TTC標準
Standard

JT-X1051

情報技術 ― セキュリティ技術 ― ISO/IEC 27002 に基づく 電気通信事業者のための 情報セキュリティ管理策の 実践のための規範

Information technology – Security techniques –
Code of practice for information security controls
based on ISO/IEC 27002
for telecommunications organizations

第 1 版

2018 年 2 月 15 日制定

一般社団法人

情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

目次

<参考>

１．　国際勧告等との関係

本標準は、電気通信事業者において情報セキュリティ管理策を実施するにあたってのガイドラインを規定しており、2016 年 4 月に発行された ITU-T 勧告 X.1051 に準拠している。

２．　上記国際勧告等に対する追加項目等

本標準に関連する国際標準（X.1051）に対するオプション選択項目、国内仕様として追加した項目、原標準に対する変更項目は無い。

３．　改版の履歴

版　数	改　訂　日	改　版　内　容
1	2018 年 2 月 15 日	制定

４．　工業所有権

本標準に係る「工業所有権等の実施に係る確認書」の提出状況は TTC のホームページでご覧になれます。

５．　その他

(1) 参照する主な勧告、標準

本文中に記載する。

６．　標準作成部門

第 1 版：セキュリティ専門委員会（WG2100）

1　適用範囲

本標準は、電気通信事業者において情報セキュリティ管理策を実施するにあたってのガイドラインを規定するものである。

本標準を利用して情報セキュリティマネジメントシステムを実施することによって、電気通信事業者は、機密性、完全性、可用性、及びその他のセキュリティ特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　引用規格

以下の国際規格は、本文中に引用されることによって、この標準の一部を構成する。本書の出版時において、以下の版が有効であった。すべての勧告及び国際規格は改定されることがあり、本標準に基づいて契約を行う関係者は、以下にある国際規格の最新版を適用する可能性について検討することが推奨される。

- ISO/IEC 27000, *情報技術– セキュリティ技術–情報セキュリティマネジメントシステム– 概要及び用語*
- ISO/IEC 27002:2013, *情報技術–セキュリティ技術–情報セキュリティ管理策のための実践の規範*

3　定義及び略語

3.1　定義

本標準では、ISO/IEC 27000及び以下において与えられる定義を適用する。

3.1.1 コロケーション

他の電気通信事業者の施設内に電気通信設備を設置すること。

3.1.2 通信センター

電気通信事業を提供するための電気通信設備を収容する施設。

3.1.3 重要通信

災害の予防もしくは救援、及び悪条件下における秩序維持のために必要な事項を内容とする通信。

注：日本では、電気通信事業法第八条にて定義されている。

3.1.4 通信の秘密保持

通信の存在、通信内容、発信者（送信元）、着信者（宛先）、及び通信日時を非開示とする要件。

3.1.5 優先電話

緊急事態における特定の端末による電気通信で、一般の通話を規制することにより、優先的に処理されるべき電話。

注：その特定の端末は有線・無線ネットワークにおいて様々なサービス（VoIP、公衆交換電話網(PSTN)上の音声通信、IPデータトラフィックなど）にまたがることがある。

3.1.6 電気通信アプリケーション

エンドユーザにより使用され、ネットワークベースのサービスとして構築されるVoIPなどのアプリケーション。

3.1.7 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。

注：日本では、電気通信事業法第二条にて定義されている。

3.1.8 電気通信機器室

電気通信事業を提供するための装置が設置される建物内の安全な場所又は部屋。

3.1.9 電気通信設備

電気通信を行うための機械、器具、線路その他の電気的設備。

注：日本では電気通信事業法第二条にて定義されている。

3.1.10　電気通信事業者

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主体。

3.1.11 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。

注：日本では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三十二条にて定義されている。

3.1.12　電気通信サービス

電気通信設備を用いた通信、又は他の通信手段を用いた、電気通信サービス利用者若しくは電気通信サービス加入者の間で提供される通信。

3.1.13　電気通信サービス加入者（顧客）

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、又は組織。

注：日本では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三条の五にて定義されている。

3.1.14　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、又は組織。

注：日本では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三条の四にて定義されている。

3.1.15　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。

注：日本では電気通信事業法第五十二条にて定義されている。

3.1.16　利用者

自社の情報処理設備又はシステムを利用する者、又は組織。例えば、従業員、契約相手及び第三者の利用者を指す。

3.2　略語

本標準では、以下の略語を適用する。

CIA	Confidentiality, Integrity and Availability（機密性、完全性及び可用性）
DDoS	Distributed Denial of Service（分散サービス妨害）
DNS	Domain Name System（ドメイン名システム）
DoS	Denial of Service（サービス妨害）
HVAC	Heating, Ventilation, and Air Conditioning（暖房、換気及び空調）
IP	Internet Protocol（インターネットプロトコル）
IRC	Internet Relay Chat（インターネットリレーチャット）
ISAC	Information Sharing and Analysis Centre（情報共有分析センター）
ISMS	Information Security Management System （情報セキュリティマネジメントシステム）

NMS	Network Management System（ネットワークマネジメントシステム）
OAM & P	Operations, Administration, Maintenance and Provisioning （運用、実務管理、維持及び提供）
PSTN	Public Switched Telephone Network（公衆交換電話網）
SIP	Session Initiation Protocol（セッション開始プロトコル）
SLA	Service Level Agreement（サービス品質保証）
SMS	Short Message Service（ショートメッセージサービス）
SOA	Statement of Applicability（適用宣言書）
URL	Uniform Resource Locator（ユニフォームリソースロケータ）
VoIP	Voice over Internet Protocol（ボイスオーバーIP）

4　概要

4.1　本標準の構成

本標準は、ISO/IEC 27002と同様なフォーマットで構成されている。ISO/IEC 27002に記載される目的、管理策に追加の情報が不要な場合は、ISO/IEC 27002への参照のみが記載されている。電気通信分野における固有の管理策、実施の手引きについては、附属書A（Normative）に記載される。

電気通信事業に特化した補足的な手引きが必要な管理策の場合は、ISO/IEC 27002の管理策をそのまま掲載することとし、その後にその管理策に関連する電気通信事業者向けの手引きを記載する。電気通信分野向けの手引きや関連情報は、以下の章に含まれている。

- 情報セキュリティのための組織（第6章）
- 人的資源のセキュリティ（第7章）
- 資産の管理（第8章）
- アクセス制御（第9章）
- 物理的及び環境的セキュリティ（第11章）
- 運用のセキュリティ（第12章）
- 通信のセキュリティ（第13章）
- システムの取得、開発及び保守（第14章）
- 供給者関係（第15章）
- 情報セキュリティインシデント管理（第16章）
- 事業継続マネジメントにおける情報セキュリティの側面（第17章）

4.2　電気通信事業者における情報セキュリティマネジメントシステム

4.2.1 目標

あらゆる組織にとって情報は重要である。電気通信の場合、情報は任意の2点間で電子的に伝送されるデータに加えて、送信者及び受信者の位置データなどのメタデータから構成される。情報がどのように伝送されるか、また伝送中にキャッシュされたり保存されたりするかに関わらず、情報は常に適切に保護されることが望ましい。

電気通信事業者とその情報システム及びネットワークは、盗聴、高度かつ執拗な脅威（APT: Advanced Persistent Threat）、テロリズム、スパイ行為、妨害行為、破壊行為、情報漏洩、誤り及び不可抗力の事態を含む広範囲にわたる原因によるセキュリティ脅威にさらされている。これらのセキュリティ脅威は、電気通信事業者の内部又は外部から引き起こされるもので、結果として組織に損害を与えることになる。

電気通信回線の盗聴などにより一度情報セキュリティが破られると、その組織は損害を被る可能性がある。したがって、情報セキュリティマネジメントシステム（ISMS）の継続的改善により、組織が情報セキュリティを確保することは不可欠である。

本標準内に記述される管理策に基づいて適切な管理策を導入することにより、効果的な情報セキュリティを確保することができる。これらの管理策は、電気通信設備、サービス、業務用アプリケーションにおいて、確立され、実施され、監視され、レビューされ、改善される必要がある。これらの活動により、組織はそのセキュリティ目的及びそれを通じて事業目的を満たすことが可能となる。

電気通信事業者はさまざまなタイプの利用者に対して、情報を処理し、伝送し、保存するための設備を提供する。この情報は個人を特定できる情報や、機微な個人又は業務データの場合がある。あらゆる場合において情報は正しいレベルの配慮と注意、及び、プライバシーと機微性を最優先として機密性、完全性、可用性（CIA）を確保するために提供される適切なレベルの保護により取り扱うことが望ましい。

