



5分でできる!情報セキュリティ自社診断

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

- 本解説書は情報セキュリティに関する基本的なセキュリティ対策を組織的に取り組もうと考えている企業・組織の責任者、担当者の方を対象と想定しています。

本解説書の使い方

- 「5分でできる!情報セキュリティ自社診断」は、自社の弱みを把握し基本的対策を決定します。
- 本解説書では、対策が必要な理由、対策をしないと何が起きるか、対策の具体例、について解説します。
- 本解説書を参考に、「5分でできる!情報セキュリティ自社診断」を実施し、現状の対策状況を客観的に可視化し、「今すぐ改善すべき点」や「優先順位の高い対策」を導き出しましょう。

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。



**情報セキュリティ対策が行われていない企業とは
お付き合いしたくない!?
仕事も出せない!?**



情報セキュリティ対策はビジネス上必須です!!

基本的なセキュリティ対策を組織的に取り組むために 5分でできる!情報セキュリティ自社診断を活用してください

5分でできる!情報セキュリティ自社診断

25項目の設問に答えるだけで

自社の情報セキュリティの問題点を簡単に把握できます

Part1:基本的対策

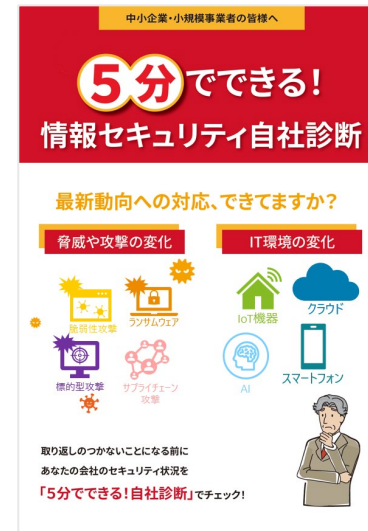
6項目

Part2:従業員としての対策

11項目

Part3:組織としての対策

8項目



No	診断内容
Part 1 基本的対策	1 パソコンやスマートフォンなど情報機器の OS やソフトウェアは常に最新の状態にしていますか？
	2 パソコンやスマートフォン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 データの共有設定を必要の人に限定していますか？
	5 故障や誤操作、ウイルス感染などによる重要情報 ^{※2} の消失に備えて定期的にバックアップを取得していますか？
	6 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？
Part 2 従業員としての対策	7 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？
	8 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？
	9 重要情報の受け渡しは、暗号化など安全な手段で行っていますか？
	10 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？
	11 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？
	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 重要情報が記載された書類や重要なデータが保存された媒体を破壊する時は、復元できないようにしていますか？
	15 離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？
	16 関係者以外の事務所への立ち入りを制限していますか？
Part 3 組織としての対策	17 退社時にノートパソコンや備品を施設保管するなど盗難防止対策をしていますか？
	18 内部ネットワークを守るため、不正アクセス対策機能を設定していますか？
	19 ウェブサイトで公開すべきでない情報を公開していませんか？
	20 従業員に情報セキュリティに関する教育や注意喚起を行っていますか？
	21 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？
	22 重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23 クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握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？

Part1:基本的対策



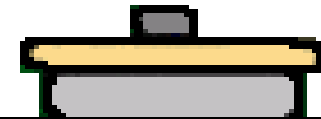
- 脆弱性対策
- ウイルス対策
- パスワード管理
- 機器の設定
- バックアップ
- 情報収集

Part1:基本的対策

- No.1 OSやソフトウェアは常に最新の状態にする
- No.2 ウイルス対策ソフトを導入し適切に利用する
- No.3 強固なパスワードを使用する
- No.4 共有設定を見直す
- No.5 定期的にバックアップを取る
- No.6 脅威や攻撃の手口を知り、対策に活かす

No.1 OSやソフトウェアは常に最新の状態にする

 パソコンやスマートフォンなど
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？



No.1 OSやソフトウェアは常に最新の状態にする

● 対策が必要な理由

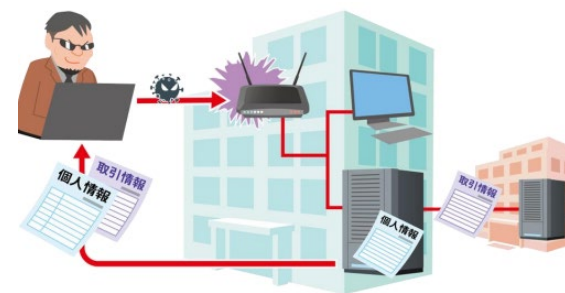
- OSやソフトウェアには脆弱性(※)が発見される場合がある
- 最新のOSやソフトウェアは、既知の脆弱性が解消されている

● 対策をしないと何が起きるか

- 攻撃者に脆弱性が悪用されて
 - パソコンやサーバーに不正アクセスされる
 - ウイルスに感染する

(※)脆弱性（ぜいじゃくせい）

セキュリティ上の脅威となりうるシステムやアプリケーション（ソフトウェア）の欠陥、あるいは設計上の問題点のこと。“セキュリティホール”とも呼ばれている。



OSやソフトウェアを危険な状態から守るため常に最新の状態にしましょう！

● 具体的な対策

■OSやソフトウェアは最新版を利用する

- ✓ WindowsUpdate (WindowsOSの場合)、ソフトウェア・アップデート (macOSの場合) などベンダの提供するサービスを実行する
- ✓ Adobe Reader、ブラウザなど利用中のソフトウェアを最新版にする
- ✓ 利用中のソフトウェアに脆弱性が存在しないか、MyJVNバージョンチェッカ (次頁参照) で確認する
- ✓ 脆弱性が存在した場合は手順に沿って修正パッチを適用する
- ✓ サポートが有効なOS、ソフトウェア、ネットワーク機器を利用する

■オフィスで使用するPCだけでなくテレワークで使用するPCなどのソフトウェアやルーターなどのファームウェアも最新版を利用する

最新の状態に更新しました!!



<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

ソフトウェア製品名 ▲	チェック結果 ▲(×○一冊)	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	

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)

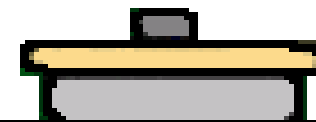
バージョンアップ方法は下記のURLを参照ください。
<http://jvndb.jvn.jp/apis/myjvn/vschecklist.html#spid255>

No.2 ウイルス対策ソフトを導入し適切に利用する

 パソコンやスマートフォンなどには
ウイルス対策ソフトを導入し、
ウイルス定義ファイル^(※)は
最新の状態にしていますか？

(※)ウイルス定義ファイル

コンピュータウイルスを検出するためのデータベースファイル。
「パターンファイル」とも呼ばれます。



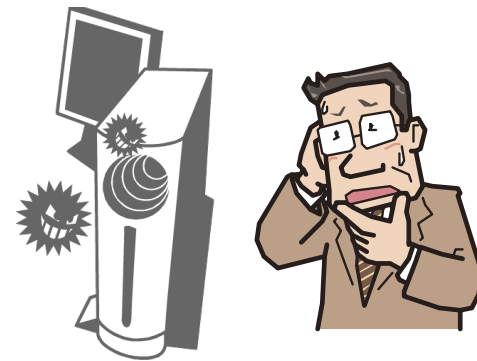
No.2 ウイルス対策ソフトを導入し適切に利用する

● 対策が必要な理由

- パソコンやサーバーはインターネットに接続した時点で攻撃者からの攻撃の対象となるおそれがある
- 攻撃は日々増えているため利用者の注意で防ぐことは難しい

● 対策をしないと何が起きるか

- ウイルス感染の危険性が高まる
- PCがウイルスに感染すると
 - PCが正常に動かなくなる（フリーズ、データ破壊など）
 - 情報が勝手に社外へ送られる
 - 情報が消えたり、暗号化されて開けなくなる
 - 社内の他のPCへ感染が広がり被害が拡大する



ウイルス感染防止のためウイルス対策ソフトを導入しましょう！

● 具体的な対策

■ ウイルス対策ソフトの導入と設定する

- ✓ ウイルス対策ソフトや統合型セキュリティ対策ソフト(※1)を導入する
- ✓ OSのセキュリティ機能(※2) を有効化する
- ✓ ウイルス対策ソフトは水際でウイルスを発見するので感染を予防できる自動保護（リアルタイム保護）設定を推奨
- ✓ 「発見したらすぐ駆除する」設定を推奨



■ ウイルス定義ファイルは常に最新の状態とする

- ✓ ウイルスの手配書であるパターンファイル（ウイルス定義ファイル）は自動更新設定にして常に最新の状態にすることを推奨



(※1) ウイルス対策、ファイアウォール、パスワード管理など多様な脅威を防ぐ機能を1つにまとめたソフトウェア

(※2) Windowsのセキュリティ機能Windows Defenderの有効化、macOSのセキュリティ機能XProtectなど

<参考>ウイルスの感染経路を理解する(1/2)

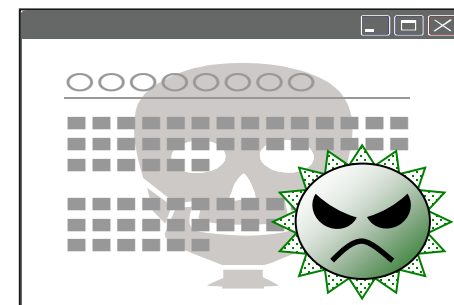
●メールからのウイルス感染

- メール添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



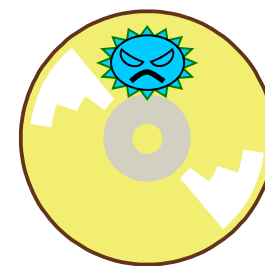
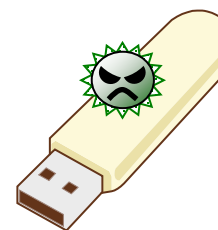
●ウェブサイトからのウイルス感染

- ウイルスが仕掛けられたウェブサイトを閲覧して感染
- 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



<参考>ウイルスの感染経路を理解する(2/2)

●メールからのウイルス感染の対策例

- ・メーラーのセキュリティ設定を強化する（例えば外部コンテンツブロック設定など）
- ・メール本文はテキスト形式にする（HTML形式は見栄えは良いが不正な仕掛けが施せる）
- ・スパムメールのフィルタリング

