「重要インフラのサイバーセキュリティに係る行動計画」の概要

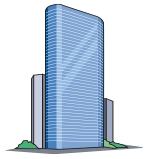
官民連携による重要インフラ防護の推進

- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

NISCによる総合調整

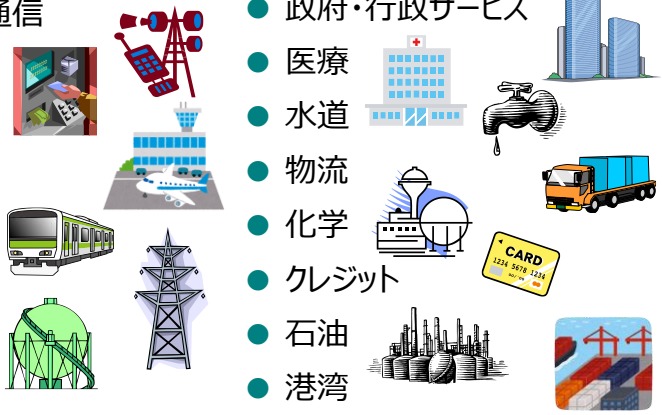
重要インフラ所管省庁

- 金融庁
  [金融]
- 総務省
  [情報通信、行政]
- 厚生労働省
  [医療、水道]
- 経済産業省
  [電力、ガス、化学、クレジット、石油]
- 国土交通省
  [航空、空港、鉄道、物流、港湾]



重要インフラ(全１５分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油
- 港湾



関係機関等

- サイバーセキュリティ関係省庁
  [総務省、経済産業省等]
- 事案対処省庁
  [警察庁、防衛省等]
- 防災関係府省庁
  [内閣府、各省庁等]
- サイバーセキュリティ関係機関
  [NICT、IPA、JPCERT/CC等]
- サイバー空間関連事業者
  [サプライチェーン等に関わるベンダー等]

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

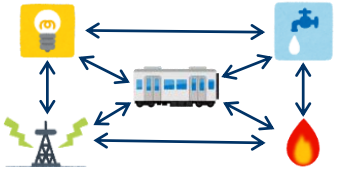
安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

行動計画の基本的考え方・要点

1.「重要インフラ防護」の目的

重要インフラにおいて、任務保証の考え方を踏まえ、
①重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること
②重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ること
の両面から、強靱性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現すること。

2. 関係主体の責務

- 関係主体の責務は、サイバーセキュリティ基本法(平成26年法律第104号)を基本とする。
- 国は、サイバーセキュリティに関する総合的な施策を策定し、及び実施する。
- 地方公共団体は、サイバーセキュリティに関する自主的な施策を策定し、及び実施する。
- 重要インフラ事業者は、サービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、自主的かつ積極的にサイバーセキュリティの確保に努める。
- サイバー関連事業者その他の事業者は、その事業活動に関し、自主的かつ積極的にサイバーセキュリティの確保に努める。

3. 基本的な考え方

- 重要インフラを取り巻く情勢は、システム利用の高度化、複雑化、サイバー空間の脅威の急速な高まりを受け、重要インフラ事業者等においては、経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応を一層促進する。特に、経営の重要事項としてサイバーセキュリティを取り込む方向で推進する。
- 自組織の特性を明確化し、経営層からシステム担当者までの各階層の視点を有機的に組み合わせたリスクマネジメントを活用し、自組織に最も適した防護対策を実施する。
- 重要インフラを取り巻く脅威の変化に適確に対応するため、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応を実施する。

4. 障害対応体制の強化に向けた取組

- リスクマネジメントによる事前対応と危機管理の組合せにより、障害対応体制を強化する。
- 組織におけるサイバーセキュリティに対する経営者と専門組織の関係を明確にする。
- サイバーセキュリティ基本法第2条の定義を踏まえ、外部からの攻撃のみならず、システム調達、設計及び運用に関係する事象を含め対応できるよう障害対応体制を整備・運用する。

