# 【2位】サプライチェーンや委託先を狙った攻撃

- **対策**
  - **組織(自組織で実施)**

**【被害を受けた後の対応】**

- インシデント対応体制を整備し、対応する
- 被害への補償請求

# 【2位】サプライチェーンや委託先を狙った攻撃

- **対策**
  - **組織(自組織に関わる組織と共に実施)**

**【被害の予防／被害に備えた対策】**

- 取引先や委託先との連絡プロセスの確立
- 取引先や委託先の情報セキュリティ対応の確認、監査
- 情報セキュリティの認証取得および維持
  - ISMS、P マーク、SOC2 等を取得し、定期的な見直しと運用維持
- 公的機関等が公開している資料※1の活用


【出典】 ※1 サイバーセキュリティ経営ガイドラインと支援ツール(経済産業省)
https://www.meti.go.jp/policy/netsecurity/mng_guide.html
外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書(内閣サイバーセキュリティセンター)
https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf
自動車産業サイバーセキュリティガイドライン(一般社団法人日本自動車工業会)
https://www.jama.or.jp/operation/it/cyb_sec/cyb_sec_guideline.html

# 【2位】サプライチェーンや委託先を狙った攻撃

- **対策**
  - **組織(自組織に関わる組織と共に実施)**

**【被害を受けた後の対応】**

- 適切な報告／連絡／相談を行う
  - 上司、CSIRT、関係組織、公的機関等

# まとめ

## 情報セキュリティ対策の基本を実践

・「10大脅威」の順位は毎回変動するが、基本的な対策の重要性は変わらない

## 各脅威の手口の把握および対策を実践

・脅威に備えるためには攻撃手口や動向、および自組織が抱える要因等を把握することが重要

・「10大脅威」のランキングは、各組織において実施すべき対策の優先度とは必ずしも一致はしない

そのため、組織ごとの状況を考慮して対策の優先度を決定する

# まとめ

## 共通対策を実践

- 対策の種類単位で見ると、複数の脅威に有効な対策がある
- 以下の「共通対策」を「情報セキュリティ対策の基本」と共に実施することで、より効率的に広範囲な対策を進めることが可能

※情報セキュリティ10大脅威 2025 のページで共通対策の詳細な解説資料を公開中

| 共通対策 |
| --- |
| 認証を適切に運用する |
| 情報リテラシー、モラルを向上させる |
| 添付ファイル開封や、リンク、URL のクリックを安易にしない |
| 適切な報告/連絡/相談を行う |
| インシデント体制の整備し対応を行う |
| サーバーや PC、ネットワークに適切なセキュリティ対策を行う |
| 適切なバックアップ運用を行う |

# 詳細な資料のダウンロード

- 情報セキュリティ10大脅威　2025

  本資料に関する詳細な内容はWebサイトをご覧ください

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


※こちらの QR コードをスマートフォンの
QR コードリーダーアプリで読み込む
ことでもアクセスできます

# 中小企業の情報セキュリティ対策ガイドライン

# 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

- 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進め方などを分りやすく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」と、経営者が実行すべき「重要7項目の取組」を記載
    （第1部）
  - 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
    （第2部）
  - 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

# 第3.1版の主な変更点について

- **第1部　経営者編**
  - 関連法令や被害事例を最新の内容に見直し
- **第2部　実践編**
  - テレワークの情報セキュリティに関する解説を追加
  - セキュリティインシデント対応に関する解説を追加
- **付録**
  - 付録1「情報セキュリティ5か条」、付録3「5分でできる！情報セキュリティ自社診断」の対策例を最新の内容に見直し
  - 付録4「情報セキュリティハンドブック（ひな形）」、付録5「情報セキュリティ関連規程（サンプル）」にテレワークの情報セキュリティに関するひな形、サンプルを追加
  - 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」を追加

