資料 6-2

NISC National Information Security Center

重要インフラの情報セキュリティ対策に係る第3次行動計画（案）の概要

２０１４年３月１１日

重要インフラ専門委員会　事務局

「重要インフラの情報セキュリティ対策に係る第3次行動計画（案）」の全体概要

これまでの取組み

重要インフラ

「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、わが国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの※」との定義　※サイバーセキュリティ戦略（平成25年6月10日　情報セキュリティ政策会議決定）より抜粋

環境の変化

- IT依存度の高まり　→　システム障害時の影響の広範囲化・対応の困難化
- 複雑化・巧妙化するサイバー攻撃

行動計画の意義

重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画(注)

（参考）第1次行動計画（平成17年12月13日 情報セキュリティ政策会議決定）
第2次行動計画（平成21年2月3日　情報セキュリティ政策会議決定）

（注）日本再興戦略-JAPAN is BACK-（平成25年6月14日閣議決定）及びサイバーセキュリティ戦略において今年度内に新たな行動計画を策定する方針を決定

重要インフラの情報セキュリティ対策に係る第2次行動計画

主な施策

1. 安全基準等の整備及び浸透
2. 情報共有体制の強化
3. 共通脅威分析
4. 分野横断的演習　等

主な課題

社会・技術面での環境変化を踏まえた改善・補強が必要な箇所が存在

1. 重要インフラ事業者等のPDCAサイクルとの整合に基づく指針の見直し
2. 大規模IT障害発生時の対応体制の明確化
3. 演習・訓練に係る関係主体の連携の在り方の模索
4. 環境変化・脅威に適切に対応するための取組
5. 広報公聴、国際連携の強化に追加すべき基盤強化に資する取組　等

第2次行動計画の基本的な骨格を維持しつつ、
第2次行動計画の課題等を踏まえた修正・補強

重要インフラの情報セキュリティ対策に係る第3次行動計画（案）

施策群の構成と主要なポイント

1. 安全基準等の整備及び浸透	対策途上や中小規模の重要インフラ事業者等への情報セキュリティ対策の「成長モデル」の訴求
2. 情報共有体制の強化	平時の体制の延長線上にある大規模IT障害対応時の情報共有体制の明確化
3. 障害対応体制の強化	関係主体が実施する演習・訓練の全体像把握と相互連携による障害対応体制の総合的な強化
4. リスクマネジメント	重要インフラ事業者等におけるリスクに対する評価を含む包括的なマネジメントの支援
5. 防護基盤の強化	関連国際標準・規格や参照すべき規程類の整理・活用・国際展開　等

- ◆重要インフラ分野を現行の10分野から13分野に拡大（化学、クレジット及び石油の各分野を追加）
- ◆行動計画の要点として、「経営層に期待する在り方」等を示すとともに、PDCAサイクルに基づく事業者等の対策例とこれに関連する国の施策を一覧化
- ◆客観的な評価指標の提示とこれに基づく定期的な評価・改善の実施

