重要インフラの情報セキュリティ対策に係る
第２次行動計画の施策の成果と課題について

平 成 ２ ５ 年 １ １ 月 ２ ９ 日

重 要 イ ン フ ラ 専 門 委 員 会

目次

I. 総論

1. 概要

「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（2009年２月、2012年４月改定)」（以下「第２次行動計画」という。）は、「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)」及び「重要インフラの情報セキュリティ対策に係る行動計画（2005年12月)」（以下「第１次行動計画」という。）に続く、我が国の重要インフラの情報セキュリティ対策として位置付けられたものであり、2009年度以降、当該行動計画に沿った施策の推進が図られてきた。

本資料は、今般、第２次行動計画の期末を迎えるに当たり、諸施策の実施状況を点検し、成果と課題をとりまとめたものである。

2. 第２次行動計画の施策の成果と課題（概要）

第２次行動計画は、次の５つの施策群から構成されている。

１．安全基準等の整備及び浸透
２．情報共有体制の強化
３．共通脅威分析
４．分野横断的演習
５．環境変化への対応

以下に、各施策の成果と課題の概要を記載する。

2.1 成果

今回、これら施策群の評価を行うに際し、第２次行動計画は2009年時点での重要インフラを取り巻く最新知見を踏まえて策定されたものであることを考慮した。各施策に係る詳細については次章（II.各施策の成果と課題）にて示すが、第２次行動計画における所期の目標については一定の成果を挙げたと評価できるものであった。

安全基準等の整備及び浸透については、情報セキュリティ対策に取り組む関係主体が自らなすべき必要な対策を理解し、各々が必要な取組を定期的な自己検証の下で行うことを目指した結果、指針と安全基準等の一体的・安定的な見直しサイクルを確立し、情報セキュリティ対策の啓発推進等を強化した。

情報共有体制の強化については、刻々と変化する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及び複雑・巧妙化するサイバー攻撃等に対応することを目的に、官民連携による情報連絡・情報提供の枠組みの構築・確立及び当該枠組みの運用の安定化、各セプター・セプター間における情報共有体制の整備及び重要インフラ事業

者等における必要情報の享受・活用を実現した。

共通脅威分析については、重要インフラ全体の防護能力の維持・強化に不可欠である分野横断的な状況の把握・分析に基づく共通脅威分析の検討を行った結果、重要インフラ事業者等における事業継続計画策定等に資する基礎資料を提供し、分析結果の一部を指針に反映した。

分野横断的演習については、ＩＴ障害発生に備えた全分野を網羅する官民各主体参加の模擬的な演習を通じて相互の連絡・連携における仕組みの検証機会の提供に取り組んだ結果、演習参加組織数・人数は増加傾向にあり、演習で得られた知見に基づく重要インフラ事業者等のＩＴ障害時の早期復旧手順及び事業継続計画等の検証を通じた情報セキュリティ対策に貢献した。

環境変化への対応のうち広報公聴活動については、重要インフラの情報セキュリティ施策の結果資料、重要インフラ専門委員会の会議資料等を内閣官房のWebサイトに掲載し、公表するとともに、情報セキュリティ政策に係る講演等を行った。リスクコミュニケーションの充実については、情報セキュリティに係る関係機関との意見交換会の開催、セプターカウンシルにおける相互理解ＷＧの開催を行った。国際連携の推進については、メリディアン会合、サイバーストーム演習への参加等を通じて諸外国との連携を行った。こうした取組を通じて、環境変化に伴う脅威の察知能力の向上に努めた。

2.2 課題

各施策の実施を通じて、社会・技術面での環境変化を踏まえた改善・補強を要する課題も抽出された。詳細については次章（II.各施策の成果と課題）にて示すが、各施策の主たる課題を以下に記載する。

安全基準等の整備及び浸透においては、情報セキュリティ対策は重要インフラ事業者等自身のみならず重要インフラ全体の防護能力の維持・強化にも効力が及ぶこと、重要インフラ事業者等から対策の実情を踏まえた段階的な（優先順位付けされた）指針の提示要望があること等から、各重要インフラ事業者等の情報セキュリティ対策に資することを目的に、重要インフラ事業者等のPDCAサイクルとの整合に基づく見直しを課題とする。

情報共有体制の強化においては、実効性のある情報共有体制の構築を目的に、分野間における情報共有頻度の格差の解消、「脅威の類型」の細分化、大規模ＩＴ障害対応時の情報共有体制について、平時の体制の延長線上への構築、新たな関係主体との連携の在り方の整理等を課題とする。

