電気通信分野における
サイバーセキュリティに係る
安全基準（第１版）

安全・信頼性協議会

令和５年８月 31 日

目次

変更履歴

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

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
改訂　第4版　　平成30年10月1日
改訂　第4.1版　令和2年3月16日
改訂　第4.2版　令和3年12月10日

電気通信分野におけるサイバーセキュリティに係る安全基準

（令和5年8月31日「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」より改題及び改定）

制定　第1版　　令和5年8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重要インフラサービス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、事業者が重要インフラサービス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、重要インフラサービス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。その防護に当たっては、「重要インフラのサイバーセキュリティに係る行動計画」に記載された「任務保証の考え方」を踏まえ、サービスの提供に必要な情報システムのセキュリティを確保し、サイバー攻撃等による重要インフラサービス障害等の発生を可能な限り減らすとともに、障害等が発生した際の早期検知や、迅速な復旧を図ることが重要となる。

このため、重要インフラ分野において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、情報セキュリティ戦略本部（議長：内閣官房長官）において「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（以下、政府指針）が決定されている。（平成１８年２月初版決定、令和5年7月4日「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指針」から改題および改定）

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。

なお、「重要インフラの情報セキュリティ対策に係る第４次行動計画」は令和４年６月１７日に「重要インフラのサイバーセキュリティに係る行動計画」に改題され、「第４次行動計画」を踏襲しつつ全面改訂された。本改訂に伴い、経営層 の内部統制システム構築義務には、適切なサイバーセキュリティを講じる義務が含まれる。

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

リスクを修正する対策（リスクを修正するためのあらゆるプロセス、方針、仕掛け、実務及びその他の処置を含む。）(ISO/IEC 27000:2018)

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）

あらゆる情報処理のシステム、サービス若しくは基盤、又はこれらを収納する物理的場所。(ISO/IEC 27000:2018)

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、信頼性などの特性を維持することを含めることもある。(ISO/IEC 27000:2018)

カ 情報セキュリティ事象

情報セキュリティ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し得る未知の状況を示す、システム、サービス又

はネットワークの状態に関連する事象。(ISO/IEC 27000: 2018)

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: 2018)

ク　方針

トップマネジメントによって正式に表明された組織の意図及び方向付け。(ISO/IEC 27000: 2018)

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望ましくないインシデントの潜在的な原因。(ISO/IEC 27000: 2018)

ツ　ぜい弱性

一つ以上の脅威によってつけ込まれる可能性がある、資産又は管理策の弱点。(ISO/IEC 27000: 2018)

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。

ト　CSIRT

コンピュータセキュリティインシデントへの対応、対策活動を行なっている組織（チーム）のこと。（日本シーサート協議会　運営規約　平成29年3月22日改定）

（2）　重要インフラに関する用語及び定義（「重要インフラのサイバーセキュリティに係る行動計画（2022年6月17日　サイバーセキュリティ戦略本部）」より）

ア　サイバーセキュリティ

サイバーセキュリティ基本法第 2 条に規定するサイバーセキュリティをいう。電磁的方式による情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること。

イ　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って、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、重要インフラ分野に属するもの。

ウ　重要インフラ分野

重要インフラについて業種ごとに指定する分野であり、具体的には、「情報通信」、「金融」、「航空」、「空港」、「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 14 分野。

エ　重要インフラ事業者

サイバーセキュリティ基本法第 3 条第 1 項に規定する重要社会基盤事業者をいう。国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者。具体的には、重要インフラ分野に属する事業を行う者のうち、「重要インフラのサイバーセキュリティに係る行動計画（2022 年 6 月 17 日　サイバーセキュリティ戦略本部）」「別紙1　対象となる重要インフラ事業者等と重要システム例」の「対象となる重要インフラ事業者等」欄において指定するもの（地方公共団体を除く）。

オ　重要インフラ事業者等

サイバーセキュリティ基本法第 12 条第 2 項第 3 号に規定する重要社会基盤事業者等をいう。重要インフラ事業者及びその組織する団体並

びに地方公共団体。

カ　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定めるもの。

キ　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。

ク　重要インフラサービス障害

システムの不具合により、重要インフラサービスの安全かつ持続的な提供に支障が生じること。

ケ　システムの不具合

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。

コ　サービス維持レベル

任務保証の考え方に基づき、重要インフラサービスが安全かつ持続的に提供されていると判断するための水準のこと。

サ　機能保証の考え方

重要インフラサービスは、それ自体が国民生活及び社会経済活動を支える基盤となっており、その提供に支障が生じると国民の安全・安心に直接的かつ深刻な負の影響が生じる可能性がある。このため、各関係主体は、重要インフラサービスを安全かつ持続的に提供するための取組（機能保証）が求められる。

なお、本行動計画において、「機能保証」とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。すなわち、各関係主体が重要インフラ防護の目的を果たすために、情報セキュリティ対策に関する必要な努力を適切に払うことを求める考え方である。

なお、「重要インフラのサイバーセキュリティに係る行動計画」では「機能保証」の記載が削除された。

シ　任務保証の考え方

サイバーセキュリティ戦略（令和 3 年 9 月 28 日閣議決定）において示す、「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、

その安全かつ持続的な提供に関する責任を全うするという考え方。

ス　ＯＴ

情報通信技術（ＩＴ）を利用した制御システム等の運用技術のこと。

セ　サイバー攻撃リスク

サイバー攻撃に起因して事業に生じ得るリスク。

ソ　関係主体

内閣官房、重要インフラ所管省庁、サイバーセキュリティ関係省庁、事案対処省庁、防災関係府省庁、重要インフラ事業者等、セプター及びセプター事務局、セプターカウンシル、サイバーセキュリティ関係機関並びにサイバー空間関連事業者。なお、重要インフラ防護に関係する主体に対して、サイバーセキュリティ基本法における責務が規定されている。

タ　セプター

重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織。

Capability for Engineering of Protection, Technical Operation, Analysis and Response の略称(CEPTOAR)。

チ　セプターカウンシル

各重要インフラ分野で整備されたセプターの代表で構成される協議会で、セプター間の情報共有等を行う。政府機関を含め他の機関の下位に位置付けられるものではなく独立した会議体。

（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３条第７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３条第８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解説３－７－１第三者提供の制限の原則（第１７条第１項関係）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３８条参照）

ス　個人情報

生存する個人に関する情報であって、以下のいずれかに該当するものをいう。

① 当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。）で作られる記録をいう。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（個人識別符号を除く。）をいう。以下同じ。）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。）

（個人情報の保護に関する法律第２条第１項）

② 個人識別符号が含まれるもの。個人識別符号とは、以下のいずれか

に該当するものをいう。

i) 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの

ii) 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され､若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

（個人情報の保護に関する法律第２条第２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。

ソ　特定利用者情報

電気通信役務に関して取得する利用者に関する情報であって、①通信の秘密に該当する情報または②利用者を識別することができる情報であって総務省令で定めるもの。

（４）　クラウドに関する用語定義

ア　クラウドサービス

定義されたインタフェースを使って呼び出されるクラウドコンピューティング経由で提供される一つ以上の能力。（ISO/IEC 17788:2014（JIS X 22123-1:2022））

事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

（政府機関等のサイバーセキュリティ対策のための統一基準（令和３年度版））

（政府情報システムのためのセキュリティ評価制度（ISMAP）基本規程）

イ　クラウドコンピューティング

セルフサービスのプロビジョニング（provisioning）及びオンデマンド管理を備える、スケーラブルで伸縮自在な共有できる物理的又は仮想的

なリソース共用へのネットワークアクセスを可能にするパラダイム。

注記　リソースの例には、サーバ、OS、ネットワーク、ソフトウェア、アプリケーション及びストレージが含まれる。（ISO/IEC 17788:2014（JIS X 22123-1:2022））

ウ　クラウドサービスプロバイダ

クラウドサービスを利用できるようにするパーティ。（ISO/IEC 17788:2014（JIS X 22123-1:2022））

エ　クラウドサービスカスタマ

クラウドサービスを使うためにビジネス関係にあるパーティ。（ISO/IEC 17788:2014（JIS X 22123-1:2022））

（５）　「政府機関等のサイバーセキュリティ対策のための統一基準（令和３年度版）」で定義される特に重要な用語

ア　暗号化消去

「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。

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

「任務保証の考え方」を踏まえ、サービスの提供に必要な情報システムのセキュリティを確保し、サイバー攻撃等による重要インフラサービス障害等の発生を可能な限り減らすことが重要である。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、サービスの安全かつ持続的な提供への影響が大きいと思われる脅威を以下に示す。

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。

なお参考として以下にサイバー攻撃リスクの７つの特性を示す。「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指針（第５版）改定版【別紙３】を参考に、手順を策定することが望ましい。

（ア） 攻撃者の存在と多様な攻撃目的

サイバー攻撃は、自然災害等とは異なり、目的を持った攻撃者によって引き起こされる。その攻撃目的は、金銭・情報の窃取、主義・主張の表明、システム破壊によるサービスの停止等多様化している。組織的に計画されて行われる攻撃から内部犯行による攻撃まで、多様な攻撃者・攻撃目的に応じた様々な手法による攻撃が考えられるが、事前に攻撃者や攻撃目的を知ることは困難なケースが多い。

（イ） 攻撃手口の高度化

サイバー攻撃の手口は絶えず考え出され高度化している。新たな脆弱性を狙った攻撃のように現行技術をベースとした対策だけでは回避困難な攻撃や、事業者側が想定していない新しい手口で行われる攻撃等が考えられる。

また、新しい手口で攻撃が行われた場合、その影響の度合や範囲を正確に把握できない可能性がある。

（ウ） 急激な被害拡大に繋がる攻撃が行われる可能性

サイバー攻撃の被害は、攻撃を受けた箇所を起点にネットワークを介して急速に拡大する可能性がある。特定の端末に感染したマルウェアが同一組織内のネットワーク上にある別の端末に自身を複製することで被害が広がるケースや、外部委託先で発生したサイバー攻撃の被害が自社システムにまで広がるケース、自社システムが不正に操作され、他社への攻撃に利用されることで自らが加害者の立場になってしまうケースも考えられる。

（エ） 執拗な攻撃が行われる可能性

サイバー攻撃は、その目的が達成されるまで執拗に行われる可能性がある。システ復旧の際、被害に遭う以前の状態に漫然と戻した場合にまた同じ攻撃が行われ被害を受けるケースや、システム復旧対応中に再度攻撃が行われるケース、攻撃への対処後にそれを回避する方法で再度攻撃が行われるケースも考えられる。

