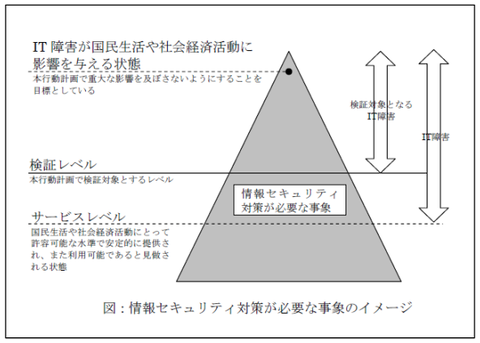
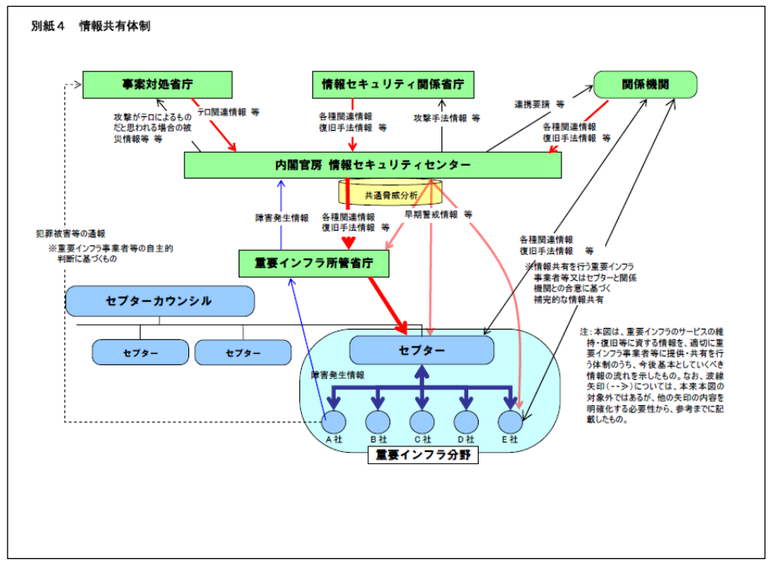
サイバーセキュリティ戦略（案）の重要インフラ関連記載と第2 次重要インフラ行動計画・次期行動計画との関係と検討を要する点

資料2

次期戦略　関連記載	第2次行動計画　関連記載	次期行動計画　見直しの方向性	備考（検討を要する点等その他補足、留意点）
	Ⅰ　総論	＜専門委員会＞（30回）　資料3「第2次行動計画の見直しの方向性について」 1　経緯と現状認識 （3）今後の見直しの方向性 　重要インフラ行動計画は、2005年の策定以来、第1次、第2次と重要インフラ分野における情報セキュリティ対策を着実に進展させてきており、 ①　安全基準等の整備及び浸透 ②　情報共有体制の強化 ③　共通脅威分析 ④　分野横断的演習 ⑤　環境変化への対応 という、第2次行動計画の各施策は有効に機能しているものと考えられる。したがって、次期行動計画において、これらの施策群により構成される基本的な骨格は引き続き維持することが適当である。 　その上で、重要インフラ分野における情報セキュリティ対策をさらに発展させるべき詳細項目を検討し、必要な補強を行うことが適当である。	
	1　目標 （1）　行動計画の目標 （略） （2）　基本的な方向性 （略） （3）　理想とする将来像 （略）		
わが国において、現在、重要インフラとは位置づけられていないが、現行10分野と同等にその機能障害が国民生活及び社会経済活動に多大な影響を及ぼす分野について、今後、当該インフラにおける情報システムの位置付けを踏まえ、重要インフラの範囲及びそれぞれの性格に応じた対応の在り方等について、検討を行う。	2　定義と対象範囲 （1）　重要インフラと重要インフラ事業者等 「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、低下又は利用不可能な状態に陥った場合に、わ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である。 第2次行動計画では、「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。）」、「医療」、「水道」及び「物流」の 10 分野の重要インフラを防護対象とする。 「重要インフラ事業者等」とは上記 10 分野に属する事業を営む者のうち、別紙1の「対象となる事業者」に指定された者及びこれらの者から構成される団体である。 （2）　重要インフラサービスと重要システム 「重要インフラサービス」とは重要インフラ事業者等が提供するサービス及びそのサービスを利用するために必要な一連の手続きのうち、国民生活や社会経済活動に与える影響の度合いを考慮して、特に防護すべきとして重要インフラ分野毎に定めるものである。第2次行動計画で対象とした分野毎の重要インフラサービスを別紙2に示す。なお、分野によっては対象としたサービスの代表例のみを示している場合がある。 「重要システム」とは、重要インフラサービスを提供するために必要な情報システムのうち、重要インフラサービスに与える影響の度合いを考慮して、重要インフラ事業者毎に定めるものである。第2次行動計画で対象となる重要システムの例を別紙1に示す。 なお、別紙1及び別紙2は、情報セキュリティ対策の対象を当該重要インフラサービス及び当該重要システムに限定することを意図してまとめたものではない。ここに挙げていない重要インフラサービス及び重要システムについても、国民生活や社会経済活動に影響を与えるおそれがあるものに対しては、第2次行動計画に基づき情報セキュリティ対策に取り組む必要がある。 （3）　サービスレベルと検証レベル 第2次行動計画においては、重要インフラサービスが国民生活や社会経済活動にとって許容可能な水準で安定的に提供され、また利用可能であると見做される状態を「サービスレベル」とする。サービスレベルは別紙2の「検証レベル」を参考として各重要インフラ事業者毎に定めるものとする。 各重要インフラ事業者等はサービスレベルを維持することを目標として情報セキュリティ対策に取り組むことが望ましい。また、サービスレベルは各重要インフラ事業者等の事業継続計画の目標と乖離しないものとすることが望ましい。 重要インフラサービスが一定水準を下回った場合にこれを検証対象とすることとし、この水準を「検証レベル」とする。各分野毎の検証レベルを別紙2に示す。 （4）　IT障害 「IT 障害」とは、重要インフラサービスにおいて発生する障害（サービスレベルを維持できない状態等）のうち、IT の機能不全が引き起こすものである。 ここで IT の機能不全とは、重要システムをはじめとした重要インフラサービスの提供に必要な情報システムが設計時の期待通りの機能を発揮しない状態を指す。 第2次行動計画に基づく取組みの評価・検証に際しては、IT 障害のうち検証レベルを逸脱するものの発生状況を検証することとしている。 （5）　脅威 第2次行動計画においては、IT 障害を引き起こしうる要因を「脅威」と呼ぶ。脅威には多種多様なものがあり、またその態様は分野毎の特性によって様々であるが、第2次行動計画では別紙3のとおり4種に類型化している。 重要インフラ事業者等は自らの重要インフラサービスの安定的供給と事業継続性を確保すると共に、	＜専門委員会＞（31回）　資料6－1「重要インフラの定義及び対象について」 2　次期行動計画における「重要インフラ」を検討するに当たっての検討項目 　別添に、わが国及び欧米各国における「重要インフラ」の定義及び対象分野の一覧表を示す。この表からは、 ・他国においては、「重要インフラ」の定義は、システム的（仮想的）なものだけでなく、物理的なものも包含。また、その定義は、法律や国家戦略等比較的高いレベルで行われている。 ・我が国において、情報セキュリティ対策上防護すべきとしている対象分野は、他国でも同様に防護の対象とされている。 ものと見ることができる。 ・情報セキュリティ上防護すべき対象を検討する際、1（1）～（3）で述べた重要インフラそのもの、重要インフラ事業者、重要インフラサービス及び重要システムの定義については、引き続き同様の定義を行うことが適当であると考えられるが、 ①　この定義により規定される重要インフラ分野 ②　この定義により規定される関係主体 について、その加除修正を検討する必要がある。 （1）重要インフラ分野 行動計画における防護の対象が、「その分野におけるサービス等の中で特に防護すべき対象として定めたものによるサービスを提供するために必要な情報システム」と規定されていることから、情報システムを有する分野が対象であることは明確である。