資料２

平成２４年３月２１日
重要インフラ専門委員会事務局

最近の環境変化への対応についての
重要インフラ第２次行動計画への反映について（報告案）

１　概要

重要インフラの情報セキュリティ対策については、平成２１年（２００９年）２月、第２次情報セキュリティ基本計画の策定と同時に「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。）が策定されており、策定当初には、３年で見直すこととされていた。

一方、基本計画については、平成２２年５月に「国民を守る情報セキュリティ戦略」（以下、「戦略」という。）が策定されたが、重要インフラの情報セキュリティ対策については、環境変化に対応するような特段の問題はなかったことから、戦略においても第２次行動計画に基づいて実施することとなった。

しかしながら、戦略策定後、①東日本大震災発生時における複数のＩＴシステムの同時的な障害発生及びその際の事業継続計画（ＢＣＰ：Business Continuity Plan）の実施、②政府関係機関や重要インフラ事業者を含む我が国の主要企業のＩＴシステム（制御システムを含む）に対するサイバー攻撃等、いくつかの環境変化が生じていることから、現在までの第２次行動計画の施策の実施状況を点検し、早急に取組を強化・補強すべき点について第２次行動計画に反映を行うこととする。また、第２次行動計画の期間を戦略の実施期間に合わせて平成２５年度まで延長することとする。

２　検討の経緯

平成２４年２月９日に第２７回重要インフラ専門委員会を開催し、第２次行動計画にもとづき取り組むこととされている情報セキュリティ対策についての施策の推進状況を点検するとともに、第２次行動計画上強化・補強すべき点について議論を行い、以下の項目のとおり整理することとした。

（１）情報セキュリティ政策会議において、早急に第２次行動計画に反映する（すなわち、今年度に対応する）ことが必要な部分として例示した次の３項目について、具体的にどのような強化・補強を行うことが必要か。

（政策会議において強化・補強が必要であると例示した項目）

① ＢＣＰ等の充実

東日本大震災における教訓を踏まえた、安全基準等の策定に当たっての指針（特にＢＣＰ）の一層の充実

② 環境変化を踏まえた安全基準の改善

標的型攻撃など最近の環境変化を踏まえて、制御システム等についての安全基準の検証を行い、必要に応じて第２次行動計画、指針等を改定

③ 情報共有体制の強化

平素からの情報収集・情報共有体制の充実

（２）上述（１）①～③に掲げる項目に関して、①ほど早急な対応は必要としないが、行動計画上強化・補強することが必要な点として何があるのか。

（３）（１）、（２）以外の事項について中長期的に検討が求められる点として何があるのか。

専門委員から出された意見をもとに、平成２４年３月２１日に第２８回専門委員会を開催し、第２次行動計画改訂案をとりまとめた。また、その実施に際して注意すべき事項（例：『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。）等への反映）についてもとりまとめた。

なお、中長期的な検討が求められるとされた事項については、引き続き検討を行い、次期行動計画策定時にその結果を反映することとする。

３　検討の結果

前述２における（１）～（３）についての専門委員会における意見及びその対応（案）は以下のとおりである。

（１）情報セキュリティ政策会議において、早急に行動計画に反映する（すなわち、今年度に対応する）ことが必要な部分として例示した次の３項目について、具体的にどのような強化・補強を行うことが必要か。

① 事業継続計画（ＢＣＰ）等の充実

東日本大震災における教訓を踏まえた、安全基準等の策定に当たっての指針（特にＢＣＰ）の一層の充実

（意見）

東日本大震災発生時にＩＴシステムにおいて発生した障害とその対応を鑑み、特にＩＴシステムに関するＢＣＰを作成あるいは見直し、複合的に障害が発生した場合においても、事業継続計画を適切に実行できることが求められる。その際、中央防災会議における検討動向等と整合性をとって進めることが望ましい。

（対応（案））

行動計画　Ⅱ　１.（１）指針の継続的改善　において、ＢＣＰに関する記述を修正・追加（第４章を参照）。

なお、「指針」及び「指針　対策編」の見直しの際には、現在実施中の「東日本大震災における重要インフラに係る対応状況等の調査」の結果、分野横断的演習における気づき等を踏まえ、通信途絶時の対策等ＩＴ－ＢＣＰに関する項目を追記することとする。

② 環境変化を踏まえた安全基準の改善

標的型攻撃など最近の環境変化を踏まえて、制御システム等についての安全基準の検証を行い、必要に応じて行動計画、指針等を改定

（意見）

情報システム自体の変化に対応して整合性を確保しつつ、可用性などの安全基準を見直していくことが望ましい。

（対応（案））

行動計画　Ⅱ　１.（２）安全基準等の継続的改善　において、対策が求められる例として「標的型攻撃」、「制御システムへの攻撃」を追加（第４章を参照）。

安全基準等の浸透状況を調査する際、攻撃の動向、情報システムの変化等、環境変化への対応状況を精査し、必要に応じて「指針」または「対策編」に必要な項目を追加するとともに、国際標準に準拠した評価認証機関の活用またはセキュリティ検証施設の活用等制御システムのセキュリティ評価・検証を容易にするための方策を追加することとする。

