重要インフラ専門委員会報告書

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

情報セキュリティ政策会議
重要インフラ専門委員会

2005 年 12 月 13 日

目次

(1) 内閣官房が取り組むべき事項
　ア　重要インフラ分野横断的な対策
　イ　体系的な情報共有体制の整備
　ウ　各主体の防護能力向上支援
　エ　内閣官房の機能強化
(2) 各重要インフラ事業者等及び重要インフラ所管省庁が取り組むべき事項
　ア　各重要インフラ事業者等及び重要インフラ所管省庁が整備・強化すべき機能
　　①　全体的な取組み
　　②　体系的な情報共有体制の整備
　イ　各重要インフラ事業者等において構築すべき体制
　ウ　重要インフラ所管省庁において構築すべき体制
(3) 情報セキュリティ関係省庁が取り組むべき事項
(4) 事案対処省庁が取り組むべき事項
(5) その他関係省庁・関係機関が取り組むべき事項
(6) 情報セキュリティ基盤の強化
　ア　専門性を持った人材の育成
　イ　成果の利用を念頭においた研究開発の推進
　ウ　地域レベルの取組みの促進
　エ　国際連携のあり方

8　行動計画の推進体制
(1) 進捗状況の評価・検証
(2) 行動計画の見直し
(3)　今後検討すべき課題

9　その他

参考資料

（参考）　重要インフラの情報セキュリティ対策に係る行動計画（情報セキュリティ政策会議決定（案））までの検討の経緯

はじめに

我が国政府が2000年末に重要インフラのサイバーテロ対策に係る初めての官民連携の枠組みとしての特別行動計画を決定したのは約5年前であった。その後、何度かのフォローアップが行われたものの、特別行動計画自体の見直しは行われてこなかった。

この間、海外では、9月11日の同時多発テロを経験した米国をはじめ、重要インフラがサイバー攻撃の標的にされる脅威は増大しているとの認識が強まっている一方、国内では、システム障害による金融サービスや航空管制の停止や大地震の発生に伴う広域的な電力、通信などの停止を経験したほか、コンピュータ・ウィルス感染による重要情報漏えいの事例が後を絶たない状況にあるなど、重要インフラ分野における情報セキュリティ対策の強化に向け、従来の取組み体制を見直す必要性が出てきたといえる。

このため、高度情報通信ネットワーク社会推進戦略本部（以下、「IT戦略本部」）は、情報セキュリティ専門調査会情報セキュリティ基本問題委員会において、昨年10月から審議を開始し、本年4月に第2次提言「重要インフラにおける情報セキュリティ対策の強化に向けて」をとりまとめ、公表した。第2次提言の直接の起草は、情報セキュリティ基本問題委員会第2分科会が担当し、有識者や重要インフラ事業者からの代表委員の方々とともに議論し、提言案のとりまとめを行った。

第2次提言の主なポイントは、国民や企業が安心して依存しうる重要インフラのセキュリティを確保する際に、情報セキュリティ対策の位置づけ自体を再認識することから出発し、重要インフラの定義や対象範囲の見直し、想定脅威範囲の拡大を行った上で、各重要インフラ間の相互依存性という新たな脆弱性にも配慮しながら、官民の連携を通じた的確な対応体制と取組み強化の方向性を提示することにあった。

その後、第2次提言は本年5月のIT戦略本部に報告、了承され、本提言の内容を受けた政府内の検討が新たに設置された情報セキュリティ政策会議の場で開始された。7月に開かれた情報セキュリティ政策会議の初回会合では、「早期に着手すべき政府統一的・横断的課題」の中で、重要インフラにおける対策の加速・強化が決定され、2000年策定の「重要インフラのサイバーテロ対策に係る特別行動計画」の改定に向けた検討を行うことが明示された。本年9月の情報セキュリティ政策会議第2回会合では、その改定方針に当たる「重要インフラの情報セキュリティ対策に係る基本的考え方」が決定され、本年末を目処に新たな行動計画としてとりまとめるべく、重要インフラ

専門委員会を設置し、行動計画の具体化を進めていくことが了承された。

これを受けて設置された重要インフラ専門委員会は、安全保障、法律、情報セキュリティ、相互依存性解析や演習・インシデントレスポンス等広範な分野の専門家に加え、新規追加分野も含めた重要インフラ10分野の各事業者の代表を集めた大組織となった。本委員会には、第2分科会メンバから当時、座長であった私も含め9名の方々に加わっていただくことになった。

12月の新たな行動計画のとりまとめを睨んで、事務局とともに諸般の事情を勘案して審議スケジュールを組んだものの、10月上旬に初回会合を皮切りに、ほぼ毎週に会合を開くという極めてハードな審議スケジュールにならざるを得なかった。有識者委員及び各事業者代表委員の諸兄並びにオブザーバとしてご出席いただいた関係府省庁の方々には、ご多忙な中、本委員会の審議に多大のご理解とご協力を頂戴したことをこの場をお借りして改めて感謝申し上げたい。

この議論を通じて当委員会メンバが痛感したことは、重要インフラの多様性と企業文化・意識改革の重要性と難しさの2点である。重要インフラの多様性については、そもそも重要インフラとされている10分野それぞれについて、基本的には「業法」と呼ばれる許認可を通じて官と民の関係が規定されているとはいえ、事業発達の歴史も産業構造も各分野によって極めて多様であり、ITや情報セキュリティとの関わりの程度についてはなおさらである。連絡体制の強化や情報セキュリティ水準の設定についても、なかなか一律に議論することには異論が続出し、調整は難航した。また、分野内情報共有の仕組み創設についても、従来の企業の枠を越えて障害や脆弱性に関する情報を共有することについての必要性に対する疑問や不安が表明された場面もあった。

確かに、国内経済（国内総生産）の約2割を占める重要インフラは、その定義にもあるように、国民生活や社会経済活動を支える「公器」としての使命と責任を担う反面、重要インフラとされている事業の9割以上は民間主体によって保有され、運用されているという実態がある。また、近年の規制緩和の流れの中で、重要インフラの安全対策は自主保安の原則に立って、一義的には各重要インフラ事業者が担うべきものとされている。欧米をはじめとする海外諸国においても、ほぼ同様の状況にあり、業界内の情報共有も含め、大部分の取組みは、法的強制力ではなく、民間側の主体的協力をベースに進められているのも事実である。今後とも、重要インフラの情報セキュリティを議論する際には、社会的責任と事業経営の論理とのバランスをどう図っていくかは長期的な課題であり続けるであろう。

本委員会の議論もこうした困難に直面しながらも、何とかとりまとめにたどり着くことが

できたのは、これからの国内の重要インフラの安全性と信頼性を確保していくためには、社会全体のＩＴへの依存が進む中で、日増しに増大していく各種脅威への対策が個々の取組みだけでは限界に達しつつあるという共通認識と、現状のまま手を拱いているわけにはいかないという関係者の危機感と使命感に支えられた面があったといっても過言ではない。官民連携を促進する上での法制度整備や人的、財政的リソースの確保等、中・長期的な取組み課題は山積するものの、先ずは実施可能なものから取組みを開始し、継続的な見直しと改善を通じて、さらに完全なものを指向していくというアプローチを採用していくことが現時点での妥当な選択であることが本委員会の基本的なコンセンサスとなっている。

本報告書では、「重要インフラの情報セキュリティ対策に係る基本的考え方」に基づき、重要インフラの定義及び対象範囲、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」、情報共有体制の強化、情報共有・分析機能、重要インフラ分野横断的な情報共有体制、相互依存性解析、分野横断的な演習及び各主体における取組みの各項目ごとに、アクションプランとしての具体化を図ることにより、今後、政府内で検討が行われる新たな行動計画の原案（事務局預け版）を提示している。年末に決定される新行動計画が今後の我が国の重要インフラの情報セキュリティの強化に向けた第一ステップとなると同時に、関係者の不断の取組みを切に期待する。

2005年　12月 13日
情報セキュリティ政策会議
重要インフラ専門委員会
委員長　浅野正一郎

委員名簿

【委員長】

浅野　正一郎　情報･システム研究機構　国立情報学研究所　教授

【委員】

石井　健睿	社団法人日本水道協会　工務部長
伊藤　友里恵	有限責任中間法人 JPCERT ｺｰﾃﾞｨﾈｰｼｮﾝｾﾝﾀｰ　経営企画室業務統括
稲垣　隆一	弁護士
岩田　隆	社団法人日本ガス協会　技術部長
大場　満	東京地下鉄株式会社　鉄道本部　安全･技術部長
雄川　一彦	日本電信電話株式会社　第二部門次世代ﾈｯﾄﾜｰｸ推進室　担当部長
金澤　亨	野村證券株式会社　コーポレートIT戦略部長
久保田　啓一	日本放送協会　技術局計画部　統括担当部長
九萬原　敏已	電気事業連合会　情報通信部長
外川　雅通	住友生命保険相互会社　情報システム部　上席調査役
郡山　信	財団法人金融情報システムセンター　監査安全部長
小西　甲	日本通運株式会社　情報システム部　管理情報システム専任部長
静　正樹	株式会社東京証券取引所　経営企画部長
神保　謙	慶應義塾大学　専任講師
田中　正史	全日本空輸株式会社　IT推進室担当部長
土居　範久	中央大学　教授
中尾　康二	KDDI 株式会社　技術開発本部　情報セキュリティ技術部長
中原　周司	あいおい損害保険株式会社　理事　システム統括部長
沼澤　勝美	日本医師会総合政策研究機構　事務管理部長
深谷　聖治	東日本旅客鉄道株式会社　総合企画本部　経営企画部　担当部長
前田　淳一	東京都総務局IT推進室　副参事(情報技術担当)
松田　栄之	新日本監査法人　公会計本部　シニアマネージャー
宮下　典久	三井住友銀行　情報システム企画部　管理グループ長
森田　元	株式会社日本航空　IT戦略企画室部長
渡辺　研司	長岡技術科学大学　経営情報系助教授

（五十音順、敬称略）

別紙1

年　月　日
情報セキュリティ政策会議決定（案）

重要インフラの情報セキュリティ対策に係る行動計画

1　目的と範囲

重要インフラの情報セキュリティ対策に係る行動計画（以下「行動計画」という。）の目的は、「重要インフラの情報セキュリティ対策に係る基本的考え方（2005年9月15日高度情報通信ネットワーク社会推進戦略本部（以下 IT 戦略本部という）情報セキュリティ政策会議決定）」を踏まえ、重要インフラの各事業において発生する障害（サービスの停止や機能の低下等）のうち IT の機能不全が引き起こすもの（以下「IT 障害」という。）から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重要インフラを防護し、重要インフラ事業者等[1]の事業継続への取組みを強化するための取ることが望ましい重要インフラ事業者等の自主的な対策について示すとともに、重要インフラ事業者等の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を図るため、内閣官房を中心とした政府及び各重要インフラ分野において実施することが望ましい施策を既存の法令、防災計画等の枠組み等との整合を図りつつ具体化することにより、官民の緊密な連携の下、重要インフラの情報セキュリティ対策を強化することにある。

なお、本行動計画に基づき、各主体がそれぞれの取組みを行うに当たっては、現在の技術の改善と協働体制の整備に関する事項に限らず、法と制度、経営、さらに取組みに携わる人材の総合的開発に関する事項にも積極的な取組みを行うこととする。

