情報通信ネットワーク
安全・信頼性基準
解説

設備等基準の対策項目

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。

解説

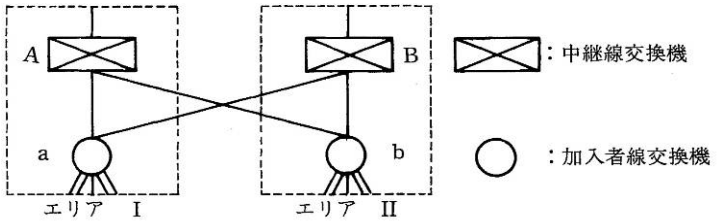
通信を安定的に提供し、災害等の発生時において、疎通の全面的停止を防止するため、通信の取扱いの地理的範囲やネットワーク全体のバランス等を考慮しながら、重要な通信センターを地域的に分散して設置する。

「通信センター」とは、情報通信ネットワークにおける交換機能、通信処理機能、又は情報処理機能を有するセンターをいう。

●措置例●

交換機（呼制御サーバを含む）の分散設置

災害時における交換機能停止時においてもある程度の通信サービスを確保するため、交換機を信頼性の得られる遠隔地に分散する。



交換機の分散設置

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。

解説

重要な通信センターの障害等に対処するため、重要な通信センターを他の通信センターでバックアップ可能な代替機能をもつようにする。

単一の通信センターのみで構成されるネットワークの場合でも、バックアップ機能を設けることが望ましい。

●措置例●

１　同様な機能を持つ中継交換設備等を分散して設置した場合は、処理能力に余裕のある設計とし、実質的な処理量の増加に対処できる構成とする。

２　他のセンター設備のバックアップを行う場合、ファイルの一致が必要なものについては、メンテナンスによるファイルの一致やミラーファイル等の手段の確保を行う。

３　単一の通信センターのみの場合は、他の事業者によるバックアップなどの手段の確保を行う。

(2)　代替接続系統の設定

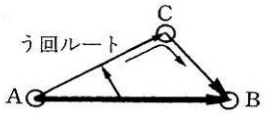
交換網の場合は、二つの重要な通信センター間を結ぶ接続系統の障害に対し、その代替となる他の通信センター経由のう回接続系統を設けること。

解説

交換網において、伝送路設備（伝送設備及び線路設備）や交換設備の障害時に通信の停止を防止するため、う回接続系統（う回ルート）を設ける。う回接続系統の適用としては、う回付与及びう回路変更の機能拡大がある。

１　う回付与

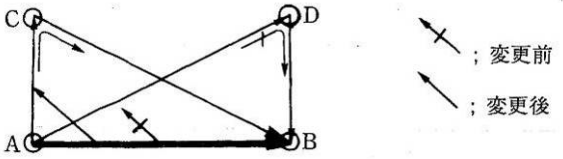
通信センター間回線を他の通信センター経由の回線にう回させる。



う回付与

２　う回路変更

他の通信センター経由の回線のあふれ先を全面的又は部分的に変更する。



う回路変更

(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。

解説

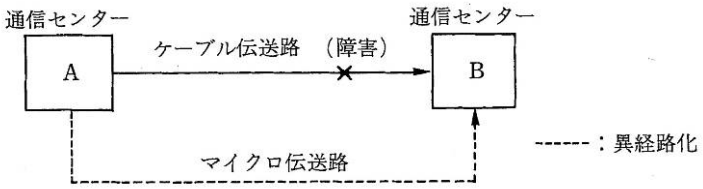
伝送路設備の障害に対処するため、疎通する通信量等を考慮し、重要な通信センター間を結ぶ伝送路設備については、複数の経路に設置する。

特に地震等の大規模災害に対しては異なる伝送媒体（例えば、マイクロ伝送路とケーブル伝送路）、異なる地理的経路（例えば、東海経由と北陸経由）による複数の経路が考えられる。

●措置例●

１　異なる伝送媒体による複数の経路

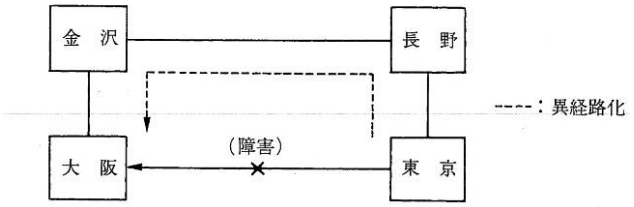
一つの伝送路が故障になった時でも、他の伝送路収容の回線により、通信サービスの一部が維持できるように対地間の伝送路を異なる伝送媒体により複数設置する。



異なる伝送媒体

２　異なる地理的経路による複数の経路

通信網としての信頼性を向上させるため、複数のう回経路を設け、１つの経路が障害になってもサービスに支障をきたさないように構成する。



異なる地理的経路

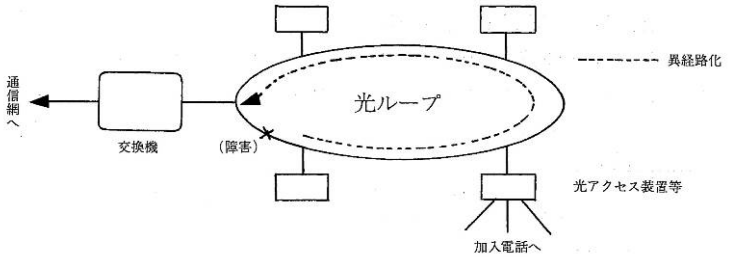
イ　重要な光加入者伝送路は、ループ化等による２ルート化を促進すること。

解説

都市部等の基幹的な光加入者伝送路は、加入者伝送路の障害に対処するため、ループ化等により２ルート化を図ることで、通信の確保を図る。

●措置例●

光加入者伝送路の光ケーブルを一定のエリア内でループ状に構築し、加入者網を形成することで、通信の信頼性確保を図る。



光加入者ケーブルのループ化

ウ　交換設備相互間を接続する伝送路設備は、複数の経路により設置すること。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。

解説

地理的に困難な場合等の一部例外を除き、交換設備相互間を接続する伝送路設備の複数経路化する。

なお、例外規定の「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」とは、具体的には、とう道への収容その他の災害に強い回線敷設等の措置であって、当該地域において伝送路設備を複数経路により設置した場合と同等以上の効果が得られるものを念頭においたものである。

エ　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、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の措置を講ずること。

解説

従来から、交換設備相互間を接続する伝送路設備については複数経路化によりその冗長性を確保することとしていたが、多くの電気通信事業者では、より経済的に冗長性を確保するため、ループ状の網構成を採用された。しかしながら、ループ状の網構成では、一箇所の被災によりループの全体について冗長性が失われてしまうことから、複数箇所の被災が想定される大規模災害では、ネットワークの機能が損なわれ、広域にわたり通信が停止することが危惧される。

このため、ループ状の網構成については、ループにより囲まれる地域を横断する伝送路設備の追加的な設置、臨時の電気通信回線の設置に必要な機材の配備その他

の必要な措置を講じる。

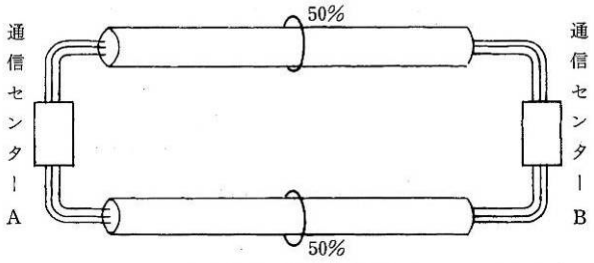
(4)　電気通信回線の分散収容
　　重要な通信センター間を結ぶ電気通信回線の収容は、異なる伝送路設備に分散して行うこと。

解説

伝送路等の障害に対処するため、重要な通信センター間を結ぶ電気通信回線（一つの伝送区間に設定された物理的な通信回路のことであり、例えば、光ファイバーケーブル内又は同軸ケーブル内の個々の心線、マイクロ無線において一対の送受信装置で構成されたシステムがこれに該当）の収容は異なる伝送路設備に分散して行う。

●措置例●

通信センター間を接続する伝送路設備（伝送設備及び線路設備）が複数で設定されている場合に、電気通信回線を分散して収容することにより、一の伝送路設備が故障となった場合でも､他の伝送路設備に収容されている電気通信回線によって通信センター間の通信の疎通を図る。



電気通信回線の分散収容例

(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場合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、その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。

解説

複数の電気通信事業者が共用する設備に限らず、当該設備の事故が全国的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、災害時も考慮し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するなどの対策が必要である。

(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
　　サーバ及びゲートウェイの設備は、通信量の増加を考慮した適切な容量のものを設置すること。

解説

スマートフォンの急激な普及により、一部の携帯電話事業者において、トラヒックの瞬間かつ急激な増加（バーストトラヒック）や制御信号の増加を一因とする電気通信事故等が多数発生した。

端末からの通信量の増加により、メールサーバやルータ等のゲートウェイの設備への負担が増加することから十分な設備容量を確保することが必要である。

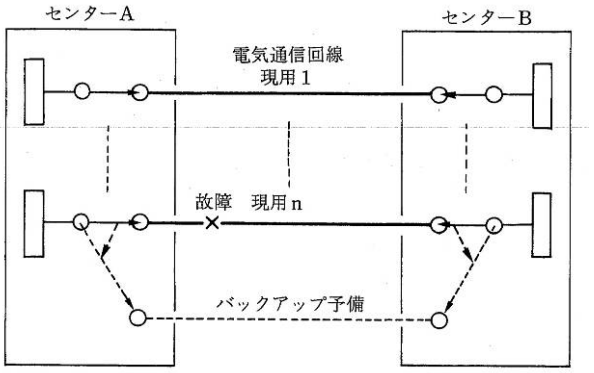
(7)　予備の電気通信回線の設定等

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。

解説

重要な伝送路設備（伝送設備及び線路設備）には、その故障発生時に疎通の停止を防止するため、他の疎通確保の手段が無い場合は、所要の予備の電気通信回線を設定する。

各事業者及びユーザは、対象となっている電気通信回線設備の信頼度と、必要とする信頼度の双方について考慮しつつ、必要にして十分な予備を確保することが大切である。



予備の電気通信回線

他の疎通確保の手段の例としては、「マイクロエントランス回線」や「衛星回線」等が挙げられる。

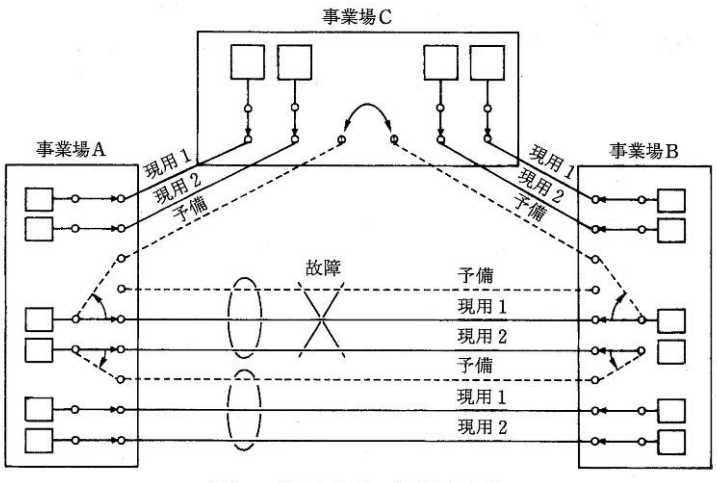
イ　重要な伝送設備には、予備の電気通信回線に速やかに切り換える機能を設けること。

解説

重要な伝送設備（多重変換装置等）には、伝送設備を構成する機器の故障等の発生時等に疎通の停止を防止するため、伝送ルート単位又は回線単位で予備の電気通信回線へ切り替える機能を設ける。

●措置例●

伝送設備には図に例示するような予備の電気通信回線及び回線切替装置を設置し、電気通信回線の故障等には予備の電気通信回線へ切替えを行い、信頼性を確保する。



（注）　↙及び↶は，切替をしめす。

回線切り替えの例

(8)　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し、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し、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。

解説

ア､イ　情報通信ネットワークを構成する重要な伝送路設備等の動作状況を監視し、設備故障や回線品質の低下を速やかに検知、通報を行う機能を設ける。

ウ､エ　情報通信ネットワークを構成する重要な伝送路設備又は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。

「重要な電気通信回線」とは、通信センター間又は通信センターと集線センター（主として利用者の端末と当該センターとの間の電気通信回線を集線する機能を有する小規模なセンター）間の電気通信回線をいい、集線センターと利用者の端末との間の電気通信回線等の端末回線は除かれる。

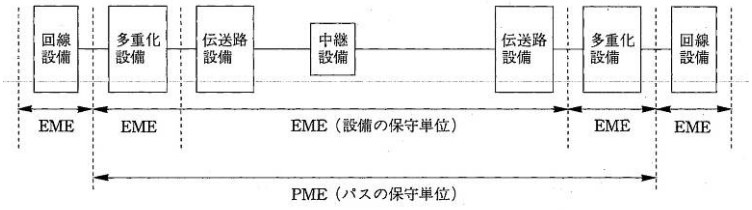
●措置例●

１　Maintenance Entity（ME）の概念

ネットワークを保守する上で、故障となった設備、または、回線を特定するために、保守区分を明確にする必要がある。この保守上の単位を Maintenance Entity（ME）と呼んでいる。

保守単位の一例として、①ネットワークを構成している回線設備、多重化設備、伝送路設備について、個々に動作状況を監視し、異常を検出、通知する設備の保守単位と、②複数の設備により構成させる回線（パス）を監視し、異常を検出、通知する回線（パス）の保守単位等で定義されている。

実際には、回線設備、多重化設備、伝送路設備に監視機能を設けて、設備、パスの警報を検出、通知している。



【保守単位 Maintenance Entity（ME）の例】

２　ディジタル伝送設備の故障検出方式

ディジタル伝送設備では、一般に多重化された信号の位置を識別するために挿入したフレーム信号等を監視し、フレームの不一致や符号誤りを検出することにより、故障と判断して警報を発出する方式がある。また、ディジタル伝送設備の入出力の信号の有無を監視して故障を検出する方式もある。

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し、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異常ふくそう等を制御する措置を講ずる場合は、この限りでない。

解説

情報通信ネットワーク内の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。

天災地変又は社会的異常現象等により、特定対地もしくは、特定加入者に対する呼が､一時的に殺到するとか､特定の局からの発信呼が急増するなどの理由により、ふくそう状態になる。

特定の地域に対する呼が集中的に発生した場合には、トラヒックの状態を絶えず監視しながら、う回規制などの措置を適時的確に行い、ただちに網の混乱を防止する。

なお、データ通信用のネットワーク等では、交換設備から端末設備等の発信機能を制御する通信方式を採用している場合のように、原理的に異常ふくそうが発生するおそれがないものがあるので、この場合は適用しないことをただし書により定めている。

また、経路制御情報は、通信の到達性を確保するため、各事業者が設定し、接続する事業者間であらかじめ送受信されており、当該情報に基づいてパケットの転送経路の制御が行われる。誤り等により大量かつ詳細な経路制御情報が設定された場合、大量の通信が意図しない経路に流入（元の経路から流出）することとなり、インターネット全体に甚大な影響を及ぼすことが想定される。

このような事態を可能な限り迅速に収束させるためには、各事業者がトラヒックに異常な増大や減少が発生していないか等を自動でチェックし、異常等をアラートで知らせる機能を設けることが有効である。

（平成 31 年度にまた書き以降を追加）

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異常ふくそう等を制御する措置を講ずる場合は、この限りでない。

解説

交換設備の疎通能力を著しく低下させる異常ふくそうを防止するため､通信の接続規制を行う機能を具備する。

発信系の異常ふくそうに対しては、通信が集中している交換設備において発信規制を行い､着信系の異常ふくそうに対しては異常ふくそうを起こしている交換設備への通信を受け付けている他のそれぞれの交換設備で接続規制を行う。

「これと同等の機能」とは､例えば中継系で異常ふくそうが発生している場合に、異常ふくそうが発生しているところをう回して疎通を確保する機能、手動により接続規制する機能等である。

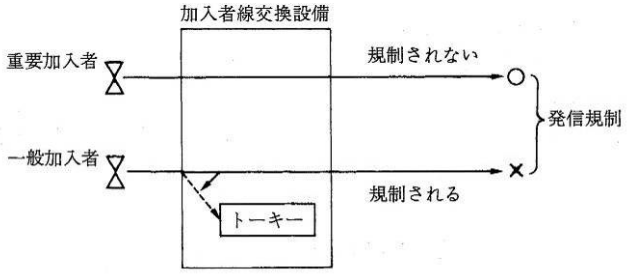
なお、データ通信用のネットワーク等では、交換設備から端末設備等の発信機能を制御する通信方式を採用している場合のように、原理的に異常ふくそうが発生するおそれがないものがあるので、この場合は適用しないことをただし書により定めている。

●電話交換、回線交換等の例●

１　発信規制

加入者線交換設備において、自局発信呼の増大等により処理能力が一定の限度を超えた場合、自動発信規制をかける。また、状況に応じた規制が必要な場合には手動規制を行う。

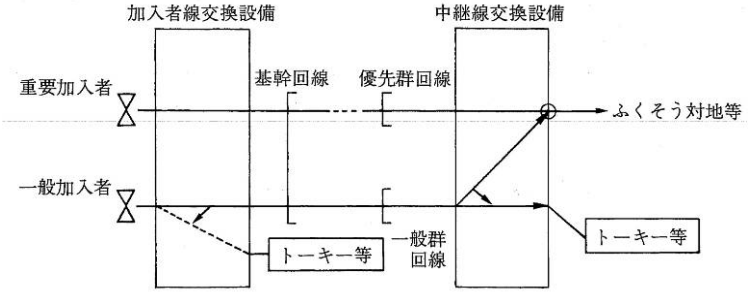
発信規制時は、重要加入者以外の一般加入者を規制し、着信については規制しない。



発信規制

２　出接続規制

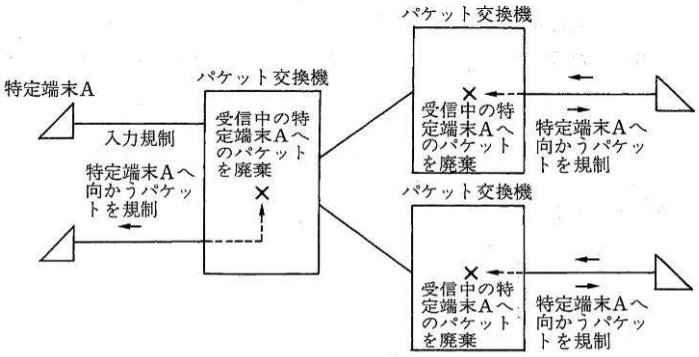
特定対地、特定加入者への接続を制限する。



出接続規制例

●パケット交換の例●

特定端末へのパケット集中により異常ふくそうが生じた場合、この端末へ向かうパケットをネットワーク内のすべてのパケット交換機で規制する。また該当端末からの入力を規制する。



パケット交換による接続規制例

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異常ふくそう等を制御する措置を講ずる場合は、この限りでない。

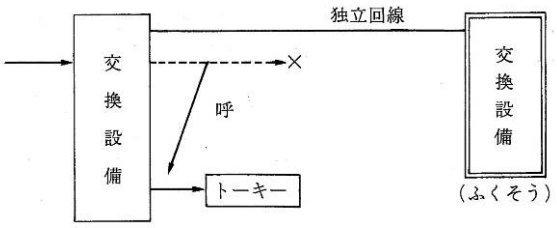
解説

異常ふくそうを悪化させないよう、呼の不接続に伴う再呼を防止するため、電話交換ではアナウンス設備（トーキー）を設置し、不接続となった呼をアナウンス設備に接続する機能を有し、回線交換においては、異常ふくそうを示すサービス信号等により異常ふくそうを通知する機能を設ける。

●電話交換の例●

１　加わる呼規制

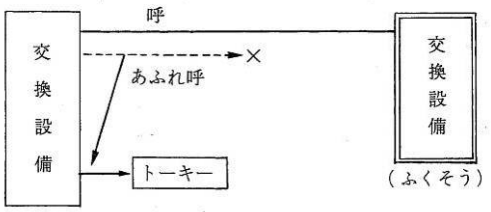
交換設備の、ある方路への接続に際して、その方路への接続動作を行わず、直ちに案内トーキーに接続する。



加わる呼規制

２　あふれ呼規制

交換設備で、ある方路への接続に際して、空き回線があれば正常に接続し、回線全話中のときは案内トーキーに接続する。この措置は、再呼により、更にふくそうを増大させないように、ふくそう状況等を案内して、再呼の減少を図るために行うものであってトラヒックの規制は行わない。



あふれ呼規制

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。

解説

情報通信ネットワーク内の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。

●措置例●

ネットワーク集中管理システムにより、サービスごと、対地ごと並びに回線ごとに、加わった呼数・呼量、あふれた呼数、接続できなかった呼数の状況を把握し、トラヒックの統合的な監視を行う。

国際接続において、相手国の国内トラヒック状況を理解する上で有効な監視項目には、各回線群の使用率、完了率等がある。

ケ　災害時優先通信の機能により他の通信の制限又は停止を行う場合は、災害時優先通信及び他の通信の疎通の状況を記録する機能を設けること。

解説

平成２４年の事業用電気通信設備規則の改正により、電気通信事業者は、必要最小限の通信規制により重要通信の疎通を確保するため、災害時優先通信と一般通信の疎通状況に関するデータを保存・分析した上で、ネットワークの設計容量や通信規制の実施方法等を見直すことが求められているため、災害時優先通信及び他の通信の疎通の状況を記録する機能を設ける。

コ　インターネットの経路制御情報等の制御信号のうち不要又は不正なものの送受信を防ぐために有効な機能を設けること。

解説

インターネットの経路制御情報（通信の到達性を確保するため、各事業者が設定し、接続する事業者間であらかじめ送受信されるものであり、当該情報に基づいてパケットの転送経路の制御が行われる。）等制御信号のうち不要又は不正なものの送受信を防ぐために有効な機能を設ける。

経路制御情報は、ある事業者の誤設定により大量かつ詳細な経路制御情報が不要に送信又は受信されてしまうと、他の事業者に広範囲かつ甚大な影響を及ぼすことが想定される。同様に、不正な経路制御情報が送信又は受信されてしまうと、他の事業者に重大な影響を及ぼす懸念がある。

インターネットの安定性を確保するため、不要又は不正な経路制御情報をルータにおいてフィルターする仕組みや、一定量以上の経路制御情報を受け取らないようリミッターを設定する仕組みがあり、このような設定は、経路制御情報の受信防止又は送信防止の有効な手段になり得る。

例えば、他の電気通信事業者から経路制御情報を受信する際は、Prefix フィルター※1により、細かい経路制御情報を受信しないよう設定したり、AS-PATH フィルター※2により、長い AS-PATH 長の経路を受信しないよう設定したり、リミッターにより、設定した閾値以上の経路制御情報を受信しないよう設定したりする対応が考えられる。また、経路制御情報を他の電気通信事業者等に配信する際は、Prefix フィルターにより、自らの AS 内部で使用している細かい経路制御情報をそのまま外部に配信しないようにする設定が考えられる。

しかしながら、こうした設定が自らの利用者や他事業者にも影響を与える恐れがあることから、各事業者がそれぞれのネットワーク構成及び他事業者との接続状況等を熟知した上で当該設定の影響を十分に検討し、かつ、それぞれの運用の考え方に照らして、柔軟かつ適切な設定を行うことが重要である。

なお、不要又は不正な経路制御情報の送受信による障害の発生を防止するためには、あらかじめ接続先と当該情報の送受信の範囲を明確にすることも有効である。

※1　Prefix は、IP アドレスの中のネットワークアドレスを示す部分をいう。Prefix の長さはアドレス空間の深さを表し、Prefix フィルターはその Prefix の長さを基にフィルタリングを行うフィルターをいう。

※2　AS は Autonomous System の略で、ある経路制御方針によって運営されるネットワークのことをいう。宛先に到達するまでに経由した AS のリストを AS-PATH といい、AS-PATH フィルターはこの AS-PATH を基にフィルタリングを行うフィルターをいう。

（平成 31 年度告示改正により新規追加）

(9)　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し、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ないように対策を継続的に講ずること。

解説

ア　ソフトウェアにおいては、設計手法、開発の自動化等の研究が進められるとともに試験環境の充実が図られているが、ソフトウェアの大規模化の傾向もあり、誤りを完全に排除することは非常に困難である。このため、所要の品質が確保されるよう試験内容の選定、商用設備導入前に関係部門合同での導入判定を実施する等を行うなど、品質の検収作業の充実を図る。

イ　ソフトウェアの変更やバージョンアップに当たっては、ソフトウェア開発支援ツールの活用、確認試験の充実等により容易に誤りが混入しないような措置を講じる。また、システムデータや局データの投入に当たっては、人為的ミスによる

障害を避けるため、ヒューマンインターフェースの向上を図るとともに、ソフトウェア側にガードをかける。

（例）パスワード、論理チェック等

ウ　重要なデータ等はハードディスク等の２次媒体に予め保管し、原データが破壊されても復元が容易に行えるようにする。また、ソフトウェアのファイルのバージョン管理を徹底する。

エ　ソフトウェア内部で論理矛盾等により異常が発生した場合には、速やかに検知し、警報等により当該ソフトウェアの異常箇所を保守者に通報する機能を設ける。

オ　サイバー攻撃等に関する最新の情報収集に努め、ソフトウェアに脆弱性が発見された場合には、迅速なパッチ適用等によりいち早く脆弱性を取り除く等、各事業者が検討して必要な対策を講じることが適当である。

カ　新しいシステムの導入に当たつては、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、ソフトウェアの不具合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。

解説

新しいシステムの導入に当たっては、システムへの高負荷時に問題が明らかになることが一般的であるので、実環境に近い状態で十分な検証確認試験等を実施し、ハードウェアの初期故障やソフトウェアのバグによる障害ができる限り発生しないようにすることが必要である。

特に、ソフトウェア内で証明書が利用されている場合は、証明書の有効期限切れによる突然の機能停止を避けるため、検証確認試験等において、システムの日付を未来日（機器の運用予定期間完了日等）に設定し動作確認を行うことも有効と考えられる。

（令和元年度に、特に以降を追加）

キ　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。

解説

特に IP 系接続サービスでは現用及び予備の装置があるにもかかわらず、切替えが行われない例が多く発生している。これは、切替え動作を行うソフトウェアの不具合が原因の多くを占めているため、その信頼性を確保することが必要である。

ク　ソフトウェアの導入又は更新に当たつては、ウイルス等の混入を防ぎ、セキュリティを確保すること。

解説

情報通信ネットワークにおいてソフトウェアの重要性が増大しており、信頼性の高いソフトウェアを採用することやソフトウェア更新時の信頼性を確保することが必要である。

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。

解説

ソフトウェアの脆弱性は開発段階で極力なくすことが必要であるが、運用開始後新たな脆弱性が発見されることも少なくなく、そのような場合は迅速なパッチ適用等によりいち早く脆弱性を取り除く等、各事業者が検討して必要な対策を講じることが適当である。

コ　交換機の制御等に用いられる重要なソフトウェアについては、復元できるよう複数世代のものを保管すること。

解説

交換機の制御等に用いる重要なソフトウェアは、不具合（バグ）による機能停止に備え、現世代に加え、前世代のソフトウェアを複数世代にわたり保管（バックアップ）しておく。

なお、重要なソフトウェアの不具合により事故が発生し、前世代のソフトウェアに切替えて復旧させる場合などは、その機能を完全には維持できない可能性を考慮して、最低限の機能を維持する方法・手順を定めておくこと。

前世代のソフトウェアに切替える場合には、現世代のソフトウェアにより実現している機能やサービスの一部の提供ができなくなることも考えられることから、そのような場合に備え、各世代で提供可能な機能等の差分は何かを管理するとともに、前世代のソフトウェアに切り戻すために必要な方法・手段をあらかじめ定めておくことが重要である。

（令和元年度告示改正により追加）

サ　交換機の制御等に用いられる重要なソフトウェアについては、ソフトウェア不具合等により電気通信役務の提供が停止することがないよう、当該ソフトウェアの導入・更新時は十分な検証を行い、その信頼性を確保すること。

解説

通信ネットワーク全体に占めるソフトウェアの比重が増大することに伴い、同一のソフトウェアで様々なシステムが動作するようになる。その場合、当該ソフトウェアに異常が発生した際に、同一のソフトウェアを利用するシステムが全て機能不全に陥るなど、従前より被害が広範囲に及ぶおそれがある。そこで、その被害の低減に努めるため、交換機の制御等に用いられる重要なソフトウェアについては、電気通信事業者が当該ソフトウェアを導入・更新する際に、以下の項目について検証を行うことが必要である。

●措置例●

（1）音声伝送役務、（2）データ伝送役務及び（3）監視制御等の各項目に関して、

- 正常動作確認試験（設計した機能が正常に動作するか確認する　等）
- 要求機能確認試験（新たに機能を追加した際に従前の機能を含めて正常に動作するか確認する　等）
- 過負荷試験（トラヒックが増大した際に最低限の機能が維持されることを確認する　等）
- 長時間安定化試験（長時間運用しても安定的に十分なパフォーマンスを発揮することを確認する　等）
- 障害時における動作確認及び切替動作試験（障害発生時に冗長系へ正常に切り替わり役務が維持することを確認する　等）
- その他（ソフトウェアのインストール試験、バックアップ試験、ロールバック試験、ログ出力試験、OS 動作試験、バージョンアップ試験　等）

（令和２年度告示改正により追加）

(10)　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。

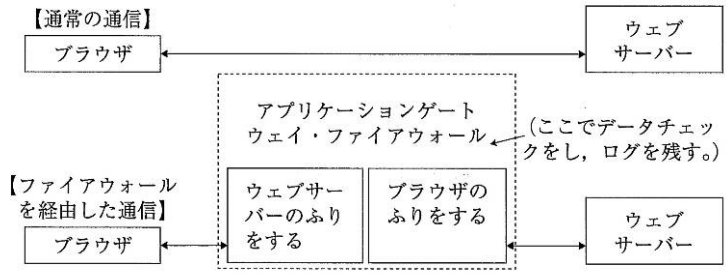
解説

ファイアウォールは、インターネットからサイト等への入口で関所的な役割を果たすもので、その仕組みから、大きく分けるとパケットの伝送をコントロールする「パケットフィルタリング」と通信を中継するプロキシ･プログラムを使用する「アプリケーションゲートウェイ」の２つの機能に分けられる。

●措置例●

このような機能を理解し、ファイアウォールを導入し、適切な設定を行い運用することが必要である。

ファイアウォールの導入に当たっては、ファイアウォールの二重化等効果的な方法を専門業者に委託することも考えられる。



アプリケーションゲートウェイの機能の例

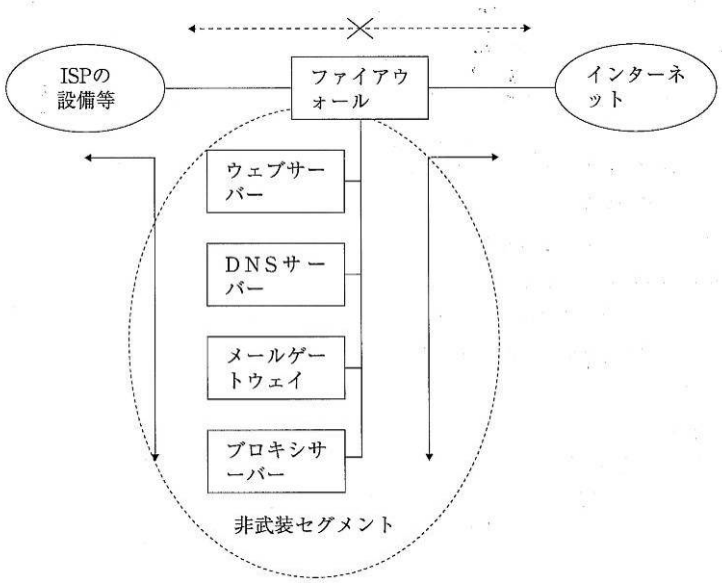
イ　インターネットへ接続する場合は、非武装セグメント構成を採用すること。

解説

非武装セグメント（DMZ: demilitarized zone）は、ファイアウォールに接続されるセグメントであり、インターネット側又は内部ネットワーク側からアクセスできる。ファイアウォールに加えて、この DMZ を設けることにより、内部ネットワークへのアクセスは、DMZ サーバ群からのみ許容されインターネットから直接アクセスすることを制限するため、内部ネットワークのサーバへの外部からの不正アクセスに対し、信頼性を高めることができる。

●措置例●

外部のインターネットと内部のネットワークの間にファイアウォールを設置し、そのファイアウォールに接続される非武装セグメントを構成し、このセグメントに公開用 WEB サーバ、メールサーバ等を配置する。



非武装セグメントの例

ウ　インターネットへ接続する場合は、telnet、ftp 等サービス提供に不要な通信の接続制限を行うこと。

解説

不正アクセス等を回避するためtelnet(システムリモート制御プロトコル)やftp（ファイル転送プロトコル）等については、外部からのアクセスの制限を行うなどとともに、サーバが提供するサービスについても必要最小限のサービスに限定することが必要である。

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。

解説

インターネットは不特定多数の者が利用するネットワークであるため、広く一般に公開するネットワークとセキュリティの確保が不可欠な自社内ネットワークは、区別したネットワーク構成とする必要がある。

●措置例●

開放網と閉域網とのネットワーク構成については、物理的に明確に区別させる方法と仮想閉域網（VPN：Virtual private network）により措置する方法の２つがある。このうち仮想閉域網については、暗号化や認証技術等を使用して閉域網を構成するものである。

オ　インターネットへ接続する場合は､サーバ等におけるセキュリティホール対策を講ずること。

解説

セキュリティホールは、ハッカーからの攻撃の標的となるところから、これを未然に防止するため、最新のセキュリティホール情報の収集やセキュリティホール検知ソフト等の活用により、セキュリティホールの検知に努めることと、これが確認された場合､最新のパッチの投入を行うなど適切､かつ､迅速な対応が必要である。

●措置例●

１　適時なソフトウェアのバージョンアップの実施、又はパッチの適用

２　セキュリティホールとなるdaemon(基本的なプロセスをバックグラウンド

で実行するプログラム）の停止
３　最新のセキュリティ情報に基づく対応の実施

等

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機能を設けること。

解説

ネットワークやサーバ等の重要部分の監視は、ハッカー等からの脅威を防止する意味からも重要であり、また、異常が発見された時の対応も含め、対応体制を確立しておくことが必要である。

●措置例●

具体的な対応としては、第１に、不正アタックや侵入者の検知等を行う IDS（intrusion detection system：侵入検知システム）の導入が挙げられるが、このシステムは、急速な発展を遂げているところであり、システムの導入・更改に当たっては最新のシステムの導入が必要である。

また、侵入が検知された場合の通報者、通報方法等についてもシステム導入時点において決定しておくことが必要である（無線呼出により通報するようなシステム構成も可能である）。

第２には、日常的な監視体制の確立や攻撃を受けた際の対応手順をあらかじめ決めておくこと、重要ファイルのバックアップ、情報セキュリティ技術のスキルアップ等の取り組みが必要である。

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。

解説

情報セキュリティ対策として有効な手段といわれているのは、ネットワーク等の監視と一体的にセキュリティ対策上重要なログの記録及び保存を行い、その解析により適切な措置を講ずることである。

ログは、ネットワークやサーバ等で発生した各種の情報を記録、保存できるものであるが､適切なログ管理を行うためにはログの定期チェックなどの体制整備が不可欠である。

なお、ログは「通信の秘密」に属する事項であるが、セキュリティ対策のため必要かつ相当な範囲でログを保存することは正当な業務行為として違法性がないものと考えられる。しかし、通信の秘密の保護の観点からは、その取扱いには特に慎重な配慮が必要であり、原則として取扱規程においてその保存期間を適切に定め、保存期間を超えたものは遅滞なく消去することが必要である。

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。

解説

インターネットでは、不特定多数の者がアクセスを行い、その中に悪意を持った第三者によるサイバーテロの脅威が存在するおそれがある。インターネットでサイバーテロを防御するには､「自分の家の鍵は自分でかける」といった自衛が基本である。サイバーテロの手法はコンピュータ技術の進展に伴い、日々多様化する傾向にあるため、その対策に関してもできる限り継続的に最新の情報セキュリティ技術を

