

SEC01-08-2 専門員の所掌業務及び 調査分析項目

1 改版履歴

1.1 【2020 年 1 月 29 日】「中小企業向けサイバーセキュリティ対策の極意」の改訂（追補資料の作成）の詳細を SEC01-01-01 へ移行

1.2 【2019 年 10 月 9,24 日】資料目次作成及びリンク

参照: [資料目次](#)

1.3 【2019 年 9 月 26 日】専門員要件の追加

参照: [専門員の所掌業務及び行動規範の概要](#)

1.4 【2019 年 7 月 26 日】ポータルサイトの追加仕様

参照: [ポータルサイト新規ページ仕様](#)

1.5 【2019 年 7 月 25 日】極意の校正予定箇所の提示(現行構成毎)

参照: [「中小企業向けサイバーセキュリティ対策の極意」の改訂（追補資料の作成）](#)

1.6 【2019 年 6 月 21 日】極意の校正予定箇所の提示

1.7 【2019 年 6 月 13 日】2019 年実施項目【案】、項目表の併合

1.8 【2018 年 10 月 24 日】所掌業務内容の明確化

1.9 【2018 年 10 月 11 日】「情報収集・整理・蓄積と発信」のイメージ図を最終ページに移動

1.10 【2018 年 6 月 6 日】係会議資料として提出

2 **1** 資料目次

2.1 **2** 専門員の所掌業務及び行動規範の概要

参照: [専門員の所掌業務及び行動規範の概要](#)

2.2 **2** 専門員の所掌業務の詳細内容

参照: [専門員の所掌業務の詳細内容](#)

2.2.1 **3** ポータルサイト新規ページ仕様

参照: [ポータルサイト新規ページ仕様](#)

2.2.2 **3** 中小企業向けサイバーセキュリティ対策情報の発信【体系的な情報アーカイブ】

参照: [中小企業向けサイバーセキュリティ対策情報の発信【体系的な情報アーカイブ】](#)

2.2.3 **3** 「中小企業向けサイバーセキュリティ対策の極意」の改訂（追補資料の作成）

参照: [「中小企業向けサイバーセキュリティ対策の極意」の改訂（追補資料の作成）](#)

2.2.4 **3** 「中小企業向けサイバーセキュリティ対策の極意」の内容の詳細化（解説資料の作成）

参照: [「中小企業向けサイバーセキュリティ対策の極意」の内容の詳細化（解説資料の作成）](#)

2.2.4.1 **4** SEC01-01「中小企業向けサイバーセキュリティ対策の極意」解説書を参照

ドキュメントを参照: [Sec01-01「中小企業向けサイバーセキュリティ対策の極意」解説書.html](#)

2.2.5 **3** 中小企業向けサイバーセキュリティ対策のハンドブック【対策情報の書庫】【ナレッジデータベース】の維持・更新

参照: [中小企業向けサイバーセキュリティ対策のハンドブック【対策情報の書庫】【ナレッジデータベース】の維持・更新](#)

2.3 **2** 別添資料

参照: [別添資料](#)

2.4 **2** TCYSS での情報収集・整理・蓄積と発信

参照: [TCYSS での情報収集・整理・蓄積と発信](#)

3 **1** 専門員の所掌業務及び行動規範の概要

3.1 **2** 所掌事務

3.1.1 **3** (1) サイバーセキュリティに関する中小企業からの相談対応（窓口・電話・メールなど）及び相談記録作成⇒【受付業務】

参照: [\(1\) サイバーセキュリティに関する中小企業からの相談対応（窓口・電話・メールなど）及び相談記録作成](#)

3.1.2 **3** (2) サイバーセキュリティに関する中小企業支援施策の実施に関する業務（※普及啓発セミナーの運営、事例集作成等）⇒【情報発信】

参照: [\(2\) サイバーセキュリティに関する中小企業支援施策の実施に関する業務（※普及啓発セミナーの運営、事例集作成等）](#)

