Sec01-02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

1. 改訂履歴
   1. 【2020年2月25日】再構成
   2. 【2020年2月14日】モバイルセキュリティ関連を整理し追加

参照: [モバイルセキュリティ関連](#モバイルセキュリティ関連)

* 1. 【2020年1月30日】ファイル種別追加
  2. 【2019年7月4日】IoT・5Gセキュリティ総合対策（案）追加
  3. 【2019年3月20日】ポータルサイト掲載分の更新（情報セキュリティ10大脅威2019, 中小企業の情報セキュリティ対策ガイドライン）
  4. 【2018年10月10日】
  5. 【2018年9月26日】Sec01-04を吸収

1. ファイル種別
   1. xmind→html版

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

* 1. MindManager→html版

ドキュメントを参照: [Sec01-02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.html](https://bluemoon55.github.io/Sharing_Knowledge/MindManager/Sec01-02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.html)

1. 【参考】「中小企業サイバーセキュリティ対策の極意ポータルサイト」掲載分

ドキュメントを参照: [cybersecurity-tokyo.jp](https://cybersecurity-tokyo.jp/)

* 1. 外部の情報紹介

ドキュメントを参照: [links](https://cybersecurity-tokyo.jp/links/)

* + 1. その1 情報サイト編
       1. ここからセキュリティ！ 情報セキュリティ・ポータルサイト【IPA】

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

* + - 1. 情報セキュリティ対策支援サイト【IPA】

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

* + - 1. 国民のための情報セキュリティサイト【総務省】

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

* + - 1. みんなでしっかりサイバーセキュリティ【NISC】

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

* + - * 1. ネットワークビギナーのための情報セキュリティハンドブック

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

* + 1. その2 ガイドライン編
       1. 中小企業の情報セキュリティ対策ガイドライン【IPA】

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

* + - * 1. https://www.ipa.go.jp/files/000072151.pdf

ドキュメントを参照: [000072151.pdf](https://www.ipa.go.jp/files/000072151.pdf)

* + - 1. サイバーセキュリティ経営ガイドライン【経済産業省】

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

* + - * 1. http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM\_Guideline\_v2.0.pdf

ドキュメントを参照: [CSM\_Guideline\_v2.0.pdf](http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf)

* + - * 1. https://www.ipa.go.jp/files/000056148.pdf

ドキュメントを参照: [000056148.pdf](https://www.ipa.go.jp/files/000056148.pdf)

* + 1. その3 情報収集編
       1. 情報セキュリティ10大脅威2019【IPA】

ドキュメントを参照: [10threats2019.html](https://www.ipa.go.jp/security/vuln/10threats2019.html)

* + - * 1. https://www.ipa.go.jp/files/000071831.pdf

ドキュメントを参照: [000065376.pdf](https://www.ipa.go.jp/files/000065376.pdf)

* + - 1. 企業（組織）における最低限の情報セキュリティ対策のしおり【IPA】

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

* + - * 1. https://www.ipa.go.jp/security/keihatsu/shiori/management/01\_guidebook.pdf

ドキュメントを参照: [01\_guidebook.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf)

* + 1. その4 個別案件編
       1. なりすましECサイト対策マニュアル【セーファインターネット協会】

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

* + - * 1. https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi\_manual.pdf

ドキュメントを参照: [narisumashi\_manual.pdf](https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi_manual.pdf)

* + - 1. IPAテクニカルウォッチ「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】

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

* + - * 1. https://www.ipa.go.jp/files/000066952.pdf

ドキュメントを参照: [000066952.pdf](https://www.ipa.go.jp/files/000066952.pdf)

* + - 1. 情報セキュリティサービス審査登録制度【IPA】

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

1. 【全般】啓発情報提供サイト
   1. 中小企業サイバーセキュリティ対策の極意ポータルサイト【東京都】

ドキュメントを参照: [cybersecurity-tokyo.jp](https://cybersecurity-tokyo.jp/)

* 1. ここからセキュリティ！ 情報セキュリティ・ポータルサイト【IPA】
     1. 官民ボードで運営
        1. Subtopic  
           
     2. 1.被害にあった？（侵害の予兆を含む）
        1. 02.ウイルスに感染したら（ランサムウェアを含む）
        2. 03.不正アクセス
        3. 04.情報漏えい
        4. 05.ワンクリック詐欺
        5. 06.フィッシング詐欺・なりすまし
           1. 061.フィッシング詐欺・なりすまし被害
           2. 062.なりすまされたECサイト
        6. 07.詐欺メール
           1. 071.迷惑メール
           2. 072.標的型攻撃メール
           3. 073.ビジネスメール詐欺
        7. 08.サービス妨害（DoS攻撃等）
        8. 09.嫌がらせ、 誹謗中傷
     3. 2.事前に対策を（事象毎の予防策）
        1. 01.対策の基本
           1. 011.企業における対策の基本
           2. 012.家庭で行う対策
           3. 013.子どもを守るための対策
        2. 02.ウイルス対策（ランサムウェアを含む）
        3. 03.不正アクセス対策
        4. 04.情報漏えい
        5. 05.ワンクリック詐欺
        6. 06.フィッシング詐欺・なりすまし
           1. 061.フィッシング詐欺・なりすまし被害
           2. 062.なりすまされたECサイト
        7. 07.詐欺メール
           1. 071.迷惑メール
           2. 072.標的型攻撃メール
           3. 073.ビジネスメール詐欺
        8. 08.サービス妨害（DoS攻撃等）
        9. 09.嫌がらせ、 誹謗中傷
        10. 10.個別対策項目
            1. 101.パスワード
        11. 20.ガイドライン等
            1. 201.教育機関向け
            2. 202.個人ユーザ向け
            3. 203.事業者向け
     4. 3.教育・学習
        1. 01.一般向け
           1. 011.小学生向け
           2. 012.中高校生向け
           3. 013.ホームユーザ向け
        2. 02.中小企業向け
        3. 03.経営者向け
        4. 04.システム管理者
        5. 05.一般社員・職員
     5. 4.セキュリティチェック
        1. 01.クイズ形式
        2. 02.安全性を診断しよう
        3. 03.試験・資格
     6. 5.データ＆レポート
        1. 01.参考になる資料、 情報サイト
  2. みんなでしっかりサイバーセキュリティ【NISC】

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

* 1. 基礎知識｜国民のための情報セキュリティサイト【総務省】

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

* + 1. インターネットを使ったサービス｜基礎知識｜国民のための情報セキュリティサイト【総務省】

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/service/index.html)

* + - 1. インターネットって何？
      2. インターネットの仕組み
      3. ホームページの仕組み
      4. 電子メールの仕組み
      5. ブログの仕組み
      6. 電子掲示板の仕組み
      7. SNS（ソーシャルネットワーキングサービス）の仕組み
      8. チャットの仕組み
      9. メーリングリストの仕組み
      10. ショッピングサイトの仕組み
      11. ネットオークションの仕組み
      12. インターネットバンキングの仕組み
      13. クラウドサービスとは？
      14. スマートフォンとは？
      15. 無線LANの仕組み
    1. どんな危険があるの？｜基礎知識｜国民のための情報セキュリティサイト【総務省】

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/index.html)

* + - 1. ウイルスとは？
      2. ウイルスの感染経路と主な活動
         1. ウイルスの感染経路
         2. ウイルスの主な活動
      3. 不正アクセスとは？
         1. ホームページやファイルの改ざん
         2. 他のシステムへの攻撃の踏み台に
      4. 詐欺等の犯罪
      5. 事故・障害
      6. 脆弱性（ぜいじゃくせい）とは？
      7. 情報発信に関するトラブル
    1. インターネットの安全な歩き方｜基礎知識｜国民のための情報セキュリティサイト【総務省】

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/risk/index.html)

* + - 1. IDとパスワード
         1. 認証の仕組みと必要性
         2. 設定と管理のあり方
      2. ウイルスに感染しないために
      3. 不正アクセスに遭わないために
      4. 詐欺や犯罪に巻き込まれないために
      5. 事故・障害への備え
      6. 情報発信の心得
    1. 情報セキュリティ関連の技術｜基礎知識｜国民のための情報セキュリティサイト【総務省】

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/structure/index.html)

* + - 1. ファイアウォールの仕組み
      2. 暗号化の仕組み
      3. SSLの仕組み
      4. ファイル共有ソフトとは？
    1. 情報セキュリティ関連の法律・ガイドライン｜基礎知識｜国民のための情報セキュリティサイト

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/legal/index.html)

* + - 1. 法律違反の事例
      2. 刑法
      3. サイバーセキュリティ基本法
      4. 著作権法
      5. 電気通信事業法
      6. 電子署名及び認証業務に関する法律
      7. 電子署名に係る地方公共団体の認証業務に関する法律
      8. 電波法
      9. 特定電子メールの送信の適正化等に関する法律
      10. 不正アクセス行為の禁止等に関する法律
      11. 有線電気通信法
  1. 一般利用者の対策｜国民のための情報セキュリティサイト【総務省】

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

* + 1. 基本的な対策

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/index.html)

* + - 1. ソフトウェアを最新に保とう
      2. ウイルス対策をしよう
         1. ウイルス対策ソフト
         2. 記憶媒体からのウイルス感染
      3. ホームページ閲覧の危険性
      4. パスワードの設定と管理
      5. フィッシング詐欺に注意
      6. ワンクリック詐欺に注意
      7. 無線LANの安全な利用
      8. 機器の廃棄
      9. 個人に関する情報の取扱い
      10. プライバシー情報の取扱い
      11. サポート期間が終了するソフトウェアに注意
      12. サーバ証明書の切り替えによる影響について
    1. インターネット上のサービス利用時の脅威と対策

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/index.html)

* + - 1. 【インターネット】
         1. ホームページ閲覧における注意点
         2. ネットオークションにおける危険性
         3. ショッピングサイトの利用
         4. インターネットバンキングの注意点
         5. SNS利用上の注意点
         6. クラウドサービス利用上の注意点
         7. 動画配信サイトなどの注意点
         8. オンラインゲームの注意点
      2. 【電子メール】
         1. ウイルス添付メールなどへの対応
         2. 迷惑メールへの対応
         3. チェーンメールの問題点
         4. メールの誤送信
      3. 【情報機器】
         1. 家族共用パソコンの注意点
         2. 携帯電話・スマートフォン・タブレット端末の注意点
         3. ゲーム機の注意点
         4. インターネット対応機器（家電、 記憶媒体等）の注意点
      4. 【その他】
         1. ファイル共有ソフトの利用とその危険性
    1. 情報発信の際の注意

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/attention/index.html)

* + - 1. 著作権侵害に注意
      2. 個人情報の公開の危険性
      3. ネットを使ったいやがらせや迷惑行為
      4. 発信内容は慎重に
    1. 事故・被害の事例

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/index.html)

* + - 1. 事例1：資料請求の情報が漏洩した
      2. 事例2：私の名前で誰かがメールを
      3. 事例3：ホームページを見ただけで・・・
      4. 事例4：猛威！デマウイルス
      5. 事例5：メールが他人に読まれている？
      6. 事例6：ネットストーカーに注意
      7. 事例7：ウイルス対策はしていたはずなのに・・・
      8. 事例8：送った覚えがないのに・・・
      9. 事例9：オークションの商品が届かない
      10. 事例10：メールの儲け話に注意
      11. 事例11：中古パソコンによるデータの漏洩
      12. 事例12：クレジットカード番号が盗まれた
      13. 事例13：ファイル共有ソフトが原因で・・・
      14. 事例14：ワンクリック詐欺に注意
      15. 事例15：自分の名前で勝手に書き込みが・・・
      16. 事例16：インターネットバンキングで情報が盗まれた
      17. 事例17：有名サイトからダウンロードしたはずなのに・・・
      18. 事例18：ブロードバンドルータから認証情報が盗まれた・・・
  1. 企業・組織の対策｜国民のための情報セキュリティサイト【総務省】

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

* + 1. 組織幹部のための情報セキュリティ対策

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/index.html)

* + - 1. 【技術的対策】
      2. 情報セキュリティ対策の必要性
      3. 情報セキュリティの概念
      4. 必要な情報セキュリティ対策
      5. 情報セキュリティマネジメントとは
         1. 情報セキュリティマネジメントの実施サイクル
         2. 情報セキュリティポリシーの概要と目的
         3. 情報セキュリティポリシーの内容
         4. 情報セキュリティポリシーの策定
         5. 情報セキュリティ教育の実施
         6. 情報セキュリティポリシーの評価と見直し
         7. 事故やトラブル発生時の対応
      6. 個人情報取扱事業者の責務
    1. 社員・職員全般の情報セキュリティ対策

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/index.html)

* + - 1. 安全なパスワード管理
      2. ソフトウェアの情報セキュリティ対策
      3. ウイルス対策
      4. 電子メールの誤送信
      5. 標的型攻撃への対策
      6. 悪意のあるホームページ
      7. バックアップ
      8. 安全な無線LANの利用
      9. 廃棄するパソコンやメディアからの情報漏洩（ろうえい）
      10. 外出先で業務用端末を利用する場合の対策
      11. 持ち運び可能なメディアや機器を利用する上での危険性と対策
      12. ソーシャルエンジニアリングの対策
      13. クラウドサービス利用時の注意点
      14. SNS利用上の注意点
    1. 情報管理担当者の情報セキュリティ対策

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/index.html)

* + - 1. 【技術的対策】
         1. ソフトウェアの更新
         2. ウイルス対策
         3. ネットワークの防御
         4. 不正アクセスによる被害と対策
         5. 外出先で業務用端末を利用する場合の対策
         6. SQLインジェクションへの対策
         7. 標的型攻撃への対策
         8. 安全な無線LAN利用の管理
         9. ユーザ権限とユーザ認証の管理
         10. バックアップの推奨
         11. セキュリティ診断
         12. ログの適切な取得と保管
         13. サポート期間が終了するソフトウェアに注意
      2. 【情報セキュリティポリシー】
         1. 情報セキュリティポリシーの導入と運用
         2. ソーシャルエンジニアリングの対策
         3. クラウドサービスを利用する際の情報セキュリティ対策
         4. SNSを利用する際の情報セキュリティ対策
         5. 社員の不正による被害と対策
         6. 廃棄するパソコンやメディアからの情報漏洩
         7. 持ち運び可能な記憶媒体や機器を利用する上での危険性と対策
      3. 【物理セキュリティ】
         1. サーバの設置と管理
         2. 機器障害への対策
    1. 事故・被害の事例

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/case/index.html)

* + - 1. 事故・被害の事例
         1. 事例1：資料請求の情報が漏洩した
         2. 事例2：ホームページが書き換えられた
         3. 事例3：顧客のメールアドレスが漏洩
         4. 事例4：他人のIDで不正にオンライン株取引
         5. 事例5：中古パソコンによるデータの漏洩
         6. 事例6：情報セキュリティ対策は万全だったはずなのに・・・
         7. 事例7：ファイル共有ソフトが原因で・・・
         8. 事例8：SQLインジェクションでサーバの情報が・・・
         9. 事例9：標的型攻撃で、 企業の重要情報が・・・
         10. 事例10：自分の名前で勝手に書き込みが・・・
         11. 事例11：公式アカウントが乗っ取られた
         12. 事例12：有名サイトからダウンロードしたはずなのに・・・
         13. 事例13：クラウドサービスに預けていた重要データが消えた
    1. 脆弱性の注意喚起

ドキュメントを参照: [index.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/vulnerability/index.html)

* + - 1. Internet Explorerの脆弱性について
      2. Apache Strutsの脆弱性について
      3. OpenSSLの脆弱性について
  1. @police－被害事例と対処法【警察庁】

ドキュメントを参照: [index.html](http://www.npa.go.jp/cyberpolice/case/pc/index.html)

* + 1. PCユーザ 被害事例と対処法

ドキュメントを参照: [index.html](http://www.npa.go.jp/cyberpolice/case/pc/index.html)

* + - 1. ID・パスワードを盗まれて「なりすまし」に遭った
      2. 身に覚えのない料金請求をされた
      3. パソコンのハードディスクの中身がインターネット上に公開された
      4. 携帯電話の情報が勝手に登録された
      5. Keylogger（キーロガー）によって個人情報を盗まれた
      6. フィッシング詐欺に遭った
      7. 会社の顧客情報が流出した
      8. 身に覚えの無い国際電話利用料金の請求が来た
      9. 有料サイトの利用料金を請求するメールが来た
      10. インターネットを利用中に、 ブラウザクラッシャーに遭った
      11. ネットストーカーに困っている
      12. 悪徳商法やネット詐欺にあった
      13. 掲示板に個人情報を書き込まれた
      14. パソコンがウイルスに感染してしまった
      15. 迷惑メールが来たがどうすれば良いか
    1. システム/ネットワーク管理者 被害事例と対処法

ドキュメントを参照: [index.html](http://www.npa.go.jp/cyberpolice/case/server/index.html)

* + - 1. 自組織内の機密情報が、 ファイル共有ソフトにより流出した
      2. 組織内で管理する個人情報がスタッフによって外部へ流出した
      3. Webサイトの掲示板に、 悪意のある書き込みを大量にされた
      4. 自組織のドメイン名に詐称された迷惑メールをばらまかれた
      5. 自分が管理する掲示板上の書き込みに対して削除を求められた
      6. 他組織のホストへウイルスを感染させてしまった
      7. サーバがウイルスに感染してしまった
      8. サーバがクラックされ、 ページが書き換えられた
      9. スパムメールの踏み台にされた
      10. DoS攻撃を受けて、 サーバが利用不能になった
      11. サーバに侵入され個人情報が流出した

1. 一般ユーザ向け【零細企業を含む】
   1. インターネットを安全に利用するための情報セキュリティ対策９か条 【NISC・IPA】

ドキュメントを参照: [leaflet\_20150201.pdf](http://www.nisc.go.jp/security-site/files/leaflet_20150201.pdf)

* + 1. OS やソフトウェアは常に最新の状態にしておこう
       1. 新たにひろまるコンピュータウイルスに対抗するため製造元から 無料で配布される最新の改良プログラムにアップデートしましょう。
    2. パスワードは貴重品のように管理しよう
       1. パスワードは自宅の鍵と同じく大切です。 パスワードは他人に知られないように、 メモをするなら人目に触れない場所に保管しましょう。
    3. ログインID・パスワード絶対教えない用心深さ
       1. 金融機関を名乗り、 銀行口座番号や暗証番号、 ログインIDやパスワード、 クレジットカード情報の入力を 促すような身に覚えのないメールが届いた場合、 入力せず無視しましょう。
    4. 身に覚えのない添付ファイルは開かない
       1. 身に覚えのない電子メールにはコンピュータウイルスが潜んでいる可能性があります。 添付されたファイルを開いたり、 URL（リンク先）をクリックしないようにしましょう。
    5. ウイルス対策ソフトを導入しよう
       1. ウイルスに感染しないように、 コンピュータにウイルス対策ソフトを導入しましょう。 （家電量販店などで購入できます）
    6. ネットショッピングでは信頼できるお店を選ぼう
       1. 品物や映画や音楽も購入できるネットショッピング。 詐欺などの被害に遭わないように信頼できるお店を選びましょう。 身近な人からお勧めのお店を教わるのも安心です。
    7. 大切な情報は失う前に複製しよう
       1. 家族や友人との思い出の写真など、 大切な情報がパソコンの故障によって失われることのないよう、 別のハードディスクなどに複製して保管しておきましょう。
    8. 外出先では紛失・盗難に注意しよう
       1. 大切な情報を保存したパソコン、 スマートフォンなどを自宅から持ち出すときは機器やファイルにパスワードを設定し、 なくしたり盗まれないように注意て持ち歩きましょう。
    9. 困ったときはひとりで悩まず まず相談
       1. 詐欺や架空請求の電子メールが届く、 ウイルスにより開いているウェブページが閉じないなどの被害に遭遇したら、 一人で悩まず各種相談窓口に相談しましょう。
  1. ネットの危険からお子様を守るために、 保護者ができる3つのポイント 【2017年4月6日政府広報】

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html)

* + 1. 1.自分の携帯電話やスマートフォンを持つ子供が増えている

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#section2)

* + 1. 2.子供たちのインターネット利用に潜む危険

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#section2)

* + 1. 3.保護者ができる3つのポイント

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#section3)

* + 1. ポイント1　被害者にも加害者にもしないために、 適切なインターネットの利用を促しましょう

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#point1)

* + 1. ポイント2　家庭のルールをお子様と一緒に作り、 成長と共に少しずつ改定していきましょう

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#point2)

* + 1. ポイント3　不適切な情報や危険な出会い等を防ぐために、 フィルタリングを賢く利用しましょう

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#point3)

* + 1. 子供の携帯電話利用に関するトラブルの例

ドキュメントを参照: [3.html](http://www.gov-online.go.jp/useful/article/201303/3.html#column1)

* + - 1. 総務省「インターネットトラブル事例集」

ドキュメントを参照: [jireishu.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/jireishu.html)

* + 1. 関連リンク
       1. 内閣府「青少年有害環境対策（青少年のインターネット利用環境整備を含む）」

ドキュメントを参照: [index.html](http://www8.cao.go.jp/youth/youth-harm/index.html)

* + - 1. 総務省「インターネットトラブル事例集」

ドキュメントを参照: [jireishu.html](http://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/jireishu.html)

* + - 1. 総務省「国民のための情報セキュリティサイト」

ドキュメントを参照: [index.htm](http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm)

* + - 1. 法務省「インターネットを悪用した人権侵害をなくしましょう」

ドキュメントを参照: [jinken88.html](http://www.moj.go.jp/JINKEN/jinken88.html)

* 1.  ネットワークビギナーのための情報セキュリティハンドブックVer.2.11（小冊子） 【2017年02月08日NISC】

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

* + 1. 電子書籍【無料】【2017年７月13日】
       1. ibooksStore、 Kindle ストア、 ebookjapan、 BOOKFAN、 コミックシーモア、 d ブック、 ひかりTV ブック、 music.jp 、 DMM.com 、 Kinoppy 、 Yahoo! ブックストア、 GooglePlay ブックス、 GALAPAGOS STORE、 セブンネットショッピング、 honto、 漫画全巻ドットコム、 Dijital ehon、 ニコニコ静画、 cdjapan eBooks 、 Neowing eBooks 、 フジテレビオンデマンド、 BOOKWALKER、 BookLive!、 ブックパス、 ReaderStore、 BookPlace、 楽天Kobo
       2. https://www.amazon.co.jp/

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

* + 1. PDF版【2017年02月08日】
       1. 全体版（68.8MB）

ドキュメントを参照: [handbook-all.pdf](https://www.nisc.go.jp/security-site/files/handbook-all.pdf)

* + - 1. 部分版（各章別）
      2. プロローグ　サイバー攻撃ってなに？（7.5MB）

ドキュメントを参照: [handbook-prologue.pdf](https://www.nisc.go.jp/security-site/files/handbook-prologue.pdf)

* + - 1. 第1章　基本のセキュリティ～ステップバイステップでセキュリティを固めよう～（19.5MB）

ドキュメントを参照: [handbook-01.pdf](https://www.nisc.go.jp/security-site/files/handbook-01.pdf)

* + - 1. 第2章　セキュリティを理解して、 ネットを安全に使う（7.0MB）

ドキュメントを参照: [handbook-02.pdf](https://www.nisc.go.jp/security-site/files/handbook-02.pdf)

* + - 1. 第3章　スマホ・パソコンのより進んだ使い方やトラブル対処の仕方（13.0MB）

ドキュメントを参照: [handbook-03.pdf](https://www.nisc.go.jp/security-site/files/handbook-03.pdf)

* + - 1. 第4章　被害に遭わないために、 知らない間に加害者にならないために（6.3MB）

ドキュメントを参照: [handbook-04.pdf](https://www.nisc.go.jp/security-site/files/handbook-04.pdf)

* + - 1. 第5章　自分を守る、 家族を守る、 災害に備える（12.8MB）

ドキュメントを参照: [handbook-05.pdf](https://www.nisc.go.jp/security-site/files/handbook-05.pdf)

* + - 1. エピローグ　来たるべき新世界（4.6MB）

ドキュメントを参照: [handbook-epilogue.pdf](https://www.nisc.go.jp/security-site/files/handbook-epilogue.pdf)

* + - 1. 用語集・情報セキュリティ関連サイト一覧・索引（2.1MB）

ドキュメントを参照: [handbook-glassary.pdf](https://www.nisc.go.jp/security-site/files/handbook-glassary.pdf)

* + 1. 目次
       1. 人物紹介
       2. おうちのCSIRTになってね
       3. Black Hat the Cracker
    2. プロローグ サイバー攻撃ってなに？誰がやっているの？どんなことが起こるの？～サイバー攻撃のイメージ
       1. S1. サイバー攻撃のイメージ
          1. S1. サイバー攻撃って誰がやっているの？どうするの？
          2. コラム：攻撃者とハッカーとクラッカー
          3. コラム：攻撃者が使う武器「マルウェア」

どんな種類があるの？

どんな機能を持つの？

どんなものが感染したり、 感染させたり、 悪さするようになるのか

* + - * 1. S2. サイバー攻撃の例

偽サイトでのフィッシング詐欺や重要情報の不正送信

ランサムウェアで身代金要求

ボットネットに組み込まれる

* + - * 1. S3. サイバー関連の犯罪やトラブル

なりすましや略取・誘拐（連れ去り）

セクスティング

ネットいじめ

* + - * 1. S4. 人の心の隙を突く「ソーシャルエンジニアリング」攻撃

「ソーシャルエンジニアリング」は現実でもネットでも心の隙を突いてだます

* + 1. 第1章 基本のセキュリティ～ステップバイステップでセキュリティを固めよう！
       1. S1. 4つのポイントでセキュリティを守る
          1. P1. システムを最新に保つ。 セキュリティソフトを入れて防ぐ

様々な段階でセキュリティを守る

* + - * 1. P2. 複雑なパスワードと多要素認証で侵入されにくくする
        2. P3. 攻撃されにくくするには侵入に手間（コスト）がかかるようにする

守りを何重にもして侵入されにくくする

* + - * 1. P4. 心の隙を作らないようにする（対ソーシャルエンジニアリング）
      1. S2. 環境を最新に保つ、 セキュリティソフトを導入する
         1. P1. セキュリティソフトを導入して守りを固めよう

単純なウイルス検知ソフト

進化したセキュリティソフト（ふるまい検知、 ヒューリスティック分析）

手配書が間に合わないゼロディ攻撃も

* + - * 1. P2. パソコン本体とセキュリティの状態を最新に保とう

本体もOSもセキュリティソフトも重要ソフトもアップデート

* + - * 1. P3. スマートフォンやネットワーク機器も最新に保とう

アプリやセキュリティソフトの更新は基本的に自動にし、 まめにチェック

ネットにつながる家電もファームウェア更新、 設定ページのID・パスワードは変更しておくこと

* + - * 1. P4. ソフトやアプリは信頼できる場ところ所から。 権限にも気をつける

不審な場所からアプリをインストールしない。 権限に気をつける

* + - * 1. コラム：必要ならばスマホにはセキュリティパックを検討しよう

必要性を感じるなら、 スマホにはセキュリティパック導入を検討しよう

スマホの改造をしてはいけません

スマート家電の中にはパソコンやスマホがある？

* + - * 1. コラム：パソコンやスマホを最新の状態に保っても防げない攻撃がある。 それがゼロディ攻撃！

ゼロディ攻撃とは？ 対処の例

ゼロディ攻撃に対抗するには？

* + - 1. S3. 複雑なパスワードと多要素認証で侵入されにくくする
         1. P1. パスワードの安全性を高める

パスワードは少なくとも英大文字小文字＋数字＋記号で10桁

* + - * 1. P2. パスワードの使い回しをしない

同じパスワードを使い回さない。 似たパスワード、 法則性のあるパスワードはｘ

* + - * 1. P3. パスワードを適切に保管する

パスワードを使用する場所に置かない。 パソコンの中もｘ

パスワードはノートに書いて保管するか、 パスワード管理アプリで守る

ブラウザの自動入力にパスワードを覚えさせない

* + - * 1. P4. 秘密の質問にはまじめに答えない。 多要素や生体認証を使う

秘密の質問にはまじめに答えない。 答えは使い回さない

多要素認証やログイン通知でセキュリティを向上

* + - * 1. コラム：パスワードはどうやって漏れるの？どう使われるの？

様々なID・パスワードの抜き取り方法

盗んだID・パスワードを使い様々なサービスを乗っ取れるか試す

* + - 1. S4. 攻撃されにくくするには、 手間（コスト）がかかるようにする
         1. 攻撃されにくくするには手間がかかるようにする
         2. 金銭目的ではない攻撃にも備えよう
         3. 攻撃者に操られて内側から鍵を開けてしまわないように心がまえを持とう
      2. S5. 心の隙を作らないようにする（対ソーシャルエンジニアリング）
         1. 古典的なソーシャルエンジニアリング
         2. デジタル世代のソーシャルエンジニアリング
         3. 標的型メールの例
         4. フィッシングメールの例
         5. 悪意はないが拡散してしまう例
         6. コラム：軍事スパイ、 産業スパイに狙われてしまったら

職業スパイにはコストによる防御が効かない

スパイ活動の今昔

* + - * 1. コラム：映画「ザ・ハッカー」にみるソーシャルエンジニアリング
        2. コラム：スパムメールとその由来
    1. 第2章セキュリティを理解して、 ネットを安全に使う
       1. S1. パスワードを守る、 パスワードで守る
          1. P1. パスワードってなに？
          2. P2. 3種類の「パスワード」を理解する

1を「PINコード」

2を「ログインパスワード」

3を「暗号キー」

* + - * 1. P3. 「PI Nコード」と「ログインパスワード」に求められる複雑さの違い
        2. P4. 「暗号キー」に求められる複雑さ
        3. P5. どちらの「パスワード」か、 わかりにくい例

トピック：パスワードを破る手段は色々

ブルートフォース攻撃（総当たり攻撃）

リスト型攻撃（アカウントリスト/パスワードリスト攻撃）

辞書攻撃（ディクショナリアタック）

* + - * 1. P6. 総当たり攻撃以外のパスワードを破る攻撃や生体認証を使った防御

トピック：多要素認証の構成要素は？

①知っているもの

②持っているもの

③本人自身に関するもの

トピック：指紋認証が破られることも

* + - * 1. P7. パスワードの定期変更は必要なし。 流出時は速やかに変更する
        2. P8. パスワード流出時の便乗攻撃に注意
        3. P9. 厳重なパスワードの保管

トピック：ブラウザにはパスワード保存しない

トピック：パスワード管理方法の例

トピック：パスワード管理方法のメリットデメリット

* + - * 1. P10. パスワード情報をクラウドで利用する善し悪し
        2. P11. ノートやスマホを失くした場合のリカバリ考察
        3. P12. 次善の策のソーシャルログイン。 二段階認証などで防御
        4. P13. ソーシャルログインで連携される情報に注意

トピック：ソーシャルログインに使えるアカウント

二段階認証

ログイン通知

トピック：ソーシャルログインとサービス・アプリ連携の違い

ソーシャルログイン

アプリ・サービス連携

トピック：アプリなどの連携は定期的に棚卸ししよう

* + - * 1. P14. ソーシャルログインとは性格が違うサービス連携
        2. コラム：暗号化の超簡単説明

トピック：暗号化ってなに？

平文での通信は読めてしまう

暗号化の魔法は内容を読めなくする

暗号化したものを送れば攻撃者が読めない

事前に決めておいた方法（暗号化方法）と呪文（「暗号キー」）で暗号文を復元（復号）する

トピック：暗号が破られる場合

暗号化方法の種類はいろいろ

暗号破られ①　呪文がバレている！

暗号破られ②　方法が古くて解読可能！

暗号破られ③　呪文が簡単すぎて解読される

* + - 1. S2. 通信を守る、 無線LANを安全に利用する
         1. P1. それぞれの状況に合わせた暗号化の必要性

トピック：それぞれの状況に合わせた暗号化

通信の暗号化

ファイルの暗号化

* + - * 1. P2. 無線LAN通信(Wi-Fi)の構成要素

トピック：暗号を使う無線LANの構成要素

トピック：公衆無線LANが安全とは限らない

トピック：「暗号キー」共有は接続しちゃダメ

* + - * 1. P3. 暗号化なしや、 方式が安全ではないものは危険
        2. P4. 暗号化方式が安全でも「暗号キー」が漏れれば危険
        3. P5. 家庭内での安全な無線LANの設定（暗号化方式
        4. P6. 家庭内での安全な無線LANの設定（その他

トピック：家庭でのWi-Fiの利用

①出荷時の管理者パスワード、 「暗号キー」の変更

②「暗号キー」は家族のヒミツ

③ルータと機器の安全な運用

* + - * 1. P7. 公衆無線LAN の安全な利用
        2. P8. 個別の「暗号キー」を用いる方式の無線LAN
        3. P9. 公衆無線LAN に関して新規に購入したスマホなどで行うこと

トピック：公衆無線LAN通信の表示の意味

①スマホやパソコンの画面から見た無線LAN暗号化

②詳細な区分けから見た無線LAN暗号化

トピック：新しいスマホを購入したら

* + - * 1. P10. 公衆無線LAN が安全ではない場合の利用方法
        2. P11. 自前の暗号化による盗聴対策
        3. P12. まとめて暗号化するVPN、 現状は過信できないが今後に期待

トピック：様々な場所から安全なアクセスを可能にするVPN新しいスマホを購入したら

①詳細なVPNのイメージ

②簡単なVPNのイメージ

* + - 1. S3. ウェブを安全に利用する、 暗号化で守る
         1. P1. 無線LAN の暗号化とVPNの守備範囲

トピック：それぞれの暗号化の守備範囲

①無線LANの暗号化

②VPNによる暗号化

③ウェブ、 メールの暗号化

④VPN＋ウェブメールの暗号化

* + - * 1. P2. 全ての通信と、 その一部であるウェブの通信
        2. P3. httpsで始まる暗号化通信にはどんなものがあるか
        3. P4. より厳格な審査の「EVSSL証明書
        4. P5. 「EV-SSL証明書」を持つサイトを見分ける方法
        5. P6. 有効期限が切れた証明書は拒否する
        6. P7. 他にも証明書に関する警告が出るサイトは接続しない
        7. P8. ウェブサービスのログインは二段階認証などを使う

トピック：httpsの暗号化通信で情報を守る

個人情報の入力は基本的には

トピック：攻撃者が不正に取得した証明書に注意

トピック：証明書の内容をチェックする

* + - * 1. P9. 二段階認証を破る「中間者攻撃」

トピック：間に入ってなりすます中間者攻撃の例

①中間者攻撃で二段階認証が破られる例

②中間者攻撃で二段階認証が破られにくい例

トピック：ウェブを使ったサイバー攻撃の例

①メール等による感染

②水飲み場攻撃による感染

* + - * 1. P10. ウェブを使ったサイバー攻撃に対応する
      1. S4. メールを安全に利用する、 暗号化で守る
         1. P1. メールにおける暗号化
         2. P2. スパムメールの嵐と、 メールの暗号化
         3. P3. 受信側も暗号化で保護
         4. P4. メールにおける暗号化の守備範囲

トピック：メールの送受信は暗号化されているか

メールソフトやアプリが暗号化（SSL）利用になっているか？

トピック：しかしSSLの通信は自分のサーバまで

トピック：暗号化している同じサービスを利用する

* + - * 1. P5. 暗号化から見たウェブメールの利用と、 同一サービス内の暗号化
        2. P6. 怪しいメールとはなにか.. .
        3. P7. マルウェア入りの添付ファイルに気をつける

トピック：ウェブメールの送受信は暗号化されているか

トピック：怪しいメールとはなにか

①仕事のメールを装う

② 銀行、 カード会社、 ECサイト、 プロバイダ関係を装うメール

トピック：本当の仕事仲間のメールでも攻撃は来る

* + - * 1. P8. メールアドレスのウェブサービスなどからの流出
        2. P9. 流出・スパム対策としての、 変更可能メールアドレスの利用
        3. P10. 通信の安全と永続性を考えたSNSやメールの利用

トピック：マルウェア入りファイルの偽装

トピック：メールアドレスを変えてスパムメールから逃げる

* + - 1. S5. データファイルを守る、 暗号化で守る
         1. トピック：データの暗号化は保険
         2. トピック：データを持ち運ぶときは必ず暗号化メディアを使う
         3. トピック：「暗号キー」が1個の方式（共通鍵暗号方式）
         4. トピック：「暗号キー」が2個の方式（公開鍵暗号方式）
         5. コラム：クラウドサービスからのデータ流出。 原因は？
    1. 第3 章 スマホ・パソコンのより進んだ使い方やトラブルの対処の仕方
       1. 1. スマホのセキュリティ設定.. .
          1. 1 スマホにはロックをかけよう。 席において離れたり、 人に貸したりするのはｘ
          2. 2 情報漏れを防ぐ①
          3. 3 情報漏れを防ぐ②
          4. 4 スムーズな機種変更と、 予期せぬデータ流出の防ぎ方
          5. 5 防水機能を過信してデータを失わないように
          6. コラム：GPS、 位置情報、 ジオタグの管理
       2. 2. パソコンのセキュリティ設定..
          1. 1 パソコンを買ったら初期設定などを確実に
          2. 2 暗号化機能等でセキュリティレベルを高める
          3. 3 マルウェア感染に備え、 バックアップ体制を整える
          4. 4 売却や廃棄するときはデータを消去する
          5. 5 盗難や紛失のとき、 スマホとパソコン、 どっちが安全？
          6. コラム：ダブルラインでトラブルに備える
       3. 3. 屋外・海外でのネットワーク利用..
          1. 1 一見なにもないように見えて、 危険がいっぱい
          2. 2 インターネットカフェの利用
       4. 4. それでも攻撃を受けてしまったときの対処..
          1. 1 兆候に気をつけて被害が出たら対処
          2. コラム：究極の防御手段「ネットにつながない」エアギャップ

有線でも無線でも、 つながっていないパソコンにはマルウェアは感染しない

しかし、 USBメモリを介して感染することも

ネットに接続していなくても、 少量のデータであれば盗める

オンラインで銀行口座が狙われるなら

インターネットバンキングを止めるという手も

* + - * 1. コラム：無料ということの意味は何か

試食サービスのコストの例

無料ウェブサービスの例

無料の公衆無線LANサービスの例

* + 1. 第4章 被害に遭わないために、 知らない間に加害者にならないために
       1. 1. 攻撃者に乗っ取られるとこんなことが起こる
          1. 1 被害に遭わない、 そして加害者にならないために
          2. 2 盗まれた情報は犯罪に使われる
          3. 3 乗っ取られた機器はサイバー攻撃に使われる
          4. 4 IoTも乗っ取られる。 知らずにマルウェアの拡散も
       2. 2. サイバー関連でやってはいけないこと
          1. 1 アニメ・マンガ・音楽の違法なシェア。 パクリなどの著作権侵害
          2. 2 ゲームの不正行為。 恋人や家族でもプライバシーは守る
          3. 3 クラッキングはクールじゃない！
          4. コラム：モラルを逸脱すると炎上を生む

モラルを逸脱することが炎上を生む

自作自演やアオリ行為、 嘘の書き込み

* + 1. 第5 章 自分を守る、 家族を守る、 災害に備える
       1. 1. SNSやネットとのつきあい方、 守り方
          1. 1 SNSやネットの楽しみと気をつけること
          2. 2 SNSやネットの怖さ、 こんなことが実際に起こっている

略取

ストーカー

犯罪勧誘

ネットいじめ

リベンジポルノ・デジタルタトゥー

* + - * 1. 3 SNSやネットとのつきあい方の基本

個人情報は基本的に公開しない

会ったことがない人とむやみに友だちにならない

現実世界で会おうとする人を警戒する。 出会い系に近づかない

個人が特定される情報はSNSなどに投稿しない

* + - * 1. 4 存在するデータは流出することがある。 流出したら消すことは難しい
        2. コラム：SNSや学校裏サイトを使ったいじめに備える（いじめ経験者からのアドバイス）
        3. コラム：デマに踊らされない！　ソースを探せ！　確かめよう！
      1. 2. デジタルテクノロジーで家族を守る.. .
         1. 1 子ども達を守る
         2. 2 お年寄りを守る
      2. 3. 大災害やテロに備える..
         1. 1 まずは自分の身の安全を確保する
         2. 2 電池をもたす、 情報収集をする
         3. 3 ラジオ、 ワンセグを使った情報収集
         4. 4 徒歩帰宅。 海外での災害やテロに備えて
         5. コラム：屋外でのゲームを安全に楽しむ
         6. 5 ネットを使わない移動トレーニング（現代オリエンテーリング）
         7. コラム：デジタル遺産相続
    1. エピローグ 来たるべき新世界
       1. 1 ネットの「今」と、 どう守っていくか
       2. 2 デジタルネイティブと未来
       3. 3 バーチャル空間を超えて世界へ
       4. 4 おわりに
    2. 用語集.
    3. 情報セキュリティ関連サイト一覧
       1. 情報セキュリティ関連のサイト
       2. 海外旅行関連のサイト
       3. 災害時関連のサイト
       4. 災害時関連のサイト
       5. いじめ対策関連
       6. Twitterアカウント
       7. アプリ（Android、 iOS）
       8. その他
    4. 索引..
  1. マンガで学ぶサイバーセキュリティ【NISC】【初心者向け】

ドキュメントを参照: [CSmanga\_JPN.pdf](http://www.nisc.go.jp/security-site/files/CSmanga_JPN.pdf)

* + 1. スマートフォンのセキュリティ
       1. 注意点
          1. 最近ではパソコンだけでなく、 スマートフォンでも悪意のあるウイルスが横行している
          2. ウイルス感染は「無料のアプリ」からが多い
          3. OSやアプリのバージョンが古いままだと、 ウイルス感染の危険性あり
       2. 対策
          1. スマートフォンへのウイルス対策ソフトの導入を検討しよう
          2. アプリの詳細、 提供企業やレビューを確認し、 信頼できるサイトからアプリをダウンロードしよう
          3. OSやアプリは常に最新のバージョンにアップデートしよう
       3. 豆知識
          1. 最近ではマンガのような、 画面をロックしてお金を要求するウイルス（ランサムウェアと呼ぶ）が流行している
          2. スマートフォンだけでなく、 PCも被害が出ているので注意しよう
          3. 迷惑メールの添付ファイルを実行すると、 ウイルスに感染してしまうこともあるため、 注意しよう
    2. 無線LANのセキュリティ
       1. 注意点誰でも接続できる無線LANのアクセスポイントの中には、 悪意をもって設置されているものがある
          1. 悪意をもって設置されたアクセスポイントに接続すると、 通信内容を見られてしまうことがある
          2. インターネット接続業者が提供している公衆無線LANでも、 通信が暗号化などで保護されていないものがあり、 通信内容が傍受されるおそれがある
       2. 対策
          1. 不審な公衆Wi-Fiには接続しない
          2. 公衆Wi-Fiに接続する場合は、 出来るだけ暗号化された、 信頼できるWi-Fiを利用しよう
       3. 豆知識
          1. ファイル共有機能をONにして公衆Wi-Fiに接続すると、 同じWi-Fiにつないでいる人からデータが見られてしまう
          2. 公衆Wi-Fiを使う場合は、 設定に注意しよう
          3. 自宅のWi-Fiにはきちんとパスワードをかけ、 知らない人が接続できないようにしよう
    3. インターネット上の詐欺
       1. 注意点
          1. インターネット上には、 ネットショッピングやインターネットバンキング等を利用する上で、 お金に関する詐欺が存在する
          2. ユーザを巧妙な偽サイト（フィッシングサイト）に誘導して騙す手法も増加している
          3. 安易にjメールを信用してUrlや添付ファイルを開くと、 偽物のサイトに飛んでしまったり、 ウイルスに感染してしまうことがある
       2. 対策
          1. ウェブサイトのURLやメール所送付先が正規のものか、 注意深く確認しよう
          2. 言語がカタコトだったり。 連絡先が書いていないなど、 疑わしいサイトは利用しない
       3. 豆知識
          1. フィッシングサイトでは銀行のウェブサイトを模倣して、 インターネットバンキングのIDやパスワードを盗むものも多く存在するため、 注意しよう。
    4. SNSの利用上の注意
       1. 注意点
          1. SNSでは、 悪意のあるユーザが、 女性などの画像を使用してなりすまし、 接触を図ってくることがある
          2. 悪意のあるユーザは「直接会おう」などと接近してくることもあり、 犯罪に巻き込まれることもある
       2. 対策
          1. 見知らぬユーザとは、 コンタクトをとらない
          2. 「会おう」などと誘われても絶対に会わない
       3. 豆知識
          1. 見知らぬ人が接触してくるのは、 悪事を目的としていることが多い
          2. 見知らぬ人が写真や住所、 電話番号など、 個人情報を要求してくることもあるが、 決して応じないこと
          3. 知り合いに成りすまして接近してくることも有るので、 知っている人だからと言って油断しない
  1. IPA 対策のしおり【IPA】

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

* + 1. IPA対策のしおりシリーズ
       1. ウイルス対策のしおり（第10版）PDF（815KB）

ドキュメントを参照: [01\_virus.pdf](https://www.ipa.go.jp/security/antivirus/documents/01_virus.pdf)

* + - 1. スパイウェア対策のしおり（第10版）PDF（822KB）

ドキュメントを参照: [02\_spyware.pdf](https://www.ipa.go.jp/security/antivirus/documents/02_spyware.pdf)

* + - 1. ボット対策のしおり（第10版）PDF（1.0MB）

ドキュメントを参照: [03\_bot.pdf](https://www.ipa.go.jp/security/antivirus/documents/03_bot.pdf)

* + - 1. 不正アクセス対策のしおり（第6版）PDF（779KB）

ドキュメントを参照: [04\_fusei.pdf](https://www.ipa.go.jp/security/antivirus/documents/04_fusei.pdf)

* + - 1. 情報漏えい対策のしおり（第7版）PDF（795KB）

ドキュメントを参照: [05\_roei.pdf](https://www.ipa.go.jp/security/antivirus/documents/05_roei.pdf)

* + - 1. インターネット利用時の危険対策のしおり（第4版）

ドキュメントを参照: [06\_kiken.pdf](https://www.ipa.go.jp/security/antivirus/documents/06_kiken.pdf)

* + - 1. 電子メール利用時の危険対策のしおり（第4版）PDF（1.1MB）

ドキュメントを参照: [07\_mail.pdf](https://www.ipa.go.jp/security/antivirus/documents/07_mail.pdf)

* + - 1. スマートフォンのセキュリティ<危険回避>対策のしおり

ドキュメントを参照: [08\_smartphone.pdf](https://www.ipa.go.jp/security/antivirus/documents/08_smartphone.pdf)

* + - 1. 初めての情報セキュリティ対策のしおり（第1版）

ドキュメントを参照: [09\_hazimete.pdf](https://www.ipa.go.jp/security/antivirus/documents/09_hazimete.pdf)

* + - * 1. スライド版PDF（2.4MB）

ドキュメントを参照: [09\_hazimete\_slide.pdf](https://www.ipa.go.jp/security/antivirus/documents/09_hazimete_slide.pdf)

* + - 1. 標的型攻撃メール<危険回避>対策のしおり（第1版）PDF

ドキュメントを参照: [10\_apt.pdf](https://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf)

* + - 1. 無線LAN<危険回避>対策のしおり（第1版）

ドキュメントを参照: [11\_wireless\_lan.pdf](https://www.ipa.go.jp/security/antivirus/documents/11_wireless_lan.pdf)

* + - 1. 暗号化による<情報漏えい>対策のしおり（第1版）

ドキュメントを参照: [12\_crypt.pdf](https://www.ipa.go.jp/security/antivirus/documents/12_crypt.pdf)

* + 1. IPAセキュリティマネジメントのしおりシリーズ
       1. 企業（組織）における最低限の情報セキュリティ対策のしおり+1PDF

ドキュメントを参照: [01\_guidebook.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf)

* + - 1. 「新5分でできる情報セキュリティ自社診断シート」

ドキュメントを参照: [5minutes.html](https://www.ipa.go.jp/security/keihatsu/sme/guideline/5minutes.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

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. 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

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. 情報セキュリティ対策ベンチマーク（企業・組織のためのセキュリティ対策自己診断ツール Ver.4.x）

ドキュメントを参照: [04\_benchmark.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/04_benchmark.pdf)

* + 1. 姉妹冊子
       1. クラウドサービス安全利用のすすめPDF（2.5MB）

ドキュメントを参照: [cloud\_tebiki\_handbook\_V1.pdf](https://www.ipa.go.jp/security/cloud/cloud_tebiki_handbook_V1.pdf)

* + - 1. 情報漏えい発生時の対応ポイント集PDF （0.8MB）

ドキュメントを参照: [rouei\_taiou.pdf](https://www.ipa.go.jp/security/awareness/johorouei/rouei_taiou.pdf)

* 1. 「やられたかな？その前に」【2015年10月14日 ISOG-J】

ドキュメントを参照: [Yararetakana-Guide-20151014.pdf](http://isog-j.org/output/2015/Yararetakana-Guide-20151014.pdf)

* + 1. 概要
       1. 従業員数や端末数
          1. どの程度の台数が存在し、 調査が必要か概要を確認する。
       2. 問 1～5
          1. 相談の経緯について

現在の被害の有無や外部からの指摘といった状況についてのヒヤリングとなる。

相談の際に被害はまだないのだが不安がある場合は不安な箇所がどこかといったところからのヒヤリングとなる。

* + - 1. 問 6～10
         1. 症状の詳細について

主にシステム管理を行っている方への質問となる。

既に何か症状がある場合、 どのような症状があるかの確認となる。

わからない場合は「□わからない」を選択頂きたい。

症状はシステム利用者に聞くことや、 主観での回答でも良い。 調査を開始する際に、 ネットワーク、 サーバ、 パソコンや端末、 ログや心当たりをヒヤリングしておくことで、 どこから着手するかの手がかりとなる。

* + - 1. 問 11～14
         1. 現在の管理状況について

主にシステム管理を行っている方への質問となる。

調査に必要な現状把握の設問である。 ネットワークやシステムに関連した社内文書の有無や、 調査の対象となるログについて確認する。

調査の中心がログの分析となる場合、 社内のどこに何があるかがはっきりしていると、 分析の手がかりとなる。

分析作業のために、 ログの保管場所や保存期間を把握する必要がある。

IT 関連をいつもお願いしている事業者や関連業者があれば記載をお願いしたい。

普段からのどの程度のセキュリティの対策を行っているかなどの把握が調査の手助けとなる。

* + - 1. 問 15～19
         1. 社内の組織体制について

主に事案や事件の対応者や責任者の方向けの質問となる。

明確に組織が存在しない場合は、 システム管理者の方の回答でも良い。

今後の相談や調査、 社内の対応に向けての確認となる。

調査や分析では、 お客様の協力が必要不可欠である。

業者との窓口という意味だけではなく、 調査や分析に当たって、 社内の手続きを含めてどういった手順で進めることができるかを事前に把握する。

* + - 1. 問 20～22
         1. IPA 10 大脅威 2017の基本対策

主に事案や事件の対応者や責任者の方向けの質問となる。

明確に組織が存在しない場合は、 システム管理者の方の回答でも良い。

セキュリティの基本対策がどの程度実施されているか確認する。

対策の内容によって調査や分析の手助けになる部分があるかの確認となる。

各項目の詳細な内容については「10 大脅威 2017」を確認されたい。

* + 1. 問診票

ドキュメントを参照: [Yararetakana-Guide-CheckList-20151014.docx](http://isog-j.org/output/2015/Yararetakana-Guide-CheckList-20151014.docx)

* + - 1. 問合せ者
         1. 会社名：
         2. 従業員数（　　　　　　）人、 　端末数（　　　　　）台、 　拠点数（　　　　　）箇所
      2. 相談のきっかけや経緯について伺います。
         1. 問1：外部から通報や連絡がありましたか？

例：情報が漏えいしている、 改ざんされている、 パソコンがおかしくなった、 など

□はい　（連絡元と、 連絡の内容：　　　　　　　　　　　　　　　　）　□いいえ

* + - * 1. 問2：過去にサイバー攻撃と思われる被害を受けたことはありますか？

□はい　（被害の状況：　　　　　　　　　　　　　　　　　　　　　）　□いいえ

* + - * 1. 問3：相談しようとするまでに、 何か対処はしましたか？

□はい　（時系列でお答えください：　　　　　　　　　　　　　　　）　□いいえ

* + - * 1. 問4：現在どのような不安がありますか？（複数回答可）

□公開しているサーバへの攻撃がある　□パソコンがウイルスに感染している

□内部から情報が漏えいしている　□その他（　　　　　　　　　　）

* + - * 1. 問5：相談のきっかけや経緯についてできるだけ具体的にお書きください
      1. 主にシステム管理者の方に、 現在の症状についてより詳細に伺います
         1. 問6：ネットワークが繋がりにくい・使えない

□はい　 ・いつごろからですか？　（　　　　　　　　　　　　　　　　　　　） ・頻度はどの程度ですか？（1回だけ・数回・決まった時間・決まった曜日） ・どのような時に症状を感じますか？　（　　　　　　　　　　　　　）

□いいえ　□わからない

* + - * 1. 問7：サーバの反応が悪い・反応がなくなる

□はい　 ・いつごろからですか？　（　　　　　　　　　　　　　　　　　　　） ・頻度はどの程度ですか？（1回だけ・数回・決まった時間・決まった曜日） ・どのようなサーバですか？　（　　　　　　　　　　　　　　　　　）

□いいえ　□わからない

* + - * 1. 問8：PC・携帯端末の反応が悪い・動かなくなる

□はい　 ・いつごろからですか？　（　　　　　　　　　　　　　　　　　　） ・頻度はどの程度ですか？（1回だけ・数回・決まった時間・決まった曜日） ・どのような端末ですか？　（　　　　　　　　　　　　　　　　　） ・何台で起こっていますか？　（　　　　　　　　　　　　　　　　）

□いいえ　□わからない

* + - * 1. 問9：不正な通信、 アクセスの形跡がある・気になるログがある

□はい　　 ・いつごろからですか？　（　　　　　　　　　　　　　　　　　　） ・どのような内容、 不審点がありますか？　（　　　　　　　　　　）

□いいえ　□わからない

* + - * 1. 問10：症状が始まった頃に、 下記のような出来事がありましたか？

□はい　　 ・システム変更を行った / 新しいソフトを導入した ・怪しいサイトやメールにアクセスした ・情報記録媒体を紛失した ・その他不安なこと（　　　　　　　　　　　　　　　　　　　　　）

□いいえ　□わからない

* + - 1. 主にシステム管理を行っている方に、 管理状況について伺います
         1. 問11：情報機器や情報資産、 ネットワークの構成について把握されていますか？

□はい　□いいえ　□わからない

* + - * 1. 問12：ネットワークやシステムのログを取得していますか？

□はい　□いいえ　□わからない

* + - * 1. （問12が「はい」の方にお聞きします） 問13：ログの保存期間は決めていますか？

□はい　（期間：　　　　　　　　　　　　　　）　□いいえ　□わからない

* + - * 1. 問14：普段から付き合いのあるセキュリティ事業者やITサービス事業者はいますか？

□はい　（会社名：　　　　　）※複数社あれば複数社お答え下さい

□いいえ　□わからない

* + - 1. 主に事案や事件の対応者や責任者の方に、 社内の組織体制についてお聞きします
         1. 問15：事案や事件の窓口担当者は決めていますか？

□はい　□いいえ

* + - * 1. 問16：相談について事案や事件対応責任者の了解を得ていますか？

□はい　□いいえ

* + - * 1. 問17：事案や事件の上位職への相談や報告をする順序は決まっていますか？

□はい　□いいえ　□わからない

* + - * 1. 問18：既にどこかへ報告しましたか？

□はい（責任者、 経営陣、 関係者（監督官庁、 取引先、 顧客））　□いいえ

* + - * 1. 問19：社内での調査や対処をする権限を持つ責任者や担当者がいますか？

□はい　□いいえ　□わからない

* + - 1. 主に事案や事件の対応者や責任者の方に、 IPA 「10大脅威 2017」で示された「セキュリティ対策の基本」をどの程度実施しているかの確認です。
         1. 問20：「対策の前に」はどの程度実施していますか？（複数回答可）

　□守りたい情報資産の把握

（情報資産とその場所： 　　　　　　　　　　　　　　　　　　　　　　　　　）

　□自発的なセキュリティ対策への取り組み

　□計画を策定し、 必要な予算の確保

* + - * 1. 問21： 現在行っているセキュリティ対策はどのようなものですか？（複数回答可）

□利用しているソフトウェアを更新・最新のものに（OSやアプリケーションなど）

□セキュリティソフト（ウイルス対策ソフトなど）の導入

□パスワードの適切な管理と認証の強化（多要素認証など）

□ソフトウェアや機器の設定を見直す（サーバ・ネットワーク設定の管理）

□ソフトウェアや機器の脆弱性や犯罪への対策などの情報収集

* + - * 1. 問22：その他に実施している対策はありますか？（複数回答可）

□文書による実施すべき対策の明文化　　□システムによる制限や強制

□バックアップやシステムの冗長化　　□検査や監査

□認証の取得（プライバシーマークやISO/IEC27001 など）

□その他（　　　　　　　　　　　　　　　　　　　　　　　　　　　　　）

* 1. 2017年度版「撃退！迷惑メール」迷惑メール対策BOOK【迷惑メール相談センター】

ドキュメントを参照: [gmeiwaku\_book.pdf](https://www.dekyo.or.jp/soudan/data/info/gmeiwaku_book.pdf)

* + 1. ☆1　こんなメールに気をつけよう
       1. 1.メールde詐欺
       2. 2.架空請求メール
       3. 3.銀行を装ったメール
       4. 4.芸能人を装ったメール
       5. 5.不正アプリをインストールさせようとするメール
       6. 6.懸賞金当選メール
       7. 7.宅配便の不在通知を装ったメール
       8. 8.ウイルスメール
       9. 9.チェーンメール
    2. ☆2　迷惑メールをブロックしよう
       1. 1.どうやって設定するの？
       2. 2.スマートフォンのおすすめ設定
       3. 3.ケータイのおすすめ設定
       4. 4.パソコンで設定する時は？
    3. ☆3　迷惑メールを予防しよう
       1. 1.迷惑メールの受信にはきっかけがあります
       2. 2.アドレスを使い分けよう
       3. 3.覚えておきたい迷惑メールへの対処法
    4. ☆4　スマートフォンのセキュリティ
       1. 1.スマートフォンに必須！セキュリティ対策
       2. 2.狙われるスマートフォンの個人情報
       3. 3.不正アプリインストールや個人情報流出を防ぐ
    5. ☆5　子どものスマートフォン利用案内
       1. 1.子どもの安全なスマートフォン利用のために
       2. 2.スマートフォンを持たせる前にまず確認してください
       3. 3.家庭でスマホ利用のルールを作る
       4. 4.フィルタリングを設定する
       5. 5.有害サイトから守る
       6. 6.有害アプリから守る
       7. 7.こんな時どうする？保護者のお悩みにお答えします
    6. ☆6　迷惑メールでお困りの方へ
       1. 1.迷惑メールは法律違反
       2. 2.情報提供のお願い
       3. 3.トラブル別相談窓口
       4. 4.用語解説
       5. 5.迷惑メール相談センターのご案内
    7. ☆7　おまけ
       1. 1.ぼくたち、 サギかもファミリーです
       2. 2.ヒヤリ・ハット体験SONGができました

1. 一般企業向け（特に中小企業）
   1. 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

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

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

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

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

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

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

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

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

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

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

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？

（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

* + - * 1. 「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。
      1. （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
      2. （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

「いつ・誰の・どんな情報を・誰に」提供したか？

「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」

* + - * 1. 外国にある第三者に提供する場合に守るべきこと

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 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)

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. Subtopic
  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

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。

* + - * 1. 想定読者

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。

* + - 1. 全体解説
         1. （1）本ガイドラインの構成

本編２部と付録より構成

* + - * 1. （2）本ガイドラインの使い方

①経営者の方

②経営者の指示のもとで重要な情報を管理する方

【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) 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）

(2) 顧客の喪失

(3) 業務 の喪失

(4) 従業員 への影響

* + - * 1. 経営者が負う責任

(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

(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

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)

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。

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

【図5】ガイドラインの使用方法

* + - * 1. 情報セキュリティ５か条

【表4】情報セキュリティ5か条

OSやソフトウェアは常に最新の状態にしよう！

ウイルス対策ソフトを導入しよう！

パスワードを強化しよう！

共有設定を見直そう！

脅威や攻撃の手口を知ろう！

* + - * 1. 5分でできる！情報セキュリティ自社診断

Part1 基本的対策

Part2 従業員としての対策

Part3 組織としての対策

* + - * 1. 情報セキュリティポリシーの策定

（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

（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

（3）委託時の情報セキュリティ対策

（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

（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）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

（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。

（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）

（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

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。

　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。

。 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。

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。

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

。 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。

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。

* + - 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
    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！

従業員のマイナンバー、 住所、 給与明細

お客様や取引先の連絡先一覧

取引先ごとの仕切り額や取引実績

新製品の設計図などの開発情報

組織の経理情報

取引先から取扱注意と言われた情報

* + - * 1. 漏れたら大変！こんなダメージが！

被害者への損害賠償などの支払い

取引停止、 顧客の他社への流出

ネットの遮断などによる生産効率のダウン

従業員の士気低下

* + - * 1. まずは始めてみよう

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。

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。

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。

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.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.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,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.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.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？

* + - * 1. Part2 従業員としての対策

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？

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？

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？

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？

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？

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？

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？

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？

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？

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？

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？

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？

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？

* + - * 1. Part3 組織としての対策

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？

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？

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？

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？

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？

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？

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？

* + - * 1. さらなる情報セキュリティ対策の検討するには

「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。

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/)

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

「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。

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/)

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)

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

OSとソフトウェアのアップデート

ウイルス対策ソフトの導入

パスワードの管理

アクセス制限

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

電子メールの利用

インターネットの利用

データのバックアップ

クリアデスク・クリアスクリーン

重要情報の持ち出し

入退室

電子媒体・書類の廃棄

* + - * 1. ３ 全社共通のルール

私有情報機器の利用

クラウドサービスの利用

* + - * 1. ３ 従業員のみなさんへ

従業員の守秘義務

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

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

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

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

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

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

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) 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？

(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？

(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？

(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？

(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？

(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？

(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？

(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？

(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？

(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？

(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）

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。

1.情報セキュリティ基本方針

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

3.安全管理措置に関する事項

4.委託の取り扱い

5.継続的改善

6.特定個人情報等の開示

* + - * 1. 組織的対策（当社全体）

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。

1.情報セキュリティのための組織

2.情報セキュリティ取組みの監査・点検/点検

3.情報セキュリティに関する情報共有

* + - * 1. 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.雇用条件

2.取締役及び従業員の責務

3.雇用の終了

4.情報セキュリティ教育

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.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

2.情報資産の社外持ち出し

3.媒体の処分

3.1媒体の廃棄

3.2媒体の再利用

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.総則

1.1目的

1.2定義

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

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

4.委託の取扱い

4.1委託

4.2再委託

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

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.アクセス制御方針

2.利用者の認証

3.利用者アカウントの登録

4.利用者アカウントの管理

5.パスワードの設定

6.従業員以外の者に対する利用者アカウントの発行

7.機器の識別による認証

8.端末のタイムアウト機能

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.セキュリティ領域の設定

2.関連設備の管理

3.セキュリティ領域内注意事項

4.搬入物の受け渡し

* + - * 1. ＩＴ機器利用（業務で利用する情報処理設備・機器）

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

2.ＩＴ機器の利用

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

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.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

2.ＩＴ基盤の運用

3.クラウドサービスの導入

4.脅威や攻撃に関する情報の収集

5.廃棄・返却・譲渡

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.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.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）

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

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

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

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

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

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.情報セキュリティのための組織

* + - * 1. 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.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）

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。

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。

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。

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。

* + - * 1. （モバイルPC、 記憶媒体について）

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。

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。

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。

* + 1. 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。
    2. 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）

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。

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。

* + - * 1. （内部から外部へのアクセス）

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。

* + - 1. 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。
      2. 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。
    1. 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. 一般企業向け
   1. CISO等セキュリティ推進者の経営・事業に関する役割調査【2018年6月28日IPA】
      1. 概要
         1. 「サイバーセキュリティ経営ガイドライン」（経済産業省とIPAが共同策定）(\*1)には、 経営者が認識すべき3原則が掲げられています。 その中で、 経営層はサイバーセキュリティリスクを認識し、 リーダーシップをとって対策を進めることが必要とあります。
         2. 一方、 「サイバーセキュリティ人材育成プログラム」（サイバーセキュリティ戦略本部）(\*2)では、 経営層自らがサイバーセキュリティ対策を企画・立案し、 実務者層を動かすことは困難であるとしています。 そのため同プログラムは、 経営層を補佐し、 経営戦略とサイバーセキュリティに関する業務課題を理解したうえで、 様々な役割を持った実務者層を指揮する「橋渡し人材」が必要であるとしています。
         3. 「CISO等セキュリティ推進者の経営・事業に関する役割調査」では、 CISO(\*3)およびその補佐役となる橋渡し人材等のセキュリティ推進者が担う役割、 とくにセキュリティへの取組みが経営と事業に貢献するようマネジメントする役割（以下、 経営・事業に関する役割）について、 その実態や期待されている内容を調査するため、 文献調査・有識者へのインタビュー調査・アンケート調査を行っています。
         4. 調査結果に基づいて、 CISO等セキュリティ推進者の経営・事業に関する役割7つについて整理し、 各役割の目的や役割を遂行する際のポイント等をまとめたプラクティスを、 調査報告書の別冊として作成しました。
      2. －別冊－CISO等セキュリティ推進者の経営・事業に関する役割プラクティス【2018年6月28日IPA】
         1. CISO等セキュリティ推進者の経営・事業に関する役割7つについて整理し、 各役割の目的や役割を遂行する際のポイント等をまとめたプラクティス
         2. 1. はじめに
            1. 1.1 目的

経営層によるセキュリティ対策の主体的取組の推進には、 経営層の示す経営方針に基づくセキュリティ対策を実践し、 実務課題を踏まえた経営戦略を提示し、 企業内の総合調整や実務者層をまとめリードできる人材が必要である

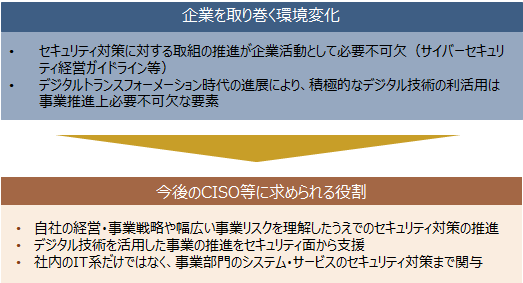
CISO等には技術的な役割だけではなく、 自社の経営方針・事業戦略とセキュリティ対策の整合等、 経営・事業的貢献の観点からセキュリティ対策を推進する「経営・事業的役割」が今後求められると考えられる。

さらに、 昨今、 デジタルトランスフォーメーションと呼ばれるように、 企業においても、 社内システムのみならず、 事業部門の情報システムや、 工場等で利用される制御システムにおいても、 デジタル技術活用を進めることで新たな事業価値を生み出すべく取組が進展しつつある。

そのため、 より広範囲な業種・業態において積極的なデジタル技術の活用が事業推進上必要不可欠な要素となりつつある。

一方で、 過剰なセキュリティ対策は、 利便性や業務効率化を下げる場合もあり、 スピードを持って事業を促進するためには、 CISO等が事業を深く理解しつつ、 適切なリスク評価を行うことで事業とセキュリティのバランスを取り、 セキュリティの面から事業推進を支援する役割の重要性が増している。

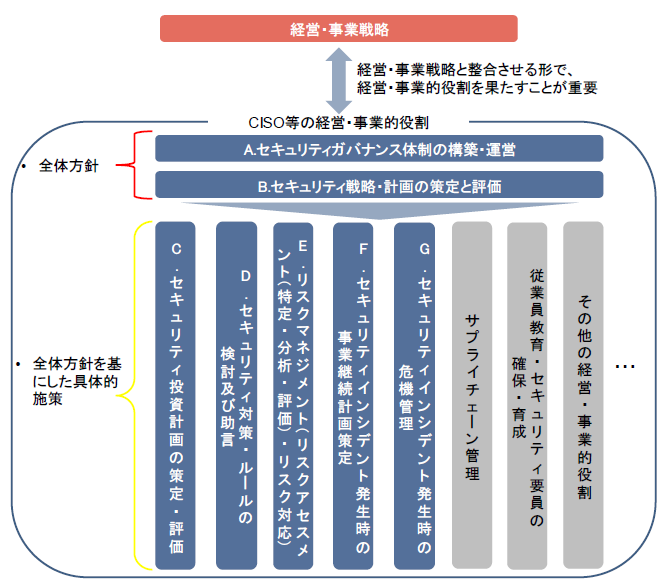
図 1-1 今後のCISO等に求められる役割

Subtopic  


ITサービス業や金融業等、 従来からITが事業の根幹であるような業種と、 製造業や卸売業・小売業等、 今後デジタル技術の活用が本格化する業種とでは、 CISO等が担う経営・事業的役割も異なると想定される。

* + - * 1. 1.2 経営・事業的役割の全体像

図 1-2 CISO等の経営・事業的役割の全体像

Subtopic  


CISO等の経営・事業的役割は、 企業の経営・事業戦略と整合する形でセキュリティ対策が実施されるように、 遂行することが望ましい。

CISOは3つの防衛線（Three lines of defense）1のセカンドラインのトップ

業務執行部門が業務においてリスクの特定及び管理を行う第1の防衛線

業務執行部門のリスク管理の状況を業務執行部門から独立したリスク管理部門等がモニタリングする第2の防衛線

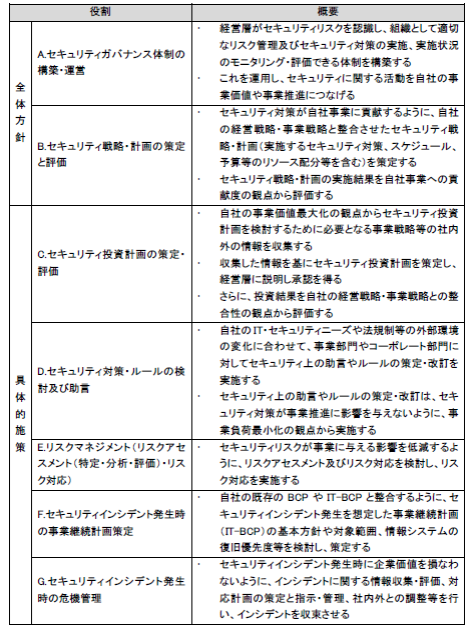
防衛線の有効性を合理的に保証する内部監査部門を第3の防衛線

としたリスク管理の仕組みのこと。

CISO等は自社の社内ITシステムだけではなく、 事業部門が保有・提供しているITシステム・ITサービスのセキュリティ対策にまで関与していくことが望ましい。

特に重要と考えられる役割としてA~Gの7つの役割を選定した。 選定した役割の概要は表 1-1の通りで、 2章～8章では選定した役割について役割の目的や作業プロセス等の詳細を説明する。

表 1-1 本書で対象とする経営・事業的役割の概要

Subtopic  


全体方針

A.セキュリティガバナンス体制の構築・運営

 経営層がセキュリティリスクを認識し、 組織として適切なリスク管理及びセキュリティ対策の実施、 実施状況のモニタリング・評価できる体制を構築する

 これを運用し、 セキュリティに関する活動を自社の事業価値や事業推進につなげる

B.セキュリティ戦略・計画の策定と評価

 セキュリティ対策が自社事業に貢献するように、 自社の経営戦略・事業戦略と整合させたセキュリティ戦略・計画（実施するセキュリティ対策、 スケジュール、 予算等のリソース配分等を含む）を策定する

 セキュリティ戦略・計画の実施結果を自社事業への貢献度の観点から評価する

具体的施策

C.セキュリティ投資計画の策定・評価

 自社の事業価値最大化の観点からセキュリティ投資計画を検討するために必要となる事業戦略等の社内外の情報を収集する

 収集した情報を基にセキュリティ投資計画を策定し、 経営層に説明し承認を得る

 さらに、 投資結果を自社の経営戦略・事業戦略との整合性の観点から評価する

D.セキュリティ対策・ルールの検討及び助言

 自社のIT・セキュリティニーズや法規制等の外部環境の変化に合わせて、 事業部門やコーポレート部門に対してセキュリティ上の助言やルールの策定・改訂を実施する

 セキュリティ上の助言やルールの策定・改訂は、 セキュリティ対策が事業推進に影響を与えないように、 事業負荷最小化の観点から実施する

E.リスクマネジメント（リスクアセスメント（特定・分析・評価）・リスク対応）

 セキュリティリスクが事業に与える影響を低減するように、 リスクアセスメント及びリスク対応を検討し、 リスク対応を実施する

F.セキュリティインシデント発生時の事業継続計画策定

 自社の既存のBCPやIT-BCPと整合するように、 セキュリティインシデント発生を想定した事業継続計画（IT-BCP）の基本方針や対象範囲、 情報システムの復旧優先度等を検討し、 策定する

G.セキュリティインシデント発生時の危機管理

 セキュリティインシデント発生時に企業価値を損なわないように、 インシデントに関する情報収集・評価、 対応計画の策定と指示・管理、 社内外との調整等を行い、 インシデントを収束させる

サブトピック 7

* + - * 1. 1.3 経営・事業的役割間の関係と本書の活用方法

図 1-3において、 各役割から伸びる矢印は、 その役割の作業成果物（アウトプット）が、 矢印の先の役割の作業を進めるためのインプットとなることを示している

図 1-3 役割間のインプット・アウトプット関係

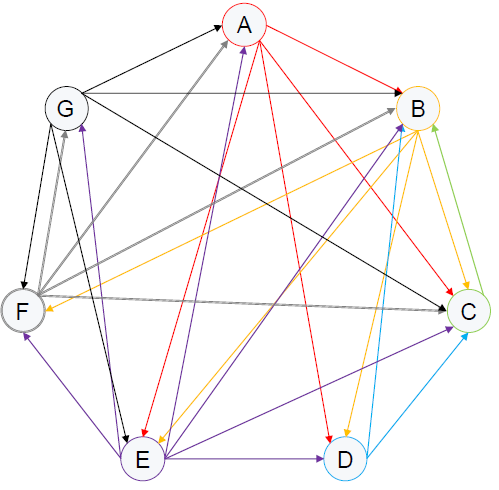
Subtopic  


表 1-2 各役割の作業成果物

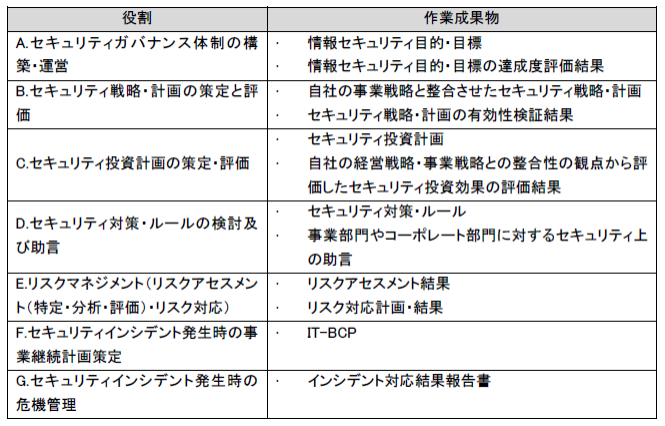
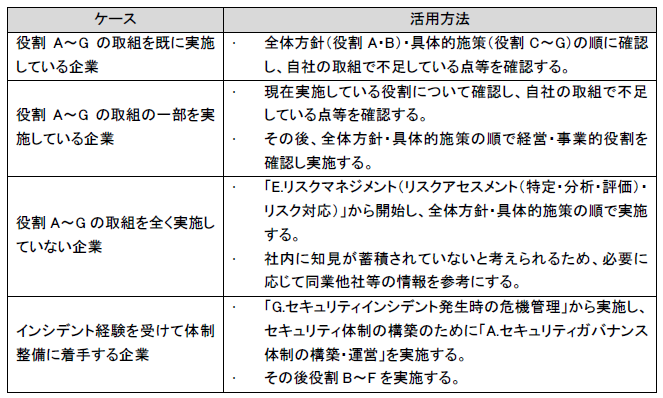
Subtopic  


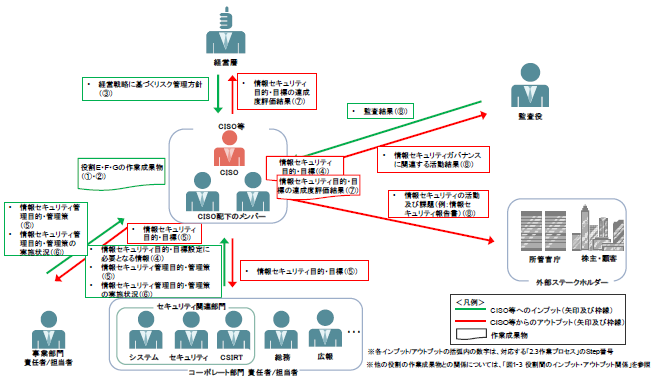
表 1-3 ケース別本書の活用方法

Subtopic  


* + - 1. 2. セキュリティガバナンス体制の構築・運営（A）
         1. 2.1 目的・狙い

本役割は経営層がセキュリティリスクを認識し、 組織として適切なリスク管理とセキュリティ対策が実施するための体制を構築・運用し、 自社の事業価値や事業推進に貢献することを目的としている。

図 2-1 「セキュリティガバナンス体制の構築・運営」の全体像

Subtopic  


* + - * 1. 2.2 役割の作業内容

・経営者による方針決定等の機能を有するセキュリティガバナンスのフレームワークの構築

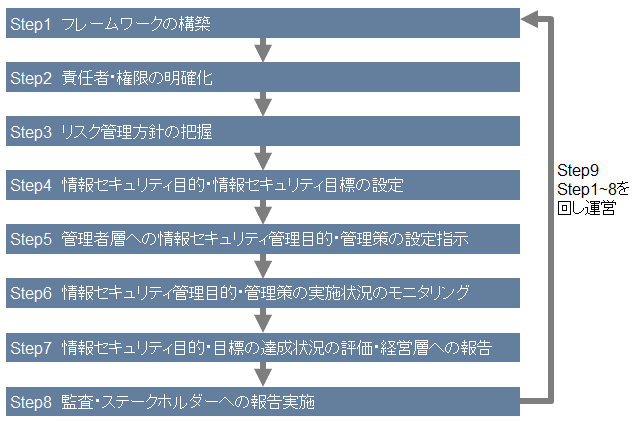
・経営層が示すリスク管理方針に基づいた情報セキュリティ目的・情報セキュリティ目標の設定

・情報セキュリティ目的・情報セキュリティ目標の達成状況を評価し経営層に報告

・外部監査や外部ステークホルダーへの報告実施

* + - * 1. 2.3 作業プロセス

図 2-2 「セキュリティガバナンス体制の構築･運営」の作業プロセス

Subtopic  


Step1 フレームワークの構築

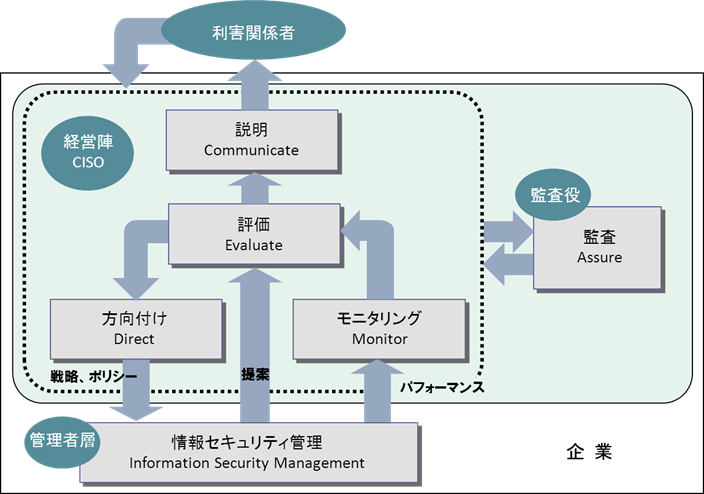
・経営者による方針決定

・組織内の状況をモニタリングする仕組み

・利害関係者に対する開示

・利害関係者による評価の仕組み

図 2-3 情報セキュリティガバナンスのフレームワーク

Subtopic  


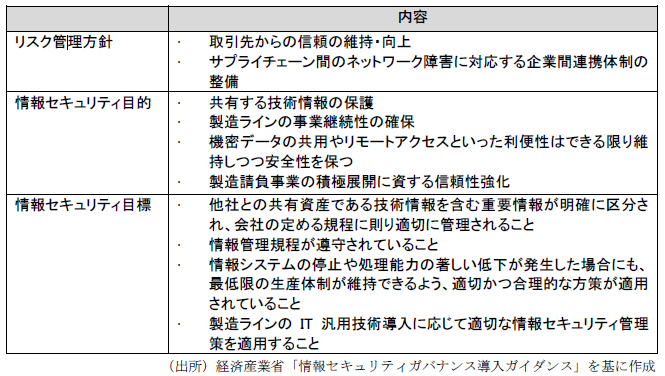
（出所）経済産業省「情報セキュリティガバナンス導入ガイダンス」を基にISO/IEC 27014:2013 の内容を一部反映

Step2 責任者・権限の明確化

Step3 リスク管理方針の把握

Step4 情報セキュリティ目的・情報セキュリティ目標の設定

表 2-1 情報セキュリティ目的・情報セキュリティ目標の例

Subtopic  


Step5 管理者層への情報セキュリティ管理目的・管理策の設定指示

Step4で設定した情報セキュリティ目的・目標を事業部門・コーポレート部門の管理者層に伝える。 さらに、 管理者層に対し情報セキュリティ目的・目標を実現するための情報セキュリティ管理目的・管理策の設定を指示する。

情報セキュリティ管理目的・管理策の設定にあたり、 事業部門等セキュリティ人材等が不足していると考えられる組織に対しては、 CISO等が必要に応じて支援することが望ましい。

Step6 情報セキュリティ管理目的・管理策の実施状況のモニタリング

Step7 情報セキュリティ目的・目標の達成状況の評価・経営層への報告

Step8 監査・ステークホルダーへの報告実施

セキュリティガバナンスに関わる活動に関して監査を依頼し、 監査結果を基に見直しを実施する。

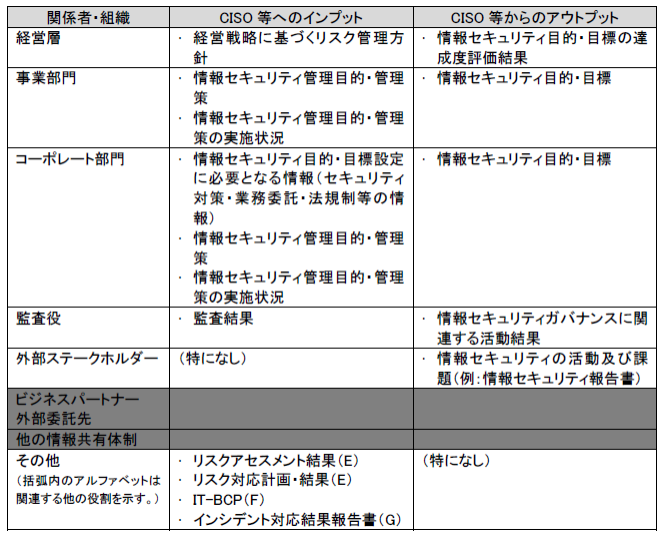
また、 外部ステークホルダーに対して、 自社のセキュリティに対する取組について報告を実施する

Step9 情報セキュリティガバナンス体制の運営

Step1～8の取組を回し、 情報セキュリティガバナンス体制を運営する。

* + - * 1. 2.4 作業に必要な情報

表 2-2 「セキュリティガバナンス体制の構築・運営」に必要となる情報

Subtopic  


* + - * 1. 2.5 作業の目標成果

・情報セキュリティ目的・目標

・情報セキュリティ目的・目標の達成度評価結果

* + - * 1. 2.6 作業で協同・連携する社内外の関係者と協同・連携の内容

・情報セキュリティ目的・情報セキュリティ目標達成のための、 事業部門・コーポレート部門に対する連携・支援

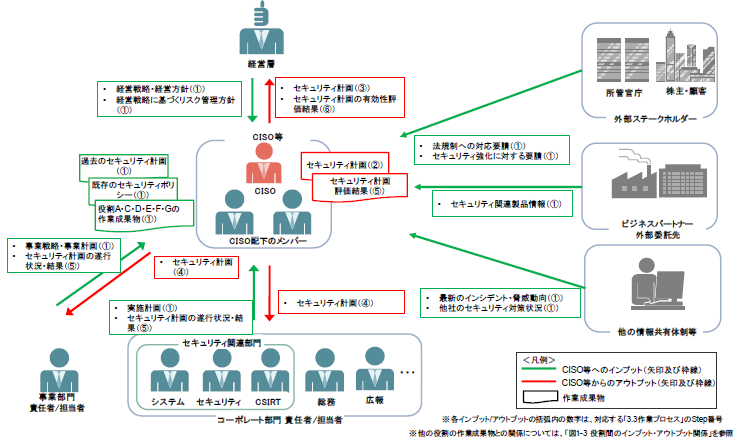
・外部ステークホルダーに対する自社のセキュリティ対策に関する情報開示

* + - 1. 3. セキュリティ戦略・計画の策定と評価（B）
         1. 3.1 目的・狙い

本役割は、 自社の経営戦略・事業戦略と整合したセキュリティ戦略・計画（実施するセキュリティ対策や実施スケジュール、 予算等のリソース配分等）を策定し、 自社の事業価値や事業推進につなげることを目的としている。