また、インターネットに接続していないクローズド環境や、汎用性の低いシステムで構成される環境であっても、システム構成やシステム仕様等に関する情報を様々な手段で時間をかけて収集した上で攻撃が行われるケースも考えられる。

（オ） 同時多発的な攻撃が行われる可能性

サイバー攻撃では物理的な距離に関係なく、広範囲にわたるターゲットを同時に攻撃することが可能である。自組織の複数の拠点に同時に攻撃が行われるケースや、自組織のシステムとサプライヤーのシステムに同時に攻撃が行われるケース、メインシステムと非常用システムに同時に攻撃が行われるケース等が考えられる。

（カ） 検知が困難な攻撃が行われる可能性

サイバー攻撃に対して十分な検知策を講じていない場合、攻撃を認識できず長期間にわたり攻撃を受け続ける可能性がある。不正行為の検知に繋がるログを削除して回避しようとするケースや、実態とは異なる数値を表示して正常に動作しているように見せかけ不正行為を行うケース等も存在し、検知が遅れるほど被害が拡大する可能性が高くなる。また、攻撃を検知した以降も、攻撃者及び攻撃目的を特定するのは困難なケースが多い。

（キ） 誤った判断や対処を誘発する攻撃が行われる可能性

サイバー攻撃によって、誤った判断や対処が誘発される可能性がある。例として、監視や制御等に使用する管理システムに実態と異なるアラートや数値を表示して判断を誤らせるケースや、障害対応

時にシステム操作が意図しない動作を引き起こすようにシステムを不正変更（数値を上げる操作で数値が下がる、システム停止の操作でシステムが停止しない等）するケース等が考えられる。

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、既存の法令や国が定めるガイドライン等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や国が定めるガイドライン等を電気通信分野の「安全基準等」として遵守する。他の業界団体等が定める、または他の分野に関するガイドライン等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）。なお、同施行規則を適宜改正し、仮想化の進展、IoT 機器を通じた攻撃の増加など、技術の変化に対応するようにしている。特に近年の IoT 機器を悪用したサイバー攻撃については、NICT と連携し、パスワ

ード設定等に不備のある機器の利用者に注意喚起することを定めた規定（電気通信事業法第 116 条の 2）も定められた。

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)

なお、令和５年の改正法施行において、総務大臣が指定した電気通信事業者は、情報管理規程等の作成・評価・必要時の改正等の実施や、情報送信指令通信（Cookie）に関する送信情報等の開示が義務づけられた。

（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２９年総務省告示第１５２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。

（エ） 外国の個人情報保護に関する法律・ガイドライン等

電気通信事業が、外国の利用者の個人情報または外国から移転された個人情報を扱う場合、当該国・地域の法律・ガイドライン等が適用される可能性がある。そのため、適用されうる法律・ガイドライン等を調査・確認し、必要な手続、措置を行う必要がある。

代表的な例として、EU 域においては、一般データ保護規則（General Data Protection Regulation: GDPR）(規則 2016/679)が定められている。日本個人情報保護委員会は、2016 年 4 月以降、欧州委員会と、日本と EU 域間における相互の円滑な個人データ移転を図る枠組みの構築について交渉を重ね、2019 年 1 月 23 日を以って、日本個人情報保護委員会及び欧州委員会において、お互いの十分性認定を発効することを決定した。また同日、日本個人情報保護委員会は、EU 域から移転された個人データの扱いについて「個人情報の保護に関する法律に係る EU 域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」を施行した。これにより、上記補完ルールを順守することによって、日本の個人情報取扱事業者は、EU 域から移転された個人データを安全かつ円滑に取り扱えることとなった。

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。

さらに、「令和元年房総半島台風」を受けた停電対策等の充実を図る改訂が実施

されたが、この改訂による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３版）（一般社団法人日本インターネットプロバイダー協会、一般社団法人電気通信事業者協会、一般社団法人テレコムサービス協会、一般社団法人日本ケーブルテレビ連盟及び一般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、２０１４年７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（一般社団法人日本インターネットプロバイダー協会、一般社団法人電気通信事業者協会、一般社団法人テレコムサービス協会、一般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、２０１９年１２月改定）

本ガイドラインは、ネットワークの品質を確保するために実施する帯域制御に関して５種類の制御方法について整理している。また、これにより一般ユーザの円滑なネットワーク利用を確保し、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、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３版）（一般社団法人電気通信事業者協会、一般社団法人テレコムサービス協会、一般社団法人日本インターネットプロバイダー協会及び一般社団法人日本ケーブルテレビ連盟、２０１０年２月策定、２０２０年３月改訂）

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）（一般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、「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。

５．分野別のセキュリティガイドライン

（１）　クラウドセキュリティ

① 国内外のガイドラインと認証制度等

近年の傾向として、サービス・事業分野別にさまざまなガイドラインが策定され、分野固有のリスクを想定したセキュリティ対策が重視されている。

特に、クラウドサービスにおいて、その普及に伴い、従来の情報システム、情報通信サービスにはないリスクの存在と対応の必要性が議論され、クラウドサービスの情報セキュリティ規格として、国内においては、クラウドサービス提供における情報セキュリティ対策ガイドライン（総務省　2014 年 4 月策定)、クラウド情報セキュリティ管理基準（経済産業省　2012 年 8 月策定）が策定され、国際標準規格として、ISO/IEC 27017:2015 が策定された。なお、クラウド情報セキュリティ管理基準をもとにクラウド情報セキュリティ監査制度（CS マーク)、ISO/IEC 27017 をもとに ISMS クラウドセキュリティ認証制度が運用されており、その取得が要件等とされていることも増えている。

電気通信事業者においても、電気通信サービスをクラウドサービスとして提供する可能性が高くなっており、上記ガイドライン、規格等を参考に、クラウド固有のリスクを想定した管理策を実施することも重要である。

② クラウドサービスの安全性評価制度

政府でも 2018 年 6 月に「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018 年 6 月 7 日 CIO 連絡会議決定）を定め、クラウド・バイ・デフォルト原則を掲げ、クラウドサービスの導入を推進している。反面クラウドサービス特有のリスクに起因するセキュリティへの懸念等も存在しており、「未来投資戦略 2018」（2018 年 6 月 15 日閣議決定）において、クラウドサービスの安全性評価について検討を開始することとした。これを受け、経済産業省と総務省が、2018 年 8 月より「クラウドサービスの安全性評価に関する検討会」を開催し、クラウドサービスの安全性評価制度を、2020 年秋に政府機関等が利用を開始できるよう準備を進め、予定通り 2020 年 10 月より 1 回目のクラウドサービス事業者登録申請が開始され、「ISMAP」として制度運用が開始された。

本制度は、政府調達の候補となるクラウドサービスをセキュリティの観点から選定するため、クラウドサービスに対して要求するべき基本的な情報セキュリティ管理・運用の要求事項（管理基準）を定め、その上で、情報セキュリティ監査の枠組みを活用し、独立した第三者が政府の定める基準・手続きに従って監査した結果に基づき、要求事項を満たしていると評価したクラウドサービスを登録する制度である。

ISMAP の制度運用が開始された以降は、政府機関等にクラウドサービスを提供する事業者は、本制度への対応が必要である。また、本制度は、政府調達における利用を第一に想定しているものの、制度運用が本格化した際には、重要産業分野等をはじめとした民間においても活用することを前提としている。左記に伴い、将来的には、電気通信事業者内で、クラウドサービスを開発、利用等する場合においても、本制度に対応する可能性があるため、当該

制度の動向については今後、留意する必要がある。

2022 年 11 月より、セキュリティ上のリスクの小さな業務・情報の処理に用いる SaaS サービス向けに、ISMAP-LIU 制度が開始された。

III. 具体的な対策

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重要インフラサービス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重要インフラサービス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１０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 組織統治におけるサイバーセキュリティ対策
② リスクマネジメントの活用と危機管理対策
③ 組織的対策
④ 人的対策
⑤ 物理的対策
⑥ 技術的対策
⑦ クラウドサービスのセキュリティ対策
⑧ ランサムウェア対策
⑨ 重要インフラサービス障害の観点から見た事業継続性確保のための対策
⑩ 外部委託における情報セキュリティ確保のための対策

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、「ISO/IEC 27002:2022 情報セキュリティ、サイバーセキュリティ及びプライバシー保護 － 情報セキュリティ管理策」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 ISO/IEC 27002 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、ISO/IEC 27002（または ITU-T X.1051）を参照されたい。

また、電気通信サービスをクラウドサービスとして提供する際の対策に含まれるべき項目の内、「ISO/IEC 27017:2015 情報技術 ― セキュリティ技術 ― ISO/IEC 27002 に基づくクラウドサービスのための情報セキュリティ管理策の実践のための規範」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 ISO/IEC 27017 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、ISO/IEC 27017 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）	クラウドサービスの対策
1．組織統治におけるサイバーセキュリティ対策		1．（1）サイバー攻撃対策				
2．リスクマネジメントの活用と危機管理対策	2．（1）共通					
3．組織的対策	3．（1）共通	3．（2）サイバー攻撃対策	3．（3）ネットワーク輻そう対策	3．（4）故障・災害等対策	3．（5）重要情報漏えい対策	
4．人的対策	4．（1）共通					
5．物理的対策	5．（1）共通			5．（2）故障・災害等対策		
6．技術的対策	6．（1）共通	6．（2）サイバー攻撃対策	6．（3）ネットワーク輻そう対策		6．（4）重要情報漏えい対策	
7．クラウドサービスのセキュリティ対策						7．（1）クラウドサービス利用時の対策 7．（2）クラウドサービス提供時の対策
8．ランサムウェア対策	8．（1）共通					
9．重要インフラサービス障害の観点から見た事業継続性確保のための対策	9．（1）共通	9．（2）サイバー攻撃対策	9．（3）ネットワーク輻そう対策	9．（4）故障・災害等対策	9．（5）重要情報漏えい対策	
10．外部委託における情報セキュリティ確保のための対策	10．（1）共通				10．（2）重要情報漏えい対策	

１．組織統治におけるサイバーセキュリティ対策

重要インフラのサイバーセキュリティの確保には、任務保証の観点から取り組むべきである。任務保証とは、サイバーセキュリティ戦略（令和 3 年 9 月 28 日閣議決定）において示す、「企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保すること。サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービス を見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方」である。