3.1.3 **3** (3) 課長級、課長代理級からの指示に基づく各種資料作成業務⇒【情報収集・整理・蓄積】

参照: [\(3\) 課長級、課長代理級からの指示に基づく各種資料作成業務](#)

3 (4) その他付随する業務

参照: [\(4\) その他付随する業務](#)

3.1.3.1 **4** ガイドブック送付依頼受付及び発送

3.1.3.2 **4** 会議等設営準備

3.1.3.3 **4** 係内庶務

3.2 **2** 求められる能力（専門員公募要項より）

3.2.1 事務処理(WORD,EXCEL 等のパソコン操作を含む)について一定の知識・能力を有する

3.2.1.1 社会人の常識とされる「IT パスポート試験」レベルの知識・能力

3.2.2 サイバーセキュリティや情報システムに関する基本的な知識を有していることが望ましい

3.2.2.1 IT 関連の基礎技術とされる「基礎情報技術者試験」認定レベルの知識・能力

3.2.2.2 可能であれば、「情報セキュリティマネジメント試験」認定レベルの知識・能力

3.2.3 職務を遂行する意欲を有している

3.2.3.1 公務員倫理、職業倫理に沿った行動の中で、自己の能力を発揮し自己実現する

3.3 **2** 基本姿勢

3.3.1 専門員の所掌事務を具体的な業務として目標を設定し、その目標の達成を目指す

3.3.2 IT およびセキュリティの最新動向を把握して、専門員としてのスキル、知識の維持・向上を図り、モチベーションを維持する（スキル・知識を陳腐化させない）

3.3.3 公務員倫理、東京都コンプライアンス、職業倫理に沿って行動する

3.4 **2** 専門員としての行動規範

3.4.1 **3** 非常勤専門員の役割

3.4.1.1 学識・知識・経験等に基づき、業務に補助的に従事し、行政運営を補完する

3.4.2 **3** ワーク・ライフ・インテグレーションを目指す

3.4.2.1 自らの人生観を軸に、職業生活と個人生活を柔軟、かつ高い次元で統合し、双方の充実を求めること

3.4.2.2 それによって生産性や成長拡大を実現するとともに生活の質を高め、充実感と幸福感を得るなどの相乗効果を目指す働き方

3.4.2.3 自己の能力を発揮、自己実現して、創造性のある仕事を効率的・効果的に。確かにできていることを日々のアウトプットで検証。

3.5 **2** 所掌分担の明示の目的

3.5.1 相談対応の回答内容の均質化を目指す

3.5.1.1 専門員の知識・ノウハウの形式知化（ドキュメント化）

3.5.1.2 ドキュメントによる情報の共有とノウハウの蓄積

3.5.2 相談対応の回答レベルの向上に努める

3.5.2.1 日常での情報収集、整理

3.5.3 専門員の交代時の引き継ぎの円滑化を図る

3.5.3.1 ドキュメントによる引き継ぎ

4 **1** 専門員の所掌業務の詳細内容

4.1 **2** （１） サイバーセキュリティに関する中小企業からの相談対応（窓口・電話・メールなど）及び相談記録作成

4.1.1 （相談対応の質の向上、均質化）

4.1.2 方針

4.1.2.1 一次対応担当（フロントエンド）、二次対応担当（バックオフィス）の創設

4.1.2.2 一次対応は、日常のルーティンワーク（定型業務）

4.1.2.3 一次対応担当が受付け、調整の必要度を判断し、二次対応担当へディスパッチ。二次対応担当が回答する。

4.1.3 電話

4.1.3.1 一次対応担当は、簡易な回答もしくは二次対応へのディスパッチ

4.1.3.1.1 簡易な相談は、一次対応担当が回答。複合的な内容、技術的な案件は、相談のカテゴリを確認し、二次対応担当へ引継ぎ。

4.1.3.1.2 ディスパッチに必要な最低限の情報を担当内で共有