本役割で策定するセキュリティ戦略・計画は企業のセキュリティ対策に関する全体方針であり、 このセキュリティ戦略・計画を基に、 4 章以降の役割の具体的な施策が実施される。

図 3-1 「セキュリティ戦略・計画の策定と評価」の全体像

Subtopic  


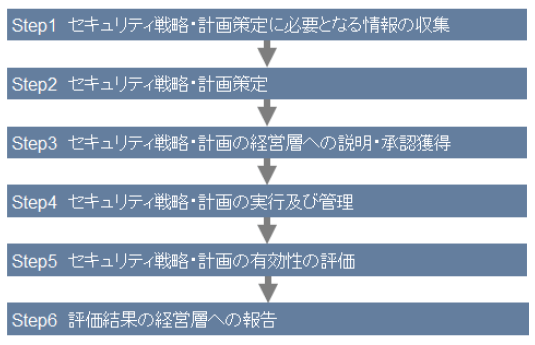
* + - * 1. 3.2 役割の作業内容

・自社の経営戦略・事業戦略と整合させたセキュリティ戦略・計画の策定

・セキュリティ戦略・計画の実施結果の評価

* + - * 1. 3.3 作業プロセス

図 3-2 「セキュリティ戦略・計画の策定と評価」の作業プロセス

Subtopic  


Step1 セキュリティ戦略・計画策定に必要となる情報の収集

・経営戦略・経営方針

・事業戦略・事業計画

・自社に影響を与える法規制

・最新のインシデント・脅威動向

・情報セキュリティ目的・目標（A）

・セキュリティ投資計画（C）

・セキュリティ対策・ルール（D）

・リスクアセスメント結果（E）

・IT-BCP（F）

・インシデント対応結果報告書（G）

Step2 セキュリティ戦略・計画策定

Step1で収集した情報を基に、 セキュリティ戦略・計画を策定する。 セキュリティ戦略・計画には、 実施するセキュリティ対策や実施スケジュール、 予算等のリソース配分等が含まれる

Step3 セキュリティ戦略・計画の経営層への説明・承認獲得

Step2で策定したセキュリティ戦略・計画を経営層に対して説明し、 承認を得る。 経営層から承認が得られなかった場合は、 Step2に戻り必要な修正を実施する。

Step4 セキュリティ戦略・計画の実行及び管理

Step3で承認されたセキュリティ戦略・計画を実行する。 事業部門・コーポレート部門が実行するセキュリティ戦略・計画に関しては、 CISO等が実行状況をモニタリングし管理するとともに、 必要に応じて支援する

Step5 セキュリティ戦略・計画の有効性の評価

事業部門・コーポレート部門のセキュリティ戦略・計画の実行状況・結果を把握し、 セキュリティ戦略・計画の有効性を評価する。 セキュリティ戦略・計画の有効性を評価する際は、 自社の経営戦略・事業戦略との整合性や自社の事業価値への貢献等の観点から実施することが望ましい。

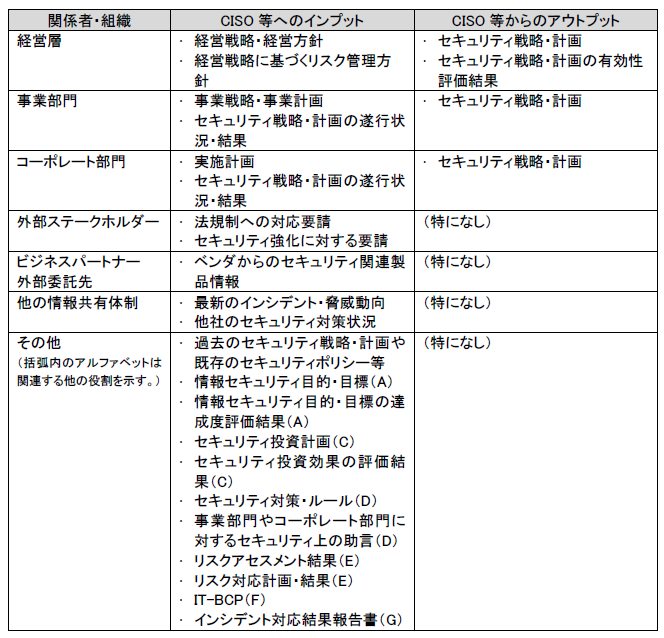
評価結果は次年度以降のセキュリティ戦略・計画を策定する際に活用する。

Step6 評価結果の経営層への報告

Step5の評価結果を経営層へ報告する。

* + - * 1. 3.4 作業に必要な情報

表 3-1 「セキュリティ戦略・計画の策定と評価」に必要となる情報

Subtopic  


* + - * 1. 3.5 作業の目標成果

・自社の事業戦略と整合させたセキュリティ戦略・計画

・セキュリティ戦略・計画の有効性検証結果

* + - * 1. 3.6 作業で協同・連携する社内外の関係者と協同・連携の内容

・社内外の関係者からのセキュリティ戦略・計画策定に必要となる情報の収集

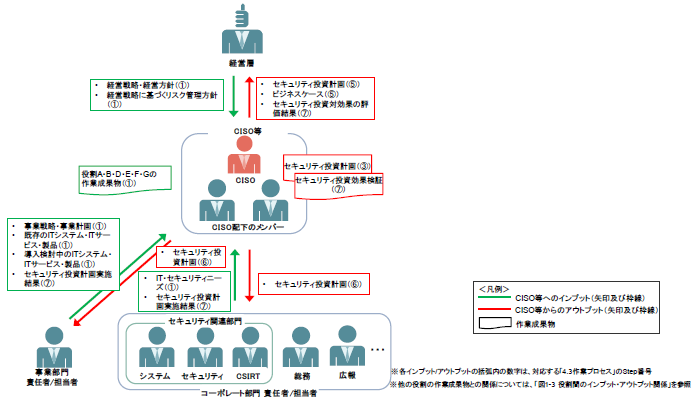
・事業部門・コーポレート部門と連携したセキュリティ戦略・計画の実行

* + - 1. 4. セキュリティ投資計画の策定・評価（C）
         1. 4.1 目的・狙い

本役割は、 「セキュリティ戦略・計画の策定・評価」の役割で策定されたセキュリティ戦略・計画を基に、 必要となるセキュリティ対策を検討し、 対策実施に必要なセキュリティ投資計画を策定するものである。 策定するセキュリティ投資計画には、 新規のITサービス・ITシステムの導入だけではなく、 既存のITサービス・ITシステムの継続利用等の判断も含まれる。

本役割の遂行にあたっては、 セキュリティ投資が自社の企業価値の最大化につながるようにセキュリティ投資計画を策定し、 自社の経営戦略・事業戦略との整合性の観点から投資の有効性を評価することが望ましい。

図 4-1 「セキュリティ投資計画の策定・評価」の全体像

Subtopic  


* + - * 1. 4.2 役割の作業内容

・自社の企業価値最大化につながるセキュリティ投資計画の策定

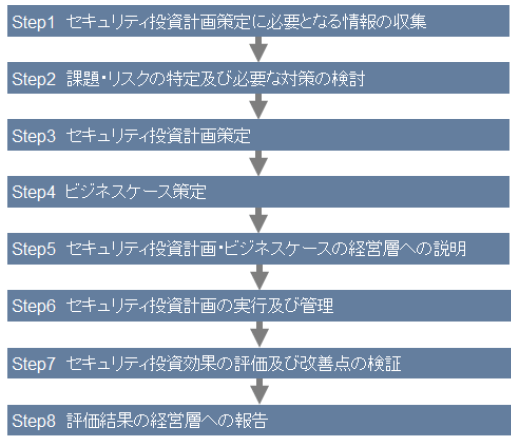
・セキュリティ投資計画の有効性を示すビジネスケース5の策定

・セキュリティ投資計画・ビジネスケースの経営層への説明・承認獲得

・セキュリティ投資計画の実行及び投資効果の検証

* + - * 1. 4.3 作業プロセス

図 4-2 「セキュリティ投資計画の策定・評価」の作業プロセス

Subtopic  


Step1 セキュリティ投資計画策定に必要となる情報の収集

・経営戦略・経営方針

・事業戦略・事業計画

・既存または導入検討中のITシステム・ITサービス・製品

・情報セキュリティ目的・目標（A）

・セキュリティ戦略・計画（B）

・セキュリティ対策・ルール（D）

・リスクアセスメント結果（E）

・IT-BCP（F）

・インシデント対応結果報告書（G） 等

Step2 課題・リスクの特定及び必要な対策の検討

Step1で収集した情報を元に、 自社のセキュリティ上の課題やリスクを特定し、 必要な対策を検討する。

Step3 セキュリティ投資計画策定

Step2で検討した対策を導入するために必要となるセキュリティ投資計画を策定する。

セキュリティ投資計画の策定にあたっては、 自社の事業価値最大化につながるよう、 経営戦略・事業戦略と整合させるように策定することが望ましい。

Step4 ビジネスケース策定

・セキュリティ投資の目的・必要性

・必要なリソース

・実施スケジュール

・期待される投資効果 等

Step5 セキュリティ投資計画・ビジネスケースの経営層への説明

Step3・Step4で策定したセキュリティ投資計画・ビジネスケースを経営層に説明し、 承認を得る。 経営層からの承認が得られなかった場合、 Step3に戻り必要な修正を行う。

Step6 セキュリティ投資計画の実行及び管理

経営層から承認を得たセキュリティ投資計画を実行する。 事業部門やコーポレート部門が実行するセキュリティ投資計画については、 その進捗状況等をCISO等が管理する。

Step7 セキュリティ投資効果の評価及び改善点の検証

セキュリティ投資計画の実行結果を基に、 セキュリティ投資の投資効果・改善点を検証する。

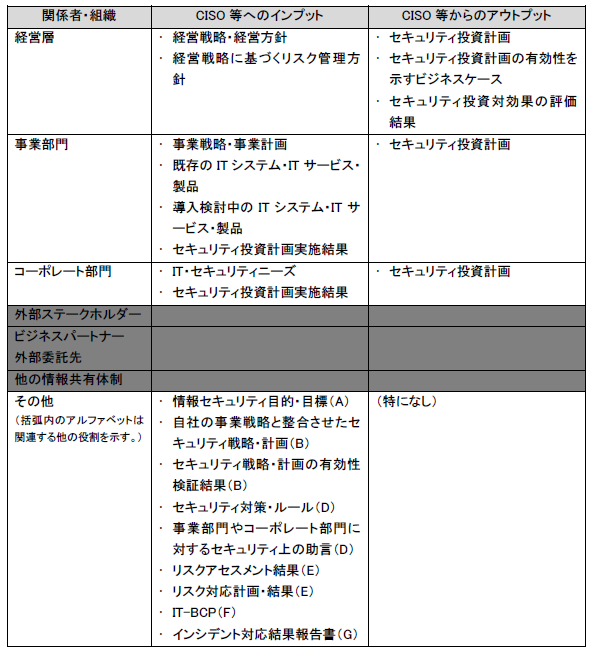
投資効果の検証の際には、 自社の経営戦略・事業戦略との整合性や、 自社事業推進にどの程度貢献したか等の観点から実施することが望ましい。

セキュリティ投資効果の検証結果に関しては、 次年度以降のセキュリティ戦略・計画の策定やセキュリティ投資計画の策定に活用する。

Step8 評価結果の経営層への報告

Step7で実施したセキュリティ投資効果の検証結果を経営層に報告する。

* + - * 1. 4.4 作業に必要な情報

Subtopic  


* + - * 1. 4.5 作業の目標成果

・セキュリティ投資計画（導入する製品・サービスや投資金額、 実施時期、 投資効果等を含む）

・自社の経営戦略・事業戦略との整合性の観点から評価したセキュリティ投資効果の評価結果

* + - * 1. 4.6 作業で協同・連携する社内外の関係者と協同・連携の内容

・自社の経営戦略・事業戦略等の把握・セキュリティ上の課題の検討に必要となる情報の提供・意見交換

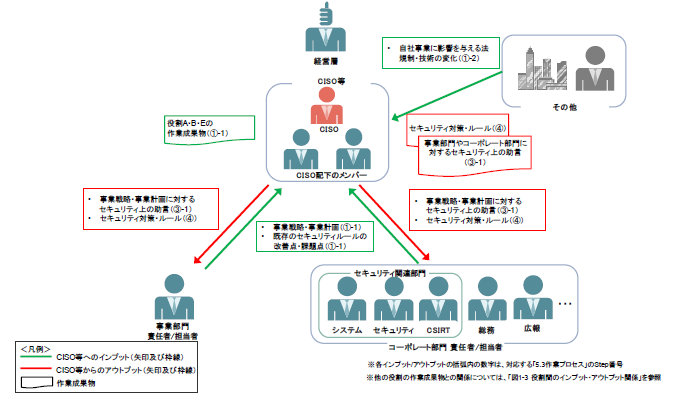
・事業部門やコーポレート部門に対するセキュリティ投資計画の実行支援及び進捗状況の管理

* + - 1. 5. セキュリティ対策・ルールの検討及び助言（D）
         1. 5.1 目的・狙い

事業部門やコーポレート部門の社内部門の新規の事業展開や新たなITシステム・ITサービスの利用等の内部環境の変化や、 法規制や新規技術の登場等の外部環境の変化に合わせて、 CISO等にはセキュリティ上の助言や新たなルールの策定、 既存ルールの改訂等の対応が求められる。

本役割では社内外の環境変化に合わせて、 CISO等がセキュリティ上の助言やルールの策定・改定を行うものである。 本役割を遂行する際には、 セキュリティ対策が事業推進に影響を与えないよう、 事業負荷を最小にする観点から検討することが望ましい。 また、 CISO等の役割が事業の推進を成功に導くようにセキュリティ対策・ルールを整備することであることに留意する必要がある。

図 5-1 「セキュリティ対策・ルールの検討及び助言」の全体像

Subtopic  


* + - * 1. 5.2 役割の作業内容

・事業部門・コーポレート部門等からの内部情報の収集及び法規制や技術動向等の外部情報の収集

・収集した情報を基にした、 自社のIT利活用ニーズの把握及びセキュリティ上の課題の検討

・検討した課題を基にした、 事業部門・コーポレート部門に対するセキュリティ上の助言

・検討した課題を基にした、 既存のルールの改訂または新規ルールの策定及び見直し

実施するタイミングとしては以下のものが考えられる。

・年度計画検討時

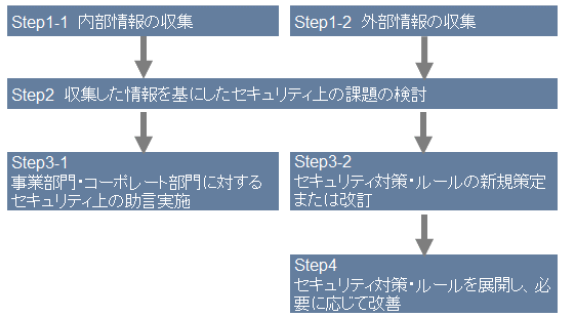
・新規事業検討時

・新規のITサービス導入検討時

・自社に影響を与える法規制や新規技術の登場時

* + - * 1. 5.3 作業プロセス

図 5-2 「セキュリティ対策・ルールの検討及び助言」の作業プロセス

Subtopic  


Step1-1 内部情報の収集

事業部門及びコーポレート部門に対して、 事業計画（ITシステム・ITサービスを利用した新規事業や新規のITシステム・ITサービスの検討・導入等）や既存のセキュリティルール等に関する改善要望等の情報を収集する。

内部情報の収集にあたっては、 他の役割の成果物である以下のものもインプットとなる。

・情報セキュリティ目的・目標（A）

・自社の事業戦略と整合させたセキュリティ戦略・計画（B）

・リスクアセスメント結果（E）

・リスク対応計画・結果（E）

Step1-2 外部情報の収集

自社事業に影響を与える法規制の変化や新規技術の動向等について、 定期的に情報を収集する。

Step2 収集した情報を基にしたセキュリティ上の課題の検討

Step1-1及びStep1-2で収集した情報を基に自社のIT利活用ニーズ等を把握し、 セキュリティ上の課題がないか検討する。

Step3-1 事業部門・コーポレート部門に対するセキュリティ上の助言の実施

Step2で検討した課題を基に、 事業部門・コーポレート部門に対して、 事業推進・業務運営に必要となるセキュリティ対策の実施等、 セキュリティ上の助言を行う。

助言はセキュリティ対策が事業推進・業務運営の妨げにならないよう、 事業部門・コーポレート部門の負荷を最小にする観点から検討することが望ましい。

Step3-2 セキュリティ対策・ルールの新規策定または改訂

Step2で検討した課題を基に、 セキュリティに関するルールの新規策定または既存のルールの改訂を行う。

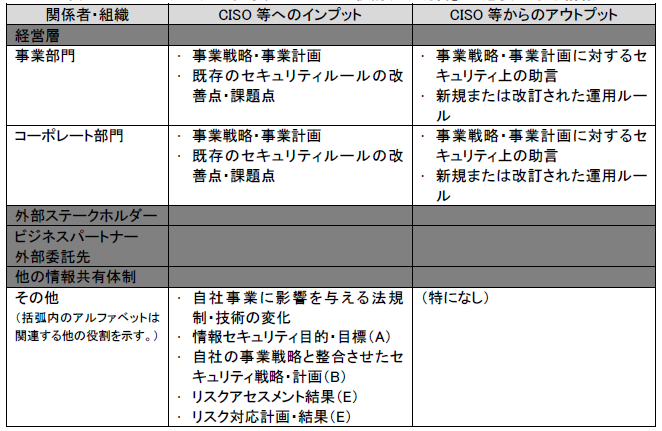
ルールの策定・改訂の際は、 セキュリティに関するルールが事業推進・業務運営の妨げにならないよう、 事業部門・コーポレート部門の負荷を最小にする観点から検討することが望ましい。

Step4 セキュリティ対策・ルールを展開し、 必要に応じて改善

策定・改訂したセキュリティに関するルールを社内に展開する。 また、 必要に応じて改善する。

* + - * 1. 5.4 作業に必要な情報

表 5-1 「セキュリティ対策・ルールの検討及び助言」に必要となる情報

Subtopic  


* + - * 1. 5.5 作業の目標成果

・社内外の環境変化に対応した事業部門及びコーポレート部門に対するセキュリティ上の助言

・社内外の環境変化に対応したセキュリティ対策・ルール

* + - * 1. 5.6 作業で協同・連携する社内外の関係者と協同・連携の内容

・自社のIT利活用ニーズの把握・セキュリティ上の課題の検討に必要となる情報提供・意見交換

・事業部門のセキュリティ対策の実施等に関して、 コーポレート部門（主にセキュリティ関連部門）と連携した支援

* + - 1. 6. リスクマネジメント（リスクアセスメント（特定・分析・評価）・リスク対応）（E）
         1. 6.1 目的・狙い

セキュリティ対策はセキュリティに関わるリスクに対応することである。

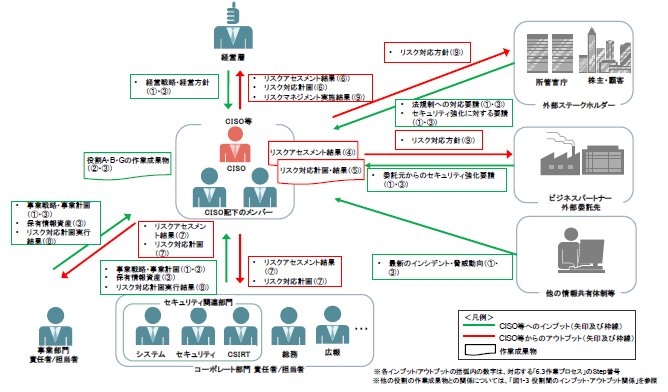
しかし、 対策にかけられる組織のリソースには限りがあることから、 リスクを明確にし、 対応の優先順位をつけ、 最適な対策を選択する必要がある。

また、 組織が抱えるリスクは組織の状況により異なり、 保有する情報資産や脅威の変化に伴い変化していくことから、 セキュリティリスクに対しては、 いったん評価・対応して終わりではなく、 適切に管理していかなければならない。

さらに、 リスクの評価基準は企業としての判断であることから、 経営・事業的な観点でリスクを評価し対応を検討していくことが必要である。

本役割は、 自社のセキュリティ関連のリスクへの対応方針を定め、 リスクが事業に与える影響を低減することを目的としている。 図

図 6-1 「リスクマネジメント」の全体像

Subtopic  


* + - * 1. 6.2 役割の作業内容

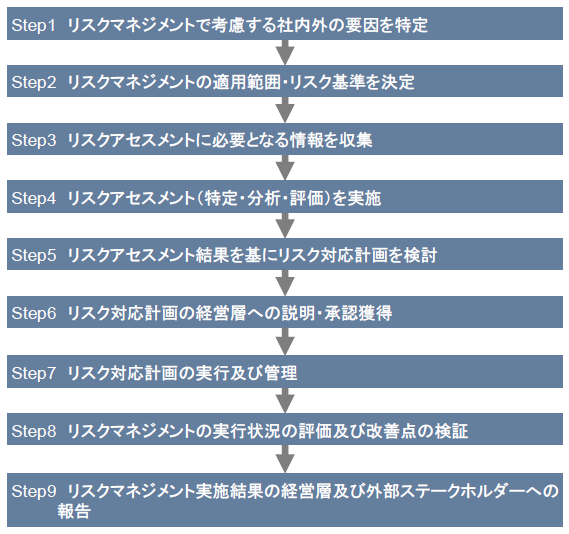
セキュリティに関わるリスクアセスメント（特定・分析・評価）を行う。

リスクアセスメント結果に基づき、 リスク対応計画の策定を行う。

リスク対応計画に基づいた、 実行及び管理を行う。

* + - * 1. 6.3 作業プロセス

図 6-2 「リスクマネジメント」の作業プロセス

Subtopic  


Step1 リスクマネジメントで考慮する社内外の要因を特定

組織の目的を明確にし、 リスクマネジメントにおいて考慮するのが望ましい社内外の要因を特定する。

外部環境とは、 政治や経済、 法規制、 金融，技術等の社会動向全般、 競争環境等市場の動向、 ステークホルダーの状況等であり

内部環境とは、 組織体制、 方針・戦略、 組織文化、 情報システム、 ステークホルダーの状況等である。

Step2 リスクマネジメントの適用範囲・リスク基準を決定

リスクマネジメントを適用する範囲と、 リスクを評価するために使用する基準を定める。 評価基準は、 組織の目的やリソース等の状況、 及び法律や規制の要求事項等によって検討される。

評価基準は、 例えば事象の起こりやすさ、 影響の種類や特徴、 リスクレベル、 複数のリスクの考慮等である。

Step3 リスクアセスメントに必要となる情報を収集

リスクアセスメント（特定・分析・評価）を行うために必要な情報を収集する

Step4 リスクアセスメント（特定・分析・評価）を実施

リスク特定では、 リスク源やその事象が発生しうる原因・結果を特定し、 リスクの一覧を作成する。

リスク分析では，リスク評価や対応計画の策定に必要な情報を整理する。 分析の際には、 リスク源、 原因と結果、 起こりやすさ等を考慮する。

リスク評価では、 リスク分析結果に基づき、 対応が必要なリスクや実施の優先順位に関して意思決定を行う。

Step5 リスクアセスメント結果を基にリスク対応計画を検討

リスクアセスメントの結果、 明確になったリスクに対して、 対応方法及び実施時期を明確にし、 リスク対応計画として定める。

リスクの対応方針には

「リスクの低減」

「リスクの保有」

「リスクの回避」

「リスクの移転」

Step6 リスク対応計画の経営層への説明・承認獲得

Step5で策定したリスク対応計画を経営層に対して説明し、 承認を得る。 経営層から承認が得られなかった場合は、 Step5に戻り必要な修正を実施する。

Step7 リスク対応計画の実行及び管理

経営層から承認を得たリスク対応計画を実行する。 事業部門やコーポレート部門が実行するリスク対応計画については、 その進捗状況等をCISO等が管理する。

Step8 リスクマネジメントの実行状況の評価及び改善点の検証

リスク対応計画の実行結果を基に、 リスク対応の効果・改善点を検証する。

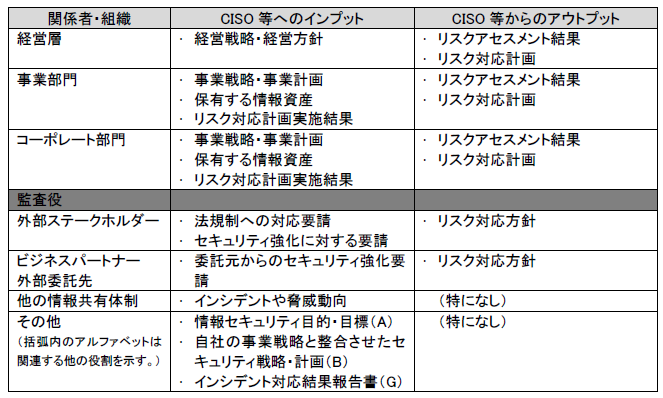
リスク対応計画の改善点に関しては、 次年度以降のリスク対応計画の策定に活用する。

Step9 リスクマネジメント実施結果の経営層及び外部ステークホルダーへの報告

Step8で実施されたリスクマネジメントの実施結果を経営層に対して説明し、 承認を得る。 外部ステークホルダーに対する報告により、 リスクマネジメントに関わる説明責任を果たす

* + - * 1. 6.4 作業に必要な情報

表 6-1 「リスクマネジメント」に必要となる情報

Subtopic  


* + - * 1. 6.5 作業の目標成果

リスクアセスメント結果

リスク対応計画・結果

* + - * 1. 6.6 作業で協同・連携する社内外の関係者と協同・連携の内容

・事業部門における事業リスクと、 セキュリティ部門のセキュリティリスク、 コーポレート部門における企業リスクを踏まえ、 リスクアセスメントを実施する。

・事業部門、 セキュリティ部門、 コーポレート部門がそれぞれ実施可能なリスク対応計画を策定する。

・リスクアセスメント結果を経営層に説明する。

* + - 1. 7. セキュリティインシデント発生時の事業継続計画策定（F）
         1. 7.1 目的・狙い

セキュリティインシデントは、 場合によってその企業の事業そのものの継続自体を脅かすこともある。

しかし、 地震等の自然災害と異なり、 セキュリティインシデントは原因や影響がすぐに特定できないことから、 ITサービスにインシデントが発生しても事業継続のためにITサービスを維持するのか、 被害拡大防止や原因究明のためにITサービス停止するのかの意思決定を企業として行う必要がある。

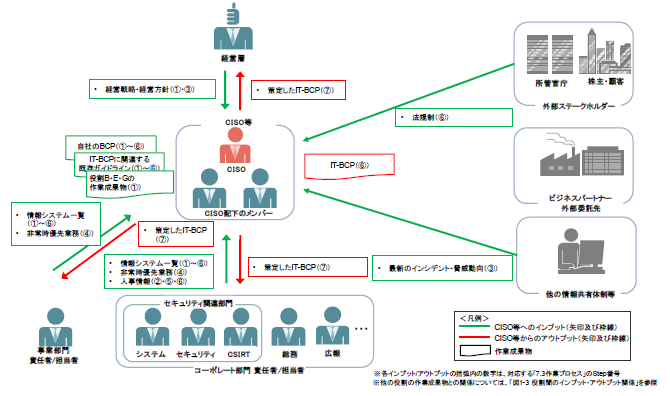
また、 仮にITサービスを停止したとしても、 企業価値を損なわないために、 事業継続できるよう行動計画を定めておくことが必要である。

本役割は、 サイバー攻撃等のセキュリティインシデント発生を想定したIT-BCPを策定することを目的としている。

なお、 本役割では、 セキュリティインシデントを考慮した事業継続に関わる行動計画・ルール等を便宜的に「セキュリティインシデント発生時のIT-BCP」と呼ぶ

何らかの特定の計画をドキュメントとして策定することが目的ではなく、 企業が既に有するBCPやIT-BCPと整合性の取れた形でセキュリティインシデント発生時に事業継続の観点を含んだ計画・ルール等を定めることを目的とするものである。

図 7-1 「セキュリティインシデント発生時の事業継続計画策定」の全体像

Subtopic  


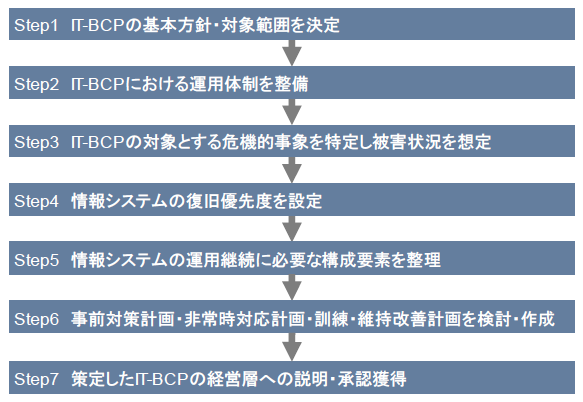
* + - * 1. 7.2 役割の作業内容

・事業継続との関係を考慮した上で、 インシデントを想定したIT-BCPを策定する。

・インシデント発生時の対応を円滑に行うために、 社内外にIT-BCPを説明し、 承認を得る。

* + - * 1. 7.3 作業プロセス

図 7-2 「セキュリティインシデント発生時の事業継続計画策定」の作業プロセス

Subtopic  


Step1 IT-BCPの基本方針・対象範囲を決定

セキュリティインシデント発生時の事業継続計画策定にあたり、 基本方針や対象範囲（対象となる事象、 システムの範囲等）を定める。

Step2 IT-BCPにおける運用体制を整備

セキュリティインシデント発生時の事業継続計画策定の対象範囲を踏まえ、 関係する組織（情報システム部、 事業部門、 コーポレート部門等）との間で検討・運用体制を整備する。

Step3 IT-BCPの対象とする危機的事象を特定し被害状況を想定

危機的事象における状況を明らかにし、 対象とするシステムの早期復旧や稼働継続を阻害する要因である被害状況を想定する。

Step4 情報システムの復旧優先度を設定

被害発生時に優先して復旧する業務を設定し、 目標とする復旧時間を確認した上で、 復旧優先度を定める。

Step5 情報システムの運用継続に必要な構成要素を整理

業務の復旧に必要なシステムを洗い出し、 そのシステムの復旧に必要な構成要素を分析する。 さらに、 システムの復旧優先度に従い、 対策目標を設定する。

必要な情報の収集にあたっては、 事業部門の協力を得る必要があり、 対策目標を定める際も、 事業部門の体制を考慮の上、 実現可能な計画を立案する必要があることから、 事業部門との良好なコミュニケーションを図ることが重要である。

Step6 事前対策計画・非常時対応計画・訓練・維持改善計画を検討・作成

危機的事象の発生時にシステムに生じる被害想定に対するシステムの脆弱性に関して、 その脆弱性を解消する対策を検討し、 事前対策計画として策定する。

システムの復旧活動に必要な対応体制を整備し、 発生から復旧までの対応を示した対応フローや手順書を非常時対応計画として策定する。

担当者の理解力や対応力を高めるために、 訓練計画を策定する。

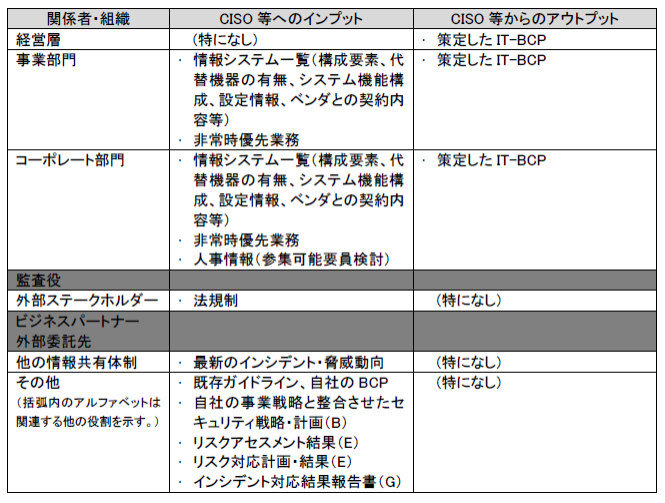
事前対策計画、 非常時対応計画、 訓練計画をそれぞれ定期的に見直し、 事業継続計画の実効性を継続的に維持するために、 維持改善計画を策定する。

Step7 策定したIT-BCPの経営層への説明・承認獲得

Step6で策定したIT-BCPを経営層に対して説明し、 承認を得る。 経営層から承認が得られなかった場合は、 Step6に戻り必要な修正を実施する。

* + - * 1. 7.4 作業に必要な情報

表 7-1 「セキュリティインシデント発生時の事業継続計画策定」に必要となる情報

Subtopic  


* + - * 1. 7.5 作業の目標成果

IT-BCP

* + - * 1. 7.6 作業で協同・連携する社内外の関係者と協同・連携の内容

・事業部門における事業継続要求と、 セキュリティ部門のセキュリティ対応可能な内容、 コーポレート部門における広報等の必要な対応内容を踏まえ、 実効的なIT-BCPを作成する。

・経営層、 事業部門、 コーポレート部門に対して、 IT-BCPを説明し、 承認を得る。

* + - 1. 8. セキュリティインシデント発生時の危機管理（G）
         1. 8.1 目的・狙い

セキュリティインシデント6により、 個人情報や機微情報が流出したり、 インフラ供給や重要なサービスの停止により社会に影響を与えたりした場合、 経営者は社会から経営責任が問われる可能性がある。

しかし、 サイバー攻撃は避けられないリスクである以上

非常時に迅速な対応が可能となるよう事前に対応計画や体制を整備すること

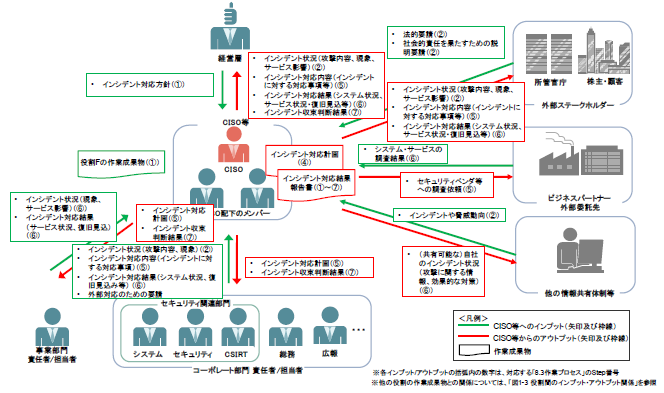
またインシデント発生後の通知先や開示が必要な項目に関して説明できるよう準備しておくこと

そして万が一インシデントによる被害が発生しても、 対応計画に則り、 適切に状況判断しながら、 対処していくこと

が、 企業価値を損なわないために必要である。

本役割は、 経営層がセキュリティインシデントの発生時、 企業価値を損なわないための機能を確実に維持することを目的としている。

図 8-1 「セキュリティインシデント発生時の危機管理」の全体像

Subtopic  


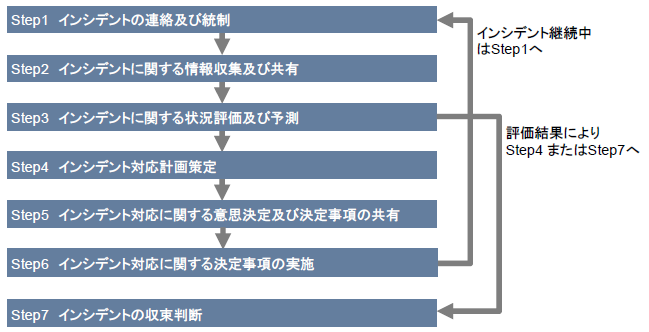
* + - * 1. 8.2 役割の作業内容

・インシデントに関する情報収集・評価を行い、 対応計画の策定と指示・管理を行う。

・社内外との調整等を行い、 インシデントを収束させる。

* + - * 1. 8.3 作業プロセス

図 8-2 「セキュリティインシデント発生時の危機管理」の作業プロセス

Subtopic  


Step1 インシデントの連絡及び統制

インシデントの状況を認識し、 経営層からのインシデント対応方針に基づき、 危機対応のための体制を構築する。

Step2 インシデントに関する情報収集及び共有

インシデントに関する情報を社内外から収集し、 経営層及びインシデント対応を行う各部門に共有する。

Step3 インシデントに関する状況評価及び予測

収集されたインシデントに関する情報に基づき、 インシデントや事業に関する状況を評価すると共に、 今後のインシデントの変化や事業の状況、 それに伴う事業に対する影響について予測を行う。

インシデントが収束したと判断した場合、 Step7に進む。

Step4 インシデント対応計画策定

Step3におけるインシデントに関する状況評価及び予測に基づき、 インシデント対応計画を策定する。

インシデント対応計画については、 各事業部門の責任者も策定する。 内容の整合性等については、 危機時に全社的に組織される危機管理委員会等の統率組織等において調整を行う等が考えられる。

Step5 インシデント対応に関する意思決定及び決定事項の共有

Step4で策定したインシデント対応計画に基づき、 セキュリティ関連部門を含むコーポレート部門や事業部門に対して、 各部門の所掌範囲に応じたインシデント対応計画についての指示を行う。

なお、 事業部門に対する指示は、 事業部門の責任者経由である場合と、 事業部門に直接である場合がある。

Step6 インシデント対応に関する決定事項の実施

インシデント対応に関する対応事項を実施する。 対応事項を指示した場合は、 その対応状況について把握を行う。

対応状況については、 （1）経営層／CISO等の指示があった場合、 （2）状況の変化があった場合、 （3）（状況の変化がなくとも）一定時間が経過した場合、 等、 適時のタイミングで把握し、 Step1に進む。

Step7 インシデントの収束判断

Step3のインシデントに関する状況評価結果により、 インシデントが収束したと判断する。

なお収束判断としては

(1)インシデントに対する応急措置が終了した場合

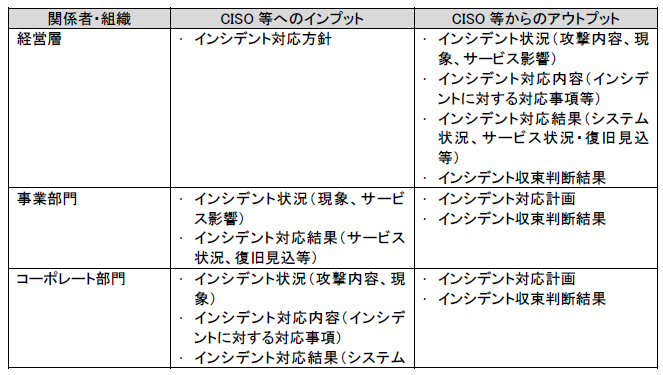
(2)インシデントの原因調査・復旧対応が終了した場合

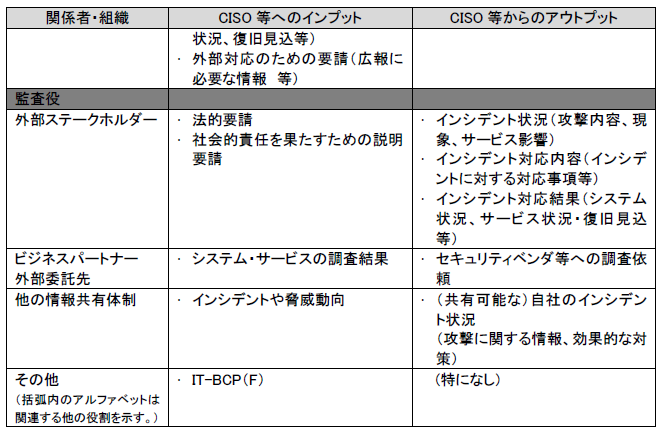
(3)正式な事故報告書の作成・影響を受けた顧客へのフォロー・再発防止策の検討等事後対応が終了した場合

等が想定される。

* + - * 1. 8.4 作業に必要な情報

表 8-1 「セキュリティインシデント発生時の危機管理」に必要となる情報

Subtopic  


Subtopic  


* + - * 1. 8.5 作業の目標成果

・インシデント対応結果報告書（社内向け）

* + - * 1. 8.6 作業で協同・連携する社内外の関係者と協同・連携の内容

・経営層に対して、 インシデント状況やインシデント対応内容・結果、 サービスの状況等についての適時の報告

・企業価値を損なわないための、 外部ステークホルダーに対する自社のインシデント状況、 サービスへの影響等に関する情報開示

・他の情報共有機関等とのインシデントや脅威動向に関する情報共有

* + - 1. 9. 付録： CISO等の経営・事業に関する役割のストーリー
         1. 1. 準大手産業機器メーカーA社： セキュリティガバナンス体制の構築・運営(A)
         2. 2． 中堅アパレルメーカーＸ社： セキュリティ投資計画の策定(C)
  1. 情報セキュリティ 10 大脅威2018【2018年3月IPA】
     1. 個人
        1. 第1位　インターネットバンキングやクレジットカード情報の不正利用
           1. ウイルス感染やフィッシング詐欺により、 インターネットバンキングの認証情報やクレジットカード情報が攻撃者に窃取され、 不正送金や不正利用が行われている。 2017年は、 インターネットバンキングの被害額は減少傾向だが、 新たに仮想通貨取引所の利用者を狙った攻撃が確認されている。
        2. 第2位　ランサムウェアによる被害
           1. ランサムウェアとは、 PCやスマートフォンにあるファイルの暗号化や画面のロックを行い、 復旧させることと引き換えに金銭を要求する手口に使われるウイルスである。 2017年は、 OSの脆弱性を悪用し、 感染した端末が接続しているネットワークを経路として感染を拡大させるタイプも登場している。 また、 感染した端末だけではなく、 その端末からアクセスできる共有サーバーや外付けHDDに保存されているファイルも暗号化されてしまう。
        3. 第3位　ネット上の誹謗・中傷
           1. コミュニティサイト（ブログ、 SNS、 掲示板等）上で、 個人や組織に対して誹謗・中傷や犯罪予告をする書き込みが行われている。 コミュニティサイトへの書き込みは、 匿名性や手軽さから安易に投稿してしまう傾向にある。 また、 SNSを使った犯罪は社会的な問題となっており、 2017年は殺人事件まで発展した事例もあった。
        4. 第4位　スマートフォンやスマートフォンアプリを狙った攻撃の可能性
           1. 不正アプリを利用者がインストールしてしまうことで、 スマートフォン内の重要な情報を窃取されたり、 不正に操作される被害が確認されている。 また、 データの暗号化等を行うランサムウェアに加えて、 2017年は個人情報を公開すると脅すランサムウェアも確認されている。 さらに、 これらの不正アプリは公式マーケットにも紛れ込んでおり、 公式マーケットであってもインストール前にアプリの信頼性について確認する等の警戒が必要である。
        5. 第5位　ウェブサービスへの不正ログイン
           1. ウェブサービスに不正ログインされ、 金銭的な被害や個人情報が窃取される等の被害が確認されている。 2017年に確認されたウェブサービスへの不正ログインの多くがパスワードリスト攻撃により行われている。 インターネットには多数のウェブサービスが存在しており、 ウェブサービスの利用者がパスワードの使いまわしや推測されやすいパスワードを使用している場合に、 不正ログインが行われてしまう。
        6. 第6位　ウェブサービスからの個人情報の窃取
           1. 2017年も引き続き、 ウェブサービスの脆弱性が悪用され、 ウェブサービス内に登録されている個人情報やクレジットカード情報を窃取される事件が多発している。 それらの情報を窃取されると、 攻撃者により個人情報を悪用して不審なメールを送信されたり、 クレジットカードを不正利用される可能性がある。
        7. 第7位　情報モラル欠如に伴う犯罪の低年齢化
           1. 2017年も未成年者がIT犯罪の加害者として逮捕、 補導される事件が確認されている。 IT犯罪に悪用できるツールや知識がインターネットを通じて誰でも入手・利用できるようになったことで、 情報モラルの欠如した未成年者が、 IT犯罪に手を染めやすくなっている。 また、 未成年者のPCやスマートフォンの所持も当たり前となってきており、 教員や親の監視が行き届きにくい。
        8. 第8位　ワンクリック請求等の不当請求
           1. PCやスマートフォンを利用中にアダルトサイトや出会い系サイト等にアクセスすることで金銭を不当に請求されるワンクリック請求の被害が依然として発生している。 1度のクリックによる請求だけでなく、 複数回のクリックをさせることで、 請求の正当性を主張して不当請求されてしまう事例も確認されている。
        9. 第9位　IoT 機器の不適切な管理
           1. 昨今、 IoT機器の利用が進んでいるが、 利用者はIoT機器がネットワークに接続されている機器であることを意識せずに利用してしまい、 適切な管理が行われていない。 そのような管理されていないIoT機器が攻撃者に狙われ、 分散型サービス妨害（DDoS）攻撃等に悪用されてしまう被害が確認されている。
        10. 第10位　偽警告
            1. PCやスマートフォンでウェブサイトを閲覧中に、 突然「ウイルスに感染している」等の偽警告を表示し、 利用者の不安を煽り、 偽警告の指示に従わせ、 個人情報等を窃取される被害が発生している。 偽警告は本物の警告と誤認されるように巧妙な細工が施されており、 被害者は信じて指示に従ってしまう。
     2. 組織
        1. 第1位　標的型攻撃による情報流出
           1. 企業や民間団体や官公庁等、 特定の組織を狙う、 標的型攻撃による攻撃が引き続き発生している。 メールの添付ファイルやウェブサイトを利用してPCにウイルスを感染させられると、 別のPCに感染を拡大され、 最終的に個人情報や業務上の重要情報が窃取される。
        2. 第2位　ランサムウェアによる被害
           1. ランサムウェアとは、 PC やスマートフォンにあるファイルの暗号化や画面のロックを行い、 復旧させることと引き換えに金銭を要求する手口に使われるウイルスである。 2017年は、 OSの脆弱性を悪用し、 感染した端末が接続しているネットワークを経路として感染を拡大させるタイプも登場している。 また、 感染した端末だけではなく、 その端末からアクセスできる共有サーバーや外付けHDDに保存されているファイルも暗号化されてしまう。 組織内のファイルが広範囲で暗号化された場合、 事業継続にも支障が出る可能性がある。
        3. 第3位　ビジネスメール詐欺
           1. 「ビジネスメール詐欺」（Business E-mail Compromise：BEC）は巧妙に細工したメールのやりとりにより、 企業の担当者を騙し、 攻撃者の用意した口座へ送金させる詐欺の手口である。 詐欺行為の準備としてウイルス等を悪用し、 企業内の従業員の情報が窃取されることもある。 これまでは主に海外の組織が被害に遭ってきたが、 2016年以降、 海外取引をしている国内企業でも被害が確認されている。
        4. 第4位　脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加
           1. 脆弱性対策情報の公開は、 脆弱性の脅威や対策情報を広く呼び掛けられるメリットがある。 一方、 その情報を攻撃者に悪用され、 対策前のシステムを狙う攻撃が行われている。 また、 近年では脆弱性情報の公開後、 その脆弱性を悪用した攻撃が本格化するまでの時間が短くなっている傾向がある。
        5. 第5位　セキュリティ人材の不足
           1. セキュリティ上の脅威は今後さらに増大するだけでなく、 新たな脅威も発生し続けていくことが予想される。 これらの脅威に対応するためにはセキュリティの知識、 技術を有するセキュリティ人材が欠かせないが、 圧倒的に不足しており、 問題視されている。 セキュリティ人材が手薄の組織では、 十分なセキュリティ対策、 対応をとることが難しく、 脅威の増大に伴い実被害につながることも考えられる。
        6. 第6位　ウェブサービスからの個人情報の窃取
           1. 2017年も引き続き、 ウェブサービスの脆弱性が悪用され、 ウェブサービス内に登録されている個人情報やクレジットカード情報等の重要な情報を窃取される被害が発生している。 それらの情報を窃取されると、 攻撃者により顧客や利用者の個人情報を悪用して不審なメールを送信されたり、 クレジットカードを不正利用される可能性がある。
        7. 第7位　IoT 機器の脆弱性の顕在化
           1. 2016年に引き続き、 IoT機器の脆弱性を悪用しウイルスに感染させることで、 インターネット上のサービスやサーバに対して、 大規模な分散型サービス妨害（DDoS）攻撃が行われる等の被害が確認されている。 また、 国内で発売されているIoT製品において脆弱性が発見されており、 機器を乗っ取られる、 または撮影機能等を悪用して個人情報を窃取されるといった危険性があることが公表されている。
        8. 第8位　内部不正による情報漏えい
           1. 組織内部の従業員や元従業員により、 私怨や金銭目的等の個人的な利益享受のため組織の情報が不正に持ち出されている。 また、 組織の情報持ち出しのルールを守らずに不正に情報を持ち出し、 さらにその情報を紛失し、 情報漏えいにつながることもある。 内部不正が発覚した場合、 組織は、 原因追求等の対応に追われ、 また社会的信用の失墜等にもつながる。
        9. 第9位　サービス妨害攻撃によるサービスの停止
           1. ウイルスに感染し、 ボットネット化した機器からDDoS（分散型サービス妨害）攻撃が行われ、 ウェブサイトやDNSサーバーが高負荷状態となり、 利用者がアクセスできなくなる被害が確認されている。 2017年は公式のアプリストアに公開されたスマートフォンアプリがボットネット化し、 DDoS攻撃が行われている。
        10. 第10位　犯罪のビジネス化（アンダーグラウンドサービス）
            1. 犯罪に使用するためのサービスやツールがアンダーグラウンド市場で取り引きされ、 これらを悪用した攻撃が行われている。 攻撃に対する専門知識に詳しくない者でもサービスやツールを利用することで、 容易に攻撃を行えるため、 サービスやツールが公開されると被害が広がるおそれがある。
  2. 監査人の警鐘 ‐ 2018年 情報セキュリティ十大トレンド【2018年1月5日JASA】

ドキュメントを参照: [security\_trend\_top10.html](http://www.jasa.jp/seminar/security_trend_top10.html)

* + 1. 多様化・巧妙化するランサムウェアの被害拡大
    2. 最新の対策もすり抜ける標的型攻撃による甚大な被害の発生
    3. セキュリティ機能が乏しいIoT製品への攻撃による社会的混乱
    4. クラウドなど集中管理による社会的規模の被害発生
    5. 考慮不足の働き方改革に起因する事故の発生
    6. 日本語ビジネスメール詐欺被害の拡大
    7. ガバナンス欠如のIT投資による重大インシデントの発生
    8. 成長しないマネジメントシステムによる組織活力の低下
    9. 形だけCSIRT/名ばかりセキュリティ人材による弊害の発生
    10. GDPR違反の摘発
  1. 2017年セキュリティ10大ニュース【2017年12月So-net】

ドキュメントを参照: [newstopics\_201712.html](http://www.so-net.ne.jp/security/news/newstopics_201712.html?SmRcid=mlc_ml_security_topics)

* + 1. 架空請求急増――実在企業かたるメール、 SMSが大量に出回る
    2. フィッシング多発――LINE、 グーグル、 アップル、 アマゾン、 マイクロソフト
    3. マルウェアメール頻発――添付の文書ファイルやメール内リンクで感染
    4. ランサムウェア騒動――Windows Updateとバックアップで対策
    5. 不正ログイン多発――「PW使い回し」狙うリスト攻撃でポイント不正利用
    6. 不正アクセス多発――脆弱性攻撃で大量の個人情報、 クレカ情報流出
    7. アマゾン「マーケットプレイス」で通販詐欺大量発生――返金後も残る不安
    8. ネット接続機器の問題が次々明らかに――脆弱性が放置される機器も多数
    9. マルウェア感染――文書ファイル、 スクリプトファイルが主流に
    10. Windows Vista、 Office 2007サポート終了――パッチ提供の緊急事態も
    11. 参考URL
        1. <注1：架空請求>
           1. ・実在企業名で「有料動画の未納料金が発生している」と脅すSMS詐欺に注意
           2. http://security-t.blog.so-net.ne.jp/2017-03-02

ドキュメントを参照: [2017-03-02](http://security-t.blog.so-net.ne.jp/2017-03-02)

* + - * 1. ・架空請求で高齢男性が被害5270万円――メールだけでなくハガキにも注意
        2. http://security-t.blog.so-net.ne.jp/2017-04-27-1

ドキュメントを参照: [2017-04-27-1](http://security-t.blog.so-net.ne.jp/2017-04-27-1)

* + - * 1. ・架空請求SMSのバラマキが連日発生、 被害相談でヒットする詐欺サイトにも注意
        2. http://security-t.blog.so-net.ne.jp/2017-05-29

ドキュメントを参照: [2017-05-29](http://security-t.blog.so-net.ne.jp/2017-05-29)

* + - * 1. ・「コンビニ払い」の架空請求に注意――仮想通貨購入口座に入金させる新手口
        2. http://security-t.blog.so-net.ne.jp/2017-07-03

ドキュメントを参照: [2017-07-03](http://security-t.blog.so-net.ne.jp/2017-07-03)

* + - * 1. ・「心当たりのないメール・SMSには反応しないで」国民生活センターが呼びかけ
        2. http://security-t.blog.so-net.ne.jp/2017-07-07-2

ドキュメントを参照: [2017-07-07-2](http://security-t.blog.so-net.ne.jp/2017-07-07-2)

* + - * 1. ・「架空請求詐欺」件数が1.7倍に。 今年上半期の特殊詐欺（警察庁）
        2. http://security-t.blog.so-net.ne.jp/2017-08-16

ドキュメントを参照: [2017-08-16](http://security-t.blog.so-net.ne.jp/2017-08-16)

* + - * 1. ・架空請求の被害急増――はがき、 メール、 SMSで届く未払い料金の請求に注意
        2. http://security-t.blog.so-net.ne.jp/2017-11-21

ドキュメントを参照: [2017-11-21](http://security-t.blog.so-net.ne.jp/2017-11-21)

* + - * 1. ・SMSを用いて有料動画サイトの未払料金などの名目で金銭を支払わせようとする「株式会社DMM.comをかたる事業者」に関する注意喚起［PDF］（消費者庁）
        2. http://www.caa.go.jp/policies/policy/consumer\_policy/information/pdf/170228adjustments\_1.pdf

ドキュメントを参照: [170228adjustments\_1.pdf](http://www.caa.go.jp/policies/policy/consumer_policy/information/pdf/170228adjustments_1.pdf)

* + - * 1. ・SMSを用いて有料動画の未納料金の名目で金銭を支払わせようとする「アマゾンジャパン合同会社等をかたる架空請求」に関する注意喚起［PDF］（消費者庁）
        2. http://www.caa.go.jp/policies/policy/consumer\_policy/information/pdf/consumer\_policy\_information\_171114\_0001.pdf

ドキュメントを参照: [consumer\_policy\_information\_171114\_0001.pdf](http://www.caa.go.jp/policies/policy/consumer_policy/information/pdf/consumer_policy_information_171114_0001.pdf)

* + - 1. <注2：フィッシング>
         1. ・2016年12月の国内フィッシング事情
         2. http://security-t.blog.so-net.ne.jp/2017-01-27

ドキュメントを参照: [2017-01-27](http://security-t.blog.so-net.ne.jp/2017-01-27)

* + - * 1. ・2017年1月の国内フィッシング事情
        2. http://security-t.blog.so-net.ne.jp/2017-02-06

ドキュメントを参照: [2017-02-06](http://security-t.blog.so-net.ne.jp/2017-02-06)

* + - * 1. ・2017年2月の国内フィッシング事情
        2. http://security-t.blog.so-net.ne.jp/2017-03-06

ドキュメントを参照: [2017-03-06](http://security-t.blog.so-net.ne.jp/2017-03-06)

* + - * 1. ・2017年3月、 4月の国内フィッシング事情
        2. http://security-t.blog.so-net.ne.jp/2017-05-09-3

ドキュメントを参照: [2017-05-09-3](http://security-t.blog.so-net.ne.jp/2017-05-09-3)

* + - * 1. ・2017年5月の国内フィッシング事情
        2. http://security-t.blog.so-net.ne.jp/2017-06-08-1

ドキュメントを参照: [2017-06-08-1](http://security-t.blog.so-net.ne.jp/2017-06-08-1)

* + - * 1. ・2017年6月の国内フィッシング事情
        2. http://security-t.blog.so-net.ne.jp/2017-07-05

ドキュメントを参照: [2017-07-05](http://security-t.blog.so-net.ne.jp/2017-07-05)

* + - * 1. ・2017年7月の国内フィッシング事情
        2. http://security-t.blog.so-net.ne.jp/2017-08-07

ドキュメントを参照: [2017-08-07](http://security-t.blog.so-net.ne.jp/2017-08-07)

* + - * 1. ・2017年8月の国内フィッシング事情
        2. http://security-t.blog.so-net.ne.jp/2017-09-11-1

ドキュメントを参照: [2017-09-11-1](http://security-t.blog.so-net.ne.jp/2017-09-11-1)

* + - * 1. ・2017年9月の国内フィッシング事情
        2. http://security-t.blog.so-net.ne.jp/2017-10-06-2

ドキュメントを参照: [2017-10-06-2](http://security-t.blog.so-net.ne.jp/2017-10-06-2)

* + - * 1. ・2017年10月の国内フィッシング事情
        2. http://security-t.blog.so-net.ne.jp/2017-11-24

ドキュメントを参照: [2017-11-24](http://security-t.blog.so-net.ne.jp/2017-11-24)

* + - * 1. ・2017年11月の国内フィッシング事情
        2. http://security-t.blog.so-net.ne.jp/2017-12-21

ドキュメントを参照: [2017-12-21](http://security-t.blog.so-net.ne.jp/2017-12-21)

* + - 1. <注3：マルウェアメール>
         1. ・さまざまな件名でマルウェア（ウイルス）付き日本語メール拡散中
         2. http://security-t.blog.so-net.ne.jp/2017-01-23

ドキュメントを参照: [2017-01-23](http://security-t.blog.so-net.ne.jp/2017-01-23)

* + - * 1. ・さまざまな件名で届く「バンキングマルウェア」メール――感染しないチェック法
        2. http://security-t.blog.so-net.ne.jp/2017-05-26

ドキュメントを参照: [2017-05-26](http://security-t.blog.so-net.ne.jp/2017-05-26)

* + - * 1. ・請求書を装うマルウェアメールに注意、 Excelマクロでマルウェア感染
        2. http://security-t.blog.so-net.ne.jp/2017-06-05

ドキュメントを参照: [2017-06-05](http://security-t.blog.so-net.ne.jp/2017-06-05)

* + - * 1. ・Excelファイルの添付メールに注意、 マルウェア感染のおそれ
        2. http://security-t.blog.so-net.ne.jp/2017-07-20

ドキュメントを参照: [2017-07-20](http://security-t.blog.so-net.ne.jp/2017-07-20)

* + - * 1. ・日本郵便など騙るマルウェアメールに注意――添付ファイルで不正送金ウイルス感染
        2. http://security-t.blog.so-net.ne.jp/2017-07-27-2

ドキュメントを参照: [2017-07-27-2](http://security-t.blog.so-net.ne.jp/2017-07-27-2)

* + - * 1. ・請求書メールに注意、 添付ファイルでマルウェア感染
        2. http://security-t.blog.so-net.ne.jp/2017-09-01

ドキュメントを参照: [2017-09-01](http://security-t.blog.so-net.ne.jp/2017-09-01)

* + - * 1. ・実在企業装うDL型マルウェアメール相次ぐ――リンク先クリックで感染のおそれ
        2. http://security-t.blog.so-net.ne.jp/2017-09-29

ドキュメントを参照: [2017-09-29](http://security-t.blog.so-net.ne.jp/2017-09-29)

* + - * 1. ・「詳しくはこちら」クリックに注意――自然な日本語のマルウェアメールが続々
        2. http://security-t.blog.so-net.ne.jp/2017-10-12-1

ドキュメントを参照: [2017-10-12-1](http://security-t.blog.so-net.ne.jp/2017-10-12-1)

* + - * 1. ・クレカの請求案内装うマルウェアメールに注意――明細確認で感染のおそれ
        2. http://security-t.blog.so-net.ne.jp/2017-10-24

ドキュメントを参照: [2017-10-24](http://security-t.blog.so-net.ne.jp/2017-10-24)

* + - * 1. ・実在企業装うマルウェアメールに注意、 リンクのクリックで感染のおそれ
        2. http://security-t.blog.so-net.ne.jp/2017-11-08

ドキュメントを参照: [2017-11-08](http://security-t.blog.so-net.ne.jp/2017-11-08)

* + - * 1. ・実在企業装うマルウェアメール頻発――ダウンロード型、 添付型それぞれの手口
        2. http://security-t.blog.so-net.ne.jp/2017-11-28

ドキュメントを参照: [2017-11-28](http://security-t.blog.so-net.ne.jp/2017-11-28)

* + - * 1. ・インターネットバンキングマルウェアに感染させるウイルス付メールに注意（JC3）
        2. https://www.jc3.or.jp/topics/virusmail.html

ドキュメントを参照: [virusmail.html](https://www.jc3.or.jp/topics/virusmail.html)

* + - 1. <注4：ランサムウェア>
         1. ・ランサムウェアの被害拡大、 今すぐWindows Updateとバックアップを（IPA）
         2. http://security-t.blog.so-net.ne.jp/2017-05-19-1
         3. ・さまざまな件名で届く「バンキングマルウェア」メール――感染しないチェック法
         4. http://security-t.blog.so-net.ne.jp/2017-05-26
         5. ・猛威ふるうランサムウェア、 国内上陸前に対策を
         6. http://security-t.blog.so-net.ne.jp/2017-06-29
         7. ・請求書メールに注意、 添付ファイルでマルウェア感染
         8. http://security-t.blog.so-net.ne.jp/2017-09-01
         9. ・文書ファイル悪用感染に新手口――誤操作でPC内ファイル暗号化のおそれ
         10. http://security-t.blog.so-net.ne.jp/2017-11-06
      2. <注5：不正ログイン>
         1. ・「リスト型攻撃」相次ぐ――同じID・パスワードの使いまわしに注意
         2. http://security-t.blog.so-net.ne.jp/2017-10-06
      3. <注6：不正アクセス>
         1. ・不正アクセス相次ぐ～通販サイトで情報漏えい、 便乗フィッシングに注意
         2. http://security-t.blog.so-net.ne.jp/2017-01-06
         3. ・情報流出事故相次ぐ――都税と住宅金融機構のクレカ支払いサイト、 ジェトロ、 法政大
         4. http://security-t.blog.so-net.ne.jp/2017-03-14-2
         5. ・不正アクセスで情報流出　日本郵便、 沖縄電力、 2社のオンラインショップ
         6. http://security-t.blog.so-net.ne.jp/2017-03-17-1
         7. ・サーバーソフトの欠陥でクレカ情報など流出――不正使用630万円
         8. http://security-t.blog.so-net.ne.jp/2017-04-27-2
         9. ・サーバーソフトの欠陥による個人情報流出、 国交省や総務省のサイトでも
         10. http://security-t.blog.so-net.ne.jp/2017-06-13
      4. <注7：通販詐欺>
         1. ・大手通販サイトで「注文した商品が届かない」トラブル続出
         2. http://security-t.blog.so-net.ne.jp/2017-04-28
      5. <注8：機器の脆弱性>
         1. ・Androidなど「Bluetooth搭載端末」数十億台に影響する脆弱性が明らかに
         2. http://security-t.blog.so-net.ne.jp/2017-09-14
         3. ・ルーターやネットワークカメラに脆弱性――危険な状態で使っていないかチェックを
         4. http://security-t.blog.so-net.ne.jp/2017-09-15
         5. ・多数の無線LAN機器に影響する脆弱性が明らかに――通信が盗聴されるおそれ
         6. http://security-t.blog.so-net.ne.jp/2017-10-20
         7. ・ドコモのモバイルルーター「Wi-Fi STATION L-02F」に脆弱性、 早急に更新を
         8. http://security-t.blog.so-net.ne.jp/2017-11-07-1
         9. ・バッファローの有線ルータに脆弱性、 最新のファームウェアに更新を
         10. http://security-t.blog.so-net.ne.jp/2017-12-05-1
         11. ・BlueBorne：様々な Bluetooth 実装に複数の脆弱性(jvn)
         12. https://jvn.jp/vu/JVNVU95513538/index.html
         13. ・KRACK：Wi-Fi Protected Access II (WPA2) ハンドシェイクにおいて Nonceおよびセッション鍵が再利用される問題（jvn）
         14. https://jvn.jp/vu/JVNVU90609033/index.html
      6. <注9：マルウェア感染>
         1. ・さまざまな件名でマルウェア（ウイルス）付き日本語メール拡散中
         2. http://security-t.blog.so-net.ne.jp/2017-01-23
         3. ・Word文書送り付けるゼロデイ攻撃が発生中、 Officeに影響する脆弱性発覚
         4. http://security-t.blog.so-net.ne.jp/2017-04-11-2
         5. ・さまざまな件名で届く「バンキングマルウェア」メール――感染しないチェック法
         6. http://security-t.blog.so-net.ne.jp/2017-05-26
         7. ・請求書を装うマルウェアメールに注意、 Excelマクロでマルウェア感染
         8. http://security-t.blog.so-net.ne.jp/2017-06-05
         9. ・Excelファイルの添付メールに注意、 マルウェア感染のおそれ
         10. http://security-t.blog.so-net.ne.jp/2017-07-20
         11. ・日本郵便など騙るマルウェアメールに注意――添付ファイルで不正送金ウイルス感染
         12. http://security-t.blog.so-net.ne.jp/2017-07-27-2
         13. ・うっかり操作でマルウェア感染、 IPAが文書ファイルの新たな悪用手口を解説
         14. http://security-t.blog.so-net.ne.jp/2017-08-02
         15. ・請求書メールに注意、 添付ファイルでマルウェア感染
         16. http://security-t.blog.so-net.ne.jp/2017-09-01
         17. ・実在企業装うDL型マルウェアメール相次ぐ――リンク先クリックで感染のおそれ
         18. http://security-t.blog.so-net.ne.jp/2017-09-29
         19. ・「詳しくはこちら」クリックに注意――自然な日本語のマルウェアメールが続々
         20. http://security-t.blog.so-net.ne.jp/2017-10-12-1
         21. ・クレカの請求案内装うマルウェアメールに注意――明細確認で感染のおそれ
         22. http://security-t.blog.so-net.ne.jp/2017-10-24
         23. ・文書ファイル悪用感染に新手口――誤操作でPC内ファイル暗号化のおそれ
         24. http://security-t.blog.so-net.ne.jp/2017-11-06
         25. ・実在企業装うマルウェアメールに注意、 リンクのクリックで感染のおそれ
         26. http://security-t.blog.so-net.ne.jp/2017-11-08
         27. ・実在企業装うマルウェアメール頻発――ダウンロード型、 添付型それぞれの手口
         28. http://security-t.blog.so-net.ne.jp/2017-11-28
         29. ・危険な「添付ファイル」――感染を防ぐ基本設定、 誤開封後の対処法
         30. http://www.so-net.ne.jp/security/news/newstopics\_201708.html
      7. <注10：サポート終了>
         1. ・（サポート終了）Vistaは4月11日、 Office 2007は10月10日――対策必須
         2. http://security-t.blog.so-net.ne.jp/2017-02-13
         3. ・MS、 4月度のセキュリティパッチを公開　Vistaのパッチはこれが最後
         4. http://security-t.blog.so-net.ne.jp/2017-04-12-1
         5. ・マイクロソフト、 6月度の月例セキュリティパッチを公開――XPやVista用のパッチも
         6. http://security-t.blog.so-net.ne.jp/2017-06-14-1
         7. ・マイクロソフト、 月例セキュリティパッチを公開。 「Office 2007」サポート終了
         8. http://security-t.blog.so-net.ne.jp/2017-10-12
         9. ・実在企業装うマルウェアメール頻発――ダウンロード型、 添付型それぞれの手口
         10. http://security-t.blog.so-net.ne.jp/2017-11-28
         11. ・2017年6月のセキュリティ更新プログラム（月例）（マイクロソフト）
         12. https://blogs.technet.microsoft.com/jpsecurity/2017/06/14/201706-security-bulletin/

ドキュメントを参照: [201706-security-bulletin](https://blogs.technet.microsoft.com/jpsecurity/2017/06/14/201706-security-bulletin/)

* 1.  サイバーセキュリティ経営ガイドライン Ver 2.0【2017年11月16日METI】

ドキュメントを参照: [20171116003-1.pdf](http://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf)

* + 1. サイバーセキュリティ経営ガイドライン・概要
       1. I．サイバーセキュリティは経営問題
          1. セキュリティ対策の実施を「コスト」と捉えるのではなく、 将来の事業活動・成長に必須なものと位置づけて「投資」と捉えることが重要
          2. セキュリティ投資は必要不可欠かつ経営者としての責務である。
       2. II．経営者が認識すべき３原則
          1. (1) 経営者は、 サイバーセキュリティリスクを認識し、 リーダーシップによって対策を進めることが必要
          2. (2) 自社は勿論のこと、 ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
          3. (3) 平時及び緊急時のいずれにおいても、 サイバーセキュリティリスクや対策に係る情報開示など、 関係者との適切なコミュニケーションが必要
       3. III．サイバーセキュリティ経営の重要１０項目
          1. 指示１：サイバーセキュリティリスクの認識、 組織全体での対応方針の策定
          2. 指示２：サイバーセキュリティリスク管理体制の構築
          3. 指示３：サイバーセキュリティ対策のための資源（予算、 人材等）確保
          4. 指示４：サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
          5. 指示５：サイバーセキュリティリスクに対応するための仕組みの構築
          6. 指示６：サイバーセキュリティ対策におけるPDCAサイクルの実施
          7. 指示７：インシデント発生時の緊急対応体制の整備
          8. 指示８：インシデントによる被害に備えた復旧体制の整備
          9. 指示９：ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握
          10. 指示１０：情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供
    2. １．はじめに
       1. １．１．サイバーセキュリティ経営ガイドラインの背景と位置づけ
          1. 本ガイドラインのVer1.0、 及び1.1は、 経済産業省と独立行政法人情報処理推進機構（IPA）の共催である「サイバーセキュリティリスクと企業経営に関する研究会」、 Ver2.0は「サイバーセキュリティ経営ガイドライン改訂に関する研究会」においてそれぞれ検討が行われ、 とりまとめたものである。
          2. また、 内閣サイバーセキュリティセンター（NISC）では、 企業の経営層を対象としてグローバルな競争環境の変化の中でサイバーセキュリティをより積極的な経営への「投資」と位置づけ、 企業の自発的な取組を促進するため、 サイバーセキュリティの基本的な考え方と企業の視点別の取組方法について、 考え方を示した文書（「企業経営のためのサイバーセキュリティの考え方」5）を策定している。

中小企業の情報セキュリティ対策ガイドライン(IPA)

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

企業経営のためのサイバーセキュリティの考え方（NISC）

ドキュメントを参照: [keiei.pdf](http://www.nisc.go.jp/active/kihon/pdf/keiei.pdf)

* + - 1. １．２．本ガイドラインの構成と活用方法
         1. 巻頭の概要は経営者向け、 ２章～３章はサイバーセキュリティ対策を実施する上での責任者である担当幹部（CISO等）及びセキュリティ担当者向けである。
         2. 経営者においては、 最低限、 巻頭の概要に目を通した上で、 ３原則を認識し、 重要１０項目についてCISO等に指示をすべきである。
         3. CISO等は、 経営者の指示に基づき、 重要１０項目の各解説頁の「対策例」も参考にしつつ、 セキュリティ対策の取組みを、 セキュリティ担当者に対してより具体的に指示をし、 推進することが必要である。
         4. また、 本ガイドラインでは、 重要１０項目の実施にあたって、 参考となる情報を付録として提示している。 各付録の内容は以下の通りである。

付録A 重要１０項目が適切に実施されているかどうかを確認するためのチェックシート

付録B サイバーセキュリティ対策を実施する上で参考となる資料等

付録C インシデント発生時に原因調査等を行う際、 組織内で整理しておくべき事項

付録D 重要１０項目とISO/IEC27001、 27002の関係性

付録E 本ガイドラインで使用している用語の定義

* + - * 1. なお、 内部犯行による情報漏えい等のリスクへの対処については、 必要に応じ、 「組織における内部不正防止ガイドライン」（IPA）6を参照することで、 より効果的な対策が可能となる。

組織における内部不正防止ガイドライン（IPA）

ドキュメントを参照: [000044615.pdf](https://www.ipa.go.jp/files/000044615.pdf)

* + - * 1. また、 サイバーセキュリティ対策にこれから取り組む企業においては「中小企業の情報セキュリティ対策ガイドライン」（IPA）も参考となる。
    1. ２．経営者が認識すべき３原則
       1. （１） 経営者は、 サイバーセキュリティリスクを認識し、 リーダーシップによって対策を進めることが必要
          1. 【経営者自らがリーダーシップを発揮して適切な経営資源の配分を行う】
          2.  ビジネス展開や企業内の生産性の向上のためにITサービス等の提供やITを利活用する機会は増加傾向にあり、 サイバー攻撃が避けられないリスクとなっている現状において、 経営戦略としてのセキュリティ投資は必要不可欠かつ経営者としての責務である。
          3.  また、 サイバー攻撃などにより情報漏えいや事業継続性が損なわれるような事態が起こった後、 企業として迅速かつ適切な対応ができるか否かが会社の命運を分ける。
          4.  このため、 サイバーセキュリティリスクを多様な経営リスクの中での一つとして位置づけ、 サイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO等）を任命するとともに、 経営者自らがリーダーシップを発揮して適切な経営資源の配分を行うことが必要である。
       2. （２） 自社は勿論のこと、 ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
          1. 【自社のみならず、 サプライチェーンのビジネスパートナーやシステム管理等の委託先を含めたセキュリティ対策を徹底する】
          2.  サプライチェーンのビジネスパートナーやシステム管理等の委託先がサイバー攻撃に対して無防備であった場合、 自社から提供した重要な情報が流出してしまうなどの問題が生じうる。
          3.  このため、 自社のみならず、 サプライチェーンのビジネスパートナーやシステム管理等の委託先を含めたセキュリティ対策を徹底することが必要である。
       3. （３） 平時及び緊急時のいずれにおいても、 サイバーセキュリティリスクや対策に係る情報開示など、 関係者との適切なコミュニケーションが必要
          1. 【平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行う】
          2.  万一サイバー攻撃による被害が発生した場合、 関係者と、 平時から適切なセキュリティリスクのコミュニケーションができていれば，関係者の不信感の高まりを抑えることができる。
          3.  このため、 平時から実施すべきサイバーセキュリティ対策を行っていることを明らかにするなどのコミュニケーションを積極的に行うことが必要である。
    2. ３．サイバーセキュリティ経営の重要１０項目
       1. 経営者は、 CISO等に対して、 以下の１０項目を指示し、 着実に実施させるとともに、 実施内容についてCISO等から定期的に報告を受けることが必要である。 自組織での対応が困難な項目については、 外部委託によって実施することも検討する。
       2. ３．１．サイバーセキュリティリスクの管理体制構築
          1. 指示１ サイバーセキュリティリスクの認識、 組織全体での対応方針の策定

サイバーセキュリティリスクを経営リスクの一つとして認識し、 組織全体での対応方針（セキュリティポリシー）を策定させる。

対策を怠った場合のシナリオ

・経営者がサイバーセキュリティリスクへの対応を策定し、 宣言していないと、 サイバーセキュリティ対策などの実行が組織の方針と一貫したものとならない。

・トップの宣言により、 ステークホルダー（株主、 顧客、 取引先など）の信頼性を高め、 ブランド価値向上につながるが、 宣言がない場合は、 企業におけるサイバーセキュリティへの重要度がステークホルダーに伝わらず信頼性を高める根拠がないこととなる。

* + - * 1. 指示２ サイバーセキュリティリスク管理体制の構築

サイバーセキュリティ対策を行うため、 サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる。

その際、 組織内のその他のリスク管理体制とも整合を取らせる。

対策を怠った場合のシナリオ

・サイバーセキュリティリスクの管理体制を整備していない場合、 組織としてサイバーセキュリティリスクの把握が出来ない。

・組織内におけるその他のリスク管理体制との整合を取らないと、 組織全体としてのリスク管理の方針と不整合が生じる恐れがある。

* + - * 1. 指示３ サイバーセキュリティ対策のための資源（予算、 人材等）確保

サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる。

対策を怠った場合のシナリオ

・適切な予算確保が出来ていない場合、 組織内でのサイバーセキュリティ対策の実施や人材の確保が困難となるほか、 信頼できる外部のベンダへの委託が困難となる恐れがある。

・適切な処遇の維持、 改善ができないと、 有能なサイバーセキュリティ人材を自社にとどめておくことができない。

* + - 1. ３．２．サイバーセキュリティリスクの特定と対策の実装
         1. 指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

経営戦略の観点から守るべき情報を特定させた上で、 サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、 リスクに対応するための計画を策定させる。

その際、 サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、 残留リスクを識別させる。

対策を怠った場合のシナリオ

・企業の経営戦略に基づき、 各企業の状況に応じた適切なリスク対応を実施しなければ、 過度な対策により通常の業務遂行に支障をきたすなどの不都合が生じる恐れがある。

・受容できないリスクが残る場合、 想定外の損失を被る恐れがある

* + - * 1. 指示５ サイバーセキュリティリスクに対応するための仕組みの構築

サイバーセキュリティリスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築させる。

対策を怠った場合のシナリオ

・サイバーセキュリティリスクに応じた適切な対策が行われていない場合、 サイバー攻撃が発生した場合の被害が拡大する可能性がある。

・技術的な取組を行っていたとしても、 攻撃の検知・分析とそれに基づく対応ができるよう、 適切な運用が行われていなければ、 サイバー攻撃の状況を正確に把握することができず、 攻撃者に組織内の重要情報を窃取されるなどの、 致命的な被害に発展する恐れがある。

* + - * 1. 指示６ サイバーセキュリティ対策におけるPDCAサイクルの実施

計画を確実に実施し、 改善していくため、 サイバーセキュリティ対策をPDCAサイクルとして実施させる。

その中で、 定期的に経営者に対策状況を報告させた上で、 問題が生じている場合は改善させる。

また、 ステークホルダーからの信頼性を高めるため、 対策状況を開示させる。

対策を怠った場合のシナリオ

・PDCA（Plan[計画]、 Do[実行]、 Check[実施状況の確認・評価]、 Act[改善]）を実施する体制が出来ていないと、 立てた計画が確実に実行されない恐れがある。

・最新の脅威への対応ができているかといった視点も踏まえて組織のサイバーセキュリティ対策を定期的に見直さないと、 サイバーセキュリティを巡る環境変化に対応できず、 新たに発生した脅威に対応できない恐れがある。

・適切な開示を行わなかった場合、 社会的責任の観点から、 事業のサイバーセキュリティリスク対応についてステークホルダーの信頼を失うとともに、 インシデント発生時に企業価値が大きく低下する恐れがある。

* + - 1. ３．３．インシデント発生に備えた体制構築 3
         1. 指示７ インシデント発生時の緊急対応体制の整備

影響範囲や損害の特定、 被害拡大防止を図るための初動対応、 再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT等）を整備させる。

被害発覚後の通知先や開示が必要な情報を把握させるとともに、 情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。

また、 インシデント発生時の対応について、 適宜実践的な演習を実施させる。

対策を怠った場合のシナリオ

・緊急時の対応体制を整備していないと、 原因特定のための調査作業において、 組織の内外の関係者間のコミュニケーションが取れず、 速やかな対処ができない。

・速やかな情報開示が行われない場合、 顧客や取引先等にも被害が及ぶ恐れがあり、 損害賠償請求など責任を問われる場合がある。

・法的な取り決めがあり、 所管官庁等への報告が義務づけられている場合、 速やかな通知がないことにより、 罰則等を受ける場合がある。

・演習を実施していないと、 不測の事態が起こった際に、 担当者が緊急時に適切に行動することが出来ない。

* + - * 1. 指示８ インシデントによる被害に備えた復旧体制の整備

インシデントにより業務停止等に至った場合、 企業経営への影響を考慮していつまでに復旧すべきかを特定し、 復旧に向けた手順書策定や、 復旧対応体制の整備をさせる。

BCPとの連携等、 組織全体として整合のとれた復旧目標計画を定めさせる。

また、 業務停止等からの復旧対応について、 適宜実践的な演習を実施させる。

対策を怠った場合のシナリオ

・重要な業務が適切な時間内に復旧できず、 企業経営に致命的な影響を与える恐れがある。

・演習を実施していないと、 不測の事態が起こった際に、 担当者が緊急時に適切に行動することが出来ない。

* + - 1. ３．４．サプライチェーンセキュリティ対策の推進
         1. 指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

監査の実施や対策状況の把握を含むサイバーセキュリティ対策のPDCAについて、 系列企業、 サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせる。

システム管理等の委託について、 自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。

中小企業自らがセキュリティ対策に取り組むことを宣言する制度

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

対策を怠った場合のシナリオ

・系列企業やサプライチェーンのビジネスパートナーにおいて適切なサイバーセキュリティ対策が行われていないと、 これらの企業を踏み台にして自社が攻撃されることもある。 その結果、 他社の２次被害を誘発し、 加害者となる恐れもある。 また、 緊急時の原因特定などの際に、 これらの企業からの協力を得られないことにより事業継続に支障が生ずる。

・システム管理などの委託業務において、 自組織で対応する部分と委託する部分の境界が不明確となり、 対策漏れが生じる恐れがある。

* + - 1. ３．５．ステークホルダーを含めた関係者とのコミュニケーションの推進
         1. 指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び 提供

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、 サイバー攻撃に関する情報共有活動へ参加し、 積極的な情報提供及び情報入手を行わせる。

また、 入手した情報を有効活用するための環境整備をさせる。

対策を怠った場合のシナリオ

・情報共有活動への参加により、 解析した攻撃手法などの情報を用いて、 他社における同様の被害を未然に防止することができるが、 情報共有ができていないと、 社会全体において常に新たな攻撃として対応することとなり、 企業における対応コストが低減しない。

* + 1. 付録Ａ サイバーセキュリティ経営チェックシート
       1. ※本チェックシートは、 基本的な項目を示しており、 企業の状況に応じて追加対策等を行うことも重要である
       2. ※以降では、 本チェック項目とNISTが提供するサイバーセキュリティフレームワーク10との対応関係も合わせて提示する（括弧書きはサイバーセキュリティフレームワークのサブカテゴリーの識別子に対応）
       3. Framework for Improving Critical Infrastructure Cybersecurity(NIST)

ドキュメントを参照: [cybersecurity-framework-021214.pdf](https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf)

* + - 1. ＜経営者がリーダーシップをとったセキュリティ対策の推進＞
         1. （サイバーセキュリティリスクの管理体制構築）

指示１ サイバーセキュリティリスクの認識、 組織全体での対応方針の策定

経営者がサイバーセキュリティリスクを経営リスクの1つとして認識している

(－)

経営者が、 組織全体としてのサイバーセキュリティリスクを考慮した対応方針（セキュリティポリシー）を策定し、 宣言している

ID.GV-1: 自組織の情報セキュリティポリシーを定めている。

A.5.1.1 情報セキュリティのための方針群

法律や業界のガイドライン等の要求事項を把握している

ID.GV-3: プライバシーや市民の自由に関する義務を含む、 サイバーセキュリティに関する法規制上の要求事項を理解し、 管理している。

A.18.1 法的及び契約上の要求事項の順守

DE.DP-2: 検知活動は必要なすべての要求事項を満たしている。

A.18.1.4 プライバシー及び個人を特定できる情報（PII）の保護

指示２ サイバーセキュリティリスク管理体制の構築

組織の対応方針（セキュリティポリシー）に基づき、 CISO等からなるサイバーセキュリティリスク管理体制を構築している

(－)

サイバーセキュリティリスク管理体制において、 各関係者の役割と責任を明確にしている

ID.GV-2: 情報セキュリティ上の役割と責任について、 内部と外部パートナーとで調整・連携している。

A.6.1.1 情報セキュリティの役割及び責任

A.7.2.1 経営陣の責任

組織内のリスク管理体制とサイバーセキュリティリスク管理体制の関係を明確に規定している

ID.GV-4: ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している。

(ISO N/A)

指示３ サイバーセキュリティ対策のための資源（予算、 人材等）確保

必要なサイバーセキュリティ対策を明確にし、 経営会議などで対策の内容に見合った適切な費用かどうかを評価し、 必要な予算を確保している

(－)

サイバーセキュリティ対策を実施できる人材を確保し、 各担当者が自身の役割を理解している（組織の内外問わず）

PR.AT-2: 権限を持つユーザが役割と責任を理解している。

A.6.1.1 情報セキュリティの役割及び責任

A.7.2.2 情報セキュリティの意識向上， 教育及び訓練

PR.AT-3: 第三者である利害関係者（例：供給業者、 顧客、 パートナー）が役割と責任を理解している。

A.6.1.1 情報セキュリティの役割及び責任

A.7.2.2 情報セキュリティの意識向上， 教育及び訓練

PR.AT-4: 上級役員が役割と責任を理解している。

A.6.1.1 情報セキュリティの役割及び責任

A.7.2.2 情報セキュリティの意識向上， 教育及び訓練

PR.AT-5: 物理セキュリティおよび情報セキュリティの担当者が役割と責任を理解している。

A.6.1.1 情報セキュリティの役割及び責任

A.7.2.2 情報セキュリティの意識向上， 教育及び訓練

組織内でサイバーセキュリティ人材を育成している

PR.AT-1: すべてのユーザに情報を周知し、 トレーニングを実施している。

A.7.2.2 情報セキュリティの意識向上， 教育及び訓練

組織内のサイバーセキュリティ人材のキャリアパスの設計を検討、 及び適正な処遇をしている

(－)

