「重要インフラのサイバーテロ対策に係る特別行動計画」関連資料

＜目次＞

重要インフラのサイバーテロ対策に係る特別行動計画
(概要)

1　目的

いわゆるサイバーテロなど、情報通信ネットワークや情報システムを利用した、国民生活や社会経済活動に重大な影響を及ぼす可能性があるいかなる攻撃からも重要インフラを防護する。

2　対象とする重要インフラ分野

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。）

3　官民におけるサイバーテロ対策

(1) 被害の予防（セキュリティ水準の向上）

被害を予防するため、その前提として、対象となる重要インフラの情報システムのリスク分析を行い、情報システムの重要度に応じた対策を講ずることによって、恒常的に各重要インフラ分野のセキュリティ水準の向上を図る。

(2) 官民の連絡・連携体制の確立・強化

セキュリティ情報（セキュリティ改善に必要な情報）及び警報情報（サイバー攻撃の発生情報等の警戒や緊急対処に必要な情報）の共有、予防・対処等を連携して行うための官民における体制の確立・強化を図る。

(3) 官民連携によるサイバー攻撃の検知と緊急対処

各重要インフラ分野においてサイバー攻撃を受けた場合又はそのおそれがある場合の対応策を定めるとともに、官民全体で対処能力の強化を行う。

(4) 情報セキュリティ基盤の構築

サイバーテロ対策を進めていくため、人材の育成、研究開発、普及啓発、法制度の整備等の情報セキュリティ基盤の構築を推進する。

(5) 国際連携

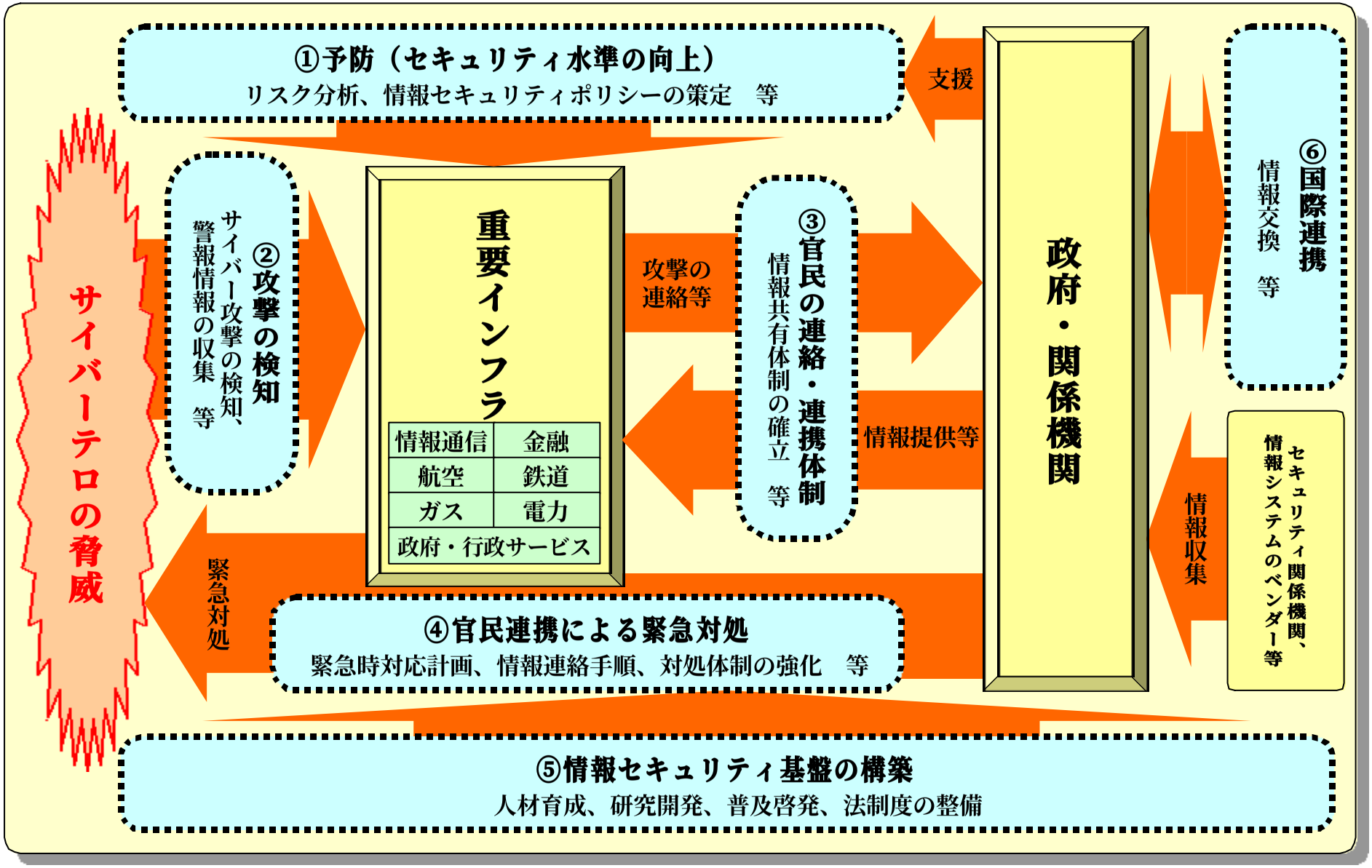
サイバー攻撃は、国境を越えて行われる可能性があることから、このような攻撃に適切に対処するため、国際的な連携を推進する。

4　行動計画の見直し

この行動計画は、官民の連絡・連携体制の確立を中心としてとりまとめた初めてのものであり、政府は、この進捗を踏まえ、定期的及び必要に応じ見直しをする。

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概要

目的　いわゆるサイバーテロなど、情報通信ネットワークや情報システムを利用した、国民生活や社会経済活動に重大な影響を及ぼす可能性があるいかなる攻撃からも重要インフラを防護する。



平成１２年１２月１５日
情報セキュリティ対策推進会議

重要インフラのサイバーテロ対策に係る特別行動計画

１　特別行動計画の目的

この特別行動計画の目的は、いわゆるサイバーテロなど、情報通信ネットワークや情報システムを利用した、国民生活や社会経済活動に重大な影響を及ぼす可能性があるいかなる攻撃からも、重要インフラを防護することである。

政府は、内閣官房を中心として、官民の緊密な協力の下、この計画の実施に努めることとし、民間重要インフラ分野の事業者及び地方公共団体（以下「民間重要インフラ事業者等」という。）においては、この計画を指針として、自主的な取組の強化を図るものである。また、政府は、民間重要インフラ事業者等における計画の実施に当たっては、必要な協力を行うこととする。

２　いわゆるサイバーテロの脅威

産業や政府の活動の多くは、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る。重要インフラにおいても、電力供給、交通、電子政府等の国民生活や社会経済活動に不可欠なサービスの安定的供給や公共の安全の確保等に関する重要な役割を情報システムが果たすようになってきている。

このような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（以下「サイバー攻撃」という。）が行われた場合には、国民生活や社会経済活動の混乱、国民の生命の危険などの重大な被害が生ずるおそれがある。このような攻撃は、他の物理的攻撃と異なり、情報システムに侵入する技術を有する者であれば、一台のコンピュータによって行うことも可能な一方、国民生活や社会経済に

