NISC National Information Security Center

重要インフラに関する情報セキュリティ政策について

2010年 1月25日

内閣官房情報セキュリティセンター（NISC）
内閣参事官　丹代　武

目次

- 情報セキュリティ対策が求められる背景
- 内閣官房情報セキュリティセンターについて
- 第２次行動計画の目標と方向性
- 第２次行動計画の対象
- 情報セキュリティ対策の５つの柱
- 関係主体の役割と取組み
- 評価・検証と見直し
- 参考情報

情報セキュリティ対策が求められる背景

重要インフラにおけるＩＴ利用状況

ＩＴは、重要インフラサービスの利便性向上や重要インフラ事業者等の業務効率化など広範に利用されている。今後も、ＩＴの利用は経済社会の発展とともに拡大すると予想される。

携帯電話の高機能化

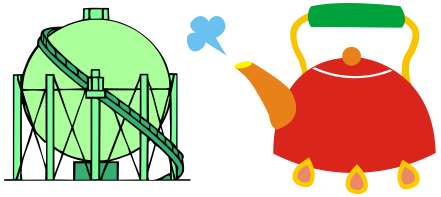
地上波デジタル放送への移行

ＡＴＭの利用

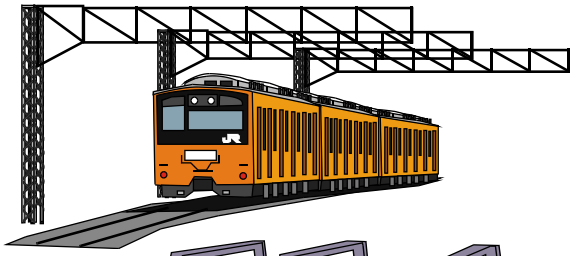
インターネットによる証券取引

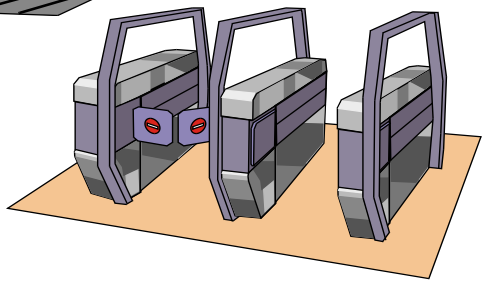
ＰＣ利用者数の増加

ガス安全システム

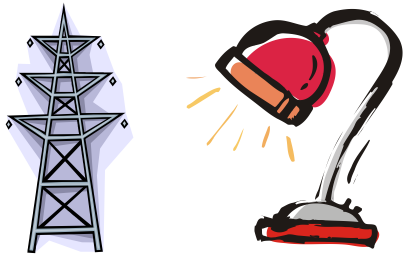


鉄道運行システム、ＩＣカード

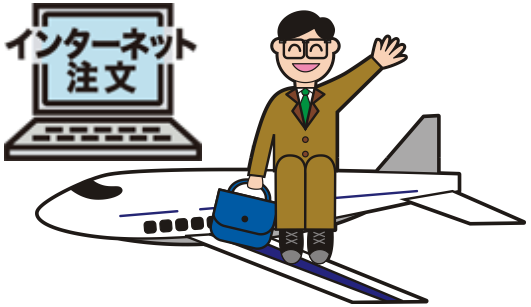




送電システム



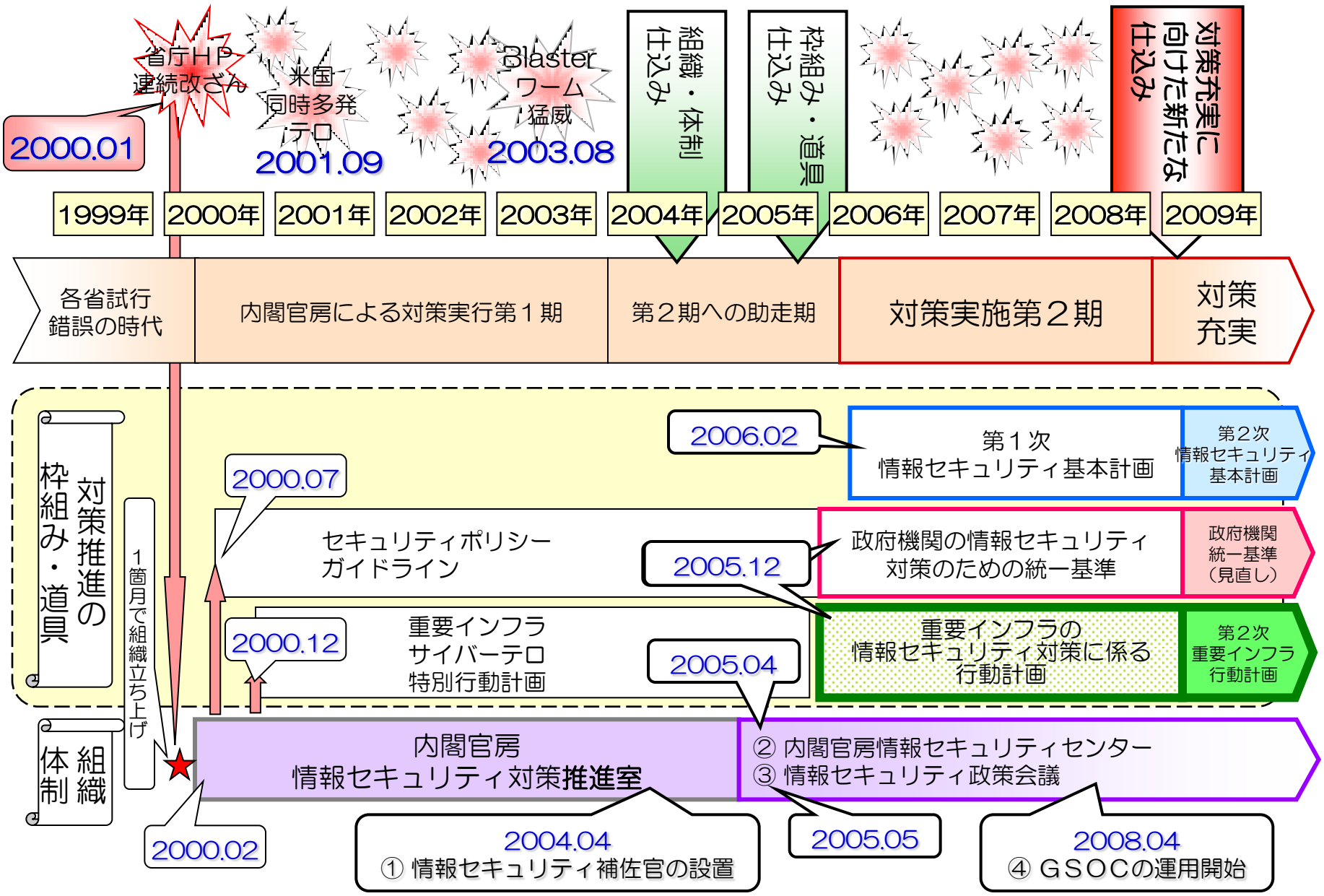
航空チケットのインターネット予約



ＩＴ障害が国民生活や社会経済活動へ及ぼす影響

重要インフラ分野		IT障害やその影響の例
情報通信･放送		･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、ガ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

内閣官房における情報セキュリティ政策の流れ



情報セキュリティ政策会議の構成

情報セキュリティ政策会議 官民における統一的・横断的な情報セキュリティ対策の推進を図る

【閣僚構成員】
内閣官房長官　【議長】
内閣府特命担当大臣（科学技術政策）【議長代理】
国家公安委員会委員長
総務大臣
経済産業大臣
防衛大臣

【有識者構成員】	
小野寺　正	KDDI株式会社代表取締役社長兼会長
黒川　博昭	富士通株式会社相談役
土屋　大洋	慶應義塾大学大学院准教授
野原　佐和子	株式会社イプシ・マーケティング研究所代表取締役社長
前田　雅英	首都大学東京法科大学院教授
村井　純	慶應義塾大学教授

（活動中の各種専門委員会）

重要インフラ専門委員会 我が国全体の重要インフラ防護に資する情報セキュリティに係る事項について調査検討

浅野　正一郎【委員長】	情報・システム研究機構　国立情報学研究所　教授
伊藤　悦郎	東日本旅客鉄道（株）　総合企画本部システム企画部次長
稲垣　隆一	弁護士
大塚　順三	日本放送協会　総合企画室〔情報システム〕次長
大林　厚臣	慶應義塾大学大学院経営管理研究科　教授
雄川　一彦	日本電信電話（株）技術企画部門次世代ﾈｯﾄﾜｰｸ推進室 担当部長
岸本　博之	（財）金融情報システムセンター　監査安全部長
阪上　啓二	野村證券（株）　ＩＴ基盤戦略部長
佐藤　久光	東京都総務局行政改革推進部　副参事
神保　謙	慶應義塾大学　総合政策学部　准教授
田口　靖	（社）日本水道協会　工務部長
竹原　秀臣	電気事業連合会　情報通信部長
土居　範久	中央大学　理工学部教授