セキュリティ担当者以外も含めた従業員向けセキュリティ研修等を継続的に実施している

PR.AT-1: すべてのユーザに情報を周知し、 トレーニングを実施している。

A.7.2.2 情報セキュリティの意識向上， 教育及び訓練

* + - * 1. （サイバーセキュリティリスクの特定と対策の実装）

指示４ サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

守るべき情報を特定し、 当該情報の保管場所やビジネス上の価値等に基づいて優先順位付けを行っている

ID.AM-1: 企業内の物理デバイスとシステムの一覧を作成している。

A.8.1.1 資産目録

A.8.1.2 資産の管理責任

ID.AM-2: 企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している。

A.8.1.1 資産目録

A.8.1.2 資産の管理責任

ID.AM-3: 企業内の通信とデータの流れの図を用意している。

A.13.2.1 情報転送の方針及び手順

ID.AM-4: 外部情報システムの一覧を作成している。

A.11.2.6 構外にある装置及び資産のセキュリティ

ID.AM-5: リソース（例：ハードウェア、 デバイス、 データ、 ソフトウェア）を、 分類、 重要度、 ビジネス上の価値に基づいて優先順位付けしている。

A.8.2.1 情報の分類

特定した守るべき情報に対するサイバー攻撃の脅威、 脆弱性を識別し、 経営戦略を踏まえたサイバーセキュリティリスクとして把握している

ID.RA-3: 内外からの脅威を特定し、 文書化している。

(ISO N/A)

ID.RA-1: 資産の脆弱性を特定し、 文書化している。

A.12.6.1 技術的脆弱性の管理

A.18.2.3 技術的順守のレビュー

ID.RM-1: リスク管理プロセスが自組織の利害関係者によって確立、 管理され、 承認されている。

(ISO N/A)

サイバーセキュリティリスクが事業にいかなる影響があるかを推定している

ID.RA-4: ビジネスに対する潜在的な影響と、 その可能性を特定している。

(ISO N/A)

ID.RA-5: リスクを判断する際に、 脅威、 脆弱性、 可能性、 影響を考慮している。

A.12.6.1 技術的脆弱性の管理

ID.RM-2: 自組織のリスク許容度を決定し、 明確にしている。

(ISO N/A)

サイバーセキュリティリスクの影響の度合いに従って、 リスク低減、 リスク回避、 リスク移転のためのリスク対応計画を策定している

ID.RA-6: リスクに対する対応を定め、 優先順位付けしている。

(ISO N/A)

ID.RM-3: 企業によるリスク許容度の決定が、 重要インフラにおける自組織の役割と、 その分野に特化したリスク分析の結果に基づいて行われている。

(ISO N/A)

サイバーセキュリティリスクの影響の度合いに従って対策を取らないと判断したものを残留リスクとして識別している

ID.RA-6: リスクに対する対応を定め、 優先順位付けしている。

(ISO N/A)

ID.RM-3: 企業によるリスク許容度の決定が、 重要インフラにおける自組織の役割と、 その分野に特化したリスク分析の結果に基づいて行われている。

(ISO N/A)

指示５ サイバーセキュリティリスクに対応するための仕組みの構築

重要業務を行う端末、 ネットワーク、 システム、 またはサービスにおいて、 ネットワークセグメントの分離、 アクセス制御、 暗号化等の多層防御を実施している。

アクセス制御（PR.AC）: 資産および関連施設へのアクセスを、 承認されたユーザ、 プロセス、 またはデバイスと、 承認された活動およびトランザクションに限定している。

A.9 アクセス制御

A.11 物理的及び環境的セキュリティ

A.13 通信のセキュリティ

データセキュリティ（PR.DS）: 情報と記録（データ）を情報の機密性、 完全性、 可用性を保護するために定められた自組織のリスク戦略に従って管理している。

A.8 資産の管理

A.12 運用のセキュリティ

A.13 通信のセキュリティ

A.14 システムの取得、 開発及び保守

システム等に対して脆弱性診断を実施し、 検出された脆弱性に対処している。

PR.IP-12: 脆弱性管理計画を作成し、 実施している。

A.12.6.1 技術的脆弱性の管理

A.18.2.2 情報セキュリティのための方針群及び標準の順守

検知すべきイベント（意図していないアクセスや通信）を特定し、 当該イベントを迅速に検知するためのシステム・手順・体制（ログ収集や分析のための手順書策定）を構築している。

DE.AE-1: ネットワーク運用のベースラインと、 ユーザとシステム間の予測されるデータの流れを特定し、 管理している。

(ISO N/A)

DE.AE-5: インシデント警告の閾値を定めている。

(ISO N/A)

DE.DP-3: 検知プロセスをテストしている。

A.14.2.8 システムセキュリティの試験

意図していないアクセスや通信を検知した場合の対応計画（検知したイベントによる影響、 対応者などの責任分担等）を策定している

DE.AE-4: イベントがもたらす影響を特定している。

(ISO N/A)

DE.DP-1: 説明責任を果たせるよう、 検知に関する役割と責任を明確に定義している

A.6.1.1 情報セキュリティの役割及び責任

DE.DP-4: イベント検知情報を適切な関係者に伝達している。

A.6.1.2 職務の分離

サイバー攻撃の動向等を踏まえて、 サイバーセキュリティリスクへの対応内容（検知すべきイベント、 技術的対策の強化等）を適宜見直している

DE.DP-5: 検知プロセスを継続的に改善している。

A.16.1.6 情報セキュリティインシデントからの学習

従業員に対して、 サイバーセキュリティに関する教育（防御の基本となる対策実施（ソフトウェアの更新の徹底、 マルウェア対策ソフトの導入等）の周知、 標的型攻撃メール訓練など）を実施している。

PR.AT-1: すべてのユーザに情報を周知し、 トレーニングを実施している。

A.7.2.2 情報セキュリティの意識向上， 教育及び訓練

指示６ サイバーセキュリティ対策におけるPDCAサイクルの実施

経営者が定期的に、 サイバーセキュリティ対策状況の報告を受け、 把握している

(－)

サイバーセキュリティにかかる外部監査を実施している

(－)

サイバーセキュリティリスクや脅威を適時見直し、 環境変化に応じた取組体制（PDCA）を整備・維持している

PR.IP-7: 保護プロセスを継続的に改善している。

(ISO N/A)

サイバーセキュリティリスクや取組状況を外部に公開している

(－)

* + - * 1. （インシデント発生に備えた体制構築）

指示７ インシデント発生時の緊急対応体制の整備

組織の内外における緊急連絡先・伝達ルートを整備している（緊急連絡先には、 システム運用、 Webサイト保守・運用、 契約しているセキュリティベンダの連絡先含む）

RS.CO-3: 対応計画に従って情報を共有している。

A.16.1.2 情報セキュリティ事象の報告

RS.CO-4: 対応計画に従って、 利害関係者との間で調整を行っている。

(ISO N/A)

RS.CO-5: サイバーセキュリティに関する状況認識を深めるために、 外部利害関係者との間で任意の情報共有を行っている。

(ISO N/A)

サイバー攻撃の初動対応マニュアルを整備している

PR.IP-9: 対応計画（インシデント対応および事業継続）と復旧計画（インシデントからの復旧および災害復旧）を実施し、 管理している。

A.16.1.1 責任及び手順

A.17.1.1 情報セキュリティ継続の計画

A.17.1.2 情報セキュリティ継続の実施

復旧計画（RC.RP）: サイバーセキュリティイベントによる影響を受けたシステムや資産をタイムリ ーに復旧できるよう、 復旧プロセスおよび手順を実施し、 維持している。

A.16.1.5 情報セキュリティインシデントへの対応

インシデント対応の専門チーム（CSIRT等）を設置している

RS.CO-1: 対応が必要になった時の自身の役割と行動の順番を従業員は認識している。

A.6.1.1 情報セキュリティの役割及び責任

A.16.1.1 責任及び手順

経営者が責任を持って組織の内外へ説明ができるように、 経営者への報告ルート、 公表すべき内容やタイミング等を定めている

RS.CO-2: 定められた基準に沿って、 イベントを報告している。

A.6.1.3 関係当局との連絡

A.16.1.2 情報セキュリティ事象の報告

インシデント対応の課題も踏まえて、 初動対応マニュアルを見直している

RC.IM-1: 学んだ教訓を復旧計画に取り入れている。

(ISO N/A)

RC.IM-2: 復旧戦略を更新している。

(ISO N/A)

インシデント収束後の再発防止策の策定も含めて、 定期的に対応訓練や演習を行っている

PR.IP-10: 対応計画と復旧計画をテストしている。

A.17.1.3 情報セキュリティ継続の検証、 レビュー及び評価

指示８ インシデントによる被害に備えた復旧体制の整備

被害が発生した場合に備えた業務の復旧計画を策定している

ID.BE-5: 重要サービスの提供を支援する、 レジリエンスに関する要求事項を定めている。

A.11.1.4 外部及び環境の脅威からの保護

A.17.1.1 情報セキュリティ継続の計画

A.17.1.2 情報セキュリティ継続の実施

A.17.2.1 情報処理施設の可用性

PR.IP-9: 対応計画（インシデント対応および事業継続）と復旧計画（インシデントからの復旧および災害復旧）を実施し、 管理している。

A.16.1.1 責任及び手順

A.17.1.1 情報セキュリティ継続の計画

A.17.1.2 情報セキュリティ継続の実施

復旧計画（RC.RP）: サイバーセキュリティイベントによる影響を受けたシステムや資産をタイムリ ーに復旧できるよう、 復旧プロセスおよび手順を実施し、 維持している。

A.16.1.5 情報セキュリティインシデントへの対応

復旧作業の課題を踏まえて、 復旧計画を見直している

RC.IM-1: 学んだ教訓を復旧計画に取り入れている。

(ISO N/A)

RC.IM-2: 復旧戦略を更新している。

(ISO N/A)

組織の内外における緊急連絡先・伝達ルートを整備している

RC.CO-1: 広報活動を管理している。

(ISO N/A)

RC.CO-2: イベント発生後に評判を回復している。

(ISO N/A)

RC.CO-3: 復旧活動について内部利害関係者と役員、 そして経営陣に伝達している。

(ISO N/A)

定期的に復旧対応訓練や演習を行っている

PR.IP-10: 対応計画と復旧計画をテストしている。

A.17.1.3 情報セキュリティ継続の検証、 レビュー及び評価

* + - 1. ＜サプライチェーンセキュリティ対策の推進＞
         1. 指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

システム管理などについて、 自組織のスキルや各種機能の重要性等を考慮して、 自組織で対応できる部分と外部に委託する部分を適切に切り分けている

ID.BE-3: 企業のミッション、 目標、 活動に関して優先順位を定め、 伝達している。

(ISO N/A)

ID.BE-4:重要サービスを提供する上での依存関係と重要な機能を把握している。

ISO/IEC 27001:2013 A.11.2.2, A.11.2.3, A.12.1.3

A.11.2.2 サポートユーティリティ（ライフライン事業者）

A.11.2.3 ケーブル配線のセキュリティ

A.12.1.3 容量・能力の管理

委託先が実施すべきサイバーセキュリティ対策について、 契約書等により明確にしている

ID.AM-6: すべての従業員と第三者である利害関係者（例：供給業者、 顧客、 パートナー）に対して、 サイバーセキュリティ上の役割と責任を定めている。

A.6.1.1 情報セキュリティの役割及び責任

ID.BE-1: サプライチェーンにおける企業の役割を特定し、 伝達している

A.15.1.3 ICTサプライチェーン

A.15.2.1 供給者のサービス提供の監視及びレビュー

A.15.2.2 供給者のサービス提供の変更に対する管理

PR.IP-8: 保護技術の有効性について、 適切なパートナーとの間で情報を共有している。

A.16.1.6 情報セキュリティインシデントからの学習

系列企業、 サプライチェーンのビジネスパートナーやシステム管理の運用委託先などのサイバーセキュリティ対策状況（監査を含む）の報告を受け、 把握している

(－)

* + - 1. ＜ステークホルダーを含めた関係者とのコミュニケーションの推進＞
         1. 指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

各種団体が提供するサイバーセキュリティに関する注意喚起情報やコミュニティへの参加等を通じて情報共有（情報提供と入手）を行い、 自社の対策に活かしている

ID.RA-2: 情報共有フォーラム／ソースより、 脅威と脆弱性に関する情報を入手している。

A.6.1.4 専門組織との連絡

マルウェア情報、 不正アクセス情報、 インシデントがあった場合に、 IPAへの届出や一般社団法人JPCERTコーディネーションセンターへの情報提供、 その他民間企業等が推進している情報共有の仕組みへの情報提供を実施している

ID.RA-2: 情報共有フォーラム／ソースより、 脅威と脆弱性に関する情報を入手している。

A.6.1.4 専門組織との連絡

* + 1. 付録Ｂ サイバーセキュリティ対策に関する参考情報
       1. 重要１０項目全般に関連する参考情報
          1. サイバーセキュリティ経営ガイドライン解説書[Ver.1.0]（IPA）

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

（サイバーセキュリティ経営ガイドラインの３原則、 重要１０項目を具体的に実施するための考え方について解説。 ）

* + - * 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]（IPA）

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

(中小企業がセキュリティ対策に取り組む上でのポイントを解説したガイドライン。 最低限対策が求められる「情報セキュリティ5か条」や、 企業のセキュリティ対策状況を診断する「5分でできる！情報セキュリティ自社診断」等の付録も提供。 )

* + - * 1. ISO/IEC 27002:2013（ISO/IEC）

（情報マネジメントシステムの仕様を定めた国際標準規格であり、 情報セキュリティ管理のベストプラクティスを提供。 ）

* + - * 1. Framework for Improving Critical Infrastructure Cybersecurity [Version 1.0]（NIST）【2014 年2 月12 日】

ドキュメントを参照: [cybersecurity-framework-021214.pdf](https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf)

重要インフラに係わる企業向けに実施すべきセキュリティ対策を「特定」、 「防御」、 「検知」、 「対応」、 「復旧」の5つの機能に分類し、 さらにそれらの機能を22のカテゴリーで提示した米国のガイドライン。 重要インフラ以外の企業でも活用可能。 ）

重要インフラのサイバーセキュリティを向上させるためのフレームワーク【IPA和訳】

ドキュメントを参照: [000038957.pdf](https://www.ipa.go.jp/files/000038957.pdf)

* + - * 1. SP800-53 [Rev.4]（NIST）

ドキュメントを参照: [NIST.SP.800-53r4.pdf](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)

（連邦政府機関が実施すべきセキュリティ対策を提示した米国のガイドライン。 米国連邦政府向けのクラウドサービスを提供する際に、 本ガイドラインへの準拠が要求される場合がある。 ）

* + - * 1. SP800-171 [Rev.1]（NIST）

ドキュメントを参照: [NIST.SP.800-171r1.pdf](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf)

（連邦政府機関以外の組織及び情報システムに対するCUI11を保護する上で実施すべきセキュリティ対策を提示した米国のガイドライン。 米国連邦政府関係の業務を受託する際に、 本ガイドラインへの準拠が要求される場合がある。 ）

* + - 1. 指示３に関連する参考情報
         1. ITのスキル指標を活用した情報セキュリティ人材育成ガイド[2015年5月]（IPA）

ドキュメントを参照: [000039528.pdf](https://www.ipa.go.jp/files/000039528.pdf)

（サイバー攻撃等を防ぐためにどのような対策が必要で、 その対策を実施するためにはどのような人材が必要なのかを例示し、 人材育成を行うためのヒントをまとめたガイドライン。 ）

* + - * 1. 職場の情報セキュリティ管理者のためのスキルアップガイド[2015年9月]（IPA）

ドキュメントを参照: [000047872.pdf](https://www.ipa.go.jp/files/000047872.pdf)

（セキュリティ上の脅威を取り上げ、 被害を防ぐためにはどのような対策を実施すべきかを例示し、 セキュリティ管理者としての役割を具体的に提示したガイドライン。 ）

* + - 1. 指示４に関連する参考情報
         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]（IPA）

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

（本ガイドラインの4章にてリスク分析の手法を解説。 また、 リスク分析の実施を支援するリスク分析シートも付録して提示。 ）

* + - 1. 指示５に関連する参考情報
         1. 「高度標的型攻撃」対策に向けたシステム設計ガイド[2014年9月]（IPA）

ドキュメントを参照: [000046236.pdf](https://www.ipa.go.jp/files/000046236.pdf)

（標的型攻撃対策として、 システム内部への侵入を前提とした上で、 侵害拡大防止及び監視強化を目的とした内部対策について解説したガイドライン。 ）

* + - * 1. 高度サイバー攻撃への対処におけるログの活用と分析方法[1.0版]（JPCERT/CC）

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

（サイバー攻撃への備えと効果的な対策の観点から、 一般的に利用される機器に攻撃者の活動の痕跡をログとして残すための考え方、 それらのログから痕跡を見つけ出す方法等を記載したガイドライン。 ）

* + - * 1. 組織における内部不正防止ガイドライン[第4版]（IPA）

ドキュメントを参照: [000057060.pdf](https://www.ipa.go.jp/files/000057060.pdf)

（組織における内部不正を防止するために実施すべき対策として、 10の観点（コンプライアンス、 職場環境等）のもと30項目の対策を提示したガイドライン。 ）

* + - * 1. 秘密情報の保護ハンドブック[平成28年2月]（経済産業省）

ドキュメントを参照: [trade-secret.htm](http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.htm)

（秘密情報の漏えいを未然に防止するための対策例を集めて紹介したハンドブック。 ）

* + - 1. 指示６に関連する参考情報
         1. 情報セキュリティマネジメントシステム（ISMS）適合性評価制度（JIPDEC）

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

（情報セキュリティマネジメントシステムにおける国際標準規格ISO/IEC27001に基づいて第三者認証を行う制度。 ）

* + - * 1. サイバーセキュリティマネジメントシステム（CSMS）適合性評価制度（JIPDEC）

ドキュメントを参照: [csms.html](https://isms.jp/csms.html)

（産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムにおける国際標準規格IEC62443-2に基づいて第三者認証を行う制度。 ）

* + - * 1. 情報セキュリティ管理基準（経済産業省）

ドキュメントを参照: [index.html](http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html)

（情報セキュリティマネジメントの構築から具体的な管理策に至るまで包括的な内容を含み、 国際標準規格ISO/IEC27001とも整合を持った基準。 ）

* + - * 1. 情報セキュリティ対策ベンチマーク（IPA）

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

（Web上で質問に答えることによって、 自社のセキュリティ対策の実施状況を散布図、 レーダーチャート、 スコア等で表示するツール。 自社の対策状況を他社の対策状況と比較することも可能。 ）

* + - * 1. 安全なウェブサイトの作り方[第7版]（IPA）

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

（セキュリティを考慮したWebサイトを作成するための技術的な対策を提示したガイドライン。 別冊としてWebサイトに脆弱性が存在していないかを確認するためのテスト項目を提示したウェブ健康診断仕様等も提供。 ）

* + - * 1. JVN（IPA、 JPCERT/CC）

ドキュメントを参照: [jvn.jp](https://jvn.jp/)

（日本で使用されているソフトウェア等の脆弱性関連情報とその対策情報を提供する、 脆弱性対策情報ポータルサイト。 ）

* + - 1. 指示７に関連する参考情報
         1. CSIRT構築マテリアル（JPCERT/CC）

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

（組織的なインシデント対応を行うためのCSIRTを構築する上で、 「構想フェーズ」、 「構築フェーズ」、 「運用フェーズ」のそれぞれの段階で考慮すべきポイントを解説したガイドライン。 ）

* + - * 1. CSIRT構築に役立つ参考資料（日本シーサート協議会）

ドキュメントを参照: [build-wg-document.html](http://www.nca.gr.jp/activity/build-wg-document.html)

（CSIRTの構築に際し、 構築初心者／経営者向け説明時／構築担当者の企画・構築・運用の各段階におけるドキュメント類をまとめた参考資料集。 ）

* + - 1. 指示８に関連する参考情報
         1. 事業継続ガイドライン[平成25年8月改定]（内閣府）

ドキュメントを参照: [guideline03.pdf](http://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline03.pdf)

（事業継続計画の策定・改善にあたって、 事業継続の必要性を明示し、 実施が必要な事項、 望ましい事項等を提示したガイドライン。 ）

* + - 1. 指示９に関連する参考情報
         1. 情報サービス・ソフトウェア産業における下請適正取引等の推進のためのガイドライン[平成29年3月]（経済産業省）

ドキュメントを参照: [140313shitaukeGL3.pdf](http://www.chusho.meti.go.jp/keiei/torihiki/2014/140313shitaukeGL3.pdf)

（下請適正取引等の推進を図ることを目的として策定したものであり、 個人情報保護やセキュリティ対策に係る取り組み等の考慮すべき事項を解説したガイドライン。 ）

* + - * 1. SECURITY ACTION セキュリティ対策自己宣言（IPA）

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

（中小企業がセキュリティ対策に取り組むことを自己宣言する制度。 ）

* + - 1. 指示１０に関連する参考情報
         1. 届出・相談・情報提供（不正アクセスやウイルス等に関する届出）（IPA）

ドキュメントを参照: [todoke-top-j.html](https://www.ipa.go.jp/security/outline/todoke-top-j.html)

（コンピュータウイルス、 不正アクセス、 脆弱性関連情報等に関する届出を行う際の届出様式、 届出先、 届出状況等を提供するWebサイト。 ）

* + - * 1. 標的型サイバー攻撃特別相談窓口（IPA）

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

（標的型サイバー攻撃を受けた際に、 専門的知見を有する相談員が対応する窓口。 ）

* + - * 1. サイバー情報共有イニシアティブ（J-CSIP）（IPA）

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

（重要インフラで利用される機器の製造業者、 電力業界、 ガス業界、 化学業界、 石油業界、 資源開発業界、 自動車業界、 クレジット業界において情報共有と早期対応を行うための活動。 ）

* + - * 1. @police（警察庁）

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

（サイバー犯罪・サイバーテロの未然防止及び被害の拡大防止を図るために、 ネットワークセキュリティに関する様々な情報を提供するWebサイト。 ）

* + 1. 付録C インシデント発生時に組織内で整理しておくべき事項

ドキュメントを参照: [20171116003-2.xlsx](http://www.meti.go.jp/press/2017/11/20171116003/20171116003-2.xlsx)

* + - 1. インシデント発生時、 原因調査等を行う際に組織内で整理しておくべき事項を示す。 本資料の内容を参考に原因調査等を行い、 必要な事項については適宜経営者や関係者に報告を行うことが望ましい。 本付録では、 以下の5つの表を提供する。 インシデントの状況に応じて該当する表を利用すること（案件により複数の表を利用することもある。 例えば、 不正アクセスにより情報漏えいが発生した場合は表1、 表2、 表4を利用する）
      2. 表1 基本項目 全てのインシデントで共通して調査すべき項目
      3. 表2 情報漏えいに係る項目 情報漏えいが発生した際に調査すべき項目
      4. 表3 ウイルス感染に係る項目 ウイルス感染が発生した際に調査すべき項目
      5. 表4 不正アクセスに係る項目 不正アクセスを受けた際に調査すべき項目
      6. 表5 （D）DoSに係る項目 （D）DoS攻撃を受けた際に調査すべき項目
    1. 付録Ｄ 国際規格ISO/IEC27001及び27002との関係
    2. 付録Ｅ 用語の定義
       1. （1） インシデント
          1. サイバーセキュリティ分野において、 サイバーセキュリティリスクが発現・現実化した事象のこと。
       2. （2） 監査
          1. 組織内においてサイバーセキュリティ対策が適切に実施されているかどうかを判定するために、 監査証拠を収集し、 それを客観的に評価するための、 体系的で、 独立し、 文書化したプロセスのこと。 監査は、 内部監査（第一者）または外部監査（第二者・第三者）のいずれでも、 または複合監査（複数の分野の組合せ）でもあり得る。
       3. （3） サイバー攻撃
          1. コンピュータシステムやネットワークに、 悪意を持った攻撃者が不正に侵入し、 データの窃取・破壊や不正プログラムの実行等を行うこと。
       4. （4） サイバーセキュリティ
          1. サイバーセキュリティとは、 電子データの漏えい・改ざん等や、 期待されていたITシステムや制御システム等の機能が果たされないといった不具合が生じないようにすること。
       5. （5） サイバーセキュリティリスク
          1. サイバーセキュリティリスクとは、 サイバーセキュリティに関連して不具合が生じ、 それによって企業の経営に何らかの影響が及ぶ可能性のこと。
       6. （6） 残留リスク
          1. リスク対応（回避、 低減、 移転）後に残るリスク。 保有リスクともいう。
       7. （7） 情報セキュリティ報告書
          1. 企業の情報管理・情報システム等のセキュリティの取組の中でも社会的関心の高いものについて情報開示することにより、 当該企業の取組が顧客や投資家などのステークホルダーから適正に評価されることを目指すもの。
          2. （参考： 経済産業省の「情報セキュリティ報告書モデル」：

ドキュメントを参照: [2007\_JohoSecurityReportModelRevised.pdf）](http://www.meti.go.jp/policy/netsecurity/docs/secgov/2007_JohoSecurityReportModelRevised.pdf）)

* + - 1. （8） ステークホルダー
         1. 意思決定もしくは活動に影響を与え、 影響されることがあるまたは影響されると認知している、 あらゆる人または組織。 具体的には、 株主、 債権者、 顧客、 取引先等である。
      2. （9） セキュリティポリシー
         1. 企業・組織におけるセキュリティに関する理念である意図と方針を経営者が正式に表明したもの。 セキュリティポリシーに沿って、 組織内セキュリティ対策が規定される。
      3. （10）多層防御
         1. 物理層、 ネットワーク層からデータ層までの多層防御を導入することで、 １つの機器やソフトウェアに依存する拠点防御対策や、 単一の境界防御層（主としてネットワーク境界）に依存する対策の場合より、 未知のマルウェアや新たな攻撃手法の登場により容易に突破されるリスクの軽減が期待される。
         2. IPAでは、 多層防御の１例として、 以下四つのポイントを紹介している。 ①ソフトウェア感染リスクの低減、 ②重要業務を行う端末やネットワークの分離、 ③重要情報が保存されているサーバでの制限、 ④事後対応の準備。
      4. （11）ビジネスパートナー
         1. 業務の委託先や受託元、 物品・サービスの調達先等の取引関係のある企業のこと。
      5. （12）マルウェア
         1. セキュリティ上の被害を及ぼすウイルス、 スパイウエア、 ボットなどの悪意をもったプログラムを指す総称。 これらのプログラムは、 使用者や管理者の意図に反して（あるいは気づかぬうちに）コンピュータに入り込み悪意ある行為を行う。
      6. （13）リスク
         1. 国際規格（ISO/IEC 27000）では、 ｢諸目的に対する不確かさの影響｣と定義されている。
      7. （14）リスク対応（回避、 低減、 移転、 保有）
         1. 対処の方法には、 大きく分けて「リスク回避」、 「リスク低減」、 「リスク移転」、 「リスク保有」の４つがある。 なお、 さらに詳細化した分類として、 JIS Q 0073リスクマネジメント用語では、 リスク回避、 機会を追及するためのリスクを取るまたは増加させる、 リスク源の除去、 起こりやすさを変更すること、 結果を変えること、 リスク移転、 リスク保有の７分類が定義されている。
         2. ① リスク回避

「リスク回避」とは、 脅威発生の要因を停止あるいは全く別の方法に変更することにより、 リスクが発生する可能性を取り去ることである。 例えば、 「インターネットからの不正侵入」という脅威に対し、 外部との接続を断ち、 Web上での公開を停止してしまうような場合などが該当する。

* + - * 1. ② リスク低減

「リスク低減」とは、 脆弱性に対してセキュリティ対策を講じることにより、 脅威発生の可能性を下げることである。 ノートパソコンの紛失、 盗難、 情報漏えいなどに備えて保存する情報を暗号化しておく、 サーバ室に不正侵入できないようにバイオメトリック認証技術を利用した入退室管理を行う、 従業員に対するセキュリティ教育を実施することなどが該当する。

* + - * 1. ③ リスク移転

「リスク移転」とは、 リスクを他社などに移すことである。 例えば、 リスクが顕在化したときに備え、 保険で損失をカバーすることや、 組織内のITシステムの運用を他社に委託し、 契約などにより不正侵入やマルウェア感染の被害に対して損害賠償などの形で移転すること等が該当する。

* + - * 1. ④ リスク保有

「リスク保有」とは、 ある特定のリスクにより、 起こり得る損失の負担を受容することである。

* + - 1. （15）リスク評価
         1. リスクの大きさが、 受容可能かまたは許容可能かを決定するために、 リスク分析の結果をリスク基準（リスクの重大性を評価するために目安とする条件であり、 組織の目的並びに外部環境および内部環境に基づいたもの）と比較するプロセスのこと。
      2. （16）リスク分析
         1. リスクの特質を理解し、 リスクレベル（ある事象の結果とその起こりやすさとの組合せとして表現される、 リスクの大きさ）を決定するプロセスのこと。
      3. （17）ログ
         1. コンピュータの利用状況やデータの通信記録。 操作を行った者のIDや操作日付、 操作内容などが記録される。 セキュリティ上、 インシデントの原因追究などに利用する。
      4. （18）BCP（Business Continuity Plan）
         1. 企業が自然災害、 テロ攻撃、 サイバー攻撃などによる被害が発生した場合において、 中核となる事業の継続、 早期復旧を実現するために、 平時及び緊急時における事業継続のため手段等を取り決めておく計画のこと。
      5. （19）CISO（Chief Information Security Officer）
         1. 経営陣の一員、 もしくは経営トップからその役を任命された、 セキュリティ対策を実施する上での責任者のこと。
      6. （20）CSIRT（Computer Security Incident Response Team）
         1. インシデントの発生に対応するための体制のこと。
      7. （20）PDCA
         1. Plan - Do - Check - Act の略。 品質改善や環境マネジメントでよく知られた手法であり、 次のステップを繰り返しながら、 継続的に業務を改善していく手法の１つのこと。
         2. 1.Plan：問題を整理し、 目標を立て、 その目標を達成するための計画を立てる。
         3. 2.Do：目標と計画をもとに、 実際の業務を行う。
         4. 3.Check：実施した業務が計画通り行われて、 当初の目標を達成しているかを確認し、 評価する。
         5. 4.Act：評価結果をもとに、 業務の改善を行う。
  1. 情報セキュリティ白書2017【2017年7月IPA】

ドキュメントを参照: [2017.html](https://www.ipa.go.jp/security/publications/hakusyo/2017.html)

* + 1. 序章 2016年度の情報セキュリティの概況
    2. 第1章 情報セキュリティインシデント・脆弱性の現状と対策
       1. 1.1 2016年度に観測されたインシデント状況
       2. 1.2 情報セキュリティインシデント別の状況と事例
       3. 1.3 攻撃・手口の動向と対策
       4. 1.4 情報システムの脆弱性の動向
       5. 1.5 情報セキュリティ対策の状況
    3. 第2章 情報セキュリティを支える基盤の動向
       1. 2.1 日本の情報セキュリティ政策の状況
       2. 2.2 情報セキュリティ関連法の整備状況
       3. 2.3 国別・地域別の情報セキュリティ政策の状況
       4. 2.4 情報セキュリティ人材の現状と育成
       5. 2.5 情報セキュリティマネジメント
       6. 2.6 国際標準化活動
       7. 2.7 評価認証制度
       8. 2.8 情報セキュリティの普及啓発活動
       9. 2.9 情報セキュリティ産業の規模と成長の動向
       10. 2.10 その他の情報セキュリティの状況
    4. 第3章 個別テーマ
       1. 3.1 制御システムの情報セキュリティ
       2. 3.2 IoTの情報セキュリティ
       3. 3.3 スマートデバイスの情報セキュリティ
       4. 3.4 金融の情報セキュリティ
       5. 3.5 オリンピックに向けた情報セキュリティ対策
    5. 付録 情報セキュリティ10大脅威2017・資料・ツール
       1. 情報セキュリティ10大脅威2017
       2. 資料A 2016年のコンピュータウイルス届出状況
       3. 資料B 2016年のコンピュータ不正アクセス届出状況
       4. 資料C ソフトウェア等の脆弱性関連情報に関する届出状況
       5. ツール 各ツールの紹介
  1. 匿名加工情報の事例集（JIPDEC認定個人情報保護団体対象事業者向け）【PDF】【2017年7月JIPDEC】

ドキュメントを参照: [AOP\_006.pdf](https://www.jipdec.or.jp/protection_org/u71kba00000001hh-att/AOP_006.pdf)

* 1. 改正個人情報保護法（2017年5月改正施行）対応

ドキュメントを参照: [news005.html](http://www.atmarkit.co.jp/ait/articles/1704/24/news005.html)

* + 1. 背景
       1. 攻撃を検知するためだけのIT投資とは、 いわば 守りの投資 であり、 企業に利益を生み出すものではありません
       2. そのため、 経営者に投資の目的を納得させるのが難しい場合もあるでしょう
       3. 事実としてサイバー攻撃への対処は経営課題であり、 そのための投資は企業にとって不可欠
       4. なぜなら、 それによって企業のイノベーションに弊害が及ぶからです
    2. 「全体最適」の視点でバランスの取れたセキュリティ対策を
       1. サイバー攻撃の脅威を無視することは、 新しい事業を生み出す先進的なアイデアとエネルギーを奪ってしまうことを意味する
       2. マルウェアの侵入には入口対策とエンドポイント対策で対処し、 外部との通信路の確立やサーバとの不正通信は出口対策や内部対策で防ぐといった具合
       3. さらに、 もしこれらが突破されてしまった場合にはログを取得／保全して説明責任を果たせるように するなど、 システム全体でバランスの取れた設計を考えることが何よりも重要
    3. 統合的にデザインすることがセキュリティの強化につながる
       1. セキュリティの強化を意識しすぎるあまり、 業務運用にまで悪影響を及ぼしては本末転倒だ。 業務上、 必要な経路は開きつつ、 適切に監視を行うことが肝要
       2. システムを設計する際やイノベーションを起こすためのプラットフォームを構築する際、 セキュリティは全体最適の視点で設計する
       3. 業務全体のデザインとセキュリティのデザインを合わせて統合的にデザイン
       4. こうすることでセキュリティ施策の価値が一層高まり、 セキュリティのための投資ではなくイノベーションのための投資として説明し、 経営者から必要な投資を得やすくなるのです
    4. 改正個人情報保護法のポイント
       1. 個人情報の定義が変更され、 従来の個人情報に加えて個人識別符号の定義（免許証番号、 マイナンバー、 生体情報など）が追加
       2. 人種や病歴、 犯罪歴といった要配慮個人情報が新設
       3. 改正個人情報保護法にどう対応すべきかを解説したガイドラインは2016年11月30日に公開

ドキュメントを参照: [preparation](http://www.ppc.go.jp/personal/preparation/)

* + - * 1. ポイントは「組織的安全管理措置」に記載された「取扱状況の把握及び安全管理措置の見直し」
        2. これは監査できちんとチェックし、 経営者に報告して改善を図っているかを問うもの
        3. もし現状の安全管理措置が十分でない場合でも、 きちんと監査が行われていれば対応レベルは向上していくはず
        4. 今後は、 個人情報に関して何かインシデントが起きた際には、 報告命令や業務改善命令、 緊急命令などの大きな権限を持つ個人情報保護委員会から何らかの指導を受けるといった事態も起こり得るため
    1. 匿名加工情報でデータの利活用が容易に
       1. 匿名加工を施して本人を再識別できないようにした情報ならば、 本人の同意なしで他社に提供できるようになる
    2. クレジットカード番号など民間付与の番号も個人情報に海外移転にも規制
       1. 個人情報の定義が明確化され、 氏名、 住所、 電話番号などの一般的な個人情報に加えて、 マスターと突合して個人が特定できる情報も個人情報として取り扱われることとなった。
       2. 例えば、 民間企業が扱うクレジットカード番号、 口座番号、 企業固有の顧客番号、 社員番号、 会社のメールアドレスなども対象となる。
       3. また、 個人識別符号が新たに定義され、 パスポート番号、 運転免許証番号、 健康保険者番号、 マイナンバーなどの公文書に振られた番号、 さらにはDNA配列、 指紋、 静脈、 虹彩といった身体の一部および歩行時の姿勢や動作など人の動きを表したものも対象となり、 これらに対して格別の安全管理措置が求められる
       4. 技術的安全管理対策の観点では、 暗号化について新たな指針が提示された。
       5. 2017年2月16日に個人情報保護委員会が告示「個人データの漏えい等の事案が発生した場合等の対応について」を公表。 この中では、 個人情報を高度に暗号化した場合は秘匿性が高まるため、 万一漏えいした際にも、 国（および本人）への報告義務は許容されるなどの指針が示されている。
    3. 2018年には「EUデータ保護規則」が施行
       1. 「忘れられる権利」や、 自分の個人情報を持つ企業に対して他社への移転を要求する「データポータビリティ」が追加されるなど、 いくつかの規制強化が図られている。
       2. EUデータ保護規則では、 これに対応した仕組みを初めから設計（バイデザイン）して業務に組み込む（バイデフォルト）ことを求めており、 自社で監査して何か問題があれば報告すべしとされている。 これは企業の情報セキュリティ施策にも大きくかかわる方針であり、 今後、 各社のIT部門が特に留意すべき点だと言えよう。
    4. データを中心に据えた「多層防御」で機密情報を守る
       1. システム側で対応すべき事項として「暗号化」と「ログの収集と監査／検知」、 そして「アクセス制御」
       2. バイデザイン／バイデフォルトでシステムおよびデータベースにセキュリティを組み込んでいくアプローチ
    5. 「暗号化、 アクセス制御が不十分」─アセスメントで見えた日本企業の課題
       1. 1つ目の視点はデータの暗号化と伏字化、
       2. 2つ目は職務分掌、
       3. 3つ目はデータの漏えい検知と証跡管理
    6. 「個人情報の保護に関する法律」（2005年4月施行,2017年5月改正施行）
  1. 「企業における営業秘密管理に関する実態調査」報告書について【2017年3月17日IPA】

ドキュメントを参照: [ts\_kanri](https://www.ipa.go.jp/security/fy28/reports/ts_kanri/)

* + 1. 調査報告書（PDF：1.7MB）

ドキュメントを参照: [000057774.pdf](https://www.ipa.go.jp/files/000057774.pdf)

* + 1. 概要説明資料（PDF：1.42MB）

ドキュメントを参照: [000057775.pdf](https://www.ipa.go.jp/files/000057775.pdf)

* + 1. 調査報告書-資料編（アンケート調査結果）（PDF：1.75MB）

ドキュメントを参照: [000057776.pdf](https://www.ipa.go.jp/files/000057776.pdf)

* + 1. 調査報告書-資料編（判例調査結果）（PDF：867KB）

ドキュメントを参照: [000057777.pdf](https://www.ipa.go.jp/files/000057777.pdf)

* 1. 組織における内部不正防止ガイドライン（日本語版） 第4版ガイドライン【2017年1月31日IPA】

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

* + 1. 1.背景
    2. 2.概要
       1. 2-1.内部不正防止の基本原則
       2. 2-2.本ガイドラインの構成と活用方法
       3. 2-3.内部不正対策の体制構築の重要性
       4. 2-4.内部不正対策の体制
          1. 2-4-1.最高責任者
          2. 2-4-2.総括責任者
          3. 2-4-3.総括責任者の任命について
          4. 2-4-4.各部門／担当者の参画及び協力体制
    3. 3. 用語の定義と関連する法律
       1. 3-1.用語
       2. 3-2.関連する法律
    4. 4. 内部不正を防ぐための管理のあり方
       1. 4-1.基本方針（経営者の責任、 ガバナンス）
       2. 4-2.資産管理（秘密指定、 アクセス権指定、 アクセス管理等）
          1. 4-2-1.秘密指定
          2. 4-2-2.アクセス権指定
       3. 4-3.物理的管理
       4. 4-4.技術・運用管理
       5. 4-5.証拠確保
       6. 4-6.人的管理
       7. 4-7.コンプライアンス
       8. 4-8.職場環境
       9. 4-9.事後対策
       10. 4-10.組織の管理
    5. 付録Ⅰ：内部不正事例集
    6. 付録Ⅱ：内部不正チェックシート
    7. 付録Ⅲ：Q&A 集
    8. 付録Ⅳ：他ガイドライン等との関係
    9. 付録Ⅴ：基本方針の記述例
    10. 付録Ⅵ：内部不正防止の基本5原則と25分類
    11. 付録Ⅶ：対策の分類
  1.  【てびき】情報管理も企業力～秘密情報の保護と活用～【2016年12月5日METI】

ドキュメントを参照: [trade-secret.html](http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html)

* + 1. 秘密情報の保護ハンドブックの手引き
    2. １．こんなこと、 あるある!? 秘密情報にまつわるトラブル
       1. 大口の取引先から図面を見せてほしいと言われて提示したら・・・
       2. プロジェクトの開発リーダーだった従業員が退職を申し出てきたが、 転職先は競合他社で・・・
       3. 自社開発の技術にもかかわらず、 他社から「盗まれた!」と言われた。
       4. コラム：トラブルに巻き込まれないよう、 社内の秘密情報をうまく把握し、 活用させて企業力を高めていきましょう！
    3. ２．対策は身近なところから！企業を守るための漏えい対策３ステップ
       1. 保有する情報を洗い出します
       2. 秘密とする情報を決めましょう
       3. 情報に合わせた対策の選択と決定をしましょう
          1. 物理的・技術的な防御

１．秘密情報に近寄りにくくするための対策

接近の制御

２．秘密情報の持ち出しを困難に「するための対策

持出し困難化

* + - * 1. 心理的な抑止

３．漏えいが見つかりやすい環境づくりのための対策

視認性の確保

４．秘密情報だと思わなかった！という事態を招かないための対策

秘密情報に対する認識向上

* + - * 1. 働きやすい環境の整備

５．社員のやる気を高め、 秘密情報を持ち出そうという考えを起こさせないための対策

信頼関係の維持・向上等

* + 1. ３．実際にあった！？事例と対策とそのポイント
       1. 従業員向けの対策
       2. 従業員・退職者向けの対策
       3. 取引先向けの対策
       4. 外部者向けの対策
       5. 自社技術で商品をつくったのに、 他社の技術を使ったと言われた
       6. コラム：備えあれば憂いなし！自社の立場を守るためにできること
       7. コラム：他社の秘密情報を意図せず侵害しないために
       8. 転職者を受け入れて新製品を開発したら、 秘密情報の侵害だと訴えられた
    2. ４．万が一秘密情報が漏えいしてしまったら・・・
       1. 情報漏えいには兆候があります！
       2. 漏えいの疑いがあったらできるだけ早く適切な対応を取りましょう
       3. 被害回復のためにも日頃からの備えが大切です
       4. 情報漏えいしたら早めの相談を！
          1. 独立行政法人工業所有権情報・研修館（INPIT）

営業秘密・知財戦略ポータルサイト

ドキュメントを参照: [tradesecret](http://www.inpit.go.jp/katsuyo/tradesecret/)

相談窓口：03-3581-1101 ex.3844

全国47都道府県の知財総合支援窓口

ドキュメントを参照: [chizai-portal.jp](http://chizai-portal.jp/)

ナビダイヤル:0570-082100

* + - * 1. 情報処理推進機構(IPA)
        2. 全国都道府県警察　営業秘密侵害事犯窓口

警視庁生活経済課

* 1.  企業経営のためのサイバーセキュリティの考え方の策定について【2016年8月2日NISC】

ドキュメントを参照: [09shiryou07.pdf](http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf)

* + 1. http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf

ドキュメントを参照: [09shiryou07.pdf](http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf)

* + 1. サイバーセキュリティ戦略本部

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

* + - 1. http://www.nisc.go.jp/conference/cs/index.html

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

* + 1. 経営層に期待される 認識 や経営戦略を企画する人材層に向けた実装のためのツールを示す
    2. 基本方針
       1. ーサイバーセキュリティは、 より積極的な経営への「投資」へー
       2. サイバーセキュリティをやむを得ない「費用」でなく、 積極的な経営への「投資」と位置づけ、 企業としての「挑戦」と、 それに付随する「責任」として取り組むことが期待される
    3. I.基本的考え方
       1. 二つの基本的認識
          1. ＜①挑戦＞

新しい製品やサービスを創造するための戦略の一環として考えていく

Subtopic

* + - * 1. ＜②責任＞

サイバーセキュリティに取り組むことは社会的な要求・要請であり、 自社のみならず社会全体の発展にも寄与する

* + - 1. 三つの留意事項
         1. ＜①情報発信による社会的評価の向上＞

「セキュリティ品質」を高め、 品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。

そのような取組に係る姿勢や方針を情報発信することが重要。

* + - * 1. ＜②リスクの一項目としてのサイバーセキュリティ＞

提供する機能やサービスを全うする（機能保証）という観点から、 リスクの一項目としてのサイバーセキュリティの視点も踏まえ、 リスクを分析し、 総合的に判断。

経営層のリーダーシップが必要。

* + - * 1. ＜③サプライチェーン全体でのサイバーセキュリティの確保＞

サプライチェーンの一部の対策が不十分な場合でも、 自社の重要情報が流出するおそれあり。

一企業のみでの対策には限界があるため、 関係者間での情報共有活動への参加等が必要。

* + 1. II.企業の視点別の取組
       1. ITの利活用やサイバーセキュリティへの取組において、 各企業の事業規模のみならず、 その認識の違いなどを踏まえて取り組んでいく必要がある
       2. ITの利活用を事業戦略上に位置づけ、 サイバーセキュリティを強く意識し、 積極的に競争力強化に活用しようとしている企業
          1. （積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）
          2. 【経営者に期待される認識】

積極的なITの利活用を推進する中で、 製品やサービスの「セキュリティ品質」を一層高め、 自社のブランド価値の向上につなげるべく、 システムの基盤におけるセキュリティの向上、 情報・データの保護、 製品等の安全品質向上に取り組む。

様々な関係者との協働が重要であるため、 情報提供に主体的に取り組む。

決して現存する標準や取り組みなどに満足することなく、 実空間とサイバー空間の融合が高度に深化した明日の世界をリードし、 変革していく存在となることが期待される。

* + - * 1. 【実装に向けたツール】

IoTセキュリティに関するガイドライン（「IoTセキュリティのための一般的枠組」等）

自社のブランド価値としてのサイバーセキュリティに係る積極的な情報発信

* + - 1. IT・セキュリティをビジネスの基盤として捉えている企業
         1. （IT・サイバーセキュリティの重要性は理解しているものの、 積極的な事業戦略に組み込むところまでは位置づけていない企業）
         2. 【経営者に期待される認識】

経営者のリーダーシップによって、 社会的責任としてのサイバーセキュリティ対策に取り組む。

サプライチェーンやビジネスパートナー、 委託先を含めた対策を行う。

平時・緊急時のいずれにおいても、 情報開示などの適切なコミュニケーションを行う。

* + - * 1. 【実装に向けたツール】

サイバーセキュリティ経営ガイドライン

企業等がセキュリティ対策に取り組む上での保険等のリスク管理手法の活用

サイバーセキュリティを経営上の重要課題として取り組んでいることの情報発信

* + - 1.  自らセキュリティ対策を行う上で、 事業上のリソースの制約が大きい企業
         1. （主に中小企業等でセキュリティの専門組織を保持することが困難な企業）
         2. 【経営者に期待される認識】

サプライチェーンを通じて中小企業等の役割はますます重要となる中、 消費者や取引先との信頼関係醸成の観点から経営者自らサイバーセキュリティ対策に関心を持ち、 取り組む。

外部の能力や知見を活用しつつ、 効率的に進める方策を検討する。

* + - * 1. 【実装に向けたツール】

効率的なセキュリティ対策のためのサービスの利用（中小企業向けクラウドサービス等）

 サイバーセキュリティに関する相談窓口やセミナー、 地域の相談員等の活用

* 1.  企業（組織）における最低限の情報セキュリティ対策のしおり+1【2015年8月21日 2017年6月30日IPA】【第5版】

ドキュメントを参照: [01\_guidebook.pdf](https://www.ipa.go.jp/security/keihatsu/shiori/management/01_guidebook.pdf)

* + 1. 参照
       1. 中小企業の情報セキュリティ対策ガイドライン（第2版）【2016年11月15日IPA】

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

* + - 1. 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/

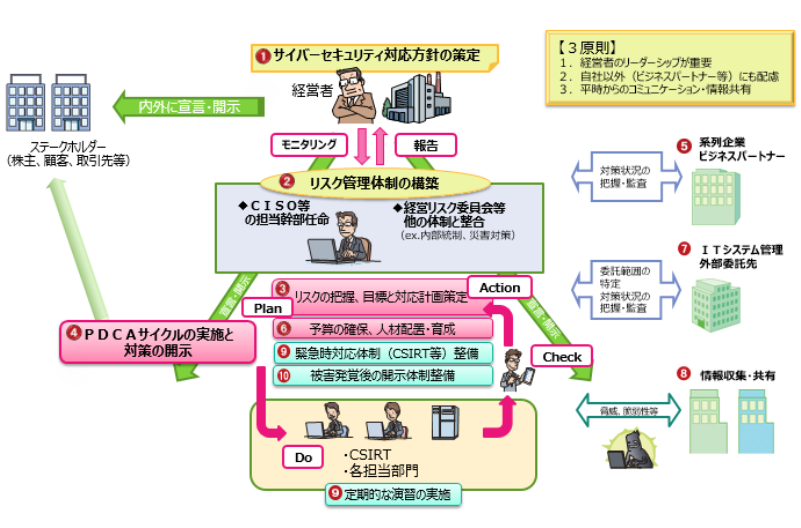
ドキュメントを参照: [guideline](https://www.ipa.go.jp/security/keihatsu/sme/guideline/)

* + - 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. 構成
       1. 5分でできる！情報セキュリティ自社診断（付録2）は、 25の設問に答えるだけで自社のセキュリティレベルを把握することができる自社診断シートと、 その解説パンフレットに加え、 情報セキュリティ対策を従業員に会社のルールとして周知する時に活用できる情報セキュリティハンドブックのな形で構成しています。
       2. 組織として最初に取り組むべき情報セキュリティ対策の自社診断シート　基本的対策、 従業員としての対策、 組織としての対策、 全25項目
    2. Part1 基本的対策
       1. №1 パソコン等の脆弱性対策
          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 パソコン等のウイルス対策
          1. 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 パソコン等のパスワード管理
          1. 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 重要情報へのアクセス(権)管理
          1. 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 脅威情報等の情報共有
          1. 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？
    3. Part2 従業員としての対策
       1. №6 標的型攻撃メール対策等
          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 電子メールの誤送信防止
          1. 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 電子メールでの重要情報漏えい対策
          1. 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のセキュリティ対策
          1. 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トラブル防止
          1. 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等の保全対策
          1. 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 重要情報の事務所等での管理
          1. 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 重要情報の持ち出し等の管理
          1. 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 パソコン等の第三者利用制限
          1. 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 事務所等への不正侵入対策
           1. 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 事務所等での重要機器の管理
           1. 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 事務所等での入退出管理
           1. 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 不要になった重要情報の廃棄管理
           1. 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？
    4.  　　Part3 組織としての対策【要確認】
       1. №19 守秘義務等の従業員への徹底
          1. 19.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？
       2. №20 従業員へのセキュリティ意識付け
          1. 20.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？
       3. №21 BYOD対応のセキュリティ対策
          1. 21.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？
       4. №22 取引先とのセキュリティ協議
          1. 22.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？
       5. №23 外部サービスのセキュリティ対策
          1. 23.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？
       6. №24 BCPを踏まえたセキュリティ事故対策
          1. 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 セキュリティルールの策定と運用
          1. 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？
    5. 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。
  1.  サイバーセキュリティ経営ガイドライン解説書Ver.1.0【2016年12月IPA】

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

* + 1. 0. はじめに
       1. 本解説書の想定読者
       2. 本解説書の構成
       3. サイバーセキュリティ経営の原則
       4. 経営者が決定すべき事項
       5. 経営者が責務を果たしているかどうかの問い
       6. 解説の記述方法
    2. 1．サイバーセキュリティ対応方針の策定
       1. セキュリティポリシーの策定
          1. セキュリティポリシーの主な検討項目
       2. セキュリティポリシーの周知
          1. 組織内への周知の重要性
          2. 組織外への公開の重要性
          3. セキュリティポリシー群の種類
          4. セキュリティポリシーの公開
          5. 企業例示について
          6. 企業例示「セキュリティポリシーの策定」
    3. 2．リスク管理体制の構築
       1. サイバーセキュリティリスク管理体制
          1. サイバーセキュリティリスク管理体制の構築方法
          2. サイバーセキュリティリスク管理体制の構築の必要性と経営者の責任
       2. CISO 等に求められること
          1. CISO 等の役割
       3. 既存のリスク管理体制との関係
          1. 既存の管理体制との整合
          2. 既存のリスク管理体制との関係性の明確化
          3. 企業例示「管理体制の構築検討」
    4. 3．リスクの把握、 目標と対応計画策定
       1. 資産の特定
          1. 守るべき資産の特定
          2. 法令等による要求事項の明確化
          3. 情報のライフサイクルに着目した資産のリスト化
          4. ネットワーク上の守るべき資産の特定
       2. サイバー攻撃の脅威を識別
       3. リスクの把握
          1. 適切なリスク分析の重要性
          2. リスク分析手法の種類について
          3. 事業継続を踏まえたビジネスインパクト分析
       4. リスク対応計画の策定
          1. リスク対応方法の検討
          2. リスクに応じた対策の目標と対応計画の策定
          3. 企業例示「リスク対応の検討」
    5. 4．PDCAサイクルの実施と対策の開示
       1. 環境変化に応じたフレームワーク（PDCA）の構築
          1. フレームワーク（PDCA）の構築
          2. フレームワーク（PDCA）のサイクル
          3. 計画見直し方法の検討
       2. 対策状況の把握
          1. 対策状況の把握方法
          2. 経営者への報告内容
          3. KPI の設定・モニタリング
          4. 経営層による評価
          5. 内部監査と外部監査
       3. 対策状況の開示
          1. 企業例示「PDCA の検討」
    6. 5．系列企業・ビジネスパートナーの対策実施及び状況把握
       1. 系列企業・ビジネスパートナーを含めた対策の実施
          1. ビジネスパートナー等との対策実施・連携の検討
       2. ビジネスパートナーの対策状況の把握
          1. ビジネスパートナーの対策状況を把握する方法
          2. より効果的に対策状況を確認する方法
          3. 企業例示「関係者の対応状況把握
    7. 6．予算確保・人材配置及び育成
       1. 必要な対策費用の確保
          1. 対策費用の承認を得るためのポイント
          2. 経営者が判断できる材料とは
       2. 必要な人材の確保・育成
          1. 必要な人材と育成
          2. セキュリティ担当者の育成
          3. 一般従業員の研修
          4. 積極的な外部リソースの活用
          5. 企業例示「資源の確保」
    8. 7．ITシステム管理の外部委託
       1. 自組織による対応と外部委託による対応
          1. 外部委託する範囲を選択するポイント
       2. 委託先のサイバーセキュリティの確保
          1. 委託先への依頼方法
          2. 連携体制の整備・構築
          3. 外部委託先としてクラウドサービス事業者を選定する際のポイント
          4. 企業例示「IT システム管理の外部委託先への対応」
    9. 8．情報収集と情報共有
       1. 情報収集と自社での有効活用
          1. 情報収集の重要性
          2. 情報を常に最新の状態に保つ
          3. 収集した情報を活用するための環境整備
       2. 情報共有・情報提供
          1. 情報共有・提供の重要性
          2. 社会全体での対策向上
          3. 企業例示「情報収集及び情報共有の検討」
    10. 9．緊急時対応体制の整備と演習の実施
        1. CSIRT の構築
           1. CSIRT の構築方法
           2. CSIRT の設計で検討すべき事項
           3. 危機管理に求められる機能
        2. 緊急連絡先・初動対応マニュアルの整備
           1. 緊急時の初動対応フローの整備（マニュアルの策定）
           2. 報告体制・エスカレーション基準
           3. 社外を含めた緊急連絡先
           4. 初動対応事項・復旧事項
           5. 事後対応事項
        3. 定期的・実践的な演習の実施
           1. 初動対応マニュアルの有効性の検証
           2. 社内組織（部門）間のコミュニケーション、 共同作業の有効性の検証
           3. CSIRT 要員のスキル・量の十分性の確認
           4. セキュリティ技術対策の効率性・十分性の確認
           5. 訓練・演習の考え方
           6. 定期的な訓練実施
           7. 企業例示「緊急時の対策検討」
    11. 10．被害発覚後の必要な情報の把握、 開示体制の整備
        1. 被害発覚後の情報収集体制および開示すべき項目の整備
           1. 開示・報告すべき情報の把握
           2. 通知先のリスト化と通知用のフォーマット作成
           3. 通知に必要な情報の整理と周知
           4. 組織の内外への開示・報告内容、 タイミング
           5. 開示・報告先について留意すべき点
        2. 組織内外へ経営者が説明できる体制の整備
           1. 経営者への報告ルートや報告ルールの整備
           2. 企業例示「被害発覚時の準備」
    12. 付録1：ガイドラインの3原則と重要10項目の概要図
    13. 付録2：参照情報
    14. 付録3：サイバーセキュリティ経営チェックシートの実施の目安と確認事項
    15. 別添 ：サイバーセキュリティ対策に関連する被害事例
    16. ＜付録1ガイドラインの3原則と重要10項目の概要図＞
        1. Subtopic  
           
  1. サイバーセキュリティ経営ガイドライン解説書Ver.1.0別添：被害事例集【2016年12月IPA】

ドキュメントを参照: [000056149.xlsx](https://www.ipa.go.jp/files/000056149.xlsx)

* 1.  企業経営のためのサイバーセキュリティの考え方の策定について【2016年8月2日NISC】
  2. 情報セキュリティポリシーサンプル改版（1.0版）【2016年3月29日JNSA】

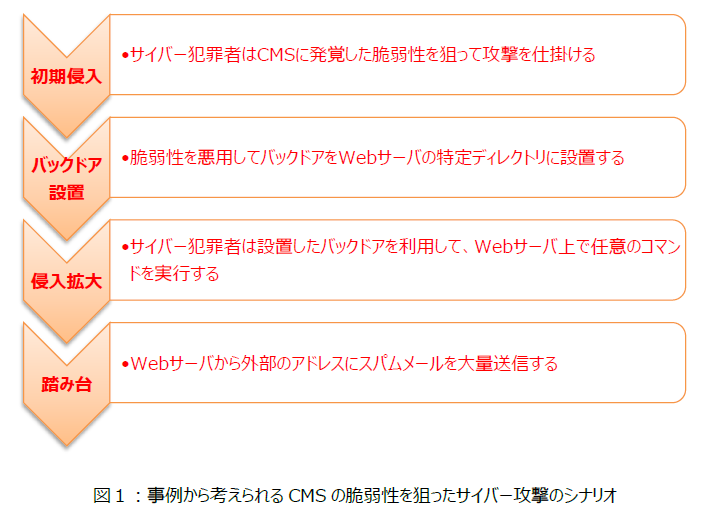
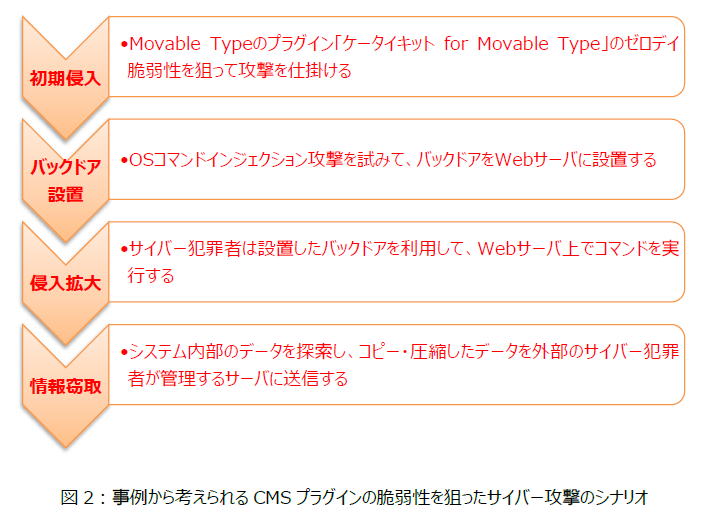
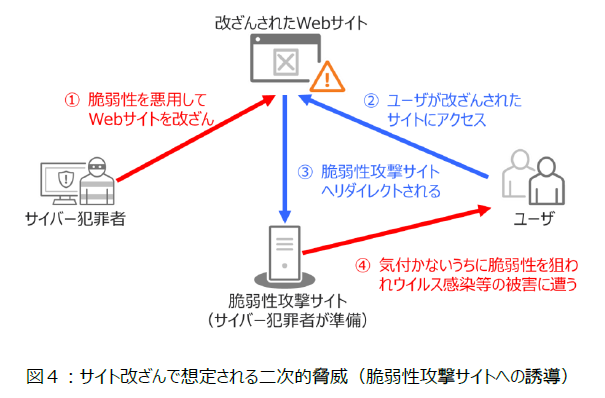
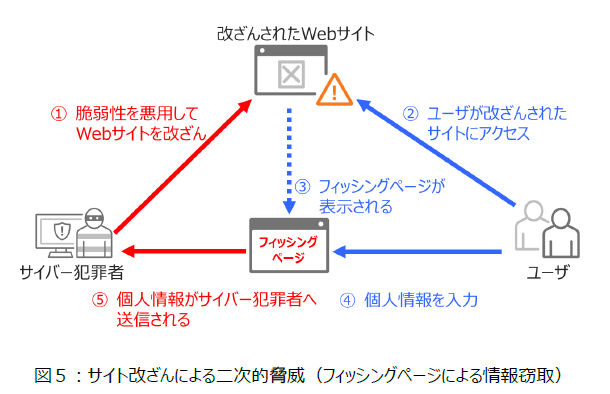
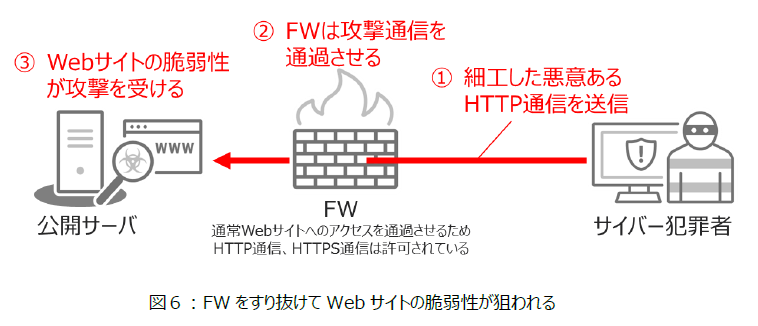
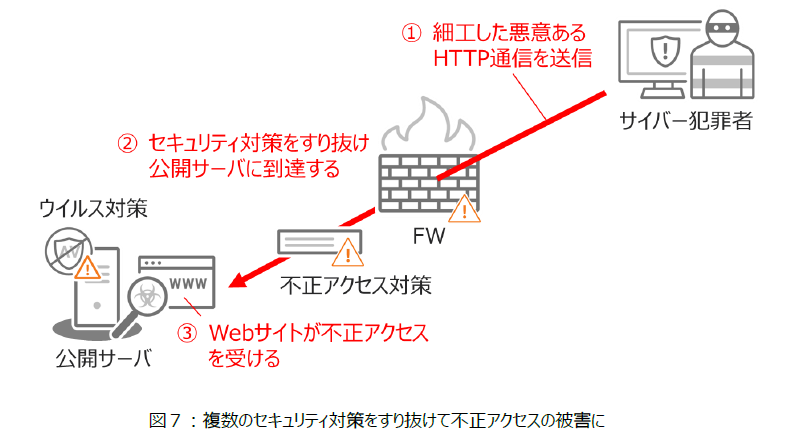
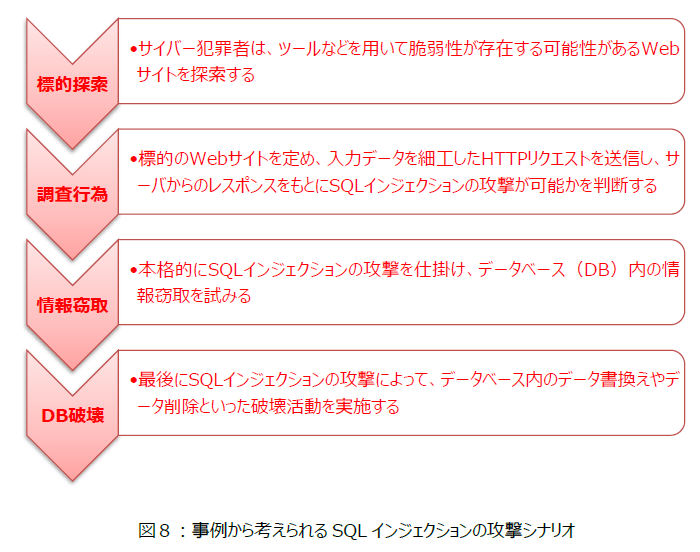
ドキュメントを参照: [policy](http://www.jnsa.org/result/2016/policy/)

* 1. すぐ役立つ！法人で行うべきインシデント初動対応 ~「不審な通信」その時どうする~【2016年11月1日トレンドマイクロ】

ドキュメントを参照: [20161031014833.html](http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20161031014833.html)

* + 1. 1 はじめに インシデント対応の実情
    2. 2 「インシデント発生」を把握し対応開始を判断する
       1. 2.1 インシデントの発生に気づくために
       2. 2.2 インシデント対応を判断するために
       3. 2.3 まとめ インシデントの把握と対応判断のポイント
    3. 3 「不審な通信」、 その時に行うべきインシデント対応
       1. 3.1 インシデント対応の考え方
       2. 3.2 「影響範囲の確認」のために必要な対応
       3. 3.3 「脅威の封じ込め/根絶」のために必要な対応
       4. 3.4 被疑端末への対応
       5. 3.5 まとめ 具体的なインシデント対応のポイント
    4. 4 「適切な対応」を迅速に行うために
       1. 4.1 インシデント発生を把握し対応開始を判断するための事前準備
       2. 4.2 インシデント対応を適切かつ迅速に行うための事前準備
    5. 5 まとめ
  1. 2016 年インシデント事例から学ぶ「Web サイトのセキュリティ対策」【トレンドマイクロ】

ドキュメントを参照: [select.asp](https://app.trendmicro.co.jp/doc_dl/select.asp?type=1&cid=233)

* + 1. はじめに . 3
    2. 攻撃パターン①：コンテンツ管理システムまたはそのプラグインの脆弱性が狙われた . 3
       1. 事例①：地域情報サイトが攻撃を受け、 約60 万件のスパムメールを送信 3
          1. Subtopic  
             
       2. 事例②：大手放送局等がCMS プラグインの脆弱性を狙われ、 大量の個人情報が漏えい . 4
          1. Subtopic  
             
       3. インシデント事例から学ぶべきポイント 5
    3. 攻撃パターン②：不正サイトに誘導するコードやフィッシングページが設置された 6
       1. 事例①：サイトの一部が改ざん、 ユーザを不正サイトへ誘導 6
          1. Subtopic  
             
       2. 事例②：不正アクセスを受け、 自社のWeb サイトがフィッシングページを表示 . 7
          1. Subtopic  
             
       3. インシデント事例から学ぶべきポイント 8
    4. 攻撃パターン③：ベーシックな対策だけのサイトへの攻撃 9
       1. 事例①：ファイアウォール導入や脆弱性診断を実施していた企業が、 Web サイトからの情報漏えい被害に 9
          1. Subtopic  
             
       2. 事例②：不正アクセス対策をすり抜ける攻撃により顧客情報の一部が漏えい . 10
          1. Subtopic  
             
       3. インシデント事例から学ぶべきポイント 10
    5. 攻撃パターン④：Web アプリケーションの脆弱性を狙ったインジェクション攻撃 . 11
       1. 事例①：SQL インジェクションの攻撃によって、 個人情報の一部が漏えい . 11
          1. Subtopic  
             
       2. 事例②：Web アプリケーションの脆弱性を悪用したバックドアの設置 . 12
          1. Subtopic  
             
       3. インシデント事例から学ぶべきポイント 13
    6. 2016 年インシデント事例から学ぶべきポイントとサーバ対策 . 14
    7. トレンドマイクロ製品による総合サーバセキュリティ対策 15
  1. スマートフォン等の業務利用における情報セキュリティ対策の実施手順策定手引書【2015年 5月21日NISC】

ドキュメントを参照: [02shiryou0305.pdf](http://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0305.pdf)

* + 1. 1．総則
       1. 1.1 本書の目的・位置付け
       2. 1.2 本書が対象とする者
       3. 1.3 本書の使い方
       4. 1.4 用語の定義
    2. 2．スマートフォン等の特性と業務利用におけるリスク
       1. 2.1 スマートフォン等の特性
       2. 2.2 スマートフォン等の特性及び業務利用における脅威
          1. 表２－１ スマートフォン等の業務利用における脅威と対策の例
    3. 3．スマートフォン等の業務利用の形態
       1. 3.1 端末の配備
       2. 3.2 利用する場所
       3. 3.3 私物端末の利用
       4. 3.4 情報システムの利用形態
    4. 4．目的及び適用範囲の明確化
       1. 4.1 目的の明確化
       2. 4.2 対象とする業務
       3. 4.3 利用者
    5. 5．業務・サービスの利用要件の策定
       1. 5.1 端末やOSの種類
       2. 5.2 端末機能・サービスの要件
          1. 表５－１ 端末機能・サービスの利用要件及び利用制限の例
       3. 5.3 業務用アプリの導入
       4. 5.4 通信ネットワークの要件
       5. 5.5 情報セキュリティ対策要件
          1. (1) ソフトウェアの脆弱性対策
          2. (2) 不正プログラム対策
          3. (3) のぞき見防止対策
          4. (4) 盗難・紛失対策
          5. (5) ログ管理機能
          6. (6) 端末管理ツール（MDM：Mobile Device Management）の導入
          7. 表５－２ MDMの主な機能

端末ロックの遠隔制御

端末個体ごとに、 遠隔制御でロック、 アンロックを実施

リモートデータワイプ

端末内全データ削除、 個別データ/特定フォルダ削除、 業務領域のみ削除 等

暗号化

外部メモリ出力時のデータ暗号化/復号、 個別データの暗号化/復号

端末機能制御

カメラ、 スクリーンショット、 近距離無線通信、 外部メモリ出力等の機能制限

端末状態監視

端末状態の取得（OS、 アプリ、 改造の有無、 起動中アプリ 等）

死活監視、 ログ収集、 位置情報取得、 アラートメールの送信、 管理者向け統計処理

ポリシー設定及び実行

パスワードポリシー設定、 MDMポリシー（リモートデータワイプの条件、 機能制限 等）設定

メーラーや無線LAN接続、 証明書等の端末構成の設定変更 等

資産管理

端末所有者の属性管理や端末個体情報(機種、 電話番号 等）の管理 等

アプリ配信及び削除

業務用アプリの配信と自動インストール、 遠隔削除

アプリ利用制限

非公認アプリのインストール制限や強制終了、 アプリのアクセス許可制御

外部媒体経由のアプリインストール制御 等

MDMサーバ接続

SSL・VPNによる通信路暗号化、 GCM等によるエージェント・MDMサーバ間通信路の維持 等

フィルタリング機能

ウェブフィルタ、 メールフィルタ等の設定情報管理やアクセスログの収集

不正プログラム対策ソフトウェアの管理

不正プログラム対策ソフトウェアのバージョンやパターンファイルの管理、 最新版への更新、 スキャンログの収集、 スキャン実行の要求 等

バックアップ

端末データのバックアップやリスア

* + - 1. 5.6 私物端末の業務利用に際して留意すべき事項
         1. 表５－３ 私物端末の業務利用する際に留意すべき事項と要件策定例

業務情報と私的な情報の混在の回避

 端末内の私的な情報と業務情報を混在させないよう、 これらを明確に分けるための仕組みを導入する

 業務用アプリ導入又は端末に業務情報を保存させない仕組みを導入する

家族や友人への貸与の禁止

 私的な利用においても家族や友人が利用することを禁止することを合意した者のみに私物端末の利用を認める

外出先等での端末の盗難・紛失

 業務利用する際の利用場所を限定する

 私的利用時を含めて端末ロックやデータワイプ機能の設定を必須し、 対策の実施について合意した者のみに私物端末の利用を認める

利用するネットワークの制限

 私的な利用時であっても安全性の確認できないサイトや通信ネットワークへの接続を禁止するなどの利用手順を策定し、 合意した者のみに私物端末の利用を認める

ソフトウェア更新や不正プログラム対策の実施

 ソフトウェア更新や不正プログラム対策ソフトウェアの実行を義務付け、 合意したのみに私物端末の利用を認める（OSの更新により業務用アプリが正常動作しなくなる可能性について留意が必要）

業務用アプリのインストール

 業務用アプリのインストール可能な端末を所有していて、 かつインストールに合意した者のみに私物端末の利用を認める

点検内容の明確化

 業務用アプリ、 MDMやMAMにより点検を自動化する

 あらかじめ点検内容を明確化し、 合意した者のみに私物端末の利用を認める

* + 1. 6．実施手順の整備
       1. 6.1 責任者の設置と運用管理体制の整備
       2. 6.2 利用手順の整備
          1. 表６－１ 利用者が遵守すべき端末の利用手順に関する注意事項の例

利用の原則

行政事務の遂行以外の目的で端末を利用しないこと

不要不急な業務においては極力利用しないこと

不要な情報は端末に残留させず、 速やかに消去すること

他の手段が無い場合に限り利用すること

利用手順の遵守

利用手順を遵守すること

定められた手順以外の方法で業務を行わないこと

手順外の処理を行う必要が生じた場合は、 事前に責任者の許可又は承認を得ること

利用を終了した場合は、 速やかに手続すること

利用中にインシデント等が発生した場合は、 手順に従って管理者等へ速やかに連絡し、 必要な措置を講ずること

端末管理の徹底

盗難・紛失が起こらないように、 日常的に端末の管理を厳重に行うこと

家族や知人、 第三者が端末操作や画面をのぞき見する行為に注意すること

禁止事項

管理責任者の許可なく、 端末の設定を変更しないこと

安全性が確認できないアプリケーションや利用が禁止されているソフトウェアをインストールしないこと

許可された通信回線以外に接続しないこと

PCに接続しないこと（充電等の場合であってもNG）

端末は家族や知人、 第三者に端末を貸与しないこと

* + - 1. 6.3 運用管理手順の整備
  1. なりすましECサイト対策マニュアル【2015年3月一般社団法人セーファーインターネット協会】

ドキュメントを参照: [narisumashi\_manual.pdf](https://www.saferinternet.or.jp/system/wp-content/uploads/narisumashi_manual.pdf)

* + 1. 1. はじめに
       1. EC サイト運営者の方向け
    2. 2. なりすましEC サイトとは
       1. 実在するサイトの外観（屋号、 商標、 サイト意匠・構成、 使用している画像等）を模倣することにより、 あたかも当該サイトである又は当該サイトと関係のあるサイトであるかのように消費者を誤認させ、 商品代金をだましとったり、 模倣品、 海賊版その他購入しようとした品と全く別個の物を送りつけるサイト
    3. 3. なりすましEC サイトの特徴
       1. 日本語が不自然
       2. 振込先が個人名（外国人の場合が多い）
       3. 支払い方法が銀行振込のみとなっている
       4. 問い合せ先のメールアドレスがフリーメールアドレス
       5. 「特定商取引に関する表示」が曖昧（店舗名・住所・電話番号・メール の表示が欠けている）
       6. 価格が極端に安い
       7. フォームの崩れやリンク切れなど、 Web サイトの作り方に粗雑な点が見られる
       8. 有名ブランド名＋激安 などの表示がある
    4. 4. 被害実態（アンケート結果）
       1. 4.1. 被害実態
       2. 4.2. 対策状況
    5. 5. 当事者たちの責任関係
    6. 6. 対処法、 予防法
       1. 6.1. 対処法
          1. 6.1.1. 問い合わせ対応

問い合わせ対応文－なりすましEC サイト対策協議会

ドキュメントを参照: [template002.docx](http://www.saferinternet.or.jp/system/wp-content/uploads/template002.docx)

* + - * 1. 6.1.2. 削除要請

削除依頼文－なりすましEC サイト対策協議会

ドキュメントを参照: [template003.docx](http://www.saferinternet.or.jp/system/wp-content/uploads/template003.docx)

* + - * 1. 6.1.3. 都道府県警察サイバー犯罪相談窓口への連絡

都道府県警察本部のサイバー犯罪相談窓口等一覧

ドキュメントを参照: [soudan.htm](http://www.npa.go.jp/cyber/soudan.htm)

* + - 1. 6.2. 予防法
         1. 6.2.1. 注意喚起

サイト掲示用注意喚起文－なりすましEC サイト対策協議会

ドキュメントを参照: [template001.docx](http://www.saferinternet.or.jp/system/wp-content/uploads/template001.docx)

* + - * 1. 6.2.2. 被害に遭っているかの確認

自身が運営するEC サイトの店舗名を検索サイトで検索し、 自身が運営する以外のドメインでEC サイトが存在するかをチェックする

自身が運営するEC サイトの店舗名やサービス名等を検索サイトのアラートサービスに登録し、 自身が運営する以外のドメインでEC サイトが存在するかをチェックする

自身が運営するEC サイトで掲載している画像を検索サイトで画像検索し、 同じ画像を掲載しているEC サイトが存在するかをチェックする

自身が運営するEC サイトに掲載している文章を検索サイトで検索し、 文章を盗用したEC サイトが存在するかをチェックする

* + - * 1. 6.2.3. 商標権の取得等
        2. 6.2.4. 電子証明書（SSL サーバ証明書）

シマンテック 技術者でなくても分かる 電子証明書とPKI 入門

ドキュメントを参照: [page.jsp](http://www.symantec.com/ja/jp/page.jsp?id=pki-basics)

GMO グローバルサインSSL とは？

ドキュメントを参照: [knowledge](https://jp.globalsign.com/service/ssl/knowledge/)

* + - * 1. 6.2.5. ウェブサイトや運営者情報の登録

公益社団法人日本通信販売協会 オンラインマーク制度

ドキュメントを参照: [ost](http://www.jadma.org/ost/)

株式会社TradeSafe TradeSafe トラストマーク

ドキュメントを参照: [www.tradesafe.co.jp](http://www.tradesafe.co.jp/)

JIPDEC(一般財団法人日本情報経済社会推進協会) ROBINS シール

ドキュメントを参照: [robinsseal](http://robins-cbr.jipdec.or.jp/usecase/robinsseal/)

* + - * 1. 6.2.6. その他

シマンテック セキュアメール ID

ドキュメントを参照: [secure-mail-id](http://www.symantec.com/ja/jp/secure-mail-id/)

GMO グローバルサイン S/MIME とは

ドキュメントを参照: [smime](https://jp.globalsign.com/service/clientcert/knowledge/smime/)

JIPDEC(一般財団法人日本情報経済社会推進協会) S/MIME とは

ドキュメントを参照: [smime](http://jcan.jipdec.or.jp/smime/)

dkim.jp dkim とは

ドキュメントを参照: [about-dkim](http://www.dkim.jp/dkim-jp/about-dkim/)

JIPDEC(一般財団法人日本情報経済社会推進協会) 安心マーク

ドキュメントを参照: [anshinmark](http://robins-cbr.jipdec.or.jp/usecase/anshinmark/)

* + 1. 7. おわりに
    2. 8. 関係関連団体・政府機関紹介
  1. Sec01-02-10 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

ドキュメントを参照: [Sec01-02-10](https://bluemoon55.github.io/Sharing_Knowledge/Cyber_Security/Deliverables/mind2html/Sec01-02-10)

* + 1. 改版履歴
       1. 2018年12月25日　独立文書化
       2. 【2018年5月IPA】
    2. はじめに （Executive Summary
    3. 対象読者と活用範囲
       1. ウェブサイトの運営者を主な対象読者としている。 ウェブサイトの運営にあたっては、 経営者、 企画者、 開発者、 運用管理者等がそれぞれの立場で関与することになる。
       2. 自組織でウェブサイトを構築する際に組織の内情や実施可能なセキュリティ対策、 セキュリティインシデント発生時の対応可能範囲等をもとに運営形態を選定する他、 ウェブサイトの構築を外部委託するケースでは、 運営形態に応じて必要となるセキュリティ対策項目の選定と発注要件の決定に活用して頂くことも想定している。
    4. ウェブサイト運営のライフサイクル
       1. 1.企画
       2. 2.設計
       3. 3.実装/構築
       4. 4.テスト
       5. 5.運用/利用
       6. 6.廃棄
    5. ウェブサイト運営形態の選定の重要性
    6. 各章節の想定読者
       1. 経営者：ウェブサイトの運営方針や、 組織としてのセキュリティの全体的な方針を決定する者を指す。
       2. ウェブサイト企画者：ウェブサイトで提供するコンテンツや、 サービス,具体的なセキュリティ方針を企画・決定する立場の者を指す。
       3. ウェブサイト開発者：ウェブサーバの構築や、 ウェブアプリケーションの開発、 方針に従ったセキュリティ対策の実装に携わる者を指す。
       4. ウェブサイト管理者：構築されたウェブサイトを保守・運用管理する立場の者を指す。
    7. 1. ウェブサイトの運営形態について
       1. 表1-1 運営形態の分類と説明
          1. モール
          2. ASP SaaS 型クラウドサービス
          3. PaaS 型クラウドサービス レンタルサーバ
          4. IaaS 型クラウドサービス
          5. ハウジング
          6. オンプレミス
       2. 1.1. 様々な運営形態が登場した背景
       3. 1.2. 各運営形態の特徴
          1. 運営形態を検討、 選定する上で、 選定を判断する観点や指標

①機能：計画しているウェブサイトの機能を満たせるか、 機能の自由度はどれだけあるか

②期間：開設までに要する期間（工数）、 サービスインの計画との整合性

③調達：運営するために調達が必要となる物理環境、 機材、 ソフトウェア等

④体制：開設、 運営していくのに必要となる人的資源、 体制

⑤費用：開設での一次費用、 運用における経年費用、 トータル費用等

⑥セキュリティ：安全な運用を維持するために対応すべきセキュリティ対策

* + - * 1. 表1-2-1 運営形態毎の選定項目の比較

①ウェブサイトの機能の自由度

②ウェブサイト開設までの日数

③ウェブサイト開設のため調達が必要な物品数

④ウェブサイト開設・運営に必要な人的資源

⑤-1ウェブサイト開設に必要な費用

⑤-2ウェブサイトの維持・運営に必要な費用

⑥検討が必要なセキュリティ対策項目

* + - * 1. 1.2.1 モール、 ASP、 SaaS 型クラウドサービスの特徴

表1-2-2 モール、 ASP、 SaaS でのメリットとデメリット

* + - * 1. 1.2.2 PaaS 型クラウドサービス、 レンタルサーバ、 IaaS 型クラウドサービスの特徴

表1-2-3 PaaS、 レンタルサーバ、 IaaS でのメリットとデメリット

* + - * 1. 1.2.3 ハウジング、 オンプレミスの特徴

表1-2-4 ハウジング、 オンプレミスでのメリットとデメリット

* + - * 1. 1.2.4 業種による利用傾向

ウェブサイトで公開されている各運営形態の情報27を参照すると、

ASP やモールの運営形態を選ぶ場合は、

ウェブサイト運営サービスに付加される別のサービスを利用できることが選定の理由として挙げられていた。 サーバの構築や運営の技術を持たない個人商店や中小企業等の利用が多くみられ、 そういった企業がEC サイトを出店する際に、 サポートサービスのEC サイト経営の相談サービス等が提供されていることを選定の基準にしているとのコメントが見られた。

レンタルサーバやクラウドの場合は、

ASP やモールと異なり独自のドメインを取得するサービスが提供されており、 企業紹介のウェブサイトを導入する際に利用されているようである。 選定の理由として挙げられているのは導入するサービスや使用するソフトウェアを自由に選択できる点である28。 機材管理の工数が必要ないこと、 サービスの提供開始までに要する時間が短いこと、 特にクラウドの場合は処理性能等のスケーラビリティが確保されていることがある。

* + 1. 2. 各運営形態の選定に向けたアプローチ
       1. 2.1. 運営形態の選定のアプローチについて
          1. 図2-1-1 実現したい目的を優先した観点における選定フロー
          2. 図2-1-2 運用・維持を優先した観点における選定フロー

判断基準

1.システム構築体制

2.アプリ開発体制

3.運用保守体制

4.セキュリティ対策維持管理体制

* + - 1. 2.2. 運営形態毎の自由度
         1. 図 2-2-1 ASP やレンタルサーバでのウェブサイト運営
         2. 図 2-2-2 オンプレミスのウェブサイト運営
      2. 2.3. 運営形態毎に調達が必要となる機材
         1. 表 2-3-1 運営形態毎に調達が必要な機材
         2. サーバ室
         3. 電源管理
         4. ネットワーク回線
         5. サーバ、 OS
         6. ミドルウェア
         7. ウェブアプリケーション
         8. コンテンツ
      3. 2.4. 運営形態毎に発生する費用項目
         1. 表2-4-1 運営形態毎に必要となる費用
         2. サーバ室の整備費用
         3. ネットワーク回線の敷設費用
         4. ネットワーク機器の購入費用
         5. サーバの購入費用
         6. ウェブアプリケーションの開発費用・購入費用
         7. ウェブサーバの構築費用
         8. ウェブサイトの運用管理費用
         9. サービス利用費用、 課金
      4. 2.5. 運営形態毎の責任範囲
         1. 表2-5-1 運営形態毎の責任範囲
         2. サービスの停止
         3. データの破壊・消去
         4. 情報漏洩
         5. 改ざん
      5. 【コラム】 「契約の免責事項
         1. メンテナンスまたは不慮の事故等により、 サービス停止等によるサービス利用者の逸失利益や損害について、 提供者は一切の責任を負わないものとする
         2. 不測の事故等により、 サービス利用者のサーバ上に蓄積されているデータが喪失、 流失、 損壊等が発生した場合、 提供者は一切の責任を負わないものとする
      6. 2.6. 各運営形態で検討が必要なセキュリティ対策
         1. 表2-6-1 運営形態毎に検討すべきセキュリティ対策
         2. セキュリティ対策項目

