別紙１

「ネットワークのIP化に対応した電気通信設備に係る技術的条件」のうち「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」

一部答申

平成24年11月28日

情報通信審議会

第１章　情報通信ネットワーク安全・信頼性基準の概要

1.1　現在の技術基準等の概要

1.1.1　電気通信設備に係る規制の概略

電気通信事業法では、電気通信回線設備（伝送路設備及びこれと一体として設置される交換設備並びにこれらの附属設備）を設置した電気通信事業者に対し、その事業の用に供する電気通信設備（事業用電気通信設備）を総務省令で定める技術基準に適合するよう維持する義務を課している（なお、類似の義務は、基礎的電気通信役務を提供する電気通信事業者に対しても、その基礎的電気通信役務を提供する事業の用に供する電気通信設備について課されている。）。

関係電気通信事業者は、事業用電気通信設備の使用を開始しようとするときは、当該事業用電気通信設備が技術基準に適合することについて、自ら確認し、その結果を総務大臣に届け出なければならない。

また、関係電気通信事業者は、電気通信役務の確実かつ安定的な提供を確保するため、事業用電気通信設備の管理規程を定め、電気通信事業の開始前に、総務大臣に届け出なければならない。

1.1.2　技術基準の構成

事業用電気通信設備に係る技術基準は、事業用電気通信設備規則により定められており、通常は利用者の管理・運用に委ねられるべき端末設備及び自営電気通信設備を除く設備（すなわち電気通信回線設備）については、次のような構成となっている。

第一節 電気通信回線設備の損壊又は故障の対策
第二節 秘密の保持
第三節 他の電気通信設備の損傷又は機能の障害の防止
第四節 他の電気通信設備との責任の分界
第五節 音声伝送役務の提供の用に供する電気通信回線設備

電気通信設備の安全・信頼性対策は、このうち「第一節 電気通信回線設備の損壊又は故障の対策」において規定されている。具体的には、電気通信回線設備について、「アナログ電話用設備等」（アナログ電話、ISDN（音声のみ）、0AB～J-IP 電話、携帯電話及び PHS の設備）と「その他の電気通信回線設備」（050-IP 電話、データ通信等に代表される設備）とに区分し、その区分毎に技術的条件を規定している。

1.1.3　情報通信ネットワーク安全・信頼性基準

電気通信事業法の技術基準適合維持義務の対象とされない電気通信設備であっても、社会的に重要なもの又はそれに準ずるものについては、その安全・信頼性対策の指標として

「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）が定められており、電気通信事業者等の自主的な対応を促している。

また、技術基準適合維持義務の対象となる電気通信設備であっても、電気通信事業者に対して一律に適用すべきではなく、各電気通信事業者による自主的な判断に基づき講じられるべき対策もある。情報通信ネットワーク安全・信頼性基準では、こうした対策をも含んでいる。

1.2　情報通信ネットワーク安全・信頼性基準の概要

1.2.1　安全・信頼性対策に関する基準

情報通信ネットワークの安全・信頼性対策に関する基準には、①電気通信事業法に基づく強制規格としての技術基準と、②ガイドラインとしての「情報通信ネットワーク安全・信頼性基準」（①の内容を含む。以下「安全・信頼性基準」という。）がある（図 1.2.1-1 参照）。

昭和 60 年４月の電気通信事業法の施行により、電気通信事業の分野に競争原理が導入され、多数の新規通信事業者が参入した。これにより、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って、基本的かつ総括的なガイドラインが必要となったことから、各種情報通信ネットワークの安全・信頼性対策の自発的な実施促進を図ることを目的に、「情報通信ネットワーク安全・信頼性基準」が制定された。以後、安全・信頼性基準は、社会的背景を踏まえて、適宜改正されている。

表 1.2.1-1　情報通信ネットワークの安全・信頼性対策に関する基準

		a.事業法第41条第1項及び第2項に規定する事業用電気通信設備※（電気通信回線設備事業用ネットワーク）	b.左記以外の電気通信事業用設備（その他の電気通信事業用ネットワーク）	c.自営情報通信ネットワーク	d.ユーザネットワーク
①強制基準	（電気通信事業法）事業用電気通信設備規則	電気通信事業用の設備について、予備機器の設置、故障検出、異常ふくそう対策、耐震対策、停電対策、防火対策等の技術基準を規定。	—		
②ガイドライン	情報通信ネットワーク安全・信頼性基準（昭和62年2月14日郵政省告示第73号）	①に加え、ソフトウェア対策、情報セキュリティ対策、設計・施工・運用等における管理等を詳細に規定。	電気通信事業法の技術基準の対象とならない電気通信事業者のネットワーク、自営情報通信ネットワーク、ユーザネットワークについて、予備機器の設置、故障検出、異常ふくそう対策、耐震対策、停電対策、防火対策等を詳細に規定。 また、ソフトウェア対策、情報セキュリティ対策、設計・施工・運用等における管理等も規定。		

※ 電気通信回線設備（送信の場所と受信の場所との間を接続する伝送路設備及びこれと一体として設置される交換設備並びにこれらの付属設備。）を設置する電気通信事業者が、その電気通信事業の用に供する電気通信設備（事業法第41条第1項関係）及び基礎的電気通信役務を提供する電気通信事業の用に供する電気通信設備（事業法第41条第2項関係）

表 1.2.1-2　情報通信ネットワークの形態

情報通信ネットワークの形態		主な適用事業者
電気通信事業用ネットワーク	a. 電気通信回線設備事業用ネットワーク	NTT 東日本・西日本、NTT ドコモ、KDDI、ソフトバンクテレコム、ソフトバンクモバイル、通信事業を行う CATV 事業者等のネットワーク
	b. その他の電気通信事業用ネットワーク	ISP、メールサービス提供者等のネットワーク
		電子ショッピングモール、ネットオークション提供事業者、電子掲示板の提供事業者等のネットワーク
電気通信事業以外のネットワーク	c. 自営情報通信ネットワーク	電力会社、鉄道会社等の民間事業者及び国や都道府県のネットワーク
	d. ユーザネットワーク	基幹的な企業内 LAN を設置する者のネットワーク

1.2.2　安全・信頼性基準の構成

安全・信頼性基準は、「設備等基準」と「管理基準」の２つで構成されている。設備等基準は、情報通信ネットワークを構成する設備及び当該設備を設置する環境の基準（６４項目１５６対策、別表第１）を定めている。

管理基準は、情報通信ネットワークの設計、施工、維持及び運用の管理の基準（５５項目８７対策、別表第２）を定めている。

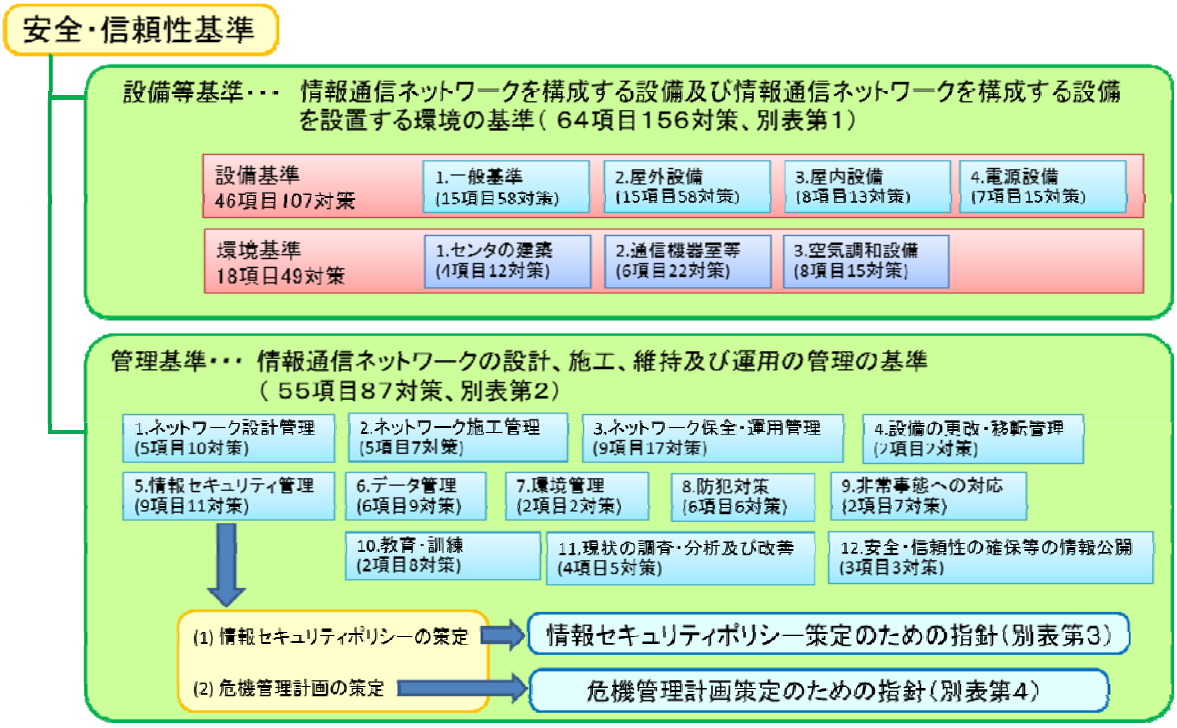

図 1.2.2-1　情報通信ネットワーク 安全・信頼性基準の構成

1.3　安全・信頼性基準の改正経緯

昭和６２年に制定された安全・信頼性基準は、情報通信ネットワークの急速な高度化、多様化の進展、電気通信サービスに影響を与えた大規模災害の発生や新たなセキュリティ脅威など、制定後の状況変化を踏まえ、情報通信ネットワークの環境変化に対応した新たな安全・信頼性対策の確保に向けて以下のような改正を行ってきた。

- 平成６年の改正の概要
  基準の制定から７年が経過し、情報通信ネットワークの急速な高度化・多様化から新たな安全・信頼性対策が必要となったため、基準を改正した。
  - ソフトウェアの信頼性向上対策
    ネットワークにおけるソフトウェアの役割の増大に伴う、ソフトウェアの信頼性向上対策の充実化。
  - 災害対策の一層の充実
    地震対策、火災対策に係る基準の充実、増加する基地局等の屋外・屋内設備等の雷害対策を新設。
    情報通信ネットワークのふくそうを防止し、有効活用を図るため、必要に応じて利用者への協力依頼・周知のための措置を新設。
  - ネットワークの相互接続の進展への対応
    ネットワークの相互接続の進展に伴う、相互接続のためのネットワークの設計監理、施工管理及び保全・運用管理を追加。
- 平成８年の改正の概要
  平成７年に発生した阪神淡路大震災の教訓を踏まえ、基準を改正した。
  - 停電対策
    地震発生直後からの長時間の停電による交換機や基地局の停止など、停電に伴う障害の影響が大規模であったことから、交換設備及び基地局について停電対策を追加。
  - 耐震対策
    被災すると影響が大きいと考えられる設備について、直下型地震又は海溝型巨大地震を考慮して対策を充実化。
  - 防火対策等
    大規模な火災や家屋の倒壊等によって加入者ケーブルが大きな影響を受けたことから、加入者ケーブルの被災を防ぐための対策を追加。
  - バックアップ対策
    エントランス回線などの多ルート化や非常用無線設備の配備等によるバックアップ対策を充実化。
  - 災害対策機器の配備

速やかな復旧を可能にするために使用する機器の配備などの応急復旧対策を追加。

- その他
  地震発生直後の電話のふくそう等における運用面での対策を充実化。

- 平成９年の改正の概要
  インターネットが爆発的に普及したことから、これまで十分でなかったネットワークの情報セキュリティに関する基準を改正した。
  - パスワード更新時の文字列チェック
    パスワードの文字列のランダム性をチェックし、一般的な単語は排除する仕組みを新設。
  - アクセス要求の記録等ログ管理の徹底
    保護することが求められる重要な情報については、その情報に対するアクセス要求を記録し、これを定期的に分析すると同時に、問題発生時の証拠として保存することを新設。

- 平成１２～１３年の改正の概要
  政府機関等におけるホームページ改ざん事案が発生したことから、電気通信事業におけるサイバーテロ対策として、基準を改正した。
  - 情報セキュリティ対策、情報セキュリティ管理など
    ハッカー及びコンピュータウィルス対策として、設備等基準及び管理基準を追加し、情報セキュリティポリシー策定のための指針（別表第３）を追加。また、サイバーテロが発生した場合の緊急対応体制を整備するため、危機管理計画策定のための指針（別表第４）を追加。

- 平成１６年の改正の概要
  電気通通信事業法の一部改正により、一種・二種の事業区分の廃止等が行われたことから、基準を改正した。
  - ネットワーク体系の区分変更
    「電気通信回線設備事業用ネットワーク」「その他の電気通信事業用ネットワーク」「自営情報通信ネットワーク」「ユーザネットワーク」の４区分に変更。
  - 安全・信頼性の確保等の情報公開
    ネットワークの安全・信頼性の確保に関する取組状況、情報通信ネットワークの事故・障害の状況及びサービスの特質等の周知の追加。

- 平成２０年の改正の概要
  IP 電話等の増加に伴い事故の影響が広域化・長時間化する傾向にあることや、サイバー攻撃に対する情報セキュリティの確保の問題が社会的課題となってきたことから、これらの対策として基準を改正した。
  - ソフトウェアの信頼性向上対策
    ソフトウェアの脆弱性対策、ウイルス対策、定期的なソフトウェアの点検及びリ

スク分析を追加。

- 緊急通報の確保
  緊急通報手段を提供するサービスのメンテナンス時における措置を追加。

- バックアップの分散化等
  予備電源設置・冗長化などの予備機器等の配備基準の明確化。

- 停電対策
  設備の重要度に応じた十分な規模の予備電源の確保の追加。

- 品質・機能検査の充実化
  サーバ等機器導入前の機能確認、セキュリティ対策の手法の追加や、災害時におけるユーザの振舞いや端末の挙動がネットワークに与える影響の事前確認を追加。

- 相互接続への対応
  相互接続を行う場合の作業分担、連絡体系、責任の範囲等の保全運用体制を明確にし、非常時等の事業者間の連携・連絡体制の整備を追加。

- サイバー攻撃に備えた管理体制
  サイバー攻撃発生時の迅速な情報共有方法を追加。

- 重要データの漏えい防止対策
  個人情報以外の重要な設備情報（特に他社のセキュリティ情報等）の漏えいを防止するための適切な措置を追加。

1.4　現行安全・信頼性基準の見直しについて

1.4.1　東日本大震災を踏まえた事業用電気通信設備規則の改正

電気通信事業者は、阪神淡路大震災等の経験を踏まえ、技術革新や経済合理性等を勘案しつつ、電気通信設備の安全・信頼性向上、重要通信の確保、通信サービスの早期回復を基本として、これまでも災害対策に努めてきたところである。

しかしながら、東日本大震災において広範囲かつ長期間にわたるふくそうや通信途絶等の状態が生じたことから、総務省では平成 23 年 4 月から「大規模災害等緊急事態における通信確保の在り方に関する検討会」を開催し、緊急事態における通信確保に関し、国、通信事業者、通信機器メーカー等の各主体が取り組むべき措置、利用者や自治体等に対し協力を求める措置等を取りまとめた。

また、ＩＰネットワーク設備委員会においては、上記の被害の特徴、主な要因等を踏まえ、電気通信設備の安全・信頼性の向上に向け下記の対策等について検討し、その結果は、事業用電気通信設備規則等の一部改正に反映され、平成 24 年 9 月 1 日に施行された。

・停電対策
・中継伝送路切断等の対策
・津波・冠水対策
・設備故障・破壊対策
・通信ふくそう対策及び重要通信確保

1.4.2　スマートフォン時代に対応した電気通信設備の安全・信頼性基準の検討

平成 23 年度からスマートフォンが急激に普及する中、一部携帯電話事業者において電気通信設備の設計や配備、工事の手順等における問題により重大な事故が多発しており、国民生活や社会経済活動に大きな影響を与えている

電気通信サービスに対する利用者の信頼を回復するとともに、安定的なサービス提供を実現するためには、設備の整備・管理面も含めた対策、幅広い取組が求められている。特に、スマートフォンについては、大容量データの送受信、常時接続、多様なアプリケーションからの制御信号の増加等の特性も考慮して、障害対策を検討していく必要がある。

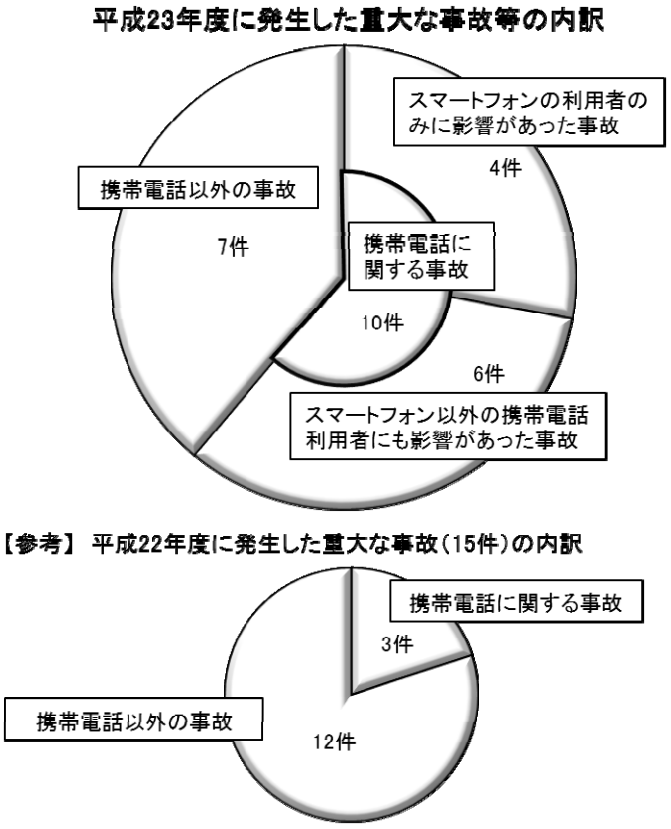

図 1.4.2-1　重大な事故の内訳

1.4.3　安全・信頼性基準の見直しの必要性

東日本大震災を踏まえた事業用電気通信設備規則の見直し、スマートフォン時代に対応した電気通信設備の安全・信頼性基準の検討の必要性に加えて、標的型攻撃のような最近の情報セキュリティに関する脅威等を踏まえた対策の強化も求められている。

そのため、電気通信設備の耐災害性、スマートフォン時代に対応した電気通信設備の安全・信頼性の確保や情報セキュリティ対策の強化の観点から、電気通信事業者等のネットワークの安全・信頼性対策に関するガイドラインである「情報通信ネットワーク安全・信頼性基準」等について、総合的に見直す必要がある。

第 2 章　情報通信ネットワーク 安全・信頼性基準の見直し

第 2 章においては、第 1 章 1.4 見直しの必要性を踏まえて、「情報通信ネットワーク安全・信頼性基準」（以下「安全・信頼性基準」という。）の見直しが必要とされる事項について検討を行った。

検討に際しては、主に次の６つの事項及びその観点を踏まえ、現行の安全・信頼性基準に追加、改正すべき基準（対策の内容、実施指針）があるか検証を行った。

（１）事業用電気通信設備規則の改正により技術基準が見直された事項

事業用電気通信設備規則の改正内容は、電気通信設備の安全・信頼性向上を目的としてなされたものであり、現行の安全・信頼性基準の見直しに際しては、当該改正内容を反映することが重要である。

（２）「大規模災害等緊急事態における通信確保の在り方についての最終取りまとめ」、「ＩＰネットワーク設備委員会報告」の提言事項であって、安全・信頼性基準への反映が必要と認められる事項

標記の検討会等における審議結果の多くは、（１）の事業用電気通信設備規則の改正に反映されているが、審議結果の中には、電気通信設備の安全・信頼性向上に関連する技術基準以外の提言や利用者保護の観点から取り組むべき事項など重要な提言も含まれているため、これら提言内容を反映することが重要である。

（３）携帯電話通信障害対策連絡会により共有化されたベストプラクティスで、安全・信頼性基準へ反映が必要と認められる事項

標記の検討会で共有化されたベストプラクティスは、実際の電気通信事故の分析の通じて得られた貴重な教訓、経験であることから、これらベストプラクティスを反映することが重要である。

（４）電気通信事業法以外の関係法令の規定、電気通信事業関係団体の取組状況により、安全・信頼性基準への反映が必要と認められる事項

電気通信事業法以外の法令等に基づき、電気通信サービスの提供に関して、電気通信事業者に要請されている事項の中には、電気通信設備の安全・信頼性向上に関連する事項や利用者保護の観点から取り組むべき事項も含まれているため、当該要請事項を反映することが重要である。

（５）情報セキュリティ対策の強化に必要と認められる事項

情報セキュリティ対策を巡る状況は急激に変化していることから、状況変化に対応した適切な見直しが重要である。

（６）その他見直しが必要と認められる事項

利用者保護の観点からの規定の整備、基準の現行化に伴う規定の整備等

次に、上記観点を踏まえ、現行安全・信頼性基準に反映すべき見直しの概要を示す。

2.1　事業用電気通信設備規則の改正により技術基準が見直された事項

平成 23 年 3 月 11 日に発生した東日本大震災は、通信インフラに広範囲、長時間にわたる被害やふくそうを発生させた。こうした大震災による通信インフラへの影響を減少させるため、平成 24 年 2 月 17 日付け情報通信審議会答申（「ネットワークの IP 化に対応した電気通信設備に係る技術的条件」のうち「電気通信設備の安全・信頼性対策に関する事項」（一部答申））において、電気通信設備の安全・信頼性の向上に向けた具体的方策が示された。

この答申を受けて、事業用電気通信設備規則等が改正され、平成 24 年９月１日に施行された。事業用電気通信設備規則の改正概要は以下のとおりである。

- 交換設備相互間の伝送路設備に対する複数経路の設置の強化＜第四条第四項＞
- 発電機等に用いる燃料の確保に関する努力規定の追加＜第十一条第二項及び第四十四条第二項＞
- 地方自治体の防災対策の拠点に対する停電対策の強化＜第十一条第三項及び第四十四条第三項＞
- 大規模災害対策に関する措置の追加＜第十五条の三及び第四十七条の二＞
- 災害時優先通信及び他の通信の疎通状況の記録･分析の追加＜第三十五条の二の二＞

上記の省令改正に伴って、現行基準の見直しが必要とされる事項の検討結果は、次のとおりである。

（設備等基準）

2.1.1　交換設備相互間の伝送路設備に対する複数経路の設置の強化について　＜第四条第四項関係＞

現行基準には、重要な通信センター間の伝送路設備を複数経路で設置する旨の対策は存在するが、省令で追加された交換設備相互間の伝送路設備に対する複数経路の設置に関する対策はない。

交換設備相互間の伝送路設備に複数経路の設置を講じることは、伝送路設備の障害発生時における通信の途絶防止に資することから、基準に改正省令内容を追加することが適当である。

（実施指針[1]）

事業	その他	自営	ユーザ
◎	―	―	―

【関係基準：別表第１　第１　１．（３）追加】

2.1.2　発電機等に用いる燃料の確保に関する努力規定の追加について
＜第十一条第二項及び第四十四条第二項関係＞

現行基準には、既に電源設備の停電対策として燃料の確保に関する対策は存在するが、同対策の現状における実施指針は「実施が望ましい」との分類であるため、実施指針を、改正省令内容を踏まえて現状より強化することが適当である。

また、燃料以外の物資（例えば発電機の冷却用水）を必要とする場合も想定されることから「燃料等」とすることが適当である。

（実施指針）

事業	その他	自営	ユーザ
○→◎＊	○	○	○

【関係基準：別表第１　第１　４．（７）エ】

2.1.3　防災対策の拠点に対する停電対策の強化について
＜第十一条第三項及び第四十四条第三項関係＞

現行基準には、停電対策に関する一般的な対策は存在するが、地方自治体の庁舎など防災対策の拠点となる特定施設の通信機器の維持、強化を図る観点からの情報通信ネットワークに対する停電対策の強化を求める対策はない。

地方自治体に設置されている通信設備に対する停電対策の強化は、防災上必要な通信の確保に資することから、基準に改正省令内容を追加することが適当である。

（実施指針）

事業	その他	自営	ユーザ
◎	―	―	―

【関係基準：別表第１　第１　４．（７）追加】

[1] 実施指針に記載されている記号については、それぞれ次の意味を示している。
◎・・・・実施すべきである。
◎＊・・・技術的な難易度等を考慮して段階的に実施すべきである。
○・・・・実施が望ましい。
－・・・・対象外。

2.1.4　大規模災害対策に関する措置の追加について（Ⅰ）
＜第十五条の三及び第四十七条の二関係＞

現行基準には、既に重要な通信センター等の地理的分散設置に関する対策が存在するが、同対策の現状における実施指針は「実施が望ましい」との分類であるため、実施指針を、省令改正を踏まえて現状より強化することが適当である。

（実施指針）（重要な通信センターの分散）

事業	その他	自営	ユーザ
○→◎＊	○	○	○

【関係基準：別表第１　第１　１.（１）ア】

（実施指針）（モバイルインターネット接続サービスにおける設備の分散等）

事業	その他	自営	ユーザ
○→◎＊	－	－	－

【関係基準：別表第１　第１　１.（５）】

また、同改正により、電気通信事業者は、ループ状に接続する大規模な伝送路設備は複数箇所の故障等により通信が停止しないよう、当該大規模な伝送路設備を横断する伝送路設備の追加的な設置の措置を求められていることから、基準に改正省令内容を追加することが適当である。

（実施指針）

事業	その他	自営	ユーザ
◎＊	－	－	－

【関係基準：別表第１　第１　１.（３）追加】

2.1.5　大規模災害対策に関する措置の追加について（Ⅱ）
＜第十五条の三及び第四十七条の二関係＞

現行基準には、火災、水害等個々の災害に関する対策は存在するが、個々の災害の複合化、広域化、長期化などを想定した大規模な災害時に関する対策はない。また、地方自治体が定める防災に関する計画（ハザードマップ）等の情報を考慮した電気通信設備の設置場所等の決定に関する対策も講じられていない。

大規模災害時においても、電気通信役務の提供に重大な支障が生じないよう措置を講じることは、防災上必要な通信を確保するために重要であることから、基準に改正省令内容を追加することが適当である。

（実施指針）

事業	その他	自営	ユーザ
◎＊	○	○	○

【関係基準：別表第１　第１　１.（１６）追加　及び　第２　１.（１）追加】

（設備等基準及び管理基準）

2.1.6　災害時優先通信及び他の通信の疎通状況の記録・分析の追加について＜第三十五条の二の二関係＞

現行基準には、災害時優先通信及び通信の疎通状況の記録・分析に関する対策はない。

災害時においては、災害時優先通信の確保やふくそうを防ぐために通信制限が行われるが、その際の疎通状況を記録・分析することは、災害時における優先通信の確保や優先通信以外の通信への過剰な通信制限の回避、また、情報通信ネットワークの通信容量の見直しの際の重要な検討資料となるため、基準に改正省令内容を追加することが適当である。

（実施指針）

事業	その他	自営	ユーザ
◎	―	―	―

【関係基準：別表第１　第１　１.（９）追加及び別表第２　３.（４）追加】

（設備等基準）

2.1.7　緊急通報＜第三十五条の二関係＞

平成１８年１月に事業用電気通信設備規則が改正され、緊急通報を行う事業用電気通信回線設備に対して、緊急通報の接続等に関する要件が規定された。

当該省令には、緊急通報した端末の場所を管轄する警察機関等へ接続すること等が規定されており、現在の緊急通報に不可欠なものとなっていることから、基準に省令内容を追加することが適当である。

なお、重要通信である緊急通報は、電気通信事業法第８条において、電気通信事業者が優先的に取り扱わなければならない通信として規定されている。

（実施指針）

事業	その他	自営	ユーザ
◎	―	―	―

【関係基準：別表第１　第１　１.（１４）追加】

2.2 「大規模災害等緊急事態における通信確保の在り方について最終取りまとめ」及び「ＩＰネットワーク設備委員会報告」の提言事項であって、安全・信頼性基準への反映が必要と認められる事項

2.2.1 「大規模災害等緊急事態における通信確保の在り方について 最終取りまとめ」について

東日本大震災の発生により、広範囲かつ長期間にわたり、ふくそうや通信途絶等の状態が生じたことを踏まえ、総務省においては、「大規模災害等緊急事態における通信確保の在り方に関する検討会」を開催し、今後の大規模災害等にも対応できるよう、「通信手段の確保」に焦点をあてその在り方について検討がなされ、平成 23 年 12 月に最終取りまとめが公表された。

検討会の提言は、次の 2.2.2 に報告するＩＰネットワーク設備委員会の検討結果を踏まえ、事業用電気通信設備規則の改正に反映されているところであるが、当該検討会における提言の中には、技術基準以外の提言や利用者保護の観点から取り組むべき事項など、重要な提言も含まれている。

以下に、見直しの検討に参照した提言概要を示す。

「大規模災害等緊急事態における通信確保の在り方について（最終取りまとめ）」
・大ゾーン基地局の全国設置
・自社の災害対応体制の検証と必要に応じた見直し

（設備等基準）

2.2.1.1 大ゾーン基地局について

現行基準には、臨時に設置する電気通信回線や可搬型無線基地局により通信の途絶を防止する応急対策は存在するが、臨時の大ゾーン基地局の設置による対策はない。

大ゾーン基地局の設置は、防災上重要な通信を確保する必要がある拠点の障害時における迅速な応急対策として有効であることから、基準にその旨を追加することが適当である。

（実施指針）

事業	その他	自営	ユーザ
○	―	―	―

【関係基準：別表第１　第１　１．（１３）追加】

（管理基準）

2.2.1.2　自社の災害対応体制の検証と必要に応じた見直しについて

現行基準には、非常事態への対応として、体制の明確化、復旧対策の手順化に関する対策は存在するが、体制の検証・見直しについては考慮されていない。

災害対応体制（事業継続計画、災害対応マニュアル等）を、必要に応じ検証・見直しすることは、災害時における迅速・適確な対応に資することから、基準に追加することが適当である。

