Sec01-01-04\_「中小企業向けサイバーセキュリティ対策の極意」(第2版)【追補および解説】

# メタデータ

## 改版履歴

### 2021年5月7～14日\_Web版追補および解説候補の洗い出し

### 2021年4月26日\_情報資産台帳の作成と詳細リスク分析（INFORMATION 6-4追補原稿）大幅加筆

### 2021年4月26日\_情報資産台帳の作成と詳細リスク分析（INFORMATION 6-4追補原稿）大幅加筆

### 2021年4月16日サイバーセキュリティ経営ガイドライン [Ver.2.0]【METI/IPA】参照

### 2021年4月15日初版：「情報資産台帳の作成と詳細リスク分析」初稿

## 作成日

## 作成者

## 件名

## 概要

# 参考資料

## 中小企業の情報セキュリティ対策ガイドライン第3版

## サイバーセキュリティ経営ガイドライン [Ver.2.0]（経済産業省/IPA）

## 情報技術－セキュリティ技術－情報セキュリティマネジメントシステム

### JISQ 27001（ISO/IEC 27001）要求事項

### JISQ 27002（ISO/IEC 27002）情報セキュリティ管理策の実践のための規範

#### JISQ27017（ISO/IEC 27017）－JISQ 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範

## 情報セキュリティマネジメント試験

### 情報セキュリティマネジメントに要求される知識と技能【シラバス】（Bib05-13）

# Sec01-01-04-list\_Web版追補および解説候補

## 概要

### 改版履歴

#### 2021年6月8日\_EPUB版⇒Web版として先行して追補する候補選択

#### 2021年5月31日\_候補大幅追加

#### 2021年5月25日\_仕掛かり分チェック

#### 2021年5月13日\_全編にわたってリストアップ

### アイコン凡例

#### EPUB版⇒Web版として先行して追補する候補

#### Web版に追補する候補

#### 執筆中、仕掛かり中

#### 冊子体追補候補

#### 担当

## Mission1

### 1-3：Webサービスからの個人情報窃取

#### 【Web版Appendix】本人に認証サービス（3Dセキュア）クレジットカードの認証方式を追加

 【Web版Appendｘ引用先】割賦販売法の改定とクレジットカードのセキュリティ「改正割賦販売法について」PD経済産業省　商取引監督課２０１８年４月

 https://www.caa.go.jp/policies/policy/local\_cooperation/local\_consumer\_administration/meeting\_001/pdf/meeting\_001\_180419\_0017.pdf

### 1-4：集中アクセスによるサービス停止

#### 【Web版Appendix】集中アクセスによるサービス停止　「コラム」中小企業DDos攻撃の被害事例

 事例ー＞DDosの攻撃内容の説明に大規模で巧妙なDDos攻撃の増加傾向に懸念アカマイ、短期間で2度の大規模DDos攻撃を緩和事例を分かりやすく追加Akamai (アカマイ) Web セキュリテ

 https://www.lac.co.jp/service/product/akamai.html

### 1-6：Webサイトの改ざん

#### 【Web版Update】ECサイトの脆弱性をついた事案も発生

  ★【Web版Appendix】脆弱性診断システム適用範囲について、脆弱性診断Tool

  【Web版Appendix】Metasploit Framework

  【Web版Appendix】OWASP ZAP

#### ★【Web版Appendix】共通脆弱性識別子CVE(Common Vulnerabilities and Exposures)

### 1-7:インターネットバンキングの不正送金

#### 【Web版Appendix】詐欺サイトもSSL化が当たり前　フィツシング詐欺被害回避の方法

 ラック株式会社

### 1-10：Webサービスへの不正ログイン

#### 【Web版Appendix】IDと認証セキュリティ

### 1-12：IoT機器を踏み台にした攻撃

#### 【Web版Appendix】NICT「NOTICE」の実証事例の結果

### 1-13：中小企業におけるサイバー攻撃被害の例

#### 【Web版Appendix】POINT２中小企業を含んだサプライチェーンが狙われている

  サプライチェーンセキュリティの必要性を追加又は主要な参考文書引用先を例示

 サプライチェーンセキュリティの必要性

 サイバーセキュリティ経営ガイドラインの改定ポイント 経済産業省商務情報政策局サイバーセキュリティ課

 https://www.meti.go.jp/policy/netsecurity/downloadfiles/overview.pdf

 IPA　NIST関連文書 https://www.ipa.go.jp/security/publications/nist/

  NIST\_SP800-171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

 Protecting Controlled Unclassified Information in Nonfederal Systems

#### 【Web版Appendix】サプライチェーンの情報セキュリティマネジメント IS02703, NIST\_SP800-61（サプライチェーンマネージメント）

#### 【Web版Appendix】★サプライチェーンコンソシアムSC3の概要（IPA、経済産業省）

### 1-14：ビジネスメール詐欺（BEC)に注意

#### 【Web版Appendix】トレンドマイクロ　「ビジネスメール詐欺の被害に遭わないために、知って知っておくべき兆候をBEC被害の事例（具体的）に追加

 https://blog.trendmicro.co.jp/archives/tag/bec

#### 【Web版Appendix】ビジネスメール詐欺の被害」と回避策

 法人間の外国送金の資金をだまし取る詐欺にご注意追加　(BEC (Business E-mail Compromise) / foreign remittance fraud）

