資料２

「重要インフラの情報セキュリティ対策に係る行動計画」見直しにあたっての論点整理（案）

2008年 4月 ○日
重要インフラ専門委員会

１. はじめに

重要インフラにおいては、そのサービスの安定的供給が最優先課題であるという面から、各事業において発生する IT 障害が国民生活・社会経済活動に重大な影響を及ぼさないよう対策を実施することが必要である。その一方で、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重要インフラ事業者等の取組みだけでは限界に達しつつあるのが現実である。

そこで、重要インフラ事業者等の自主的な取組みを基本としつつ、官民の緊密な連携の下での情報セキュリティ対策の強化を目指して「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１３日・情報セキュリティ政策会議決定）（以下「行動計画」という。）が定められ、以降、政府及び各重要インフラ分野において種々の取組みがなされてきた。

行動計画は、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、継続的な見直しと改善を通じ情報セキュリティ対策の向上を図っていくという視点に立って策定されたものであり、「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」こととなっている。これにもとづき、本委員会においては、２００７年１２月から見直し作業に着手したところである。

本文書は、行動計画の見直しを進めていくに当たって、現行動計画の下でのこれまでの取組みの成果をまとめるとともに、具体的に検討すべき論点を一旦整理することで、今後の検討作業の効率的かつ確実な進捗を図るものである。

２. これまでの取組みと成果

２－１ 安全基準等の整備

安全基準等の整備については、２００６年度及び２００７年度において、それぞれ以下に掲げる取組みがなされた。その結果、重要インフラ全１０分野において、望ましいと考えられるレベルを満たす情報セキュリティ対策が実施されるための「安全基準等」が整備されるとともに、PDCA サイクルにおいて、政府の「指針」（「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（２００６年２月２日・情報セキュリティ政策会議決定）（以下同じ。）の観点も盛り込んでの見直しが行われるようになった。また、「指針」に基づく分野横断的な検証によって各分野毎の安全

基準等の特徴等が明らかになることで、分野間でのノウハウの共有のための環境整備も進展している。

【２００６年度の主な取組み】
○　全１０分野において安全基準等の策定・見直しを実施。
○　各分野の安全基準等について「指針」との対応状況についての評価を実施。
○　「指針」の見直しを実施。

【２００７年度の主な取組み】
○　「指針」の改定を踏まえ全１０分野において安全基準等の見直しを実施。
○　各分野の安全基準等について、「指針」との対応状況や「相互依存性解析」を踏まえた検証を実施。
○　安全基準等の浸透状況等に関する調査を実施。
○　「指針」の見直しを実施。

２－２ 情報共有体制の強化

情報共有体制の強化については、２００６年度及２００７年度において、それぞれ以下に掲げる取組みがなされた。その結果、重要インフラ分野における官民の各主体間での情報共有、連絡・連携のための基本的枠組みが構築された。

【２００６年度の主な取組み】
○　各重要インフラ所管省庁にリエゾン（内閣官房併任）をおき、内閣官房情報セキュリティセンターとの間で情報連絡・情報提供を行うための体制を整備。
○　重要インフラ既存７分野（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス）においてCEPTOARを整備。新規追加３分野（医療、水道、物流）において、２００７年度中のCEPTOAR整備に向け基本的に合意。
○　CEPTOAR-Council（仮称）の設置に向けた検討の場を設置。

【２００７年度の主な取組み】
○　ＣＥＰＴＯＡＲ特性把握マップのとりまとめ、情報共有訓練及びＣＥＰＴＯＡＲも参加した官民連携による分野横断的演習を実施。
○　新規追加３分野においてCEPTOARを整備。
○　「「重要インフラ連絡協議会（CEPTOAR-Council)」（仮称）の創設についての基本的な考え方」をとりまとめ。

２－３ 相互依存性解析及び分野横断的な演習の実施

相互依存性解析及び分野横断的な演習については、２００６年度及２００７年度において、それぞれ以下の取組みがなされた。その結果、相互依存性解析については、

重要インフラ分野間における相互依存性に対する認識の共有・共通化が図られるとともに、動的相互依存性解析の実施を通じて重要インフラ事業者間には相互依存関係はあるものの、それぞれに適切な対策が施されていることが判明した。一方で、その対策が時間的経過や状況の変化により対策の想定状況を越えた場合には、サービスの停止や機能の低下に至る可能性があることも確認した。

