

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 1.3 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見直しが必要と認められる基準

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輻輳を発生させた。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が改正され、平成 24 年 9 月 1 日に施行された。主な省令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）

事業	その他	自営	ユーザ
◎	—	—	—

【関係基準：別表第 1 第 1 1. (3) の追加】

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】

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が、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。

重要通信である緊急通報は、電気通信事業法第8条により、電気通信事業者は優先的に取り扱わなければなら通信として位置づけられ、当該接続等を確保するための規定の趣旨については、今回の見直しに合わせ、基準に新たな対策として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.(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、次に節に報告するIPネットワーク設備委員会の審議を踏まえ、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措置対策は存在するが、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に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17日に報告書が取りまとめられた。

当該報告書は、同日、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
- ・輻輳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、消費者団体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その他利用者の災害対策の事前準備に役立つ事項。
- 災害時に必要な事項
輻輳、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、衛星携帯電話の貸与）、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 TCA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、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^{※1}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わ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。

※1 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。

※2 PHS事業者においては、通信インフラの特性を考慮し個別対応とする。

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例

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例
(いずれも省略)

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	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）	・ 性能、カバー範囲（半径約〇km等）、音声最大接続数	
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

※ PHS事業者においては、通信インフラの特性を考慮し個別対応とする。

図 2.2.2.3.2-1 車載型の移動無線基地局の公表例

図 2.2.2.3.2-2 可搬型の移動無線局の公表例

（いずれも省略）

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。

2.2.2.4 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に、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 輻輳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・PHS事業者に限定されたものであり、IPネットワーク設備委員会の提言、消費者団体等が電気通信事業者に求める事項の全てを満たすものではないが、初めて具体的な公表内容の共通化が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、既存情報提供媒体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頻発したことを受けて、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ことを総務省から要請した。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）については、同連絡会において情報が共有された。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。

○ バーストラヒック及び制御信号対策

- ・ 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。また、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の協力のお願いを実施。
- ・ 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）」を发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。

○ 事業者間の情報共有

- ・ 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。

（管理基準）

2.3.1 バーストラヒック及び制御信号等対策について（P）

現行基準には、将来の規模の拡大やトラヒック増加を考慮した設計についての対策は存在するが、最近のスマートフォンの普及によるトラフィックの急激な増加や制御信号の増加を考慮した明確な対策はない。

トラフィックの急激な増加や制御信号の増加を要因とする電気通信事故が発生している現状を踏まえて、電気通信事業者が取り組んでいる制御信号や端末の挙動を抑制する対策、実環境に近い過負荷試験等によるバーストラヒック対策等は、事故の未然防止につながることから、基準に追加することが適当である。

【関係基準：別表第2 1.（2）イ及びエ】

（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容量の確保）

事業	その他	自営	ユーザ
◎*→◎	—	—	—

【関係基準：別表第1 第1 1.（6）】

（実施指針）（バーストラヒック及び制御信号等対策）

事業	その他	自営	ユーザ
◎*	—	—	—

【関係基準：別表第2 1.（2）追加】

(実施指針) (品質・機能検査の充実化)

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。

【関係基準：別表第2 12.（2）】

2.3.6 事業者間の情報共有について

現行基準には、電気通信事業者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 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等を、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端末の利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〉

【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)】

- ・ 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。

(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、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
○	→○	—	—

【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)

事業	その他	自営	ユーザ
◎	◎	—	—

【関係基準：別表第2 12. (5) 追加】

(実施指針) (児童ポルノブロッキング)

事業	その他	自営	ユーザ
◎※	◎※	—	—

【関係基準：別表第2 12. (5) 追加】

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、安全・信頼性基準に不足している項目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、整合性の確認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項目の比較を行った。

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項目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項目によって、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、ふくそう防止の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、コンピュータウイ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。

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)(案)

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。 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						実施指針		根拠資料		論点(方向性)	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	事業	その	自営	ユー	資料名	内容	〔 ○…基準への反映 △…解説への反映 〕				
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業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> 電気通信業務に係る情報の管理、電気通信業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業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。 ○現行基準は災害時も想定しているものと考えられることから、改正省令を根拠資料として適用。 ○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業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。 ○努力義務規定が新たに設けられた趣旨を踏まえて、実施指針(対策の実施レベル)を現状より強化することが適当である。 ○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》	【KDDI】 →実施指針については、現行通り○に留める、もしくは◎*とする。 理由: 重大な支障を及ぼす設備について、複数の地域に分散を図ることは重要なことですが、システム構成上や、地形的な問題により、センター分散ができない設備も存在します。そのため、現行通りの指針にとどめるか、各事業者で、技術的な課題を解決しつつ、段階的に実施することが適当と考えます。 【ソフトバンクモバイル・テレコム】 論点(方向性)の記載について、既にガイドラインの本文から読み取れる内容であるため、本文の見直しは不要と考えます。 また、省令において努力義務規定であることから、実施指針においても「○(望ましい)」の現行の記載の通りで問題無いものと考えます。 【TCA】 実施指針について、省令上は努力義務であり、重要な通信設備は複数の地域に分散させることが望ましいが、システム構成上や地形的な理由により分散設置できない設備も存在することから、実施指針は○のままとした。	努力規定が新たに設けられた趣旨を踏まえれば、現行の実施指針(○)の見直し(対策レベルの上位化)を行うことが適当と考える。 (なお、事業規模、設備規模から地理的な分散化が不要と想定される事業者の場合は、実際的には、上位の実施指針となっていたとしても、当該実施指針が求められるものとはならない。)		
	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業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> 電気通信業務に係る情報の管理、電気通信業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業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。 ○現行基準は災害時も想定されているものと考えられることから、改正省令を根拠資料として適用。 ○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である。 ○「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。	【ソフトバンクモバイル・テレコム】 論点(方向性)の記載について、既にガイドラインの本文から読み取れる内容であるため、本文の見直しは不要と考えます。 また、省令において努力義務規定であることから、実施指針においても「○(望ましい)」の現行の記載の通りで問題無いものと考えます。 【TCA】 事務局の論点(方向性)に賛同します。			
(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回線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。	○	ー	○	ー							
	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。	○	ー	○	ー							
	(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されたことから、基準に省令改正された内容を追加することが適当である。 ○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が、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2.1.4参照》	【ソフトバンクモバイル・テレコム】 ただし書きの具体例は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 地形の状況や代替措置については、総務省と都度相談するものと考えており、具体例の解説への記載は行わず、基準への以下の記載に留めることとした。 <基準案> 交換設備相互間の伝送路設備は、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。 <実施指針>◎:実施すべきである	TCAの考え方を踏まえ、検討することとしたい。		
(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業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、臨時的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が新たに規定されたことから、基準に省令改正された内容を努力義務として追加することが適当である。 ○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》	【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 手段や条件等を限定しないよう、基準へ省令の内容をそのまま反映させることとし、実施指針は努力義務規定であることから「○」とした。 <基準案> 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、臨時的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促進すること。 <実施指針>○:実施が望ましい	TCAの考え方を踏まえ、検討することとしたい。			

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)(案)

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					実施指針		根拠資料		論点(方向性) 〔○…基準への反映 △…解説への反映〕	構成員の意見	構成員の意見に対する事務局の回答	
項目	対策	事業	その	自営	ユー	資料名	内容					
(4)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。	○	-	○	-							
(5)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業務の提供に重大な支障が生ず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> 電気通信業務に係る情報の管理、電気通信業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業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。	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業務の提供に重大な支障を生ず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> 電気通信業務に係る情報の管理、電気通信業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業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。 ○現行基準は災害時も想定されているものと考えられることから、改正省令を根拠資料として適用。 ○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業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。 ○努力義務の規定化により、実施指針を現状より強化することが適当である。 ○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)	【KDDI】 一実施指針については、現行通り○に留める、もしくは◎*とする。 理由:重大な支障を及ぼす設備について、複数の地域に分散を図ることは重要なことですが、システム構成上や、地形的な問題により、センター分散ができない設備も存在します。そのため、現行通りの指針にとどめるか、各事業者で、技術的な課題を解決しつつ、段階的に実施することが適当と考えます。 【ソフトバンクモバイル・テレコム】 論点(方向性)の記載について、既にガイドラインの本文から読み取れる内容であるため、本文の見直しは不要と考えます。 また、省令において努力義務規定であることから、実施指針においても「○(望ましい)」の現行の記載の通りで問題無いものと考えます。 【TCA】 論点記載の方向で合意。 実施指針について、省令上は努力義務であり、重要な通信設備は複数の地域に分散させることが望ましいが、システム構成上や地形的な理由により分散設置できない設備も存在することからも、実施指針は○のままにしたい。	努力規定が新たに設けられた趣旨を踏まえれば、現行の実施指針(○)の見直し(対策レベルの上位化)を行うことが適当と考えます。 (なお、事業規模、設備規模から地理的な分散化が不要と想定される事業者の場合は、実際的には、上位の実施指針となっていたとしても、当該実施指針が求められるものとはならない。)		
(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。	◎*	-	-	-	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業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。	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業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。	○最近のスマートフォンの普及によるトラフィックの急激な増加、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。 ○現行基準の「通信の集中」という文言では、想定外のトラフィックも含まれるように解釈できるので、それを含まないように「通信量の増加」という文言に変更することが適当である。	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 モバイルインターネット接続サービスには、端末、ネットワーク、お客様の利用動向など様々なトラフィック変動要素があり、設備容量として「通信の集中」を考慮していても、これらのトラフィック変動要素から想定外のトラフィックが発生した場合、処理することができない場合がある。 現状の基準では、想定外のレベルの「通信の集中」についても考慮することが必要と取られてしまいうため、対策の文言を想定可能な「通信量の増加」に修正したい。	TCAの考え方を踏まえ、現行基準の「通信の集中」という表現から、「通信量の増加」に修正することとしたい。 なお、実施指針については、見直し(対策レベルの上位化)を検討することとしたい。
(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。	○	-	-	-	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。	○本基準は電子メール対策が事業者側のネットワークでしか対応できなかった時点での規定であり、現時点では、事業者側のネットワークだけでなく、利用者側での対応も可能となっている現状にあるため、「別表第2 管理基準 12.安全・信頼性の確保等の情報公開」の新(5)に移行することが適当である。 ○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側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、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。 (本文2.4参照)	○本基準は電子メール対策が事業者側のネットワークでしか対応できなかった時点での規定であり、現時点では、事業者側のネットワークだけでなく、利用者側での対応も可能となっている現状にあるため、「別表第2 管理基準 12.安全・信頼性の確保等の情報公開」の新(5)に移行することが適当である。 ○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側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、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。 (本文2.4参照)	【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 本根拠資料は、本基準における「設備や設備管理」における安全・信頼性、や「情報セキュリティポリシーや危機管理計画の策定にあたって配慮すべき事項」いずれでもないため、検討にそぐわないものと考えます。	次項欄を参照。	
(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業務提供事業者は、携帯電話インターネット接続業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端末の利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業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。	○現行基準には「電子メールの受信を拒否する等の機能」についての記載はあるが、既に法令化されている「青少年有害情報フィルタリングサービス」の機能についての基準がないため、追加することが必要ではないか。 ○同様な機能について規定されている(7)との整合性を図ることが必要ではないか。 (本文2.4参照)	【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 本根拠資料は、本基準における「設備や設備管理」における安全・信頼性、や「情報セキュリティポリシーや危機管理計画の策定にあたって配慮すべき事項」いずれでもないため、検討にそぐわないものと考えます。	(7)の基準は電子メール対策が事業者側のNWでしか対応できなかった時点での規定。しかし、現時点では、事業者側のNWだけでなく、利用者側での対応も可能となっている現状にあるため、(7)の基準と追加の新基準に関しては、利用者への情報提供の仕組み(別表第2 管理基準 12.安全・信頼性の確保の情報公開等)で対応することとしたい。		