システムセキュリティ対策

技術的対策

物理

・サーバ室

・入退管理

ネットワーク

・FW　・IDS/IPS

・WAF ・VPN

・ウイルス対策製品

・サンドボックス型製品

・DDoS対策

アプリケーション

・改ざん検知

・認証　・アクセス制御

・データ保護

運用管理的対策

セキュリティパッチ

・パッチ適用

・仮想パッチ適用

監視

・ログ収集、 分析

インシデント対応

・バックアップ

・切り分け　　・抜線

人的対策

要員教育

・ポリシー教育

・技術教育

業務セキュリティ対策

社員教育

・リテラシー教育

ユーザ・顧客管理

・ポリシー教育

・情報取扱い規則

コンテンツ管理

・コンテンツ更新ルール

* + - 1. 【コラム】 「既知の脆弱性が存在するウェブサイトに関する届出」
    1. 3. セキュリティ対策要件および強化のポイント
       1. 各セキュリティ対策が、 どのような要件を満たすべきか、 どの程度の強度レベルを必要とするか、 等については、 構築するウェブサイトにおいて実現する機能やサービスや事業モデルによって、 大きく異なってくる。
       2. 3.1. 実現する機能、 サービスに対する考慮のポイント
          1. 3.1.1 企業等の組織が公開するウェブサイトでのポイント

改ざんされることで、 サイト利用者が不利益を被る場合が考えられる。 また、 偽の情報を掲載されてしまったことで、 サイト運営者の信用失墜が発生する。

ウェブサイト改ざんの被害は、 運営組織の大小や掲載されている情報の内容によらず、 事業継続の大きな障害となりうる。 このことから、 「我社のウェブサイトには漏洩して問題がある情報はない」というケースにおいても、 簡単に安心することはできない。

改ざん被害にあわないためには、 ウェブサイトで使用しているソフトウェアを常に最新の状態に保つことが、 第一の対策となる。

モールやASP の運営形態

ソフトウェアのアップデートはサービス提供者が実施する対策

サービス提供者を選定する段階で、 外部機関によるペネトレーションテストを定期的に実施していたり、 ウェブサイト改ざん検知の機能を提供していたりするサービス提供者を選択することが重要

例えば、 「外部の●●社の脆弱性診断を毎年実施し、 脆弱性が検出されないことを確認している」といった、 明確な対策状況の回答が得られることが望ましい。

* + - * 1. 3.1.2 EC サイトでのポイント

EC サイト等では決済機能を提供するため、 ウェブサイト上でクレジットカード情報や、 口座情報等の取り扱いが必要である。 万が一、 EC サイトで不正アクセスや情報漏洩等が発生した場合、 サイト利用者のみならず、 関係している組織に対しても、 重大な被害が発生する。

ASP やモール、 SaaS 型クラウドサービスを利用して運営する場合

決済機能を含む様々なプログラムはサービス提供者によって実装されるものである。 そのため、 サイト運営者による攻撃を検知するためのプログラムの実装や、 脆弱性の修正等の管理をすることができない

サービス提供者を選択する時点で、 外部からの攻撃を検知・遮断するための監視システムを導入しているか、 業界団体や政府機関が定めるセキュリティ基準に準拠した対策を行っているかについて調査する必要がある。

日本国内のサービス提供者であればPCI DSSへの準拠について確認が必須である38

PCI DSS は、 国際クレジットカード国際カードブランド5 社が共同で設立したPCI SecurityStandards Council によって運用、 管理されている基準であり、 日本国内ではクレジットカード情報を自社内で取り扱う企業に対して、 2018 年3 月までにPCI DSS へ準拠することが義務となっている。

レンタルサーバやPaaS・IaaS 型のクラウドサービス、 ハウジング、 オンプレミスの運営形態の場合

決済機能はサイト運営者が何らかの形で導入する必要がある。 たとえば、 自組織で決済機能を開発する方法や、 クレジットカード会社が提供するサービスを利用するといった方法が考えられる。

ウェブサイトに独自に決済機能を開発する場合、 自組織内で機微な情報を取り扱う必要が発生する。

これによりPCI DSS 準拠へのセキュリティ対策・維持の負荷が増大するため、 外部の決済代行会社に決済機能を委託することで、 サイト運営者の負担を軽減することも一考である。

サイト運営者は悪意ある第三者がサイト利用者になりすまして商品の購入や、 他者の決 済情報を盗み取ることができないようにすることも必要である。

正規の利用者になりすまして情報を盗み取る場合、 正規のサイト利用者と攻撃者を識別することが困難である。

なりすましの被害を受ける原因

1. 簡単で短いパスワードを設定していた

2. 個人情報から類推しやすいパスワードを設定していた

3. 他のウェブサービスで同じパスワードを設定していた

なりすましを防ぐためには、 3.2 節で説明するサイト運営者側の対策だけでなく、 サイト利用者に対して簡単なパスワードの禁止やパスワードの使いまわしをしないこと等の啓発が必要である。

* + - * 1. 3.1.3 SNS サイトや掲示板サイト等でのポイント

悪意ある書き込みや改ざんには十分留意する必要がある。

例えば、 クロスサイト・スクリプティングの脆弱性の場合

攻撃者がスクリプトを含む内容を投稿することで偽の情報を表示されてしまう。 このような被害を防ぐために、 投稿される内容にスクリプトが含まれていれば、 ウェブサイト上にそのまま出力しないよう特定の記号はエンコードして表示する必要がある。

クロスサイト・リクエスト・フォージェリの脆弱性がある場合

サイト利用者が意図しない操作を実行させられてしまう可能性が存在し、 結果的に登録情報の書き換えや、 意図しない内容を投稿させられてしまうといった被害につながる。

これを防ぐために、 登録情報の変更等の重要な処理の際にはパスワードの再入力を求めることや、 外部のウェブサイトから転送された通信であるか調査する機能を実装する等の対策が必要である。

この他の攻撃

他者のセッションを乗っ取り、 他人になりすまして記事を投稿する等がある。 その対策としては、 攻撃者によるセッションID の推測や、 被害者に任意のセッションID を使用させない（セッションID の固定をさせない）ウェブアプリケーションの設計にすることが必要である。

* + - * 1. 3.1.4 画像投稿サイト等のファイルアップロードサイトでのポイント

違法なファイルをアップロードされる以外にも、 実行形式のファイルをアップロードされてしまうことにより、 アップロードサイトのサーバ上で不正なファイルを実行されてしまう可能性がある。

このようなことが可能な場合、 スクリプトを含むファイルをアップロードし、 外部からそのファイルを参照することで、 任意のスクリプトをサーバ上で実行されてしまう被害が考えられる。

スクリプトを実行されることで、 ウェブサイトの改ざんや、 サーバの設定の改ざんにつながる可能性がある。

また、 ウイルスを含むファイルをアップロードされた場合、 サーバにウイルスが感染し、 外部から不正な命令を受け付けるようにされてしまう可能性もある。

このようなリスクを回避するために、 アップロード可能なファイル形式を制限するだけでなく、 アップロードされたサーバ上でファイルのウイルスチェックを行う等の対策を講じることが必要である。

また、 特定のユーザ以外にアクセスを許可しないファイルが、 誰でもURL を直接指定することで閲覧できてしまうといった、 アクセス制限不備の問題が考えられる。

このような脆弱性がある場合、 アップロードされたファイルが不特定多数のサイト利用者から参照可能になってしまう。

この場合、 個人を特定できてしまう情報を含むファイルが、 URL を直接指定するだけで参照できるといった被害が発生する。

このような被害を防止するために、 ファイルのアクセス制限を適切に設定することが求められる。

* + - 1. 3.2. セキュリティ強化のポイント
         1. 技術的な対策の観点

(1) ネットワーク攻撃、 不正アクセス対策

・外部からの攻撃が発生しているかの把握（攻撃の検知等）

Subtopic

・外部からの攻撃からの防御（攻撃の遮断等）

Subtopic

(2) DDoS攻撃対策

・攻撃通信をネットワークに入れないためにどうするか

(3) なりすまし対策

・パスワードの管理体制の強化

・使用する接続方式、 認証方式の強化

サイト利用者に普及・啓発すべき対策について以下で解説する。

長く複雑なパスワードを設定するようにサイト利用者に要求すれば

・パスワードを使いまわす可能性の増加

・利便性の低下によるサイト利用者の減少

その一つの答えとして、 次に解説する二要素認証や二段階認証が存在する。

(4) 重要情報の保護対策

・データベースをインターネット公開領域(いわゆるDMZ45)に配置しない

・重要情報の暗号化

・情報を変更、 参照する際の再認証

重要情報の暗号化について

ウェブサイトに登録した情報を変更、 参照する際の再認証の必要性について

(5) 事業継続対策

サーバ等の機材故障やインターネット上から攻撃を受けた場合にウェブサイトの停止期間を最小化するためには、 事業継続計画（Business continuity planning）を検討する必要がある。

事業継続を目的とした対策には以下の２点等が存在

・予備システムを設置する

・バックアップを定期的に取得する

・予備システムを設置する

インターネットからの攻撃が行われ、 サーバが破壊されてしまった場合、 データやサービスの復旧には長期間の作業が必要となる。 このような場合に、 破壊されたサーバと同一の構成の予備システムがあれば、 ウェブサイト復旧までの時間を大幅に削減することが可能である。

注意すべき点として、 予備システムを有効に活用するためには、 主となるサーバと可能な限り同じデータを持ち、 同一のソフトウェアバージョンに揃える必要がある。

また、 予備システムが主となるサーバとは別の拠点に設置されていれば、 大規模な地域災害時への対策にも繋がる。

前述の予備システムを設置できない場合は、 次に説明するバックアップの取得が重要になる。

・バックアップを定期的に取得する

インターネット上から攻撃を受け、 ウェブサーバが破壊された際に、 ウェブサーバや重要情報のバックアップを取得していればバックアップデータを元にウェブサイトを速やかに復旧することができる。

多くの場合、 バックアップを取得するために専用のソフトウェアを購入する必要はなく、 OS の機能としてバックアップを取得することができる。

しかし、 バックアップデータを取得していても、 ウェブサーバ上に保管していれば、 ウェブサーバが攻撃を受けた際に同時にバックアップデータも破壊されてしまう可能性がある。

また、 バックアップデータを盗まれることで、 攻撃者が偽サイトを作成することを可能にしてしまうことも考えられる。 サーバ上に保管していない場合でも、 ネットワークに接続された端末に保管されていれば、 ウイルスがネットワークに侵入した際にバックアップデータが破壊・窃取を受ける可能性がある。

以上の理由から、 バックアップデータは外付けハードディスク等に保存し、 ネットワークから切り離して保管しておくことが望ましい。

* + - * 1. その他の対策の観点

(1) ログの収集、 分析

(2) 各種基準への準拠

近年では、 ウェブサイトへの攻撃による被害に対応した保険商品等が提供されている。 しかし、 このような保険に加入する場合は、 保険企業やセキュリティ関連組織等が定める基準に準拠したウェブサイト運用が行われていることが条件となっている場合が多い。

また、 ウェブサイトの性質やウェブサイト上で取り扱う情報によっては、 所轄官庁が取り扱いの基準を定めている場合がある。

国内であれば、 経済産業省やNISC46、 海外であればNIST47等の公的機関がセキュリティ要件について様々なガイドラインや基準を定めている。

サービス提供者を選択する際に注意すべき点として、 以下の２点を挙げる。

・関係する団体が定める必須のセキュリティ基準を満たしているか

EC サイト等の決済機能を有するウェブサイトであれば、 使用する決済機能を提供する企業や、 業界団体が定めるセキュリティ基準基準を満たしているかについて確認が必要である。

代表例として、 PCI DSS がある。 3.1.2 項でも解説した通り、 国内でクレジットカードの決済機能を導入する場合は、 PCI DSS に準拠することが求められる。

この他に、 サイト運営者が所属する業界や団体が定めるセキュリティ基準がないか確認し、 その基準を満たしているサービス提供者を選択すべきである。

・必須ではないが、 自発的にセキュリティ基準に則った対策を実施しているか

サービス提供者が自発的に何らかの基準に従ったセキュリティ対策を実施しているか、 という観点で選択を行うべきである。

サービス提供者が自発的に何らかの基準に従ったセキュリティ対策を実施しているか

一例をあげると、 モールやASP のサービス提供者を選択する場合であれば、 総務省が定めた「ASP・SaaS における 情報セキュリティ対策ガイドライン」に準拠しているか、 といった観点で確認することが考えられる。

これは、 ASP やSaaS のサービス提供者に対し、 実施すべきセキュリティ対策について解説した資料である。

着目すべき基準については、 ウェブサイトのサービス内容や運営形態によっても変わるため、 サイト運営者自身で調査することが必要である。

(3) セキュリティ専門事業者の活用

情報セキュリティを専門としない組織が独自に脆弱性診断や脆弱性対策を行うことは困難と考えられる。 そのため、 脆弱性の検査を行う情報セキュリティ専門の企業による診断を受けることが望ましい。

レンタルサーバ等では、 サーバの構築をサイト運営者自身で行う必要がある。

また、 サイト運営者によっては、 使用するウェブアプリケーションを独自に開発する場合もあり、 サーバや独自開発のウェブアプリケーションに脆弱性を作りこんでいないか、 十分に検査する必要がある。

しかしながら、 サイト運営者自身で脆弱性の検査を十分に行うことは困難であると考えられる。

特にハウジングやオンプレミスによる運営形態では、 サーバだけでなくネットワーク機器等にも脆弱性がないか調査する必要がある。

このような場合には、 脆弱性の検査を専門としたセキュリティ企業に、 サーバやウェブアプリケーションの脆弱性検査の委託を検討する必要がある。 セキュリティ専門企業については、 経済産業省が「情報セキュリティ監査企業台帳」を公開している。

(4) サービス終了時の情報の破棄

サーバの機器故障やウェブアプリケーションの老朽化、 事業方針の変更等により、 ウェブサイトの運用の終了や、 次期システムへ移行する時期が訪れる。

このような際に適切にデータの破棄が行われていない場合、 ハードウェアを取得した第三者によって重要情報が盗み取られる被害が想定される。 このような被害を防ぐため、 重要情報や情報記録媒体の破棄について対応を検討しておく必要がある。

モールやASP、 レンタルサーバ等ではウェブサイトのプログラムのみならず、 サイト利用

者の個人情報についても、 サービス提供者の管理するサーバ上で管理される。 そのため、 ウェブサイトの運営を終了し、 ASP 等の利用契約を解除する際、 データの破棄・消去をサービス提供者がどのように取り扱いしているかについて、 サービス提供者の選択時に確認する必要がある。

例えば、 使用していたサーバのハードディスクの破壊について証明書を発行する、 米国国防総省が定めるDoD 5220.22-M に従ったデータの消去を保証しているといった観点がある。

各組織がハードウェアを管理するオンプレミス等の運営形態の場合は、 前述の規格に沿って組織内でデータの削除やハードディスクの破壊を実施、 または専門業者に依頼しての実施を検討する必要がある。

* + 1. おわりに
       1. ウェブサイトで提供したいサービスや運営形態の手軽さだけでなく、 日々の運営でセキュリティを維持し続けることができるかといった点についても目を向けて頂き、 安全なウェブサイトの運営が可能な運営形態を選定するようにしてほしい。
    2. 補足資料
       1. 【補足1】ウェブサイト構築・運営の委託について
          1. 中小企業をはじめとして、 ウェブサイトの構築や運営を外部企業に委託する場合が数多く存在している。 ASP やモールの運営形態が目的と合致せず、 自組織内でウェブサイトを作成する技術がない場合は正しい選択である。
          2. しかしながら、 外部企業にウェブサイトの構築を委託した際、 契約内容にウェブサイトの脆弱性検査や運用開始後に脆弱性が見つかった場合の対応が盛り込まれておらず、 脆弱性を抱えたままコンテンツの更新だけが行われているウェブサイトが存在しており、 IPA に対して届出が行われている。
          3. このようなウェブサイトを運営するサイト運営者に脆弱性の連絡を行った際、 組織内で修正できないためウェブサイトを構築した企業に依頼する場合がある。
          4. しかし、 修正のための追加費用が発生してしまうことが原因で対応が行われないという事態が発生している。
          5. ウェブサイトに存在する脆弱性への対応は組織毎に判断すべき内容であるが、 重大な問題を抱えたまま運営し、 個人情報の流出等が発生する場合もあるため、 可能な限り脆弱性は解消することが望ましい。
          6. 前述したような事例となることを避けるために、 ウェブサイト構築・運営を委託する際には、 契約する際の項目に脆弱性の検査や脆弱性が見つかった場合の対応を明確に記載することが望ましいといえる。
       2. 【補足2】ログの取得について
          1. ログイン履歴
          2. アクセスログ
          3. 通信ログ
          4. ログを取得する際は以下の点に注意する

①意図しないログが残っていないか調査する

②取得場所以外の場所にログを保存する

* + - 1. 【補足3】バックアップの取得間隔について
         1. 実際にバックアップの取得期間をどのように設定するべきかについては、 ウェブサイトの運用計画を定める段階で、 ウェブサイトの目的や更新頻度等からどれぐらいの期間のデータの喪失を許容できるかといった観点で定めることが必要である。
    1. 【付録A】ウェブサイト構築・運営に関する参考資料
       1. 「ウェブサイト構築のライフサイクル」の各フェーズで参考となる資料を一覧にまとめた表である。
       2. 1.企画
          1. 1 情報セキュリティ10 大脅威 2018

https://www.ipa.go.jp/security/vuln/10threats2018.html

ドキュメントを参照: [10threats2017.html](https://www.ipa.go.jp/security/vuln/10threats2017.html)

IPA

* + - * 1. 2 情報セキュリティ白書

https://www.ipa.go.jp/security/publications/hakusyo/2017.html

ドキュメントを参照: [2017.html](https://www.ipa.go.jp/security/publications/hakusyo/2017.html)

IPA

* + - * 1. 3 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/)

IPA

* + - * 1. 4　中小企業のためのクラウドサービス安全利用の手引き

https://www.ipa.go.jp/security/cloud/tebiki\_guide.html

ドキュメントを参照: [tebiki\_guide.html](https://www.ipa.go.jp/security/cloud/tebiki_guide.html)

IPA

* + - * 1. 5 ウェブサイト構築事業者のための脆弱性対応ガイド

https://www.ipa.go.jp/security/fy20/reports/vuln\_handling/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/fy20/reports/vuln_handling/index.html)

IPA

* + - * 1. 6 セキュリティ担当者のための脆弱性対応ガイド

https://www.ipa.go.jp/security/fy22/reports/vuln\_handling/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/fy22/reports/vuln_handling/index.html)

IPA

* + - * 1. 7 ソフトウエア管理ガイドライン

http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanriguide.htm

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

経済産業省

* + - * 1. 8 効果的なサイバー防御のためのCIS クリティカルセキュリティコントロール

https://sans-japan.jp/resources/CriticalSecurityControls.html

ドキュメントを参照: [CriticalSecurityControls.html](https://sans-japan.jp/resources/CriticalSecurityControls.html)

Center For Internet Security

* + - * 1. 9 事業継続計画策定ガイドライン

http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents\_000039.html

ドキュメントを参照: [seccontents\_000039.html](http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000039.html)

経済産業省

* + - * 1. 10 経営者が知っておくべきセキュリティリスクと対応について

https://www.jpcert.or.jp/research/aptrisk.html

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

Delta Risk Limited Liability Company

* + - * 1. 11 システム開発ライフサイクルにおけるセキュリティの考慮事項

https://www.ipa.go.jp/security/publications/nist/index.html

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

米国国立標準技術研究所

* + - * 1. 12 データベースセキュリティガイドライン

http://www.db-security.org/report/guideline\_seika.html

ドキュメントを参照: [guideline\_seika.html](http://www.db-security.org/report/guideline_seika.html)

データベース・セキュリティ・コンソーシアム

* + - * 1. 13 DB 内部不正対策ガイドライン

http://www.db-security.org/report/ag\_seika.html

データベース・セキュリティ・コンソーシアム

* + - * 1. 14 Payment Card Industry（PCI）データセキュリティ基準 (PCI DSS)

https://ja.pcisecuritystandards.org/minisite/env2/

ドキュメントを参照: [env2](https://ja.pcisecuritystandards.org/minisite/env2/)

PCI Security Standards Council

* + - * 1. 15 連邦政府の情報および情報システムに対するセキュリティ分類規格

https://www.ipa.go.jp/security/publications/nist/index.html

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

米国国立標準技術研究所

* + - * 1. 16 政府機関の情報セキュリティ対策のための統一基準（平成28 年度版）

https://www.nisc.go.jp/active/general/kijun28.html

ドキュメントを参照: [kijun28.html](https://www.nisc.go.jp/active/general/kijun28.html)

内閣サイバーセキュリティセンター

* + - 1. 2.設計
         1. 17 ウェブサイト改ざんの脅威と対策

https://www.ipa.go.jp/security/technicalwatch/20140829.html

ドキュメントを参照: [20140829.html](https://www.ipa.go.jp/security/technicalwatch/20140829.html)

IPA

* + - * 1. 18 Web Application Firewall 読本

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

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

IPA

* + - * 1. 19 安全なウェブサイトの作り方

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)

IPA

* + - * 1. 20 攻撃者に狙われる設計・運用上の弱点についてのレポート

https://www.ipa.go.jp/security/technicalwatch/20140328.html

IPA

* + - * 1. 21 インシデント対応マニュアルの作成について

https://www.jpcert.or.jp/csirt\_material/build\_phase.html

ドキュメントを参照: [build\_phase.html](https://www.jpcert.or.jp/csirt_material/build_phase.html)

JPCERT/CC

* + - * 1. 22 情報資産の重み-対策レベル対応表

http://www.db-security.org/report.html

ドキュメントを参照: [report.html](http://www.db-security.org/report.html)

データベース・セキュリティ・コンソーシアム

* + - * 1. 23 DB セキュリティガイドライン-他フレームワーク対応表

http://www.db-security.org/report.html

ドキュメントを参照: [report.html](http://www.db-security.org/report.html)

データベース・セキュリティ・コンソーシアム

* + - * 1. 24 ITシステムのためのリスクマネジメントガイド

https://www.ipa.go.jp/security/publications/nist/index.html

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

米国国立標準技術研究所

* + - * 1. 25 連邦情報システムのためのセキュリティ計画作成ガイド 改訂第1 版

https://www.ipa.go.jp/security/publications/nist/index.html

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

米国国立標準技術研究所

* + - 1. 3.実装/構築
         1. 26 安全なウェブサイトの作り方

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)

IPA

* + - * 1. 27 ウェブサイト改ざんの脅威と対策

https://www.ipa.go.jp/security/technicalwatch/20140829.html

ドキュメントを参照: [20140829.html](https://www.ipa.go.jp/security/technicalwatch/20140829.html)

IPA

* + - * 1. 28 攻撃者に狙われる設計・運用上の弱点についてのレポート

https://www.ipa.go.jp/security/technicalwatch/20140328.html

ドキュメントを参照: [20140328.html](https://www.ipa.go.jp/security/technicalwatch/20140328.html)

IPA

* + - * 1. 29 IPA セキュア・プログラミング講座

https://www.ipa.go.jp/security/awareness/vendor/programming/

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

IPA

* + - * 1. 30 ウェブサイトにおける脆弱性検査手法の紹介（ソースコード検査編）

https://www.ipa.go.jp/security/technicalwatch/20140306.html

ドキュメントを参照: [20140306.html](https://www.ipa.go.jp/security/technicalwatch/20140306.html)

IPA

* + - * 1. 31 CERT C コーディングスタンダード

https://www.jpcert.or.jp/sc-rules/

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

JPCERT/CC

* + - * 1. 32 連邦政府情報システムのためのセキュリティ管理策アセスメントガイド

https://www.ipa.go.jp/security/publications/nist/index.html

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

米国国立標準技術研究所

* + - 1. 4.テスト
         1. 33 安全なウェブサイトの作り方

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)

IPA

* + - * 1. 34 ウェブサイトにおける脆弱性検査手法(ウェブアプリケーション検査編)

https://www.ipa.go.jp/security/technicalwatch/20160928-2.html

ドキュメントを参照: [20160928-2.html](https://www.ipa.go.jp/security/technicalwatch/20160928-2.html)

IPA

* + - * 1. 35 システム監査企業台帳

http://www.meti.go.jp/policy/netsecurity/sys-kansa/

ドキュメントを参照: [sys-kansa](http://www.meti.go.jp/policy/netsecurity/sys-kansa/)

経済産業省

* + - * 1. 36 情報セキュリティ監査企業台帳

http://www.meti.go.jp/policy/netsecurity/is-kansa/

経済産業省

* + - 1. 5.運用/利用
         1. 37 ウェブサイト運営者のための脆弱性対応ガイド

https://www.ipa.go.jp/security/fy19/reports/vuln\_handling/index.html

ドキュメントを参照: [index.html](https://www.ipa.go.jp/security/fy19/reports/vuln_handling/index.html)

IPA

* + - * 1. 38 インシデントハンドリングマニュアル

http://www.jpcert.or.jp/csirt\_material/operation\_phase.html

ドキュメントを参照: [operation\_phase.html](http://www.jpcert.or.jp/csirt_material/operation_phase.html)

JPCERT/CC

* + - * 1. 39 CSIRT ガイド

http://www.jpcert.or.jp/csirt\_material/operation\_phase.html

ドキュメントを参照: [operation\_phase.html](http://www.jpcert.or.jp/csirt_material/operation_phase.html)

JPCERT/CC

* + 1. 【付録B】複数の観点による運営形態の選定 アプローチ
       1. 図B-1 ウェブサイト構築時の観点に基づくフローチャート
       2. 図B-2 ウェブサイト運用時の観点に基づくフローチャート
       3. 図B-3 セキュリティインシデント発生時の観点から見たフローチャート
       4. 図B-4 セキュリティインシデント対応体制構築の観点から見たフローチャート
  1. 情報セキュリティ読本　四訂版- IT時代の危機管理入門 -【2014年11月4日IPA】

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

* + 1. 第4章　組織の一員としての情報セキュリティ対策
    2. 1.      1. 組織のセキュリティ対策
       1. 計画（Plan） - 体制の整備とポリシーの策定
       2. 実行（Do） - 導入と運用
       3. 点検（Check） - 監視と評価
       4. 処置（Act） - 見直しと改善
       5. 1.1.     1） 計画（Plan）- 体制の整備とポリシーの策定
          1. 組織内の体制を確立する
          2. セキュリティポリシーを策定する
          3. 対策事項の立案と手順書の整備
          4. 1.1.1.      組織内の体制を確立する

情報セキュリティを推進するための体制を組織内に作ることが出発点

実施担当者と、 その役割、 権限、 責任を定める

望ましい体制

経営陣が中心となって取り組む

全社横断的な体制

トップダウンの管理体制

* + - * 1. 1.1.2.      セキュリティポリシーの策定

セキュリティポリシーとは

組織として一貫したセキュリティ対策を行うために、 組織のセキュリティ方針と対策の基準を示したもの

セキュリティポリシーの階層

基本方針

対策基準

対策実施手順

策定前の準備

情報資産の「何を守るのか」を決定する

「どのようなリスクがあるのか」を分析する

責任者と担当者を明確にする

組織体の長＝情報セキュリティの最高責任者

* + - * 1. 1.1.3.      対策事項の立案と手順書の整備

対策基準とは

情報資産を脅威から守る方法を具体的に定めたもの

実施手順とは

対策基準を実際の行動に移す際の手順書（マニュアルのようなもの）

最初に設定する内容とその手順

定期的に実施する対策の手順

インシデント発生時の対策と手順

* + - 1. 1.2.     2） 実行（Do）- 導入と運用
         1. 導入フェーズ
         2. 運用フェーズ
         3. 1.2.1.      導入フェーズ

構築と設定

ウイルス対策ソフトやファイアウォールなどのセキュリティ装置の導入、 暗号機能の導入

OS、 アプリケーションのセキュリティ設定

設定における注意点

デフォルト設定は使用しない

不要なサービスの停止

脆弱性の解消

最新の修正プログラムを適用

レベルに応じたアクセス制御

組織のメンバーごとにアクセスレベルを設定

アクセスできる範囲と操作権限を制限する

* + - * 1. 1.2.2.      運用フェーズ

セキュリティポリシーの周知徹底とセキュリティ教育

役割と責任、 セキュリティ対策上のルールを周知

被害に遭わないために脅威と対策を教える

脆弱性対策

定期的な情報収集とパッチの適用

異動/退職社員のフォロー

退職者のアカウントは確実に削除（セキュリティホールになりうる）

* + - 1. 1.3.     3） 点検（Check） - 監視と評価 -
         1. 監視と評価
         2. セキュリティ事故への対処
         3. 1.3.1.      監視と評価

ネットワークを監視し、 異常や不正アクセスを検出する

通信、 不正アクセスの監視

異常検知、 不正アクセス検知、 脆弱性検査

ポリシーが守られているか自己または第三者による評価を行う

自己点検（チェックリストなどにより実施）

情報セキュリティ対策ベンチマークでの自己診断

情報セキュリティ監査

* + - * 1. 1.3.2.      セキュリティ事故への対処

セキュリティポリシーに則ったインシデント対応

特に注意すべき点

被害状況を調査し、 二次災害を防ぐ

原因を特定し、 再発防止策を徹底する

実施した対応の記録、 各種届出（必要な場合）

対応窓口を設置し、 正確な情報を提供する

Subtopic

* + - 1. 1.4.     4） 処置（Act） - 見直しと改善
         1. セキュリティポリシーを見直し、 改善点を検討する
         2. セキュリティマネジメントサイクルの実施にともない、 情報セキュリティ対策を高めることが重要
    1. 2.      2. 従業員としての心得
       1. 規則を知り、 遵守する
       2. 情報セキュリティ上の脅威と対策を知る
       3. 「自分だけは 」、 「これぐらいなら 」は通用しない
          1. 必ず上司に報告・相談する
       4. 特に、 情報漏えいに気を付ける
    2. 3.      3. 気を付けたい情報漏えい
       1. 情報漏えいの経路と原因
       2. 情報漏えいを防止するための管理対策のポイント
       3. 企業や組織の一員としての情報セキュリティ心得
       4. 3.1.     情報漏えいの経路と原因
          1. 情報漏えいの経路

PC本体、 スマートフォン、 タブレット端末、

外部記憶媒体（USBメモリなど）、

紙媒体、 P2Pファイル交換ソフト

* + - * 1. 情報漏えいの原因

管理ミス、 誤操作、 紛失・置忘れが約8割

* + - * 1. 人為的なミスを防ぐことが重要
      1. 3.2.     情報漏えいを防止するための管理対策のポイント
         1. P2Pファイル交換ソフトは使用しない
         2. 私物パソコン等を業務で使用しない（持ち込ませない）
         3. 個人情報や機密情報を外部に持ち出さない（記憶媒体にコピーしない）
         4. 社用のノートパソコンを持ち出す場合は、 ルールを決めて厳密に管理する
      2. 3.3.     企業や組織の一員としての情報セキュリティ心得
         1. 企業や組織の情報や機器を、 許可なく持ち出さない
         2. 私物のノートパソコンやプログラムなどを、 許可なく、 企業や組織に持ち込まない
         3. 企業や組織の情報や機器を未対策のまま放置しない
         4. 企業や組織の情報や機器を未対策のまま廃棄しない
         5. 個人に割り当てられた権限を他の人に貸与または譲渡しない
         6. 業務上知り得た情報を公言しない
         7. 情報漏えいを起こした場合は速やかに報告する
    1. 4.      4. 終わりのないプロセス
       1. 一度、 導入・設定すればそれで終わり、 というものではない。
       2. 運用、 見直し、 フィードバックを繰り返すプロセスが必要。
       3. 技術面だけでなく、 管理面も強化する
       4. 技術的対策と管理的対策はクルマの両輪の関係
    2. 5.      情報セキュリティにおけるさまざまな対策
       1. 参考） IPAセキュリティセンター「情報セキュリティマネジメントについて」
       2. http://www.ipa.go.jp/security/manager/protect/management.html
       3. 参考）読者層別：情報セキュリティ対策実践情報：
       4. http://www.ipa.go.jp/security/awareness/awareness.html
  1. 米国の「20の重要なセキュリティ対策」及びオーストラリアの「35の標的型サイバー侵入に対する軽減戦略」【2010年】

ドキュメントを参照: [27.6keigennsennryakuhp.pdf](https://ssl.bsk-z.or.jp/kakusyu/pdf/27.6keigennsennryakuhp.pdf)

* + 1. サブトピック 1
  1. コンピュータセキュリティインシデント対応ガイド（NIST SP 800-61）【2008年3月NIST】

ドキュメントを参照: [000025341.pdf](https://www.ipa.go.jp/files/000025341.pdf)

* + 1. NIST（米国立標準技術研究所）が体系化した英文で80ページほどの文書。 セキュリティ対策を次の4つのフェーズに分けて考えている。
    2. （1）準備：やられないよう備える
    3. （2）検知・分析：やられてもすぐに察知できる
    4. （3）根絶・復旧・封じ込め：やられた場合の被害を小さくし、 すぐビジネスを復旧させる
    5. （4）事件発生後の対応：再発防止と最後の水際の対策を考える
  1. JIPDEC経営読本「情報管理はマネーです」【2017年JIPDEC】

ドキュメントを参照: [jipdec\_keieidokuhon\_a4.pdf](https://www.jipdec.or.jp/library/u71kba00000072hw-att/jipdec_keieidokuhon_a4.pdf)

* 1. IPAテクニカルウォッチ「ランサムウェアの脅威と対策」【2017年1月IPA】

ドキュメントを参照: [000057314.pdf](https://www.ipa.go.jp/files/000057314.pdf)

* 1. IPAテクニカルウォッチ「標的型攻撃メールの例と見分け方」【2017年1月IPA】

ドキュメントを参照: [000043331.pdf](https://www.ipa.go.jp/files/000043331.pdf)

* 1. 情報漏えい発生時の対応ポイント集(第3版) 【2012年10月IPA】

ドキュメントを参照: [rouei\_taiou.pdf](http://www.ipa.go.jp/security/awareness/johorouei/rouei_taiou.pdf)

* 1. 「高度サイバー攻撃対処のためのリスク評価等のガイドライン 付属書」 【2016年10月NISC】

ドキュメントを参照: [riskguide-appendix.pdf](https://www.nisc.go.jp/active/general/pdf/riskguide-appendix.pdf)

* 1. 『高度標的型攻撃』対策に向けたシステム設計ガイド【2014年9月IPA】

ドキュメントを参照: [000046236.pdf](https://www.ipa.go.jp/files/000046236.pdf)

* 1. モバイルセキュリティ関連
     1. ●MDM導入・運用検討ガイド【経済産業省】

ドキュメントを参照: [MDMGuideV1.pdf](https://www.jssec.org/dl/MDMGuideV1.pdf)

* + 1. ●情報セキュリティ対策の基本 スマートフォン編 - IPA【IPA】

ドキュメントを参照: [000059213.pdf](https://www.ipa.go.jp/files/000059213.pdf)

* + 1. ●スマートフォン＆タブレットの業務利用に関するセキュリティガイドライン【経済産業省】

ドキュメントを参照: [seccontents\_000142.html](https://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000142.html)

* + 1. ●私物端末の業務利用におけるセキュリティ要件の考え方【内閣官房】

ドキュメントを参照: [byod.pdf](https://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/byod.pdf)

* + 1. ●テレワークセキュリティガイドライン第４版【総務省】

ドキュメントを参照: [000545372.pdf](https://www.soumu.go.jp/main_content/000545372.pdf)

* + 1. ●導入事例　大分県庁　【Soliton】

ドキュメントを参照: [pref-oita.html](https://www.soliton.co.jp/case_study/pref-oita.html)

* + 1. NISTガイドライン
       1. Mobile Device Security: Cloud and Hybrid Builds
          1. Executive Summary

ドキュメントを参照: [mds-nist-sp1800-4a-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4a-draft.pdf)

* + - * 1. Approach, Architecture, and Security Characteristics

ドキュメントを参照: [mds-nist-sp1800-4b-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4b-draft.pdf)

* + - * 1. How-To Guide

ドキュメントを参照: [mds-nist-sp1800-4c-draft.pdf](https://www.nccoe.nist.gov/sites/default/files/library/sp1800/mds-nist-sp1800-4c-draft.pdf)

1. 重要インフラ・政府機関向け（独法を含む）
   1. サイバーセキュリティ基本法（2016年4月15日改正）
      1. 目的
         1. サイバーセキュリティに関する施策を総合的かつ効果的に推進し、 もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、 国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。
   2. 【未整理】サイバーセキュリティ2018【2018年7月25日NISC】

ドキュメントを参照: [cs2018.pdf](https://www.nisc.go.jp/active/kihon/pdf/cs2018.pdf)

* 1. サイバーセキュリティ2017【2017年８月25日NISC】

ドキュメントを参照: [cs2017.pdf](https://www.nisc.go.jp/active/kihon/pdf/cs2017.pdf)

* 1. 重要インフラの情報セキュリティ対策に係る第4次行動計画【2017年4月18日NISC】

ドキュメントを参照: [infra\_rt4.pdf](https://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf)

* + 1. 重要インフラの情報セキュリティ対策に係る第４次行動計画（案）の概要

ドキュメントを参照: [pubcom\_ap4\_abst.pdf](https://www.nisc.go.jp/active/infra/pdf/pubcom_ap4_abst.pdf)

* 1. サイバーセキュリティ戦略【2015年９月４日閣議決定】

ドキュメントを参照: [cs-senryaku-kakugikettei.pdf](https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf)

* 1. 政府機関の情報セキュリティ対策のための統一規範

ドキュメントを参照: [kihan28.pdf](http://www.nisc.go.jp/active/general/pdf/kihan28.pdf)

* 1. 政府機関等の情報セキュリティ対策の運用等に関する指針

ドキュメントを参照: [shishin28.pdf](http://www.nisc.go.jp/active/general/pdf/shishin28.pdf)

* 1.  政府機関等の対策基準策定のためのガイドライン（平成 30 年度版）

ドキュメントを参照: [guide30.pdf](https://www.nisc.go.jp/active/general/pdf/guide30.pdf)

* + 1. 【2018年7月25日NISC】
    2. 第 1 部 総則
       1. 1.1 目的
       2. 1.2 対策基準の策定手順
       3. 1.3 本ガイドラインの改定
       4. 1.4 統一基準、 本ガイドライン及び実施手順の関係
       5. 1.5 統一基準で定義されている用語
          1. (1) 情報の格付の区分
          2. (2) 情報の取扱制限
          3. (3) 統一基準 1.3「用語定義」において定義されている用語
       6. 1.6 一般用語の解説
       7. 1.7 基本対策事項及び解説の読み方
    3. 第 2 部 情報セキュリティ対策の基本的枠組み
       1. 2.1 導入・計画
          1. 2.1.1 組織・体制の整備
          2. (1) 最高情報セキュリティ責任者及び最高情報セキュリティ副責任者の設置
          3. (2) 情報セキュリティ委員会の設置
          4. (3) 情報セキュリティ監査責任者の設置
          5. (4) 統括情報セキュリティ責任者・情報セキュリティ責任者等の設置
          6. (5) 最高情報セキュリティアドバイザーの設置
          7. (6) 情報セキュリティ対策推進体制の整備
          8. (7) 情報セキュリティインシデントに備えた体制の整備
          9. (8) 兼務を禁止する役割
          10. 2.1.2 対策基準・対策推進計画の策定
          11. (1) 対策基準の策定
          12. (2) 対策推進計画の策定
       2. 2.2 運用
          1. 2.2.1 情報セキュリティ関係規程の運用

(1) 情報セキュリティ対策の運用

(2) 違反への対処

* + - * 1. 2.2.2 例外措置

(1) 例外措置手続の整備

(2) 例外措置の運用

* + - * 1. 2.2.3 教育

(1) 教育体制の整備・教育実施計画の策定

(2) 教育の実施

* + - * 1. 2.2.4 情報セキュリティインシデントへの対処

(1) 情報セキュリティインシデントに備えた事前準備

(2) 情報セキュリティインシデントへの対処

(3) 情報セキュリティインシデントの再発防止・教訓の共有

* + - 1. 2.3 点検
         1. 2.3.1 情報セキュリティ対策の自己点検

(1) 自己点検計画の策定・手順の準備

(2) 自己点検の実施

(3) 自己点検結果の評価・改善

* + - * 1. 2.3.2 情報セキュリティ監査

(1) 監査実施計画の策定

(2) 監査の実施

(3) 監査結果に応じた対処

* + - 1. 2.4 見直し
         1. 2.4.1 情報セキュリティ対策の見直し

(1) 情報セキュリティ関係規程の見直し

(2) 対策推進計画の見直し

* + 1. 第 3 部 情報の取扱い
       1. 3.1 情報の取扱い
          1. 3.1.1 情報の取扱い

(1) 情報の取扱いに係る規定の整備

(2) 情報の目的外での利用等の禁止

(3) 情報の格付及び取扱制限の決定・明示等

(4) 情報の利用・保存

(5) 情報の提供・公表

(6) 情報の運搬・送信

(7) 情報の消去

(8) 情報のバックアップ

* + - 1. 3.2 情報を取り扱う区域の管理
         1. 3.2.1 情報を取り扱う区域の管理

(1) 要管理対策区域における対策の基準の決定

(2) 区域ごとの対策の決定

(3) 要管理対策区域における対策の実施

* + 1. 第 4 部 外部委託
       1. 4.1 外部委託
          1. 4.1.1 外部委託

(1) 外部委託に係る規定の整備

(2) 外部委託に係る契約

(3) 外部委託における対策の実施

(4) 外部委託における情報の取扱い

* + - * 1. 4.1.2 約款による外部サービスの利用

(1) 約款による外部サービスの利用に係る規定の整備

(2) 約款による外部サービスの利用における対策の実施

* + - * 1. 4.1.3 ソーシャルメディアサービスによる情報発信

(1) ソーシャルメディアサービスによる情報発信時の対策

* + - * 1. 4.1.4 クラウドサービスの利用

(1) クラウドサービスの利用における対策

* + 1. 第 5 部 情報システムのライフサイクル
       1. 5.1 情報システムに係る文書等の整備
          1. 5.1.1 情報システムに係る台帳等の整備

(1) 情報システム台帳の整備

(2) 情報システム関連文書の整備

* + - * 1. 5.1.2 機器等の調達に係る規定の整備

(1) 機器等の調達に係る規定の整備

* + - 1. 5.2 情報システムのライフサイクルの各段階における対策
         1. 5.2.1 情報システムの企画・要件定義

(1) 実施体制の確保

(2) 情報システムのセキュリティ要件の策定

(3) 情報システムの構築を外部委託する場合の対策

(4) 情報システムの運用・保守を外部委託する場合の対策

* + - * 1. 5.2.2 情報システムの調達・構築

(1) 機器等の選定時の対策

(2) 情報システムの構築時の対策

(3) 納品検査時の対策

* + - * 1. 5.2.3 情報システムの運用・保守

(1) 情報システムの運用・保守時の対策

* + - * 1. 5.2.4 情報システムの更改・廃棄

(1) 情報システムの更改・廃棄時の対策

* + - * 1. 5.2.5 情報システムについての対策の見直し

(1) 情報システムについての対策の見直し

* + - 1. 5.3 情報システムの運用継続計画
         1. 5.3.1 情報システムの運用継続計画の整備・整合的運用の確保

(1) 情報システムの運用継続計画の整備・整合的運用の確保

* + 1. 第 6 部 情報システムのセキュリティ要件
       1. 6.1 情報システムのセキュリティ機能
          1. 6.1.1 主体認証機能

(1) 主体認証機能の導入

(2) 識別コード及び主体認証情報の管理

* + - * 1. 6.1.2 アクセス制御機能

(1) アクセス制御機能の導入

* + - * 1. 6.1.3 権限の管理

(1) 権限の管理

* + - * 1. 6.1.4 ログの取得・管理

(1) ログの取得・管理

* + - * 1. 6.1.5 暗号・電子署名

(1) 暗号化機能・電子署名機能の導入

(2) 暗号化・電子署名に係る管理

* + - 1. 6.2 情報セキュリティの脅威への対策
         1. 6.2.1 ソフトウェアに関する脆弱性対策

(1) ソフトウェアに関する脆弱性対策の実施

* + - * 1. 6.2.2 不正プログラム対策

(1) 不正プログラム対策の実施

* + - * 1. 6.2.3 サービス不能攻撃対策

(1) サービス不能攻撃対策の実施

* + - * 1. 6.2.4 標的型攻撃対策

(1) 標的型攻撃対策の実施

* + - 1. 6.3 アプリケーション・コンテンツの作成・提供
         1. 6.3.1 アプリケーション・コンテンツの作成時の対策

(1) アプリケーション・コンテンツの作成に係る規定の整備

(2) アプリケーション・コンテンツのセキュリティ要件の策定

* + - * 1. 6.3.2 アプリケーション・コンテンツ提供時の対策

(1) 政府ドメイン名の使用

(2) 不正なウェブサイトへの誘導防止

(3) アプリケーション・コンテンツの告知

* + 1. 第 7 部 情報システムの構成要素
       1. 7.1 端末・サーバ装置等
          1. 7.1.1 端末

(1) 端末の導入時の対策

(2) 端末の運用時の対策

(3) 端末の運用終了時の対策

(4) 要機密情報を取り扱う機関等が支給する端末（要管理対策区域外で使用する場合に限る）及び機関等支給以外の端末の導入及び利用時の対策

* + - * 1. 7.1.2 サーバ装置

(1) サーバ装置の導入時の対策

(2) サーバ装置の運用時の対策

(3) サーバ装置の運用終了時の対策

* + - * 1. 7.1.3 複合機・特定用途機器

(1) 複合機

(2) IoT 機器を含む特定用途機器

* + - 1. 7.2 電子メール・ウェブ等
         1. 7.2.1 電子メール

(1) 電子メールの導入時の対策

* + - * 1. 7.2.2 ウェブ

(1) ウェブサーバの導入・運用時の対策

(2) ウェブアプリケーションの開発時・運用時の対策

* + - * 1. 7.2.3 ドメインネームシステム（DNS）

(1) DNS の導入時の対策

(2) DNS の運用時の対策

* + - * 1. 7.2.4 データベース

(1) データベースの導入・運用時の対策

* + - 1. 7.3 通信回線
         1. 7.3.1 通信回線

(1) 通信回線の導入時の対策

(2) 通信回線の運用時の対策

(3) 通信回線の運用終了時の対策

(4) リモートアクセス環境導入時の対策

(5) 無線 LAN 環境導入時の対策

* + - * 1. 7.3.2 IPv6 通信回線

(1) IPv6 通信を行う情報システムに係る対策

(2) 意図しない IPv6 通信の抑止・監視

* + 1. 第 8 部 情報システムの利用
       1. 8.1 情報システムの利用
          1. 8.1.1 情報システムの利用

(1) 情報システムの利用に係る規定の整備

(2) 情報システム利用者の規定の遵守を支援するための対策

(3) 情報システムの利用時の基本的対策

(4) 電子メール・ウェブの利用時の対策

(5) 識別コード・主体認証情報の取扱い

(6) 暗号・電子署名の利用時の対策

(7) 不正プログラム感染防止

* + - 1. 8.2 機関等支給以外の端末の利用
         1. 8.2.1 機関等支給以外の端末の利用

(1) 機関等支給以外の端末の利用可否の判断

(2) 機関等支給以外の端末の利用規定の整備・管理

(3) 機関等支給以外の端末の利用時の対策

* + 1. 付録
  1. 政府機関向け「アマゾン ウェブ サービス」対応セキュリティリファレンス

ドキュメントを参照: [aws\_security.html](http://dc.jp.nttdata.com/service/cloud/aws_security.html)

* + 1. NISC「政府機関等の情報セキュリティ対策のための統一基準群（平成28年度版）」の最新基準に対応したAWS利用のためのリファレンス
    2. 【参考】政府機関の情報セキュリティ対策のための統一基準（平成28年度版）

ドキュメントを参照: [kijyun28.pdf](http://www.nisc.go.jp/active/general/pdf/kijyun28.pdf)

* + 1. 【参考】府省庁対策基準策定のためのガイドライン（平成28年度版）

ドキュメントを参照: [guide28.pdf](http://www.nisc.go.jp/active/general/pdf/guide28.pdf)

* 1. 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」の策定について【2015年5月NISC】

ドキュメントを参照: [sbd\_sakutei.html](http://www.nisc.go.jp/active/general/sbd_sakutei.html)

* + 1. 情報システムに係る政府調達におけるセキュリティ要件策定マニュアル ◦「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」

ドキュメントを参照: [SBD\_manual.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_manual.pdf)

* + 1. 「同　マニュアル　付録A.対策要件集」

ドキュメントを参照: [SBD\_manual\_annex\_a.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_manual_annex_a.pdf)

* + 1. 「同　マニュアル　付録B.政府機関統一基準群対応表」

ドキュメントを参照: [SBD\_manual\_annex\_b.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_manual_annex_b.pdf)

* + 1. 「同　マニュアル　付録D.用語解説」

ドキュメントを参照: [SBD\_manual\_annex\_d.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_manual_annex_d.pdf)

* + - 1. 「同　マニュアル活用ワークシート」(MS-Excel形式)

ドキュメントを参照: [SBD\_manual\_worksheet.xlsx](http://www.nisc.go.jp/active/general/xls/SBD_manual_worksheet.xlsx)

* + - 1. 「同　マニュアル活用ワークシート」（活用例）

ドキュメントを参照: [SBD\_manual\_worksheet\_example.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_manual_worksheet_example.pdf)

* + 1. 「情報システムに係る政府調達におけるセキュリティ要件策定マニュアル」概要

ドキュメントを参照: [SBD\_overview.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_overview.pdf)

* + 1. 情報セキュリティを企画・設計段階から確保するための方策に係る検討会　報告書

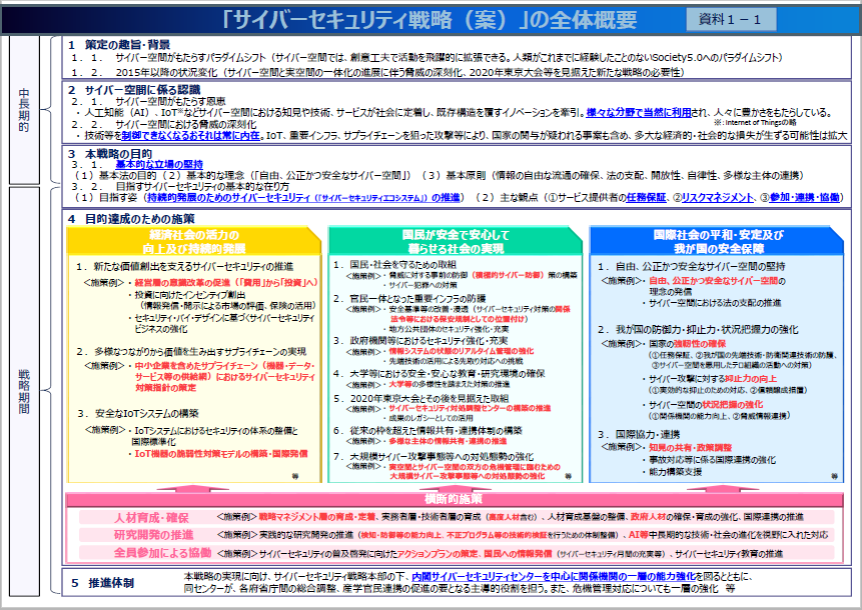
ドキュメントを参照: [SBD\_report.pdf](http://www.nisc.go.jp/active/general/pdf/SBD_report.pdf)

* 1. 地方公共団体における情報セキュリティポリシーに関するガイドライン【2015年3月総務省】

ドキュメントを参照: [000348656.pdf](http://www.soumu.go.jp/main_content/000348656.pdf)

1. 法令・規則・規約
   1. 施策・政策・統計
      1. サイバーセキュリティ基本法（2016年4月15日改正）
         1. 目的
            1. サイバーセキュリティに関する施策を総合的かつ効果的に推進し、 もって経済社会の活力の向上及び持続的発展並びに国民が安全で安心して暮らせる社会の実現を図るとともに、 国際社会の平和及び安全の確保並びに我が国の安全保障に寄与することを目的とする。
      2. 【校正中】サイバーセキュリティ戦略（案）（2018年6月2日NISC）

ドキュメントを参照: [18shiryou01.pdf](https://www.nisc.go.jp/conference/cs/dai18/pdf/18shiryou01.pdf)

* + - 1. 目的を達成するため、 戦略が寄与する政策領域ごとに、 今後３年間に執るべき諸施策の目標や実施方針
      2. 「サイバーセキュリティ戦略（案）」の全体概要
         1. Subtopic  
            
      3. 1. 策定の趣旨・背景
         1. 1.1. サイバー空間がもたらすパラダイムシフト
         2. 1.2. 2015 年以降の状況変化
      4. 2. サイバー空間に係る認識
         1. 2.1. サイバー空間がもたらす恩恵

(1) サイバー空間におけるサービスの進展と社会への定着

(2) AI の劇的な進化

(3) IoT の進展

* + - * 1. 2.2. サイバー空間における脅威の深刻化

(1) 業務・機能・サービス障害による社会への多大な影響

(2) 情報の毀損及び漏えいによる競争力低下

(3) 金銭の窃取・詐取等の損害

* + - 1. 3. 本戦略の目的
         1. 3.1. 基本的な立場の堅持

(1) 基本法の目的

(2) 基本的な理念

(3) 基本原則

① 情報の自由な流通の確保

② 法の支配

③ 開放性

④ 自律性

⑤ 多様な主体の連携

* + - * 1. 3.2. 目指すサイバーセキュリティの基本的な在り方

(1) 目指す姿

(2) ３つの観点

① サービス提供者の任務保証～業務・サービスの着実な遂行～

② リスクマネジメント～不確実性の評価と適切な対応～

③ 参加・連携・協働～個人・組織による平時からの対策と連携・協働～

* + - 1. 4. 目的達成のための施策
         1. 4.1. 経済社会の活力の向上及び持続的発展

ポイント

サイバー空間と実空間の一体化が加速的に進展する中、 「Society5.0」の実現に向け て、 グーバルな規模でこれまで取引がなかった異なる業種の企業間取引が生まれて いる。

また、 その取引自体が自動化されたものになるなど、 従来のサプライチェーン を超えた多様かつ流動的な形態を見せている。

そして、 このような形態においては、 サプライチェーンのつながりの端で起こったサイバーセキュリティの問題が、 実空間、 さらには、 経済社会全体にこれまで以上に広く波及し、 甚大な悪影響を及ぼすおそれ がある。

このようなリスクを認識し、 サプライチェーン全体を俯瞰した取組を推進す ることが不可欠である。

新たな価値創出を支えるサイバーセキュリティの推進

(1) 経営層の意識改革

(2) サイバーセキュリティに対する投資の推進

(3) 先端技術を利活用したイノベーションを支えるサイバーセキュリティビジネスの強化

多様なつながりから価値を生み出すサプライチェーンの実現

(1) サイバーセキュリティ対策指針の策定

サプライチェーンにおけるつながりが多様かつ流動的な形態になる中、 サイバーセキュリティの確保を進めていくためには、 サプライチェーン全体に対して、 一貫性をもった必要な対策が実装されることが不可欠である。 また、 このような取組を通じて、 モノやサービスに関わる品質が新たな価値を生み出すことが期待される。

具体的には、

官民が連携して、 サプライチェーンにおける脅威を明確化し、 運用レベルでの対策が実施できるような業種横断的な指針を策定するとともに、 その普及を図る。

その際には、 中小企業を含めた事業者が実際に対策を行いやすくするため、 事業者の事情を踏まえた現実的に実施が可能な内容で、 かつ、 分かりやすいものとなるように十分に配慮する。

また、 事業者がリスクと対策費用のバランスを意識できるものとすることも重要である。

産業分野毎のサプライチェーンに関わるつながり方や守るべきもの、 脅威の差異を意識しつつ、 IoT 機器や組織等に求められる具体的な対応策を産業分野毎に示していく必要がある。

さらに、 サプライチェーンがグーバルに拡がる中で、 我が国における対策指針に基づくサイバーセキュリティ対策がグーバルに認められるようにするため、 海外におけるルール化の動きも反映する必要がある。

(2) サプライチェーンにおけるサイバーセキュリティを確保できる仕組みの構築

サプライチェーン全体としてのサイバーセキュリティを確保するためには、 製造される機器、 生成されて流通するデータ、 それらを利用したサービス等のサプライチェーンの構成要素における信頼の確保が不可欠である。

このため、 それぞれの構成要素がセキュリティ要件を満たした形で生成・流通されるよう、 要件の明確化を図るとともに、 その要件が満たされていることを確認等することにより信頼を創出する仕組みの構築が必要である。

また、 サプライチェーンにおける調達者が機器・サービス等の利用に際し、 その信頼を確認できるよう、 官民が連携して、 信頼性が証明されている機器・サービス等のリストの作成と管理を行う仕組みの構築が必要である。

さらに、 これらがサプライチェーンのつながりにおいて、 連続的な仕組みとなるよう、 トレーサビリティ39を確認するための仕組みと、 創出された信頼そのものに対する攻撃を検知・防御するための仕組みを検討する。

(3) 中小企業の取組の促進

中小企業は、 サイバー攻撃により、 金銭的な損害や信用の低下が生じた場合、 経営に与えるインパクトが大企業と比べて大きい。

また、 中小企業が踏み台となって自社のみならず取引先までサイバー攻撃の影響が拡大することも懸念されている。

一方、 中小企業は、 必ずしも高いサイバーセキュリティに関する知識やスキルを有しているとはいえず、 サイバーセキュリティに対して十分な投資を行うことが難しいという事情を踏まえた上で、 サイバーセキュリティ対策を推進する必要がある。

このため、 国は、 中小企業を対象として、 安全な情報システムの利活用モデルの提示を含む理解しやすいサイバーセキュリティ対策の事例集を作成するとともに、 サイバーセキュリティ保険の活用促進、 中小企業がサイバーセキュリティに関するトラブル等について相談できる仕組みの強化を行う。

また、 官民が連携して、 サイバーセキュリティに取り組んでいる中小企業が、 それを自主的に宣言できる仕組みなどの可視化の取組を促進するとともに、 インセンティブの仕組みとの連携により、 効果的に中小企業のサイバーセキュリティを進めるための仕組み作りを行う。

安全なIoT システムの構築

(1) IoT システムにおけるサイバーセキュリティの体系の整備と国際標準化

これまで、

IoT システムのサイバーセキュリティ対策については、 官民が連携し、 ガイドラインの策定を始めとする安全なIoT システムの実現に向けた様々な取組を推進してきた。

今後は、 安全なIoT システムが価値を創出することに重点を置き、 一定の整合性・一貫性をもって戦略的に取り組む必要がある。

このため、

我が国がこれまで示してきた安全なIoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素41に基づき、 各主体の間で対策に係る基本理念、 目標、 方法、 期限等についての共通認識の醸成と、 各分野・各主体の役割や機能の明確化を図った上で、 自律的にサイバーセキュリティに関わる取組を進めつつ、 各主体が協働した取組を推進する。

また、 国は、 こうした取組を促すため、 官民の各主体が抱える課題42やそれぞれの取組について、 全体像が俯瞰できる形で可視化するとともに、 情報共有を行うための仕組みを構築する。

さらに、 IoT システムにおける価値創出の仕組みを、 我が国の安全・安心といった強みを活かしながらグーバルな規模で展開し、 安全なIoT システムの普及によって国際経済の発展に貢献するため、 官民が連携の下、 安全なIoT システムを実現するために求められるサイバーセキュリティに関する基本的な要素等の国際標準化に向けた取組を推進する。

(2) 脆弱性対策に係る体制の整備

IoT 機器に対するサイバー攻撃等の深刻化に対応するため、

ネットワークの安全・信頼性を確保する観点で、 産官学民及び民間企業相互間の連携と役割分担の下、 対策を推進することが重要である。

このため、 官民が連携して、 IoT 機器の脆弱性について、 設計・製造、 運用、 そして破棄までのライフサイクル全体を見通したサイバーセキュリティ対策や、 ネットワーク上の脆弱な IoT 機器の対策等のための体制整備が必要である。

ライフサイクルを見通した IoT 機器のサイバーセキュリティ対策については、

それぞれの機器の利用方法やサイバーセキュリティ上の脅威、 諸外国の検討状況や技術の進展の動向等を十分踏まえた上で、 機器製造事業者、 電気通信事業者、 利用者等の各々の主体の相互理解と連携の下で取り組むべきである。 その中で、 官民が連携して、 それぞれの IoT 機器について、 その特性や利用方法等を踏まえつつ必要なサイバーセキュリティの要件を整理し、 その要件を満たすIoT 機器の利用を推奨する。

また、 ネットワーク上の脆弱な IoT 機器の対策については、

パスワード設定に不備のある機器の調査・特定を行い、 電気通信事業者において当該機器の利用者への注意

喚起を円滑に行えるよう、 所要の制度整備を着実に進める。 また、 対策の実施に当たっては、 関係省庁等が一体となって、 電気通信事業者、 機器製造事業者等と連携して取り組む。

将来的には、

これらの我が国の対策をモデルとして、 国際的な連携や標準化等を通じて海外に展開し、 安全なネットワークの環境整備に貢献をしていく。

* + - * 1. 4.2. 国民が安全で安心して暮らせる社会の実現

国民・社会を守るための取組

(1) 安全・安心なサイバー空間の利用環境の構築

(2) サイバー犯罪への対策

官民一体となった重要インフラの防護

(1) 行動計画に基づく主な取組

① リスクマネジメントの推進

② 安全基準等の改善・浸透

③ 深刻度評価基準

④ 官民の枠を超えた訓練・演習の実施

⑤ 制御系システムのセキュリティ対策

(2) 地方公共団体のセキュリティ強化・充実

政府機関等におけるセキュリティ強化・充実

(1) 情報システムのセキュリティ対策の高度化・可視化

① 情報システムの防御能力の向上と状態の把握

② 政府機関等における横断的な連携の高度化による被害の発生・拡大の防止

(2) クラウド化の推進等による効果的なセキュリティ対策

(3) 先端技術の活用による先取り対応への挑戦

(4) 監査を通じたサイバーセキュリティの水準の向上

(5) 組織的な対応能力の充実

大学等における安全・安心な教育・研究環境の確保

(1) 大学等の多様性を踏まえた対策の推進

(2) 大学等の連携協力による取組の推進

2020 年東京大会とその後を見据えた取組

(1) 2020 年東京大会に向けた態勢の整備

(2) 未来につながる成果の継承

従来の枠を超えた情報共有・連携体制の構築

(1) 多様な主体の情報共有・連携の推進

(2) 情報共有・連携の新たな段階へ

大規模サイバー攻撃事態等への対処態勢の強化

* + - * 1. 4.3. 国際社会の平和・安定及び我が国の安全保障への寄与

自由、 公正かつ安全なサイバー空間の堅持

(1) 自由、 公正かつ安全なサイバー空間の理念の発信

(2) サイバー空間における法の支配の推進

我が国の防御力・抑止力・状況把握力の強化

(1) 国家の強靱性の確保

① 任務保証

② 我が国の先端技術・防衛関連技術の防護

③ サイバー空間を悪用したテ組織の活動への対策

(2) サイバー攻撃に対する抑止力の向上

① 実効的な抑止のための対応

② 信頼醸成措置

(3) サイバー空間の状況把握の強化

① 関係機関の能力向上

② 脅威情報連携

国際協力・連携

(1) 知見の共有・政策調整

(2) 事故対応等に係る国際連携の強化

(3) 能力構築支援

* + - * 1. 4.4. 横断的施策

人材育成・確保

(1) 戦略マネジメント層の育成・定着

(2) 実務者層・技術者層の育成

(3) 人材育成基盤の整備

(4) 各府省庁におけるセキュリティ人材の確保・育成の強化

(5) 国際連携の推進

研究開発の推進

(1) 実践的な研究開発の推進

(2) 中長期的な技術・社会の進化を視野に入れた対応

全員参加による協働

* + - 1. 5. 推進体制
    1. サイバーセキュリティ戦略（2015年9月4日閣議決定）
       1. 2020年代初頭までを見据えつつ、 サイバーセキュリティ政策の基本的な方向性を示す
       2. １ サイバー空間に係る認識
          1. サイバー空間は、 「無限の価値を産むフンティア」である人工空間であり、 人々の経済社会の活動基盤
          2. あらゆるモノがネットワークに連接され、 実空間とサイバー空間との融合が高度に深化した「連接融合情報社会(連融情報社会)」が到来。 同時に、 サイバー攻撃の被害規模や社会的影響が年々拡大、 脅威の更なる深刻化が予想
       3. ２ 目的
          1. 「経済社会の活力の向上及び持続的発展」、 「国民が安全で安心して暮らせる社会の実現」、 「国際社会の平和・安定及び我が国の安全保障」に寄与する。
          2. そのために、 「自由、 公正かつ安全なサイバー空間」を創出・発展させる
       4. ３ 基本原則
          1. ① 情報の自由な流通の確保② 法の支配③ 開放性④ 自律性⑤ 多様な主体の連携
       5. ４ 目的達成のための施策
          1. ①後手から先手へ／ ②受動から主導へ／ ③サイバー空間から融合空間へ
          2. 経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

■安全なIoTシステムの創出

安全なIoT活用による新産業創出

■セキュリティマインドを持った企業経営の推進

経営層の意識改革、 組織内体制の整備

■セキュリティに係るビジネス環境の整備

ファンドによるセキュリティ産業の振興

* + - * 1. 国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■国民・社会を守るための取組

事業者の取組促進、 普及啓発、 サイバー犯罪対策

■重要インフラを守るための取組

防護対象の継続的見直し、 情報共有の活性化

■政府機関を守るための取組

攻撃を前提とした防御力強化、 監査を通じた徹底

* + - * 1. 国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義～

■我が国の安全の確保

警察・自衛隊等のサイバー対処能力強化

■国際社会の平和・安定

国際的な「法の支配」確立、 信頼醸成推進

■世界各国との協力・連携

米国・ASEANを始めとする諸国との協力・連携

* + - * 1. 横断的施策

■研究開発の推進

攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

■人材の育成・確保

ハイブリッド型人材の育成、 実践的演習、 突出人材の発掘・確保、 キャリアパス構築

* + - 1. ５ 推進体制
         1. 官民及び関係省庁間の連携強化、 東京オリンピック・パラリンピック競技大会等に向けた対応
    1. サイバーセキュリティ2016【2016年サイバーセキュリティ戦略本部】

ドキュメントを参照: [cyber-security2016.pdf](https://www.nisc.go.jp/active/kihon/pdf/cyber-security2016.pdf)

* + 1. 「政府機関等の情報セキュリティ対策のための統一基準群（平成28年度版）」（2016年8月31日サイバーセキュリティ戦略本部決定）
       1. http://www.nisc.go.jp/active/general/kijun28.html

ドキュメントを参照: [kijun28.html](http://www.nisc.go.jp/active/general/kijun28.html)

* + 1. 企業経営のためのサイバーセキュリティの考え方の策定について（2016年8月2日）【NISC】

ドキュメントを参照: [09shiryou07.pdf](http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf)

* + - 1. http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf

ドキュメントを参照: [09shiryou07.pdf](http://www.nisc.go.jp/conference/cs/dai09/pdf/09shiryou07.pdf)

* + - 1. サイバーセキュリティ戦略本部

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

* + - * 1. http://www.nisc.go.jp/conference/cs/index.html

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

* + - 1. 経営層に期待される 認識 や経営戦略を企画する人材層に向けた実装のためのツールを示す
      2. 基本方針
         1. ーサイバーセキュリティは、 より積極的な経営への「投資」へー
         2. サイバーセキュリティをやむを得ない「費用」でなく、 積極的な経営への「投資」と位置づけ、 企業としての「挑戦」と、 それに付随する「責任」として取り組むことが期待される
      3. I.基本的考え方
         1. 二つの基本的認識

＜①挑戦＞

新しい製品やサービスを創造するための戦略の一環として考えていく

Subtopic

＜②責任＞

サイバーセキュリティに取り組むことは社会的な要求・要請であり、 自社のみならず社会全体の発展にも寄与する

* + - * 1. 三つの留意事項

＜①情報発信による社会的評価の向上＞

「セキュリティ品質」を高め、 品質向上に有効な経営基盤の一つとしてセキュリティ対策を位置付けることで企業価値を高めることが必要。

そのような取組に係る姿勢や方針を情報発信することが重要。

＜②リスクの一項目としてのサイバーセキュリティ＞

提供する機能やサービスを全うする（機能保証）という観点から、 リスクの一項目としてのサイバーセキュリティの視点も踏まえ、 リスクを分析し、 総合的に判断。

経営層のリーダーシップが必要。

＜③サプライチェーン全体でのサイバーセキュリティの確保＞

サプライチェーンの一部の対策が不十分な場合でも、 自社の重要情報が流出するおそれあり。

一企業のみでの対策には限界があるため、 関係者間での情報共有活動への参加等が必要。

* + - 1. II.企業の視点別の取組
         1. ITの利活用やサイバーセキュリティへの取組において、 各企業の事業規模のみならず、 その認識の違いなどを踏まえて取り組んでいく必要がある
         2. ITの利活用を事業戦略上に位置づけ、 サイバーセキュリティを強く意識し、 積極的に競争力強化に活用しようとしている企業

（積極的にITによる革新と高いレベルのセキュリティに挑戦するあらゆる企業）

【経営者に期待される認識】

積極的なITの利活用を推進する中で、 製品やサービスの「セキュリティ品質」を一層高め、 自社のブランド価値の向上につなげるべく、 システムの基盤におけるセキュリティの向上、 情報・データの保護、 製品等の安全品質向上に取り組む。

様々な関係者との協働が重要であるため、 情報提供に主体的に取り組む。

決して現存する標準や取り組みなどに満足することなく、 実空間とサイバー空間の融合が高度に深化した明日の世界をリードし、 変革していく存在となることが期待される。

【実装に向けたツール】

IoTセキュリティに関するガイドライン（「IoTセキュリティのための一般的枠組」等）

自社のブランド価値としてのサイバーセキュリティに係る積極的な情報発信

* + - * 1. IT・セキュリティをビジネスの基盤として捉えている企業

（IT・サイバーセキュリティの重要性は理解しているものの、 積極的な事業戦略に組み込むところまでは位置づけていない企業）

【経営者に期待される認識】

経営者のリーダーシップによって、 社会的責任としてのサイバーセキュリティ対策に取り組む。

サプライチェーンやビジネスパートナー、 委託先を含めた対策を行う。

平時・緊急時のいずれにおいても、 情報開示などの適切なコミュニケーションを行う。

【実装に向けたツール】

サイバーセキュリティ経営ガイドライン

企業等がセキュリティ対策に取り組む上での保険等のリスク管理手法の活用

サイバーセキュリティを経営上の重要課題として取り組んでいることの情報発信

* + - * 1.  自らセキュリティ対策を行う上で、 事業上のリソースの制約が大きい企業

（主に中小企業等でセキュリティの専門組織を保持することが困難な企業）

【経営者に期待される認識】

サプライチェーンを通じて中小企業等の役割はますます重要となる中、 消費者や取引先との信頼関係醸成の観点から経営者自らサイバーセキュリティ対策に関心を持ち、 取り組む。

外部の能力や知見を活用しつつ、 効率的に進める方策を検討する。

【実装に向けたツール】

効率的なセキュリティ対策のためのサービスの利用（中小企業向けクラウドサービス等）

 サイバーセキュリティに関する相談窓やセミナー、 地域の相談員等の活用

* + 1. サイバーセキュリティ関連施策に関する平成29年度予算重点化方針

ドキュメントを参照: [yosanhoshin29.pdf](http://www.nisc.go.jp/active/kihon/pdf/yosanhoshin29.pdf)

* + 1. サイバーセキュリティ政策の評価に係る基本方針

ドキュメントを参照: [cs\_hyouka\_houshin.pdf](http://www.nisc.go.jp/active/kihon/pdf/cs_hyouka_houshin.pdf)

* + 1. 情報セキュリティ白書2017【2017年7月IPA】

ドキュメントを参照: [2017.html](https://www.ipa.go.jp/security/publications/hakusyo/2017.html)

* + - 1. 序章 2016年度の情報セキュリティの概況
      2. 第1章 情報セキュリティインシデント・脆弱性の現状と対策
         1. 1.1 2016年度に観測されたインシデント状況
         2. 1.2 情報セキュリティインシデント別の状況と事例
         3. 1.3 攻撃・手の動向と対策
         4. 1.4 情報システムの脆弱性の動向
         5. 1.5 情報セキュリティ対策の状況
      3. 第2章 情報セキュリティを支える基盤の動向
         1. 2.1 日本の情報セキュリティ政策の状況
         2. 2.2 情報セキュリティ関連法の整備状況
         3. 2.3 国別・地域別の情報セキュリティ政策の状況
         4. 2.4 情報セキュリティ人材の現状と育成
         5. 2.5 情報セキュリティマネジメント
         6. 2.6 国際標準化活動
         7. 2.7 評価認証制度
         8. 2.8 情報セキュリティの普及啓発活動
         9. 2.9 情報セキュリティ産業の規模と成長の動向
         10. 2.10 その他の情報セキュリティの状況
      4. 第3章 個別テーマ
         1. 3.1 制御システムの情報セキュリティ
         2. 3.2 IoTの情報セキュリティ
         3. 3.3 スマートデバイスの情報セキュリティ
         4. 3.4 金融の情報セキュリティ
         5. 3.5 オリンピックに向けた情報セキュリティ対策
      5. 付録 情報セキュリティ10大脅威2017・資料・ツール
         1. 情報セキュリティ10大脅威2017
         2. 資料A 2016年のコンピュータウイルス届出状況
         3. 資料B 2016年のコンピュータ不正アクセス届出状況
         4. 資料C ソフトウェア等の脆弱性関連情報に関する届出状況
         5. ツール 各ツールの紹介
  1. ISMS
     1. 情報セキュリティマネジメント（ISMS）に準拠した対策【ISO/IEC27001:2013（管理項目35, 管理策114）】
        1.  管理的対策
           1. A.5 情報セキュリティのための方針群

A.5.1 情報セキユリティのための経営陣の方向性

情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項並びに関連する法令及び規制に従って提示するため。

A.5.1.1 情報セキュリティのための方針群

情報セキュリティのための方針群は，これを定義し，管理層が承認し，発行し，従業員及び関連する外部関係者に通知することが望ましい。

CSF

ガバナンス（ID.GV）

ID.GV-1 自組織の情報セキュリティポリシーを定めている。

A.5.1.2 情報セキュリティのための方針群のレビュー

情報セキュリティのための方針群は，あらかじめ定めた間隔で，又は重大な変化が発生した場合に，それが引き続き適切，妥当かつ有効であることを確実にするためにレビューすることが望ましい。

* + - * 1. A.6 情報セキュリティのための組織

A.6.1 内部組織

組織内で情報セキュリティの実施及び運用に着手し，これを統制するための管理上の枠組みを確立するため。

A.6.1.1 情報セキュリティの役割及び責任

全ての情報セキュリティの責任を定め，割り当てることが望ましい。

CSF

資産管理（ID.AM）

ID.AM-6

ガバナンス（ID.GV）

ID.GV-2

意識向上およびトレーニング（PR.AT）

PR.AT-2

PR.AT-3

PR.AT-4

PR.AT-5

検知プロセス（DE.DP）

DE.DP-1

伝達（RS.CO）

RS.CO-1

A.6.1.2 職務の分離

相反する職務及び責任範囲は，組織の資産に対する，認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために，分離することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-4

データセキュリティ（PR.DS）

PR.DS-5

A.6.1.3 関係当局との連絡

関係当局との適切な連絡体制を維持することが望ましい。

CSF

伝達（RS.CO）

RS.CO-2

A.6.1.4 専門組織との連絡

情報セキュリティに関する研究会又は会議，及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持することが望ましい。

CSF

リスクアセスメント（ID.RA）

ID.RA-2

A.6.1.5 プロジェクトマネジメントにおける情報セキュリティ

プロジェクトの種類にかかわらず，プロジェクトマネジメントにおいては，情報セキュリティに取り組むことが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-2

A.6.2 モバイル機器及びテレワーキング

モバイル機器の利用及びテレワーキングに関するセキュリティを確実にするため。

A.6.2.1 モバイル機器の方針

モバイル機器を用いることによって生じるリスクを管理するために，方針及びその方針を支援するセキュリティ対策を採用することが望ましい。

A.6.2.2 テレワーキング

テレワーキングの場所でアクセス，処理及び保存される情報を保護するために，方針及びその方針を支援するセキュリティ対策を実施することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-3

* + - * 1. A.8 資産の管理

A.8.1 資産に対する責任

組織の資産を特定し，適切な保護の責任を定めるため。

A.8.1.1 資産目録

情報及び情報処理施設に関連する資産を特定することが望ましい。 また，これらの資産の目録を，作成し，維持することが望ましい。

CSF

資産管理（ID.AM）

ID.AM-1

ID.AM-2

A.8.1.2 資産の管理責任

目録の中で維持される資産は，管理されることが望ましい。

注6.1.2及び6.1.3では，情報セキュリティのリスクを運用管理することについて責任及び権限をもつ人又は主体をリスク所有者としている。 情報セキュリティにおいて，多くの場合，資産の管理責任を負う者はリスク所有者でもある。

CSF

資産管理（ID.AM）

ID.AM-1

ID.AM-2

A.8.1.3 資産利用の許容範囲

情報の利用の許容範囲，並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施することが望ましい。

A.8.1.4 資産の返却

全ての従業員及び外部の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産の全てを返却することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-11

A.8.2 情報分類

組織に対する情報の重要性に応じて，情報の適切なレベルでの保護を確実にするため。

A.8.2.1 情報の分類

情報は，法的要求事項，価値，重要性，及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から，分類することが望ましい。

CSF

資産管理（ID.AM）

ID.AM-5

A.8.2.2 情報のラベル付け

情報のラベル付けに関する適切な一連の手順は，組織が採用した情報分類体系に従って策定し，実施することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

保護技術（PR.PT）

PR.PT-2

A.8.2.3 資産の取り扱い

資産の取扱いに関する手順は，組織が採用した情報分類体系に従って策定し，実施することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-1

PR.DS-2

PR.DS-3

PR.DS-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-6

保護技術（PR.PT）

PR.PT-2

A.8.3 媒体の取扱い

媒体に保存された情報の認可されていない開示，変更，除去又は破壊を防止するため。

A.8.3.1 取外し可能な媒体の管理

組織が採用した分類体系に従って，取外し可能な媒体の管理のための手順を実施することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-3

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-6

保護技術（PR.PT）

PR.PT-2

A.8.3.2 媒体の処分

媒体が不要になった場合は，正式な手順を用いて，セキュリティを保って処分することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-3

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-6

A.8.3.3 物理的媒体の輸送

情報を格納した媒体は，輸送の途中における，認可されていないアクセス，不正使用又は破損から保護することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-3

保護技術（PR.PT）

PR.PT-2

* + - * 1. A.12 運用のセキュリティ

A.12.1 運用の手順及び責任

情報処理設備の正確かつセキュリティを保った運用を確実にするため。

A.12.1.1 操作手順書

操作手順は，文書化し，必要とする全ての利用者に対して利用可能とすることが望ましい。

A.12.1.2 変更管理

情報セキュリティに影響を与える，組織，業務プロセス，情報処理設備及びシステムの変更は，管理することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

A.12.1.3 容量・能力の管理

要求されたシステム性能を満たすことを確実にするために，資源の利用を監視・調整し，また，将来必要とする容量・能力を予測することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-4

A.12.1.4 開発環境、 試験環境及び運用環境の分離

開発環境，試験環境及び運用環境は，運用環境への認可されていないアクセス又は変更によるリスクを低減するために，分離することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-7

A.12.2 マルウェアからの保護

情報及び情報処理施設がマルウェアから保護されることを確実にするため。

A.12.2.1 マルウェアに対する管理策

マルウェアから保護するために，利用者に適切に認識させることと併せて，検出，予防及び回復のための管理策を実施することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-6

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-4

低減（RS.MI）

RS.MI-2

A.12.3 バックアップ

データの消失から保護するため。

A.12.3.1 情報のバックアップ

情報，ソフトウェア及びシステムイメージのバックアップは，合意されたバックアップ方針に従って定期的に取得し，検査することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-4

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-4

A.12.4 ログ取得及び監視

A.12.4.1 イベントログ取得

利用者の活動，例外処理，過失及び情報セキュリティ事象を記録したイベントログを取得し，保持し，定期的にレビューすることが望ましい。

CSF

保護技術（PR.PT）

PR.PT-1

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-3

分析 (RS.AN)

RS.AN-1

A.12.4.2 ログ情報の保護

ログ機能及びログ情報は，改ざん及び認可されていないアクセスから保護することが望ましい。

CSF

保護技術（PR.PT）

PR.PT-1

A.12.4.3 実務管理者及び運用担当者の作業ログ

システムの実務管理者及び運用担当者の作業は，記録し，そのログを保護し，定期的にレビューすることが望ましい。

CSF

保護技術（PR.PT）

PR.PT-1

分析 (RS.AN)

RS.AN-1

A.12.4.4 クロックの同期

組織又はセキュリティ領域内の関連する全ての情報処理システムのクロックは，単一の参照時刻源と同期させることが望ましい。

CSF

保護技術（PR.PT）

PR.PT-1

A.12.5 運用ソフトウエアの管理

運用システムの完全性を確実にするため。

A.12.5.1 運用システムに関わるソフトウェアの導入

運用システムに関わるソフトウェアの導入を管理するための手順を実施することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-6

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

A.12.6 技術的ぜい弱性管理

技術的ぜい弱性の悪用を防止するため。

A.12.6.1 技術的脆弱性の管理

利用中の情報システムの技術的ぜい弱性に関する情報は，時機を失せずに獲得することが望ましい。 また，そのようなぜい弱性に組織がさらされている状況を評価することが望ましい。 さらに，それらと関連するリスクに対処するために，適切な手段をとることが望ましい。

CSF

リスクアセスメント（ID.RA）

ID.RA-1

ID.RA-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-12

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-8

低減（RS.MI）

RS.MI-3

A.12.6.2 ソフトウェアのインストールの制限

利用者によるソフトウェアのインストールを管理する規則を確立し，実施することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

A.12.7 情報システムの監査に対する考慮事項

運用システムに対する監査活動の影響を最小限にするため。

A.12.7.1 情報システムの監査に対する管理

運用システムの検証を伴う監査要求事項及び監査活動は，業務プロセスの中断を最小限に抑えるために，慎重に計画し，合意することが望ましい。

CSF

保護技術（PR.PT）

PR.PT-1

* + - * 1. A.15 供給者関係

A.15.1 供給者関係における情報セキュリティ

供給者がアクセスできる組織の資産の保護を確実にするため。

A.15.1.1 供給者関係のための情報セキュリティの方針

組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化することが望ましい。

CSF

保守（PR.MA）

PR.MA-2

A.15.1.2 供給者との合意におけるセキュリティの取扱い

関連する全ての情報セキュリティ要求事項を確立し，組織の情報に対して，アクセス，処理，保存若しくは通信を行う，又は組織の情報のための IT 基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意することが望ましい。

A.15.1.3 ICTサプライチェーン

供給者との合意には，情報通信技術（以下，ICT という。 ）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めることが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-1

A.15.2 供給者のサービス提供の管理

供給者との合意に沿って，情報セキュリティ及びサービス提供について合意したレベルを維持するため。

A.15.2.1 供給者のサービス提供の監視及びレビュー

組織は，供給者のサービス提供を定常的に監視し，レビューし，監査することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-1

保守（PR.MA）

PR.MA-2

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-6

A.15.2.2 供給者のサービス提供の変更に対する管理

関連する業務情報，業務システム及び業務プロセスの重要性，並びにリスクの再評価を考慮して，供給者によるサービス提供の変更（現行の情報セキュリティの方針群，手順及び管理策の保守及び改善を含む。 ）を管理することが望ましい。

* + - * 1. A.16 情報セキュリティインシデント管理

A.16.1 情報セキュリティインシデントの管理及びその改善

セキュリティ事象及びセキュリティ弱点に関する伝達を含む，情報セキュリティインシデントの管理のための，一貫性のある効果的な取組みを確実にするため。

A.16.1.1 責任及び手順

情報セキュリティインシデントに対する迅速，効果的かつ順序だった対応を確実にするために，管理層の責任及び手順を確立することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-9

異常とイベント（DE.AE）

DE.AE-2

伝達（RS.CO）

RS.CO-1

A.16.1.2 情報セキュリティ事象の報告

情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけ速やかに報告することが望ましい。

CSF

検知プロセス（DE.DP）

DE.DP-4

伝達（RS.CO）

RS.CO-2

A.16.1.3 情報セキュリティ弱点の報告

組織の情報システム及びサービスを利用する従業員及び契約相手に，システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点は，どのようなものでも記録し，報告するように要求することが望ましい。

A.16.1.4 情報セキュリティ事象の評価及び決定

情報セキュリティ事象は，これを評価し，情報セキュリティインシデントに分類するか否かを決定することが望ましい。

CSF

異常とイベント（DE.AE）

DE.AE-2

分析 (RS.AN)

RS.AN-4

A.16.1.5 情報セキュリティインシデントへの対応

情報セキュリティインシデントは，文書化した手順に従って対応することが望ましい。

CSF

対応計画（RS.RP）

RS.RP-1

分析 (RS.AN)