③ 情報共有体制の強化

平素からの情報収集・情報共有体制の充実

（意見）

情報共有に関して、全てを共有することが難しい。米国でも情報共有の重要性は理解されているが、重要インフラ業界との間の情報共有の仕組みを機能させるのに大変な苦労をしているようだ。このため、情報共有を具体的に進めるための施策を行動計画にも盛り込むことが望ましい。

（対応（案））

行動計画　Ⅱ　２.（４）セプターカウンシル　において、重要インフラ事業者等と政府機関等の密接な意見交換や事業者にも役立つ情報の共有等、取組みを具体的に追加（第４章を参照）。

セプターカウンシルにおいては、システムの運用状況の客観的判断材料等事業者間で共有可能な情報の追加等を具体的に検討

（２）上述（１）①～③に掲げる項目に関して、①ほど早急な対応は必要としないが、行動計画上強化・補強することが必要な点として何があるのか。

（意見）

民間同士あるいは官民における情報共有を進めるため、企業秘密を確保しつつ、必要な者との間で共有を行うために求められる要件の緩和条件やその仕組みについての検討を進めることが求められる。

（対応（案））

現行の情報共有の枠組みによる情報共有を進めるとともに、現行を超える情報共有の在り方については、その必要性を含めて中長期的な課題として検討することとする。

（３）（１）、（２）以外の事項について中長期的に検討が求められる点として何があるのか。

（意見）

企業はシステム監査について内部で体制を整備することが必要であり、人員の確保、育成及び活用について十分な配慮を行うとともに、システム調達から廃棄までの全体のライフサイクルの中で、システムやデータについての情報セキュリティについて考えてほしい。

ネットワークを含めたシステムの高度化・複雑化が進展し、各階層（レイヤ）の運用者が異なる等により、セキュリティ対策が講じられない部分が生じることが想定される。このような部分における課題と対応に必要な対策を検討すべき。

現在の情報セキュリティ対策は、重要インフラにおける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重要インフラを防護するとともに、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観点から講じられているが、防護対策を意図的に破られた場合にどのような対応を行う必要があるかについては更なる検討の余地がある。

（対応（案））

人材の育成については、別途人材育成・普及啓発専門委員会において議論されている内容を踏まえて、重要インフラを対象とした方策について中長期的な課題として検討することとする。

ライフサイクルを踏まえたセキュリティの確保については、ライフサイクル全体を考えた際に現行のセキュリティ対策に追加することが望ましい事項について中長期的な課題として検討することとする。

システムの高度化・複雑化に伴い求められる、特に階層と階層の間でのセキュリティ対策については、技術面での環境変化への対応に関して中長期的な課題として検討することとする。

防護のための対策が破られた場合に求められる情報セキュリティ対策については、システム運用面で求められる対策に関して中長期的な課題として検討することとする。

４　行動計画　改訂（案）

３（１）における改訂（案）及び行動計画期間の延長を盛り込んだ改訂（案）は次のとおりである。（赤字が追加・修正を行った部分、取り消し線は削除を行った部分。）

Ⅰ　総論

５．行動計画の改訂

第２次行動計画策定後、平成２２年５月に「国民を守る情報セキュリティ戦略」（以下、「戦略」という。）が策定されたが、重要インフラの情報セキュリティ対策については、環境変化に対応するような特段の問題はなかったことから、戦略においても第２次行動計画に基づいて実施することとなった。

しかしながら、戦略策定後、①東日本大震災発生時における複数のＩＴシステムの同時的な障害発生及びその際の事業継続計画（ＢＣＰ：Business Continuity Plan）の実施、②政府関係機関や重要インフラ事業者を含む我が国の主要企業のＩＴシステム（制御システムを含む）に対するサイバー攻撃等、いくつかの環境変化が生じていることから、第２次行動計画の施策の実施状況を点検し、早急に取組を強化・補強すべき点について第２次行動計画に反映を行った。また、行動計画の期間を延長し、次回の見直しを平成２５年度に行うこととした。

Ⅱ　計画期間内に取り組む情報セキュリティ対策

１．安全基準等の整備及び浸透

（１）指針の継続的改善

社会動向の変化等に対応し、また新たな知見を適時反映していくために、指針の分析・検証を１年毎、及び必要に応じて実施し、その結果を公表することとする。なお、指針の改定に関する検討は原則として３年に１度実施するものとする。ただし、必要に応じて追加的に検討を実施し、必要があると認められた場合には指針の改定を行うこととする。

