第２次提言

我が国の重要インフラにおける情報セキュリティ対策の強化に向けて

平成１７年４月２２日

高度情報通信ネットワーク社会推進戦略本部
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

目次

はじめに

平成12年2月に定められた高度情報通信ネットワーク社会形成基本法は、高度情報通信ネットワーク社会を、「インターネットその他の高度情報通信ネットワークを通じて自由かつ安全に多様な情報又は知識を世界的規模で入手し、共有し、又は発信することにより、あらゆる分野における創造的かつ活力ある発展が可能となる社会」と定義し、すべての国民が情報通信技術の恵沢を享受できる社会であること、経済改革の推進及び国際競争力が強化されること、ゆとりと豊かさを実感できる国民生活を実現すること、さらに、活力ある地域社会の実現及び住民福祉の向上という4点を、高度情報通信ネットワーク社会形成において実現すべき要件として明確に掲げている。さらに第九条（社会経済構造の変化に伴う新たな課題への対応）は、

「高度情報通信ネットワーク社会の形成に当たっては、情報通信技術の活用により生ずる社会経済構造の変化に伴う雇用その他の分野における各般の新たな課題について、適確かつ積極的に対応しなければならない。」

と定めている。本法律が成立して5年が経過したが、まさにこの IT の活用により生ずる社会経済構造の変化が、我が国のほぼ全ての領域において同時並行的に進行している。これにより、総体として数年前の我が国の状況とは比較できないほどの変化をもたらす一方で、数多くの新たな課題も顕在化してきており、今こそ課題解決に対する積極的な取組みが急務となってきている。

取り組むべき新たな課題のうち、多くの有識者、実務家等が、情報セキュリティへの取組み強化を指摘している。さらに高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）における議論においても、情報セキュリティに対する一層の推進を掲げ、特に「安全・安心」をキーワードとして多種多様な取組みを展開しているところである。

我が国の国民生活と社会経済活動が大きく依存する重要インフラ領域における情報セキュリティへの取組みは、平成12年12月に取りまとめられた「重要インフラのサイバーテロ対策に係る特別行動計画」に基づいて、官民の活動が展開されてきた。しかしながら、重要インフラ事業における IT 活用の更なる進展、重要インフラ事業に係る相互依存性の必要性が増す中で、最近の大規模システム障害発生の現状を省みると、原因として、単にサイバー攻撃だけではなく、IT に立脚する脅威全般を認知する必要があり、それに対する重要インフラ防護を設計することが極めて重要な課題となってきている。欧米諸国において確立した、重要インフラ防護（CIP: Critical Infrastructure Protection）、あるいは、重要情報インフラ防護（CIIP: Critical Information Infrastructure Protection）の考え方を、我が国の状況を的確に反映した形で取りまとめ、その考え方に基づいた具体的かつ合理的な情報セキュリティ対策を官民連携の下に積極的に展開していくことが必要である。

このような認識から、情報セキュリティ基本問題委員会では、平成16年10月より、重要インフラ防護のための中長期的政策と官民連携のあり方について議論を重ねてきた。さらに、本委員会の下に、重要インフラ事業者、テロ対策の専門家、IT 関連の専門家等からなる第2分科会を組織し、「第2次提言」の素案作成を依頼した。本提言は、第2分科会が作成した

素案に対し、さらに情報セキュリティ基本問題委員会における検討結果を付加したものである。

本委員会としては、この第2次提言を受けて、政府が重要インフラ防護の考え方を、情報セキュリティ、安全保障・危機管理及び防災等を実行する各関係機関と共に確立し、同時に重要インフラにおける具体的かつ実効性のある情報セキュリティ対策の実施を促進し、重要インフラが提供するサービスに対する障害の未然防止、障害発生時の障害影響領域の最小化と迅速な復旧、加えて、発生した障害の原因究明と得られた知見の再利用を積極的に行いながら障害の再発防止及び重要インフラの事業継続性の確保に活かしていく体制を、我が国に実現していくことを切に願う。

平成17年4月22日

高度情報通信ネットワーク社会推進戦略本部
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委員長
金 杉 明 信

情報セキュリティ基本問題委員会委員名簿

【委員長】

金杉　明信　　日本電気㈱代表取締役 執行役員 社長

【委員】

伊藤　泰彦　　KDDI㈱取締役(執行役員専務)＜委員長代理＞

後藤　滋樹　　早稲田大学教授

寺島　実郎　　㈱三井物産戦略研究所所長

中村　直司　　㈱NTT データ代表取締役副社長

村井　純　　慶應義塾大学教授

(五十音順)

情報セキュリティ基本問題委員会第2分科会委員名簿
(重要インフラにおける情報セキュリティ対策強化検討分科会)

【座長】

浅野正一郎	情報･システム研究機構　国立情報学研究所教授

【委員】

石幡　吉則	電気事業連合会情報通信部長
板橋　功	(財)　公共政策調査会第一研究室長
稲垣　隆一	弁護士
大場　満	東京地下鉄(株)　鉄道本部安全･技術部長
雄川　一彦	日本電信電話(株)　第二部門担当部長
喜入　博	KPMG ビジネスアシュアランス(株)　顧問
郡山　信	(財)　金融情報システムセンター監査安全部長
小林　俊徳	(社)　日本ガス協会技術部長
土居　範久	中央大学　理工学部教授
中尾　康二	KDDI(株)技術開発本部情報セキュリティ技術部長
廣川　聡美	横須賀市企画調整部情報政策担当部長
前川　徹	早稲田大学　国際情報通信研究センター客員教授 ／(株)　富士通総研主任研究員
松尾　明	中央青山監査法人代表社員
三輪　信雄	(株)　ラック代表取締役社長
森田　元	(株)　日本航空 IT 戦略企画室部長
渡辺　研司	長岡技術科学大学　経営情報系助教授

(五十音順)

第1章　重要インフラにおける情報セキュリティ対策の基本理念

我が国が構築を進める高度情報通信ネットワーク社会では、社会のすべての領域において情報技術（IT）の利用を積極的に進め、国民生活、社会経済活動に活力を与え、高い生産性を保持し、ひいては力ある社会を形成していくことを目標としている。このプロセスを健全に、かつ、確実に進めるためには、情報セキュリティについての確固たる政策とその着実な実施が重要である。高度情報通信ネットワーク社会推進戦略本部（以下、「IT戦略本部」とする）においても、従前より情報セキュリティへの取組み強化が議論されてきた。本章では、特に政府が取り組む情報セキュリティ政策において、本提言が対象とする重要インフラにおける情報セキュリティ対策をなぜ強化しなければならないのか、重要インフラにおける情報セキュリティ強化の方向性、そして、その基本理念についてまとめる。

1．1．重要インフラにおける「情報セキュリティ」に関する現状認識

1．1．1．社会のIT化

近年の我が国のIT化の進展は、誰の目からも明らかに、急速に変化を遂げている状況にある。平成12年からのe-Japan戦略[1]、さらにe-Japan 戦略Ⅱ[2]によって官民一体になって進められてきた高度情報通信ネットワーク社会形成は着実に進められている。特に、行政活動の効率化と生産性向上のための政府、地方公共団体におけるITの積極的利用は言うまでもなく、民間企業においても景気低迷の中での生産性向上や収益率改善のためにITがさまざまな領域に応用されている。また、インターネットを中心とする基盤環境の急速な整備は目を見張るものがあり、諸外国と比較しても、最も安価に、最も広い帯域を個人、企業が思う存分利用できる環境が構築されてきた。これにより、個人生活や社会経済活動も、IT を活用するのが極めて自然な行為になっている。これは、近年の急激な電子商取引の拡大、さまざまな重要データをインターネット経由で交換するシステムの拡がりに見ることができる。また、平成17年2月には、e-Japan 戦略 Ⅱ の最終年に、その取組みを確固たるものにするために政策パッケージが取りまとめられ[3]、高度情報通信ネットワーク社会形成の、いわばラストスパートに政府が取り組む。これにより、より多くの領域でのIT化が促進されることは言うまでもない。

---

[1] e-Japan戦略（平成13年1月22日IT戦略本部決定）
（http://www.kantei.go.jp/jp/singi/it2/kettei/010122honbun.html）

[2] e-Japan戦略II（平成15年7月2日IT戦略本部決定）
（http://www.kantei.go.jp/jp/singi/it2/kettei/030702ejapan.pdf）

[3] IT政策パッケージ－2005―世界最先端のIT国家の実現に向けて―（平成17年2月24日IT戦略本部決定）
（http://www.kantei.go.jp/jp/singi/it2/kettei/050224/050224pac.html）

一方、国民生活と社会経済活動が、一層 IT に依存する状況が拡がるほど、IT そのものが依存可能な基盤になるための官民の努力が必須である。また、数多くの個人情報漏洩、国民生活に多大な影響を与えた情報通信システム障害、情報システムと情報資産の集中と拡大を受けて、我が国の様々な領域での情報セキュリティ対策の充実に対する社会的要請を強める状況を生み出している。

1.1.2. これまでの情報セキュリティ基本問題委員会の取組み

政府は、平成16年7月27日、IT戦略本部情報セキュリティ専門調査会の下に「情報セキュリティ基本問題委員会」を設置し、IT 社会の基盤となる情報セキュリティに関する基本的な課題について、専門家の知見を集約して「国家としてのグランドデザイン」を策定するとともに、実施可能な対策について優先順位を付して具体的に提示するための検討を、集中的に行っている。

その中で、まず、1) 情報セキュリティ政策全般の実行体制のあり方、2) 政府自身の情報セキュリティ対策のあり方の2つの課題について検討を行い、平成16年11月16日に「第1次提言」[4]としてとりまとめ、IT 戦略本部に提示した。この中で、政府機関、重要インフラ、企業、個人における情報セキュリティへの取組みを、より戦略的かつ体系的なものとし、バランスと実効性をもった政策の実施が重要であるということを提示し、1)「情報セキュリティ政策会議（仮称）」と、2)「国家情報セキュリティセンター（仮称）」の設置を提言した。

これを受け、平成16年12月7日には、IT戦略本部において、1)「情報セキュリティ政策会議（仮称）」の設置を検討すること、さらには、2)「国家情報セキュリティセンター（仮称）」を設置することを決定[5]し、現在政府において、その具体像のとりまとめを実施している。これにより、より政府が一体となった総合的な情報セキュリティ政策の立案、実施が可能になることを期待している。

1.1.3. 重要インフラに対する取組みの重要性

本委員会では、1) 政策全般の実行体制のあり方と、2) 対象領域の一つとしての「政府機関における情報セキュリティ対策」のあり方、を「第1次提言」として提示した。一方、情報セキュリティ対策の充実は、政府機関だけではなく、我が国の様々な領域において充実させるべき状況にある。このため、本委員会は、我が国の社会経済活動と国民生

---

[4] 情報セキュリティ基本問題委員会第1次提言「情報セキュリティ問題に取り組む政府の機能・役割の見直しに向けて」（http://www.bits.go.jp/kaigi/kihon/index.html#teigen）

[5] 「情報セキュリティ問題に取り組む政府の機能・役割の見直しに向けて」（平成16年12月7日IT戦略本部決定）（http://www.bits.go.jp/kaigi/kihon/teigen/kettei.html）

活を支える重要インフラの重要性を勘案し、重要インフラにおける情報セキュリティ対策のあり方の検討を平成16年10月より開始した。

重要インフラは、我が国の社会経済活動と国民生活を支える基本的なサービスを提供している。仮に、重要インフラで大規模な障害が発生するならば、さまざまな領域へ大きな影響を与えることが予想される。大規模な障害から重要インフラを防護するための取組みは、さまざまなリスクを勘案して行われなければならない。重要インフラでは、その基幹業務を構成するシステム[6]に、ITが年々多用されるようになってきている。この意味で、重要インフラにおける情報セキュリティ対策の充実は必須である。

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月に取りまとめられた「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」とする)[7] に基づいて取り組んできた。これまでさまざまな施策を実施してきたが、現在まで、特に特別行動計画に基づき政府大で実行されている政策の効果を検証しながら、社会情勢の変化等を踏まえて、そのあり方を見直していくことが必要であることは言うまでもない(下記図1参照)。

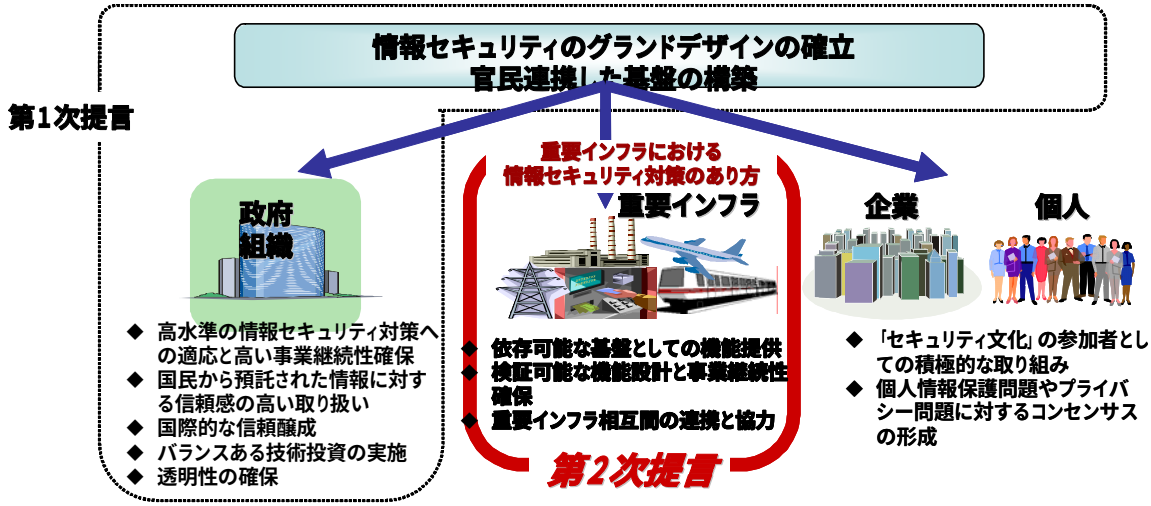


図1:第2次提言の位置付け

1.2.重要インフラとは何か

本提言をまとめるにあたり、まず「重要インフラ」の定義と、「重要インフラの防護」とは何かを明確にすることが必要である。

---

[6] 重要インフラの利用するシステムは、各重要インフラのサービス提供そのものに直接関係するシステム(以下「制御系システム」とする。)と、課金システムや業務計画の立案のためのシステム等各重要インフラのサービス提供を側面的に支えるシステム(以下「情報系(業務系、事務処理系)システム」とする。)の二種類に大別されることを、本報告書では前提として取り扱う。