RS.AN-1

低減（RS.MI）

RS.MI-1

RS.MI-2

復旧計画（RC.RP）

RC.RP-1

A.16.1.6 情報セキュリティインシデントからの学習

情報セキュリティインシデントの分析及び解決から得られた知識は，インシデントが将来起こる可能性又はその影響を低減するために用いることが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-8

検知プロセス（DE.DP）

DE.DP-5

分析 (RS.AN)

RS.AN-2

改善（RS.IM）

RS.IM-1

A.16.1.7 証拠の収集

組織は，証拠となり得る情報の特定，収集，取得及び保存のための手順を定め，適用することが望ましい。

CSF

分析 (RS.AN)

RS.AN-3

* + - * 1. A.17 事業継続マネジメントにおける情報セキュリティの側面

A.17.1 情報セキュリティ継続

情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むことが望ましい。

A.17.1.1 情報セキュリティ継続の計画

組織は，困難な状況（adverse situation）（例えば，危機又は災害）における，情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-9

A.17.1.2 情報セキュリティ継続の実施

組織は，困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための，プロセス，手順及び管理策を確立し，文書化し，実施し，維持することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-4

PR.IP-9

A.17.1.3 情報セキュリティ継続の検証、 レビュー及び評価

確立及び実施した情報セキュリティ継続のための管理策が，困難な状況の下で妥当かつ有効であることを確実にするために，組織は，定められた間隔でこれらの管理策を検証することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-10

PR.IP-4

A.17.2 冗長性

情報処理施設の可用性を確実にするため。

A.17.2.1 情報処理施設の可用性

情報処理施設は，可用性の要求事項を満たすのに十分な冗長性をもって，導入することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-5

* + - * 1. A.18 順守

A.18.1 法的及び契約上の要求事項の順守

情報セキュリティに関連する法的，規制又は契約上の義務に対する違反，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

A.18.1.1 適用法令及び契約上の要求事項の特定

各情報システム及び組織について，全ての関連する法令，規制及び契約上の要求事項，並びにこれらの要求事項を満たすための組織の取組みを，明確に特定し，文書化し，また，最新に保つことが望ましい。

A.18.1.2 知的財産権

知的財産権及び権利関係のあるソフトウェア製品の利用に関連する，法令，規制及び契約上の要求事項の順守を確実にするための適切な手順を実施することが望ましい。

A.18.1.3 記録の保護

記録は，法令，規制，契約及び事業上の要求事項に従って，消失，破壊，改ざん，認可されていないアクセス及び不正な流出から保護することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-4

A.18.1.4 プライバシー及び個人を特定できる情報（PII）の保護

プライバシー及び PII の保護は，関連する法令及び規制が適用される場合には，その要求に従って確実にすることが望ましい。

CSF

検知プロセス（DE.DP）

DE.DP-2

A.18.1.5 暗号化機能に対する規制

暗号化機能は，関連する全ての協定，法令及び規制を順守して用いることが望ましい。

CSF

ガバナンス（ID.GV）

ID.GV-3

A.18.2 情報セキュリティのレビュー

組織の方針及び手順に従って情報セキュリティが実施され，運用されることを確実にするため。

A.18.2.1 情報セキュリティの独立したレビュー

情報セキュリティ及びその実施の管理（例えば，情報セキュリティのための管理目的，管理策，方針，プロセス，手順）に対する組織の取組みについて，あらかじめ定めた間隔で，又は重大な変化が生じた場合に，独立したレビューを実施することが望ましい。

A.18.2.2 情報セキュリティのための方針群及び標準の順守

管理者は，自分の責任の範囲内における情報処理及び手順が，適切な情報セキュリティのための方針群，標準類，及び他の全てのセキュリティ要求事項を順守していることを定期的にレビューすることが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-12

A.18.2.3 技術的順守のレビュー

情報システムを，組織の情報セキュリティのための方針群及び標準の順守に関して，定めに従ってレビューすることが望ましい。

CSF

リスクアセスメント（ID.RA）

ID.RA-1

* + - 1.  人的対策
         1. A.7 人的資源のセキュリティ

A.7.1 雇用前

従業員及び契約相手がその責任を理解し，求められている役割にふさわしいことを確実にするため。

A.7.1.1 選考

全ての従業員候補者についての経歴などの確認は，関連する法令，規制及び倫理に従って行うことが望ましい。 また，この確認は，事業上の要求事項，アクセスされる情報の分類及び認識されたリスクに応じて行うことが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-11

A.7.1.2 雇用条件

従業員及び契約相手との雇用契約書には，情報セキュリティに関する各自の責任及び組織の責任を記載することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

A.7.2 雇用期間中

従業員及び契約相手が，情報セキュリティの責任を認識し，かつ，その責任を遂行することを確実にするため。

A.7.2.1 経営陣の責任

経営陣は，組織の確立された方針及び手順に従った情報セキュリティの適用を，全ての従業員及び契約相手に要求することが望ましい。

CSF

ガバナンス（ID.GV）

ID.GV-2

A.7.2.2 情報セキュリティの意識向上， 教育及び訓練

組織の全ての従業員，及び関係する場合には契約相手は，職務に関連する組織の方針及び手順についての，適切な，意識向上のための教育及び訓練を受け，また，定めに従ってその更新を受けることが望ましい。

CSF

意識向上およびトレーニング（PR.AT）

PR.AT-1

PR.AT-2

PR.AT-3

PR.AT-4

PR.AT-5

A.7.2.3 懲戒手続き

情報セキュリティ違反を犯した従業員に対して処置をとるための，正式かつ周知された懲戒手続を備えることが望ましい。

A.7.3 雇用の終了及び変更

雇用の終了又は変更のプロセスの一部として，組織の利益を保護するため。

A.7.3.1 雇用の終了又は変更に関する責任

雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定め，その従業員又は契約相手に伝達し，かつ，遂行させることが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-11

* + - 1.  物理的対策
         1. A.11 物理的及び環境的セキュリティ

A.11.1 セキュリティを保つべき領

組織の情報及び情報処理施設に対する認可されていない物理的アクセス，損傷及び妨害を防止するため。

A.11.1.1 物理的セキュリティ境界

取扱いに慎重を要する又は重要な情報及び情報処理施設のある領域を保護するために，物理的セキュリティ境界を定め，かつ，用いることが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-2

A.11.1.2 物理的入退管理策

セキュリティを保つべき領域は，認可された者だけにアクセスを許すことを確実にするために，適切な入退管理策によって保護することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-2

保守（PR.MA）

PR.MA-1

A.11.1.3 オフィス， 部屋及び施設のセキュリティ

オフィス，部屋及び施設に対する物理的セキュリティを設計し，適用することが望ましい。

A.11.1.4 外部及び環境の脅威からの保護

自然災害，悪意のある攻撃又は事故に対する物理的な保護を設計し，適用することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-5

アクセス制御（PR.AC）

PR.AC-2

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-5

A.11.1.5 セキュリティを保つべき領域での作業

セキュリティを保つべき領域での作業に関する手順を設計し，適用することが望ましい。

A.11.1.6 受渡場所

荷物の受渡場所などの立寄り場所，及び認可されていない者が施設に立ち入ることもあるその他の場所は，管理することが望ましい。 また，可能な場合には，認可されていないアクセスを避けるために，それらの場所を情報処理施設から離すことが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-2

A.11.2 装置

資産の損失，損傷，盗難又は劣化，及び組織の業務に対する妨害を防止するため。

A.11.2.1 装置の設置及び保護

装置は，環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置し，保護することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-5

A.11.2.2 サポートユーティリティ（ライフライン事業者）

装置は，サポートユーティリティの不具合による，停電，その他の故障から保護することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-4

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-5

A.11.2.3 ケーブル配線のセキュリティ

データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は，傍受，妨害又は損傷から保護することが望ましい。

CSF

ビジネス環境（ID.BE）

ID.BE-4

アクセス制御（PR.AC）

PR.AC-2

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-5

A.11.2.4 装置の保守

装置は，可用性及び完全性を継続的に維持することを確実にするために，正しく保守することが望ましい。

CSF

保守（PR.MA）

PR.MA-1

PR.MA-2

A.11.2.5 資産の移動

装置，情報又はソフトウェアは，事前の認可なしでは，構外に持ち出さないことが望ましい。

CSF

保守（PR.MA）

PR.MA-1

A.11.2.6 構外にある装置及び資産のセキュリティ

構外にある資産に対しては，構外での作業に伴った，構内での作業とは異なるリスクを考慮に入れて，セキュリティを適用することが望ましい。

CSF

資産管理（ID.AM）

ID.AM-4

A.11.2.7 装置のセキュリティを保った処分又は再利用

記憶媒体を内蔵した全ての装置は，処分又は再利用する前に，全ての取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること，又はセキュリティを保って上書きしていることを確実にするために，検証することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-3

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-6

A.11.2.8 無人状態にある利用者装置

利用者は，無人状態にある装置が適切な保護対策を備えていることを確実にすることが望ましい。

A.11.2.9 クリアデスク・クリアスクリーン方針

書類及び取外し可能な記憶媒体に対するクリアデスク方針，並びに情報処理設備に対するクリアスクリーン方針を適用することが望ましい。

CSF

保護技術（PR.PT）

PR.PT-2

* + - 1.  技術的対策
         1. A.9 アクセス制御

A.9.1 アクセス制御に対する業務上の要求事項

情報及び情報処理施設へのアクセスを制限するため。

A.9.1.1 アクセス制御方針

アクセス制御方針は，業務及び情報セキュリティの要求事項に基づいて確立し，文書化し，レビューすることが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

A.9.1.2 ネットワークおよびネットワークサービスへのアクセス

利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを，利用者に提供することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-4

データセキュリティ（PR.DS）

PR.DS-5

保護技術（PR.PT）

PR.PT-3

A.9.2 利用者アクセスの管理

システム及びサービスへの，認可された利用者のアクセスを確実にし，認可されていないアクセスを防止するため。

A.9.2.1 利用者登録及び登録削除

アクセス権の割当てを可能にするために，利用者の登録及び登録削除についての正式なプロセスを実施することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.2.2 利用者アクセスの提供（プロビジョニング）

全ての種類の利用者について，全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために，利用者アクセスの提供についての正式なプロセスを実施することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.2.3 特権的アクセス権の管理

特権的アクセス権の割当て及び利用は，制限し，管理することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-4

データセキュリティ（PR.DS）

PR.DS-5

A.9.2.4 利用者の秘密認証情報の管理

秘密認証情報の割当ては，正式な管理プロセスによって管理することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.2.5 利用者アクセス権のレビュー

資産の管理責任者は，利用者のアクセス権を定められた間隔でレビューすることが望ましい。

A.9.2.6 アクセス権の削除または修正

全ての従業員及び外部の利用者の情報及び情報処理施設に対するアクセス権は，雇用，契約又は合意の終了時に削除し，また，変更に合わせて修正することが望ましい。

A.9.3 利用者の責任

利用者に対して，自らの秘密認証情報を保護する責任をもたせるため。

A.9.3.1 秘密認証情報の利用

秘密認証情報の利用時に，組織の慣行に従うことを，利用者に要求することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.4 システム及びアプリケーションのアクセス制御

システム及びアプリケーションへの，認可されていないアクセスを防止するため。

A.9.4.1 情報へのアクセス制限

情報及びアプリケーションシステム機能へのアクセスは，アクセス制御方針に従って，制限することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-4

データセキュリティ（PR.DS）

PR.DS-5

A.9.4.2 セキュリティに配慮したログオン手順

アクセス制御方針で求められている場合には，システム及びアプリケーションへのアクセスは，セキュリティに配慮したログオン手順によって制御することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.4.3 パスワード管理システム

パスワード管理システムは，対話式とすることが望ましく，また，良質なパスワードを確実とするものが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-1

A.9.4.4 特権的なユーティリティプログラムの使用

システム及びアプリケーションによる制御を無効にすることのできるユーティリティプログラムの使用は，制限し，厳しく管理することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-4

データセキュリティ（PR.DS）

PR.DS-5

A.9.4.5 プログラムソースコードへのアクセス制御

プログラムソースコードへのアクセスは，制限することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

* + - * 1. A.10 暗号

A.10.1 暗号による管理策

情報の機密性，真正性及び／又は完全性を保護するために，暗号の適切かつ有効な利用を確実にするため。

A.10.1.1 暗号による管理策の利用方針

情報を保護するための暗号による管理策の利用に関する方針は，策定し，実施することが望ましい。

A.10.1.2 鍵管理

暗号鍵の利用，保護及び有効期間（lifetime）に関する方針を策定し，そのライフサイクル全体にわたって実施することが望ましい。

* + - * 1. A.13 通信のセキュリティ

A.13.1 ネットワークセキュリティ管理

ネットワークにおける情報の保護，及びネットワークを支える情報処理施設の保護を確実にするため。

A.13.1.1 ネットワーク管理策

システム及びアプリケーション内の情報を保護するために，ネットワークを管理し，制御することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-3

PR.AC-5

データセキュリティ（PR.DS）

PR.DS-2

保護技術（PR.PT）

PR.PT-4

A.13.1.2 ネットワークサービスのセキュリティ

組織が自ら提供するか外部委託しているかを問わず，全てのネットワークサービスについて，セキュリティ機能，サービスレベル及び管理上の要求事項を特定し，また，ネットワークサービス合意書にもこれらを盛り込むことが望ましい。

A.13.1.3 ネットワークの分離

情報サービス，利用者及び情報システムは，ネットワーク上で，グループごとに分離することが望ましい。

CSF

アクセス制御（PR.AC）

PR.AC-5

データセキュリティ（PR.DS）

PR.DS-5

A.13.2 情報の転送

組織の内部及び外部に転送した情報のセキュリティを維持するため。

A.13.2.1 情報転送の方針及び手順

あらゆる形式の通信設備を利用した情報転送を保護するために，正式な転送方針，手順及び管理策を備えることが望ましい。

CSF

資産管理（ID.AM）

ID.AM-3

アクセス制御（PR.AC）

PR.AC-3

PR.AC-5

データセキュリティ（PR.DS）

PR.DS-2

PR.DS-5

保護技術（PR.PT）

PR.PT-4

A.13.2.2 情報転送に関する合意

合意では，組織と外部関係者との間の業務情報のセキュリティを保った転送について，取り扱うことが望ましい。

A.13.2.3 電子的メッセージ通信

電子的メッセージ通信に含まれた情報は，適切に保護することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-2

PR.DS-5

A.13.2.4 秘密保持契約又は守秘義務契約

情報保護に対する組織の要件を反映する秘密保持契約又は守秘義務契約のための要求事項は，特定し，定めに従ってレビューし，文書化することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-5

* + - * 1. A.14 システムの取得、 開発及び保守

A.14.1 情報システムのセキユリティ要求事項

ライフサイクル全体にわたって，情報セキュリティが情報システムに欠くことのできない部分であることを確実にするため。 これには，公衆ネットワークを介してサービスを提供する情報システムのための要求事項も含む。

A.14.1.1 情報セキュリティ要求事項の分析及び仕様化

情報セキュリティに関連する要求事項は，新しい情報システム又は既存の情報システムの改善に関する要求事項に含めることが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-2

A.14.1.2 公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮

公衆ネットワークを経由するアプリケーションサービスに含まれる情報は，不正行為，契約紛争，並びに認可されていない開示及び変更から保護することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-2

PR.DS-5

PR.DS-6

A.14.1.3 アプリケーションサービスのトランザクションの保護

アプリケーションサービスのトランザクションに含まれる情報は，次の事項を未然に防止するために，保護することが望ましい。

CSF

データセキュリティ（PR.DS）

PR.DS-2

PR.DS-5

PR.DS-6

A.14.2 開発及びサポートプロセスにおけるセキュリティ

情報システムの開発サイクルの中で情報セキュリティを設計し，実施することを確実にするため。

A.14.2.1 セキュリティに配慮した開発のための方針

ソフトウェア及びシステムの開発のための規則は，組織内において確立し，開発に対して適用することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-2

A.14.2.2 システムの変更管理手順

開発のライフサイクルにおけるシステムの変更は，正式な変更管理手順を用いて管理することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

A.14.2.3 オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー

オペレーティングプラットフォームを変更するときは，組織の運用又はセキュリティに悪影響がないことを確実にするために，重要なアプリケーションをレビューし，試験することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

A.14.2.4 パッケージソフトウェアに対する制限

パッケージソフトウェアの変更は，抑止し，必要な変更だけに限ることが望ましい。 また，全ての変更は，厳重に管理することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-1

PR.IP-3

A.14.2.5 セキュリティに配慮したシステム構築の原則

セキュリティに配慮したシステムを構築するための原則を確立し，文書化し，維持し，全ての情報システムの実装に対して適用することが望ましい。

CSF

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-2

A.14.2.6 セキュリティに配慮したシステム開発環境

組織は，全てのシステム開発ライフサイクルを含む，システムの開発及び統合の取組みのためのセキュリティに配慮した開発環境を確立し，適切に保護することが望ましい。

A.14.2.7 外部委託による開発

組織は，外部委託したシステム開発活動を監督し，監視することが望ましい。

CSF

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-6

A.14.2.8 システムセキュリティの試験

セキュリティ機能（functionality）の試験は，開発期間中に実施することが望ましい。

CSF

検知プロセス（DE.DP）

DE.DP-3

A.14.2.9 システムの受入れ試験

新しい情報システム，及びその改訂版・更新版のために，受入れ試験のプログラム及び関連する基準を確立することが望ましい。

A.14.3 試験データ

試験に用いるデータの保護を確実にするため。

A.14.3.1 試験データの保護

試験データは，注意深く選定し，保護し，管理することが望ましい。

* + - 1. ISMSになくCSFにある項目
         1. ID 特定

資産管理（ID.AM）

ビジネス環境（ID.BE）

ID.BE-2

重要インフラとその産業分野における企業の位置付けを特定し、 伝達している。

ID.BE-3

企業のミッション、 目標、 活動に関して優先順位を定め、 伝達している。

ガバナンス（ID.GV）

ID.GV-4

ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している。

リスクアセスメント（ID.RA）

ID.RA-3

内外からの脅威を特定し、 文書化している。

ID.RA-4

ビジネスに対する潜在的な影響と、 その可能性を特定している。

ID.RA-6

リスクに対する対応を定め、 優先順位付けしている。

リスク管理戦略（ID.RM）

ID.RM-1

リスク管理プロセスが自組織の利害関係者によって確立、 管理され、 承認されている。

ID.RM-2

自組織のリスク許容度を決定し、 明確にしている。

ID.RM-3

企業によるリスク許容度の決定が、 重要インフラにおける自組織の役割と、 その分野に特化したリスク分析の結果に基づいて行われている。

* + - * 1. PR 防御

アクセス制御（PR.AC）

意識向上およびトレーニング（PR.AT）

データセキュリティ（PR.DS）

情報を保護するためのプロセスおよび手順（PR.IP）

PR.IP-7

保護プロセスを継続的に改善している。

保守（PR.MA）

保護技術（PR.PT）

* + - * 1. DE 検知

異常とイベント（DE.AE）

DE.AE-1

ネットワーク運用のベースラインと、 ユーザとシステム間の予測されるデータの流れを特定し、 管理している。

DE.AE-3

イベントデータを複数の情報源やセンサーから収集し、 相互に関連付けている。

DE.AE-4

イベントがもたらす影響を特定している。

DE.AE-5

インシデント警告の閾値を定めている。

セキュリティの継続的なモニタリング (DE.CM)

DE.CM-1

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 ネットワークをモニタリングしている。

DE.CM-2

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 物理環境をモニタリングしている。

DE.CM-7

権限のない従業員、 接続、 デバイス、 ソフトウェアのモニタリングを実施している。

検知プロセス（DE.DP）

* + - * 1. RS 対応

対応計画（RS.RP）

伝達（RS.CO）

RS.CO-4

対応計画に従って、 利害関係者との間で調整を行っている。

RS.CO-5

サイバーセキュリティに関する状況認識を深めるために、 外部利害関係者との間で任意の情報共有を行っている。

分析 (RS.AN)

低減（RS.MI）

改善（RS.IM）

RS.IM-2

対応戦略を更新している。

* + - * 1. RC 復旧

復旧計画（RC.RP）

改善（RC.IM）

RC.IM-1

学んだ教訓を復旧計画に取り入れている。

RC.IM-2

復旧戦略を更新している。

伝達（RC.CO）

RC.CO-1

: 広報活動を管理している

RC.CO-2

イベント発生後に評判を回復している。

RC.CO-3

復旧活動について内部利害関係者と役員、 そして経営陣に伝達している。

* + 1. ISMSユーザーズガイド -JIS Q 27001:2014対応【2014年4月14日JIPDEC】

ドキュメントを参照: [JIP-ISMS111-30.html](https://isms.jp/JIP-ISMS111-30.html)

* + 1. 情報セキュリティマネジメントシステム(ISMS) 適合性評価制度
       1. ISMS適合性評価制度とは
          1. JIS Q 27001:2014もしくはISO/IEC 27001:2013を認証基準とした情報セキュリティの運用管理に対する第三者評価制度である
       2. 認証審査
          1. 評価機関により、 JIS Q 27001:2014もしくはISO/IEC 27001:2013に基づいて認証審査が行われる
       3. JIPDEC
          1. 適合性評価制度に基づく適合性評価機関（認証機関）を認定する

適合性評価機関の認定、 不認定、 保留、 取消し又は一時停止等を審議する。

* + - 1. 情報セキュリティ関連の調達時に提示する要件（例）
         1.  情報セキュリティマネジメントシステム(ISMS)適合性評価制度の認証機関により、 ISMS認証を取得した機関（企業、 部署）

補足：外部委託作業時及び内容に関してのセキュリティ要件ではないが、 作業時に情報セキュリティに対するルールを順守する意識が高いと想定される

* + - 1. 参考資料
         1. 情報セキュリティマネジメントシステム(ISMS)適合性評価制度の概要

https://www.isms.jipdec.or.jp/about/index.html

ドキュメントを参照: [index.html](https://www.isms.jipdec.or.jp/about/index.html)

ISMS適合性評価制度の運用

ISMS適合性評価制度は、 組織が構築したISMSがJIS Q 27001（ISO/IEC 27001）に適合しているか審査し登録する「認証機関」、 審査員の資格を付与する「要員認証機関」、 及びこれら各機関がその業務を行う能力を備えているかをみる「認定機関」からなる総合的な仕組みである。 なお、 審査員になるために必要な研修を実施する「審査員研修機関」は要員認証機関が承認する。

Subtopic  


* + - * 1. ISMS認証機関一覧

https://www.isms.jipdec.or.jp/lst/isr/index.html

ドキュメントを参照: [index.html](https://www.isms.jipdec.or.jp/lst/isr/index.html)

* + - * 1. ISMS認証取得組織検索

https://www.isms.jipdec.or.jp/lst/ind/index.html

ドキュメントを参照: [index.html](https://www.isms.jipdec.or.jp/lst/ind/index.html)

* + - * 1. Subtopic
    1. 情報セキュリティマネジメント（ISMS）に準拠した対策【ISO/IEC27001:2013（管理項目35, 管理策114）】
       1. 管理的対策
          1. A5.情報セキュリティのための方針群

情報セキユリティのための経営陣の方向性

情報セキュリティのための方針群

情報セキュリティのための方針群は， これを定義し， 管理層が承認し， 発行し， 従業員及び関連する外部関係者に通知しなければならない

情報セキュリティのための方針群のレビュー

情報セキュリティのための方針群は， あらかじめ定めた間隔で， 又は重大な変化が発生した場合に， それが引き続き適切， 妥当かつ有効であることを確実にするためにレビューしなければならない。

* + - * 1. A6.情報セキュリティのための組織

内部組織

情報セキュリティの役割及び責任

全ての情報セキュリティの責任を定め， 割り当てなければならない

職務の分離

相反する職務及び責任範囲は組織の資産に対する， 認可されていない若しくは意図しない変更又は不正使用の危険性を低減するために， 分離しなければならない。

関係当局との連絡

関係当局との適切な連絡体制を維持しなければならない。

専門組織との連絡

情報セキュリティに関する研究会又は会議、 及び情報セキュリティの専門家による協会・団体との適切な連絡体制を維持しなければならない。

プジェクトマネジメントにおける情報セキュリティ

プジェクトの種類にかかわらず， プジェクトマネジメントにおいては， 情報セキュリティに取り組まなければならない。

モバイル機器及びテレワーキング

モバイル機器の方針

モバイル機器を用いることによって生じるリスクを管理するために、 方針及びその方針を支援するセキュリティ対策を採用しなければならない

テレワーキング

テレワーキングの場所でアクセス， 処理及び保存される情報を保護するために方針及びその方針を支援するセキュリティ対策を実施しなければならない。

* + - * 1. A8.資産の管理

資産に対する責任

資産目録

情報，情報に関連するその他の資産及び情報処理施設を特定しなければならない。 また，これらの資産の目録を，作成し，維持しなければならない。

資産の管理責任

目録の中で維持される資産は，管理されなければならない。

注6.1.2及び6.1.3では，情報セキュリティのリスクを運用管理することについて責任及び権限をもつ人又は主体をリスク所有者としている。 情報セキュリティにおいて，多くの場合，資産の管理責任を負う者はリスク所有者でもある。

資産利用の許容範囲

情報の利用の許容範囲，並びに情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則は，明確にし，文書化し，実施しなければならない。

資産の返却

全ての従業員及び外部の利用者は，雇用，契約又は合意の終了時に，自らが所持する組織の資産の全てを返却しなければならない。

情報分類

情報の分類

情報は，法的要求事項，価値，重要性，及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から，分類しなければならない。

情報のラベル付け

情報のラベル付けに関する適切な一連の手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない。

資産の取り扱い

資産の取扱いに関する手順は，組織が採用した情報分類体系に従って策定し，実施しなければならない

媒体の取扱い

取外し可能な媒体の管理

組織が採用した分類体系に従って、 取外し可能な媒体の管理のための手順を実施しなければならない

媒体の処分

媒体が不要になった場合は、 正式な手順を用いて、 セキュリティを保って処分しなければならない

物理的媒体の輸送

情報を格納した媒体は，輸送の途中における，認可されていないアクセス、 不正使用又は破損から保護しなければならない。

* + - * 1. A12.運用のセキュリティ

運用の手順及び責任

操作手順

変更管理

容量・能力の管理

開発環境、 試験環境及び運用環境の分離

マルウェアからの保護

マルウェアに対する管理策

バックアップ

情報のバックアップ

グ取得及び監視

イベントグ取得

グ情報の保護

実務管理者及び運用担当者の作業グ

クックの同期

運用ソフトウエアの管理

運用システムに関わるソフトウェアの導入

技術的ぜい弱性管理

技術的脆弱性の管理

ソフトウェアのインストールの制限

情報システムの監査に対する考慮事項

情報システムの監査に対する管理

* + - * 1. A15.供給者関係

供給者関係における情報セキュリティ

供給者関係のための情報セキュリティの方針

組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について，供給者と合意し，文書化しなければならない。

供給者との合意におけるセキュリティの取扱い

関連する全ての情報セキュリティ要求事項を確立しなければならず，また，組織の情報に対して，アクセスラ処理，保存若しくは通信を行う，又は組織の情報のためのIT基盤を提供する可能性のあるそれぞれの供給者と，この要求事項について合意しなければならない

ICTサプライチェーン

供給者との合意には，情報通信技術（ICT）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めなければならない

供給者のサービス提供の管理

供給者のサービス提供の監視及びレビュー

組織は，供給者のサービス提供を定常的に監視し，レビューし，監査しなければならない。

供給者のサービス提供の変更に対する管理

関連する業務情報業務システム及び業務プセスの重要性，並びにリスクの再評価を考慮して，供給者によるサービス提供の変更（現行の情報セキュリティの方針群，手順及び管理策の保守及び改善を含む。 ）を管理しなければならない。

* + - * 1. A16.情報セキュリティインシデント管理

情報セキュリティインシデントの管理及びその改

責任及び手順

情報セキュリティインシデントに対する迅速，効果的かつ順序だった対応を確実にするために，管理層の責任及び手順を確立しなければならない

情報セキュリティ事象の報告

情報セキュリティ事象は，適切な管理者への連絡経路を通して，できるだけ速やかに報告しなければならない。

情報セキュリティ弱点の報告

組織の情報システム及びサービスを利用する従業員及び契約相手に，システム又はサービスの中で発見した又は疑いをもった情報セキュリティ弱点はどのようなものでも記録し報告するように要求しなければならない。

情報セキュリティ事象の評価及び決定

情報セキュリティ事象は，これを評価し，情報セキュリティインシデントに分類するか否かを決定しなければならない。

情報セキュリティインシデントへの対応

情報セキュリティインシデントは，文書化した手順に従って対応しなければならない。

情報セキュリティインシデントからの学習

情報セキュリティインシデントの分析及び解決から得られた知識は，インシデントが将来起こる可能性又はその影響を低減するために用いなければならない。

証拠の収集

組織は，証拠となり得る情報の特定，収集，取得及び保存のための手順を定め，適用しなければならない。

* + - * 1. A17.事業継続マネジメントにおける情報セキュリティの側面

情報セキュリティ継続

情報セキュリティ継続の計画

組織は，困難な状況（ adversesituation) （例えば，危機又は災害）における情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しなければならない。

情報セキュリティ継続の実施

組織は，困難な状況の下で情報セキュリティ継続に対する要求レベルを確実にするための，プセス，手順及び管理策を確立し，文書化し，実施し，維持しなければならない

情報セキュリティ継続の検証、 レビュー及び評価

確立及び実施した情報セキュリティ継続のための管理策が，困難な状況の下で妥当かつ有効であることを確実にするために，組織は，定められた間隔でこれらの管理策を検証しなければならない。

冗長性

情報処理施設の可用性

情報処理施設は可用性の要求事項を満たすのに十分な冗長性をもって，導入しなければならない

* + - * 1. A18.順守

法的及び契約上の要求事項の順守

適用法令及び契約上の要求事項の特定

知的財産権

記録の保護

プライバシー及び個人を特定できる情報（PII）の保護

暗号化機能に対する規制

情報セキュリティのレビュー

情報セキュリティの独立したレビュー

情報セキュリティのための方針群及び標準の順守

技術的順守のレビュー

* + - 1. 人的対策
         1. A7.人的資源のセキュリティ

雇用前

選考

全ての従業員候補者についての経歴などの確認は， 関連する法令， 規制及び、 倫理に従って行わなければならない。 また， この確認は， 事業上の要求事項アクセスされる情報の分類及び認識されたリスクに応じて行わなければならない

雇用条件

従業員及び契約相手との雇用契約書には， 情報セキュリティに関する各自の責任及び組織の責任を記載しなければならない。

雇用期間中

経営陣の責任

経営陣は， 組織の確立された方針及び手順に従った情報セキュリティの適用を全ての従業員及び契約相手に要求しなければならない

情報セキュリティの意識向上， 教育及び訓練

組織の全ての従業員， 及び関係する場合には契約相手は， 職務に関連する組織の方針及び手順についての， 適切な， 意識向上のための教育及び訓練を受けなければならず， また， 定めに従ってその更新を受けなければならない。

懲戒手続き

情報セキュリティ違反を犯した従業員に対して処置をとるための， 正式かつ周知された懲戒手続を備えなければならない

雇用の終了及び変更

雇用の終了又は変更に関する責任

雇用の終了又は変更の後もなお有効な情報セキュリティに関する責任及び義務を定めその従業員又は契約相手に伝達し，かつ，遂行させなければならない。

* + - 1. 物理的対策
         1. A11.物理的及び環境的セキュリティ

セキュリティを保つべき領

物理的セキュリティ境界

物理的入退管理策

オフィス， 部屋及び施設のセキュリティ

外部及び環境の脅威からの保護

セキュリティを保つべき領域での作業

受渡場所

装置

装置の設置及び保護

サポートユーティリティ（ライフライン事業者）

ケーブル配線のセキュリティ

装置の保守

資産の移動

構外にある装置及び資産のセキュリティ

装置のセキュリティを保った処分又は再利用

無人状態にある利用者装置

クリアデスク・クリアスクリーン方針

* + - 1. 技術的対策
         1. A9.アクセス制御

アクセス制御に対する業務上の要求事項

アクセス制御方針

ネットワークおよびネットワークサービスへのアクセス

利用者アクセスの管理

利用者登録及び登録削除

利用者アクセスの提供（プビジョニング）

特権的アクセス権の管理

利用者の秘密認証情報の管理

利用者アクセス権のレビュー

アクセス権の削除または修正

利用者の責任

秘密認証情報の利用

システム及びアプリケーションのアクセス制御

情報へのアクセス制限

セキュリティに配慮したグオン手順

パスワード管理システム

特権的なユーティリティプグラムの使用

プグラムソースコードへのアクセス制御

* + - * 1. A10.暗号

暗号による管理策

暗号による管理策の利用方針

鍵管理

* + - * 1. A13.通信のセキュリティ

ネットワークセキュリティ管理

ネットワーク管理策

ネットワークサービスのセキュリティ

ネットワークの分離

情報の転送

情報転送の方針及び手順

情報転送に関する合意

電子的メッセージ通信

秘密保持契約又は守秘義務契約

* + - * 1. A14.システムの取得、 開発及び保守

情報システムのセキユリティ要求事項

情報セキュリティ要求事項の分析及び仕様化

公衆ネットワーク上のアプリケーションサービスのセキュリティの考慮

アプリケーションサービスのトランザクションの保護

開発及びサポートプセスにおけるセキュリティ

セキュリティに配慮した開発のための方針

システムの変更管理手順

オペレーティングプラットフォーム変更後のアプリケーションの技術的レビュー

パッケージソフトウェアに対する制限

セキュリティに配慮したシステム構築の原則

セキュリティに配慮したシステム開発環境

外部委託による開発

システムセキュリティの試験

システムの受入れ試験

試験データ

試験データの保護

* 1. NIST CSF　(重要インフラにおけるサイバーセキュリティフレームワーク)
     1. 重要インフラにおけるサイバーセキュリティフレームワーク1.0版（CSF)【2014年2月12日NIST】

ドキュメントを参照: [000038957.pdf](https://www.ipa.go.jp/files/000038957.pdf)

* + - 1. フレームワークの概要
         1. フレームワークコア
         2. フレームワークインプレメンテーションティア
         3. フレームワークプロファイル
    1. CSF フレームワークコア
       1. ID 特定
          1. 資産管理（ID.AM）

組織が事業目的を達成することを可能にするデータ、 職員、 デバイス、 システム、 施設を特定し、 事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。

ID.AM-1

企業内の物理デバイスとシステムの一覧を作成している。

参考情報

CCS CSC 1

COBIT 5 BAI09.01, BAI09.02

ISA 62443-2-1:2009 4.2.3.4

ISA 62443-3-3:2013 SR 7.8

 ISO/IEC 27001:2013 A.8.1.1

 ISO/IEC 27001:2013 A.8.1.2

NIST SP 800-53 Rev. 4 CM-8

ID.AM-2

企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している。

参考情報

CCS CSC 2

COBIT 5 BAI09.01, BAI09.02, BAI09.05

ISA 62443-2-1:2009 4.2.3.4

ISA 62443-3-3:2013 SR 7.8

 ISO/IEC 27001:2013 A.8.1.1

 ISO/IEC 27001:2013 A.8.1.2

NIST SP 800-53 Rev. 4 CM-8

ID.AM-3

企業内の通信とデータの流れの図を用意している。

参考情報

CCS CSC 1

COBIT 5 DSS05.02

ISA 62443-2-1:2009 4.2.3.4

 ISO/IEC 27001:2013 A.13.2.1

NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9,

PL-8

ID.AM-4

外部情報システムの一覧を作成している。

参考情報

COBIT 5 APO02.02

 ISO/IEC 27001:2013 A.11.2.6

NIST SP 800-53 Rev. 4 AC-20, SA-9

ID.AM-5

リソース（例：ハードウェア、 デバイス、 データ、 ソフトウェア）を、 分類、 重要度、 ビジネス上の価値に基づいて優先順位付けしている。

参考情報

COBIT 5 APO03.03, APO03.04, BAI09.02

ISA 62443-2-1:2009 4.2.3.6

 ISO/IEC 27001:2013 A.8.2.1

NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14

ID.AM-6

すべての従業員と第三者である利害関係者（例：供給業者、 顧客、 パートナー）に対して、 サイバーセキュリティ上の役割と責任を定めている。

参考情報

COBIT 5 APO01.02, DSS06.03

ISA 62443-2-1:2009 4.3.2.3.3

 ISO/IEC 27001:2013 A.6.1.1

NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

* + - * 1. ビジネス環境（ID.BE）

自組織のミッション、 目標、 利害関係者、 活動を理解し、 優先順位付けを行っている; この情報はサイバーセキュリティ上の役割、 責任、 リスク管理上の意思決定を伝達するために使用される。

ID.BE-1

サプライチェーンにおける企業の役割を特定し、 伝達している

参考情報

COBIT 5 APO08.04, APO08.05, APO10.03,

APO10.04, APO10.05

 ISO/IEC 27001:2013 A.15.1.3

 ISO/IEC 27001:2013 A.15.2.1

 ISO/IEC 27001:2013 A.15.2.2

NIST SP 800-53 Rev. 4 CP-2, SA-12

ID.BE-2

重要インフラとその産業分野における企業の位置付けを特定し、 伝達している。

参考情報

COBIT 5 APO02.06, APO03.01

NIST SP 800-53 Rev. 4 PM-8

ID.BE-3

企業のミッション、 目標、 活動に関して優先順位を定め、 伝達している。

参考情報

COBIT 5 APO02.01, APO02.06, APO03.01

ISA 62443-2-1:2009 4.2.2.1, 4.2.3.6

NIST SP 800-53 Rev. 4 PM-11, SA-14

ID.BE-4

重要サービスを提供する上での依存関係と重要な機能を把握している。

参考情報

 ISO/IEC 27001:2013 A.11.2.2

 ISO/IEC 27001:2013 A.11.2.3

 ISO/IEC 27001:2013 A.12.1.3

NIST SP 800-53 Rev. 4 CP-8, PE-9, PE-11,PM-8, SA-14

ID.BE-5

重要サービスの提供を支援する、 レジリエンスに関する要求事項を定めている。

参考情報

COBIT 5 DSS04.02

 ISO/IEC 27001:2013 A.11.1.4

 ISO/IEC 27001:2013 A.17.1.1

 ISO/IEC 27001:2013 A.17.1.2

 ISO/IEC 27001:2013 A.17.2.1

NIST SP 800-53 Rev. 4 CP-2, CP-11, SA-14

* + - * 1. ガバナンス（ID.GV）

自組織に対する規制、 法律、 リスクと、 自組織の環境、 運用上の要求事項を管理しモニタリングするためのポリシー、 手順、 プロセスを理解しており、 サイバーセキュリティリスクの管理者に伝達している。

ID.GV-1

自組織の情報セキュリティポリシーを定めている。

参考情報

COBIT 5 APO01.03, EDM01.01, EDM01.02

ISA 62443-2-1:2009 4.3.2.6

 ISO/IEC 27001:2013 A.5.1.1

NIST SP 800-53 Rev. 4 -1 controls from all families

ID.GV-2

情報セキュリティ上の役割と責任について、 内部と外部パートナーとで調整・連携している。

参考情報

COBIT 5 APO13.12

ISA 62443-2-1:2009 4.3.2.3.3

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.7.2.1

NIST SP 800-53 Rev. 4 PM-1, PS-7

ID.GV-3

プライバシーや市民の自由に関する義務を含む、 サイバーセキュリティに関する法規制上の要求事項を理解し、 管理している。

参考情報

COBIT 5 MEA03.01, MEA03.04

ISA 62443-2-1:2009 4.4.3.7

 ISO/IEC 27001:2013 A.18.1

NIST SP 800-53 Rev. 4 -1 controls from all families (except PM-1)

ID.GV-4

ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している。

参考情報

COBIT 5 DSS04.02

ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8,4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3

NIST SP 800-53 Rev. 4 PM-9, PM-11

* + - * 1. リスクアセスメント（ID.RA）

企業は自組織の業務（ミッション、 機能、 イメージ、 評判を含む）、 自組織の資産、 個人に対するサイバーセキュリティリスクを把握している。

ID.RA-1

資産の脆弱性を特定し、 文書化している。

参考情報

CCS CSC 4

COBIT 5 APO12.01, APO12.02, APO12.03,APO12.04

ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9,4.2.3.12

 ISO/IEC 27001:2013 A.12.6.1

 ISO/IEC 27001:2013 A.18.2.3

NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8,RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5

ID.RA-2

情報共有フォーラム／ソースより、 脅威と脆弱性に関する情報を入手している。

参考情報

ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12

 ISO/IEC 27001:2013 A.6.1.4

NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5

ID.RA-3

内外からの脅威を特定し、 文書化している。

参考情報

COBIT 5 APO12.01, APO12.02, APO12.03,APO12.04

ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12

NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12,PM-16

ID.RA-4

ビジネスに対する潜在的な影響と、 その可能性を特定している。

参考情報

COBIT 5 DSS04.02

ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12

NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9,PM-11, SA-14

ID.RA-5

リスクを判断する際に、 脅威、 脆弱性、 可能性、 影響を考慮している。

参考情報

COBIT 5 APO12.02

 ISO/IEC 27001:2013 A.12.6.1

NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16

ID.RA-6

リスクに対する対応を定め、 優先順位付けしている。

参考情報

COBIT 5 APO12.05, APO13.02

NIST SP 800-53 Rev. 4 PM-4, PM-9

* + - * 1. リスク管理戦略（ID.RM）

自組織の優先順位、 制約、 リスク許容度、 想定を定め、 運用リスクの判断に利用している。

ID.RM-1

リスク管理プロセスが自組織の利害関係者によって確立、 管理され、 承認されている。

参考情報

COBIT 5 APO12.04, APO12.05, APO13.02,BAI02.03, BAI04.02

ISA 62443-2-1:2009 4.3.4.2

NIST SP 800-53 Rev. 4 PM-9

ID.RM-2

自組織のリスク許容度を決定し、 明確にしている。

参考情報

COBIT 5 APO12.06

ISA 62443-2-1:2009 4.3.2.6.5

NIST SP 800-53 Rev. 4 PM-9

ID.RM-3

企業によるリスク許容度の決定が、 重要インフラにおける自組織の役割と、 その分野に特化したリスク分析の結果に基づいて行われている。

参考情報

NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11,SA-14

* + - 1. PR 防御
         1. アクセス制御（PR.AC）

資産および関連施設へのアクセスを、 承認されたユーザ、 プロセス、 またはデバイスと、 承認された活動およびトランザクションに限定している。

PR.AC-1

承認されたデバイスとユーザの識別情報と認証情報を管理している。

参考情報

CCS CSC 16

COBIT 5 DSS05.04, DSS06.03

ISA 62443-2-1:2009 4.3.3.5.1

ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9

 ISO/IEC 27001:2013 A.9.2.1

 ISO/IEC 27001:2013 A.9.2.2

 ISO/IEC 27001:2013 A.9.2.4

 ISO/IEC 27001:2013 A.9.3.1

 ISO/IEC 27001:2013 A.9.4.2

 ISO/IEC 27001:2013 A.9.4.3

NIST SP 800-53 Rev. 4 AC-2, IA Family

PR.AC-2

資産に対する物理アクセスを管理し、 保護している。

参考情報

COBIT 5 DSS01.04, DSS05.05

ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8

 ISO/IEC 27001:2013 A.11.1.1

 ISO/IEC 27001:2013 A.11.1.2

 ISO/IEC 27001:2013 A.11.1.4

 ISO/IEC 27001:2013 A.11.1.6

 ISO/IEC 27001:2013 A.11.2.3

NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9

PR.AC-3

リモートアクセスを管理している。

参考情報

COBIT 5 APO13.01, DSS01.04, DSS05.03

ISA 62443-2-1:2009 4.3.3.6.6

ISA 62443-3-3:2013 SR 1.13, SR 2.6

 ISO/IEC 27001:2013 A.6.2.2

 ISO/IEC 27001:2013 A.13.1.1

 ISO/IEC 27001:2013 A.13.2.1

NIST SP 800-53 Rev. 4 AC-17, AC-19, AC-20

PR.AC-4

最小権限および職務の分離の原則を取り入れて、 アクセス権限を管理している。

参考情報

CCS CSC 12, 15

ISA 62443-2-1:2009 4.3.3.7.3

ISA 62443-3-3:2013 SR 2.1

 ISO/IEC 27001:2013 A.6.1.2

 ISO/IEC 27001:2013 A.9.1.2

 ISO/IEC 27001:2013 A.9.2.3

 ISO/IEC 27001:2013 A.9.4.1

 ISO/IEC 27001:2013 A.9.4.4

NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16

PR.AC-5

適宜、 ネットワークの分離を行って、 ネットワークの完全性を保護している。

参考情報

ISA 62443-2-1:2009 4.3.3.4

ISA 62443-3-3:2013 SR 3.1, SR 3.8

 ISO/IEC 27001:2013 A.13.1.1

 ISO/IEC 27001:2013 A.13.1.3

 ISO/IEC 27001:2013 A.13.2.1

NIST SP 800-53 Rev. 4 AC-4, SC-7

* + - * 1. 意識向上およびトレーニング（PR.AT）

自組織の職員およびパートナーに対して、 関連するポリシー、 手順、 契約に基づいた、 情報セキュリティに関連する義務と責任を果たせるようにするために、 サイバーセキュリティ意識向上教育と、 十分なトレーニングを実施している。

PR.AT-1

すべてのユーザに情報を周知し、 トレーニングを実施している。

参考情報

CCS CSC 9

COBIT 5 APO07.03, BAI05.07

ISA 62443-2-1:2009 4.3.2.4.2

 ISO/IEC 27001:2013 A.7.2.2

NIST SP 800-53 Rev. 4 AT-2, PM-13

PR.AT-2

権限を持つユーザが役割と責任を理解している。

参考情報

CCS CSC 9

COBIT 5 APO07.02, DSS06.03

ISA 62443-2-1:2009 4.3.2.4.2, 4.3.2.4.3

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.7.2.2

NIST SP 800-53 Rev. 4 AT-3, PM-13

PR.AT-3

第三者である利害関係者（例：供給業者、 顧客、 パートナー）が役割と責任を理解している。

参考情報

CCS CSC 9

COBIT 5 APO07.03, APO10.04, APO10.05

ISA 62443-2-1:2009 4.3.2.4.2

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.7.2.2

NIST SP 800-53 Rev. 4 PS-7, SA-9

PR.AT-4

上級役員が役割と責任を理解している。

参考情報

CCS CSC 9

COBIT 5 APO07.03

ISA 62443-2-1:2009 4.3.2.4.2

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.7.2.2

NIST SP 800-53 Rev. 4 AT-3, PM-13

PR.AT-5

物理セキュリティおよび情報セキュリティの担当者が役割と責任を理解している。

参考情報

CCS CSC 9

COBIT 5 APO07.03

ISA 62443-2-1:2009 4.3.2.4.2

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.7.2.2

NIST SP 800-53 Rev. 4 AT-3, PM-13

* + - * 1. データセキュリティ（PR.DS）

情報と記録（データ）を情報の機密性、 完全性、 可用性を保護するために定められた自組織のリスク戦略に従って管理している。

PR.DS-1

保存されているデータを保護している。

参考情報

CCS CSC 17

COBIT 5 APO01.06, BAI02.01, BAI06.01,

DSS06.06

ISA 62443-3-3:2013 SR 3.4, SR 4.1

 ISO/IEC 27001:2013 A.8.2.3

NIST SP 800-53 Rev. 4 SC-28

PR.DS-2

伝送中のデータを保護している。

参考情報

CCS CSC 17

COBIT 5 APO01.06, DSS06.06

ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2

 ISO/IEC 27001:2013 A.8.2.3

 ISO/IEC 27001:2013 A.13.1.1

 ISO/IEC 27001:2013 A.13.2.1

 ISO/IEC 27001:2013 A.13.2.3

 ISO/IEC 27001:2013 A.14.1.2

 ISO/IEC 27001:2013 A.14.1.3

NIST SP 800-53 Rev. 4 SC-8

PR.DS-3

資産について撤去、 譲渡、 廃棄プロセスを正式に管理している。

参考情報

COBIT 5 BAI09.03

ISA 62443-2-1:2009 4. 4.3.3.3.9, 4.3.4.4.1

ISA 62443-3-3:2013 SR 4.2

 ISO/IEC 27001:2013 A.8.2.3

 ISO/IEC 27001:2013 A.8.3.1

 ISO/IEC 27001:2013 A.8.3.2

 ISO/IEC 27001:2013 A.8.3.3

 ISO/IEC 27001:2013 A.11.2.7

NIST SP 800-53 Rev. 4 CM-8, MP-6, PE-16

PR.DS-4

可用性を確保するのに十分な容量を保持している。

参考情報

COBIT 5 APO13.01

ISA 62443-3-3:2013 SR 7.1, SR 7.2

 ISO/IEC 27001:2013 A.12.3.1

NIST SP 800-53 Rev. 4 AU-4, CP-2, SC-5

PR.DS-5

データ漏えいに対する保護対策を実施している。

参考情報

CCS CSC 17

COBIT 5 APO01.06

ISA 62443-3-3:2013 SR 5.2

 ISO/IEC 27001:2013 A.6.1.2

 ISO/IEC 27001:2013 A.7.1.1

 ISO/IEC 27001:2013 A.7.1.2

 ISO/IEC 27001:2013 A.7.3.1

 ISO/IEC 27001:2013 A.8.2.2

 ISO/IEC 27001:2013 A.8.2.3

 ISO/IEC 27001:2013 A.9.1.1

 ISO/IEC 27001:2013 A.9.1.2

 ISO/IEC 27001:2013 A.9.2.3

 ISO/IEC 27001:2013 A.9.4.1

 ISO/IEC 27001:2013 A.9.4.4

 ISO/IEC 27001:2013 A.9.4.5

 ISO/IEC 27001:2013 A.13.1.3

 ISO/IEC 27001:2013 A.13.2.1

 ISO/IEC 27001:2013 A.13.2.3

 ISO/IEC 27001:2013 A.13.2.4

 ISO/IEC 27001:2013 A.14.1.2

 ISO/IEC 27001:2013 A.14.1.3

NIST SP 800-53 Rev. 4 AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4

PR.DS-6

ソフトウェア、 ファームウェア、 および情報の完全性の検証に、 完全性チェックメカニズムを使用している。

参考情報

ISA 62443-3-3:2013 SR 3.1, SR 3.3, SR 3.4,SR 3.8

 ISO/IEC 27001:2013 A.12.2.1

 ISO/IEC 27001:2013 A.12.5.1

 ISO/IEC 27001:2013 A.14.1.2

 ISO/IEC 27001:2013 A.14.1.3

NIST SP 800-53 Rev. 4 SI-7

PR.DS-7

開発・テスト環境を実稼働環境から分離している。

参考情報

COBIT 5 BAI07.04

 ISO/IEC 27001:2013 A.12.1.4

NIST SP 800-53 Rev. 4 CM-2

* + - * 1. 情報を保護するためのプロセスおよび手順（PR.IP）

（目的、 範囲、 役割、 責任、 経営コミットメント、 組織間の調整を扱う）セキュリティポリシー、 プロセス、 手順を維持し、 情報システムと資産の保護の管理に使用している。

PR.IP-1

情報技術／産業用制御システムのベースラインとなる設定を定め、 維持している。

参考情報

CCS CSC 3, 10

COBIT 5 BAI10.01, BAI10.02, BAI10.03,BAI10.05

ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3

ISA 62443-3-3:2013 SR 7.6

 ISO/IEC 27001:2013 A.12.1.2

 ISO/IEC 27001:2013 A.12.5.1,

 ISO/IEC 27001:2013 A.12.6.2

 ISO/IEC 27001:2013 A.14.2.2

 ISO/IEC 27001:2013 A.14.2.3

 ISO/IEC 27001:2013 A.14.2.4

NIST SP 800-53 Rev. 4 CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

PR.IP-2

システムを管理するためのシステム開発ライフサイクルを導入している。

参考情報

COBIT 5 APO13.01

ISA 62443-2-1:2009 4.3.4.3.3

 ISO/IEC 27001:2013 A.6.1.5

 ISO/IEC 27001:2013 A.14.1.1

 ISO/IEC 27001:2013 A.14.2.1

 ISO/IEC 27001:2013 A.14.2.5

NIST SP 800-53 Rev. 4 SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8

PR.IP-3

設定変更管理プロセスを導入している。

参考情報

COBIT 5 BAI06.01, BAI01.06

ISA 62443-2-1:2009 4.3.4.3.2, 4.3.4.3.3

ISA 62443-3-3:2013 SR 7.6

 ISO/IEC 27001:2013 A.12.1.2

 ISO/IEC 27001:2013 A.12.5.1

 ISO/IEC 27001:2013 A.12.6.2

 ISO/IEC 27001:2013 A.14.2.2

 ISO/IEC 27001:2013 A.14.2.3

 ISO/IEC 27001:2013 A.14.2.4

NIST SP 800-53 Rev. 4 CM-3, CM-4, SA-10

PR.IP-4

情報のバックアップを定期的に実施、 保持し、 テストしている。

参考情報

COBIT 5 APO13.01

ISA 62443-2-1:2009 4.3.4.3.9

ISA 62443-3-3:2013 SR 7.3, SR 7.4

 ISO/IEC 27001:2013 A.12.3.1

 ISO/IEC 27001:2013 A.17.1.2

 ISO/IEC 27001:2013 A.17.1.3

 ISO/IEC 27001:2013 A.18.1.3

NIST SP 800-53 Rev. 4 CP-4, CP-6, CP-9

PR.IP-5

自組織の資産の物理的な運用環境に関するポリシーと規制を満たしている。

参考情報

COBIT 5 DSS01.04, DSS05.05

ISA 62443-2-1:2009 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6

 ISO/IEC 27001:2013 A.11.1.4

 ISO/IEC 27001:2013 A.11.2.1

 ISO/IEC 27001:2013 A.11.2.2

 ISO/IEC 27001:2013 A.11.2.3

NIST SP 800-53 Rev. 4 PE-10, PE-12, PE-13, PE-14, PE-15, PE-18

PR.IP-6

ポリシーに従ってデータを破壊している。

参考情報

COBIT 5 BAI09.03

ISA 62443-2-1:2009 4.3.4.4.4

ISA 62443-3-3:2013 SR 4.2

 ISO/IEC 27001:2013 A.8.2.3

 ISO/IEC 27001:2013 A.8.3.1

 ISO/IEC 27001:2013 A.8.3.2

 ISO/IEC 27001:2013 A.11.2.7

NIST SP 800-53 Rev. 4 MP-6

PR.IP-7

保護プロセスを継続的に改善している。

参考情報

COBIT 5 APO11.06, DSS04.05

ISA 62443-2-1:2009 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8

NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-8, PL-2, PM-6

PR.IP-8

保護技術の有効性について、 適切なパートナーとの間で情報を共有している。

参考情報

ISO/IEC 27001:2013 A.16.1.6

NIST SP 800-53 Rev. 4 AC-21, CA-7, SI-4

PR.IP-9

対応計画（インシデント対応および事業継続）と復旧計画（インシデントからの復旧および災害復旧）を実施し、 管理している。

参考情報

COBIT 5 DSS04.03

ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1

 ISO/IEC 27001:2013 A.16.1.1

 ISO/IEC 27001:2013 A.17.1.1

 ISO/IEC 27001:2013 A.17.1.2

NIST SP 800-53 Rev. 4 CP-2, IR-8

PR.IP-10

対応計画と復旧計画をテストしている。

参考情報

ISA 62443-2-1:2009 4.3.2.5.7, 4.3.4.5.11

ISA 62443-3-3:2013 SR 3.3

 ISO/IEC 27001:2013 A.17.1.3

NIST SP 800-53 Rev.4 CP-4, IR-3, PM-14

PR.IP-11

人事に関わる対策にサイバーセキュリティ（例：アクセス権限の無効化、 従業員に対する審査）を含めている。

参考情報

COBIT 5 APO07.01, APO07.02, APO07.03, APO07.04, APO07.05

ISA 62443-2-1:2009 4.3.3.2.1, 4.3.3.2.2,　4.3.3.2.3

 ISO/IEC 27001:2013 A.7.1.1

 ISO/IEC 27001:2013 A.7.3.1

 ISO/IEC 27001:2013 A.8.1.4

NIST SP 800-53 Rev. 4 PS Family

PR.IP-12

脆弱性管理計画を作成し、 実施している。

参考情報

 ISO/IEC 27001:2013 A.12.6.1

 ISO/IEC 27001:2013 A.18.2.2

NIST SP 800-53 Rev. 4 RA-3, RA-5, SI-2

* + - * 1. 保守（PR.MA）

産業用制御システムと情報システムのコンポーネントの保守と修理をポリシーと手順に従って実施している。

PR.MA-1

自組織の資産の保守と修理は、 承認・管理されたツールを用いて、 タイムリーに実施し、 ログを記録している。

参考情報

COBIT 5 BAI09.03

ISA 62443-2-1:2009 4.3.3.3.7

 ISO/IEC 27001:2013 A.11.1.2

 ISO/IEC 27001:2013 A.11.2.4

 ISO/IEC 27001:2013 A.11.2.5

NIST SP 800-53 Rev. 4 MA-2, MA-3, MA-5

PR.MA-2

自組織の資産に対する遠隔保守は、 承認を得て、 ログを記録し、 不正アクセスを防げる形で実施している。

参考情報

COBIT 5 DSS05.04

ISA 62443-2-1:2009 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8

 ISO/IEC 27001:2013 A.11.2.4

 ISO/IEC 27001:2013 A.15.1.1

 ISO/IEC 27001:2013 A.15.2.1

NIST SP 800-53 Rev. 4 MA-4

* + - * 1. 保護技術（PR.PT）

関連するポリシー、 手順、 契約に基づいて、 システムと資産のセキュリティと耐性・復旧力を確保するための、 技術的なセキュリティソリューションを管理している。

PR.PT-1

ポリシーに従って監査記録／ログ記録の対象を決定、 文書化し、 そうした記録を実施して、 レビューしている。

参考情報

CCS CSC 14

COBIT 5 APO11.04

ISA 62443-2-1:2009 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4

ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12

 ISO/IEC 27001:2013 A.12.4.1

 ISO/IEC 27001:2013 A.12.4.2

 ISO/IEC 27001:2013 A.12.4.3

 ISO/IEC 27001:2013 A.12.4.4

 ISO/IEC 27001:2013 A.12.7.1

NIST SP 800-53 Rev. 4 AU Family

PR.PT-2

ポリシーに従って取り外し可能な外部記録媒体を保護し、 そうした媒体の使用を制限している。

参考情報

COBIT 5 DSS05.02, APO13.01

ISA 62443-3-3:2013 SR 2.3

 ISO/IEC 27001:2013 A.8.2.2

 ISO/IEC 27001:2013 A.8.2.3

 ISO/IEC 27001:2013 A.8.3.1

 ISO/IEC 27001:2013 A.8.3.3

 ISO/IEC 27001:2013 A.11.2.9

NIST SP 800-53 Rev. 4 MP-2, MP-4, MP-5, MP-7

PR.PT-3

最小機能の原則を取り入れて、 システムと資産に対するアクセスを制御している。

参考情報

COBIT 5 DSS05.02

ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1,　4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4

ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7

 ISO/IEC 27001:2013 A.9.1.2

NIST SP 800-53 Rev. 4 AC-3, CM-7

PR.PT-4

通信ネットワークと制御ネットワークを保護している。

参考情報

CCS CSC 7

COBIT 5 DSS05.02, APO13.01

ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6

 ISO/IEC 27001:2013 A.13.1.1

 ISO/IEC 27001:2013 A.13.2.1

NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7

* + - 1. DE 検知
         1. 異常とイベント（DE.AE）

異常な活動をタイムリーに検知し、 イベントがもたらす可能性のある影響を把握している。

DE.AE-1

ネットワーク運用のベースラインと、 ユーザとシステム間の予測されるデータの流れを特定し、 管理している。

参考情報

COBIT 5 DSS03.01

ISA 62443-2-1:2009 4.4.3.3

NIST SP 800-53 Rev. 4 AC-4, CA-3, CM-2,　SI-4

DE.AE-2

攻撃の標的と手法を理解するために、 検知したイベントを分析している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8

ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2

 ISO/IEC 27001:2013 A.16.1.1

 ISO/IEC 27001:2013 A.16.1.4

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, SI-4

DE.AE-3

イベントデータを複数の情報源やセンサーから収集し、 相互に関連付けている。

参考情報

ISA 62443-3-3:2013 SR 6.1

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, IR-8, SI-4

DE.AE-4

イベントがもたらす影響を特定している。

参考情報

COBIT 5 APO12.06

NIST SP 800-53 Rev. 4 CP-2, IR-4, RA-3, SI-4

DE.AE-5

インシデント警告の閾値を定めている。

参考情報

COBIT 5 APO12.06

ISA 62443-2-1:2009 4.2.3.10

NIST SP 800-53 Rev. 4 IR-4, IR-5, IR-8

* + - * 1. セキュリティの継続的なモニタリング (DE.CM)

サイバーセキュリティイベントを検知し、 保護対策の有効性を検証するために、 情報システムと資産を離散間隔でモニタリングしている。

DE.CM-1

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 ネットワークをモニタリングしている。

参考情報

CCS CSC 14, 16

COBIT 5 DSS05.07

ISA 62443-3-3:2013 SR 6.2

NIST SP 800-53 Rev. 4 AC-2, AU-12, CA-7,CM-3, SC-5, SC-7, SI-4

DE.CM-2

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 物理環境をモニタリングしている。

参考情報

ISA 62443-2-1:2009 4.3.3.3.8

NIST SP 800-53 Rev. 4 CA-7, PE-3, PE-6, PE-20

DE.CM-3

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 個人の活動をモニタリングしている。

参考情報

ISA 62443-3-3:2013 SR 6.2

 ISO/IEC 27001:2013 A.12.4.1

NIST SP 800-53 Rev. 4 AC-2, AU-12, AU-13,CA-7, CM-10, CM-11

DE.CM-4

悪質なコードを検出できる。

参考情報

CCS CSC 5

COBIT 5 DSS05.01

ISA 62443-2-1:2009 4.3.4.3.8

ISA 62443-3-3:2013 SR 3.2

 ISO/IEC 27001:2013 A.12.2.1

NIST SP 800-53 Rev. 4 SI-3

DE.CM-5

悪質なモバイルコードを検出できる。

参考情報

ISA 62443-3-3:2013 SR 2.4

 ISO/IEC 27001:2013 A.12.5.1

NIST SP 800-53 Rev. 4 SC-18, SI-4. SC-44

DE.CM-6

発生する可能性のあるサイバーセキュリティイベントを検知できるよう、 外部サービスプロバイダの活動をモニタリングしている。

参考情報

COBIT 5 APO07.06

 ISO/IEC 27001:2013 A.14.2.7

 ISO/IEC 27001:2013 A.15.2.1

NIST SP 800-53 Rev. 4 CA-7, PS-7, SA-4, SA-9, SI-4

DE.CM-7

権限のない従業員、 接続、 デバイス、 ソフトウェアのモニタリングを実施している。

参考情報

NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3,　CM-8, PE-3, PE-6, PE-20, SI-4

DE.CM-8

脆弱性スキャンを実施している。

参考情報

COBIT 5 BAI03.10

ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7

 ISO/IEC 27001:2013 A.12.6.1

NIST SP 800-53 Rev. 4 RA-5

* + - * 1. 検知プロセス（DE.DP）

異常なイベントをタイムリーに、 かつ正確に検知するための検知プロセスおよび手順を維持し、 テストしている。

DE.DP-1

説明責任を果たせるよう、 検知に関する役割と責任を明確に定義している。

参考情報

CCS CSC 5

COBIT 5 DSS05.01

ISA 62443-2-1:2009 4.4.3.1

 ISO/IEC 27001:2013 A.6.1.1

NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14

DE.DP-2

検知活動は必要なすべての要求事項を満たしている。

参考情報

ISA 62443-2-1:2009 4.4.3.2

 ISO/IEC 27001:2013 A.18.1.4

NIST SP 800-53 Rev. 4 CA-2, CA-7, PM-14, SI-4

DE.DP-3

検知プロセスをテストしている。

参考情報

COBIT 5 APO13.02

ISA 62443-2-1:2009 4.4.3.2

ISA 62443-3-3:2013 SR 3.3

 ISO/IEC 27001:2013 A.14.2.8

NIST SP 800-53 Rev. 4 CA-2, CA-7, PE-3,　PM-14, SI-3, SI-4

DE.DP-4

イベント検知情報を適切な関係者に伝達している。

参考情報

COBIT 5 APO12.06

ISA 62443-2-1:2009 4.3.4.5.9

ISA 62443-3-3:2013 SR 6.1

 ISO/IEC 27001:2013 A.16.1.2

NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7,　RA-5, SI-4

DE.DP-5

検知プロセスを継続的に改善している。

参考情報

COBIT 5 APO11.06, DSS04.05

ISA 62443-2-1:2009 4.4.3.4

 ISO/IEC 27001:2013 A.16.1.6

NIST SP 800-53 Rev. 4, CA-2, CA-7, PL-2,　RA-5, SI-4, PM-14

* + - 1. RS 対応
         1. 対応計画（RS.RP）

検知したサイバーセキュリティイベントにタイムリーに対応できるよう、 対応プロセスおよび手順を実施し、 維持している。

RS.RP-1

イベントの発生中または発生後に対応計画を実施している。

参考情報

COBIT 5 BAI01.10

CCS CSC 18

ISA 62443-2-1:2009 4.3.4.5.1

 ISO/IEC 27001:2013 A.16.1.5

NIST SP 800-53 Rev. 4 CP-2, CP-10, IR-4, IR-8

* + - * 1. 伝達（RS.CO）

法執行機関からの支援を必要に応じて得られるよう、 内外の利害関係者との間で対応活動を調整している。

RS.CO-1

対応が必要になった時の自身の役割と行動の順番を従業員は認識している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4

 ISO/IEC 27001:2013 A.6.1.1

 ISO/IEC 27001:2013 A.16.1.1

NIST SP 800-53 Rev. 4 CP-2, CP-3, IR-3, IR-8

RS.CO-2

定められた基準に沿って、 イベントを報告している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.5

 ISO/IEC 27001:2013 A.6.1.3

 ISO/IEC 27001:2013 A.16.1.2

NIST SP 800-53 Rev. 4 AU-6, IR-6, IR-8

RS.CO-3

対応計画に従って情報を共有している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.2

 ISO/IEC 27001:2013 A.16.1.2

NIST SP 800-53 Rev. 4 CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4

RS.CO-4

対応計画に従って、 利害関係者との間で調整を行っている。

参考情報

ISA 62443-2-1:2009 4.3.4.5.5

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

RS.CO-5

サイバーセキュリティに関する状況認識を深めるために、 外部利害関係者との間で任意の情報共有を行っている。

参考情報

NIST SP 800-53 Rev. 4 PM-15, SI-5

* + - * 1. 分析 (RS.AN)

適切な対応を確実にし、 復旧活動を支援するために、 分析を実施している。

RS.AN-1

検知システムからの通知を調査している。

参考情報

COBIT 5 DSS02.07

ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7,

4.3.4.5.8

ISA 62443-3-3:2013 SR 6.1

 ISO/IEC 27001:2013 A.12.4.1

 ISO/IEC 27001:2013 A.12.4.3

 ISO/IEC 27001:2013 A.16.1.5

NIST SP 800-53 Rev. 4 AU-6, CA-7, IR-4, IR-5, PE-6, SI-4

RS.AN-2

インシデントがもたらす影響を把握している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8

 ISO/IEC 27001:2013 A.16.1.6

NIST SP 800-53 Rev. 4 CP-2, IR-4

RS.AN-3

フォレンジクスを実施している。

参考情報

ISA 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1

 ISO/IEC 27001:2013 A.16.1.7

NIST SP 800-53 Rev. 4 AU-7, IR-4

RS.AN-4

対応計画に従ってインシデントを分類している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.6

 ISO/IEC 27001:2013 A.16.1.4

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-5, IR-8

* + - * 1. 低減（RS.MI）

イベントの拡大を防ぎ、 その影響を緩和し、 インシデントを根絶するための活動を実施している。

RS.MI-1

インシデントを封じ込めている。

参考情報

ISA 62443-2-1:2009 4.3.4.5.6

ISA 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4

 ISO/IEC 27001:2013 A.16.1.5

NIST SP 800-53 Rev. 4 IR-4

RS.MI-2

インシデントを低減している。

参考情報

ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.10

 ISO/IEC 27001:2013 A.12.2.1

 ISO/IEC 27001:2013 A.16.1.5

NIST SP 800-53 Rev. 4 IR-4

RS.MI-3

新たに特定された脆弱性に関して、 許容できるリスクである場合にはその旨を文書化し、 そうでない場合には低減している。

参考情報

 ISO/IEC 27001:2013 A.12.6.1

NIST SP 800-53 Rev. 4 CA-7, RA-3, RA-5

* + - * 1. 改善（RS.IM）

現在と過去の意思決定／対応活動から学んだ教訓を取り入れることで、 自組織の対応活動を改善している。

RS.IM-1

学んだ教訓を対応計画に取り入れている。

参考情報

COBIT 5 BAI01.13

ISA 62443-2-1:2009 4.3.4.5.10, 4.4.3.4

 ISO/IEC 27001:2013 A.16.1.6

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

RS.IM-2

対応戦略を更新している。

参考情報

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

* + - 1. RC 復旧
         1. 復旧計画（RC.RP）

サイバーセキュリティイベントによる影響を受けたシステムや資産をタイムリーに復旧できるよう、 復旧プロセスおよび手順を実施し、 維持している。

RC.RP-1

イベントの発生中または発生後に復旧計画を実施している。

参考情報

CCS CSC 8

COBIT 5 DSS02.05, DSS03.04

 ISO/IEC 27001:2013 A.16.1.5

NIST SP 800-53 Rev. 4 CP-10, IR-4, IR-8

* + - * 1. 改善（RC.IM）

学んだ教訓を将来的な活動に取り入れることで、 復旧計画およびプロセスを改善している。

RC.IM-1

学んだ教訓を復旧計画に取り入れている。

参考情報

COBIT 5 BAI05.07

ISA 62443-2-1:2009 4.4.3.4

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

RC.IM-2

復旧戦略を更新している。

参考情報

COBIT 5 BAI07.08

NIST SP 800-53 Rev. 4 CP-2, IR-4, IR-8

* + - * 1. 伝達（RC.CO）

コーディネーティングセンター、 インターネットサービスプロバイダ、 攻撃システムのオーナー、 被害者、 その他のCSIRT、 ベンダなどの、 内外の関係者との間で復旧活動を調整している。

RC.CO-1

広報活動を管理している。

参考情報

COBIT 5 EDM03.02

RC.CO-2

イベント発生後に評判を回復している。

参考情報

COBIT 5 MEA03.02

RC.CO-3

復旧活動について内部利害関係者と役員、 そして経営陣に伝達している。

参考情報

NIST SP 800-53 Rev. 4 CP-2, IR-4

* 1. NIST SP 800-37 (連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド： セキュリティライフサイクルによるアプローチ)
     1. 連邦政府情報システムに対するリスクマネジメントフレームワーク適用ガイド： セキュリティライフサイクルによるアプローチ

ドキュメントを参照: [000025329.pdf](https://www.ipa.go.jp/files/000025329.pdf)

* + 1. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
    2. 第1章 はじめに
       1. 情報セキュリティの必要性とリスクを管理する必要性
          1. 公共および民間部門の情報システムに対する攻撃（複数）が成功した場合、 米国の国家安全上の利益および経済安全上の利益に深刻な、 または重大な被害が及ぶ可能性がある。 これらの脅威の危険性が重大であり、 かつ増大していることから、 組織内のあらゆる階層のリーダーが、 適切な情報セキュリティの確保、 および情報システム関連のセキュリティリスク8の管理における自身の責務を理解することが必要不可欠になる。
       2. 1.1 背景
          1. RMF（Risk Management Framework：リスクマネジメントフレームワーク）

堅牢で継続的監視プロセスの実施により、 リアルタイムに近いリスクマネジメントおよび情報システムの継続的な運用認可の概念を促進する。

主要な任務および業務上の機能をサポートする情報システムに関して、 費用対効果の高い、 リスクベースの意思決定を行うのに必要な情報をシニアリーダー提供するための、 オートメーション（automation）の利用を促進する。

エンタープライズアーキテクチャおよびシステム開発ライフサイクルに情報セキュリティを組み入れる。

セキュリティ管理策の選択、 実施、 アセスメント、 および監視、 ならびに情報システムの運用認可に重点を置く。

リスクエグゼクティブ（機能）を通じて、 情報システムレベルのリスクマネジメントプロセスを、 組織レベルのリスクマネジメントプロセスにリンクする

組織の情報システムに導入され、 それらのシステムによって継承されるセキュリティ管理策（すなわち、 共通管理策）に対する責任と説明責任を定める。

* + - 1. 1.2 目的および適用性
         1. 情報システム関連のセキュリティリスクの管理を、 組織の任務／業務上の目的、 およびリスクエグゼクティブ（機能）を通じてシニアリーダーが定めた全般的なリスク戦略に確実に適合させる。
         2. 必要なセキュリティ管理策を含む情報セキュリティ要求事項を、 組織のエンタープライズアーキテクチャおよびシステム開発ライフサイクルに確実に組み入れる。
         3. （継続的な監視を通じて）一貫性のある、 十分な情報に基づいた、 継続的なセキュリティ運用認可判断を支援すると同時に、 セキュリティおよびリスクマネジメント関連の情報の透明性、 ならびに互恵契約（reciprocity）11を支援する。
         4. 適切なリスク軽減戦略の実施により、 連邦政府内の情報および情報システムのセキュリティを向上させる。
         5. 本ガイドラインは、 国家安全保障にかかわるシステムに対する同様のガイドラインについても補足を行えるように、 技術的な観点から広範囲にわたって作成されたものであり、 そのようなシステムに対する政策権限を行使する適切な連邦政府職員による承認があれば、 そのようなシステムに適用することができる。
         6. 州政府、 地方政府、 および隊組織はもとより、 民間部門の組織においても、 必要に応じて本ガイドラインの使用を検討することが推奨される。
      2. 1.3 対象となる読者
         1. 任務／業務上のオーナーシップに責任を持つ者、 または、 受託者責任を持つ者（例：連邦政府機関の長、 最高経営責任者、 最高財務責任者）
         2. 情報システムの開発および統合に責任を持つ者（例：プログラムマネージャ、 IT製品の開発者、 情報システムの開発者、 情報システムのインテグレータ、 エンタープライズアーキテクト、 情報セキュリティアーキテクト）
         3. 情報システムおよび／またはセキュリティの管理／監督に責任を持つ者（例：シニアリーダー、 リスクエグゼクティブ、 運用認可責任者、 最高情報責任者、 上級情報セキュリティ責任者
         4. 情報システムおよびセキュリティ管理策のアセスメントおよび監視に責任を持つ者（例：システム評価者、 アセサー／アセスメントチーム、 検証および有効性確認を行う第三者アセサー、 監査官、 または情報システムのオーナー）
         5. 情報セキュリティの導入および運用に責任を持つ者（例：情報システムのオーナー、 共通管理策のプロバイダ、 情報のオーナー／スチュワード、 任務／業務のオーナー、 情報セキュリティアーキテクト、 情報システムセキュリティエンジニア／責任者）。
      3. 1.4 本文書の構成
         1. 第2章では、

情報システム関連のセキュリティリスクの管理に関連する基本概念を説明する。 内容には次のようなものが含まれる。 (i) リスクマネジメントに対する組織全体としての見解、 およびリスクマネジメントフレームワークの適用(ii) システム開発ライフサイクルへの情報セキュリティ要求事項の組み入れ(iii) 情報システム境界の確立、 および(iv) システム固有の管理策、 ハイブリッド管理策、 または共通管理策として分類されたセキュリティ管理策の、 情報システムへの割り当て。

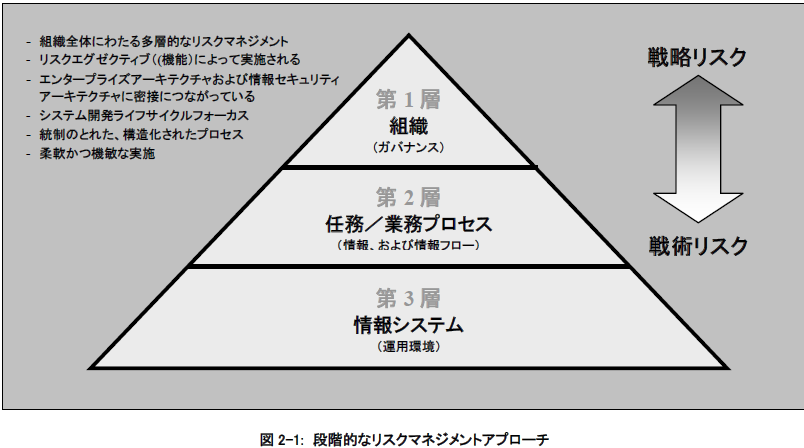
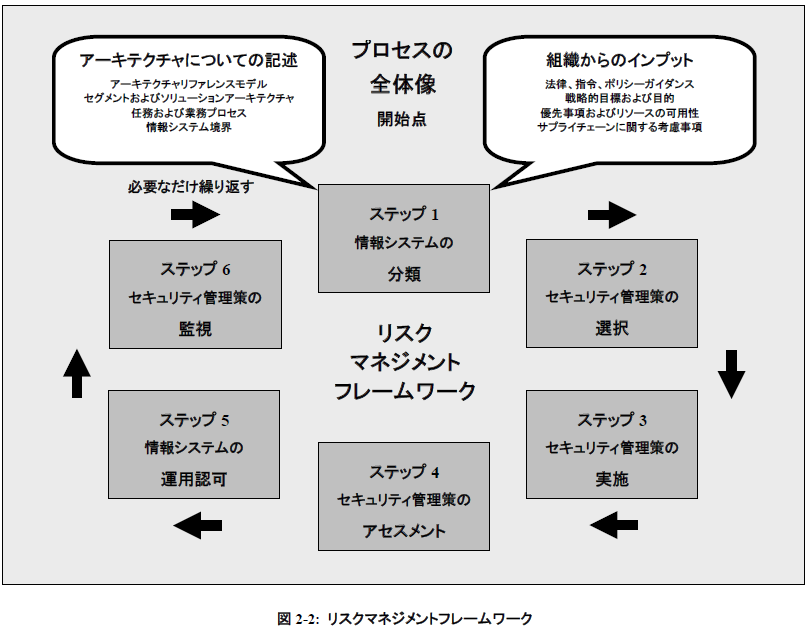
* + - * 1. 第3章では、

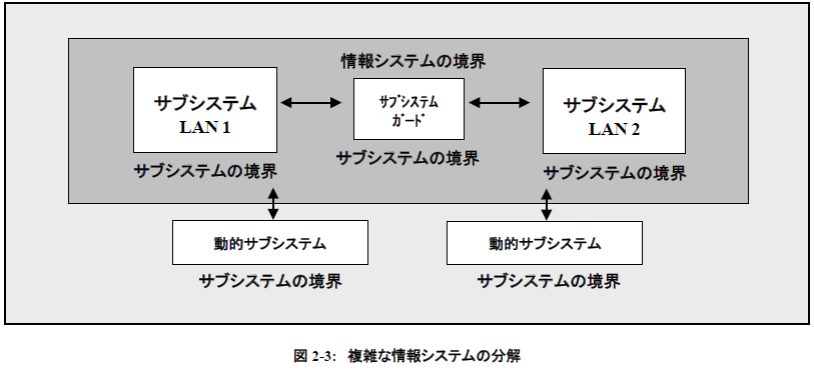
リスクマネジメントフレームワークを情報システムに適用するのに必要なタスクについて記述する。 内容には次のようなものが含まれる。 (i) 情報および情報システムの分類(ii) セキュリティ管理策の選択(iii) セキュリティ管理策の導入(iv) セキュリティ管理策の有効性のアセスメント(v) 情報システムの運用認可、 および(vi) セキュリティ管理策、 および情報システムのセキュリティ状態の継続的な監視。

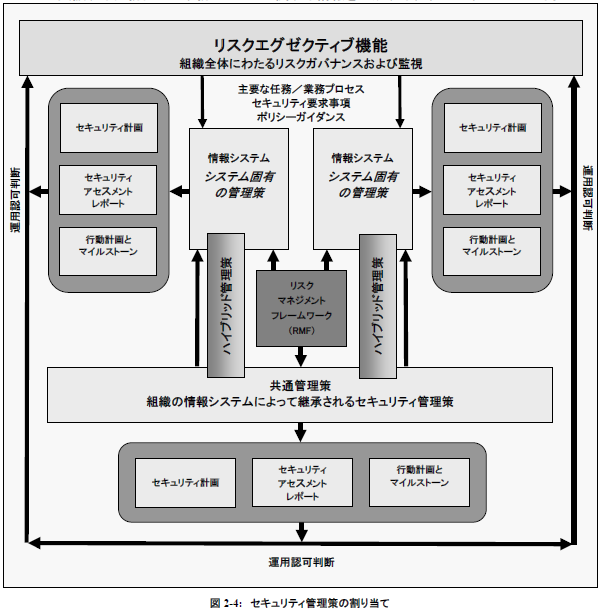
* + - * 1. （補足）付録 では、

リスクマネジメントフレームワークの情報システムへの適用に関する追加情報を提供する。 内容には次のようなものが含まれる。

(i) 参考文献(ii) 用語集(iii) 略語(iv) 役割と責任(v) RMFタスクの要約(vi) 情報システムのセキュリティ運用認可(vii) 情報システムのセキュリティ状態の監視(viii) 運用上のシナリオ(ix) 外部環境におけるセキュリティ管理策。

* + 1. 第2章 基本項目
       1. 2.1 統合された組織全体にわたるマネジメント
          1. Subtopic  
             
          2. Subtopic  
             
       2. 2.2 システム開発ライフサイクル
       3. 2.3 情報システム境界
          1. 2.3.1 情報システムの境界の設定
          2. 2.3.2 複雑な情報システムの境界

Subtopic  


* + - * 1. 2.3.3 技術の変化および情報システム境界への影響
      1. 2.4 セキュリティ管理策の割り当て
         1. Subtopic  
            
    1. 第3章 プロセス
       1. リスクマネジメントフレームワークの適用
          1. リスクマネジメントフレームワークおよび関連するRMFタスクは、 情報システムのオーナーと共通管理策の提供者の両方に適用される。 情報システムの運用認可を支援するのに加えて、 RMFタスクは、 組織の情報システムが継承する共通管理策の選択、 開発、 実施、 アセスメント、 運用認可、 および継続的な監視を支援する。 共通管理策の提供者（組織にとって内部・外部の両方）によるRMFタスクの実施により、 共通管理策によって提供されるセキュリティ機能が、 情報の保護に関する彼らのニーズに適した保証レベルで、 情報システムオーナーによって継承される。 このアプローチでは、 情報システムおよび、 それらのシステムを支援するインフラに導入されるセキュリティ管理策の有効性の重要性を認識している。
          2. RMFの各タスクは、 シーケンシャルに記述されているが、 組織は、 組織が確立したマネジメントおよびシステム開発ライフサイクルプロセスに適合させるために、 あるいは、 タスクの実施に関して、 より費用対効果が高く効率的なソリューションを実現するために、 シーケンシャルな構造からの逸脱を選択してもよい。 タスクの順序付けがどうなっているかにかかわらず、 情報システムの運用を開始する前に実施すべき最後のステップは、 運用認可責任者がリスクを明示的に受容することである。 組織は、 RMFの特定のタスクを反復する形で実施したり、 システム開発ライフサイクルの異なるフェーズにおいて実施することもできる。 たとえば、 セキュリティ管理策アセスメントは、 システム開発時、 システム導入時、 およびシステム運用／保守時（継続的な監視の一環として）に実施される可能性がある。
          3. 組織は、 組織内の選択されたプロセスおよび活動の熟成度に基づいて、 RMFの特定のタスクに対しては、 大きな労力をかけて、 残りのタスクに対しては、 より少ないリソースを割り当ててもよい。 RMFは、 ライフサイクルをベースしているため、 情報システムやその運用環境に対する変更を組織がどのように管理するかによっては、 時間の経過とともに多くのタスクを再訪する必要性が生じる。 情報システムに対する情報セキュリティ関連リスクの管理は、 シニアリーダーが実施する、 組織全体にわたる大規模のリスクマネジメント活動の一部とみなされている。 RMFによって、 情報システムの運用および使用により生じるリスクを軽減するための統制のとれた構造化されたアプローチと、 極めて動的な運用環境において組織の主要な任務および業務を支援するのに必要な柔軟性と機敏さとの、 両方が同時に提供されなければならない。
       2. 3.1 RMFステップ1-情報システムの分類
          1. タスク1-1 セキュリティ分類

情報システムを分類し、 セキュリティ分類の結果をセキュリティ計画に記載する。

* + - * 1. タスク1-2 情報システムに関する記述

情報システム（システム境界を含む）について説明し、 その内容をセキュリティ計画に記載する。

* + - * 1. タスク1-3 情報システムの登録

組織内の適切な計画局／管理局に情報システムを登録する。

* + - 1. 3.2 RMF ステップ 2-セキュリティ管理策の選択
         1. タスク2-1 共通管理策の明確化

組織の情報システムに対する共通管理策として組織が提供しているセキュリティ管理策を明確にし、 セキュリティ計画（またはそれと同等の文書）に記載する。

* + - * 1. タスク2-2 セキュリティ管理策の選択

情報システムに導入するセキュリティ管理策を選択し、 それらの管理策について、 セキュリティ計画に記載する。

* + - * 1. タスク2-3 監視戦略

セキュリティ管理策の有効性、 ならびに、 情報システムおよびシステムの運用環境に対して提案されている、 あるいは、 実際に実施された変更を、 継続的に監視するための、 戦略を策定する。

* + - * 1. タスク2-4 セキュリティ計画の承認

セキュリティ計画をレビューし、 承認する。

* + - 1. 3.3 RMF ステップ 3-セキュリティ管理策の実施
         1. タスク3-1 セキュリティ管理策の実施

セキュリティ計画に記載されているセキュリティ管理策を実施する。

* + - * 1. タスク3-2 セキュリティ管理策の文書化

必要に応じて、 セキュリティ管理策の実施について、 機能面での記述（予定しているインプット、 予想される挙動、 および予想されるアウトプットを含む）と併せて、 セキュリティ計画に記載する。

* + - 1. 3.4 RMF ステップ 4-セキュリティ管理策のアセスメント
         1. タスク4-1 アセスメントの準備

セキュリティ管理策のアセスメント計画を策定、 レビューし、 承認する。

* + - * 1. タスク4-2 セキュリティ管理策のアセスメント

セキュリティアセスメント計画に記載されているアセスメント手順に従ってセキュリティ管理策をアセスメントする。

* + - * 1. タスク4-3 セキュリティアセスメントレポート

セキュリティ管理策のアセスメントを通じて発見された問題、 導かれた結論および推奨事項を文書化した、 セキュリティアセスメントレポートを用意する。

* + - * 1. タスク4-4 是正活動

セキュリティアセスメントレポートに記載されている結論と推奨事項に基づいて、 セキュリティ管理策に対する初期の是正活動を実施し、 是正された管理策（複数）を適宜、 再アセスメントする。

* + - 1. 3.5 RMF ステップ 5-情報システムの運用認可
         1. タスク5-1 行動計画とマイルストーン

セキュリティアセスメントレポートに記載されている結論と推奨事項に基づいて、 行動計画とマイルストーンを作成する（ただし、 既に実施されたすべての是正活動を除く）。

* + - * 1. タスク5-2 セキュリティ運用認可パッケージ

セキュリティ運用認可パッケージをまとめて、 運用認可責任者に提出し、 裁定を仰ぐ。

* + - * 1. タスク5-3 リスクの判断

組織の業務（任務、 機能、 イメージ、 または評判を含む）、 組織の資産、 個人、 他の組織、 または国家に対するリスクを判断する。

* + - * 1. タスク5-4 リスクの受容

組織の業務、 組織の資産、 個人、 他の組織、 または国家に対するリスクが受容できるかどうかを判断する。

* + - 1. 3.6 RMF ステップ 6-セキュリティ管理策の監視
         1. タスク6-1 情報システムやその運用環境に対する変更

情報システムおよびシステムの運用環境に対して提案されている、 あるいは、 実際に実施された変更がもたらすセキュリティへの影響を判断する。

* + - * 1. タスク6-2 継続的なセキュリティ管理策アセスメント

組織が定めた監視戦略に従って、 情報システムに導入される、 または情報システムによって継承される技術面、 管理面、 および運用面でのセキュリティ管理策の中から選択された管理策のサブセットをアセスメントする。

* + - * 1. タスク6-3 継続的な是正活動

継続的監視活動の結果、 リスクアセスメント結果、 および行動計画とマイルストーンにリストアップされている重要な項目に基づいて是正活動を実施する。

* + - * 1. タスク6-4 重要な更新

継続的監視プロセスの結果に基づいて、 セキュリティ計画、 セキュリティアセスメントレポート、 および行動計画とマイルストーンを更新する。

* + - * 1. タスク6-5 セキュリティ状況の報告

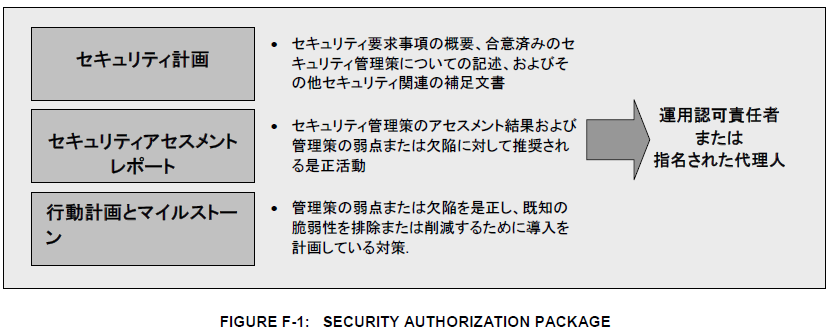
監視戦略に従って、 継続的に、 情報システムのセキュリティ状況（情報システムに導入されるセキュリティ管理策、 および情報システムによって継承されるセキュリティ管理策の有効性を含む）を運用認可責任者および組織内の他の適切な職員に報告する。

* + - * 1. タスク6-6 継続的なリスク判断および受容

監視戦略に従って、 情報システムのセキュリティ状況に関する報告内容（情報システムに導入される、 または情報システムによって継承されるセキュリティ管理策の有効性を含む）を継続的に見直すことによって、 組織の業務、 組織の資産、 個人、 他の組織、 または国家に対するリスクが、 ひきつづき受容可能か否かを判断する

* + - * 1. タスク6-7 情報システムの切り離しおよび廃止

必要に応じて、 情報システムの廃止戦略を実施する。 この戦略は、 システムがサービスから切り離された時に必要となる活動を実施するためのものである。

* + 1. 付録 A 参考文献
    2. 付録B 用語集
    3. 付録C 略語
    4. 付録D 役割と責任
       1. D.1 政府機関の長（最高経営責任者） （HEAD OF AGENCY （CHIEF EXECUTIVE OFFICER））
       2. D.2 リスクエグゼクティブ（機能） （RISK EXECUTIVE （FUNCTION））
       3. D.3 最高情報責任者（CHIEF INFORMATION OFFICER）
       4. D.4 情報のオーナー／スチュワード（INFORMATION OWNER/STEWARD）
       5. D.5 上級情報セキュリティ責任者（SENIOR INFORMATION SECURITY OFFICER）
       6. D.6 運用認可責任者（AUTHORIZING OFFICIAL）
       7. D.7 運用認可責任者が指名する代理人（AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE）
       8. D.8 共通管理策の提供者（COMMON CONTROL PROVIDER）
       9. D.9 情報システムのオーナー（INFORMATION SYSTEM OWNER）
       10. D.10 情報システムセキュリティ責任者（INFORMATION SYSTEM SECURITY OFFICER）
       11. D.11 情報セキュリティアーキテクト（INFORMATION SECURITY ARCHITECT）
       12. D.12 情報システムセキュリティエンジニア（INFORMATION SYSTEM SECURITY ENGINEER）
       13. D.13 セキュリティ管理策アセサー（SECURITY CONTROL ASSESSOR）
    5. 付録E RMFの各タスクの要約
    6. 付録F セキュリティ運用認可
       1. F.1 運用認可パッケージ（AUTHORIZATION PACKAGE）
          1. セキュリティ計画
          2. セキュリティアセスメントレポート
          3. 行動計画とマイルストーン
          4. 情報システムのセキュリティ分類
          5. セキュリティ管理策の具体的な弱点または欠陥
          6. セキュリティ管理策において特定された弱点または欠陥の重大性（すなわち、 それらの弱点または欠陥が、 情報システムの全体的なセキュリティ状態、 ならびに、 組織のリスクへの暴露65に及ぼす直接的／間接的な影響）
          7. 提案されている、 セキュリティ管理策に関して特定された弱点または欠陥に対処するためのリスク軽減アプローチ（たとえば、 リスク軽減活動の優先順位付け、 リスク軽減に必要なリソースの割り当て）、 および
          8. セキュリティ管理策の弱点または欠陥の一部の受容に関する組織の根拠。
          9. Subtopic  
             
       2. F.2 運用認可判断（AUTHORIZATION DECISIONS）
          1. 運用の認可
          2. 運用の不許可
       3. F.3 運用認可の判断文書（AUTHORIZATION DECISION DOCUMENT）
          1. 運用認可の判断
          2. 運用認可のための諸条件
          3. 運用認可の満了日
          4. リスクエグゼクティブ（機能）から得られる情報（提供される場合）
       4. F.4 継続的な運用認可（ONGOING AUTHORIZATION）
       5. F.5 タイプ運用認可（TYPE AUTHORIZATION）
       6. F.6 運用認可アプローチ（AUTHORIZATION APPROACHES）
    7. 付録G 継続的な監視
       1. G.1 監視戦略（MONITORING STRATEGY）
       2. G.2 監視すべきセキュリティ管理策の選択（SELECTION OF SECURITY CONTROLS FOR MONITORING）
       3. G.3 主要ドキュメントの更新および状況報告（KEY DOCUMENT UPDATES AND STATUS REPORTING）
    8. 付録H 運用上のシナリオ
    9. 付録I 外部環境におけるセキュリティ管理策
  1. NIST SP 800-53 (連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策)
     1. 連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策

ドキュメントを参照: [000056415.pdf](https://www.ipa.go.jp/files/000056415.pdf)

* + 1. NIST SP 800-53 Rev. 4: NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, 2013 年 4 月（2014 年 1 月 15 日時点での更新内容を含む）.
    2. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

ドキュメントを参照: [NIST.SP.800-53r4.](http://dx.doi.org/10.6028/NIST.SP.800-53r4.)

