資料２

重要インフラの情報セキュリティ対策に係る基本的考え方

平成１７年９月１５日
情報セキュリティ政策会議決定

１　目的

重要インフラの情報セキュリティ対策に係る基本的考え方（以下「基本的考え方」という。）の目的は、IT 戦略本部情報セキュリティ専門調査会情報セキュリティ基本問題委員会第２次提言（平成 17 年 4 月 22 日）（以下「第２次提言」という。）を踏まえ、重要インフラの各事業において発生する障害（サービスの停止や機能の低下等）のうち IT の機能不全が引き起こすもの（以下「IT 障害」という。）から重要インフラを防護し、重要インフラ事業者の事業継続性を確保するための取るべき対策について基本的方向性を示すことにある。

そして、重要インフラ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ため、今年末を目処に、この基本的考え方に基づいて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いて実施すべき施策を個別化・具体化した「重要インフラの情報セキュリティ対策に係る行動計画（仮称）」（以下「行動計画」という。）を策定し、官民の緊密な連携の下、重要インフラの情報セキュリティ対策を強化することとする。

具体的には、現行の特別行動計画及びこれに基づく取組みを発展・強化させた新たな行動計画を取り纏めることとする。

２　これまでの対策とその問題点

これまで、重要インフラにおける情報セキュリティ対策については、平成 12 年 12 月に取り纏められた「重要インフラのサイバーテロ対策に係る特別行動計画」（以下「特別行動計画」という。）等に基づいて取り組んでいる。

特別行動計画の策定当時においては、既に、産業や政府の多くの機能が情報システムに依存するようになってきており、更に加速的な情報化・ネットワーク化の進展が見込まれていた。このような状況において、特別行動計画は、情報通信ネットワークや情報システムを利用した電子的な攻撃（以下「サイバー攻撃」という。）という社会の IT 化に伴う新たな脅威から重要インフラを防護するための、我が国として初めての官民協力の枠組みとして一定の役割を果たしたといえる。

しかし、特別行動計画が策定された平成 12 年当時から比べると、IT の利用度はさらに高まっており、各事業において、IT 障害によるサービスの停止や機能の低下等が発生する危険性はますます大きくなってきている。このような IT 障害は、サイバー攻撃等の意図的要因だけではなく、人為的ミスなどの非意図的要因や地震・津波などの自然災害など、多種多様な原因によって発生しうるものである。

かかる現状を踏まえれば、IT 障害から重要インフラを防護するためには、従来のようにサイバー攻撃のみを脅威の中心に据えるのでは不十分であり、想定する脅威について見直すことが必要である。

また、重要インフラの情報セキュリティ水準の向上については、これまでは重要インフラ事業者及び地方公共団体（以下「重要インフラ事業者等」という。）がそれぞれリスク分析や情報セキュリティポリシーの策定などの取組みを実施することを基本とし、政府は、その向上に資するため、各事業者等の取組を支援するという立場であった。

しかし、重要インフラは互いに依存しあっており、個別の取組では対応が難しい問題も拡大していることから、我が国全体として重要インフラにおける情報セキュリティ水準を向上させていくという観点からは、例えば重要インフラ相互間の依存性解析や分野横断的演習を行うなど、重要インフラ横断的な総合的対策を強化することが必要となってきている。

さらに、重要インフラの IT への依存度が更に高まりつつある状況を踏まえれば、従来の情報共有の体制を拡充・強化するなど、重要インフラ防護をより一層強化することが必要なのはもちろんである。

3　対象範囲

(1) 対象範囲等の見直し

情報セキュリティ対策を推進すべき重要インフラの範囲を定めるにあたっては、そもそも重要インフラとは何かを定めることが必要である。そこで、今後は、第２次提言を踏まえ、重要インフラを「他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状況に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるもの」と定義する。

1) 対象分野の見直し

行動計画に基づいて対策を推進すべき対象分野としては、このように定義する重要インフラのうち、そのサービスの提供が情報システムに大きく依存しているため、IT 障害についての総合的な取組みが必要と考えられる分野とする。具体的には、従来重要インフラ分野とされてきた「情報通信」、「金融」、「航空」、「鉄道」、「電力」、「ガス」、「政府・行政サービス（地方公共団体を含む）」に加え、新たに、「医療」、「水道」、「物流」を追加する。

なお、政府・行政サービス（地方公共団体を含む）のうち、国に関する部分については、「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」（平成 16 年 12 月 7 日 IT 戦略本部決定）を踏まえた情報セキュリティ対策を推進する。