4.2.2 電気通信において必要なセキュリティの考慮

電気通信における一般的なセキュリティフレームワークの要求事項は、さまざまな要因に由来してきた。

a) 大惨事におけるサービスの可用性（特に緊急サービス）を含め、提供されるネットワーク及びサービスの信頼性に対する顧客又は加入者の要請

b) サービスの可用性、公平な競争、及びプライバシー保護を確実なものとするために、訓令、規制、法令によるセキュリティに対する公的機関の要請

c) 運用及び事業利益を保護し、顧客及び国民に対する責務を果たすことを目的として、セキュリティに対するネットワーク運用者及びサービス提供者自身の要請

更に、電気通信事業者は、次のような環境的、及び運用的なセキュリティインシデントを考慮することが望ましい。

a) 電気通信サービスは、ルータ、交換機、ドメインネームサーバ、転送リレーシステム、ネットワーク管理システム（NMS）などの相互接続された設備に強く依存している。したがって、電気通信におけるセキュリティインシデントは、様々な装置／設備で発生しうるものであり、そのインシデントは、ネットワークを経由して他の装置／設備に瞬く間に伝播する恐れがある。

b) 電気通信設備に加えて、ネットワークプロトコル、及びネットワークトポロジーのぜい弱性により、深刻なセキュリティインシデントが生まれる可能性もある。特に有線と無線ネットワークの融合により、相互運用性を確保できるプロトコルを開発する重要な試みも必要となってくる。

c) 電気通信事業者の主要な懸念事項は、ネットワークの停止時間を引き起こすセキュリティ侵害の可能性である。このようなネットワークの停止は、顧客との関係、収入減、及び復旧コストの観点から極めて高コストとなりうる。国の電気通信インフラの可用性に対する意図的な攻撃は、国家のセキュリティ問題とみなすことができる。

d) 電気通信事業者のマネジメントネットワーク及びシステムは、ハッカーの侵入を受けやすい。そのような侵入のための共通な動機は、電気通信サービスを対象とした窃盗行為である。このような窃盗行為は、診断機能を呼び出し、会計記録を改ざんし、プロビジョニング・データベースを改変し、加入者通話を盗聴するなどの様々な方法により、巧みに実装されている。

e) 外部からの侵入に加えて、事業者は、ネットワーク管理データベースの不正な改ざんや権限の無い人による設定変更などの内部から発生するセキュリティ侵害を懸念している。このような事態は偶発的あるいは恣意的に起こる。

f) 電気通信サービスはワームやウィルスなどの末端システムや通信インフラストラクチャを攻撃するマルウェアにより破壊される場合がある。DoS/DDoSは通信インシデントの主要原因であり、通信信号を遮断や阻止、又は過負荷を起こさせるために同時に何百ものシステムからひとつのシステムやネットワークに対してデータを送り込むなどの種々の方法により引き起こされる場合がある（附属書A TEL 13.1.6を参照）。

様々な電気通信環境における異なる不正の発生源から電気通信事業者における情報資産を保護するためには、電気通信事業のためのセキュリティガイドラインが、電気通信事業者における情報セキュリティマネジメントの導入において不可欠である。

このセキュリティガイドラインは、以下に対して適用することが望ましい。

a) 利害関係者（供給者、顧客、監督機関など）からの情報セキュリティ要求事項を満足するような信用を追及する電気通信事業者

b) ISMSの実施を通して、ビジネスの優位性を追求する電気通信事業者

c) 電気通信産業のための情報セキュリティに関連する製品及びサービスの利用者及び供給者

d) ISO/IEC 27001の要求事項への適合のために、ISMSの評価、及び監査を実施する電気通信事業者の内部又は外部担当者

e) 事業者に適切なISMSに関する助言又は訓練を与える、電気通信事業者の内部又は外部担当者

f) 国境を越えた法規制の要求事項の遵守、及び、運用を行う若しくは通過する全ての国の法的要件への適合を確実にすること

4.2.3 保護されるべき情報資産

情報セキュリティマネジメントを確立するためには、事業者が組織に関するすべての資産を明確にし、識別することが不可欠である。資産の属性を分類し、資産の重要性を考慮することは、適切な管理策を実施することを可能とする。

電気通信事業者が保護するべき情報資産は8.1.1節に記載されている。

4.2.4 情報セキュリティマネジメントの確立

4.2.4.1 セキュリティ要求事項の確立方法

電気通信事業者にとって、セキュリティ要求事項を識別することは極めて重要なことである。セキュリティ要求事項は以下の3つの要因によって導き出せる。

a) 組織全体における事業戦略及び事業目的を考慮して、通信事業者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を特定し、事故に対するぜい弱性及び事故の可能性を評価し、潜在的な影響を推定する。

b) 電気通信事業者が満たさなければならない法令、規則及び契約上の要求事項、国境を越えた法規制対応並びにその社会文化的環境。特に電気通信事業者のための法令的要求事項の例として、通信の秘密（附属書A TEL.18.1.6）及び重要通信の確保（附属書A TEL.18.1.7）がある。社会文化的要求事項の例としては、多くの手段により送信され、中継され、受信される通信の完全性確保、認可された人間によって運用される固定又は無線電気通信設備の可用性、及び他の電気通信設備に対して危害を与えないことなどがある。

c) 電気通信事業者がその運用を支え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。

4.2.4.2　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、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。管理策のための支出は、セキュリティ障害に起因する事業損害に対してバランスが取れている必要がある。リスクアセスメントの結果は、次のことを導き、決定することに役に立つ。

- 適切な管理活動
- 情報セキュリティリスクの管理の優先順位
- これらの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

リスクアセスメントの結果に影響を及ぼす可能性がある変化に対応するため、リスクアセスメントは最低でも年に1度、定期的に繰り返すことが望ましい。

4.2.4.3　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とするように、管理策を選択し実施することが望ましい。

本標準は、一般的な情報セキュリティマネジメントに加え、電気通信事業者に特化した要求事項を考慮して、補足的な手引き及び電気通信に固有の管理策を提供する。したがって、電気通信事業者は本標準から管理策を選定して実施することが推奨される。また、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、リスク受容基準、リスク対応における選択肢、及び当該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を基に下した組織的な判断に依存するものであり、その選択はすべての関連する国内外の法令及び規則にも従うことが望ましい。

5　情報セキュリティのための方針群

ISO/IEC 27002 第5章の管理目的及び内容を適用する。

注：電気通信固有の法令及び規則の要求事項及び、それらに適合し証拠を残す方法に関する要求事項を考慮することが必要となる可能性がある。

6　情報セキュリティのための組織

6.1　内部組織

目的：組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立するため。

6.1.1 情報セキュリティの役割及び責任

管理策

全ての情報セキュリティの責任を定め、割り当てることが望ましい。

実施の手引き

ISO/IEC 27002 6.1.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信インフラに対する全てのリスクへの責任を持ち、そのリスク管理責任を持つ執行責任者を任命することが望ましい。

電気通信事業者は事業用電気通信設備の設置、保守、運用に関する事項の監督責任者として、正式の資格又は適切な知識と技能を持つ電気通信技術者及びその他の要員を任命することが望ましい。電気事業技術者及びその他の要員は、割り当てられた役割及び責任を伝えられ、正式に合意していることが望ましい。

暗号が使用される場合、暗号管理に特化した役割を設け、この担当者は暗号の管理と暗号システムの利

用と保護に関して適切な訓練を受けることが望ましい。

関連情報

ISO/IEC 27002 6.1.1の関連情報を適用する。

6.1.2 職務の分離

ISO/IEC 27002 6.1.2の管理策及び内容を適用する。

6.1.3 関係当局との連絡

管理策

関係当局との適切な連絡体制を維持することが望ましい。

実施の手引き

ISO/IEC 27002 6.1.3の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者が、電気通信サービス利用者に関連する情報について、法執行機関又は捜査機関から照会を受けた場合には、電気通信事業者は情報を開示する前に、その照会が国の法規制に沿った正当な手順及び手続に則っていることを確認する必要がある。

電気通信事業者のアプリケーション及びインフラストラクチャは、重要インフラストラクチャの一部と考えることができ、地域、社会、経済の全体的な機能に不可欠な場合がある。したがって、このようなシステムの運用者である電気通信事業者は、全ての関連当局と連絡体制を維持しておくことが望ましい。

関連情報

ISO/IEC 27002 6.1.3の関連情報を適用する。

6.1.4 専門組織との連絡

ISO/IEC 27002 6.1.4の管理策及び内容を適用する。

6.1.5 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 6.1.5の管理策及び内容を適用する。

6.2　モバイル機器及びテレワーキング

ISO/IEC 27002 6.2の管理目的及び内容を適用する。

7　人的資源のセキュリティ

7.1　雇用前

目的：従業員及び契約相手がその責任を理解し、求められている役割にふさわしいことを確実にするため。

7.1.1 選考

管理策

全ての従業員候補者についての経歴などの確認は、関連する法令、規則及び倫理に従って行うことが望ましい。また、この確認は、事業上の要求事項、アクセスされる情報の分類及び認識されたリスクに応じて行うことが望ましい。