共通脅威分析においては、共通脅威分析の対象・位置付けや実施頻度の見直しに向けて、調査対象を全分野の共通脅威に限定せず、全分野に及ばずとも影響が大きな脅威を

調査対象に加える運営に係る検討や、効果性を高めるため、時間的経過や環境変化の顕在化に応じた脅威等の詳細分析等を課題とする。

分野横断的演習においては、区々である各組織のＩＴ利用形態や情報管理態勢から演習環境の設定に限界があり、大幅な参加者拡大が望めない。このことから、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課題抽出機会の提供を目的に、演習成果の更なる普及・浸透を、参加者拡大のみに依存せず、重要インフラ分野全体に図ることを課題とする。また、演習評価に基づく運営の質的改善、重要インフラのＩＴ障害発生時の対応を踏まえた関係主体の在り方の検討、並びに重要インフラ所管省庁及び防災関係省庁が主催する演習・訓練との連携についての検討を課題とする。

環境変化への対応のうち広報公聴活動においては、次期行動計画における本施策と他施策との整合の下、目的と情報開示範囲に応じた広報公聴活動の見直しを課題とする。リスクコミュニケーションの充実においては、国際標準と整合したリスクマネジメントの定義、機微情報の秘匿と情報の有用性のバランスを念頭に置いた情報共有の見直し、及び中長期的な実現・利用と脅威の影響の大きさが予想される新たなＩＴ技術等を対象にした環境変化のテーマに係る中長期的な継続調査・検討を課題とする。国際連携の推進においては、国境を越えて形成されたサイバー空間において深刻化・グローバル化するリスクへの迅速な対応に向けて、諸外国との連携推進を継続するとともに、ASEAN等のアジア太平洋地域や欧米等の二国間、多国間、地域的枠組みの積極的な活用を通じた国際連携の強化を課題とする。

II. 各施策の成果と課題

1. 安全基準等の整備及び浸透

第２次行動計画における本施策の期待される成果並びに成果検証の指標の考え方及び具体的な指標は次のとおりである。

- 「安全基準等の整備及び浸透」に期待される成果は、重要インフラ事業者等における各種の対策の更なる充実と、その着実な実践である。
- そのため、指針と安全基準等の項目の充実と、個別事業者等の安全基準等に基づいた取組みの確実な実施に着目した指標を設定する。
- 具体的な指標は、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とする。

1.1 実施状況

情報セキュリティ対策に取り組む関係主体が、自らなすべき必要な対策を理解し、各々が必要な取組を定期的な自己検証の下で行うことを目指し、安全基準等の整備及び浸透に取り組んだ。

具体的には、内閣官房はサイバー攻撃の高度化等の環境変化、東日本大震災にて生じた複合的システム障害やデータ滅失等への対応にて得た教訓等を踏まえ、「指針の継続的改善」として2010年度及び2012年度に指針本編の改定及び対策編の新設・改定を行った。

加えて、「安全基準等の継続的改善」として重要インフラ所管省庁による同改善状況を、「安全基準等の浸透」として重要インフラ事業者等による情報セキュリティの対策状況を年度ごとに調査・報告を行った。

1.2 成果

指針において、対策項目を「要検討事項」と「参考事項」に分類し、335項目の具体例を採録した。また、浸透状況等の調査によると、調査対象の約50%の重要インフラ事業者等が定期的な自己検証を、約70%が自己検証を行っているとの結果を得た。

このことから、指針と安全基準等の一体的・安定的な見直しサイクルを確立するとともに、情報セキュリティ対策の啓発推進を強化する等、重要インフラ防護に向けて一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

1.3 課題

サイバー攻撃についてはますます複雑・巧妙化しており、例えば他事業者等を経由した侵入、他事業者等から窃取した可能性がある情報による侵入及びユーザー情報窃取、他事業者等になりすました上でのDoS攻撃等が見受けられる状況にある。

このことを各重要インフラ事業者等の情報セキュリティ対策に照らした場合、情報セキュリティ対策は重要インフラ事業者等自身のみならず重要インフラ全体の防護能力の維持・強化にも効力が及ぶ等、その重要性が従来より増加している状況にあると言える。

加えて、重要インフラ事業者等からは、指針に対して「対策について、段階的な（優先順位付けされた）指針にするとわかりやすい」、「対策編で更なる具体的内容を提示してほしい」等との意見がある。

これらに鑑み、各重要インフラ事業者等の情報セキュリティ対策に資することを目的とした重要インフラ事業者等のPDCAサイクルとの整合に基づく本項の施策見直しを内閣官房の課題とする。

