資料３－２

【改定案】

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

２００６年　２月　２日
情報セキュリティ政策会議決定
（改　定）　2007年　月　日

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[1]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、当該事業分野の特質及び当該事業者の特質を踏まえ、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。

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

---

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：各事業において発生する障害（サービスの停止や機能の低下等）のうち、ITの機能不全が引き起こす障害

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行動計画（2005年12月13　日高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議決定）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。

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 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準じて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」が重要インフラ事業者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、何らかの対処がなされていることが望ましい項目を列記し、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。

このため、本指針においては、サイバーテロ対策の視点に加え、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、新たな脅威の原因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。

なお、重要インフラ分野及び事業者によって、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、本指針では項目を記載するに留めており、対策項目の具体化は各事業分野又は各事業者毎に検討されることを期待する。この場合、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。

---

[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。

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. 本指針を踏まえた安全基準等策定若しくは見直しへの期待

本指針は、個々の重要インフラ分野及び重要インフラ事業者等において、既にどのような安全基準等が定められているかについて考慮していないため、本指針に記載した全ての項目を既に包含した安全基準等を持つ重要インフラ分野又は重要インフラ事業者等も存在し得る。

ただし、本指針は、あくまで最低限の情報セキュリティ対策が講じられるよう安全基準等の策定若しくは見直しを支援するために策定されたものであることから、個々の安全基準等においては、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、別途決定する「政府機関の情報セキュリティ対策のための統一基準」（以下「統一基準」という。）及び関連文書を適宜参照することが望ましい。

Ⅱ 「安全基準等」で規定が望まれる項目

1.「安全基準等」の対象範囲及び対象とする脅威

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[5]又はビジネスプロセス
（3）情報システムの運用

また、対象とする脅威として、以下のような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定義することが望ましい。

（1）サイバー攻撃による IT 障害

不正侵入、改ざん、不正コマンド実行、情報かく乱、ウイルス攻撃、サービス不能（DoS: Denial of Service）攻撃、情報漏えい等

---

5 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。金融機関のコンピュータシステムにおける入出金処理のように、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。

（2）非意図的要因による IT 障害

システムの仕様やプログラム上の欠陥（バグ）、操作ミス、故障、情報漏えい　等

（3）災害による IT 障害

地震、水害、落雷、火災等の災害による電力供給の途絶、通信の途絶、コンピュータ施設の損壊等、重要インフラの機能不全。

2.「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。

3. 具体的項目

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、以下の事項を盛り込むことが望ましい。なお、策定若しくは見直しに当たっては、その実効性及び合理性を十分に勘案すること。

（1）「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」の遵守が必要である又は望ましい旨を規定する。

なお、当該重要インフラ分野での特性を考慮した表現で記述されるべきである。

（2）対象範囲と想定する脅威

保護対象は何であるか、また、想定する脅威は何であるかを規定する。

なお、保護対象及び想定する脅威については、可能な限り具体的に記述するべきである。

（3）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。

（4）対策項目

「安全基準等」に盛り込む具体的な対策に当たっては、以下の 4 つの柱と3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。）。なお、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。

① 4つの柱

ア 組織・体制及び資源の確保

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[6]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、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兼務を禁止する役割の設定や違反への対応、例外措置の規定、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

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

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、各段階におけるセキュリティ対策が明示されるべきである。

---

6 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

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

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。[7]

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社外での行為の防止等、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

入退出の管理や安全区域の確保、停電時へ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。

---

[7] 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

電子計算機の設置時、運用時、運用終了時における対策が明示されるべきである。

（ウ） アプリケーションソフトウェア

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

（エ） 通信回線及び通信回線装置

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 3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

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。

（イ） 事業継続計画との整合性への配慮

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。

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、各分野において策定されているもしくは策定が予定されている「個人情報の保護に関するガイドライン」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

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

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

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

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

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、各重要インフラ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

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事が必要である。この場合、国際規格を踏まえた既存の取り組み等を参考に検討するべきである。

（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

基本契約の締結や委託内容・取扱い情報の重要性に応じたとるべき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

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。

Ⅲ フォローアップ

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。

（1）本指針の見直し

・内閣官房は、1年ごと、及び必要に応じて適時に、本指針の見直しを推進する。

・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、本指針改定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の状況やそれに基づくリスク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

相互依存性解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。

（2）「安全基準等」の継続的検証

「安全基準等」が適宜適切なものとなるよう、以下のような継続的な検証を行う。

①「安全基準等」の見直し

「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、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。

〇内閣官房

・内閣官房は、「安全基準等」の策定状況を、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、所要の見直しに必要な参考資料、情報等の提供を継続的に行う。

〇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、情報共有・分析機能（CEPTOAR）の整備状況も踏まえ、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。

②「安全基準等」に対する準拠状況の評価

重要インフラ事業者等は「安全基準等」に対する準拠状況の評価を実施していくために、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。