（実施指針）

事業	その他	自営	ユーザ
◎	○	◎	○

【関係基準：別表第２　９.（１）追加】

2.2.2　「ＩＰネットワーク設備委員会報告」の提言事項であって、安全・信頼性基準への反映が必要と認められる事項

東日本大震災や台風により、通信インフラにおいてふくそうや通信の途絶等が発生したことに伴い、電気通信設備に支障が生じた場合の国民生活、経済社会活動への影響が大きくなっていること等を受けて、電気通信設備の安全・信頼性対策の強化に向けた方策について、ＩＰネットワーク設備委員会において検討され、平成 24 年 2 月 3 日に報告書が取りまとめられた。

当該報告書は、平成 24 年 2 月 17 日、情報通信審議会により「ネットワークの IP 化に対応した電気通信設備に係る技術的条件」のうち「電気通信設備の安全・信頼性対策に関する事項」として一部答申され、この答申を踏まえ、2.1 の事業用電気通信設備規則の改正が行われている。

以上のとおり、審議会の審議結果は、事業用電気通信設備規則の改正に反映されているところであるが、当該検討会等における提言の中には、技術基準以外の提言や利用者保護の観点から取り組むべき事項など、重要な提言も含まれている。

以下に、見直しの検討に参照した提言概要を示す。

（ＩＰネットワーク設備委員会報告）
- 津波対策の強化
- 停電対策が強化された携帯電話基地局のカバーエリア等の情報の公表
- 災害対策が強化された大ゾーン基地局のカバーエリア等の情報の公表
- ネットワークの設計容量に関する基本的考え方、通信規制や重要通信の優先取扱いに係る手法等に関する情報の公表
- ふくそうが発生した場合の状況及び通信規制の実施状況の公表

・災害時における音声通話以外の通信手段の利用等の呼びかけ

2.2.2.1　津波対策の強化について

現行基準には、水害対策はあるが、津波対策に関する対策はない。

東日本大震災時では、非常に大規模な津波が発生したことにより、通信ビルや携帯電話基地局をはじめとする多くの電気通信設備が甚大な被害が発生した。

津波対策を講じることは、津波襲来時における通信の確保が期待されることから、対策にその旨を追加することが適当である。

（実施指針）

事業	その他	自営	ユーザ
◎＊	◎＊	◎＊	◎＊

【関係基準：別表第１　第１　２．（６）－２追加】

2.2.2.2　情報の公表に関する検討

構成員である地方自治体、独立行政法人 国民生活センターからの意見聴取の結果、電気通信事業者に求められる情報の公表の在り方については、次のとおり整理された。

- 事業者は、災害対策の取組に関し情報提供を行う際には、利用者と事業者間の情報格差を埋めるよう、努めなければならない。
- 利用者に提供される情報は、できる限り事業者間で統一された基準により、事業者毎の情報提供内容の差異を少なくする必要がある。
- 事業者は、利用者の自主的かつ合理的な電気通信サービスの選択を可能とし、災害時に適切な電気通信サービスの利用を促進するための情報を提供する必要がある。

また、情報提供されるべき事項としては、事前提供、災害時、災害対策後など時系列毎に必要とされる事項が整理された。

- 事前提供が必要な事項
  災害時における事業者の取組（停電対策、応急対策、通信規制等）、災害時に有効なツール、災害時の速報情報（通信可能エリアに関する情報等）の掲載場所・方法、災害時に有効なサービスや利用が困難になるサービスなど災害時の電気通信サービスの利用上の留意点に関する事項、災害時、利用者の主な活動地域でどの程度使えるかという目安とその他参考情報等。
- 災害時に必要な事項
  ふくそう、通信規制の状況及び災害時に有効なツールへの誘導、通信可能エリアと復旧見込みに係る情報、災害時の電気通信サービスの利用上の留意点、被災地における電気通信サービスの提供状況（臨時公衆電話、臨時ショップ、携帯電話用チャージャー等の設置箇所等）、相談窓口、減免措置等その他利用者の災害時の対応に役立つ事項。
- 災害対策後に必要な事項
  災害時の通信、被害状況及びその分析、今後の取組への反映。

2.2.2.3　業界団体における情報の公表に関する検討結果について

2.2.2.2 の整理を踏まえ、構成員である社団法人電気通信事業者協会（以下「ＴＣＡ」という。）において、携帯電話事業者（ＮＴＴドコモ、ＫＤＤＩ、ソフトバンクモバイル、イー・アクセス）の停電対策・災害対策が強化された携帯電話基地局のカバーエリア等の情報の公表の在り方について検討が行われた。ＴＣＡにおける検討結果を次に示す。

2.2.2.3.1　停電対策を強化した携帯電話基地局に関する情報の公表について

蓄電池の増強や発電機の設置等により、停電後も長時間サービスを提供可能な能力を有する携帯電話基地局について、当該携帯電話基地局がカバーするエリアの情報を公開する。具体的な公表内容等については、以下のとおりとすることが望ましい。

停電後２４時間※以上、通話サービスが提供可能な携帯電話基地局については、停電対策を強化した基地局として、各社のホームページ上でその基地局のカバーエリアが分かるようなマップまたは情報（施設名称等）を掲載する。

停電対策を強化した携帯電話基地局以外の局については、最低３時間以上の停電対策が講じられているので、一律に扱うこととする。

最低３時間以上の停電対策が講じられていない一部エリアや地下街などの屋外については、場所により状況が異なるため、個別の問い合わせに対応することとする。

※　常時設置されている設備の容量から算出し、臨時に設置する設備は含まない。

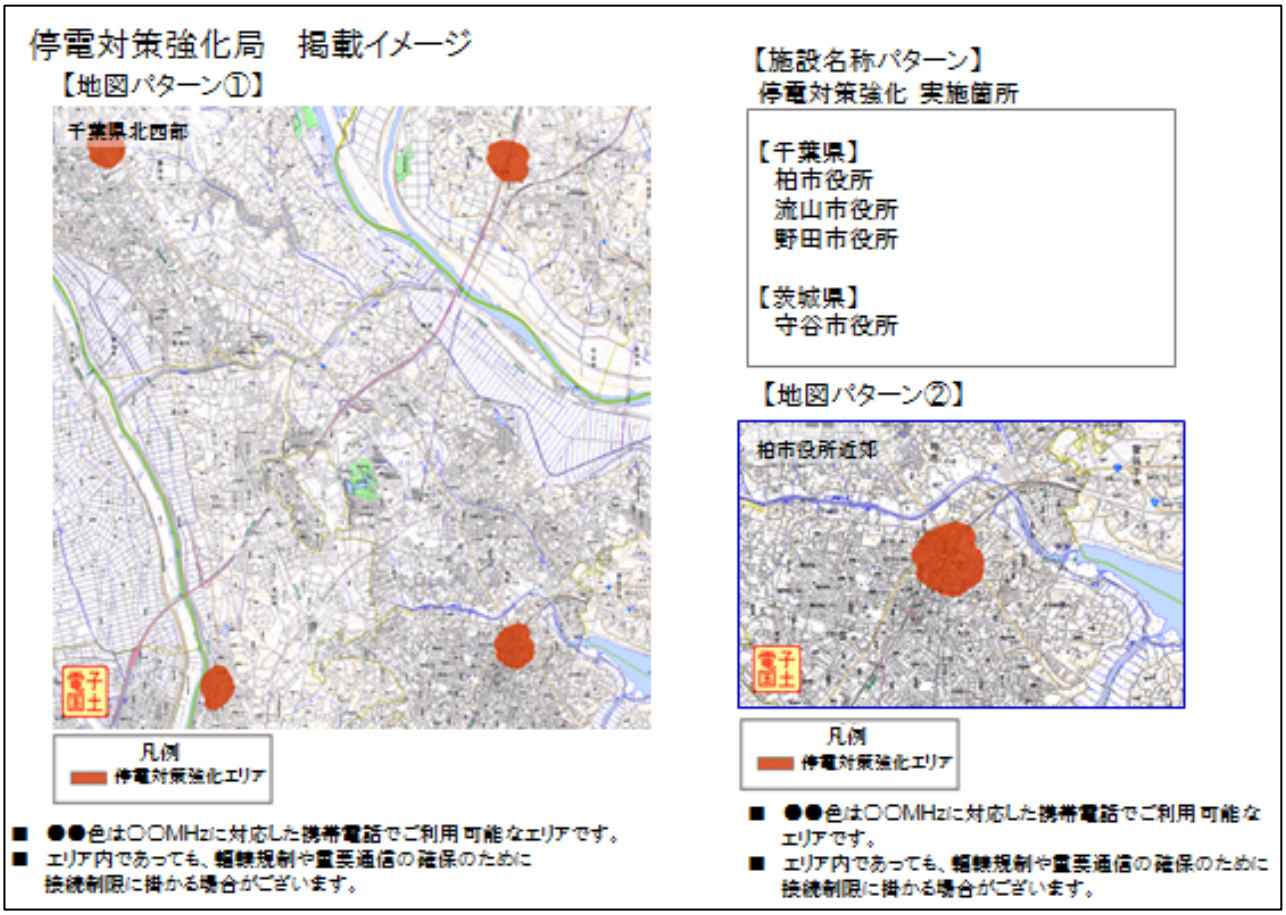

図 2.2.2.3.1-1　停電対策を強化した携帯電話基地局の表示イメージ

停電時に携帯電話がご利用いただけない場合がある施設・スポット

停電発生時、携帯電話がご利用いただけない場合がある施設・スポットをご案内いたします。

停電時は屋外など電波の届く場所に移動し、ご利用いただきますようお願いいたします。

市町村名	対象施設・スポット	
○○市	店舗	A ショッピングセンター、B デパート、･･･
	医療機関	C 大学病院、D 医院、･･･
	ホテル	E 旅館、F ホテル、･･･
	公共施設	G 地下街、H 合同庁舎、･･･
△△町	･･･	･･･

図 2.2.2.3.1-2　停電対策が講じられていない携帯電話基地局の表示イメージ

2.2.2.3.2　災害対策に関する装備品・資材に関する情報の公表について

災害の備えとして、通信ネットワークの復旧や、被災者への救援に必要な装備品、資材の配備台数を各社のホームページ上に公表する。具体的な公表項目等については、以下のとおりとすることが望ましい。

なお、必要時にレンタルで確保するケースが多い可搬型発電機等については、実態に合わないため対象外とする。

表 2.2.2.3.2-1　災害対策に関する情報の公表

項目	内容	配備数の表示方法
移動電源車	・外観写真	管区毎に台数を記載
通信衛星対応の移動無線基地局（車載型）	・外観写真 ・性能、カバー範囲（半径約○km 等）、音声最大接続数	管区毎・タイプ別に台数を記載
地上マイクロ回線対応の移動無線局（車載型）		
上記以外の移動無線基地局（車載型）		
可搬型の移動無線基地局		全国総数を記載

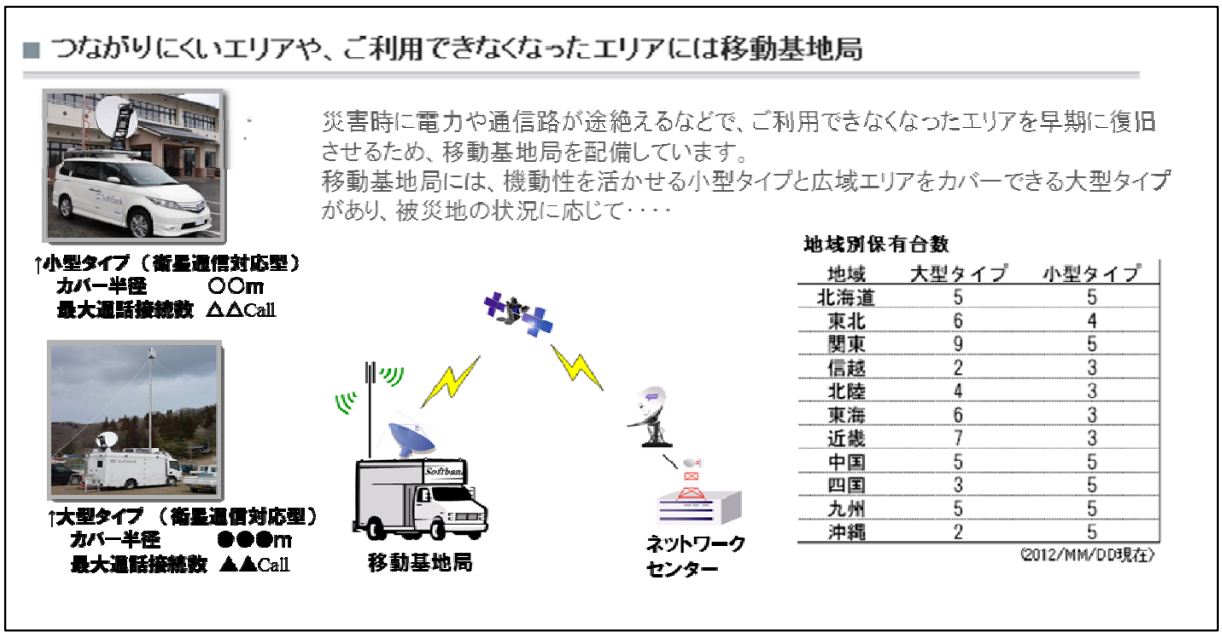

図 2.2.2.3.2-1　衛星通信対応の移動無線基地局（車載型）の公表イメージ

図 2.2.2.3.2-2　可搬型の移動無線基地局の公表イメージ

2.2.2.3.3　ネットワークの設計容量に関する基本的考え方、通信規制や重要通信の優先的取扱いに係る手法等に関する情報の公表について

ネットワークの設計容量に関する基本的考え方、通信規制や重要通信の優先的取扱いに係る手法等に関しては、電気通信事業者に共通した形で示すことが難しく、利用者に理解しやすい形で情報を公表するために、引き続き議論していくことが必要である。

2.2.2.3.4　災害対策等の情報の公表について

電気通信事業者は、利用者が簡単に災害対策等の情報を閲覧できるように、各社ホームページでの掲載位置やトップページから情報掲載ページまでの導線に配慮する。

また、ＴＣＡのホームページからも、各携帯電話事業者・ＰＨＳ事業者の災害対策情報に関するページにリンクを貼り、利便性の向上を図る。

2.2.2.4　情報の公表に関する現行基準の見直し

以上のＴＣＡにおける検討結果も踏まえ、情報の公表に関しての現行基準の見直しについては、以下のとおりである。

2.2.2.4.1　停電対策・災害対策が強化された携帯電話基地局のカバーエリア、ネットワークの設計容量に関する基本的考え方、通信規制や重要通信の優先的取扱いに係る手法等に関する情報の公表について

（管理基準）

現行基準には、既に「情報通信ネットワークの安全・信頼性の確保の取組状況を適切な方法により利用者に対して公開すること」との対策が存在しており、ＩＰネットワーク設備委員会の提言にある「停電対策・災害対策が強化された携帯電話基地局のカバーエリア、ネットワークの設計容量に関する基本的考え方、通信規制や重要通信の優先的取扱いに係る手法等」の公表等の考え方は、現行基準の対策の内容に含まれているものと考えられる。

しかしながら、ＩＰネットワーク設備委員会の提言に基づく情報の公表については、利用者にとって災害時においては極めて有用な情報になり得るため、情報の公表に関する電気通信事業者間の取組に差異が生じないよう、現行基準に適切な措置（現行対策の改正、新たな対策の追加、またはその他の措置）を講じることが適当である。

【関係基準：別表第２　１２.（１）関連】

2.2.2.4.2　ふくそうが発生した場合の状況及び通信規制の実施状況の公表について

現行基準には、ふくそう発生時の通信規制の実施状況等の公表に関する対策はない。

当該情報が公表されることによって、ふくそう発生時における他の通信手段を選択する利用者の増加、繰り返しダイヤルの減少が期待できるため、ネットワークの負荷軽減に有効と考えられることから、対策にその旨を追加することが適当である。

（実施指針）

事業	その他	自営	ユーザ
◎	◎	―	―

【関係基準：別表第２　１２.（２）追加】

2.2.2.4.3　災害時における音声通話以外の通信手段の利用等の呼びかけについて

現行基準には、災害時における音声通話以外の通信手段の利用等の呼びかけに関する対策はない。

手短な通信、音声お届けサービスや災害伝言用サービスの活用に関する周知・要請を行うことにより、災害時における通話の疎通の改善が期待されることから、対策にその旨を追加することが適当である。

（実施指針）

事業	その他	自営	ユーザ
◎	―	―	―

【関係基準：別表第２　１２.（３）追加】

2.2.2.5　情報の公表に関する今後の進め方について

ＴＣＡにおける検討結果は、電気通信事業者間で可能な限り共通化した公表事項を設けるとともに、事業者毎の情報提供内容の差異を少なくするとの観点を踏まえ、現時点において実現可能な範囲でまとめられたものである。これらの検討結果は、携帯電話事業者に限定されたものであり、ＰＨＳやその他のサービスについてまとめられたものではなく、また、ＩＰネットワーク設備委員会の提言等において電気通信事業者に求められている事項の全てを満たすものではないが、具体的な公表内容の共通化が初めて図られた点においては、評価されるべきものである。

今後、残された課題（ネットワークの設計容量に関する基本的考え方、通信規制や重要通信の優先的取扱いに係る手法等）については、引き続き、総務省と電気通信事業者間において継続して公表に向けての議論がなされることが重要である。

また、電気通信事業者にあっては、上記の情報の公表に併せて、自社の災害時の対策に関する紹介においては、災害時においても電気通信サービスが通常通りに利用できるといった過度な期待を利用者が抱くことがないよう、適切な情報提供に努めるとともに、既存情報提供内容の検証を行うことが期待される。

2.3　携帯電話通信障害対策連絡会により共有化されたベストプラクティスで、安全・信頼性基準へ反映が必要と認められる事項

重要なインフラである携帯電話における通信障害が続発したことを受けて、総務省は携帯電話通信障害対策連絡会を開催し、これまでに発生した重大な事故と同様の通信障害の発生を防止するため、各電気通信事業者の設備について総点検を実施するよう要請した。その後、各社の総点検の結果報告をとりまとめ、全事業者の今後の取組強化に参考となるもの（いわゆるベストプラクティス）として、同連絡会において情報共有されている。このうち、基準の見直しの検討で参照したベストプラクティスの概要を以下に示す。

○ バーストトラヒック及び制御信号等対策

・ スマートフォンの制御信号を抑制するため、1回の無線接続で複数のアプリケーションが通信を行えるように無線接続手順の変更を実施予定。
・ 故障発生時等の過負荷にも確実に対応するため、各装置の最大処理能力を超える負荷で試験を実施するとともに、商用網でのトラヒック変動に確実に対応するため、複数トラヒック条件での試験を実施。このような取組を開発プロセスに組み込み、過負荷時の安定動作に向けた負荷試験の強化を継続的に実施。
・ 主要なシステムの導入時の負荷試験について、過負荷条件として商用網のトラヒックパターンを利用して、机上試験のみならず、実機試験を実施していることを確認。
・ 他社の事故で利用者認証サーバの処理能力不足が原因であったことを踏まえ、自社サーバについて一時的なトラフィックの増加にも十分対応できる処理能力であることを確認。

○ ハードウェアの信頼性向上

・ 設備導入時のハードウェアの品質評価に関するガイドラインを制定し、社内の基準を統一。予備系装置への切替が円滑に動作しない場合の緊急手段（電源断、リセット等）に対する評価も追加。

○ バックアップ切替動作の確認

・ 新装置の導入以前（導入判定等）において、設備部門、開発部門、監視部門、技術支援部門の間でバックアップ切替動作の結果を点検するプロセスが確立していることを確認。

○ 社内の関係部門間の連携

・ 3万以上の利用者を収容する全ての設備の作業は、常時サービス監視部門と作業実施部門間の電話会議で作業進捗を連絡する等の連携強化。

○ 事故情報等の周知

・ 社内緊急体制確立前に、保守・監視・措置部門から災害対策対応部門へ「緊急速報（情報周知）」を発出できるよう対応フローを整備。これにより、故障等を認知後、速やかにホームページ等で情報提供するための体制を確立。また、利用者対応部門でも、「緊急速報（情報周知）」を基に利用者対応ができるよう対策を講じるとともに、ショップにおいて、掲載したホームページを印刷して店頭に掲示する体制を構築。

○ 電気通信事業者間等の情報共有
・ 携帯電話事業者全社及び電気通信事業者協会において、電気通信事故の再発防止策のうち他事業者の今後の取組強化に参考となるもの（いわゆるベストプラクティス）について業界で情報共有し、事故防止に向けての取組を確認
・ 被災した通信設備の復旧について、今回の取組のうち、有効な取組をベストプラクティスとして共有しつつ、移動基地局の更なる配備や衛星回線の活用など、今回の対応を踏まえた応急復旧対応に関する取組を進める。
・ アプリを提供する企業にモバイルネットワークに配慮したアプリ設計について協力要請。

2.3.1　バーストトラヒック及び制御信号等対策について

（設備等基準）

2.3.1.1　モバイルインターネット接続サービスにおける設備容量の確保について

現行基準には、既にモバイルインターネット接続サービスの設備容量に関する対策が存在する。現行基準の表現である「通信の集中」については、震災時など一時的なトラヒックの急激な増加に対しても十分に対応できるような印象を与える記述であるため、実際に即した「通信量の増加」の表現に変更することが適当である。

また、現状の実施指針は「技術的な難易度等を考慮して段階的に実施すべきである。」との分類であるが、最近のスマートフォンの普及による通信量の増加を一因とする電気通信事故の発生を踏まえ、実施指針を現状より強化することが適当である。

（実施指針）

事業	その他	自営	ユーザ
◎＊→◎	－	－	－

【関係基準：別表第１　第１　１.（６）】

（管理基準）

2.3.1.2　将来のトラヒック増加等を考慮した設計について

現行基準には、将来の規模の拡大、トラヒック増加及び機能の拡充を考慮した設計をす

るように記載されているが、「端末の挙動」に関する観点が含まれていない。
　端末の挙動によって電気通信事故が生じたケースがあったことから、今後はネットワーク設計においても端末の挙動によるトラヒック増加をも十分に考慮することが必要と考えられるため、対策にその旨を追加することが適当である。
【関係基準：別表第２　１.（２）イ】

2.3.1.3　バーストトラヒック及び制御信号対策について

　現行基準には、最近の電気通信事故の要因として挙げられているバーストトラヒック及び制御信号を抑制するための対策は存在しない。
　後述する 3.2.2 及び 3.2.3 に示す対策を講じることによって、電気通信事故の減少が期待できることから、バーストトラヒック及び制御信号対策を講じることを対策に追加することが適当である。
（実施指針）

事業	その他	自営	ユーザ
◎	―	―	―

【関係基準：別表第２　１.（２）追加】

2.3.1.4　過負荷試験の実施について

　現行基準には、最大処理能力を超えた負荷をかけて通信機器等の試験を実施することについての対策はない。過負荷がかかったときの通信機器等の動作を事前に確認することは、事故の未然防止に資するものであることから、対策に追加することが適当である。
（実施指針）

事業	その他	自営	ユーザ
○	―	―	―

【関係基準：別表第２　１.（５）追加】

2.3.2　ハードウェアの信頼性向上について

　現行基準には、ソフトウェアの信頼性向上についての対策は存在するが、ハードウェアの信頼性向上についての対策はない。
　設備導入時の重要なハードウェアの品質評価や、当該品質評価に基づく内部の検証等は、事故の未然防止に資するものと考えられることから、基準に追加することが適当である。
（実施指針）

事業	その他	自営	ユーザ
◎	◎	◎	◎

【関係基準：別表第２　１.（５）追加】

2.3.3　バックアップ切替動作の確認について

現行基準には、機器等の冗長化によって信頼性を向上させる対策は存在するが、冗長化された機器の切替動作を確認する対策はない。

バックアップ切替が正常に動作するか確認することは、事故の未然防止に資するものと考えられることから、基準に追加することが適当である。

（実施指針）

事業	その他	自営	ユーザ
◎	◎	○	○

【関係基準：別表第２　１.（５）追加】

2.3.4　社内の関係部門間の連携について

現行基準には、ベンダー、事業者等の関係者間の連携についての対策は存在するが、社内の関係部門間との連携についての対策はない。

社内の関係部門間の連携が図られていれば、電気通信事故の防止、利用者への被害拡大の回避が可能であった事例が散見されることから、現行対策の改正または追加により措置を講じることが適当である。

【関係基準：別表第２　１.（１）、２.（１）、３.（１）及び４.（１）関連】

2.3.5　事故情報等の周知について

現行基準には、事故・障害等の状況を利用者に対して公開する旨の対策は存在するが、同対策には公開するタイミングに関する記述がない。

事故･障害等の情報は利用者に対して迅速に提供することが重要であるから､｢速やかに｣公開するようにタイミングの概念を追加することが適当である。

【関係基準：別表第２　１２.（２）】

2.3.6　電気通信事業者間等の情報共有について

現行基準には、電気通信事業者間や電気通信事業者とアプリケーション開発事業者の間

の情報共有についての対策はない。

電気通信事故の状況、再発防止策や災害時における有効な応急対策など事業者共通の問題となりえる事例を情報共有することは、業界全体の事故、災害対策にも有効であること、また、電気通信事業者とアプリケーション開発事業者の間で、ネットワークの負荷を考慮したアプリケーションの開発手法等について情報共有することは、3.2.3 に後述する制御信号等対策にも有効であることから、対策に追加することが適当である。

（実施指針）（事業者間の情報共有）

事業	その他	自営	ユーザ
◎＊	－	－	－

【関係基準：別表第２　１２.（６）追加】

（実施指針）（電気通信事業者とアプリケーション開発事業者間の情報共有）

事業	その他	自営	ユーザ
○	－	－	－

【関係基準：別表第２　１２.（６）追加】

2.4　電気通信事業法以外の関係法令の規定、電気通信事業関係団体の取組状況により、安全・信頼性基準への反映が必要と認められる事項

電気通信事業法関係法令以外に、情報通信ネットワークの安全・信頼性基準への反映が必要と考えられる法令を、以下に挙げる。

【青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律（平成二十年六月十八日法律第七十九号）】

- 携帯電話インターネット接続役務提供事業者は、携帯電話インターネット接続役務を提供する契約の相手方又は携帯電話端末若しくはＰＨＳ端末の使用者が青少年である場合には、青少年有害情報フィルタリングサービスの利用を条件として、携帯電話インターネット接続役務を提供しなければならない。ただし、その青少年の保護者が、青少年有害情報フィルタリングサービスを利用しない旨の申出をした場合は、この限りでない。＜第１７条第１項＞
- インターネット接続役務提供事業者は、インターネット接続役務の提供を受ける者から求められたときは、青少年有害情報フィルタリングソフトウェア又は青少年有害情報フィルタリングサービスを提供しなければならない。ただし、青少年による青少年有害情報の閲覧に及ぼす影響が軽微な場合として政令で定める場合は、この限りでない。＜第１８条＞

（管理基準）

現行基準には、上記の法令等と同様な利用者保護、電気通信サービスの不適正利用の観点からの対策として、電子メール対策（別表第１　設備等基準　第１　設備基準　１．一般基準(7)電子メールによる一方的な広告・宣伝等への対策）が存在する。

当該基準は、電子メールの受信拒否機能が事業者のネットワークでしか対応できなかったときに策定されたものであり、現在においては利用者での端末においても迷惑メール対策が可能となっている。

また、インターネット上での利用者保護、不適正利用対策の対象としては、迷惑メールだけでなく、有害情報からの青少年保護を目的とした「青少年有害情報フィルタリング」等が電気通信事業者に要請されている。

こうした状況を踏まえ、現状基準に、迷惑メールの取組に加え、「青少年有害情報フィルタリング」等、電気通信事業者が実際に取り組んでいる活動を利用者に適切に周知することを新たな対策として規定することは、利用者保護及び不適正利用対策の観点から、適当である。

なお、迷惑メールの対策は、モバイルインターネット接続サービスに限定した記述であったが、当該対策にモバイルインターネット接続サービスに限定する理由がないことから、「モバイルインターネット接続サービス」の表現を削除することが適当である。

更に、これら利用者保護に係る不適正利用対策に関する分類は、後述する「１２．安全・信頼性の確保等の情報公開、電気通信事業者の取組み等」の「電気通信サービスの不適正利用の防止に関する周知、取組み」として、管理基準に位置づけることが適当である。

（実施指針）（迷惑メール）

事業	その他	自営	ユーザ
○	ー→○	―	―

【関係基準：別表第１　第１　１．（７）→　別表第２　１２．（５）移行】

（実施指針）（フィルタリング等）

事業	その他	自営	ユーザ
◎	◎	―	―

【関係基準：別表第２　１２．（５）追加】　注　実施指針については、対策の内容により異なる。

2.5　情報セキュリティ対策の強化に必要と認められる事項

情報セキュリティ対策に関する事項の見直しについては、関係機関が策定した情報セキュリティに関するガイドラインとの比較と、情報セキュリティに関する事故事例との比較を行うことによって、現行安全・信頼性基準に不足している対策がないか検討を行った。

2.5.1　関係ガイドラインとの比較

情報セキュリティに関するガイドラインは複数存在するが、特に安全・信頼性基準と関連性が深く、整合性の検証が必要と考えられる２つのガイドライン（内閣官房情報セキュリティセンターの「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第３版）対策編」と（社）電気通信事業者協会の「電気通信分野における情報セキュリティ確保に係る安全基準（第２版)」）について、これらのガイドラインには存在して、安全・信頼性基準にはない情報通信ネットワークのセキュリティに関する対策の比較を行った。

