

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

電気通信分野における
情報セキュリティ対策協議会
平成 18 年 6 月 29 日

まえがき

情報通信ネットワークは、我が国の社会経済活動を活性化させ、国民生活をより豊かなものとするのに役立ってきた。この趨勢は、今後とも続いていくことは間違いない。他方、情報通信ネットワークが我々の日常生活に浸透することに伴い、それがサイバー攻撃、ウイルス等によって機能不全に陥ったり、不正アクセスや情報漏洩が生じたりすることによって、被害の拡大が続いている。関係する報道に促されるように、情報セキュリティに対する社会全般の認識は高まりを見せており、その対策への取組みが企業の経営品質を表すものとみなされつつある。

情報セキュリティ対策の重要性が広く強調されるようになる一方で、何をもちて情報セキュリティ対策が十分あるいは不十分とするかは判然としない。とりわけ電気通信分野は、通信の秘密の保護、重要通信の優先取扱い、事業者間等の責任分界の明確化など、固有の法令上の要求事項があり、情報セキュリティ対策の評価の難度は高い。そのような観点から、総務省が、電気通信事業者における情報セキュリティ対策を強化するための具体的な手引きとして、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。以下「指針」という。）を公表した。

素より情報セキュリティ体制の構築は、事業者サイドのいわば責務であり、重要インフラの情報セキュリティ対策に係る行動計画（2005年12月情報セキュリティ政策会議決定）では、民が官と連携して関係事業者が守るべき情報セキュリティの水準を定めた安全基準等を策定することが求められている。今後、行動計画に呼応する形で、電気通信事業者の情報セキュリティ体制構築の底上げをより確かなものとしていくため、電気通信事業者において関係法令や電気通信事業の特性を考慮したセキュリティポリシーである当該指針を、電気通信業界のガイドラインとして導入・普及を図ることが重要である。さらに、より高いセキュリティの確保に向けて、情報セキュリティマネジメント全般にわたる事業者間の情報交換や協調・連携が活発化することが望まれる。

以上を踏まえ、電気通信分野における情報セキュリティ対策協議会は、「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」をここに定める。今後、当該ガイドラインが、電気通信事業における情報セキュリティマネジメントの確立・運用・確認・見直しに活用されることを通じ、我が国の国民生活・社会経済活動をより一層豊かにしていくことを期待する。

平成18年 6月

電気通信分野における情報セキュリティ対策協議会

0. はじめに

このガイドラインの目的は、電気通信事業者に対し、その事業環境に特有の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示すものである^(注1)。

(注1) 換言すれば、このガイドラインは、情報セキュリティマネジメントが構築され、維持され、改善されていることを認証するに当たっての要件を記述しているものではない。すなわち、本ガイドラインは、情報セキュリティマネジメントの構築・維持・改善のための手引きとなるものである。

情報セキュリティマネジメントの実践規範については、ISO/IEC^(注2)17799の第1版が2000年に、第2版が2005年に国際規格として発行されている。なお、2007年4月には、ISO/IEC 17799の規格番号が変更となり、ISO/IEC 27002と採番される予定である。

(注2) 国際標準化機構と国際電気標準会議の共同技術委員会の略。

しかし、電気通信事業においては、次の要求事項が更に強調されなければならない。

通信の秘密に属する事項の機密性の確保

電磁的方式により発信され、伝送され、又は受信される情報の完全性の確保

権限のある者による有線又は無線の施設の可用性の確保

第1に、機密性の確保に関しては、電気通信事業者の取扱中に係る通信の秘密は、何人も侵してはならないものであり、また、電気通信事業に従事する者は、取扱中に係る通信に関して知り得た他人の秘密を守ることが求められる。

第2に、完全性の確保に関しては、電磁的方式により発信され、伝送され、又は受信される情報が正確かつ完全なものとなるよう、有線又は無線の施設の設置及び使用が規律される必要がある。

第3に、可用性の確保に関しては、権限のある者が、必要なときに、有線又は無線の施設にアクセスできることを確保することが求められる。

これらに加え、電気通信事業においては、非常事態が発生したときに重要通信を優先的に取り扱わなければならない等の特別の法制上の要求事項がある。

このように、電気通信事業においては、情報セキュリティの確保に当たって、特有の専門性が要求されるものである。

これに加え、電気通信事業における有効な情報セキュリティマネジメントの必要性は、無線、インターネット、ブロードバンド等に係る技術の利用が拡大するに伴い、より切実なものとなっている。すなわち、情報セキュリティマネジメントが適切に実施されないまま、無線、インターネット、ブロードバンド等に係る技術が広く利用される場合には、通信の秘密に属する事項の機密性が侵され、電磁的方式により発信され、伝送され、又は受信される情報の完全性が維持されず、権限のある者が必要なときに有線又は無線の施設にアクセスできない、といったリスクを増大させるであろう。

また、電気通信事業者は、その電気通信設備を他人の通信の用に供することによって電気通信サービスを提供するものであり、組織内の情報処理施設を従業者や請負業者等が利用するという側面にとどまらず、自社の電気通信設備に自社組織外の多数の電気通信サービス利用者がアクセスしてくる、という側面を考慮しなければならない。

更に、電気通信事業者は、他の電気通信事業者との間で電気通信設備を接続又は共用することにより、又は他の電気通信事業者から卸電気通信役務の提供を受けることによって電気通信サービスを提供するものであり、そのセキュリティは他の電気通信事業者のセキュリティに依存しているのが実情である。

加えて、昨今、サイバー攻撃、ウイルス、ワーム等のインターネット上の脅威が増大しており、電気通信事業者は、電気通信サービスの安全・安心な提供のため、このガイドラインに規定する管理策等を適用しつつ、情報セキュリティ対策を講じることが望ましい。一方で、こうした対策が、通信の秘密の保護、個人情報の保護等の法的要求事項に違反しないよう、関係法令等を遵守した上で、情報セキュリティ対策を実行すべきである。

したがって、あらゆる電気通信事業者は、その事業規模、業務区域及びサービスの種類等に関わらず、通信の秘密に属する事項の機密性の確保、電磁的方式により発信され、伝送され、又は受信される情報の完全性の確保、及び 権限のある者による有線又は無線の施設の可用性の確保のために、適切な管理策をもたなければならない。

以上から、電気通信事業者は、管理策の選択及び実施に関して、電気通信事業分野に特有のガイドラインを必要としているものであり、電気通信事業における情報セキュリティマネジメントに関して共通のガイドラインをもつことは、個々の電気通信事業者にとっても利益になるものである。

ISO/IEC 17799 に記述されている事項は、電気通信事業にとっても重要であるが、電気通信事業においてどう実施することが望ましいかという点に関しては、追加的な説明を必要とする事項もあり、また、電気通信事業分野に特有の管理策が求められる事項もある。

このガイドラインは、一般に求められる情報セキュリティマネジメントだけでなく、電気通信事業においてどう実施することが望ましいかという追加的な説明や、電気通信事業に特有の管理策が求められる事項を加え、これらを一覧性をもってまとめ、電気通信事業分野において情報セキュリティに責任を有する者に対するガイドラインを示すことを企図しており、国際電気通信連合（ITU）で 2004 年に勧告化された X.1051 の内容を大幅に拡充しているものである。

このガイドラインの想定読者

このガイドラインは、電気通信事業者、電気通信事業分野における情報セキュリティに責任を有する者、セキュリティベンダ、監査人、通信機器ベンダ等を読者として想定しているものである。

このガイドラインを実装するメリット

ISO/IEC 17799 は、広範かつ種々の要素が複合した規格であり、電気通信事業を直接の対象としたものではない。

そこで、このガイドラインでは、電気通信事業分野に特有の課題に留意を払いつつ、電気通信事業分野において情報セキュリティマネジメントシステムを実装する上での一貫したガイドラインを示すことを企図したものである。

このガイドラインを参照することによって、電気通信事業者にとっては、通信の秘密に属する事項の機密性の確保、電磁的方式により発信され、伝送され、又は受信される情報の完全性の確保、及び 権限のある者による有線又は無線の施設の可用性の確保、に関する責任を果たすことが容易になる。

また、このガイドラインを参照して情報セキュリティマネジメントシステムを実装する結果として、電気通信事業者にとっては、情報セキュリティインシデントの数や影響度等を減少させることにより事業継続性の確保が期待でき、経営資源をより生産的な活動に回すことができる。

更に、電気通信事業分野における情報セキュリティ確保に関する一貫した取組みは、従業員のモラルを向上させ、通信の秘密に属する事項の機密性の確保、電磁的方式により発信され、伝送され、又は受信される情報の完全性の確保、及び 権限のある者による有線又は無線の施設の可用性の確保に対する公衆の信頼を増進させるものである。

1. 適用範囲

このガイドラインは、電気通信事業において情報セキュリティマネジメントシステムを実装するに当たってのガイドラインを規定するものであり、このガイドラインを参照して情報セキュリティマネジメントシステムを実装することによって、電気通信事業者は、通信の秘密に属する事項の機密性の確保、電磁的方式により発信され、伝送され、又は受信される情報の完全性の確保、及び 権限のある者による有線又は無線の施設の可用性の確保に関する要求水準を充たすことが期待される。

