**2019年サイバーセキュリティ対策業務実施項目【案】**

2019年5月24日改訂

2019年4月12日係会議提出

サイバーセキュリティ専門員

# 実施項目

## サイバーセキュリティ関連情報の収集・蓄積（情報の知識化）

### 「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

* サイバーセキュリティ経営ガイドラインの重要10項目の改訂対応【中山】
  + サプライチェーン
* ブロックチェーン
* 総務省、NICTのNotice対応
* なりすましECサイト対策
* IoTセキュリティ、クラウドセキュリティ
* 守りのIT投資
  + 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）
  + テレワークソリューション（Wifiネットワークセキュリティ）
  + 法律違反の可能性への対応方法の解説【？】
    - GDPR対応
    - 個人情報保護法改正への対応
* 攻めのIT投資
  + 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【中山】
    - Society5.0, Connected Industry, DX, CPS対応
    - 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【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Revishon2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
* 関連情報、参考文献の充実

### 外部プレゼンテーション用資料の作成

* ドキュメント、スライド

### 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

### 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習得

* 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

## サイバーセキュリティ関連情報の発信の充実（知識の提供）

### ポータルサイト、SNS等での発信

* 中小企業に伝えたいホットな情報
  + ⇒Twitterで発信
  + ポータルサイトのトピックスで発信

### 「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

* 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
  + 「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。
* 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

### 外部プレゼンテーション、出張相談

* ⇒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

## 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【要検討】

* 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等の情報共有ツールの利用促進

# 専門員の知見等のドキュメント化

## 業務ハンドブック【専門員用】の更新

* 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）
  + 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）
  + セミナー等での情報収集・整理
* 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
* 第5編　実践的なノウハウ・知識の提供用資料（知見の発信）
* 付録

## その他資料の更新

# 実施管理

* 実施内容はすべてドキュメント化する。
* 専門員の業務報告を、週次もしくは隔週で作成する。

# TCYSSとしてパフォーマンス

* サイバーセキュリティ対策として、インシデント発生時に早期の検知と被害の拡大を防止することが特に重要である。
* ポータルサイトにおいて、東京都発行の小冊子「中小企業向けサイバーセキュリティ対策の極意」の追補版として、サイバーセキュリティ侵害に関する新たな事象と予防策、各関係機関が提供しているガイドラインの情報等を整理して発信していく。
* 中小企業のセキュリティ侵害により、サプライチェーン全体に被害が広がることや、攻撃者の踏み台として悪用される可能性がある。特に中小企業の経営者へのサイバーセキュリティ啓発や、情報共有を継続的に行っていく必要がある。