また、分野横断的演習については、NISC、重要インフラ所管省庁、重要インフラ事業者等、さらにはCEPTOARがそれぞれプレイヤーとして参加し、緊急時における情報共有・情報連絡について、具体的事象を想定したシナリオによる演習を実施し、IT障害発生時における情報共有・情報連絡手法等について確認と検証がなされた。

【２００６年度の主な取組み】

○　各重要インフラ分野の依存関係を可視化できる仕組み（静的相互依存性解析）の構築に向けた試行的な相互依存性解析の実施。

○　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「研究的演習」の実施。

○　具体的なシナリオの下に会議形式で課題を討議する「机上演習」の実施

【２００７年度の主な取組み】

○　「動的依存性解析」の実施、及び「相互依存性解析報告書」の取りまとめ。

○　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「機能演習」の実施。

２－４　総括（行動計画の進捗状況）

重要インフラにおいては、以上のとおり２００５年１２月の現行動計画策定以降、それぞれの分野及び主体において情報セキュリティ対策の向上に向けた取組みがなされてきた。また、２００８年度においても、別表のとおり各施策に取り組まれることとなっており、現行動計画に位置づけられた各取組みは、着実に進捗している。

その結果、個々の重要インフラ事業者等による情報セキュリティ対策については、着実に向上していることが確認できているが、一方で、情報共有体制の有効活用という課題もまだ残っている（「２００６年度の情報セキュリティ政策の評価等」及び「２００７年度の情報セキュリティ政策の評価等」参照）。

３．行動計画見直しに際しての基本的スタンス・視点

今回の行動計画の見直しを進めるにあたっては、上述した現行動計画の下での取組みと成果を踏まえつつ、次期行動計画の下での取り組みが重要インフラにおける情報セキュリティ対策の更なる向上に資するものとなるよう、次のような基本的スタンスに立ち検討作業を行っていくことが必要である。

○　実態を把握した上で現実の具体的な経緯に即した課題の検証を行い、実社会における影響を踏まえた実効性のある内容となるように注意する。その際、技術的視点に偏らないよう留意するとともに、利用者の視点も意識して検討を行う。

○　重要インフラ事業者等の自主的な取組みが大原則であることを踏まえつつ、官民の役割・責任の適切な分担の下で重要インフラにおける情報セキュリティ対策が着実に向上するための枠組みについて検討を行う。

4. 行動計画見直しに当たって検討すべき論点

4－1　本委員会での議論等を通じて認識された課題

本委員会においては、現行動計画策定以降、あわせて１１回の会合を開催し、有識者及び各重要インフラ分野の委員により、情報セキュリティ対策の向上のための取組みについての検討が重ねられてきたところであるが、その議論等を通じ、情報セキュリティ対策を推進するに当たり以下のような課題があることが改めて認識された。

○　各重要インフラ分野において、ＩＴへの依存度（ＩＴの機能不全とサービス低下の距離感)、ＩＴの観点での他分野との相互依存関係などは様々である。それに応じた各分野における取組みにも多様性が存在する。

○　情報セキュリティ対策を考える際には、経営（コスト配分・サービスの維持レベルなど）やコンプライアンス、内部統制の視点も踏まえるべき要素の一つである。

○　重要インフラ事業者等の立場から見ると、「個々の利用者（顧客)」へのサービス提供と「公益」の観点から求められる対応の２つの側面があり、両者は必ずしも常に一致するものではない。

○　IT 障害から重要インフラを防護する観点からは、障害の未然防止だけでなく、障害発生時に影響を最小限に抑えるための対応（早期対応、応急対応など）も重要である。

○　個々の重要インフラ事業者等による情報セキュリティ対策については向上が進んでいるものと考えられる一方で、障害リスクの発生時の情報や、「経験」から得られる知見の共有については、現時点において活発に進んでいるものとは確認できておらず、今後の課題である。

