電気通信分野における
情報セキュリティ確保に係る
安全基準（第 3 版）

安全・信頼性協議会

平成 28 年 5 月 31 日

目次

変更履歴

制定　第１版　　平成 18 年 9 月 29 日
改訂　第 1.1 版　平成 21 年 4 月 17 日
改訂　第２版　　平成 22 年 12 月 10 日
改訂　第 2.1 版　平成 26 年 1 月 30 日
改訂　第３版　　平成 28 年 5 月 31 日

I. 総論

１．はじめに

国民生活や社会経済活動の基盤である重要インフラ事業における IT 化の進展や相互の依存関係の増大に伴い、重要インフラ上で発生する IT 障害に対する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。それには、事業者が IT 障害に対して十分な対策をなしているのか自己検証しつつ、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、重要インフラの各分野が、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できるようにすることを目的に、情報セキュリティ政策会議（議長：内閣官房長官）において「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」（以下、政府指針）が決定されている。（平成１８年２月初版決定、平成２７年５月第４版改定）

政府指針においては、各重要インフラ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」としており、その中には下記のようなものが含まれるとしている。

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」

「電気通信分野における情報セキュリティ確保に係る安全基準（以下、本ガイドライン）」は、電気通信分野における「安全基準等」の一つとして、電気通信分野の特性を踏まえ、取り組むことが望ましいと考えられる情報セキュリティ対策の基準について業界団体が定めるガイドラインを、政府指針に基づき策定したものである。なお、本ガイドラインにおいては、重要インフラ専門委員会にて決定された「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４版）　対策編」（以下、対策編）（平成２２年７月公表、平成２７年５月改定）の内容も適宜盛り込まれている。対策編については、各社毎の取組みにおいても、内規の見直し等、必要に応じて対策の改善に活用されることを期待する。

本ガイドラインの策定にあたっては、既存の法令や国際標準を参考にし、電気通信事業の各サービス分野（電話、ISP など）で広く活用できる基準とした。電気通信業界の各事業者が情報セキュリティ対策を推進するにあたり、各社の情報セキュリティ要件を踏まえ、本ガイドラインを有効に活用されることを期待する。

また、本ガイドラインでは電気通信事業者だけでなく、電気通信設備提供者（メーカ等）が取り組むことが望ましい対策についても明示した。電気通信設備提供

者と電気通信事業者が、相互に連携して情報セキュリティ対策の高度化を進めることを期待する。

本ガイドラインで規定する内容は、対象とする事業者等に対し情報セキュリティ対策の強化に向けて推奨される取り組み内容を示したものであり、事業者等の具体的な取組みにより、情報セキュリティレベルを向上させていくことが肝要である。

また、本ガイドラインは「電気通信分野を取り巻く環境」や、「新たな情報セキュリティ問題の発生」などの変化に、継続的に対応させていく必要がある。そのため、本ガイドラインの内容については、政府指針の改定時を含め、必要に応じて随時に見直しを推進するものとする。

２．用語及び定義

（１） 一般的な情報セキュリティ用語及び定義

ア 資産

組織にとって価値をもつもの。(ISO/IEC 13335-1:2004)

イ 管理策

リスクを管理する手段（方針、手順、指針、実践、又は組織構造を含む。）であり、実務管理的、技術的、経営的又は法的な性質をもつことがあるもの。(ISO/IEC 27000:2012)

ウ 指針

方針の中に設定された目標を達成するためになすべきこと及びその方法を明らかにした記述。(ISO/IEC 13335-1:2004)

エ 情報処理施設（情報処理設備）

情報処理のシステム、サービス若しくは基盤のいかなるもの、又はそれらを収納する物理的場所。(ISO/IEC 27002:2013)

オ 情報セキュリティ

情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めてもよい。(ISO/IEC 27000:2012)

カ 情報セキュリティ事象

システム、サービス又はネットワークにおける特定の状態の発生。特定の状態とは、情報セキュリティ基本方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関連するかもしれない未知の状況を示していることをいう。(ISO/IEC 27000:2012)

キ 情報セキュリティインシデント

望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、事業運営を危うくする確率及び情報セキュリティを脅かす確率が高いもの。(ISO/IEC 27000:2012)

ク　方針

経営陣が正式に表明した包括的な意思及び方向付け。（ISO/IEC 27000:2012）

ケ　リスク

事象の発生確率と事象の結果の組合せ。(ISO Guide73:2009)

コ　リスク分析

リスク因子を特定するための、及びリスクを算定するための情報の系統的使用。(ISO Guide73:2009)

サ　リスクアセスメント

リスク分析からリスク評価までのすべてのプロセス。(ISO Guide73:2009)

シ　リスクコミュニケーション

意思決定者と他のステークホルダーの間における、リスクに関する情報の交換、又は共有。(ISO Guide73:2009)

ス　リスク評価

リスクの重大さを決定するために、算定されたリスクを与えられたリスク基準と比較するプロセス。(ISO Guide73:2009)

セ　リスクマネジメント

リスクに関して組織を指揮し管理する調整された活動。(ISO Guide73:2009)

注記　リスクマネジメントは一般にリスクアセスメント、リスク対応、リスクの受容及びリスクコミュニケーションを含む。

ソ　リスク対応

リスクを変更させるための方策を、選択及び実施するプロセス。(ISO Guide73:2009)

タ　第三者

当該問題に関して、当事者と無関係であると認められる個人又は団体。(ISO Guide73:2009)

チ　脅威

システム又は組織に損害を与える可能性があるインシデントの潜在的な原因。(ISO/IEC 13335-1:2004)

ツ　ぜい弱性

一つ以上の脅威がつけ込むことができる、資産又は資産グループがもつ弱点。(ISO/IEC 13335-1:2004)

テ　サイバー攻撃

情報通信ネットワーク上で、特定の情報システムや、ネットワークそのものなどに対して行われる電子的な攻撃。

（２）　重要インフラに関する用語及び定義（「重要インフラの情報セキュリティ対策に係る第３次行動計画（2015 年 5 月 25 日改訂　サイバーセキュリティ

戦略本部)」より）

ア　重要インフラ

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。

イ　重要インフラ事業者等

「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」、「物流」、「化学」、「クレジット」及び「石油」の各重要インフラ分野に属する事業を営む者等のうち、「重要インフラの情報セキュリティ対策に係る第３次行動計画（2015 年 5 月 25 日サイバーセキュリティ戦略本部改訂)」（以下「第３次行動計画」という。）別紙１における「対象となる重要インフラ事業者等」に指定された事業者等及び当該事業者等から構成される団体。

ウ　重要インフラサービス

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ごとに第３次行動計画別紙２に定めるもの。

エ　重要システム

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等ごとに定めるもの。

オ　IT 障害

IT の不具合のうち、重要インフラサービスの提供水準が第３次行動計画別紙２における「サービス維持レベル」を下回るもの。

カ　IT の不具合

重要インフラ事業者等の情報システムが、設計時の期待通りの機能を発揮しない又は発揮できない状態となる事象。

キ　サービスレベル

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。

（３）　電気通信分野における情報セキュリティ用語及び定義

ア　電気通信

有線、無線その他の電磁的方式により、符号、音響又は映像を送り、伝え、又は受けることをいう。（電気通信事業法第２条第１号）

イ　電気通信設備

電気通信を行なうための機械、器具、線路その他の電気的設備をいう。（電気通信事業法第２条第２号）

ウ　電気通信サービス

電気通信設備を用いて他人の通信を媒介し、その他電気通信設備を他人の通信の用に供すること。（電気通信事業法第２条第３号参照）

エ　電気通信事業

電気通信サービスを他人の需要に応ずるために提供する事業。（電気通信事業法第２条第４号参照）

オ　重要通信

災害の予防若しくは救援、交通、通信若しくは電力の供給の確保又は秩序の維持のために必要な事項を内容とする通信。公共の利益のため緊急に行なうことを要するその他の通信であって総務省令で定めるものについても、同様に扱う。（電気通信事業法第８条第１項参照）

カ　通信センター

電気通信事業を提供するための交換機能、通信処理機能または情報処理機能を有する電気通信設備を収容する施設。

キ　電気通信設備室

電気通信事業を提供するための電気通信設備を設置している部屋。

ク　電気通信サービス利用者

電気通信サービスを利用する者をいう。（電気通信事業における個人情報保護に関するガイドライン第２条第３号参照）

ケ　電気通信サービス加入者

電気通信事業者との間で電気通信サービスの提供を受ける契約を締結する者をいう。（電気通信事業における個人情報保護に関するガイドライン　第２条第４号参照）

コ　利用者

自社の情報処理施設又はシステムを利用する者をいう。例えば、従業員、契約相手及び第三者の利用者を指す。なお、「電気通信サービス利用者」は、電気通信サービスを介して事業者の電気通信設備等を利用する者と捉えられることから、「電気通信サービス利用者」を含む。

サ　通信の秘密

通信内容にとどまらず、通信当事者の住所・氏名、発受信場所、通信日時等通信の構成要素、通信回数等通信の存在の事実の有無を含む。（電気通信事業における個人情報保護に関するガイドライン第１５条解説参照）

シ　通信履歴

電気通信サービス利用者が電気通信を利用した日時、当該通信の相手方その他の電気通信サービス利用者の通信にかかる情報であって通信内容以外のものをいう。（電気通信事業における個人情報保護に関するガイドライン第２３条参照）

ス　個人情報

生存する個人に関する情報であって、当該情報に含まれる氏名、生年

月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。（個人情報の保護に関する法律第２条第１項）

セ　重要情報

電気通信設備やオペレーションサポートシステム上に格納・管理され、電気通信サービスの提供に不可欠な情報や、電気通信設備の設計・保守・運用等に関する情報をいう。例えば、お客様の契約内容、電気通信設備の設備構成及び通信ログ等の情報を指す。

３．本ガイドラインの公開の取扱い

本ガイドラインで規定する安全基準については、公開とする。

４．対象範囲

本ガイドラインが適用されるべき範囲について、（１）対象事業者、（２）対象サービス、（３）対象資産の観点で説明する。

（１）　対象事業者

主な適用対象となる事業者を、以下の範囲とする。

①　電気通信事業者

電気通信サービスを提供する事業者。電気通信事業法第４１条第１項又は第２項に規定する電気通信設備を設置してサービスを提供する事業者（電気通信回線設備事業者）、及び、それ以外の事業者（電気通信回線設備事業者から設備等を借用して電気通信サービスを行なう事業者等）を含む。

②　電気通信設備提供者（メーカ等）

電気通信事業者からの依頼、要求等に応じて、電気通信設備を構成する装置の全部または一部を提供する者。

（２）　対象サービス

電気通信事業者が提供する全ての電気通信サービスを対象とする。

特に、音声通信（電話等）や ISP サービス（インターネット接続、電子メール、Web, 映像配信等）等の電気通信サービスへの適用を想定する。

（３）　対象資産

電気通信事業者が所有・管理する電気通信設備と、運営に関わるオペレーションサポートシステム、それらに係る情報を対象資産とする。

５．対象とする脅威

本ガイドラインでは電気通信事業において顕在化する可能性が高く、また、事業継続性への影響が大きいと思われる IT 障害を引き起こす以下の４つの要因を対

象脅威とする。

① サイバー攻撃

不正侵入、データ改ざん・破壊、不正コマンド実行、ウィルス攻撃、サービス不能（DoS: Denial of Service）攻撃等のサイバー攻撃を対象脅威とする。

特に、電気通信サービスの安定的な提供を妨げ、また他者の通信を阻害する恐れが高い DoS/DDoS（Distributed DoS）攻撃を、主なサイバー攻撃として想定する。

② ネットワーク輻そう

様々な要因で発生するネットワーク上での発信や送信の大量集中により、ネットワーク設備の動作の低下あるいは停止を引き起こす恐れのあるネットワーク輻そうを対象脅威とする。代表的なネットワーク輻そうとして、イベント的に開催される受付等に大量のアクセスが集中して発生するもの（企画型輻そう）、および、災害時に被災地の住民に対する安否の確認および、被災地内での連絡により発生するもの（災害型輻そう）がある。ネットワーク輻そうの発生により、トラフィックを制御・通過させる電気通信設備がダウンし、あるいは、他の電気通信サービス利用者の通信の疎通を妨げる恐れがあり、適切な対応が必要である。

③ 故障・災害等

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、機器故障等の非意図的要因を対象脅威とする。

また、地震、水害、落雷、火災等の災害による電力設備の損壊、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や、電力供給の途絶、水道供給の途絶等の他分野からの障害の波及を対象脅威とする。

④ 重要情報漏えい

電気通信事業者が取り扱う情報の中でも、特に重要情報の漏えいについては、電気通信サービスの安定的な提供に支障をきたす恐れがあり、企業ブランド価値の毀損や被害者からの訴訟等様々なリスクを伴うものであることから、過失や搾取、内部不正等による重要情報の漏えいを対象脅威とする。

