資料4

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次行動計画の概要及び次期行動計画の検討状況について

2013年 10月4日
重要インフラ専門委員会事務局

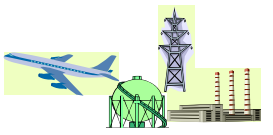
第2次重要インフラ行動計画の全体像

NISC

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など。）
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]
- 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

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年2月策定、平成24年4月改定）

（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

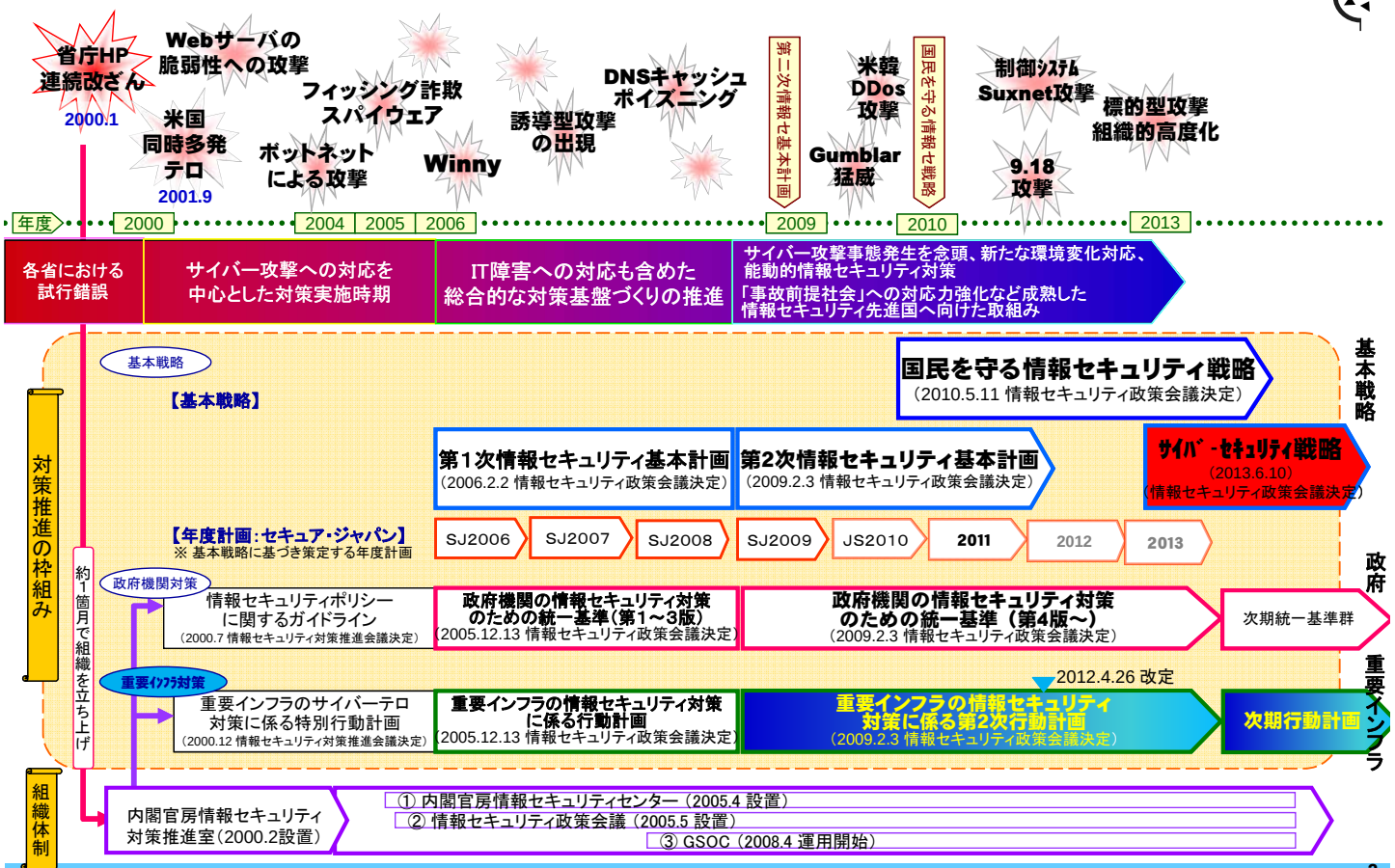
（4）分野横断的演習

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

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



サイバーセキュリティ戦略の概要(重要インフラ関連)

1. 環境の変化

サイバー空間と実空間の「融合・一体化」
► 情報通信技術の普及・高度化・利活用の進展

サイバー空間を取り巻く「リスクの深刻化」
► リスクの甚大化・拡散・グローバル化

2. 基本的な方針

(1) 目指すべき社会像:「サイバーセキュリティ立国」の実現

国家の安全保障・危機管理、社会経済の発展、国民の安全・安心確保のため、「世界を率先する」「強靭で」「活力ある」サイバー空間を構築し、サイバー攻撃等に強く、イノベーションに満ちた、世界に誇れる社会を実現

