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６

安全基準等策定指針・手引書の改定について

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9月20日

◆安全基準等策定指針・手引書の概要

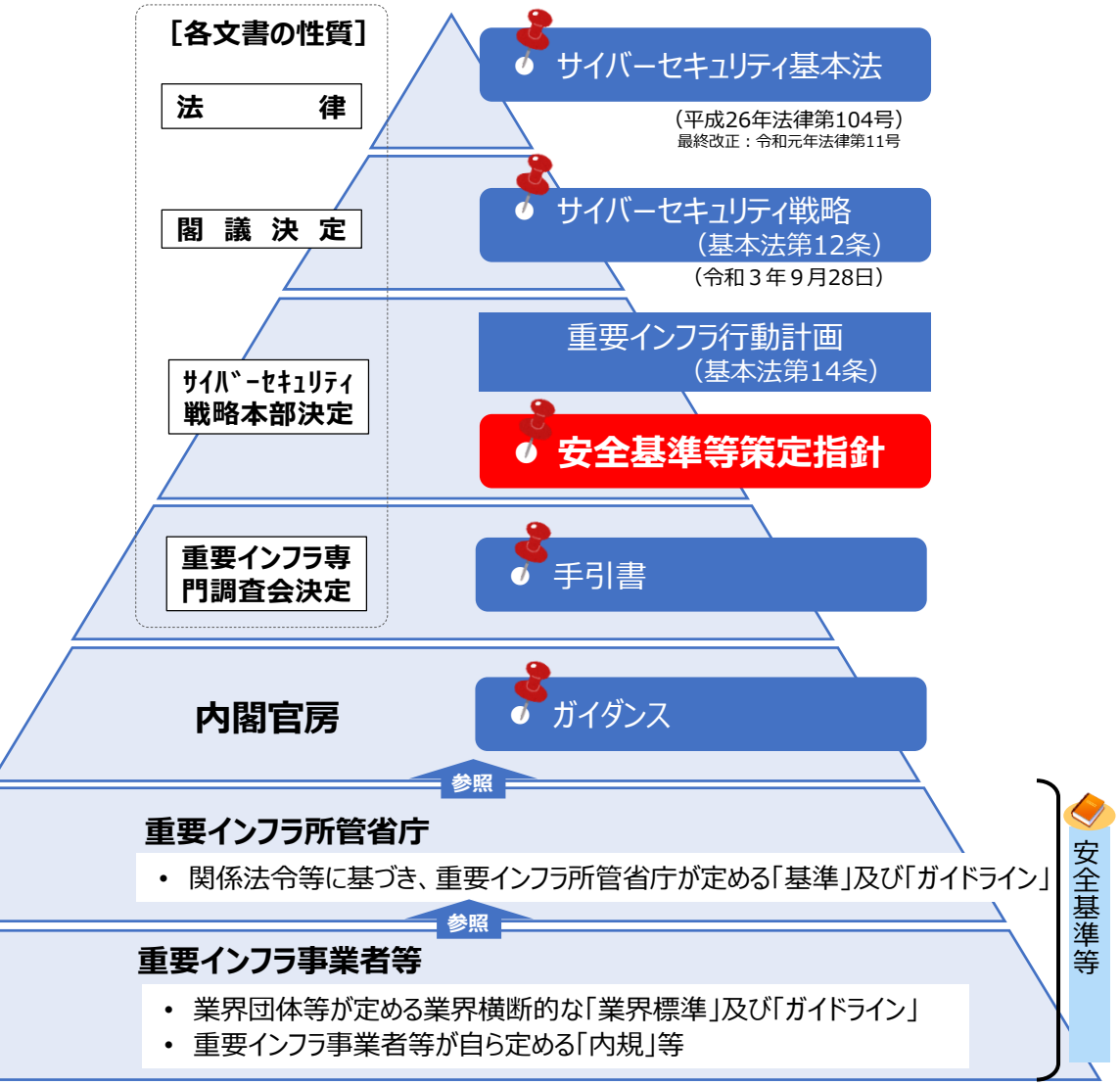
◆改定の目的・進め方・スケジュール

◆論点と指針改定の方向性

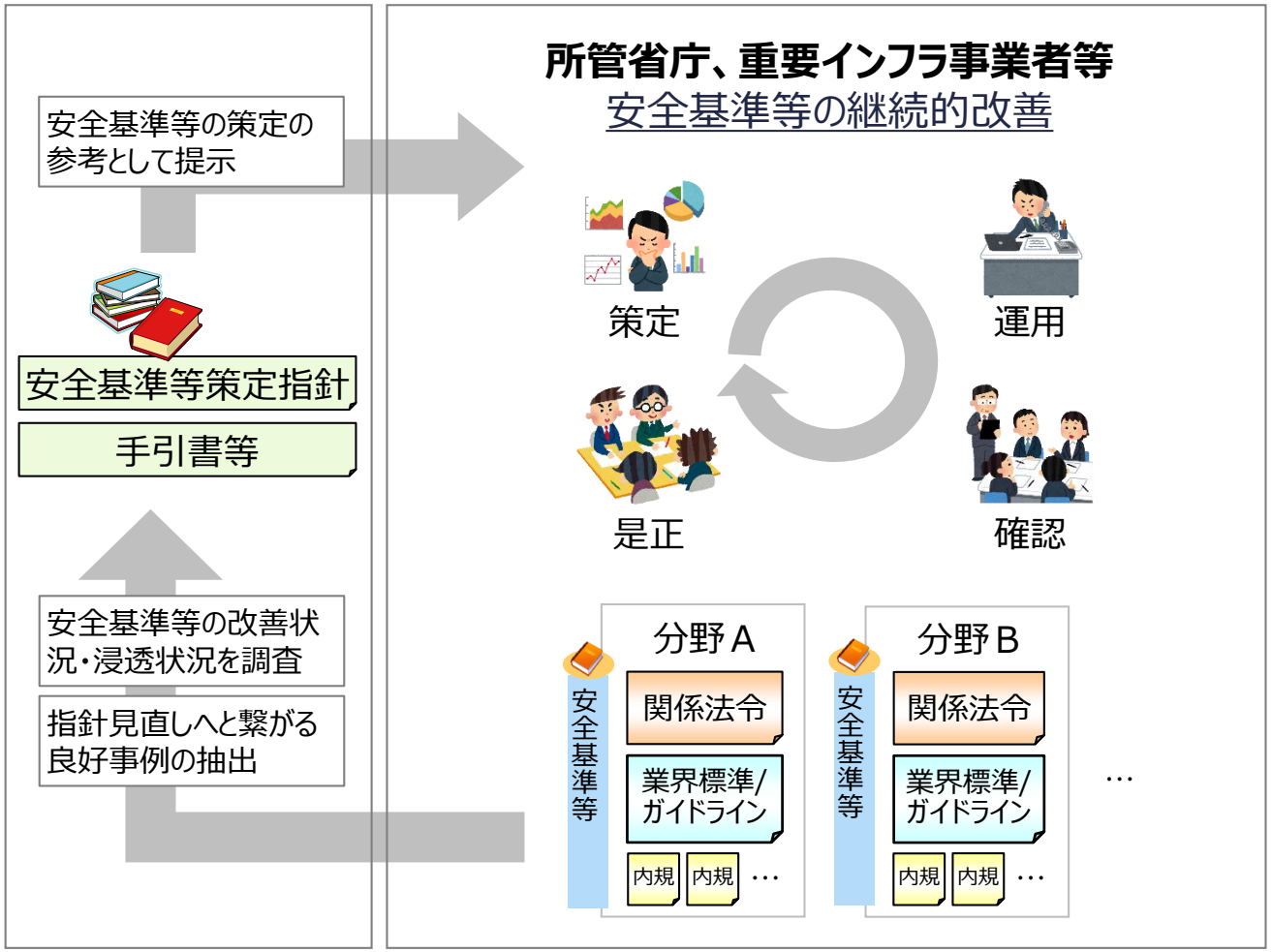
◆手引書改定の方向性

関連文書の位置付けと安全基準等策定指針の概要

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。



【安全基準等策定指針の活用方法】

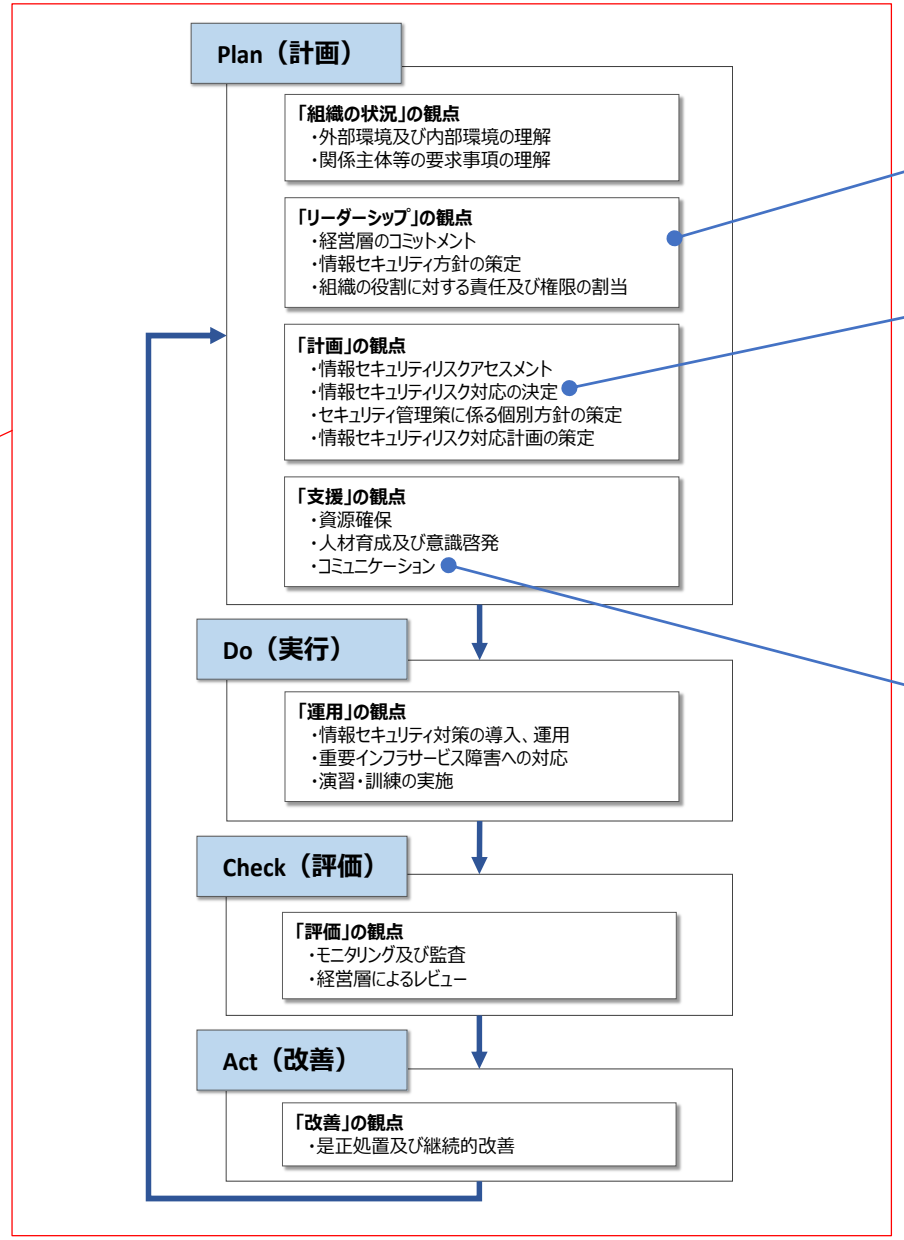


現行の「安全基準等策定指針」の構成

Ⅰ．目的及び位置付け
1. 重要インフラにおける情報セキュリティ対策の重要性
2.「安全基準等」とは何か
3. 指針の位置付け
4. 指針を踏まえた「安全基準等」の継続的改善及び浸透への期待