2. 用語及び定義

2.1 一般的な情報セキュリティ用語及び定義

2.1.1 資産

組織にとって価値をもつもの。(ISO/IEC 13335-1:2004)

2.1.2 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 17799:2005)

2.1.3 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)

2.1.4 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 17799:2005)

2.1.5 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 17799:2005)

2.1.6 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 TR 18044:2004)

2.1.7 情報セキュリティインシデント

望まない又は予期しない単独又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 TR 18044:2004)

2.1.8 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 17799:2005)

2.1.9 リスク

事象の発生確率と事象の結果の組合せ。(ISO/IEC Guide73: 2002)

2.1.10 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/IEC Guide73: 2002)

2.1.11 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/IEC Guide73: 2002)

2.1.12 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/IEC Guide73: 2002)

2.1.13 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/IEC Guide73: 2002)

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。

2.1.14 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/IEC Guide73: 2002)

2.1.15 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/IEC Guide 2: 1996)

2.1.16 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)

2.1.17 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)

2.2 電気通信分野における情報セキュリティ用語及び定義

2.2.1 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 第15条)

2.2.2 通信履歴

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)

2.2.3 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、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)

2.2.4 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。

2.2.5 電気通信設備

電気通信を行うための機械、器具、線路その他の電氣的設備。(電気通信事業法 第2条)

2.2.6 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)

2.2.7 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)

2.2.8 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。(電気通信事業法 第8条)

2.2.9 災害時優先電話

輻そう発生時において一般の電話からの通信に対して規制を行うことによって、発信した

通信が優先的に取扱われるよう設定された電話をいう。

2.2.10 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。

2.2.11 電気通信サービス利用者

電気通信事業者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)

2.2.12 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)

2.2.13 端末設備

電気通信回線設備の一端に接続される電気通信設備であって、一の部分の設置の場所が他の部分の設置の場所と同一の構内(これに準ずる区域内を含む。)又は同一の建物内であるもの。(電気通信事業法 第52条)

2.2.14 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

2.2.15 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

3. このガイドラインの構成

このガイドラインは、5 . 以降で ISO/IEC 17799 の構成を用いている。

目的(Objective)については、基本的に ISO/IEC 17799 を採用しているが、電気通信事業に特有の目的として、「9.3 自社の管理外の場所でのセキュリティ」を追加している。

管理策(Control)についても、基本的に ISO/IEC 17799 を採用しているが、電気通信事業に特有の管理策として、「9.1.7 通信センターの物理的な安全確保」、「9.1.8 電気通信設備室における安全確保」、「9.1.9 物理的に隔離された運用区画」、「9.3.1 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」、「9.3.2 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」、「9.3.3 相互接続における責任分界の明確化」、「10.6.3 電気通信サービス提供におけるセキュリティ管理」、「10.6.4 スパムメール対応」、「10.6.5 Dos/DDoS 攻撃対応」、「11.4.8 利用者による事業者の識別と認証」、「15.1.7 通信の秘密」、「15.1.8 重要通信の確保」、「15.1.9 非常事態の対応」を追加している。

実施の手引き (implementation guidance) については、ISO/IEC 17799 に規定されている一般企業向けの実施の手引きに加えて、電気通信事業に特有の実施の手引きを追記している。

関連情報 (other information) についても、必要に応じ、電気通信事業に特有の事項を追記している。

なお、管理策や実施の手引きの文末の括弧内に法令名・条項番号のみが記載されている場合、その管理策や実施の手引きは法令の要求する必須事項に当たる。また、当該括弧内の法令名・条項番号に加えて「参照」と記載されている場合は、その実施の手引きは推奨事項に当たる。

4. 電気通信分野における情報セキュリティマネジメント

4.1 目的

情報は、他の重要な事業資産と同様、組織事業の基礎を成し、紙に印刷若しくは手書きされ、電子的に保存され、郵便若しくは電子的な手段によって伝達され、映写され、又は会話として話されるものであり、どのような形態のものであろうとも、また、どのような手段によって共有又は保存されようとも、常に適切に保護されることが望ましい。

しかしながら、組織や組織の情報システム及びネットワークは、コンピュータを用いた不正行為、スパイ行為、妨害行為、破壊行為、情報漏洩、地震、火災又は洪水を含む広範囲にわたる原因によるセキュリティ脅威に直面している。悪意のあるコード、コンピュータ不正侵入及びサービス妨害攻撃のような被害をもたらす要因は、より一般化し、より大がかりになり、ますます巧妙になってきている。

仮に、組織の情報システムが破られること等により、情報セキュリティが侵害された場

合、組織が被る被害は計り知れないことから、組織は、経営陣によって承認された情報セキュリティ基本方針を定め、これに従って従業者教育や情報セキュリティ対策を実施し、見直しを図り、情報セキュリティを確保することが不可欠である。

情報セキュリティの確保は、方針、手続、手順、組織構造、並びにソフトウェア及びハードウェア機能を含む一連の適切な管理策を組織固有の情報セキュリティ目標及び事業目標に合うように、確立、実施、監視、レビュー及び改善を行うことで達成される。

特に、自らの電気通信設備をユーザの通信の用に供する電気通信事業者は、「通信の秘密」に属する情報を始めとして多くのユーザ情報を取り扱っており、情報をより適切に管理することが求められる。

電気通信事業者は、情報セキュリティ確保の重要性を認識した上で、このガイドラインを踏まえ、自社における情報セキュリティ目標を設定し、リスクアセスメントに基づき適切な管理策を選択し、必要な情報セキュリティ対策や社員教育を実施し、これらを見直し、継続的に情報セキュリティの確保に努めることが重要である。

4.2 保護されるべき資産

情報セキュリティマネジメントを確立する上で必要不可欠なことは、組織が持つ資産を洗い出し、組織が保有する資産を確認することである。この資産の属性や価値を明確にすることで適切な管理策の適用が可能となる。

電気通信事業者が保護すべき資産については、「7.1.1 資産目録」(関連情報)を参照のこと。

4.3 情報セキュリティマネジメント確立のための観点

4.3.1 セキュリティ要求事項の導出方法

電気通信事業者にとって、電気通信事業者におけるセキュリティ要求事項を識別することは極めて重要である。これは主に次の三つに由来する。

(1) 電気通信事業者における事業戦略及び目的を考慮して、自組織に対するリスクアセスメントを実施することによって得られるもの。

リスクアセスメントによって資産に対する脅威及び脆弱性が特定され、脅威が現実のものとなる可能性が評価され、潜在的な影響が推定される。

(2) 電気通信事業者が満たさなければならない法令、規則及び他事業者や顧客との契約上の要求事項、並びに電気通信事業に対する社会文化的環境。

特に電気通信事業者に要求される法令上の要求事項としては、通信の秘密の確保(15.1.7 参照)、重要通信の確保(15.1.8 参照)等があげられる。また、社会文化的環境からの要請としては、電磁的方式により発信され、伝送され、又は受信される情報の完全性の確保、権限のある者による有線又は無線の施設の可用性の確保、他人の電気通信設備の機能に障害を与えないこと等があげられる。

(3) 電気通信事業者が自らの事業活動を推進するために開発した情報処理に関する一連の原則、目的及び事業上の要求事項。

4.3.2 セキュリティリスクアセスメント

セキュリティ要求事項は、リスクを評価するための基準を明確にし、体系的にセキュリティリスクアセスメントを実施することによって識別される。セキュリティ上の管理策にかかる費用は、そのセキュリティ障害に起因する事業損害の規模に対してバランスが取れている必要がある。また、リスクアセスメントの結果は、次のことを導き、決定することに役立つ。

- ・適切な管理活動
- ・優先して取り扱うセキュリティリスク
- ・セキュリティリスクから保護するために選択された管理策の実施の優先順位

事業環境等の変化によって、セキュリティリスクも変化する可能性があるため、リスクアセスメントは定期的に繰り返すことが望ましい。

4.3.3 管理策の選択

セキュリティ要求事項及びリスクを識別し、リスク対応を決定したならば、リスクを受容可能なレベルまで低減することを確実にするように、管理策を選択し実施することが望ましい。

このガイドラインは、一般に求められる情報セキュリティマネジメントに関する管理策に加えて、電気通信事業に特有の要求事項を考慮し、電気通信事業者による管理策の実施を支援する手引きを含んだものであり、電気通信事業者は、このガイドラインから管理策を選択し、実施することが望ましい。また、事業者固有の要求に合わせて新しい管理策を適切に設計することも可能である。

セキュリティ管理策の選択は、リスクの受容基準、リスク対応における選択肢、及び電気通信事業者が採用している全般的なリスク管理の取組み方、契約上の要求事項等を基に下した組織的な判断に依存するものであり、すべての関連する国内外の法令及び規則に則ったものであることが望ましい。

