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（案）の概要

１．本行動計画のポイント

◆ 重要インフラサービスを、安全かつ持続的に提供できるよう、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らし、迅速な復旧が可能となるよう、経営層の積極的な関与の下、情報セキュリティ対策に関する取組を推進。（機能保証の考え方）

◆ また、取組を通じ、オリパラ大会に関係する重要なサービスの安全かつ持続的な提供も図る。

２．重要インフラの情報セキュリティ対策の現状と課題

◆ 第３次行動計画に基づく施策群により、自主的な取組が浸透しつつあるが、ＰＤＣＡのうちＣＡに課題。一部で先導的な取組も進展。

◆ 機能保証のため、情報系(ＩＴ)に限らず、制御系(ＯＴ)を含めた情報共有の質・量の改善や、重要インフラサービス障害に備えた対処態勢の整備が必要。

◆ 国内外の多様な主体との連携、情報収集・分析に基づく国民への適切な発信の継続・改善が必要。

３．本行動計画の３つの重点

次の３つを重点として、第３次行動計画の５つの施策群の補強・改善を図る。

①　先導的取組の推進(クラス分け)

■ 他分野からの依存度が高く、比較的短時間のサービス障害でも影響が拡大するおそれがある分野(例：電力、通信、金融)において、一部事業者における先導的な取組（ＩＳＡＣ※の設置やリスクマネジメントの確立等）を強化・推進

※所属事業者間で秘密保持契約を締結するなど、より機密性の高い情報の共有等を目的とした組織

■ 上記先導的な取組みの、当該重要インフラ分野内の他の事業者等及び他の重要インフラ分野への展開による我が国全体の防護能力の強化

②　オリパラ大会も見据えた情報共有体制の強化

■ サービス障害の深刻度判断基準の導入に向けた検討

■ 連絡形態の多様化（連絡元の匿名化、セプター※事務局・情報セキュリティ関係機関経由）による情報共有の障壁の排除。分野横断的な情報を内閣官房に集約する仕組みの検討

※重要インフラ事業者等の情報共有を担う組織

■ ホットライン構築も可能な情報共有システムの整備（自動化、省力化、迅速化、確実化）

■ 情報連絡・情報提供の範囲にＯＴ、ＩｏＴ等を含むことを明確化（ＩＴ障害→重要インフラサービス障害）

■ 演習の改善、演習成果の浸透による防護能力の維持・向上

■ サプライチェーンを含む「面としての防護」に向け範囲の拡大

③　リスクマネジメントを踏まえた対処態勢整備の推進

■ 「機能保証に向けたリスクアセスメントガイドライン」の提供及び説明会の実施等によるリスクアセスメントの浸透

■ 事業継続計画及び緊急時対応計画（コンティンジェンシープラン）の策定等による重要インフラ事業者等の対処態勢の整備

■ 事業者等における内部監査等の取組において、リスクマネジメント及び対処態勢における監査の観点の提供等による「モニタリング及びレビュー」を強化

４．本行動計画の期間

➢ 第４次行動計画（案）はオリパラ大会開催までを視野に入れ、大会終了後に見直しを実施。その間であっても、必要に応じて見直す。

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

官民連携による重要インフラ防護の推進

重要インフラにおいて、機能保証の考え方を踏まえ、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、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。

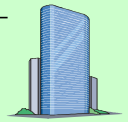
重要インフラ（１３分野）

- 情報通信
- 金融
- 航空
- 鉄道
- 電力
- ガス
- 政府・行政サービス（含・地方公共団体）
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油

ＮＩＳＣによる調整・連携

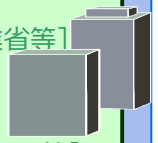
重要インフラ所管省庁（５省庁）

- 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、鉄道、物流］



関係機関等

- 情報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］
- 情報セキュリティ関係機関［NICT、IPA、JPCERT等］
- サイバー空間関連事業者［各種ベンダー等］