混乱を引き起こすこと等を目的として組織的に大規模な攻撃が行われることも懸念されている。

外国においては、金融関係等の情報システムが被害を受けた事例や、個人がいわゆるハッカーとして、重要インフラ等の情報システムに対する侵入、サービス不能攻撃(DoS 攻撃)、コンピュータウイルスの流布等によって重大な被害を起こした事例もあり、このような脅威は現実のものとなってきている。米国においては、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に対して、国家計画の策定などに取り組んでいるところである。

また、インターネット等の他のネットワーク等との接続が進むことによって相互依存性が高まっていくこと及び情報システムの仕様の標準化や共通化が進展していることから、現時点では外部からの侵入の危険性が少ない情報システムについても、このような脅威は増大していくこととなる。さらには、内部関係者の関与等の脅威にさらされる可能性は常に存在しており、また、他のネットワークとは接続していないとされている情報システムであっても、外部からの侵入の危険性を排除することはできないことを認識しなければならない。

3　重要インフラ分野

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。ただし、新たな脅威等を踏まえ、本行動計画で対象とする重要インフラ分野について、適宜、見直しを行うこととする。

各重要インフラ分野を所管する省庁は、所管分野がこの計画を適切に実施できるよう協力することとする。

なお、いわゆるサイバーテロの脅威から、我が国の重要インフラを防護するため、これらの重要インフラ以外の分野においても、必要に応じ、この特別行動計画を参考として、対策の強化を図ることが重要である。

４　被害の予防（セキュリティ水準の向上）

被害を予防するためには、その前提として、対象となる重要インフラの情報システムのリスク分析を行い、情報システムの重要度に応じた対策を講ずることによって、恒常的に各重要インフラ分野のセキュリティ水準の向上を図ることが必要である。

(1) 民間重要インフラ分野等のセキュリティ水準の向上

○　民間重要インフラ事業者等は、「情報セキュリティポリシーに関するガイドライン」（平成１２年７月１８日、情報セキュリティ対策推進会議決定）や各省庁の情報セキュリティ関連ガイドライン、ＯＥＣＤのセキュリティガイドライン等を参考としてリスク分析や情報セキュリティポリシーを策定するなど、セキュリティ水準の向上に努める。

○　各民間重要インフラ分野及び地方公共団体（以下「民間重要インフラ分野等」という。）においては、仕様が共通する情報システムを使用する場合又は互いに情報システムを接続する場合において、分野に共通するリスクに対し適切な対処を行うため、各民間重要インフラ分野等における対策指針の策定について検討する。

○　政府は、民間重要インフラ事業者等のセキュリティ水準の向上に資するために、情報の提供、助言、指導等、民間重要インフラ事業者等の取組に対する支援の一層の推進に努める。

(2) 電子政府の構築に向けたセキュリティ水準の向上

○　各省庁は、平成１５年度までに電子政府の基盤を構築することを踏まえ、「情報セキュリティポリシーに関するガイドライン」を踏まえて策定したポリシーに従い、セキュリティ水準の向上のため必要な措置を講ずる。

○　内閣官房の専門調査チームによる、各省庁の情報システムのセキュリティ対策に係る技術的調査・助言等を実施する。

５　官民の連絡・連携体制の確立・強化

各重要インフラ分野においては、セキュリティ情報（セキュリティ改善に必要な情報）及び警報情報（サイバー攻撃の発生情報等の警戒や緊急対処に必要な情報）の共有、予防・対処等を連携して行うための官民における体制の確立・強化を図ることが必要である。

特に、いわゆるサイバーテロの脅威が増大していくなか、サイバーテロ対策に関する官民の連絡・連携体制を確立することは急務であることから、各分野における状況を踏まえ、本計画決定後一年以内を目標として、次の体制を構築することが必要である。

(1) 各民間重要インフラ分野等における連絡・連携体制

各民間重要インフラ分野等において、次の役割を担うサイバーテロ対策に係る事業者間の連絡・連携体制を、既存の連絡体制を活用しつつ構築する。

○　各分野に共通するセキュリティ情報及び警報情報の収集､連絡及び共有

○　サイバー攻撃が発生した場合又はそのおそれがある場合における連絡体制

○　政府及び関係機関との一元化された連絡の実施　等

(2) 他分野の重要インフラ事業者との連絡・連携体制

ネットワークを介して、他分野の重要インフラ事業者と情報システムを相互接続している場合には、サイバーテロ対策に関し互いの連絡・連携体制を必要に応じ構築する。

(3) 政府における連絡・連携体制の確立

政府においては、内閣官房を中心とし、次の役割を担う連絡・連携体制を構築する。

○　セキュリティ情報及び警報情報の収集、連絡及び共有

○　サイバー攻撃が発生した場合又はそのおそれがある場合における情報集約

○　政府部内、関係機関及び各民間重要インフラ事業者等との連絡　等

(4) 情報の取扱い

情報の収集及び共有に際しては、民間重要インフラ事業者等から適切に情報が提供されるよう、あらかじめ、情報の取扱いが厳正な管理の下で行われることなどを関係者間で合意するなど、関係者間における信頼関係の構築に努める必要がある。

(5) 民間重要インフラ事業者等に対する協力

政府は、セキュリティ情報及び警報情報の提供等、民間重要インフラ事業者等に対する協力に努める。

6　官民連携によるサイバー攻撃の検知と緊急対処

各重要インフラ分野においてサイバー攻撃を受けた場合又はそのおそれがある場合の対応策を定めるとともに、官民全体で対処能力の強化を行う必要がある。

(1) サイバー攻撃の検知

○　政府及び民間重要インフラ事業者等は、基幹をなす重要な情報システムに障害が発生した場合に、それがサイバー攻撃か否かを判断することが困難であることを前提に、想定される事態を十分に踏まえ、障害の内容、発生箇所、障害の範囲等、事案に対する適切な対処を行えるようあらかじめ手順を定める。

○　政府及び民間重要インフラ事業者等は、政府関係機関、情報セキュリティ関係団体、情報システムのベンダー等からセキュリティ情報及び警報情報の収集を行う。

(2) 緊急時対応計画の策定

○　各民間重要インフラ分野等においては、サイバー攻撃が発生した場合又はそのおそれがある場合の対策及び緊急時対応計画の策定について、5で定める連絡体制を活用しつつ検討を行う。

（緊急時対応計画に想定される事項）

・連絡、被害拡大防止、証拠保全、復旧（応急）、再発防止等

また、この計画においては、迅速な対応を可能とするよう、サイバー攻撃の検知後の時間経過に応じた手順をとりまとめることが重要である。

○　緊急時における対処には、高度な判断を必要とする場合があることから、責任と権限を有する適切な者が速やかな判断を行うことができるよう、緊急時対応計画等の手続に定める。

(3)　緊急時における情報の連絡手順

○　サイバー攻撃を受けた場合又はそのおそれを示す情報を得た場合の緊急時における情報の連絡手順を次のとおりとする。

ア　サイバー攻撃に関する情報の連絡

①　サイバー攻撃を受け、又はそのおそれを示す情報を得た省庁又は民間重要インフラ事業者等は、速やかな対処を講ずるとともに、分野内の他の民間重要インフラ事業者等、所管官庁、関係機関等の定められた連絡担当者に当該情報を連絡する。