2. 情報共有体制の強化

第２次行動計画における本施策の期待される成果並びに成果検証の指標の考え方及び具体的な指標は次のとおりである。

- 「情報共有体制の強化」により期待される成果は、関係主体間で共有する情報についての整理がなされ、情報提供、情報連絡等に必要な環境整備等が進展し、各セプター、セプターカウンシルの自主的な活動が充実強化された結果として、重要インフラ事業者等が必要な情報を享受し、活用できるようになっていることである。
- そのため、整備された情報共有体制と共有された情報の充実に着目した指標を設定する。
- 具体的な指標は、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とする。

2.1 実施状況

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の変化、複雑・巧妙化するサイバー攻撃等に応じた情報セキュリティ対策への反映を通じた重要インフラ全体の防護能力の維持・強化に資することを目的に、官民の各主体が協力する情報共有体制の維持・向上に取り組んだ。

具体的には、「共有すべき情報の整理」及び「情報提供、情報連絡の充実」として、2009年３月に「第２次行動計画の情報連絡・情報提供に関する実施細目」（以下「実施細目」という。）を改定し、以降、関係主体間における具体的な情報連絡・情報提供方法の一層の充実、共有すべき情報項目の定期的な評価を行いつつ、情報共有を行った。

なお、共有すべき情報の整理については、「ＩＴ障害の未然防止」、「ＩＴ障害の拡大防止・迅速な復旧」及び「ＩＴ障害の原因等の分析・検証」による再発防止の３つの観点から、政府機関、関係機関、重要インフラ所管省庁、重要インフラ事業者等の各関係主体に応じた共有すべき情報の抽出と整理を行った。

加えて、内閣官房、重要インフラ所管省庁、重要インフラ事業者等との間でセプター訓練を行った。

「セプターの強化」としては、情報通信分野においてケーブルテレビ業界が2012年12月に「ケーブルテレビCEPTOAR」を発足し、2013年４月に正式に活動を開始した。

「セプターカウンシル」の取組としては、全セプターから構成される幹事会を定期的に開催するとともに、情報共有活動の強化に向けた「Webサイト応答時間計測システム」及び「標的型攻撃に関する情報共有体制（C4TAP)」が創設され、情報共有活動の充実を図ってきた。また、東日本大震災ではセプターカウンシルで培われた人的ネットワークを活用し、回線負荷の少ないファイル形式での情報提供及びアクセス集中回避に向けたボランティアミラーサイトの利活用を推奨する等、多発するＩＴ障害や

輻輳（ふくそう）においても円滑な情報提供がなされた。

2.2 成果

第２次行動計画期間中において、実施細目に基づき、重要インフラ所管省庁を経由して重要インフラ事業者等から567件の情報連絡を、内閣官房から157件の情報提供をそれぞれ行うとともに（2013年９月末時点）、毎年行っているセプター訓練には延べ58セプターが参加した。

なお、ＩＴ障害発生時の連絡共有体制については、当該体制が有効に機能した結果として、図表１に示すとおり、件数が増加している状況にある。

図表１　情報連絡のうちサイバー攻撃に関するものの推移

サイバー攻撃に関する情報連絡	2009年度	2010年度	2011年度	2012年度	2013年度（9月末時点）
不正アクセス、DoS攻撃	３件	４件	12件	55件	96件
コンピュータウイルスへの感染	０件	１件	２件	６件	３件
その他の意図的要因（不審メール等）	０件	０件	１件	15件	２件
合計	３件	５件	15件	76件	101件

また、セプターカウンシルについては、「ケーブルテレビCEPTOAR」の活動開始に伴い、参加セプター数は13となった。

このことから、官民連携による情報連絡・情報提供の枠組みの構築・確立及び当該枠組みの運用の安定化、各セプター・セプター間における情報共有体制の整備及び重要インフラ事業者等における必要情報の享受・活用の実現において一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

2.3 課題

サイバー攻撃に係る情報連絡件数が増加傾向にある一方、大規模ＩＴ障害の発生に関する連絡はなく、重要インフラ所管省庁、情報セキュリティ関係省庁及び関係機関と内閣官房との間で情報連絡・情報提供が完結した。

また、情報共有体制の運用にて以下の課題が見受けられた。

- 分野間における情報共有頻度に格差が生じつつあり、情報連絡の対象に該当するものの対象と認識されない情報がある。
- 攻撃手法の複雑・巧妙化に伴い、定義する「脅威の類型」では十分な情報連絡に至らない場合が生じつつある。加えて現行の関係主体だけでは十分な連携に至らない可能性が生じつつある。