行動計画の取組①： 障害対応体制の強化

重要インフラ事業者等は組織全体としてサイバーセキュリティの確保に取り組んだ上で、官民の相互連携を密にした障害対応体制の強化を推進する。

取組のポイント

- ✓ 組織統治の一部としての障害対応体制の整備
- ✓ サプライチェーンも含めた包括的な対応

行動計画期間中の取組

（1）組織統治の一部としての障害対応体制

- 経営層、CISO、戦略マネジメント層、システム担当等組織全体及びサプライチェーン等に関わる事業者を含めた障害対応体制の強化を推進

（2）障害対応体制の強化に向けた取組

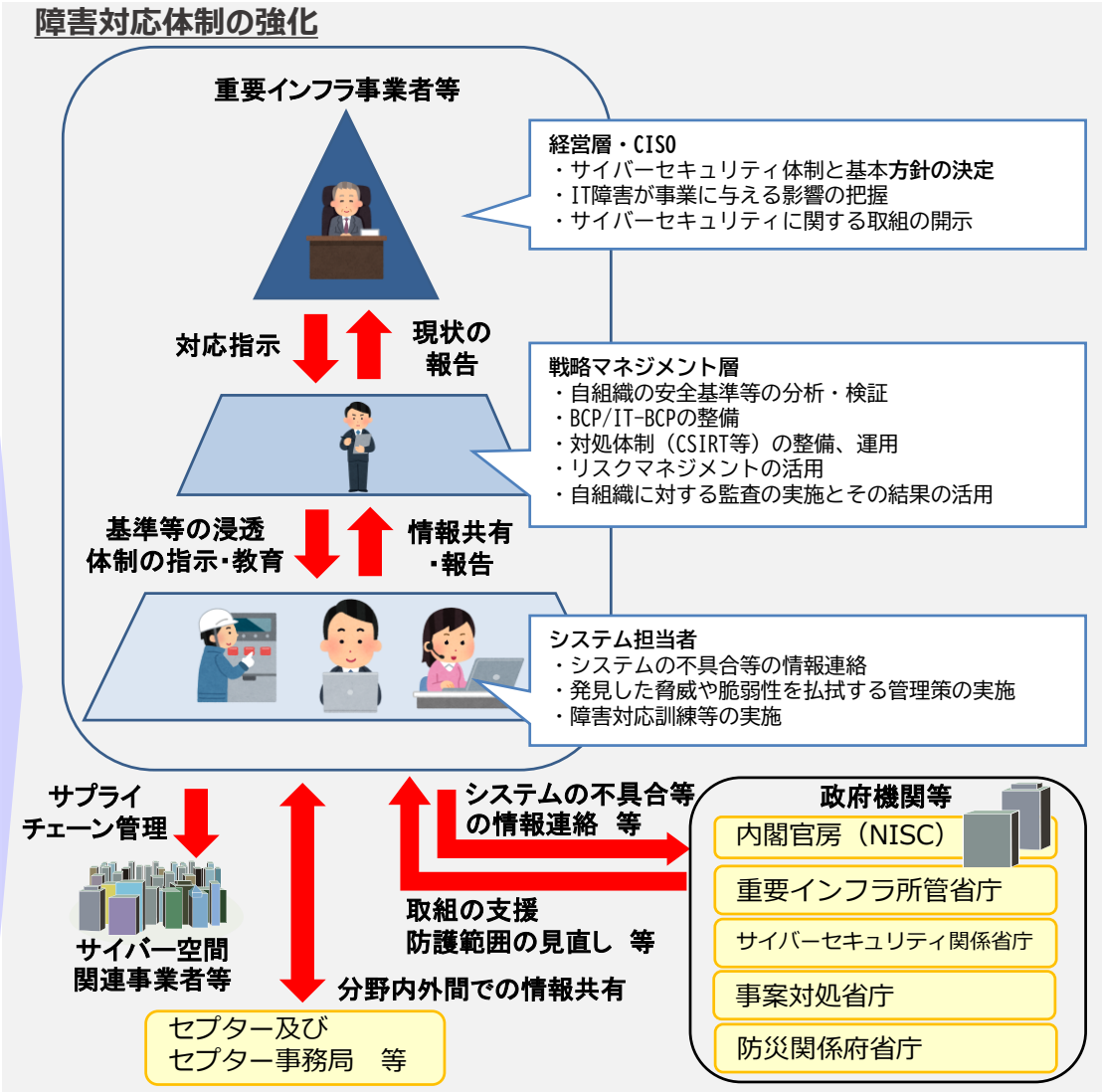
- 障害対応体制を強化するため、BCP/IT-BCP、CSIRT、監査体制等の効果的な取組を推進