（米国において重要インフラと規定されている食糧・農業や原子力（廃棄物）は、情報セキュリティ上の観点では防護の対象にはならない。） また、情報セキュリティ対策の策定主体が明確であることや情報共有を適切に行う主体が存在していることも、実際の施策を推進することが可能な否かを判断する重要な観点である。これらの観点を適切に満たしていない分野を重要インフラとした場合、その情報セキュリティ対策を適切に講じ、情報共有を行う主体がないため、実効性に乏しいものとなるおそれがある。 さらに、情報セキュリティ対策の適切な浸透や障害事例等の適切な報告を期待する上で、第2次行動計画が前提としている「各分野における業務を規律する法令」（「業法」）や所管省庁への障害報告スキームの有無も、施策推進の可否を判断する重要な観点である。情報セキュリティ上の障害事例を報告し、その情報の全部または一部を情報共有する上で、業法等に基づく報告に基づく所管省庁から適切な情報提供は適切かつ効率的な枠組みと考えられる。 現状の10分野については、引き続き重要インフラ分野として規定することが適当であると考えられるが、10分野以外の分野を追加の可否を検討する際には、当該分野が「重要」であるか否かの観点とともに、上述の実効性の観点をも勘案しながら個別の事情に照らして検討する必要がある。 （2）関係主体 1（4）で述べたとおり、関係主体として、NISC、所管省庁、情報セキュリティ関係省庁、事	「重要インフラの定義及び対象について」 ・サイバー空間関連事業者（ITベンダー、セキュリティベンダー）の関係主体への追加については、すでに検討を開始。 戦略『当該インフラの情報システムの位置付けを踏まえ』及び　専門委員会における論点（防護対象となり得る分野の判断基準）である以下の3点 ①　（重要システムである）情報システムを有する分野 ②　情報セキュリティ対策の策定主体が明確であり、また情報共有を適切に行う主体が存在する分野 ③　情報セキュリティ対策の適切な浸透や障害事例等の適切な報告を期待する上で、業法、所管省庁への障害報告スキームが存在する分野 を勘案し、 －既存の重要インフラと同等の影響を持ち得、かつ①を満足する分野であり、 （ア）②及び③を満足するものは、重要インフラへの追加を検討。 （イ）②または③を満足しないものは、安全基準に相当する基準の策定状況、情報共有体制等について定期的に調査・分析を行い、（ア）の状態に至った時点で、重要インフラへの追加を検討。 具体的な候補として検討する分野は、専門委員会における議論及びNISC実施

	自らの IT 障害が他の重要インフラ事業者等の重要インフラサービスの安定的供給と事業継続性の確保への脅威になる可能性にも留意することが必要である。 　また、脅威は大きく社会全体で対策が望まれる脅威と、個別の重要インフラ事業者等が中心となって対策する脅威がある。特に前者については分野横断的な連携を積極的に図る事が求められる。 （6）　情報セキュリティ対策 　第2次行動計画においては「情報セキュリティ対策」とは、重要インフラの IT 障害が国民生活や社会経済活動に影響を与えないようにするための幅広い取組みを指す。情報セキュリティ対策には IT 障害への対策に加えて、IT の機能不全への対策を含む。情報セキュリティ対策の対象となる事象のイメージは下図のとおりである。 　情報セキュリティ対策には大別して、IT 障害の発生を可能な限り未然に防止する予防的対策と、IT 障害発生時の迅速な復旧等の確保によりその影響を可能な限り最小化する事後的対策がある。予防的対策の観点からは、IT 障害を引き起こす原因となる IT の機能不全そのものを取り除く対策を講じる手法と、IT の機能不全を一定の範囲で受容した上でそのサービスへの影響を制御する対策を講じる手法のふたつがある。これらのいずれの手法に従って対策を講じるべきかは状況によって異なる。 　この際、IT の機能不全を受容することとしていたとしても、当該機能不全の重要インフラサービスへの影響の制御に失敗し、結果的に IT 障害が発生することとなれば、事後の改善策としては当該機能不全を取り除く対策が必要となる場合がありえる。そのため第2次行動計画では、IT 障害に対する情報セキュリティ対策と同様に、IT の機能不全に対する情報セキュリティ対策も重視している。 　第2次行動計画では重要インフラ事業者等による情報セキュリティ対策を単に「対策」と、また政府による情報セキュリティ対策を「施策」と呼ぶ。 （7）　関係主体 　第2次行動計画に基づいて情報セキュリティ対策に取り組むことを想定している「関係主体」は、内閣官房、重要インフラ所管省庁（金融庁、総務省、厚生労働省、経済産業省、国土交通省）、情報セキュリティ関係省庁（警察庁、総務省、経済産業省、防衛省）、事案対処省庁（警察庁、消防庁、海上保安庁、防衛省）、関係機関（警察庁サイバーフォース、NICT、AIST、IPA、Telecom-ISAC Japan、JPCERT/CC等）、重要インフラ事業者等、セプター、セプターカウンシル等をさす。 　各関係主体が各々の役割に応じて情報セキュリティ対策に取り組むに当たっては、当該関係主体が単独で取り組むほか、IT ベンダーとの連携によって取り組むことが適切な場合がある。また、情報の共有に当たっては、必要に応じて内閣府及び関係省庁間等の既存の情報共有体制と連携を行う。	案対処省庁、関係機関、セプター及びセプターカウンシルが記載されており、その情報共有体制についても第2次行動計画　別紙4で整理されている。 　一方、重要システムの構築・運用に実際に携わっている IT ベンダーや重要システムの防護のために多数使用されている情報セキュリティ対策を実装するソフトウェア等の製作・運用に携わっているセキュリティ・ベンダーについては、今年度の共通脅威分析の結果からも明らかなように、重要システムの運用や防護に大きな役割を果たしていると考えられるにも関わらず、その位置付けや期待される機能は明確ではないままに留まっている。 　したがって、IT ベンダーやセキュリティ・ベンダーについては、その位置付けや期待される機能を重要インフラ分野における情報共有体制の中で明らかにすることが適当ではないか。  図：情報セキュリティ対策が必要な事象のイメージ	の調査により選定することとする。 また、関係主体として、防災関係省庁（例：内閣府（防災担当））の扱いも検討する必要がある。
	3　第1次行動計画の成果 （1）　安全基準等の整備及び浸透 　（略） （2）　情報共有体制の強化 　（略） （3）　相互依存性解析 　（略） （4）　分野横断的演習 　（略）		
	4　第2次行動計画期間における取組みの要点 5　行動計画の改定 　（略）		
	Ⅱ　計画期間内に取り組む情報セキュリティ対策		
