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2次行動計画」

安心があたりまえ
～誰もが安心できる社会基盤に～

2009年2月20日

内閣官房情報セキュリティセンター(NISC)
http://www.nisc.go.jp/

内閣参事官　上　原　仁

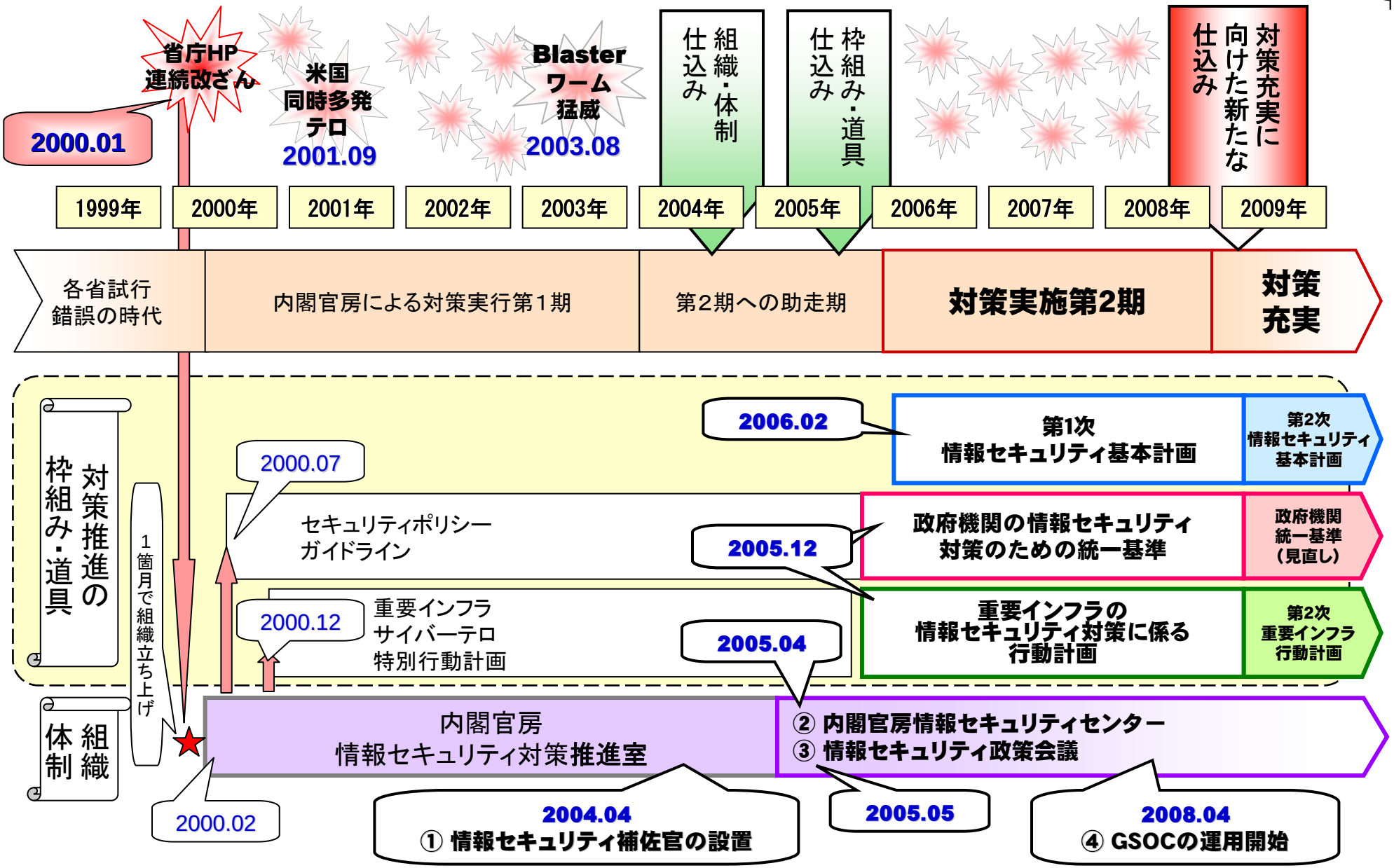
NISC National Information Security Center

目　次

NISC National Information Security Center

これまでの取組

内閣官房における情報セキュリティ政策の流れ（2000年以降の概要）



情報セキュリティ政策会議及び内閣官房情報セキュリティセンター（NISC）の設置

➢「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」（2004年12月7日IT戦略本部決定）を受け、情報セキュリティ問題に関する政府中核機能の強化に向けて機能・体制等を整備中

- ➢2005年4月25日、内閣官房情報セキュリティセンター（NISC：National Information Security Center）を設置
- ➢2005年5月30日、IT戦略本部の下に「情報セキュリティ政策会議」を設置

IT戦略本部

情報セキュリティ政策会議

内閣官房情報セキュリティセンター（NISC）

官民から専門家を集約
（2009年1月現在74名）

情報セキュリティ基本戦略等、根幹となる事項を決定

①情報セキュリティ政策に関する基本戦略の立案

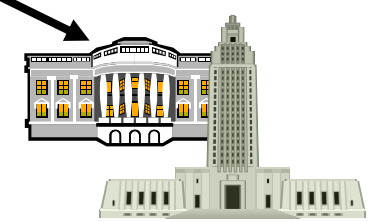
④重要インフラの情報セキュリティ対策

②政府機関の総合対策促進

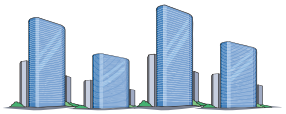
③政府機関の事案対処支援

重要インフラ所管省庁：金融庁／総務省／厚生労働省／国土交通省／経済産業省

情報セキュリティ関係省庁：警察庁／総務省／経済産業省／防衛省



◆諸外国との情報交換・連携の一元化
◆国際的な信頼醸成



政府機関（各省庁）

重要インフラ

企業

個人

情報セキュリティ政策の構造

「第１次情報セキュリティ基本計画」（2006年2月2日　情報セキュリティ政策会議決定）

2006～2008年度の3ヵ年計画。全主体が適切な役割分担を果たす「新しい官民連携モデル」の構築を目指す。

	政府機関・地方公共団体	重要インフラ	企　業	個　人
3ヵ年の目標	すべての政府機関が「政府機関統一基準」が求める水準に	IT障害を限りなくゼロに	対策の実施状況を世界トップクラスの水準に	「IT利用に不安を感じる」個人を限りなくゼロに
各実施領域の重要政策	◆ 政府機関統一基準に基づく各省庁の評価 ◆ サイバー攻撃等への緊急対応能力の強化	◆重要インフラ行動計画 ・安全基準等の整備の推進 ・情報共有体制の強化 ・相互依存性解析 ・分野横断的演習実施	◆ 第三者評価制度の活用 ◆ ウィルス等への体制強化	◆ セキュリティ教育の推進 ◆ 広報啓発の強化 ◆ ユーザーフレンドリーなサービスの提供等

横断的な重要政策

- 情報セキュリティ技術戦略の推進
- 情報セキュリティ人材の育成確保
- 国際連携・協調の推進
- 犯罪の取締り、権利利益の保護救済

第2次計画（2009年2月3日 情報セキュリティ政策会議決定）

2005年度 | 2006年度 | 2007年度 | 2008年度 | 2009年度

評価2006 → セキュア・ジャパン2006
評価2007 → セキュア・ジャパン2007
評価2008 → セキュア・ジャパン2008
セキュア・ジャパン2009

「セキュア・ジャパン」：基本計画の遂行を確実にするため、毎年の政府の重点施策をまとめた年度計画

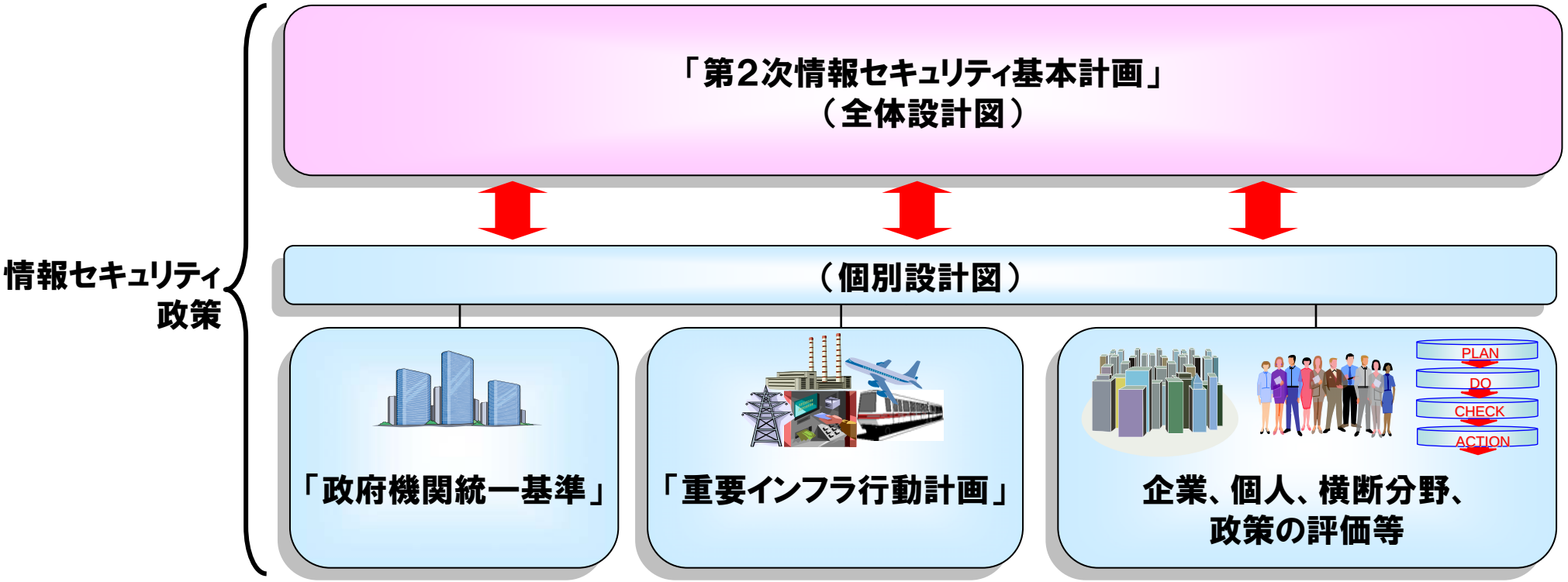
NISC National Information Security Center