2　重要インフラの定義と対象

(1) 重要インフラの定義及び対象分野

本行動計画における「重要インフラ」とは、「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、我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」と定義する。

---

[1] 「重要インフラ事業者等」とは、「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」の各分野に属する事業を営む者のうち別紙１の「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を指す。(以下、同様。)

当面の対象分野は、「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」及び「物流」の10分野とし、それぞれの分野ごとに本行動計画に基づき対策を推進すべき重要インフラ事業者等は、国民生活や社会経済活動に与える重大な影響を考慮し、別紙1に掲げるとおりとする。

なお、「重要インフラ」の対象分野及び対象事業者等については、今後も、ITの利用の進展・拡大及びその事業環境への影響等の変化に対応して不断の見直しを行うものとする。

(2) IT障害への脅威及び各分野別重要システムの例示

本行動計画の対象とするIT障害への脅威の範囲は、情報通信ネットワークや情報システムを利用した電子的な攻撃（以下「サイバー攻撃」という。）等の意図的要因に加え、システム障害や人為的なミス、あるいはアウトソーシング等の情報技術の適用方法の変化に伴う構造的な脅威等の非意図的要因、さらには地震・津波などの災害など、以下に例示する多種多様な脅威の全てを対象とする。

ア IT障害への脅威の例示

① サイバー攻撃によるIT障害への脅威

不正侵入、データ改ざん・破壊、不正コマンド実行、ウィルス攻撃、サービス不能攻撃（DoS: Denial of Service）、情報漏えい、重要情報の搾取　等

② 非意図的要因によるIT障害への脅威

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、マネジメントの欠陥、内部不正　等

③ 災害によるIT障害への脅威

地震、水害、落雷、火災等の災害による電力供給の途絶、通信の途絶、コンピュータ施設の損壊等、重要インフラ事業者等におけるITの機能不全

イ 各分野別重要システムの例示

行動計画に定める「重要インフラの基幹をなす重要な情報システム」（以下「重要システム」という。）については、国民生活や社会経済活動に与える影響の度合いを考慮の上で、各重要インフラ分野ごとに定めることとする。

なお、具体的に対象となる重要システムの詳細については、別紙 1 に掲げる各分野別重要システムの例示を参考にしつつ、各重要インフラ事業者等において定めることとする。

3 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」

(1) 位置づけ

国民生活や社会経済活動の基盤である重要インフラにおける IT 化の進展や相互の依存関係の増大に伴い、重要インフラの IT 障害に対して、分野を越えた横断的情報セキュリティ対策を一層強化していくことが喫緊の課題となっている。この課題を早期に解決していくためには、平時から IT 障害の未然防止を視野に置きつつ、各重要インフラ分野において、当該事業分野や当該事業者等の特質を踏まえ、適切な情報セキュリティ対策が早急になされることが必要である。

しかしながら、情報セキュリティに関しては、その対策が見えにくいことから、当該対策が十分ではないため、重要インフラ事業者等自らが十分な対策をなしているのかを自己検証しつつ、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 障害から重要インフラを防護する対策を進めることが重要である。

このため、内閣官房が策定する「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」（以下「指針」という。）を踏まえて、それぞれの事業分野は、必要又は望ましい情報セキュリティ対策の水準を2006年9 月を目処に「安全基準等」に明示するよう努力する。さらに、指針については 1 年ごと、及び必要に応じて適時に、見直すこととし、「安全基準等」については、情報セキュリティを取り巻く環境の変化に応じ、随時見直しを行う。

(2) 「安全基準等」の策定若しくは見直しの実施

各重要インフラ分野において、以下の通り、「安全基準等」の策定若しくは見直しを行う。

ア 主体の決定及び体制の確立

「安全基準等」を策定若しくは見直しをする主体については、各重要インフラ分野ごとの特性に応じ、重要インフラ所管省庁、重要インフラ事業者等の調整によって決定する。

また、策定主体が複数となる場合は相互に連携し、単一あるいは階層構造の「安全基準等」を策定若しくは見直しをする体制を確立する。

イ 対象範囲の決定

保護すべき情報資産[2]や対象範囲をあらかじめ決定する。

---

[2] 情報システム及びそこに蓄積されている情報

ウ リスク分析の実施

決定した対象範囲と想定する脅威を元に、あらかじめリスク分析を行う。

エ 対策項目及び実施レベルの明示

各重要インフラ事業者等が対策を講ずる際に、どの対策をどのレベルまで実施すべきかを可能な限り「安全基準等」に客観的に明示する。その際、個々の重要インフラ事業者等における対策の水準が「安全基準等」を満たしているかを、各重要インフラ事業者等自らが各事業分野の特性等を踏まえて、適切な形で検証できるよう配慮する。

オ 既存法令等との関係

既存の事業法等、関連法令との関係を予め整理し、整合性を確保する。

カ 相互依存性、相互協力支援体制への配慮

他の重要インフラ分野との相互依存性や、分野内の他重要インフラ事業者等との相互協力支援体制、及び重要インフラ事業者等が立地する地域の政府地方支分部局、地方公共団体、地方の情報セキュリティ関係組織との連携などに配慮して対策を立案する。

4 情報共有体制の強化

重要インフラ事業者等のサービスの維持・復旧については、一義的には重要インフラ事業者等が責を担うものであるが、各重要インフラ事業者等がサービスを維持・復旧することがより容易になるよう、官民の各主体が協力することが重要である。

中でも、IT 障害に関する情報については、1) IT 障害の未然防止、2) IT 障害の拡大防止・迅速な復旧、3) IT 障害の要因等の分析・検証による再発防止の3つの側面がそれぞれにおいて重要であり、政府等は重要インフラ事業者等に対し適宜・適切に提供し、また重要インフラ事業者等間並びに相互依存性のある重要インフラ分野間においてはこれら情報を共有する体制を強化することが必要である。

IT 障害に関する情報としては以下のようなものが含まれる。

1) 未然防止・・・障害発生の脅威に係る情報（防護方策等を含む）
2) 拡大防止・復旧・・・障害発生後の影響伝搬予測及び復旧に資する情報

3) 再発防止･･･事後分析に資する情報の共同収集及び分析･検証の結果

また、IT 障害の未然防止の観点から、各重要インフラ事業者等において、何らかの障害が発生した場合に、他の IT 障害に波及するあるいは影響を及ぼす可能性がある場合は、できる限り情報共有を図るよう配慮することが重要である。

なお、このような官民の情報共有、連絡･連携のための仕組み（別紙2参照）については、その妥当性を確保するため、平時においても各主体の連携状況を分野横断的演習などを通じて模擬的に検証し、緊急時の対応力を強化していくと同時に、必要な場合には仕組みの見直しにつなげていくことが重要である。

さらに、このような情報共有体制の実現･強化（別紙3－1参照）のためには、既に各主体が有する機能を最大限活用するとともに、各主体の役割を明確化し、また特定の主体に過度の負担が発生しないよう配慮する必要がある。

(1) 官民の情報提供･連絡

ア 重要インフラ事業者等への情報提供

① 情報提供のための連携体制

内閣官房は、重要インフラ所管省庁を通じて重要インフラ事業者等に提供する情報の集約及び重要インフラ事業者等への情報提供にあたり、関係省庁、関係機関と連携する。

（ア） 情報セキュリティ関係省庁（警察庁、防衛庁、総務省、経済産業省）･事案対処省庁（警察庁、防衛庁、消防庁、海上保安庁など）･関係機関（警察庁サイバーフォース、NICT[3]、IPA[4]、Telecom-ISAC Japan[5]、JPCERT/CC[6] 等）[7]から提供される幅広い情報の集約。

（イ） 攻撃がテロによるものと思われる場合における被災情報等の事案対処省庁への提供及び攻撃手法情報等の情報セキュリティ関係省庁への提供。

---

3 独立行政法人情報通信研究機構
4 独立行政法人情報処理推進機構
5 2002 年に「インシデント情報共有・分析センター（Telecom-ISAC Japan）」として設立。2005 年 2 月に「財団法人データ通信協会」に編入。
6 有限責任中間法人 JPCERT コーディネーションセンター
7 「第 1 次提言」（2004 年 11 月 16 日　情報セキュリティ基本問題委員会：3.1.3.(1)③；脚注 4 参照）及び「情報セキュリティ問題に取り組む政府の機能・役割の見直しに向けて」（2004 年 12 月 7 日 IT 戦略本部決定；脚注 5 参照）における定義を引いたものであり、以下本行動計画内において、「関係機関」とは、「警察庁サイバーフォース」、NICT、IPA、Telecom-ISAC Japan、JPCERT/CC　等」を指す。

(ウ) 情報の集約・分析においては、必要に応じ、関係機関に連携等を要請。

(エ) 災害に関する情報については、内閣官房、内閣府及び関係省庁間の既存の情報共有体制の下で情報を集約及び共有。

② 情報の質の強化（分析情報、影響度等）

提供する情報については、以下の点を考慮しつつ、その質の強化を図る。

(ア) 情報を突き合わせることによる精度の向上

(イ) これに基づく重要度・優先度の判断

(ウ) 相互依存性解析に基づく影響予測

(エ) 他の重要インフラ分野のサービス停止・低下が原因で発生した IT 障害について、その内容、規模により、統計的な発生状況を把握

③ 情報提供の仕組み

内閣官房から重要インフラ所管省庁を通じて重要インフラ事業者等に至る情報提供の手順は以下のとおりとする。

(ア) 重要インフラ所管省庁に対する情報提供は、各省庁ごとに選任されたリエゾン（内閣官房併任）を通じて行う。なお、早期警戒情報等であって特に緊急性を有する場合には、内閣官房から直接 CEPTOAR（後述）又は個別重要インフラ事業者等へ提供するとともに、重要インフラ所管省庁のリエゾンに同報する。

(イ) その際、情報の参照者にとっての当該情報の活用を容易化することを目的に、その重要度や種類、性格等に応じた情報の分類及び取扱い範囲が一目で認識できるよう、識別方法の適正化を図ることとする。

(ウ) リエゾンは CEPTOAR(後述)を通じ、所管分野における情報共有を図る。

(エ) 早期警戒情報等については、その取扱いに注意を要することから、情報提供先と内閣官房との間で情報の取扱いに関する取り決めが合意されていることを条件とする。

④ 提供情報の範囲及び内容

情報提供は、注意喚起等、各重要インフラ事業者等の対策に資するものと

して行うものであり、情報を提供するその範囲及び事項は次のとおりとする。

（ア） 情報を提供する範囲は、当該情報に直接関係する重要インフラ事業者等（業界固有のシステムの場合には当該業界内、他の分野に関係する場合は関係するすべての分野）とする。

（イ） 政府は、情報提供にあたっては、情報連絡を行った重要インフラ事業者等が不利益を被らないよう、適切な措置を講ずる必要がある。また、提供する情報の内容は、提供目的達成のために合理的関連性を有する事項に限るものとする。

イ 重要インフラ事業者等からの情報連絡

① 情報連絡の対象となる IT 障害（別紙3－2～4参照）

情報連絡の対象となるIT障害は、次に掲げる場合であって、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして重要インフラ事業者等が連絡を要すると判断したものを含むものとする。