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)(案)

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		実施指針				根拠資料		論点(方向性) 〔○…基準への反映〕 〔△…解説への反映〕	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	事業	その	自営	ユー	資料名	内容			
	(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。	○児童ポルノに関するインターネット上の情報の切断に関する取組みが各電気通信事業者において行われていることから、基準にその旨を追加することが必要ではないか。 《本文2.4参照》	【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【JAIPA】 根拠資料として、以下を追加することを提案します。 [資料]児童ポルノ排除総合対策 平成22年7月27日犯罪対策関係会議決定 [内容]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ことあり、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、ISPIによる閲覧防止措置(ブロッキング)を講ずる必要がある。 【TCA】 本根拠資料は、本基準における「設備や設備管理における安全・信頼性」や「情報セキュリティポリシーや危機管理計画の策定にあたって配慮すべき事項」いずれでもないため、検討にそぐわないものとする。	同上
(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。	◎	-	◎	-			△マイクロ回線や衛星回線については、基準の「他の疎通確保の手段」の具体例として有用であることから、解説に例として追加することが適当である。	【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 手段や条件等を限定しないように記載することとしたい。 ＜解説案＞ 「他の疎通確保の手段」として「マイクロエントランス無線回線」や「衛星回線」等の利用が考えられる。	TCAの解説案を踏まえ、検討することとしたい。
	イ 重要な伝送路設備には、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に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に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に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。	○	○	○	○					
	(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った場合において、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」が新たに規定されたことから、基準に省令改正された内容を追加することが適当である。 ○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》	【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 本内容は、管理基準「3. ネットワーク保全・運用(4)監視、保守及び制御」において追加されると考えるが、本項目では具体的にどのような基準に追加されるのか方針が知りたい。	改正省令の記載を参考に基準案を作成する予定である。 (なお、別表第2においても当該省令を引用して基準を追加することを提案しているが、重複して基準化することについては問題ないものとする。)

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)(案)

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〕	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	実施指針				資料名	内容			
(10)ソフトウェアの信頼性向上対策	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間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。	△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。	〔NTT〕 現行、実施指針が「◎(実施すべきである)」とされておりませんが、導入判定を確実にこなすべく対象範囲については、様々な解釈があると考えられます(例えば、ベンダから供給されるOS等のバージョンアップ等)ので、「呼処理等に影響を及ぼすソフトウェア」等範囲を明確にする記載等についても検討することが望ましいと考えます。 〔ソフトバンクモバイル・テレコム〕 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。 〔イー・アクセス〕 組織や体制については各社の経営や業態に強く依存するため、一部の事業者殿の事例をそのまま基準化するのはなく、解説における取り組み事例として挙げる程度に留めておくことが適当であると考えます。 〔TCA〕 組織や体制については各社の経営や業態に強く依存するため、一部の事業者殿の事例をそのまま基準化するのはなく、解説における取り組み事例として挙げる程度に留めておくこととしたい。 <解説案> 「電気通信業務に係る情報の管理、電気通信業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業務の提供に重大な支障を及ぼすおそれのあるものに係るソフトウェアを導入する場合は、商用設備導入前に関係部門間で品質の検証を行うこと。」	全ての事業者者に共通する事項のみを基準化等するのではなく、一部の事業者の取り組みだけでも、安全・信頼性向上に資する取組であれば参照されるべき事項として、基準化等していくことが適当と考えているところ。 なお、TCAの意見について(解説への反映)は、検討することとしたい。
						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。	△PDCAサイクル等の取組み事例については、基準の品質の検証の具体例として、解説への記載を検討。	〔ソフトバンクモバイル・テレコム〕 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。 〔TCA〕 PDCAサイクルについては品質管理の手法の一つであるため、「別表第2 管理基準 11 現状の調査・分析及び改善 (4)改善」へ解説にて記載したい。 <解説案> 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。	TCAの考え方を踏まえ、検討することとしたい。
	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。	◎	◎	二	二			○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》	〔ソフトバンクモバイル・テレコム〕 当時当該文言を記載した背景を鑑み、削除を行うかどうかの検討を行うことが妥当と考えます。 〔TCA〕 中小固定系事業者への影響の懸念があるのではないか。	
	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。	◎	◎	二	二			○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》	〔ソフトバンクモバイル・テレコム〕 当時当該文言を記載した背景を鑑み、削除を行うかどうかの検討を行うことが妥当と考えます。 〔TCA〕 論点記載の内容に同意。	
	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。	◎	◎	◎*	◎*	ベストプラクティス (NTTドコモ)	他社の事故事例を参考に、セキュリティ監査の対象として「設備工事用のデータ設定サーバ」を追加。	△セキュリティ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、解説への記載を検討。	〔ソフトバンクモバイル・テレコム〕 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。 〔TCA〕 NW構成やその運用方法が各社により異なることから、具体的な記載が必ずしも有効では無いため、記載しないこととしたい。	根拠資料に挙げられている内容について、他の適切な項目への移動を検討したい。
	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。	◎	◎	○	○	ベストプラクティス (ソフトバンクモバイル)	事業用設備の設定・操作について、本人認証、ログ取得、外部ネットワークとの遮断を実施していることを確認。			
(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。	◎*	-	◎*	-					
(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。	◎	-	◎*	-					

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)(案)

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〕	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	実施指針			資料名	内容			
		事業	その	自営			ユー		
	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。	○	○	○	○		<p>○現行基準に「その他の電気通信事業用ネットワーク」と「ユースネットワーク」に対する実施指針が示されているが、これらのネットワークに移動用交換設備の配備が必要とする理由が想定できないため、当該ネットワークの実実施指針の見直しが必要ではないか。</p> <p>○IP化の進展に伴い本基準に記載されてい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。</p> <p>《本文2.6参照》</p>	<p>【TCA】 その他の電気通信事業用ネットワーク及びユーザネットワークの実実施指針見直し(「○」⇒「-」)については賛同いたします。しかしながら、本項における左記対策に対し、固定系音声役務提供事業者ではこれまで、アナログ/ISDNインタフェースの張り出し設備等を有し、有事の際はこれらを配備・活用することをもって対策としてきたが、IP化の進展に伴い同方式による応急復旧措置の維持が困難になることが想定されることから、本対策の内容の見直しについて、この機会に検討していただきたい。</p>	TCAの考え方を踏まえ、本基準を削除する方向で検討することとしたい。
	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。	○	-	○	-		<p>○東日本大震災時に各電気通信事業者が実際に実施した応急復旧対策を踏まえて、実施方針を変更する必要ではないか。を検討したが、障害の状況や事業者毎によって応急復旧対策の内容が異なることから、現行基準のままが適当である。</p>	<p>【ソフトバンクモバイル・テレコム】 事業者毎に実際に実施した応急復旧対策の内容や手段は異なることから、実施指針においては「○(望ましい)」の現行の記載の通りとすることを要望いたします。</p> <p>【TCA】 障害の状況に応じて、必ずしも設置が可能であるか不確定であり、また、事業者毎に実際に実施した応急復旧対策の内容や手段は異なることから、実施指針においては「○(望ましい)」の現行の記載の通りとしたい。</p>	TCAの考え方を踏まえ、実施指針については、現行をベースに検討することとしたい。
	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。	○	-	○	-		○上記と同趣旨。	<p>【ソフトバンクモバイル・テレコム】 事業者毎に実際に実施した応急復旧対策の内容や手段は異なることから、実施指針においては「○(望ましい)」の現行の記載の通りとすることを要望いたします。</p> <p>【TCA】 障害の状況に応じて、必ずしも設置が可能であるか不確定であり、また、事業者毎に実際に実施した応急復旧対策の内容や手段は異なることから、実施指針においては「○(望ましい)」の現行の記載の通りとしたい。</p>	TCAの考え方を踏まえ、実施指針については、現行をベースに検討することとしたい。
	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。	○	-	○	-		○上記と同趣旨。	<p>【ソフトバンクモバイル・テレコム】 事業者毎に実際に実施した応急復旧対策の内容や手段は異なることから、実施指針においては「○(望ましい)」の現行の記載の通りとすることを要望いたします。</p> <p>【TCA】 障害の状況に応じて、必ずしも設置が可能であるか不確定であり、また、事業者毎に実際に実施した応急復旧対策の内容や手段は異なることから、実施指針においては「○(望ましい)」の現行の記載の通りとしたい。</p>	TCAの考え方を踏まえ、実施指針については、現行をベースに検討することとしたい。
	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)					<p>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</p> <p>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。</p>	<p>○根拠資料に挙げられている、大ゾーン基地局の整備については、ネットワークの耐災害性向上に資することから、基準にその旨を追加することが必要ではないか。</p> <p>○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措置対策は存在するが、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に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。</p> <p>《本文2.2.1.1参照》</p>	<p>【KDDI】 →実施指針については○とする。 理由:大ゾーン基地局の整備により、実際に対災害性の向上が図られたかどうかの実績が、現時点ではございません。そのため、今後の災害時における効果を確認する必要があると考えます。現時点では、「実施が望ましい」とすることが適当と考えます。</p> <p>【ソフトバンクモバイル・テレコム】 大ゾーン基地局は耐災害性のための手段の一つに過ぎないため、手段を限定するような記載を行うことは相応しくないと考えます。また、「(16)大規模災害対策(追加)」に対災害性に関する記載の項目があり、冗長なため、削除を要望いたします。</p> <p>【TCA】 ＜基準案＞ 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は、大規模災害等緊急事態において、代替手段により通信の確保が可能であること。 実施指針は○</p>	TCAの考え方を踏まえ、検討することとしたい。

