Sec01-08-2 専門員の所掌業務及び調査分析項目

# 改版履歴

## 【2021年12月16日】2022年度公募要項を反映して見直し

## 【2021年4月22日】「Sec01-08-2-2\_組織の位置づけと業務実施姿勢」追加

## 経過

### 【2021年4月13日】項立て大幅改訂

### 【2021年4月6日】新体制への対応準備

### 【2021年4月2日】打ち合わせ用詳細部分非表示設定

### 【2021年4月1日】URL更新

### 【2020年2月7日】長文折り返し設定

### 【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

### 【2019年10月9,24日】資料目次作成及びリンク

### 【2019年9月26日】専門員要件の追加

### 【2019年7月26日】ポータルサイトの追加仕様

### 【2019年7月25日】極意の校正予定箇所の提示(現行構成毎)

### 【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

# 資料目次

## Sec01-08-2-2\_組織の位置づけと業務実施姿勢

## Sec01-08-2-3\_専門員の所掌業務及び行動規範【骨子】

## Sec01-08-2-4\_専門員の所掌業務【要約】

## 別添資料

### Sec01-08-2-5\_専門員業務ハンドブック【要約】

### Sec01-08-2-6\_相談対応手順【要約】

### Sec01-08-2-6\_SNSおよびポータルからの更新情報の発信手順【要約】

## TCYSSでの情報収集・整理・蓄積と発信【概念図】

# 従来の問題点

## 専門員の職務内容は、発足前の想定のままであり、6年の間に業務の実態は変わっている

## 委託の問題点

### ガイドブック作成、サーバ運用等の外部委託コストが高い

### 委託ではきめ細かな情報発信が困難

### ノウハウが組織に蓄積しない

## 職員のスキル向上が望ましい

### Word,Excelが使えるレベルのITリテラシーでは、業務を遂行できない

### 専門員の採用に当たっては、経験、知識とITヒューマンスキルを重視すべきでは

## その他

### 相談の適切な対応のためには、障害状況等を事前に整理された形で確認でき、 情報を整理して回答できるメール、チャットのほうが効果的

### テレワーク時、職員と共通のSkype、Teamsビデオ会議、都庁メールを使えないことが、 円滑なコミュニケーションの阻害要因の一つになっていないか

# Sec01-08-2-2\_組織の位置づけと業務実施姿勢

## 商工部として中小企業の事業の発展を支援

### 経営支援課の中小企業の発展のための施策の１つとして、IT活用の推進があり、IT活用を阻害する要因の１つとしてセキュリティ対策を考える

## 中小企業支援の戦略

### 専門員は、中小企業において、「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ことを支援する。

#### ※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

#### ②守りのIT・セキュリティ対策

#### ①攻めのIT・セキュリティ対策

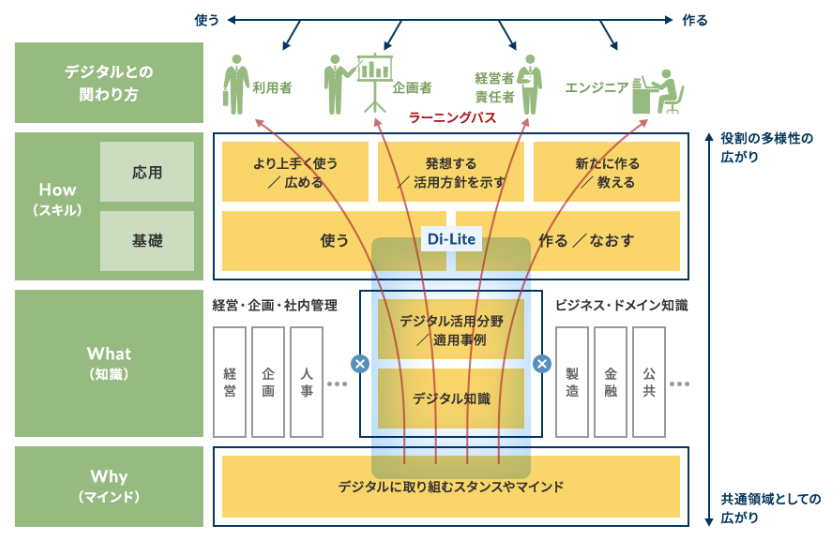
### 「デジタルリテラシー」習得の啓発、推進

#### 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」

#### 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

### 「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」

##### 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

###### 発送する/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

### 実施に当たって

#### 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

## 専門員の業務実施戦術

### 中小企業のセキュリティ対策を支援する組織として、「デジタルリテラシー・スキルフレームワーク」に沿って、中小企業を支援するための、体系的・網羅的な知識・スキルの保有に努める。

### 成果の見える化

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