重要インフラについて、重要インフラ事業者等におけるリスク評価手法に基づく情報セキュリティ対策の重点化を図るため、各分野における直近の安全基準等の策定・変更状況及びリスク分析を通じて、分野横断的に講じることが望ましいリスクを洗い出し、安全基準等を策定するための指針の中に反映するプロセスを確立する。	1　安全基準等の整備及び浸透 　第2次行動計画期間においては、事業継続の観点からの具体的内容の補充を含め、指針の位置づけや記載内容の具体性のレベルの見直しを行う。 　また、重要インフラ事業者等の PDCA サイクルとの整合性を踏まえた安全基準等の整備の推進などの底上げに資する取組みのみならず、個別の先進的な対策を伸ばしその浸透を図る観点からの取組みも推進する。 （1）　指針の継続的改善 　社会動向の変化等に対応し、また新たな知見を適時反映していくために、指針の分析・検証を1年毎、及び必要に応じて実施し、その結果を公表することとする。なお、指針の改定に関する検討は原則として3年に1度実施するものとする。ただし、必要に応じて追加的に検討を実施し、必要があると認められた場合には指針の改定を行うこととする。 　なお、指針の改定に関する検討にあたっては、東日本大震災において重要インフラ分野に生じた複合的な障害における教訓を踏まえ、事業継続計画において情報セキュリティ上のリスクを十分想定する必要が生じている状況や、事業継続計画に関する国際規格化の進展状況等を踏まえつつ、分野横断的な観点からも実効的であるかを検証できるように指針の内容を充実させるものとする。 　各重要インフラ事業者等の自主的な取組みに資する項目を充実させるために、指針に記載される事項を「要検討事項」と「参考事項」に分類し、対策項目の具体化の例示を行う事により、引き続き記載事項の充実を図ることとする。 　「要検討事項」とは対策の底上げの観点から全分野共通で特段の理由のない限り対策することが望まれる事項であり、安全基準等に規定する必要性を各分野が検討するべき事項とする。また「参考事項」とは進んだ対策として盛り込む事が望ましい事項とし、各分野が任意で参考とする事項とする。 　要検討事項及び参考事項は、現行指針の項目に加え、行動計画に基づく各重要インフラ分野及び重要インフラ事業者等の取組みから得られる知見・教訓等を候補として必要に応じて充実させていくこととする。 （2）　安全基準等の継続的改善 　各分野においては、対策の経験から得られた知見を安全基準等に反映するため、安全基準等の継続的な改善に取り組むこととする。なお、安全基準等の検証に際しては、指針や毎年実施される指針の	＜専門委員会における議論なし＞	基本的には現行動計画における （1）指針の継続的改善 （2）安全基準等の継続的改善 （3）安全基準等の浸透 の3施策は維持。 　これに加え、浸透状況調査における調査項目に、攻撃・脆弱性等に関するリスク要因についての安全基準の策定状況、対策の有無等に関するものを追加し、その調査結果を必要に応じて、対策の提示及び必要に応じた指針・対策編への反映を行うプロセスについては、施策としてどのように扱うかを含めて、今後検討する必要がある。 　なお、行動計画策定に当たり、「安全基準等の整備・浸透」は、他施策のいずれからもアウトカムの展開先になることから、各施策の成果展開をどのタイミングで行うこととするのか（浸透状況調査

	分析・検証の結果を踏まえた検討を行うこととするが、その際標的型攻撃、制御システムへの攻撃への対策等最近の環境変化に対応しているか否かの分析・検証も行い、必要に応じて安全基準等の改定を行うこととする。 情報セキュリティ対策に関する知見の共有を促進するために、従来検証対象となっている安全基準等の他に、情報セキュリティ対策に関する基準又は参考文書類を、可能な範囲で共用できるよう改めて広く安全基準等として整理することとする。 安全基準等に基づく対策状況については、関係性を有する主体間で互いに把握しておくことが重要である。そのため、情報セキュリティ監査又はそれに相当するものの実施や、情報セキュリティ報告書又はそれに相当するものの作成等の自主的な取組みを一層推奨し、分野や重要インフラ事業者等における情報セキュリティ対策の対外的な説明に努める。 (3)　安全基準等の浸透 各重要インフラ分野は、安全基準等の浸透に向けて、安全基準等にて定められた対策の推進に加えて、対策を実装するための環境整備にも努める。事業者自らが定める「内規」を含めた安全基準等の浸透を確実なものとするために、「安全基準等の浸透状況等に関する調査」を引き続き定期的に実施することとする。調査項目・調査主体等については、適宜見直しを行うこととする。		の項目への反映、指針・対策編の改定のきっかけ等）についても、評価・検証方法を決定する際に考慮する必要あり。 （参考）ここでいう「リスク分析」は、各分野に顕在化しているリスクについての分析（第２次行動計画の「IT依存度調査に基づくリスクの洗い出し」と近い）であり、情報通信技術そのものまたはその利活用の進展により、その全部または一部が重要インフラに入る可能性があるものの動向調査及びリスク分析とは対象が異なることに注意が必要。）
障害情報及び攻撃・脅威・脆弱性等に関する情報については、重要インフラ事業者等及びCEPTOARとの間における情報共有を推進するとともに、重要インフラ事業者等による事業所管省庁等への迅速な報告、自主的判断に基づく事案対処省庁への通報及び関係機関との情報共有についても、個人情報・秘密情報に配慮した上で促進する。	２ 情報共有体制の強化 第2次行動計画期間においては、関係主体間で共有する情報についての整理を行い、情報提供、情報連絡等に必要な環境整備等を推進するとともに、各セプター、セプターカウンシルの自主的な活動の充実強化を推進する。情報共有体制の全体像は、別紙4に示すとおりとする。 （1）　共有すべき情報の整理 「IT 障害に関する情報」とは、情報セキュリティ対策に資する IT 障害、IT の機能不全等に関する幅広い情報である。 IT 障害に関する情報には、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つの側面が含まれる。 対象とする脅威、様々な社会動向の変化等を踏まえた上で、情報セキュリティ関連情報の流通に関する既存の枠組みに配慮しつつ、共有すべき情報について整理を行うこととする。この際、IT 障害に関する情報の3つの側面を踏まえた上で、関係主体の活動や保有する情報、法制度等による制約を整理するとともに、関係主体の保有する情報毎に、重要インフラ事業者等にとって有用な情報の共有のありかた（即応性の観点等を含めたタイミング、様式、方法など）を検討することとする。 また、情報提供、情報連絡の実践等を通じて、分野横断的な観点において、必要な情報と提供可能な情報の整理を継続的に見直すこととする。 （2）　情報提供、情報連絡の充実 ア 情報提供、情報連絡の基本 重要インフラ事業者等のサービスの維持・復旧がより容易になるようにするためには、官民の各主体が協力することが重要であるとの観点から、第1次行動計画の下において、「実施細目」やセプターの整備を中心とした情報共有体制の構築を進めてきており、情報の共有が開始されている。