実施の手引き

ISO/IEC 27002 7.1.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、従業員に対して取扱いに慎重を要する情報へのアクセスを与える職位の候補者については、詳細な確認を考慮することが望ましい。集約の結果として取り扱いに注意を要する状態になり得

るデータへの無制限なアクセスを提供することになるため、電気通信設備又は通信情報への従業員のアクセスを与える職位に対しても適用されることが望ましい。

7.1.2 雇用条件

管理策

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することが望ましい。

実施の手引き

ISO/IEC 27002 7.1.2の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者が考慮すべき通信の秘密及び重要通信の確保に関連する法的な権利及び責任は、法律及び規制の中に含まれる。

電気通信事業者は、個人を特定できる情報やその他の機密情報の保護と非開示に加えて、電気通信事業者が提供する通信サービスを維持することに対する責任を雇用条件の中で明確にし、記載することが望ましい。

電気通信事業者は、その電気通信サービスに従事する者全てに、以下の内容に関して、最新の状態で認識していることを確認することが望ましい。

a) サービスの利用者の個人を特定できる情報及び、その他の秘密情報を保護する責任

b) 電気通信サービスの運用業務を通じて特権的に得られた情報の非開示に関する責任

関連情報

ISO/IEC 27002 7.1.1の関連情報を適用する。

7.2 雇用期間中

ISO/IEC 27002 7.2の管理目的及び内容を適用する。

7.3 雇用の終了及び変更

ISO/IEC 27002 7.3の管理目的及び内容を適用する。

8 資産の管理

8.1 資産に対する責任

目的：組織の資産を特定し、適切な保護の責任を定めるため。

8.1.1 資産目録

管理策

情報及び情報処理施設に関連する資産を特定することが望ましい。また、これらの資産の目録を、作成し、維持することが望ましい。

実施の手引き

ISO/IEC 27002 8.1.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

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、接続している又は、関連する他の電気通信事業者の電気通信設備との責任が明確になるよう識別し、文書化することが望ましい。

資産のリストは、ネットワーク設備、ネットワークサービス、業務用ソフトウェアのための情報資産を含む、あらゆる価値のある電気通信資産を分かりやすく網羅していることが望ましい。

関連情報

ISO/IEC 27002 8.1.1の関連情報を適用する。

8.1.2 資産の管理責任

ISO/IEC 27002 8.1.2の管理策及び内容を適用する。

8.1.3 資産利用の許容範囲

ISO/IEC 27002 8.1.3の管理策及び内容を適用する。

8.1.4 資産の返却

ISO/IEC 27002 8.1.4の管理策及び内容を適用する。

8.2　情報分類

目的： 組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にするため。

8.2.1 情報の分類

管理策

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、分類することが望ましい。

実施の手引き

ISO/IEC 27002 8.2.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

情報を分類するに当たっては、組織における取扱に慎重を要する情報及び重要情報のための一般要求事項に加え、電気通信事業者として以下の事項も考慮することが望ましい。

a) 情報が法的に規定された開示要求の対象となる可能性がある場合

b) 緊急時又は緊急事態となる可能性がある場合に優先的に取り扱う必要のある重要通信に関する情報と、非重要通信に関する情報との区別（附属書A TEL18.1.7参照）

c) 大量のデータを検索することにより、分類された情報又は取扱いに慎重を要する情報が推測できる、集約による影響の認識

関連情報

ISO/IEC 27002 8.2.1の関連情報を適用する。

8.2.2 情報へのラベル付け

ISO/IEC 27002 8.2.2の管理策及び内容を適用する。

8.2.3 資産の取扱い

ISO/IEC 27002 8.2.3の管理策及び内容を適用する。

8.3　媒体の取扱い

ISO/IEC 27002 8.3の管理目的及び内容を適用する。

9　アクセス制御

9.1　アクセス制御に対する業務上の要求事項

目的：情報及び情報処理施設へのアクセスを制限するため。

9.1.1 アクセス制御方針

管理策

アクセス制御方針は、業務上及び情報セキュリティの要求事項に基づいて確立し、文書化し、レビューすることが望ましい。

実施の手引き

ISO/IEC 27002 9.1.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、限られた数のプロファイル及び制御された利用者アクセス許可のセットを適用可能な、ロールベースアクセス制御を導入することが望ましい。

通信会社は、同じセキュリティ機能や規格をサポートしていない可能性のある供給者に恒常的に接触するため、全てのアクセスに対して改善と時機を失しない削除を行うための追跡を確実にすることが重要となる。

許可されたユーザのみが、特定電話番号、音声メール、その他の割り当てられたデータサービスなどの通信サービスを使用するためにアクセスできるようにすることが望ましい。

関連情報

ISO/IEC 27002 9.1.1の関連情報を適用する。

9.1.2 ネットワーク及びネットワークサービスへのアクセス

ISO/IEC 27002 9.1.2の管理策及び内容を適用する。

9.2　利用者アクセスの管理

ISO/IEC 27002 9.2の管理目的及び内容を適用する。

9.3　利用者の責任

ISO/IEC 27002 9.3の管理目的及び内容を適用する。

9.4　システム及びアプリケーションのアクセス制御

ISO/IEC 27002 9.4の管理目的及び内容を適用する。

10　暗号

ISO/IEC 27002 第10章の管理目的及び内容を適用する。

11　物理的及び環境的セキュリティ

11.1 セキュリティを保つべき領域

目的：組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。

11.1.1　物理的セキュリティ境界

管理策

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め、かつ、用いることが望ましい。

実施の手引き

ISO/IEC 27002 11.1.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、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) 電気通信事業者の運用センターには、適切な物理的な侵入者検知システムを設置することが望ましい。

b) 伝送設備、交換設備、及び電気通信用インフラストラクチャなどの電気通信事業用設備は、データセンター（IDC）で管理される顧客設備等の他設備とは物理的に分離して設置することが望ましい。

c) いかなる場合においても事業用資産の保護を確実にするため、厳格にすべてのローカルセキュリティ方針を順守して、物理的な障壁を有効に導入することが望ましい。また、物理的な障壁が有効に機能しない場合、又はセキュリティ方針が守られない場合には、適切なレベルの責任をもつ経営者により問題を直ちに解決することが不可欠である。

関連情報

ISO/IEC 27002 11.1.1の関連情報を適用する。

11.1.2 物理的入退管理策

管理策

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することが望ましい。

実施の手引き

ISO/IEC 27002 11.1.2の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、次の指針を考慮することが望ましい。

a) 適切な物理的セキュリティ管理策を、すべての電気通信事業者の運用室及び管理センターに適用することが望ましい。

b) 入室時には、適切な訪問者のデータが記録され、認可されていない開示から十分に保護することが望ましい。

c) 訪問者の記録は、それらに含まれる情報の機密性、完全性、可用性（CIA）を維持するよう、物理的かつ電子的に保護することが望ましい。

11.1.3 オフィス、部屋及び施設のセキュリティ

ISO/IEC 27002 11.1.3の管理策及び内容を適用する。

11.1.4 外部及び環境の脅威からの保護

ISO/IEC 27002 11.1.4の管理策及び内容を適用する。

11.1.5 セキュリティを保つべき領域での作業

ISO/IEC 27002 11.1.5の管理策及び内容を適用する。

11.1.6 受渡場所

ISO/IEC 27002 11.1.6の管理策及び内容を適用する。

11.2 装置

目的：資産の損失、損傷、盗難又は劣化、及び組織の業務に対する妨害を防止するため。

11.2.1 装置の設置及び保護

管理策

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、保護することが望ましい。

実施の手引き

ISO/IEC 27002 11.2.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

複数の事業者のシステムが同一のデータセンターに電気通信設備として設置されている場合、電気通信事業者はシステムに格納された顧客情報を保護するための適切な対策を実施することが望ましい。このようなシステムは、例えば分離されたセキュリティを保つべき領域内に配置されるなどの、追加的なセキュリティを適切に持つことが望ましい。

11.2.2　サポートユーティリティ

管理策

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することが望ましい。

実施の手引き

ISO/IEC 27002 11.2.2の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

特に、移動体通信基地局などの隔離された地域における電源設備は、あらゆる負荷に耐えられる容量を有し、停電期間中の主電源の障害に耐えられる能力をもった無停電電源装置を備えることが望ましい。それが不可能な場合は、重要装置に対する無停電電源供給を行う機構を具備することが望ましい。特に隔離された地域においては、自家発電機を用いて、バッテリーを補強することが必要な場合がある。

どの設備室にも、外部環境条件がメーカーの指針外で設備を運転する結果とならないように、適切な暖房、換気、空調（HVAC）サービスを具備することが望ましい。

関連情報

ISO/IEC 27002 11.2.2の関連情報を適用する。

電気通信事業者向けの関連情報

電気通信事業者は、電気通信サービスが中断なく確実に提供されるように、サポートユーティリティが適切に保守され、継続的に提供を受けられることを、契約に明記することが望ましい。