以下において順次整理する具体的な論点に関し、今後検討を進めて行くに当たっては、これらの課題を踏まえた議論が必要である。

４－２ 行動計画の基本的枠組みに関する事項

① 対策の目的（目標)、視点

「重要インフラにおける IT 障害発生ゼロ」よりも適切な目標はあるかといった点や、「未然防止」「拡大防止」「再発防止」のバランスをどう考えるか、いずれかに重点をおくべきか、また、個人情報保護の観点をどう位置づけるべきかといった点について検討が必要である。

これらの点については、本委員会におけるこれまでの議論の過程において、以下のような意見が出されている。

- ＩＴ障害発生をゼロに近づける努力は必要ではあるが、重要インフラ事業者の事業体としての側面から、料金設定や経営資源の配分の問題を鑑みると、目標としては合理的なレベルがあるはずである。
- 重要インフラといえども完璧ではないことを認めることで、ユーザー側の自助の範囲を考えるきっかけになるのではないか。その上で、政府・重要インフラ事業者・ユーザーの役割分担の議論もそろそろ始めるべきではないか。
- 未然防止を目指すことは重要であるが、現実には１００％発生防止は不可能であり、問題発生時に何ができるかについて検討しておく必要がある。
- 「障害が発生しないこと」よりも「重大な障害に至らない」ことの方が大事であり、未然防止よりも拡大防止に力点を置くべきではないか。

② 「重要インフラ分野」の分類、位置づけ

現在の１０分野の分類や位置づけは適切か、実態に即し見直し（分割・追加等）の必要はないかといった点について検討が必要である。

③ 枠組みの柔軟化

IT への依存度、インターネットとの接続（直接・間接)、維持すべきサービスレベル、社会や利用者への影響の度合い、分野間の依存関係、事業規模等を踏まえ、対策の優先度を分野や事業者等単位などで柔軟に考えるべきではないかといった点や、「分野」単位よりも「事業者等」単位の方が進捗しやすい事項もあるのではないかといった点について検討が必要である。

これらの点については、本委員会におけるこれまでの議論の過程において、サービスレベルについては、情報セキュリティ対策の視点ではなく、重要インフラ事業者の幅広い視野の中で検討すべきものであるといった意見や、１つの重要インフラ分野の中であっても、情報資産やその管理方法、起こる事象は様々であり、これらについて一元的に取扱い方を決めるのは不可能ではないかといった意見が出されている。

④ 「重要インフラ事業者等」「重要システム」

行動計画の（別紙１）に掲載されている「重要インフラ事業者等」や「重要システム」について、実態や利用者の観点に即した修正の必要はないか検討が必要である。

この点については、本委員会におけるこれまでの議論の過程において、以下のような意見が出されている。

・「重要インフラサービスの提供を担う重要なシステム」に特化した取組みとすべきである。
・重要インフラのサービスに直接関わるシステムの範囲とすべきであり、その他システムは、一般「企業」としての枠組みの中で論じるべき。
・新たな対象範囲だけでなく、現在の行動計画で定義されているものについても妥当性を再確認する必要がある。

⑤　IT 障害への脅威の例示

現在の脅威の例示は、実態に即して適切か検討が必要である。

この点については、本委員会におけるこれまでの議論の過程において、「国民生活及び社会経済活動に多大なる影響を及ぼす事象」と「利用者の利便性の低下」を明確に区別し、前者について検討すべきではないかとの意見が出されている。

⑥　他の取組みとの関係の整理

情報共有や連携の部分で、防災担当機関や事案対処省庁、その他関係機関の取組みと競合する部分はあるか、補完しあえる部分はどこかといった点や、個々の事業分野における業法との関係で競合する部分はあるかといった点について検討が必要である。

これらの点については、本委員会におけるこれまでの議論の過程において、以下のような意見が出されている。

・障害発生時の対応手順について、先後関係などを前もって議論しておく必要があるのではないか。どれも大事な事項であるがゆえに、それぞれが別々に議論するのではなく、一元的な議論が必要。
・全くの自由市場の中で安全対策を求めるには限界がある。複数の事業者が競合する社会においては、安全対策のための投資が原因で競争に負けてしまう可能性への配慮も必要。重要インフラ事業者に何かを依頼するのであれば、それに応じた法体系や政策的なインセンティブを考えておく必要がある。