重要インフラサービスの安全かつ持続的な提供を不確かなものとするリスクを許容水準まで低減することは、 重要インフラ事業者等として果たすべき社会的責任であり、その実践は経営層としての責務である。 重要インフラサービスの安全かつ持続的な提供に あたり、サイバーセキュリティの確保が不可欠で あることを念頭に、既存の組織統治[1] の取組（組織方針、体制構築、監査、情報開示等）においてサイバーセキュリティも扱うべく、次に掲げる項目を安全基準等に規定することが望まれる。[2]

（１） サイバー攻撃対策

ア 組織方針

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 3.1 参照）

（ア） 組織方針とサイバーセキュリティ

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 3.1.1 参照）

組織方針（経営方針、リスクマネジメント方針等 にあたる文書に、重要インフラのサイバーセキュリティ確保に関する事項も組み入れる。例えば、「重要インフラサー ビスの 安全かつ持続的な提供を実現する」「サイバーセキュリティに対する脅威からの被害がサービス提供を阻害するリスクの一つである」「リスクマネジメントの対象と

---

[1] 安全基準等策定指針では、組織統治とは、「組織の活動やその経営者・理事等の行動を規律する仕組み」及び「組織の不正を防止し、組織の財務の健全性および組織の競争力・持続可能性を高めるための仕組み」を意味する。なお、コーポレートガバナンス・コード（ 2021 年 6 月 11 日株式会社東京証券取引所）におけるコーポレートガバナンスの定義「会社が、株主をはじめ顧客・従業員・地域社会等の立場を踏まえた上で、透明・公正かつ迅速・果断な意思決定を行うための仕組み」や、会社法（平成 17 年法律第 86 号）の求める内部統制システム「会社が営む事業の規模、特性等に応じたリスク管理体制」の構築も念頭に置かれるべきである。

[2] 経済産業省「サ イバーセキュリティ経営ガイドライン」、内閣サイバーセキュリティセンター（以下「 NISC 」という。）「サイバーセキュリティ関係法令 Q&A ハンドブック」が参考になる。

してサイバーセキュリティに関する事項を含める」といった要素を盛り込み、また、あわせて維持するサービス範囲・水準を示すことが望ましい。

（イ） サイバーセキュリティ方針

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 3.1.2 参照）

組織方針を踏まえ、次が記載されたサイバーセキュリティ方針を策定する。

- セキュリティ対策の目的や方向性
- 関係主体等からの要求事項への対応
- 経営層によるコミットメント

イ 組織内外のコミュニケーション

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 3.2 参照）

組織内外のコミュニケーションにおいて、サイバーセキュリティリスク、インシデント等の情報を取り扱う。

組織内のガバナンスや内部統制、その他のリスクマネジメントにおけるコミュニケーションの一部として、サイバーセキュリティに関する環境変化、インシデントの発生状況・得られた教訓、セキュリティ対策の実施状況・有効性評価等に関し、経営層と担当者層との間で定期的な対話の機会等を設ける 。

セキュリティ・バイ・デザインを共通の価値として認識し、製品・サービス企画時等の内部協議プロセスの関係者にサイバーセキュリティを担当する部署を加えることが望ましい。

組織内外の関係者間でサイバーセキュリティに関する役割、責任分担、情報共有の体制等について意見交換を行うことが望ましい。

ウ 経営リスクとしての サイバーセキュリティリスクの管理

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 3.3 参照）

組織全体[3] のリスクマネジメントの一部として、サイバーセキュリティリスク及びそれが事業運営に及ぼす影響について経営層が理解し評価できる体制を整備する。すなわち、組織方針を踏まえ、サイバーセキュリテ

[3] 経営層、CISO、戦略マネジメント層、担当者層といった縦の階層のほか、 情報システム部門、事業部門、広報部門といった横方向にも留意。

ィを確保できないことによって組織の情報システム及び情報を活用する事業、事業者としての信頼、その他の経営リスクがどのような影響を受けるのかといった視点からもリスクを 管理し、個々の情報システム及び情報自体のセキュリティに関する視点においてもリスクを分析する 。また、自組織にとどまらず、ビジネスパートナーや委託先等、サプライチェーン全体にわたるセキュリティ対策への目配り[4] を行う。

経営層は、重要インフラサービスの提供に不可欠な情報システムは何か、それらがどのようにサイバー脅威にさらされる可能性があるか、どのようなセキュリティ対策をとるべきかを理解することを念頭に、サイバーセキュリティリスクについて可能な限り理解するよう努めることが望ましい。

エ　責任及び権限の割当て

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 3.4 参照）

サイバーセキュリティリスクの管理について、サイバーセキュリティを担当する部署及び従業員を決定するとともに責任及び権限を割り当てる[5] 。特に、経営層の責任において、サイバーセキュリティに関する責任者（CISO 等）を任命する[6] 。当該責任者は、サイバーセキュリティに関する知見を有する者であるとともに、組織内の職階において、平時に、またとりわけ有事に、組織トップと 直接コミュニケーションできる者として位置付けられるべきであり、経営層に相当する者の中から任命されることが望ましい。

---

[4] 在来形の部品調達などの形態や規模にとどまらないクラウドサービスの利用等のデジタル環境を介した外部とのつながりの全てを含むサプライチェーン全体を俯瞰し、総合的にサイバーセキュリティを確保すべきである。

[5] 適切な管理体制の構築を前提としつつ、サイバーセキュリティに関する専門的な事項については、外部委託、業界団体との連携等により補完してもよい。

[6] 会社法第 362 条第 4 項の柱書及び同項第 3 号は、取締役会を設置する株式会社について「取締役会は、支配人その他の重要な使用人の選任及び解任の決定を取締役に委任することができない」旨を定めている。 CISO 等の任命は「重要な使用人の選任」に該当するため、取締役会設置会社の場合には、必ず取締役会で決定しなければならないことになる。同法第 348 条第 3 項の柱書及び同項第 3 号は、取 締役会を設置しない株式会社について、「取締役は、支配人の選任及び解任の決定を各取締役に委任することができない」旨を定めている。 CISO 等は通常「支配人」には該当しないものの、取締役会を設置する会社とのバランスを考えると、取締役会を設置しない会社においても、 CISO 等を任命する際には取締役の過半数の賛成を得ることが必要であると考えるべきである（同条第 2 項を参照）。
また、サイバーセキュリティに関する内部統制システムの構築において、「必要な内部組織及び権限」等について取締役会で決定されるべき事項としている。（ NISC 「サイバーセキュリティ 関係法令 Q&A ハンドブック」〔 2020 年 3 月 2 日〕）

オ　資源の確保

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 3.5 参照）

経営層は、セキュリティ対策に必要な資源（予算・人材等）について、組織の価値を維持・増大していく上で、組織活動におけるコストや損失を減らすために必要不可欠な投資[7] であるとの考え方[8] のもとで配分する。

カ　監査 ・モニタリング

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 3.6 参照）

情報セキュリティ監査、システム監査等の監査[9]（難しい場合には少なくとも 自己点検を経営層の責任において実施する。現状のシステムやセキュリティ対策の問題点を検出するために、脆弱性診断、ペネトレーションテスト等を実施することが望ましい。

セキュリティ対策 の導入・運用に伴うリスクの状況変化（事象の発生頻度の変化や、事象の結果の影響度の変化等）を定期的に確認する。また、サイバーセキュリティ方針に基づき設定した目標の達成状況、 サイバーセキュリティ方針・各種計画の有効性・妥当性等 について、定期的に、又は状況変化に応じて確認する。

キ　情報開示

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 3.7 参照）

国民の安心感の醸成を図る観点から、組織内の既存の情報開示体制を活用し、可能な範囲でサイバーセキュリティに関する取組を開示[10] する。サイバーセキュリティに関する次の情報を開示することが望ましい。

---

7 投資の概念については、会計、経営等様々な領域で定義が異なる。ここでは、直接の利益（リターン）を期待するものではないが、将来的なリスクを抑制し、リスクと利益の総和においてプラスの結果をもたらすための手段という意味で用いている。

8 一般に、セキュリティ対策への投資による直接的な収益を算出することは困難であり、サイバーセキュリティに関しては考え方の転換が必要。

9 内部監査を担当する部局は、組織トップの下に設けられることが多いが、その場合でも、事案の性質に応じて、報告先は組織トップとする場合と監査役等とする場合とを使い分けることとすべきである（デュアルレポートライン。経済産業省「グループ・ガバナンス・システムに関する実務指針」〔 2019 年 6 月 28 日〕 72 頁以下）。

10 サイバーセキュリティに関する組織の情報を開示することは、組織の社会への説明責任を果たすとともに、組織運営上の重要課題としてセキュリティ対策に積極的に取り組んでいるとしてステークホルダーから正当に評価されることが期待できる。

・ 組織方針・ サイバーセキュリティ方針
・ 維持する サービス範囲・水準
・ リスク管理体制
・ サイバーセキュリティに関する責任者の 知見
・ 資源の確保
・ リスクの把握と対応計画策定
・ 緊急対応体制・復旧体制
・ インシデントの発生状況

ク　継続的改善

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 3.8 参照）

サイバーセキュリティに関する監査・モニタリング の結果や、最新のセキュリティ動向も踏まえ、組織統治の枠組みの継続的改善を行う。サイバーセキュリティを担当する部署においては、 経営層からの指示、モニタリング・レビュー、危機管理、演習・訓練等を踏まえ、サイバーセキュリティ方針、各種計画等の継続的 改善 を行う。

改善を継続的に実施することで、サイバーセキュリティも含めたリスクマネジメントの考え方が組織に浸透し、組織風土に定着するよう努めることが望ましい。

2．リスクマネジメントの活用と危機管理対策

リスクマネジメントによる事前対応と、危機管理の両面からサイバーセキュリティの確保に取り組む ことが重要である 。

自組織の特性やリスクを特定した上で、①自組織の現在のセキュリティ対策の実施状況等に係る自己評価、②本来あるべき状況や要件との差異の分析、③分析結果を踏まえた自組織に不足している対策の優先順位付け、④具体的な対策の実施を繰り返せるよう、次に掲げる項目を安全基準等に規定することが望まれる。

（1）　共通

ア　組織状況の理解

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.1 参照）

重要インフラサービスに関する外部環境（政治、経済、社会等）及び内部環境（組織体制、戦略、能力等）の状況について、近い将来の状況

も含めて整理する。また、関係法令[11]、契約等に規定された義務、供給者・ 委託先が提示する制限事項等、関係者からの要求事項を整理する。任務保証の観点から次のような組織の特性を理解することが望ましい。

