内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

資料４

安全基準等策定指針・手引書の改定骨子（案）について

内閣サイバーセキュリティセンター
重要インフラグループ
2022年12月22日

指針改定骨子案の概要

➢ 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. 新たな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
- **組織方針の策定**時にサイバーセキュリティに関する事項も考慮する
- サイバーセキュリティに関するリスクが**経営リスクの一つ**であり、さらに、**その他の経営リスクに影響を及ぼすリスク**であると捉える
- **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
- **取締役会に相当する場**においてサイバーセキュリティに関する責任者についても任命する
- 責任者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
- 障害発生時における**事業継続計画（BCP）等の一部**として、IT-BCP等の情報システムに係る障害対応方針を策定する
- **内部監査・監査役等監査の一部**としてサイバーセキュリティに関する監査を実施する
- **既存の開示制度を積極的に活用**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
- 任務保証の観点から自組織の特性を理解する
- 自組織の現在のセキュリティ水準及び目標とするセキュリティ水準を決定し、その差異を分析する
- 差異を解消するためのセキュリティ対策を検討し、その適用の程度について優先順位付けを行い、自組織に適したセキュリティ対策を決定する
- 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
- セキュリティ対策によって、サイバーセキュリティに関するリスクをどの程度回避、軽減が出来たかを測定・評価する　等

2. 最近の動向を踏まえた追記

✓対策項目に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

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

指針改定骨子案の目次

- **経営層向け**を念頭とした取組を記載。
- 組織統治に関するセクションを新設。
- 現行指針に『「リーダーシップ」の観点』として記載されている事項を整理。
- **経産省「サイバーセキュリティ経営ガイドライン」**をベースに、「組織統治の一部としてのサイバーセキュリティ」という観点がより明確になるよう取組を記載。

- **CISO、戦略マネジメント層向け**を念頭とした取組を記載。
- 基本的には現行指針の内容を踏襲。
- サプライチェーン・リスクマネジメントに関するサブセクションを新設。
- **NIST「サイバーセキュリティフレームワーク」**をベースに、自組織の特性を踏まえた自組織に適したセキュリティ対策の実施に係る取組を追記。

- **戦略マネジメント層、担当者層向け**を念頭とした取組を記載。
- 基本的には現行指針の内容を踏襲。
- 最近の動向を踏まえ、ランサムウェア対策、クラウドサービス利用時の対策に係るサブセクションを新設。
- **「政府機関等の情報セキュリティ対策のための統一基準」（サイバーセキュリティ戦略本部決定）**との整合をとり、遠隔制御等に関する対策を追記。

手引書改定骨子案の概要

➢ 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、リスクマネジメントプロセス全体について記載された「リスクマネジメント手引書」に改定する。

1. 新たな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水準の特定手法
- ✓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
  - – 目標とするセキュリティ水準の決定手法
- ✓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

