 Sec01-02-20\_中小企業の情報セキュリティ対策ガイドライン

ドキュメントを参照: [Sec01-02-20\_中小企業の情報セキュリティ対策ガイドライン.html](https://bluemoon55.github.io/Sharing_Knowledge/Cyber_Security/Deliverables/mind2html/Sec01-02-20_中小企業の情報セキュリティ対策ガイドライン.html)

1. 改版履歴
   1. 2019年12月18日　第3版補足
   2. 2019年12月17日　第3版追加
   3. 2018年12月25日　独立文書化
2. 中小企業の情報セキュリティ対策ガイドライン公開ページ

ドキュメントを参照: [guideline](http://www.ipa.go.jp/security/keihatsu/sme/guideline/)

1. Sec01-02-20-3\_中小企業の情報セキュリティ対策ガイドライン（第3版）
   1. 中小企業の情報セキュリティ対策ガイドライン第3版（全60ページ、32.56MB）

ドキュメントを参照: [000055520.pdf](https://www.ipa.go.jp/files/000055520.pdf)

* 1. 本文
     1. 経営者の皆様へ
        1. 情報セキュリティ対策は、経営に大きな影響を与えます！
        2. 経営者が自ら動かなければ、法的・道義的責任を問われます！
        3. 組織として対策するために、担当者への指示が必要です！
     2. 本ガイドラインの対象
        1. 業種を問わず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）を対象として、その経営者と情報管理を統括する方
     3. 本ガイドラインの全体構成
     4. 本ガイドラインの活用方法
        1. 情報セキュリティに組織的に取り組んだ経験は必要ありません。本ガイドラインにより、事業の特徴に応じ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。
        2. 「第１部 経営編」は、全ての経営者に読んでいただきたい内容です。まずはご一読ください。「第２部 実践編」は、あなたの組織にあったSTEP から進めてください。
        3. Step1 まず始める
           1. 情報セキュリティ5か条
        4. Step2 現状を知り改善する
           1. 情報セキュリティ自社診断
           2. 情報セキュリティポリシー基本方針策定
           3. 「 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
           4. 「 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
        5. Step3 本格的に取り組む
           1. 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
           2. 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
           3. 委託時に必要となる対策を検討するとともに、点検や改善に努める
        6. Step4 改善を続ける
           1. 「５. より強固にするための方策」（P.30）を参照して、自社に必要な対策を追加実施
           2. 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
     5. 第 1部 経営者編
        1. 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. (1) 金銭の喪失
           2. (2) 顧客の喪失
           3. (3) 業務 の停滞
           4. (4) 従業員 への影響
        2. 2.経営者が負う責任
           1. (1) 経営者などに問われる法的責任

・個人情報

・他社から預かった秘密情報

・自社の秘密情報

・株価に影響を与える可能性のある未公開内部情報

【表２】情報管理が不適切な場合の処罰など

* + - * 1. (2) 関係者や社会に対する責任

・営業停止、売上高の減少、企業イメージの低下などで、自社に損害をもたらずだけでなく、取引先に対する信頼関係の喪失、業界やサービス全体のイメージダウン

法令順守・顧客・取引先・従業員

* + - * 1. コラム

個人情報保護法

不正競争防止法

* + - 1. 3.経営者は何をやらなければならないのか
         1. サイバーセキュリティ経営ガイドライン【2015年12月METI・IPA】の内容を中小企業向けに編集
         2. (1)認識すべき「３原則」

原則１ 情報セキュリティ対策は経営者のリーダシップのもとで進める

さまざまな脅威がもたらすリスクに対する対策は、経営者が判断して意思決定し、自社の事業に見合った情報セキュリティ対策を実施します。

セキュリティ対策をしないことによる損失、対策に要する投資、ITの利活用を推進することによる利益を勘案して判断

セキュリティ対策をしないことによる損失＞対策に要する投資

ITの利活用を推進することによる利益＞対策に要する投資

コラム

情報セキュリティガバナンス

情報セキュリティガバナンスの概念（METI/経済産業省）

ドキュメントを参照: [secgov-concept.html](https://www.meti.go.jp/policy/netsecurity/secgov-concept.html)

原則２ 委託先における情報セキュリティ対策まで考慮する

自社同様に十分な注意を払い、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

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

普段から自社の情報セキュリティ対策や、事故が起きたときの対応について、関係者に明確に説明できるように経営者自身が理解し、整理しておくことが重要です。

* + - * 1. (2)実行すべき「重要７項目の取組」

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

「当社は中小企業の情報セキュリティ対策ガイドラインに基づき情報セキュリティ対策を実践する。」「当社は顧客情報の流出防止を徹底することから情報セキュリティ対策を開始する。」

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

万が一事故（インシデント7）が起きてしまった場合、被害を最小限に止めるために、あらかじめ準備することも含みます。

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

事業を行う上で見込まれる情報セキュリティのリスクを把握した上で、必要十分な対策を検討させます。検討した対策ごとに予算を与え、担当者を任命し、実行を指示します。

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

最初から最適な形で実現することはどんな会社でも難しいもの。また情報技術は進化が早く、加えて脅威も変化します。

取組５ 緊急時の対応や復旧のための体制を整備する

被害原因を速やかに追究して被害の拡大を防ぐ体制を作るとともに、的確な復旧手順をあらかじめ作成しておくことにより、緊急時に適切な指示を出すことができます。

整備後には予定どおりに機能するかを確認するため、被害発生を想定した模擬訓練を行うと、意識づけや適切な対応のために効果的です。

経営者のふるまいについても、あらかじめ想定しておけば、冷静で的確な対応が可能になります。

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

契約書に情報セキュリティに関する相手先の責任や実施すべき対策を明記し、合意する

利用規約やサービスに付随する情報セキュリティ対策等を確認したうえで選定するよう担当者に指示する

取組７ 情報セキュリティに関する最新動向を収集する

情報セキュリティに関する最新動向を発信している公的機関8などを把握しておき、常時参照することで、新たな脅威に備えるようにします。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有します。

* + - * 1. コラム

「SECURITY ACTION」一つ星を宣言しよう！

* + 1. 第 2部 実践編
       1. 1.実践編の進め方
          1. 【表３】重要７項目の取り組みと実践編の対応表
       2. 2.できるところから始める
          1. (1)情報セキュリティ５か条

①OS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！

* + - 1. 3.組織的な取り組みを開始する
         1. (1)情報セキュリティ基本方針の作成と周知
         2. (2)実施状況の把握

「５分でできる！情報セキュリティ自社診断」（付録３）を利用して、情報セキュリティ対策が、どれくらい実施できているかを把握します。

自社診断は、表４に示す25項目の設問に答えるだけで情報セキュリティ対策の実施状況が把握できるツールです。

【表４】自社診断のための25項目

* + - * 1. (3)対策の決定と周知
        2. コラム

「SECURITY ACTION」二つ星へステップアップ！

* + - 1. 4.本格的に取り組む
         1. (1)管理体制の構築

①責任分担と連絡体制の整備

【表５】情報セキュリティ管理のための役割と責任分担（例）

②緊急時対応体制の整備

* + - * 1. (2)IT利活用方針と情報セキュリティの予算化
        2. (3)情報セキュリティ規程の作成

①対応すべきリスクの特定

考慮点

関連する業務や情報に係る外部状況（法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など）

内部状況（経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など）

②対策の決定

いつ事故が起きてもおかしくない、あるいは事故が起きると大きな被害になるなど、リスクが大きなものを優先して対策を実施し、事故が起きる可能性が小さいか、発生しても被害が軽微であるなど、リスクが小さなものについては、現状のままにするなど、合理的に対応します。

③規程の作成

【表７】情報セキュリティ関連規程（サンプル）の概要

* + - * 1. (4)委託時の対策

コラム

委託と受託

* + - * 1. (5)点検と改善

その１）「情報セキュリティ５か条」や「５分でできる！情報セキュリティ自社診断」に基づく点検

その２）策定した情報セキュリティ対策に関するルール・規程に基づく点検

コラム

情報セキュリティ点検の実施例

* + - 1. 5.より強固にするための方策
         1. 構成

(1)情報収集と共有

情報セキュリティに関する情報収集の方法と情報共有の枠組みについて説明します。

(2)ウェブサイトの情報セキュリティ

ウェブサイトを安全に構築し、運用するためのポイントを説明します。

(3)クラウドサービスの情報セキュリティ

クラウドサービスを安全に利用するためのポイントを説明します。

(4)セキュリティサービス例と活用

情報セキュリティに関する外部サービスを説明します。

(5)技術的対策例と活用

ITを活用する際の技術的対策について説明します。

(6)詳細リスク分析の実施方法

「リスク分析シート」（付録７）を活用した詳細リスク分析の実施方法を説明します。

* + - * 1. (1)情報収集と共有

①情報収集の方法

②情報共有の枠組み

参考情報

（情報収集の方法）

■ここからセキュリティ！

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

ドキュメントを参照: [kokokara](https://www.ipa.go.jp/security/kokokara/)

■ IPA セキュリティセンター

https://www.ipa.go.jp/security/

ドキュメントを参照: [security](https://www.ipa.go.jp/security/)

■ IPA 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/

ドキュメントを参照: [security](https://www.ipa.go.jp/security/)

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

ドキュメントを参照: [icat.html](https://www.ipa.go.jp/security/vuln/icat.html)

■ JPCERT/CC

https://www.jpcert.or.jp/

ドキュメントを参照: [www.jpcert.or.jp](https://www.jpcert.or.jp/)

■警察庁 @police

https://www.npa.go.jp/cyberpolice/

ドキュメントを参照: [cyberpolice](https://www.npa.go.jp/cyberpolice/)

（情報共有の枠組み）

■日本シーサート協議会

https://www.nca.gr.jp/

ドキュメントを参照: [www.nca.gr.jp](https://www.nca.gr.jp/)