「第2次情報セキュリティ基本計画 」について

全体設計図である「第2次情報セキュリティ基本計画」、分野単位の個別設計図

○情報セキュリティ政策は、情報セキュリティ問題全般に関する全体設計図である「第2次情報セキュリティ基本計画」と、分野別の個別設計図の組み合わせで推進する。

○このような組み合わせに基づくことで、個別分野縦割り的対応を排し、我が国全体として分野横断的・政策領域横断的な視点を持って、複雑化する情報セキュリティ問題への的確な対応を進める。



「第1次情報セキュリティ基本計画」の成果と「第2次情報セキュリティ計画」の目標（目指す「姿」）

1. 第1次基本計画（'06～'08年）

成果

情報セキュリティ政策の立上げ

◆関係者の「気付き」を高めた

→ P to Pソフトで情報流出の危険性

→ サイバー攻撃で情報を盗まれる危険性

→ システム障害で事業が止まる危険性

◆とりあえず政策推進の枠組みは構築

→ 政府機関の統一基準に基づく対策と評価

→ 重要インフラ事業者間の情報共有体制

→ 日米、日ASEANで情報交換を行う枠組み

◆（問題が生じないための）事前対策の取組みはある程度進展

→ 但し、日々新たなリスクが生まれ、また変化している

2. 第2次基本計画（'09年～'11年）

目標

政策の継続と更なる発展

◆事前対策は当たり前のことに

◆問題が生じても、冷静かつ迅速に事後対応・復旧活動を推進できる

◆情報を管理する側に加えて、情報を預ける側も取組みの対象に

「第2次情報セキュリティ基本計画」の全体像 ［1］

○「第2次情報セキュリティ基本計画」は、情報セキュリティ問題全般に係る中長期計画（全体設計図）として、今後の我が国の取組みに関する、１）基本的考え方と、２）重点政策の方向性を提示。

○具体的には、2009年度～2011年度までの3カ年計画として策定。これまで同様、本計画に基づいた年度ごとの推進計画である「セキュア・ジャパン」を策定するとともに、年度ごとの取組み状況や社会変化などに関する評価等を行う予定。

第１次基本計画からの「発展」と「継続」

1. 具体的取組みの持続的な推進、新たな課題への政策的対応
   （第1次基本計画で構築した取組みの各種枠組みを持続的に活用）

2. 「事故前提社会」への対応力強化
   （十分な事前対策の取組みにも関わらず、万が一問題が生じた場合を考えて準備を怠らない）

3. 合理性に裏付けられたアプローチの実現
   （情報資産の価値、リスクの大きさに応じた合理的（最適）な水準の対策を実現）

第2次基本計画の基本的考え方

●基本目標　→　「ITを安心して利用できる環境」の構築
（第1次基本計画と同様。IT基本法第22条の実現）

●取組みにあたっての基本理念　→　「セキュリティ立国」の思想の成熟
（IT時代の力強い「個」と「社会」の確立へ）
（目指す「姿」は、最適な水準の取組みとセキュリティの実現であり、絶対的な無謬性の追求ではない　→　絶対的な無謬性から脱却するには国民や社会全体の意識改革も不可欠）

●基本目標の実現に向けた取組み　→　官民の各主体が適切な役割分担を果たす「新しい官民連携モデル」＋（対策実施側のみならず）情報提供側も視野に入れた取組みの推進
（第1次基本計画の下では、対策実施主体及び対策支援主体による「新しい官民連携モデル」を追求。状況変化を踏まえ、新たに情報提供側も視野に入れた取組みを推進）

第2次基本計画の下で取組みを行う政策領域

●課題の把握から事前対策、事後対応まで視野に入れた取組み
（事前対策のみならず、万が一問題が生じた場合も視野に入れて事後対応の準備を進める）

●技術面での対応から制度面、人的側面の対応まで視野に入れた取組み
（技術開発から人材育成のような側面まで幅広く取組みを進める）

●国内における対策の推進から、情報セキュリティ確保のために国際的になされる活動も視野に入れた取組み
（IT利用・活用においては国境を越えるのは当然となっており、国内の取組みと国際的な取組みを有機的に結びつけた取組みとする）

●国民の日常生活や経済活動といった個別主体に関係の深い領域から、安全保障や文化といった我が国全体に関係の深い領域にまで対応した取組み
（情報セキュリティ問題は相当程度幅が広いことに鑑み、様々な観点から柔軟かつ領域横断的に取組みを進める）

「第2次情報セキュリティ基本計画」に基づく取組み－今後3年間の重点政策－

主な重点政策①（4領域）3年間の

政府機関・地方公共団体	重要インフラ	企業	個人
◆能動的に情報セキュリティ対策を推進する体制確立（最高情報セキュリティアドバイザー設置、年次報告書の報告・公表） ◆事業継続性確保の検討、サイバー攻撃等への緊急対応能力強化	◆ 情報共有体制の強化 ◆ 重要インフラ連絡協議会の設置 ◆ 分野横断的な演習、共通脅威分析の実施	◆ 情報セキュリティ監査等第三者評価制度の活用推進 ◆ 対策容易化のためのツール提供 ◆ 中小企業の対策促進 ◆ コンピュータウィルス等への対応体制の強化	◆ 学校や地域における教育モラル等の教育の推進 ◆ 個人の質問対応を行えるようなサポータの育成 ◆ サービス提供事業者や対策支援主体によるリスク情報等の個人への適切な提供促進
政府機関統一基準	**重要インフラ行動計画**	**各省庁による施策**	**各省庁による施策**

主体 情報提供

自身の有する情報を預ける主体（新たな課題として、関係機関等が協力しながら取組みを検討・推進）

主な重点政策②（横断的事項）3年間の

情報セキュリティ技術戦略の推進
- ◆セキュリティ対策を埋め込んだ機器の開発促進
- ◆「グランドチャレンジ型」技術開発の推進

情報セキュリティ人材の育成確保
- ◆ 政府機関における人材の育成・確保
- ◆ 保有するスキルの見える化の推進

国際連携・協調の推進
- ◆ 世界の脅威動向を把握するための官民連携確立
- ◆ アジアにおける知恵の結集と水準の向上

犯罪の取締り、権利利益の保護救済
- ◆ 犯罪取締りのための基盤整備の推進
- ◆ 権利利益の保護・救済のための基盤性の推進

※その他、「情報セキュリティ対策を実施する主体」の取組みを支援する主体の取組みも促進する。

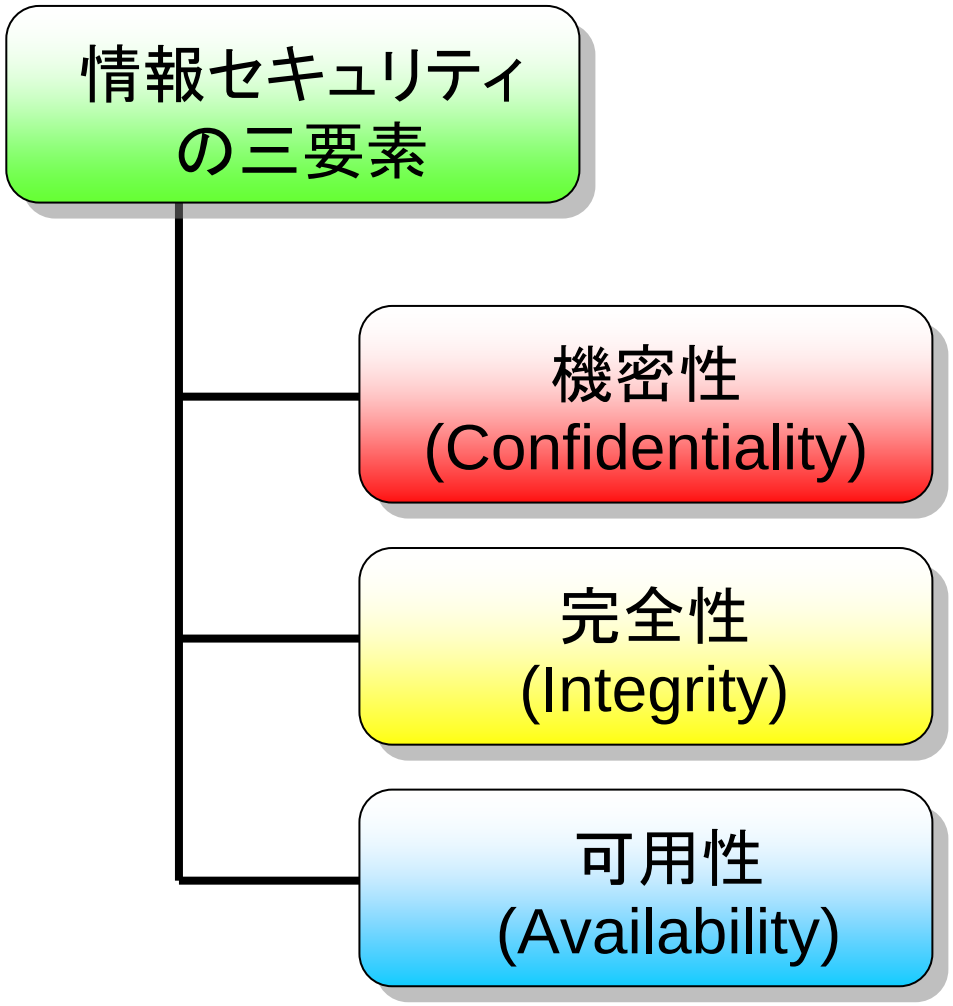
NISC National Information Security Center

行動計画の策定の背景

IT障害を引き起こす脅威の例

脅威の類型	脅威の例
サイバー攻撃をはじめとする意図的要因	不正侵入、データ改ざん・破壊、不正コマンド実行、ウイルス攻撃、サービス不能攻撃（DoS：Denial of Service）、情報漏えい、重要情報の詐取、内部不正　等
非意図的要因	操作・設定ミス、プログラム上の欠陥（バグ）、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障　等
災害や疾病	地震、水害、落雷、火災等の災害による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設の損壊　等
他分野の障害からの波及	電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの）　等