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)(案)

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					実施指針		根拠資料		論点(方向性) 〔○…基準への反映 △…解説への反映〕	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	事業	その	自営	ユー	資料名	内容				
(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。	○省令に緊急通報の接続等について規定(平成18年1月改正)されているため、基準に追加することが適当である。	[TCA] 論点記載の方向で合意。		
	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ずること。	◎	◎	-	-						
(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。	◎	◎	○	○			○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》	[TCA] 論点記載の方向で合意。		
(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業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ず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、臨時的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ずること。 <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> 電気通信業務に係る情報の管理、電気通信業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業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に関する措置が新たに規定されたことから、基準に省令改正された内容を追加することが適当である。 ○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、電気通信業務の提供に重大な支障が生じないよう措置を講ずることは、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》	[ソフトバンクモバイル・テレコム] ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 [TCA] 当該項目の根拠資料に挙げられた省令は、(3)等においても挙げられ、新たな基準の追加提案がされているため、当該項目の追加は重複しているため、当該項目においては、具体的にどのように基準に追加されるのか方針が知りたい。	改正省令の記載を参考に基準案を作成する予定。 本追加項目は、ご指摘のとおり、他の基準との関係から重複感もあるが、大規模災害への対策を規定した当該規定は、安全信頼性対策の基本でもあることから、重複記載するだけの意義はあるものとする。 再掲、重複掲載である事項については、誤解のないよう、解説において説明することとする。	
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。	◎	◎	◎	◎			△解説の「地盤液状化地域では、マンホール周辺を砕石で埋め戻すなどして、耐震性の向上を図る。」との記載について、マンホール以外の電柱等の具体例も考えられることから、解説への記載を検討したが、通信事業者のみでの取組みとしては十分に対応できないことから、現状のまが適当である。	[ソフトバンクモバイル・テレコム] ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 [TCA] 通信事業者のみで取り組んでも、十分な対応ができないため、追加は見送り願いたい。	TCAの考え方を踏まえ、検討することとしたい。	

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)(案)

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〕	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	実施指針				資料名	内容			
(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。	◎	◎	◎	◎	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。	○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、項目名を「水害対策」から「津波・水害対策」に変更することが必要ではないか。 △津波対策の例について、解説への記載を検討。	【ソフトバンクモバイル・テレコム】 ・項目名の変更について異議はございません。 ・解説やガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。	津波対策は、地域防災計画の見直しとの関連もあることから、「水害対策」とは別の基準・実施方針(新基準の追加措置)として検討することとしたい。
(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。	○東日本大震災において津波による被害が発生したことから、津波対策を講じる旨の基準を新たに追加することが適当である。 △津波対策の具体例については、解説に記載することが適当である。 ○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》 △着雪対策について、解説への記載を検討。	【ソフトバンクモバイル・テレコム】 津波対策については、政府中央防災会議等で審議されているように、①最大レベル(発生の頻度は低いものの壊滅的な打撃を与えるレベル)②①以外のレベル(発生の頻度は比較的高く、大きな支障を及ぼすレベル)とそれぞれのレベルに応じた対策を講じる旨検討されていることから、水害対策と同等の扱いにすることは適切ではないと考えます。 更には、津波対策は、地域の移転計画等が盛り込まれる地域防災計画と連動した検討を行うことも必要であり、一通信事業者のみでの対策実施は容易でないと考えますので、今回追記することは見送っていただきます。	
(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。	◎	◎	◎*	◎*				【ソフトバンクモバイル・テレコム】 解説やガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。	着雪対策を講じるような状況にないのであれば、見直しは不要とする。
(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。	◎	◎	◎*	◎*				【イー・アクセス】 本作業班やIPネットワーク設備委員会、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で未議論であると考えます。まず、着雪による通信サービスへの影響の分析から基準化の可否等検討すべきと考えます。	
(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。	◎	◎	◎	◎				【TCA】 本作業班やIPネットワーク設備委員会、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で未議論であると考えます。まず、着雪による通信サービスへの影響の分析から、基準化の可否等検討すべきと考えます。	
	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。	△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。	【ソフトバンクモバイル・テレコム】 解説やガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。	【TCA】 電波防護指針を反映する旨であれば、異論はございません。

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)(案)

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					実施指針		根拠資料		論点(方向性) 〔○…基準への反映 △…解説への反映〕	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	事業	その	自営	ユー	資料名	内容				
	イ とう道等には、施設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。	○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》	[TCA] 論点記載の内容に合意。		
						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。	△根拠資料に挙げられている、「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」については、中継ケーブルの耐災害性向上に資することから、解説への記載を検討したが、通信事業者のみでの取組みとしては十分に対応できないことから、現状のままが適当である。	[NTT] 一般的に地中化は高コストであり、自治体様等との共同溝の推進とあわせて推進が必要と考えます。通信事業者単独での推進には限界がございますことをご理解頂き、国(政府)の施策としても精力的に推進頂きたいと考えております。 【ソフトバンクモバイル・テレコム】 「下越し」工法は一例と考えますので、工法を限定することが無いように、解説やガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 [TCA] 構成員の意見の通り、通信事業者単独での取組みでは十分な対応ができないため、追加は見送り願いたい。	TCAの考え方を踏まえ、追加を見送る方向で検討したい。	
(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ずること。	◎	◎	◎	◎						
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。	◎	◎	○	○			△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が、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、解説から削除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いることから、「東日本大震災」を追加することが適当である。	[TCA] 論点記載の内容に合意。		
(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。	◎	◎	◎	◎			○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》	[TCA] 論点記載の内容に合意。		
	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。	○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。 △「交換機のプール化」の取組み事例については、現行基準の「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。 《本文2.6参照》	[ソフトバンクモバイル・テレコム] ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。 [TCA] ・「等」を削除することについて賛同 ・交換機のプール化については、各社が採用している通信方式、NW構成により、実施可否はあるが、「予備機器等への切り替え」の具体例のひとつとして、解説へ追記することには異論無し。		
(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。	○	○	○	○						

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)(案)

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〕	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	実施指針				資料名			
		事業	その	自営	ユー				
(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。	◎	◎	◎	◎				
	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。	◎	◎	○	○		△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が、最近の分析を踏まえて、「発生確率は低い」という文言について、解説から削除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いることから、「東日本大震災」を追加することが適当である。	[TCA] 論点記載の内容に合意。	
(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。	○省令の規定ふりに合わせることを適当である。 《本文2.6参照》	[TCA] 論点記載の内容に合意。 <基準案> 交換設備については、自家発電機及び蓄電池の設置その他これに準じ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)(案)

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		実施指針				根拠資料		論点(方向性) 〔○…基準への反映 △…解説への反映〕	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	事業	その	自営	ユー	資料名	内容			
	(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	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。	○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、基準にその旨を追加することが必要ではないか。	【ソフトバンクモバイル・テレコム】 「無停電化」と「バッテリーの長時間化」は電源の安定確保の手段の一つであるため、手段を限定するような記載は相応しくないと考えます。ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 また、本項目は改正省令に定める災害対策を強化すべき拠点における基地局限定の理解のため、「改正省令に定める災害対策を強化すべき拠点における基地局においては」等の追記を要望いたします。 【イー・アクセス】 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は、基地局の無停電化等は、一部の事業者の取組事例であったほか、「全ての通信設備が、どのような長時間の停電にも耐えるようにバッテリー等を設置することは費用負担等の面から現実的ではない。」とも整理されたところ。 本基準が規模の大小問わず広く事業者等に適用される観点では、停電対策についても取り組み可能な範囲で基準化すべきであり、一部の事業者殿の事例をそのまま基準化することは避けるべきと考えます。 【ウィルコム】 「都道府県庁、市役所又は町村役場においては」等の前提の追記が必要と考えます。 また「バッテリーの長時間化」が表現として適切と考えます。 【TCA】 ＜解説案＞ 基地局の「バッテリーの長時間化」については、電源の安定確保のために重要。	下欄のウの解説に追加することとした。
	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。	△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。		
	エ 自家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。		○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。 ○省令に努力義務として規定されたことから、実施指針を現状より強化することが適当である。 ○また、冷却用に水を必要とする自家発電機もあるため、現行基準の「燃料」を「燃料等」に変更することが適当である。 ○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》	【ソフトバンクモバイル・テレコム】 ・論点(方向性)の記載について、既にガイドラインの本文から読み取れる内容であるため、本文の見直しは不要と考えます。 また、省令において努力義務規定であることから、実施指針においても「○(望ましい)」の現行の記載の通りで問題ないものと考えます。 ・「燃料等」への記載変更は異議ございません。 【TCA】 ・論点(方向性)の記載について、既にガイドラインの本文から読み取れる内容であるため、本文の見直しは不要。 ・省令において努力義務規定であることから、実施指針においても「○(望ましい)」の現行の記載の通りで問題ない。 ・「燃料等」への記載変更は異議無し。	努力規定が新たに設けられた趣旨を踏まれば、現行の実施指針(○)の見直し(対策レベルの上位化)を行うことが適当と考える。
						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。	【ソフトバンクモバイル・テレコム】 「石油会社との間の優先給油契約の締結等」は電源の安定確保の手段の一つであるため、手段を限定するような記載は相応しくないと考えます。 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 「契約締結」は一例であるため、従来記載の内容で十分であると考えられるが、「一手段として」という趣旨であれば、追加に異議はない。	
	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。	◎	◎	○	○					