採用することが必要である。

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。

解説

コンピュータウイルスは、新種のウイルスが日々大量に発生する中で、被害の拡大も危倶されるところであり、ウイルスの種類によっては、自らが加害者となる危険性がある。したがって、各機関から発せられるウイルス情報の収集など日常的に危機意識を持ち、何時でも適切な対応が可能な体制づくりが必要である。

ネットワーク上からパスワードを取得して自動送出する不正プログラムやDDoS攻撃に加担する不正プログラム等の混入についても同様に、日常的な危機意識の醸成が不可欠である。

（参考） DDoS 攻撃

DDoS（Distributed Denial of Service：分散協調型サービス拒否）攻撃とは、複数の場所からWWWサーバなどに処理能力を超える大量のデータを送りつける等の方法により、そのサーバなどをダウンさせる攻撃である。

●措置例●

１　常駐監視機能を持ったウイルス対策ソフトを使用

２　ウイルス対策ソフトに使用するウイルスパターンファイルは常に最新のものを利用

３　クライアントPC、ファイルサーバ、メールサーバ等について、それぞれウイルス対策ソフトを導入

４　外部アクセスが可能なネットワークには、ウイルス侵入をリアルタイムで警告する機能を持ったウイルス対策ソフトを利用

等

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抑圧する措置を講ずること。

解説

ネットワークの機能を管理・運営するコンピュータから企業情報や個人情報等の重要な情報が漏えいしないように対策を講じる必要がある。

漏えい電磁波の主な発生部位としてCRTディスプレイ、信号ケーブル等があげられるところから、この部分への措置が必要である。

●措置例●

１　CRTディスプレイに代えて液晶ディスプレイを使用

２　信号ケーブルについては、光ファイバーケーブルを使用

３　筐体等からの電磁波漏えいについては、情報機器そのもののシールドに加えて、建物全体又は通信機械室等をシールド

４　電源ラインやコネクタ部分等からの電磁波漏えいについては適切なフィルタを挿入

５　CRTディスプレイ等から漏えいする電磁波の信号と類似の信号を発生させることにより、漏えいする電磁波から情報が分離することができないように電磁環境に十分配慮して情報をマスク

等

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。

解説

当事者に対して固有のパスワード等の情報を付与し、それを直接キー入力するか又はIDカード､ICカード等に蓄積し読み取らせることやディジタル署名等により、正当な利用者の識別・確認を行う機能を設ける。又は、声紋、指紋等の個人にとって固有な事象を判別することにより、本人の識別・確認を行う。

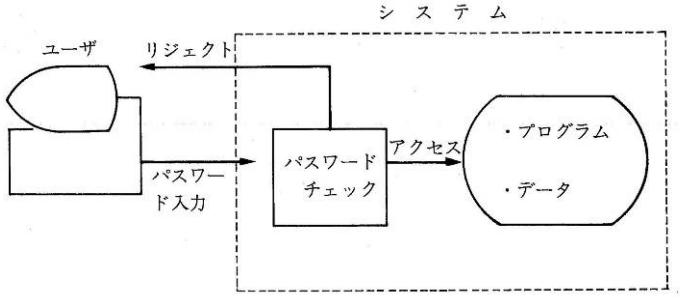
●措置例●

１　パスワードによる識別、確認方法

利用者の識別、確認の手段の中でもパスワードによる方法は、ID カード、鍵などと組み合わせて多くのシステムで採用されており、英数字及び特殊文字を含む４～８桁の文字から構成されるのが一般的である。パスワードの桁数は、利用者の総数と、人間が容易に記憶できる長さとの兼ね合いで決定される。

なお、パスワードの漏えいの防止の観点から、パスワードを画面に表示したり、プリンタに印字したりするなどしてパスワードが第三者の目に触れることのないよう､充分な配慮がなされなければならない｡また､ハッカー(コンピュータ侵入者）対策として、利用者に対しては、パスワードを厳重に管理する（短いパスワードや容易に想定できるパスワードの使用を避けるとか、パスワードを頻繁に変更する）ように注意を喚起することが重要である。また、システムがユーザの利用権を確認した上でおり返し電話するコールバック方式の採用等が考えられる。

パスワードによる利用者の識別、確認の例を以下に示す。



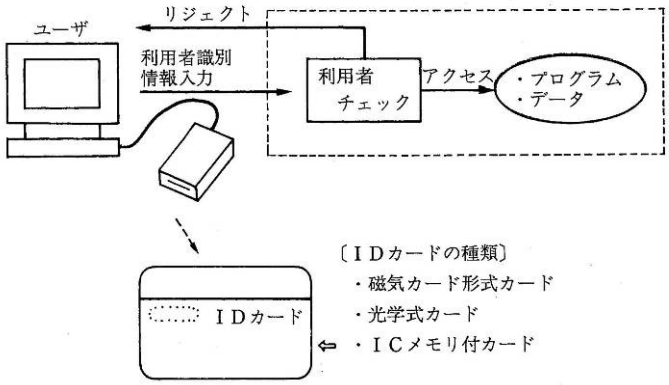
パスワードによる識別

２　ID カードの使用

ID カードの使用は､利用者の識別のために金融機関等で一般に用いられている方法であり､正当な ID カードを持っていれば､それを所持する人は正当な利用者としてみなされる。これは、パスワード等を利用した確認と併用されることが多い。

IDカードには､プラスチックに磁気ストライプをセットした磁気カード形式、ホログラフィック模様をセットした光学式、あるいは、IC メモリを埋め込んだ書き込み可能なものなどがある。

ID カードによる利用者の識別、確認の例を以下に示す。



ID カードによる識別

３　指紋

あらかじめ記憶させた指紋とスキャナで読み込んだ指紋の特徴を比較して利用者の正当性を確認しようとするものであり、高度な画像情報処理技術が要求される。

４　声紋

人間の音声は多数の異なる周波数の合成であることから、その周波数群を分析し、その中からいくつかの周波数を取り出し、これを紋様として視覚化したものが声紋であり、その特徴を識別し利用者を確認する。

５　手形

手の大きさ、指の太さ、長さなどの特徴を識別し、使用者を確認する。

６　署名

筆順、筆圧、速度、加速度等をあらかじめ計測し基準データとして登録しておき、端末を利用する時の実測データと比較して判別する。

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。

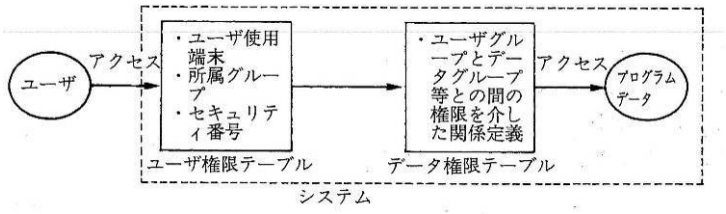
解説

システムにアクセスを行う利用者や運用者等に対し、アクセス可能領域や使用可能な命令の範囲に制限を設けること等により、システムや他人のデータの破壊や窃取を防止する。

コンピュータ資源（データ、ディスク・ボリューム、テープ・ボリューム、プログラム等）の破壊やデータの不当な開示を防止するためには、コンピュータ資源へのアクセスを適切にコントロール（アクセス・コントロール）することが必要である。誰がどのような範囲でコンピュータ資源にアクセスできるか明確な基準を設定することがアクセス・コントロールの基礎である。アクセス・コントロールの具体例を以下に示す。

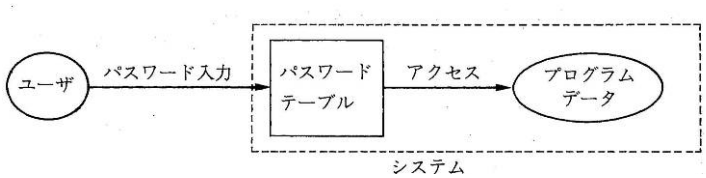
●措置例●

１ アクセス権限テーブルによる方法



アクセス・コントロール（アクセス権限テーブルによる方法）

２　パスワードによる方法



アクセス・コントロール（パスワードによる方法）

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。

解説

パスワード盗用を防止するため、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。

排除する条件として一般的な単語のほか、次のような条件を設定することも考えられる。

●措置例●

１　パスワードの最低文字数

パスワードの最低文字数を定めておき、それに満たないものは排除する。

２　文字の種類の組合せ

アルファベット（A～Z)、数字（0～9）及び特殊文字（.、－）の 3 種類の文字の組合せを条件とする。

３　同一文字の使用制限

7777…のような同一文字のパスワードを設定しないよう、異なる文字を一定数以上使用していないパスワードは排除する。

４　login 名の使用制限

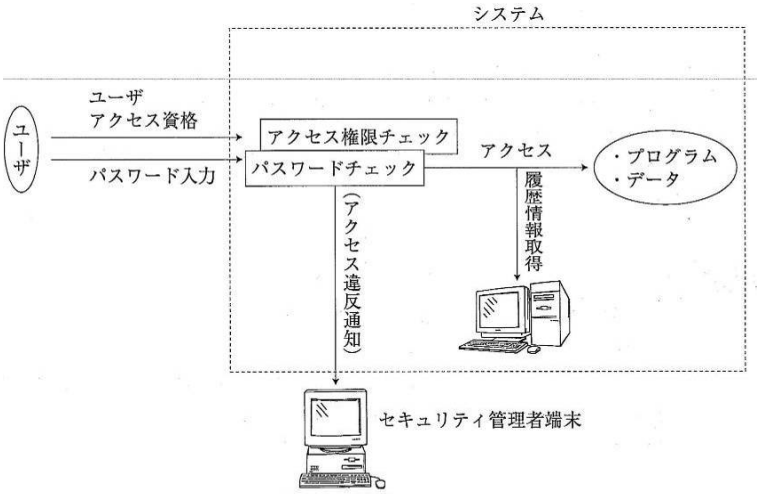
login 名と同じ若しくは含むものの使用を制限する。

セ　アクセス失敗回数の基準を設定するとともに、基準値を超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。

解説

セ　不正アクセス等に対処するため、アクセス失敗回数の基準を設け、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。

ソ　保護が必要な情報については、そのアクセス要求を記録し、定期的に分析・報告すると同時に、問題発生時の監視根拠として保存する機能を設ける。なお、アクセス違反があったときにセキュリティ管理者端末に通報するなどの機能を設けることも有効である。

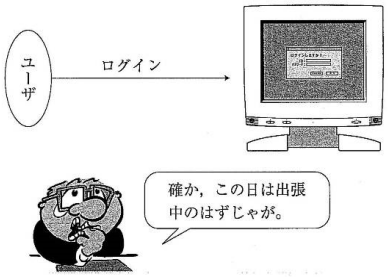


アクセス監視

タ　ネットワークへのアクセス履歴の表示又は照会を行う機能を設けること。

解説

ユーザが不正アクセスの有無を確認できるようにするため、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。



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。

解説

利用者が講じるべき防御策として、パスワードの随時変更を始めとするパスワードの管理が重要であることから、不正アクセスに対処するため、利用者に対して注意喚起する機能を設けることが有効である。

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接続する場合に、再開の意思を確認する機能を設けること。

解説

悪質なハッカーの一般的な傾向としては、一定期間以上ネットワークを利用していない、いわゆる休眠状態の利用者のネットワークや ID、セキュリティの甘いサーバを探し、そこをベースキャンプとして活動する場合が多い。

そこで、ユーザへの注意喚起として、長期遊休ユーザのログイン時には、プロバイダー側から利用者に対して本人の確認を行うとともに、再開の意思を確認する機能を設ける。

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。

解説

通信される情報の機密の度合いにより、利用者またはネットワークにおいて秘話

化措置や暗号化措置を講じる。

●措置例●

1　秘話化措置

同一の電話回線に接続される他の電話機等によって通話の内容が聴取されないように秘話措置の付加等の措置を講ずる。

2　暗号化措置

暗号の目的は、正当な送受信問でのみ意味を理解できるメッセージ交換を可能にし、第三者に情報が渡っても理解できない様にすることである。通信回線上での暗号化はどの部分に暗号機能を持たせるかにより以下のように分類される。

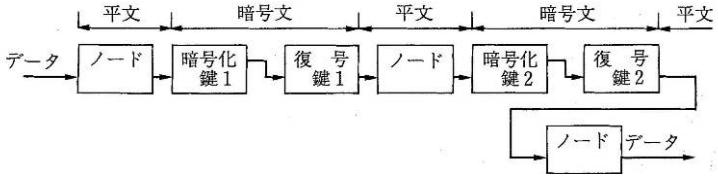
①　リンク暗号方式

②　ノード暗号方式

③　端点間暗号方式（エンド・ツー・エンド方式）

①　リンク暗号方式

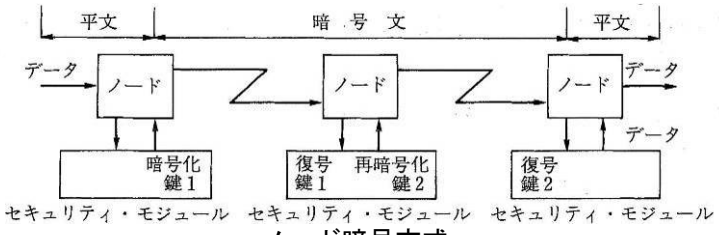
ネットワーク内で隣接するノードとノードを接続するリンク上でのみ暗号化されているがノードで処理されている間は平文となっている方式である。情報の行先を示す経路情報を暗号化することも可能である。



リンク暗号方式

②　ノード暗号方式

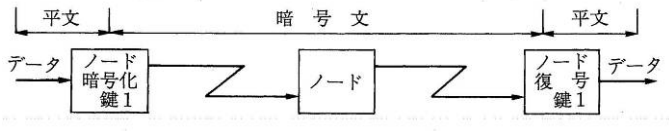
この方式は、リンク方式の弱点（ノードで処理されている問は平文となっている）を補うもので、データはノード内のセキュリティ・モジュールにより暗号化、復号及び再暗号化が行われる方式である。経路情報は平文のままである（暗号化してはならない）。



ノード暗号方式

③　端点間暗号方式（エンド・ツー・エンド方式）

データはユーザ間の伝送全体を通じて一貫して暗号化されている方式である。リンクやノード暗号方式とは異なり、端点問暗号方式では各ユーザは数個の鍵を持ち、暗号を使用する相手ユーザ毎に鍵を使い分けることができる。データは最終目的地に到着して初めて復号が行われ、中間ノードやそれに付属するセキュリティ・モジュールにおいては決して平文の形を取らない。経路情報は平文のままである（暗号化してはならない）。



端点間暗号方式

リンクやノードの暗号方式では暗号機能はネットワークでのみ実行され、ユーザにとっては透過であるといえる。

端点間暗号方式の場合、暗号機能がシステム・サービスを通じて自動的に提供されるときにはユーザにとって透過である。(もしユーザが特別な暗号化が必要ならば暗号使用は透過でなくなる。)

透過な端点間暗号方式をサポートする上でシステムが行わなければならないサービスのひとつは、通信を行うユーザ間のデータを暗号化し復号化するための暗号鍵の選択ないし割当である。

ホスト側に暗号機能を組み込む方法としては以下の方法がある。

① 中央処理装置（CPU）自体へ組み込む
② フロント・エンド・プロセッサへ組み込む
③ CPU チャネルに付加する独立装置に組み込む

どの方法を採るかについては費用対効果の比較検討が必要であるが、③の方法は設計方式の異なる CPU に適応する場合でも一種類の装置設計で良いという利点がある。

リンクの暗号方式では、暗号化されたデータが通過する通信路にあるすべてのノードの入出口に独立した暗号装置を備えなければならない。

また、ノード暗号方式では、暗号化されたデータが通過する通信路にあるすべてのノードが独自のセキュリティ・モジュールを備えていなければならない。

一方､端点間暗号方式では暗号化されたメッセージを作り出し､受け取るノードだけが暗号能力を備えていればよいことになり、ネットワーク内で暗号機能を具備すべき箇所が著しく減少する。

ト　適切な漏話減衰量の基準を設定すること。

解説

アナログ系音声伝送サービスにおいて、了解性漏話による通信内容の漏えいを防止するため、ネットワークとして適切な漏話減衰量を設定し、ネットワーク構成する交換設備や伝送路設備等毎に基準を設定する。

了解性漏話は誘導回線から被誘導回線へ情報が伝達され、他人に通信の内容が漏えいする現象である。この了解性漏話の規定は、電気通信回線設備の端点（利用者の設置する端末設備または他の電気通信事業者との接続点）における必要条件規定であり、事業者はこの端点において了解性漏話がないように自らの電気通信回線設備の各構成要素を設計しなければならない。

ここで、了解性漏話の度合いを支配する要因としては、電話機の伝送品質、室内騒音、発声レベル、回線雑音、局内雑音、加入者線路損失、及び漏話減衰量の周波数特性等種々であり、了解性漏話を規定するためには、これらの要因について条件を設定する必要がある。しかしながら、これらの要因は、必ずしも全利用者全事業者にとって同一ではない。

一例として、数字了解度を基本とする了解性漏話に関する管理上の目標設定例を以下に示す。

〔目標 その１〕

漏話による数字了解度は、ほとんどの加入者において、30%を越えないものとする。

〔目標 その２〕

目標その１を満足するために、交換設備、伝送設備等の漏話減衰量は次表の値

をめざすべきこととする。

設　備　種　別	漏　話　減　衰　量	記　　事
搬　送　回　線	66dB	
音　声　回　線	68dB	中継器挿入回線を含む
加　入　者　線	68dB	
交　　換　　局	70dB	

漏話減衰量

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。

解説

ネットワークが不正使用されることを防止するため、たとえば、呼の設定に係る情報が漏えいしないように十分な暗号化を行う、ネットワークへの接続要求時にユーザ認証を行うなどの措置を行う。

(11)　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。

解説

大規模な災害等の発生時においても通信の疎通の確保が図れるよう、災害対策用の移動無線設備等の機器を配備する措置や、他事業者との相互契約による共同バックアップ体制をとる措置等を講ずる。

●災害対策用の移動無線設備等の機器を配備する措置例●

１　衛星携帯電話の配備：地上通信設備が復旧していない場所での通信を確保

２　衛星車載基地局の配備：エリアとしての携帯電話通信を確保する

３　可搬型無線ＬＡＮ基地局の配備：避難所等でのデータ通信を確保

等

(12)　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。

解説

ケーブルの被災に備え、応急復旧用ケーブルを配備する。

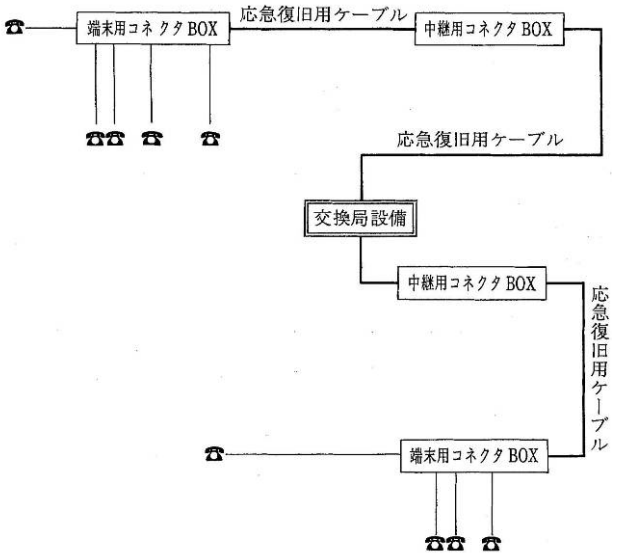
●措置例●

特に、ケーブル故障の復旧は、接続工程に多くの時間を費やすので、接続部分は極力、コネクタ化する方法が望ましい。

(参考)

光ケーブルが社外工事等で被災した場合は、内部構造の異常が発生している可能性がある。

このような場合は、余裕を持って復旧範囲を長めに設定することが、最終的に復旧時間の短縮につながる。(過大張力を受けた範囲は、通信設備の長期信頼性から張り替えを考慮したほうが良い。)

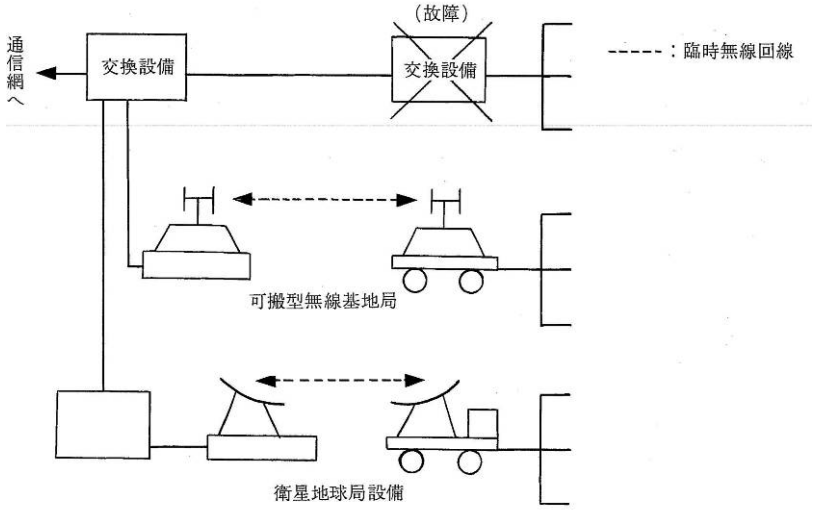


応急復旧対策（応急復旧ケーブルの配備）

イ　災害時等において、衛星携帯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。

解説

災害時等で通信設備が被災した場合、速やかな通信の疎通を確保するために、電話等を臨時に設置するための移動用地球局、可搬型無線設備等の無線設備を配備し、通信の確保を図る。

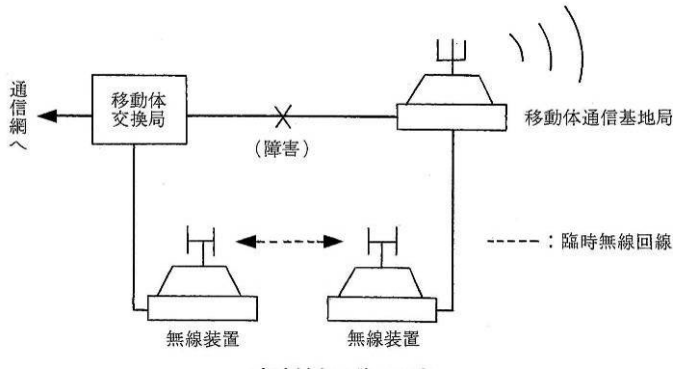


臨時の電気通信回線の設定

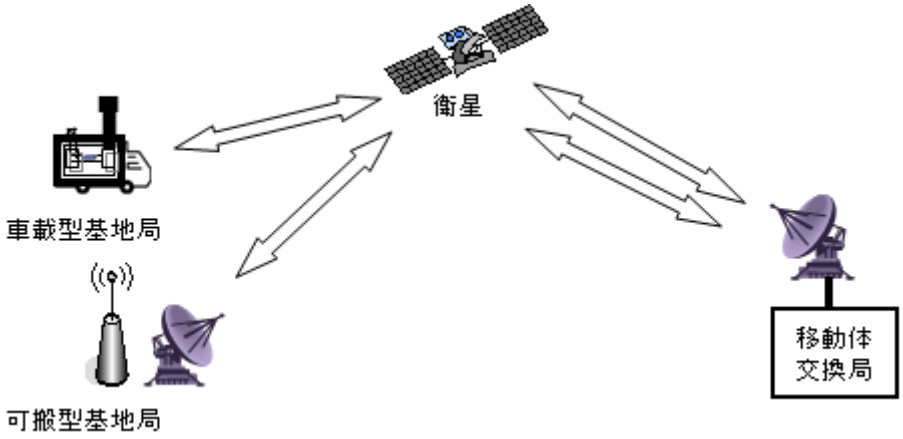
ウ　移動体通信基地局と交換局の間の回線に障害が発生した場合等に、無線設備により、臨時に対向の電気通信回線の設定が可能であること。

解説

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、復旧までの間の通信の疎通を確保するため、可搬型無線設備を配備し、臨時に基地局との対向の電気通信回線を設定し、通信の確保を図る。



（無線による）臨時対向回線の設定

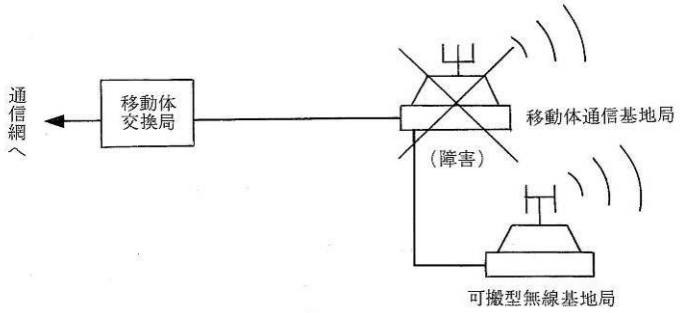


（車載型基地局、可搬型基地局による）臨時対向回線の設定

エ　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。

解説

移動体通信基地局に障害が発生した場合等に備え、臨時に設定できる可搬型無線基地局を配備し、復旧までの間の通信の確保を図る。



臨時の基地局の設置

オ　防災上重要な通信を確保する必要がある拠点をカバーする移動体通信基地局に障害が発生した場合等に、大ゾーン基地局により臨時の大ゾーンエリアの提供又はこれに準ずる措置を講ずることが可能であること。

解説

「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」において、東日本大震災を踏まえ、応急復旧対策としての大ゾーン基地局の全国設置等の取組が進められている旨が記載されている。

「これに準ずる措置」とは、通信障害エリアを少なくするために、送信アンテナ

のチルト角を変更することや、フェムトセル基地局を適切に配置すること等が挙げられる。

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つた場合には、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。

解説

自然災害等で伝送路が途絶した場合、予備回線や予備機器への切替えの他、臨時の他手段での伝送路構築を可能とするよう準備をしておく。

●臨時の他手段に関する対策例●

衛星回線や地上マイクロ無線を活用した伝送路の構築　等

キ　台風等により災害が発生するおそれがある場合は、当該災害の発生に備え、被害が想定される電気通信設備に関し、応急復旧用ケーブルの事前配備等の応急復旧対策をあらかじめ講ずること。

解説

台風等により災害が発生するおそれがある場合は、各通信事業者における応急復旧対策として、移動電源車や予備ケーブル等の応急復旧資機材をあらかじめ被災が想定される地域に配備することや、その運用に必要な人員の確保・配備に積極的に取り組むことが重要である。

（令和２年度告示改正により追加）

(13)　緊急通報の確保

ア　緊急通報を扱う電気通信事業用ネットワークは、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できる機能等を有すること。

解説

事業用電気通信設備規則において、緊急通報を扱う事業用電気通信設備に関する規定が記載されていることから、設備基準においても規定化する。

「端末設備等」、「警察機関等」の定義については事業用電気通信設備規則に記載されている。

「接続できる機能等」の「等」については、事業用電気通信設備規則第３５条の２第１項第二号及び第三号に規定されている事項を実現する機能を指す。

イ　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限り緊急通報が利用できるよう適切な措置を講ずること。また、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。

解説

緊急通報が常に利用できるようにするため、できるだけシステム稼動状態でメンテナンスを可能とするよう適切な措置を講ずる。また、メンテナンス時にサービスを停止する場合は、多様な手段を活用して、ユーザに通知をする。

（別表第２　第３．１．(13)カに再掲）

(14)　予備機器等の配備基準の明確化

予備電源の設置、冗長化等の予備機器等の配備基準の明確化を図ること。

解説

装置構成においては、様々な冗長構成について考慮して適切な冗長構成を選択することが必要である。また、装置が提供する機能などを考慮して冗長化構成の

基準を策定することも必要である。

さらに、仮想化技術（SDN/NFV）を活用して、ネットワークを構成するハードウェア上でソフトウェアにより実現される各種機能を統合管理する装置（仮想化管理システム）を用いてハードウェアの故障時の予備系への切替えを柔軟に行うなど機能の冗長化等を実現する場合は、仮想化管理システムについて予備機器の配備等による冗長構成をとり、障害時等にサービスを継続できることが必要である。

（令和元年度に、さらに以降を追加）

(15)　大規模災害対策

ア　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、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設置、臨時の電気通信回線の設置に必要な機材の配備その他の必要な措置を講ずること。

解説

従来から、交換設備相互間を接続する伝送路設備については複数経路化によりその冗長性を確保することとしていたが、多くの電気通信事業者では、より経済的に冗長性を確保するため、ループ状の網構成を採用された。

しかしながら、ループ状の網構成では、一箇所の被災によりループの全体について冗長性が失われてしまうことから、複数箇所の被災が想定される大規模災害では、ネットワークの機能が損なわれ、広域にわたり通信が停止することが危惧される。

このため、ループ状の網構成については、ループにより囲まれる地域を横断する伝送路設備の追加的な設置、臨時の電気通信回線の設置に必要な機材の配備その他の必要な措置を講じる。

イ　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、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。

解説

都道府県庁等の防災上必要な通信機能の維持のためには、新たに都道府県庁等で使用されている移動端末と接続されている基地局と交換設備との間を接続する伝送路設備の冗長性を強化する必要があるため、当該伝送路設備については予備の電気通信回線を設置することし、その伝送路設備はなるべく複数の経路により設置するべきとしたものである。

なお、この規定における「都道府県庁等」とは、事業用電気通信設備規則第 11 条第３項に記載されている「都道府県庁、市役所、特別区の区役所又は町村役場の用に供する主たる庁舎」を指す。

（令和６年度設備規則改正により「なお」の段落を追加）

ウ　電気通信役務に係る情報の管理、電気通信役務の制御又は端末設備等の認証等を行うための電気通信設備であつて、その故障等により、広域にわたり電気通信役務の提供に重大な支障を及ぼすおそれのあるものは、複数の地域に分散して設置すること。この場合において、一の電気通信設備の故障等の発生時に、他の電気通信設備によりなるべくその機能を代替することができるようにすること。

解説

IP 化の進展に伴い、基幹的な電気通信設備の故障等がネットワーク全体に影響を及ぼす事例が散見されており、その故障による影響を低減するため、地理的分散及び相互代替を講じるべきとしたものである。

対象となる電気通信設備は、メール、接続認証、ＤＮＳ等を提供するためのルータ、スイッチ、サーバ等である。

エ　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。

解説

一の被災により、複数経路化された伝送路設備のいずれもが同時に影響を受けることがないよう、互いになるべく離れた場所に設置するべきとしたものである。

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。

解説

有線電気通信設備令及び同令施行規則等で定めるところによるほか、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ついては、強風下（最大瞬間風速60m/s 程度）において、設備が損壊しない構造とする。また、風による振動（ダンシング）での障害防止措置を講ずる。

「屋外設備」とは、屋外に設置している電線（一般に電話線やケーブルで中継器も含む。)、空中線（パラボラアンテナ等の各種アンテナ類）及びこれらの附属設備（電線の端子函等）並びにこれらを支持し又は保蔵するための工作物（電線を設置している管路、マンホール、とう道等及び空中線を設置している鉄塔等）である。電気通信事業用ネットワーク､自営情報通信ネットワーク以外の情報通信ネットワークでは、該当する設備は構内に自ら設置する部分等に限られる。

●措置例●

１　ダンシング防止

ダンシングとは、自己支持形ケーブルに発生しやすい現象で、受風面積が大きいため、風によって揚力を生じケーブル自体のねじれ振動と相乗し、一種の自励振動が発生するものである。この自励振動により支持網より線や心線が破断することがある。防止措置としては、ケーブルの支持間隔を短くする方法、カテナリ方式で吊架する方法、ケーブルにねん回を挿入する方法がある。

２　給電系導波管等の横揺れ防止

鉄塔等に設置されたパラボラアンテナ等に給電するために設置される導波管等は、風による横揺れを防止するよう鉄塔等にしっかり固定する。

(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

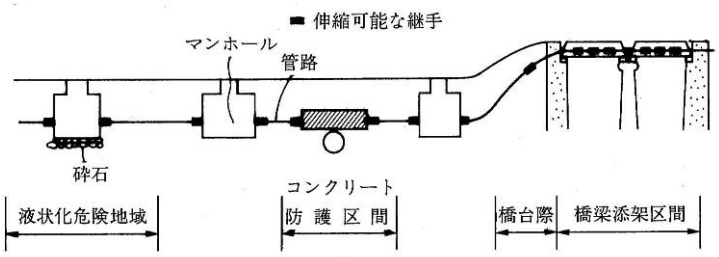
地震等による強力な振動（震度５強程度）や道路、架橋等にみられる定常的な振動に対して、安定的に所定の機能を維持できるような措置を講ずる。

●措置例●

１　管路

マンホールと地下管路との接続箇所､コンクリートで管路を防護した区間際、橋台際等に必要に応じ伸縮可能な継手を入れるなどするとともに、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。

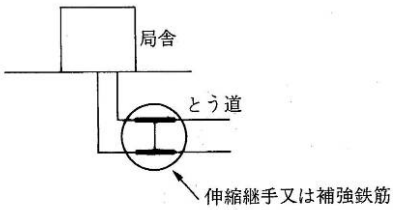
橋梁添架管路では、橋台際、橋げたの不連続箇所、所定の間隔の箇所に伸縮可能な継手を入れるなどして耐震性の向上を図る。



管路の振動対策

２　とう道

局舎ととう道の接合部及び土質急変箇所等に、必要に応じ伸縮継手又は補強鉄筋を設置する。



とう道の振動対策

(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。

解説

雷害には、落雷による電撃電流が直接機器に影響を与える直撃雷、落雷時の地表表面の電界分布による電荷の移動が地表上にある電線類の影響を及ぼす誘導雷等がある。

雷害対策の基本は、以下のとおりである。

１　雷サージの流入出経路を遮断

２　雷サージ流入経路の低インピーダンス化を計り、設備内に流入する雷サージを低減

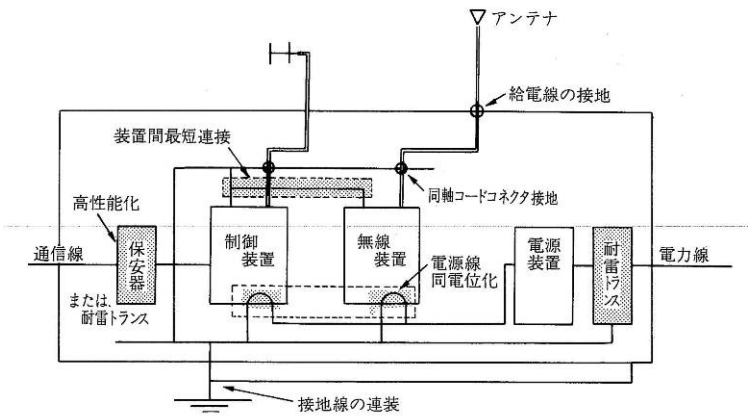
３　アレスタ等の保護素子を挿入し、電位差を機器の耐力以下に抑圧

４　装置間の接地端子を連接し、装置間の同電位化

通信設備を設置している局舎においては、アンテナ等の屋外設備、通信線設備、電力設備等の雷の侵入経路が多数あり､耐力の弱い経路から侵入する｡したがって、雷害対策は、一部分についてのみではなく、系全体について対策を講じる必要がある。

屋外設備のうち、アンテナは鉄塔等の最先端部に取り付ける場合が多いが、避雷針のついている鉄柱にアンテナ、ハイブリッド等が設置されている場合は、給電線に雷サージが流入し、または、誘起される場合があるため、機械室直前では外部導体を接地系に接続して雷サージを流失させるとともに、機械室内においても接地系に接続する。

なお、通信線の線間、通信線と接地系間の電位差を装置耐力以下の電圧に抑圧させるため、通信線にはアレスタを挿入するとともに、直撃雷の影響を受ける可能性のある局舎及びその対向局舎等にはアレスタを使用する。