情報セキュリティ対策とは



認められた者しかその情報にアクセスできないこと

情報が破壊、改ざん、消去されないこと

障害や妨害が無く、情報システムを使えること

IT障害やその影響の例（抜粋）

重要インフラ分野		IT障害やその影響の例
情報通信		・電気通信サービスの停止、放送サービスの停止
金融	銀行 生命保険・損害保険 証券会社 金融商品取引所	・預金の払い出し、振込等資金移動、融資業務の停止 ・保険金の支払い停止 ・保険金の支払い停止 ・有価証券売買の停止　等
航空		・運航の遅延、欠航、航空機の安全運航に対する支障等
鉄道		・列車運行の遅延、運休、列車の安全安定輸送に対する支障等
電力		・電力供給の停止、電力プラントの安全運用に対する支障等
ガス		・ガスの供給の停止、スプラントの安全運用に対する支障等
政府・行政サービス		・政府・行政サービスに対する支障 ・個人情報の漏洩、盗聴、改ざん
医療		・診療支援部門における業務への支障等
水道		・水道による水の供給の停止 ・不適当な水質の水の供給　等
物流		・輸送の遅延・停止 ・貨物の所在追跡困難

基本的な方向性

○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

○他方、単独で取り組む対策のみで、多様な脅威への対応が万全であることを確認することは困難

分野内の他事業者、
他分野の事業者等との連携の充実が必要

第2次行動計画

各関係主体による様々な情報セキュリティ対策を、

- 重要インフラ事業者等がとることが望ましい自主的な対策
- 内閣官房を中心とした政府及び関係機関等において実施することが望ましい施策

からなる体系的な枠組みとして整理。

NISC National Information Security Center

第2次行動計画

重要インフラの情報セキュリティ対策に係る第2次行動計画の全体像

○「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こと」を目指すとともに、「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にすること」を目標に官民が連携して重要インフラ防護に取り組む

○ 新たに分野毎(*)に重要インフラサービスの検証レベルを設定して着実に改善を実施

○ 第1次行動計画において設定した施策の4つの柱に着実に取組み、また経験を改善につなげるとともに、新たに「環境変化への対応」を5つめの柱に掲げ、変化に対する察知能力の向上と機敏な対応に取り組む

※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（地方公共団体を含む）、医療、水道、物流

第1次行動計画の成果
【2006年度～2008年度】

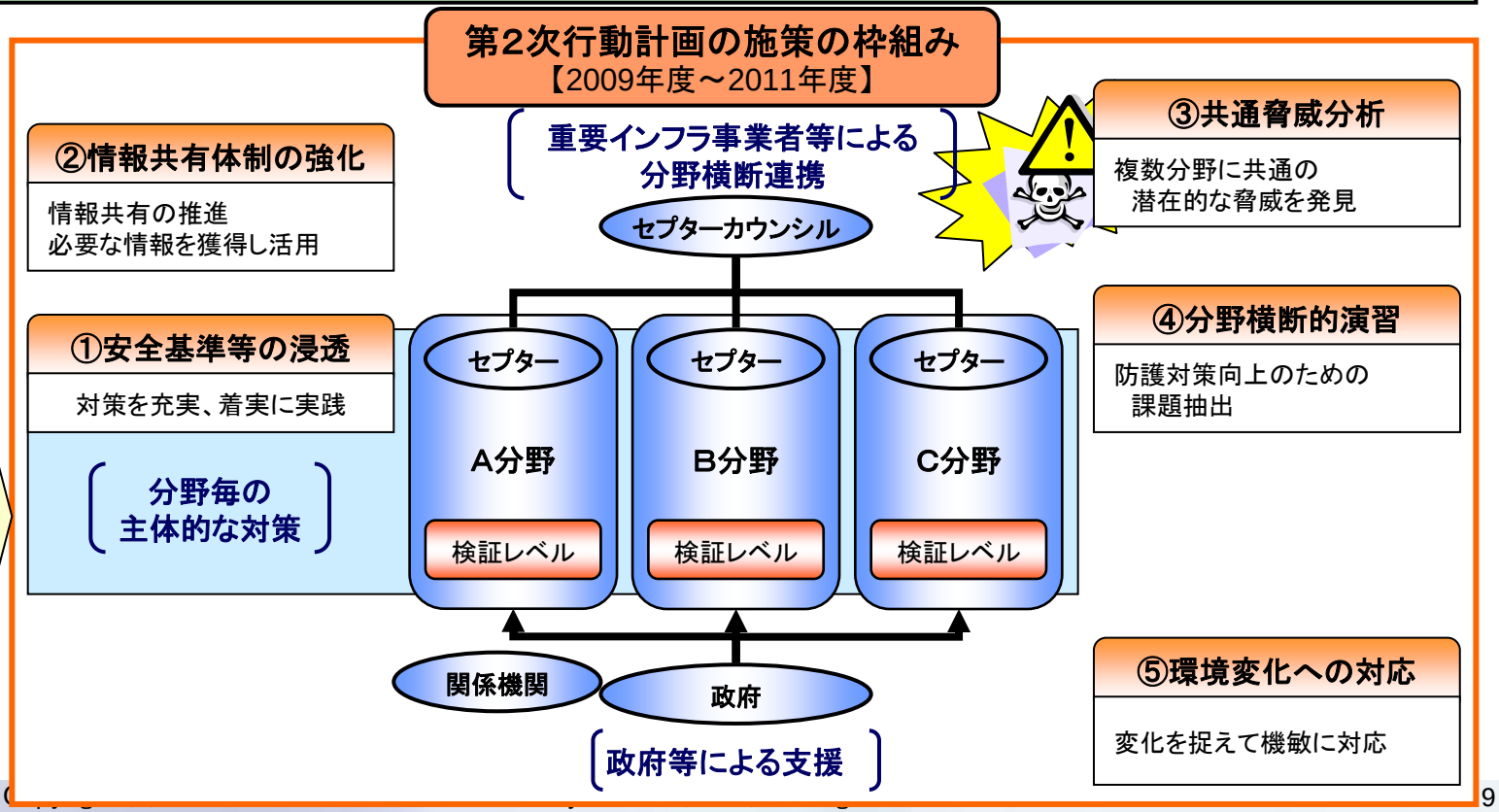
①安全基準等
- 「重要インフラにおける情報セキュリティの確保に係る「安全基準等」策定にあたっての指針」を策定、改定
- 各分野にて安全基準等の策定、見直し