2) 対象とする事業の見直し等

今年末を目処に、今般新たに追加された重要インフラ分野においては、その対象とする事業を定めるとともに、従来の重要インフラ分野においても、事業選定当時からの事業環境の変化及び IT への依存度の進展等を踏まえ、対象とする事業の見直しを行うこととする。

なお、「重要インフラ」となる対象分野及び対象事業については、今後も、IT の進展・利用拡大及びその事業環境への影響等の変化に対応して不断の見直しを継続する。

(2) 想定する脅威の見直し

IT 障害を引き起こす脅威には、サイバー攻撃等の意図的要因だけでなく、システム障害や人為的なミス、あるいはアウトソーシング等の情報技術の適用方法の変化に伴う構造的な脅威等の非意図的要因、さらには地震・津波などの自然災害など、多種多様なものが考えられる。

したがって、基本的考え方においても、これら多種多様な脅威の全てを想定する脅威とする。

(3) 新たに重要インフラとなる対象分野及び対象事業の取り組みの推進について

IT の進展・利用拡大及びその事業環境への影響等の変化により、新たに重要インフラとなる対象分野及び対象事業については、施策実施のための準備

期間等を勘案しつつ、出来るだけ早い時期に、基本的考え方を踏まえた施策を実施すべく取り組むこととする。

４　情報セキュリティ水準の向上のための具体的対策

従来、重要インフラにおける情報セキュリティの確保、IT 障害発生時の原因分析・復旧等は個々の分野毎に実施されてきたところであるが、各重要インフラにおける IT 利用が進展するにつれ、重要インフラ相互の依存関係が増大しつつある。

このため、各重要インフラ分野や事業において、サービスを阻害する原因となる IT 障害への対策を確実に実施することはもちろんのこと、他の分野や事業への波及を防ぐため、分野内及び分野間での対策レベルの格差を最小限にするなど、統一的な防護策を推進することが重要である。

なお、防護策の推進にあたっては、重要インフラ分野や事業ごとに、IT への依存度、国民生活や社会経済活動への影響の程度、事業の形態等により、情報セキュリティ対策として求められる適切なレベルは異なるものであることに留意するものとする。

(1) 分野横断的な状況把握（相互依存性解析等）の実施

相互依存性が高まる中、我が国全体としての重要インフラ対策を向上させていくためには、分野横断的な状況の把握が不可欠である。

このため、それぞれの重要インフラに起こりうる脅威が何であるかを把握するとともに、ある重要インフラに IT 障害が生じた場合に、他のどの重要インフラに影響が波及するかという相互依存性の把握が必要であり、平成 18 年度末を目処に、重要インフラ横断的な状況把握（相互依存性解析等）を実施することを検討する。

(2)分野毎の「安全基準・ガイドライン」の作成・評価

サービスを阻害する原因となる IT 障害への対策を確実に実施していくため、内閣官房により作成される重要インフラ横断的な「安全基準・ガイドライン」策定のための指針を踏まえ、内閣官房の支援の下、重要インフラ所管省庁及び重要インフラ事業者等が協力し、重要インフラ分野毎に、遅くとも平成 18 年９月末を目処に、技術的基準及び運用基準についての「安全基準・ガイドライン」の策定・見直し等を行うこととする。

なお、「安全基準・ガイドライン」は、最低限講ずべき対策のレベルを示

すものを基本とするが、各重要インフラ分野ごとの特性に応じ、望ましい対策レベルを示す推奨ガイドラインとして策定する場合もあり得る。

さらに、当該「安全基準・ガイドライン」が想定される脅威と比して相当のものであるか検証するため、相互依存性解析に基づいた評価等を内閣官房及び重要インフラ所管省庁が共同して実施する。

５　官民の連絡・連携、情報共有体制の強化とその実効性の確保

重要インフラのサービスの維持・復旧については、一義的には重要インフラ事業者等が責を担うものであるが、各事業者がサービスを維持・復旧することがより容易になるよう、官民の各主体が協力することが重要である。

中でも、IT 障害に関する情報については、1) IT 障害の未然防止、2) IT 障害の拡大防止・迅速な復旧、3) IT 障害の要因等の分析・検証による再発防止の３つの側面がそれぞれにおいて重要であり、政府等は重要インフラ事業者等に対し適宜・適切に提供し、また事業者間においてはこれら情報を共有する体制を強化することが必要である。

また、このような官民の情報共有、連絡・連携のための仕組みについては、その妥当性を確保するため、平時においても各主体の連携状況を分野横断的演習などを通じて模擬的に検証し、緊急時の対応力を強化していくと同時に、必要な場合には仕組みの見直しにつなげていくことが重要である。

