



情報セキュリティ6か条

解説編

2026年9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

本解説書の対象者

- 本解説書は、これから情報セキュリティ対策に取り組む個人事業主や中小企業の方を対象としています。

本解説書の使い方

- 情報セキュリティ6か条は、大切な情報や日々の業務を守るために、必ず実施していただきたい基本的な対策です。
- 本解説書を参考に、まずは情報セキュリティ6か条の実践から取り組んでください。
- 一度に全てを実施することが難しい場合でも、できることから着実に進め、情報セキュリティ6か条の実践を目指しましょう。

情報セキュリティ対策は必要？

近年、組織（企業や団体）を狙ったサイバー攻撃が増加しています。攻撃によって顧客情報や技術情報が盗まれたり、コンピュータが使えなくなって業務が停止したりする被害が発生しています。

また、自社だけでなく、取引先や委託先を経由して被害が広がるケースもあります。

サイバー攻撃の被害に遭うと、信用を失ったり、損害賠償を求められたり、事業の継続が困難になったりするおそれがあります。

このようなリスクから組織を守るために、日頃から情報セキュリティ対策に取り組むことが重要です。



情報セキュリティ 6 か条

- 情報セキュリティの脅威は多数ありますが、基本的な対策の重要性は長年変わりません。
- 情報セキュリティ 6 か条を常に意識することが重要です。

分類	No.	情報セキュリティ 6 か条	目的
脆弱性対策	1	OSやソフトウェアは常に最新の状態にしよう！	脆弱性を解消して脆弱性を悪用した攻撃によるリスクを低減する
ウイルス対策	2	ウイルス対策ソフトを導入しよう！	ウイルスによる攻撃を検知してブロックする
パスワード管理	3	パスワードを強化しよう！	パスワード窃取・悪用による情報漏えい等のリスクを低減する
機器の設定	4	共有設定を見直そう！	誤った設定が悪用され、攻撃を受けないようにする
バックアップ	5	バックアップを取ろう！	PCやサーバーのデータ削除や暗号化に備える
情報収集	6	脅威や攻撃の手口を知ろう！	手口から重要視すべき対策を理解する

OSやソフトウェアは常に最新の状態にしよう！

- 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る。
- 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。

<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)など、OSベンダの提供する修正プログラムを適用する。
- Adobe Readerやブラウザなど利用中のソフトウェアを最新版にする。
- サポートのあるOS、ソフトウェア、ネットワーク機器を利用する。



(ご参考) Windows Update: よくあるご質問 (マイクロソフト)
<https://support.microsoft.com/ja-jp/windows/deployment/updates-lifecycle/windows-update-faq>

<参考> MyJVNバージョンチェッカ

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

- PCにインストールされているソフトウェア製品のバージョンが最新であることを簡単な操作で確認する無償ツール

実行ボタンを押すだけ！



MyJVNバージョンチェッカ for .NET (v1.0)

実行 終了 全てを選択 選択をクリア 結果出力

「選択」されたソフトウェア製品を「実行」ボタンを押下後ツール下部の内容を参考にしてください。
(<http://jvndb.jvn.jp/apis/myjvn/>)

クリックするとチェック結果の表示順を切り替えることができます。

チェック結果 ▲(X/O一瞬)

ソフトウェア製品名 ▲	チェック結果 ▲(X/O一瞬)	結果詳細 ▲
☒ Adobe Flash Player (ActiveX)	× 最新のバージョンではありません	表示
☒ JRE	× 最新のバージョンではありません	表示
☒ VMware Player	× 最新のバージョンではありません	表示
☒ Adobe Reader	○ 最新のバージョンです	表示
☒ Lhaplus	○ 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	
☒ Lunascape	— 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	

チェック結果

詳細情報

JRE バージョン情報詳細
あなたのPCに現在インストールされているアプリケーションの判定結果は以下の通りです

判定	【インストールバージョン】	【最新バージョン】
×	1.6.0.37	※1.7.x以降を最新バージョンとして判定しています。1.6.xは不要であればアンインストールをしてください。
×	1.7.0.09	1.7.0.71/72 (2014/10/15時点)