なお、指針の改定に関する検討にあたっては、東日本大震災において重要インフラ分野に生じた複合的な障害における教訓を踏まえ、事業継続計画において情報セキュリティ上のリスクを十分想定する必要が生じている状況~~重要インフラ事業者等において事業継続計画の策定が進みつつある状況~~や、事業継続計画に関する国際規格化の進展状況等を踏まえ

つつ、分野横断的な観点からも実効的であるかを検証できるように指針の内容を充実させるものとする。

各重要インフラ事業者等の自主的な取組みに資する項目を充実させるために、指針に記載される事項を「要検討事項」と「参考事項」に分類し、対策項目の具体化の例示を行う事により、引き続き記載事項の充実を図ることとする。

「要検討事項」とは対策の底上げの観点から全分野共通で特段の理由のない限り対策することが望まれる事項であり、安全基準等に規定する必要性を各分野が検討するべき事項とする。また「参考事項」とは進んだ対策として盛り込む事が望ましい事項とし、各分野が任意で参考とする事項とする。

要検討事項及び参考事項は、現行指針の項目に加え、行動計画に基づく各重要インフラ分野及び重要インフラ事業者等の取組みから得られる知見・教訓等を候補として必要に応じて充実させていくこととする。

（２）安全基準等の継続的改善

各分野においては、対策の経験から得られた知見を安全基準等に反映するため、安全基準等の継続的な改善に取り組むこととする。なお、安全基準等の検証に際しては、指針や毎年実施される指針の分析・検証の結果を踏まえた検討を行うこととするが、その際標的型攻撃、制御システムへの攻撃への対策等最近の環境変化に対応しているか否かの分析・検証も行い、必要に応じて安全基準等の改訂を行うこととする。

情報セキュリティ対策に関する知見の共有を促進するために、従来検証対象となっている安全基準等の他に、情報セキュリティ対策に関する基準又は参考文書類を、可能な範囲で共用できるよう改めて広く安全基準等として整理することとする。

安全基準等に基づく対策状況については、関係性を有する主体間で互いに把握しておくことができることが重要である。そのため、情報セキュリティ監査又はそれに対する相当するものの実施や、情報セキュリティ報告書又はそれに相当するものの作成等の自主的な取組みを一層推奨し、分野や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対外的な説明に努める。

２．情報共有体制の強化

（４）セプターカウンシル

セプターカウンシルは、各セプターにより構成される共助・互恵の活動の取組み~~の場として創設を目指す~~を促進するために創設されたものであり、相互理解及びベストプラクティス等の具体的な事例共有等の分野横断的な情報共有が行われることが望まれる。

また、政府機関等とは独立した活動が可能な位置付けにあることから、情報共有の改善等のための検討に関し自ら積極的な活動に取り組むことが期待される。特に重要インフラ事業者等と政府機関等の協力関係を今後一層深めていくためには、両者の間の状況認識等の共有を進めていくことが重要であることから、~~重要インフラ事業者等と政府機関等との意見交換を行うなどの~~平時から重要インフラ事業者等と政府機関等の意見交換を密接に行うことが望まれる。また、事業者間においても相互に役立つ情報の共有を進めるなどの取組みがなされることが望まれる。なお、この取組みを進めるに当たって、セプターカウンシルの事務局を努める内閣官房においては、２（１）カ②に示す環境整備を行うことが重要である。

Ⅳ　評価・検証と見直し

１　行動計画の推進体制

（６）行動計画の見直し

第２次行動計画については、対策の成果、施策の成果、補完調査、評価の内容等（以下「評価等」という。）を踏まえ、また、脅威、ＩＴ障害、ＩＴを利用したサービス等に関する社会情勢等の変化等をふまえ、３年毎または必要に応じ、見直しを行う。~~第２次行動計画期間中においては、少なくとも策定から２年後から１２ヶ月かけて見直すこととする~~再度の見直しについては、平成２５年度に行うものとする。

特に見直しの要点となるのは、目標とそれに基づく基本的な方向性、重要インフラ事業者等の対象範囲、関係主体とすべき主体の対象範囲、対策や施策の追加や廃止、想定すべき脅威の例示、対象とすべき重要インフラサービスの範囲、サービスレベル、検証レベル、評価指標の設定等である。またこれに併せて、各用語の定義や行動計画の対象範囲についても、必要に応じて見直しを行うものとする。

第２次行動計画の見直しに際しては、各分野の特性や取組状況に配慮しつつ、事業者の取組みが自主性に基づくものであることを踏まえた検

討を行うことが必要である。また、第２次行動計画が想定し得なかった事象が発生した場合はこれに対応できるようにすることが重要である。

　行動計画の見直しは重要インフラ専門委員会において行うこととし、委員会の合意を経て、情報セキュリティ政策会議で新たな行動計画を決定するものとする。

（参考）

第２次行動計画期間中の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）指針の継続的改善

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）安全基準等の継続的改善

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）安全基準等の浸透

「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）その他

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

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）情報提供、情報連絡の充実

「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。

（３）セプターの強化

「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。

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

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）広報公聴活動

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。