[7] 「重要インフラのサイバーテロ対策に係る特別行動計画」(平成12月12月15日情報セキュリティ対策推進会議)(http://www.bits.go.jp/sisaku/2000_1215/1215actionplan.html)

平成12年に策定された特別行動計画では、「重要インフラ分野」について、「いわゆるサイバーテロの脅威[8]により、国民生活や社会経済活動に重大な影響を与えると考えられる重要インフラ分野を、当面、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。）とする。」と定義した。つまり、いわゆるサイバーテロの脅威を前提とし、それによって重大な影響がある基盤を、対象とする「重要インフラ」として位置付けている。しかし、「重要インフラ」そのものの定義を行っておらず、入口と出口が逆転したかのような構造となってしまっている。したがって、そもそも重要インフラとは何か、という点につき以下のような定義を行い、そのインフラを防護することを目的とした「情報セキュリティ対策」のあり方を検討した。

- 重要インフラとは、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、または利用不可能な状況に陥った場合に、我が国の国民生活また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をいう。重要インフラの防護とは、これら事業において発生する障害を回避し、サービスを維持・復旧するための総合的な取組みを意味する。重要インフラの防護を充実することは、我が国の能力を保全し、ひいては安全保障・危機管理に資する[9]ことになる。

1．3．第2次提言の射程ー「重要インフラにおける情報セキュリティ対策」とは何かー

1．3．1．「重要インフラにおける情報セキュリティ対策」の立ち位置

(1) 「重要インフラ」のサービスの維持・復旧と「IT 障害」への取組み

前節（1．2．）での「重要インフラ」と「重要インフラの防護」の定義を出発点とすると、「重要インフラにおける情報セキュリティ対策」においても、「重要インフラ」のサービスの維持・復旧を図ることを第一義的な目的とするとの視点が重要である。そして、その第一義的な目的を前提としながら、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障害（以下、「IT 障害」[10]とする。）につい

[8] 「いわゆるサイバーテロの脅威」とは、特別行動計画上は、「高度な技術を有する犯罪者集団やテロリスト集団などが重要なネットワークを攻撃することによる、経済的な被害、混乱、死傷者等をもたらす脅威」（平成12年「重要インフラのサイバーテロ対策に係る特別行動計画」の「2．いわゆるサイバーテロの脅威」参照）とされているが、「サイバーテロとは何か」という点についての明確な定義がないとの問題点が多く指摘されている。

[9] 安全保障・危機管理の観点からは、「政府・行政サービス（地方公共団体を含む）」のうち、政府機関の情報セキュリティ対策も重要であるが、本部分については、別途、基本問題委員会第1次提言を踏まえた取組みを実施中である。

[10] 第2分科会の議論においては、「障害」では事件性が想起されないのではないかとの指摘が一部の委員か

ての総合的な取組みとして位置付けることが適当である（図2参照）。

なお、この際、重要インフラの障害全般の回避に向けた取組み（重要インフラ防護）の強化が併せて行われ、両者が連携を深めることにより、IT 障害回避のための基盤（重要インフラにおける情報セキュリティ対策）が、より強化されていくとの視点も重要である。

また、IT 障害については、重要インフラで利用されている情報システムにおいて、情報システム及び情報資産を用いて実施される業務とそこから発生する重要インフラのサービスを守るという観点から、全ての構成要素、すなわち、1)情報システムそのもの、2)情報システム上に蓄積される情報資産、3)情報システム間でやりとりされるトランザクション、さらに、4)情報システムの運用の4つの構成要素を対象として、その防護方策を考える。この際、防護方策は、単に技術的手法だけに限定するだけでなく、非技術的手法にも視野を広げ、総合的な対応を実行するとともに、意図的な行為だけでなく、広く IT 障害について対象とする。

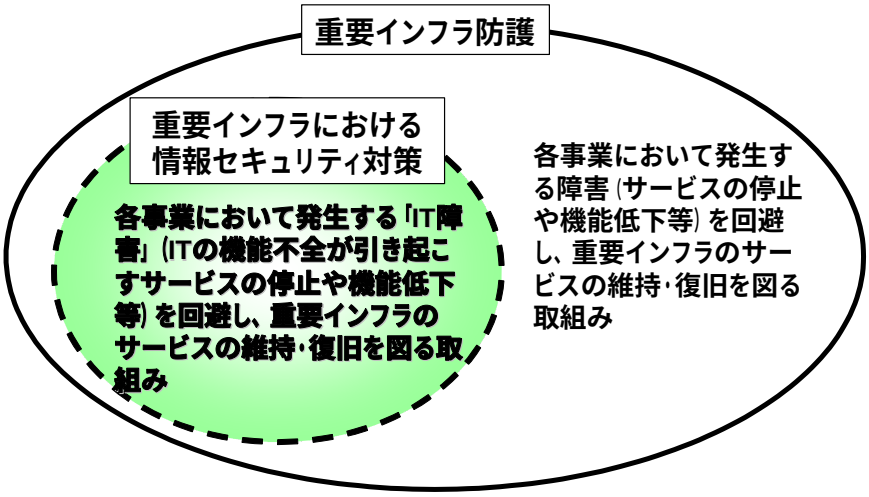


図2：重要インフラ防護全体と「重要インフラにおける情報セキュリティ対策」の関係

（2） 「ビルトイン型」対応の必要性

障害発生時に対策本部を設置して対応するような形だけではなく、あらかじめ優先度に応じて順次障害発生のシナリオと対応策を作成し、定期的に訓練や評価を行い、不備を補填し、連絡網や手順を共有するような「ビルトイン型」の対応が必要である。また、2002年に勧告された OECD の「情報システム及びネットワークのセキュリティのためのガイドライン」で述べられているように、情報システムやネットワークの構築後に情報セキュリティを勘案することは困難であり、重要インフラにかかわるシステムの設計段階で情

らあった。

報セキュリティを組み入れることが強く望まれる。加えて、基本となる考え方は技術革新の進展や社会状況の変化に機敏に対応できることが必要である。

(3) 変化への対応の確保の必要性

「重要インフラにおける情報セキュリティ対策」を検討するに当たっては、重要インフラそのものが何であるかを具体的に示す重要インフラの環境情報について適切な理解を持ち、重要インフラそのものの変化を、その検討に反映しなければならない。重要インフラにおけるITの利用は、事業領域、事業者によって大きな違いがある。ある事業領域では、重要インフラそのものがITによって大部分が構成されている場合もあるが、別の事業領域ではIT利用が他事業領域と比較して限定的にしか導入されていないものもある。このような事業領域、事業者ごとの差異を理解し、合理性の高い対策を組み立てていくことが必須である。また、ITの利用形態そのものも絶えず変化しており、その変化に対する対応を確保することも必要である。

(4) 重要インフラ事業者における管理レベルの目標設定の必要性

重要インフラ事業者においては、情報セキュリティの管理レベルを定め、事業者の外部及び内部環境の変化を常に注視し、その変化に対応した取組みを行い、最高の管理レベルの実現を目標とすることが必要である。このためには、事業者内における方針やルールを定めるだけではなく、その実施状況を定期的に確認し、環境変化に対応するために常日頃から改善を図る活動が、重要インフラ事業者において展開されることが必須である。

(5) 個々の重要インフラ事業者による単独の取組みからの脱却

重要インフラの担い手の多くは民間事業者であり、常に同業者との競争環境に置かれている。このため、具体的な情報セキュリティ対策の取組み状況、手法、実施ノウハウなどは、企業経営ノウハウとして取り扱われることが十分考えられることであり、無条件に事業者間で共有されるものではない。このため、重要インフラにおける情報セキュリティ対策を強化･促進させるためには、事業者間における情報共有の必要性･有効性を、政府が事業者に対して積極的に説明する必要がある。これにより、私企業である重要インフラ事業者の企業経営論理と、重要インフラ事業者における情報セキュリティ対策強化の手法が整合性を持ち、その積極的な促進を政府として後押しできる体制を確保できる。

(6) 適法性、透明性、人権保障の確保

障害シナリオや対応策等具体的な情報セキュリティ対策の取り扱いにあたっては、法的根拠を明確にし、透明性を確保し、国民に対する説明責任を果たさなければならない。さらに、政府の活動は、人権保障の確保の観点から、活動を設計することが必須である。情報セキュリティに係る活動においても、例外なく適法性、透明性、人権保障を確保しなければならない。また OECD ガイドラインで述べられている「民主主義の原則」の確保に留意することが必要である。

(7) 英知の集約と共有

重要インフラにおける情報セキュリティ対策の英知を集約して共有するための、知識と情報のハブ機能を設計する。重要インフラにおける情報セキュリティ問題に取り組むためには、技術領域から非技術領域までの広い視点を持ち、周到かつ戦略的な方策を生み出さなければならない。情報システムに対する脅威が人為的なものである場合、脅威を生み出す集団よりも技術的にも運用的にも高いレベルの知見を軸として防護方策を作成しなければ、情報システムを守ることは到底できない。この観点から重要インフラにおける情報セキュリティに資する英知を集約する構造を作り、同時に得られた知見を共有する基盤を作り出す。

1.3.2. 対策の三側面

重要インフラにおける情報セキュリティ対策において、第一義的に目的とすべき「重要インフラのサービスの維持・復旧」を図るとは、すなわち、1)IT障害を未然に防止し、2)IT障害が発生した場合はその拡大の防止・迅速な復旧を図り、3)その再発を防止することである。この三つの側面について、実効性の高い対策が講じられるよう設計を行わなければならないのは言うまでもない。

IT障害の未然防止では、具体的な障害を想定し、それぞれに適切な防御策を勘案することが必要である。また、その防御策を開発する場合に、原因解明に基づいて適切なフィードバックを行い、不断の改良を行うことが必要である。

IT障害の拡大防止・迅速な復旧では、まず、発生した障害を早期発見する対策を平時より行うことが求められる。障害発生後の復旧策は各重要インフラ事業者の取組みに負うことが多いが、原因解明と、復旧プロセスにおける知見集約によるプロセス改善の可能性についても十分考慮すべきである。

IT障害の再発防止では、それまで行われてきた予防策の評価、発生してしまった障害の原因究明、さらには復旧作業を通して得られた知見といった、分析に基づいた適切なフィードバックを生み出し、現在の対策の改善を促していくことが主な取組みとなる。

このために、重要インフラにおける情報セキュリティ対策の有効性の分析機能の充実が必須である。この分析機能を、官民の役割分担の中で適切に位置づけ、さらに、フィードバックを生み出し、既存の対策に反映させることを忘れてはならない。

1．3．3．対策の対象領域

前節（1．2．）の重要インフラの定義から、重要インフラの利用者にとっては、意図的、非意図的要因に関わらず、そのサービス供給が阻害されれば、多くの損害を被ることが十分予想され、同時に社会経済活動への影響が危惧される。

したがって、そのサービス供給を阻害する要因を広く視野に入れ、その中におけるITの機能不全に起因する部分に係る対策をもって、「重要インフラにおける情報セキュリティ対策」の射程としていくことが必要である。これは、従来から中心的に取組みの対象となってきたサイバー攻撃[11]だけなく、人為的なミス、IT の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及びネットワークやハードウェア障害等の非意図的要因や、地震・津波などの自然災害など、多種多様な脅威を勘案し、これらの脅威が重要インフラの構成要素である IT に与える影響を最小化する対策の実施を希求することにほかならない。

1．4．各主体の役割分担原則

重要インフラにおける情報セキュリティ対策を実施するに当たっては、官民の様々な主体が、それぞれの役割を果たし、我が国全体として官民連携した強固な基盤を構築していくことが必要である。同時に、各主体の役割分担を考えるときに、我が国の現状を踏まえ、各主体が以下の原則を理解し、行動することが必須である。

1．4．1．重要インフラ事業者の役割

重要インフラの多くは民間事業主体が担っているほか、重要インフラと政府との関係は各事業法等の法令に従って、政府が関与可能な範囲とインフラ事業者が最低限実施すべき範囲とを規定している。

一方で、それぞれの重要インフラ事業者においては、種々の競争環境の中で法令に定められた以上の対応を実施する一方で、重要インフラが相互に依存しあっている現状においては、個々の重要インフラ事業者の自主的対応のみでは適切な対応が困難

---

11 「サイバー攻撃」とは、「重要インフラの基幹をなす重要な情報システムに対して、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」のことを指す（平成12年「重要インフラのサイバーテロ対策に係る特別行動計画」の「2．いわゆるサイバーテロの脅威」参照）。

な状況が生じつつあるのも事実である。また、IT の利用の進展に伴い、そうした状況が一層加速されているのが現状である。

したがって、一義的には、重要インフラ事業者の自主的対応によって担われることを原則としつつも、各重要インフラの重要性と社会的使命の大きさを考慮すれば、官民が連携しながら、各主体がそれぞれの役割と責務に基づき、保有する知見・能力を最大限活用して重要インフラ防護に臨むことが必要である。