 全国社団法人全国銀行協会

 https://www.zenginkyo.or.jp/topic/detail/nid/3561/

 ・発生している事案

 ・法人に対する対策事例

## Mission2

### 2-8：テレワーク等での持ち出し・持ち込み機器対策

#### 【Web版Appendix】VPNの脆弱性攻撃増加　テレワーク認証情報搾取

### 2-9：電子メールの安全利用

#### 【Web版Appendix】＜電子メールのなりすまし対策＞

 SPF送信電子メール認証のイメージ図を追加する

### 2-10：標的型攻撃メールへの対応

#### 【Web版Appendix】巧妙な標的型攻撃メール事例

#### 【Web版Appendix】Emotetからの攻撃も含まれる事例（JPCERT/CC）

#### 【Web版Appendix】IceIDウイルスダンローダ

#### 【Web版Appendix】★EDP（エンドポイントセキュリティ）関連調査

#### 【Web版Appendix】★TRUSTeマーク認証について調査概要

 信頼という名の個人情報認証 TRUSTe（トラストイー）は、信頼(TRUST)できる事業者選びの指標

## Mission3

### 3-1：サイバーセキュリティ対策が経営に与える重大な影響

#### 【Web版Appendix】MDM（Mobile Device Management）

 ビジネスで使用するスマートフォンなどのモバイルデバイスの、システム設定などを統合的・効率的に管理する手法。

### 3-3：経営者に問われる責任

#### 【Web版Appendix】組織の姿勢3分類(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】より)

### 3-5：ITの活用診断

#### 【Web版Appendix】視点6分類

### 3-6：サイバーセキュリティ対策診断

#### 【Web版Appendix】費用対効果

#### 【Web版Appendix】セキュリティ診断Toolの紹介（ペネトレーションテストを含む）

### 3-8：業務の効率化、 サービスの維持のために

#### 【Web版Appendix】ITを活用したサービスの構築・運用に掛かる費用は、 経費ではなく先行投資

#### 【Web版Appendix】生産性向上のための「デジタル・ワークプレイス」

#### 【Web版Appendix】テレワークではじめる働き方改革

#### 【Web版Appendix】テレワークでのクラウドサービス活用等（総務省テレワークガイド）

#### 【Web版Appendix】 Web会議サービスを使用する際のセキュリティ注意事項

 クラウドIPA　情報セキュリティ対策

 https://www.ipa.go.jp/security/announce/webmeeting.html

### 3-9：経営者が認識すべきサイバーセキュリティ経営の3原則

#### 【Web版Appendix】経営者として取り組むべき「重要7項目の取組」

### 3-10：【経営者がやらなければならない】サイバーセキュリティ経営の重要10項目

#### 【Web版Appendix】最近のサイバー攻撃の状況を踏まえ、経営者の皆様へサイバーセキュリティの取組の強化に関する注意喚起を行います【2020年12月18日METI】

#### 【Web版Appendix】サイバーセキュリティ経営ガイドライン実践状況の可視化ツールの活用【2021年夏アップデート予定】

#### 【Web版Appendix】サイバーセキュリティ経営ガイドライン実践のためのプラクティス

### 3-11：次世代技術を活用したビジネス展開

#### 【Web版Appendix】【解説】DX推進はビジネス飛躍のチャンス

#### 【Web版Appendix】「デジタルアーキテクチャ・デザインセンター（DADC）」の活動

#### 【Web版Appendix】デジタルトランスフォーメーションの加速に向けた研究会の中間報告書『DXレポート2

#### 【Web版Appendix】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【NISC】

#### 【Web版Appendix】次世代サービス、技術の利用に当たってのサイバーセキュリティ対策

#### 【Web版Appendix】DXレポート（ITシステム2025年の崖の克服

#### 【Web版Appendix】AIが人間をアシストする「インテリジェント・ワークプレイス」の活用におけるサイバーセキュリティ対策

#### 【Web版Appendix】【参考情報】ITの最新トレンド

#### 【Web版Appendix】IoTや5Gを活用した新規セキュリティビジネスの紹介

### 3-12：IoT、 ビッグデータ, AI、 ロボットの活用

#### 【Web版Appendix】攻めのIT投資対応、Society5.0時代に必要なセキュリティ対策【要素別】

 【Web版Appendix】IoT関連セキュリティ対応

 【Web版Appendix】クラウドサービスとセキュリティ

 【Web版Appendix】５Gセキュリティ対応

 【Web版Appendix】BYODセキュリティ対応

### 3-13：IoTが果たす役割と効果

### 3-14：人工知能（AI）が果たす役割と効果

#### 【Web版Appendix】「AI白書」の要点

### 3-15：IoTを活用する際のサイバーセキュリティ上の留意点

#### 【Web版Appendix】機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き【2021年4月20日METI】

#### 【Web版Appendix】CMS認証　IEC63443認証　ISO 国際規格（ISO/IEC JTC 1）に提案し開発中

 ISO/IEC 27030（ITセキュリティ） 2018/4－

 • ISO/IEC 30147（IoT）

### 3-16：IoTを活用する一般利用者のための基本ルール

#### 【Web版Appendix】IPA 安全安心なIoT実現に向けた重要ポイント

 ～「つながる世界の開発指針」と関連ガイド活用のススメ

 https://www.ipa.go.jp/files/000073864.pdf

### 【Web版Appendix】サイバー・フィジカル・セキュリティ対策フレームワーク対応

#### 【Web版Appendix】サイバー・フジカル・セキュリティ対策フレームワーク対応\_NIST\_SP800―161\_サプライチェーンリスクマネージメント

#### 【Web版Appendix】サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）（2019年4月METI）対応

#### 【Web版Appendix】NIST SP800-171 「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」 改訂Revishon2対応

 【Web版Appendix】NIST SP 800-171の要求事項と「サイバー・フィジカル・セキュリティ対策フレームワーク」との対応表

#### 【Web版Appendix】NIST SP800-53「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」改訂Rev4.0対応

#### 【Web版Appendix】NIST SP800-53とNISTサイバ－セキュリティフレームワークの概要と利用方法

#### 【Web版Appendix】スマートホームの安心・安全に向けたサイバー・フジカル・セキュリティ対策ガイドライン　経済産業省

#### 【Web版Appendix】★サプライチェーンサイバーセキュリティについてISO27036をベースにその具体的 コントロールの導入と評価方法を中小企業向け導入対策

#### 【Web版Appendix】★サプライチェーンコンソシアムSC3の概要（IPA、経済産業省）

#### 【Web版Appendix】★IoT活用企業におけるプライバシー保護に関する考慮

 一般社団法人 重要生活機器連携セキュリティ協議会（Connected Consumer Device Security Council）

## Mission4

### 4-7：大規模災害などによる事業中断と事業継続管理

#### 【Web版Appendix】IT/BCPの範囲とフレームワーク

#### 【Web版Appendix】ISO/IEC2203 事業継続

## Mission5

## Information6

### 6-2：その他の主な報告・連絡・相談窓口等

#### 【Web版Appendix】サイバーセキュリティ報告・連絡・相談窓口一覧【詳細資料】

### 6-3：セキュリティお役立ち情報リンク【単独セクションで、詳細化中】

#### 【Web版Appendix】次世代ITおよびサイバーセキュリティ対策に関する文献、サイト一覧【詳細資料】

 ※内容を充実させ、最新情報として都度更新

 サイバーセキュリティ関連の基本文書（法律・基本計画・各種方針等）

 サイバーセキュリティ関連の各種白書・年次報告書類

 各実施事項の参考情報

 全般

 DX 関連

 IoTセキュリティ関連

 テレワーク関連

 AI関連

 インシデント対応関連

 個人情報保護関連

 GDPR

  SP 800-53 Rev.5 情報システムおよび組織のセキュリティおよびプライバシー管理

 システム開発（外部委託）

 人材育成関連

 【追加】デジタルリテラシー領域「Di-Lite」

法令・規則

 各実施関連機関

 【追加】「デジタルリテラシー協議会」

#### 【Web版Appendix】一般ユーザ向け：次世代ITおよびサイバーセキュリティ対策に関する啓発用資料【IT利用局面毎】

 インターネットでの不正行為を発見した場合

 ECサイト利用

 電子メール

 ・・・

#### 【Web版Appendix】近い将来のITの利活用と必要な人材育成に資する資料

### 6-4：中小企業の情報セキュリティ対策ガイドライン

#### 【Web版Appendix】6-4\_Appendix\_中小企業の情報セキュリティ対策ガイドラインの概要【構成】

#### できるところから始める

#### 組織的な取り組みを開始する

 【Web版Appendix】6-4-X\_Appendix\_【付録4】情報セキュリティハンドブック（ひな型）の使い方（ポイント）

#### 本格的に取り組む

  【Web版Appendix】6-4-X\_Appendix\_サイバーセキュリティ経営チェックシート【「サイバーセキュリティ経営ガイドライン」Ver2.0 付録A】

     【Web版Appendix】6-4-1\_Appendix\_情報資産台帳の作成と詳細リスク分析

     【Web版Appendix】6-4-1\_Appendix\_情報セキュリティ関連規程に記載すべき項目の概要

#### より強固にするための方策

  【Web版Appendix】ACTION4 対策をより強化する

 ３クラウドサービスの情報セキュリティセキュリティ対策３段階で検討しましょう。、＜ー３段階の説明を追加する

  【Web版Appendix】ISMAP　情報セキュリティ監査ガイドライン　経済産業省

### 6-5：中小企業のためのクラウドサービス安全利用手引き

#### 【Web版Appendix】クラウドセキュリティ監視Tool　CASBYの活用

#### 【Web版Appendix】ゼロトラストセキュリティでは、新たな「境界」の考え方であるSDP（Software Defined Perimeter）展開されている

#### 【Web版Appendix】「ゼロトラストモデル」とは―クラウド時代の次世代セキュリティモデル

### 6-6：IT活用に不可欠なIT人材の確保と育成

#### 【Web版Appendix】6-6-1\_Appendix\_次世代技術を活用したビジネス展開のためのデジタルリテラシーの習得

 デジタルリテラシー領域「Di-Lite」

 マインド

デジタルに取り組むスタンス、マインド

 知識体系

デジタル活用分野/適用事例

デジタル知識

 スキル

使う、作る/なおす

より上手に使う/広める

発想する/活用方針を示す

新たに作る/教える

 「Di-Lite」のベースとなるカリキュラム

 ITパスポート試験（IPA実施)

 データサイエンティスト検定リテラシーレベル（JDLA実施)

 G検定（JDLA実施)

    【Web版Appendix】6-6-2\_Appendix\_近い将来のITの利活用と必要な人材（「サイバーセキュリティ研究開発戦略」の要約）

#### 6-6-10\_Appendix\_iコンピテンシ・ディクショナリ(iCD)

### 6-7：情報セキュリティ関連法令

#### 【Web版Appendix】プライバシイ保護法の国際化とCBPR認証（Cross　Border Privacy Rule

#### 【Web版Appendix】改正民法と瑕疵担保期間の延長

#### 【Web版Appendix】個人保護保護法の改正（デジタル庁）

### 6-X：デジタルリテラシー

#### 【Web版Appendix】6-X-X\_Appendix\_組織人として持つべきデジタルリテラシー【スキル項目と啓発資料】

 経営者として

 システム管理者として

 従業員として

### 6-X：個人情報保護・プライバシーへの対応

#### 【Web版Appendix】プライバシイバイデザイン　７原則　DX企業のプライバシ－ガバナンスガイド　経済産業省

#### 【Web版Appendix】改正個人情報保護のポイント

 ・利用停止

 ・漏えい等報告、本人通知

 ・不適正利用の禁止

 ・認定団体制度の充実

 ・公表事項等

 ・仮名加工情報

 ・個人関連情報

 ・越境移転

### ６－X：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調査

#### 【Web版Appendix】1）ISMSクラウドセキュリティ認証(ISO27001/ISO27017) 2）CSマーク 3）CSA STAR認証(CSA Security) 4）StarAudit Certification 5）FedRAMP 6）SOC2,SOC2＋

#### 【Web版Appendix】★クラウドアクセス可視化・制御ソリューション CASB(Cloud Access Security Broker)

#### 【Web版Appendix】★ISMSクラウドセキュリティ認証(ISO27001/ISO27017

#### 【Web版Appendix】★JNSA「緊急事態宣言解除後のセキュリティ・チェックリスト解説書」 日本セキュリティネットワーク協会

#### 【Web版Appendix】★eKYCとは

  KYCをオンライン上で実現するための仕組みです。本人確認を電子的に行うことから、eKYC（electronic\_Know\_Your\_Customer）と略して呼ばれます。