バージョンアップ方法は下記のURLを参照ください。
<http://jvndb.jvn.jp/apis/myjvn/vschecklist.html#spid255>

ウイルス対策ソフトを導入しよう！

- 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するウイルスが増えている。
- 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する。

<対策例>

- ・パソコン等の情報機器にウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にする。
- ・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。
- ・ファイアウォールや脆弱性対策など複数の機能を搭載した統合型のセキュリティ対策ソフトを導入する。



<参考>ウイルスの感染経路を理解する

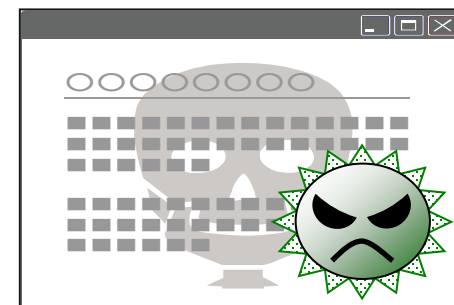
●メールからのウイルス感染

- メールの特付ファイルを開いて感染
- メール本文中のURLへアクセスして感染



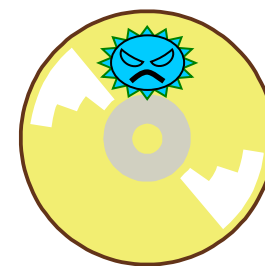
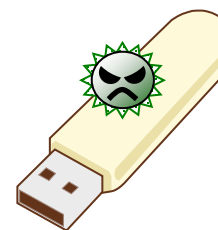
●ウェブサイトからのウイルス感染

- ウイルスが仕掛けられたウェブサイトを開覧して感染
- ウェブサイトからダウンロードしたファイルを開いて感染



●外部記憶媒体からのウイルス感染

- 出所不明のUSBメモリを接続して感染
- 納品物のCD-ROMを読み込んで感染

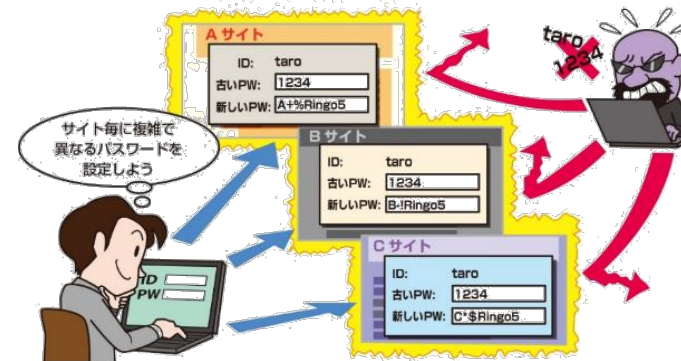


パスワードを強化しよう！

- 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えている。
- パスワードは「長く」「複雑に」「使い回さない」ようにして強化する。

<対策例>

- ・パスワードは英数字記号含めて10文字以上にする。
- ・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。
- ・可能な場合は多段階認証、多要素認証、パスキーなどの認証強化機能を利用する。
- ・初期設定パスワードを見直す。



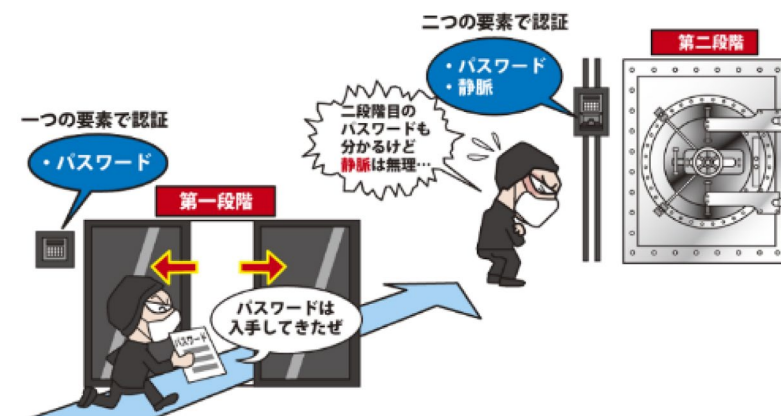
<参考>多要素認証、パスキーを利用しよう

●多要素認証とは

「知っているもの」「持っているもの」「本人に関するもの」のうち、2つ以上を組み合わせることを多要素認証といいます。

例えば、「知っているもの」とはパスワードやPINコード等の”覚えている情報”、「持っているもの」はキャッシュカードやOTP（ワンタイムパスワード）トークン等の”所持しているもの”、「本人に関するもの」とは静脈や指紋、顔の情報等の”身体的特徴等”を指します。