4.1.3.1.2.1 緊急：セキュリティ侵害発生

4.1.3.1.2.1.1 法律違反の可能性

4.1.3.1.2.1.2 法律相談

4.1.3.1.2.2 緊急：システム障害

4.1.3.1.2.3 事前予防対策

4.1.3.1.2.4 対策全般（啓発関連）

4.1.3.1.2.5 生活安全関連

4.1.3.1.2.5.1 法律違反の可能性がある場合は警視庁に

4.1.3.1.2.5.1.1 あらかじめ、事象と適用法規条文をマニュアル化しておく

4.1.3.1.2.6 セキュリティ関連外

4.1.3.1.2.7 ガイドブック送付依頼

4.1.3.1.3 具体的な対応策は即答せず、一旦電話を保留。二次対応担当での調査に時間が掛かりそうな場合は、再度かけ直しをお願いする

4.1.3.2 二次対応担当は、回答案の作成

4.1.3.2.1 状況把握

4.1.3.2.2 具体的な対応策検討

4.1.3.2.2.1 FAQ、ガイドブック、事前調査資料、最新ウェブ情報に基づいて検討

4.1.3.2.2.2 法律に違反する可能性がある場合は、警視庁に問い合わせ

4.1.3.2.2.3 必要に応じて IPA に問い合わせ

4.1.3.2.2.4 可能であれば、TCYSS メンバーに確認

4.1.3.2.3 回答案

4.1.3.2.3.1 基本は具体的な対応策を提示できる専門機関へナビゲート

4.1.3.2.3.1.1 対策の概念、簡易な処置を列挙

4.1.3.2.3.2 「相談・届出先クイックリスト」を参考に具体的に相談を受けてくれそうな機関を列挙

4.1.3.3 二次対応担当は相談者に回答

4.1.3.3.1 ①具体的な解決策

4.1.3.3.2 ②相談を受けてくれそうな機関を紹介

4.1.3.4 相談内容記録

4.1.4 WEB フォームでの相談受付、メールでの回答

4.1.4.1 WEB フォームに申請があった時の通知メールの確認

4.1.4.2 （※今後 HP 内に受理フォームを検討）

4.1.4.3 以下の手順は、電話相談に準ずる

4.1.5 窓口対応

4.1.5.1 ガイドブックに記載の内容をベースに詳細な解説が求められた場合

4.1.5.2 相談対応者、書記役の 2 名で対応

4.2 **2** （2）サイバーセキュリティに関する中小企業支援施策の実施に関する業務（※普及啓発セミナーの運営、事例集作成等）

4.2.1 （中小企業の経営者、システム管理者が知っておくべき情報を厳選して発信）

4.2.2 **3** 啓発資料の作成及び普及啓発活動の実施【知識・情報の発信】

4.2.2.1 **4** ポータルサイト新規ページ仕様

4.2.2.1.1 セキュリティの部屋

4.2.2.1.1.1 トップページ

4.2.2.1.1.1.1 お知らせ

4.2.2.1.1.1.2 更新情報

4.2.2.1.1.2 ガイドブック特設ページ

4.2.2.1.1.2.1 初版内容＋追補情報

4.2.2.1.1.2.2 HTML 版

4.2.2.1.1.2.2.1 トピック毎 100 ページ程度

4.2.2.1.1.2.3 PDF 版

4.2.2.1.1.2.3.1 現行 1+6 文書

4.2.2.1.1.2.4 EPUB 版

4.2.2.1.1.2.4.1 機械的に変換したリフロー版ミッション毎 6 文書

4.2.2.1.1.3 脆弱性・ウイルス情報

4.2.2.1.1.3.1 ○日々のニュースウォッチ情報

4.2.2.1.1.3.2 ⇒TWITTER でも発信

4.2.2.1.1.4 東京都の取組

4.2.2.1.1.4.1 サイバーセキュリティに関連する取組