これらに鑑み、実効性のある情報共有体制の構築を目的とした情報共有頻度の格差を解消すること、「脅威の類型」を細分化すること、大規模ＩＴ障害対応時の情報共有体制を平時の体制の延長線上に構築すること、情報共有体制の更なる強化に向けた共有すべき情報項目の見直しをすること及び既存の関係主体とサイバー空間関連事業者や防災関係省庁等の新たな関係主体との連携の在り方を整理することを内閣官房の課題とする。

また、政府機関を含め、他の機関から独立した会議体であるセプターカウンシルについては、従来にも増して各セプターの主体的な判断に基づく情報共有活動を行うことが望まれる。

3. 共通脅威分析

第２次行動計画における本施策の期待される成果並びに成果検証の指標の考え方及び具体的な指標は次のとおりである。

- 「共通脅威分析」に期待される成果は、指針の継続的改善及び重要インフラ事業者等における事業継続計画策定等に資する基礎資料を提供することである。
- そのため、毎年度当初に、重要インフラ事業者等の必要性を勘案して策定する共通脅威分析の検討項目に対する年度末時点の達成度に着目した指標を設定する。
- 具体的な指標は、実施した検討項目件数、各検討結果の重要インフラ事業者等による評価とする。

3.1 実施状況

重要インフラ全体の防護能力の維持・強化に不可欠である分野横断的な状況の把握・分析に基づく共通脅威分析の検討を行った。

具体的には、各分野におけるＩＴ利用の進展に応じて、図表２に示すとおり、様々な視点でＩＴに係る技術、環境等を対象とした各分野共通に起こり得る脅威を把握するための分析を毎年度行った。

図表２　共通脅威分析の各年度の分析内容

2009年度	重要インフラにおける共通脅威の分類（環境変化調査と共同実施） （重要インフラ分野共通のＩＴに関する技術、システム、環境等、広い範囲を対象として、脅威の候補を抽出し、「重要インフラ分野共通に起こり得る脅威とは何か」という視点で絞り込み、優先度付けによって分析対象を明確化）
2010年度	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環境 （重要インフラにおけるクラウドの範囲、導入に際しての脅威と対応方策、導入の可能性と形態、諸外国との比較等を調査・分析）
2011年度	重要システム等の堅ろう性 （制御システムを含む国内外のサイバー攻撃事例や対策動向等に着目した調査・分析を行い、堅ろう化手法を提示）
2012年度	重要インフラ分野における同時多発型ＩＴ障害発生時の復旧対応について （外部依存性、特にシステムベンダのリソース集中の脅威に焦点をあてた課題とベストプラクティスの提示及び過去の相互依存性解析の再確認調査の実施）
2013年度	次期行動計画策定のための今後の脅威候補対象（環境変化調査と共同実施） （クラウド、スマートフォン・タブレット端末、BYOD及びリモートメンテナンスの４つのトピックに対する環境変化調査と、M2M、ビッグデータ、スマートコミュニティー等の将来の新たな社会インフラ構造変化を見据えた長期的な環境変化調査を実施）

「相互依存性解析の継続」については、第２次行動計画において共通脅威分析の中で継続的に取り組むこととされたことから、図表２のとおり2012年度に当該調査も行った。

「共通脅威分析の検討」については、共通脅威分析のテーマを各重要インフラ事業

者等にとって優先度の高いものとするため、ＩＴ技術等に係る環境変化調査や東日本大震災からの「気付き」に基づくものを選定した。また、効果的な情報共有の実現に向け、重要インフラ事業者等、重要インフラ所管省庁、関係機関及び有識者が参加する検討会にてリスクコミュニケーションを図りながら分析を進めた。

3.2 成果

図表２に示すとおり、本施策にて実施の検討項目数は十分であると考えられる。

また、分野横断的演習の参加事業者等へのアンケートによると、各年度平均で75%以上の重要インフラ事業者等から、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の評価を得た（2009年度：82%、2010年度：80%、2011年度：66%、2012年度：86%)。

このことに加え、本施策によって重要インフラ事業者等における事業継続計画策定等に資する基礎資料を提供し、分析結果の一部を指針に反映したことから、重要インフラサービスの維持､復旧への活用への貢献において一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