11.2.3　ケーブル配線のセキュリティ

管理策

データを伝送する又は情報サービスをサポートする通信ケーブル及び電源ケーブルの配線は、傍受、妨害又は損傷から保護されていることが望ましい。

実施の手引き

ISO/IEC 27002 11.2.3の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

盗聴及び傍受装置、あるいはケーブルに対するいかなる改変も、能動的手段によるかアクセスポイントの通常監査にて確実に検知できるように、ケーブルを設置することが望ましい。

11.2.4　装置の保守

ISO/IEC 27002 11.2.4の管理策及び内容を適用する。

11.2.5　資産の移動

ISO/IEC 27002 11.2.5の管理策及び内容を適用する。

11.2.6　構外にある装置及び資産のセキュリティ

ISO/IEC 27002 11.2.6の管理策及び内容を適用する。

11.2.7　装置のセキュリティを保った処分又は再利用

ISO/IEC 27002 11.2.7の管理策及び内容を適用する。

11.2.8　無人状態にある利用者装置

ISO/IEC 27002 11.2.8の管理策及び内容を適用する。

11.2.9　クリアデスク・クリアスクリーン方針

ISO/IEC 27002 11.2.9の管理策及び内容を適用する。

12　運用のセキュリティ

12.1 運用の手順及び責任

目的：情報処理設備の正確かつセキュリティを保った運用を確実にするため。

12.1.1　操作手順書

管理策

操作手順は、文書化し、必要とするすべての利用者に対して利用可能とすることが望ましい。

実施の手引き

ISO/IEC 27002 12.1.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、インシデント、緊急事態又は危機対処手順を発動すべき条件を、運用手順書の中に明記することが望ましい（16.1参照）。

12.1.2　変更管理

管理策

情報セキュリティに影響を与える、組織、業務プロセス、情報処理設備及びシステムの変更は、管理することが望ましい。

実施の手引き

ISO/IEC 27002 12.1.2の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、施設の新設、移転、及び撤去の手順及び記録を考慮することが望ましい。

物理的かつ論理的変更を含むインフラストラクチャに対する変更は、変更管理プロセスの対象となることが望ましい。該当する場合、本プロセスは指定されたリスク所有者からの承認を求めることが望ましい。リスクアセスメントを含む変更の結果は、定期的にセキュリティ監査を受けることが望ましい。

関連情報

ISO/IEC 27002 12.1.2を適用。

12.1.3　容量・能力の管理

ISO/IEC 27002 12.1.3の管理策及び内容を適用する。

12.1.4　開発環境、試験環境及び運用環境の分離

管理策

開発環境、験環境及び運用環境は、運用環境への認可されていないアクセス又は変更によるリスクを低減するために、分離することが望ましい。

実施の手引き

ISO/IEC 27002 12.1.4の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者においては、開発環境、試験環境で使用するデータの中身は、実際の電気通信システムやサービスでの試験に適していることが望ましい。試験データに取扱に慎重を要する情報（例えば、個人を特定できる情報や通話記録）が含まれる場合、プログラムのバグや誤操作による意図しない情報漏洩を回避するために適切な管理策を導入することが望ましい。

さらに、取扱に慎重を要する情報を含めた運用情報の収集、運用情報から試験データの作成、及び試験終了後の試験データの廃棄といったデータライフサイクルを考慮して、扱われる試験データは適切に管理されることが望ましい。

可能な場合、運用データから生成した、非運用データ又は匿名化されたデータを試験用に使用することが望ましい。

開発担当者は、運用システムの支援のために使用される一時的認可のための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やその他の認証トークンを取得することが望ましい。管理策ではそのような認可が使用後には無効とされるか認証トークンが変更されることを確実にすることが望ましい。

関連情報

ISO/IEC 27002 12.1.4の関連情報を適用する。

12.2 マルウェアからの保護

ISO/IEC 27002 12.2の管理目的及び内容を適用する。

12.3 バックアップ

ISO/IEC 27002 12.3の管理目的及び内容を適用する。

12.4 ログ取得および監視

目的：イベントを記録し、証拠を作成するため

12.4.1 イベントログ取得

管理策

利用者の活動、例外処理、故障、情報セキュリティの事象を記録したイベントログを生成、保存し定期的にレビューすることが望ましい。

実施の手引き

ISO/IEC 27002 12.4.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、電気通信用データ（例えば、課金、料金請求、苦情対応、不正利用防止、当局による法的アクセス等）の保存のための適切な保存期間を設定することが望ましく、また、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、当該データを遅滞なく消去することが望ましい。このことは、適用される事業及び法規制の要求事項に従って実施されることが望ましい。

関連情報

ISO/IEC 27002 12.4.1の関連情報を適用する。

電気通信事業者向けの関連情報

通信の秘密を確保するための適切な手段を講じることが望ましい。（附属書A TEL 18.1.6 参照）

12.4.2 ログ情報の保護

ISO/IEC 27002 12.4.2の管理策及び内容を適用する。

12.4.3 実務管理者及び運用担当者の作業ログ

ISO/IEC 27002 12.4.3の管理策及び内容を適用する。

12.4.4 クロックの同期

ISO/IEC 27002 12.4.4の管理策及び内容を適用する。

12.5 運用ソフトウェアの管理

目的：運用システムの完全性を確実にするため。

12.5.1 運用システムに関わるソフトウェアの導入

管理策

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することが望ましい。

実施の手引き

ISO/IEC 27002 12.5.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、運用システムの破壊のリスクを最小限に抑えるために、変更管理のための次の指針を考慮することが望ましい

a) 重要システムのアプリケーション又はオペレーティングシステムソフトウェアに対する変更は、十分にテストされること。このようなアップグレードをロールバックする手順を含めること。

b) 取扱いに慎重を要する業務用ソフトウェアである場合には、少なくとも3世代分のソフトウェアを保持すること。

c) 試験システム上での、アップデート、パッチ及び変更の回帰テスト及び、運用環境に導入する前にそれらが正しく作動することの確認。

12.6 技術的ぜい弱性管理

目的：技術的ぜい弱性の悪用を防止するため

12.6.1 技術的ぜい弱性の管理

管理策

ISO/IEC 27002 12.6.1の管理策及び内容を適用する。

12.6.2 ソフトウェアのインストールの制限

管理策

利用者によるソフトウェアのインストールを管理する規則を確立し、実施することが望ましい。

実施の手引き

ISO/IEC 27002 12.6.2の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

ネットワークの構成要素や、オペレーティングシステムなどの取り扱いに注意を要するシステムに対しては、検証済みかつ承認されたソフトウェアのみをインストールすることが望ましい。

取り扱いに注意を要するシステムには、認可された保守要員のみがソフトウェアをインストールできるようにすることが望ましい。この制限を取り扱いに注意を要するシステムの管理端末にも適用することが望ましい。

取り扱いに注意を要するシステムの性能とセキュリティの両方又はどちらか一方に悪影響を与える可能性のあるソフトウェアは、管理し監視することが望ましい。

12.7 情報システム監査に対する考慮事項

ISO/IEC 27002 12.7の管理目的及び内容を適用する。

13　通信セキュリティ

13.1 ネットワークセキュリティ管理

目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため

13.1.1　ネットワーク管理策

ISO/IEC 27002 13.1.1の管理策及び内容を適用する。

13.1.2　ネットワークサービスのセキュリティ

管理策

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むことが望ましい。

実施の手引き

ISO/IEC 27002 13.1.2の実施の手引きを適用する。

関連情報

ISO/IEC 27002 13.1.2の関連情報を適用する。

電気通信事業者向けの関連情報

電気通信事業者にとって、ネットワーク利用者に提供するサービスのセキュリティ向上には、以下のものを含む。

a) ネットワークサービスの設定に加えて、運用、管理、保守、プロビジョニング（OAM & P）の確保
b) ネットワークサービス（例えば、VoIPサービスのためのセッション開始プロトコル(SIP)）により利用される制御情報及びシグナリング情報のセキュリティ確保
c) ネットワークサービス（例えば、VoIPトラフィック）の利用におけるエンドユーザのデータや音声情報のセキュリティ確保