(2) 基本的な考え方

① 情報の自由な流通の確保 ► 表現の自由やプライバシーの保護等が確保され、経済成長等を享受
② 深刻化するリスクへの新たな対応 ► リスクの変化に迅速・的確に対応できる多層的な取組が必要
③ リスクベースによる対応の強化 ► 動的対応力を通じ、リスクの性質を踏まえた対応の強化が必要
④ 社会的責務を踏まえた行動と共助 ► 多種多様な主体が各々の役割を発揮し、相互連携・共助が必要

(3) 各主体の役割

① 国 ► サイバー空間の外交・防衛・犯罪対策、政府機関等における対策強化・対処態勢整備 等
② 重要インフラ事業者等 ► 現行10分野の取組強化、新たな分野における必要な対策の実施 等
(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)
③ 企業や教育・研究機関 ► 情報共有等の集団的対策、産学連携による高度技術・人材の供給 等
④ 一般利用者や中小企業 ►「他者に迷惑かけない」認識醸成やリテラシー向上など自律的取組、情報共有 等
⑤ サイバー空間関連事業者 ► 製品等の脆弱性への対応、インシデント認知・解析、国際競争力の強化 等

3. 取組分野

② 重要インフラ事業者等における対策:政府機関等における対策に準じた取組

例
- 重要インフラ事業者等とサイバー空間関連事業者との間の、攻撃情報等の情報共有を促進。
- GSOCが保有するインシデント情報等を重要インフラ事業者等と共有するための仕組みを整備。
- 重要インフラの範囲及び対応の在り方等を検討し、対策をとりまとめた新たな「行動計画」を策定。

（参考）重要インフラの定義及び対象

1　現行の定義等
　情報セキュリティ対策における「重要インフラ」は、第2次行動計画において定義。

（1）　重要インフラの定義
　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社会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　（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（平成21年2月3日制定、平成24年4月26日改定）　Ⅰ　総論　2　定義と対象範囲　より抜粋）

（2）　重要インフラ及び重要インフラ事業者の対象
　（1）を踏まえ、第2次行動計画において、「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。）」「物流」「水道」及び「医療」の10分野を防護対象と規定。
　対象となる「重要インフラ事業者等」は、上記10分野に属する事業を営む者のうち、第2次行動計画　別紙1において「対象となる事業者」に指定された者及びこれらの者から構成される団体と規定。

（3）　重要インフラサービス及び重要システム
　「重要インフラサービス」は、重要インフラ事業者等が提供するサービス及びそのサービスを利用するために必要な一連の手続きのうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野毎に規定。第2次行動計画　別紙2において、対象とした分野毎の重要インフラサービスを規定（分野によっては対象としたサービスの代表のみ例示している場合あり）。
　「重要システム」とは、重要インフラサービスを提供するために必要な情報システムのうち、重要インフラサービスに与える影響の度合いを考慮して、重要インフラ事業者毎に規定。第2次行動計画　別紙1において対象となる重要システムの例を規定。

（4）　関係主体
　重要インフラに係る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」として規定

・内閣官房
・重要インフラ所管省庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省）
・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）
・事案対処省庁（警察庁、消防庁、海上保安庁、防衛省）
・関係機関（警察庁サイバーフォース、NICT、AIST、IPA、Telecom-ISAC Japan、JPCERT/CC 等）
・重要インフラ事業者等
・セプター、セプターカウンシル等