3.3 課題

重要インフラ分野が有する重要システムにおいては、ＩＴ依存度、事業規模、運用体制、他分野との独立性等が分野において区々であることから、環境変化等により生じる新たな脅威が必ずしも全分野の共通脅威とはなり得ない。一方、新たな脅威が全分野の共通脅威ではない場合であっても、複数分野における脅威の影響の大きさから分析を必要とする場合があり得る。このことから、重要インフラ防護の維持・向上に資することを目的として、複数分野における脅威であってもその影響の大きさに応じて調査対象に加えることが必要である。

また、共通脅威分析は、時間的経過や環境変化の顕在化に応じて、その変化に潜む重要インフラに共通的な脅威等を詳細に分析することで効果性の高い結果が得られる。このことから、共通脅威分析の位置付けや実施頻度の見直しが必要である。

さらに、分析結果の指針反映に止まっている施策間の連携については、他施策が抽出した脅威等を本施策の検討項目に取り上げる等、施策間における成果の相互利活用についての検討が必要である。

これらの検討・見直しを内閣官房の課題とする。

4. 分野横断的演習

第２次行動計画における本施策の期待される成果並びに成果検証の指標の考え方及び具体的な指標は次のとおりである。

- 「分野横断的演習」に期待される成果は、重要インフラ事業者等のＩＴ障害発生時の早期復旧手順、事業継続計画の検証などに対する貢献である。演習で得られた知見を現実のＩＴ障害発生時の事業継続、早期復旧活動に効果的に活用できるものとするためには、より現実の状況に近い演習の実施が重要であり、それぞれの役割を担当する多くのプレイヤーの参加が望ましい。
- そのため、演習参加者の拡大と演習で得られた知見が、重要インフラ事業者等の取組みに貢献したかどうかに着目した指標を設定する。
- 具体的な指標は、演習の延べ参加者数と、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とする。

4.1 実施状況

重要インフラ分野におけるＩＴ依存度の進展及びＩＴを巡る様々な脅威の顕在化が見られる中、ＩＴ障害発生に備えた全分野を網羅する官民各主体参加の模擬的な演習を通じた相互の連絡・連携における仕組みの検証はますます重要になっていることから、その機会の提供に取り組んだ。

内閣官房主催の分野横断的演習はこれら仕組みを検証する我が国唯一の取組であり、第１次行動計画期間中の2006年度より毎年行ってきた。具体的には、第２次行動計画期間において、相互依存性解析から得た各分野の依存度が高い電力・通信・水道の途絶想定に基づく影響の波及に係る検証を分野横断的演習の３か年計画として設定し、詳細は環境や参加者のニーズ等を踏まえ、各実施年度の検討会にて決定した。

2010年度以降、日常使用するインフラ環境の利用、柔軟な演習参加者の設定等、より効果的、実践的な演習とするために、参加事業者等による自職場演習を導入した。

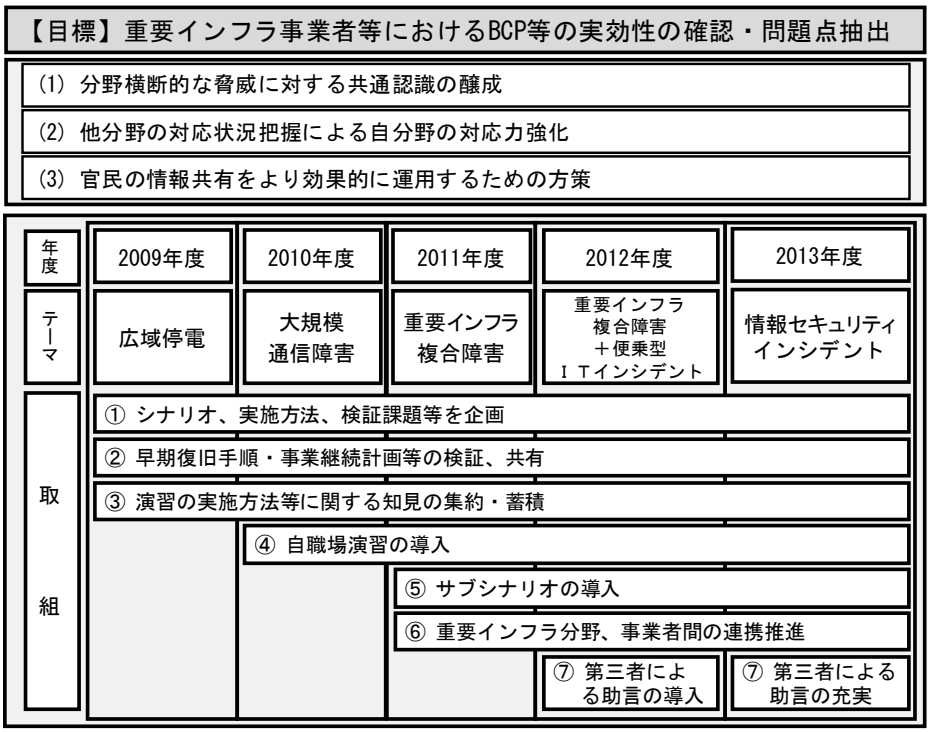
2011年度は、2011年発災の東日本大震災の経験を踏まえた複合障害（電力・通信・水道・ガス）を想定した演習テーマとするとともに、希望する分野が独自で設定したシナリオを「サブシナリオ」として状況に付加し、分野固有の課題検証を可能とした。