●ウェブサイトからのウイルス感染の対策例

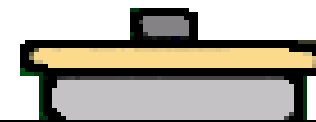
- ・ブラウザのセキュリティ設定を強化する
（例えば必要時以外のスクリプトの抑止、不要なアドオンの抑止など）
- ・ウェブサイトフィルタリングの利用

●外部記憶媒体からのウイルス感染の対策例

- ・私物を含む業務以外で使用するUSBメモリの利用禁止（用途外利用の禁止）
- ・USBメモリの私的な貸し借り禁止
- ・出所が不明なUSBメモリは開かない
- ・納品物はウイルスチェックをしてから開く

No.3 強固なパスワードを使用する

 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？



No.3 強固なパスワードを使用する

● 対策が必要な理由

- 単純なパスワードは推測や解析されやすく、総当たり攻撃などによって容易に突破されるおそれがある

● 対策をしないと何が起きるか

- パスワードを推測されアカウントに不正にログインされる（なりすまし）
- 不正にログインされると
 - 社内システムアクセスされ重要な情報や個人情報が窃取される
 - メールを勝手に送付される
 - SNSに勝手に投稿される
 - 勝手に買い物をされる
 - 口座から不正送金される



パスワードが推測されないようパスワードを強化しましょう！

● 具体的な対策

■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

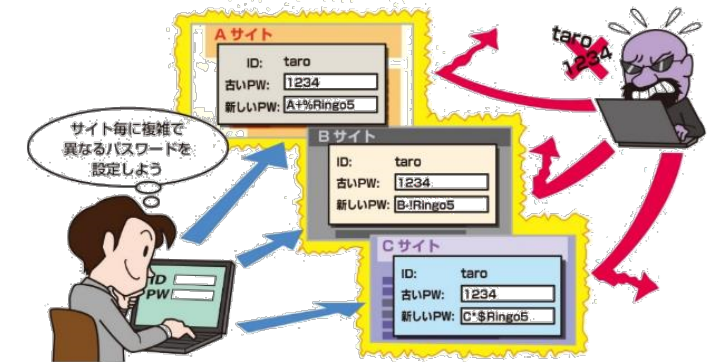
- ✓ 推測されやすいパスワード（名前や誕生日など）は使わない
- ✓ 推測しづらく自分が忘れないパスワードにする
- ✓ 長いパスワードにする
- ✓ 大文字・小文字・数字・記号を組み合わせる
- ✓ 同じIDやパスワードを複数のPCやシステムで使いまわさない

■パスワードは必要に応じて変更する

- ✓ 初期パスワードは必ず変更する
- ✓ 担当者変更のタイミングなどで変更する

■他人の目に触れる場所にパスワードを残さないようにする

■可能な場合は、多要素認証^(※1)やパスキー^(※2)などを用いて強化する



(※1) 3つの要素（知っているもの、持っているもの、本人自身に関する）のうち、2つ以上の要素を用いて利用者認証を行うもの。

(※2) サービス側の「公開鍵」と、自分の端末内の「秘密鍵」をペアで照合して利用者認証を行うもの。

<参考>使い回さないパスワード作成の例

コアパスワードとサービスごと固有の文字列を作り、組み合わせる

～コアパスワードの作り方～

1. **短いフレーズ**を作る

テレビが好き

2. **ローマ字**にする

terebigasuki

3. 一部を**大文字**にする

terebi**G**Asuki

4. **記号**を追加する

terebiGAsuki**!!**

5. **数字**を追加する

terebiGAsuki**!!06**

完成した**コアパスワード**に
サービス固有の文字列を
追加してパスワードを作る

・いろは銀行の場合

IrhterebiGAsuki!!06

・IPAサービスの場合

IPAterebiGAsuki!!06

詳しくは**コチラ**を**Check!!**「安心相談窓口だより 不正ログイン被害の原因となるパスワードの使い回しはNG」

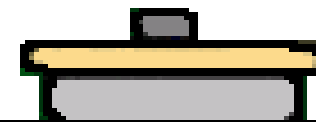
<https://www.ipa.go.jp/security/anshin/mgdayori20160803.html>

No.4 共有設定を見直す

 **重要情報^(※)に対する適切なアクセス制限を行っていますか？**

(※)重要情報

営業秘密など事業に必要で組織にとって価値のある情報や顧客や従業員の個人情報など管理責任を伴う情報のことです。
本解説書では重要な方法について前後の文脈に合わせて
「重要情報」「重要な情報」「情報」と表記します。



No.4 共有設定を見直す

● 対策が必要な理由

- 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などの共有設定が許可した人のみに限定されていないと、本来アクセスを許可していない利用者からも重要な情報を見たり使ったりできるおそれがある

● 対策をしないと何が起きるか

- 重要な情報が無関係な人に覗き見られる
- 重要な情報が第三者に窃取され悪用される
- システムを勝手に操作される



無関係な人に情報を見られないよう共有設定を見直しましょう！

● 具体的な対策

■無関係な人がサービスや機器を使うことができない設定にする

- ✓ ウェブサービス、ネットワーク接続の複合機・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
- ✓ 使用するパソコンは他者と共有しない
- ✓ 共有せざるを得ない場合は、別のアカウントを作成する
- ✓ 外出先でフリーWi-Fiを使うときにはパソコンのファイル共有をオフにする
- ✓ クラウドサービスやネットワーク接続機器は必要な人にのみ共有されるよう設定する



No.5 定期的にバックアップを取る

 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？



No.5 定期的にバックアップをとる取る

● 対策が必要な理由

- ・ パソコンやサーバーの中に保管している情報は、故障や誤操作で消えたり、ウイルス感染で暗号化されてしまうおそれがある

● 対策をしないと何が起きるか

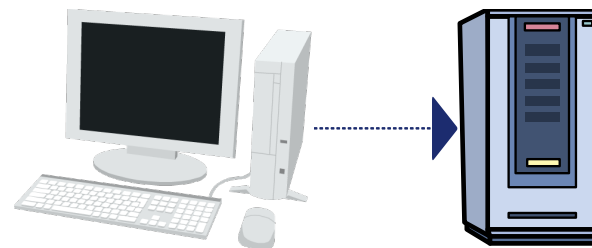
- ・ 情報が参照ができなくなり業務が滞る（業務が停止する可能性もあり）
- ・ 情報が消失して二度と復元できなくなる
- ・ 情報の復元に時間がかかる（＝コストがかかる）

事業を止めないため重要な情報を定期的にバックアップしましょう！

● 具体的な対策例

■ 重要情報のバックアップを定期的に行う

- ✓ バックアップの対象とする情報を決める（対象とする情報は定期的に見直す）
- ✓ 取得方法、取得間隔、世代管理、保管期間を決める
- ✓ バックアップした情報を安全な場所に保管する



■ バックアップした情報を戻せるか定期的を確認する

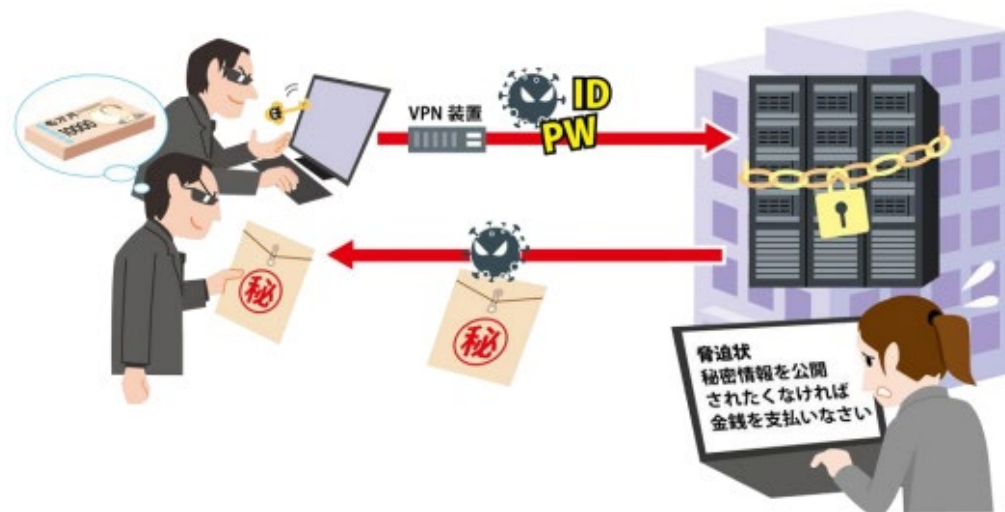
- ✓ バックアップした情報を用いて復元するための手順書を準備する
- ✓ 手順書を用いて復元できることを確認する

■ バックアップした情報を保護する（次頁参照）

- ✓ 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
- ✓ バックアップした情報はネットワークから切り離して保管する

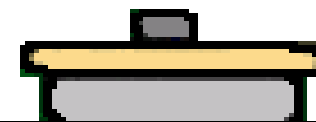
<参考>ランサムウェアとは

- 「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語です。
- 感染したパソコンに特定の制限（暗号化）をかけ、その制限の解除と引き換えに金銭を要求する挙動から、このような不正プログラムをランサムウェアと呼んでいます。
- バックアップした情報はネットワークから切り離して保管するなど保護しないと、ランサムウェアによって暗号化されるおそれがあります。



No.6 脅威や攻撃の手口を知り対策に活かす

 **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？**



No.6 脅威や攻撃の手口を知り対策に活かす

● 対策が必要な理由

- 脅威や攻撃の手口は日々進化しているため、それらを把握していないと被害を防ぐことが難しい

● 対策をしないと何が起きるか

- 脅威や攻撃の手口を知らないと、攻撃者の仕掛けた罠に気づけず
 - フィッシングにより偽サイトに誘導される
 - 上司や取引先になりすましたメールに騙される
 - ウイルス感染によりファイルが暗号化されたり情報が窃取される

脅威や攻撃の手口を知り対策に活かしましょう！

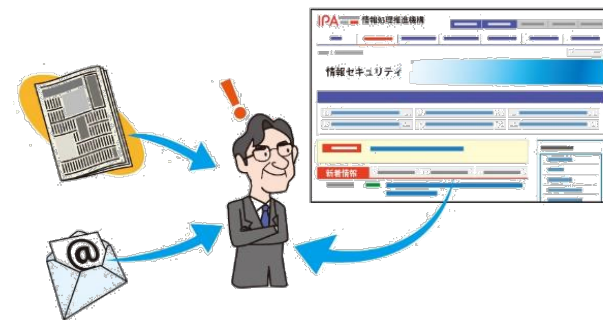
● 具体的な対策例

■最新の脅威や攻撃に関する情報を収集する

- ✓ IPA^(*1)、NCO^(*2)、JPCERT/CC^(*3)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ービス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する