（ア） サイバー攻撃に起因する IT 障害の場合

1） 重要システムに重大な障害が発生した時

2） 重要システムに対するサイバー攻撃を検知した時又は攻撃の予告があった時

3） 重要システムに対するサイバー攻撃による被害を検知した時

（イ） 非意図的要因に起因する IT 障害の場合
重要システムに重大な IT 障害が発生した時

（ウ） 災害に起因する IT 障害の場合

1） 重要システムに重大な IT 障害が発生した時

2） 2 次被害により重要システムに IT 障害が発生すると考えられる時

なお、上記に該当しない場合においても、各重要インフラ事業者等の障害が他の重要インフラ事業者等の IT 障害に波及あるいは影響を及ぼす恐れがある場合など、IT 障害の未然防止、被害の拡大防止等に資すると考えられる

場合や上記に該当するかどうか不明な場合については、重要インフラ所管省庁又は内閣官房に対して相談することが望ましい。

② 連絡すべき情報

連絡すべき情報については、IT 障害発生時における利用可能な連絡手段、連絡担当者等の連絡を確保するための情報を必須とするほかは、その時点で判明している情報を随時連絡することとする。この際、全容が判明する前の断片的又は不確定なものであっても差し支えないものとする。

なお、以下に掲げる事項について、判明した範囲で随時連絡するように努めるものとする。

（ア） 対象システム

ハードウエア、ソフトウエア（システムの名称、バージョン、パッチ処理の適用状況等）

（イ） 対処状況

1） 対策の概要（システムの停止・復旧、セキュリティ改善策等）
2） 既に連絡を行った先（CEPTOAR（後述）、関係機関、事案対処省庁等）

（ウ） 他の重要インフラ事業者等に対する波及の可能性

（エ） その他

なお、上記情報連絡を行う際に必要な IT 障害に関する共通の分類及びカテゴリの設定等の実施細目については、各重要インフラ事業者等の運用性等も勘案し、内閣官房が別途定める。

③ 連絡を受けた情報の取扱い

本連絡・連携体制において連絡された情報の取扱いについて、内閣官房及び連絡を受けた重要インフラ所管省庁は、法令等に定めがある場合又は連絡を行う重要インフラ事業者等の了承がある場合を除き、原則として行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号。以下「情報公開法」という。）第 5 条第 2 号ロに規定する情報（任意提供情報）として取り扱うものとする。なお、当該情報が情報公開法第 5 条第 2 号本文但し書きに規定する情報に該当する場合には、公開されることがある。

ただし、他の重要インフラ事業者等における情報セキュリティ対策を進める

ため、内閣官房は、次の事項に該当する場合には、連絡をした重要インフラ事業者等が特定されないよう情報を加工した上で、情報提供を行うものとする。

（ア） セキュリティホール等を発見した場合や、プログラム・バグを発見した場合等であって、他の重要インフラ事業者等に同じ問題が生じるおそれがあると認められる場合

（イ） サイバー攻撃の発生又は攻撃の予告がある場合、災害による被害が予測される場合等、他の重要インフラ事業者等の重要システムが危険にさらされていると認められる場合

ウ 提供・連絡手段

内閣官房は、上記の情報提供・情報連絡に際して機密情報を取扱い可能とするための仕組みを整備する。

IT 障害発生時の連絡手段については、重要インフラ事業者等と重要インフラ所管省庁との間及び政府部内において事前に明確化することとする。この際、電話、FAX、e-mail 等、二以上の連絡手段を明示するものとする。

なお、e-mail 等インターネットを用いて機密に関する情報の連絡を行う場合には、リスク分析や費用対効果などに応じて暗号等の導入の必要性について検討することとする。

(2) 情報共有・分析機能（CEPTOAR）

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することにより、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ため、各重要インフラ分野内に「情報共有・分析機能」（CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response）の整備を進める。なお、本行動計画に掲げられた10分野の中でも、一つの分野内で業態が大きく異なる場合には、共通要素の多い重要インフラ事業者等群ごとに複数の CEPTOAR が存在することもあり得る。

ア 機能・役割

① 政府からの情報提供窓口

内閣官房から重要インフラ所管省庁を通じて情報提供を受けた際に、CEPTOAR からその関係構成員である重要インフラ事業者等に対して当該情

報を速やかに提供する。

② 関係機関等との情報共有

各重要インフラ分野の IT の利用形態に合わせた詳細な情報など、上記①の情報を補完する情報入手について、関係機関や他分野 CEPTOAR 等との間で相互に合意される場合には、その合意に基づき直接情報共有を行う。

イ CEPTOAR に求められる要件

CEPTOAR は、以下の機能を最低要件として備える必要がある。

① 内閣官房が提供する情報の取扱いに関する取極め、機密保持及び外部への情報提供に関し、構成員間で合意されたルールが存在すること。

② 緊急時に各構成員及び外部との連絡が可能な窓口（POC: Point of Contact）が設定されていること。

なお、将来的には、分野内の情報集約及び情勢判断を行う能力があるコーディネータが設置されることが望ましい。

また、分野の特性等に応じて、既存の事故情報等の情報共有体制を活用しながら効率的かつ効果的な体制を構築することにより、上記要件を付加していく方向もあり得る。

ウ CEPTOAR 整備方策

CEPTOAR整備にあたっては、各重要インフラ分野ごとの特性や事情に応じ、既存の重要インフラ事業者団体等の機能の活用や整備への支援も含め、重要インフラ所管省庁及び重要インフラ事業者等間の協議を通じ、最適な方策で具体化が行われることが望ましい。

エ 整備目標

可能な限り早期に重要インフラ所管省庁及び重要インフラ事業者等間での協議を開始し、2006年度末までに各重要インフラ分野ごとにCEPTOARが整備されることを目指すこととするが、新規追加分野については、CEPTOAR 整備に関する重要インフラ所管省庁及び重要インフラ事業者等間での基本的合意を2006年度末までに完了する(2007年度に実際の整備がなされる)ことを目指す。

オ 今後の展開の可能性

本行動計画に基づく各分野内及び分野間での情報の共有は、我が国の重要インフラの情報セキュリティ対策を強化する上での必要性についての関係者

間の共通の理解と合意に基づき推進されるものであるが、長期的には、本行動計画にいう情報共有を容易に、確実に、安心して行うという観点から、分野内で重要インフラ事業者等が情報共有するにあたって、情報公開や、機密性の保持に関する法制度の整備などについて検討していくことが望ましい。

(3) 「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）

ア 分野横断的な情報共有の場の創設

我が国全体としての重要インフラの情報セキュリティ対策をより一層強化していくためには、重要インフラ事業者等において、分野横断的な情報共有の推進を図り、多様な知見をサービスの維持・復旧に活かしていくことが重要である。このため、各 CEPTOAR 間での横断的な情報共有の場として「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）を創設する。

イ 「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の構成及び機能

「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）は、それぞれの分野に整備された CEPTOAR の代表で構成される協議会とし、各重要インフラ分野ごとのサービスの維持・復旧に係る情報のうち、複数の重要インフラ分野に共通するもの、及び分野を越えたベストプラクティス等の共有を行うものとする。

ウ 設置に向けた手順

2006年度内に整備されたCEPTOARの代表から構成される検討の場を重要インフラ所管省庁の協力を得て、内閣官房内に設置することとする。

5 相互依存性解析

従来、重要インフラにおける情報セキュリティの確保、IT 障害発生時の原因分析・復旧等は個々の分野ごとに実施されてきたところである。しかしながら各重要インフラ分野における IT 利用が進展するにつれ、重要インフラ分野相互の依存関係が増大しつつある。

このような相互依存性の高まりの中、我が国全体としての重要インフラの情報セキュリティ対策を向上させていくためには、分野横断的な状況の把握・解析が不可欠である。

このため、それぞれの重要インフラ分野に起こりうる脅威が何であるかを把握するとともに、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という相互依存性の解析が必要である。

このような相互依存性解析の結果が、重要インフラの情報セキュリティの向上に関

し、次のような効果が期待される。

① より実効性の高い事業継続計画（BCP）策定に必要な基礎資料の提供。
② 大規模災害発生時における、復旧優先順位の決定のための基礎資料の提供。
③ IT 障害の被害拡大防止のための、重要インフラ分野間の連携対処のための基盤提供。

(1) 相互依存性解析の目的

重要インフラの情報セキュリティ確保にあたっては、分野内のみを視野に入れるだけでなく、重要インフラ分野間での相互依存性の認識とレジリエンシー[8]の評価が必要である。すなわち、潜在的なリスク・チェーン（線形・非線型）の顕現化に伴う、事故・障害要因の連鎖的伝搬に対してのマネジメント（回避・コントロール・想定など）には相互依存性解析が必要である。

このため内閣官房は、重要インフラ事業者等及び重要インフラ所管省庁の協力を得つつ、相互依存性解析に関する既存の方法論を調査・評価し、依存構造のモデル化について検討した上で、重要インフラ分野横断的に相互依存性解析を実施する。

なお、この解析結果は重要インフラ事業者等の「安全基準等」策定・見直し、事業継続計画策定時の意思決定、及び重要インフラ所管省庁の政策・検査などに反映する。

(2) 相互依存性解析実施の流れ

相互依存性解析を実施し、重要インフラの情報セキュリティ確保を行っていく上で、以下の流れに基づいて基本設計を行うことが望ましい。

ア 可能な限り早期に、試行を始めて重要インフラ分野間の依存性とその脆弱性を可視化・認識する（認識：Awareness）。

イ 依存構造のモデル化や「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）などの仕組みの導入により脆弱性の検知・事前対応体制を構築する（予防：Prevention）。

ウ 重要インフラ防護体制における継続的な取組み（内外の相互依存性要因の変化に対応）として推進する（防護：Protection）。

---

[8] 耐障害性と復旧機能

エ　発生する事故･障害への緊急対応時の判断支援ツールとしても活用できるよう機能拡充を可能とする（対応：Response）。

オ　事業復旧時の業務オペレーション、システム再設計に考慮すべき相互依存性要因、影響度などのシミュレーション情報を提供する（復旧：Recovery）。

カ　分野横断的演習等を通じて、相互依存性解析を検証する（検証：Validation）。

(3) 必要情報の入手

現実的な相互依存性解析結果を得るためには、より現実に近い付与条件等の情報が不可欠である。

これら必要とされる情報の入手方法には、各重要インフラ事業者等から提供されるという形態と、内閣官房及び重要インフラ所管省庁が国内外事例、文献調査、国内外の研究者からの助言、海外政府機関等からの情報から得るという形態が考えられる。

(4) 開始時期及び実施間隔

2006年度中に試行を行い、その後、何れかの重要インフラ事業者等において基幹システムや業務プロセスなどに、大規模な更新･変更が行われた際等に必要に応じて実施する。

6 分野横断的な演習

想定される具体的な脅威シナリオの類型をもとに、毎年度テーマを設定し、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野の CEPTOAR 等の協力を得て、重要インフラ分野横断的な演習を行うこととする。

なお、2006年度においては以下の実施手順及び実施体制に従い、「研究的演習」及び「机上演習[9]」を実施し CEPTOAR の整備に資するとともに、段階的に2007年度の「機能演習[10]」(Functional Exercise)の実施を目指す。また、これらの演習を通じ、機能検証だけでなく、現行の法制度、重要インフラ事業者等の経営上の仕組み上の障害、及びそれらの観点における脅威の抽出なども研究課題としていくことを検討する。