 2018年に改正された「犯罪による収益の移転防止に関する法律」により、「オンラインで完結する自然人の本人特定事項の確認方法」として、以下の4つの方法が認められるようになりました。

 「本人確認書類の画像」と「本人の容貌の画像」の送信

 「本人確認書類のICチップ情報」と「本人の容貌の画像」の送信

 「本人確認書類の画像もしくは本人確認書類のICチップ情報」の送信と事業者による「銀行などへの顧客情報の照会」

 「本人確認書類の画像もしくは本人確認書類のICチップ情報」と「事業者による顧客名義口座への少額振り込みと、そのインターネットバンキング記録の画像」の送信

#### 【Web版Appendix】★FIDO2認証が主要な認証方式として有効化

 ・多要素認証機能のクラウドサービスを開始 Akamai 社 多要素認証機能のクラウドサービス「Akamai MFA」の国内提供を開始したと発表しました。 FIDO2（Fast IDentity Online）に準拠し、スマートフォンの専用アプリで利用できるようにしています。

#### 【Web版Appendix】★海外の主要規格との対応関係

 NIST Cybersecurity Framework のサブカテゴリと「サイバー・フィジカル・セキュリティ対策フレー ムワーク」対応表のマッピング

#### 【Web版Appendix】★MITRE ATT ＆CK　セキュリティ攻撃パターン分類の利用方法

#### 【Web版Appendix】★OWASP（The Open Web Application Security Project）とは、

 Webアプ有名な取り組みの1つとして「OWASP Top 10」の 公表

# 作成済みコンテンツ

## INFORMATION 6

### 6-3\_Appendix：セキュリティお役立ち情報リンク

#### 巻末の「主な参考文献」は実態と合っていないので削除

#### Sec01-01-03\_「中小企業向けサイバーセキュリティ対策の極意」【本文案】で更新作業中

### 6-4：中小企業の情報セキュリティ対策ガイドライン

#### 6-4-1\_Appendix\_情報資産台帳の作成と詳細リスク分析

#### 6-4-X\_Appendix\_情報セキュリティ関連規程に記載すべき項目の概要【 付録5】

### 6-6：IT活用に不可欠なIT人材の確保と育成

#### 6-6-1\_Appendix\_次世代技術を活用したビジネス展開のためのデジタルリテラシーの習得

# Sec01-01-04\_6.3AP\_セキュリティお役立ち情報リンク

## 国等の基本文書、白書、解説文書

### 基本文書

#### （法律・基本計画・各種方針等）

#### 経済財政運営と改革の基本方針（骨太方針）【閣議決定】

経済財政運営と改革の基本方針2021【経済財政諮問会議にて策定中】

https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/2020/decision0717.html

#### IT総合戦略室\_デジタル・ガバメント実行計画【内閣府】

https://cio.go.jp/guides

デジタル・ガバメント推進標準ガイドライン解説書【内閣府IT総合戦略室】

https://cio.go.jp/guides#kaisetusyo

デジタル・ガバメント推進標準ガイドライン実践ガイドブック【内閣府IT総合戦略室】

https://cio.go.jp/guides#guidebook

#### デジタル社会形成基本法【内閣府】

https://cio.go.jp/node/2734

### 基本文書（サイバーセキュリティ関連）

#### （法律・基本計画・各種方針等）

#### サイバーセキュリティ基本法

https://www.soumu.go.jp/main\_sosiki/joho\_tsusin/security/basic/legal/11.html

#### サイバーセキュリティ戦略【NISC】

https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf

#### サイバーセキュリティ2020【NISC】

https://www.nisc.go.jp/active/kihon/pdf/cs2020.pdf

#### セキュリティ関連NIST文書【IPA】

https://www.ipa.go.jp/security/publications/nist/index.html

#### 重要インフラのサイバーセキュリティを改善するためのフレームワーク【NIST】

NIST SP800-172\_制御された未分類の情報を保護するための強化されたセキュリティ要件：NIST Special Publication 800-171の補足【2021年2月】

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf

https://www.ipa.go.jp/files/000071204.pdf

#### 重要インフラの情報セキュリティ対策に関する主な資料【NISC】

https://www.nisc.go.jp/active/infra/siryou.html

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(ZIP)【NISC】

https://www.nisc.go.jp/active/infra/files/tebikishorev.zip

#### サイバーセキュリティ研究開発戦略【NISC】

https://www.nisc.go.jp/conference/cs/kenkyu/dai16/pdf/16shiryou0201.pdf

### 各種白書・年次報告書類

#### 情報通信白書【総務省】

https://www.soumu.go.jp/johotsusintokei/whitepaper/

#### AI白書【IPA】

https://www.ipa.go.jp/ikc/our\_activities/rs\_01.html

#### 情報セキュリティ白書【IPA】

https://www.ipa.go.jp/ikc/our\_activities/rs\_03.html

#### IT人材白書【IPA】

https://www.ipa.go.jp/jinzai/jigyou/about.html

#### 迷惑メール白書2020 参考編／資料編

https://www.dekyo.or.jp/soudan/aspc/wp.html

#### 情報セキュリティ10大脅威【IPA】

https://www.ipa.go.jp/security/vuln/10threats2021.html

### 情報セキュリティマネジメント（ISMS）関連

#### ISMS適合性評価制度【JIPDEC】

https://isms.jp/isms.html

#### JIS Q 27002\_2014 情報技術?セキュリティ技術?情報セキュリティ管理策の実践のための規範【JIPDEC】

#### ISMSユーザーズガイド-JISQ270012014(ISO\_IEC270012013)対応【JIPDEC】

## 各実施事項毎の参考情報【経営者、管理者向け】

### サイバーセキュリティ全般

#### 企業経営のためのサイバーセキュリティの考え方【NISC】

（サイバーセキュリティに関する組織の視点6分類のベースとなる資料）

https://www.nisc.go.jp/active/kihon/pdf/keiei.pdf

#### サイバーセキュリティ経営ガイドライン【METI】

https://www.meti.go.jp/policy/netsecurity/mng\_guide.html

#### サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）関連【METI】

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）を策定しました

https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html

サイバーサプライチェーンリスク. マネジメント

サイバー・フィジカル・セキュリティ対策フレームワーク ～Society5.0 における新たなサプライチェーン （バリュークリエイションプロセス）の信頼性の確保に向けて～

https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

#### サイバーセキュリティ協議会【METI】

サイバーセキュリティ協議会

https://www.nisc.go.jp/conference/cs/kyogikai/

昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書【METI】

https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊-成果報告書【METI】

https://www.ipa.go.jp/security/fy2019/reports/sme/otasuketai\_houkoku.html

#### サイバーサプライチェーンリスクマネジメント調査報告【IPA】

https://www.ipa.go.jp/security/fy28/reports/scrm/index.html

#### 中小企業の情報セキュリティ対策ガイドライン（第3版）【IPA】

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

### サイバーセキュリティ対策に関する参考情報【サイバーセキュリティ経営ガイドラインVer 2.0関連】

#### https://www.meti.go.jp/policy/netsecurity/mng\_guide.html

#### 重要１０項目全般に関連する参考情報

サイバーセキュリティ経営ガイドライン解説書 [Ver.2.0]（IPA）

（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解説。）

https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html

中小企業の情報セキュリティ対策ガイドライン [第3版]（IPA）

(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。)

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

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。）

Framework for Improving Critical Infrastructure Cybersecurity [Version 1.0]（NIST）