②情報共有体制
- 官民の情報提供・連絡の体制を整備し、情報提供・情報連絡を開始
- 各分野にてセプターを整備
- セプターカウンシルを創設（予定）

③相互依存性解析
- 静的相互依存性解析を実施
- 動的相互依存性解析を実施

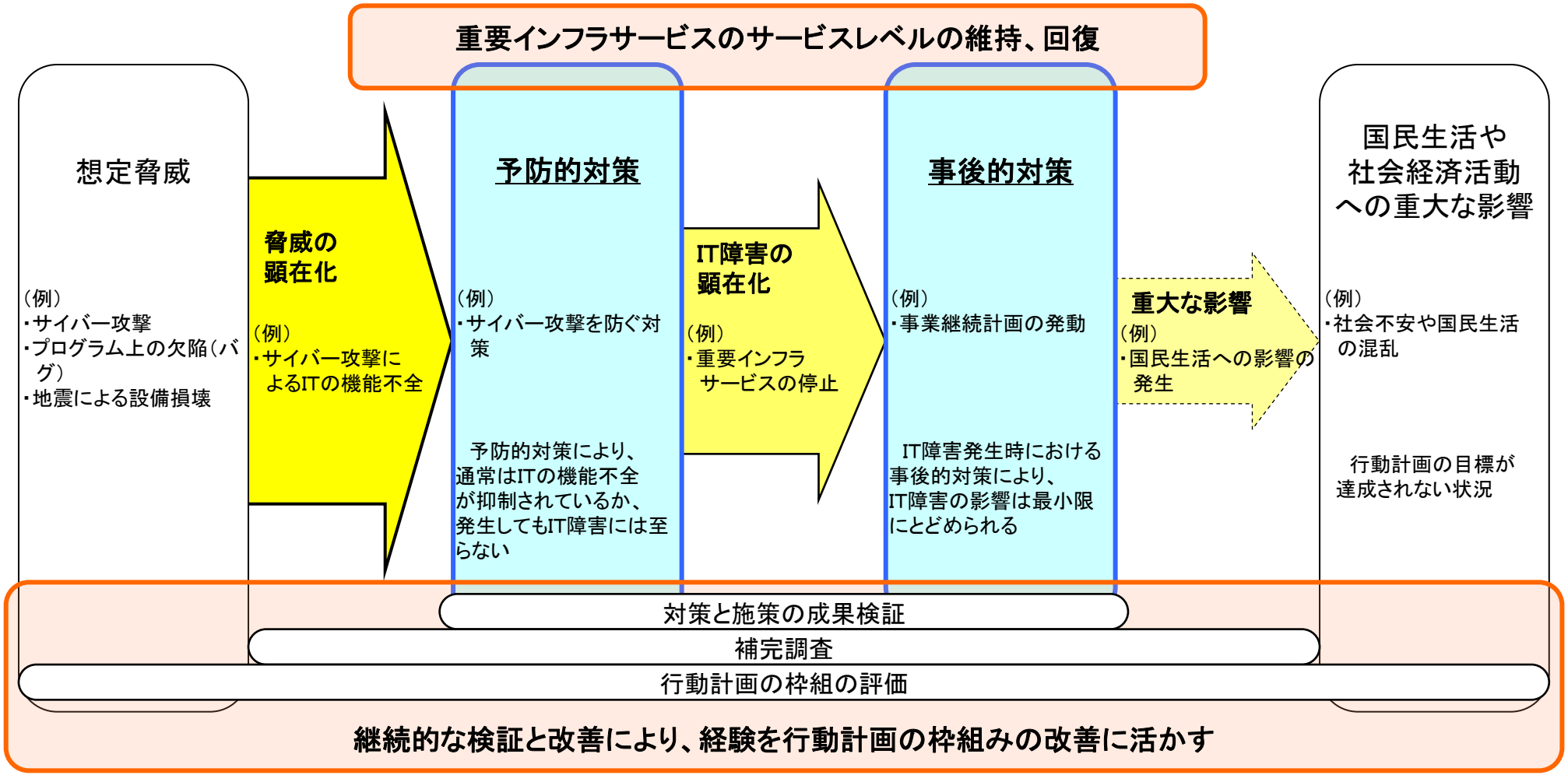
④分野横断的演習
- 研究的演習、机上演習を実施
- 機能演習を実施

第2次行動計画の施策の枠組み
【2009年度～2011年度】



情報セキュリティ対策のスコープ

・事業継続性を確保するためには、予防的体策と事後的対策の両方が必要
・情報セキュリティ対策の継続的な検証と改善に取り組む



［参考］ 第2次行動計画の概要

○ 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にすることを目標として継続

	第1次行動計画（2006-2008）	第2次行動計画（2009-2011）
総論	➢想定する脅威や防護すべき重要システム等の対策の範囲を設定 ➢情報セキュリティ対策に関する官民連携の施策の枠組みを構築	➢**サービスレベルと検証レベルを定義**、脅威等の対象範囲を見直し ➢アウトカムとなる**「理想とする将来像」を提示**
情報セキュリティ対策の柱	**1 安全基準等の整備**	**1 安全基準等の整備及び浸透**
	➢「『安全基準等』策定にあたっての指針」を策定 ➢各分野毎に上記指針を踏まえた「安全基準等」を策定・改定	➢「『安全基準等』策定にあたっての指針」の充実 ➢各分野毎に「安全基準等」の継続的な改善の実施と、確実な浸透
	2 情報共有体制の強化	**2 情報共有体制の強化**
	➢IT障害に対応するための、官民の情報提供・連絡の体制を整備 ➢各分野毎に「セプター（情報共有・分析機能）」を整備 ➢分野横断的な情報共有の場として「セプターカウンシル」を設立	➢情報セキュリティ対策に資する、共有すべき情報を整理 ➢情報の分析等のセプターに期待される機能を示し、必要な支援を実施 ➢分野横断的な情報共有等のセプターカウンシルに望まれる事項を提示
	3 相互依存性解析	**3 共通脅威分析**
	➢相互依存性解析の問題提起と実施効果等を記載 ➢内閣官房を中心に、相互依存性解析を試行	➢潜在的なリスクチェーンの把握等のため相互依存性解析を継続 ➢検討対象を技術、システム、環境等に拡大した分野共通の脅威を分析
	4 分野横断的演習	**4 分野横断的演習**
	➢内閣官房の企画・立案の下、各分野が参加する形態で「研究的演習」、「机上演習」、「機能演習」を段階的に実施	➢具体的なIT障害の発生を想定した分野横断的演習を継続的に実施
		5 環境変化への対応
		➢広く協力、支援を得るため**広報公聴活動**を実施 ➢国際会合や他国機関との対話を通じた**国際連携**を推進
評価・検証	➢3年毎又は必要に応じて行動計画を見直し	➢分野毎にIT障害の**検証レベルを設定**し、また施策毎に**検証指標を設定**して、情報セキュリティ対策の継続的な検証と改善に取り組む ➢指標だけでは把握しきれない状況を収集するために、**補完調査を実施** ➢3年毎又は必要に応じて行動計画を見直し

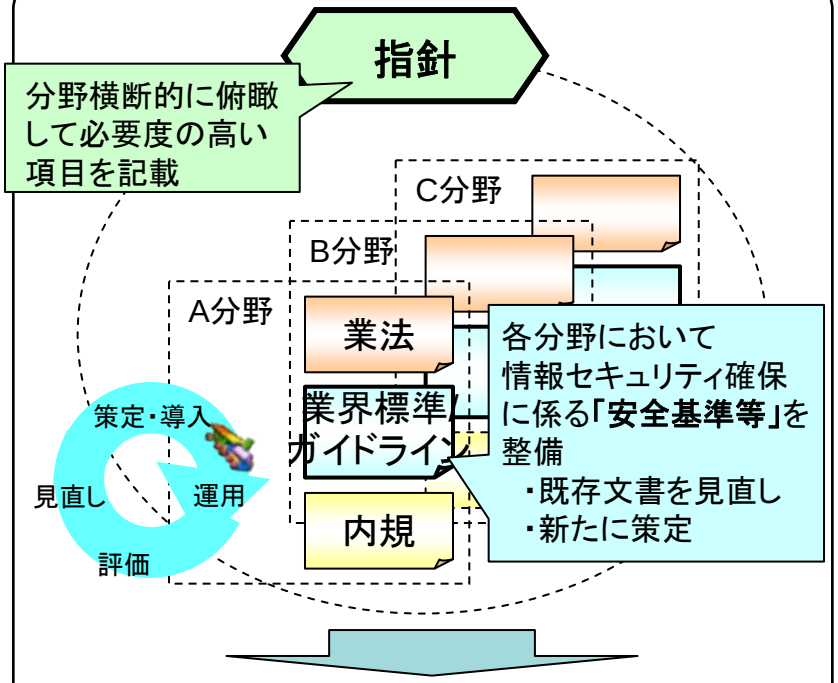
NISC National Information Security Center

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

○　指針（※）の位置づけや記載内容の具体性のレベルの見直しを行う
○　重要インフラ事業者等のPDCAサイクルとの整合性を踏まえた安全基準等の整備の推進などの底上げに資する取組みのみならず、個別の先進的な対策を伸ばしその浸透を図る観点からの取組みも推進する

第1次行動計画における取組み



- 「自らが何をすべきか」が理解可能な状況
- 安全基準等の見直し及び指針の見直しを通じて適宜適切なものとなるよう随時検討

安全基準等の整備及び浸透

第2次行動計画における取組み

（1）指針の継続的改善

- 「要検討事項」（全分野共通で特段の理由がない限り対策が望まれる事項）と「参考事項」（進んだ対策として各分野が任意で参考とする事項）に分類する
- 対策項目の具体化の例示を行う

（2）安全基準等の継続的改善

- 各分野にて主体的にPDCAサイクルを回す
- 情報セキュリティ監査や情報セキュリティ報告書等の自主的な取組みを一層推奨する
- 毎年一定時期に実態把握を行う

（3）安全基準等の浸透

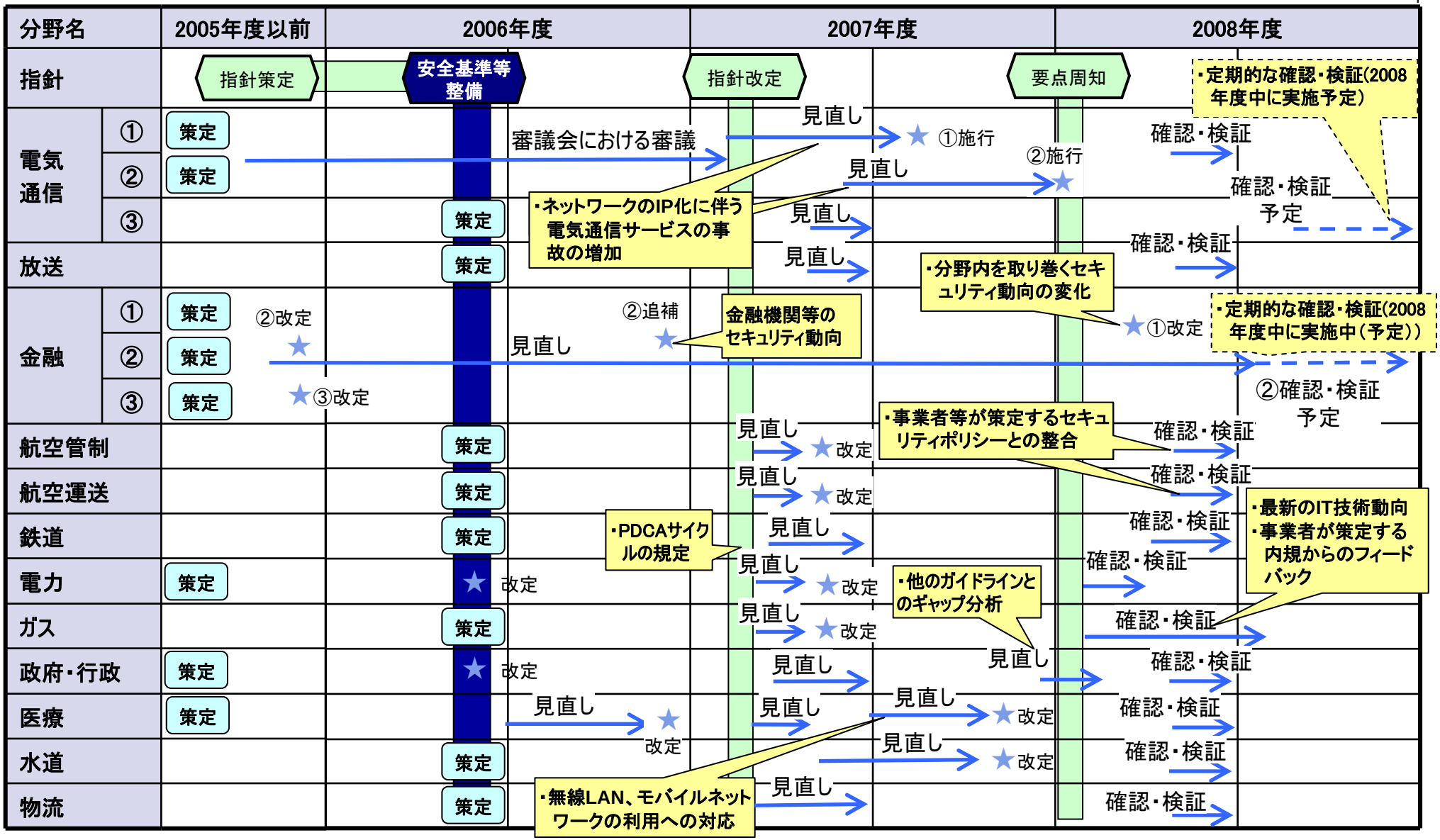
- 各分野にて対策の推進に加え、対策を実装するための環境整備にも努める
- 毎年一定時期に「安全基準等の浸透状況等に関する調査」を実施し、「内規」を含めた対策状況の客観的な把握を行う

