

一般社団法人日本自動車部品工業会
DX対応委員会サイバーセキュリティ部会 CSセミナー#02

中小企業向け 情報セキュリティ関連規程の作り方

2025年12月18日
独立行政法人 情報処理推進機構
セキュリティセンター 普及啓発・振興部
普及啓発グループ



芳賀 政伸 (中小企業診断士)



芳賀 政伸

Masanobu

Haga

中小企業診断士、システム監査技術者、医療情報技師
東京都立産業技術高等専門学校客員教授

【略歴】

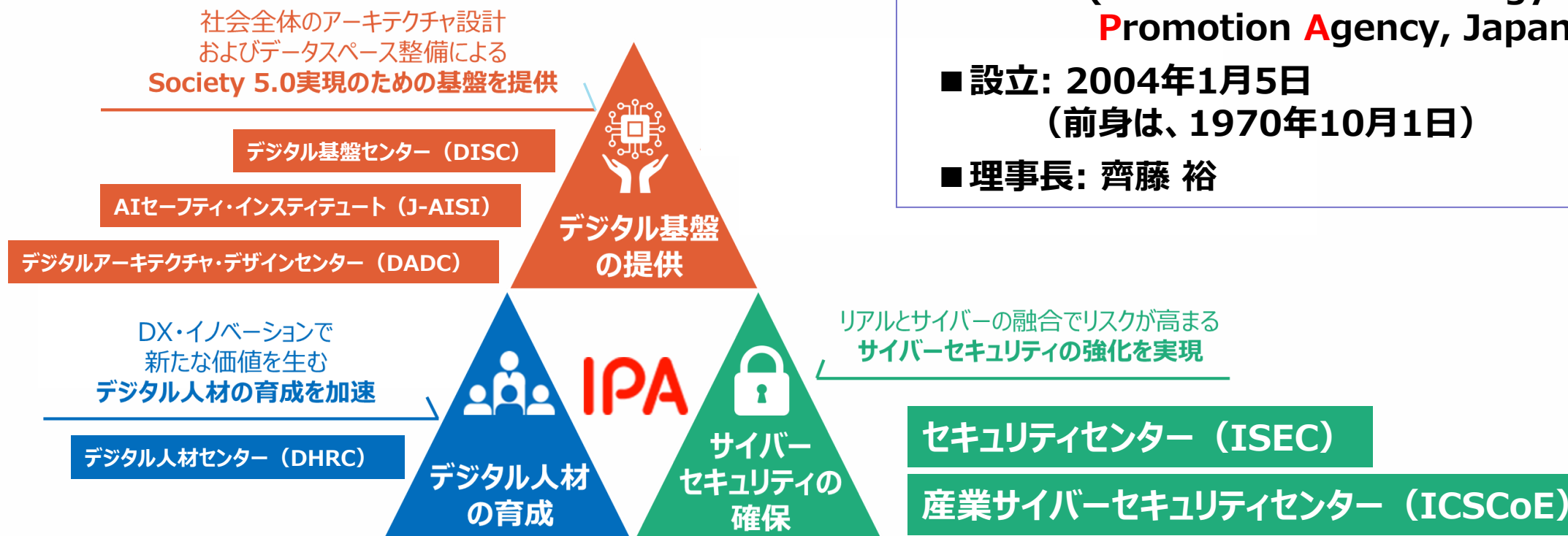
2000年より情報セキュリティ関連業務に従事。官公庁・自治体・金融機関・医療機関・一般企業向けの情報セキュリティコンサルティング及び監査、中小企業の情報セキュリティ統括役員（CISO）等の経験を有する。IPAでは、中小企業のサイバーセキュリティ対策支援事業を担当、各種セミナー等で講演を行う。

独立行政法人情報処理推進機構（IPA）について



日本のIT国家戦略を技術面、人材面から支える経済産業省所管の独立行政法人です。
誰もが安心してITのメリットを実感できる「**頼れるIT社会**」の実現を目指しています。

「**人材**」、「**セキュリティ**」、「**デジタル基盤**」の3つの中核事業



- 名称: 独立行政法人情報処理推進機構
(Information-technology Promotion Agency, Japan)
- 設立: 2004年1月5日
(前身は、1970年10月1日)
- 理事長: 齊藤 裕

サイバーセキュリティに関する業務概要

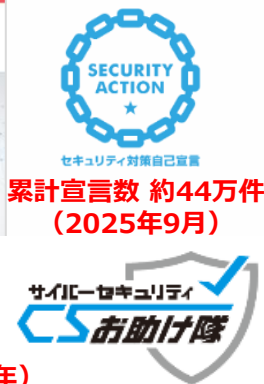
普及啓発／地域・中小企業支援

・地域・中小企業支援

- セキュリティ自己宣言制度
- サイバーセキュリティお助け隊
- セキュリティ相談窓口

・普及啓蒙コンテンツの発信

- セキュリティ10大脅威
- 情報セキュリティ白書
- AIセキュリティ調査



相談受付件数12,787件 (2024年)

サイバー攻撃の検知分析／対処支援

・サイバー情勢の地政学分析

・標的型サイバー攻撃の対策支援

・情報共有 (攻撃対策情報、脆弱性情報、ウイルス・不正アクセス届出)

・不正通信監視 (独法等)

・サイバー事故原因究明



脆弱性データベース
約23万件登録 (2025年3月)

情報共有枠組
業界数14 (組織数305)
(2025年7月現在)

ガイドライン策定／セキュリティ評価・認証

・セキュリティガイドライン (中小企業向け、内部不正対策等)

・情報セキュリティ監査・評価

- 情報セキュリティ監査 (独法等)、政府システム監査
- クラウドセキュリティ評価 (ISMAP)
- 制御システムリスクアセスメント支援

・評価認証・暗号

- IoT製品セキュリティラベリング (JC-STAR)、JISEC
- 暗号動向調査



セキュリティ人材育成

・国家資格「情報処理安全確保支援士」

登録者数24,937名 (2025年10月1日時点)

・中核人材育成プログラム

累計492名修了 (2017年～)

・若手人材発掘 (セキュリティ・キャンプ)

2004年度からの受講者 累計3,107名

・情報セキュリティコンクール

2024年度の応募 約3万点



第一部： セキュリティポリシーの作成について

情報セキュリティ10大脅威

<https://www.ipa.go.jp/security/10threats/10threats2025.html>



- IPAが情報セキュリティ対策の普及を目的に2006年から毎年発行している資料
- 前年に発生したセキュリティ事故や攻撃の状況等から**IPAが脅威候補を選出**、セキュリティ専門家や企業のシステム担当等から構成される「**10大脅威選考会**」が**投票**、**TOP10入りした脅威を「10大脅威」**として脅威の概要、被害事例、対策方法等を解説

<解説書>



脅威に対して様々な立場の方が存在

立場ごとに注意すべき脅威も異なるはず

- 家庭等でパソコンやスマホを利用する人 **「個人」**
- 企業や政府機関などの組織
- 組織のシステム管理者や社員・職員 **「組織」**



「個人」と「組織」の2つの立場で
脅威を解説

情報セキュリティ10大脅威2025

「組織」における脅威動向

- ランサムウェア攻撃、サプライチェーンや委託先を狙った攻撃が昨年に引き続き上位。標的型攻撃も5位と依然として大きな脅威。内部不正の4位にも着目。
- 個々の企業の脆弱性を突いた攻撃だけでなく、サプライチェーンや委託先を狙った攻撃からの脅威が高まっている傾向。

順位	2023	2024	2025
1	ランサムウェアによる被害	ランサムウェアによる被害	ランサム攻撃による被害
2	サプライチェーンの弱点を悪用した攻撃	サプライチェーンの弱点を悪用した攻撃	サプライチェーンや委託先を狙った攻撃
3	標的型攻撃による機密情報の窃取	内部不正による情報漏えい等の被害	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	標的型攻撃による機密情報の窃取	内部不正による情報漏えい等
5	テレワーク等のニューノーマルな働き方を狙った攻撃	修正プログラムの公開前を狙う攻撃 (ゼロデイ攻撃)	機密情報等を狙った標的型攻撃
6	修正プログラムの公開前を狙う攻撃 (ゼロデイ攻撃)	不注意による情報漏えい等の被害	リモートワーク等の環境や仕組みを狙った攻撃
7	ビジネスメール詐欺による金銭被害	脆弱性対策情報の公開に伴う悪用増加	地政学的リスクに起因するサイバー攻撃
8	脆弱性対策情報の公開に伴う悪用増加	ビジネスメール詐欺による金銭被害	分散型サービス妨害攻撃（DDoS 攻撃）
9	不注意による情報漏えい等の被害	テレワーク等のニューノーマルな働き方を狙った攻撃	ビジネスメール詐欺
10	犯罪のビジネス化（アンダーグラウンドサービス）	犯罪のビジネス化（アンダーグラウンドサービス）	不注意による情報漏えい等

結果（被害）
相互の関連も…

サイバー攻撃の
手段（対象）
・サプライチェーン
・システムの脆弱性
・VPN/リモートアクセス
…

情報セキュリティ10大脅威にみる 情報セキュリティ対策の基本

- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない



「情報セキュリティ対策の基本」
を常に意識することが重要

情報セキュリティ対策の基本

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視するべき対策を理解する

脅威から会社をどう守るのか 効果的な解決方法は？

- セキュリティ対策では、“**ふだんからの「人」の対策**”と“**有事に向けた「仕組み」による対策**”の**両方に並行して取組む**ことが重要。

自工会/部工会・ サイバーセキュリティガイドライン

JAMA・JAPIA

自工会/部工会・サイバーセキュリティガイドライン

自動車産業における
サイバーセキュリティ対策の一層の進展のために

2.3 版

2025 年 9 月 1 日



Japan Automobile Manufacturers Association, Inc.