4.2.2.1.1.5 サイバーセキュリティ対策情報の書棚 【書庫】 【知識
庫】 【ナレッジベース】 【アーカイブ】

4.2.2.1.1.5.1 関係機関提供の参考文献、WEB ページの内容要約及び
情報入手先へのリンク

4.2.2.1.1.5.1.1 【参照】IPA ここからセキュリティ_中小企業向け
ページ

ドキュメントを参照: company.html

4.2.2.1.1.5.2 個別調査分析資料

4.2.2.1.1.5.2.1 政策・制度、サイバーセキュリティ、次世代 IT

4.2.2.1.1.5.2.2 ○文献内容要約（サイバーセキュリティ関連）

4.2.2.1.1.5.2.3 ○情報処理基本フレーム

4.2.2.1.1.5.2.4 ○IT 関連基本フレームワーク

4.2.2.1.1.5.2.5 ○セキュリティ関連基本フレームワーク

4.2.2.1.1.5.2.6 ○IT 関連

4.2.2.1.1.5.2.7 ○IT リテラシー関連書籍

4.2.2.1.1.5.2.8 ○IT 技術関連

4.2.2.1.1.5.2.9 ○次世代技術トレンド関連書籍

4.2.2.1.1.5.2.10 ○サイバーセキュリティ関連

4.2.2.1.1.5.2.11 ○守るべき知的財産関連

4.2.2.1.1.5.3 （次世代技術の実践結果報告）

4.2.2.1.1.5.3.1 ○ディープラーニング、ロボット、ビッグデータ、
IOT、クラウドサービス等,...

4.2.2.1.1.5.3.2 ○日々の自習、セミナーを通じて取得した知見の報
告書

4.2.2.1.1.5.4 出張相談等でのプレゼン用資料

4.2.2.1.1.5.4.1 【例】ガイドブック内容詳細解説

4.2.2.1.1.5.4.2 【例】SOCIETY5.0 時代に必要なセキュリティ対策

4.2.2.1.1.5.4.3 【例】EC サイトの構築・運営におけるセキュリティ対策

4.2.2.1.1.5.4.4 【例】BCP におけるセキュリティ対策

4.2.2.1.2 作業内容及び質レベル

4.2.2.1.2.1 各ページの要件

4.2.2.1.2.1.1 中項目毎にデザインされたテンプレートを用意する

4.2.2.1.2.1.2 新規ページ発信のフローと担当

4.2.2.1.2.1.2.1 情報収集：職員

4.2.2.1.2.1.2.2 テンプレートを使って原案作成：職員

4.2.2.1.2.1.2.3 CMS ステージングページにアップ：職員？業者？

4.2.2.1.2.1.2.4 コピーライト（編集）：業者？

4.2.2.1.2.1.2.5 校閲：職員

4.2.2.1.2.1.2.6 承認：責任者

4.2.2.1.2.1.2.7 CMS 公開手続き：業者？

4.2.2.1.2.2 作業条件？

4.2.2.1.2.2.1 HTML,CSS,JAVASCRIPT

4.2.2.1.2.2.2 東京都職員が追加・更新・削除

4.2.2.1.2.3 対応ブラウザ？

4.2.2.1.2.3.1 CHROME, EDGE, SAFARI

4.2.2.1.2.3.2 フルスクリーン PC, タブレット, スマホ毎に最適化表示

4.2.2.2 「中小企業向けサイバーセキュリティ対策の極意」の追補情報の発信

4.2.2.2.1 ポータルサイトで「中小企業向けサイバーセキュリティ対策の極意」の追補情報、解説情報の発信

4.2.2.2.1.1 内容は、（３）の資料作成の項を参照

参照: [「中小企業向けサイバーセキュリティ対策の極意」の改訂（追補資料の作成）](#)

4.2.2.2.2 「中小企業向けサイバーセキュリティ対策の極意の解説書及び内容の改訂」で収集・蓄積した情報をもとに、デザイン、編集、コピーライト業務を外部に委託する。

