

☐ Sec01-08-2 専門員の所掌業務及び調査分析項目

☐ 改版履歴

- 【2019年6月21日】極意の校正予定箇所の提示
- 【2019年6月13日】2019年実施項目【案】、項目表の併合
- 【2018年10月24日】所掌業務内容の明確化
- 【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
- 【2018年6月6日】係会議資料として提出

☐ ① 専門員の所掌業務及び行動規範の概要

- ☑ ② 所掌事務
- ☑ ② 基本姿勢
- ☑ ② 専門員としての行動規範
- ☑ ② 所掌分担の明示の目的

☐ ① 専門員の所掌業務の詳細内容

- ☑ 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
- ☑ 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）
- ☑ ② (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】 【予測調査】（専門員としてのスキル、知識の習得と蓄積）
- ☑ 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）
 - 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 [🔗](#)
- ☑ ③ 😊 「中小企業向けサイバーセキュリティ対策の極意」の内容の最新化（追補資料の作成）
 - （「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 「サイバーセキュリティ経営ガイドライン2.0対応」
- ☑ ⑤ 「サイバーセキュリティ経営ガイドライン」Ver2.0の重要10項目の分類及び内容の改訂に伴う記述の加筆訂正
 - 🖱️ 改訂箇所：Mission3-10 (p.98～109)を改訂

☐ ガイドライン改訂前の主な課題

- 昨今のサイバー攻撃の巧妙化により入口出口対策などの事前対策だけでは対処が困難。
- 米国のサイバーセキュリティフレームワークでも事前対策だけでなく、事後（検知、対応、復旧）対策を要求。
- 一方で従来のガイドラインはCSIRTの構築などの「対応」に関する項目はあるものの、「検知」や「復旧」に関する内容が弱く、国際的な状況を踏まえるとガイドラインとの整合性が不十分。

☐ ポイント（経産省発表） [🔗](#)

☐ 重要10項目の整理

- 新規に2項目（(5)対策実施と(8)復旧）追加するとともに、既存の項目を再整理。
- 重要10項目の並びについても、3原則、及び作業の時系列を意識して再整理。
- (7)の参考資料として付録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」を新規に追加。

☐ 事後対策の強化 ～検知・復旧対策の実施～

- 重要項目 指示5として「攻撃の検知」に関する、「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」を追加
- 重要項目 指示8として「復旧」に関する、「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」を追加

☐ サプライチェーン対策の強化


- 重要項目 指示9の「サプライチェーンのビジネスパートナーや委託先等を含めたサイバーセキュリティ対策の実施及び状況把握」において、委託先におけるリスクマネーの確保や委託先の組織としての活用の把握（ISMSやSECURITY ACTION）等の留意点を追記
- セキュリティ要件を満たさない事業者、製品、サービスはグローバルサプライチェーン、国内サプライチェーンからはじき出されるおそれ