⑦　評価の手法

目標、評価指標、対策の進捗度合いの把握方法等について、どう設定すべきか検討が必要である。

この点については、本委員会におけるこれまでの議論の過程において、重要インフラの多様性を考えると、重要インフラ分野全体に対する安全基準の評価は困難であるとの意見が出されている。

4－3 安全基準等の整備

①　「指針」の位置づけ、記載内容の具体性のレベル【重要整理事項】

「指針」に記載される事項について、「安全基準等」に盛り込む「べき」事項と盛り込むことが「望ましい」事項に仕分けをし、その位置づけを明確にすべきではないかといった点や、記載内容の具体性のレベルとして、現在の「指針」より具体的に記述する必要はあるかといった点について検討が必要である。

これらの点については、本委員会におけるこれまでの議論の過程において、具体的な対応の仕方については重要インフラ事業者に任せることとし、国としては「指針」という形でチェック項目を洗い出す、という形が適切ではないかとの意見が出されている。

② 事業者等の PDCA サイクルとの整合性【重要整理事項】

「指針」改定のサイクルや時期について、事業者等の実態に即してどう考えるべきか、また NISC として実態を把握するためにはどのような方法が適切かといった点について検討が必要である。

③ 事業継続計画との関係

「指針」や「安全基準等」に事業継続の観点を補充する必要はないか、盛り込むとすれば、事業継続計画との整合性をどう取るべきかといった点について検討が必要である。

④ リスク開示の在り方

安全基準等において前提とするリスクを開示することについては、リスク管理の観点からどう考えるべきか検討が必要である。

4－4 情報共有体制の強化

① 情報共有の目的等について【重要整理事項】

情報共有体制について、例えば、「IT 障害（リスク）発生時の対応」「経験やベストプラクティスの共有」「一般的な状況認識」など目的や段階に応じて使い分けることを考えるべきではないかといった点や、その前提として、共有が望まれる情報、共有の方法、情報の利用者、利用の仕方、タイミングについて整理すべきではないかといった点について検討が必要である。

これらの点については、本委員会におけるこれまでの議論の過程において、平常時、リスク発生時の重要インフラ間の連携の在り方を考え、整理していくことが今後のメインの検討課題となるのではないかとの意見が出されている。

② NISC の役割について【重要整理事項】

分析機能や「関係機関」との結節点としての機能など、明確化すべき NISC の役割は何かについて検討が必要である。

③ 「情報共有」の障害除去【重要整理事項】

重要インフラにおける情報共有の障害となりうる事象は何か、それを除去するために

有効な方策は何かといった点や、守秘義務や免責等の法律的課題についても検討が必要である。また、現実の情報の流れに照らし、現在の「実施細目」等の仕組みにおいて見直すべき部分はあるかといった点についても検討が必要である。

これらの点については、本委員会におけるこれまでの議論の過程において、所管省庁への報告事項以外の情報を提供することについては、法的責任への波及などの懸念もあり躊躇せざるを得ず、各機関の自主的な努力の範囲内でも一定の成果は上がるかもしれないが、より有意義な情報共有のためには、何らかの工夫が必要との意見が出されている。

④　CEPTOAR について

各重要インフラ分野における主体的取組みの下で、重要インフラにおける情報共有を進めるという観点から、ＣＥＰＴＯＡＲがより有効的かつ効果的に機能するための工夫は考えられないか検討が必要である。

⑤　その他

情報共有体制の充実強化のためには、行動計画上の「関係機関」や、「基幹システム」との連携についても検討すべきではないか、その他連携を検討すべき相手はないかといった点や、IT 障害に至らない、いわゆる「ヒヤリハット」についても共有できるような体制が必要ではないかといった点について検討が必要である。

これらの点については、本委員会におけるこれまでの議論の過程において、災害時のサービス維持、復旧等に向けた人員、機材、自家発電用燃料等の輸送のために極めて重要な役割を持つ「道路インフラ」のサービス維持、復旧状況に関する情報の共有についても検討対象に加えることはできないかとの意見が出されている。