---

9 演習参加者が１つのシナリオを元に、会議形式で課題討議を行いながら実施する演習。

10 実際の組織の指示判断系統機能を用いて模擬的に検証するための演習。

(1) 実施手順

演習概念の理解や具体課題の案出に応じた段階的実施を念頭においた計画とする。

ア 2006年度目標

① 演習実施の概念、演習課題の設定及び演習手法の理解等を主眼とした演習（「研究的演習」）を実施する。
② 類似業態単位又は重要インフラ分野横断的な共通事項単位に議論発掘のための「机上演習」を実施する。
③ 「机上演習」を通じ共通／分野ごとの想定脅威及び対処シナリオを整理する。
④ 同時に、各 CEPTOAR の整備に向けた検討に資する。

イ 2007年度目標

① 各 CEPTOAR の整備後、共通／分野ごとの演習シナリオに基づく「機能演習」を実施し、技術及び組織運営上の課題事項を検証する。
② 検証結果に基づき、重要インフラ分野横断的な共通事項の範囲を必要に応じて拡大する。

(2) 実施体制

ア 研究的演習実施体制

① 内閣官房において「研究的演習実施計画」を立案する。
② 内閣官房の監修の下、各重要インフラ分野から参加する形態で実施する。

イ 机上演習実施体制

① 内閣官房において「机上演習実施計画」を立案する。
② 内閣官房の監修の下、机上演習の仮設定課題を準備し各重要インフラ分野から参加する形態で実施する。

ウ 機能演習実施体制（2007年度）

① 内閣官房と、各重要インフラ所管省庁、各 CEPTOAR からなる「演習計画チ

ーム」を編成する。

② 演習計画チームは「機能演習実施計画[11]」を立案する。

7 各主体において取り組むべき事項と横断的施策

(1) 内閣官房が取り組むべき事項

ア 重要インフラ分野横断的な対策

内閣官房は、関係省庁の協力を得て、各重要インフラ分野に共通の分野横断的に実施すべき以下の事項を実施する。

① 脅威と障害発生のメカニズム及びその対策についての継続的調査・分析

② 災害、物理的テロ等への対応との連動体制の構築

③ 相互依存性解析の実施

④ 毎年度ごとにテーマを決めた「分野横断的演習」の企画・実施

⑤ 各重要インフラ分野ごとの「安全基準等」の策定・見直し支援

⑥ 相互依存性解析等に基づく各重要インフラ分野ごとの「安全基準等」の評価

イ 体系的な情報共有体制の整備

内閣官房は、関係省庁の協力を得て、重要インフラ防護に資する官民の体系的な情報共有体制の整備を推進する。

① テロ関係情報、脅威等に関する情報、攻撃手法及び復旧手法に関する情報等、重要インフラ事業者等に提供すべき情報の集約

② 政府から重要インフラ事業者等への情報提供体制の整備

（ア） 整理・集約した情報を、重要インフラ所管省庁を通じて、重要インフラ

11 機能演習実施計画には演習シナリオを統裁（コントロール）するための計画や、CEPTOAR／重要インフラ事業者等の参加形態等が規定される。

事業者等に対して提供する。

(イ) 相互依存性解析等による優先度設定に基づき、脆弱性情報等の提供のための枠組みを強化

(ウ) 情報の提供に当たっては、情報の受領者が当該情報を活用しやすいように、整理した上で、情報の重要度(影響度)に応じて体系立った採番の実施を検討

(エ) 情報セキュリティ関係省庁、事案対処省庁及び関係機関との連携を強化

③ IT障害発生時等緊急時における重要インフラ事業者等間の調整を行うセンター機能の創設

④ 「重要インフラ連絡協議会(CEPTOAR-Council)」(仮称)の設立支援等

ウ 各主体の防護能力向上支援

内閣官房は各主体の防護能力の向上を支援するため、以下の施策を推進する。

① 分野横断的演習等を通じた、高度な情報セキュリティ人材の育成

② 重要インフラ所管省庁の担当者を、リエゾンとして内閣官房に併任

エ 内閣官房の機能強化

上記ア～ウまでについて2006年度から本格稼働すべく、内閣官房情報セキュリティセンターは以下の施策を推進する。

① 「政府機関の事案対処支援」(IT 戦略本部決定(平成 16 年 12 月 7 日)2.③)において収集・分析した情報の活用
② 重要インフラ所管省庁におけるリエゾンとの緊密な連携等を行うべく、各重要インフラ分野ごとの担当者を設置して専門性の確保
③ 各重要インフラ分野における企業情報等をも扱うため、人的・物理的側面からもその機密の保持を確保し、信頼性の高い情報交換を行うことのできる環境の整備

(2) 各重要インフラ事業者等及び重要インフラ所管省庁が取り組むべき事項

ア　各重要インフラ事業者等及び重要インフラ所管省庁が整備･強化すべき機能

各重要インフラ事業者等及び重要インフラ所管省庁は、以下の機能の整備に取り組む。

①　全体的な取組み

各重要インフラ所管省庁は、我が国全体として重要インフラ防護を強化するために、内閣官房が行う対策と連動して、以下の取組みを行う。

（ア）　災害、物理的テロ等への対応との連動体制の構築

（イ）　内閣官房と協働し、毎年度ごとにテーマを決めた「分野横断的演習」の企画･実施

（ウ）　各重要インフラ分野ごとの「安全基準等」の策定･見直し、その支援及び評価

②　体系的な情報共有体制の整備

各重要インフラ所管省庁及び重要インフラ事業者等は、実効性のある官民の連絡･連携体制のために、内閣官房で行う対策と連動して、以下の取組みを行う。

（ア）　保有する能力･機能に応じた、重要インフラ事業者等に提供すべき情報（テロ関係情報、脅威等に関する情報、攻撃手法及び復旧手法に関する情報等）の収集

（イ）　内閣官房からの提供情報を、各 CEPTOAR を通じて、各重要インフラ事業者等に提供

（ウ）　各重要インフラ分野内の情報共有の推進（CEPTOAR の整備等）

（エ）　「想定する脅威の見直し」に対応し、重要インフラ事業者等からの IT 障害に係る連絡情報の範囲等を法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして重要インフラ事業者等が連絡を要すると判断したものに拡大

（オ）　重要インフラ所管省庁の担当者を、リエゾンとして内閣官房に併任

イ　各重要インフラ事業者等において構築すべき体制

各重要インフラ事業者等は、上記機能を迅速かつ効果的に実現するために、

以下の取組みを行う。

① 内閣官房における体制構築にあわせ、各重要インフラ分野内における情報共有推進のための体制（CEPTOAR の整備）や「安全基準等」策定・見直しのための体制を構築し、2006年度より活動を開始。

② 分野横断的な情報共有の推進（「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の設立等）についても同時並行で検討。

③ 重要インフラ所管省庁との緊密な情報共有体制の構築

ウ 重要インフラ所管省庁において構築すべき体制

各重要インフラ所管省庁は上記の機能を迅速かつ効果的に実現するために、以下の取組みを行う。

① 上記各重要インフラ分野内の情報共有推進のための体制構築（CEPTOAR の整備）や「安全基準等」策定・見直しのための支援体制構築

② 重要インフラ分野横断的な情報共有の推進（「重要インフラ連絡協議会（CEPTOAR-Council）」（仮称）の設置等）への支援体制の構築について検討

③ 重要インフラ事業者等との緊密な情報共有体制の構築

④ 重要インフラ所管省庁から重要インフラ事業者等への支援、助言等

(3) 情報セキュリティ関係省庁が取り組むべき事項

従前より情報セキュリティに関する取組みを政策的に行っている情報セキュリティ関係省庁は、内閣官房を中心とした我が国全体としての重要インフラ防護に資するために、以下の取組みを行う。

ア 保有する能力・機能に応じ、テロ関連情報、脅威等に関する情報、攻撃手法及び復旧手法に関する情報等の収集

イ 我が国としての情報の適切な収集・提供・共有を行う体制強化のための、内閣官房との連携

ウ 対処能力の向上等、情報セキュリティ関係省庁における取組みの継続的な実

施

(4) 事案対処省庁が取り組むべき事項

サイバーテロ等の事案への対処を行う事案対処省庁は、内閣官房を中心とした我が国全体としての重要インフラ防護体制に資するために、以下の取組みを行う。

ア　保有する能力・機能に応じ、テロ関係情報、脅威等に関する情報、攻撃手法及び復旧手法に関する情報等の収集

イ　我が国としての情報の適切な収集・提供・共有を行う体制強化のための、内閣官房との連携

ウ　対処能力の向上等、サイバーテロ等への対処に係る、事案対処省庁における取組みの継続的な実施

(5) その他関係省庁・関係機関が取り組むべき事項

前述の各実施主体以外においても、我が国全体としての重要インフラ防護体制の強化のため、以下の取組みを行う。

官民連携に基づく情報提供・共有体制を補完する情報の、重要インフラ事業者等や CEPTOAR への提供

(6) 情報セキュリティ基盤の強化

ア　専門性を持った人材の育成

高等教育機関（大学院等を中心）において、他分野の学生・社会人を相互に受け入れる交換枠を設けるなど、多面的能力を有する人材を育成する制度やリカレント教育のあり方を検討する。また、当該分野の人材育成を目的に含む大学院や講座の新設への積極的な支援を行う。

また、演習・訓練及びセミナー等を通じて、重要インフラ所管省庁及び重要インフラ事業者等を中心に、高度な IT スキルを有する人材の育成を図る。

イ　成果の利用を念頭においた研究開発の推進

情報セキュリティに関する研究開発・技術開発戦略の立案に際し、重要インフラにおける IT 障害の原因となりうる「IT の機能不全」への対策全体に資する視

点を付与することにより、日々進化する脅威への対応能力の強化に資する研究開発を促進する。

ウ 地域レベルの取組みの促進

関係する政府地方支分部局、地方公共団体、重要インフラ事業者等及び地方の情報セキュリティ関係組織間での情報共有及び連絡・連携の体制を、政府の体制と連動する形で平時より整備する。

エ 国際連携のあり方

政府は、OECD や G8 におけるサイバーテロ対策など情報セキュリティに関する国際的な取組みを推進する。

また、政府及び重要インフラ事業者等は、情報セキュリティに関する諸外国の情報収集に努めるほか、機密情報の取扱い等に留意しつつ、重要インフラ防護のための早期警戒・監視・警報ネットワーク等へ積極的に参加すること等により、諸外国の関係機関との情報交換や共同訓練等の国際的な連携を強化する。

8 行動計画の推進体制

(1) 進捗状況の評価・検証

本行動計画の進捗状況の評価・検証については、情報セキュリティ政策会議において毎年行う。

(2) 行動計画の見直し

本行動計画については、その進捗状況の評価・検証結果を踏まえ、3 年ごと（策定から 2 年後、進捗状況を踏まえ 12 ヶ月かけて見直す）又は必要に応じ、見直しを行う。

(3) 今後検討すべき課題

本行動計画の目的は、広く IT 障害から国民生活や社会経済活動を守ることにあり、その実現には、重要インフラ事業者等の自主的な対策や、内閣官房を中心とした政府及び各重要インフラ分野における施策を、官民の緊密な連携を通じて、政府及び民間が各々の役割に応じた責任をもって取り組んでいくことが原則である。

なお、中・長期的には、重要インフラ事業者等の独自性を確保しつつ国全体が重要インフラの情報セキュリティ対策のために様々なセクターからのリソースの投入を促進する観点から、国が情報共有のより一層の円滑化に向けた法整備など

必要な措置を講じることについても検討していく必要がある。

9 その他

本行動計画の決定に伴い、「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年12月15日 情報セキュリティ対策推進会議決定）は廃止する。