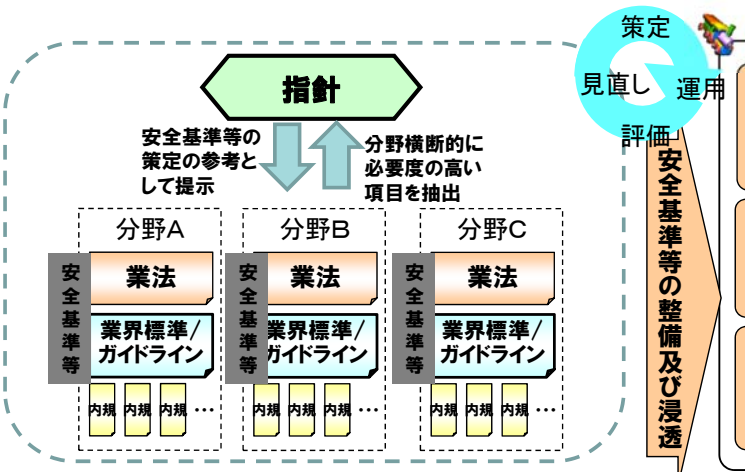
（参考）日米欧における重要インフラの定義と対象分野

	日本（10分野）	米（18分野）	英（9分野）	独（10分野）
防護対象	情報システム	物理的・仮想的なｼｽﾃﾑ・資産	設備、ｼｽﾃﾑ、施設・ﾈｯﾄﾜｰｸ	組織構造・物理構造
定義	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社会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	米国にとって非常に重要な物理的または仮想的なｼｽﾃﾑや資産であり、それらの無力化や破壊によりｾｷｭﾘﾃｨ、国家の経済安全保障、国民の公衆衛生や安全、またはそれらの組み合わせを衰えさせるような影響を与えるもの	国家の機能や国内の日常生活が依存する本質的なｻｰﾋﾞｽの提供のために不可欠な設備、ｼｽﾃﾑ、施設及びﾈｯﾄﾜｰｸ	国家の社会・経済にとって非常に重要な組織構造及び物理構造であり、その故障や劣化が持続的な供給不足、公共の安全やｾｷｭﾘﾃｨへの障害、またはその他の重大な結果をもたらすようなもの
対象分野	①　情報通信 ②　金融 ③　航空、④鉄道、⑤　物流 ⑥　電力、⑦ガス ⑧　政府・行政サービス（地方公共団体を含む。） ⑨　水道 ⑩　医療	①　通信 情報技術（IT） ②　銀行・金融 ③　④⑤輸送システム ⑥⑦　エネルギー ⑧　政府施設 ⑨　水道 ⑩　公衆衛生・医療 緊急サービス 食糧・農業 化学 商業施設 重要製品・材料製造 ダム 軍事武器基盤 国家的記念建造物等 原子力（炉、部材、廃棄物） 郵便配送	①　通信 ②　金融 ③　④⑤輸送 ⑥⑦エネルギー ⑧　政府 ⑧　水道 ⑨　保健・医療 緊急サービス 食糧	①　情報通信技術■ ②　金融・保険業□ ③　④⑤輸送■ ⑥　電力供給■ ⑧　議会・政府機関・公的機関・法執行機関□ ⑨　上下水道■ ⑩　公衆衛生・（食糧）□ 緊急・救急ｻｰﾋﾞｽ・災害対応□ メディア・文化的資産□ ■技術的ｲﾝﾌﾗ、□社会経済ｻｰﾋﾞｽｲﾝﾌﾗ

安全基準等の整備及び浸透

・ NISCが「指針」を策定し、必要度の高い情報セキュリティ対策を示す
・ 重要インフラ分野において「指針」を参考に「安全基準等」（業法、業界標準／ガイドライン、内規等）を策定

各重要インフラは、各分野における安全基準等に従ってシステムを運用
「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」
・・・重要インフラ１０分野横断的な情報セキュリティ基準を定めたもの。
「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」対策編
・・・対策の具体例を記載した項目集