情報セキュリティ政策の全体像と重要インフラとの関係

各省における試行錯誤

サイバー攻撃への対応を中心とした対策実施時期

IT障害への対応も含めた総合的な対策基盤づくりの推進

サイバー攻撃事態発生を念頭、新たな環境変化対応、能動的情報セキュリティ対策
「事故前提社会」への対応力強化等成熟した情報セキュリティ先進国へ向けた取組

対策推進の枠組み

約1箇月で組織を立ち上げ

基本戦略

【基本戦略】

国民を守る情報セキュリティ戦略
（2010.5.11 情報セキュリティ政策会議決定）

第１次情報セキュリティ基本計画
（2006.2.2 情報セキュリティ政策会議決定）

第２次情報セキュリティ基本計画
（2009.2.3 情報セキュリティ政策会議決定）

ｻｲﾊﾞｰｾｷｭﾘﾃｨ戦略
（2013.6.10）
（情報セキュリティ政策会議決定）

【年度計画】
※ 基本戦略に基づき策定する年度計画

SJ2006 SJ2007 SJ2008 SJ2009 JS2010 JS2011 JS2012 SS2013

政府機関対策

情報セキュリティポリシーに関するガイドライン
（2000.7 情報ｾｷｭﾘﾃｨ対策推進会議決定）

政府機関の情報セキュリティ対策のための統一基準（第１～3版）
（2005.12.13 情報セキュリティ政策会議決定）

政府機関の情報セキュリティ対策のための統一基準（第４版～）
（2009.2.3 情報セキュリティ政策会議決定）

第３次統一基準群

重要ｲﾝﾌﾗ対策

重要インフラのサイバーテロ対策に係る特別行動計画
（2000.12 情報ｾｷｭﾘﾃｨ対策推進会議決定）

重要インフラの情報セキュリティ対策に係る行動計画
（2005.12.13 情報セキュリティ政策会議決定）

2012.4.26 改定

重要インフラの情報セキュリティ対策に係る第２次行動計画
（2009.2.3 情報セキュリティ政策会議決定）

第３次行動計画

組織体制

内閣官房情報セキュリティ対策推進室（2000.2設置）

① 内閣官房情報セキュリティセンター（2005.4 設置）
② 情報セキュリティ政策会議（2005.5 設置）
③ GSOC（2008.4 運用開始）

基本戦略

政府

重要インフラ

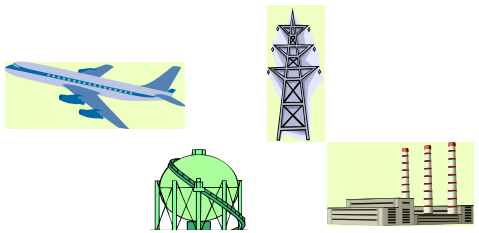
第2次行動計画の全体像

官民連携による重要インフラ防護の推進

重要インフラにおけるIT障害が国民生活、社会活動に重大な影響を及ぼさないことを目指す
①予防的な対策と再発防止対策の両側から対処（具体的には、安全基準の整備、情報共有体制の強化等。）
②重要インフラ事業者等における情報セキュリティ対策の浸透状況や急速な技術進展等を踏まえたＰＤＣＡの促進

重要インフラ（10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



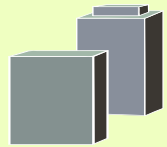
NISCによる
調整・連携

重要インフラ所管省庁（5省庁）

- 金融庁 ［金融分野］
- 総務省 ［情報通信分野、行政分野］
- 厚生労働省 ［医療分野、水道分野］
- 経済産業省 ［電力分野、ガス分野］
- 国土交通省 ［航空分野、鉄道分野、物流分野］

関係機関等

- 情報セキュリティ関係省庁
- 事案対処省庁
- その他関係機関



重要インフラの情報セキュリティに係る第2次行動計画（平成21～25年度）

（1）安全基準等の整備・浸透

重要インフラ各分野に横断的な「指針」に基づいて、「安全基準」等の浸透を図る

（2）情報共有体制の強化

障害・攻撃に関する情報の共有により、個々の主体による孤立した対応から、社会全体としての対応を促進

重要インフラ防護対策の向上

（3）共通脅威分析

複数分野に共通する潜在的な脅威の分析

（4）分野横断的演習

防護対策向上のための課題抽出

環境変化への対応

刻々と変化する環境の変化への対策の機敏な対応

第3次行動計画の策定までの流れ

サイバーセキュリティ戦略

● 「基本的な考え方」
- 情報の自由な流通の確保
- 深刻化するリスクへの新たな対応
- リスクベースによる対応の強化
- 社会的責務を踏まえた行動と共助

● 「重要インフラ事業者等における対策」
- 情報システム等の特性に応じた情報セキュリティ対策の重点化
- 障害、攻撃・脅威・脆弱性等の情報共有の推進
- サイバー攻撃に対する連携対応能力の強化
- 制御系機器・システム等における国際標準との整合、評価・認証スキームの導入
- 重要インフラの分野等の見直し

