

☐ ① Sec01-08-5【成果物】専門員業務ハンドブック【目次】


■ 【2018年6月8日】

☐ ② 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）を参照
- 「専門員の職務内容詳細」（Sec01-08-2）を参照

☐ ② 第2編 相談対応マニュアル（相談対応時参照用）

☐ 個別ケース別相談対応手順

- 内容詳細は、「相談対応手順書（マニュアル）」（Sec01-08-3）を参照 

☐ 汎用手順

- サイバーセキュリティ相談・届出先クイックリスト
- 情報セキュリティ緊急対応ガイド【汎用】
- 相談対応の手引きレファレンスリスト【相談員用】
- サイバーセキュリティ対策相談対応の手引き（メモ）

☐ ② 第3編 個別調査分析資料（知見の蓄積）

- （実践的なスキル・知識を持つことにより、相談対応、啓発活動の質の向上を目指す）

☐ ガイドブック内容詳細解説資料（虎の巻）

☐ ガイドブック記述内容に沿って補足する情報

- 「サイバーセキュリティ対策ガイドブック解説書【Web用詳細版】」（Sec01-01）を参照

☐ ガイドブックに記載されていない最新情報

☐ 「経営者は何を備えればよいのか？」（Mission3）の、新たなトレンドへの対応


☐ 経営者がやらなければならない重要10項目の新たなガイドラインの解説

- 「サイバーセキュリティ経営ガイドライン」の改訂版での対策の考え方（Mission3-10の改訂版）

☐ 「業務の効率化、サービスの維持のために」（守りのIT投資）に活用すべきITと活用におけるサイバーセキュリティ対策





- 生産性向上のための「デジタル・ワークプレイス」の導入におけるサイバーセキュリティ対策

☐ 従業員エクスペリエンスを向上（働き方改革等）するシステムの導入におけるサイバーセキュリティ対策

- テレワークソリューション
- インテリジェント・ワークプレイス 

- Expand - Collapse
- ▢ 「ビジネスを発展させるために」（攻めのIT投資）に活用
おけるサイバーセキュリティ対策（Society5.0時代の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への対応
 - Society5.0, Connected Industriesの実現に向けて、産業界に求められるセキュリティ対策の全体像
 - ▢ 想定されるリスクと対策の整理
 - サプライチェーンを構成する企業のフィジカル空間での繋がり
 - フィジカル空間とサイバー空間の繋がり
 - サイバー空間とサイバー空間の繋がり
 - ▢ 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」の活用におけるサイバーセキュリティ対策
 - ▢ IoT（ICS）サイバーセキュリティ対策ガイド編
 - ▢ 1.フィジカルセキュリティスコープ
 - ・情報セキュリティ（IT）とコントロールセキュリティ（ICS）
 - ・セキュリティ上の課題
 - ・ITとOTセキュリティ対象
 - ・SCADシステムのコンポーネント
 - ▢ 2.IoTリスクアセスメント
 - ・リスクマネージメン
 - ・フィジカルセキュリティ
 - ・ネットワークセキュリティ
 - ・IoT/ICS固有のリスク特定と対応
 - ・資産の分類
 - ・脅威とリスク分析
 - ・リスク対応策と継続的監視及び修正
 - ▢ 3.IoTサイバーセキュリティ攻撃のシナリオ
 - IoT（ICS）サイバー攻撃
 - □特定
 - □防御
 - □検知
 - □対応
 - □復旧
 - ▢ 4.セキュリティ対策/ベストプラクティス
 - ・プロアクティブセキュリティモデル
 - ・5Keyセキュリティポイント
 - ・セキュリティリスク標準
 - ・Tool/Service