* + 1. 第1 章はじめに
       1. 1.1 目的および適用範囲
       2. 1.2 対象と想定する読者
       3. 1.3 セキュリティ管理策に関する他の発行文書との関係
       4. 1.4 組織の責任
       5. 1.5 本文書の構成
    2. 第2 章基本事項
       1. 2.1 多層から成るリスクマネジメント
       2. 2.2 セキュリティ管理策の構造
       3. 2.3 セキュリティ管理策ベースライン
       4. 2.4 セキュリティ管理策の指定方法
       5. 2.5 外部サービスプロバイダ
       6. 2.6 保証と信用
       7. 2.7 改訂と拡張
    3. 第3 章プロセス
       1. 3.1 管理策ベースラインを選択する
       2. 3.2 ベースラインセキュリティ管理策を調整する
       3. 3.3 オーバーレイを作成する
       4. 3.4 管理策の選択プロセスを文書化する
       5. 3.5 新規に開発するシステムとレガシーシステム
    4. 付録 A 参考文献
    5. 付録 B 用語集
    6. 付録 C 略語
    7. 付録 D セキュリティ管理策ベースラインの要約
    8. 付録 E 保証と信用性
    9. 付録 F セキュリティ管理策カタログ
    10. 付録 G 情報セキュリティプログラム
    11. 付録 H 国政情報セキュリティ標準
    12. 付録 I オーバーレイテンプレート
    13. 付録 J プライバシー管理策カタログ
  1. NIST SP 800-61 (コンピュータセキュリティインシデント対応ガイド)
     1. コンピュータセキュリティインシデント対応ガイドSP800-61 rev.1翻訳版【2008年03月NIST】

ドキュメントを参照: [000025341.pdf](https://www.ipa.go.jp/files/000025341.pdf)

* + 1. 要旨
       1. 1. はじめに
          1. 1.1. 権限
          2. 1.2. 目的および適用範囲

本書は、 事件に効果的かつ効率的に対応するための実用的な手引きとなることで、 各組織が情報セキュリティインシデントによるリスクを軽減するのに役立てることを意図したものである。

* + - * 1. 1.3. 対象とする読者

CSIRT、 システム管理者とネットワーク管理者、 セキュリティスタッフ、 技術サポートスタッフ、 最高情 報責任者(CIO)、 コンピュータセキュリティプログラムマネージャ向け

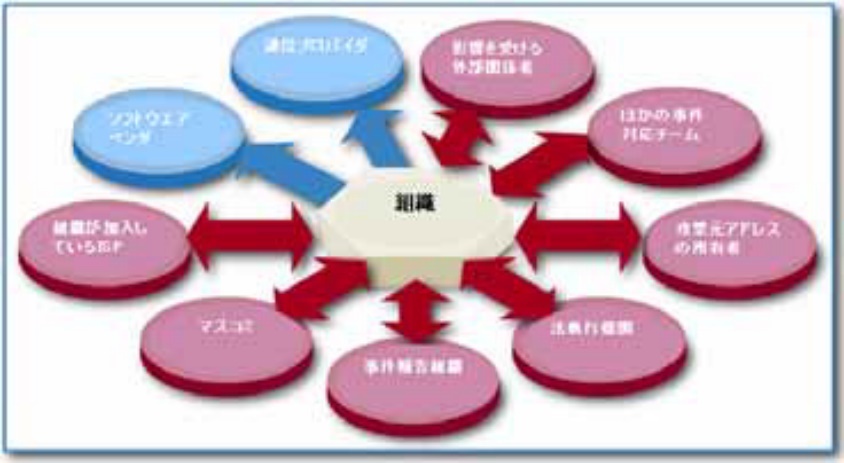
* + - * 1. 1.4. ドキュメントの構成
      1. 2. コンピュータセキュリティインシデント対応能力の組織化
         1. 2.1. 事象と事件
         2. 2.2. インシデント対応の必要性
         3. 2.3. インシデント対応のポリシー、 計画および手順の作成

2.3.1. ポリシーの要素

2.3.2. 計画の要素

2.3.3. 手順の要素

2.3.4. 外部の関係者との情報共有

Subtopic  


* + - * 1. 2.4. インシデント対応チームの構成

2.4.1. チームのモデル

2.4.2. チームモデルの選択

2.4.3. インシデント対応要員

2.4.4. 組織内の依存関係

* + - * 1. 2.5. インシデント対応チームのサービス
        2. 2.6. 推奨事項
      1. 3. 事件処理
         1. Subtopic  
            
         2. 3.1. 準備

3.1.1. 事件処理に備える

3.1.2. 事件の予防

* + - * 1. 3.2. 検知と分析

3.2.1. 事件の分類

3.2.2. 事件の兆候

3.2.3. 前兆と兆候のソース

3.2.4. 事件の分析

3.2.5. 事件の文書化

3.2.6. 事件の優先順位付け

3.2.7. 事件の通知

* + - * 1. 3.3. 封じ込め、 根絶、 復旧

3.3.1. 封じ込め戦略の選択

3.3.2. 証拠の収集と処理

3.3.3. アタッカーの特定

3.3.4. 根絶と復旧

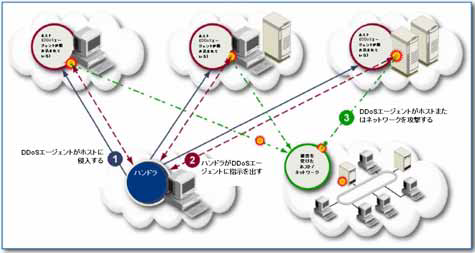
* + - * 1. 3.4. 事件後の対応

3.4.1. 教訓

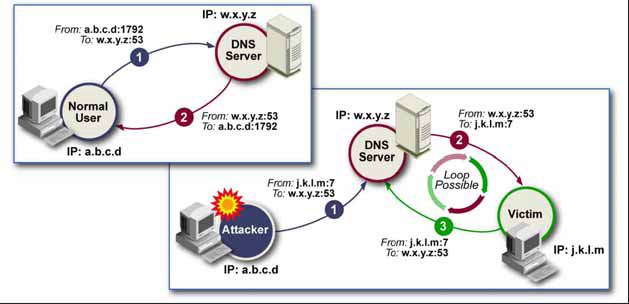
3.4.2. 収集された事件データの利用

3.4.3. 証拠の保管

* + - * 1. 3.5. 事件処理のチェックリスト
        2. 3.6. 推奨事項
      1. 4. サービス不能事件の処理
         1. 4.1. 事件の定義と例

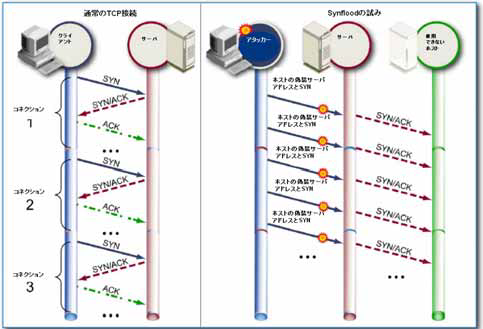
Subtopic  


4.1.1. リフレクタ攻撃

Subtopic  


4.1.2. アンプ(amplifier)攻撃

4.1.3. Flood攻撃

Subtopic  


* + - * 1. 4.2. 準備

4.2.1. 事件処理の準備

4.2.2. 事件の予防

* + - * 1. 4.3. 検知と分析
        2. 4.4. 封じ込め、 根絶、 復旧

4.4.1. 封じ込め戦略の選択

4.4.2. 証拠の収集と処理

* + - * 1. 4.5. サービス不能事件の処理のためのチェックリスト
        2. 4.6. 推奨事項
      1. 5. 悪意のコードによる事件の処理
         1. 5.1. 事件の定義と例

5.1.1. ウイルス

5.1.2. ワーム

5.1.3. トロイの木馬

5.1.4. 悪意のあるモバイルコード

5.1.5. 混合攻撃

5.1.6. 追跡クッキー

5.1.7. 攻撃ツール

5.1.8. マルウェア以外の脅威

* + - * 1. 5.2. 準備

5.2.1. 事件処理の準備

5.2.2. 事件の予防

* + - * 1. 5.3. 検知と分析
        2. 5.4. 封じ込め、 根絶、 復旧

5.4.1. 封じ込め戦略の選択

5.4.2. 証拠の収集と処理

5.4.3. 根絶と復旧

* + - * 1. 5.5. 悪意のコードによる事件の処理のためのチェックリスト
        2. 5.6. 推奨事項
      1. 6. 不正アクセス事件の処理
         1. 6.1. 事件の定義と例
         2. 6.2. 準備

6.2.1. 事件処理の準備

6.2.2. 事件の予防

* + - * 1. 6.3. 検知と分析
        2. 6.4. 封じ込め、 根絶、 復旧

6.4.1. 封じ込め戦略の選択

6.4.2. 証拠の収集と処理

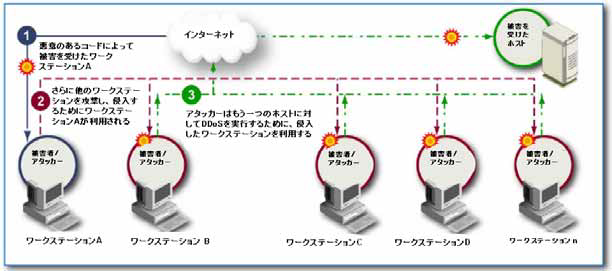
6.4.3. 根絶と復旧

* + - * 1. 6.5. 不正アクセス事件を処理するためのチェックリスト
        2. 6.6. 推奨事項
      1. 7. 不適切な使用による事件の処理
         1. 7.1. 事件の定義と例
         2. 7.2. 準備

7.2.1. 事件処理の準備

7.2.2. 事件の予防

* + - * 1. 7.3. 検知と分析
        2. 7.4. 封じ込め、 根絶、 復旧
        3. 7.5. 不適切な使用の事件を処理するためのチェックリスト
        4. 7.6. 推奨事項
      1. 8. 複合要素の事件の処理
         1. 8.1. 事件の定義と例

Subtopic  


* + - * 1. 8.2. 準備、 検知、 分析
        2. 8.3. 封じ込め、 根絶、 復旧
        3. 8.4. 複合要素の事件を処理するためのチェックリスト
        4. 8.5. 推奨事項
    1. 付録
       1. 付録 A 推奨事項
          1. A.1 コンピュータセキュリティインシデント対応能力の組織化

A.1.1 インシデント対応ポリシー、 計画、 および手順の作成

+ インシデント対応ポリシーを作成する

+ インシデント対応ポリシーをもとに、 インシデント対応計画を作成する

+ インシデント対応手順を作成する

+ 事件関連の情報共有に関するポリシーと手順を確立する

+ 適切な事件報告組織に、 事件についての関係情報を提供する

A.1.2 インシデント対応チームの構成とサービス

+ インシデント対応チームモデルを選ぶ際には、 関係する要因を検討すること

+ インシデント対応チームには適切なスキルをもった人間を選ぶこと

+ 事件処理に参加してもらう必要がある、 組織内のほかのグループを明確にする

+ チームが提供するサービスを決める

* + - * 1. A.2 準備

+ 事件処理で利用できそうなツールとリソースを入手する

+ ネットワーク、 システム、 アプリケーションを十分に安全な状態に保つことで、 事件の発生を予防する

A.2.1 サービス不能事件

+ ファイアウォールルールセットを設定して、 リフレクタ攻撃を予防する

+ 境界ルーターを設定してアンプ攻撃を防ぐ

+ 組織のインターネットサービスプロバイダ(ISP)や二次プロバイダから、 ネットワークベースのDoS攻撃の処理において、 どういった支援が得られるのかを確認する

+ セキュリティソフトウェアを設定し、 DoS攻撃を検知する

+ ネットワーク境界で、 明示的に許可されていないすべての送受信トラフィックを拒否するように設定する

A.2.2 悪意のコードの事件

+ 悪意のコードの問題について、 ユーザに自覚させる

+ ウイルス対策ソフトウェアベンダーの広報を読む

+ 重要なホストには、 ホスト型のIDPS(ファイル完全性チェッカーを含む)を配備する

+ ウイルス対策ソフトウェアを使用し、 最新のウイルスシグネチャを使って最新に保つ

+ 疑いのあるファイルをブロックするようにソフトウェアを設定する

+ 開かれているWindowsの共有を解除する

A.2.3 不正アクセス事件

+ 侵入検知ソフトウェアを設定して、 不正なアクセスを取得しようという試みに対して警報を発生する

+ すべてのホストに対して、 ログの一元化のための設定を行う

+ 全ユーザにパスワードを変更させるための手順を確立する

+ ネットワーク境界で、 明示的に許可されていないすべての受信トラフィックを拒否するように設定する

+ モデムや仮想プライベートネットワーク(VPN)を含むすべてのリモートアクセス手段のセキュリティを高める

+ 公にアクセスできるサービスは、 安全な非武装地帯(DMZ)ネットワークセグメントに置く

+ ホスト上で不必要なサービスはすべて無効にし、 重要なサービスは分離する

+ ホストベースのファイアウォールソフトウェアまたはパーソナルファイアウォールを使用して、 各ホストが攻撃にさらされないようにする

+ パスワードポリシーの作成と実施

A.2.4 不適切な使用の事件

+ 不適切な使用の事件の処理について、 組織の人事部および法務部と話し合う

+ 責任問題について組織の法務部と話し合う

+ 特定の種類の不適切な使用を検知するように侵入検知ソフトウェアを設定する

+ ユーザの活動に関する基本的な情報をログに記録する

+ すべての電子メールサーバを、 不正なメール中継で利用できないように設定する

+ すべての電子メールサーバでスパムフィルタリングを実行する

+ URLフィルタリングソフトウェアを実行する

A.2.5 複合要素の事件

+ 一元化したログとイベント相関処理ソフトウェアを使用する

* + - * 1. A.3 検知と分析

+ いくつもの種類のセキュリティソフトウェアが生成した警報を使って、 前兆や兆候を見つける

+ 外部の者が事件を報告する仕組みを確立する

+ 全システムにログと監査の基準レベルを義務付け、 重要なシステムではより高い基準レベルを義務付ける

+ ネットワークとシステムのプロファイル

+ ネットワーク、 システム、 アプリケーションの正常な動作を理解する

+ 一元化されたログ取得とログ保管ポリシーの作成

+ イベント相関処理の実施

+ すべてのホストの時刻を同期させておく

+ 情報の知識ベースの維持と利用

+ 経験が少ないスタッフのための診断マトリックスの作成

+ 事件が起きた疑いがある場合には、 すぐに全情報の記録を開始する

+ 事件データの保護

+ 影響のあるリソースの重要性や事件の技術的な影響に基づき、 ビジネスインパクトごとに事件に優先順位を付ける

+ 組織のインシデント対応ポリシーの中に、 事件報告に関する項目を盛り込む

* + - * 1. A.4 封じ込め、 根絶、 復旧

+ 事件を封じ込めるための戦略と手順の確立

+ 証拠収集と処理のための、 確立された手順に従うこと

+ 揮発性データを証拠としてシステムから取得する

+ ファイルシステムのバックアップではなく、 完全なフォレンジックディスクイメージを使って、 システムのスナップショットを取得する

A.4.1 サービス不能事件

+ いくつかの対策を順に並べた封じ込め戦略を作成する

A.4.2 悪意のコードの事件

+ 悪意のコードによる事件は、 できるだけ早く封じ込める

A.4.3 不正アクセス事件

+ 変更管理情報をインシデント対応チームに提供する

+ リスク軽減とサービス維持のバランスを考えた封じ込め戦略を選択する

+ rootが奪取されたと思われるシステムはリストアまたは再インストールする

A.4.4 複合要素の事件

+ 最初の事件を封じ込めてから、 事件のほかの要素の兆候を探す

* + - * 1. A.5 事後活動

+ 大きな事件の後には反省会を開催する

A.5.1 不正アクセス事件

+ 事件の各要素の処理に個別に優先順位を付ける

* + - 1. 付録 B 事件処理のシナリオ
         1. B.1 シナリオの質問

準備:

1. あなたの組織では、 この活動を事件とみなしますか? もしそうなら、 この活動は、 組織のどのポリシーに違反していますか? (セクション2.1)

2. この種のインシデントの発生を防止し、 その影響を限定するために、 どのような措置を講じていますか？(セクション3.1.2)

検知と分析:

1. あなたの組織では、 インシデントのどんな前兆（あれば）を検知しますか？前兆があった場合、 あなたの組織はインシデントが起きる前に行動を起こそうとしますか？ (セクション3.2.2、 3.2.3)

2. あなたの組織では、 インシデントのどんな兆候を検知しますか？どの兆候があったらインシデントが起きた可能性があると考えますか？ (セクション3.2.2、 3.2.3)

3. インシデント対応チームは、 どうやってこのインシデントを分析し検証しますか？ (セクション3.2.4)

4. チームはこのインシデントを、 組織内のだれに／どのグループに報告しますか？ (セクション3.2.7)

5. インシデント対応チームは、 どのようにしてこのインシデントの対応に優先順位をつけますか？ (セクション3.2.6)

封じ込め、 根絶、 復旧:

1. このインシデントを封じ込めるために、 あなたの組織はどんな方策を採用しますか？この方策がほかよりも望ましいのはなぜですか？ (セクション3.3.1)

2. インシデントを封じ込めないと、 何が起きる可能性がありますか？ (セクション3.3.1)

3. あなたの組織では、 どんな証拠ソース(あれば)を取得しますか? 証拠はどのようにして取得しますか? どこに保管しますか? どれだけの期間保管しますか? (セクション3.2.5、 3.3.2、 3.4.3)

事後活動:

1. このインシデントに関する反省会にはだれが参加しますか？ (セクション3.4.1)

2. 将来同様のインシデントの発生を防ぐには何ができますか？ (セクション3.1.2)

3. 同様のインシデントの検知を向上させるためには何ができますか？ (セクション3.1.2)

一般的な質問:

1. このインシデントの対応には、 インシデント対応チームのメンバーが何人参加しますか？(セクション2.4.3)

2. インシデント対応チーム以外で、 組織内のどのグループがこのインシデントの処理に関連しますか？(セクション2.4.4)

3. チームからどの外部関係者にこのインシデントを報告しますか？いつ報告しますか？報告はどのように行いますか？ (セクション2.3.2)

4 . 外部関係者への連絡事項には、 ほかに何がありますか？ (セクション2 . 3 . 2 )

5. このインシデントへの対応にあたって、 どのツールやリソースを使用しますか？ (セクション3.1.1)

6. インシデントが別の日の別の時間（就業時間内と就業時間外）に起きていたら、 対応方法にどのような面で違いが生じていましたか？ (セクション2.4.2)

7. インシデントが物理的に別の場所（オンサイトとオフサイト）で起きていたら、 対応方法にどのような面で違いが生じていましたか？ (セクション2.4.2)

* + - * 1. B.2 シナリオ

シナリオ1: DNS (Domain Name System)サーバのサービス不能

シナリオ2: 内部で生成されたスパム

シナリオ3: ワームとDDoSエージェントへの感染

シナリオ4: 盗まれたクレジットカード番号の使用

シナリオ5: 侵入されたデータベースサーバ

シナリオ6: ウイルスデマ情報

シナリオ7: FTPサーバ上の不正なデータ

シナリオ8: 外部へのDDoS攻撃

シナリオ9: 給与支払い記録への不正アクセス

シナリオ10: ハッキングツールのダウンロード

シナリオ11: 消えたホスト

シナリオ12: 在宅勤務の侵害

シナリオ13: テロリストの脅威

シナリオ14: フレームとポートスキャニング

シナリオ15: ピアツーピアのファイル共有

シナリオ16: 不明なワイヤレスアクセスポイント

* + - 1. 付録 C 事件に関係するデータフィールド
         1. C.1 基本的なデータフィールド

+ 事件報告者の連絡先情報

- 名前

- 組織ユニット(機関、 部門、 部、 チーム)

- 電子メールアドレス

- 電話番号

- 場所(住所、 オフィスの部屋番号など)

+ 事件の詳細

- 事件を発見した日付と時刻(タイムゾーンを含む)

- 事件が発生した日付と時刻(タイムゾーンを含む)

- 事件の種類(サービス不能、 悪意のコード、 不正アクセス、 不適切な使用など)

- 事件の物理的な位置(市、 州など)

- 事件の現在の状態(攻撃が継続中など)

- 事件のソースや原因(わかる場合)。 ホスト名とIPアドレスを含む。

- 事件の説明(どうやって検知したか、 何が起きたかなど)

- オペレーションシステムの種類、 オペレーションシステムのバージョンおよびパッチレベル

- ウイルス対策ソフトウェアがインストールされ、 有効かつ最新になっているか(はい／いいえ)

- 影響を受けたリソースの説明(ネットワーク、 ホスト、 アプリケーション、 データなど)。 システムのホスト名とIPアドレス、 および機能を含む。

- 事件を緩和するための要素

- 事件の技術的な影響の見積(データ消去、 システムクラッシュ、 アプリケーション利用不可など)。 (セクション2.3.6を参照して、 事件の重大さの格付けと影響の格付けを行うこと)

- 実施した対応活動(ホストの停止、 ホストのネットワークからの切断など)

- 連絡するほかの組織(ソフトウェアベンダーなど)

- 事件の最中に侵害された個人情報(あれば)の種類

+ 一般的なコメント

* + - * 1. C.2 事件処理担当者のデータフィールド

+ インシデント対応の現在のステータス

+ 事件の概要

+ 事件処理活動

- すべての処理担当による活動の記録

- 関連する全団体の連絡先情報

- 収集した証拠の一覧

+ 事件処理担当者のコメント

+ 事件の原因(アプリケーションの設定ミス、 ホストのパッチ未適用など)

+ 事件のコスト115

+ 事件のビジネスインパクト116

* + - 1. 付録 D 用語集
      2. 付録 E 頭字語
      3. 付録 F 印刷されたリソース
      4. 付録 G オンラインのツールとリソース
      5. 付録 H よく聞かれる質問
      6. 付録 I 危機処理のステップ
         1. 以下に、 技術の専門家が重大な事件が発生したことを確信したものの、 組織に利用できるインシデント対応能力がない場合に実施すべき主なステップを示す。
         2. この付録は、 現在危機に直面していて、 このドキュメント全体を読む時間がないという人にとって、 基本的な参考資料となる。
         3. 1. すべてを記録に残すこと

これには、 実行するあらゆる行動、 あらゆる証拠、 ユーザ、 システムオーナー、 事件に関係するその他の人とのあらゆる会話を含む。

* + - * 1. 2. 支援してくれる同僚を捜す

二人以上で協力すれば、 事件処理ははるかに容易になる。 たとえば、 ひとりが行動している間、 もう一人はそれを記録する。

* + - * 1. 3. 証拠を分析して事件が起きたことを確認する

必要に応じてさらに調査(インターネットサーチエンジン、 ソフトウェアマニュアルなど)し、 証拠をよく理解する。 組織内の技術専門家に連絡し、 助けを求める。

* + - * 1. 4. 事件が起きたと思われる場合には、 組織内の適切な人に通知する

これには最高情報責任者(CIO)、 情報セキュリティ部門長、 ローカルセキュリティマネージャが含まれる。 事件の詳細をだれかと話す場合は慎重に行う。 その事件により個人情報が流出したと思われる場合は、 組織のデータ侵害ポリシーが規定する関係者に、 その旨を通知する。 知る必要がある人にしか話さないようにし、 十分安全な通信手段を使用する(アタッカーが電子メールサービスを侵害した場合、 事件に関する電子メールは送らないこと)。

* + - * 1. 5. US-CERT(政府の諸官庁と機関の場合)および／または他の外部組織に事件を通知する。

まずは、 誤って機密情報を公開しないように、 事件に関して広報部、 法務部、 および／またはマネジメント層と話し合う。 その後、 US-CERTおよび／または他の外部組織に事件を報告し、 事件対応の支援を要請する。

* + - * 1. 6. 進行中の事件を止める

そのための最も一般的な方法は、 影響を受けたシステムをネットワークから切断することである。 サービス不能(DoS)攻撃などでは、 ファイアウォールやルーターの設定を変更して、 事件の一部になっているネットワークトラフィックを止めなくてはならない場合もある。

* + - * 1. 7. 事件の証拠を保管する

影響を受けたシステムのバックアップを作成する(ファイルシステムのバックアップではなく、 ディスクイメージのバックアップが望ましい)。 また、 事件に関連する証拠が入ったログファイルをコピーする。

* + - * 1. 8. 事件のすべての影響を一掃する

これには、 悪意のコードの感染ファイル、 不適切なデータ(海賊版ソフトウェアなど)、 トロイの木馬のファイル、 事件がもたらしたシステムへの変更に対する作業が含まれる。 システムが完全に侵害された場合は、 一から再構築するか、 正しいことがわかっているバックアップからリストアする。

* + - * 1. 9. 悪用されたすべての脆弱性を見つけて修正する

事件はオペレーティングシステムやアプリケーションの脆弱性を利用することで起きた可能性が高い。 そのような脆弱性を見つけて取り除くか軽減し、 再発しないようにすることが重要である。

* + - * 1. 10. 運用が通常に戻ったことを確認する

事件により影響を受けたデータ、 アプリケーション、 その他のサービスが通常の運用に戻ったことを確認する。

* + - * 1. 11. 最終レポートの作成

このレポートには、 事件処理プロセスを詳述する。 また、 何が起きたかを要約し、 もし正式なインシデント対応能力があれば、 どれだけ早く状況を処理し、 リスクを軽減し、 被害を制限できたかも記載する。

* + - 1. 付録 J 連邦政府機関による事件報告の分類
  1. NIST SP 800-63 (電子的認証に関するガイドライン)
     1. 電子的認証に関するガイドライン Electronic Authentication Guideline
     2. 2017年に改訂された
        1. IDを利用する場面ごとのリスクに応じて検証プロセスの強度を選択するという考え方が導入された
        2. 「パスワードは定期変更すべき」「パスワードは複数の」文字種で混成すべき」などの、 従来は常識とされてきた対策についても、 実効性や技術の進展に合わせた見直しが図られてる
        3. パスワードに代わる認証手段として、 指紋や顔画面などを活用した生体認証や、 認証結果を完全にやりとりできる「FIDO」の普及が期待されている
        4. 携帯電話をWebサービス全般の汎用的な認証手段として利用するための「Mobile Connect」が注目されている
        5. FIDO(Fast Identity Onlinbe)
           1. 生体認証やデバイス認証などのパスワード認証に代わる認証方式を実現する際のフレームワーク
           2. 認証結果を公開鍵暗号方式により」ネットワーク上で安全にやりとりするための仕様が定められており、 認証に必要な秘密情報は認証を行う端末のみに保存され、 ネットワーク上での伝送やサーバーに保存する必要がない
        6. モバイル認証（GSMA Mobile Connect）
           1. 移動通信事業者（MNO:Mobile Network Operator）の業界団体であるGSMアソシエーション（GSMA）が普及を推進している、 携帯端末をWebサービスの認証機器として使用できるようにするための仕様「Mobile Connect」
     3. 文書
        1. SP 800-63-3
           1. Digital Identity Guidelines
           2. IDフレームワーク全体の概要、 リスクに応じた保証レベル(IAL/AAL/FAL)の選択
        2. SP 800-63-A
           1. Enrollment and Identity Proofing Requirements
           2. ID登録と身分確認におけるアイデンティティ保証レベル(IAL)の定義
        3. SP 800-63-B
           1. Authentication and Lifecycle Management
           2. 認証保証レベル(AAL)の導入と各認証方式に求められる要件、 脅威／プライバシー／ユーザビリティ面での考察ポイント
        4. SP 800-63-C
           1. Federation and Assertions
           2. 信頼関係を結んだシステム間での認証連携（フェデレーション）におけるフェデレーション保証レベル(FAL)の導入と各レベルに求められる要件、 プライバシーに考慮した属性連携
  2. CSC20 （効果的なサイバー防御のための重要なセキュリティコントロール）
     1. 「Critical Security Controls for Effective Cyber Defense」（効果的なサイバー防御のための重要なセキュリティコントロール）は、 Version6.0が2015年10月に米国のCenter for Internet Securityから公開された。
     2. サイバー攻撃に対する重要なセキュリティ対策を20のコントロールに分類・優先度付けをしたもので、 極力自動化された技術的対策が主体となっている。
     3. CSC1 許可および無許可の機器のインベントリ
     4. CSC2 許可および無許可のソフトウェアのインベントリ
     5. CSC3 モバイル機器、 ラップトップ、 ワークステーション、 サーバにおけるハードウェアおよびソフトウェアのセキュアな構成
     6. CSC4 継続的な脆弱性診断と改修
     7. CSC5 管理者権限のコントロールされた使用
     8. CSC6 監査ログの保守、 監視、 および分析
     9. CSC7 電子メールとWebブラウザの保護
     10. CSC8マルウェア防御
     11. CSC9 ネットワークポート、 プロトコル、 サービスの制限およびコントロール
     12. CSC10 データ復旧能力
     13. CSC11 ファイアウォールやルーター、 スイッチなどのネットワーク機器のセキュアな構成
     14. CSC12 境界防御
     15. CSC13 データ保護
     16. CSC14 知る必要性に基づいた、 管理されたアクセス
     17. CSC15 無線のアクセスコントロール
     18. CSC16 アカウントのモニタリングおよびコントロール
     19. CSC17 不足を補完するためのセキュリティスキル評価および適切なトレーニング
     20. CSC18 アプリケーションソフトウェアのセキュリティ
     21. CSC19 インシデント対応と管理
     22. CSC20 ペネトレーションテストおよびレッドチームによる訓練
  3. Top35 （標的型サイバー侵入の軽減戦略）
     1. 「Strategies to Mitigate Targeted Cyber Intrusions」(Top35 Mitigation Strategies)
     2. 「Strategies to Mitigate Targeted Cyber Intrusions」（標的型サイバー侵入の軽減戦略）は、 2014年2月に2014年版がオーストラリアの国防信号局から公開されています。 標的型攻撃を主な脅威と想定したセキュリティ対策を、 優先度順に35のカテゴリーで示したものです。
  4. GDPR（General Data Protection Regulation：一般データ保護規則）
     1. GDPR（General Data Protection Regulation：一般データ保護規則）【個人情報保護委員会】

ドキュメントを参照: [GDPR](https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/)

* + - 1. GDPR（General Data Protection Regulation：一般データ保護規則）
         1. EU（※）では、 EU域内の個人データ保護を規定する法として、 1995年から現在に至るまで適用されている「EUデータ保護指令（Data Protection Directive 95）」に代わり、 2016年4月に制定された「GDPR（General Data Protection Regulation：一般データ保護規則）」が2018年5月25日に施行されます。
         2. GDPRは個人データやプライバシーの保護に関して、 EUデータ保護指令より厳格に規定します。
         3. また、 EUデータ保護指令がEU加盟国による法制化を要するのに対し、 GDPRはEU加盟国に同一に直接効力を持ちます。
         4. ※ EU：EU加盟国及び欧州経済領域（EEA）の一部であるアイスランド、 ノルウェー、 リヒテンシュタイン
         5. なお、 EU各国の個人情報保護機関については、 こちらをご覧ください。

ドキュメントを参照: [EU-DPA](https://www.ppc.go.jp/enforcement/cooperation/cooperation/EU-DPA/)

* + - 1. EU域外適用に関する影響
         1. GDPRはEU域外の事業者へも適用されます。 各組織・企業等の業務への影響について、 あらかじめ備えておく必要があります。
         2. 欧州委員会（European Commission）がWebサイトに掲載している資料の内、 以下の日本語仮訳を作成いたしましたので掲載いたします。
         3. Infographic（外部サイト（欧州委員会））

ドキュメントを参照: [index\_en.htm](http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm)

日本語仮訳付PDF (PDF：1090KB) （中小企業向けの、 簡単にまとめられたGDPR説明）

ドキュメントを参照: [EC-Infographic.pdf](https://www.ppc.go.jp/files/pdf/EC-Infographic.pdf)

* + - * 1. Fact Sheet "Questions and Answers-Data protection reform package"（外部サイト（欧州委員会））

ドキュメントを参照: [press-release\_MEMO-17-1441\_en.htm](http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm)

日本語仮訳付PDF (PDF：318KB) （GDPRによるデータ保護改革案についての質疑応答概略）

ドキュメントを参照: [Factsheet-20170524QandA.pdf](https://www.ppc.go.jp/files/pdf/Factsheet-20170524QandA.pdf)

* + - 1. 越境データ移転
         1. GDPRは、 EU域内の個人データのEU域外への移転について規定します。
         2. EU域内から域外へ個人データを移転するには、
         3. 十分な個人データ保護の保障

（欧州委員会が、 データ移転先の国が十分なレベルの個人データ保護を保障していることを決定）

* + - * 1. BCR（Binding Corporate Rules：拘束的企業準則）の締結

（企業グループで1つの規定を策定し、 データ移転元の管轄監督機関が承認）

* + - * 1. SCC（Standard Contractual Clauses：標準契約条項）の締結

（データ移転元とデータ移転先との間で締結し、 欧州委員会が承認）

* + - * 1. 明確な本人同意
        2. 等、 一定の条件を満たさなくてはなりません。
      1. 日EU間の越境データ移転
         1. 我が国においては、 個人情報保護法が外国にある第三者への個人データの提供について規定しています。 個人データを越境移転するためには、

我が国と同等の水準にあると認められる個人情報保護制度を有している外国として委員会規則で定めるもの

必要な措置を継続的に講ずるため、 委員会規則に定める基準に適合する体制を整備している個人情報取扱事業者

あらかじめ外国にある第三者への提供を認める旨の本人の同意がある場合

* + - * 1. 等、 一定の条件を満たさなくてはなりません。
        2. 日EU間においては、 双方の規定の下で、 相互に円滑な個人データ移転を行う環境を確保することを目指し、 当委員会と欧州委員会は対話を重ねてきています。
        3. 2017年12月14日には、 個人情報保護委員会熊澤委員と欧州委員会ヨウロバー委員が、 日EU間の個人データ移転について会談を行い、 双方の制度間の関連する相違点に対処するための、 法令改正を行わない形での解決策について確認するとともに、 今後、 その詳細について作業すること、 また、 2018年第一四半期に、 最終合意することを想定し、 委員レベルで会談をもつことで一致しました。
        4. 上記の会談について、 熊澤委員とヨウロバー委員は「共同プレスステートメント」 (PDF：149KB) を発出しました。

ドキュメントを参照: [291215\_pressstatement.pdf](https://www.ppc.go.jp/files/pdf/291215_pressstatement.pdf)

* + - * 1. 「共同プレスステートメント」（2017年12月14日） (PDF：149KB)

ドキュメントを参照: [291215\_pressstatement.pdf](https://www.ppc.go.jp/files/pdf/291215_pressstatement.pdf)

* + - 1. 参考（外部サイト）
         1. GDPR（欧州連合（EU）Webサイト）

ドキュメントを参照: [oj](http://eur-lex.europa.eu/eli/reg/2016/679/oj)

* + - * 1. 2018 reform of EU data protection rules（欧州委員会（EC）Webサイト）

ドキュメントを参照: [2018-reform-eu-data-protection-rules\_en](https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en)

* + - * 1. Questions and Answers - GDPR - Factsheets 24 January 2018（欧州委員会（EC）Webサイト）

ドキュメントを参照: [press-release\_MEMO-18-387\_en.htm](http://europa.eu/rapid/press-release_MEMO-18-387_en.htm)

* + - * 1. GDPRガイドライン（欧州委員会（EC）Webサイト）

ドキュメントを参照: [item-detail.cfm](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

Guidelines on the right to "data portability", wp242rev.01\_en（PDF）

Guidelines on Data Protection Officers ( DPOs ), wp243rev.01\_en（PDF）

Guidelines on The Lead Supervisory Authority, wp244rev.01\_en（PDF）

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, wp248rev.01（PDF）

Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679, wp253（PDF）

Guidelines on Data Protection Impact Assessment (DPIA), wp248（PDF）

Guidelines on the right to "data portability"（PDF）

WP242 ANNEX-Frequently asked questions（PDF）

Guidelines on Data Protection Officers ( DPOs ) （PDF）

WP243 ANNEX - Frequently asked questions（PDF）

Guidelines for identifying a controller or processor's lead supervisory authority（PDF）

WP244 ANNEX II-Frequently asked questions（PDF）

未承認のガイドライン等については、 以下の欧州委員会（EC）Webサイトをご覧ください。

http://ec.europa.eu/newsroom/just/item-detail.cfm?item\_id=50083

ドキュメントを参照: [item-detail.cfm](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083)

* + - * 1. Data Protection Reform - Factsheets 16 January 2017（EU加盟国の各国語）

ドキュメントを参照: [item-detail.cfm](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=52404)

* + 1. 欧州連合における個人情報保護の枠組みGDPR、 その現状と対策のポイント【2017年08月01日富士通マーケティング】

ドキュメントを参照: [001.html](http://www.fujitsu.com/jp/group/fjm/mikata/column/sawa2/001.html)

* + - 1. GDPRの概要
         1. 2016年5月4日付EU官報に掲載、 同年5月24日に発効、 行政罰を伴う適用開始は2018年5月25日であり、 ここからが実質の施行日となる。
         2. EUを含む欧州経済領域（EEA：EU加盟国28カ国＋アイスランド、 リヒテンシュタイン、 ノルウェー）域内で取得した「氏名」「メールドレス」「クレジットカード番号」などの個人データをEEA域外に移転することを原則禁止とする。 「個人」とは域内所在者のほか、 現地日系企業の現地採用従業員および日本から派遣される駐在員も含まれる点に注意。
         3. 個人データの範囲は、 職業上の電子メールアドレス、 オンライン識別子（IPアドレス／クッキー識別子）、 身体的、 生理学的、 遺伝子的、 精神的、 経済的、 文化的、 社会的固有性に関する要因も含まれる。
         4. EEA域内の現地法人・支店・駐在員を置くすべての企業・団体・機関が対象。
         5. EEA域内に上記支店などを置かない企業でも、 インターネット取引などで域内における所在者の個人情報を取得・移転する場合は適用対象となる。
         6. 個人情報の移転が適法となるのは、 十分性が認められる国・地域であるか、 適切な保護措置を取った場合とされるが、 十分性が認められた国は少なく、 日本企業は十分性が認められていないため、 保護措置を適切に施す必要がある。
         7. 違反の場合の制裁金は、 全世界年間売上高の4％以下または2000万ユーロ以下のいずれか高い方など。
         8. サイバーアタックなどで情報漏えいが発生したときの当局への報告や、 本人の求めに応じた個人情報の訂正などを怠った場合も制裁金の対象となることがある。
      2. 個人情報保護法との違い
         1. 前段に記述したとおり、 日本では個人情報の概念は氏名や住所などその人を特定できる情報という考え方になりますが、 GDPRではIDなど、 照合しないと個人が特定できないようなものも対象とされる点に注意が必要です。 また、 履歴データなども個人名がなければ問題なさそうに思えますが、 GDPRではこれも個人情報に該当します。
      3. GDPRが日本の企業に及ぼす影響
         1. 日本国内では本社と支店や系列企業の間での個人情報の移転は、 同じ企業内のセキュリティ措置で保護されていれば問題はありません。 しかし、 GDPR施行下では支店や系列企業内であってもEU域内から個人情報を移転することは原則できません。 ディスプレイで閲覧できる場合も移転とみなされる点に注意したいところです。
         2. 大きな影響を受けるのは、 EUを含めたEEA域内に支店や営業所、 系列企業などを持つグローバル企業でしょう。 現地採用の社員の個人情報はもちろん、 日本から出向している社員もEEA域内の事業所に勤務した場合は対象となるため、 扱いをルールに従ったものにしなければなりません。
         3. 海外に拠点を持つグローバル企業に限らず、 EEA域内の法人や団体とパートナー関係にある場合も注意しなければなりません。 GDPRの概要にも示したとおり、 日本のECサイトからEEA域内の在住者が購入をした場合も対象となるので、 技術提携や販売パートナーのような関係の企業との間においても十分な配慮が求められます。
      4. 日本企業の対応策
         1. 日本とは個人情報の定義や考え方が異なる点に留意し、 プライバシーポリシーに反映させる必要があります。 実務上、 EU域内の個人情報を移転する際は、 十分性があると認められていない日本では企業ごとに以下の手続きをしなければなりません。

「拘束的企業準則BCR（Binding Corporate Rules）」に準拠したルールを文書化して、 EUのデータ保護機関から承認を得る。 時間と費用を要するが承認されれば、 事業グループ内での地域を超えた個人情報の移動が、 ルールに従った範囲で可能となる。

「標準契約条項SCC（Standard Contractual Clauses）」はデータの移転を案件単位にして結ぶもので、 欧州委員会で決定された契約書のひな型であり、 当事者間でデータ移転契約として締結。 契約に即した履行体制が敷かれていることが前提である。 EU各国で条件が異なるため、 それぞれで事前承認取得などの作業が求められる。

* + - * 1. GDPRについてまとめてみました。 実質の施行となる2018年5月までに残された期間は余裕があるとはいえず、 この直前や施行されてから必要性に気づくのでは遅すぎます。 訪日旅客が増え、 東京オリンピックも近いため、 国内だけでサービス業を営む会社でもGDPRの内容を確認しておくことをお勧めします。
    1. EU一般データ保護規則（GDPR）の概要と企業が対応すべき事項【情報センサー2017年2月号】

ドキュメントを参照: [2017-02-05.html](https://www.eyjapan.jp/library/issue/info-sensor/2017-02-05.html)

* + - 1. Ⅰ EU一般データ保護規則の概要
         1. 1. GDPRとは

EU一般データ保護規則（General Data Protection Regulation：GDPR）は欧州連合（EU）における新しい個人情報保護の枠組みであり、 個人データ（personal data）の処理と移転に関するルールを定めた規則です。 1995年から適用されたEUデータ保護指令（Data Protection Directive 95）に代わり、 EU加盟諸国に対して直接効力が発生する法規制としてGDPRが2016年4月に制定されました。

* + - * 1. 2. GDPRの規制事項

(1) 個人データの処理

個人データを処理するに当たり、 企業は管理者（Controller）として、 次のような規制事項を遵守することが求められます。

個人データの処理および保管に当たり、 適切な安全管理措置を講じなければならない。

処理を行う目的の達成に必要な期間を超えて個人データを保持し続けてはならない。

個人データの侵害（情報漏えい）が発生した場合、 企業はその旨を監督機関に対し72時間以内に通知しなければならない。

定期的に大量の個人データを取扱う企業などでは、 データ保護オフィサー（Data Protection Officer）を任命しなければならない。

(2) 個人データの移転

EEA（欧州経済領域）の域内から域外への個人データの移転は原則として禁止され、 例えば日本のように欧州委員会によって適切な個人情報保護制度を有していると認められていない国への情報移転に当たっては、 企業は拘束的企業準則（Binding Corporate Rules）の策定、 標準契約条項（Standard Contract Clauses）の締結など、 適切な施策の下で一定の要件を満たす必要があります。

(3) 基本的権利の保護

GDPRはデータ主体（Data Subject）すなわち本人の基本的権利を保護するという考え方が強く打ち出されています（GDPR第1条）。 例えば個人データの取得に際しては、 以下のようなルールが定められています。

企業は管理者として自らの身元や連絡先、 処理の目的、 第三者提供の有無、 保管期間、 データ主体の有する権利などについて、 明瞭で分かりやすい表現によりデータ主体に通知しなければならない。

企業は前記に関して明確な方法により同意を得るとともに、 データ主体が同意を自由に撤回することができる権利を適切に行使できるようにしなければならない。

個人データをデータ主体から直接取得していない場合、 企業は当該情報の入手先を本人に通知しなければならない。

こうした主な規制事項を含め、 GDPRでは全部で173項目の前文とともに99条にわたる規制事項がきめ細かく定められています。

* + - 1. Ⅱ 日本企業への影響
         1. 1. 影響を受ける企業

GDPRはEUで定められたルールですが、 以下のような場合は日本の企業であっても適用対象となり、 必ずしも無関係であるとは限らない点に注意が必要です。

(1) EUに子会社、 支店、 営業所を有している企業

EU域内に所在地がある当該子会社などにとってGDPRは直接の適用対象であり、 当該企業は日本に本社を有している場合でも、 管理者としてGDPRへの対応が必要となります。

(2) 日本からEUに商品やサービスを提供している企業

EU域内の個人（消費者）に対して日本から商品やサービスを提供している場合、 たとえEU域内に子会社などがなかったとしても、 当該企業は個人データの取得や処理に当たりGDPRに沿った手続を実施する必要があります。

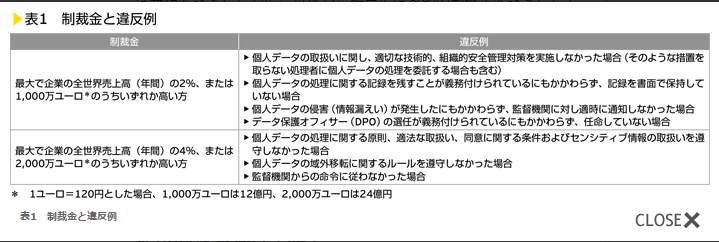
(3) EUから個人データの処理について委託を受けている企業

データセンター事業者やクラウドベンダーなどのように、 EU域内の企業から個人データの処理などを受託している日本企業の場合、 当該受託企業は処理者（Processor）として個人データの域外移転に関してGDPRが定めるルールに準拠する必要があります。

* + - * 1. 2. 違反時のインパクト

Ⅰ 2. で述べたように、 GDPRは適用対象となる企業に対しさまざまな義務を課すとともに、 違反した場合には多額の制裁金を課すことでルールの遵守を厳格に働きかけています（GDPR第83条）（＜表1＞参照）。

表1 制裁金と違反例

Subtopic  


最大で企業の全世界売上高（年間）の2%、 または1,000万ユーロのうちいずれか高いほう

個人データの取扱いに関し、 適切な技術的、 組織的安全管理対策を実施しなかった場合（そのような措置を取らない処理者に個人データの処理を委託する場合も含む）

個人データの処理に関する記録を残すことが義務付けられているにもかかわらず、 監督機関に対して適時に通知しなかった場合

個人データの侵害（情報漏えい）が発生したにもかかわらず、 監督機関に対し適時に通知しなかった場合

データ保護オフィサー（DPD）の選任が義務付けられているにもかかわらず、 任命していない場合

最大で企業の全世界売上高（年間）の4%、 または2,000万ユーロのうちいずれか高いほう

個人データの処理に関する原則、 適法な取扱い、 同意に関する条件およびセンシティブ情報の取扱いを遵守しなかった場合

個人データの域外移転に関するルールを遵守しなかった場合

監督機関からの命令に従わなかった場合

* + - 1. Ⅲ GDPRへの対応に向けて
         1. 日本においても個人情報保護法が改正され、 2017年5月30日から全面施行となります。 しかし、 個人データを取扱う保護レベルとしては、 日本はいまだ欧州委員会による十分性の認定を受けるに至っていません。 このため、 日本企業が事業活動を積極的にグローバル展開していく中で、 個人データをEUとの間で円滑に流通させるためには、 各企業がGDPRに沿った対応について自主的に取り組む必要があります。
         2. GDPRの要求事項は多岐にわたるため、 企業は各条文の内容の理解にとどまらず自社の置かれている状況を適切に把握した上で、 次のような実務対応計画を慎重に進めていくことが望ましいと考えられます。
         3. 【準備フェーズ】

各拠点においてどのような個人データが存在し、 どのような経路で流通しているのかについて現状を調査する（データマッピング）。 その上でGDPR対応として必要な作業について担当部署、 作業ボリュームを把握することにより、 次フェーズに向けた全体計画およびスケジュールを決定する。

* + - * 1. 【対応フェーズ】

準備フェーズの計画に基づき、 GDPR対応として求められる個人データ保護の管理態勢（組織内の役割分担、 規程類の整備、 運用ルールの決定など）を構築し、 関係者に周知徹底する。

* + - * 1. 【運用フェーズ】

新たに制定した規程類、 ルールにのっとって適切に運用が行われているかどうかを評価し、 必要に応じて規程等の見直しまたは運用の改善を実施する。

* + - * 1. 以上を踏まえ、 企業は18年5月の適用開始に向けて、 限られた時間の中で効率的かつ速やかにGDPR対応を推進していくことが重要となってきます。

1. 未整理
   1. 【未整理】NIST SP.800-82R2　Guide to Industrial Control Systems (ICS) Security

ドキュメントを参照: [nist.sp.800-82r2.pdf](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf)

* 1. 【未整理】ENISA「IoTのベースラインセキュリティに関する提言」概要【2018年1月19日IPA】

ドキュメントを参照: [000063605.pdf](https://www.ipa.go.jp/files/000063605.pdf)

* 1.  【未整理】NIST Special Publication 800-171r1 連邦政府外のシステムと組織における管理された非格付け情報の保護
     1. 【IPA和訳】
  2. 【未整理】クラウドコンピューティングのためのセキュリティガイダンスv4.0

ドキュメントを参照: [guidance.html](http://www.cloudsecurityalliance.jp/guidance.html)

* + 1. CSA\_Guidance\_V4.0\_J\_V1.1\_20180724

ドキュメントを参照: [CSA\_Guidance\_V4.0\_J\_V1.1\_20180724.pdf](https://cloudsecurityalliance.jp/j-docs/CSA_Guidance_V4.0_J_V1.1_20180724.pdf)

* 1. 【未整理】危険な12の落とし穴　クラウドの重大セキュリティ脅威＋2017インシデント事例集【一般社団法人日本クラウドセキュリティアライアンス（CSAジャパン）】

ドキュメントを参照: [treacherous-12-top-threats-Industry-insight\_J\_V2.1\_20180521.pdf](http://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2018/05/treacherous-12-top-threats-Industry-insight_J_V2.1_20180521.pdf)

* 1. 【未整理】「つながる世界」を破綻させないためのセキュアなIoT製品開発13のステップ【CSAジャパン　IoTワーキンググループ】

ドキュメントを参照: [future-proofing-the-connected-world\_J\_20170520.pdf](https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/future-proofing-the-connected-world_J_20170520.pdf)

* 1. 【未整理】IoTへのサイバー攻撃仮想ストーリー集

ドキュメントを参照: [scenario.pdf](https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/scenario.pdf)

* + 1. 一般社団法人日本クラウドセキュリティアライアンス（CSAジャパン）
  1. 【未整理】国内標的型サイバー攻撃分析レポート
     1. https://www.trendmicro.com/ja\_jp/about/press-release/2018/pr-20180625-01.html

ドキュメントを参照: [pr-20180625-01.html](https://www.trendmicro.com/ja_jp/about/press-release/2018/pr-20180625-01.html)

* 1. 【未整理】重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書（第1版）
     1. NISC サイバーセキュリティ戦略本部　重要インフラ専門調査会

1. 【参考】IT関連（原本は「Bib10-08国の事業が実施に至るまで」）
   1. IT戦略本部
   2. 高度情報通信ネットワーク社会形成基本法（IT基本法）（2015年2月1日改訂施行）

ドキュメントを参照: [honbun.html](http://www.kantei.go.jp/jp/singi/it2/hourei/honbun.html)

* 1. 「世界最先端IT国家創造宣言」の改定（高度情報通信ネットワーク社会推進戦略本部（IT戦略本部））（2016.5.20閣議決定)

ドキュメントを参照: [siryou1.pdf](http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20160520/siryou1.pdf)

* + 1. Ⅰ.世界最先端 IT 国家創造宣言に基づくこれまでの成果
       1. １. これまでの代表的な成果
          1. (１) 行政情報システム改革を通じた利用者志向の行政サービスの実現
          2. (２) マイナンバー制度を活用した国民生活の利便性の向上
          3. (３) 安全・安心なデータ流通の促進
          4. (４) 農業のIT 化による国際競争力強化
          5. (５) 世界で最も安全で環境にやさしく経済的な道路交通社会の実現
       2. ２．IT 利活用による目指すべき社会の実現に向けた今後の重点的な取組方針
    2. II. 「国から地方へ、 地方から全国へ」（IT 利活用の更なる推進のための３つの重点項目）
       1. １．[重点項目１] 国・地方のIT 化・業務改革（BPR）の推進
          1. (１) 国のIT 化・業務改革（BPR）の更なる推進
          2. (２) 地方公共団体のIT 化・業務改革（BPR）の推進
          3. (３) ガバナンス体制の強化
       2. ２．[重点項目２] 安全・安心なデータ流通と利活用のための環境の整備
          1. (１) 利用者志向のデータ流通基盤の構築
          2. (２) データ流通の円滑化と利活用の促進
          3. (３) 課題解決のためのオープンデータの「実現」（オープンデータ2.0）
       3. ３．[重点項目３] 超少子高齢社会における諸課題の解決
          1. (１) ビッグデータを活用した社会保障制度の変革
          2. (２) マイナンバー制度等を活用した子育て行政サービスの変革
          3. (３) IT 利活用による諸課題の解決に資する取組

① 産業競争力の強化

② 地方創生の実現

③ マイナンバー制度を活用した国民生活の利便性の向上

④ 安全で災害に強い社会の実現

* + 1. III. 推進体制等
       1. １．政府 CIO の司令塔機能の発揮
       2. ２．関係本部等との連携体制
       3. ３．進捗管理における評価指標の設定・管理
       4. ４．国際貢献及び国際競争力の強化に向けた国際展開
  1. 電子行政オープンデータ戦略（2012年7月4日IT戦略本部）【再掲】

ドキュメントを参照: [denshigyousei.html](http://www.kantei.go.jp/jp/singi/it2/denshigyousei.html)

* + 1. ○電子行政オープンデータ戦略の概要（抜粋）61
    2. Ⅰ．基本的方向性
       1. ＜基本原則＞
       2. － 政府自ら積極的に公共データを公開すること
       3. － 機械判読可能な形式で公開すること
       4. － 営利目的、 非営利目的を問わず活用を促進すること
       5. － 取組可能な公共データから速やかに公開等の具体的な取組に着手し、 成果を確実に蓄積していくこと
    3. Ⅱ．具体的な施策
       1. １．公共データ活用の推進
          1. ①公共データ活用ニーズの把握
          2. ②データ提供方法等に係る課題の整理、 検討
          3. ③民間サービスの開発
       2. ２．公共データ活用のための環境整備
          1. ①公共データ活用のために必要なルール等の整備

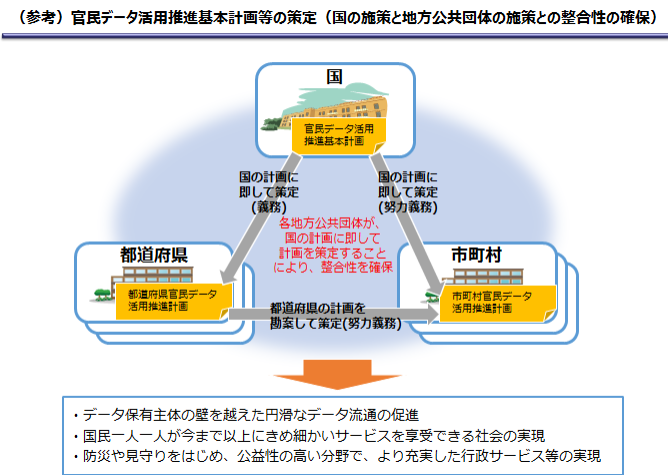
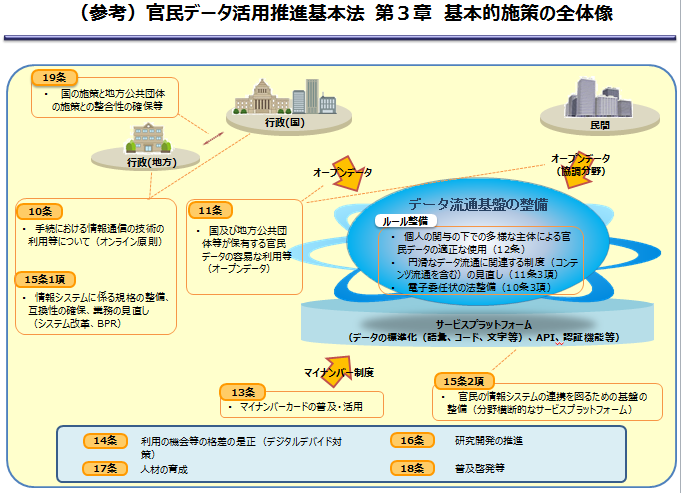
各府省におけるデータ公開時の著作権の取扱い、 利用条件、 機械からのアクセスルール、 利用者と提供者の責任分担の在り方、 機微情報の取扱いの在り方等について、 利用者の利便性と権利者の権利の保護に十分配意しつつ、 公共データ活用のために必要なルール等を整備する。

* + - * 1. ②データカタログの整備
        2. ③データ形式・構造等の標準化の推進等
        3. ④提供機関支援等についての検討
  1. 電子行政オープンデータ推進のためのロードマップ（2013年6月14日IT戦略本部決定）

ドキュメントを参照: [siryou3.pdf](http://www.kantei.go.jp/jp/singi/it2/kettei/pdf/20130614/siryou3.pdf)

* 1. 官民データ活用推進基本法（平成28年法律第103号）
  2. 「オープンデータ基本指針」（案）「オープンデータ基本指針」（案）【2017年5月23日官民データ活用推進基本計画実行委員会】

ドキュメントを参照: [gijisidai.html](http://www.kantei.go.jp/jp/singi/it2/senmon_bunka/data_ryutsuseibi/opendata_wg_dai3/gijisidai.html)

* + 1. 体制
       1. 高度情報通信ネットワーク社会推進戦略本部（IT本部）
       2. 官民データ活用推進戦略会議
          1. ＜法律（官民データ活用推進基本法）により設置（平成28年12月14日）
          2. 議　 長：内閣総理大臣 副議長：情報通信技術（IT）政策担当大臣、 内閣官房長官、 総務大臣、 経済産業大臣 議　 員：議長・副議長を除く全国務大臣、 政府CIO及び有識者
       3. 官民データ活用推進基本計画実行委員会
          1. ＜官民データ活用推進戦略会議議長決定により設置（平成29年3月31日）＞
          2. 会長：民間委員、 （委員会構成：民間委員＋各省庁局長級
    2. 概念
       1. Subtopic  
          
       2. Subtopic  
          
    3. オープンデータ基本指針（案）の概要
       1. 本基本指針の位置づけ
          1. 平成28年12月14日に公布・施行された「官民データ活用推進基本法」において、 国、 地方公共団体、 事業者が保有する官民データの容易な利用等について規定された。 本文書は、 これまでの取り組みを踏まえ、 オープンデータ・バイ・デザイン（注）の考えに基づき、 国、 地方公共団体、 事業者が公共データの公開及び活用に取り組む上での基本方針をまとめたものである。
       2. １．オープンデータの意義
          1. （１）国民参加・官民協働の推進を通じた諸課題の解決、 経済活性化
          2. （２）行政の高度化・効率化
          3. （３）透明性・信頼の向上
       3. ２．オープンデータの定義
          1. ①　営利目的、 非営利目的を問わず二次利用可能なルールが適用されたもの
          2. ②　機械判読に適したもの
          3. ③　無償で利用できるもの
       4. ３．オープンデータに関する基本的ルール
          1. （１）公開するデータの範囲

・・・各府省庁が保有するデータは、 原則オープンデータとして公開。 公開することが適当でない公共データは、 公開できない理由を原則開示するとともに、 限定的な関係者間での共有を図る「限定公開」といった手法も積極的に活用。

* + - * 1. （２）公開データの二次利用に関するルール

・・・ 原則、 政府標準利用規約を適用。

* + - * 1. （３）公開環境

・・・特にニーズが高いと想定されるデータは、 一括ダウンロードを可能とする仕組みの導入や、 APIを通じた提供を推進。

* + - * 1. （４）公開データの形式等

・・・機械判読に適した構造及びデータ形式で掲載することを原則。 法人情報を含むデータは、 法人番号を併記。

* + - * 1. （５）公開済みデータの更新

・・・可能な限り迅速に公開するとともに適時適切な更新。

* + - 1. ４．オープンデータの公開・活用を促す仕組み
         1. （１）オープンデータ・バイ・デザインの推進

・・・行政手続き及び情報システムの企画・設計段階から必要な措置

* + - * 1. （２）利用者ニーズの反映

・・・各府省庁の保有データとその公開状況を整理したリストを公開 利用者ニーズを把握の上、 ニーズに即した形での公開

* + - 1. ５．推進体制
         1. （１）相談窓口の設置

・・・総合的な相談窓口（内閣官房IT総合戦略室）・相談窓口（各府省庁）の設置

* + - * 1. （２）推進体制

・・・内閣官房IT総合戦略室は、 政府全体のオープンデータに関する企画立案・総合調整、 各施策のレビュー、 フォローアップを実施等

* + - 1. ６．地方公共団体、 独法、 事業者における取組
         1. 地方公共団体

・・・官民データ法の趣旨及び本基本指針を踏まえて推進。

* + - * 1. 独立行政法人

・・・国費によって運営されていること又は実施している事業や研究があることに鑑み、 基本指針に準拠して取組を推進することが望ましい。

* + - * 1. 公益事業分野の事業者

・・・その公益性に鑑み、 本基本指針及び利用者ニーズを踏まえて推進することが望ましい。

* + 1. オープンデータ・バイ・デザインの推進（案）
       1. １．オープンデータ・バイ・デザインの定義
          1. 「行政が保有するデータについては、 オープンデータを前提として情報システムや業務プロセス全体の企画、 整備及び運用を行う」
       2. ２．オープンデータ・バイ・デザインの具体的な内容
          1. 行政が保有するデータを原則としてオープンデータ化するとともに、 利用者が活用しやすい形で公開するため、 行政手続及び情報システムの企画・設計段階から必要な措置を講じる。
          2. （１）一括ダウンロードやAPIを通じたデータ提供

特にニーズが高いと想定されるデータは一括ダウンロードを可能とする仕組みの導入や、 APIを通じた提供を推進する

* + - * 1. （２）メタデータの公開

公開データについて適切なメタ情報を付与し、 政府のデータカタログサイトへ漏れなく登録がされるようにする

* + - * 1. （３）機械判読に適したファイル形式およびデータ構造

公開可能なデータを抽出/出力/公開するための仕組みをシステム要件に含める

公開データがJSON・CSV等、 機械判読に適したファイル形式で公開されるようにする

各府省庁が行う委託・請負契約に当たっては、 報告書等の成果物を機械判読に適したファイル形式で納品されるようにする

* + - * 1. （４）データ構造やデータ形式の標準化

可能な限り標準化された形式やコード体系等でデータを格納・出力する法人情報を含むシステムの開発・更新に当たっては、 法人番号の併記を原則とする

* + - * 1. （５）公開済みデータの更新

データ公開後も適切にデータの更新がされるように仕組みや運用体制を構築する

* + - 1. また、 データベース構築にあたっては、 オープンデータを前提とする（非公開とすることに合理的な理由がないものについては、 予算計上を認めないこととする）。
      2. 今後オープンデータ・バイ・デザインの取組は、
         1. 「デジタル・ガバメント推進方針」の動き※と連携しながら進めていく。

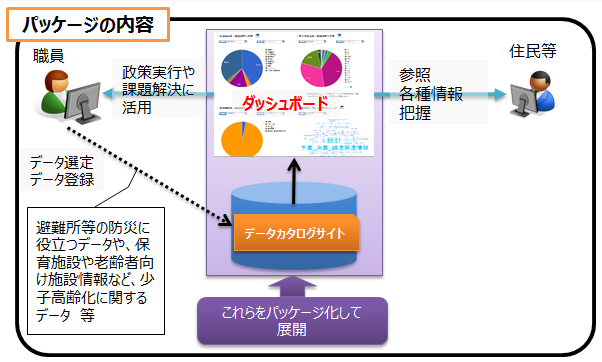
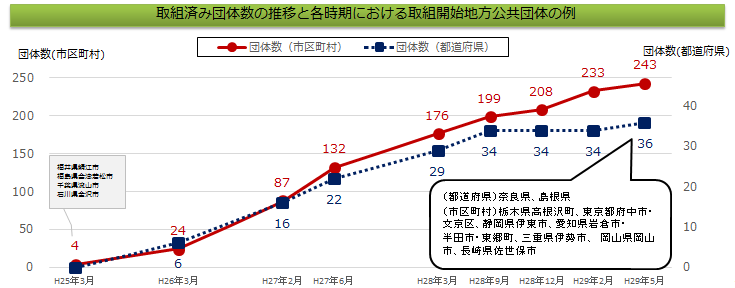
デジタル・ガバメント推進方針【2017年5月】

デジタル・ガバメント実行計画【2017年内】

【2018年以降】

実行計画に基づく各種取組の推進

各府省における中長期的な計画の策定、 推進　等

* + - * 1. 企画・設計時の具体的な実施事項については「政府情報システムの整備および管理に関する標準ガイドライン」及び同実務手引書に盛り込み、 政府情報システム全体への浸透を図ることとする。
    1. 地方公共団体の取り組み促進（案）
       1. 地方公共団体におけるオープンデータへの取組を加速する改良版パッケージの提供。
          1. オープンデータに取組む意思や必要性は感じているが、 具体的な取組方法が分からない地方公共団体を支援するため、 関係諸団体と連携し、 オープンデータのデータカタログとダッシュボードアプリケーションをパッケージ化して提供することで、 地方公共団体によるオープンデータの導入・活用を促進する。
       2. Subtopic  
          
       3. ■期待される効果
          1. ・防災関連や少子高齢化など地域課題に関係するデータの公開による、 地域課題解決の一助
          2. ・公開と活用両方の自治体展開パッケージの提供による、 地方公共団体の取組を容易化
          3. ・標準化の推進（登録データのフォーマット標準例の提供等）
          4. パッケージはオープンソースとしてGitHubで公開することにより、 他の地方公共団体に展開可能とする (※) 。
       4. ※パッケージ一式導入用：
          1. https://github.com/nes-opendata/odpkg-docker
       5. ※ダッシュボードのみ導入用：
          1. https://github.com/nes-opendata/odpkg-dashboard
       6. オープンデータに取り組む地方公共団体数
          1. Subtopic  
             
       7. 導入予定
          1. ・福岡市、 久留米市へダッシュボードを導入。 （平成29年4月公開）
          2. ・長崎県（平成29年6月公開予定）、 京都府（平成29年6月公開予定）へパッケージを導入。
  1. 世界最先端ＩＴ国家創造宣言・官民データ活用推進基本計画【2017年5月30日付け閣議決定】
     1. 本文

ドキュメントを参照: [ITsengen\_honbun.pdf](https://cio.go.jp/sites/default/files/uploads/documents/ITsengen_honbun.pdf)

* + - 1. 第１部 総論 . 3
         1. Ⅰ IT 戦略の新たなフェーズに向けて（「データ」がヒトを豊かにする社会の実現） 3

Ⅰ－１ これまでのIT 戦略 3

Ⅰ－２ IT 戦略の新たなフェーズに向けて（「データ」大流通時代の到来） 3

Ⅰ－３ 「データ」の上で、 ヒト、 モノ、 カネが活いきる社会 . 5

Ⅰ－４ 「データ」がヒトを豊かにする社会、 「官民データ利活用社会」のモデル構築 . 6

* + - * 1. Ⅱ 「官民データ利活用社会」のモデルの構築に向けて 8

Ⅱ－１ IT をめぐる諸動向 8

Ⅱ－１－(1) 技術・サービスの動向等 . 8

Ⅱ－１－(2) データ利活用への期待の高まり . 9

Ⅱ－２ 我が国の置かれた状況等 10

Ⅱ－２－(1) 急速な人口構造の変化等に伴う諸課題 10

Ⅱ－２－(2) 今の国民が生活において求めるもの（国民視点での取組の強化） 10

Ⅱ－３ 「官民データ利活用社会」のモデルの構築 11

Ⅱ－３－(1) 我が国の置かれた諸状況を踏まえたデータ利活用による新たなライフスタイルの提案 . 11

Ⅱ－３－(2) 官民データの利活用に向けた環境整備 12

Ⅱ－３－(3) 我が国が目指す社会の構築等 14

* + - * 1. Ⅲ 推進体制 .15

Ⅲ－１ 官民データ活用推進基本計画のPDCA . 15

Ⅲ－２ 他の推進本部等との連携 16

* + - * 1. Ⅳ 地方公共団体との連携・協力 .18
        2. Ⅴ 事業者等との連携・協力 .18
      1. 第２部 官民データ活用推進基本計画 . 20
         1. Ⅰ 官民データ活用推進基本計画に基づく推進の施策 .20

Ⅰ－１ 官民データ活用の推進に関する施策についての基本的な方針 20

Ⅰ－１－(1) 基本計画の策定とその着実な実施 20

Ⅰ－１－(2) 重点分野の指定（分野横断的なデータ連携を見据えつつ） 21

Ⅰ－１－(3) 国と各地方公共団体の施策の整合性の確保 23

Ⅰ－１－(4) 成果の横展開 24

Ⅰ－１－(5) 官民データ活用によるEBPM の推進 . 24

Ⅰ－２ 具体的施策 25

* + - * 1. Ⅱ 施策集 37

Ⅱ－１

Ⅱ－１－(1) 行政手続等のオンライン化原則【基本法第10 条関係】 39

Ⅱ－１－(2) オープンデータの促進【基本法第11 条第１項及び第２項関係】、 データの円滑な流通の促進【基本法第11 条第３項関係】 44

Ⅱ－１－(3) データ利活用のルール整備【基本法第12 条関係】 52

Ⅱ－１－(4) マイナンバーカードの普及・活用【基本法第13 条関係】 56

Ⅱ－１－(5) 利用の機会等の格差の是正（デジタルデバイド対策）【基本法第14 条関係】. 61

Ⅱ－１－(6) 情報システム改革・業務の見直し【基本法第15 条第１項関係】 65

Ⅱ－１－(7) データ連携のためのプラットフォーム整備【基本法第15 条第２項関係】 70

Ⅱ－１－(8) 研究開発【基本法第16 条関係】 77

Ⅱ－１－(9) 人材育成、 普及啓発等【基本法第17 条、 第18 条関係】 . 83

Ⅱ－１－(10) 国の施策と地方の施策との整合性の確保等【基本法第19 条関係】 . 88

Ⅱ－１－(11) 国際貢献及び国際競争力の強化に向けた国際展開 89

* + 1. 別表

ドキュメントを参照: [ITsengen\_beppyo.pdf](https://cio.go.jp/sites/default/files/uploads/documents/ITsengen_beppyo.pdf)

* + 1. 用語集 【後日、 別シートに移行予定】

ドキュメントを参照: [ITsengen\_yougosyu.pdf](https://cio.go.jp/sites/default/files/uploads/documents/ITsengen_yougosyu.pdf)