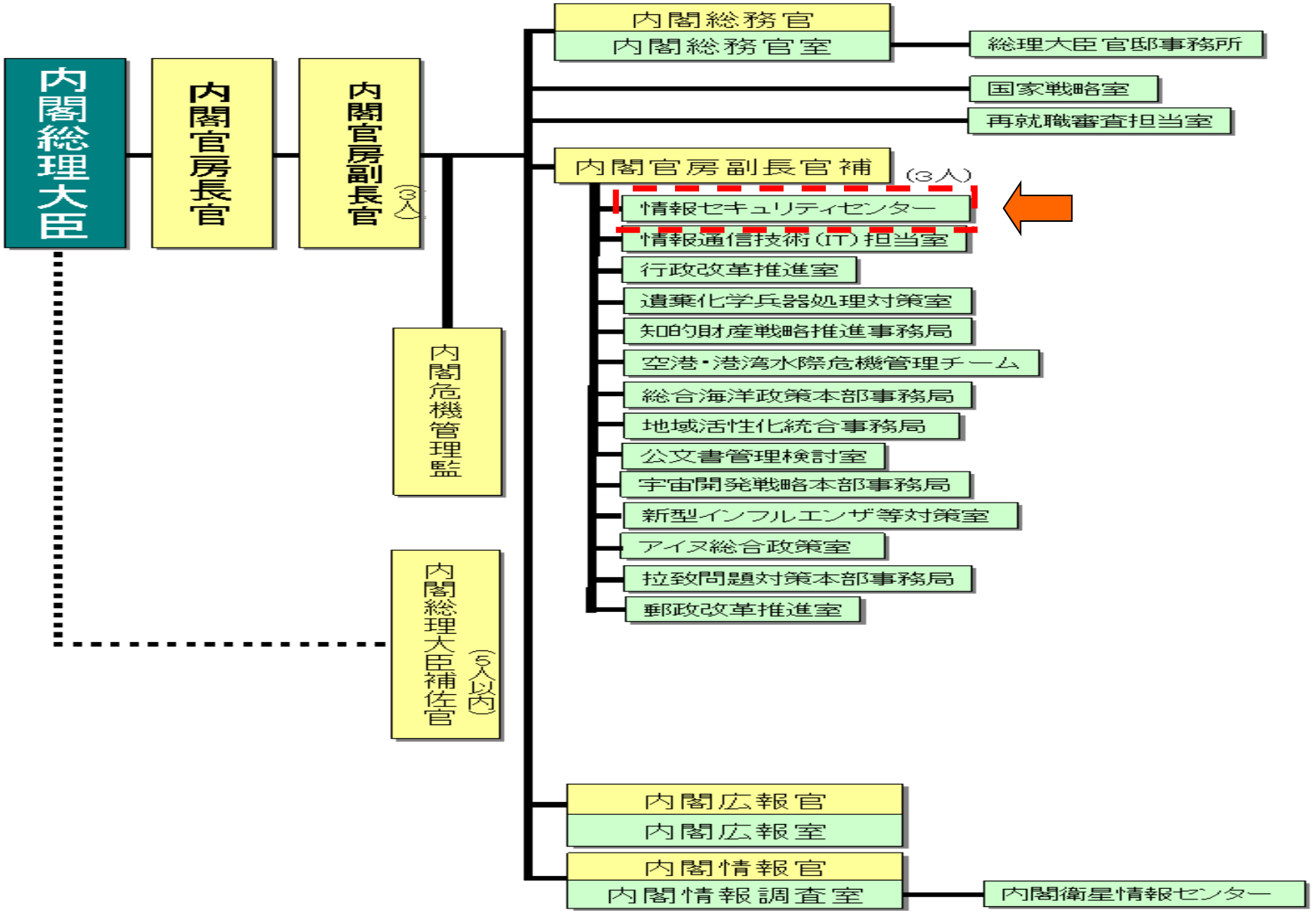
中尾　康二	KDDI（株）　運用統括本部　情報セキュリティフェロー
永瀬　裕伸	日本通運（株）　ＩＴ推進部　専任部長
早貸　淳子	一般社団法人　JPCERTｺｰﾃﾞｨﾈｰｼｮﾝｾﾝﾀｰ　常務理事
広瀬　雅行	（株）東京証券取引所ＩＴ企画部長
松田　栄之	新日本有限責任監査法人　公会計本部ディレクター
宮島　理一郎	定期航空協会　IT専門委員
持田　恒太郎	（株）三井住友フィナンシャルグループ　IT企画部
森山　拓哉	住友生命保険（相）　情報システム部システムリスク管理室長
矢野　一博	日本医師会総合政策研究機構　主任研究員
山川　浩之	（社）日本ガス協会　技術部長
山本　志郎	日本興亜損害保険（株）ＩＴ企画部
渡辺　研司	長岡技術科学大学　大学院技術経営研究科准教授
渡邊　正美	東京地下鉄（株）　鉄道本部　安全・技術部長

情報ｾｷｭﾘﾃｨ報告書専門委員会 政府機関の情報セキュリティ報告書作成のためのガイドラインの策定、情報セキュリティ報告書の定量的評価等の手法等について調査検討

技術戦略専門委員会 情報セキュリティに係る研究開発及び技術開発並びにそれらの成果利用の戦略に係る事項について調査検討

内閣官房情報セキュリティセンターについて

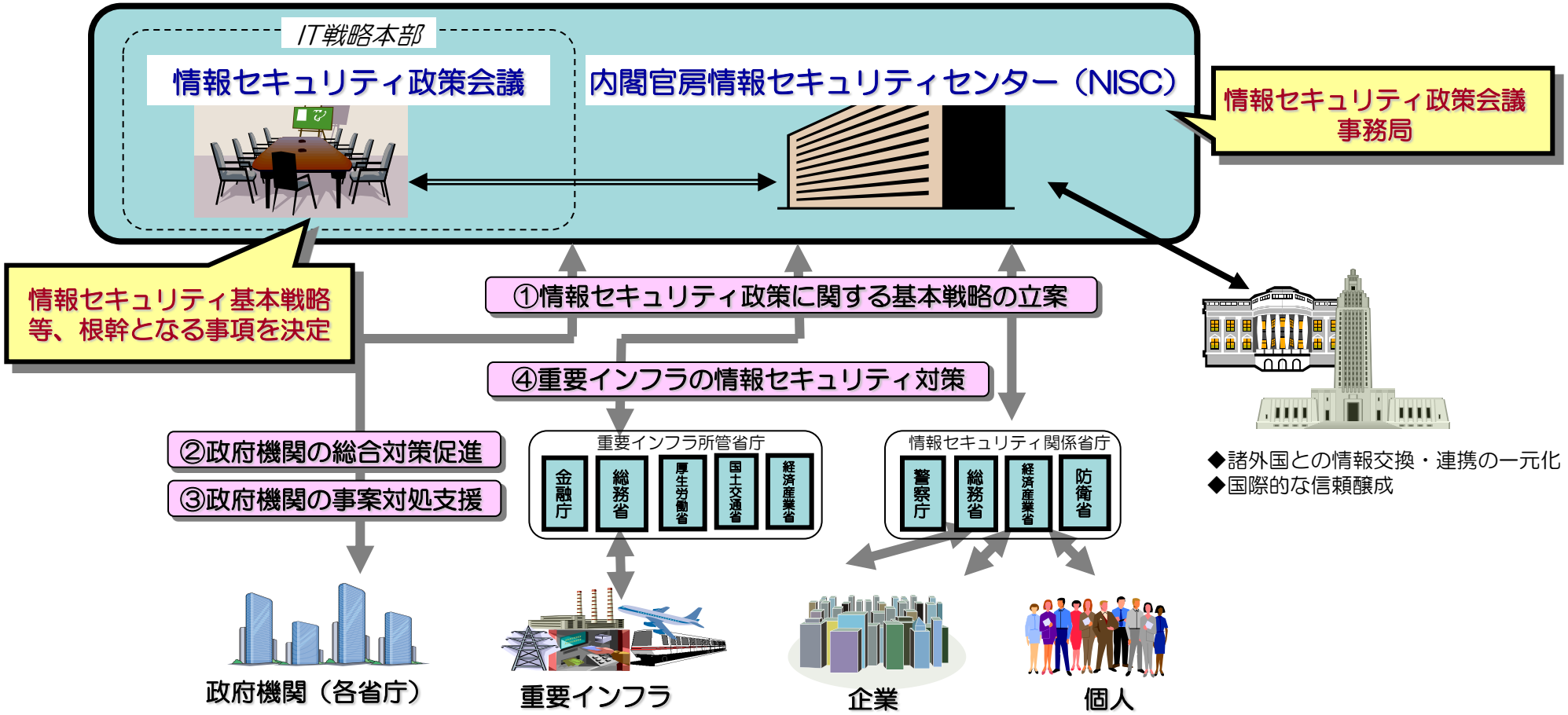
内閣官房組織図（2010年1月現在）



内閣官房情報セキュリティセンター（NISC）の役割

「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

- 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



情報セキュリティセンターの組織

官民から専門家を集約（2010年1月現在約80名）

センター長
内閣官房副長官補（安全保障・危機管理）

副センター長

情報セキュリティ補佐官
（2名）

副センター長

基本戦略立案グループ
- 全体戦略（「情報セキュリティ基本計画」）策定
- 研究開発・技術開発戦略の立案
- 情報共有・対策その他の官民連携の推進　等

政府機関総合対策促進グループ
- 政府統一的な「対策基準」の策定
- 政府統一的な情報セキュリティ対策の「評価」等

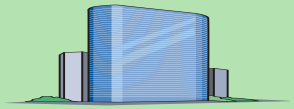
事案対処支援グループ
- 早期警戒情報の収集・分析機能の強化
- 情報セキュリティ関係機関との連携強化　等

