

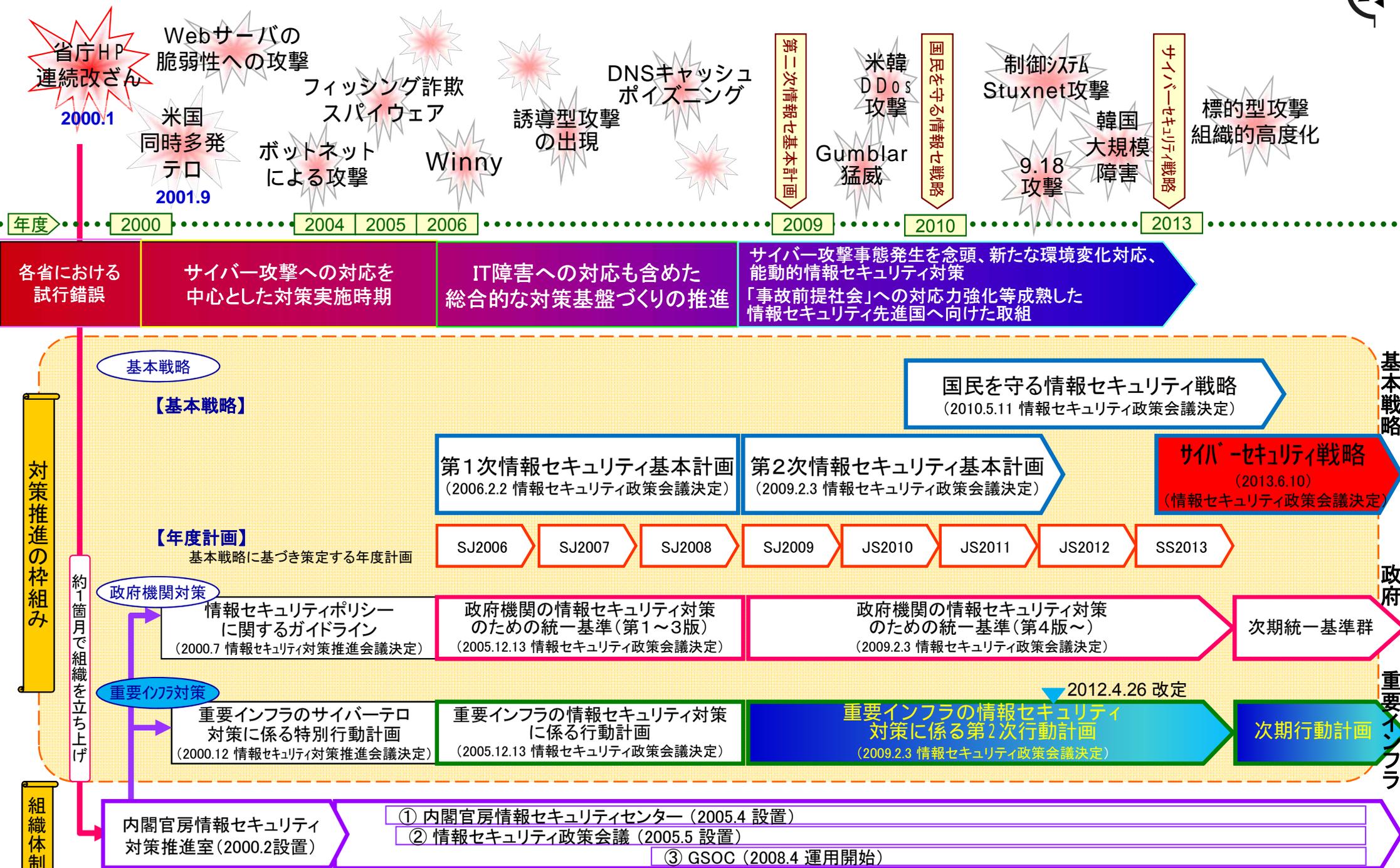


次期 重要インフラ行動計画（草案） とその策定に当たっての考え方

2013年11月29日

重要インフラ専門委員会 事務局

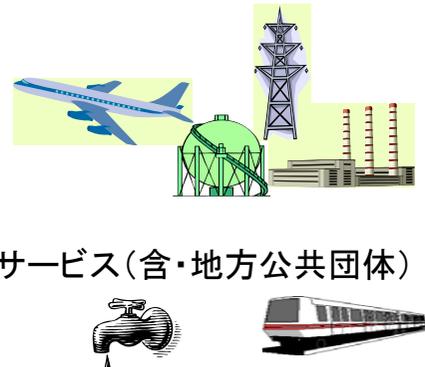
情報セキュリティ政策の全体像と重要インフラとの関係



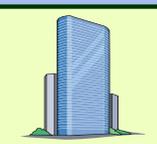
官民連携による重要インフラ防護の推進

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
予防的な対策と再発防止対策の両側から対応(具体的には、安全基準の整備、情報共有体制の強化等。)
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

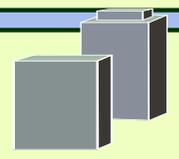
重要インフラ(10分野)

- 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
- 

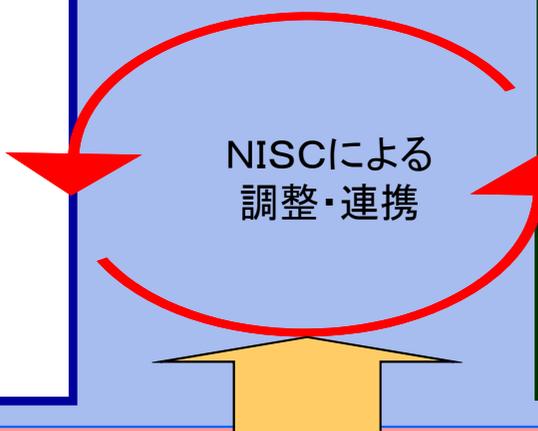
重要インフラ所管省庁(5省庁)

- 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]
 - 国土交通省 [航空分野、鉄道分野、物流分野]
 - 経済産業省 [電力分野、ガス分野]
- 

関係機関等

- 情報セキュリティ関係省庁
 - 事案対応省庁
 - その他関係機関
- 

NISCによる
調整・連携



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

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
 - ・ サイバー演習等の実施の促進
 - ・ 制御系機器・システム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