1.4.2. 政府の役割

政府の側では、①全体の枠組みを構築し総合調整する「内閣官房」、②重要インフラ事業者と法令に従って直接に接する「重要インフラ所管省庁」、③警察庁、防衛庁、消防庁、海上保安庁などの「事案対処省庁」、④情報セキュリティに関する取組みを政策的に行っている「情報セキュリティ関係省庁[12]」、⑤各事業法ではなく基本的な法制度、研究開発・技術開発、人材育成など、側面的に対策に影響を及ぼす「その他の関係省庁」といった主体が存在するが、これら各主体が持つ知見・能力の連携を図り、最大限活用することが必須である。

1.4.3. 構造

重要インフラを担う事業者は、地理的にも役割的にも大きく分散している。したがって、全ての事業者に対して働きかける中央集権型の構造だけではなく、事業者が主体的に知識共有を行い、事業者の実情にあった情報の適切な管理等を行うことのできる分散型の構造が必要である。

また、役割分担を考える中では、コスト負担構造には十分な検討が必要である。具体的には重要インフラにおける情報セキュリティ対策の充実、機能強化を進めるコストを、誰が、どのような形で負担するのかということを真摯に検討しなければならない。例えば、各事業法等の法令によって明記されている重要インフラ事業者の義務を拡大する方向は、サービス提供コストを上昇させ、直接的な経営圧迫を生み、新規参入障壁になることや市場における競争性を阻害する可能性を持っている。一方、重要インフラが持つ社会的責任を勘案すれば、最低限度の対策実施を各事業者に求めていくことも、政府としては怠ることができない。この二つの考え方を踏まえ、それぞれの役割分担の中で、適切なコスト負担をしていくことのコンセンサス形成について、各主体は努力する必要がある。また、コスト構造を考える中で、コスト軽減についても戦略的な取組みが必要である。我が国の重要インフラがもつ強みとして「高い信頼性」を達成するノウハウは、各

[12] 警察庁、防衛庁、総務省、経済産業省の4省庁を指す（末尾関連資料参照）。

重要インフラ事業者において保有されているが、これをパッケージ化によって他者に活用されうる資産として形作ることはされていない。仮にパッケージ化が行われたとしたら、他者においてパッケージを利用することで、情報セキュリティ対策導入コストの低減を図れる可能性がある。また、このパッケージが国際的にも利用可能であるならば、国際標準化の試みや、他国への技術供与という道も開ける可能性がある。このような、コストを巡る取組みには、戦略的な観点が必要である。

さらに、重要インフラで発生する事案では、事件性を有する事案が発生することも想定しなければならない。この場合には、適正な手続きに基づき捜査機関との協力等も重要であることは言うまでもない。

第2章　想定される脅威シナリオとその影響の例示

重要インフラ事業者におけるサービスの維持･復旧のための種々の取組みは、これまでも災害対策、障害対策などの観点から検討が行われ、各事業者の自主努力の中で実施されてきた。しかし、重要インフラにおける情報セキュリティ対策という、重要インフラに組み込まれているITに焦点を当てた対策については、重要インフラ事業者においても、また、重要インフラを所管する政府においても、明確な目標と方針を持って検討することは難しいという認識が一般的である。これは、ITの機能不全をもたらす原因として想定される脅威の多くが目に見えないこと、障害発生により間接被害を受ける関係者の範囲が広いこと、さらに、重要インフラ分野ごとにITの利用状況の大きな違いが存在すること、事業領域によって復旧に対する考え方が大きく違うことなどが原因である。したがって、現実にIT障害が発生しない時点で、具体的な脅威ごとにITの機能不全の発生が予想される重要インフラの範囲や各主体に要求される対策について、議論に参加する関係者が共通に認識とイメージを持ちつつ、検討の立ち位置を明確化してというアプローチが極めて重要である。

本章では、重要インフラにおける情報セキュリティに対する脅威の中から、顕在化する可能性が高いIT障害の典型例を「象徴的ケーススタディ」として提示する。さらに各脅威に属する事象がITの機能不全を引き起こすことにより、現実のサービス供給の阻害に至るプロセスを、因果関係を軸に可視化することを試みる。この思考実験の過程で、関係する重要インフラの範囲と、どのような状況が発生しうるかについて、関係主体が明確にイメージを共有できるようにし、そこで求められる対策について、より具体的な要件と組み立て方についての共通認識を形成することを試みる。

2．1．日常生活に隣接し、実在する脅威を可視化する重要性

政府及び関連組織等のホームページへの DoS 攻撃や改ざん事案の発生をみても明らかなように、サイバー攻撃の脅威は身近に存在するという認識は誰もが共有している。また、オンライン･システムの障害により、根幹となるサービス停止が発生する事例も一部の重要インフラ分野で実際に起こっている。さらに、平成7年に発生した阪神･淡路大震災や直近の新潟県中越地震の例をみても、局所的とはいえ、地震の直接被害や主要な重要インフラのサービス停止によって各重要インフラの情報システムにダメージが発生するおそれは現実に直視しなければならない状況になってきている。

このように程度の差はあれ、漠然と脅威の拡がりについて認識されているにもかかわらず、重要インフラにおける情報セキュリティ対策についての本格的な議論が進まない背景には、1）各重要インフラにおいて、これらの脅威や情報システムの機能不全及びサービス供給障害との因果関係が明確になっておらず、具体的なIT障害の被害想定がしにくい、2）重要インフラ相互の依存性が各重要インフラのサービス供給に及ぼす影

響について個別分野ごとには把握しきれない、という課題が存在していると考えられる。

ここでは、重要インフラにおける情報セキュリティ対策についての具体的検討に資するため、共通の作業仮説として、上記課題を踏まえたIT障害の発生シナリオを設定することにする。

2．2．脅威の典型例についての障害発生シナリオ

2．2．1．同時多発サイバー攻撃によるIT障害を想定した影響

(1) 重要インフラの制御系システムに対する同時多発サイバー攻撃によるIT障害の想定例

ここでは重要インフラにおける制御系システムに対して、同時多発サイバー攻撃によるIT障害と、その障害によって引き起こされる事象について考える。

一般に重要インフラの制御系システムは、通常の通信系からの隔離、フェールセーフ機構の導入、さらには、運用上のさまざまな安全規定により、手厚く防護されているシステムである。このため、制御系システムに対して同時多発サイバー攻撃が行われる可能性は極めて低いと考えられている。しかし、これまでの重要インフラにおける制御系システムに対して攻撃が成功した例を考えると、安全規定違反が放置された状況があり、システム管理が対象外としていたシステムからの侵入が成功し、さらに、システムそのものの欠陥（バグ）等の脆弱性を利用することができたといった、まさに「思いもよらなかった」攻撃が構成されている。このことから、重要インフラにおいて同時多発サイバー攻撃が発生する可能性は極めて低いとしながら、その可能性をゼロということはできない。特に、テロリストが行うサイバー攻撃の場合、入念な計画立案、内部協力者の存在など、現在の障害対策の想定外要因が存在することを考慮する必要がある。

また、情報処理振興事業協会（当時）が平成11年度に行った「石油プラントのネットワーク安全性検証実験」によれば、制御系システムの評価は「リスクが中程度の脆弱性があり強固ではない」という結果を得ている。したがって、1）制御系システムの詳細情報を入手、解析することが可能であり、2）何らかの方法により制御系システムに直接アクセスできる方法が提供され、3）使用されている制御系システムがある程度の導入数がある場合、同時多発サイバー攻撃の実現可能性が増すことが十分考えられる。

例えば、電力、ガス、大規模化学プラント等の制御ネットワークへ侵入し、内部関係者からの情報をもとに障害をもたらすコマンドを実行することや、異常な動作をするようにシステムそのものを改ざんすることも技術的には可能である。このような攻撃を、同一事

業者の情報系システムに対するDDoS攻撃[13]などと組み合わせて実施することにより、攻撃そのものへの対応に手一杯となった重要インフラ事業者が、サービスの停止に追い込まれることが想定される。具体的には、次のようなシナリオが考えられる。

① 重要インフラ事業者の情報系システムに対して、大規模な DDoS 攻撃を仕掛け、通常業務に対して多大な影響を与える。
② 内部関係者から得られた情報により、制御系ネットワークへ侵入を試み、制御系システムの改ざんと、異常動作を引き起こすコマンドの実行を行う。
③ 同型式のシステムに対して、次々とその攻撃を拡大。
④ IT 障害と、他の要因（内部犯行、人的ミス、機器の動作不良等）が重なり、サービス継続のための主要機能を著しく損なう。
⑤ 障害が単一事業所にとどまらず、国内の複数個所で同時に障害が広がる。
⑥ 結果として、重要インフラ事業者のサービス供給が停止し、その結果他の重要インフラのサービス供給や、国民生活に直接かつ甚大な影響（国民の生命、身体または財産に重大な被害）が発生する。

実際の発生確率は非常に低いと考えられるものの、このようなシナリオは、特定の重要インフラに限られたものではなく、主要機能に広く IT を用いている重要インフラでは想定可能なものである。例えば、上記シナリオに登場するように、IT技術を用いた攻撃による障害と、人的ミス等の他の要因の複合によって生じる物理的な被害は、電力分野では発電の停止、ガス分野ではガス製造装置の制御系に侵入し、ガス製造・供給の不安定性を誘起しえる。また、鉄道分野においては、攻撃による列車運行管理システムのダウンへの対応時に人的ミスが重った場合には列車運転に大きな支障が生じるおそれがある。さらに、水道分野においては、浄水場の制御系システムに侵入し、給水不能の状態に陥れる、航空分野においては、予約・搭乗や運行管理システムが長時間停止した場合、大規模な出発遅延や欠航につながるおそれがある。

(2) 当該IT障害の影響範囲

テロリズムは、ある特定の目的（政治的、あるいは宗教的等）をもって、不法な暴力を用いて、あるいは用いると脅すことにより、人を殺傷し、あるいは人に脅威を与え、社会を混乱させる行為である。

前項で述べたシナリオでは、重要インフラの事業所における製造施設の物理的な被害や人的な被害が、重要インフラで用いられている制御系システムへの侵入、改ざん、異常動作を引き起こすコマンドの実行などによって発生している点に注視しなければな

[13] 分散型サービス妨害攻撃（Distributed Denial of Service）のこと。

らない。もしこのようなケースが現実に発生した場合には、「他の重要インフラでも同様のことが起こるのではないか」、「鉄道は大丈夫か」、「ガス製造施設は大丈夫か」、「化学プラントは大丈夫か」など、社会的な不安の連鎖が広がる可能性がある。これは、まさにテロリストの意図するところであり、国民生活や社会、経済の混乱の招き、ひいては我が国そのものの信用問題ともなる。

また、同形式プラント（製造時期は異なるが、基本設計と利用される技術が同じもの）においては、制御システムの設計や制御プログラムの構造も類似しているケースが多いと考えられることから、一つのあるプラントの構造が解明できれば、その応用で他の同様のプラントの制御プログラムを書き換え、操作コマンドを追加される可能性があることは否定できない。

一方、テロリストは、より効果的に人々に恐怖心を抱かせ、社会的な混乱を起こさせるために、同時多発でテロを起こすことが、これまでの物理的なテロ事件においてもしばしば行われているところである。また、時差で多発テロを起こすこともある。これは、警察、消防等のファースト・レスポンダーや報道等が集まる頃合いに、同じ場所で第二のテロを行うことにより、より多くの人を殺傷するためである。

サイバーテロは、一般的には以下のような特徴があることから、テロリストにとって、非常に魅力的な攻撃手法であると言える。

① 低コストでの攻撃が可能（インターネット環境さえあれば、ネット・カフェ等からでも攻撃が可能）
② 攻撃に要する部隊が不要（専門的な技術者1人で、数カ所の攻撃も可能）
③ 犯人が特定されるリスクが低い
④ 地理的、時間的制約がなく、いつでもどこからでも攻撃が可能
⑤ 経済・社会に大きなダメージを与えることが可能
⑥ サイバー攻撃を防御するのは極めて難しい

このようなことから、同時多発でテロを起こすことは、テロリストにとって効果的であり、もし同じプラントが世界各地にある場合には、日本国内での同時多発のみならず、世界規模での同時多発テロの可能性すら考え得るという認識を持たなければならない。

(3) 考えられる攻撃の主体と能力及び可能性

中東のテロ組織であるハマスやヒズボラ、アル・カイダ等のテロ組織がIT分野に高い関心を示していることは、これまでの米国政府の報告書等で明らかになっている。とりわけアル・カイダについては、これまでも重要インフラへの攻撃に関心を示してきており、インターネットやコンピュータ技術に精通するテロリストの存在も指摘されている。

2003年10月18日には、オサマ・ビン・ラディン（UBL）が「我々は、この抑圧的な戦争に参加する全ての国々、特に英国、スペイン、オーストラリア、ポーランド、日本、イタリアに対し、適当な時期と場所において報復する権利を有する」として、日本を名指しした

声明を出している。さらに、この後も UBL やアル･カイダの幹部で UBL に次ぐ No. 2の地位にあるとされるアイマン･ザワヒリが「日本」に言及した声明を出しており、これらのメッセージは、アル･ジャジーラの放送やウェブ･サイトを通じて、世界中のイスラムテロリストやその予備軍達が耳にしているであろうし、アル･ジャジーラのアラビア語や英語のホームページにも掲載されている。ゆえに、UBL が「日本」に言及した、すなわち UBL が「日本をターゲットの一つとして考えてよい」と考えているということは、世界中のイスラムテロリスト達が認識していると考える必要がある。

東南アジアには、東南アジア諸国一帯で活動する JI（ジェマ･イスラミア）というアル･カイダと関係の深い組織もあり、これらのテロリストが、いつ日本を攻撃対象にしてもおかしくない状況にある。

また、米国や英国等は物理的な面でもIT面でも防御を強化しており、攻撃対象が比較的セキュリティの弱い国や民間企業の施設等、いわゆる「ソフトターゲット」にシフトしていることも注意を要するところである。