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（案）

安全基準等の整備・浸透

重要インフラ各分野に横断的な対策の策定とそれに基づく、各分野の「安全基準」等の整備・浸透の促進

情報共有体制の強化

連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施、演習・訓練間の連携による重要インフラサービス障害対応体制の総合的な強化

リスクマネジメント及び対処態勢の整備

リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの支援

防護基盤の強化

重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

第４次行動計画の基本的考え方・要点

「重要インフラ防護」の目的

重要インフラにおいて、機能保証の考え方を踏まえ、自然災害やサイバー攻撃等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、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。

「基本的な考え方」

情報セキュリティ対策は、一義的には重要インフラ事業者等が自らの責任において実施するものである。
重要インフラ全体の機能保証の観点から、官民が一丸となった重要インフラ防護の取組を通じて国民の安心感の醸成を目指す。

- 重要インフラ事業者等は事業主体として、また社会的責任を負う立場としてそれぞれに対策を講じ、また継続的な改善に取り組む。
- 政府機関は、重要インフラ事業者等の情報セキュリティ対策に関する取組に対して必要な支援を行う。
- 取組に当たっては、個々の重要インフラ事業者等が単独で取り組む情報セキュリティ対策のみでは多様な脅威への対応に限界があることから、他の関係主体との連携をも充実させる。

各関係主体（重要インフラ事業者等、政府機関、情報セキュリティ関係機関等）の在り方

- 自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、相互に自主的に協力する。
- 重要インフラサービス障害の規模に応じて、情報に基づく対応の５Ｗ１Ｈを理解しており、重要インフラサービス障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

重要インフラ事業者等の経営層の在り方

- 情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し、機能保証の観点から情報セキュリティ対策に取り組むこと。
- 自社の取組が社会全体の発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。
- 情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報の開示等に取り組むこと。
- 上記の各取組に必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。

第４次行動計画 施策①：安全基準等の整備及び浸透

重要インフラ防護能力の維持・向上を目的として、セキュリティ対策のPDCAに沿って「指針」及び「安全基準等」の継続的改善を推進する。

※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
※指針・・・・・・安全基準等の策定・改定に資するため、分野横断的に必要度の高い対策項目を収録したもの

現状の課題

- 自主的に見直しの必要性を判断し改善できるサイクル自体は重要インフラ事業者等の行動規範として浸透しつつあるが、PDCAサイクルのCheck（確認）及びAct（是正）における取組の定着が課題である