* + - * 1. (2)ウェブサイトの情報セキュリティ

①ウェブサイト運営形態の検討

【表８】運営形態ごとの特徴

②ウェブサイトの構築

③ウェブサイトの運営

参考情報

■ウェブサイト開設等における運営形態の選定方法に関する手引き（IPA）

https://www.ipa.go.jp/security/technicalwatch/20180530.html

ドキュメントを参照: [20180530.html](https://www.ipa.go.jp/security/technicalwatch/20180530.html)

■安全なウェブサイトの作り方（IPA）

https://www.ipa.go.jp/security/vuln/websecurity.html

ドキュメントを参照: [websecurity.html](https://www.ipa.go.jp/security/vuln/websecurity.html)

■安全なウェブサイトの運用管理に向けての20 ヶ条（IPA）

https://www.ipa.go.jp/security/vuln/websitecheck.html

ドキュメントを参照: [websitecheck.html](https://www.ipa.go.jp/security/vuln/websitecheck.html)

* + - * 1. (3)クラウドサービスの情報セキュリティ

概要

インターネットの普及と技術の進展により、情報システムを所有せず、インターネット上で提供されるサービスとして利用することが増えています。

必要なときに利用するだけという“クラウド化”によって、所有することで発生していた費用や手間が削減され、柔軟な運用が可能です。

その一方で、情報システムの一部が、サービスを提供する事業者の管理下に置かれることになるため、所有とは異なる観点で情報セキュリティ対策を配慮する必要があります。

①クラウドサービスの選定

②クラウドサービスの運用

③クラウドサービスのセキュリティ対策

【表９】中小企業のためのクラウドサービス安全利用のための15項目

コラム

クラウドサービス選択時に参考となる制度等

IT活用を支援する情報処理支援機関

中小企業者等の生産性向上に資するIT ツールや中小企業のIT 活用を支援するITベンダーを法令に基づいて認定し、中小企業者がIT ツール選定するために必要となる情報を開示しています。

●認定情報処理支援機関（スマートSMEサポーター）制度（中小企業庁）

https://smartsme.go.jp/

ドキュメントを参照: [smartsme.go.jp](https://smartsme.go.jp/)

中小企業が使いやすいITツールの開発促進や中小企業のIT 導入を通じた生産性向上を図ります。認定を受けたITベンダーの情報セキュリティ対策の実施状況を確認できます。

* + - * 1. (4)情報セキュリティサービスの活用

概要

外部の情報セキュリティサービスを利用することで、より強固で有効な対策を実施することができます。

昨今では、様々なサービスが提供されています。情報セキュリティ人材が社内に不足している場合や、情報セキュリティの向上に有用です。

①情報セキュリティコンサルテーション

②情報セキュリティ教育サービス

③情報セキュリティ監査サービス

④脆弱性診断サービス

⑤デジタルフォレンジックサービス

⑥セキュリティ監視・運用サービス

コラム

情報セキュリティサービス基準審査登録制度

●情報セキュリティサービス基準適合サービスリスト

https://www.ipa.go.jp/security/it-service/service\_list.html

ドキュメントを参照: [service\_list.html](https://www.ipa.go.jp/security/it-service/service_list.html)

* + - * 1. (5)技術的対策例と活用

①ネットワーク脅威対策

②コンテンツセキュリティ対策

③アクセス管理

④システムセキュリティ管理

⑤暗号化

⑥データの破棄

* + - * 1. (6)詳細リスク分析の実施方法

手順1 情報資産の洗い出し

●情報資産管理台帳の作成

●情報資産ごとの機密性・完全性・可用性の評価

●機密性・完全性・可用性の評価値から重要度を算定

【表10】情報資産の機密性・完全性・可用性に基づく重要度の定義

【表11】情報資産の重要度判断基準

付録の利用方法（手順1）

手順2 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

リスク値 ＝ 重要度 × 被害発生可能性

【表13】リスク値の算定基準

【表14】脅威例に応じたリスクのレベル

【表15】被害発生可能性　換算表

付録の利用方法（手順2）

手順3 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決める

①リスクを低減する

②リスクを保有する

③リスクを回避する

④リスクを移転する

付録の利用方法（手順3）

コラム

「情報セキュリティに関連した保険商品」とは

リスク分析の手法あれこれ

①ベースラインアプローチ

②非形式的アプローチ

③詳細リスク分析

④組合せアプローチ

* + 1. 情報セキュリティに関する参考情報
       1. ［1］ サイバーセキュリティ経営ガイドライン [Ver.2.0]（経済産業省/IPA）
          1. http://www.meti.go.jp/policy/netsecurity/mng\_guide.html

ドキュメントを参照: [mng\_guide.html](http://www.meti.go.jp/policy/netsecurity/mng_guide.html)

* + - 1. ［2］組織における内部不正防止ガイドライン（IPA）
         1. https://www.ipa.go.jp/security/fy24/reports/insider/

ドキュメントを参照: [insider](https://www.ipa.go.jp/security/fy24/reports/insider/)

* + - 1. ［3］脆弱性対策情報ポータルサイト（IPA/JPCERTコーディネーションセンター）
         1. https://jvn.jp/

ドキュメントを参照: [jvn.jp](https://jvn.jp/)

* + - 1. ［4］ JISQ 27001（ISO/IEC 27001）情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項
      2. ［5］ JISQ 27002（ISO/IEC 27002）情報技術－セキュリティ技術－情報セキュリティ管理策の実践のための規範
      3. ［6］ JISQ27017（ISO/IEC 27017）　情報技術－セキュリティ技術－JISQ 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範
      4. ［7］ 情報セキュリティマネジメント試験
         1. https://www.jitec.ipa.go.jp/1\_11seido/sg.html

ドキュメントを参照: [sg.html](https://www.jitec.ipa.go.jp/1_11seido/sg.html)

* + 1. 本書で用いてる語の説明
       1. インシデント
       2. （情報の）可用性
       3. （情報の）完全性
       4. （情報の）機密性
       5. クラウドサービス
       6. 個人情報
       7. サイバーセキュリティ
       8. 【×】CSIRT（ シーサート、Computer Security Incident Response Team）
       9. 情報セキュリティ
       10. 【×】情報セキュリティインシデント
       11. 情報セキュリティに関連した保険商品
       12. 情報セキュリティポリシー
       13. 情報セキュリティマネジメントサイクル
       14. ソーシャルエンジニアリング
       15. ランサムウェア
    2. おわりに
       1. 第2版の公開から約2年が経過し、この度第3版をお届けすることとなりました。
       2. この第3版では、「サイバーセキュリティ経営ガイドライン」（経済産業省、IPA）の改訂や、中小企業を取り巻く環境の変化（クラウドサービスなど外部サービスの利用の増加、ウェブサイトの改ざん被害の増加）へ対応した内容追加を行うとともに、利用者の皆様からの意見も踏まえ、より解りやすく、より進めやすくなるよう、全面的な見直しを行いました。
       3. 中小企業は、情報セキュリティ対策に十分な経営資源を割り当てることができないという不利を抱える一方で、経営者から「従業員の顔が見える」という有利な条件を備えています。つまり、経営者が直接担当者や従業員に対策を指示することができ、対策の結果についても直接報告を受けることができるなど、大企業に比べて迅速に対応ができるという有利な条件を備えています。
       4. そうしたなかで一歩一歩情報セキュリティ対策をすすめていくために、本ガイドラインをご活用いただければ幸いです。
  1. 付録1：「情報セキュリティ５か条」
     1. 情報セキュリティ5か条（全2ページ、726KB）

ドキュメントを参照: [000055516.pdf](https://www.ipa.go.jp/files/000055516.pdf)

* + - 1. こんな情報があるはず！
         1. 従業員のマイナンバー、住所、給与明細
         2. お客様や取引先の連絡先一覧
         3. 取引先ごとの仕切り額や取引実績
         4. 新製品の設計図などの開発情報
         5. 組織の経理情報
         6. 取引先から取扱注意と言われた情報
      2. 漏れたら大変！こんなダメージが！
         1. 被害者への損害賠償などの支払い
         2. 取引停止、顧客の他社への流出
         3. ネットの遮断などによる生産効率のダウン
         4. 従業員の士気低下
      3. まずは始めてみよう
         1. ①OSやソフトウェアは常に最新の状態に使用！

OSやソフトウェアのセキュリティ上の問題点を放置していると、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やソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

* + - * 1. 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。

* + - * 1. 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窃取したID・パスワードが流用されることで、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。

* + - * 1. ④共有設定を見直そう！

データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため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。クラウドサービスや機器は必要な人にのみ共有されるよう設定しましょう。

* + - * 1. 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。

* 1. 付録2：「情報セキュリティ基本方針（サンプル）
     1. 情報セキュリティ基本方針（サンプル）（全1ページ、35KB）

ドキュメントを参照: [000072146.docx](https://www.ipa.go.jp/files/000072146.docx)

* 1. 付録3：「５分でできる！情報セキュリティ自社診断」
     1. 5分でできる！情報セキュリティ自社診断（全8ページ、3.9MB）

ドキュメントを参照: [000055848.pdf](https://www.ipa.go.jp/files/000055848.pdf)

* + - 1. Part1 基本的対策
         1. 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. 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. 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. 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. 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？
      2. Part2 従業員としての対策
         1. 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？
         2. 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？
         3. 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？
         4. 9.無線LAN を利用する時は強固な暗号化を必ず利用するなどのように、無線LAN を安全に使うための対策をしていますか？
         5. 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？
         6. 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？
         7. 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？
         8. 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？
         9. 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？
         10. 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？
         11. 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？
         12. 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？
         13. 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？
      3. Part3 組織としての対策
         1. 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？
         2. 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？
         3. 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？
         4. 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？
         5. 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？
         6. 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？
         7. 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？
      4. 情報セキュリティ対策支援サイト
         1. https://security-shien.ipa.go.jp/