4.3.4 重要な成功要因

電気通信事業者における情報セキュリティの実施を成功させるためには、次に示した要素が重要である。

- a) 事業目的を反映した情報セキュリティ基本方針、目的及び活動
- b) 組織の文化に合った情報セキュリティの実施、維持、監視及び改善のための取組み方並びに枠組み
- c) すべての管理者層からの目に見える形での積極的な支持及び関与

- d) 情報セキュリティ要求事項、リスクアセスメント及びリスクマネジメントの十分な理解
- e) セキュリティ意識向上を達成するための、すべての管理者、従業員及び関係者に対する情報セキュリティの効果的な普及
- f) すべての管理者、従業員及び関係者への、情報セキュリティ基本方針及び標準類に関する手引きの配布
- g) 情報セキュリティマネジメントの活動への資金提供
- h) 適切な意識向上、訓練及び教育の実施
- i) 効果的な情報セキュリティインシデント管理プロセスの確立
- j) 情報セキュリティマネジメントの実施状況を評価し、改善のための提言をフィードバックするために用いる測定システムの実施

注記 情報セキュリティの測定は、このガイドラインの適用範囲外である。

(注意)

電気通信事業において情報セキュリティマネジメントを確立するに当たり、電気通信事業者として考慮することが望ましい管理策、実施の手引き、関連情報について、以下「5. セキュリティ基本方針」から「15. コンプライアンス」において定めている。ただし、ここに定められる電気通信事業者のための事項は、ISO/IEC 17799 (情報セキュリティマネジメントの実践のための規範) において既に定められる管理策、実施の手引きの適用を可能とすることから、適用可能部分についてはこれを採用している。

そこで、以下では、ISO/IEC 17799 の適用可能部分の記載は省略(「ISO/IEC17799 参照」とのみ明記)することとし、特に電気通信事業において考慮することが望ましい事項を記述している。

5. セキュリティ基本方針

5.1 情報セキュリティ基本方針 (ISO/IEC17799 参照)

5.1.1 情報セキュリティ基本方針文書 (ISO/IEC17799 参照)

5.1.2 情報セキュリティ基本方針のレビュー (ISO/IEC17799 参照)

6.情報セキュリティのための組織

6.1 内部組織 (ISO/IEC17799 参照)

6.1.1 情報セキュリティに対する経営陣の責任 (ISO/IEC17799 参照)

6.1.2 情報セキュリティの調整 (ISO/IEC17799 参照)

6.1.3 情報セキュリティ責任の割当て (ISO/IEC17799 参照)

6.1.4 情報処理設備の認可プロセス (ISO/IEC17799 参照)

6.1.5 秘密保持契約 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

(中略)

特に、電気通信事業者においては、保護される情報の定義の例として、通信の秘密に属する事項がある。

6.1.6 関係当局との連絡 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

(中略)

特に、電気通信事業者が、裁判所や捜査機関から照会を受けた場合には、法令上の手続に従った照会であることを確認することが望ましい(電気通信事業における個人情報保護ガイドライン第23条参照)。

6.1.7 専門組織との連絡 (ISO/IEC17799 参照)

6.1.8 情報セキュリティの他者によるレビュー (ISO/IEC17799 参照)

6.2 外部組織 (ISO/IEC17799 参照)

6.2.1 外部組織に関係したリスクの識別 (ISO/IEC17799 参照)

6.2.2 顧客対応におけるセキュリティ (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

a) ~ k) (略)

l) 電気通信事業者の電気通信設備又は他の電気通信サービス利用者の電気通信設備の機能に障害を与えないよう契約事項をあらかじめ明確化しておくこと(電気通信事業法第41条第3項4号参照)。

m) 電気通信事業者の電気通信設備と電気通信サービス利用者の電気通信設備との責任の分界が明確であるようにすること(電気通信事業法第41条第3項5号)。

n) スパムメール等の送信により、電気通信サービスの円滑な提供に支障を生じる恐れがあると認められる場合において、電気通信サービスの提供を拒否することがあり得る旨をあらかじめ明確化しておくこと(10.6.4 参照)。

6.2.3 第三者との契約におけるセキュリティ対処 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

a) ~ v) (略)

w) 他の電気通信事業者の電気通信設備との接続に際して、互いの電気通信設備及び利用者の電気通信設備の機能に障害を与えないようにすること(電気通信事業法第41条第3項4号)。

x) 他の電気通信事業者の電気通信設備との責任の分界が明確化であるようにすること(電気通信事業法第41条第3項5号)。

7. 資産の管理

7.1 資産に対する責任 (ISO/IEC17799 参照)

7.1.1 資産目録 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

(中略)

特に、電気通信事業者が資産目録を作成し、維持するに当たっては、接続している他の電気通信事業者の電気通信設備との責任分界が明確になるよう識別し、文書化されることが望ましい。

関連情報

電気通信事業者に係る資産には多くの種類があり、それには以下のものが含まれる。

a) 情報：

電気通信サービス運用関係、顧客関係、契約関係、組織内の業務関係等の情報

(例) 通信データ、経路情報、加入者情報、ブラックリスト情報、登録サービス情報、運用情報、事故情報、構成情報、顧客情報、請求情報、トラフィック統計情報等、契約書、システムに関する文書、調査情報、ユーザマニュアル、訓練資料、操作又は支援手順、継続計画、緊急時の計画、代替手段、監査証跡、アーカイブ情報等

b) ソフトウェア：

電気通信サービス運用関係、組織内の業務関係等で利用するソフトウェア

(例) 通信制御ソフトウェア、運用管理ソフトウェア、顧客情報管理ソフトウェア、請求ソフトウェア等業務用ソフトウェア、システムソフトウェア、開発用ツール及びユーティリティ等

c) ハードウェア：

電気通信設備、電気通信回線設備、端末設備、コンピュータ装置、媒体等

(例) 交換機、ケーブル、端末機器、コンピュータ装置(サーバ、パソコン等)、媒体等

d) サービス：

電気通信サービス、情報処理サービス、非電気通信サービス等

(例) 固定電話サービス、携帯電話・PHSサービス、加入者線(光・ADSL)サービス、専用線・データ系回線サービス、インターネット接続サービス、データセン

タサービス、CATVサービス、コンテンツ配信サービス、ASPサービス等

e) 建物及び支援ユーティリティ設備

建物のほか、建物内で使用する諸設備

(例) 建物、電気設備、空調設備、消火設備等

f) 人

組織内部の人材、組織外部の人材等

(例) 従業員、契約相手、第三者の利用者、電気通信サービス加入者、電気通信サービス利用者、電気通信サービス以外のサービス利用者等

g) その他の無形資産

上記 a) ~ f) 以外の無形資産

(例) 組織の体制、ノウハウ、評判、イメージ等

(中略)

7.1.2 資産の管理責任者 (ISO/IEC17799 参照)

7.1.3 資産利用の許容範囲 (ISO/IEC17799 参照)

7.2 情報の分類 (ISO/IEC17799 参照)

7.2.1 分類の指針 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

(中略)

特に、電気通信事業者が情報を分類するに当たっては、電気通信事業者として以下の事項を考慮することが望ましい。

- a) 通信の秘密に属する事項とそれ以外の事項との分類 (15.1.7 d) 注 2 参照)
- b) 非常事態が発生し又は発生するおそれがある場合において優先的取扱いを必要とする機関の重要通信とそれ以外の通信 (15.1.8 参照)

7.2.2 情報のラベル付け及び取扱い (ISO/IEC17799 参照)

8. 人的資源のセキュリティ

8.1 雇用前 (ISO/IEC17799 参照)

8.1.1 役割及び責任 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

a) ~ e) (略)

特に、電気通信事業者は、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のため、一定の資格の保有者等相応の知識技能を有する者を配置し、その役割及び責任を定義し、配置される当人にも伝えることが望ましい。

8.1.2 選考 (ISO/IEC17799 参照)

8.1.3 雇用条件 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

a) (略)

b) (中略)。電気通信事業者が考慮すべき法的な責任及び権利としては、通信の秘密又は重要通信の確保に関連して制定された法律 (15.1.7 又は 15.1.8 参照) が含まれる。

c) ~ g) (略)

(中略)

特に、電気通信事業者は、電気通信事業に従事する者が、通信の秘密に関して、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならないこと及びその職を退いた後においても同様であることを周知徹底することが望ましい (15.1.7 参照) (電気通信事業法第4条第2項参照)。

8.2 雇用期間中 (ISO/IEC17799 参照)

8.2.1 経営陣の責任 (ISO/IEC17799 参照)

8.2.2 情報セキュリティの意識向上、教育及び訓練 (ISO/IEC17799 参照)

8.2.3 懲戒手続 (ISO/IEC17799 参照)

8.3 雇用の終了又は変更 (ISO/IEC17799 参照)

8.3.1 雇用終了時の責任 (ISO/IEC17799 参照)

8.3.2 資産の返却 (ISO/IEC17799 参照)

8.3.3 アクセス権の削除 (ISO/IEC17799 参照)

9.物理的及び環境的セキュリティ

9.1 セキュリティを保つべき領域 (ISO/IEC17799 参照)