■従業員はセキュリティの懸念を感じたら速やかに報告する

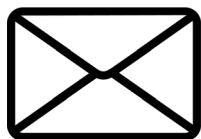


(*1) IPA 独立行政法人情報処理推進機構 <https://www.ipa.go.jp/security/guide/keihatsu.html>

(*2) NCO | みんなで使おうサイバーセキュリティ・ポータルサイト <https://security-portal.cyber.go.jp/>

(*3) JPCERT コーディネーションセンター <https://www.jpccert.or.jp/>

<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/>

Part2:従業員としての対策



- 電子メール
- 無線LAN
- インターネット
- 情報管理
- 事務所の安全管理

Part2:従業員としての対策

- No.7 身に覚えのない電子メールは疑ってみる
- No.8 宛先の送信ミスを防ぐ
- No.9 重要情報を送信する時は保護する
- No.10 無線LANの盗聴や無断使用を防ぐ
- No.11 インターネットを介したトラブルを防ぐ
- No.12 重要情報の放置を禁止する
- No.13 重要情報は安全な方法で持ち出す
- No.14 重要情報は復元できないように消去する
- No.15 機器を勝手に操作させない
- No.16 見知らぬ人には声をかける
- No.17 機器・備品の盗難防止対策を行う

No.7 身に覚えのない電子メールは疑ってみる

 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？



No.7 身に覚えのない電子メールは疑ってみる

● 対策が必要な理由

- 電子メールはサイバー攻撃の入り口になりやすい
- 取引先や上司を装ったメールに騙されるおそれがある（見た目だけで安全が判断しにくい）
- 電子メールの添付ファイルや本文中のURLリンクは攻撃手段として利用されるおそれがある

● 対策をしないと何が起きるか

- ウイルスが添付されたメールを開封してウイルスに感染する
- メールに記載されているURLリンクをクリックして偽のWebサイトに誘導されて
 - 重要な情報を入力させ窃取される
 - 入会金や登録料などの名目料金の支払いを求められる

「まずは疑う」ことでウイルス感染や情報漏えいを防ぎましょう！

● 具体的な対策例

■ 不審な電子メールを安易に開かない

- ✓ メールの送信元を確認してから開く
- ✓ メールに記載されているURLリンクを安易にクリックしない

■ メールソフトに迷惑メール対策機能がある場合は有効にする

■ 不審なメールを受信したら社内に共有する

- ✓ 不審なメールのタイトルや送信元を情報セキュリティ管理者などに連絡し周知、注意喚起する
- ✓ 不審なメールを開いてしまった場合、情報セキュリティ管理者などに連絡し対処する（放置しない）



No.8 宛先の送信ミスを防ぐ

 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？



No.8 宛先の送信ミスを防ぐ

● 対策が必要な理由

- 電子メールやFAXは人が送信するため宛先を間違える「うっかりミス」が発生するおそれがある
- 電子メールやFAXは一度送付すると取り消しが難しい

● 対策をしないと何が起きるか

- 電子メールやFAXの宛先を間違えると本来送付すべき相手に届かず業務に影響が発生する
- 電子メールの宛先を間違えるとメールアドレスと内容が漏洩する
- 一度送付すると完全に回収できないため、情報が拡散されるおそれがある

宛先の送信ミス防ぐことで情報漏洩や拡散を防ぎましょう！

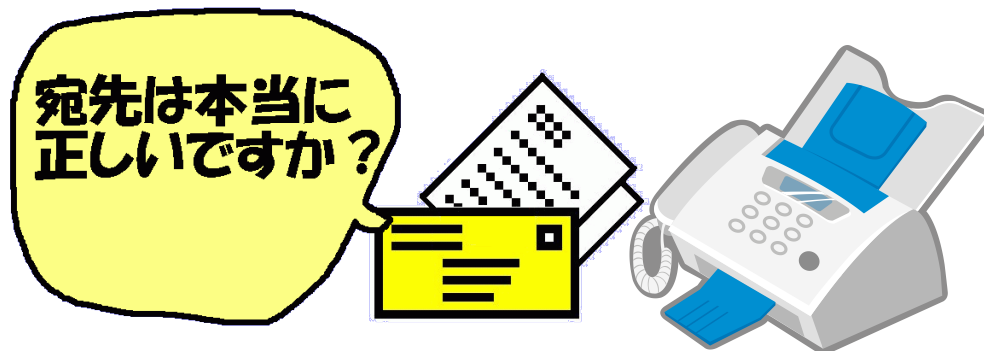
● 具体的な対策例

■ 電子メールやFAXの誤送信防止の対策を行う

- ✓ 電子メールの宛先（TO/CC/BCC）を確認する
- ✓ 電子メールの送信前に本文・添付ファイル・宛先を最終確認する
- ✓ メールソフトに宛先チェック、送信保留、取り消しなど誤送信防止機能がある場合は有効にする

■ 送信先を間違えたことに気が付いたら報告する

- ✓ 送信先を間違えてしまった場合、情報セキュリティ管理者などに連絡し対応を相談する（放置しない）



No.9 重要情報を送信する時は保護する

 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？



No.9 重要情報を送信する時は保護する

● 対策が必要な理由

- 電子メールは完全に安全な通信手段ではないため、インターネットを経由している途中で関係のない人に見られるおそれがある

● 対策をしないと何が起こるか

- 電子メールで重要な情報を保護せずに送付すると、通信経路が盗聴されていた場合に情報が漏洩したり・改ざんされたりする

電子メールで送付する重要情報を保護して情報漏洩を防ぎましょう！

● 具体的な対策例

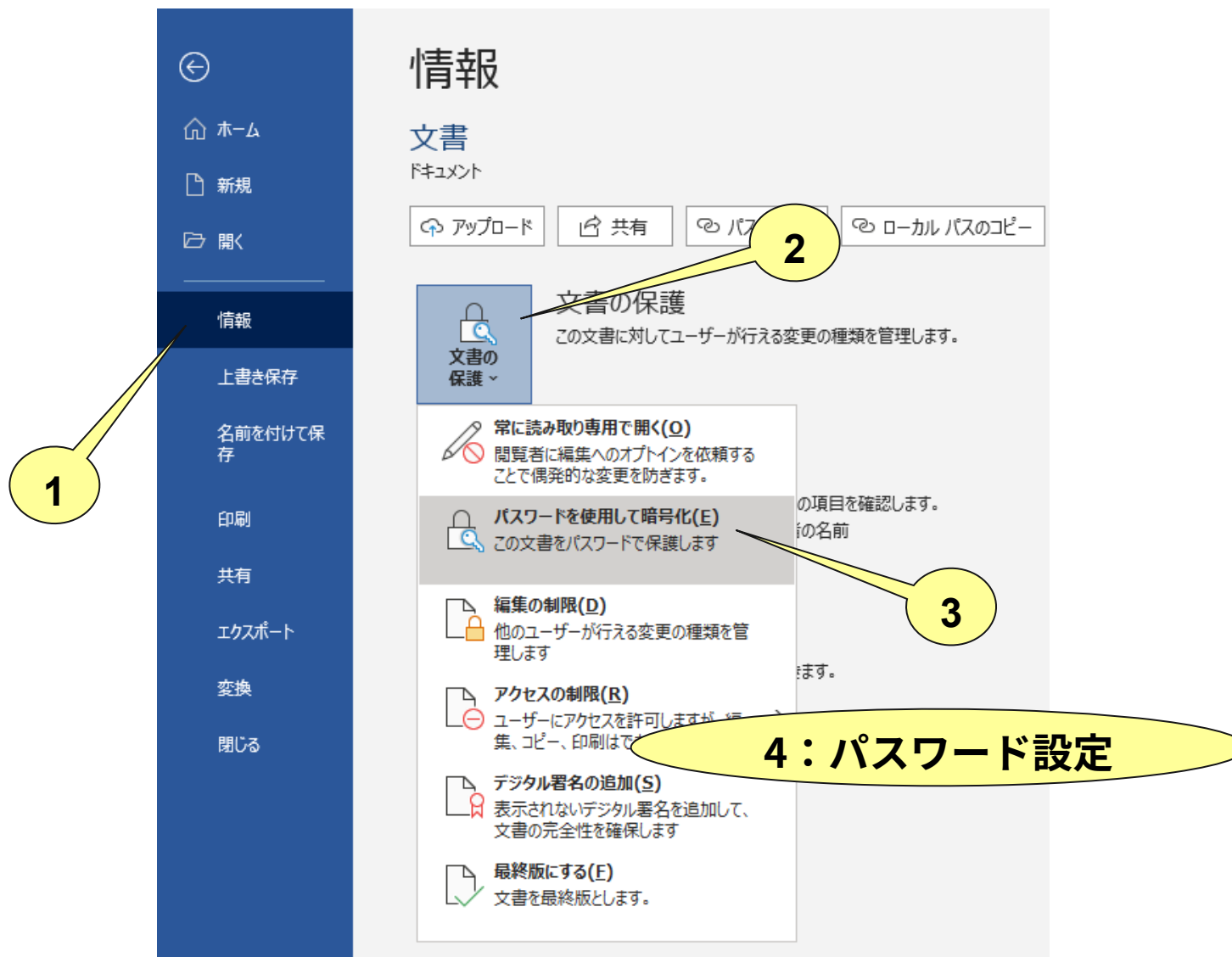
■ 電子メールで重要な情報を送付する場合は保護する

- ✓ 重要な情報は電子メールの本文に書かず文書ファイルに書いて強固なパスワードで保護する
 - ✓ パスワードはあらかじめ決めておくか、携帯電話のショートメッセージサービス（SMS）などの別手段で知らせる
- ✓ 盗聴やなりすましを防ぎ、改ざんの検知ができるS/MIME(※)などの暗号技術を利用する
- ✓ 法人向けデータ転送サービスやウェブサービスを利用し、利用者のみがアクセス可能なフォルダで重要情報を受け渡しする



(※) S/MIME(Secure/Multipurpose Internet Mail Extensions)電子メールの盗聴及び改ざんを防止する技術

<参考> Microsoft Word のパスワード設定



The screenshot shows the Microsoft Word 'Information' pane. On the left, a blue sidebar contains navigation options: ホーム (Home), 新規 (New), 開く (Open), 情報 (Information), 上書き保存 (Save Overwrite), 名前を付けて保存 (Save As), 印刷 (Print), 共有 (Share), エクスポート (Export), 変換 (Convert), and 閉じる (Close). A yellow callout with the number '1' points to the '情報' (Information) option in the sidebar.