次期行動計画

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

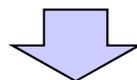
● 社会・技術面での環境変化を踏まえた改善・補強が必要な箇所が存在

- 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、次期行動計画の策定に反映

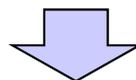
第2次行動計画での主な成果

- 指針と安全基準等の一体的・安定的な見直しサイクルを確立
- 情報セキュリティ対策の啓発推進を強化



主な課題

- 対策の重要性の増加
 - 事業者自身のみならず重要インフラ全体の防護能力の維持・強化にも効力が及ぶ
- 指針への事業者等の要望
 - 「対策について、段階的な(優先順位付けされた)指針にするとわかりやすい」
 - 「対策編で更なる具体的内容を提示してほしい」



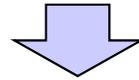
次期行動計画における施策像

- 重要インフラ防護能力の維持・強化、特に対策途上の事業者等による実効的かつ自主的な取組に資するPDCAサイクルの明確化

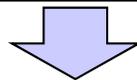
第2次行動計画での主な成果

- 官民連携による情報連絡・提供の枠組みを確立、それに基づく運用の安定化
- 民民間（セプター・セプター間）の情報共有体制を整備
- 事業者等における必要な情報の享受・活用

主な課題



- 情報の更なる細分化
 - －複雑化・巧妙化する攻撃手法に応じた連絡・提供手法の細分化
- 分野間における情報共有の頻度の格差
 - －情報連絡・提供が日常的に行われている分野とそうではない分野の顕在化
- 新たな関係主体との連携の在り方
 - －サイバー空間関連事業者、防災関係府省庁等との連携の在り方
- 大規模IT障害対応時における情報共有体制
 - －関係主体の全体像の把握、平時の体制の延長線上への構築