13.1.3　ネットワークの分離

管理策

情報サービス、利用者及び情報システムは、ネットワーク上で、グループごとに分離することが望ましい。

実施の手引き

ISO/IEC 27002 13.1.3の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

開発と管理ネットワークの適切な分離には、特に注意することが望ましい。

ホスティングにより提供された顧客ネットワークと関連データは、ホスティング以外の運用ネットワーク及び他のデータから適切に分離することが望ましい。

関連情報

ISO/IEC 27002 13.1.3の関連情報を適用する。

13.2 情報の転送

目的：組織の内部及び外部に転送した情報のセキュリティを維持するため。

13.2.1　情報転送の方針及び手順

ISO/IEC 27002 13.2.1の管理策及び内容を適用する。

13.2.2　情報転送に関する合意

ISO/IEC 27002 13.2.2の管理策及び内容を適用する。

13.2.3　電子的メッセージ通信

ISO/IEC 27002 13.2.3の管理策及び内容を適用する。

13.2.4　秘密保持契約又は守秘義務契約

ISO/IEC 27002 13.2.4の管理策及び内容を適用する。

14　システム取得、開発及び保守

14.1 情報システムのセキュリティ要求事項

ISO/IEC 27002 14.1の管理目的及び内容を適用する。

14.2 開発及びサポートプロセスにおけるセキュリティ

ISO/IEC 27002 14.2の管理目的及び内容を適用する。

14.3 試験データ

ISO/IEC 27002 14.3の管理目的及び内容を適用する。

15　供給者関係

15.1 供給者関係における情報セキュリティ

目的：供給者がアクセスできる組織の資産の保護を確実にするため。

15.1.1　供給者関係のための情報セキュリティの方針

管理策

組織の資産に対する供給者のアクセスに関連するリスクを軽減するための情報セキュリティ要求事項について、供給者と合意し、文書化することが望ましい。

実施の手引き

ISO/IEC 27002 15.1.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

供給者に対して取り扱いに注意を要する情報（個人を特定できる情報や通話記録など）のアクセス権を与える場合、電気通信事業者は以下を行うことが望ましい。

- 供給者が適切にその情報を保護できることを確実にする。
- このような取り扱いに注意を要する情報の扱い方を、供給者との秘密保持契約又は守秘義務契約に含める。（ISO/IEC 27002 13.2.4を参照）
- 国境を越えた要求事項を含む、あらゆる法規制の要求事項に適合する。

15.1.2　供給者との合意におけるセキュリティ

管理策

関連する全ての情報セキュリティ要求事項を確立し、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することが望ましい。

実施の手引き

ISO/IEC 27002 15.1.2の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、特定されたセキュリティ要求事項を満たすために、契約には、以下の事項を含める

ことを考慮することが望ましい。

a) 他の電気通信事業者との関係において、互いの電気通信設備又はそれらの設備に接続する他の利用者の電気通信設備の機能への損傷又は障害を与えないように明確にすること

b) 電気通信サービス設備と他の事業者の該当設備に関して、電気通信事業者間の責任の分界が明確であるようにすること

関連情報

ISO/IEC 27002 15.1.2の関連情報を適用する。

15.1.3 ICTサプライチェーン

管理策

供給者との合意には、情報通信技術（以下、ICT という。）サービス及び製品のサプライチェーンに関連する情報セキュリティリスクに対処するための要求事項を含めることが望ましい。

実施の手引き

ISO/IEC 27002 15.1.3の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者とその顧客間の供給者契約には、取り扱いに注意を要する顧客データの非開示を確実とする適切な管理策を含めることが望ましい。例えば番号案内が第三者により提供されている場合、供給者との契約には電話番号やIDなどの顧客データの開示に関する要求事項を含めることが望ましい。

複数の供給者により他の通信と共に重要通信が提供される場合、電気通信事業者は重要通信の優先順位付けに関して既存の契約に含まれていることをサプライチェーン全体を通じて確実とすることが望ましい。

供給者から提供されるサービスが取り扱いに注意を要する情報を含む場合、適切な供給者との契約が存在することが望ましい。これらには、データ所有者の事前合意なしに契約範囲内の情報へのアクセスを容認するような外注を禁止する条項を含めることが望ましい。供給者が業務を外注する必要がある場合、電気通信事業者はその取扱いに注意を要する情報に関する適切なレベルの保護があらかじめ合意されており、サプライチェーン全体を通じて維持されていることを確実とすることが望ましい。

15.2 供給者のサービス提供の管理

ISO/IEC 27002 15.2の管理目的及び内容を適用する。

16 情報セキュリティインシデント管理

16.1 情報セキュリティインシデントの管理及びその改善

目的：セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にするため。

16.1.1 責任及び手順

管理策

情報セキュリティインシデントに対する迅速、効果的で整然とした対応を確実にするために、責任体制及び手順を確立することが望ましい。

実施の手引き

ISO/IEC 27002 16.1.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

サービス合意レベルがもはや適合しない場合、電気通信事業者は、ハードウェア停止、ネットワーク障害、及びその会社の定める構成などの実際の顧客における構成運用について、顧客及びその従業員に影響

を与える顧客からの申告事項を上申することが望ましい。

インシデント対応手順には、情報セキュリティインシデントに関する情報を顧客に提供するための基準やタイミングの要求事項を含めることが望ましい。

すべての顧客は、問題発生時の申告（エスカレーション）手続きを認知することが望ましく、それらの関連書類を保有することが望ましい。

例えば、顧客からの申告事項は、以下の基準に従い、優先付けすることができる。

a) 顧客サイトが完全にダウン状態であるかサービスレベル合意書（SLA）の要求事項から外れる恐れがある

b) 顧客のサイトが電力等の供給停止により深刻な影響を受けようとしている。一つ若しくはそれ以上のシステムがダウンしている、又は大量のパケット喪失、及び/若しくはパケット遅延が生じている

c) 顧客へのサービスの品質低下

d) 顧客からの要請

電気通信事業者は、重要な公益事業として電気通信サービスを提供する責務から、電気通信システムにおけるインシデントを正確かつ適時に検知し、分析するだけでなく、情報セキュリティインシデントの阻止、インシデント要因の排除、及び復旧のためのメカニズムや手続きを確立することが望ましい。

ISO/IEC 27002 16.1.1に提案されるアクションに加えて、このようなメカニズム及び手順には以下が含まれることが望ましい。

a) 適切な内部要員及び、必要に応じて規制機関や緊急サービス、重要インフラ関係者などの外部の組織に、インシデントを報告する。

b) 電気通信システムを隔離する。システムを検査する必要がある場合は、可能であればその使用を停止し、再立ち上げ前にすべての電気通信運用ネットワークから切断することが望ましい。

c) 影響を受けたシステムが通常通り機能していることを確認し、インシデントから復旧する。必要であれば、将来における関連する動作を監視するための追加モニタリングを実施する。

関連情報

ISO/IEC 27002 16.1.1の関連情報を適用する。

電気通信事業者向けの関連情報

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電気通信ISAC[注]などの関連組織を通じて共有することが望ましい。

注：日本では、ICT-ISAC が相当する。

16.1.2 情報セキュリティ事象の報告

ISO/IEC 27002 16.1.2の管理策及び内容を適用する。

16.1.3 情報セキュリティ弱点の報告

ISO/IEC 27002 16.1.3の管理策及び内容を適用する。

16.1.4 情報セキュリティの事象の評価及び決定

管理策

情報セキュリティの事象は、これを評価し、情報セキュリティインシデントに分類するか否かを決定することが望ましい。

実施の手引き

ISO/IEC 27002 16.1.4の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者はセキュリティの事象をインシデントと分類する場合に、顧客への影響を考慮することが望ましい。

16.1.5　情報セキュリティインシデントへの対応

管理策

情報セキュリティインシデントは、文書化した手順に従って対応することが望ましい。

実施の手引き

ISO/IEC 27002 16.1.5の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、必要な場合、適切な通信チャンネルや他の形態の通信を通じて、インシデントを迅速に関連する顧客に報告することが望ましい。

顧客への通知の必要性は提供されるサービスの性質に依存する。

16.1.6　情報セキュリティインシデントからの学習

管理策

情報セキュリティインシデントの解析と解消により得られた知識は、今後のインシデントの可能性や影響を低減するために使用することが望ましい。

実施の手引き

ISO/IEC 27002 16.1.6の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

電気通信事業者は、以下の行動を考慮して、学んだ教訓を共有し、インシデント管理を改善するためのメカニズム及び手続きを構築することが望ましい。

a) インシデント対応終了後に、そこから学習した検討課題を議論する会議を開催する。この会議では、セキュリティ対策、及びインシデント対応プロセス自身の改善に向けた方法を検討することが望ましい。

b) 対応したインシデントの数、対応の総時間、コストなどのようなインシデントに関わるデータを収集する。さらに、それをインシデント管理手法の改善のために活用する。

c) 訴訟、法規制、及びコストを考慮して、関連証拠を保持する（16.1.7参照）。

関連情報

ISO/IEC 27002 16.1.6の関連情報を適用する。

16.1.7　証拠の収集

ISO/IEC 27002 16.1.7の管理策及び内容を適用する。

17　事業継続マネジメントにおける情報セキュリティの側面

17.1 情報セキュリティ継続

目的：情報セキュリティ継続を組織の事業継続マネジメントシステムに組み込むことが望ましい。

17.1.1　情報セキュリティ継続の計画

ISO/IEC 27002 17.1.1の管理策及び内容を適用する。

17.1.2　情報セキュリティ継続の実施

管理策

組織は、困難な状況の下で情報セキュリティ継続に対する要求レベルを確実に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、維持することが望ましい。