（3）官民一体となった障害対応体制の強化

- 政府と重要インフラ事業者等の相互連携を密にした官民一体としての対応を検討

（4）重要インフラに係る防護範囲の見直し

- 環境変化に対応するため、サプライチェーンを含めた「面としての防護」の確保及び国の安全等の確保の観点からの取組



行動計画の取組②： 安全基準等の整備及び浸透

自組織に最適な防護対策を実施するため、重要インフラ事業者等の関係主体における「安全基準等」の整備及び浸透の取組を推進する。

※ 安全基準等・・・関係法令、業界標準／ガイドライン、内規等の総称

取組のポイント

- ✓ 社会動向や周辺環境の変化に適応した、自組織に適した安全基準等の整備
- ✓ 監査や演習等によるリスク評価を経た安全基準等の継続的な改善

行動計画期間中の取組

（1）指針の継続的改善

- **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**方策の強化や、サプライチェーンに関する基準の整備
- 自組織に適した継続的改善のための基準の整備

（2）安全基準等の継続的改善

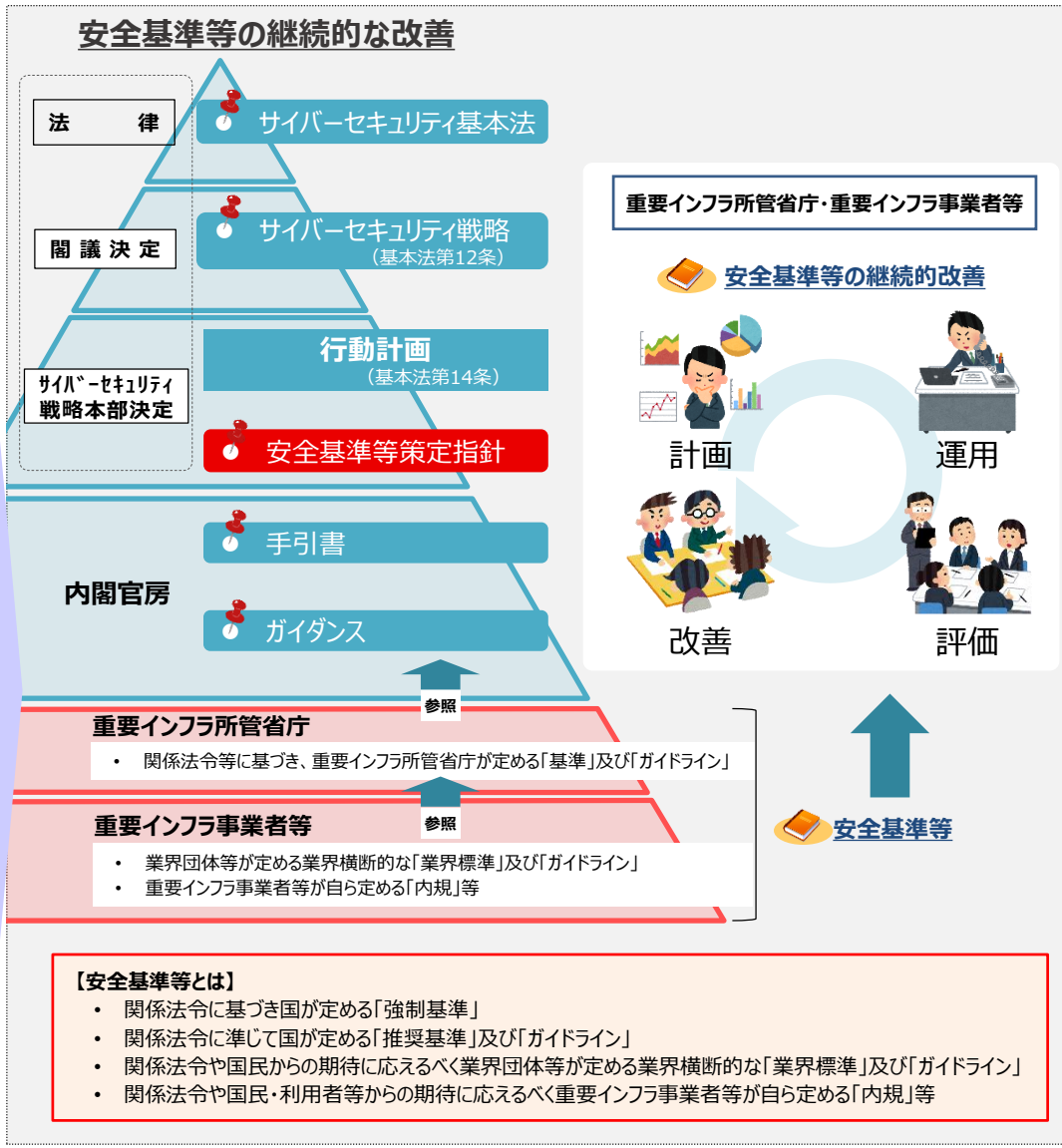
- **内部・外部監査**や演習への参加等による**リスク評価**を経た、安全基準等の継続的な改善
- 重要インフラ所管省庁による安全基準等の改善状況を調査