※「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』策定にあたっての指針」（2007年6月14日改定　情報セキュリティ政策会議決定）

【参考】安全基準等一覧（2009年1月時点）

分野		安全基準等の名称
情報通信	電気通信	電気通信事業法、電気通信事業法施行規則、事業用電気通信設備規則等（関連する告示を含む） 情報通信ネットワーク安全・信頼性基準 電気通信分野における情報セキュリティ確保に係る安全基準（第1版）
	放送	放送における情報インフラの情報セキュリティ確保に関わる「安全基準等」策定ガイドライン
金融		金融機関等におけるセキュリティポリシー策定のための手引書 金融機関等コンピュータシステムの安全対策基準・解説書 金融機関等におけるコンティンジェンシープラン策定のための手引書
航空	航空運送	航空運送事業者における情報セキュリティ確保に係る安全ガイドライン
	航空管制	航空管制システムにおける情報セキュリティ確保に係る安全ガイドライン
鉄道		鉄道分野における情報セキュリティ確保に係る安全ガイドライン
電力		電力制御システム等における技術的水準・運用基準に関するガイドライン
ガス		製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン
政府・行政		地方公共団体における情報セキュリティポリシーに関するガイドライン
医療		医療情報システムの安全管理に関するガイドライン第3版
水道		水道分野における情報セキュリティガイドライン
物流		物流分野における情報セキュリティ確保に係る安全ガイドライン

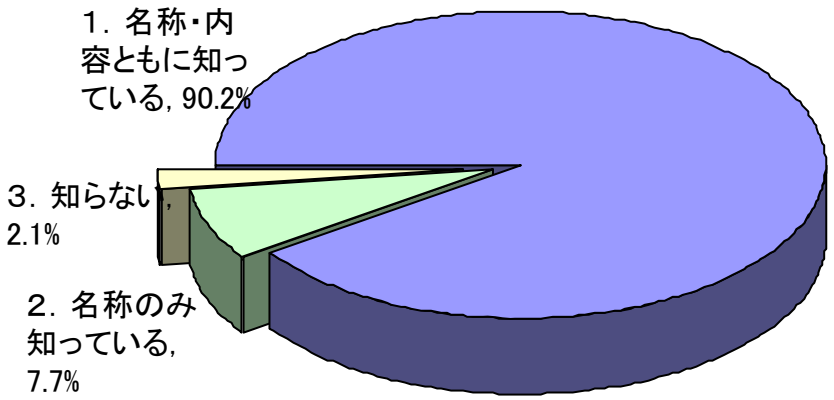
【参考】安全基準等に係る3年間の取り組みについての総括



【参考】「安全基準等の浸透状況等に関する調査」（2007年度）より

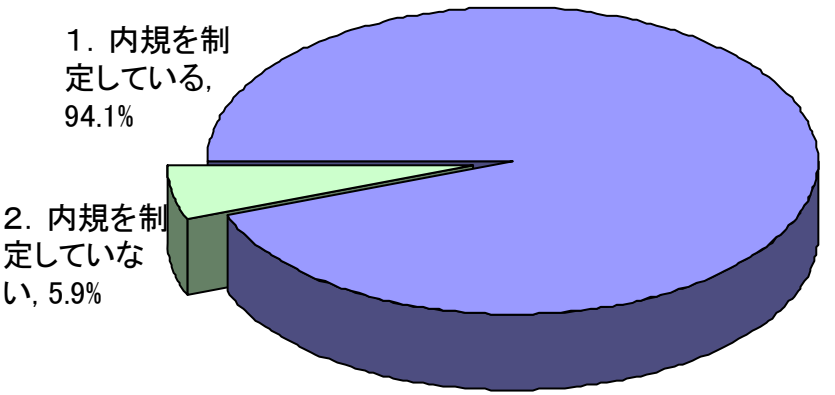
（1）安全基準等の認知

回収数合計：2,846



（2）内規の制定

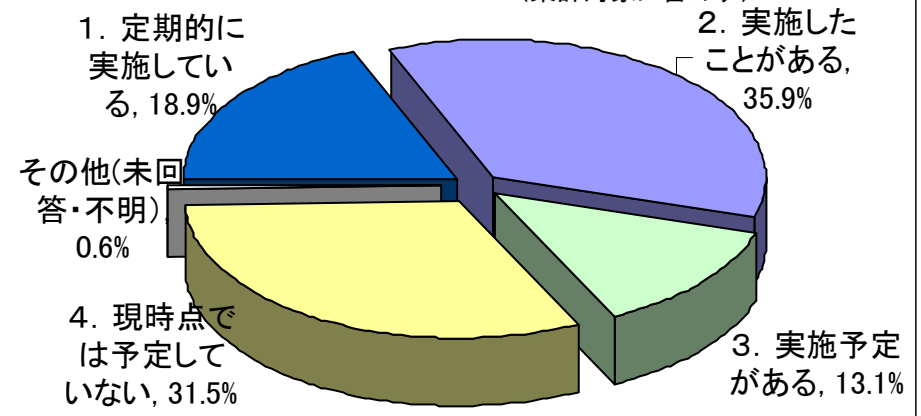
回収数合計：2,846



（3）内規見直しの検討

回収数合計：2,233

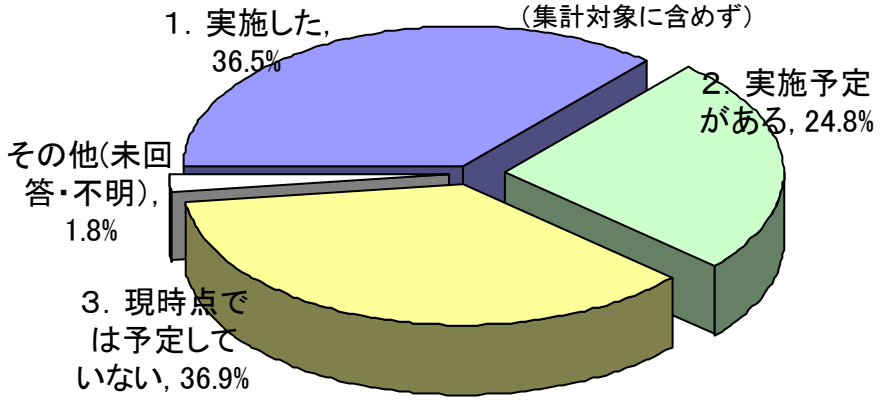
※金融は読み替え可能項目なし（集計対象に含めず）



（4）内規の改定

回収数合計：359

※金融、政府・行政サービスは読み替え可能項目なし（集計対象に含めず）



NISC National Information Security Center

情報共有体制の強化

2 情報共有体制の強化

◆第１次行動計画において構築した「官民の情報共有の枠組み」を踏襲し、第２次行動計画では「官民連携、情報提供の充実」を目指す。

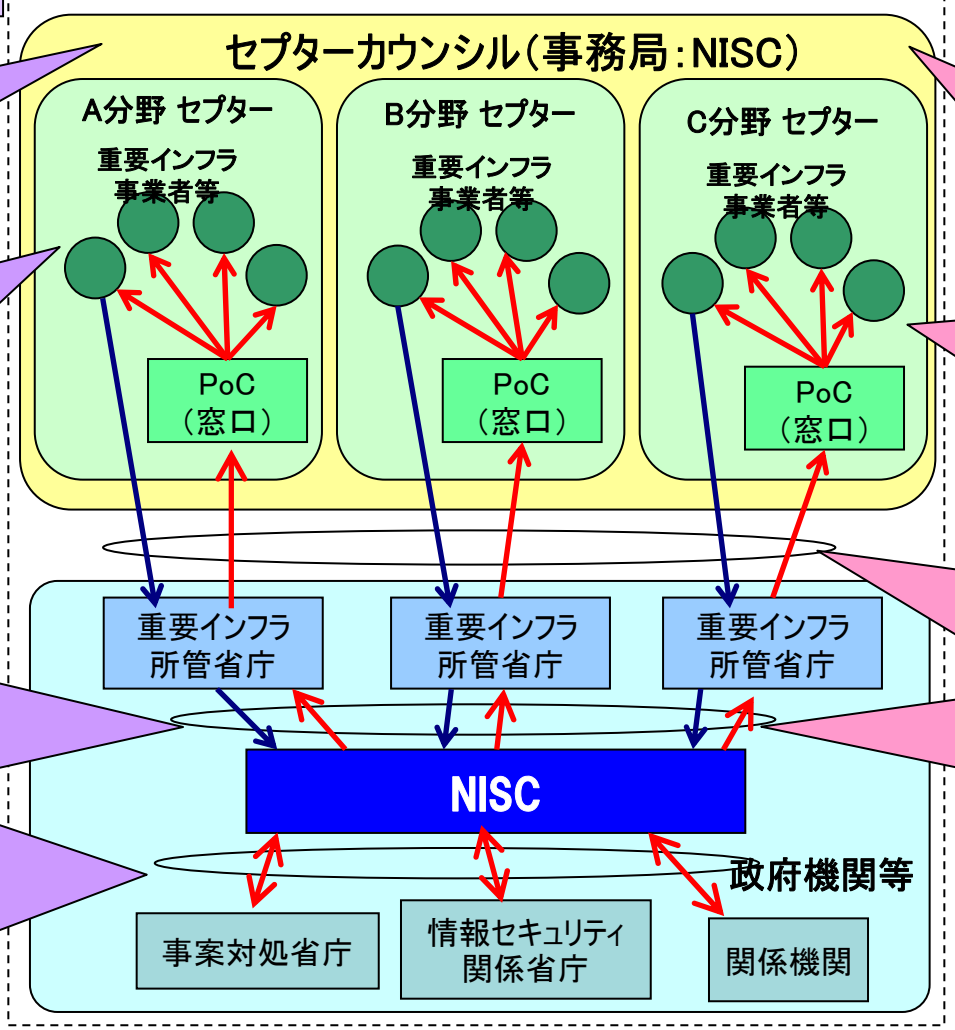
◆第１次行動計画の成果

◎セプターカウンシルの創設（予定）
・各セプターによる分野横断的な情報共有の推進

◎セプターの整備
・分野内における情報共有・分析機能の整備
・政府から提供される情報に対する窓口の設置

◎官民の情報提供・連絡体制の整備
・NISCと所管省庁の間の手続きとして「実施細目(※)」を策定
・重要インフラ事業者等からNISCへの情報連絡（青線）、NISCから重要インフラ事業者等への情報提供（赤線）の運用を開始