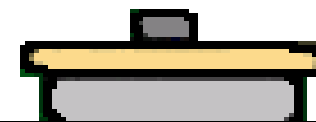
The main pane is titled '情報' (Information) and '文書' (Document). It shows buttons for 'アップロード' (Upload), '共有' (Share), 'パスワード' (Password), and 'ローカルバスのコピー' (Copy to Local Bus). A yellow callout with the number '2' points to the 'パスワード' (Password) button.

Below the buttons, the '文書の保護' (Protect Document) section is expanded. It shows a list of protection options: '常に読み取り専用で開く(O)' (Always open as read-only), 'パスワードを使用して暗号化(E)' (Encrypt with password), '編集の制限(D)' (Restrict editing), 'アクセスの制限(R)' (Restrict access), 'デジタル署名の追加(S)' (Add digital signature), and '最終版にする(E)' (Mark as final). A yellow callout with the number '3' points to the 'パスワードを使用して暗号化(E)' option.

A yellow callout with the number '4' points to the 'パスワード設定' (Password Settings) dialog box, which is not fully visible but is indicated by the callout.

No.10 無線LANの盗聴や無断使用を防ぐ

 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？



No.10 無線LANの盗聴や無断使用を防ぐ

● 対策が必要な理由

- 無線LANは配線が不要なため、オフィスの中で手軽にネットワークを構築できるが、セキュリティ設定をしていないと外部からアクセスされるおそれがある

● 対策をしないと何が起きるか

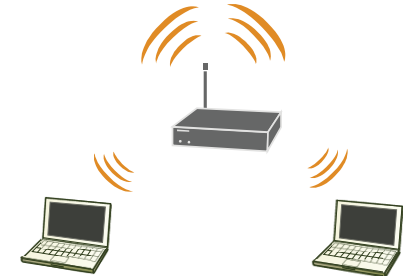
- 適切なセキュリティ設定がなされていないと通信内容を盗聴され、重要な情報が漏れる
- 無線LANのアクセスポイントに不正接続されて社内ネットワークに侵入されて
 - 社内の重要な情報の窃取、改ざんされる
 - ウイルスを感染させられることによるデータの消失、暗号化される
 - 攻撃や妨害で通信が遅くなる（止まる）

無線LANのセキュリティ設定を行い盗聴や不正接続を防ぎましょう！

● 具体的な対策例

■セキュリティ設定を強化する

- ✓ 強固な暗号方式（WPA3など）を選択する
- ✓ 推測されにくいパスワードを設定する



■モバイルルーターやスマートフォンのテザリング機能を使わないときはオフにする

■無線LANを使う際の制限・制限をルール化する

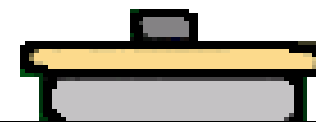
- ✓ アクセスポイント（SSID）が正規のものであることを確認する（偽アクセスポイントに接続しないよう注意）
- ✓ パスワードなしで接続可能、またはパスワードが公開されている場合は重要情報や個人情報やりとりはしない
- ✓ 重要な情報をやりとりする場合は、HTTPS通信（TLS/SSL）^(※1)に対応したウェブサイト、またはVPN^(※2)通信を利用する

(※1) TLS/SSL(Transport Layer Security/Secure Socket Layer) インターネット上で通信を暗号化し、第三者による盗聴や改ざんを防ぐ技術

(※2) VPN(Virtual Private Network) 私設仮想回線 インターネットや公衆回線網を使っても、専用線接続と同じようなセキュリティを保つことができる技術

No.11 インターネットを介したトラブルを防ぐ

 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？



No.11 インターネットを介したトラブルを防ぐ

● 対策が必要な理由

- インターネット上には悪意のあるウェブサイトやセキュリティ上の問題があるサイトなどが多くある
- SNSは拡散力が高く誤解や炎上などのトラブルが起きやすい

● 対策をしないと何が起きるか

- 悪意のあるウェブサイトやセキュリティ上の問題があるウェブサイトを閲覧することでウイルス感染する
- 意図せぬ情報の掲載
 - ホワイトボードや社内資料などの社外秘情報の映り込み
 - SNSや掲示板に悪ふざけした投稿の掲載で会社に被害を及ぼす



インターネット利用のルールを決めてトラブルを防ぎましょう！

● 具体的な対策例

■インターネットを利用する際の注意・制限をルール化する

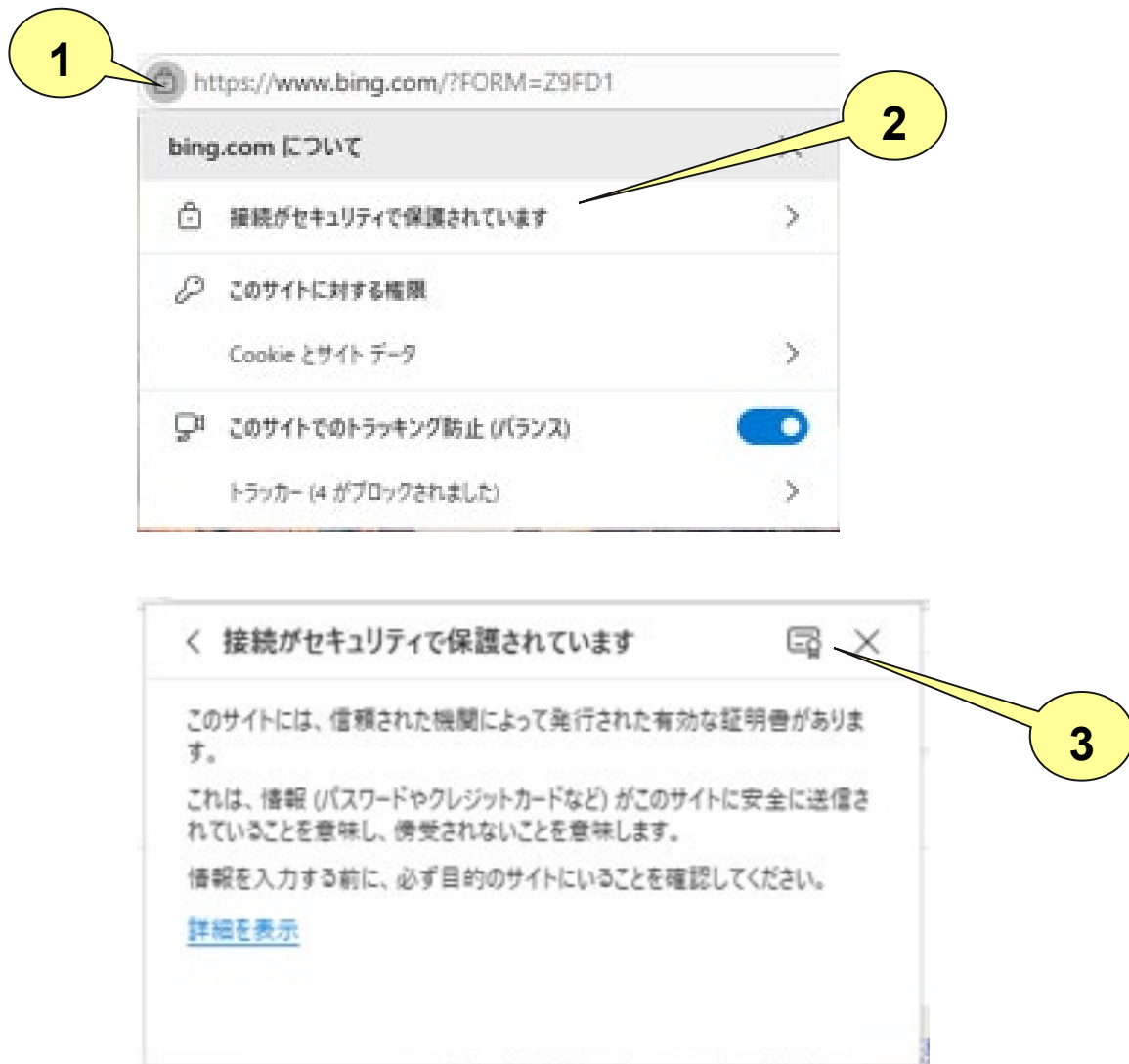
- ✓ ウェブサイトを閲覧するときには運営者の身分証明書であるサーバー証明書を確認する
- ✓ URLが「http」ではなく「https」になっていること（s=secure「安全」を意味する）
- ✓ URLの左側に通信が暗号化されている事を示す鍵マークが表示されていること
- ✓ URLの左側の鍵マークをクリックしサーバーの証明書を確認（次頁参照）
- ✓ SNSに重要情報や個人情報に記載しない

■ブラウザのセキュリティ機能を活用する

- ✓ URLがhttpsでない安全ではないサイトの場合に警告を出す
- ✓ 有害なサイトやダウンロードから保護する
- ✓ ポップアップや広告のブロック（怪しい広告やボタンをブロックして詐欺を防止）

■Webフィルタリングやプロキシ・サーバーなど技術的対策を利用して、アクセスできるサイトを制限する

<参考>ブラウザの証明書表示



4：証明書表示

証明書ビューアー: r.bing.com

全般(G) 詳細(D)

発行先

共通名 (CN)	r.bing.com
組織 (O)	Microsoft Corporation
組織単位 (OU)	<Not Part Of Certificate>

発行者

共通名 (CN)	Microsoft TLS G2 ECC CA OCSP 02
組織 (O)	Microsoft Corporation
組織単位 (OU)	<Not Part Of Certificate>

有効期間

発行日	2026年5月20日水曜日 2:42:36
有効期限	2026年12月4日金曜日 2:42:36

SHA-256 フィンガープリント

証明書	423826298618187d0de82e3047b003f3df3ab58f9112a7d6646c47a0f4ed22d3
公開キー	0e80db5164f1af226ab14be7f40025270e769abe10aca91297fcb8a5b1a50db0