当該情報共有体制の枠組みが出来上がったところであることを考え合わせ、第2次行動計画における情報提供、情報連絡は、これまでの情報共有体制を踏襲しつつ、情報提供の内容を充実したものとすることを基本とし、別添に示すところにより情報提供、情報連絡を行うものとする。 イ 情報提供、情報連絡の充実 内閣官房、重要インフラ所管省庁、セプター、重要インフラ事業者等において各々が整備している情報共有に係るルールの整合を図ることとする。また、内閣官房から重要インフラ事業者等への情報提供について、必要に応じて情報共有に求められる機能等の検討を行い各主体間で共有を目指すこととする。 また、事例や経験の共有を強化するために、第1次行動計画で実施してきた相互依存性解析で得られた知見や、今後行われる共通脅威分析で得られる知見に基づいた波及先に関する分析を行うとともに、関係機関等の有する分析機能の活用を検討することとする。 （3）　セプターの強化 セプターに具備すべき要件として、第1次行動計画で定められた以下の 2 点の要件については引き続きこれを維持し、内閣官房から提供する情報の共有を図ることとする。 ①内閣官房が提供する情報の取扱いに関する取決め、機密保持及び外部への情報提供に関し、構成員間で合意されたルールが存在すること。 ②緊急時に各構成員及び外部との連絡が可能な窓口（POC）が設定されていること。 なお、今後は、セプターにおける情報の収集、把握・分析、内部での共有、他セプターやセプターカウンシルへの発信などといった機能の展開が期待される。 また、各セプターは分野内の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の設置や、IT障害に至らない事例や現行情報連絡の対象とならない IT 障害の事例についての情報共有の機能、セプター間やセプターカウンシル等との情報共有等に必要な機能の充実について、重要インフラ事業者等の自主的な取組みの中で図られることが望まれる。 （4）　セプターカウンシル セプターカウンシルは、各セプターにより構成される共助・互恵の活動の取組みを促進するために創設されたものであり、相互理解及びベストプラクティス等の具体的な事例共有等の分野横断的な情報共有が行われることが望まれる。 また、政府機関等とは独立した活動が可能な位置づけにあることから、情報共有の改善等のための検討などに関し、その特徴を活かして積極的な活動に取り組むことが期待される。特に重要インフラ事業者等と政府機関等の協力関係を今後一層深めていくためには、両者の間の状況認識等の共有を進めていくことが重要であることから、平時から重要インフラ事業者等と政府機関等の意見交換を密接に行うことが望まれる。また、事業者間においても相互に役立つ情報の共有を進めるなどの取組みがなさ	＜専門委員会＞（31回） 資料6－2「情報共有体制の強化について」 1 実施細目による情報共有について （2） 検討の方向性について 実施細目による情報共有体制においては、関係主体間の情報共有は情報セキュリティの根幹を成すものとして機能している。この体制は通常の運用だけでなく、分野横断的演習や他の訓練、演習においても利用、検証されており、重要インフラの情報セキュリティ対策において今後とも重要かつ必要不可欠なものとなっている。従ってその体制を定めた実施細目は引き続き継続することが適当と考えられる。 一方、サイバー攻撃の状況や各分野における IT 利用の深化等の現状認識を踏まえると、IT障害そのものに加えIT障害につながる恐れのある脅威についての情報連絡、情報共有について一層の充実が望まれる。例えば、情報が漏洩したり、標的メールを受信、感染した場合など、他分野への波及防止、事例の集積による傾向の分析等有益な情報が得られることが期待される。最近のサイバー攻撃等の状況を踏まえ共有すべき新たな情報が存在するとの認識の下、情報連絡様式やIT障害の分類等について、見直しを検討してはどうか。 2 セプターカウンシルにおける情報共有体制について （2） 検討の方向性について セプターカウンシルにおける活動は、事業者間の自立的な情報共有体制として着実に充実している。2012年の第2次行動計画改定では、平時から重要インフラ事業者等と政府機関等の意見交換を密接に行うことや、事業者間において相互に役立つ情報の共有の進め方などの取組を進めることが指摘されており、このような視点で共有すべき情報を意識し整理しつつ、引き続きこうした取組を推進、充実することが適当と考えられる。 別紙４　情報共有体制 	第２次行動計画における情報共有体制の全体像「別紙４」における関係機関、情報セキュリティ関係省庁及び事案対処省庁との関係（提供、共有される情報の内容、各機関の位置付け）の見直し・再整理が必要。 （新たに検討を要する団体、組織等） ① 防災関係省庁（例：内閣府（防災担当）） ② 新たな所管省庁（⑤関連） ③ ｻｲﾊﾞｰ空間関連事業者（ｼｽﾃﾑﾍﾞﾝﾀﾞｰ） ④ ｻｲﾊﾞｰ空間関連事業者（ｾｷｭﾘﾃｨﾍﾞﾝﾀﾞｰ） ⑤ 現在、重要インフラと位置付けられていない分野 － 現在重要インフラと位置付けられていないが影響が既存の10分野と同等程度あるもの － 情報通信技術そのものまたはその利活用の進展により、その全部または一部が重要インフラに入る可能性があるもの なお、情報セキュリティ関係機関については、専門委員会において、その位置付けの再整理を求められていることから、その検討が必要。 また、連携する（可能性のある）情報共有体制（特に標的型・不審メール関係）として新たにJ－CSIP、GSOCがあるが、その扱いの情報共有体制における記載ぶりについて検討が必要。

	れることが望まれる。なお、この取組みを進めるに当たって、セプターカウンシルの事務局を努める内閣官房においては、2（1）カ②に示す環境整備を行うことが重要である。		