なお、SMSで送信されるワンタイムパスワードを窃取しようとするフィッシングの手口も確認されていますので、不審なメールやWebサイトに騙されないよう十分に注意して操作することが重要です。



●パスキーとは

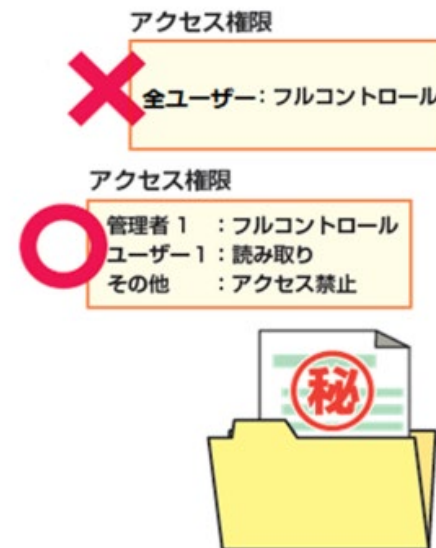
パスキーは、利用者が所持するスマートフォンやパソコンと、指紋認証・顔認証・PINコードなどを組み合わせて本人確認を行う仕組みです。パスワードやSMSで送信される認証コードを入力しないため、フィッシングによる認証情報の窃取に強い認証方式です。

共有設定を見直そう！

- 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増えている。
- 無関係な人に情報が見られない、利用されない設定になっていることを確認する。

<対策例>

- ・ウェブサービスや、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は速やかに設定を変更(削除)する。
- ・使用するパソコン等は他者と共有しない。共有せざるを得ない場合は、別途ユーザーアカウントを作成する。



<参考>クラウドサービスの設定ミス

●クラウドサービスからの情報流出

出典) NCO「インターネットの安全・安心ハンドブック」

クラウドの設定に関する権限や設定のミスを突いて、外部からの攻撃を受けることになってしまい、情報漏えいが生じる事例などがあります。

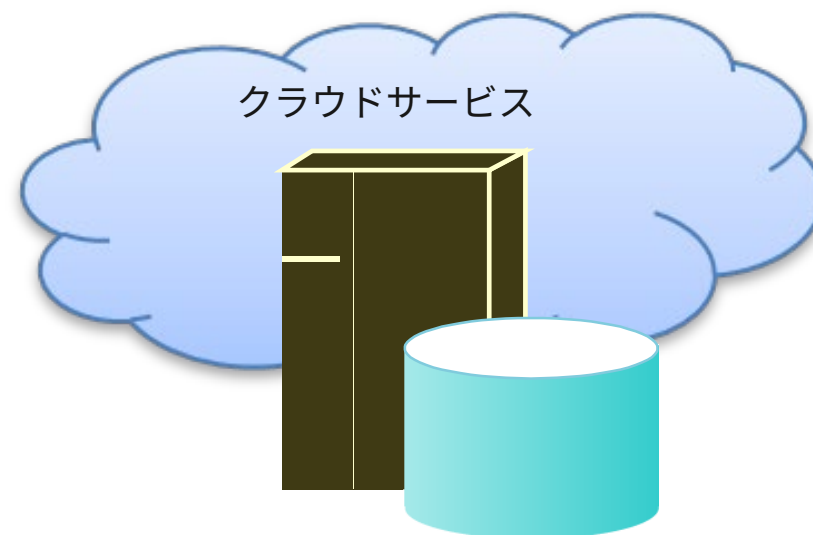
クラウドサービスの中には、例えば情報の非公開の決定や他のサービス連携の選択を行うための管理権限を、利用者に与えていないものもあります。この場合には、予期しない形で情報の漏えいが生じる危険性を伴うため、サービス利用前に十分確認しましょう。