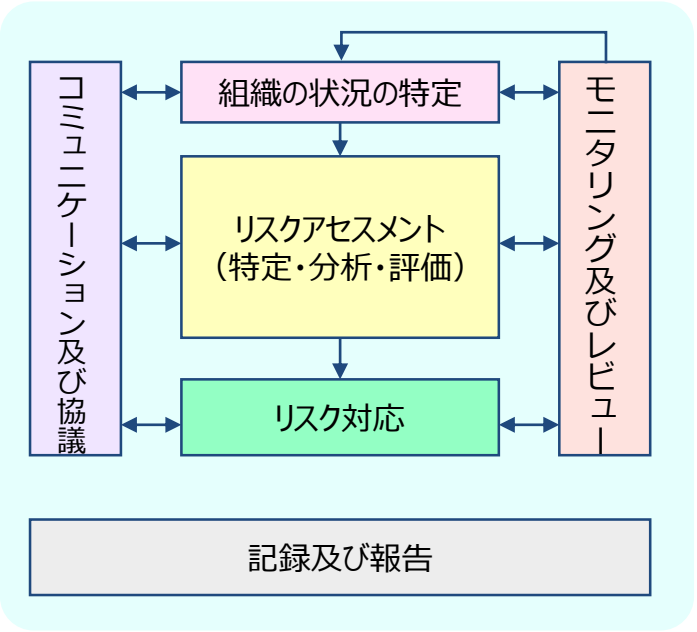
2．リスクマネジメントに関する記載の追記

- ✓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

- ✓読みやすさの観点から構成の整理等を実施

リスクマネジメントのプロセス



「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」（重要インフラ専門調査会決定）を基に作成

改定に向けた論点

※前回会合から御意見を基に更新

① 組織統治の一部としてサイバーセキュリティを組み入れることについて具体的に記載するにあたり、分野・組織によって風土や既存の体制が異なり、また、特に小規模な組織においてはセキュリティに係る人材・予算を確保するのも容易ではなく、実現可能性の観点から懸念がある。これを踏まえ、どのような具体的取組を記載するか。

② サプライチェーンは分野・事業者によって関わり方や裾野が異なるところ、指針において対象とするサプライチェーンの類型・範囲をどこに設定するか。その上で、優先的に対処すべきサプライチェーン・リスクとしてどのようなものを想定し、それに対してどのように対処することとするか。

③ 制御システムのサイバーセキュリティの確保について、どのような具体的取組を記載するか。

④ 任務保証の考え方（＝情報保護だけではなくサービス影響に重点を置いた考え方）による取組をさらに促進するにはどうすればよいか。

⑤ 最低限実施すべき取組（ベースライン）を明らかにする必要があるのではないか。

⑥ 実効性を確保するにはどうすればよいか。

⑦ 国内外に既に確立された関連文書があるところ、どのように整理すべきか。

論点１　組織統治の一部としてサイバーセキュリティの組み入れ

➢ 組織統治の一部としてサイバーセキュリティを組み入れることについて具体的に記載するにあたり、分野・組織によって風土や既存の体制が異なり、また、特に小規模な組織においてはセキュリティに係る人材・予算を確保するのも容易ではなく、実現可能性の観点から懸念がある。これを踏まえ、どのような具体的取組を記載するか。

（主な御意見）

- 組織の経営リスクにサイバーセキュリティを組み込んだリスクマネジメントを実施すべき。
- 分野・事業者それぞれの組織風土があるため、組織の既存の体制を生かせる柔軟な取組にすべき。
- 中小規模の組織にとって過度な負担にならない、実現可能な取組とすべき。
- 取締役の誰かをCISOとすることは現実的ではない。取締役会に相当する場においてCISOを任命することとすべき。
- CISOの知識・技能だけを追求するのではなく、組織体制で補う方法も検討すべき。
- 重要インフラ事業者だけでは限界があり、サプライチェーン事業者が重要インフラを支える体制作りが重要。

（対応方針案）

- 経産省「サイバーセキュリティ経営ガイドライン」をベースに、「組織統治の一部としてのサイバーセキュリティ」の観点がより明確になるよう追記する。
- 分野・組織によって風土や既存の体制が異なることから、組織の既存の組織統治体制においてサイバーセキュリティを扱うとの記載に留める。
- 取締役に相当する者からのCISOの任命、CISOの知識・技能等について、ベースライン（～すること）と先進事項（～が望ましい）に書き分ける。

  II.3.　体制の構築

  ✓ リスクマネジメントに係る責任者を取締役会に相当する場において任命する際に、サイバーセキュリティに関する責任者についても任命すること。

  ＊ 取締役に相当する者の中からCISO（最高情報セキュリティ責任者）を任命することが望ましい。

  ✓ 責任者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こと。

  ＊ サイバーセキュリティに関する責任者は、サイバーセキュリティについて十分な知識及び技能を保持していることが望ましい。

- 実現可能性の観点から、適切な管理体制の構築を前提としつつ、サイバーセキュリティに関する専門的な事項については、外部委託、業界団体との連携等により補完してもよい旨を補足する。