第2次行動計画

●目標
- 重要インフラにおけるIT障害の発生を限りなくゼロにする

●基本的考え方
- 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

●各施策の成果と課題
- 安全基準等の整備・浸透
- 情報共有体制の強化
- 共通脅威分析
- 分野横断的演習
- 環境変化への対応

重要インフラ専門委員会における検討

- 戦略の基本的考え方の反映
- 第2次行動計画の理念・基本的考え方の継承の是非
- 戦略に記載の対策を踏まえた検討項目の整理
- 第2次行動計画の成果と課題を踏まえた検討項目の整理

→

- 「重要インフラ防護」の目的の明確化
- 「基本的考え方」の整理と具体化
- 考慮すべき課題と施策群の在り方の整理
- 第2次行動計画の施策群の修正、補強等

パブリックコメントを経て情報セキュリティ政策会議にて決定

第3次行動計画

第2次行動計画の成果と課題

第2次行動計画での主な成果

- 所期の目標について一定の成果を挙げたものと評価
  （第2次行動計画が策定当時の最新知見を踏まえた作成であることを考慮）
  - 指針・安全基準等のPDCAサイクルを確立
  - 関係主体間の情報共有体制を構築、運用の安定化
  - 事業者等におけるBCP策定に資する基礎資料を提供
  - 演習を通じた事業者等のIT障害時の早期復旧手順、BCPの検証に活用
  - 広報公聴活動の実施、関係主体間のコミュニケーションの充実、諸外国との連携の実現

主な課題

- 社会・技術面での環境変化を踏まえた改善・補強が必要な箇所が存在
  - 事業者等のPDCAサイクルとの整合に基づく指針の見直し
  - 大規模IT障害対応時の情報共有体制を平時の体制の延長線上で構築
  - その影響の大きさに応じた複数分野における脅威を調査対象に追加
  - 演習成果の更なる普及・浸透、演習・訓練に係る関係主体の連携の在り方
  - 広報公聴、中長期的な環境変化の調査、国際連携の強化

上記の課題及びサイバーセキュリティ戦略における関係課題を踏まえ、第3次行動計画の策定に反映

重要インフラ分野の見直し

サイバーセキュリティ戦略

「我が国において、現在、重要インフラとは位置づけられていないが、現行10分野と同等にその情報システムの障害が国民生活及び社会経済活動に多大な影響を及ぼす恐れのある分野について、今後、当該インフラにおける情報システムの位置づけを踏まえ、重要インフラの範囲及びそれぞれの性格に応じた対応の在り方等について、検討を行う。」

検討結果

区分	視点・必要性	分野
当該分野が有する情報システムが障害に至った場合の影響を考慮して追加する分野	情報サービス提供価値、情報システムが処理するサービスの提供規模	クレジット
	制御が困難な状態において生じ得るリスクの大きさ	化学、石油
既存の重要インフラ分野における情報システムに与える影響を考慮して追加する分野	既存の重要インフラ分野との間で認め得る相互依存性	石油（再掲）

- 第3次行動計画において、既存の10分野に加え、上記3分野を追加
- 追加分野については、重要インフラ分野としての活動開始に向け準備中
  －安全基準等の整備、情報共有体制の確立等に向けた活動計画の策定　等

