Sec01-02-54\_各種ガイドブックの内容要約\_一般企業向け【特に中小企業】

ドキュメントを参照: [Sec01-02-50\_サイバーセキュリティ関連\_各種ガイドブックの内容要約.mmap](file:///D:\Cloud_Storage\OneDrive%20-%20ＮＰO知的資源イニシアティブ（ＩＲＩ）\git_repository_Duo\Sharing_Knowledge3\MindManager3\Sec01-02-50_サイバーセキュリティ関連_各種ガイドブックの内容要約.mmap)

1. 改訂履歴
   1. 【2020年6月15日】最新文献追加
2. 一般企業向け【特に中小企業】
3. 知財関連
   1. 「Bib10-08「知の共有化」に関連した国等の政策の要約」を参照
   2. 「第四次産業革命を視野に入れた知財システムの在り方に関する検討会」の報告書の中小企業部分抜粋

ドキュメントを参照: [20170419002.html](http://www.meti.go.jp/press/2017/04/20170419002/20170419002.html)

* + 1. 中小企業等の視点からの検討
       1. 現状と課題
          1. IoTが進む中、 中小企業等においても、

データや標準化を活用して、 国境を越えて世界展開できる

一方、 その裏返しで、 突如知財の問題にさらされるリスクが高まっている

* + - * 1. 中小企業等を取り巻くビジネス環境が変化している状況の下

IoT化に対応したビジネスに飛鳥な特許を国内外で取得できない恐れがある

* + - * 1. 第四次産業革命の下で、 オープン・イノベーションが促進される中

自社のクーズ領域を守る手段としての知財の重要性に関する認識が十分でない

* + - * 1. 社会を改革するキーテクノジーの多くが中小企業等で生み出されてきたことに鑑み

中小企業等の有する技術の標準化をすいしんしていくこと

大企業と中小企業との間で一方の有する技術を他方が活用することの重要性

大企業と中小企業との連携促進が不可欠

* + - * 1. 中小企業の分類

IT化に対応できている企業

ITを活用してサービスを提供する側の企業

そのような企業から提供されるサービスを利用する企業

IT化に対応できていない企業

* + - 1. 今後実施することが適当な取り組み
         1. 第四次産業革命やIoT化に対応したビジネス環境の変化に対応するため

中小企業等が知財戦略を推進し、 知財を権利化・活用することが一層求められる

* + - * 1. 一方、 特許庁では

知財分野における地域・中小企業支援という観点から

2016年9月に「地域知財活性化行動計画」を策定

本計画に基づいて、 中小企業等に対し

知財制度や支援施策の普及啓発、 情報提供、 各種相談・支援対応等の取り組みが実施されている

国内外での特許取得支援

相談から出願、 侵害対策まで一体となった海外旋回支援

* + - * 1. 中小企業等が有する優れた技術については

新市場創造型標準化制度を利用した迅速な標準化を実現することにより、 市場拡大を支援する

* + - * 1. 加えて、 中小企業等と大企業との連携の推進への取り組みの一環として

「地方創生のための事業プデューサー派遣事業」を活用し、 大企業と中小企業との間での知財のマッチング等を推進

金融機関が有する地域の企業情報を活用した知財マッチングびじねすの促進を図る

* + - * 1. 中小企業等と大企業との連携に当たっては

企業における営業秘密に関する認識

双方のコンプライアンスに対する意識を向上させることが不可欠

知財総合支援窓で大企業と連携する中小企業等を支援

中小企業等が大企業と連携する際の留意点や連携の過程で発生した懸念等についての相談受付

中小企業等の営業秘密が他社に渡ることを防ぐべく

不正競争防止法の精度や秘密情報の保護ハンドブック等の周知など営業秘密の保護。 管理に関する普及啓発を進めていく

* + - * 1. 中小企業等と大企業との対応な連携への取り組みが推進される環境の醸成

1. 中小企業向け「はじめての個人情報保護法」～シンプルレッスン～【2017年6月個人情報保護委員会】

ドキュメントを参照: [1706\_simplelesson.pdf](https://www.ppc.go.jp/files/pdf/1706_simplelesson.pdf)