重要インフラ対策グループ
- 行動計画の推進
- 横断的な対策基準の策定
- 共通脅威分析
- 分野横断的演習の実施　等

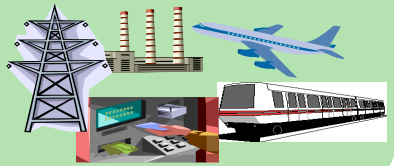
国際戦略グループ
- 情報セキュリティに関する我が国の国際戦略の立案
- 諸外国の関係機関等との緊密な連携　等

企業　個人

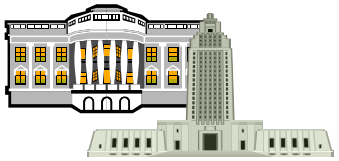
各政府組織



重要インフラ



諸外国関係機関



第２次行動計画の目標と方向性

第２次行動計画の目標

目標：「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」

第２次行動計画の２つの側面

第１次行動計画からの「**継続**」

「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

重要インフラの情報セキュリティ対策に取り組む関係主体の、ＩＴ障害が重大な影響を及ぼさないよう**不断の努力を怠らない**という基本姿勢の表れ

第１次行動計画を踏まえた「**発展**」

分野ごとの重要インフラサービスの合理的な水準をサービスレベルとして定める

各分野の特性を踏まえつつ、**現状に即して**情報セキュリティ対策の実効性を継続的に改善できるようにする

「重要インフラ事業者等のサービスの維持」のためのＩＴ障害の予防的対策と「ＩＴ障害発生時の迅速な復旧等の確保」のための事後的対策の両方について広く具体化

基本的な方向性

重要インフラ事業者等が主体的に連携できる環境を構築するために、各主体が努めるべき基本的な方向性を整理

1）指針の遵守に加えて、先進的な対策の活用に努めること

2）技術面、経営面、法制面での対応の調和を図ること

3）顧客サービスの視点と社会的責任の視点の双方に配慮すること

4）ＩＴ障害の予防的対策に努め、また予防的対策を過信しないこと

5）ＩＴ障害に関する情報は可能な限り共有すべきと理解すること

理想とする将来像

第2次行動計画に基づく取組みによって以下のような将来像を目指す

各関係機関の主体的な取り組み及び連携の確立

- 関係主体は守るべき重要インフラサービスと必要な対策を理解
- 関係主体はIT障害発生時に誰とどのような情報を共有すべきかを理解

IT障害に関する情報共有の価値の普遍化

- 「情報セキュリティガバナンス」の考え方が重要インフラ事業者等に十分に浸透
- 重要インフラ事業者等は、IT障害の発生は隠すべきものではなく関係者間で共有すべきものであるという認識の所有

将来像

- IT障害は発生していないか、発生しても社会経済活動に重大な影響を与える事態には至らない
- 関係主体が連携して重要インフラ防護に取り組んでいることが広く国民に知られ、国民に安心感を与えるようになっている
- 各関係主体の情報セキュリティ対策に関する取り組みが社会の持続的な発展を支えるものとして確実に定着している

環境変化への機敏な対応体制の普遍化

- 重要インフラ事業者等は、IT障害の脅威やリスクの変化を適切に察知して、各々自主的に対策を進め、また必要に応じて調整を実施

内閣官房を中心とした速やかな解決体制の構築

- 情報セキュリティ対策に資する多様な情報が内閣官房に集積
- 特異重大な脅威等の場合には、内閣官房、専門委員会、セプターカウンシルの連携により、解決策の実現に向けた調整を速やかに実施

第２次行動計画の対象

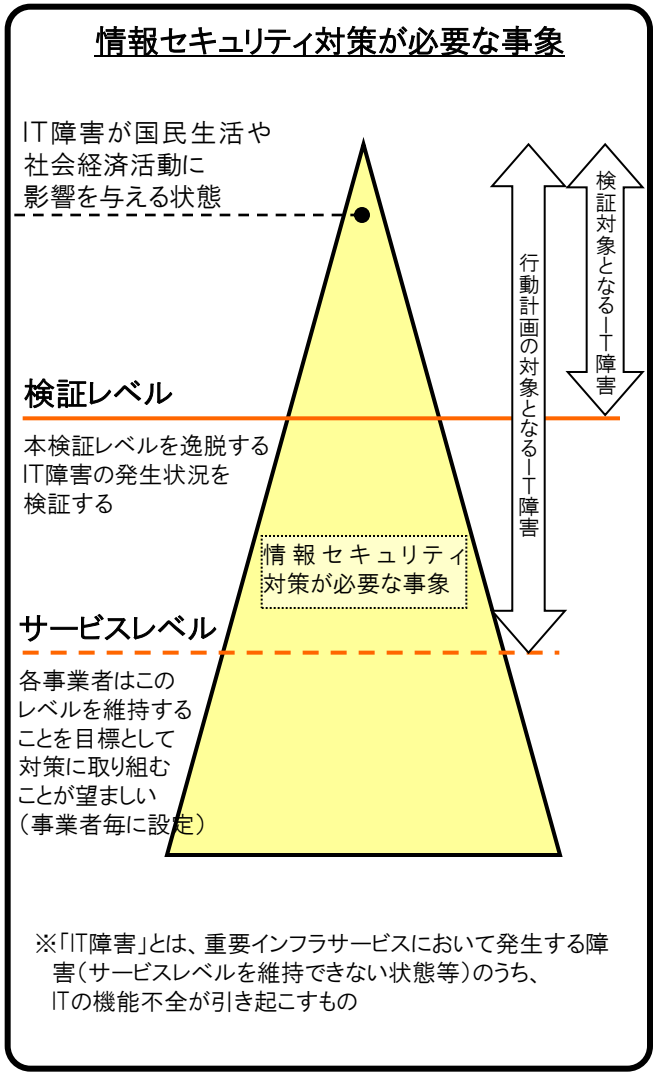
防護対象となる重要インフラ分野・サービス

国民生活及び社会経済活動の基盤となる重要インフラ10分野が対象

重要インフラ分野		重要インフラサービス（手続きを含む）	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

検証対象となるＩＴ障害

- IT障害の発生状況を検証するために、検証レベルを設定
- 重要インフラ事業者等は、検証レベルを参考として事業者毎にサービスレベルを設定



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

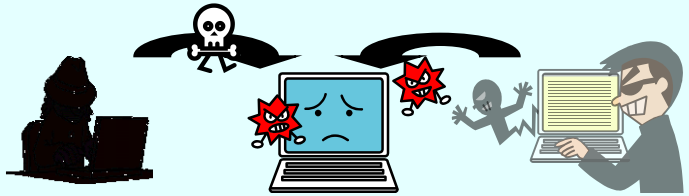
※概要を示すため表現を簡素化している。正確な表記は第2次行動計画の別紙2を参照。

ＩＴ障害を引き起こしうる脅威

ＩＴ障害を引き起こしうる要因を脅威と呼び、４種類に類型化

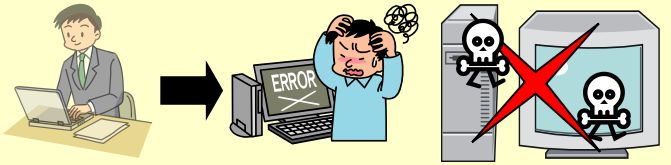
サイバー攻撃をはじめとする意図的要因

（例）
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



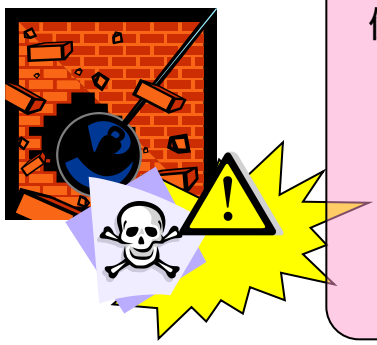
非意図的要因

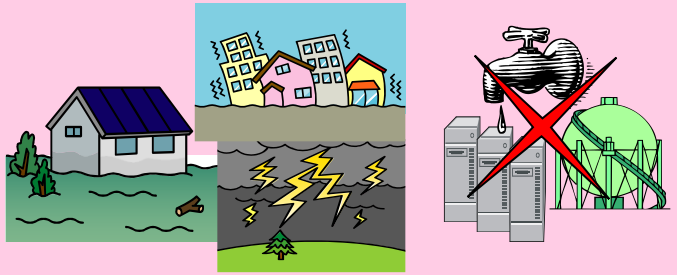
（例）
操作・設定ミス、プログラム上の欠陥（バグ）、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障　等



災害や疾病

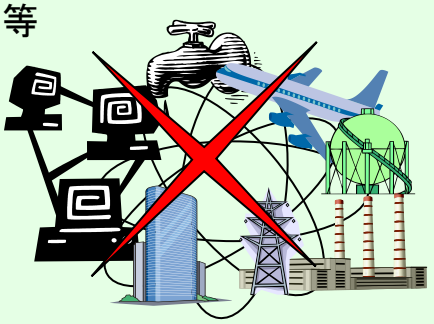
（例）
地震、水害、落雷、火災等の災害による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピューター施設の損壊　等