実施の手引き

ISO/IEC 27002 17.1.2の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

優先度に応じた緩やかなサービス縮小（グレースフルデグレーション）計画を作成することが望ましい。

事業継続計画には種々の形態において情報を保護する情報セキュリティ継続性に関する条項を含めることが望ましい。事業継続計画を作成導入するにあたり、電気通信事業者は、電気通信サービスの災害復旧計画と電気通信サービス顧客の重要通信の確保を含めることを考慮することが望ましい。

電気通信事業者はまた、災害復旧のためその要員を電気通信運用区画にいつ派遣するかについても考慮することが望ましい。

関連情報

ISO/IEC 27002 17.1.2の関連情報を適用する。

17.1.3　情報セキュリティ継続の検証、レビュー及び評価

ISO/IEC 27002 17.1.3の管理策及び内容を適用する。

17.2 冗長性

目的：情報処理設備の可用性確保

17.2.1　情報処理施設の可用性

管理策

情報処理設備は、可用性の要求事項を満たすのに十分な冗長性をもって、導入することが望ましい。

実施の手引き

ISO/IEC 27002 17.2.1の実施の手引きを適用する。

電気通信事業者向けの実施の手引き

重要通信及び国家の重要インフラを支援する電気通信設備（附属書A TEL. 18.1.7参照）は、可用性の喪失によりサービス提供に影響がないよう十分な冗長性を持つことが望ましい。

18　順守

ISO/IEC 27002 18章の管理目的及び内容を適用する。

附属書A

電気通信事業者のための拡張管理策集

（本附属書は本標準の第5章から第18章までと同様に扱われる。）

この附属書は、電気通信事業者のための追加の管理策をまとめたものとして、新しい目的、新しい管理策及び新しい実施の手引きを提供する。新しい管理策に関連するISO/IEC 27002の管理目的は、内容を修正することなく再記述している。組織が、ISO/IEC 27001に適合するよう意図されたISMSにおいてこれらの管理策を実施する場合、その適用宣言書（SOA）を本附属書に記述される管理策を含めることにより拡張することが望ましい。

TEL. 9　　アクセス制御

TEL. 9.5　　ネットワークのアクセス制御

目的：ネットワークを利用したサービスへの認可されていないアクセスを防止するため。

TEL. 9.5.1　　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、認証することができるための適切な管理策を提供することが望ましい。

実施の手引き

電気通信サービスが遠隔の利用者により、又はモバイル環境を通じて利用される場合、そのような利用は機密性の侵害の対象となる可能性がある。これはサービスの正当な利用者になりすました者や、サービスの安全性を損なうマルウェアにより引き起こされる場合がある。従って、利用者が電気通信事業者との間でその通信を相互認証するための適切な管理策を適用することが望ましい。

利用者が電気通信事業者を認証できない場合、電気通信事業者は利用者に対して認証機能が利用できない事実及び、これにより想定される一般的なリスクを喚起することが望ましい。

関連情報

識別及び認証のために暗号技術を利用する場合には、いくつかの方式を選択することができる。

利用者が電気通信事業者を正しく識別及び認証できない場合に想定される脅威の一つとして、中間者攻撃がある。

TEL. 11　　物理的及び環境的セキュリティ

TEL. 11.1　　セキュリティを保つべき領域

目的：組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止するため。

TEL. 11.1.7　　通信センターのセキュリティ

管理策

電気通信事業を提供するための交換設備のような電気通信設備が収容される通信センターの物理的セキュリティを設計し、開発し、適用することが望ましい。

実施の手引き

電気通信事業を提供するための交換設備などの電気通信設備（以降、通信センターという）を保護するため、以下を行うことが望ましい。

a) 通信センターは、震動や地殻運動などの自然災害の発生源から離れた水平な土地に設置することが望ましい。

b) 通信センターは、地下水位及び氾濫原より十分高くすることが望ましい。

c) 通信センターは、化学工場などの人工災害の発生原因がないところが望ましい。

d) 通信センターには、環境からの損害を最も受けにくい場所を選択することが望ましい。環境からの損害を受けやすい場所を選択する場合、自然災害[g)を参照] 及び極高低温を含む既知の災害に対する適切な対策を講じることが望ましい。

e) 通信センターには、環境が強い電磁界の影響を受けにくい場所を選択することが望ましい。強い電磁界にさらされる敷地を選択する場合、電気通信機器室を保護するため電磁シールドで適切な対策を講じることが望ましい。

f) 通信センターは、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しないことが望ましい。

g) 通信センターの建物は、下記を含む自然災害や事象による影響を最小限とするよう設計することが望ましい。

- 地震
- 火災
- 雷
- 洪水
- 漏水

h) 通信センターの建物は、必要とされる床荷重に耐えられる十分な構造的安定性を備えていることが望ましい。

i) 通信センターには、自動火災警報装置を設置することが望ましい。

j) 全ての通信機器がメーカーのガイドラインに従って運用できるように、HVAC制御装置を配備することが望ましい。

TEL. 11.1.8　通信機器室のセキュリティ

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る部屋の物理的セキュリティを設計し、開発し、適用することが望ましい。

実施の手引き

全ての電気通信機器室及び施設は、アクセス制御システム、CCTV（Closed Circuit Television）及び警報システムの使用、火災や有害な環境条件に対する防護などの適切な物理的及び環境的セキュリティ管理策を適用することが望ましい。

電気通信サービスを提供するための設備が配置されている部屋（以降、通信機器室という）を保護するために、次の手引きを考慮することが望ましい。

a) 通信機器室は、自然災害などの外的な影響を受けにくい場所に設置することが望ましい。

b) 通信機器室は、認可されていない者の侵入を受けにくい場所に設置することが望ましい。またそのような侵入を防止するために適切な対策を講じることが望ましい。

c) 通信機器室は、浸水の恐れが少ない場所に設置することが望ましい。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、床の嵩上げ、止水壁、特別な排水設備の設置などの必要な対策を講じることが望ましい。

d) 通信機器室は、強い電磁界による損傷を最も受けにくい場所に設置することが望ましい。通信機器室を強い電磁界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は、電磁シー

ルドその他の対策で保護することが望ましい。特に、電源設備が通信機器室内に設置される場合、電磁界からの干渉を防止するための対策を適切にとることが望ましい。

e) 重要な設備は、適切な物理的保護がなされた専用の通信機器室の中に配置することが望ましい。

f) 通常予測できる規模の地震などにより、床、壁、天井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対策を講じることが望ましい。

g) 床、壁、天井などに使用される素材は、不燃性又は耐火性とすることが望ましい。

h) 静電気への対策を講じることが望ましい。

i) 通信機器室に連結するダクトは、延焼を遅延、又は防止する設計とすることが望ましい。

j) 必要な場合には、データ保管室とデータ保管用の金庫を電磁妨害から保護するための対策を講じることが望ましい。

k) 必要に応じて、データ保管室及び専用のデータ倉庫には防火対策を講じることが望ましい。

l) 通信機器室及び空調設備室には、自動火災警報装置を設置することが望ましい。

m) 通信機器室及び空調設備室には、消火器を設置することが望ましい。

n) 通信機器室は、空調を行うことが望ましい。

o) 重要な設備を収容する通信機器室の空調は、オフィスやその他の部屋の空調とは別のシステムで稼動させることが望ましい。

p) HVAC制御は、無停電電源装置に接続し、電力損失が運用環境に影響を及ぼさないようにすることが望ましい。

TEL. 11.1.9　物理的に隔離された運用領域のセキュリティ

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る物理的に隔離された運用領域には、物理的なセキュリティを設計し、開発し、実施することが望ましい。

実施の手引き

携帯電話基地局など、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る物理的に隔離された運用領域（以降、隔離運用領域という）を保護するために、次の管理策を考慮することが望ましい。

a) 隔離運用領域は、国又は地域の必須の基準に適合するだけの耐震性を備えることが望ましい。

b) 隔離運用領域は、自動的に火災を検知し動作する消火設備を設置することが望ましい。

c) 隔離運用領域は、設備障害、電源障害、火災、湿度及び温度などを検知するために、遠隔のオフィスから監視することが望ましい。

d) 隔離運用領域を囲む安全な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境界を設けることが望ましい。一般的には無人で運用されるため、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ことが望ましい。

TEL. 11.3　他組織の管理下におけるセキュリティ

目的：電気通信事業者が自社の構外（コロケーションなど）に設置する装置を、物理的及び環境的な脅威から保護するため。

TEL. 11.3.1　他の電気通信事業者の構内に設置される装置

管理策

電気通信事業者が自社の構外に装置を設置する場合には、環境上の脅威又は危険、並びに認可されていないアクセスの可能性のリスクを低減するように、保護された場所に設置することが望ましい。