II. 既存の法令・ガイドライン等

本ガイドラインは対象とする脅威に対して、既存の法令・ガイドラインを補完し電気通信分野における情報セキュリティの高度化を推進するものである。事業者等は、本ガイドラインで規定する安全基準や各事業者等が定める内規の他、以下に示す既存の法令・ガイドライン等を電気通信分野の「安全基準等」として遵守または参考にすることとする。

１．電気通信事業法等

（１）　電気通信事業法及び関連する省令等

電気通信事業法は、電気通信事業の公共性から、電気通信事業者に対して、「利用者の利益の保護」と「円滑なサービスの提供」等の目的達成のため、様々な義務を課している。

「利用者の利益の保護」のためには、憲法で保障される通信の秘密の保護をはじめとし、電気通信事業法においても公平なサービスの提供義務等が定められている。

また、「円滑なサービスの提供」のためには、安定的なサービスの提供が不可欠であり、この目的のため、特に、電気通信設備を設置して電気通信サービスを提供する事業者においては、その電気通信設備の安全性・信頼性等を確保するための技術基準に適合することが求められ（第４１条)、設備に関する詳細な技術基準が、事業用電気通信設備規則（昭和６０年郵政省令第３０号）で定められている。

この設備に関する技術基準については、それらへの適合性を事業者自らが確認し、その結果について総務大臣に届出を行なう技術基準適合確認制度が規定され（第４２条)、また、総務大臣は、電気通信設備が技術基準に適合していないと認められるときには、事業者に対し、技術基準に適合するように設備を修理・改造等をすることを命じることができる（第４３条)。

また、事業者は、電気通信設備の管理規程を定め、総務大臣に届け出る旨、規定されているが（第４４条)、それらの管理規程で届け出るべき内容は、電気通信事業法施行規則（昭和６０年郵政省令第２５号）で定められている。

特に、サイバー攻撃に対する対策の規定としては、事業用電気通信設備規則に、ウィルスや DDoS 攻撃、不正アクセス等から設備を防護することを定めた規定（同規則第６条）があり、またネットワーク輻そうに対する対策の規定としては、ネットワーク輻そうを検出して通信の集中を規制する機能等を設備に具備することを定めた規定（同規則第８条）がある。また、事業者の定める管理規程で、事業用電気通信設備の工事、維持及び運用における情報セキュリティ対策に関する事項を定めることとなっている。(電気通信事業法施行規則第２９条)。

また、電気通信事業法は、事業者が、天災、事変その他の非常事態が発生等した場合に、災害の予防や救援、交通、通信等を確保するための重要通信を優先的に取り扱わなければならない旨を定め（事業法第８条)、その重要通信の範囲について電気通信事業法施行規則で定めている（同規則第５５条)。

更に、事業者は、電気通信サービスの一部を停止したとき、又は電気通信業務に関し通信の秘密の漏えいその他の重大事故が生じたときには、その旨を遅滞なく、総務大臣に報告することとなっている（事業法第２８条、施行規則第５７条、第５８条)

（２）　他の法令等

電気通信事業者は、更に、その他の関連する法令等を遵守することにより、安定的なサービスの提供に努めている。それらの既存の法令・ガイドラインのうち、代表的なものを示す。

（ア）　不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）

電気通信事業者のみならず、情報処理設備に対してアクセス制御を行なって外部の利用者等に利用させる場合には、そのアクセス権の適正な管理に努めるとともに、不正アクセス行為を防御するための必要な措置を講ずるよう努める必要がある（第８条）。

（イ）　特定電子メールの送信の適正化等に関する法律（平成１４年法律第２６号）

電子メール通信サービスを提供する電気通信事業者は、その電気通信サービス利用者に対して、特定電子メール等による電子メールの送受信上の支障の防止のためのサービスに関わる情報の提供に努めるとともに、特定電子メールなどによる送受信上の支障の防止のための技術の開発又は導入に努めなければならない（第１０条）。

（ウ）　電気通信事業における個人情報保護に関するガイドライン（平成１６年総務省告示第６９５号）

個人情報保護法（平成１５年法律第５７号）の制定に伴い、電気通信事業における個人情報保護の方針について規定したものであり、発信者情報や位置情報を含む、電気通信事業で扱う個人情報の保護の原則が規定されている。

２．情報通信ネットワーク安全・信頼性基準（昭和６２年郵政省告示第７３号）

電気通信事業者が年々増加し、多数の情報通信ネットワークが運用され、多種多様なサービスが展開される中で、情報通信ネットワークにおける安全・信頼性対策全般にわたる基本的かつ総合的な指標として「情報通信ネットワークにおける安全・信頼性基準」のガイドラインが制定され、活用されている。

このガイドラインは、（１）設備及び設備を設置する環境の基準である設備等基準と、（２）設計・施工及び運用の段階での管理基準とに区分され、定められている。

特に、２００１年の改正で、インターネットへの接続を前提とした情報セキュリティ対策の観点から、ファイアウォールの設置等の設備等基準が規定され、また、情報セキュリティポリシーや危機管理計画の策定をするための指針が新たに追加されている。それ以後の改正においても、モバイルインターネット接続サービスにおける設備等の安全性対策の規定が盛り込まれるようになっている。

また、２００７年５月の情報通信審議会情報通信技術分科会「ネットワークの

IP 化に対応した安全・信頼性対策に関する事項」を踏まえ、設備等基準（60 項目 146 対策 → 64 項目 156 対策）、管理基準（50 項目 73 対策 → 55 項目 87 対策）を見直し、２００８年に公布・施行された。

その後、２０１２年の情報通信審議会の答申を受け、東日本大震災を受けた自然災害対策等の充実・見直しを行い、２０１３年３月に公布・施行されているが、情報セキュリティに関する基準の見直しは含まれていない。

なお、このガイドラインで規定された基準のうち一定の対策が実施されている情報通信ネットワークを登録し公表する制度として「情報通信ネットワーク安全・信頼性対策実施登録規程」（昭和６２年郵政省告示第７４号）が制定されている。

３．電気通信業界におけるガイドライン

（１） 電気通信事業における情報セキュリティマネジメントガイドライン (ISM-TG)

世界規模でのコンピュータウィルスの蔓延や、個人情報の漏えい事案の増加、重要インフラにおける情報システムの障害発生等により、組織における情報セキュリティマネジメントの重要性が高まっている。

この情報セキュリティマネジメントの確立・普及に向け、国際標準化機構（ISO）と国際電気標準会議（IEC）が策定した国際規格（ISO/IEC 27002）があり、これを基に、一般の企業を対象とした汎用的な情報セキュリティマネジメント構築とその適合性評価制度の整備・展開が、各国で進んでいる。

また、国際電気通信連合（ITU）では、我が国が中心となって検討を進め、電気通信事業分野を対象とした情報セキュリティマネジメントの指針が ITU-T X.1051 (07/2004)として２００４年７月に勧告されている。

電気通信分野では、総務省が開催した「次世代ＩＰインフラ研究会」の「第二次報告書」（２００５年公表）において、当分野を対象とした情報セキュリティマネジメント指針の普及促進の必要性が提言され、この提言により検討を進めた結果として、ISO/IEC 27002:2005 及び ITU-T X.1051 (07/2004)に対して、電気通信事業者が遵守すべき要求事項等を盛り込んだ「電気通信事業における情報セキュリティマネジメント指針」（２００６年３月３１日公表）が策定されている。

この指針文書は、ISO/IEC27002:2005 の１１個のセキュリティマネジメント領域に対して必要な管理策を盛り込んでいるが、電気通信事業者として技術的・法的に導入するべき目的、管理策等について、ITU-T X.1051 (07/2004) の項目及び、法令上の要求事項等からくる独自の項目について新たに追加し盛り込んでいる。

「電気通信事業における情報セキュリティマネジメントガイドライン（ISM-TG）」は、上記の指針文書をベースに、電気通信事業者が遵守すべき情報セキュリティマネジメントを実践するための規範を、業界ガイドラインとして策定したものであり、「電気通信分野における情報セキュリティ対策協

議会」にて２００６年６月２９日に決定している。なお、ISM-TG の主管は、２００９年度から「安心・安全インターネット推進協議会」に引き継がれている。一方、ITU-T X.1051 (07/2004)は、改訂の際に、我が国より「電気通信事業における情報セキュリティマネジメント指針」及び ISM-TG の内容が ITU-T に提案され、2008 年 12 月に第２版として ITU-T X.1051 (02/2008)が発行されると共に、ITU-T と ISO/IEC JTC１との連携により ISO/IEC 27011:2008 としても発行されている。

（２） 他のガイドライン

電気通信サービスの安全・信頼性確保のため、電気通信業界では ISM-TG 以外にも各種のガイドラインを自主的に定めている。それらのガイドラインのうち、代表的なものを示す。なお、下記のガイドラインは、特に記載のない限り、一般向けに広く公開されているものである。

（ア） 電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン（第２版）（社団法人日本インターネットプロバイダー協会、社団法人電気通信事業者協会、社団法人テレコムサービス協会、社団法人日本ケーブルテレビ連盟及び財団法人日本データ通信協会 テレコム・アイザック推進会議、２００７年５月策定、２０１１年３月改定）

電気通信事業者が大量通信等（DoS 攻撃等のサイバー攻撃、ワームの伝染及び迷惑メールの大量送信等）を識別しその通信の遮断などの対処を実施するにあたって、電気通信事業法等の関係法令に留意し適法に実施するための参考資料である。

（イ） 帯域制御の運用基準に関するガイドライン（社団法人日本インターネットプロバイダー協会、社団法人電気通信事業者協会、社団法人テレコムサービス協会、社団法人日本ケーブルテレビ連盟及び MVNO 協議会、２００８年５月策定、２０１２年３月改定）

ヘビーユーザによるネットワーク帯域の占有が恒常化すると他の一般ユーザを含めた全体の通信速度の低下が発生する。これを回避して一般ユーザの円滑なネットワーク利用を確保するため、帯域制御を行う場合の合理的範囲についての基本的枠組みと、事業法上の「通信の秘密」及び「利用の公平」の確保との関係について整理している。また、帯域制御を実施する場合の情報開示の在り方についても、基本的な枠組みを提示している。

（ウ） 電気通信サービスにおける事故及び障害発生時の周知・情報提供の方法等に関するガイドライン（第１版）（社団法人電気通信事業者協会、社団法人テレコムサービス協会、社団法人日本インターネットプロバイダー協会及び社団法人日本ケーブルテレビ連盟、２

０１０年２月策定）

電気通信サービスにおける事故及び障害の発生時の周知・情報提供の方法等に関し、利用者及び報道機関にとって分かりやすいものとなるように、電気通信事業者の統一的な対応を促進するために定めたガイドラインである。

（エ） 情報通信審議会答申（H19.5.24）を踏まえた情報セキュリティの確保に関する基本方針並びにネットワークの信頼性に関するガイドライン（第１版）（社団法人電気通信事業者協会　安全・信頼性協議会、２０１０年６月策定）

情報通信審議会答申（平成１９年５月２４日）を受け、電気通信事業者共通の課題に対し、各々の事業者が取り組むべき基本的事項についてとりまとめたものである。

４．セキュリティ評価基準等(ISO/IEC 15408 等)

重要インフラにおける情報システムの障害発生等により、より安全性・信頼性の高い情報システムを構築したいというニーズが高まっている。この目的のために、組織が IT 製品等を調達するにあたり、セキュリティ評価及び認証制度により認証された製品等を優先的に取扱うことが考えられる。

セキュリティ評価及び認証制度とは、IT 製品・システムについて、そのセキュリティ機能や目標とするセキュリティ保証レベルを、第三者が評価し、結果を公的に検証し、公開する制度であり、このための評価基準として ISO/IEC が定めた情報セキュリティ評価の国際標準（ISO/IEC 15408）が、国際的にも国内的にも幅広く利用されている。

ISO/IEC 15408 は、欧米各国・地域でそれぞれ独自に定めていたセキュリティ評価基準を統一化して国際標準化したものであり、１９９９年１２月に ISO/IEC で制定された。

国内においては、ISO/IEC 15408 と同等の規定である JIS X 5070 を策定するとともに、２００１年より、ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度が独立行政法人情報処理推進機構により運用されている。また、２００３年には、国際的なセキュリティ評価及び認定の調整機関である CCRA（Common Criteria Recognition Arrangement）に加盟し、IT 関連製品の本制度に関して、欧米諸国との相互承認を行える体制が確立されている。

電気通信事業においても、これらの IT セキュリティ評価及び認証制度を電気通信機器等の調達仕様書に活用し、あるいは、社内での独自システム開発における情報セキュリティレベルの設定として ISO/IEC 15408 を活用することにより、より安全性・信頼性の高い電気通信設備の構築が可能になると思われる。

また、IT 設備の信頼性向上については、「情報システムの信頼性向上に関するガイドライン第２版」（経済産業省　２００９年３月２４日発表）により情報システ

ムの企画・開発から保守・運用にわたり必要な対策を実施し、あるいは、「システム管理基準」（経済産業省　２００４年１０月８日発表）により、情報システムにまつわるリスクのコントロールを適切に実施することも重要である。