一般社団法人 日本自動車工業会
総合政策委員会
ICT 部会
サイバーセキュリティ分科会



Japan Auto Parts Industries Association

一般社団法人 日本自動車部品工業会
総合技術委員会
DX 対応委員会
サイバーセキュリティ部会

よくあるご質問

中小企業において、「自動車産業サイバーセキュリティガイドライン」自己評価点検で判明した課題にどのように取組むか？

IPAからのご提案

ふだんからの「人」の対策（防御等）

- ・ サイバーセキュリティマネジメント**体制**の整備
- ・ 情報セキュリティ**規程**の作成、周知徹底
- ・ 教育等による社員**意識**醸成、向上



有事に向けた「仕組み」による対策（検知、対応、復旧等）

- ・ 目に見えないサイバー**攻撃**を可視化
- ・ 何か起きた場合の**緊急対応・復旧**

中小企業の情報 セキュリティガイドライン



本日の ご説明

サイバーセキュリティ お助け隊サービス



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

<https://www.ipa.go.jp/security/guide/sme/about.html>



- 中小企業の経営者や実務担当者が、情報セキュリティ**対策の必要性**を理解し**情報を安全に管理**するための具体的な手順等を示したリファレンスマニュアル、ツール&サンプル集
- 本編2部と付録より構成
 - ・ 経営者が認識すべき**「3原則」**、経営者がやらなければならない**「重要7項目の取組」**を記載
 - ・ 情報セキュリティ対策の具体的な進め方を分かりやすく説明
 - ・ すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等の**ひな形**を付録
 - ・ **「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」**を追加



※2023年4月26日 第3.1版公表

中小企業の情報セキュリティガイドライン（第1部 経営者編）

経営者が認識すべき「3原則」

● 経営者は、以下の**3原則**を認識し、対策を進める

原則 1 情報セキュリティ対策は経営者の**リーダーシップ**で進める

- 経営者は、IT 活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシップを発揮して対策の実施を主導

原則 2 **委託先**の情報セキュリティ対策まで考慮する

- 必要に応じて委託先が実施している情報セキュリティ対策も確認し、不十分な場合は対処を検討



原則 3 関係者とは常に情報セキュリティに関する**コミュニケーション**をとる

- 情報セキュリティに関する取組方針を明確に整理し、常日頃より関係者に伝えておくことで、サイバー攻撃によるウイルス感染や情報漏えいなどが発生した際にも、関係者の不信感の高まりを抑えることが可能



中小企業の情報セキュリティガイドライン（第1部 経営者編）

実行すべき「重要7項目の取組」

- 経営者は、以下の **7 項目** を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

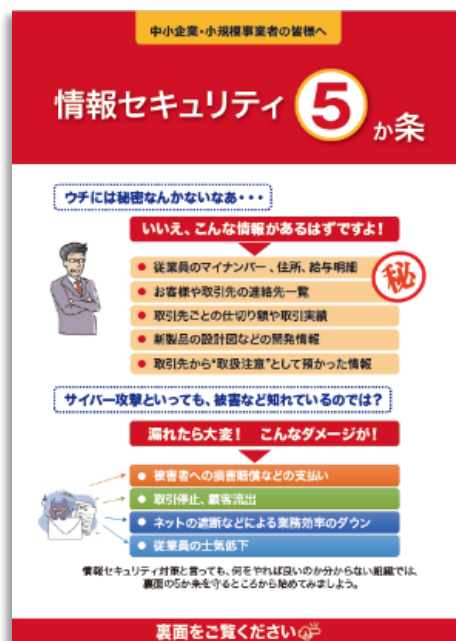
取組 1	情報セキュリティに関する 組織全体の対応方針 を定める
取組 2	情報セキュリティ対策のための 予算や人材 などを確保する
取組 3	必要と考えられる対策を 検討させて実行を指示 する
取組 4	情報セキュリティ対策に関する 適宜の見直し を指示する
取組 5	緊急時の対応や復旧のための 体制を整備 する
取組 6	委託や外部サービス利用の際にはセキュリティに関する 責任を明確 にする
取組 7	情報セキュリティに関する 最新動向を収集 する

中小企業の情報セキュリティガイドライン（第2部 実践編） 具体的な対策の進め方

● できるところから始めて段階的にステップアップ

Step1

できるところから始める



情報セキュリティ 5 か条

Step2

組織的な取り組みを開始
する



5分でできる!
情報セキュリティ自社診断

Step3

本格的に取り組む



情報セキュリティ関連規程

Step4

より強固にするための方策

- 情報収集と共有
- ウェブサイトの情報セキュリティ
- クラウドサービスの情報セキュリティ
- テレワークの情報セキュリティ
- セキュリティインシデント対応
- セキュリティサービス例と活用
- 技術的対策例と活用
- 詳細リスク分析の実施方法

より強固にするため方策

できるところから始める 情報セキュリティ5か条

Step1
できるところから始める



● 情報セキュリティ対策と言っても、何をやれば良いのか？

情報セキュリティ10大脅威でみる

情報セキュリティ対策の基本

- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない

攻撃の糸口	情報セキュリティ対策の基本	目的
ソフトウェアの脆弱性	ソフトウェアの更新	脆弱性を解消し攻撃によるリスクを低減する
ウイルス感染	セキュリティソフトの利用	攻撃をブロックする
パスワード窃取	パスワードの管理・認証の強化	パスワード窃取によるリスクを低減する
設定不備	設定の見直し	誤った設定を攻撃に利用されないようにする
誘導（罠にはめる）	脅威・手口を知る	手口から重要視すべき対策を理解する

情報セキュリティ **5** か条

を守るところから始めてみましょう。

- 1 OSやソフトウェアは常に最新の状態にしよう！**
- 2 ウイルス対策ソフトを導入しよう！**
- 3 パスワードを強化しよう！**
- 4 共有設定を見直そう！**
- 5 脅威や攻撃の手口を知ろう！**

中小企業・小規模事業者の皆様へ

情報セキュリティ **5** か条

ウチには秘密なんかないなあ・・・

いいえ、こんな情報があるはずですよ！

- 従業員のマイナンバー、住所、給与明細
- お客様や取引先の連絡先一覧
- 取引先ごとの仕切り額や取引実績
- 新製品の設計図などの開発情報
- 取引先から「取扱注意」として預かった情報

サイバー攻撃といっても、被害など知れているのでは？

漏れたら大変！ こんなダメージが！

- 被害者への損害賠償などの支払い
- 取引停止、顧客流出
- ネットの遮断などによる業務効率のダウン
- 従業員の士気低下

情報セキュリティ対策と言っても、何をやれば良いのか分からない組織では、裏面の5か条を守るところから始めてみましょう。

裏面をご覧ください

中小企業の情報セキュリティ対策ガイドライン
付録1：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に

Step1
できるところから始める

- 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。
- OSやソフトウェアには、**修正プログラム**を適用する、もしくは**最新版**を利用する。

<対策例>

- Windows Update(Windows OSの場合)/ソフトウェア・アップデート(Mac OSの場合)/OSバージョンアップ(Android の場合)
- Adobe Flash Player/Adobe Reader/Java実行環境(JRE) など利用中のソフトウェアを最新版にする



MyJVNバージョンチェッカの活用

<http://jvndb.jvn.jp/apis/myjvn/>



JVN iPedia 脆弱性対策情報データベース

JVN は、日本で使用されているソフトウェアなどの脆弱性関連情報とその対策情報を提供し、情報セキュリティ対策に資することを目的とする脆弱性対策情報ポータルサイトです。JPCERT コーディネーションセンターと独立行政法人情報処理推進機構 (IPA)が共同で運営しています。