別紙 1

各重要インフラ分野において対象となる重要システム等

分野	情報システムの障害、不正な処理などの脅威・危険性	対象となる重要インフラ事業者等（注 1）	対象となる重要システム例（注 2）
情報通信	・電気通信サービスの停止 ・電気通信サービスの安全・安定供給に対する支障等 ・放送サービスの停止	・主要な電気通信事業者 ・主要な放送事業者	・ネットワークシステム ・オペレーションサポートシステム ・ニュース・番組制作システム ・編成・運行システム
金融　銀行 生命保険・損害保険 証券会社 証券取引所	・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 ・有価証券売買の停止　等	・銀行、信用金庫、信用組合、農業協同組合等 ・生命保険・損害保険・証券会社　等 ・証券取引所　等	・勘定系システム ・資金証券系システム ・国際系システム ・対外接続系システム ・保険業務システム ・証券取引システム ・取引所システム　等 （オープンネットワークを利用したサービスを含む。）
航空	・運航の遅延、欠航 ・航空機の安全運航に対する支障等	・主たる定期航空運送事業者 ・国土交通省（航空管制・気象）	・運航システム ・予約・搭乗システム ・整備システム ・貨物システム ・航空管制システム ・気象情報システム
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	・JR 各社及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
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	・一般電気事業者、日本原子力発電（株）及び電源開発（株）	・制御システム ・運転監視システム
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	・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
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	・各府省庁 ・地方公共団体	・各府省庁及び地方公共団体の情報システム（電子政府・電子自治体への対応）
医療	・診療支援部門における業務への支障等	・医療機関	・電子カルテ管理システム ・遠隔医療システム
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	・水道事業者及び水道用水供給事業者（ただし、小規模なものを除く。）	・水道施設や水道水の監視システム ・水道施設の制御システム等
物流	・輸送の遅延・停止	・大手物流事業者	・集配管理システム

	・貨物の所在追跡困難		・貨物追跡システム ・倉庫管理システム

注 1　ここに掲げている対象事業者は、重点的に対策を実施すべき重要インフラ事業者等であり、今後、事業環境の変化及び IT への依存度の進展等を踏まえ、対象とする事業の見直しを行うこととする。
注 2　対象となる重要システムの詳細については、脅威・危険性や例を踏まえ、重要インフラ事業者等において定める。

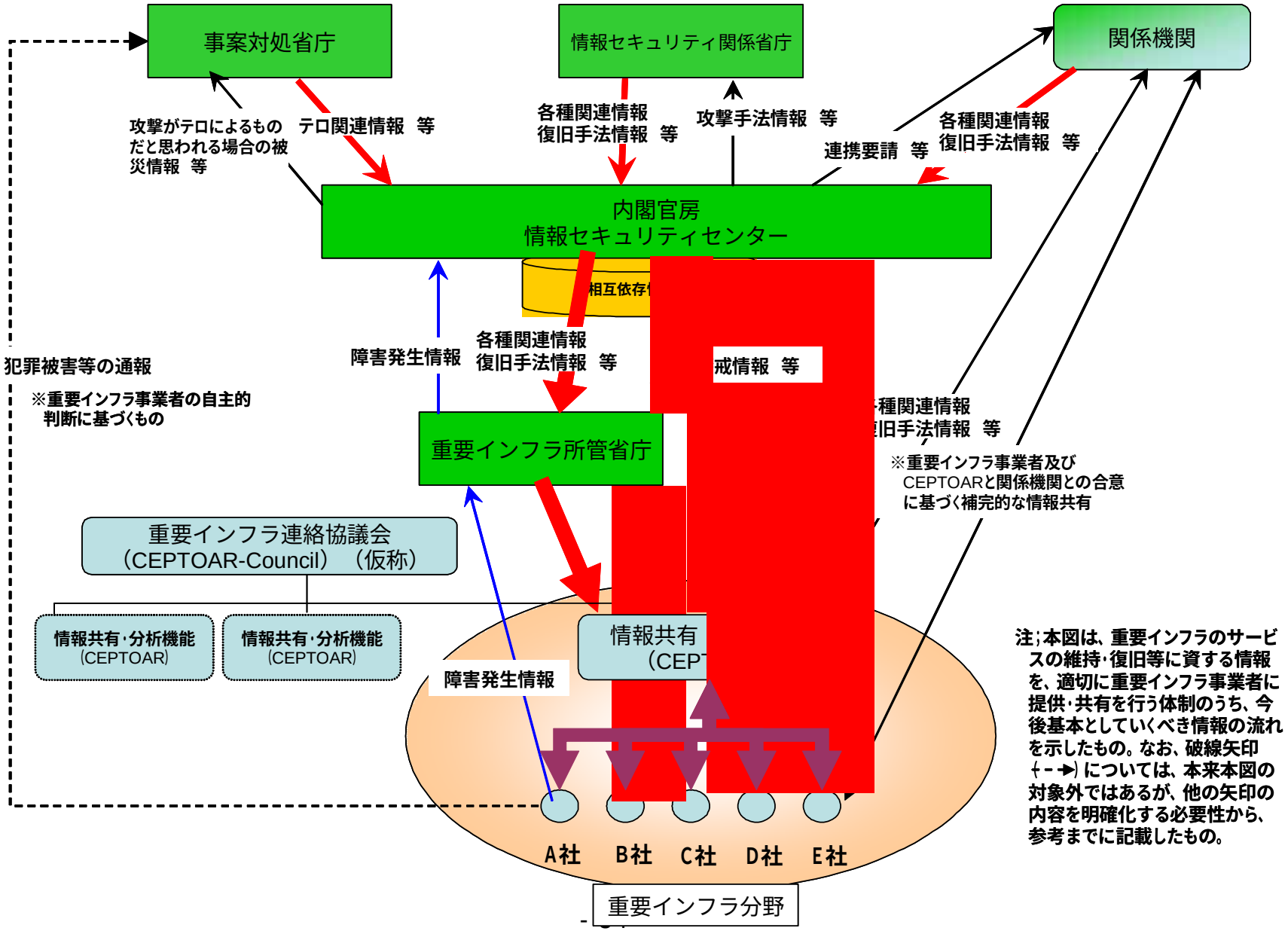
別紙 2

IT 障害発生時における連絡体制等

分野		既存の連絡体制	IT 障害発生時における緊急時の連絡体制	情報セキュリティ関連情報の共有各分野におけるセキュリティ対策等の検討体制
情報通信		(1) 重要インフラ事業者等→政府 ・電気通信事業法に基づく、業務の停止等の総務大臣への報告 ・災害対策基本法に基づく、災害応急対策における電気通信設備の被害状況等報告 ・放送中止事故、重要無線通信妨害等の総務省への連絡 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・ウィルス発生等緊急情報を業界内及び総務省との間で通報・共有	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・既存の連絡体制を活用して実施	・ウィルス発生等の情報共有体制を活用して実施
金融	銀行 生命保険・損害保険 証券会社 証券取引所	(1) 重要インフラ事業者等→政府 ・業法に基づく、サービス遅延・停止等の内閣総理大臣（金融庁）への報告 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・事業者団体を通じて実施	・全国銀行協会、（財）金融情報システムセンター（FISC）等の事業者団体を通じて実施
航空		(1) 重要インフラ事業者等→政府 ・航空法に基づく、航空機の事故等に関する国土交通大臣への報告 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・IT障害に関する連絡窓口を設置 ・航空保安体制の不具合に関する情報を関係機関で共有（空港単位）	(1) 重要インフラ事業者等→政府 ・事故時は既存の事故報告体制により実施。 ・事故に至らないIT障害に関しては、IT障害の連絡体制により実施。 (2) 政府→重要インフラ事業者等 ・連絡窓口を通じて重要インフラ事業者等へ直接連絡	
鉄道		(1) 重要インフラ事業者等→政府、政府→重要インフラ事業者等 ・鉄道事故等報告規則に基づく、鉄道運転事故等に関する国土交通大臣への報告 ・IT障害に関する連絡体制を整備 (2) 重要インフラ事業者等間 ・特になし	(1) 重要インフラ事業者等→政府、政府→重要インフラ事業者等 ・事故時は既存の事故報告体制により実施。	
電力		(1) 重要インフラ事業者等→政府 ・防災業務計画、電気関係報告規則に基づく、発電所事故等に関する経済産業大臣への連絡 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・特になし	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・事業者団体を通じて実施	・事業者団体を通じて実施

ガス	(1) 重要インフラ事業者等→政府 ・ガス事業法施行規則に基づく、一定規模のガス供給支障等の経済産業大臣への報告 (2) 政府→重要インフラ事業者等、重要インフラ事業者等間 ・災害によりガス供給支障が発生した場合等における、ガス協会「救援措置要綱」に基づく業界内連絡	(1) 重要インフラ事業者等→政府 ・既存の連絡体制を活用して実施 (2) 政府→重要インフラ事業者等 ・事業者団体を通じて実施	・業界内の委員会等を通じて実施
政府・行政サービス	(1) 各府省庁→内閣官房 ・「政府機関の情報システムに関する緊急時の連絡等について」に基づく連絡 (2) 内閣官房→各府省庁 ・「政府機関の情報システムに関する緊急時の連絡等について」に基づく情報提供 (3) 地方公共団体→政府 ・「地方公共団体の情報システムに係る緊急時の連絡等について」に基づく情報提供 (4) 政府→地方公共団体 ・「地方公共団体の情報システムに係る緊急時の連絡等について」に基づく情報提供	(1) 各府省庁→内閣官房、内閣官房→各府省庁 ・政府部内連絡体制で実施 (2) 地方公共団体→政府、政府→地方公共団体 ・既存の連絡体制を活用性して実施	・政府部内連絡体制で実施
医療	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等	
水道	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等	(1) 重要インフラ事業者等→政府等 (2) 政府等→重要インフラ事業者等	
物流	(1) 重要インフラ事業者等→政府 ・貨物自動車運送事業法、貨物利用運送事業法、倉庫業法に基づく、車両重大事故、貨物重大事故、倉庫火災等の国土交通大臣への報告 (2) 政府→重要インフラ事業者等 ・内閣府　災害対策基本法に定める指定公共機関	(1) 重要インフラ事業者等→政府 (2) 政府→重要インフラ事業者等	・事業者団体を通じて実施