第3次行動計画における施策群と補強・改善の方向性等

- 第2次行動計画の施策群の基本的な骨格の維持
- 必要に応じた個別施策とその実施体制等の見直しによる当該施策の修正・補強

第3次行動計画における施策群	第2次行動計画の施策群との対応	第2次行動計画からの補強・改善の方向性
1．安全基準等の整備及び浸透	「[1] 安全基準等の整備及び浸透」を基本的に踏襲	○他施策の結果を指針・対策編に反映するプロセスの明示 ○指針による成長モデル等の訴求及び対策の実情の調査
2．情報共有体制の強化	「[2] 情報共有体制の強化」を基本的に踏襲	○新たな関係主体を含めた情報共有体制における各関係主体の位置付けの見直し及び関係主体間の関係の再整理 ○サイバー攻撃関係情報の増加を踏まえた共有すべき情報（脅威の類型等）の見直し ○平時における対応を念頭に置いた大規模IT障害対応時の事案対処体制の明確化
3．障害対応体制の強化	「[4] 分野横断的演習」を整理	○重要インフラ関係の演習・訓練の全体像を把握した上でIT障害対応体制の総合的な強化 ○新たな関係主体との連携を念頭に置いた横断的演習の質的改善
4．リスクマネジメント	「[3] 共通脅威分析」を「[5] 環境変化への対応」の一部と統合した上で整理	○環境変化等に応じて生じる複数分野において大きな影響を生じ得るリスク源、将来的に多大な影響が予想される環境変化についての中長期的な調査の実施 ○重要インフラ事業者等が自らの状況を正しく認識し、活動目標を主体的に定めるに当たって必要となるリスクマネジネントの訴求
5．防護基盤の強化	「[5] 環境変化への対応」を「[3] 共通脅威分析」と統合される部分を除いた上で整理	○広報公聴、国際連携に加え、関連する国際標準・規格、参照すべき規程類の整理、活用方法の提示を追加

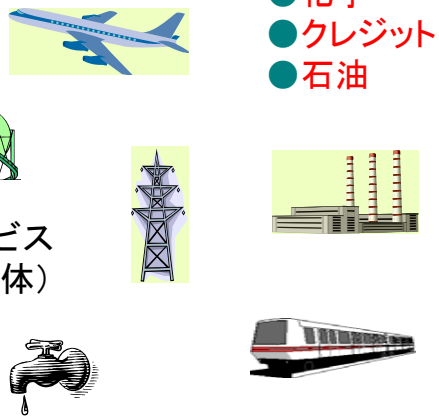
第3次行動計画の全体像

官民連携による重要インフラ防護の推進

重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するIT障害が国民生活や社会経済活動に
重大な影響を及ぼさないよう、IT障害の発生を可能な限り減らすとともにIT障害発生時の迅速な復旧を図ることで重要インフラを防護する

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

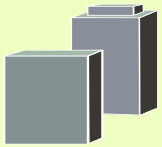


NISCによる
調整・連携

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
- 事案対処省庁
- 防災関係府省庁
- 情報セキュリティ関係機関
- サイバー空間関連事業者

重要インフラの情報セキュリティに係る第３次行動計画

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

IT障害関係情報の共有による、官民の関係者全体での平時・大規模IT障害発生時における連携・対応体制の強化

障害対応体制の強化

官民が連携して行う演習等の実施によるIT障害対応体制の総合的な強化

リスクマネジメント

重要インフラ事業者等におけるリスク評価を含む包括的なマネジメントの支援

防護基盤の強化

広報公聴活動、国際連携の強化、規格・標準及び参照すべき規程類の整理・活用・国際展開

第3次行動計画の基本的考え方・要点

基本的考え方

●「重要インフラ防護」の目的

- 重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するIT障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、IT障害の発生を可能な限り減らすとともにIT障害発生時の迅速な復旧を図ることで重要インフラを防護する。

●「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。また、重要インフラ防護における官民が一丸となった取組を通じて国民の安心感の醸成、社会の成長、強靭化及び国際競争力の強化を目指す。