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。）

https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

SP800-53 [Rev.4]（NIST）

（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。）

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

SP800-171 [Rev.1]（NIST）

（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。）

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

#### 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）の確保」に関連する参考情報

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）

（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。）

https://www.ipa.go.jp/files/000039528.pdf

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）

（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。）

https://www.ipa.go.jp/files/000047872.pdf

#### 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」に関連する参考情報

中小企業の情報セキュリティ対策ガイドライン[第3版]（IPA）

（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。）

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

#### 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」に関連する参考情報

「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）

（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。）

https://www.ipa.go.jp/files/000046236.pdf

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）

（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。）

https://www.jpcert.or.jp/research/apt-loganalysis.html

組織における内部不正防止ガイドライン [第4版]（IPA）

（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。）

https://www.ipa.go.jp/files/000057060.pdf

秘密情報の保護ハンドブック [平成 28 年 2 月]（経済産業省）

（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。）

http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

#### 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」に関連する参考情報

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）

（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。）

https://isms.jp/isms.html

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）

（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。）

https://isms.jp/csms.html

情報セキュリティ管理基準（経済産業省）

（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。）

http://www.meti.go.jp/policy/netsecurity/is-kansa/index.html

情報セキュリティ対策ベンチマーク（IPA）

（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。）

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

安全なウェブサイトの作り方 [第 7 版]（IPA）

（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。）

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

JVN（IPA、JPCERT/CC）

（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。）

https://jvn.jp/

#### 指示７「インシデント発生時の緊急対応体制の整備」に関連する参考情報

CSIRT 構築マテリアル（JPCERT/CC）

（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。）

https://www.jpcert.or.jp/csirt\_material/

CSIRT 構築に役立つ参考資料（日本シーサート協議会）

（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。）

http://www.nca.gr.jp/activity/build-wg-document.html

#### 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」に関連する参考情報

事業継続ガイドライン [平成 25 年 8 月改定]（内閣府）

（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。）

http://www.bousai.go.jp/kyoiku/kigyou/pdf/guideline03.pdf

#### 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および状況把握」に関連する参考情報

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）

（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。）

http://www.chusho.meti.go.jp/keiei/torihiki/2014/140313shitaukeGL3.pdf

SECURITY ACTION セキュリティ対策自己宣言 （IPA）

（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。）

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

#### 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および提供」に関連する参考情報

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）

（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。）

https://www.ipa.go.jp/security/outline/todoke-top-j.html

標的型サイバー攻撃特別相談窓口（IPA）

（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。）

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

サイバー情報共有イニシアティブ（J-CSIP）（IPA）

（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。）

https://www.ipa.go.jp/security/J-CSIP/

@police（警察庁）

（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。）

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

### DX関連

#### Society5.0【内閣府】

https://www8.cao.go.jp/cstp/society5\_0/

#### サイバーフィジカルシステム（CPS)【JEITA】

https://www.jeita.or.jp/cps/about/

#### DXレポート ～ITシステム「2025年の崖」克服とDXの本格的な展開～【METI】

https://www.meti.go.jp/shingikai/mono\_info\_service/digital\_transformation/20180907\_report.html

#### デジタルトランスフォーメーションを推進するためのガイドライン（DX推進ガイドライン）Ver.1【2018年12月METI】

https://www.meti.go.jp/press/2018/12/20181212004/20181212004.html

#### DX時代における企業のプライバシーガバナンス【METI】

https://www.meti.go.jp/policy/it\_policy/privacy/privacy.html

#### 産業界におけるデジタルトランスフォーメーションの推進 【METI】

#### デジタル・トランスフォーメーション（DX）推進に向けた企業とIT人材の実態調査【METI】

https://www.ipa.go.jp/ikc/reports/20200514\_1.html

#### DXレポート2中間取りまとめ【METI】

https://www.meti.go.jp/press/2020/12/20201228004/20201228004.html

#### DXの推進に関するお役立ちコンテンツ一覧【IPA】

https://www.ipa.go.jp/ikc/imanavi.html

#### DX促進に向けた文書を公開～企業ビジネスモデルの変革によるDX実現を後押し～【2020年11月IPA】

https://www.ipa.go.jp/ikc/reports/20200609.html

プラットフォームデジタル化指標について【2020年6月】

https://www.ipa.go.jp/files/000082761.pdf

#### 【解説書等】

【参考】DX推進指標自己分析結果分析レポート【2020年5月28日IPA】

https://www.ipa.go.jp/ikc/reports/20200528.html

【参考】プラットフォームデジタル化指標について【2020年6月IPA】

https://www.ipa.go.jp/files/000082761.pdf

【参考】DX推進セミナー～DXの実現に向けた取り組み～

https://www.ipa.go.jp/ikc/seminar/20200302.html

### テレワーク関連

#### テレワーク実施者の方へ【NISC】

https://www.nisc.go.jp/security-site/telework/

テレワークを実施する際にセキュリティ上留意すべき点について【2020年4月9日NISC】

https://www.nisc.go.jp/active/general/pdf/telework20200414.pdf

#### ★テレワーク総合情報サイト【総務省】

https://telework.soumu.go.jp/

#### テレワークセキュリティガイドライン（第５版）【総務省】

https://www.soumu.go.jp/main\_sosiki/cybersecurity/telework/

#### インターネットの安全・安心ハンドブック【NISC】

https://www.nisc.go.jp/security-site/handbook/

#### サイバーセキュリティ経営ガイドライン【METI/IPA】

https://www.meti.go.jp/policy/netsecurity/mng\_guide.html

#### 中小企業の情報セキュリティ対策ガイドライン【IPA】

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

#### ★テレワーク総合ポータルサイト【厚生労働省】

https://telework.mhlw.go.jp/info/doc/

テレワークの適切な導入及び実施の推進のためのガイドライン

https://www.mhlw.go.jp/content/000759469.pdf

テレワークの適切な導入及び実施の推進のためのガイドライン（リーフレット）

https://www.mhlw.go.jp/content/000766329.pdf

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【2019年12月厚生労働省】

https://telework.mhlw.go.jp/wp/wp-content/uploads/2019/12/H28hatarakikatakaikaku.pdf

#### テレワークを行う際のセキュリティ上の注意事項【IPA】

https://www.ipa.go.jp/security/announce/telework.html

#### テレワーク勤務のサイバーセキュリティ対策！ 警視庁

https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/telework.html

### AI関連

#### 「AI利活用ハンドブック～AIをかしこく使いこなすために～」

https://www.caa.go.jp/policies/policy/consumer\_policy/meeting\_materials/review\_meeting\_004/ai\_handbook.html

#### AI・データの利用に関する契約ガイドライン【METI】

https://cio.go.jp/node/2651

### IoTセキュリティ関連

#### 欧州ネットワーク情報セキュリティ機関（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】

https://www.ipa.go.jp/files/000063605.pdf

#### IoT・5Gセキュリティ総合対策【2019年8月総務省】

https://www.soumu.go.jp/main\_content/000641510.pdf

IoT・5Gセキュリティ総合対策プログレスレポート2020【2020年5月サイバーセキュリティタスクフォース】【総務省】

https://www.soumu.go.jp/main\_content/000688845.pdf

#### IoTセキュリティチェックリスト【JPCERT/CC】

https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html

#### IoTセキュリティガイドライン ver1.0【総務省と経済産業省による「IoT推進コンソーシアム　IoTセキュリティワーキンググループ」】

http://www.iotac.jp/wg/security/

IoTセキュリティガイドライン ver1.0概要

https://www.soumu.go.jp/main\_content/000428394.pdf

#### IoT・5Gセキュリティ総合対策プログレスレポート2020【2020年5月サイバーセキュリティタスクフォース】【総務省】

https://www.soumu.go.jp/main\_content/000688845.pdf

#### 【スライド資料】IoT機器への対策を含むサプライチェーンサイバーセキュリティの強化【2018年METI商務情報政策局】

http://www.iotac.jp/wp-content/uploads/2016/01/03\_%E8%B3%87%E6%96%99%EF%BC%93-%E7%B5%8C%E7%94%A3%E7%9C%81%E8%AA%AC%E6%98%8E%E8%B3%87%E6%96%99.pdf

#### IoTセキュリティチェックリスト

https://www.jpcert.or.jp/research/IoT-SecurityCheckList.html

#### IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）

https://www.meti.go.jp/press/2020/11/20201105003/20201105003.html

#### 【削除】IoTセキュリティ対応マニュアル産業保安版

https://www.meti.go.jp/policy/safety\_security/industrial\_safety/sangyo/hipregas/files/security\_manual.pdf

#### 「安全なIoTシステムのためのセキュリティに関する一般的枠組」【NISC】

https://www.nisc.go.jp/active/kihon/res\_iot\_fw2016.html

### IT-BCP関連

#### IT-BCP【平成25年NISC】

### インシデント対応

#### インシデント発生時に組織内で整理しておくべき事項（サイバーセキュリティ経営ガイドライン\_付録C）【METI】

https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM\_Guideline\_app\_C.xlsx