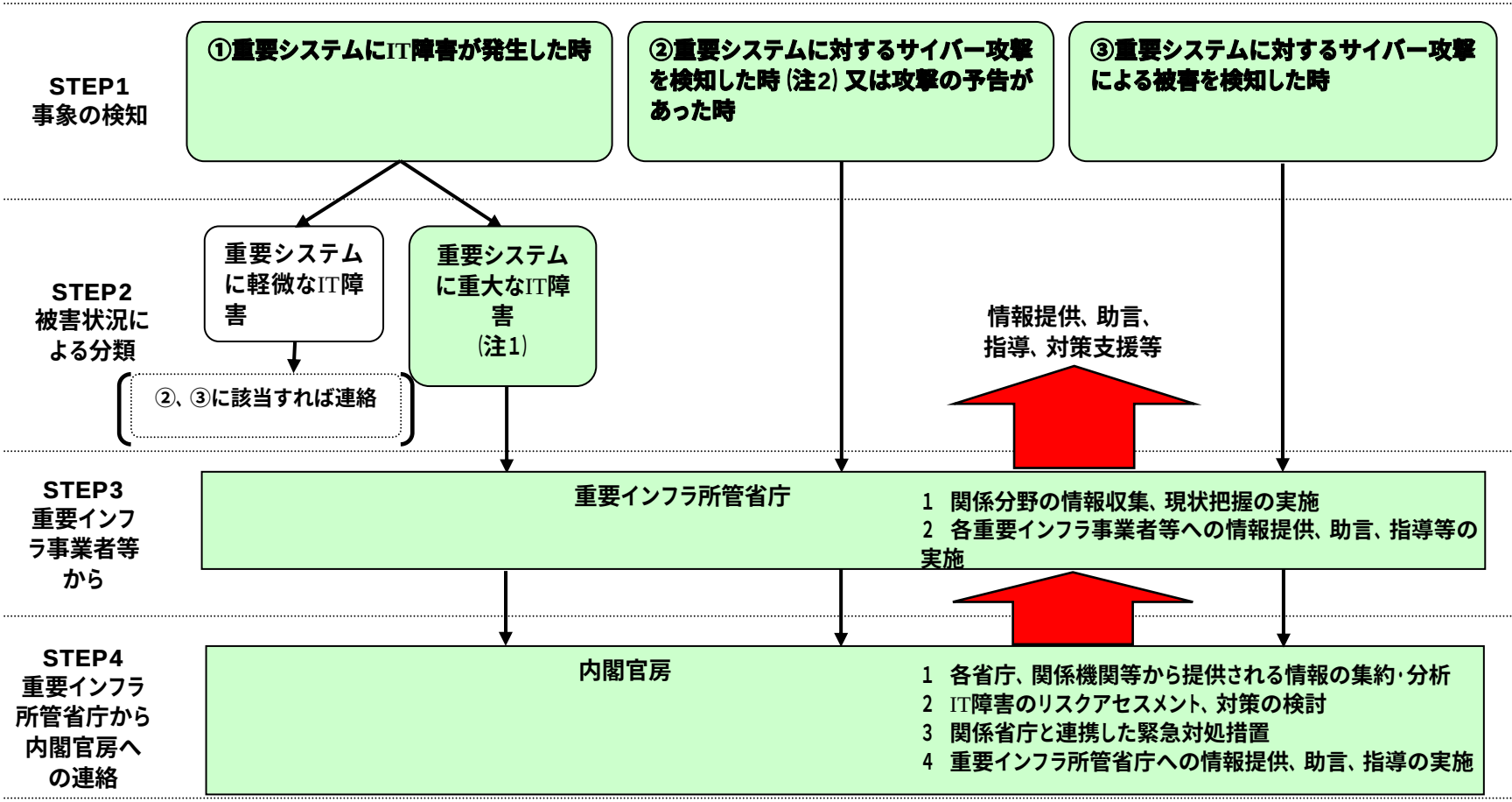
別紙 3-1



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、破線矢印（- - ▶）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。

別紙3-2

情報連絡の対象となるIT障害（サイバー攻撃の場合）

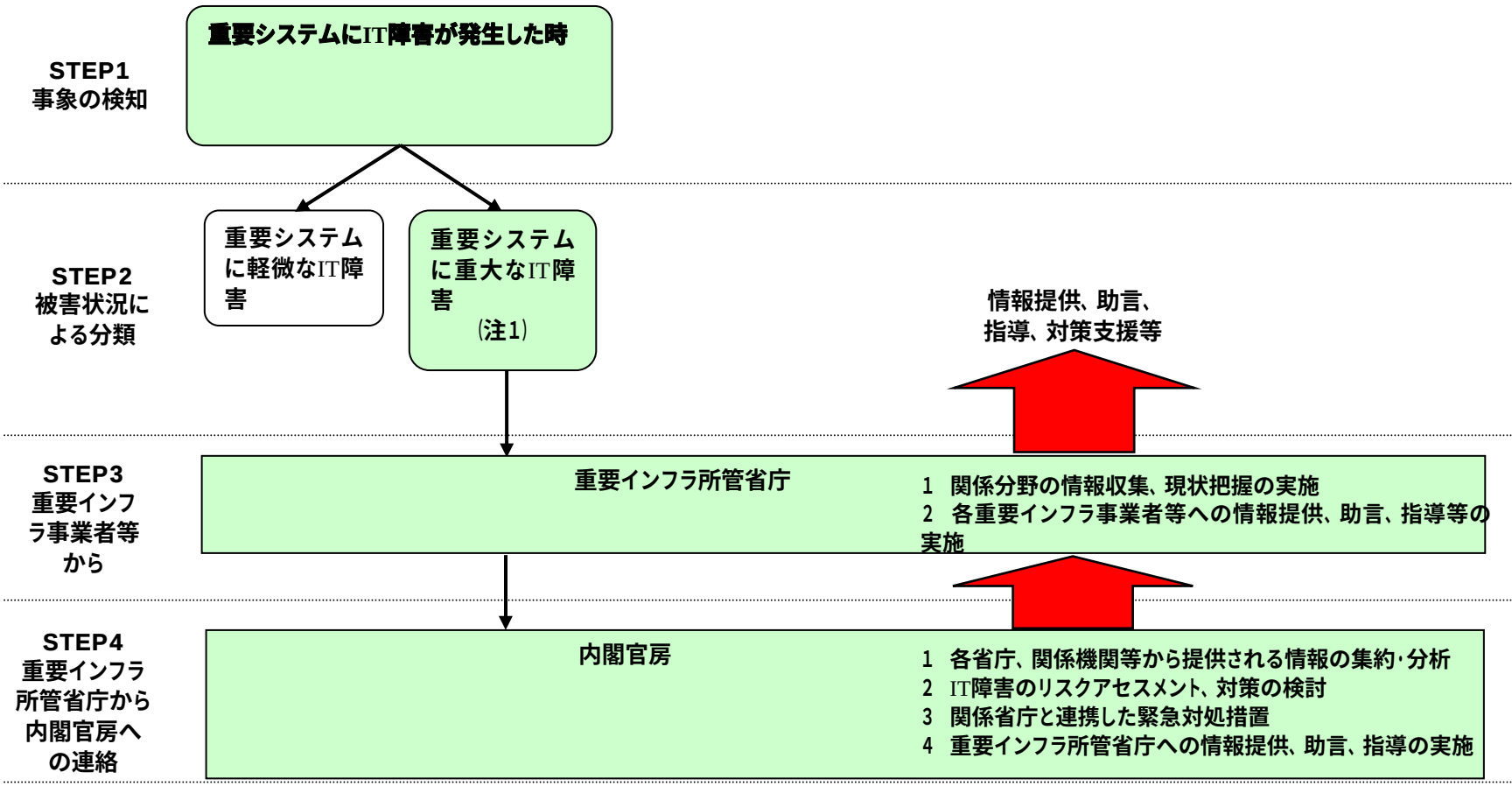


（注1） 「重大なIT障害」とは、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして重要インフラ事業者等が連絡を要すると判断したものを含む。

（注2） 「サイバー攻撃を検知した時」については、「被害は発生していないが、そのおそれが高い攻撃を検知した場合」に限ることとする（別紙4参照）。

別紙3-3

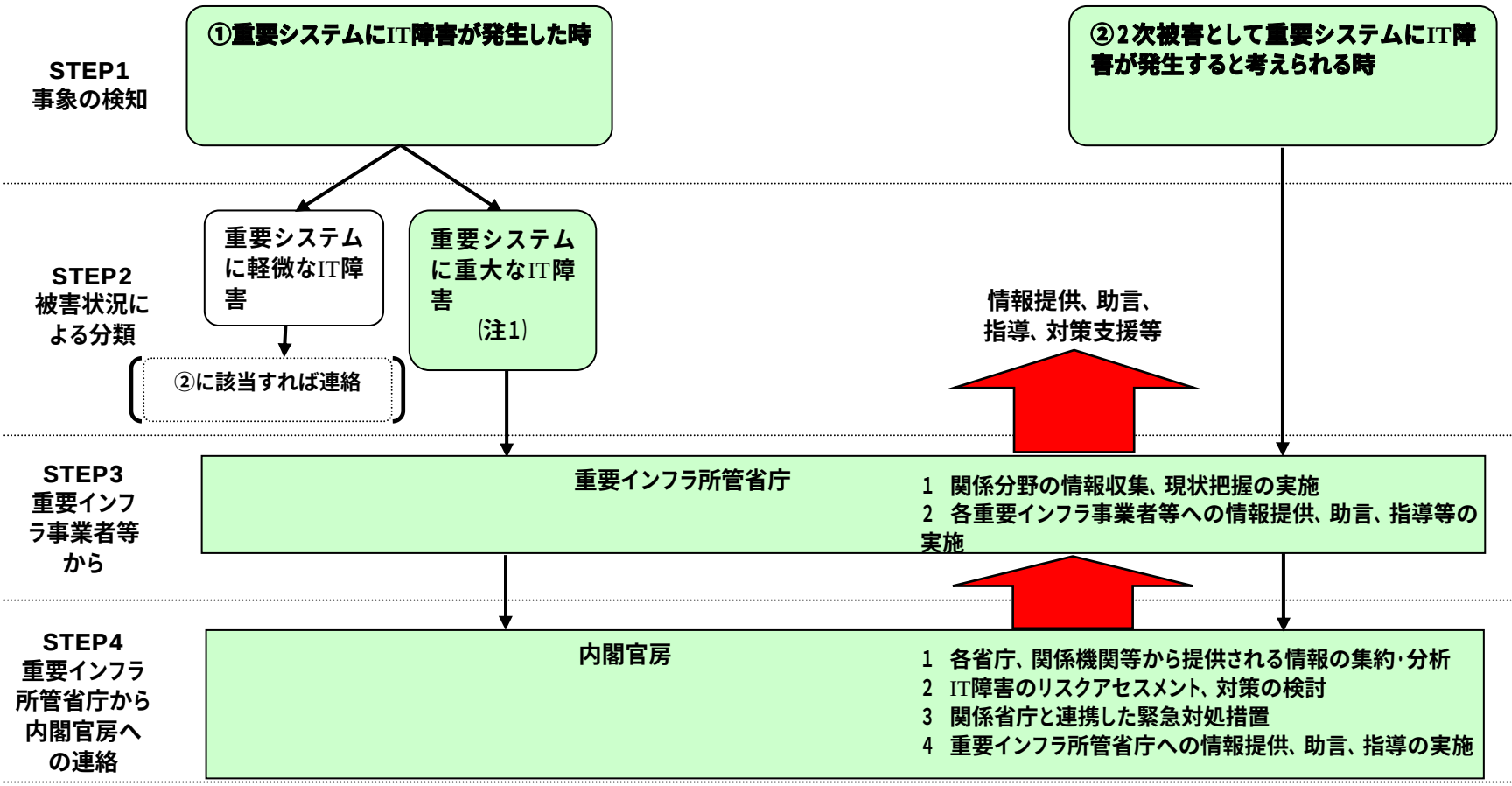
情報連絡の対象となるIT障害（非意図的要因の場合）



（注1） 「重大なIT障害」とは、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして重要インフラ事業者等が連絡を要すると判断したものを含む。

別紙3-4

情報連絡の対象となるIT障害（災害の場合）



（注1） 「重大なIT障害」とは、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして重要インフラ事業者等が連絡を要すると判断したものを含む。

