資料４

NISC National Information Security Center

「重要インフラの情報セキュリティ対策に係る行動計画」の見直しの論点整理（骨子案）

２００８年 ３月４日

内閣官房 情報セキュリティセンター（NISC）

行動計画見直しに際しての基本的スタンス

基本的スタンス

○　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。

※ **重点整理事項** は、9月までに一定の結論を得ることを目指し優先的に検討すべき事項。

行動計画見直しに当たって検討すべき論点（1）

重要インフラ専門委員会での議論等を通じて認識された課題

○　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。一方で、リスク管理が実質的に必須化してしまうという現実もある。

○　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。

行動計画見直しに当たって検討すべき論点（2）

行動計画の基本的枠組みに関する事項

重点整理事項

○ ***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。
・「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。
・個人情報保護の観点をどう位置づけるべきか。

○ ***「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。

○ ***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。
・「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。

○ ***「重要インフラ事業者等」「重要システム」***

・行動計画（別紙1）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。

○ ***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。

○ ***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。
・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。

○ ***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。

行動計画見直しに当たって検討すべき論点（3）

安全基準等の整備について

重点整理事項

○ ***「指針」の位置づけ、記載内容の具体性のレベル***

・「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。

・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。

○ ***事業者等のPDCAサイクルとの整合性***

・「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。

○ ***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。

○ ***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。

行動計画見直しに当たって検討すべき論点（４）

情報共有体制の強化について

重点整理事項

○ *情報共有の目的等について*

・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。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。

○ *NISCの役割について*

・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。

○ *「情報共有」の障害除去*

・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。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はないか。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。

○ *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。

○ *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。

・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。

行動計画見直しに当たって検討すべき論点（5）

相互依存性解析･分野横断的演習について

重点整理事項

○ ***相互依存性解析の継続について***

･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。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。

○ ***分野横断的演習の継続について***

･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、目的はあるか。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。併せて実施体制や方法について見直す必要はないか。

○ ***「事案対処」の観点からの課題検証について***

･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。その際「事案対処省庁」との連携の在り方や課題について具体的に検討しておく必要があるのではないか。

○ ***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。

･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すべきではないか。

行動計画見直しに当たって検討すべき論点（6）

その他

重点整理事項

○ ***NISCの果たすべき役割***

・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、具体的なニーズはないか。例えば、次のようなニーズはどうか。

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

○ ***国際的取組みとの整合性について***

・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。

○ ***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。

・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。

○ ***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。