Ⅱ．「安全基準等」で規定が望まれる項目
1. 策定目的
2. 対象範囲
3. 関係主体の役割
4. 対策項目
- 4.1.「Plan（計画）」の観点
  - 4.1.1.「組織の状況」の観点
  - 4.1.2.「リーダーシップ」の観点
  - 4.1.3.「計画」の観点
  - 4.1.4.「支援」の観点
- 4.2.「Do（実行）」の観点
  - 4.2.1.「運用」の観点
- 4.3.「Check（評価）」の観点
  - 4.3.1.「評価」の観点
- 4.4.「Act（改善）」の観点
  - 4.4.1.「改善」の観点

ISO27001（情報セキュリティマネジメントシステム）をベースに構成



経営層の実施事項を記載

個別の取組を記載
・人的管理
・資産管理
・アクセス制御
・バックアップ
・ログ取得
・脆弱性対策
・委託先管理　など

経営層と実務者層の定期的なコミュニケーションの重要性について言及

「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」概要

- 「重要インフラの情報セキュリティ対策に係る第４次行動計画」では、**情報セキュリティ確保に係るリスクアセスメントの考え方や具体的な作業手順に関するフレームワークを「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（第１版）」**（以下「手引書」という。）**として取りまとめ**、重要インフラサービスの安全かつ持続的な提供の実現を図る観点から**リスクアセスメントに係る主要なプロセスを整理**している。

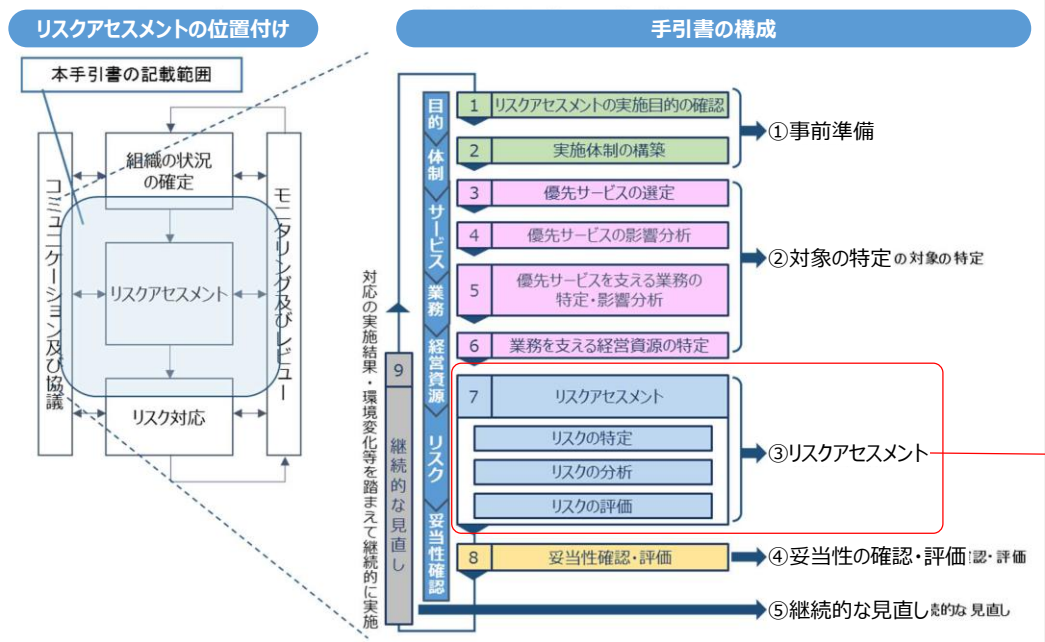
【手引書の概要】

目的　重要インフラ事業者等におけるリスクアセスメントの理解を深め、その精度や水準の向上に寄与するとともに、**重要インフラ事業者等による自律的な情報セキュリティ対策を促進**。

内容　各重要インフラ事業者等が社会経済システムの中で果たすべき役割・機能を見極め、これを発揮するために、許容できないリスクが無い状態（＝安全）を確保しつつ、サービス提供を継続する」という観点から、**情報セキュリティリスクの特定・分析・評価を実践するための手順を記載**。

【リスクアセスメントの対象と手引書の構成】

- リスクアセスメントのプロセスを**「事前準備」「対象の特定」「実施」「妥当性の確認・評価」「継続的な見直し」の５つのステップに分割し、各ステップにおける手順を記載**。

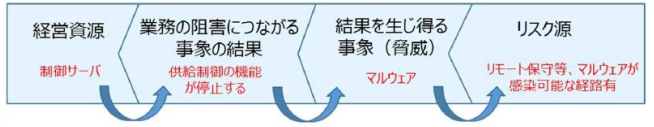


※リスクアセスメントの精度や水準は事業者等の力量に依存するため、本手引書ではリスクアセスメントの観点や参考となる作業手順を示し、どのような事業者等でも一定以上の水準が確保されることを企図としている。

【リスクアセスメントの流れ】

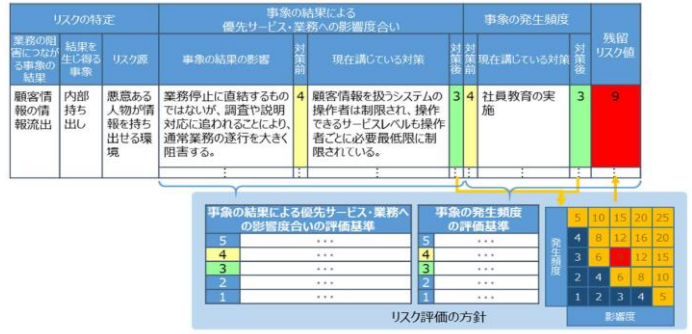
リスクの特定

- 優先サービスの提供に必要な業務に係る**経営資源の洗い出し**



リスクの分析

- 「事象の結果による優先サービス・業務への影響の度合い」と「事象の発生頻度」を分析し、**対策を実施しても残存するリスク（残留リスク値）を導出**



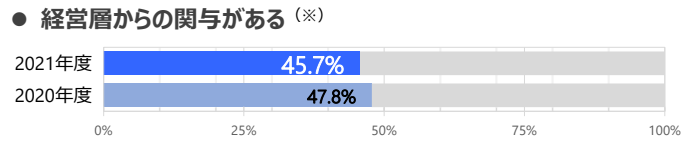
リスクの評価

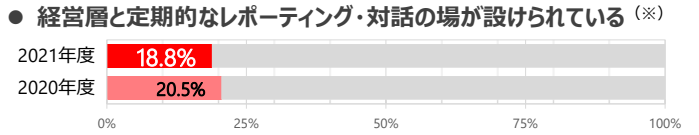
- 洗い出されたリスクから、経営層による全社的な意思決定に基づく**リスク対応の実施対象とするリスクを選別**し、そのリスクに係る**組織内の責任主体を明確化**する。

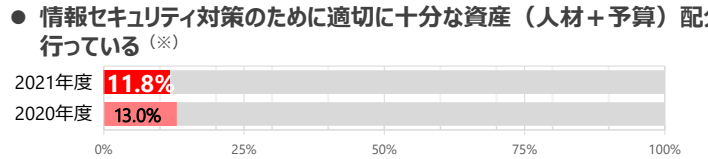
重要インフラ事業者等における取組の実施状況（2021年度浸透状況調査結果）

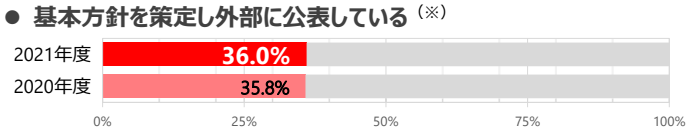
- 重要インフラの各分野における**情報セキュリティ対策の実施状況は多くの項目において高い水準で推移**しており、**安全基準等は浸透しつつある**と一定の評価ができる。一方で、項目によって実施状況に差があり、**Plan（計画）に係る項目として比較して、Do（実行）、Check（評価）に係る項目の実施状況は相対的に低い**ことから、これらを改善していくことが今後の課題である。
- 複雑化・巧妙化する情報セキュリティ上の脅威に対処していくためには、環境の変化にあわせて対策の見直しと改善を行っていく必要がある。重要インフラ事業者等においては、**PDCAサイクルを構築し、着実に情報セキュリティの確保に向けた取組を進めていくことが期待**される。