#### 設定した目標の達成に向けて調査・分析した情報が、組織の共有知識として蓄積されるように、体系化して形式知化（ドキュメント化）する

### スキルの向上

#### 専門員としてのスキル、 知識の向上を図り、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）

### 情報の収集

#### 一般的な知識は浅くても広く

##### 最新のITおよびセキュリティ関連動向を、文献調査、セミナー等により見聞し、情報の所在、概要を収集する

#### 専門的な知識は深く

##### 見聞した情報では、実践的な知見が得られない最新の技術に関しては、試行・実践により、実践的な技能を収集する

### 情報の整理・知識化

#### 収集した知識を整理して、ドキュメント化し、組織の体系的・網羅的な知識として蓄積する

### 知識の発信

#### 集積した知識は、費用対効果を考慮して、効率的な手段で、効果の高い内容を優先的に発信する

# Sec01-08-2-3\_専門員の所掌業務及び行動規範【骨子】

## 公務員倫理とワーク・ライフ・インテグレーション

### 特定の組織、個人の利益、自らの利益の追求者であってはいけない

### 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・効果的に実施する

## 非常勤職員の制度イメージ（制度設計資料より）

### 会計年度任用職員は、専門的な知識経験に基づく職

### 非常勤職員は、経験とスキルに基づき補助的な業務に従事し、行政運営を補完する。

### 経験とスキルに基づいて、主体的かつ協調的に業務を遂行する意欲を有すること。

#### 主体的と協調的の両方の姿勢が必要

## 所掌事務

### （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 ※メールフォーム、電話、窓口、出張相談など ⇒【受付業務】

#### 相談受付

#### 対応策検討

#### 回答案作成

#### 回答

### （２）サイバーセキュリティ対策の普及啓発の実施に関する業務 ※普及啓発用の資料の作成及びWeb等での発信 ⇒【情報発信】

#### 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】

##### 相談内容FAQ、情報収集・整理・蓄積した内容から発信情報作成・更新

##### ⇒ガイドブックEPUB、ポータルサイトに反映

#### 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

#### 関係機関との連携

##### 【新規】IPA及び他の相談対応窓口との実務連携

##### 【活動なし】TCYSSメンバーとの情報交換及び連携

### （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】

#### 情報の知識化（情報収集・整理・蓄積、予測調査）

##### （専門員としてのスキル維持、知識の習得と蓄積）

#### 知識化された情報から要約資料、解説資料作成

##### ⇒ガイドブックEPUB、ポータルサイト用原稿作成

##### EPUBドキュメント（xhtml化）、ポータルサイト（html化）

#### 知識化された情報から「知識の保管庫（ナレッジベース）」の作成

##### 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・知識の集約

##### 専門員の暗黙知を形式知化 （相談対応等の質の均質化）

### （４）その他、課長級、課長代理級からの指示に基づく付随する業務 ※「中小企業のサイバーセキュリティ対策関連事業」の企画・実施に関連する情報収集・整理を含む。

#### 「中小企業のサイバーセキュリティ対策関連事業」の成果の知識化と、普及啓発用資料の発信

## 求められる能力（専門員公募要項より）

### （１）ITシステム・ネットワークシステムの構築・運用、セキュリティ対策の指導等の実務経 験を有する者。

#### 基礎情報技術者試験もしくは、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者。

#### 中小企業のセキュリティポリシー作成に関する脆弱性診断やリスク分析の実施に関する相談対応（コンサル）等の経験

#### ※自分でできないことを人に助言するのは難しい

#### ※試験（知識）より、実務経験（スキル）のほうが有効

### （２）Webコンテンツ等（html,xhtml）の作成・編集について一定の知識・能力を有する者。

#### ガイドブック、ポータルサイトの更新業務（html,xhtml編集）について一定の知識・能力を有する者。

#### ※軽微な改修は、職員がやるほうが効率的

### （３）経験とスキルに基づいて、主体的かつ協調的に業務を遂行する意欲を有すること。 ※一定のコミュニケーション力を持つこと

#### iコンピテンシ―ディクショナリ（iCD)で示されたITヒューマンスキルは、想像力、実行・実践力、コミュニケーション力

#### https://icd.ipa.go.jp/icd/icd/skill-dictionary/skillref

#### 創造力

##### 問題発見力

##### 問題分析力

##### 仮説設定力

##### 論理思考力

#### 実行・実践力

##### 俯瞰力

##### 深耕力

##### 継続力

##### 革新力

#### コミュニケーション力

##### 相手の考えを理解する力

##### 自分の考えを伝える力

##### 共感を呼ぶ力

## 専門員としての行動規範

### 会計年度任用職員の役割

#### 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

### ワーク・ライフ・インテグレーションを目指す

#### 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

#### 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

#### 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。 