実行ボタンを押すだけ！

チェック対象のソフトウェア製品名一覧

ソフトウェア製品名	チェック結果 (○が最新)	結果詳細
Adobe Flash Player (ActiveX)	○ 最新のバージョンです	表示
Adobe Reader	○ 最新のバージョンです	表示
JRE	○ 最新のバージョンです	表示
Unplus	○ 最新のバージョンです	表示
Adobe Flash Player (Plug-in)	— インストールされていないか、対象外のバージョンです	
Adobe Shockwave Player	— インストールされていないか、対象外のバージョンです	
Becky Internet Mail	— インストールされていないか、対象外のバージョンです	
Lunaspape	— インストールされていないか、対象外のバージョンです	
Mozilla Firefox	— インストールされていないか、対象外のバージョンです	
Mozilla Thunderbird	— インストールされていないか、対象外のバージョンです	
OpenOffice.org	— インストールされていないか、対象外のバージョンです	

チェック対象を“○”か“×”で表示

チェック結果の詳細を表示

バージョンアップ方法は下記URLを参照ください。
<http://jvndb.jvn.jp/apis/myjvn/updates.html>

② ウイルス対策ソフトを導入

Step1
できるところから始める

- 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したりするウイルスが増加。
- 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。

<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(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)を導入する



ウイルス対策ソフト に関する勘違い

- ④ ウイルス対策ソフトは万能薬？
これさえあればウイルスなんか怖くない？
 - ➡ ウイルス対策ソフトの利用は予防手段のひとつ
 - ➡ 新種のウイルスや亜種を取り逃がす場合もある
 - ➡ 壊されたファイルやシステム環境は復旧でない
- ➡ だから…

過信は禁物 !!

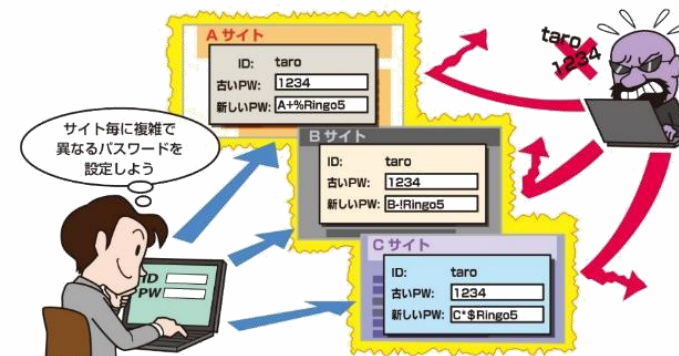
③ パスワードを強化

Step1
できるところから始める

- 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**が増加。
- パスワードは「**長く**」、「**複雑に**」、「**使い回さない**」ようにして強化を。

＜対策例＞

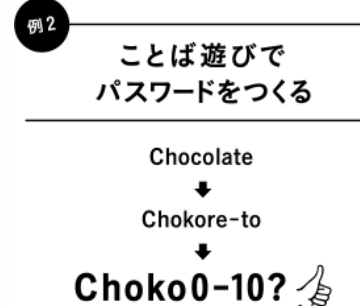
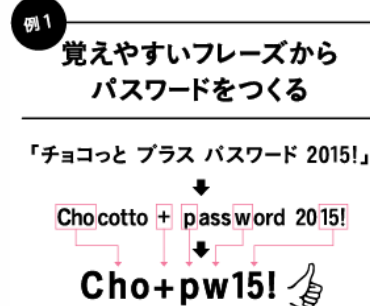
- ・ パスワードは英数字記号含めて長い文字数にする
- ・ 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- ・ 同じID・パスワードをいろいろなウェブサービスで使い回さない



安全なパスワードとは？

IPA「チョコっとプラスパスワード」から
<https://www.ipa.go.jp/chocotto/pw.html>

- ✓ 最低でも8文字以上の文字数で構成されている。
- ✓ パスワードの中に数字や、「@」、「%」、「!」などの記号も混ぜている。
- ✓ パスワード内のアルファベットに大文字と小文字の両方を入れている。
- ✓ サービスごとに違うパスワードを設定している。



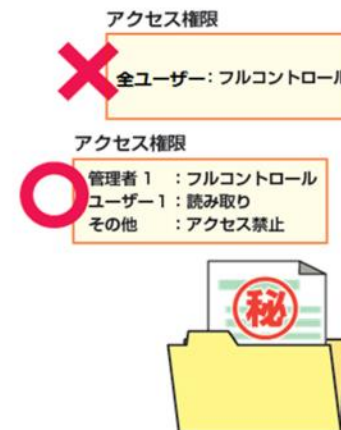
④ 共有設定を見直す

Step1
できるところから始める

- 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。
- 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の確認を。

<対策例>

- ・ ウェブサービスの共有範囲を限定する
- ・ ネットワーク接続の複合機やカメラ、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設定の変更(削除)漏れがないように注意する



例えばこんな対策...

- ネットワーク接続可能なオフィス機器やウェブサービスは、特定の人やグループしかアクセスできないようにするアクセス制御機能を備えていることが多い。
- ファイルサーバーなどのオフィス機器や、業務で利用するウェブサービスに業務重情報などを保存する場合は、必要な人だけしかアクセスできないように、アクセス制御機能を活用する。



Windows10
の設定画面

⑤ 脅威や攻撃の手口を知る

Step1
できるところから始める

- **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**が増加。
- 脅威や攻撃の手口を知って適切な対策を！

＜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



組織的な情報収集を

サイバーセキュリティ注意喚起サービス「icat for JSON」

<https://www.ipa.go.jp/security/vuln/icat.html>

「icat for JSON（アイキャット・フォー・ジェイソン）」は、IPAが公開した「重要なセキュリティ情報」をリアルタイムに配信するサービスです。組織のポータルサイトや会員向けウェブサイトなどに設置をすることで、ウェブサイト利用者に向けてセキュリティ対策をリアルタイムに周知することが可能になります。



組織的な取り組みを開始する 情報セキュリティ基本方針の公開

Step2
組織的な取り組みを
開始する



● 組織的なセキュリティの取り組みの第一歩として「情報セキュリティ基本方針」を定め、外部に向けて公開する

➤ 情報セキュリティ基本方針

情報セキュリティに関する企業としての方針、取り組みの指針などを明文化したもの、自社のウェブサイトや会社案内等にて公開

情報セキュリティ基本方針の記載項目例

- ・ 経営者の責任
- ・ 社内体制の整備
- ・ 従業員の取り組み
- ・ 法令及び契約上の要求事項の遵守
- ・ 違反及び事故への対応

中小企業の情報セキュリティ対策ガイドライン 付録2

情報セキュリティ基本方針(サンプル)

中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。
※赤字箇所は、自社の事情に応じた内容(役職名、担当者など)に書き換えてください。
※青字箇所は、自社の事情に応じた文言を選択してください。

情報セキュリティ基本方針

株式会社〇〇〇〇(以下、当社は、お客様からお預かりした/当社の/情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

1. 経営者の責任
当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。
2. 社内体制の整備
当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内
の正式な規則として定めます。
3. 従業員の取り組み
当社の従業員は、情報セキュリティのために必要とされる知識、技術を得得し、情報セキュリティへの取り組みを確かなものにします。
4. 法令及び契約上の要求事項の遵守
当社は、情報セキュリティに関わる法令、規則、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。
5. 違反及び事故への対応
当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努めます。

制定日: 20〇〇年〇月〇日
株式会社〇〇〇〇
代表取締役社長 〇〇〇〇

中小企業の情報セキュリティ対策ガイドライン
付録2: 情報セキュリティ基本方針 (サンプル)

● 「5分でできる！情報セキュリティ自社診断」を実施し、自社の情報セキュリティの問題点を把握する

➤ 5分でできる！情報セキュリティ自社診断

25個の診断項目に答えるだけで、自社の情報セキュリティの問題点を簡単に把握できる診断ツール（診断ツールはシート版を提供）

<https://www.ipa.go.jp/security/keihatsu/sme/guideline/5minutes.html>

前提：重要な情報（資産）って…

- ✓ 企業にとってその情報が企業外に漏れると、企業の事業運営上で重大な問題を引き起こす可能性のある情報が重要な情報
＜例＞ お客様から預かっている個人情報
企業で働く従業員の個人情報
企業運営のための企業情報
ノウハウ等の機密情報
- ✓ 何が重要な情報が理解することが情報セキュリティ対策の第一歩