論点２　サプライチェーン・リスクへの対応

➢ サプライチェーンは分野・事業者によって関わり方や裾野が異なるところ、指針において対象とするサプライチェーンの類型・範囲をどこに設定するか。その上で、優先的に対処すべきサプライチェーン・リスクとしてどのようなものを想定し、それに対してどのように対処することとするか。

（主な御意見）

- サプライチェーンの類型（機器、ソフトウェア、サービス等）や何次サプライヤーまでが対象かを明確にすべき。
- 想定するサプライチェーン・リスクを明示すべき。
- グループ会社や取引先会社における脆弱性対策が必要。
- 経済安保の取組と整合するようにすべき。
- 外部委託先のサービス途絶を想定したコンティンジェンシープランを作成すべき。

（対応方針案）

- サプライチェーンとは、一般的に、ある製品の原材料が生産されてから、最終消費者に届くまでのプロセスを意味するものであり、安全基準等策定指針においては、外部組織が関与する製品（機器・ソフトウェア）及びサービス（クラウドサービス・保守運用役務等）を自組織で調達・利用するプロセスとする。

  ※サイバーセキュリティ戦略（令和3年9月28日閣議決定）においては、サプライチェーンの構成要素として、「機器、ソフトウェア、データ、サービス」を例示。
- 対応すべき代表的なサプライチェーンに係る脅威として①サプライチェーンの過程で設備に不正機能等が埋め込まれること、②政治経済情勢による設備・サービスの供給途絶、③サービスにおける不適切な情報の取扱い・サービスの可用性の毀損、④海外拠点、グループ組織、取引先等を経由したサイバー攻撃を挙げる。

  ※重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部）においては、①～③を例示。
- サプライチェーンの対象範囲については、まずは直接の供給者を対象とし、リスクに応じてその範囲を設定する。また、各供給者がその先の供給者を対象とするサプライチェーン・リスクマネジメントの実施状況を把握することで、サプライチェーン全体のリスクマネジメントを実施する。
- 事業者間の契約を通じて、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化するとともに、対策の導入支援や共同実施等、サプライチェーン全体での方策の実効性を高めることとする。
- 望ましい取組として、サービス途絶を想定した事業継続計画等の作成、インシデント発生時や脆弱性情報の把握時における情報共有の実施等を例示する。

論点３　制御システムのサイバーセキュリティの確保

➢ 制御システムのサイバーセキュリティの確保について、どのような具体的取組を記載するか。

（主な御意見）

- 制御システムは独自仕様の機器・通信プロトコルで構成され、また、閉域環境で稼働しており、セキュリティ上の懸念はないと考えている分野もある。
- 今後、経済合理性等の観点から、制御システムにおいても汎用機器の利用や公共通信網への接続が進むことも考えられ、設備更改の際には、セキュリティリスクに適切に対応する必要がある。
- ホワイトリスト方式やEDR※の導入が有効ではないか。

※ EDR(Endpoint Detection and Response):デバイスへの攻撃や侵入を防ぐのではなく、デバイスの挙動監視などによって侵入を防げなかった脅威を検知・対処するセキュリティ対策。

（対応方針案）

- 「制御システムに汎用機器が用いられ、また、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」こととする。
- 取組の例示として、「IPA『制御システムセキュリティリスク分析ガイド 第2版 ～セキュリティ対策におけるリスクアセスメントの実施と活用～』を参考とした、事業被害ベースのリスク分析の実施」を挙げる。
- 制御システムに対する具体的なセキュリティ対策として、米国 Cybersecurity Performance Goals（CPG）を参考に、制御システムに特化したサイバーセキュリティ責任者の設置、デフォルトパスワードの変更、パッチ適用等による脆弱性対策、多要素認証の導入、物理ポートの無効化等の取組を例示する。

論点４　任務保証の考え方の取組の促進

➢ 任務保証の考え方（＝情報保護だけではなくサービス影響に重点を置いた考え方）による取組をさらに促進するにはどうすればよいか。

（参考）2021年度の調査結果によれば、回答のあった重要インフラ事業者のうち、機能保証の考え方を取り入れたリスクアセスメントを実施しているとの回答数は３割程度。

（主な御意見）

- 最近のランサムウェアによるサービス停止を踏まえると、サービス継続に重点を置いた考え方はより重要になっていると考える。
- 現行の安全基準等策定指針においてもサービス影響に重点を置いた考え方を踏まえて取り組むこととされており、既に十分に取り組めている。

