重要インフラのサイバーセキュリティに係る安全基準等策定指針(案)の概要

各重要インフラ分野に共通して求められるサイバーセキュリティの確保に向けた取組をまとめた「安全基準等策定指針」について、新たな重要インフラ行動計画が策定されたことを踏まえ、組織統治、サプライチェーンを含めたリスクマネジメント等の観点から改定する。

1. 行動計画を踏まえた見直し

✓ 組織統治に関するセクションを新設し、サイバーセキュリティとの関係を整理
- 組織方針（経営方針、リスクマネジメント方針等）にあたる文書に、重要インフラのサイバーセキュリティ確保に関する事項も組み入れる
- 組織内外のコミュニケーション（報告、意思決定等）の枠組みにおいて、サイバーセキュリティに関するリスク、インシデント等の情報も取り扱う
- 経営層がサイバーセキュリティに関するリスク及びそれが業務運営に及ぼす影響を理解し評価できる体制を整備する
- 経営層の責任においてサイバーセキュリティに関する責任者を任命する
- 組織全体の監査の一部としてサイバーセキュリティに関する監査を実施する
- 既存の開示体制を活用し、国民の安心感の醸成を図る観点から、可能な範囲でサイバーセキュリティに関する取組を開示する　等

✓サイバーセキュリティリスクマネジメントの活用・危機管理に係る事項を追記
- サプライチェーン・リスクマネジメントを実施し、事業者間の契約を通じてその実効性を確保する
- 組織状況と資産を把握し、任務保証の考え方に基づくリスクアセスメントを実施する（特に、事業被害シナリオを活用したリスク分析を推奨）
- 遠隔監視・制御等のために外部と接続される場合があること等を念頭に、制御システムについても適切にリスクアセスメントを実施する
- マチュリティーモデルの活用等により、セキュリティ対策の適用の程度について優先順位付けを実施する　等

2. 最近の動向を踏まえた追記

✓ランサムウェア対策、クラウドサービス利用に係る対策等を追記

3. その他

✓表現・内容を簡潔にし、手順等の詳細は手引書に移動

✓ベースライン（最低限実施すべき事項）と推奨事項（実施が望ましい事項）が明確になるように書き分け

安全基準等策定指針（案）に記載の取組概要

組織統治

- **組織方針・サイバーセキュリティ方針の策定**
  - ✓「重要インフラサービスの安全かつ持続的な提供を実現」
  - ✓ サイバーセキュリティ確保の目的、方向性
  - ✓ 維持するサービスの範囲・水準
  - ✓ 経営層によるコミットメント　等を記載（※）
- **組織内外のコミュニケーション**
  - ✓ セキュリティリスク、インシデント等に関するコミュニケーション
- **リスク管理体制**
  - ✓ サイバーセキュリティリスクを評価・管理する体制の構築
- **責任及び権限の割当て**
  - ✓ サイバーセキュリティに関する責任者の任命
- **監査・モニタリング**
  - ✓ 経営層の責任における監査の実施
  - ✓ 脆弱性診断、ペネトレーションテスト等の実施（※）
- **情報開示**
  - ✓ サイバーセキュリティ方針、リスク管理体制（※）等の開示
- **継続的改善**
  - ✓ 監査・モニタリング、演習・訓練等を踏まえた改善

※の項目は推奨事項

リスクマネジメント・危機管理

- **組織状況の理解**
  - ✓ 重要インフラサービスの外部環境、内部環境の把握
  - ✓ 関係主体からの要求事項の整理
  - ✓ リスク管理体制・個別対策の現状把握
- **リスクアセスメントの実施**
  - ✓ 組織状況と資産を踏まえたリスクアセスメントの実施
  - ✓ 目標とする将来像の決定
- **セキュリティ対策・程度の決定**
  - ✓ 将来像と現状のかい離を埋めるためのセキュリティ対策の検討
  - ✓ マチュリティモデルを活用し対策の程度・優先順位を決定
- **個別方針の策定**
  - ✓ 実施する個々のセキュリティ対策に対する個別方針の策定
- **リスク対応計画の策定**
  - ✓ 実施事項、責任者、達成期限、評価方法（※）等の明文化
- **サプライチェーン・リスクマネジメントの実施**
  - ✓ 不正機能の埋め込み、サービスの供給途絶等のリスクへの対応
  - ✓ 事業者間の契約において、サイバーセキュリティリスクへの対応の役割と責任範囲の明確化
- **事業継続計画等の策定**
  - ✓ コンティンジェンシープラン、事業継続計画、事業復旧計画の策定
  - ✓ IT-BCPの策定（※）
- **人材育成・意識啓発の実施**
  - ✓ 部署・役職に応じて必要なサイバーセキュリティに関する能力の確保
  - ✓ サイバー被害事例の共有（※）等による意識啓発
- **CSIRT等の整備**
  - ✓ 情報システム等の監視、問題発生時の解析・調査等を実施する体制の構築
  - ✓ 制御システム関連部門との連携体制の整備（※）
- **平時の運用**
  - ✓ セキュリティ対策の導入、運用プロセスの確立・実行
  - ✓ 組織内外との情報共有
- **危機管理の実施**
  - ✓ 事業継続計画に則った初動・復旧対応の実施
- **演習・訓練の実施**
  - ✓ リスクマネジメント・危機管理体制の有効性検証のための演習・訓練の実施