第２次行動計画における取組

（１）指針の継続的改善
- **要検討事項：全分野共通の対策が望まれる事項**
- **参考事項：進んだ対策として任意で参考とする事項**

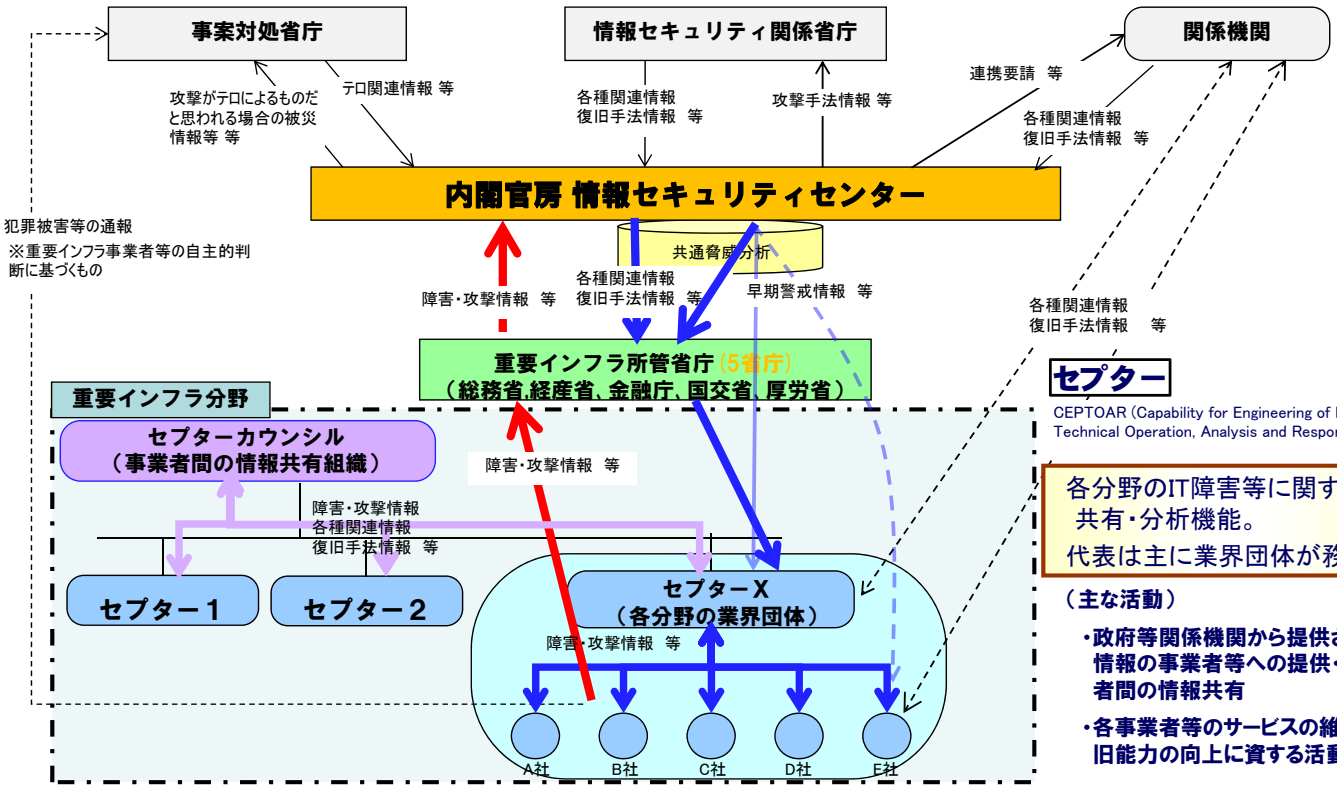
（２）安全基準等の継続的改善
- 各分野において安全基準等を見直し、PDCAサイクルを回す

（３）安全基準等の浸透
- 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、対策状況を客観的に把握

※「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」
（２０１３年２月２２日改定　情報セキュリティ政策会議決定）
※「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 対策編」
（２０１３年３月２６日改定　重要インフラ専門委員会決定）

重要インフラ分野における情報共有体制

官民の緊密な連携の下、関係主体が情報セキュリティ対策の強化に努め、重要インフラサービスの維持及びIT障害発生時の迅速な復旧等の確保に努める。



各分野のIT障害等に関する情報共有・分析機能。
代表は主に業界団体が務める。

（主な活動）
- **政府等関係機関から提供される情報の事業者等への提供・関係者間の情報共有**
- **各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**

セプター及びセプターカウンシル

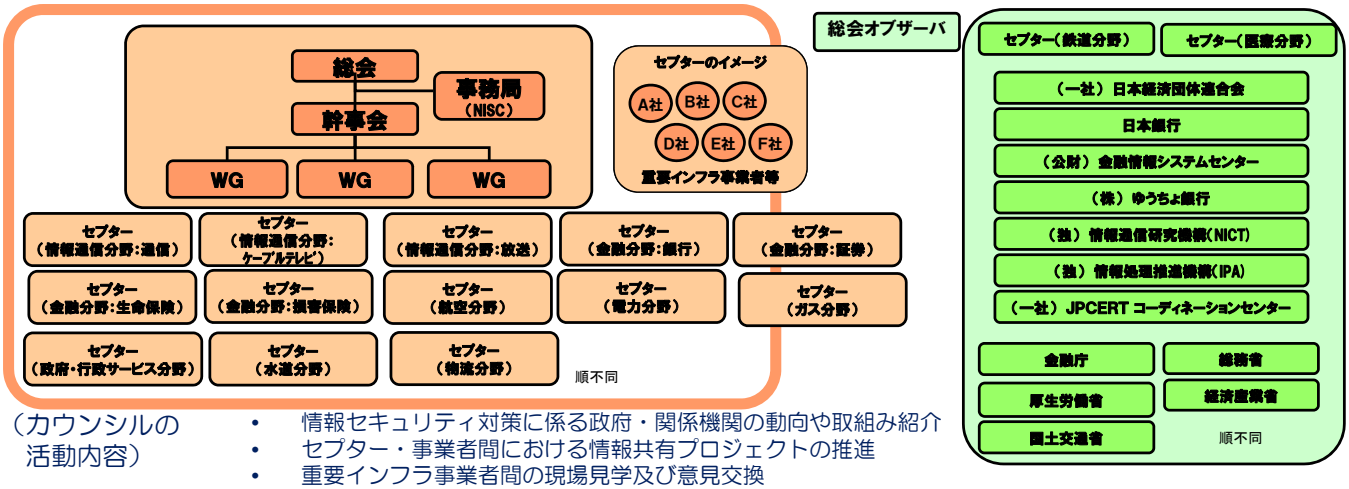
セプター（CEPTOAR：Capability for Engineering of Protection, Technical Operation, Analysis and Response）

