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。

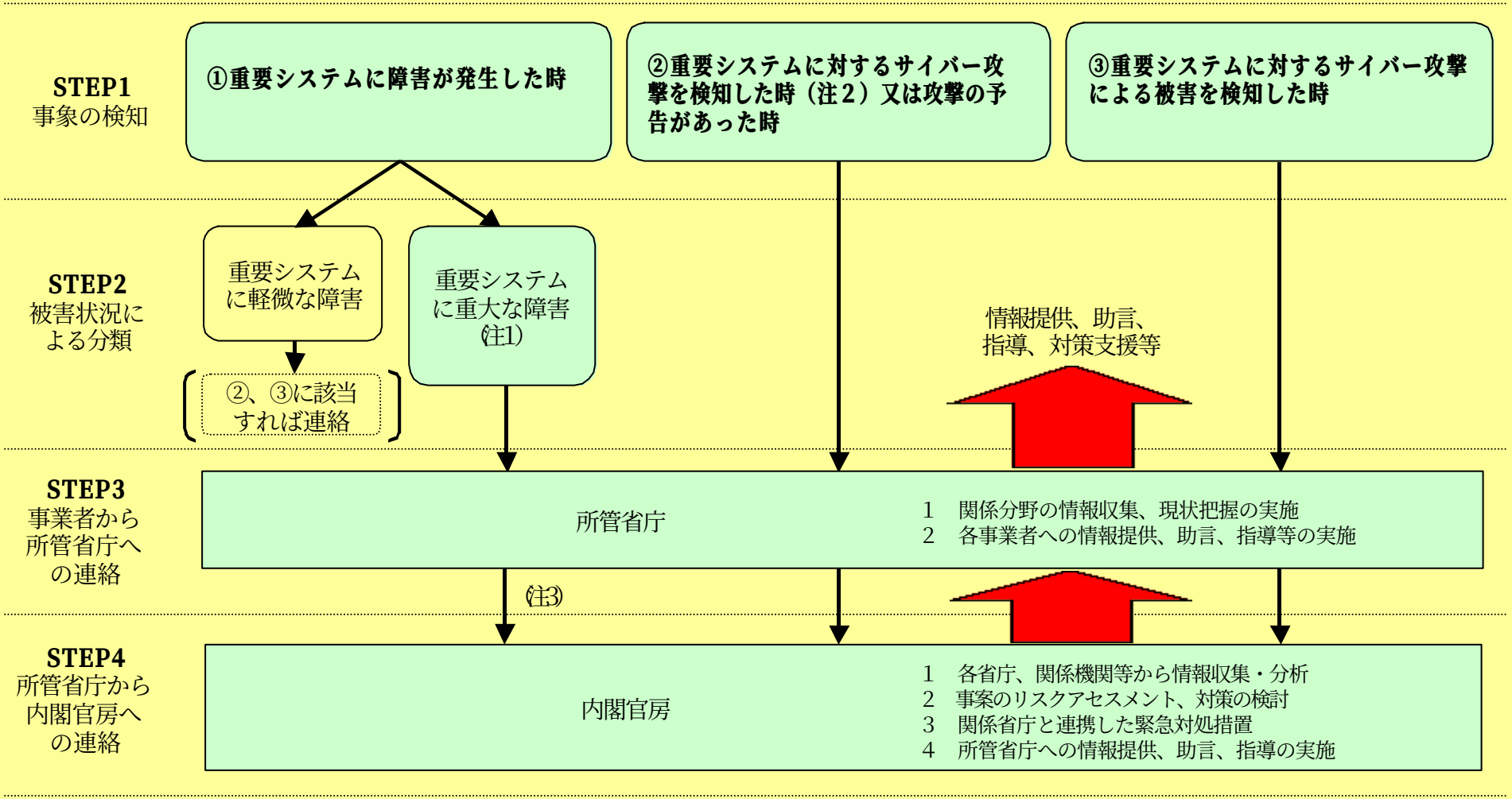
（別紙2）

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	⑴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 ⑵ 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。