なお、このような情報共有体制の実現・強化のためには、既に各主体が有する機能を最大限活用するとともに、各主体の役割を明確化し、また特定の主体に過度の負担が発生しないよう配慮する必要がある。

(1) 情報共有体制の強化

1) 重要インフラ分野内での情報共有強化

各重要インフラ分野内の情報共有を促進し、当該分野全体における取組の底上げを図るため、遅くとも平成 18 年度末を目処に、重要インフラ事業者等を主体とした「情報共有・分析センター（ISAC: Information Sharing & Analysis Center) 」（仮称）等の各分野内情報共有機構の創設を図るなど、情報共有体制の整備を推進する。

その際、当面、内閣官房を中心とする情報提供・共有体制を可能な限り早期に稼働させるため、当該機構の検討に当たっては、以下の機能を備える必要がある。

○　外部への情報提供及び機密保持に関し、構成員間で合意されたルール

が存在すること

○　緊急時に各構成員及び外部との連絡が可能な窓口（POC: Point of Contact）が設定されていること

なお、将来的には、情報集約及び情勢判断を行う能力があるコーディネータが配置されることが望ましい。

2) 重要インフラ事業者等に対する情報共有体制の整理・強化

以下の図の通り、特別行動計画に基づく情報提供の枠組みを拡大・発展させることとし、内閣官房において体系的な情報の集約・整理等を行い、重要インフラ事業者等に対して情報を提供する体制を整理・強化する。

○　各主体は、それぞれの保有する能力・機能に応じ、重要インフラ事業者等に提供すべき情報（テロ関連情報、脅威等に関する情報、攻撃手法及び復旧手法に関する情報等）を収集する。

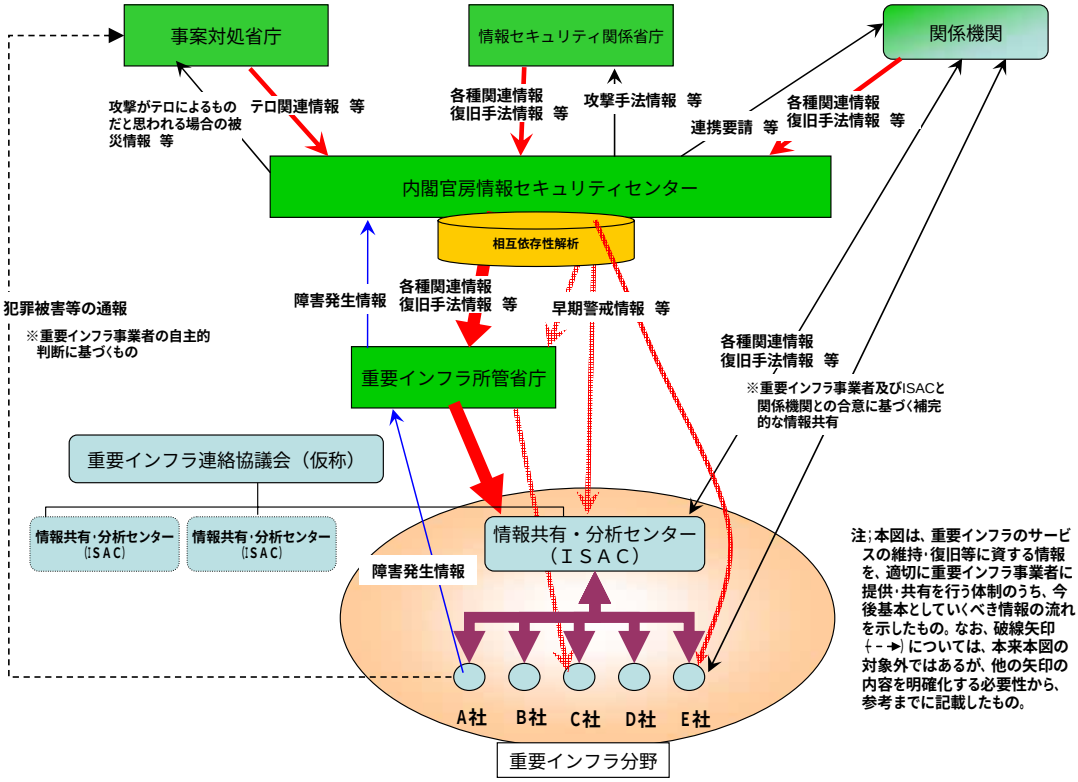
○　各主体が収集した情報は、内閣官房に集約するとともに、内閣官房において当該情報を体系的に整理する。