### 個人情報保護関連

#### GDPR（General Data Protection Regulation：一般データ保護規則）k【個人情報保護委員会】

https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/

#### DX企業のプライバシーガバナンスガイドブックver1.0【2020年8月3日METI】

https://www.meti.go.jp/press/2020/08/20200828012/20200828012.html

### システム開発・運用（外部委託）

#### 政府機関等の対策基準策定のためのガイドライン【NISC】

https://www.nisc.go.jp/active/general/kijun30.html

#### 改正民法に対応した「情報システム・モデル取引・契約書」を公開 ～ユーザ企業・ITベンダ間の共通理解と対話を促す～【IPA】

https://www.ipa.go.jp/ikc/reports/20191224.html

### 人材育成

#### デジタルリテラシー関連

「デジタルリテラシー協議会」

https://www.dilite.jp/

次世代技術を活用したビジネス展開のためのデジタルリテラシーの習得

#### iCD関連

iコンピテンシディクショナリ（iCD）について

https://www.ipa.go.jp/jinzai/hrd/i\_competency\_dictionary/index.html

#### ITSS+関連

ITSS+・ITスキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報

https://www.ipa.go.jp/jinzai/itss/itssplus.html

データサイエンス領域

https://www.ipa.go.jp/files/000063897.xlsx

アジャイル領域

https://www.ipa.go.jp/files/000065571.pdf

IoTソリューション領域

https://www.ipa.go.jp/files/000065568.pdf

セキュリティ領域

https://www.ipa.go.jp/files/000058688.xlsx

#### DX関連

デジタル・トランスフォーメーション推進人材の機能と役割のあり方に関する調査【2020年5月15日IPA】

https://www.ipa.go.jp/ikc/reports/20190412.html

#### サイバーセキュリティ関連

情報セキュリティマネジメントに要求される知識と技能【シラバス】【情報セキュリティマネジメント試験】

https://www.jitec.ipa.go.jp/sg/

【参考】【まとめ】情報セキュリティマネジメントに要求される知識と技能【シラバス】（Bib05-13）

https://bluemoon55.github.io/Sharing\_Knowledge2/MindManager2/Bib05-13.html

サイバーセキュリティ体制構築・人材確保の手引き(サイバーセキュリティ経営ガイドライン：付録F)（PDF形式）（令和2年９月30日公開）

http://www.meti.go.jp/policy/netsecurity/downloadfiles/tebiki.pdf

#### 情報処理技術者試験

情報処理技術者試験・情報処理安全確保支援士試験

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

## 法令・規則

### サイバーセキュリティ関係法令\_Q&AハンドブックVer1.0

#### https://www.nisc.go.jp/security-site/law\_handbook/index.html

### 迷惑メール関係法令・窓口等【迷惑メール白書2020】【P.142～145】

#### https://www.dekyo.or.jp/soudan/data/anti\_spam/whitepaper/2020/wp2020.pdf

## 一般ユーザ向け啓発資料【IT利用局面毎】

### インターネット利用

#### 小さな中小企業とNPO向け情報セキュリティハンドブック【NISC】

https://www.nisc.go.jp/security-site/blue\_handbook/index.html

#### インターネットの安全・安心ハンドブック【NISC】

https://www.nisc.go.jp/security-site/handbook/index.html

#### ネット接続製品の安全な選定・利用ガイド【IPA】

https://www.ipa.go.jp/security/vuln/report/notice/guideforconsumer.html

### インターネットでの不正行為を発見した場合

#### 違法情報・有害情報、誹謗中傷情報

#### 違法・有害情報相談センターへの相談

### ECサイト利用

#### 利用者向けフィッシング詐欺対策ガイドライン【2020年6月フィッシング対策協議会】

https://www.antiphishing.jp/report/guideline/consumer\_guideline2020.html

http://www.antiphishing.jp/report/consumer\_antiphishing\_guideline\_2020.pdf

#### なりすましECサイト対策対応マニュアル【2015年3月セーファーインターネット協会】

https://www.saferinternet.or.jp/wordpress/wp-content/uploads/narisumashi\_manual.pdf

### 電子メール

#### 特定電子メールの送信の適正化等に関する法律のポイント（2020年度版）【日本データ通信協会迷惑メール相談センター】

https://www.soumu.go.jp/main\_sosiki/joho\_tsusin/d\_syohi/pdf/m\_mail\_pamphlet.pdf

#### チェーンメール対策BOOK\_「撃退！チェーンメール 」（2021年度版）【日本データ通信協会迷惑メール相談センター】

https://www.dekyo.or.jp/soudan/data/chain/chainbook.pdf

#### 詐欺メール対策リーフレット「そのメール、詐欺カモ！？」（2021年度）【日本データ通信協会迷惑メール相談センター】

https://www.dekyo.or.jp/soudan/data/info/A4\_maildesagi.pdf

#### 迷惑メール対策BOOK\_「撃退！迷惑メール」（2021年度版）【日本データ通信協会迷惑メール相談センター】

https://www.dekyo.or.jp/soudan/contents/info/pamphlet\_gm.html

## サイバーセキュリティ関連組織が開設するポータルサイト

### 内閣サイバーセキュリティセンター（NISC）

#### https://www.nisc.go.jp/

#### みんなでしっかりサイバーセキュリティ

https://www.nisc.go.jp/security-site/index.html

#### みんなで使おうサイバーセキュリティ・ポータルサイト

https://security-portal.nisc.go.jp/

### 情報処理推進機構（IPA）

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

#### 情報セキュリティ トップページ

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

#### 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

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

#### SECURITY ACTION セキュリティ対策自己宣言

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

#### サイバー情報共有イニシアティブ（J-CSIP）

https://www.ipa.go.jp/security/J-CSIP/

### JPCERTコーディネーションセンター（JPCRT/CC）

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

#### 緊急情報を確認する

https://www.jpcert.or.jp/menu\_alertsandadvisories.html

#### 脆弱性対策情報データベース（JVN）

https://jvn.jp/

#### JPCERT/CCに依頼する

https://www.jpcert.or.jp/menu\_reporttojpcert.html

### 総務省

#### 国民のための情報セキュリティサイト（総務省）

https://www.soumu.go.jp/main\_sosiki/joho\_tsusin/security/

#### リンク集｜国民のための情報セキュリティサイト - 総務省

https://www.soumu.go.jp/main\_sosiki/joho\_tsusin/security/link.html

### 経済産業省

#### サイバーセキュリティ政策

https://www.meti.go.jp/policy/netsecurity/index.html

### 日本サイバー犯罪対策センター（JC3）

#### https://www.jc3.or.jp/

### 情報セキュリティ広場（警視庁）

#### https://www.keishicho.metro.tokyo.jp/kurashi/cyber/index.html

### セーファーインターネット協会（一般社団法人）

#### https://www.saferinternet.or.jp/

# Sec01-01-04\_6.4\_0\_AP\_中小企業の情報セキュリティ対策ガイドライン（INFORMATION 6-4追補原稿）

## INFORMATION 6-4 App.01 中小企業の情報セキュリティ対策の段階的レベルアップ

### はじめに

### 経営者編

#### 認識すべき３原則

#### 実行すべき「重要７項目の取組」

### 実践編

#### できるところから始める

【付録1】情報セキュリティ5か条

#### 組織的な取り組みを開始する

（１）情報セキュリティ基本方針の作成と周知

【付録2】情報セキュリティ基本方針（サンプル）

（２）実施状況の把握

【付録3】5分でできる情報セキュリティ自社診断

（３）対策の決定と周知

【付録4】情報セキュリティハンドブック（ひな型）

#### 本格的に取り組む

（１）管理体制の構築

【付録5】情報セキュリティ関連規程（サンプル）：「自社の管理体制」

（２）IT利活用方針と情報セキュリティの予算化

（３）情報セキュリティ規程の作成

①対応すべきリスクの特定

②対策の決定

③規程の作成

【付録5】情報セキュリティ関連規程（サンプル）をベースに

  【Web版Appendix】6-4-X\_Appendix\_情報セキュリティ関連規程に記載すべき項目の概要【 付録5】

（４）委託時の対策

契約書や覚書に具体的な対策を明記

（５）点検と改善

作成したドキュメント通りに実行されているか？

  【Web版Appendix】6-4-X\_Appendix\_サイバーセキュリティ経営チェックシート【「サイバーセキュリティ経営ガイドライン」Ver2.0 付録A】