III. 具体的な対策

対象事業者は、自らの責任において情報セキュリティ対策を実効的かつ自主的に取り組むための PDCA サイクルを構築・実行して、継続的に改善していく必要がある。

効果が見えにくい情報セキュリティ対策を推進するためには、対象事業者は、自らの情報セキュリティの状況を把握し、自らの情報セキュリティ対策の基準を定め、適切かつ定期的に、情報セキュリティ対策を実施・改善することが必要である。また、多様な脅威に対応するためには、他の重要インフラ事業者等、政府機関、情報セキュリティ関係機関との連携を充実させることも必要である。

対象事業者の経営層は、以下の必要性を認識し、実施できるようにすることが重要である。

-リスクアセスメントに係る方針、基準

-情報セキュリティ対策実施のための計画策定及び経営資源の確保

-情報セキュリティ対策の運用状況の把握と、運用状況の検証

-教育・訓練等による IT 障害等への対応手順等の検証と、改善策の検証

対象事業者が自らの情報セキュリティ対策の基準として定める電気通信分野における安全基準は、重要インフラとしての電気通信事業における IT 障害に対する具体的な対策として、網羅的かつ高度な情報セキュリティ対策の項目及び水準を定める必要がある。本ガイドラインは、既存の法令・ガイドラインをベースとしながら、それらの基準等では十分規定されていない重点課題である IT 障害の対象脅威に対して、備えるべき情報セキュリティ対策の項目及び水準を明示するものとする。

安全基準として盛り込む具体的な対策が網羅的なものになるよう、本ガイドラインは、次の６つの観点毎に以降の章構成を設け、それぞれの観点で必要となる情報セキュリティ対策の項目及び水準を記述する。

① 組織・体制及び資源の対策（第１章）
② 情報についての対策（第２章）
③ 情報セキュリティ要件の明確化に基づく対策（第３章）
④ 情報システムについての対策（第４章）
⑤ IT 障害の観点から見た事業継続性確保のための対策（第５章）
⑥ 外部委託における情報セキュリティ確保のための対策（第６章）

また、上記観点毎の具体的な情報セキュリティ対策の記述において、全ての脅威に共通して対応すべき一般的対策（共通項目）と、対象脅威毎に固有の情報セキュリティ対策とを区分して、記述するものとする。この対象脅威としては、先に示した（１）サイバー攻撃、（２）ネットワーク輻そう、（３）故障・災害等、（４）重要情報漏えい、の４つとする。

なお、一般的対策（及び対象脅威毎の対策の一部）に含まれるべき項目のうち、「電気通信事業における情報セキュリティマネジメントガイドライン（ISM-TG）」に記載がある内容については、その管理策をそのまま引用し、引用元の ISM-TG

での章番号を括弧書きで示している。該当する管理策についての実施の手引きや、関連情報については、ISM-TG（または ITU-T X.1051）を参照されたい。

本ガイドラインで規定する具体的対策項目の記述構成を表 1 に示す。(各項目欄における**数番号**は、本ガイドラインの第Ⅲ編中における章節を示す。)

表 1　具体的対策の規定項目と本ガイドライン（第Ⅲ編）の構成

	共通 （一般的対策）	サイバー攻撃 （DDoS 攻撃等）	ネットワーク輻そう （企画型輻そう、災害型輻そう）	故障・災害等	重要情報漏えい （設備情報等）
1．組織・体制及び資源の対策	1．（1）共通 （内容）情報セキュリティの基本方針・組織体制・役割	1．（2）サイバー攻撃対策 （内容）情報セキュリティインシデントの管理責任体制	1．（3）ネットワーク輻そう対策 （内容）ネットワーク輻そう対応体制・対応方針	1．（4）故障・災害等対策 （内容）故障・災害等への対応体制・対応方針	1．（5）重要情報漏えい対策 （内容）重要情報管理体制・対応方針
2．情報についての対策	2．（1）共通 （内容）資産に対する責任、情報の分類、媒体の取扱い、情報の交換	2．（2）サイバー攻撃対策 （内容）サーバ等に格納された情報の管理			2．（3）重要情報漏えい対策 （内容）重要情報に対する責任、重要情報の分類、重要情報の内部漏えい・盗難等への対策
3．情報セキュリティ要件の明確化に基づく対策	3．（1）共通 （内容）ネットワークセキュリティ管理、アクセス制御	3．（2）サイバー攻撃対策 （内容）サイバー攻撃に対するネットワーク管理策			3．（3）重要情報漏えい対策 （内容）重要情報漏えいに対するネットワーク管理策
4．情報システムについての対策	4．（1）共通 （内容）情報システム及び設備の対策、監視		4．（2）ネットワーク輻そう対策 （内容）ネットワーク輻そうに対するサービス可用性確保	4．（3）故障・災害等対策 （内容）故障・災害等に対するサービス可用性確保	
5．IT 障害の観点から見た事業継続性確保のための対策	5．（1）共通 （内容）事業継続管理、情報等の管理、障害検知・切分け、緊急時連絡、訓練・演習等	5．（2）サイバー攻撃対策 （内容）サイバー攻撃対応手順、被害拡大措置、復旧	5．（3）ネットワーク輻そう対策 （内容）ネットワーク輻そう対応手順、被害拡大措置	5．（4）故障・災害等対策 （内容）故障・災害等に関する対応手順	5．（5）重要情報漏えい対策 （内容）重要情報漏えい対応手順
6．外部委託における情報セキュリティ確保のための対策	6．（1）共通 （内容）秘密保持、外部組織との連携、第三者提供サービスの管理				6．（2）重要情報漏えい対策 （内容）外部委託先での重要情報の取扱い

１．組織・体制及び資源の対策

（１） 共通

ア 情報セキュリティ基本方針

（ISM-TG 管理策 5.1 [ITU-T X.1051 5.1]参照）

（ア） 情報セキュリティ基本方針文書

（ISM-TG 管理策 5.1.1 [ITU-T X.1051 5.1.1]参照）

（イ） 情報セキュリティ基本方針のレビュー

（ISM-TG 管理策 5.1.2 [ITU-T X.1051 5.1.2]参照）

イ リスクマネジメント

（ア） リスクマネジメントの実施

内部及び外部とのコミュニケーションにより、必要な情報の取得、意見の交換等を行ないつつ、組織の状況を設定する。設定した状況において、発生する可能性のあるリスクの特定、分析、評価を行ない、適切な情報セキュリティ対策を決定する。また、上記プロセスをモニタリング及びレビューし、組織に相応しい情報セキュリティ対策を維持・改善することで、その有効性を高めてゆくことが望ましい。

（「重要情報インフラにおける情報セキュリティ対策の優先順位付けに係る手引書」参照）

ウ 情報セキュリティのための内部組織

（ISM-TG 管理策 6.1 [ITU-T X.1051 6.1]参照）

（ア） 情報セキュリティに対する経営陣の責任

（ISM-TG 管理策 6.1.1 [ITU-T X.1051 6.1.1]参照）

（イ） 情報セキュリティの調整

（ISM-TG 管理策 6.1.2 [ITU-T X.1051 6.1.2]参照）

（ウ） 情報セキュリティ責任の割当て

（ISM-TG 管理策 6.1.3 [ITU-T X.1051 6.1.3]参照）

エ 人的資源のセキュリティ

（ISM-TG 管理策 8.1 [ITU-T X.1051 8.1]参照）

（ア） 役割及び責任

（ISM-TG 管理策 8.1.1 [ITU-T X.1051 8.1.1]参照）

（イ） 雇用条件

（ISM-TG 管理策 8.1.3 [ITU-T X.1051 8.1.3]参照）

（ウ） 経営陣の責任

（ISM-TG 管理策 8.2.1 [ITU-T X.1051 8.2.1]参照）

（エ） 情報セキュリティの意識向上、教育及び訓練

（ISM-TG 管理策 8.2.2 [ITU-T X.1051 8.2.2]参照）

（オ） 情報セキュリティ人材の配置・中長期的な育成等

電気通信サービスを安定的かつ確実に提供するため、情報セキュリティに関する専門的な知識・技能を有する者を配置することが望ましい。

また、そのような人材を配置・育成等するための具体的な計画を策定することが望ましい。例えば、情報セキュリティに関する資格の取得や、業界団体等による研修コースの活用による技術者育成、ITスキル標準等を活用した社内人材育成マップ等の作成とこれに基づく社内教育コースの整備など。

（カ） 懲戒手続

（ISM-TG 管理策 8.2.3 [ITU-T X.1051 8.2.3]参照）

オ 監査の実施

（ア） 情報セキュリティの他者によるレビュー

（ISM-TG 管理策 6.1.8 [ITU-T X.1051 6.1.8]参照）

（イ） 情報システム監査に対する管理策

（ISM-TG 管理策 15.3.1 [ITU-T X.1051 15.3.1]参照）

（ウ） 情報システム監査ツールの保護

（ISM-TG 管理策 15.3.2 [ITU-T X.1051 15.3.2]参照）

カ　役割の分割

（ア）　職務の分割

（ISM-TG 管理策 10.1.3 [ITU-T X.1051 10.1.3]参照）

キ　情報セキュリティ対策の目標

（ア）　サービスレベルの決定

事業者等は、対象とする電気通信サービスについてサービスレベルを定め、その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。具体的な目標を定めた際は、大まかなスケジュール（ロードマップ）、及び詳細化した計画を作成し、情報セキュリティ対策に取り組むことが望ましい。

ここで、サービスレベルは、電気通信事業法施行規則第 58 条の「重大な事故」の基準（第３次行動計画におけるサービス維持レベルに対応）を踏まえ、事故の影響利用者数や継続時間等を考慮して各事業者が内規等で定めることとする。サービスレベルは、各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。

ク　情報セキュリティ確保の取組み状況の公開

（ア）　情報セキュリティ確保の取組み状況の公開

事業者等は、電気通信サービスの提供又は電気通信設備の運用における情報セキュリティ確保の取組み状況に係り、その実施体制や対策状況などを、提供する情報の範囲に留意しつつ、利用者等が容易に知りえる方法によって公表することが望ましい。例えば、情報セキュリティ報告書や、CSR 報告書、各種ディスクロージャ資料等に情報セキュリティ確保の取組状況を盛り込み、ホームページや配布物等により提供するなど。

ケ　IT に係る環境変化に伴う脅威のための対策

（ア）　IT に係る環境変化に伴う脅威のための対策

社会環境や技術環境等の変化に伴って IT 障害を引き起こす新たな脅威が顕在化した際、それらの脅威を要因とする IT 障害によるサービスへの影響等を考慮し、必要に応じて適切な対策を導入することが望ましい。例えば、情報システムの性能向上等による暗号の危殆化や、IPv6 への移行に伴う初期故障や運用ノウハウの不足、普及している技術・プロトコル・ソフトウェア等における脆弱性の顕在化等による影響を評価し、対策を検討するなど。

（２）　サイバー攻撃対策

ア　情報セキュリティインシデントの管理及びその改善

（ISM-TG 管理策 13.2 [ITU-T X.1051 13.2]参照）

（ア）　責任及び手順

（ISM-TG 管理策 13.2.1 [ITU-T X.1051 13.2.1]参照）

（３）　ネットワーク輻そう対策

ア　ネットワーク輻そうの対応体制・対応方針

（ア）　対応責任者の設定、対応方針の策定

電気通信サービスの提供又は電気通信設備の維持・運用に係る組織において、ネットワーク輻そうに対する対応責任者を定めると共に対応方針を策定し、ネットワーク輻そうに対する予防措置および発生時の迅速な対応等に努めることが望ましい。

（４）　故障・災害等対策

ア　故障・災害等に対する緊急対応体制・対応方針

（ア）　故障・災害等に対応する緊急対応体制・計画書の整備

故障・災害等に対応する緊急対応体制・計画書を整備することが望ましい。特に、緊急連絡体制図や故障対応手順を整備し、常に現行化することが望ましい。

また、緊急対応体制・計画書の整備にあたっては、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することが望ましい。

（５）　重要情報漏えい対策

ア　重要情報管理体制・対応方針

（ア）　重要情報管理体制及び方針

重要情報の管理について全社的な管理責任者を定め、重要情報に対する全社的な管理方針を策定することが望ましい。

２．情報についての対策

（１）　共通

ア　資産に対する責任

（ISM-TG 管理策 7.1 [ITU-T X.1051 7.1]参照）

（ア） 資産目録

（ISM-TG 管理策 7.1.1 [ITU-T X.1051 7.1.1]参照）

（イ） 資産の管理責任者

（ISM-TG 管理策 7.1.2 [ITU-T X.1051 7.1.2]参照）

（ウ） 資産利用の許容範囲

（ISM-TG 管理策 7.1.3 [ITU-T X.1051 7.1.3]参照）

イ 情報の分類

（ISM-TG 管理策 7.2 [ITU-T X.1051 7.2]参照）

（ア） 情報分類の指針

（ISM-TG 管理策 7.2.1 [ITU-T X.1051 7.2.1]参照）

（イ） 情報のラベル付け及び取扱い

（ISM-TG 管理策 7.2.2 [ITU-T X.1051 7.2.2]参照）

ウ 媒体の取扱い

(ISM-TG 管理策 10.7 [ITU-T X.1051 10.7]参照)