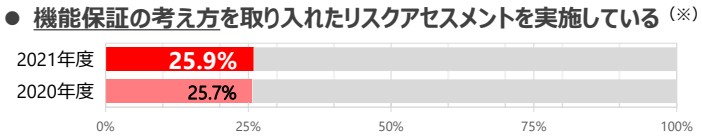
各取組の実施状況［過去度の調査との比較］

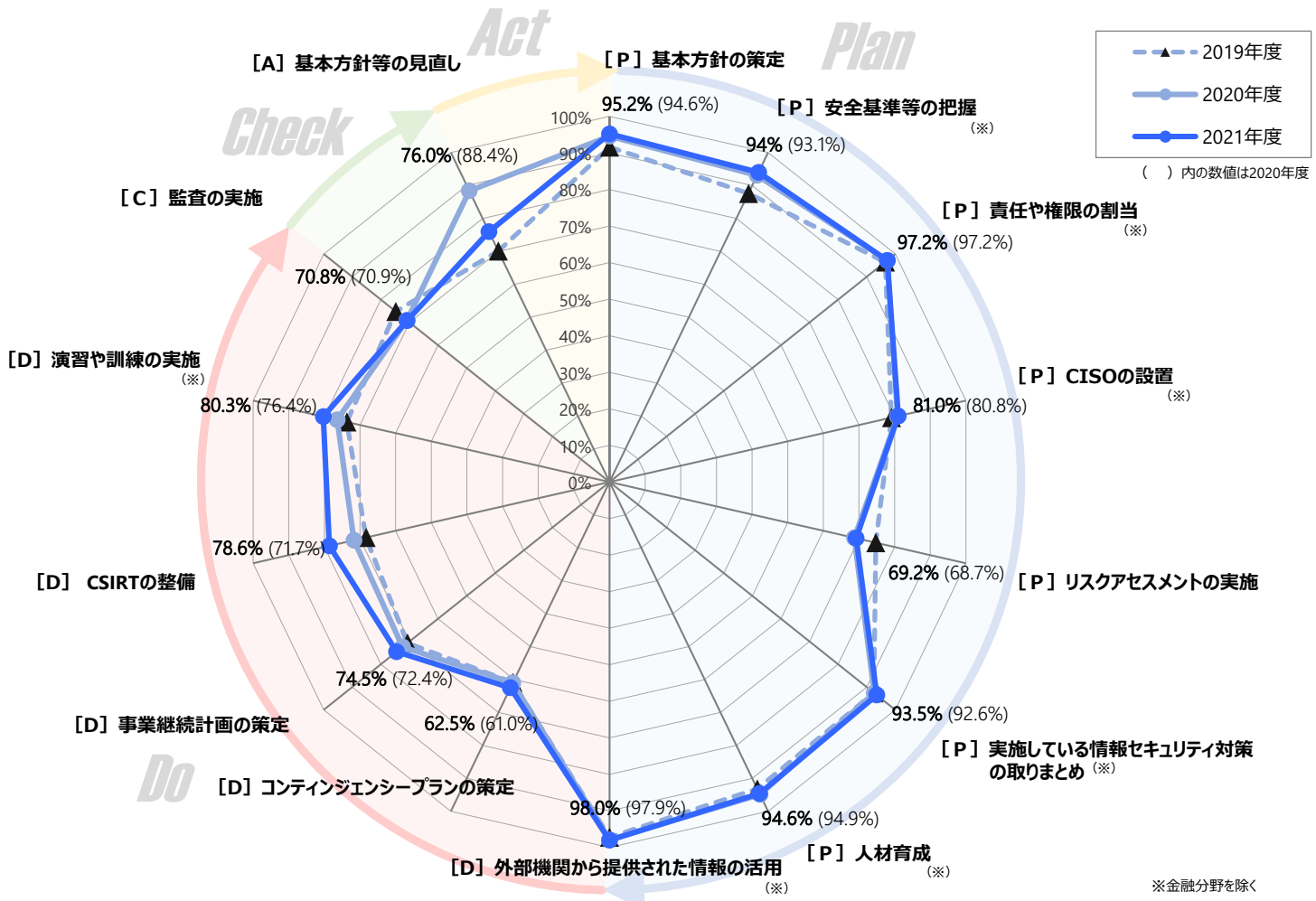












◆安全基準等策定指針・手引書の概要

◆改定の目的・進め方・スケジュール

◆論点と指針改定の方向性

◆手引書改定の方向性

改定の目的と進め方

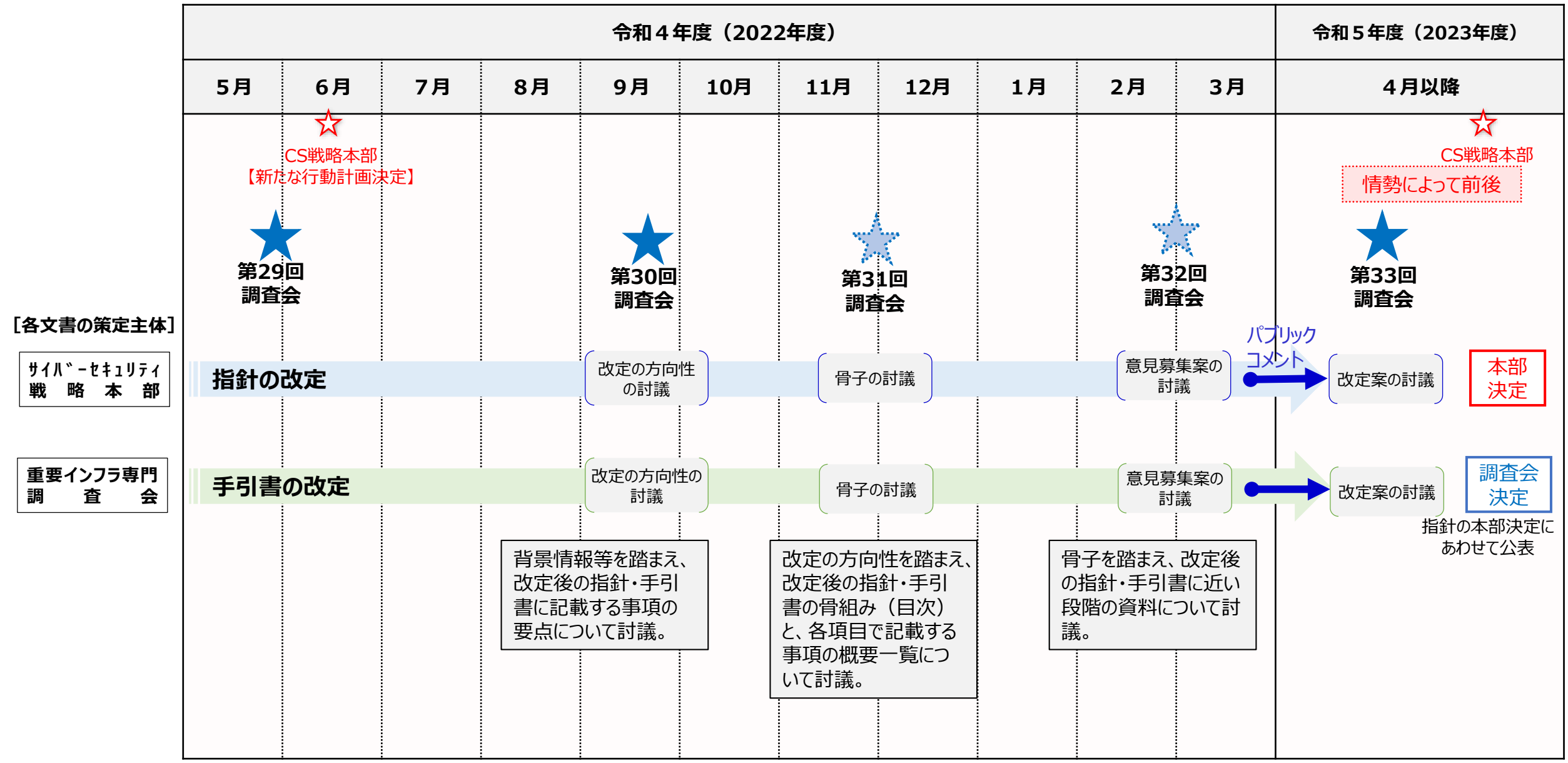
１．目的

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について安全基準等策定指針及び手引書の見直しを行う。

２．改定の進め方

- ◆ 指針・手引書の内容を連動させ、同時に改定の検討を進める 。
- ◆ NISCが指針・手引書の事務局案を作成し、重要インフラ専門調査会で審議する。
- ◆ 各文書の性質を踏まえて内容をスリム化し、手順等の詳細は下位文書に記載する。
- ◆ 政府統一基準群、サイバーセキュリティ経営ガイドライン等の関連文書との整合性を確保する。
- ◆ 重要インフラ調査会での審議と並行して、セプター等の枠組みを活用し重要インフラ事業者等との調整を行う。
- ◆ 指針については2023年度前半のCS戦略本部決定を目指し、あわせて手引書を重要インフラ専門調査会で決定する。

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

◆安全基準等策定指針・手引書の概要

◆改定の目的・進め方・スケジュール

◆論点と指針改定の方向性

◆手引書改定の方向性

新たな行動計画における安全基準等策定指針に関する記載

➢ 新たな行動計画では、①組織統治、②サプライチェーン、③自組織に適した防護対策、④その他の観点から指針を改定する旨を記載。

○ **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。

これまでの重要インフラ専門調査会委員からの御意見

【ベースラインの明示】

◆ **重要インフラ事業者等が最低限実施すべき取組（ベースライン）を明示し、一定のセキュリティレベルを確保すべき。**

- ①重要サービスインフラの設計・構築・運用、②情報管理、③人材管理、④脅威ベース検証、⑤組織・ガバナンス体制、などについて、分野共通なものと分野・業態別のものを規定することが考えられる。
- 事前のリスク分析を義務化することを考えてはどうか。
- 米国の一部の州ではIT専門の取締役を置くよう法律で義務付けている。

【成熟度評価とリスク評価の活用】

◆ **マチュリティ（成熟度）評価とリスク評価による体制強化のフレームワークを整備すべき。**

- C2M2等の成熟度の考え方を取り入れるべき。
- 経営陣が目標設定を行いやすくするため、成熟度を自己評価し、その結果を相互交換・自主的なベンチマークが出来る仕組みを作ってはどうか。
- 自主的な能力成熟度評価によるギャップ分析と脅威シナリオベースのリスク評価を通して、自律的に態勢強化を図るフレームワークの整備を促すべき。
- システム障害が事業に与える影響を評価するなどの取り組みが必要ではないか。

【サイバーセキュリティに対する意識の改革】

◆ **セキュリティ対策が単なるコストではなく企業価値向上への重要施策であるという認識を経営者に啓発すべき。**

- 例えば、既に「デジタル・ガバナンス・コード」においてサイバーセキュリティが評価項目になっている。その他の指標への組み入れや政府からの取り組み喚起を積極的に行うべき。
- セキュリティ対策によって、サービスインが早くなるといった付加価値を与えられる取組が必要ではないか。

【サプライチェーン対応】

◆ **サプライチェーンに関する指針を策定すべき。**

【ランサムウェア対応】

◆ **ランサムウェア被害にあった際の対処に関するガイドラインを作成すべき。**

【人的資源のセキュリティ】

◆ **重要インフラの従事者に対するセキュリティクリアランスを設けるべき。**

【取組状況の調査】

◆ **事業者の声を拾って次の施策に活かしていくべき。また、事業者へ還元されるものがあると回答へのモチベーションになるのではないか。**

最近のインシデントの類型と必要な対策

➢ 主なインシデントと対策

- **ランサムウェア**に感染しデータを暗号化された。
  （対策）侵入を前提とした多層防御を備えたシステム設計、バックアップの実施、侵入を前提とした多重防御
- **マルウェア（Emotet）**に感染し情報が漏えいした。
  （対策）不審メールへの警戒意識の醸成、マクロの自動実行の無効化、不正通信の検知と遮断、侵入を前提とした多重防御
- **委託先や海外拠点**のセキュリティアップデートが適用されていないVPNの脆弱性を攻撃された。
  （対策）サプライチェーン管理、インターネットに接続する資産管理、セキュリティアップデートの適用
- **外部サービスにおける設定不備**により情報が漏えいした。
  （対策）サービス提供前の脆弱性診断の実施、サプライチェーンに関わる事業者とのコミュニケーション
- **外部サービスの障害**によりサービスが停止した。
  （対策）リスクに応じた外部サービスの利用、外部サービスの不具合を前提とした多重化・多様化等による代替手段の確保
- **システムの設計・運用不備やアクセス集中による高負荷**により、サービスが停止した。
  （対策）サイバーセキュリティの確保を念頭に置いたシステムの企画・設計・運用、サービス提供前の脆弱性診断の実施
- **私有端末に内部情報が自動バックアップ**されており、**フィッシング**によって情報が漏えいした。
  （対策）自動バックアップ設定の確認、不審メールへの警戒意識の醸成
- 職員が意図的に資産・情報を**外部に売却**した。
  （対策）資産管理の徹底、セキュリティクリアランスの導入

既に現在の安全基準等策定指針に関連する記載があるが、
より「わかりやすく」「具体的に」実施を求めることが必要ではないか

➢ インシデント横断的な対策

- 組織としてリスク認識を持ち、リスクマネジメントシステムを構築し、必要なリソースを配分することが必要
- インシデントの発生は完全には防げないとの前提で、インシデントの発生を想定した計画や対策が必要
- サプライチェーンに関わる事業者からの積極的な協力が必要

経営層が自ら認識するだけではなく、CISO、戦略マネジメント層、担当者層といった各階層からのボトムアップも重要ではないか

改定に向けた論点（案）

①新たな行動計画に記載した指針改定項目について、どのような具体的取組を掲載するか。

＊「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」という考え方の分かりやすい説明が必要ではないか。
＊機器、ソフトウェア、データ、サービス等のサプライチェーンの構成要素について、サプライチェーン全体での対策強化をどのように実現するか。
＊組織によって風土等が異なることを踏まえつつ、自組織に適した対策の実施を促す。
＊制御システム・人材育成等に係る対策は、従来より難しい課題として残ってきたところ。

②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軸足を置いた考え方）による取組をさらに促進するにはどうすればよいか。

＊調査結果によれば、「任務保証の考え方」が浸透していない。

③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。

＊調査結果によれば、横ばいのまま改善しない取組項目がある。指針の記載内容は「あくまでも望ましい取組の例示」とされており、メッセージ性が弱いのではないか。

④成熟度による評価を促進するにはどうすればよいか。

＊重要インフラ事業者等には、自組織に適した対策を決定・実施するリソース（人材、予算、知見等）が不足していると思われる組織、先進的な組織が混在している。

⑤実効性を確保するにはどうすればよいか。

＊国として、最低限実施すべき取組が実施される状況を実現するために、何をすればよいか。
例えば、国によるチェックの強化により実施を促すことが考えられるが、どうか。

⑥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。

＊関連文書名を提示するだけでよいか、それとも再整理したものを改めて指針として示すべきか。

指針改定内容案①-1　組織統治

➢ リスクマネジメントには、組織全体のPDCAと対策系のPDCAがあり、両者の関係を明確にしつつ、組織統治の一部としてサイバーセキュリティ「も」実施するという考え方を浸透させる。