2012年度は複合障害の復旧段階への対応に加え、サイバー攻撃等近年の環境変化をテーマとするとともに、演習時のプレイヤー（参加事業者等）の判断・行動等への有識者等による助言制度を採用し、第三者視点に基づくＩＴ障害発生時の早期復旧手順及び事業継続計画等への検証における新たな気付きを提供し得る機会を提供した。

2013年度は政府機関や主要企業に対して頻発するサイバー攻撃等の現状や参加者からの要望を踏まえた情報セキュリティインシデントをそれぞれテーマとして設定した。

これら取組を図表３に示す。

図表３　第２次行動計画期間中の分野横断的演習の取組



なお、第２次行動計画以外にも、図表４に示すとおり、重要インフラ所管省庁においても個別の重要インフラ分野でのサイバー関連の対処能力向上を目指した演習・訓練を主催した。

図表４　重要インフラ所管省庁が主催する演習・訓練

省庁	名称	概要	対象者	実施期間	備考
総務省	電気通信事業分野におけるサイバー攻撃対応演習	サイバー攻撃等によるインターネットの機能不全に対応するために、複数の電気通信事業者等が参加し演習を行うことにより、高度なＩＴスキルを有する人材を育成し、電気通信事業者間の緊急対応体制を強化	電気通信事業者	2006～2008年度	国の施策としては終了（テレコムアイザック推進会議にて継続中）
経済産業省	情報セキュリティ対策推進事業	制御システムに対するサイバー攻撃の脅威を認識し、セキュリティインシデント発生の検知手順・障害対応手順の妥当性について検証	2012年度は、電力・ガス・ビル分野	2012～2016年度	
	電力卸取引市場におけるサイバー演習	卸売電気業界における経済的損失を最小限にとどめるためのインシデントレスポンスに係る対応体制、連絡体制等の確認検証	電力卸売	2006年度	机上演習 終了済
国土交通省	重要インフラの情報セキュリティ対策に係る机上演習	高度化・煩雑化するＩＴ障害からの防御を目的とした重要インフラ分野におけるセキュリティ対策評価・検証、関係者の熟度及び対応能力の検証	物流分野（航空･鉄道）	2007～2009年度	机上演習 終了済

4.2 成果

ＩＴ障害発生時の事業継続・早期復旧活動において演習で得た知見を効果的に活用するためには、より現状に近い演習の実施が不可欠であり、前述の時宜に応じた演習テーマ設定やサブシナリオの導入等は現状に近づけた演習の実現に寄与したと考えられる。

また、各年度の演習参加規模や参加事業者等へのアンケートにて得た、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は図表５に示すとおり推移している。

図表５　各年度の演習参加規模及びアンケート回答結果

年度	演習参加規模	有意義と回答した 参加事業者等の割合
2009年度	30組織、116名	82%
2010年度	38組織、141名	80%
2011年度	37組織、131名	66%
2012年度	42組織、148名	86%

官民あるいは他事業者等との情報連携が不可欠であるＩＴ障害発生時の早期復旧に向けて、より多くのプレイヤー参加が演習効果を高めることに資することから、上表のとおりプレイヤーである演習参加組織数・人数は増加傾向にあり、その効果も増していると考えられる。

このことから、演習で得られた知見に基づく重要インフラ事業者等のＩＴ障害発生時の早期復旧手順及び事業継続計画等の検証を通じた情報セキュリティ対策への貢献において一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

4.3 課題

区々である各組織のＩＴ利用形態・情報管理態勢に対応し得る演習環境の設定は大規模化するほど困難であり、大幅な参加者拡大が望めない中、結果として演習成果を直接享受できるのは重要インフラ事業者等の一部に限定されている。このことから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課題抽出機会の提供を目的として、参加者の拡大に依存することなく、重要インフラ分野全体に演習成果の更なる普及・浸透を図ることが必要である。