（3）安全基準等の浸透

- 重要インフラ事業者等におけるサイバーセキュリティ確保に向けた取組について、実態把握のための調査

（4）安全基準等の文書の明確化

- 安全基準等策定指針、安全基準等の理解促進のため、文書の一覧化や文書間の関係性を明確化



行動計画の取組③： 情報共有体制の強化

個々の重要インフラ事業者等が日々変化するサイバーセキュリティ動向に対応できるよう、官民間や分野内外間における情報共有体制の更なる強化に取り組む。

取組のポイント

- ✓ これまでの行動計画で構築され定着している情報共有体制の継承・発展
- ✓ 重要インフラ事業者等の自主的な取組の活性化

行動計画期間中の取組

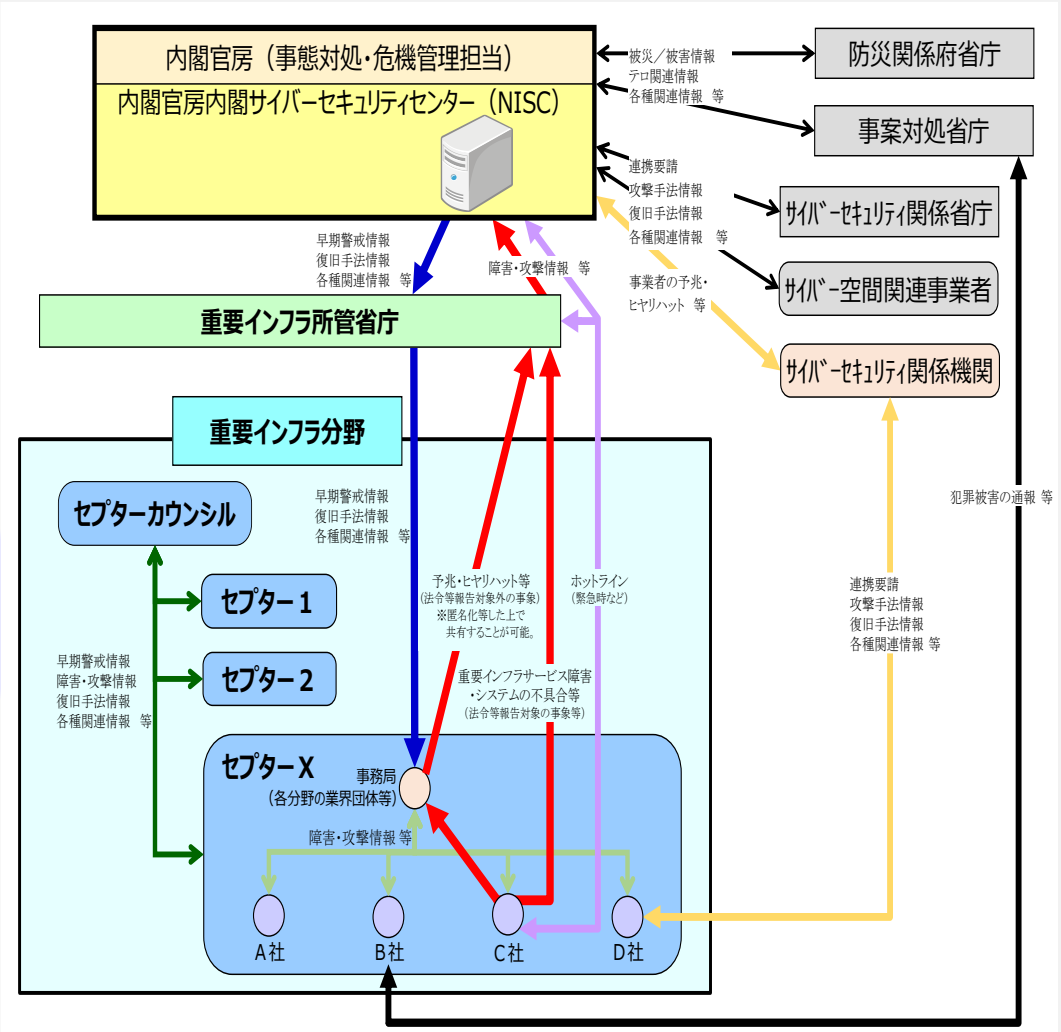
（１）情報共有の更なる促進

- 共有された情報のリスクマネジメント等への積極的な活用
- 重要インフラサービス障害に係る情報及び脅威や脆弱性情報の集約、分析、共有
- 共有すべき情報の明確化（情報系だけでなく制御系やIoTシステムも対象となること等を明示）
- 環境変化等が生じた場合における適時適切な見直し