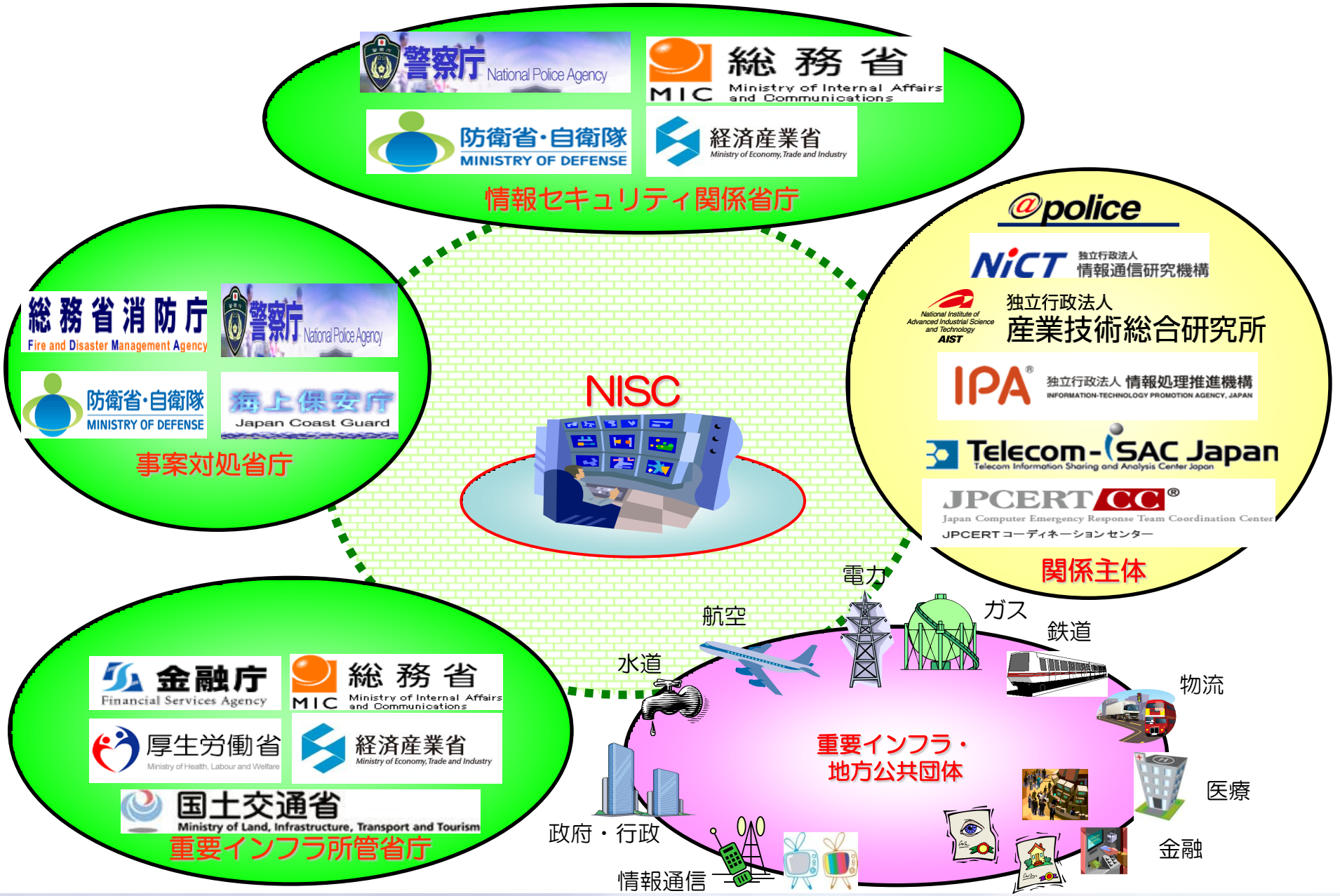


他分野の障害からの波及

（例）
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に取り組むことを想定している関係主体



情報セキュリティ対策の５つの柱

情報セキュリティ対策の５つの柱

・ 第１次行動計画から行ってきた取組みを継続・発展　⇒　①～④
・ 第２次行動計画から開始した新たな取組み　⇒　⑤

①安全基準等の整備及び浸透

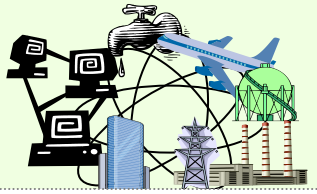
各分野の安全基準等の継続的改善及び浸透に資するため、「安全基準等策定にあたっての指針」の見直しを実施。

②情報共有体制の強化

共有すべき情報の整理を行い、情報共有に必要な環境整備を推進するとともにセプターカウンシル等の活動を充実強化。

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

③共通脅威分析

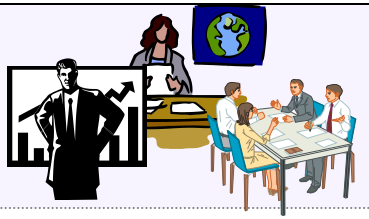


重要インフラ分野共通に起こり得る脅威を分析し、重要インフラサービスの維持・復旧に関する基礎資料を提供。

④分野横断的演習

官民の情報共有体制の見直しや重要インフラ事業者等の事業継続計画策定等に資する分野横断的演習を実施。

⑤環境変化への対応

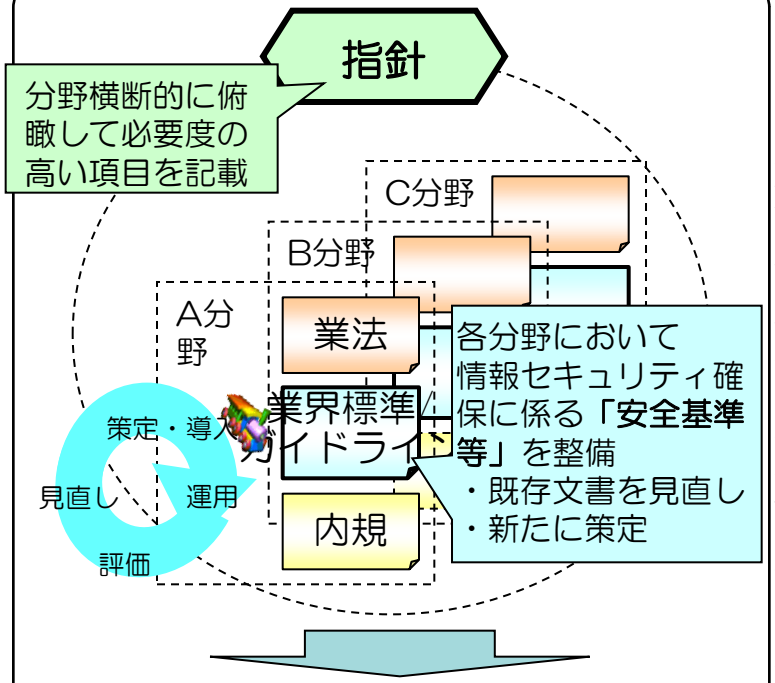


環境の変化に情報セキュリティ対策を機敏に対応させていくため、広報公聴活動やリスクコミュニケーションを充実。

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) 指針に記載する情報セキュリティ対策項目(パブコメ案)

＜対策項目＞

（1）4つの柱

ア　組織・体制及び資源の対策
イ　情報についての対策
ウ　情報セキュリティ要件の明確化に基づく対策
エ　情報システムについての対策

（2）5つの重点項目

ア　IT障害の観点から見た事業継続性確保のための対策
イ　情報漏えい防止のための対策
ウ　外部委託における情報セキュリティ確保のための対策
エ　IT障害発生時の利用者の対応のための情報の提供等の対策
オ　ITに係る環境変化に伴う脅威のための対策

（参考）　安全基準等の状況把握のための取組

調査名	安全基準等の継続的改善状況等の把握及び検証	安全基準等の浸透状況等に関する調査
1）対象	重要インフラ分野	重要インフラ事業者
2）目的	各重要インフラ分野の取り組み等の実態把握を行い、指針の分析・検証の結果を踏まえた改善の状況や、重要インフラ分野毎の独自の改善の状況について、客観的な把握、検証を行う	重要インフラ事業者自らが定める「内規」を含めた対策状況の客観的な把握を行う
3）方法	重要インフラ所管省庁を通じた調査	重要インフラ所管省庁を通じたアンケート等の実施
4）項目	①「安全基準等」の見直し状況等 ②各分野の安全基準等の特徴等	①安全基準等の整備状況に関する事項 ②情報セキュリティ対策の実施状況に関する事項 ③安全基準等に対する準拠状況 ④政府への提言、要望等
5）頻度	毎年実施	毎年実施
6）次回実施	2010年2月（予定）	2010年4－6月（予定）
備考	前回調査実績（10分野12業種）	前回調査実績（3019事業者）