* 1. １．「個人情報保護法」とは
     1. 個人の権利・利益の保護と個人情報の有用性(社会生活やビジネス等への活用)とのバランスを図るための法律
     2. 民間事業者の個人情報の取扱いについて規定
     3. 従来は、 取り扱う個人情報の数が5,000人分以下の事業者には適用されていませんでしたが、 平成29年5月30日からは、 すべての事業者に適用されています
  2. ２．「個人情報」とは
     1. 生存する個人に関する情報で、 特定の個人を識別することができるもの
  3. ３．事業者が守るべき４つのルール
     1. 勝手に使わない！
        1. 利用目的を特定して、 その範囲内で利用する。
        2. 利用目的を通知又は公表する。
     2. なくさない！ 漏らさない！
     3. 勝手に人に渡さない！
     4. お問合わせに対応！
  4. ４．
     1. （１）取得・利用に関するルール
        1. 「要配慮個人情報」とは？
           1. （例）人種、 信条、 社会的身分、 病歴、 犯罪の経歴、 犯罪により害を被った事実、 身体障害等の障害があること等
        2. 「要配慮個人情報」を取得する場合は、 あらかじめ本人の同意が必要。
     2. （２）保管に関するルール
        1. 漏えい等が生じないよう、 安全に管理する。
        2. 従業者・委託先にも安全管理を徹底する。
        3. 1　基本方針の策定
        4. 2　個人データの取扱いに係る規律の整備
        5. 3　組織的安全管理措置
        6. 4　人的安全管理措置
        7. 5　物理的安全管理措置
        8. 6　技術的安全管理措置
     3. （３）提供に関するルール
        1. 第三者に提供する場合は、 あらかじめ本人から同意を得る。
        2. 第三者に提供した場合・第三者から提供を受けた場合は、 一定事項を記録する。
        3. 記録事項・保存期間について
           1. 「いつ・誰の・どんな情報を・誰に」提供したか？
           2. 「いつ・誰の・どんな情報を・誰から」提供されたか？＋「相手方の取得経緯」
        4. 外国にある第三者に提供する場合に守るべきこと
           1. ① 外国にある第三者に提供することについて、 本人の同意を得る。
           2. ② 外国にある第三者が、 適切な体制を整備している（※）。

※APEC越境プライバシールール（CBPR）システム

ドキュメントを参照: [CBPR\_ppc.pdf](http://www.ppc.go.jp/files/pdf/CBPR_ppc.pdf)

* + - * 1. ③ 外国にある第三者が個人情報保護委員会が認めた国に所在している。
    1. （４）本人からの開示請求等に関するルール
       1. 本人から開示等の請求があった場合はこれに対応する。
       2. 苦情等に適切・迅速に対応する。
  1. (参考1) 罰則
     1. 罰則について
        1. 事業者の法遵守の状況は、 個人情報保護委員会が監督します。
        2. 必要に応じて、 報告を求めたり立入検査を行い、 実態に応じて指導・助言、 勧告、 命令を行います。
     2. 匿名加工情報
        1. ビッグデータの活用を推進するための制度。
        2. 「匿名加工情報」とは、 特定の個人を識別できないように個人情報を加工し、 その個人情報を復元できないようにした情報（利用目的や第三者提供の制限なく、 一定の取扱いルールの下、 自由な流通・利活用を促進）。
        3. 匿名加工情報の加工基準や取扱いルールについては、 ガイドラインや事務局レポートをご参照ください。
  2. (参考2) 認定個人情報保護団体
     1. 事業者の個人情報の適切な取扱いの確保を目的として、 国の認定を受けた民間団体。
     2. 対象事業者への情報提供、 個人情報に関する苦情の処理等を行う。
  3. (参考3) 個人情報保護法相談ダイヤル等
     1. 個人情報保護法に関する質問等
        1. 03－6457－9849
     2. 事業者の個人情報の取扱いに関する苦情相談
        1. ・事業者の苦情受付窓口
        2. ・消費生活センター等の地方公共団体の窓口
        3. ・認定個人情報保護団体
  4. 【 巻末資料】中小企業向け「これだけは！」チェックリスト10
     1. 取得・利用
        1. 取り扱っている個人情報について、 利用目的を決めていますか？
        2. その利用目的は、 本人に通知するか公表していますか？
     2. 保管
        1. （組織的安全管理措置）個人情報の取扱いのルールや責任者を決めていますか？
        2. （人的安全管理措置・従業者監督）個人情報の取扱いについて従業員に教育を行っていますか？
        3. （物理的安全管理措置）個人情報が含まれる書類や電子媒体について、 誰でも見られる場所・盗まれやすい場所に放置していませんか？
        4. （技術的安全管理措置）パソコン等で個人情報を取り扱う場合、 セキュリティ対策ソフトウェア等をインストールして最新の状態にしていますか？
        5. 個人情報の取扱いを委託する場合、 契約を締結する等、 委託先に適切な管理を求めていますか？
     3. 提供
        1. 本人以外に個人情報を提供する場合、 本人に同意をとっていますか？
        2. 本人以外に個人情報を提供したり、 本人以外から個人情報を受け取る際、 相手方や提供年月日等について記録を残していますか？
     4. 開示請求等
        1. 本人から自分の個人情報を見せてほしいと言われたり、 訂正してほしいと言われた際には、 対応していますか？
     5. サブトピック