- 自組織が果たすべき役割・機能と、それを踏まえて維持・継続することが必要なサービス
- 最低限提供するサービスの範囲・水準
- サービス提供を維持するために必要な業務や経 営資源

さらに、サイバーセキュリティに関する部門においては、組織状況を理解した上で、現段階におけるセキュリティ対策の実施状況等の実態を把握する。

イ リスクアセスメント

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.2 参照）

情報システム、ソフトウェア、情報等の資産を特定する。組織状況と資産を踏まえ、任務保証の考え方に基づくリスクアセスメントを実施する。重要インフラサービスの継続提供を不確かなものとするシナリオを作成し、リスク分析を実施することが望ましい。

- 重要インフラサービスの継続的提供を不確かなものとするリスクとしては、自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等があり、リスクの特性に応じたリスク分析手法を選択する。
- 制御システム[12] に 汎用機器 が用いられ、また、遠隔監視・制御等のために外部と接続される場合がある[13] ことを念頭に、制御システムについても適切にリスクアセスメントを実施する[14] 。
- 情報システムの運用中も、サイバー攻撃に関する新たな脅威の発生等の環境変化に応じて適宜リスクアセスメントを実施する。
- 本来あるべき状況や要件を検討し、目標とする将来像を決定する。

---

11 例えば、重要インフラの事業法、個人情報の保護に関する法律（平成 15 年法律第 57 号）、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号）等。NISC「サイバーセキュリティ関係法令 Q&A ハンドブック」を参照。

12 社会インフラや工場・プラントの監視・制御や生産・加工ラインにおいて、他の機器やシステムを管理・制御するために用いられている機器群。

13 一般に、重要インフラの制御システムは、独自仕様の機器や通信プロトコルで構成され、また、外部と接続のない閉域環境で運用される。

14 IPA 「制御システムのセキュリティリスク分析ガイド第 2 版～セキュリティ対策におけるリスクアセスメントの実施と活用～」に記載されている具体的な作業手順等が参考になる。

ウ　サイバーセキュリティリスク対応

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.3 参照）

（ア） リスク対応の決定

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.3.1 参照）

目標とする将来像 と実態のかい離を埋めるために 実施すべきセキュリティ対策を検討する。 セキュリティ対策の程度については、成熟度モデルを活用しつつ、自組織における評価基準等をもって優先順位付けする。

リスク対応により、重要インフラサービス障害の発生を抑止するのみならず、発生した障害が経済 社会 に与える影響を許容範囲内に抑制するための検知・対応・復旧の各機能を実現する。

（イ） 個別方針の策定

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.3.2 参照）

リスク対応の中で決定した個々のセキュリティ対策 において 遵守すべき行為や判断等の基準を個別方針（例：アクセス制御方針、情報分類方針等）としてまとめ、組織内へ伝達する。また、必要に応じて委託先に対しても伝達する。

（ウ） リスク対応計画の策定

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.3.3 参照）

サイバーセキュリティに関する リスク対応計画を策定する。計画には次を記載することが望ましい。

- 目標とする 将来像
- 実施事項
- 必要な資源
- 責任者
- 達成期限
- 結果の評価方法

エ　サプライチェーン・リスクマネジメント

（重要インフラのサイバーセキュリティに係る安全基準等策定指針

4.4 参照）

対応すべき代表的なサプライチェーン[15] に係る脅威は次のとおり。

- 不正機能等の埋め込み
- サービスの供給途絶
- 外部サービスにおける情報の 不適切な 取扱い
- 海外 拠点、グループ組織、取引先等を経由した サイバー 攻撃

自組織の重要システムや機能とサプライチェーンの依存関係の把握、供給者のセキュリティ対策の状況の把握を行う。

サプライチェーン・リスクに関するリスクアセスメント及びリスク対応を行う。 海外拠点については、現地の法令、文化等も踏まえた対応を行う。

直接の供給者を対象に、事業者間の契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化する。さらに、リスクに応じて直接の供給者に連なる供給者への関与の程度を決定しつつ、各供給者がその先の供給者を対象にサプライチェーン・リスクマネジメントの実施状況を把握することで、サプライチェーン全体のリスクマネジメントを実施することが望ましい。また、セキュリティ対策の導入支援や共同実施等により、サプライチェーン全体での方策の実効性を高めることが望ましい。

なお、供給者のうち外部委託における情報セキュリティ確保のための詳細は「１０.外部委託における情報セキュリティ確保のための対策」を参照。

オ　事業継続計画等

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.5 参照）

サイバーインシデントが事業継続に及ぼす影響を踏まえ、事業継続に関する悪影響を許容範囲に抑制するための初動から完全復旧までの対応方針(コンテンジェンシープラン、事業継続計画[16] 、事業復旧計画[17] 等)

---

15 サプライチェーンとは、一般に、ある製品の原材料が生産されてから、最終消費者に届くまでのプロセスを意味するものであり、安全基準等策定指針においては、外部組織が関与する 製品 （機器・ソフトウェア 又は サービス （クラウドサービス、保守管理役務等 を自組織で調達・利用するプロセスとする。

16 大地震等の自然災害、感染症のまん延、テロ等の事件、大事故、サプライチェーン（供給網）の途絶、突発的な経営環境の変化など不測の事態が発生しても、重要な事業を中断させない、又は中断しても可能な限り短い期間で復旧させるための方針、体制 、手順等を示した計画。(内閣府「事業継続ガイドライン」〔令和 3 年 4 月〕 3 頁)

17 平時のサービス水準までの完全復旧対応の方針 。

にサイバーセキュリティを組み入れる。事業継続計画等には、サプライチェーンに係る脅威への対応を盛り込む。事業継続計画とあわせて、情報システムに係る記載を詳細化した対応方針（IT-BCP 等）[18] も策定することが望ましい。システム障害の影響が組織全体に波及する際、IT-BCP から事業継続計画へ円滑に移行していくことが望ましい 。

なお、事業継続性確保のための詳細については「９.重要インフラサービス障害の観点から見た事業継続性確保のための対策」を参照。

カ　人材育成 ・ 意識啓発

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.6 参照）

「サイバーセキュリティは全員参加（Cyber security by All ）」との考え方のもと、全ての従業員がサイバーセキュリティの内規等への理解を深め、また、部署・役職に応じて必要な水準のサイバーセキュリティに関する能力を確保できるよう、人材育成・意識啓発を行う。

- セキュリティ対策業務に従事する人材 を確保するため、キャリアパスの設計や外部人材活用の検討をすることが望ましい。
- セキュリティ対策業務に従事する人材 に対し、 「情報処理安全確保支援士」 等の資格 取得 、演習・訓練への参加等 を 推進 することが望ましい。
- セキュリティ対策が不十分だった場合に生じる影響例を示す等の方法により セキュリティ対策の重要性について 啓発をすることが望ましい。

キ　CSIRT 等の整備

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.7 参照）

CSIRT[19] としての機能を持つ体制を整備する。CSIRT 等は、役割分担や対応手順等を関連部門と合意する。特に、制御システムを保有する場合には、制御システム関連部門と連携できる体制を整備することが望ましい。

---

18 サイバーセキュリティ基本法（平成 26 年法律第 104 号）におけるサイバーセキュリティの定義には、情報システムの安全性及び信頼性の確保のために必要な措置も含まれる。

19 Computer Security Incident Response Team の略 シーサート。企業や行政機関等において、情報システム等にセキュリティ上の問題が発生していないか監視するとともに、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う体制のこと。

ク　平時の運用

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.8 参照）

（ア） セキュリティ対策の導入、運用プロセスの確立・実行

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.8.1 参照）

リスク対応計画を踏まえ、セキュリティ対策の導入、運用プロセスの確立・実行、CSIRT 等の運用を行う。 重要インフラサービス障害に繋がる可能性のある事象（サイバー攻撃、情報システムの異常状態等）を早期検知する仕組みを構築するとともに、関係部署等との 情報 共有、トリアージ[20] 等の運用プロセスを確立する ことが望ましい。

（イ） 情報共有

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.8.2 参照）

NISC『「 重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書』及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和 5 年 3 月 8 日 サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会 も踏まえ、組織内外と情報共有を実施する。

収集した脅威情報・対策情報を踏まえ、追加のリスクアセスメント及びリスク対応の要否の判断を行う。

- ISAC 等の分野専門性の高い情報共有活動に参加し、情報収集することが望ましい。
- 連絡体制 が最新の 情報 に更新されているか確認すること が望ましい。
- 有益な情報を得るには自ら適切な情報提供を行う必要があることを自覚し、組織内外に情報提供を行うことが望ましい。

ケ　危機管理

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.9 参照）

サイバー攻撃等の予兆を認識した場合、現在のセキュリティ対策で対処可能かを確認し、必要に応じて、対策の見直しや新たな対策の導入等

[20] サイバー攻撃等の事象の 影響分析及び対応の優先順位付けのこと。

を速やかに実施する。また、重要インフラサービス障害が発生した場合、事業継続計画 等 に従った初動・復旧対応を実施する。サイバーセキュリティを担当する部署は、 初動・復旧 対応に関する経営層の意思決定を支援するとともに、組織内外と情報共有を実施する。

コ　演習・訓練

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 4.10 参照）

リスクマネジメントによる事前対応と、危機管理の両面から、体制や取組の有効性を検証するため、実践的な演習・訓練を定期的に実施し、課題の抽出及び改善を行う。経営層も交え、組織全体での演習・訓練[21] を実施することが望ましい。また、他の重要インフラ事業者、サプライチェーンに係る事業者等と合同の演習・訓練、過去のインシデント対応事例の研究等 を実施することが望ましい。

３．組織的対策

（１）　共通

ア　情報セキュリティのための方針群

（ISO/IEC 27002 管理策 5.1 [ITU-T X.1051 5.1.1, 5.1.2]参照）

イ　情報セキュリティのための組織

（ア）　情報セキュリティの役割および責任

（ISO/IEC 27002 管理策 5.2 [ITU-T X.1051 6.1.1]参照）

（イ）　職務の分離

（ISO/IEC 27002 管理策 5.3 [ITU-T X.1051 6.1.2]参照）

（ウ）　プロジェクトマネジメントにおける情報セキュリティ

（ISO/IEC 27002 管理策 5.8 [ITU-T X.1051 6.1.5, 14.1.1]参照）

[21] 例えば、NISC が主催する「分野横断的演習」。

ウ　経営層[22] の責任

（ア） 経営層の責任

（ISO/IEC 27002 管理策 5.4 [ITU-T X.1051 7.2.1]参照）

（イ） リーダーシップ

経営層は情報セキュリティリスクへの対処に当たり、下記の「経営層の在り方」を認識し、「企業経営のためのサイバーセキュリティの考え方（「普及啓発・人材育成専門調査会」（平成２７年２月１０日　サイバーセキュリティ戦略本部決定)）」、「サイバーセキュリティ経営ガイドライン（経済産業省及び独立行政法人情報処理推進機構にて策定)」等を参考としつつ、適切な行動を取ることが期待される。