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)(案)

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。 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				根拠資料		論点(方向性) 〔○…基準への反映 △…解説への反映〕	構成員の意見	構成員の意見に対する事務局の回答		
項目	対策	実施指針 事業 其の 自営 ユー		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)	(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っても、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場合は、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) (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)	○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されたことから、基準に省令改正された内容を追加することが適当である。 ○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》	【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【イー・アクセス】 設備規則の改正省令案に基づき基準を設けるのであれば、強行規定との整合性を取る観点からも、下線部については、「省令に都道府県庁、市役所又は町村役場の防災上必要な通信を確保するための停電対策の強化への考慮が新たに規定」と、字句をそのまま反映することが適当であると考えます。 【TCA】 ＜基準案＞ 防災上必要な通信を確保するために、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は、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っ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事ができる場合を除き、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停電対策を講じなければならない。 実施指針は、◎	TCAの考え方を踏まえ、検討することとしたい。		
第2 環境基準										
1 センターの建築物	(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されたことから、基準に省令改正された内容を努力規定として追加することが適当である。 ○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が、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》	【NTT】 現在、南海トラフ巨大地震等の被災想定の見直しにおきましては、巨大地震も想定され、各自治体様におかれましてはハード/ソフトの両面での対策を検討しなければならない状況と推測いたします。当該被災想定エリアに日常の通信需要が多くなる場合、通信施設の当該エリアへの設置は避けられず、かつ、このような激甚災害を適切に回避する対策は必ずしも講じられるものではございません。ガイドラインへの記載におかれましては、このような実情を踏まえた記載についてもご考慮いただけますようお願い申し上げます。 【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 手段や条件等を限定しないよう、基準へ省令の内容をそのまま反映させることとしたい。 省令上は努力義務であるため、実施指針は○としたい。 ＜基準案＞ 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。	TCAの考え方を踏まえ、検討することとしたい。		
	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。	◎	◎	◎*	◎*	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。	○東日本大震災において津波による被害が発生していることから、「風水害等」を「津波、風水害等」に変更することが必要ではないか。	【TCA】 津波対策については、政府中央防災会議等で審議されているように、①最大レベル(発生の頻度は低いものの壊滅的な打撃を与えるレベル) ②①以外のレベル(発生の頻度は比較的高く、大きな支障を及ぼすレベル)とそれぞれのレベルに応じた対策を講じる旨検討されていることから、水害対策と同等の扱いにすることは適切ではないと考えます。 更には、津波対策は、地域の移転計画等が盛り込まれる地域防災計画と連動した検討を行うことも必要であり、一通信事業者のみでの対策実施は容易でないと考えますので、今回追記することは見送っていただきたい。	2. 屋外設備(6)水害対策の検討の中で整理することとして、本基準の見直しは行わないこととする。
	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。	◎	◎	◎*	◎*					

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)(案)

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〕	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	実施指針				資料名			
		事業	その	自営	ユー				
(3) 出入制限機能	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。	◎	◎	◎	◎				
	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出入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。	◎	◎	◎	◎				
	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。	◎	◎	◎	◎				
(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。	◎*	◎*	◎*	◎*				
	イ 出入口には、施錠機能を設けること。	◎	◎	◎	◎				
(4) 出入制限機能	イ 重要な設備を収容する通信機械室の出入口には、出入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出入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。	◎	◎	◎	◎				
	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。	◎	◎	◎*	◎*				
(5) 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。	◎	◎	◎*	◎*				
	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。	◎	◎	◎*	◎*				

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)(案)

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〕	構成員の意見	構成員の意見に対する事務局の回答
項目	対策	実施指針				資料名			
		事業	その	自営	ユー				
(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)(案)

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。 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						実施指針		根拠資料		論点(方向性) ○…基準への反映 △…解説への反映	構成員の意見	統一意見
項目	対策	事業	その	自営	ユー	資料名	内容					
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)	◎	◎	◎	◎					<p>○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が、現行基準の想定では、ベンダー、事業者等の関係者間の連携には触れられていないもの、社内の関係部門間との連携については触れられていないため、設計管理体制の明確化に加えて、基準にその旨を追加することが適当である。</p> <p>〔参考〕 2.ネットワーク施工管理(1)体制の明確化の根拠資料 3.ネットワーク保全・運用管理(1)体制の明確化の根拠資料 4.設備の更改・移転管理(1)体制の明確化の根拠資料</p> <p>○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》</p>	<p>【TCA】 設計管理の明確化、関係部門間の連携については、「(1)体制の明確化」に含まれていることから、追加は不要と考えるが、具体的にどのように基準に追加したいのか方針が知りたい。</p> <p>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が、現行基準の想定では、ベンダー、事業者等の関係者間の連携には触れられていないもの、社内の関係部門間との連携については触れられていないため、基準への追加が必要と考えているところ。 具体的には、ネットワーク設計管理における「関係部門間の連携」の主旨を明記する方針(2.(1)、3.(1)、4.(1)も同様に修正することを想定)である。 TCAの指摘のとおり、「(1)体制の明確化」に含まれる内容と判断される場合は、現行基準の改正も考えられる。</p>	<p>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が、現行基準の想定では、ベンダー、事業者等の関係者間の連携には触れられていないもの、社内の関係部門間との連携については触れられていないため、基準への追加が必要と考えているところ。 具体的には、ネットワーク設計管理における「関係部門間の連携」の主旨を明記する方針(2.(1)、3.(1)、4.(1)も同様に修正することを想定)である。 TCAの指摘のとおり、「(1)体制の明確化」に含まれる内容と判断される場合は、現行基準の改正も考えられる。</p>
(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	<ul style="list-style-type: none"> 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、データセンターの地域分散等)の検討を行う。等 	<p>△根拠資料に挙げられている、大規模災害時においても通信の疎通能力を維持するための各種設備増強については、情報通信ネットワークの基本的機能として満足させるための具体的な取組であることから、解説にその旨を追加することが適当である。</p>	<p>【ソフトバンクモバイル・テレコム】 できる限り疎通能力の向上を図る所存ですが、「大規模災害時においても疎通能力を維持」については、必ずしも大規模災害時の全ての通信を維持できるとは限らないため、「大規模災害時においてもできる限り疎通能力を維持」等の表記に変更頂き、ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【イー・アクセス】 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を引用するのであれば、冒頭部分は下線部のとおり修正いただくことが適当と考えます。 「根拠資料に挙げられている、大規模災害時においてできる限り通信の疎通能力を向上するための各種設備増強については、～(以下略)。</p> <p>【TCA】 ＜解説案＞ 大規模災害時においてもできる限り疎通能力を維持するための各種取組を行うこと。</p>	<p>TCAの考え方を踏まえ、解説の記載を検討することとしたい。</p>		
	イ 将来の規模の拡大、トラフィ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) 事業用電気通信設備規則の改正(平成24年9月1日施行)	<ul style="list-style-type: none"> 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をお願いを実施。 <p>(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った場合は、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。</p>	<p>○最近、スマートフォンの普及等による急激なトラフィック増加を要因とする事故が発生しているため、電気通信事業者は、設備増強やスマートフォンのアプリケーション(ソフトウェア)に起因する制御信号を抑制するための対策等を実施。 ○当該事故の要因となった事象を抽出し、基準に反映していくことは適当である。 ○現行基準には、端末の挙動に関する観点が含まれていないが、今後はネットワーク設計において端末の動作についても十分に考慮することが必要と考えられるため、基準にその旨を追加することが適当である。 △設計に関する取組み事例(左記の省令による分析結果を含む)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。</p>	<p>【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【TCA】 ・基準については、既存の文言中の「トラフィックの増加」の範囲に含まれると考えられるため、追加しないものとした。 ・解説については、事業者や採用しているシステム種別に特化した記載をすることは望ましく無いため、追加しないものとした。 ・具体的にどのように基準に追加したいのか方針が知りたい。</p>	<p>TCAの考え方及び資料安作24-3の議論を踏まえ、検討することとしたい。</p> <p>スマートフォンの普及などにより多発した電気通信事故を踏まえ、当該事故の要因となった事象を抽出し、基準に反映していくことが必要と考える。 具体的には、現行基準の「トラフィック増加」の主旨に「端末の挙動を含む。」という観点を加える方向で検討を行うこととしたい。</p>		

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)(案)