実施の手引き

他の電気通信事業者の敷地に設置する装置を保護するため、次の管理策を考慮することが望ましい。

a) 他の電気通信事業者との境界及び接点を明確にし、要請があった場合に、装置を他の事業者の装置から容易に切り離せることが望ましい。

b) サポートユーティリティの提供についての契約を、他の電気通信事業者と締結することが望ましい。

c) 管理者は、装置が設置される場所が適切であり、要求されるセキュリティレベルを満たしていることを確認することが望ましい。

関連情報

他の電気通信事業者の構内のセキュリティレベルが事業者自身の構内のセキュリティレベルと整合性を保つように、求められるセキュリティレベルを満たすための契約および規則を他の電気通信事業者と事前に確認しておくことが望ましい。

TEL. 11.3.2　顧客の領域に設置する設備

管理策

電気通信事業者が電気通信サービス顧客の装置と接続するために顧客の構内に装置を設置する場合には、環境上の脅威又は危険からのリスク及び、認可されていないアクセスによるリスクを低減するように自社の装置を保護することが望ましい。

実施の手引き

顧客の敷地に設置する装置を保護するため、次の管理策を考慮することが望ましい。

a) キャビネットのような、顧客の敷地に設置される装置は頑丈で、認可されないアクセスに対して適切に保護されていることが望ましい。

b) 装置の改変や、改変しようとする試みは検出可能であることが望ましい。

c) 顧客との境界及び接点を明確にし、要請があった場合に、装置を顧客から容易に切り離せることが望ましい。

d) 遠隔からの装置の状態の監視又は、装置の操作ができることが望ましい。

TEL. 11.3.3　相互接続の電気通信サービス

管理策

相互接続された電気通信サービスの提供において、電気通信事業者は識別されたリスクを回避するために時機を失せずに分割し隔離できるように、他の電気通信事業者との明確に定義された境界及び接点を特定することが望ましい。

実施の手引き

相互接続された電気通信事業者のサービスが正常に運用されているか否かを確認するための、適切な管理策を備えておくことが望ましい。

問題を診断し是正措置を実施するために、電気通信事業者は、相互接続点において設備を他の電気通信事業者の設備から切り離し、また再接続するための手段を備えておくことが望ましい。

電気通信事業者は、相互接続点におけるトラフィックの状態を常時監視することが望ましい。

電気通信事業者は、顧客の通信によって、相互接続された電気通信事業者の円滑なサービス提供に支障を生じている場合、当該顧客への通信サービスの提供を停止することがある旨を、約款又は契約に明記しておくことが望ましい。

TEL. 13　　通信のセキュリティ

TEL. 13.1　　ネットワークセキュリティ管理

目的：ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にするため。

TEL. 13.1.4　　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さまざまな事業計画にセキュリティレベルを定め、サービスを提供する前に、顧客にそれを通知した上で、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。

実施の手引き

電気通信事業者は電気通信サービス顧客のために、次の活動を実施することが望ましい。

a) 電気通信サービスのセキュリティ上の特徴、サービスレベル及び管理要件の仕様化と、それらについての明確な文書の提示。

b) 不正通信、サイバー犯罪及びマルウェア等から電気通信サービス利用者を保護するための啓発活動。

電気通信事業者は、次の事項も考慮することが望ましい。

c) 不正傍受の防止や他の電気通信サービス提供者との相互接続を確実にすることなど、関連法令や規制に準拠した管理策の実施。

d) 緊急時における重要通信などの、特別なサービスレベルが要求される通信の提供。（TEL. 18.1.7参照）

e) 提供するサービス毎に、次のようなセキュリティ管理策の実施。

IP接続サービス/データセンターサービス：

1) 電子メール、ファックス、ショートメッセージサービス（SMS）の配信、自動呼出しなどの迷惑通信に対する管理策（TEL. 13.1.5参照）

2) DoS/DDoS攻撃に対する制限（TEL. 13.1.6参照）

3) 技術的なぜい弱性管理のための管理策（ISO/IEC 27002 12.6.1参照）

電話サービス/携帯電話サービス：

4) 重要通信の取扱い

5) 緊急時の優先電話の確保

6) 電話の輻輳

マネージドサービス：

7) 認証／暗号の利用

8) 特権モードの慎重な取扱い

f) サービス提供上の情報の管理において、次の項目を厳正に維持するためのセキュリティ管理策の実施。

1) 通話明細情報を含む通信の守秘を確実にすること

2) 個人を特定できる情報の保護

電気通信事業者は、提供する電気通信サービスを維持するために、次の管理策を適用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、及び緊急時の早急な修理。

h) 電気通信サービス用交換設備の適切な保守又は、そのトラフィック負荷の常時監視、緊急時のトラフィック輻輳を回避するためのバックアップ設備や他のルートへの切換。

i) ルータなどの交換設備が通常時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DoS攻撃を受けた場合の、電気通信設備の機能を維持するための方法や手順。

j) インターネット経路情報及び、DNSなどの制御情報の適切な管理。

TEL. 13.1.5 スパムへの対応

管理策

電気通信事業者はスパムへの対応方針を規定し、電子メール通信に適した良好かつ望ましい環境を確立するために適切な管理策を導入することが望ましい。

実施の手引き

電気通信事業者が電気通信サービス利用者からの申告によりスパムを認識し、そのスパムの発信者が自組織の顧客であった場合、その顧客に対し、スパムの送信を停止するよう要請することが望ましい。

スパム送信者による攻撃と判定された場合、攻撃の影響を最小限とするために電気通信事業者はその顧客へのサービスを停止することが望ましい。

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が送られてくる場合、当該事業者に対しスパムを遮断するために必要な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、その要請に対し適切な対応を実施することが望ましい。

スパム対策の効果をあげるため、電気通信事業者は、他の電気通信事業者及び国内外のスパム対策組織との協力を密に行うことが望ましい。

電気通信事業者は、国の法規制に従って、スパムに対する対応方針を策定し、実施し、その方針を一般に公開することが望ましい。

TEL. 13.1.6 DoS/DDoS攻撃への対応

管理策

電気通信事業者はDoS/DDoS攻撃への対応方針を規定し、電気通信サービスのための良好かつ望ましい環境を用意するために、適切な管理策を導入することが望ましい。

実施の手引き

電気通信事業者が、異常トラフィックパターンや電気通信設備の不安定な運用状態などによってDos/DDoS攻撃のインシデントを認識した場合、電気通信設備の継続的かつ安定した運用を確実とするために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、電気通信事業者は次の対策を考慮することが望ましい。

a) 攻撃を受けている対象のサイト向けのパケットのフィルタリング

b) DoS/DDoS攻撃で使用されている通信ポートの制限

c) 攻撃対象となる電気通信設備の縮退運用又は停止

DoS/DDoS攻撃者が自組織の顧客である場合は、電気通信設備に対するDoS/DDoS攻撃を防ぐために、電気通信事業者は当該顧客への電気通信サービスを停止することが望ましい。

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のネットワークからのDoS/DDoS攻撃を受けた場合、電気通信事業者は当該事業者に対しDoS/DDoS攻撃を停止するための必要な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、その要請に対し適切な対応を実施することが望ましい。

DoS/DDoS攻撃対策の効果をあげるため、電気通信事業者は、他の電気通信事業者及び国内外のサイバーテロ対策組織との協力を密に行うことが望ましい。

TEL. 18　順守

TEL. 18.1　法的及び契約上の要求事項の順守

目的： 情報セキュリティに関連する法的、規制又は契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。

TEL. 18.1.6　通信の秘密保持

管理策

電気通信事業者によって取扱われる通信の秘密が確保されることが望ましい。

実施の手引き

秘密保持または守秘義務に関する要件を識別するために、電気通信事業者は以下の非開示事項に対する保護の必要性を考慮することが望ましい。

a) 通信の存在
b) 通信の内容
c) 通信の発信元（送信元）
d) 通信の着信先（宛先）
e) 通信の日時情報

電気通信事業者は、次の指針を考慮することが望ましい。

a) 通信の秘密が侵されないように、電気通信設備を適切に維持すること。
b) 電気通信設備は、電気通信サービス利用者の端末設備と電気通信回路との接続点において、他の通信の内容が通常の利用において意図せず開示されることを防ぐための必要な措置を講じること。
c) 電気通信設備に保存された電気通信サービス利用者の記録とデータへの許可のないアクセス、又は破壊や改ざんを防止するため、必要な措置を講じること。
d) 顧客の通信に関わるいかなる情報へも、電気通信事業者の職員が許可なく、又は違法に利用することを禁止すること。
e) 通信データは、保存する目的に必要な範囲内で保存期間を定め、保存期間経過後又は目的を達成した後は、遅滞なく消去すること。
f) 法的執行又は電気通信サービス利用者自身の同意がある場合を除いては、通信の秘密に属する事項の第三者への提供を禁止すること。
g) 発信者番号通知サービスを提供する場合には、電気通信サービス利用者がケースバイケースで、発信者番号の通知の有無を決定できる機能を設けること。
h) 法的執行又は電気通信サービス利用者自身の同意がある場合を除いては、発信者番号の第三者への提供を禁止すること。
i) 電話番号案内サービスを提供する場合は、電気通信サービス加入者に対し、電話番号又は他のサービスに関連するIDを電話帳に記載するかどうかの選択をできるようにすること。利用者が電話番号の記載をしないことを求める場合には、電気通信事業者は遅滞なく当該利用者の情報を電話番号案内サービスの対象から除外すること。
j) 電気通信事業者は、法執行機関やその他の捜査機関から、通信の秘密に属する事項を含む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、国の法規制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。