確かにできてきることを日々のアウトプットで検証。

## 所掌事務の内容の明示の目的と意義

### ドキュメントによる情報の共有とノウハウの蓄積

#### 専門員の知識・ノウハウを形式知化し、発信情報、相談対応の回答内容の均質化を目指す

##### 個人的な暗黙知ではなく、共有可能な知識として

### 次世代技術、環境の活用のための実践的技術・知識の蓄積

#### 相談者が現在利用もしくは今後利用すべき次世代IT技術、セキュリティ対策技術を、専門員として試行もしくは実利用することにより、より実践的な情報発信および相談対応を可能にする

##### 単に見聞した知識ではなく

### 日々の有用な情報発信に努める

#### Twitter,ポータルサイトでは、定常的に有用な情報発信することにより、アクセスが多くなり、組織としての存在意義を高める

# Sec01-08-2-4\_専門員の所掌業務【要約】

## （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

### （相談対応の質の向上、 均質化）

### 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。

### 相談受付手段

#### 電話での相談受付・回答

#### Webフォームでの相談受付・回答

#### 【新規】メールでの相談受付・回答

#### 窓口対応

### 相談対応手順手順

#### 相談対応手順（Sec01-08-2内別添）

## （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）

### （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）

### 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/更新情報

##### お知らせ

#### 【拡充】ポータルサイト/関係機関提供情報

##### トピックス

##### 脅威情報

#### 【新規】「中小企業向けサイバーセキュリティ対策の極意」の解説および追補情報の発信

##### 「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（虎の巻）として発信

##### 第２版解説＋追補情報

##### HTML版

##### PDF版

##### EPUB版（リフロー版）

#### 中小企業向けサイバーセキュリティ対策情報の発信【関連情報を体系的に発信する】

##### 所掌業務（３）の「専門員ハンドブックとして整理したIT・サイバーセキュリティ関連の知識」をもとに体系的に発信

##### 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

###### インデックスページ

  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）【2020年12月最終更新：更新再開予定】

###### S01\_基本方針（各種方針・計画書・白書・報告書類）

00\_基本文書

CAB,NISC,METI,IPA,・・・

###### S02\_実施手順（管理者向け）

NIST,CAB,NISC,METI,IPA,JIPDEC,総務省,厚生労働省・・・

###### S03\_実施手順（一般ユーザ向け）

警視庁,IPA,ihaho,消費者庁・・・

###### S05\_緊急時対応マニュアル類（専門員）

相談・届出先クイックリスト

・・・

###### S10\_TCYSS業務

###### S90\_サイバーセキュリティ

サイバーセキュリティ事象毎

###### DX01\_Society5.0

次世代IT技術全般

##### 個別調査分析資料

###### 政策・制度、 サイバーセキュリティ、 次世代IT

###### 〇文献内容要約（サイバーセキュリティ関連）

###### 〇情報処理基本フレーム

###### 〇IT関連基本フレームワーク

###### 〇セキュリティ関連基本フレームワーク

###### 〇IT関連

###### 〇ITリテラシー関連書籍

###### 〇IT技術関連

###### 〇次世代技術トレンド関連書籍

###### 〇サイバーセキュリティ関連

###### 〇守るべき知的財産関連

##### （次世代技術の実践結果報告）

###### 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,…

###### 〇日々の自習、 セミナーを通じて取得した知見の報告書

#### 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

##### 【例】ガイドブック内容詳細解説

##### 【例】Society5.0時代に必要なセキュリティ対策

##### 【例】ECサイトの構築・運営におけるセキュリティ対策

##### 【例】BCPにおけるセキュリティ対策

### 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

### 【強化】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、 一般構成員のうち、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,Slack等】