4.2.2.2.3 2020 年度、「中小企業向けサイバーセキュリティ対策の極意」の改訂版を電子書籍で発行、予算が付けば、冊子体も発行

4.2.2.3 中小企業向けサイバーセキュリティ対策情報の発信【体系的な情報アーカイブ】

4.2.2.3.1 ポータルサイト内「サイバーセキュリティ対策情報の書棚」「ナレッジデータベース」「アーカイブ」

4.2.2.3.2 IT・サイバーセキュリティ関連の情報を体系的に整理して発信（専門員ハンドブックをベースに）

参照: [中小企業向けサイバーセキュリティ対策のハンドブック【対策情報の書庫】【ナレッジデータベース】の維持・更新](#)

4.2.2.3.3 第 0 編 目次

4.2.2.3.3.1 業務の成果を目次案に沿って整理し年次の成果物とする

4.2.2.3.4 第 1 編 はじめに

4.2.2.3.5 SUBTOPIC

4.2.2.3.5.1 第 2 編 相談対応マニュアル（相談対応時参照用）

【専門員用非公開】

4.2.2.3.5.1.1 ○個別ケース別相談対応手順

4.2.2.3.5.1.2 ○汎用対応手順

4.2.2.3.6 第 3 編 個別調査分析資料（知見の蓄積）

4.2.2.3.6.1 （関係機関提供の参考文献、WEB ページのリスト及び内容要約）

4.2.2.3.6.2 ○文献内容要約（サイバーセキュリティ関連）

4.2.2.3.6.3 ○情報処理基本フレーム

4.2.2.3.6.4 ○IT 関連基本フレームワーク

4.2.2.3.6.5 ○セキュリティ関連基本フレームワーク

4.2.2.3.6.6 ○IT 関連

4.2.2.3.6.7 ○IT リテラシー関連書籍

4.2.2.3.6.8 ○IT 技術関連

4.2.2.3.6.9 ○次世代技術トレンド関連書籍

4.2.2.3.6.10 ○サイバーセキュリティ関連

4.2.2.3.6.11 ○守るべき知的財産関連

4.2.2.3.6.12 ○日々のニュースウォッチ情報

4.2.2.3.6.13 ○日々の自習、セミナーを通じて取得した知見の報告書

4.2.2.3.7 第4編 次世代技術の実践習得

4.2.2.3.7.1 ○ディープラーニング、ロボット、ビッグデータ、IOT、クラウドサービス等、…

4.2.2.3.8 第5編 実践的なノウハウ・知識の提供用資料（知見の発信）

4.2.2.3.8.1 ○サイバーセキュリティ対策説明資料（プレゼン資料）

4.2.2.3.8.2 ○公開用成果物

4.2.2.3.9 付録

4.2.2.3.9.1 ○サイバーセキュリティ関連文献全文検索ツールおよびデータ

4.2.2.3.9.2

4.2.2.4 **4** 中小企業に伝えたいホットな情報発信

4.2.2.4.1 ⇒TWITTERで発信

4.2.2.4.2 ポータルサイトのトピックスで発信

4.2.2.5 **4** プレゼン用マスタースライド及び解説文を事前作成及び改訂

4.2.2.5.1 【例】ガイドブック内容詳細解説

4.2.2.5.2 【例】SOCIETY5.0時代に必要なセキュリティ対策

4.2.2.5.3 【例】ECサイトの構築・運営におけるセキュリティ対策

4.2.2.5.4 【例】BCPにおけるセキュリティ対策

4.2.3 **3** 出張相談・個別助言

4.2.3.1 ⇒各種セミナーで相談受付だけでなく、プレゼンの時間も確保

4.2.3.2 都支援事業等でのプレゼンテーションおよび個別相談対応

4.2.3.3 ガイドブックを読了後、より詳細な解説及び助言を求める組織向け

4.2.3.4 警視庁が行うセミナーとは棲み分け