TEL. 18.1.7　重要通信

管理策

電気通信事業者は、自然災害、事故又はその他の非常事態が発生した場合、又は発生するおそれがある場合は、そのようなインシデントの予防又はその影響の軽減、インシデントからの復旧、若しくは公共の秩序の維持に必要な重要通信を優先させることが望ましい。

実施の手引き

電気通信事業者は、例えば以下の事業者における重要通信、及び/又は国の法規制の取決めにもとづく重要通信を確保するために、重要度や優先度順に緩やかに停止できる機能を導入することで、電気通信活動の一部の中断又は制限することを考慮することが望ましい。

a) 気象機関
b) 水防機関
c) 消防救助機関
d) 災害救助機関
e) 公共秩序の維持に直接関わる機関
f) 国防に直接関わる機関
g) 海上の保安に直接関わる機関
h) 輸送の確保に直接関わる機関
i) 通信サービスに直接関わる機関
j) 電力の供給に直接関わる機関
k) 給水に直接関わる機関
l) ガスの供給に直接関わる機関
m) 選挙管理機関
n) 報道機関
o) 金融機関
p) 医療機関
q) 食糧供給に直接関わる機関
r) 重要サービスを提供する政府機関
s) その他の重要通信を取り扱う国又は地方の機関
t) 国の法規制又は他の要件により定められた、その他の重要通信

電気通信事業者が電気通信設備を他の電気通信事業者と相互接続する場合、その円滑かつ継続的な運用を確保するために重要通信の優先的な取扱いについて契約を締結するために必要な措置を講じることが望ましい。

TEL. 18.1.8　緊急対策の合法性

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ることが望ましい。そのような措置は適切であり、過剰にならないことが望ましい。

実施の手引き

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不測の事態に備えてあらかじめ手順を定めておき、定義した緊急事態措置が、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について、法令の専門家の助言と指導を仰ぐことが望ましい。

電気通信事業者は、例えば電気通信サービス顧客の設備との接続が、電気通信事業者の電気通信設備や他の電気通信サービス顧客の設備、他の建物の敷地に障害を与える場合、又は人への安全とセキュリティ

に影響を与える可能性がある場合には、そのインシデントに対応するために電気通信サービスを停止するなどの必要な措置を行う場合があることを、あらかじめ電気通信サービス顧客に認識させ、周知することが望ましい。

附属書B

ネットワークセキュリティのための補足的な手引き

（参考）

B.1　ネットワーク攻撃に対抗するためのセキュリティ対策

B.1.1 ネットワーク攻撃に対抗するための防護

a)　ネットワーク設備の保護

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送りつけられた悪意のあるマルウェアによって意図に反する動作が起こることにより、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、電気通信設備を適切に防護する措置を実施することが望ましい。

電気通信事業者は、サイバー攻撃（DDoS攻撃等）から、サーバ、ルータ等のIPネットワーク設備を保護するため、通信ポート、IPアドレス、プロトコル毎に、通信フィルタリング、又は帯域制限の機能を備えておくことが望ましい。電気通信サービスによっては、信号処理レベルでの通信制限や、ユーザ認証、アクセス権管理等と連動した通信フィルタリングの機能を備えておくことが望ましい。

b)　発信元偽装への対策

電気通信事業者は、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の発信元偽装を防ぐため、ユーザ認証を行うシステムにおいては、たとえば、一定の文字数以上で容易に推測されないパスワードの設定義務化や、ワンタイムパスワードやハードトークンによるパスワードの厳格な管理及び又は強力な認証機能の導入により、無許可アクセスに対する適切なセキュリティ管理を実施することが望ましい。

重要通信を取り扱う電気通信設備においては、利用者の発信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、IDがハードコーディングされた端末の利用や、登録時及び接続要求時に、事前に登録したパスワードにより発信者番号等を電気通信ネットワーク設備で検証できる機能の導入等が望ましい。

c)　不正な形式の通信信号への対策

電気通信事業者は、不正な形式の通信信号（例えば、不正に長いパケット）に対して防護する措置を導入することが望ましい。

例えば、不正な形式のパケット（ネットワーク攻撃により生成される場合が多い）がIPネットワーク設備の故障を起こす場合があるため、電気通信事業者は、電気通信サービスや施設保護のためにこのようなパケットを破棄することが望ましい。

B.1.2 利用者への注意喚起

a)　電気通信サービス利用者への注意喚起

電気通信サービス利用者のマルウェア感染したPCからの意図しないサイバー攻撃を抑止し、また、発生したネットワーク攻撃に迅速かつ適切に対応するため、電気通信事業者は、自社設備に過大な負荷がかかる場合には、電気通信サービスの利用を制限することがあることを、サービス約款等に明記することが望ましい。

電気通信事業者は、ネットワーク攻撃を引き起こす可能性のある脅威（例えば、ウィルス、ボットネット）について、利用者に注意喚起を行い、利用者が必要な措置を講じるよう電気通信サービス利用者に啓発することが望ましい。

注：「ボットネット」という用語は、共通のコマンドや制御機能のもとで、ワーム、トロイの木馬、又はバックドアのようなプログラムを起動するコンピュータ群（ゾンビPCと呼ばれている）を指す。ボットネットを介して攻撃を行う者（「ボットハーダー」）は、インターネットリレーチャット（IRC）等を利用し、通常、不正な目的のために、遠隔でコンピュータ群をコントロールできる。

B.2　ネットワーク輻輳に対するネットワーク対策

B.2.1 情報収集

a)　輻輳を発生させる恐れがある情報の事前収集

電気通信事業者は、ネットワークの輻輳を発生させる恐れのある災害やイベントについて、事前に情報を得るための運用規定を定めることが望ましい。例えば、気象情報や企画イベント情報を収集するための体制等を確立することが望ましい。収集した情報の報告体制及び報告手順を定め、関係者に周知徹底することが望ましい。

b)　障害等の誘発現象に対する情報の事前収集

災害、事故、その他の社会現象は、電気通信設備の故障或いはネットワーク輻輳を誘発することが多いため、電気通信事業者は、定期的に関連情報を収集しノウハウの蓄積に努め、事前に対策を検討することが望ましい。

B.2.2 ネットワーク輻輳への対策

a)　ネットワーク輻輳検出・規制機能

電気通信設備には、ネットワーク輻輳が発生した場合に、輻輳を検知し、通信の集中を回避する機能を備えておくことが望ましい。

重要通信を取り扱う電気通信システムは、フィルタリングなどの輻輳制御処理がこれらの重要サービス提供に対して悪影響しないようにするための性能回復力を持つことが望ましい。

電気通信事業者電気 r は、対象となる通信設備の処理の限界値を把握し、限界値に到達する前に接続要求数を制御する機能を備えておくことが望ましい。可能であれば、トラフィックの分散処理を行うことが望ましい。

b)　一時的な処理量向上のための措置

想定される混乱や災害の規模等を考慮し、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・構成変更を考慮することが望ましい。

参考文献

– ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements.*

– ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management.*

– ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts.*

– ISO/IEC 27033-2:2012, *Information technology – Security techniques – Network security – Part 2: Guidelines for the design and implementation of network security.*

– ISO/IEC 27033-3:2010, *Information technology – Security techniques – Network security – Part 3: Reference networking scenarios – Threats, design techniques and control issues.*

– ISO/IEC 27033-4:2014, *Information technology – Security techniques – Network security – Part 4: Securing communications between networks using security gateways*.

– ISO/IEC 27033-5:2013, *Information technology – Security techniques – Network security – Part 5: Securing communications across networks using Virtual Private Networks (VPNs).*

– ISO/IEC 27035-1:2016, *Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management.*

– ISO/IEC 27035-2:2016, *Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response*

– ISO/IEC 27036-1:2014, *Information technology – Security techniques – Information security for supplier relationships – Part 1: Overview and concepts*.

– ISO/IEC 27036-2:2014, *Information technology – Security techniques – Information security for supplier relationships – Part 2: Requirements.*

– ISO/IEC 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security.*

– ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS)*