* + - 1. アクセシビリティ
         1. 情報通信分野においては、 高齢者や障害者等、 ハンディを持つ人にとって、 情報やウェブサービス、 ソフトウェア等が円滑に利用できることを意味する。
      2. アジャイル
         1. ソフトウェア開発手法の1 つで、 開発対象を多数の小さな機能に分割し、 反復(イテレーション) と呼ばれる短い開発期間単位ごとに1 つの機能を開発・ソフトウェアリリースを行う手法である。 短いサイクルで一連のPDCA を回す開発手法であり、 日々生じる変化にすばやく適応することに主眼が置かれている。
      3. 医療等ID
         1. 医療等ID は、 患者の医療情報の連携や研究利用など、 保健医療分野の情報連携を安全で効率的に行うための、 一意的な識別子のことである。 「医療等分野における番号制度の活用等に関する研究会」(平成27 年12 月報告書取りまとめ)において、 具体的な制度設計等が取りまとめられた。
      4. ウェアラブル端末
         1. 腕や頭部などの身体に装着して利用する情報端末のこと。 デバイスに搭載されたセンサーを通じて装着している人の生体情報を取得・送信し、 クラウド上で解析しフィードバックすることで、 フィットネスやヘルスケア分野などでの活用が期待されている。 また、 スマートフォンと連携してのハンズフリーでのアプリ操作や、 産業分野での作業支援などにも使われ始めている。
      5. オープンデータ
         1. 一般的には、 データは誰もが制限なしにアクセス、 再利用、 そして再配布できるように、 利用可能にすべきであるという概念のことであるが、 本戦略においては、 公的機関が保有するデータを、 民間が編集・加工等をしやすい形で、 インターネットで公開することを意味する。
      6. オープンデータ・バイ・デザイン
         1. 行政が保有するデータについて、 オープンデータを前提として情報システムや業務プロセス全体の企画、 整備及び運用を行うこと。
      7. おもてなしシステム
         1. 訪日外国人の同意の下、 属性（性別・年代・国籍等）や行動履歴（宿泊・買い物・移動等）に関するデータを事業者間で共有・活用し、 先進的かつ多様なサービス・決済環境を提供する仕組みのこと。
      8. 海事生産性革命(i-Shipping)
         1. IT を利活用して船舶の設計から建造、 運航に至る全てのフェーズにおいてイノベーションの創出・生産性向上を目指す政府の取り組みの総称。
      9. 課題解決型オープンデータ
         1. データの公開のみにとどまらず、 公開されたデータを積極的に利活用することによって様々な社会課題の解決を目指す、 オープンデータに係る取組のこと。
      10. 共通語彙基盤
          1. 氏名や住所等語彙の表記・意味・データ構造を共通化してデータの交換・活用を容易にする基盤のこと。
      11. 業務改革（BPR）
          1. BPR はBusiness Process Reengineering の略である。 既存の組織やビジネスルールを抜本的に見直し、 利用者の視点に立って、 業務プロセス全体について職務、 業務フロー、 管理機構、 情報システムを再設計すること。
      12. クラウドサービス
          1. インターネット等のブロードバンド回線を経由して、 データセンタに蓄積されたコンピュータ資源を役務（サービス）として、 第三者（利用者）に対して遠隔地から提供すること。
      13. クラウド・バイ・デフォルト
          1. システム導入に際し、 クラウドサービスの活用を前提とする考え方のこと。
      14. 公共価値
          1. 制度の不知等利用者の置かれた環境にかかわらず、 公平・公正な行政サービスを享受できること、 行政サービスの利用が簡便でメリットがあること、 また、 行政機関が保有する資産を利用することで新たなビジネスを創造できること等、 利用者たる国民等にとっての行政サービスの有用性を意味する。
      15. 公的個人認証サービス
          1. 公的個人認証サービスとは、 オンラインで（＝インターネットを通じて）申請や届出といった行政手続などやインターネットサイトにログインを行う際に、 他人による「なりすまし」やデータの改ざんを防ぐために用いられる本人確認の手段。 「電子証明書」と呼ばれるデータを外部から読み取られるおそれのないマイナンバーカード等のIC カードに記録することで利用が可能となる。
          2. 電子証明書には、 以下の２種類がある。
          3. 署名用電子証明書・・・インターネット等で電子文書を作成・送信する際に利用（例 e-Tax 等の電子申請）。 「作成・送信した電子文書が、 利用者が作成した真性なものであり、 利用者が送信したものであること」を証明する。
          4. 利用者証明用電子証明書・・・インターネットサイトやコンビニ等のキオスク端末等にログインする際に利用（例 マイナポータルへのログイン、 コンビニでの公的な証明書の交付）。 「ログインした者が、 利用者本人であること」を証明。
      16. コネクテッドカー
          1. 情報端末としての機能を有する自動車のことであり、 車両の状態や周囲の道路状況などの様々なデータをセンサーにより取得し、 ネットワークを介して集積・分析することで、 新たな価値を生み出すことが期待されている。
      17. コネクテッド・ワンストップ
          1. 民間サービスを含め、 複数の手続・サービスがどこからでも一か所で実現 することを原則とする考え方のこと。
      18. サービスデザイン思考
          1. サービスを利用する際の利用者の一連の行動に着目し、 利用者がその手続を利用しようとした背景や、 手続を利用するに至るまでの過程、 利用後の行動までを一連の流れとして捉え、 利用者の心理や行動等を含めた体験（UX：ユーザーエクスペリエンス）全体を最良とすることを目標にしてサービス全体を設計する考え方のこと。
      19. シェアリングエコノミー
          1. 個人等が保有する活用可能な資産等（スキルや時間等の無形のものを含む。 ）を、 インターネット上のマッチングプラットフォームを介して他の個人等も利用可能とする経済活性化活動のこと。
      20. 準天頂衛星
          1. 日本で常に天頂付近に１機以上の測位衛星が位置し、 複数の軌道面にそれぞれ配置された測位衛星を組合せて位置を測定する衛星及びそのシステムのこと。 全国をほぼ100%カバーする高精度の衛星測位サービスの提供が可能である。
      21. 情報銀行
          1. 情報利用信用銀行の略で、 個人とのデータ活用に関する契約等に基づき、 PDS等のシステムを活用して個人のデータを管理するとともに、 個人の指示又は予め指定した条件に基づき個人に代わり妥当性を判断の上、 データを第三者（他の事業者）に提供する事業のこと。 データの提供・活用に関する便益は、 データ受領事業者から直接的又は間接的に本人に還元される。
      22. スマートホーム
          1. IoT 技術等によって家庭内の機器をネットワークでつなぎ、 制御することで、 生活者のニーズに応じた効率的かつ快適なサービスの提供を可能とした住まいのこと。
      23. 政府共通プラットフォーム
          1. 「新たな情報通信技術戦略」(平成22 年５月IT 戦略本部決定)に基づき、 国の行政情報システム全体の運用コストの削減、 セキュリティ強化等を図ることを目的とする情報システム基盤。 クラウドコンピューティング技術を活用した本基盤（平成25 年３月から稼働）の活用により、 各府省が別々に整備・運用している行政情報システムを可能なものから統合・集約化している。
      24. 政府統計の総合窓口（e-Stat）
          1. 各府省が公表する統計データを一つにまとめ、 統計データの検索をはじめとした、 さまざまな機能を備えた政府統計のポータルサイトのこと。 各府省が公表している統計表をExcel・CSV・PDF 形式でダウンロードすることが可能。
      25. 地理空間情報（Ｇ空間情報）
          1. 地理空間上の特定の地点又は区域の位置を示す情報（位置情報）と、 これに関連付けられた様々な情報のこと。
      26. ディープラーニング
          1. ニューラルネットワーク（機械学習におけるアルゴリズムの1 つ）を用いた機械学習における技術の1 つである。 情報抽出を一層ずつ多階層にわたって行うことで、 高い抽象化を実現する。 従来の機械学習では、 学習対象となる変数（特徴量）を人が定義する必要があった。 ディープラーニングは、 予測したいものに適した特徴量そのものを大量のデータから自動的に学習することができる点に違いがある。
      27. デジタルデバイド
          1. インターネットやパソコン等の情報通信技術を利用できる者と利用できない者との間に生じる格差のこと。
      28. デジタルファースト
          1. デジタル技術を徹底的に活用し、 デジタル処理を前提としたサービス設計を行うこと。
      29. データ取引市場
          1. データ保有者と当該データの活用を希望する者を仲介し、 売買等による取引を可能とする仕組み（市場）のこと。 価格形成・提示、 需給マッチング、 取引条件の詳細化、 取引対象の標準化、 取引の信用保証等の機能を担うことが想定される。
      30. テレワーク
          1. テレワークとは、 ICT を活用し、 場所や時間を有効に活用できる柔軟な働き方のことであり、 雇用型と自営型に大別される。 雇用型テレワークとは、 ICT を活用して、 労働者が所属する事業場と異なる場所で、 所属事業場で行うことが可能な業務を行うこと（例：在宅勤務、 モバイルワーク、 サテライトオフィスでの勤務）を言い、 自営型テレワークとは、 ICT を活用して、 請負契約等に基づき、 遠隔で、 個人事業者・小規模事業者等が業務を行うこと（例：ＳＯＨＯ、 在宅ワーク、 クラウドソーシング）を言う。
      31. 電子委任状
          1. 法人の代表者から与えられている権限の範囲を表示する電磁的記録のこと。
      32. 匿名加工情報
          1. 特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、 当該個人情報を復元することができないようにしたもののこと。
          2. 匿名加工情報は、 個人情報に関するルールは適用されず、 加工基準に従った加工その他の一定のルールのもと、 本人の同意を得ることなく自由に利活用することができる。 これにより、 新事業や新サービスの創出や、 国民生活の利便性の向上に寄与することが期待される。
      33. 農地情報公開システム
          1. 農地の集積・集約化を進めるため、 各市町村の農業委員会が整備している農地台帳に基づく農地情報を電子化・地図化して公開する全国一元的なクラウドシステム（平成27 年４月稼働）のこと。
      34. バックオフィス連携
          1. 地方公共団体を含む各行政機関が保有する情報を行政機関間でやり取りすること。 行政手続の際に必要な添付書類の省略を始めとした利便性の向上等が期待される。
      35. ビッグデータ
          1. ボリュームが膨大でかつ構造が複雑であるが、 そのデータ間の関係性などを分析することで新たな価値を生み出す可能性のあるデータ群のこと。 例えば、 ソーシャルメディア内のテキストデータ・画像、 携帯電話・スマートフォンが発信する位置情報、 時々刻々と生成されるセンサデータなどがある。
      36. 府省庁連携災害情報共有方式(SIP4D)
          1. 府省庁横断で災害情報を共有する仕組みのこと。
      37. ブロックチェーン
          1. 複数のデータを塊り（ブロック）にし、 暗号化してチェーンのように繋ぎ合わせて情報を管理する仕組みのこと。 複数の端末で運用するため、 耐障害性が高く、 またデータの改竄もほぼ不可能と言われている。
      38. 法人インフォメーション
          1. 政府の許認可、 委託契約受注、 補助金交付、 表彰受賞等の法人の情報等を一括で検索、 閲覧できるWeb システムのこと。
      39. 法人番号
          1. 設立登記法人、 国の機関、 地方公共団体、 その他の法人や人格のない社団等に対し、 国税庁長官より1 法人につき1 つ指定される13 桁の番号のこと。 マイナンバーとは異なり、 自由な利活用が可能。 なお、 法人の支店や事業所、 個人事業主等には法人番号は指定されない。
      40. マイナポータル
          1. マイナンバー制度の導入に併せて新たに構築した、 国民一人ひとりがアクセスできるポータルサイトのこと。 具体的には、 自己情報表示機能、 情報提供等記録表示機能、 プッシュ型サービス、 ワンストップサービス等を提供する基盤であり、 国民一人ひとりが様々な官民のオンラインサービスを受けられるよう、 平成29 年秋頃に本格運用を開始予定である。
      41. マイナンバー（個人番号）
          1. 日本国内に住民票を有する全ての方が一人につき1 つ持つ12 桁の番号のこと。
          2. 外国籍でも住民票を有する方には住所地の市町村長から通知される。 マイナンバーは行政を効率化し、 国民の利便性を高め、 公平、 公正な社会を実現するための社会基盤。 その利用範囲は法令等で限定されており、 平成28 年1 月から順次、 社会保障、 税、 災害対策分野の行政手続で利用されている。
      42. 官民ラウンドテーブル
          1. 行政運営上の意見交換や懇談の場のことであり、 官民が我が国の向上・活性化に向けて、 持続的な対話を行っていくことを目的としている。
      43. リカレント教育
          1. 近年の技術革新の著しい進展や産業構造の変化などに対応して学校教育の終了後、 技術系人材を含む職業人を中心とした社会人に対して行われる教育のこと。
      44. レセプトデータ
          1. レセプト（保険医療機関又は保険薬局が保険者に医療費を請求する際に提出する診療報酬明細書や調剤報酬明細書）に記載されているデータのこと。
      45. レピュテーションリスク（風評リスク）
          1. 企業に関する否定的な評価・評判が世間に周知されることで企業の信用やブランド価値等が悪化し、 結果的に損失を被るリスクのこと。
      46. ワンスオンリー
          1. 一度行政機関が提出を受けた情報は、 原則再度の提出を求めない仕組みのこと。
      47. ４Ｋ
          1. 現行のハイビジョンを超える解像度の映像のこと。 水平方向の画素数が約4 千であることから、 4K と呼ばれる。 超高精細度テレビジョン放送に対応する規格として、 平成24 年にITU（国際電気通信連合）で勧告化されるなど、 国際標準化がなされている。 4K は現行ハイビジョンの4 倍の解像度となる。
      48. ５Ｇ
          1. 「超高速」だけでなく、 「多数接続」「超低遅延」といった特徴を持ち、 平成32 年の実現が期待されている次世代の移動通信システムのこと。 我が国においても産学官連携の推進団体である「第５ 世代モバイル推進フォーラム（5GMF）」の設立（平成26 年９月30 日）、 研究開発の推進、 国際連携の強化などの取組が進められている。 現行LTE と比べて100 倍の接続機器数（100 万台/km2）、 100 倍の通信速度（10Gbps）などが要求条件とされており、 ITU をはじめ、 世界各国でも実現に向けた取組が本格化している。
      49. ８Ｋ
          1. 現行のハイビジョンを超える解像度の映像のこと。 水平方向の画素数が約8 千であることから、 8K と呼ばれる。 超高精細度テレビジョン放送に対応する規格として、 平成24 年にITU（国際電気通信連合）で勧告化されるなど、 国際標準化がなされている。 8K は現行ハイビジョンの16 倍の解像度となる。
      50. 人工知能（AI）
          1. Artificial Intelligence（人工知能）の略である。 コンピュータを使って、 学習・推論・判断など人間の知能のはたらきを人工的に実現するための技術。
      51. API
          1. Application Programming Interface の略。 複数のアプリケーション等を接続（連携）するために必要なプログラムを定めた規約のこと。
      52. AR（拡張現実）
          1. Augmented Reality の略である。 現実の環境にコンピュータを用いて情報を付加することにより人工的な現実感を作り出す技術の総称。 情報を付加された環境そのものを示すこともある。
      53. CIO
          1. Chief Information Officer の略である。 日本語では「最高情報責任者」「情報システム担当役員」「情報戦略統括役員」などと訳される。 企業や行政機関等といった組織において情報化戦略を立案、 実行する責任者のこと。
      54. e-ラーニング
          1. パソコンやタブレット、 スマートフォンを使ってオンラインで学ぶ学習形態のこと。
      55. EBPM
          1. Evidence Based Policy Making の略で、 統計や業務データなどの客観的な証拠に基づく政策立案のこと。
      56. Fintech
          1. 金融（Finance）と技術（Technology）を掛け合わせた造語であり、 主に、 ITを活用した革新的な金融サービス事業を指す。
      57. HHI
          1. Herfindahl-Hirschman Index（ハーフィンダール・ハーシュマン指数）の略である。 当該市場における各事業者の有するシェアの二乗和として算出され、 市場集中度を表す指標のこと。
      58. i-Construction
          1. 調査・測量から設計、 施工、 検査、 維持管理・更新までの全ての建設生産プロセスでICT 等を活用して、 建設現場の生産性の向上を目指す。
      59. IoT
          1. Internet of Things（モノのインターネット）の略である。 自動車、 家電、 ロボット、 施設などあらゆるモノがインターネットにつながり、 情報のやり取りをすることで、 モノのデータ化やそれに基づく自動化等が進展し、 新たな付加価値を生み出すというコンセプトを表した語である。
      60. ITS
          1. Intelligent Transport Systems（高度道路交通システム）の略である。 道路交通の安全性、 輸送効率、 快適性の向上等を目的に、 最先端の情報通信技術等を用いて、 人と道路と車両とを一体のシステムとして構築する新しい道路交通システムの総称。
      61. KPI
          1. Key Performance Indicators の略で、 目標の達成度を評価するための主要な評価指標のこと。
      62. Ｌアラート（災害情報共有システム）
          1. 避難勧告・指示等といった、 安心・安全に関わる公的情報など、 住民が必要とする情報が迅速かつ正確に住民に伝えられることを目的とした情報基盤のこと。 全国の情報発信者（地方公共団体等）が発信した情報を、 地域を越えて全国の情報伝達者（メディア等）に一斉に配信できるので、 住民はテレビ、 ラジオ、 携帯電話、 ポータルサイト等の様々なメディアを通じて情報を入手することが可能となる。
      63. MVNO
          1. Mobile Virtual Network Operator の略で仮想移動体通信事業者のこと。
      64. PDS
          1. Personal Data Store の略で、 他者保有データの集約を含め、 個人が自らの意思で自らのデータを蓄積・管理するための仕組み（システム）のこと。 第三者への提供に係る制御機能（移管を含む）を有する。 運用形態としては、 個人が自ら保有する端末等でデータを蓄積・管理する（事業者は本人の同意によりデータを活用できる）分散型と、 事業者が提供するサーバ等でデータを蓄積・管理する（個人は当該事業者にデータの蓄積・管理を委託する）集中型がある。
          2. 実際にデータをやり取りする形態と、 データをやり取りせず必要な時にアクセス権（閲覧のみ可、 コピー不可など）を提供・管理する形態もある。
      65. PHR
          1. Personal Health Record の略である。 個人が自らの生活の質(QOL=Quality of Life)の維持や向上等を目的として、 自らの健康に関する情報を収集・保存・活用する仕組みのこと。
      66. SNS
          1. Social Networking Service(Site)の略である。 個人間の交流を支援するサービス（サイト）で、 参加者は共通の興味、 知人などをもとに様々な交流を図ることができる。
      67. Society5.0
          1. 狩猟社会、 農耕社会、 工業社会、 情報社会に続くような新たな社会を生み出す変革を科学技術イノベーションが先導していく、 という概念である。
      68. VR
          1. Virtual Reality の略である。 コンピュータ上に仮想的な世界を作り出し、 あたかも現実にそこにいるかの様な体験をさせる技術。 \_\_
    1. 概要

ドキュメントを参照: [ITsengen\_gaiyou.pdf](https://cio.go.jp/sites/default/files/uploads/documents/ITsengen_gaiyou.pdf)

* 1. 「政府情報システムの整備及び管理に関する標準ガイドライン」(2015年3月19日更新、 2014年12月3日各府省CIO連絡会議決定）および「実務手引書」

ドキュメントを参照: [infosystem-guide.html](http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/infosystem-guide.html)

* + 1. http://www.soumu.go.jp/main\_sosiki/gyoukan/kanri/infosystem-guide.html

ドキュメントを参照: [infosystem-guide.html](http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/infosystem-guide.html)

* + 1. 世界最先端IT国家創造宣言(2013年6月14日閣議決定。 2014年6月24日変更)に基づき、 政府におけるITガバナンス強化のため、 情報システム調達やプロジェクト管理に関する共通ルールとして策定
  1. 人材育成・人材確保
     1. IT人材白書2017【2017年4月25日IPA】

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

* + - 1. デジタル大変革時代、 本番へ
         1. 時代環境が大きく変わる時、 それにそぐわないビジネスは淘汰されていく
         2. デジタル変革とも呼ぶべき第4次産業革命の入り口にいる
         3. デジタル時代にふさわしい新たなビジネスを生み出して行く必要がある

旧来の仕組みの高度化、 洗練は否定されるべきではないが

* + - * 1. デジタルトランスフォーメーション が重要

仕事の進め方や社会のあり方をゼロベースで刷新し、 時代に適合するように自らを変える

* + - * 1. それに歩みを進めるかどうか、 つまり企業の方向性を決めるのは、 言うまでもなく経営者

経営者の役割： 時代の潮流を捉え、 自社が変化の中で発展できる道を探り、 ビジョンをはっきりと示す

* + - * 1. 同時に従来から続く組織構造の破壊や再構築も必要

求められるのは、 周囲を巻き込みながら改革を進める能力やビジネスとデジタルを結び付けて全体をデザインする能力を持った新しい時代のリーダー

ITエンジニアがリーダーへと成長するには挑戦する意欲を持つ

さまざまな経験を積み、 多様な人と関わる環境が必要

* + - * 1. 企業が行わなければならないのは、 誰もが挑戦できる環境、 開かれた場を作ること
        2. 個々のIT人材は、 自らも デジタルトランスフォーメーション の流れの中にあることを意識

その中で活躍できる人材となれるように、 自らの能力を高めていくことが重要である

そのためには情報への感度を高め、 自ら挑戦する場を求める姿勢が重要になる。 普段の仕事に専念しているだけでは不十分と考えなければならない。

* + - 1. 企業に向けたメッセージ
         1. IT企業

デジタル変革が進む中では、 IT企業は デジタルトランスフォーメーション に資する技術力や提案力を磨き、 ユーザー企業のパートナーとして新たな事業価値を生み出していく役割を担う必要がある。

そのためにはユーザー企業やベンチャー企業などとの「協働」関係を築くことも欠かせない。

* + - * 1. ユーザー企業（IT部門）

デジタルトランスフォーメーション を推進するのか、 それとも現状維持を選択するのか。

第4次産業革命が進むにつれて、 発展するビジネスと縮小するビジネスが明確になっていく。

CIOやIT部門は、 そのことを認識し、 変化を主導する側に立つ必要がある。

そのために一刻も早く現状把握を行い、 ビジョンを明確にし、 戦略を遂行しなければならない。

デジタルトランスフォーメーション を実現するには、 ビジネスとデジタルのスキルを併せ持った人材が重要となる。

それがあって初めて、 イノベーティブなデジタル技術を持つ企業や、 他業種など多様な企業間での連携を進められる

その視点に立って、 人材の育成と獲得をしていく必要がある。

従来、 社内でIT業務の中核を担ってきたIT部門は今、 再び挑戦を迫られている。

デジタル変革に伴って生じる新たな事業や業務において重要な役割を担うことへの挑戦でもある。

* + - 1. IT人材個人に向けたメッセージ
         1. デジタル時代は、 個々のIT人材にとって活躍の場を広げられるまたとないチャンスである。
         2. 所属する企業で新たな試みをすることもできるし、 起業のチャンスも開けている。
         3. クラウドコンピューティングやモバイルの進展で、 個人や少数のチームでできることが飛躍的に拡大している
         4. このことを認識し、 目の前の業務だけにとらわれることなく、 広く視野を持って進むべき道を探り、 学ぼう。 勉強会やコミュニティなど、 学びの場は周囲にある。 自己研鑽によって能力を高めれば高めただけ、 社会をリードする人材になっていく。
      2. 1．デジタルトランスフォーメーション時代のIT人材
         1. デジタルトランスフォーメーション とは何か

ITの進展やインフラの整備によって、 ビジネスや社会のあり方が変わり始めている。

あらゆるものがインターネットに接続するIoTの拡がりや、 ビッグデータ活用、 人工知能（AI）の様々な分野への適応が始まっている。

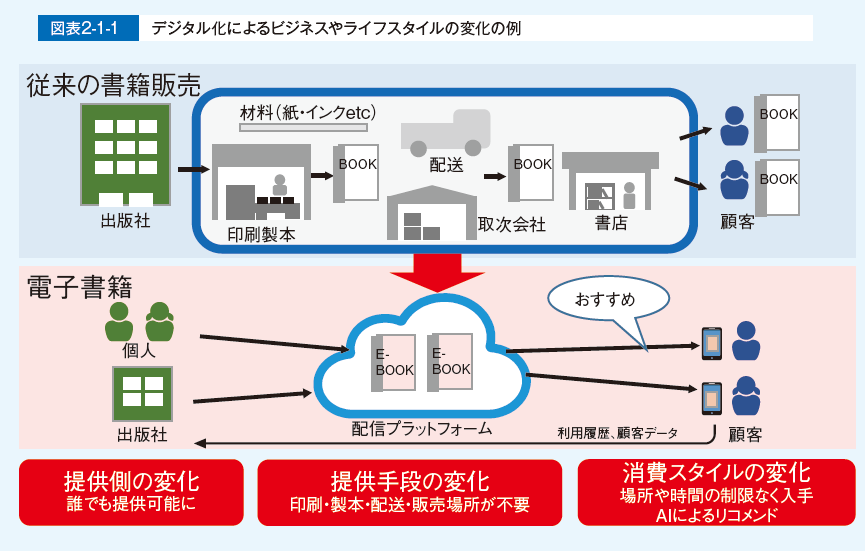
デジタル化を進めるということは、 様々な要素（アナログデータも含む）をデジタル化、 数値化して扱うことを意味する。

共通に扱えるデータへと変換することによって、 処理や分析が可能になり、 フィードバックまで含めた一連の流れを作ることが可能になる。

デジタル化の本質は、 以上のようなデータ駆動型へのビジネスや社会の変革にある。

既存のビジネスや業務に新技術を取り入れるだけでなく、 ビジネスモデルを変え、 経済活動のみならず、 個人の生活や社会構造にまで影響が及ぶ。

その変化は、 デジタルトランスフォーメーション や デジタル革命 と呼ばれている。

Subtopic  


デジタル化によって起こる変化の一例として、 紙の書籍から電子書籍へのデジタル化を図式化したものである。

* + - * 1. すでに始まっている デジタルトランスフォーメーション

「IoTやビッグデータ、 AIなど技術の進展等によって、 社会や産業、 企業、 人のあり方や働き方が大きく変化すると言われている。 この変化に対してどのように捉えているか」

ネットサービス実施企業は

、 「すでに変化の中にいる」が約40%である。 インターネットを活用し、 データを扱うビジネスを実施しているという性質上、 変化に対して敏感だと言える。

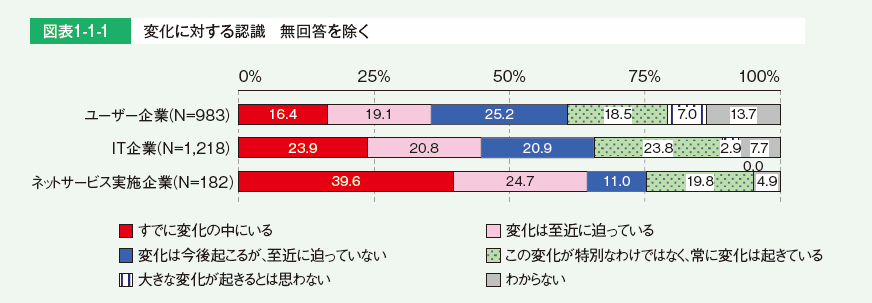
事業会社であるユーザー企業では

「変化は今後起こるが、 至近に迫っていない」という回答の割合が最も高い。

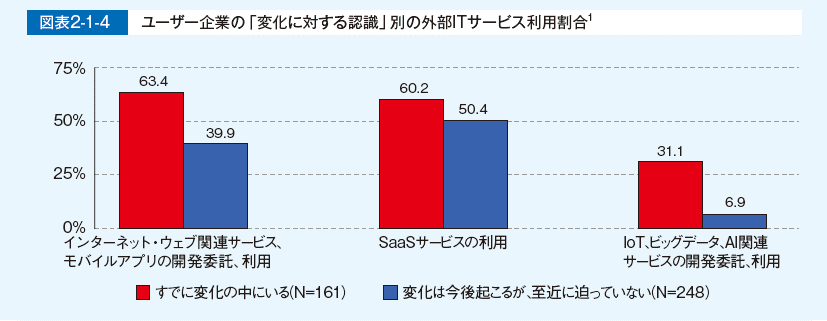
「大きな変化が起きるとは思わない」や「わからない」も他の企業区分に比較して高い割合を占めている。

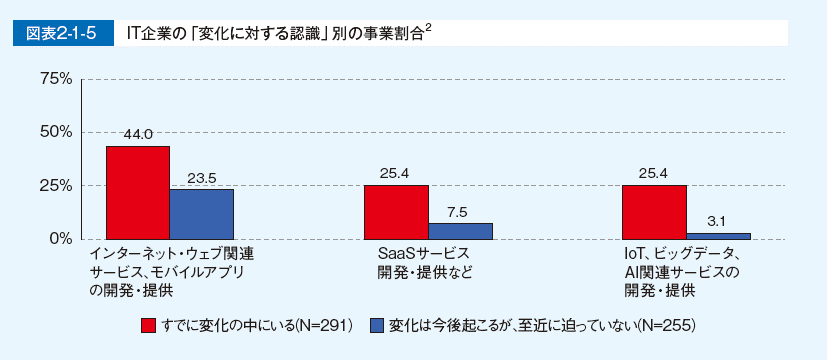
一方、 IT企業では、

「すでに変化の中にいる」、 「変化は至近に迫っている」、 「変化は今後起こるが、 至近に迫っていない」、 「この変化が特別なわけではなく、 常に変化は起きている」の回答割合がほぼ同率だった。

Subtopic  


* + - * 1. 外部ITサービス利用状況、 現在の事業【変化に対する認識別】

Subtopic  


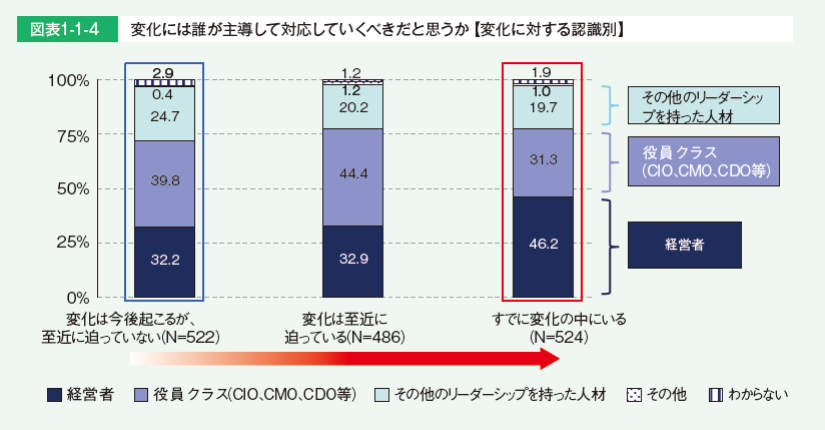
Subtopic  


* + - * 1. デジタルトランスフォーメーション が進む企業では、 経営者による主導の重要性を認識

デジタルトランスフォーメーションには、 大きな変化が伴うため、 業務の部分的なデジタル対応やIT導入による効率化のみでは対応できない。

変化 には誰が主導して対応していくべきか尋ねた。

「すでに変化の中にいる」企業では、 他の認識の企業に比べて「経営者」が主導していくべきだという回答の割合が高い。

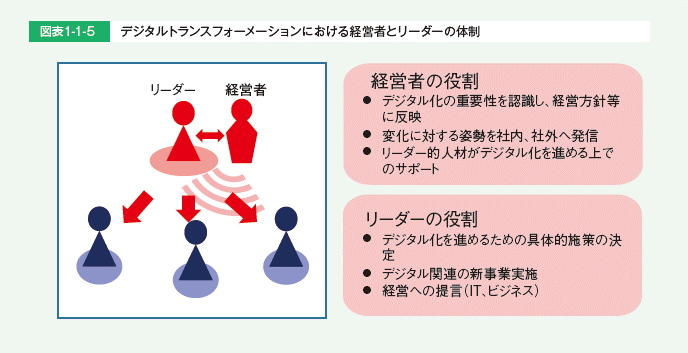
Subtopic  


* + - * 1. デジタルトランスフォーメーション の鍵を握るリーダー的人材

全体方針を示す経営者に加え、 具体的な推進を行う人材も存在している。

デジタル化の具体的な施策の決定や新事業の立ち上げなどを主導する、 リーダー的な役割を担う人材が大きな役割を果たしている。

この人材は、 例えばCIOや、 デジタル推進部門、 デジタル技術を用いた新事業部門、 IT系部門などに存在し、 それぞれのデジタル化を推進している。

Subtopic  


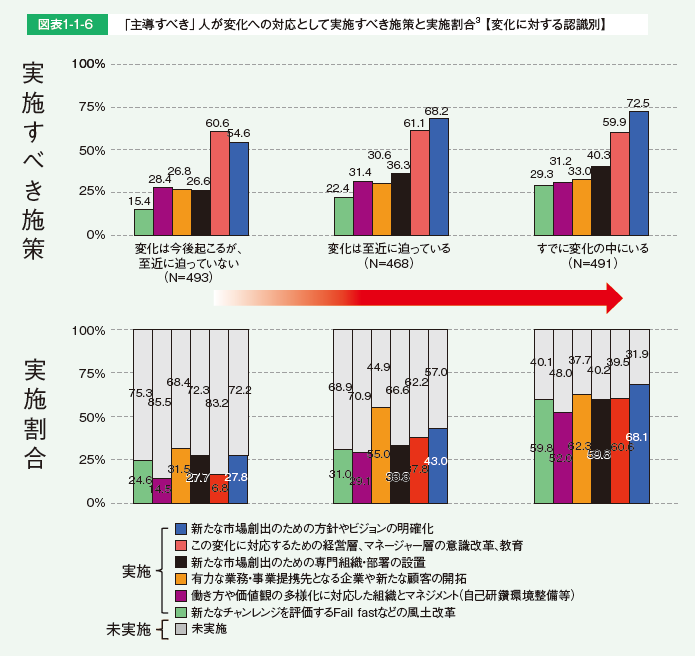
* + - * 1. 方針やビジョンの明確化」、 「専門組織・部署の設置」、 「Fail fastなどの風土改革」を重要視

デジタル化を「主導すべき」人が実施すべき施策

「新たな市場創出のための方針やビジョンの明確化」

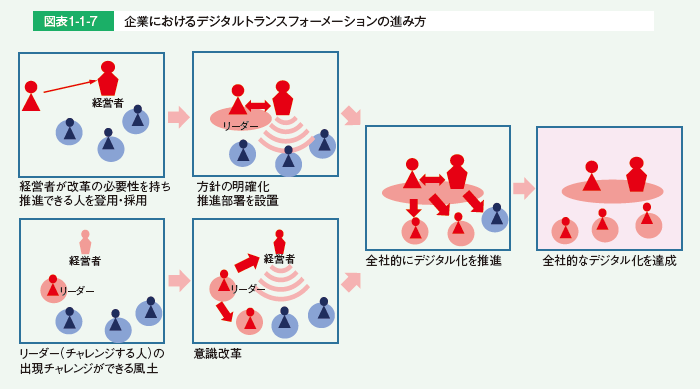
「新たな市場創出のための専門組織・部署の設置」

「新たなチャレンジを評価するFail fastなどの風土改革」

Subtopic  


* + - * 1. 経営者とリーダーが周囲を巻き込み、 改革を進める

リーダー的存在が企業内の複数個所に存在する場合もあるが、 経営者と現場に近いリーダーとがともに改革を進めていく大きな流れは変わらない。

Subtopic  


* + - * 1. デジタル化の推進をリードする人材に必要な能力と環境

・デジタル化を推進するリーダーに求められるのは、 他人を巻き込む力 、 ビジネスとデジタルの知見

・デジタル化を推進するリーダーが育ってきた背景は、 多様な経験と新しいものへの挑戦 、 ネットワーク、 外部とのつながり

・デジタル化を推進するリーダーの育成に重要となる環境の整備

Subtopic  


* + - * 1. デジタル化に携わる人材

必要な能力

もともと製品の社内開発・運用を行ってきた企業の場合、

社内に既存の技術力はあり、 加えて具体的な技術（データ解析やAI、 クラウド等）が求められている。

また、 具体的な要素技術だけでなく、 システムの構造設計を行い開発する能力（システムアーキテクト）の重要についても挙げられていた。

一方、 これまでITが深くかかわっていなかった事業がデジタル化した場合、

今までIT部門が行っていた外部企業への開発委託を事業部門が直接行うことになり、 ITを事業に適用する能力や、 機能設計や要件定義を行う能力が求められる。

人材の獲得方法と育成

事業のデジタル化に必要なIT能力を、 既存の人材でまかなうのは難しいとの意見があった。

デジタル化した事業を行っている企業では、 ネット系の企業等でデジタルビジネスの経験がある者を中途採用し、 事業の推進を行っている例が見られる。

また、 新しい技術（データ活用やAI、 IoTなど）を持った人材に関しては、 中途採用の難しさを挙げる企業が多く、 新卒採用した人材を育成して人材確保する傾向が見られ、 新卒を採用する際に理数系人材を重視する企業もいくつかあった。

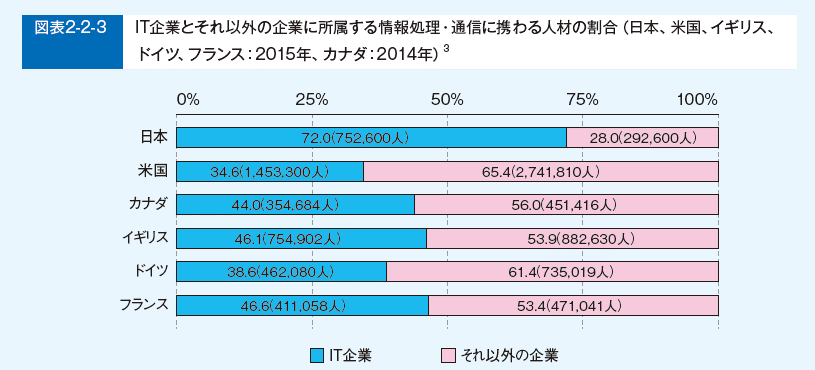
育成のスピードアップと高い技術力を持った人材の輩出につなげたい考えである。

ただし、 内部人材育成の難しさを挙げる企業もあり、 必要な技術を持った人材を中途採用できる場合は行い、 できない場合はアウトソーシングや、 外部との連携を行うことで技術を補完する場合もあった。

* + - 1. 2．日本と米国の情報処理・通信に携わる人材
         1. 日米、 欧州等の情報処理・通信に携わる人材の所属企業

日本はIT企業に所属する情報処理・通信に携わる人材の割合が72%と突出して高くなっている。

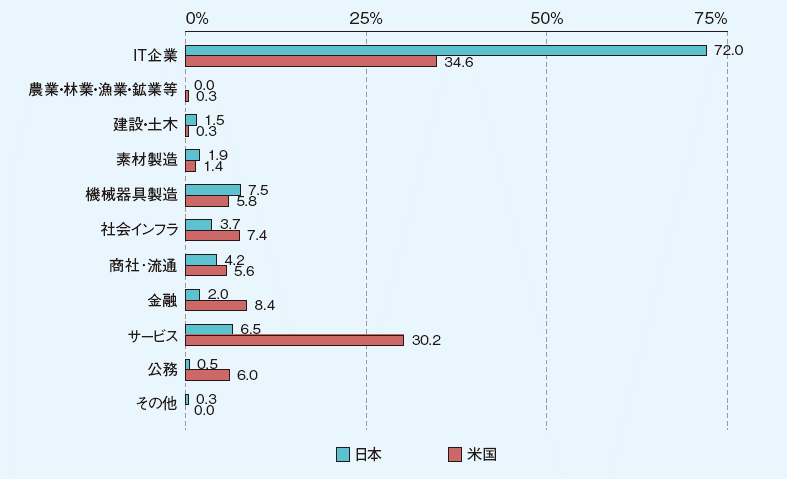
一方、 日本以外の国は、 IT企業以外の割合が5割を超えており、 米国はIT企業以外に所属する情報処理・通信に携わる人材の割合が65.4%と最も高くなっている。

Subtopic  


* + - * 1. 日米の情報処理・通信に携わる人材の業種別人材の割合

米国では、 「IT企業」に次いで「サービス」の割合が30.2%と高くなっている。

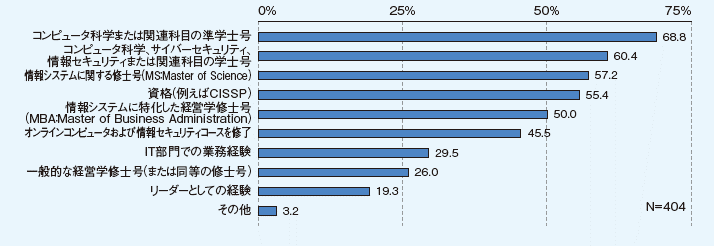
「金融」については日本の2%に対し米国では8.4%、 「公務」については日本の0.5%に対し米国が6%と、 日本より幅広い業種に情報処理・通信に携わる人材が所属していることがわかる。

Subtopic  


* + - * 1. 米国における情報セキュリティ技術者に必要なスキルや経験

「コンピュータ科学または関連科目の準学士号」の割合が68.8%と最も高く、 「コンピュータ科学、 サイバーセキュリティ、 情報セキュリティまたは関連科目の学士号」（60.4%）、 「情報システムに関する修士号（MS（Master of Science））」（57.2%）と続き、 学歴を重視する傾向が見られる。

「資格（例えばCISSP）」が55.4%と、 資格への関心も高い。

Subtopic  


* + - * 1. 米国の組織のCISOに必要なスキルや経験

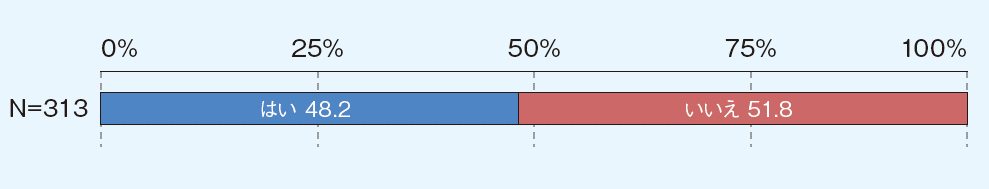
「リーダーとしての経験」の割合が92.1%と最も高く、 「IT部門での業務経験」（72.8%）、 「一般的な経営学修士号（または同等の修士号）」（71.3%）と続いている。

情報セキュリティ技術者にとって必要なスキルや経験の調査結果とは違い、 経験を重視する傾向が見られる。

Subtopic  


* + - * 1. 米国の組織におけるサイバーセキュリティ：トレーニングプログラム開発のための大学との連携・協業状況

約5割もの組織がサイバーセキュリティトレーニングプログラムの開発のために大学と連携・協業していることがわかる。

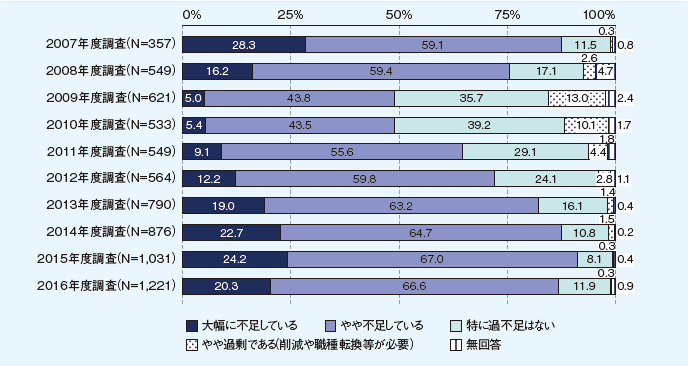
Subtopic  


* + - 1. 3．IT人材不足の動き
         1. IT人材の 量 に対する過不足感【過去10年の変化】

IT企業では、 リーマンショック以来高まり続けていたIT人材の 量 に対する不足感の高まりがやや緩和した。

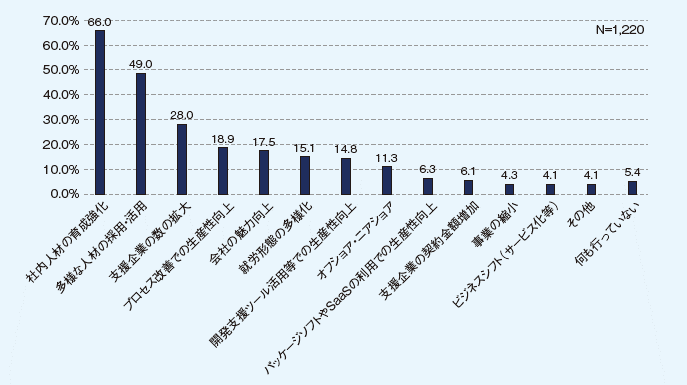
「大幅に不足している」と答えた割合が、 2015年度調査の24.2%から、 今年度では20.3%と減少している。

また、 「特に過不足はない」は2015年度調査の8.1%から、 今年度では11.9%と増加している。

Subtopic  


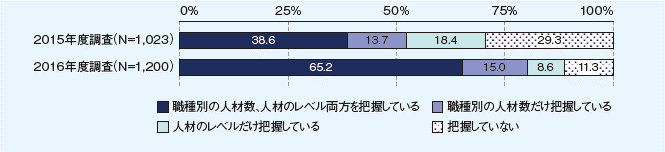
* + - * 1. 人材不足改善の取り組みのうち効果があったもの

「社内人材の育成強化」が最も多く、 66％に上っている。

Subtopic  


* + - * 1. IT人材の「職種別の人材数」と「人材のレベル」の把握状況【経年】

計画的な人材育成には人材把握が必要となるが、 今年度調査では、 「職種別の人材数、 人材のレベル両方を把握している」割合が大きく増加していた。

Subtopic  


* + - * 1. IT人材の 量 に対する過不足感【過去9年の変化】

2010年ごろに不足感が減少した以降、 2014年度調査までは不足感に大きな変化のなかったユーザー企業だが、 2015年度調査の結果ではIT人材の 量 について、 「大幅に不足している」「やや不足している」と回答した割合が増加した。

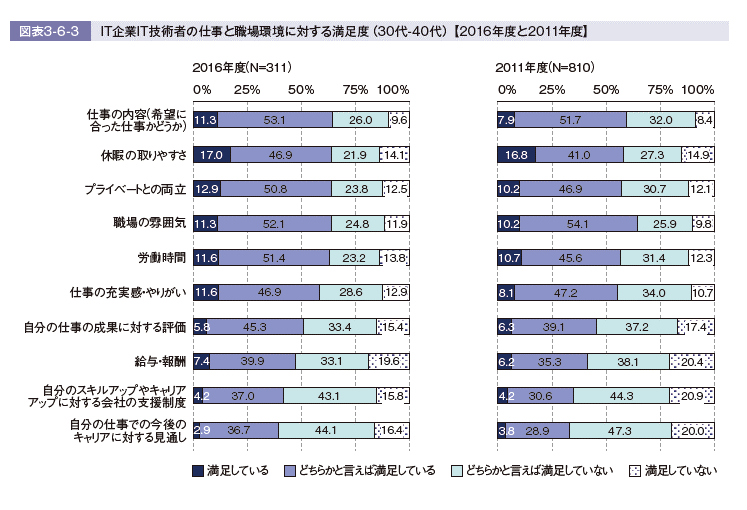
今年度も引き続き不足感が増す傾向にある。

Subtopic  


* + - 1. 4．IT人材動向（IT人材の意識の比較【2016年度と2011年度】）
         1. 仕事や職場の環境に対する満足度（30代-40代）【2016年度と2011年度】

2016年度、 2011年度共に「仕事内容（希望に合った仕事かどうか）」、 「休暇の取りやすさ」、 「プライベートとの両立」「職場の雰囲気」に対する満足度は高い。

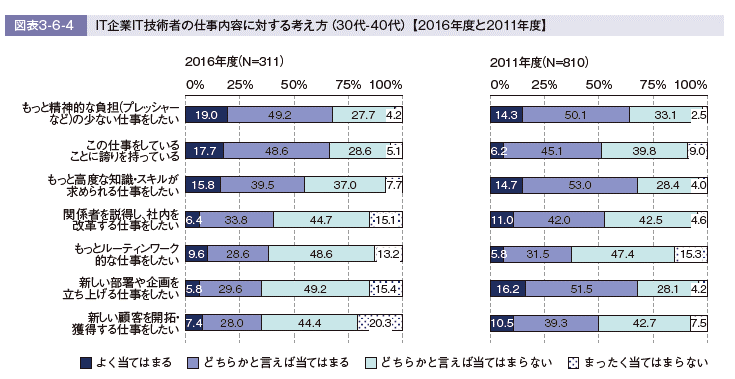
全項目に対して微増微少はあるが、 変化は読み取れない。

Subtopic  


* + - * 1. 仕事内容に対する考え方（30代-40代）【2016年度と2011年度】

「この仕事をしていることに誇りを持っている」では、 「よく当てはまる、 どちらかと言えば当てはまる」では2011年度の51.3％から2016年度の66.3％と増加した。

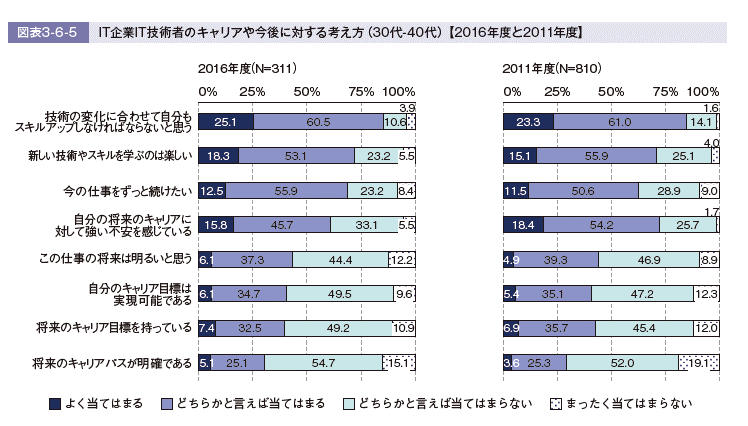
一方、 「新しい部署や企画を立ち上げる仕事をしたい」では「よく当てはまる、 どちらかと言えは当てはまる」の合計が、 2011年度の67.7％から2016年度の35.4％、 「関係者を説得し、 社内改革する仕事をしたい」も同様に2011年度53％から2016年度の40.2％と割合が低下している。

Subtopic  


* + - * 1. キャリアやスキルアップに対する考え方（30代-40代）2016年度と2011年度】

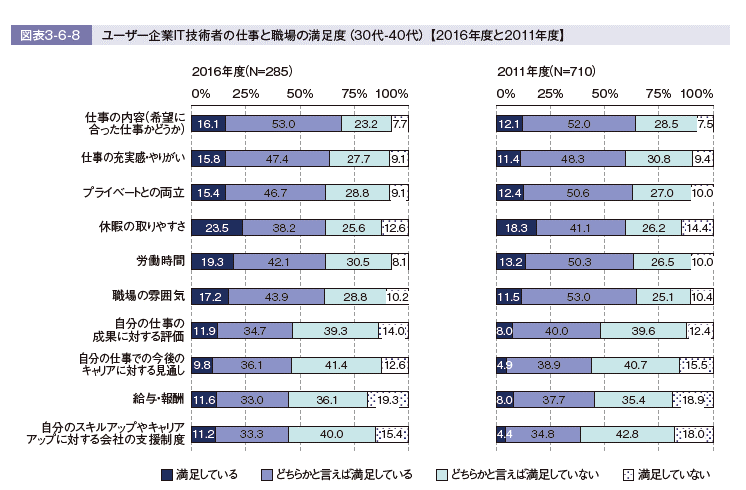
2016年度、 2011年度共に「技術の変化に合わせて自分もスキルアップしなければならないと思う」について「よく当てはまる、 どちらかと言えは当てはまる」と回答した割合は8割台半ばであり、 「新しい技術やスキルを学ぶのは楽しい」の割合も共に7割強である。

一方、 「将来のキャリアパスが明確である」で「よく当てはまる、 どちらかと言えは当てはまる」と回答した割合は2011年度と2016年度共に約3割であり傾向に変化はない。

Subtopic  


* + - * 1. 仕事と職場環境に対する満足度（30代-40代）【2016年度と2011年度】

全項目において「満足している」の割合が増加している。

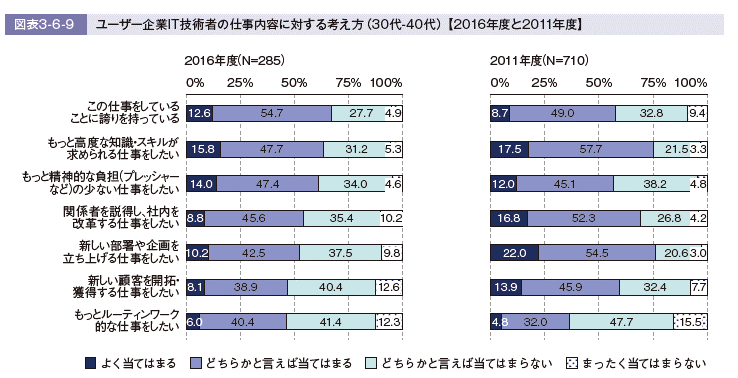
Subtopic  


* + - * 1. 仕事内容に対する考え方（30代-40代）【2016年度と2011年度】

「この仕事をしていることに誇りを持っている」では「当てはまる、 どちらかと言えは当てはまる」を合計した割合が2011年度の57.7％から2016年度の67.3％と増加している。

一方、 「新しい部署や企画を立ち上げる仕事をしたい」では「当てはまる、 どちらかと言えは当てはまる」の合計は、 2011年度の76.5％から2016年度の52.7％へと23.8ポイント低下した。

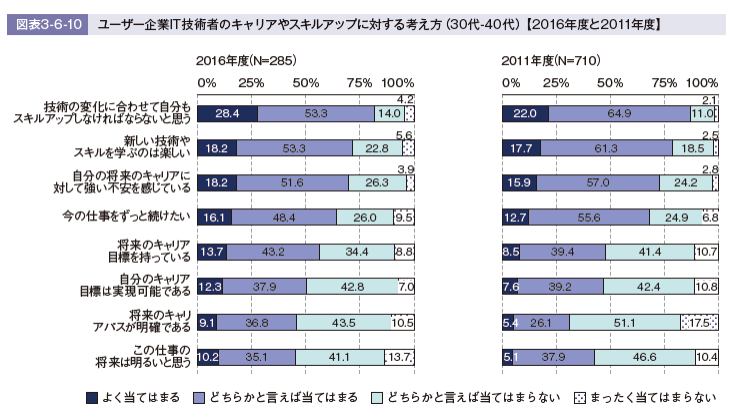
また、 「新しい顧客を開拓・獲得する仕事をしたい」の割合も2011年度の59.8％から2016年度の47％へと低下している。

Subtopic  


* + - * 1. キャリアやスキルアップに対する考え方（30代-40代）2016年度と2011年度】

「将来のキャリアパスが明確である」では「当てはまる、 どちらかと言えは当てはまる」を合計した割合が2011年度の31.5％から2016年度の45.9と増加し、 「将来のキャリア目標を持っている」、 「自分のキャリア目標は実現可能である」のいずれにおいても割合が増加している。

しかしその一方で、 「自分の将来のキャリアに対して強い不安を感じている」に対する「よく当てはまる」の割合はやや増加しており、 キャリアは明確なったものの、 不安感は弱まってはいないように見受けられる。

Subtopic  


* + 1. 情報技術者試験

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

* + 1. iコンピテンシディクショナリ

ドキュメントを参照: [i\_competency\_dictionary](https://www.ipa.go.jp/jinzai/hrd/i_competency_dictionary/)

* 1. 人材育成・人材確保【セキュリティ関連】
     1. ■ITのスキル指標を活用した情報セキュリティ人材育成ガイド【2015年5月IPA】

ドキュメントを参照: [000039528.pdf](http://www.ipa.go.jp/files/000039528.pdf)

* + - 1. あなたの企業に迫る脅威～ あなたの企業は大丈夫ですか？
      2. ＜脅威１＞ 標的型攻撃・サイバー攻撃
         1. 必要な対策は実施されていますか？

ウィルス対策ソフトを社内のすべてのコンピュータに導入し、 ウィルスチェックやウィルス対策ソフトの更新を頻繁に実施していますか。

社内のメール利用者に対して、 「怪しいメールは開封しない」、 「疑わしいメールのＵＲＬはクリックしない」、 「不審な添付ファイルは開かない」などの基本事項についての教育が徹底されていますか。

ウィルス対策ソフトから「ウィルスに感染した」という警告メッセージが表示された場合、 まず何をすればよいか、 すべての従業員が十分に理解していますか。

標的型攻撃を防御・検知するためのシステムの監視を行っていますか。 また、 そのような機能をもったセキュリティ対策ソフトを導入していますか。

ウィルス感染や情報漏えいが発覚した場合の組織としての緊急対応手順は定められていますか。 また、 その手順は関係者に周知されていますか。

* + - * 1. あなたの企業は 大丈夫？被害を防ぐためには、 こんな役割も重要です！

システム運用において、 セキュリティ障害管理 （事故の検知、 初動対応、 分析、 復旧等）のタスクを実行する役割

* + - * 1. その役割を担う人材の例

セキュリティ アドミニストレータ （インシデントハンドラ）

自社内のセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧業務の実施において、 自らあるいは適切な対応者をアサインして対応にあたる役割。 被害の拡大防止のために、 適切かつ迅速な対応が求められる。

ITサービスマネジメント（システム管理）

顧客の情報システムの日々の運用業務やシステム基盤の管理業務を担い、 円滑な運用を実現する役割。 運用時にセキュリティインシデントをモニタリングし、 インシデントが発生した場合には、 被害拡大防止等の初動対応を担う。

Subtopic

* + - 1. ＜脅威２＞ 不正アクセス
         1. 必要な対策は実施されていますか？

123456, admin, password などの単語を避けることは当然ながら、 意味のある単語にしない、 最低８文字以上にする、 定期的に変更するなど、 パスワードに関する基本的なルールが社内で徹底されていますか。

自分の席を離れる際は、 パスワードで保護されたスクリーンセーバーでパソコンを保護することをルール化していますか。

退職した従業員の ID など、 不要な ID を放置せず、 きちんと削除していますか。

ユーザーごとにアクセス権を設定し、 定期的な見直しや管理を行っていますか。

企業内のネットワークやコンピュータに、 ファイアウォールなどの外部からの不正アクセスを検知・遮断する仕組みを導入していますか。

自社が提供しているサービスについて、 不正アクセス対策を実施していますか。 （例：不正アクセス対策 http://www.ipa.go.jp/security/fusei/ciadr.html）

* + - * 1. 被害を防ぐためには、 こんな役割も重要です

システム運用において、 セキュリティ管理のタスクを実行する役割

* + - * 1. その役割を担う人材の例

セキュリティ アドミニストレータ （ＩＳセキュリティアドミニストレータ）

自社の情報セキュリティ対策の具体化や実施を統括する役割。 企業全体としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込み、 対策の立案や実施（指示・統括）、 その見直しなどを行う。 また、 利用者に対する教育等も実施する。

ITサービスマネジメント（運用管理）

顧客の情報システムの運用管理の責任者として、 ITサービスマネジメントの統括責任を担う。 セキュリティの面では、 運用するシステムのセキュリティマネジメントに関する方針や計画を策定し、 具体的な対策の実施を統括する。

* + - 1. ＜脅威３＞ エクスプイト
         1. 必要な対策は実施されていますか？

社内のコンピュータ上で利用しているソフトウェアの修正プグラム（セキュリティパッチ）が公表されたら迅速に適用していますか。 セキュリティパッチが適用されずに長期間そのまま利用されているコンピュータはありませんか。

セキュリティパッチの適用状況をきちんと把握していますか。 また、 それを把握し、 管理する担当者は決められていますか。

情報システムを設計・開発する際に、 セキュリティに関する仕様や基準、 要求事項などを明確にしていますか。

開発した情報システムのテストを行う際に、 外部からの攻撃などを意識したセキュリティに関するテストも実施していますか。

現在運用している自社のWEBシステムに脆弱性がないか、 検査を行ったことはありますか。

* + - * 1. 被害を防ぐためには、 こんな役割も重要です！

システム開発・構築において、 システム設計における セキュリティ面の検討や決定などのタスクを実行する役割

* + - * 1. その役割を担う人材の例

システムテザイナー

自社で用いるシステムの要件定義から、 システム基盤（インフラストラクチャ）の分析・設計及び構築を担う役割。 ネットワークの構成やアプリケーション基盤の設計の際に、 セキュリティを考慮した設計を行う。

ITスペシャリスト（セキュリティ）

情報システムの設計・開発・運用において、 情報セキュリティに関する高い専門性を発揮するスペシャリスト。

セキュリティインシデントが発生した際は、 高度な技術的スキルを駆使して原因の究明や復旧対応等も担う。

* + - 1. ＜脅威４＞ クラウド利用におけるデータ消失・流出
         1. 必要な対策は実施されていますか？

外部のクラウドサービスを利用する際のリスク（データの消失・流出や改ざんなど）について認識していますか。

* + - * 1. 情報セキュリティ強化対応スキル指標のご紹介

自社のどのような情報がクラウドサービス上にあるか、 把握していますか。

* + - * 1. 情報セキュリティを担う人材育成のヒント

クラウドサービスの利用・管理に関する責任者や実務担当者を決めていますか。

* + - * 1. 組織において求められる情報セキュリティ対策

クラウドサービスを提供する事業者が実施しているセキュリティ対策の具体的な内容や水準を把握していますか。

クラウドサービスを利用する際の ID やパスワードは、 適切に管理していますか。 特に「なりすまし」を防ぐために、 推測されにくいものになっていますか。

クラウドサービスの停止時や障害発生時に、 情報が手元で（自社内で）利用できるような対策が取られていますか。

* + - * 1. 被害を防ぐためには、 こんな役割も重要です！

ITシステム企画において、 システム化計画の具体化 （要件定義、 アーキテクチャの設計等）のタスクを実行する役割

* + - * 1. その役割を担う人材の例

ＩＳアーキテクト

自社内の情報システム基盤の構築・維持・管理を主に担う役割。 自社のIT戦略に基づき、 自社システムのアーキテクチャ設計を行うほか、 基盤の整備や品質統制のための取り組みなども行う。

ITアーキテクト（セキュリティアーキテクチャ）

強固なセキュリティ対策が求められる情報システムのアーキテクチャの設計を担う役割。 システムの企画・開発・構築・運用の各工程において、 情報セキュリティ対策が十分に機能し、 維持されることを担保する組織設計、 ルール設計、 プセス設計もあわせて行う。

* + - 1. ＜脅威５＞ スマートデバイスからの情報漏えい
         1. 必要な対策は実施されていますか？

紛失・盗難対策として、 スマートフォンなどのモバイル機器の利用時に、 パスワード入力しなければ使えない「パスワードック」を設定していますか。

ウィルス対策として、 スマートフォンなどのモバイル機器のOSを、 常に最新のバージョンにアップデートしていますか。

スマートフォンのアプリは、 メーカーやキャリアのアプリケーション・ストアなど、 信頼できる場所からインストールしていますか。

業務で利用するスマートフォンなどのモバイル機器に、 業務とは関係のないアプリが数多くインストールされていませんか。

私用のモバイル機器を業務上で利用することは、 現状ではあまり推奨されませんが、 利用可とする場合は、 モバイル機器用のセキュリティソフトを導入するなど、 適切なセキュリティ対策を利用者に義務付けていますか。

* + - * 1. 被害を防ぐためには、 こんな役割も重要です

事業戦略、 経営戦略の中で情報セキュリティ戦略の策定のタスクを実行する役割

* + - * 1. その役割を担う人材の例

セキュリティアドミニストレータ（情報セキュリティアドミニストレータ）

自社の情報セキュリティ戦略やポリシーの策定等を推進する役割。 戦略策定のほか、 戦略実行体制の確立や開発組織の統括も担う。 また、 企業内のセキュリティ業務全体を俯瞰し、 アウトソース等のリソース配分の判断・決定も行う。

コンサルタント（情報リスクマネジメント）

ビジネス機能内で情報マネジメントが適切に実現される土台としての組織体制の整備や組織内の各種ルール整備等に関する支援を担う役割。 組織ガバナンスやリスクマネジメント、 コンプライアンス等に関する領域において、 ITソリューションを前提としたコンサルティングを行う。

* + - 1. ＜脅威６＞ 内部不正・うっかりミス
         1. 必要な対策は実施されていますか？

一時的な従業員も含め、 重要な情報を扱う作業は、 管理監督者の目の届くところで行われていますか。 単独で重要な情報にアクセスしている従業員はいませんか。

社員の管理・監督権限に応じて、 適切なアクセス権限を設定していますか。 多くの従業員が、 管理者アカウントを自由に利用できるような設定になっていませんか。

重要な顧客情報などを保存しているコンピュータは、 管理者の目の届くところに置く、 別室に置いて入退室記録をつける、 部屋に鍵をかけるなどの対策を行っていますか。

個人情報などの機密情報については、 保存されているファイルにもパスワードを設定するなど、 二重三重の対策を工夫していますか。

重要な情報が保存されているコンピュータでは、 アクセスグを記録していますか。

重要な情報については、 担当者を決めて定期的にバックアップを取っていますか。

* + - * 1. 被害を防ぐためには、 こんな役割も重要です！

情報セキュリティマネジメントにおいて、 セキュリティ方針の策定、 セキュリティ基準の策定のタスクを実行する役割

* + - * 1. その役割を担う人材の例

セキュリティアドミニストレータ（ＩＳｾｷｭﾘﾃｨｱﾄﾞﾐﾆｽﾄﾚｰﾀ）

情報セキュリティ戦略やポリシーを具体的なルールや計画に落とし込み、 その実行（ないしは実行の指示）のほか、 維持・管理や見直しを行う役割。 また、 インシデント対応に備えて日頃のマネジメントや教育等の実施も担当する。

コンサルタント（情報リスクマネジメント）

ビジネス機能内で情報マネジメントが適切に実現される土台としての組織体制の整備や組織内の各種ルール整備等に関する支援を担う役割。 組織ガバナンスやリスクマネジメント、 コンプライアンス等に関する領域において、 ITソリューションを前提としたコンサルティングを行う。

* + - 1. 情報セキュリティ強化対応スキル指標のご紹介

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

* + - * 1. 「iコンピテンシ・ディクショナリ」とは、 ITスキル標準（ITSS）や情報システムユーザースキル標準（UISS）、 組込みスキル標準（ETSS）の３つのスキル標準を包含する形で整理した、 タスクとスキルのデータのことです。 この iコンピテンシ・ディクショナリを参照することで、 ３つのスキル標準の区別を意識することなく、 スキル指標としてIT関連業務に携わる人材の役割、 タスクやスキルを確認することができます。
      1. 情報セキュリティを担う人材育成のヒント
         1. 情報セキュリティを担う人材の育成についての悩み

自社の情報セキュリティ対策

現場が情報セキュリティの重要性を理解してくれない。

セキュリティに関する事故を経験したことがあるかないかによって、 現場のセキュリティ意識は大きく異なる。 以前事故が発生したことをきっかけに、 経営者がセキュリティ対策を現場横断的な重要なテーマとして掲げ、 全社的な取り組みを始めることができた

経営層に対して、 情報セキュリティ対策の重要性を効果的に伝えられず、 企業全体としての対策が進まない。

企業にとってのセキュリティ対策は、 今や単なる事故の予防ではなく、 企業のサービスの機能・品質の向上の一環であるということを、 経営者に伝える必要がある。

経営層に対してセキュリティの重要性を伝えられる人材の有無によって、 経営層の理解が変わる。 これは、 経営とITの関係と同じであり、 経営と現場をつなぐキーマンの育成 が鍵である。

情報セキュリティ担当者のスキルアップが難しい。

ユーザー企業には、 専任の情報セキュリティ担当者は少なく、 担当者は数年で異動・交代することが一般的であるため、 限られた期間で効果的にスキルアップする必要がある。 情報セキュリティマネジメントに関する資格などの学習も効果的である。

情報セキュリティを担う専門人材の育成

専門性の高い人材の育成方法が分からない。

専門性は高いが、 スキルの幅が広がらない。

専門性は高いが、 ビジネスマインドが身につかない。

* + - 1. 組織において求められる 情報セキュリティ対策のレベル
         1. 自社の属性に合った情報セキュリティ対策のレベルを見極めていく
    1. 情報処理安全確保支援士試験チェックシート
       1. 第1章　情報セキュリティ及びITの基礎
          1. 情報セキュリティの主な特性として，機密性・完全性・可用性の三つがある。 また，真正性，責任追跡性，否認防止及び信頼性を，情報セキュリティの付加的な特性とする場合がある。
          2. 情報セキュリティ対策には，抑止・抑制，予防・防止，検知・追跡，回復などの機能がある。 情報セキュリティ対策は，これらの機能のうち必ず一つ以上の機能をもっている。
          3. サイバー攻撃とは， 企業，組織，個人のコンビュータや情報システムに対し，ネットワークを介して侵入したり，不正なプグラムやコマンド，パケットを送りつけたりして，情報窃取，改ざん，破壊，サービス妨害等の攻撃や不正行為をすることである。
          4. 情報資産にアクセスする人間，プセス，プグラム等に対して，常に必要最小限の権限のみを付与するように徹底する。 これをf最小権限の原則Jという。
          5. 同ーの者に関連する複数の業務を行う権限を与えると，確認不足によるミスや不正行為などを発生させる原因となるため，業務ごとに担当を適切に分離する。 これを「責務の分離（職務分離）の原則jという。
          6. 組織内やシステムで発生する様々な事象について，それを発生させた主体（利用者，端末，プセス，プグラム等）を一意に識別・特定し追跡・検証できるようにする。
          7. 情報セキュリティマネジメントとは，「明確な方針や規定に基づいて，組織の情報資産の機密性，完全性，可用性などの特性を適切に維持・管理すること」と定義できる。
          8. 問合せ元のアドレスや問合せ対象ドメインの制限なく，名前解決要求に応じるDNSサーバ（キャッシュサーバ）は「オープンリゾルバjと呼ばれる。 オープンリゾルバはDNSキャッシュボイズニング攻撃に対して脆弱である。
          9. GETメソッドを使用したWebアフリケーションでは，URしから入力データが読み取られたり，改ざんされたりする可能性がある。 また， Referrerグから入力データが漏えいする可能性がある。
          10. POSTメソッドを使用すれば入力データがURLに含まれないため，GETメソッドよりも秘匿性が高まるが，入力データをグに記録するにはアプリケーション側で対応する必要がある。
          11. シンクライアントを実現する主な方式として，ネットワークブート方式と画面転送方式がある。 画面転送方式には，サーバベース型，プレードPC型， VDI型があり，これらの中で近年主流となっているのがユーザの利便性とコストバフォーマンスのバランスのとれたVDIである。
       2. 第2章　情報セキュリティにおける脅威
          1. ポートスキャンとはターゲツ卜となるホスト上で開いている（通信可能な状態となっている）ポートをスキャン（探査）することである。
          2. TCPハーフスキャン（ステルススキャン）はコネクションを確立しないためターゲットホストのグには記録されない。
          3. 管理者権限で実行されているサービスに対してBOF攻撃を行い，シェルなどに置き換えることに成功すれば，侵入者は管理者権限でそのホストを操作できることになる。
          4. BOF攻撃はソフトウ工アのバグが原因となっているため，その対策は， OSや使用しているソフトウェアのバージョンアップ，パッチの適用を確実に行うことで，既知のセキュリティホールを塞ぐことである。
          5. 侵入者は，所有者がrootで， setuid/setgid属性をもってプグラムを実行し，非常にサイズの大きい入力データを与えることでBOF状態を引き起こし， root権限を手に入れることができる。
          6. BOF攻撃への対策として所有者がrootで＇setuid/setgid属性をもつフグラムを探し，不要なものを削除するか， setuid/setgid属性を解除する。
          7. rootkitとは，侵入に成功した攻撃者が，その後の不正な活動を行いやすくするために自身の存在を隠ぺいすることを目的として｛吏用するソフトウェアなどをまとめたパッケージの呼称（俗称）である。
          8. パスワードクラックとは， 何通りものパスワードを繰返し試してパスワードを破る行為であり，推測によるもの，辞書ファイルを用いたもの，総当たりによるもの（ブルートフォース攻撃）などがある。
          9. ワンタイムパスワード方式，バイオメトリック認証システムなど，パスワードクラックが困難な認証システムにするのが確実な対策手段であり，従来の固定式パスワードを用いる場合にはアカウントのックアウト設定が有効な対策手段となる。
          10. TCPでは，シーケンス番号の交換によって通信の信頼性を高めているが，この仕組みを悪用し，他のホストのセッションに割り込んでシーケンス番号やIPアドレスを矛盾なく操作することができればセッションハイジャックが成立する可能性がある。
          11. UDPでは，クライアントからのリクエストに対し，正規のサーバよりも先にレスポンスを返すことでセッションハイジャックが成立する可能性がある。
          12. Webアプリケーションではセッション管理の脆弱性を攻略し，URL，クッキー， hiddenフィールド、 などlこセットされたセッション管理情報を推測／盗聴することによってセッションハイジヤックが成立する可能性がある。
          13. 攻撃者自身のMACアドレスと正規のホストのIPアドレスとを組み合わせた偽のARP応答パケットを送信することでARPキャッシュの内容を書き換え，セッションをハイジャックする手法をARPスプーフイングもしくはARPキャッシュポイズニングという。
          14. DNSサーバがゾーン転送要求に制限をかけていないと，不正なゾーン転送要求により，サイトのネットワーク構成やサーバの構成が攻撃者に推測されてしまう可能性がある。
          15. DNSキャッシュボイス・ニンク攻撃とは，DNSサーバからの名前解決要求に対して不正な名前解決情報を付加して返すことでDNSのキャッシュを汚染し，ユーザを悪意あるサイトに誘導する攻撃である。 DNSの送信元ポート番号とトランザクションIDが推測されやすいと，この攻撃による被害を受けやすい。
          16. SYNFlood攻撃とは，発信元アドレスを偽装したSYNパケットを特定のポートに大量に送りつけることで，正常なサービスの提供を妨害する行為である。
          17. コネクションレスであるUDPやICMPでは発信元アドレスの偽装が容易であるため，攻撃に悪用された場合，攻撃者を特定するのは困難である。
          18. smurf攻撃とは，ターゲヅトホストのIPアドレスに発信元アドレスを偽装したICMPecho requestを踏み台ネットワークのブードキャストアドレスに送りつけ，その応答パケットによってDoS攻撃を成立させる手法で、 ある。
          19. DDoS攻撃とはインターネット上にある多数の踏み台サイトにあらかじめ仕掛けておいた攻撃プグラムから，一斉にDos攻撃を仕掛けることで，ターゲットサイトのネットワークの帯域をあふれさせる攻撃手法である。 近年， DDoS攻撃はポットネットによって実行されるケースが大半となっている。
          20. DDoS攻撃への対策として，十分な回線帯域を確保し，十分な処理能力を有する機器を使用するとともに，負荷分散，帯域制限などによって攻撃を緩和するほか，CONサービスやCONプバイダ等が提供するDDoS攻撃対策サービスを利用することも選択肢となる。
          21. クスサイトスクリプティング（XSS）とは，ユーザの入力データを処理するWebアプリケーションや，Web ページ．を操作するJavaScript等に存在する脆弱性を悪用し，ユーザのPC上で不正なスクリプトを実行させる攻撃手法である。
          22. xssは，その仕組みにより，反射型xss，格納型XSS,DOM Based XSSの3種類に分類される。 DOMBasedxssは，スクリプ卜によるWebページ出力処理（DOM操作）に不備があることによる脆弱性である。
          23. SQLインジヱクションとは，ユーザの入力データをもとにSOL文を編集してDBにアクセスする仕組みに
          24. なっているWebアプリケーションに対して不正なSOL文を入力することで，機密情報を不正に取得したり，DBを不正に操作したりする攻撃手法である。
          25. OSコマンドインジェクションとはユーザの入力データをもとに，OSのコマンドを呼び出して処理する
          26. Webアプリケーションにおいて，不正なコマンドを入力することで，任意のファイルの読出し，変更，削除，パスワードの不正取得などを行う攻撃手法である。
          27. HTTPヘッダインジェクションとは，ユーザの入力データをもとに， HTTPメッセージのレスポンスを生成するWebアプリケーションにおいて，不正なデータを入力することで任意のヘッダフィールドやメッセージボディを追加したり複数のレスポンスに分割したりするなどの攻撃を行う手法である。
          28. メールヘッダインジェクションとはユーザがフォームに入力したデータをもとにメールを送信するWebアプリケーションにおいて，不正なメールヘッダを混入させることにより意図していないアドレスに迷惑メールを送信するなど，メール送信機能を悪用した攻撃手法である。
          29. xssやSOLインジェクションに対しては，ユーザの入力データ中にスクリプトやSQL文として特別な意味をもっメタキャラクタが存在した場合，それらをエスケープ処理することで対処する。
          30. OSコマンドインジェクションに対しては，OSコマンドの呼出しが可能な関数を極力使用しないようにすることと，使用する場合にはルールに従わないデータを無効とし，一切処理しないようにする必要がある。
          31. HTTPヘッダインジ、 エクションに対しては，HTTPレスポンスヘッダ生成に用いるユーザ入力データに改行コードが含まれていた場合には削除するほか，ヘッダ出力用のAPIやライブラリを使用するなどの対策が有効である。
          32. マルウェアへの対策は各ホストにウイルス対策ソフトを導入することに加え，ファイアウオール， IPS，サンドボックス，SMTPゲートウェイ，プキシサーバなど，通信経路上での検知・駆除対策を複合的に実施する必要がある。
          33. ボット（bot）とはワームの一種で，コンビュータに感染するだけでなく攻撃者によって遠隔地から操作ができ，機能拡張なども行うよう作られた悪質なプグラムであり，その操作にはIRC,P2Pソフトなどが悪用される。
          34. ランサムウェアとは感染したコンビュータのファイルやハードディスクを勝手に暗号化する等して正常に利用できない状態にした後それを解除するための身代金の支払いを要求するタイフのマルウェアである。
          35. 標的型攻撃とは特定の組織や団体等をターゲットとして，その取引先や関係者，公的機関などを煽ってマルウェアや不正なリンクが埋め込まれたメールを送信することで相手を編し，情報を盗もうとする手法である。
          36. 水飲み場型攻撃とは攻撃者がターゲツトとなる組織の社員／職員等が日頃頻繁に利用しているWebサイト（水飲み場）を改ざんすることで同組織のPCをマルウェアに感染させる手である。
          37. 出対策とは，マルウェアの侵入・感染を許したとしても，その拡散や，機密情報や個人情報の外部への流出などの被害を防ぐために行う対策である。
          38. マルウェアの検出手法としては，パターンマッチング法が代表的だが，パターンファイルに登録されていないものは検出できない。 既知のウイルスの亜種や，未知のウイルスなどの検出にはヒューリスティック法やビヘイビア法が有効である。
       3. 第3章　情報セキュリティにおける脆弱性
          1. 公開Webサーバと社内専用のファイルサーバなど，アクセスを許可する範囲（人，機器等）が明らかに異なるホストが同一セグメントに混在しているネットワークは脆弱であり，機密性，完全性の侵害につながるリスクが高い。
          2. 発信元IPアドレスにプライベートアドレスが設定されたインターネットからのインバウンド、 パケットなど，明らかに発信元アドレスが偽装されているパケットについては，ルータやファイアウオールによって遮断する必要がある。
          3. 広く普及しているメールサーバソフトウェアの旧バージョンでは，メールの投稿にあたってユーザを認証する仕組みがなかったため発信元メールアドレスの詐称が堂々と行われるほか，組織外の第三者から別な第三者へのメール投稿を受け付け$中継してしまう。
          4. 組織外の第三者から別の第三者へのメール投稿を受け付け，中継してしまうことを第三者中継（Third-PartyMail Relay）という。 なお，第三者中継をオープンリレー，それを行うSMTPサーバをオープンリレー(SMTP）サーバとも呼ぶ。
          5. OP25Bとは，ISPのSMTPサーバを経由せず，直接インターネットに出ていく25番ポートあてのパケットを遮断することで，スパムメールの発信を防ぐ技術である。
          6. OP25Bが設定された環境で正当なユーザがISP以外のSMTPサーバを使用してメールを発信する場合には，投稿専用のSubmissionポート（587/TCP）を使用するとともに， SMTP-AUTHによってユーサ．認証を行う。
          7. 発信元情報を偽装したメールを発見し，排除する技術として，発信元のIPアドレスやディジタル署名によってメール受信側で発信元SMTPサーバを認証する仕組み（送信ドメイン認証）が近年実用化されている。
          8. 標準的なPOP3ではUSER/PASSコマンドによってユーザ認証を行うが，その際ユーザIDとパスワードは
          9. 平文のままネットワーク中を流れていくため，経路上でのパケット盗聴により，ユーザの認証情報が盗まれてしまう可能性が高い。
          10. POP3の脆弱性への対策としては，APOP,POP3over TLS (POP3S) SSHによるポートフォワーデイングなどがある。
          11. DNSSECは，ディジタル署名を用いて応答レコードの正当性，完全性を確認する方式であり，DNSキャッシュポイズニング攻撃への有効な対策となる。
          12. UDP53番ポートを使用するDNSの通常の名前解決では，一つのパケットに格納できるデータが512オクテットに制限されているがDNSの拡張機構であるEDNSOを用いることにより，最大65,535オクテットまで拡張することができる。
          13. DNSの脆弱性への対策として， DNSサーバを，代理名前解決を行わないコンテンツサーバと，ゾーン情報をもたない代理名前解決専用のキャッシュサーバに分離し，後者を利用可能なホストの範囲を制限する方法などがある。
          14. Webアプリケーションでは， URLパラメタ，hiddenフィールド，クッキーのいずれかの手段でセッション管理を行うが，それらのうちどれを用いていたとしても，HTTPで通信していればセッション管理情報の漏えいが発生する可能性がある。
          15. クッキーの有効期限は可能な限り短く，また有効範囲は可能な限り狭くすることに加え， HTTPS(TLS）を使用しているページでは必ず、 secure属性を設定し，盗聴によってクッキーが盗まれるのを防ぐ必要がある。
          16. HttpOnly属性をクッキーに設定することにより，適用範囲をHTIP/HTIPS通信だけに限定し，xssによってクッキーが盗まれるのを防ぐことが可能となる。
          17. 重要なセッション管理情報はすべてWebサーバ側で管理し， URLパラメタ，クッキー， hiddenフィールドには，セッションの識別情報（ID）しか含めないようにする。
          18. セッションIDには十分な長さをもった乱数やハッシュ値を用いる（GETメソッドを使用している場合は特に重要）。
          19. HTTPのベーシック認証では盗聴によって認証情報が漏えいする可能性があるため，使用する場合にはHTTPSによって暗号化する。
          20. Webサーバが詳細なエラーメッセージをクライアントに返す設定になっていると機密情報の漏えいにつながる可能性があるため，必要最小限のエラーメッセージのみを返すように設定する。
          21. CSRFとは， Webアプリケーションのユーザ認証やセッション管理の不備を突いて，サイトの利用者に，Web アプリケーションに対する不正な処理要求を行わせる手法である。
       4. 第4章　情報セキュリティマネジメントの実践
          1. 情報セキュリティ対策の効果を高めるためには，リスク分析によって組織に内在する様々な情報リスクを洗い出すとともに，その影響度を分析・評価し，有効な対策を導き出す必要がある。 この一連の取組みをリスクアセスメントという。
          2. 詳細リスク分析では，分析の対象となる組織や情報システムにおける情報資産，脅威，脆弱性を洗い出し，それらの関連性からリスクを洗い出し，その大きさを評価する。
          3. リスクコントールとは，潜在的なリスクに対して，物理的対策，技術的対策，運用管理的対策によって，発生を抑止したり，損失を低減させたりすることである。
          4. リスクファイナンシングとは， リスクが顕在化して損失が発生した場合に備えて，損失の補壌や対応費用などの確保をしておくことである。
          5. 組織の重要な情報資産を適切に保護するためには，その重要度などに応じて整理・分類するとともに，取扱い方法を明確にする必要がある。
          6. 特定組織におけるCSIRTには，インシデン卜発生時にその対応を主導し，情報を集約して顧客，株主，経営者，監督官庁等に適時報告するとともに，現場組織等に適時対応を指示することなどが求められる。 また，平常時の活動として，セキュリティ情報の収集，業界団体，他のCSIRT等と連携し，インシデント発生に備えた対応を行うことなども重要な役割となる。
          7. BCMを確立するには，まずビジネスインパクト分析(BIA）を行い，重要業務の停止時に目標時間内に復旧させるための具体的な計画や手順を事業継続計画(BCP）として策定する必要がある。
       5. 第5章　情報セキュリティ対策技術
          1. (1)侵入検知・防御

ホスト要塞化の主な実施項目としては，最適なパーティション設計とセキュアなファイルシステムの選択，最新バージョンのソフトウェアのインストールとパッチ適用，不要なサービスや機能の停止，アカウントの停止／削除とパスワードの強化，システムリソースに対する最小限のアクセス権の設定適切なギング設定，などがある。

OS，サーバソフトウェアに対する脆弱性検査で、 は，発見された脆弱性に直ちに対処するとともに，同じ製品構成の他のホストにも同様の脆弱性が存在する可能性が高いため，それを確認し，対処する必要がある。

Webアプリケーションに対する脆弱性検査では，発見された脆弱性に直ちに対処するとともに，そのページを開発したベンダが開発した他のアプリケーションにも同様な脆弱性が存在する可能性が高いため，それを確認し，対処する必要がある。

パケットフィルタ型（スタティックパケットフィルタ型）ファイアウオールとは，パケットのヘッダ情報に含まれるIPアドレスポート番号などによって中継の可否を判断するもので，パケットのアプリケーション層のデータ（ぺイード）についてはチェックしない。

ダイナミックパケットフィルタ型ファイアウオールとは，最初にコネクションを確立する方向のみを意識した基本的なACしを事前に登録しておき，実際に接続要求があると，個々の通信を管理テーブルに登録するとともに必要なルールが動的に作成され，フィルタリング処理を行う方式である。

ファイアウオールでは，許可されたプトコルに対するポートスキャンや，BOF攻撃などOSやミドルウェアの脆弱性を突いた攻撃， SOLインジエクションなどWebアプリケーションの脆弱性を突いた攻撃，DoS系の攻撃などを防ぐことはできない。

一般的なNIDSは主に登録されたシグネチャ（攻撃パターンのデータベース）とのマッチング，異常検知（アノマリ検知）というこつの手法を用いて攻撃や不正アクセスを検知する。

アノマリ検知とは取り込んだパケットをRFCのプトコル仕様など（正常なパターン）と比較し，仕様から逸脱したものを異常として検知する手法である。

HIDSは監視対象となるホストに常駐し，グインの成功／失敗，特権ユーザへの昇格，システム管理者用プグラムの起動，特定のファイルへのアクセス，プグラムのインストールなどのイベントをリアルタイムに監視する。

IDSの誤検知の割合を測るための指標として，フォールスポジティブとフォールスネガティブの二つがある。 前者は不正ではない事象を不正行為として検知してしまうことを指し，後者は本来検知すべき不正行為を見逃してしまうことを指す。

NIDSには誤検知のほか，一部の高性能な機種を除き暗号化されたパケットを検知できない，サイト独自のアプリケーションの脆弱性を突いた攻撃を検知できない，不正アクセスを防御できない，内部犯罪の検知は困難，などの機能上の限界や運用上の課題がある。

侵入防御システム（IPS）とは，従来のNIDSをインライン接続することで＇ ，NI DSと同等の侵入検知機能と，NIDSよりも強力な防御機能を備えた製品である。 誤検知が発生しやすかったアノマリ検知機能の強化などが図られている。

IPSをインライン接続することによってパケットを遮断する場合，フォールスポジティブが発生すれば正常なアクセスが遮断されてしまう。 逆に，フォールスネガティブが発生すれば攻撃を見逃してしまう。 また，誤検知ではなくとも攻撃が多発すればIPSの処理能力等の問題でネットワークのパフォーマンスやアベイラビリティを低下させてしまう可能性がある。

一般的なIPSでは，フェールオープン機能を用いることで，障害が発生した場合にはパケットをそのまま通過させ， トラフィックが遮断されないようにすることも可能である。

Webアプリケーションファイアウオール（WAF）とは， XSS, SQLインジェクションなど， Webアプリケーションに対する攻撃を検知・排除する製品である。

一般的なWAFにはSSL暗号化／復号機能や負荷分散機能が内蔵されている。 そのため， SSLアクセラレータ，ードバランサを併用することなくWebサイトを運用することも可能である。

リバースプキシ型のWAFを経由したリクエストは，発信元の情報がWAFに置き換えられるため， Webサーバのアクセスク上では実際の発信者を特定できなくなる。 そのため， WAFによっては実際の発信者のアドレスを引き継いで渡す機能もある。

近年普及しつつあるサンドボックスとは，実環境から隔離されたセキュアな仮想環境のことであり，当該環境でマルウェアの可能性がある不審なファイル等を実行させ，その振る舞いを観察することでマルウェアであるかどうかを判定する。

* + - * 1. (2)アクセス制御と認証

ファイルやシステム資源などの所有者が，読取り，書込み，実行などのアクセス権を設定する方式を任意アクセス制御（DAC）という。 DACでは所有者の裁量次第でファイルなどへのアクセス権が決定するため，十分な機密保護を行うのは困難である。

保護する対象である情報と，それを操作するユーザなどに対してそれぞれセキュリティのレベルを付し，それを比較することによって強制的にアクセス制限を行う方式を強制アクセス制御（MAC）という。 MACでは，たとえファイルの所有者であったとしても，アクセス権を自由に決定することはできない。

認証の対象として，人の認証（本人認証），物（機器，デバイス等）の認証情報の認証（メッセージ認証）の三つがある。 また，本人認証として，バイオメトリクスによる認証，所有物による認証，記憶や秘密による認証の三つがある。

認証された利用者に対して，定められた機能などを実行するための権限を与えることを「認可(Authorization)J という。

チャレンジレスポンス方式とはサーバから送られた乱数文字列である「チャレンジ」と，クライアントのパスワードである「シード」(Seed ：種）を組み合わせて計算した結果を「レスポンス」としてサーバに返し，サーバも同様の計算を行って求めたレスポンスとの比較によってユーザ を認証する方式である。

ワンタイムパスワード方式は，認証のたびに毎回異なるパスワードを使用することでセキュリティを確保するが，そのためには生成するパスワードに規則性や連続性がなく（ランダムであることにユーザがパスワードを覚えなくてもよいようになっている必要がある。

チャレンジレスポンス方式やS/Keyによる認証における問題として，サーバの正当性を確認する仕組みがないと通信経路上に不正なホストが存在し，それによってセッションをハイジヤックされてしまう可能性がある。 これを中間者攻撃（Man-in-the-MiddleAttack）と呼ぶ。

認証システムに対する中間者攻撃の脅威に対しては，SSL/TLSのように通信に先立ちディジタル証明書によってクライアントがサーバの正当性を確認する方式を採用することなどが対抗策となる。

ICカードに対する攻撃手法は， ICチップの破壊を伴うもの（破壊攻撃）と伴わないもの（非破壊攻撃，もしくはサイドチャネル攻撃）に大別される。 前者の代表的なものとして，プービングやリバースエンジニアリングがあり，後者の代表的なものとしては， DPA,SPA，グリッチ，光照射などがある。

ICチップの脆弱性評価に関する事実上の基準となっているのはJIWGである。 JIWGはICカードの評価の公平性や客観性を実現するための解釈の統ーや， ISO/IEC 15408をICカードの評価に適用する際の解釈の統一を目的としたワーキンググループである。