1.  Sec01-02-20 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）⇒独立文書化

ドキュメントを参照: [Sec01-02-20](https://bluemoon55.github.io/Sharing_Knowledge/Cyber_Security/Deliverables/mind2html/Sec01-02-20)

* 1. 改版履歴
     1. 2018年12月25日　独立文書化
     2. 【2017年5月10日IPA】
  2. 一式公開ページ

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

* 1. 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）【本文】

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. サブトピック
          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. SECURITY ACTION【2017年4月IPA】

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

* 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
  2. 経営に欠かせない 情報セキュリティ
     1. IT社会では、 企業経営においても、 IT活用による「攻め」と同時に、 情報セキュリティによる「守り」が不可欠です。 身近なところから情報セキュリティ対策を始めましょう。
  3. 一つ星
     1. 中小企業の情報セキュリティ対策ガイドライン付録の「情報セキュリティ5か条」に取組むことを宣言した中小企業等であることを示すロゴマーク
     2. 情報セキュリティ5か条

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

* 1. 二つ星
     1. 中小企業の情報セキュリティ対策ガイドライン付録の「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、 情報セキュリティポリシー（基本方針）\*1を定め、 外部に公開したことを宣言した中小企業等であることを示すロゴマーク
     2. 5分でできる！情報セキュリティ自社診断パンフレット(PDF)

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

* + 1. 5分でできる！情報セキュリティ自社診断シート(PDF)

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

* + 1. 中小企業の情報セキュリティ対策ガイドライン(PDF)

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

* 1. SECURITY ACTIONロゴマークの使用申込

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

1. 中小企業における組織的な情報セキュリティ対策ガイドラインチェック項目【2012年9月3日IPA】

ドキュメントを参照: [02\_checklist.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/02_checklist.pdf)