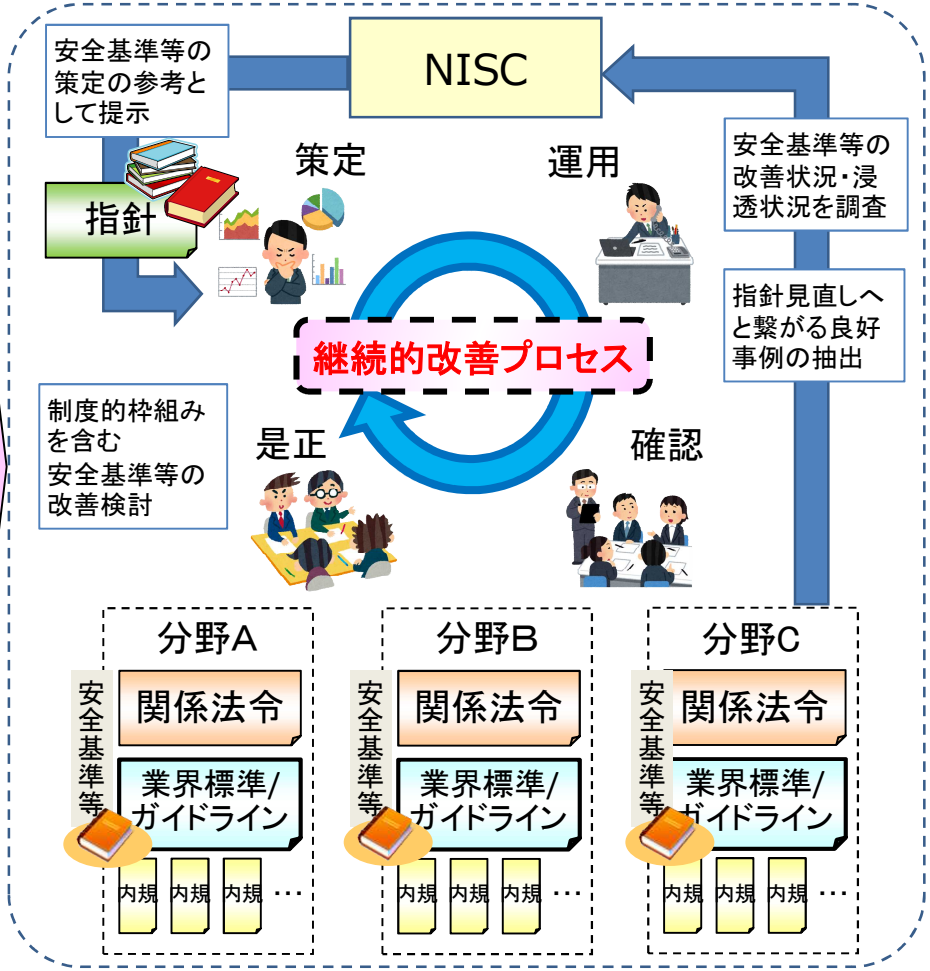
行動計画期間中の施策

（１） 指針の継続的改善
- 情報セキュリティ文化の醸成やPDCAサイクルの実行に責任を持つ経営層が認識すべき事項及び行動を指針改定時に詳細化
- 機能保証の考え方を踏まえた事業継続計画・コンティンジェンシープラン等の対処態勢整備の必要性を指針改定時に明記

（２） 安全基準等の継続的改善
- セキュリティ対策のPDCAサイクルに沿った業界標準/ガイドラインの改善プロセスの推進
- 情報セキュリティの取組の保安規制への位置付けや、関係法令等におけるサービス維持レベルの具体化等、制度的枠組みを含めた検討の実施

（３） 安全基準等の浸透
- 重要インフラ事業者等への毎年のアンケート調査により、セキュリティ対策状況を把握するとともに、アンケートへの回答を通じ、事業者等が対策の課題、解決策等を認識可能となるよう支援

第４次行動計画に基づく取組



第４次行動計画 施策②：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情報セキュリティ動向に迅速に対応できるよう、官民間や分野内外間における情報共有の強化に取り組む。

現状の課題

- 情報共有を行う意義・必要性の訴求
- 迅速かつ効果的な情報共有体制の検討
- 共有すべき情報の理解・浸透・活性化
- 民間の自主的取組に関する普及・促進　　等