雷害対策概念図

(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。

解説

類焼による設備の機能障害を防止するため、不燃化又は難燃化の措置を講じる。

●措置例●

1　ケーブルの難燃化対策

①　難燃性外被ケーブルの使用

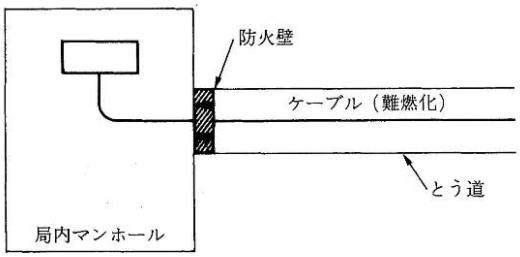
②　シート状の耐火材料等による、ケーブルの難燃化の実施

2　火を使わない工法の実施

とう道内におけるケーブルの接続作業等では、極力火気を使用しない工法を適用する。

3　とう道内防火壁の設置

とう道内で万一発生した火災が、局内マンホールに類焼し、通信機械設備へ影響を及ぼさないようにするため、とう道と局内マンホールとの境への防火壁の設置又はこれに準ずる措置を講ずる。



防火壁による火災対策

(5)　耐水性の対策

ア　水中に設置する屋外設備には、耐水機能を設けること。

解説

水中に設置する設備においては、設備を構成する素材及び設備構造上、耐水機能を持つようにする。

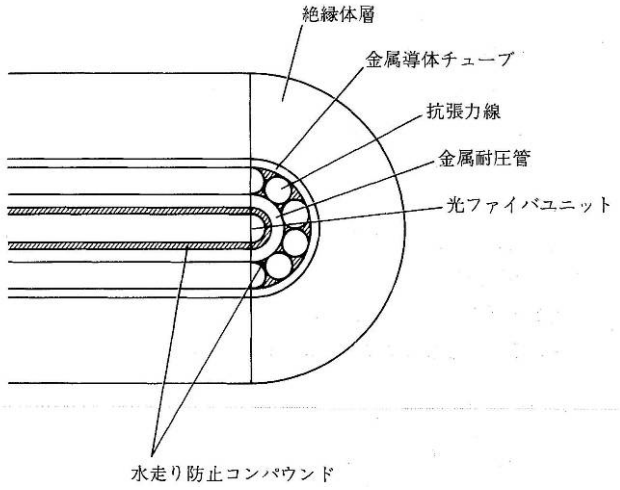
●措置例●

海底ケーブル等は、ケーブル内への水の侵入を防ぐために、ケーブル外被を厚くするとともに、ケーブル内に防水コンパウンドを充填する。

光海底ケーブルでは、ケーブル内へ水が侵入すると光ファイバの機械的強度が

劣化するのみでなく、電気化学反応や金属材料の腐食により、水素ガスが発生し、光ファイバの伝送損失を増加させる問題が生じる。このため、耐水措置として、絶縁体層及び金属導体チューブ等により、外部からの水の侵入を防ぎ、またケーブル内空隙に防水コンパウンドを充填し、ケーブルが破断した場合でも、破断点より、ケーブル長手方向へ水走りを防ぐ。

次図に耐水構造を含めた光海底ケーブルの水走り防止等の一例を示す。



光海底ケーブルの水走り防止例

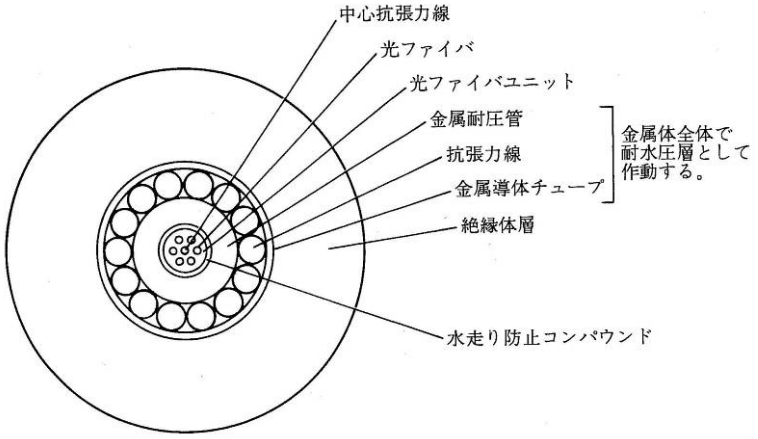
イ　水中に設置する屋外設備には、水圧による故障等の発生を防止する措置を講ずること。

解説

水中に設置する設備においては、予想される水圧や潮流圧に対して設備損傷及び機能障害を起こさないよう措置を講ずる。

●措置例●

海底ケーブル等はケーブル外被厚や心線被覆厚を厚くすること等により、水圧による座屈を防止する。特に光海底ケーブルでは、機械的に弱い光ファイバを深海底の高水圧（水深 8,000ｍでは約 800kg／c ㎡の水圧になる。）から、長期にわたって保護するため、光ファイバを金属製の耐圧管に収容する。以下に耐圧構造を含めた光海底ケーブル断面図の一例を示す。



光海底ケーブルの耐圧構造例

(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、

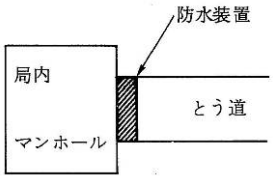
やむを得ない場合であつて、防水措置等を講ずるときは、この限りでない。

解説

水害のおそれのある場所には極力設備の設置を避け、やむを得ず設置する場合は防水措置等を講ずる。

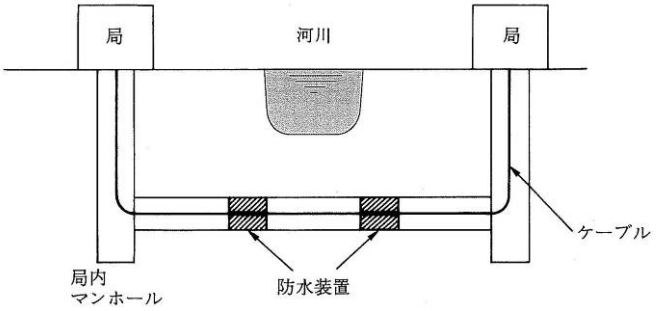
●措置例●

1　地盤が低く、高潮、路面冠水等によりとう道への浸水の可能性のある地域については、局内マンホールととう道との境に防水装置を設置する等必要な措置を講ずる。



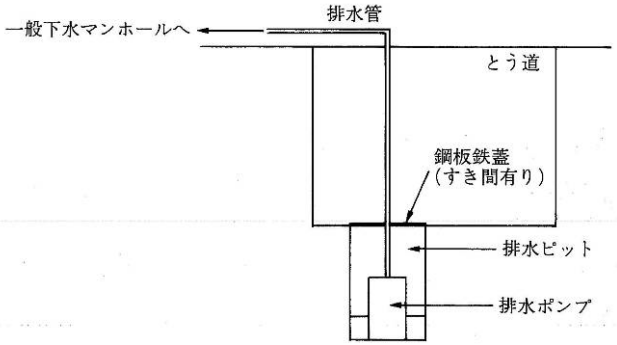
とう道の水害対策例１

2　大きな河川の下をとう道が横断している場合は、必要により河川の両側に防水装置を設置する。



とう道の水害対策例２

3　とう道内の必要な箇所には排水ポンプ等の排水設備を設置する。



とう道の水害対策例３

(7)　津波対策

津波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、やむを得ない場合はこの限りでない。

解説

東日本大震災において高い津波が発生し、沿岸地域に配備されていた通信設備の倒壊・水没・流失、地下ケーブルや管路等の断裂・損壊、電柱の倒壊、架空ケーブルの損壊、携帯電話基地局の倒壊・流失などの被害が発生した。広域な通信の確保等に影響のある重要な屋外設備は、やむを得ない場合を除いて津波のおそれのある場所には配置しないことが適切である。

(8)　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。

解説

寒冷地等の凍結のおそれのある場所に設置する屋外設備においては、凍結による機能障害防止措置を講ずる。

例えば、寒冷地における管路収容ケーブルの場合、管路内の増水が凍結し、その膨張圧によってケーブルの圧壊、変形を生ずる危険性があるのでこれを防止するため適当な凍結防止措置を施す。

(9)　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。

解説

臨海地域、空気汚染地域等塩害や腐食性ガス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おいては、塩害や腐食性ガス又は粉塵による害の防止措置を講ずる。塩害や腐食性ガス又は粉塵による害の受けやすい屋外設備としては、架空ケーブル及び接続部、つり線、ケーブルリング、電柱（金属性）、支線などがある。腐食の著しい場合は、人命の危険を招くことになるため、臨海地域、空気汚染地域等においては、腐食防止措置を講ずる。

●措置例●

1　耐食性のある材質のものを使用する。

2　防食材料を塗覆する。

3　塩害や腐食性ガス又は粉塵による害により故障等が発生する前に設備を取り替える。

(10)　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、その条件下で安定的に動作するものであること。

イ　温度差の著しい場所又は温度変化の急激な環境に設置する屋外設備は、その条件下で安定的に動作するものであること。

解説

高温度又は低温度の環境に設置する屋外設備においては、その周囲条件下で安定的に機能するような耐温度構造とする。また、温度差の著しい環境下や温度変化の急激な環境下に設置する屋外設備においては、温度変化による影響の少ない素材の使用又は伸縮に対応できる設置方法を用いる。

●措置例●

1　高温となる環境に設置する設備

・　軟化点の高い材質（ケーブル外被、心線絶縁体等）を使用する。

2　低温となる環境に設置する設備

・　脆化（可塑性や延性を失うこと）温度の低い材質（曲げ応力、せん断応力等の発生する箇所に使用する材料）を使用する。

3　温度変化の急激な環境下に設置する設備

・　温度伸縮の少ない材質を使用する。

・　ケーブルについては、スラック（ゆるみ）を入れ、温度伸縮を吸収する。

・　つり線の張力は温度変化による増加を想定する。

(11)　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。

解説

　高湿度となるおそれのある場所には、極力設備の設置を避け、やむを得ず設置する場合は、密封構造等の耐湿度措置や防錆措置を講ずる。

●措置例●

　１　耐食性のある材質を使用する。

　２　防錆塗料を塗布する。

　３　高湿度により故障等が発生する前に設備を取り替える。

(12)　高信頼度

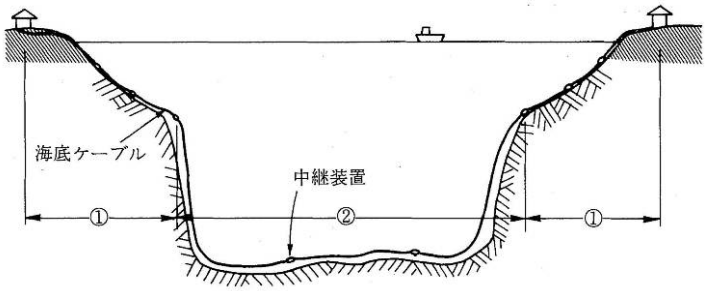
　　海底、宇宙空間等の特殊な場所に設置する重要な屋外設備については、高信頼度部品の使用等による高信頼度化を図ること。

解説

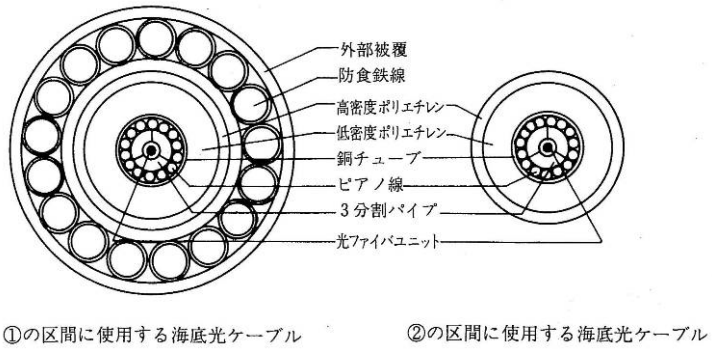
　海底や宇宙空間等の特殊な場所に設置する重要な屋外設備においては、それを構成する装置の高信頼度化を図り、設備としての信頼性を確保する。

●措置例●

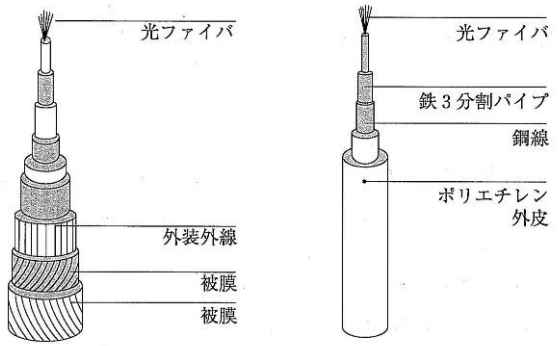
　海底伝送路設備は、故障時の復旧に長時間を要する。従って、高い水圧に耐え、なおかつ信頼性の高い設備とするため、高信頼度部品の使用、ケーブルの耐圧構造及び浅海部の鉄線外装化などにより故障率を低下させて信頼度を高める。



ケーブル敷設図



長距離ケーブルの構成



①の区間に使用する海底光ファイバーケーブル　②の区間に使用する海底光ファイバーケーブル

長距離海底光ファイバーケーブルの構成

(13)　第三者の接触禁止 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。 イ　とう道等には、施錠等の侵入を防止する措置を講ずること。

解説

屋外設備に対し、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。なお、無線設備に対しては、電波法第３０条において、人体への危害や物件への損傷を防止するため、容易に立ち入りできないように安全施設を設置することが義務づけられている。

●措置例●

１　敷地内への立ち入り防止､設備への接触を防止するため防止柵を設置する。

・　防止珊は高さ２ｍ程度とし、簡単に乗り越えられない構造とする。

・　防止柵は外部から容易に破壊されない構造とし、必要により、防犯警報装置を設置する。

２　多条数のケーブルを収容するとう道や重要ケーブルを収容するマンホール等においては、施錠、接着、封印等の侵入防止装置を講ずる。

３　架空電線の支持物については、有線電気通信設備令及び同施行規則で定めるところによる。

(14)　故障時の検知、通報 ア　重要な屋外設備には､故障等を速やかに検知し､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。

解説

重要な屋外設備の故障等が発生した場合、速やかに設備の故障等を検知、通報する機能を設ける。また、故障等の箇所を識別する機能を設ける。

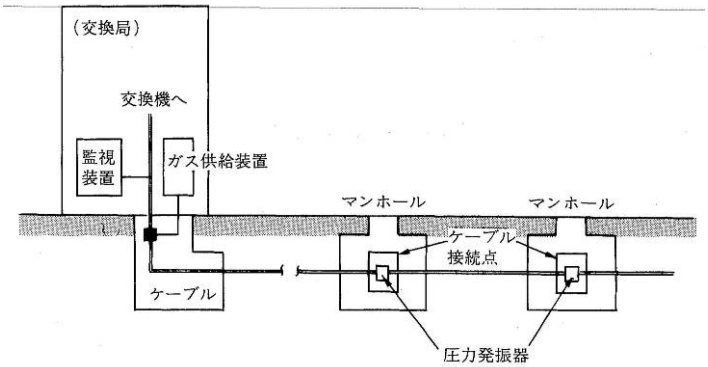
●措置例●

１　ケーブル

ケーブルの信頼性確保のため、接続部あるいは外被に損傷等が発生した場合に、異常区間が推定可能なパイロット線による絶縁監視、ガス圧監視等の遠隔監視システムを設置する。

【ガス圧遠隔監視システムの例】

ケーブル内に供給されているガスがケーブル外被の損傷等によりガス漏えいが発生した場合に、各ケーブル接続点に予め設置されているガスの圧力発振器の測定値をビル内に設置されている監視装置に測定用回線を通じて転送し、ガス圧力分布から漏えい箇所を推定するシステムである。



〔システム装置イメージ図〕

２　とう道

一度火災が発生すると、入溝者や通信施設にかなりの被害を与えるおそれがあるため、とう道内の災害に対して火災、有毒ガス等を検知し、災害の種別、発生場所等の情報を通報する機能を有したシステムを設置する。

(15)　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。

解説

屋外に設置する重要な設備において故障が発生した場合、速やかに正常機器に置換できるよう予備機器の適切な配備を行う。予備機器の配備区分及び数量は、設備の重要度、現用装置数、故障発生率、復旧時間等を考慮して決定する。

「これに準ずる措置」とは、多数の同一機器により負荷分散を行い、特に予備機器がなくともいずれかの機器の停止時には、残りの機器によって全体としての機能を確保できる場合、予備機器の配備に当たって予備機器を一か所に集中配備している場合等をいう。

配備区分

１　集中配備……使用頻度の少ないものについて地域ごとに場所を選定して集中的に配備するもの。

２　専用配備……保全・運用エリア単位で専用して使用するもの。

３　共通配備……近隣の保全・運用エリア間で共用して使用するもの。

(16)　通信ケーブルの地中化

災害時等の建物の倒壊、火災、津波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。

解説

災害時等の建物の倒壊、大規模な火災、津波等による通信ケーブルの被災を防ぐため、架空より被災率の低い通信ケーブルの地中化を実施する。

通信ケーブルの地中化は、莫大な投資と整備期間が必要であることから、通信ケーブルの重要性等を考慮して計画的に行うことが必要である。

(17)　発火・発煙防止

他の電気通信事業者の屋外設備に電気通信設備を設置する場所の提供を受けている全ての電気通信設備について、設備を設置する電気通信事業者が発火・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。

解説

他事業者の屋外設備にコロケーションしている設備が発火した場合には、同一設備に設置されている全ての事業者の利用者の通信に影響を与えるおそれがあり、社会的影響が大きいため発火・発煙防止等の対策が必要である。

●措置例●

１　難燃性の被覆を有するケーブル等を使用すること

２　火気使用を制限すること

３　発火・発煙などのおそれのある物等を配備または持ち込まないこと

３　屋内設備

(1)　地震対策

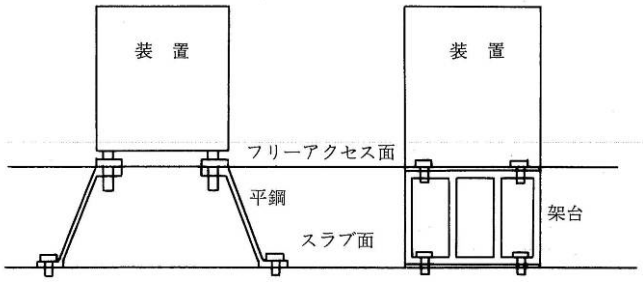
ア　通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。

解説

屋内設備（交換機、コンピュータ、多重化装置、端局中継装置等の屋内に設置する設備）を床面等に取付けを行う場合、通常想定される規模の地震（震度５強程度）により、設備の転倒や移動を防止する措置を講ずる。

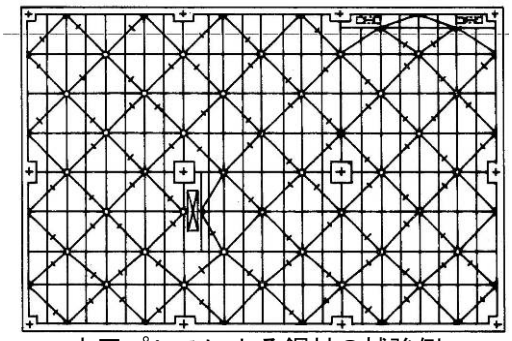
●措置例●

１　架構成をとる交換設備や伝送設備等は、一般に架の上部及び下部を固定するが、自立形の場合は、下部のみ固定する。架の固定方法としては、上部は天井、壁、柱に固定された鋼材に、下部は床面に固定金物又はボルトで固定する。



設備の転倒、移動防止装置

２　鋼材については、次のように、水平プレス（斜め材）を設置し、耐震補強を行うことが有効である。



水平プレスによる鋼材の補強例

３　免震構造には、空気バネにより上下方向の免震を図る方式および積層ゴムにより水平方向の免震を図る方式等があり、これらを組み合わせることにより水平・上下動両方に対しての免震化が可能となる。

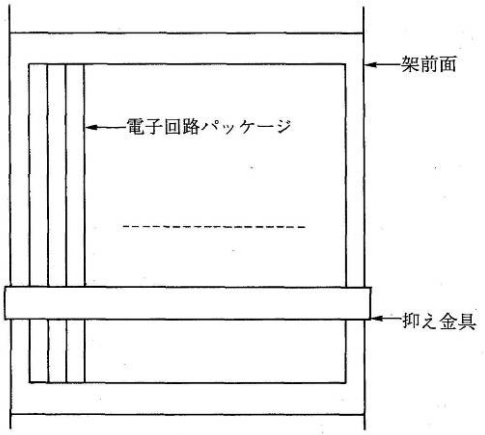
イ　通常想定される規模の地震による屋内設備の構成部品の接触不良及び脱落を防止する措置を講ずること。

解説

地震等の強震動を受けた場合、設備の構成部品である基盤等の脱落、接触不良を起こさないような防止措置を講ずる。また、東日本大震災においては、屋内設備の上に置いてあったビスが揺れによって設備内部に落ち、電源設備をショートさせて故障した事例が発生しているため、屋内設備周辺は可能な限り整理整頓しておくことが望ましい。

●措置例●

地震等により、設備の構成部品は、架前面の抑え金具により脱落を防止する。



設備の構成部品の脱落防止例

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

障害が発生した場合、電気通信サービスや自己の業務に重大な影響を及ぼすおそれのある電気通信設備については、直下型地震又は海溝型巨大地震に起因する高レベルの地震動を目標として、その通信機能を失わないよう耐震性を強化する。具体的には、最近における最大規模の地震である阪神・淡路大震災及び東日本大震災の規模が目標となる。

(2)　雷害対策

雷害が発生するおそれのある場所に設置する重要な屋内設備には、雷害による障害の発生を防止する措置を講ずること。

解説

同一屋内でも接地系が独立であれば、落雷時には接地系間で大きな電位差が発生するため、接地系を連接して同電位化する。

装置間の電位差を最小限にするために、関連装置間の接地端子を接地線で最短接続して、装置間全体の同電位化を図るとともに、電源線と装置の同電位化のために電源線及びその端子と装置設備端子を接続する。

なお、通信線の場合、通信線と接地系間の電位差を装置耐力以下の電圧に抑圧させるため、通信線にアレスタ（避雷器）を挿入する。

●措置例●

１　局内接地系の連接による同電位化を図る。

２　装置間の電位差を最小にするために、関連装置間の接地を最短接続する。

３　通信線にアレスタを挿入する。

(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。

解説

火災の発災及び類焼を防止するため、保護措置の設置、不燃化又は難燃化等の措置を講ずる。

●措置例●

１　保護装置の設置

装置、部品等の故障による過電流加熱を防止するため、適当な装置単位に

ヒューズやMCCB（配線用遮断器）を挿入する。

２　ケーブル等の対策

①　フロアを跨がり敷設されるケーブルを通す貫通口は、火災の際、延焼通路となるほか、煙突効果により火勢を強めるので、十分な防火措置を行う。

②　重要な通信設備には難燃化ケーブルを使用するか難燃化の対策を施す

３　通信設備の不燃化等

①　通信設備は可燃部品の使用を回避する。

②　劣化により発火の危険性のある大容量コンデンサー等の部品については、定期的な取替え等の措置を講ずる。

(4)　高信頼度

ア　重要な屋内設備の機器には、冗長構成又はこれに準ずる措置を講ずること。

解説

重要な屋内設備（障害が発生した場合に電気通信サービスや自己の業務に重大な影響を及ぼすおそれのある設備）の機器で単体にて十分な信頼度が得られないものについては、重要度に応じ２重化構成、複数の現用機器に対しては１つの予備を持つｎ＋１又は故障した機器を運用状態から切り離すプール化等の冗長構成とし、設備機能の確保を図る。もしくは、これに準ずる措置として予備機器等の配備の措置を講ずる。

なお、通信の安定的提供や信頼性確保のための基本的考え方として、

１　高信頼度部品の採用（機器等の高信頼度設計）

２　冗長構成の採用

３　正常部品による故障前置換

４　故障時修理時間の短縮等

がある。

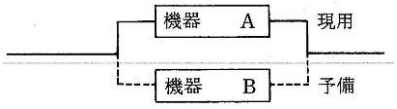
●措置例●

重要な設備では障害による処理の中断を防止するため、予備機器を設置した冗長構成をとり、故障時直ちに予備機器に切換えて正常運転を続行する方法と、全ての設備を運用状態にしておき、故障時直ちに故障した機器を切り離し、他の機器で故障した機器の処理を担う方法がある。

機器の重要性等により予備の機器数を変更する考え方には、大別して次の３種がある。

１　２重化方式

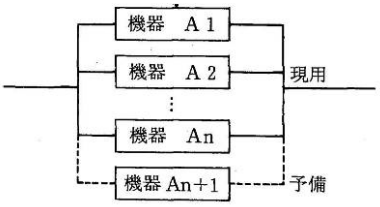
同じ機器を２組用意する方式で、一方が障害になっても、もう一方を使用して正常運転を続行できる。



２重化方式

２　ｎ＋１予備方式

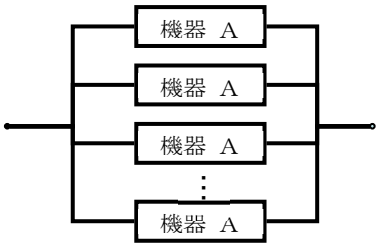
いくつかの同じ機器（ｎ個の現用機器）に対し、共通の予備機器（１個の予備機器）を設ける方式。ｎ個の現用機器の内の１つが障害となってもその影響する範囲が限定される場合、共通の予備機器に切換え、運転を続行できる。



ｎ＋１予備方式

３　プール化方式

いくつかの同じ機器（ｎ個の現用機器）で運転を行い、１つが障害となっても他の現用機器で障害となった機器の処理を担うことで正常運転を継続できる。



プール化方式

イ　重要な屋内設備の機器は､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。

解説

重要な設備においては、機器の故障時に速やかに予備機器への切換え（再構成機能）又は故障した機器の運用状態からの切り離しを行い、設備としての機能を確保する。

次のようなときに再構成機能が働く。

１　現用機器が故障のとき、速やかに予備機器に切換える。

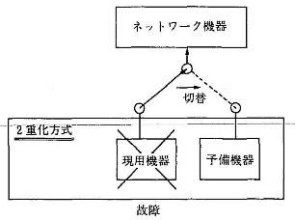
２　機器の定期試験などのために、正常運転系から被試験機器を取り外す。

３　故障回復又は試験終了後、機器を正常運転系に戻す。

●措置例●

１　２重化方式の場合

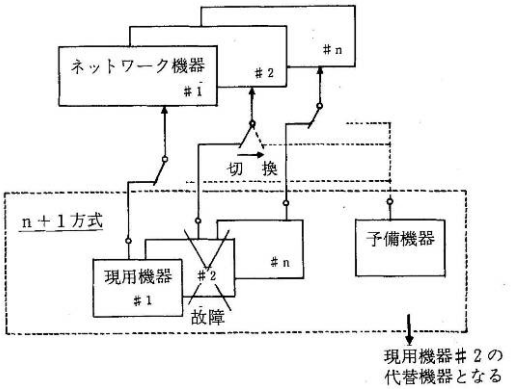
一つの現用機器に対して、現用と同一の予備機器を一つ設置し、現用機器が故障時、プログラム制御で速やかに予備機器に切り替えるとともに警報、ベル鳴動、ランプ表示、メッセージ出力により故障発生を保守者に通知する。



予備機器への切換え（２重化方式）

２　ｎ＋１方式の場合

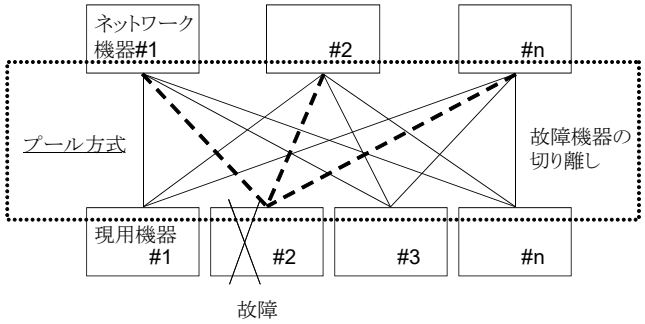
複数の現用機器に対して、現用と同一の予備機器を一つ設置し、現用機器のいずれかが故障時、プログラム制御で速やかに故障機器を予備機器に切替えるとともに、警報、ベル鳴動、ランプ表示、メッセージ出力により故障発生を保守者に通知する。



予備機器への切換え（ｎ＋１方式）

３　プール化方式の場合

複数の現用機器は、１つ以上の現用機器が故障となっても担える処理量で運用を行い、現用機器のいずれかが故障時、プログラム制御で速やかに故障機器を現用機器から除外し、他の現用機器で処理を続行する。故障となった機器においては、警報、ベル鳴動、ランプ表示、メッセージ出力により故障発生を保守者に通知する。



予備機器への切替え（プール化方式）

(5)　故障等の通知、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し、通報する機能を設けること。

解説

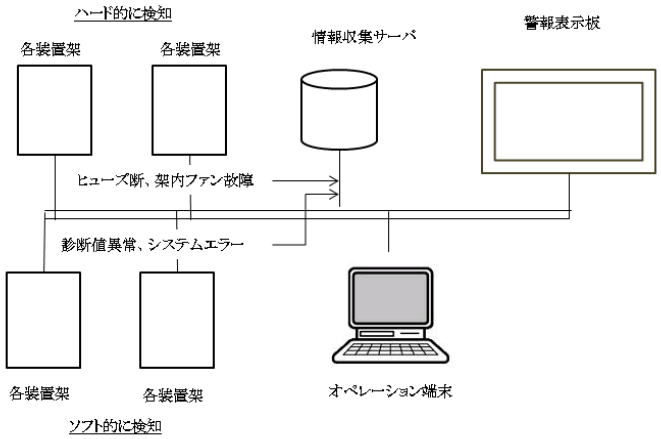
重要な設備の故障及び設備の機能障害が発生した場合、その故障等の発生を速やかに検知、通報する機能を設ける。

●措置例●

交換機の検知機能の例として次のものがある。

ハードウェア：供給電源断の検知、設備架内ファン故障の検知

ソフトウェア：プログラム及びデータ類の正常性チェック、処理時間のチェック



故障等の検知、通報例

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。

解説

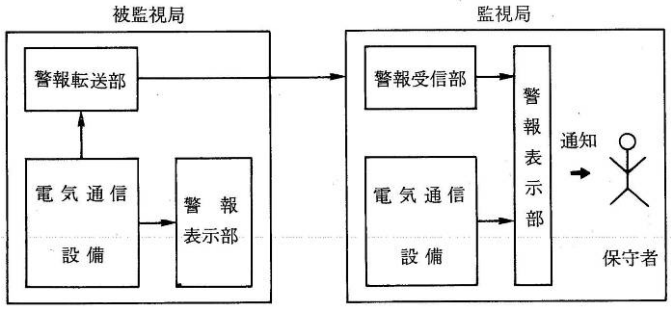
無人施設の重要な設備においては、設備の故障等を検知した場合、速やかに通報する遠隔通報機能を設ける。

「これに準ずる措置」とは、定期的巡回等の措置をいう。

●措置例●

検出した故障警報は、警報表示のベル、ランプ等により可視・可聴表示して保守者に通知する。

故障警報の一般的な転送系統を図に示す。



故障警報の転送

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。

解説

設備の故障等を検知した場合、ハードウェア又はソフトウェアによって、故障等の箇所の識別を行う機能を設ける。

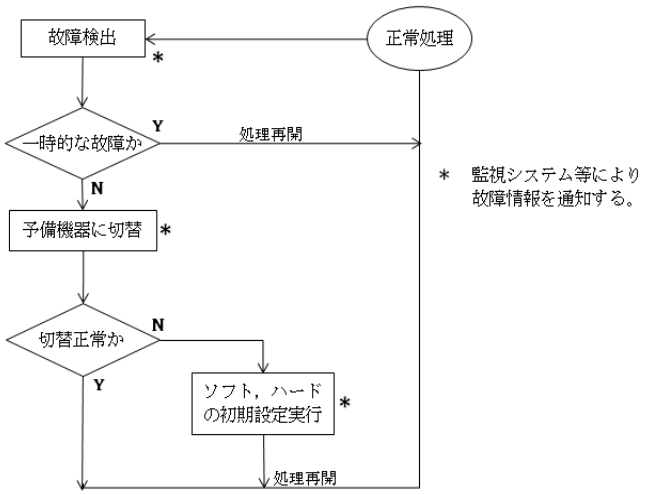
●措置例●

１　交換設備

正常運転動作中に設備の故障が発生すると、交換機では、ハードウェアとソフトウェアの連携動作によって自動的に故障装置を検出し、予備装置への切替を行って正常運転の連続性を確保する。

また、故障装置内部の故障箇所を限定するために、診断プログラムが用意されており、これは保守者の操作（コマンド投入）により起動される。

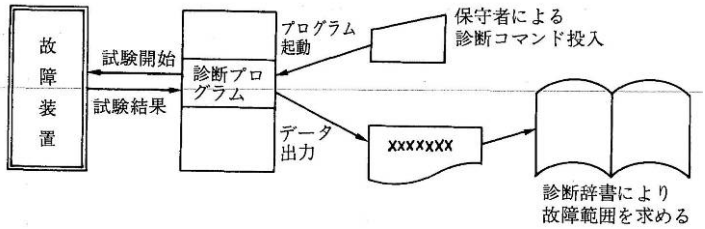
①　故障検出時の処理の流れ



故障検出時の処理の流れ

② 手動診断

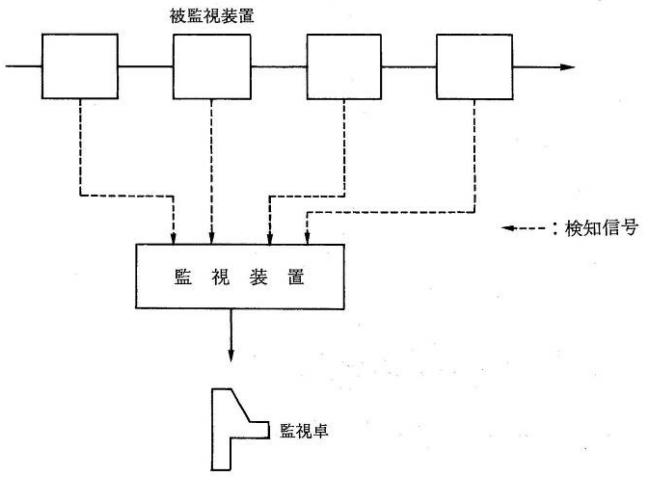
故障情報により故障装置を判定し、保守者の診断コマンド投入操作で故障装置内部の故障位置を限定する。さらに、この故障位置を限定するために診断コマンド投入後の出力データに基づいて故障位置を求めるためのマニュアルを用意する。



手動診断概念図

2　伝送設備

被監視装置毎に警報線により、パラレル信号を監視装置に引込む方法と、被監視装置の警報をシリアル信号に多重化し監視装置に引き込む方法がある。監視卓のマンマシンインターフェースとしては、ランプ、LED、CRT、ラインプリンタ等がある。



伝送設備の故障個所の識別

(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。

解説

設備の点検や故障箇所の探索等の機器試験を行うため、試験機器の適切な配備の措置、又はこれに準ずる措置を講じる。

「これに準ずる措置」とは、試験機器の配備は設備の工事、維持又は運用を行うセンターごとに行うのが原則であるが、使用頻度が少ない試験機器、特殊な用途に使用する高価な試験機器等については、複数のセンターの試験機器を一か所に集中配備できることを意味している。

試験機器は、各種の規格が満足されているか否か、相手側との互換性があるか否か等を判別可能なものであり、配備数は設備の重要度、試験機器の使用頻度等により決定する。また、測定器等においては、その校正周期等を定め、管理を実施する。

(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。

解説

重要な屋内設備において故障が発生した場合、速やかに正常機器に置換できるよう予備機器の適切な配備を行う。予備機器の配備区分及び数量は、設備の重要度、現用装置数、故障発生率、復旧時間等を考慮して決定する。

「これに準ずる措置」とは、多数の同一機器により負荷分散を行い、特に予備機器がなくともいずれかの機器の停止時には、残りの機器によって全体としての機能を確保できる場合、予備機器の配備にあたって複数の事業場の予備機器を一か所に集中配備している場合等をいう。

特に、0AB～J 番号を使用する電話システム等の重要なサービスに使用する呼制御サーバは、予備機器の配備を行い、障害時やふくそう時にサービスを継続できる構成とする。