ドキュメントを参照: [security-shien.ipa.go.jp](https://security-shien.ipa.go.jp/)

* + - 1. 自社診断の後は社内ルールの周知に取り組もう！
         1. 情報セキュリティハンドブック（ひな形）

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - 1. 情報セキュリティ対策の取り組みを外部にアピールしよう！
         1. SECURITY ACTION 二つ星

https://www.ipa.go.jp/security/security-action/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/security-action/index.html)

* 1. 付録4：「情報セキュリティハンドブック（ひな形）
     1. 情報セキュリティハンドブック（ひな形）（全11ページ、212KB）

ドキュメントを参照: [000055529.pptx](https://www.ipa.go.jp/files/000055529.pptx)

* + - 1. １ 全社基本ルール
         1. OSとソフトウェアのアップデート
         2. ウイルス対策ソフトの導入
         3. パスワードの管理
         4. アクセス制限
         5. セキュリティに対する注意

独立行政法人情報処理推進機構（(略称：IPA）　重要なセキュリティ情報

http://www.ipa.go.jp/security/index.html

ドキュメントを参照: [index.html](http://www.ipa.go.jp/security/index.html)

JVN （Japan Vulnerability Notes）

http://jvn.jp/index.html

ドキュメントを参照: [index.html](http://jvn.jp/index.html)

一般社団法人 JPCERT コーディネーションセンター(略称：JPCERT/CC)

https://www.jpcert.or.jp/

ドキュメントを参照: [www.jpcert.or.jp](https://www.jpcert.or.jp/)

* + - 1. ２ 仕事中のルール
         1. 電子メールの利用
         2. インターネットの利用
         3. データのバックアップ
         4. クリアデスク・クリアスクリーン
         5. 重要情報の持ち出し
         6. 入退室
         7. 電子媒体・書類の廃棄
      2. ３ 全社共通のルール
         1. 私有情報機器の利用
         2. クラウドサービスの利用
      3. ３ 従業員のみなさんへ
         1. 従業員の守秘義務
         2. 事故が起きてしまったら
  1. 付録5：「情報セキュリティ関連規程（サンプル）
     1. 情報セキュリティ関連規程（サンプル）（全51ページ、179KB）

ドキュメントを参照: [000055794.docx](https://www.ipa.go.jp/files/000055794.docx)

* + 1. 1.組織的対策
       1. 1.情報セキュリティのための組織
       2. 2.情報セキュリティ取組みの監査・点検/点検
       3. 3.情報セキュリティに関する情報共有
    2. 2.人的対策
       1. 1.雇用条件
       2. 2.従業員の責務
       3. 3.雇用の終了
       4. 4.情報セキュリティ教育
       5. 5.人材育成
    3. 3.情報資産管理
       1. 1.情報資産の管理
          1. 1.1情報資産の特定と機密性の評価
          2. 1.2情報資産の分類の表示
          3. 1.3情報資産の管理責任者
          4. 1.4情報資産の利用者
       2. 2.情報資産の社外持ち出し
       3. 3.媒体の処分
          1. 3.1媒体の廃棄
          2. 3.2媒体の再利用
       4. 4.バックアップ
          1. 4.1バックアップ取得対象
          2. 4.2バックアップ媒体の取り扱い
          3. 4.3クラウドサービスを利用したバックアップ
    4. 4.アクセス制御及び認証
       1. 1.アクセス制御方針
       2. 2.利用者の認証
       3. 3.利用者アカウントの登録
       4. 4.利用者アカウントの管理
       5. 5.パスワードの設定
       6. 6.従業員以外の者に対する利用者アカウントの発行
       7. 7.機器の識別による認証
       8. 8.端末のタイムアウト機能
       9. 9.標準設定等
          1. 9.1アクセス制御対象情報システム及びアクセス制御方法
          2. 9.2利用者認証方法
          3. 9.3利用者アカウント・パスワードの条件
          4. 9.4機器の認証方法
    5. 5.物理的対策
       1. 1.セキュリティ領域の設定
       2. 2.関連設備の管理
       3. 3.セキュリティ領域内注意事項
       4. 4.搬入物の受け渡し
    6. 6.IT機器利用
       1. 1.ソフトウェアの利用
          1. 1.1標準ソフトウェア
          2. 1.2ソフトウェアの利用制限
          3. 1.3ソフトウェアのアップデート
          4. 1.4ウイルス対策ソフトウェアの利用

1.4.1ウイルス検知

1.4.2ウイルス対策ソフト定義ファイルの更新

1.4.3社外機器のLAN接続

* + - * 1. 1.5ウイルス対策の啓発
      1. 2.ＩＴ機器の利用
      2. 3.クリアデスク・クリアスクリーン
         1. 3.1クリアデスク
         2. 3.2クリアスクリーン
      3. 4.インターネットの利用
         1. 4.1ウェブ閲覧
         2. 4.2オンラインサービス

＜インターネットバンキング・電子決済＞

＜オンラインストレージ＞

* + - * 1. 4.3 SNSの個人利用
        2. 4.4電子メールの利用

＜誤送信防止＞

＜メールアドレス漏えい防止＞

＜傍受による漏えい防止＞

＜添付ファイル暗号化の方法＞

＜クラウド型メールの利用＞

＜禁止事項＞

* + - * 1. 4.5ウイルス感染の防止
      1. 5.私有ＩＴ機器・電子媒体の利用
         1. 5.1利用開始時
         2. 5.2利用期間中

5.2.1社内での利用

* + - * 1. 5.3利用終了時
      1. 6.標準等
         1. 6.1標準ソフトウェア
         2. 6.2ソフトウェアのアップデート方法
         3. 6.3ウイルス対策ソフトウェアの定義ファイルの更新方法
    1. 7.IT基盤運用管理
       1. 1.管理体制
       2. 2.ＩＴ基盤の情報セキュリティ対策
          1. 2.1サーバー機器の情報セキュリティ要件
          2. 2.2サーバー機器に導入するソフトウェア
          3. 2.3ネットワーク機器の情報セキュリティ要件
       3. 3.ＩＴ基盤の運用
       4. 4.クラウドサービスの導入
       5. 5.脅威や攻撃に関する情報の収集
       6. 6.廃棄・返却・譲渡
       7. 7.ＩＴ基盤標準
          1. 7.1サーバー機器情報セキュリティ要件
          2. 7.2ＩＴ基盤標準ソフトウェア
          3. 7.3標準ネットワーク機器
          4. 7.4ネットワーク機器情報セキュリティ要件
          5. 7.5クラウドサービス情報セキュリティ対策評価基準
    2. 8.システム開発及び保守
       1. 1.新規システム開発・改修
       2. 2.脆弱性への対処
       3. 3.情報システムの開発環境
       4. 4.情報システムの保守
       5. 5.情報システムの変更
    3. 9.委託管理
       1. 1.委託先評価基準
       2. 2.委託先の選定
       3. 3.委託契約の締結
       4. 4.委託先の評価
       5. 5.再委託
       6. 9-1 業務委託契約に係る機密保持条項
       7. 9-2　委託先情報セキュリティ対策状況確認リスト
    4. 10.情報セキュリティインシデント対応ならびに事業継続管理
       1. 1.対応体制
       2. 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. 3.インシデントの連絡及び報告
       4. 4.対応手順
          1. 4.1漏えい・流出発生時の対応
          2. 4.2改ざん・消失・破壊・サービス停止発生時の対応
          3. 4.3ウイルス感染時の初期対応
          4. 4.5届出及び相談
       5. 5.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
          1. 5.1想定される情報セキュリティインシデント
          2. 5.2復旧責任者及び関連連絡先
          3. 5.3事業継続計画
    5. 11.個人番号及び特定個人情報の取り扱い
       1. 個人番号及び特定個人情報の適正な取り扱いに関する基本方針
       2. 1.関係法令・ガイドライン等の遵守
       3. 2.利用目的
       4. 3.安全管理措置に関する事項
       5. 4.委託の取り扱い
       6. 5.継続的改善
       7. 6.特定個人情報等の開示
       8. 個人番号及び特定個人情報取扱規程
  1. 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」
     1. クラウドサービス安全利用の手引き（全8ページ、2.8MB）

ドキュメントを参照: [000072150.pdf](https://www.ipa.go.jp/files/000072150.pdf)

* + 1. クラウドサービスとは？
    2. クラウドサービスを利用する前に確認しましょう！
    3. 利用者がやるべきことを知っておきましょう！
    4. クラウドサービス安全利用チェックシート
       1. Ⅰ．選択するときのポイント
       2. Ⅱ．運用するときのポイント
       3. Ⅲ．セキュリティ管理のポイント
    5. 解説編
       1. Ⅰ．選択するときのポイント
          1. チェックシートNo.1:どの業務で利用するか明確にする
          2. チェックシートNo.2:クラウドサービスの種類を選ぶ
          3. チェックシートNo.3:取扱う情報の重要度を確認する
          4. チェックシートNo.4:セキュリティのルールと矛盾しないようにする
          5. チェックシートNo.5:クラウド事業者の信頼性を確認する
          6. チェックシートNo.6:クラウドサービスの安全・信頼性を確認する
          7. ☛クラウドサービス選択時に参考となる制度等
       2. Ⅱ．運用するときのポイント
          1. チェックシートNo.7:管理担当者を決める
          2. チェックシートNo.8:利用者の範囲を決める
          3. チェックシートNo.9:利用者の認証を厳格に行う
          4. チェックシートNo.10:バックアップに責任を持つ
       3. Ⅲ．セキュリティ管理のポイント
          1. チェックシートNo.11:付帯するセキュリティ対策を確認する
          2. チェックシートNo.12:利用者サポートの体制を確認する
          3. チェックシートNo.13:利用終了時のデータを確保する
          4. チェックシートNo.14:適用法令や契約条件を確認する
          5. チェックシートNo.15:データ保存先の地理的所在地を確認する
    6. 情報セキュリティ対策に役立つ情報
       1. クラウドサービス利用のための情報セキュリティマネジメントガイドライン（経済産業省）
          1. クラウドサービスの利用にかかわるリスク対応のためにJIS Q 27002（実践のための規範）から適切な管理策を選択し，導入するための助言とその最適な実施のための手引を提供している
          2. http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf

