重要インフラにおける情報セキュリティ確保に係る

「安全基準等」策定にあたっての指針（第３版）

平成 22 年 5 月 11 日
平成 25 年 2 月 22 日 改定
情 報 セキュリティ政 策 会 議

重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第3版）

Ⅰ　目的及び位置づけ

１．重要インフラにおける情報セキュリティ確保のために

国民生活や社会経済活動の基盤である重要インフラ[1]におけるIT化の進展や相互の依存関係の増大に伴い、重要インフラのIT障害[2]に対して、分野を越えた横断的情報セキュリティ対策を一層強化していくことが喫緊の課題となっている。

この課題を早期に解決していくためには、各重要インフラ事業者等[3]において、当該事業分野の特性及び当該事業者の特性を踏まえ、適切な情報セキュリティ対策が早急になされることが必要である。

２.「安全基準等」の必要性

各重要インフラ事業者等においては、各々が行う事業に国民生活が大きく依存していることを自覚し、国民の期待に応えるべく、より高品質なサービスを途絶えることなく提供すべく日々努力しているところである。

しかしながら、こと情報セキュリティに関しては、対策の効果が目に見えにくいことから、当該対策が十分であるか、事業者自らが十分な対策をなしているのか、を自己検証しつつ、国民生活や社会経済活動に重大な影響を及ぼさないよう IT 障害から重要インフラを防護する対策を進めることが重要である。その際、未然防止のための対策と、IT 障害発生後の拡大防止・早期復旧に向けた対応のバランスを取ることが望ましい。

このため、それぞれの事業分野においてその特性に応じた必要又は望ましい情報セキュリティ対策の水準を「安全基準等」という形で明示し、個々の事業者が、重要インフラの担い手としての意識に基づく自主的な取り組みのもと、その「安全基準等」を満たすべく努力し、また満たしているか否かを自ら検証することが必要である。

３.「安全基準等」とは何か

各重要インフラ事業者等は、一般に「業法」と呼ばれる、当該事業分野に属する事業を営む者を規律する法制度の下に、国が定める様々な基準に従い、業を営んでいる。[4]

しかしながら、本指針においては

---

1 「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、我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」を指す。

2 「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。

3 「重要インフラ事業者等」とは、「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」の各分野に属する事業を営む者のうち、「重要インフラの情報セキュリティ対策に係る第2次行動計画（2009 年 2 月 3　日情報セキュリティ政策会議決定）」（以下「第 2 次行動計画」という。）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を指す。

4 地方公共団体は、地方自治法に基づき、地域における行政を自主的かつ総合的に実施している。

① 業法に基づき国が定める「強制基準」
② 業法に準じて国が定める「推奨基準」及び「ガイドライン」
③ 業法や国民からの期待に応えるべく事業者団体等が定める業界横断的な「業界標準」及び「ガイドライン」
④ 業法や国民及び契約者等からの期待に応えるべく事業者自らが定める「内規」

等、いずれかの形で各事業者が様々な判断、行為を行うに当たり、基準又は参考にするものとして策定された文書類を「安全基準等」と呼ぶ。

求められる情報セキュリティ対策が、確実になされるためには、これら「安全基準等」において、情報セキュリティ対策の項目及び水準が文書として明定されることが必要であり、上記①から④を一覧することにより、「自らが何をすべきか」が重要インフラの事業に携わる全ての関係者にとって理解可能な状況となっていることが望まれる。

4. 本指針の位置づけ

上述のように、情報セキュリティ対策の実施に当たり、もっとも困難なのは、「何をすべきか」「どの程度すべきか」の判断である。

このため、重要インフラ分野においてサービス提供継続及び国民の信頼性に応えるとの観点から情報セキュリティ対策を実施する場合、特段の理由のない限り対策することが望まれる事項に加え、任意で参考とする事項を列記し、「安全基準等」の策定・改定を支援することが本指針の目的である。

その上で、本指針においては、サイバー攻撃をはじめとする意図的要因に加え、災害、非意図的要因などサービス提供に影響を及ぼす可能性のある様々な事象を念頭に置き、さらに重要インフラのサービス供給の根幹をなす制御系システムにおける対策のみならず、新たな脅威として加えた疾病や他分野の障害からの波及や国民の信頼感喪失の原因となる情報漏えいへの対策も念頭に置いて、実施することが望ましい項目を列記している。