（ア） 取外し可能な媒体の管理

(ISM-TG 管理策 10.7.1 [ITU-T X.1051 10.7.1]参照)

エ 情報の交換

(ISM-TG 管理策 10.8 [ITU-T X.1051 10.8]参照)

（ア） 情報交換の方針及び手順

(ISM-TG 管理策 10.8.1 [ITU-T X.1051 10.8.1]参照)

（２） サイバー攻撃対策

ア 情報の管理

（ア） サーバ等に格納された情報の管理

外部からアクセス可能なサーバ等に格納された情報について、その利用者に対する利用の許容範囲を定め、適切なアクセス管理を実施することが望ましい。

（３）　重要情報漏えい対策

ア　重要情報に対する責任

（ア）　重要情報管理責任者の設定

各組織における重要情報の管理責任者を組織の長に定めて、重要情報の管理に努めることが望ましい。

（イ）　重要情報の一覧の整備

重要情報の範囲を明確にし、管理すべき重要情報について、重要情報管理責任者の管轄組織毎に保管リストを作成・維持することが望ましい。

イ　重要情報の分類

（ア）　重要情報の格付け（ランク）／取扱いルール

重要情報の全社的な管理方針に基づく情報のランク付けにより、その重要度に応じた取扱いを行なうことが望ましい。具体的な取扱い方法は内規等で定めることが望ましい。例えば、保管場所や持出し手順、開示手続きなど。

ウ　重要情報の盗難、紛失、流出への対策

（ア）　紙資料等の保管ルール

情報に括り付けられたランクの表示方法、及び、ランクに応じた保管ルールとその運用方法について内規等で定めることが望ましい。例えば、施錠可能なキャビネットへの保管、キャビネットの鍵の適切な管理、閲覧等の利用時の管理者の許可、利用履歴の取得、利用履歴の定期的なチェックなど。

（イ）　端末への資料の保管、持出しに関するルールや制限

資料を端末にダウンロードする、又は資料がダウンロードされた端末を持ち出すことがある場合には、端末、及びその設置場所に関して、入室権限者・利用者の制限や持ち出しの制限・承認手続き等を内規等で定めることが望ましい。また、管理情報の重要性によっては、入退記録や、入室者の管理を目的とした常時監視（カメラ）等を導入することが望ましい。

（ウ）　紙資料や可搬電子媒体の持ち出し管理（管理簿等）

重要情報の取り出し・持出し・抽出を行なう際は、その記録と責

任者の承認等のルールについて内規等で定めることが望ましい。

３．情報セキュリティ要件の明確化に基づく対策

（１） 共通

ア ネットワークセキュリティ管理

（ISM-TG 管理策 10.6 [ITU-T X.1051 10.6]参照）

（ア） ネットワーク管理策

（ISM-TG 管理策 10.6.1 [ITU-T X.1051 10.6.1]参照）

（イ） ネットワークサービスのセキュリティ

（ISM-TG 管理策 10.6.2 [ITU-T X.1051 10.6.2]参照）

（ウ） 電気通信サービス提供におけるセキュリティ管理

電気通信事業者は、自らが提供する電気通信サービスのセキュリティレベルを定め、電気通信サービス加入者に対して表明した上で、提供する電気通信サービスを適切に維持管理することが望ましい。

（ISM-TG 管理策 10.6.3 [ITU-T X.1051 A.10.6.3]参照）

（エ） スパムメール対応

電気通信事業者は、電子メールの利用について良好な環境の整備を図るために、スパムメールへの対応方針を定め、対策を実施することが望ましい。

注)「スパムメール」とは、受信者の同意を得ずに送信される広告宣伝メール、架空アドレス宛に送信されるメール又は送信者情報を偽って送信されるメールをいう。（ISM-TG 管理策 10.6.4 [ITU-T X.1051 A.10.6.4]参照）

イ 利用者アクセスの管理

（ISM-TG 管理策 11.2 [ITU-T X.1051 11.2]参照）

（ア） 利用者登録

（ISM-TG 管理策 11.2.1 [ITU-T X.1051 11.2.1]参照）

（イ） 特権管理

（ISM-TG 管理策 11.2.2 [ITU-T X.1051 11.2.2]参照）

（ウ） 利用者パスワードの管理

（ISM-TG 管理策 11.2.3 [ITU-T X.1051 11.2.3]参照）

（エ） 利用者アクセス権のレビュー

（ISM-TG 管理策 11.2.4 [ITU-T X.1051 11.2.4]参照）

ウ　ネットワークのアクセス制御

（ISM-TG 管理策 11.4 [ITU-T X.1051 11.4]参照）

（ア） ネットワークサービスの利用についての方針

（ISM-TG 管理策 11.4.1 [ITU-T X.1051 11.4.1]参照）

（イ） 外部から接続する利用者の認証

（ISM-TG 管理策 11.4.2 [ITU-T X.1051 11.4.2]参照）

（２） サイバー攻撃対策

ア　サイバー攻撃に対するネットワーク管理策

（ア） ネットワークの防護措置

電気通信設備は、電気通信サービス利用者又は他の事業者の電気通信設備から受信したプログラム等により、事業者の意図に反する動作を行うこと等により電気通信サービスの提供に重大な支障を及ぼすことがないよう必要な防護措置を講じること。（事業用電気通信設備規則第６条）

サイバー攻撃（DDoS 攻撃等）から、サーバ、ルータ、その他の IP ネットワーク設備を保護するため、特定の通信が攻撃に使用される場合を想定し、物理又は論理ポートや、IP アドレス、プロトコル毎に、IT 障害を防止するために必要最小限の範囲で通信フィルタリング又は帯域制限ができることが望ましい。サービスによっては、信号処理レベルでの通信制御や、利用者認証、アクセス権限管理等と連動した通信フィルタリング等が実施できることが望ましい。

（イ） 発信者身元偽装対策

IP アドレスの偽装対策を実施することが望ましい。

サイバー攻撃の踏み台として発信者身元偽装に悪用されないため、利用者認証を行うシステムにおいては、パスワードの厳格な管理や、強い認証機能の導入等、不正アクセス対策を徹底することが望ましい。例えば、一定以上の文字長で容易に推測されないパスワード設

定の義務化や、ワンタイムパスワードやハードトークンによる認証の導入が考えられる。

重要通信を扱う電気通信設備は、発信者番号等の偽装を防止する仕組みを導入することが望ましい。例えば、ハードコーティングされた端末 ID、または、設定したパスワードにより、発信者番号等を、登録時および発信要求時にネットワーク側でチェックする機能の導入など。

（ウ） 電気通信サービス利用者等への注意喚起

電気通信サービス利用者等からのサイバー攻撃を抑止や、攻撃発生時に迅速・適切な対応を実施するため、自社設備に過大な負荷を与える通信が発生した場合には利用を制限することがある旨、サービス約款等にて明示することが望ましい。

サイバー攻撃（DDoS 攻撃等）を発生させる等の原因となるウィルス、ボット等について電気通信サービス利用者等に注意喚起を行い、自ら対策をとるように促すことが望ましい。

（エ） セキュリティパッチ等の適用

定期的に、及び必要に応じて随時に、セキュリティパッチ等を適用することにより、サイバー攻撃に利用される恐れがあるソフトウェア等の脆弱性を修復することが望ましい。

セキュリティパッチ等の適用のための具体的運用方法について内規等で定めることが望ましい。例えば、適切なセキュリティパッチを管理するシステムの導入や管理体制の明確化、セキュリティパッチを適用する為のプロセス確立など。

（オ） 設備等に関する脆弱性情報等の迅速な入手

電気通信設備提供者（メーカ等）から、関連する設備の脆弱性やセキュリティパッチ等の情報について迅速に提供を受ける仕組みを、運用保守契約等により構築することが望ましい。

（3） 重要情報漏えい対策

ア 重要情報漏えいに対するネットワーク管理策

（ア） 厳密な利用者認証、アクセス管理、不正アクセス対策

システム利用にあたりアクセス管理を行なうために、利用者の識別・認証等のシステムを導入し、アクセス制限等を実施することが

望ましい。また、利用者のアクセス履歴を記録し、定期的に監査を実施することが望ましい。

（イ） データアクセスに関わるログ取得・保管

重要情報へのアクセスはログ取得・保管を義務付け、その管理方法・運用ルールについて内規等で定めることが望ましい。例えば、取得するログの種類（アクセスログ、エラーログ等)、アクセス主体やアクセス元を特定できる情報の取得(アカウント、IP アドレス等)、重要度に応じた取得タイミングや保管期間の規定など。

（ウ） データ不正アクセスの検知の実施

システム上に格納されている重要情報への不正アクセスを検知するための措置を講じることが望ましい。例えば、システムログを定期的及び必要に応じてチェックする、不正アクセスを検出する機能を導入するなど。

４．情報システムについての対策

（１） 共通

ア セキュリティを保つべき領域

（ISM-TG 管理策 9.1 [ITU-T X.1051 9.1]参照）

（ア） 物理的セキュリティ境界

（ISM-TG 管理策 9.1.1 [ITU-T X.1051 9.1.1]参照）

（イ） 物理的入退管理策

（ISM-TG 管理策 9.1.2 [ITU-T X.1051 9.1.2]参照）

（ウ） 通信センターの物理的な安全確保

電気通信事業を提供するための交換設備等の電気通信設備を収容する施設の物理的なセキュリティを設計し、適用することが望ましい。（ISM-TG 管理策 9.1.7 [ITU-T X.1051 A.9.1.7]参照）

（エ） 電気通信設備室における安全確保

電気通信事業を提供するために電気通信設備が設置された部屋の物理的なセキュリティを設計し、適用することが望ましい。（ISM-TG 管理策 9.1.8 [ITU-T X.1051 A.9.1.8]参照）

（オ） 物理的に隔離された運用区画

電気通信事業を提供するために電気通信設備を設置している物理的に隔離された運用区画の物理的なセキュリティを設計し、適用することが望ましい。（ISM-TG 管理策 9.1.9 [ITU-T X.1051 A.9.1.9] 参照）

イ　装置のセキュリティ

（ISM-TG 管理策 9.2 [ITU-T X.1051 9.2]参照）

（ア） 装置の設置及び保護

（ISM-TG 管理策 9.2.1[ITU-T X.1051 9.2.1]参照）

（イ） サポートユーティリティ

（ISM-TG 管理策 9.2.2[ITU-T X.1051 9.2.2]参照）

（ウ） 装置の安全な処分又は再利用

（ISM-TG 管理策 9.2.6 [ITU-T X.1051 9.2.6]参照）

ウ　自社の管理外の場所に設置する設備のセキュリティ

（ISM-TG 管理策 9.3 [ITU-T X.1051 A.9.3]参照）

（ア） 他の電気通信事業者の領域に設置する設備のセキュリティ

電気通信事業者が他の電気通信事業者の領域に自社の設備を設置する場合には、環境上の脅威及び危険からのリスク並びに権限のないアクセスの可能性を軽減するように保護された場所に設置することが望ましい。（ISM-TG 管理策 9.3.1 [ITU-T X.1051 A.9.3.1]参照）

（イ） 電気通信サービス加入者の領域に設置する設備のセキュリティ

電気通信事業者が、電気通信サービス加入者の電気通信設備と接続するために電気通信サービス加入者の領域に自社の設備を設置する場合には、環境上の脅威及び危険からのリスク並びに権限のないアクセスの可能性を軽減するように自社の設備を保護することが望ましい。（ISM-TG 管理策 9.3.2 [ITU-T X.1051 A.9.3.2]参照）

（ウ） 相互接続における責任分界の明確化

他の電気通信事業者の電気通信設備との相互接続点において、責任分界が明確化され、危険を回避するために容易に切り離せることが望ましい。（ISM-TG 管理策 9.3.3 [ITU-T X.1051 A.9.3.3]参照）

エ　システムの計画作成及び受け入れ

（ISM-TG 管理策 10.3 [ITU-T X.1051 10.3]参照）

（ア） システムの容量・能力の管理

（ISM-TG 管理策 10.3.1 [ITU-T X.1051 10.3.1]参照）

（イ） システムの受け入れ

（ISM-TG 管理策 10.3.2 [ITU-T X.1051 10.3.2]参照）

オ　情報システムのセキュリティ要求事項

（ISM-TG 管理策 12.1 [ITU-T X.1051 12.1]参照）

（ア） セキュリティ要求事項の分析及び仕様化

（ISM-TG 管理策 12.1.1 [ITU-T X.1051 12.1.1]参照）

カ　システムファイルのセキュリティ

（ISM-TG 管理策 12.4 [ITU-T X.1051 12.4]参照）

（ア） 運用ソフトウェアの管理

（ISM-TG 管理策 12.4.1 [ITU-T X.1051 12.4.1]参照）

キ　開発及びサポートプロセスにおけるセキュリティ

（ISM-TG 管理策 12.5 [ITU-T X.1051 12.5]参照）

（ア） 変更管理手順

（ISM-TG 管理策 12.5.1 [ITU-T X.1051 12.5.1]参照）

ク　監視

（ア） 故障検出

電気通信設備は、電源停止、共通制御機器の動作停止等の電気通信サービスの提供に直接係る機能に重大な支障を及ぼす故障等の発生時には、これを直ちに検出し、オペレータ等に通信する機能を備えること。（事業用電気通信設備規則第５条）

