Sec93_01_01_サイバーセキュリティ経営ガイドラインVer2.0_付録D_国際規格ISOIEC27001及び27002との関係

1. 概要

「サイバーセキュリティ経営ガイドラインVer2.0」の「付録D_国際規格ISOIEC27001及び27002との関係」を切り出し、可視化したもの

情報セキュリティマネジメント（ISMS）への適用の検討のために使用することを想定。

原本
- 「サイバーセキュリティ経営ガイドラインVer2.0」【2017年11月16日METI】
- https://www.meti.go.jp/policy/netsecurity/mng_guide.html

改版履歴　2022年1月5日 初版

2. 付録D 国際規格ISO/IEC27001及び27002との関係

重要１０項目　ISO/IEC 27001（●）、ISO/IEC 27002（・）

指示１
サイバーセキュリティリスクの認識、組織全体での対応方針の策定
- ●5.1_リーダーシップ及びコミットメント方針
- ●5.2_方針

指示２
サイバーセキュリティリスク管理体制の構築
- ●5.3_リスク及び機会、責任及び権限
- ・6.1.1_情報セキュリティの役割及び責任

指示３
サイバーセキュリティ対策のための資源（予算、人材等）確保
- ●7.1_資源
- ●7.2_力量

指示４
サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
- ●6.1_リスク及び機会に対処する活動
- ●6.2_情報セキュリティ目的及びそれを達成するための計画策定
- ・5.1.1_情報セキュリティのための方針群
- ・5.1.2_情報セキュリティのための方針群のレビュー

指示５
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　・6.2 モバイル機器及びテレワーキング
- ・9_アクセス制御
- ・10_暗号
- ・11_物理的及び環境的セキュリティ
- ・12_運用のセキュリティ
- ・13_通信のセキュリティ

- 指示６ サイバーセキュリティ対策における PDCA サイクルの実施　●7.4 コミュニケーション
  - ●8.1_運用の計画及び管理
  - ●8.2_情報セキュリティリスクアセスメント
  - ●8.3_情報セキュリティリスク対応
  - ●9.1_監視、測定、分析及び評価
  - ●9.2_内部監査
  - ●9.3_マネジメントレビュー
  - ●10.1_不適合及び是正処置
  - ●10.2_継続的改善
  - ・17.1.1_情報セキュリティ継続の計画
  - ・17.1.2_情報セキュリティ継続の実施
  - ・17.1.3_情報セキュリティ継続の検証、レビュー及び評価
  - ・18.1.1_適用法令及び契約上の要求事項の特定
  - ・18.2.1_情報セキュリティの独立したレビュー
  - ・18.2.2_情報セキュリティのための方針群及び標準の順守
  - ・18.2.3_技術的順守のレビュー
- 指示７ インシデント発生時の緊急対応体制の整備　・16.1.1 責任及び手順
  - ・16.1.2_情報セキュリティ事象の報告
  - ・16.1.3_情報セキュリティ弱点の報告
  - ・16.1.4_情報セキュリティ事象の評価及び決定
  - ・16.1.5_情報セキュリティインシデントの対応
- 指示８ インシデントによる被害に備えた復旧体制の整備　・17.1.1 情報セキュリティ継続の計画
  - ・17.1.2_情報セキュリティ継続の実施
  - ・17.1.3_情報セキュリティ継続の検証、レビュー及び評価
- 指示９ ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握　●8.1 運用の計画及び管理
  - ・15.1.1 供給者関係のための情報セキュリティの方針
  - ・15.1.2_供給者との合意におけるセキュリティの取扱い
  - ・15.1.3_ICT サプライチェーン
  - ・15.2.1_供給者のサービス提供の管理及びレビュー
  - ・15.2.2_供給者のサービス提供の変更に対する管理
- 指示１０ 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供 ・6.1.3 関係当局との連絡
  - ・6.1.4_専門組織との連絡