２　情報共有体制の強化

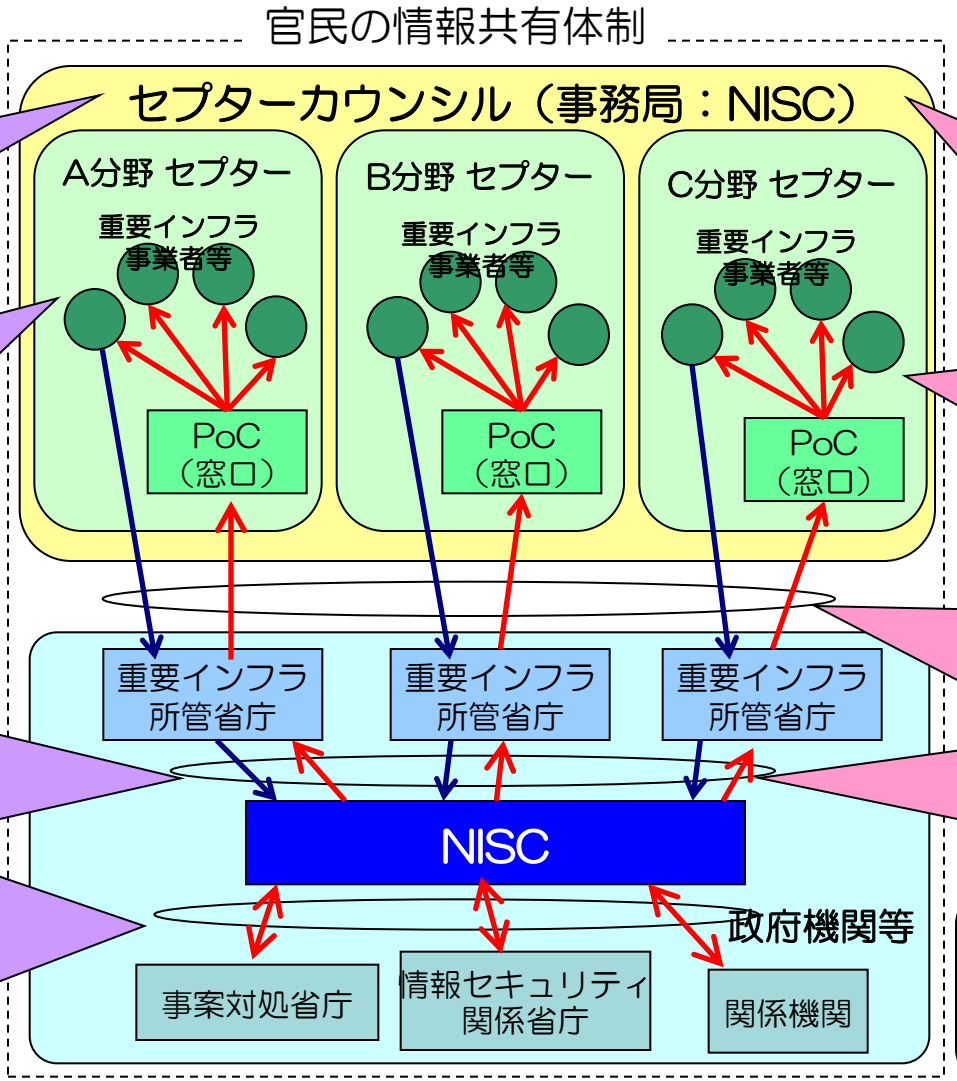
第１次行動計画において構築した「官民の情報共有の枠組み」を踏襲し、第２次行動計画では「官民連携、情報提供の充実」を目指す。

◆第１次行動計画の成果

◎セプターカウンシルの創設（平成21年2月）
・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



◆第２次行動計画の取組み

◎セプターカウンシル
・各セプターにより構成される共助・互恵の活動の取組みの場
・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
・セプターにおける情報の収集、把握・分析、情報の共有・発信
・コーディネータの設置等の自主的な取組みへの期待

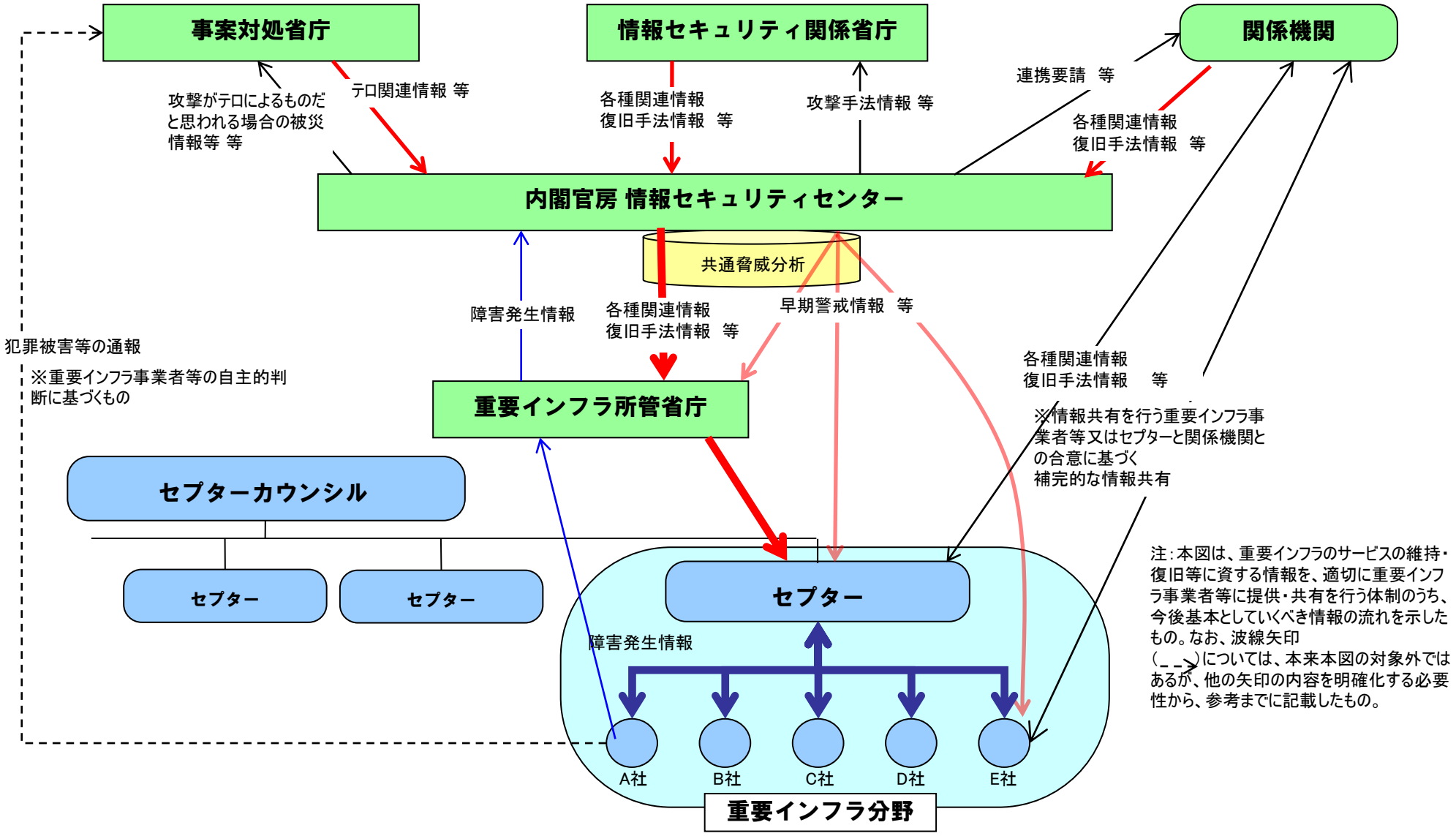
◎情報提供・情報連絡の充実
・実施細目を含めた各経路間の情報取り扱いルールの整合
・関係機関等が保有する分析機能の活用
・セキュリティに関して有用な活動を行う機関との連携の推進

