Sec01-08-2 専門員の所掌業務及び調査分析項目

1. ****

専門員の所掌業務及び行動規範の概要

* 1. ****

**所掌事務**

* + 1. **（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】**
    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）⇒【情報発信】**
    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】**
    4. **（４） その他付随する業務**
  1. ****

**求められる能力（専門員公募要項より）**

* + 1. 情報セキュリティマネジメント試験（あるいは同等以上）合格者、または同等以上の能力を有するもの
       - 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
       - 「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
    2. 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
       - 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. 職務を遂行する意欲を有している
       - 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
  1. ****

**基本姿勢**

* + 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
    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. 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

1. 専門員の所掌業務の詳細内容
   1. **（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**
      1. 方針
         * 一次対応は、 日常のルーティンワーク（定型業務）
         * 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。
      2. **電話**
         * 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
           + 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
         * 二次対応担当は、 回答案の作成
           + 回答案

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

「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リストアップしておく

* + - * 二次対応担当は相談者に回答
        + ①具体的な解決策
        + ②相談を受けてくれそうな機関を紹介
      * 相談内容記録
    1. **Webフォームでの相談受付、 メールでの回答**
       - Webフォームに申請があった時の通知メールの確認
       - （※今後HP内に受理フォームを検討）
       - 以下の手順は、 電話相談に準ずる
    2. **窓口対応**
       - 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
       - 相談対応者、 書記役の2名で対応
  1. **（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）**
     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）
     2. **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】**
        + **ポータルサイトからの情報発信**
        + ****

**「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**

* + - * + 「中小企業向けサイバーセキュリティ対策の極意」作成時の要約前の情報をベースに解説文として発信
      * ****

**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】**

* + - * + **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」**
        + 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）
        + 第0編　目次
        + 第1編　はじめに
        + 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】
        + 第3編　個別調査分析資料（知見の蓄積）

（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）

* + - * + 第4編次世代技術の実践習得

〇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,…

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

〇サイバーセキュリティ対策説明資料（プレゼン資料）

〇公開用成果物

* + - * + 付録
      * **中小企業に伝えたいホットな情報発信**
        + Twitterで発信
        + ポータルサイトのトピックスで発信
      * **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**
    1. **出張相談・個別助言**
       - ⇒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
       - **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**
       - **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**
       - 警視庁が行うセミナーとは棲み分け
    2. **関係機関との連携**
       - **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**
         * 第一類、 第二類、 一般構成員のどのレベルか
       - NISC、 IPAとの情報交換及び連携
         * 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
         * IPAセキュリティセンターとのホットライン
       - 警視庁、 TCYSSメンバーとの情報交換及び連携
         * Yammerに代わる情報共有ツールの利用促進【Teams,Zoom,等
    3. **FAQの作成・更新**

;

* 1. **（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**
     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）
     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）
    1. **「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. **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**
       - 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」
       - 概要
         * 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
         * **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**
       - 第1編　はじめに
       - ****

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】

* + - * + 案件別対応手順【専門員用】
        + インシデント対応フロー及び解説【相談者向け】
      * 第3編　個別調査分析資料（知見の蓄積）
        + 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
        + **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**

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

* + - * + 収集方法

独学・自習

情報処理技術者試験レベルの知識の習得

情報処理安全確保支援士試験

応用情報技術者試験

情報セキュリティマネジメント試験

システム開発・運用の新技術等の習得

プログラミング言語

各種機械学習モジュールのAPI利用

・・・

Webサービス試用

相談者の実利用環境の把握

関連機関のサービスの把握

セミナー等での情報収集

サイバーセキュリティセミナー

次世代IT技術セミナー

新技術・新製品紹介展示会

関係機関との情報交換

NISC,経産省,総務省等との情報交換

警視庁、 IPA、 TCYSSメンバーとの情報交換

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

* + - * + 収集内容

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

CISC, METI, IPA

NIST SPシリーズ

JPCERT, USCERT

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

言語

Python、 Java

Webサービス、 ツールの試用

相談者の実利用環境の把握

関連機関のサービスの把握

AIシステム稼働環境

セミナー、 イベント参加での情報収集

サイバーセキュリティセミナー

次世代IT関連セミナー

〇情報処理基本フレーム

〇第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2020

　技術動向、 利用動向、 制度政策動向、 社会実装課題と対策

※データサイエンス領域のスキル標準「ITSS+」

※アジャイル開発のスキル標準「ITSS+」

※セキュリティ領域のスキル標準「ITSS+」

〇人材育成

※IT人材白書

※iコンピテンシ・ディクショナリ

　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

※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

※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

〇情報処理実践技術

※パブリッククラウド環境、 プライベート仮想環境

※DevOpsによる迅速なソフトウェア開発

〇セキュリティ関連基本フレームワーク

「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

<https://www.ipa.go.jp/files/000025329.pdf>;

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】

<https://www.ipa.go.jp/files/000038957.pdf>;

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

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)

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)

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）

NIST SP.800-82R2　Guide to Industrial Control Systems (ICS) Security

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

※ISO27001（情報セキュリティマネジメント）

※NIST CSF（サイバーセキュリティフレームワーク）

※NIST SP 800-61(インシデント対応)

※NIST SP 800-63 (電子的認証に関するガイドライン)

※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)

〇セキュリティ関連実践情報

※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）

※「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）

※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）

※サプライチェーン

※DevSecOps(セキュアなソフトウェア開発ライフサイクル)

* 1. **（４） その他付随する業務**

1. TCYSSでの情報収集・整理・蓄積と発信
   1. Subtopic