ドキュメントを参照: [cloudsec2013fy.pdf](http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf)

* + - 1. クラウドセキュリティガイドライン活用ガイドブック（経済産業省）
         1. 実際に発生した事故や、事業者が抱える様々なセキュリティ上の課題をベースに、ITサービスとしてのクラウドサービスに関するリスクと対策を、事業者と利用者のそれぞれについて解説している
         2. http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf

ドキュメントを参照: [cloudseckatsuyou2013fy.pdf](http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf)

* + - 1. クラウドサービスの安全・信頼性に係る情報開示指針（総務省）
         1. クラウドサービスの安全・信頼性を向上させることを目的として、利用者のサービス選定における情報収集の負担を軽減する観点から、クラウドサービス事業者によるクラウドサービスに係る情報開示のあり方を示した指針
         2. http://www.soumu.go.jp/main\_content/000477838.pdf

ドキュメントを参照: [000477838.pdf](http://www.soumu.go.jp/main_content/000477838.pdf)

* + - 1. SECURITY ACTION セキュリティ対策自己宣言（独立行政法人情報処理推進機構）
         1. 中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度で、自社の状況に応じて「一つ星」と「二つ星」の2段階の取組み目標を用意している
         2. https://www.ipa.go.jp/security/security-action/

ドキュメントを参照: [security-action](https://www.ipa.go.jp/security/security-action/)

* 1. 付録7：「リスク分析シート」
     1. リスク分析シート（全7シート、99KB）

ドキュメントを参照: [000055518.xlsx](https://www.ipa.go.jp/files/000055518.xlsx)

* + 1. 利用方法
    2. 台帳記入例
    3. 重要度定義
    4. 情報資産管理台帳
    5. 脅威の状況
    6. 対策状況チェック
    7. 診断結果

1. 【旧版】中小企業の情報セキュリティ対策ガイドライン（第2.1版）

ドキュメントを参照: [000055520.pdf](http://www.ipa.go.jp/files/000055520.pdf)

* 1. 本文
     1. 経営者の皆様へ
        1. 情報セキュリティ対策は、経営に大きな影響を与えます！
        2. 経営者が自ら動かなければ、法的・道義的責任を問われます！
        3. 組織として対策するために、担当者への指示が必要です！
     2. 対象組織と想定する読者
        1. 経営者層・システム管理者層
        2. 対象組織
           1. 本ガイドラインは、業種を問わず中小企業及び小規模事業者（法人のほか、個人事業 主や各種団体も含む） 1を対象として作成されています。
        3. 想定読者
           1. 組織の経営者と、経営者の指示のもとで重要な情報を管理する方を読者と想定して います。
     3. 全体解説
        1. （1）本ガイドラインの構成
           1. 本編２部と付録より構成
        2. （2）本ガイドラインの使い方
           1. ①経営者の方
           2. ②経営者の指示のもとで重要な情報を管理する方
           3. 【図3】情報セキュリティ対策の進め方

Step1 まず始める

情報セキュリティ5か条

Step2 現状を知り改善する

情報セキュリティ自社診断

Step3 本格的に取り組む

情報セキュリティポリシーの策定

Step4 改善を続ける

情報セキュリティ対策のさらなる改善に向けて

* + 1. 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. (1) 金銭の喪失

【表2】最近のサイバー攻撃等による情報漏えい等の経済的損失例

情報漏えい

教育サービス事業者で顧客の個人情報が3504件が漏えい（2014年）

システム開発・運用を行っている委託先の再委託先社員による不正取得と名簿の売却

株式を公開している雑貨卸事業者でインターネット上の株主向けサービスに登録された株主の個人情報6187件（他社の株主個人情報含め12014件）が漏えいした（2015年）

運営委託先サービスサイトへの不正アクセス

航空会社の顧客の個人情報4131件が漏えいした（2014年）

菓子食品製造事業者で個人情報29999件が漏えいした（2015年）

国内半導体製造事業者の技術jに関する機密情報が韓国の同業者に漏えい（2014年）

メガネ販売事業者でオンラインショップ顧客のクレジットカード情報2059件の漏えい（2013年）

ウイルス感染

米国の病院で院内ネットワークで共有する電子カルテシステムがウイルスによる攻撃により動作しなくなり診療不能に（2016年）

ランサムウェアに感染し、ファイルが暗号化されたため

ウェブサイト改ざん

観光バス事業者のホームページが改ざんされ閲覧するとウイルスに感染する恐れ（2014年）

* + - * 1. (2) 顧客の喪失
        2. (3) 業務 の喪失
        3. (4) 従業員 への影響
      1. 経営者が負う責任
         1. (1) 経営者などに問われる法的責任

・個人情報

・他社から預かった秘密情報

・自社の秘密情報

・株価に影響を与える可能性のある未公開内部情報

* + - * 1. (2) 関係者や社会に対する責任

・営業停止、売上高の減少、企業イメージの低下などで、自社に損害をもたらずだけでなく、取引先に対する信頼関係の喪失、業界やサービス全体のイメージダウン

法令順守・顧客・取引先・従業員

* + - 1. 経営者は何をすればよいか
         1. サイバーセキュリティ経営ガイドライン【2015年12月METI・IPA】の内容を中小企業向けに編集

ドキュメントを参照: [20151228002-2.pdf](http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf)

* + - * 1. 経営者が認識する必要な「３原則」

原則１ 情報セキュリティ対策は経営者のリーダシップのもとで進める

さまざまな脅威がもたらすリスクに対する対策は、経営者が判断して意思決定し、自社の事業に見合った情報セキュリティ対策を実施します。

セキュリティ対策をしないことによる損失、対策に要する投資、ITの利活用を推進することによる利益を勘案して判断

セキュリティ対策をしないことによる損失＞対策に要する投資

ITの利活用を推進することによる利益＞対策に要する投資

原則２ 委託先における情報セキュリティ対策まで考慮する

自社同様に十分な注意を払い、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

原則３ 情報セキュリティに関する関係者とのコミュニケーションは、どんなときにも怠らない

普段から自社の情報セキュリティ対策や、事故が起きたときの対応について、関係者に明確に説明できるように経営者自身が理解し、整理しておくことが重要です。

* + - * 1. 企業が重要 として実施する「重要 7項目の取組」

取組１ 情報 セキュリティ に関するリスクを認識し組織全体での対応方針を定める

「当社は中小企業の情報セキュリティ対策ガイドラインに基づき情報セキュリティ対策を実践する。」「当社は顧客情報の流出防止を徹底することから情報セキュリティ対策を開始する。」

取組２ 情報セキュリティ対策を行うための資源（予約、人材など）を確保する

万が一事故（インシデント7）が起きてしまった場合、被害を最小限に止めるために、あらかじめ準備することも含みます。

取組３ 情報セキュリティのリスクを把握し、どこまで情報セキュリティ対策を行うのかを定めたうえで担当者に実行させる

事業を行う上で見込まれる情報セキュリティのリスクを把握した上で、必要十分な対策を検討させます。検討した対策ごとに予算を与え、担当者を任命し、実行を指示します。

取組４ 情報セキュリティ対策に関する定期的な見直しを行う

最初から最適な形で実現することはどんな会社でも難しいもの。また情報技術は進化が早く、加えて脅威も変化します。

取組５ 業務委託する場合や外部ITシステムやサービスを利用する場合は、自社で必要と考える情報セキュリティ対策が担保されるようにする

契約書に情報セキュリティに関する相手先の責任や実施すべき対策を明記し、合意する

利用規約やサービスに付随する情報セキュリティ対策等を確認したうえで選定するよう担当者に指示する

取組６ 情報セキュリティに関する最新動向を収集する

情報セキュリティに関する最新動向を発信している公的機関8などを把握しておき、常時参照することで、新たな脅威に備えるようにします。また、知り合いやコミュニティへの参加で情報交換を積極的に行い、得られた情報について、業界団体、委託先などと共有します。

取組７ 緊急時の社内外の連絡先や被害発生時に行うべき内容について準備しておく

万が一のインシデントに備えて、緊急時の連絡体制を整備します。、経営者の対応についても、あらかじめ決めておけば、冷静で的確な対応が可能になります。

* + 1. 第 2部 管理実践編
       1. 情報セキュリティ管理の進め方
          1. 【図5】ガイドラインの使用方法
       2. 情報セキュリティ５か条
          1. 【表4】情報セキュリティ5か条
          2. OSやソフトウェアは常に最新の状態にしよう！
          3. ウイルス対策ソフトを導入しよう！
          4. パスワードを強化しよう！
          5. 共有設定を見直そう！
          6. 脅威や攻撃の手口を知ろう！
       3. 5分でできる！情報セキュリティ自社診断
          1. Part1 基本的対策
          2. Part2 従業員としての対策
          3. Part3 組織としての対策
       4. 情報セキュリティポリシーの策定
          1. （1）基本的な考え方

