資料３

平 成 ２ ４ 年 ２ 月 ９ 日
重要インフラ専門委員会事務局

第２次行動計画期間中の施策推進状況について（案）

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」（以下「第２次行動計画」という。）は、2009 年 2 月に情報セキュリティ政策会議において決定され、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いる。

「セキュア・ジャパン 2009」「情報セキュリティ 2010」「情報セキュリティ 2011」において、重要インフラについても、各年度の実施計画を定めているが、この間基本戦略として、2010 年 5 月には新たに「国民を守る情報セキュリティ戦略」が決定された。これらの戦略、実施計画においても、当該行動計画に基づいて諸施策が推進されている。今回、早急に対応すべき取組を検討するに当たり、諸施策の実施状況を点検することとする。

２．行動計画期間中における諸施策の実施状況について

（１） 安全基準等の整備及び浸透

① 社会動向の変化等に対応し、新たな知見を指針に適時反映していくために、指針の分析・検証を毎年度実施している。2009 年度の分析・調査を受け、「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（第３版）」を、第２３回情報セキュリティ政策会議（2010 年 5 月）にて決定した。主な変更点は以下の通り。

ⅰ）従来からの全分野に亘る情報セキュリティ対策の底上げの観点から必要な対策に加えて、新たに個別の先進的な対策を取り込めるような記載とし、発展性を持たせた。

ⅱ）従来からの情報セキュリティ対策について、利用者視点から、ＩＴ障害発生時に於けるサービス状況等の利用者への情報提供、また、新型インフルエンザ等新たな脅威への対応を盛り込んだ。

また、重要インフラ分野及び事業者が安全基準等を定めるにあたり、実践的な参考となるよう、具体例を記した「指針対策編」を重要インフラ専門委員会（2010 年 7 月）で新たに策定した。

② 重要インフラ所管省庁における「安全基準等」の分析・検証及び改定等の実施状況ならびに今後の実施予定等の把握及び検証を毎年度実施している。

③ 「安全基準等」の重要インフラ事業者への浸透状況等に関する調査を毎年度実施している。

④　東日本大震災が重要インフラの情報システムの安定運用に及ぼした影響及び重要インフラサービスに波及した状況について調査を実施中。情報システムの安定運用の視点で、重要インフラの安全基準等の指針やＩＴ－ＢＣＰに盛り込むべき課題を抽出し検討予定。

（２）　情報共有体制の強化

①　共有すべき情報の整理については、政府機関、関係機関、所管省庁、事業者等の各主体に応じて共有すべき情報の洗い出しと整理を行った。障害発生時の連絡体制については実施細目に基づく情報共有が機能してきており、セプターカウンシルを中心に平時における情報共有についての検討が継続されている。

②　「第２次行動計画の情報連絡・情報提供に関する実施細目」について、2009年 3 月に改訂を行い、NISC と重要インフラ所管省庁、情報セキュリティ関係省庁、事案対処省庁、関係機関における具体的な実施事項を規定し、実施細目に基づく情報共有を図ってきたところ。2010 年 9 月には、尖閣諸島の中国領有を主張する民間団体のサイトに日本政府機関等へのサイバー攻撃を呼びかける記載があり、重要インフラ所管省庁等を通じた情報共有体制を強化した体制を敷いたが、実施細目に基づく連絡体制が有効に機能することが確認された。

「セプター訓練」について、重要インフラ所管省庁の協力を得つつ、セプターの情報共有体制の維持・向上のため、情報疎通機能確認等の機会の提供を年１回（計３回）実施し、延べ３０セプターが参加している。

③　セプターの強化については、重要インフラ所管省庁の協力を得て、各年度末にセプターの特性、活動状況を前広に把握するとともに、セプター特性把握マップをとりまとめている。

行動計画で示している全１０分野の１４セプターにおいて情報共有活動を継続して行っているほか、６分野（９セプター）において共有情報の事例分析等を実施している。

全セプターが分野横断的演習に参加しているほか、個々のセプターで自主的な活動を展開している。また、セプターカウンシルの場を利用しセプター間での情報共有を進めている。

④　セプターカウンシルについては、2009 年 2 月に設立され、各セプター間の横断的な情報共有体制として機能するとともに、重要インフラ事業者等と政府機関等の協力関係を深めている。具体的には全セプターから成る幹事会を定期的に開催し、2012 年 1 月末現在３つのワーキンググループ（ⅰ相互理解、ⅱ情報収集、ⅲ情報共有推進）において活発に活動しているほか、サイバー攻撃対応力ＷＧでは報告書をとりまとめている。

東日本大震災に際しては、セプターカウンシルの情報共有のネットワークを活用して、回線へ負荷の少ないファイル形式での情報提供の呼びかけや、アクセス集中が顕著な分野に対するボランティアミラーサイト提供の案内など、障害や輻輳の多発する中での円滑な情報提供を主導した。