故障検出のための具体的運用方法について内規等で定めることが望ましい。例えば、輻そうを検出するための閾値の設定、運用監視センターによる監視体制確立など。

（イ） ルータ、サーバ等の監視機能の導入

ルータやサーバ、その他の IP ネットワーク設備の動作状態を監視するための技術的措置を講ずることが望ましい。例えば、サーバ等

の監視機能、トラフィック監視機能の導入など。

（ウ） 動作ログ・通信トラフィック量ログ等の取得・保管

正当な業務として動作ログや通信トラフィック量ログ等を取得・分析・保管するための具体的運用方法について内規等で定めることが望ましい。例えば、取得するログの種類（アクセスログ、呼種別等）、取得するパラメータ（回線利用率、一定時間あたりパケット数、等）、重要度に応じた取得タイミングや保管期間の規定など。

ケ　暗号の使用

（ア） 暗号方式の選択と鍵管理

電気通信設備または通信を保護するために暗号を使用する場合には、安全な暗号方式を使用することが望ましい。例えば、新規にシステムを構築する、あるいはシステムを更新する際に「電子政府推奨暗号リスト」に記載されている等、安全性が継続的に検証されている暗号方式を採用するなど。

また、暗号で使用する鍵について、改ざん、紛失、及び破壊から保護する、又は秘密にすべき鍵の漏洩を防止する等、適切に管理することが望ましい。

（2） ネットワーク輻そう対策

ア　ネットワーク輻そうに対するサービス可用性確保

（ア） ネットワーク輻そう検出・規制機能

電気通信設備は、ネットワーク輻そうが発生した場合に、これを検出し、かつ、通信の集中を規制する機能等を有すること。（事業用電気通信設備規則第８条）

重要通信を扱う電気通信設備においては、通信規制の実施にあたり、重要通信の疎通に大きな影響がないように配慮することが望ましい。

対象システムの処理の適正・限界値を把握し、限界値に到達する前に要求処理の規制措置を実施することが望ましい。可能であればトラフィックの分散処理を行なうことが望ましい。

（イ） 輻そうを発生させる恐れがある企画等の事前情報収集

輻そうを発生させる恐れがある災害、企画イベントについて事前に情報を得るための運用規定について内規等で定めることが望まし

い。例えば、気象情報・企画イベント情報の取得の体制の確立など。

収集した事前情報について報告体制、手順を定め、関係者に周知徹底することが望ましい。

（ウ） 事前の通信規制措置

企画イベントの規模等を考慮し、必要な範囲・レベルの事前通信規制措置を決定・実行するための具体的運用方法について内規等で定めることが望ましい。

（エ） 一時的な処理量向上のための措置

企画イベントの規模や災害の程度等を考慮し、必要であれば、分散処理センターの利用や、一時的な設備の増強・構成変更等が可能であることが望ましい。

（オ） 重要通信の識別・優先

重要通信を優先的に取り扱うこと。（電気通信事業法第８条、電気通信事業法施行規則第５５条、第５６条）

また、他の事業者と相互接続する場合には、重要通信の優先的な取扱いについての取り決め、及び優先的に取り扱うための措置等を実施すること。（電気通信事業法第８条第３項、電気通信事業法施行規則第５６条の２）

（カ） 故障等の誘発現象に対する事前情報収集

災害、事故、その他の社会現象は電気通信設備の故障あるいは輻そうを誘発する場合が多いため、平時においてもこれらの情報収集とノウハウの蓄積に努め、事前の措置方法の検討を行なうことが望ましい。

（キ） 通信トラフィック量、利用率の定期的観測・分析

通信トラフィック量を収集する具体的運用方法について内規等で定めることが望ましい。例えば、定期的なトラフィック収集、規制時のトラフィック収集等の実施、その分析結果から必要に応じた対策フロー等の確立、分析のための統計指標の策定など。

（ク） 計画的な設備等の増強

定期的な測定結果を分析評価し、ネットワーク性能を適正に保つ

ための具体的運用方法について内規等で定めることが望ましい。例えば、トラフィックの伸び率と予想される需要を考慮して将来のトラフィック予測を行い、それに合わせて設備の増強計画を立てるなど。

（３） 故障・災害等対策

ア 故障・災害等に対するサービス可用性確保

（ア） 予備機器の設置等

アナログ電話用設備等における交換設備及び伝送路設備の機器は、その機能を代替することができる予備機器が設置、配備等され、かつ、故障等の発生時に予備機器に速やかに切り替えが可能であること。（事業用電気通信設備規則第４条第１項、第４条第３項）

故障等が発生した場合に予備機器に速やかに切り替えるための設定交換フロー等について内規等で定めることが望ましい。また、関係者が予備機器への切り替えに習熟するための訓練等を実施することが望ましい。

注）アナログ電話用設備等とは、アナログ電話用設備、総合デジタル通信用設備（音声伝送サービスの提供の用に供するものに限る。以下同じ。）、電気通信番号規則第９条第１項第１号に規定する電気通信番号を用いて電気通信サービスを提供するインターネットプロトコル電話用設備、携帯電話用設備及びＰＨＳ用設備のことをいう。（事業用電気通信設備規則第３条の２）

（イ） 設備等提供メーカでの予備機器等の配備

災害や故障時に必要な設備等の準備や配備に関するルールを、運用保守契約等によって予め締結しておくことが望ましい。

（ウ） 応急復旧機材の配備

アナログ電話用設備等において、電気通信設備の工事、維持又は運用を行なう事業場には、設備の故障等が発生した場合における応急復旧工事、臨時の電気通信回線の設置、電力の供給その他の応急復旧措置を行うために必要な機材の配備又はこれに準ずる措置がなされること。（事業用電気通信設備規則第７条第２項）

また、その他の電気通信設備において、電気通信設備の工事、維持又は運用を行なう事業場には、設備の故障等が発生した場合に電気通信サービスの提供に重大な支障を及ぼすことがないよう、応急

復旧工事、臨時の電気通信回線の設置、電力の供給その他の応急復旧措置を行うために必要な復旧機材の配備又はこれに準ずる措置がなされること。（事業用電気通信設備規則第１６条の３）

（エ） データ等の定常的バックアップ

データ等の定常的バックアップのため、重要なデータ、優先度の高いデータ等を定め、そのレベルに応じたバックアップの具体的方法について内規等で定めることが望ましい。例えば、バックアップ方法（リモート実行等)、バックアップ周期、バックアップメディア交換手順、バックアップデータ保管場所、保管期間、バックアップデータからの回復手順など。また、関係者がバックアップデータからの回復手順に習熟するための訓練等を実施することが望ましい。

（オ） ネットワーク経路の二重化

アナログ電話用設備等における伝送路設備には、予備の電気通信回線を設置すること。また、交換設備相互間を接続する伝送路設備は、複数の経路により設置すること。（事業用電気通信設備規則第４条第２項、第４条第４項）

（カ） オペレーションセンタの分散化・二重化

地理的に異なった複数センターを設置・運営することが望ましい。また、当該センターの被災等に備え、他センターへ代替できる体制を整えておくことが望ましい。

（キ） 通信経路の迂回措置

通常の通信経路において障害が発生し、あるいは通信の疎通に問題があるとみなされる場合に、迂回措置が行なえるような技術的手段を導入することが望ましい。

迂回措置を速やかに行なえるよう、可能であれば、自動で迂回できるような技術的対応策を導入することが望ましい。

５．IT 障害の観点から見た事業継続性確保のための対策

（１） 共通

ア 事業継続管理における情報セキュリティの側面

(ISM-TG 管理策 14.1 [ITU-T X.1051 14.1]参照)

（ア） 事業継続管理手続きへの情報セキュリティの組込み

（ISM-TG 管理策 14.1.1 [ITU-T X.1051 14.1.1]参照）

（イ） 事業継続及びリスクアセスメント

（ISM-TG 管理策 14.1.2 [ITU-T X.1051 14.1.2]参照）

（ウ） 情報セキュリティを組み込んだ事業継続計画の策定及び実施

（ISM-TG 管理策 14.1.3 [ITU-T X.1051 14.1.3]参照）

（エ） 事業継続計画策定の枠組み

（ISM-TG 管理策 14.1.4 [ITU-T X.1051 14.1.4]参照）

（オ） 事業継続計画の試験、維持及び再評価

（ISM-TG 管理策 14.1.5 [ITU-T X.1051 14.1.5]参照）

イ IT 障害に対応するための情報等の管理

（ア） 設備（ハード・ソフト）管理

設備データの構築・更新を確実に実施することが望ましい。社内外への工事情報通知体制・通知内容等について内規で定めておくことが望ましい。

工事の事前事後の正常性確認方法や工事時の障害防止措置等についても明確化しておくことが望ましい。

（イ） 再発防止管理

IT 障害の回復後、類似の障害再発防止ならびに再発時における措置等の改善策の強化を図ることが望ましい。例えば、IT 障害等のデータを原因別、部門別等、統計的に分析し、実施した措置、故障減少施策等の成果測定を行なうなど。

（ウ） 障害情報の管理

障害情報の管理方法、項目等の具体的運用方法について内規等で定めることが望ましい。例えば、サービス種別毎の障害情報をデータベース化し、類似システムの点検等に活用するなど。

ウ　IT 障害の検知と切り分け

（ア）　IT 障害の検知・可視化

アラーム等の送付や監視画面への表示により、IT 障害の検知・表示がリアルタイムに可能な監視ツールを導入することが望ましい。

（イ）　IT 障害（サイバー攻撃、故障等）の切り分け手順等の整備

IT 障害及びその原因となる脆弱性の切り分けについての具体的な手順を内規で定めておくことが望ましい。例えば、設備、機器、サーバ等における具体的な切り分け手順や、切り分けに必要な情報収集手順、報告手順等の明確化など。

エ　緊急時の情報連絡

（ア）　電気通信サービス加入者等からの通報窓口の設定・対応フロー

通報に該当する状況を電気通信サービス加入者及び連携する事業者に明示した上で、通報窓口を設置し、トラブル等の報告があれば、迅速に事実確認を行って対応することが望ましい。

通報がなされた際の、通報窓口から社内等関係部署（復旧および対応を行なう部門等）への連絡経路及び連絡フローについて内規等で定めることが望ましい。

（イ）　IT 障害等情報の社内エスカレーション手順等の整備

IT 障害等に関わる情報の社内エスカレーションについて内規等で定めることが望ましい。例えば、エスカレーションルールの確立や、社内窓口の設定など。同様に、他システムへの影響の調査、事実関係の確認、及び外部委託先との情報共有等についても、内規等で定めることが望ましい。また、関係者がエスカレーションをはじめとする各種手順等に習熟するための訓練等を実施することが望ましい。

（ウ）　IT 障害発生時の監督官庁への連絡や危機管理広報

事業者は、通信の秘密の漏えいや、電気通信サービスの全部または一部の提供を停止させた事故、重要通信の優先を目的としたサービスの停止が発生した場合には、その旨をその理由又は原因とともに、遅滞なく、総務大臣に報告すること。（電気通信事業法第２８条、電気通信事業法施行規則第５７条、第５８条）

その他法令、その他ガイドライン、社会的倫理をふまえて、監督官庁への連絡・危機管理広報を行なう IT 障害のレベルを内規等で定

めることが望ましい。

（エ） IT 障害発生時の電気通信サービス利用者等への周知

IT 障害発生時には、必要に応じて、ホームページ等により、電気通信サービス利用者等に周知することが望ましい。

IT 障害発生時の周知のための具体的運用方法として、周知を行う障害規模の分類、周知を行う体制等について内規等で定めることが望ましい。

オ　IT 障害対応の訓練・演習の計画・実施

（ア） IT 障害に対応する訓練の実施

IT 障害に迅速に対応するため、防災訓練や故障対応リハーサル等を定期的に実施し、人材育成に努めることが望ましい。また、訓練の結果を受け、体制・計画の見直しを必要に応じて実施することが望ましい。

（イ） IT 障害発生演習におけるメーカ等との協調

電気通信事業者が IT 障害発生時の演習をするにあたり、電気通信設備提供者（メーカ等）と協調した原因分析・復旧等のフローの確認等を行うための体制を、運用保守契約等により構築することが望ましい。