- 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。

要　点

～ 行動計画推進に当たって期待する関係主体、更には事業者等の経営層に期待すること ～

●各関係主体の在り方

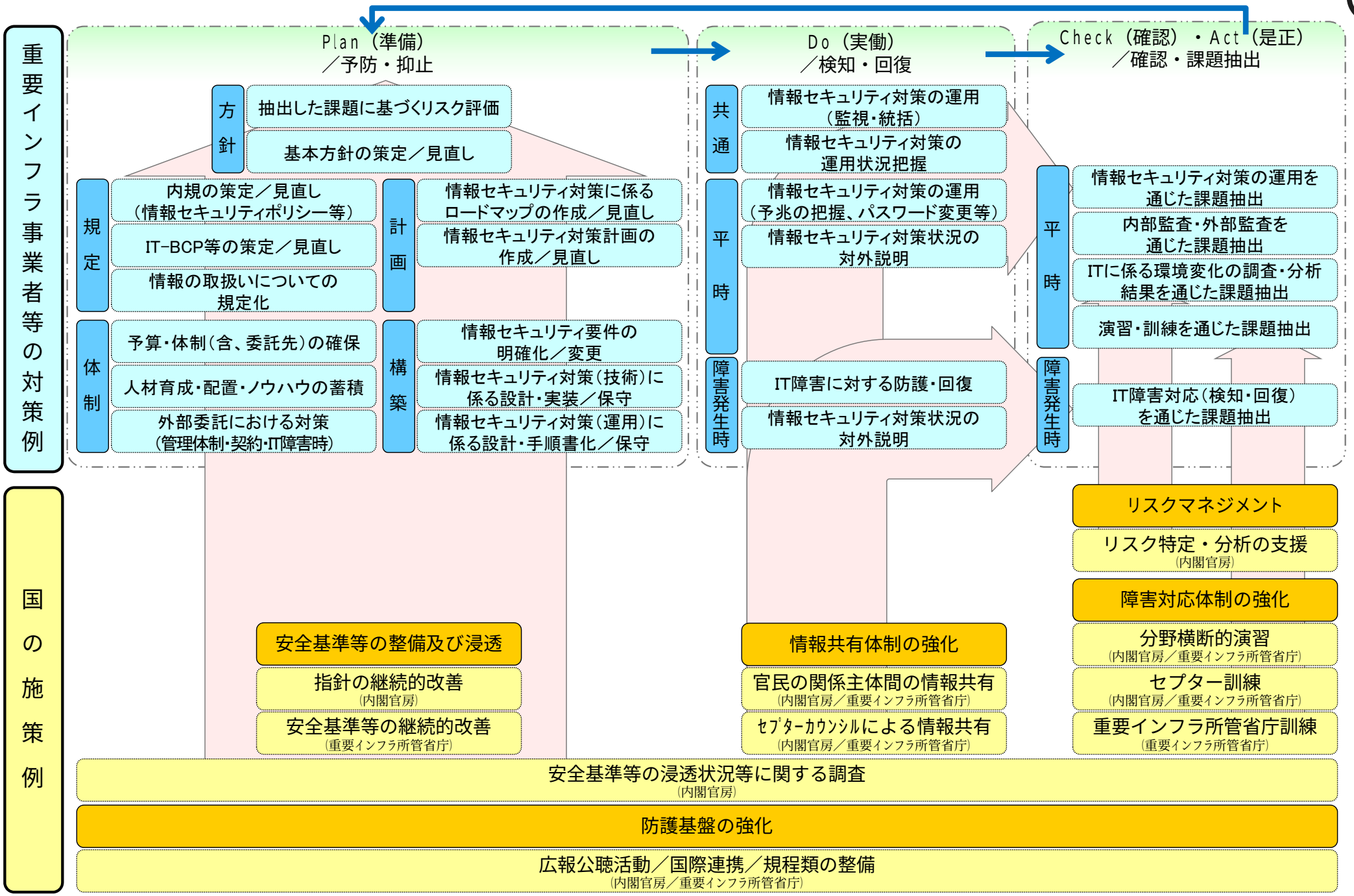
- 自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認する。また、他の関係主体の活動状況を把握し、相互に自主的に協力する。
- IT障害の規模に応じて、情報に基づく対応の5W1Hを理解しており、IT障害の予兆及び発生に対し冷静に対処ができる。多様な関係主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応ができる。

●重要インフラ事業者等の経営層の在り方

経営層は、上記の在り方に加え、以下の項目の必要性を認識し、実施できていること。

- 上記の目的達成に当たっての情報セキュリティを中心とするリスク源の認識。
- 上記のリスク源の評価及びそれに基づく優先順位を含む方針の策定。
- システムの構築・運用及び当該方針の実行に必要な計画の策定、並びに予算・体制・人材等の経営資源の継続的な確保。
- システムの運用状況の把握等を通じた当該方針の実行の有無の検証。
- 演習・訓練等を通じた他関係主体との情報共有を含む障害対応体制の検証及び改善策の有無の検証。