### FAQの作成・更新

#### 方針

##### 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】

##### 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

#### FAQ分類【別シートで更新】

##### FAQ分類（ガイドブック項立てに沿った分類）

##### FAQ分類（「ここからセキュリティ」を参照）

## （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

### 【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）

### 「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）

#### 第2版改訂過程

##### 「中小企業向けサイバーセキュリティ対策の極意」【目次案】（Sec01-01-02）【2020年8月最終更新】

##### 「中小企業向けサイバーセキュリティ対策の極意」【本文案】（Sec01-01-03）【2021年3月最終更新】

### 「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）

#### 第2版改訂過程

#### 「中小企業向けサイバーセキュリティ対策の極意」解説書（Sec01-01）【2020年2月最終更新】

### 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

###### 【参照】「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）

##### 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

##### 調査によって得た知見を他の人が活用できる知識として形式知化する（暗黙知⇒形式知）

#### 詳細

##### 【参照】「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）

##### 【詳細】専門員業務ハンドブック【目次】（Sec01-08-5）

#### 目次

##### 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）

##### 第4編次世代技術の実践習得

##### 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）

#### 内容

##### 専門員業務ハンドブック（Sec01-08-2内別添）

## （４） その他付随する業務

### 会議等設営準備

### 係内庶務

# Sec01-08-2-5\_専門員業務ハンドブック【要約】

## 第0編　目次

### 【成果物】専門員業務ハンドブック【目次】（Sec01-08-5）【2020年5月最終更新】

### 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

## 第1編　はじめに

### サイバーセキュリティ担当の業務の位置づけ（Sec01-08-1）【2020年5月最終更新】

### 専門員の所掌業務及び調査分析項目（Sec01-08-2 ）【本資料】

## 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】

### 相談対応手順書（マニュアル）（Sec01-08-3）【校正作業停止中】

#### 対応手順【専門員用】

##### 個別ケース別相談対応手順

##### 汎用対応手順

#### サイバーセキュリティ相談・届出先クイックリスト

### 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）

### 日々収集した次世代IT技術、セキュリティ関連の文献、Webサイト情報の所在場所、 内容の要約作成及び蓄積

### ガイドブック内容詳細解説資料（虎の巻）

#### 「中小企業向けサイバーセキュリティ対策の極意」解説書（Sec01-01）【2020年2月最終更新：更新凍結中】

### 関係機関提供の参考文献リスト及び内容要約

#### 