中小企業・小規模事業者の皆様へ

新 5分でできる！
情報セキュリティ自社診断

最新動向への対応、できていますか？

脅威や攻撃の変化 IT環境の変化

標的型攻撃
ランサムウェア
パスワードリスト攻撃
クラウド
IoT機器
スマートフォン

取り返しのつかないことになる前に
あなたの会社のセキュリティ状況を
「5分でできる！自社診断」でチェック！

5分でできる！情報セキュリティ自社診断 自社診断のための25項目

Step2
組織的な取り組みを
開始する



- 25項目の設問に答え、自社の
情報セキュリティ対策の実施状況を把握

基本的対策 5項目

脆弱性対策、ウイルス対策、パスワード強化など

従業員としての対策 13項目

標的型攻撃メール、電子メール、ウェブ利用、
持ち出し、廃棄など

組織としての対策 7項目

守秘義務、教育、委託先管理、ルール化 など

No	診断内容	チェック			
基本的対策	1 パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	実施して いる	一部実施 している	実施して いない	わから ない
	2 パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル ^{※1} は最新の 状態にしていますか？				
	3 パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？				
	4 重要情報 ^{※2} に対する適切なアクセス制限を行っていますか？				
	5 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？				
従業員としての対策	6 電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？	4	2	0	-1
	7 電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？				
	8 重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護 していますか？				
	9 無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？				
	10 インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていま すか？				
	11 パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを 取得していますか？				
	12 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫など に安全に保管していますか？				
	13 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？				
	14 離席時にパソコン画面の覗き見や勝手な操作:				
	15 関係者以外の事務所への立ち入りを制限して:				
	16 退社時にノートパソコンや備品を施錠保管す:				
	17 事務所が無人になる時の施錠忘れ対策を実施				
	18 重要情報が記載された書類や重要なデータが:				
組織としての対策	19 従業員に守秘義務を理解してもらい、業務上 守らせていますか？	4	2	0	-1
	20 従業員にセキュリティに関する教育や注意喚				
	21 個人所有の情報機器を業務で利用する場合の				
	22 重要情報の授受を伴う取引先との契約書には、				
	23 クラウドサービスやウェブサイトの運用など して選定していますか？				
	24 セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備を していますか？				
	25 情報セキュリティ対策（上記1～24など）をルール化し、従業員に明示していますか？				

組織的な取り組みを開始する 対策の決定と周知

Step2
組織的な取り組みを
開始する

IPA


- 問題があった項目は「5分でできる！ 情報セキュリティ自社診断 解説編」を参考に対策を決定
- 付録「情報セキュリティハンドブック(ひな形)」を編集して社内周知

「5分でできる！ 情報セキュリティ自社診断 解説編」

解説編

Part 1 基本的対策

No.1~5は企業の規模や用途を問わず、必ず対策していただきたい5項目です。いずれも一度やればよいものではなく、継続的な対策実施が必要のため、運用ルールとして社内定着させる必要があります。



診断編 NO.1 脆弱性対策

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、もしくは最新版を利用するようにしましょう。

対策例 Windows Updateを実施する(Windows OSの場合)、Adobe Flash Player・Adobe Reader・Java実行環境などの利用中のソフトウェアを最新版にするなど。

診断編 NO.2 ウイルス対策

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、ファイルの暗号化を強制的に実行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最新状態になるように設定する、悪質なセキュリティ対策ソフトの導入を抑制するなど。

診断編 NO.4 情報の取扱い

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装置の設定を見直したために、関係のない人に情報を見られるトラブルが増えています。関係のない人が、ウェブサービスや装置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 ウェブサービスの共有機能を見直し、ネットワーク接続の装置の共有設定、ハードディスク(HDD)などの共有機能を見直し、関係のない人のアクセスの制限(閲覧・操作)が行えないように設定するなど。

診断編 NO.5 脅威や攻撃の手法を知り、対策を講じる

取引先や関係者と偽装して、ウイルスや不正アクセスの誘導や攻撃の手法を知り、脅威や攻撃の手法を知り、対策を講じる。

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法を知り、関係のない人への誘導や攻撃の手法を知り、対策を講じる。

対策例を参考にして決定

診断編 NO.1 脆弱性対策

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、もしくは最新版を利用するようにしましょう。

対策例

Windows Updateを実施する(Windows OSの場合)、Adobe Flash Player・Adobe Reader・Java実行環境などの利用中のソフトウェアを最新版にするなど。



情報セキュリティハンドブック
を編集して従業員へ周知

1-1 全社基本ルール

OSとソフトウェアのインストール・更新に関するルール

- パソコンのインストール・更新は、必ず事前に承認を得る。
- 業務上必要なソフトウェアのインストール・更新は、承認を得る。
- 承認を得たソフトウェアのインストール・更新は、承認を得た範囲内で実施する。
- 承認を得たソフトウェアのインストール・更新は、承認を得た範囲内で実施する。

2-1 仕事中的ルール

電子メールの送信に関するルール

- メール送信する際は、必ず宛先を確認する。
- メール送信する際は、必ず宛先を確認する。
- メール送信する際は、必ず宛先を確認する。
- メール送信する際は、必ず宛先を確認する。

3-1 全社共通のルール

私有情報機器の利用

自己診断No. 2.1

● 私有の情報機器を業務で利用する場合は以下を順守する。

情報機器の種類	順守事項
パソコン ※自宅パソコンでも業務を行う場合を含む	<ul style="list-style-type: none">● 社内へ無断で持ち込むことを禁止する● 業務利用を禁止する● 社内LANへの接続を禁止する● ウイルス対策ソフト、アプリケーションソフトは総務部システム担当が指定したものを導入し、許可を得たうえで利用する● 業務終了後に業務用データは総務部システム担当の指定するツールで完全に消去する● 従業員個人のメールアドレスに業務用データを添付して送信することを禁止する● 社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する
スマートフォン タブレット端末 携帯電話など 記憶・通信機能備えた機器	<ul style="list-style-type: none">● 会社で貸与した機器を利用する● 地図検索、路線案内を除き業務利用を禁止する● 充電を除き、社内パソコンへの接続を禁止する● ウイルス対策ソフト、アプリケーションソフトのインストールは総務部システム担当が指定したものを導入し、許可を得たうえで利用する● 取引先アドレスを除く業務用データの保存を禁止する● 従業員個人のメールアドレスに業務用データを添付して送信することを禁止する● 社用メールアドレスで受信したメールを従業員個人のアドレスに転送することを禁止する
USBメモリ 外付けHDDなどの記憶機能備えた機器・媒体	<ul style="list-style-type: none">● 会社で貸与した機器を利用する● 私有物の利用を禁止する● 総務部システム担当の許可を得て利用する● 業務終了後に業務用データは総務部システム担当の指定するツールで完全に消去する

第二部： 情報セキュリティ関連規程の作り方

本格的に取り組む 情報セキュリティ関連規程

Step3
本格的に取り組む



◇情報セキュリティ管理規程（サンプル）

	名称	概要	項目
1	組織的対策	情報セキュリティのための管理体制の構築や点検、情報共有などのルール	1.情報セキュリティのための組織 2.情報セキュリティ取組みの監査・点検/点検 3.情報セキュリティに関する情報共有
2	人的対策	取締役及び従業員の責務や教育、人材育成などのルール	1.雇用条件 2.従業員の責務 3.雇用の終了 4.情報セキュリティ教育 5.人材育成
3	情報資産管理	情報資産の管理や持ち出し方法、バックアップ、破棄などのルール	1.情報資産の管理 2.情報資産の社外持ち出し 3.媒体の処分 4.バックアップ
4	アクセス制御及び認証	情報資産に対するアクセス制御方針や認証のルール	1.アクセス制御方針 2.利用者の認証 3.利用者アカウントの登録 4.利用者アカウントの管理 5.パスワードの設定 6.従業員以外の者に対する利用者アカウントの発行 7.端末の識別による認証 8.端末のタイムアウト機能 9.標準設定等

	名称	概要	項目
5	物理的対策	セキュリティを保つべきオフィス、部屋及び施設などの領域設定や領域内での注意事項などのルール	1.セキュリティ領域の設定 2.関連設備の管理 3.セキュリティ領域内注意事項 4.搬入物の受け渡し
6	IT機器利用	IT機器やソフトウェアの利用などのルール	1.ソフトウェアの利用 2. I T 機器の利用 3.クリアデスク・クリアスクリーン 4.インターネットの利用 5.私有 I T 機器・電子媒体の利用 6.標準等
7	IT基盤運用管理	サーバーやネットワーク等のITインフラに関するルール	1.管理体制 2. I T 基盤の情報セキュリティ対策 3. I T 基盤の運用 4.クラウドサービスの導入 5.脅威や攻撃に関する情報の収集 6.廃棄・返却・譲渡 7. I T 基盤の情報セキュリティ要件及び標準