No.12 重要情報の放置を禁止する

 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？



No.12 重要情報の放置を禁止する

● 対策が必要な理由

- 重要な情報が誰でも「見える」「手に取れる」状態は、関係のない人に情報を見られたり持ち出されたりするおそれがある

● 対策をしないと何が起きるか

- 重要な情報を含む書類、電子媒体（USBメモリ、CD/DVDなど）、プリンタに置き忘れた資料などが紛失、盗難にあう



重要情報の置き忘れを無くし情報の紛失や盗難を防ぎましょう！

● 具体的な対策例

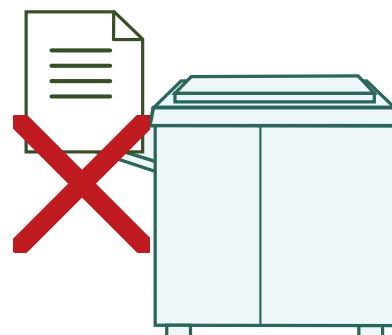
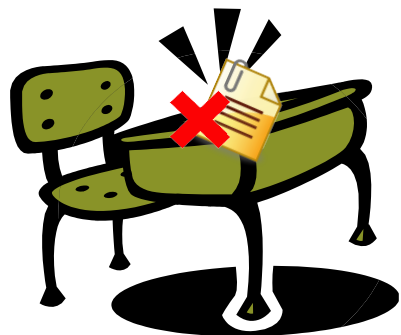
■机の上をきれいに整理整頓する

- ✓ 離席する場合は机の上に「何もない状態」にする
- ✓ 退社前に必ず片付ける

■印刷物はプリンタに放置せずすぐに回収する

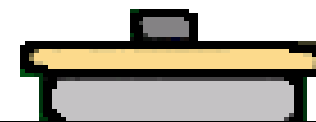
■重要情報を印刷した紙の裏側をメモに使わない

■自宅に重要情報または個人情報を含む書類や電子媒体を保管する場合は、鍵付き引き出しやケースに保管し、利用時以外は施錠する



No.13 重要情報は安全な方法で持ち出す

 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？



No.13 重要情報は安全な方法で持ち出す

● 対策が必要な理由

- ・ 情報を持ち出すと、思わぬ盗難やうっかり紛失することがある

● 対策をしないと何が起きるか

- ・ 紛失・盗難により第三者に情報が漏れる
- ・ 紛失・盗難により情報が消滅して業務が行えなくなる場合がある
- ・ 誰がいつ、どのような情報を持ち出したのかがわからないと、情報が漏れた範囲や影響度が把握できない

重要情報は安全な方法で持ち出し、情報漏えいを防ぎましょう！

● 具体的な対策例

■持ち出し時のルールを策定する

- ✓ 重要情報の持ち出しは必要最小限にする
- ✓ 重要情報の持ち出しは許可制にして持ち出し内容を記録する
- ✓ カフェや駅など公共の場所でテレワークを行うときにはパソコンや書類を放置しない
- ✓ 書類のまま持ち出す場合はカバンに入れて肌身離さず持ち歩く
(電車の網棚などに放置しない)

■紛失や盗難にあっても情報が見られないようにする

- ✓ ノートパソコン、スマートフォン、USBメモリなどにパスワードロックをかける
- ✓ 情報を暗号化する



No.14 重要情報は復元できないように消去する

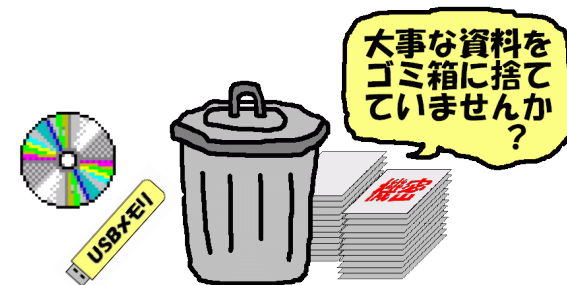
 重要情報が記載された書類や重要なデータが保存された媒体を廃棄する時は、復元できないようにしていますか？



No.14 重要情報は復元できないように消去する

● 対策が必要な理由

- 重要な情報が記載された書類をゴミ箱にそのまま捨てると、関係者以外の目に触れてしまうおそれがある
- 電子機器・電子媒体に保存された電子データはファイルを削除しても復元できる場合がある



● 対策をしないと何が起こるか

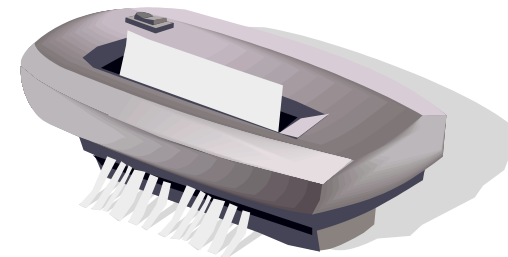
- 重要な情報が記載された書類、電子機器、電子媒体がごみ箱やゴミ捨て場から盗まれて第三者に情報が漏れる
- 電子機器、電子媒体に保存されたデータが復元されて情報が漏れる
- 廃棄業者によって電子媒体が転売されて情報が漏れる

復元できない状態にして廃棄し情報漏えいを防ぎましょう！

● 具体的な対策例

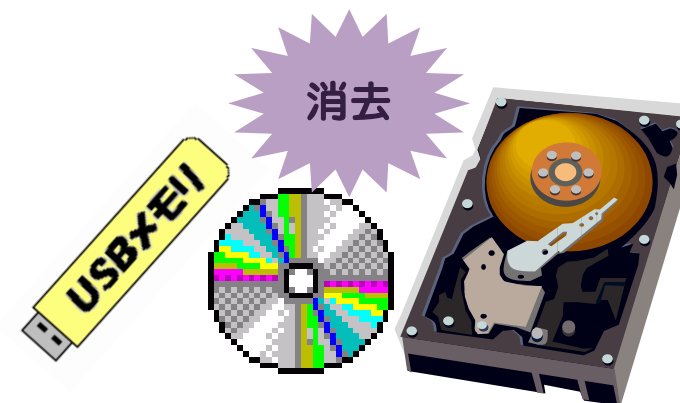
■書類を復元できない状態にして廃棄する

- ✓ シュレッダーなどで細断する
- ✓ 専門業者に書類の溶解を委託して証明書を取得する



■電子データを復元できない状態にして廃棄する

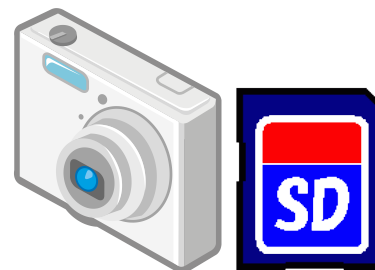
- ✓ 消去ソフトを利用してデータを消却してから廃棄する
- ✓ データを上書きして元のデータが見えないようしてから廃棄する
- ✓ 暗号化しているデータは鍵を廃棄する
- ✓ 電子媒体を物理的に壊してから廃棄する
- ✓ 専門業者に消去処分を委託して証明書を取得する



<参考>デジタルカメラ・スマートフォンの廃棄

● デジタルカメラの廃棄

- SDカードなどは本体から抜き取り専用ソフトでデータを消去するか、SDカードを物理的に破壊
- 本体の初期化



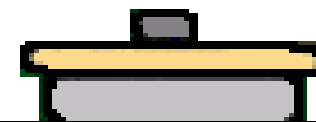
● スマートフォンの廃棄

- SIMカード、microSDカードを抜きだす（必要に応じて消去）
- アカウントの解除
- 工場初期化状態にリセット
- キャリアショップや業者に廃棄処理を依頼



No.15 機器を勝手に操作させない

 離席時にパソコン画面の覗き見や
勝手な操作ができないように
していますか？



No.15 機器を勝手に操作させない

● 対策が必要な理由

- ・ パソコンやサーバーにログインしたまま離席すると「誰でも使える状態」となっている

● 対策をしないと何が起こるか

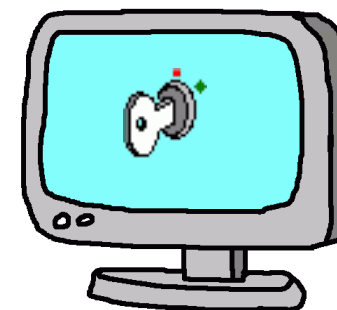
- ・ 不正に操作されて情報が洩れたり改ざん、消去などが発生する
- ・ 誤操作による意図しない情報の改ざん、紛失、消去などにつながる

機器を勝手に操作させないことで情報を守ましょう！

● 具体的な対策例

■ 機器を勝手に操作させないための対策をする

- ✓ 離席時ににスクリーンロックをかける
 - ✓ Windows OSの場合 「Windows キー + L」 または 「Ctrl + Alt + Delete」
 - ✓ MacOSの場合 「Controlキー+ command +Q」
- ✓ スクリーンセーバーを設定し、自動でロックする
- ✓ 退社時にパソコンやサーバーをシャットダウンする
- ✓ 使用していないアカウントは削除する



■ 作業中にパソコンの画面のぞき見られないようにする

- ✓ パソコンに「のぞき見防止フィルタ」をとりつける

No.16 見知らぬ人には声をかける

 関係者以外の事務所への立ち入りを制限していますか？



No.16 見知らぬ人には声をかける

● 対策が必要な理由

- ・ 関係者以外の立ち入りを制限していないと、不審者が侵入するおそれがある
- ・ サーバルームや書庫・金庫には重要な情報が保管されている

● 対策をしないと何が起きるか

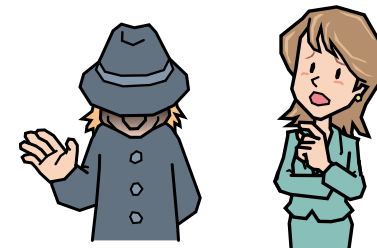
- ・ 社外から第三者に侵入されて、重要な情報の紛失・盗難、改ざん、消去など被害に遭う
- ・ 第三者に社内を勝手に撮影されて見せてはいけない情報が漏れる

関係者以外を勝手に侵入させないことで情報を守りましょう！

● 具体的な対策例

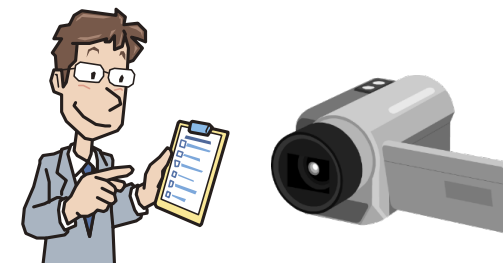
■ 外部から侵入されないための対策を行う

- ✓ 見知らぬ人を見たら声掛けする、不審に思ったら報告する
- ✓ 受付カウンターの設置や守衛を配置する
- ✓ 施錠管理を徹底する
 - ✓ オフィスの入り口だけでなく各部屋も施錠（サーバールーム、書庫、金庫など）
- ✓ 見た目で従業員か否かを識別できるようにする（名札、制服、入館証など）