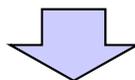


次期行動計画における施策像

- 新たな関係主体を含めた情報共有体制の構築及び共有される情報の再整理
- 平時における対応を念頭に置いた大規模IT障害対応時の体制の明確化

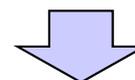
第2次行動計画での主な成果

- 事業者等におけるBCP策定に資する基礎資料を提供
- 分析結果の一部を指針に反映



主な課題

- 分析対象、位置付け及び実施頻度の見直し
 - 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
 - 時間的経過、環境変化等の顕在化に応じた効果を高めるための脅威等の詳細分析

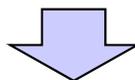


次期行動計画における施策像

- 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持ち得るリスク源の調査
- 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メントの訴求

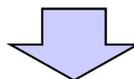
第2次行動計画での主な成果

- 事業者等のIT障害時の早期復旧手順、BCPの検証に活用
- 演習への参加組織・人数の増加



主な課題

- 演習実施規模の拡大の限界
 - －重要インフラ分野全体への成果の普及・浸透方策
- 演習の質的改善
 - －PDCAサイクルによる将来の演習への反映、他施策への反映
- 関連演習・訓練との連携
 - －全体像の把握、実施機関間の連携

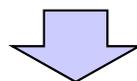


次期行動計画における施策像

- 重要インフラ関係の演習・訓練の全体像を把握した上での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

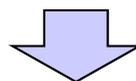
第2次行動計画での主な成果

- 関係資料の公表・提供、継続的な広聴
- 関係主体間のコミュニケーションの充実・相互理解の向上
- 諸外国との更なる連携の実現



主な課題

- 広報公聴活動の見直し
 - －施策の目的と情報開示範囲に応じた見直し
- 「リスクコミュニケーション」の見直し
 - －国際標準との整合をとった形での包括的なリスクマネジメントの在り方
 - －将来的に影響が大きいことが予想される環境変化についての中長期的な調査
- 国際連携の強化
 - －ASEAN等の二国間、多国間、地域的枠組みを活用した国際連携



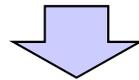
次期行動計画における施策像

- 重要インフラの防護基盤強化に資する施策の追加（他施策に属すものを除く）
 - －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 等々
- リスク特定・分析の充実
 - －将来的に影響が大きいことが予想される環境変化についての中長期的な調査

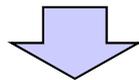
サイバーセキュリティ戦略

- 我が国において、現在、重要インフラとは位置付けられていないが、現行10分野と同等にその情報システムのIT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付けを踏まえ、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。

見直しの視点



検討対象	視点
情報システム	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
制御システム	制御が困難な状態において生じ得るリスクの大きさ
共通	既存分野における重要システムに与える影響 既存分野との間で認め得る相互依存性
既存分野での補強・拡大	既存分野で活動に至っていないものの追加



次期行動計画において想定される分野及びその活動

- 既存の10分野に加え、数分野が新たに追加見込み
 - ー 所管省庁、セプター事務局候補の業界団体等との合意を得た時点で公表
- 重要インフラ分野としての活動開始準備
 - ー 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

第2次行動計画と次期行動計画との対比

- 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2次行動計画	次期行動計画における施策群	補強・改善の方向性
①安全基準等の整備及び浸透	第2次行動計画を基本的に踏襲	<ul style="list-style-type: none"> ・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	第2次行動計画を基本的に踏襲	<ul style="list-style-type: none"> ・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(脅威の種類等)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応体制の明確化
③共通脅威分析	「⑤環境変化への対応」の一部と統合し、「リスクマネジメント」として整理	<ul style="list-style-type: none"> ・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持ち得るリスク源、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 ・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メントの訴求
④分野横断的演習	「障害対応体制の強化」として整理	<ul style="list-style-type: none"> ・重要インフラ関係の演習・訓練の全体像を把握した上での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
⑤環境変化への対応	「リスクマネジメント」に統合される部分を除き、「防護基盤の強化」として整理	<ul style="list-style-type: none"> ・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