（２）重要インフラ事業者等の活動の更なる活性化

- 経営層のリーダーシップの下、障害対応体制の構築・強化
- セプター内、セプター間の情報共有の更なる充実
- ISACへの参画及びISAC間の情報共有の促進
- より実態に即した形でのセプター訓練の実施

重要インフラにおける情報共有体制



行動計画の取組④： リスクマネジメントの活用

重要インフラサービスの継続的提供の強靭性確保のため、自組織に適した防護対策の計画・実施、評価・改善の繰り返しによる継続的な取組を推進する。

取組のポイント

- ✓ 自組織に適した防護対策の実現
- ✓ 環境変化による新たなリスク・リスク源の把握
- ✓ 重要インフラ分野間の相互依存性の解析

行動計画期間中の取組

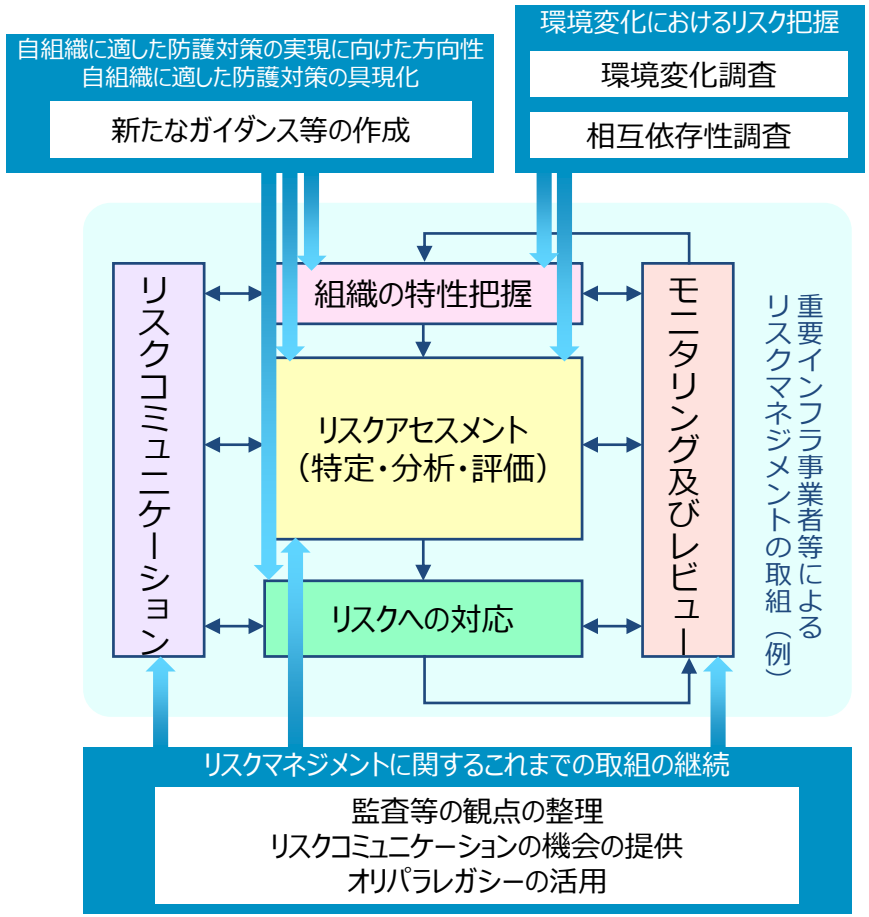
（1）リスクマネジメントの推進

- 自組織のプロファイルを明確化し、自組織に適した防護対策の実現に向けた取組の推進
- 有効な対策や既存の基準類の活用方法について検討し、手引書の見直し、新たなガイダンス等を整備する

（2）リスクに関する調査・分析

- デジタル化を伴うDXの進展によるサイバー空間の変容等によるリスクに対応するため、環境変化調査を実施する
- 重要インフラサービス障害等が生じた場合に、他のどの重要インフラ分野に影響が波及するかという相互依存性に関する調査を実施する。