■ 外部から侵入された場合に状況を追跡できるようにする

- ✓ 入退出の記録を残す
 - ✓ 入退をチェックリストに記録する
 - ✓ 最終退出者と退出時間の記録を残す（次頁参照）
- ✓ 監視カメラを設置する（侵入の抑止効果も期待できる）



＜参考＞最終退場時のチェックリストの例

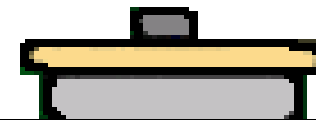
- ・ 日付
- ・ 退出時間
- ・ 退出者名
- ・ 情報チェック
 - ・ 机の上に重要な情報が出たままになっていないか
 - ・ 書類・CD/DVD・ノートP C・USBメモリ・・・
- ・ 電源チェック
 - ・ パソコン・モニター・サーバー・・・
 - ・ コピー機・シュレッダー・・・
- ・ 消灯チェック
- ・ 施錠チェック



チェックリストを使うことで最終退場者による責任意識の向上も期待できます

No.17 機器・備品の盗難防止対策を行う

 退社時にノートパソコンや備品を
施錠保管するなど盗難防止対策を
していますか？



No.17 機器・備品の盗難防止対策を行う

● 対策が必要な理由

- 機器（ノートパソコン、タブレット端末、電子媒体など）や備品などは手軽に持ち運べる便利さがある反面、盗難のおそれがある
- 機器には会社の「重要な情報」が含まれている場合がある

● 対策をしないと何が起きるか

- 重要な情報が含まれている機器が盗難に遭う
- 機器の盗難により資産が紛失する
- 盗難にあった機器が攻撃の入り口として利用される

機器や備品の盗難を防止し資産や重要情報を守りましょう！

● 具体的な対策例

■ 盗難防止の対策を行う

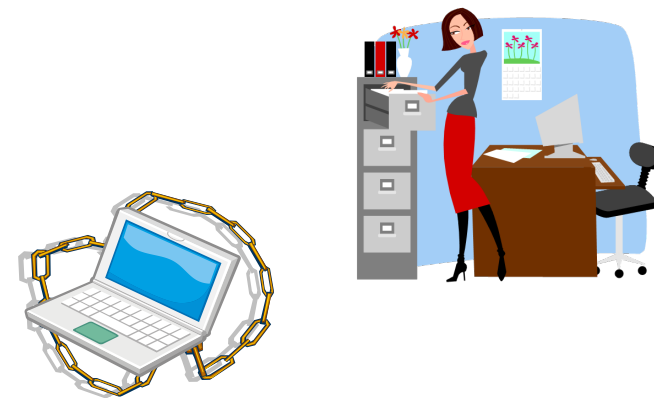
- ✓ 退社時に機器・備品は引き出しやロッカーにしまい施錠する
- ✓ 機器にセキュリティワイヤーを取り付ける

■ 盗難にあっても情報が見られないようにする

- ✓ パスワードロックをかける
- ✓ 情報を暗号化する
- ✓ 遠隔ロック、遠隔初期化の設定

■ 機器を追跡できるようにする

- ✓ スマートフォンの「探す」を有効化しておく
 - ✓ iPhone: 「iPhoneを探す」をON、Android: 「デバイスを探す」をON
- ✓ PCのOSの追跡機能を設定しておく



Part3:組織としての対策



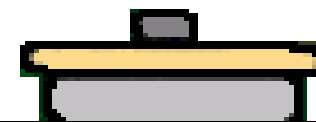
- ネットワーク管理
- ウェブサイト管理
- 従業員教育
- 私物機器の利用
- 取引先管理
- 外部サービスの利用
- 事故への備え
- ルールの周知

Part3:組織としての対策

- No.18 外部から内部ネットワークへの不要な通信を遮断する
- No.19 ウェブサイトを安全に運用する
- No.20 従業員に情報セキュリティ教育を行う
- No.21 個人所有端末の業務での利用可否を決める
- No.22 取引先に秘密保持を要請する
- No.23 信頼できる外部サービスを使う
- No.24 事故発生に備えて事前に準備する
- No.25 情報セキュリティ対策をルール化する

No.18 外部から内部ネットワークへの不要な通信を遮断する

 社内ネットワークに対する不要な通信を遮断していますか？



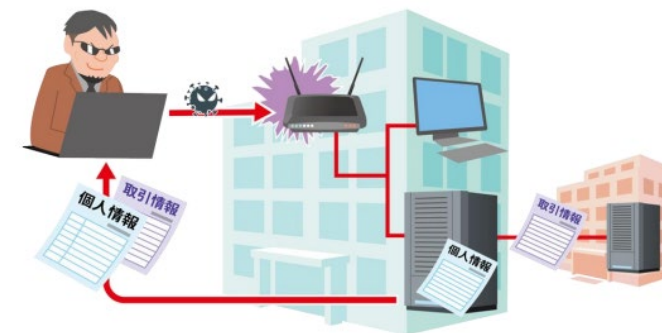
No.18 外部から内部ネットワークへの不要な通信を遮断する

● 対策が必要な理由

- 外部からの不要な通信は悪意のある攻撃の入り口となり、社内ネットワークに侵入されるおそれがある
- 万一侵入されると、被害が他の機器やシステムに拡大するおそれがある

● 対策をしないと何が起きるか

- 外部から社内ネットワークに侵入されて
 - システムや情報を勝手に操作される
 - 情報が漏れる
 - 情報を悪用される
 - 悪意のあるプログラムが送り込まれてウイルス感染する
- 外部からの大量アクセスで社内システムに高負荷を与え業務が停止する



不要な通信を遮断し社内ネットワークへの侵入を防ぎましょう！

● 具体的な対策例(1/2)

■ 使っていない通信を遮断する

- ✓使っていないリモート接続サービスは停止する（RDP、Telnetなど）
- ✓ネットワークに接続されている機器のファイアウォール^(※1)機能で外部からの不正なアクセスを拒否する

■ 不正なアクセスや操作を検知する

- ✓アクセスログを確認し、社外からの侵入や社内外の不信な操作や異常を検知して遮断や防御の対策をとる

■ 不正な侵入をされにくくようにする

- ✓ネットワーク機器のファームウェアの更新
- ✓ネットワーク機器の初期パスワードの変更

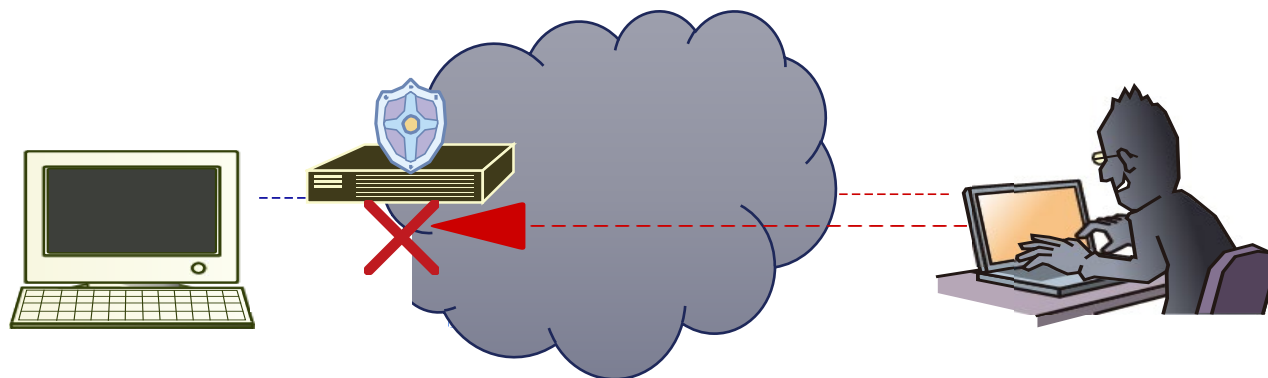
(※1) ファイアウォール：通信をさせるかどうかを判断し許可する、または拒否する技術。

例えば、インターネットと社内LANとの間に設置して、外部からの不正なアクセスを社内のネットワークに侵入させないようにできます。

● 具体的な対策例(2/2)

■不正な侵入を検知して遮断する

- ✓ 社内ネットワークとインターネットへの出入口に、社内ネットワークへの不正侵入を検知する機器(IDS^(※2)やUTM^(※3)など)を導入する



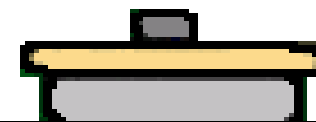
(※2) IDS(Intrusion Detection System)：侵入検知システム、システムやネットワークに対する不正なアクセスなどを検知して管理者に通知する技術。

例えば、インターネットとファイアウォールの間に設置することで、不正アクセスと思われる通信を検知して管理者に通知できます。

(※3) UTM(Unified Threat Management)：統合脅威管理、ファイアウォールやIDS・IPS、メールフィルタリング、URL フィルタリングなど複数の異なるセキュリティ機能を一つのハードウェアに統合して、社内ネットワークとインターネットの脅威であるウイルスの侵入や不正アクセス、サイバー攻撃などを検知し、防御するツールです。

No.19 ウェブサイトを安全に運用する

 **ウェブサイト**に情報を公開する前に
重要情報・非公開情報・古い情報が
含まれていないか確認していますか？



No.19 ウェブサイトを安全に運用する

● 対策が必要な理由

- 会社のウェブサイトはインターネット上に公開されており、不特定多数からアクセス可能となっているため攻撃の対象となるおそれがある
- 会社のウェブサイトは顧客や取引先との接点であり正しい情報を安全に発信する責任がある

● 対策をしないと何が起きるか

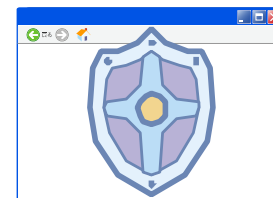
- 通信の内容が盗聴されてログイン情報や個人情報などの重要な情報が漏れる
- 外部からウェブサイトに侵入され管理者権限をのっとられて
 - ウェブサイトの内容が偽の情報に書き換えられる
 - 偽のウェブサイトへ誘導するように書き換えられる
 - ウイルスを仕掛けられてウェブサイトにアクセスすると感染する