参考資料

警察庁サイバーフォースの情報セキュリティ関連業務と保有情報等

業務	概要	保有情報	その他
インターネット上での事象の把握	・サイバーフォースセンター等においてインターネット上での事象等の監視を行い、攻撃手法の発見、関係各機関への情報提供などを行う。	・ネットワークトラフィックの分析情報 ・ボットネットに関する情報　等	・@police（警察庁情報セキュリティポータルサイト）にて、定点観測情報を公表
産業界等との連携	・重要インフラ事業者等への個別訪問、セミナーや訓練の実施、重要インフラ事業者等の要請に応じて行われる脆弱性試験等を通じて、適切な情報セキュリティ対策について助言を行う。	・脆弱性情報　等	
国際的な法執行機関間の連携	・国際的な法執行機関間の情報の共有のための基盤構築と運営を行う。	・左記から得られるセキュリティ関連情報　等	
サイバーテロ及びサイバー犯罪への対応	・サイバー犯罪及びサイバーテロに対し都道府県警と連携して対応する。	・各種対応等を通じて得られたセキュリティ関連情報 ・脆弱性情報　等	・関係する資料（ログ等）の解析等
研究開発等	・サイバーテロ対策技術の向上を目指し、産学官連携による共同研究・開発を通じて、警察庁がこれまでに蓄積した情報セキュリティ技術と民間の有する情報セキュリティ技術の融合を図る。	・脆弱性評価技術 ・防御技術 ・ログ保存技術　等	

NICTの情報セキュリティ関連業務と保有情報等

業務	概要	保有情報	その他
インシデント分析業務支援 （Telecom-ISAC Japanと連携）	・高度分析センターによる、インシデント分析処理のための基盤システムの構築支援　等	・インシデントの統計分析情報（比率分析、閾値学習分析等）	・インシデントログはTelecom-ISAC Japanより提供。
暗号アルゴリズムの安全性評価等	・電子政府推奨暗号リストにおける暗号アルゴリズムの安全性評価等	・暗号アルゴリズムに関する国内外の最新動向	・IPAと連携して実施。
被災者安否情報登録検索システムの研究開発	・災害時において被災者の安否情報を登録・検索するIAAシステムに関する研究開発	・被災者安否情報登録検索の統計分析情報	
情報セキュリティに係る各種研究開発等	・安全・安心な通信路・通信網、情報通信危機管理基盤技術に関する研究等	・担当研究分野に係る最新動向	

IPAの情報セキュリティ関連業務と保有情報等

業務	概要	保有情報	その他
ウィルス対策	・一般利用者、組織からウイルス検出・被害の届出を受け、その件数、概要、具体的な対策を公表 ・被害時の対処等の相談の受付対応実施 ・ウイルス対策ソフトに障害が発生した場合の対外情報発信	ウイルス関連情報 ・届出集計データ ・相談事例データ ・ウイルス解析データ（検体含む）	・IPAのウェブページにて、注意喚起及び統計情報（月次、及び4半期）を公表 ・ウイルス対策ソフトに係る対外情報発信のために、国内大手ウイルス対策ソフトベンダーとのネットワークを構築
不正アクセス対策	・一般利用者、組織から不正アクセスの検出・被害の届出を受け、その件数、概要、具体的な対策を毎月公表 ・被害時の対処等の相談の受付対応、等	不正アクセス関連情報 ・届出集計データ ・相談事例データ、等	・IPAのウェブページにて、注意喚起及び統計情報（月次、4半期）を公表
ソフトウエアの脆弱性対策	・ソフトウェアの脆弱性に関する届出の受付、分析・再現検証、JPCERT/CCへの連絡等 ・統計情報、注意喚起、啓発資料を作成・公表	・未公開の国内脆弱性関連情報（JPCERT/CCと共有）	・IPAのウェブページにて、脆弱性解説資料（図解資料）及び統計情報（4半期毎）を公表 ・JVNホームページについては、JPCERT/CCと共同運営
ウェブアプリケーション/ウェブサイトの脆弱性対策	・発見者からの届出をウェブサイト運営者に連絡し、確認・修正を依頼。サイト運営者の希望により修正の確認も実施 ・統計情報、注意喚起情報、啓発資料の公表	・脆弱性の存在する／したURL ・脆弱性の詳細、等	・IPAのウェブページにて、統計情報（4半期毎）を公表 ・注意喚起については、IPAウェブページに掲載するほか、関連団体へも連絡
情報セキュリティに係る各種調査研究等	・電子政府推奨暗号リストにおける暗号アルゴリズムの安全性評価等 ・情報セキュリティ面でのIT製品・システムの安全性評価・認証制度の運営 ・韓国KISA、独フラウンホファSIT等との共同研究の実施、等	・暗号アルゴリズムに関する国内外の最新動向 ・安全性の高いIT製品に関する国内外の最新動向、等	・暗号アルゴリズムの安全性評価等については、NICTと連携して実施

Telecom-ISAC Japanの情報セキュリティ関連業務と保有情報等

業務	概要	保有情報	その他
インシデント情報収集・分析・提供	・国内ISP事業者が連携しIPS運用に深刻な影響を与えるDDoS攻撃の実態調査ならびに、この事象が発生した際に国内ISP事業者が連携して行う緊急避難的連携手順を構築し、深刻なDDoS攻撃を検知した際に手順を適用している。 ・ IPS運用にとり当面の脅威となるボットネットに対する国内の実態本格調査を行うため、国内ISP事業者が調査用設備の構築・運用で連携し、ボットネットがインターネット運用に与える影響の測定や技術的対策等の検討を、セキュリティベンダー、アンチウイルスソフト業者等にも呼びかけ異業種横断的な連携で行う。 ・実際の運用を円滑にするため、オペレーションセンターを構築・運用。	・トラフィック情報 ・インシデント情報 ・上記情報に関する分析情報、等	・収集したインシデント情報の傾向分析、頻度分析、影響度分析等より高度な分析を実施する分析センターの他、それらの真偽度の確認のためのテストベット（試験環境）を構築中。 ・国内ISP事業者と連携し、トラフィック情報、インシデント情報等の広域収集を実施する広域モニターシステムを構築中。 ・申請を受けたインシデント情報の分析結果を提供するインシデントハンドリングシステムを構築中。
マルウェア対策	・ワーム、ボットネット等のインターネット通信に多大な影響 を及ぼすマルウェア対策 ・国内ISP事業者横断にAbuse部門の連携を体制構築。上記活動の成果であるマルウエア対策の一斉同時通知や自社以外で管理するネットワークからの不正行為抑止情報を交換。	・ウィルス、ワーム、ボットなどに関する情報	・平成16年度、JPCERT/CCと共同でボットに関する調査を実施。 ・マイクロソフト社との協力強化（Telecom-ISACより同社に対してワーム「Antinny」の駆除を要請、今月12日より駆除機能が提供開始。）
外部機関との連携・協調	・JPCERT/CC、他国Telecom-ISACとの連携を図り、情報交換・共有などの連携共同作業を実施。	・JPCERT/CC、他国Telecom-ISACからの情報、等	・海外から国内サイトに対するDoS攻撃などのトラフィック増加などに対し、JPCERT/CCと連携して対応。
技術フォーラム、セミナーの開催	・技術フォーラムを通じ、テレコム企業間の技術・情報共有を実施。 ・Telecom-ISACへの要求条件を整理、検討。	・テレコム企業における技術情報	

JPCERT/CC の情報セキュリティ関連業務と保有情報等

業務	概要	保有情報	その他
インシデント・レスポンス	・インシデント情報の受付、対応 ・国内からのインシデント情報をもとにした海外CSIRT (Computer Security Incident Response Team)等への連携依頼や、海外CSIRT等からのインシデント情報をもとにした国内ISP事業者等への協力依頼等	・サーバやネットワークへの不審なアクセス情報（DoS攻撃、HP改ざん、不正アクセスなど） ・フィッシング情報、等	・FIRST(世界180のCSIRTがメンバー)、APCERT(アジア大洋州13地域17組織のCSIRT参加)のネットワークや米国CERT/CC・英国NISCCといった海外CSIRT等との密接なネットワークを保有 ・海外からのネットワークトラフィックの増加（DoS攻撃など）に対し、Telecom ISAC等と連携して対応 ・国内外関係機関との連携により、フィッシングサイトの閉鎖コーディネーション等を実施
脆弱性情報流通	・未公開のソフトウェア脆弱性情報について国内ITベンダ(100以上)、海外ベンダとコーディネーションを行い、修正ソフトを公表 ・JVNホームページにおいて、国内ITベンダの脆弱性対応状況の他、CERT/CCやNISCC等が公表する脆弱性関連情報も公開	・未公開のソフトウェア脆弱性関連情報 ・最新の公開済みソフトウェア脆弱性情報、対策情報等 ・国内ベンダの対応窓口(POC)情報等	・脆弱性関連情報には、IPAに報告された未公開のものの他、米国CERT/CCや英国NISCCから提供された未公開のもの、インターネット上の公開情報から収集したもの等も含まれる ・米国CERT/CC、英国NISCC等との連携により、海外ベンダとのコーディネーションも実施。(例：銀行・証券会社で利用されている韓国系ソフトの脆弱性を修正、等) ・平成16年度、Telecom-ISACと共同でボットに関する調査を実施
定点観測	・インターネット上の観測情報を収集：JPCERT/CC自身が保有する ISDAS システムの他、SOC (Security Operation Center)事業者が連携した IMAS や、ヨーロッパ eCSIRT.net による定点観測システムに関与	・ISDASが収集する情報 ・IMAS、eCSIRT.net にて観測、保有している情報、等	・ISDASで収集したスキャン(探索)情報については、JPCERT/CCのウェブサイト上でグラフにより公表 ・IMAS、eCSIRT.net の情報についての対外提供は限定的
早期警戒	・上記3つの業務において入手した国内外情報のうち、早期警戒が必要であると判断されたものにつき、個別限定的に提供	・上記3事業の情報 ・その他海外からの入手情報	・提供に際しては、対策情報を確認し、かつ、守秘が確保されることが前提 ・その他、サイバーセキュリティ演習の企画

重要インフラにおける情報共有の現状

	情報共有体制	情報共有に係る主な関連業界団体	その他
電力	既存の事故情報等の情報共有体制を活用する。	電気事業連合会（電事連）	・電事連において「電力におけるサイバーテロ対策危機管理ガイドライン」を策定した。
ガス	既存の事故情報等の情報共有体制を活用する。	日本ガス協会	・日本ガス協会において「製造・供給に係わる制御系システムの情報セキュリティ対策」を策定した。
情報通信	既存の事故情報等の情報共有体制を活用する。また、情報セキュリティ事案に特化した情報共有体制である。Telecom-ISAC Japanにて、ウィルス情報等の情報共有を実施している。	Telecom ISAC Japan 電気通信事業者協会	・Telecom ISACは、研究開発にも積極的に取り組んでいる。 ・「情報通信ネットワーク安全・信頼性基準」（総務省）の中で「危機管理計画策定のための指針」を規定している。
金融	情報システムやオンラインネットワークの情報セキュリティに関して確立された既存の連絡体制を活用する。	金融情報システムセンター 全国銀行協会	・金融庁および日銀の検査にて、銀行の情報システムが対象となっている。
航空	航空機事故情報等の共有体制は存在するが、情報セキュリティ事案に特化した情報共有体制はない。		・国土交通省と事業者間で、情報システムに関する事案発生時には、個別に連絡体制を構築している。
鉄道	鉄道事故情報等の共有体制は存在するが、情報セキュリティ事案に特化した情報共有体制はない。		・国土交通省と事業者間で、情報セキュリティに関する緊急事案発生時の対応体制を構築することとしている。
政府・自治体	内閣官房において緊急対応支援チーム(NIRT)を編成する。警察庁においてサイバーフォースを設置する。自治体の総合行政ネットワークについては、既存の行政連絡体制を活用する。	地方自治情報センター（LASDEC）	