比較結果は別添２のとおりであり、安全・信頼性基準はこれらのガイドラインをほぼカバーしていると考えられる。

2.5.2　「情報通信ネットワーク 安全・信頼性基準」と情報セキュリティに関する事故事例との比較

最近の情報セキュリティに関する事故について、事故の要因となった問題点を公開された情報から分析し、安全・信頼性基準と照らし合わせ、安全・信頼性基準に不足している対策はないか確認を行った。

確認結果は別添３のとおりであり、安全・信頼性基準に記載されている対策は、事故の要因となった問題点をカバーしていると考えられる。

2.5.3　検討結果

以上の比較結果を踏まえると、情報セキュリティに関する安全・信頼性基準の見直しが必要との結論を導き出すまでには至らなかった。

なお、現行の安全・信頼性基準など情報セキュリティに関するガイドライン、方針は情報セキュリティ対策を網羅的に規定化しているため、漏れ等はない傾向にあるが、新たな脅威に対しては、迅速に具体的な対策を講じることが重要であるとの意見があった。

2.6　その他見直しが必要と認められる事項

現行基準には、ふくそう防止にための利用者への周知、協力要請、メンテナンスによる緊急通報停止時の周知、コンピュータウィルス情報の利用者周知等の利用者保護の対策が、設置等基準、管理基準の中に散在している。

こうした対策は、それぞれ関連する対策の中で基準化していくことのほか、利用者保護の観点を踏まえ、利用者視点からの電気通信サービスの課題等を一括した枠組み（「１２．安全・信頼性の確保等の情報公開、電気通信事業者の取組み等」）の中で、再掲していくことが適当である。　【関係基準：別表第２　３．（９）ア　等】

また、現行基準の表現の一般化や、通信技術の進展等によって使われなくなる機器に関する基準の削除など、規定の整備による基準の見直しを行うことが適当である。【関係基準：別表第１　第１　１．（１０）カ　等】

2.7　その他

現行基準は、告示である「情報通信ネットワーク安全・信頼性基準」（昭和６２年２月１４日郵政省告示第７３号）により制定されているほか、実務上の要請から、当該告示の「解説」が作成されている。

現行基準の見直しに伴う当該解説の見直しについては、現行基準の見直しの趣旨を踏まえて、別添１の「情報通信ネットワーク安全・信頼性基準の見直しに関する論点（方向性）」に記載されていた内容を含め、総務省、電気通信事業者協会等の関係団体で行っていくことが適当である。

第３章　スマートフォン普及に伴う技術基準の見直し

3.1　スマートフォンに係る電気通信事故の概要

3.1.1　スマートフォン関係の事故の多発

電気通信事業法令では、電気通信設備の故障により電気通信役務の全部又は一部（付加的な機能の提供に係るものを除く。）を停止させた事故であって、影響を受けた利用者の数が３万以上かつその影響時間が２時間以上のもの（又は、海底ケーブル等の重要な電気通信設備の故障により全て通信の疎通が２時間以上不能となったもの）を重大な事故と位置付け、発生時の即時報告と、30 日以内の詳細報告を求めている。

平成２３年度は、１７件の重大な事故が発生している。このうち、スマートフォンの利用者のみに影響があった事故は４件、スマートフォン以外の携帯電話利用者にも影響があった事故は６件発生している。

前年度（平成２２年度）に発生した重大な事故１５件のうち、携帯電話に関する事故は３件のみであったから、特に平成２３年度にスマートフォン関係の事故が多発したと判断される。

スマートフォンは、急速に普及しており、平成２３年度末の契約数は前年度の約２．６倍に達すると予測されている。また、携帯電話端末の年間国内出荷台数のうち、スマートフォンの占める比率が急速に上昇を続けており、平成２４年度には６０％を超えるとの見通しもある。このため、今後もスマートフォン関係の事故の多発が危惧されることから、その安全・信頼性対策の向上を通じて、事故の発生を防止し、又はその影響の極小化を図ることが適切である。

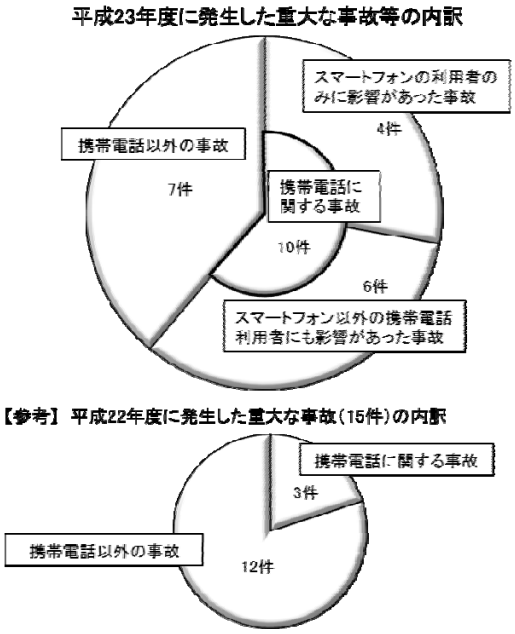

図 3.1.1-1　重大な事故等の内訳

3.1.2　事故原因の分析

平成２３年度に発生した１７件の重大な事故のうち、スマートフォンに関係する１０件について、その概要を分類すると、おおむね次のとおりである。

表 3.1.2-1　事故原因の分析

分　　類	スマートフォンに関係する事故の件数	うちスマートフォンのみに関係するもの	原　因　等 （スマートフォンのみの事故について記載）
○冗長機能の不具合に関する事故	－	－	
・予備設備等への切替に失敗した事故	3		
・予備設備等に切り替わったが、認証関係設備でふくそうが発生した事故	1	1	○中継スイッチが故障。一旦ネットワークから切断された多数の端末から接続に係る認証要求が一斉に行われたことにより、認証サーバの処理能力が大幅に低下。
・予備設備等に切り替わったが、その後の切替手順に不備があった事故	2	2	○スマートフォンに対してＩＰアドレスを割り当てる装置が故障。予備設備への切替後も、切替手順の不備により、携帯電話端末と予備設備間の通信確立に時間を要した。 ○中継スイッチが故障。スイッチ復旧後も、切替手順の不備により、一部の通信確立に時間を要した。
○設備の設計・設定・配備に誤りが存在した事故	2	1	○利用者のメールボックス情報等を格納するサーバ（メール情報サーバ）への問合せ件数が、同時アクセスの上限値を超過したことにより、同サーバの処理能力が大幅に低下。
○電源設備で障害が発生し、サーバへの電源の供給が停止した事故	1		
○事業用電気通信設備に不正プログラムが混入し、設定情報が削除された事故	1		

すなわち、スマートフォンの普及により増加することが危惧される事故としては、第一に、冗長機能の不具合に関するものが想定される。

スマートフォンに限らず、冗長機能については一般的に不具合やそれに関連する事故の多いことが知られている。しかし、スマートフォン関係の事故の特色として、予備設備等に切り替わった後に「認証関係設備でふくそうが発生した」又は「その後の切替手順に不

備があった」といった事例の多いことについては、注意を要する。
　また、「設備の設計・設定・配備に誤りが存在した」という事例のあったことも留意すべきである。

①　認証関係設備におけるふくそうの発生
　スマートフォンでは、携帯電話として一般的な位置登録や認証を行う設備とは別に、個別のサービスを提供するためのサービス毎の認証関係設備が設定される。
　スマートフォンを収容する電気通信設備に何らかのトラブルがあり、予備設備に切り替わる場合、当該切替えに係るスマートフォンの接続状態は損なわれ、予備設備に改めて接続し直すこととなる。すなわち、トラブルのあった電気通信設備に収容されるスマートフォンの端末数が多ければ、認証関係設備には、同時に多数の認証の処理要求が行われることとなる。
　平成２３年度には、予備設備への切替えに伴い、認証関係設備にこのように瞬間的に多数の処理要求が行われた結果、当該認証関係設備の機能が損なわれ、重大な事故に至ったものが１件あった。
　以下では、瞬間的に多数生じるこうした処理要求のことを、「バーストトラフィック」と呼称する。

②　切替手順の不備
　平成２３年度には、予備設備等に切り替わった後の切替手順に不備があったための重大な事故の事例が２件見受けられた。このうち１件は、「①認証関係設備におけるふくそうの発生」と同様にバーストトラフィックが発生した影響により設備が不安定となったことに起因するものであり、他の１件は設備の故障に起因する偶発的なものである。

③　設備の設計・設定・配備の誤り
　平成２３年度には、設備の設計・設定・配備に誤りがあったための重大な事故の事例が２件見受けられた。このうち１件はスマートフォンのみに関係するものであり、他の１件はスマートフォン以外も含めた多くの携帯電話に支障が生じたものである。いずれも、端末から送信される信号量の見積もりを誤り、十分な処理能力を具備した設備を配備できなかったことに起因するものである。
　特に、長時間にわたり多くの携帯電話に支障が生じた後者の事例では、利用者によりスマートフォンに搭載されたさまざまなアプリに起因して発生する制御信号が事業者の想定を大幅に超えていたことが原因である。

3.2　電気通信事故を踏まえて技術基準の見直しの必要性

3.2.1　バーストトラフィック対策及び制御信号対策の必要性
　スマートフォンはなお一層の普及が見込まれることから、今後も重大な事故の発生が危

惧される。その最大の事故原因として想定されるものは、「バーストトラフィックの発生」であり、次いで「制御信号の増加」である。

将来的な事故の発生を防止し、又はその影響の極小化を図るためには、あらかじめこれらに対する措置を講じることが適切である。

3.2.2　バーストトラフィック対策

バーストトラフィックの発生による事故を防止するための対策としては、まず、バーストトラフィックの発生自体を防止又は抑制することが考えられる。

バーストトラフィックは、例えば設備の切替え等に伴い、多数の端末が同時に処理を要求するために発生するものであるから、次のような措置を講じることが効果的である。これらはいずれも、一部の事業者で既に採用されているものである。

①設備が予備に切り替わった場合、これまでは HLR が端末から改めて位置情報を取得していたが、交換機から位置情報を取得する等、一斉に端末への位置情報要求を行わない仕組みを用いることする（位置情報等の抑制）

②ネットワーク内で通信が途切れた場合、これまでは全ての端末が再接続していたが、途切れた際に通信中の端末のみが再接続することとする（再接続の抑制）

上記のほか、バーストトラフィックが発生した場合であっても、あらかじめそれに耐えられる設備増強を図る等、事業者の実情に合わせた各種の対策が想定される。

3.2.3　制御信号等対策

制御信号その他のトラフィックの増加による事故を防止するための対策としては、根本的には、関係設備の処理能力の増強が求められる。

また、スマートフォンの場合には、複数のアプリケーションが多量の制御信号を発信しており、現にそれを原因とする重大な事故が発生している。このため、制御信号の量の低減に向けて、次のような措置を講じることが効果的である。これらはいずれも、一部の事業者で既に採用されているものである。

①Network Controlled Fast Dormancy や GCM 等、標準化や国際動向に沿って対策として有効な手法を各事業者が積極的に取り入れ、制御信号量の低減対策を講じることとする（制御信号抑制技術の採用）

②トラフィックが特定の設備に過度に集中しないよう、端末を柔軟に分散して収容できる設備構成とする（負荷の分散）

上記のほか、制御信号の量を予測してあらかじめ十分な余裕度をもって設備増強を図る、制御信号の送信特性に応じてネットワークを最適化する等、事業者の実情に合わせた各種の対策が想定される。

3.3　技術基準の見直しの案

以上から、スマートフォンの普及に伴う事故の発生を防止し、又はその影響の極小化を図るため、新たにバーストトラフィック対策及び制御信号対策を講じることとし、関係の

技術基準を見直すべきである。

見直しに当たっては、スマートフォンを含む携帯電話の設備について、例えば次のような措置を講じることとするべきである。

①バーストトラフィック対策

・バーストトラフィックの発生を防止又は抑制する措置（例：位置情報等の取得のための手順の見直し、一斉再接続の抑制等）

又は

・バーストトラフィックの発生を考慮し、十分に余裕を持った処理能力の確保

②制御信号対策

・制御信号の増加による処理を低減させるための措置（例：制御信号抑制技術の採用、負荷の分散等）

又は

・制御信号の増加を考慮し、十分に余裕を持った処理能力の確保

いずれの対策においても、ネットワークの構成や個々の設備の機能の違い等に応じて、個別の措置の講じられる対象となる設備は異なることとなる。しかし、一般に、スマートフォンを含む携帯電話の端末が他の設備の制御の下で動作していること、また、各事業者が端末以外の設備により現に各種の対策を講じていることから、上記対策に係る措置については、端末以外の電気通信設備について講じられることを念頭においている。

なお、ごく少数の端末設備を収容する小規模の設備等、そもそもこれら対策を講じる必要がないものについては、適用対象から除外することが適当である。

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
第1　設備基準								
1.一般基準								
(1)通信センターの分散	ア 当該センターの損壊又は当該センターが収容する設備の損壊若しくは故障（以下「故障等」という。）が情報通信ネットワークの機能に重大な支障を及ぼす通信センター（以下「重要な通信センター」という。）は、地域的に分散して設置すること。	○ ↓ ◎＊	○	○	○	事業用電気通信設備規則の改正（平成24年9月1日施行）	（大規模災害対策） ＜第15条の3＞ 電気通信事業者は、大規模な災害により電気通信役務の提供に重大な支障が生じることを防止するため、事業用電気通信回線設備に関し、あらかじめ次の各号に掲げる措置を講じるように努めなければならない。 ＜第15条の3第3号＞ 電気通信役務に係る情報の管理、電気通信役務の制御又は端末設備等の認証等を行うための電気通信設備であつて、その故障等により、広域にわたり電気通信役務の提供に重大な支障を及ぼすおそれのあるものは、複数の地域に分散して設置すること。この場合において、一の電気通信設備の故障等の発生時に、他の電気通信設備によりなるべくその機能を代替することができるようにすること。	○省令に大規模災害対策の努力義務が規定化。 ○現行基準の「重大な支障を及ぼす通信センターは,地域的に分散して設置すること」と改正省令の「広域にわたり電気通信役務の提供に重大な支障を及ぼすおそれのあるものは、複数の地域に分散して設置すること」の趣旨は同一と認められることから、本文の見直しは不要。 【検討結果】 ○現行基準には、既に重要な通信センター等の地理的分散設置に関する対策が存在するが、同対策の現状における実施指針は「実施が望ましい」との分類であるため、実施指針を、省令改正を踏まえて現状より強化することが適当である。 《本文2.1.4参照》
						IPネットワーク設備委員会報告	機能停止により電気通信役務の提供に広域にわたり重大な支障を及ぼすおそれのある基幹的な電気通信設備について、地理的分散を図ること。	
	イ 重要な通信センターについては、他の通信センターでバックアップできる機能を設けること。	○	○	○	○	事業用電気通信設備規則の改正（平成24年9月1日施行）	（大規模災害対策） ＜第15条の3＞ 電気通信事業者は、大規模な災害により電気通信役務の提供に重大な支障が生じることを防止するため、事業用電気通信回線設備に関し、あらかじめ次の各号に掲げる措置を講じるように努めなければならない。 ＜第15条の3第3号＞ 電気通信役務に係る情報の管理、電気通信役務の制御又は端末設備等の認証等を行うための電気通信設備であつて、その故障等により、広域にわたり電気通信役務の提供に重大な支障を及ぼすおそれのあるものは、複数の地域に分散して設置すること。この場合において、一の電気通信設備の故障等の発生時に、他の電気通信設備によりなるべくその機能を代替することができるようにすること。	○省令に大規模災害対策の努力義務が規定化。 ○現行基準の「他の通信センターでバックアップできる機能を設けること」と改正省令の「他の電気通信設備によりなるべくその機能を代替することができるようにすること」の趣旨は同一と認められることから、本文の見直しは不要。 【検討結果】 ○「なるべく」との表現があることから、現行の実施指針の見直しは不要である。
(2)代替接続系統の設定	交換網の場合は、二つの重要な通信センター間を結ぶ接続系統の障害に対し、その代替となる他の通信センター経由のう回接続系統を設けること。	○	○	○	○			
(3)異経路伝送路設備の設置	ア 重要な通信センター間を結ぶ伝送路設備は、複数の経路により設置すること。	○	－	○	－			
	イ 重要な光加入者伝送路は、ループ化等による2ルート化を促進すること。	○	－	○	－			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目		対策	実施指針				資料名	内容	
			事業用	その他	自営	ユーザ			
		（追加）	◎	－	－	－	事業用電気通信設備規則の改正（平成24年9月1日施行）	（予備機器等） ＜第4条第4項＞ 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されなければならない。ただし、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は、この限りでない。	○省令に交換設備相互間を接続する伝送路設備に対する複数経路の設置が新たに規定化。 【検討結果】 ○現行基準には、重要な通信センター間の伝送路設備を複数経路で設置する旨の対策は存在するが、省令で追加された交換設備相互間の伝送路設備に対する複数経路の設置に関する対策はない。交換設備相互間の伝送路設備に複数経路の設置を講じることは、伝送路設備の障害発生時における通信の途絶防止に資することから、基準に改正省令内容を追加することが適当である。 《本文2.1.1参照》
							IPネットワーク設備委員会報告	交換設備相互間の伝送路設備については、地理的に複数の経路を設置することが困難な場合、又は同等以上の耐災害性の確保が期待できる他の措置が講じられている場合を除き、複数の経路により設置すること。	
		（追加）	◎＊	－	－	－	事業用電気通信設備規則の改正（平成24年9月1日施行）	（大規模災害対策） ＜第15条の3＞ 電気通信事業者は、大規模な災害により電気通信役務の提供に重大な支障が生じることを防止するため、事業用電気通信回線設備に関し、あらかじめ次の各号に掲げる措置を講じるように努めなければならない。 ＜第15条の3第1号＞ 三以上の交換設備をループ状に接続する大規模な伝送路設備は、複数箇所の故障等により広域にわたり通信が停止しないよう、当該伝送路設備により囲まれる地域を横断する伝送路設備の追加的な設置、臨時の電気通信回線の設置に必要な機材の配備その他の必要な措置を講じること。	○省令にループ状の大規模な伝送路設備により囲まれる地域を横断する伝送路設備の追加的な設置に関する努力義務が新たに規定化。 【検討結果】 ○省令改正により、電気通信事業者は、ループ状に接続する大規模な伝送路設備は複数箇所の故障等により通信が停止しないよう、当該大規模な伝送路設備を横断する伝送路設備の追加的な設置の措置を求められていることから、基準に改正省令内容を追加することが適当である。 《本文2.1.4参照》
	⑷電気通信回線の分散収容	重要な通信センター間を結ぶ電気通信回線の収容は、異なる伝送路設備に分散して行うこと。	○	－	○	－			
	⑸モバイルインターネット接続サービスにおける設備の分散等	重要な設備の事故等が全国的な又は相当広範囲の利用者に影響する場合は、当該設備について、地域的に分散して設置するとともに分散した設備を複数の経路で接続し、故障等による影響範囲を限定すること。	○ ↓ ◎＊	－	－	－	事業用電気通信設備規則の改正（平成24年9月1日施行）	（大規模災害対策） ＜第15条の3＞ 電気通信事業者は、大規模な災害により電気通信役務の提供に重大な支障が生じることを防止するため、事業用電気通信回線設備に関し、あらかじめ次の各号に掲げる措置を講じるように努めなければならない。 ＜第15条の3第3号＞ 電気通信役務に係る情報の管理、電気通信役務の制御又は端末設備等の認証等を行うための電気通信設備であつて、その故障等により、広域にわたり電気通信役務の提供に重大な支障を及ぼすおそれのあるものは、複数の地域に分散して設置すること。この場合において、一の電気通信設備の故障等の発生時に、他の電気通信設備によりなるべくその機能を代替することができるようにすること。	○省令に大規模災害対策の努力義務を新たに規定。 ○現行基準の「全国的な又は相当広範囲の利用者に影響する場合は、当該設備について、地域的に分散して設置する」と改正省令の「広域にわたり電気通信役務の提供に重大な支障を及ぼすおそれのあるものは、複数の地域に分散して設置すること」の趣旨は同一と認められることから、本文の見直しは不要である。 【検討結果】 ○現行基準には、既に重要な通信センター等の地理的分散設置に関する対策が存在するが、同対策の現状における実施指針は「実施が望ましい:○」との分類であるため、実施指針を、省令改正を踏まえて現状より強化することが適当である。 《本文2.1.4参照》
							IPネットワーク設備委員会報告	機能停止により電気通信役務の提供に広域にわたり重大な支障を及ぼすおそれのある基幹的な電気通信設備について、地理的分散を図ること。	

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
(6)モバイルインターネット接続サービスにおける設備容量の確保	サーバー及びゲートウェイの設備は、通信の集中を考慮した適切な容量のものを設置すること。	◎＊ ↓ ◎	－	－	－	ベストプラクティス（ソフトバンクモバイル）	他社の事故で利用者認証サーバの処理能力不足が原因であったことを踏まえ、自社サーバについて一時的なトラフィックの増加にも十分対応できる処理能力であることを確認。	【検討結果】 ○現行基準には、既にモバイルインターネット接続サービスの設備容量に関する対策が存在する。現行基準の表現である「通信の集中」については、震災時など一時的なトラヒックの急激な増加に対しても十分に対応できるような印象を与える記述であるため、実際に即した「通信量の増加」の表現に変更することが適当である。 　また、現状の実施指針は「技術的な難易度等を考慮して段階的に実施すべきである。」との分類であるが、最近のスマートフォンの普及による通信量の増加を一因とする電気通信事故の発生を踏まえ、実施指針を現状より強化することが適当である。 《本文2.3.1.1参照》
(7)電子メールによる一方的な広告・宣伝等への対策	モバイルインターネット接続サービスにおいては、利用者が指定した特定の条件に該当する電子メールの受信を拒否する等の機能を設けること。	○	－ ↓ ○	－	－			【検討結果】 ○当該基準は、電子メールの受信拒否機能が事業者のネットワークでしか対応できなかったときに策定されたものであるため、設備等基準に分類されていたもので、現在においては利用者での端末においても迷惑メール対策が可能となっている。 　迷惑メールの分類は、「12. 安全・信頼性の確保等の情報公開、電気通信事業者の取組み等」の「電気通信サービスの不適正利用に関する周知、取組み」として、管理基準に位置づけることが適当である。 ○また、迷惑メールの対策は、モバイルインターネット接続サービスに限定した記述であるが、当該対策にモバイルインターネット接続サービスに限定する必要もないことから、「モバイルインターネット接続サービス」の表現を削除することが適当である。 《本文2.4参照》
(8)予備の電気通信回線の設定等	ア 重要な伝送路設備には、予備の電気通信回線を設定すること。ただし、他に疎通確保の手段がある場合は、この限りでない。	◎	－	◎	－			【検討結果】 △基準の「他の疎通確保の手段」の例として、解説に「マイクロエントランス無線回線」や「衛星回線」等を紹介することが適当。
	イ 重要な伝送設備には、予備の電気通信回線に速やかに切り換える機能を設けること。	◎	◎	◎	◎			
(9)情報通信ネットワークの動作状況の監視等	ア 重要な伝送路設備の動作状況を監視し、故障等を速やかに検知、通報する機能を設けること。	◎	－	◎＊	－			
	イ 重要な電気通信回線の動作状況を監視し、故障等を速やかに検知、通報する機能を設けること。	－	◎	－	◎＊			
	ウ 重要な伝送路設備の動作状況を統合的に監視する機能を設けること。	○	－	○	－			
	エ 重要な電気通信回線の動作状況を統合的に監視する機能を設けること。	－	○	－	○			
	オ 交換設備には、トラヒックの疎通状況を監視し、異常ふくそう等を速やかに検知、通報する機能を設けること。ただし、通信が同時に集中することがないようこれを制御する措置を講ずる場合は、この限りでない。	◎	◎	○	○			
	カ 交換設備には、通信の接続規制を行う機能又はこれと同等の機能を設けること。ただし、通信が同時に集中することがないようこれを制御する措置を講ずる場合は、この限りでない。	◎	◎	○	○			
	キ 交換設備には、利用者に異常ふくそうを通知する機能を設けること。ただし、通信が同時に集中することがないようこれを制御する措置を講ずる場合は、この限りでない。	◎	○	○	○			
	クトラヒックの疎通状況を統合的に監視する機能を設けること。	○	○	○	○			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目		対策	実施指針				資料名	内容	
			事業用	その他	自営	ユーザ			
		（追加）	◎	－	－	－	事業用電気通信設備規則の改正（平成24年9月1日施行）	（災害時優先通信の優先的取扱い） ＜第35条の2の2第2項＞ 事業用電気通信回線設備は、前項第一号の機能により他の通信の制限又は停止を行つた場合において、災害時優先通信及び他の通信の疎通の状況を記録することができるものでなければならない。	○省令に電気通信回線設備の機能として、「災害時優先通信及び他の通信の疎通の状況を記録することができる機能」が新たに規定化。 【検討結果】 ○現行基準には、災害時優先通信及び通信の疎通状況の記録・分析に関する対策はない。 　災害時においては、災害時優先通信の確保やふくそうを防ぐために通信制限が行われるが、その際の疎通状況を記録・分析することは、災害時における優先通信の確保や優先通信以外の通信への過剰な制限の回避、また、情報通信ネットワークの通信容量の見直しの際の重要な検討資料となるため、基準に改正省令内容を追加することが適当である。 《本文2.1.6参照》
	(10)ソフトウェアの信頼性向上対策	ア ソフトウェアを導入する場合は、品質の検証を行うこと。	◎	◎	◎＊	◎＊	ベストプラクティス（NTTドコモ）	新ソフトウェアの商用設備への導入前に、開発部門及び運用部門合同で品質指標に基づいたソフトウェアの導入判定が実施されていることを確認。	【検討結果】 △新ソフトウェアの商用設備導入前の関係部門合同での導入判定については、事故の未然防止に資することから、解説に追加することが適当である。
		イ ソフトウェア及びデータを変更するときは、容易に誤りが混入しないよう措置を講ずること。	◎	◎	◎＊	◎＊			
		ウ システムデータ等の重要データの復元ができること。	◎	◎	◎＊	◎＊			
		エ ソフトウェアには、異常の発生を速やかに検知、通報する機能を設けること。	○	○	○	○			
		オ ソフトウェアには、サイバー攻撃等に対する脆弱性が無いように対策を継続的に講ずること。	◎	◎	◎＊	◎＊			
		カ モバイルインターネット接続サービスにおいて、新しいシステムの導入に当たっては、実際に運用する場合と同一の条件や環境を考慮し、ハードウェアの初期故障、ソフトウェアのバグによる障害が可能な限り発生しないよう十分なシミュレーションを実施すること。	◎	◎	－ ↓ ○	－ ↓ ○			【検討結果】 ○現行基準の「モバイルインターネット接続サービスにおいて、」という文言を削除することにより、基準を一般化することが適当である。 《本文2.6参照》
		キ IP系接続サービスにおいては、現用及び予備機器の切替えを行うソフトウェアは十分な信頼性を確保すること。	◎	◎	－ ↓ ○	－ ↓ ○			【検討結果】 ○現行基準の「IP系接続サービスにおいては、」という文言を削除することにより、基準を一般化することが適当である。 《本文2.6参照》
		ク ソフトウェアの導入、更新にあたってはウイルス等の混入を防ぎ、セキュリティを確保すること。	◎	◎	◎＊	◎＊			
		ケ 定期的にソフトウェアを点検し、リスク分析を実施すること。	◎	◎	○	○			
	(11)情報セキュリティ対策	ア インターネットへ接続する場合は、ファイアウォールを設置して適切な設定を行うこと。	◎	◎	◎	◎			
		イ インターネットへ接続する場合は、非武装セグメント構成を採用すること。	◎	◎	◎	◎			
		ウ インターネットへ接続する場合は、telnetやftp等サービス提供に不用な通信の接続制限を行うこと。	◎	◎	◎	◎			
		エ インターネットへ接続する場合は、開放網と閉域網とを区別したネットワーク構成を採用すること。	◎	◎	◎	◎			
		オ インターネットへ接続する場合は、サーバー等におけるセキュリティホール対策を講ずること。	◎	◎	◎	◎			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添１