②　情報の連絡を受けた省庁は、当該情報を内閣官房に連絡するとともに、攻撃を受けた民間重要インフラ事業者等に対する指示、助言等を行う。

③　内閣官房は、関係省庁等との連携を図り、情報収集等を行う。

イ　警報情報の連絡

①　内閣官房は、攻撃又はそのおそれを示す情報の内容から必要な場合には、各省庁に警報情報を連絡する。

②　各省庁は、内閣官房から警報情報を受けた場合には、所管する民間重要インフラ事業者等に速やかに当該情報を連絡する。

○　政府及び民間重要インフラ事業者等は、必要に応じサイバーテロ対策の訓練を実施する。

○　政府及び民間重要インフラ事業者等は、攻撃による被害によって国民生活や社会経済活動に影響を生じた場合には、関係者に対し、迅速かつ適切な情報の提供を行うよう努める。

(4) 政府における緊急対処体制の強化

○　サイバー攻撃が発生した場合又はそのおそれがある場合において、内閣官房は、各省庁等との協力・連携を図り、情報集約を行うとともに、政府として対処が必要な場合には、対処方針について各省庁との調整を行う。

○　内閣官房は、このための所要の連携体制を各省庁等の協力を得て構築するとともに、各省庁は、サイバーテロ対策に係る情報収集体制及び対処体制を強化する。

7　情報セキュリティ基盤の構築

サイバーテロ対策を進めていくため、人材の育成、研究開発、法制度の整備等の情報セキュリティ基盤の構築を推進することが必要である。

また、重要インフラをサイバー攻撃から防護するためには、重要インフラのみならず、一般の情報システムを運用・利用する者が、いわゆるサイバーテロの脅威を認識し、セキュリティ対策の重要性についての理解を深め、必要なセキュリティ対策を講じることが重要であることから、広く一般に対して、普及啓発を行うことが必要である。

(1) 人材育成の推進

○　政府及び民間重要インフラ事業者等は、職員等に対する教育・訓練、セキュリティ技術の専門家の継続的な養成等に努める。

(2) 研究開発の推進

○　政府及び民間重要インフラ事業者等は、いわゆるサイバーテロの脅威に対して強固な基盤を構築するために必要な技術開発、脅威の分析、対策・技術に関する調査研究等を、官民の協力・連携を図りながら推進する。

(3) 普及啓発の推進

○　政府は、不正アクセス行為の発生状況等の公表、不正アクセス行為からの防御に関する啓発及び国内外のいわゆるサイバーテロの脅威に関する知識の普及等を行う。

○　政府は、民間重要インフラ事業者等の職員等を対象とした情報セキュリティに関する研修等を推進する。

(4) 法制度の整備

○　政府は、国際的動向との調和及び情報通信ネットワークにおける安全確保の観点から、関連する刑事基本法制など法制度の整備を検討する。

８　国際連携

サイバー攻撃は、国境を越えて行われる可能性があることから、このような攻撃に適切に対処するため、国際的な連携を推進することが必要である。

○　政府及び民間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。

○　政府は、ＯＥＣＤやＧ８におけるサイバーテロ対策に関連する国際的な取組に対する協力を推進する。

○　政府は、諸外国の関係機関との間の情報交換や共同訓練等、国際的な連携強化を推進する。

９　行動計画の見直し

この行動計画は、官民の連絡・連携体制の確立を中心としてとりまとめたサイバーテロ対策の初めてのものであり、政府は、この行動計画の進捗を踏まえ、定期的及び必要に応じ、この行動計画の見直しを実施する。

平成１３年１０月２日
情報セキュリティ専門調査会

サイバーテロ対策に係る官民の連絡・連携体制について
(概要)

１　経　緯

「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年１２月１５日、情報セキュリティ対策推進会議決定）において、１年以内にサイバーテロ対策に係る官民の連絡・連携体制の構築することとしており、これに基づき、体制・運用に関する基本的な考え方を策定したもの。

２　概　要

（１）連絡体制

サイバー攻撃発生時等における政府と事業者との間の連絡は、重要インフラ分野ごとに、既存の連絡体制等の活用により、各重要インフラ分野を所管する省庁を通じて行う。

（２）情報連絡の対象となる事案

情報連絡の対象には、重要システムに対するサイバー攻撃による被害のほか、サイバー攻撃の検知、攻撃の予告等が含まれる。

（３）情報連絡の手段

事案発生時の連絡手段は、事前に２ルート以上を明確化する。

（４）政府及び事業者における対応

事案発生時には、事業者、所管省庁及び内閣官房のそれぞれにおいて、情報共有、緊急時対処等の適切な措置を講ずる。

（５）情報の取扱い

政府及び各事業者は、連絡された情報の取り扱いには十分留意することとする。

また、情報共有する範囲及び事項については、必要最小限とする。

３　今後の予定

本連絡・連携体制の運用に関し必要な具体的事項を、年内を目途に政府及び各重要インフラで協議の上定める。

平成１３年１０月２日
情報セキュリティ専門調査会

サイバーテロ対策に係る官民の連絡・連携体制について

「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年１２月１５日、情報セキュリティ対策推進会議。以下「特別行動計画」という。）を踏まえ、以下の考え方に基づき、サイバーテロ対策に係る官民の連絡・連携体制の構築を進めることとする。

１　対象となる重要な情報システム等

特別行動計画に定める「重要インフラの基幹をなす重要な情報システム」（以下「重要システム」という。）及び特別行動計画の対象となる事業者については、いわゆるサイバーテロによって国民生活や社会経済活動に与える重大な影響を考慮し、重要インフラ分野ごとに定めることとする（別紙１参照）。

なお、具体的に対象となる重要システムの詳細については、別紙１に掲げる重要システムの例を踏まえ、各事業者において定めることとする。

２　サイバー攻撃発生時等における連絡体制等

（１）　連絡体制

サイバー攻撃発生時等における政府と事業者との間の連絡は、重要インフラ分野ごとに、既存の事故、障害時等における連絡体制等の活用又は業界団体等におけるサイバーテロに関する連絡窓口の構築等により、各重要インフラ分野を所管する省庁（以下「所管省庁」という。）を通じて行うものとする（別紙２参照）。

また、各重要インフラにサービスを提供する情報サービス産業事業者については、個々の重要インフラ事業者を通じて行うものとする。

なお、各重要インフラ分野内における情報共有及び検討体制については、事業者間で共通する課題がある場合など、情報共有等が有効な場合に業界団体を中心として行うこととする。

（２） 情報連絡の対象となる事案

情報連絡の対象となる事案は、①重要システムに重大な障害が発生した時、②重要システムに対するサイバー攻撃を検知した時又は攻撃の予告があった時及び③重要システムに対するサイバー攻撃による被害を検知した時とする（別紙３参照）。

この場合において、

①の「重大な障害」とは、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして事業者が連絡を要すると判断したものを含むものとする。

②の「重要システムに対するサイバー攻撃を検知した時」については、「被害は発生していないが、そのおそれが高い攻撃を検知した場合」に限ることとする（別紙４参照）。

なお、①、②及び③のいずれにも該当しない場合においても、サイバー攻撃の未然防止、被害の拡大防止等に資すると考えられる事案について情報の提供を行うこと並びに①、②及び③に該当するかどうか不明な場合について所管省庁又は内閣官房に対して相談を行うことを妨げるものではない。