① 自社に適合したポリシーを策定

【図6】セキュリティポリシー文書構成

② 情報セキュリティリスクの大きなものから重点的に対策を実施

【図7】リスクの「保有」の考え方

* + - * 1. （2） ポリシー策定までの流れ

【図8】情報セキュリティポリシー策定までの流れ

手順１ 情報資産台帳を作成する

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

機密性、完全性、可用性それぞれの評価値11を記入します（表6）。

機密性・完全性・可用性の評価値から重要度を判定します（表7）。

【表6】情報資産の機密性・完全性・可用性の評価基準

機密性・完全性・可用性 重要度

【表7】情報資産の重要度判断基準

付録の利用方法（手順１）

手順2 リスク値の算定

リスク値=重要度（機密性ｘ完全性ｘ機密性）ｘ被害発生可能性の合計（脅威の起きる可能性ｘ脆弱性の大きさ）

【表9】リスク値の算定基準

【表10】脅威例に応じたリスクのレベル

付録の利用方法（手順2）

手順3 情報セキュリティ対策を決定（対策を決める）

ア）リスクを低減する

　自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げます。

イ）リスクを保有する

　事故が発生しても許容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持します。

ウ）リスクを回避する

　仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくします。

リスクを許容する

付録の利用方法（ツールA）

手順4 情報セキュリティポリシーを策定（対策をルールにする）

付録の利用方法（手順4）

【表11】情報セキュリティポリシーサンプル

1 組織的対策

2 人的対策

3 情報資産管理

4 マイナンバー対応

5 アクセス制御及び認証

6 物理的対策

7 IT機器利用

8 IT基盤運用管理

9 システムの開発及び保守

社内でシステム開発を行う場合

10 委託管理

業務委託を行う場合

11 情報セキュリティインシデント対応及び事業継続管理

12 社内体制図

従業員数２名以上

13 委託契約書サンプル

委託先と秘密情報や個人情報等の重要な情報の授受が発生する場合

* + - * 1. （3）委託時の情報セキュリティ対策
        2. （4）情報セキュリティ対策の実行

① 通常時の役割

経営者

管理者層

一般従業員

② 緊急時の対応

※しおり

① 緊急時の指揮命令と対応の優先順位の決定

② インシデントへの対応（インシデントレスポンス）

③ インシデントの影響と被害の分析

④ 情報収集と自社に必要な情報の選別

⑤ 社内関係者への連絡と周知

⑥ 外部関係機関との連絡

* + - * 1. （5）チェックと改善

① チェックの方法

② 改善の方法

* + - 1. 情報セキュリティ対策のさらなる改善に向けて
         1. （1）情報セキュリティマネジメントサイクルによる継続的改善

　ISO/IEC27001 が定めているマネジメントシステム（管理のしくみ）の考え方の基本は、Plan（計画）、Do（実行）、Check（チェック）、Act（改善）の４段階の活動（PDCA サイクル13）を順に繰り返すことを通じて改善していくことにあります。情報セキュリティ対策で見ると、それぞれ次の活動に相当します。

Plan：情報セキュリティ対策の計画立案または見直し

Do：情報セキュリティ対策の実践

Check：監査・点検による活動の有効性確認と経営者による必要な改善箇所の決定

Act：改善の実施

* + - * 1. （2）情報セキュリティ対策に関する標準規格

付録３で示す対策は、中小企業でも取り組みやすいように情報セキュリティの国際規格であるISO/IEC 27002（情報セキュリティ管理策の実践のための規範）から抜粋し、解りやすい表現にしています。

* + - * 1. （3）情報セキュリティ監査・点検の実施

質問（ヒアリング）：従業員や委託先の管理者などに直接質問して回答を求める

閲覧（レビュー）：情報セキュリティポリシーの関連手続きで申請書などの帳票や、コンピュータのログ、設定内容など実行の証拠となるものを見て確認する

観察（視察）：監査・点検者が現場に赴き、情報セキュリティ対策を行う当事者が情報セキュリティポリシーに従った行動をしていることを目視で確認する

技術診断：技術的対策の運用状況などについて、監査・点検者が自ら機器を操作することによって検証する（情報システムや社内ネットワークの脆弱性を確認するために、専用ソフトウェアを使い技術的な脆弱性を診断することもある）

* + - * 1. （4）改善の実施

経営者や管理者層での議論、検討を通じて、情報セキュリティポリシーや具体的な対策に関する従業員や関係者の理解を促し、不備を改善し、今後に向けた改善につなげていきます。

* + 1. おわりに
       1. Subtopic
          1. 標的型攻撃の巧妙化により、適切な対策を実施していても被害を完全に防ぐことが困難になる中、異常事態の発生を素早く検知し、被害を最小限に抑制するための体制が注目されるなど、対策面も変化しています。また、マイナンバー法の施行、個人情報保護法の改正などに伴い、企業規模を問わず情報セキュリティに対する社会的要請、法的責任が拡大し、中小企業においても情報セキュリティへの取り組みは優先課題となっています。
          2. 一方で、中小企業では依然として資金面や人材面での制約から情報セキュリティ対策の実施が難しいといわれており、実際の統計からも大企業に比較すれば対策が進んでいない傾向が認められます。
          3. 。こうした状況を踏まえ、近年、変化・増大する脅威に対する情報セキュリティ対策を、適切かつ有効なものとすることを目的として、本ガイドラインの初版の内容を抜本的に見直し、改訂版を作成することとしました。
          4. 中小企業は情報セキュリティ対策に十分な経営資源を割り当てることができないという不利を抱える一方で、経営者を含め「従業員の顔が見える」という有利な条件を備えています。
          5. 情報セキュリティの第一歩は、経営者が情報セキュリティの重要性を自ら認識し、そのことを従業員に伝え、従業員がその対策を行う意義を理解することです
          6. 。つまり、「従業員の顔が見える」ということは経営者が直接管理者・担当者に対策を指示することができ、対策の結果についても直接報告を受けることができるなど、大企業に比べて迅速に対応ができるという有利な条件を備えています。
          7. また、この特質を生かすことで、大企業では必要となるセキュリティ監視や情報共有のための設備が不要とできるため、大企業よりも費用をかけずに対策を実現することも可能です。
    2. 本書で用いてる語の説明
       1. インシデント
       2. （情報の）可用性
       3. （情報の）完全性
       4. （情報の）機密性
       5. クラウドサービス
       6. 個人情報
       7. サイバーセキュリティ
       8. CSIRT（ シーサート、Computer Security Incident Response Team）
       9. 情報セキュリティ
       10. 情報セキュリティインシデント
       11. 情報セキュリティに関連した保険商品
       12. 情報セキュリティポリシー
       13. 情報セキュリティマネジメントサイクル
       14. ソーシャルエンジニアリング
       15. ランサムウェア
  1. ◦付録1：
     1. 情報セキュリティ5か条（全2ページ、721KB）pdf

ドキュメントを参照: [000055516.pdf](http://www.ipa.go.jp/files/000055516.pdf)

* + - 1. こんな情報があるはず！
         1. 従業員のマイナンバー、住所、給与明細
         2. お客様や取引先の連絡先一覧
         3. 取引先ごとの仕切り額や取引実績
         4. 新製品の設計図などの開発情報
         5. 組織の経理情報
         6. 取引先から取扱注意と言われた情報
      2. 漏れたら大変！こんなダメージが！
         1. 被害者への損害賠償などの支払い
         2. 取引停止、顧客の他社への流出
         3. ネットの遮断などによる生産効率のダウン
         4. 従業員の士気低下
      3. まずは始めてみよう
         1. ①OSやソフトウェアは常に最新の状態に使用！

OSやソフトウェアのセキュリティ上の問題点を放置していると、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やソフトウェアに修正プログラムを適用する、もしくは最新版を利用しましょう。

* + - * 1. 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。

* + - * 1. 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窃取したID・パスワードが流用されることで、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。

* + - * 1. ④共有設定を見直そう！

データ保管などのクラウドサービスやネットワーク接続の複合機の設定を間違ったため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。クラウドサービスや機器は必要な人にのみ共有されるよう設定しましょう。

* + - * 1. 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。

* 1. ◦付録2：
     1. 5分でできる！情報セキュリティ自社診断シート（全2ページ、417KB）pdf

ドキュメントを参照: [000055517.pdf](http://www.ipa.go.jp/files/000055517.pdf)