9.1.1 物理的セキュリティ境界 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

適切ならば、物理的セキュリティ境界について、次の指針を考慮し、実施することが望ましい。

a) ~ g) (略)

h) 伝送設備や交換設備等事業用電気通信設備は、データセンター (IDC) の顧客設備等他の設備とは物理的に分離して設置する。

i) 特に、電気通信事業者においては、事業用電気通信設備のセキュリティ確保のため、物理的な障壁をその他の管理策とともに、有効に導入する。また、物理的な障壁、又はその他の管理策が有効に機能しない場合には、経営者等により責任を持って解決される。

9.1.2 物理的入退管理策 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

次の指針を考慮することが望ましい。

a) ~ e) (略)

f) 訪問者の入退の日付・時刻を記録する際には、他の来訪者の情報を保護すること。例えば、入場と退場の日付・時刻の記録は容易に見ることのできる場所に置かない。

なお、取扱いに慎重を要する情報を処理又は保管する領域へのアクセスの場合は、来訪者の入場時及び退場時にその荷物を確認し、危険物の持込や物品の不正な持出を防止する。

g) 電気通信事業者が事業用電気通信設備を運用するための電気通信設備室は、生体認証手法などの入退管理策を組み合わせることにより、適切な保護を行う。

9.1.3 オフィス、部屋及び施設のセキュリティ (ISO/IEC17799 参照)

9.1.4 外部及び環境の脅威からの保護 (ISO/IEC17799 参照)

9.1.5 セキュリティを保つべき領域での作業 (ISO/IEC17799 参照)

9.1.6 一般の人の立寄り場所及び受渡し場所 (ISO/IEC17799 参照)

9.1.7 通信センターの物理的な安全確保

管理策

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。

電気通信事業者向けの実施の手引き

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（以下「通信センター」という。）を保護するために、以下に示す事項を実施することが望ましい。

- a) 通信センターには、堅固な地盤の敷地を選ぶ。この条件を満たさない敷地を選ぶ場合には、事前に不均衡な沈下を防止するための適切な手段を講じる。
- b) 通信センターには、風水害などの影響を受けにくい環境にある敷地を選ぶ。この条件を満たさない敷地を選ぶ場合には、事前に風水害に対する適切な手段を講じる。
- c) 通信センターには、強力な電磁場の影響を受けにくい敷地を選ぶ。この条件を満たさない敷地を選ぶ場合には、事前に電磁シールド等で電気通信設備室を保護するための適切な手段を講じる。
- d) 通信センターには、爆発や発火の危険がある物品を保存している施設に隣接する敷地は避ける。
- e) 通信センターの建物は、耐震構造、免震構造又は制震構造とする。
- f) 通信センターの建物は、必要とされる床荷重に対し必要な構造上の耐性を備える。
- g) 通信センターの建物は、耐火建築物または準耐火建築物とする。
- h) 通信センターには、必要とされるすべての場所に自動火災警報装置を設置する。

9.1.8 電気通信設備室における安全確保

管理策

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。

電気通信事業者向けの実施の手引き

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（以下「電気通信設備室」という。）を保護するために、以下の管理策が考慮されることが望ましい。

- a) 電気通信設備室は自然災害などの外的な影響を受けにくい場所を選ぶ。
- b) 電気通信設備室は権限のない第三者の侵入を受けにくい場所を選ぶ。しかしながら、侵入を防止するために適切な手段が講じられている場合にはこの限りではない。
- c) 電気通信設備室は、浸水の恐れが少ない場所を選ぶ。仮に浸水の恐れのある場所に設置しなければならない場合は、床の高上げ、止水壁又は特別な排水設備の設置等必要な手段を講じる。
- d) 電気通信設備室は電磁場の影響を受けにくい場所を選ぶ。電磁場の影響を受けやすい場所に設置しなければならない場合には、電磁シールドその他により保護する。
- e) 電気通信設備室の扉は、十分な強度を備えたものとする。
- f) 通常予想される規模の地震により、天井、壁、床などに使用されている素材が崩壊、又は落下しないような防止策を講じる。
- g) 床、壁、天井等に使用される素材は難燃性あるいは不燃性の素材を用いる。
- h) 静電気を防止するための方策を講じる。
- i) 電気通信設備室に電源供給設備を導入する場合、必要に応じて、電磁場からの干渉を避けるための手段を講じる。
- j) 電気通信設備室の貫通口は、火災の拡大を阻止するように設計する。
- k) 必要な場合には、データ保管室とデータを電磁的干渉から保護するための手段を講じる。
- l) 必要に応じて、データ保管室及び専用のデータベースが設置されている領域等に耐火手段を講じる。
- m) 電気通信設備室、空調設備室など、必要な全ての場所に自動火災警報装置を設置する。
- n) 電気通信設備室、空調設備室など、必要な全ての場所に消火設備又は消火器を設置する。
- o) 必要に応じて、電気通信設備室に適切な設備容量を有する空調設備を設置する。
- p) 空調設備の荷重を十分考慮するとともに、通常想定される規模の地震による転倒又は移動を防止する措置を講じる。
- q) 空調設備には、温湿度及び空気清浄度を適正な範囲内に維持する機能や急激な温度変化が生じないよう制御する機能を設ける。
- r) 凍結のおそれのある場所に設置する空調設備には、凍結による故障等の発生を防止する措置を講じる。
- s) 空調設備の排水口等の漏水を防止する措置を講じる。
- t) 腐食性ガス(SO₂等)や粉塵が混入するおそれのある場所に設置する空調設備には、触媒、フィルター等によりこれを排除する機能を設ける。

- u) 重要な設備を収容する電気通信設備室の空調を行う空調設備は、冗長構成とする。
- v) 重要な設備を収容する電気通信設備室の空調を行う空調設備には、故障等を速やかに検知、通報する機能を設ける。
- w) 重要な設備を収容する電気通信設備室の空調設備は、オフィスやその他の部屋の空調設備とは別のシステムにより稼働させる。電気通信設備室を適切に温度調節する手段が講じられている場合は、この限りではない。

9.1.9 物理的に隔離された運用区画

管理策

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。

電気通信事業者向けの実施の手引き

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（以下「隔離運用区画」という。）を保護するために、以下の管理策が考慮されることが望ましい。

- a) 隔離運用区画は、国又は地域の強制力のある基準に適合するだけの耐震性を備える。
- b) 隔離運用区画には、自動的に火災を検知し動作する消火設備を設置する。
- c) 隔離運用空間は、設備障害、電源障害、火災、湿度及び気温などを検知するために、遠隔のオフィスから監視する。
- d) 隔離運用区画を囲むフェンスの設置など、適切な手段により物理的なセキュリティ上の保護策を設ける。通常は自社によって運営されるため、インシデントが発生した際の運用センターへの自動警報機能を備える。

9.2 装置のセキュリティ (ISO/IEC17799 参照)

9.2.1 装置の設置及び保護 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

(中略)

特に、データセンターにおいて、同業種の複数企業のシステムを導入している場合、顧客情報を適切に保護することが望ましい。それらのシステムは別の階又は異なる場所に設置することが望ましい。

9.2.2 サポートユーティリティ (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

(中略)

特に、移動体通信基地局等隔離された区画における電源設備は、様々な負荷に対する十分な容量を確保することが望ましい。これが困難である場合には、脆弱な部分にかかる負荷を監視する仕組みを備えることが望ましい。停電対策としてバッテリーを設置することが望ましい。他局により通信エリアをカバーできない移動体通信基地局のような隔離された区画においては、バッテリーの容量を増大させ、又は非常用の発電機や電源車を配備することが望ましい。

関連情報

(中略)

支援ユーティリティの保守や支援ユーティリティ提供者からの継続的供給に関する事項については、電気通信サービスの継続的な提供を確保するために、契約書等によってその履行を確保することが望ましい。

9.2.3 ケーブル配線のセキュリティ (ISO/IEC17799 参照)

9.2.4 装置の保守 (ISO/IEC17799 参照)

9.2.5 構外にある装置のセキュリティ (ISO/IEC17799 参照)

9.2.6 装置の安全な処分又は再利用 (ISO/IEC17799 参照)

9.2.7 資産の移動 (ISO/IEC17799 参照)

9.3 自社の管理外の場所に設置する設備のセキュリティ

目的

電気通信事業者が自社の管理外の場所に設置する設備を物理的及び環境的な脅威から保護するため。

電気通信事業者が自社の管理外の場所に自社の設備を設置する場合には、その場所が、経営陣によって承認されたセキュリティレベルを維持できる適切な場所であることを事前に確認することが望ましい。

9.3.1 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

管理策

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。

電気通信事業者向けの実施の手引

他の電気通信事業者の領域に設置する自社の設備のセキュリティを確保するため、電気通信事業者は次の事項を考慮することが望ましい。

- a)他の電気通信事業者との分界点を明確にし、容易に切り離せる
- b)支援ユーティリティ供給についての取決めが他の電気通信事業者と結ばれている

他の電気通信事業者の領域が自社の領域と同じセキュリティレベルとなるように、他の電気通信事業者との間にセキュリティに関する取決めを行う、また、利用規約等により事前に確認を行うことが望ましい。