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)	構成員の意見	統一意見	
項目	対策	実施指針							
		事業	その	自営	ユー				
	(追加)								
					<p>ベストプラクティス (NTTドコモ)</p> <ul style="list-style-type: none"> ・パケット交換機とspモードシステム間で接続ルートを遮断が発生した場合に、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、商用網でのトラフィック変動に確実に対応するため、複数トラフィ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。 <p>ベストプラクティス (KDDI)</p> <p>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)。</p> <p>ベストプラクティス (ソフトバンクモバイル)</p> <p>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。</p> <p>ベストプラクティス (UQコミュニケーションズ)</p> <p>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。</p> <p>安全信頼性検討作業班資料 (NTTドコモ)</p> <p>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。</p> <p>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)</p> <p>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。</p> <p>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)</p> <p>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。</p>	<p>○パーストラフィック及び制御信号の増加を要因とする事故が発生していることから、その対策を考慮したネットワーク設計が必要であるため、新たに基準化することが適当である。</p> <p>△パーストラフィック及び制御信号の増加対策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、解説に記載することが適当である。</p> <p>△また、トラフィックオフロード等についての対策例等についても、解説に記載することが適当である。</p>	<p>【NTT】 本件はスマートフォンに特化した事故に関する追加案と理解しておりますが、『パーストラフィック』の記載表現は、対象とする範囲を拡大されるものと考えますので、表現について引き続き議論させていただきたいと考えております。</p> <p>【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【TCA】 パーストラフィックの予見及び実態把握が難しく、パーストラフィックを考慮した設計が困難であることから、設計指針の記述は行わず、「(5)品質・機能検査の充実化」に適切な対策について記載する。</p>	<p>TCAの考え方及び資料安作24-3の議論を踏まえ、検討することとしたい。</p>	
(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。	◎	◎	-	-				
(5)品質・機能検査の充実化	(追加)								
						<p>○設備導入時の重要なハードウェアの品質評価のガイドラインの制定や、当該ガイドライン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、新たに基準化することが適当である。</p> <p>△根拠資料に挙げられている、機器導入時の品質検証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、解説に記載することが適当である。</p> <p>○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。</p> <p>△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》</p>	<p>○設備導入時の重要なハードウェアの品質評価のガイドラインの制定や、当該ガイドライン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、新たに基準化することが適当である。</p> <p>△根拠資料に挙げられている、機器導入時の品質検証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、解説に記載することが適当である。</p> <p>○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。</p> <p>△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》</p>	<p>【NTTドコモ】 事業者間で統一的な品質評価ガイドラインの制定はその内容が具体的・詳細であると、方式や装置や要求品質が各社で異なるため遵守が困難であると考えます。各事業者が遵守でき、かつ、効果がある基準とその表記内容については、各事業者に検討を委ねるのが良いと考えます。引き続き事業者間で議論を深めたいと考えます。</p> <p>【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【イー・アクセス】 「ハードウェアの品質評価ガイドライン」は通信事業者にとって一般的なものでないと考えられ、また記載内容についても開示等されているわけでもないことから、そのまま基準化するのではなく、解説における一部事業者間の取組み事例程度に留めておくことが適当と考えます。</p> <p>【TCA】 装置それぞれで求める信頼性や動作が異なるため、統一的なガイドラインの制定は困難であり、基準・解説への追加は不要と考えるが、具体的</p>	<p>一の事業者の取組であっても安全・信頼性対策に資する取組については、基準化を進めていくことが重要と考えているところ。</p> <p>本項目は、以下の2つの観点を踏まえて、導入判定の統一基準の策定と、基準に基づいた品質の検証の基準化を定める方針である。</p> <p>①すべてのハードウェアではなく重要なハードウェアを想定したものであること。 ②業界横断的な統一を想定したガイドラインではなく、社内またはグループ内での統一を想定したものであること。</p>
	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。	◎	◎	◎	◎				

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)(案)

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。 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					実施指針		根拠資料		論点(方向性)	構成員の意見	統一意見
項目	対策	実施指針				資料名	内容	論点(方向性)	構成員の意見	統一意見	
		事業	その	自営	ユー						
	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。	◎	◎	ー	ー	ベストプラクティス (KDDI)	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。	<p>○最近の通信事故について、端末の挙動が要因として挙げられていることから、基準にその旨を追加することが適当である。 △ふくそう回避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、解説にその旨を追加することが適当である。</p> <p>P</p> <p>○新装置導入におけるバックアップ切替動作の結果の点検については、事故の未然防止に資するものと考えられることから、新たに基準化することが適当である。</p> <p>○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》</p>	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。	TCAの考え方及び資料安作24-3の議論を踏まえ、検討することとしたい。	
	(追加)					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フィ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。		【TCA】 「エ」項は現状のままとし、パーストラフィック対策としての「オ」項を新たに追加し、「想定を超えるパーストラフィックが発生した場合において、それによる影響を回避するために適切な処理を行うことで事故につながらないようにすること、及び過負荷試験等で事前に確認すること」を基準案として追加してはどうか。 実施指針は○。		
	(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。		○新装置導入におけるバックアップ切替動作の結果の点検については、事故の未然防止に資するものと考えられることから、新たに基準化することが適当である。	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。	TCAの考え方を踏まえ、検討することとしたい。
	(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プ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、商用網でのトラフィック変動に確実に対応するため、複数トラフィ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。		○パーストラフィックを要因とした通信障害が発生していることから、各装置の最大処理能力を超える負荷での試験を実施し、トラフィック変動に対応すること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、新たに基準化することが適当である。 △パーストラフィック対策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。	【TCA】 ・基準への追加については、以下の文案および実施指針としたい。 ＜基準案＞ 「バックアップ方式による信頼性を確保する新規装置導入にあたっては、事前にバックアップ切替動作の結果を点検すること」 ＜実施指針＞ ○:実施が望ましい	
2.ネットワーク施工管理	(1)体制の明確化	◎	◎	◎	◎	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)。	<p>P</p> <p>○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が、現行基準の想定では、ベンダー、事業者等の関係者間の連携には触れられているものの、社内の関係部門間との連携については触れられていないため、現行基準の施工管理体制の明確化に加えて、基準化することが適当である。</p> <p>○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》</p>	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。	TCAの考え方及び資料安作24-3の議論を踏まえ、検討することとしたい。	
	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。					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。		【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。		
	(追加)					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。		【イー・アクセス】 各社設備も異なり、それぞれの方法で、最大トラフィック時の対策を実施していることや、過負荷に備えたベンダーとの連携方法も各社まちまちである事を考慮すれば、過負荷試験の実施は、解説での一部事業者の取り組み事例として整理することが適当と考えます。		
										【TCA】 ＜基準案＞ 「想定を超えるパーストラフィックが発生した場合において、それによる影響を回避するために適切な処理を行うことで事故につながらないようにすること、及び過負荷試験等で事前に確認すること」 実施指針は、○。	
						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。		【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。	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が、現行基準の想定では、ベンダー、事業者等の関係者間の連携には触れられているものの、社内の関係部門間との連携については触れられていないため、基準への追加が必要と考えているところ。 具体的には、ネットワーク施工管理における「関連部門間の連携」の主旨を明記する方針(1.(1)、3.(1)、4.(1)も同様に修正することを想定)である。 TCAの指摘のとおり、「(1)体制の明確化」に含まれる内容と判断される場合は、現行基準の改正も考えられる。	
						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。		【TCA】 ネットワーク施工管理体制の明確化については、「(1)体制の明確化」に含まれていることから、追加は不要と考えるが、具体的にどのように基準に追加したいのかが方針が知りたい。		

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)(案)

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					実施指針		根拠資料		論点(方向性) (○…基準への反映 △…解説への反映)	構成員の意見	統一意見
項目	対策	事業	その	自営	ユー	資料名	内容				
(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。	△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。		(6)を参照。	
						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。	△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。	◎	◎	◎	◎						
	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。	◎	◎	◎	◎						
(6)導入時の対応等(追加)						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。	◎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、基準にその旨を追加することが必要ではないか。	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。	TCAの考え方を踏まえ、(2)作業工程の明確化の解説に追加することで、検討することとしたい。	
						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。		【TCA】 状況によって「利用者の少ないエリア・時間帯」に先行導入することが効果的とは限らないため、基準ではなく解説への追記としたい。 「(2)作業工程」の項目と冗長なため、「(2)作業工程」の解説に以下の文言で追加することとしたい。 <解説案> 大規模障害のおそれのある作業実施時には、障害発生時の影響を最小化するため、工事作業実施時には予めその作業手順を関連部門間相互の確認、また、障害発生時の影響エリア、復旧手順を明らかにし、復旧に掛かる時間を想定した上で慎重に作業にとりかかること。		
						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。	◎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、基準にその旨を追加することが必要ではないか。	【TCA】 「(2)作業工程」の項目と冗長なため、「(2)作業工程」の解説に以下の文言で追加することとしたい。 <解説案> 大規模障害の恐れのある作業実施時には、障害発生時の影響を最小化するため、工事作業実施時には予めその作業手順を関連部門間相互の確認、また、障害発生時の影響エリア、復旧手順を明らかにし、復旧に掛かる時間を想定した上で慎重に作業にとりかかること。	TCAの考え方を踏まえ、(2)作業工程の明確化の解説に追加することで、検討することとしたい。	
						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.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。	◎	◎	◎	◎						

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)(案)

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)	構成員の意見	統一意見
項目	対策	実施指針				資料名	内容			
		事業	その	自営	ユー					
	(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。		○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が、現行基準の想定では、ベンダー、事業者等の関係者間の連携には触れられているものの、社内の関係部門間との連携については触れられていないため、現行基準の保全・運用管理体制の明確化に加えて、基準化することが適当である。	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。	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が、現行基準の想定では、ベンダー、事業者等の関係者間の連携には触れられているものの、社内の関係部門間との連携については触れられていないため、基準への追加が必要と考えているところ。 具体的には、ネットワーク保全・運用管理における「関連部門間の連携」の主旨を明記する方針(1.(1)、2.(1)、4.(1)も同様に修正することを想定)である。 TCAの指摘のとおり、「(1)体制の明確化」に含まれる内容と判断される場合は、現行基準の改正も考えられる。
(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。		○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 (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。		△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) 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。				
	(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。		○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、基準に追加することが必要ではないか。 △その他具体例について、解説への記載を検討。	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。	障害発生時の復旧手順については、既に解説書にも触れられていることから「(3)作業の手順化」の解説への記載を行うことで、検討することとした。
						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。			【TCA】 ・基準案への追加については、想定することが難しい障害もあり、複合要因など全ての問題をクリアすることは困難である。そのため、技術的課題を踏まえて検討をお願いしたい。	
(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、予備設備への切替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。	◎*	◎*	◎*	◎*					