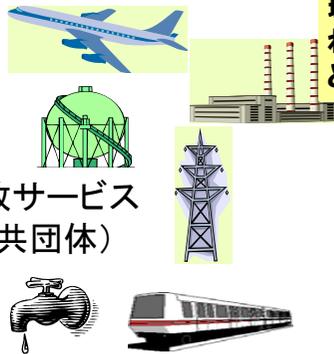
(参考) 重要インフラの範囲の見直しの結果、数分野を追加見込み

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、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(10分野+α)

- 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



新規分野の追加
現在重要インフラと位置付けられていないが影響が既存分野と同等程度あるもの等

NISCによる
調整・連携

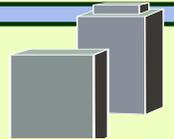
重要インフラ所管省庁(5省庁)

- 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]
- 国土交通省 [航空分野、鉄道分野、物流分野]
- 経済産業省 [電力分野、ガス分野]



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



防災関係府省庁
サイバー空間関連事業者

次期重要インフラ行動計画(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



IT障害・攻撃に関する情報の共有による、官民の関係者全体での連携体制の強化

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障害対応能力の向上

リスクマネジメント



脅威等がもたらすリスクに関するマネジメントの促進及び当該マネジメントを支援するリスク特定・分析結果の提示

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備

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、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り、次の取組を行うことが必要

- 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、事業者等の単独のものだけでなく、分野内の他事業者や他分野の事業者等のもの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