9.3.2 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

管理策

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。

電気通信事業者向けの実施の手引

電気通信サービス加入者の領域に設置する自社の設備のセキュリティを確保するため、電気通信事業者は、次の事項を考慮することが望ましい。

- a) 電気通信サービス加入者の領域に設置する自社の設備が容易に開けることができない頑丈な筐体とする
- b)電気通信サービス加入者の領域との分界点を明確にし、容易に切り離せる
- c)遠隔操作によって設備の状態を監視でき、又は操作ができる

関連情報

電気通信サービス加入者の領域は、一般に、電気通信事業者の領域よりセキュリティレベルが低いことから、設備の設置場所については、権限のない者が容易に近づけないところ等、十分に考慮することが望ましい。

9.3.3 相互接続における責任分界の明確化

管理策

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。

電気通信事業者向けの実施の手引

電気通信サービスの提供に問題が発生した場合に、相互に接続している電気通信事業者は、自社の電気通信設備の正常性を確認するための手段を持っていることが望ましい。

自社の電気通信設備の正常性を確認するために、相互接続点において、他の電気通信事業者の電気通信設備との切り離し及び再接続が容易にできることが望ましい。

相互接続点における伝送の状況を常時監視できるようにすることが望ましい。

電気通信サービス加入者からの通信によって、接続している他の電気通信事業者の電気通信サービスの円滑な提供に支障を生じている場合には、当該電気通信サービス加入者からの通信を伝送しないことができる旨を、約款又は契約上で明らかにしておくことが望ましい。

10 通信及び運用管理

10.1 運用の手順及び責任 (ISO/IEC17799 参照)

10.1.1 操作手順書 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

a) ~ h) (略)

i) 特に電気通信事業者にあっては定常の運用手順からインシデント対応手順 (13.2 参照) への移行条件

(中略)

10.1.2 変更管理 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

a) ~ f) (略)

g) 施設の新設・移転・撤去の手順及び記録

(中略)

10.1.3 職務の分離 (ISO/IEC17799 参照)

10.1.4 開発施設、試験施設及び運用施設の分離 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

a) ~ e) (略)

f) (中略)

開発環境、試験環境で使用するデータは、擬似データを使用する。やむを得ず、取扱いに慎重を要する情報を含むデータ(例えば、個人情報、通話記録情報)等を使ったテストを行う場合には、プログラムのバグ、誤操作等の原因により意図しない情報漏洩を防ぐための管理を行う。

この場合のデータの管理は、このデータ生成のために取扱いに慎重を要する情報を含めた業務情報を収集する段階からデータの作成、試験終了後にデータの廃棄までに至るまで、このデータのライフサイクルの中で適切に行う。

g) 開発担当者は、運用システムの管理用パスワードの発行に関する管理策が適切に適用されている場合にだけ、管理者用パスワードを取得する。

管理策ではそのようなパスワードが使用後には変更されることを確実にする。

10.2 第三者が提供するサービスの管理 (ISO/IEC17799 参照)

10.2.1 第三者が提供するサービス (ISO/IEC17799 参照)

10.2.2 第三者が提供するサービスの監視及びレビュー (ISO/IEC17799 参照)

10.2.3 第三者が提供するサービスの変更に対する管理 (ISO/IEC17799 参照)

10.3 システムの計画作成及び受入れ (ISO/IEC17799 参照)

10.3.1 容量・能力の管理 (ISO/IEC17799 参照)

10.3.2 システムの受入れ (ISO/IEC17799 参照)

10.4 悪意のあるコード及びモバイルコードに対する保護 (ISO/IEC17799 参照)

10.4.1 悪意のあるコードに対する管理策 (ISO/IEC17799 参照)

10.4.2 モバイルコードに対する管理策 (ISO/IEC17799 参照)

関連情報

(中略)

(モバイルコードには、)具体的には、埋め込みスクリプト、ActiveX®、Java™などがある。

(モバイルコードは、幾つかのミドルウェアサービスと関係している。)そのため、悪意のあるコードに対する一般的な管理策に加え、ミドルウェアの観点での管理策が必要とされる場合もある。

(中略)

10.5 バックアップ (ISO/IEC17799 参照)

10.5.1 情報のバックアップ (ISO/IEC17799 参照)

10.6 ネットワークセキュリティ管理 (ISO/IEC17799 参照)

10.6.1 ネットワーク管理策 (ISO/IEC17799 参照)

10.6.2 ネットワークサービスのセキュリティ (ISO/IEC17799 参照)

10.6.3 電気通信サービス提供におけるセキュリティ管理

管理策

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。

電気通信事業者向けの実施の手引

電気通信事業者は電気通信サービス加入者に対して、次の事項を実施することが望ましい。

a) セキュリティの特徴、サービスレベル、管理の要求事項を明確にし、電気通信サービス加入者に説明すること。

b) スパムメール、インターネット犯罪、コンピュータウイルス等から電気通信サービス加入者を保護するための啓発活動を行うこと。

電気通信事業者は、電気通信サービス仕様の検討において次の事項を考慮することが望

ましい。

- c) 関連法令（電気通信事業法等）に準拠した管理策の実施。例えば、盗聴防止、他の電気通信事業者との相互接続等。
- d) 特別なサービスレベルが要求される通信の提供。例えば災害時優先通信等（15.1.9 参照）。
- e) 提供するサービス毎によって、例えば、以下のセキュリティ対策の実施。

IP 接続サービス・データセンターサービス

- ・スパムメール対策(10.6.4 参照)
- ・DoS/DDoS 攻撃対策(10.6.5 参照)
- ・脆弱性対策（12.6.1 参照）

電話サービス・携帯電話 PHS サービス

- ・重要通信の優先取扱い
- ・災害時優先電話の確保
- ・輻輳対策

マネージド型サービス

- ・認証 / 暗号化の利用
- ・特権モードの厳重な取扱い

- f) サービス提供上の情報の管理において、以下の項目を厳正に維持するためのセキュリティ対策の実施。
 - ・通信の秘密（通話明細情報を含む）の確保（15.1.7 参照）
 - ・個人情報の保護

また、電気通信事業者は、提供する電気通信サービス維持のために次の対策を実施することが望ましい。

- g) 伝送ケーブルなどの伝送設備の適切な保守。緊急の場合の、できる限り早急な修理の実施。
- h) 電気通信サービスのための交換設備（ルータ、スイッチ、交換機等）の十分な保守。また、交換設備における通信負荷の常時監視。緊急の場合では、深刻なトラフィックの輻輳を回避するために、バックアップ設備又は他のルートへの切り替え。

- i) DoS/DDoS 攻撃等を受けた場合、ルータなどのスイッチ設備は通常の状態と比較して大量のトラフィックを処理しなければならなくなるため、電気通信設備の機能を維持するための方法や手順をあらかじめ備えておくこと。
- j) インターネットの経路情報及び DNS などの制御情報の適切な管理。

関連情報

電気通信サービス事業者は、電気通信サービスの提供に際し、適切でない理由により、電気通信サービス加入者に対して表示画面上において URL 表示を隠蔽するような表示を行ったり、利用者端末においてセキュリティチェック機能の停止または低下を促すような操作を強いることのないよう、電気通信サービス仕様に配慮することが望ましい。

10.6.4 スパムメール対応

管理策

電気通信事業者は、電子メールの利用についての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。

電気通信事業者向けの実施の手引

電気通信事業者が電気通信サービス利用者からの申告を受けてスパムメールの存在を認識し、そのスパムメールの発信者が自社の電気通信サービス加入者であった場合、その電気通信サービス加入者に対し、スパムメールの送信を停止するよう要請することが望ましい。

こうした要請をしたにもかかわらず、電気通信サービス加入者による十分な対応が確認できない場合、または対応が期待できない場合は、当該スパムメールの流入を阻止するために、電気通信役務の提供を拒むことができる（特定電子メールの送信の適正化等に関する法律第 11 条参照）。

電気通信設備を相互に接続している他の電気通信事業者からスパムメールが送られてくる場合、当該他の事業者に対しスパムメールの送信を停止するための措置を要請することが望ましい。また、要請を受けた事業者は、その要請に対し速やかに適切な対応を実施することが望ましい。

スパムメール対応の効果をあげるため、事業者間の緊密な連携、及び国内外のスパムメール対策組織との協調・連携を積極的に行うことが望ましい。

電気通信事業者は、スパムメールに対するポリシーを一般に公開することが望ましい。

10.6.5 DoS/DDoS 攻撃対応

管理策

電気通信事業者は、電気通信サービスの利用についての良好な環境の整備を図るために、DoS/DDoS 攻撃への対応方針を定め、対策を実施することが望ましい。

電気通信事業者向けの実施の手引

電気通信事業者が、電気通信設備に対する DoS/DDoS 攻撃の存在を何らかの手段によって認識した場合は、電気通信設備の安定運用継続のため、適切な対策を講じることが望ましい。