（対応方針案）

- 実態としては任務保証の考え方は既に浸透しているものの、調査結果と乖離がある状況。何をもって「任務保証の考え方を踏まえた」ことになるのか明確でないことが理由と考えられるため、任務保証の考え方を踏まえた取組例を追記する。
  - ＊ 任務保証の観点から自組織の特性を理解する
    - ✓ 自組織が果たすべき役割・機能を発揮するために維持・継続することが必要なサービス
    - ✓ 関係者のニーズ・期待や法制面での要求事項等を満たすために最低限許容されるサービス範囲・水準
    - ✓ サービス提供を維持するために必要な業務や経営資源
  - ＊ 社会経済に与える影響を最小化するために検知・対応・復旧といった危機管理を実施する
- 現行指針では、重要インフラサービス障害発生時における初動から完全復旧までの対応方針（事業継続計画等）を策定することとしているが、組織全体の事業継続計画等とサイバーセキュリティの関係が明らかでなかったことから、事業継続計画等の一部としてIT-BCP等の情報システムに係る対応方針も策定するとの記載に改める。

論点５　ベースラインの設定

➢ 最低限実施すべき取組（ベースライン）を明らかにする必要があるのではないか。

（主な御意見）

- 分野・事業者によって状況が異なるため、ベースラインを一律に設定するのは難しいのではないか。
- 大規模災害時等においても最低限許容されるサービス水準の設定をベースラインとしてはどうか。
- 成熟度評価を経営者の責務の一部として推進すべき。

（対応方針案）

- 個別具体の取組（バックアップ、多要素認証等）については、分野・事業者によって状況が異なるため、ベースラインとして設定せず、各分野ごとに目標とするセキュリティ水準が設定されることを期待する。
- 他方、組織管理に関する取組について、あくまで「目標」としてベースラインを設定することは、重要インフラにおける一定のセキュリティ水準を確保する上で有意義と思われる。そのため、次のような取組をベースラインとする。
    - ＊ 組織統治に関する事項（経営リスクの一部としてサイバーセキュリティリスクを扱うなど）
    - ＊ 任務保証に係る事項（最低限許容されるサービス範囲・水準の公開など）
    - ＊ 目標とするセキュリティ水準の設定・達成度の評価
    - ＊ セキュリティサプライチェーン・リスクマネジメントの実施　等

論点６　実効性の確保

➢ 実効性を確保するにはどうすればよいか。

（主な御意見）

- 事業者が実施したリスク評価と管理策の妥当性を確認してはどうか。
- 法令に基づき国からの立入検査が実施されており、既に実効性は確保されている。
- 事業者に実施可能だと思ってもらえることが重要。組織規模に応じた取組例を記載することにより、実施を促してはどうか。
- サイバーセキュリティの確保に取り組んでいる組織が社会から評価され、メリットに繋がる枠組みを作ってはどうか。
- 民間だけでなく行政もスピード感を持ってPDCAを回すべき。
- 国からの人材育成・資金等に関する支援策を期待する。
- NISCに重要インフラのサイバーセキュリティに関するレッドチームを設置してはどうか。

（対応方針案）

- 毎年NISCが実施している浸透状況調査、制度改善状況調査といった調査の枠組みを活用し、ベースラインを中心に重要インフラ事業者等の取組状況を把握する。
  - ＊ リスク評価と管理策の実施状況についても把握することとするが、その内容の妥当性の確認については、分野によって状況が異なることから、各分野に委ねる。
  - ＊ 各分野において、法令に基づく枠組み等において実効性が確保されることを期待する。
- 分野によって状況が異なることから、組織規模に応じた取組例は記載しないこととする。
- レッドチームの設置については、NISCが主催する「分野横断的演習」において実機演習を実施するなども含めて、引き続き検討する。
- 東京2020オリンピック・パラリンピック競技大会を踏まえ、重要インフラ事業者等に対してリスクマネジメントを一層浸透させる。
  - ＊ 東京大会では、事業者による手順書に沿ったリスクアセスメント及びNISCからのフィードバックを通じて取組の実効性を確保した。
  - ＊ 当該手順書については現行の重要インフラ手引書に反映済み。さらに、分野・事業者ごとに適したリスク評価のアプローチの選択、平時と大規模国際イベント時等におけるメリハリのついた対策の決定等について追記し、説明会やワークショップ等を通じてリスクマネジメントの促進を図る。