2．2．2．非意図的要因によるIT障害を想定した影響

一般的に、重要インフラの制御系システムについては、インターネットをはじめとする外部ネットワークとの隔離を、サイバー攻撃を含む外部脅威への対策としてあげる事業者が多いが、プログラム上の欠陥（バグ）やプログラム設定ミス等の非意図的要因によりIT障害が発生する可能性は、国内で実際に発生した事例が散見されるように、常に存在している。ここでは、典型的な制御系 LAN において、非意図的要因によりIT障害が引き起こされるケースを想定し、当該障害による影響範囲について考察する。

（1） 制御系 LAN を持つ重要インフラにおいて起こり得る非意図的な要因による IT 障害の想定例

ここでは、一般的に重要インフラにおいて使用されている制御系 LAN 管理下の個別制御系システム、操業 LAN 管理下の操業管理系システム、全社基幹 LAN 管理下の全社基幹系からなる設備と業務及び関連する情報がある場合を想定し、主としてシステムプログラム上の欠陥（バグ）に起因するIT障害の発生の可能性について考える。

制御系 LAN においては多数の制御系システムが専用のハードウェアやファームウェアを使用して様々な計測データの交換を行っており、オペレータコンソールと呼ばれる操作･監視コンソール画面によって制御が行われている。オペレータコンソールにより膨大な設備及び機器の操作と監視が少人数の熟練した技術者によって効率良く行われている。当該制御系 LAN においては、各システムは予め綿密な試験を行い、システム導入後にファームウェアやハードウェアの更新が行われるケースが多い。しかしながら、(3) の過去の障害事例が示すように、この事前の試験段階では想定し得ない使用状況

が出現することによって動作不良が発生する危険性は否定できない。
具体的な想定例として以下の2つを挙げる。

① オペレータコンソールの機能不全

大規模プラントの制御系システムのオペレータコンソールのように様々なサブシステムの集中操作と監視が可能なシステムの場合、万が一オペレータコンソール機能自体が障害を受け停止した場合には、オペレータコンソールの管理下にある広範囲の設備と機器を手動による復旧に切り替えることは非常に大きな負担となる。また、このような大規模な情報システムにシステム上の不具合が発生した場合、異なるベンダーが開発した年代の異なるサブシステムの集合体の中から、実際にIT障害の引き金になったシステム上の不具合箇所の特定を行うことは非常に難しい。

② ファームウェア上のバグ

一方、制御系 LAN につながっている個々の機器類で用いられるファームウェアにバグがあり、特定の制御バス[14]系に属する制御機能に不具合が発生し、本来オペレータコンソールの管理下にある設備や機器の操作と監視が不能となるような場合も考えられる。このようにある種のシステム上の問題解決のためにハードウェアベンダーが開発し納入したファームウェアが、同時に深刻な障害をもたらす予期せぬバグをプログラムに埋め込んでしまうといったケースである。
このようなファームウェアはオープンではなくベンダー固有の制御系 LAN 向きのものであり、多くの制御の現場で同一ベンダーの製品が用いられている。クローズドシステムは世界中で広く使用されているものではないので、汎用製品と異なり、特定状況下における動作不良の報告件数も限られることから、開発段階で全ての使用状況における問題を事前に全て試験により洗い出すことは現実には困難である。したがって、同時に多くの現場において同じプログラム上の問題を持つファームウェアがバージョンアップを期に導入されてしまうケースが発生する。

(2) 当該IT障害の影響範囲

本事例は、制御系 LAN を持つプラント設備を運用している産業、電力やガスのような重要インフラ事業者のみならず、石油、石油化学、一般化学などの大規模プラント設備においても共通に起こりうる事象である。

---

[14] バス(bus): コンピュータ内部で各回路がデータをやり取りするための伝送路。

例えば、当該制御バスのファームウェアに特定使用状況下において、制御不能となるバグが作用して、制御バス上の全てのオペレータコンソールがホワイトアウト[15]し、設備と機器の動作状況が見えなくなってしまうような状況は十分考えられる。そのような場合、操作と監視が不可能となった設備と機器は、手動で緊急停止処置を講じなければならない事態となる。その結果、電力の場合は発電が一時的に停止することもあり得る。短時間であっても発電所の休止は多くの電力需要家に影響を与え、特に、オフィスにおいてコンピュータが使用出来なくなり、長時間に及ぶ場合には、バックアップ電源などを備える他の重要インフラであっても影響は深刻となり安全な市民生活が脅かされることも考えられる。

(3) 非意図的な要因による過去の IT 障害事例

ここで想定したような重要インフラにおける情報システムのバグや操作ミスなどの非意図的要因に起因する IT 障害として、これまで以下のようなものが報道されている。その多くは、大規模なシステム統合やシステム改修に伴うプログラムの入れ替え時に発生しているのが特徴である。

- 新幹線で、自動列車制御装置(ATC)の設定を解除した応急処置訓練後に、設定を戻さずに40キロ走行。(平成14年6月)
- 主要幹線鉄道にてシステムの曜日設定のミスで、土曜日に平日ダイヤで運行を行い4時間の運休が発生。(平成15年1月)
- 航空交通管制部にある飛行計画情報処理システム（FDP）がダウンし、215便が欠航。（平成15年3月）
- 政府機関でシステム移行に関わるプログラム修正にミスがあり、口座振替ができない、小包の行方の照会が出来ない、税金や社会保険料のデータ送信の遅れなどが生じた。(平成15年4月)
- 県警の免許交付作業を行なうシステムのメンテナンス中に必要なプログラムが削除されてしまい、免許証の即日交付に影響が生じた。(平成15年5月)
- オンライン専業の銀行で，ユーザーによる残高照会や振り込みなどのサービスがパソコンやブラウザフォン経由のインターネット、電話、提携 ATM のすべての手段で全面的に停止。 (平成15年5月)
- 7金融機関との間で、日銀ネット側の送受信機能のバグにより、一部の電文の送受信が停止。(平成15年7月)

---

[15] ホワイトアウト(white-out): コンピュータ・コンソールが稼働している最中に画面表示が不能となった状態。電源供給の途絶による機能停止により、コンピュータ・システムが制御不能となるブラック・アウト(black-out)に対比される用語。

- 証券取引所で、プログラムが正常に作動せず売り買いの約定が合わない取引が誤って成立したため、買付株数の不足分について証券取引所が一時的に買い取った。(平成15年10月)
- 2つの保険会社が合併前にそれぞれのシステムにおいてプログラムミスがあり、保険契約者への配当金の一部に支払い不足があったと発表。その他保険会社でも同様のミスによる支払い不足があることが判明。(平成15年10月)
- 県警の交通管制システムに障害が発生し、市内各地にある信号機のうち128台が正常に点灯しなくなり渋滞が発生。(平成15年12月)
- 「対外接続ソフト」の日付処理のバグによって、約20の大手銀行、地方銀行において、他行 ATM（現金自動預け払い機）での現金引き出しや残高確認などができなくなった。 (平成16年1月)
- 医療系のコンピュータープログラムにミスがあり、本来腎臓移植を受けられるはずだった6人の移植待機患者が、臓器提供者の白血球型（HLA型）と十分適合しないと判定され、移植を受けられなかった。(平成16年1月)

さらに、海外においては、以下のような事例が報告されている。

- 2000年問題で、米国の国防総省は軍事偵察衛星(スパイ衛星)のシステムが2～3時間故障し、画像受信が不能となったことを発表。(平成11年12月)
- ドメイン登録業者がホスティングする Web アドレスシステムソフトウェアのバグにより、最大で3万のWebサイトと電子メールアドレスが数時間、オフラインになった可能性がある。(平成15年7月)

このように多くの事例が報告されているが、これらの複数の IT 障害が重なって起こった場合には、より深刻な被害に発展していく可能性が高い。また、バグや操作ミス、設定ミスなどの人為的要因は再発防止対策に多大なる努力が行われているものの、今後も同様以上の IT 障害が起こり得る可能性は否定できないのが実情である。

2．2．3．自然災害によるIT障害を想定した影響

(1) 自然災害による IT 障害の想定例

地震、雷、高潮、大雨等、IT障害の原因となりうる様々な自然災害が想定できるが、ここでは、我が国の特徴的な災害である「地震」に起因するIT障害について考える。

地震については、その大きさ及び影響面積の広さが多様であるが、ここでは、例えば、阪神淡路大震災や新潟県中越地震級の地震を想定する。

地震に起因し、様々な重要インフラにおいて、以下のような IT 障害が起こり得る。

① 直接通信インフラが損壊を受けるケース

震源近傍にて、道路、鉄道等に沿って敷設した回線が破断されたり、一部の携帯電話基地局のアンテナ等が、据付ビルの倒壊等に伴い崩落することにより、震源近傍のみならず、比較的広域にて電話や通信回線が利用できなくなる。また、震源近傍の電信柱倒壊や地下埋設ケーブルの破断により、その地域の通信が遮断するケースもあり得る。

この際、道路事情の悪化に伴い、回線の破断点の確認に遅れが出るとともに、回線破断地域については、回線の再敷設を試みるものの、道路事情の悪化により工事が開始できない地域が多発し、復旧が遅れる。

② 直接当該インフラの IT 障害を引き起こすケース

震源近傍にて、高架橋の破壊や路盤流出に伴い、鉄道の信号線が破断され、比較的広範囲において自動列車制御装置（ATC）、自動列車停止装置（ATS）などが動作不能となり、鉄道の運行が極めて困難となる。

③ 他のインフラのサービス停止の影響で当該インフラの IT 障害を引き起こすケース

震源近傍の大半の発電所が自動運転停止したり、震源近傍の高圧線が破断されることにより、広範囲の停電が起こる。また、震源近傍の電柱が倒壊し、狭い範囲の停電が発生する。こうした停電により、通信設備の給電が商用電源から非常用電源（蓄電池（バッテリー）、自家発電機）に切り替えられるものの、地震発生から時間が経過すると、停電地域の携帯電話基地局が次々とバッテリー切れを起こし、携帯電話の不通地域が広がる。また、停電地域の小規模交換機等がバッテリー切れを起こし、固定回線の不通地域も拡大する。この際、移動電源車を手配するも、道路事情の悪化に伴い、必要地域に近付けず、被災後も時間経過と共に不通地域が拡大しうるという特性を持つ。さらに、停電が数日に渡り、かつ道路事情が改善されない場合には、自家発電用の燃料が枯渇することにより大規模設備が停止し、地震発生から数日後に、きわめて広範囲が不通地域となるおそれもある。

金融機関においては、自らの設備には異常がないとしても、停電地域においては、窓口の情報システムが稼働せず、金融取引等が実質不可能になるとともに、コンピュータセンター間や銀行間ネットワークの通信障害により、オンラインサービスが停止し、口座開設支店以外での預金引きおろし等が困難になる。

(2) 当該 IT 障害の影響範囲

地震は、広域性を有することから、発生時点から広範な重要インフラに多大な障害を及ぼす。

しかしながら、道路の崩落･陥没等に伴い、人員輸送、物資輸送が困難となることから、

道路インフラの復旧が、他のインフラの障害確認や復旧工事の円滑実施に多大な影響を及ぼすこととなる。

また、初期段階においては、通信サービスが停止したことに伴い、確認された障害の情報集約を困難とし、他の重要インフラの復旧の初動に悪影響を及ぼすこととなる。

さらに、通信インフラに関しては、電力の復旧が遅れた場合、地震発生からしばらく経ってからもバッテリー切れなどによる通信障害が新たに発生するため、当該情報の広報状況によっては、被災地住民等を無用の混乱に陥れる可能性がある。

また、金融については、自らの保有する情報システムになんら異常を来たさなかったとしても、電力または通信に障害が発生することに伴い、実質的にサービス提供が停止することになる。

いずれにせよ、複数のインフラの障害が、それぞれのインフラの復旧を妨げることとなり、大規模自然災害が発生した場合には、被災地域住民や当該地域の企業等の社会・経済活動に甚大な影響を及ぼす。

同時に、停電と通信障害が夜間に同時発生した場合には、当該地域が暗闇に包まれ、また警察への通報等も困難となることから、治安が悪化することなども推測される。

(3) 通信インフラの視点から見た当該IT障害の復旧に関する知見

① 電力に関わる影響

1) 商用電源の停電が発生した場合

電気通信設備において、停電が発生した場合は、通常装備しているバッテリーにより、数時間程度の継続動作は可能である。また、非常用発電機を装備したビルでは、さらに2日間ほどの継続運用が可能となる。しかし、非常用発電機を装備していない設備の場合は、必要に応じて「移動電源車」を用いた継続運用を手配する。

2) 通信インフラとの関係

電力障害に関わる復旧状況を可能な限り正確に把握することにより、電気通信設備の復旧計画、移動電源車の配備計画などを練る段階で非常に有効となる。通信インフラとしては、電力障害の復旧状況把握といった関連で、電力インフラとの連携が期待されるところである。

② 道路事情に関わる影響

1) 道路の崩落・陥没などが発生した場合

電気通信設備の障害、倒壊、破損などの設備復旧・回復を実施する段階で、

現場への道路が崩落･陥没していて当該設備が存在する場所に駆け付けることができない状況が発生することがある。このような場合には、応急的な復旧を迅速に行うことができない。

2) 通信インフラとの関係

通信インフラの設備復旧･回復作業において、道路の崩落･陥没状況をいち早く把握する必要がる。しかしながら、道路の復旧、再構築は、大規模な物理的な修復が必要となる場合が多く、1日～2日で完了するものは少ないため、道路障害のため到達できない現場の電気通信設備の復旧について、多くの時間を要することは避けられない。

第3章　現状の問題点と対策を具体化していく上での視点

本章においては、第1章に提示した基本理念及び前章に提示した例示に基づき、現状の問題点と、対策を具体化していく上での視点を整理する。

3．1．現状の問題点

本節においては、まず特別行動計画策定以降に行われてきた、重要インフラにおける情報セキュリティ対策に係る取組みが、社会情勢等の変化に対応して実施されているか否かという観点から、現状の問題点を整理する。