行動計画期間中の施策

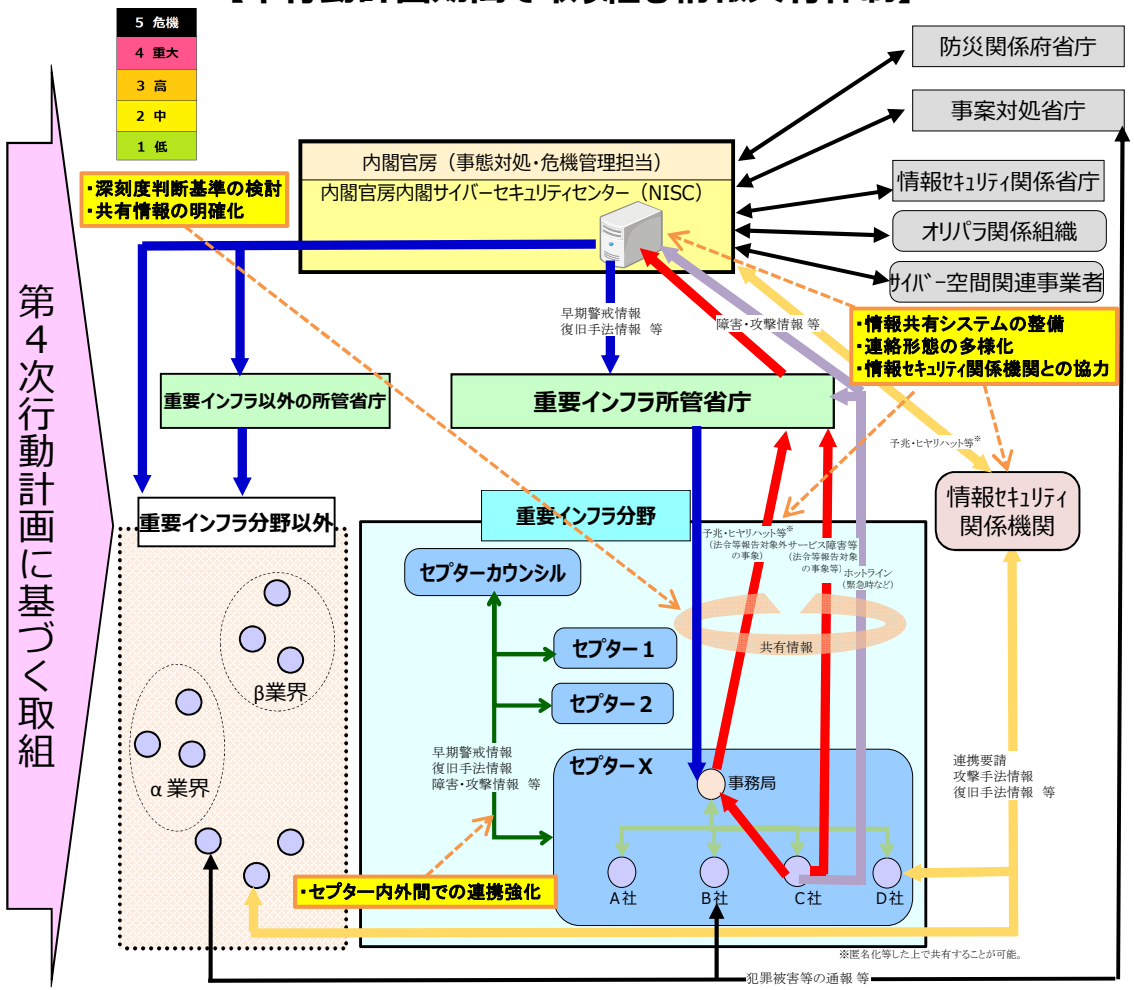
（１）情報共有体制の充実
- 新たな連絡形態(セプター事務局経由)の導入
- オリパラ大会等を見据えた情報共有システムの整備
- 情報セキュリティ関係機関との積極的な協力

（２）情報共有の更なる促進
- 重要インフラサービス障害の深刻度判断基準の検討
- 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