* 1. 1. 情報セキュリティに対する組織的な取り組み
     1. 1.1 情報セキュリティに関する経営者の意図が従業員に明確に示されている
        1. 経営者が情報セキュリティポリシーの策定に関与し、 実現に対して責任を持つこと。
        2. 情報セキュリティポリシーを定期的に見直しすること。
     2. 1.2 情報セキュリティ対策に関わる責任者と担当者を明示する
        1. 責任者として情報セキュリティと経営を理解する立場の人を任命すること。
        2. 責任者は、 各セキュリティ対策について（社内外を含め）、 責任者、 担当者それぞれの役割を具体化し、 役割を徹底すること。
     3. 1.3 管理すべき重要な情報資産を区分する
        1. 管理すべき重要な情報資産を、 他の情報資産と分類すること。
        2. 情報資産の管理者を定めること。
        3. 重要度に応じた情報資産の取り扱い指針を定めること。
        4. 重要な情報資産を利用できる人の範囲を定めること。
     4. 1.4 重要な情報については、 入手、 作成、 利用、 保管、 交換、 提供、 消去、 破棄における取り扱い手順を定める
        1. 各プロセスにおける作業手順を明確化し、 決められた担当者が、 手順に基づいて作業を行っていること。
        2. 重要な情報に対して、 漏洩や不正利用を防ぐ保護対策を行っていること。
        3. （例）
        4. 重要な情報を利用できる人に対してのみ、 アクセス可能とすること。
        5. 重要な情報の利用履歴を残しておくこと。
        6. 重要な情報を確実に消去・廃棄すること。 等
     5. 1.5 外部の組織と情報をやり取りする際に、 情報の取り扱いに関する注意事項について合意を取る
        1. 契約書や委託業務の際に取り交わす書面等に、 情報の取り扱いに関する注意事項を含めること。
        2. （例）
        3. システム開発を委託する際の本番データ利用時の際の情報管理、 例えば管理体制や受託情報の取り扱い・受け渡し・返却、 廃棄等について、 注意事項を含めること。
        4. 関係者のみにデータの取り扱いを制限すること。
        5. 外部の組織との間で情報を授受する場合、 情報受渡書を持っておこなうこと。
        6. 契約に基づく作業を遂行することによって新たに発生する情報（例：新たに作製された、 金型・図面・モックアップ等々）の取扱を含めること。
        7. 等
     6. 1.6 従業者（派遣を含む）に対し、 セキュリティに関して就業上何をしなければいけないかを明示する
        1. 従業者を採用する際に、 守秘義務契約や誓約書を交わしていること。
        2. 従業者が順守すべき事項を明確にしていること。
        3. 違反を犯した従業員に対する懲戒手続きが整備されていること。
        4. 在職中及び退職後の機密保持義務を明確化するため、 プロジェクトへの参加時など、 具体的に企業機密に接する際に、 退職後の機密保持義務も含む誓約書を取ること。
     7. 1.7 情報セキュリティに関するルールの周知と、 情報セキュリティに関わる知識習得の機会を与える
        1. ポリシーや関連規程を従業員に理解させること。
        2. 実践するために必要な教育を定期的に行っていること。
  2. 2. 物理的セキュリティ
     1. 2.1 重要な情報を保管したり、 扱ったりする場所の入退管理と施錠管理を行う
        1. 重要な情報を保管したり、 扱ったりする区域を定めていること。
        2. 重要な情報を保管している部屋（事務室）又はフロアーへの侵入を防止するための対策を行っていること。
        3. 重要な情報を保管している部屋（事務室）又はフロアーに入ることができる人を制限し、 入退の記録を取得していること。
     2. 2.2 重要なコンピュータや配線は地震などの自然災害や、 ケーブルの引っ掛けなどの人的災害が起こらないように配置・設置する
        1. 重要なコンピュータは許可された人だけが入ることができる安全な場所に設置すること。
        2. 電源や通信ケーブルなどは、 他の人が容易に接触できないようにすること。
        3. 重要なシステムについて、 地震などによる転倒防止、 水濡れ防止、 停電時の代替電源の確保などを行っていること。
     3. 2.3 重要な書類、 モバイルPC、 記憶媒体などについて、 整理整頓を行うと共に、 盗難防止対策や確実な廃棄を行う
        1. （重要な書類について）
           1. 不要になった場合、 シュレッダーや焼却などして確実に処分すること。