（２）　サイバー攻撃対策

ア　サイバー攻撃対応手順等の整備

（ア） 攻撃の危険度等のレベル設定／レベル毎の対策フロー

サイバー攻撃検出後の具体的対策フローについて内規等で定めることが望ましい。例えば、対応の責任体制、レベルの判断基準、レベル毎の対応手順、担当者への周知の徹底など。

（イ） サイバー攻撃への対応手順等の整備

サイバー攻撃に迅速に対応するための具体的運用方法を内規等で定めることが望ましい。例えば、設備、機器、サーバ等の障害切り分け手順の明確化など。

具体的な対応手順の策定にあたっては、検証機を利用した事前シミュレーション等により対応方法を確認した上で、手順書を作成することが望ましい。また、サーバ等の環境設定やセキュリティパッ

チ等で、回避できるサイバー攻撃については、可能な限り事前に対処する事が望ましい。

イ　サイバー攻撃の被害拡大防止措置

（ア）　通信トラフィックの緊急的制御

事業者または第三者の設備に深刻な影響がある場合の応急措置方法を内規等で規定することが望ましい。例えば、一時的なフィルタリングや、攻撃利用回線等を閉塞する対抗手段や、対策フローの確立など。

また、措置の実施にあたり、サービス提供に影響がある場合は、事前に電気通信サービス加入者及び連携する事業者の了解を得るか、何らかの方法で通知がなされることが望ましい。

（イ）　攻撃利用回線の一時停止

設備に深刻な影響がある攻撃に利用された場合の応急措置方法を内規等で規定することが望ましい。例えば、一時的なフィルタリングや、攻撃利用回線等を閉塞する対策手段や対策フローの確立など。

また、措置の実施については事前に電気通信サービス加入者及び連携する事業者の了解を得るか、何らかの方法で通知がなされていることが望ましい。

（ウ）　対象設備の縮退運転／一時停止

サイバー攻撃を受けているサーバ等の設備に深刻な影響がある場合の措置方法を内規等で定めることが望ましい。例えば、該当サーバ等の切り離しによる縮退運転や、回復のための一次停止等の対策フロー確立など。

また、措置の実施については事前に電気通信サービス加入者及び連携する事業者の了解を得るか、何らかの方法で通知がなされていることが望ましい。

（エ）　攻撃元ネットワーク事業者等への攻撃停止要請等

対外窓口を通じた攻撃元ネットワーク事業者あるいは上位 ISP 事業者への直接的な依頼、あるいは関連する事業者団体や連絡会での攻撃停止要請等について内規等で定めることが望ましい。例えば、攻撃停止要請フローや連絡体制の明確化など。

攻撃停止要請にあたっては、攻撃の証拠等を取得し把握しておき、

攻撃元ネットワーク等の管理者等が事実を確認した上で実行することが望ましい。

ウ　サイバー攻撃からの復旧

（ア）　攻撃元の特定／恒久的措置等

原因究明のため、サーバのログ等から攻撃元を特定できるよう環境構築しておくことが望ましい。例えば、ログ等からサイバー攻撃に関するイベント情報を抽出し、発信元 IP アドレス等から攻撃元を割り出すなど。

自網の電気通信サービス利用者が攻撃を繰り返す場合には必要な対応策を実施できることが望ましい。

また、同等の攻撃パターンが繰り返し起こるような場合には、正常な通信を確保するのに必要な限度において、該当の攻撃パターンを識別して遮断等を実施することが望ましい。

（イ）　攻撃元情報の管理

同一の攻撃元がサイバー攻撃等を繰り返すような場合に、事前にサイバー攻撃があることを予測して必要な対応措置が行えるよう、攻撃元情報を管理できるような枠組みを構築することが望ましい。

エ　サイバー攻撃に対する訓練・演習

（ア）　サイバー攻撃等に対する演習

サイバー攻撃を模擬した仮想攻撃の手法等による演習や診断を定期的に実施することが望ましい。

サイバー攻撃演習の際の確認内容や実施方針について内規等で定めることが望ましい。例えば、サイバー攻撃時の一次対応、組織間の協調、復旧までの手順、攻撃元特定の手順など。

（3）　ネットワーク輻そう対策

ア　ネットワーク輻そう対応手順等の整備

（ア）　輻そう発生時対策手順等の整備

企画型・災害等の輻そうに対応するための手順について内規等で定めることが望ましい。例えば、規制手順、規制しきい値、解除のタイミングなど。

イ　ネットワーク輻そうの検知・被害拡大防止措置

（ア）　輻そう状態の通知／発生箇所の特定

サービス内容や輻そうの程度に応じてリアルタイムに輻そう状態をオペレータに通知することが望ましい。通知するアラームやメッセージから、輻そう状態の発生箇所が特定できるようになっていることが望ましい。

輻そう状態の通知、及び、発生箇所の特定のための具体的運用方法について内規等で定めることが望ましい。

（イ）　緊急時の通信規制措置・解除

トラフィックの輻そうが検知された場合は分散・規制等を行い、通信の安定が保てるようにすることが望ましい。また、対応措置が取られ、復旧した場合はその制限の解除を行なうことが望ましい。

輻そう発生時の通信規制措置・解除のフローについて内規等で定めておくことが望ましい。例えば、規制する対象の明確化、解除のタイミング、解除の方法・手順など。

（ウ）　電気通信サービス加入者端末／回線に対する規制・通知

輻そうに対応するための通信規制等の実施にあたり、天災等やむを得ない緊急事態を除き、電気通信サービス加入者及び連携する事業者に事前に通知を行なうことが望ましい。

電気通信サービス加入者了承の上での規制を基本とし、了承が得られない場合においても、他への影響度が深刻である場合に規制を実施することが望ましい（その旨、約款等に定めることが望ましい）。

通信規制等を実施するにあたっての電気通信サービス加入者等への情報提供のための具体的運用方法について内規等で定めることが望ましい。例えば、トーキー案内や放送機関への告知要請、端末メッセージ案内の活用、ホームページ等による周知など。

（エ）　相互接続網に対する制御・通知

他の事業者の電気通信設備を接続する交換設備は、ネットワーク輻そうの発生により他の事業者の電気通信設備に対して重大な支障を及ぼすことのないよう、直ちにネットワーク輻そうの発生を検出し、かつ、通信の集中を規制する機能等を有すること。（事業用電気通信設備規則第２２条）

ネットワーク輻そうの発生により他の事業者に影響を及ぼす恐れ

がある場合は速やかに該当する事業者に連絡し、また、復旧後の連絡についても速やかに実施することが望ましい。

（４） 故障・災害等対策

ア 故障・災害等対応手順書等の整備

（ア） 故障等の発生時に備える対応手順等の整備

対象設備の規模、サービスレベルの低下度合い等により、障害区分を定義して管理することが望ましい。

個々の設備、機器、サーバ等の障害切り分け手順や、本格復旧までの手順等について内規等で定めることが望ましい。

（イ） 装置故障時のメーカ等との連携

電気通信設備提供者（メーカ等）との間で、故障発生時の原因究明・復旧のために必要な情報の共有や連携フローの整備を、運用保守契約等により実施することが望ましい。

（ウ） 災害時の IT 設備に関わる対応・復旧の手順等の整備

災害対策としての設備復旧の対応手順を内規で定めておくことが望ましい。例えば、遠隔地にある待機系システムへの切り替え、重要通信の復旧の優先など。

（エ） 災害対応時のメーカ等との連携

電気通信設備提供者（メーカ等）との間で、災害発生時にサービスを迅速に復旧させるための方策の整備を、運用保守契約等により実施することが望ましい。

（オ） 故障・災害等対応時の外部委託先との連携

故障・災害等発生時にサービスを迅速に復旧させるため、外部委託先の対応作業および要員の優先的な確保等の方策を、外部委託先との契約締結時に盛り込むことが望ましい。

（５） 重要情報漏えい対策

ア 重要情報漏えい対応手順書等の整備

（ア） 重要情報漏えい対応手順書の整備

重要情報の漏えいを検知し、また検知後に対応するための手順について内規等で定めることが望ましい。例えば、漏えいした情報の

範囲の特定、漏えい経路の特定、漏えいした場合のシステム・端末のネットワークからの切り離し、システム・端末の調査など。

イ　重要情報漏えいの被害拡大防止措置

（ア）　漏えいの継続可能性に対する措置

重要情報漏えいの発覚時に、漏えいが継続して起こる危険性があると判断される場合には、対象通信の遮断や、対象サーバ等をネットワークから隔離できるよう、運用フロー等を内規等で定めることが望ましい。

６．外部委託における情報セキュリティ確保のための対策

（１）　共通

ア　秘密保持

（ア）　秘密保持契約

（ISM-TG 管理策 6.1.5 [ITU-T X.1051 6.1.5]参照）

イ　外部組織

（ISM-TG 管理策 6.2 [ITU-T X.1051 6.2]参照）

（ア）　第三者との契約におけるセキュリティ対処

（ISM-TG 管理策 6.2.3 [ITU-T X.1051 6.2.3]参照）

ウ　第三者が提供するサービスの管理

（ISM-TG 管理策 10.2 [ITU-T X.1051 10.2]参照）

（ア）　第三者が提供するサービス

（ISM-TG 管理策 10.2.1 [ITU-T X.1051 10.2.1]参照）

（イ）　第三者が提供するサービスの監視及びレビュー

（ISM-TG 管理策 10.2.2 [ITU-T X.1051 10.2.2]参照）

（ウ）　第三者が提供するサービスの変更に対する管理

（ISM-TG 管理策 10.2.3 [ITU-T X.1051 10.2.3]参照）

（２）　重要情報漏えい対策

ア　外部委託先での重要情報の取扱い

（ア）　外部委託時の重要情報取扱いに関するルール

外部委託先との契約時に、情報管理に関する確認書の提出を内規

等で定めることが望ましい。確認書には、重要情報の取扱いのルールに関する記述及び、そのルールを遵守する旨を盛り込む。また、外部委託にて個人情報を取り扱う場合には、法令に従って適切に取り扱う旨を盛り込む。

Ⅳ. その他の特記事項

１．定期的な見直し

本ガイドラインで規定する安全基準は、電気通信事業の動向の変化、並びに情報セキュリティを取り巻く環境の変化に応じ、随時検討を行ない、必要に応じて見直していくことが必要である。

このため、電気通信事業者等は、所管官庁である総務省と相互に協力し、本ガイドラインの内容が適宜適切なものとなるよう、政府指針の改定時を含め、必要に応じて随時に見直しを行なう。

２．対策チェックシート

本ガイドラインに記載した具体的な情報セキュリティ対策の項目及び水準（第Ⅲ編の内容）について、事業者が、それぞれの対策の実施状況を自ら定期的に点検し、必要に応じて対策の改善（内規の見直し等を含む）を行なうための、対策チェックシートを表 2 に示す。

情報セキュリティ対策の強化に向けた取り組みでは電気通信設備を提供するメーカ等との連携が重要なことから、電気通信事業者及び電気通信設備提供者（メーカ等）の立場において取り組むことが望ましい対策をとりまとめた。

電気通信事業者における本対策チェックシートの適用にあたっては、各事業者の電気通信設備や提供サービスの形態等による固有の情報セキュリティ対策要件がありえること、また、現状想定していない新たな脅威の発生により事業者による対応が求められることがあること、等を考慮し、各事業者の自主的な判断により、対策チェックシート項目以外の必要な対策等を実施することが望ましい。

表 2　対策チェックシート

情報セキュリティ対策確認項目	推奨区分	
	電気通信事業者	メーカ等
1. 組織・体制及び資源の対策		
(1)共通		
情報セキュリティ基本方針文書は、経営陣によって承認され、全従業員および関連する外部関係者に公表し、通知されているか	○	○
情報セキュリティ基本方針は、あらかじめ定められた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当及び有効であることを確実にするためにレビューされているか	○	○
内部及び外部とのコミュニケーションにより、必要な情報の取得、意見の交換等を行ないつつ、組織の状況を設定しているか 設定した状況において、発生する可能性のあるリスクの特定、分析、評価を行ない、適切な情報セキュリティ対策を決定しているか 組織の状況の設定、及び適切な情報セキュリティ対策の決定のプロセスをモニタリング及びレビューし、組織に相応しい情報セキュリティ対策を維持・改善して、その有効性を高めているか	○	○
経営陣は、情報セキュリティの責任に関する明りょうな方向付け、自らの関与の明示、責任の明確な割当て及び承認を通して、組織内におけるセキュリティを積極的に支持しているか	○	○
情報セキュリティ活動は、組織の中の、関連する役割及び職務機能をもつさまざまな部署の代表が調整して行っているか	○	○
すべての情報セキュリティ責任を、明確に定めているか	○	○
従業員、契約相手及び第三者の利用者のセキュリティの役割及び責任を、組織の情報セキュリティ基本方針に従って定め、文書化しているか	○	○
従業員、契約相手及び第三者の利用者は、契約上の義務の一部として、情報セキュリティに関する、これらの者の責任及び組織の責任を記載した雇用契約書に同意し、署名しているか	○	○
経営陣は、組織の確立された方針及び手順に従ったセキュリティの適用を、従業員、契約相手及び第三者の利用者に要求しているか	○	○
組織のすべての従業員、並びに、関係するならば、契約相手及び第三者の利用者は、職務に関連する組織の方針及び手順についての適切な意識向上のための教育・訓練を受け、また、定めに従ってそれを更新しているか	○	○