リスクマネジメントの活用



行動計画の取組⑤： 防護基盤の強化

重要インフラの防護基盤の強化のため、障害対応体制の有効性検証、人材育成、関係機関との連携、国際連携、広報広聴活動等、行動計画の全体を支える共通基盤的な取組を推進する。

取組のポイント

- ✓ 障害対応体制の有効性検証の実施
- ✓ IT部門だけでなく、幅広い部門の人材育成
- ✓ 効果的な広報チャネルを活用した情報発信　　等

行動計画期間中の取組

（1）障害対応体制の有効性検証
- 分野横断的演習による障害対応体制の検証
- 演習で得た課題を活用した障害対応体制の改善

（2）人材育成等の推進
- 経営層と緊密な連携を行えるよう、戦略マネジメント層の育成
- IT部門に限らない、組織全体の意識向上

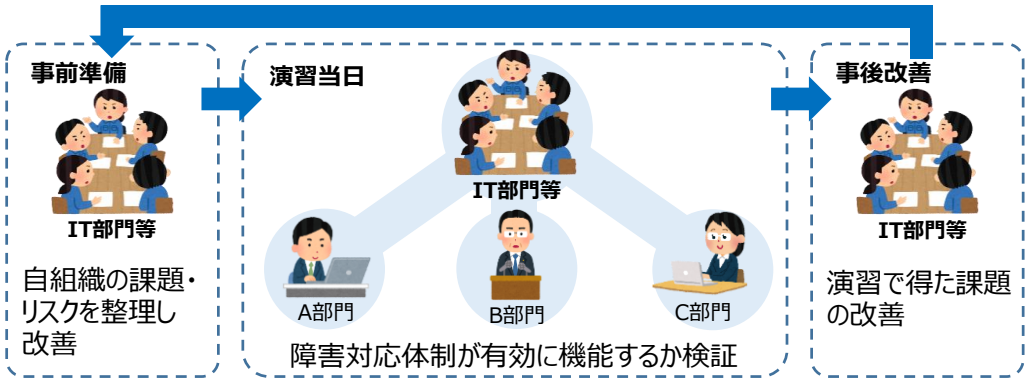
（3）国際連携の推進
- 政府間や事業者間の様々な枠組みを活用した多面的・多角的な国際連携の推進

（4）警察・デジタル庁との連携強化
- サイバー犯罪や、DXに伴う新たな技術に対する意識向上による全体としてのセキュリティ確保の推進

（5）広報広聴活動の推進
- 行動計画の枠組みや取組の国民への積極的な発信
- 関連文書及び関連規格の整備

防護基盤の強化に向けた取組

障害対応体制の有効性検証



人材育成等

- 戦略マネジメント層の育成
- 組織全体の意識向上

国際連携

ASEAN　MERIDIAN Connecting and Protecting

二国間、地域間、多国間の連携

警察・デジタル庁との連携強化

警察庁 National Police Agency　デジタル庁

- サイバー犯罪の警察への通報等
- DXに伴う新技術への意識向上を通じたサイバー空間の安全確保

広報広聴活動

Webサイト、SNS、ニュースレター、講演等を通じた発信

「重要インフラ事業者等による対策例」と各対策に関連する「政府機関等の施策例」

NISC

サイバーセキュリティ基本法における関係主体の責務の理解

重要インフラ事業者等の対策例

Plan（計画）／特定・予防

方針
- 経営の重要事項にサイバーセキュリティを位置付け
- 基本方針の策定／見直し
- リスクマネジメントの活用
  ・組織のプロファイルの明確化　・要件と実態の差異の分析
  ・改善項目の洗い出し　・防護対策の検討と優先順位付け

体制
- 監査体制、情報共有体制、CSIRT等の整備
- 予算・人材の確保
- 人材育成・配置・ノウハウの蓄積
- 外部委託における対策

規定
- 内規の策定／見直し（サイバーセキュリティポリシー等）
- BCP・コンティンジェンシープラン等の策定／見直し
- 情報の取扱いについての規定化

計画
- サイバーセキュリティに係るロードマップの作成／見直し
- サイバーセキュリティに係る計画の作成／見直し

構築
- サイバーセキュリティ（技術）に係る設計・実装／保守
- サイバーセキュリティ（運用）に係る設計・手順書化／保守

Do（実施）／検知・復旧

共通
- サイバーセキュリティに係る対策の運用（監視・統括）
- サイバーセキュリティに係る対策の運用状況把握
- 関係主体間による情報共有

平時
- サイバーセキュリティに係る対策の運用（攻撃傾向の把握等）
- サイバーセキュリティに係る状況の対外説明

障害発生時
- 重要インフラサービス障害に対する防護・復旧
- BCP・コンティンジェンシープラン等の実行
- 重要インフラサービス障害対応状況の対外説明

Check（確認）・Act（是正）／確認・課題抽出

平時
- サイバーセキュリティに係る対策の運用を通じた課題抽出
- 内部監査・外部監査を通じた課題抽出
- 環境変化の調査・分析結果を通じた課題抽出
- 演習・訓練を通じた課題抽出