また、演習の評価に基づいて、次年度演習のテーマ設定、運営改善、他施策へ展開する等、演習運営の質的な改善を目指すことが必要である。

さらには、重要インフラのＩＴ障害発生時の対応には、重要システムを構成する製品、プラットフォーム等の提供サービス、重要システムを支える技術等の提供者の協

力を要する可能性を踏まえ、演習における関係主体の在り方を改めて検討することが必要である。

なお、重要インフラ所管省庁が独自に主催する重要インフラ事業者等を対象とする演習・訓練に加え、防災関係省庁が主催するＩＴに係る物理的障害発生を想定した政府機関内での対処を検証する訓練も実施されていることから、各機関との連携について検討することを要する。

これらの検討・見直しを内閣官房の課題とする。

5. 環境変化への対応

第２次行動計画における本施策の期待される成果並びに成果検証の指標の考え方及び具体的な指標は次のとおりである。

- 「環境変化への対応」に挙げた施策のうち、「広報公聴活動」に期待される成果は、行動計画の枠組みついて広く国民の理解を得ることと、第２次行動計画への協力者を関係主体以外にも拡大することである。
- そのため、第２次行動計画の周知機会の充実に着目した指標を設定する。
- 具体的な指標は、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とする。
- 「環境変化への対応」に挙げた施策のうち、「リスクコミュニケーション」に期待される成果は、関係主体間で互いの活動への理解の向上と、連携を図りやすい環境の醸成である。
- そのため、関係主体間のコミュニケーション機会の充実に着目した指標を設定する。
- 具体的な指標は、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とする。

5.1 実施状況

(1) 広報公聴活動

国民に対する説明責任を果たすことを目的として広報公聴活動を行った。

具体的には、広報活動として、第２次行動計画に基づき行った重要インフラの情報セキュリティ施策の結果である、指針、環境変化調査及び共通脅威分析の調査報告書、分野横断的演習の成果展開資料、重要インフラ専門委員会の会議資料等について、内閣官房のWebサイトに掲載し、公表した。

公聴活動として、各種セミナーやフォーラム等の場を活用し、情報セキュリティ政策に係る講演等を四半期に１回程度の頻度で行った。加えて、国内外の情報セキュリティに関する情報を「NISC重要インフラニュースレター」として関係省庁や重要インフラ事業者等に月に２件程度の頻度でメール配信を行った。

また、指針の改定に際しては、Webサイトにてパブリックコメントを求め、意見聴取を行った。

(2) リスクコミュニケーションの充実

リスクや情報セキュリティ対策の方法に係る認識の共有及び情報セキュリティ対策の連携効果の向上を目的として、関係機関等との意見交換を行った。

具体的には、内閣官房は情報セキュリティに係る関係機関との意見交換会を四半期ごとに開催し、情報セキュリティに係る取組や共通脅威等に係る意見交換を行った。また、セプターカウンシルにおいては、2010年６月に情報共有活動の推進を目的とし

た相互理解WGを設置し、各重要インフラ事業分野が有する重要システムの利用現場や施設等の見学・紹介を行った。

さらに、2009年度から2010年度までにかけて関係主体間にて行うリスクコミュニケーションのテーマの提供を目的として、環境変化に伴う脅威についての調査・抽出をした上で、以下の詳細調査を行った。

・サイバー攻撃動向等の環境変化を踏まえた重要インフラのシステムの堅ろう化
・情報システムのサプライチェーンにおける情報セキュリティ
・スマートグリッドの普及とその重要インフラの情報セキュリティにもたらす影響
・制御システムのオープン化が重要インフラの情報セキュリティに与える影響
・東日本大震災における重要インフラの情報システムに係る対応状況等
・重要インフラ分野におけるＩＴ依存度調査（水道分野及び医療分野）

これらの調査結果については、セプターカウンシルへの情報共有やリスクコミュニケーションの充実に活用した。

(3) 国際連携の推進

国際会合への参加や他国機関等との連携を通じて情報インフラ防護のためのベストプラクティス等に係る最新動向の把握・情報共有を行った。

具体的には、重要インフラ政策に携わる政府機関が相互連携について検討を行うメリディアン会合に毎年参加し、日本の情報セキュリティ政策等を紹介するとともに、欧米やアジア各国の重要インフラ防護担当者との意見交換を通じて、情報セキュリティ政策の国際的な動向に係る情報収集を行った。