（３）民間活動の更なる活性化
- セプター内、セプター間の情報共有の更なる充実
- 先進的な取組を行うISAC等の活動の展開

【本行動計画期間で取り組む情報共有体制】



第４次行動計画 施策③：障害対応体制の強化

重要インフラ事業者における重要インフラサービス障害対応の実態や演習ニーズに適合した演習・訓練の充実による重要インフラ防護能力の維持・向上。

現状の課題

- より効果的で実用的な分野横断的演習の企画推進
- 参加者拡大や、重要インフラサービス障害発生時の関係主体間の在り方に適合した演習成果の普及・浸透

行動計画期間中の施策

（１）分野横断的演習の継続と改善

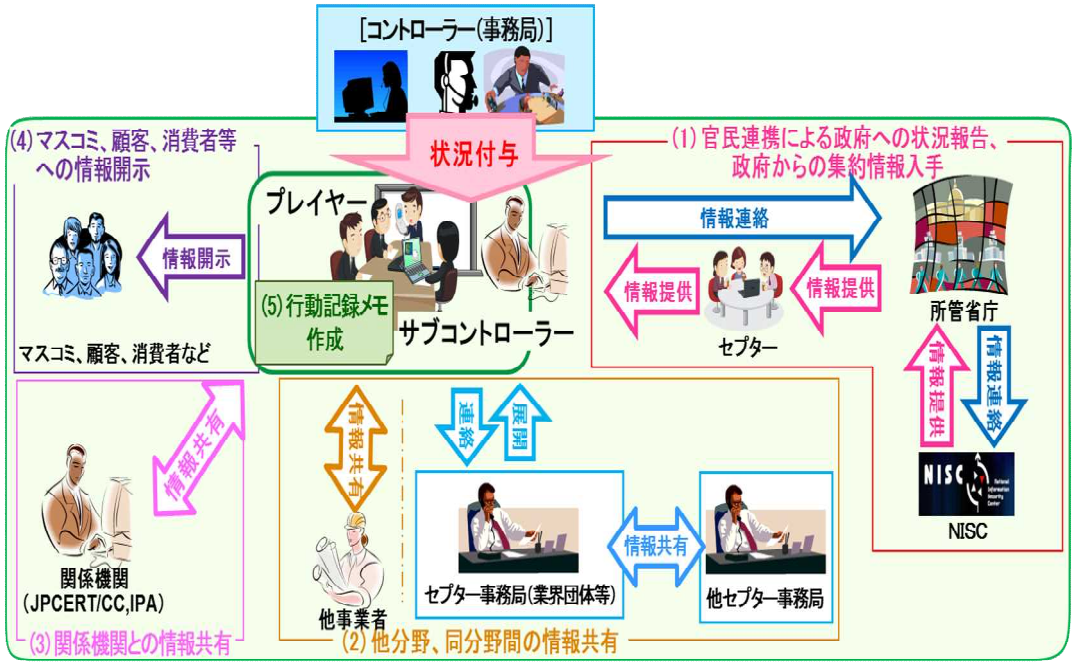
- 重要インフラ事業者の実態に即した演習企画
  - ・重要インフラ事業者の演習ニーズ取り込み
  - ・最新の攻撃手法を考慮した演習シナリオ整備
  - ・外縁の事業者や密接に関連する関係主体の参画

（２）参加者大幅増に即した演習成果の浸透

- 新規参加への促進
- 他演習・訓練との相互連携
- 経営理解増進に寄与する演習企画
- 自社演習実施に資する演習ノウハウの還元
  - ・仮想的な演習環境の提供　等

第４次行動計画に基づく取組

分野横断的演習の概要（ステークホルダー相関図）



分野横断的演習の継続と充実

- より実態に即した演習企画
- 外縁の事業者も含めた新規参加の促進
- 他演習・訓練との相互連携
- 経営理解増進に資する演習企画
- 演習ノウハウの還元

重要インフラ防護能力の維持・向上

第４次行動計画 施策④：リスクマネジメント及び対処態勢の整備

重要インフラサービスの安全・持続的な提供に向けて、重要インフラ事業者等が実施するリスクマネジメント及びこれを踏まえた対処態勢整備を推進する。

現状の課題

- リスクアセスメントの重要性については認識が広まりつつあるが、その考え方や実施方法については十分に浸透していない。
- 重要インフラサービス障害が発生した際に備えた対処態勢整備の必要性が高まっているが、具体的な方向性・支援策等が示されていない。