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）【2020年12月最終更新：更新再開予定】

### 今後の社会動向

### 次世代IT技術関連

### サイバーセキュリティ関連

### デジタル情報関連

### 内容例

#### 項目例

##### 〇文献内容要約（サイバーセキュリティ関連）

##### 〇情報処理基本フレーム

##### 〇IT関連基本フレームワーク

##### 〇セキュリティ関連基本フレームワーク

##### 〇IT関連

##### 〇ITリテラシー関連書籍

##### 〇IT技術関連

##### 〇次世代技術トレンド関連書籍

###### 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,…

##### 〇サイバーセキュリティ関連

##### 〇守るべき知的財産関連

##### 〇日々のニュースウォッチ情報

##### 〇日々の自習、 セミナーを通じて取得した知見の報告書

#### 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

##### 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】

###### CSF フレームワークコア

ID 特定

PR 防御

DE 検知

RS 対応

RC 復旧

##### 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

###### 「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

###### 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

##### 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)

### 知識の収集方法

#### 独学・自習

##### 情報処理技術者試験レベルの知識の習得

###### ITストラテジスト試験

###### 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

 Python

 Java

###### 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

## 第4編次世代技術の実践習得

### 先進技術の実践によるノウハウ習得

### 次世代IT利用環境・ツールの活用実践

#### 相談者の実利用環境の課題把握

#### 関連機関のサービスの把握

#### Webサービス、 ツールの試用

### ソフトウェア開発環境の活用実践

#### 開発環境

##### AIシステム稼働環境

##### ・・・

#### 言語

##### Python,R,Java

##### ・・・

## 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）

### 所掌事務（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で公開するドキュメントの作成

#### （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）

### サイバーセキュリティ対策説明資料（プレゼン資料）

### 次世代IT活用のための説明資料（プレゼン資料）

## 付録

# Sec01-08-2-6\_相談対応手順【要約】

## 電話受付

### 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

#### 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。

#### ディスパッチに必要な最低限の情報を担当内で共有

##### 緊急：セキュリティ侵害発生

###### 法律違反の可能性

###### 法律相談

##### 緊急：システム障害

##### 事前予防対策

##### 対策全般（啓発関連）

##### 生活安全関連

###### 法律違反の可能性がある場合は警視庁に

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