本格的に取り組む 情報セキュリティ関連規程

Step3
本格的に取り組む



◇情報セキュリティ管理規程（サンプル）

	名称	概要	項目
8	システム開発及び保守	独自に開発及び保守を行う情報システムに関するルール	1.新規システム開発・改修 2.脆弱性への対処 3.情報システムの開発環境 4.情報システムの保守 5.情報システムの変更
9	委託管理	業務委託にあたっての選定や契約、評価のルール（委託先チェックリストのサンプルが付属）	1.委託先評価基準 2.委託先の選定 3.委託契約の締結 4.委託先の評価 5.再委託
10	情報セキュリティインシデント対応及び事業継続管理	情報セキュリティに関する事故対応や事業継続管理などのルール	1.対応体制 2.情報セキュリティインシデントの影響範囲と対応者 3.インシデントの連絡及び報告 4.対応手順 5.届出及び相談 6.情報セキュリティインシデントによる事業中断と事業継続管理 7.事業継続計画
11	テレワークにおける対策	テレワークのセキュリティ対策についてのルール	1.テレワーク共通ルール 2.情報機器のセキュリティ 3.ネットワーク機器のセキュリティ：テレワークのネットワーク環境 4.勤務中のルール 5.データ・書類の保存 6.社内問い合わせ・緊急連絡先

【参考】自動車産業向けサンプル規程の作成

- 令和5年度「業界セキュリティガイドライン等の策定支援業務」において、「自工会/部工会・サイバーセキュリティガイドライン 2.1版」（LV1）に対応した「自動車産業向けサンプル規程」を作成した。

◇情報セキュリティ関連規程（サンプル） 自工会/部工会・サイバーセキュリティガイドライン V2.1対応版

「自工会/部工会・サイバーセキュリティガイドライン 2.1版」LV1 50項目と、「中小企業の情報セキュリティガイドライン」の実施項目を突合し、不足項目を付録5 サンプル規程に追記した。

業界ガイドラインと「中小企業の情報セキュリティガイドライン」突合表（イメージ）

項目	項目番号	項目名	項目内容	項目番号	項目名	項目内容	項目番号	項目名	項目内容	項目番号	項目名	項目内容	項目番号	項目名	項目内容	項目番号	項目名	項目内容	項目番号	項目名	項目内容
1	1.1	組織的対策	組織的対策	1.1	組織的対策	組織的対策	1.1	組織的対策	組織的対策	1.1	組織的対策	組織的対策	1.1	組織的対策	組織的対策	1.1	組織的対策	組織的対策	1.1	組織的対策	組織的対策
	1.2	人的対策	人的対策	1.2	人的対策	人的対策	1.2	人的対策	人的対策	1.2	人的対策	人的対策	1.2	人的対策	人的対策	1.2	人的対策	人的対策	1.2	人的対策	人的対策
	1.3	情報資産管理	情報資産管理	1.3	情報資産管理	情報資産管理	1.3	情報資産管理	情報資産管理	1.3	情報資産管理	情報資産管理	1.3	情報資産管理	情報資産管理	1.3	情報資産管理	情報資産管理	1.3	情報資産管理	情報資産管理
	1.4	アクセス制御及び認証	アクセス制御及び認証	1.4	アクセス制御及び認証	アクセス制御及び認証	1.4	アクセス制御及び認証	アクセス制御及び認証	1.4	アクセス制御及び認証	アクセス制御及び認証	1.4	アクセス制御及び認証	アクセス制御及び認証	1.4	アクセス制御及び認証	アクセス制御及び認証	1.4	アクセス制御及び認証	アクセス制御及び認証
2	2.1	物理的対策	物理的対策	2.1	物理的対策	物理的対策	2.1	物理的対策	物理的対策	2.1	物理的対策	物理的対策	2.1	物理的対策	物理的対策	2.1	物理的対策	物理的対策	2.1	物理的対策	物理的対策
	2.2	IT機器利用	IT機器利用	2.2	IT機器利用	IT機器利用	2.2	IT機器利用	IT機器利用	2.2	IT機器利用	IT機器利用	2.2	IT機器利用	IT機器利用	2.2	IT機器利用	IT機器利用	2.2	IT機器利用	IT機器利用
	2.3	IT基盤運用管理	IT基盤運用管理	2.3	IT基盤運用管理	IT基盤運用管理	2.3	IT基盤運用管理	IT基盤運用管理	2.3	IT基盤運用管理	IT基盤運用管理	2.3	IT基盤運用管理	IT基盤運用管理	2.3	IT基盤運用管理	IT基盤運用管理	2.3	IT基盤運用管理	IT基盤運用管理
	2.4	システム開発及び保守	システム開発及び保守	2.4	システム開発及び保守	システム開発及び保守	2.4	システム開発及び保守	システム開発及び保守	2.4	システム開発及び保守	システム開発及び保守	2.4	システム開発及び保守	システム開発及び保守	2.4	システム開発及び保守	システム開発及び保守	2.4	システム開発及び保守	システム開発及び保守
3	3.1	委託管理	委託管理	3.1	委託管理	委託管理	3.1	委託管理	委託管理	3.1	委託管理	委託管理	3.1	委託管理	委託管理	3.1	委託管理	委託管理	3.1	委託管理	委託管理
	3.2	情報セキュリティインシデント対応及び事業継続管理	情報セキュリティインシデント対応及び事業継続管理	3.2	情報セキュリティインシデント対応及び事業継続管理	情報セキュリティインシデント対応及び事業継続管理	3.2	情報セキュリティインシデント対応及び事業継続管理	情報セキュリティインシデント対応及び事業継続管理	3.2	情報セキュリティインシデント対応及び事業継続管理	情報セキュリティインシデント対応及び事業継続管理	3.2	情報セキュリティインシデント対応及び事業継続管理	情報セキュリティインシデント対応及び事業継続管理	3.2	情報セキュリティインシデント対応及び事業継続管理	情報セキュリティインシデント対応及び事業継続管理	3.2	情報セキュリティインシデント対応及び事業継続管理	情報セキュリティインシデント対応及び事業継続管理
	3.3	テレワークにおける対策	テレワークにおける対策	3.3	テレワークにおける対策	テレワークにおける対策	3.3	テレワークにおける対策	テレワークにおける対策	3.3	テレワークにおける対策	テレワークにおける対策	3.3	テレワークにおける対策	テレワークにおける対策	3.3	テレワークにおける対策	テレワークにおける対策	3.3	テレワークにおける対策	テレワークにおける対策
	3.4	その他	その他	3.4	その他	その他	3.4	その他	その他	3.4	その他	その他	3.4	その他	その他	3.4	その他	その他	3.4	その他	その他



中小企業の情報セキュリティ対策ガイドライン 付録5	
情報セキュリティ関連規程(サンプル)	
自工会/部工会・サイバーセキュリティガイドライン V2.1 対応版 (1/9 版)	
中小企業向けの情報セキュリティ関連規程のサンプルです。必要な対策を選択し、編集することで自社の情報セキュリティ関連規程を作成することができます。 ※赤字箇所は、自社の事情に応じた内容(役職名、担当者名など)に書き換えてください。 ※青字箇所は、自社の事情に応じた文言を選択してください。 ※黄色蛍光箇所は、中小企業の情報セキュリティ対策ガイドライン第3版からの変更箇所を表しております。 ※緑色蛍光箇所は、自工会/部工会ガイドライン対応として追記された項目です。	
目次	
1 組織的対策	1 ページ
2 人的対策	3 ページ
3 情報資産管理	5 ページ
4 アクセス制御及び認証	9 ページ
5 物理的対策	13 ページ
6 IT機器利用	15 ページ
7 IT基盤運用管理	23 ページ
8 システム開発及び保守	27 ページ
9 委託管理	29 ページ
10 情報セキュリティインシデント対応及び事業継続管理	32 ページ
11 テレワークにおける対策	38 ページ
(Ver.2.1)	

【参考】自動車業界向けサンプル規程の適用評価例

- 業界ガイドライン（業界向けサンプル規程）適用の評価先として、業界に属する中小企業を業界団体の推薦等により選定し、セキュリティ専門家（情報処理安全確保支援士※）によるマネジメント指導（訪問）を1社あたり4回実施した。