各重要インフラ分野におけるIT障害に関して、情報共有体制を強化するための「情報共有・分析機能」。

IT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する。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

重要インフラの情報セキュリティ対策の向上を図るため、分野横断的な情報共有の推進を目的として、2009年2月に創設。
重要インフラ事業者の自主的な活動として、政府機関から独立した会議体であり、12分野（セプター）で構成 （NISCは事務局として活動を支援）



（カウンシルの活動内容）

- 情報セキュリティ対策に係る政府・関係機関の動向や取組み紹介
- セプター・事業者間における情報共有プロジェクトの推進
- 重要インフラ事業者間の現場見学及び意見交換
- 災害発生時における異業種間の互助活動　　等

重要インフラ　セプター一覧表(10分野、15セプター)

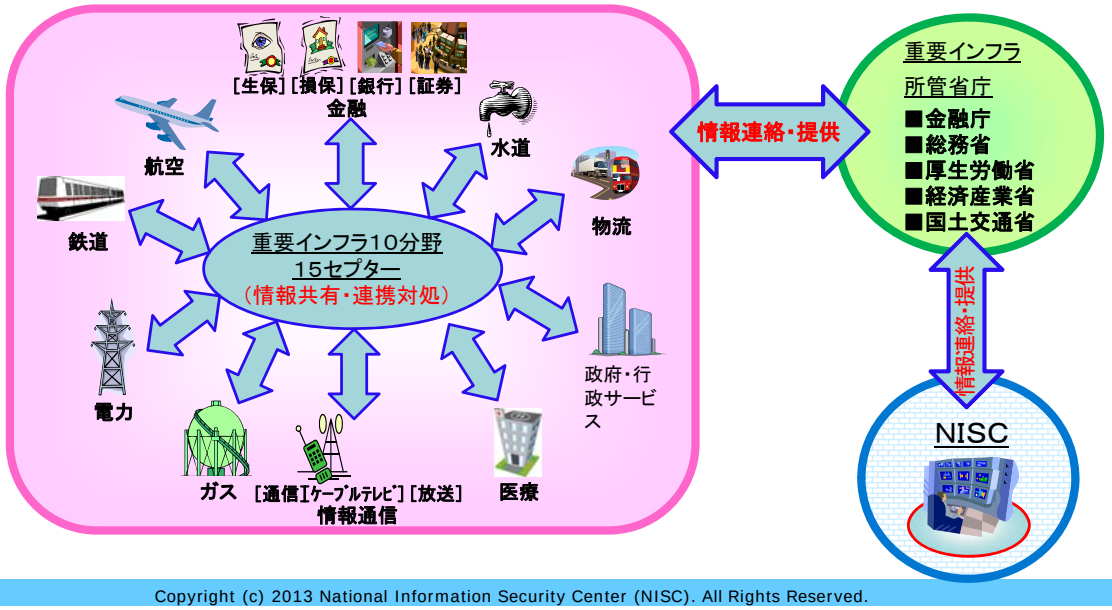
2013年3月末日現在

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
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	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CEPTAOR	電力CEPTOAR	GASCEPTOAR	自治体CEPTOAR	医療CEPTOAR	水道CEPTOAR	物流CEPTOAR
事務局	一般財団法人日本データ通信協会 テレコム・アイザック推進会議	一般社団法人日本ケーブルテレビ連盟	一般社団法人日本民間放送連盟	一般社団法人全国銀行協会事務システム部	日本証券業協会IT管理部	社団法人生命保険協会総務部コンプライアンス統括グループ	一般社団法人日本損害保険協会業務企画部共同システム開発室	国土交通省航空局 安全企画課	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	一般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	厚生労働省医政局研究開発振興課医療技術情報推進室	社団法人日本水道協会総務部総務課	一般社団法人日本物流団体連合会
構成員（内訳）	27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)	246社 (一般社団法人日本ケーブルテレビ連盟の正会員ケーブルテレビ事業者)	194社・団体 (日本放送協会、地上系民間基幹放送事業者、一般社団法人日本民間放送連盟)	1,561社 (銀行、信用金庫、信用組合、労金、商工中金、農協等)	253社 8機関 (証券会社、取引所等証券関係機関)	43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)	29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、定期航空協会及び官庁（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 (主要な一般都市ガス事業者10社)	47都道府県 1,742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）)	8水道事業体 (会員水道事業体のうち会長都市並びに地方支部長都市) [補足] 障害の内容によって、構成員を通じ、全国の日本水道協会の会員水道事業体(1,350事業体)への情報を提供。	16社6団体 (物流事業者)
緊急窓口	2007年4月より運用開始	2012年12月より運用開始	2007年4月より運用開始										2008年4月より運用開始		
情報の取扱いルール	2007年1月制定	2012年11月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2006年9月制定	2007年3月制定	2007年3月制定	2008年3月制定	2008年3月制定	2008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	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、WEB	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	脆弱性に関する情報等 メール、電話、携帯電話、FAX、電子会議室、TV会議、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