（３）情報連絡の内容

情報連絡の内容については、①事案発生時における利用可能な連絡手段、連絡担当者等の連絡を確保するための情報を必須とするほかは、②その時点で判明している情報を随時連絡することとする。この際、当該情報が全容が解明するまえの断片的又は不確定なものであっても差し支えないものとする。

なお、以下に掲げる事項について、判明した範囲で随時連絡するように努めるものとする。

ア　対象システム

・ハードウエア、ソフトウエア（システムの名称、バージョン、パッチの適用状況等）

イ　事案概要

・事案の分類（①重要システムにおける障害、②サイバー攻撃の検知、③予告、④サイバー攻撃による被害）

・攻撃の種別（不正アクセス、サービス不能攻撃、情報漏えい・改ざん、システ

ム破壊等）
・原因（セキュリティホール、侵入経路、不正プログラム等）
・インフラサービスへの影響等被害の程度
ウ　対処状況
・対策の概要（システムの停止・復旧、セキュリティ改善策等）
・その他の連絡先（警察・セキュリティ関係機関等）
エ　他の事業者に対する攻撃の可能性
オ　その他

（４） 連絡手段

事案発生時の連絡手段については、事業者と所管省庁の間及び政府部内において事前に明確化することとする。この際、電話、FAX、e-mail 等２以上の連絡手段を明示するものとする。

なお、e-mail 等インターネットを用いて機密に関する情報の連絡を行う場合には、リスク分析や費用対効果などに応じて暗号等の導入の必要性について検討することとする。

3　政府及び事業者における対応

（１） 所管省庁における対応

所管省庁は、各事業者から２により連絡を受理した場合（重要システムに重大な障害が発生した時に行われる連絡で、当該障害が設定ミス・操作ミスや業務の便宜のために行った行為等サイバー攻撃を原因とするものでないことが明らかである場合を除く。）には、速やかに内閣官房へ連絡するとともに、関係所管分野の事業者等からの情報収集、現状把握等に努めるものとする。

また、内閣官房からの指示、情報提供等を踏まえて、各事業者に情報の提供、対処方法、体制等についての助言、指導等を行うものとする。

（２） 内閣官房における対応

内閣官房は、各所管省庁からの情報、関係機関等からの関連情報等を収集・分析

するとともに、事案の重要度に応じ、各所管省庁を通じた情報提供や助言、指導、対策支援等、関係省庁と連携した各種の緊急対処措置を講ずることとする。

（３） 事業者における対応

各事業者は、特別行動計画に定める緊急時対応計画に想定される事項（連絡、被害拡大防止、証拠保全、復旧（応急）、再発防止等）について、速やかに適切な措置を執るものとする。

４　情報の取扱い

（１）情報共有に関する考え方

ア　共有の原則

本連絡・連携体制において連絡された情報の取扱いについては、法令等に定めがある場合又は連絡を行う事業者の了承がある場合を除き、連絡を受ける所管官庁及び内閣官房以外に提供しないものとする。

ただし、官民連携してサイバーテロ対策を進めるため、次の事項に該当する場合には他の事業者及び関係機関等との情報共有を行うものとする。

① セキュリティホール等を発見した場合であって、他の事業者に同じ問題が生じるおそれがあると認められる場合

② サイバー攻撃の発生又は攻撃の予告がある場合であって、他の事業者の重要システムが危険にさらされていると認められる場合

また、政府及び各事業者は、共有された情報につき、その保秘に十分留意しなければならないものとする。

イ　共有の範囲及び内容

情報共有（提供）は、注意喚起等として各事業者の対策に資するものとして行うものであることから、情報を共有（提供）するその範囲及び事項は次のとおりとする。

① 情報を共有（提供）する範囲は、当該情報に直接関係する事業者等（業界固有のシステムの場合には当該業界内、他の分野に関係する場合は関係するすべての分野）とする

② 共有（提供）する情報の内容は、情報連絡を行った事業者が不利益を被らないよう、具体的な対策を実施するために必要な事項に限るものとする。また、企業名や分野名を提供する必要がある場合については、原則として同意を得た上で行うものとする。

（２）情報の公開に関する考え方

事業者から提供された情報は、原則として行政機関の保有する情報の公開に関する法律（平成１１年法律第４２号。以下「情報公開法」という。）第５条第２号ロに規定する情報（任意提供情報）として取り扱うものとする。ただし、これは本官民連絡・連携体制の枠組みの中で情報を提供（共有）することを妨げるものではない。（なお、当該情報が情報公開法第５条第２号本文但し書きに規定する情報に該当する場合には、公開されることがある。）

５　その他

（１）本連絡・連携体制の運用に関し必要な具体的事項については、年内を目途に政府及び各重要インフラで協議の上定めることとする。

（２）本連絡・連携体制の効率的かつ効果的な運用を図るため、政府及び各事業者は訓練を実施するものとする。また、内閣官房は、平素より関係省庁及び関係機関の協力を得て、広くセキュリティ情報（セキュリティ改善に必要な情報）の収集、分析を行うとともに、これらを本連絡・連携体制の運用により得られた成果と併せて各重要インフラに随時提供するよう努めるものとする。

（３）本申し合わせは、警報情報（サイバー攻撃の発生情報等の警戒や緊急対処に必要な情報）の共有に関する事項を中心として定めるものであるが、２(1)に定める連絡の体制は、セキュリティ情報についても、政府と重要インフラ分野各事業者間の情報共有、連絡、相談の枠組み等として活用し得るものとする。

（４）本申し合わせについては、運用の状況、情勢の変化等を踏まえ、随時見直しを行うものとする。

各重要インフラ分野において対象となる重要システム等 （別紙1）

分野（注1）	サイバー攻撃による情報システムの障害、不正な処理などの脅威・危険性	対象となる事業者（注2）	対象となる重要システム例（注3）
情報通信	・電気通信サービスの停止 ・電気通信業務に関する通信の秘密の漏洩 ・番組制作・放送運行、緊急災害対応など情報発信機能の障害	・第一種及び特別第二種等の主要な電気通信事業者 ・放送事業者（NHK、衛星放送、ケーブルテレビを含む。）	・電気通信事業用設備 ・通信管理業務システム ・放送業務用システム群
情報サービス	・情報システム共通のセキュリティホールによる広範な障害等	・重要インフラにおける重要システムを管理・運営する情報サービス産業事業者	
金　融	・預金の払い出し、振込等資金移動、融資業務などの業務の停止等	・銀行、信用金庫、信用組合、農業協同組合等	・勘定系システム ・資金証券系システム ・国際系システム ・対外接続系システム （オープンネットワークを利用したサービスを含む。）
航　空	・運航の遅延、欠航 ・航空機の安全運航に対する支障等	・定期航空協会加盟事業者 ・国土交通省（航空管制・気象）	・運航システム ・予約・搭乗システム ・整備システム ・貨物システム ・航空管制システム ・気象情報システム
鉄　道	・列車運行の遅延、運休 ・列車の安全安定輸送に対する支障等	・ＪＲ及び大手民間鉄道事業者等の主要な鉄道事業者	・列車運行管理システム ・電力管理システム ・座席予約システム
電　力	・電力供給の停止 ・電力プラントの安全運用に対する支障等	・一般電気事業者、日本原子力発電（株）及び電源開発（株）	・制御システム ・運転監視システム
ガ　ス	・ガスの供給の停止 ・ガスプラントの安全運用に対する支障等	・主要なガス事業者	・プラント制御システム ・遠隔監視・制御システム
政府・行政サービス	・政府、行政サービスに対する支障 ・個人情報の漏洩、盗聴、改ざん	・各省庁 ・地方公共団体	・各省庁及び地方公共団体の情報システム（電子政府への対応）