☐ 事後対策の強化 ～インシデント発生時の対応～

- インシデント発生時に組織として調査しておくべき事項をまとめた付録Cを追加

☐ <情報共有活動における情報提供の記載を強調>

- 重要10項目の（10）において、従来は「情報の入手とその有効活用」となっていた部分を「情報の有効活用」に修正。
- ⑤ その他の改訂ポイント
 - <NISTのサイバーセキュリティフレームワークとの対応関係の提示>
 - 改訂箇所：Information6-7(p.183以降)として追加
 - 付録Aの各チェック項目について、NISTのサイバーセキュリティフレームワークと対応する項目を提示。
 - <冒頭の説明の見直し>
 - 改訂箇所：「はじめに」(p.8～9)を改訂
 - 「サイバーセキュリティ経営ガイドライン・概要」の説明を全体的に修正。
 - IoTやAIの活用といった最近の情勢をふまえるとともに、サプライチェーンセキュリティの必要性が高まっていることや、セキュリティ対策を怠ると他社に迷惑をかけることもある等についても言及。
 - <統計データのアップデート>
 - 改訂箇所：「はじめに」,Mission1-13(p.8～9,42～43)を改訂
 - 1. 1節「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」で参照している統計データをアップデート。それに伴い説明文も修正。
 - <その他>
 - 経営者、CISOを対象読者としていることから、冗長な表現を見直し、全体の記載を簡素化。
 - 改訂箇所：改訂部分は同時に表現も見直す
- ⑥ 「サイバーセキュリティ経営ガイドライン」Ver2.0 付録A サイバーセキュリティ経営チェックシートの内容の反映
 - 改訂箇所：Information6-7(p.183以降)として追加
 - 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されている
- ④ 中小企業の情報セキュリティ対策ガイドライン第3版対応
 - リスク分析の位置付けの変更
 - 改訂箇所：Mission3-17～20, Information6-6 (P.124～131,180～183)を改訂
- ④ サイバーセキュリティ脅威のトレンド対応
 - ⑤ なりすましECサイトの被害と回避策の記述の充実
 - 改訂箇所：Mission1-12 (P.41)のあとに追加
 - 事業者サイド
 - 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【2018年5月IPA】
 - 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アーインターネット協会】
 - 利用者サイド
- ⑥ ビジネスメール詐欺の被害と回避策の記述の充実
 - 改訂箇所：Mission1-12 (P.41)のあとに追加
- IoT機器調査及び利用者への注意喚起プロジェクト（NOTICE対応）
 - 改訂箇所：Information6-8(p.183以降)として追加
- ④ IT最新トレンド対応
 - 改訂箇所：Mission3-11,コラム(p.110～131)を改訂、必要に応じて追加
- ⑤ Society5.0時代に必要なセキュリティ対策
 - 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の技術の活用の必要性和、活用におけるセキュリティ対策の記述の充実
- IoT関連
 - NIST SP.800-82R2 Guide to Industrial Control Systems (ICS) Security 【再掲】
 - 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】
 - 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】
- クラウドセキュリティ
 - クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年度版【METI】
 - 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（第2版）2018年7月【総務省】
- APIセキュリティ
- ブロックチェーンにおけるセキュリティ
- インターネットアクセスにおけるセキュリティの新技術

- ☐ IDと認証セキュリティ
 - 利便性とセキュリティの両立へ向けた新たな動向
- ☐ FIDO(Fast Identity Online)
- 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
- ☐ モバイル認証 (GSMA Mobile Connect)
 - 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
- ☐ 認証セキュリティとNIST SP 800-63の改定
 - 「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
- ☐ ⑤ 個別対策
 - ※システム管理者としての基本技術の解説（安全・安心ハンドブック（NISC）参照）
 - ※クレジットカード PCI/DSS（Payment Card Industry Data Security Standard）
 - ※ブロックチェーン技術の応用
 - ※Wifiセキュリティ
 - ※ランサムウェア
- ☐ ⑤ サイバーセキュリティ分野で機械学習が活用される背景と期待
 - ☐ サイバーセキュリティ分野で機械学習が活用される背景
 - 従来型サイバーセキュリティ対策の限界
 - ☐ 機械学習への期待
 - マルウェア検知への応用
 - ネットワーク異常検知への応用
 - ソースコードレビューへの応用
 - セキュリティ監視の運用支援への応用
 - ☐ 機械学習を活用する上で押さえるべきポイント
 - 誤検知の可能性が避けられない
 - 判定結果の分析が困難である
 - 全てに万能な機械学習アルゴリズムは存在しない
- ☐ ④ 働き方改革関連
 - 🚩 改訂箇所：Mission3-11,コラム(p.110～131)に追加
- ☐ ⑤ 生産性向上のための「デジタル・ワークプレイス」
 - デジタル化時代のデバイスやテクノロジーを駆使して、働くプロセスや場所・コミュニケーション、コラボレーションのあり方を新たに組み立てようとする考え方
- ☐ ⑥ 従業員エクスペリエンスを向上するシステムの連携
 - 従業員にとって、いつでもどこでも柔軟な働き方ができるインフラやアプリケーションが一貫して提供されることで、仕事をする上での利便性やユーザビリティが向上する
- ☐ テレワークソリューション
 - 【担当：伊藤】
- ☐ 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】
 - ☐ システム方式
 - リモートデスクトップ
 - 仮想デスクトップ
 - クラウド型アプリ
 - 会社PC持ち帰り
 - ☐ 端末デバイス
 - リッチクライアント
 - シンククライアント
 - タブレット型PC
 - スマートフォン
 - 携帯電話