#### より強固にするための方策

（１）情報収集と共有

①情報収集の方法

②情報共有の枠組み

（２）ウェブサイトの情報セキュリティ

（３）クラウドサービスの情報セキュリティ

【付録6】クラウドサービス安全利用の手引き

（４）情報セキュリティサービスの活用

（５）技術的対策例と活用

（６）詳細リスク分析の実施方法

 【Web版Appendix】6-4-1\_Appendix\_情報資産台帳の作成と詳細リスク分析

【付録7】 リスク分析シート

# Sec01-01-04\_6.4\_1\_AP\_情報資産台帳の作成と詳細リスク分析（INFORMATION 6-4追補原稿）

## 概要

### 事業規模が大きくなったり、情報システムが複雑になると、想定外のリスクを見落とし、対策が不十分になることがあります。そこでここでは、もれなくリスクを特定し、対策を検討する手法を提示します。

### 「中小企業の情報セキュリティ対策ガイドライン」に沿って「本格的に取り組む」アクションとして、①管理体制の構築、②IT活用方針と情報セキュリティの予算化、③情報セキュリティ規程の作成、④委託時の対策、⑤点検と改善が、挙げられています。

### ③情報セキュリティ規程の作成に当たっては、まず、どんな情報資産を保有し、それぞれの情報資産に対してどんなリスクがあるか、それを見極めた上で、どのような情報セキュリティ対策をするかを決定することがことが重要です。

### ここでは、「情報資産の洗い出し」、「リスク値の算定」、「リスク対策の決定」の手法を手順を追って紹介します。

## 策定の流れ

### 手順1 情報資産の洗い出し

#### まずは、情報資産台帳として、自社で管理している情報資産を悉皆的にリストアップする。

#### ●情報資産管理台帳の作成

特に、セキュリティ侵害を受けると事業の継続を脅かされると思われる情報資産に関しては、保存場所はどこか、個人情報を含むか、なども調査しておく。

#### ●情報資産ごとの機密性・完全性・可用性の評価

情報資産毎に、機密性、完全性、可用性が損なわれた場合の事業への影響や、法律で安全管理義務があるなどを勘案して、評価値を算定する。

#### ●機密性・完全性・可用性の評価値から重要度を算定

情報資産ごとの機密性、完全性、可用性の評価値をもとに、重要度を算定する。

### 手順２ リスク値の算定

#### 情報資産毎に、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定する。

### 手順３ 情報に対するリスク対策を決定

#### リスクの大きな情報資産を優先して、リスク対策（リスクの低減、回避、移転、保有）の分類で、情報セキュリティ対策を決定する。

### 次のステップ：情報セキュリティ規程の作成

#### 情報に対するリスク対策で分類された内容を具体的に講じられるように、情報セキュリティ規程を作成する。

## 手順1 情報資産の洗い出し

### 業種、事業内容、IT環境によって保有する情報資産は異なるため、自社の情報資産を一通り洗い出し、情報資産ごとの機密性・完全性・可用性を評価し、それぞれの評価値から重要度を算定する

### ●情報資産管理台帳の作成

#### 情報資産管理台帳は洗い出した情報資産を「見える化」するための方法の一つ



#### 情報資産諸元

①業務分類

情報資産に関連する業務や部署名を記入します。情報資産は業務に関連して発生しますので、まず関連業務や部署を特定し、その業務や部署で利用している情報を洗い出すと記入漏れが少なくなります。

②情報資産名称

情報資産の内容を簡潔に記入します。正式名称がないものは社内の通称で構いません。管理方法や重要度が同じものは1行にまとめます。

③備考

必要に応じて説明等を記入します。

④利用者範囲

情報資産を利用してよい部署等を記入します。

⑤管理部署

情報資産の管理責任がある部署等を記入します。小規模事業者であれば担当者名を記入しても構いません。

⑥媒体・保存先

情報資産の媒体や保存場所を記入します。書類と電子データの両方で保存している場合は、それぞれ完全性・可用性（機密性は同一）や脅威・脆弱性が異なるので2行に分けて記入します。 例）見積書「電子データを事務所PC に保存」「印刷して書類を保管」

⑦個人情報の種類

各項目が個人情報保護法、マイナンバー法で定義されています。

⑧重要度

重要度定義シートまたは中小企業の情報セキュリティ対策ガイドラインP.45表10を参照して、情報資産の機密性、完全性、可用性それぞれの評価値を記入します。3種類の評価値から中小企業の情報セキュリティ対策ガイドラインP.46表11に基づき重要度が表示されます。なお、⑦でいずれかの個人情報が「有」の場合、重要度は自動的に「2」となります。

⑨保存期限

法定文書は法律で定められた保存期限を、それ以外は利用が完了して廃棄、消去が必要となる期限を記入します。

⑩登録日

登録した日付を記入します。内容を更新した場合は更新日に修正します。

### ●情報資産ごとの機密性・完全性・可用性の評価

#### 機密性、完全性、可用性が損なわれた場合の事業への影響や、法律で安全管理義務があるなど、評価基準を参考に評価値２～０を記入します。

#### 機密性

アクセスを許可された者だけが情報にアクセスできる

機密性レベル２

法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている

守秘義務の対象や限定提供データ12 として指定されている

漏えいすると取引先や顧客に大きな影響がある

自社の営業秘密として管理すべき（不正競争防止法による保護を受けるため）漏えいすると自社に深刻な影響がある

機密性レベル１

漏えいすると業務に大きな影響がある

機密性レベル０

漏えいしても業務にほとんど影響はない

#### 完全性

情報や情報の処理方法が正確で完全である

機密性レベル２

法律で安全管理（漏えい、滅失又はき損防止）が義務付けられている

改ざんされると自社に深刻な影響または取引先や顧客に大きな影響がある

機密性レベル１

改ざんされると業務に大きな影響がある

機密性レベル０

改ざんされても事業にほとんど影響はない

#### 可用性

許可された者が必要な時に情報資産にアクセスできる

可用性レベル２

利用できなくなると自社に深刻な影響または取引先や顧客に大きな影響がある

可用性レベル１

利用できなくなると事業に大きな影響がある

可用性レベル０

利用できなくなっても事業にほとんど影響はない

### ●機密性・完全性・可用性の評価値から重要度を算定

#### 重要度は、機密性、完全性、可用性いずれかの最大値で判断します。 「情報資産管理台帳」に記入した機密性・完全性・可用性の評価値をもとに、判断基準に従い、重要度を算定します。

※下記の場合は、算定結果に関わらず、重要度は２とします。

企業の存続を左右しかねない場合

事故が起きると法的責任を問われる

取引先、顧客、個人に大きな影響がある

事業に深刻な影響を及ぼす

個人情報を含む場合

#### 情報資産の重要度の判断基準

重要度レベル２

機密性・完全性・可用性評価値のいずれかまたはすべてが「2」の情報資産

重要度レベル１

機密性・完全性・可用性評価値のうち最大値が「1」の情報資産

重要度レベル０

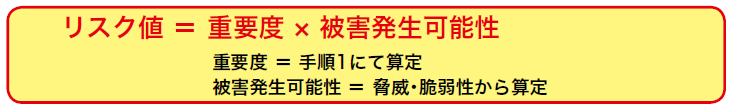
機密性・完全性・可用性評価値すべてが「0」の情報資産

## 手順２ リスク値の算定

### 優先的・重点的に対策が必要な情報資産を把握する

#### 洗い出した情報資産について、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定

### リスク値＝重要度×被害発生可能性



### 「被害発生可能性」

#### 「被害発生可能性」は「脅威の起こりやすさ」と「脆弱性のつけ込みやすさ」の２つの数値から算出

#### 脅威の起こりやすさ

脅威レベル３

通常の状況で脅威が発生する（いつ発生してもおかしくない）

脅威レベル２

特定の状況で脅威が発生する（年に数回程度）

脅威レベル１

通常の状況で脅威が発生することはない

#### 脆弱性のつけ込みやすさ

脆弱性レベル３

対策を実施していない（ほぼ無防備）

脆弱性レベル２

部分的に対策を実施している

脆弱性レベル１

必要な対策をすべて実施している

#### 被害発生可能性

被害発生可能性=脅威レベル÷（4－脆弱性レベル）



被害発生可能性レベル３

通常の状況で被害が発生する（いつ発生してもおかしくない）

被害発生可能性レベル２

特定の状況で被害が発生する（年に数回程度）

被害発生可能性レベル１

通常の状況で被害が発生することはない

## 手順３ 情報セキュリティ対策を決定

### リスクの大きな情報資産に対して必要とされる対策を決める

### リスク対策の分類

#### リスクを低減（リスクの発生確率を下げる対策）

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る

例：重要な情報へのアクセス制御、ソフトウェアの更新の徹底

#### リスクを回避（リスクが発生する可能性を除去する対策）

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す

例：端末の持ち出し禁止 （外部での盗難のリスクを回避）

#### リスクを移転（リスクを他者等の移す対策）

自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで自社の負担を下げる

例：クラウドサービスの利用、サイバー保険の加入

#### リスクを保有（残留リスクとして識別）

事故が発生しても許容する

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、現状を維持する

## 参考資料

### 中小企業の情報セキュリティ対策ガイドライン第3版【IPA】

#### 第2部実践編

より強固にするための方策

詳細リスク分析の実施方法

### サイバーセキュリティ経営ガイドライン [Ver.2.0]【METI/IPA】

#### サイバーセキュリティ経営の重要10項目

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

# Sec01-01-04\_6.4\_2\_AP\_情報セキュリティ関連規程に記載すべき項目の概要【付録5】（INFORMATION 6-4追補原稿）(p-083-03.html)

## INFORMATION 6-4 App.03 情報セキュリティ関連規程に記載すべき項目

### 概要

#### 企業を取り巻くリスクは、事業内容や取り扱う情報、職場環境、ITの利用状況などによっても異なることがあり、汎用的な規程をそのまま使っても、自社に適さないことが考えられます。そこでここでは、効率的に自社に適した規程を作成する方法を解説します。