わが国において、現在、重要インフラとは位置づけられていないが、現行10分野と同等にその機能障害が国民生活及び社会経済活動に多大な影響を及ぼす分野について、今後、当該インフラにおける情報システムの位置付けを踏まえ、重要インフラの範囲及びそれぞれの性格に応じた対応の在り方等について、検討を行う。 （再掲）	3 共通脅威分析 第2次行動計画期間においては、第1次行動計画で実施してきた、ある重要インフラ分野に IT 障害が生じた場合に他のどの重要インフラ分野に影響が波及するか、という相互依存性解析を継続するとともに、重要インフラ分野共通に起こりうる脅威が何であるかを把握するための検討を行う。 このため、従来行ってきた「静的相互依存性解析」や「動的相互依存性解析」の結果を踏まえ、研究機関等との連携を深めつつ、内閣官房、重要インフラ所管省庁、重要インフラ事業者等が協力して活動を進める。 なお、本分析の結果は、引き続き次のような重要インフラのサービス維持・復旧への活用が期待される。 ①より実効性の高い事業継続計画策定に必要な基礎資料の提供 ②大規模災害発生時における復旧優先順位の決定のための基礎資料の提供 ③IT 障害の被害拡大防止のための、重要インフラ分野間の連携対処のための基盤提供 （1） 相互依存性解析の継続 重要インフラの情報セキュリティ確保にあたっては、重要インフラ分野間での相互依存性の認識と、問題に柔軟に対応できる対策が必要である。すなわち、相互依存性解析は、潜在的なリスク・チェーンの顕現化と、事故・障害要因の連鎖的伝搬に対してのマネジメント（回避・コントロール・想定など）に必要である。このことから、第2次行動計画でも相互依存性解析に継続的に取り組むものとする。 （2） 共通脅威分析の検討 各重要インフラ分野における IT 利用が一層の進展を見せる中、我が国全体としての重要インフラの情報セキュリティを向上させていくためには、分野横断的な状況の把握、分析が従来以上に不可欠である。このため、それぞれの重要インフラ分野に共通に起こりうる脅威が何であるかを把握するための分析を行うこととする。この分析と相互依存性解析を合せて共通脅威分析と呼ぶこととし、重要インフラ分野共通の IT に関する技術、システム、環境等、広い範囲を対象とする分析を実施する。	＜専門委員会における議論なし＞	これまでの議論では、 ① 安全基準等の整備及び浸透 ② 情報共有体制の強化 ③ 障害対応体制の強化（仮称：横断的演習の拡充、他省庁演習との連携等を含む） に加え、何らかのリスク調査・分析が必要ではないかと事務局では考えているところ。 （相互依存性解析、現在重要インフラと位置付けられていないが影響が既存の10分野と同等程度あるものの実情、これから情報通信技術そのものまたはその利活用の進展により、その全部または一部が重要インフラに入る可能性があるものの動向調査及びリスク分析等）
また、重要インフラ事業者、サイバー空間関連事業者及び関係CSIRTの間で、民間組織間の信頼関係を前提に、サイバー演習等の実施を促進しサイバー攻撃に対する連携対応能力の強化を図る。	4 分野横断的演習 第2次行動計画期間においては、第 1 次行動計画において得られた分野横断的な演習手法に関する知見を踏まえ、各重要インフラ所管省庁、各重要インフラ事業者等、各重要インフラ分野のセプター等の協力を得て、重要インフラ分野横断的な演習を実施する。また、演習シナリオの検討、演習の実施を通じて、「分野横断的な脅威に対する共通認識の醸成」や「他分野の対応状況把握による自分野の対応力強化」、「官民の情報共有をより効果的に運用するための方策」などが得られることにより、分野横断的な重要インフラ防護対策の向上を目指す。なお、重要インフラ分野における現行の法制度や重要インフラ事業者等の経営上の仕組みに関することも含め、演習で得られた課題は、改善に向けた取組みに活用できるよう、分野間及び関係主体間で共有する。 （1） 分野横断的演習の実施 IT 障害を引き起こす要因である脅威に関する最新動向を把握し、それら脅威に対する分野横断的な重要インフラ防護対策の向上を目指し、具体的な IT 障害発生を想定した演習シナリオの検討とそれに基づく分野横断的な演習を継続的に実施することにより、課題の抽出及び演習実施のための知見の整備を行う。なお、演習の実施に当たっては、重要インフラ事業者等を中心に、演習シナリオ及び適切な演習手法の検討を行うものとする。情報セキュリティ対策に関する課題や官民の情報共有に関する課題など、演習で抽出された課題については、情報共有体制の見直しなどに活用することで、分野横断的な重要インフラ防護対策の向上を図る。 また、重要インフラ事業者等の早期復旧手順や事業継続計画などについても、各分野が任意に検討できる事項として演習シナリオに組み込むことにより、分野間及び関係主体間の自律的かつ効果的な協調・連携を図る観点からの取組みの推進が期待される。 演習は、IT 障害への対応を検証する上で有効な手法であることから、シナリオ作成、運営手法等、分野横断的演習を通じて得られた演習実施のための知見について、各重要インフラ事業者等が自分野の取組みに活用できるよう整理し、提供することにより、重要インフラ事業者等の情報セキュリティ対策の向上に資することが期待される。	＜専門委員会＞（31回） 資料6－3「分野横断的演習について」 3．方向性（案） （1） 総論 重要インフラ分野の情報システムへの依存度が更に進み、かつ、情報システムをめぐる様々な脅威が一段と顕在化する等の状況下においては、緊急事態（各分野に影響を及ぼし得るサービス障害、広い分野にわたる情報セキュリティインシデント等）の発生に備えて模擬的な演習を実施し、重要インフラ相互間の情報共有や連絡・連携の仕組みを検証し、必要に応じて見直しを図ることが益々重要になってきている。 このため、新規行動計画期間中においては、引き続き、官民の重要インフラ関係者の協力を得て、分野横断的演習を実施することが適当であると考えられる。 演習の目標については、現行の3目標を継承しつつ、2．の課題を踏まえた以下の方向性各論（（2）～（5））が演習の実施効果に及ぼす影響等を勘案し、必要に応じて内容の補強・深度化を図るものとする。 特に、内閣官房においては、分野横断的演習の実施を通じて演習に関する知見を蓄積するのみならず、他省庁主催の演習との連携などを通じて重要インフラ関係の演習・訓練の全容を把握し、その上で今後の演習全体のあり方を整理するとともに、他省庁、セプター、重要インフラ事業者等に対し演習に関する各種ノウハウを提供できるよう努めるものとする。 （2） 演習成果の分野全体への浸透 演習成果の活用は実態面では演習参加者を中心とした一部の事業者等にとどまっており、施策面でも演習と他の重要インフラ施策の連携が十分とは言えない状況にある。 このため、次期行動計画の期間中においては、次のような演習成果を各分野の事業者等全体に浸透させる取り組みを進めることが求められる。 ① 演習参加者等の拡充及び演習成果の周知活動の充実 演習参加者（組織、人員）の範囲は人的・予算的な面での制約を受けるが、可能な範囲で演習参加事業者等の一層の拡充に努めることとする。特に、首都圏以外の事業者や準大手以下の事業者等の参加を促す取り組みを検討する。また、演習成果展開用資料の充実、業界団体の会合や講演会・研修会・セミナー等の様々な機会を活用した資料説明など、演習成果の周知活動の充実を図るものとする。 ② 演習成果の重要インフラ基盤強化策への反映 演習成果を分野全体に確実に普及・浸透させるためには、①のような実態的な取り組みにとどまらず、演習成果を他の重要インフラ基盤強化施策（安全基準等の整備及び浸透、情報共有体制の強化等）に反映させることが有効である。