<役立つ情報>

総務省「クラウドの設定ミス対策ガイドブック」

情報の流出のおそれに至る事案の発生を防止する観点から、クラウド設定について分かりやすく解説している。

https://www.soumu.go.jp/main_content/000944467.pdf



バックアップを取ろう！

- 故障や誤操作、ウイルス感染などにより、パソコンやサーバーの中に保存したデータが消えたり、暗号化されたりしてしまうことがある
- 事業が継続できるようバックアップを取得しておくようにする

＜対策例＞

- ・ 重要情報のバックアップを定期的に行う。
- ・ バックアップに使用する装置・媒体は、バックアップ時のみパソコンと接続する。
- ・ バックアップの取得方法を決める。
（オンラインバックアップの活用等）
- ・ バックアップしたデータを安全な場所に保管する。
- ・ バックアップしたデータを戻せるか定期的に確認する。

<参考>バックアップを取る

●3-2-1ルール

データのコピーは本体を含め3つ以上持ち、それらは2種類のメディアでバックアップを保管し、そのうち1つは稼働システムとは異なる拠点等で保存する。

<例> パソコン本体+バックアップ用記憶装置+クラウドサーバー

●Windowsのバックアップ

Windowsには3つの標準バックアップ機能がありますので、利用目的に応じて使い分けましょう。

① Windowsバックアップ

- 利用者のデータや設定をクラウド（OneDrive）に保存する機能
- OneDrive容量に依存

② ファイル履歴

- 重要ファイルを定期的にバックアップする機能
- パソコン故障時はWindowsの再インストールが必要

③ システムイメージ

- パソコン全体を丸ごと保存する機能
- ハードディスク故障時の復旧に有効
- ランサムウェア対策にも有効

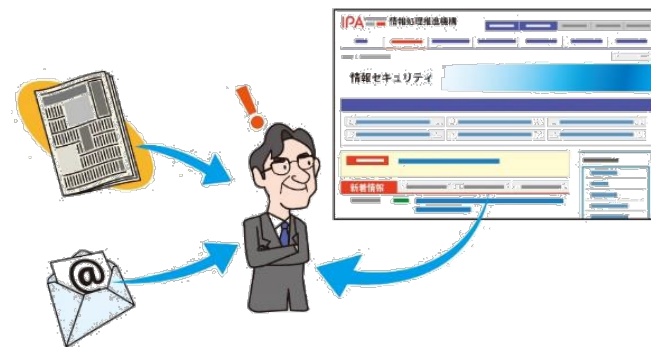


脅威や攻撃の手口を知ろう！

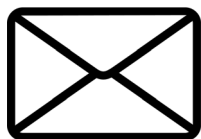
- 取引先や関係者と偽ってウイルス付きのメールを送ってきたり、正規のウェブサイト に似せた偽サイトを立ち上げたりしてID・パスワードを盗もうとする巧妙な手口が増えている。
- 脅威や攻撃の手口を知って対策を取るようになる。

<対策例>

- ・IPAセキュリティセンターやNCO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ウェブサイトなどが提供する注意喚起を確認する。
- ・管理者が従業員に適宜注意喚起し、従業員はセキュリティの懸念は速やかに報告する。



<参考>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/about/mail/>



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://x.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/ipaprijp/>



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/>

インシデントが発生する前提での対策を

重要!!

- 情報セキュリティ6か条で示した対策は、組織の規模に関わらず、必ず実行すべき基本的な対策です。また、情報漏えいやウイルス感染などのインシデント（情報セキュリティ上の事故や被害）は、どれか一つの対策だけで防げるものではありません。
- 例えば、ウイルス対策ソフトはウイルス感染防止の対策の一つですが、新種のウイルスを検知できない場合もあります。また、ウイルスによってファイルやシステム環境が破壊されると、ウイルス対策ソフトだけでは元に戻すことはできません。そのため、バックアップによる復旧対策も必要となります。
- このように、ウイルス感染や不正ログインを「防ぐ」対策だけでなく、操作ミスやウイルス感染が発生してしまった場合に「復旧する」対策も重要です。インシデントの発生を前提として、複数の対策を組み合わせるを実施しましょう。

【ご参考】IPAが提供する ツール、制度等

中小企業の情報セキュリティ対策ガイドライン第4.0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などを示したガイドラインです。