#### ①対応すべきリスクの特定

経営者が避けたい重大事故から対応すべきリスクを特定

#### ②対策の決定

・リスクの大きなものを優先して対策を実施

・リスクが小さなものは許容するなど、合理的に対応

#### ③規程の作成

「情報セキュリティ関連規程（サンプル）」を参考に、自社に適した規定にするために修正を加える

### 情報セキュリティ関連規程の概要

#### 1.組織的対策：

情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。

#### 2.人的対策：

取締役及び従業員の責務や教育、人材育成などのルールを定めます。

#### 3.情報資産管理：

情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。

#### 4.アクセス制御及び認証：

情報資産に対するアクセス制御方針や認証のルールを定めます。

#### 5.物理的対策：

セキュリティ領域の設定や領域内での注意事項などのルールを定めます。

#### 6.IT機器利用：

IT機器やソフトウェアの利用などのルールを定めます。

#### 7.IT基盤運用管理：

サーバーやネットワーク等のITインフラに関するルールを定めます。

#### 8.システムの開発及び保守：

独自に開発及び保守を行う情報システムに関するルールを定めます。

#### 9.委託管理：

業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルが付属します。

#### 10.情報セキュリティインシデント対応ならびに事業継続管理：

情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。

#### 11.個人番号及び特定個人情報の取り扱い：

マイナンバーの取り扱いに関するルールを定めます。

### 1.組織的対策：

#### 情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。

#### 1.1.情報セキュリティのための組織

情報セキュリティ対策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、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。

#### 1.2.情報セキュリティ取組みの監査・点検/点検

#### 1.3.情報セキュリティに関する情報共有

入手先

・IPA

[情報セキュリティ]

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

[ここからセキュリティ]

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

・JVN（Japan Vulnerability Notes）

https://jvn.jp/index.html

・JPCERT/CC

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

・個人情報保護委員会

http://www.ppc.go.jp/

### 2.人的対策：

#### 取締役及び従業員の責務や教育、人材育成などのルールを定めます。

#### 2.1.雇用条件

#### 2.2.従業員の責務

#### 2.3.雇用の終了

#### 2.4.情報セキュリティ教育

#### 2.5.人材育成

### 3.情報資産管理：

#### 情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。

#### 3.1.情報資産の管理

3.1.1.情報資産の特定と機密性の評価

3.1.2.情報資産の分類の表示

3.1.3.情報資産の管理責任者

3.1.4.情報資産の利用者

#### 3.2.情報資産の社外持ち出し

#### 3.3.媒体の処分

3.3.1.媒体の廃棄

3.3.2.媒体の再利用

#### 3.4.バックアップ

3.4.1.バックアップ取得対象

3.4.2.バックアップ媒体の取り扱い

3.4.3.クラウドサービスを利用したバックアップ

### 4.アクセス制御及び認証：

#### 情報資産に対するアクセス制御方針や認証のルールを定めます。

#### 4.1.アクセス制御方針

#### 4.2.利用者の認証

#### 4.3.利用者アカウントの登録

#### 4.4.利用者アカウントの管理

#### 4.5.パスワードの設定

#### 4.6.従業員以外の者に対する利用者アカウントの発行

#### 4.7.機器の識別による認証

#### 4.8.端末のタイムアウト機能

#### 4.9.標準設定等

4.9.1.アクセス制御対象情報システム及びアクセス制御方法

4.9.2.利用者認証方法

4.9.3.利用者アカウント・パスワードの条件

4.9.4.機器の認証方法

### 5.物理的対策：

#### セキュリティ領域の設定や領域内での注意事項などのルールを定めます。

#### 5.1.セキュリティ領域の設定

#### 5.2.関連設備の管理

#### 5.3.セキュリティ領域内注意事項

#### 5.4.搬入物の受け渡し

### 6.IT機器利用：

#### IT機器やソフトウェアの利用などのルールを定めます。

#### 6.1.ソフトウェアの利用

6.1.1.標準ソフトウェア

6.1.2.ソフトウェアの利用制限

6.1.3.ソフトウェアのアップデート

6.1.4.ウイルス対策ソフトウェアの利用

6.1.4.1.ウイルス検知

6.1.4.2.ウイルス対策ソフト定義ファイルの更新

6.1.4.3.社外機器のLAN接続

6.1.5.ウイルス対策の啓発

#### 6.2.IT機器の利用

#### 6.3.クリアデスク・クリアスクリーン

#### 6.3.1.クリアデスク

#### 6.3.2.クリアスクリーン

#### 6.4.インターネットの利用

6.4.1.ウェブ閲覧

6.4.2.オンラインサービス

6.4.3.SNSの個人利用

6.4.4.電子メールの利用

6.4.5.ウイルス感染の防止

#### 6.5.私有IT機器・電子媒体の利用

6.5.1.利用開始時

6.5.2.利用期間中

6.5.2.1.社内での利用

6.5.3.利用終了時

#### 6.6.標準等

6.6.1.標準ソフトウェア

6.6.2.ソフトウェアのアップデート方法

6.6.3.ウイルス対策ソフトウェアの定義ファイルの更新方法

### 7.IT基盤運用管理：

#### サーバーやネットワーク等のITインフラに関するルールを定めます。

#### 7.1.管理体制

#### 7.2.IT基盤の情報セキュリティ対策

7.2.1.サーバー機器の情報セキュリティ要件

7.2.2.サーバー機器に導入するソフトウェア

7,2.3.ネットワーク機器の情報セキュリティ要件

#### 7.3.IT基盤の運用

#### 7.4.クラウドサービスの導入

#### 7.5.脅威や攻撃に関する情報の収集

#### 7.6.廃棄・返却・譲渡

#### 7.7.IT基盤標準

7.7.1.サーバー機器情報セキュリティ要件

7.7.2.IT基盤標準ソフトウェア

7.7.3.標準ネットワーク機器

7.7.4.ネットワーク機器情報セキュリティ要件

7.7.5.クラウドサービス情報セキュリティ対策評価基準

### 8.システムの開発及び保守：

#### 独自に開発及び保守を行う情報システムに関するルールを定めます。

#### 8.1.新規システム開発・改修

#### 8.2.脆弱性への対処

#### 8.3.情報システムの開発環境

#### 8.4.情報システムの保守

#### 8.5.情報システムの変更

### 9.委託管理：

#### 業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルが付属します。

#### 9.1.委託先評価基準

#### 9.2.委託先の選定

#### 9.3.委託契約の締結

#### 9.4.委託先の評価

#### 9.5.再委託

### 10.情報セキュリティインシデント対応ならびに事業継続管理：

#### 情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。

#### 10.1.対応体制

#### 10.2.情報セキュリティインシデントの影響範囲と対応者

#### 10.3.インシデントの連絡及び報告

#### 10.4.対応手順

10.4.1.漏えい・流出発生時の対応

10.4.2.改ざん・消失・破壊・サービス停止発生時の対応

10.4.3.ウイルス感染時の初期対応

10.4.4.欠番

10.4.5.届出及び相談

#### 10.5.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

10.5.1.想定される情報セキュリティインシデント

10.5.2.復旧責任者及び関連連絡先

10.5.3.事業継続計画

### 11.個人番号及び特定個人情報の取り扱い：

#### マイナンバーの取り扱いに関するルールを定めます。

#### 11.1.関係法令・ガイドライン等の遵守

#### 11.2.利用目的

#### 11.3.安全管理措置に関する事項

#### 11.4.委託の取り扱い

#### 11.5.継続的改善

#### 11.6.特定個人情報等の開示

#### 【参考】「個人番号及び特定個人情報取扱規程」サンプル

# Sec01-01-04\_6.4\_3\_AP\_情報セキュリティ基本方針および情報セキュリティハンドブックの概要【付録2・4】（INFORMATION 6-4追補原稿）

## 概要

### 「できるところから始める」の次のステップとしての「組織的な取り組み」は、「5分でできる！情報セキュリティ自社診断」を実施し、「情報セキュリティ基本方針」を定め、公開すること。これにより「SECURITY ACTION」の２段階目の「二つ星」を使用することができます。