本指針はあくまで重要インフラ分野を横断的に俯瞰して必要度が高いと考えられる項目及び先進的な取組みとして参考とすることを期待する項目を記載したものであり、また「情報セキュリティ対策」に特化して記載したものであることから、

①事業分野又は事業者によっては、その事業の態様等の理由から、本指針に記載する項目の中に、規定する必要がないものもあり得ること
②事業分野又は事業者によっては、その事業の態様等の理由から、本指針に記載していない項目について、規定する必要がある場合もあり得ること

を念のため付言する。

なお、本指針に掲げた各項目及び当該項目の水準等を、「安全基準等」のうちどの文書にて定めるのかについては、各業法の規定及び既に定められている「安全基準等」の構成等を踏まえ、各事業分野ごとに検討されることを期待する。

５．本指針の構成

本指針では、後述のⅡ（「安全基準等」で規定が望まれる項目）において、「要検討事項」と「参考事項」を列記している。ここで、「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事業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、各事業分野が任意で参考とする事項とする。

また、重要インフラ分野及び重要インフラ事業者等によって、それぞれの項目の重要度が異なると考えられることから、必要に応じて参考にできるよう本指針の別冊として対策編を設け、対策項目の具体化の例示を行うこととし、対策編は、重要インフラ専門委員会[5]にて取りまとめることとする。また対策編では、「安全基準等」の継続的改善において参考となる文献について整理し、各事業分野又は各事業者等の自主的な取組みに資する項目を充実することとする。

６．本指針を踏まえた「安全基準等」の継続的改善及び浸透への期待

本指針は、あくまで重要インフラ分野を横断的に俯瞰して必要度が高いと考えられる項目及び先進的な取組みとして参考とすることを期待する項目を記載したものであり、また「情報セキュリティ対策」に特化して記載したものであることから、重要インフラ分野及び重要インフラ事業者等が個々の「安全基準等」を策定または改定する際においては、より高度な情報セキュリティ水準の実現を目指し、本指針に示された項目を満たすだけでなく、一層高度かつ網羅的な「安全基準等」となるよう、随時検討がなされることを期待する。

このような観点からは、各種規格をはじめとする国内外のベストプラクティスを積極的に参考にしていくとともに、「政府機関の情報セキュリティ対策のための統一基準」及び関連文書を適宜参照することが望ましい。

これらを踏まえ、個々の重要インフラ分野においては、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。

また、「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。

Ⅱ　「安全基準等」で規定が望まれる項目

１．「安全基準等」策定の目的

重要インフラが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、情報セキュリティ対策を実施するにあたって「安全基準等」の遵守が必

5　「重要インフラ専門委員会」は、わが国全体の重要インフラ防護に資する情報セキュリティに係る事項について、調査検討を行う専門委員会として置かれている（「重要インフラ専門委員会の設置について（平成17年9月15日情報セキュリティ政策会議決定）」より）

要である又は望ましい旨を規定する。

なお、「安全基準等」の策定においては、第 2 次行動計画にて定めた「重要インフラサービス [6]と重要システム [7]」及び「サービスレベル [8]と検証レベル [9]」について、各重要インフラ分野の特性を考慮した検討が必要である。

2.「安全基準等」の対象範囲

「安全基準等」の保護対象は何であるかを可能な限り具体的に規定する。その際、重要インフラ事業者等が提供するサービスを明確化した上で、IT 障害により重要インフラ事業者等の事業継続性に密接に関連するすべての構成要素を保護対象として定義することが望ましい。保護対象としては、例えば下記のものが想定される。

(1)情報資産(情報システム及びそこに蓄積されている情報)

(2)情報システム間でやりとりされるトランザクション [10]又はビジネスプロセス

(3)情報システムの開発・運用・保守

3.「安全基準等」の対象とする脅威

対象とする脅威として、顕在化する可能性が高い IT 障害を想定し、事業継続性への影響度等各重要インフラ分野の特性等を考慮して、可能な限り具体的に定義することが望ましい。対象とする脅威としては、例えば下記のものが想定される。

(1)サイバー攻撃をはじめとする意図的要因

不正侵入、データ改ざん・破壊、不正コマンド実行、ウイルス攻撃、サービス不能(DoS: Denial of Service)攻撃、情報漏えい、重要情報の搾取、内部不正 等