（組織統治に関する記載例）

- ◆ 経営層は、組織統治において、リスク管理措置を承認し、その実施を監督し、内外に説明する**責任**を負っており、**リスクにはサイバーセキュリティリスクが含まれる**。
- ◆ 組織として、**内部統制システム**が構築されていることを前提とし、そこで**サイバーセキュリティに関する事項も取り扱う**こと。
- ◆ 経営又はリスクマネジメントの方針にあたる文書において、「**サイバーセキュリティが阻害されることがサービス提供の停止のリスクの一つ**」「**リスクマネジメントの対象としてサイバーセキュリティに関する事項を含める**」といった要素を盛り込むこと。
- ◆ 各階層の**役割と責任**を明確化すること。（参考として、次スライドのような図を掲載）
- ◆ サイバーセキュリティに関する責任者（以下「CISO」という。）を**取締役会から設置**すること。
- ◆ CISOがサイバーセキュリティリスク及びそれが事業運営に及ぼす影響を理解し評価するために**十分な知識及び技能**を保持できるよう研修を定期的に受けるなどの取組を行うこと。
- ◆ サイバーセキュリティに関する事項を含めて**情報開示**すること。例えば、重大なサイバーセキュリティインシデントを受けたと判断した後のサイバーセキュリティインシデントに関する情報や、CISOが十分な知識及び技能を保持していることに関する情報など。
- ◆ 体制の適切性を担保するための**監査**（内部監査及び監査役等・社外取締役によるもの）を実施すること。

（米国の例）重要インフラ制御システムのサイバーセキュリティパフォーマンス目標と目的（2021.09暫定）

1. リスクマネジメントとサイバーセキュリティガバナンス
   - マネジメントシステムに対する既知のリスクを特定し、文書化し、優先順位をつける。
   - 統制システム資産の許容される使用及びアクセスの概要を含む、特定された優先度の高いリスクを受容、回避、軽減、又は移転する方針を確立し、実施する。
   - サイバーセキュリティプログラムに対する効果的なマネジメントの支援を実証する。
   - これらのパフォーマンス目標で特定された目的、およびその他の部門または企業のサイバーセキュリティ要件（有資格者の費用を含む）を実行するために十分な専用の資金を定期的に提供する。

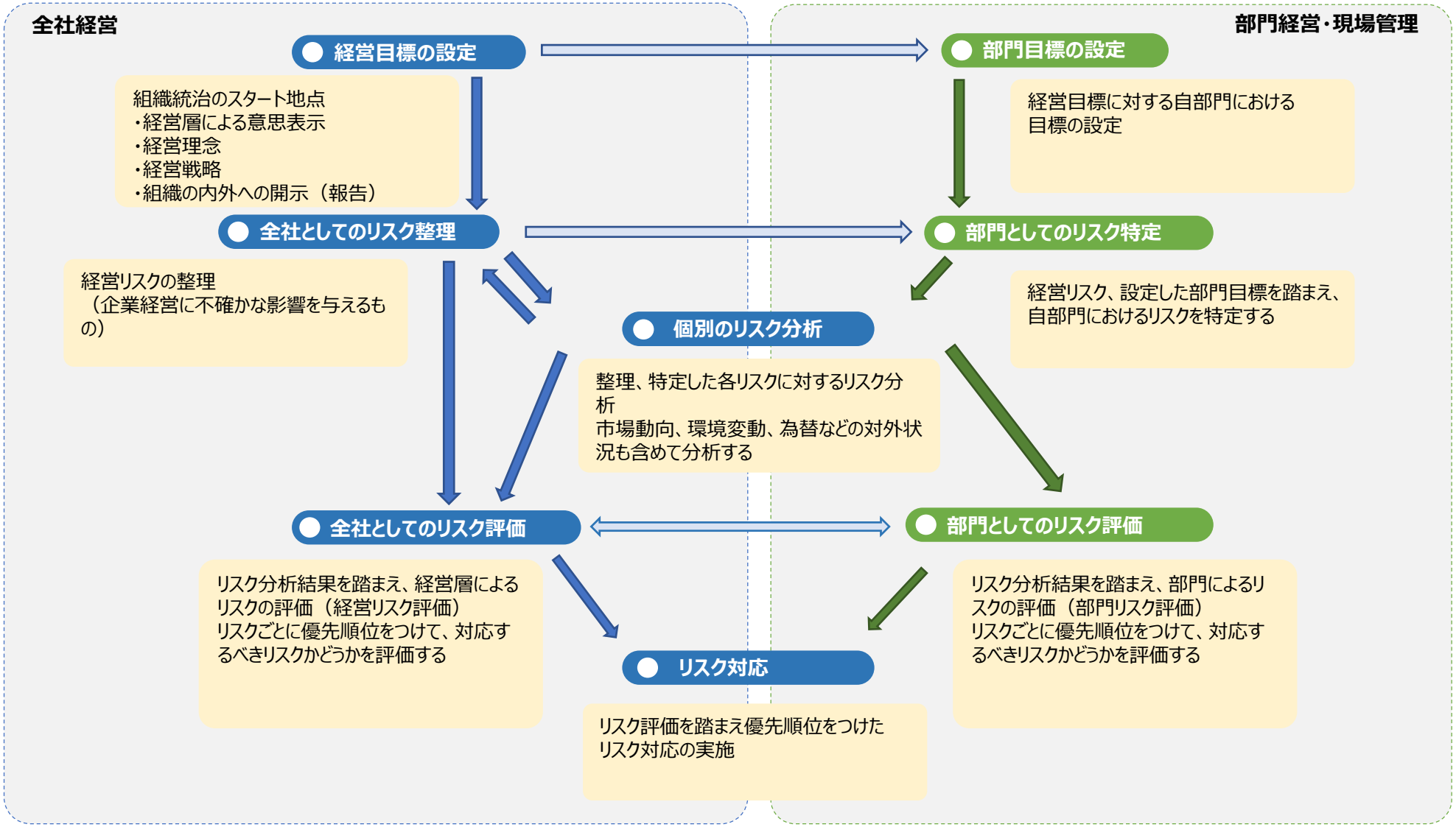
（EUの例）NIS2指令案

第17条　ガバナンス

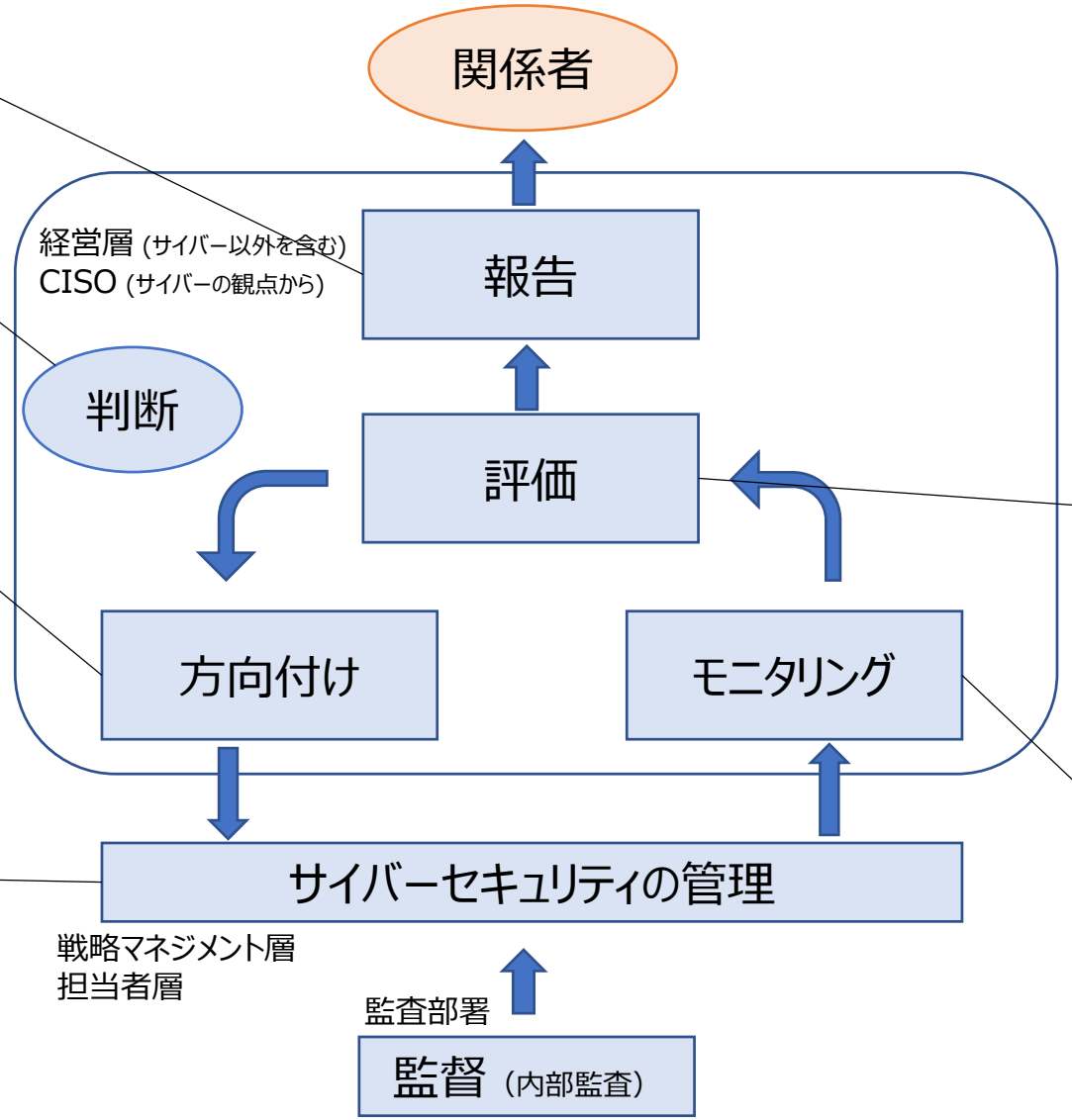
1　加盟国は、重要な事業体のマネジメント層が、第18条を遵守するために当該事業体がとるサイバーセキュリティリスク管理措置を承認し、その実施を監督し、当該事業体が本条に基づく義務を遵守しない場合に説明責任を負うことを確保するものとする。

2　加盟国は、マネジメント層のメンバーが、サイバーセキュリティリスク及び管理慣行並びにそれらが事業体の運営に及ぼす影響を理解し評価するために十分な知識及び技能を得るための特定の研修を定期的に受けることを確保しなければならない。

組織統治（リスク対応まで）のイメージ例



セキュリティガバナンスのイメージ例



経営層：リスク管理の責任者として各主体に状況を報告する。

CISO：有事の際は事業継続・停止の是非等を経営層の一員として判断する。

経営層：経営戦略やそれに基づくリスク管理の方針を提示する。
CISO：経営もしくはそれに近い立場からリスク管理方針をサイバーセキュリティの観点から解釈し、サイバーセキュリティの目的・目標と、その実現に必要な体制や経営資源の提供を設定する。

戦略マネジメント層：CISOから示された目的・目標を受け止め、それを実現するための管理目的・管理策を設定し、管理策の適用状況をモニタリングする。担当者を統括する。

方向付け、モニタリング及び評価が適切に遂行されていることを確認し、必要に応じて問題の改善を促す。

監査役等・社外取締役

監督

経営層： CISOから投資効果の影響や目的・目標の達成度評価の報告を受ける。リスク管理方針が達成できたか、リスクが変化していないかを評価し、必要に応じてリスク管理方針の修正を行う。
CISO：管理策は適切に実施されたか、体制や経営資源は適切であったか、インシデントは減少したか、法令違反は起きていないか、目的・目標は達成されたかを評価する。

経営層：経営戦略やそれに基づくリスク管理の方針の前提となる経営環境の変化をモニタリングする。
CISO：サイバーセキュリティマネジメントの一連の活動の進捗・達成状況等とあわせて、投資効果や目的・目標の達成度を評価するための有効な指標によってモニタリングする。