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		電気通信サービスを安定的かつ確実に提供するため、情報セキュリティに関する専門的な知識・技能を有する者を配置しているか そのような人材を配置・育成等するための具体的な計画を策定しているか	○	○
		セキュリティ違反を犯した従業員に対する正式な懲戒手続を備えているか	○	○
		情報セキュリティ及びその実施のマネジメントに対する組織の取組みについて、あらかじめ計画した間隔で、又はセキュリティの実施に重大な変化が生じた場合に、独立したレビューを実施しているか	○	○
		運用システムの点検を伴う監査要求事項及び活動は、業務プロセスの中断のリスクを最小限に抑えるために、慎重に計画され、合意されているか	○	○
		情報システムを監査するツールの誤用又は悪用を防止するために、それらのツールへのアクセスが抑制されているか	○	○
		組織の資産に対する、認可されていない若しくは意図しない変更又は誤用の危険性を低減するために、職務及び責任範囲が分割されているか	○	○
		対象とする電気通信サービスについてサービスレベルを定め、その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んでいるか 具体的な目標を定めた際は、大まかなスケジュール（ロードマップ）、及び詳細化した計画を作成し、情報セキュリティ対策に取り組んでいるか サービスレベルは、電気通信事業法施行規則第58条の「重大な事故」の基準を踏まえ、事故の影響利用者数や継続時間等を考慮して定めているか サービスレベルは、事業継続計画の目標と乖離しないものとしているか	○	－
		電気通信サービスの提供又は電気通信設備の運用における情報セキュリティ確保の取組み状況に係り、その実施体制や対策状況などを、提供する情報の範囲に留意しつつ、利用者等が容易に知りえる方法によって公表しているか	○	－
		社会環境や技術環境等の変化に伴ってIT障害を引き起こす新たな脅威が顕在化した際、それらの脅威を要因とするIT障害によるサービスへの影響等を考慮し、必要に応じて適切な対策を導入しているか	○	○
	（2）サイバー攻撃対策			
		情報セキュリティインシデントに対する迅速、効果的で整然とした対応を確実にするため、責任体制及び手順を確立しているか	○	○
	（3）ネットワーク輻そう対策			

情報セキュリティ対策確認項目	推奨区分	
	電気通信事業者	メーカ等
電気通信サービスの提供又は電気通信設備の維持・運用に係る組織において、ネットワーク輻そうに対する対応責任者を定めると共に対応方針を策定し、ネットワーク輻そうに対する予防措置および発生時の迅速な対応等に努めているか	○	－
(4)故障・災害等対策		
故障・災害等に対応する緊急対応体制・計画書を整備しているか 緊急対応体制・計画書の整備にあたって、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しているか	○	－
(5)重要情報漏えい対策		
重要情報の管理について全社的な管理責任者を定め、重要情報に対する全社的な管理方針を定めているか	○	○
2. 情報についての対策		
(1)共通		
すべての資産を明確に識別し、また、重要な資産すべての目録を作成し、維持しているか	○	○
情報及び情報処理施設と関連する資産のすべてについて、組織の中に、その管理責任者を指定しているか	○	○
情報及び情報処理施設と関連する資産の利用の許容範囲に関する規則を明確にし、文書化し、実施しているか	○	○
組織に対しての価値、法的要求事項、取扱いに慎重を要する度合い及び重要性の観点から、情報を分類しているか	○	○
組織が採用した分類体系に従って、情報に対するラベル付け及び取扱いに関する適切な一連の手順を策定し、実施しているか	○	○
取外し可能な媒体の管理のための手順を備えているか	○	○
あらゆる形式の通信設備を利用した情報交換を保護するために、正式な交換方針、手順及び管理策を備えているか	○	○
(2)サイバー攻撃対策		
外部からアクセス可能なサーバ等に格納された情報について、その利用者に対する利用の許容範囲を定め、適切なアクセス管理を実施しているか	○	○
(3)重要情報漏えい対策		
各組織における重要情報の管理責任者を組織の長に定めて、重要情報の管理に努めているか	○	○

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		重要情報の範囲を明確にし、管理すべき重要情報について、重要情報管理責任者の管轄組織毎に保管リストを作成・維持しているか	○	○
		重要情報の全社的な管理方針に基づく情報のランク付けにより、その重要度に応じた取扱いを行なっているか 重要情報の具体的な取扱い方法を定めているか	○	○
		情報に括り付けられたランクの表示方法、及び、ランクに応じた保管ルールとその運用方法を定めているか	○	○
		資料を端末にダウンロードする、又は資料がダウンロードされた端末を持ち出すことがある場合には、端末、及びその設置場所に関して、入室権限者・利用者の制限や持ち出しの制限・承認手続き等を定めているか 管理情報の重要性によって、入退記録や、入室者の管理を目的とした常時監視（カメラ）等を導入しているか	○	○
		重要情報の取り出し・持出し・抽出を行なう際の、その記録と責任者の承認等のルールを定めているか	○	○
3. 情報セキュリティ要件の明確化に基づく対策				
	（1）共通			
		ネットワークを脅威から保護するために、また、ネットワークを用いた業務用システム及び業務用ソフトウェア（処理中の情報を含む。）のセキュリティを維持するために、ネットワークを適切に管理し、制御しているか	○	－
		すべてのネットワークサービスについて、セキュリティ特性、サービスレベル及び管理上の要求事項を特定し、また、いかなるネットワークサービス合意書にもこれらを盛り込んでいるか	○	－
		提供する電気通信サービスのセキュリティレベルを定め、電気通信サービス加入者に対して表明した上で、提供する電気通信サービスを適切に維持管理しているか	○	－
		電子メールの利用について良好な環境の整備を図るために、スパムメールへの対応方針を定め、対策を実施しているか	○	－
		すべての情報システム及びサービスへのアクセスを許可及び無効とするために、利用者の登録・登録削除についての正式な手順を備えているか	○	－
		特権の割当て及び利用は、制限し、管理しているか	○	－
		パスワードの割当ては、正式な管理プロセスによって管理しているか	○	－

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		管理者は、正式なプロセスを使用して、利用者のアクセス権を定められた間隔でレビューしているか	○	－
		利用することを特別に認可したサービスへのアクセスだけを、利用者に提供しているか	○	－
		遠隔利用者のアクセスを管理するために、適切な認証方法を利用しているか	○	－
	(2)サイバー攻撃対策			
		電気通信サービス利用者又は他の事業者の電気通信設備から受信したプログラム等により、事業者の意図に反する動作を行なうこと等により電気通信サービスの提供に重大な支障を及ぼすことがないよう、電気通信設備は必要な防護措置を講じているか サイバー攻撃(DDoS 攻撃等)から、サーバ、ルータ、その他の IP ネットワーク設備を保護するため、特定の通信が攻撃に使用される場合を想定し、物理又は論理ポートや、IP アドレス、プロトコル毎に、IT 障害を防止するために必要最小限の範囲で通信フィルタリング又は帯域制御を行なうことを可能としているか サービスによっては、信号処理レベルでの通信制御や、利用者認証、アクセス権限管理等と連動した通信フィルタリング等を行なうことを可能としているか	○	－
		IP アドレスの偽装対策を実施しているか サイバー攻撃の踏み台として発信者身元偽装に悪用されないため、利用者認証を行なうシステムにおいて、パスワードの厳格な管理や、強い認証機能の導入等、不正アクセス対策を徹底しているか 重要通信を扱う電気通信設備は、発信者番号等の偽装を防止する仕組みを導入しているか	○	－
		電気通信サービス利用者等からのサイバー攻撃の抑止や、攻撃発生時の迅速・適切な対応を実施するため、自社設備に過大な負荷を与える通信が発生した場合には利用を制限することがある旨、サービス約款等にて明示しているか サイバー攻撃(DDoS 攻撃等)を発生させる等の原因となるウィルス、ボット等について電気通信サービス利用者等に注意喚起を行い、自ら対策するように促進しているか	○	－
		定期的に、及び必要に応じて随時に、セキュリティパッチ等を適用することにより、サイバー攻撃に利用される恐れがあるソフトウェア等の脆弱性を修復しているか セキュリティパッチ等の適用のための具体的運用方法を定めているか	○	－

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		メーカ等から、関連する設備の脆弱性やセキュリティパッチ等の情報について迅速に提供を受ける仕組みを、運用保守契約等により構築しているか	○	○
	(3)重要情報漏えい対策			
		システム利用にあたりアクセス管理を行うために、利用者の識別・認証等のシステムを導入し、アクセス制限等を実施しているか 利用者のアクセス履歴を記録し、定期的に監査を実施しているか	○	－
		重要情報へのアクセスはログ取得・保管を義務付け、その管理方法・運用ルールを定めているか	○	－
		システム上に格納されている重要情報への不正アクセスを検知するための措置を講じているか	○	－
4. 情報システムについての対策				
	(1)共通			
		情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界(例えば、壁、カード制御による入口、有人の受付)を用いているか	○	－
		セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護されているか	○	－
		電気通信事業を提供するための交換設備等の電気通信設備を収容する施設の物理的なセキュリティを設計し、適用しているか	○	－
		電気通信事業を提供するために電気通信設備が設置された部屋の物理的なセキュリティを設計し、適用しているか	○	－
		電気通信事業を提供するために電気通信設備を設置している物理的に隔離された運用区画の物理的なセキュリティを設計し、適用しているか	○	－
		装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置又は保護されているか	○	－
		装置は、サポートユーティリティの不具合による、停電、その他の故障から保護されているか	○	－
		記憶媒体を内蔵した装置は、処分する前に、取扱いに慎重を要するデータ及びライセンス供与されたソフトウェアを消去していること、又は問題が起きないように上書きしていることを確実にするために、すべてが点検されているか	○	－
		他の電気通信事業者の領域に自社の設備を設置する場合には、環境上の脅威及び危険からのリスク並びに権限のないアクセスの可能性を軽減するように保護された場所に設置しているか	○	－

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		電気通信サービス加入者の電気通信設備と接続するために電気通信サービス加入者の領域に自社の設備を設置する場合には、環境上の脅威及び危険からのリスク並びに権限のないアクセスの可能性を軽減するように自社の設備を保護しているか	○	－
		他の電気通信事業者の電気通信設備との相互接続点において、責任分界が明確化され、危険を回避するために容易に切り離すことを可能としているか	○	－
		要求されたシステム性能を満たすことを確実にするために、資源の利用を監視・調整し、また、将来必要とする容量・能力を予測しているか	○	－
		新しい情報システム及びその改訂版・更新版の受入れ基準を確立し、また、開発中及びその受入れ前に適切なシステム試験を実施しているか	○	－
		新しいシステム又は既存のシステムの改善に関する業務上の要求事項を記述した文書において、セキュリティの管理策についての要求事項を仕様化しているか	○	－
		運用システムにかかわるソフトウェアの導入を管理する手順を備えているか	○	－
		変更の実施は、正式な変更管理手順の使用によって、管理されているか	○	－
		電源停止、共通制御機器の動作停止等の電気通信サービスの提供に直接係る機能に重大な支障を及ぼす故障等の発生時に、これを直ちに検出し、オペレータ等に通信する機能を、電気通信設備が備えているか 故障検出のための具体的運用方法を定めているか	○	－
		ルータやサーバ、その他のIPネットワーク設備の動作状態を監視するための技術的措置を講じているか	○	－
		正当な業務として動作ログや通信トラフィック量ログ等を取得・分析・保管するための具体的運用方法を定めているか	○	－
		電気通信設備または通信を保護するために暗号を使用する場合には、安全な暗号方式を使用しているか 暗号で使用する鍵について、改ざん、紛失、及び破壊から保護する、又は秘密にすべき鍵の漏洩を防止する等、適切に管理しているか	○	○
	(2)ネットワーク輻そう対策			