　また、情報の整理に当たっては、情報参照者が当該情報の活用が容易となるよう、その重要度や種類、性格等に応じた情報の流れが一目で認識出来るよう、体系的な識別方式を採用することとする。

○　内閣官房は、集約・整理した情報を、原則として重要インフラ所管省庁を通じ、重要インフラ事業者等に対して提供する。

　また、重要インフラ所管省庁は、基本的には、各分野の運用に関し直接的な知見を有する分野内の情報共有体制を通じて、各重要インフラ事業者等に情報提供を行う。

○　各重要インフラ事業者等や各重要インフラ分野内の情報共有機構が、当該組織の IT の利用形態に合わせた詳細な情報など、上記体制による提供情報を補完する情報の入手を希望する場合、関係機関との合意による契約等に基づき直接情報共有を行うこととする。



図：情報提供・共有体制のイメージ

3) 分野横断的な情報共有の強化

重要インフラ事業者等側においても、平成 18 年度末までを目処に重要インフラ分野横断的な情報共有機構（「重要インフラ連絡協議会」（仮称））の整備を推進する等により、分野横断的な情報共有の推進を図り、多様な知見をサービスの維持・復旧に活かすこととする。

4) IT 障害等に係る情報に関する連絡体制の強化及び情報の充実

ＩＴ障害全般を射程に入れていくことに対応するとともに、重要インフラ分野間の相互依存性に基づいた IT 障害発生に係る情報提供を適切に実施するため、事業者からの提供情報の範囲について見直しを行う。

なお、事業者がより積極的に情報提供が出来るような環境整備について引き続き検討する。

(2) 連絡・連携する「情報」の充実及び質の向上

重要インフラ事業者等に提供すべき情報の質の強化を図るため、内閣官房と、情報セキュリティ関係省庁、事案対処省庁及び関係機関との間で情報収

集のための連携の強化を図る。

内閣官房から各重要インフラ事業者等に対し情報提供を実施するに当たっては、当該情報について的確な分析を行った上で、相互依存性解析等による優先度設定に基づき、提供情報の取捨を各重要インフラ分野毎に行う。また、平成 17 年度末を目処に、脆弱性情報等の早期警戒情報提供（優先的情報提供を含む）のための枠組みを整備する。

(3) IT 障害発生時対応の強化

平成 17 年度末を目処に、各重要インフラ事業者等の業務量の最小化を図ることを目的として、IT 障害発生時等緊急時に重要インフラ分野間のコーディネーションを実施できる機能を内閣官房に整備するとともに、重要インフラ所管省庁から重要インフラ事業者等への支援、助言等の機能を強化する。

なお、将来的には、個別重要インフラ分野における事業者間のコーディネーションを実施できる機能を情報共有機構内に構築することが望ましい。

(4) 分野横断的演習を通じた機能・体制の検証と見直し

1) 類型化された脅威シナリオに基づく分野横断的演習の実施

想定される脅威の拡がりに対応した具体的脅威シナリオの類型を下に毎年度ごとにテーマを設定し、各重要インフラ事業者等、各重要インフラ分野内の情報共有機構の協力を得て行う重要インフラ横断的な演習を行うこととし、第１回演習を平成 18 年度中を目処に企画・実施することを検討する。

2) 分野横断的演習結果を踏まえた対応能力の向上

分野横断的演習の結果を踏まえ、情報共有及び連絡・連携体制の見直しを行うとともに、各重要インフラ所管省庁の対応能力の向上に反映させる。

６　情報セキュリティ基盤の強化

重要インフラの情報セキュリティ対策を推進するため、人材の育成、研究開発等の情報セキュリティ基盤の構築を進めることが必要である。

(1) 人材育成・研究開発

1) 専門性を持った人材の育成

高等教育機関（大学院等を中心）において、他分野の学生・社会人を相互に受け入れる交換枠を設けるなど、多面的能力を有する人材を育成する制度やリカレント教育のあり方を検討する。

また、演習・訓練及びセミナー等を通じて、重要インフラ所管省庁及び重要インフラ事業者等を中心に、高度な IT スキルを有する人材の育成を図る。

2) 成果の利用を念頭においた研究開発の推進

情報セキュリティに関する研究開発・技術開発戦略の立案に際し、重要インフラにおける IT 障害の原因となりうる「IT の機能不全」への対策全体に資する視点を付与することにより、日々進化する脅威への対応能力の強化に資する研究開発を促進する。