官民の情報共有体制



◆第２次行動計画の取組み

◎セプターカウンシル
・セプターカウンシルにおいて取り組むことが望まれる事項を明示
・情報共有の改善等や政府機関等との意見交換への期待

◎セプターの強化
・情報の収集、把握・分析等セプターに期待される機能を明示
・NISCは、事例紹介等でセプター強化のための支援を強化

◎情報提供・情報連絡の充実
・実施細目を含めた各経路間の情報取り扱いルールの整合
・関係機関等が保有する分析機能の活用
・セキュリティに関して有用な活動を行う機関との連携の推進

◎共有すべき情報の整理
・関係主体の保有する情報毎に、重要インフラ事業者にとって有用な情報の共有の在り方を検討

※「重要インフラの情報セキュリティ対策に係る行動計画」の情報連絡・情報提供に関する実施細目

CEPTOAR（情報共有・分析機能）の整備促進

セプター

CEPTOAR: **C**apability for **E**ngineering of **P**rotection, **T**echnical **O**peration, **A**nalysis and **R**esponse

「**IT障害の未然防止**、発生時の**被害拡大防止・迅速な復旧**及び**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、関係重要インフラ事業者等間で共有**」

⇒ 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

機能・役割	・政府からの情報提供窓口 ・関係機関、他分野CEPTOAR等との情報共有（相互の合意に基づく）
要　件	・**情報の取り扱いルール**及び**緊急時に連絡可能な窓口**（最低要件） ・将来的には、**分野内の情報集約、情勢判断**を行えるコーディネータの設置が望ましい

【参考】「CEPTOAR特性把握マップ」について

平成20年3月末日現在

	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
概要	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	地方公共団体	医療	水道	物流
	名称	T－CEPTOAR	放送における情報共有体制	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	電力におけるIT障害に係る情報共有・分析機能	GAS CEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR
	事務局	財団法人マルチメディア振興センター	総務省情報通信政策局地上放送課	全国銀行協会事務システム部	日本証券業協会 IT管理室	社団法人生命保険協会 総務部組織人事グループ	社団法人日本損害保険協会 業務企画部企画安全グループ	国土交通省 航空局 航空安全推進課 航空保安対策室	国土交通省 鉄道局危機管理室	電気事業連合会 情報通信部	社団法人日本ガス協会 保安技術グループ	財団法人地方自治情報センター 自治体セキュリティ支援室	厚生労働省	社団法人日本水道協会 総務部庶務課	社団法人日本物流団体連合会
	整備状況等	平成19年3月末に整備											平成20年3月末に整備		
	構成員（主な事業者等）	29社・団体（固定系のネットワークインフラを設置する電気通信事業者、アクセス系の電気通信事業者、ISP事業者、携帯電話事業者等）	195社・団体（日本放送協会及び地上系一般放送事業者）	1，738社（銀行、信用金庫、信用組合、労金、商工中金、農協等）	317社 10機関（証券会社、取引所等証券関係機関）	41社（社団法人生命保険協会の定款に定める社員および特別会員）	28社（含むオブザーバー3社）（情報システム委員会参加会社）	2グループ 3機関（航空運送事業者及び官庁（航空局・気象庁））	22社1団体 1機関（鉄道事業者22社、1団体及び官庁（鉄道局））	12社2機関（一般電気事業者、日本原電（株）、電源開発（株）、電気事業連合会、電力中央研究所）	10社（政令指定都市8社、同等の事業者2社）	1，863団体（都道府県及び市区町村）	1グループ 2機関（医療機関、日本医師会（情報共有機能）、保健医療福祉情報システム工業会（情報分析機能））	1，393水道事業体（全国の会員水道事業体）	16社6団体（物流事業者）
機能	緊急窓口（POC）	平成19年4月より運用開始											平成20年4月より運用開始		
	情報の取扱いルール	平成19年1月制定	平成19年3月制定	平成19年3月制定	平成19年3月制定	平成19年3月制定	平成19年3月制定	平成19年3月制定	平成19年3月制定	平成18年9月制定	平成19年3月制定	平成19年3月制定	平成20年3月制定	平成20年3月制定	平成20年3月制定
	情報と連絡手段	障害事例情報等 メール、電話、FAX	障害事例情報等 メール、電話、FAX	障害事例情報等 メール、電話	障害事例情報等 メール、電話、FAX、WEB	障害事例情報等 メール、電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話	障害事例情報等 メール、電話、携帯電話、FAX WEB、会議体	障害事例情報等 メール、電話、携帯電話、FAX	障害事例情報等 メール、電話、WEB	障害事例情報等 メール、電話、携帯電話、衛星電話、FAX	障害事例情報等 メール、電話、携帯電話、衛星電話、FAX	障害事例情報等 メール、電話
特徴	その他	運営委員会のもとに、業態の違いによる4つのSGを設置し、全体として密な情報共有の実現を目指す。 Telecom-ISAC Japan及び社団法人電気通信事業者協会における情報共有等の先進的な取組が母体。 T-PoC（T-CEPTOARのPoC）及び4つのSGの代表者によって構成される運営委員会において、情勢判断等を実施。	既存の災害対応時等の連絡体制を活用する体制とした。	情報セキュリティ対策委員会及び財団法人金融情報システムセンターによる障害事例分析等を実施し、分析結果を通知する機能を有する。	各証券関連団体及び財団法人金融情報システムセンターによる障害事例分析等を実施する機能を有する。	分野内の利用システム調査を年1回実施。 社団法人生命保険協会及び財団法人金融情報システムセンターによる障害事例分析等を実施し、分析結果を通知する機能を有する。	分野内の利用システム調査を年1回実施。 社団法人日本損害保険協会及び財団法人金融情報システムセンターによる障害事例分析等を実施し、分析結果を通知する機能を有する。	航空局による障害事例分析等を実施し、分析結果を通知する機能を有すると共に、分析結果をデータベース化する機能を有する。	国土交通省鉄道局危機管理室が鉄道CEPTOARの窓口となり、現在運用されている鉄道事故等報告規則等に基づく報告を活用して情報の共有を図ることとしている。	12社2機関は、Face to Faceを含め、情報共有を行う。行動計画で対象とする12社に留まらず、分析機能をサポートすべく、電力中央研究所も体制に参画する。	分野内の利用システム調査を実施。 業界内でIT障害の判断基準となる考え方を共有できるよう、実務者による常設のWGが、未然防止策や再発防止策等の具体的な取り組み課題を適切にサポートする。	地方公共団体の情報セキュリティレベルの向上を支援するための各種事業を実施。 情報セキュリティに関する各種情報を、行政専用ネットワーク（LGWAN）を活用したメール及びポータルサイトにより提供。	都道府県等を通じた既存の（地震等災害時の）情報連絡体制を活用する。 保健医療福祉情報システム工業会を活用して障害事例の調査・分析を行い、各医療機関への情報提供等を行う。	日本水道協会の会長都市及び7地方支部長都市の8構成員を連絡拠点とし、既存の情報連絡体制を活用して会員水道事業体との情報連絡・共有を図る。 既存の会議体を活用して障害事例の調査・分析を行い、全国の会員水道事業体への情報提供等を行う。	様々な物流関連の業態が存在する分野である。 事務局が各分野団体の窓口となり、IT障害情報については必要に応じて関係者間の情報共有を図る。