##### セキュリティ関連外

##### ガイドブック送付依頼

#### 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

#### 状況把握

#### 具体的な対応策検討

##### 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

##### 法律に違反する可能性がある場合は、 警視庁に問い合せ

##### 必要に応じてIPAに問い合わせ

##### 可能であれば、 TCYSSメンバーに確認

#### 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

###### 対策の概念、 簡易な処置を列挙

##### 「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

## 【新規】メールでの相談受付

### 手続き

#### 相談受付メールアドレス宛てのメールの確認

#### （※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

## Webフォームでの相談受付、

### 手続き

#### 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

## 窓口対応

### 手続き

#### 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

# Sec01-08-2-6\_SNSおよびポータルからの更新情報の発信手順【要約】

## Twitter

### ホットニュースのウォッチ

#### Twitter Security関連リスト

##### Twitter Security関連リスト【個別例：中山】

###### マルウェア情報局 @MalwareInfo\_JP

###### 内閣サイバー(注意・警戒情報)@nisc\_forecast

###### IPA（情報処理推進機構） @IPAjp

###### JVN 脆弱性レポート @jvnjp

###### IPA（ICATalerts）@ICATalerts

###### マイクロソフト セキュリティチーム @JSECTEAM

###### マカフィー株式会社 @McAfee\_JP

###### カスペルスキー 公式 @kaspersky\_japan

###### ノートン 公式 ツイッター @NortonJapan

###### トレンドマイクロ認証済みアカウント @trendmicro\_jp

###### エフセキュアブログ @FSECUREBLOG

###### 情報セキュリティのラック @lac\_security

###### JPCERTコーディネーションセンター @jpcert

#### はてな　セキュリティ関連ブックマーク【個別例：中山】

##### タグ：セキュリティ

#### ニュースインデックスサイト

##### GoogleNews

###### セキュリティ, 脆弱性, 脅威

#### セキュリティ関連情報提供サイト【個別例：中山】

##### ＠IT Security&Trustフォーラム

##### Security NEXT

##### セキュリティホール memo

##### 高木浩光＠自宅の日記

##### 統合版 JPCERT/CC RSS

##### 日本のセキュリティチーム

### 投稿すべきニュースの選別および発信方法決定

#### Webページ記事：

##### URL付きtweet

#### Twitter記事：

##### そのままのRetweet

##### コメント付きRetweet

###### コメント付きの場合は、コメント原稿作成

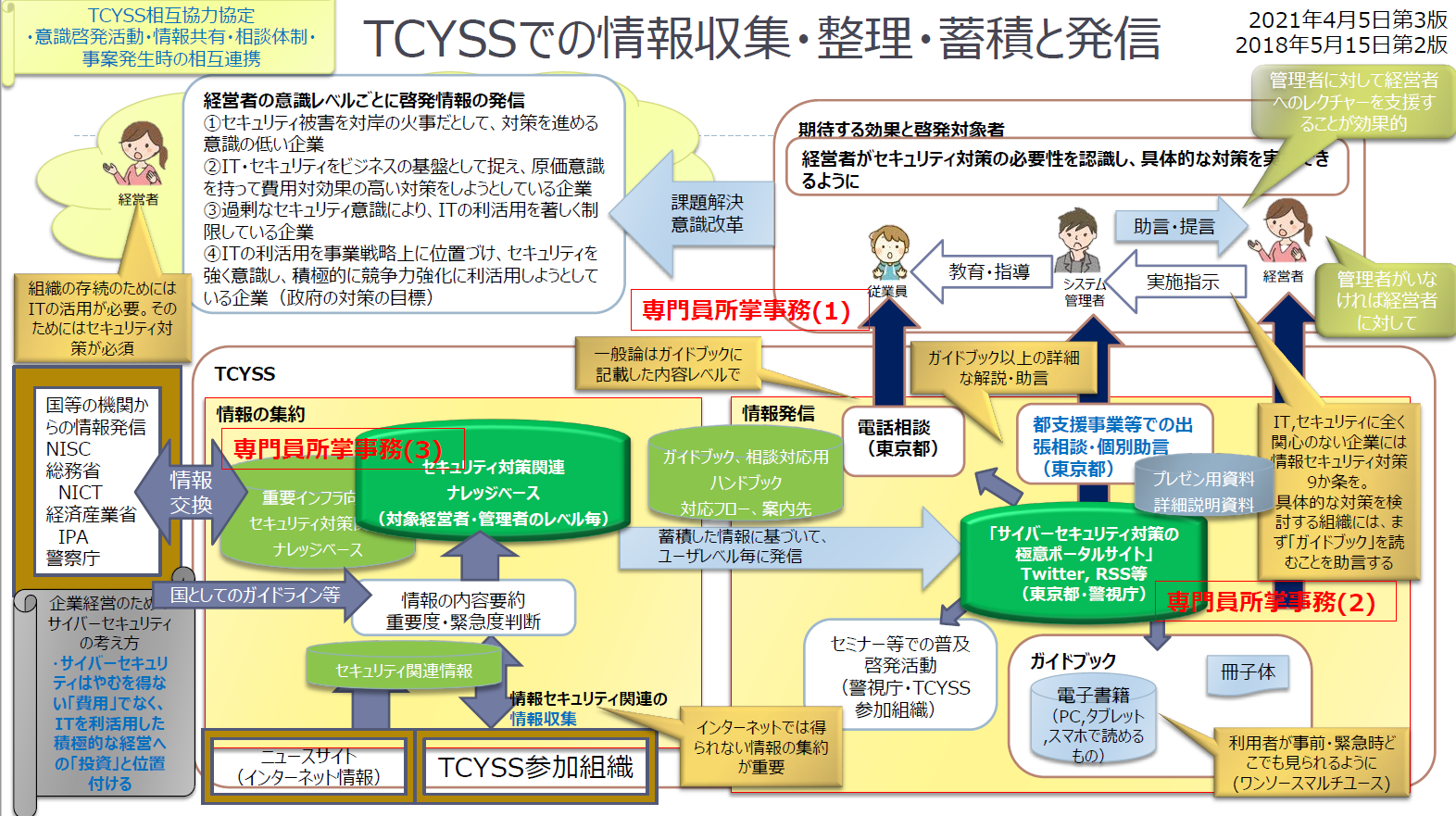
### Twitterで発信

## ポータルからの更新情報

### 更新情報

#### 【要検討】お知らせ、トピックスへの記事選定、原稿作成、発信について

# TCYSSでの情報収集・整理・蓄積と発信【概念図】



# 別添資料

## 【成果物】専門員業務ハンドブック【目次】（Sec01-08-5）

## 「中小企業向けサイバーセキュリティ対策の極意」解説書（Sec01-01）

## 相談対応手順書（マニュアル）（Sec01-08-3）