［経営層の在り方］

・情報セキュリティの確保は経営層が果たすべき責任であり、経営者自らがリーダーシップを発揮し 、任務保証の考え方を踏まえ、情報セキュリティ対策に取り組むこと

・自社の取組が社会全体発展にも寄与することを認識し、サプライチェーン（ビジネスパートナーや子会社、関連会社）を含めた情報セキュリティ対策に取り組むこと。

・情報セキュリティに関してステークホルダーの信頼・安心感を醸成する観点から、平時における情報セキュリティ対策に対する姿勢やインシデント発生時の対応に関する情報開示等に取り組むこと。

・上記の各取組に必要な情報を的確に収集するとともに、必要な予算・体制・人材等の経営資源を継続的に確保し、リスクベースの考え方により適切に配分すること。

・情報セキュリティリスクへの対応が事業に与えた効果と影響の検証結果を踏まえ、取締役会ほか経営上の重要会議においてさらなる情報セキュリティリスク対応戦略の見直しの必要性及びその内容についての意思決定を行うこと。

（ウ） コミュニケーション

経営層は、情報セキュリティ対策を推進する実務者層との間で、定期的な対話の機会等を設け、コミュニケーションを活性化するこ

---

[22] 組織の代表者として統括責任を負う者（CEO、理事長、首長等)、組織の業務を執行する者、及び、もしあれば、取締役会・理事会等。ISO/IEC 27002 の対訳版では、「経営陣」としているが、内閣サイバーセキュリティセンター「重要インフラのサイバーセキュリティに係る安全基準等策定指針」では「経営層」としている。本基準においては、「経営層」で用語を統一する。

とが重要である。その際、実務者層においては、経営層が情報セキュリティリスクへの対応状況を正確に把握し、状況に応じた的確な判断や調整を行うことを可能とするため、対話の機会を通じて、経営層に対して正確な情報提供や進言を行うことが重要となる。

エ　情報及びその他の関連資産の管理

（ア）　情報及びその他の関連資産の目録

（ISO/IEC 27002 管理策 5.9 [ITU-T X.1051 8.1.1, 8.1.2]参照）

（イ）　情報及びその他の関連資産の許容される利用

（ISO/IEC 27002 管理策 5.10 [ITU-T X.1051 8.1.3, 8.2.3]参照）

（ウ）　情報の分類

（ISO/IEC 27002 管理策 5.12 [ITU-T X.1051 8.2.1]参照）

（エ）　情報のラベル付け

（ISO/IEC 27002 管理策 5.13 [ITU-T X.1051 8.2.2]参照）

（オ）　データの管理

システムのリスク評価に応じて、データの保護や保管場所の考慮し、適切なデータ管理を行うことが望ましい。

また、事業環境の変化を捉え、インターネットを介したサービス（クラウドサービス等）を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在(II.既存の法令・ガイドライン等を参照)について留意することが望ましい。

オ　情報の転送

（ISO/IEC 27002 管理策 5.14 [ITU-T X.1051 13.2.1]参照）

カ　アクセス制御

（ア）　アクセス制御

（ISO/IEC 27002 管理策 5.15 [ITU-T X.1051 9.1.2]参照）

（イ）　識別情報の管理

（ISO/IEC 27002 管理策 5.16 [ITU-T X.1051 9.2.1]参照）

（ウ） 認証情報

（ISO/IEC 27002 管理策 5.17 [ITU-T X.1051 9.2.4]参照）

（エ） アクセス権

（ISO/IEC 27002 管理策 5.18 [ITU-T X.1051 9.2.2, 9.2.5]参照）

キ 情報セキュリティの独立したレビュー

（ISO/IEC 27002 管理策 5.35 [ITU-T X.1051 18.2.1]参照）

ク 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。

ケ 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。

コ 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重要インフラサービス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

る重要インフラサービス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 脅威インテリジェンス

（ISO/IEC 27002 管理策 5.7 参照）

イ 情報セキュリティインシデント管理の計画策定及び準備

（ISO/IEC 27002 管理策 5.24 [ITU-T X.1051 16.1.1]参照）

ウ 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） 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。

イ 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。

ウ 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。

エ 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。

４．人的対策

（１） 共通

ア 雇用条件

（ISO/IEC 27002 管理策 6.2 [ITU-T X.1051 7.1.2]参照）

イ 情報セキュリティの意識向上、教育及び訓練

（ISO/IEC 27002 管理策 6.3 [ITU-T X.1051 7.2.2]参照）

ウ 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。

特に、制御システム等の運用環境を保有する事業者等においては、重要インフラサービス障害発生時の対応に OT 関連部門の専門知識が要求される可能性を十分に認識しておく必要がある。

エ 懲戒手続

（ISO/IEC 27002 管理策 6.4 [ITU-T X.1051 7.2.3]参照）

５．物理的対策

（１） 共通

ア 物理的セキュリティ

（ア） 物理的セキュリティ境界

（ISO/IEC 27002 管理策 7.1 [ITU-T X.1051 11.1.1]参照）

（イ） 物理的入退

（ISO/IEC 27002 管理策 7.2 [ITU-T X.1051 11.1.2]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。([ITU-T X.1051 TEL.11.1.7]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。([ITU-T X.1051 TEL.11.1.8]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。([ITU-T X.1051 TEL.11.1.9]参照）

イ 物理的セキュリティの監視

（ISO/IEC 27002 管理策 7.4 参照）

ウ 装置のセキュリティ

（ア） 装置の設置及び保護

（ISO/IEC 27002 管理策 7.8[ITU-T X.1051 11.2.1]参照）

（イ） 記憶媒体

（ISO/IEC 27002 管理策 7.10 [ITU-T X.1051 8.3.1]参照）

（ウ） サポートユーティリティ

（ISO/IEC 27002 管理策 7.11[ITU-T X.1051 11.2.2]参照）

（エ） 装置のセキュリティを保った処分又は再利用

（ISO/IEC 27002 管理策 7.14 [ITU-T X.1051 11.2.7]参照）

ただし、クラウドサービス等で、情報を保存した装置や電磁的記録媒体等を物理的に処分することが難しい場合、暗号化消去（保存した情報の暗号化に利用した暗号鍵を消去する）によって、安全な処分ができる。

エ　自社の管理外の場所に設置する設備のセキュリティ

（[ITU-T X.1051 TEL.11.3]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。（[ITU-T X.1051 TEL.11.3.1]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。（[ITU-T X.1051 TEL.11.3.2]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。（[ITU-T X.1051 TEL.11.3.3]参照）

（２） 故障・災害等対策

ア　物理的及び環境的脅威からの保護

（ア） 物理的及び環境的脅威からの保護

（ISO/IEC 27002 管理策 7.5 [ITU-T X.1051 11.1.4]参照）

イ　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。

６．技術的対策

（１） 共通

ア 特権的アクセス権

（ISO/IEC 27002 管理策 8.2 [ITU-T X.1051 9.2.3]参照）

イ 容量・能力の管理

（ISO/IEC 27002 管理策 8.6 [ITU-T X.1051 12.1.3]参照）

ウ マルウェアに対する保護

（ISO/IEC 27002 管理策 8.7 [ITU-T X.1051 12.2.1]参照）

エ 構成管理

（ISO/IEC 27002 管理策 8.9）

オ　情報の削除

（ISO/IEC 27002 管理策 8.10）

カ　データマスキング

（ISO/IEC 27002 管理策 8.11）

キ　データ漏えい防止

（ISO/IEC 27002 管理策 8.12）

ク　運用システムへのソフトウェアの導入

（ISO/IEC 27002 管理策 8.19 [ITU-T X.1051 12.5.1]参照）

ケ　ネットワークセキュリティ管理

（ア）　ネットワークセキュリティ

（ISO/IEC 27002 管理策 8.20 [ITU-T X.1051 13.1.1]参照）

（イ）　ネットワークサービスのセキュリティ

（ISO/IEC 27002 管理策 8.21 [ITU-T X.1051 13.1.2]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。（ [ITU-T X.1051 TEL.13.1.4]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。([ITU-T X.1051 TEL.13.1.5]参照）

コ　ウェブフィルタリング

（ISO/IEC 27002 管理策 8.23）

サ　セキュリティに配慮したコーディング

（ISO/IEC 27002 管理策 8.28）

シ　開発及び受入れにおけるセキュリティテスト

（ISO/IEC 27002 管理策 8.29 [ITU-T X.1051 14.2.8, 14.2.9]参照）

ス　変更管理

（ISO/IEC 27002 管理策 8.32 [ITU-T X.1051 14.2.2]参照）

セ　監査におけるテスト中の情報システムの保護

（ISO/IEC 27002 管理策 8.34 [ITU-T X.1051 12.7.1]参照）

ソ　監視

（ア）　監視活動

（ISO/IEC 27002 管理策 8.16 参照）

（イ）　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。

（ウ）　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。

（エ）　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。

タ　暗号の使用

（ア）　暗号の利用

（ISO/IEC 27002 管理策 8.24 参照[ITU-T X.1051 10.1.1, 10.1.2]参照）

（イ）　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）　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、重要インフラサービス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）　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。

（４） 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。

7．クラウドサービスのセキュリティ対策

（1） クラウドサービス利用時の対策

ア クラウドサービスの利用における情報セキュリティ

（ISO/IEC 27002 管理策 5.23 参照）

イ クラウドサービス利用時の対策

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 5.5.2 参照）

- 利用するクラウドサービス の仕様を確認し 理解を深める。
- 責任共有モデルを理解し、 クラウドサービス提供者 との 責任範囲等 を明確にする。
- 情報公開 等の 設定 に ミスがないか確認する。
- サービス仕様が変わる際には影響を確認する。
- 多岐にわたるステークホルダーを把握し、情報共有体制・インシデント対応体制を構築する。
- クラウドサービスの利用終了時に、クラウドサービス上のデータの取り扱いについて確認する。