米国におけるISACの一覧 -1

重要インフラISAC	範囲	資金モデル	対象	分析能力	共有メカニズム
金融 Financial Services ISAC (1999/10設立)	銀行、証券会社、保険会社を含む200メンバが参加、金融セクタの90%の資産をカバーする	・何段階かのメンバーシップフィーにより運営 ・契約会社であるMITREが実際の運用を行う	サイバー 物理	週7日24時間運営 業界のニーズに基づき、監視デスクが脅威、インシデント、警告の分析・分類を実施	・告知システムを用いたテキストベースのアラートに加え、電話によるバックアップ ・隔週でDHS及びSAICと諜報情報に関する電話会議
化学・危険物 Chemical ISAC (2002/4設立)	化学業界の538メンバが参加、うち企業が285社で、化学業界の90%をカバー.	米国化学協会(ACC)のChemical Transportation Emergency Centerが資金提供及び運営を担当	サイバー 物理	週7日24時間運営. 分析センターの立ち上げ準備中	・電子メールによるアラート、警告. ・Chemistry ISAC Webサイト ・DHSセキュア通信ネットワークを用いたDHSとの隔週電話会議
緊急サービス Emergency Management & Response ISAC (2000/10設立)	FEMAリージョンのうち10領域、EMRセクタの6の主要な組織が参加し、重要なEMRセクタの100%をカバー	・FEMAのOffice of Cyber Securityが資金提供、USFAからも一部資金を受ける ・運用は外注	サイバー 物理	週7日24時間運営試行中 脅威、攻撃、脆弱性、アノマリー、セキュリティベストプラクティスに関する分析と啓発	・電子メッセージング ・電話と必要な場合は秘話電話装置を利用
エネルギー Electric ISAC (ES-ISAC) (2000/10設立)	NERCメンバの90%以上がISACメンバに参加、大規模から小規模の電力配電会社と、地域電力配電会社、電力取引会社(パワーマーケッター)が加入	NERCが資金提供、管理、運営を実施	サイバー 物理	週7日24時間運営. ES-ISACとNERCは、電力インフラに影響を及ぼす運用上の事故やサイバーインシデントの報告のガイドラインを提供するIndications, Analysis, and Warnings Program (IAW) を開発	・秘話電話、FAX、ウェブサーバ、電子メール、衛星電話 ・事故報告、警告、脆弱性分析、関連文書に係る情報を一般公開しているWebに掲載
エネルギー Energy ISAC (2001/11設立)	石油とガス業界から80強のメンバが参加、同業界の85%程度をカバー	・エネルギー省（DOE）が資金提供 ・運営が外注	サイバー 物理	週7日24時間運営 脅威、脆弱性、インシデントの分析の実施 セキュリティ情報と対策の提供	・電話会議、FAX、電子メール、ポケットベル ・セキュアなウェブサイトにより、詳細な警告情報をメンバだけに提供

米国におけるISACの一覧 -2

重要インフラISAC	範囲	資金モデル	対象	分析能力	共有メカニズム
食品 Food ISAC (2002/2設立)	食品業界の業界団体及びそのメンバ、40団体以上が加盟	・資金提供無し ・ボランティアが運営、人材はメンバ団体が提供	物理	週7日24時間運営 分析能力無し、DHSの分析に依存	・電子メール、Watch Commander List ・セキュア電子メールシステムを構築中
政府 State Gov. ISAC (2003/1設立)	カンザス州を除49州およびコロンビア特別区	ニューヨーク州が資金提供及び運用、必要に応じて適切なリソースを提供	サイバー 物理及び自然災害	週7日24時間運営. 掲示板、アドバイザリ、アラートなどを発行	・月次電話会議、電子メール、電話
情報技術・通信 IT-ISAC (2000/12設立)	デスクトップOSの90%、データベースの85%、デスクトップコンピュータの50%、ルータの85%、ソフトウェアセキュリティの65%をカバー	・資金提供および運営は創設メンバ、資金面ではメンバーシップ料も貢献 ・実運営は外注	サイバー 物理	週7日24時間運営. サイバーアラートとアドバイザリの分析と、物理的な問題に関する報告	CWIN、暗号化電子メール、SSLウェブサイト、携帯電話、VoIP電話、GETS7優先通話システム
情報技術・通信 Telecom ISAC (2000/1設立)	回線プロバイダの95%、回線ベンダの60%以上、携帯プロバイダの95%、携帯ベンダの90%、インターネットサービス加入者の42%、インターネットサービスネットワークの90%、システムインテグレータの連邦政府IT市場上位6社、DNS[1]ルートの15%、グローバルトップレベルドメイン運営者.	・資金提供はDHS NCS ・運営はNCC ・基本的には政府機関の職員により運営	サイバー 物理及び自然災害	週7日24時間運営. 電話通信網に影響を与える危機を回避するためのデータ分析	電子メール、電話、FAX、会議、CWIN
情報技術・通信 Research & Education Networking ISAC (2003/2設立)	200大学が加盟、国の研究教育用ネットワークに接続する全大学とカレッジは基本メンバーシップを持つ	資金提供及び運営はインディアナ大学	サイバー	週7日24時間運営 高等教育機関に対する、ネットワークセキュリティ関連の脆弱性と脅威に関する情報の受信と配布	・公開情報なネットワークに関する集約された情報のみに限定 ・特定の組織や個人が特定できる情報は一般に報告せず ・詳細且つセンシティブな情報は影響を受ける機関の中でのみ共有

[1] DNS: Domain Name Service インターネットの名前解決を行うサービスで、そのうち最上位となるDNSルートサーバは世界に13箇所設置

米国におけるISACの一覧 -3

重要インフラISAC	範囲	資金モデル	対象	分析能力	共有メカニズム
運輸 Public Transit ISAC (2002/1設立)	約100の主要な運輸関連組織が加盟	・連邦政府が資金提供 ・運営は外注	サイバー 物理	週7日24時間運営. セキュリティ情報の収集、分析、配布	・電子メール、セキュア電子メール、公開Webサイト ・HSOC[1]、運輸省（DOT）、TSA[2]のオペレーションセンターへのリンク
運輸 Surface Transportation ISAC (2002/5設立)	北米の主要な貨物輸送事業者の95%と、Amtrakが加盟	・資金はメンバーシップ料によるが、Federal Transit Administration (FTA)からの資金提供も受けている ・運営は外注	サイバー 物理及び自然災害	週7日24時間運営試行中. 警告、脅威情報、アドバイザリを業界とコールセンターを通じて運転者に伝える複数のチャネル	Highway ISACのWebサイト、高速道路監視センター、FAX、電子メール、印刷物、黄色信号
飲料水・浄水 Water ISAC (2002/12設立)	275-300の小-大規模の配水組織が加盟、セキュアポータルを持つ45%をカバー、電子メールアラートを受信する事業者の85%をカバー	・資金はメンバーシップ料によるが、EPAからの資金提供を受けている ・運営は外注、AMWA[3]からの支援を受けている	サイバー 物理	週7日24時間運営. 本セクタに潜在的な脅威となりうる脅威とインシデント情報の分析	暗号化電子メール、セキュアポータル、セキュア掲示板、チャットルーム
その他 Real Estate ISAC (2003/4設立)	ホテル、不動産仲買、ショッピングセンター等、10の業界団体が加盟	・業界団体が資金提供 ・運営は外注	物理	週7日24時間運営. 脅威分析はDHSに依存	双方向通信ネットワークとウェブサイト、必要に応じて経営陣による電話会議
農業　N.A.	-	-	-	-	-
防衛産業 N.A.	-	-	-	-	-
郵便・運送 N.A.	-	-	-	-	-
公衆衛生・健康 N.A.	-	-	-	-	-

[1] HSOC: Homeland Security Operations Center
[2] TSA: Transportation Security Administration
[3] AMWA: Association of Metropolitan Water Agencies

米国におけるISAC運用実態例

	対象・メンバ	組織	費用	備考
IT-ISAC	・IT業界（SW,HW,サービス） ・ITAA[1]が主導 ・25社	・非営利の民間団体 ・ISSが運営を担当 ・ITAAが勧誘など	・年50千ドルの有料会員と無料会員から構成	・メンバ間の情報交換は、一旦ISSに情報を集約後、匿名化してから共有する ・影響が大きい脆弱性などに関してはIT-ISACにとどまらず、ITAAを通じて広報を行う
ESISAC	・電力業界を対象（発電,送電,etc.） ・地理的には米加を100%カバー	・NERC[2]に設置 ・5名のスタッフ	・ISACメンバーシップは無料、費用はNERCが負担	・概ねボランタリーに運営されている ・これまで500件以上のインシデントをDHSに自主的に報告(内約90%は物理インシデント)
Telecom ISAC	・DHS NCS ・32社が加盟 （ネットワークプロバイダ、機器ベンダ、ソフトウェアベンダ等）	・NCSが運営 ・独自のスタッフ ・民間企業GD (General Dynamics) から情報を購入	・政府が費用を負担	・メンバの一部は政府のセキュリティクリアランスを保持（機密情報を受け取ることができる）
FS-ISAC	・金融業界を対象（銀行,保険,証券） ・90%をカバー（99%が目標） ・ボードメンバ12社、一般100社以上	・民間企業SAICが事務局、サイバーアナリシスなども実施	・年750ドル、10千ドルの有料会員と無料会員から構成	・機微情報は政府には提供していない ・各社は法律で政府に対する報告義務を負う(DHSに対する報告義務は無い)

[1] ITAA: Information Technology Association Of America 米国情報技術協会
[2] NERC: North American Electric Reliability Council北米電力信頼度協議会

(参考) 重要インフラの情報セキュリティ対策に係る行動計画 (情報セキュリティ政策会議決定 (案)) までの検討の経緯

【情報セキュリティ政策会議】

平成 17 年 9 月 15 日　第 2 回会合

「重要インフラの情報セキュリティ対策に係る基本的考え方」の決定

【重要医インフラ専門委員会】

平成 17 年 10 月 11 日　第 1 回会合

(1) 重要インフラ専門委員会の設置について
(2) 会議の公開等について
(3) 重要インフラの情報セキュリティ対策に係る基本的考え方について
(4) 重要インフラ専門委員会 開催スケジュール について
(5) 「重要インフラの情報セキュリティ対策に係る行動計画 (案) 」各論点について個別討議

平成 17 年 10 月 17 日　第 2 回会合

「重要インフラの情報セキュリティ対策に係る行動計画 (案) 」各論点について個別討議

平成 17 年 10 月 24 日　第 3 回会合

「重要インフラの情報セキュリティ対策に係る行動計画 (案) 」各論点について個別討議

平成 17 年 11 月 1 日　第 4 回会合

「重要インフラの情報セキュリティ対策に係る行動計画 (案) 」について

平成 17 年 11 月 8 日　第 5 回会合

「重要インフラの情報セキュリティ対策に係る行動計画 (案) 」について