# ガイドラインの対象

- **対象組織**
  - 全ての業種の中小企業および小規模事業者
    （法人、個人事業主、各種団体も含む）

- **想定読者**
  - 経営者と情報セキュリティ対策を実践する責任者・担当者

# ガイドラインの構成

| | 構　成 | 概　要 |
|---|---|---|
| 本編 | 第１部　経営者編 | 経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。 |
| 本編 | 第２部　実践編 | 情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。 |
| 付録 | 付録１　情報セキュリティ５か条 | 組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。 |
| 付録 | 付録２　情報セキュリティ基本方針（サンプル） | 組織としての情報セキュリティに対する基本方針書のサンプルです。 |
| 付録 | 付録３　５分でできる！情報セキュリティ自社診断 | あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。 |
| 付録 | 付録４　情報セキュリティハンドブック（ひな形） | 従業員に対して対策内容を周知するために作成するハンドブックのひな形です。 |
| 付録 | 付録５　情報セキュリティ関連規程（サンプル） | 情報セキュリティに関する社内規則を文書化したもののサンプルです。 |
| 付録 | 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 | クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。 |
| 付録 | 付録７　リスク分析シート | 情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。 |
| 付録 | 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 | 情報漏えいやシステム停止などのインシデント対応のための手引きです。 |

# 第1部　経営者編

## 1. 情報セキュリティ対策を怠ることで企業が被る不利益

(1) 金銭の損失
(2) 顧客の喪失
(3) 事業の停止
(4) 従業員への影響

## 2. 経営者が負う責任

(1) 経営者などに問われる法的責任
(2) 関係者や社会に対する責任

## 3. 経営者は何をやらなければならないのか

(1) 認識すべき「3原則」
(2) 実行すべき「重要7項目の取組」

経営者は何をやらなければならないのか

# (1) 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、説明責任を果たすことができ、信頼関係を維持することが可能

経営者は何をやらなければならないのか

# (2) 実行すべき「重要7項目の取組」

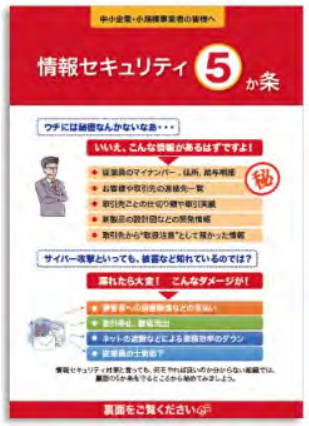
- 経営者は、以下の重要7項目を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

| | |
|---|---|
| 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 |

# 第2部　実践編

- できるところから始めて段階的にステップアップ

| 取組状況とアクション | 本ガイドラインの活用方法 |
|---|---|
| **Step1**<br>まず始めましょう | これまで情報セキュリティ対策を特に意識していない場合は**「2. できるところから始める」**(P.19) 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。<br>進め方<br>「情報セキュリティ５か条」を社内で配付するなど、まずできるところから開始してください。 |
| **Step2**<br>現状を知り改善しましょう | Step1 は実施できていて次に進める場合は<br>**「3. 組織的な取り組みを開始する」**(P.20) を参照して、「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、できていない対策の実行に努めてください。<br>進め方<br>・「情報セキュリティ基本方針（サンプル）」を参考に基本方針を作成してください。<br>・「５分でできる！情報セキュリティ自社診断」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。<br>・「情報セキュリティハンドブック（ひな形）」を参考に具体的な対策を定めて従業員に周知してください。 |
| **Step3**<br>本格的に取り組みましょう | Step2 までは実施できていて次に進める場合は<br>**「4. 本格的に取り組む」**(P.24) を参照して、自社のリスクに応じた対策規程を作成し、運用後は点検して改善を図ってください。<br>進め方<br>・情報セキュリティ管理の体制を構築し、対策の予算を確保してください。<br>・対応すべきリスクと対策を検討し、「情報セキュリティ関連規程（サンプル）」を参考に規程を作成してください。<br>・委託時に必要となる対策を検討するとともに、点検や改善に努めてください。 |
| **Step4**<br>改善を続けましょう | **「5. より強固にするための方策」**(P.32) を参照して、自社に必要な対策を追加実施してください。Step1 や Step2 に取り組んでいる企業でも、Step4 を参照して必要な対策があれば実行してください。 |