3．1．1．「守るべきものは何か」という視点の不足

第1章でも示したように（1．2.参照）、特別行動計画においては、「重要インフラ分野」について、「いわゆるサイバーテロの脅威により、国民生活や社会経済活動に重大な影響を与えると考えられる重要インフラ分野を、当面、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。）とする。」と定義している。すなわち、そもそも「重要インフラとは何か」、または「重要インフラを守るとは何か」という点から出発しておらず、「サイバーテロ」という脅威を前提とし、それによって重大な影響がある基盤を、対象とする重要インフラとして定め、それに対する対策を講ずるという形をとっている。

しかしながら、そもそも重要インフラとは国民生活及び社会経済活動の基盤であることに鑑みれば、「サイバーテロ」という脅威を前提とすることによって、「重要インフラを守る」との全体像が曖昧になり、入口と出口が逆転したかのような形となってしまっていると言える。

3．1．2．脅威の拡がりに対する対応上の問題

現在の特別行動計画及び「サイバーテロ対策に係る官民の連絡・連携体制」（以下、「特別行動計画等」とする）は、重要インフラにおけるサイバー空間の情報セキュリティに関する脅威に対する、我が国として初めての官民協力の枠組みとして評価できる。しかしながら、サイバー攻撃、すなわち意図的な攻撃への対応を中心に構成されており、潜在的に存在する他の脅威に対する検討やサービス供給を直接支える制御系システムへの対策についての検討が不足していると言える。

一方で、特別行動計画が策定された平成12年当時から比べても、各重要インフラの制御系、情報系のシステムを問わず、IT の利用度が高まっている。したがって、制御系、情報系のシステムにおけるITの機能不全により、IT 障害が発生しうる各重要インフラの

サービスの範囲が確実に拡がっており、「重要インフラにおける情報セキュリティ対策の射程」（1．3．）から考えても、単に、サイバー攻撃を脅威の中心に据えた対応は限界に来ていると言える。

3．1．3．脅威が顕在化する可能性についての認識の共有不足

特別行動計画の策定から現在まで、またはそれ以前においても、我が国において、「大規模なサイバー攻撃による重要インフラのサービス停止障害が発生したことはない」との認識が支配的となっており、その具体的事例について、共通の議論がなされてこなかったことから、これらに対する認識が不足していると言える。

しかしながら、大規模なサイバー攻撃による障害を見ても、海外ではそうした事例、またはそれと疑われる事例もある[16]ほか、我が国においても、平成15年8月に、MS-Blaster と呼ばれるコンピュータウイルスによって、重要インフラのシステム停止障害が発生した事例は記憶に新しい。また、阪神･淡路大震災や新潟県中越地震の事例に鑑みれば、かかる広域災害により IT 障害が起こりうるものであることが強く再認識されたところである。

したがって、サイバー攻撃の脅威をとってみても「起こっていないから問題ない」との立脚点ではなく、「起こる可能性が常にある」との視点からの対応が必要であることに加え、サイバー攻撃以外の潜在的脅威がIT障害を引き起こす可能性についての認識を、関係者が共有できるメカニズムが必要であると言える。

3．1．4．関係者による個別対応の限界

特別行動計画等は、重要インフラにおけるサイバー空間の情報セキュリティに関する脅威に対する、我が国として初めての官民協力の枠組みであり、すなわち、各関係者が個別に対応を行うのではなく、情報の共有等を図りながら、官民全体でその脅威に対処していくことを定めたものである。

しかしながら、特別行動計画策定後も、関係者間の信頼関係の不足から外部との情報共有に対して過度に慎重となるという実態や、関連情報が企業経営ノウハウとして取り扱われるという実態等から、各関係者の個別対応への依存状態から抜け切れておらず、ここで定められた情報共有等の枠組みが十分に機能しているとは言い難い。したがって、官民協力の全体枠組みを積極的に活用していくための構造変化を、再検討すべ

[16] 例えば、豪クイーンズランド州で、市の水道施設の制御システムに侵入した犯人が、未処理の汚水100万リットルを河川及び沿岸部に流し込んだ事例(2000/03)、米カリフォルニア州の電力会社の送電網システムに外部者が不正侵入した事例(2001/06)、世界のルート DNS サーバ13箇所に対する DDoS 攻撃が行われ、うち9箇所が一時影響を受けた事例(2002/10)などがある。

き時期に来ていると言える。

3．2．対策を具体化していく上での検討視点の整理

上記の問題点を解決するためには、第一に、現在の特別行動計画等も、重要インフラのサービス供給の維持・復旧という大目的が、今般の検討の視点[17]と同一の方向性であることから、この従来の枠組みを尊重し、発展していく形で具体策を提示することが必要となる。加えて第2に、この従来の枠組みには不足している点についての具体策の提示を行うことが適当である。

以下、本節においては、次章において上記問題点についての具体的解決策を提示するにあたり、そこで立脚すべき検討の視点につき、1）従来の枠組みを尊重し、発展させていく形での検討の視点と、2）これまで不足していた観点を追加し強化していく形での検討の視点とに分けて整理する。

3．2．1．従来の考え方を尊重し、発展させていく形での検討の視点

現在の特別行動計画等もそうであるように、重要インフラのサービス供給の維持・復旧が今般の検討の大目的であることに鑑みると、従来の考え方を尊重し、発展させていく形での検討の前提として、その供給が制限されるようなIT障害を、1）未然に防止し、2）IT障害が発生した場合はその拡大の防止・迅速な復旧を図り、3）その再発を防止するという3つの側面から検討していくことが適当である。各論としては、以下のような視点が重要となる。

（1） 各重要インフラ事業者への提供情報の充実

基本理念で示された議論の射程及び各主体の役割分担原則を踏まえつつ、上記の3つの側面それぞれに資する情報が適切に各重要インフラ事業者に対して提供される体制を構築することが一義的には重要となる。そして、このために、各重要インフラ事業者、重要インフラ所管省庁及び内閣官房を中心に官民連携の体制を強化していくことや、各主体の能力向上を図ることが必要となる。

（2） 官民連携体制のハブ機能の強化

官民連携体制のハブとなる内閣官房においては、重要インフラ事業者に対してサー

[17] 1．3．1．（1）参照。

ビスの維持･復旧のために提供する情報を充実させるため、1）情報セキュリティ関係省庁、事案対処省庁及び関係機関（警察庁サイバーフォース、NICT[18]、IPA[19]、Telecom-ISAC Japan[20]、JPCERT/CC[21] 等）[22]などとの連携を強化するとともに、2）収集された情報を総合的に分析する機能を強化することが必要となる。

（3） 現場での人材育成

具体的対策が確実に効果を上げていくためには、各重要インフラ事業者、重要インフラ所管省庁等の現場での人材育成も視野に入れていくことが必要である。

3．2．2．これまで不足していた観点を追加し、強化していく形での検討の視点

上記に加え、これまでの特別行動計画等では強調されていなかった観点を追加し、強化していく形での検討の視点としては、以下のような点が挙げられる。

（1） 重要インフラ横断的状況把握機能の強化

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対策を向上させていく観点から、重要インフラ相互間の依存性解析を行うなど、重要インフラ横断的な状況把握機能を強化する視点を加えることが必要である。

（2） 重要インフラ事業者及び重要インフラ所管省庁の対応能力の向上

重要インフラの安全対策に直接の責任を有する重要インフラ所管省庁の対応能力の向上に一層の配慮が必要である。

また、事業法等の体系との整合化を図りながら、各重要インフラ分野ごとに異なる脅威に応じ、最低限講ずべき情報セキュリティ対策を定めていく[23]などの取組みを実施し、

---

18 独立行政法人情報通信研究機構

19 独立行政法人情報処理推進機構

20 平成14年に「インシデント情報共有･分析センター（Telecom-ISAC Japan）」として設立。平成17年2月に「財団法人データ通信協会」に編入。

21 有限責任中間法人 JPCERT コーディネーションセンター

22 「第1次提言」（3．1．3．(1)③;脚注 4 参照）及び「情報セキュリティ問題に取り組む政府の機能･役割の見直しに向けて」（平成16年12月7日 IT 戦略本部決定;脚注 5 参照）における定義を引いたものであり、以下本提言内において、「関係機関」とは、「警察庁サイバーフォース、NICT、IPA、Telecom-ISAC Japan、JPCERT/CC 等」を指す。

23「災害及び攻撃から重要インフラを防御するため、その情報システムが最低限満たすべき技術的水準及び運用基準について2004年9月までに官民で協力しつつ検討する（内閣官房及び関係府省）。」【e-Japan 戦略Ⅱ加速化パッケージ（平成16年2月6日IT戦略本部決定）】

重要インフラ事業者の自主的な対応を促進していくとの視点も必要である。

(3) 自然災害、物理的テロ等への対応における関係省庁等との連携の強化

自然災害[24]、物理的テロ等への対応との連動が必要であるとの観点から、特別行動計画等に基づく内閣官房、重要インフラ所管省庁及び各重要インフラ事業者間の情報共有、連絡・連携体制に加えて、内閣官房は、事案対処省庁や情報セキュリティ関係省庁、関係機関などとの連携を強化していくことが必要である。

(4) その他の視点

重要インフラにおいて利用される IT について、そのセキュリティ機能の強化の実現を図ることが重要である。その際、研究開発から実際の利用段階までを見据えた、体系的な取組みのあり方を視野に入れていくことが必要である。

また、重要インフラと政府との関係は、法令によって政府が関与可能な範囲とインフラ事業者が最低限行うべき範囲とが規定されるものであるという点、コスト面での実現可能性を視野に入れていくことが必要であるとの点についても、対策の具体化に当たっては重要な視点である。

[24]大規模災害等の緊急事態における情報収集等については内閣情報集約センターが担当しており、同センターとの連携も図っていく必要がある。

第4章　問題点解決のための具体的方策

本章では、前章で示した問題点と対策を具体化していく上での視点を前提とし、今後実行すべき具体的方策を提示する。

4．1．対象範囲等の見直し

本節では、想定する脅威の拡がりとそれに対応した対象事業及び分野の見直しに関する具体的方策を提示する。

4．1．1．想定する脅威の見直し

前章（3．1．2．）に述べたように、IT障害を引き起こす脅威には、サイバー攻撃だけなく、人為的なミスやITの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や、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。

これら多種多様な脅威に対応した総合的な対策を実施していく必要がある。

また、こうした想定する脅威の見直しに対応して、その概念や障害発生のメカニズムに関して確立した知見が存在しないこと等を踏まえれば、実在する脅威ごとに想定されるリスク、具体的にIT障害の発生に至るメカニズム及びその対策について、継続的に研究する機能も必要である。

4．1．2．対象事業及び分野の見直し

IT 利用の進展に伴う各事業サービスの供給や利用形態に与える変化や第1章で示した重要インフラの定義に照らし、現実のサービスの停止または機能低下等が国民生活や社会経済活動に多大なる影響を与えると考えられる対象分野や各分野の対象事業についても見直しが必要である。

このため、特別行動計画等で定めた情報通信、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）の既存7分野についても対象事業の見直しを行うとともに、1）医療[25]や水道、2）これまで重要インフラとして明示されていなかったものの、IT の利用拡大によってITの機能不全がサービス供給に多大な影響を及ぼす状況となり、また仮にサービス供給に障害が生じた場合に国民生活及び社会経済活動のみならず、他の重要インフラ分野へ多大な影響を及ぼしうると考えられる物流等を含め

[25] 「医療」については、既に「特別行動計画」のフォローアップにおいて、分野追加への検討が明記されている。

るべく、対象分野及び対象事業の見直しを行う。

また、当面の見直しを行うだけでなく、「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。

なお、政府・行政サービス（地方公共団体を含む）のうち、国が実施する部分については、第1次提言を踏まえた情報セキュリティ対策を推進する。

4．2．官民連携した機能・体制の強化

本節では、重要インフラにおけるIT障害への対策のうち、我が国全体として総合的に対応するに相応しい機能・体制の強化に向け、必要となる具体的方策を提示する。

4．2．1．重要インフラ横断的な状況把握機能の強化

（1） 機能・体制強化の方向性

前章でも指摘したように、従来の重要インフラにおけるサービスの維持、復旧等は個々の重要インフラ分野ごとに継続的な取組みが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 の利用が進展し、各重要インフラのサービス維持に当たっては、重要インフラ相互の依存が必須となっている現状等を踏まえれば、我が国全体として重要インフラの対策を向上させていくため、我が国全体での重要インフラ横断的な状況の把握が必要である。

また、適切なアクションプラン構築のため、それぞれの重要インフラの脅威への対応状況及び重要インフラが持つ脅威への対処能力を把握することが必要である。

（2） 具体的方策

それぞれの重要インフラのサービス提供が維持されるためには、他の重要インフラのサービス提供も維持されることが必要となっている。

このため、それぞれの重要インフラがもつ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を事前に把握するため、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。

4．2．2．総合的な対策の強化

(1) 機能･体制強化の方向性

サイバー攻撃だけでなく、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」全般に事業者自らが総合的に対応する能力を強化することが必要である。

なお、具体的方策の実施にあたっては、1)他の重要インフラ等へのIT障害の波及を考慮する観点から、相互依存性解析の結果を踏まえるという視点、2)重要インフラ所管省庁の対応能力を向上させるとの視点、3)各府省庁が有する情報セキュリティに関する機能や取組みを最大限に活用するという視点等が重要である。

(2) 具体的方策

具体的には、以下の方策を実施する。

① 重要インフラ分野ごとの「安全基準･ガイドライン」の作成

重要インフラ防護の観点から求められる種々の対策の中で、重要インフラが最低限講ずべき、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には、技術的水準及び運用基準についての「安全基準･ガイドライン」を策定することが効果的な方策である。共通の指針を元にこのような「安全基準･ガイドライン」を策定することは、重要インフラ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ためには有効であり、統一的な重要インフラ防護に資するものと考えられる。このため、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とが協力をしつつ、各重要インフラ分野ごとに「安全基準･ガイドライン」を策定する。