対策を例示（各組織が適切な対策・程度を決定）

対策項目（※）

- **組織的対策**
  - ✓ 資産の管理
  - ✓ 供給者管理
  - ✓ 運用管理
  - ✓ システムの取得・開発・保守
  - ✓ インシデント管理　等
- **人的対策**
  - ✓ 従業員の管理
  - ✓ 委託先管理
  - ✓ テレワーク・遠隔制御
  - ✓ エスカレーション　等
- **物理的対策**
  - ✓ セキュリティ確保領域の管理
  - ✓ 設備配置等における災害対策
  - ✓ 装置の管理　等
- **技術的対策**
  - ✓ 利用者アクセスの管理
  - ✓ 情報システム等のアクセス制御
  - ✓ 暗号を活用した情報管理
  - ✓ 通信のセキュリティ
  - ✓ 多層防御　等
- **動向を踏まえた対策**
  - ✓ ランサムウェア対策
  - ✓ クラウドサービス利用時の対策

重要インフラのサイバーセキュリティ部門における リスクマネジメント等手引書(案)の概要

➢ リスクアセスメントに係る主要なプロセスを整理した「重要インフラにおける機能保証の考え方に基づくリスクアセスメント手引書」について、安全基準等策定指針の「4. リスクマネジメントの活用と危機管理」におけるリスクマネジメント等の主要なプロセス及び「5. 対策項目」における主なセキュリティ対策に関して、サイバーセキュリティ部門における取組を念頭に記載したものに改定する。

1. 行動計画を踏まえた見直し

✓ 自組織の特性の明確化について明示
- 自組織の特性の明確化の重要性
- 自組織の特性把握と現在のセキュリティ対策の実施状況の特定手法

✓制御システムのリスクアセスメント手法について追記

✓自組織に適した防護対策の決定手法の追記

✓サプライチェーン・リスクのリスク管理策例の追記
- 供給者の事業計画や提供実績等の確認
- サプライチェーンとのネットワーク接続点におけるセキュリティの確認　等