(2)非意図的要因

設計・開発の不備、操作・設定ミス、プログラム上の欠陥(バグ)、メンテナンス不備、内部・外部監査機能の不備、外部委託管理の不備、マネジメントの欠陥、機器故障等

---

6 「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。

7 「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。

8「サービスレベル」とは、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指す。第 2 次行動計画では、「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」としている。

9 第 2 次行動計画において、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。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。

10 関連する複数の処理を一つの処理単位としてまとめたもの。一連の作業を全体として一つの処理として管理するために用いる。

(3) 災害や疾病

地震、水害、落雷、火災等の災害による電力設備の損壊、通信設備の損壊、水道設備の損壊、コンピュータ施設の損壊、大規模・広範囲にわたる疾病による要員不足に伴うコンピュータ施設の運用に係る機能不全　等

(4) 他分野の障害からの波及

電力供給の途絶、通信の途絶、水道供給の途絶（相互依存性解析の成果で判明しているもの）　等

4. 重要インフラ事業者等の担う役割

それぞれの対策を担うべき主体が不明確にならないよう、所管省庁が担うべき役割、分野全体として担うべき役割、個別の重要インフラ事業者等の担うべき役割を規定するべきである。加えて、第２次行動計画にて定めた各分野の検証レベルを踏まえ、各重要インフラ事業者等がサービスレベルを決定する際に参考となるよう遵守すべき水準を明らかにすることが望ましい。

5.「安全基準等」の公開

重要インフラの国民生活への影響や社会的責任の大きさ等に鑑み、国民に対し安全・安心に取り組む姿勢を表明する観点から、「安全基準等」に公開に関する規定を置き、可能な限り公開されることが望ましい。

この際、公開することにより脅威の増大等が想定される項目等については、当該項目が非公開であることを明示するとともに、何故公開すべきでないのかを明記することが望ましい。

6. 対策項目

各重要インフラ分野において策定若しくは見直しされる「安全基準等」は、以下の４つの柱と5つの重点項目を盛り込むことが望ましい。（重点項目によっては、4つの柱に包含して記述することも考えられる。）。また、対応については、その情報システムや情報の重要度、利用状況に応じた対応をとるべきである。

なお、「安全基準等」の継続的改善に当たっては、その実効性及び合理性を十分に勘案すること。

（1）4つの柱

ア　組織・体制及び資源の対策

（ア） 組織・体制及び人的資源の確保【要検討事項】

各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PDCAサイク

ル [11]を機能させるために、その運用等に係る組織及び体制の確立及びこれを支える資源の確保が重要である。

情報セキュリティ対策は、それに係るすべての職員が、職制及び職務に応じて与えられている権限と責務を理解した上で、準備された資源によって、負うべき責務を履行することで実現される。

このため、情報セキュリティ対策を実施する組織・体制及び資源の確保について明示されることが必要である。

なお、組織・体制及び資源の確保には、例えば、情報セキュリティに関わる人材育成や教育といった基礎的・長期的な取り組みから、情報セキュリティ対策の実効性を確保する上で必要な自己点検・監査の実施等具体的な対策項目が含まれる。

（イ） 情報セキュリティ人材の育成等 【参考事項】

知的財産としての「人財」という観点から、情報セキュリティ人材の育成や要員の管理を行うことが望ましい。

（ウ） 外部監査等による情報セキュリティ対策の評価 【参考事項】

技術的な対策は多くの事業者等で行われているが、今後は外部監査等による情報セキュリティ対策の評価を行うことが望ましい。

イ 情報についての対策

各重要インフラ事業者等における情報セキュリティ対策においては、情報のライフサイクルに着目し、各段階において遵守すべき事項を定め、各職員の業務の流れにおける情報保護の対策を示すことが重要である。

（ア） 情報の格付け 【要検討事項】

取扱う情報について、その重要度に応じた適切な措置を講じるため、機密性、完全性、可用性の観点から、情報の格付け（ランク）や、取扱制限（例：複製禁止、持出禁止、再配付禁止）が明示されるべきである。

（イ） 情報の取扱い 【要検討事項】

情報の作成、入手、利用、保存、移送、提供及び消去等、情報のライフサイクルに着目し、各段階における情報セキュリティ対策が明示されるべきである。

---

11 典型的なマネジメントサイクルの 1 つで、計画（plan）、実行（do）、評価（check）、改善（act）のプロセスを順に実施し、最後の改善を次の計画に結び付け、らせん状に品質の維持・向上や継続的な業務改善活動などを推進するマネジメント手法。