「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「国の施策例」



第3次行動計画期間における評価

基本的考え方

① 本行動計画に基づく取組の着実な進展・継続的な改善
⇒ 結果（アウトプット）を測る視点から、各年度における進捗状況を確認

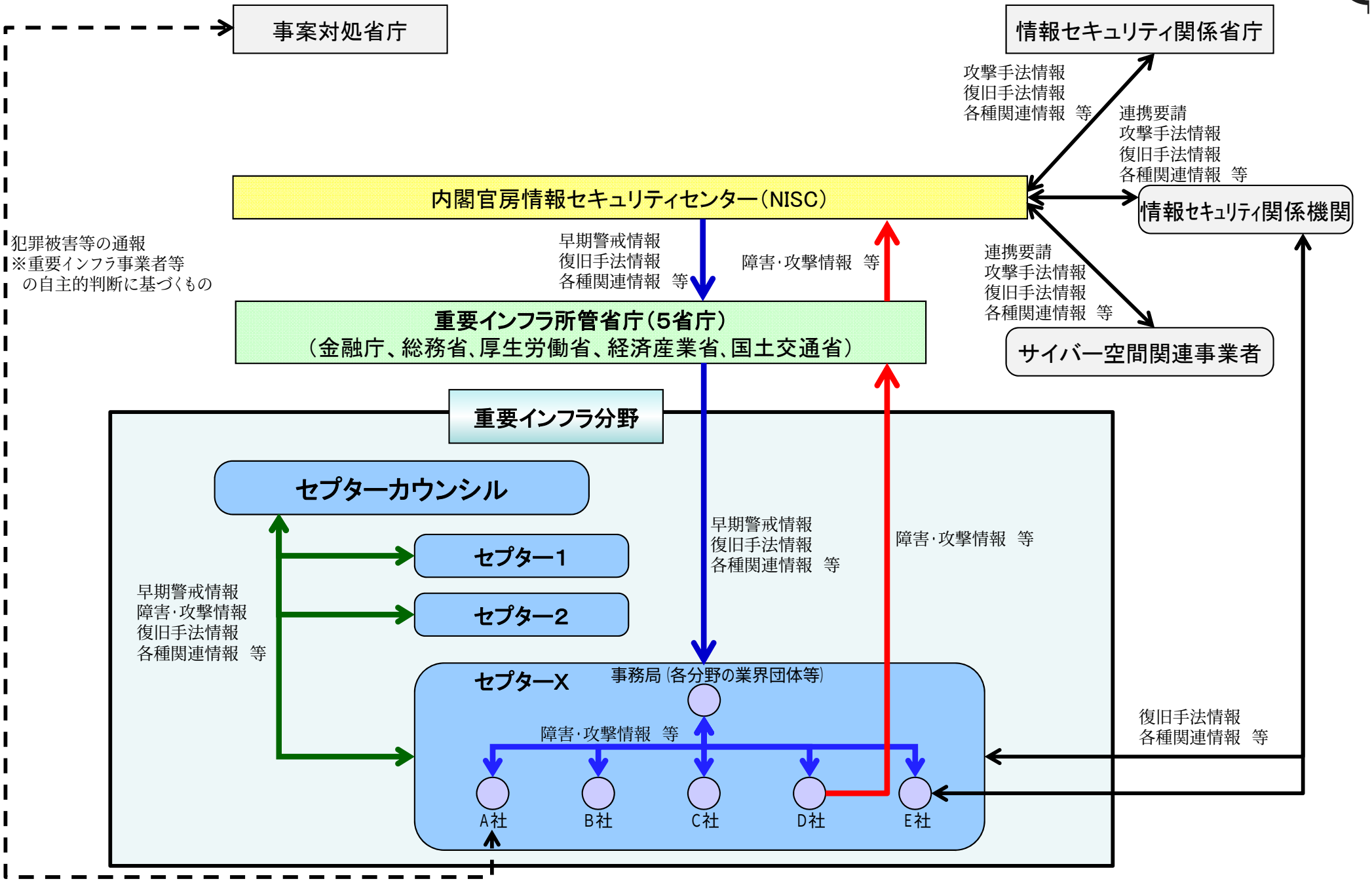
② 本行動計画の取組の妥当性の検証・必要に応じた見直し
⇒ 成果（アウトカム）を測る視点から、行動計画期間中の成果を確認