必要とされる具体的な対策については、DoS/DDoS 攻撃の種別によって異なるが、以下のような対策を考慮することが望ましい。

- ・対象被害サイトへのパケットのフィルタリング
- ・DoS/DDoS 攻撃で使用される通信ポートの制限
- ・対象となる電気通信設備の縮退運転、または運転一時停止 など

DoS/DDoS攻撃の発信者が自社の電気通信サービス加入者であることが判明した場合は、電気通信事業者の電気通信設備又は他の電気通信サービス利用者の電気通信設備の機能に障害を与えることを避けるために、電気通信役務の提供停止等の措置を講じることがありうることを、あらかじめ明確化しておくことが望ましい(6.2.2参照)。

電気通信設備を相互に接続している他の電気通信事業者経由の DoS/DDoS 攻撃がある場合、当該他の事業者に対し DoS/DDoS 攻撃の対応するための措置を要請することが望ましい。また、要請を受けた事業者は、その要請に対し速やかに適切な対応を実施することが望ましい。

DoS/DDoS 攻撃対応の効果をあげるため、事業者間の緊密な連携、及び国内外のサイバー攻撃対策組織との協調・連携を積極的に行うことが望ましい。

10.7 媒体の取扱い (ISO/IEC17799 参照)

10.7.1 取外し可能な媒体の管理 (ISO/IEC17799 参照)

10.7.2 媒体の処分 (ISO/IEC17799 参照)

10.7.3 情報の取扱手順 (ISO/IEC17799 参照)

10.7.4 システム文書のセキュリティ (ISO/IEC17799 参照)

10.8 情報の交換 (ISO/IEC17799 参照)

10.8.1 情報交換の方針及び手順 (ISO/IEC17799 参照)

10.8.2 情報交換に関する合意 (ISO/IEC17799 参照)

10.8.3 配送中の物理的媒体 (ISO/IEC17799 参照)

10.8.4 電子的メッセージ通信 (ISO/IEC17799 参照)

10.8.5 業務用情報システム (ISO/IEC17799 参照)

10.9 電子商取引サービス (ISO/IEC17799 参照)

10.9.1 電子商取引 (ISO/IEC17799 参照)

10.9.2 オンライン取引 (ISO/IEC17799 参照)

10.9.3 公開情報 (ISO/IEC17799 参照)

10.10 監視 (ISO/IEC17799 参照)

10.10.1 監査ログ取得 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

(中略)

なお、電気通信事業者が電気通信サービス利用者の通信履歴を取り扱うに当たっては、課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な範囲内で保存期間を定め、当該保存期間経過後又は当該利用目的を達成した後には、通信履歴を遅滞なく消去すること(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10条及び同ガイドラインの解説第23条)。

関連情報

(中略)

通信の秘密の保護上、適切な方策をとることが望ましい(15.1.7 参照)。

(可能な場合には、)(後略)

10.10.2 システム使用状況の監視 (ISO/IEC17799 参照)

10.10.3 ログ情報の保護 (ISO/IEC17799 参照)

10.10.4 実務管理者及び運用担当者の作業ログ (ISO/IEC17799 参照)

10.10.5 障害のログ取得 (ISO/IEC17799 参照)

10.10.6 クロックの同期 (ISO/IEC17799 参照)

11 アクセス制御

11.1 アクセス制御に対する業務上の要求事項 (ISO/IEC17799 参照)

11.1.1 アクセス制御方針 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

(中略)

電気通信事業者においては、利用者の物理的な管理下にある設備（例えば、携帯電話端末、セットトップボックス等）内に存在する資産の所有者の違いを考慮して適切なアクセス権を設定することが望ましい。例えば、携帯電話端末内のアドレス帳は利用者に管理権があるため、そのアクセス権は利用者だけに制限され、携帯電話端末ハードウェアの設計情報及び端末識別情報は利用者のアクセスが禁止されることが望ましい。

11.2 利用者アクセスの管理 (ISO/IEC17799 参照)

11.2.1 利用者登録 (ISO/IEC17799 参照)

11.2.2 特権管理 (ISO/IEC17799 参照)

11.2.3 利用者パスワードの管理 (ISO/IEC17799 参照)

11.2.4 利用者アクセス権のレビュー (ISO/IEC17799 参照)

11.3 利用者の責任 (ISO/IEC17799 参照)

11.3.1 パスワードの利用 (ISO/IEC17799 参照)

11.3.2 無人状態にある利用者装置 (ISO/IEC17799 参照)

11.3.3 クリアデスク・クリアスクリーン方針 (ISO/IEC17799 参照)

11.4 ネットワークのアクセス制御 (ISO/IEC17799 参照)

11.4.1 ネットワークサービスの利用についての方針 (ISO/IEC17799 参照)

11.4.2 外部から接続する利用者の認証 (ISO/IEC17799 参照)

11.4.3 ネットワークにおける装置の識別 (ISO/IEC17799 参照)

11.4.4 遠隔診断用ポート及び環境設定用ポートの保護 (ISO/IEC17799 参照)

11.4.5 ネットワークの領域分割 (ISO/IEC17799 参照)

11.4.6 ネットワークの接続制御 (ISO/IEC17799 参照)

11.4.7 ネットワークルーティング制御 (ISO/IEC17799 参照)

11.4.8 電気通信サービス利用者による電気通信事業者の識別及び認証

管理策

電気通信事業者は、利用者が電気通信事業者を識別し認証する管理策を提供することが望ましい。

電気通信事業者向けの実施の手引

電気通信サービス利用者が遠隔地から、又は無線区間を経由してサービスを使用する場合、事業用電気通信設備のなりすましにより電気通信サービス利用者の通信の秘密が侵されることのないように、電気通信事業者は、電気通信サービス利用者が事業者を識別し認証する管理策を提供することが望ましい。

電気通信事業者は、電気通信サービス利用者が電気通信事業者を認証できない場合に、認証ができない事実及びこれにより想定される一般的なリスクを電気通信サービス利用者に対して注意喚起することが望ましい。

関連情報

識別及び認証の管理策には暗号技術を利用したいくつかの方式を選択することができる。

利用者が事業者を正しく識別及び認証しない場合に想定される脅威の例としては、無線基地局等の偽装による盗聴(Evil Twins)、Web サイトの偽装による不正行為等がある。

11.5 オペレーティングシステムのアクセス制御 (ISO/IEC17799 参照)

11.5.1 セキュリティに配慮したログオン手順 (ISO/IEC17799 参照)

11.5.2 利用者の識別及び認証 (ISO/IEC17799 参照)

11.5.3 パスワード管理システム (ISO/IEC17799 参照)

11.5.4 システムユーティリティの利用 (ISO/IEC17799 参照)

11.5.5 セッションタイムアウト (ISO/IEC17799 参照)

11.5.6 接続時間の制限 (ISO/IEC17799 参照)

11.6 業務用ソフトウェア及び情報のアクセス制御 (ISO/IEC17799 参照)

11.6.1 情報へのアクセス制限 (ISO/IEC17799 参照)

11.6.2 取扱いに慎重を要するシステムの隔離 (ISO/IEC17799 参照)

11.7 モバイルコンピューティング及びテレワーキング (ISO/IEC17799 参照)

11.7.1 モバイルコンピューティング及び通信 (ISO/IEC17799 参照)

11.7.2 テレワーキング (ISO/IEC17799 参照)

12.情報システムの取得、開発及び保守

12.1 情報システムのセキュリティ要求事項 (ISO/IEC17799 参照)

12.1.1 セキュリティ要求事項の分析及び仕様化 (ISO/IEC17799 参照)

12.2 業務用ソフトウェアでの正確な処理 (ISO/IEC17799 参照)

12.2.1 入力データの妥当性確認 (ISO/IEC17799 参照)

12.2.2 内部処理の管理 (ISO/IEC17799 参照)

12.2.3 メッセージの完全性 (ISO/IEC17799 参照)

12.2.4 出力データの妥当性確認 (ISO/IEC17799 参照)

12.3 暗号による管理策 (ISO/IEC17799 参照)

12.3.1 暗号による管理策の利用方針 (ISO/IEC17799 参照)

12.3.2 かぎ(鍵)管理 (ISO/IEC17799 参照)

12.4 システムファイルのセキュリティ (ISO/IEC17799 参照)

12.4.1 運用ソフトウェアの管理 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

運用システムを損なうリスクを最小限に抑えるために、変更を管理する、次の指針を考慮することが望ましい。

a) ~ b) (略)

c) (前略) ルータ、スイッチ、交換機等の十分に注意が必要なシステムに対して、業務用ソフトウェア及びオペレーティングシステムソフトウェアを導入する際には、試験データを用いて実行させるプログラムの実行パスの試験を行う。

d) ~ f) (略)

g) (中略)

仮にそれが、取扱いに慎重を要するアプリケーションソフトウェアである場合には、3世代分のソフトウェアを保持する。

h) (略)

12.4.2 システム試験データの保護 (ISO/IEC17799 参照)

12.4.3 プログラムソースコードへのアクセス制御 (ISO/IEC17799 参照)