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第１　設備等基準

情報通信ネットワーク　安全・信頼性基準							根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目		対策	実施指針				資料名	内容	
			事業用	その他	自営	ユーザ			
		カ インターネットへ接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されること。	◎	◎	◎	◎			
		キ インターネットへ接続する場合は、ネットワーク上のパケット並びにサーバー及びネットワーク機器の動作に関するログの適切な記録及び保存を行うこと。	◎	◎	◎	◎			
		ク インターネットへ接続する場合は、最新の情報セキュリティ技術を採用すること。	◎	◎	◎	◎			
		ケ コンピュータウィルス及び不正プログラム混入対策を講ずること。	◎	◎	◎	◎			
		コ ネットワークの機能を管理・運営するコンピュータから重要な情報が漏えいしないように、電磁波の低減対策、又は電磁環境に配慮した上で漏えい電磁波をマスクする措置を講ずること。	◎＊	◎＊	◎＊	◎＊			
		サ 利用者の識別・確認を要する通信を取り扱う情報通信ネットワークには、正当な利用者の識別・確認を行う機能を設けること。	◎	◎	◎	◎			
		シ アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずること。	◎	◎	◎	◎			
		ス 利用者のパスワードの文字列をチェックし、一般的な単語を排除する機能を設けること。	○	○	○	○			
		セ アクセス失敗回数の基準を設定するとともに、基準値を越えたものについては、履歴を残しておく機能を設けること。	○	○	○	○			
		ソ 保護することが求められる重要な情報については、その情報に対するアクセス要求を記録し、保存する機能を設けること。	○	○	○	○			
		タ ネットワークへのアクセス履歴の表示あるいは照会が行える機能を設けること。	○	○	○	○			
		チ 一定期間以上パスワードを変更していない利用者に対して注意喚起する機能を設けること。	○	○	○	○			
		ツ 一定期間以上ネットワークを利用していない利用者がネットワークにアクセスする際に、再開の意思を確認する機能を設けること。	○	○	○	○			
		テ 機密度の高い通信には、秘話化又は暗号化の措置を講ずること。	○	○	○	○			
		ト 適切な漏話減衰量の基準を設定すること。	◎	◎	◎＊	◎＊			
		ナ ネットワークの不正使用を防止する措置を講ずること。	○	○	○	○			
	(12)通信の途絶防止対策	通信の途絶を防止する措置を講ずること。	◎＊	－	◎＊	－			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】◎:実施すべきである。　○:実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
(13)応急復旧対策	ア 重要な伝送路設備には、応急復旧用ケーブルの配備等の応急復旧対策を講ずること。	◎	－	◎＊	－			
	イ 移動用交換設備の配備等の応急復旧対策を講ずること。	○	○	○	○			【検討結果】 ○IP化の進展に伴い、本基準に記載されている対策による応急復旧が困難になることが想定されることから、本基準を削除することが適当である。 《本文2.6参照》
	ウ 災害時等において、衛星地球局等の無線設備により、臨時電話等の設置が可能であること。	○	－	○	－			【検討結果】 現状のままとする。
	エ 移動体通信基地局と交換局の間の回線に障害が発生した場合等に、無線設備により、臨時に対向の電気通信回線の設定が可能であること。	○	－	○	－			上記に同じ。
	オ 移動体通信基地局に障害が発生した場合等に、可搬型無線基地局により、臨時の電気通信回線の設定が可能であること。	○	－	○	－			上記に同じ。
	カ 他の伝送設備の障害時に、通信の疎通が著しく困難となった場合、予備の設備等により臨時の電気通信回線の設定が可能であること。	○	－	○	－			
	（追加）	○	－	－	－	大規模災害等緊急事態における通信確保の在り方について 最終取りまとめ	今回の震災を踏まえ、大ゾーン基地局の全国設置や伝送路の多ルート化など、各事業者は、ネットワークの耐災害性向上のための取組を予定又は検討しているところである。	【検討結果】 ○現行基準には、臨時に設置する電気通信回線や可搬型無線基地局により通信の途絶を防止する応急対策は存在するが、臨時の大ゾーン基地局の設置による対策はない。 大ゾーン基地局の設置は、防災上重要な通信を確保する必要がある拠点の障害時における迅速な応急対策として有効であることから、基準にその旨を追加することが適当である。 《本文2.2.1.1参照》
(14)緊急通報の確保	（追加）	◎	－	－	－	事業用電気通信設備規則	（緊急通報を扱う事業用電気通信回線設備） ＜第35条の2＞（アナログ電話用設備の例） 電気通信番号規則第十一条各号に規定する電気通信番号を用いた警察機関、海上保安機関又は消防機関（以下「警察機関等」という。）への通報（以下「緊急通報」という。）を扱う事業用電気通信回線設備については、次の各号に適合するものでなければならない。 一　緊急通報を、その発信に係る端末設備等の場所を管轄する警察機関等に接続すること。 二　緊急通報を発信した端末設備等に係る電気通信番号、その他当該発信に係る情報として総務大臣が別に告示する情報を、当該緊急通報に係る警察機関等の端末設備に送信する機能を有すること。ただし、他の方法により同等の機能を実現できる場合は、この限りでない。 三　緊急通報を受信した端末設備から終話信号が送出されない限りその通話を継続する機能又は警察機関等に送信した電気通信番号による呼び返し若しくはこれに準ずる機能を有すること。	○平成18年1月の省令改正により、緊急通報の接続等について規定化。 【検討結果】 ○平成18年1月に事業用電気通信設備規則が改正され、緊急通報を行う事業用電気通信回線設備に対して、緊急通報の接続等に関する要件が規定された。 当該省令には、緊急通報した端末の場所を管轄する警察機関等へ接続すること等が規定されており、現在の緊急通報に不可欠なものとなっていることから、基準に省令内容を追加することが適当である。 なお、重要通信である緊急通報は、電気通信事業法第8条において、電気通信事業者が優先的に取り扱わなければならない通信として規定されている。 《本文2.1.7参照》
	緊急通報手段を提供するサービスは、メンテナンス時にもできるだけ緊急通報が利用できるよう適切な措置を講ずること。なおメンテナンス時にサービス停止が必要な場合はユーザに通知する措置を講じること。	◎	◎	－	－			
(15)バックアップの分散化等	予備電源設置・冗長化などの予備機器等の配備基準の明確化を図ること。	◎	◎	○	○			【検討結果】 ○項目名と対策の内容が相違しているため、項目名を変更することが適当である。 《本文2.6参照》

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添１

【実施指針について】◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第１　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
(16)大規模災害対策（追加）		◎＊	○	○	○	事業用電気通信設備規則の改正（平成24年9月1日施行）	（大規模災害対策） ＜第１５条の３＞ 電気通信事業者は、大規模な災害により電気通信役務の提供に重大な支障が生じることを防止するため、事業用電気通信回線設備に関し、あらかじめ次の各号に掲げる措置を講じるように努めなければならない。 ＜第１５条の３第１号＞ 三以上の交換設備をループ状に接続する大規模な伝送路設備は、複数箇所の故障等により広域にわたり通信が停止しないよう、当該伝送路設備により囲まれる地域を横断する伝送路設備の追加的な設置、臨時の電気通信回線の設置に必要な機材の配備その他の必要な措置を講じること。 ＜第１５条の３第２号＞ 都道府県庁等において防災上必要な通信を確保するために使用されている移動端末設備に接続される基地局と交換設備との間を接続する伝送路設備については、第四条第二項の規定にかかわらず、予備の電気通信回線を設置すること。この場合において、その伝送路設備は、なるべく複数の経路により設置すること。 ＜第１５条の３第３号＞ 電気通信役務に係る情報の管理、電気通信役務の制御又は端末設備等の認証等を行うための電気通信設備であつて、その故障等により、広域にわたり電気通信役務の提供に重大な支障を及ぼすおそれのあるものは、複数の地域に分散して設置すること。この場合において、一の電気通信設備の故障等の発生時に、他の電気通信設備によりなるべくその機能を代替することができるようにすること。 ＜第１５条の３第４号＞ 伝送路設備を複数の経路により設置する場合には、互いになるべく離れた場所に設置すること。	○省令に大規模災害対策の努力義務が新たに規定化。 【検討結果】 ○現行基準には、火災、水害等個々の災害に関する対策は存在するが、個々の災害の複合化、広域化、長期化などを想定した大規模な災害時に関する対策はない。 大規模災害時においても、電気通信役務の提供に重大な支障が生じないよう措置を講じることは、防災上必要な通信を確保するために重要であることから、基準に改正省令内容を追加することが適当である。 《本文2.1.5参照》
2.屋外設備								
(1)風害対策	ア 強度の風圧を受けるおそれのある場所に設置する屋外設備には、強風下において故障等の発生を防止する措置を講ずること。	◎	◎	◎	◎			
	イ 風による振動に対し、故障等の発生を防止する措置を講ずること。	◎	◎	◎	◎			
(2)振動対策	地震等による振動に対し、故障等の発生を防止する措置を講ずること。	◎	◎	◎	◎			
(3)雷害対策	雷害が発生するおそれのある場所に設置する重要な屋外設備には、雷害による障害の発生を防止する措置を講ずること。	◎＊	◎＊	○	○			
(4)火災対策	火災が発生するおそれのある場所に設置する屋外設備には、不燃化又は難燃化の措置を講ずること。	○	○	○	○			
(5)耐水等の対策	ア 水中に設置する屋外設備には、耐水機能を設けること。	◎	－	◎	－			
	イ 水中に設置する屋外設備には、水圧による故障等の発生を防止する措置を講ずること。	◎	－	◎	－			
(6)水害対策	水害のおそれのある場所には、重要な屋外設備を設置しないこと。ただし、やむを得ない場合であって、防水措置等を講ずる場合は、この限りでない。	◎	◎	◎	◎			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目		対策	実施指針				資料名	内容	
			事業用	その他	自営	ユーザ			
(6)-2 津波対策（追加）			◎＊	◎＊	◎＊	◎＊	IPネットワーク設備委員会報告	非常に大規模な津波が発生したことにより、通信ビルや携帯電話基地局をはじめとする多くの電気通信設備が流失又は浸水したり、電柱が倒壊、ケーブルが切断されたりするなど、甚大な被害が発生した。	【検討結果】 ○現行基準には、水害対策はあるが、津波対策に関する対策はない。 東日本大震災時では、非常に大規模な津波が発生したことにより、通信ビルや携帯電話基地局をはじめとする多くの電気通信設備が甚大な被害が発生した。津波対策を講じることは、津波襲来時における通信の確保が期待されることから、対策にその旨を追加することが適当である。 《本文2.2.2.1参照》
(7)凍結対策		凍結のおそれのある場所に設置する屋外設備には、凍結による故障等の発生を防止する措置を講ずること。	◎	◎	◎＊	◎＊			
(8)塩害等対策		塩害、腐食性ガスによる害又は粉塵による害のおそれのある場所に設置する屋外設備には、これらによる故障等の発生を防止する措置を講ずること。	◎	◎	◎＊	◎＊			
(9)高温・低温対策	ア	高温度又は低温度の場所に設置する屋外設備は、当該条件下で安定的に動作するものであること。	◎	◎	◎	◎			
	イ	温度差の著しい場所又は温度変化の急激な環境に設置する屋外設備は、当該条件下で安定的に動作するものであること。	◎	◎	◎	◎			
(10)高湿度対策		高湿度となるおそれのある場所に設置する屋外設備には、耐湿度措置、防錆措置等を講ずること。	◎	◎	◎	◎			
(11)高信頼度		海底、宇宙空間等の特殊な場所に設置する重要な屋外設備については、高信頼度部品の使用等による高信頼度化を図ること。	◎	－	◎	－			
(12)第三者の接触防止	ア	設備に第三者が容易に触れることができないような措置を講ずること。	◎	◎	◎	◎	電波法 （昭和25年5月2日法律第131号）	（安全施設） ＜第三十条＞ 無線設備には、人体に危害を及ぼし、又は物件に損傷を与えることがないように、総務省令で定める施設をしなければならない。	【検討結果】 △電波法の電波防護に関する規定について、解説に追加することが適当である。
	イ	とう道等には、施錠等の侵入を防止する措置を講ずること。	◎	◎＊	◎＊	◎＊			
(13)故障等の検知、通報	ア	重要な屋外設備には、故障等を速やかに検知、通報する機能を設けること。	◎	◎	◎＊	◎＊			
	イ	重要な屋外設備には、故障等の箇所を識別する機能を設けること。	○	○	○	○			
(14)予備機器等の配備		重要な屋外設備には、予備機器等の適切な配備又はこれに準ずる措置を講ずること。	◎	◎	◎	－			
(15)通信ケーブルの地中化		災害時等の建物の倒壊、火災等による通信ケーブルの被災を防ぐため、通信ケーブルの地中化等を促進すること。	○	－	○	－	IPネットワーク設備委員会報告	非常に大規模な津波が発生したことにより、通信ビルや携帯電話基地局をはじめとする多くの電気通信設備が流失又は浸水したり、電柱が倒壊、ケーブルが切断されたりするなど、甚大な被害が発生した。	【検討結果】 ○東日本大震災において津波による被害も発生していることから、「～倒壊、火災等による～」を「～倒壊、火災、津波等による～」に変更することが適当である。 《本文2.6参照》
							NTT東日本報道発表（平成24年3月1日）	1－2. 流出した橋梁区間の中継伝送路の河川下越し橋梁が流された区間の本格復旧では、河川の下越しに管路を新設し、中継ケーブルを敷設することで、信頼性向上を図る。	
(16)発火・発煙防止		他事業者の屋外設備にコロケーションしているすべての電気通信設備について、設備を設置する事業者が発火・発煙防止等安全・信頼性確保のための所要の措置を講じること。	◎	◎	◎	◎			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
3.屋内設備								
(1)地震対策	ア 通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。	◎	◎	◎	◎			
	イ 通常想定される規模の地震による屋内設備の構成部品の接触不良及び脱落を防止する措置を講ずること。	◎	◎	◎	◎			
	ウ 重要な屋内設備に関する地震対策は、大規模な地震を考慮すること。	◎	◎	○	○			【検討結果】 △解説において、直下型地震又は海溝型巨大地震は発生確率は低いと記載されているため、最近の分析を踏まえて「発生確率は低いが、」という文言について修正することが適当である。また、最近における最大規模の地震として阪神・淡路大震災のみが挙げられてるが、これに「東日本大震災」を追加することが適当である。
(2)雷害対策	雷害が発生するおそれのある場所に設置する重要な屋内設備には、雷害による障害の発生を防止する措置を講ずること。	◎＊	◎＊	○	○			
(3)火災対策	重要な屋内設備には、不燃化又は難燃化の措置を講ずること。	○	○	○	○			
(4)高信頼度	ア 重要な屋内設備の機器等には、冗長構成又はこれに準ずる措置を講ずること。	◎	◎	◎	◎			【検討結果】 ○現行基準の「重要な屋内設備の機器等」の記載について、「等」が示すものが明確でないため削除することが適当である。《本文2.6参照》
	イ 重要な屋内設備の機器等は、速やかに予備機器等への切換えができるものであること。	◎	◎	◎	◎	ベストプラクティス（ソフトバンクモバイル）	他社の事故事例を参考に、加入者交換機のソフトウェア更新作業中に障害が発生した場合を想定した作業手順と復旧手順について、以下を確認。 ① 現用系のソフトウェアファイルを外部媒体に事前バックアップする手順が確立。 ② 障害発生時には、上記バックアップファイルを用いて交換機を立ち上げる手順が確立しており、30分程度で復旧可能。 ③ 交換機のプール化により、障害の発生した交換機をネットワークから切り離すことで、早期の復旧が可能。	【検討結果】 ○現行基準の「重要な屋内設備の機器等」の記載について、「等」が示すものが明確でないため削除することが適当である。《本文2.6参照》 △「交換機のプール化」の取組み事例については、予備機器等への切換え」の具体例として有用であることから、解説に追加することが適当である。
(5)故障等の検知、通報	ア 重要な屋内設備には、故障等の発生を速やかに検知、通報する機能を設けること。	◎	◎	◎	◎			
	イ 無人施設の重要な屋内設備には、遠隔通報機能を設けること。ただし、これに準ずる措置を講ずる場合は、この限りでない。	◎	◎	◎	◎			
	ウ 重要な屋内設備には、故障等の箇所を識別する機能を設けること。	○	○	○	○			
(6)試験機器の配備	試験機器の適切な配備又はこれに準ずる措置を講ずること。	◎	◎	◎	◎			
(7)予備機器等の配備	重要な屋内設備には、予備機器等の適切な配備又はこれに準ずる措置を講ずること。	◎	◎	◎	◎			
(8)コロケーション先の電気通信設備の保護	他の事業者のビルにコロケーションしているすべての電気通信設備には、安全・信頼性を確保する適切な措置を講ずること。	◎	◎	◎	◎			
4.電源設備								
(1)電力の供給条件	ア 情報通信ネットワークの所要電力を安定的に供給できること。	◎	◎	◎	◎			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添１

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第１　設備等基準

情報通信ネットワーク　安全・信頼性基準							根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目		対策	実施指針				資料名	内容	
			事業用	その他	自営	ユーザ			
		イ 電圧を許容限度内に維持するための措置を講ずること。	◎	◎	◎	◎			
		ウ 周波数を許容限度内に維持するための措置を講ずること。	◎	◎	◎	◎			
	(2)地震対策	ア 通常想定される規模の地震による転倒、移動及び故障等の発生を防止する措置を講ずること。	◎	◎	◎	◎			
		イ 重要な電源設備に関する地震対策は、大規模な地震を考慮すること。	◎	◎	○	○			【検討結果】 △解説において、直下型地震又は海溝型巨大地震は発生確率は低いと記載されているため、最近の分析を踏まえて「発生確率は低いが、」という文言について修正することが適当である。また、最近における最大規模の地震として阪神・淡路大震災のみが挙げられてるが、これに「東日本大震災」を追加することが適当である。
	(3)雷害対策	雷害が発生するおそれがある場所に設置する重要な設備に電力を供給する電源設備には、雷害による障害の発生を防止する措置を講ずること。	◎＊	◎＊	○	○			
	(4)火災対策	重要な設備に電力を供給する電源設備には、不燃化、難燃化又は保護装置の設置等の措置を講ずること。	◎＊	◎＊	○	○			
	(5)高信頼度	重要な設備に電力を供給する電源設備の機器には、冗長構成又はこれに準ずる措置を講ずること。	◎	◎	◎	◎			
	(6)故障等の検知、通報	ア 電源設備の故障等、ヒューズ断又は停電の発生を速やかに検知、通報する機能を設けること。	◎	◎	◎	◎			
		イ 重要な設備を収容する無人施設の電源設備には、遠隔通報機能を設けること。ただし、これに準ずる措置を講ずる場合は、この限りでない。	◎	◎	◎	◎			
	(7)停電対策	ア 次のいずれかの措置を講ずること。 ① 自家用発電機を設置すること。 ② 蓄電池を設置すること。 ③ 複数の系統で受電すること。 ④ 移動電源設備を配備すること。	◎	◎	◎＊	◎＊			
		イ 交換設備については、蓄電池の設置及び、自家用発電機の設置又はこれに準ずる措置を講ずること。	◎	○	○	○	事業用電気通信設備規則	（停電対策） ＜第１１条＞ 事業用電気通信回線設備は、通常受けている電力の供給が停止した場合においてその取り扱う通信が停止することのないよう自家用発電機又は蓄電池の設置その他これに準じる措置（交換設備にあつては、自家用発電機及び蓄電池の設置その他これに準じる措置）が講じられていなければならない。	【検討結果】 ○省令の規定ぶりに合わせることが適当。 《本文2.6参照》
		ウ 移動体通信基地局については、移動電源設備又は予備蓄電池を事業場等に配備すること。	◎	－	－	－	大規模災害等緊急事態における通信確保の在り方について 最終取りまとめ	電源の安定的確保を図る観点から、基地局の無停電化やバッテリーの長時間化の推進。	【検討結果】 △根拠資料に挙げられている、「基地局の無停電化」と「バッテリーの長時間化」については、電源の安定確保に資するものであることから、解説に追加することが適当である。

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添１

【実施指針について】◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第１　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
	エ 自家用発電機の設置又は移動電源設備の配備を行う場合には、その燃料について、十分な量の備蓄又はその補給手段の確保を行うこと。	○ ↓ ◎＊	○	○	○	事業用電気通信設備規則の改正（平成24年9月1日施行）	（停電対策） ＜第１１条第２項及び第４４条第２項＞ 前項の規定に基づく自家用発電機の設置又は移動式の電源設備の配備を行う場合には、それらに使用される燃料について、十分な量の備蓄又は補給手段の確保に努めなければならない。	○省令に発電機の燃料の確保に関する努力義務が規定化。 ○現行基準の停電対策と改正省令の停電対策は同一の趣旨と認められることから、基本的には本文の見直しは不要である。 【検討結果】 ○現行基準には、既に電源設備の停電対策として燃料の確保に関する対策は存在するが、同対策の現状における実施指針は「実施が望ましい」との分類であるため、実施指針を、省令改正を踏まえて現状より強化することが適当である。 　また、燃料以外の物資（例えば発電機の冷却用水）を必要とする場合も想定されることから「燃料等」とすることが適当である。 《本文2.1.2参照》
						大規模災害等緊急事態における通信確保の在り方について 最終取りまとめ	燃料の確保のため、石油会社との間の優先給油契約の締結等の連携強化を進める。	△石油会社との間の優先給油契約の締結等については、具体的な燃料確保のための取組みの一手段として、解説に追加することが適当である。
	オ 設備の重要度に応じた十分な規模の予備電源の確保を行うこと。	◎	◎	○	○			
	（追加）	◎	－	－	－	事業用電気通信設備規則の改正（平成24年9月1日施行）	（停電対策） ＜第１１条第３項＞ 防災上必要な通信を確保するため、都道府県庁、市役所又は町村役場の用に供する主たる庁舎（以下「都道府県庁等」という。）に設置されている端末設備（当該都道府県庁等において防災上必要な通信を確保するために使用される移動端末設備を含む。）と接続されている端末系伝送路設備及び当該設備と接続されている交換設備並びにこれらの附属設備に関する前二項の措置は、通常受けている電力の供給が長時間にわたり停止することを考慮したものでなければならない。ただし、通常受けている電力の供給が長時間にわたり停止した場合であつても、他の端末系伝送路設備により利用者が当該端末設備を用いて通信を行うことができるときは、この限りでない。 （※対象は電気通信事業の用に供する電気通信回線設備）	○省令に地方自治体の防災対策の拠点に対する停電対策の強化への考慮が新たに規定化 【検討結果】 ○現行基準には、停電対策に関する一般的な対策は存在するが、地方自治体の庁舎など防災対策の拠点となる特定施設の通信機器の維持、強化を図る観点からの情報通信ネットワークに対する停電対策の強化を求める対策はない。 　地方自治体に設置されている通信設備に対する停電対策の強化は、防災上必要な通信の確保に資することから、基準に改正省令内容を追加することが適当である。 《本文2.1.3参照》
							（停電対策） ＜第４４条第３項＞ 防災上必要な通信を確保するため、都道府県庁等に設置されている端末設備と接続されている端末系伝送路設備と接続されている交換設備及びその附属設備に関する前二項の措置は、通常受けている電力の供給が長時間にわたり停止することを考慮したものでなければならない。 （※対象は基礎的電気通信役務を提供する電気通信事業の用に供する電気通信回線設備）	

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添１

【実施指針について】◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第１　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
第２　環境基準								
１　センターの建築物								
(1)立地条件及び周囲環境への配慮	（追加）	◎＊	○	○	○	事業用電気通信設備規則の改正（平成24年9月1日施行）	（大規模災害対策） ＜第１５条の３第５号及び第４７条の２第２号＞ 地方公共団体が定める防災に関する計画及び地方公共団体が公表する自然災害の想定に関する情報を考慮し、電気通信設備の設置場所を決定若しくは変更し、又は適切な防災措置を講じること。	○省令に地方公共団体が定める防災に関する計画（ハザードマップ）等の情報を考慮した電気通信設備の設置場所の決定等が新たに規定化。 【検討結果】 ○現行基準には、火災、水害等個々の災害に関する対策は存在するが、個々の災害の複合化、広域化、長期化などを想定した大規模な災害時に関する対策はない。また、地方自治体が定める防災に関する計画（ハザードマップ）等の情報を考慮した電気通信設備の設置場所等の決定に関する対策も講じられていない。 　大規模災害時においても、電気通信役務の提供に重大な支障が生じないよう措置を講じることは、防災上必要な通信を確保するために重要であることから、基準に改正省令内容を追加することが適当である。 《本文2.1.5参照》
						IPネットワーク設備委員会報告	電気通信設備、設備を収容する建築物及び屋外設備等の設置やその災害対策に関しては、各自治体が作成するハザードマップ等の被害想定を考慮した対策を講じること。	
	ア 強固な地盤上の建築物を選定すること。ただし、やむを得ない場合であって、不同沈下を防止する措置を講ずる場合は、この限りでない。	◎	◎	◎＊	◎＊			
	イ 風水害等を受けにくい環境の建築物を選定すること。ただし、やむを得ない場合であって、防風、防水等の措置を講ずる場合は、この限りでない。	◎	◎	◎＊	◎＊			
	ウ 強力な電磁界による障害のおそれのない環境の建築物を選定すること。ただし、やむを得ない場合であって、通信機械室等に電磁シールド等の措置を講ずる場合は、この限りでない。	◎	◎	◎	◎			
	エ 爆発や火災のおそれのある危険物を収容する施設に隣接した建築物は回避すること。	○	○	○	○			
(2)建築物の選定	ア 耐震構造であること。	◎	◎	◎＊	◎＊			
	イ 建築基準法（昭和25年法律第201 号）第2条に規定する耐火建築物又は準耐火建築物であること。	◎	◎	◎＊	◎＊			
	ウ 床荷重に対し、所要の構造耐力を確保すること。	◎	◎	◎	◎			
(3)入出制限機能	ア 建築物の出入口には、施錠機能を設けること。	◎	◎	◎	◎			
	イ 通常利用する出入口には、設備の重要度に応じた適切な入出管理機能を設けること。ただし、これに準ずる措置を講ずる場合は、この限りでない。	◎	◎	◎	◎			
	ウ セキュリティを保つべき領域の具体的な基準を設定し、運用すること。	◎	◎	◎	◎			
(4)火災の検知、消火	ア 自動火災報知設備を適切に設置すること。	◎	◎	◎＊	◎＊			
	イ 消火設備を適切に設置すること。	◎	◎	◎	◎			
２　通信機械室等								
(1)通信機械室の位置	ア 自然災害等の外部からの影響を受けるおそれの少ない場所に設置すること。	◎	◎	◎	◎			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目		対策	実施指針				資料名	内容	
			事業用	その他	自営	ユーザ			
		イ 第三者が侵入するおそれの少ない場所に設置すること。ただし、第三者が容易に侵入できないような措置が講じられている場合は、この限りでない。	◎	◎	◎	◎			
		ウ 浸水のおそれの少ない場所に設置すること。ただし、やむを得ない場合であって、床のかさ上げ、防水壁等の措置を講ずる場合又は排水設備を設置する場合は、この限りでない。	◎	◎	◎＊	◎＊			
		エ 強力な電磁界による障害のおそれの少ない場所に設置すること。ただし、やむを得ない場合であって、電磁シールド等の措置を講ずる場合は、この限りでない。	◎	◎	◎	◎			
	⑵通信機械室内の設備等の設置	ア 保守作業が安全かつ円滑に行える空間を確保すること。	◎	◎	◎	◎			
		イ じゅう器等には、通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。	◎	◎	◎	◎			
	⑶通信機械室の条件	ア 重要な設備を収容する通信機械室は、専用に設け、十分な強度を持つ扉を設けること。	◎	◎	◎＊	◎＊			
		イ 床、内壁、天井等に使用する内装材は、通常想定される規模の地震による落下、転倒等を防止する措置を講ずること。	◎	◎＊	◎＊	◎＊			
		ウ 床、内壁、天井等に使用する内装材には、建築基準法第2条に規定する不燃材料又は建築基準法施行令（昭和25年政令第338号）第1条に規定する準不燃材料若しくは難燃材料を使用すること。	◎	◎＊	◎＊	◎＊			
		エ 静電気の発生又は帯電を防止する措置を講ずること。	◎＊	◎＊	◎＊	◎＊			
		オ 通信機械室に電源設備等を設置する場合は、必要に応じ、電磁界による障害を防止する措置を講ずること。	◎	◎	◎	◎			
		カ 通信機械室の貫通孔には、延焼を防止する措置を講ずること。	◎＊	◎＊	◎＊	◎＊			
	⑷入出制限機能	ア 出入口には、施錠機能を設けること。	◎	◎	◎	◎			
		イ 重要な設備を収容する通信機械室の出入口には、入出管理機能を設けること。また、設備の重要度に応じた適切な入出管理機能を設けること。	◎	◎	◎	◎			
		ウ セキュリティを保つべき領域の具体的な基準を設定し、運用すること。	◎	◎	◎	◎			
	⑸データ類の保管	ア システムデータ等の重要なデータは、データ保管室又は専用のデータ保管庫に収容すること。	◎	◎	◎＊	◎＊			
		イ データ保管室及びデータ保管庫には、施錠機能を設けること。	◎	◎	◎＊	◎＊			
		ウ データ保管室及びデータ保管庫には、必要に応じ、電磁界による障害を防止する措置を講ずること。	◎	◎	◎	◎			
		エ データ保管庫には、通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。	◎	◎	◎＊	◎＊			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添１