（注） 本マップは、各セプター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。

分野横断的演習

［目的］
　大規模なIT障害の要因となり得る事態に際し、重要インフラ各分野が的確に情報共有・連携し、IT障害の未然防止やIT障害に係る被害の最小化・早期復旧に関する検証を行なうことを目的とし、内閣官房情報セキュリティセンターの施策として、2006年度より継続実施（計7回）。
［参加機関］ 42組織148名（平成24年度実績）
　重要インフラ事業者等： 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、医療、水道、物流）
　セプター： 10分野の15セプター
　政府： 重要インフラ所管省庁（金融庁、総務省、厚労省、経産省、国交省）及び内閣官房情報セキュリティセンター（NISC）



分野横断的演習　～過去の実施実績～

第1次行動計画（2006～2008年度）

【目標】 官民連携の充実

＜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等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（2009～2013年度）

【目標】重要インフラ事業者におけるBCP等の実効性の確認・問題点抽出

①分野横断的な脅威に対する共通認識の醸成
②他分野の対応状況把握による自分野の対応力強化
③官民の情報共有をより効果的に運用するための方策

年度	2009年度	2010年度	2011年度	2012年度	2013年度
テーマ	広域停電	大規模通信障害	重要インフラ複合障害	重要インフラ複合障害＋便乗型ITインシデント	情報セキュリティインシデント
取組み	① シナリオ、実施方法、検証課題等を企画				
	② 早期復旧手順・事業継続計画等の検証、共有				
	③ 演習の実施方法等に関する知見の集約・蓄積				
		④ 自職場演習の導入			
			⑤ サブシナリオの導入		
			⑥ 重要インフラ分野、事業者間の連携推進		
				⑦ 第三者による助言の導入	⑦ 第三者による助言の充実

共通脅威分析

重要インフラ分野に共通に起こりうる脅威の把握と分析を実施。
あわせて、相互依存性解析（ある重要インフラ分野にIT 障害が生じた場合に他のどの重要インフラ分野に影響が波及するか）についても継続的に取り組み。

■ IT障害発生要因

〇サイバー攻撃をはじめとする意図的要因
〇非意図的要因（機器故障）
〇災害や疾病（大規模な地震）
〇他分野の障害からの波及

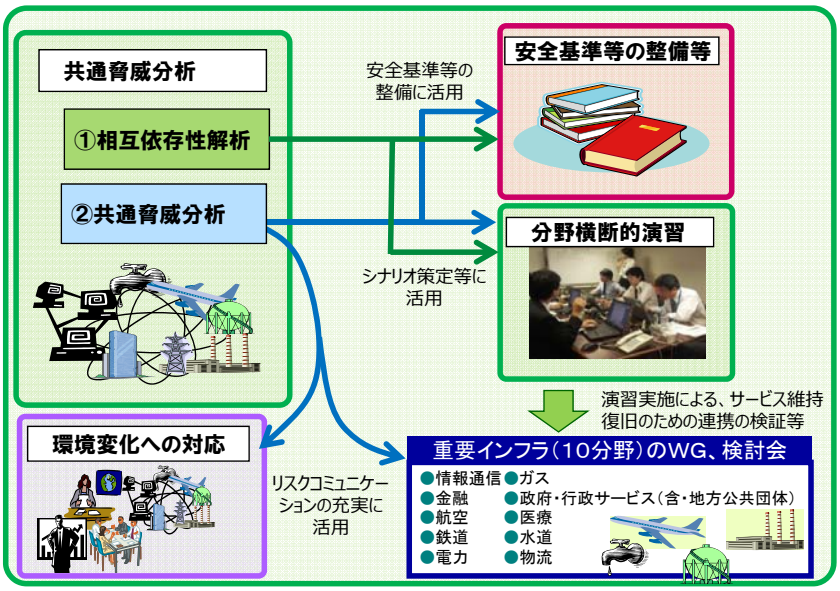
■ IT障害の定義

「 IT障害 」=「 重要システムの機能不全による
サービスの停止・低下等 」

ここで、
「 重要システム 」
＝「 重要インフラの基幹をなす重要な情報システム 」

※「重要インフラの情報セキュリティ対策に係る第2次行動計画改訂版」 別紙1の対象となる重要インフラと重要システムを参照

＜共通脅威分析結果の活用＞



共通脅威(相互依存性解析を含む)の検討と分野横断的演習は、同じWG、検討会で実施してきている。
分野委員以外に、所管省庁、関係機関(IPA,JPCERT)、有識者が参加。