ウ 情報セキュリティ要件の明確化に基づく対策

各重要インフラ事業者等における情報セキュリティ対策においては、情報システムにおいて、その重要性に応じた適切な措置を講じるため、機密性、完全性、可用性等の観点から、アクセス制御の観点など導入すべき情報セキュリティ機能を示すとともに、セキュリティホール、不正プログラム及びサービス不能攻撃等の脅威を防ぐために遵守すべき事項を定め、情報システムにおいて講ずべき対策を示すことが重要である。

（ア） 情報セキュリティ確保のために求められる機能 【要検討事項】

主体認証（利用者及び機器等の認証）、アクセス制御、権限管理、証跡管理、負荷分散、冗長化など基本的な情報セキュリティ機能の観点から、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。

（イ） 情報セキュリティについての脅威 【要検討事項】

セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。

エ 情報システムについての対策

現在、各重要インフラ事業の継続及びサービスの維持は、業務系、制御系を問わず、情報システムへの依存度が高くなっている。

このため、明確化した情報セキュリティ要件に対応した対策項目を、ライフサイクルに応じて装置やシステムごとに規定することが重要である。[12]

また、社外での情報処理の制限や情報セキュリティ水準の低下を招く行為の防止等、個別事象への対応事項として対策すべきと思われる項目も規定されることが重要である。その際、処理性能確保のための設計やシステム品質確保等の対策を考慮することが重要である。

なお、安全な情報システムの構築を推進するため、客観的に評価された暗号、製品等を導入することを併せて検討することも重要である。

（ア） 施設と環境 【要検討事項】

入退出の管理や安全区域の確保、停電時、断水時の対応等情報システムの設置・運用に係る施設や環境面での対策が明示されるべきである。

---

12 ITの適用やITへの依存の範囲拡大・高度化・ブラックボックス化（そもそも依存自体が見えにくくなってきていること、及び依存自体は明らかであっても技術やノウハウの理解が十分でなく的確な対応が困難になってきていること）が進みつつあるという認識に立つことが重要である。

（イ） 電子計算機 【要検討事項】

電子計算機の設置時、運用時（保守時を含む。）、運用終了時における対策が明示されるべきである。

なお、システムの統合、更新時には十分な検証等が望まれる。

（ウ） アプリケーションソフトウェア 【要検討事項】

アプリケーションソフトウェアの導入時、運用時（保守時を含む。）、運用終了時における対策が明示されるべきである。

なお、システムの統合、更新時には十分な検証等が望まれる。

（エ） 通信回線及び通信回線装置 【要検討事項】

通信回線及び通信回線装置の構築から運用、運用終了又は停止に至るまでの対策が明示されるべきである。

(2)5つの重点項目

ア IT 障害の観点から見た事業継続性確保のための対策

重要インフラは、我が国の国民生活や社会経済活動を支える基盤であり、大規模な障害が発生した場合には、さまざまな領域へ甚大な影響を与えることが予想される。

したがって、重要インフラのサービスの維持・復旧を図るためには、事業継続性の確保に向けた取組みを強化することが必要であり、IT 障害に備えた総合的な対策について規定されることが重要である。

（ア） 事業継続性確保のための個別対策の実施 【要検討事項】

IT 障害を未然に防止するための措置、IT 障害の発生を早期発見するための措置、及びIT障害が発生した場合の拡大防止や迅速復旧のための措置が明示されるべきである。その際、東日本大震災に見られた広域災害・複合障害や新型インフルエンザ等、社会全体で対応が望まれる脅威についても考慮されるべきである。あわせて、事業継続に必要なデータが東京に一極集中している状況を踏まえ、首都直下地震についても考慮されるべきである。

（イ） 事業継続計画との整合性への配慮 【要検討事項】

事業継続計画が策定される場合には、顕在化する可能性が高いIT障害として様々なケースを想定して事業継続計画に組み入れるとともに、適宜点検し、必要に応じ対策の改善を行うべきである。その際、相互依存関係にある重要インフラ分野間（情報通信、電力、水道分野等と他分野との間）にお