* + - 1. Part1 基本的対策
         1. 1.Windows Update※1 を行うなどのように、常にOS やソフトウェアを安全な状態にしていますか？
         2. 2.パソコンにはウイルス対策ソフトを入れてウイルス定義ファイル※2 を自動更新するなどのように、パソコンをウイルスから守るための対策を行っていますか？
         3. 3,パスワードは自分の名前、電話番号、誕生日など推測されやすいものを避けて複数のウェブサイトで使いまわしをしないなどのように、強固なパスワードを設定していますか？
         4. 4.ネットワーク接続の複合機やハードディスクの共有設定を必要な人だけに限定するなどのように、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. 5.利用中のウェブサービス※3 や製品メーカーが発信するセキュリティ注意喚起を確認して社内共有するなどのように、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？
      2. Part2 従業員としての対策
         1. 6.受信した不審な電子メールの添付ファイルを安易に開いたり本文中のリンクを安易に参照したりしないようにするなど、電子メールを介したウイルス感染に気をつけていますか？
         2. 7.電子メールを送る前に目視にて送信アドレスを確認するなどのように、宛先の送信ミスを防ぐ仕組みを徹底していますか？
         3. 8.重要情報をメールで送る時は重要情報を添付ファイルに書いてパスワード保護するなどのように、重要情報の保護をしていますか？
         4. 9.無線LAN を利用する時は強固な暗号化を必ず利用するなどのように、無線LAN を安全に使うための対策をしていますか？
         5. 10.業務端末でのウェブサイトの閲覧やSNS への書き込みに関するルールを決めておくなどのように、インターネットを介したトラブルへの対策をしていますか？
         6. 11.重要情報のバックアップを定期的に行うなどのように、故障や誤操作などに備えて重要情報が消失しないような対策をしていますか？
         7. 12.重要情報を机の上に放置せず書庫に保管し施錠するなどのように、重要情報の紛失や漏えいを防止していますか？
         8. 13.重要情報を社外へ持ち出す時はパスワード保護や暗号化して肌身離さないなどのように、盗難や紛失の対策をしていますか？
         9. 14.離席時にコンピュータのロック機能を利用するなどのように、他人に使われないようにしていますか？
         10. 15.事務所で見知らぬ人を見かけたら声をかけるなどのように、無許可の人の立ち入りがないようにしていますか？
         11. 16.退社時に机の上のノートパソコンや備品を引き出しに片付けて施錠するなどのように、盗難防止対策をしていますか？
         12. 17.最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？
         13. 18.重要情報を廃棄する場合は、書類は細断したり、データは消去ツールを使ったりするなどのように、重要情報が読めなくなるような処分をしていますか？
      3. Part3 組織としての対策
         1. 19.クラウドサービスなど外部サービスを利用する時は利用規約やセキュリティ対策を確認するなどのように、サービスの安全・信頼性を把握して選定していますか？
         2. 20.社内外での個人所有のパソコンやスマートフォンの業務利用を許可制にするなどのように、業務で個人所有端末の利用の可否を明確にしていますか？
         3. 21.採用の際に守秘義務や罰則規定があることを知らせるなどのように、従業員に秘密を守らせていますか？
         4. 22.情報管理の大切さなどを定期的に説明するなどのように、従業員に意識付けを行っていますか？
         5. 23.契約書に秘密保持（守秘義務）の項目を盛り込むなどのように、取引先に秘密を守ることを求めていますか？
         6. 24.秘密情報の漏えいや紛失、盗難があった場合の対応手順書を作成するなどのように、事故が発生した場合に備えた準備をしていますか？
         7. 25.情報セキュリティ対策（上記1～24 など）を会社のルールにするなどのように、情報セキュリティ対策の内容を明確にしていますか？
      4. さらなる情報セキュリティ対策の検討するには
         1. 「5 分でできる！情報セキュリティ自社診断」の次のステップとして、ガイドラインを活用したポリシーの策定やベンチマークでの自己診断を実施してみよう。
         2. 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/keihatsu/sme/guideline/

ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - * 1. 情報セキュリティ対策ベンチマーク

https://www.ipa.go.jp/security/benchmark/

ドキュメントを参照: [benchmark](https://www.ipa.go.jp/security/benchmark/)

* + - 1. 自社診断シートで100 点満点を目指すには
         1. 「5 分でできる！情報セキュリティ自社診断パンフレット」のほか、以下のページで提供されている資料もより具体的な対策の検討に有用ですのでご活用ください。
         2. 情報セキュリティ対策支援サイトiSupport

https://www.ipa.go.jp/security/isec-portal/

ドキュメントを参照: [isec-portal](https://www.ipa.go.jp/security/isec-portal/)

* + - * 1. 対策のしおり

https://www.ipa.go.jp/security/antivirus/shiori.html

ドキュメントを参照: [shiori.html](https://www.ipa.go.jp/security/antivirus/shiori.html)

* + - * 1. 映像で知る情報セキュリティ

https://www.ipa.go.jp/security/keihatsu/videos/

ドキュメントを参照: [videos](https://www.ipa.go.jp/security/keihatsu/videos/)

* + 1. 一般職員向け 情報セキュリティハンドブックひな形（全11ページ、444KB）PowerPoint

ドキュメントを参照: [000055529.pptx](http://www.ipa.go.jp/files/000055529.pptx)

* + - 1. １ 全社基本ルール
         1. OSとソフトウェアのアップデート
         2. ウイルス対策ソフトの導入
         3. パスワードの管理
         4. アクセス制限
         5. セキュリティに対する注意

独立行政法人情報処理推進機構（(略称：IPA）　重要なセキュリティ情報

http://www.ipa.go.jp/security/index.html

ドキュメントを参照: [index.html](http://www.ipa.go.jp/security/index.html)

JVN （Japan Vulnerability Notes）

http://jvn.jp/index.html

ドキュメントを参照: [index.html](http://jvn.jp/index.html)

一般社団法人 JPCERT コーディネーションセンター(略称：JPCERT/CC)

https://www.jpcert.or.jp/

ドキュメントを参照: [www.jpcert.or.jp](https://www.jpcert.or.jp/)

* + - 1. ２ 仕事中のルール
         1. 電子メールの利用
         2. インターネットの利用
         3. データのバックアップ
         4. クリアデスク・クリアスクリーン
         5. 重要情報の持ち出し
         6. 入退室
         7. 電子媒体・書類の廃棄
      2. ３ 全社共通のルール
         1. 私有情報機器の利用
         2. クラウドサービスの利用
      3. ３ 従業員のみなさんへ
         1. 従業員の守秘義務
         2. 事故が起きてしまったら
  1. ◦付録3：
     1. <ツールA>リスク分析シート（全5シート、79KB）excel

ドキュメントを参照: [000055518.xlsx](http://www.ipa.go.jp/files/000055518.xlsx)

* + - 1. 情報資産台帳記入例
      2. 情報資産管理台帳
      3. 脅威の状況
         1. 書類

秘密書類の事務所からの盗難

秘密書類の外出先での紛失・盗難

情報搾取目的の内部不正による書類の不正持ち出し

業務遂行に必要な情報が記載された書類の紛失

* + - * 1. 可搬電子媒体

秘密情報が格納された電子媒体の事務所からの盗難

秘密情報が格納された電子媒体の外出先での紛失・盗難

情報搾取目的の内部不正による電子媒体の不正持ち出し

業務遂行に必要な情報が記載された電子媒体の紛失

* + - * 1. 事務所PC

情報搾取目的の事務所PCへのサイバー攻撃

情報搾取目的の事務所PCでの内部不正

事務所PCの故障による業務に必要な情報の喪失

事務所PC内データがランサムウェアに感染して閲覧不可

不正送金を狙った事務所PCへのサイバー攻撃

* + - * 1. モバイル機器

情報搾取目的でのモバイル機器へのサイバー攻撃

情報搾取目的の不正アプリをモバイル機器にインストール

秘密情報が格納されたモバイル機器の紛失・盗難

* + - * 1. 社内サーバー

情報搾取目的の社内サーバーへのサイバー攻撃

情報搾取目的の社内サーバーでの内部不正

社内サーバーの故障による業務に必要な情報の喪失

* + - * 1. クラウド

安易なパスワードの悪用によるアカウントの乗っ取り

バックアップを怠ることによる業務に必要な情報の喪失

* + - 1. 対策状況チェック
         1. (1) 組織的セキュリティ対策

経営者の主導で情報セキュリティの方針を示していますか？

情報セキュリティの方針に基づき、具体的な対策の内容を明確にしていますか？

情報セキュリティ対策を実施するための体制を整備していますか？

情報セキュリティ対策のためのリソース（人材、費用）の割当を行っていますか？

* + - * 1. (2) 人的セキュリティ対策

秘密情報を扱う全ての者（パートタイマー、アルバイト、派遣社員、顧問、社内に常駐する委託先要員等を含む）に就業規則や契約等を通じて秘密保持義務を課していますか？

従業員の退職に際しては、退職後の秘密保持義務への合意を求めていますか？

会社の秘密情報や個人情報を扱うときの規則や、関連法令による罰則に関して全従業員に説明していますか？

* + - * 1. (3) 情報資産管理

管理を必要とする情報資産は、すべて情報資産管理台帳に記載することを定めていますか？

秘密情報は業務上必要な範囲でのみ利用を認めていますか？

秘密情報の対象となるファイルやデータを丸秘マークや格付け表示等で識別可能とすることを定めていますか？

秘密情報を社外へ持ち出す時はデータを暗号化したり、パスワード保護をかけたりするなどの盗難・紛失対策を定めていますか？

秘密情報を机の上に放置せず施錠保管するなどして、のぞき見されたり紛失しないようにしていますか？

情報資産のバックアップに関する手順を定め、手順が遵守されていることを確認していますか？

秘密情報の入ったパソコンや紙を含む記録媒体を廃棄する場合、ゴミとして処分する前に、データの完全消去用のツールを用いたり、物理的に破壊したりすることで、データを復元できないようにすることを定めていますか？

* + - * 1. (4) マイナンバー対応

特定個人情報の取扱ルール（管理担当者の割当て、関連規程の整備、記録の保存、定期的点検）が定められていますか？

特定個人情報に関する漏えい等の事案に備えた報告連絡体制が整備されていますか？

特定個人情報の保護のための安全管理措置（人的、物理的、技術的のそれぞれ）を行うことが定められていますか？

* + - * 1. (5) アクセス制御と認証

業務で利用するすべてのサーバに対して、アクセス制御の方針が定められていますか？

サーバのアクセス権限は、従業員の退職や異動に応じて随時更新され、定期的なレビューを通じてその適切性が検証されていますか？

情報を社外のサーバ等に保存したり、グループウェアやファイル受渡サービスなどを用いたりする場合は、アクセスを許可された人以外が閲覧できることのないよう、適切なアクセス制御を行うことを定めていますか？