配備区分

１　集中配備……使用頻度の少ないものについて地方ごとに場所を選定して集中的に配備するもの。

２　専用配備……各交換局所等で専用して使用するもの。

３　共用配備……各交換局所等で共用して使用するもの。

(8)　電気通信設備を設置する場所の提供を受けている電気通信設備の保護

他の電気通信事業者のビルに電気通信設備を設置する場所の提供を受けている全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。

解説

事業用電気通信設備を収容し、又は設置する通信機械室、コンテナ等及びとう道において、他の電気通信事業者に電気通信設備を設置する場所を提供する場合（以下「コロケーション」という。）は、当該電気通信設備が発火等により他の電気通信設備に損傷を与えないよう措置されたものであることを当該他の電気通信事業者からその旨を記載した書面の提出を受ける方法その他の方法により確認しなければならないことが定められている。

このため、コロケーションサービスを提供する事業者は、設備を設置する者から書面の提出を受ける等により電気通信設備に損傷を与えないよう措置されていることを確認する。

一方、コロケーションサービスを受ける者は、発火・発煙の防止等の安全・信頼性が確保されるよう適切な措置を講じる。

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必要な電力を安定的に供給できること。

解説

　電源設備（受電設備、整流装置、定電圧定周波数装置（CVCF）、コンバータ装置等、商用電源又は発電設備等から電力を受電して交換設備等の電気通信設備へ電源を供給するまでに必要な設備）については、負荷の性質や最大負荷を明確にし、全ての通信設備の最大需要電力を確保する。電源設備の供給能力は、常に各負荷設備の所要電力を安定的に供給できるものとする。負荷設備の消費電力が変動する場合、ピーク時にも負荷設備が正常に動作できる容量を確保する必要がある。

　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。

解説

　通信本体系設備の許容限度内に維持するよう電圧、周波数の制御を行う。
　電源設備の故障や負荷の変動に伴う電圧降下や周波数の変動に対して、適正な制御を行い、電源の安定供給を図る。

●措置例●

　交流電源装置としては、交流入力電源の停電に際し、負荷電力の連続性を確保することのできる無停電電源システム（UPS）を使用する。

(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、故障等の発生を防止する措置を講ずること。

解説

　電源設備の停止は、電気通信設備の機能停止につながるため、通常想定される規模の地震（震度５強程度）の震動に対して給電系統、燃料、冷却水、排気の系統等が十分蓄えられる構造とする。

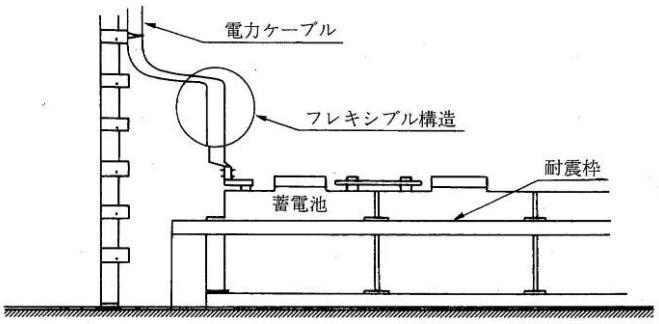
●措置例●

１　給電系統

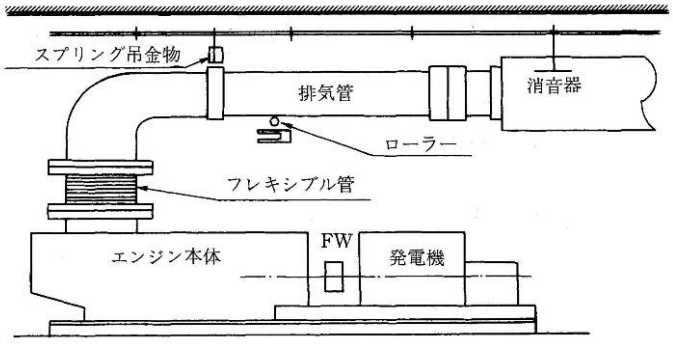
　振動系の異なる装置を結ぶ給電系統は、適切な箇所で余長又はフレキシブルな構造を採用し、振動を吸収する。

２　エンジン発電機等

　エンジン発電機につながる燃料、冷却水、排気系統の配管は地震やエンジン運転の振動による折損等の故障の発生を防止するため、三軸方向にフレキシブルな構造とする。



蓄電池の配線例



エンジン排気管の施行例

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

障害が発生した場合、電気通信サービスや自己の業務に重要な影響を及ぼすおそれのある電気通信設備に電力を供給する電源設備については、直下型地震又は海溝型巨大地震に起因する高レベルの地震動に対して給電系統、燃料、冷却水、排気の系統等が十分耐えられることを目標とした耐震構造とする。具体的には、最近における最大規模の地震である阪神･淡路大震災及び東日本大震災の規模が目標となる。

(3)　雷害対策 雷害が発生するおそれがある場所に設置する重要な設備に電力を供給する電源設備には、雷害による障害の発生を防止する措置を講ずること。

解説

電力線は雷サージに対してインピーダンスが低く、雷サージが流れやすいため、接地系設備の連接やアレスタの挿入などを検討する。

●措置例●

1　局内接地系の連接による同電位化を図る。
2　装置間の電位差を最小にするために、関連装置間の接地を最短接続する。
3　アレスタを挿入する。
4　電力線への耐雷トランス設備を検討する。

(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、保護装置等の設置等の措置を講ずること。

解説

電源設備は、過電流による加熱や漏電等による火災の危険があり、エンジン等可燃物を扱う装置もあることから、十分な火災対策を講じる。

●措置例●

1　保護装置の設備
　①　装置、部品等の故障による加熱を防止するため、適切な保護装置を設置する。過電流リレー、電力ヒューズ．MCCB（配線用遮断器)、温度警報装置等
2　ケーブル等の対策
　①　過電流による加熱等で、電力ケーブルが焼損することの無いよう、難熱化の措置を講ずる。
　②　大電流ケーブル近隣にある構造物は耐熱不燃性の材料を用い、過電流によ

る加熱等への配慮を行う。

③　電力ケーブル等の床、壁の貫通部は防火処置を行う。

3　受変電設備等

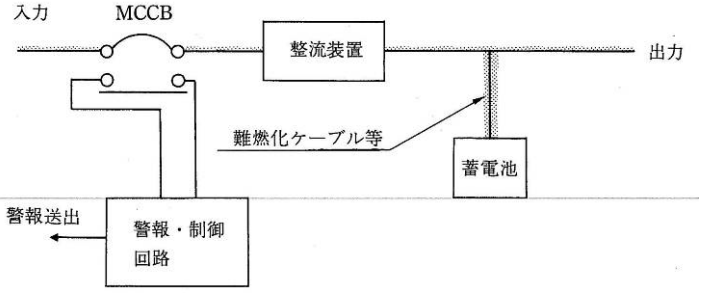
①　商用電源の受変電設備等は、万一、発火した場合でも他の設備への延焼を防止するため、キュービクル等安全性の高い構造のものを使用する。

②　高湿度環境で使用する電源設備は、漏電による火災を防止するため、防湿構造とするか、漏電遮断器を設置する。

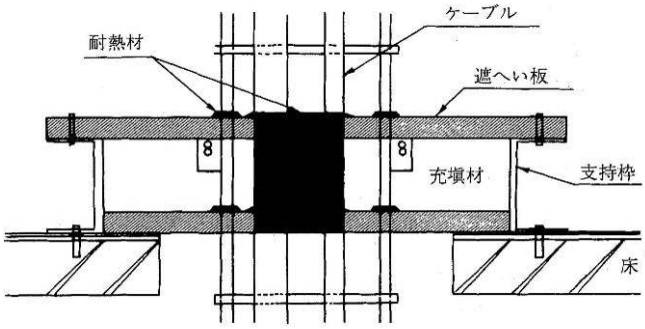
例 とう道配電設備

4　蓄電池設備

蓄電池設備は、万一発火した場合でも他の設備への延焼を防止するため、難燃性の電槽・蓋を使用する等の措置を講ずる。



電源設備の保護装置例



床貫通部の防火装置例

(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。

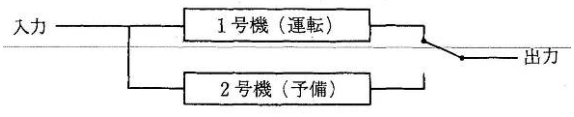
解説

重要な設備に電力を供給する電源設備においては、電源設備を構成する機器は２重化又はｎ＋１等の冗長構成とし､信頼性の向上を図る｡｢これに準ずる措置｣とは、電源設備の整流器等の故障に対処し蓄電池を設置すること等をいう。

●措置例●

1　待機冗長運転方式

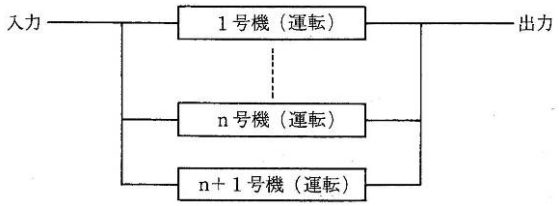
常時は現用機から負荷に電力を供給し、現用機が故障のときは、予備機に切替える方式である。



待機冗長運転方式

2　並列常用冗長運転方式

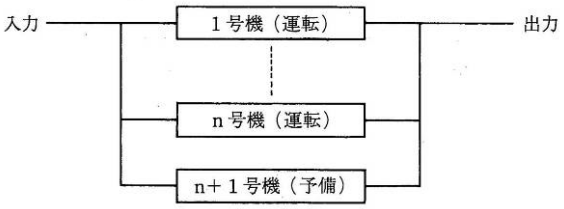
本方式は、ｎ台分の装置の容量を必要とする負荷に対し、（ｎ＋１）台で運転し、いずれか１台が故障しても電力供給を可能とする方式である。



並列常用冗長運転方式

３　待機形並列常用冗長運転方式

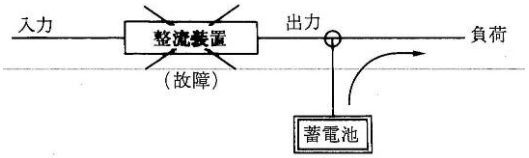
本方式は、ｎ台分の装置の容量を必要とする負荷に対し、（ｎ＋１）台分の装置構成で、常時はｎ台で運転しており、故障時には予備機が運転を開始する方式である。



待機形並列常用冗長運転方式

４　蓄電池の設置例

整流装置が故障した場合、蓄電池から瞬断なく電力を供給する。



蓄電池の設置

(6)　故障等の検知、通報

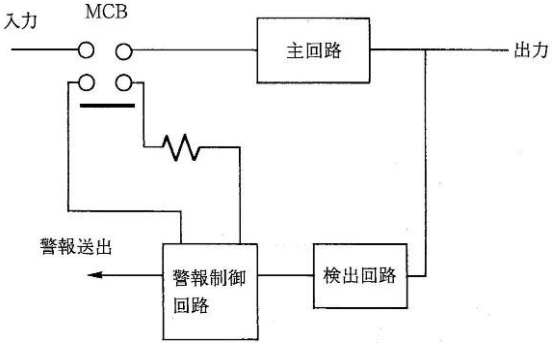
ア　電源設備の故障等、ヒューズ断又は停電の発生を速やかに検知し、通報する機能を設けること。

解説

電源設備の故障、ヒューズ断及び停電が発生した場合、速やかに検知、通報する機能を設ける。

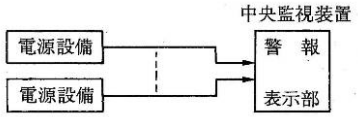
●措置例●

出力電圧異常等を検出回路によって検出し、警報制御回路によって故障装置を系から切離すとともに、外部にその警報を送出する。



電源設備の故障検出例

故障時にはベル・ランプ等により可視・可聴表示して保守者に通知する。



電源設備の故障検知

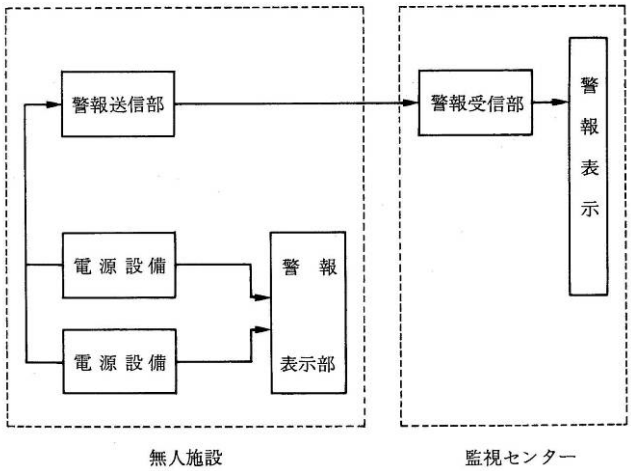
イ　重要な設備を収容する無人施設の電源設備には、遠隔通報機能を設けること。ただし、これに準ずる措置を講ずる場合は、この限りでない。

解説

重要な設備を収容する無人施設の電源設備においては､遠隔通報機能を具備する。「これに準ずる措置」とは、定期的巡回等の措置をいう。

●措置例●

電源設備の警報をまとめ、保守者のいる監視センターに転送する。



無人施設の電源設備の遠隔通報

(7)　停電対策

ア　次のいずれかの措置を講ずること。

①　自家用発電機を設置すること。

②　蓄電池を設置すること。

③　複数の系統で受電すること。

④　移動電源設備を配備すること。

解説

次の①～④のいずれかの措置を講ずる。なお、山上の無線中継所においては停電状況が都市部に比べて悪いこと、保守担当事業所からの早急な駆けつけが困難なこと等を勘案して長時間の連続運転が可能な予備発電装置を設置する。

また､豪雪地域や台風常襲地域等の自然災害の影響を受けやすい地域で保守担当事業所からの駆けつけが困難な交換局・コンテナ局等においては蓄電池の増容量、可搬型発電機の配備を行い、長時間停電に備える。

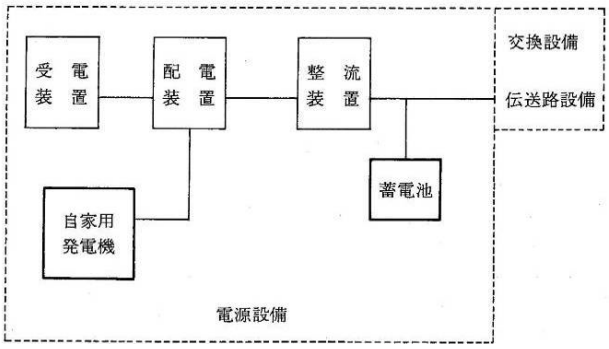
その他、自家用発電機、蓄電池等の予備電源設備の供給時間は、基本的には、設備の重要度、電源設備の故障頻度等の要因を考慮して定める。

①　停電時に電源を確保するため、自家用発電機を設置する。また自家用発電機の容量は、空気調和設備等の負荷を考慮した容量とする。自家用発電機の燃料については、十分な量を備蓄しておくか、補給手段を明確にしておく。

●措置例●

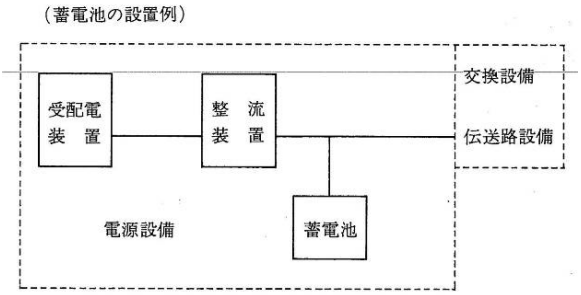
通常は商用電源を受電し、交換設備、伝送路設備に電源を供給するが、商用電

源停電時においても通信が停止することがないよう自家用発電機を設置する。
※停電後、自家用発電機を運転開始し電力供給を行う。
なお、自家用発電機が運転するまで蓄電池より給電を行う。



自家用発電機の設置例

② 停電時に電源を確保するため、蓄電池を設置する。
●措置例●
通常は商用電源を受電し、交換設備、伝送路設備に電源を供給するが、商用電源停電時においても通信が停止することがないよう蓄電池を設置する。
（蓄電池の設置例）



※停電時は蓄電池から瞬断なく電力を供給する。
蓄電池の設置例

③ 経路の異なる変電所より複数系統で受電する構成とする。
可能な場合には、異なる変電所等から異経路で受電することにより、商用電源の停電に対処する。なお、異系統受電は該当の電力会社によっては困難な場合があるので、事前に該当電力会社と協議する必要がある。

④ 電源設備の故障及び停電の発生時における電源確保のため、移動電源設備を配備する。配備にあたっては、以下の点に留意する。但し、移動電源設備を配備するまでの間は、蓄電池等により電源を確保しておく必要がある。
- 受配電設備には移動電源設備の給電用ケーブル接続部を設けておくこと。
- 移動電源給電用接続部も定期点検を行うこと。
- 移動電源設備及び移動電源設備に給油するためのタンク等の屋外設置スペースを確保し、かつ、そのスペースの清掃を行っておくこと。
- 移動電源設備の給電容量は、整流装置や空調装置等で停電等発生時に必要となる設備に給電できる容量であること。
- 移動電源系統の電力確保については、関係法規等に準拠し、作業者の安全については特に考慮すること。

イ 交換設備については、自家用発電機及び蓄電池の設置その他これに準ずる措置を講ずること。
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。

エ　自家用発電機の設置又は移動電源設備の配備を行う場合には、その燃料等について、十分な量の備蓄又はその補給手段の確保を行うこと。
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。

解説

イ　交換設備については、停止による通信への影響が大きいことから、長時間の停電対策として、適切な容量をもつ蓄電池の設置に加え、燃料の供給体制が確保される限り継続的に給電可能な自家用発電機による予備電源の２系統化若しくはこれに準ずる措置を実施し、停電に対する交換機の停止を回避する。

ウ　電源の安定的確保を図る観点から、移動体通信基地局の無停電化やバッテリーの長時間化の推進策として、蓄電池の設置に加え、移動電源設備又は予備蓄電池を配備し、基地局への給電または蓄電池への充電若しくは蓄電池の交換を行う。

また、地下鉄の構内など予備電源設備等のスペースが限られている箇所においては、共同設置など他の事業者と積極的に連携をとることが適当である。

エ　大規模災害時における広域・長時間の停電に備え、自家用発電機または移動電源設備に必要な燃料や、発動発電機の冷却に必要な水を備蓄し、又はその供給体制を予め確保する。具体的に、燃料については石油会社との間で災害時における優先給油契約等を締結することが望ましい。

オ　設備の重要度に応じて十分な規模の予備電源を確保できるよう、適切な建物やコロケーションスペースの選定、自前の予備電源の設置などの対策を講じる。

カ　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少なくとも 24 時間にわたり停止することを考慮すること。ただし、通常受けている電力の供給が 24 時間にわたり停止した場合であつても、他の端末系伝送路設備により利用者が当該端末設備を用いて通信を行うことができるときは、この限りでない。

解説

東日本大震災で発生した停電の規模は想定を超え、広範囲かつ長時間に及んだため、都道府県庁等の防災上必要な通信機能の維持に係る電気通信回線設備について特に長時間の停電を考慮した対策を講じることとしたものである。

また、令和元年房総半島台風においては、更に長時間の停電が発生したことに伴い、長時間にわたり通信サービス断となった。そのため、電気通信事業者による停電対策の取組状況等を踏まえ、都道府県庁等の防災上必要な通信機能の維持に係る電気通信回線設備について、少なくとも「24 時間」にわたる停電を考慮した対策を講じることとしたものである。具体的な措置として、自家用発電機や蓄電池の追加設置、移動電源車の配備等が考えられるが、追加整備にかかるコストや設置場所の耐荷重等物理的な制約も加味し、技術的な難易度等を考慮して段階的に実施されるべきである。

なお、この規定における「都道府県庁等」とは、事業用電気通信設備規則第 11 条第３項に記載されている「都道府県庁、市役所、特別区の区役所又は町村役場の用に供する主たる庁舎」を指し、「他の端末系伝送路設備」とは、当該端末で通信可能な別周波数帯を利用する別の端末系伝送路設備や近くにある別の端末系伝送路設備などを指す。

（令和２年度告示改正により「また、」の段落を追加し「なお、」の段落を改正）
（令和６年度設備規則改正により「特別区の区役所」を追加）

キ　人の生命及び身体の安全の確保のために必要な通信を確保するため、災害拠点病院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少なくとも 24 時間にわたり停止することを考慮すること。ただし、通常受けている電力の供給が 24 時間にわたり停止した場合であつても、他の端末系伝送路設備により利用者が当該端末設備を用いて通信を行うことができるときは、この限りでない。

解説

人命に関わる対応の優先度は災害発生時においても高く、被災現場における医療活動の拠点となる「災害拠点病院」は「防災基本計画」（令和２年５月 29 日中央防災会議決定）上にも明記されているとおり重要である。そのため、人の生命及び身体の安全を確保するために必要な通信を行えるようにするため、災害拠点病院の通信機能の維持に係る電気通信回線設備について、少なくとも「24 時間」にわたる停電を考慮した対策を講じることが望ましいとしたものである。

なお、「他の端末系伝送路設備」とは、当該端末で通信可能な別周波数帯を利用する別の端末系伝送路設備や近くにある別の端末系伝送路設備などを指す。

（令和２年度告示改正により新規追加）

ク　防災上必要な通信を確保するため、大規模な災害の対策の拠点として機能する都道府県庁の用に供する主たる庁舎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少なくとも 72 時間にわたり停止することを考慮すること。ただし、通常受けている電力の供給が 72 時間にわたり停止した場合であつても、他の端末系伝送路設備により利用者が当該端末設備を用いて通信を行うことができるときは、この限りでない。

解説

大規模な災害において対策拠点となる都道府県庁の用に供する主たる庁舎の防災上必要な通信機能の維持に係る電気通信回線設備については、さらなる対応として、少なくとも「72 時間」にわたる停電を考慮した対策を講じることが望ましいとしたものである。

なお、「他の端末系伝送路設備」とは、当該端末で通信可能な別周波数帯を利用する別の端末系伝送路設備や近くにある別の端末系伝送路設備などを指す。

（令和２年度告示改正により新規追加）

ケ　防災上必要な通信を確保するため、離島又は半島地域に所在する市役所又は町村役場の用に供する主たる庁舎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少なくとも 72 時間にわたり停止することを考慮すること。ただし、通常受けている電力の供給が 72 時間にわたり停止した場合であつても、他の端末系伝送路設備により利用者が当該端末設備を用いて通信を行うことができるときは、この限りでない。

解説

災害時において、現場への到達までに時間がかかる離島や令和６年能登半島地震で、離島と同様に地理的制約により現場への到達までに時間がかかることが判明した半島地域の市役所又は町村役場の用に供する主たる庁舎の防災上必要な通信機能の維持に係る電気通信回線設備については、さらなる対応として、少なくとも「72

時間」にわたる停電を考慮した対策を講じることが望ましいとしたものである。

なお、「半島地域」とは、半島振興法（昭和 60 年法律第 63 号）第２条で指定された半島振興対策実施地域を想定しているが、当該地域以外の半島地域における停電対策の実施を妨げるものではない。

また、「他の端末系伝送路設備」とは、当該端末で通信可能な別周波数帯を利用する別の端末系伝送路設備や近くにある別の端末系伝送路設備などを指す。

（令和２年度告示改正により新規追加）

（令和６年度告示改正により半島地域の記載を追加）

コ　防災上必要な通信を確保するため、災害応急対策を実施する国の行政機関又は国の地方行政機関の用に供する主たる庁舎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少なくとも 72 時間にわたり停止することを考慮すること。ただし、通常受けている電力の供給が 72 時間にわたり停止した場合であつても、他の端末系伝送路設備により利用者が当該端末設備を用いて通信を行うことができるときは、この限りでない。

解説

災害時において、災害応急対策を実施する国の行政機関又は国の地方行政機関の用に供する主たる庁舎の防災上必要な通信機能の維持に係る電気通信回線設備については、少なくとも「72 時間」にわたる停電を考慮した対策を講じることが望ましいとしたものである。

なお、「国の行政機関」又は「国の地方行政機関」とは、それぞれ災害対策基本法（昭和 36 年法律第 223 号）第２条第３号に規定する指定行政機関又は同条第４号に規定する指定地方行政機関を指す。

また、「他の端末系伝送路設備」とは、当該端末で通信可能な別周波数帯を利用する別の端末系伝送路設備や近くにある別の端末系伝送路設備などを指す。

（令和６年度告示改正により新規追加）

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　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（ハザードマップ等）を考慮し、電気通信設備の設置場所を決定すること。

解説

これまで地方公共団体が定める防災に関する計画（地域防災計画）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（ハザードマップ）を考慮する観点がなかったため、新たにこれらを考慮して、電気通信設備の設置場所を決定することとしたものである。

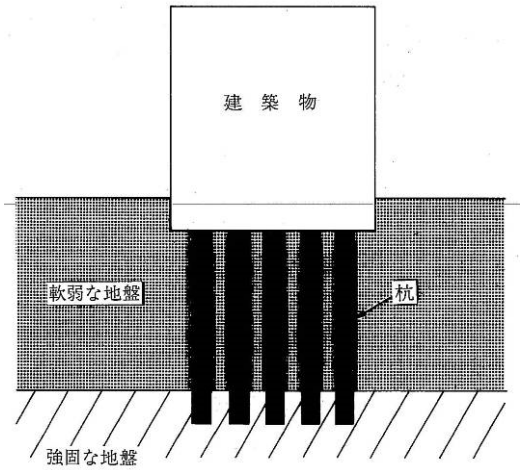
イ　強固な地盤上の建築物を選定すること。ただし、やむを得ない場合であつて、不同沈下を防止する措置を講ずる場合は、この限りでない。

解説

地震等の災害を考慮して、強固な地盤上の建築物を選定する。やむを得ず軟弱な地盤上に設置しなければならない場合は、パイル打設、地盤改良等の不同沈下（構造物の各部で不均一な沈下を生じる現象）防止措置を行った後、建築物の建設を行う。あるいはそのような措置が講じられている建築物を選定する。

●不同沈下防止措置●

地盤改良は困難な場合が多いので、一般には強固な地盤まで杭（パイル）を打設する。



不同沈下防止装置

ウ　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つて、防風、防水等の措置を講ずる場合は、この限りでない。

解説

風水害等の被害を受けにくい場所を選定する。やむを得ず風水害等の被害を受けやすい場所に建築物を設置又は既存建築物を利用する場合は防風措置や防水措置を講じる。

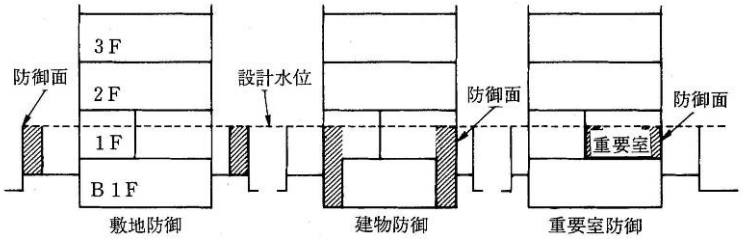
●防水措置の例●

過去の浸水高水位及び潮汐現象並びに自然環境、土地利用計画等から設計水位

を決定し、この水位に対して下記の措置をとる。

・　敷地かさ上げ、高床式、その他適切な方式とする。
・　設計水位以上に開口部を設ける。
・　設計水位以下の開口部を防水（潮）板で防御する。
・　流木等による、防御機能の破壊を回避できるよう考慮する。
・　外壁の防水性能の保持をはかり、各種配管の建物内への引込みは、設計水位以上に立上げるか、もしくは外壁貫通本数の集約、集中化をはかり水密性能を高め、点検できるよう考慮する。

排水系統には、防潮弁を設ける。



水害対策の例

なお、塩害対策が必要な場合は塩害の度合を調査し、その程度に応じた対策を施すこと。

エ　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つて、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。

解説

強力な電界、磁界による設備障害のおそれのある場所への建築物の設置は、極力回避する。やむを得ず当該地域に建築物を設置又は既存建築物を利用する場合は、通信機械室にシールド等の措置を講ずる。

オ　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。

解説

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。

●措置例●

１　ガスタンク等の危険物に隣接した場所は回避する。
２　多量の可燃物や危険物を収納する施設が隣接した場所は回避する。

(2)　建築物の選定

ア　耐震構造であること。

解説

建築物は、耐震構造とし、地震の発生時に建築物の倒壊や破壊等による設備への被害及び従事者への危険を防止する。

又、地震等による内壁、天井等への剥離、倒壊によって、設備及び保守、運用者等に危険がないよう措置する。

●措置例●

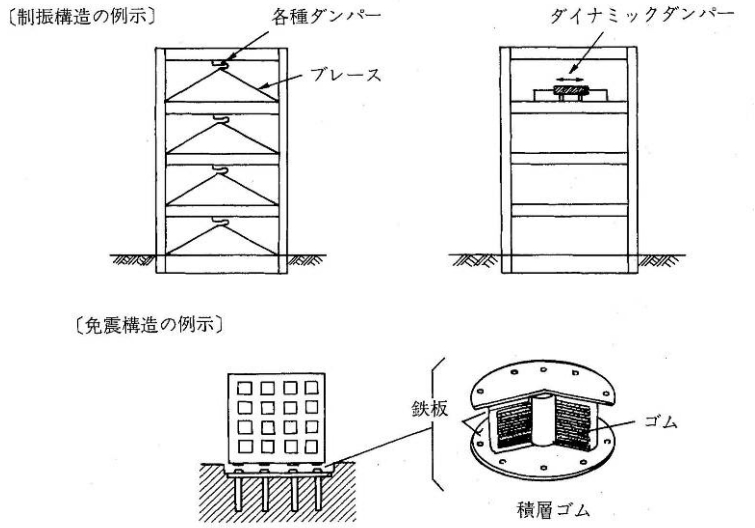
１　耐震構造

建物は、鉄筋コンクリート造、鉄骨鉄筋コンクリート造又は鉄骨造とし、建築基準法施行令に規定された方法により構造計算を行って地震に対して安全に

設計する。
また、建物内部での地震の揺れを考慮した制振・免震構造の採用も考えられる。

２　内壁・天井等の剥離、倒壊の防止

既製間仕切壁、ライン天井など地震時に転倒・落下のおそれのある内装材は、ボルト、ブレース等により、構造体に固定する。



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。

解説

建築物は耐火建築物又は準耐火建築物とし、火災の発生時に、建物全体への延焼を防
止し、近隣火災からの類焼を防止し、設備への被害及び従事者への危険を防止する。

●措置例●

１　内壁、天井等は、不燃材料又は準不燃材料を使用し、適切な防火区画を設けることにより、火災発生時の延焼を防止する。

２　建物外周壁は、近隣からの火災による類焼のおそれが全くない場合を除き、十分な耐火性能を有する構造とし、開口部は防火シャッター、鉄扉などそれらに見合った性能の防御方法を講ずることが望ましい。

３　防火シャッター等は、ヒューズ装置又は火災感知器により、火災時に自動閉鎖する構造とすることが望ましい。

ウ　床荷重に対し、所要の構造耐力を確保すること。

解説

設備重量を十分に考慮した床荷重に対して必要な構造耐力を確保する。

１　床荷重

通信用設備、空気調和設備等を収容する部分の床荷重は、各設備の重量及び配置に基づき、床用、大ばり・柱・基礎用及び地震力計算用の各々について適切に設定する。

２　構造耐力

建物の床構造、柱・はり及び基礎は、上記の床荷重に対して安全であることを構造計算により確認する。

(3)　入出制限機能

ア　建築物の出入口には、施錠機能を設けること。

解説

出入口には施錠機能を設ける。

●措置例●

1　出入口の扉は、建築基準法施行令第 112 条第 1 項に規定される特定防火設備、防火戸等、防犯上、防火上十分な性能を有するものを使用し、施錠機能を設ける。扉の錠は、非常時においても、従事者の安全を考慮し、屋内から鍵を用いることなく、解鍵が容易な機能を有しているものとする。また、自動扉の場合は､停電時においてもバッテリー等により開閉可能なものとする。

2　受付と出入口が離れている場合はリモートロックが可能な錠を設備し、モニターテレビとインターホンにより入出制限を行う。

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。

解説

建築物の通常利用する出入口には、受付や監視装置等の入出管理機能を設ける。「これに準ずる措置」とは、通信機械室に入出管理機能を設ける措置をいう。

●措置例●

1　通常利用する出入口は１カ所とし、警備員を配置する。出入口では入出管理が可能な受付を設ける。

・　入退館者の識別及び記録を行う。
・　インターホン等による非常時の担当部門への連絡
・　持ち込み物品及び持ち出し物品の確認。
・　出入口のリモートロック

2　主要出入口の入退出は､電気錠を使用した入出管理装置により入退館資格を識別し､記録及び扉の開閉を行うことが望ましい｡また､入出管理装置は､技術の進展に沿って適時見直すことが望ましい。

入出管理装置例：

①　磁気カード装置　磁気カードをカードリーダーに挿入して解錠する。
②　ホログラムカード装置　レーザー光で刻印したカードをカードリーダーに挿入して解錠する。
③　ICカード　プラスチックカードにICチップを内蔵させたカードで、磁気カードに比べ記憶容量が非常に大きく､偽造や不正使用が難しく、情報の機密保持性、安全性が極めて高い特徴がある。カードリーダーで読み取り解錠する。
④　電磁波カード装置　カードをセンサーに近づけることにより解錠する。
⑤　暗証番号入力装置　プッシュボタンにより暗証番号を入力し解錠する。
⑥　生体認証装置　登録された掌形、掌紋等の生体情報を識別し解錠する。

3　監視用テレビシステム等を設置し、重要区画、主要出入口の監視を行う。

4　重要な設備を収容する建築物においては、必要に応じて防犯警報装置を設置する。

防犯警報装置例：

① マグネットスイッチ：磁気の動作により窓や扉の開閉を感知する。
② 赤外線感知器：侵入者が赤外線ビームを遮断することにより検知する。
③ 振動感知器：ガラス面等に接着しておき破壊時の振動を検知する。
④ トラップセンサー：塀や柵等に取り付けて張力や電流の変化により乗り越え、切断等を検知する。

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。

解説

電気通信設備を保守・維持・運用する者以外の者が、みだりに施設に入室して事業用電気通信設備を操作して、運用を妨げたり通信の秘密を侵したりすることがないよう、各々の領域のセキュリティのあり方について適切な基準を設定し、運用することが必要である。

(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。

解説

火災の発生を速やかに検知し、通報を行う自動火災報知設備を適切に設置する。

●措置例●

1 センターの建築物には、消防法施行令による自動火災報知設備を設置する。
2 消防法施行令により設置除外となる延面積1,000㎡未満又は地階、無窓階、3階以上の床面積300㎡未満の建築物に対しても設置する。
3 コンテナ等については消防法施行令により設置除外となるが、消防法施行令に準拠した自動火災報知設備を設置する。
4 無人建築物及びコンテナについては、火災発報信号を保守担当が常駐する有人建築物に送信する設備を設ける。

関連法規：消防法施行令第21条
消防法施行規則第23条、24条、24条の2

イ 消火設備を適切に設置すること。

解説

火災発生時に被害を最小限に留めるため、センターの建築物には消火器等の消火設備を適切に設置する。

●措置例●

消防法施行令により設置除外となる延面積300㎡未満又は地階、無窓階、3階以上の床面積50㎡未満の建物についても消火器を設置する。

関連法規：消防法施行令第6条～第22条及び同施行規則他

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。

解説

自然災害時の影響を考慮し、又、外部より第三者が容易に侵入できないよう建築物内での適正な場所に通信機械室を設ける。

「第三者が容易に侵入できないような措置」とは、建築物の間仕切の構造が十分な強度を有する等、第三者が容易に侵入できないようにすることをいう。

●措置例●

イの具体例としては、外部者が多く出入りする玄関の付近、又はエレベーターホール付近などを避けることが考えられる。

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つて、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。

解説

やむを得ず浸水のおそれのある場所に通信機械室を設置する場合は、床のかさ上げ、防水壁等の措置を講ずるか又は排水設備を設置する。

●措置例●

１　建築物に風水害防止の措置がとられていても、風害時には想定外の漏水、排水管又はその他の排水管からの水の逆流などが発生する。これに備えるために、土嚢、排水ポンプ等の応急資材を保有しておく。

２　通信機械室に対し、事務室や水を使用する施設が上階にある場合又は隣接する場合は、これらによる漏水、浸透水、火災時の消火用水等による被害が予想される。やむを得ず、このような配置関係をとる場合は、床（天井）、壁に防水措置を施す。