いて、リスクコミュニケーション等の連絡・連携に平時より努めるべきである。

イ 情報漏えい防止のための対策

昨今、各重要インフラ分野において機密情報や重要情報等の漏えい等が発生している。重要インフラにおけるこれら情報の漏えい等はその機能の停止・低下等につながるおそれがあるため各分野において発生防止及び再発防止の対策に取り組む必要がある。

なお、重要インフラにおける機密・重要情報等には個人情報も含まれうるが、重要インフラの機能の停止・低下等につながらない個人情報についても、各分野の「個人情報の保護に関するガイドライン」等との整合性を確保した上で、相当するレベルの対策を「安全基準等」に包含し、情報の種類によらず講ずべき情報漏えい対策が総覧可能であることが望ましい。

（ア） 保護すべき情報の類型化 【要検討事項】

漏えい対策の対象となる保護すべき情報を類型化し、明示されるべきである。

（イ） 保護すべき情報の管理 【要検討事項】

保護すべき情報及び当該情報が記録された媒体を安全に取扱う（作成、入手、利用、保存、移送、提供及び消去等）ための措置が明示されるべきである。

（ウ） 不正アクセスによる脅威への対策 【要検討事項】

保護すべき情報が保存されたPCや外部記録媒体の盗難、紛失及び当該PCや外部記録媒体からの情報漏えいを防止するための措置や、保護すべき情報を処理するウェブやメール等のアプリケーションからの情報の漏えいを防止するための措置が明示されるべきである。

（エ） 内部関係者による脅威への対策 【要検討事項】

内部関係者による情報漏えいを抑止するための措置、情報漏えいの追跡性確保のための措置の他、情報セキュリティに関するリテラシーを向上させるための措置や取扱いミスを低減させるための措置が明示されるべきである。

（オ） 情報漏えい発生時の対応策の整備 【要検討事項】

情報漏えいの発生に備えて、当該事象へ対応するための体制及び対処手順等が明示されるべきである。

ウ　外部委託における情報セキュリティ確保のための対策

昨今、各重要インフラ分野における重要情報の漏えいが発生している。その漏えい経路は、重要インフラ事業者等の内部からのみでなく、委託先からのものも含まれている場合が多い。

また、各重要インフラ分野における事業継続性の確保には委託先と連携した情報セキュリティレベルの向上が必須であり、各事業者等による委託先の情報セキュリティ確保に向けた対策を併せて規定することが望ましい。

（ア） 委託先管理の仕組み 【要検討事項】

外部委託可能な範囲の明確化や委託先の選定基準、委託先に求める情報セキュリティ対策項目や事業者としての管理方法等が明示されるべきである。

（イ） 外部委託実施における情報セキュリティ確保対策の徹底【要検討事項】

基本契約の締結や委託内容・取扱い情報の重要性に応じて、必要な情報漏えい防止策等の強化対策事項の契約への盛り込み等、契約者双方の責任の明確化と合意形成が明示されるべきである。

（ウ） IT 障害発生時の対応策の整備 【要検討事項】

IT 障害発生時における委託先の措置や重要インフラ事業者等としての対処方法（委託先及び委託元との間の連絡体制や委託先と委託元が一体となったトラブル対処方法等）が明示されるべきである。

エ　IT障害発生時の利用者の対応のための情報の提供等の対策

重要インフラにおけるサービスの停止・低下が発生した際、利用者が安心して対応が行えるよう情報提供を行うべきである。

（ア） IT障害による重要インフラサービスの停止等の情報の提供 【要検討事項】

重要インフラサービスの停止状況、復旧（可能であれば見込みを含む。）等の情報の適時の提供の方策が明示されるべきである。

（イ） IT障害防止のための取組みに関する情報の提供 【要検討事項】

利用者の安心に資する観点から、重要インフラサービスの停止・低下を防止するための情報セキュリティ対策に関する取組みについて、提供範囲に留意しつつ、対外的な説明に努めるべきである。

オ　ITに係る環境変化に伴う脅威のための対策 【要検討事項】

社会環境や技術環境等の状況は刻々と変化しており、IT 障害を引き起こす新たな脅威が顕在化することがある。このような脅威として、電子計算機の性能の向上により暗号の解読が容易になる「暗号の危殆化」や、インターネットの普及によるIPv4アドレス枯渇に伴う「IPv6 への移行」等が考えられる。