           2. 重要な書類を保管するキャビネットには、 施錠管理を行うこと。
           3. 重要な情報が存在する机上、 書庫、 会議室などは整理整頓を行うこと。
           4. 郵便物、 FAX、 印刷物などの放置は禁止。 重要な書類の裏面を再利用しないこと。
        2. （モバイルPC、 記憶媒体について）
           1. 保存した情報が不要になった場合、 消去ソフトを用いるなど、 確実に処分していること。
           2. モバイルPC、 記憶媒体については、 盗難防止の対策を行うこと。
           3. 私有PCを会社に持ち込んだり、 私有PCで業務を行ったりしないこと。
  3. 3. 情報システム及び通信ネットワークの運用管理
     1. 3.1 情報システムの運用に関して運用ルールを策定する
        1. システム運用におけるセキュリティ要求事項を明確にしていること。
        2. 情報システムの運用手順書（マニュアル）を整備していること。
        3. システムの運用状況を点検していること。
        4. システムにおいて実施した操作や障害、 セキュリティ関連イベントについてログ（記録）を取得していること。
        5. 設備（具体例）の使用状況を記録していること。
     2. 3.2 ウイルス対策ソフトをはじめとしたアプリケーションの運用を適切に行う
        1. ウイルス対策ソフトを導入し、 パターンファイルの更新を定期的に行っていること。
        2. ウイルス対策ソフトが持っている機能（ファイアウォール機能、 スパムメール対策機能、 有害サイト対策機能）を活用すること。
        3. 各サーバやクライアントPCについて、 定期的なウイルス検査を行っていること。
        4. Winny等、 組織で許可されていないソフトウェアのインストールの禁止、 あるいは使用制限を行っていること。
     3. 3.3 導入している情報システムに対して、 最新のパッチを適用するなどの脆弱性対策を行う
        1. 脆弱性の解消（修正プログラムの適用、 Windows update等）を行っていること。
        2. 脆弱性情報や脅威に関する情報の入手方法を確認し、 定期的に収集すること。
        3. 情報システム導入の際に、 不要なサービスの停止など、 セキュリティを考慮した設定を実施するなどの対策が施されているかを確認すること。
        4. Webサイトの公開にあたっては、 不正アクセスや改ざんなどを受けないような設定・対策を行い、 脆弱性の解消を行うこと。
        5. Webブラウザや電子メールソフトのセキュリティ設定を行うこと。
     4. 3.4 通信ネットワークを流れる重要なデータに対して、 暗号化などの保護策を実施する
        1. 必要に応じて、 SSL等を用いて通信データを暗号化すること。
        2. 外部のネットワークから内部のネットワークや情報システムにアクセスする場合に、 VPNなどを用いて暗号化した通信路を使用していること。
        3. 電子メールをやり取りする際に、 重要な情報についてはファイルにパスワードを付ける、 又は暗号化すること。
     5. 3.5 モバイルPCやUSBメモリなどの記憶媒体やデータを外部に持ち出す場合、 適切なパスワード設定や暗号化などの対策を実施する
        1. モバイルPCやUSBメモリ等の使用や外部持ち出しについて、 規程を定めていること。
        2. 外部でモバイルPCやUSBメモリ等を使用する場合の紛失や盗難対策を講じていること。
        3. モバイルPCやUSBメモリ等を外部に持出す際は、 利用者の認証（ID・パスワード設定、 USBキーやICカード認証、 バイオメトリクス認証等）を行うこと。
        4. 保存されているデータを、 重要度に応じてHDD暗号化、 BIOSパスワード設定などの技術的対策を実施すること。
        5. PCを持出す場合の持出者、 持出・返却管理を実施すること。
        6. 盗難、 紛失時に情報漏えいの脅威にさらされた情報が何かを正確に把握するため、 持ち出し情報の一覧、 内容管理を行うこと。
  4. 4. 情報システムのアクセス制御の状況及び情報システムの開発、 保守におけるセキュリティ対策
     1. 4.1 情報（データ）や情報システムへのアクセスを制限するために、 利用者IDの管理（パスワードの管理など）を行う
        1. 利用者毎にIDとパスワードを割当て、 そのIDとパスワードによる識別と認証
        2. を確実に行うこと。
        3. 利用者IDの登録や削除に関する規程を整備すること。