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第１　設備等基準

情報通信ネットワーク　安全・信頼性基準							根拠資料		論点（方向性）〔○･･･基準への反映 △･･･解説への反映〕
項目		対策	実施指針				資料名	内容	
			事業用	その他	自営	ユーザ			
		オ データ保管室及びデータ保管庫には、必要に応じ、耐火措置を講ずること。	◎	◎	◎＊	◎＊			
	(6)火災の検知、消火	ア 自動火災報知設備を適切に設置すること。	◎	◎	◎	◎			
		イ 消火設備を適切に設置すること。	◎	◎	◎	◎			
3.空気調和設備									
	(1)空気調和設備の設置	ア 通信機械室は、必要に応じ、空気調和を行うこと。	◎	◎	◎	◎			
		イ 荷重を十分考慮して設置すること。	◎	◎	◎	◎			
		ウ 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ずること。	◎	◎	◎	◎			
	(2)空気調和設備室への入出制限	出入口には、施錠機能を設けること。	◎＊	◎＊	◎＊	◎＊			
	(3)空気調和の条件	ア 適切な設備容量とすること。	◎	◎	◎	◎			
		イ 温湿度及び空気清浄度を適正な範囲内に維持する機能を設けること。	◎	◎	◎	◎			
		ウ 急激な温度変化が生じないよう制御する機能を設けること。	○	○	○	○			
		エ 重要な設備を収容する通信機械室の空気調和は、事務室等の空気調和と別系統とすること。ただし、通信機械室の空気調和が損なわれないような措置を講ずる場合は、この限りでない。	◎	◎	◎	◎			
		オ 重要な設備を収容する通信機械室の空気調和を行う空気調和設備は、冗長構成とすること。	◎＊	◎＊	○	○			
	(4)凍結防止	凍結のおそれのある場所に設置する空気調和設備には、凍結による故障等の発生を防止する措置を講ずること。	◎	◎	◎＊	◎＊			
	(5)漏水防止	排水口等の漏水を防止する措置を講ずること。	◎	◎	◎＊	◎＊			
	(6)有毒ガス等	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気調和設備には、触媒、フィルター等によりこれを排除する機能を設けること。	◎	◎	◎＊	◎＊			
	(7)故障等の検知、通報	重要な設備を収容する通信機械室の空気調和を行う空気調和設備には、故障等を速やかに検知、通報する機能を設けること。	◎＊	◎＊	◎＊	◎＊			
	(8)火災の検知、消火	ア 空気調和設備室には、自動火災報知設備を適切に設置すること。	◎	◎	◎	◎			
		イ 空気調和設備室には、消火設備を適切に設置すること。	◎	◎	◎	◎			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク 安全・信頼性基準						根拠資料		論点（方向性）（○…基準への反映 △…解説への反映）
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
1.ネットワーク設計管理								
(1)体制の明確化	意思決定、作業の分担、責任の範囲等の設計管理体制を明確にすること。	◎	◎	◎	◎			
	（追加）	◎	◎	◎	◎			【検討結果】 ○現行基準には、ベンダー、事業者等の関係者間の連携についての対策は存在するが、社内の関係部門間との連携についての対策はない。 社内の関係部門間の連携が図られていれば、電気通信事故の防止、利用者への被害拡大の回避が可能であった事例が散見されることから、上記現行対策の改定または追加により措置を講じることが適当である。 《本文2.3.4参照》
(2)設計指針の明確化等	ア 情報通信ネットワークの基本的機能を明確にすること。	◎	◎	◎	◎	大規模災害等緊急事態における通信確保の在り方について 最終取りまとめ	・できる限り疎通能力の向上を図る観点から、交換機等の設計容量の向上等を進める。 ・携帯メールの遅延防止を図る観点から、メールサーバ等の容量の増強等、疎通能力の向上に向けた取組を進める。 ・首都圏における大規模災害発生時にもインターネットが機能するよう、ネットワークの冗長性を確保する方策（インターネットの相互接続ポイント、データセンタの地域分散等）の検討を行う。等	【検討結果】 △情報通信ネットワークの基本的機能として、大規模災害時においてもできる限り通信の疎通能力を維持することを、解説に追加することが適当である。
	イ 将来の規模の拡大、トラヒック増加及び機能の拡充を考慮した設計とすること。	◎	◎	◎	◎	ベストプラクティス（NTTドコモ）	・高度化推進室を設置し、spモードシステムの再検証、スマートフォンが5,000万台に増加しても耐えうるシステムへの拡張に向けた検討を推進。 ・スマートフォンの制御信号を抑制するため、1回の無線接続で複数のアプリケーションが通信を行えるように無線接続手順の変更を実施予定。また、アプリを提供する企業（約700社）にモバイルネットワークに配慮したアプリ設計についての協力のお願いを実施。	【検討結果】 ○現行基準には、将来の規模の拡大、トラヒック増加及び機能の拡充を考慮した設計をするように記載されているが、「端末の挙動」に関する観点が含まれていない。 端末の挙動によって電気通信事故が生じたケースがあったことから、今後はネットワーク設計においても端末の挙動によるトラヒック増加をも十分に考慮することが必要と考えられるため、対策にその旨を追加することが適当である。 《本文2.3.1.2参照》
						事業用電気通信設備規則の改正（平成24年9月1日施行）	（災害時優先通信の優先的取扱い） ＜第35条の2の2第3項＞ 電気通信事業者は、第一項第一号の機能により他の通信の制限又は停止を行つた場合は、前項の記録を分析し、できる限り多くの通信の疎通を確保するよう通信の制限又は停止の時間、程度等の実施の方法及び事業用電気通信回線設備の通信容量について必要に応じて見直しを行うものとする。	

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク 安全・信頼性基準						根拠資料		論点（方向性）　〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
	（追加）	◎	－	－	－	ベストプラクティス（NTTドコモ）	・パケット交換機とspモードシステム間で接続ルート故障が発生した場合に、システムへの再接続信号を抑制するために、通信中利用者のみが再接続を行うように処理を変更。 ・サービス制御装置で予備機に切替が発生した場合に、spモードシステムに影響を与えないようにするために、エリア情報を更新する処理を変更。 ・故障発生時等の過負荷にも確実に対応するため、各装置の最大処理能力を超える負荷で試験を実施するとともに、商用網でのトラヒック変動に確実に対応するため、複数トラヒック条件での試験を実施。このような取組を開発プロセスに組み込み、過負荷時の安定動作に向けた負荷試験の強化を継続的に実施。 ・スマートフォンの制御信号を抑制するため、1回の無線接続で複数のアプリケーションが通信を行えるように無線接続手順の変更を実施。	【検討結果】 ○現行基準には、最近の電気通信事故の要因として挙げられているバーストトラヒック及び制御信号を抑制するための対策は存在しない。 報告書本文3.2.2及び3.2.3に示す対策を講じることによって、電気通信事故の減少が期待できることから、バーストトラヒック及び制御信号対策を講じることを対策に追加することが適当である。 《本文2.3.1.3参照》
						ベストプラクティス（KDDI）	今年度導入予定のLTEは、装置間を結合させた実環境に一層近い状態で過負荷試験を実施（H24.7実施予定）。	
						ベストプラクティス（ソフトバンクモバイル）	他社の事故で利用者認証サーバの処理能力不足が原因であったことを踏まえ、自社サーバについて一時的なトラフィックの増加にも十分対応できる処理能力であることを確認。	
						ベストプラクティス（UQコミュニケーションズ）	商用設備と同等の構成の検証環境において、利用者情報管理サーバ等に対して限界値の負荷を課した中で切替試験を実施。その際、他の設備に影響を与えないことを確認。	
						安全信頼性検討作業班資料（NTTドコモ）	ネットワーク内で通信が途切れた場合、これまでは全ての端末が再接続していたが、途切れた際に通信中の端末のみが再接続することとする。	
						安全信頼性検討作業班資料（エリクソン、日本電気、NTTドコモ、KDDI）	Network Controlled Fast DormancyやGCM等、標準化や国際動向に沿って対策として有効な手法を各事業者が積極的に取り入れ、制御信号量の低減対策を講じる。	
						安全信頼性検討作業班資料（エリクソン、日本電気、NTTドコモ、KDDI）	トラフィックが特定の設備に過度に集中しないよう、端末を柔軟に分散して収容できる設備構成とする。	
(3)設計工程の明確化等	設計工程を明確にするとともに、工程間の調整を行うこと。	◎	◎	◎＊	◎＊			
(4)相互接続への対応	ア 相互接続を考慮した設計とすること。	○	○	－	－			
	イ 相互接続を行う場合は、接続先との間で設計工程を明確にするとともに、工程間の調整を行うこと。	◎	◎	－	－			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク 安全・信頼性基準						根拠資料		論点（方向性）（○…基準への反映 △…解説への反映）
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
(5)品質・機能検査の充実化	（追加）	◎	◎	◎	◎	ベストプラクティス（KDDI）	・設備導入時のハードウェアの品質評価に関するガイドラインを制定し、社内の基準を統一。予備系装置への切替が円滑に動作しない場合の緊急手段（電源断、リセット等）に対する評価も追加。 ・スマートフォンのデータトラフィックの急増により直接的な影響を受ける24システムについて、アクセス集中時の動作仕様、考慮すべき設定情報等を抽出。4システムについては、設定情報の見直しを実施。さらに、移動系、固定系を含めた91システムに拡大して点検を行った結果、全システムについて動作仕様、設定情報に問題がないことを確認。	【検討結果】 ○現行基準には、ソフトウェアの信頼性向上についての対策は存在するが、ハードウェアの信頼性向上についての対策はない。 設備導入時の重要なハードウェアの品質評価や、当該品質評価に基づく内部の検証等は、事故の未然防止に資するものと考えられることから、基準に追加することが適当である。 《本文2.3.2参照》
	ア サーバ等機器導入前の機能確認を十分に実施すること。	◎	◎	◎	◎			
	イ 機器等の製造・販売等を行う者から提供されるシステムについての検査手法、品質評価手法を事前に確認すること。	◎	◎	◎	◎			
	ウ セキュリティ対策の手法、事前確認を十分行うこと。	◎	◎	◎	◎			
	エ ネットワークふくそうを回避するため、災害時におけるユーザの振舞いや端末の挙動がネットワークに与える影響を事前確認すること。	◎	◎	－	－			
	（追加）	◎	◎	○	○	ベストプラクティス（NTTドコモ）	新装置の導入以前（導入判定等）において、設備部門、開発部門、監視部門、技術支援部門の間でバックアップ切替動作の結果を点検するプロセスが確立していることを確認。	【検討結果】 ○現行基準には、機器等の冗長化によって信頼性を向上させる対策は存在するが、冗長化された機器の切替動作を確認する対策はない。 バックアップ切替が正常に動作するか確認することは、事故の未然防止に資するものと考えられることから、基準に追加することが適当である。 《本文2.3.3参照》
	（追加）	○	－	－	－	ベストプラクティス（NTTドコモ）	・パケット交換機とspモードシステム間で接続ルート故障が発生した場合に、システムへの再接続信号を抑制するために、通信中利用者のみが再接続を行うように処理を変更。 ・サービス制御装置で予備機に切替が発生した場合に、spモードシステムに影響を与えないようにするために、エリア情報を更新する処理を変更。 ・故障発生時等の過負荷にも確実に対応するため、各装置の最大処理能力を超える負荷で試験を実施するとともに、商用網でのトラヒック変動に確実に対応するため、複数トラヒック条件での試験を実施。このような取組を開発プロセスに組み込み、過負荷時の安定動作に向けた負荷試験の強化を継続的に実施。 ・スマートフォンの制御信号を抑制するため、1回の無線接続で複数のアプリケーションが通信を行えるように無線接続手順の変更を実施。 ・主要な59システム（2,309台）の導入時の負荷試験について、過負荷条件として商用網のトラヒックパターンを利用して、机上試験のみならず、実機試験を実施していることを確認。	【検討結果】 ○現行基準には、最大処理能力を超えた負荷をかけて通信機器等の試験を実施することについての対策はない。過負荷がかかったときの通信機器等の動作を事前に確認することは、事故の未然防止に資するものであることから、対策に追加することが適当である。 《本文2.3.1.4参照》

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク 安全・信頼性基準						根拠資料		論点（方向性）（○…基準への反映 △…解説への反映）
項目	対策	実施指針						
		事業用	その他	自営	ユーザ	資料名	内容	
						ベストプラクティス（KDDI）	・今年度導入予定のLTEは、装置間を結合させた実環境に一層近い状態で過負荷試験を実施（H24.7実施予定）。 ・スマートフォンのデータトラフィックの急増により直接的な影響を受ける24システムについて、アクセス集中時の動作仕様、考慮すべき設定情報等を抽出。4システムについては、設定情報の見直しを実施。さらに、移動系、固定系を含めた91システムに拡大して点検を行った結果、全システムについて動作仕様、設定情報に問題がないことを確認。	
						ベストプラクティス（ソフトバンクモバイル）	他社の事故で利用者認証サーバの処理能力不足が原因であったことを踏まえ、自社サーバについて一時的なトラフィックの増加にも十分対応できる処理能力であることを確認。	
						ベストプラクティス（UQコミュニケーションズ）	商用設備と同等の構成の検証環境において、利用者情報管理サーバ等に対して限界値の負荷を課した中で切替試験を実施。その際、他の設備に影響を与えないことを確認。	
2.ネットワーク施工管理								
(1)体制の明確化	作業の分担、責任の範囲等の施工管理体制を明確にすること。	◎	◎	◎	◎			
	（追加）	◎	◎	◎	◎	ベストプラクティス（KDDI）	3万以上の利用者を収容する全ての設備の作業は、サービス監視部門と作業実施部門間で常時電話会議で作業進捗を連絡する等の連携強化。	【検討結果】 ○現行基準には、ベンダー、事業者等の関係者間の連携についての対策は存在するが、社内の関係部門間との連携についての対策はない。 社内の関係部門間の連携が図られていれば、電気通信事故の防止、利用者への被害拡大の回避が可能であった事例が散見されることから、現行対策の改正または追加により措置を講じることが適当である。 《本文2.3.4参照》
						ベストプラクティス（NTTドコモ）	重大な事故が発生した場合に全社的な対応を行うため、利用者対応部門及び経営幹部へ情報を迅速に提供する体制を整備。	
(2)作業工程の明確化等	作業工程を明確にするとともに、その管理を行うこと。	◎	◎	◎	◎	ベストプラクティス（KDDI）	商用設備への新ソフトウェアの導入に関するガイドラインを制定し、利用者が少ないエリアや時間帯での先行導入、不測の事態の復旧体制や手順等について、社内ルールを統一。	【検討結果】 △新設備等導入時において利用者の少ないエリア・時間帯に先行導入することは、事故影響の縮小に資することから、解説に追加することが適当である。
						ベストプラクティス（NTTドコモ）	他社の事故事例を参考に、重要通信ビルについては、電源設備の工事作業を深夜帯に変更するよう、運用ルールの見直しを実施。	
						ベストプラクティス（ウィルコム、WCP）	工事の際の障害発生に備え、切戻の手順・所用時間の見通しが事前に共有されていることを確認。	【検討結果】 △工事の際の障害発生に備えて切戻の手順・所要時間の見通しを事前に共有することは、事故時間の縮小に資することから、解説に追加することが適当である。
						ベストプラクティス（NTTドコモ）	従来からの工事実施部門及び工事管理部門による工事手順書の個別チェックに加え、設備設計部門、設備計画部門による工事・影響エリア、切り戻し手順等の相互チェックによる手順書の充実、未経験工事についての本社の開発・技術支援部門による支援体制の強化。	
(3)相互接続への対応	相互接続を行う場合は、接続先との間で作業工程を明確にするとともに、その管理を行うこと。	◎	◎	－	－			
(4)委託工事管理	ア 工事を委託する場合は、委託契約により工事及び責任の範囲を明確にすること。	◎	◎	◎	◎			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク 安全・信頼性基準							根拠資料		論点（方向性）（○…基準への反映 △…解説への反映）
項目		対策	実施指針 事業用	その他	自営	ユーザ	資料名	内容	
	イ	工事を委託する場合は、作業手順を明確にするとともに、監督を行うこと。	◎	◎	◎	◎			
	ウ	外部委託における情報セキュリティ確保のための対策を行うこと。	◎	◎	◎	◎			
(5)検収試験管理		検収試験においては、実データを使用しないこと。ただし、やむを得ない場合であって、通信の秘密の保護及びデータの保護に十分に配慮する場合は、この限りでない。	◎	◎	◎	◎			
3.ネットワーク保全・運用管理									
(1)体制の明確化		作業の分担、連絡体系、責任の範囲等の保全・運用管理体制を明確にすること。	◎	◎	◎	◎			
		（追加）	◎	◎	◎	◎	ベストプラクティス（NTTドコモ）	重大な事故が発生した場合に全社的な対応を行うため、利用者対応部門及び経営幹部へ情報を迅速に提供する体制を整備。	【検討結果】 ○現行基準には、ベンダー、事業者等の関係者間の連携についての対策は存在するが、社内の関係部門間との連携についての対策はない。 社内の関係部門間の連携が図られていれば、電気通信事故の防止、利用者への被害拡大の回避が可能であった事例が散見されることから、現行対策の改正または追加により措置を講じることが適当である。 《本文2.3.4参照》
							ベストプラクティス（KDDI）	3万以上の利用者を収容する全ての設備の作業は、サービス監視部門と作業実施部門間で常時電話会議で作業進捗を連絡する等の連携強化。	
(2)基準の設定		保全・運用基準を設定するとともに、保全・運用に関する各種データの集計管理を行うこと。	◎	◎	◎	◎			
(3)作業の手順化		保全・運用作業の手順化を行い、保守点検の手順書の作成を行うこと。	◎	◎	◎	◎＊	ベストプラクティス（KDDI）	3万以上の利用者を収容する91システムに係る1,043のサービス復旧手順書の点検を実施し、障害発生時の影響時間の最小化を考慮したサービス復旧手順になっていること、関連する他のシステムに輻輳が連鎖することを回避するための手順があることを確認。	【検討結果】 △障害発生時の影響時間を最小化する復旧手順に関する留意点は、事故影響の縮小に資するものと考えられることから、解説にその旨を追加することが適当である。
							ベストプラクティス（ソフトバンクモバイル）	他社の事故事例を参考に、加入者交換機のソフトウェア更新作業中に障害が発生した場合を想定した作業手順と復旧手順について、以下を確認。 ① 現用系のソフトウェアファイルを外部媒体に事前バックアップする手順が確立。 ② 障害発生時には、上記バックアップファイルを用いて交換機を立ち上げる手順が確立しており、30分程度で復旧可能。 ③ 交換機のプール化により、障害の発生した交換機をネットワークから切り離すことで、早期の復旧が可能。	
							ベストプラクティス（ソフトバンクモバイル）	商用の利用者情報管理サーバ、交換機に対して毎月定期試験を実施し、予備機への切替え、本番機への切戻しの試験を実施するとともに、他の設備に対して影響を与えないことを確認。	
(4)監視、保守及び制御	ア	設備の動作状況を監視し、故障等を検知した場合は、必要に応じ、予備設備への切換え又は修理を行うこと。	◎	◎	◎	◎			
	イ	情報通信ネットワークの動作状況を監視し、必要に応じ、接続規制等の制御措置を講ずること。	◎＊	◎＊	◎＊	◎＊			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目	対策	実施指針						
		事業用	その他	自営	ユーザ	資料名	内容	
	（追加）	◎	－	－	－	事業用電気通信設備規則の改正（平成24年9月1日施行）	（災害時優先通信の優先的取扱い） ＜第３５条の２の２第２項＞ 事業用電気通信回線設備は、前項第一号の機能により他の通信の制限又は停止を行つた場合において、災害時優先通信及び他の通信の疎通の状況を記録することができるものでなければならない。 ＜第３５条の２の２第３項＞ 電気通信事業者は、第一項第一号の機能により他の通信の制限又は停止を行つた場合は、前項の記録を分析し、できる限り多くの通信の疎通を確保するよう通信の制限又は停止の時間、程度等の実施の方法及び事業用電気通信回線設備の通信容量について必要に応じて見直しを行うものとする。	【検討結果】 ○現行基準には、災害時優先通信及び通信の疎通状況の記録・分析に関する対策はない。 災害時においては、災害時優先通信の確保やふくそうを防ぐために通信制限が行われるが、その際の疎通状況を記録・分析することは、災害時における優先通信の確保や優先通信以外の通信への過剰な制限の回避、また、情報通信ネットワークの通信容量の見直しの際の重要な検討資料となるため、基準に改正省令内容を追加することが適当である。 《本文2.1.6参照》
(5)相互接続への対応	ア 相互接続を行う場合は、作業の分担、連絡体系、責任の範囲等の保全・運用体制を明確にし、非常時等の事業者間の連携・連絡体制の整備を行うこと。	◎	◎	－	－			
	イ 移動体通信において国際間のローミングサービスを行う場合は、外国の電気通信事業者との間の作業の分担、連絡体系、責任の範囲等の保全・運用体制を明確にすること。	◎	－	－	－			
	ウ モバイルインターネット接続サービスにおいて、コンテンツ等の供給を受けるために接続を行う場合は、その条件及び保全・運用体制を明確にすること。	◎	－	－	－			【検討結果】 ○現行基準の「モバイルインターネット接続サービスにおいて、」という文言を削除することにより、基準を一般化することが適当である。 《本文2.6参照》
	エ 相互接続性の試験・検証方式を明確にすること。	◎	◎	－	－			
(6)委託保守管理	ア 保守の委託を行う場合、契約書により保守作業の範囲及び責任の範囲を明確にすること。	◎	◎	◎	◎			
	イ 保守を委託する場合は、作業手順を明確にするとともに、監督を行うこと。	◎	◎	◎	◎			
	ウ 故障、障害等における迅速な原因分析のための事業者とベンダや業務委託先との連携体制を確立すること。	◎	◎	◎	◎			
	エ 業務委託先の選別の評価要件の設定を行うこと。	◎	◎	◎	◎			
(7)保守試験管理	保守試験においては、実データを使用しないこと。ただし、やむを得ない場合であって、通信の秘密の保護及びデータの保護に十分に配意する場合は、この限りでない。	◎	◎	◎	◎	ベストプラクティス（NTTドコモ）	主要な59システム（2,309台）の導入時の負荷試験について、過負荷条件として商用網のトラヒックパターンを利用して、机上試験のみならず、実機試験を実施していることを確認。	【検討結果】 △商用網のトラヒックパターンを利用した試験の取組み事例については、基準の具体例として有用であることから、解説に追加することが適当である。
(8)情報の収集	部外工事に係る情報や企画型ふくそうの原因となる情報等、情報通信ネットワークの健全な運用に必要な情報の収集のための措置を講ずること。	◎	○	○	○			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添１

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第２　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
(9)ふくそう対策	ア 情報通信ネットワークのふくそうを防止し、有効活用を図るため、必要に応じて利用者への協力依頼・周知のための措置を講ずること。	◎	◎	－	－			【検討結果】 ○本基準は利用者への周知に関する基準であるため、「１２.安全・信頼性の確保等の情報公開」に再掲させることが適当である。 ○情報通信ネットワークのふくそうを防止し、有効活用を図ることは、必要に応じたとき以外においても重要であることから、「必要に応じて」という文言は、基準から削除することが適当である。 《本文2.6参照》
	イ 災害時等において著しいふくそうが発生し、又はふくそうが発生するおそれがある場合に、情報通信ネットワークの有効活用を図るため、相互接続する事業者が協調して通信規制等の措置を講ずるとともに、ふくそうの波及防止手順の整備及び長期的視点の対策に取り組むこと。	◎	◎	－	－			
4.設備の更改・移転管理								
(1)体制の明確化	作業の分担、連絡体系、責任の範囲等の管理体制を明確にすること。	◎	◎	◎＊	◎＊			
	（追加）	◎	◎	◎	◎	ベストプラクティス（NTTドコモ）	重大な事故が発生した場合に全社的な対応を行うため、利用者対応部門及び経営幹部へ情報を迅速に提供する体制を整備。	【検討結果】 ○現行基準には、ベンダー、事業者等の関係者間の連携についての対策は存在するが、社内の関係部門間との連携についての対策はない。 　社内の関係部門間の連携が図られていれば、電気通信事故の防止、利用者への被害拡大の回避が可能であった事例が散見されることから、現行対策の改正または追加により措置を講じることが適当である。 《本文2.3.4参照》
						ベストプラクティス（KDDI）	3万以上の利用者を収容する全ての設備の作業は、サービス監視部門と作業実施部門間で常時電話会議で作業進捗を連絡する等の連携強化。	
(2)作業工程の明確化等	作業工程を明確にするとともに、その管理を行うこと。	◎	◎	◎＊	◎＊	ベストプラクティス（KDDI）	商用設備への新ソフトウェアの導入に関するガイドラインを制定し、利用者が少ないエリアや時間帯での先行導入、不測の事態の復旧体制や手順等について、社内ルールを統一。	【検討結果】 △新設備等導入時等において利用者の少ないエリア・時間帯に先行導入することは、事故影響の縮小に資することから、解説に追加することが適当である。
						ベストプラクティス（NTTドコモ）	他社の事故事例を参考に、重要通信ビルについては、電源設備の工事作業を深夜帯に変更するよう、運用ルールの見直しを実施。	
5.情報セキュリティ管理								
(1)情報セキュリティポリシーの策定	情報セキュリティポリシーを策定し、適宜見直しを行うこと。	◎	◎	◎	◎			
(2)危機管理計画の策定	不正アクセス等への対処を定めた危機管理計画を策定し、適宜見直しを行うこと。	◎	◎	◎	◎			
(3)情報セキュリティ監査の実施	監査のチェック項目の策定と定期的な内部・外部セキュリティ監査を実施し、その結果を踏まえ情報セキュリティ対策全体の見直しを行うこと。	◎	◎	○	○			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）（○…基準への反映 △…解説への反映）
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
(4)コンピュータウィルス情報緊急通報体制の整備								【検討結果】 ○以下の「イ」の変更により、コンピュータウィルス情報以外の対策も含まれることから、項目名を変更することが適当である。 《本文2.6参照》
	ア 新たなコンピュータウイルスを発見した場合等、コンピュータウイルスに関する情報を広く一般に周知する必要があるときは、電気通信業界で定めた緊急連絡先に、直ちに連絡すること。	◎	◎	－	－			
	イ コンピュータウィルスに関する情報を入手したときは、自社内に対して速やかに周知するとともに、利用者に対してウェブへの掲示、メールニュース等適切な方法により速やかに情報提供する等、被害の拡大を防止するための措置を講ずること。	◎	◎	◎	◎			【検討結果】 ○コンピュータウィルスに関する情報に加え、端末設備やソフトウェアの脆弱性についても、情報通信ネットワークに影響を与える可能性があり、周知及び被害の拡大を防止するための措置を講じる必要があることから、端末設備やソフトウェアの脆弱性が読み取れる表現に変更することが適当である。 ○また、本基準は利用者への周知に関する基準であるため、「12.安全・信頼性の確保等の情報公開」に再掲させることが適当である。 《本文2.6参照》
(5)情報セキュリティに関する情報収集	最新の情報セキュリティに関する技術情報や業界動向を入手し、それらを情報セキュリティ対策に反映させること。	◎	◎	◎	◎			
(6)知識・技能を有する者の配置	情報セキュリティに関する資格の保有者等一定以上の知識・技能を有する者を配置すること。	◎＊	◎＊	◎＊	◎＊			
(7)情報セキュリティに関する利用者への周知	情報通信ネットワークに対して利用者が与える又は情報通信ネットワークの利用者が受ける可能性のある影響とその対策について利用者に周知すること。	◎	◎	－	－			【検討結果】 ○本基準は利用者への周知に関する基準であるため、「12.安全・信頼性の確保等の情報公開」に再掲させることが適当である。 《本文2.6参照》
(8)社内の重要情報の管理	ア ネットワーク内の装置類やサービスの属性に応じた情報を分類すること。	◎	◎	◎	◎			
	イ 情報管理に関する内部統制ルールを整備すること。	◎	◎	◎	◎			
(9サイバー攻撃に備えた管理体制	サイバー攻撃発生時の迅速な情報共有方法を確立すること。	◎	◎	－	－			
6.データ管理								
(1)体制の明確化	作業の分担、連絡体系、責任の範囲等のデータ管理体制を明確にすること。	◎	◎	◎	◎			
(2)基準の設定	データ管理基準を設定すること。	◎	◎	◎	◎			
(3)作業の手順化	データ取扱作業の手順化を行うこと。	◎	◎	◎	◎			
(4)データの記録物の管理	ア 設備の仕様及び設置場所等のデータ並びに利用者に関するデータの記録物については、重要度による分類及び管理を行うこと。	◎	◎	◎	◎			
	イ 設備の仕様及び設置場所等のデータ並びに利用者に関するデータに対する従事者の守秘義務の範囲を明確にするとともに、その周知、徹底を図ること。	◎	◎	◎	◎			
	ウ 利用者の暗証番号等の秘密の保護に配慮すること。	◎	◎	◎	◎			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）　〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
	エ 記録媒体の性能向上やシステム間の接続の拡充などによるリスク・脅威の拡大に応じた適時の点検・見直しを行うこと。	◎	◎	◎	◎			
(5)ファイル等の遠隔地保管	重要なプログラム、システムデータ及び利用者に関するデータのファイル等については、前世代及び現世代のものを地域的に十分隔たった場所に別に保管すること。	○	○	○	○			
(6)重要データの漏えい防止対策	個人情報以外の重要な設備情報（特に他社のセキュリティ情報等）の漏えいを防止するための適切な措置を講ずること。	◎	◎	○	○			
7.環境管理								
(1)建築物の保全	保全点検を定期的に行うこと。	◎	◎	◎	◎			
(2)空気調和設備の保全	保全点検を定期的に行うこと。	◎	◎	◎	◎			
8.防犯管理								
(1)体制の明確化	防犯体制を明確にすること。	◎	◎	◎	◎			
(2)管理の手順化	防犯管理の手順化を行うこと。	◎	◎	◎	◎			
(3)建築物、通信機械室等の入出管理	建築物、通信機械室等の入出管理を行うこと。	◎	◎	◎	◎			
(4)かぎ、暗証番号等の管理	出入口のかぎ及び暗証番号等の適切な管理を行うこと。	◎	◎	◎	◎			
(5)防犯装置の管理	防犯装置の保全点検を定期的に行うこと。	◎	◎	◎	◎			
(6)入出管理記録の保管	入出管理記録は、一定の期間保管すること。	○	○	○	○			
9.非常事態への対応								
(1)体制の明確化	ア 連絡体系、権限の範囲等の非常事態時の体制を明確にすること。	◎	◎	◎	◎			
	イ 非常事態時における社員・職員、復旧に必要な業務依託先などへの連絡手段、社員・職員の参集手段の確保等の体制を整えること。	◎	◎	○	○	ベストプラクティス（NTTドコモ）	・迅速な故障回復を実現するため、従来から24時間監視していた監視・措置部門に加え、設備部門、技術支援部門、開発部門、ベンダの24時間即時対応体制を構築し、故障解析の迅速化、情報連絡・支援体制を確立。 ・重大な事故が発生した場合に全社的な対応を行うため、利用者対応部門及び経営幹部へ情報を迅速に提供する体制を整備。	【検討結果】 △社内の部門間の連絡体制に関する取組み事例については、基準の具体例として有用であることから、解説に追加することが適当である。
	ウ 非常事態時における広域応援体制を明確にすること。	○	○	○	○			【検討結果】 △災害の規模によって自動的に広域応援体制が発動される事例について、災害対策の迅速化に資することから、解説に一例として追加することが適当である。
	エ 相互接続を行う事業者等の間において、非常災害時の連絡体制や連絡内容を明確にすること。	◎	◎	○	○			
	オ 非常事態時における応急活動、復旧活動に際しては、国等の関係機関との連絡体制を明確にすること。	◎	◎	○	○			
	カ 非常事態時において、応急活動、復旧活動にかかわる連絡手段を確保するために必要な措置を講ずること。	◎	◎	○	○			