IEEE802.1Xは，ネットワーク環境でユーザ認証を行うための規格である。 もともとは有線LAN向けの仕様として策定が進められたがその後EAPとして実装され，現在では無線LAN環境における認証システムの標準仕様として広く利用されている。

IEEE802.1Xは，クライアントであるサプリカント(Supplicant）システム，アクセスポイン卜やLANスイッチなど，認証の窓となる機器である認証装置(Authenticator），認証サーバ（RADIUSサーバなど）から構成される。

EAP-TLSは，サーバ・サフリカントでTLSによる相互認証を行う方式であり認証成立後にはTLSのマスタシークレットをもとにユーザごとに異なる暗号鍵を生成・配付し，定期的に変更するため，無線LANのセキュリティを高めることができる。

EAP-TTLSは，TLSによるサーバ認証によってEAPトンネルを確立後，そのトンネル内で様々な方式を用いてサプリカントを認証する方式であり， EAP-TLSと閉じ仕組みにより，無線LANのセキュリティを高めることができる。

PEAPは，EAP-TTLSとほぼ問機の方式だが，サプリカントの認証はEAP準拠の方式に限られる。 EAPTLS,EAP-TTLSと同じ仕組みにより，無線LANのセキュリティを高めることができる。

EAP-MD5は， M05によるチャレンジレスポンス方式によってパスワードを暗号化しサプリカントの認証のみを行う方式である。 認証フセスそのものは暗号化されず，暗号鍵の生成・配付等も行わないため，無線LANでの使用には向かない（有線LAN向き）。

シングルサインオン（SSO）を実現するには，各サーバ間でユーザの識別情報を交換する必要があるが，それを行うための仕組みとして，クッキーを用いる方式，リバースプキシサーバを用いる方式， SAMLを用いる方式があるo

クッキーを用いたsso認証システムでは，クッキーが共有可能な範囲内（同一ドメイン内）でしか使用できない，クライアントがクッキーの使用を制限している場合には使用できない等の問題がある。 一方，リパースプキシ方式については，ネットワーク構成の制約により，複数のドメインにまたがったシステムでssoを実現するのは困難である。

SAMLとは，認証情報を安全に交換するためのXML仕様であり，OASISによって策定された。 SAMLはSOAPをベースとしており同一ドメイン内や特定のベンダ製品にとどまらない大規模なサイトなどにおいて，相互運用性の高いssoの仕組みゃ，セキュアな認証情報管理を実現する技術である。

SAMLでは，認証結果の伝達，属性情報の伝達，アクセス制御情報の伝達，のそれぞれにアサーションと呼ばれるセキュリティ情報を扱うほかアサーションへのリファレンス情報などからなる「Artifact」と呼ばれる情報が使用されている。

SAMLでは，ldPとSP闘で要求・応答メッセージを送受信するためにHTTPやSOAP等のプトコルにマッピングする方法（バインディング方法） として，SOAP, HTTP Redirect, HTTP POST, HTTPArtifactなどの穫類がある。

一般的に，アイデンティティ管理（ID管理）は，ディレクトリ，プビジョニング，アクセス制御（管理），ワークフーなどのシステムとそれを運用管理するためのポリシ，手順，体制などによって実現される。

* + - * 1. (3)暗号

AESとは，DESの後継となる米国政府標準の共通鍵暗号方式である。 NISTによる審査の結果，ベルギーのJoanDaemen氏とVincentRijmen氏が開発したfRjjndaelJ （レインダール）という方式が選ばれた。 ブック長は128ビットで＼ 使用する鍵の長さは128/192/256ビ、 ツトの中から選択できる。

ブック暗号では，処理を複雑にし，暗号の強度を高める暗号化手法（暗号モード）が確立されており，CBC(Ci pher Block Chaining）やCFB(Cipher Feedback)などがある。 CBCは一つ前の平文ブックの暗号結果と次の平文ブックをXOR演算し，その結果を暗号化する方式であり，広く使用されている。

ハッシュ関数とは，任意の長さの入力データをもとに，固定長のビット列（ハッシュ値メッセージダイジ、 エスト）を出力する関数であり，衝突発見困難性，第2原像計算困難性，原像計算困難性（一方向性）の三つの性質が求められる。

SHA-1には，ある条件下でハッシュ値の衝突を意図的に起こすことができるという脆弱性が発見されていることから，次世代ハッシュ関数（SHA-3）が決定されるまでの措置として， SHA-2に移行することが推奨されていたが，NIST主催の次世代暗号コンペティションの結果，2012年10月にfKeccakJ がSHA-3に選出された。

MAC（メッセージ認証コード）とは通信データの改ざん有無を検知し完全性を保証するために通信データから生成する固定長のコード（ビット列）である。 MACには，ブック暗号を用いたCMAC，ハッシュ関数を用いたもの（HMAC）などがある。

HMACは，ハッシュ値の計算時に，通信を行う両者が共有している秘密鍵の値を加えてその通信固有のハッシュ値を求めるようにすることで通信データの改ざんを検知する仕組みである。

フィンガプリントとは，ディジタル証明書や公開鍵，メールなどの電子データが改ざんされていないことを証明するために使用するデータであり，ハッシュ関数を用いて対象となる電子データから生成する。

PC環境において暗号化に用いる鍵を安全に生成して格納したり，暗号化・復号処理等を実行したりするための技術として， 近年TPM(Trusted PlatformModule）が広く用いられている。 TPMは耐タンパ性に優れたセキュリティチッフであり，通常PCのマザーボードに直付けする形で搭載されている。

Diffie-Hellman鍵交換アルゴリズムは，離散対数問題が困難であることを安全性の根拠にしており，安全でない通信路を使って暗号化に用いる秘密対称鍵を生成し，共有することを可能にするものである。

SAとは，IPsecにおける論理的なコネクション（トンネル）であり，制御用に用いるISAKMPSAと，実際の通信データを送るために用いるIPsecSAがある。 IPsec通信を始める際には最初に制御用のISAK MPSAが作られ，次にIPsecSAが作られる。

ISAKMPSAはIPsecゲートウ工イ聞で一つ（上り下り兼用）作られるが， IPsecSAは，各ホスト問において，通信の方向や使用するプトコル（AH, ESP）ごとに別々のSAが作られる。 IPsecSAの識別情報として，あて先IPアドレス，フトコル，SPIが使用される。

AH（認証ヘッダ）は，主に通信データの認証（メツセージ認証）のために使用されるプトコルであり，通信データを暗号化する機能はない。

ESP（暗号化ぺイード） は通信データの認証（メッセージ、 認証）と，暗号化の両方の機能を提供するプトコルである。

AHではMACを用いてパケット全体のICVを作成するため，完全性チェックの精度を高めることが可能だが，その反面， NATを使用している場合には経路上でIPアドレスが変更されてしまうため完全性チェックが正常に行えなくなってしまうという問題がある。

ESPもAHと同様にMACを用いてICVを生成するが，AHとは異なり，IPアドレスについては計算の対象としていないため，NATを行ってもICVは影響を受けずに済む。 ただし， NAPTについては正常に行えないため，対処が必要となる。

IKEバージョン1(IKEv1）は， SAや鍵管理の仕様を規定したISAKMP/Oakleyを実装した汎用的なプトコルであり，500/UDPを使用する。 IKEv1の鍵交換方式として，ISAKMPSAの作成に使用するメインモード＼ アグレッシブモード， IPsecSAの作成に使用するクイックモードなどが、 ある。

IKEでは，通信に先立って通信相手を認証する。 その方式としては，通信を行う者同士が，あらかじめ鍵を共有しておき，それによって相手を認証する［事前共有鍵認証jのほか，「ディジタル署名認証jや「公開鍵暗号認証jなどがある。

メインモードで事前共有鍵認証を行う場合，通信相手を識別するIDは暗号化されるが，IDにはIPアドレスしか使用できないという制約がある。 そのため，モバイル接続のように，毎回動的にIPアドレスが、 設定される環境では使用できない。

アグレッシブモードで事前共有鍵認証を行う場合，IDは暗号化されないが，最初に送信されるため，IDにFQDNなどを使用して事前共有鍵との対応付けを行うことができる。 そのためIPアドレスが動的に設定される環境でも使用することができる。

クイックモードでは前フェース で確立したISAKMPSAを使用して通信が行われるためパケットのぺイード部分が暗号化される。

リモートアクセス環境でのIPsec通信では，SAの作成時に端末機器を認証（デバイス認証）するだけでなく，端末の使用者も認証（ユーザ認証）する必要がある。 IPsecでは，これを行う手段として， XAUTHが広く利用されている。

NAPTを使用する環境では，AH,ESPともにそのままではIPsecを使用することができないため， IPsecのパケットに新たなUDPヘッダを追加（カプセル化）することによって対応する方法が広く用いられている。

SSL/TLSは， トランスポート層とアプリケーション層の間に位置付けられ，その内部は下位層のRecordプトコルと，上位層の四つのプトコル（HandshakeプトコJレ，ChangeCipher Specプトコル，Alertプトコル，ApplicationDataプトコル）から構成される。

Recordプトコルは，上位層からのデータを214バイト以下のブックに分割し，圧縮，MACの生成，暗号化の処理を行って送信する。 データ受信時には，復号，MACの検証，伸張の処理を行って上位層に引き渡す。

Handshakeフトコルはサーバ・クライアント間で新たにセッションを確立する，もしくは既存のセッションを再開する際に，暗号化アルゴリズム，鍵，ディジタル証明書など，通信に必要なパラメタを相手とネゴシエーションして決定する。

SSL/TLSにおける「セッションjとは， Handshakeプトコルによるサーバとクライアントの鍵交換（ネゴシエーション）の結果生成された，マスタシークレツトによって特定される仮想的な概念である。 一方「コネクションJは，セッションに従属して存在する通信チャネルであり，一つのセッションには，必要に応じて複数のコネクションが存在する。

HSTSは， Webサイトが， HTTPSでアクセスしたブラウザに対し，当該ドメイン（サフドメインにも適用可能）への次回以降のアクセスにおいて， max-age で指定した有効期限（秒単位）まで， HTTPSの使用を強制させる機構である。

S/MIMEは不特定多数のユーザ問で安全性，信頼性の高い通信を行うことを想定しているため，利用にあたって各ユーザは公的な第三者機関が発行するディジタル証明書（S/MIME証明書）を取得することが前提となる。

X.509は，ITU-Tが1988年に勧告したディジタル証明書及びCALの標準仕様でありISO/IEC 9594-8として国際規格化されている。 X.509では，ディジタル証明書の発行者が拡張フィールドに独自の情報を追加できるようになったほか， 2000年にはX.509v3の改訂が行われ，新たにAC（属性証明書），ACAL （属性証明書失効リスト）が定義された。

OCSPレスポンダとは，ディジタル証明書の失効有無をリアルタイムで応答するサーバであり，CAやVAが運営する。 クライアン卜はOCSPレスポンダに問い合わせることによって自力でCRしを取得したり照合したりする手間を省くことができる。

SCVPはOCSPと同様に証明書の有効性検証をリアルタイムで行う仕組みであるがOCSPではディジタル証明書の失効情報のみをチェックするのに対し，SCVPでは信頼関係（有効期限，署名など）も含めてチェックする。

タイムスタンプとは，電子文書に対して，信頼される第三者機関である時刻認証局（TSA）が付す時刻情報を含んだ電子データでありその電子文書が「いつ」作成されたかということと「その時刻以降改ざんされていなしリことを保証するものである。

過去のある時点でディジタル署名が有効であったことを検証するために，当該署名に対する公開鍵証明書，当該証明書からルート証明書に至るまでのパス上のすべての公開鍵証明書， 及びそれらに関する失効情報等をすべて集め，それらに対するタイムスタンプを付したものをアーカイブタイムスタンプという。

アーカイブタイムスタンプは関連する技術の危殆化によって有効性が失われてしまう前に，その時点の最新技術を用いて次のアーカイブタイムスタンプを取得する必要がある。 これは，電子文書を保存している限り，必要に応じて繰返し行っていく必要がある。

* + - 1. 第8章　システム開発におけるセキュリティ対策
         1. システム要件や利用環境等に応じた適切なセキュリティ機構を有し，脆弱性への対処がなされたセキュアなアプリケーションを開発するためには，開発工程の初期段階からセキュリティ対策に取り組む必要がある。
         2. CIC＋＋ 言語のgets,strcpy, strcat, sprintf, scant,sscanf, fscanfなどの関数では，入力データをサイズの制限なくメモリ内の変数領域に格納してしまうため，バッファオーバフー（BOF）状態を引き起こす可能性が高い。
         3. 上記の関数への対策としては，バッファに書き込むサイズを指定できる関数（fgets, strncpy, strncat,snprintf等）で代用するか，精度を指定してバッファに書き込む最大サイズを制限することである。
         4. CIC＋＋言語をはじめ，多くのプグラム言語で，ナル文字は文字列の終端を示すものとなるため，文字列を処理する関数はナル文字を見付けると読込みなどの処理を終了する，バッファに文字列を格納する関数は，末尾にナル文字を付加する，などの処理を行う場合が多い。
         5. 末尾にナル文字を付加する関数を使用する際には，文字列を格納する先のバッファのサイズとして，格納する対象となる文字列の長さに加えナル文字分（1バイト）が必要である。 これを怠るとBOFの問題が発生する可能性が高まる。
         6. Javaで採用されているサンドボックスモデルとは，ネットワークなどを通じて外部から受け取ったプグラムを，セキュリティが確保された領域で動作させることによって，プグラムが不正な操作や動作をするのを防ぐ仕組みである。
         7. レースコンディション（競合状態）とは，並列して動作する複数のプセスやスレッドが，同一のリソース（ファイル，メモリ，デバイス等）ヘほぼ同時にアクセスしたことによって競合状態が．引き起こされ，その結果，予定外の処理結果が生じるという問題である。
         8. ECMAScriptにおいて，外部からの入力値を文字列リテラルとして扱う場合にはメタキャラクタをエスケープ処理する必要がある。 エスケープ処理が必要な文字として最低限次の四つが挙げられる。 「＼ ＼＼」「 ＼ 」「 ＼ 」「改行 ＼n」。
         9. ECMAScriptにおいて，グーバル変数は関数の外で「var」を用いて定義し ーカル変数は使用する関数の中で「var」を用いて定義する。 「var」を使用せずに定義した変数はすべてグーバル変数として解釈されるが，発見が困難なバクを作り出す大きな要因となるため，避けなければならない。
         10. Ajax(Asynchronous JavaScript + XML） とは，JavaScriptなどのスクリプト言語を使ってサーバと非同期通信を行うことで、 Webページ全体を再描画することなく，ページの必要な箇所だけを部分的に更新することを可能にする技術である。
         11. XMLHttpRequestは各種ブラウザに実装されている組込みオブジエクト（API）であり，周期通信，非同期通信の双方をサポートしている。
         12. JSON(JavaScript Object Notation）とは，ECMA-262標準第3版準拠のJavaScript(ECMAScript）をもとにした軽量のデータ記述方式である。
         13. JSONP (JSON with Padding）とは，くscript＞タグのsrc属性にはクスドメイン通信の制限がなく，別ドメインのURしを指定できることを利用することで，JavaScript (ECMAScript）とJSONを用いてクスドメイン通信を実現する技術である。
      2. 第9章　情報セキュリティに関する法制度
         1. ISO/IEC 15408は，オペレーテイングシステム，アプリケーションプグラム，通信機器，情報家電など，セキュリティ機能を備えたすべてのIT関連製品や，それらを組み合わせた一連の情報システムのセキュリティレベルを評価するための国際規格である。
         2. CMMI（能力成熟度モデル統合版）は，米国国防総省が米国カーネギーメン大学に設置したソフトウェア工学研究所で考案された能力成熟度モデルの一つであり，システム開発を行う組織がプセス改善を行うためのガイドラインとなるものである。
         3. PCIDSS (Payment Card Industry Data SecurityStandard）とは，クレジットカード情報や取引情報の保護を目的として国際ぺイメントブランド5社が共同で策定したセキュリティ基準であり，対策を実施する頻度や許容期間などが具体的に示されているのが大きな特徴となっている。
         4. ISO/IEC 20000とはIT関連サービスを提供する組織が，顧客の求める品質を確保し，維持・改善するための要求事項を規定した国際規格であり， ITサービスマネジメントにおける業務プセスや管理手法を体系的に整理した書籍群であるITILに基づいている。
         5. 行政手続における特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）は，年金や納税等，異なる分野の個人情報を照合できるようにするとともに，行政の効率化や公正な給付と負担を実現し，手続の簡素化による国民の負担軽減を図ることなどを主な目的としている。
         6. サイバーセキュリティ基本法は，サイバーセキュリティに関する施策や戦略を明確に定め，総合的かつ効果的に推進することにより，経済社会の活力向上，持続的発展，国民が安全で安心して暮らせる社会の実現，国際社会の平和及び安全の確保，国の安全保障への寄与などを目的にしている。
         7. 知的財産権のうち，特許権，実用新案権，意匠権，商標権の四つを［産業財産権Jという。
         8. 産業財産権の存続期間は，特許権が出願日から20年，実用新案権が出願白から10年，意匠権が登録日から最長20年，商標権が登録日から10年（継続使用による更新可能）となっている。
         9. 著作権とは，創作された表現を保護する権利であり，著作物を創作した時点で成立し，著作者の死後， 50年を経過するまでの間，存続する。 ただし，映画の著作物の保護期間は公表後70年となっているo
         10. 不正競争防止法が保護の対象としているのは「秘密として管理されている有用な技術上又は営業上の情報であって，公然と知られていないもの」である。
         11. 内部統制とは，企業において業務が正常かつ有効に行われるよう各種の手続や仕組み，プセスを整備し，それを遂行することによって，企業の活動全般を適切にコントールすることをいう。
         12. COBIT(COBITS）は，ITガバナンス及びITマネジメントに関する実践規範であり，ガイドライン文書， フレームワーク，プセス参照モデル等からなる。

1. 次世代環境及び技術関連
   1. AI
      1. IoT、 ビッグデータ、 AI等に関する 経済産業省の施策について【2016年3月METI】

ドキュメントを参照: [3\_01\_sano.pdf](https://www.iajapan.org/iot/event/2016/pdf/3_01_sano.pdf)

* 1. IoT
     1. IoTセキュリティガイドラインver1.0【2016年7月5日総務省・経済産業省】

ドキュメントを参照: [20160705002.html](http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html)

* + - 1. 目的等
         1. セキュリティ確保の観点から求められる基本的な取組を、 セキュリティ・バイ・デザインを基本原則としつつ、 明確化することによって、 産業界による積極的な開発等の取組を促すとともに、 利⽤者が安⼼してIoT機器やシステム、 サービスを利⽤できる環境を生み出す
         2. 関係者が取り組むべきIoTのセキュリティ対策の認識を促すとともに、 その認識のもと、 関係者間の相互の情報共有を促すための材料を提供すること
         3. 守るべきものやリスクの⼤きさ等を踏まえ、 役割・⽴場に応じて適切なセキュリティ対策の検討が⾏われることを期待
      2. 各指針と要点
         1. 方針

IoTの性質を考慮した基本方針を定める

経営者がIoTセキュリティにコミットする

内部不正やミスに備える

* + - * 1. 分析

IoTのリスクを認識する

守るべきものを特定する

つながることによるリスクを想定する

* + - * 1. 設計

守るべきものを守る・設計を考える

つながる相手に迷惑をかけない設計をする

不特定の相手とつなげられても安全安心を確保できる設計をする

安全安心を実現する設計の評価・検証を行う

* + - * 1. 構築・接続

ネットワーク上での対策を考える

機能及び用途に応じて適切にネットワーク接続する

初期設定に留意する

認証機能を導入する

* + - * 1. 運用・保守

安全安心な状態を維持し、 情報発信・共有を行う

出荷・リリース後も安全安心な状態を維持する

出荷・リリース後もIoTリスクを把握し、 関係者に守ってもらいたいことを伝える

IoTシステム・サービスにおける関係者の役割を認識する

脆弱な機器を把握し、 適切に注意喚起を行う

* + - * 1. 一般利用者のためのルール

問合せ窓やサポートがない機器やサービスの購入・利用を控える

インターネットに接続する機器やサービスの問合せ窓やサポートがない場合、 何か不都合が生じたとしても、 適切に対処すること等が困難になる。 問合せ窓やサポートがない機器やサービスの購入・利用は行わないようにする。

初期設定に気をつける

・機器を初めて使う際には、 IDやパスワードの設定を適切に行う。 パスワードの設定では、 「機器購入時のパスワードのままとしない」、 「他の人とパスワードを共有しない」、 「他のパスワードを使い回さない」等に気をつける。

・取扱説明書等の手順に従って、 自分でアップデートを実施してみる。

使用しなくなった機器については電源を切る

使用しなくなった機器や不具合が生じた機器をインターネットに接続した状態のまま放置すると、 不正利用される恐れがあることから、 使用しなくなった機器は、 そのまま放置せずに電源を切る。

機器を手放す時はデータを消す

情報が他の人に漏れることのないよう、 機器を捨てる、 売るなど機器を手放す時は、 事前に情報を削除する。

* + - 1. 今後の検討
         1. リスク分析に基づく分野別の対策について

IoTは、 様々な分野に浸透していくことになるが、 分野ごとに求められるセキュリティレベルが異なるため、 多くのIoT機器が利用されている、 もしくは利用が想定される分野では、 具体的なIoTの利用シーンを想定し、 詳細なリスク分析を行った上で、 その分野の性質、 特徴に応じた対策を検討する必要がある。

* + - * 1. 法的責任関係について

IoTにおいては、 製造メーカ、 SIer、 サービス提供者、 利用者が複雑な関係になることが多い。 よって、 サイバー攻撃により被害が生じた場合の責任の在り方については、 今後出現するIoTサービスの形態や、 IoTが利用されている分野において規定されている法律などに応じて整理を行っていく必要がある。

* + - * 1. IoT時代のデータ管理の在り方について

IoTシステムでは、 利用者の個人情報等のデータを保持・管理等を行う者又は場所が、 サービスの形態により変わってくる。 IoTシステムの特徴を踏まえつつ、 個人情報や技術情報など重要データを適切に保持・管理等を行うことが必要であり、 その具体的な方法について、 検討していく必要がある。

* + - * 1. IoTに対する総合的なセキュリティ対策について

IoT社会の健全な発展の実現には、 既に実施されている、 情報処理推進機構（IPA）、 情報通信研究機構（NICT）、 JPCERT/CC及びTelecom ISAC Japan(ICT ISAC Japan)のサイバーセキュリティに関する取組に加え、 一般利用者に対するIoT機器のマルウェア感染に関する注意喚起などの取組について、 官民連携による強化を検討する。

* + - * 1. 本ガイドラインの見直しについて

上記のような検討事項の取組や、 IoTを取り巻く社会的な動向、 脆弱性・脅威事象の変化、 対策技術の進歩等を踏まえて、 今後、 必要に応じて改訂を行っていく必要がある。

* + 1. 安全なIoTシステムの創出【2016年3月1日NISC】

ドキュメントを参照: [03shiryou05.pdf](http://www.nisc.go.jp/conference/cs/kenkyu/dai03/pdf/03shiryou05.pdf)

* + - 1. 任務保証の考え方に基づく取組
         1. 業務責任者（任務責任者）がシステム責任者（資産責任者）と、 機能やサービスを全うするという観点からリスクを分析し、 協議し、 残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける「機能保証（任務保証）」の考え方に基づく取組が必要
      2. セキュリティ品質の実現が企業価値
         1. ・IoTシステムのサービスの効用と比較してセキュリティリスクを許容し得る程度まで低減
         2. ・高いレベルのセキュリティ品質の実現が企業価値や国際競争力の源泉に
      3. セキュリティ・バイ・デザインの推進
         1. ・連携される既存システムを含めて、 IoTシステム全体の企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザインの推進が重要。
      4. データとシステム全体のセキュリティ確保
         1. IoTシステムはデータの流通プラットフォーム。
         2. データとシステム全体のセキュリティ確保を行う必要がある。
      5. システム間の相互連携の際のリスク評価
         1. レベルの異なるIoTシステムを相互連携させる場合は、 残存リスクを客観的に評価し、 許容範囲内に収めるためのリスク評価が必要
    1. コンシューマ向けIoTセキュリティガイド【2016年6月24日JNSA】

ドキュメントを参照: [iot](http://www.jnsa.org/result/iot/)

* + 1. IoT早期導入者のためのセキュリティガイダンス【2016年2月24日CSA】

ドキュメントを参照: [Security\_Guidance\_for\_Early\_Adopters\_of\_the\_Internet\_of\_Things\_J\_160224.pdf](https://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf)

* + 1. Guide to Industrial Control Systems (ICS) Security【NIST SP.800-82R2】【JPCERT和訳】

ドキュメントを参照: [NISTSP800-82r2\_20160314.pdf](https://www.jpcert.or.jp/research/2016/NISTSP800-82r2_20160314.pdf)

* + 1. IoTセキュリティ　標準／ガイドライン　ハンドブック　2017年度版【2018年5月8日JNSA】
    2. コンシューマ向けIoTセキュリティガイド【2016年8月1日JNSA】
    3. IoTソリューション領域へのスキル変革の指針【2018年4月10日IPA】
    4. IoTソリューション領域へのスキル変革の指針\_参考文献【2018年4月10日IPA】
    5. 【未整理】IoTへのサイバー攻撃仮想ストーリー集【一般社団法人日本クラウドセキュリティアライアンス（CSAジャパン）】

ドキュメントを参照: [scenario.pdf](https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/scenario.pdf)

* + 1. 【未整理】「つながる世界」を破綻させないためのセキュアなIoT製品開発13のステップ【CSAジャパン　IoTワーキンググループ】

ドキュメントを参照: [future-proofing-the-connected-world\_J\_20170520.pdf](https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/future-proofing-the-connected-world_J_20170520.pdf)

* + 1. 【未整理】工場における産業用IoT導入のためのセキュリティファーストステップ【2018年8月JPCERT/CC】

ドキュメントを参照: [ICS-Security1stStep2018.pdf](https://www.jpcert.or.jp/ics/ICS-Security1stStep2018.pdf)

* + 1. 【未整理】「IoTセキュリティ基盤を活用したが安心安全な社会の実現に向けた実証実験」の結果の公表【2018年6月総務省情報流通行政局】

ドキュメントを参照: [000560886.pdf](http://www.soumu.go.jp/main_content/000560886.pdf)

* + 1. 旧版
       1. 【未整理】IoTセキュリティ総合対策プログレスレポート2018【2018年7月　サイバーセキュリティタスクフォース】

ドキュメントを参照: [000566458.pdf](http://www.soumu.go.jp/main_content/000566458.pdf)

* + - 1. 【未整理】「IoTセキュリティ総合対策」（文書）【2017年12月　総務省情報流通行政局】

ドキュメントを参照: [000510701.pdf](http://www.soumu.go.jp/main_content/000510701.pdf)

* + 1. 【未整理】「IoTセキュリティ総合対策」について（講演会スライド）【2018年2月28日　総務省情報流通行政局】

ドキュメントを参照: [000543066.pdf](http://www.soumu.go.jp/main_content/000543066.pdf)

* + 1. 【未整理】IoTセキュリティ総合対策プログレスレポート2019【2018年5月　サイバーセキュリティタスクフォース】

ドキュメントを参照: [000623344.pdf](http://www.soumu.go.jp/main_content/000623344.pdf)

* + 1.  IoT・5Gセキュリティ総合対策（案）【2019年6月総務省サイバーセキュリティタスクフォース】

ドキュメントを参照: [01cyber01\_02000001\_00031.html](http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00031.html)

* + - 1. 目次
         1. はじめに
         2. Ⅰ 背景
         3. Ⅱ 施策展開の枠組み
         4. Ⅲ 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策

（１）IoTのセキュリティ対策

① IoT機器の設計・製造・販売段階での対策

② IoT機器の設置・運用・保守段階での対策

③ 脆弱性等を有するIoT機器の調査と注意喚起

④ サイバー攻撃に関する電気通信事業者間の情報共有

（２）5Gのセキュリティ対策

① ソフトウェア脆弱性への対応

② ハードウェア脆弱性への対応

（３）クラウドサービスのセキュリティ対策

（４）スマートシティのセキュリティ対策

（５）トラストサービスの在り方の検討

（６）公衆無線LANのセキュリティ対策

（７）重要インフラとしての情報通信分野のセキュリティ対策

（８）地域の情報通信サービスのセキュリティの確保

* + - * 1. Ⅳ 横断的施策

（１）研究開発の推進

① 基礎的・基盤的な研究開発等の推進

② 広域ネットワークスキャンの軽量化

③ ハードウェア脆弱性への対応【再掲】

④ スマートシティのセキュリティ対策【再掲】

⑤ 衛星通信におけるセキュリティ技術の研究開発

⑥ AIを活用したサイバー攻撃検知・解析技術の研究開発

⑦ 量子コンピュータ時代に向けた暗号の在り方の検討

⑧ 重要インフラ等におけるサイバーセキュリティの確保

⑨ IoT 社会に対応したサイバー・フィジカル・セキュリティ対策

（２）人材育成・普及啓発の推進

① 実践的サイバー防御演習（CYDER）の実施

② 2020東京大会に向けたサイバー演習の実施

③ 若手セキュリティ人材の育成の促進

④ 地域のセキュリティ人材育成

（３）国際連携の推進

① ASEAN各国との連携

② 国際的なISAC間連携

③ 国際標準化の推進

④ サイバー空間における国際ルールを巡る議論への積極的参画

（４）情報共有・情報開示の促進

① サイバー攻撃に関する電気通信事業者間の情報共有【再掲】

② 事業者間での情報共有を促進するための基盤の構築

③ サイバーセキュリティ対策に係る情報開示の促進

④ サイバーセキュリティ対策に係る投資の促進

⑤ 国際的なISAC間連携【再掲】

* + - * 1. Ⅴ 今後の進め方
      1. 内容抜粋
         1. はじめに

IoTをはじめとするICTの利活用が一層進展していく中で、 今後、 5Gのサービスが開始することが予定されているほか、 Society5.0に向けた適切なデータ管理・流通の重要性やサプライチェーンリスクへの対応などの必要性が増大するなど、 サイバーセキュリティリスクへの対策の一層の強化は急務となっている。

今般、 「IoTセキュリティ総合対策」策定・公表後の様々な状況変化などを踏まえつつ、 IoT・5G時代にふさわしいサイバーセキュリティ政策の在り方について検討し、 「IoT・5Gセキュリティ総合対策」として整理したものである。

* + - * 1. Ⅰ 背景

（１）ICT利活用の進展

ICT（Information and Communications Technology：情報通信技術）によって、 我が国の社会・経済は大きく変革を遂げてきた。 人々の日々のコミュニケーションや情報収集、 企業活動、 購買行動、 就労、 余暇など、 社会・経済のあらゆる場面でICTの利活用が浸透している。 令和の時代に入り、 この流れは今後も加速していくことが想定される。

このような変化をもたらしたICTの発展の態様については大きく以下の５つに大別することができる。

①ブロードバンド化（小容量通信から大容量通信へ）

②モバイル化（固定から移動へ）

③クラウド化（オンプレミス1からクラウドへ）

④IoT化（人からモノへ）

⑤AI化（人からAIへ）

2020年（令和２年）に5Gサービスが本格的に開始されることにより、 このような流れはより一層加速していくことが予測され、 我が国が目指すべき社会像としてのSociety5.0の到来を迎え、 今後、 サイバー空間と実空間の一体化が一層進展していくことが想定される。

（２）サイバーセキュリティリスクの増大や脅威の深刻化

社会・経済全体のあらゆる場面でのICTの利活用が水や空気のように浸透してきたところであるが、 同時に必然的にサイバーセキュリティリスクも増大している状況である。

サイバーセキュリティリスクは、 インシデントの影響度の大きさ×発生確率で表されるが、 社会・経済のICTへの依存度が高まれば高まるほど、 インシデントが発生した際の脅威や影響も飛躍的に増大し、 またインシデントが発生する確率も高くなる。

そのため、 サイバーセキュリティの確保は、 ICTの利活用による社会や経済の持続的・安定的な発展のために必要不可欠な取組となっている。

、 直近で特に対策が必要となるサイバーセキュリティ上の留意事項としては以下のような点が挙げられる。

① 5Gのサービス開始に伴う新たなリスク

今後サービスが開始される予定の5Gについては、 従来までの移動通信システムと比較して、 ①超高速、 ②超低遅延、 ③多数同時接続であるという特徴を有しており、 IoTシステムの基盤技術として、 電気通信事業者のみならず、 様々な主体や産業分野での利活用が期待されている。

他方、 サイバーセキュリティの観点からは、 5Gのネットワークはネットワーク機能の仮想化・ソフトウェア化やモバイルエッジコンピューティング2（以下「MEC」という。 ）など、 従来のネットワークとは構造等の点において異なる特徴を有することが想定されるから、 その点を踏まえ、 5Gのネットワークのセキュリティ確保の在り方について検討する必要がある。

また、 5Gのサービス開始により、 従来に比べて産業用途でのIoT機器の設置・運用が今後も増加していくことが想定されるため、 IoT機器のセキュリティの確保（脆弱性対策を含む）の重要性が今後さらに高まっていくことが想定される。

さらに、 従来はインターネットから隔離された形で運用されていた産業機器やインフラなどが無線経由でインターネットに接続される可能性が高くなることから、 IT系（情報系）だけでなく、 OT系（制御系）のシステムのセキュリティ対策も今後より一層重要になることが想定される。

② サプライチェーンリスクの管理の重要性

今日では、 サイバー空間と実空間の一体化の進展や、 サプライチェーンのグローバル化の進展により、 ソフトウェアやハードウェアのサプライチェーンなど、 ICTの製品やサービスを製造・流通する過程において不正なプログラムやファームウェアの組み込み、 又は改ざんなどが行われるリスクへの対応3が求められている。

また、 製品やサービスそのもののリスクだけではなく、 委託等の契約関係がある関係者の間でサイバーセキュリティ対策が不十分な者が踏み台となって他者へのサイバー攻撃がなされ、 被害が伝播する「被害のチェーン」が発生するおそれもある。

そのため昨今では、 企業単体ではなく、 サプライチェーン単位でのサイバーセキュリティ対策が求められている状況4であり、 特に地域の中小企業では、 人材を含めたリソース不足のため、 サイバーセキュリティ対策が遅れている可能性があることから、 対策の強化の取組が必要不可欠となっている。

③ Society5.0の実現に向けた適切なデータの流通・管理の重要性

Society5.0はサイバー空間と実空間を高度に融合させることにより、 経済的発展と社会的発展の解決を両立する「人間中心の社会」であり、 言い換えれば、 サイバー空間と実空間の間でデータが循環して、 相互に作用し、 これを前提とした様々なサービスが提供され、 人々の生活に浸透し、 恩恵をもたらす社会である。

そのSociety5.0の実現の鍵となるのがデータであり、 データの利活用・管理の利便性を高めるクラウドサービスの安全性の確保や、 データ収集・分析を都市や地域の機能やサービスを効率化・高度化に生かすスマートシティのセキュリティの確保等の重要性が高まっている。 また、 データ流通の有効性を担保するための基盤として、 ネット利用者の本人確認やデータの改ざん防止等の仕組みであるトラストサービスの必要性も高まっている。

また、 経済のグローバル化が進展する今日においては、 国内のみならず国際的なデータの移転も大幅に増加している5。 この点、 諸外国に目を転じてみれば、 EUのGDPR（一般データ保護規則：General Data Preservation Rule）、 米国のFISMA（連邦情報セキュリティマネジメント法：Federal Information Security Management Act）、 中国のサイバーセキュリティ法など、 各国の政府が企業などに対して国境を越えてデータを移転させないような法規制を導入している例も出始めているところである。

そのため、 上述のような流れも認識しつつ、 機密性（Confidentiality）・完全性（Integrity）・可用性（Availability）・真正性（Authenticity）等の確保の観点からの適切なデータの管理・流通の在り方、 及びそれを実現するための手段等について検討する必要がある。

⑥ 大規模な国際イベント等の開催

大規模かつ非日常の国際イベントは最高度の注目を集めることから、 サイバー攻撃の標的となるおそれがある。

この点、 2019年（令和元年）にはG20やラグビーワールドカップ、 2020年（令和２年）には2020年東京オリンピック・パラリンピック競技大会（以下「2020東京大会」という。 ）の開催が予定されている。

そのため、 過去の経験も踏まえつつ、 大会に関係する重要なサービスを担う事業者のリスクマネジメントや対処体制の構築、 訓練・演習の強化など、 特に重要インフラ事業者、 重要サービス事業者等において、 これまで実施されてきた対策の一層の強化が求められる。

また、 2020東京大会が無事成功裏に終わったとしても、 社会に対するサービスの提供を行うという「任務」8を担う重要インフラ事業者等にとっては、 サイバー攻撃への対処態勢の強化は日常的に重要な課題であり、 引き続き、 平時・有事の対策を着実に実行することが求められる。

上記のような状況を踏まえ、 昨今でサイバーセキュリティ対策は一層重要度を増していることから、 2017年（平成29年）10月に策定・公表した「IoTセキュリティ総合対策」を発展的に改編する形で、 IoT・5G時代にふさわしいサイバーセキュリティ政策の在り方として、 今般「IoT・5Gセキュリティ総合対策」を策定することとしたものである。

* + - * 1. Ⅱ 施策展開の枠組み

概要

サイバーセキュリティ対策は広範な政策分野であり、 その推進に当たっては各主体の適切な役割分担の下での連携・協働が必要である。

この点、 総務省に期待される役割は、 まず情報通信サービス・ネットワークの、 特に重点的に対応すべき個別分野のセキュリティの在り方について包括的な検討の上、 関係府省庁や民間企業と連携しつつ、 政策を実効的に推進していくことである。

さらに、 当該分野での政策をより効果的に実施するための研究開発の推進や、 情報通信サービス・ネットワークのユーザも含めた人材育成・普及啓発の推進、 国際連携の推進、 サイバーセキュリティに関する情報共有・情報開示の促進観点からの取組を並行して進めていく必要がある。

そのため、 本文書では、 総務省として取り組むべき具体的な施策について、 「Ⅲ 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策」と「Ⅳ 横断的施策」の「（１）研究開発の推進」、 「（２）人材育成・普及啓発の推進」、 「（３）国際連携の推進」、 「（４）情報共有・情報開示の促進」という項目で整理を行っている。

なお、 施策の検討・展開の際には、 それぞれの取組において、 例えば以下のような観点について留意しつつ、 施策の有効性を確保する必要がある。

① ネットワーク側とユーザ側の双方の観点からの施策展開

情報通信サービス・ネットワーク全体の安全性や信頼性を確保するためには、 ネットワーク側とユーザ側の双方の視点でサイバーセキュリティ対策を推進するための施策を検討する必要がある。

② 情報通信サービス・ネットワークのレイヤー構造

情報通信サービス・ネットワークについては、 機能に着目して構造的にアプリケーション層、 プラットフォーム層、 ネットワーク層、 端末層と分類が可能であるが、 それぞれの層において留意すべき脅威とセキュリティ要件の在り方について検討する必要がある。

③ 時間軸を意識した施策展開

IoT機器のライフサイクル、 人材育成のスパンなど、 施策の効果の発現に関する時間軸を意識した政策立案を行う必要がある。

④ 政策バリューチェーンの構築

例えば、 研究開発の成果を情報通信サービス・ネットワークの個別分野の施策に反映しつつ、 その成果について国際的な展開を図る、

また、 情報通信サービス・ネットワークの個別分野のセキュリティに関する施策と人材育成の施策を連携させて、 地域のサイバーセキュリティ確保を一体的に推進するなど、 個別施策を有機的に連携させ、 横断的で一貫性のある施策展開を図る必要がある。

* + - * 1. Ⅲ 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策

概要

総務省においてセキュリティの確保に取り組むべき情報通信サービス・ネットワークの個別分野としては、 以下のような分野が考えられる。

まず、 今後の5Gサービスの開始を迎え、 IoT及び5Gのセキュリティ対策は重要な政策課題となっており、 既に始まっている取組と合わせて重点的に取り組んでいく必要がある。

また、 Society5.0の実現に向けたデータ流通や管理の需要性が増している中で、 クラウドサービスの安全性の確保やスマートシティのセキュリティの確保も必要性が高まっているほか、 データ流通の有効性を担保するための基盤としてのトラストサービスの在り方の検討も必要となっている。

さらに、 昨今ではサプライチェーンの弱いところを狙った攻撃が散見されることから、 我が国の情報通信サービス・ネットワーク全体のセキュリティの確保のため、 地域の情報通信サービス・ネットワークのセキュリティ強化も必要である。

その上で、 2020東京大会及びその後を見据え、 公衆無線LANのセキュリティの確保や、 重要インフラ分野・重要サービス分野としての情報通信分野のセキュリティの確保などにも取り組む必要がある。

なお、 具体的施策の検討・実施に当たっては、 前述（Ⅱ）の①～④の観点などに留意する必要がある。

（１）IoTのセキュリティ対策

IoT機器の脆弱性については、 IoT機器の①設計・製造・販売（輸入を含む。 ） 段階、 ②設置・運用・保守段階において適切な対策をとる必要がある。

また、 既にインターネットに接続されて設置・運用されているIoT機器が多数あることが想定されることから、 IoT機器の脆弱性等の調査を実施するとともに、 利用者への注意喚起や情報共有の取組等を推進する必要がある。

① IoT機器の設計・製造・販売段階での対策

設計・製造・販売段階においては、 製造業者におけるIoT機器のセキュリティ・バイ・デザインの考え方を十分に浸透させるとともに、 対策がとられた機器の市場への展開を促進させることが重要となる。

この点、 IoT機器に関する基本的なセキュリティ対策については、 電気通信事業法（昭和59年法律第86号）の枠組みにおいて端末設備等規則（昭和60年郵政省令第31号）を改正し、 強制規格としての技術基準が策定9されている（2019年（平成31年）３月１日公布、 2020（令和２年）年４月１日施行）。 また、 当該改正後の同規則の各規定等に係る端末機器の基準認証に関する運用について明確化を図る観点から、 総務省において2019年（平成31年）４月に「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第１版)」を策定・公表している。 今後は、 当該技術基準の運用開始に向けた準備を進めることが必要である。

また、 IoT機器に関するセキュリティ対策の上乗せ部分については、 民間団体がセキュリティ要件のガイドラインを策定し、 さらに当該要件に適合したIoT機器に対して適合していることを示すマークを付す認証（Certification）制度の構築の準備を進めていることから、 このような民間の任意の認証（Certification）制度の普及が期待される。

② IoT機器の設置・運用・保守段階での対策

機器の性格上セキュリティ対策を取ることが困難なものや海外製品など、 流通するIoT機器の中から、 脆弱性を有するIoT機器を完全に排除することは困難であることから、 機器の設置・運用・保守段階（ネットワークへの接続時又は接続後）において、 脆弱性を有する機器が存在することを前提として、 セキュアなIoTシステム構築を実現する仕組みが重要である。

また、 IoT機器は広範な利用者が利用することが想定されており、 利用者によっては、 IoT機器やセキュリティに関する知識が十分に無いことが想定される。 したがって、 例えば、 IoT機器の設置後に新たな脆弱性が発見された場合に、 当該IoT機器の製造業者によって脆弱性のパッチがユーザサポートの一環として提供されるなど、 各種事業者の側において対策が実施される仕組みの構築が重要である。

IoTシステム・サービス全体としてのセキュリティの確保に関しては、 IoT機器だけでなく、 ネットワーク側での対処の在り方についても検討が必要である。 この点で、 IoT機器の不正検知等のため、 IoT機器とインターネットの境界上にセキュアゲートウェイ（IoTセキュアゲートウェイ）を設置する取組が考えられる。 本取組について、 Ⅲ－（４）のスマートシティのセキュリティ対策の取組等を通じ、 実際の導入を進める仕組みや方策について検討することが重要である。

③ 脆弱性等を有するIoT機器の調査と注意喚起

前述の①、 ②の対策については、 実効性を発揮するまでに一定程度の時間を有することから、 まずは既に設置されているIoT機器に関する脆弱性等の有無の調査を実施し、 必要な対応を速やかに実施する必要がある。

この点、 国立研究開発法人情報通信研究機構（以下「NICT」という。 ）の業務に、 パスワード設定等に不備のあるIoT機器の調査等を５年間の時限措置として追加する等を内容とする国立研究開発法人情報通信研究機構法の改正を実施し、 2019年（平成31年）２月より、 NICTがIoT機器を調査し、 電気通信事業者を通じて利用者への注意喚起を行うプロジェクト「NOTICE10」を開始したところであり、 引き続き、 本プロジェクトの着実な実施を通じ、 既に現在設置されているIoT機器のセキュリティ対策を進めることが必要である。

また、 「NOTICE」の取組に加えて、 既にマルウェアに感染しているIoT機器をNICTの「NICTER」プロジェクトで得られた情報を基に特定し、 電気通信事業者を通じて利用者へ注意喚起を行う取組を実施することも必要である。

さらに上述の取組の実施にあたり、 専用のサポートセンターを設置し、 行政相談窓口や消費生活センター等と連携しつつ、 ウェブサイトや電話による問合せ対応を通じて利用者に適切なIoT機器のセキュリティ対策を案内することも必要である。

加えて、 これらの取組については、 IoT機器のセキュリティ対策のベストプラクティスとして、 Ⅳ－（３）の国際連携の推進などの取組を通じ、 海外各国に対して発信し、 各国の取組につながるよう働きかけることが重要である。

④ サイバー攻撃に関する電気通信事業者間の情報共有

脆弱性を有するIoT機器が踏み台となったことが確認された際、 被害の拡大を防止するため、 ISPによる、 当該ISPの利用者の端末とC&Cサーバ11の間の通信を遮断する等の取組が必要である。

この点、 総務省では、 2018年（平成30年）５月の改正電気通信事業法において、 電気通信事業者が「送信型対電気通信設備サイバー攻撃」への対応を共同して行うため、 攻撃の送信元情報の共有やC&Cサーバの調査研究等の業務を行う第三者機関（認定送信型対電気通信設備サイバー攻撃対処協会。 以下「認定協会」という。 ）を総務大臣が認定する制度を創設し、 2019年（平成31年）１月に一般社団法人ICT-ISAC12が認定されたところである。

今後は認定協会の活動について、 マルウェアに感染している可能性の高いIoT端末等やC&Cサーバであると疑われる機器の検知や利用者への注意喚起等の電気通信事業者が行う対策に向け、 円滑な実施のための支援を行うなどの取組を促進することが重要である。

また、 こうした認定協会の活動や「NOTICE」の実施状況も踏まえ、 電気通信事業者等が協力してサイバー攻撃への対処を行う際の基盤となる効果的な情報共有の在り方について引き続き検討することが重要である。

（２）5Gのセキュリティ対策

① ソフトウェア脆弱性への対応

今後サービスが開始される予定の5Gについては、 従来までの移動通信システムと比較して、 ①超高速、 ②超低遅延、 ③多数同時接続であるという特徴を有しており、 IoTシステムの基盤技術として、 電気通信事業者のみならず、 様々な主体や産業分野での利活用が期待されている。

一方、 5Gのネットワークに関しては、 ネットワーク機能の仮想化・ソフトウェア化が進むことから、 新たなサイバーセキュリティ上の課題が懸念される。 また、 新たにネットワークのエッジ（基地局とコア網の間に設置）で通信処理や高度な演算・データ処理がなされるモバイルエッジコンピューティング（

MEC）が利用されることから、 ネットワークインフラとしての機能維持のためには、 基地局やコア網のみならず、 MECも含めた各構成要素（デバイス、 クラウド、 アプリケーション等）全体を考慮したセキュリティの確保が必要不可欠である。

そのため、 5Gの各構成要素におけるソフトウェアを含むセキュリティを総合的かつ継続的に担保する仕組みを整備し、 ガイドライン等によって対策の共有等を図ることを通じ、 5Gを構築・活用する重要インフラ事業者等への周知・啓発を図ることが必要である。

また、 5Gのセキュリティの確保は、 国際的にも重要な政策課題であることから、 作成したガイドライン等について国際機関等への提案も視野に入れるなど、 諸外国との連携を図ることが期待される。

② ハードウェア脆弱性への対応

機器のセキュリティについては、 機器にインストールされているソフトウェアだけでなく、 集積回路の設計工程において、 ハードウェア脆弱性が存在する可能性が指摘されている。

そのため、 総務省では、 2017年度（平成29年度）より、 戦略的情報通信研究開発推進事業（SCOPE）において、 ハードウェア脆弱性の検知技術の研究開発を実施し、 膨大な数の回路設計図をビッグデータとして収集・蓄積しつつ、 脆弱性が存在する可能性のあるチップを、 AIを活用して類型化し、 ハードウェア脆弱性を発見するための研究開発を実施してきたところである。

5Gの時代を見据え、 サプライチェーンリスクへの対応の観点から、 ソフトウェアやファームウェアに対する対策と合わせて、 引き続き、 ビッグデータやAIを活用しつつハードウェアに組み込まれるおそれのある脆弱性を検出する技術の研究開発等を推進することが必要である。

（３）クラウドサービスのセキュリティ対策

ICTの利活用が社会全体として進展する中、 インターネット上のリソースを臨機応変に活用するクラウドサービスは、 サービスアプリケーションから多様なIoTプラットフォームまで、 様々なICTソリューションを支えており、 データの利活用・管理における中核のサービスとなっている。

その中で、 我が国の政府においても「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018年（平成30年）６月７日CIO連絡会議決定）を定め、 情報システム調達に際しては、 コスト削減や柔軟なリソースの増減等の観点から、 クラウドサービスの利用を第一候補として検討を行う旨の方向性が示されているところである。

この点、 諸外国では、 2010年代に政府が情報システム調達においてクラウドファーストを掲げ、 その後間もなく、 政府が主導してクラウドサービスの安全性を評価する制度を構築・運用している事例があり、 2018年（平成30年）に上述のクラウド・バイ・デフォルト原則を採用した我が国においても、 安全性評価の制度の検討が必要な段階に到達している。

そのため、 総務省と経済産業省において、 クラウドサービスの安全性評価に関する検討を行うことを目的として、 2018年（平成30年）８月より、 「クラウドサービスの安全性評価に関する検討会」を開催し、 2019年（平成31年）３月に制度の枠組みが示されたところである。

本枠組みを踏まえつつ、 官民双方が一層安全・安心にクラウドサービスを採用し、 継続的に利用していくため、 クラウドサービスの安全性評価制度について、 引き続き、 総務省において、 経済産業省と連携しつつ、 2020年（令和２年）の制度の開始を目指して、 評価基準や制度の確立に向けた検討を進めることが必要である。

（４）スマートシティのセキュリティ対策

スマートシティは、 先進的技術の活用により、 都市や地域の機能やサービスを効率化・高度化し、 各種の課題の解決を図るとともに、 快適性や利便性を含めた新たな価値を創出する取組であり、 Society5.0の先行的な実現の場である。

この点、 総務省では、 都市に設置されたセンサーから収集・生成・蓄積・解析されるデータを活用し、 その解析結果を都市経営の課題解決などに活用するデータ利活用型スマートシティ事業を2017年度（平成29年度）から実施しているところである。 なお、 今後は政府のスマートシティに係る各事業の連携や分野間のデータ連携等を協力推進していくため、 関係本部・省庁で連携13していくこととされている。

他方、 スマートシティでは、 インターネットに接続するセンサー・カメラ等が散在し、 多様なデータが流通しているため、 常にサイバー攻撃のリスクにさらされるおそれがある。

また、 様々なデータが共通プラットフォーム上で流通する中で、 データの真正性の確保や適切なデータ流通の管理の仕組みの構築等も必要である。 さらに、 システムとしてのスマートシティの構築・運用には多様な主体が関わることから、 システム全体としてのセキュリティの在り方について多様な関係者間で一定の共通認識の醸成が必要である。

そのため、 スマートシティ上の様々なユースケース（分野）やアーキテクチャ、 相互運用性などを踏まえつつ、 スマートシティに求められるセキュリティ要件について検討を行い、 明確化を図る必要がある。

また、 スマートシティの取組は国際的にもEUの研究開発プロジェクトHorizon 2020やNISTが主導するGCTC（Global City Teams Challenge14）プロジェクトでも展開されており、 総務省ではEUと連携した、 スマートシティ分野のセキュリティ・プライバシ保護を含む日EU共同研究（Fed4IoT15）を2018年（平成30年）から実施している。

そのため、 上述の成果については諸外国と連携の上、 国際標準化や必要に応じた国際的な議論の場への提案を検討するなど、 諸外国との調和を意識して展開を図ることが重要である。

さらに、 スマートシティのシステムでは、 多種多様なIoT機器が活用されることが想定されることから、 そのセキュリティの確保に当たっては、 IoT機器そのもののセキュリティの強化だけでなく、 ネットワークの側でIoT機器の不正検知等を実施するための仕組みが有効であり、 実際の運用に関して、 Ⅲ－（１）－②のIoT機器とインターネットの境界上にセキュアゲートウェイを設置する取組との連携の在り方も検討することが重要である。

（５）トラストサービスの在り方の検討

Society5.0の実現に向けて、 サイバー空間の自由で安心・安全なデータの流通を実現するためには、 データの信頼性を確保する仕組みとして、 データの改ざんや送信元のなりすまし等を防止するトラストサービスが不可欠である。

そのため、 総務省では、 「プラットフォームサービスに関する研究会」の下に「トラストサービス検討ワーキンググループ」を設置し、 2019年（平成31年）１月から、 以下のようなトラストサービスに関する現状や課題について検討を行っている。

１）人の正当性を確認できる仕組み（電子署名）

２）組織の正当性を確認できる仕組み（組織を対象とする認証、 ウェブサイト認証）

３）IoT機器等のモノの正当性を確認できる仕組み

４）データの存在証明・非改ざんの保証の仕組み（タイムスタンプ）

５）データの送達等を保証する仕組み（eデリバリー）

一方、 EUにおいては2016年（平成28年）７月に発効したeIDAS（electronic Identification and Authentication Services）規則により、 電子署名、 タイムスタンプ、 eシール等のトラストサービスについて包括的に規定している状況である。

そのため、 国際的な相互運用性の確保の観点からも、 引き続き、 同ワーキンググループにおいて、 制度的課題等について整理を行い、 トラストサービスの在り方について2019年（令和元年）中を目途に結論が得られるよう、 検討を進めることが必要である。

（６）公衆無線LANのセキュリティ対策

公衆無線LANについては、 2020年東京大会に向けて、 観光や防災の観点から、 その普及が進んでいるところである。 他方、 多くの公衆無線LANのサービスにおいて、 依然としてサイバーセキュリティに対する配慮に欠けるものも多く、 これらのサービスを踏み台にした攻撃や情報漏洩などのインシデントが発生するおそれもある。

そのため、 公衆無線LANの利用者や提供者向けの公衆無線LANの利用の手引きの普及を図るなど、 利用者・提供者において必要となるセキュリティ対策に関する周知啓発の充実を図ることが重要である。

その際、 Ⅲ－（８）の地域の情報通信サービスのセキュリティの確保の取組で構築する連絡体制を活用し、 効果的な周知啓発を図ることが重要である。

（７）重要インフラとしての情報通信分野のセキュリティ対策

情報通信分野は、 「重要インフラの情報セキュリティに係る第４次行動計画」（平成29年４月18日サイバーセキュリティ戦略本部決定 平成30年７月25日サイバーセキュリティ戦略本部改定。 以下「第４次行動計画」という。 ）において、 特にその機能が停止又は低下した場合に国民生活・社会経済活動に多大なる影響を及ぼしかねないサービスとして重要インフラの14分野の１つに指定されている。

第４次行動計画を踏まえ、 重要インフラ各分野に横断的な指針として「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」（平成30年４月サイバーセキュリティ戦略本部決定 令和元年５月サイバーセキュリティ戦略本部改定）が定められており、 同指針を踏まえ、 官民で連携して、 安全基準等の整備及び浸透の取組が進められている。

この点、 電気通信においては、 各年の取組として、 「電気通信事故検証会議」等の枠組みを通じ、 電気通信事故の分析・検証等を行うとともに、 事故再発防止のため、 「情報通信ネットワーク・安全信頼性基準」等の見直しの必要性について検討を行っている。

また、 2018年度（平成30年度）には、 前述のⅢ－（１）－④のとおり、 「送信型対電気通信設備サイバー攻撃」に関する送信元情報の共有やC&Cサーバの調査研究等を行う第三者機関として認定協会を総務大臣が認定する制度を創設した。 さらに本制度改正に関連して、 「送信型対電気通信設備サイバー攻撃」が原因である電気通信事故の発生状況を把握する観点から当該事故の報告を求めるため、 電気通信事業報告規則を改正する制度整備が行われている。

以上のような取組も踏まえつつ、 引き続き、 必要に応じて情報通信分野のセキュリティ対策に関する制度的枠組みの改善等に向けた取組が行われることが期待される。

（８）地域の情報通信サービスのセキュリティの確保

我が国の情報通信サービス・ネットワークの安全性や信頼性の確保の観点からは、 全国規模や首都圏でサービスを提供している事業者だけでなく、 地域単位で情報通信サービスを提供している事業者におけるサイバーセキュリティの確保も重要な課題である。

他方、 地域においては、 首都圏と比較してサイバーセキュリティに関する情報格差が存在するほか、 経営リソースの不足等の理由により、 セキュリティ対策が十分でないケースが存在するおそれがある。

そのため、 業界団体やセキュリティ関係機関等と連携しつつ、 地域の事業者のサイバーセキュリティ対策の質の向上に向けた連絡体制を構築することが必要である。 なお、 当該施策の展開に当たっては、 Ⅲ－（６）の公衆無線

LANのセキュリティの確保やⅣ－（２）－①の実践的サイバー防御演習（CYDER）の実施、 Ⅳ－（２）－④の地域のセキュリティ人材育成の取組等との連携を図り、 効果的に地域の情報通信サービスのセキュリティ対策の質の向上を図ることが重要である。

* + - * 1. Ⅳ 横断的施策

（１）研究開発の推進

① 基礎的・基盤的な研究開発等の推進

② 広域ネットワークスキャンの軽量化

③ ハードウェア脆弱性への対応【再掲】

④ スマートシティのセキュリティ対策【再掲】

⑤ 衛星通信におけるセキュリティ技術の研究開発

⑥ AIを活用したサイバー攻撃検知・解析技術の研究開発

⑦ 量子コンピュータ時代に向けた暗号の在り方の検討

⑧ 重要インフラ等におけるサイバーセキュリティの確保

⑨ IoT 社会に対応したサイバー・フィジカル・セキュリティ対策

（２）人材育成・普及啓発の推進

① 実践的サイバー防御演習（CYDER）の実施

② 2020東京大会に向けたサイバー演習の実施

③ 若手セキュリティ人材の育成の促進

④ 地域のセキュリティ人材育成

（３）国際連携の推進

① ASEAN各国との連携

② 国際的なISAC間連携

③ 国際標準化の推進

④ サイバー空間における国際ルールを巡る議論への積極的参画

（４）情報共有・情報開示の促進

① サイバー攻撃に関する電気通信事業者間の情報共有【再掲】

② 事業者間での情報共有を促進するための基盤の構築

③ サイバーセキュリティ対策に係る情報開示の促進

④ サイバーセキュリティ対策に係る投資の促進

⑤ 国際的なISAC間連携【再掲】

* + - * 1. Ⅴ 今後の進め方

「IoT・5Gセキュリティ総合対策」の推進に際しては、 定期的に検証を行い、 進捗状況を把握するとともに、 本分野における技術革新や最新のサイバー攻撃の態様を踏まえ、 必要に応じて随時見直しを行っていくことが望ましい。 また、 対策の推進に際しては、 内閣官房内閣サイバーセキュリティセンターや経済産業省をはじめ、 関係府省庁との連携の下に進めていく必要がある。

「IoT・5Gセキュリティ総合対策」の推進は、 2020年東京大会の成功に向けても必須である。 重要インフラの防御対策強化の観点を含め、 関係するステークホルダーの連携によるビジョンの共有と取組の強化が不可欠である。

* 1. クラウド
     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2013年版【METI】

ドキュメントを参照: [20140314004-3.pdf](http://www.meti.go.jp/press/2013/03/20140314004/20140314004-3.pdf)

* + 1. クラウドサービス提供における情報セキュリティ対策ガイドライン【2014年4月総務省】

ドキュメントを参照: [01ryutsu03\_02000073.html](http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html)

* + 1. クラウドセキュリティ関連ISO規格
       1. ■ISO/IEC27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項（スライド）【JIPDEC】

ドキュメントを参照: [JIP-ISMS517-10.pdf](https://www.isms.jipdec.or.jp/doc/JIP-ISMS517-10.pdf)

* + - 1. ■ISMSクラウドセキュリティ認証の概要（スライド）【JIPDEC】

ドキュメントを参照: [shiryou-1.pdf](https://www.isms.jipdec.or.jp/seminar/cloud/shiryou-1.pdf)

* + - 1. ■ISO/IEC27017:2015に基づくクラウドセキュリティの構築のポイント（スライド）【JIPDEC】

ドキュメントを参照: [shiryou-2.pdf](https://www.isms.jipdec.or.jp/seminar/cloud/shiryou-2.pdf)

* 1. テレワーク
     1. 【新規】テレワークではじめる働き方改革テレワークの導入・運用ガイドブック【厚生労働省】

ドキュメントを参照: [01\_01.pdf](https://work-holiday.mhlw.go.jp/material/pdf/category7/01_01.pdf)

* + - 1. システム方式
         1. リモートデスクトップ
         2. 仮想デスクトップ
         3. クラウド型アプリ
         4. 会社ＰＣ持ち帰り
      2. 端末デバイス
         1. リッチクライアント
         2. シンクライアント
         3. タブレット型PC
         4. スマートフォン
         5. 携帯電話
      3. セキュリティ
         1. 本人認証
         2. 端末認証
         3. 端末管理
         4. 暗号化通信
         5. ストレージ暗号化
    1. 【校正中】テレワークセキュリティガイドライン第４版【2018年4月総務省】

ドキュメントを参照: [000545372.pdf](http://www.soumu.go.jp/main_content/000545372.pdf)

* + - 1. はじめに
         1. テレワークとは？

在宅勤務

モバイル

サテライトオフィス

* + - 1. 1. テレワークにおける情報セキュリティ対策の考え方
         1. （ア） 「ルール」「人」「技術」のバランスがとれた対策の実施

図 1 テレワークにおける脅威と脆弱性について

図 2 情報セキュリティ対策におけるバランスの考え方

【コラム】 中小企業の情報セキュリティ対策を支援する取組

* + - * 1. （イ） テレワークの方法に応じた対策の考え方

表1 テレワークの６種類のパターン

リモートデスクトップ方式

仮想デスクトップ方式

クラウド型アプリ方式

セキュアブラウザ方式

アプリケーションラッピング方式

会社ＰＣの持ち帰り方式

図3 リモートデスクトップ方式

図4 仮想デスクトップ方式

図5 クラウド型アプリ方式

図6 セキュアブラウザ方式

図7 アプリケーションラッピング方式

図8 会社PC の持ち帰り方式

（自社にふさわしいテレワークの方式の検討）

（クラウドサービスの利用について）

図9 クラウドサービスへの移行

* + - * 1. （ウ） 経営者、 システム管理者及びテレワーク勤務者それぞれの立場

＜システム管理者＞

＜テレワーク勤務者＞

* + - 1. 2. テレワークセキュリティ対策のポイント
         1. （ア） 経営者が実施すべき対策

（情報セキュリティ保全対策の大枠）

経営者は、 テレワークの実施を考慮した情報セキュリティポリシーを定め定期的に監査し、 その内容に応じて見直しを行う。

社内で扱う情報について、 その重要度に応じたレベル分けを行った上で、 テレワークでの利用可否と利用可の場合の取扱方法を定める。

テレワーク勤務者が情報セキュリティ対策の重要性を理解した上で作業を行えるようにするため、 定期的に教育・啓発活動を実施させる。

情報セキュリティ事故の発生に備えて、 迅速な対応がとれるように連絡体制を整えるとともに、 事故時の対応についての訓練を実施させる。

テレワークにおける情報セキュリティ対策に適切な理解を示した上で、 必要な人材・資源に必要な予算を割り当てる。

* + - * 1. （イ） システム管理者が実施すべき対策

（情報セキュリティ保全対策の大枠）

システム全体を管理する重要な立場であることを自覚し、 情報セキュリティポリシーに従ってテレワークのセキュリティ維持に関する技術的対策を講じるとともに定期的に実施状況を監査する。

情報のレベル分けに応じて、 電子データに対するアクセス制御、 暗号化の要否や印刷可否などの設定を行う。

テレワーク勤務者の情報セキュリティに関する認識を確実なものにするために、 定期的に教育・啓発活動を実施する。

情報セキュリティ事故の発生に備えて、 迅速な対応がとれるように連絡体制を確認するとともに、 事故時の対応についての訓練を実施する。

（悪意のソフトウェアに対する対策）

フィルタリング等を用いて、 テレワーク勤務者が危険なサイトにアクセスしないように設定する。

テレワーク勤務者がテレワーク端末にアプリケーションをインストールする際は申請させ、 情報セキュリティ上の問題がないことを確認した上で認める。

貸与用のテレワーク端末にウイルス対策ソフトをインストールし、 最新の定義ファイルが適用されているようにする。

貸与用のテレワーク端末のＯＳ及びソフトウェアについて、 アップデートを行い最新の状態に保つ。

私用端末をテレワークに利用させる際は、 その端末に必要な情報セキュリティ対策が施されていることを確認させた上で認める。

ランサムウェアの感染に備え、 重要な電子データのバックアップを社内システムから切り離した状態で保存する。

金融機関や物流業者からの事務連絡を装うなどの不審なメールが迷惑メールとして分類されるよう設定する。

（端末の紛失・盗難に対する対策）

台帳等を整備し、 貸与するテレワーク端末の所在や利用者等を管理する。

（重要情報の盗聴に対する対策）

テレワーク端末において無線LAN の脆弱性対策が適切に講じられるようにする。

（不正侵入・踏み台に対する対策）

社外から社内システムへアクセスするための利用者認証について、 技術的基準を明確に定め、 適正に管理・運用する。

テレワーク勤務者がインターネット経由で社内システムにアクセスする際のアクセス方法を定める。 また、 社内システムとインターネットの境界線にはファイアウォールやルータ等を設置し、 アクセス状況を監視するとともに、 不必要なアクセスを遮断する。

社内システムへのアクセス用のパスワードとして、 強度の低いものを用いることができないように設定する。

（外部サービスの利用に対する対策）

メッセージングアプリケーションを含むＳＮＳに関する従業員向けの利用ルールやガイドラインを整備し、 その中でテレワーク時の利用上の留意事項を明示する。

ファイル共有サービス等のパブリッククラウドサービスの利用ルールを整備し、 情報漏えいにつながる恐れのある利用方法を禁止する。

* + - * 1. （ウ） テレワーク勤務者が実施すべき対策

（情報セキュリティ保全対策の大枠）

テレワーク作業中は、 利用する情報資産の管理責任を自らが負うことを自覚し、 情報セキュリティポリシーが定める技術的・物理的及び人的対策基準に沿った業務を行い、 定期的に実施状況を自己点検する。

テレワークで扱う情報について、 定められた情報のレベル分けとレベルに応じたルールに従って取り扱う。

定期的に実施される情報セキュリティに関する教育・啓発活動に積極的に取り組むことで、 情報セキュリティに対する認識を高めることに務める。

情報セキュリティ事故の発生に備えて、 直ちに定められた担当者に連絡できるよう連絡体制を確認するとともに、 事故時に備えた訓練に参加する。

（悪意のソフトウェアに対する対策）

マルウェア感染を防ぐため、 ＯＳやブラウザ（拡張機能を含む）のアップデートが未実施の状態で社外のウェブサイトにはアクセスしない。

アプリケーションをインストールする際は、 システム管理者にその旨を申請し、 許可を受けたアプリケーションのみをインストールする。

（私用端末利用の場合）テレワークで利用する端末にインストールするアプリケーションは、 安全性に十分留意して選択する。

作業開始前に、 テレワーク端末にウイルス対策ソフトがインストールされ、 最新の定義ファイルが適用されていることを確認する。

作業開始前に、 テレワーク端末のＯＳ及びソフトウェアについて、 アップデートが適用され最新の状態であることを確認する。

テレワークにはルールに定められた情報セキュリティ対策が適用されているものを使用し、 スマートフォン、 タブレット等に関しては不正な改造（脱獄、 root 化等）を施さない。

テレワーク作業中にマルウェアに感染した場合、 その報告漏れや遅れが被害拡大につながる恐れがあることを自覚し、 電子メールの添付ファイルの開封やリンク先のクリックに一層の注意を払う。

（端末の紛失・盗難に対する対策）

オフィス外に情報資産を持ち出すとき、 その原本を安全な場所に保存しておく。

機密性が求められる電子データを極力管理する必要が無いように業務の方法を工夫する。 やむを得ない場合は必ず暗号化して保存するとともに、 端末や電子データの入った記録媒体（ＵＳＢメモリ等）等の盗難に留意する。

（重要情報の盗聴に対する対策）

機密性が求められる電子データを送信する際には必ず暗号化する。

無線LAN 利用に伴うリスクを理解し、 テレワークで利用する場合は確保すべきセキュリティレベルに応じた対策が可能な範囲で利用する。

第三者と共有する環境で作業を行う場合、 端末の画面にプライバシーフィルターを装着したり、 作業場所を選ぶ等により、 画面の覗き見防止に努める。

（不正侵入・踏み台に対する対策）

社外から社内システムにアクセスするための利用者認証情報（パスワード、 ＩＣカード等）を適正に管理する。

インターネット経由で社内システムにアクセスする際、 システム管理者が指定したアクセス方法のみを用いる。

テレワークで使用するパスワードは、 使い回しを避け、 一定以上の長さで他人に推測されにくいものを用いるように心がける。

（外部サービスの利用に対する対策）

メッセージングアプリケーションを含むＳＮＳをテレワークで利用する場合、 社内で定められたＳＮＳ利用ルールやガイドラインに従って利用するようにする。

テレワークでファイル共有サービス等のパブリッククラウドサービスを利用する場合、 社内ルールで認められた範囲で利用する。

* + - 1. 3. テレワークセキュリティ対策の解説
         1. （ア） 情報セキュリティ保全対策の大枠

１

経営者1

経営者は、 テレワークの実施を考慮した情報セキュリティポリシーを定め定期的に監査し、 その内容に応じて見直しを行う。

管理者1

システム全体を管理する重要な立場であることを自覚し、 情報セキュリティポリシーに従ってテレワークのセキュリティ維持に関する技術的対策を講じるとともに定期的に実施状況を監査する。

勤務者1

テレワーク作業中は、 利用する情報資産の管理責任を自らが負うことを自覚し、 情報セキュリティポリシーが定める技術的・物理的及び人的対策基準に沿った業務を行い、 定期的に実施状況を自己点検する。

＜経営者＞基本対策事項

図10 情報セキュリティポリシーの構成

＜経営者＞推奨対策事項

図 11 情報セキュリティに関するＰＤＣＡサイクル

２

経営者2

社内で扱う情報について、 その重要度に応じたレベル分けを行った上で、 テレワークでの利用可否と利用可の場合の取扱方法を定める。

管理者2

情報のレベル分けに応じて、 電子データに対するアクセス制御、 暗号化の要否や印刷可否などの設定を行う。

勤務者2

テレワークで扱う情報について、 定められた情報のレベル分けとレベルに応じたルールに従って取り扱う。

＜経営者・システム管理者＞基本対策事項

＜経営者・システム管理者＞推奨対策事項

図 12 情報のレベル分け

テレワーク トラブル事例 と 対策 〈１〉～情報のレベル分けに関するトラブル事例～

【コラム】 紙媒体での情報の持ち出し

３

経営者3

テレワーク勤務者が情報セキュリティ対策の重要性を理解した上で作業を行えるようにするため、 定期的に教育・啓発活動を実施させる。

管理者3

テレワーク勤務者の情報セキュリティに関する認識を確実なものにするために、 定期的に教育・啓発活動を実施する。

勤務者3

定期的に実施される情報セキュリティに関する教育・啓発活動に積極的に取り組むことで、 情報セキュリティに対する認識を高めることに務める。

＜経営者・システム管理者＞基本対策事項

＜テレワーク勤務者＞基本対策事項

図13 情報セキュリティ教育

図14 イントラネットやポスターによる啓発

＜経営者・システム管理者＞推奨対策事項

４

経営者4

情報セキュリティ事故の発生に備えて、 迅速な対応がとれるように連絡体制を整えるとともに、 事故時の対応についての訓練を実施させる。

管理者4

情報セキュリティ事故の発生に備えて、 迅速な対応がとれるように連絡体制を確認するとともに、 事故時の対応についての訓練を実施する。

勤務者4

情報セキュリティ事故の発生に備えて、 直ちに定められた担当者に連絡できるよう連絡体制を確認するとともに、 事故時に備えた訓練に参加する。

＜経営者・システム管理者・テレワーク勤務者＞基本対策事項

＜経営者・システム管理者・テレワーク勤務者＞推奨対策事項

５

経営者5

テレワークにおける情報セキュリティ対策に適切な理解を示した上で、 必要な人材・資源に必要な予算を割り当てる。

＜経営者＞基本対策事項

* + - * 1. （イ） マルウェアに対する対策

５

管理者5

フィルタリング等を用いて、 テレワーク勤務者が危険なサイトにアクセスしないように設定する。

勤務者5

マルウェア感染を防ぐため、 ＯＳやブラウザ（拡張機能を含む）のアップデートが未実施の状態で社外のウェブサイトにはアクセスしない。

＜テレワーク勤務者＞基本対策事項

＜システム管理者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈２〉～マルウェア感染に関するトラブル事例～

６

管理者6

テレワーク勤務者がテレワーク端末にアプリケーションをインストールする際は申請させ、 情報セキュリティ上の問題がないことを確認した上で認める。

勤務者6

アプリケーションをインストールする際は、 システム管理者にその旨を申請し、 許可を受けたアプリケーションのみをインストールする。

（私用端末利用の場合）テレワークで利用する端末にインストールするアプリケーションは、 安全性に十分留意して選択する。

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈３〉～ウイルス対策ソフトに関するトラブル事例～

７

管理者7

貸与用のテレワーク端末にウイルス対策ソフトをインストールし、 最新の定義ファイルが適用されているようにする。

勤務者7

作業開始前に、 テレワーク端末にウイルス対策ソフトがインストールされ、 最新の定義ファイルが適用されていることを確認する。

＜システム管理者＞基本対策事項

＜テレワーク勤務者＞基本対策事項

テレワーク トラブル事例 と 対策 〈４〉～アプリケーション利用に関するトラブル事例～

【コラム】 次世代ウイルス対策ソフト

８

管理者8

貸与用のテレワーク端末のＯＳ及びソフトウェアについて、 アップデートを行い最新の状態に保つ。

勤務者8

作業開始前に、 テレワーク端末のＯＳ及びソフトウェアについて、 アップデートが適用され最新の状態であることを確認する。

＜システム管理者＞基本対策事項

＜テレワーク勤務者＞基本対策事項

テレワーク トラブル事例 と 対策 〈５〉～アップデートに関するトラブル事例～

９

管理者9

私用端末をテレワークに利用させる際は、 その端末に必要な情報セキュリティ対策が施されていることを確認させた上で認める。

勤務者9

テレワークにはルールに定められた情報セキュリティ対策が適用されているものを使用し、 スマートフォン、 タブレット等に関しては不正な改造（脱獄、 root 化等）を施さない。

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

10

管理者10

ランサムウェアの感染に備え、 重要な電子データのバックアップを社内システムから切り離した状態で保存する。

＜システム管理者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈６〉～ランサムウェアに関するトラブル事例～

11

管理者11

金融機関や物流業者からの事務連絡を装うなどの不審なメールが迷惑メールとして分類されるよう設定する。

勤務者10

テレワーク作業中にマルウェアに感染した場合、 その報告漏れや遅れが被害拡大につながる恐れがあることを自覚し、 電子メールの添付ファイルの開封やリンク先のクリックに一層の注意を払う。

＜テレワーク勤務者＞基本対策事項

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

【コラム】 社内SNS の利用

テレワーク トラブル事例 と 対策 〈７〉～不審メールに関するトラブル事例～

* + - * 1. （ウ） 端末の紛失・盗難に対する対策

11

勤務者11

オフィス外に情報資産を持ち出すとき、 その原本を安全な場所に保存しておく。

【対象】パターン⑥（会社PC の持ち帰り方式）

＜テレワーク勤務者＞推奨対策事項

12

管理者12

台帳等を整備し、 貸与するテレワーク端末の所在や利用者等を管理する。

勤務者12

機密性が求められる電子データを極力管理する必要が無いように業務の方法を工夫する。 やむを得ない場合は必ず暗号化して保存するとともに、 端末や電子データの入った記録媒体（ＵＳＢメモリ等）等の盗難に留意する。

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈８〉～端末の紛失に関するトラブル事例～

* + - * 1. （エ） 重要情報の盗聴に対する対策

13

勤務者13

機密性が求められる電子データを送信する際には必ず暗号化する。

＜テレワーク勤務者＞基本対策事項

テレワーク トラブル事例 と 対策 〈９〉～公衆無線LAN 利用に関するトラブル事例～

13

管理者13

テレワーク端末において無線LAN の脆弱性対策が適切に講じられるようにする。

勤務者14

無線LAN 利用に伴うリスクを理解し、 テレワークで利用する場合は確保すべきセキュリティレベルに応じた対策が可能な範囲で利用する。

＜テレワーク勤務者＞基本対策事項

＜テレワーク勤務者＞推奨対策事項

図16 無線LAN 利用上のリスク

15

勤務者15

第三者と共有する環境で作業を行う場合、 端末の画面にプライバシーフィルターを装着したり、 作業場所を選ぶ等により、 画面の覗き見防止に努める。

＜テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈１０〉～画面の覗き見に関するトラブル事例～

* + - * 1. （オ） 不正アクセスに対する対策

16

管理者14

社外から社内システムへアクセスするための利用者認証について、 技術的基準を明確に定め、 適正に管理・運用する。

勤務者16

社外から社内システムにアクセスするための利用者認証情報（パスワード、 ＩＣカード等）を適正に管理する。

【対象】パターン①（リモートデスクトップ方式）、 パターン②（仮想デスクトップ方式）、 パターン⑤（アプリケーションラッピング方式）、 パターン⑥（会社PC の持ち帰り方式）

＜システム管理者＞基本対策事項

＜テレワーク勤務者＞推奨対策事項

17

管理者15

テレワーク勤務者がインターネット経由で社内システムにアクセスする際のアクセス方法を定める。 また、 社内システムとインターネットの境界線にはファイアウォールやルータ等を設置し、 アクセス状況を監視するとともに、 不必要なアクセスを遮断する。

勤務者17

インターネット経由で社内システムにアクセスする際、 システム管理者が指定したアクセス方法のみを用いる。

＜システム管理者＞基本対策事項

図17 ファイアウォールの設置

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈１１〉～「踏み台」に関するトラブル事例～

18

管理者16

社内システムへのアクセス用のパスワードとして、 強度の低いものを用いることができないように設定する。

勤務者18

テレワークで使用するパスワードは、 使い回しを避け、 一定以上の長さで他人に推測されにくいものを用いるように心がける。

＜システム管理者＞基本対策事項

＜システム管理者＞推奨対策事項

＜テレワーク勤務者＞推奨対策事項

図 18 アカウントのパスワード管理

【コラム】 パスワードの管理方法

テレワーク トラブル事例 と 対策 〈１２〉～パスワード管理に関するトラブル事例～

【コラム】 ID・パスワードをブラウザに記憶させても大丈夫？

* + - * 1. （カ） 外部サービスの利用に対する対策

19

管理者17

メッセージングアプリケーションを含むＳＮＳに関する従業員向けの利用ルールやガイドラインを整備し、 その中でテレワーク時の利用上の留意事項を明示する。

勤務者19

メッセージングアプリケーションを含むＳＮＳをテレワークで利用する場合、 社内で定められたＳＮＳ利用ルールやガイドラインに従って利用するようにする。

＜システム管理者・テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈１３〉～SNS 利用に関するトラブル事例～

20

管理者18

ファイル共有サービス等のパブリッククラウドサービスの利用ルールを整備し、 情報漏えいにつながる恐れのある利用方法を禁止する。

勤務者20

テレワークでファイル共有サービス等のパブリッククラウドサービスを利用する場合、 社内ルールで認められた範囲で利用する。

＜システム管理者＞基本対策事項

＜テレワーク勤務者＞推奨対策事項

テレワーク トラブル事例 と 対策 〈１４〉～パブリッククラウド利用に関するトラブル事例～

* + - 1. 用語集
      2. 参考リンク集
         1. テレワークではじめる働き方改革 テレワークの導入・運用ガイドブック（厚生労働省）

http://work-holiday.mhlw.go.jp/material/pdf/category7/01\_01.pdf

厚生労働省と総務省による3 年間の実証事業を通じて得られた知識、 ノウハウをもとに、 テレワークによる効果、 テレワークを導入した場合の労務管理の仕方や労務管理ツールの利用方法、 セキュリティを確保したICT システム・ツールの選択方法等やその手順を紹介しています。

* + - * 1. サイバーセキュリティ経営ガイドライン（経済産業省）

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)

サイバー攻撃から企業を守る観点で、 経営者が認識する必要のある「3 原則」、 及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要10 項目」をまとめたものです。

* + - * 1. 中小企業の情報セキュリティ対策ガイドライン（独立行政法人情報処理推進機構）

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/)

中小企業にとって重要な情報を漏えいや改ざん、 喪失などの脅威から保護することを目的とする情報セキュリティ対策の考え方や実践方法について説明するもので、 本編2 部構成と、 「5 分でできる！情報セキュリティ自社診断シート」を含む7 種類の付録で構成されています。

* + - * 1. SECURITY ACTION（独立行政法人情報処理推進機構）

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)

上述の「中小企業の情報セキュリティガイドライン」の付録に示されている情報セキュリティ対策に取り組むことを自己宣言することで、 「SECURITY ACTION」ロゴマークを自社の名刺、 封筒、 会社案内、 ウェブサイト等に表示させることができ、 自社の取組を対外的にアピールすることができます。

* + - * 1. 情報セキュリティ理解度チェック（NPO 日本ネットワークセキュリティ協会）

http://slb.jnsa.org/eslb/

ドキュメントを参照: [eslb](http://slb.jnsa.org/eslb/)

自社の従業員における情報セキュリティの理解度がどの程度かを把握する仕組みを提供しています。 チェックの対象は「電子メールに関する知識」「インターネットの利用法」「ウイルスに関する知識」「パスワードの管理」などテレワークでも有用な知識を幅広く扱っています。

基本的な機能の利用は無料ですが、 機能強化した有料版もあります。

* + - * 1. 経営と IT 化相談窓口（NPO IT コーディネータ協会）

https://www.itc.or.jp/management/diagnosis/

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

中小企業が抱える経営課題の解決支援のため、 中小企業支援に関する専門知識や豊富な実績を有する人材として資格認定されたIT コーディネータを紹介する窓口です。

* + - * 1. 情報処理安全確保支援士制度（独立行政法人情報処理推進機構）

https://www.ipa.go.jp/siensi/index.html

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

サイバーセキュリティに関する専門的な知識・技能を有する人材である情報処理安全確保支援士の登録制度が平成29 年度に開始されました。 上記ウェブサイトにて登録された情報処理安全確保支援士の得意分野や連絡先等の情報を参照することができます。

* 1. 教育分野
     1. 教育分野におけるクラウド導入に対応する情報セキュリティに関する手続きガイドブック【総務省】

ドキュメントを参照: [000417633.pdf](http://www.soumu.go.jp/main_content/000417633.pdf)

* + - 1. 第1章　クラウド導入のプセスと情報セキュリティに係る手続き
         1. １．１　調達のプセスと情報セキュリティの関係
      2. 第2章　情報セキュリティ手続きにおける「準備段階」の留意点
         1. ２．１　教育用コンテンツに関する情報収集
         2. ２．２　法令やポリシーに関する情報収集
      3. 第3章　情報セキュリティ手続きにおける「計画段階」の留意点
         1. ３．１　クラウド上で取り扱う情報資産の洗い出し
         2. ３．２　クラウドを中心としたICT環境に関するリスクの洗い出し
         3. ３．３　リスクおよび情報セキュリティポリシーを踏まえた仕様書の作成
      4. 第4章　情報セキュリティに関する手続きにおける「運用段階」の留意点
         1. ４．１　緊急時対応計画の整備
         2. ４，２　研修の実施
         3. ４．３　情報セキュリティに関する監査
         4. ４．４　著作権等
    1. 教育ＩＣＴの新しいスタイルクラウド導入ガイドブック2015【総務省】

ドキュメントを参照: [000358976.pdf](http://www.soumu.go.jp/main_content/000358976.pdf)

* + - 1. 第5 章情報セキュリティポリシー
         1. 5.1 教育現場にふさわしい情報セキュリティポリシーとは
         2. 5.2 クラウドに対応した情報セキュリティポリシーとは
         3. 5.3 学校における情報セキュリティポリシーの事例
      2. Column　先進事例④　教育用SNS

1. その他資料
   1. マイナンバー制度とマイナンバーカード【総務省HP】

ドキュメントを参照: [kojinbango\_card](http://www.soumu.go.jp/kojinbango_card/)

* 1. 自治体CIO育成研修集合研修SLAの考え方【総務省】

ドキュメントを参照: [cio\_text18\_ps\_5.pdf](http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/local_support/pdf/cio_text18_ps_5.pdf)

* 1. ICTの進化が雇用と働き方に及ぼす影響に関する調査研究（平成28年情報通信白書）【2016年総務省】

ドキュメントを参照: [nd270000.html](http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/html/nd270000.html)