このような情報システムの基盤を支える社会環境や技術環境等の変化について、IT障害発生の未然防止のための適切な対策を検討すべきである。

Ⅲ　フォローアップ

1. フォローアップの考え方

各重要インフラ分野における情報セキュリティの確保について、自主保安原則に基づき、各事業者が自らの管理下にある情報資産に責任を持ち、それぞれの事業形態や情報システムの形態に適応した情報セキュリティ対策を講じていくことが原則である。しかしながら、最近のIT障害事例をみれば、各規程の適切な運用も含めた対策の実効性を一層確保していくことが必要である。

このため、以下のフォローアップを実施し、情報セキュリティ対策の一層の推進を図ることとする。

2. 本指針の継続的改善

（1）指針（本編）改定に関する検討

・内閣官房は、原則として3年に1度、本指針の改定に関する検討を実施する。

（2）指針の分析・検証

・内閣官房は、1年毎、及び必要に応じて適時に、指針の分析・検証を行い、その結果を必要に応じて指針の追補版として周知する。重要インフラ事業者等において事業継続計画の策定が進みつつある状況や、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。

・内閣官房は定常的なIT障害の発生状況の把握を通じ、各重要インフラ分野に共通する横断的な対策課題の分析・検討を行い、本指針の継続的改善のための基礎資料として整備する。

・各重要インフラ事業者等における事業継続性確保対策の検討にとって、重要インフラ間の相互依存性や共通脅威に関する情報は重要と考えられることから、今後、内閣官房が各重要インフラ所管省庁及び重要インフラ事業者等の協力を得て共通脅威分析を実施する際には、その結果を本指針や各重要インフラ分野における「安全基準等」の見直しの基礎資料として提供する。

3.「安全基準等」の継続的改善

「安全基準等」は、情報セキュリティを取り巻く環境の変化に応じ、適宜適切なものとなるよう随時見直しが行われるべきものである。このため、以下に示す各主体の役割に基づき取組みを推進する。

（1）重要インフラ所管省庁及び重要インフラ事業者等

・重要インフラ所管省庁及び重要インフラ事業者等は、相互に協力し、「安全基準等」について適宜適切なものとなるよう、随時検討を行う。

・重要インフラ所管省庁及び重要インフラ事業者等は、「安全基準等」の策定若しくは見直しを行う際に、各重要インフラ事業者等における同基準等に基づく対策基準の検討並びに対策の実効性の確認が容易となるよう配慮することが重要である。具体的には、国際規格等を踏まえて、また各重要インフラの事業分野ごとの特性に応じて設定された評価基準に基づく監査について「安全基準等」に明示することを検討する。

・重要インフラ所管省庁は、重要インフラ事業者等と協力して、各重要インフラ分野におけるIT障害の発生状況を把握するとともに、セプター（情報共有・分析機能）の状況も踏まえ、当該分野の「安全基準等」に反映されるべき対策項目について検討を行う。

・重要インフラ事業者等は、情報セキュリティ監査又はそれに相当するものの実施を自主的な取組みとして実施することを検討する。

（2）内閣官房

・内閣官房は、「安全基準等」の継続的改善状況を、各重要インフラ所管省庁の協力を得て把握する。

・内閣官房は各重要インフラ所管省庁等に対し、所要の継続的改善に必要な参考資料、情報等の提供を継続的に行う。

4.「安全基準等」の浸透

（1）重要インフラ所管省庁及び重要インフラ事業者等

・重要インフラ事業者等は「安全基準等」の浸透に向けて情報セキュリティ対策の実施状況を自ら定期的に点検し、必要に応じて内規の見直しを行う等、対策の改善を行う。また、各対策の実効性を確保する観点から、必要に応じ重要インフラ所管省庁と連携して、各種演習、訓練等を実施する等、対策を実装するための環境整備にも努める。

・重要インフラ所管省庁は、重要インフラ事業者等に対して、対策を実装するための環境整備を含む「安全基準等」の浸透を図る。また、毎年一定時期に内

閣官房が実施する「安全基準等」の浸透状況等の調査に協力する。

（2）内閣官房

・内閣官房は、重要インフラ所管省庁の協力を得つつ、「『安全基準等』の浸透状況等に関する調査」を毎年一定時期に行い、対策状況の客観的な把握を行う。