- セキュリティ
 - 本人認証
 - 端末認証
 - 端末管理
 - 暗号化通信
 - ストレージ暗号化
 - 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】
 - 私用端末のビジネス利用
 - 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】 
- ⑤ **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」**
 - AIが従業員の能力を補い、人間が気づかない部分をコンピュータがアシストすることが可能になりつつある
- ④ **IT関連投資**
 - ⑤ **守りのIT投資**
 -  **改訂箇所：Mission3-8(p.94～95)を改訂**
 - （デジタル・ワークプレイス）
 - 事業継続計画（BCP）の一環としてのサイバーセキュリティ対策（明文化）
 - 【担当：伊藤】
 -  **改訂箇所：Mission4-1(p.134～144)を改訂**
 - 法律違反の可能性への対応方法の解説
 - 【担当：小林】
 -  **改訂箇所：Information6-4(p.172～173)の改訂**
 - GDPR対応
 - 個人情報保護法改正への対応
 - 
 - ⑤ **攻めのIT投資**
 -  **改訂箇所：Mission3-11,コラム(p.110～131)に追加**
 - AIが人を支援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
 - 【担当：中山】
 - Society5.0, Connected Industry, DX, CPS対応
 - ○第4次産業革命
 - ※**DXレポート（ITシステム2025年の崖の克服）**
 - ※科学技術イノベーション統合戦略（内閣府）
 - ※Society5.0
 - ※Connected Industry
 - ※AI白書2019
 - IoT、ビッグデータ、機械学習、クラウドサービス等の活用におけるサイバーセキュリティ対策
 - 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
 - 【担当：早出】
 - 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
 - サプライチェーン全体での対策（中小企業向け）
 - 対応計画（BCP対応）
 - 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Revision2対応
 - 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
 - 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
 - ④ **制度・施策**
 -  **改訂箇所：Information6-7(p.185～)に追加**
 - 情報セキュリティサービス審査登録制度及びシステム監査基準（2018年改訂）【METI/IPA】 
 - 情報セキュリティ監査サービス
 - 脆弱性診断サービス

- デジタルフォレンジックサービス
- セキュリティ監視・運用サービス

☐ 中小企業のサイバーセキュリティ対策支援体制のモデル構築（サイバーセキュリティお助け隊）（2019年～）【METI/IPA】

☐ 2019年度

- 宮城県・岩手県・福島県
- 新潟県
- 長野県・群馬県・栃木県・茨城県
- 神奈川県
- 石川県
- 愛知県
- 大阪府・京都府・兵庫県
- 広島県

☐ 【参考】サイバーインシデント緊急対応企業一覧【JNSA】

- インシデント緊急対応費用

④ 関連法規

- 【担当：小林】
- 改訂箇所：Information6-4(p.172～173)の改訂
- セキュリティ事象に関連する法規の内容要約、事象毎に適用の可能性のある法律名、条文を整理する
- ガイドブックのMission1-1～13を例に適用が想定される法律名、条文を例示
- 不正競争防止法、個人情報保護法、

☐ GDPR対応

- GDPR（General Data Protection Regulation：一般データ保護規則）に対応した個人情報保護策について記述

③ 専門員用業務ハンドブックの維持・更新【ナレッジデータベース】

- 全員

② (4) その他付随する業務

☐ 別添資料

☐ ① TCYSSでの情報収集・整理・蓄積と発信