ウェブサイトを安全に運用することで改ざんやウイルス感染を防ぎましょう！

● 具体的な対策例

■ 安全なシステムや通信を使う

- ✓ CMS^(※1)やECサイト構築ソフトなどの脆弱性対策をする（システムや構築ソフトウェアに脆弱性があると作成したウェブサイトが脆弱になる）
- ✓ 自社のウェブサイトがHTTPS^(※2)通信に対応しているか確認する
- ✓ WAF^(※3)を導入してウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護する



■ 不要な環境や情報を削除する

- ✓ 開発工程やテスト環境などで使用した不要なアカウントは削除する
- ✓ 公開ファイルに個人情報などの非公開情報が含まれていないことを確認する
- ✓ 期間限定のページや不要になったウェブサイトは閉鎖する



※(1)CMS(Contents Management System)：入力フォームを用いてページの作成、更新、管理などの作業を行えるように支援するシステムの総称

※(2)HTTPS(HyperText Transfer Protocol Secure)：Webブラウザとサーバーの間でデータをやり取りする際にデータを暗号化した安全性の高い通信プロトコル

※(3) WAF(WebApplicationFirewall)：ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを保護する技術。

例えば、ファイアウォールやIDS/IPSとウェブサーバーの間に設置することで、ウェブアプリケーションがやり取りするデータを監視して攻撃を検出できます

No.20 従業員にセキュリティ教育を行う

従業員にセキュリティに関する教育や
注意喚起を行なっていますか？



No.20 従業員にセキュリティ教育を行う

● 対策が必要な理由

- ・ 従業員は日々業務において様々な情報を取り扱っているため、慣れによってセキュリティへの意識が低下するおそれがある

● 対策をしないと何が起きるか

- ・ 情報セキュリティ対策のルールがあるだけでは守られない
- ・ 人によって理解や判断がバラバラとなり、対策に漏れや不足が発生する
- ・ ルール違反に気が付かず、ルール違反が常態化する
- ・ セキュリティインシデントが発生しても気が付かず、報告されない
- ・ 従業員が情報セキュリティ対策の必要性和内容を理解していないと正しい行動ができない

従業員にセキュリティ教育を行いセキュリティ意識を向上させましょう！

● 具体的な対策例

■情報管理のルールについて教育を行う

- ✓ 重要情報を取り扱う場合は十分注意するよう説明する
- ✓ 法令や契約について説明する
- ✓ セキュリティインシデントが発生した場合の被害、影響を説明する
- ✓ 採用・退職の際に守秘義務について説明し、守秘に関する覚書を交わす



■定期的に繰り返して教育を行う（繰り返すことで理解を深める）

- ✓ 朝礼、部内会議など、繰り返し実施する会議体の中で実施する
- ✓ テーマを決めて5分程度の教育とディスカッションを定期的に行う
- ✓ メールや動画の配信を繰り返して行う
- ✓ いつでも見られるようにルールを冊子やファイルで配布する
- ✓ ポスターなどで見えるところにルールを掲示する

<参考>IPA 情報セキュリティ教材・ツール

<https://www.ipa.go.jp/security/sec-tools/index.html>

情報セキュリティ教材・ツール

情報セキュリティ教材・ツール

企業・組織向け

学校向け・一般向け

企業・組織向け

情報セキュリティ教材

情報セキュリティ

10大脅威

組織編

情報セキュリティ10大脅威【組織編】

前年に発生したセキュリティ事故や攻撃の状況等から組織向けの脅威を選出し順位付けし、手口や事例、対策等を解説しています。解説資料は冊子版と簡易説明資料（スライド形式）がダウンロードいただけます。簡易説明資料（スライド形式）は英語版もございます。

[情報セキュリティ10大脅威【組織編】について、もっと詳しく](#)

セキュリティ
インシデント対応
机上演習教材



セキュリティインシデント対応机上演習教材

セキュリティインシデント対応の一連の流れを机上で演習する教材（パワーポイント）とその実施マニュアルです。セキュリティ意識向上と対策強化にご活用ください。

[セキュリティインシデント対応机上演習教材について、もっと詳しく](#)

映像で知る情報セキュリティ



映像で知る情報セキュリティ【企業・組織向け】

情報セキュリティの脅威と対策をドラマを通じて学べる映像シリーズです。YouTubeでの視聴のほか、主な情報セキュリティ対策動画は動画ファイルでの提供も行っております。

[映像で知る情報セキュリティ【企業・組織向け】について、もっと詳しく](#)

5分
でできる！

情報セキュリティポイント学習

5分でできる！情報セキュリティポイント学習

中小企業で働く方を対象とした、1テーマ5分で情報セキュリティについて勉強できる学習ツールです。各テーマの最後に確認テストが付いています。学習理解の確認にお役立てください。

[5分でできる！情報セキュリティポイント学習について、もっと詳しく](#)

AppGoat

突いてみますか？脆弱性



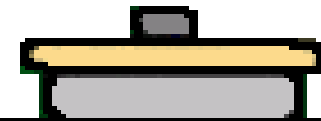
脆弱性体験学習ツール AppGoat

脆弱性の概要や対策方法等の脆弱性に関する基礎的な知識を実習形式で体系的に学べるツールです。ウェブアプリケーションの脆弱性対策に必要なスキルを習得したい開発者やウェブサイトの管理者におすすめです。

[脆弱性体験学習ツール AppGoatについて、もっと詳しく](#)

No.21 個人所有端末の業務での利用可否を決める

 個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？



No.21 個人所有端末の業務での利用可否を決める

● 対策が必要な理由

- 個人所有のパソコンやスマートフォンはセキュリティ対策のレベルが一定ではない（ウイルス対策の有無、OSの更新状況など）
- 個人所有の端末は会社がコントロールできない（アプリのインストール、家族と共有など）
- セキュリティインシデント発生時に会社のルールが適用できない（端末の隔離、調査、廃棄など）

● 対策をしないと何が起きるか

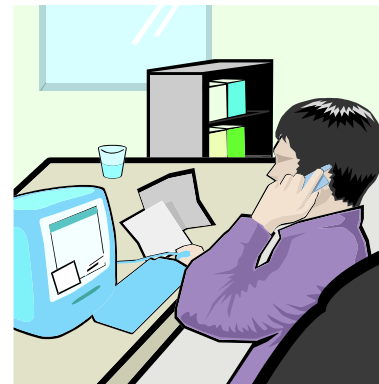
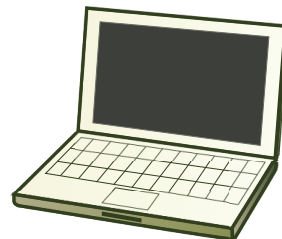
- 重要情報が漏れたり、ウイルス感染したりする
- インシデントの責任所在が不明となる
- 録音、画像保存、写真などをSNSにアップされる

業務での利用可否を決めウイルス感染や情報漏えいを防ぎましょう！

● 具体的な対策例

■ 個人所有端末利用時のルールを決める

- ✓ 業務利用を許可制にする（業務上必要な場合のみ許可する）
- ✓ 個人所有端末のセキュリティ条件を決める（OSの最新化、ウイルス対策ソフトの導入など）
- ✓ 個人所有端末に会社情報を保存しない
- ✓ 紛失時のルールを決める
- ✓ テレワークで個人所有端末やWi-Fiルーター、家庭のインターネット回線を利用する場合のルールを決める



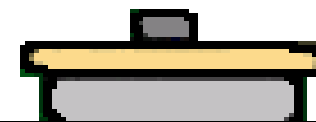
＜参考＞BYODとは

- BYOD(Bring Your Own Device)とは業務で個人の端末を使うことを意味します。
- コスト低減や作業効率化などのメリットはありますが、個人端末での情報の持ち出しによる情報漏えいの危険性などのデメリットもあります。
- 個人端末を業務で勝手に使うのは危険です。
- 必要な場合は会社（組織）に許可を得た上で、ルールに従って使うことを推奨します。



No.22 取引先に秘密保持を要請する

 重要情報の授受を伴う取引先との
契約書には、秘密保持条項を規定
していますか？



No.22 取引先に秘密保持を要請する

● 対策が必要な理由

- 事業を行う上で取引先と重要な情報の共有が必要となることがある
- 取引先が情報の内容から判断して「当然秘密にしてくれるだろう」という一方的な期待は危険（情報が適切に管理されないおそれがある）

● 対策をしないと何が起きるか

- 自社だけで秘密を守っていても、取引先が守らなければ情報が漏れる
- 取引先と共有した重要情報が無断利用や悪用される
- 取引先の再委託先に重要情報が漏れる

取引先に秘密保持を要請し重要情報を守りましょう！

● 具体的な対策例

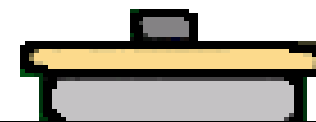
- 取引先と秘密保持や具体的な対策を明記した契約や覚書を交わす
- 取引先が再委託を行う場合は、取引先と同等の秘密保持を要請する
- 秘密保持や情報セキュリティ対応方針を公表している取引先を選定し、情報セキュリティ対策の実施状況を確認する
- 定期的な確認を実施する
 - ✓定期的に秘密保持契約の内容を確認する
 - ✓定期的に秘密保持の対策が実施されているか確認する



No.23 信頼できる外部サービスを使う



クラウドサービスやウェブサイトの
運用などで利用する外部サービスは、
安全・信頼性を把握して選定して
いますか？



No.23 信頼できる外部サービスを使う

● 対策が必要な理由

- 外部サービスは多くの利用者に公開されているため攻撃の対象となりやすい
- サービス提供者のセキュリティ対策・運用体制・補償内容が、自社の要求や法令に合わない場合がある

● 対策をしないと何が起きるか

- 外部サービスの脆弱性や設定ミスをつかれ、攻撃者から不正アクセスされる
- サービス停止や障害により業務が停止する可能性がある
- 個人情報を海外に保存する場合、法律や契約上の要件に抵触することがある
- 障害などの場合に十分な補償を受けられない可能性がある
- 障害で情報が消滅し、復旧できない事態が発生する可能性がある

信頼できる外部サービスを使い重要情報を守りましょう！

● 具体的な対策

■利用規約や補償内容、セキュリティ対策などを確認して事業者を選定する

- ✓ セキュリティ対策内容の確認
 - ✓ 例：セキュリティ認証取得、第三者による監査報告、セキュリティポリシーの公開など
- ✓ 外部サービスが補償する稼働時間や補償内容の確認
- ✓ 外部サービスの事業者との間の責任範囲の明確化
- ✓ インシデント報告義務の確認
- ✓ 「中小企業のためのクラウドサービス安全利用の手引き」など、ガイドラインを活用してクラウドサービスを安全に利用する（次頁参照）