【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					実施指針		根拠資料		論点(方向性) (○…基準への反映 △…解説への反映)	構成員の意見	統一意見
項目	対策	事業	その	自営	ユー	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った場合において、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った場合は、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。	○省令に災害時優先通信及び他の通信の疎通状況を記録すること及びその記録を分析する旨が新たに規定されたことから、基準に省令改正された内容を追加することが適当である。 ○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)	【ソフトバンクモバイル・テレコム】 解説やガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 手段や条件等を限定しないよう、基準へ省令の内容をそのまま反映させることとしたい。 省令上は義務であるため、実施指針は◎。 <基準案> 「災害時優先通信の優先的な取り扱いを確保するために他の通信の制限又は停止を行った場合において、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こと。」	TCAの考え方を踏まえ、検討することとしたい。	
(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。	◎	-	-	-						
	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慮する場合は、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フィ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。	△商用網のトラフィ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。	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えるので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 以下の記載としたい。 <解説案> 保守作業後の検取試験において、やむを得ず実データを使用する場合は、通信の秘密の保護及びデータの保護に十分に配慮する。 実データの使用は、データによっては通信の秘密の漏えい、またデータの棄損及び滅失に繋がる可能性が高く、更に異常処理に対する検証が十分に行い得ないこともあり、検取試験においては、想定される商用網のトラフィックパターン等を考慮すること。	TCAの考え方を踏まえ、検討することとしたい。	
(8)情報の収集	部外工事に係る情報や企画型ふくそ原因となる情報等、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。	◎	○	○	○						
	(追加)					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。	○「ヒヤリハット事例の収集」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、基準にその旨を追加することが必要ではないか。	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えるので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 ヒヤリハット事例の収集については品質管理の手法の一つであるため、「別表第2 管理基準 11現状の調査・分析及び改善(4)改善」へ解説にて記載することとしたい。 <解説案> 「自社で発生した「ヒヤリハット事例」を蓄積して事故予防に資することが重要」	TCAの考え方を踏まえ、検討することとしたい。	

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)(案)

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。 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					根拠資料		論点(方向性) ○…基準への反映 △…解説への反映	構成員の意見	統一意見	
項目	対策	実施指針				資料名				内容
		事業	その	自営	ユー					
(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。	◎	◎	ー	ー			<p>○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」に移動(又は再掲)させることが適当である。</p> <p>○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、必要に応じて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。</p> <p>《本文2.6参照》</p>	<p>【ソフトバンクモバイル・テレコム】 ・ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 ・文言削減には異議ございません。</p> <p>【TCA】 ・12(3)項への移動については異論なし。 ・「必要に応じて」を外すことについては、目ごろからHP等で啓発することで条件を満たすものであれば問題無い。しかし、小さい輻輳でも正月のように必ず協力依頼すべきということになるのであれば外さないことしたい。</p>	<p>個々の事業者としては、目頃からHPで利用者への情報提供を行っていただければ、利用者への協力依頼・周知のための措置は講じられているものと考えます。</p>
	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。	◎	◎	ー	ー					
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)					<p>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。</p> <p>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。</p>	<p>○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が、現行基準の想定では、ベンダー、事業者等の関係者間の連携には触れられているものの、社内の関係部門間との連携については触れられていないため、現行基準の作業の分担、連絡体系、責任の範囲等の管理体制の明確化に加えて、関係部門間の連携も重要であることから、基準にその旨を追加することが適当である。</p> <p>○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》</p>	<p>【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【イー・アクセス】 ・事業者規模や成り立ち等により、必ずしも全ての事業者が部門細分化されているわけではないことから、広く電気通信事業者等に適用される基準ではなく解説における、一部事業者での事例として整理することが適当な内容と考えます。</p> <p>【TCA】 設備の更改・移転管理体制の明確化については、「(1)体制の明確化」に含まれていることから、追加は不要と考えるが、具体的にどのように基準に追加したいのか方針が知りたい。</p>	<p>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が、現行基準の想定では、ベンダー、事業者等の関係者間の連携には触れられているものの、社内の関係部門間との連携については触れられていないため、基準への追加が必要と考えているところ。 具体的には、設備の更改・移転管理における「関連部門間の連携」の主旨を明記する方針(2.(1)、3.(1)、4.(1)も同様に修正することを想定)である。 TCAの指摘のとおり、「(1)体制の明確化」に含まれる内容と判断される場合は、現行基準の改正も考えられる。</p>	
(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。	◎	◎	◎*	◎*	<p>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。</p> <p>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。</p>	<p>△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。</p>		<p>下記(3)を参照</p>	
(3)設備の更改(追加)						<p>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。</p> <p>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。</p>	<p>○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、基準にその旨を追加することが必要ではないか。</p>	<p>【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【TCA】 「(2)作業工程の明確化等」の項目と冗長なため、「(2)作業工程の明確化等」の解説に以下の文言で追加することとしたい。 ＜解説案＞ 新規設備、ソフトウェアの導入にあたっては、不具合発生時のお客様影響の極小化を考慮し、先行導入エリア、時間帯を検討することが重要。</p>	<p>TCAの考え方を踏まえ、検討することとしたい。</p>	
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。	◎	◎	◎	◎					

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)(案)

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	構成員の意見	統一意見	
項目	対策	実施指針				資料名				内容
		事業	その	自営	ユー					
	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。	○	○	○	○					
(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)空調調和設備の保全	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、復旧に必要な業務委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。	△社内で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。	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 下記下線部の追加をすることとしたい。 (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。 解説 ※変更せず ●例● 次のような内容を含んだ災害対策規定を作成し、組織・体制を予め定めておく。 1 災害予防と事前措置 2 災害応急対策 (1)災害情報 (2)準備警戒 (3)通信設備に対する応急措置 (4)通信疎通に対する応急措置 (5)社内及び協力会社等との情報共有、要員措置および応急対策用資材 (6)避難及び救護 3 災害復旧 4 地震防災応急対策 5 防災に関する組織 (1)災害対策総本部 (2)災害対策本部 (3)災害対策部 (4)災害対策連絡室	TCAの考え方を踏まえ、検討することとしたい。
	ウ 非常事態時における広域応援体制を明確にすること。	○	○	○	○			△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。	【イー・アクセス】 本内容は作業班で未議論と考えます。基準化にあたっては、東日本大震災にて各社とも臨機応変に応援体制を組んだ実態や、応援体制を予め固定化することが、災害時の機動性をかえって失わせることはないかどうかをふまえ、要否も含め慎重な検討が必要であると考えます。 【TCA】 ももとの災害時の体制が異なるため、一例としての事例を記載してもすべての事業者に適用できるわけではないため、解説への記載はしないこととしたい。	災害対策の迅速化を図るため、既に事例のような体制を確立している事業者もあることから、取組の一例として紹介していきたいと考えている。 なお、安全・信頼性の向上に資する取組であれば、一事業者の取り組みであっても紹介していくことが重要と考える。
	エ 相互接続を行う事業者等において、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)(案)

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					実施指針		根拠資料		論点(方向性) (○…基準への反映 △…解説への反映)	構成員の意見	統一意見
項目	対策	事業	その	自営	ユー	資料名	内容				
	(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。	○根拠資料に挙げられている、災害対応体制の検証・見直しについては、災害時における迅速・適確な対応に資することから、新たに基準化することが適当である。 ○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)	【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定することを要望いたします。	最近の傾向として、見直し規定を設けることは一般的であるため、基準への追加を検討する。	
	(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)PDCAサイクル(追加)					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。	○PDCAサイクルを導入することは、継続的な業務改善活動を担保するものであり、ネットワークの適正な維持・運用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必要ではないか。 △「ヒヤリ・ハット事例の収集」に関する取組みについては、PDCAサイクルに関するものであることから、解説への記載を検討(3.-(2))において基準への追加を検討。	【ソフトバンクモバイル・テレコム】 ベストプラクティスを根拠とした見直しにおいては、議論が尽くされていないと考えますので、ガイドライン化においてはTCA等で議論を尽くした後の策定することを要望いたします。	TCAの考え方を踏まえ、検討することとしたい。 具体的には(11)4改善において、反映していくこととしたい。	
	(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。	△「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。	【TCA】 ＜解説案＞ 「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サイクルや自社で発生した「ヒヤリ・ハット事例」を蓄積し、事故予防に資するものと考えられる」と記載することとしたい。	TCAの考え方を踏まえ、検討することとしたい。
						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。				
		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							○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」の変更が適当である。 (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)(案)