評価の全体像

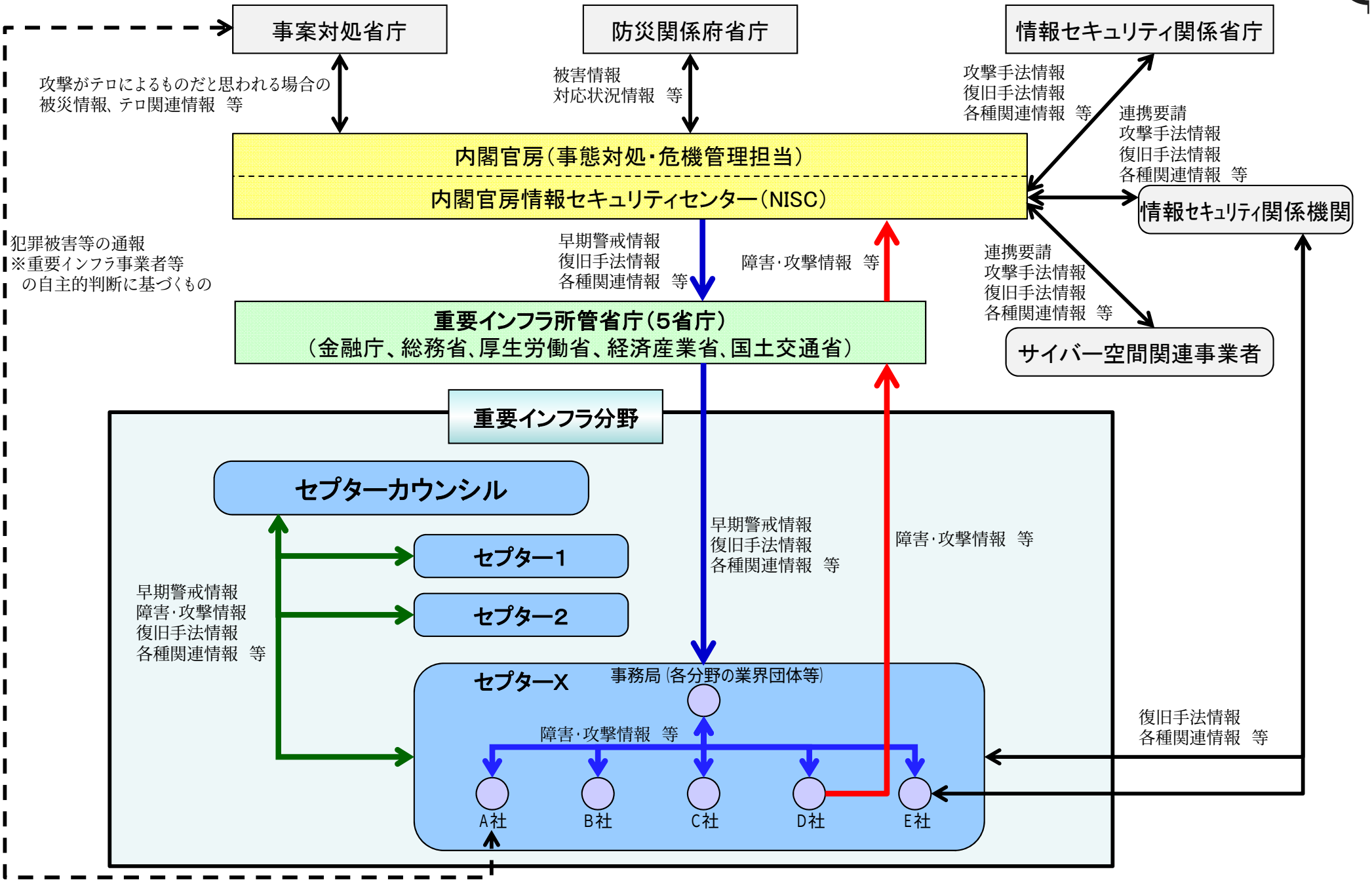
5W1H	結果（アウトプット） 個々の取組がどのような成果を挙げたか？	成果（アウトカム） 関係主体が実際にどの程度目標（理想とする社会像）に近づいたか？
評価対象	①重要インフラ事業者等の対策※ ②情報セキュリティ対策の施策群	重要インフラ防護能力の維持・向上に資する情報セキュリティ対策・施策の全体（＝第3次行動計画の枠組み）
評価主体	情報セキュリティ政策会議 （重要インフラ専門委員会）	情報セキュリティ政策会議 （重要インフラ専門委員会）
評価時期	各年度末	原則として3年に1度（行動計画期間終了時）
評価手法	①重要インフラ事業者等による対策の総合的な確認・検証に用いる指標 ②政府機関等による施策の確認・検証に用いる指標 に基づいて取組の進捗状況を検証	行動計画期間の目標（理想とする社会像）に対する達成度合いを総合的に実施（施策群の個別の成果に補完的な情報も加味）