（2） クラウドサービス提供時の対策

ア クラウドサービスカスタマとクラウドサービスプロバイダとの関係

（ISO/IEC 27017-CLD.6.3 参照）

（ア） クラウドコンピューティング環境における役割及び責任の共有及び分担

（ISO/IEC 27017-CLD.6.3.1 参照）

イ 資産に対する責任

（ア） クラウドサービスカスタマの資産の除去

（ISO/IEC 27017-CLD.8.1.5 参照）

ウ 共有する仮想環境におけるクラウドサービスカスタマデータのアクセス

制御

（ISO/IEC 27017-CLD.9.5 参照）

（ア） 仮想コンピューティング環境における分離

（ISO/IEC 27017-CLD.9.5.1 参照）

エ　ログ取得及び監視

（ア） クラウドサービスの監視

（ISO/IEC 27017-CLD.12.4.5 参照）

オ　ネットワークセキュリティ管理

（ア） 仮想及び物理ネットワークのセキュリティ管理の整合

（ISO/IEC 27017-CLD.13.1.4 参照）

８．ランサムウェア対策

（１） 共通

（重要インフラのサイバーセキュリティに係る安全基準等策定指針 5.5.1 参照）

- 速やかなパッチ適用等による脆弱性対策を講じる。
- 海外拠点、サプライチェーンを含めて資産管理をする。
- システムソフトウェア及びデータのバックアップを行い、バックアップから復旧可能なことを定期的に確認する。
- バックアップデータをネットワークから隔離し保存する。
- 役割等に基づいてネットワークを分割する。
- 攻撃を受けた後に調査できるようにログなどを保存する。
- ベンダーなどの関係者と協力関係を構築する。
- 攻撃を受けた際は所管省庁や警察に連絡し、逐次時系列で状況を保存する。
- ランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むことが望ましい。

９．重要インフラサービス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　情報セキュリティ継続

（ア） 事業の中断・阻害時の情報セキュリティ

（ISO/IEC 27002 管理策 5.29 [ITU-T X.1051 17.1.1, 17.1.2, 17.1.3] 参照）

（イ） 事業継続のための ICT の備え

（ISO/IEC 27002 管理策 5.30 参照）

（ウ） サイバー攻撃に対する計画

重要インフラサービス障害を引き起こす事象のひとつである「サイバー攻撃」への備えを目的として、コンテンジェンシープラン及び事業継続計画を策定・改定する場合には、「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書【別紙】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照することが望ましい。

イ　重要インフラサービス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

重要インフラサービス障害の回復後、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、重要インフラサービス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　重要インフラサービス障害の検知と切り分け

（ア） 重要インフラサービス障害の検知・可視化

アラーム等の送付や監視画面への表示により、重要インフラサービス障害の検知・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） 重要インフラサービス障害（サイバー攻撃、故障等）の切り分け手順等の整備

重要インフラサービス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） 重要インフラサービス障害等情報の社内エスカレーション手順等の整備

重要インフラサービス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） 重要インフラサービス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重要インフラサービス障害の

レベルを内規等で定めることが望ましい。

（エ） 重要インフラサービス障害発生時の電気通信サービス利用者等への周知

重要インフラサービス障害発生時には、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。

重要インフラサービス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 重要インフラサービス障害対応の訓練・演習の計画・実施

（ア） 重要インフラサービス障害に対応する訓練の実施

重要インフラサービス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） 重要インフラサービス障害発生演習におけるメーカ等との協調

電気通信事業者が重要インフラサービス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。

コンテンジェンシープラン及び事業継続計画を策定・改定する場

合には、「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指針（第５版）改定版【別紙３】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照することが望ましい。

また、コンテンジェンシープラン及び事業継続計画の実行に必要な組織体制のひとつとして、CSIRT（又は同等機能を持つ組織）を事業者等の内部に整備することが望ましい。

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。

１０． 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） 機密保持契約又は守秘義務契約

（ISO/IEC 27002 管理策 6.6 [ITU-T X.1051 13.2.4]参照）

イ 供給者関係におけるセキュリティ

（ア） 供給者との合意における情報セキュリティの取扱い

（ISO/IEC 27002 管理策 5.20 [ITU-T X.1051 15.1.2]参照）

ウ 供給者のサービス提供の管理

（ア） 供給者のサービス提供の監視、レビュー及び変更管理

（ISO/IEC 27002 管理策 5.22 [ITU-T X.1051 15.2.1, 15.2.2]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. 組織統治におけるサイバーセキュリティ対策		
(1) サイバー攻撃対策		
ア 組織方針 組織方針（経営方針、リスクマネジメント方針等 にあたる文書に、 重要インフラのサイバーセキュリティ確保に関する事項も組み入れているか	○	○
ア 組織方針 **組織方針を踏まえ、次が記載されたサイバーセキュリティ方針を策定しているか** **・セキュリティ対策の目的や方向性** **・関係主体等からの要求事項への対応** **・経営層によるコミットメント**	○	○
イ 組織内外のコミュニケーション 組織内外のコミュニケーションにおいて、サイバーセキュリティリスク、インシデント等の情報を取り扱っているか	○	○
イ 組織内外のコミュニケーション **組織内のガバナンスや内部統制、その他のリスクマネジメントにおけるコミュニケーションの一部として、サイバーセキュリティに関する環境変化、インシデントの発生状況・得られた教訓、セキュリティ対策の実施状況・有効性評価等に関し、経営層と担当者層との間で定期的な対話の機会 等を設けているか**	○	○
ウ 経営リスクとしての サイバーセキュリティリスクの管理 組織全体のリスクマネジメントの一部として、サイバーセキュリティリスク及びそれが事業運営に及ぼす影響について経営層が理解し評価できる体制を整備しているか	○	○
ウ 経営リスクとしての サイバーセキュリティリスクの管理 自組織にとどまらず、ビジネスパートナーや委託先等、サプライチェーン全体にわたるセキュリティ対策への目配りを行っているか	○	○

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
		エ 責任及び権限の割当て サイバーセキュリティリスクの管理について、サイバーセキュリティを担当する部署及び従業員を決定するとともに責任及び権限を割り当てているか。 特に、経営層の責任において、サイバーセキュリティに関する責任者（CISO 等）を任命しているか	○	○
		オ 資源の確保 経営層は、セキュリティ対策に必要な資源（予算・人材等）について、組織の価値を維持・増大していく上で、組織活動におけるコストや損失を減らすために必要不可欠な投資であるとの考え方のもとで配分しているか	○	○
		カ 監査・モニタリング 情報セキュリティ監査、システム監査等の監査（難しい場合には少なくとも 自己点検を経営層の責任において実施しているか	○	○
		カ 監査・モニタリング セキュリティ対策 の導入・運用に伴うリスクの状況変化（事象の発生頻度の変化や、事象の結果の影響度の変化等）を定期的に確認しているか	○	○
		カ 監査・モニタリング サイバーセキュリティ方針に基づき設定した目標の達成状況、サイバーセキュリティ方針・各種計画の有効性・妥当性等 について、定期的に、又は状況変化に応じて確認しているか	○	○
		キ 情報開示 国民の安心感の醸成を図る観点から、組織内の既存の情報開示体制を活用し、可能な範囲でサイバーセキュリティに関する取組を開示しているか	○	○
		ク 継続的改善 サイバーセキュリティに関する監査・モニタリング の結果や、最新のセキュリティ動向も踏まえ、組織統治の枠組みの継続的改善を行っているか	○	○

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
ク 継続的改善 **サイバーセキュリティを担当する部署においては、経営層からの指示、モニタリング・レビュー、危機管理、演習・訓練等を踏まえ、サイバーセキュリティ方針、各種計画等の継続的 改善 を行っているか**	○	○
2 リスクマネジメントの活用と危機管理対策		
(1) 共通		
ア 組織状況の理解 重要インフラサービスに関する外部環境（政治、経済、社会等）及び内部環境（組織体制、戦略、能力等）の状況について、近い将来の状況も含めて整理しているか	○	○
ア 組織状況の理解 関係法令、契約等に規定された義務、供給者・ 委託先が提示する制限事項等、関係者からの要求事項を整理しているか	○	○
ア 組織状況の理解 サイバーセキュリティに関する部門において、組織状況を理解した上で、現段階におけるセキュリティ対策の実施状況等の実態を把握しているか	○	○
イ リスクアセスメント 情報システム、ソフトウェア、情報等の資産を特定する。組織状況と資産を踏まえ、任務保証の考え方に基づくリスクアセスメントを実施しているか	○	○
ウ サイバーセキュリティリスク対応 目標とする将来像 と実態のかい離を埋めるために 実施すべきセキュリティ対策を検討しているか	○	○
ウ サイバーセキュリティリスク対応 セキュリティ対策の程度については、マチュリティモデルを活用しつつ、自組織における評価基準等をもって優先順位付けを実施しているか	○	○

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
		ウ サイバーセキュリティリスク対応 リスク対応の中で決定した個々のセキュリティ対策 において遵守すべき行為や判断等の基準を個別方針（例：アクセス制御方針、情報分類方針等）としてまとめ、組織内や、必要に応じて委託先に対しても伝達しているか	○	○
		ウ サイバーセキュリティリスク対応 サイバーセキュリティに関する リスク対応計画を策定しているか	○	○
		エ サプライチェーン・リスクマネジメント 自組織の重要システムや機能とサプライチェーンの依存関係の把握や供給者のセキュリティ対策の状況の把握を行っているか	○	○
		エ サプライチェーン・リスクマネジメント サプライチェーン・リスクに関するリスクアセスメント及びリスク対応を行っているか	○	○
		エ サプライチェーン・リスクマネジメント 海外拠点について、現地の法令、文化等も踏まえた対応を行っているか	○	○
		エ サプライチェーン・リスクマネジメント 直接の供給者を対象に、事業者間の契約において、サイバーセキュリティリスクへの対応に関して担うべき役割と責任範囲を明確化しているか	○	○
		オ 事業継続計画等 サイバーインシデントが事業継続に及ぼす影響を踏まえ、事業継続に関する悪影響を許容範囲に抑制するための初動から完全復旧までの対応方針（コンテンジェンシープラン、 事業継続計画、 事業復旧計画等）にサイバーセキュリティを組み入れているか	○	○
		カ 人材育成・意識啓発 「サイバーセキュリティは全員参加（Cyber security by All ）」との考え方のもと、全ての従業員がサイバーセキュリティの内規等への理解を深め、また、部署・役職に応じて必要な水準のサイバーセキュリティに関する能力を確保できるよう、人材育成・意識啓発を行っているか	○	○