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)	構成員の意見	統一意見	
項目	対策	実施指針				資料名				内容
		事業	その	自営	ユー					
(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。	◎	◎	-	-			<p>○IPネットワーク設備委員会の提言を踏まえ、より具体的な安全・信頼性の確保に向けた事業者の取組を公開していくことが適当である。</p> <p>○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。</p> <p>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》</p>	<p>【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【TCA】 社会的に影響が大きい故障については自社の判断で記者会見を実施してきており、現在の規程で十分と考える。</p>	<p>ご意見は、電気通信事故発生時の情報公開についてのものであるが、事務局からの提案は、日頃からの事業者の取り組みを公開していくことの重要性を示しているものである点をご理解いただきたい。</p>
(追加)						<p>IPネットワーク設備委員会報告</p> <p>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。</p>	<p>○根拠資料に挙げられている、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については、利用者にとって適切な災害対策を講じる上で有効と考えられることから、新たに基準化することが適当である。</p> <p>△詳細は解説に記載することが適当である。</p> <p>《本文2.2.2.4.1参照》</p>	<p>【NTTドコモ】 作業班においては各事業者がそれぞれの立場で見解を述べた状況であり、十分な議論が尽くされていないと考えます。具体的にどのようなレベルの内容とし、どのような表記とするか、TCA等において内容精査を含め継続議論し、事業者側から案を提示させていただきたいと考えます。</p> <p>【ソフトバンクモバイル・テレコム】 本作業班において、「利用者にとって有効な情報の公開となることが目的であり、混乱や過度な期待を持たせる情報の公開とならないような情報の公開を目指していくこと」が確認できたことから、「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については、利用者にとって適切な災害対策を講じる上で有効と考えられることから」を「災害対策については、利用者にとって混乱や過度な期待を持たせない範囲における有効な情報を公開することについて」等の表記に変更頂き、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【イー・アクセス】 ・本内容については、IPネットワーク設備委員会報告での「利用者等にとって参考となる情報を適切な形で」の公開をベースに今回本作業班で議論した結果、下記が構成員のおおまかな共通認識になっているものと考えます。 -利用者にとって参考となる情報の分別が必要なこと。 -応急復旧機材についての具体的な配備状況や配備場所の公表について、設備防犯上の考慮が必要であること。 -情報公開は、公表以外の方法(個別開示等)もあり得ること。 ・上記をふまえ、本基準の論点案は下線部を追記いただくことが必要であると考えます。 「根拠資料に挙げられている、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については、利用者にとって参考となり、かつ適切な形であれば利用者にとって適切な災害対策を講じる上で有効と考えられることから、基準に追加することが必要ではないか。」</p> <p>【ウィルコム】 公表のレベルについては各事業者に任せる形が適当と考えます。当社としては「各市区町村役場付近」という形で公表することとしたい。</p> <p>【TCA】 上欄の内容に含まれる内容であり、また、停電対策とその結果の公開に係る対応に含まれていることから、不要と考える。</p>	<p>TCAの考え方を踏まえ、上記基準に公開内容を反映する見直しを行うか、又は上記基準の解説として公開内容を記載するかを、検討することとしたい。</p>	

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)(案)

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	構成員の意見	統一意見
項目	対策	実施指針		資料名	内容			
		事業	その			自営	ユー	
	(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。	○△上記と同趣旨。	<p>【NTTドコモ】 作業班においては各事業者がそれぞれの立場で見解を述べた状況であり、十分な議論が尽くされていないと考えます。具体的にどのようなレベルの内容とし、どのような表記とするか、TCA等において内容精査を含め継続議論し、事業者側から案を提示させていただきたいと考えます。</p> <p>【ソフトバンクモバイル・テレコム】 本作業班において、「利用者にとって有効な情報の公開となること」が目的であり、混乱や過度な期待を持たせる情報の公開とならないような情報の公開を目指していくことが確認できたことから、「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については、利用者にとって適切な災害対策を講じる上で有効と考えられることから」を「災害対策については、利用者にとって混乱や過度な期待を持たせない範囲における有効な情報を公開することについて」等の表記に変更頂き、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【イー・アクセス】 ・本内容については、IPネットワーク設備委員会報告での「利用者等にとって参考となる情報を適切な形で」の公開をベースに今回本作業班で議論した結果、下記が構成員のおおまかな共通認識になっているものと考えます。 -利用者にとって参考となる情報の分別が必要なこと。 -応急復旧機材についての具体的な配備状況や配備場所の公表について、設備防犯上の考慮が必要であること。 -情報公開は、公表以外の方法(個別開示等)もあり得ること。 ・上記をふまえ、本基準の論点案は下線部を追記いただくことが必要であると考えます。 「根拠資料に挙げられている、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については、利用者にとって参考となり、かつ適切な形であれば利用者にとって適切な災害対策を講じる上で有効と考えられることから、基準に追加することが必要ではないか。」</p> <p>【ウィルコム】 公表のレベルについては各事業者に任せる形が適当と考えます。当社としては「各市区町村役場付近」という形で公表することとしたい。</p> <p>【TCA】 上欄の内容に含まれる内容であり、また、停電対策とその結果の公開に係る対応に含まれていることから、不要と考える。</p>	同上

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)(案)

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	構成員の意見	統一意見
項目	対策	実施指針			資料名	内容			
		事業	その	自営			ユー		
	(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。	○△上記と同趣旨。	<p>【NTTドコモ】 作業班においては各事業者がそれぞれの立場で見解を述べた状況であり、十分な議論が尽くされていないと考えます。具体的にどのようなレベルの内容とし、どのような表記とするか、TCA等において内容精査を含め継続議論し、事業者側から案を提示させていただきたいと考えます。</p> <p>【KDDI】 →項目を分け、実施指針については○とする。 理由:災害時において発生する輻輳は、例えば地震における震度や被害内容等により大きく異なるため、設計容量に関する考え方の如何に関わらず、発生する問題です。そのため、設計容量を公開していたとしても、災害対策を講じる上で有効であるとはいえないため、現時点では、「実施が望ましい」とすることが適当と考えます。</p> <p>【ソフトバンクモバイル・テレコム】 本作業班において、「利用者にとって有効な情報の公開となることが目的であり、混乱や過度な期待を持たせる情報の公開とならないような情報の公開を目指していくこと」が確認できたことから、「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については、利用者にとって適切な災害対策を講じる上で有効と考えられることから」を「災害対策については、利用者にとって混乱や過度な期待を持たせない範囲における有効な情報を公開することについて」等の表記に変更頂き、ガイドライン化においてはTCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【イー・アクセス】 ・本内容については、IPネットワーク設備委員会報告での「利用者等にとって参考となる情報を適切な形で」の公開をベースに今回本作業班で議論した結果、下記が構成員のおおまかな共通認識になっているものと考えます。 -利用者にとって参考となる情報の分別が必要なこと。 -応急復旧機材についての具体的な配備状況や配備場所の公表について、設備防犯上の考慮が必要であること。 -情報公開は、公表以外の方法(個別開示等)もあり得ること。 ・上記をふまえ、本基準の論点案は下線部を追記いただくことが必要であるとされます。 「根拠資料に挙げられている、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については、利用者にとって参考となり、かつ適切な形であれば利用者にとって適切な災害対策を講じる上で有効と考えられることから、基準に追加することが必要ではないか。」</p> <p>【ウィルコム】 災害時等は輻輳が発生してしまうものであるという点を含め、基本的考え方のみを公表することが望ましいと考えます。</p> <p>【TCA】 設計容量は今後の議論であり、現時点での記載はしないこととしたい。</p>	ご意見を踏まえ、上記基準に公開内容を反映する見直しを行うか、又は上記基準の解説として公開内容を記載するかを、検討することとしたい。 なお、設計容量、重要通信の優先的取扱いについては、総務省と電気通信事業者で引き続き議論していくこととしたい。
(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。	◎	◎	-	-	<p>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)」を发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。</p> <p>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。</p> <p>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。</p>	<p>○現行基準では公開のタイミングに関する考え方が示されていないが、通信障害の状況を「速やかに」利用者へ情報提供することは利用者保護に資すること。また、ベストプラクティスとして「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」との取組みが実際に実施されていることから、基準に公表のタイミングに関する考え方を反映することが適当である。 ○「公開」より積極的ニュアンスのある「公表」が表現として適当ではないか。 △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。</p> <p>○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)</p>	<p>【ソフトバンクモバイル・テレコム】 「電気通信サービスにおける事故及び障害発生時の周知・情報提供の方法等に関するガイドライン」 (http://www.teleso.or.jp/consortium/serviceimprove/20100203_press.html)が既にあることから、反映させることは不要で、当該ガイドラインを検討のうえ必要に応じて修正することを要望いたします。</p> <p>【TCA】 ・「電気通信サービスにおける事故及び障害発生時の周知・情報提供の方法等に関するガイドライン」が別途定められていることから、基準については「すみやかに利用者に対して公開」を追加することに留めるものとする。 ＜基準案＞ 「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、すみやかに利用者に対して公開すること」 ＜解説案＞ 情報通信ネットワークのふくそう状況及び通信規制の状況を勘案し、適切な方法により、すみやかに利用者に対して公開すること。</p>	TCAの考え方を踏まえ、検討していくこととしたい。

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)(案)

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					実施指針		根拠資料		論点(方向性) (○…基準への反映 △…解説への反映)	構成員の意見	統一意見
項目	対策	事業	その	自営	ユー	資料名	内容				
	(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。	<p>○根拠資料に挙げられている、ふくそう状況及び通信規制の実施状況の公表については、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、新たに基準化することが適当である。</p> <p>○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》</p>	<p>【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【TCA】 上欄の内容に含まれる内容であり基準への追加はしないこととした。もし「ふくそう状況及び通信規制の実施状況の公表」に関する取り組みを明記される際は、解説として記載されることが適当と考えます。</p>	<p>ご意見を踏まえ、上記基準に公開内容を反映する見直しを行うか、又は上記基準の解説として公開内容を記載するかを、検討することとした。</p>	
(3)サービス提供不可に陥るケース等の周知								<p>○項目名について、平時からの周知についても考慮すると、項目名の変更が適当である。 《本文2.6参照》</p>			
	情報通信ネットワークにおいて、従来サービスとの違いを広く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。	◎	◎	-	-			<p>○「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》</p>			
	(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呼びかけること。	<p>○IPネットワーク設備委員会の提言を踏まえ、手短な通信、災害伝言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、新たに基準化することが適当である。</p> <p>○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。</p> <p>○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》</p>	<p>【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【TCA】 3(9)A項に記載があり冗長のため、基準への追記はしないこととした。</p>	<p>災害用音声お届けサービスを含めた災害用伝言サービスの利用促進を図るよう、事業者の取組みを期待するものから基準化を考えているものである。</p>	
	(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ずること。	◎	◎	-	-			<p>「第1 設備基準 1一般基準 (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があるため、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》</p>			

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)(案)

