資料２－１

重要インフラ分野における情報セキュリティ対策向上の取組みについて（案）

重要インフラ専門委員会

（１）重要インフラにおける情報セキュリティ対策の取組み方針

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。このような安全対策は、一義的には各重要インフラ事業者等が担うべきものであるが、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、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を開始し、継続的な見直しと改善を通じて、情報セキュリティ対策の向上を図っていくというアプローチが妥当との判断に立ち、「重要インフラの情報セキュリティ対策に係る行動計画」（以下「行動計画」という。）が本委員会で検討され、情報セキュリティ政策会議において２００５年１２月１３日に決定されたところである。

行動計画においては、重要インフラ関係の４本の施策の柱（①安全基準等の整備　②情報共有体制の強化　③相互依存性解析の実施　④分野横断的な演習の実施）と、各主体における取組み項目を示し、各項目ごとにアクションプランとして具体化を図ることにより、重要インフラの情報セキュリティ対策の向上につなげていくことにしている。その実現に向けては、重要インフラ事業者等の自主的な対策や、内閣官房を中心とした政府及び各重要インフラ分野における施策が、官民の緊密な連携を通じて、各々の役割に応じた責任の下で取り組まれることが原則である。

（２）２００９年の目指すべき「姿」

重要インフラにおける情報セキュリティ対策の目指すところとしては、「第一次情報セキュリティ基本計画」（２００６年２月２日・情報セキュリティ政策会議決定）（以下「第一次基本計画」という。）において、「２００９年度初めには、重要インフラにおける IT 障害の発生を限りなくゼロにすること」としている。

ここで「重要インフラにおける IT 障害の発生を限りなくゼロにすることを目指す」とは、すなわち、「IT 障害の発生を可能な限り未然に防止するために必要な対策、及び、IT 障害が発生した際の影響を可能な限り極小化するために必要な対策が常に適切に講じられている社会を目指す」ことであり、重要インフラ分野におけるサービスの安定的供給機能を維持しつつリスクに適切に対応する社会を目指すことである。

そのような社会の特徴を挙げれば、以下のとおりである。

（A）自らの情報セキュリティ対策が十分であるか、各重要インフラ事業者等による自己検証がなされている。

（B）IT 障害の未然防止、拡大防止・迅速な復旧、再発防止の３つの側面において重要となる情報について、官民の各主体間で情報共有、連絡・連携がなされている。

（C）重要インフラ分野間における IT 障害に関する相互依存関係を踏まえ、重要インフラ分野での対応が適切になされている。

また、
（D）単にある時点において十分な対策がとられていることだけでなく、検証や見直し、さらなる強化に向けた取組み等の情報セキュリティ対策の向上に向けた取組み（すなわち PDCA サイクル）が、官民連携して継続的に行われている
ことも重要な特徴である。

（３）評価のための指標

冒頭に述べたとおり、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。そのため、重要インフラの情報セキュリティ対策については、第一次基本計画及びその具体的取り組みについて定めた行動計画に従って、官民の緊密な連携の下で、情報セキュリティ対策の強化を目指しているところである。

これらの取組みは、いずれも IT 障害の発生を可能な限り未然に防止するために必要な対策、及び、IT 障害が発生した際の影響を可能な限り極小化するために必要な具体的対策であり、それぞれの取組みが（２）に述べた目指すべき社会につながるものである。よって行動計画に定める取組みの進捗度合いをみることで「重要インフラ分野におけるサービスの安定的供給機能の維持とリスクへの適切な対応」の実現度合いを把握することができる。

以上のことを勘案し、重要インフラ分野における情報セキュリティ対策の評価は、対策向上を目的に行動計画で定めた４本の施策の柱それぞれについて、各年度ごとの目標（具体的取組み）に対する実施状況を把握し、その進捗度合いを指標とすることにより、サービスの安定的供給機能の維持とリスクへの適切な対応の実現度合いを把握して行うこととする。

また、これとは別に、IT 障害が実際に発生した場合には、各関係主体（内閣官房、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野の CEPTOAR 等）が、IT 障害に応じ、情報共有体制も活用しながら、要因や課題等の分析を行い、得られた知見を情報セキュリティ対策の向上へ活用する。

（４）情報セキュリティ対策向上に向けて

重要インフラ分野における情報セキュリティ対策の評価は、目標として設定した具体的取組みに対する進捗状況について、内閣官房において取りまとめた報告をもとに重要インフラ専門委員会で行うこととなる。さらに同委員会においては、報告された実施状況や実際の IT 障害の発生状況等も踏まえながら、行動計画に掲げられている取組みの着実な進捗を確保することに留意しつつ、次年度における目標を設定する。

これにより、毎年度の評価を通じて、行動計画に掲げた取組みの着実な進捗を目指し、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目指すものである。

また、国民生活、社会経済活動における IT の利用は引き続き進展や拡大が予想されること、加えて IT 障害を発生させる要因や脅威は常に変化し続けるものであることから、重要インフラ分野における情報セキュリティ対策については、２００９年以降も継続的にその向上に取り組んでいくことが必要である。

そのため、行動計画については、「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ヶ月掛けて見直す）又は必要に応じ、見直しを行う」（行動計画８（２））こととなっている。

行動計画の見直しに当たっては、４本の施策の柱の進捗度合いや発生したIT障害の分析に加え、内閣官房として、各重要インフラ所管省庁の協力を得て、重要インフラ分野における情報セキュリティ対策向上の状況について以下の各点を含めた調査・把握を行い、また分野横断的な演習で得られた知見等も活用して、次なる対応の必要性を検討する。

○「安全基準等」の策定・見直しや、それを踏まえた情報セキュリティ対策の実施状況等、各重要インフラ分野における取り組みの状況を把握する。

○官民の情報提供・連絡体制、CEPTOAR、CEPTOAR-Council（仮称）を通じた、官民の各主体間の情報連絡・共有、連携の状況を把握する。

○重要インフラ分野間における IT 障害に関する相互依存関係を踏まえた、重要インフラ分野での対応の状況を把握する。