サーバで用いるパスワードは、適切なもののみが受け入れられる機能を通じて設定されていますか？

業務で利用する暗号化機能及び暗号化に関するアプリケーションは、その運用方針が明確に定められていますか？

* + - * 1. (6) 物理的セキュリティ対策

業務を行う場所に、第三者が許可無く立入できないようにするための対策（物理的に区切る、見知らぬ人には声をかける、等）が講じられていますか？

最終退出者は事務所を施錠し退出の記録（日時、退出者）を残すなどのように、事務所の施錠を管理していますか？

高いセキュリティを確保する区域には、許可された者以外は接近できないような保護措置がなされていますか？

秘密情報を保管および扱う場所への個人所有のパソコン・記録媒体等の持込み・利用は禁止されていますか？

* + - * 1. (7) IT機器利用

セキュリティ更新を自動的に行うなどにより、常にソフトウェアを安全な状態にすることを定めていますか？

ウイルス対策ソフトウェアが提供されている製品については、用途に応じて導入し、定義ファイルを常に最新の状態にすることを定めていますか？

業務で利用するIT機器で用いるパスワードに関するルール（他人に推測されにくいものを選ぶ、機器やサービスごとに使い分ける、他人にわからないように管理する、等）ことを定めていますか？

業務で利用する機器が誰かに勝手に使われないようにするための措置（離席時にパスワード付きのスクリーンセーバーが動作する、持ち運び可能な機器は施錠できる場所に格納する、等）を定めていますか？

業務で利用するIT機器の設定について、不要な機能は無効にする、セキュリティを高める機能を有効にするなどの見直しを行うことを定めていますか？

社外で業務を行う場合のルールを定めていますか？

業務での個人所有機器の利用について、禁止しているか、利用する場合のルールを定めていますか？

受信した電子メールが不審かどうかを確認することを求めていますか？

電子メールアドレスの漏えい防止のためのBCC利用ルールを定めていますか？

インターネットバンキングやオンラインショップなどを利用する場合に偽サイトにアクセスしないための対策を定めていますか？

* + - * 1. (8) IT基盤運用管理

IT機器と台帳との棚卸（実機確認）を行うとともに、社内ネットワークに許可なく接続された機器や無線LAN基地局がないことを確認していますか？

サーバで利用するアプリケーションは、ブラックリスト方式（利用してはいけないものを明示）またはホワイトリスト方式（利用してよいものを明示）のいずれかで特定していますか？

業務で利用するすべてのサーバに対して、脆弱性及びマルウェアからの保護のための対策を講じていますか？

サーバで用いた機器の廃棄の手順を定めていますか？

業務で利用するすべてのサーバやネットワーク機器に対して、必要性に応じてイベントログや通信ログの取得及び保存の手順を定めた上で、定期的にレビューしていますか？

サーバを対象とする監査を行うことを定めていますか？

ファイアウォールなど、外部からの攻撃の影響を防ぐための対策を導入していますか？

業務で使っているネットワーク機器のパスワードを初期状態のまま使わず、推測できないパスワードを設定して運用していますか？

クラウドサービスを利用する場合は、費用だけでなく、情報セキュリティや信頼性に関する仕様を考慮して選定していますか？

最新の脅威や攻撃についての情報収集を行い、必要に応じて社内で共有していますか？

* + - * 1. (9) システム開発及び保守

情報システムの開発を行う場合、開発環境と運用環境とを分離していますか？

セキュアな開発を行うための手続きを定めていますか？

情報システムの保守を行う場合、既知の脆弱性が存在する状態で情報システムを運用しないようにするための対策を講じていますか？

* + - * 1. (10) 外部委託管理

契約書に秘密保持（守秘義務）、漏洩した場合の賠償義務、再委託の制限についての項目を盛り込むなどのように、委託先が遵守すべき事項について具体的に規定していますか？

委託先との秘密情報の受渡手順を定めていますか？

委託先に提供した秘密情報の廃棄または消去の手順を定めていますか？

* + - * 1. (11) 情報セキュリティインシデント対応ならびに事業継続管理

秘密情報の漏えいや紛失、盗難があった場合の対応手順書を作成するなどのように、事故の発生に備えた準備をしていますか？

インシデントの発生に備えた証拠情報の収集手順を定め、運用していますか？

事業継続計画における情報セキュリティ対策を定めていますか？

* + - 1. 診断結果
    1. <ツールB>情報セキュリティポリシーサンプル【2016年11月30日IPA】

ドキュメントを参照: [000055794.docx](https://www.ipa.go.jp/files/000055794.docx)

* + - 1. 組織的対策（基本方針）
         1. 情報セキュリティ基本方針を当社のホームページで公表する。/情報セキュリティ基本方針を本社各部署に掲示し従業員及び関係者に周知する。/情報セキュリティ基本方針を顧客の要請の応じ適宜に公表する。
         2. 1.情報セキュリティ基本方針
         3. 2. 個人番号及び特定個人情報の適正な取扱いに関する基本方針
         4. 3.安全管理措置に関する事項
         5. 4.委託の取り扱い
         6. 5.継続的改善
         7. 6.特定個人情報等の開示
      2. 組織的対策（当社全体）
         1. 情報セキュリティ対策活動を推進するための組織として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。
         2. 1.情報セキュリティのための組織
         3. 2.情報セキュリティ取組みの監査・点検/点検
         4. 3.情報セキュリティに関する情報共有
      3. 人的対策（全従業員（役員、社員、派遣社員、パート・アルバイトを含む））
         1. 1.雇用条件
         2. 2.取締役及び従業員の責務
         3. 3.雇用の終了
         4. 4.情報セキュリティ教育
         5. 5.人材育成

＜情報セキュリティに関わる推奨資格＞

* + - 1. 情報資産管理（当社事業に必要で価値がある情報及び個人情報）
         1. 1.情報資産の管理

1.1情報資産の特定と重要度の評価

1.2情報資産の分類と表示

1.3情報資産の管理責任者

1.4情報資産の利用者

* + - * 1. 2.情報資産の社外持ち出し
        2. 3.媒体の処分

3.1媒体の廃棄

3.2媒体の再利用

* + - * 1. 4.バックアップ

4.1バックアップ取得対象

4.2バックアップ媒体の取扱い

4.3クラウドサービスを利用したバックアップ

* + - 1. マイナンバー対応（特定個人情報（マイナンバーを内容に含む個人情報））
         1. 1.総則

1.1目的

1.2定義

* + - * 1. 2.特定個人情報等の取り扱い

2.1利用目的の特定

2.2取得に際しての利用目的の通知等

2.3取得の制限

2.4個人番号の提供の求めの制限

2.5本人確認

2.6利用目的外の利用の制限

2.7特定個人情報ファイルの作成の制限

2.8特定個人情報等の保管

2.9データ内容の正確性の確保

2.10特定個人情報等の提供

2.11特定個人情報等の削除・廃棄

2.12特定個人情報等を誤って収集した場合の措置

2.13安全管理措置

* + - * 1. 3. 組織及び体制

3.1事務取扱担当者・責任者

3.2苦情対応

3.3従業員の義務

* + - * 1. 4.委託の取扱い

4.1委託

4.2再委託

* + - * 1. 5.安全管理措置

5.1組織的安全管理措置

5.1.2取扱規程等に基づく運用

5.1.2取扱規程等に基づく運用

5.1.3取扱状況を確認する手段の整備

5.1.4情報漏えい等事案に対応する体制の整備

5.2人的安全管理措置

5.3物理的安全管理措置

5.3.1特定個人情報等を取り扱う領域の管理

5.3.2ＩＴ機器及び電子媒体等の盗難等の防止

5.3.3電子媒体等を持ち出す場合の漏えい等の防止

5.3.4個人番号の削除、機器及び電子媒体等の廃棄

5.4技術的安全管理措置

5.4.1アクセス制御

5.4.2アクセス者の識別と認証

5.4.3外部の不正アクセス等の防止

5.4.4情報漏えい等の防止

* + - * 1. 6.特定個人情報等の開示、訂正等、利用停止等

6.1特定個人情報等の開示等

6.2特定個人情報等の訂正等

6.3特定個人情報等の利用停止等

* + - 1. アクセス制御及び認証（情報資産の利用者及び情報処理施設）
         1. 1.アクセス制御方針
         2. 2.利用者の認証
         3. 3.利用者アカウントの登録
         4. 4.利用者アカウントの管理
         5. 5.パスワードの設定
         6. 6.従業員以外の者に対する利用者アカウントの発行
         7. 7.機器の識別による認証
         8. 8.端末のタイムアウト機能
         9. 9.標準設定等

9.1アクセス制御対象情報システム及びアクセス制御方法

9.2利用者認証方法

9.3利用者アカウント・パスワードの条件

9.4機器の認証方法

* + - 1. 物理的対策（情報処理設備が設置される領域）
         1. 1.セキュリティ領域の設定
         2. 2.関連設備の管理
         3. 3.セキュリティ領域内注意事項
         4. 4.搬入物の受け渡し
      2. ＩＴ機器利用（業務で利用する情報処理設備・機器）
         1. 1.ソフトウェアの利用

1.1標準ソフトウェア

1.2ソフトウェアの利用制限

1.3ソフトウェアのアップデート

1.4ウイルス対策ソフトウェアの利用

1.4.1ウイルス検知

1.4.2ウイルス対策ソフト定義ファイルの更新

1.4.3社外機器のLAN接続

1.5ウイルス対策の啓発

* + - * 1. 2.ＩＴ機器の利用
        2. 3.クリアデスク・クリアスクリーン

3.1クリアデスク

3.2クリアスクリーン

* + - * 1. 4.インターネットの利用

4.1ウェブ閲覧

4.2オンラインサービス

＜インターネットバンキング・電子決済＞

＜オンラインストレージ＞

4.3ＳＮＳの利用

4.4電子メールの利用

＜誤送信防止＞

＜メールアドレス漏えい防止＞

＜傍受による漏えい防止＞

＜クラウド型メールの利用＞

＜禁止事項＞

4.5ウイルス感染の防止

5.私有ＩＴ機器・電子媒体の利用

5.1利用開始時

5.2利用期間中

5.2.1社内での利用

5.3利用終了時

6.標準等

6.1標準ソフトウェア

6.2ソフトウェアのアップデート方法

6.3ウイルス対策ソフトウェアの定義ファイルの更新方法

* + - 1. ＩＴ基盤運用管理（情報資産を扱うサーバ・ネットワーク等のＩＴインフラ）
         1. 1.管理体制

1.1 ＩＴ基盤の情報セキュリティ対策

1.1.1サーバー機器の情報セキュリティ要件

1.1.2サーバー機器に導入するソフトウェア

1.1.3ネットワーク機器の情報セキュリティ要件

* + - * 1. 2.ＩＴ基盤の運用
        2. 3.クラウドサービスの導入
        3. 4.脅威や攻撃に関する情報の収集
        4. 5.廃棄・返却・譲渡
        5. 6.ＩＴ基盤標準