具体的には、毎年度の演習で得られた気づき等を重要インフラ基盤強化施策に反映させ、その結果を次年度の演習で検証するプロセスの構築が求められる。 （3） ベンダー等の関与 重要インフラのIT障害発生時における応急対応・復旧対応については、システムの運用保守に関わるベンダー等の関与が不可欠である。 従来の演習にベンダー等は参加していないが、次期行動計画における関係主体としてベンダー等の位置付けを検討することを想定しており、ベンダー等の演習への参加の在り方も併せて検討することが適当であると考えられる。なお、検討に当たっては、演習に参加するベンダーの選定方法や参加形態、他の演習参加者との情報共有の範囲等について特に留	左記 （1）総論を参照。 サイバー空間関連事業者については、ベンダー等の関与を検討していることから、すでに検討範囲に織り込み済み（セキュリティベンダーに関しては、別途検討が必要）。 また、関係CSIRTについては、その関与の在り方を検討する必要があるが、現時点での考え方（案）は以下のとおり。 ① 重要インフラ事業者（既存参加者）のCSIRT 基本的に問題なし ② ベンダー等のCSIRT ベンダーの位置付けに依存するが、具体的な貢献が見える場合は、CSIRTとしての参加も検討してよいと思料。 ③ ①、②以外のCSIRT プレイヤーと当該CSIRT間で具体的に提供・共有される情報がある場合のみ、参加の可否を考える可能性あり（それ以外では参加を認めない）

		意する必要がある。 （4） IT障害対応演習と物理的障害対応訓練との連携 東日本大震災の教訓、あるいは、サイバー攻撃の高度化・複雑化の傾向を勘案すれば、自然災害や人為的な攻撃によるIT障害発生時に備えて、ITシステムの稼働継続、早期復旧に向けた対応を関係者間で検証することは益々重要なものとなっている。このため、例えば、分野横断的演習において、大規模自然災害やサイバー攻撃に伴う物理的な被害を考慮したシナリオを策定し、防災・危機管理関係者の参加をも得て、災害及びIT障害の双方に対応するための演習を実施すべきとの考え方もあり得る。 しかしながら、現実にこのような演習を実施とする場合、立場の異なる極めて多くの関係者が演習に関与することとなり、これら関係者間の意見調整を行い、複雑なシナリオの策定、情報共有の方法や情報共有し得る情報の範囲の設定等の課題に対応することが求められるが、現在の人的・予算的制約の中でこれらの条件を全て満足することは非常に困難であることが想定される。 当面の対応策としては、まずは関係部局に対して、防災関係の演習・訓練にITシステムの維持・復旧に向けた取り組みを反映するよう働きかけることを通じて、情報セキュリティ関係部局と防災関係部局の連携強化を徐々に進めていくことが現実的かつ効果的であると考えられる。 （5） 重要インフラ所管省庁等の実施する演習との連携強化 最近、分野横断的演習のほか、重要インフラ所管省庁においても独自にサイバー関連事態対処演習を実施するようになっている。 分野横断的演習は、重要インフラ関係者間の情報共有・連携対処を検証するための演習であるのに対し、所管省庁等の演習は現時点では実機を使用しサイバー攻撃に対する事業者の技術面での対処能力の向上を図るための演習であり、その実施目的や期待される効果が異なっている。 このため、これらの演習を相互に連携・補完し合いながら実施することにより、効率的かつ効果的に重要インフラの防護能力の向上を図っていくことが期待される。 この観点から、次期行動計画の策定時には、重要インフラ所管省庁等のサイバー演習を関係施策として位置付けた上で、演習成果の相互活用を始め、演習間の連携強化を図っていくことが求められる。	
第2次行動計画の見直しを実施した上で、新たな行動計画を策定する。	5 環境変化への対応 社会環境や技術環境等の状況は刻々と変化しているため、情報セキュリティ対策の有効性を保ち続けるためには、環境の変化に情報セキュリティ対策を機敏に対応させていく必要がある。 そのため、広く国民に対しての広報公聴活動、当事者間のリスクコミュニケーション、国際連携等を通じて、関係主体各々が第2次行動計画策定時に想定しなかった環境の変化を察知する能力の向上に努めることとする。また、こうした環境の変化に対して、第2次行動計画の枠組みだけでは十分に対応できない場合は、内閣官房は必要な対応が可能となるような体制の検討を行うこととする。 （1） 広報公聴活動 IT 障害が発生した際の影響を可能な限り極小化するためには、重要インフラ事業者等による情報セキュリティ対策の強化のみならず、国民が状況を踏まえ冷静に対応できるようになることもまた重要である。 そのため、我が国の重要インフラ防護に関わる関係主体が行動計画に基づき実施した取組みを広報することによって、国民に対しての説明責任を果たすとともに、国民が冷静な対応をとる上で必要な情報が得られるように努める。また、広報公聴活動を通じて第2次行動計画に関心をもつ主体を増やすことが、広く協力、支援を得るためにも重要である。 広報活動としては、行動計画に基づく関係主体の取組みを Web 等を活用して幅広く発信することとする。特に、重要インフラ専門委員会等の会議資料については可能な限り公開することとする。関係主体は自らの取組みを可能な範囲で公表することが望ましい。 また、公聴活動としては、セミナー等の機会を広く捉えて行動計画の紹介を行うとともに意見聴取に努める。また、Web を活用して意見を受け付け、これを行動計画の推進の参考とするとともに、行動計画の見直しの材料として活用する。 （2） リスクコミュニケーションの充実 各関係主体が互いの連携を進めるためにはリスクコミュニケーションを充実させることが重要である。リスクコミュニケーションとは、情報セキュリティ対策において連携すべき関係者間で、リスクについての誤解や理解不足を解消し、また関係者間で及ぼしあうリスクについての認識を共有するためのコミュニケーションである。これによって、連携して対処すべきリスクや対策の方法についての共通認識が得られるとともに、情報セキュリティ対策において連携効果を高めることができると期待される。またより強固な信頼関係が得られると期待される。 そのため、関係主体間の直接的なコミュニケーションの機会の拡大を図ることとする。 なお、リスクコミュニケーションは関係主体間で必要な範囲で行うべきものであって、例えば機密情報に当たるものを一般に開示すること等を意図しているものではない。当然ながら、開示することによって脅威が増すことが懸念される情報については、状況に応じて慎重な扱いを要するものである。 （3） 国際連携の推進 国際的には、「重要情報インフラ」と呼ばれる概念の下で、その防護のためのベストプラクティスの共有が進められている。具体的には、重要情報インフラを支える制御システム等への脅威の分析や対策のためのベストプラクティスの共有や、重要情報インフラ間の相互依存性の解析等についての議論が行われている。