■外部サービスを適切に使うための設定・管理を行う

- ✓ 安全に運用するための運用ルールや担当者を決める
- ✓ パスワードなどの認証機能について適切に設定・管理を実施する



<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

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

● クラウドサービスを選択し、安全に運用するための15項目のポイントを解説した手引き

選択するときのポイント

事業者の信頼性確認、サービスの安全性・信頼性確認、
取扱う情報の重要度を確認など

運用するときのポイント

運用管理者の決定、利用者認証を厳格に実施、
バックアップに責任を持つなど

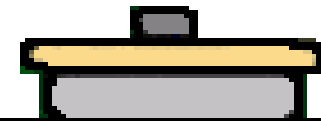
セキュリティ管理のポイント

サポート体制を確認、適用法令や契約条件を確認、
データ保存先の地理的所在地の確認など



No.24 事故発生に備えて事前に準備する

 セキュリティインシデント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？



No.24 事故発生に備えて事前に準備する

● 対策が必要な理由

- セキュリティインシデントはいつ起きるか予測ができない
- 人のミスは完全になくすことができない
- 事前に対応を準備しておかないと事業継続できなくなるおそれがある



● 対策をしないと何が起きるか

- 誰が何をするか決まっていないと現場が混乱し、状況の把握、判断ができず初動が遅れ被害が拡大する
- 顧客への説明ができない、報告が遅れる
- 復旧手順が決まっていないと何をして良いかわからず、復旧に時間がかかる

セキュリティインシデントに備えて事前に準備しましょう！

● 具体的な対策例

■セキュリティインシデント発生時の体制を整備する

- ✓ 対応責任者、現場対応者の役割分担、連絡体制を決める

■セキュリティインシデント発生時の作業手順書を作成し、従業員に周知する

- ✓ ウイルス感染、重要情報の流出、紛失、盗難などが発生した場合の作業手順
- ✓ 「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」などを活用し、誰がいつ何をするのかをまとめる（次頁参照）

■セキュリティインシデント発生時に相談できる先を決めておく

- ✓ 例：セキュリティベンダー、親会社など

■セキュリティインシデント発生時の対応に関する訓練を行う

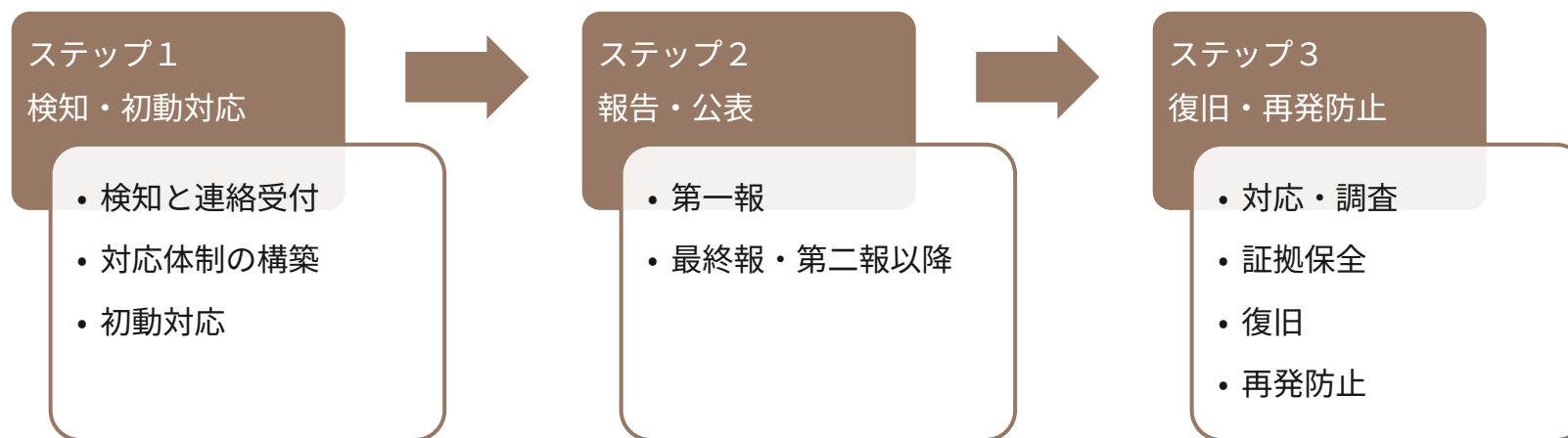
- ✓ 定期的に手順書の内容や連絡先の見直しを行う



<参考> 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

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

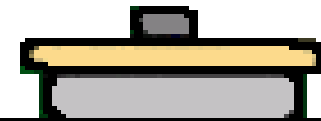
- インシデント発生時の対応について、「検知・初動対応」「報告・公表」「復旧・再発防止」の3つのステップに分けて検討事項を説明
- インシデント対応時に整理しておくべき事項や相談窓口・報告先などを紹介



No.25 情報セキュリティ対策をルール化する

 情報セキュリティ対策_(※)をルール化し、
従業員に明示していますか？

(※) No.1～24で決定した対策など



No.25 情報セキュリティ対策をルール化する

● 対策が必要な理由

- ・ 従業員がどう行動すべきか明確にするため
- ・ 組織として一貫した運用を実現するため

● 対策をしないと何が起きるか

- ・ 従業員が判断に迷い、都度指示を仰ぐ必要が生じる
- ・ 人によって対応が異なり、セキュリティの穴や対応遅延が発生する
- ・ 重大インシデント発生時に対応手順が不明確で被害が拡大する

情報セキュリティ対策をルール化し組織として情報を守りましょう！

● 具体的な対策例

■情報セキュリティ対策のルールを策定し社内で共有する

- ✓ 診断シート項目のNo.1からNo.24までをルール化する
- ✓ 「情報セキュリティハンドブック（ひな形）」を活用する(次頁参照)
- ✓ ルールは従業員がいつでも見られるようにする
 - ✓ 共有サーバーに配置して場所を周知する、冊子やファイルで配布する

■情報セキュリティ対策のルールを見直す

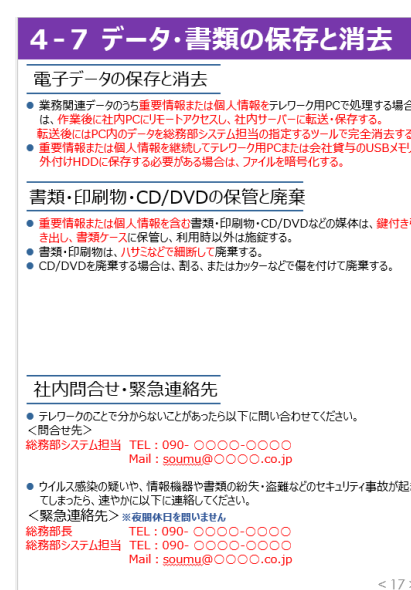
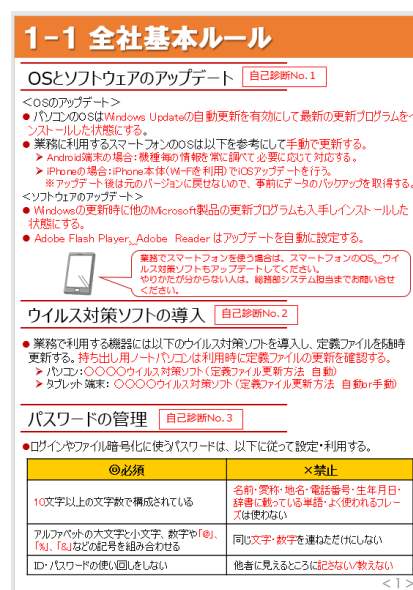
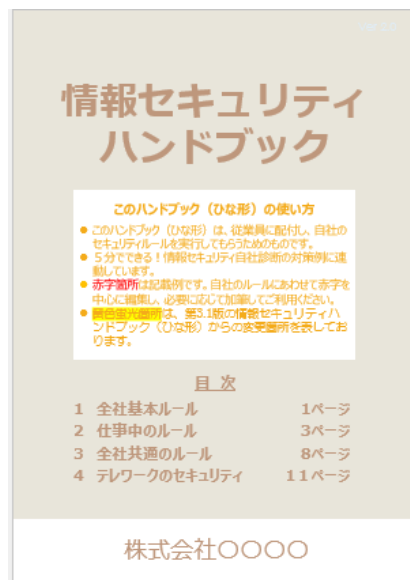
- ✓ 新たな攻撃や社内外で発生したセキュリティインシデントの事例などを参考にして定期的にルールを見直す



<参考>情報セキュリティハンドブック（ひな形）

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

- 従業員に対して自社のセキュリティルールを周知させるために作成するハンドブックのひな形です
- 5分でできる！情報セキュリティ自社診断の対策例に連動しています
- 自社のルールにあわせて記載例の赤字を中心に編集し、必要に応じて加筆してご利用ください



【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
- 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



●「★二つ星」を宣言しよう！

「★二つ星」は、「5分でできる!情報セキュリティ自社診断」を活用して情報セキュリティ対策に取り組む企業の証として、自社のPRに活用できます。

ここからセキュリティ！

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

- 「ここからセキュリティ！」は国内の30を超える公的機関・民間団体・企業が提供する情報セキュリティに関する情報を集めたポータルサイトです。
- 「被害に遭ったら」「対策する」「教育・学習」「セキュリティチェック」「データ&レポート」といったニーズ別に分類しており、欲しい情報を見つけやすくしています。



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

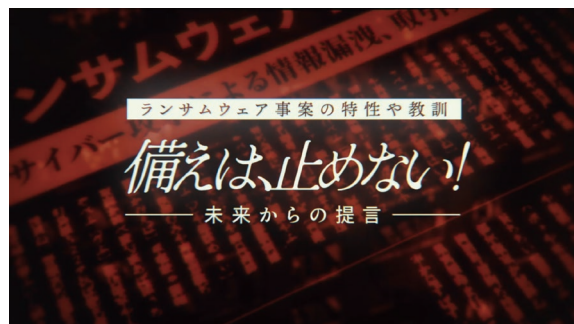
cs-support@ipa.go.jp

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

<https://www3.jitec.ipa.go.jp/JitesCbt/index.html>



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/>