行動計画期間中の施策

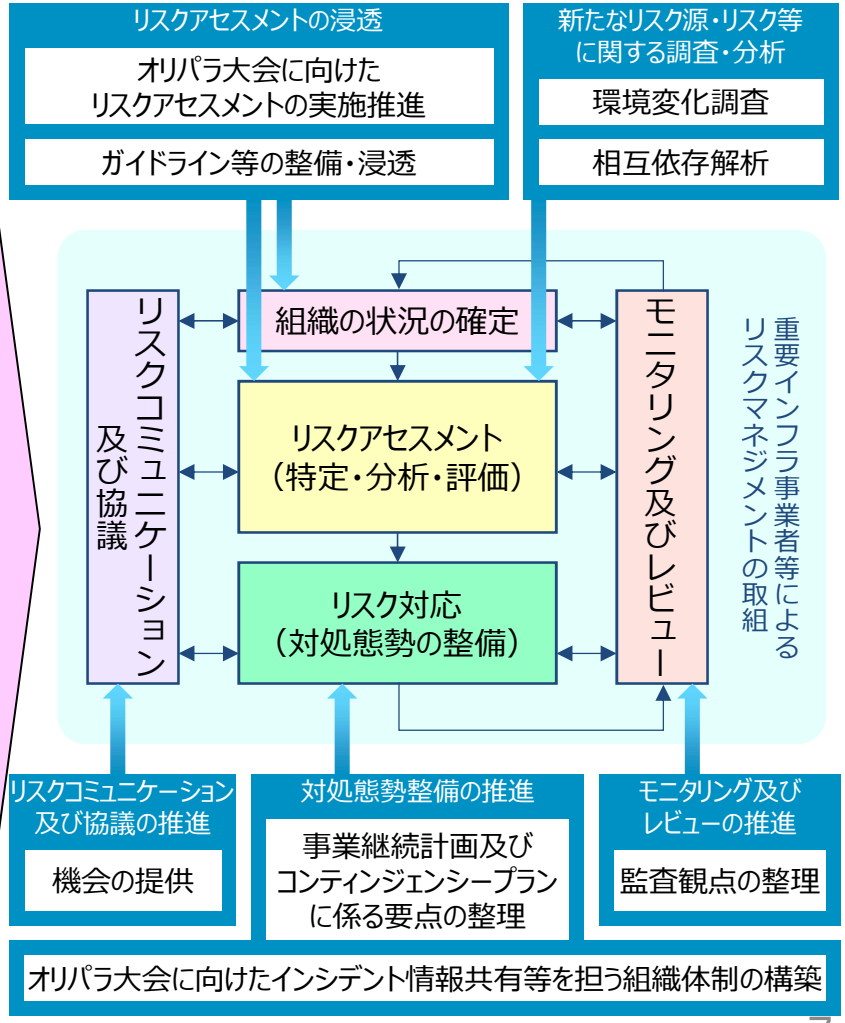
（１）リスクマネジメントの標準的な考え方

（２）リスクマネジメントの推進

- リスクアセスメントの浸透
  - ・オリパラ大会に向けたリスクアセスメントの実施推進
  - ・機能保証の考え方に立脚したリスクアセスメントガイドライン等の整備・浸透
- 新たなリスク源・リスク等に関する調査・分析
  - ・環境変化調査　・相互依存性解析
- 対処態勢整備の推進
  - ・機能保証の考え方を踏まえた事業継続計画及びコンティンジェンシープランの要点の整理
  - ・オリパラ大会に向けたインシデント情報共有等を担う組織体制の構築
- リスクコミュニケーション及び協議の推進
  - ・内部ステークホルダー間、関係主体間での情報・意見交換の機会の提供
- モニタリング及びレビューの推進
  - ・重要インフラ事業者等が自主的に行う内部監査等の監査観点の整理

（３）本施策と他施策との相互反映プロセスの確立

第４次行動計画に基づく取組



第４次行動計画 施策⑤：防護基盤の強化

防護範囲の見直し、広報広聴、国際連携、規程類の整備、経営層への働きかけ、人材育成等、重要インフラ防護の全体を支える共通基盤的な取組を強化する。

現状の課題

- 環境変化を踏まえた面としての防護
- 広報広聴活動の一層の充実
- 国際的な情報セキュリティ対策水準の向上
- 情報セキュリティに関する経営層の意識向上
- 情報セキュリティ人材の質的・量的な充実