        4. パスワードの定期的な見直しを求めること。 また、 空白のパスワードや単純な文字列のパスワードを設定しないよう利用者に求めること。
        5. 離席する際は、 パスワードで保護されたスクリ
        6. ーンセーバーでパソコンを保護すること。
        7. 不要になった利用者IDを削除すること。
     2. 4.2 重要な情報に対するアクセス権限の設定を行う
        1. 重要な情報に対するアクセス管理方針を定め、 利用者毎にアクセス可能な情報、 情報システム、 業務アプリケーション、 サービス等を設定すること。
        2. 職務の変更や異動に際して、 利用者のアクセス権限を見直すこと。
     3. 4.3 インターネット接続に関わる不正アクセス対策（ファイアウォール機能、 パケットフィルタリング、 ISPサービス 等）を行う
        1. （外部から内部へのアクセス）
           1. 外部から内部のシステムにアクセスする際、 利用者認証を実施すること。
           2. 保護すべき重要な情報が保存されるシステムは、 それ以外のシステムが接続しているネットワークから物理的に遮断する、 もしくはセグメント分割することによりアクセスできないようにすること。
        2. （内部から外部へのアクセス）
           1. 不正なプログラムをダウンロードさせる恐れのあるサイトへのアクセスを遮断するような仕組み（フィルタリングソフトの導入等）を行っていること。
     4. 4.4 無線LANのセキュリティ対策（WPA2の導入等）を行う
        1. 無線LANにおいて重要な情報の通信を行う場合は、 暗号化通信（WPA2等）の設定を行うこと。
        2. 無線LANの使用を許可する端末（MAC認証）や利用者の認証を行うこと。
     5. 4.5 ソフトウェアの選定や購入、 情報システムの開発や保守に際して、 情報セキュリティを前提とした管理を行う
        1. ソフトウェアの導入や変更に関する手順を整備していること。
        2. システム開発において、 レビューの実施と記録を残していること。
        3. 外部委託によるソフトウェア開発を行う場合、 使用許諾、 知的所有権などについて取り決めていること。
        4. 開発や保守を外部委託する場合に、 セキュリティ管理の実施状況を把握できること。
  5. 5. 情報セキュリティ上の事故対応
     1. 5.1 情報システムに障害が発生した場合、 業務を再開するために何をすべきかを把握する
        1. 情報システムに障害が発生した場合の、 最低限運用の必要な時間帯と許容停止時間を明確にしておくこと。
        2. 障害対策の仕組みが組織として効果的に機能するよう、 よく検討していること。
        3. システムの切り離し（即応処理）、 必要なサービスを提供できるような機能（縮退機能）、 情報の回復や情報システムの復旧に必要となる機能などが、 障害時に円滑に機能するよう確認しておくこと。
        4. 日常のシステム運用の中で、 バックアップデータや運用の記録などを確保しておくこと。
        5. 障害発生時に必要な対応として、 障害発生時の報告要領（電話連絡先の認知等）、 障害対策の責任者と対応体制、 システム切替え・復旧手順、 障害発生時の業務実施要領等の準備を整えておくこと。
        6. （例）
        7. 大容量データの復元には時間を要するため、 復元に要する時間の事前見積りの実施。
        8. 関係者への障害対応要領の周知や、 必要なスキルに関する教育や訓練などの実施を行っていること。
     2. 5.2 情報セキュリティに関連する事件や事故等（ウイルス感染、 情報漏えい等）の緊急時に、 何をすべきかを把握する
        1. ウイルス感染や情報漏えい等の発生時、 組織内の関係者への報告、 緊急処置の適用基準や実行手順、 被害状況の把握、 原因の把握と対策の実施、 被害者への連絡や外部への周知方法、 通常システムへの復旧手順、 業務再開手順などを整えておくこと。
        2. （例）
        3. ウイルス感染の場合、 ウイルス定義ファイルを最新の状態にしたワクチンソフトにより、 コンピュータの検査を実施し、 ワクチンソフトのベンダのWebサイト等の情報を基に、 検出されたウイルスの駆除方法などを試すことが必要となる。
        4. 情報漏えいの場合、 事実を確認したら速やかに責任者に報告し、 対応体制を取ること、 対応についての判断を行うため5W1Hの観点で調査し情報を整理すること、 対策本部で対応方針を決定すること、 被害の拡大防止と復旧のための措置を行うことが必要となる。 また、 漏洩した個人情報の本人、 取引先などへの通知、 監督官庁等への報告、 ホームページやマスコミ等による公表についても検討する必要がある。