論点７　関連文書の整理

➢ 国内外に既に確立された関連文書があるところ、どのように整理すべきか。

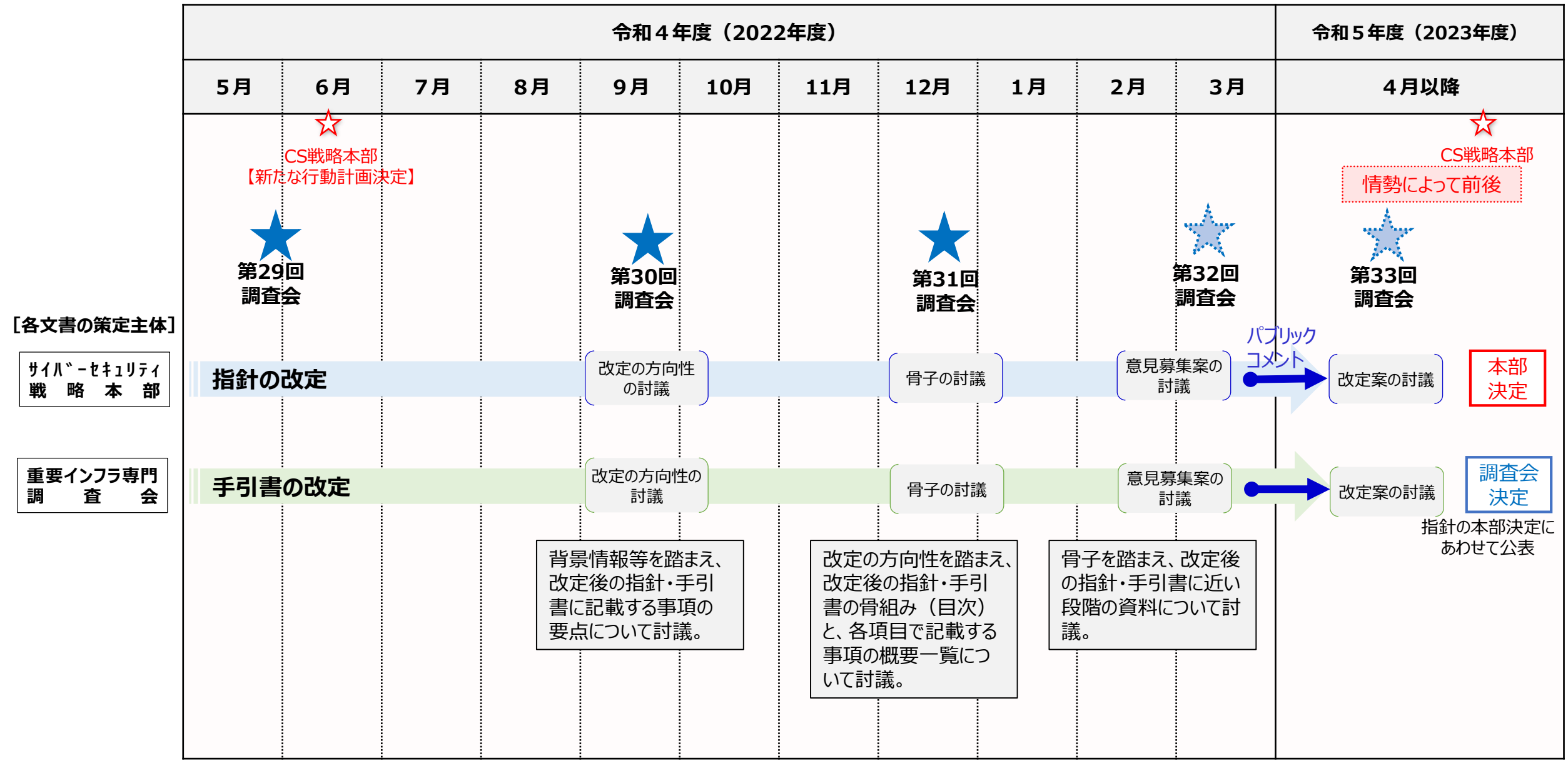
（主な御意見）

- 国内法や国際規格、国際フレームワークなどと整合をとるべき。
- 想定読者を明示すべき。
- 文書構成が複雑であり、シンプルなものに作り直してはどうか。

（対応方針案）

- 想定読者（経営層・CISO・戦略マネジメント層・担当者層）をセクションの冒頭に明示する。
- 今後、記載事項と関連文書の対応関係について、現行指針を踏襲しリスト化する。
- 「政府機関等の情報セキュリティ対策のための統一基準」（サイバーセキュリティ戦略本部決定）との整合をとる。
- 経産省「サイバーセキュリティ経営ガイドライン」をベースに、「組織統治の一部としてのサイバーセキュリティ」という観点がより明確になるよう取組を記載する。【再掲】
- 引用している主要な国際規格であるISO/IEC 27000及びNIST サイバーセキュリティフレームワーク(CSF)について、CSFは重要インフラ向けとして策定されているのに対し、ISO27000は汎用的な情報保護のための枠組みとして策定されており、CSFの方が任務保証の考え方に近いことから、特にCSFとの整合を意識する。
- 米国CPGの取組を参考にする。
    * 米国CPGは、様々な重要インフラ分野・事業者に適用可能となるよう柔軟性を持たせ、効率よく効果が得られると思われる取組を目標としてリストアップしたものであり、日本においても、望ましい取組として活用することができると思われる。
- 文書構成のシンプル化については、指針、手引書、ガイダンスといった文書構成は既に行動計画において規定しており、変更しないこととする。ただし、既存の文章を含めて簡潔な記載に改める。