4.2.4 **3** 関係機関との連携

4.2.4.1 **4** サイバーセキュリティ基本法に基づいた「サイバーセキュリティ協議会」への参画

4.2.4.1.1 第一類、第二類、一般構成員のどのレベルか

4.2.4.2 **4** NISC、IPA との情報交換及び連携

4.2.4.2.1 インターネットでは公開されていないセキュリティ関連情報の共有

4.2.4.2.2 IPA セキュリティセンターとのホットライン

4.2.4.3 **4** 警視庁、TCYSS メンバーとの情報交換及び連携

4.2.4.3.1 YAMMER に代わる情報共有ツールの利用促進

4.2.5 **3** FAQ の作成・更新

4.2.5.1 方針

4.2.5.1.1 過去の相談記録、ガイドブック、事前調査資料等に基づいて、内容を分類して汎化した Q&A を作成し、相談用手元資料とする
【相談回答の均質化】

4.2.5.1.2 Q&A 項目：分類（キーワード）、質問例、回答例（対応策、ナビゲーション先）、参考にした情報、質問者に参考になる情報の所在場所

4.2.5.2 FAQ 分類【別シートで更新】



4.2.5.2.1 FAQ 分類（ガイドブック項立てに沿った分類）


4.2.5.2.2 FAQ 分類（「ここからセキュリティ」を参照）

ドキュメントを参照: company.html

4.3 (3) 課長級、課長代理級からの指示に基づく各種資料作成業務

4.3.1 【情報収集・整理・蓄積】【予測調査】（専門員としてのスキル、知識の習得と蓄積）

4.3.2   「中小企業向けサイバーセキュリティ対策の極意」の改訂（追補資料の作成）

4.3.2.1  SEC01-01-01_「中小企業向けサイバーセキュリティ対策の極意」の改訂（追補資料の作成）へ移行

ドキュメントを参照: Sec01-01-01_「中小企業向けサイバーセキュリティ対策の極意」の改訂（追補資料の作成）.html

4.3.2.2 （2019 年 7 月 25 日）

4.3.2.3（「中小企業向けサイバーセキュリティ対策の極意」で改訂もしくは追記すべき内容の調査と原稿作成）

4.3.3 **3** 「中小企業向けサイバーセキュリティ対策の極意」の内容の詳細化（解説資料の作成）

4.3.3.1 SEC01-01「中小企業向けサイバーセキュリティ対策の極意」解説書を参照

ドキュメントを参照: [Sec01-01「中小企業向けサイバーセキュリティ対策の極意」解説書.html](#)

4.3.4 **3** 中小企業向けサイバーセキュリティ対策のハンドブック【対策情報の書庫】【ナレッジデータベース】の維持・更新

4.3.4.1 ポータルサイト内「サイバーセキュリティ対策情報の書棚」「ナレッジデータベース」「アーカイブ」

4.3.4.2 **4** 概要

4.3.4.2.1 **5** 各機関が提供している情報のポイントを、事前調査資料として作成及び改訂

4.3.4.2.1.1 「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」（SEC01-02）を参照


4.3.4.2.2 **5** 日々のセキュリティ関連の文献、WEB サイト情報の収集（ブックマーク）、内容要約作成及び蓄積

4.3.4.2.2.1 詳細は、「サイバーセキュリティ担当による情報収集・整理・蓄積・提供」（SEC01-06）を参照

4.3.4.2.3 詳細は、SEC01-08-5【成果物】専門員業務ハンドブック【目次】

ドキュメントを参照: [Sec01-08-5【成果物】専門員業務ハンドブック【目次】.html](#)