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク 安全・信頼性基準						根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
	（追加）	◎	○	◎	○	大規模災害等緊急事態における通信確保の在り方について 最終取りまとめ	自社の災害対応体制（事業継続計画、災害対応マニュアル等）の検証を行い、必要に応じ見直しを行う。	【検討結果】 ○現行基準には、非常事態への対応として、体制の明確化、復旧対策の手順化に関する対策は存在するが、体制の検証・見直しについては考慮されていない。 災害対応体制（事業継続計画、災害対応マニュアル等）の必要に応じた検証・見直しを行うことは、災害時における迅速・適確な対応に資することから、基準に追加することが適当である。 《本文2.2.1.2参照》
(2)復旧対策の手順化	復旧対策の手順化を行うこと。	◎	◎	◎	◎			
10.教育・訓練								
(1)体制の明確化	教育・訓練に関する計画の策定及び実施を行う体制を明確にすること。	◎	◎	◎＊	◎＊			
(2)教育・訓練の内容	ア 教育・訓練の目的を明確にするとともに、終了後の実施効果により計画の修正を行うこと。	◎	◎	◎＊	◎＊			
	イ 情報通信ネットワークの円滑な運用に必要な知識及び判断能力を養うための教育・訓練を行うこと。	◎	◎	◎	◎＊			
	ウ データ投入等における信頼性の高い作業能力を養うための教育・訓練を行うこと。	◎	◎	◎	◎			
	エ 設備の保全に関する知識を養うための教育・訓練を行うこと。	◎	◎	◎＊	◎＊			
	オ 防災に関する教育・訓練を行うこと。	◎	◎	◎	◎			
	カ 防犯に関する教育・訓練を行うこと。	◎	◎	◎	◎			
	キ 情報セキュリティに関する教育・訓練を行うこと。	◎	◎	◎	◎			
11.現状の調査・分析及び改善								
(1)体制の明確化	情報通信ネットワークの維持及び運用に関して、現状の調査・分析を行う体制を明確にすること。	◎	◎	◎	◎			
(2)基準の設定	情報通信ネットワークの維持及び運用に関して、現状の調査・分析を行う項目、評価方法等の基準を設定すること。	◎	◎	◎	◎			
(3)作業の手順化	情報通信ネットワークの維持及び運用に関して、現状の調査・分析作業の手順化を行うこと。	◎	◎＊	◎＊	◎			
(4)改善	ア 情報通信ネットワークの維持及び運用に関して、現状の調査・分析結果を、必要に応じ、情報通信ネットワークの維持及び運用体制並びに手順書に反映させること。	◎	◎	◎	◎	ベストプラクティス（NTTドコモ）	工事実施時の人為ミス等による不具合を未然に防止するため、全国で実際に行った工事に関するヒヤリ・ハット事例を収集するとともに手順書等に反映し、全社的に展開。	【検討結果】 △「ヒヤリハット事例の収集」や「PDCAサイクル」を行うことは、事故予防に資するものと考えられることから、解説に追加することが適当である。
						ベストプラクティス（NTTドコモ）	・商用システムでの不具合発生状況等が設計や試験内容に反映されており、総合的なPDCAサイクルが実行されていることを確認。 ・工事実施時の人為ミス等による不具合を未然に防止するため、全国で実際に行った工事に関するヒヤリ・ハット事例を収集するとともに手順書等に反映し、全社的に展開。	

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）　〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
	イ 情報通信ネットワークの維持及び運用に関して、現状の調査・分析結果を、必要に応じ、教育・訓練計画に反映させること。	◎	◎	◎＊	◎＊			
12.安全・信頼性の確保等の情報公開								【検討結果】 ○事業者間の情報共有に関する事項の追加等を考慮すると、現項目名「12.安全・信頼性の確保等の情報公開、電気通信事業者の取組み等」の変更が適当である。 《本文2.6参照》
(1)ネットワークの安全・信頼性の確保に係る取組状況	情報通信ネットワークの安全・信頼性の確保の取組状況を適切な方法により利用者に対して公開すること。	◎	◎	－	－			【検討結果】 ○現行基準には、既に「情報通信ネットワークの安全・信頼性の確保の取組状況を適切な方法により利用者に対して公開すること」との対策が存在しており、IPネットワーク設備委員会の提言にある「停電対策・災害対策が強化された携帯電話基地局のカバーエリア、ネットワークの設計容量に関する基本的考え方、通信規制や重要通信の優先的取扱いに係る手法等」の公表等の考え方は、現行基準の対策の内容に含まれているものと考えられる。 しかしながら、IPネットワーク設備委員会の提言に基づく情報の公表については、利用者にとって災害時においては極めて有用な情報になり得るため、情報の公表に関する電気通信事業者間の取組に差異が生じないよう、現行基準に適切な措置（現行対策の改正、新たな対策の追加、またはその他の措置）を講じることが適当である。 《本文2.2.2.4.1参照》
	（追加）	◎	－	－	－	IPネットワーク設備委員会報告	停電対策が強化された携帯電話基地局のカバーエリア等、利用者等にとって参考となる情報を適切な形で公表すること。なお、応急復旧機材については、例えば、移動電源車の台数だけではなく、その能力、電気通信設備本体の停電対策、ネットワークの規模等を総合的に勘案しなければ有効性の判断が難しいことから、情報の公表範囲等について、総務省、電気通信事業者等で検討すること。	上記に同じ。
	（追加）	◎	－	－	－	IPネットワーク設備委員会報告	災害対策が強化された大ゾーン基地局のカバーエリア等、利用者等にとって参考となる情報を適切な形で公表すること。なお、応急復旧機材については、例えば、車載基地局の台数だけではなく、その能力、電気通信設備本体のバックアップ対策、ネットワークの規模等を総合的に勘案しなければ有効性の判断が難しいことから、情報の公表範囲等について、総務省、電気通信事業者等で検討すること。	上記に同じ。
	（追加）	◎	－	－	－	IPネットワーク設備委員会報告	ネットワークの設計容量に関する基本的考え方、通信規制や重要通信の優先的取扱いに係る手法等に関する情報を公表すること。なお、これらの情報については、その評価等に専門的な知識が必要であるため、国民に分かりやすい内容となるよう、公表内容等について総務省、電気通信事業者等で検討すること。	上記に同じ。

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）　〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針						
		事業用	その他	自営	ユーザ	資料名	内容	
(2)ネットワークの事故・障害の状況	情報通信ネットワークの事故・障害の状況を適切な方法により利用者に対して公開すること。	◎	◎	－	－	ベストプラクティス（NTTドコモ）	社内緊急体制確立前に、保守・監視・措置部門から災害対策対応部門へ「緊急速報（情報周知）」を発出できるよう対応フローを整備。これにより、故障等を認知後、速やかに（30分程度）ホームページ等で情報提供するための体制を確立。また、利用者対応部門でも、「緊急速報（情報周知）」を基に利用者対応ができるよう対策を講じるとともに、ドコモショップにおいて、掲載したホームページを印刷して店頭に掲示する体制を構築。	【検討結果】 ○現行基準には、事故・障害等の状況を利用者に対して公開する旨の対策は存在するが、同対策には公開するタイミングに関する記述がない。 事故・障害等の情報は早く利用者に対して提供することが重要であり、利用者保護に資することから、「速やかに」公開するようにタイミングの概念を追加することが適当である。 《本文2.3.5参照》 △周知に関する複数の取組み事例については、基準の具体例として有用であることから、解説に追加することが適当である。
						ベストプラクティス（NTTドコモ）	利用者に影響のある工事について、事前に影響エリアの地図をホームページに掲載。	
						ベストプラクティス（KDDI）	・利用者への影響を迅速に把握する手段の一つとして、ツイッターの書き込みから情報収集する取組を導入。 ・利用者への多面的な故障情報提供を図るため、ツイッター等のソーシャルメディアを活用。	
	（追加）	◎	◎	－	－	IPネットワーク設備委員会報告	輻輳が発生した場合には、その状況及び通信規制の実施状況を速やかに公表すること。	【検討結果】 ○現行基準には、ふくそう発生時の通信規制の実施状況等の公表に関する対策はない。 当該情報が公表されることによって、ふくそう発生時における他の通信手段を選択する利用者の増加、繰り返しダイヤルの減少が期待できるため、ネットワークの負荷軽減に有効と考えられることから、対策にその旨を追加することが適当である。 《本文2.2.2.4.2参照》
(3)サービスの特質等の周知	情報通信ネットワークにおいて、サービスを提供できなくなる場合などについて利用者に周知すること。	◎	◎	－	－			
	（再掲） 情報通信ネットワークのふくそうを防止し、有効活用を図るため、必要に応じて利用者への協力依頼・周知のための措置を講ずること。	◎	◎	－	－			【検討結果】 ○「3.ネットワーク保全・運用管理(9)ふくそう対策」に挙げられている「情報通信ネットワークのふくそうを防止・有効活用のための協力依頼・周知」の主旨に関しては、公表、周知に該当する事項であるため、「12.安全・信頼性の確保等の情報公開」(3)に再掲することが適当である。 ○情報通信ネットワークのふくそうを防止し、有効活用を図ることは、必要に応じたとき以外においても重要であることから、「必要に応じて」という文言は、基準から削除することが適当である。 《本文2.6参照》
	（追加）	◎	－	－	－	IPネットワーク設備委員会報告	不要不急の電話を控えること及び通話時間をできるだけ短くすることについて周知・要請し、災害用伝言サービスを含めた音声通話以外の通信手段の利用等を呼びかけること。	【検討結果】 ○現行基準には、災害時における音声通話以外の通信手段の利用等の呼びかけに関する対策はない。 手短な通信、音声お届けサービスや災害伝言用サービスの活用に関する周知・要請を行うことにより、災害時における通話の疎通の改善が期待されることから、対策にその旨を追加することが適当である。 《本文2.2.2.4.3参照》 △災害用伝言サービスの利用において、通信事業者が異なるものであっても操作は同じであることが望ましいことから、通信事業者は、利用方法及び利用までの経路（導線）を統一するよう努めることが適当である。

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）　〔○･･･基準への反映 △･･･解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
	（再掲） 緊急通報手段を提供するサービスは、メンテナンス時にもできるだけ緊急通報が利用できるよう適切な措置を講ずること。なおメンテナンス時にサービス停止が必要な場合はユーザに通知する措置を講じること。	◎	◎	－	－			【検討結果】 「第1　設備基準　1ー般基準　(14)緊急通報の確保」において、緊急通報のメンテナンス時にサービスが停止される場合のユーザへの周知に関する基準は、情報公開に関する本項目にも再掲することが適当である。 《本文2.6参照》
(4)情報セキュリティに関する取組（追加・再掲）	（追加）	◎	◎	－	－			【検討結果】 ○現行基準の「12.安全・信頼性の確保等の情報公開(1)ネットワークの安全・信頼性の確保に係る取組状況」の解説において、「各事業者の情報セキュリティ確保に関する基本方針」を利用者が容易に知りえる方法によって、公表するよう、努める旨が記載されている。 ○情報セキュリティの基本方針は、利用者が情報通信ネットワークを利用する上で重要な情報であることから、基準に追加することが適当である。 《本文2.6参照》
	（再掲） コンピュータウィルスに関する情報を入手したときは、自社内に対して速やかに周知するとともに、利用者に対してウェブへの掲示、メールニュース等適切な方法により速やかに情報提供する等、被害の拡大を防止するための措置を講ずること。	◎	◎	◎	◎			【検討結果】 ○「5.情報セキュリティ管理(4)コンピュータウィルス情報緊急通報体制の整備」のイについて、利用者への周知に関する内容であることから、「12.安全・信頼性の確保等の情報公開」(4)に再掲することが適当である。 《本文2.6参照》
	（再掲） 情報通信ネットワークに対して利用者が与える又は情報通信ネットワークの利用者が受ける可能性のある影響とその対策について利用者に周知すること。	◎	◎	－	－			【検討結果】 ○「5.情報セキュリティ管理(7)情報セキュリティに関する利用者への周知」について、利用者への周知に関する内容であることから、「12.安全・信頼性の確保等の情報公開」(4)に再掲することが適当である。 《本文2.6参照》

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）

別添1

【実施指針について】◎:実施すべきである。　○:実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）　（○･･･基準への反映　△･･･解説への反映）
項目	対策	実施指針				資料名	内容	
		事業用	その他	自営	ユーザ			
(5)電気通信サービスの不適正利用の防止に関する周知・取組み（追加）	（移行） モバイルインターネット接続サービスにおいては、利用者が指定した特定の条件に該当する電子メールの受信を拒否する等の機能を設けること。	○	－ ↓ ○	－	－			【検討結果】 ○現行基準には、本項で参照している法令等と同様な利用者保護、電気通信サービスの不適正利用対策の観点から、電子メール対策（別表第1　設備等基準　第1　設備基準　1．一般基準(7)電子メールによる一方的な広告・宣伝等への対策）が存在する。 当該基準は、電子メールの受信拒否機能が事業者のネットワークでしか対応できなかったときに策定されたものであり、現在においては利用者での端末においても迷惑メール対策が可能となっている。 また、インターネット上での利用者保護、不適正利用対策の対象としては、迷惑メールだけでなく、有害情報からの青少年保護を目的とした「青少年有害情報フィルタリング」、児童の権利を著しく侵害する画像の閲覧防止を目的とした「児童ポルノブロッキング対策」等が電気通信事業者に要請されている。 こうした状況を踏まえ、現状基準に、迷惑メールの取組に加え、「青少年有害情報フィルタリング」、「児童ポルノブロッキング対策」を新たな対策として規定することは、利用者保護の観点から、適当である。 なお、迷惑メールの対策は、モバイルインターネット接続サービスに限定した記述であったが、当該対策にモバイルインターネット接続サービスに限定する理由がないことから、「モバイルインターネット接続サービス」の表現を削除することが適当である。 更に、これらの不適正利用に係る分類は、「12．安全・信頼性の確保等の情報公開、電気通信事業者の取組み等」の「電気通信サービスの不適正利用の防止に関する周知・取組み」として、新たに管理基準に位置づけることが適当である。 《本文2.4参照》
	（追加）	◎	◎	－	－	青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律（平成二十年六月十八日法律第七十九号）	＜第17条第1項＞ 携帯電話インターネット接続役務提供事業者は、携帯電話インターネット接続役務を提供する契約の相手方又は携帯電話端末若しくはPHS端末の使用者が青少年である場合には、青少年有害情報フィルタリングサービスの利用を条件として、携帯電話インターネット接続役務を提供しなければならない。ただし、その青少年の保護者が、青少年有害情報フィルタリングサービスを利用しない旨の申出をした場合は、この限りでない。	
	（追加）	◎＊	◎＊	－	－	児童ポルノブロッキングの実施について（各通信事業者の報道資料より抜粋）	児童ポルノのアドレスリストに掲載されているサイトの閲覧を制限するブロッキングを実施。	
						児童ポルノ排除総合対策（平成22年7月27日犯罪対策閣僚会議決定）	3 インターネット上の児童ポルノ画像等の流通・閲覧防止対策の推進 ⑤ ブロッキングの導入に向けた諸対策の推進 インターネット上の児童ポルノについては、児童の権利を著しく侵害するものであり、インターネット・ホットラインセンターが把握した画像について、サイト管理者等への削除要請や警察の捜査・被疑者検挙が行われた場合等でも、実際に画像が削除されるまでの間は画像が放置されるところであり、児童の権利を保護するためには、サーバーの国内外を問わず、画像発見後、速やかに児童ポルノ掲載アドレスリストを作成し、ISPによる閲覧防止措置（ブロッキング）を講ずる必要がある。	
(6)電気通信事業者間等の情報共有（追加）	（追加）	◎＊	－	－	－	携帯電話通信障害対策連絡会	携帯電話事業者全社及び電気通信事業者協会において、電気通信事故の再発防止策のうち他事業者の今後の取組強化に参考となるもの（いわゆるベストプラクティス）について業界で情報共有し、事故防止に向けての取組を確認	【検討結果】 ○現行基準には、電気通信事業者間や電気通信事業者とアプリケーション開発事業者の間の情報共有についての対策はない。 電気通信事故の状況、再発防止策や災害時における有効な応急対策など事業者共通の問題となりえる事例を情報共有することは、業界全体の事故、災害対策にも有効であること、また、電気通信事業者とアプリケーション開発事業者の間で、ネットワークの負荷を考慮したアプリケーションの開発手法等について情報共有することは、3.2.3に後述する制御信号等対策にも有効であることから、対策に追加することが適当である。 《本文2.3.6参照》
						大規模災害等緊急事態における通信確保の在り方について最終取りまとめ	被災した通信設備の復旧について、今回の取組のうち、有効な取組をベストプラクティスとして共有しつつ、移動基地局の更なる配備や衛星回線の活用など、今回の対応を踏まえた応急復旧対応に関する取組を進める。	
						ベストプラクティス（ソフトバンクモバイル）	他社の事故で利用者認証サーバの処理能力不足が原因であったことを踏まえ、自社サーバについて一時的なトラフィックの増加にも十分対応できる処理能力であることを確認。	
	（追加）	○	－	－	－	ベストプラクティス（NTTドコモ）	アプリを提供する企業（約700社）にモバイルネットワークに配慮したアプリ設計についての協力のお願いを実施。	

情報通信ネットワーク　安全・信頼性基準の見直しに関する論点（方向性）　別添1

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第3　情報セキュリティポリシー策定のための指針

情報通信ネットワーク 安全・信頼性基準		根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目	内容	資料名	内容	
1～4 （略）				
5　情報セキュリティポリシーの構成例	情報セキュリティポリシーの構成例と各項目における記述内容を以下に示す。ここでは、方針を「情報セキュリティ運営に関する方針」と「情報資産に関する方針」に大きく分け、前者では管理の各段階に応じた項目、後者では情報資産の大きな区分である「情報」、「情報システム」、そして、情報資産を保護するための「アクセス制御」という項目立てとしている。			
1　総則 （略）				
2　方針				
(1) セキュリティ運営に関する方針 （略）				
(2) 情報資産に関する方針				
ア 情報	適用範囲内の情報についての管理方法を明確化することで、情報の漏えい、破壊、改ざん等を防止する。また、プライバシーにかかわる情報を取り扱う際に遵守すべき事項を明確化する。			【検討結果】 「プライバシーにかかわる情報」「プライバシー情報」の「プライバシー」に関する用語の定義が明確でないこと、また、事業者等に対して、明確でない事項の遵守を求めることは不適当であることから、個人情報保護法（平成15年5月30日法律第57号）、「電気通信事業における個人情報保護に関するガイドライン」（平成16年総務省告示第695号）に定義されている「個人情報」の表現に統一することが適当である。 《本文2.6参照》
（ア）情報管理	情報の漏えい、破壊、改ざん等による被害等に応じて、情報を区分する。情報の区分と情報の取得・生成、保管、流通、利用及び廃棄という各段階における情報の取扱方法を明確にし、組織員による情報の取扱方法を統一化する。			
（イ）プライバシー情報	通信の秘密を含むプライバシー情報の漏えいは深刻な権利利益侵害につながるおそれが高いため、電気通信事業者に対しては、「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」（平成16年総務省告示第695号）が制定されている。 プライバシー情報の適切な利用と保護が極めて重要であるとの認識により、プライバシー情報の取扱いについては、個別の項目を設け、個人情報の収集、利用・提供、適正管理、責任の明確化等について、遵守すべき方針を明確に記述する。			【検討結果】 「プライバシーにかかわる情報」「プライバシー情報」の「プライバシー」に関する用語の定義が明確でないこと、また、事業者等に対して、明確でない事項の遵守を求めることは不適当であることから、個人情報保護法（平成15年5月30日法律第57号）、「電気通信事業における個人情報保護に関するガイドライン」（平成16年総務省告示第695号）に定義されている「個人情報」の表現に統一することが適当である。 《本文2.6参照》
イ、ウ （略）				

別表第4　危機管理計画策定のための指針 （略）

「情報通信ネットワーク　安全・信頼性基準」と関係ガイドラインとの比較　　別添2

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						参考資料	
項目		対策	実施指針			資料名	内容
			事業用	その他	自営	ユーザ	
第1　設備基準							
	(10)ソフトウェアの信頼性向上対策	ア ソフトウェアを導入する場合は、品質の検証を行うこと。	◎	◎	◎＊	◎＊	
		イ ソフトウェア及びデータを変更するときは、容易に誤りが混入しないよう措置を講ずること。	◎	◎	◎＊	◎＊	
		ウ システムデータ等の重要データの復元ができること。	◎	◎	◎＊	◎＊	
		エ ソフトウェアには、異常の発生を速やかに検知、通報する機能を設けること。	○	○	○	○	
		オ ソフトウェアには、サイバー攻撃等に対する脆弱性が無いように対策を継続的に講ずること。	◎	◎	◎＊	◎＊	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（イ）情報セキュリティに付いての脅威【要検討事項】 セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。 ○サービス不能攻撃 ・通信フィルタリング ・通信回線の冗長化 ・通信事業者との連携 ・電子計算機、通信回線装置及び通信回線の監視と記録
							電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	3.（1）共通 ネットワークを脅威から保護するために、また、ネットワークを用いた業務用システム及び業務用ソフトウェア（処理中の情報を含む。）のセキュリティを維持するために、ネットワークを適切に管理し、制御しているか
		カ モバイルインターネット接続サービスにおいて、新しいシステムの導入に当たっては、実際に運用する場合と同一の条件や環境を考慮し、ハードウェアの初期故障、ソフトウェアのバグによる障害が可能な限り発生しないよう十分なシミュレーションを実施すること。	◎	◎	ニ	ニ		

【実施指針について】 ◎:実施すべきである。　○:実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目			対策	実施指針			資料名	内容
				事業用	その他	自営	ユーザ	
			キ IP系接続サービスにおいては、現用及び予備機器の切替えを行うソフトウェアは十分な信頼性を確保すること。	◎	◎	―	―	
			ク ソフトウェアの導入、更新にあたってはウイルス等の混入を防ぎ、セキュリティを確保すること。	◎	◎	◎＊	◎＊	
			ケ 定期的にソフトウェアを点検し、リスク分析を実施すること。	◎	◎	○	○	
		(11)情報セキュリティ対策	ア インターネットへ接続する場合は、ファイアウォールを設置して適切な設定を行うこと。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	3.（2）サイバー攻撃対策 サイバー攻撃（DDoS攻撃等）から、サーバ、ルータ、その他のIPネットワーク設備を保護するため、特定の通信が攻撃に使用される場合を想定し、物理又は論理ポートや、IPアドレス、プロトコル毎に、IT障害を防止するために必要最小限の範囲で通信フィルタリング又は帯域制御を行なうことを可能としているか サービスによっては、信号処理レベルでの通信制御や、利用者認証、アクセス権限管理等と連動した通信フィルタリング等を行なうことを可能としているか
			イ インターネットへ接続する場合は、非武装セグメント構成を採用すること。	◎	◎	◎	◎		
			ウ インターネットへ接続する場合は、telnetやftp等サービス提供に不用な通信の接続制限を行うこと。	◎	◎	◎	◎		
			エ インターネットへ接続する場合は、開放網と閉域網とを区別したネットワーク構成を採用すること。	◎	◎	◎	◎		

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目			対策	実施指針			資料名	内容
				事業用	その他	自営	ユーザ	
			オ インターネットへ接続する場合は、サーバー等におけるセキュリティホール対策を講ずること。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ウ(イ)情報セキュリティに付いての脅威【要検討事項】 セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。 ○セキュリティホール ・情報収集 ・対応計画の策定 ・対応内容の記録 ・定期チェック ・不正アクセスの監視・検出(IDSの使用) ・通信フィルタリング(ファイアウォール) ・外部ネットワークからの遮断等 ・アンチウイルスソフトウェアの使用(端末、ゲートウェイ)、メンテナンス、定期検査、セキュリティパッチ適用 ・利用していない通信ポート等の非活性化、マクロ実行の抑制 ・早期発見・早期回復対策(監視、障害の検出、障害箇所の切り分け、障害時の縮退・再構成、取引制限、リカバリ機能)
			カ インターネットへ接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されること。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ウ(ア)情報セキュリティ確保のために求められる機能【要検討事項】 主体認証(利用者及び機器等の認証)、アクセス制御、権限管理、証跡管理、負荷分散、冗長化など基本的な情報セキュリティ機能の観点から、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。
								電気通信分野における情報セキュリティ確保に係る安全基準(第2版)	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

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目			対策	実施指針			資料名	内容
				事業用	その他	自営	ユーザ	
			キ インターネットへ接続する場合は、ネットワーク上のパケット並びにサーバー及びネットワーク機器の動作に関するログの適切な記録及び保存を行うこと。	◎	◎	◎	◎	
			ク インターネットへ接続する場合は、最新の情報セキュリティ技術を採用すること。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	3.（2）サイバー攻撃対策 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
			ケ コンピュータウィルス及び不正プログラム混入対策を講ずること。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（イ）情報セキュリティに付いての脅威【要検討事項】 セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。 ○不正プログラム ・情報収集 ・OS／アプリケーションのセキュリティ設定 ・アンチウイルスソフトウェアの導入 ・パターンファイルの更新 ・パッチ適用 ・定期的なウイルス検査
								電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	3.（2）サイバー攻撃対策 電気通信サービス利用者又は他の事業者の電気通信設備から受信したプログラム等により、事業者の意図に反する動作を行なうこと等により電気通信サービスの提供に重大な支障を及ぼすことがないよう、電気通信設備は必要な防護措置を講じているか
			コ ネットワークの機能を管理・運営するコンピュータから重要な情報が漏えいしないように、電磁波の低減対策、又は電磁環境に配慮した上で漏えい電磁波をマスクする措置を講ずること。	◎＊	◎＊	◎＊	◎＊		

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目			対策	実施指針			資料名	内容
				事業用	その他	自営	ユーザ	
			サ 利用者の識別・確認を要する通信を取り扱う情報通信ネットワークには、正当な利用者の識別・確認を行う機能を設けること。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ウ(ア)情報セキュリティ確保のために求められる機能【要検討事項】 ○主体認証 ・主体認証機能の導入 ・主体認証技術の選択(知識、所有、生体認証、及び多要素認証等) ・利用者IDの管理 ・主体認証情報の管理(暗号化、パスワードの定期変更・最低文字数の制限等) ・利用者の責任(パスワードの利用、端末管理、クリアデスク・クリアスクリーン方針) ・不正使用検知時における主体認証の利用停止措置
								電気通信分野における情報セキュリティ確保に係る安全基準(第2版)	3.(1)共通 すべての情報システム及びサービスへのアクセスを許可及び無効とするために、利用者の登録・登録削除についての正式な手順を備えているか 特権の割当て及び利用は、制限し、管理しているか 利用することを特別に認可したサービスへのアクセスだけを、利用者に提供しているか 遠隔利用者のアクセスを管理するために、適切な認証方法を利用しているか 3.(2)サイバー攻撃対策 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 3.(3)重要情報漏えい対策 システム利用にあたりアクセス管理を行うために、利用者の識別・認証等のシステムを導入し、アクセス制限等を実施しているか

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目			対策	実施指針			資料名	内容
				事業用	その他	自営	ユーザ	
			シ アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずること。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ウ(ア)情報セキュリティ確保のために求められる機能【要検討事項】 〇アクセス制御 ・アクセス制御機能の導入 ・利用者アクセスの管理(利用者登録、特権管理、利用者パスワードの管理、利用者アクセス権のレビュー等) ・ネットワークのアクセス制御方針の策定
								電気通信分野における情報セキュリティ確保に係る安全基準(第2版)	1.(1)共通 情報システムを監査するツールの誤用又は悪用を防止するために、それらのツールへのアクセスが抑制されているか 2.(1)共通 あらゆる形式の通信設備を利用した情報交換を保護するために、正式な交換方針、手順及び管理策を備えているか 2.(2)サイバー攻撃 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
			ス 利用者のパスワードの文字列をチェックし、一般的な単語を排除する機能を設けること。	○	○	○	○		
			セ アクセス失敗回数の基準を設定するとともに、基準値を越えたものについては、履歴を残しておく機能を設けること。	○	○	○	○		
			ソ 保護することが求められる重要な情報については、その情報に対するアクセス要求を記録し、保存する機能を設けること。	○	○	○	○	電気通信分野における情報セキュリティ確保に係る安全基準(第2版)	3.(3)重要情報漏えい対策 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
			タ ネットワークへのアクセス履歴の表示あるいは照会が行える機能を設けること。	○	○	○	○		