6.1サーバー機器情報セキュリティ要件

6.2ＩＴ基盤標準ソフトウェア

6.3標準ネットワーク機器

6.4ネットワーク機器情報セキュリティ要件

6.5クラウドサービス情報セキュリティ対策評価基準

＜適合性評価制度の種類＞

* + - 1. システム開発及び保守（当社が独自に開発及び保守を行う情報システム）
         1. 1.情報システムの開発

1.1新規システム開発・改修

1.2脆弱性への対処

1.3情報システムの開発環境

1.4情報システムの保守

1.5情報システムの変更

* + - 1. 外部委託管理（情報資産を取り扱う業務の委託）
         1. 1.委託先の評価（クラウドサービスの利用を除く）

1.1委託先評価基準

1.2委託先の選定

1.3委託契約の締結

1.4委託先の評価

1.5再委託

* + - 1. 情報セキュリティインシデント対応ならびに事業継続管理（情報セキュリティ事故対応及び事業継続管理）
         1. 事象が発生した場合に、混乱しないように事前に対応策を明確にしておくことが肝要
         2. 1.対応体制

最高責任者、対応責任者、一次対応者を明確にする

* + - * 1. 2.情報セキュリティインシデントの影響範囲と対応者

想定する影響範囲を事故レベル（0～3）で分類し、それぞれの対応者を明確にする

* + - * 1. 3.インシデントの連絡及び報告

レベル1以上のインシデントが発生した場合、発見者が速やかに指示を仰ぐべき対応者を明確にする

* + - * 1. 4.対応手順

基本【中山】

事象の検知、報告受付(Detect)

事実確認、対応の判断 被害の局所化(拡大防止)(Triage)

緊急連絡

原状保全

原因調査

早期復旧・事業継続 (Respond)

恒久的対策（再発防止策）

通常運用

4.1漏えい・流出発生時の対応

事象：社外秘又は極秘情報資産の盗難、流出、紛失

事故レベル3【中分類付け】【中山】

事象の検知、報告受付(Detect)

①発見者は即座にインシデント対応責任者及び代表取締役社長に報告する。

事実確認、対応の判断 被害の局所化(拡大防止)(Triage)

②インシデント対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行する。

③インシデント対応責任は被害者/本人対応を準備する。

④インシデント対応責任は問合せ対応を準備する。

緊急連絡

⑤インシデント対応責任は影響範囲・被害の大きさによっては総務部に報道発表の準備を申請する。

⑥インシデント対応責任者はサイバー攻撃等の不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に届け出る。

⑦インシデント対応責任者は個人情報の漏えいの場合には監督官庁に届け出る。

代表取締役は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。

原状保全

原因調査

早期復旧・事業継続 (Respond)

恒久的対策（再発防止策）

通常運用

事故レベル3【基本手順】

①発見者は即座にインシデント対応責任者及び代表取締役社長に報告する。

②インシデント対応責任者は原因を特定するとともに、二次被害が想定される場合には防止策を実行する。

③インシデント対応責任は被害者/本人対応を準備する。

④インシデント対応責任は問合せ対応を準備する。

⑤インシデント対応責任は影響範囲・被害の大きさによっては総務部に報道発表の準備を申請する。

⑥インシデント対応責任者はサイバー攻撃等の不正アクセスによる被害の場合は都道府県警察本部のサイバー犯罪相談窓口に届け出る。

⑦インシデント対応責任者は個人情報の漏えいの場合には監督官庁に届け出る。

代表取締役は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。

事故レベル2

①発見者は発見次第、システム管理者に報告する。

②システム管理者は漏えい先を調査し、インシデント対応責任者に報告する。

③システム管理者は社内関係者に周知する。

事故レベル１

※情報漏えい・流出は全て事故レベル2以上

4.2改ざん・消失・破壊・サービス停止発生時の対応

情報資産の意図しない改ざん、消失、破壊 情報資産が必要なときに利用できない

事故レベル3【中分類付け】【中山】

事象の検知、報告受付(Detect)

手順の確認

作業記録の作成

①発見者は即座にインシデント対応責任者及び代表取締役社長に報告する。

事実確認、対応の判断 被害の局所化(拡大防止)(Triage)

②システム管理者は原因を特定し、応急処置を実行する。

影響範囲の特定

ネットワーク接続やシステムの遮断もしくは停止

緊急連絡

③インシデント対応責任者は社内に周知するとともに総務部情報システム担当に連絡する。

原状保全

各種ログの保全

スナップショットの保存

場合によっては、ストレージ装置全体

原因調査

⑦システム管理者は原因対策を実施する。

要因の特定

早期復旧・事業継続 (Respond)

④電子データの場合はシステム管理者がバックアップによる復旧を実行する。

⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。

⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。

恒久的対策（再発防止策）

再発防止策の実施

監視体制の強化

作業結果の報告

作業の評価、ポリシー・運用体制・運用手順の見直し

通常運用

代表取締役は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。

事故レベル3【基本手順】

①発見者は即座にインシデント対応責任者及び代表取締役社長に報告する。

②システム管理者は原因を特定し、応急処置を実行する。

③インシデント対応責任者は社内に周知するとともに総務部情報システム担当に連絡する。

④電子データの場合はシステム管理者がバックアップによる復旧を実行する。

⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。

⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。

⑦システム管理者は原因対策を実施する。

代表取締役は社内及び影響範囲の全ての組織・人に対応結果及び対策を公表する。

事故レベル2

①発見者は発見次第、システム管理者に報告する。

②システム管理者は原因を特定し、応急処置を実行する。

③インシデント対応責任者は社内に周知するとともに総務部情報システム担当に連絡する。

④電子データの場合はシステム管理者がバックアップによる復旧を実行する。

⑤機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。

⑥書類・フィルム原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する。

⑦システム管理者は原因対策を実施する。

事故レベル1

①発見者は発見次第、システム管理者に報告する。

②システム管理者は原因を特定し、応急処置を実行する。

③電子データの場合はシステム管理者がバックアップによる復旧もしくは再作成・入手を実行する。

④機器の場合はシステム管理者が修理、復旧、交換等の手続きを行う。

⑤書類・フィルム等の原本の場合は情報セキュリティ部門責任者が可能な範囲で修復する

⑥システム管理者は原因対策を実施する

事故レベル0

発見者は発見次第、発生可能性のあるインシデントと想定される被害をシステム管理者に報告する。

4.3ウイルス感染時の初期対応

悪意のあるソフトウェアに感染

従業員は、業務に利用しているパソコン、サーバー又はスマートフォン、タブレット（以下「コンピュータ」といいます。）がウイルスに感染した場合には、以下を実行する。

①ネットワークからコンピュータを切断する。

②システム管理者に連絡する。

③ウイルス対策ソフトの定義ファイルを最新版に更新する。

④ウイルス対策ソフトを実行しウイルス名を確認する。

⑤ウイルス対策ソフトで駆除可能な場合は駆除する。

⑥駆除後再度ウイルス対策ソフトでスキャンし、駆除を確認する。

⑦システム管理者に報告する。

以下の場合など従業員自身で対応できないと判断される場合はシステム管理者に問い合わせる。

ウイルス対策ソフトで駆除できない。

システムファイルが破壊・改ざんされている。

ファイルが改ざん・暗号化・削除されている。

4.5届け出及び相談

システム管理者は、インシデント対応後に以下の機関への届け出又は相談を検討する。

＜届け出・相談先＞

独立行政法人 情報処理推進機構セキュリティセンター(IPA/ISEC)

ウイルスの届け出先 https://www.ipa.go.jp/security/outline/todokede-j.html TEL: 03-5978-7518 E-mail：virus@ipa.go.jp

不正アクセスに関する届出 E-Mail：crack@ipa.go.jp FAX：03-5978-7518

情報セキュリティ安心相談窓口 https://www.ipa.go.jp/security/anshin/index.html TEL:03-5978-7509 E-mail：anshin@ipa.go.jp

* + - * 1. 5.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

代表取締役は、情報セキュリティインシデントの影響により当社事業が中断した場合に備え、以下を定める。

5.1想定される情報セキュリティインシデント

以下のインシデントによる事業の中断を想定する。

情報セキュリティインシデント：大型地震の発生に伴う設備の倒壊、回線の途絶、停電等にによる○○システム停止

想定理由：当社の事業は、商品の販売から請求回収までの業務を○○システムに依存しているため、停止した場合は事業の継続が困難になり多大な損失が発生

5.2復旧責任者及び関連連絡先

被害対象毎に、復旧責任者、関係者連絡先をリスト化しておく

5.3事業継続計画

インシデント対応責任者は、想定する情報セキュリティインシデントが発生し、事業が中断した際の復旧責任者の役割認識及び関係者連絡先について、有効に機能するか検証する。

復旧責任者は、被害対象に応じて復旧から事業再開までの計画を立案する。

* + - 1. 社内体制図（当社の情報セキュリティ管理）
         1. 1.情報セキュリティのための組織
      2. 委託契約書機密保持条項サンプル（外部委託契約の締結時）
         1. 1.委託契約時の機密保持契約条項

＜機密保持条項サンプル＞

1. 責任分担と連絡体制の整備