- ▣ 5.セキュリティギャップ分析
 - ・セキュリティ対策とギャップ分析（例）
- 6.IoTセキュリティインシデント事例
- 7.IoTセキュリティ基準と参考資料
- ▣ 8.IoTセキュリティのプレイヤー
 - 供給者、デリバリー、利用者、
- ▣ 9.（参考情報）
 - BCPとサイバーセキュリティ
- 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
- ▣ 事業継続計画（BCP）の一環としての一連のサイバーセキュリティ対策の明文化の実施の考え方
- ▣ 事前だけでなく事後の「緊急時対応」も含めた一連の対応として、フェーズごとの対策
 - 特定
 - 防御
 - 検知
 - 対応
 - 復旧
- **GDPR違反にならないために行うべきこと**
- ▣ **法律違反の可能性への対応方法の解説**
 - （ガイドブック内の用語解説から独立した項目として解説）
- ▣ **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がある法律名、条文の解説**
 - サイバーセキュリティ基本法, 不正アクセス禁止法
- ▣ 個人情報保護法
 - 個人情報保護に関するガイドライン, 特定個人情報の適正な取扱いに関するガイドライン, マイナンバー法施行令（行政手続における特定の個人を識別するための番号の利用等に関する法律施行令）
 - **GDPR対応も**
- ▣ **刑法**
 - 不正指令電磁的記録に関する罪（ウイルス作成罪）, 電子計算機使用詐欺罪, 電子計算機損壊等業務妨害罪, 電磁的記録不正作出及び供用罪, 支払用カード電磁的記録不正作出等罪, 詐欺罪
- ▣ その他のセキュリティ関連法規
 - 電子署名及び認証業務等に関する法律, プロバイダ責任制限法, 特定電子メール法

- ▢ 知財関連
 - 著作権法, 産業財産権法, 不正競争防止法,
- ▢ 労働関連・取引関連法規
 - 労働基準法, 労働者派遣法, 男女雇用機会均等法, 公益通報者保護法, 労働安全衛生法, 下請法, インターネットを利用した取引, 特定商取引法, 電子消費者契約法
- ▢ その他の法律・ガイドライン・技術者倫理
 - IT基本法, e-文書法（電磁的記録）, 電子帳簿保存法, コンプライアンス, 情報倫理・技術者倫理
- 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
- ▢ サイバーセキュリティ脅威の新たなトレンドへの対応方法の解説
 - なりすましECサイトの被害と回避策
 - ビジネスメール詐欺の被害と回避策
 - （ドメイン詐欺メール）
- ▢ セキュリティ侵害の事例集（FAQ作成の参考用）
 - サイバーセキュリティ担当相談対応記録
 - セキュリティ侵害事例紹介サイト（FAQ候補） 
 - ここからセキュリティ！ 情報セキュリティ・ポータルサイト（IPA）【FAQ候補】 
- ▢ 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
- ▢ インデックスリスト（メタデータ）
 - 各機関が提供している文献、Web情報の所在場所情報
- ▢ 内容要約（Description）
 - ▢ サイバーセキュリティ関連の国等の施策を事前調査情報として整理
 - 「サイバーセキュリティ関連各種施策等の内容要約」（Sec01-04）を参照
 - ▢ 各機関が提供している参考文献、Web情報のポイントを、事前調査情報として整理
 - 「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
 - ▢ 情報収集元
 - 「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
- ▢ 自習、セミナーを通じて取得した知見を報告書としてまとめる
 - 【業務レポート】



☐ ② 第4編 実践的なノウハウ・知識の提供用資料（知見の発信）

☐ ② サイバーセキュリティ対策説明資料（プレゼン資料）

- スライド及び解説書

☐ テーマ例

- Society5.0時代に必要なセキュリティ対策
- IoTの活用におけるセキュリティ対策
- ECサイトの構築・運営におけるセキュリティ対策
- BCPの一環としてのセキュリティ対応計画
- . . .



☐ 公開用成果物

- 専門員ハンドブックの内容のうち、利用者への普及啓発において有益と思われる情報を整理して、利用者向け情報としてWeb等で公開する
- サイバーセキュリティ事象毎に法律違反となる可能性のある法律と条項
- GDPR違反とならないために行うべきこと
- IoTの開発及び利用におけるサイバーセキュリティ対策
- . . .



☐ ② 付録

- 2016～2017年度相談受付内容要約及び得られた知見