スケジュール



＊別途、指針・手引書の検討状況を踏まえつつNISCにおいてガイダンスを検討、策定

参考資料

米国CISA サイバーセキュリティパフォーマンス目標（CPG）

経緯

- 2021年7月28日、バイデン大統領は、重要インフラ制御システムのサイバーセキュリティの改善に関する国家安全保障覚書5（NSM-5）を発行した。NSM-5では、連邦政府と重要インフラ事業者が自発的に協力して、重要インフラ分野におけるサイバーセキュリティのパフォーマンス目標を策定することを求めている。これらの目標は、重要インフラ分野の経営者及び運用者が従うべき基本的なサイバーセキュリティの実践についての理解を醸成するためのものである。
- 2022年10月25日、米国CISAは、同覚書を受け、重要インフラ事業者向けとして、分野横断サイバーセキュリティパフォーマンス目標（CPG）を公表した。
- CPGを踏まえて、今後、分野ごとの目標が策定される予定。

概要

- CPGは重要インフラ事業者が自主的に実施すべき共通のセキュリティ対策を列挙したもの。

（主な特徴）

✓ 全ての対策を網羅するものではなく、分野横断的に実施効果の高いと思われる最低限の対策を記載。
✓ 経営層が理解できるよう、平易な表現で具体的な実施事項を記載。
✓ 制御システムのセキュリティ対策にも焦点。
✓ セキュリティ投資の優先順位付けに役立つワークシートを提供。
✓ 各対策と関連性の高いNIST CSFのサブカテゴリーとのマッピングを記載。

（対策の８カテゴリー）

●アカウント・セキュリティ	●デバイス・セキュリティ	●データ・セキュリティ	●ガバナンスとトレーニング
●脆弱性管理	●サプライチェーン/サードパーティ	●対応と復旧	●その他