2. リスクマネジメントに関する記載の追記

✓モニタリング及びレビューについて追記
- リスクの見える化（可視化）によるモニタリング、レビュー手法

✓リスクコミュニケーションについて追記
- 組織内外とのコミュニケーションの在り方

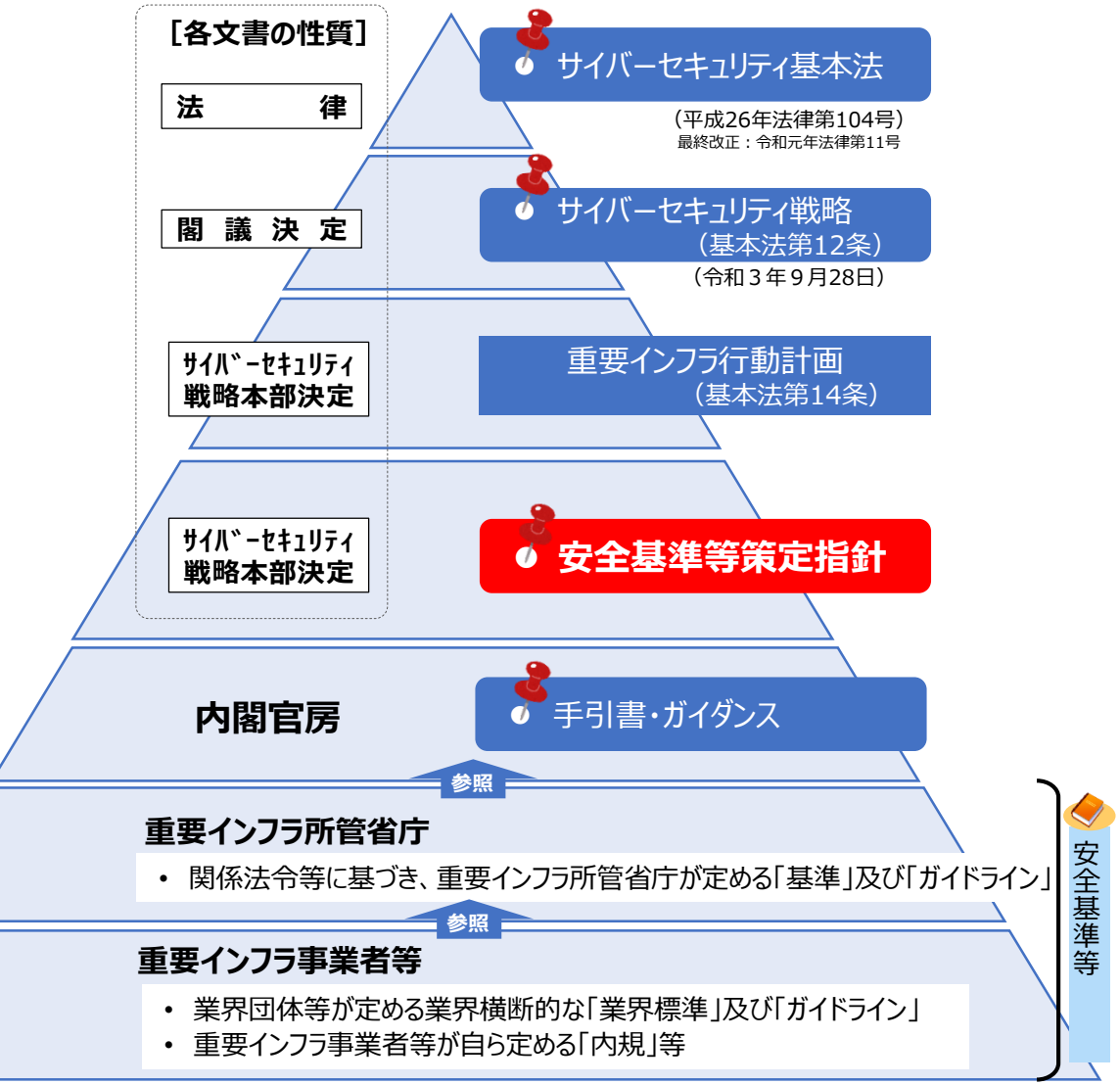
3. その他

✓リスクアセスメントの具体的手順について、「機能保証のためのリスクアセスメント・ガイドライン」を参照する形式に変更

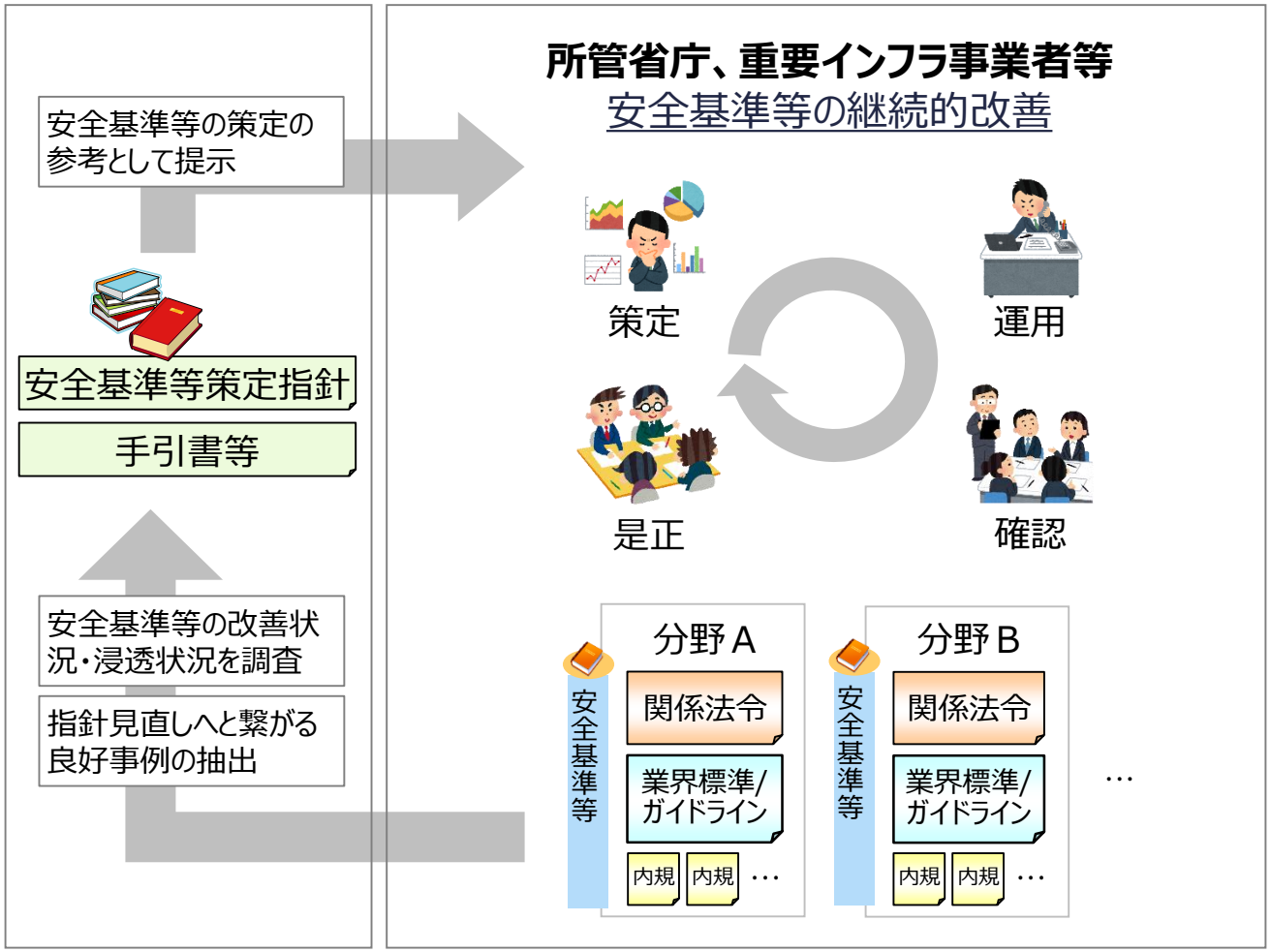
✓指針における対策項目に関する詳細説明について記載

（参考）文書の位置付け

安全基準等策定指針とは、重要インフラサービスの安全かつ持続的な提供を図る観点から、**安全基準等において規定が望まれる項目を整理・記載**し、重要インフラ事業者や重要インフラ所管省庁の「安全基準等」の策定・改定を支援することを目的とするもの。**手引書**とは、安全基準等策定指針に記載された項目に関して**具体的な手順等の参考情報**を示すもの。



【安全基準等策定指針の活用方法】



（参考）重要インフラ行動計画における記載

○ **重要インフラのサイバーセキュリティに係る行動計画(令和４年６月17日サイバーセキュリティ戦略本部決定)(抜粋)**

IV.計画期間内の取組

2.安全基準等の整備及び浸透　2.1安全基準等策定指針の継続的改善

内閣官房は、特に障害対応体制の強化の観点から、安全基準等策定指針及び手引書の見直しを行う。安全基準等策定指針及び手引書の見直しについては、3年に1度の実施を原則とする。他方、社会動向の大きな変化等、現行の安全基準等策定指針及び手引書では十分ではない事象が発生した場合は、この限りでない。さらに、安全基準等策定指針及び手引書の関連文書であるガイダンス等については、昨今のランサムウェアによる攻撃の増加を一例とする周辺環境の激変やインシデント等に速やかに対応できるよう、運用等から得られた知見を踏まえて適時に改定する。また、国際標準や海外の指針のうち日本でも参考にすべきものがあれば適宜採り入れることを検討する。