◎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提供のあり方を整理

※「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

2　情報共有体制の強化（続き）

（第２次行動計画　別紙４より）



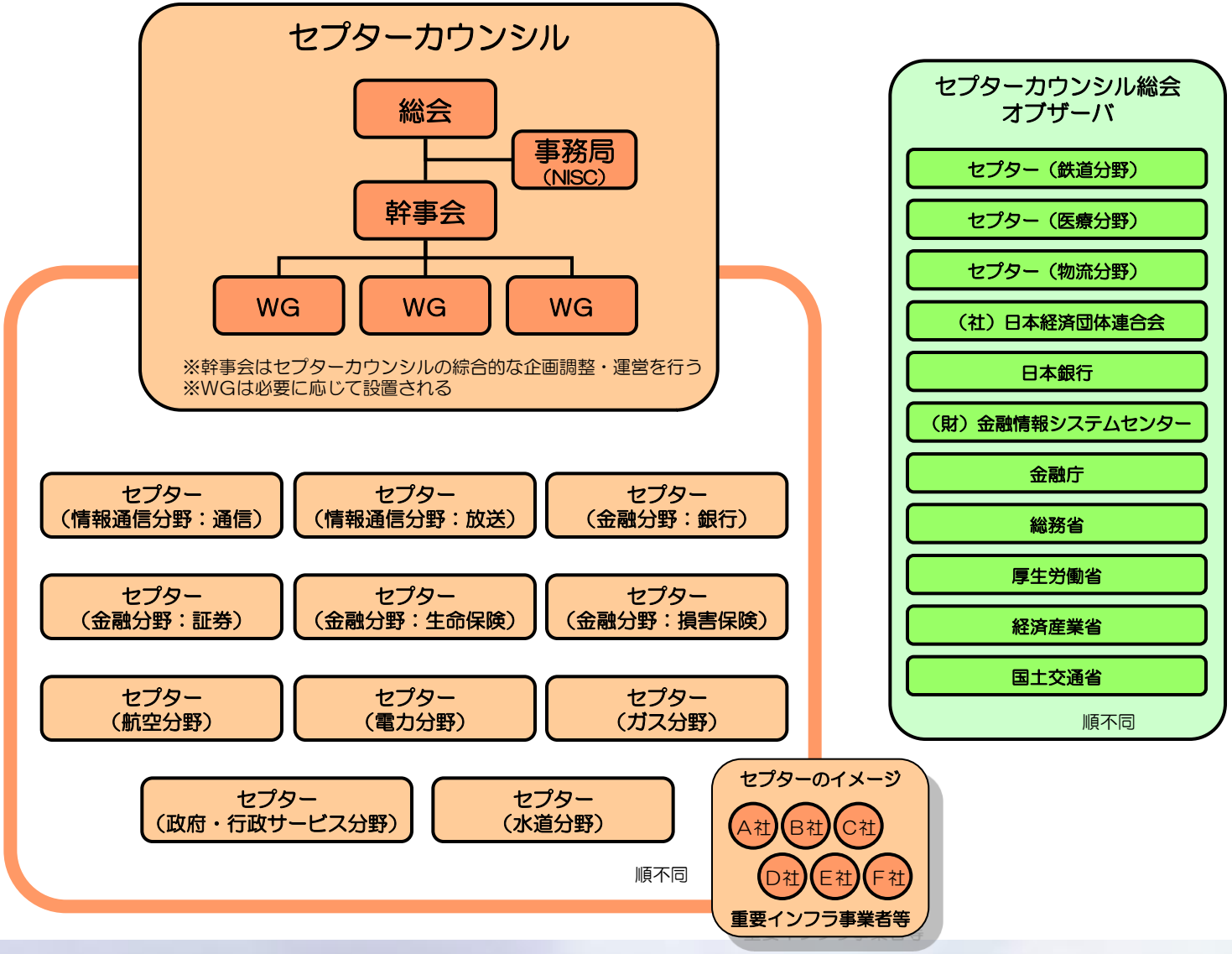
注：本図は、重要インフラのサービスの維持・復旧等に資する情報を、適切に重要インフラ事業者等に提供・共有を行う体制のうち、今後基本としていくべき情報の流れを示したもの。なお、波線矢印（_ _>）については、本来本図の対象外ではあるが、他の矢印の内容を明確化する必要性から、参考までに記載したもの。

共有すべき情報のイメージ（検討例）

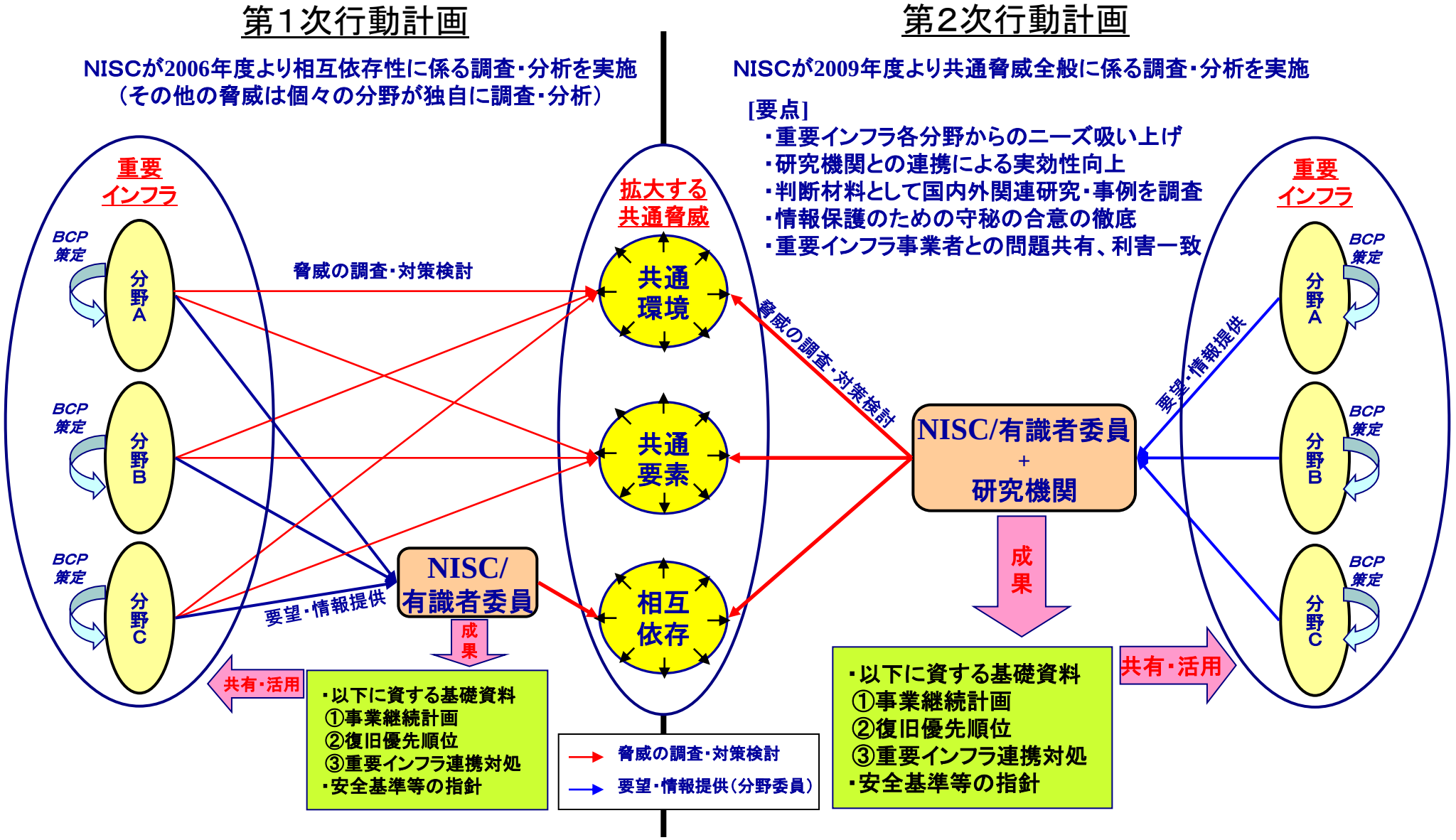
情報ソース ＼ 共有情報	A. 再発防止の観点で有益な情報	B.未然防止の観点で有益な情報 a.各種規程、制度、環境変化等に関する情報	B.未然防止の観点で有益な情報 b.個別の事例等に関する情報	B.未然防止の観点で有益な情報 c.予兆・警報に関する情報	C. 障害の拡大防止・復旧のため必要となる情報
政府機関（下記の機関以外）		◎海外動向 ・犯罪事例 ・障害事例 ・技術動向　…等	◎脅威の動向 ・脅威の内容 ・脅威への対処方法 ・攻撃事例 ・攻撃方法 ・NISCの見解、コメント等 ◎演習、訓練等から得られた課題等	◎国事等（ソーシャルイベント）	◎緊急事態（大規模サイバー攻撃等）時の広報等 ・対策室の設置/閉鎖情報（連絡体制の変更）等 ◎災害情報 ・災害の現地情報　・被害の復旧見込み
NISC(重要インフラG以外)	◎IT障害事例 ・障害の内容 ・障害の原因 ・発生時の応急対処 ・IT障害の相関関係 ・体制の変更等長期的対策 ・教訓 （・過去の障害事例一覧） 等 ◎ヒヤリハット事例 ・内容 ・原因 ・再発防止策 ・教訓 等				
公開情報					
NISC重要インフラG		◎関係各種規程類 ・指針等 ◎制度変更等の情報 ◎社会・技術動向 ◎参考文献、会合の案内 ・共通脅威分析等の報告書 ・最新技術動向 ・セミナー等の開催情報 ・人的交流の情報 等 ◎統計情報の提供 ・IT障害、サイバー攻撃の発生状況 等		◎個別の脆弱性に対する情報 ・脆弱性情報 ・対策 ・NISCからの見解、コメント等 ◎予兆についての情報 ・予兆（不審なアクセスの多発、不審メールの急増等）情報 ・トラフィックの観測情報 ・NISCの見解、コメント等	◎個別の脅威（攻撃）についての情報 ・攻撃の内容 ・攻撃手法 ・対策方法 （・NISCによるとりまとめ） 等
関係機関・関係省庁・研究機関等			◎情報セキュリティ対策情報 ・重要インフラ事業者等の分析報告、プレゼンテーション、業界レポート、ベストプラクティス、関係機関等のレポートの公表、等		◎IT障害情報 ・障害の内容　・障害の原因 ・発生時の応急対処 ・IT障害の相関関係 ・障害に対する対策 ・復旧見込み 等
所管省庁・セプター・重要インフラ事業者等		◎情報セキュリティ対策への取組み状況 ・セプター活動状況の紹介、CSR報告書等		◎重要インフラへのサイバー攻撃等の速報	
その他の情報ソース（ベンダー等）					
情報共有のタイミング	（ア）平時（要警戒時・障害発生時以外のタイミング） → リアルタイム性は不要			（イ）要警戒時・障害発生時 → リアルタイム性が必要（実施細目に基づく取扱い）	
情報共有の方法	・ニュースレター ・Webサイト ・意見交換会 ・セミナー ・セプターカウンシル/ワーキング			・ニュースレター ・Webサイト ・実施細目に基づく情報連絡/情報提供	・実施細目に基づく情報連絡/情報提供 （※緊急事態等における別の連絡体制や手続きがある場合を除く）