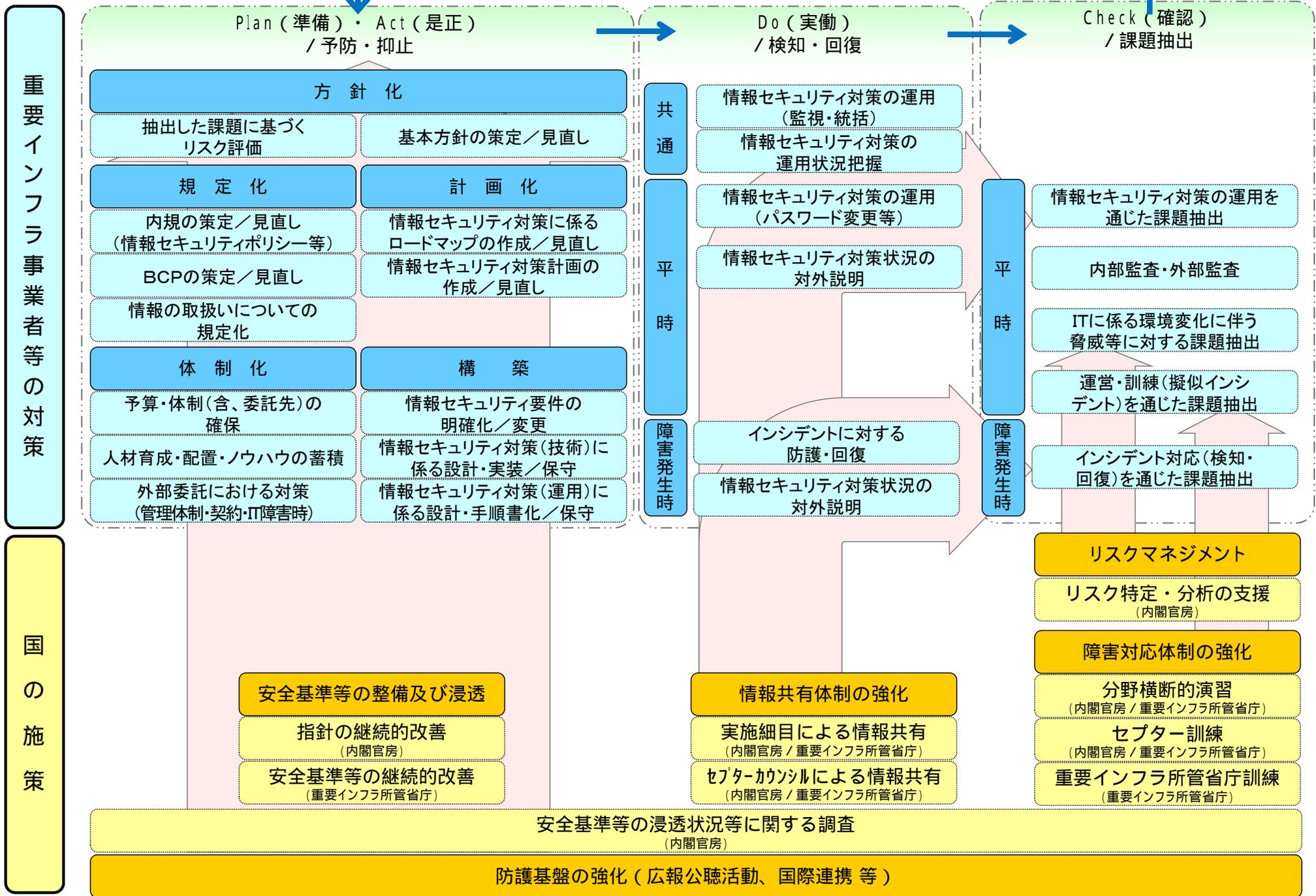
- 自らの状況を正しく認識し、活動目標を主体的に策定するとともに、各々必要な取組の中で定期的に自らの対策・施策の進捗状況を確認。また、他の関係主体の活動状況を把握し、互いに自主的に協力
- IT障害の規模に応じて、情報の5W1Hを理解しており、IT障害の発生時に冷静に対処可能。多様な主体間でのコミュニケーションが充実し、自主的な対応に加え、他の関係主体との連携、統制の取れた対応が可能
- 以上のような、重要インフラ防護への連携した取組を広く国民に周知し、国民の安心感を醸成

●重要インフラ事業者等の経営層の在り方

上記の在り方に加え、当該経営層は、以下の項目を認識し、セキュリティ・ガバナンスを実施できていること

- 重要インフラ防護を達成するに当たっての情報セキュリティ対策を含むリスク源の特定、分析及び評価
- 上述のリスク源に対する方針の策定
- システムの構築・運用、当該方針の実行に必要な計画の策定及び経営資源の継続的な確保
- 計画策定後の一定期間経過時における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IT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」と各対策に関連する「国の施策」



評価の基本的考え方

本行動計画に基づく取組を着実に進め、また継続的に改善させること。

⇒ **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**

本行動計画の取組の妥当性を検証し、必要に応じて見直すこと。

⇒ **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

目的	評価の種類	評価の観点
取組の継続的改善	年度評価	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？
取組の妥当性の 見直し	期間評価	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？

評価手法と主体

5W1H	結果(アウトプット)	成果(アウトカム)
評価対象	<ul style="list-style-type: none"> ①重要インフラ事業者等の対策 ②個別の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・強化に資する情報セキュリティ対策・施策の全体(=本行動計画の枠組み)
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	行動計画期間終了時
評価手法	取組の進捗状況を <ul style="list-style-type: none"> ①重要インフラ事業者等による対策の総合的な確認・検証に用いるための指標 ②政府機関等による施策の確認・検証に用いるための指標 に基づいて検証	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①かつ分析的②に実施 <ul style="list-style-type: none"> ①各施策群毎の個別の成果に補完的な情報も加味 ②サービス維持レベルを超えたIT障害の発生状況を確認・検証

※事業者等の自主的な対策の評価は自己評価に委ねる。

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。