本行動計画期間中に新たに整備を行う安全基準等策定指針に係る事項は以下のとおりとする。

(1)組織統治に関する基準の整備

組織統治の一部としてサイバーセキュリティを取り入れる方策に係る記載を強化すべく、「サイバーセキュリティ関係法令Q&Aハンドブックver1.0」(令和２年３月２日)で規定している①内部統制システムとサイバーセキュリティとの関係、②サイバーセキュリティと取締役等の責任、③サイバーセキュリティ体制の適切性を担保するための監査等、④サイバーセキュリティと情報開示、を活用するなどして、安全基準等策定指針の記載を充実させる。

(2)サプライチェーンに関する基準の整備

サプライチェーンに起因する重要インフラサービス障害の連鎖に係るリスク、例えば、①サプライチェーンの過程で製品に不正機能等が埋め込まれるリスク、②政治経済情勢による機器・サービスの供給途絶のリスク、③クラウドサービス等の外部サービスにおける情報の取扱い・可用性に係るリスク等の高まりを踏まえ、サプライチェーン・リスクへの対応について安全基準等策定指針の記載を充実させる。

(3)自組織に適した継続的改善のための基準の整備

自組織に適した対策に係る基本的な考え方を安全基準等策定指針に盛り込み、具体的な実施手法を示す関連文書等の作成を実施する。

(4)その他基準の整備

プラントや工場等の制御システムへのサイバー攻撃等の脅威に迅速に対応するため、ITとOTの横断的な組織整備や、OTのセキュリティ人材の育成の重要性を訴求する。

4.リスクマネジメントの活用　4.1リスクマネジメントの推進

(2) 自組織に適した防護対策の具現化

内閣官房は、前号に示した重要インフラ事業者等が自組織に適した防護対策の実現を支援するため、手引書の見直しに加え、既存の基準類をどのように自組織に活用するかを含めた新たなガイダンス等を整備する。