●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」などの**ひな形**を付録



SECURITY ACTION

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

●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段階の取り組み目標を用意



1段階目（一つ星）

「情報セキュリティ6か条」に取り組むことを宣言



2段階目（二つ星）

「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティ基本方針を定め、外部に公開したことを宣言



●「★一つ星」を宣言しよう！

「★一つ星」は、これから「情報セキュリティ6か条」に取り組むことを宣言するものであり、対策実施前でもお申込みいただけます。

サイバーセキュリティ相談窓口

- ◆ IPAでは企業組織向けに、セキュリティに関する総合的な相談窓口を設けています。
- ◆ セキュリティインシデント等が発生した際などにご活用ください。



受付可能な相談内容	
各種インシデント発生時の 初動対応に関する相談	• 起きている事象をヒアリングして、被害が発生しているか否かを判断します • 被害が発生している場合、有効な応急処置についてご案内します • インシデント対応を行う専門業者一覧の紹介をします • 他に必要な相談・報告先等の紹介をします
標的型サイバー攻撃に関する インシデント相談	• 国家支援型と推定される標的型サイバー攻撃（APT）を受けた場合は、専門的知見をもとに支援を実施します
その他の情報セキュリティに関する 一般的な相談	• 中小企業などにおける、情報セキュリティ対策ガイドラインや各種支援ツール・支援施策などをご案内します
脅威情報に関する 情報提供	• IPAによる被害拡大防止策の実施や注意喚起のために、標的型サイバー攻撃や、その他の脅威情報に関して情報提供を受付けています。



メール

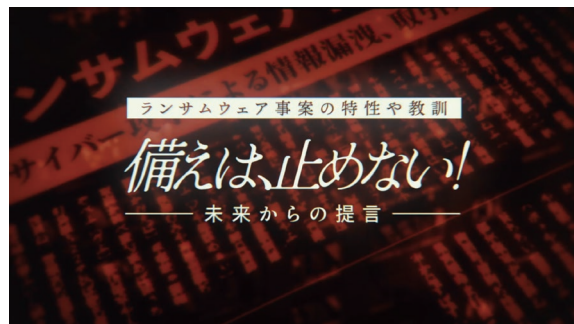
cs-support@ipa.go.jp

ウェブサイト

<https://www.ipa.go.jp/security/support/soudan.html>

映像で知る情報セキュリティ

2026年度制作映像



ランサムウェア事案の特性や教訓
「備えは、止めない！～未来からの提言～」



今、そこにある脅威
～内部不正による情報流出のリスク～



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)

👉 YouTube内のIPA Channelで公開中
主要な映像は動画ファイルでも配布

[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
[共通・一般向け] ワンクリック請求、偽警告、不正ログイン、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

IPA Channel



動画ファイル申込



研修・教育に最適！
社内研修やeラーニング教材としてご利用いただけます。

ITパスポート試験

ITパスポート試験

国家試験

令和の時代の
『あたりまえ』

累計受験者数
100万人
突破!

IPA
ITパス公式キャラクター
上峰 亜衣 (うえみね あい)
Profile▶社会人2年目、23歳。
大手企業の経営企画部門に所属。
業務に必要なITと経営に関する基礎知識を
得るため、ITパスに挑戦。2回目合格(75点)。
ITパスで得た幅広い知識を活かして、日々、奮闘中。

ITパスポート公式キャラクター

上峰亜衣(うえみねあい)

「iパス」は、ITを利活用する**すべての社会人・これから社会人になる学生**が備えておくべき
ITに関する基礎的な知識が証明できる国家試験です。

試験勉強を通じ、幅広い分野の基礎知識が取得可能！

- 情報セキュリティや情報モラルに関する知識が身に付きます。
- 企業コンプライアンス・法令遵守に貢献する正しい知識が身に付きます。
- 経営戦略、財務など、経営全般に関する基礎知識が身に付きます。
- 業務に必要なITの基礎知識が身に付きます。

独立行政法人情報処理推進機構 セキュリティセンター

電子メール isec-pr-cssp@ipa.go.jp

URL <https://www.ipa.go.jp/security/>