注１）　対象とする重要インフラ分野については、医療分野等を含めることなど引き続き検討することとしている。

注２）　ここに掲げている対象事業者は、重点的に対策を実施すべき事業者であり、各分野のこれら以外の事業者についても同様の対策を講ずることが望ましい。
また、主要な事業者としているものは、Ｙ２Ｋ対策等における対象事業者に準じるものである。

注３）　対象となる重要システムの詳細については、脅威・危険性や例を踏まえ、事業者において定める。

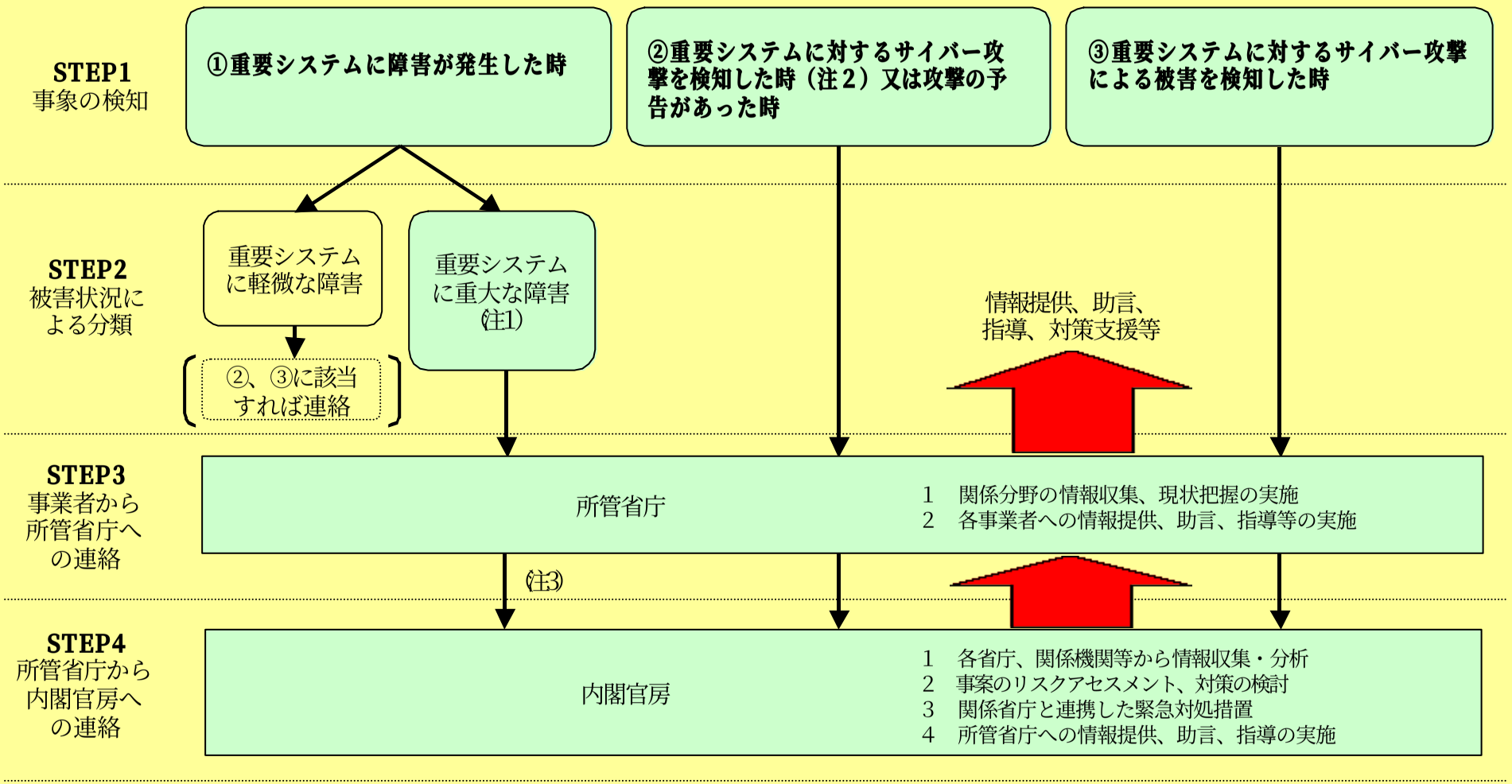
(別紙2)

サイバー攻撃発生時等における連絡体制等

分野	既存の連絡体制	サイバー攻撃発生時等における 緊急時の連絡体制	情報セキュリティ関連情報の共有 各分野におけるセキュリティ対策等の検討体制
情報通信	（1）事業者→政府 ・電気通信事業法に基づく、業務の停止等の総務大臣への報告 ・災害対策基本法に基づく、災害応急対策における電気通信設備の被害状況等報告 ・放送中止事故、重要無線通信妨害等の総務省への連絡 （2）政府→事業者、事業者間 ・ウイルス発生等緊急情報を業界内及び総務省との間で通報・共有	（1）事業者→政府 ・既存の連絡体制を活用して実施 （2）政府→事業者 ・既存の連絡体制を活用して実施	・ウイルス発生等の情報共有体制を活用して実施
情報サービス		・各重要インフラにサービスを直接提供する事業者は、個々のインフラ事業者を通じて対応。 ・ベンダー等の事業者は、情報の提供・公開を通じて取組を支援。	
金　融	（1）事業者→政府 ・銀行法に基づく、預金払い戻し、為替等の決済機能に遅延・停止等の内閣総理大臣（金融庁）への報告 （2）政府→事業者、事業者間 ・特になし	(1)事業者→政府 ・既存の連絡体制を活用して実施 （2）政府→事業者 ・業界団体を通じて実施	・全銀協、ＦＩＳＣ等の業界団体を通じて実施
航　空	（1）事業者→政府 ・航空法に基づく、航空機の事故等に関する国土交通大臣への報告 （2）政府→事業者、事業者間 ・サイバーテロに関する連絡窓口を設置 ・航空保安体制の不具合に関する情報を関係機関で共有（空港単位）	（1）事業者→政府 ・事故時は事故処理規程に基づき実施 ・遅延、犯行予告は連絡窓口を通じて実施 （2）政府→事業者 ・連絡窓口を通じて事業者へ直接連絡	
鉄　道	（1）事業者→政府、政府→事業者 ・鉄道事故等報告規則に基づく、鉄道運転事故等に関する国土交通大臣への報告 ・サイバーテロに関する連絡体制を整備 (2) 事業者間 ・特になし	（1）事業者→政府、政府→事業者 ・事故時は既存の事故報告体制により実施。 ・事故に至らないサイバーテロに関しては、サイバーテロの連絡体制により実施。	
電　力	（1）事業者→政府 ・防災業務計画、電気関係報告規則に基づく、発電所事故等に関する経済産業大臣への連絡 （2）政府→事業者、事業者間 ・特になし	（1）事業者→政府 ・既存の連絡体制を活用して実施 （2）政府→事業者 ・業界団体を通じて実施	・業界団体を通じて実施
ガ　ス	（1）事業者→政府 ・ガス事業法施行規則に基づく、一定規模のガス供給支障等の経済産業大臣への報告 （2）政府→事業者、事業者間 ・災害によりガス供給支障が発生した場合等における、ガス協会「救援措置要綱」に基づく業界内連絡	（1）事業者→政府 ・既存の連絡体制を活用して実施 （2）政府→事業者 ・業界団体を通じて実施	・業界内の委員会等を通じて実施
政府 地方公共団体	（1）各省庁→内閣官房 ・「政府機関の情報システムに関する緊急時の連絡等について」に基づく連絡 （2）内閣官房→各省庁 ・「政府機関の情報システムに関する緊急時の連絡等について」に基づく情報提供	・政府部内連絡体制で実施	・政府部内連絡体制で実施