（参考）セプターカウンシルの概要

・各セプターにより構成される共助・互恵の活動の取組みの場
・11のセプターの参加を得て、平成21年2月に創設。当面の間、ＮＩＳＣが事務局を務める



3　共通脅威分析



2009年度の共通脅威分析各目標の活動内容

1. 重要インフラ分野におけるITに係る脅威の抽出・分類

① 重要インフラ事業者等へのアンケート調査と集計結果の分析等を行い、脅威の対象範囲や、重要インフラ事業者等の抱える課題を抽出・分類する。
② 国内のIT障害事例を把握し、共通脅威分析の方向付け等に資する情報を蓄積する。

2. 協力可能な研究機関の把握と連携準備

研究機関や研究者へのアンケート調査等により、調査・分析に必要な情報や専門的な意見の提供が可能な、あるいは、近い将来共通脅威分析の業務の一端を担うことが可能な連携先を把握し、連携の打診等を行う。

3. 優先度の高い共通脅威の調査・分析

① 1. で抽出・分類した脅威より、優先度の高い共通脅威を選定し、実態、背景、原因などを分析して、各課題の特徴や有効な対策等を把握する。
② 共通脅威全般に関する国内外の研究・調査の動向を把握し、共通脅威分析の方向付けや新たな共通脅威の発見等に資する情報を蓄積する。
③ 平成20年度の相互依存性解析で作成した分野間のデータ送受信に係る分析ワークシートをブラッシュアップし、重要インフラ事業者等の運用に資するよう実用性の向上を図る。

4　分野横断的演習

第1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2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

5　環境変化への対応

環境の変化に情報セキュリティ対策を機敏に対応させることを目指す

環境⇒刻々と変化

○ＩＴ利用動向　○ＩＴ技術動向　○脅威動向等

環境の変化を察知する能力の向上を図る

広報公聴活動

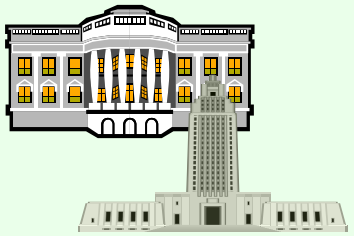
○Webを活用した情報発信や意見受付
○ニュースレターの発行
○会議資料の公開
○セミナー等の開催

リスクコミュニケーションの充実

○連携して対処すべきリスクや対策に関する共通認識の形成
○連携効果の高まり
○強固な信頼関係の構築

国際戦略の推進

○重要情報インフラに関するベストプラクティスの共有
○国際会合や他国機関等との対話を通じた最新動向の把握

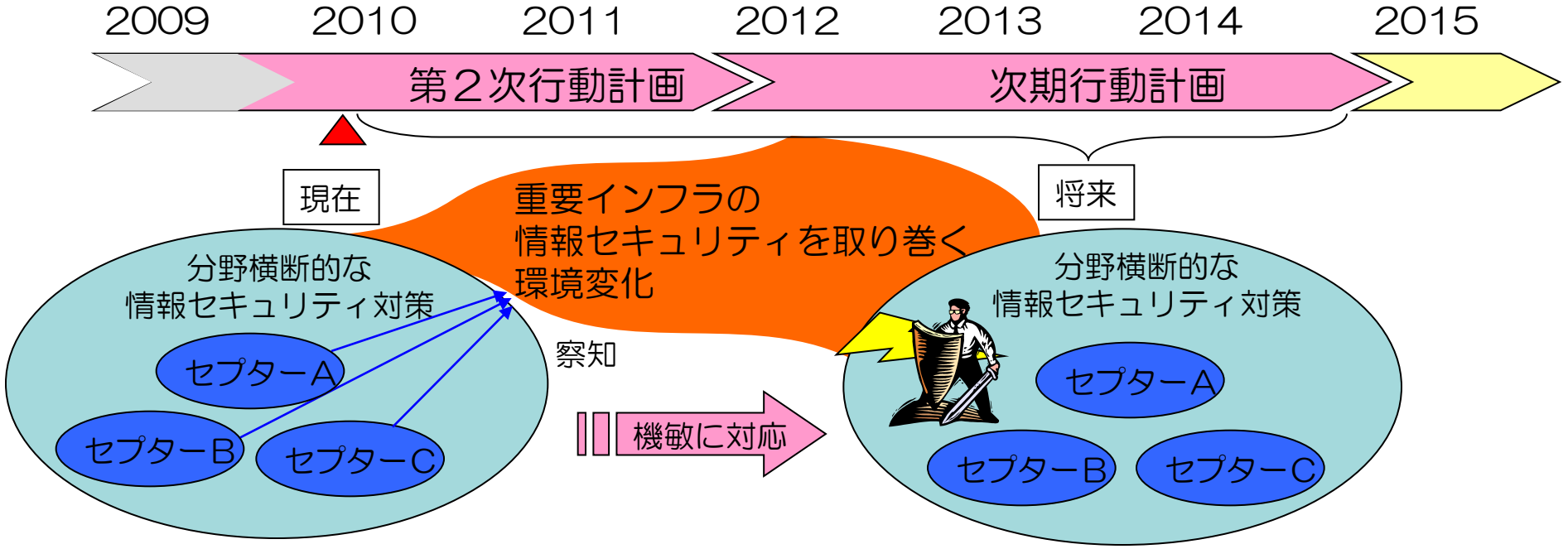


情報セキュリティ基盤の強化

○高度なITスキルを有する人材の育成
○脅威への対応能力の強化に資する研究開発
○地域レベルの連絡・連携

5　環境変化への対応（続き）

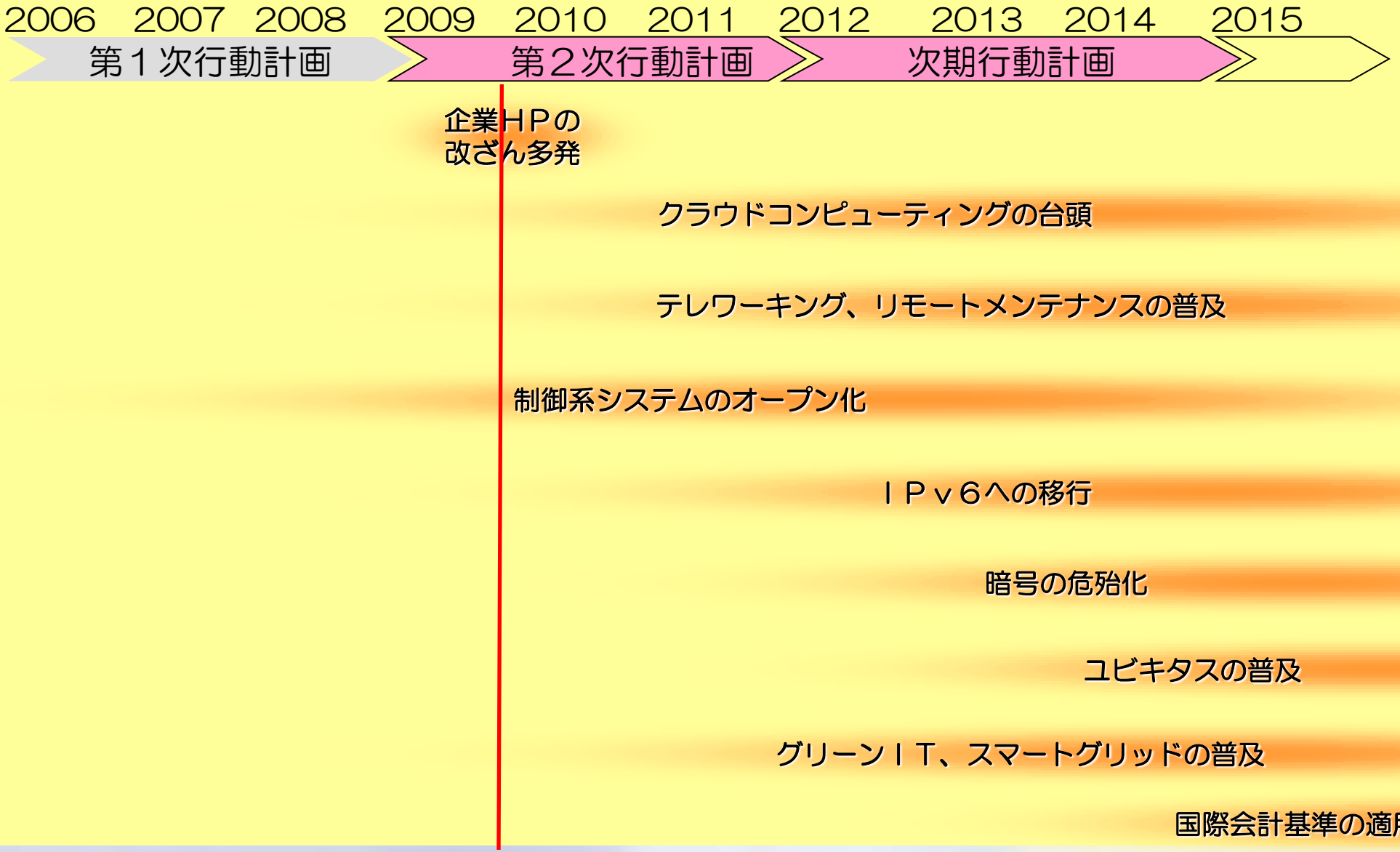
環境変化対応の目標　：①環境の変化を察知する手法を開発する
　②開発した手法を用いて環境の変化の察知する
環境変化の定義　：重要インフラを取り巻く制度・政策、ＩＴ利用、ＩＴ技術、脅威等において今後情報セキュリティに影響を与えると見込まれる変化
時間的視野　：現行行動計画の見直しや次期行動計画の策定に反映するため、2014年度（5年後）頃までに対応が必要となる環境変化を視野に入れる
期待するアウトプット：◎環境変化を察知する手法のまとめ
　◎察知した環境変化とそれに起因する脅威のまとめ