※重要インフラ事業者等の自主的な対策の評価は自己評価に委ねる。

（参考）平時の情報共有体制



（参考）大規模IT障害対応時の情報共有体制



（参考）サイバーセキュリティ戦略　重要インフラ関連部分

3．取組分野
（1）「強靱な」サイバー空間の構築
②重要インフラ事業者等における対策

重要インフラ分野については、国民生活、社会経済活動や行政活動等のあらゆる活動が安定的に続けられるようにすることが必要であり、防護対象となる情報システム等の特性に応じ、政府機関等に準じた情報セキュリティ対策に取り組むことが必要である。

具体的には、重要インフラについて、重要インフラ事業者等におけるリスク評価手法に基づく情報セキュリティ対策の重点化を図るため、各分野における直近の安全基準等の策定・変更状況の把握・評価及びリスク分析を通じて、分野横断的に講じることが望ましいリスクを洗い出し、安全基準等を策定するための指針の中に反映するプロセスを確立する。

障害情報及び攻撃・脅威・脆弱性等に関する情報については、引き続き重要インフラ事業者等及びCEPTOARとの間における情報共有を推進するとともに、業種間での情報共有が難しい標的型攻撃に関する情報については、秘密保持契約に基づく情報共有体制を深化・拡充する。また、重要インフラ事業者等による事業所管省庁への迅速な報告、自主的判断に基づく事案対処省庁への通報及び関係機関との情報共有については、個人情報・秘密情報に配慮した上で促進する。さらに、重要インフラ事業者等、サイバー空間関連事業者及び関係CSIRTの間で、民間組織間の信頼関係を前提に、サイバー演習等の実施を促進しサイバー攻撃に対する連携対応能力の強化を図る。

重要インフラ分野におけるサプライチェーン・リスクへの対応強化を図るとともに、情報セキュリティの評価・認証の導入を進めていくことが重要である。具体的には、重要インフラ事業者等とサイバー空間関連事業者との脆弱性情報や攻撃情報等の情報共有等による連携の促進、SCADA等の制御系機器・システム等の調達・運用における国際標準に則った評価・認証導入の在り方の検討や、制御系機器・システムの評価・認証機関の設立に向けた取組を進めていく。

我が国において、現在、重要インフラとは位置づけられていないが、現行10分野と同等にその情報システムの障害が国民生活及び社会経済活動に多大な影響を及ぼす恐れのある分野について、今後、当該インフラにおける情報システムの位置づけを踏まえ、重要インフラの範囲及びそれぞれの性格に応じた対応の在り方等について、検討を行う。

以上を踏まえ、第2次行動計画の見直しを実施した上で、新たな行動計画を策定する。

さらに、これまで我が国では、大規模サイバー攻撃事態等を想定して、初動対処訓練の実施など事案発生時の対処態勢を構築するとともに、平素及び事案発生時の情報収集・集約体制の強化を図ってきている。今後も、大規模サイバー攻撃事態等が発生した際に官民が連携して的確な対応を行うことができる態勢を整備するため、必要に応じて諸外国の事例も参考としつつ、大規模サイバー攻撃事態等の発生を想定した関係者による対処訓練を毎年度実施するなど対処態勢を強化する。