12.5 開発及びサポートプロセスにおけるセキュリティ (ISO/IEC17799 参照)

12.5.1 変更管理手順 (ISO/IEC17799 参照)

12.5.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー (ISO/IEC 17799 参照)

12.5.3 パッケージソフトウェアの変更に対する制限 (ISO/IEC17799 参照)

12.5.4 情報の漏えい (ISO/IEC17799 参照)

12.5.5 外部委託によるソフトウェア開発 (ISO/IEC17799 参照)

12.6 技術的ぜい弱性の管理 (ISO/IEC17799 参照)

12.6.1 技術的ぜい弱性の管理策 (ISO/IEC17799 参照)

13 情報セキュリティインシデントの管理

13.1 情報セキュリティ事象及び弱点の報告 (ISO/IEC17799 参照)

13.1.1 情報セキュリティ事象の報告 (ISO/IEC17799 参照)

13.1.2 セキュリティ弱点の報告 (ISO/IEC17799 参照)

13.2 情報セキュリティインシデントの管理及びその改善 (ISO/IEC17799 参照)

13.2.1 責任及び手順

電気通信事業者向けの実施の手引

(中略)

e) 電気通信サービス加入者や情報処理施設の利用者に関する事項は、より上位の対処事項とする。当該事項には、ハードウェアの故障、ネットワーク障害といった既存の電気通信サービス加入者の情報管理に関する事項、電気通信サービス加入者と情報処理施設の利用者の両方に影響を及ぼす企業の情報管理に関する事項が含まれる。

すべての電気通信サービス加入者や情報処理施設の利用者に対して、関連書類等によってそれぞれのエスカレーション手順を知らせる。

例えば、電気通信サービス加入者や情報処理施設の利用者に関する事項は、以下に従い、優先付けすることができる。

- 1) 電気通信サービス加入者のサイトが完全に停止、または SLA の要求を満たしていない。
- 2) 電気通信サービス加入者のサイトが停電により深刻な影響を受けようとしている。
 - 1 ないしそれ以上のシステムがダウンしているか、相当なパケットの喪失または/かつ遅延が生じている。
- 3) 電気通信サービス加入者へのサービスの品質低下
- 4) 電気通信サービス加入者からの要請

f) 電気通信事業者においては、必要な場合には、関係する電気通信サービス加入者に対し、直接、電子メールやホームページを通じて、インシデントを迅速に報告する。

関連情報

電気通信事業者は、情報セキュリティインシデントに関する情報を、Telecom-ISAC Japan 等の情報共有・分析を行う組織を通じて共有することが望ましい。

13.2.2 情報セキュリティインシデントからの学習 (ISO/IEC17799 参照)

13.2.3 証拠の収集 (ISO/IEC17799 参照)

14 事業継続管理

14.1 事業継続管理における情報セキュリティの側面 (ISO/IEC17799 参照)

14.1.1 事業継続管理手順への情報セキュリティの組み込み (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

a) ~ f) (略)

g) 情報処理施設の管理運用に関わる人員の安全を確保するとともに、情報処理設備、特に電気通信設備及び組織の資産の保護を確実にする。

h) ~ j) (略)

14.1.2 事業継続及びリスクアセスメント (ISO/IEC17799 参照)

14.1.3 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 (ISO/IEC17799 参照)

電気通信事業者向けの実施の手引

(中略)

電気通信事業者における事業継続計画の策定においては、電気通信サービスの応急復旧対策も組み入れることが望ましい。

電気通信事業者における事業継続計画の策定においては、電気通信サービス加入者の重要通信の確保も考慮することが望ましい。

(中略)

関連情報

(中略)

自社の電気通信設備が損害を受けなくても、隣接する建物や空間が不可抗力により損害を受けたり立ち入りが規制されることにより、自社の電気通信設備を実質的に利用できなくなる可能性がある。その場合の対応についても考慮することが望ましい。

14.1.4 事業継続計画策定の枠組み (ISO/IEC17799 参照)

14.1.5 事業継続計画の試験、維持及び再評価 (ISO/IEC17799 参照)

15 順守

15.1 法的要求事項の順守 (ISO/IEC17799 参照)

15.1.1 適用法令の識別 (ISO/IEC17799 参照)

15.1.2 知的財産権 (IPR) (ISO/IEC17799 参照)

15.1.3 組織の記録の保護 (ISO/IEC17799 参照)

15.1.4 個人データ及び個人情報の保護 (ISO/IEC17799 参照)

15.1.5 情報処理施設の誤用防止 (ISO/IEC17799 参照)

15.1.6 暗号化機能に対する規制 (ISO/IEC17799 参照)

15.1.7 通信の秘密

管理策

電気通信事業者は、通信の秘密を守らなければならない(電気通信事業法第4条)。

電気通信事業者向けの実施の手引

電気通信事業者は、次の措置を講じることが望ましい。

- a) 通信の秘密が侵されないように、事業用電気通信設備を維持すること(電気通信事業法第41条第1項及び第3項第3号電子通信分野における個人データ処理及びプライバシーの保護に関する欧州議会及び欧州理事会指令(以下、単に「EU指令」という。)第4条)。
- b) 事業用電気通信設備は、電気通信サービス利用者が端末設備を接続する点において、他の通信の内容が電気通信設備の通常の使用の状態では判読できないように必要な秘匿措置を講じること(事業用電気通信設備規則第17条)。
- c) 事業用電気通信設備に電気通信サービス利用者の通信の内容その他これに係る情報を蓄積する場合にあっては、当該電気通信サービス利用者以外の者が端末設備を用いて容易にその情報を知得し、又は破壊することを防止するため、当該電気通信サービス利用者だけに与えた識別符号の照合確認その他の防止措置を講じること(事業用電気通信設備規則第18条)。
- d) 通信当事者の同意がある場合又は違法性阻却事由がある場合(注1)を除いては、通信の秘密に属する事項(注2)を利用しないこと(電気通信事業法第4条、刑法第35条～第37条、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6条第4項)。

(注1) 違法性阻却事由がある場合とは、裁判官の発付した令状に従う場合、現に犯罪をおかしている者が存在し被害者及び捜査機関からの要請により逆探知を行う場合、人の生命や身体等に差し迫った危険がある旨の緊急通報がある場合において当該通報先からの要請により逆探知を行う場合その他の正当行為、正当防衛又は緊急避難に該当する場合をいう。

(注2) 通信の秘密に属する事項とは、通信内容にとどまらず、通信当事者の住所・氏名、発受信場所及び通信日時等通信の構成要素並びに通信回数等通信の存在の事実の有無を含む。

- e) 電気通信サービス利用者の通信履歴（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係る情報であって通信内容以外のものをいう。）を取り扱うに当たっては、原則として利用目的に必要な範囲内で保存期間を定め、当該保存期間経過後又は当該利用目的を達成した後は、通信履歴を遅滞なく消去すること（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条第1項及び同ガイドライン解説第23条の解説（5））。
- f) 通信当事者の同意がある場合又は違法性阻却事由がある場合を除いては、通信の秘密に属する事項を他人に提供しないこと（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条第2項）。
- g) 発信者情報通知サービス（発信電話番号、発信者の位置を示す情報等発信者に関する情報を受信者に通知する電話サービス）を提供する場合には、通信ごとに、発信者情報の通知を阻止する機能を設けること（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25条第1項）。
- h) 通信当事者の同意がある場合又は違法性阻却事由がある場合を除いては、発信者情報を他人に提供しないこと（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25条第3項）。
- i) 電気通信サービス加入者の電気通信番号の案内に係る業務を行う場合は、電気通信サービス加入者に対し、電気通信番号の案内を省略するかどうかの選択の機会を与え、電気通信サービス加入者が省略を選択したときは、遅滞なく当該電気通信サービス加入者の電気通信番号に係る情報を案内業務の対象から除外すること（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28条第1項）。
- j) 法執行機関から、通信の秘密に属する事項その他電気通信サービス利用者に係る情報の提供を求められた場合には、法令に適合した手続きに従った要請であることを確認すること（電気通信事業における個人情報保護ガイドライン第28条第1項）。

15.1.8 重要通信の確保

管理策

電気通信事業者は、天災、事変その他の非常事態が発生し、又は発生するおそれがあるときは、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）を優先的に取り扱わなければならない（電気通信事業法第8条第1項）。

電気通信事業者向けの実施の手引

電気通信事業者は、次に掲げる機関が重要通信を行うため、他の通信の接続を制限又は停止することを考慮すること（電気通信事業法第8条第2項及び電気通信事業法施行規則第56条）。

- a) 気象機関
- b) 水防機関
- c) 消防機関
- d) 災害救助機関
- e) 秩序の維持に直接関係がある機関
- f) 防衛に直接関係がある機関
- g) 海上の保安に直接関係がある機関
- h) 輸送の確保に直接関係がある機関
- i) 通信役務の提供に直接関係がある機関
- j) 電力の供給に直接関係がある機関
- k) 水道の供給に直接関係がある機関
- l) ガスの供給に直接関係がある機関
- m) 選挙管理機関直接関係がある機関
- n) 新聞社等の機関直接関係がある機関
- o) 金融機関
- p) その他重要通信を取り扱う国または地方公共団体の機関