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
		キ CSIRT 等の整備 CSIRT としての機能を持つ体制を整備しているか。 CSIRT 等は、役割分担や対応手順等を関連部門と合意しているか	○	○
		ク 平時の運用 リスク対応計画を踏まえ、セキュリティ対策の導入、運用プロセスの確立・実行、CSIRT 等の運用を行っているか	○	○
		ク 平時の運用 NISC『「重要インフラのサイバーセキュリティに係る行動計画」に基づく情報共有の手引書』及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（令和 5 年 3 月 8 日 サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会 も踏まえ、組織内外と情報共有を実施しているか	○	○
		ケ 危機管理 サイバー攻撃等の予兆を認識した場合、現在のセキュリティ対策で対処可能かを確認し、必要に応じて、対策の見直しや新たな対策の導入等を速やかに実施しているか	○	○
		ケ 危機管理 重要インフラサービス障害が発生した場合、事業継続計画 等に従った初動・復旧対応を実施する。サイバーセキュリティを担当する部署は、 初動・復旧 対応に関する経営層の意思決定を支援するとともに、組織内外と情報共有を実施しているか	○	○
		コ 演習･訓練 リスクマネジメントによる事前対応と、危機管理の両面から、体制や取組の有効性を検証するため、実践的な演習・訓練を定期的に実施し、課題の抽出及び改善を行っているか	○	○
3. 組織的対策				
	(1)共通			
		ア 情報セキュリティのための方針群 **情報セキュリティのための方針群は、これを定義し、管理層が承認し、発行し、従業員及び関連する外部関係者に通知されているか**	○	○

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 情報セキュリティのための方針群 情報セキュリティのための方針群は、あらかじめ定められた間隔で、又は重要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	○	○
イ 情報セキュリティのための組織 全ての情報セキュリティの責任を定め、割り当てているか	○	○
イ 情報セキュリティのための組織 相反する業務及び責任範囲は、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不正使用の危険性を低減するために、分離されているか	○	○
イ 情報セキュリティのための組織 プロジェクトの種類に関わらず、プロジェクトマネジメントにおいては、情報セキュリティに取組んでいるか	○	○
ウ 経営者の責任 経営層は、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全ての従業員及び契約相手に要求しているか	○	○
ウ 経営者の責任 経営層は 情報セキュリティリスクへの対処に当たり、下記の「経営層の在り方」を認識し、「企業経営のためのサイバーセキュリティの考え方(「普及啓発・人材育成専門調査会」(平成27年2月10日 サイバーセキュリティ戦略本部決定))」、「サイバーセキュリティ経営ガイドライン(経済産業省及び独立行政法人情報処理推進機構にて策定)」等を参考としつつ、適切な行動を取っているか	○	○
ウ 経営者の責任 経営層は、情報セキュリティ対策を推進する実務者層との間で、定期的な対話の機会等を設け、コミュニケーションを活性化しているか 実務者層においては、経営層が情報セキュリティリスクへの対応状況を正確に把握し、状況に応じた的確な判断や調整を行うことを可能とするため、対話の機会を通じて、経営層に対して正確な情報提供や進言を行っているか	○	○
エ 情報及びその他の関連資産の管理 情報及び情報処理施設に関連する資産を特定しているか これらの資産の目録を作成し、維持しているか	○	○
エ 情報及びその他の関連資産の管理 目録の中で維持される資産は、管理されているか	○	○

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
		エ 情報及びその他の関連資産の管理 情報の利用の許容範囲、並びに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は、明確にし、文書化し、実施しているか	○	○
		エ 情報及びその他の関連資産の管理 資産の取扱いに関する手順は、組織が採用した情報分類体系に従って策定し、実施しているか	○	○
		エ 情報及びその他の関連資産の管理 情報は、法的要求事項、価値、重要性、及び認可されていない開示又は変更に対して取扱いに慎重を要する度合いの観点から、分類しているか	○	○
		エ 情報及びその他の関連資産の管理 情報のラベル付けに関する適切な一連の手順は、組織が採用した情報分類体系に従って策定し、実施されているか	○	○
		エ 情報及びその他の関連資産の管理 システムのリスク評価に応じて、データの保護や保管場所の考慮し、適切なデータ管理を行っているか 事業環境の変化を捉え、インターネットを介したサービス(クラウドサービス等)を活用するなど新しい技術を利用する際には、国内外の法令や評価制度等の存在(既存の法令・ガイドライン等を参照)について留意しているか	○	○
		オ 情報の転送 あらゆる形式の通信設備を利用した情報転送を保護するために、正式な転送方針、手順及び管理策を備えているか	○	○
		カ アクセス制御 利用することを特別に認可したネットワーク及びネットワークサービスへのアクセスだけを、利用者に提供しているか	○	－
		カ アクセス制御 アクセス権の割り当てを可能にするために、利用者の登録・登録削除についての正式なプロセスを実施しているか	○	－
		カ アクセス制御 秘密認証情報の割当ては、正式の管理プロセスによって管理しているか	○	－
		カ アクセス制御 全ての種類の利用者について、全てのシステム及びサービスへのアクセス権を割り当てる又は無効化するために、利用者アクセスの提供についての正式なプロセスを実施しているか	○	－

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
		カ アクセス制御 資産の管理責任者は、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	○	－
		キ 情報セキュリティの独立したレビュー 情報セキュリティ及びその実施の管理に(例えば、情報セキュリティのための管理目的、管理策、方針、プロセス、手順)対する組織の取組みについて、あらかじめ定めた間隔で、又は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	○	○
		ク 情報セキュリティ対策の目標 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	○	－
		ケ 情報セキュリティ確保の取組み状況の公開 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	○	－
		コ 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重要インフラサービス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重要インフラサービス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	○	○
	⑵サイバー攻撃対策			
		ア 脅威インテリジェンス 脅威インテリジェンス(脅威の防止や検知に利用できる情報)の収集・分析を行っているか	○	○
		イ 情報セキュリティインシデント管理の計画策定及び準備 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	○	○

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
		ウ 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しているか	○	○
	⑶ネットワーク輻そう対策			
		ア ネットワーク輻そう対策 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	○	－
	⑷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 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	○	－
	⑸重要情報漏えい対策			
		ア 重要情報管理体制・対応方針 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定めているか	○	○
		イ 重要情報に対する責任 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	○	○
		イ 重要情報に対する責任 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	○	○
		ウ 重要情報の分類 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	○	○
		エ 重要情報の盗難、紛失、流出への対策 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	○	○

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
		エ 重要情報の盗難、紛失、流出への対策 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	○	○
		エ 重要情報の盗難、紛失、流出への対策 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	○	○
4. 人的対策				
	(1)共通			
		ア 雇用条件 従業員及び契約相手との雇用契約書には、情報セキュリティに関する各自の責任及び組織の責任を記載しているか	○	○
		イ 情報セキュリティの意識向上、教育及び訓練 組織の全ての従業員、及び関係する場合には、契約相手は、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及び訓練を受けているか	○	○
		ウ 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 制御システム等の運用環境を保有する事業者等においては、重要インフラサービス障害発生時の対応にOT関連部門の専門知識が要求される可能性を十分に認識しているか	○	○
		エ 懲戒手続き 情報セキュリティ違反を犯した従業員に対しての処置をとるための、正式かつ周知された懲戒手続を備えているか	○	○
5. 物理的対策				
	(1)共通			

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 物理的セキュリティ 取扱いに慎重を要する又は重要な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を定義し、かつ、用いているか	○	－
		ア 物理的セキュリティ 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	○	－
		ア 物理的セキュリティ 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	○	－
		ア 物理的セキュリティ 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	○	－
		ア 物理的セキュリティ 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	○	－
		イ 物理的セキュリティの監視 組織の敷地を物理的に監視しているか	○	－
		ウ 装置のセキュリティ 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し、又は保護されているか	○	－
		ウ 装置のセキュリティ 組織が採用した分類体系に従って、取外し可能な媒体の管理のための手順を実施しているか	○	○
		ウ 装置のセキュリティ 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	○	－
		ウ 装置のセキュリティ 記憶媒体を内蔵した全ての装置は、処分又は再利用する前に、全ての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、又はセキュリティを保って上書きしていることを確実にするために、検証されているか	○	－

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
		エ　自社の管理外の場所に設置する設備のセキュリティ 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	○	－
		エ　自社の管理外の場所に設置する設備のセキュリティ 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	○	－
		エ　自社の管理外の場所に設置する設備のセキュリティ 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	○	－
	⑵故障・災害等対策			
		ア　物理的及び環境的脅威からの保護 自然災害、悪意のある攻撃又は事故に対する物理的な保護を設計し、適用しているか	○	－
		イ　故障・災害等に対するサービス可用性確保 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	○	－
		イ　故障・災害等に対するサービス可用性確保 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
		イ 故障・災害等に対するサービス可用性確保 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	○	－
		イ 故障・災害等に対するサービス可用性確保 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	○	－
		イ 故障・災害等に対するサービス可用性確保 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）	○	－
		イ 故障・災害等に対するサービス可用性確保 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	○	－
		イ 故障・災害等に対するサービス可用性確保 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	○	－
6. 技術的対策				
	(1) 共通			

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 特権的アクセス権 特権的アクセス権の割当て及び利用は、制限し、管理しているか	○	－
		イ 容量・能力の管理 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	○	－
		ウ マルウェアに対する保護 マルウェアから保護するための対策(検出、予防、対策)を実施しているか	○	－
		エ 構成管理 ハードウェア、ソフトウェア、サービス(クラウド含む)、ネットワーク等の構成管理を行っているか	○	－
		オ 情報の削除 情報は不要になった際に削除しているか	○	－
		カ データマスキング アクセス制御方針や法的要求事項を考慮し、データマスキングを利用しているか	○	－
		キ データ漏えい防止 情報漏えいを検知し防止するため、利用者データの管理、データ漏えいの検知を行っているか	○	－
		ク 運用システムへのソフトウェアの導入 運用システムに関わるソフトウェアの導入を管理するための手順を実施しているか	○	－
		ケ ネットワークセキュリティ管理 システム及びアプリケーション内の情報を保護するために、ネットワークを管理し、制御しているか	○	－
		ケ ネットワークセキュリティ管理 組織が自ら提供するか外部委託しているかを問わず、全てのネットワークサービスについて、セキュリティ機能、サービスレベル及び管理上の要求事項を特定し、また、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	○	－
		ケ ネットワークセキュリティ管理 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	○	－