４－５　相互依存性解析・分野横断的演習

①　相互依存性解析の継続について【重要整理事項】

次期行動計画においても、引き続き相互依存性解析を行う意義、目的はあるか、引き続き行うとした場合、実施体制や方法について見直す必要はないかといった点について検討が必要である。また、例えば対象とするシステムを拡げたり、事業復旧計画レベルでの相互依存性を検証するなど、新たな検討項目を追加する必要はないかといった点についても検討が必要である。

②　分野横断的演習の継続について【重要整理事項】

次期行動計画においても、引き続き分野横断的演習を行う意義や目的はあるかといった点や、引き続き行うとした場合、例えば既に行った演習テーマの掘り下げや、演習規模の拡大など、向かうべき方向性についてどう考えるべきか、実施体制や方法について見直す必要はないかといった点について検討が必要である。

③　「事案対処」の観点からの課題検証について【重要整理事項】

分野横断的演習において「事案対処」の観点からの課題について検証する場合、その方法として如何なる方法が適当かといった点について検討が必要である。また、その際には「事案対処省庁」との連携の在り方や課題についての具体的な検討が必要である。

④　その他

解析や演習を行うに当たっては、事業者の意思決定プロセスも踏まえた検証とする必要があるのではないかといった点について検討が必要である。また、他に実施される関連演習との連携や、国際的連携の可能性についても検討が必要である。

4－6 その他

①　NISC の果たすべき役割【重要整理事項】

各重要インフラ分野における情報セキュリティ対策の向上を支援する立場であるNISCに対し、例えば次のような具体的なニーズはないか検討が必要である。

ⅰ）分野間での対策の整合性維持のための情報提供（事業継続計画、事業復旧計画など）

ⅱ）重要インフラ全体としての取組み（公益的側面）に関する個人への広報広聴活動

ⅲ）その他、重要インフラ事業者等の負担を軽減するための支援

この点については、本委員会におけるこれまでの議論の過程において、セキュリティに係るコストに関しては、事業者負担を軽減する措置を講じるような検討が必要との意見が出されている。

②　国際的取組みとの整合性について【重要整理事項】

例えば、OECD における議論の前提となる「重要情報インフラ」という概念と、我が国における「重要インフラ」との関係について、どのように整理すべきか、などの国際的取組みとの整合性についても検討が必要である。

この点については、本委員会におけるこれまでの議論の過程において、欧米における重要インフラの環境・取組みの違いを踏まえ、日本型の重要インフラにおける情報セキュリティ政策とするべきといった意見や、情報セキュリティ対策の向上が「国際競争力」に繋がることなど、重要インフラ事業者にとっての企業環境への配慮も必要ではないかといった意見が出されている。

③　各主体において取り組むべき事項と横断的施策について

内閣官房、各重要インフラ事業者等及び所管省庁、情報セキュリティ関係省庁、事案対処省庁が取り組むべき事項をどのように整理すればよいかといった点や、人材育成、研究開発、地域レベルの取組み促進、国際連携などの横断的施策についてどのように取り組むことが望まれるかといった点について検討が必要である

④　行動計画の推進体制について

次回の見直し期間をどのように設定するのが適当か、今回同様に３年ごとの見直しで問題ないか検討が必要である。

５．行動計画見直し作業のスケジュール

行動計画の見直しは、２００９年２月を目処に現在行われている「第２次情報セキュリティ基本計画」の検討作業と歩調をあわせて行うことが適当であり、２００８年１２月までに政府としての案（パブリックコメントに付すための案）を取りまとめることが目標となる。

今後、本委員会の場で、前節において掲げた論点について具体的に検討を進めることとなるが、見直し作業を効率的に行うためには、論点を「行動計画の枠組みに関わるもの」と「その枠組みの中での具体的な取組みに関するもの」に仕分けし、前者に関する検討を優先的に進めていくことが適当である。具体的には、４－２の各論点及び４－３から４－６に掲げた各論点のうち【重要整理事項】とあるものについて、９月までに一定の結論を得ることを目指し精力的に検討を進めることとする。

また、本文書で整理した論点については、あくまで現時点において具体的な検討が必要と考えられる事項であり、今後の見直し作業の中で新たに検討すべき論点が認識された場合には、積極的にこれを検討していくことが適当である。