（注） 本マップは、各CEPTOARの自主的な整備状況を把握し、マップとして取り纏めたもの。

Ver.2

NISC National Information Security Center

共通脅威分析

3 共通脅威分析の概要

－複数の重要インフラ分野で共通の知見を必要とする共通脅威を分析－

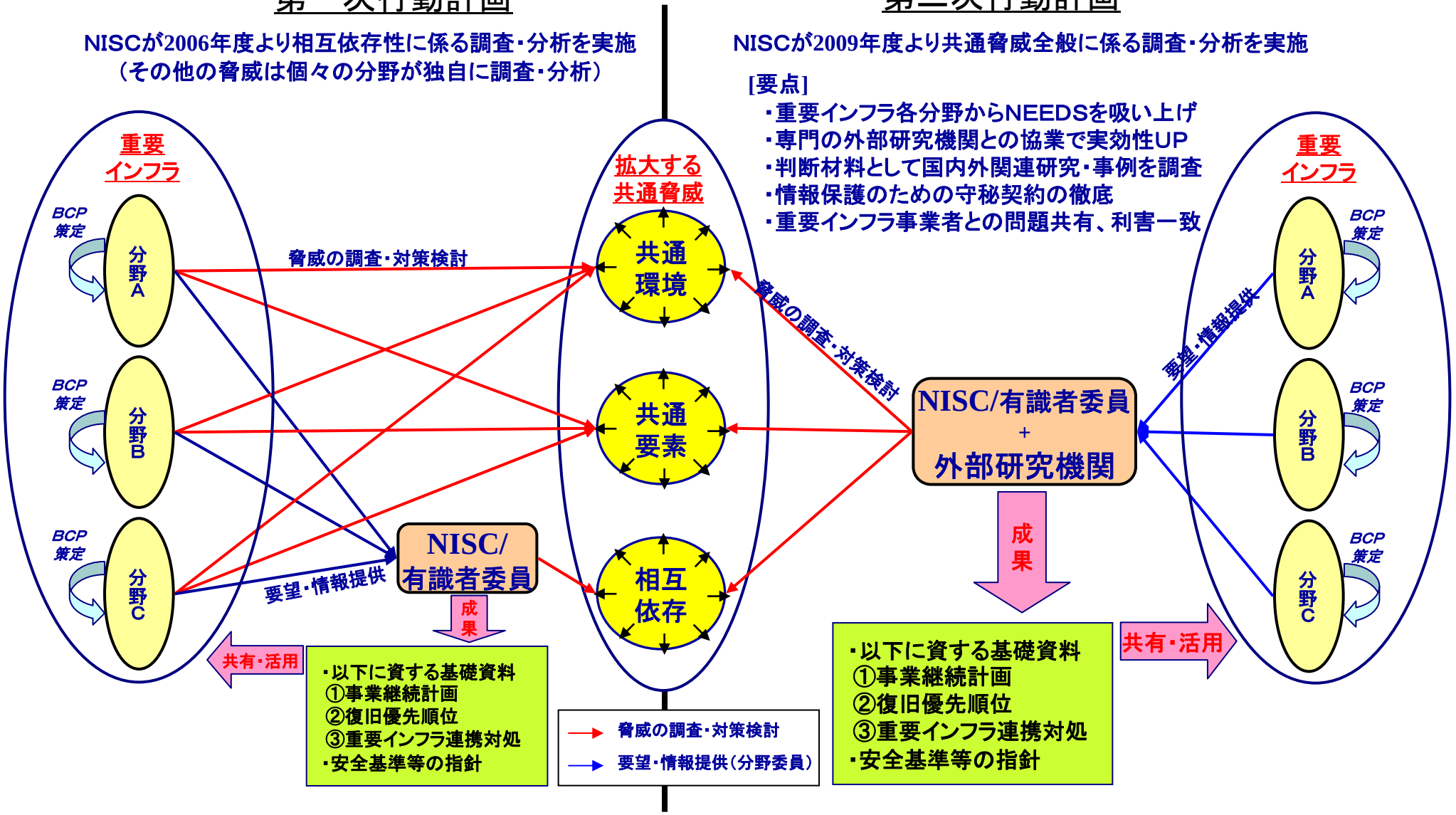
第一次行動計画

NISCが2006年度より相互依存性に係る調査・分析を実施
（その他の脅威は個々の分野が独自に調査・分析）

第二次行動計画

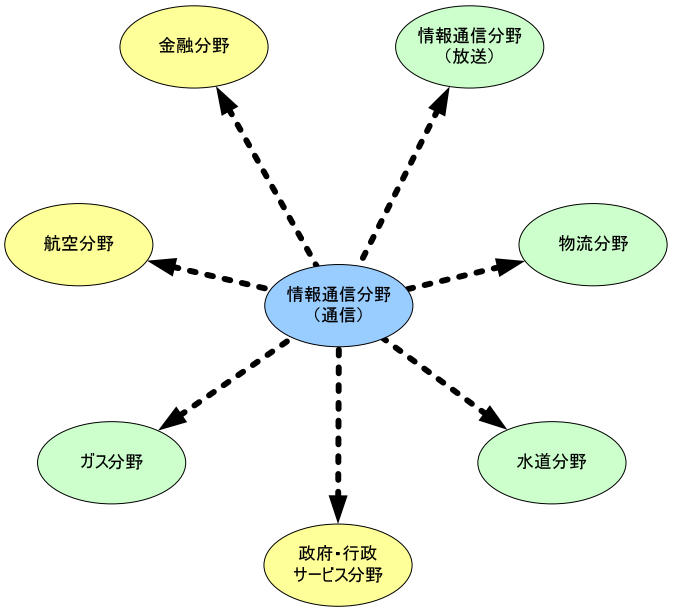
NISCが2009年度より共通脅威全般に係る調査・分析を実施

[要点]
- 重要インフラ各分野からNEEDSを吸い上げ
- 専門の外部研究機関との協業で実効性UP
- 判断材料として国内外関連研究・事例を調査
- 情報保護のための守秘契約の徹底
- 重要インフラ事業者との問題共有、利害一致

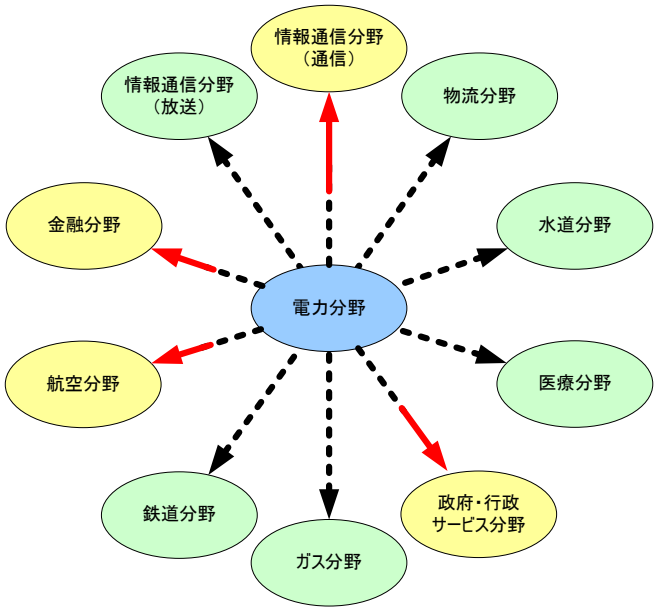


相互依存性解析の検討結果

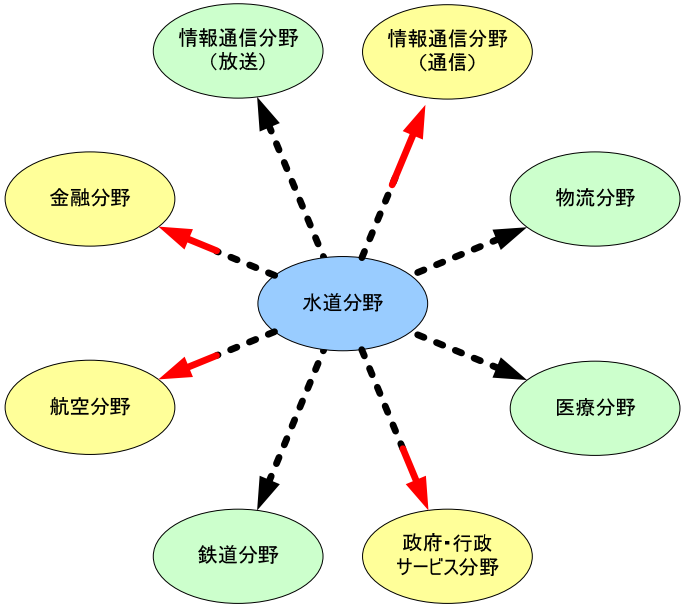
◆相互依存性を次のように捉える
- ある重要インフラ分野にIT障害が生じた場合に、他の重要インフラ分野に影響が波及する場合。
- ある重要インフラ分野にサービスの停止や機能の低下等が生じた場合に、他の重要インフラ分野の重要システムに影響が波及する場合。



通信分野と他分野との相互依存性



電力分野と他分野との相互依存性



水道分野と他分野との相互依存性

凡例

分野間の相互依存性

時間経過に伴う状況変化等により変化する可能性のある分野間の相互依存性

A分野 → B分野　A分野のサービスの停止や機能の低下等により、B分野の重要システムが機能不全（又は定常運用ではない状態）となる可能性がある。

A分野　重要システムとサービスの独立性が高い分野。

A分野　重要システムとサービスの独立性が低い分野。

※上記相互依存性関係において、一般的には各分野におけるサービスに影響しないよう、適切な対策がとられている。

※上記における各分野に係る記載は、各分野の主要な事業者へのヒアリングに基づくものであることに留意が必要である。

NISC National Information Security Center

分野横断的演習

4 分野横断的演習

第一次行動計画

＜2006年度＞ 官民連携の仕組みづくり

研究的演習
演習実施概念、演習課題設定、演習手法の理解等を主眼として実施。

机上演習
脅威として災害を設定し、会議形式の演習を実施。

＜2007年度＞ 官民連携体制の機能向上

機能演習
脅威としてDDoS攻撃を設定し、チーム毎に個室に分かれ、メールのみを利用した演習を実施。

＜2008年度＞ 官民連携体制の実効性向上

機能演習
参加者にIT障害の発生原因を知らせないなどより現実に近い状況で、起こった現象に関する関係者間の情報共有により原因を特定し、サービスの維持・早期復旧や事業継続等を行っていく演習を実施。

分野横断的な演習手法に関する知見

第二次行動計画

分野横断的な重要インフラ防護対策の向上

目標

- 分野横断的な脅威に対する共通認識の醸成
- 他分野の対応状況把握による自分野の対応力強化
- 官民の情報共有をより効果的に運用するための方策

得るもの

演習に関する施策

① シナリオ、実施方法、検証課題等を企画し、演習を実施
② IT障害発生時の早期復旧手順・事業継続計画の検討状況等を把握し、その結果を演習参加者等に提供
③ 演習の向上策検討
④ 演習の実施方法等に関する知見の集約・蓄積