（別紙3）

情報連絡の対象となる事案



（注1）　「重大な障害」とは、法令等で報告が義務づけられている事故、障害、業務遅延等のほか、特異重大なものとして事業者が連絡を要すると判断したものを含む。

（注2）　「サイバー攻撃を検知した時」については、「被害は発生していないが、そのおそれが高い攻撃を検知した場合」に限ることとする（別紙4参照）。

（注３）　重大な障害が設定ミス・操作ミスや業務の便宜のために行った行為等サイバー攻撃を原因とするものでないことが明らかである場合は、連絡を要しない。

（別紙4）

「サイバー攻撃を検知した時」について

連絡の要否	例
連絡の対象となるもの （被害は発生していないが、そのおそれが高い攻撃を検知した場合）	**○重要システムへの影響が相当程度予想される攻撃を検知した場合（注）** ・外部から侵入できないはずの内部ネットワークにある重要システムに不正アクセスの試みが行われた場合 ・重要システム内で重要システムに障害を与えるおそれのあるコンピュータウイルスが発見された場合 ・攻撃パターンや過去の事例等の状況から、重要システムに重大な影響を及ぼすおそれがあると思われる攻撃が行われた場合 **○重要システムに対して特定のグループ等から明らかな意図・目的を持って攻撃が行われたことを検知した場合**
連絡の対象とならないもの	**○重要システムに対する攻撃の予備行為として行われたおそれのあるものを検知した場合** ・外部から重要システムに対するアクセスを可能とするバックドアを発見した場合 ・外部から重要システムに対するアクセスを可能とする不審なモデム等を発見した場合 ・重要システムに対する攻撃を行うプログラム（ツール）が仕掛けられているのを発見した場合 ・メンテナンス用の接続口から第三者のアクセスを可能とする不正な設定を発見した場合
	○重要システムに対する攻撃に必要な情報を窃取する行為を検知した場合 ・重要システムに関するシステム構成や設定情報などが盗まれた場合 ・重要システムに関するパスワードや暗号鍵等が盗まれた場合 ・重要システムに直接接続されたゲートウエイにスニファが仕掛けられた場合
	○重要システムに関係しないシステムへの攻撃を検知した場合 ・インターネットに接続されたファイアウォールに対する単なるポートスキャンを検知した場合 ・専ら宣伝広告用のホームページサーバに対する不正アクセス・改ざんを検知した場合 ・専ら事務用の電子メールサーバへのコンピュータウイルスの到来を検知した場合

注）　事例・情勢等の適切な判断が行えるよう、「重要システムに障害を与えるおそれのあるコンピュータウイルス」や「攻撃パターンや過去の事例等の状況から、重要システムに重大な影響を及ぼすおそれのあると思われる攻撃」については、政府から情報提供を行い、これらの情報を参考に連絡の対象となるか否かを事業者において判断する。

平成14年3月28日

重要インフラのサイバーテロ対策に係る特別行動計画」のフォローアップ等について（概要）

1. 趣　旨

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年12月15日　情報セキュリティ対策推進会議。以下「特別行動計画」という。）策定後の諸情勢の変化を踏まえ、各重要インフラ分野における特別行動計画への取組状況等についてのフォローアップを進めるとともに、それらの取組強化に向けた検討を行う。

2. 概　要

Ⅰ　官民における取組みの進捗状況等

特別行動計画に示された官民において取り組むべき各事項に関し、

・重要インフラ所管の各省庁による主な施策の実施状況等

・民間重要インフラ事業者等やその事業者団体等における取組状況のうち当該所管省庁が現時点で把握しているもの

について取りまとめ。

Ⅱ　特別行動計画における取組みの強化に向けた検討課題

⑴ 民間重要インフラ事業者等の取組状況については、これを把握するための体制・枠組みや取組みの実効性の確保方策につき、必ずしもその受皿や方策が整っていないのが現状。

⑵ 事業者等の情報セキュリティ確保に関する取組みを一層促進するべく、以下の検討課題に関し、今後の方向性や具体策について重要インフラ分野ごとに検討を推進。

① 重要インフラの情報システムに関する現状把握・検証

② 民間重要インフラ事業者等におけるサイバーテロ対策状況の把握

③ 民間重要インフラ事業者等におけるサイバーテロ対策の実効性の確保

④ その他政府における検討事項　（サイバーテロ対策の一層の促進方策）

⑶ なお医療分野については、今後のⅡ化の進展状況等を見極めつつ、重要インフラ分野の1つに位置付けることについて、検討を推進。

3. 今後の進め方

「e-Japan 重点計画」の目標・期限である2005年を目途に各課題への対応を推進

⑴ 検討課題①～③について

・WG において全体的な方向性等を検討

・分野ごとの方向性や具体的方策、実施（実現）時期等につき各分野内にて検討

・検討結果につきWG へ報告・取りまとめ、情報セキュリティ対策推進会議等において了承

・各分野ごとに具体的方策の実施

⑵ 検討課題④について

・①～③の検討状況を踏まえ、具体的方策につき検討

「重要インフラのサイバーテロ対策に係る特別行動計画」のフォローアップ等について

<趣旨>

「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年12月15日 情報セキュリティ対策推進会議。以下「特別行動計画」という。）策定後の諸情勢の変化を踏まえ、各重要インフラ分野における特別行動計画への取組状況等についてのフォローアップを進めるとともに、それらの取組強化に向けた検討を行うこととする。

Ⅰ 官民における取組みの進捗状況等

特別行動計画に示された官民において取り組むべき各事項について、主な施策の実施状況は以下のとおりである。

1 被害の予防（セキュリティ水準の向上）

(1) 民間重要インフラ分野等のセキュリティ水準の向上

- 金融庁では、金融検査マニュアルに基づく定期的な検査において、情報セキュリティポリシーの策定等についてチェックを実施。
- 総務省では、平成13年3月に「地方公共団体における情報セキュリティポリシーに関するガイドライン」を策定し、地方公共団体に提示したほか、「情報通信ネットワーク安全・信頼性基準」（総務省告示）により情報通信分野における「情報セキュリティポリシーの策定のための指針」を規定。
- 電力分野においては、事業者団体にて「電力におけるサイバーテロ対策危機管理ガイドライン」を作成。
- その他、各所管省庁は事業者団体等における現状調査や行政上の指導・監督等を通じて、民間重要インフラ事業者等のセキュリティ水準向上について指導。