【実施指針について】 ◎:実施すべきである。　○:実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目			対策	実施指針 事業用	その他	自営	ユーザ	資料名	内容
			チ 一定期間以上パスワードを変更していない利用者に対して注意喚起する機能を設けること。	○	○	○	○		
			ツ 一定期間以上ネットワークを利用していない利用者がネットワークにアクセスする際に、再開の意思を確認する機能を設けること。	○	○	○	○		
			テ 機密度の高い通信には、秘話化又は暗号化の措置を講ずること。	○	○	○	○		
			ト 適切な漏話減衰量の基準を設定すること。	◎	◎	◎＊	◎＊		
			ナ ネットワークの不正使用を防止する措置を講ずること。	○	○	○	○		
第2　環境基準									
	1　センターの建築物								
		(1)立地条件及び周囲環境への配慮	ア 強固な地盤上の建築物を選定すること。ただし、やむを得ない場合であって、不同沈下を防止する措置を講ずる場合は、この限りでない。	◎	◎	◎＊	◎＊	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	4.（1）共通 装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置又は保護されているか
			イ 風水害等を受けにくい環境の建築物を選定すること。ただし、やむを得ない場合であって、防風、防水等の措置を講ずる場合は、この限りでない。	◎	◎	◎＊	◎＊		
			ウ 強力な電磁界による障害のおそれのない環境の建築物を選定すること。ただし、やむを得ない場合であって、通信機械室等に電磁シールド等の措置を講ずる場合は、この限りでない。	◎	◎	◎	◎		
			エ 爆発や火災のおそれのある危険物を収容する施設に隣接した建築物は回避すること。	○	○	○	○		
		(2)建築物の選定	ア 耐震構造であること。	◎	◎	◎＊	◎＊		
			イ 建築基準法（昭和25年法律第201 号）第2条に規定する耐火建築物又は準耐火建築物であること。	◎	◎	◎＊	◎＊		

【実施指針について】 ◎:実施すべきである。　○:実施が望ましい。　ー:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準								参考資料	
項目			対策	実施指針				資料名	内容
				事業用	その他	自営	ユーザ		
			ウ 床荷重に対し、所要の構造耐力を確保すること。	◎	◎	◎	◎		
		(3)入出制限機能	ア 建築物の出入口には、施錠機能を設けること。	◎	◎	◎	◎		
			イ 通常利用する出入口には、設備の重要度に応じた適切な入出管理機能を設けること。ただし、これに準ずる措置を講ずる場合は、この限りでない。	◎	◎	◎	◎		
			ウ セキュリティを保つべき領域の具体的な基準を設定し、運用すること。	◎	◎	◎	◎		
		(4)火災の検知、消火	ア 自動火災報知設備を適切に設置すること。	◎	◎	◎＊	◎＊		
			イ 消火設備を適切に設置すること。	◎	◎	◎	◎		
	2	通信機械室等							
		(1)通信機械室の位置	ア 自然災害等の外部からの影響を受けるおそれの少ない場所に設置すること。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	4.（1）共通 電気通信事業を提供するための交換設備等の電気通信設備を収容する施設の物理的なセキュリティを設計し、適用しているか 電気通信事業を提供するために電気通信設備が設置された部屋の物理的なセキュリティを設計し、適用しているか 電気通信事業を提供するために電気通信設備を設置している物理的に隔離された運用区画の物理的なセキュリティを設計し、適用しているか
			イ 第三者が侵入するおそれの少ない場所に設置すること。ただし、第三者が容易に侵入できないような措置が講じられている場合は、この限りでない。	◎	◎	◎	◎		
			ウ 浸水のおそれの少ない場所に設置すること。ただし、やむを得ない場合であって、床のかさ上げ、防水壁等の措置を講ずる場合又は排水設備を設置する場合は、この限りでない。	◎	◎	◎＊	◎＊		

【実施指針について】 ◎:実施すべきである。　○:実施が望ましい。　ー:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目	対策	実施指針					資料名	内容
		事業用	その他	自営	ユーザ			
	エ 強力な電磁界による障害のおそれの少ない場所に設置すること。ただし、やむを得ない場合であって、電磁シールド等の措置を講ずる場合は、この限りでない。	◎	◎	◎	◎			
(2)通信機械室内の設備等の設置	ア 保守作業が安全かつ円滑に行える空間を確保すること。	◎	◎	◎	◎			
	イ じゅう器等には、通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。	◎	◎	◎	◎			
(3)通信機械室の条件	ア 重要な設備を収容する通信機械室は、専用に設け、十分な強度を持つ扉を設けること。	◎	◎	◎＊	◎＊			
	イ 床、内壁、天井等に使用する内装材は、通常想定される規模の地震による落下、転倒等を防止する措置を講ずること。	◎	◎＊	◎＊	◎＊			
	ウ 床、内壁、天井等に使用する内装材には、建築基準法第2条に規定する不燃材料又は建築基準法施行令（昭和25年政令第338号）第1条に規定する準不燃材料若しくは難燃材料を使用すること。	◎	◎＊	◎＊	◎＊			
	エ 静電気の発生又は帯電を防止する措置を講ずること。	◎＊	◎＊	◎＊	◎＊			
	オ 通信機械室に電源設備等を設置する場合は、必要に応じ、電磁界による障害を防止する措置を講ずること。	◎	◎	◎	◎			
	カ 通信機械室の貫通孔には、延焼を防止する措置を講ずること。	◎＊	◎＊	◎＊	◎＊			
(4)入出制限機能	ア 出入口には、施錠機能を設けること。	◎	◎	◎	◎			

【実施指針について】 ◎:実施すべきである。　○:実施が望ましい。　ー:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準								参考資料	
項目			対策	実施指針				資料名	内容
				事業用	その他	自営	ユーザ		
			イ 重要な設備を収容する通信機械室の出入口には、入出管理機能を設けること。また、設備の重要度に応じた適切な入出管理機能を設けること。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	4.（1）共通 情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いているか セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護されているか
			ウ セキュリティを保つべき領域の具体的な基準を設定し、運用すること。	◎	◎	◎	◎		
		⑸データ類の保管	ア システムデータ等の重要なデータは、データ保管室又は専用のデータ保管庫に収容すること。	◎	◎	◎＊	◎＊		
			イ データ保管室及びデータ保管庫には、施錠機能を設けること。	◎	◎	◎＊	◎＊		
			ウ データ保管室及びデータ保管庫には、必要に応じ、電磁界による障害を防止する措置を講ずること。	◎	◎	◎	◎		
			エ データ保管庫には、通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。	◎	◎	◎＊	◎＊		
			オ データ保管室及びデータ保管庫には、必要に応じ、耐火措置を講ずること。	◎	◎	◎＊	◎＊		
		⑹火災の検知、消火	ア 自動火災報知設備を適切に設置すること。	◎	◎	◎	◎		
			イ 消火設備を適切に設置すること。	◎	◎	◎	◎		

「情報通信ネットワーク　安全・信頼性基準」と関係ガイドラインとの比較　　別添2

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　ー:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						参考資料	
項目	対策	実施指針				資料名	内容
		事業用	その他	自営	ユーザ		
1.ネットワーク設計管理							
(5)品質・機能検査の充実化	ウ セキュリティ対策の手法、事前確認を十分行うこと。	◎	◎	◎	◎		
2.ネットワーク施工管理							
(4)委託工事管理	ウ 外部委託における情報セキュリティ確保のための対策を行うこと。	◎	◎	◎	◎		
3.ネットワーク保全・運用管理							
(6)委託保守管理	ア 保守の委託を行う場合、契約書により保守作業の範囲及び責任の範囲を明確にすること。	◎	◎	◎	◎		
5.情報セキュリティ管理							
(1)情報セキュリティポリシーの策定	情報セキュリティポリシーを策定し、適宜見直しを行うこと。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティの基本方針の策定 ○自己点検・内部監査の実施 ・情報セキュリティ対策の見直し
						電気通信分野における情報セキュリティ確保に係る安全基準(第2版)	1. 組織・体制及び資源の対策 (1)共通 情報セキュリティ基本方針は、あらかじめ定められた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当及び有効であることを確実にするためにレビューされているか
(2)危機管理計画の策定	不正アクセス等への対処を定めた危機管理計画を策定し、適宜見直しを行うこと。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(2)イ(ウ)不正アクセスによる脅威への対策【要検討事項】 保護すべき情報が保存されたPCや外部記録媒体の盗難、紛失及び当該PCや外部記録媒体からの情報漏えいを防止するための措置や、保護すべき情報を処理するウェブやメール等のアプリケーションからの情報の漏えいを防止するための措置が明示されるべきである。

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						参考資料	
項目		対策	実施指針			資料名	内容
			事業用	その他	自営	ユーザ	
	(3)情報セキュリティ監査の実施	監査のチェック項目の策定と定期的な内部･外部セキュリティ監査を実施し、その結果を踏まえ情報セキュリティ対策全体の見直しを行うこと。	◎	◎	○	○	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア　組織・体制及び資源の対策 (ア)組織・体制及び人的資源の確保【要検討事項】 ○自己点検・内部監査の実施 ・自己点検の実施 ・内部監査の実施 ・情報セキュリティ対策の見直し (ウ)外部監査等による情報セキュリティ対策の評価【参考事項】 技術的な対策は多くの事業者で行われているが、今後は外部監査等による情報セキュリティ対策の評価を行うことが望ましい。 ・情報セキュリティ監査等の実施 ・情報セキュリティ対策の見直し
	(4)コンピュータウィルス情報緊急通報体制の整備	ア 新たなコンピュータウイルスを発見した場合等、コンピュータウイルスに関する情報を広く一般に周知する必要があるときは、電気通信業界で定めた緊急連絡先に、直ちに連絡すること。	◎	◎	－	－		
		イ コンピュータウィルスに関する情報を入手したときは、自社内に対して速やかに周知するとともに、利用者に対してウェブへの掲示、メールニュース等適切な方法により速やかに情報提供する等、被害の拡大を防止するための措置を講ずること。	◎	◎	◎	◎		
	(5)情報セキュリティに関する情報収集	最新の情報セキュリティに関する技術情報や業界動向を入手し、それらを情報セキュリティ対策に反映させること。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1.（1）共通 社会環境や技術環境等の変化に伴ってIT障害を引き起こす新たな脅威が顕在化した際、それらの脅威を要因とするIT障害によるサービスへの影響等を考慮し、必要に応じて適切な対策を導入しているか
	(6)知識・技能を有する者の配置	情報セキュリティに関する資格の保有者等一定以上の知識・技能を有する者を配置すること。	◎＊	◎＊	◎＊	◎＊	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1.（1）共通 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

【実施指針について】 ◎:実施すべきである。　○:実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						参考資料	
項目		対策	実施指針			資料名	内容
			事業用	その他	自営	ユーザ	
	(7)情報セキュリティに関する利用者への周知	情報通信ネットワークに対して利用者が与える又は情報通信ネットワークの利用者が受ける可能性のある影響とその対策について利用者に周知すること。	◎	◎	－	－	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1.（1）共通 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
	(8)社内の重要情報の管理	ア ネットワーク内の装置類やサービスの属性に応じた情報を分類すること。	◎	◎	◎	◎		
		イ 情報管理に関する内部統制ルールを整備すること。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	2.（1）共通 情報及び情報処理施設と関連する資産のすべてについて、組織の中に、その管理責任者を指定しているか 組織に対しての価値、法的要求事項、取扱いに慎重を要する度合い及び重要性の観点から、情報を分類しているか 2.（3）重要情報漏えい対策 各組織における重要情報の管理責任者を組織の長に定めて、重要情報の管理に努めているか 重要情報の範囲を明確にし、管理すべき重要情報について、重要情報管理責任者の管轄組織毎に保管リストを作成・維持しているか 重要情報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
	(9)サイバー攻撃に備えた管理体制	サイバー攻撃発生時の迅速な情報共有方法を確立すること。	◎	◎	－	－	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1.（2）サイバー攻撃対策 情報セキュリティインシデントに対する迅速、効果的で整然とした対応を確実にするため、責任体制及び手順を確立しているか
6.データ管理								
	(1)体制の明確化	作業の分担、連絡体系、責任の範囲等のデータ管理体制を明確にすること。	◎	◎	◎	◎		

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						参考資料	
項目		対策	実施指針			資料名	内容
			事業用	その他	自営	ユーザ	
	(2)基準の設定	データ管理基準を設定すること。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)イ(イ)情報の取扱い【要検討事項】 情報の作成、入手、利用、保存、移送、提供及び消去等、情報のライフサイクルに着目し、各段階における情報セキュリティ対策が明示されるべきである。 ○情報の作成と入手 ・目的外の作成・入手の禁止 ・台帳等作成 ・作成・入手時における情報の格付けと取扱制限の決定 ・作成時点の情報の格付けの継承 ・格付けの変更手続き ○情報の利用 ・情報の利用に関する許可及び届出に係る措置 ・目的外利用の禁止 ・格付け及び取扱制限に従った情報の取扱い ・格付け及び取扱制限の見直し ・アクセス履歴の保存 ・アクセス制御・出力制御 ・離席時の対策(端末ロック等) ○情報の保存 ・格付けに応じた情報の保存(アクセス制御、記録媒体の保管、パスワード・電子署名・暗号化による保護、バックアップ・複写、更新履歴管理の取扱い等の記載) ・情報の保存期間に従った管理 ○情報の移送 ・情報の移送に関する許可及び届出に係る措置 ・作業責任者・手続きの明確化 ・作業担当者の識別、認証、権限付与 ・移送手段の選択 ・書面の保護対策 ・電磁的記録の保護対策(パスワード設定、暗号化、電子認証等))

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　ー:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目		対策	実施指針				資料名	内容
			事業用	その他	自営	ユーザ		
								○情報の提供 ・提供に関する許可及び届出 ・付加情報の削除 ○情報の消去 ・情報の消去に関する許可及び届出 ・電磁的記録の消去手続き（消去の確認、消去記録の保管等） （1）ウ（ア）情報セキュリティ確保のために求められる機能 ○権限管理 ・権限管理機能の導入 ・利用者IDと主体認証情報の付与管理 ・利用者IDと主体認証情報における代替手段等の適用 ○証跡管理 ・証跡管理機能の導入実施 ・証跡取得と保存 ・取得した証跡の点検、分析及び報告 ・証跡管理に関する利用者への周知
	(3)作業の手順化	データ取扱作業の手順化を行うこと。	◎	◎	◎	◎		
	(4)データの記録物の管理	ア 設備の仕様及び設置場所等のデータ並びに利用者に関するデータの記録物については、重要度による分類及び管理を行うこと。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）イ（ア）情報の格付け【要検討事項】 取扱う情報について、その重要度に応じた適切な措置を講じるため、機密性、完全性、可用性の観点から、情報の格付け（ランク）や、取扱制限（例：複製禁止、持出禁止、再配布禁止）が明示されるべきである。 ○重要性に応じた適切な措置 ・試算の洗出し（体制。洗出し項目、洗出し基準等） ・情報のライフサイクルと情報の格付けに応じた情報セキュリティ対策

【実施指針について】 ◎:実施すべきである。　○:実施が望ましい。　ー:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目		対策	実施指針				資料名	内容
			事業用	その他	自営	ユーザ		
							電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	2.（1）共通 すべての資産を明確に識別し、また、重要な資産すべての目録を作成し、維持しているか 2.（3）重要情報漏えい対策 重要情報の全社的な管理方針に基づく情報のランク付けにより、その重要度に応じた取扱いを行なっているか 重要情報の具体的な取扱い方法を定めているか 情報に括り付けられたランクの表示方法、及び、ランクに応じた保管ルールとその運用方法を定めているか
		イ 設備の仕様及び設置場所等のデータ並びに利用者に関するデータに対する従事者の守秘義務の範囲を明確にするとともに、その周知、徹底を図ること。	◎	◎	◎	◎		
		ウ 利用者の暗証番号等の秘密の保護に配慮すること。	◎	◎	◎	◎		
		エ 記録媒体の性能向上やシステム間の接続の拡充などによるリスク・脅威の拡大に応じた適時の点検・見直しを行うこと。	◎	◎	◎	◎		
	(5)ファイル等の遠隔地保管	重要なプログラム、システムデータ及び利用者に関するデータのファイル等については、前世代及び現世代のものを地域的に十分隔たった場所に別に保管すること。	○	○	○	○		

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						参考資料	
項目		対策	実施指針			資料名	内容
			事業用	その他	自営	ユーザ	
	(6)重要データの漏えい防止対策	個人情報以外の重要な設備情報（特に他社のセキュリティ情報等）の漏えいを防止するための適切な措置を講ずること。	◎	◎	○	○	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(2)イ(ア)保護すべき情報の類型化【要検討事項】 漏えい対策の対象となる保護すべき情報を類型化し、明示されるべきである。 ○保護すべき情報の類型化 ・情報分類の指針、情報のラベル付け及び取扱い、重要情報の格付け ・情報資産の洗出し方法（体制、洗出し項目、洗出し基準）、情報、情報システムについてのランク付け ・情報資産の機密性、完全性、可用性に基づく分類 ・安全管理上の重要度に応じた分類（安全性が損なわれた場合の影響の大きさに応じた分類） ・個人データ取扱台帳の整備、リスクアセスメント結果に応じた分類 (2)イ(イ)保護すべき情報の管理 保護すべき情報及び当該情報が記録された媒体を安全に取扱う（作成、入手、利用、保存、移送、提供及び消去等）ための措置が明示されるべきである。 ○情報の作成と入手 ・目的外の作成・入手の禁止 ・台帳等作成 ・作成・入手時における情報の格付けと取扱制限の決定 ・作成時点の情報の格付けの継承 ・格付けの変更手続き ○情報の利用 ・情報の利用に関する許可及び届出に係る措置 ・目的外利用の禁止 ・格付け及び取扱制限に従った情報の取扱い ・格付け及び取扱制限の見直し ・アクセス履歴の保存 ・アクセス制御・出力制御 ・離席時の対策（端末ロック等）

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目		対策	実施指針				資料名	内容
			事業用	その他	自営	ユーザ		
								・要保護情報の利用にあたっての措置（情報交換の方針及び手順、取外し可能な媒体の管理、重要情報の内部漏えい、盗難、紛失、流出への対策） ・書類や電子媒体の持ち出し管理（書類等の保管ルール、端末への資料の保管、持出しに関するルールや制限） ○情報の保存 ・格付けに応じた情報の保存（アクセス制御、記録媒体の保管、 パスワード・電子署名・暗号化による保護、バックアップ・複写、 更新履歴管理の取扱い等の記載） ・情報の保存期間に従った管理 ・安全な場所への保管（自然災害を被る可能性が低い地域への保管、外部記録媒体の耐火、耐熱、耐水及び耐湿を講じた施設への保管） ・内容表示の記号化（媒体等に保存情報内容が想定できるタイトル表示をすることの禁止） ・バックアップの分散、隔地保管 ○情報の移送 ・情報の移送に関する許可及び届出に係る措置 ・作業責任者・手続きの明確化 ・作業担当者の識別、認証、権限付与 ・移送手段の選択 ・書面の保護対策 ・電磁的記録の保護対策（パスワード設定、暗号化、電子認証等） ○情報の提供 ・情報の提供に関する許可及び届出 ・付加情報の削除 ○情報の消去 ・情報の消去に関する許可及び届出 ・電磁的記録の消去手続き（消去の確認、消去記録の保管等）

【実施指針について】 ◎:実施すべきである。　○ :実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目		対策	実施指針				資料名	内容
			事業用	その他	自営	ユーザ		
							電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1.（2）イ（イ）保護すべき情報の管理 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 1.（5）重要情報漏えい対策 重要情報の管理について全社的な管理責任者を定め、重要情報に対する全社的な管理方針を定めているか
7.環境管理								
	(1)建築物の保全	保全点検を定期的に行うこと。	◎	◎	◎	◎		
	(2)空気調和設備の保全	保全点検を定期的に行うこと。	◎	◎	◎	◎		
8.防犯管理								
	(1)体制の明確化	防犯体制を明確にすること。	◎	◎	◎	◎		
	(2)管理の手順化	防犯管理の手順化を行うこと。	◎	◎	◎	◎		
	(3)建築物、通信機械室等の入出管理	建築物、通信機械室等の入出管理を行うこと。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）エ（ア）施設と環境【要検討事項】 入退出の管理や安全区域の確保、停電時、断水時の対応等情報システムの設置・運用に係る施設や環境面での対策が明示されるべきである。 ○入退出の管理 ・入退出管理（障壁、施錠、主体認証、入退出履歴の記録、継続的に立ち入る者の承認、侵入監視装置の設置、最小限の施設表示） ・訪問者、清掃業者及び物品の搬出入業者の管理（身分の記録、入室審査手順、立ち入り制限区域の設定、職員等の立ち会い・付き添い、ストラップ・IDカード、情報システムに接触できない場所での受け渡し）
	(4)かぎ、暗証番号等の管理	出入口のかぎ及び暗証番号等の適切な管理を行うこと。	◎	◎	◎	◎		
	(5)防犯装置の管理	防犯装置の保全点検を定期的に行うこと。	◎	◎	◎	◎		
	(6)入出管理記録の保管	入出管理記録は、一定の期間保管すること。	○	○	○	○		
9.非常事態への対応								
	(1)体制の明確化	ア 連絡体系、権限の範囲等の非常事態時の体制を明確にすること。	◎	◎	◎	◎		

【実施指針について】 ◎:実施すべきである。　○:実施が望ましい。　－:対象外。
◎＊:技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準							参考資料	
項目		対策	実施指針					
			事業用	その他	自営	ユーザ	資料名	内容
		イ 非常事態時における社員・職員、復旧に必要な業務依託先などへの連絡手段、社員・職員の参集手段の確保等の体制を整えること。	◎	◎	○	○		
		ウ 非常事態時における広域応援体制を明確にすること。	○	○	○	○		
		エ 相互接続を行う事業者等の間において、非常災害時の連絡体制や連絡内容を明確にすること。	◎	◎	○	○		
		オ 非常事態時における応急活動、復旧活動に際しては、国等の関係機関との連絡体制を明確にすること。	◎	◎	○	○		
		カ 非常事態時において、応急活動、復旧活動にかかわる連絡手段を確保するために必要な措置を講ずること。	◎	◎	○	○		
	(2)復旧対策の手順化	復旧対策の手順化を行うこと。	◎	◎	◎	◎		
10.教育・訓練								
	(1)体制の明確化	教育・訓練に関する計画の策定及び実施を行う体制を明確にすること。	◎	◎	◎＊	◎＊	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(イ)情報セキュリティの人材の育成等【参考事項】 知的財産としての「人財」という観点から、情報セキュリティ人材の育成や要員の管理を行うことが望ましい。
	(2)教育・訓練の内容	キ 情報セキュリティに関する教育・訓練を行うこと。	◎	◎	◎	◎		

別表第３　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準			参考資料	
項目		対策	資料名	内容
1　目的				
この指針は、情報通信ネットワークの健全な発展に寄与することを目的とし、適正なリスク管理を実現させるための基本となる情報セキュリティポリシー策定のための指針として定めたものである。				
2　情報セキュリティの管理				
情報セキュリティを適切に管理していくためには、情報セキュリティの「方針立案」、「対策実施」、「運用・監視」及び「監査・診断」の各段階において、以下の対策を行う必要がある。				
(1) 方針立案				
	ア 情報セキュリティポリシー及び実施手順の策定	情報セキュリティを適正に管理していくために、組織における情報セキュリティ対策に関する統一方針として情報セキュリティポリシーを策定する。 また、情報セキュリティポリシーに基づき、実際の業務・作業レベルまで考慮した情報セキュリティ実施手順を策定する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティ基本方針の策定
	イ 情報セキュリティ組織体制の整備	情報セキュリティに関して、責任所在の明確化やセキュリティ情報の共有化を行うために、情報セキュリティ組織体制を整備する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティに関する組織体制の整備（責任者・責任部門・委員会等の設置、役割・責任分担の明確化等）
(2) 対策実施				
	情報セキュリティポリシーの普及・教育	情報セキュリティポリシーが適正に実施されるよう、普及・教育活動を行い、情報セキュリティに対する自覚や意識の向上を目指す。	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」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○教育・訓練の実施 ・情報セキュリティ対策の教育・訓練計画の策定 ・教育・訓練実施記録の保管
(3) 運用・監視				
	ア 情報セキュリティポリシーに沿った運用	情報セキュリティポリシーを理解し、情報セキュリティポリシーに沿った運用を適正に実行する。		
	イ 例外の管理	業務を遂行する中で、情報セキュリティポリシーが適用できない場合が発生する可能性もある。情報セキュリティポリシーから逸脱した際に、適正に管理する仕組みを確立する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティ関係規程の整備（違反への対処、例外措置等）

別表第３　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準				参考資料	
項目			対策	資料名	内容
	ウ 情報セキュリティ侵害時の対応の明確化		情報セキュリティ侵害が起きた際、速やかに侵害の事実、状況を伝達できるよう伝達経路を明確化する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ア（ア）組織・体制及び人的資源の確保【要検討事項】 〇組織・体制の確立 ・IT障害発生時の体制・対応手順の整備（「重要インフラの情報セキュリティ対策に係る第2次行動計画」が想定するサイバー攻撃、非意図的要因、災害や疾病等の脅威が引き起こすIT障害に関わる情報の集約及び共有体制を含む）
(4) 監査・診断					
	ア 情報セキュリティ監査		情報セキュリティポリシーが組織内において正しく実行されていることを把握するため定期的に監査する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ア（ア）組織・体制及び人的資源の確保【要検討事項】 〇自己点検・内部監査の実施 ・自己点検の実施 ・内部監査の実施 （ウ）外部監査等による情報セキュリティ対策の評価【参考事項】 ・情報セキュリティ監査等の実施
	イ 情報セキュリティポリシーの見直し		情報セキュリティ監査結果や情報セキュリティを取り巻く環境等を考慮し、情報セキュリティポリシーを定期的に見直し、改訂を行う。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ア（ア）組織・体制及び人的資源の確保【要検討事項】 〇自己点検・内部監査の実施 ・情報セキュリティ対策の見直し （ウ）外部監査等による情報セキュリティ対策の評価【参考事項】 ・情報セキュリティ対策の見直し
3　情報セキュリティポリシーの構成等					
情報セキュリティの環境は技術動向、組織状況により変化することから、次のように情報セキュリティポリシーを目的、原則及び方針の三段階に階層化させることで、下位の方針のみを見直し、時代・環境変化に対応することができる。					
(1)　目的			情報セキュリティポリシーにおいて最も基本となるもので、組織としての情報セキュリティへの取組の目的を定めるものである。最高権限者の声明として記述し、組織全体で積極的に情報セキュリティに取り組むことを明確化することが望ましい。		

別表第３　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準			参考資料	
項目		対策	資料名	内容
	(2)　原則	目的に基づき、情報セキュリティを実現するための組織方針、組織理念等組織の基本的な考え方を定めるものである。利便性とセキュリティのバランスをどのように取るかといった、情報セキュリティ全体の考え方の根幹となる。		
	(3)　方針	原則に基づき、情報セキュリティを実現するための基本方針をテーマごとに具体化し定めるものである。各方針に対し、責任の所在を明確化する必要がある。		
	(4)　実施手順	定められた情報セキュリティポリシーを確実に実施するため、情報セキュリティポリシーに基づき、具体的な手順や方法を実施手順として定めることが一般的である。実施手順では、情報システムが最低限備えるべき具体的セキュリティ要件や、各情報システムの利用方法等、各方針に沿い、実際の業務、手順、方法等を記述することとなる。		
4　情報セキュリティポリシーの策定				
	情報セキュリティポリシーは、組織として取り決めた最も重要な規程となるため、組織の幹部の関与により策定することが一般的である。 情報セキュリティポリシーの策定に当たり、各部門の業務に何らかの制約や変更を要請することがあるため、経営企画部門、総務部門といった社内規定を担当する部門が中心となり、各部門よりメンバーを召集して策定の為のチームを設立し、策定を行うことが望ましい。 なお、情報セキュリティポリシーには、情報システム部門、人事部門、監査部門等の部署の役割が非常に大きいため、これらの部門からの積極的参加を要請する。 また、外部コンサルティングサービスを提供する機関を活用し、策定に当たってのスケジュール、策定方法、記述事項等についての助言を得ることが好ましい。 情報セキュリティポリシーを策定する際の実施手順を以下に示す。			
	(1)　情報セキュリティポリシー策定チームの編成	各部門よりメンバーを召集し策定のためのチームを設立する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティに関する組織体制の整備(責任者・責任部門・委員会等の設置、役割・責任分担の明確化等)
	(2)　「目的」及び「原則」の明確化	組織としての情報セキュリティに関する考えの根幹となる「目的」及び「原則」を定める。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティ基本方針の策定
	(3)　情報セキュリティポリシーの適用範囲の明確化	情報セキュリティポリシーがどの範囲まで適用されるのかを明確化する。		

別表第３　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準			参考資料	
項目		対策	資料名	内容
	(4)　情報資産の洗い出し	現在、組織が保有する情報資産とその価値を明確化する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(2)イ(ア)保護すべき情報の類型化【要検討事項】 〇保護すべき情報の類型化 ・情報分類の指針、情報のラベル付け及び取扱い、重要情報の格付け ・情報資産の洗出し方法(体制、洗出し項目、洗出し基準)、情報、情報システムについてのランク付け
	(5)　情報資産を取り巻く脅威とその脅威に対するリスクの分析	保護すべき情報資産を明らかにし、脅威の発生頻度、影響度を基にリスクを分析する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(2)イ(ア)保護すべき情報の類型化【要検討事項】 〇保護すべき情報の類型化 ・情報資産の機密性、完全性、可用性に基づく分類 ・安全管理上の重要度に応じた分類(安全性が損なわれた場合の影響の大きさに応じた分類)
	(6)　「方針」の明確化	各情報資産を保護するために、組織としてどのような方針をもって対策を行うかを明確化する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 〇組織・体制の確立 ・情報セキュリティ基本方針の策定
5　情報セキュリティポリシーの構成例				
情報セキュリティポリシーの構成例と各項目における記述内容を以下に示す。 ここでは、方針を「情報セキュリティ運営に関する方針」と「情報資産に関する方針」に大きく分け、前者では管理の各段階に応じた項目、後者では情報資産の大きな区分である「情報」、「情報システム」、そして、情報資産を保護するための「アクセス制御」という項目立てとしている。				
【構成例のため、以下省略。】				
1　総則				
	(1) 目的	情報セキュリティの必要性と組織としての情報セキュリティの目的を記述する。最高権限者の声明として記述することで、情報セキュリティに対して組織全体で積極的に取り組むことを表明することが望ましい。		
	(2) 適用範囲	人、組織、場所、情報資産、技術等の切り口で情報セキュリティポリシーが適用される範囲を明確化する。		