「情報セキュリティガバナンス導入ガイダンス」経済産業省、2009.6 を参考に作成

指針改定内容案①-2　サプライチェーン

- リスクマネジメントの一部として、サプライチェーン・リスクマネジメントに取り組む旨を安全基準等策定指針に記載する。
  - 対応すべき代表的なリスクとして、「不正機能等の埋め込み」「サービスの供給途絶」「外部サービスにおける情報の取扱い」を挙げる。
  - 事業者間の契約を通し、サプライチェーンのセキュリティ対策の確認等を行うことで実効性を担保する。
- 重要インフラ及びサプライチェーン事業者の対策例を政府統一基準群、NIST SP800-161等を参考に検討し、ガイドラインに記載する。
  - サプライチェーン、海外拠点等の**関係者全体にわたる対策状況の把握と防護対策**の実施
  - 重要インフラ事業者等・サプライチェーン等に関わる事業者間での**役割と責任の明確化**
  - クラウドサービス等の**外部サービスの選定の考え方**の活用（例：ISMAP）
  - サプライチェーン全体での脆弱性情報やサイバーインシデントなどの適切な**情報共有**の実施（例：SBOM）
  - サプライチェーン等に関わる事業者との**合同訓練**
  - サプライチェーンの下流における契約履行に係る**セキュリティ対策費用を経費として評価**　など

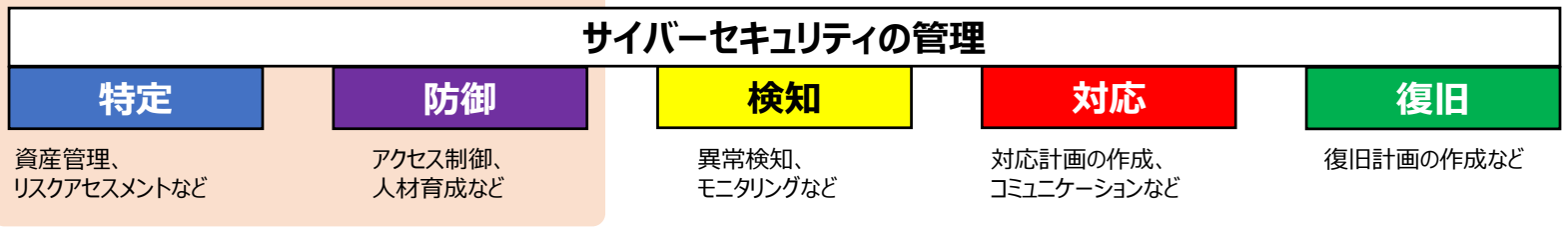
対応すべき代表的なリスク例	生じうる事象	ガイドラインで示す対策例（イメージ）	参考
調達システムに対する • セキュリティ対策の未実施 • 不正な変更	• 情報漏えい • 重要インフラサービスの停止	• 調達過程における一貫した品質管理が担保できることを選定基準に取り入れる • 指定したセキュリティ要件が実装されているか、不正プログラムが混入していないかを確認する検査体制の構築	• 政府機関等の対策基準策定のためのガイドライン（以下「政府調達ガイドライン」）p167
• （委託先ではなく）再委託先の従業員による不正な変更	• 情報漏えい • システム破壊	• 再委託の禁止 • 委託先が再委託先を監督し責任を負うことが可能な体制であるかの確認	• 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書（以下「政府調達仕様書策定手引書」） p8,12
• 調達システムに対する部品交換等の維持管理役務の提供途絶 • 外部サービスの提供途絶 • 自然災害等による委託役務の停止・縮退	• 重要インフラサービスの停止	• 部品の供給役務の継続提供の担保 • 供給者の事業計画や提供実績等の確認 • 委託先の事業実施場所の確認、立地条件の考慮	• 政府調達ガイドライン p120
外部サービス利用における • 情報の取扱いに関する設定ミス • 国内外のセキュリティ管理の仕組みの違い	• 情報漏えい • 重要インフラサービスの停止	• 信用できるサービスを選定 • 情報の返却や抹消などについて確実に確認できる手段を定め、合意をとる	• 政府情報システムのためのセキュリティ評価制度（ISMAP） • 政府調達仕様書策定手引書p13

サプライチェーン： 一般的には、取引先との間の受発注、資材の調達から在庫管理、製品の配送まで、いわば事業活動の川上から川下に至るまでのモノや情報の流れのこと。これらに加えてさらに、IT におけるサプライチェーンでは、製品の設計段階や、情報システム等の運用・保守・廃棄を含めてサプライチェーンと呼ばれることがある。(「重要インフラのサイバーセキュリティに係る行動計画」より)

指針改定内容案①-3,②　自組織に適した防護対策・任務保証

- 組織に応じた防護策を決定できるようにするため、NIST CSFなどを参考に、自組織の特性やリスクを特定した上で、①サイバーセキュリティの取組の現在の成熟度に係る自己評価、②自組織における本来あるべき状況や要件との差異の分析、③分析結果を踏まえた自組織に不足している対策の優先順位付け、④具体的な対策の実施を繰り返すこととする。
  - 詳細については手引書に記載する。
- 任務保証の考え方を具体化するにあたり、NIST SP800-53などを参考に検討し追記する。

NIST CSFにおける
セキュリティ対策の５分類　→



現行の安全基準等策定指針が主にカバーしている部分

現行の安全基準等策定指針では、「早期検知の仕組みの構築」「コンティンジェンシープラン及び事業継続計画の策定と運用」「CSIRTの整備」「演習によるスキルアップ」等を規定

対応・復旧に至らないことが望ましいものの
サービス停止による影響を最小限に抑えることも重要

（NIST SP800-53などを参考とした、任務保証の考え方による取組イメージ例）
・自組織のサービス停止が社会経済に与える影響の把握　　・重要システムや機能の特定
・復旧までに許容可能な時間の設定　　・他の重要インフラなどからのニーズの理解
・社会経済に与える影響を最小化するための復旧優先順位などの復旧方針の検討

「任務保証の考え方を踏まえたリスクアセスメント」「事業継続計画の策定」「CSIRTの整備」「インシデント発生時の情報共有体制の構築・共有」
「インシデント発生時にスムーズに判断・対応できるようにするためのトレーニング」などの対策へ

コンティンジェンシープラン：重要インフラ事業者等が重要インフラサービス障害の発生又はそのおそれがあることを認識した後に経営層や従業員等が行うべき初動対応（緊急時対応）に関する方針、手順、態勢等をあらかじめ実行面から具体的に定めたものを指す。
事業継続計画：機能保証の考え方を踏まえ、重要インフラ事業者等が重要インフラサービス障害により影響を受けた重要インフラサービスを許容可能な時間内に許容可能な水準まで復旧させることを目的して、その復旧に向けた目標水準、優先順位その他の方針、手順、態勢等をあらかじめ定めたものを指す。（「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」より）

指針改定内容案①-4　制御システム

- 現行指針ではCSMS認証基準(IEC62443-2-1)をセキュリティ管理策の参照先として挙げ、また、「制御システム関連部門の人材が必要となることについて考慮」すべき旨を記載。
- 制御システムは独自仕様の機器や通信プロトコルで構成される、閉域環境で稼働するといったことから、依然としてサイバーセキュリティに係るリスク認識が希薄な場合がある。他方、DXの進展により、制御システムにおいても汎用機器や共通規格の通信プロトコルでの運用が浸透。
- このため、組織全体のリスクマネジメントの中で、制御システムのリスクについても適切に評価し、リスク対策を講じるよう追記する。
- 個別の対策については、従来のCSMS認証基準に加え、NIST SP800-82*等を参考とし、制御システムに求められるリスクベースのリスクアセスメント、プラクティス、参考文献等を手引書に記載する。

*Guide to Industrial Control Systems (ICS) Security　産業用制御システム（ICS）セキュリティガイド

制御システムに関する誤解とリスク例

◆「インターネットとつながっていないからセキュリティ対策は不要」
- リモート監視・保守やワイヤレス通信などの接続箇所がある可能性
- USBメモリなどを介して感染（2010年 Stuxnet）

◆「ファイアウォールを導入しているので問題ない」
- ファイアウォール製品の脆弱性管理、設計管理

◆「うちの会社が狙われるわけがない」
- 内部犯のリスク
- その認識が狙いやすいと思われる

◆「制御系のプロトコルが分かっている攻撃者はいない」
- 汎用OS、共通プロトコル化の流れ
- 仕様書やデフォルトパスワードは公表されている

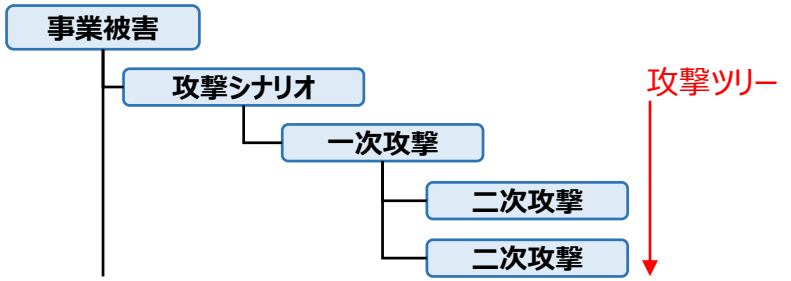
◆「安全対策、冗長化をしている」
- 安全規格標準に適用していればセキュアであるわけではない
- 安全計装自体が攻撃されることもある（2017年 TRITON）

安全基準等策定指針

制御システムについてもサイバーリスクが存在しうるという認識のもとで、リスクアセスメント、リスク対策を実施する

手引書

CSMS認証基準、NIST SP800-82、IPAガイド等を参考とし、制御システムに求められるリスクベースのリスクアセスメント、プラクティス、参考文献等を記載



（例）事業被害ベースのリスクアセスメントにおける攻撃リスク分析

出典：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～」

指針改定内容案③⑤　ベースライン・実効性

- 組織によって状況は異なることから、指針の記載内容は「あくまでも望ましい取組の例示」とされているところ、組織によらず必要な取組を最低限実施すべき取組（ベースライン）として記載する。
- 特に、組織統治・リスクマネジメントは、個別具体の対策と性質が異なりあらゆる組織において不可欠と思われるため、ベースラインと位置付けることが考えられる。
- さらに、対策の改善を促すにはチェック機能の強化が効果的と思われるため、監査・情報開示の取組を強化する。

（ベースラインの例）

① サイバーセキュリティに関するリスクマネジメント（体制構築、情報開示など）システムを整備し実効性のある活動を実施すること。
② どの分野でも一般的に求められる具体的な取組事項（ログ管理、バックアップなど）を実施すること。
③ 組織として最低限確保すべき任務保証のレベル（例えば、サービス停止時間を１時間以内に抑えるなど）を明示すること。

（実効性確保のために、指針改定にあわせて今後の検討事項の例）

- 重要インフラ事業者等の取組状況を把握するため、国は、引き続き選択肢式の調査の実施に加え、開示情報の確認や聞き取り調査などの調査方法を検討する。
- 経営層がサイバーセキュリティリスクを認識し、的確な体制構築、投資の決定、対策の指示を実行できるように、国は、経営層の意識向上につながるプログラム策定の参考となるカリキュラム例を提供する。

指針改定内容案⑥　関連文書の整理

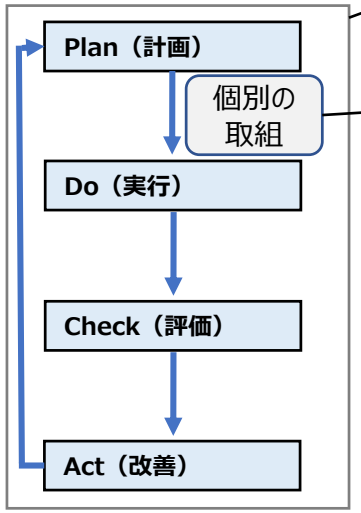
- 組織統治におけるサイバーセキュリティは各取組の前提となる事項でることから、新たなセクションを設けて冒頭に記載。
- セキュリティ方針はリスクマネジメントの過程で策定される文書であるため、わかりやすくなるよう構成を整理。
- 従来のリスクマネジメントに関する事項において、NIST CSFを参考に自組織に適した防護対策に関する記載を充実。