なお、上記「安全基準･ガイドライン」の策定に当たっては、以下の点を考慮することが必要である

1) 各重要インフラ分野ごとにⅰ)ITへの依存度、ⅱ)自然災害等の経験によりこれまでに構築してきた総合的な対策の内容に基づくこと。

2) 各事業法等の枠組みの下での、法的根拠に基づく強制基準、政府の策定する現行の事業法等に準じた性能規定[26]からなる推奨基準及びガイドライン、並びに民間が自ら定める業界標準、さらに業界各事業者が技術基準等の仕様レベルでの規定に関して自らの対処水準を定める自主基準･ガイドライン等の階層構造を念頭に

[26] 保安規程に、事業の継続性の確保に関する情報セキュリティ対策を講じることを盛り込む 等

おくこと。

3) 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される場合もあり得ること。

4) 各業界での「安全基準・ガイドライン」策定の後、必要に応じて「安全基準・ガイドライン」を更新する際には、業界間での情報交換を促進し、実効性の確保を図ること。

② 重要インフラ分野ごとの「安全基準・ガイドライン」の評価

重要インフラごとに策定される「安全基準・ガイドライン」に対し、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。

③ 重要インフラ所管省庁のリエゾン

内閣官房における重要インフラ分野への対応能力向上を図るため、重要インフラ所管省庁の担当者をリエゾンとして内閣官房に併任する。

4．2．3．重要インフラのサービスの維持・復旧等に資する情報を適切に提供・共有する体制の強化

(1) 機能・体制強化の方向性

① 3つの側面に応じた体制の強化

前述のように、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が責を担うべきであり、そのためには、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、各主体が協力することが重要である。

その中でも、IT障害に関する情報について、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つの側面それぞれに資するものを、適切に重要インフラ事業者に対して提供し、また事業者間で共有を行う体制を強化することが必要である。

すなわち、「IT障害の未然防止」の観点からは、障害発生の脅威に係る情報（防護方策等を含む）について、政府等から重要インフラ事業者へ円滑に提供する体制、並びに重要インフラ分野内において情報共有を行う体制を強化し、事業者個別の自主保安、障害の防止能力向上を促進していくべきである。

また、「IT障害の拡大防止・迅速な復旧の観点」からは、当該障害を早期に発見できる対策を平時より実施するとともに、何らかの障害が発生した場合には、相互依存性解析を踏まえて、当該障害発生に起因する脅威の具体化情報を適切な者に提供するとともに、既に障害が発生している重要インフラ事業者に対し復旧に資する情報の提供を行うなど、提供情報の充実や質の向上を図る等、官民の連絡・連携体制の一層強化を図るべきである。

さらに、「IT障害の要因等の分析・検証による再発防止」の観点からは、事業者における事後分析に資する情報を各主体が協同して収集するとともに、分析・検証の結果を重要インフラ分野内及び分野間で共有することが重要である。

② 既存機能の活用と人的・金銭的コストへの配慮

また、上記の実施に当たっては、既に各主体が有する機能について最大限活用を図るとともに、各主体の役割の明確化をし、かつ個別の主体に過度の負担が発生しないよう配慮した体制の構築が必要である。

特に、体制の構築・運用には多大な人的・金銭的コストが必要であり、特に緊急時には、膨大な量の業務が発生することが想定されることから、その望ましい分担のあり方を念頭に置き、実効性のある仕組みを構築するとともに、緊急時であっても平時と同様の仕組みで運用可能な体制となるよう、意識を払う必要がある。

(2) 具体的方策

具体的には、以下の方策を実施する（なお、以下の方策を実施した後の、新たな情報提供・共有体制のイメージについて、図3参照）。

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

重要インフラ各事業者のサービスの維持・復旧能力の向上のため、個々の事業者が努力するだけでなく、各重要インフラ内の情報共有を推進し、当該分野全体における取組みの底上げを図ることが重要である。

そのため、重要インフラ事業者を主体とした「情報共有・分析センター」（ISAC：Information Sharing & Analysis Center）等の各重要インフラ内情報共有機構の創設を図るなど、各重要インフラ内の情報共有体制を確立する。情報共有機構については、既に情報通信分野の一部においては

「Telecom-ISAC Japan」[27]として情報共有だけでなく、IT 障害への共同対処も行うなど、具体的な活動が開始されており、また地方公共団体間における情報共有体制の構築に向けた検討が行われつつあるところである。

なお、各重要インフラ分野において情報共有機構の検討を行うに当たっては、業界団体等、種々の情報を共有することが可能な既存の枠組みを活用することも可能であるが、既に取組みが進んでいる先行分野の体制構築に係る知見を共有しつつ、以下の機能を備える必要があることを考慮すべきである。

ⅰ）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

ⅱ）緊急時に各構成員及び外部との連絡が可能な窓口（POC[28]）が設定されていること

ⅲ）情報集約及び情勢判断を行う能力のあるコーディネータが配置されていること

また、情報共有体制の構築・運用には、人的・金銭的コスト負担が発生することが想定され、重要インフラ事業者に過度の負担が発生しないよう、体制のあり方、運用のあり方、及びコスト負担のあり方を検討する必要がある。

2）重要インフラ事業者に対する情報提供体制の整理・強化

重要インフラ事業者に対する情報提供については、特別行動計画に基づく情報提供の枠組みを拡大・発展させた、下記の体制において行う。

ⅰ） 素情報の収集

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。

ⅱ） 各種情報の整理

各主体が収集した情報は、可能な限りにおいて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、その情報の重要度や種類、性格等に応じて、体系的な採番・附番を行うことを検討すべきである。

---

[27] 脚注 20 参照。

[28] Point of Contact の略。

iii) 各種情報の提供

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、各事業分野の運用に関し直接的な知見を有する「各重要インフラ内の情報共有体制」を通じて、各重要インフラ事業者に情報提供を行う。

iv) その他の情報共有

個々の重要インフラ事業者や分野内情報共有機構が、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こともあり得る。

そのような場合であって、かつ関係機関と相互にその必要性が合意される場合には、契約等に基づき直接情報共有を行うことが適当である。

3) 我が国重要インフラ全体における情報共有の強化

サービスの維持･復旧に係る情報は、個別の重要インフラ分野ごとに完全に独立したものではなく、内容によっては複数の重要インフラ分野に共通したものであることもある。その場合、当該情報に最も精通した重要インフラ分野による検討結果を他の重要インフラ分野と共有することが極めて有用となる。

また、重要インフラ分野間の相互依存性を勘案すると、それぞれの重要インフラ分野が、他のインフラ分野における取組み状況等について相応に把握していることも重要となってくる。

そのため、重要インフラ横断的な情報共有の推進（例：重要インフラ横断的な情報共有機構（「重要インフラ連絡協議会」（仮称））の設立等）を図り、多様な知見をサービスの維持･復旧に活かすことを可能とする。

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

前述したように、多種多様な脅威を想定し、IT 障害全般を射程に入れていくこと（4．1．1．）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、特別行動計画等に基づく事業者からの提供情報の範囲について見直しを行うことが必要である。

なお、IT 障害が発生した場合には、各事業法等に基づき各重要インフラ事業者から重要インフラ所管省庁に対する報告義務が発生することがあるため、本項における事業者から内閣官房に対する情報提供は、各事業法等に基づく事業者から所管省庁に対する報告の範囲等を実効的に拡大しつつ、所管省庁から内閣官房に報告を行う形式で実施することが適当である。

ただし、本項に基づき拡大的に提供される情報は、サービスの維持･復旧を

最優先させるという観点から、あくまで緊急対処のために提供されるものであるため、提供される情報の内容によっては、各重要インフラ所管省庁が、当該情報を元に各事業法等に基づく処分等を実施することについては慎重な対応が必要である。また、重要インフラ事業者が、より積極的に情報提供ができるよう、その環境整備について引き続き検討することが求められる。

② 連絡・連携する「情報」の充実及び質の向上

1) 内閣官房が収集する情報の充実及び質の向上

重要インフラ事業者に提供すべき情報の質の強化を図るため、当該情報は内閣官房が独力で収集するだけでなく、情報セキュリティ関係省庁、事案対処省庁及び関係機関から内閣官房に対して積極的に情報提供がなされるべきである。この情報提供が円滑に実施され、また提供される情報が詳細かつ時宜を得たものとなるよう、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連携の強化を図る。

また、情報セキュリティ関係省庁、事案対処省庁及び関係機関は、内閣官房に提供する情報が質・量ともに充実するよう、能力向上のための措置を継続的に実施する。

2) 内閣官房から提供する情報の充実及び質の向上

内閣官房から各重要インフラ事業者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ごとに行うとともに、脆弱性情報等の早期警戒情報提供（優先的情報提供[29]を含む）のための枠組みを整備する。

なお、優先的情報提供については、それにより伝達される情報を知る者が可能な限り少数であることが望まれるとともに、当該情報を伝達すべき者には確実に伝達することが期待されることから、①の情報提供の体制を基本としつつも、情報を受け取る者が適切に制約されるよう、運用上の工夫を行うことが必要となる。

③ IT 障害発生時対応の強化

（1）に示したように、平時から緊急時と同様の仕組みによって、情報共有等を実施す

[29] 例えば、公表前の脆弱性情報を特定の者に優先的に提供し、早期の対処を促す仕組み。

ることが適当であるが、緊急時には情報収集及び復旧に係る業務量が膨大となることが想定される。

このため、各重要インフラ事業者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への支援、助言等の機能を強化する。

さらに、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持つことが望まれる。

また、IT 障害発生時に内閣官房が重要インフラ分野間のコーディネーションを迅速かつ的確な対応を行えるよう、重要インフラ所管省庁の担当者を、平時からリエゾンとして内閣官房に併任する。

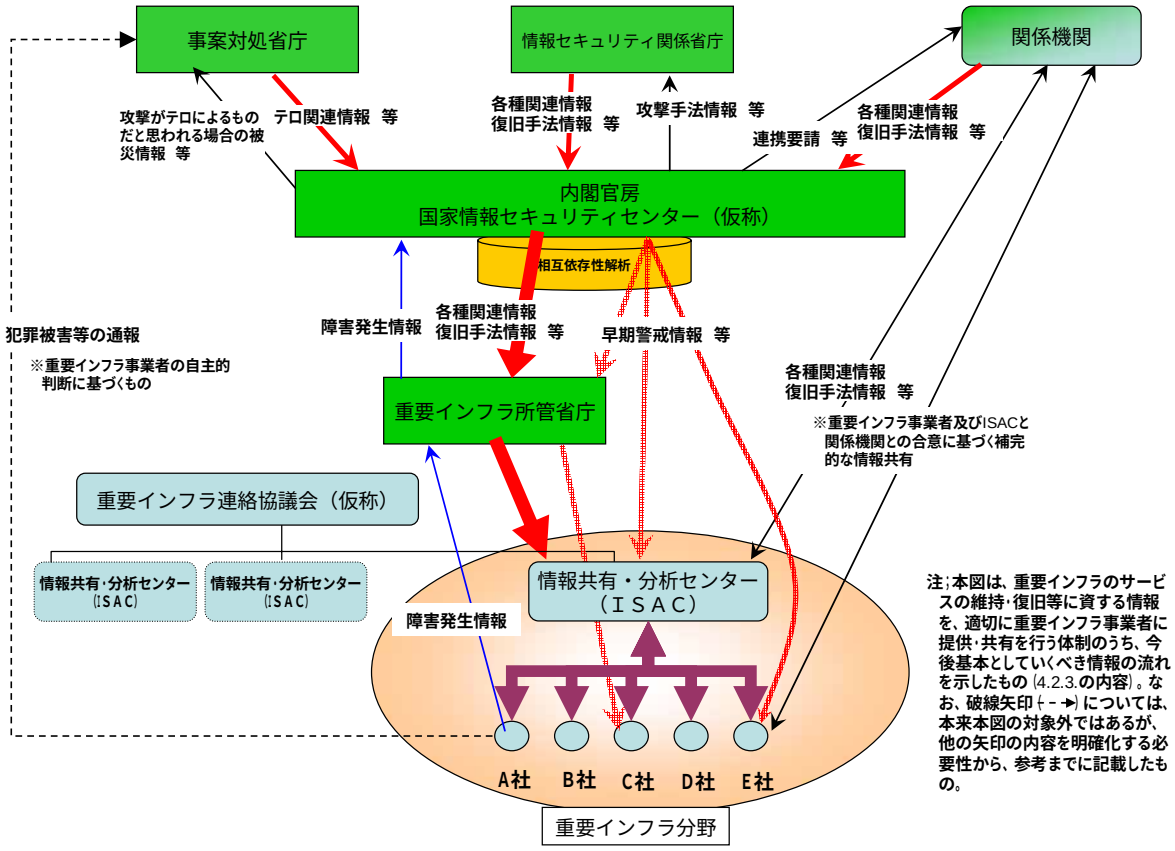


図3：情報提供・共有体制のイメージ

4．2．4．総合的演習を通じた機能･体制の検証と見直し

官民の情報共有、連絡･連携のための仕組みがいかに入念に制度設計されたとしても、実際のIT障害の発生及び未然防止の場面で有効に機能しなくては意味をなさない。特に、前節（4．2．3．）に示したように、想定脅威の拡大と重要インフラ間の相互依存性の増大により、連携、協力すべき主体の範囲は飛躍的に拡がっており、各主体間での情報共有や連携の仕組みの妥当性も平時から各主体が連携する状況を総合的演習の形で模擬的に再現し検証しながら、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。