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
ケ ネットワークセキュリティ管理 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	○	－
コ ウェブフィルタリング 外部Web サイトへのアクセス制御を行っているか	○	－
サ セキュリティに配慮したコーディング セキュリティに配慮したコーディング原則をソフトウェア開発に適用しているか	○	－
シ 開発及び受入れにおけるセキュリティテスト セキュリティ機能(functionality)の試験は、開発期間中に実施されているか	○	－
シ 開発及び受入れにおけるセキュリティテスト 新しい情報システム、及びその改訂版・更新版のために、受入れ試験のプログラム及び関連する基準を確立しているか	○	－
ス 変更管理 開発のライフサイクルにおけるシステムの変更は、正式な変更管理手順を用いて管理されているか	○	－
セ 監査におけるテスト中の情報システムの保護 監査の実施 情報システムに対する管理策 運用システムの検証を伴う監査要求事項及び活動は、業務プロセスの中断を最小限に抑えるために、慎重に計画し、合意されているか	○	－
ソ 監視 ネットワーク、システム、アプリケーションについて、利用者のシステムへのアクセス、利用者の異常なシステム上の行動などを監視しているか	○	－
ソ 監視 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	○	－
ソ 監視 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	○	－
ソ 監視 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	○	－

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
		タ 暗号の使用 暗号の利用に関する方針を策定し、実施しているか	○	－
		タ 暗号の使用 暗号鍵の利用、保護及び有効期間に関する方針を策定し、ライフサイクル全体で実施しているか	○	－
		タ 暗号の使用 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	○	－
	⑵ 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 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、重要インフラサービス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	○	－
		ア サイバー攻撃に対するネットワーク管理策 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	○	－

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　サイバー攻撃に対するネットワーク管理策 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	○	－
		ア　サイバー攻撃に対するネットワーク管理策 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	○	－
		ア　サイバー攻撃に対するネットワーク管理策 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	○	－
	⑶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 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	○	－
		ア　ネットワーク輻そうに対するサービス可用性確保 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	○	－
		ア　ネットワーク輻そうに対するサービス可用性確保 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	○	－
		ア　ネットワーク輻そうに対するサービス可用性確保 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	○	－

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　ネットワーク輻そうに対するサービス可用性確保 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	○	－
		ア　ネットワーク輻そうに対するサービス可用性確保 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	○	－
		ア　ネットワーク輻そうに対するサービス可用性確保 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	○	－
		ア　ネットワーク輻そうに対するサービス可用性確保 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	○	－
	⑷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 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	○	－
		ア　重要情報漏えいに対するネットワーク管理策 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	○	－
		ア　重要情報漏えいに対するネットワーク管理策 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	○	－
7. クラウドサービスのセキュリティ対策				
	⑴クラウドサービス利用時の対策			
		ア クラウドサービスの利用における情報セキュリティ 組織がクラウドサービスを利用するときのセキュリティ対策、利用するための手順を確立しているか	○	－
		イ クラウドサービス利用時の対策 利用するクラウドサービス の仕様を確認しているか	○	－

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
		イ クラウドサービス利用時の対策 責任共有モデルを理解し、クラウドサービス提供者との責任 範囲等 を明確にしているか	○	－
		イ クラウドサービス利用時の対策 情報公開 等の設定 に ミスがないか確認しているか	○	－
		イ クラウドサービス利用時の対策 サービス仕様が変わる際には影響を確認しているか	○	－
		イ クラウドサービス利用時の対策 ステークホルダーを把握し、情報共有体制・インシデント対応体制を構築してるか	○	－
		イ クラウドサービス利用時の対策 クラウドサービスの利用終了時のクラウドサービス上のデータの取り扱いについて確認しているか	○	－
	⑵クラウドサービス提供時の対策			
		ア クラウドサービスカスタマとクラウドサービスプロバイダとの関係 クラウドサービスの利用に関して共有し分担する情報セキュリティの役割を遂行する責任は、クラウドサービスカスタマ及びクラウドサービスプロバイダのそれぞれにおいて特定の関係者に割り当て、文書化し、伝達し、実施しているか	○	－
		イ 資産に対する責任 クラウドサービスプロバイダの施設にあるクラウドサービスカスタマの資産は、クラウドサービスの合意の終了時に、時機を失せずに除去されるか又は必要な場合には返却されているか	○	○
		ウ 共有する仮想環境におけるクラウドサービスカスタマデータのアクセス制御 クラウドサービス上で稼動するクラウドサービスカスタマの仮想環境は、他のクラウドサービスカスタマ及び認可されていない者から保護されているか	○	－
		エ ログ取得及び監視 クラウドサービスカスタマは、クラウドサービスカスタマが利用するクラウドサービスの操作の特定の側面を監視する能力をもっている	○	－
		オ ネットワークセキュリティ管理 仮想ネットワークを設定する際には、クラウドサービスプロバイダのネットワークセキュリティ方針に基づいて、仮想ネットワークと物理ネットワークとの間の設定の整合性を検証しているか	○	－
8. ランサムウェア対策				
	⑴共通			

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
速やかなパッチ適用等により、脆弱性対策を講じているか	○	○
海外拠点、サプライチェーンを含めて資産管理を行っているか	○	○
システムソフトウェア及びデータのバックアップを行い、バックアップから復旧可能なことを定期的に確認しているか	○	○
バックアップデータをネットワークから隔離し保存しているか	○	○
役割等に基づいてネットワークを分割しているか	○	○
攻撃を受けた後に調査できるようにログなどを保存しているか	○	○
ベンダーなどの関係者と協力関係を構築しているか	○	○
攻撃を受けた際は所管省庁や警察に連絡し、逐次時系列で状況を保存するようなルールが規定されているか	○	○
ランサムウェア攻撃を助長しないようにするためにも、金銭の支払いは厳に慎むことがルールとして規定されているか	○	○
9. 重要インフラサービス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 情報セキュリティ継続 組織は、困難な状況(adverse situation)(例えば、危機又は災害)における、情報セキュリティ及び情報セキュリティマネジメントの継続のための要求事項を決定しているか	○	－
ア 情報セキュリティ継続 組織は、困難な状況のもとで情報セキュリティ継続に対する要求レベルを保証するための、プロセス、手順及び管理策を確立し、文書化し、実施し、維持しているか	○	－
ア 情報セキュリティ継続 確立及び実施した情報セキュリティ継続のための管理策が、困難な状況の下で有効であることを確実にするために、組織は、定められた間隔でこれらの管理策を検証しているか	○	－

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 情報セキュリティ継続 重要インフラサービス障害を引き起こす事象のひとつである「サイバー攻撃」への備えを目的として、コンティンジェンシープラン及び事業継続計画を策定・改定する場合には、「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指針(第5版)改定版【別紙3】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照しているか	○	－
		イ 重要インフラサービス障害に対応するための情報等の管理 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	○	－
		イ 重要インフラサービス障害に対応するための情報等の管理 重要インフラサービス障害の回復後、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	○	－
		イ 重要インフラサービス障害に対応するための情報等の管理 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	○	－
		ウ 重要インフラサービス障害の検知と切り分け アラーム等の送付や監視画面への表示により、重要インフラサービス障害の検知・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	○	－
		ウ 重要インフラサービス障害の検知と切り分け 重要インフラサービス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	○	－
		エ 緊急時の情報連絡 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	○	－

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
		エ 緊急時の情報連絡 重要インフラサービス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	○	－
		エ 緊急時の情報連絡 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重要インフラサービス障害のレベルを定めているか	○	－
		エ 緊急時の情報連絡 重要インフラサービス障害発生時には、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 重要インフラサービス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	○	－
		オ 重要インフラサービス障害対応の訓練・演習の計画・実施 重要インフラサービス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	○	－
		オ 重要インフラサービス障害対応の訓練・演習の計画・実施 重要インフラサービス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	○	○
	⑵サイバー攻撃対策			
		ア サイバー攻撃対応手順等の整備 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	○	－

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 サイバー攻撃対応手順等の整備 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定めているか コンテンジェンシープラン 及び事業継続計画を策定・改定する場合には、「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指針(第5版)改定版【別紙3】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照しているか コンテンジェンシープラン 及び事業継続計画の実行に必要な組織体制のひとつとして、CSIRT(又は同等機能を持つ組織)を事業者等の内部に整備しているか 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	○	－
		イ サイバー攻撃の被害拡大防止措置 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	○	－
		イ サイバー攻撃の被害拡大防止措置 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	○	－
		イ サイバー攻撃の被害拡大防止措置 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	○	－

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
		イ サイバー攻撃の被害拡大防止措置 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	○	－
		ウ サイバー攻撃からの復旧 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	○	－
		ウ サイバー攻撃からの復旧 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	○	－
		エ サイバー攻撃に対する訓練・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	○	－
	⑶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 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	○	－
		イ ネットワーク輻そうの検知・被害拡大防止措置 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
		イ ネットワーク輻そうの検知・被害拡大防止措置 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	○	－
		イ ネットワーク輻そうの検知・被害拡大防止措置 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	○	－
		イ ネットワーク輻そうの検知・被害拡大防止措置 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	○	－
	⑷故障・災害等対策			
		ア 故障・災害等対応手順書等の整備 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	○	－
		ア 故障・災害等対応手順書等の整備 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	○	○
		ア 故障・災害等対応手順書等の整備 災害対策としての設備復旧の対応手順を定めているか	○	－

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
		ア 故障・災害等対応手順書等の整備 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	○	○
		ア 故障・災害等対応手順書等の整備 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	○	○
	⑸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 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	○	○
		イ 重要情報漏えいの被害拡大防止措置 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、運用フロー等を定めているか	○	○
10. 外部委託における情報セキュリティ確保のための対策				
	⑴共通			
		ア 秘密保持 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、文書化されているか	○	○
		イ 供給者関係におけるセキュリティ 関連する全ての情報セキュリティ要求事項を確立しなければならず、また、組織の情報に対して、アクセス、処理、保存、若しくは通信を行う、又は組織の情報のためのIT基盤を提供する可能性のあるそれぞれの供給者と、この要求事項について合意しているか	○	○
		ウ 供給者のサービス提供の管理 組織は、供給者のサービス提供を定常的に監視し、レビューし、監査しているか	○	○
		ウ 供給者のサービス提供の管理 関連する業務情報、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、供給者によるサービス提供の変更(現行の情報セキュリティ方針群、手順、及び管理策の保守及び改善を含む)を管理しているか	○	○
	⑵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
		ア 外部委託先での重要情報の取扱い 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