机上演習状況

機能演習状況

NISC National Information Security Center

環境変化への対応

広報公聴活動

広く協力、支援を得るため広報公聴活動を実施

国際連携の推進

国際会合や他国機関との対話を通じた国際連携を推進

その他

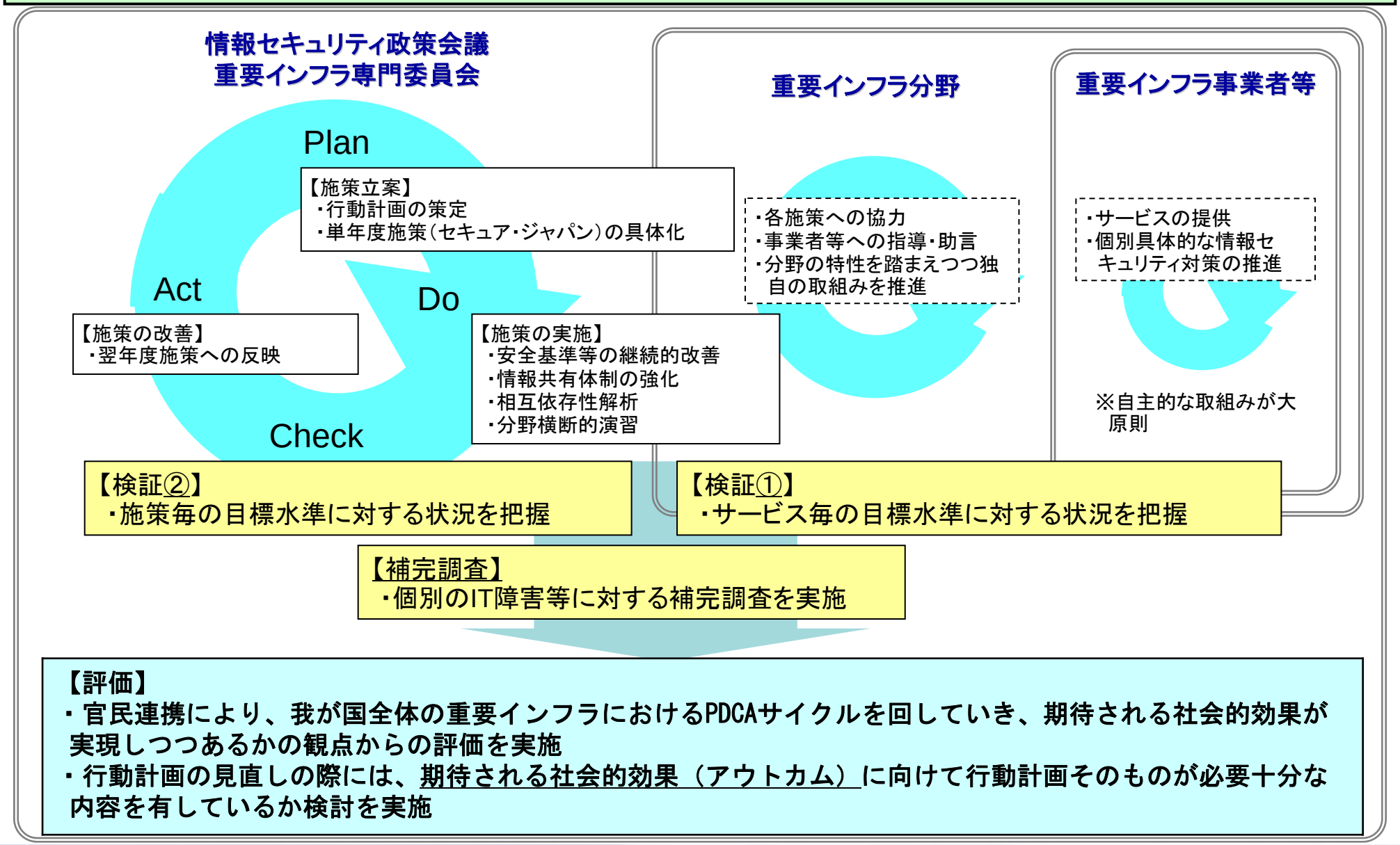
リスクコミュニケーションの充実等

NISC National Information Security Center

評価・検証と改善サイクル

評価・検証と改善サイクルの枠組み

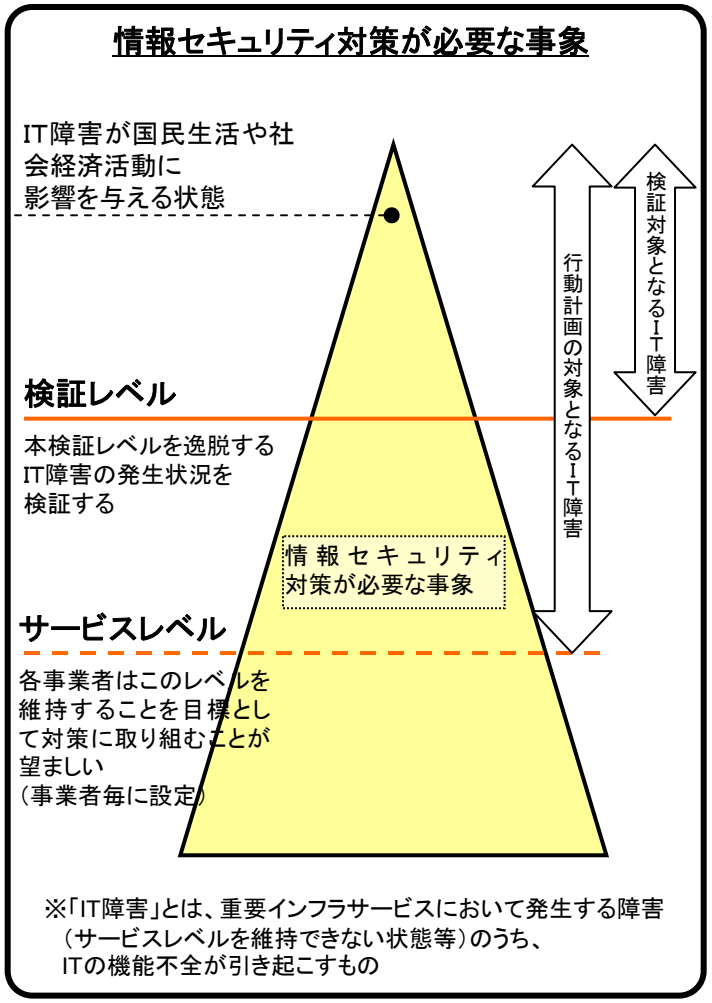
事業者、分野、政府の3層で改善サイクルを駆動



重要インフラサービスと検証レベル

○重要インフラ分野毎に業法上の義務的な取組みに加えて、新たに検証レベルを設定し、これを逸脱するIT障害の発生状況を毎年検証して行動計画の改善を期す

○重要インフラ事業者等は検証レベルによらず各々サービスレベルを定め、これを維持することを目標として対策に取り組む事が望ましい



重要インフラ分野		検証レベル （一部表現を簡素化）
情報通信		・電気通信役務の停止、品質の低下が、3万以上の利用者に対し2時間以上継続する事故が生じないこと
		・放送の停止が生じないこと
金融	銀行	・預金の払戻しの遅延、停止が生じないこと ・融資承諾をした貸付の実行の遅延、停止が生じないこと ・為替（銀行振込）の遅延、停止が生じないこと
	生命保険	・保険金等の支払いに遅延、停止が生じないこと
	損害保険	・保険金等の支払いに遅延、停止が生じないこと
	証券会社 金融商品取引所	・預り有価証券等の売却、解約代金の払い出し等に遅延、停止が生じないこと ・有価証券の売買又は市場デリバティブ取引等に遅延、停止が生じないこと
航空		・貨客の運送に支障を及ぼす定期便の欠航が生じないこと
鉄道		・旅客の輸送に支障を及ぼす列車の運休が生じないこと
電力		・供給支障電力が10万キロワット以上で、その支障時間が10分以上の供給支障事故が生じないこと
ガス		・供給支障戸数が30以上の供給支障事故が生じないこと
政府・行政サービス（地方公共団体を含む）		・住民等の権利利益の保護に支障が生じないこと ・住民等の安全・安心を確保できる時間内にシステムの復旧を行うこと
医療		・診療録等の保存に支障が生じないこと
水道		・断減水、水質異常、重大なシステム障害のうち給水に支障を及ぼすものが生じないこと
物流		・貨物運送の停止や貨物の紛失が生じないこと

※概要を示すため表現を簡素化。正確な表記は第2次行動計画を参照。

防護対象とする重要インフラサービスの例（抜粋）

重要インフラ分野		重要インフラサービス（手続きを含む）（注）	
		呼称	サービス（手続きを含む）の説明
情報通信		・電気通信役務	・電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること
		・放送	・公衆によって直接受信されることを目的とする無線通信の送信
金融	銀行	・預金、貸付、為替	・預金又は定期積金等の受入れ、資金の貸付け又は手形の割引、為替取引
	生命保険	・保険金等の支払い	・保険金等の支払請求の受付、保険金等の支払審査、保険金等の支払い
	損害保険	・保険金等の支払い	・事故受付、損害調査等、保険金等の支払い
	証券会社 金融商品取引所	・有価証券の売買等 ・金融商品市場の開設	・有価証券の売買、市場デリバティブ取引又は外国市場デリバティブ取引 ・有価証券の売買又は市場デリバティブ取引を行うための市場施設の提供、その他取引所金融商品市場の開設に係る業務
航空		・旅客、貨物の航空輸送サービス ・予約、発券、搭乗・搭載手続き	・他人の需要に応じ、航空機を使用して有償で旅客又は貨物を運送する事業 ・航空旅客の予約、航空貨物の予約、航空券の発券、料金徴収、航空旅客のチェックイン・搭乗、航空貨物の搭載
鉄道		・旅客輸送サービス ・発券、入出場手続き	・他人の需要に応じ、鉄道による旅客又は貨物の運送を行う事業 ・座席の予約、乗車券の販売、入出場の際の乗車券等の確認
電力		・一般電気事業	・一般の需要に応じ電気を供給する事業
ガス		・一般ガス事業	・一般の需要に応じ導管によりガスを供給する事業
政府・行政サービス		・地方公共団体の行政サービス	・地域における事務、その他の事務で法律又はこれに基づく政令により処理することとされるもの
医療		・診療	・診察や治療等の行為、診療録及び診療諸記録類等の記録・保存
水道		・水道による水の供給	・一般の需要に応じ、導管及びその他工作物により飲用水を供給する事業
物流		・物流	・貨物の運送及び保管

注　本行動計画の目標から、ITを全く利用していないサービスについては対象外

※概要を示すため表現を簡素化。正確な表記は第2次行動計画を参照。

政府の施策の成果検証

情報セキュリティ対策の柱毎に、重要インフラ事業者等の情報セキュリティ対策への寄与を検証

情報セキュリティ対策の柱	検証指標
安全基準等の整備及び浸透	・指針及び参考資料に採録した対策項目数 ・安全基準等に基づいて定期的な自己検証に取り組んでいる重要インフラ事業者等の数 ・指針の重要インフラ事業者等による評価
情報共有体制の強化	・内閣官房が発信した情報件数 ・セプター等で共有された情報件数 ・共有された情報が情報セキュリティ対策に資すると評価した重要インフラ事業者等の数
共通脅威分析	・共通脅威分析において実施した検討項目件数 ・共通脅威分析の検討項目について、各検討結果の重要インフラ事業者等の評価
分野横断的演習	・演習の述べ参加者数 ・演習で得られた知見が所属する組織の情報セキュリティ対策に資すると評価した重要インフラ事業者等の数
環境変化への対応	（広報公聴活動） ・Webサイトのコンテンツの充実度 ・行動計画を紹介したセミナー等の回数 （リスクコミュニケーション） ・セプターカウンシルや分野横断的演習等の関係主体間のコミュニケーションの機会の開催回数

２月２日は「情報セキュリティの日」です

ありがとうございました。

内閣官房情報セキュリティセンター
（NISC）ホームページ
http://www.nisc.go.jp/