別表第３　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準				参考資料	
項目			対策	資料名	内容
	(3) 用語及び定義		情報セキュリティポリシー内で用いる用語の意味を明確にし、読者が共通の解釈の下、理解・判断できるよう用語の定義を行う。		
	(4) 原則		組織としての情報セキュリティに対する考え方の根幹となる原則を明確にし記述する。すべての方針、対策等は、ここで記述される原則に準拠しなければならない。例として、法令の遵守を原則として記述した場合、この原則に準拠し各組織員の役割等を方針にて定める。		
2 方針					
	(1) セキュリティ運営に関する方針				
		ア 情報セキュリティ組織	組織内の情報資産を管理し、セキュリティを担保する仕組みを確立する。具体的には、経営陣による情報セキュリティフォーラムの設立と、情報セキュリティに関する責任者の割当てを行う。また、組織内で働く外部業者を適用範囲に含む際は、その管理方法（契約時の必須項目等）を明確化する。		
		イ 普及・教育	情報セキュリティに対する知識と意識を向上させ、適用範囲内すべての人が情報セキュリティポリシーを理解し、遵守するよう、情報セキュリティポリシーの普及・教育活動を行うことを記述する。		
		ウ 例外の管理	情報セキュリティポリシーから逸脱する事項を管理・統括する組織・方法を明確にする。 費用対効果を分析した結果、情報セキュリティポリシーに準拠することが得策ではない事項等が発生した際の対処方法を明確にすることで、逸脱発見者が迅速に対応を行い、組織として逸脱事項を管理・統括する体制を整備する。		
		エ 情報セキュリティ侵害時の対応	適用範囲内において、情報セキュリティ侵害が発生した際の対応手順を明確化することで、発生時に迅速に対応できる体制、方法を確立する。また、情報セキュリティポリシー違反者及びその監督責任者に対する罰則についても記述する。		
		オ 情報セキュリティ監査	情報セキュリティポリシーが組織内において正しく実行されていることを把握するため、定期的に監査する必要がある。監査組織と監査結果を把握する者を明確化する。		
		カ 情報セキュリティポリシーの改訂	情報セキュリティ監査結果や情報セキュリティを取り巻く環境等を考慮し、情報セキュリティポリシーを定期的に見直し、改訂を行う。改訂手順についても明確化する。		
	(2) 情報資産に関する方針				

別表第３　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準					参考資料	
項目				対策	資料名	内容
		ア 情報		適用範囲内の情報についての管理方法を明確化することで、情報の漏えい、破壊、改ざん等を防止する。また、プライバシーにかかわる情報を取り扱う際に遵守すべき事項を明確化する。		
			(ア) 情報管理	情報の漏えい、破壊、改ざん等による被害等に応じて、情報を区分する。情報の区分と情報の取得・生成、保管、流通、利用及び廃棄という各段階における情報の取扱方法を確にし、組織員による情報の取扱方法を統一化する。		
			(イ) プライバシー情報	通信の秘密を含むプライバシー情報の漏えいは深刻な権利利益侵害につながるおそれが高いため、電気通信事業者に対しては、「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」（平成１６年総務省告示第６９５号）が制定されている。 プライバシー情報の適切な利用と保護が極めて重要であるとの認識により、プライバシー情報の取扱いについては、個別の項目を設け、個人情報の収集、利用・提供、適正管理、責任の明確化等について、遵守すべき方針を明確に記述する。		
		イ 情報システム		適用範囲内の情報システム上にて取り扱われる電子情報の漏えい、破壊、改ざん等の防止及び情報システム停止による損害の抑止を目的とし、情報システムについての管理方法（設計、構築及び運用方法）を明確化する。		
			(ア) 情報システム設計・構築	情報システムの設計、構築時における管理体制と、情報システムに実装すべきセキュリティ機能（アクセス制御機能、フロー制御機能、暗号化制御機能等）を明確化する。		
			(イ) 情報システム運用・停止	情報システムを適切に運用するための管理体制と実施事項を明確化する。また、情報システム障害時の対応策についても明確化する。		
			(ウ) 情報システムの使用権	情報システムの利用資格管理が適切に行われないと、情報システムの不正利用を招く危険がある。そこで、情報システムの使用権を、必要な者に、必要な期間与え、情報システムの利用資格に関する義務・責任を明確化する。また、情報システムの不正利用の定義を明確化する。		
			(エ) ネットワークセキュリティ	ネットワークは情報流通の基盤であるとともに、情報侵害の経路ともなり得るため、適切に把握・管理することが必要である。セキュリティ侵害を防止するため、管理体制・実施事項を明確化する。		

別表第３　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準						参考資料	
項目					対策	資料名	内容
				(オ) コンピュータウイルス	業務で使用する機器がコンピュータウイルスに感染した場合、多大な被害が発生する可能性があるため、感染の予防及び防止が重要である。そこで、コンピュータウイルスに関しても管理体制を確立し、予防及び防止並びに感染時の対策を明確化する。また、コンピュータウイルス等による情報漏えいの防止対策も明確化する。 また、コンピュータウイルスによる情報漏えいが懸念されるため、情報漏えいを発生させる懸念のあるソフトウェアの導入を防止する等の予防措置を明確化するとともに、コンピュータウイルスに感染した場合の情報漏えいの防止対策を明確化する。		
				ウ アクセス制御	適用範囲内の情報システムの利用、建物への入館、事務室及び機械室への入室等に際しては、情報資産を保護するため、個人を識別・認証し、情報へアクセスする際に審査することが必要である。そこで、利用者を限定・把握できるよう実施事項を明確化する。		

別表第４　危機管理計画策定のための指針

情報通信ネットワーク　安全・信頼性基準		参考資料	
項目	対策	資料名	内容
1　目的			
危機管理計画は、サイバーテロについてあらかじめ対処方法を定めておくことで、実際にサイバーテロが発生した場合に迅速な対応を可能とし、早期に現状へ復旧し、被害の拡大を防ぐことを目的とするものである。この指針は、電気通信事業用ネットワークにおいてサイバーテロが発生した場合の緊急対応体制を整備するため、危機管理計画策定の指針として定めたものである。 電気通信事業用ネットワーク以外のネットワークにおける危機管理計画についても対象とするネットワーク、想定される攻撃等を考慮し、本指針を参考として策定されることが望ましい。			
2　サイバーテロの定義等			
(1)　サイバーテロの定義	サイバーテロは、コンピュータウィルスやハッカーによつて個人が被害を受けるものとは異なり、国家等の重要システムを機能不全に陥れるものであることから、この指針におけるサイバーテロの定義は、「ネットワークを通じて各国の国防、治安等をはじめとする各種分野の情報システムに侵入し、データを破壊、改ざんするなどの手段で国家等の重要システムを機能不全に陥れる行為」とする。		
(2)　攻撃対象となる重要インフラ	サイバーテロの攻撃対象となつた場合、その産業、企業のみならず、広く国民生活に重大な影響が及ぶこととなる重要インフラとして、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）等が想定される。		
(3)　重要インフラの相互依存性	各重要インフラは、他の重要インフラと独立して存立するのではなく、相互に依存し存立しており、ある重要インフラが攻撃を受けた場合、関連する他の重要インフラも影響を受ける場合が多々あることから、重要インフラを保有してサービスを提供する事業者は、他インフラへの影響も考慮した対策が必要である。		
(4) 主な攻撃方法			
サイバーテロにおける主な攻撃方法の具体例としては、次のものがある。			
ア　物理的な攻撃	電気通信施設に不正侵入し、ネットワーク管理センターを占拠する等によりネットワークのコントロールを奪い、これをまひさせるような攻撃		
イ　ホームページ改ざん	思想的な意図等により社会に広くアピールするため、ホームページの掲載内容を改ざんするもの		
ウ　分散協調型サービス拒否（以下「DDos」という。）攻撃	複数の場所からサーバーの処理能力を超える大量のデータを送り付けるなどの方法によりサーバーを停止させるもの		
エ　コンピュータウィルス	強力な感染力と破壊力を持つウィルスによる攻撃		

別表第４　危機管理計画策定のための指針

情報通信ネットワーク　安全・信頼性基準		参考資料	
項目	対策	資料名	内容
オ　不正侵入（なりすまし）	他人になりすまして侵入し、データの改ざん、削除を行うほか、他への攻撃にも使用		
３　危機管理計画の策定			
危機管理計画の策定に当たつて配慮すべき内容を以下に示す。			
(1) 対象			
ア 攻撃			
対象とするべき電気通信ネットワークのぜい弱な部分の具体例は次のとおりである。これを参考として、各電気通信事業者の状況により大規模な影響が出ることを想定し、対象となる攻撃を明確に規定			
(ア) 固定・移動電話網	物理的な攻撃、意図的なふくそうによる攻撃		
(イ) 移動電話網	電波による不正アクセス、電波による通信妨害		
(ウ) 専用回線網及び中継回線網	電波妨害		
(エ) IPネットワーク	サーバー等への攻撃、モバイルインターネットアクセスへの攻撃、コンピュータウィルス		
(オ) ネットワークの機	電磁波による情報漏えい		
イ 被害規模の対象範囲			
各電気通信事業者の状況により大規模な影響が出ることを想定して、被害規模の対象範囲を明確に規定する。 その際には、電気通信事業法施行規則（昭和60 年郵政省令第25 号）第58 条の報告を要する重大事故の基準も参考とする。			
(2) 予防			
必要に応じて次のハッカー対策、コンピュータウィルス対策等を規定し、サイバーテロに対する予防措置を			
ア インターネットに接続するための機器の配置及び構成	(ア) ファイアウォール等を設置して適切な設定を行う。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ウ(イ)情報セキュリティについての脅威【要検討事項】 セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。
	(イ) 非武装セグメント構成を採用する。		
	(ウ) 開放網と閉域網とを区別したネットワーク構成を採用する。		
	(エ) telnetやftp等サービス提供に不用な通信の接続制限を行う。		
	(オ) 最新の情報セキュリティ技術を採用する。		
	(カ) 攻撃元を特定できる機能と攻撃元のトラヒックを遮断する仕組み等を採用		
イ ソフトウェア上の対策	(ア) インターネットに接続する場合は、サーバー等におけるセキュリティホール対策を講ずる。		
	(イ) コンピュータウィルス及び不正プログラム混入対策を講ずる。		

別表第４　危機管理計画策定のための指針

情報通信ネットワーク　安全・信頼性基準			参考資料	
項目		対策	資料名	内容
	ウ 監視、管理等	(ア) インターネットに接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されるよう措置する。 また、ネットワーク上のパケット並びにサーバー及びネットワーク機器の動作に関するログの適切な記録及び保存を行う。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ウ(ア)情報セキュリティ確保のために求められる機能【要検討事項】 主体認証（利用者及び機器等の認証）、アクセス制御、権限管理、証跡管理、負荷分散、冗長化など基本的な情報セキュリティ機能の観点から、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。
		(イ) コンピュータからの漏えい電磁波の低減対策、又は電磁環境に配慮した上で漏えい電磁波をマスクする措置を講ずる。		
	エ 不正アクセス防止のためのシステム上の設定	(ア) 利用者の識別・確認を要する通信を取り扱う情報通信ネットワークには、正当な利用者の識別・確認を行う機能を設ける。		
		(イ) アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずる。		
		(ウ) 利用者のパスワードの文字列をチェックし、一般的な単語を排除する機能を設ける。		
		(エ) アクセス失敗回数の基準を設定するとともに、基準値を超えたものについては、履歴を残しておく機能を設ける。		
		(オ) 保護することが求められる重要な情報については、その情報に対するアクセス要求を記録し、保存する機能を設ける。		
		(カ) ネットワークへのアクセス履歴の表示又は照会が行える機能を設ける。		
		(キ) 一定期間以上パスワードを変更していない利用者に対して注意喚起する機能を設ける。		
		(ク) 一定期間以上ネットワークを利用していない利用者がネットワークにアクセスする際に、再開の意思を確認する機能を設ける。		
		(ケ) アクセスにおける本人認証手段には、端末認証（MACアドレス、シリアル番号等）や生体認証（指紋、静脈等）など、高度な認証方式の導入を検討する事が望ましい。		
	オ 通信の秘密の保護	(ア) 機密度の高い通信には、秘話化又は暗号化の措置を講ずる。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)エ(エ)通信回線及び通信回線装置【要検討事項】 〇構築時 ・通信の暗号化 ・通信性能の確保
		(イ) 適切な漏話減衰量の基準を設定する。		

別表第４　危機管理計画策定のための指針

情報通信ネットワーク　安全・信頼性基準				参考資料	
項目			対策	資料名	内容
		カ ネットワークの不正使用の防止	ネットワークの不正使用を防止する措置を講ずる。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（ア）情報セキュリティ確保のために求められる機能【要検討事項】 主体認証（利用者及び機器等の認証）、アクセス制御、権限管理、証跡管理、負荷分散、冗長化など基本的な情報セキュリティ機能の観点から、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。
		キ 新たな手法による攻撃に対するハード・ソフト対策の体制強化	ネットワークシステムの脆弱性に対処できるように内部統制や社内ルールを随時見直し、新たな手法による攻撃に対しても迅速にハード・ソフト両面で対処できる体制を確立・強化する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（ア）情報セキュリティ確保のために求められる機能【要検討事項】 〇自己点検・内部監査の実施 ・内部監査の実施 ・情報セキュリティ対策の見直し
		ク 他の利用者へ悪影響を与えている利用者に対する一時利用停止の明確化	他の利用者に悪影響を与えている事象を洗い出し、当該事象への対応方針を策定し、利用者の合意形成を図る。		
		ケ サーバー等への攻撃が発生した際の迅速な情報共有方法の確立			
	(3) 発生時の復旧対応				
		ア 復旧対応としては、必要に応じて次の項目を規定するとともに、既存の障害復旧マニュアル等を活用		重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）エ（エ）通信回線及び通信回線装置【要検討事項】 通信回線及び通信回線装置の構築から運用、運用終了又は停止に至るまでの対策が明示されるべきである。
		(ア) サーバー等への攻撃からの復旧対応	A DDoS攻撃により通信不能となつた場合、攻撃側サーバーの速やかな停止を依頼する。		
			B サーバーのルート権限を奪われる等により不正な処理を開始した場合、サーバーを停止する又はネットワークから切断し再起動する。		
			C サーバーが何らかの原因により不正な処理を開始した場合、ルート権限で不正な処理のプロセスを排除する。		
			D サーバーへの侵入の痕跡を発見した場合、サーバーをネットワークから隔		
			E サーバー等が通信不能となつた場合、通信不能箇所を特定し再起動などの処置を行う。		
		(イ) 伝送交換設備への攻撃からの復旧対策	A 重要な伝送路設備には、応急復旧用ケーブルの配備等の応急復旧対策を講ずる。		
			B 移動用交換設備の配備等の応急復旧対策を講ずる。		
			C 災害時等において、衛星地球局等の無線設備により、臨時電話等の設置が可能であること。		
			D 移動体通信基地局と交換局の間の回線に障害が発生した場合等に、無線設備により、臨時に対向の電気通信回線の設定が可能であること。		

別表第４　危機管理計画策定のための指針

情報通信ネットワーク　安全・信頼性基準		参考資料	
項目	対策	資料名	内容
	E　移動体通信基地局に障害が発生した場合等に、可搬型無線基地局により、臨時の電気通信回線の設定が可能であること。		
	F　他の伝送設備の障害時に、通信の疎通が著しく困難となつた場合、予備の設備等により臨時の電気通信回線の設定が可能であること。		
イ　緊急時における対処には、高度な判断を必要とする場合があることから、責任と権限を有する適切な者が速やかに判断を行うことができるように規定する。		重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（2）ア（ア）事業継続性確保のための個別対策の実施【要検討事項】 〇未然防止措置 ・指揮命令系統の明確化 ・権限委譲、代行順位の決定
ウ　複数の電気通信事業者に障害が発生し、その影響が波及して被害が拡大していくことが想定されることから、障害情報等を交換し被害を最小限に抑えるために、国、電気通信事業者、事業者団体等の関係者間で連絡体制、運用方法を明確に規定する。			
（4）　原因判明時の措置	ア　復旧対応としては、必要に応じて次の項目を規定するとともに、既存の障害復旧マニュアル等を活用することも規定する。		
	イ　障害の発生状況及び影響の拡大防止に対する協力に関して、電気通信事業者から利用者への周知方法等について規定する。		
	ウ　障害の発生原因が判明し、再度攻撃にさらされるおそれがある場合における障害の発生防止のため、必要な措置を講じることを規定する。		
	エ　ネットワークを介して、他分野の重要インフラ事業者と情報システムを相互接続している場合には、サイバーテロ対策に関し互いの連絡・連携体制を必要に応じ構築する。		
（5）　危機管理計画の見直し等	ア　技術の進展に伴い、サイバーテロによる攻撃方法等が、変化していくと考えられるため、適宜危機管理計画の見直しを行うことを規定する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（ア）情報セキュリティ確保のために求められる機能【要検討事項】 〇自己点検・内部監査の実施 ・内部監査の実施 ・情報セキュリティ対策の見直し
	イ　サイバーテロが発生した際の対処を円滑に行えるよう、必要に応じサイバーテロの発生を想定した訓練を実施することを規定する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ア（ア）組織・体制及び人的資源の確保【要検討事項】 〇教育・訓練の実施 ・情報セキュリティ対策の教育・訓練計画の策定 ・教育・訓練実施記録の保管

「情報通信ネットワーク 安全・信頼性基準」と情報セキュリティに関する事故事例との比較

１ レンタルサーバ業者の事故 （その他の電気通信事業ネットワークに該当）

（同社の第三者調査委員会による調査報告書を参考に作成）

１．１ 事故の概要

特定のサーバー群に対して実施されたメールシステム障害解消のためのメンテナンスを実施したところ、更新プログラムの不具合により、顧客の大量のデータが消失した。本来更新プログラムはプライマリーディスクのみにあてられるものの、社内マニュアルを無視した担当者の独自仕様により同一筐体内のバックアップディスクにも同時に適用してしまい、データの復元が不可能となった。

その後、消失した大量のデータを復元するために、十分に検証を行わずにオープンソースソフトウェアの復元プログラムを用いて、消失データの復元を実行し、リカバードファイルを顧客に提供したところ、第三者のデータが含まれていたことが判明した。

１．２ 安全・信頼性基準との比較

事 故	問題点	安全信頼性基準の該当箇所	対 策
・データの消失 ・メール送受信不可	データの復元ができない	別表第１ 設備等基準 第１ 設備基準 １ 一般基準 （１０）ソフトウェアの信頼性向上対策	ウ システムデータ等の重要データの復元ができること。
	プライマリーディスクとバックアップディスクの同時更新	別表第１ 設備等基準 第１ 設備基準 １ 一般基準 （１０）ソフトウェアの信頼性向上対策	イ ソフトウェア及びデータを変更するときは、容易に誤りが混入しないよう措置を講ずること。
	プログラムによってデータの完全消去が可能	別表第１ 設備等基準 第１ 設備基準 １ 一般基準	イ ソフトウェア及びデータを変更するときは、容易に誤りが混入しないよう措置を講ずること。

		（10）ソフトウェアの信頼性向上対策	
	システム変更に関する社内マニュアルの無視	別表第2　管理基準 2　ネットワーク施工管理 （2）作業工程の明確化等	作業工程を明確にするとともに、その管理を行うこと。
	同一筐体内へのバックアップ保存	別表第2　管理基準 6　データ管理 （5）ファイル等の遠隔地保存	重要なプログラム、システムデータ及び利用者に関するデータのファイル等については、前世代及び現世代のものを地域的に十分隔たった場所に別に保管すること。
第三者に他者のデータを提供	十分な検証もないまま復元プログラムの使用	別表第1　設備等基準 第1　設備基準 1　一般基準 （10）　ソフトウェアの信頼性向上対策	ア　ソフトウェアを導入する場合は、品質の検証を行うこと

2　オンラインゲーム業者の事故　（その他の電気通信事業ネットワークに該当）

（経済産業省ニュースリリースを参考に作成）

2．1　事故の概要

同社のオンラインサービスのサーバーへの不正侵入により、数千万人の利用者の個人情報が流出した。事故後の調査で、同社のオンラインサービスの委託先において、CIOなどの情報セキュリティに関する専門的な責任者が不在であること、異常発生時における報告連絡体制に係る規程等の未整備であること、公知の脆弱性について自社の確認体制が整えられていないこと、委託先との間で個人情報の取扱等、安全管理措置を遵守させる契約が締結されていないこと等、情報セキュリティ対策が十分に講じられていないことが指摘された。

2．2　安全・信頼性基準との比較

事　故	問　題　点	安全信頼性基準の該当箇所	対　策
個人情報の漏えい	ネットワークへの不正侵入	別表第1　設備等基準 第1　設備基準	オ　ソフトウェアには、サイバー攻撃等に対する脆弱性がないように対策を継続的に講ずること。

		1　一般基準 （10） ソフトウェアの信頼性向上対策	
		別表第1　設備等基準 第1　設備基準 1　一般基準 （11）情報セキュリティ対策	カ インターネットへ接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されること
	情報セキュリティに関する専門的な責任者の不在	別表第3 情報セキュリティポリシー策定のための指針 2 情報セキュリティの管理 （1）方針立案 イ　情報セキュリティ組織体制の整備	情報セキュリティに関して、責任所在の明確化やセキュリティ情報の共有化を行うために、情報セキュリティ組織体制を整備する。
	異常発生時における報告連絡体制に係る規程等の未整備	別表第2　管理基準 9 非常事態への対応 （1） 体制の明確化	ア 連絡体系、権限の範囲等の非常時の体制を明確にすること。
	公知の脆弱性に対する自社の確認体制の未整備	別表第2 5 情報セキュリティ管理 （5）情報セキュリティに関する情報収集	最新の情報セキュリティに関する技術情報や業界動向を入手し、それらを情報セキュリティ対策に反映させること。
	委託先との間に個人情報の取扱等、安全管理措置を遵守させる契約の未締結	別表第2 3 ネットワーク保全・運用 （6）委託保守運用管理	ア 保守の委託を行う場合は、契約書等により保守作業の範囲及び責任の範囲を明確にすること。

3　電気通信事業者の事故 （電気通信回線設備事業用ネットワークに該当）

（同社報道資料を参考に作成）

３．１　事故の概要

同社の業務委託先の元社員によって不正プログラムが投入され、基地局に設置されたATM伝送装置の内部データが破損し、基地局とセンター設備の間で通信ができなくなった。これにより、3G回線を利用した音声・パケット通信等のサービスが使用しづらくなった。

３．２　安全・信頼性基準との比較

事　故	問　題　点	安全信頼性基準の該当箇所	対　策
通信サービスが使用しづらい	業務委託先の元社員による情報セキュリティの脅威	別表第２ ３ ネットワーク保全・運用 （６）委託保守運用管理	ア 保守の委託を行う場合は、契約書等により保守作業の範囲及び責任の範囲を明確にすること。 イ 保守を委託する場合は、作業手順を明確にするとともに、監督を行うこと。
	不正プログラムの混入	別表第１　設備等基準 第１　設備基準 １　一般基準 （１１）情報セキュリティ対策	ケ コンピュータウイルス及び不正プログラム混入対策を講ずること。
	不正プログラムによるATM伝送装置の内部データの破損	別表第１　設備等基準 第１　設備基準 １　一般基準 （１１）情報セキュリティ対策	シ アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずること。

４「標的型サイバー攻撃の事例分析と対策レポート」（（独）情報処理推進機構（２０１２年１月））　（ユーザネットワークに該当）

４．１　概要

国内企業、衆議院・参議院が、外部から情報窃取型の標的型攻撃メールを送付され、添付されていたウイルスがシステム内部に侵入し、情報が流出してしまう事故が発生した。これを受けて、（独）情報処理推進機構が標的型サイバー攻撃への対策レポートを発行した。このレポートに記載されている対策と安全・信頼性基準との比較を行った。

4．2 安全・信頼性基準との比較

事 故	対 策	安全信頼性基準の該当箇所	対 策
情報漏えい	1) システム入り口での防御 ・ファイアウォール ・最新のウイルス対策ソフト ・侵入検知／防止システム	別表第1 設備等基準 第1 設備基準 1 一般基準 （11）情報セキュリティ対策	ア インターネットへ接続する場合は、ファイアウォールを設置して適切な設定を行うこと カ インターネットへ接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されること。 ク インターネットへ接続する場合は、最新の情報セキュリティ技術を採用すること。 ケ コンピュータウイルス及び不正プログラム混入対策を講ずること。 ナ ネットワークの不正使用を防止する措置を講ずること。
	2) 脆弱性対策 □OSやサーバーソフトウェアの定期的な脆弱性診断 □OSやサーバーソフトウェアに関する脆弱性情報の時期を逸しない収集と修正プログラムの適用 □ウェブアプリケーションへの脆弱性の作り込みの回避 ・ウェブアプリケーションファイアウォール（WAF）	別表第1 設備等基準 第1 設備基準 1 一般基準 （10） ソフトウェアの信頼性向上対策	オ ソフトウェアには、サイバー攻撃等に対する脆弱性がないように対策を継続的に講ずること。 ケ 定期的にソフトウェアを点検し、リスク分析を実施すること。
		別表第1 設備等基準 第1 設備基準 1 一般基準 （11）情報セキュリティ対策	ア インターネットへ接続する場合は、ファイアウォールを設置して適切な設定を行うこと。
		別表第2 5 情報セキュリティ管理 （5）情報セキュリティに関する情報収集	最新の情報セキュリティに関する技術情報や業界動向を入手し、それらを情報セキュリティ対策に反映させること。
	3) 標的型攻撃ルートでの対策 ・スパムフィルタ	別表第1 設備等基準 第1 設備基準	ア インターネットへ接続する場合は、ファイアウォールを設置して適切な設定を行うこと

	□URLフィルタ □外部メディア利用規則、強制利用抑止	1　一般基準 （11）情報セキュリティ対策	ウ インターネットへ接続する場合は、telnet や ftp 等サービス提供に不用な通信の接続制限を行うこと。 シ アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずること。
		別表第2 3 ネットワーク保全・運用管理 (4) 監視、保守及び制御	イ 情報通信ネットワークの動作状況を監視し、必要に応じ、接続規制等の制御措置を講ずること。
	4) ウイルス活動の阻害および抑止 （出口対策） ・端末間、他部署間のネットワーク通信の制限（ウイルスの組織内蔓延抑止） □組織の端末からの外部通信はプロキシを経由させる等の経路制御 ・組織内ネットワーク量の監視（異常さを早期に検知しウイルスの蔓延を早期に発見） □知財等のある重要なサーバーはインターネットから隔離	別表第1　設備等基準 第1　設備基準 1　一般基準 （11）情報セキュリティ対策	イ インターネットへ接続する場合は、非武装セグメント構成を採用すること。 エ インターネットへ接続する場合は、開放網と閉域網とを区別したネットワーク構成を採用すること。 カ インターネットへ接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されること。 シ アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずること。
	5) アクセス制御 □ユーザ認証 □アクセスするプログラムの特定（ホワイトリスト化）	別表第1　設備等基準 第1　設備基準 1　一般基準 （11）情報セキュリティ対策	サ 利用者の識別・確認を要する通信を取り扱う情報通信ネットワークには、正当な利用者の識別・確認を行う機能を設けること シ アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずること。
	6) 情報の暗号化	別表第1　設備等基準	テ 機密度の高い通信には、秘話化又は暗号化の措置を講

	□通信路の暗号化（Virtual Private Network などの利用） □ファイルの暗号化 □暗号鍵管理	第1　設備基準 1　一般基準 （11）情報セキュリティ対策	ずること。
		別表第2 6 データ管理 （4）データの記録物の管理	ア 設備の仕様及び設置場所等のデータ並びに利用者に関するデータの記録物については、重要度による分類及び管理を行うこと。
		別表第2 6 データ管理 （6）重要データの漏えい防止対策	重要な設備情報（特に他社のセキュリティ情報等）の漏えいを防止するための適切な措置を講ずること。
	7） システム監視、ログ分析 □ネットワークログ取得・分析 □サーバログ取得・分析 □アクセスログの監査（DB 監査ツールなど含む）	別表第1　設備等基準 第1　設備基準 1　一般基準 （11）情報セキュリティ対策	カ インターネットへ接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されること。 キ インターネットへ接続する場合は、ネットワーク上のパケット並びにサーバー及びネットワーク機器の動作に関するログの適切な記録及び保存を行うこと。
	8） 管理統制およびコンテンジェンシープラン（事前準備・事後対応） □セキュリティポリシーの徹底 □海外を含むグループ会社間でのセキュリティガバナンス □危機対応体制の整備	別表第2 5 情報セキュリティ管理 （1）情報セキュリティポリシーの策定	情報セキュリティポリシーを策定し、適宜見直しを行うこと。
	標的型攻撃メールが届いた場合の対応	別表第2 10　教育・訓練 （2）教育 ・ 訓練の内容	キ 情報セキュリティに関する教育・訓練を行うこと。