◇セキュリティ専門家によるマネジメント指導結果（自動車部品業界：4社）

- 自社のセキュリティ規程が未整備の場合、「自動車産業向けサンプル規程」がそのまま活用可能であった。サンプル規程を参照して、自社の規程の見直しを行うことも有効であった。また、ISO9001など既存のISOの取組みに、セキュリティ対策を折り込むと効率的である。
- IT専任者がいない中小企業においては、セキュリティ専門家によるマネジメント指導が有効である。例えば、ひとつの工場で他工場の担当者も参加したマネジメント指導をOJT的に行い、参加者が実施方法を自分の工場に持ち帰り、横展開する取組みも見受けられた。

企業名	A社	B社	C社	D社
所在地	三重県伊賀市	愛知県名古屋市	岐阜県関市	愛知県犬山市
業種	軸受部品製造	メッキ加工	プレス加工	金属切削加工
業界ガイドライン 適用評価＆活用 ヒント	<ul style="list-style-type: none">・ サンプル規程を用いて、<u>自社のセキュリティ規程を新規に策定</u>。・ 組織的・人的・物理的対策を優先して実施。・ 技術情報管理は、<u>ISO 9001の文書管理に基づく対策が効率的</u>。	<ul style="list-style-type: none">・ サンプル規程を参照しながら、<u>既存の規程を見直し改定</u>。・ <u>ひとつの工場で規程を見直した後、他の工場への展開</u>を行う。・ 経営層を巻き込み、体制整備等管理面の対策を推進予定。	<ul style="list-style-type: none">・ サンプル規程を参照し、<u>セキュリティ規程を策定中</u>。・ <u>ISO 9001に準じ、教育の計画立案、実施手順を作成</u>。・ 情報資産に対する<u>リスク評価が困難</u>であったが、マネジメント指導業務を通じて支援。	<ul style="list-style-type: none">・ サンプル規程を用いて、<u>自社のセキュリティ規程を新規に策定</u>。・ マネジメント指導業務を通じて、<u>情報資産のライフサイクルを通じた管理、委託先選定ルール策定、緊急連絡体制</u>等を整備。

※情報処理安全確保支援士（通称：登録セキスペ、英語名：RISS）

サイバーセキュリティ対策を推進する人材の国家資格。サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言等を行い、サイバーセキュリティの確保を支援する。登録人数：21,727名（2023年10月時点）。
<https://www.ipa.go.jp/jinzai/riss/index.html>

より強固にするための方策 情報資産の洗い出しとリスク分析

Step4
より強固にするための
方策



- 「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」の付録7「リスク分析シート」をもとに、社内での情報資産の洗い出し及びそれらに対するリスク分析を実施する。
- リスク分析結果をもとに、情報資産に対するセキュリティ対策を検討する。

情報資産の 洗い出し

どのような情報資産があるか洗い出して
重要度を判断する

リスク値の 算定

優先的・重点的に対策が必要な情報
資産を把握する

情報セキュリティ 対策の決定

リスクの大きな情報資産に対して必要
とされる対策を検討する

業務 分類	情報資産名称	備考	利用者 範囲	管理 部署	媒体・保存先	個人情報の種類			評価値				保存 期限	登録日	現状から想定されるリスク（入力不要・自動表示）			
						個人 情報	要配慮 個人情報	特定 個人 情報	機密性	完全性	可用性	重要度			脅威の発生頻度 ※「脅威の状況」 シートに入力すると表示	脆弱性 ※「対策状況チェッ ク」シートに入力すると表示	被害発生 可能性	リスク値
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			3	1	1	3		2023/4/1	3:通常の状態では脅威が発生する (いつ発生してもおかしくない)	2:部分的に対策を実施して いる	2 可能性： 中	6 リスク大
人事	社員名簿	社員基本情報	人事部	人事部	書類	有			3	3	3	3		2023/4/1	2:特定の状況で脅威が発生する (年に数回程度)	2:部分的に対策を実施して いる	1 可能性： 低	3 リスク小
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		3	3	2	3	5年	2023/4/1	2:特定の状況で脅威が発生する (年に数回程度)	2:部分的に対策を実施して いる	1 可能性： 低	3 リスク小
経理	給与システム データ	税務署提出用 源泉徴収票	給与計 算担当	人事部	事務所PC			有	3	3	2	3	7年	2023/4/1	3:通常の状態では脅威が発生する (いつ発生してもおかしくない)	2:部分的に対策を実施して いる	2 可能性： 中	6 リスク大

付録7「リスク分析シート」

より強固にするための方策 クラウドサービスの安全利用

Step4
より強固にするための
方策

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」の付録6「クラウドサービス安全利用の手引き」の考え方をもとに、社内でのクラウドサービス安全利用策を検討する。

クラウドサービスの 選定

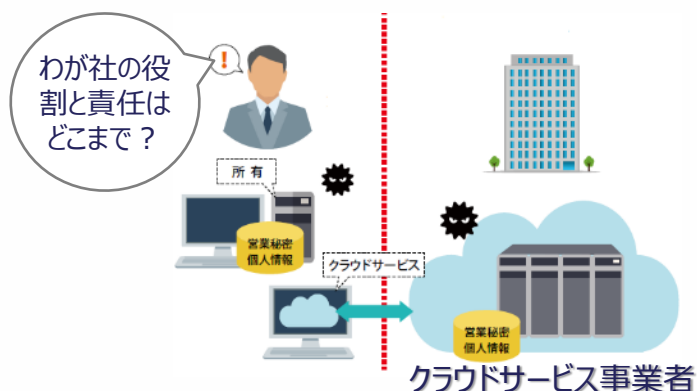
クラウド化する業務によって重視すべきセキュリティ対策は異なるため、業務のセキュリティ要件に見合ったサービスを選定する。

クラウドサービスの 運用

クラウドサービスは提供者と利用者が連携して運用するため、その特性を理解して運用する。

クラウドサービスの セキュリティ対策

クラウドサービス利用者が対応すべきセキュリティ対策を理解して実施する。



1	11	付帯するセキュリティ対策を確認する	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
2			
3	12	利用者サポートの体制を確認する	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
4			
5	13	利用終了時のデータを確保する	サービスの利用が終了したときの、データの取扱い条件について確認しましたか？
6			
7	14	適用法令や契約条件を確認する	個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？
8			
9	15	データ保存先の地理的所在地を確認する	データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？
10			

付録6「**中小企業のためのクラウドサービス安全利用の手引き**」にて
ポイント(チェックリスト)の各項目について解説



より強固にするための方策 セキュリティインシデント対応

Step4
より強固にするための
方策



● セキュリティインシデント発生時の対応に関するポイントを説明

検知・初動対応

インシデントを検知した場合は、速やかに情報セキュリティ責任者へ連絡し、被害を拡大させないための初動対応を行います。

報告・公表

顧客や関係者、行政機関、一般・メディア等に対して、必要な場合は適時の報告や情報公開を行います。

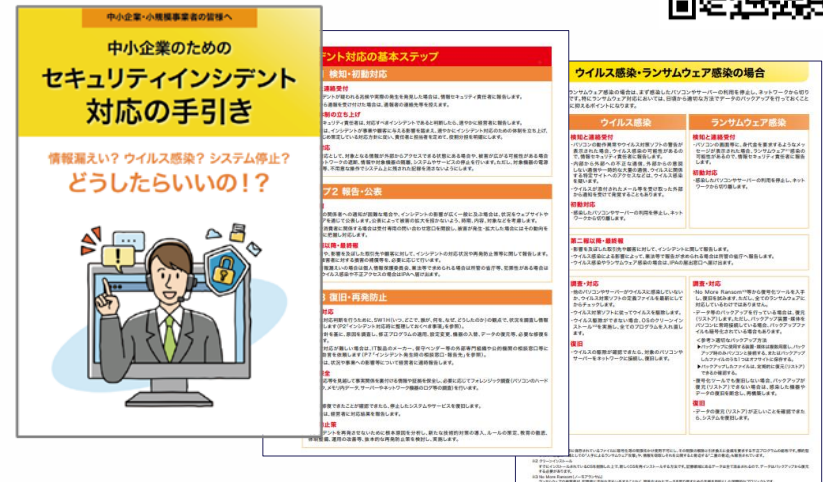
復旧・再発防止

システム管理者や外部専門組織と協力して、迅速な復旧作業や根本的な再発防止策を検討しましょう。



「ウイルス感染・ランサムウェア感染の場合」「情報漏えいの場合」「システム停止の場合」といった場合ごとに解説するほか、相談窓口や報告先も紹介

付録8「**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**」にて
対応方法の詳細や相談・報告先などを解説



(参考情報)

