項

- ✓ 本事例集は、本事業で実施したASM診断（126社）とアンケート・ヒアリング結果をもとに作成しているものであり、**必ずしもすべての中小企業にとって有効な対策とは限りません**
- ✓ 被害事例はモデルケースとして積算したものであり**シナリオや被害額等には、一部想定を含み**ます

■想定活用法（一例）

- ✓ ASMの活用にあたっては、まず**自社にどのようなIT資産（サーバ、クラウド、Webサイト、機器、アカウントなど）があるかを洗い出し、一覧化する「資産管理」**から始めます
- ✓ 次に、それらの資産に対して**ASM診断**（脆弱性や設定確認）を行い、「どこに、どのような弱点があるか」を把握します
- ✓ ASM診断で脆弱性が見つかれば、本事例集の該当ページを参照することで、**同様の事例や具体的な対策案を確認**できます
- ✓ さらに、見つかった脆弱性に関する詳細な技術情報や最新の注意喚起については、**IPAやJPCERT/CCが公開している「脆弱性対策情報（下記URL）」を参照**することで、より踏み込んだ解説や推奨設定、関連する注意事項などを確認できます
- ✓ 脆弱性を修正したのち、脆弱性診断やウェブアプリケーション診断を実施し、**「弱点が克服されたか」を確認**するとより安心です
- ✓ このように、①資産管理 → ②診断・脆弱性の把握 → ③事例集での対策検討 → ④IPA・JPCERTの脆弱性対策情報で詳細確認→⑤脆弱性診断やウェブアプリケーション診断の実施、という流れで、自社に合った現実的な対策を進めていくことを想定しています

■最新の脆弱性対策情報

最新の脆弱性対策情報はこちらで入手可能です。是非定期的に御確認ください

- ✓ 脆弱性対策情報（IPA） https://www.ipa.go.jp/security/vuln/index.html
- ✓ 注意喚起（JPCERT/CC） https://www.jpcert.or.jp/at/2026.html


IPA