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		ネットワーク輻そうが発生した場合に、これを検出し、かつ、通信の集中を規制する機能等を、電気通信設備が有しているか 重要通信を扱う電気通信設備においては、通信規制の実施にあたり、重要通信の疎通に大きな影響がないように配慮しているか 対象システムの処理の適正・限界値を把握し、限界値に到達する前に要求処理の規制措置を実施しているか	○	－
		輻そうを発生させる恐れがある災害、企画イベントについて事前に情報を得るための運用規定を定めているか 収集した事前情報について報告体制、手順を定め、関係者に周知徹底しているか	○	－
		企画イベントの規模等を考慮し、必要な範囲・レベルの事前通信規制措置を決定・実行するための具体的運用方法を定めているか	○	－
		企画イベントの規模や災害の程度等を考慮し、必要であれば、分散処理センターの利用や、一時的な設備の増強・構成変更等を行なうことを可能としているか	○	－
		重要通信を優先的に取り扱っているか 他の事業者と相互接続する場合に、重要通信の優先的な取扱いについての取り決め、及び優先的に取り扱うための措置等を実施しているか	○	－
		電気通信設備の故障あるいは輻そうを誘発する可能性がある、災害、事故、その他の社会現象の、平時における情報収集とノウハウの蓄積に努め、事前の措置方法の検討を行っているか	○	－
		通信トラフィック量を収集する具体的運用方法を定めているか	○	－
		定期的な測定結果を分析評価し、ネットワーク性能を適正に保つための具体的運用方法を定めているか	○	－
	（3）故障・災害等対策			
		アナログ電話用設備等における交換設備及び伝送路設備の機器は、その機能を代替することができる予備機器が設置、配備等され、かつ、故障等の発生時に予備機器に速やかに切り替えることを可能としているか 故障等が発生した場合に予備機器に速やかに切り替えるための設定交換フロー等を定めているか 関係者が予備機器への切り替えに習熟するための訓練等を実施しているか	○	－
		災害や故障時に必要な設備等の準備や配備に関するルールを、メーカ等との間で運用保守契約等によって予め締結しているか	○	○

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		アナログ電話用設備等において、電気通信設備の工事、維持又は運用を行なう事業場には、設備の故障等が発生した場合における応急復旧工事、臨時の電気通信回線の設置、電力の供給その他の応急復旧措置を行なうために必要な機材の配備又はこれに準ずる措置がなされているか その他の電気通信設備において、電気通信設備の工事、維持又は運用を行なう事業場には、設備の故障等が発生した場合に電気通信サービスの提供に重大な支障を及ぼすことがないよう、応急復旧工事、臨時の電気通信回線の設置、電力の供給その他の応急復旧措置を行うために必要な復旧機材の配備又はこれに準ずる措置がなされているか	○	－
		データ等の定常的バックアップのため、重要なデータ、優先度の高いデータ等を定め、そのレベルに応じたバックアップの具体的方法を定めているか 関係者がバックアップデータからの回復手順に習熟するための訓練等を実施しているか	○	－
		アナログ電話用設備等における伝送路設備には、予備の電気通信回線が設置されているか 交換設備相互間を接続する伝送路設備が、複数の経路により設置されているか（地形の状況により複数の経路の設置が困難な場合又は伝送路設備の故障等の対策として複数の経路による設置と同等以上の効果を有する措置が講じられる場合を除く）	○	－
		地理的に異なった複数センターを設置・運営しているか 当該センターの被災等に備え、他センターへ代替できる体制を整えているか	○	－
		通常の通信経路において障害が発生し、あるいは通信の疎通に問題があるとみなされる場合に、迂回措置が行えるような技術的手段を導入しているか 迂回措置を速やかに行なえるよう、可能であれば、自動で迂回できるような技術的対応策を導入しているか	○	－
5. IT 障害の観点から見た事業継続性確保のための対策				
	（1）共通			
		組織全体を通じた事業継続のために、組織の事業継続に必要な情報セキュリティの要求事項を取り扱う、管理された手続を、策定し、維持しているか	○	－
		業務プロセスの中断を引き起こし得る事象を、そのような中断の発生確率及び影響、並びに中断が情報セキュリティに及ぼす結果とともに、特定しているか	○	－

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		重要な業務プロセスの中断又は不具合発生の後、運用を維持又は復旧するために、また、要求されたレベル及び時間内での情報の可用性を確実にするために、計画を策定し、実施しているか	○	－
		すべての計画が整合したものになることを確実にするため、情報セキュリティ上の要求事項を矛盾なく取り扱うため、また、試験及び保守の優先順位を特定するために、一つの事業継続計画の枠組みを維持しているか	○	－
		事業継続計画が最新で効果的なものであることを確実にするために、定めに従って試験・更新しているか	○	－
		設備データの構築・更新を確実に実施しているか 社内外への工事情報通知体制・通知内容等について定めているか 工事の事前事後の正常性確認方法や工事時の障害防止措置等について明確化しているか	○	－
		IT 障害の回復後、類似の障害再発防止ならびに再発時における措置等の改善策の強化を図っているか	○	－
		障害情報の管理方法、項目等の具体的運用方法を定めているか	○	－
		アラーム等の送付や監視画面への表示により、IT 障害の検知・表示がリアルタイムに可能な監視ツールを導入しているか	○	－
		IT 障害及びその原因となる脆弱性の切り分けについての具体的な手順を定めているか	○	－
		通報に該当する状況を電気通信サービス加入者及び連携する事業者に明示した上で、通報窓口を設置し、トラブル等の報告があれば、迅速に事実確認を行って対応しているか 通報がなされた際の、通報窓口から社内等関係部署（復旧および対応を行なう部門等）への連絡経路及び連絡フローを定めているか	○	－
		IT 障害等に関わる情報の社内エスカレーションについて定めているか 他システムへの影響の調査、事実関係の確認、及び外部委託先との情報共有等について定めているか 関係者がエスカレーションをはじめとする各種手順等に習熟するための訓練等を実施しているか	○	－

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		通信の秘密の漏えいや、電気通信サービスの全部または一部の提供を停止させた事故、重要通信の優先を目的としたサービスの停止が発生した場合には、その旨をその理由又は原因とともに、遅滞なく、総務大臣に報告しているか その他法令、その他ガイドライン、社会的倫理をふまえて、監督官庁への連絡・危機管理広報を行なうIT障害のレベルを定めているか	○	－
		IT障害発生時には、必要に応じて、ホームページ等により、電気通信サービス利用者等に周知しているか IT障害発生時の周知のための具体的運用方法として、周知を行う障害規模の分類、周知を行う体制等を定めているか	○	－
		IT障害に迅速に対応するため、防災訓練や故障対応リハーサル等を定期的に実施し、人材育成に努めているか 訓練の結果を受け、体制・計画の見直しを必要に応じて実施しているか	○	－
		IT障害発生時の演習をするにあたり、メーカ等と協調した原因分析・復旧等のフローの確認等を行うための体制を、運用保守契約等により構築しているか	○	○
	(2)サイバー攻撃対策			
		サイバー攻撃検出後の具体的対策フローを定めているか	○	－
		サイバー攻撃に迅速に対応するための具体的運用方法を定めているか 具体的な対応手順の策定にあたっては、検証機を利用した事前シミュレーション等により対応方法を確認した上で、手順書を作成しているか サーバ等の環境設定やセキュリティパッチ等で、回避できるサイバー攻撃については、可能な限り事前に対処しているか	○	－
		事業者または第三者の設備に深刻な影響がある場合の、通信トラフィックに対する応急措置方法を定めているか 措置の実施にあたり、サービス提供に影響がある場合は、事前に電気通信サービス加入者及び連携する事業者の了解を得るか、何らかの方法で通知しているか	○	－
		設備に深刻な影響がある攻撃に利用された場合の、攻撃利用回線に対する応急措置方法を規定しているか 措置の実施については事前に電気通信サービス加入者及び連携する事業者の了解を得るか、何らかの方法で通知しているか	○	－

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		サイバー攻撃を受けているサーバ等の設備に深刻な影響がある場合の、対象設備に対する措置方法を定めているか 措置の実施については事前に電気通信サービス加入者及び連携する事業者の了解を得るか、何からの方法で通知しているか	○	－
		対外窓口を通じた攻撃元ネットワーク事業者あるいは上位ISP事業者への直接的な依頼、あるいは関連する事業者団体や連絡会での攻撃停止要請等について定めているか 攻撃停止要請にあたっては、攻撃の証拠等を取得し把握しておき、攻撃元ネットワーク等の管理者等が事実を確認した上で実行しているか	○	－
		原因究明のため、サーバのログ等から攻撃元を特定できるよう環境構築しているか 自網の電気通信サービス利用者が攻撃を繰り返す場合には必要な対応策を実施できるようにしているか 同等の攻撃パターンが繰り返し起こるような場合には、正常な通信を確保するのに必要な限度において、該当の攻撃パターンを識別して遮断等を実施できるようにしているか	○	－
		同一の攻撃元がサイバー攻撃等を繰り返すような場合に、事前にサイバー攻撃があることを予測して必要な対応措置が行えるよう、攻撃元情報を管理できるような枠組みを構築しているか	○	－
		サイバー攻撃を模擬した仮想攻撃の手法等による演習や診断を定期的に実施しているか サイバー攻撃演習の際の確認内容や実施方針を定めているか	○	－
	(3)ネットワーク輻そう対策			
		企画型・災害等の輻そうに対応するための手順を定めているか	○	－
		サービス内容や輻そうの程度に応じてリアルタイムに輻そう状態をオペレータに通知できるようにしているか 通知するアラームやメッセージから、輻そう状態の発生箇所が特定できるようになっているか 輻そう状態の通知、及び、発生箇所の特定のための具体的運用方法を定めているか	○	－

情報セキュリティ対策確認項目		推奨区分	
		電気通信事業者	メーカ等
	トラフィックの輻そうが検知された場合は分散・規制等を行い、通信の安定が保てるようにしているか 対応措置が取られ、復旧した場合はその制限の解除を行なうようにしているか 輻そう発生時の通信規制措置・解除のフローを定めているか	○	－
	輻そうに対応するために電気通信サービス加入者端末／回線に対して通信規制等を実施する場合は、天災等やむを得ない緊急事態を除き、電気通信サービス加入者及び連携する事業者に事前に通知を行っているか 電気通信サービス加入者了承の上での規制を基本とし、了承が得られない場合においても、他への影響度が深刻である場合に規制を実施する旨を、約款等で定めているか 通信規制等を実施するにあたっての電気通信サービス加入者等への情報提供のための具体的運用方法を定めているか	○	－
	他の事業者の電気通信設備を接続する交換設備は、ネットワーク輻そうの発生により他の事業者の電気通信設備に対して重大な支障を及ぼすことのないよう、直ちにネットワーク輻そうの発生を検出し、かつ、通信の集中を規制する機能等を有しているか ネットワーク輻そうの発生により他の事業者に影響を及ぼす恐れがある場合は速やかに該当する事業者に連絡し、また、復旧後の連絡についても速やかに実施しているか	○	－
（4）故障・災害等対策			
	対象設備の規模、サービスレベルの低下度合い等により、障害区分を定義して管理しているか 個々の設備、機器、サーバ等の障害切り分け手順や、本格復旧までの手順等を定めているか	○	－
	メーカ等との間で、故障発生時の原因究明・復旧のために必要な情報の共有や連携フローの整備を、運用保守契約等により実施しているか	○	○
	災害対策としての設備復旧の対応手順を定めているか	○	－
	メーカ等との間で、災害発生時にサービスを迅速に復旧させるための方策の整備を、運用保守契約等により実施しているか	○	○
	故障・災害等発生時にサービスを迅速に復旧させるため、外部委託先の対応作業および要員の優先的な確保等の方策を、外部委託先との契約締結時に盛り込んでいるか	○	○
（5）重要情報漏えい対策			

情報セキュリティ対策確認項目			推奨区分	
			電気通信事業者	メーカ等
		重要情報の漏えいを検知し、また検知後に対応するための手順を定めているか	○	○
		重要情報漏えいの発覚時に、漏えいが継続して起こる危険性があると判断される場合には、対象通信の遮断や、対象サーバ等をネットワークから隔離できるよう、運用フロー等を定めているか	○	○
6. 外部委託における情報セキュリティ確保のための対策				
	(1)共通			
		情報保護に対する組織の必要を反映する秘密保持契約又は守秘義務契約のための要求事項は、特定し、定めに従ってレビューしているか	○	○
		組織の情報若しくは情報処理施設が関係するアクセス・処理・通信・管理にかかわる第三者との契約、又は情報処理施設に製品・サービスを追加する第三者との契約は、関連するすべてのセキュリティ要求事項を取り上げているか	○	○
		第三者が提供するサービスに関する合意に含まれる、セキュリティ管理策、サービスの定義及び提供サービスレベルが、第三者によって実施、運用及び維持されることを確実にしているか	○	○
		第三者が提供するサービス、報告及び記録は、常に監視し、レビューしているか それらについて定期的な監査を実施しているか	○	○
		第三者が提供するサービスの変更(情報セキュリティ方針、手順及び管理策の保守・改善を含む)は、関連する業務システム及び業務プロセスの重要性、並びにリスクの再評価を考慮して管理されているか	○	○
	(2)重要情報漏えい対策			
		外部委託先との契約時に、情報管理に関する確認書を提出させることを定めているか 確認書には、重要情報の取扱いのルールに関する記述及び、そのルールを遵守する旨を盛り込んでいるか 外部委託にて個人情報を取り扱う場合には、法令に従って適切に取り扱う旨を盛り込んでいるか	○	○

注：推奨区分の欄中、「○」及び「－」は、それぞれ次のことを示す。

○：実施が望ましい

－：参考