行動計画期間中の施策

（１）重要インフラに係る防護範囲の見直し
- 「面としての防護」に向けた取組、国の安全等の確保の観点からの取組

（２）広報広聴活動の推進
- 行動計画の枠組みや取組等の国民への積極的な発信

（３）国際連携の推進
- 国際的な情報セキュリティ対策の水準向上のための積極的な寄与

（４）経営層への働きかけ
- 情報セキュリティに関する意識向上のための経営層への働きかけ

（５）人材育成等の推進
- 橋渡し人材の育成、演習や教育の実施、人材交流の推進等

第４次行動計画に基づく取組

「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」

重要インフラ事業者等の対策例

Plan（準備）／予防・抑止

方針
- 抽出した課題に基づくリスクアセスメント
- 基本方針の策定／見直し

規定
- 内規の策定／見直し（情報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
- 情報セキュリティ対策に係るロードマップの作成／見直し
- 情報セキュリティ対策計画の作成／見直し

体制
- 予算・体制の確保
- 人材育成・配置・ノウハウの蓄積
- 外部委託における対策

構築
- 情報セキュリティ要件の明確化／変更
- 情報セキュリティ対策（技術）に係る設計・実装／保守
- 情報セキュリティ対策（運用）に係る設計・手順書化／保守

Do（実働）／検知・回復

共通
- 情報セキュリティ対策の運用（監視・統括）
- 情報セキュリティ対策の運用状況把握
- 関係主体間による情報共有

平時
- 情報セキュリティ対策の運用（攻撃傾向の把握等）
- 情報セキュリティ対策状況の対外説明

障害発生時
- 重要インフラサービス障害に対する防護・回復
- 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
- 情報セキュリティ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
- ITに係る環境変化の調査・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

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）

安全基準等の浸透状況等に関する調査（内閣官房）

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）

障害対応体制の強化

分野横断的演習（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）

重要インフラ所管省庁訓練（重要インフラ所管省庁）

リスクマネジメント及び対処態勢の整備

リスクコミュニケーション及び協議の推進（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）

対処態勢整備の推進（内閣官房／重要インフラ所管省庁）

ﾓﾆﾀﾘﾝｸﾞ及びﾚﾋﾞｭｰの推進（内閣官房／重要インフラ所管省庁）

新たなリスク等の調査・分析（内閣官房／重要インフラ所管省庁）

防護基盤の強化

防護範囲の見直し／広報広聴活動／国際連携／ｾｷｭﾘﾃｨ・ﾊﾞｲ・ﾃﾞｻﾞｲﾝの推進／経営層への働きかけ／人材育成等の推進／規程類の整備（内閣官房／重要インフラ所管省庁）