(2) 事案対処省庁の取組の強化

５(2) で述べたとおり、事案対処省庁においても、内閣官房、情報セキュリティ関係省庁及び関係機関との間で情報収集のための連携の強化を図るほか、事案の原因究明、事案の対処、被災者に対する支援等、各事案対処省庁における取組みを継続的に実施・強化することとする。

(3) 地域レベルの取組みの促進

重要インフラにおける情報セキュリティ対策は政府レベルだけではなく、我が国全土にわたって講じられるべき問題であることから、関係する政府地方支分部局、地方公共団体、重要インフラ事業者及び地方の情報セキュリティ関係組織間での情報共有及び連絡・連携の体制を、政府の体制と連動する形で平時より整備し、政府は相互依存性解析に基づく適切な情報提供等により現場での連携活動を支援することとする。

(4) 国際連携

政府は、OECD や G8 等の国際的な枠組みにおけるサイバーテロ対策に関連する取組みに対する協力を推進する。

また、政府及び重要インフラ事業者等は、国外の情報セキュリティ関係団体等からの情報収集に努めるほか、重要インフラ防護のための早期警戒・監視・警報ネットワーク等へ積極的に参加すること等により、諸外国の関係機関との情報交換や共同訓練等の国際的な連携を強化する。

７　詳細検討の実施

(1) 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策定

今後、重要インフラの情報セキュリティ対策を具体化するため、この基本的考え方に基づき、別添の事項をその内容とする行動計画を平成 17 年末を

目処に策定する。

また、この行動計画については、その進捗を踏まえ、３年毎（策定から２年後、実施状況を踏まえ 12 ヶ月かけて見直す）又は必要に応じ、見直しを実施するものとする。

(2) 重要インフラ専門委員会の設置

重要インフラの情報セキュリティ対策に係る具体的施策の検討を行う機関として、「重要インフラ専門委員会」を、情報セキュリティ政策会議の下に、専門委員会として設置する。

重要インフラ専門委員会は、重要インフラ事業者の代表及び情報セキュリティに関する有識者から構成する。

別添

行動計画に盛り込むべき事項（案）

１　目的

２　対象範囲
(1) IT 障害の例示
(2) 対象となる事業者の同定
(3) 対象となる重要システムの例示
(4) 想定される脅威の例示

３　相互依存性解析
(1) 相互依存性解析の目的、アウトプットイメージ
(2) 実施主体
(3) 実施方法
(4) 実施間隔

４　「安全基準・ガイドライン」の作成・評価
(1) 位置づけ（業法との関係等）
- 最低限講ずべきレベルを示すものとするのか、望ましい対策レベルを示す推奨ガイドラインとするか。

(2) 評価・検証方法
(3) 評価・検証を実施する間隔

５　情報共有体制の強化
(1) 連絡体制の見直し
- 平常時、事案発生時及び再発防止における情報共有のあり方
- 内閣官房副長官補室（安全保障・危機管理担当）、内閣府防災担当との機能の分担・整理　等

(2) 情報連絡の対象となる事案
(3) 情報の整理・取扱い

６　情報共有・分析センター（仮称）
(1) 目的・機能・役割
- 共有すべき情報の種類・質
- 平常時、事案発生時及び再発防止時それぞれにおける役割

(2) 上記目的等を実現するために求められる要件
- ３要件　等

(3) 設置に当たっての所管省庁の関与のあり方
(4) 設立の方法及び手順

- 新組織を設立、既存の組織の活用　等

７　重要インフラ連絡協議会（仮称）
(1) 組織の位置づけ
(2) 目的・機能・役割
- 共有すべき情報の種類・質
- 平常時、事案発生時及び再発防止時それぞれにおける役割
- 各「情報共有・分析センター」（仮称）間の総合調整
- 相互依存性解析の実施
- 分野横断的総合演習における事業者側のとりまとめ組織
(3) 設立の方法及び手順

８　分野横断的な演習
(1) 具体的脅威シナリオの作成方法
(2) 実施主体、実施体制

９　各主体において取り組むべき事項と横断的施策
(1) 内閣官房が取り組むべき機能
(2) 各重要インフラ事業者及び重要インフラ所管省庁において取り組むべき事項
(3) 情報セキュリティ関係省庁において整備・強化すべき機能・体制
(4) 事案対処省庁において整備・強化すべき機能・体制
(5) その他関係省庁・関係機関において取り組むべき事項
(6) 人材育成、研究開発の方向性（詳細は施策パッケージに盛り込む）
(7) 国際連携のあり方

10　行動計画の推進体制
(1) 実施状況の評価・検証
(2) 行動計画の見直し