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	構成員の意見	統一意見
項目	対策	実施指針			資料名	内容			
		事業	その	自営			ユー		
(4)情報セキュリティに関する取組(追加・再掲)							<p>○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。</p> <p>○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。</p> <p>《本文2.6参照》</p>	<p>【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。</p>	9月に議論を行う情報セキュリティの項目と併せて議論したい。
							<p>○「5.情報セキュリティ管理(4)コンピュータウイ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」(3)に再掲することが適当である。</p> <p>《本文2.6参照》</p>	<p>【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。</p>	同上
							<p>○「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」(3)に再掲することが適当である。</p> <p>《本文2.6参照》</p>	<p>【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。</p> <p>【JAIPA】 情報ネットワークの不正利用を防止するための通信事業者の具体的な取組(法令違反、迷惑行為への対応等)について周知することを基準または解説に記載することを要望いたします。</p>	同上
(5)電気通信サービスの不正利用の防止に関する周知(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。	○	-	-	-		<p>○別表第1 第1 1 (7)電子メールによる一方的な広告・宣伝等への対策 より移行。</p> <p>○移行により、現行基準の内容を周知するための基準に変更することが適当である。</p> <p>○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。</p> <p>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。</p> <p>また、インターネット上での利用者保護、不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。</p> <p>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。</p> <p>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。</p> <p>更に、これらの不正利用に係る分類は、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。</p> <p>《本文2.4参照》</p>		別表第1 第1 1 (7)電子メールによる一方的な広告・宣伝等への対策 より移行。

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)(案)

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)	構成員の意見	統一意見	
項目	対策	実施指針		資料名				内容
		事業	その	自営	ユー			
	(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端末の利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。	○「青少年有害情報フィルタリングサービス」の機能について、周知する内容を基準化することが適当である。 《本文2.4参照》	【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 本根拠資料は、本基準における「設備や設備管理における安全・信頼性」や「情報セキュリティポリシーや危機管理計画の策定にあたって配慮すべき事項」いずれでもないため、検討にそぐわないものとする。	同上
	(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。	○児童ポルノに関するインターネット上の情報の切断に関する取組みが各電気通信事業者において行われていることから、その旨を周知する内容を基準化することが適当である。 《本文2.4参照》	【ソフトバンクモバイル・テレコム】 ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【JAIPA】 根拠資料として、以下を追加することを提案します。 [資料]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 [内容]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ことあり、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、ISPIによる閲覧防止措置(ブロッキング)を講ずる必要がある。 【TCA】 本根拠資料は、本基準における「設備や設備管理における安全・信頼性」や「情報セキュリティポリシーや危機管理計画の策定にあたって配慮すべき事項」いずれでもないため、検討にそぐわないものとする。	同上
(6)事業者間の情報共有(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	○業界全体で、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(いわゆるベストプラクティス)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から、基準に追加することが適当である。 △情報共有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。 ○現行基準には、電気通信事業者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から、基準に追加することが適当である。 《本文2.3.6参照》	【ソフトバンクモバイル・テレコム】 事業者共通の事例であれば共有することは可能と考えますが、ガイドライン化において手段や条件等について明記する場合は、TCA等で議論を尽くした後の策定とすることを要望いたします。 【TCA】 ・基準については、既に「携帯電話通信障害対策連絡会」が存在することから、追加はしないこととする。 ・解説については、NW構成やその運用方法が各社により異なることから、具体的な記載が必ずしも有効では無いため、追加はしないこととする。	情報共有の取組に関しては、現行基準に反映すべき事項であると考えている。
				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。			

「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	その	自営	ユー		
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。	◎	◎	二	二		

「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	その	自営	ユー		
	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。	◎	◎	二	二		
	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都合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。	◎	◎	◎	◎		

「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	その	自営	ユー		
	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

「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	その	自営	ユー		
	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 定期的な、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 コンピュータウイ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
	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。	◎*	◎*	◎*	◎*	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

「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	その	自営	ユー		
	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

「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	その	自営	ユー		
	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】 ○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
	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。	○	○	○	○	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
	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。	○	○	○	○		

「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	その	自営	ユー		
	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。	◎	◎	◎*	◎*		

「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	その	自営	ユー		
(3)入出制限機能	ウ 床荷重に対し、所要の構造耐力を確保すること。	◎	◎	◎	◎		
	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。	◎	◎	◎*	◎*		

「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	その	自営	ユー		
(2)通信機械室内の設備等の設置	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。	◎	◎	◎	◎		
	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。	◎*	◎*	◎*	◎*		
	キ 出入口には、施錠機能を設けること。	◎	◎	◎	◎		
(4)入出制限機能	ア 出入口には、施錠機能を設けること。	◎	◎	◎	◎		

「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	その	自営	ユー		
	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。	◎	◎	◎	◎		
(5)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。	◎	◎	◎*	◎*		
(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。	◎	◎	◎	◎		

「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	その	自営	ユー		
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。

「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

別表第2 管理基準

【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。

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	その	自営	ユー		
(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)コンピュータウイ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 コンピュータウイ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

「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

別表第2 管理基準

【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。

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	その	自営	ユー		
(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 組織に対するの価値、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。	◎	◎	◎	◎		

「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

別表第2 管理基準

【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。

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	その	自営	ユー		
(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	<p>(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。</p> <ul style="list-style-type: none"> ○情報の作成と入手 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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

別表第2 管理基準

【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。

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	その	自営	ユー		
							<ul style="list-style-type: none"> ○情報の提供 <ul style="list-style-type: none"> ・提供に関する許可及び届出 ・付加情報の削除 ○情報の消去 <ul style="list-style-type: none"> ・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) <p>(1)ウ(ア)情報セキュリティ確保のために求められる機能</p> <ul style="list-style-type: none"> ○権限管理 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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	<p>(1)イ(ア)情報の格付け【要検討事項】</p> <p>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。</p> <ul style="list-style-type: none"> ○重要性に応じた適切な措置 <ul style="list-style-type: none"> ・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

「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

別表第2 管理基準

【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。

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	その	自営	ユー		
						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。	○	○	○	○		

「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	その	自営	ユー		
(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	<p>(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</p> <p>(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)</p>

「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

別表第2 管理基準

【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。

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	その	自営	ユー		
							<ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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 <ul style="list-style-type: none"> ・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)

「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

別表第2 管理基準

【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。

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	その	自営	ユー		
						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。	◎	◎	◎	◎		

「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

別表第2 管理基準

【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。

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	その	自営	ユー		
	イ 非常事態における社員・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】 ○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】 ○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】 ○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			
<p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p>			
(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】 ○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 ・情報資産の洗い出し方法(体制、洗い出し項目、洗い出し基準)、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】 ○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】 ○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和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	<p>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。</p> <p>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。</p>		
		ウ アクセス制御	<p>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。</p>		

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、コンピュータウイ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 コンピュータウイルス	強力な感染力と破壊力を持つウイルスによる攻撃		

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っ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する。			
(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、コンピュータウイルス		
(オ) ネットワークの機器	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、コンピュータウイルス対策等を規定し、サイバーテロに対する予防措置を講ずる。			
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」策定にあつての指針 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要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。		
イ ソフトウェア上の対策	(カ) 攻撃元を特定できる機能と攻撃元のトラフィックを遮断する仕組み等を採用		
	(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) コンピュータウイ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】 ○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】 ○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	他の利用者へ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離する。 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		資料名	内容
	<p>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。</p> <p>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。</p>		
	<p>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。</p>	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】 ○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
	<p>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。</p>		
(4) 原因判明時の措置	<p>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。</p>		
	<p>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。</p>		
	<p>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。</p>		
	<p>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。</p>		
(5) 危機管理計画の見直し等	<p>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。</p>	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】 ○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
	<p>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。</p>	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

「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 (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。
	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出た。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 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。
		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 <input type="checkbox"/> OSやサーバーソフトウェアの定期的な脆弱性診断 <input type="checkbox"/> OSやサーバーソフトウェアに関する脆弱性	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。

<p>情報の時期を逸しない収集と修正プログラムの適用</p> <p><input type="checkbox"/>ウェブアプリケーションへの脆弱性の作り込みの回避</p> <p>・ウェブアプリケーションファイアウォール(WAF)</p>	<p>別表第1 設備等基準</p> <p>第1 設備基準</p> <p>1 一般基準</p> <p>(11)情報セキュリティ対策</p>	<p>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。</p>
	<p>別表第2</p> <p>5 情報セキュリティ管理</p> <p>(5)情報セキュリティに関する情報収集</p>	<p>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。</p>
<p>3) 標的型攻撃ルートでの対策</p> <p>・スパムフィルタ</p> <p><input type="checkbox"/>URIフィルタ</p> <p><input type="checkbox"/>外部メディア利用規則、強制利用抑止</p>	<p>別表第1 設備等基準</p> <p>第1 設備基準</p> <p>1 一般基準</p> <p>(11)情報セキュリティ対策</p>	<p>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</p> <p>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。</p> <p>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。</p>
	<p>別表第2</p> <p>3 ネットワーク保全・運用管理</p> <p>(4) 監視、保守及び制御</p>	<p>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。</p>
<p>4) ウイルス活動の阻害および抑止</p> <p>(出口対策)</p> <p>・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)</p> <p><input type="checkbox"/>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</p> <p>・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)</p>	<p>別表第1 設備等基準</p> <p>第1 設備基準</p> <p>1 一般基準</p> <p>(11)情報セキュリティ対策</p>	<p>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。</p> <p>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。</p> <p>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。</p>

<input type="checkbox"/> 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		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 <input type="checkbox"/> ユーザ認証 <input type="checkbox"/> 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 <input type="checkbox"/> 通信路の暗号化(Virtual Private Networkなどの利用) <input type="checkbox"/> ファイルの暗号化 <input type="checkbox"/> 暗号鍵管理	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	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。
	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 <input type="checkbox"/> ネットワークログ取得・分析 <input type="checkbox"/> サーバログ取得・分析 <input type="checkbox"/> 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) <input type="checkbox"/> セキュリティポリシーの徹底 <input type="checkbox"/> 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 <input type="checkbox"/> 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。