電気通信事業者は、重要通信の円滑な実施を確保するため、他の電気通信事業者と電気通信設備を相互に接続する場合には、重要通信の優先的な取扱いについて取り決めることその他の必要な措置を講じること（電気通信事業法第8条第3項）。

15.1.9 緊急時態対応の適法性確保

管理策

電気通信事業者が緊急事態においてとる措置は、正当防衛又は緊急避難として必要かつ十分な措置にとどめ、過剰なものであってはならない。

電気通信事業者向けの実施の手引

電気通信事業者は、情報セキュリティインシデントを含む緊急事態対応について、あらかじめ手順を定め、緊急事態において採る措置が、正当防衛又は緊急避難として必要かつ十分であり、過剰なものとなっていないか等について法令の専門家の助言を仰ぐことが望ましい。

電気通信事業者は、電気通信サービス加入者の電気通信設備との接続が、電気通信事業者の電気通信設備又は他の電気通信サービス利用者の電気通信設備の機能に実際に障害を与えている場合、又は他人の人体に危害を及ぼし若しくは物件に損傷を与える場合には、正当防衛行為又は緊急避難行為として、当該電気通信サービス加入者に対する電気通信サービスの提供を拒む等、通常とは異なる対応を採ることがあり得る旨を、あらかじめ電気通信サービス加入者に周知することが望ましい。

15.2 セキュリティ方針及び標準へのコンプライアンス並びに技術的コンプライアンス (ISO/IEC17799 参照)

15.2.1 セキュリティ方針及び標準の順守 (ISO/IEC17799 参照)

15.2.2 技術的順守の点検 (ISO/IEC17799 参照)

15.3 情報システム監査に対する考慮事項 (ISO/IEC17799 参照)

15.3.1 情報システム監査に対する管理策 (ISO/IEC17799 参照)

15.3.2 情報システム監査ツールの保護 (ISO/IEC17799 参照)

Annex. A 情報セキュリティマネジメントに関する文書体系

情報セキュリティマネジメントに関する文書体系は一般的に以下に示すような階層構造をとることが多い。最上位には、組織全体としての情報セキュリティ対策における根本的な考え方である「基本方針」がある。これに従い、順に「対策基準」及び「実施手順」がある。

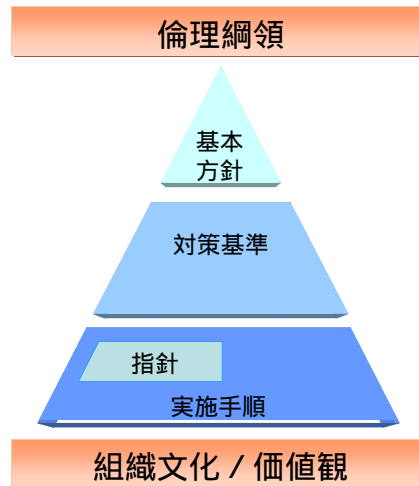


図 情報セキュリティマネジメントに関する文書体系

(1) 基本方針

資産のセキュリティ確保のため、組織としての基本方針を表明するもので、セキュリティ関連文書の頂点に位置する。

(2) 対策基準

組織の情報セキュリティに関する対策基準で、基本方針を実行に移すための具体的な対策を記述する。

(3) 指針（ガイドライン）

基本方針や対策基準といった上位のセキュリティ関連文書に準拠したより具体的な対策例を記述する。

(4) 実施手順

基本方針や対策基準、指針といった上位のセキュリティ関連文書に準拠し、より具体的な手順や操作方法等を記述する。

Annex. B 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を利用する上での参考情報

1. 電気通信事業とは

電気通信事業とは、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である。

電気通信サービスとは、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をいう。(2.用語及び定義 を参照)

2. 利害関係者

電気通信事業者は、組織における情報セキュリティを管理するため、電気通信事業者組織内の情報処理施設の利用者、電気通信サービスの利用者、電気通信サービスの加入者等といった利害関係者を識別する必要がある。

(1) 電気通信事業者組織内における情報処理施設の利用者

電気通信事業者内の情報処理施設等の利用者については、役員及び従業員、契約相手、第三者の利用者の3つに分類できる。

- a) 従業員とは、組織と直接、雇用契約を結び、職務に従事する者をいう。
- b) 契約相手とは、電気通信事業者と直接契約関係にある契約相手の企業(請負会社、人材派遣会社など)及びその契約相手の企業を仲介して組織の内若しくは外で職務に従事する者をいう。例えば、通信センタ等におけるネットワークの運用・管理業務について、請負契約により派遣された者、電気通信設備のメンテナンスについて、請負契約により派遣された者などが挙げられる。
- c) 第三者の利用者とは、電気通信事業者とは直接の契約関係にはない従業員及び契約相手以外の者(訪問者など)である。例えば、電気通信事業者が入居する建物の清掃業務に従事する者、電気通信事業者との打合せ等で来社する者等が挙げられる。

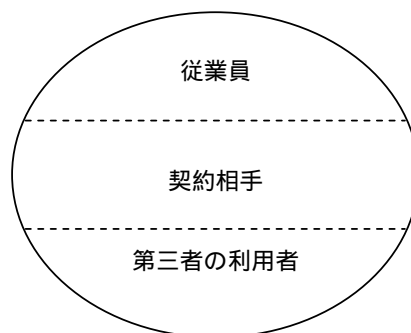


図 電気通信事業者組織内における情報処理施設の利用者

(2) 電気通信事業者が提供するサービスの利用者

電気通信事業者が提供するサービスの利用者については、電気通信サービス加入者、電

電気通信サービス利用者、電気通信サービス以外のサービス利用者の3つに分類できる。

- a) 電気通信サービス加入者は、電気通信事業者の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。
- b) 電気通信サービス利用者は、電気通信サービスを利用する者をいう。
- c) 電気通信サービス以外のサービス利用者とは、電気通信事業者が提供するサービスのうち、電気通信サービス以外のサービスを利用する者をいう。

(3) 電気通信サービス加入者と電気通信サービス利用者との関係

自社を電気通信事業者 A とした場合、電気通信事業者 A と電気通信サービスの提供に係る契約を締結している者が、電気通信サービス加入者となる。また、電気通信事業者 A と相互接続をしている電気通信事業者 B と電気通信サービスの提供に係る契約を締結した加入者は、電気通信事業者 A から見れば、電気通信サービス利用者となる。

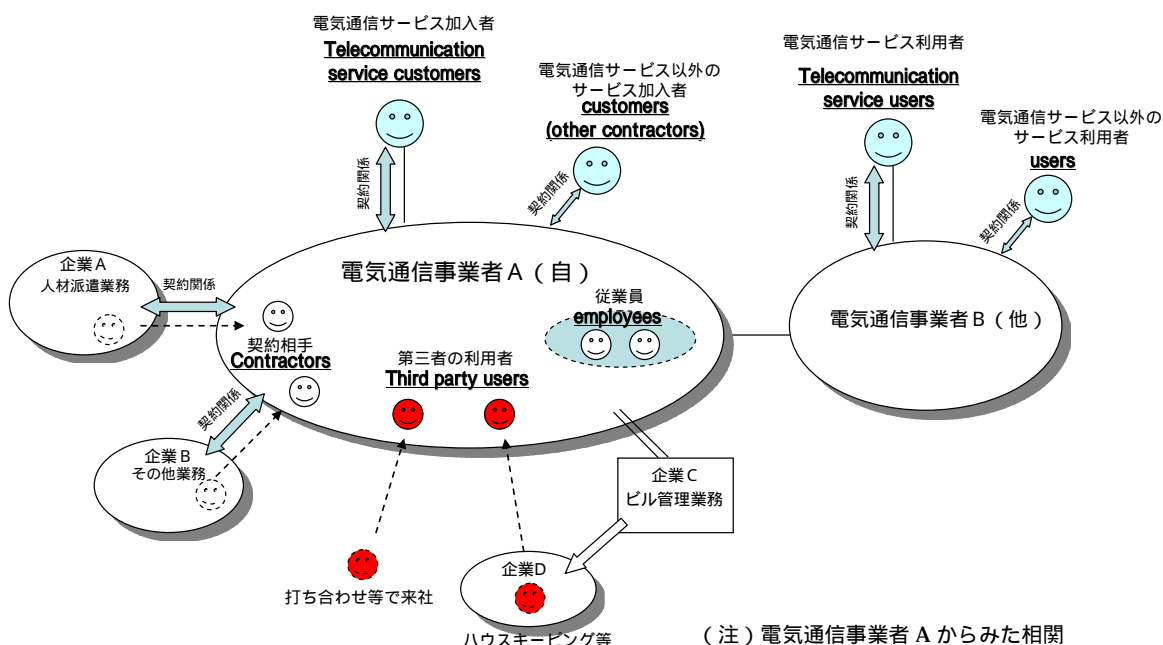


図 電気通信事業者を取り巻く利害関係