現状

I. 目的及び位置付け

II.「安全基準等」で規定が望まれる項目

1．策定目的
2．対象範囲
3．関係主体の役割
4．対策項目



リスクマネジメントに関するフレームワークを分離

改定（案）

I. 目的及び位置付け

II. 組織統治におけるサイバーセキュリティ（新設）

サイバーセキュリティ経営ガイドライン、
サイバーセキュリティ関係法令Q&Aハンドブックを参照

III. リスクマネジメントに関して実施すべき項目

ISO27001、NIST CSFを参照

IV. セキュリティ方針に規定すべき項目

1．策定目的
2．対象範囲
3．関係主体の役割
4．対策項目

政府統一基準群、NIST SP800シリーズを参考文書として掲載

- 具体的な内容については、C2M2やCIS Controlsなどの取組を候補とすることが考えられるが、**今後**、各分野のセプターへのヒアリング等を実施しながら、**共通的に必要な項目を抽出**することで決定することとしたい。
- 現在の指針に記載されている取組は、これまで共通的に必要な項目として記載されてきた経緯があることから、**引き続き記載**することとしたい。

指針の目次による新旧比較 （1/3）

改定版指針目次（案）

- はじめに
- Ⅰ．目的及び位置付け
  - 1. 重要インフラにおける情報セキュリティ対策の重要性
  - 2.「安全基準等」とは何か
  - 3. 指針の位置付け
  - 4. 指針を踏まえた「安全基準等」の継続的改善及び浸透への期待
- Ⅱ．組織統治におけるサイバーセキュリティ　（新設）
  - 1. 経営方針・リスクマネジメント方針とサイバーセキュリティ
  - 2. 体制整備とサイバーセキュリティ
    - 2.1. モニタリング・レビュー・監査・情報開示の体制の構築
    - 2.2. 役割と責任の割当、権限の明確化
  - 3. サイバーセキュリティを含めた組織統治の運用

現行指針（第5版）

- はじめに
- Ⅰ．目的及び位置付け
  - 1. 重要インフラにおける情報セキュリティ対策の重要性
  - 2.「安全基準等」とは何か
  - 3. 指針の位置付け
  - 4. 指針を踏まえた「安全基準等」の継続的改善及び浸透への期待
- Ⅱ．「安全基準等」で規定が望まれる項目
  - 4.1.「Plan（計画）」の観点
    - 4.1.2.「リーダーシップ」の観点
      - （1）経営層のコミットメント
    - 4.1.4.「支援」の観点
      - （3）コミュニケーション

指針の目次による新旧比較 （2/3）

改定版指針目次（案）

III. リスクマネジメント関して実施すべき項目

- 「Plan（計画）」
  - 1. セキュリティ方針の決定
    - 1.1. セキュリティ方針の策定
    - 1.2. セキュリティ方針の開示
  - 2. 体制整備
    - 2.1. 役割と責任の割当、権限の明確化
    - 2.2. 監査体制、情報共有体制、CSIRT整備
  - 3. 計画
    - 3.1. サイバーセキュリティに関するリスクアセスメントの実施
    - 3.2. 資源の確保
    - 3.3. 人材育成
    - 3.4. サプライチェーンの管理
    - 3.5. サイバーセキュリティ確保の計画作成
    - 3.6. セキュリティ基準、内規の作成
    - 3.7. コンティンジェンシープラン、事業継続計画の策定
- 「Do（実行）」
  - 4. 平時
    - 4.1. サイバーセキュリティに係る対策の運用
    - 4.2. 関係主体間による情報共有
  - 5. 障害発生時
    - 5.1. 重要インフラサービス障害の防護・復旧
    - 5.2. コンティンジェンシープラン・事業継続計画の実行
- 「Check/Act（評価／改善）」
  - 6. 平時
    - 6.1. サイバーセキュリティに係る対策の課題抽出
  - 7. 障害発生時
    - 7.1. 重要インフラサービス障害対応を通じた課題抽出
  - 8. 課題の改善

現行指針（第5版）

Ⅱ.「安全基準等」で規定が望まれる項目

- 1. 策定目的
- 2. 対象範囲
- 3. 関係主体の役割
- 4. 対策項目
  - 4.1.「Plan（計画）」の観点
    - 4.1.1.「組織の状況」の観点
      - （1）外部環境及び内部環境の理解
      - （2）関係主体等の要求事項の理解
    - 4.1.2.「リーダーシップ」の観点
      - （1）経営層のコミットメント → **IIへ移動**
      - （2）情報セキュリティ方針の策定
      - （3）組織の役割に対する責任及び権限の割当
    - 4.1.3.「計画」の観点
      - （1）情報セキュリティリスクアセスメント
      - （2）情報セキュリティリスク対応の決定 → **具体的な取組についてはIVへ移動**
      - （3）セキュリティ管理策に係る個別方針の策定
      - （4）情報セキュリティリスク対応計画の策定
    - 4.1.4.「支援」の観点
      - （1）資源確保
      - （2）人材育成及び意識啓発
      - （3）コミュニケーション → **IIへ一部移動**
  - 4.2.「Do（実行）」の観点
    - 4.2.1.「運用」の観点
      - （1）情報セキュリティ対策の導入、運用
      - （2）重要インフラサービス障害への対応
      - （3）演習・訓練の実施
  - 4.3.「Check（評価）」の観点
    - 4.3.1.「評価」の観点
      - （1）モニタリング及び監査
      - （2）経営層によるレビュー
  - 4.4.「Act（改善）」の観点
    - 4.4.1.「改善」の観点
      - （1）是正処置及び継続的改善

新設

別章へ移動、一部移動

指針の目次による新旧比較 （3/3）

改定版指針目次（案）

Ⅳ.「安全基準等」で規定すべき項目

1. 策定目的
2. 対象範囲
3. 関係主体の役割と責任
4. 対策項目
   1. 組織的なセキュリティ
      1.1. 資産の管理
      2.2. 運用時のセキュリティ管理
      3.3. システムの取得、開発及び保守
      4.4. インシデント管理
      5.5. 供給者関係
   2. 物理的なセキュリティ
      2.1. 物理的及び環境的セキュリティ
   3. 技術的なセキュリティ
      3.1. アクセス制御
      3.2. 暗号
      3.3. 通信のセキュリティ
   4. 人的なセキュリティ
      4.1. 人的資源のセキュリティ（外部委託）

現行指針（第5版）

Ⅱ.「安全基準等」で規定が望まれる項目

1. 策定目的
2. 対象範囲
3. 関係主体の役割
4. 対策項目
   4.1.「Plan（計画）」の観点
      4.1.3.「計画」の観点
         （２）情報セキュリティリスク対応の決定
            （ア）人的資源のセキュリティ（外部委託）
            （イ）資産の管理
            （ウ）アクセス制御
            （エ）暗号
            （オ）物理的及び環境的セキュリティ
            （カ）運用時のセキュリティ管理
            （キ）通信のセキュリティ
            （ク）システムの取得、開発及び保守
            （ケ）供給者関係
            （コ）情報セキュリティインシデント管理

（現行指針の記載例）
●バックアップ
重要インフラサービスの提供に係る情報システムの異常状態や重要なデータの誤った消去等（ランサムウェア等による不正なデータ暗号化も含む）の可能性を想定し、システムイメージやデータ等に対するバックアップの方針及び手順をあらかじめ整備する。なお、可用性確保の観点から、バックアップは十分な量を取得することが期待される。また、取得したバックアップは必要な場面で問題なく利用できることが求められるため、定期的なバックアップリカバリー検査を実施する。
重要なデータについてはバックアップをとることとし、確実に復旧できるようにすること。

組織的なセキュリティ	各対策の実施手順の整備、サプライチェーン管理など
物理的なセキュリティ	施錠、監視カメラ、重要な場所の入退室管理など
技術的なセキュリティ	マルウェア対策ソフト、多要素認証等システム技術による対策
人的なセキュリティ	従業員教育、意識啓発、注意喚起、罰則規定など

総合的なセキュリティ確保の取組のため、４つの対策分類に分けて記載する。
制御システムについては、代表的なリスクやリスクアセスメント手法などについて手引書へ記載する。
成熟度評価については、指針において、自組織に適した防護対策とあわせて考え方を記載する。対策項目ごとの成熟度については、C2M2等の参考資料を掲載することとする。

◆安全基準等策定指針・手引書の概要

◆改定の目的・進め方・スケジュール

◆論点と指針改定の方向性

◆手引書改定の方向性

手引書改定の方向性

➢ これまでの「リスクアセスメント手引書」から、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（プロファイル）の明確化について明示
- 自組織の特性(プロファイル)の明確化の重要性
- 自組織の特性把握と目標の設定手法
- 自組織の防護対策の実態と目標のギャップ分析手法

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

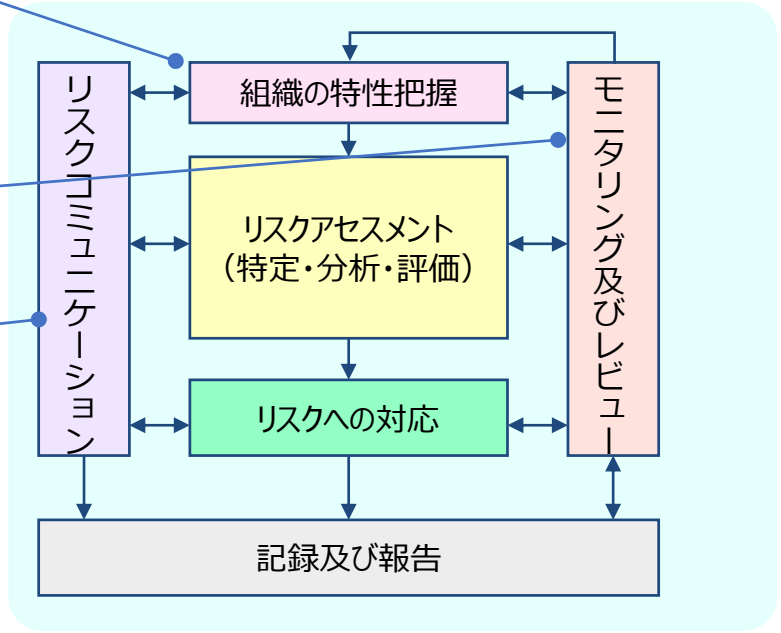
✓リスクコミュニケーションについて追記
- 組織内外とのコミュニケーションの在り方

3．既存の構成見直し

✓ 有効な記載内容については継続し、よりポイントを絞ってスリム化を実施
- リスクアセスメントの妥当性確認・評価の詳細内容については別紙へ移動

✓ より詳細な手順等については、下位にガイダンスを整備する構成へ変更

重要インフラ事業者等によるリスクマネジメントの取組（例）



参考資料

国際動向

○日米豪印(QUAD)に関する動向

- 2022年５月22日、日米豪印首脳会合（QUAD）を開催。
- 「日米豪印サイバーセキュリティ・パートナーシップ」を立ち上げ、重要インフラに関しては、年内をメドに、共通のベースラインとその実施を担保するための枠組みや、脅威情報の共有などについて検討。
- 年度内めどで、これらに関する合意形成を図る予定。
  →安全基準等策定指針の見直しや新たな調査方法の検討と整合をとりながら進める。