また、2010年９月及び2013年３月に開催された世界的規模のサイバー演習であるサイバーストームにIWWN(International Watch and Warning Network)の一員として参加し、重要インフラ分野における国際的な連携を深めた。

さらに、「NISC重要インフラニュースレター」等による海外の関連動向や情報セキュリティ上の脅威に係る情報提供及びセプターカウンシル等における各国動向等についての情報共有を行った。

5.2 成果

(1) 広報公聴活動

重要インフラの情報セキュリティ施策の結果、重要インフラ専門委員会の会議資料等については速やかに掲載を行った。

また、情報セキュリティ政策に係る講演等については、第２次行動計画期間において、23回行った（2009年度：６回、2010年度：６回、2011年度：５回、2012年度：４

回、2013年度：２回（2013年９月末時点））。さらに、「NISC重要インフラニュースレター」については102件を配信した（2013年９月末時点）。

加えて、2010年度及び2012年度に行った指針改定に際し、改定の都度、パブリックコメントによる意見聴取を行った。

このことから、充実したコンテンツの提供を通じて第２次行動計画の枠組み等に係る広報公聴活動について一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

(2) リスクコミュニケーションの充実

関係機関との意見交換会については、各年度とも四半期ごとに開催するとともに、重要インフラ事業者等とのリスクコミュニケーションとして、共通脅威分析及び分野横断的演習の検討会を計21回開催した（2009年度：５回、2010年度：５回、2011年度：５回、2012年度：５回、2013年度：１回（2013年９月末時点））。

また、相互理解WGを計16回開催（2013年９月末時点）した。

環境変化の変化に伴う情報共有等への調査結果の活用も含め、このことから、官と民、民と民における双方向のリスクコミュニケーションの促進、重要インフラ事業者等間の直接的なコミュニケーション機会の拡大、信頼関係の強化、環境変化に伴う脅威の察知能力の向上を通じて、リスクや情報セキュリティ対策の方法に係る認識の共有及び情報セキュリティ対策の連携効果の向上に向けて一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

(3) 国際連携の推進

メリディアン会合への参加にて情報セキュリティ対策に係るベストプラクティスの共有を図るとともに、サイバーストームへの参加にて共同演習等の国際的な連携を図る等、重要インフラ防護に係る国際的な取組に参画していくことで、諸外国との連携が実現できた。

このことから、情報インフラ防護のためのベストプラクティスに係る最新動向の把握・情報共有について一定の成果が得られたと評価し、第２次行動計画の所期の目標について一定の成果を挙げたと評価できる。

5.3 課題

(1) 広報公聴活動

これまでの取組は、主に重要インフラ事業者等を対象としており、国民に対する冷静な対応を取る上で必要な情報の提供と理解促進に資する情報公開には及んでいない。一方、第２次行動計画に基づく取組の多くが国民の理解・活用に直結した内容ではな

い。

これらに鑑み、次期行動計画における本施策と他施策との整合の下、目的と情報開示範囲に応じた広報公聴活動の見直しを課題とする。

(2) リスクコミュニケーションの充実

リスクコミュニケーションにおける有用な情報には機微情報を含み、開示制約から参加者を限定せざるを得ない状況にある。また、リスクコミュニケーションの前提となるリスクマネジメントの定義については、国際標準との整合をとることに留意する必要がある。

これに鑑み、機微情報の秘匿と情報の有用性の相反性を踏まえつつ、より多くの関係主体による情報共有・連携の実現に向けた情報の共有範囲の確認や共有手段の多様化等の見直しを内閣官房の課題とする。

また、ビッグデータ、M2M、スマートコミュニティー等の新たなＩＴ技術革新については中長期的な実現・利用が見込まれる状況にあり、新たなＩＴ技術革新に付随する脅威については、重要インフラサービスに大きな影響を与えることが予想される。

これに鑑み、将来的な脅威の影響の大きさが予想される環境変化のテーマについては、中長期的に継続した調査の実施に係る検討を内閣官房の課題とする。

(3) 国際連携の推進

サイバー空間においては国境を越えてグローバルに形成されており、サイバー空間に存在するリスクについては深刻化・グローバル化している。

これに鑑み、求められるリスクへの迅速な対応に向けて、引き続き諸外国との連携を推進するとともに、国際的な枠組みに限定せず、ASEAN等のアジア太平洋地域や欧米等の二国間、多国間、地域的枠組みの積極的な活用を通じた国際連携の強化を内閣官房の課題とする。