障害発生時
- 重要インフラサービス障害対応（検知・回復）を通じた課題抽出

政府機関等の施策例

障害対応体制の強化
- 組織統治の一部としての障害対応体制の促進／事業者におけるBCP・CSIRTの運用・監査等の取組支援（内閣官房／重要インフラ所管省庁）
- 官民一体となった障害対応体制の強化（内閣官房／重要インフラ所管省庁／事案対処省庁等）

安全基準等の整備及び浸透
- 安全基準等の継続的改善　（内閣官房／重要インフラ所管省庁）
- 安全基準等の浸透　（内閣官房／重要インフラ所管省庁）
- 安全基準等策定指針の継続的改善（内閣官房／重要インフラ所管省庁）

情報共有体制の強化
- 官民の関係主体間の情報共有（内閣官房／重要インフラ所管省庁）
- セプター訓練（内閣官房／重要インフラ所管省庁）

リスクマネジメントの活用
- 自らに適した防護対策の実現／リスクコミュニケーションの推進　（内閣官房／重要インフラ所管省庁）
- リスクアセスメントの浸透（内閣官房／重要インフラ所管省庁）
- 環境変化におけるリスク把握（内閣官房／重要インフラ所管省庁）

防護基盤の強化
- 人材育成等の推進／「ｾｷｭﾘﾃｨ・ﾊﾞｲ・ﾃﾞｻﾞｲﾝ」の推進／国際連携の推進／デジタル庁との連携／広報広聴活動（内閣官房／重要インフラ所管省庁）
- 障害対応体制の有効性検証（内閣官房／重要インフラ所管省庁）
- 重要インフラ所管省庁による訓練（重要インフラ所管省庁）