（参考：基準・ベースラインに関する各国動向）

米国	2021年７月28日、重要インフラ制御システムのサイバーセキュリティ向上に関する国家安全保障覚書（NSM-5）に署名。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**を策定するよう要求。2021年9月21日、米国CISAは、「重要なインフラ制御システムのサイバーセキュリティパフォーマンスの目標と目的」※を公表。本文書は暫定版であり、2022年7月に完成版が策定される予定。 ※「ベースライン目標」と「強化された目標」からなり、「**リスクマネジメントとサイバーセキュリティガバナンス**」「**サプライチェーン・リスクマネジメント**」等の９項目からなる目標を設定。
豪州	Security of Critical Infrastructure Act 2018及び修正法に基づき、サイバーセキュリティに関する高度な義務を課すことを検討中。**リスクマネジメントの実施の義務化**に加え、国は重要インフラのうち特に重要なサブセットを管理する事業者に対し、「インシデント対応計画の提出」、「演習の実施」、「脆弱性診断の実施」、「システム情報※の提出」を求めることができるようにする予定。 ※セキュリティ、診断モニタリングまたは監査を目的としてシステムに関して生成されるデータであり、ログやアラートなど。

（参考：報告義務に関する各国動向）

米国	2022年3月にサイバーインシデント報告法が上院で可決、大統領が署名して成立。重要インフラ事業者に対し、**サイバー攻撃を72時間以内、ランサムウェアの身代金支払いを24時間以内にそれぞれCISA（Cybersecurity and Infrastructure Security Agency）に報告するよう義務付け**。報告を怠った場合、CISAは事業者に罰則を課すことができる。今後、24か月以内にCISAが法律に基づく規則案を提案し、その後18か月以内に決定予定。
豪州	Security of Critical Infrastructure Act 2018及び修正法（2021年12月に成立）に基づき、2022年４月、Cyber and Infrastructure Security Centre（CISC）は、重要インフラ資産の登録及びインシデントの報告の義務付けに関するルールを決定、施行。電気、放送、交通などの重要インフラ資産については、所有者等の情報を登録しなければならず、**資産にSignificantな影響を及ぼすインシデントが生じたときは認知後12時間以内に、その他のrelevantな影響を及ぼすインシデントが生じたときは認知後72時間以内にCISCに報告しなければならない**。

(出典：米国政府、豪州政府ホームページ等)

国際動向

○欧州に関する動向

・EU　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**）

2016年にEUで採択。加盟国のリスク対策やインシデントへの対処能力に関し一定の基準を定め、また、EU域内での情報収集と共有の仕組みを整備することを目指しており、2018年5月までに加盟国レベルで国内法整備を完了することが求められる。具体的には、国家CS戦略の構築、情報セキュリティ担当の国家機関設立、サイバー攻撃時の対応チーム設置、情報共有やインシデント対応に関するEU加盟国間の協力ネットワークの構築、セキュリティ要件およびサイバーインシデント報告の義務（重要インフラ分野）を示している。なお、EUを離脱した英国もこれに準拠するスタンスである。

・EU　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**）

2022年5月暫定合意。今後、加盟各国と欧州議会での正式な承認を経て施行後、21ヶ月以内に加盟国レベルで国内法整備を完了することが求められる。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対応、報告義務の合理化、より厳しい監督措置の導入、EU全域に調和した制裁措置を含むより厳しい執行要件の導入をはかるもの。なお、EUを離脱した英国の準拠有無は不明。

（出典：欧州連合ホームページ等）

（参考：基準・ベースラインに関する各国動向）

英	2018年4月、NIS規制法2018（The Network and Information Systems Regulations 2018）が成立。セキュリティ要件への対応に関しては、**NCSCからサイバーアセスメントフレームワーク（CAF)が発表され、NIS指令のセキュリティ要件（4章14条）を実現するための4項目14指針を示している。**CAF自体は義務ではないが、セキュリティ対策に不備が認められた重要インフラ事業者に対する罰金等、罰則事項をNIS規制法において設けている。
独	2015年7月、ITセキュリティ法（IT security act）が成立。**重要インフラ事業者に対してサービス維持を目的としたセキュリティ対策の義務化が行われた。**重要インフラ事業者は、セキュリティ対策を実施しているかの監査や認証等を受けた結果をBSI（情報セキュリティ庁）に2年ごとに報告しなければならない。
仏	2013年12月、重要情報インフラ防護法が成立。**重要インフラ事業者は、国防のためにセキュリティ対策を実施することと、ANSSI、他の州のサービス、又は認定委託事業者による監査を受けることの義務が定められた**。具体的な対策は定められていないが、適切な対策がなされていない場合の罰則事項あり。なお、NIS指令に対しては、 2018年2月に成立したLOI n° 2018-113法においてこれに準拠した内容が示されている。

（参考：報告義務に関する各国動向）

英	2018年4月、NIS規制法2018（The Network and Information Systems Regulations 2018）が成立。**重要インフラ事業者に対して、ネットワークおよび情報インシデントを72時間以内に指定管轄当局に報告するよう義務付け**。情報提供を求める通知書の発行や、情報提供に応じなかった場合の罰金等、罰則事項を設けている。
独	2015年7月、ITセキュリティ法（IT security act）が成立。**重要インフラ事業は重要インフラの機能に故障や障害をもたらすか、もたらす可能性があるインシデントが発生した場合、BSI（情報セキュリティ庁）に報告するよう義務付け**。怠った場合、5万ユーロ以下の罰金となる可能性がある。
仏	2014-2019軍事計画法（LPM）。**重要インフラ事業者に対して、情報システムの運用又はセキュリティに影響を及ぼすインシデントに関して遅滞なく内閣総理大臣に報告するよう義務付け**。罰則事項あり。

（出典：英国政府ホームページ等）

米国の重要インフラ制御システムのサイバーセキュリティパフォーマンス目標と目的

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(Industrial Control System(ICS))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 (National Security Memorandom-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。

2021年9月21日、米国CISAは、「重要なインフラ制御システムのサイバーセキュリティパフォーマンスの目標と目的」の文書を公表した。重要インフラのサイバーセキュリティを大幅に改善し、重要なサービスをサイバー脅威から確実に保護するためには、連邦政府と重要インフラ事業者の自発的かつ協調的な取り組みが必要とし、このために重要インフラにおける自主的なガイダンスと必須の要件を作成することを目的としている。これは、最近の高度化するサイバー脅威に対応するために、重要インフラをサイバー脅威から確実に守るための重要インフラの所有者と運営者の自主的なガイダンスと義務的な要件を定めたサイバーセキュリティパフォーマンスの目標の暫定案を示したもの。今回の発表された目標は、暫定案であり、覚書から1年後の2022年7月に最終的な目標が定められる。また、最終的な目標と同時にセクター別のサイバーセキュリティの目標も策定される予定である。

概要

○サイバーセキュリティ目標の暫定案は、既存の連邦政府等による産業用制御システム（ICS）のサイバーセキュリティに関するガイドから検討されたもの。

○推奨されるサイバーセキュリティの実践方法を以下の9つのカテゴリに分類し、それぞれには、「目的」を実現するための「ベースライン目標」と「強化された目標」が示されている。

○「ベースライン目標」は、すべての制御システムに推奨される事項が含まれ、「強化された目標」には、国防に関連する重要なインフラが対象となる事項が含まれる。なお、ここで、国防に関連する重要なインフラについては、重要なライフライン（すなわち、エネルギー、通信、輸送、及び水）と、制御システムの障害が安全性に影響を与える可能性がある場合に対象となる。また各目標には、実装の証拠の例が示されている。

（１）リスクマネージメントとサイバーセキュリティガバナンス
（２）アーキテクチャと設計
（３）構成と変更管理
（４）物理セキュリティ
（５）システムとデータの整合性、可用性、および機密性
（６）継続的モニタリングと脆弱性管理
（７）トレーニングと啓発
（８）インシデントレスポンスとリカバリー
（９）サプライチェーン・リスクマネジメント

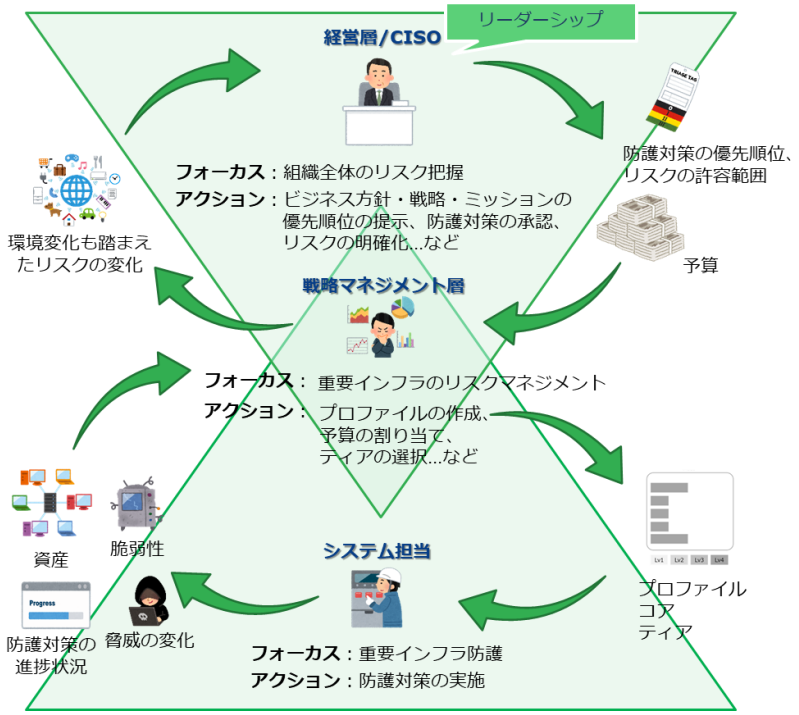
(出典：米国政府ホームページ等)

NIST CSF（重要インフラのサイバーセキュリティを向上させるためのフレームワーク）

- 米国国立標準研究所（National Institute of Standards and Technology, NIST）が2014年に発行。
- 業種や企業規模などに依存せず、サイバーセキュリティ対策の効果を数値で評価するための基準も含む体系的なガイドライン。
- 現在、第２版への改定作業中。

「コア（Core）」「ティア（Tier）」「プロファイル（Profile）」の要素で構成

コア（Core）：組織の種類や規模を問わない共通のサイバーセキュリティ対策の一覧
ティア（Tier）：対策状況を数値化し、組織を評価する基準（成熟度評価基準（4段階））
プロファイル（Profile）：組織のサイバーセキュリティ対策の「as is (現在の姿)」と「to be (目指すべき姿)」をまとめたもの



←CSFにおける各階層の関係

対策を「識別、防御、検知、対応、復旧」の５種類に分類し、具体的な内容はNIST SP-800などを参照先として記載

→

表 1: 機能とカテゴリーの識別子

機能の識別子	機能	カテゴリーの識別子	カテゴリー
ID	識別	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスクマネジメント戦略
		ID.SC	サプライチェーンリスクマネジメント
PR	防御	PR.AC	アイデンティティ管理とアクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	コミュニケーション
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	コミュニケーション

SP800シリーズ

- SP800シリーズ(Special Publications 800 Series)は、連邦政府がセキュリティ対策を実施する際に参考文書として利用することを前提として、NISTのコンピュータセキュリティ課(CSD)により作成されるガイダンス群。

リスクマネジメント	
SP800-18	連邦情報システムのためのセキュリティ計画作成ガイド
SP800-26	ITシステムのためのセキュリティ自己診断ガイド
SP800-30	ITシステムのためのリスクマネジメントガイド
SP800-37	情報システムと組織のためのリスクマネジメントフレームワーク
SP800-39	情報セキュリティのリスクマネジメント
SP800-53	連邦政府情報システムにおける推奨セキュリティ管理策
SP800-53A	連邦情報システム/組織におけるセキュリティ及びプライバシー管理の評価：効果的なアセスメント計画の構築
SP800-60	情報及び情報システムのタイプとセキュリティ分類のマッピングガイド
SP800-70	IT製品のための国家的なチェックリストプログラム