内閣官房は、国際連携を積極的に行う関係主体の協力を得て、国際会合や他国機関等との対話を通じて最新動向を把握し、機密情報の取扱い等に留意しつつ、情報共有に努める。	（新たな行動計画策定に向けた検討はすでに開始：専門委員会における関係議論全体を指す）	これまでの議論では、 ① 安全基準等の整備及び浸透 ② 情報共有体制の強化 ③ 障害対応体制の強化（仮称：横断的演習の拡充、他省庁演習との連携等を含む） に加え、何らかのリスク調査・分析が施策として必要と事務局では考えているところ。 （相互依存性解析、現在重要インフラと位置付けられていないが影響が既存の10分野と同等程度あるものの実情、これから情報通信技術そのものまたはその利活用の進展により、その全部または一部が重要インフラに入る可能性があるものの動向調査及びリスク分析 等） また、第2次行動計画「環境変化への対応」の （1）広報公聴活動 （3）国際連携の推進 については、これらの施策群に含まれない。施策群の中に勘定するか否かは別として、何らかの記載は必要。 なお、国際関係については、別途作成する予定の「サイバーセキュリティに関する国際戦略」と整合したものにする必要あり。 （現時点で関係する可能性のある項目案として、

			a. 情報共有体制の構築 例：IWWN、ASEAN 各国とのｻｲﾊﾞｰ演習 b. 制度整備支援 例：制御系ｼｽﾃﾑ・機器の国際標準化の普及・促進、相互承認枠組み策定 c. 国際会議への積極的参画 例：Meridian その他重要インフラ関係省庁が参加する国際会議への参画、情報交換 等が考えられる。）
重要インフラ分野におけるサプライチェーン・リスクへの対応強化を図るとともに、情報セキュリティの評価認証の導入を進めていくことが重要である。具体的には、重要インフラ事業者等とサイバー空間関連事業者との脆弱性情報や攻撃情報の情報共有等による連携の促進、SCADA等の制御系機器・システム等の調達・運用における国際標準に則った評価認証導入の在り方の検討や、制御系機器・システムの評価認証機関の設立に向けた取組を進めていく。	（2 情報共有体制の強化）（再掲） 5 環境変化への対応 （4） 情報セキュリティ基盤の強化 情報セキュリティ基盤の強化のために、人材育成、研究開発、地域レベルの取組みをそれぞれ推進することとする。 人材育成については、演習・訓練及びセミナー等を通じて、高度な IT スキルを有する人材の育成を図る。 研究開発については、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、脅威への対応能力の強化に資する研究開発を促進する。 地域レベルの取組みについては、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等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する事に努める。	「2 情報共有体制の強化」参照（情報共有等による連携の促進） ＜専門委員会における議論なし＞（制御系機器・システム関係）	「重要インフラ事業者等とサイバー空間関連事業者との脆弱性情報や攻撃情報の情報共有等による連携の促進」は、一般的な情報共有ではないものとして整理すべき。 制御システム関係の各種情報をどの共有体制を用いて、どのように共有するのか、また、「SCADA等の制御系機器・システム等の調達・運用における国際標準に則った評価認証導入の在り方の検討」「制御系機器・システムの評価認証機関の設立」について、行動計画に何らかの記載を行うか否かは所管省庁と要調整。（国際関係の取組みとしても検討が必要）
	Ⅲ 関係主体において取り組むべき事項 1 推進体制 （略） 2 各主体の取組み （1） 内閣官房の施策 （2） 重要インフラ所管省庁の施策 （3） 情報セキュリティ関係省庁の施策 （4） 事案対処省庁の施策 （5） 関係機関の自主的な取組みとして期待する事項 （6） 重要インフラ事業者等の自主的な対策として期待する事項 （7） セプターの自主的な対策として期待する事項 （8） セプターカウンシルの自主的な対策として期待する事項 （略）	＜専門委員会における議論なし＞	（施策群の方向性とともに関係主体の取組みを記載予定）
第2次行動計画の見直しを実施した上で、新たな行動計画を策定する。（再掲）	Ⅳ 評価・検証と見直し 1 行動計画の推進体制 （1） 行動計画の進捗状況の評価・検証 （2） 対策の成果検証 （3） 施策の成果検証 （4） 結果の評価のための補完調査 （5） 行動計画に基づく取組みの結果の評価 （略） （6） 行動計画の見直し 第2次行動計画については、対策の成果、施策の成果、補完調査、評価の内容（以下「評価等」という。）を踏まえ、また、脅威、IT 障害、IT を利用したサービス等に関する社会情勢等の変化等をふまえ、3年毎又は必要に応じ、見直しを行う。再度の見直しについては、平成25年度に行うものとする。 特に見直しの要点となるのは、目標とそれに基づく基本的な方向性、重要インフラ事業者等の対象範囲、関係主体とすべき主体の対象範囲、対策や施策の追加や廃止、想定すべき脅威の例示、対象とすべき重要インフラサービスの範囲、サービスレベル、検証レベル、評価指標の設定等である。またこれに併せて、各用語の定義や行動計画の対象範囲についても、必要に応じて見直しを行うものとする。 第2次行動計画の見直しに際しては、各分野の特性や取組状況に配慮しつつ、事業者の取組みが自主性に基づくものであることを踏まえた検討を行うことが必要である。また、第2次行動計画が想定し得なかった事象が発生した場合はこれに対応できるようにすることが重要である。 行動計画の見直しは重要インフラ専門委員会において行うこととし、委員会の合意を経て、情報セキュリティ政策会議で新たな行動計画を決定するものとする。	＜専門委員会における議論なし＞	（次期行動計画を策定するタイミングで全体を検討予定）
これまで我が国では、大規模サイバー攻撃事態等を想定して、初動	Ⅳ 評価・検証と見直し 2 既存の情報共有体制との連携 緊急事態時や災害対策等においては、第2次行動計画の情報共有の枠組みの他にも、既存の情報共	＜専門委員会における議論なし＞ ただし、「2 情報共有体制の強化」に一部関係。	大規模サイバー攻撃事態、大規模障害発生事態における対処体制及びこれら