共通脅威分析　～過去の実施実績～

Phase1 第1次行動計画（2006～2008年度）
相互依存性解析

Phase2 第2次行動計画（2009～2013年度）
共通脅威分析
※ 相互依存性解析を含む

国民を守る情報セキュリティ戦略
（2010～2013年度）

Step1	Step2	Step3	Step1	Step2	Step3	Step4	Step5
2006年度	2007年度	2008年度	2009年度	2010年度	2011年度	2012年度	2013年度
① 静的相互依存性解析	① 静的相互依存性解析の総括 ② 動的相互依存性解析	① データ送受信に係る相互依存性解析 ② 研究動向・IT障害事例調査 ③ 共通脅威分析に係る検討	①共通脅威の抽出 ②脅威の分類	①共通脅威の定義 ②テーマを選定して調査・分析	①テーマを選定して調査・分析	①テーマを選定して調査・分析	①環境変化調査からの新たな脅威候補の絞り込み
重要システムが他の重要システムにどのように依存しているか	IT障害時において時間経過とともに分野間の関係がどのように変化するか	ある重要インフラ分野にIT障害が生じた場合に他のどの重要インフラ分野に影響が波及するか	1) 外部からの脅威 2) システム自体が抱える脅威 3) 運用・管理体制における脅威 4) システムを取り巻く技術環境における脅威 5) 社会・制度における脅威 重要インフラ分野共通に起こりうる脅威は何か	・クラウドの範囲 ・導入に際しての脅威と対応方策 ・導入の可能性と形態について ・諸外国との比較 重要インフラ分野におけるクラウドコンピューティング利活用の現状と将来は	重要システムの堅ろう性について分析 制御システムを含む国内外のインシデント事例や研究動向等に着目して分析・評価する	重要インフラ分野における同時多発型IT障害時の復旧対応についての分析 外部依存性として特に特定のIT技術・構成要素、及びITベンダに着目して分析・評価する ★相互依存性の再調査	次期行動計画に向けての環境変化調査 短期的環境変化 ・クラウド ・スマートフォン/タブレット ・BYOD ・リモートメンテ 長期的環境変化 ・ビッグデータ ・M2M ・スマートコミュニティー

環境変化調査と共同で実施
気付きからテーマに反映
相互依存性の再確認調査
環境変化調査と共同で実施
新たな脅威候補の再調査・絞り込み

環境変化への対応

・ 広報公聴活動
行動計画そのものや計画に基づく各主体の取組みを広く公開・公表するとともにセミナー等による施策紹介の際に意見を聴取。
・ リスクコミュニケーションの充実
重要インフラの情報セキュリティを取り巻く社会環境や技術環境に伴い発生する新たな脅威やリスクを調査。
セプターカウンシルの情報共有体制や共通脅威分析の検討会体制を通じてリスクコミュニケーション（リスクに関する関係者間の共有認識のためのコミュニケーション）を実施 ⇒ リスクに関する共通理解の促進、有事の際の対策の向上等が期待
・ 国際連携活動の推進
国際会合や他国機関等との対話を通じて最新動向の把握及び情報共有を実施

＜2013年度の環境変化調査の候補＞

●設備等の実態調査
1) クラウドサービスの利用状況、及び情報セキュリティ対策
2) 情報セキュリティ人材の育成の現状
3) スマートフォン・タブレット端末における利用動向、及び情報セキュリティ
4) SOHO、在宅勤務等の利用動向、及び情報セキュリティ
5) 重要インフラシステムのリモートメンテナンス利用率について

●環境変化の調査
1) データセンターの利用動向、今後利用にあたって求められる要件等
2) 今後のIT環境の変化に伴い必要となる人材育成
3) 今後、BYODやSOHO、在宅勤務等の普及に伴って必要となる情報セキュリティ
4) 重要インフラシステムに関連する技術動向　（ネットワークの仮想化、スマートグリッド）
5) その他、重要インフラに影響を与える可能性のあるインフラの動向　（ITS、電子政府・電子自治体、マイナンバー等）
6) 今後、求められる制御システムにおける情報セキュリティ対策

・２０１３年度の候補を精査した結果、４つの調査対象を抽出

クラウド ／ スマートフォン・タブレット端末 ／ BYOD ／ リモートメンテナンス

・更に、長いスパンで将来を予見すべきテーマについても取り組むこととし、新たなIT技術革新の中から３つの調査対象を抽出

M2M ／ ビッグデータ ／ スマートコミュニティー

次期行動計画策定に当たっての基本理念

基本的な方針

戦略
① 情報の自由な流通の確保
② 深刻化するリスクへの新たな対応
③ リスクベースによる対応の強化
④ 社会的責務を踏まえた行動と共助

第２次行動計画
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

○第2次行動計画の基本的な方針を継続（一義的には事業者自らの責任で実施）

・重要インフラ事業者等
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（NISC、重要インフラ所管省庁等）
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みに対して必要な支援を行う
・取組方針
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。
（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が万全であることを確認することは困難）