情報セキュリティ５か条


5分でできる！
情報セキュリティ自社診断


情報セキュリティ関連規程

- 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

Step1 できるところから始める

# (1) 情報セキュリティ5か条

- 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！

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。

## ② 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。

## ③ 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ます。
パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。

## ④ 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ます。
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を確認しましょう。

## ⑤ 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てID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

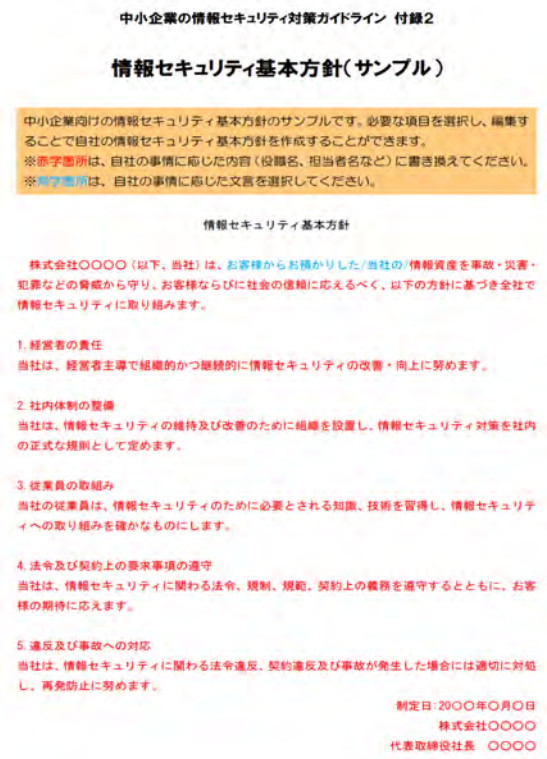
Step2 組織的な取り組みを開始する

# (1) 情報セキュリティ基本方針の作成と周知

- 経営者が定めた情報セキュリティに関する基本方針を、従業員や関係者に伝えるために簡潔な文書を作成・周知
- 付録2「情報セキュリティ基本方針（サンプル）」を編集して策定

**情報セキュリティ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



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。

情報セキュリティ基本方針

株式会社○○○○（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、技術を習得し、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、規制、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：2000年○月○日
株式会社○○○○
代表取締役社長　○○○○

Step2 組織的な取り組みを開始する

# (2) 実施状況の把握

- 自社のセキュリティ対策の実施状況を把握するために、付録3「5分でできる！情報セキュリティ自社診断」を活用
  - 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
    簡単に把握できる
    - 基本的対策　5項目
    - 従業員としての対策　13項目
    - 組織としての対策　7項目
  - 解説編の対策例を参考に、
    社内ルールを作成することができる


| 診断項目 | No | 診断内容 |
|---|---|---|
| Part 1 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？ |
| | 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？ |
| Part 2 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？ |
| | 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ができないようにしていますか？ |
| | 15 | 関係者以外の事務所への立ち入りを制限していますか？ |
| | 16 | 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？ |
| | 17 | 事務所が無人になる時の施錠忘れ対策を実施していますか？ |
| | 18 | 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棄する時は、復元できないようにしていますか？ |
| Part 3 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、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？ |
| | 20 | 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？ |
| | 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等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？ |

付録4

# 5分でできる！情報セキュリティ自社診断

| | | |
|---|---|---|
| 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？ |
| | 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？ |
| | 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？ |
| 従業員としての対策 | 14 | 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？ |
| | 15 | 関係者以外の事務所への立ち入りを制限していますか？ |
| | 16 | 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？ |
| | 17 | 事務所が無人になる時の施錠忘れ対策を実施していますか？ |
| | 18 | 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棄する時は、復元できないようにしていますか？ |
| 従業員としての対策 | 19 | 従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？ |
| | 20 | 従業員に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？ |