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。