対処訓練の実施など事案発生時の対処態勢を構築するとともに、平素及び事案発生時の情報収集・集約体制の強化を図ってきている。今後も、大規模サイバー攻撃事態等が発生した際に官民が連携して的確な対応を行うことができる態勢を整備するため、必要に応じて諸外国の事例も参考としつつ、大規模サイバー攻撃事態等の発生を想定した関係者による対処訓練を毎年度実施するなど対処態勢を強化する。	有体制がある。既存の情報共有体制が想定している事態のもと IT 障害が発生した場合には、第2次行動計画とこれら情報共有体制との連携が望まれる。このため、内閣官房は関係する府省庁の協力を得て情報共有の円滑化に向けた検討を行うこととする。		の事態を念頭に置いた訓練について、内閣官房の取組みとしての記載が必要か否か要検討。 行動計画への記載ぶりとしては、対処態勢におけるNISCの活動を規定する上で、例えば「NISCは当該初動態勢における対処及び情報共有について、既存の情報共有体制を活用しつつ、必要な対応を行う。」等、第2次行動計画同様、通常の施策とは異なる対処であることを明確にした上で必要な対処態勢をとる旨の記載とすることが適当。
	別添：情報提供・情報連絡について 1 IT障害に関する情報 「IT 障害に関する情報」とは、IT 障害、IT の機能不全等に関する情報セキュリティ対策に資する幅広い情報である。 IT 障害に関する情報には、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つの側面が含まれ、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、また重要インフラ事業者等間並びに相互依存性のある重要インフラ分野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。 IT 障害に関する情報の各側面としては以下のようなものが含まれる。 1） 未然防止 障害発生の脅威に係る情報（防護方策等を含む） 2） 拡大防止・復旧 障害発生後の影響伝搬予測及び復旧に資する情報 3） 再発防止 事後分析に資する情報の共同収集及び分析・検証の結果 2 重要インフラ事業者等への情報提供 （1） 情報提供の対象する重要インフラ事業者等の範囲 （略） （2） 情報提供の内容 （略） （3） 情報提供の仕組み （略） （4） 情報提供のための連携体制 内閣官房は、重要インフラ所管省庁を通じて重要インフラ事業者等に提供する情報の集約及び重要インフラ事業者等への情報提供にあたり、情報セキュリティ関係省庁、事案対処省庁、関係機関と連携する。 ①情報セキュリティ関係省庁、事案対処省庁、関係機関から提供される幅広い情報の集約。 ②攻撃がテロによるものと思われる場合における被災情報等の事案対処省庁への提供及び攻撃手法情報等の情報セキュリティ関係省庁への提供。 ③情報の集約・分析においては、必要に応じ、関係機関に連携等を要請。 ④災害に関する情報については、内閣官房、内閣府及び関係省庁間の既存の情報共有体制の下で情報を集約及び共有。 （5） 情報の質の強化（分析情報、影響度等） （略）	「2 情報共有体制の強化」参照	（実施細目の見直しとともに詳細を検討する必要あり）
	3 重要インフラ事業者等からの情報連絡 （1） 情報提供を行う場合と連絡する情報 情報連絡が必要となる場合は、以下の①から④に掲げる場合であって、法令等で報告が義務づけられている場合、及び重要インフラ事業者等が特異重大なものとして連絡を要すると判断した場合である。 ①サイバー攻撃をはじめとする意図的要因による次の場合 ア）IT 障害が発生した場合 イ）サイバー攻撃を検知した場合又は攻撃の予告があった場合 ウ）サイバー攻撃による被害を検知した場合 エ）IT の機能不全が顕在化した場合、脅威が発生した場合、その他特異重大なものであって、他の重要インフラ事業者等の対策に資すると考えられる場合 ②非意図的要因による次の場合 ア）IT 障害が発生した場合 イ）IT の機能不全が顕在化した場合、脅威が発生した場合、その他特異重大なものであって、他の重要インフラ事業者等の対策に資すると考えられる場合 ③災害や疾病による次の場合 ア）IT 障害が発生した場合 イ）2 次被害により IT 障害が発生すると考えられる場合 ウ）IT の機能不全が顕在化した場合、脅威が発生した場合、その他特異重大なものであって、他の重要インフラ事業者等の対策に資すると考えられる場合 ④他分野の障害からの波及による次の場合 ア）IT 障害が発生した場合	「2 情報共有体制の強化」参照	（同上）

	イ）IT の機能不全が顕在化した場合、脅威が発生した場合、その他特異重大なものであって、他の重要インフラ事業者等の対策に資すると考えられる場合 なお、上記に該当しない場合においても、各重要インフラ事業者等の障害が他の重要インフラ事業者等の IT 障害に波及あるいは影響を及ぼす恐れがある場合など、IT 障害の未然防止、被害の拡大防止等に資すると考えられる場合や上記に該当するかどうか不明な場合については、重要インフラ所管省庁又は内閣官房に対して相談することが望ましい。 （2） 情報連絡の内容 （略） （3） 情報連絡の仕組み 重要インフラ事業者等から重要インフラ所管省庁を通じて内閣官房に至る情報連絡の手順は以下のとおりとする。 ①重要インフラ事業者等は、別紙5に示された連絡体制等に基づき重要インフラ所管省庁に連絡する。 ②重要インフラ事業者等から受けた連絡については、重要インフラ所管省庁の当該分野担当のリエゾンから、内閣官房に連絡する。 ③内閣官房は、連絡された情報を適切に識別管理し、情報連絡元が指定する情報共有の可能な範囲で取り扱うものとする。 （4） 連絡された情報の取扱いに関する考え方 （略）		
これまで我が国では、大規模サイバー攻撃事態等を想定して、初動対処訓練の実施など事案発生時の対処態勢を構築するとともに、平素及び事案発生時の情報収集・集約体制の強化を図ってきている。今後も、大規模サイバー攻撃事態等が発生した際に官民が連携して的確な対応を行うことができる態勢を整備するため、必要に応じて諸外国の事例も参考としつつ、大規模サイバー攻撃事態等の発生を想定した関係者による対処訓練を毎年度実施するなど対処態勢を強化する。（再掲）	別添：情報提供・情報連絡について 4 災害やテロ等の緊急事態における情報の集約及び共有 災害やテロ等の緊急事態においては、前述の1から3に定めるところにかかわらず、「緊急事態に対する政府の初動対処体制について」（平成15年11月21日閣議決定）等に基づき、内閣官房及び関係府省庁間で情報を集約及び共有するものとする。	＜専門委員会における議論なし＞ ただし、「2 情報共有体制の強化」に一部関係。	大規模サイバー攻撃事態、大規模障害発生事態における対処体制及びこれらの事態を念頭に置いた訓練について、内閣官房の取組みとしての記載が必要か否か要検討。 行動計画への記載ぶりとしては、対処態勢におけるNISCの活動を規定する上で、例えば「NISCは当該初動態勢における対処及び情報共有について、既存の情報共有体制を活用しつつ、必要な対応を行う。」等、第2次行動計画同様、通常の施策とは異なる対処であることを明確にした上で必要な対処態勢をとる旨の記載とすることが適当。