### 情報セキュリティハンドブックは、「5分でできる！情報セキュリティ自社診断」で確認された事項を、従業員向けに明文化したものである。

### 組織としての次のステップとして、本格的に取り組むためには、「情報セキュリティ関連規程」として対策基準を明文化することが求められる。

## 情報セキュリティ基本方針（サンプル）

### 概要

#### 中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。

### 内容例

#### 株式会社○○○○（以下、当社）は、お客様からお預かりした/当社の/情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。

#### 1.経営者の責任

当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。

#### 2.社内体制の整備

当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。

#### 3.従業員の取組み

当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。

#### 4.法令及び契約上の要求事項の遵守

当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。

#### 5.違反及び事故への対応

当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努めます。

## 情報セキュリティハンドブック（ひな形）

### ハンドブック（ひな形）の使い方

#### このハンドブック（ひな形）は、従業員に配付し、自社のセキュリティルールを実行してもらうためのものです。

#### ５分でできる！情報セキュリティ自社診断の対策例に連動しています。

#### 自社のルールに合わせて編集し、全従業員に配付するなどして一人ひとりが実施すべき対策の周知に取り組んでください。

### １-１ 全社基本ルール

#### OSとソフトウェアのアップデート

パソコンやスマホなど情報機器のOS やソフトウェアは常に最新の状態にする。【自己診断No.1】

#### ウイルス対策ソフトの導入

パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にする。【自己診断No.2】

#### パスワードの管理

パスワードは破られにくい「長く」「複雑な」パスワードを設定する。【自己診断No.3】

### １-２ 全社基本ルール

#### アクセス制御

重要情報に対する適切なアクセス制限を行う。【自己診断No.4】

#### セキュリティに対する注意

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を作る。【自己診断No.5】

### ２-１ 仕事中のルール

#### 電子メールの利用

電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつける。【自己診断No.7】

電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施する。【自己診断No.8】

### ２-１ 仕事中のルール

#### 電子メールの利用

電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつける。【自己診断No.6】

### ２-３ 仕事中のルール

#### インターネットの利用

インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をする。【自己診断No.10】

#### データのバックアップ

パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得する。【自己診断No.11】

### ２-４ 仕事中のルール

#### クリアデスク・クリアスクリーン

紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管する。【自己診断No.12】

離席時にパソコン画面の覗き見や勝手な操作ができないようにする。【自己診断No.14】

#### 重要情報の持ち出し

重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をする。【自己診断No.13】

#### 重要情報の保管

紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管する。【自己診断No.12】

#### ２-５ 仕事中のルール

入退室

事務所が無人になる時の施錠忘れ対策を実施する。【自己診断No.17】

電子媒体・書類の廃棄

重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにする。【自己診断No.18】

#### ３-１ 全社共通のルール

私有情報機器の利用

個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にする。【自己診断No.21】

#### ３-2 全社共通のルール

クラウドサービスの利用

クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定する。【自己診断No.23】

#### ３-３ 従業員のみなさんへ

従業員の守秘義務

従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせる。

事故が起きてしまったら

セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をする。

# Sec01-01-04\_6.6\_1\_AP\_次世代技術を活用したビジネス展開のためのデジタルリテラシーの習得（INFORMATION 6-6追補原稿）

## INFORMATION 6-6 App.01 次世代技術を活用したビジネス展開のためのデジタルリテラシーの習得

### 概要

#### 全てのビジネスパーソンがデジタル時代のコア・リテラシーを身につけていくことが求められます。

内閣府が策定した「AI戦略2019」において、AI時代に対応した人材育成や、それを持続的に実現する仕組みの構築が戦略目標に挙げられているとおり、デジタル時代の人材育成は国全体の重要な課題となっています。

デジタルトランスフォーメーションの推進には、これまでの「デジタルを作る人材」だけでなく、「デジタルを使う人材」も含めた両輪の育成が必要となる

#### IT・データサイエンス・AIの三方面からデジタルリテラシーの向上を図る

ITの利活用を推進するIPA、データサイエンティストのスキル定義や人材育成を支援するDSS、ディープラーニング技術の産業活用を推進するJDLAが連携して、デジタルリテラシーの向上を図るために準備を進めている

### 中小企業における人材育成の戦略

#### 中小企業が、ビジネスを発展させるためには、攻めのIT投資とサイバーセキュリティ対策を講ずる必要がある

#### 「経営者、システム管理者が、「デジタルリテラシー」の知識とスキルを得て、①守りのIT・セキュリティ対策に留まらず、②事業を発展させるためのの攻めのIT・セキュリティ対策を講じるための人材の育成を推進するべきである.

※「バイモーダル」を考える

※ITの知識を持たずにセキュリティ対策を講じることは困難。セキュリティ対策は、IT活用の推進の中でセキュリティバイデザインの考え方で対処する

#### ①守りのIT・セキュリティ対策

これまで組織のITシステムは、業務の改善や効率化によるコスト削減により、経営を安定化させることに重きが置かれ、サービスの維持が図られてきた。

現状を維持するためだけでも新たなIT技術への対応と、新たな脅威への対処のためのセキュリティ対策が必要である。

#### ②攻めのIT・セキュリティ対策

しかしながら、サービスの維持だけでは、ビジネスの競争に勝ち残れない。

時代のニーズに対応した高付加価値の新たな取り組みにより、サービスを向上させていかなければ、組織の発展はおろか、継続も見込めなくなることが予想される。

より先進的な技術を活用した新たなサービスを、他社に先駆けて提供していくことが望まれる。

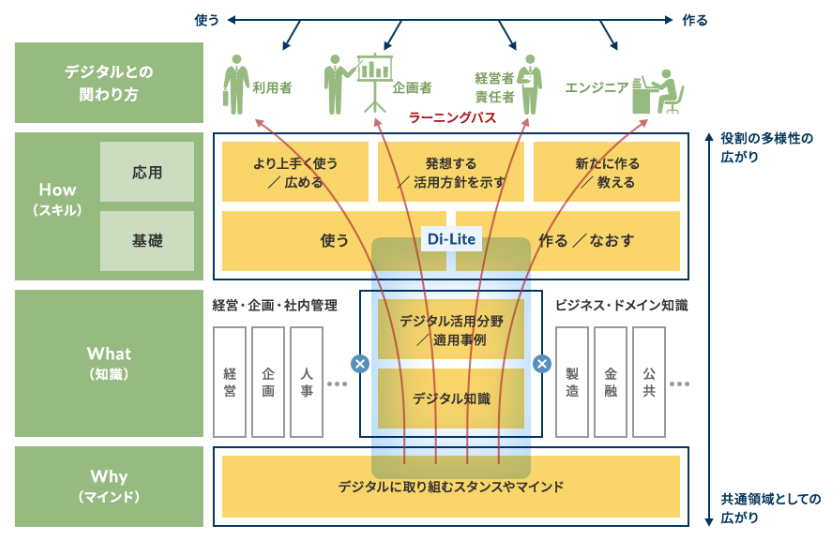
そのためにも、組織人として、ITやデジタルを利活用できるデジタルリテラシーの習得が求められる。

### 「デジタルリテラシー」の習得

#### デジタルトランスフォーメーションの推進には、これまでの「デジタルを作る人材」だけでなく、「デジタルを使う人材」が必要だが、中小企業においては、まず、「デジタルを使う人材」の育成に力を入れるべきである、

#### 「デジタルリテラシー・スキルフレームワーク」で網羅的・体系的に

概念



デジタルリテラシーの浸透に向けたツール

デジタル変革の推進による、より良い社会（Society5.0）の創出に向けて、ビジネスパーソンが身につけるべきデジタルリテラシー領域「Di-Lite」を示すために、デジタルに関連して習得すべきスキルや知識・マインドを構造的に全体像として表したもの。

デジタルリテラシー領域「Di-Lite」

デジタル技術の進展に合わせた網羅的なデジタルリテラシーとして、IT・データサイエンス・AIを使うための基礎的なスキル・知識・マインド

マインド

デジタルに取り組むスタンス、マインド

知識体系

デジタル活用分野/適用事例

デジタル知識

スキル

基礎

使う、作る/なおす

応用

より上手に使う/広める

発想する/活用方針を示す

新たに作る/教える

対象者

利用者

企画者

経営者/責任者

エンジニア

### 「デジタルリテラシー協議会」

#### 構成組織

一般社団法人データサイエンティスト協会（DSS)

一般社団法人日本ディープラーニング協会（JDLA)

独立行政法人情報処理推進機構（IPA)

#### 取り組み

産業界において日本がグローバルで戦うための競争力の源泉となる人材の育成を目指し、官民連携の会議体を運営し協議・情報発信を行う。

「データ×AI」活用に関する教育環境を整える

デジタルリテラシーの見える化

すべてのビジネスパーソンが共通言語としてデジタルリテラシーを身につけた状態を達成を目指す

協議結果を各団体が実施する検定や試験のシラバスにも反映する

ITパスポート試験（IPA実施)

データサイエンティスト検定リテラシーレベル（JDLA実施)

G検定（JDLA実施)

「Di-Lite」の設定や浸透活用、及び「Di-Lite」をはじめとするデジタルリテラシー・スキル習得を助けるためのツール提供も行う。

#### 活動内容

「Di-Lite」に関する協議（見直しと再定義）

(1)産業界やユーザーの声を反映した「Di-Lite」の更新

(2)デジタル技術の進化に合わせたデジタルリテラシー領域の網羅性確認

(3)各参加団体の実施する検定や資格制度の連携

デジタルリテラシーの浸透に向けたツール類の提供

(1)デジタルリテラシー・スキルフレームワークの提供

(2)デジタルスキルラーニングパスの提供

企業に向けた普及・啓発活動の共同推進

(1)展示会、セミナー等における普及啓発の実施、充実化

(2)記事の掲載等、ビジネスパーソン向け情報発信の充実化

# Sec01-01-04\_6.6\_2\_AP\_能力再開発「リスキリング」（INFORMATION 6-6追補原稿）

## INFORMATION 6-6 App.02 能力再開発「リスキリング」

### DAX96-03\_リスキニングの必要性と実践

# Sec01-01-04\_6.6\_2\_AP\_数理・データサイエンス・AI（リテラシーレベル）モデルカリキュラム

## サブトピック

# 極意原稿用テンプレート

## 中小企業向けサイバーセキュリティ対策の極意

### ヘッダー２

#### ヘッダー３

ヘッダー４

本文１

本文2

箇条書きタイトル１

箇条書き１

箇条書き２