考慮すべき課題と解決に当たっての方向性

課題	論点	方向性
重要インフラ事業者等における理解等のばらつき 「一義的に自らの責任で実施」の実行・意識が不十分	防護体制の成熟度の高まり 事業者等の自律性を促進しつつ、どこまでばらつきを減らすのか	・現実を見据えた実現可能な対策の推奨 ・経営層に対する一層の関与の訴求 ・参照すべき規程類の体系化、明確化 ・環境変化に対応する広報・公聴活動の一層の充実
年々深刻化する脅威に対する適切・迅速な体制・方策が不十分	一定の体制・方策を構築 （官民双方に）どのような体制・方策が更に必要になるのか	・防護対象と脅威の明確化 ・普遍的な対策・環境変化に伴う対策の分類 ・（踏み台等で）不十分な対策による責任が生じ得ることの自覚の訴求 ・リスクマネジメントの重要性の訴求
（実際に）大規模障害が生じた際の対処方法・体制の整理が不十分	平時とは異なる形で体制を構築 共有・連絡すべき情報を整理し、各主体における対応を予め定めた連携体制が必要ではないか	・事業者等にとっても特別な事態と認知できるメカニズムの構築 ・平常時の体制との変更点（追加等）を可能な限り明確化（平常時と異なる体制は非現実的）

次期行動計画策定に向けた方向性と今後の検討課題

第2次行動計画	次期行動計画における方向性（案）	要検討点
（重要インフラの範囲の見直し）	・現在、重要インフラではないが、現行10分野と同等にその機能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分野におけるシステム、サービスについての位置付けを踏まえた範囲の見直し等	・候補分野の絞り込みと参加 ・システムベンダー、セキュリティベンダー等のサイバー空間関連事業者の関係主体への追加の是非
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。 防護力向上に向け、セキュリティ対策の段階的導入等実情に即した成長モデルの提示。	・安全基準等の浸透状況の調査結果を指針・対策編に反映するプロセスを明示 ・指針による成長モデル等の訴求・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。 （範囲見直しに基づく分野・省庁の追加、リスク関係情報の共有の促進） 大規模障害発生時、平時の情報連絡・提供体制を活用しつつ、政府全体の対処態勢との連動体制を整備	・情報共有体制の全体像「別紙4」における各主体の位置付けの見直し及び各主体間の関係の再整理 ・他分野への波及防止、事例の集積による傾向の分析等に資する情報共有の在り方（脅威の類型等）の見直し ・平時の対応を念頭に置いた事案対処体制の明確化
③共通脅威分析	⑤の一部と統合して、「リスクマネジメント（仮称）」として整理。	・（リスク、脅威等の用語を再定義した上で）求められるリスク調査・分析の種類及びその結果の反映方策の明確化
④分野横断的演習	重要インフラ所管省庁の演習・訓練の全容を把握した上で、「障害対応体制の強化」として、分野横断的演習とセプター訓練を位置付け 横断的演習の成果の普及・浸透	・重要インフラ所管省庁の演習・訓練の全容の把握と連携のあり方の整理
⑤環境変化への対応	環境変化調査やリスクコミュニケーションについては、③と統合。 広報公聴活動、国際連携については、「防護基盤の強化」として整理。	・（この施策群に含まれる）広報公聴活動、国際連携の推進を含む施策の在り方の整理 ・情報セキュリティ対策に資する標準・規格の参照の在り方の整理

次期行動計画で想定される施策群の全体像

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など。）
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

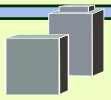
現在重要インフラと位置付けられていないが影響が既存10分野と同等程度ある（近い将来可能性が生じ得る）もの

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

（サイバー空間関連事業者を含む）

サイバーセキュリティ戦略（次期重要インフラ行動計画：現時点（未定稿））

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「指針」の策定とそれに基づく、「安全基準」等の整備・浸透の促進

情報共有体制の強化

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対応の促進

障害対応体制の強化

ｲﾝｼﾃﾞﾝﾄ発生時の官民の対応・連絡体制整備の促進と演習等の充実による対応能力の向上

ﾘｽｸﾏﾈｼﾞﾒﾝﾄ

社会経済・技術の変革等に伴い生じる変化の抽出と重要インフラに与える影響の分析を通じたリスクの管理

防護基盤の強化

国際連携、広報広聴、参照すべき規格・標準の調査、関係規程類の整備等の防護基盤の強化