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つて、電磁シールド等の措置を講ずる場合は、この限りでない。

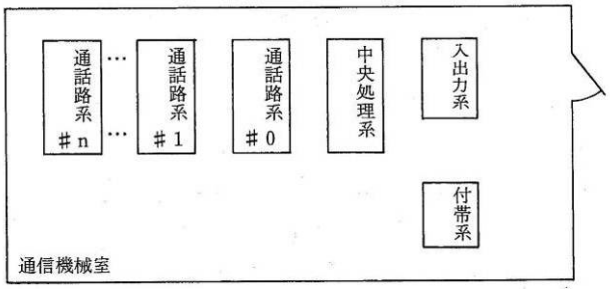
解説

強力な電界、磁界による設備障害のおそれのある場所には、通信機械室を設置しない。やむを得ず設置する場合は、電磁シールド等の障害防止措置を講ずる。

(2)　通信機械室内の設備等の位置
ア　保守作業を安全かつ円滑に行うことができる空間を確保すること。

解説

設備の設置、更改及び保守作業において、安全かつ円滑、迅速に作業が行えるよう必要な空間、通路を設け機器類を適正に配置する。



設備の配置例

関連法規：労働安全衛生規則第 543 条、544 条

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。

解説

1　じゅう器類を機械室へ設置する場合、強震動により転倒や移動を防止する措置を施す。

2　キャスター付移動台に搭載された試験機器は、通常想定される規模の地震により、移動、転倒しないよう係留する。

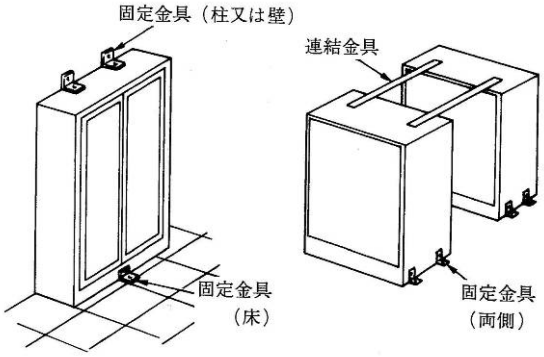
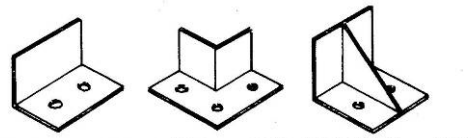


図　じゅう器類の転倒，移動防止装置



移動防止形耐震ストッパー

(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。

解説

重要な設備を収容する場合、構造上安全で、空気調和や保安管理等の容易さを考慮した専用の通信機械室を設ける。又､防火対策､効果的な空気調和などを考慮し、防火区画、消火設備区画、空気調和区画等をできるかぎり整合し、他室での事故や災害の影響を受けにくい専用通信機械室を確保する。

通信機械室に通じる通常の出入口には、入出管理、防塵等のための前室を設けることが望ましい。

イ　床、内壁、天井等に使用する内装材には、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。

解説

床、内壁、天井等に使用する内装品は、耐震措置を施し、落下又は転倒等の防止を図る。

●措置例●

１　既製間仕切壁、ライン天井など地震等に転倒、落下のおそれのある内装材は、ボルト・ブレース等により構造体に固定する。

２　フリーアクセス床は、一定の面積で区画し、区画線上の床をブレース等で補強することにより床剛性を高め、移動・転倒を防止する。

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。

解説

床、内壁、天井等に使用する内装材には建築基準法で定める不燃材料、準不燃材料又は難燃材料を使用する。

●措置例●

１　フリーアクセス床の主要部材、内壁及び天井には建築基準法、同施行令に規定された不燃材料を使用する。

２　カーテン、絨毯等は、消防法で規定する防災性能を有するものを使用する。

エ　静電気の発生又は帯電を防止する措置を講ずること。

解説

静電気の発生による電気通信設備への悪影響を防止するため、通信機械室においては静電気の発生と帯電を防止する措置を講ずる。

●措置例●

１　静電気の発生を抑制するため、温湿度を適切に維持する。

２　通信機械室の床材等に静電気の発生しにくい塩化ビニールタイル、高圧ラミネート、帯電防止カーペット等の材質を使用する。

３　床表面に静電気防止ワックス等の静電気防止剤を塗布する。

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。

解説

通信機械室に電源設備等を設置する場合であって、電磁界による影響のおそれがある場合には、シールド等の防止措置を講ずる。過電流の発生が著しい場合は、過熱しないようアルミニウム等のシールド材質を考慮する。

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。

解説

ケーブルが耐火構造又は防火構造の床又は壁面等の防火区画間を貫通する場合、火災による煙の侵入と延焼を防止するため、ケーブル貫通孔のすき間に不燃材料を充填する。

(4)　入出制限機能

ア　出入口には、施錠機能を設けること。

解説

第２　環境基準　１　センターの建築物（3）入出制限機能 アの項参照

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。

解説

第２　環境基準　１　センターの建築物（3）入出制限機能 イの項参照

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。

解説

第２　環境基準　１　センターの建築物（3）入出制限機能 ウの項参照

(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。

解説

システムデータ等の重要なデータを安全に保管できるよう、施錠機能を具備したデータ保管室又は専用のデータ保管庫を設置する。

データ保管室は、防火区画が設けられている場合は、防火区画内に設ける。データ保管室に設けない場合はデータを耐火保管庫に収容する。保管庫の設置に際しては、転倒防止等の耐震措置を講ずる。データ保管室及びデータ保管庫は、必要に応じ、電磁界による障害防止措置を講ずる。

●措置例●

１　データ保管室は、室名等の表示を行わない。入出管理を徹底し、不正行為を防止するため、専用の独立した部屋とする。

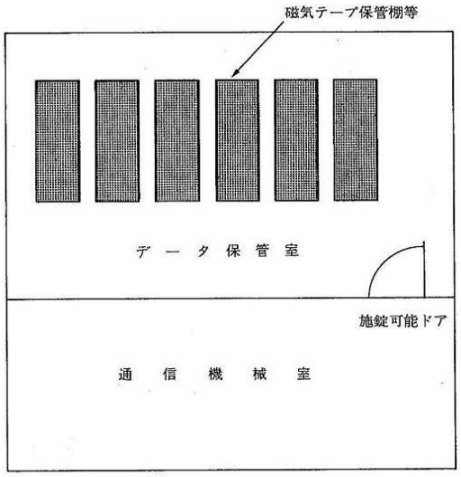
２　出入口の扉は十分な強度を持たせ、施錠機能を備える。

３　出入口は１か所とし、前室を設ける。

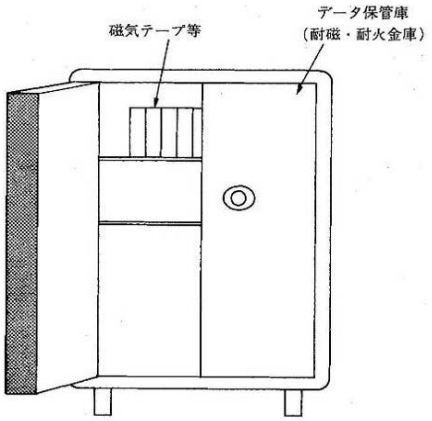
４　耐磁気措置を必要とする場合は、耐磁気保管庫を設置する。

５　データ保管室は、単独の防火区画とし、空調ダクト、扉、開閉部等も防火区画を形成する構造とする。

６　火災の検知、消火機能を有するデータ保管室である場合、データが適切に二重保管されている場合を除き、データを保管する金庫等は耐火措置を講ずる。



データ保管室の例



データ保管庫の例

(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。

解説

　消防法で定めるもののほか、重要な設備を収容する通信機械室においては、火災の発生を速やかに検知し、通報する自動火災報知設備を設置する。

　自動火災報知設備の警戒区画は、事務室等と通信機械室を区別することが望ましい。常時無人の通信機械室には、火災発報信号を保守担当者がいる部屋に通報する設備を設ける。

　イ　消火設備を適切に設置すること。

解説

　消防法で定めるもののほか、重要な設備を収容する通信機械室においては、火災発生時に水損を最小限に留めるよう不活性ガス消火設備等の消火設備を設置する。その他の消火設備の適用は消防法による。

関連法規：消防法施行令第６～22条及び同施行規則他

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。

解説

　通信機械室は、必要に応じ、空気調和設備により空気調和（空調）を行う。空気調和設備は、設備荷重を十分考慮して設置する。

　空気調和設備室を設ける場合は、通信機械室の温湿度適正保持のために必要な熱分配に支障のないよう、通信機械室近傍に配置する。また、室内に設置する空気調和設備の荷重に耐える構造とし、その占有スペースの他に、日常保守及び更改に支障のない面積と機器搬出入経路を確保する。

　ウ　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。

解説

　空気調和設備の設置に際しては、耐震措置を施し、設備の転倒を防止する措置を施す。

●措置例●

1　空気調和機（空調機）

①　空気調和機が移動、転倒しないよう床、壁又は天井の両方で固定する。

②　パッケージ形の空気調和機を機械室のフリーアクセス床に設置する場合はフリーアクセス床の補強を行うか、空気調和機の架台を建物床に固定する。

2　冷却塔、ポンプ、屋外機等

①　冷却塔等は、移動、転倒しないよう機器のコンクリート基礎に固定する。

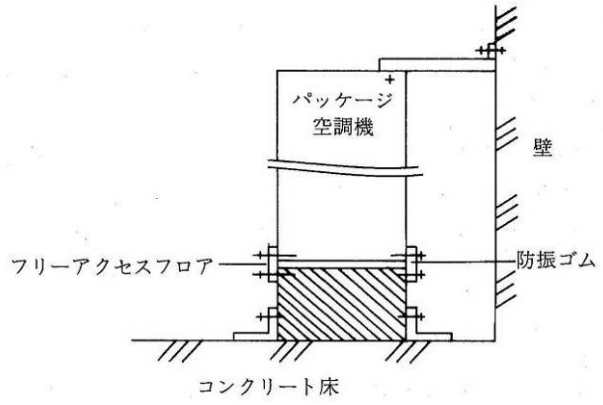
②　冷却塔の支柱は、十分な強度を有する。

③　防振支持されている機器には、耐震ストッパーを取り付ける。

3　配管、ダクト

①　地震による機器の振動等により損傷を生じないようフレキシブル継手（つぎて）を使用する。

②　壁、床に沿った配管、ダクトは、適切な間隔で触れ止めの耐震支持を行う。



パッケージ形空調機の設置例
（フリーアクセス床上設置の場合）

(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。

解説

出入口には施錠機能を設ける。

●措置例●

1　空気調和設備室の扉は防犯、防火上十分な強度を持たせ、施錠機能を備える。扉の錠は、非常時においても、従事者の安全のため室内から鍵を用いることなく解鍵が容易なものとする。

2　暗証番号入力装置やシリンダ錠を使用する。

(3)　空気調和の条件
ア　適切な設備容量とすること。

解説

外部環境及び設備の発熱量等を考慮し、適切な設備容量を確保する。

外壁貫流熱、日射、取入外気負荷等の外部環境に関わる負荷と設備の発熱、照明発熱等の建築物内部負荷とを加え合わせた空調負荷を計算し、最大負荷時に適切な温湿度を確保し得る空調容量とする。

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。

解説

温湿度及び空気清浄度を適正な範囲内に維持する。

温湿度制御を自動化し、温度勾配が高くならない等、きめ細かな制御を行う。

●措置例●

空調対象通信機械室において、気流などを考慮のうえ適当な位置に温度調節器及び湿度調節器を設置し、空調機の発停あるいは供給冷温水量などを制御し、冷却減温又は過熱を行う。また必要に応じて加湿器を設ける。これらにより温湿度を適正な範囲内に保持する。

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。

解説

通信機械室用空気調和設備は事務室用空気調和設備と別系統となる構成とする。やむを得ず他の室と共用する場合は、他室の温度変化等の影響を受けないよう措置する。

●措置例●

やむを得ず事務室又は他の機械室と共用で使用する場合は、事務室の塵あいが機械室に侵入することのないよう空気流の経路、フィルタ性能に考慮するとともに、負荷変動特性の異なる一方の室の温湿度変化などの影響が他方の室に及ぶことのないよう、それぞれの室温湿度調節が可能な制御機構を設ける等の措置を講ずる。

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。

解説

重要な設備を収容する通信機械室の空気調和を行う設備は、空気調和設備の故障による温湿度変化、特に室温上昇が、通信機器の機能維持に支障となるおそれがある場合には、通信機器の必要とする信頼性に適合する空気調和設備の信頼性を有するよう、冗長構成とする。

空気調和設備の信頼性を高めるために冷却機能要素を複数分割配置し予備の能力を用意する。これにより冷却が不足する確率を小さくする。

(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。

解説

寒冷地に設置する等、凍結のおそれのある場合は、ヒーター等により凍結防止措置を講ずる。

●措置例●

空気調和設備の冷却塔（水などの熱媒体を空気に触れさせて冷却する装置）は寒冷地の場合、凍結するおそれがある。その対策として次の方法がある。

1　水温が設定温度以下になった場合、自動的に電気ヒーターを作動させる。

2　配管部分を保温材でまく。さらに電気ヒーターを設置すれば、より効果的である。

3　温度の低下が軽度の場合は、ポンプを作動させ、凍結を防ぐ方法もある。

(5) 漏水防止

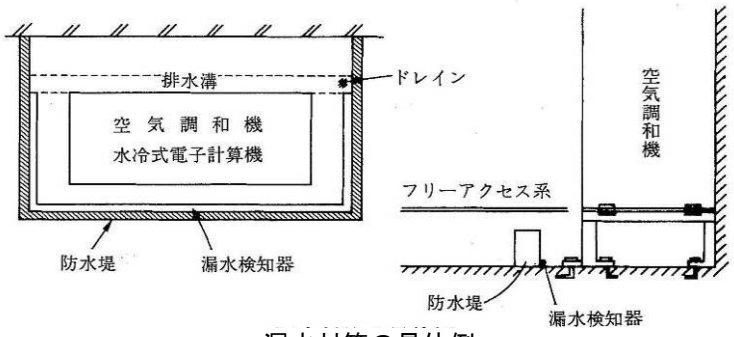
排水口等の漏水を防止する措置を講ずること。

解説

空気調和設備の故障による水漏れ又は空気調和設備の運転時に発生する結露水は、他の設備の故障の原因となる可能性が高いため、排水口等の漏水防止措置を講ずる。

●措置例●

空気調和設備の故障による水漏れ又は空調冷房運転時に発生する結露水は、床面に流れると直下階に落下し、通信機械を水損させることが考えられる。これを避けるため空気調和設備室は、床防水を施し、防水堤を備え、かつ排水口を設ける他漏水検知設備を備える。



漏水対策の具体例

(6)　有毒ガス等

腐食性ガス（SO_2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。

解説

設置環境条件等によって、腐食性ガス（SO_2等）や粉塵が混入してくるおそれがある場合は、それらを触媒、フィルタ等によって排除する機能を設ける。

●措置例●

建物周辺の環境条件等によっては、通信機器の電気接点などに悪影響を及ぼす硫黄酸化物が室内に取入れる外気に多量に含まれている場合がある。このような場合、外気フィルタとしてアルカリ含浸フィルタを採用したり、触媒を使った脱硫装置を設置したりするなどして、これを除去する。

(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し、通報する機能を設けること。

解説

空気調和設備の機能停止は、通信設備の正常稼働に重大な影響を与えるため、空気調和設備に障害が発生した場合は、それを速やかに検知する機能を具備する。

●措置例●

空気調和設備の故障が発生した場合は、電流の異常、室内温湿度の異常などを速やかに検知できる機能を有し、速やかにランプ、警報ベル、プリンタ等により通報表示する機能を具備する。中央監視装置がある場合には、これに検知、通報機能を備える。無人施設においては、遠隔通報機能を具備する。

(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。

解説

消防法で定めるもののほか、重要な設備を収容する空気調和設備室においては、火災発生時に被害を最小限に留められるよう自動火災報知設備、消火設備を適切に設置する。

関連法規：消防法施行令第６～22条及び同施行規則他

●措置例●

重要な設備を収容する空気調和設備室においては、火災発生時に水損を最小限に留めるようハロン等の不活性ガス消火設備等の消火設備を設置することが想定されるが、当該ガスを使用する場合、消火効率を維持するために空調が停止される場合があり、その結果、消火を要する設備以外の重要な設備も同時に高温度となり停止を招く危険性がある。上記を考慮し、ハロン等の不活性ガスによる消火を実施する以前に、自動火災報知設備を適切に設置することにより、空調停止を要さない早期の初期消火作業を実施する。

管理基準の対策項目

第１．方針

１．全体的・部門横断的な設備管理

(1)　情報通信ネットワークの基本的機能
　　情報通信ネットワークの基本的機能を明確にすること。

解説

運用時の作業の容易さや事業者間の連携、大規模災害時における通信の疎通をできる限り維持すること等も考慮しながら、システムの基本的な機能を明確にする。また将来の規模の拡大、端末の挙動を含むトラヒック増加に伴うふくそう監視、制御手法、障害発生時の拡大防止・極小化対策等の機能などをネットワークの設計指針に反映する。

設計指針の明確化は次の点に留意しながら遂行する。

１　システムの基本的な機能を明確にする。
２　システムの基本的な機能を満足させるための諸条件を明確にする。
３　システムの将来設計を明確にする。
４　システムの将来設計を十分に満足させるための諸条件を明確にする。

(2)　組織内の連携
　　平時及び事故発生時における担当部門（電気通信設備統括管理者又は電気通信主任技術者がいる場合は、その者を含む。）間の連携方針を策定すること。

(3)　組織外との連携
　　平時及び事故発生時における社外関係者（接続先、委託先、製造業者等をいう。）間の連携方針を策定すること。

解説

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ていることから､ネットワーク構築(設計、工事）及び維持・運用の各フェーズにおいて関連部門間での連携を図ることが重要である。

また、情報通信サービスを提供する際には、自社だけでなく、相互接続先や卸電気通信役務の卸先、運用業務等の委託先、ネットワーク機器の製造業者等の協力が必要であるため、日頃から連絡手段や相手先、報告内容の優先順位等の連携方針を策定することが重要である。

（平成27年度告示改正により追加）

２．関係法令等の遵守

提供する情報通信サービスに関する法令等を定期的に確認するとともに遵守すること。

解説

情報通信サービスの提供に当たっては、電気通信事業法及び関係法令等を遵守しなければならない。

電気通信事業法及び関連法令等は、サービスの多様化、電気通信事故の傾向を踏まえた改正を行うため、定期的に内容を確認し、遵守しているかを把握する必要がある。

（平成27年度告示改正により追加）

３．設備の設計・管理

(1) 通信需要を考慮した設計

通信需要、相互接続等を考慮した適切な設備の設計・管理方針を策定すること。

(2) 災害時を考慮した設計

災害を考慮した適切な設備の設計・管理方針を策定すること。

解説

情報通信ネットワークの構築（新規・追加等）に当たっては、通信需要の予測や相互接続の有無等を考慮する必要があり、過剰・過小な設備投資となることがないよう、適切な設備の設計・管理方針を作成し、構築を行う。

（平成27年度告示改正により追加）

４．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。

解説

安定的なサービスの提供、利用者保護の視点からも情報資産のリスク管理は不可欠である。セキュリティポリシーは、コンピュータウイルスなどによる情報漏えい等、情報資産の損失に対する抑止、予防、検知、回復について組織的・計画的に取り組むために定める統一方針であり、情報セキュリティを実践するための基本的な考え方、方向性を定めた内容となる。

セキュリティポリシー策定にあたっては、「別表第3情報セキュリティポリシー策定のための指針」を参考とすることが適当である。また、技術動向や組織体制の変化に応じて適宜見直しを行うことが必要である。

(2)　情報セキュリティに関する取組み
　　情報セキュリティポリシーを公表すること。

解説

策定したセキュリティポリシーは、公表することによって利用者に対する情報セキュリティに対する自社の取組を周知することができるので、策定次第、速やかに公表することが望ましい。

(3)　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。

解説

不正アクセスやサイバーテロ等について予め対処を定めておくことにより、実際にこれらが発生した場合迅速な対応が可能となる。危機管理計画の対象、責任体制、役割、対応内容と手順等を明確化させるとともに、模擬訓練等の実施についても明らかにしておくことが必要である。危機管理計画ガイドライン策定にあたっては、「別表第４危機管理計画策定のための指針」を参考とすることが適当である。

また、技術革新や社会の変化に応じた事例の洗い出しや組織体制の変化等に応じて適宜、次のような観点から対処方針の見直しを行うことが適当である。

●措置例１●

DoS攻撃等のサイバー攻撃等の大量通信等によるサービスへの影響を防止するため、これらの通信を遮断する等の対応が必要となる。

このような場合の対処にあたっては「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」（社団法人日本インターネットプロバイダー協会・社団法人電気通信事業者協会・社団法人テレコムサービス協会・社団法人日本ケーブルテレビ連盟　2007年５月30日策定）を参考とする。

●措置例２●

重大な影響を及ぼすサイバー攻撃や、１社のみでは解決が難しい攻撃に対しての他の事業者との協力体制等について検討する。

１　情報共有する体制の整備
２　他社へ協力を依頼するルートの整備
３　規制や接続拒否の実施基準の策定

●措置例３●

高度なセキュリティを実現するネットワークを構築するため、本人認証の手段として、端末認証（MACアドレス、シリアル番号等）、生体認証（指紋、静脈等）等、により高度な認証方式の導入を検討する。

●措置例４●

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、新手の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。

第２．体制

１．情報通信ネットワークの管理体制

(1)　職務内容
ア　情報通信ネットワークを管理する上で、経営責任者又は電気通信設備統括管理者の職務を明確にすること。

解説

電気通信回線設備を設置する電気通信事業者及び総務大臣の指定を受けた電気通信回線設備を自ら設置しないが一定規模以上の利用者に対して有料でサービスを提供する電気通信事業者は、設備管理の専門化･細分化や外部委託等が進む中で、社内の部門間や社外を含めた全体調整、安全･信頼性確保の方針･取組･体制等への経営陣の主体的関与を強化するため、経営レベルの安全管理責任者（電気通信設備統括管理者）の職務を設定することが必要である。

なお、電気通信設備統括管理者を配置しない事業者については、情報通信ネットワークの管理に当たっての経営責任者の主体的関与が重要であることを踏まえ、その職務について明確にする。

（平成 27 年度告示改正により追加）

イ　情報通信ネットワークを管理する上で、電気通信主任技術者の職務を明確にすること。
ウ　情報通信ネットワークを管理する上で、関連する部門の責任者の職務を明確にすること。
エ　情報通信ネットワークを管理する上で、各部門の担当者の職務を明確にすること。

解説

これまでも、電気通信主任技術者は法令上、「設備管理の監督責任者」に位置づけられていたが、ネットワーク･設備構成の高度化･複雑化が進展する中で、その業務範囲が不明確である点、技術の進展に応じた能力維持・向上や区分の在り方等が課題になっていた。

電気通信主任技術者は管理規程を基盤とした現場におけるＰＤＣＡサイクルの責任者であることを鑑み、担うべき役割を適切に果たせるよう、その業務範囲を明確にすることが求められる。

併せて、電気通信主任技術者だけでなく、設備管理上関係のある部門責任者及び部門担当者についても、それらの職務を明確にしておくことが事故防止の観点からも必要である。

（平成27年度告示改正により追加）

(2)　関係者間の連携
ア　情報通信ネットワークを管理する上で、各部門間の連携体制を明確にすること。
イ　情報通信ネットワークを管理する上で、社外の関係者との連携体制及び責任分界点を明確にすること。

解説

情報通信ネットワークの管理に関係する者の職責を明確にしただけでは､安全･信頼性確保は不十分であり、速やかな原因の究明、復旧対策の実施及び利用者への周

知等を可能にするため、各部門間の連携体制を明確にし、連携を密にすることが必要である。

また、社内だけでなく、相互接続先や卸電気通信役務の卸先、情報通信ネットワーク構築に関わった機器ベンダ等の関係者間の連携を密にすることも必要である。併せて、特に相互接続先との連携に当たっては、事故発生時の責任分界点を予め決めておくことが速やかな復旧に必要となる。

（平成 27 年度告示改正により追加）

ウ　他の電気通信事業者及び業界団体との間で、電気通信事故に係る情報や再発防止策を業界で共有し、事故防止に向けた体制を整えること。

解説

電気通信事故を減らす取り組みとして、事故に係る情報を事業者間で共有し、共通する課題については他社の対策例等を参考に事故の未然防止につなげる必要がある。

エ　アプリケーション開発者との間で、ネットワークの負荷を考慮したアプリケーションの開発手法等について情報共有すること。

解説

平成２３年から２４年にかけて、スマートフォンのアプリケーションの制御信号の増加を一因とする電気通信事故が多数発生した。アプリケーション開発において、ネットワークの負荷を軽減するように考慮されていれば、電気通信事故が減少することが考えられることから、アプリケーション開発者と連携を図り、開発手法等について情報共有を行うことが望ましい。

●措置例●

他システムと連動するシステムの担当者に対して、他システムの仕様や動作フロー、連動に伴い想定されるリスクを共有することで、注意喚起を図る。

２．各段階における体制

(1)　設計
ア　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。

解説

システム設計のために、意思決定、作業の分担、責任の範囲等について明確にする。

また、サービスの安定的な提供のために、機能確認内容等をベンダなど関係者で確認し、セキュリティチェックのための体制についても確認する。

ベンダ等の関係者との連携を担保する適切な契約についても確認する。

●措置例●

体制を確立するために必要な主な配慮点は以下の通りである。

１　チーム構成、人員は適切であるか。
　局面毎に、工数に見合った人数でかつ必要な技術や経験を備えたメンバーが中心となってチームを構成する。

２　チームの作業に関する責任が明確に定められているか。
　チームの職務範囲、権限、責任、作業結果の報告先、作業結果についての承認権限者を明確に定める。

３　作業標準、必要な文書類、様式、提出先を定める。

４　進捗状況が正確に把握できる体制になっているか。
　進捗状況を正確に把握し、スケジュール調整を適切に行う。

５　サーバ等機器の機能がベンダ等を含め関係者間で確認できているか。

６　ベンダ等の関係者との連携を担保する適切な契約がなされているか。

イ　設計を委託する場合は、委託業者と関連部門間での連携を図ること。

解説

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ていることから、ネットワーク構築・運用各フェーズにおいて関連部門間での連携を図ることが重要である。

(2)　工事・設備更改
ア　工事及び設備更改の実施に当たっては、作業の分担、連絡体制、責任の範囲等の管理体制を明確にすること。

解説

工事作業のために作業の分担、責任の範囲等の施工管理体制を明確にする。

●措置例●

工事関連部門、委託事業者、ベンダ、ネットワーク運用者による工事実施体制や公示手順の確認、不具合が発生したときの利用者への周知体制などの確認を行う。

また、安全管理者、電気通信主任技術者、作業責任者、作業主任者、担当者等を定めて、安全な施工管理体制を確立する。

事故は、設備、環境などが整備されていないことや、作業者の技量の未熟さ、安全意識の低さなどが原因で発生することが多いので、設備、環境などに対する整備並びに教育、訓練等を実施し、事故を未然に防止することが必要である

ネットワーク設備の更改時、移転時においては、現行システムの安全・信頼性を損なわない配慮が必要である。このため、設計、施工の段階を通じて作業

の分担、連絡体系、責任の範囲等の管理体制を明確にする。
　特に、ユーザ、電気通信事業者、ベンダ及び社内関連部門との連絡調整を適宜、適切に実施し、事故を未然に防止することが必要である。

イ　工事及び設備更改を委託する場合は、委託契約により工事及び責任の範囲を明確にすること。

解説

委託工事を行う場合、委託契約により工事及び責任の範囲を明確にする。委託工事においては、当事者間のトラブルの発生を防止するため、原則書面による契約書を取りかわす。

また、工事による設備障害の防止、作業者の安全確保、通信の秘密保護、データ保護及び設備の保護についても、必要項目を明確に記入する。

●契約書に明記する項目の例●

- 権利義務の譲渡等……第三者への譲渡等の禁止
- 安全の確保
- 機密の保持・守秘義務・保持契約
- 工事完成保証人
- 工事の一括委任又は一括下請負の禁止等
- 現場代理人及び主任技術者等の配置
- 外部委託先の監査実施
- 情報管理規程の策定
- 監督、監査の実施
- 不具合発覚時の処置（是正要求、是正結果確認等）

ウ　工事及び設備更改の実施に当たっては、委託業者を含む関連部門間での連携を図り、作業手順を明確にするとともに、監督を行うこと。

解説

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ていることから、ネットワーク構築・運用各フェーズにおいて関連部門間での連携を図ることが重要である。

サービスに大きな影響を及ぼしかねないサーバ等機器の容量や評価・試験方法等について、事前に十分確認する。またネットワークに影響が生じる可能性があるセキュリティ対策やふくそう時の端末動作についても事前に試験、確認する。

エ　相互接続に関する工事を行う場合は、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。

解説

相互接続仕様書に基づく総合工程に従って互いに必要なシステム開発やシステム改修を行うが、作業の中でドキュメントの不備、不明な点が見つかった場合、開発遅延等による工程見直しが必要になった場合等には、連絡窓口間で調整会議等を招集して仕様書の変更案を取りまとめ、履歴管理を行う。

また、システム開発等の進捗に合わせ、相互に対向試験項目を出し合い、調整の上必要な試験ネットワークを構成し、試験を行う。

●システム開発等から対向試験実施までの間における管理すべき項目の具体例●

- 対向試験項目の洗い出し

・　対向試験ネットワーク構成の決定
・　試験手順書の作成
・　マシンタイムの調整
・　試験回線の開通手配

(3)　維持・運用
ア　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。

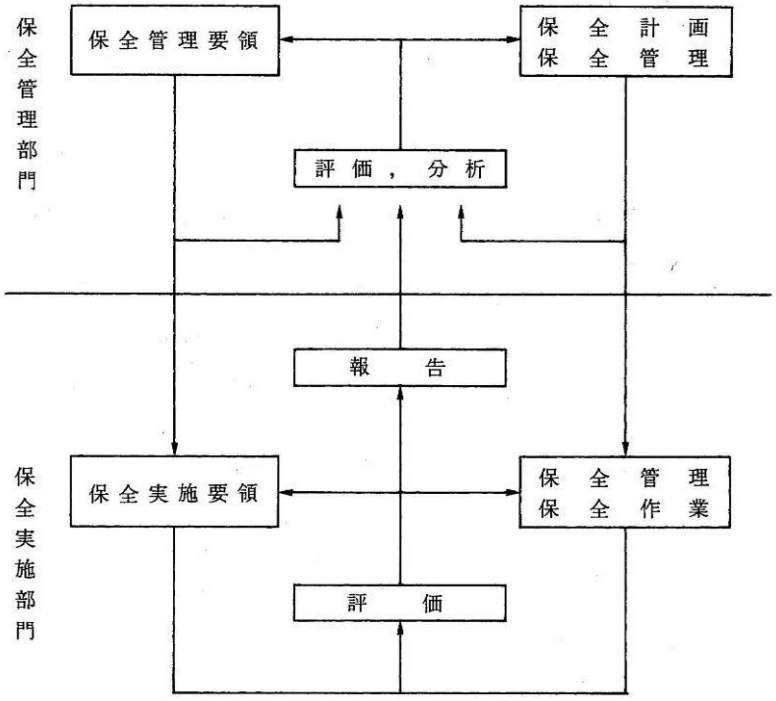
解説

ネットワークの保全・運用管理体制を明確にし、作業の分担、連絡体系、責任の範囲等を明確にするとともに、故障・災害等によるICT障害に対する責任体制・管理体制の整備を行う。

IP電話、インターネット等では相互接続事業者、関係事業者、ベンダ間での連携、連絡体制の整備を行っておくこと。

●措置例１●

保全管理体制として保全管理部門と保全実施部門を設け、保全管理部門は保全計画の策定、保全基準の設定および保全管理要領の制定等を行い、保全実施部門は実際の保全作業を実施するとともに、その実施結果等を保全管理部門に報告する。保全管理部門ではこれらの実施結果を分析し、次の保全計画の策定にフィードバックすることにより、保全業務におけるPlan－Do－Check-Actionのサイクルを構成する体制を設ける。



保全管理体制の例

●措置例２●

ネットワークの運用を行う場合、具体的には、電話、データ通信等の役務の種類によって役務の内容、情報通信ネットワーク構成が異なるので、所要の専門知識を有する要員を配置した運用体制を設ける。体制の確立に当たって、次の方法が考えられる。

１　作業内容、作業量分析
２　組織構成、作業分担案の作成

３　組織間連絡体系の明確化
４　組織分科分掌の制定
５　事業者間、社外機関との運用協定の取り決め
６　訓練
７　要員配置

●措置例３●

非常時等の際の事業者間の連携・連絡体制の整備において考慮すべき事項

１　社会的に影響の大きいイベント、災害時を考慮した関係事業者間、ベンダ、施工業者、行政機関などの連絡体制の一元管理を行う。

２　疎通状況の共有・公開など、障害の影響拡大防止、早期復旧を目的とした事業者間協力のレベルや範囲の取り決めなどを行う。

イ　重要な設備の保全・運用については、関連部門間での連携を図ること。

解説

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ていることから、ネットワーク構築・運用各フェーズにおいて関連部門間での連携を図ることが重要である。

ウ　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。

解説

●措置例●

具体的には次のような内容を網羅した委託契約を交わすことが望ましい。

保守作業の範囲

- 保守方法
- 機密の保持
- 責任の範囲
- 原因分析体制
- 保守体制
- 立ち入り場所の限定、およびその手続き
- 免責事項の内容
- 相互の提供情報内容及び連絡責任者
- 情報セキュリティの確保
- 障害時の対応、及び報告

エ　保守の委託を行う場合は、作業手順を明確にするとともに、監督を行うこと。

解説

委託保守においては、その作業手順を明確にし、所要の監督を行う。

●措置例●

具体的には前項で述べたような委託契約に基づき、作業中の立ち会い、終了後の確認を行う。その際、必ず責任者のサインを交わして相互の責任を明確にしておく。また、情報セキュリティ管理に関する監査を定期的に実施する。

オ　故障等における迅速な原因分析のための事業者と機器等の製造・販売等を行う者や業務委託先との連携体制を確立すること。

解説

故障、障害等に対して、迅速な原因分析のための事業者とベンダ・業務委託先間で連携体制などについて十分整理しておくことが望ましい。

●措置例●

1　原因分析体制や処理時間の実態を書面などで定期的に確認することなどを保守契約などに盛り込むこと。

2　ベンダなどへ解析を依頼する場合には、解析に必要な十分な情報を提供すること。

3　間欠的に故障が発生する場合においても、故障が固定化、拡大化する前にベンダなどと連携して適切な対策を立てること。

4　ベンダや業務委託先との共同訓練を実施すること。

カ　運用監視体制を構築すること。

解説

情報通信ネットワークの安定的な稼働のため、システムの稼働中はトラヒック量の推移や機器の稼働状況確認等を常に実施しなければならない。運用状況を正確に把握するためにも運用監視体制を構築し、的確な状況把握に努める必要がある。

また、運用監視体制の構築に当たっては、利用者へのサービス提供の継続性を優先するのか、ネットワーク・設備の安全性を優先するのか等の運用ポリシーを運用担当者のみならず経営層も含めて明確にしておくべきであり、さらに、当該運用ポリシーはベンダー等の外部関係者とも共有しておくべきである。

運用監視体制の構築に当たっては、別表第２ 第２．２．(3) アの考え方を参照すること。

（平成 27 年度告示改正により追加）
（平成 31 年度にまた書きを追加）

キ　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、非常時等における事業者間の連携・連絡体制の整備を行うこと。

解説

ネットワークの障害復旧に当たっては、接続先の電気通信事業者と相互に連絡を密にして早期復旧に努める必要がある。このためネットワークを相互に接続した電気通信事業者は、連絡窓口、試験点、保守規格、監視率について取り決め、協力してネットワークの保全・運用に努める。