4.3.4.3 **4** 第1編 はじめに

4.3.4.4 **4**  第2編 相談対応マニュアル（相談対応時参照用）【専門員用】【非公開】

4.3.4.4.1 案件別対応手順【専門員用】

4.3.4.4.2 インシデント対応フロー及び解説【相談者向け】

4.3.4.5 **4** 第3編 個別調査分析資料（知見の蓄積）

4.3.4.5.1 日々収集したセキュリティ関連の文献、WEBサイト情報の所在場所、内容要約作成及び蓄積

4.3.4.5.2 **3** 関係機関が発行した次世代IT技術及びサイバーセキュリティに関する実践的なノウハウ・知識の文献情報

4.3.4.5.2.1 次世代IT技術及びサイバーセキュリティに関して体系的なノウハウ・知識を、自習、セミナーを通じて取得

4.3.4.5.3 収集方法

4.3.4.5.3.1 **4** 独学・自習

4.3.4.5.3.1.1 情報処理技術者試験レベルの知識の習得

4.3.4.5.3.1.1.1 IT ストラテジスト試験

4.3.4.5.3.1.1.2 情報処理安全確保支援士試験

4.3.4.5.3.1.1.3 応用情報技術者試験

4.3.4.5.3.1.1.4 情報セキュリティマネジメント試験

4.3.4.5.3.1.2 システム開発・運用の新技術等の習得

4.3.4.5.3.1.2.1 プログラミング言語

4.3.4.5.3.1.2.1.1 PYTHON

4.3.4.5.3.1.2.1.2 JAVA

4.3.4.5.3.1.2.2 各種機械学習モジュールの API 利用

4.3.4.5.3.1.2.3 . . .