(2) 電子政府の構築に向けたセキュリティ水準の向上

- 内閣官房の専門調査チームは、各省庁における情報セキュリティポリシーの策定状況のほか、サイバーテロ対策一般に関する問題点等について、昨年5月にヒアリング及び意見交換を実施。
- 昨年10月、「電子政府の情報セキュリティ確保のためのアクションプラン」（平成13年10月10日 情報セキュリティ対策推進会議。以下「アクションプラン」という。）を策定。これに基づき、内閣官房は 2002 年夏を目途に各省庁の情報セキュリティポリシーについて再評価等を行うほか、これを受けて各省庁ではポリシーの見直しを実施予定。
- 総務省及び経済産業省では、電子政府のための暗号技術評価を実施。

2 官民の連絡・連携体制の確立・強化

昨年10月にサイバーテロ対策に関する官民の連絡・連携体制の運用に関する基本的な考え方として、「サイバーテロ対策に係る官民の連絡・連携体制について」（平成13年10月2日 情報セキュリティ専門調査会。以下「官民の連絡・連携体制」という。）を策定。

また、昨年末までに当該連絡･連携体制の運用に関し、連絡経路等の必要な具体的事項を関係者間において取りまとめ。

3　官民連携によるサイバー攻撃の検知と緊急対処

(1)サイバー攻撃の検知

・「官民の連絡･連携体制」において、情報共有の対象となる重要システム、サイバー攻撃等のほか、攻撃検知時の手順について規定。

・内閣官房は昨年中、関係省庁等から事案発生に関する情報収集を行うとともに、注意喚起等として２８件の情報を各省庁へ提供。

(2)緊急時対応計画の策定

・総務省では、「情報通信ネットワーク安全･信頼性基準」（総務省告示）により、各電気通信事業者が緊急時対応計画等を整備するにあたっての「危機管理計画策定のための指針」を規定。

・電力分野においては、各電力事業者における緊急時対応計画等に反映させるための「電力におけるサイバーテロ対策危機管理ガイドライン」を事業者団体にて作成。

(3) 緊急時における情報の連絡手順

・「官民の連絡･連携体制」に関して、連絡経路等の必要な具体的事項につき、内閣官房や重要インフラの所管省庁等関係者間において取りまとめ。

(4) 政府における緊急対処体制の強化

・アクションプランに基づき、内閣官房では電子政府等に対するサイバー攻撃などの事案が発生した場合又はそのおそれがある場合に、政府として取るべき措置や再発防止措置の実施に資するための緊急対応支援チームを平成１４年度に編成。

・警察庁では、サイバーテロの未然防止、発生時における被害の拡大防止ための監視･緊急対処体制として、機動的技術部隊（サイバーフォース）を創設。

・防衛庁では、自衛隊等の保有する情報システムに対する常時監視、システム監査、緊急事態対処等の機能を備えた体制の整備を推進。

・情報通信分野においては、総務省、電気通信事業者及び事業者団体との間にて、サイバー攻撃への対応も含めた情報セキュリティ対策のための連携体制を構築。

・電力、ガス分野においては、経済産業省、民間重要インフラ事業者等及びそれらの事業者団体との間にて、サイバー攻撃への官民合同の対応体制を整備･強化。

・航空、鉄道分野においては、各事業者と国土交通省との間で、緊急事案発生時における初動対応体制を構築。

4　情報セキュリティ基盤の構築

(1) 人材育成の推進

・警察庁及び防衛庁では、米国等の政府機関や情報セキュリティ関連団体などへ職員を派遣し、研修、情報交換等を実施。

・総務省では、昨年７月、電気通信事業法に基づく電気通信主任技術者試験に情報セキュリティに関する科目を追加。また、事業者団体が情報セキュリティ分野の人材育成を推進するための協議会を設立し、同年９月から資格認定講習を開始。

・経済産業省では、平成１３年度に情報セキュリティアドミニストレータ試験を創設したほか、

情報セキュリティ評価技術者及び情報セキュリティ設計技術者の育成事業を推進。

(2) 研究開発の推進

・ 防衛庁では、サイバー攻撃に対する対処手法の実証的研究及びコンピュータ・システム等の安全性確立のための運用ガイドラインに関する調査研究を推進。

・ 金融分野においては、財団法人金融情報システムセンターにてセキュリティポリシー、コンティンジェンシープランの策定・運用に関する研究会を平成13年に実施。

・ 総務省では、第3世代移動通信システムに関する情報セキュリティ上の対策等について研究会を開催し、昨年12月に報告書を取りまとめたほか、平成13年度からネットワークセキュリティ基盤技術の推進のための研究開発等を通信・放送機構において実施。

・ 経済産業省では、コンピュータウイルス、不正アクセス等により情報処理システムが受ける脅威の状況やそれに対する防御措置に関する技術開発を推進。

(3) 普及啓発の推進

・ 内閣官房では、平成13年度中に「情報提供システム」を整備し、情報セキュリティに関する知識の普及・啓発を目的とするインターネットWebページを立ち上げ。

・ 国家公安委員会、総務省及び経済産業省では、民間部門におけるセキュリティ意識を向上させるため、不正アクセス行為の発生状況等を公表。

・ 金融分野においては、財団法人金融情報システムセンターにより事業者を対象とした情報セキュリティに関する各種セミナーを開催。

・ 経済産業省では、コンピュータ・ウイルス等に対する被害と対策についてのセミナーを全国各地で実施。

(4) 法制度の整備

・ 法務省では、いわゆるサイバーテロを含めた各種のハイテク犯罪に対する罰則の整備、情報通信ネットワークに関する捜査手続について、適切な処罰を確保するための法整備を2005年までに行うため、諸外国の法制度調査及びハイテク犯罪に関する国内事例調査を実施。

5 国際連携

・ 内閣官房では、本年3月、関係省庁の参加を得て、米国の情報セキュリティ対策担当者との日米政府間討議を開催。

・ 警察庁、総務省、法務省、外務省及び経済産業省では、G8リヨングループハイテク犯罪サブグループに参加し、ハイテク犯罪からの重要インフラの防護について各国と情報交換。

・ 防衛庁では、平成12年度から米国防総省等との政策協議などを行うため、「IT フォーラム」等を開催。

・ 総務省では、国際電気通信連合電気通信標準化部門(ITU-T)における情報セキュリティに関する標準化活動を推進。

・ 経済産業省では、昨年9月に情報セキュリティに関するOECDワークショップを開催したほか、本年3月にはアジア太平洋地域における各国の CSIRT(Computer Security Incident Response Team)を集めた国際会議を開催。

・ 内閣官房、警察庁、総務省、外務省及び経済産業省等は、OECDにおける1992年情報システム・セキュリティ・ガイドラインの見直し作業に参加。

Ⅱ　特別行動計画における取組みの強化に向けた検討課題

民間重要インフラ事業者等の取組みの状況については、これを把握するための体制、枠組みが存しない分野もあるほか、これら取組みの実効性の確保方策について、必ずしもその受皿や方策が整っていない現状が存する。

これを踏まえ、民間重要インフラ事業者等の情報セキュリティ確保に関する取組みを一層促進するべく、以下の課題に関し、今後の方向性や具体策について重要インフラ分野ごとに検討を進めることとする。

なお医療分野については、今後のIT化の進展状況等を見極めつつ、重要インフラ分野の1つに位置付けることについて、検討を進めることとする。

【検討課題】

①重要インフラの情報システムに関する現状把握･検証

重要インフラの基幹をなす情報システムに関し、それぞれのシステム構成やそれらの外部ネットワークへの接続の有無･運用状況のほか、サイバー攻撃を受けた場合に想定される事態などにつき、各分野内での把握･検証等の方策を検討する。