（1） 類型化された脅威シナリオに基づく総合的演習の実施

4．1．で示された想定脅威の拡がりに対応した具体的脅威シナリオの類型を元に毎年度ごとにテーマを設定し、各重要インフラ事業者、各重要インフラ分野内情報共有機構等の協力を得ながら、重要インフラ横断的な総合的演習を企画･実施する。その際、以下の点を中心に検証･見直しを行っていくことが重要である。

① 情報の提供または共有範囲の妥当性と情報到達度の確認
② 各主体ごとの処理及び判断能力
③ 相互依存性が的確に反映されたか否か

（2） 総合的演習結果を踏まえた対応能力の向上

総合的演習の結果を踏まえて、情報共有及び連絡･連携体制の見直しを行うことと併せて、各重要インフラ所管省庁の対応能力を向上させていくことが重要である。

4．2．5．人材育成･研究開発

（1） 機能･体制強化の方向性

我が国全体の重要インフラ防護に資するためには、重要インフラ事業者等の担当者に、情報セキュリティやITの専門性と個別重要インフラ部門の専門性が融合した人材が継続的に配置されることが必要である。

特に、官民の情報共有体制を効果的に運用するためは、関係する各主体相互間の信頼関係が最も重要となることから、当該信頼関係の裏づけとなりうるキーパーソンの育成が強く求められる。

また、重要インフラにおけるIT利用について、その脅威への対応の強化、特に、研究開発･技術開発から実際の利用段階までを見据えた、体系的な取組みのあり方を構築

することが必要である。

なお、重要インフラにおける情報セキュリティ対策に資する研究開発・技術開発の観点からは、新しい技術によってその基盤自体がセキュアになるという、動的かつ将来に向けた取組み（例えば、情報通信インフラにおける次世代ネットワークの実現と展開など）の重要性を認識することが必要である。

(2) 具体的方策

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[30]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

「情報セキュリティ政策会議（仮称）」及び「国家情報セキュリティセンター（仮称）」において行う、「情報セキュリティに関する我が国の基本戦略」、特に「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。

4．2．6．サイバーテロ等への対処を行うための事案対処省庁の取組みの強化

上記4．2．1．から4．2．5．に示した方策は、国民生活・経済活動の根幹である重要インフラのサービスの維持と迅速な復旧等の確保を図るとの大目的（1．3．）を前提とし、重要インフラ事業者の事業継続性確保のための機能の強化・整備について提示したものであるが、これに併せ、テロ・犯罪事案が発生した場合やその事前対策等の観点からの取組みも、車の両輪として重要である。また、IT 障害等が発生した時点においては、テロ・犯罪事案か否かの判断が困難であることを踏まえた対応を行うことが重要である。

このため、例えば、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・強化することが必要である。

---

[30] 職業人を中心とした社会人に対し、学校における教育を終えて社会に出た後に行われる各種の教育のこと。「リカレント」は“循環する”を意味する語。

４．２．７．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なく、我が国全土にわたって講じられるべき問題である。特に、災害に起因する IT 障害発生時の対応の迅速性、正確性を確保する観点からは、IT 障害発生現場に近い地域レベルで官民の連絡･連携体制を強化していくことが必要である。

このため、関係する政府地方支分部局、地方自治体、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していくことが必要である。

なお、実際の連絡･連携体制の構築に当たっては、重要インフラごとに個々の事業者によるサービス対象エリアが異なること、それに伴い個別地域ごとに構築すべき体制や経費負担のあり方が異なることが予想されることを念頭に置くことが必要である。

第5章　実現のための行動計画

本章では、前章で示した「実行すべき具体的方策」を実現していくために、それぞれの実施主体が今後、いつまでを目処に取り組み、機能を整備するべきかについての行動計画を提示する。

5．1．全体の目標

前章（4．2．）でも示したように、今般提示した方策は、重要インフラにおけるIT障害への対策のうち、我が国全体として総合的に対応するに相応しい機能・体制の強化に向け、必要となるものであり、言い換えれば、新たに内閣官房の「国家情報セキュリティセンター（仮称）」が設立されるにあたり、本センターを中心として講じられる対策を基軸に展開したものと言える。

一方で、日々増大していく脅威に対する重要インフラにおける情報セキュリティ対策の強化は喫緊の課題であり、これを可及的速やかに実施に移していくことが必要である。

したがって、これを可能な限り早期に実現していくため、平成17年度より発足予定の「国家情報セキュリティセンター（仮称）」の主導の下、各関係者において必要な準備を進め、平成18年度より、内閣官房の「国家情報セキュリティセンター（仮称）」を中心とし、前章までに提示した新たな機能を有する重要インフラにおける情報セキュリティ対策の新体制が稼働することが望まれる。

この際、内閣官房は、各関係者の協力を得て、平成18年度の稼働にあわせ、前章までに示した対象範囲等の見直しや、機能・体制等の整備・強化を反映し、現行の特別行動計画の改訂案を策定し、「情報セキュリティ政策会議（仮称）」にて審議・決定を行うことを目指すものとする（平成17年度中）。

以下、①内閣官房（「国家情報セキュリティセンター（仮称）」）、②重要インフラ事業者、③重要インフラ所管省庁、④情報セキュリティ関係省庁、⑤事案対処省庁、⑥その他関係省庁・関係機関のそれぞれにおいて、整備すべき機能を提示する。

5．2．内閣官房が取り組むべき事項

5．2．1．内閣官房において整備・強化すべき機能

内閣官房は、前章に示した具体的方策のうち、以下の機能の整備に取り組む。

(1) 重要インフラ分野横断的な対策

以下の項目は、重要インフラ分野横断的に実施すべき対策であり、我が国全体として取り組む必要があることから、内閣官房において主体的に行うべきものである。

○ 実在する脅威と障害発生のメカニズム及びその対策についての継続的研究の実施（**4．1．1.**）
○ 重要インフラの自然災害、物理的テロ等への対応との連動体制の構築（**3．2．2.**）
○ 重要インフラ横断的な状況把握（相互依存性解析等）の実施（**4．2．1.**）
○ 毎年度ごとにテーマを決めた「総合的演習・訓練」の企画・実施（**4．2．4.**）
○ 各重要インフラ分野ごとの「安全基準・ガイドライン」の作成支援（**4．2．2.**）
○ 相互依存性解析に基づく各重要インフラごとの「安全基準・ガイドライン」の評価（**4．2．2.**）
○ 情報セキュリティに関する我が国の基本戦略、特に情報セキュリティに関する研究開発・技術開発戦略（センターにて立案予定）において、重要インフラ対策全体に資する視点を付与し、脅威全般への対応能力の強化に資する研究開発を促進（**4．2．5.**）

(2) 政府・重要インフラ事業者間での体系的な情報共有体制の整備

特別行動計画で規定されている官民の連絡・連携体制を発展的に拡大・強化し、俯瞰的な情報共有体制を整備する必要から、内閣官房において実施すべき対策を挙げる。

○ 保有する能力・機能に応じた、重要インフラ事業者に提供すべき情報（テロ関係情報、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）の収集（**4．2．3.**）
○ 政府から重要インフラ事業者への提供情報の強化（**4．2．3.**）
  - 整理・集約した情報を、重要インフラ所管省庁を通じて、重要インフラ事業者に対して提供
  - 相互依存性解析等による優先度設定に基づき、脆弱性情報等の優先的情報提供のための枠組みを強化
  - 情報の提供に当たっては、情報の受領者が当該情報を活用しやすいように、整理した上で、情報の重要度（影響度）に応じて体系だった採番の実施を検討
  - 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連携を強化
○ IT 障害発生時等緊急時にインフラ事業者間のコーディネーションを実施できるセン

ター機能を創設（**4．2．3．**）

○ 重要インフラ横断的な情報共有の推進（例：重要インフラ横断的な情報共有機構（「重要インフラ連絡協議会」（仮称））の設立支援等）（**4．2．3．**）

(3) 各主体との連携強化・能力向上支援

我が国全体としての重要インフラ防護に資する各主体との連携について、内閣官房が総合調整の立場から実施すべき対策を挙げる。

○ 演習・訓練及びセミナー等を通じた、高度な IT 人材の育成（**4．2．5．**）

○ 重要インフラ所管省庁の担当者を、リエゾンとして内閣官房（センター）に併任（**4．2．2．**及び**4．2．3．**）

5．2．2．内閣官房において構築すべき体制

5．1．1．の機能を迅速かつ効果的に実施すべく、内閣官房においては、平成17年度より新たに稼働する「国家情報セキュリティセンター（仮称）」に、上記の機能を総合的に実施する重要インフラ担当の専門部門を設置し、平成18年度より新体制にて活動を開始する。

その際、1)「政府機関の事案対処支援」（第1次提言2．2．3．及び IT 戦略本部決定（平成16年12月7日）2．③[31]）において収集・分析した情報を必要に応じて活用すること、2)重要インフラ所管省庁におけるリエゾンとの緊密な連携等を行うべく、各重要インフラ部門ごとの担当者を設置して専門性を確保すること、3)各重要インフラにおける情報等を扱うことから、人的・物理的側面からもその機密の保持を確保し、信頼性の高い情報交換を行うことのできる環境を整備することが必要である。

5．3．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

5．3．1．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整備・強化すべき機能

各重要インフラ事業者及び重要インフラ所管省庁は、前章に示した具体的方策のうち、以下の機能の整備に取り組む。

[31] 脚注５参照。

(1) 全体的な取組み

我が国全体として重要インフラ防護を強化するために、内閣官房が行う対策と連動して、各重要インフラ所管省庁が実施すべき取組みを挙げる。

○ 重要インフラの自然災害、物理的テロ等への対応との連動体制の構築（**3．2．2.**）
○ 内閣官房と共同し、毎年度ごとにテーマを決めた「総合的演習・訓練」の企画・実施（**4．2．4.**）
○ 各重要インフラ分野ごとの「安全基準・ガイドライン」の作成、その支援及び評価（**4．2．2.**）

(2) 政府・重要インフラ事業者間での体系的な情報共有体制の整備

実効性のある官民の連絡・連携体制のために、内閣官房で行う対策と連動して、重要インフラ事業者及び各重要インフラ所管省庁が実現すべき機能を挙げる。

○ 保有する能力・機能に応じた、重要インフラ事業者に提供すべき情報（テロ関係情報、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）の収集（**4．2．3.**）
○ 内閣官房から提供された情報を、各重要インフラ内の情報共有機構を通じて、各重要インフラ事業者に提供（**4．2．3.**）
○ 各重要インフラ内の情報共有の推進（例：「情報共有・分析センター」（ISAC）等の各重要インフラ内情報共有機構の創設等）（**4．2．3.**）
○ 「想定する脅威の見直し」（**4．1．1.**）に対応し、事業者から提供される IT 障害に係る情報の範囲等を実効的に拡大（**4．2．3.**）
○ 重要インフラ所管省庁の担当者を、リエゾンとして内閣官房（センター）に併任（再掲）

5．3．2．各重要インフラ事業者において構築すべき体制

5．3．1．の機能を迅速かつ効果的に実施すべく、各重要インフラ事業者においては下記の体制を構築する。

○ 内閣官房（センター）における体制構築（**5．2．2.**）にあわせ、各重要インフラ内の情報共有推進のための体制構築（例；「情報共有・分析センター」（ISAC）等の各重

要インフラ内情報共有機構の創設）や「安全基準・ガイドライン」作成のための体制を構築し、平成18年度より活動を開始。

○ 重要インフラ横断的な情報共有の推進（例：重要インフラ横断的な情報共有機構（（「重要インフラ連絡協議会」（仮称））の設立等）についても同時並行で実施（**4．2．3．**）

○ 所管省庁との緊密な情報共有体制の構築（**4．2．3．**）

5．3．3．重要インフラ所管省庁において構築すべき体制

5．3．1．の機能を迅速かつ効果的に実施すべく、各重要インフラ所管省庁においては下記の体制を新たに構築する。

○ 上記各重要インフラ内の情報共有推進のための体制構築や「安全基準・ガイドライン」作成のための金銭的・業務的支援のための体制を構築（**4．2．2．**及び**4．2．3．**）

○ 重要インフラ横断的な情報共有の推進（例：重要インフラ横断的な情報共有機構（（「重要インフラ連絡協議会」（仮称））の設立支援等）への支援体制の構築（**4．2．3．**）

○ 重要インフラ事業者との緊密な情報共有体制の構築（**4．2．3．**）

○ 重要インフラ所管省庁から重要インフラ事業者への支援、助言等を強化（**4．2．3．**）

5．4．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

従前より情報セキュリティに関する取組みを政策的に行っている情報セキュリティ関係省庁が、内閣官房を中心とした我が国全体としての重要インフラ防護に資するために、実施すべき取組みを以下に挙げる。

○ 保有する能力・機能に応じた、重要インフラ事業者に提供すべき情報（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）の収集（**4．2．3．**）

○ 重要インフラのサービスの維持・復旧に資する情報の適切な収集・提供・共有を行う体制の強化を行う観点からの、内閣官房との連携の強化（**4．2．3．**）

○ 情報セキュリティ関係省庁における取組み（対処能力の向上等）を継続的に実施（**4．2．3．**）

5．5．事案対処省庁において整備･強化すべき機能･体制

サイバーテロ等の事案への対処を行う事案対処省庁が、内閣官房を中心とした我が国全体としての重要インフラ防護体制に資するために、実施すべき取組みを以下に挙げる。

○ 保有する能力･機能に応じた、重要インフラ事業者に提供すべき情報（テロ関係情報、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）の収集（**4．2．3．**）
○ 重要インフラのサービスの維持･復旧に資する情報の適切な収集･提供･共有を行う体制の強化を行う観点からの、内閣官房との連携の強化（**4．2．3．**）
○ サイバーテロ等への対処を行うべく、事案対処省庁における取組み（対処能力の向上等）を継続的に実施（**4．2．6．**）