4.3.4.5.3.1.3 WEB サービス試用

4.3.4.5.3.1.3.1 相談者の実利用環境の把握

4.3.4.5.3.1.3.2 関連機関のサービスの把握

4.3.4.5.3.2 セミナー等での情報収集

4.3.4.5.3.2.1 サイバーセキュリティセミナー

4.3.4.5.3.2.2 次世代 IT 技術セミナー

4.3.4.5.3.2.3 新技術・新製品紹介展示会

4.3.4.5.3.3 関係機関との情報交換

4.3.4.5.3.3.1 セキュリティ関連機関と定期的に情報交流の場を設ける

4.3.4.5.3.3.1.1 NISC,経産省,総務省等との情報交換

4.3.4.5.3.3.1.2 警視庁、IPA、TCYSS メンバーとの情報交換

4.3.4.5.3.3.2 ユーザ側である中小企業支援団体との事例等の学習の機会を設ける

4.3.4.5.4 収集内容

4.3.4.5.4.1 1.1.3. セキュリティ関連機関のドキュメントのキャッチアップ

4.3.4.5.4.1.1 CISC, METI, IPA

4.3.4.5.4.1.2 NIST SP シリーズ

4.3.4.5.4.1.3 JPCERT, USCERT

4.3.4.5.4.2 1.1.4. サイバー・フィジカル・システムの開発・運用等の新技術等の調査報告書

4.3.4.5.4.2.1 言語

4.3.4.5.4.2.2 PYTHON、JAVA

4.3.4.5.4.2.3 WEB サービス、ツールの試用

4.3.4.5.4.2.4 相談者の実利用環境の把握

4.3.4.5.4.2.5 関連機関のサービスの把握

4.3.4.5.4.2.6 AI システム稼働環境

4.3.4.5.4.2.7 セミナー、イベント参加での情報収集

4.3.4.5.4.2.8 サイバーセキュリティセミナー

4.3.4.5.4.2.9 次世代 IT 関連セミナー

4.3.4.5.4.3 ○情報処理基本フレーム

4.3.4.5.4.3.1 ○第 4 次産業革命

4.3.4.5.4.3.2 ※DX レポート（IT システム 2025 年の崖の克服）

4.3.4.5.4.3.3 ※科学技術イノベーション統合戦略（内閣府）

4.3.4.5.4.3.4 ※SOCIETY5.0

4.3.4.5.4.3.5 ※CONNECTED INDUSTRY

4.3.4.5.4.3.6 ※AI 白書 2019

4.3.4.5.4.3.7 技術動向、利用動向、制度政策動向、社会実装課題と
対策

4.3.4.5.4.3.8 ※データサイエンス領域のスキル標準「ITSS+」

4.3.4.5.4.3.9 ※アジャイル開発のスキル標準「ITSS+」

4.3.4.5.4.3.10 ※セキュリティ領域のスキル標準「ITSS+」

4.3.4.5.4.4 ○人材育成

4.3.4.5.4.4.1 ※IT 人材白書

4.3.4.5.4.4.2 ※I コンピテンシ・ディクショナリ

4.3.4.5.4.4.3 タスクディクショナリ、スキルディクショナリ、知識
ディクショナリ

4.3.4.5.4.4.4 ※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

4.3.4.5.4.4.5 ※情報処理技術者試験（基礎、応用、情報セキュリティ
マネジメント、情報処理安全確保支援士）のシラバス

4.3.4.5.4.5 ○情報処理実践技術

4.3.4.5.4.5.1 ※パブリッククラウド環境、プライベート仮想環境

4.3.4.5.4.5.2 ※DEVOPS による迅速なソフトウェア開発

4.3.4.5.4.6 ○セキュリティ関連基本フレームワーク

4.3.4.5.4.6.1 「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」（NIST SP 800-37）に沿った記述内容の加筆訂正

ドキュメントを参照: [000025329.pdf](#)

4.3.4.5.4.6.2 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](#)

4.3.4.5.4.6.2.1 CSF フレームワークコア

4.3.4.5.4.6.2.1.1 ID 特定

4.3.4.5.4.6.2.1.2 PR 防御

4.3.4.5.4.6.2.1.3 DE 検知

4.3.4.5.4.6.2.1.4 RS 対応

4.3.4.5.4.6.2.1.5 RC 復旧

4.3.4.5.4.6.3 NIST SP 800-63（電子的認証に関するガイドライン）に対応した認証方式の適用について加筆

4.3.4.5.4.6.3.1 「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る

4.3.4.5.4.6.3.2 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

4.3.4.5.4.6.4 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)

4.3.4.5.4.6.5 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)

4.3.4.5.4.6.6 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)

4.3.4.5.4.6.7 NIST SP.800-82R2 GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY

4.3.4.5.4.6.8 ※NIST 500-37 R2.0 (リスクマネジメント) + NIST 800-53 VER.4.0 (管理策)

4.3.4.5.4.6.9 ※ISO27001 (情報セキュリティマネジメント)

4.3.4.5.4.6.10 ※NIST CSF (サイバーセキュリティフレームワーク)

4.3.4.5.4.6.11 ※NIST SP 800-61(インシデント対応)

4.3.4.5.4.6.12 ※NIST SP 800-63 (電子的認証に関するガイドライン)

4.3.4.5.4.6.13 ※IEC62443-2-1(CSMS 制御システムにおけるセキュリティマネジメントシステムの構築に向けて)

4.3.4.5.4.7 ○セキュリティ関連実践情報

4.3.4.5.4.7.1 ※サイバーセキュリティ基本法、サイバーセキュリティ戦略 (NISC)

4.3.4.5.4.7.2 ※「サイバーセキュリティ経営ガイドライン、中小企業の情報セキュリティガイドライン第3版 (METI、IPA)

4.3.4.5.4.7.3 ※サイバー・フィジカルセキュリティ対策フレームワーク（METI）

4.3.4.5.4.7.4 ※サプライチェーン

4.3.4.5.4.7.5 ※DEVSECOPS(セキュアなソフトウェア開発ライフサイクル)

4.3.4.6 **4** 第4編次世代技術の実践習得

4.3.4.6.1 先進技術の実践によるノウハウ習得

4.3.4.7 **4** 第5編 実践的なノウハウ・知識の提供用資料（発信情報の作成）

4.3.4.8 **4** 付録

4.4 **2** （4） その他付随する業務

4.4.1 会議等設営準備

4.4.2 係内庶務

5 別添資料

5.1 SEC01-08-5【成果物】専門員業務ハンドブック【目次】

ドキュメントを参照: [Sec01-08-5【成果物】専門員業務ハンドブック【目次】.html](#)

5.2 SEC01-01「中小企業向けサイバーセキュリティ対策の極意」解説書

ドキュメントを参照: [Sec01-01「中小企業向けサイバーセキュリティ対策の極意」解説書.html](#)