IPAのツール・制度のご紹介

中小企業向けサイバーセキュリティ対策支援者リスト

<https://www.ipa.go.jp/security/sme/shien/list.html>



● 情報セキュリティ規程整備をはじめ、セキュリティ対策の実施をセキュリティ専門家が支援。

◇ 中小企業向けサイバーセキュリティ対策支援者リスト

- 国家資格「**情報処理安全確保支援士（登録セキスペ）※**」の資格者のうち、**中小企業向けのサイバーセキュリティ対策支援**が実施できる専門家の**得意分野・専門領域を可視化**したリスト（支援対象地域別）
- 現段階の情報を試行公開（PDF）。今後、整備・拡充する予定

※サイバーセキュリティ対策を推進する人材の国家資格。サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言等を行い、セキュリティの確保を支援する。国家資格として厳格な秘密保持義務、信用失墜行為の禁止義務を有する。<https://www.ipa.go.jp/jinzai/riss/index.html>

- ・ 掲載専門家の**支援対象地域別**にリスト化
支援対象地域：北海道、東北、関東、甲信越、東海、近畿、中国、四国、九州、沖縄
- ・ 掲載専門家が支援可能な**指導テーマ**、支援**実績**、得意とする**業界**、支援可能**形態**、支援**料金**、保有**資格**、保有**スキル**等を記載
- ・ 専門家による中小企業指導の支援ツール（5テーマの実施要領）を整備・公表
 - ・ テーマ(1) 情報セキュリティ規程の整備
 - ・ テーマ(2) 情報資産の洗い出しとリスク分析
 - ・ テーマ(3) クラウドサービスの安全利用
 - ・ テーマ(4) セキュリティインシデント対応
 - ・ テーマ(5) 従業員向け情報セキュリティ教育



※ 相談を受けたいセキュリティ専門家がいましたら、利用者ご自身が直接連絡をお取りいただき、相談や業務依頼を行ってください。（リスト掲載の「メールアドレス」をクリックするとメーカーが立ち上がります。）

SECURITY ACTION制度

<https://www.ipa.go.jp/security/security-action/>

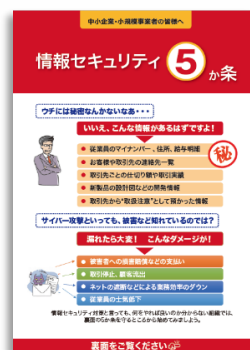


IPA

- 中小企業自らが情報セキュリティ対策に取り組むことを**自己宣言**する制度（※）
「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに**2段階の取組目標**を用意

※IPAが各企業等の情報セキュリティ対策状況等を認定する、あるいは認証等を付与する制度ではありません。

★一つ星



1段階目（一つ星）

● 情報セキュリティ5か条に取り組む

【情報セキュリティ5か条】

- OSやソフトウェアは常に最新の状態にしよう！
- ウイルス対策ソフトを導入しよう！
- パスワードを強化しよう！
- 共有設定を見直そう！
- 脅威や攻撃の手口を知ろう！

宣言者数は約44万件

（2025年9月現在）

◇ SECURITY ACTION制度のメリット

1. 情報セキュリティ対策への取組みの**見える化**

- 👉 ロゴマークをウェブサイトに掲出したり、名刺やパンフレットに印刷することで自らの取組み姿勢をアピール

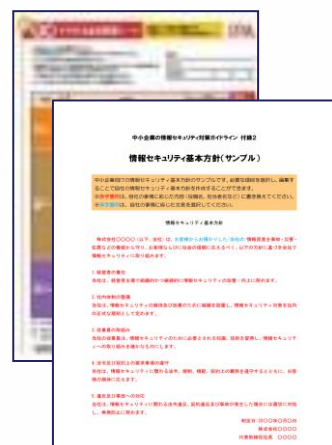
2. 顧客や取引先との**信頼関係**の構築

- 👉 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに

3. **公的補助**・民間の支援を受けやすく

- 👉 SECURITY ACTIONを要件とする補助金の申請、普及賛同企業から提供される様々な支援策が利用可能

★★二つ星



2段階目（二つ星）

● 情報セキュリティ自社診断を実施 ● 基本方針を策定

【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

サイバーセキュリティお助け隊サービス制度

<https://www.ipa.go.jp/security/sme/otasuketai-about.html>



● 中小企業のセキュリティ対策に不可欠なサービスをワンパッケージで安価に提供。

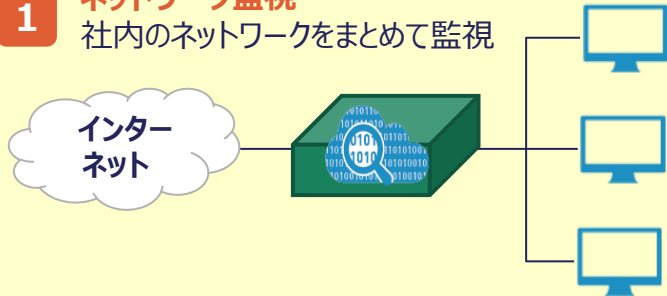


※現行サービスをベースに監視機能の強化や定期的なコンサルティングの実施等の拡充を要件とした新たな類型(2類サービス注)も創設。

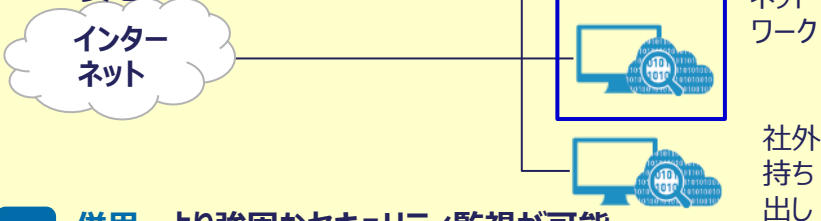
見守り

324時間65日監視をおこない、
不審な挙動やサイバー攻撃を検知
侵入等の異常に素早く気づけます

- 1 ネットワーク監視
社内のネットワークをまとめて監視



- 2 端末監視
端末を社外業務に持ち出しても
安心



- 3 併用～より強固なセキュリティ監視が可能
1 ネットワーク監視と2 端末監視の両方を導入することで、
多層防御による強固なセキュリティ監視が可能に！

駆け付け

異常が発生したときに
地域のIT事業者等が駆け付けます
(リモート支援の場合あり)

保険

簡易サイバー保険が付帯されます
※ 補償内容や限度額等はサービスにより異なりますので、詳細は提供事業者にお問合せください

中小企業でも導入、維持できる価格

- ・ネットワーク監視型：月額1万円以下
- ・端末監視型：月額2,000円以下/台
- ・併用型：これらの合算相当価格以下

注) お助け隊サービスのコンセプトは維持しつつ価格要件を緩和、提供中のお助け隊サービス1類をベースに監視機能の強化や定期的なコンサル実施などの拡充、IPAへの重大サイバー攻撃に関する情報の共有等を要件として基準の改定を実施し、2024年3月15日に公開

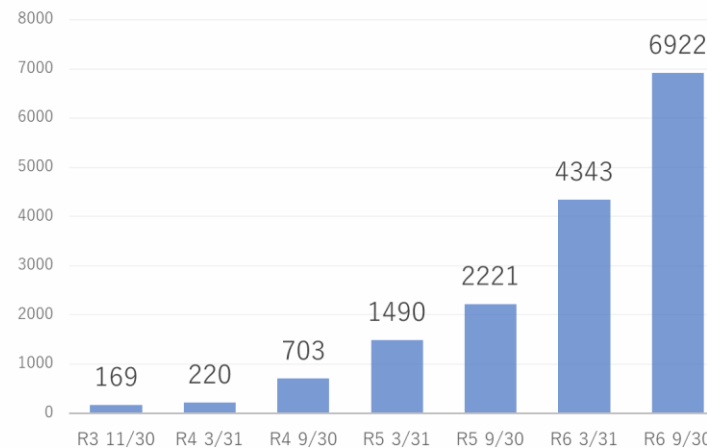
IT導入補助金セキュリティ対策推進枠見直し

見直し部分 赤字	2024	2025
補助上限	5万円～100万円	5万円～ 150万円
補助率	中小企業：1/2	小規模事業者：2/3 中小企業：1/2
対象経費	サイバーセキュリティお助け隊サービス利用料 (最大2年分)	

参考：IT導入補助金2025（中小企業庁）

https://www.chusho.meti.go.jp/koukai/yosan/r7/r6_it.pdf

お助け隊サービス導入企業数



■ 導入数

44事業者が82サービスを登録（2025年12月時点）

IoT製品セキュリティラベリング制度（JC-STAR）

- 2025年3月より、IoT製品に対するセキュリティ要件（適合基準）への適合性を自己適合宣言又は客観的評価に基づき可視化するラベリング制度の運用を開始（★1）。



