



新年度はセキュリティ教育の確認と見直しを

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

IPA 独立行政法人情報処理推進機構 セキュリティセンター

4 本ガイドラインの活用方法

本ガイドラインの活用にあたって、情報セキュリティに積極的に取り組んだ結果が必要ありません。本ガイドラインにより、事業の発展に即した情報セキュリティ対策を段階的に進めていくことができます。【第1部 経営層編】は、全ての経営者に読んでいただきたい内容です。まずは一通りご覧ください。【第2部 実践編】は、あなたの組織にあったSTEPから始めてください。

現状状況とアクション	本ガイドラインの活用方法
Step1 まず始めましょう	これまで情報セキュリティ対策を積極的に行っていない場合は「2. できることから始める編(IP2)」を参照して、「情報セキュリティ5か条」を実行してください。 留意点 「情報セキュリティ5か条」を社内で作成するなど、まずできることから開始してください。
Step2 現状を知り改善しましょう	Step1は実施できているか確認する場合は「3. 現状を把握する編(IP3)」を参照して、「5分でもできる!情報セキュリティ5か条」を参照し、自社の現状を把握し、必要に応じて対策の実行に努めてください。 留意点 「情報セキュリティ5か条」を参考に基本方針を作成してください。 「5分でもできる!情報セキュリティ5か条」で現状の対策を把握し、実施すべき対策を検討してください。 「情報セキュリティ5か条」(IP2)を参考に、具体的な対策を定めて策定に活用してください。
Step3 本格的に取り組みましょう	Step2までは実施できているか確認する場合は「4. 本格的に取り組む編(IP4)」を参照して、自社のリスクに応じた対策を策定し、運用は進捗して改善を図ってください。 留意点 「情報セキュリティ」の管理体制を構築し、対策の予算を確保してください。 対応すべきリスクと対策を検討し、「情報セキュリティ5か条」を参考に策定してください。 策定が必要となる対策を実行するとともに、改善や改定に努めてください。
Step4 改善を続けましょう	「5. より強固にするための方策」(IP5)を参照して、自社の必要対策を策定し、運用を継続してください。Step1やStep2に取り組んでいない場合は、Stepを参考に必要な対策を策定し実行してください。

Ver 1.5

情報セキュリティハンドブック

このハンドブック(04版)の使い方
このハンドブック(04版)は、従業員に配布し、自社のセキュリティルールを実行してもらうためのものです。5分でもできる「情報セキュリティ」(自社対策の原則)に準拠しています。
必ず記載した箇所は記載所です。自社のルールに合わせて手字を中心に編集し、必要に応じて追加してご利用ください。

目次

1 全社基本ルール	1ページ
2 仕事中のルール	3ページ
3 全社共通のルール	8ページ
4 テレワークのルール	12ページ

1-1 全社基本ルール

OSとソフトウェアのアップデート

自己診断No.1

<OSのアップデート>
 ●パソコンのOSはWindows Updateの自動更新を有効にして最新の更新プログラムをインストールした状態にする。
 ●業務に利用するスマートフォンOSは以下を参考として手動で更新する。
 > Android端末の場合: 機種毎の情報を元に調べ必要に応じて対応する。
 > iPhoneの場合: iPhone本体(Wi-Fiを利用)でOSアップデートを行う。
 ※アップデート後は元のバージョンに戻さないで、事前にデータのバックアップを取得する。

<ソフトウェアのアップデート>
 ●Windowsの更新時に他のMicrosoft製品の更新プログラムも入手インストールした状態にする。
 ●Adobe Flash Player、Adobe Reader はアップデートを自動に設定する。

※最近スマートフォンを扱う場合は、スマートフォンのOS、ウイルス対策ソフトもアップデートしてください。やりかたは必ず確認してください。

ウイルス対策ソフトの導入

自己診断No.2

●業務で利用する機器には以下のウイルス対策ソフトを導入し、定義ファイルを随時更新する。持ち出し用ノートパソコンは利用時に定義ファイルの更新を確認する。
 > パソコン: OOOOウイルス対策ソフト(定義ファイル更新方法 自動) 自動
 > タブレット端末: OOOOウイルス対策ソフト(定義ファイル更新方法 自動or手動)

パスワードの管理

自己診断No.3

●ログインやファイル暗号化に使うパスワードは、以下に従って設定・利用する。

○必須	×禁止
10文字以上の文字数で構成されている	名前・実称・地名・電話番号・生年月日・辞書に載っている単語・よく使われるフレーズは使わない
アルファベットの太文字と小文字、数字や「!」、「%」、「&」などの記号を組み合わせる	同じ文字・数字を連続しただけしない
ID・パスワードの使い回しをしない	他人に見えるように読めない読えない

出典 中小企業の情報セキュリティ対策ガイドライン <https://www.ipa.go.jp/security/guide/sme/about.html>

POINT

IPAのサイトでは、様々なセキュリティの資料やコンテンツが用意されており、ガイドラインの確認社内規定の確認や見直し、社員のセキュリティ教育に活用できます
 セキュリティ対策は個人の判断任せではなく、**組織としてどう対策するかが重要**です
 新入社員や人事異動等、組織の変更を迎える時期、セキュリティ対策の確認と見直しを!



対策

騙されないコツ **ゼロトラスト**の考え方を持ちましょう!

・撃退! 迷惑メール 1 ゼロトラストとは! https://www.dekyo.or.jp/soudan/contents/info/pamphlet_gm.html

知る(脅威、手口、ニュース、被害の実態等) 知っていれば防げる脅威もたくさんあります

・不審なメールはここで確認! 日本データ通信協会 <https://www.dekyo.or.jp/soudan/index.html>

・映像コンテンツ一覧 <https://www.ipa.go.jp/security/videos/list.html>

脅威となっている**ランサムウェア攻撃**、被害が拡大するといわれる**ビジネスメール詐欺**の動画は、要チェック!

・今、そこにある脅威~組織を狙うランサムウェア攻撃~ <https://www.youtube.com/watch?v=TWqJ5P8oaUM>

・What's BEC? ~ビジネスメール詐欺 手口と対策~ <https://www.youtube.com/watch?v=6DKJEG3woRU>

組織の社員全員・・・日頃から怪しいと思ったら開かず報告と情報共有、インシデント時の対応方法の確認

組織全体の対策・・・アップデートを怠らない、古い機器やソフトでサポートが切れたものは見直し、使用しない万が一のバックアップがあるか、定期的にとれているか確認を

人為的ミスの対応・・・セキュリティ対策をしていても不注意等での人為的ミスによる情報流出も増えています
機密情報の整理、情報持ち出しのルール、権限の見直し、公私を分け個人利用デバイス、クラウドサービス、USBメモリ等の利用制限なども検討を