②民間重要インフラ事業者等におけるサイバーテロ対策状況の把握

各事業者等の取組状況の把握等を行うための手法･体制等を検討する。

③民間重要インフラ事業者等におけるサイバーテロ対策の実効性の確保

各事業者等における取組みを一層効果的なものとするため、以下に例示する観点等から、官民における実効性の確保方策を検討する。

[例]

- 既存の検査体制等の活用など指導･監督の在り方
- 情報セキュリティに関する専門家等も参加した官民合同の検討体制等の在り方
- 事業者団体等における実効性担保のための体制の在り方

④その他政府における検討事項

政府においては、①から③の検討状況を踏まえ、以下に例示する観点等から、サイバーテロ対策の一層の促進方策について、その必要性を含め検討する。

[例]

- 重要インフラにおける情報セキュリティ確保のための技術基準等の在り方
- 各分野内における新たな体制構築へのサポートなど、事業者等に対する支援施策の在り方
- 重要インフラにおける取組みの実効性の確保に必要な制度的枠組みの在り方

平成14年11月28日
情報セキュリティ対策推進会議

「重要インフラのサイバーテロ対策に係る特別行動計画」に基づく取組みの推進について

1. 経緯

「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年12月15日 情報セキュリティ対策推進会議。以下「特別行動計画」という。）策定後の諸情勢の変化を踏まえ、本年3月、各重要インフラ分野における取組状況等についてのフォローアップを実施するとともに、それらの取組強化に向けた検討課題が提示された〔参考資料〕ところ、これら課題に関する各分野ごとの検討状況とそれを踏まえた具体的方策等について取りまとめたものである。

2. 各分野における検討結果の概要

本年3月の情報セキュリティ対策推進会議開催後、4回のWGを実施し、また各分野ごとに、検討課題として挙げられていた

① 重要インフラの情報システムに関する現状把握・検証
② 民間重要インフラ事業者等におけるサイバーテロ対策状況の把握
③ 民間重要インフラ事業者等におけるサイバーテロ対策の実効性の確保

について検討を行った結果は、概要以下のとおりである。

(1) 事業者の対象範囲の絞込み

分野によっては、社会的影響度、シェア、事業者数等を勘案しつつ重点的に取組みを行うべき事業者の範囲について当面絞り込むこととし、取組みの確実性、実効性を挙げることとした。

(2) 重要インフラにおける情報システムの現状評価

各重要インフラ分野における重要な情報システムに関する現状については、所管省庁等からは以下のとおり報告されており、それぞれ重要システムについて基本的に外部ネットワークとの接続を避けるなど、その安全確保に向けた努力がなされているところではあるが、今後の情報システムの更なる発展・拡充の可能性等も踏まえ、継続的な現状把握・検証の取組み等が重要である。

情報通信分野

○ 基幹的なネットワークインフラを供する電気通信事業者については、電気通信事業法に基づく技術基準を遵守しているほか、「情報通信ネットワーク安全・信頼性基

準」に従ってネットワーク機器の監視機能等を整備している。また、全国的にサービス展開するインターネット接続サービス事業者についても、認証システムやファイアウォールの導入とセキュリティ監査等によるその検証を実施。

○ 放送事業者については、NHK及び民放キー局5社の放送システム及び放送中継システムは外部ネットワークとは接続されていない。また社内業務用システムについては、ファイアウォールの設置やウイルス対策等によりセキュリティを確保。

金融分野

○ 民間各金融機関はインターネットバンキングなどのサービス提供にあたって、認証システムやファイアウォールの導入等によりセキュリティを確保。

○ 全銀システム及び東京証券取引所のシステムについては、それぞれ会員金融機関等との間で専用回線、独自のプロトコルを使用して接続されており、外部ネットワークとは直接接続されていない。また東京証券取引所のシステムでは電文の暗号化等を実施。

航空分野

○ 航空運送事業者の運航系システムについては、外部ネットワークとは直接接続されていない。またインターネット予約システムについては、ファイアウォールの設置等によりセキュリティを確保。

鉄道分野

○ 列車運行管理システム及び電力管理システム等の制御系システムは基本的に外部ネットワークとは接続されていないことに加え、鉄道用地内に設置され、他のシステムから独立して列車の衝突･脱線の防止機能を果たす保安装置により列車運行の安全性が確保されている。また事務処理系システムについては、ファイアウォールの設置やセキュリティホール対策の実施等によりセキュリティを確保。

電力分野

○ 各事業者の電力供給のための制御系ネットワークについては、基本的に他のシステムから独立していることに加え、外部ネットワークとは接続されていない。またオフィス業務のための事務系ネットワークは多重のファイアウォールの設置等によりセキュリティを確保。

ガス分野

○ ガス導管網は全国規模でネットワーク化されているものではなく、ガスの製造や供給に係る制御系システムもそれぞれの事業者ごとに他のシステムから独立したものとなっており、自営専用回線の利用等外部ネットワークへの直接接続を回避することによりセキュリティを確保。

地方公共団体関係

○ 各種の情報システムの安定的な稼動･運用が可能となるよう、システム上の措置の確認、検証等を含め、各地方公共団体におけるセキュリティ監査等の対策の実

施を促進するとともに、各団体等間を結ぶ広域ネットワークである総合行政ネットワーク等については、その情報システムに関する技術的な基準等を定め、各団体等に徹底。

(3) 検討課題への具体的方策等

① 重要インフラの情報システムに関する現状把握・検証

事業者等及び所管省庁においては、上記(2)の現状を踏まえつつ、引き続き、外部ネットワークとの接続の有無等情報セキュリティに関するチェックリスト等の策定とその活用、事業者団体加盟各社に対する調査、サイバーテロを原因とする事故・障害発生に関する一定のシナリオの作成とこれを前提とした定性的なリスク分析等の実施などを通じて、重要な情報システムの現状の把握、検証を推進していくこととしている。

② 民間重要インフラ事業者等におけるサイバーテロ対策状況の把握

事業者等及び所管省庁においては、既存の報告・連絡等の枠組みを活用するとともに、業界団体内における協議会等の活用、チェックリスト等の策定とその活用、事業者等に対する調査やヒアリングの継続的な実施等を通じて、情報セキュリティポリシーの策定状況、実施・運用状況の把握、確認等を行うなど、各事業者の取組みの把握を推進していくこととしている。

③ 民間重要インフラ事業者等におけるサイバーテロ対策の実効性の確保

事業者等及び所管省庁においては、従来の検査・監査等における情報セキュリティ対策の観点の導入、緊急時対応計画の策定、第三者等によるセキュリティ監査の実施、事業者間の情報共有化の枠組み構築、官民の合同検討会の開催、研修等の実施による人材の育成・啓発活動などを通じて、各事業者等における取組みを一層効果的なものとするための方策を引き続き推進していくこととしている。

3. 今後の予定等

今回取りまとめられた検討課題①～③に関する具体的方策等について、今後、各分野ごとに所要の体制等を構築しつつその確実な実施を図るとともに、将来的な技術基準の在り方等検討課題④(その他政府における検討事項)についての検討を引き続き進めることとし、適宜、情報セキュリティ専門調査会及び情報セキュリティ対策推進会議を開催し、各省庁からその取組状況・結果等について報告を行うこととする。