- ＩＣＴ動向に関する情報収集や、重要インフラ事業者へのヒアリングを実施中
- これまでに、ＩＰｖ６、暗号危殆化、クラウド、スマートグリッド等の環境変化を抽出

5　環境変化への対応（続き）

情報セキュリティに影響を与える可能性のある環境変化の例（関係者へのヒアリング結果より）



関係主体の役割と取組み

重要インフラの情報セキュリティ対策の推進体制

情報セキュリティ関係省庁

警察庁 National Police Agency
総務省 MIC Ministry of Internal Affairs and Communications
防衛省・自衛隊 MINISTRY OF DEFENSE
経済産業省 Ministry of Economy, Trade and Industry

事案対処省庁

総務省消防庁 Fire and Disaster Management Agency
警察庁 National Police Agency
防衛省・自衛隊 MINISTRY OF DEFENSE
海上保安庁 Japan Coast Guard

重要インフラ所管省庁

金融庁 Financial Services Agency
総務省 MIC Ministry of Internal Affairs and Communications
厚生労働省 Ministry of Health, Labour and Welfare
経済産業省 Ministry of Economy, Trade and Industry
国土交通省 Ministry of Land, Infrastructure, Transport and Tourism

関係機関

@police
NiCT 独立行政法人 情報通信研究機構
National Institute of Advanced Industrial Science and Technology AIST 独立行政法人 産業技術総合研究所
IPA 独立行政法人 情報処理推進機構 INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
Telecom-ISAC Japan Telecom Information Sharing and Analysis Center Japan
JPCERT CC® Japan Computer Emergency Response Team Coordination Center JPCERTコーディネーションセンター

重要インフラ防護体制の強化のための施策及び対策

我が国全体としての重要インフラ防護に資する施策

各重要インフラ分野に共通の分野横断的に実施すべき施策

NISC

我が国全体としての重要インフラ防護体制に資する施策

NISCで行う施策と連動した対策
自分野・他分野との情報共有の充実

NISCで行う施策と連動した施策
重要インフラ事業者等の情報セキュリティに関する活動の把握

関係主体の取組み

第２次行動計画の実現を図るため、毎年度、より具体的な施策の実施プログラムを「セキュア・ジャパン２０ＸＸ」として策定。

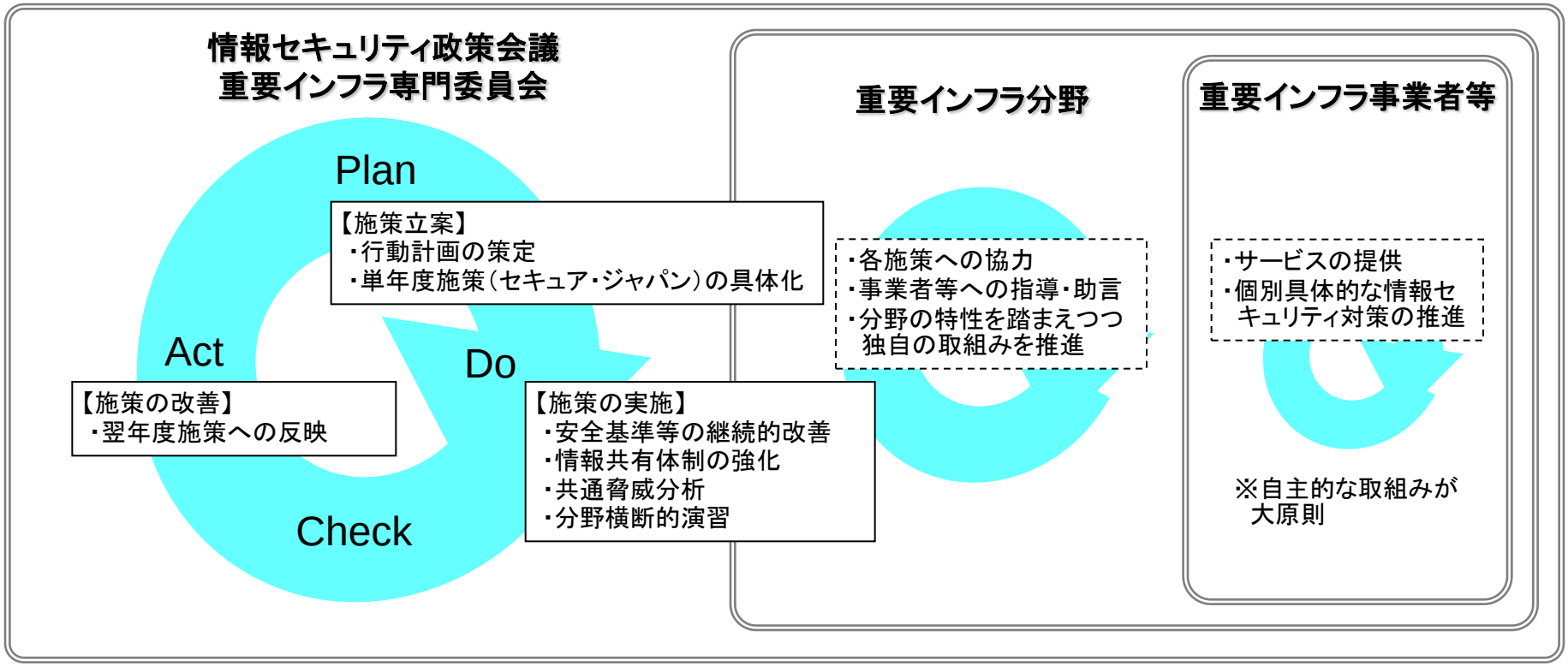
「セキュア・ジャパン２００９」に基づき、２００９年度に取り組む重点政策　連携施策

	内閣官房の取組み	重要インフラ所管省庁等の取組み
「安全基準等」の整備及び浸透	・指針の継続的改善 ・安全基準等の継続的改善状況等の把握及び検証	・安全基準等の継続的改善（重要インフラ所管省庁） ・電気通信事業における情報セキュリティマネジメントの強化（総務省） ・ネットワークのIP化に対応した電気通信システムの安全・信頼性確保（総務省）
	安全基準等の浸透（内閣官房及び重要インフラ所管省庁）	
情報共有体制の強化	・共有すべき情報の整理 ・第2次行動計画の情報連絡・情報提供に関する実施細目の見直し	・情報共有ルールの見直し（重要インフラ所管省庁） ・重要インフラで利用される情報システムの信頼性向上のための支援体制の整備（経産省）
	セプター訓練の実施（内閣官房及び重要インフラ所管省庁）	
	セプターの強化（内閣官房及び重要インフラ所管省庁）	
	・セプターカウンシルの支援	
共通脅威分析	・共通脅威分析の実施	
分野横断的演習	分野横断的演習の実施（内閣官房及び重要インフラ所管省庁）	
		・電気通信事業分野におけるサイバー攻撃への対応強化（総務省）
	情報セキュリティに関する国際会合の開催（内閣官房及び関係府省庁）	
環境変化への対応	・広報公聴活動	・重要インフラ事業者向けの啓発セミナー等の実施（経産省）
	リスクコミュニケーションの充実（内閣官房及び重要インフラ所管省庁）	
	・国際連携の推進	・ソフトウェアや情報システムの脆弱性の発生を縮減するための対策の推進（経産省） ・重要インフラ事業者に対するソフトウェア等の脆弱性関連情報の優先提供及び情報セキュリティ関連情報マネジメントの支援等（経産省） ・重要インフラ事業における制御システムの脆弱性に関する情報提供等（経産省） ・制御系システムに関する脆弱性への対応のための連携体制の構築（経産省）

評価・検証と見直し

評価・検証による継続的な改善

- 事業者、分野、政府の３層で改善サイクルを駆動
- 官民連携により、我が国全体の重要インフラにおけるPDCAサイクルを回していき、期待される社会的効果が実現しつつあるかの観点からの評価を実施
- 行動計画の見直しの際には、期待される社会的効果（アウトカム）に向けて行動計画そのものが必要十分な内容を有しているか検討を実施



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

参考情報

重要インフラに関わる主なwebサイト

- NISC
  http://www.nisc.go.jp/index.html
- 「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」
  http://www.nisc.go.jp/active/infra/pdf/infra_rt2.pdf
- 「セキュア・ジャパン２００９」
  http://www.nisc.go.jp/active/kihon/pdf/sjf_2009.pdf
- 情報セキュリティ政策会議
  http://www.nisc.go.jp/conference/seisaku/index.html
- 重要インフラ専門委員会
  http://www.nisc.go.jp/conference/seisaku/ciip/index.html

ご清聴ありがとうございました。