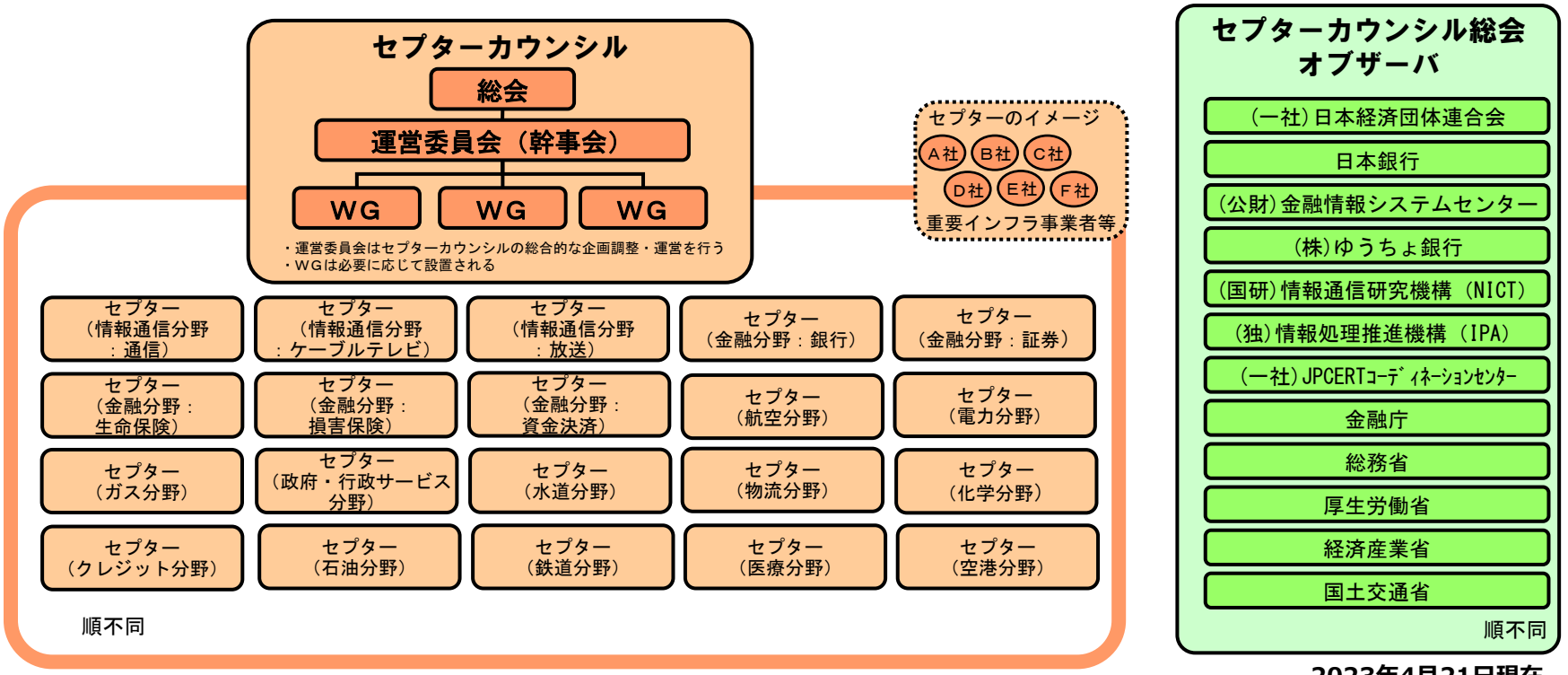
セプターとセプターカウンシル

セプター（ＣＥＰＴＯＡＲ）Capability for Engineering of Protection, Technical Operation, Analysis and Response

- 重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。
- 重要インフラサービス障害の未然防止、発生時の被害拡大防止・迅速な復旧および再発防止のため、政府等から提供される情報について、適切に重要インフラ事業者等に提供し、関係者間で情報を共有。これによって、各重要インフラ事業者等のサービスの維持・復旧能力の向上に資する活動を目指す。

セプターカウンシル

- 各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。
- 分野横断的な情報共有の推進を目的として、２００９年２月２６日に創設。



2023年4月21日現在

セプター特性把握マップ

2023年9月末日現在

重要インフラ分野	情報通信			金融					航空	空港	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	資金決済	航空	空港	鉄道	電力	ガス	政府・地方公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビCEPTOAR	放送CEPTOAR	金融CEPTOAR連絡協議会					航空CEPTOAR	空港CEPTOAR	鉄道CEPTOAR	電力CEPTOAR	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR	化学CEPTOAR	クレジットCEPTOAR	石油CEPTOAR
				銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	資金決済CEPTOAR												
事務局	(一社)ICT-ISAC	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟、日本放送協会	(一社)全国銀行協会 事務・決済システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部	(一社)日本損害保険協会 IT企画部	(一社)日本資金決済業協会 事務局	定期航空協会	空港・空港ビル協議会	(一社)日本鉄道電気技術協会	電力ISAC	(一社)日本ガス協会 技術部 製造グループ	地方公共団体情報システム機構 システム統括室リスク管理課	(公社)日本医師会 情報システム課	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員 (のべ数)	27社 1団体	306社 1団体	194社 2団体	1,276社	280社 7機関	42社	47社	193社	14社 1団体	8社	22社 1団体	24社	12社 1団体	47 都道府県 1,741 市区町村	1グループ 21機関	8水道事業体	6団体 17社	13社	51社	11社
NISCからの情報の展開先(構成員以外)	408社・団体	336社	13社	2社・団体	ー	ー	ー	9社	ー	ー	ー	21社・機関	196社・団体	ー	398社・団体	内容に応じ1,314事業体へ展開	ー	ー	ー	ー
	その他(核物質防護等の措置が要求される企業、ビルディング・オートメーション協会、サイバーディフェンス連携協議会、大学等(内容に応じ展開先を選定))																			
■ その他																				
既存事業領域を越える連携等	情報通信(ICT-ISACにおいて、一部の放送事業者及びケーブルテレビ事業者が加盟)、金融(金融ISACにおいて、加盟金融機関間で情報共有・活動連携)、航空・空港・鉄道・物流(交通ISACにおいて、参加事業者間で情報共有・活動連携)、電力(電力ISACにおいて、加入する電気事業者間で情報共有・活動連携)、化学(石油化学工業協会と日本化学工業協会の情報共有・活動連携)、クレジット(ネットワーク事業者と情報共有・活動連携)、J-CSIP(IPA：標的型攻撃等に関する情報共有)、サイバーテロ対策協議会(重要インフラ事業者等と警察との間で連携、47都道府県に設置)、早期警戒情報CISTA(JPCERT/CC: セキュリティ情報全般)																			