民間事業者を主体とする業種横断的な情報セキュリティに関する体制は

世界的にも先進的な取組みとして、ＩＷＷＮ等の国際機関にも紹介されている。

現在のところ、１０分野１２セプターの約４千社を擁する取組みとなっている。（情報（電気通信、放送）、金融（銀行、証券、生保、損保）、航空、電力、ガス、政府・行政サービス、水道及び物流が参加）

なお、ＮＩＳＣは当面の間セプターカウンシルの事務局を務めている。

（３）　共通脅威分析

共通脅威分析の検討については、各重要インフラ分野におけるＩＴ利用が一層の進展を見せる中、我が国全体としての重要インフラの情報セキュリティを向上させていくためには、分野横断的な状況の把握、分析が従来以上に不可欠である。このため、それぞれの重要インフラ分野共通に係る各種の脅威について、様々な視点でＩＴに関する技術システム、環境等を対象として分析を実施している。

各年度の分析内容は次の通りである。

・2009 年度：重要インフラにおける共通脅威の分類（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）
・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導入（①クラウドの範囲、②導入に際しての脅威と対応方策、③導入の可能性と形態について、④諸外国との比較）
・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、分析・評価）

（４）　分野横断的演習

ＩＴ障害を引き起こす要因である脅威に関する最新動向を把握し、それら脅威に対する分野横断的な重要インフラ防護対策の向上を目指し、具体的なＩＴ障害発生を想定した演習シナリオの検討とそれに基づく分野横断的な演習を継続的に実施することにより、課題の抽出及び演習実施のための知見の整理を行っている。

各年度の演習テーマについては次の通りである。

・2009 年度：広域停電（３０組織、１１６名参加）
・2010 年度：大規模通信障害（３８組織、１４１名参加）
・2011 年度：電力、通信、水道、ガスの広域的かつ複合的サービス障害（３７組織１３１名参加）

（５）　環境変化への対応

①　広報活動

内閣官房情報セキュリティセンターのホームページを用いて、行動計画に基づき実施した重要インフラの情報セキュリティ対策及びその結果を公表するとともに、重要インフラ専門委員会等の会議資料の掲載を行った。また、

広聴活動として、セミナーやフォーラム等の場を活用し、行動計画などの情報セキュリティ政策に関する講演を 2009 年より計１７回行った（2009 年度６回、2010 年度６回、2011 年度：５回（2012 年 1 月末現在））。

② リスクコミュニケーションの充実

内閣官房において、情報セキュリティに関する関係機関との意見交換会を四半期ごとに開催し、セキュリティに関する取組みや共通する脅威等について意見交換を行った。また、重要インフラ事業者等とリスクコミュニケーションを行なう場として、共通脅威分析及び分野横断的演習検討会を計１２回実施した（2009 年度：５回、2010 年度：５回、2011 年度：２回（2012 年 1 月末現在））。加えて、2010 年 6 月に、セプターカウンシルに情報共有活動の推進を目的として相互理解ＷＧを設置し、各重要インフラ事業分野のＩＴシステムの利用現場や施設等の見学や紹介等を合計９回行うなど、各重要インフラ事業者間の相互理解の促進や信頼関係の強化を図った。

③ 国際連携推進

国際会合への参加や他国機関等との連携を通じて最新動向を把握し、情報共有を行った。2009 年度以降の主な活動は以下のとおり。

- 重要インフラ政策に携わる政府機関が相互の連携について検討を行うメリディアン会合（年１回開催）に参加し、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関する情報収集を行った。
- 2010 年 9 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Ⅲ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。
- 内閣官房から関係省庁や重要インフラ事業者等へ配信しているＮＩＳＣ重要インフラニュースレター等において、海外の関連動向やセキュリティ脅威に関する情報を紹介したほか、セプターカウンシル等において各国の動向等について情報提供を行った。

（６） 補完調査

指標では捉えられない側面を補完的に調査する取組として、補完調査を実施している。期間中、以下の調査を実施しており、2011 年度については実施中である。

① 外注先からの情報流出等（2009 年度調査）

顧客情報を含む情報の処理作業を外注した際、外注先企業の従業員等がそれらの情報を自宅等に持ち帰ったところ、作業を行った個人用 PC がウィルスに感染していたため顧客情報の一部が外部流出した複数のケースを対象として調査を行った。

調査の結果、厳重な管理を要する情報を外部で処理する場合、外注先での対策の実施確認、社内外における情報流出の監視等セキュリティ対策の実効性を確保するための対策を充実させる必要が認められた。

なお、指針第３版において外部委託における情報セキュリティ確保のため

の対策を充実させた。

② 都市部で基幹通信システムが停止した場合に重要インフラ事業者が受けた影響（2010 年度調査）

政令指定都市における電話交換施設で障害が発生した際に重要インフラサービスが受けた影響を調査した。

・この施設を経由する、ほぼ全ての通信サービスを停止する等の影響を受けた。

・調査の結果、回線の二重化等の堅牢化対策を充実させる必要性が認められた。