1. 中小企業における組織的な情報セキュリティ対策ガイドライン事例集【2012年9月3日IPA】

ドキュメントを参照: [03\_casestudy.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/03_casestudy.pdf)

* 1. Case 1. 従業員の情報持ち出し
     1. 様々な情報が分類・整理されていない
     2. 従業員が機密情報か否かを判別できない
     3. 重要な情報に誰でもアクセスできるようになっている（アクセス制御が出来ていない）
  2. Case 2. 退職者の情報持ち出し、 競合他社への就職
     1. 退職後の機密保持策や競業避止対策の未整備
     2. 営業秘密管理の不徹底
  3. Case 3. 従業員による私物PCの業務利用と Winnyの利用による業務情報の漏洩事故
     1. 業務に必要なPCを支給していなかった
     2. 規定の存在が周知されていなかった
     3. 守られることが期待されない実効性の低い社内規定の存在
     4. 情報が第三者に流出した場合も想定した対策の不備
  4. Case 4. ホームページへの不正アクセス
     1. 開発管理の不備
     2. 脆弱な運用体制
     3. 不十分な不正アクセス対策
     4. 事故対応体制の未整備
  5. Case 5. 無許可の外部サービスの利用
     1. 外部サービスの無許可利用
     2. 外部サービスのサービス内容についての不十分な理解
  6. Case 6. 委託した先からの情報漏えい
     1. 委託先管理の不十分さ
     2. 法令遵守に対する意識の低さ
  7. Case 7. 在庫管理システム障害の発生
     1. 事業継続への意識の低さ
  8. Case 8. 無線LANのパスワードのいい加減な管理
     1. 無線LANの危険性に対する認識の不足
     2. パスワード管理の重要性に対する認識の不足
  9. Case 9. IT管理者の不在
     1. 特定の個人や委託先のスキルに依存しすぎている
     2. 代替要員やマニュアル等の未整備
  10. Case 10. 電子メール経由でのウイルス感染
      1. ウイルス対策ソフト等の動作の確認を定期的にしていない
      2. ウイルス対策等が十分に出来ないPCへの考慮が不十分
      3. エンドユーザーがシステム構成等を変更することへの考慮が不十分
  11. 付録1：情報セキュリティ対策チェックリスト

1. 中小企業における情報セキュリティの普及促進に関する共同宣言

ドキュメントを参照: [20170207.html](https://www.ipa.go.jp/about/press/20170207.html)

* 1. 第四次産業革命の波が押し寄せる中、 急速に変化する社会に対応するために、 中小企業においてもITの利活用による新たな商品・サービスの開発、 業務の高度化・効率化等が重要になってくる
  2. しかし、 ITの利活用の進展と相まって、 サイバー攻撃・犯罪の巧妙化等により、 情報セキュリティ上の脅威がこれまで以上に悪質化・多様化してきている
  3. そのため、 中小企業におけるITの利活用の拡大に向け、 中小企業における情報セキュリティへの意識啓発及び自発的な対策の策定、 実践を推進するよう、 下記団体は連携して活動することを宣言する
  4. 連携団体
     1. 一般社団法人中小企業診断協会
     2. 全国社会保険労務士会連合会
     3. 全国商工会連合会
     4. 全国中小企業団体中央会
     5. 特定非営利活動法人ITコーディネータ協会
     6. 特定非営利活動法人日本ネットワークセキュリティ協会
     7. 独立行政法人情報処理推進機構
     8. 独立行政法人中小企業基盤整備機構
     9. 日本商工会議所
     10. 日本税理士会連合会

1. 特定個人情報の適正な取扱いに関するガイドラン （事業者編）（個人情報保護委員会）
2. 個人情報の 保護に関する法律ついての分野別 ガイドライン（各府省庁）
3. 秘密情報の保護ハンドブック（経済産業省）【旧版？】
4.  インシデント対応マニュアルの作成について（組織内CSIRT 構築の参考資料）【2015年JPCERT/CC】

ドキュメントを参照: [18\_incident\_response\_manual\_20151126.pdf](https://www.jpcert.or.jp/csirt_material/files/18_incident_response_manual_20151126.pdf)

1.   昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について【2020年6月12日METI】

ドキュメントを参照: [昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書を取りまとめました （METI/経済産業省）](https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html)