また、これらについて変更が生じた場合には、速やかに相手側に連絡を行い、必要により協議・調整を図る。

ネットワークを相互に接続した電気通信事業者は、サービスの安定運用のための適切なオペレーションの実現のため、ネットワーク管理体制の強化に努める。

●措置例●

1　相互接続の際に事業者間で網運用・管理情報の交換に関する機密情報の管理や連絡体制などを確認する。

2　事業者間の連携促進のための情報交換連携の仕組み（事象のレベル分け、レベルに応じた情報連携の整理）や適切なオペレーションに向け事業者間のやり取りに必要な情報について整理する。

3　相互接続を考慮した電気通信事業者とベンダ間の情報フォーマットの共通化を検討する。

4　相互接続箇所における監視、切り分け手段についてメール、IP 電話などの

サービス毎に協議し、障害発生時の復旧手順を事業者間で共有した上で、障害の切り分け機能の向上につながる項目を具体化する。

5　ネットワークを相互に接続した電気通信事業者は、共同で故障箇所特定のためのデータ取得手順、切り分け手順等を検討し整備する。

ク　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。

解説

国際間のローミングサービスにおいては、運用面で外国の電気通信事業者との間の連携体制が重要である。ローミングを実現するために必要な技術情報や認証情報についての授受はもちろんのこと、サービスの運用時においても確実な連携体制を維持するとともに、障害の発生等においては迅速な対応が確保できるよう考慮する必要がある。

ケ　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。

解説

コンテンツやアプリケーションを提供する者のサーバと電気通信事業者のサーバとを接続する場合は、接続条件とともに作業の分担、連絡体系、責任の範囲等の保全・運用体制を明確する必要がある。

コ　相互接続を行う事業者等の間において、非常時の連絡体制や連絡内容を明確にすること。

解説

非常事態時の大規模かつ複数事業者にまたがる被害を想定し、相互接続を行う事業者間において、応急活動、復旧活動等を効果的に実施するため、非常事態時の相互連絡体制や重要通信の確保、故障状況の相互連絡内容等を明確にすることが必要である。その際、次のような項目について留意し、可能な対応をとること。

●措置例●

1　事業者間の連携促進のための情報交換連携の仕組み（事象のレベル分け、レベルに応じた情報連携の整理）

2　事業者間､事業者とベンダでの連携を図る際にやり取りされる情報のフォーマットの共通化

3　緊急通報や重要通信確保、故障状況の広報などに関する事業者間で共通に運用可能なマニュアルの策定

4　疎通状況の共有・公開などによる障害の影響拡大防止

(4)　情報セキュリティ対策 ア　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。

解説

ネットワークを管理する者として、情報セキュリティに関する一定以上の専門的な知識・技能を有する者（資格保有者等）を配置し、不正アクセスやコンピュータウイルスなどに対する対策を実施することは、ネットワークの安定的かつ確実な運用を確保する上で重要な要素となる。

イ　外部委託先を含めた作業の分担、連絡体系、責任の範囲等の情報セキュリティ対策体制及びデータ管理体制を明確にすること。

解説

データ管理体制を明確にし、作業の分担、連絡体系及び責任の範囲を明確にする。

●措置例●

データ管理体制の例として以下のものがある。

1　対象データを取り扱う部門の総責任者として、安全管理責任者等を設置し以下の担務を行う。

①　データ取扱い方法の決定

②　監査の実施

2　安全管理責任者の下で実際に安全管理を実行する者として安全管理者を設置し以下の担務を行う。

①　安全管理担当者へのデータ取扱い方法の具体的指示

②　工事・作業の状況の管理

3　安全管理者の下で実際に事務を処理させるため安全管理担当者を指名する。

①　入室管理

②　鍵の保管・管理

③　プログラム、データ（ファイル、ドキュメントを含む）の保管・管理

④　作業状況報告

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。

解説

業務を外部委託する場合には、守秘義務・保持契約を取り交わすとともに守秘義務・保持契約条項の具体化、秘密保持に係る誓約書の徴収、外部委託先の監査実施、監査時のチェック項目、監査において不具合が発見された際の是正処置依頼・是正処置結果の確認等を定めた情報管理規程の策定等、委託先の取組を明確化する。

(5)　ソフトウェアの導入・更改

ソフトウェアの導入・更改においては、機器等の製造・販売を行う者等関係者との連携体制及び責任の範囲を明確にすること。

解説

IP 化の進展により、設備の維持･管理、制御や機能追加等をソフトウェアで行う役割が高まることに伴い、ソフトウェア開発を外部に委託することや市販のソフトウェアをパッケージとして導入することによる「ソフトウェアのブラックボックス化」が進展している。

ソフトウェアの信頼性確保のために、導入時・更改時に発見した不具合に速やかに対応できるよう、ベンダ等関係者と連携を図る必要がある。

なお、ここでいう「責任分界点」は、電気通信事業者とベンダ等関係者双方で協議・決定することになるが、ソフトウェア納入完了時点、ソフトウェア更改時点などが考えられる。

●措置例●

1　電気通信事業者とベンダーは、ソフトウェアの単なる不具合情報の共有に留まることなく、当該ソフトウェアを利用する機器のシステム構成上の役割等についての共通理解を図った上で、当該不具合がシステム全体にどのような影響を及ぼす可能性があるのか、利用者のサービス提供にどのような影響が考えら

れるのか等のレベルまで共有できるような深い連携に努める。

２　不具合の発生確率に関わらず両系ダウンやデータの喪失の恐れのある重要な不具合情報については、ベンダー等から確実に提供されることが必要である。そのため、電気通信事業者は、ソフトウェア等の不具合情報の提供に関し、どういった情報を共有するのか等について、ベンダーとの間で具体的な提供基準を設けておき、必要に応じて当該提供基準の見直しを行う。また、電気通信事業者は、ベンダーから情報提供を受けるだけではなく、自らソフトウェアの不具合情報の積極的な収集・分析に努めることが必要である。少なくとも機器メーカーが発出するリリースノートについては、自ら収集し、不具合情報の確認を行うべきである。

（平成 27 年度告示改正により追加）
（平成 31 年度に措置例追加）

(6)　重要通信
　　重要通信を扱う場合は、その通信を確保するための体制を構築すること。

解説

電気通信事業法第８条に基づき、電気通信事業者は、非常事態が発生し、又は発生するおそれがあるときは、重要通信を確保しなければならないとされている。このため、重要通信を扱う場合はその状況を想定した体制を予め検討しておくことが必要である。

体制の構築に当たっては、別表第２ 第２．２．(3) アの考え方を参照すること。

（平成 27 年度告示改正により追加）

(7)　ふくそう対策
　　ふくそう対策を講ずるための体制を構築すること。

解説

ふくそう対策については、発生時の体制構築だけでなく、防止対策も含めて検討することが必要である。体制の検討に当たっては、上記(6)と同様の観点を考慮する必要がある。

（平成 27 年度告示改正により追加）

(8)　緊急通報
　　緊急通報を扱う場合は、その通報に関する体制を構築すること。

解説

緊急通報については、事業用電気通信設備規則だけでなく、本基準の設備等基準（第１１．(13)）においても対策を求めており、当該通報を扱う場合には必要な体制構築を予め検討することが必要である。体制構築に当たっての考慮点は、上記(6)、(7)と同様である。

（平成 27 年度告示改正により追加）

(9)　防犯対策
ア　防犯体制を明確にすること。

解説

防犯体制を明確にし、分担及び責任の範囲を明確にする。データの改ざん、窃取等に結び付く破壊活動、妨害工作又は盗難等の故意の人為的災害は、その手段、時期、場所等を予測できないため、防犯管理には十分な配慮が必要となる。

建築物及び設備面から立てられた防犯対策は、例えば建築物の周囲、外面及び開口部分、設備を設置した部屋のそれぞれの防犯対策が有機的に結合、機能するような体制作りによって、目的とする機能を発揮する。

イ　防犯管理の手順化を行うこと。

解説

異常事態発生時の対処を含め、管理の方法について手順化しておく。

異常事態発生時には、第一次対応が最も重要であるため、状況を正確に報告できることに重点を置き、代理者を含め、各人の責任分担を明確にするとともに、連絡・報告、現状分析、対策等に関し、即応できるように予め手順化しておく。

(10)　調査・分析・改善

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。

解説

情報通信ネットワークの維持及び運用に関して、現状の作業が適性であるか、手順書どおりに作業が実施されているか等についてそれぞれの現業部門で調査、分析を行う体制を明確にする。

いわゆる、情報通信ネットワークの安全・信頼性阻害要因は同ネットワーク及びネットワークを取り巻く自然環境、人的環境を含む環境条件にある。そしてこの環境条件は、当然変化し、情報通信ネットワーク自体もネットワーク構成等が変化する。従って、ある時点で策定された安全・信頼性対策が一定期間を経た後も有効に機能しているかを見直していく仕組みを作っておくことは、対策を策定するのと同様に重要である。

●措置例●

設備の運用・保全に実際に携わる部門において調査・分析を実施し、その結果を管理・計画部門へ報告する。管理・計画部門は、その結果を基に必要に応じて作業内容等を見直しする。このような実施部門と管理・計画部門との連携を図るような体制作りを行う。また、必要に応じ、管理・計画部門が実施部門を巡回点検する等の措置を講ずる。また、見直しのための調査、分析体制は一定期間毎にプロジェクトチームを作って行うのが実際的である。

プロジェクトチームは関連する部門を横断的に網羅した専門家で構成し、チームの責任者は調査、分析結果を改善に結びつけるために、上層管理者であることが望ましい。

その他、適切な評価が行われ、改善提案が行われるためには関連部門の協力が不可欠であり、そのためには上層管理者の一致した理解が必要である。これを可能にするため、上層管理者による現状分析推進委員会の類を設置することもひとつの方法である。

(11)　利用者への情報提供

利用者への情報提供を行うための体制を構築すること。

解説

一般利用者は、サービスの利用不可又は利用困難な状態になった際に、それが自らの端末が原因か事業者のネットワークに起因するものかそのままでは分からないことが多く、利用者の利便性を損なうことに繋がる。

そのため、電気通信事業者は、事故発生時の早期復旧のための体制だけでなく、

利用者に対して速やかに情報提供するための体制についても予め構築しておくことが必要である。

（平成 27 年度告示改正により追加）

(12)　事故発生時の報告等

ふくそう及び事故発生時の報告、記録及び措置を行うための体制を構築すること。

解説

ふくそう又は電気通信事故が発生した際には、総務省や相互接続先等の関係者へ速やかな状況報告が求められる。速やかな報告のためには、事象が発生した際に速やかに発生状況を記録し、必要に応じて応急措置を行わなければならないため、予め体制について構築しておくことが必要である。

（平成 27 年度告示改正により追加）

(13)　災害等の報告

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。

解説

大規模な災害等、通常の復旧手順や組織では対処が困難な事態の発生に備え障害対応マニュアルや組織枠を超えたサービス復旧のための体制を検討し、被害状況の把握、連絡体系、権限の範囲等について明確にしておく。障害が発生した場合においては、まず事業者自らサービスの早期復旧に取り組むことが必要であり、そのための予備設備の設置・手配の主体的な実施を検討する。

また、設備の故障によらない新型インフルエンザなどの脅威による非常事態が発生した場合においても、国民の安全確保や社会経済活動の維持のために情報通信ネットワークが確実に機能する体制についてあらかじめ検討のうえ明確化する。さらに、想定する脅威を随時再点検し、対策や体制の一層の充実を図ることが適当である。

●措置例●

次のような内容を含んだ災害対策規程を作成し、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　要員措置、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

イ　非常時における社員・職員、復旧に必要な業務委託先等への連絡手段、社員・職員の参集手段の確保等の体制を整えること。

解説

大規模災害による交通手段の途絶やライフラインの被災等を想定した上で､社員･職員との連絡手段、社内の部門間の連絡体制、参集手段の確保等、非常事態時の体制を整える。また、あらかじめ復旧に関係する委託業者、ベンダ等との連絡手段、体制の確保についても整備しておく。

ウ　非常時における広域応援体制を明確にすること。

解説

非常事態時は、復旧作業を行うべき事業者自体が被災者であることを想定し、必要に応じ、被災地域外を含めた広域応援体制についても整えておく。

●措置例●

1　災害の規模応じた、発動の判断、連絡系統、連絡事項等のルール化及び体制

2　被災地内における広域支援受入れ体制（活動拠点等）

エ　相互接続を行う事業者等の間において、非常時の連絡体制や連絡内容を明確にすること。

解説

非常事態時の大規模かつ複数事業者にまたがる被害を想定し、相互接続を行う事業者間において、応急活動、復旧活動等を効果的に実施するため、非常事態時の相互連絡体制や重要通信の確保、故障状況の相互連絡内容等を明確にすることが必要である。その際、次のような項目について留意し、可能な対応をとること。

●措置例●

1　事業者間の連携促進のための情報交換連携の仕組み（事象のレベル分け、レベルに応じた情報連携の整理）

2　事業者間､事業者とベンダでの連携を図る際にやり取りされる情報のフォーマットの共通化

3　緊急通報や重要通信確保、故障状況の広報などに関する事業者間で共通に運用可能なマニュアルの策定

4　疎通状況の共有・公開などによる障害の影響拡大防止

オ　非常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。

解説

応急活動、復旧活動を行う上で、適切な判断と行動をするため、災害情報、交通情報､支援物資等取り扱いなどについて正確で速やかな情報を入手する必要があり、また、状況に応じ、支援を要請する場合などが考えられることから、国、地方公共団体、指定公共機関等との連絡方法などを確認しておく。

カ　非常時において、応急活動、復旧活動に関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。

解説

非常災害時等における、ライフライン自体の被災、大規模なふくそうの発生などを想定し、以下のような対策を講じておく。

1　災害時優先電話の設置

2　携帯電話・PHS、衛星携帯電話など多様な通信手段の整備

３　被災地への着信を極力させる連絡方法（運用ルール）の確立など

キ　非常時における対応体制の検証・見直しを必要に応じて行うこと。

解説

非常時において迅速・適確な対応を実施するためには、事業継続計画、災害対応マニュアル等に記載されている対応体制を、適宜、検証・見直しを行うことが必要である。

(14)　事故発生時の記録 事故発生時等に係る原因を特定するための記録を行うための体制を構築すること。 (15)　サービス復旧 サービスの復旧を行うための体制を構築すること。 (16)　再発防止策 再発防止策を講ずるための体制を構築すること。

解説

(12)において構築する体制は、事故発生時における原因特定のための記録、サービス復旧及び再発防止策を講じるための体制も兼ねておくことで、速やかな対応に取り組むことができる。

（平成 27 年度告示改正により追加）

第３．方法

１．平常時の取組

(1)　基本的取組
ア　情報通信ネットワークの現状を調査・分析する項目、評価方法等の基準を設定すること。

解説

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、分析を行う項目及び評価方法等について基準を設ける。

●措置例●

実施要領、手順書等に定められている運用保全作業の項目及び内容がどのような形で成果となっているかについて、評価する方法等について基準を設定する。

イ　情報通信ネットワークの現状を調査・分析する作業の手順化を行うこと。

解説

情報通信ネットワーク維持及び運用に関して、現状の調査・分析作業の実施手順を明確にする。手順化のポイントは次のとおりである。

１　調査、分析の効率化
２　調査、分析の適正化
３　一定手順による調査、分析の積み重ねによる経年変化の掌握
４　組織内に周知し、調査、分析作業への協力を得る。

ウ　設計、工事、維持・運用の各工程における作業を明確にするとともに、工程間の調整及び管理を行うこと。

解説

設計工程を明確にし、工程間の調整を十分に行う。

●措置例●

通常、システム設計は以下の工程からなり、各々の工程において進捗管理がなされるとともに、設計内容を明確に示したドキュメントにより、次の設計工程へと引き継ぐ。

１　基本検討
２　基本設計
３　詳細設計
４　プログラム設計
５　試験

安全に作業を行うべく手順書を作成し、作業方法及び作業工程を明確にするとともに、工事による不具合が発生した時のリカバリー手順やその所要時間の見通しを用意・共有し、作業工程全体にわたる管理を行うことが必要である。

作業においては人為的ミスを防ぐために作業の自動化及び作業確認の強化も考慮すべきである。

また､安全かつ容易な設備増設､拡張性確保の手法を確立することが必要である。

さらに、利用者の少ないエリア・時間帯に先行導入を行い、事故影響の最小化に努める。

●措置例●

工事における作業工程の例としては、次のようなものが考えられる。

１　設計／計画

仕様書等に基づき､工事を実施するにあたって必要な施工方法､施工条件、施工時期を決定し、所要人員、所要経費等を算出する。また、工事現場の細部状況を調査把握し、設計図面を作成する。

２　工事準備

監督、作業責任者等を任命し、工事を遂行するための体制を確立する。また、工事用物品や工具、計測器などを準備する。

工事ミス時のリカバリー手順を作成する。

安全かつ容易に設備増強を実施できる手順書を作成する。

３　工事作業

基礎工事、工事用物品の配線、搬入、据付け、試験調整等の工事を行う。

作業の自動化及び作業確認の強化を実施することで人為的要因によるサービス中断を回避する。

４　検査

仕様書、設計図面等に記載された内容の通り工事がなされているか検査を行う。設計段階においては、作業環境、施行方法に対応した作業計画を設定することにより、作業の安全を確保する。

また、工事の進捗状況、稼働並びにこれに伴う問題点を把握し、調整することにより作業者の安全を図る。

併せて、作業の方法及び工程を明確にし、その管理を行う。なお、新設備導入等にあたっては、利用者の少ないエリア・時間帯に先行導入し、事故影響の最小化に努める。

●措置例●

設備の更改・移転工事における作業工程の例としては、次のようなものが考えられる。

１　基本方針の策定設備の更改移転を検討するに当たっては、次の事項についてユーザへの影響度、コスト、法制度面から検討する。

①　移行時におけるネットワークの停止
②　センター移転先の選定
③　新センターの設備
④　回線
⑤　ファイルの移行、OS のバージョンアップ等
⑥　移行前のネットワーク等変更の一時凍結
⑦　センター移転日時

２　基本計画／詳細設計

計画時に検討すべき主な項目には、次のようなものがある。

①　全般事項

・　設備の更改、移転の基本方針
・　将来計画
・　移転予算の見積
・　新センターレイアウト
・　移行作業
・　移行スケジュール
・　要員計画
・　設備管理方式

・ 連絡回線
・ ドキュメントの移転
・ 業務委託（警備、清掃等）
・ ユーザとの調整
・ 電気通信事業者との調整
・ ベンダとの調整

② システム関連
・ システム移行方法
・ 新センター設備機器
・ 回線設定
・ テスト及びテスト環境
・ 現行機器、回線の撤去
・ ファイル、OS 移行計画

③ 運用関連
・ 移転後の運用体制
・ 新センターの運用方式
・ 新センターでの運用訓練計画

３ 工事準備

作業責任者等を任命し、基本計画等に基づく工事を実施するための体制を確立するとともに、工事に必要な機材等を準備する。

４ 工事作業

基礎工事、工事用物品の手配、搬入、据付け、試験、調整等の工事を行う。

５ 試験

設計書、設計図面等に記載された内容通り工事が行われているか試験を行う。

６ 試行

新センターで、試行運転を実施し、予想される性能、品質が得られているかどうかについて確認を行う。

７ 移行

旧センターから新センターシステムを切り換える工事を行う。

なお、不測の事態に備えて、旧センターの並行利用期間、運用体制等を考慮しておくことが必要である。

８ 機器撤去

新センターが安定して稼働していることを確認した後、旧センターの機器を撤去する工事を行う。

９ 工事調整

一連の工程を通じて問題点を把握し、ユーザ、電気通信事業者、ベンダ及び社内関連部門との連絡調整を適宜かつ適切に行い､円滑な工事を実施する。

(2) 教育・訓練

ア 電気通信主任技術者、広報担当者その他の従事者（事業用電気通信設備の設計、工事、維持又は運用を委託する場合は、当該委託先の従事者を含む。以下「従業者等」という。）の教育及び訓練を実施すること。

解説

電気通信主任技術者、広報担当者その他の従事者の教育及び訓練を実施する。事業用電気通信設備の設計、工事、維持又は運用を委託する場合は、当該委託先の従

事者に対して教育及び訓練を実施する、又は当該委託先が適切に教育及び訓練を実施するように定期的な確認を含め監督を行う。

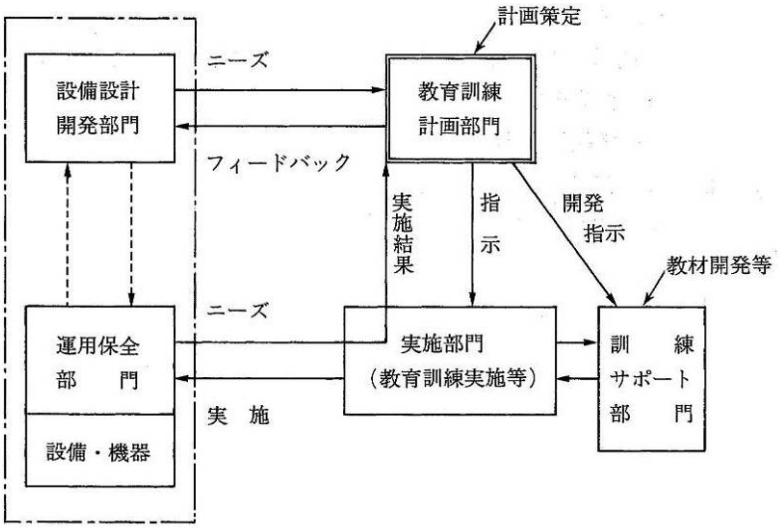
（令和５年度告示改正により追加）

イ　従業者等への教育・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。

解説

教育・訓練計画部門は、設備の計画・設計部門および適用・保全部門と密接な連携を保ち、たえず情報収集ができるような体制を整えておく。

●措置例●



教育・訓練体制の例

ウ　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。

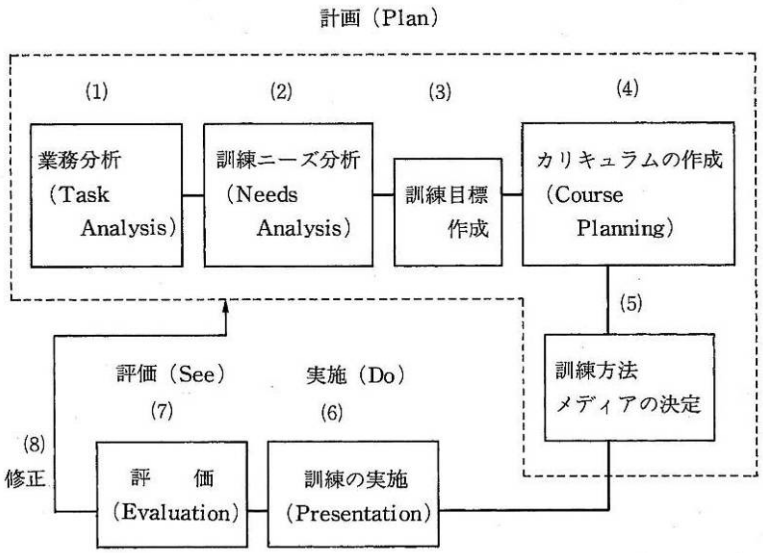
解説

教育および訓練を実施する目的を明確にし、終了後の実施効果により計画の修正を行う。

●措置例●

教育・訓練の効果を上げるため、一般によくいわれる“Plan（計画）－Do（実施）－See（評価）”のサイクルが円滑に機能することが望ましい。

次図に示すように訓練の計画と実施、それに評価が一つのフィードバック系（Closed Loop by Self Correcting）を構成し、ロジカルな考えに基づいて教育訓練を行うようにする。



訓練コースの計画、実施、評価

各ステップの作業は次のように行われる。

１　業務分析

職場には、どのような作業があり、現在それがどのように行われているか、訓練の対象となる業務の分析（Task Analysis）を行う。

２　訓練ニーズ分析

訓練ニーズを明確にする（Needs Analysis）。つまり、訓練生は現在どのような知識と技能（Initial Behavior）を持っているのか、また訓練終了時に訓練生は、どのような知識と技能（Terminal Behavior）を持っていなければならないかという訓練必要点を明確にする。

３　訓練目標作成

測定可能な訓練（行動）目標を決める。目標行動の記述は、あとで客観的に評価できるように具体的な表現とする。例えば、「～ができる」というような表現で目標行動を記述する。

４　カリキュラムの作成

目標行動に応じたカリキュラムを設定する。

５　訓練方法、メディアの決定

訓練方法（技法）やメディア（教育機器）を決める。例えば、集合訓練で実施した方が効果的かOJT（On the Job Training…仕事を実際に体験させながら、機会をとらえて訓練生に必要な指導を行う訓練方法）でやるべきか、討議方式にすべきかを検討する。

６　訓練の実施

カリキュラムに基づいて訓練を実施する。

７　評価

訓練目標はどの程度達成されたか評価する。

８　修正

評価結果に基づいて訓練コースを修正する。

エ　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。

解説

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。

●措置例●

設備故障や異常ふくそう等の発生時における疎通確保に必要な緊急措置の実施能力を養うためには、講義中心の訓練だけでなく、具体的な場（環境）において‘Learning by Doing’、すなわち、実践しながら学ぶことが必要である。

これらを実現するための方法として次の３つが考えられる。

１　実機による訓練（Embedded Training）

２　シミュレータ（模擬装置）による訓練（Simulator Training）

３　CAL（Computer Assisted Learning）システムによる模擬演習訓練（Gaming&Simulation Training）

１　実機による訓練（Embedded Training）

実機による訓練では現実性のある訓練ができる点が効果的であるが次のような欠点もある。

①　訓練種目および訓練時間が制約される。

②　実機の信頼性が確保されない。

③　実習効率が悪い。

２　シミューレータ（模擬装置）による訓練（Simulator Training）

実機にかなり近い訓練が実施可能であるが、ハードウェア的に実機と同じものを作成しなければならない。

①　高価である。

②　実機の機能変化に柔軟に対処できない。

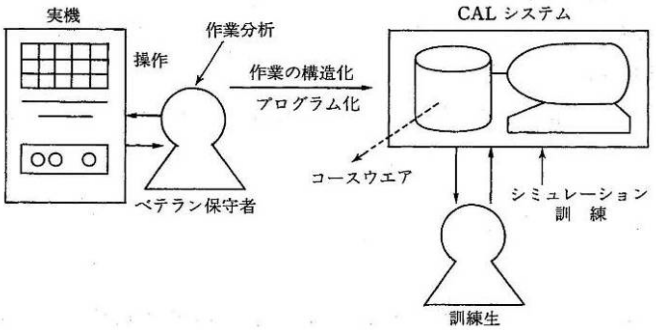
３　CAL（Computer Assisted Leaning）システムによる模擬演習訓練

CALシステムによるシミュレーション訓練では、訓練生が行動学習するための環境をソフトウェア（コースウエア）として実現させ、システムとの対話を通じて障害究明能力を養おうとする方式である。

コースウエアは次のように開発する。

ベテラン保守者が障害究明（トラブルシューティング）を行う一連の行動を観察し、そこでどのような知識が使われ、判断行動が行われているかを分析、整理し、構造化として最終的にCALコースウエアに展開する。

これは具体的な訓練対象による具体的な訓練であり、実機やシミュレータによる訓練と比べ安価であり、制約がなく極めて効率的、効果的であり、導入訓練として適している。



CALコースウェアの開発とCALによる模擬演習訓練

オ　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。

解説

定常的なデータ投入等の作業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。

投入されるデータの不良は情報通信ネットワークの利用者に影響を与える。投入データ不良の原因には、作成データの不良とデータ投入時の誤操作がある。

データ作成者、データ投入オペレータに、そのデータの使用されるシステムの内容とその重要性を認識させるとともに、個人別、データ区分別に不良を分析し改善を行う。

また、経路制御情報に不具合が発生した場合、インターネット全体に甚大な影響が出るおそれがあることに鑑みれば、経路制御情報を設定してからそれによる影響が出るまでの仕組みや、想定される影響等を含む BGP※全般に係る内容に加え、経路制御情報の設定作業における複数人体制によるチェック等必要な措置についても、教育・訓練を行うことが重要である。

さらに、経路制御情報の設定後において、トラヒックに異常な増大や減少が発生した場合に、原因や影響を把握するために確認すべき事項や復旧のために行うべき措置等について、教育・訓練を行うことが重要である。

※インターネットにおいて経路制御を行うためのプロトコルの一つをいう。

●措置例●

信頼性の高い作業能力を養うための教育については次のような方法がある。

１　専門家による講義（取扱い手順書等）

２　訓練生同士による討議（OJT 含む）

３　ビデオ教材等の教育教材による学習

４　上記３つを組み合わせた方法

（平成 31 年度にまた書き以降を追加）

カ　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。

解説

設備の保全に関する知識及び設備故障時におけるその応急修理及び原因の究明能力を養うための教育・訓練を行うこと。

●措置例●

設備保全及び設備故障時における原因究明の能力を養うためには、専門家による講義、ビデオ教材による学習等伝統的な講義中心の訓練だけでなく、より具体的な環境における実践を通じた訓練が有効である。その代表例として、ドキュメントを用いた机上の基礎技術の習得と密接に連携した OJT の実施がある。

キ　防災に関する教育・訓練を行うこと。

解説

防災に関して、通常時の保安作業及び異常事態発生時の措置について、必要な能力を養うための教育・訓練を行う。

●措置例●

防災訓練には、次のようなものがある。

１　社内訓練

被災想定にもとづいて行う社内訓練

①　情報連絡訓練

②　応急復旧訓練

③　消火訓練

④　避難訓練

⑤　その他

２　地域防災訓練

地域の防災機関､自治体等と共同で行う訓練｡訓練内容は社内訓練と同じ。

ク　防犯に関する教育・訓練を行うこと。

解説

防犯に関して、通常時の保安作業及び異常事態発生時の措置について、必要な能力を養うための教育・訓練を行う。

●措置例●

１　専門家による講義

２　ビデオ教材等の教育教材による学習

３　OJT

このうち、OJT は、仕事を体験させ、機会をとらえて訓練生に必要な指導を行う方法である。すなわち、仕事の方法、手順等、仕事に直接関連する具体的、実際的な知識あるいは仕事に対する考え方、心構え（取り組む姿勢）を即効的に教える場合に効果的である。防犯の教育・訓練として OJT による方法は特に有効である。

なお、OJT による訓練のバックグランドとしてある程度の体系的な知識が必要であるので、OJT の前提として１および２による訓練が必要である。

ケ　情報セキュリティに関する教育・訓練を行うこと。

解説

一般社員等に対し、通信の秘密の保護、各種データに関する守秘義務、パスワード管理の重要性及びコンピュータウイルスの脅威等について教育・訓練を行い、モラルの向上等を図ることが、適切なセキュリティ対策を推進する上で重要な要素となる。

●措置例●

新たな技術やリスク管理等に対応した技術者を育成するため、業界団体等による研修コースの活用などがある。

コ　電気通信設備の工事、維持及び運用に関する事項の監督に関する講習を実施すること。

解説

電気通信設備の工事、維持及び運用に関する事項の監督に関する講習を通常実施されるサイクル（電気通信主任技術者の場合３年に１度）の他に定期的（年数回、人事異動期等）に行うことで認知を高めることができる。

（平成27年度告示改正により追加）

サ　電気通信設備の工事、維持・運用に係る作業の教育及び訓練を実施すること。

解説

令和４年度において、電気通信設備の運用等に係る作業に伴う人為的ミスにより重大な事故が多発したことから、本対策を規定した。

電気通信設備の工事、維持及び運用に係る作業について、作業時における人為的ミス等を軽減させ、事故の未然防止を図るため、電気通信設備の工事、維持・運用に係る作業について、定期的に教育及び訓練を実施する。

（令和５年度告示改正により追加）

シ　応急復旧措置に係る訓練を実施すること。

解説

電気通信設備の応急復旧措置について、事故発生時の応急復旧措置の対応を早め、事故の大規模化・長時間化の防止を図るため、定期的に応急復旧措置に係る訓練を実施する。

（令和５年度告示改正により追加）

ス　広報含む社内関連部署間の連携訓練、全社一斉訓練、シナリオを共有しない訓練を実施すること。

解説

事故や災害等の障害発生後に、迅速に利用者へ周知・広報を行うことができるようにするため、広報含む社内関連部署間の連携訓練を定期的に実施することが望ましい。

また、大規模な事故や災害の発生時にも、適切に応急復旧措置や周知・広報を行い、早期復旧を図ることができるように、大規模な事故や災害を想定した全社一斉訓練を定期的に実施することが望ましい。

さらに、実際の事故や災害等の発生時には、復旧シナリオ等は存在しないことから、実際の事故や災害等の発生を想定し、シナリオを共有しない訓練についても定期的に実施することが望ましい。

（令和５年度施行規則等改正に伴い追加）

セ　全ての従業者等を対象に、毎年訓練を実施すること。

解説

電気通信設備の工事、維持及び運用に係る作業の訓練や応急復旧訓練など、工事、維持・運用等に従事する従業者への訓練については、自社及び運営委託会社等を含め、毎年、全ての従業者を対象に１回以上訓練を実施することが望ましい。

（令和５年度施行規則等改正に伴い追加）

ソ　電気通信設備の損壊又は故障等の発生リスクに係る調査等により判明した各リスクに対して復旧措置等の訓練を実施すること。

解説

「第３．方法　１．平常時の取組（14）リスク管理」において、電気通信設備の損壊又は故障等の発生リスクの調査及び分析（ア）、調査及び分析された発生リスクに対する対応措置及び応急復旧措置の整備（イ）が規定されているが、迅速な応急復旧を可能とするため、定期的に、当該電気通信設備の損壊又は故障等の発生リスクに係る調査等により判明した各リスクに対して、想定している復旧措置等の訓練を実施することが望ましい。

（令和５年度施行規則等改正に伴い追加）

(3)　設計

ア　将来の規模の拡大、トラヒック増加（端末の挙動によるものを含む。）、インターネットの経路制御情報等の制御信号の増加及び機能の拡充を考慮した設計とすること。

解説

運用時の作業の容易さや事業者間の連携、大規模災害時における通信の疎通をで

きる限り維持すること等も考慮しながら、システムの基本的な機能を明確にする。また将来の規模の拡大、端末の挙動を含むトラヒック増加に伴うふくそう監視、制御手法、障害発生時の拡大防止・極小化対策等の機能などをネットワークの設計指針に反映する。

設計指針の明確化は次の点に留意しながら遂行する。

１　システムの基本的な機能を明確にする。

２　システムの基本的な機能を満足させるための諸条件を明確にする。

３　システムの将来設計を明確にする。

４　システムの将来設計を十分に満足させるための諸条件を明確にする。

また、現状において、インターネットの経路制御情報は、日々増えているところであり、ルータの設計においては経路制御情報の将来的な増加（瞬間的かつ急激な増加を除く。）の見通しを踏まえて、ネットワークの設計指針への反映を検討することが重要である。

●措置例●

コスト面等の観点から、特定の機器に、システム構成内において本来期待される機能以外の機能を追加的に設ける場合、当該機器の導入時は障害発生のリスクが低いとしても、導入時からしばらく経過した時期にはトラヒック増加等の影響により、当該機器の処理量がひっ迫することで障害発生のリスクを高める可能性がある。上記を考慮し、システム構成内でも特に重要な機能を担う機器に関しては、追加的に機能を設けることはせず、本来期待される機能に専念させる。

（平成 31 年度告示改正によりまた書きを追加）

イ　トラヒック及びインターネットの経路制御情報等の制御信号の瞬間的かつ急激な増加の対策を講じた設計とすること。

解説

平成 23 年から 24 年にかけて、スマートフォンの急激な普及により、一部の携帯電話事業者において、トラヒックの瞬間的かつ急激な増加（バーストトラヒック）や制御信号の増加を一因とする電気通信事故等が多数発生したことから、本対策を追加した。

具体的に、携帯電話用設備及びＰＨＳ用設備について以下の対策を講じる設計とすることが考えられる。

１　バーストトラフィック対策

①　バーストトラフィックの発生を防止又は抑制する措置（例：位置情報等の取得のための手順の見直し、一斉再接続の抑制等）

②　バーストトラフィックの発生を考慮し、十分に余裕を持った処理能力の確保

２　制御信号対策

①　制御信号の増加による処理を低減させるための措置（例：制御信号抑制技術の採用、負荷の分散等）

②　制御信号の増加を考慮し、十分に余裕を持った処理能力の確保

また、平成 29 年８月に発生した大規模なインターネット接続障害については、約 10 万件を超える情報（障害発生当時、一度に約２年分の経路制御情報に相当。）が配信されたことが原因の一つとなった。