5．6．その他関係省庁･関係機関において取り組むべき事項

前節までの各実施主体以外にも、我が国全体としての重要インフラ防護体制の強化のために実施すべき対策とその主体を挙げる。

○ 官民連携に基づく情報提供･共有体制を補完する情報を、重要インフラ事業者や重要インフラ内情報共有機構に提供（**4．2．3．**）
○ 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（**4．2．5．**）。
○ 地域レベルの取組みの促進（**4．2．7．**）。

以上

(参考) 第2次提言までの検討の経緯

【情報セキュリティ基本問題委員会】

2004年10月26日　第3回会合

第2分科会について

2005年1月31日　第4回会合

第2分科会の検討状況報告

2005年3月28日　第5回会合

「第2次提言(案)」の検討

【情報セキュリティ基本問題委員会第2分科会】

2004年12月9日　第1回会合

(1) 「第2分科会」の設置について
(2) 会議の公表について
(3) 本分科会での討議について

2004年12月24日　第2回会合

(1) 重要インフラ事業者委員からのヒアリング
(2) 各府省庁からのヒアリング
(その1)

2005年1月12日　第3回会合

(1) 重要インフラ事業者委員からのヒアリング
(2) 各府省庁からのヒアリング
(その2)

2005年1月21日　第4回会合

「第4回基本問題委員会への中間報告案の検討」の検討

2005年2月17日　第5回会合

(1) 第4回情報セキュリティ基本問題委員会における審議結果の報告
(2) 重要インフラが直面する脅威の具体像(サイバー攻撃を中心として) ― 三輪委員からの報告
(3) 重要インフラ間の相互依存性解析の有効性について ― 渡辺委員からの報告
(4) 第2次提言における対策の具体化項目(案)の検討

2005年3月2日　　第6回会合

「第2次提言骨子（案）」の検討

2005年3月16日　　第7回会合

「第2次提言（案）」の検討

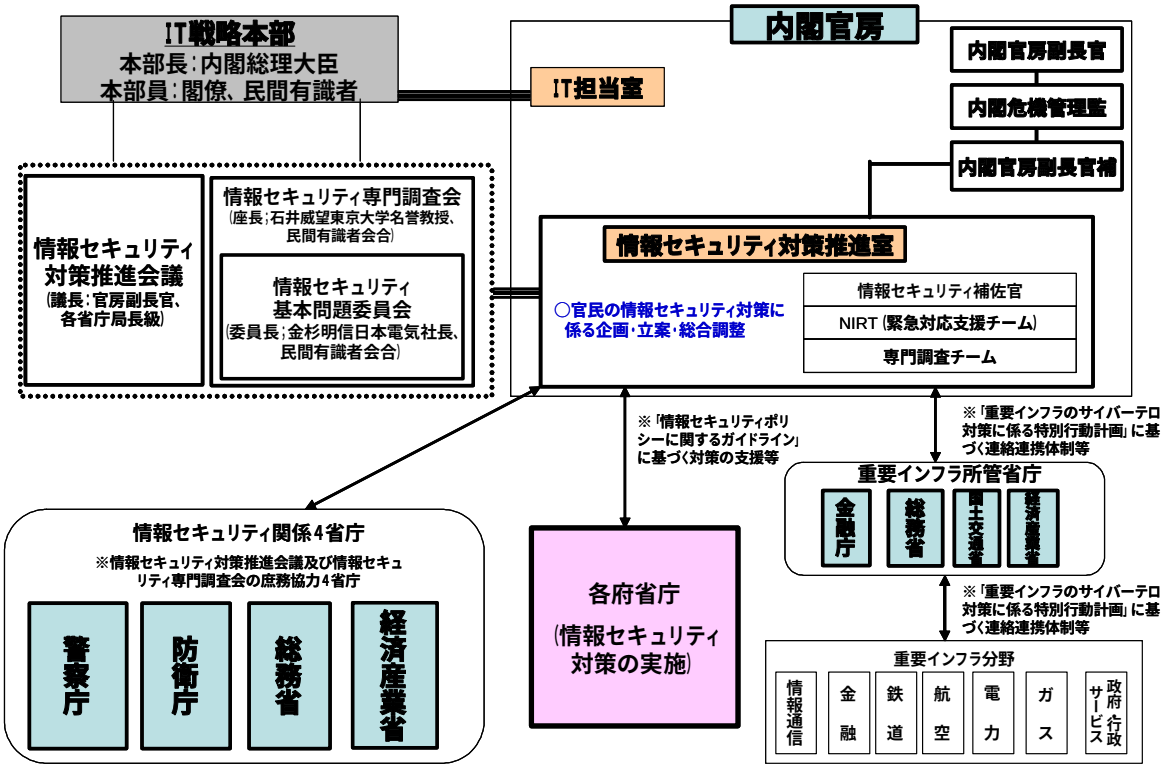
2005年3月22日　　第8回会合

「第2次提言（案）」の検討

関 連 資 料

参考資料1

我が国の情報セキュリティ対策に係る現在の体制



参考資料2

本分科会にて実施した重要インフラ事業者ヒアリングについて

【趣旨】

重要インフラにおける情報セキュリティ対策に係る政府としての取組みは、これまで特別行動計画を中核として継続的に行われてきており、重要インフラに対するヒアリング等も過去に行われた経緯がある。

一方、近年における IT 利用の急速な進展により、重要インフラを取り巻く環境が大きく変化しているとの視点があり、また本分科会で新たに掲げられた、1）サイバーテロ以外の脅威に対する対処、2）重要インフラ相互依存性に基づく対策の実施、に資するという目的で、本分科会にて、改めて重要インフラ分野ごとに情報セキュリティ対策についてのヒアリングを実施することとした。

【実施の状況】

ヒアリングは事務局にて策定した質問項目（別紙1参照）に対して回答につき、各重要インフラ分野（特別行動計画に記述された、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）の7分野）から選任された分科会委員が発表するという形式で行われた。ただし、発表内容は質問への回答のみに限定せず、広く重要インフラにて取り組んでいる対策・体制等も含んでいた。

ヒアリングは第2回（12月24日）、第3回（1月12日）の2回に分けて行われ、結果を整理したものを別紙2に掲げる。

別紙1

事業者委員からのヒアリング項目

2004年12月9日
情報セキュリティ基本問題委員会第2分科会事務局

【従来の取組みの検証】

＜Ⅰ．個々の重要インフラにおける経験等＞

1．貴業界（団体）では、いわゆる情報セキュリティ対策としてどのようなものを実施されていますか。情報通信インフラなどでは多くの対策を講じていると思いますが、その場合は、特に重要、有効と考えられる対策を挙げてください。
2．貴業界（団体）は近年「IT事故（仮称）」（注）に遭遇されたことがありますか。あるとすれば、その際どのように対処されましたか。また、その経験を踏まえて、今後措置すべき点等はございますか。
3．貴業界（団体）ではサイバーテロに対応するために、どのような対策を実施されていますか。例えば、サイバーテロを想定した演習等をされていますか。
4．貴業界（団体）は近年サイバー攻撃、あるいはそのおそれのある事態に遭遇されたことがありますか。あるとすれば、それらはどのような経験ですか。また、その際「重要インフラのサイバーテロ対策」に基づく取組みで十分対処できましたか。対処できなかったとすれば、その原因は何ですか。

＜Ⅱ．重要インフラ間の相互依存性＞

1．他の重要インフラ事業者から提供されるサービスが、貴業界（団体）における事業継続性確保のリスク要因となっていますか。なっているとすれば、具体的な対策として何をされていますか。
2．重要インフラの障害発生等による被害の最小化や復旧の迅速化のために、重要インフラ間の相互依存性を考慮する対策が重要だと考えますか。また、事業継続性の確保に向けた重要インフラ横断的な演習や重要インフラにおける情報共有・連携体制のあり方の検討等についてどのようにお考えですか。

【重要インフラを取り巻く環境の変化と脅威についての再整理】

＜III. 経営効率化と情報セキュリティ確保の関係＞

1．貴事業（団体）における IT の利活用はどの程度進んでいますか。特に、重要インフラを担うシステムについて、汎用システム製品の利活用はどの程度進んでいますか。代表的な事例を挙げてご説明下さい。（尚、ここでいうシステムは個人情報を扱うものに限定は致しません。）

2．経営効率化あるいはその他の要請から、今後とも汎用システム製品（パッケージソフト等）の利活用は進展するとお考えですか。理由とともにお教えください。

＜IV. 想定する脅威の範囲＞

1．IT を利用したシステムに関してどのような脅威を想定し、それらに起因するリスクに対してどのような対策を取っていますか。また、現在想定している脅威以外にどのような脅威を勘案すべきと考えますか。

（ア）（設問オプション）情報通信インフラにおいては特徴的なものを例示してください。

2．社内システム（制御系含む）における重要データ改ざん、および流出のリスクはどの程度大きいと考えますか。

3．2のリスクに向けた対策は、どのようなものが有効ですか。

＜V．各分野における取組みの進展の利用可能性＞

脆弱性情報、脅威情報等の提供元として、御社独自の情報源や業界内の連携体制、所管省庁からの連絡体制等が構築されていると思われますが、それに加えて、「可能な限り早期に情報を入手し対策をとる」ための情報（早期警戒情報）は必要だと考えますか？また、必要であると考える場合、この情報を円滑に入手するための新たな仕組みは必要と考えますか。

（注）サイバー攻撃に加え、情報資産に係るその他のリスク（コンピュータウイルス、不正アクセス、災害などの外部要因、従業員及び委託先の過失・犯行、システム障害などの内部要因）に起因する事件や事故を「IT 事故（仮称）」と定義する。なお、情報資産とは、重要インフラ事業者にとって価値を有する情報そのもの（企画、運転計画や営業などの情報、稼働状態逐次情報、緊急時対応情報、バックアップデータ、顧客情報、知的財産などのデータベース、資料など）と、その情報を可用化する環境（ソフトウェア（アプリケーション、システムソフトウェア、ユーティリティ ）、ハードウェア（コンピュータ装置、通信装置、メディアなど）等）を指している。

別紙2

重要インフラ事業者委員に対するヒアリング結果の概要整理

2005.1.21
情報セキュリティ基本問題委員会
第2分科会事務局

1. 個々の重要インフラにおける情報セキュリティ対策及び「IT 事故」(仮称)経験等について

【事務局まとめ】

○ 各事業者とも、情報セキュリティ対策を、制御系と情報系(業務系／事務処理系)とに分けて実施。

○ 制御系については、外部ネットワークとの分離による防護を基本とし、対策を入念に行っている事業者が太宗。

○ 情報系(業務系／事務処理系)については、情報セキュリティ対策を積極的に実施しているものの、情報漏洩や内部要因による障害発生などのリスクを強く意識している事業者が太宗。

○ 「IT 事故」(仮称)の経験については、サイバー攻撃の被害経験は少ないが、地震等の自然災害によるもの、内部的なワーム感染などの経験の指摘もあり。

○ 「サイバーテロを想定した演習」については、業界として取り組んでいる事例がある一方、災害時等を想定した一般的な訓練の一環として行っているとの事業者が太宗。また、重要インフラ間の横断的な演習の実施が有効との事業者もあり。

2. 重要インフラにおける相互依存性及び事業継続性の確保について

【事務局まとめ】

○ 多くの事業者が、特に電力事業に対し、依存性が高いと認識。事業継続性の確保のために、UPS 装置の設置やバックアップ電源の確保等の対策を行っている事業者が多い。更なる対策として、手動操作(運転員)による対応を手当てしている事業者もあり。

○ 災害等が起こった場合に、移動電源車の配備計画や電源復旧計画等の情報が共有されていると、自らの事業の迅速な復旧に役立つとの指摘もあり。

○ 情報通信事業への依存性の指摘もあり、事業継続性確保のために、自営回線の確保による対応を行っている事業者がいる一方で、NTT 等との契約による回線の多重化で対応している事業者もあり。

○ 「地域単位」で重要インフラ相互の情報共有等を行うことは、全体として事業の継続性の向上を図るために有効であるとの指摘あり。

3. 汎用システムの利活用度について

【事務局まとめ】

○ 基本的に、特に制御系のシステムについては、汎用システムではなく独自システムを構築している事業者が太宗。一方で、1）部分的に汎用システムを活用している事業者が既に存在するとともに、2）今後、経営効率化の観点から、独自のシステムから汎用システムへの切り替えの必要性についての認識を指摘する事業者もあり。

○ 情報系（業務系／事務処理系）については、インターネットの活用も含め、汎用製品によるシステム構築を行っている事業者が太宗。

4. 想定する脅威の範囲について

【事務局まとめ】

○ 自然災害、障害、不正行為に至るまで、サイバー攻撃以外にも様々な脅威を想定している事業者が太宗。

○ 外部からの攻撃等の外部的脅威に対しては、物理的入退室管理や外部ネットワークとの分離を理由に、そのリスクは小さいと認識している事業者が太宗。

○ 内部的脅威に対しては、実際に事故を経験している事業者もあるとともに、制御系のシステムに対する脅威も含め、常にそのリスクは起きる可能性があると認識している事業者が太宗。

5. 重要インフラにおける早期警戒情報等の必要性について

【事務局まとめ】

○ ソフトウェアの脆弱性情報等についての「早期警戒情報」については、外部ネットワークとの分離を理由に、その必要性は小さいとする事業者がある一方で、可能な限り早期に情報を入手することが対策の実施上有効であるとする事業者もあり。

○ 情報の信頼性と重要度の評価、情報の早期公表によるリスク評価等についての検討が必要であるとの事業者もあり。

○ 「早期警戒情報」ではないが、プラント系システムのトラブル事例等整理された情報提供が行われることは有効との事業者もあり。

○ 「早期警戒情報」に限らず、重要インフラ事業者間、自治体間、同一地域等において、情報の共有のみならず、脅威や対策を評価する仕組み、対策を助言する仕組みが重要であるとの指摘もあり。

以 上