※★2～★4については、2026年度運用に向けて、現在検討中。

JC-STAR対象製品（例）



インターネットプロトコル
(IP)を使用する通信



ルーター



ネットワークカメラ

インターネットに
接続可能なIoT製品

スマート家電



OA機器



産業用
制御機器

内部ネットワークに接続可能なIoT製品
(IPを使用した通信が可能)

製品カテゴリごとの適合基準

高 ↑ セキュリティ水準 ↓ 低	★4	通信機器	防犯関連機器	スマート家電	第三者 認証
	★4	適合基準 ★4			
	★3	適合基準 ★3	適合基準 ★3		
	★2	適合基準 ★2	適合基準 ★2	適合基準 ★2	
	★1	統一的な最低限の適合基準（★1）			自己適合 宣言

これからは
「JC-STAR 適合ラベル」で
安心を確かめよう



セキュリティ水準達成レベル
(★1～★4)
製品詳細情報へのリンク
登録番号

きちんとセキュリティ対策された製品を選びやすく！
適合ラベルの有効期間内は、セキュリティ対策向上のための更新プログラム
提供などのサポートが約束され、安心して使い続けることができます。

購入者もベンダーも、安全なIoT製品を！

IoT機器を狙ったサイバー攻撃が増加し、多くのIoT機器が乗っ取られて、社会システムを停止させるような被害が現実化している今、IoT製品を使うすべての人・企業・組織は、「被害者」だけでなく、知らないうちに「加害者」になることも！ 利用者や社会全体を守るためには、安全なIoT製品の提供・利用が欠かせないのです。
経済産業省とIPAは、適切なセキュリティ対策を施したIoT製品の普及を目指し、適合ラベルが付与された製品の購入を促進しています。JC-STARのラベル取得は、ベンダー様・販売会社様にとって、IoT製品の購入者から選ばれるための重要な取り組みとなるのです！



映像で知る情報セキュリティ

<https://www.ipa.go.jp/security/videos/list.html>



2023年度制作映像



今、そこにある脅威
～内部不正による情報流出のリスク～

2022年度制作映像



今、そこにある脅威
～組織を狙うランサムウェア攻撃～



華麗なる情報セキュリティ対策
(8話構成)

情報セキュリティに関する様々な脅威と対策を10分程度のドラマなどで分かりやすく解説した映像コンテンツ。
現在、計**34**本をYouTube内の「IPA Channel」で公開中。

社内研修等営利を目的としない用途に限り、主な映像の動画ファイルを無償で提供（ダウンロード）。

[企業・組織向け] 内部不正対策、標的型攻撃、ビジネスメール詐欺、ランサムウェア対策、中小企業向け対策、新人研修など

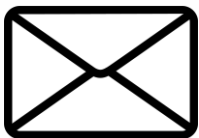
[一般向け] ワンクリック請求、スマホセキュリティ、SNS利用の心得、パスワード、小学生、中高生向けなど

活用実績 (2024/3/1時点)

◆動画ファイルの2023年度申込数 : 申込み**1,254**件 研修での受講予定者数 : 約**61**万名

◆インターネット動画再生回数 : IPA Channelで全作品の累計 約**622**万回

IPAメールニュース&公式アカウント



セキュリティ関連情報、イベント・セミナーの開催情報や情報処理技術者試験に関する情報をメール配信しています。

メールニュースご登録 <https://www.ipa.go.jp/mailnews.html>



IPAの各種情報を配信する公式アカウントです。このほか、各専門分野の最新情報を発信するアカウントもございます。

X公式アカウント <https://twitter.com/IPAjp/>



IPAのイベント情報や情報セキュリティ関連などの最新情報を配信するIPA公式アカウントです。

Facebook公式アカウント <https://www.facebook.com/ipaprpj/>



情報セキュリティやソフトウェア開発関連など、研修や個人学習に最適な映像コンテンツを見ることができます。

YouTube「IPA Channel」 <https://www.youtube.com/user/ipajp/>

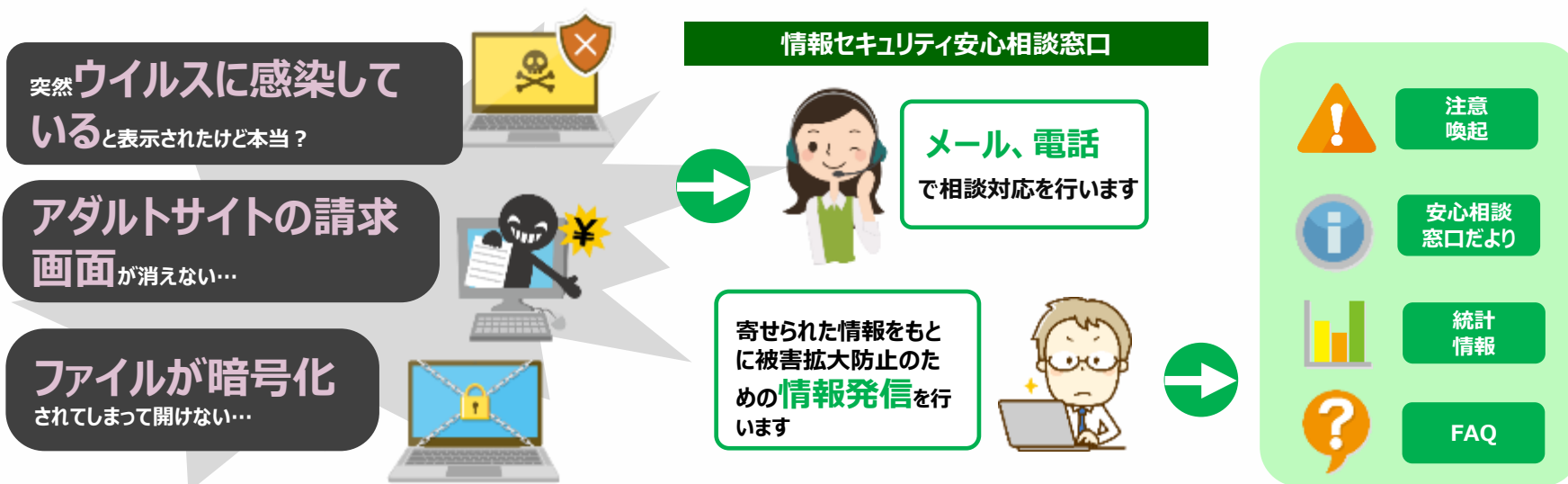


情報セキュリティ安心相談窓口

<https://www.ipa.go.jp/security/anshin/index.html>

IPA

- 一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する**技術的な相談**に対してアドバイスを提供する相談窓口。
- 相談に対して、**事象の分析や助言**を行うほか、相談内容から判明したトラブルの**傾向、手口、対策に関する情報の公開**により、国民のセキュリティリテラシーの向上と対策の促進を実施。



電話

03-5978-7509

平日10:00-12:00、13:30-17:00



メール

anshin@ipa.go.jp



ポータル

IPA安心相談

検索



企業・組織からのインシデント等に関する相談/届出/情報提供窓口のご案内

- ◆ 企業・組織向けに、コンピュータウイルス感染や不正アクセス等の**セキュリティインシデント**に関する**相談や届出、情報提供**を受け付ける窓口を設置
- ◆ セキュリティインシデント等が発生し、お困りの際に活用いただくことが可能。

窓口名	相談・届出の例
情報セキュリティ 安心相談窓口	<ul style="list-style-type: none">ランサムウェアに感染したため、対処方法について相談したい自組織のウェブサイトが改ざんされてしまったため、対処方法と再発防止策について相談したいその他、情報セキュリティに関する一般的な相談やアドバイスが欲しい（相談先の窓口が不明な場合を含む）
標的型サイバー攻撃 特別相談窓口	<ul style="list-style-type: none">標的型サイバー攻撃が疑われる事案が発生したため、相談や情報提供を行いたい
コンピュータウイルス・ 不正アクセス に関する届出窓口	<ul style="list-style-type: none">ランサムウェア感染事象が発生したため、インシデントの内容について公的機関への届出（情報提供）を行いたいサイバー攻撃被害について、サイバー保険の適用を受けるために公的機関への届出を行いたい
脆弱性関連情報の 届出受付	<ul style="list-style-type: none">日本国内で利用されているOS、ブラウザ、メーラ等の脆弱性の届出日本国内からのアクセスが想定されているインターネット上のウェブサイト等で稼動するシステムの脆弱性
脆弱性に関する 問合せ窓口	<ul style="list-style-type: none">ウェブサイトの脆弱性対策、ソフトウェアの脆弱性、また脆弱性に関する公開資料等の質問



■ URL

<https://www.ipa.go.jp/security/todokede/incidentportal.html>

詳細はこちら
のページにて



IPA