出典：米国CISA「Cross-Sector Cybersecurity Performance Goals」

欧州連合　域内共通の高度サイバーセキュリティ措置に関する指令（NIS2指令）

経緯

- 2016年、欧州連合（EU）において、「ネットワークと情報システムのセキュリティに関する指令」（NIS指令）が採択された。NIS指令はEU加盟国共通のセキュリティ水準を達成することを目的にしていたが、実施が困難となっている状況。
- 2022年11月、欧州議会とEU理事会は、NIS指令の代替案としてNIS２指令に暫定合意した。EU加盟国は、NIS２指令の発効後21ヶ月以内に国内法整備を完了することが求められる。

概要

- NIS２指令は、重要インフラ事業者のサイバーセキュリティに関し、セキュリティ要件の強化、サプライチェーンのセキュリティへの対応、報告義務の合理化、より厳しい監督措置とEU全域に調和した制裁を含むより厳しい執行要件の導入を図ることを目的としている。
- NIS指令における「基幹サービス運用者」「デジタルサービス提供者」という分類を「基幹事業体」、「重要事業体」に変更し、対象分野を追加した。
- EU加盟国は、対象事業者が以下の事項を含む組織的な対策を講じることを保証しなければならない。

（対策事項）

- ●リスク分析及び情報セキュリティに関する方針
- ●事業継続及び危機管理
- ●ネットワーク及び情報システムの開発・取得・保守に関するセキュリティ
- ●セキュリティ・トレーニング
- ●人的セキュリティ・アクセスポリシー・資産管理
- ●脆弱性の処理開示
- ●インシデント処理
- ●サプライチェーン・セキュリティ
- ●管理策の有効性評価
- ●暗号技術と暗号化使用の指針・手順
- ●多要素認証等

- インシデント報告に関して、24時間以内に最初の報告書を提出し、1カ月以内に最終報告書を提出することを義務化。

出典：欧州議会「The NIS2 Directive A high common level of cybersecurity in the EU」

各国の重要インフラ分野

	日本（14分野）	米（16分野）	英（13分野）	豪（11分野）	EU NIS２指令 （11分野＋７分野）
分野	①情報通信 ②金融 ③クレジット ④航空 ⑤空港 ⑥鉄道 ⑦物流 ⑧電力 ⑨ガス ⑩石油 ⑪化学 ⑫政府・行政サービス ⑬水道 ⑭医療	①通信 ②情報技術（IT） ③金融 ④輸送システム ⑤エネルギー ⑥化学 ⑦政府施設 ⑧上下水道 ⑨公衆衛生・医療 ⑩緊急サービス ⑪食糧・農業 ⑫商業施設 ⑬重要製造業 ⑭ダム ⑮防衛産業基盤 ⑯原子力 (炉・部材・廃棄物)	①通信 ②金融 ③輸送 ④エネルギー ⑤政府 ⑥水道 ⑦保健 ⑧緊急サービス ⑨化学 ⑩食糧 ⑪防衛 ⑫民生用原子力 ⑬宇宙	①情報通信 ②金融 ③交通 ④エネルギー ⑤医療 ⑥水道 ⑦食料・農業 ⑧防衛産業 ⑨データ・クラウドサービス ⑩教育・研究機関 ⑪宇宙	〈基幹事業体〉 ①エネルギー （電力、地域冷暖房、石油、ガス、水素） ②輸送 （航空、鉄道、水上、道路） ③銀行 ④金融市場インフラ ⑤医療 ⑥飲料水 ⑦廃水 ⑧デジタルインフラ ⑨ICTサービス ⑩行政 ⑪宇宙 ※赤字はNIS指令における基幹サービス運用者との差分 〈重要事業体〉 ①郵便・宅配便 ②廃棄物処理 ③化学品 ④食糧 ⑤製造 （医療機器、コンピュータ・電子光学機器、電気設備、機械設備、自動車・トレーラー、その他輸送機械） ⑥デジタルプロバイダー ⑦研究 ※赤字はNIS指令におけるデジタルサービス提供者との差分