対策としては､同様の障害を想定し十分な余裕をもった処理能力を確保することが考えられるものの､不要な経路制御の送受信を防ぐために有効な機能を設ける観点から設計を行うことも有効である。

しかしながら､こうした機能が自らの利用者や他事業者に影響を与える恐れがあることに留意する必要があるほか､経路制御情報の瞬間的かつ急激な増加を考慮しないことによる影響についても留意する必要がある。

（平成 31 年度告示改正によりまた書き以降を追加）

ウ　重要な機器を導入する場合は、導入判定の統一基準を策定し、その基準に基づき品質の検証を行うこと。

解説

平成 23 年度、設備の設計・設定・配備に誤りがあったため、重大な事故が発生した事例が複数見受けられた。あらかじめ導入判定の統一基準を策定し、その基準に基づいた評価等を行えば、事故を未然に防止できた可能性があることから、本対策を規定する。

エ　重要な機器を調達する場合は、サプライチェーンにおける情報セキュリティを考慮した機器を調達すること

解説

サイバー攻撃等の脅威に対する安全・信頼性対策の１つとして、セキュリティ対策を講じることが重要である。

内閣サイバーセキュリティセンター（ＮＩＳＣ）において「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」が作成・公表されているが、この中でセキュリティ上の脅威への対策として「サプライチェーン･リスク」への対応が求められている。

上記リスクは機器の調達の段階で検討することで軽減することができるため､機器の調達に当たっては考慮するよう努める必要がある。

（平成 27 年度告示改正により追加）

オ　サーバ等機器導入前の機能確認を十分に実施すること。

カ　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及び品質評価手法を事前に確認すること。

解説

サービスに大きな影響を及ぼしかねないサーバ等機器の容量や評価・試験方法等について、事前に十分確認する。またネットワークに影響が生じる可能性があるセキュリティ対策やふくそう時の端末動作についても事前に試験、確認する。

キ　設備の設定値の誤設定・誤入力防止のため、委託業者と連携し、設定変更の確認事項等を明らかにすること。

ク　設備の設定値の誤設定・誤入力防止のため、設定変更後には、実機に導入する前に確認試験を行うこと。

解説

複数の設備間の設定値の不整合、通信量増に応じた設備増は実施したが設定値の変更漏れなどの全体最適･設備横断的な視点の不足、確認項目不足等の人為ミスに起因する事故を防止するため、以下の点に留意した対応を実施することが必要である。

●措置例●

１　パラメータ投入対象の事前洗い出し

２　パラメータ投入作業の同一人物による実施

３　パラメータ投入時における２人作業

４　デフォルト値の設定

５　作業手順の遵守

６　パラメータ投入者と設備管理者間での情報共有（手順書の確認、パラメータチェック等）

（平成 27 年度告示改正により追加）

ケ　設備の不具合を事前に発見するために次の試験を実施すること。

①　デグレード試験

②　過負荷試験

③　商用環境に近い環境における試験

④　品質の定量化試験

解説

多様な観点からの試験を適切に実施し、内在する不具合を事前に発見し、サービス開始後の事故発生を未然に防止することが重要となる。具体的には、

①は、ソフトウェアの変更項目とは独立した、基本試験項目を多数用意し、既存機能に関する予測できないデグレードを防止する

②は、想定される最もトラヒック量が高い状況（時期、時間帯等）を試験の条件として設定し、当該設定下においても想定した挙動をするかどうかを確認する

③は、商用の最新トラヒックパターン、異常時の想定トラヒック、設備によりボトルネックとなるトラヒックケースに応じた試験を実施する

④は、製造･試験工程で品質管理指標値を設け、工程ごとに試験数やバグ検出数のクロスチェックを実施し、不十分と推定される場合は、再度ソースレビューや強化試験等を実施する

ことが考えられる。

（平成 27 年度告示改正により追加）

コ　トラヒックの瞬間的かつ急激な増加への対策として、各装置の最大処理能力を超える負荷試験を実施すること。この場合において、商用環境でのトラヒックパターンを参考に、複数のトラヒック条件での試験を実施すること。

解説

「第３．方法　１．平常時の取組 (3)設計 イ」において、バーストトラヒック対策が規定されているが、過負荷がかかったときの通信機器等の動作を事前に確認しておかなければ、障害時の復旧手順を確立することができないことから、本対策も規定した。

また、より現実に近い形で確認を行うため、実環境でのトラヒックパターンを参考に試験を実施する。

サ　相互接続性の試験・検証方式を明確にすること。

解説

相互接続性を十分に確保するための試験・検証を行う。

●措置例●

相互接続に関する技術的条件を明確化し、その技術条件に準拠していればどの

通信事業者のネットワークとも接続性が確保できるように取り組む。

シ　検収試験及び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つて、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。

解説

設備を導入する際に、受取側が行う検収試験（検査試験）においては、商用網のトラヒックパターンを利用して、実機試験を実施する。

検収試験において、やむを得ず実データを使用する場合には、通信の秘密の保護及びデータ保護に十分配慮する。

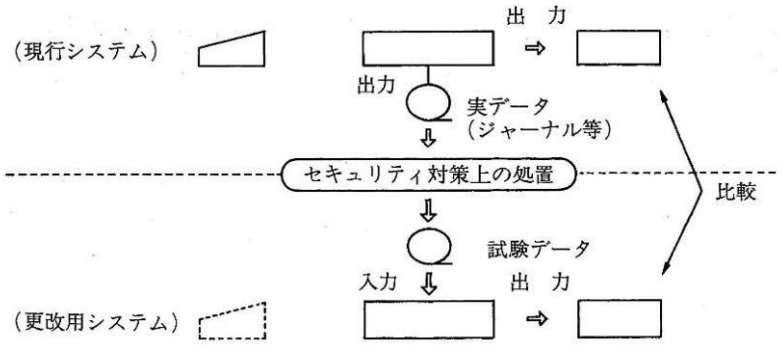
●措置例●

１　パスワード

全てスペースで置換する。パスワードのチェック機能の確認については、実データを使用しない代替方法で個別に行う。

２　氏名、口座番号等

ソートマージ処理でキーとして使用される場合には、スペースで置換できないため疑似データで置換するなど、目的とする機能確認を阻害しない範囲で処置を施す。



検収試験管理

保守作業後の検収試験においては、商用網のトラヒックパターンを利用して、実機試験を実施する。

検収試験において、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に、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、その使用を出来るかぎり回避する。

やむを得ない使用にあたっては、特に通信の秘密の漏えいに万全の注意を払う必要がある。

ス　重要な電気通信設備においては、冗長構成をとるようにすること。

解説

情報通信システムは、安定稼働のため主系と予備系の最低２系統で構築され、主系に不具合が発生した場合には速やかに予備系に切り替わることにより継続した運用を行うことが必要である。

通信センターの分散化や異経路伝送路設備の設置等の他、故障により役務提供の

継続に重大な影響を与える重要な電気通信設備についても、同様の対応をとり、安定的な運用を確保することが必要である。

（平成 27 年度告示改正により追加）

セ　冗長構成をとる電気通信設備においては、予備系への切替動作が確実に行われることを確認すること。
ソ　冗長構成をとる電気通信設備の予備系への切替えができなくなった場合の復旧手順をあらかじめ準備すること。

解説

予備系への切替は、運用形態の１つとして定期的に切り替わる設定をしていない限り、切替が必要となる状況を複数設定し、それぞれの状況下で確実に切り替わることを本番環境に投入する前に十分検証・確認することが必要である。

切替動作は、自動で行われるように設計されていることが多いが、切替動作を司る部分自体に不具合が発生することも想定し、手動で実施することも含めた復旧手順を事前に準備することが必要である。

（平成 27 年度告示改正により追加）

タ　設備及び設備を設置する建築物等の基準及び指標を策定すること。

解説

設備及び設備を設置する建築物等については､設備等基準の｢第２.環境基準　１.センターの建築物｣においても対策を定めているが、電気通信事業者として、設備についても導入のための基準を設けることで､一定の品質を確保することができる。

（平成 27 年度告示改正により追加）

チ　重要な回線については、異なる２者以上の電気通信事業者から提供を受ける等により、信頼性の向上を図ること。

解説

重要な回線については事故又は障害の発生時に大きな影響を受ける恐れがあることから、信頼性の向上を図ることが重要である。

具体的な手段としては、異なる２者以上の電気通信事業者から提供を受けることによる冗長化のほか、拠点引き込みの異経路化や収容ビルの分散等の方法が考えられ、ウェブサービス提供者においては電気通信事業者とネットワーク構成等を踏まえた相談の上、実施判断することが重要である。

（平成 31 年度告示改正により新規追加）

ツ　電気通信事業者が当該電気通信事業者以外の者が提供する設備を利用して電気通信役務を提供する際には、当該設備を利用する電気通信事業者自らが、電気通信設備として必要とされる技術基準を満たしていることを確認すること。

解説

電気通信事業者の通信ネットワークにおいて、物理的な設備の設置場所にかかわらず、インターネット等の外部回線経由で、必要に応じてネットワーク資源を提供可能なクラウドの利用が進展することに伴い、当該電気通信事業者以外の者が提供する設備に故障等が発生し､それによる電気通信役務の提供に支障が発生した場合、電気通信事業者側で原因特定・復旧等が困難となることが想定される。

したがって、従来と同等の品質を担保するため、電気通信事業者が他社設備を利用して電気通信役務を提供する際、電気通信役務全体の安全・信頼性が確保される

よう、当該設備を利用する電気通信事業者自らが、必要とされる基準を満たしていることを確認することが望ましい。

（令和２年度告示改正により新規追加）

(4)　工事

ア　委託事業者等を含めた関連部門間で工事手順書を作成するとともに、その内容の検証を行うこと。

解説

工事の実施に先立ち、工事の目的･内容や工事種別等に応じて、工事の手順・体制、工事後の試験手順、正常性確認項目、切戻し手順などを工事手順書として、手順書作成に関する社の基本指針等に基づいて作成し､内容について検証することは、工事が適切に実施されるために必要である｡具体的には､以下のようなことを行う。

●措置例●

１　工事マニュアル等に基づき作成
２　試験環境でのリハーサル等による検証
３　内容の関連部門間での相互チェック
４　工事責任者による検証
５　作業現場での事前確認

（平成 27 年度告示改正により追加）

イ　相互接続を行う場合は、接続先との間で設計・作業工程を明確にするとともに、その管理を行うこと。

解説

システム設計の段階で機能のモジュール化を図ること等により、相互接続を考慮した設計としておく。インタフェースやプロトコルについては、可能な限り国際勧告及び国内標準を採用する。

相互接続を行う場合には､相互接続実施目標時期を明確にし､相互の要求条件（技術的条件等）を相互接続仕様書としてドキュメント化した上で、総合工程を調整する。

●相互接続仕様書に盛り込む接続条件の具体例●

１　接続形態
２　番号方式
３　信号方式
４　接続シーケンス
５　課金方式
６　試験方式
７　認証方式
８　IP ルーティング
９　QOS 等品質条件
10　IP パケットデータコーディング等各種パラメータ情報等

相互接続仕様書に基づく総合工程に従って互いに必要なシステム開発やシステム改修を行うが、作業の中でドキュメントの不備、不明な点が見つかった場合、開発遅延等による工程見直しが必要になった場合等には、連絡窓口間で調整会議等を招集して仕様書の変更案を取りまとめ、履歴管理を行う。

また、システム開発等の進捗に合わせ、相互に対向試験項目を出し合い、調整の上必要な試験ネットワークを構成し、試験を行う。

●システム開発等から対向試験実施までの間における管理すべき項目の具体例●

1　対向試験項目の洗い出し
2　対向試験ネットワーク構成の決定
3　試験手順書の作成
4　マシンタイムの調整
5　試験回線の開通手配

ウ　工事中に発生する可能性がある事故等に対して、復旧手順をあらかじめ準備すること。

解説

工事の際に事故が発生した場合に、切り戻しができない、二重障害で冗長構成が機能しない、工事対象を絞るなど影響範囲を最小化する措置が不十分であるといったことを防止するため、復旧手順については工事手順書の作成と併せて検討し、手順書等にまとめることが必要である。具体的には、以下のようなことが考えられる。

●措置例●

1　切戻し手順、切戻し時間の明確化、切戻し時間を考慮した手順書の作成
2　利用者への影響の有無を確認し、必要に応じて影響の低い部分から工事を行い、順次、他設備に展開

（平成 27 年度告示改正により追加）

エ　工事終了後、各設備が想定した動作をしていることを確認すること。

解説

工事終了後には、試験を行うことになるが、試験項目の漏れや工事対象外の関連設備への試験漏れ等による事故を防ぐため、十分な検証を実施することが必要である。具体的には以下のような方法が考えられる。

●措置例●

1　実機による正常性確認、設備の異常ログの確認、試験チェック表に基づく正常性確認の実施
2　工事対象装置以外の装置に影響が及ぶ場合を考慮した広範囲の確認項目を作成し、検査を実施

（平成 27 年度告示改正により追加）

オ　設備更改時に必要となる作業をあらかじめまとめておくこと。

解説

設備更改は通常、サービスを継続している中で行われるものであるため、システムを停止させることなく実施することが必要である。しかし、更改作業中に障害等が発生することにより作業が想定よりも長時間になるだけでなく、提供しているサービスに影響が波及することがある。

このような場合を踏まえ、円滑に設備更改を行うことができるよう、予め作業を洗い出し、関係者間で情報共有を図ることが必要である。

（平成 27 年度告示改正により追加）

カ　冗長構成をとる機器は、障害が発生した際に切替動作が確実に行われることを確認すること。

解説

平成２３年度、設備の設計・設定・配備に誤りがあったため、重大な事故が発生

した事例が複数見受けられた。あらかじめ導入判定の統一基準を策定し、その基準に基づいた評価等を行えば、事故を未然に防止できた可能性があることから、本対策を規定した。切替動作の確認方法は、確認を実施する状況に応じて異なる。

●例１：システムの稼働前に実施する場合●

稼働前の実施であるため、設計段階で想定した全パターンについて十分な検証を行うことが必要である。

●例２：システム稼働後に機器を追加（増設）する場合●

この場合、システム稼働時（設計段階）には想定していなかった追加を行うことになるため、機器の追加による既に稼働している機器へ与える影響を検証環境等も活用し、場合によっては当該機器を導入しないといった可能性（別の方法にて対応する）も踏まえ十分に確認することが必要である。

●例３：システム稼働後に設計段階で見込んでいた機器の追加をする場合●

この場合、既に確認は完了しているが稼働時には導入していなかっただけであると考えられるため、基本的には速やかに導入しても他への影響等は発生しないと考えられる。

(5)　維持・運用

ア　設備の動作状況を監視し、故障等を検知した場合は、必要に応じ、予備設備への切換え又は修理を行うこと。

解説

監視、保守及び制御について、以下の措置を講ずること。

●措置例１●

設備の監視はその設備自身又は他の監視設備に、当該設備の異常状態をハード的又はソフト的に検知する機能を具備することにより、自動的に行うことが望ましい。異常状態を検出すると、ランプやブザーによる可視可聴表示やメッセージ出力により保守者に通知することにより、速やかに障害措置がとられるようにする。なお、これらの可視可聴表示やメッセージは、その緊急度に合わせてランク付けすることにより、保守者の作業が効率的に実施できるようにする。

●措置例２●

異常検出時の予備設備への自動切替え等の機能により、設備の信頼性の向上を図る。

イ　部外工事に係る情報や企画型ふくそうの原因となる情報等、情報通信ネットワークの健全な運用に必要な情報の収集のための措置を講ずること。

解説

情報通信ネットワークの保守・運用において、部外工事による障害やふくそうの防止を図るための情報等、ネットワークの健全な適用に必要な情報の収集の強化に努める。

●部外工事に係る情報の入手法の例●

１　国土交通省、都道府県、市町村における工事調整のための会議からの入手
２　道路管理者、警察からの入手
３　道路パトロールからの入手
４　CEPTOAR-Council からの入手

また、イベントなどによるトラヒックの急増と集中（企画型ふくそう）に関する情報収集に努める。

ウ　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。

解説

設計基準をもとに設備の保全基準を設けるとともに、通信の疎通に関して運用基準を設定し、それを維持するよう努める。また、保全・運用に関する各種データの集計管理を行い、設備計画、信頼性設計へ反映させる。

トラヒック状況等に応じて、これら管理基準も適切に見直しを行う。

●措置例１●

設備故障の集計管理及びその評価や設計基準を基に、適正な定期点検及び定期試験等の実施基準を定める。具体的には、設備の信頼性や保全性に関し、次のような基準を定め、これらを統計的に分析することにより、保全成果を客観的に評価する。

１　アベイラビリティ

電気通信設備等がある期間中に規定の機能を維持する時間の割合をいう。

２　MTBF（平均故障間隔）

電気通信設備等の故障と次の故障の間、すなわち無故障で動作している時間の平均値をいう。

３　MTTR（平均修理時間）

電気通信設備等の故障の修理時間、すなわち動作していない時間の平均値をいう。

４　定期点検・試験整備周期

５　老朽設備の置換基準

●措置例２●

運用基準を設定するとともに、運用関連の各種データの管理について基準を設け集計管理を行う。

１　運用基準の設定

通信の疎通を円滑にするため、ある一定の目標値を定め、それに従い、回線障害や異常ふくそうへの対応等の措置基準を定める。また、ネットワーク資源を効率よく使用するため、ルーティング順位、う回経路選択方法等を定める。

２　運用関連の各種データの管理

ネットワークは、日々刻々変化成長するものであり、ネットワークの特性を把握し、運用関連の各種データの現行化維持に努める。そのため、ネットワークの疎通状況をルート毎に数値管理する。

例　接続率、呼損率、待合せ時間分布、自動化率等また、トラヒックデータ等のネットワークに関連したデータを収集し、回線計画、設備計画等に反映する。

①　トラヒック量・分布の測定

ルート毎または区間毎のトラヒック呼量、時間分布、週間分布、歴年分布について定期的に測定して将来を予測し、その結果を回線計画、設備計画等に反映する。

②　回線の故障等の記録

回線の故障記録を保存しておき、故障時の代替ルートの計画に反映させる。また、障害の拡大防止、極小化の観点をネットワーク信頼性設計に反映させる。

③　回線情報のデータベース化

ネットワークが大規模化すれば、上記情報の管理を人手で処理するのは限界に達するので、自動測定装置の導入、回線情報をデータベース化し、必要回線数を自動算出する等の情報処理システムの構築が望ましい。

④　電気通信設備の処理能力の把握

設備機器の処理能力を適切に把握し、将来の需要予測に基づいた設備増強計画に反映する。

３　重要設備の点検

情報通信ネットワークにおいて、ルータ、パケット交換機等の重要設備に対する安全・信頼性基準・指標及び定期点検等の実施方法を策定する。

エ　保全・運用作業の手順化を行い、手順書の作成を行うこと。

解説

保全・運用基準に基づき、保全・運用作業の手順書を作成する。なお、手順書の作成に当たっては、障害発生時の影響の最小化を図れるよう考慮する。

また、インターネットの経路設定時の人為的ミスの防止のため、経路制御情報の設定後において、トラヒックに異常な増大や減少が発生した場合に、原因や影響を把握するために確認すべき事項や復旧のために行うべき措置等について、あらかじめ手順書を作成することが重要である。なお、復旧のために行った措置が二次被害を発生させる原因となる恐れがあることに留意する必要がある。

（平成 31 年度にまた書きを追加）

●措置例１●

保全作業の手順書は､保全作業を実施する上での具体的処理を記述するもので、保全作業を手順化し、その標準的な方法を手順書として定めることにより、定期試験等の保全作業や障害発生時の対応を迅速かつ確実に実施することが期待できる。手順書は、分かりやすく、正確であり、利用しやすいことが重要であり、一般に以下のような内容を記述する。

また､これらはルータ等設備の安全･信頼性基準･指標、トラヒック状況やネットワーク接続構成等により適切な見直しを行う。

１　システム概要

システム構成、処理能力、基本仕様等

２　システムの運転管理

定期的な運転管理機能の概要、実施方法、その手順等

３　定期試験・点検

定期試験・点検の概要、実施方法、その手順等

４　障害対応

障害時のデータ取得、切り分け、故障部位の特定、対応措置の概要、実施方法、その手順等

５　その他

保全作業を実施する上で必要な機能、その実施方法、その手順等

●措置例２●

伝送路障害や異常ふくそうの発生の検知、発生時の措置方法、異常ふくそうが予想される事態への予防措置等について手順書を作成し、情報通信ネットワークの安定的な運用を図る。

１　伝送路故障対応

伝送路故障時の代替伝送路による復旧措置要領を定め、ある一定期間内に

当該伝送路が復旧する見込みがないと予想されるときは、復旧措置要領に規定される代替設定措置計画を発動する。復旧措置要領には、代替復旧連絡責任者、代替復旧局、連絡体系、指示系統、復旧順位を定めるほか、実施手順書には伝送路毎の代替設定措置計画、必要なパッチプランを定める。

なお、ネットワークは常に変化成長するため、代替設定用通信設備の確保および代替設定措置計画の維持管理が重要である。

２　異常ふくそう対応

ふくそうの検知方法、ふくそう発生時の制御方法を明確にするとともに、特定の交換設備またはルートがふくそうすることが予想される場合は、他の交換局にう回させたり、強制的に回線閉塞を行ったりして、網に異常が波及しないよう網管理措置の要領を定める。

また、相互接続事業者間での連携について予め確認しておくこと。

３　故障箇所特定

故障が発生した際に故障箇所や原因の特定を迅速化し、サービスへの影響をできる限り少なくするための対策を講じる。

オ　経年劣化による自然故障が軽減するよう監視データの分析を行うこと。

解説

情報通信ネットワークを構成する機器は、経年劣化により機器の故障率が次第に上昇することを考慮し、特に自然故障による影響を軽減するよう、機器の稼働状況等のデータを収集し、自然故障に繋がる異常値を見落とすことがないようにする必要がある。

（平成 27 年度告示改正により追加）

カ　定期的に保守点検を実施すること。

キ　設備を設置する建築物及び空気調和設備の定期的な保全点検を実施すること。

解説

ネットワーク機器の定期的な保守点検は、安定的な運用ために必要なものである。保守点検の実施に当たっては、予め点検対象ごとに年間スケジュール（月次、四半期毎、年次）を立て、対象漏れ等が生じないよう注意することが必要である。

また、ネットワーク機器を設置する建築物やその建築物に設置されている空調設備等についても、機器の稼働に影響を及ぼすことから、定期的な点検が求められる。設備を設置する建築物及びその建築物に設置される空調設備等は通常、当該建築物を管理・運用している者が自らの年間スケジュールに沿った点検を実施するため、当該スケジュールについて予め把握しておくことが必要である。

（キは平成 27 年度告示改正により追加）

ク　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。

ケ　保守の委託を行う場合は、作業手順を明確にするとともに、監督を行うこと。

解説

ク　情報通信ネットワークの保守を外部に委託する場合は、保守の範囲と責任範囲を明確化にしておくことが必要である。また、委託元は、委託先の作業内容について定期的な監督を行い、実施している作業内容等が委託先と合意したものであるかどうかについて確認することが必要である。

●措置例●

具体的には次のような内容を網羅した委託契約を交わすことが望ましい。

保守作業の範囲

1　保守方法
2　機密の保持
3　責任の範囲
4　原因分析体制
5　保守体制
6　立ち入り場所の限定、およびその手続き
7　免責事項の内容
8　相互の提供情報内容及び連絡責任者
9　情報セキュリティの確保
10　障害時の対応、及び報告

ケ　委託保守においては、その作業手順を明確にし、所要の監督を行う。

●措置例●

具体的には前項で述べたような委託契約に基づき、作業中の立ち会い、終了後の確認を行う。その際、必ず責任者のサインを交わして相互の責任を明確にしておく。また、情報セキュリティ管理に関する監査を定期的に実施する。

（クは平成 27 年度告示改正により追加）

コ　故障等における迅速な原因分析のための事業者と機器等の製造・販売等を行う者や業務委託先との連携体制を確立すること。

解説

故障、障害等に対して、迅速な原因分析のための事業者とベンダ・業務委託先間で連携体制などについて十分整理しておくことが必要である。

●措置例●

1　原因分析体制や処理時間の実態を書面などで定期的に確認することなどを保守契約などに盛り込むこと。
2　ベンダなどへ解析を依頼する場合には、解析に必要な十分な情報を提供すること。
3　間欠的に故障が発生する場合においても、故障が固定化、拡大化する前にベンダなどと連携して適切な対策を立てること。
4　ベンダや業務委託先との共同訓練を実施すること。

サ　業務委託先の選別の評価要件の設定を行うこと。

解説

事業者は、情報セキュリティに関する外部認証を取得していることを外部委託先の要件として取り入れる等、外部委託先の情報セキュリティ確保に努めること。

なお、機密の保持については守秘義務・保持契約を締結するとともに、守秘義務・保持契約条項の具体化、秘密保持に係る誓約書の徴収、外部委託先の監査実施、監査時のチェック項目、監査において不具合が発見された際の是正処置依頼・是正処置結果の確認などを含めた情報管理規程の策定など、委託先の取り組みの要求条件を明確化する。

シ　通信の秘密の確保に関する取組を実施すること。

解説

「通信の秘密」は、電気通信事業法第４条において侵してはならない旨規定されている。ここでいう通信は、音声に限らずデータ伝送も適用されることに留意しつつ、事業者は、通信の秘密について厳格に対処することが必要である。

（平成 27 年度告示改正により追加）

ス　復旧対策の手順化を行うこと。

解説

臨時措置による通信の疎通確保の方法、ネットワークの復旧計画等について、手順書を作成しておく、又、事前配備した復旧用資材の使用について、手順書の作成及び管理を行う。

●措置例●

非常事態とは､通常の災害･障害の範囲を超えたネットワークへの被害であり、かなりの規模と想定される。従って、まず、要員の確保を考慮し、実際の通信の確保の作業は重大事故時の措置による｡要員の確保については､時間､交通事情、災害の発生場所、職員の住居等を考慮した連絡、呼び出し体制を作り、連絡の手段を明確にファイル化し、必要に応じて訓練を行う。

具体的手順としては、以下のようなものが考えられる。

１　障害状況の正確な把握

２　稼働可能な設備の状況把握

３　ネットワーク再構築の方法決定

①　ルート切り替え

②　代替ルート構築

③　その他

４　前項について予め被害区間を想定して復旧手順を作成する。

①　設備構成

②　接続試験手順

③　回線収容計画

④　関係連絡方法

セ　データ投入等における高い信頼性が求められる作業において、容易に誤りが混入しないよう措置を講ずること。

解説

データ投入等における高い信頼性が求められる作業において、容易に誤りが混入しないよう措置を講ずる。

経路制御情報の設定作業は、自動処理で行われる部分はあるものの、新規接続先情報の入力など人手による作業が必ず含まれる。そのため、経路制御情報の設定作業のみならず､様々な作業工程においても人為的ミスを完全に防ぐことはできない。

しかしながら、経路制御情報に不具合が発生した場合、インターネット全体に甚大な影響が出るおそれがあることに鑑みれば､経路制御情報の設定作業においては、人為的ミスによる障害を避けるため、設定が反映される前に、システムによる人為的ミスの防止を目的とした処理の実施や、複数人体制によるチェックの徹底が重要である。

（平成 31 年度告示改正により新規追加）

ソ　データを蓄積する機能を有する設備については、メモリ領域の状況等の定期

的な監視・点検を実施すること。

解説

令和４年度に、電気通信設備において過去の経路情報が自動削除されず、情報が蓄積され続けた結果、メモリが枯渇し、当該電気通信設備に不具合が生じ、重大な事故に発展する事案が発生したことから、本対策を規定した。

データを蓄積する機能を有する設備については、メモリ領域の状況等の定期的な監視・点検を実施するとともに、自動で削除等がなされない場合は、必要に応じて過去の情報の削除等を手動で行い、電気通信設備において正常な機能が発揮できる状態を維持することが望ましい。

（令和５年度施行規則等改正に伴い追加）

(6)　情報セキュリティ対策

ア　情報セキュリティに関する情報収集を行うこと。

解説

サイバー攻撃等の脅威に対する安全・信頼性対策の一つとしてセキュリティ対策を講じることは極めて重要である。情報セキュリティ対策については、定期的な情報収集をすることにより常に最新の情報を確保しておくことが必要である。

（平成 27 年度告示改正により追加）

イ　情報セキュリティ対策についてその手法及び事前確認を十分行うこと。

解説

サービスに大きな影響を及ぼしかねないサーバ等機器の容量や評価・試験方法等について、事前に十分確認する。またネットワークに影響が生じる可能性があるセキュリティ対策やふくそう時の端末動作についても事前に試験、確認する。

ウ　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。

解説

情報セキュリティ技術の高度化のスピードは、著しく、それだけに陳腐化の速度も速いといえる。最新のセキュリティ技術の情報やセキュリティ事業者の商品の開発動向等の把握とその活用は、適切なセキュリティ対策を推進する上で重要な要素となる

●措置例●

具体的には、最新の次の技術を採用することが適当である。

１　暗号技術

２　ユーザ認証技術

３　アクセス・コントロール技術

４　不正アクセス検知技術等

また、ISO（国際標準化機構）/IEC（国際電気標準会議）等によりシステム管理のガイドライン（下記参照）や技術基準が策定され、我が国でもそれらを参照しながら情報セキュリティ関連のガイドラインや技術基準が作成されているため、これらのガイドラインを考慮することが望ましい。

（参考）

１　電気通信事業における情報セキュリティマネジメントガイドライン(ISM-TG)

ISO/IEC17799 をベースに、電気通信事業者が遵守すべき情報セキュリティ

マネジメントを実践するための規範を、業界ガイドラインとして策定したものであり、「電気通信分野における情報セキュリティ対策協議会」にて 2006 年６月 29 日に決定している。

２　セキュリティ評価基準等(ISO/IEC 15408 等)

ISO/IEC 15408 は、欧米各国・地域でそれぞれ独自に定めていたセキュリティ評価基準を統一化して国際標準化したものであり、1999 年 12 月に ISO/IEC で制定された。

国内においては、ISO/IEC 15408 と同等の規定である JIS X 5070 を策定するとともに、2001 年より、ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度が独立行政法人情報処理推進機構により運用されている。

エ　コンピュータウィルス並びに端末及びソフトウェアの脆弱性に関する情報を入手したときは、必要に応じて、緊急連絡先に直ちに連絡すること。

解説

ウイルス発生時緊急情報の収集、通報を円滑に行うため、電気通信関係団体で構成する対策会議が、平成 12 年５月に設置され、緊急連絡体制が確立されている。コンピュータウイルス発生等の緊急情報は、緊急連絡網を通して関係事業者に周知され、かつ、被害状況の情報収集も円滑に行われるシステムとなっている。各事業者は、これらの連絡網や T-CEPTOAR 等にコンピュータウイルスやサイバー攻撃に関する情報を提供する体制の確立が必要である。

オ　コンピュータウィルス並びに端末及びソフトウェアの脆弱性に関する情報を入手したときは、必要に応じて、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サイトへの掲示、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。

解説

コンピュータウイルスは、自社内ネットワークへの感染及び利用者のネットワークやパソコン端末に感染する可能性があることから、大規模な拡大が危倶される情報を入手したときは、その対策を含めた情報を速やかに関係者に提供する必要がある。利用者への情報提供手段としては、ウェブへの掲示、メールニュース等が考えられる。

カ　ネットワーク内の装置類やサービスの属性に応じて情報を分類すること。

解説

取扱規程及び管理責任者を適切に設定する等により、情報の管理に関する内部統制ルールの整備を行うことは、情報を適切に保護し維持するために必要である。重要情報の流失防止のためにも、内部統制ルールに関する事項の整備を行うことが必要である。

これらの実施の適切性を担保するために、ISMS 認証等の外部認証の活用も有効である。

●例　情報漏えい対策●

社内 O&M(Operation & Maintenance)システム等のウイルス対策は行っても、社員・職員、外部の業務委託先など個人用 PC における対策をチェックすることには限界がある。

従って、自宅へ持ち帰っての業務禁止、個人用 PC へのファイル交換 SW 使用禁止等、社員・職員・委託先等への教育が不可欠であり、また、外部媒体（USB メ

モリー等）からのウイルス感染も考慮して、個人用の外部媒体使用禁止なども検討する必要がある。

自宅での業務を許可する場合においては、盗難・紛失されても遠隔操作でデータを消去・ロックできるPCを利用するなど、自衛策を講じる必要がある。

キ　データ管理基準を設定すること。

解説

データの取扱いを行う上で、データの入力、処理、出力及び保管時等における基準を設け、その管理を行う。又、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の世代管理の基準を設け、その管理を行う。利用者の暗証番号等の取扱いにおいても、管理基準を設け、他への漏えいを防止する。

また、事業者からベンダに送付されるサーバ障害ログ等、電気通信事業者以外の者が取り扱う情報の管理方法や、業務の委託（請負）先での情報管理方法についても具体的にドキュメントに定め、電気通信事業者による管理方法の変更がある場合にもベンダや委託先へ迅速に適用されることが必要である。

●措置例●

以下の項目について入出力処理及び保管時等のデータ管理基準を定める。

また、外部に委託する場合のデータ管理基準も同様の基準を定め、委託先が確実にデータ管理基準を順守していることを確認するための監査を実施する。

１　対象データの指定方法
２　データ取扱いの優先度、重要度の分類方法
３　分類された重要度による取扱い方法
４　データの保管方法
５　データ運用・管理の記録方法
６　データの正確性、正当性、妥当性の確認方法
７　データ移転時の処理方法
８　パスワード等の管理方法
９　データ管理の責任者の責務
10　障害等により機器が事業者から委託先へ移された場合のデータ取扱い基準と方法

ク　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。

解説

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、その重要度による分類を行い、取扱い者の制限を含め重要度に応じた管理を行う。

●措置例●

通信の秘密の保護、データ保護及び復元の可能性の度合いに応じ、設備に係るデータ及び文書類に関する重要度の分類を行い、この分類に基づき、コピーの禁止、発行部数限定、保有者限定、媒体の種類に応じた廃棄処分方法等の取り扱い範囲を内規等のドキュメントに定める。

ベンダ等事業者以外での保守作業が増加しており、通信の秘密や個人情報などの漏えいを防止するために、故障物品内に格納された情報の漏洩防止対策を講じることが必要である。また、記録媒体の性能向上が著しく、容量が大きいがサイズは小さくなっていることから、保管については紛失、盗難などに十分に配慮する必要が

ある。

●措置例●

１　事業者からベンダに送付されたサーバの障害ログ媒体の扱いの取り決め等、事業者以外の者が取り扱う情報の管理方法を明確にする。

２　委託（請負）先での情報管理方法や選定方法を具体化して、ドキュメントに定め、事業者の管理方法の変更を迅速に織り込んでいく。

ケ　データ取扱作業の手順化を行うこと。

解説

通常時のデータ取扱い作業について手順化を行った上で手順書を作成し、それに従って作業を行う。

手順化に当たっては、通信の安定的な疎通を図るため、各作業の目的（意味）、位置付け（関連）が明確に管理者及び作業者に理解され、データの重要度に応じた管理者及び作業者の責任範囲と権限との整合性が確保されており、非常事態発生時の措置への移行が円滑かつ混乱なく行われるよう配慮されていることが望ましい。

また、通信の秘密保護のため、データの漏えいに十分注意がなされており、データの保護に関しても取扱いが特定の者のみに偏らない等、データ取扱いの基準に合致していることが要求される。

コ　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。

サ　利用者の暗証番号等の秘密の保護に配慮すること。

解説

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で秘密を要するものについては、従事者の守秘義務の範囲を明確にし、その周知、徹底を図る。

通信設備の設計、運用及び保守に係るデータ及び文書類は間接、直接を問わず、通信度にクラス分けを行い、それぞれ取扱いに携わっている従事者に対し、データ及び文書類の持っている意味を十分に理解させ倫理を確立し、秘密性・重要度に応じた守秘義務を負わせる。業務を外部に委託する場合には、委託先がデータ管理基準を適切に設定し、確実に守る体制であることを確認する。