サイバー脅威インテリジェンス(CTI)共有	
SP800-137	連邦情報システム及び組織のための情報セキュリティ常時監視(ISCM)
SP800-150	サイバー脅威情報共有のガイド

制御システム	
SP800-82	産業用制御システム(ICS)セキュリティガイド

認証	
SP800-63	電子的認証に関するガイドライン

管理すべき重要情報(CUI)保護	
SP800-171	連邦政府以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

ゼロトラスト	
SP800-207	ゼロトラストアーキテクチャ

事業継続	
SP800-12	コンピュータセキュリティハンドブック
SP800-34	ITシステムのための緊急時対応計画ガイド
SP800-61	コンピュータインシデント対応ガイド
SP800-83	不正プログラムインシデント防止・対応ガイド

サプライチェーン	
SP800-161	システムと組織のためのサイバー・サプライチェーン・リスク管理の実践

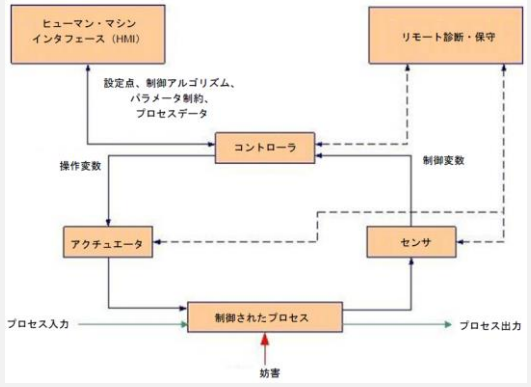
NIST SP800-82 産業用制御システムセキュリティガイド

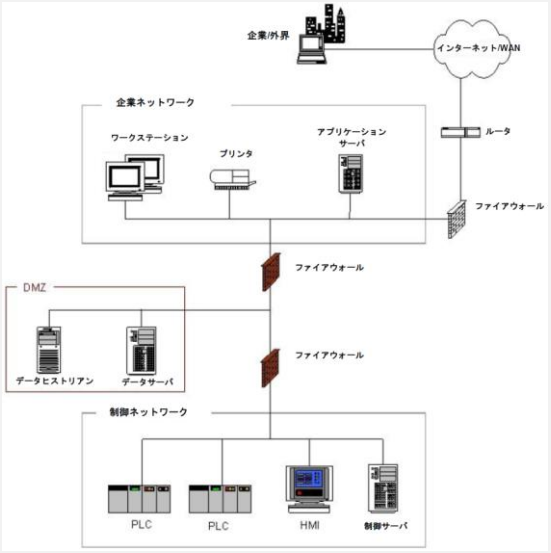
➢ 産業用制御システム（Industry Control System;ICS）に関する脅威、脆弱性、リスク管理等について記載された文書

制御システムに求められるセキュリティ管理

ICSの主な構成要素であるSCADA、PLC、DCS*と、それらが構成されたネットワークに対して求められるセキュリティ管理体制や対策が記載されている。

基本方針としては情報システムのセキュリティリスクマネジメントに準ずるが、ネットワークの分割、分離や、企業ネットワークと制御ネットワーク間の境界ファイアウォールの設計時の考慮事項などが記載されている。





出典：JPCERT/CC 「NIST SP 800-82 Guide to Industrial Control Systems(ICS) Security 対訳資料」

例：NW分離、FW設計の考慮など

➢ ネットワーク分離
制御ネットワークゾーン、企業ネットワークゾーン、最低１つのDMZの、３ゾーンでネットワークを管理することが推奨される

➢ 多層防御の考え方
単一のセキュリティ製品のみでICSを保護することは不可能と考え、２つ以上のセキュリティ技術を使い、多層防御をすることが推奨される。

➢ ファイアウォールルールの設計ポリシー
・IPアドレスとポート（アプリケーション）に固有のステートフルルールにする
・企業ネットワークのIPアドレスであれば制御ネットワークにアクセスできるようなルールは薦められない
・許可したポートの通信でも用心のために、HTTPSなどのセキュアな通信に限定するべき
・HTTP、FTPといったセキュアでない通信はスニッフィングのおそれがある
・DMZアーキテクチャを使用して、企業ネットワークと制御ネットワークが直接通信できないようなシステム設計とする

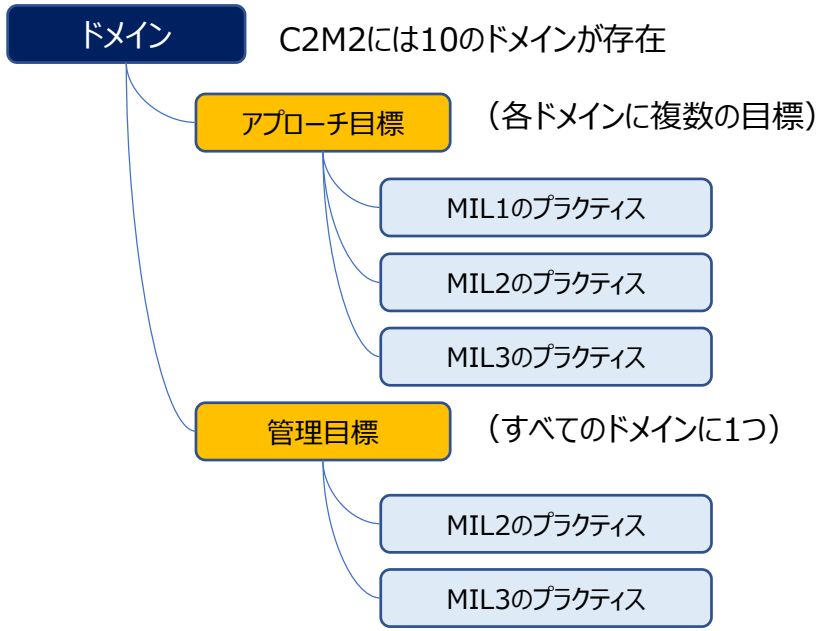
*SCADA(Supervisory Control And Data Acquisition) ： 施設内の設備・機器からの情報を一元的に監視し、制御するシステム
PLC(Programmable Logic Controller) ： 機器や設備の制御に使用される制御装置
DCS(Distributed Control System) ： 分散制御システム

ES-C2M2（電力業界のサイバーセキュリティ能力成熟度モデル）

- 米国エネルギー省が開発したサイバーセキュリティ能力成熟度モデル（C2M2）のうち、電力特有のセキュリティ問題に対応するために開発されたプログラム。
- 目標とプラクティスがドメインとしてまとめられ、10のドメイン、37の目標、311のプラクティスで構成される。

（モデルの用途）

- ✓ 電力業界におけるサイバーセキュリティ能力の強化
- ✓ 成熟度レベル（Maturity Indicator Level;MIL）に応じたサイバーセキュリティ能力の評価
- ✓ ナレッジ、ベストプラクティス、関連情報の共有
- ✓ サイバーセキュリティ向上のための必要なアクション、優先度の決定



※モデルの構成イメージ
IPA ES-C2M2解説資料より

MIL: Maturity Indicator Level

ドメイン、目標、MIL、プラクティスの例
（要員管理：サイバーセキュリティにおける責任の割当て）

ドメイン	目標	MIL	プラクティス
要員管理	（アプローチ目標）サイバーセキュリティにおける責任の割り当て	MIL1	a. 機能に対するサイバーセキュリティの責任が特定されている
			b. サイバーセキュリティに責任が特定の人員に割当てられている
		MIL2	c. サイバーセキュリティの責任が、外部のサービスプロバイダーを含め、特定の役割に割当てられている
			d. サイバーセキュリティの責任が、文書化されている（例：職務分掌規定）
		MIL3	e. サイバーセキュリティの責任と職務要件が、適切にレビューされ、更新されている
			f. サイバーセキュリティの責任が勤務評価基準に含まれている
			g. 割当てられたサイバーセキュリティの責任が管理され、対象範囲の適切さと冗長性が保証されている

CIS Critical Security Controls (Version 8)

- CIS Controls は Center for Internet Security（セキュリティ標準化に取り組む米の非営利団体）が公開している、組織内で最低限行うべきサイバーセキュリティ対策を提示したガイドライン
- 対策を18カテゴリ、計153項目に分類（Ver.8時点）。また優先度は3段階に分けており、大きな数字ほど高いレベルの対応が要求される

- 技術的な対策に重点を置いており、あらゆる企業に適用が可能
- 項目には優先度の指標として実装グループ(Implement Groups)が設定されている。IGsは3段階存在し（IG1～IG3）、うちIG1はサイバーセキュリティ対策における基本的な予防策であり、先行して取り組むべき基本対策として提示されている（数字が大きくなるほど、実装グループで要求される事柄は高くなる）
- 各組織は、事業内容や保有するデータを参考に、自組織に適したIGsを判断して、CIS Controlsに記載された項目を実施する

Implement Groups(IGs)の概要 *括弧は各グループに所属する項目数		
IG3 (153)		・IG2の要件は内包される ・サイバーセキュリティの様々な専門スキルを有する専門家が所属 ・規制やコンプライアンスの監視対象となる機密情報、機能を有し、データ侵害または攻撃が成功した場合、公共の福祉に重大な損害を与える可能性がある
	IG2 (133)	・IG1の要件は内包される ・ITインフラの管理保護責任者が所属し、リスクプロファイルを持つ複数部門が存在。 ・自社および顧客の機密情報を保管しており、データ侵害により社会的信用の低下が懸念される
		IG1 (56) ・ITおよびサイバーセキュリティの専門知識が限られる（または所属しない）中小企業が対象 ・事業継続性が最大の焦点（機密性の高い保護すべきデータは少なく、従業員、財務情報等が主な保護の対象）

参考：https://www.nri-secure.co.jp/blog/cis-controls-v8

CIS Controlsのカテゴリ	
#	Control
01	組織の資産のインベントリと管理
02	ソフトウェア資産のインベントリと管理
03	データ保護
04	組織の資産とソフトウェアの安全な構成
05	アカウント管理
06	アクセス制御管理
07	継続的な脆弱性管理
08	監査ログ管理
09	電子メールとWebブラウザの保護
10	マルウェアの防御
11	データ復旧
12	ネットワークインフラストラクチャ管理
13	ネットワークの監視と防御
14	セキュリティ意識向上とスキルのトレーニング
15	サービスプロバイダーの管理
16	アプリケーションソフトウェアセキュリティ
17	インシデントレスポンスと管理
18	ペネトレーションテスト

サイバーセキュリティ経営ガイドラインの改訂

- セキュリティはコストではなく投資であると位置づけ、経営者がリーダーシップを取ってセキュリティ対策を推進していくことが重要であることを示したガイドライン。（2017年ver2.0）
- 近年のサイバーセキュリティ経営を取り巻く情勢の変化等を踏まえ、2022年度中に改訂を実施予定。

1．経営者が認識すべき３原則

（１）経営者が、**リーダーシップを取って対策**を進めることが必要
（２）自社のみならず、**ビジネスパートナーを含めた対策**が必要
（３）平時及び緊急時のいずれにおいても、**関係者との適切なコミュニケーション**が必要

2．経営者がCISO等に指示すべき１０の重要事項

リスク管理体制の構築	**指示１** 組織全体での対応方針の策定 **指示２** 管理体制の構築 **指示３** 予算・人材等のリソース確保
リスクの特定と対策の実装	**指示４** リスクの把握と対応計画の策定 **指示５** リスクに対応するための仕組みの構築 **指示６** PDCAサイクルの実施
インシデントに備えた体制構築	**指示７** 緊急対応体制の整備 **指示８** 復旧体制の整備
サプライチェーンセキュリティ	**指示９** サプライチェーン全体の対策及び状況把握
関係者とのコミュニケーション	**指示10** 情報共有活動への参加

［出典］「第7回産業サイバーセキュリティ研究会WG2　事務局資料」（経済産業省）