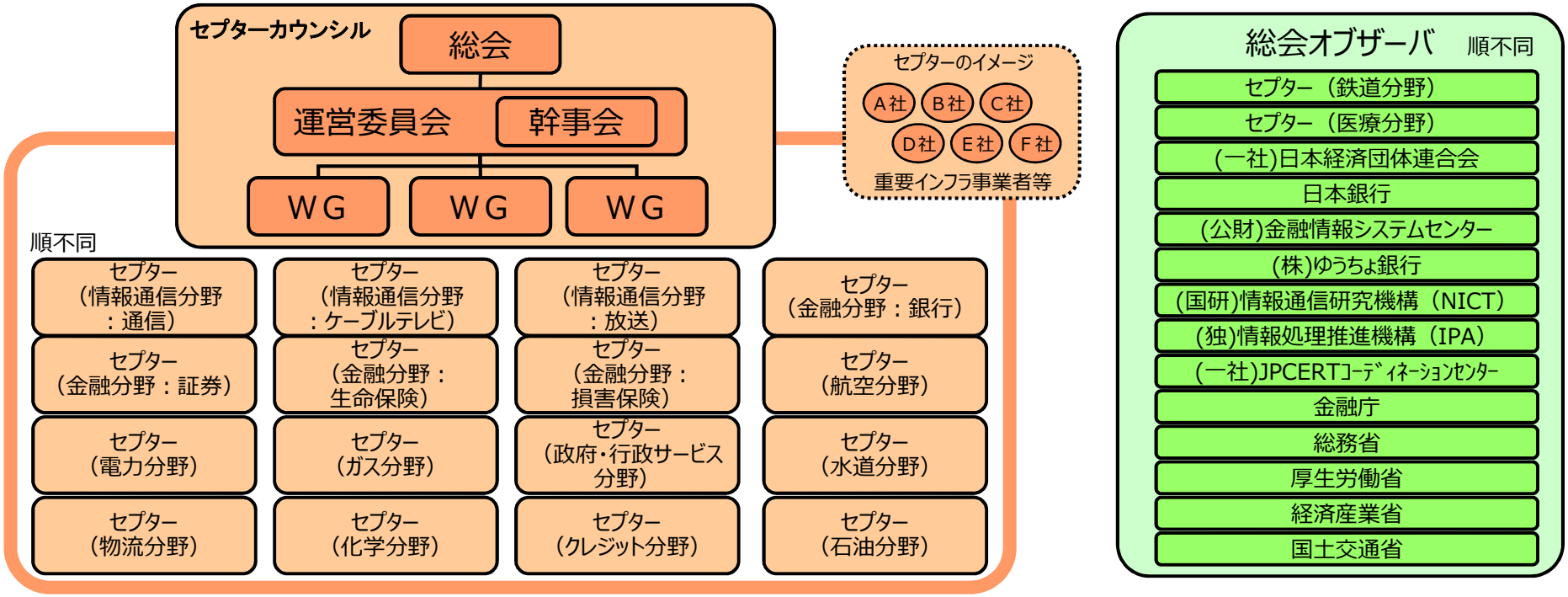
セプターとセプターカウンシル

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。



情報共有体制の強化・防護範囲の見直しに関する取組状況

2016年9月末日現在

■ セプターの拡充等

重要インフラ分野	情報通信			金融				航空	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	航空	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 銀行等CEPTOAR	証券CEPTOAR	生命保険CEPTOAR	損害保険CEPTOAR	航空分野における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
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	(一社)全国銀行協会 事務・決裁システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部組織法務グループ	(一社)日本損害保険協会 ＩＴ推進部 品質グループ	定期航空協会	(一社)日本鉄道電気技術協会	電気事業連合会 情報通信部	(一社)日本ガス協会 技術部	地方公共団体情報システム機構 情報化支援戦略部	厚生労働省 医政局 研究開発振興課 医療技術情報推進室	(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）	24社・団体	333社	194社 1団体	1,433社	260社 7機関	41社	29社（オブザーバ3社含む）	14社 1団体	22社 1団体	12社 2機関	10社	47都道府県 1,741市区町村	1グループ 6機関	8水道事業体	6団体 16社	13社	28社（10.1時点）	14社・グループ
2014年4月時点	28社・団体	252社	193社 1団体	1,411社	251社 7機関	43社	30社（オブザーバ3社含む）	2ｸﾞﾙｰﾌﾟ 3機関	22社 1団体 1機関	12社 2機関	10社	47都道府県 1,742市区町村	1グループ 2機関	8水道事業体	6団体 16社	―	―	―
NISCからの情報の展開先（構成員以外）	399社・団体										38社		375社・機関	内容に応じ1,361事業体へ展開				
	その他（核物質関連事業所等（内容に応じ展開先を選定）、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））																	
事務局の民間移行	航空分野（国土交通省航空局 → 定期航空協会）、鉄道分野（国土交通省鉄道局 →（一社）日本鉄道電気技術協会）																	

■ その他

既存事業領域を越える連携等	情報通信（Telecom-ISACの活動を新たに設立されたICT-ISACに移行し一部の放送事業者が加盟）、電力（ISAC設立を模索）、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への拡張）、制御システム（JPCERT/CCが提供するConPaS等） 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WAISE（JPCERT/CC: 情報セキュリティに係る情報全般）

（※）本頁は、2016年9月時点の状況を示すものであり、セプターの構成員に関する情報は、定期的（２回/年）に更新し、内閣ｻｲﾊﾞｰｾｷｭﾘﾃｨｾﾝﾀｰのＨＰ（http://www.nisc.go.jp/）に掲載。