●措置例●

１　社内における範囲

業務上必要な場合を除いて開示しない。

２　社外における範囲

裁判所、警察等法律上照会権限を有する者から照会があった場合でも、公共の福祉を除いて、原則として開示しない。従って、やむを得ず開示する場合の手続については、あらかじめ定めておく必要がある。

また、従事者が在職中に知り得た情報を第三者に漏らしたり、自ら利用したりしてはならない。

重要度	データ、文書等	管理方法
A	・IDカードの仕様書 ・パスワードの登録簿 等、セキュリティを保持する上で大きな影響を与えるもの	特別に指定された者のみによって厳重に保管され、それ以外の者が見ることは許されない。
B	設備の仕様書、配置図等のうち、セキュリティを保持する上で大きな影	管理責任者の元に管理され、業務遂行上必要と認められ

	響を与えるもの	る場合は、管理責任者の許可を得て見ることができる。
C	上記以外	管理責任者の元に管理され、必要時には特に許可を得ないで見ることができる。 ただし、業務遂行上、外部の者に見せる必要が生じた場合には、管理責任者の許可が必要。

データ、文書等の重要度による分類例

シ　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や脅威の拡大に応じた適時の点検及び見直しを行うこと。

解説

複数のシステムが複雑に接続する場合には、それぞれのシステムだけではなく、その相互作用によるリスク・脅威の評価も必要になるため、技術革新に合わせた適時の点検・見直しが必要である。

ス　情報管理に関する内部統制ルールを整備すること。

解説

取扱規程及び管理責任者を適切に設定する等により、情報の管理に関する内部統制ルールの整備を行うことは、情報を適切に保護し維持するために必要である。重要情報の流失防止のためにも、内部統制ルールに関する事項の整備を行うことが必要である。

これらの実施の適切性を担保するために、ISMS 認証等の外部認証の活用も有効である。

●例　情報漏えい対策●

社内 O&M(Operation & Maintenance)システム等のウイルス対策は行っても、社員・職員、外部の業務委託先など個人用 PC における対策をチェックすることには限界がある。

従って、自宅へ持ち帰っての業務禁止、個人用 PC へのファイル交換 SW 使用禁止等、社員・職員・委託先等への教育が不可欠であり、また、外部媒体（USB メモリー等）からのウイルス感染も考慮して、個人用の外部媒体使用禁止なども検討する必要がある。

自宅での業務を許可する場合においては、盗難・紛失されても遠隔操作でデータを消去・ロックできる PC を利用するなど、自衛策を講じる必要がある。

セ　監査時における確認項目の策定と定期的な内部監査及び外部監査を実施し、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。

解説

情報資産の保持という観点から、サービスを提供する当事者以外の第三者、例えば外部機関又はネットワーク運用部門と独立した部門等によるセキュリティ監査制度を導入し、不正アクセスやコンピュータウイルスなどによる情報漏えい対策等の問題点の把握等適切に努めることが必要である。監査制度導入にあたっては、より具体的なチェック項目を定め、定期的に監査を実施することが必要である。この監査結果を受け情報セキュリティ対策等全体の見直しを行うことが必要であるが、この監査制度の位置づけを明確にし、組織内で強制力が働くような仕組みにしておくことが必要である。

また、電気通信事業に係る個人情報や重要なシステム情報が外部委託先から漏えいすることを防止するため委託先等の外部機関についても電気通信事業者と同様な情報セキュリティ対策を施すことが必要である。

●措置例１●

業務を外部委託する際に守秘義務・保持契約の義務化と守秘義務・保持契約条項を明確化するとともに、外部委託先の監査チェック項目と監査の実施方法、是正処置依頼と処置結果の確認方法等、委託先との確認項目を具体的にドキュメント化し、委託先の取組みを明確化する。

●措置例２●外部監査のチェック項目の策定と定期的な内部・外部監査の実施

外部監査を依頼する場合は、チェック項目を依頼先と検討して策定することが必要である。内部監査を実施する場合は、設備の責任者立会いの元で実施することが必要である。また、年に１回以上の監査を実施することが必要である。

ソ　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。

解説

情報通信システムの重要性に鑑み、システムを停止・機能低下させるおそれのある重要なシステム情報の流出については、その事実を的確に把握し対策を講ずる。

タ　サイバー攻撃への対策を講ずるとともに、発生時には迅速に情報共有する方法を確立すること。

解説

サイバー攻撃には社内への影響だけでなく、広く事業者全体への重大な影響を及ぼす攻撃がある。サイバー攻撃に対する社内への準備とともに、事業者全体に影響を及ぼす重大な攻撃の発生に対しては可能な限り迅速に情報を共有し被害の拡大を防ぐ方策が必要である。このため、あらかじめ社内に留めるレベルか、広く事業者間で共有すべき情報の基準を明確にしておくことが必要である。

●措置例●

T-CEPTOAR 等において、以下の項目について情報共有の在り方を確立する。

１　サイバー攻撃の危険度

２　事業者間での情報共有

３　国に提供する情報

チ　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つた場所に別に保管すること。

解説

広域災害に対処するため、重要なプログラムや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は前世代のファイルも含め、同一ファイルを地域的に十分隔たった場所に別に保管しておく。

●措置例１●

媒体の火災等による破壊あるいは盗難等の事故防止のため、重要なデータ・ファイルやプログラム・ファイルは、同一のものを離隔保管する。広域災害も考慮し、安全性を確認の上、十分に離れた距離に設置された通信センターや離隔地に設けた保管設備に保管する。

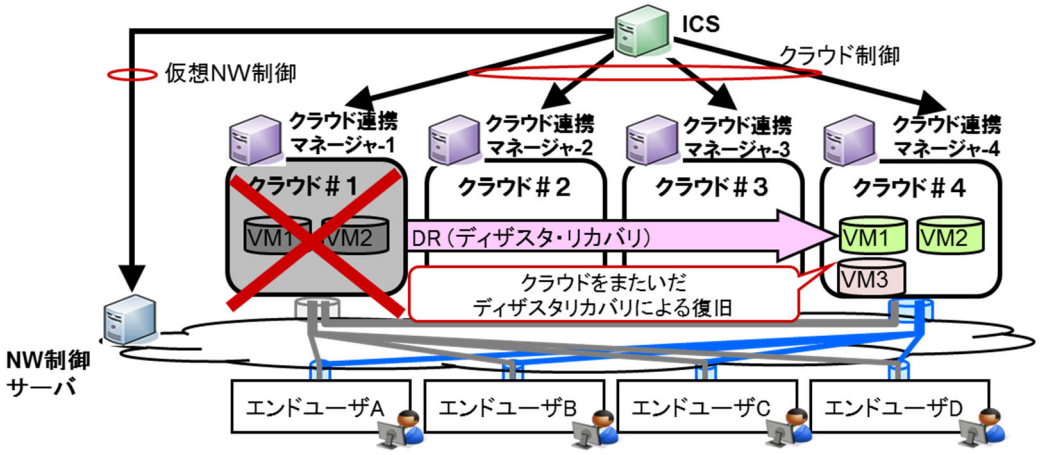
やむを得ず同一ビル内で離隔保管を行う場合は、防火区画上の分離、耐火金

庫を使用する等の安全対策上の措置を講じ、なるべく離れた場所に保管する。データ・ファイルやプログラム・ファイルを離隔地に伝送する方法としては、高速回線を用いて伝送する方法とトラック（空気調和設備付き）等によって運搬する方法がある。

保管ファイルの更新の周期や送達方法はシステムの回復に要する時間等を考慮して定める。

●措置例２●

クラウドサービスを提供する電気通信事業者においては、インタークラウド技術を活用して地理的に分散するクラウド間を跨がったディザスタリカバリを実行することにより、遠隔地にデータ・ファイルやプログラム・ファイルを運搬する方法もある。



インタークラウドサービス機能（ICS）を活用した複数クラウド連携の例

ツ　コンピュータウィルス又は不正プログラムが混入した際に、情報通信ネットワークに対して利用者が与え、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。

解説

利用者がDDoS(分散協調型サービス拒否)攻撃の踏み台となった場合に与えるネットワークへの影響や携帯電話端末への不正プログラムの侵入等を回避するため、利用者に対してその脅威と対策について周知する必要がある。

(7)　ソフトウェアの信頼性確保

ア　ソフトウェアの要求仕様は、サービス内容及び通信需要予測を踏まえて策定すること。

イ　ソフトウェア開発を委託する場合は、委託業者との連携により仕様誤認・設計開発面での誤認を防止すること。

ウ　ソフトウェア不具合による動作不良等を防止するための監視項目・方法を事前に確認すること。

解説

設備の収容者数、トラヒックやセッション数等の見誤り・考慮不足、異常呼（一定長以上のパケット等）に対する考慮不足、開発ベンダとの連携不足によるリソースの枯渇や解放漏れなどのソフトウェアバグによる電気通信事故を防止するため、ソフトウェアの要求仕様は、委託業者と連携をとり、サービスの内容や通信需要予測等を踏まえて策定することが必要である。

●措置例●

1　要求仕様を詳細に策定し、ドキュメントとして明確化

2　要求仕様との対照を行う設計レビューや手順レビューを実施することによるベンダとの間の仕様誤認や設計･開発面でのミスの防止

3　全てのソフトウェアバグの事前解消が困難であることを前提とした監視項目不足や監視方法不備などによる監視漏れの防止を目的とした設計の実施

（平成 27 年度告示改正により追加）

エ　ソフトウェアの試験は、商用環境に近い環境で試験を実施すること。

解説

商用環境を想定して作成されたソフトウェアは、試験の実施に当たっても商用環境に近い環境で実施することが重要である。

（平成 27 年度告示改正により追加）

オ　定期的にソフトウェアのリスク分析を行うとともに、更新の必要性を確認すること。

解説

導入されているソフトウェアには、導入時には判明していなかったバグや不具合への対応を実施したセキュリティパッチが適用されている場合があるが、当該パッチを即時に適用すると、これまで安定的に稼働していたシステムに予期せぬ不具合が生じる場合がある。

また、導入しているソフトウェアに、新たにバグや不具合が判明した場合であっても、稼働しているシステムに直接影響を与えないことが確認できた場合には、セキュリティパッチを適用しないことがシステムの安定的な稼働に資することもある。

このため､セキュリティパッチ等に関する情報がアナウンスされた際には､まず、セキュリティパッチ等の導入によるシステムへの影響について、事前に検証環境等により確認し、更新の必要性について確認の上で対応を行う必要がある。

（平成 27 年度告示改正により追加）

カ　使用しているソフトウェアの安全・信頼性の基準及び指標を策定すること。

解説

上記オにも関連するが、システムに採用しているソフトウェアを導入する際の基準（バグ発見時に原因特定まで遡及可能かどうか、特定された原因の横展開（当該原因が他の設備に影響を及ぼしているか否か）等）についても、ソフトウェア開発業者と認識をあわせて策定しておくことが必要である。

（平成 27 年度告示改正により追加）

キ　交換機の制御等に用いられる重要なソフトウェアについては､機器等の製造･販売を行う者等関係者との契約書等において、サービスの提供の継続に重要と考えられる有効期限等の情報を確認できることを明示すること。

解説

ソフトウェア開発を外部に委託することや市販のソフトウェアをパッケージとして導入することによる「ブラックボックス化」が進展する中、事業者がソフトウェア内で証明書が利用されていることを認識できない場合、証明書の有効期限切れによる突然の機能停止による障害が発生する危険性がある。また、ソフトウェアに起因する障害発生時に事業者において障害原因の特定及び対処に時間を要する一因と

なりうる。
そのため、特に交換機の制御等に用いられる重要なソフトウェアに関しては、機器等の製造・販売を行う者等関係者との契約書等により、サービスの提供の継続に重要と考えられる有効期限等の情報を確認できるよう明示することが重要である。

●措置例●

有効期限が設定されている証明書については、事業者がその存在を認識できるように、ソースコード中に直接埋め込まない（ハードコーディングしない）ことを契約書等に明示する。

（令和元年度告示改正により追加）

ク　ソフトウェアに有効期限が設定されている場合は、電気通信事業者が自ら又は機器等の製造･販売を行う者等関係者との契約等を通じて､確実に管理すること。

解説

ソフトウェアに有効期限が設定されている場合は、失効による機能停止を起こさないように､ライセンスや証明書等の有効期限を適切に管理することが必要である。
ソフトウェアの有効期限の管理に当たっては、電気通信事業者が自ら管理を行うか、又は機器等の製造・販売を行う者等関係者との契約等を通じて、適切に有効期限の更新が行われるよう管理を行う必要がある。

（令和元年度告示改正により追加）

(8)　重要通信の確保 重要通信を扱う場合は、その通信の確保に関する取組を実施すること。

解説

別表第２ 第２．２．(6)参照。

（平成 27 年度告示改正により追加）

(9)　ふくそう対策 ア　情報通信ネットワークのふくそうを回避するため、災害時におけるユーザの行動や端末の動作がネットワークに与える影響を事前に確認すること。

解説

サービスに大きな影響を及ぼしかねないサーバ等機器の容量や評価・試験方法等について、事前に十分確認する。またネットワークに影響が生じる可能性があるセキュリティ対策やふくそう時の端末動作についても事前に試験、確認する。

イ　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、利用者への協力依頼・周知のための措置を講ずること。

解説

情報通信ネットワークの運用に当たり、その有効活用を確保するため、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。さらにユーザへの周知の基準・内容について通信事業者間で協調して取り組むことが望ましい。

●措置例●

地震、豪雨、台風等の災害時における家族の安否確認等の増加によってふくそうが発生し、通信の疎通が確保できなくなることがある。このため、ふくそうを回避する方策として、以下のような方法により、不急の電話の自粛、災害用伝言ダイヤル等の利用等について利用者への協力依頼を行う。

１　パンフレット等による広報活動

２　防災訓練等における広報活動
３　広報車などによる広報活動
４　報道機関に対する広報依頼
５　災害用伝言ダイヤル、災害用伝言板サービス等の利用促進広報活動

ウ　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、相互接続する電気通信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。

解説

災害時において、大規模なふくそうが発生し、又はふくそうが発生するおそれがある場合には、緊急通報や災害救助機関の通信等、重要通信を確保するため、相互接続する事業者間で互いに協調して、接続規制等のふくそう対策を実施する。

また、各事業者において、ふくそうの波及防止について一層のノウハウの蓄積を図るとともに、ふくそう時における通信規制など緊急対応の実施手順や管理体制の整備、さらにふくそうを事前に防止するための設備増強等の長期的視点での対策に取り組むことが必要である。

なお、停電回復後においては、端末からのセッションリクエスト（再登録要求）の集中によるふくそうへの対策を実施することが必要である。

●措置例●

以下の項目を事業者間で協調して対応する。

１　ふくそう検知、制御方法
２　波及防止のための通信規制など緊急対応、手順
３　ふくそう時のユーザ間の公平性の確保のための対策
４　事業者間連絡体制
５　ふくそう情報、障害情報を自動通知する手段
６　ふくそう、障害履歴・事例の蓄積と対応措置改善プロセス

エ　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。

解説

情報通信ネットワークの動作作業の監視を行い、回線故障や異常ふくそう等の発生を検知した場合、速やかに接続規制やう回ルーティングの制御措置を講ずる。

●措置例１●

伝送路障害監視システムにより回線故障の発生を検知し、故障箇所及びメディアを即座に発見する。

●措置例２●

交換機から、CPU 使用率、ルートビジー情報、トラヒック呼量等の状態管理情報を取り出し、異常ふくそう等の発生を検知する。

●措置例３●

回線故障、網ふくそう等の網状態を総合的にあるグローバルに表示する網管理システムを設置し、回線故障や異常ふくそう等を検知した場合、速やかに接続規制、非常う回ルーティング等のトラヒック制御措置を講じる。この機能を担う特別の組織として、網管理センターを設け、ネットワークの運用保守に係る事業所を統括する。

オ　災害時優先通信の機能により他の通信の制限又は停止を行つた場合には、災害時優先通信及び他の通信の疎通の状況を記録・分析すること。

解説

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、記録・分析する。

(10)　緊急通報

緊急通報を扱う場合は、その通報の確保に関する取組を実施すること。

解説

別表第１　第１．　１．(13)参照。

（平成 27 年度告示改正により追加）

(11)　防犯対策

ア　防犯管理の手順化を行うこと。

解説

異常事態発生時の対処を含め、管理の方法について手順化しておく。

異常事態発生時には、第一次対応が最も重要であるため、状況を正確に報告できることに重点を置き、代理者を含め、各人の責任分担を明確にするとともに、連絡・報告、現状分析、対策等に関し、即応できるように予め手順化しておく。

イ　入出管理記録は、一定の期間保管すること。

解説

異常事態の発生時に状況分析を行うことができるよう受付簿や監視装置で取得したビデオテープ等の記録物について、一定の期間、保管管理を行う。

●措置例●

受付簿について、日時、氏名、会社名、連絡先、被面会者名、目的等、必要事項を記入させるとともに、年１、２回実施状況を監査する。ビデオテープ等の目視できない媒体の保管に当たっては、外部ラベルに日時、取扱者等必要事項を記入するとともに、必要な時に再現できるよう保管方法を考慮する。

ウ　入建築物、通信機械室等の入出管理を行うこと。

解説

監視装置や受付等により入出管理を行う。

●措置例●

不法な侵入が行われないよう、侵入口となり易い出入口、窓、排気口、排煙口等の定期点検を実施するとともに、通常の手段で利用され易い出入口については監視装置や受付者を置き、入出者の状況及び入出時の手荷物の状況について管理する。

又、それらのビデオテープや受付簿等の記録物について管理を行う。

外部からの入室者には、それが明確に判定できる表示の着用を義務付け、その立ち入り場所についても入室の目的、資格等により制限する。

エ　出入口の鍵、暗証番号等の適切な管理を行うこと。

解説

出入口の鍵の使用状況、暗証番号の付与状況については、現状の把握を行い適切に管理する。

●措置例●

出入口の鍵には、金属鍵、磁気カード鍵など実態のあるものと暗証番号など実体のないものとがあり、実体のあるものについては常にその存在場所を把握できるように、又、実体のないものについては、運用方法等によりその暗証番号を窃取されないように、管理要領を作成し、それを遵守する。

実体のあるものの管理要領としては、鍵自体の複製を防止するとともに使用数を限定し、使用者・管理者を明確に区別するとともに、出来れば一人では使用出来ない方法が望ましい。実体のないものは、運用中に暗証番号は窃取されることが想定されるため、適宜番号の変更を行う等、運用面からの管理も有効となる。

オ　建築物、防犯装置等の保全点検を定期的に行うこと。

解説

1　各種の監視装置や警報装置等の防犯装置は、定期点検を行い、正常に動作するようにしておく。

2　建築物に損壊、漏水等不良箇所が発生していないか定期的に点検する。(テナントビルのような場合は、その建築物の管理者等により点検されていればよい。)

3　建築物に損壊、漏水等不良箇所があると、これにより電気通信設備が被害を受け、場合によっては人体へ被害を与えることがある他、その発生原因が人為的なものであれば、通信設備の破壊を目的としたものとも考えられるため、建築物の状況を定期的に点検する。

4　空気調和設備が正常に機能するよう定期的に点検する。(テナントビルのような場合は、その建築物の管理者等により点検されていること。)

5　電気通信設備を良好な状態で運転を継続させるためには、その環境条件が整備されていることが必要であり、特に周囲の温度、湿度及び塵検量を適正に保たなければならない。空気調和設備の信頼度は電気通信設備の信頼度に影響するため、空気調和設備の良好な稼働を図るため、定期点検を行い、空気調和の対象となる室の温度、湿度及び塵挨の定期点検を行う。

●措置例●

1　防犯装置の稼働状況が、外部から一見して確認できるような表示機能を有するとともに、表示内容と機能状態とが一致していることを確認するため、定期点検を行う。保全点検の実施時期、試験項目、試験方法、実施者、確認者、記録方法等を定めた管理要領を作成し、点検の実施状況を検査する。また、各種監視装置及び警報装置のリセット等の操作について、特定者以外の者が不正に操作できないよう取扱規程を明確にし、遵守状況を管理する。

2　建築物の点検箇所、点検方法、期間、確認責任者、管理状況簿への記入方法等を定めた建築物管理要領を定め、継続的な管理を実施する。漏水検知器、火災報知設備等については、テストを行い、機能が十分発揮できるかどうかを確認する。

①　温度・湿度等については、記録計を設置し監視する。

②　操作盤・バルブ等については、定常状態を表示しておく。

③　水質等については、汚濁されていないかどうかを監視する。

④　予備機器がある場合には、その稼働テストを行う。

(12)　現状の調査・分析・改善

ア　災害時優先通信の機能により他の通信の制限又は停止を行った場合には、災害時優先通信及び他の通信の疎通の状況を記録・分析すること。

解説

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、記録・分析する。

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・分析を行う項目、評価方法等の基準を設定すること。

解説

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、分析を行う項目及び評価方法等について基準を設ける。

●措置例●

実施要領、手順書等に定められている運用保全作業の項目及び内容がどのような形で成果となっているかについて、評価する方法等について基準を設定する。

ウ　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。

解説

情報通信ネットワーク維持及び運用に関して、現状の調査・分析作業の実施手順を明確にする。手順化のポイントは次のとおりである。

１　調査、分析の効率化
２　調査、分析の適正化
３　一定手順による調査、分析の積み重ねによる経年変化の掌握
４　組織内に周知し、調査、分析作業への協力を得る。

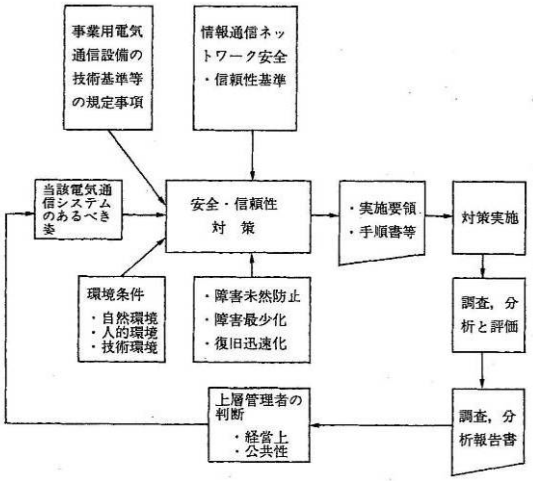
エ　情報通信ネットワークの維持及び運用に関して、現状の調査・分析結果を、必要に応じ、情報通信ネットワークの維持及び運用体制並びに手順書に反映させること。

解説

調査・分析結果に基づき、PDCAサイクルを活用しつつ情報通信ネットワークの維持及び運用体制や作業手順の適正化を行う。また、ヒヤリハット事例の収集・情報共有は、事故予防に資することから、実施すべきである。

●措置例●

調査・分析結果は、調査・分析報告書として上層管理者に提出し、上層管理者は、経営上の問題、公共性等の配慮を加え、設備、維持運用作業等に反映し、改善を図る。その概念を次図に示す。



調査・分析に基づく改善の流れ

オ　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。

解説

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、情報通信ネットワークの維持及び運用に携わる従事者の能力向上を目指し、教育及び訓練計画へ反映する。

１　新入社員訓練
２　配転者訓練
３　新業務、新設備訓練
４　業務専門訓練
５　技術専門訓練
６　運用保全訓練

(13)　ヒューマンエラー防止策

ア　情報通信ネットワークの設計、工事、維持及び運用に従事する者によるヒューマンエラーを防止するための対策を行うこと。

解説

令和４年度において、電気通信設備の運用等に係る作業に伴う人為的ミスにより重大な事故が多発したことから、令和５年度に電気通信事業規則の改正を行い、管理規程に記載すべき内容としてヒューマンエラー防止策を規定した。情報通信ネットワークの設計、工事、維持及び運用に従事する者による人為的ミスを防止するための対策を行うことが必要である。

●措置例●

具体的には、本項イ以降でも記載のとおり、以下が考えられる。

１　情報通信ネットワークの設計、工事、維持及び運用に係る作業に関するシステムの導入・自動化
２　情報通信ネットワークの設計、工事、維持及び運用に係る各作業を複数の担当者による確認・実施
３　責任者を含め多段階での作業手順の承認手続
４　ヒューマンエラー事例の関係者での共有
５　ヒヤリハット事例の収集・分析・共有

（令和５年度施行規則改正により追加）

イ　情報通信ネットワークの設計、工事、維持及び運用に係る作業についてシステムの導入や自動化を図ること。

解説

情報通信ネットワークの設計、工事、維持及び運用に係る作業について、作業の管理等に係るシステム（作業手順書の管理システムを含む。）の導入や自動化が可能な作業については自動化を行うこと等により、人為的ミスが発生する可能性を最小化することが望ましい。

（令和５年度施行規則改正により追加）

ウ　情報通信ネットワークの設計、工事、維持及び運用に係る各作業を複数の担当者で確認し実施すること。

解説

人為的ミスの軽減を図るため、情報通信ネットワークの設計、工事、維持及び運用に係る各作業を複数の担当者で確認し実施することが望ましい。

（令和５年度施行規則改正により追加）

エ　責任者を含め多段階で作業手順の承認手続を行うこと。

解説

人為的ミスの軽減を図るため、責任者を含め多段階で作業手順の承認手続を行うことが望ましい。

（令和５年度施行規則改正により追加）

オ　ヒューマンエラー事例を関係者で共有すること。

解説

関係者の意識を向上させ、同様の人為的ミスの軽減を図るため、実際に発生したヒューマンエラーの事例について、関係者で共有することが望ましい。

（令和５年度施行規則改正により追加）

カ　ヒヤリハット事例の収集・分析・共有を図ること。

解説

関係者の意識を向上させ、人為的ミスの軽減を図るため、重大な事故等には至らなかったものの、重大な事故に直結しかねない実際の事例（ヒヤリハット事例）を収集し、原因等の分析を行い、関係者で共有することが望ましい。

（令和５年度施行規則改正により追加）

(14)　リスク管理

ア　利用者の利益に及ぼす影響が大きい設備の損壊又は故障等の発生リスク（予備設備への切替不能及びサイレント故障のリスクを含む。）を適時に調査及び分析すること。

解説

令和４年度において、予備設備への切替不能やサイレント故障等を起因とする重大な事故が多発したことから、令和５年度に電気通信事業規則の改正を行い、管理規程に記載すべき内容として、利用者の利益に及ぼす影響が大きい電気通信設備の損壊又は故障等の発生リスクの分析等を規定した。

重大な事故の未然防止や事故発生時の影響の最小化等を図るためには、リスクの洗い出しを適切に行うことが重要であるため、利用者の利益に及ぼす影響が大きい

設備について、損壊又は故障等の発生リスクを適時に調査及び分析する。特に、予備設備への切替不能及びサイレント故障を原因とした重大な事故が多いことを踏まえ、予備設備への切替不能及びサイレント故障のリスクについても、適時に調査及び分析する。

（令和５年度施行規則改正により追加）

イ　調査・分析された発生リスクに対する対応措置及び応急復旧措置を整備すること。

解説

重大な事故の未然防止や事故発生時の影響の最小化等を図るためには、調査及び分析された発生リスクに対して、事前に対応措置及び応急復旧措置を整備しておくことも重要である。そのため、前項で調査及び分析された発生リスクに対して、事前に対応措置及び応急復旧措置を検討し、整備する。

（令和５年度施行規則改正により追加）

ウ　整備された対応措置及び応急復旧措置を実施した場合の電気通信役務に与える影響評価（想定復旧時間を含む。）を実施すること。

解説

重大な事故の未然防止や事故発生時の影響の最小化等を図るためには、調査及び分析された発生リスクに対して、想定復旧時間を含めて電気通信役務に与える影響評価を行うとともに、当該評価結果を踏まえ、必要に応じて、人材、設備、資金、組織等の配分の見直しを行うことが重要である。そのため、調査及び分析された発生リスクごとに、想定復旧時間を含め、整備された対応措置等を実施した場合の電気通信役務に与える影響評価を実施する。

（令和５年度施行規則改正により追加）

エ　リスクの調査及び分析等を踏まえ、事業継続計画又はこれに相当する計画を策定すること。

解説

重大な事故の多発を踏まえ、令和５年度に電気通信事業規則の改正を行い、管理規程に記載すべき内容として事業継続計画の策定を規定した。

事業者が、事故や自然災害などの緊急事態に遭遇した場合、損害を最小限にとどめつつ、事業の継続又は早期復旧を可能とするために、平常時に行うべき活動や緊急時における事業継続のための方法、手段等を予め計画に定めておくことが重要である。リスクの調査及び分析並びに整備された対応措置等を踏まえ、事業継続計画（BCP：Business Continuity Plan）等を策定する。

（令和５年度施行規則改正により追加）

オ　利用者の利益に及ぼす影響が大きい設備以外の設備の損壊又は故障等の発生リスクを適時に調査及び分析すること。

解説

重大な事故の未然防止や事故発生時の影響の最小化等を図るためには、設備の損壊又は故障等の発生リスクの洗い出しを適切に行うことが重要である。利用者の利益に及ぼす影響が大きい設備の損壊又は故障等の発生リスクの洗い出しについては、「第３．方法　１．平常時の取組（14）リスク管理　ア」で規定しているが、利用者の利益に及ぼす影響が大きい設備以外の設備についても、損壊又は故障等の発生リス

クを適時に調査及び分析することが望ましい。

（令和５年度施行規則改正により追加）

(15)　情報提供

ア　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。

解説

情報通信ネットワークの安全・信頼性の確保に係る取組みについて、セキュリティポリシーや体制、その実施状況などを、ホームページや配布物等によって利用者が容易に知りえる方法によって公表するように努めること。

また、サービス品質等の公表を行う場合は、測定の方法や範囲などが事業者によって異なる場合もあるため、これらのデータの前提となる根拠を明確にするよう努めること。

●公開内容の例●

１　各事業者における情報セキュリティ確保に関する基本方針

２　緊急通報機能など特殊な条件でのサービス利用方法

３　サービスの停止等、トラブル発生時の障害内容・復旧状況

イ　電気通信設備の安全・信頼性の確保の取組に関する次の情報を適切な方法により利用者に対して公開すること。

①　停電対策に関する情報

②　ネットワークの通信容量の設計に関する基本的考え方、通信規制、重要通信の優先的取扱いに係る手法等に関する情報

③　災害時における被災エリアの通信の確保に関する情報

解説

①　蓄電池増強や発電機設置等により、停電後、24時間以上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、ホームページ等を用いて、当該携帯電話基地局がカバーするエリアがわかるようなマップまたは情報（施設名称等）を公開すること。

②　ネットワーク設備については、平常時の通信が途絶えないように、トラヒックの将来予測から適切な通信容量で設計をしており、その設計の基本的考え方は安全・信頼性確保の点からも利用者にとって有益な情報であるため、公表すること。

その際、以下のような項目について留意して周知すること。

●措置例●

１　平常時と災害時の通信量の違いから、災害時のネットワークのおかれる状況についての説明

２　災害時に通信制限を行う必要性について、重要通信の疎通確保を含めて説明

３　防災機関などに対する災害時優先電話制度について説明

４　その他、通信をより疎通させるための対策について説明

③　災害時の通信ネットワークの早期復旧のための装備品、資材（移動電源車、移動無線基地局車等）の配備状況について、ホームページ等を用いて公開すること。

●公開内容例●

項目	内容	配備数の表示方法

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

ウ　情報通信ネットワークにおいて、サービスを提供できなくなる場合等について利用者に周知すること。

解説

情報通信ネットワークの事故・障害によっては、従来のサービスでは問題とならなかったが、新サービスでは考慮が必要となる点をあらかじめ利用者に周知しておくことが必要である。

●措置例●

従来の電話サービスでは停電時にも利用可能であったが、ＩＰ電話端末は設置場所が停電すると利用できなくなる等の事象が起こることを理解してもらうための取組を行うこと。

エ　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。

解説

情報通信ネットワークの運用に当たり、その有効活用を確保するため、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。さらにユーザへの周知の基準・内容について通信事業者間で協調して取り組むことが望ましい。

●措置例●

地震、豪雨、台風等の災害時における家族の安否確認等の増加によってふくそうが発生し、通信の疎通が確保できなくなることがある。このため、ふくそうを回避する方策として、以下のような方法により、不急の電話の自粛、災害用伝言ダイヤル等の利用等について利用者への協力依頼を行う。

１　パンフレット等による広報活動
２　防災訓練等における広報活動
３　広報車などによる広報活動
４　報道機関に対する広報依頼
５　災害用伝言ダイヤル、災害用伝言板サービス等の利用促進広報活動

オ　災害時においては、不要不急の電話を控えること及び通話時間をできるだけ短くすることについて周知・要請し、災害用伝言サービスを含めた音声通話以外の通信手段の利用等を平常時から呼びかけること。

解説

日頃から、災害発生時は発呼要求が集中しネットワークが輻輳して電話が繋が

りにくくなることをホームページやパンフレットで解説し、これらの媒体の他、各地で開催される防災訓練や報道などを通じて、利用者に、災害時は不要不急の電話を控えること並びに通話時間をできるだけ短くすること、災害時伝言サービスなど音声通話以外の通信手段の利用等を周知・要請する。また、各地の学校、市民団体等向けに開催する携帯電話端末やインターネットなど通信の利用方法やエチケットに関する講習会などの場を通じて、災害時の通信状況や適切な対応方法を利用者に浸透させていくことも有効である。

災害発生時は、速やかに、テレビ・ラジオ等の報道機関へ、視聴者に対して「電話が繋がりにくくになっており、不要不急の電話を控えること、通話時間を可能な限り短くすること」、「安否確認には、災害時音声伝言サービスを利用すること」を伝えるように要請する。

なお、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、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。

カ　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。また、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。

解説

緊急通報が常に利用できるようにするため、できるだけシステム稼動状態でメンテナンスを可能とするよう適切な措置を講ずる。また、メンテナンス時にサービスを停止する場合は、多様な手段を活用して、ユーザに通知をする。

キ　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。

解説

迷惑メールの防止策として、利用者が指定した特定の送信元アドレスに関する受信を拒否するなどの機能を設けることが望ましい。

●措置例●

1　予め指定した送信元アドレスからの電子メール受信を拒否する機能又は予め指定した送信元アドレスからの電子メールのみを受信する機能を設定する。

2　シークレットコード（電子メールを着信させるために送信側で必要な暗証番号）を設定可能とし、暗証番号を知らない相手からの電子メールを拒否する。

3　電子メールを利用しない利用者に対し、電子メール一括拒否機能を設定可能とし、一切の電子メールを受信しない。

4　利用者に容易に推測できない任意又はランダムの文字列のメールアドレスへ変更するよう促す。

ク　携帯電話インターネット接続役務提供事業者は、青少年有害情報フィルタリングサービスを提供できる体制を整えること。また、インターネット接続役務提供事業者は、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できる体制を整えること。

解説

「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」が施行されており、携帯電話インターネット接続役務提供事業者に対して、「青少年有害情報フィルタリングサービス」や「青少年有害情報フィルタリングソフトウェア」の提供すること等が記載されていることから、当該機能を提供できるよう体制を備えることが必要である。

ケ　インターネット上の児童ポルノ画像等の流通・閲覧防止対策を講じている事業者においては、その旨を周知すること。

解説

犯罪対策閣僚会議において、児童ポルノ排除総合対策が決定（平成 22 年 7 月 27 日）されており、インターネット上の児童ポルノ画像等の流通・閲覧防止対策の一つとして、児童ポルノ掲載アドレスリストを作成して閲覧防止措置（ブロッキング）する旨が挙げられている。

犯罪行為である児童ポルノ提供等を防止する措置を講じていることは、利用者が電気通信事業者を選択する際の有用な情報となることから、当該対策を講じている電気通信事業者はその旨を周知することが望ましい。

(16)　大規模災害対策

大規模な災害を考慮し、被災した施設の復旧に当たっての優先度を含め、復旧活動の調整方法について検討するとともに、応急復旧措置を行うために必要な機材について、大規模な災害時における被災エリアへの展開に関する計画を策定すること。

解説

今後、発生が想定される南海トラフ地震や首都直下地震等の大規模災害に対する備えとして、通信事業者においては、大規模災害時に被災が想定される市町村役場や災害拠点病院等の重要な拠点における通信の復旧に関する優先度を含め、応急復旧措置における関係機関との調整方法についてあらかじめ検討しておくことが重要である。また、移動電源車、可搬型基地局、衛星エントランス回線等、応急復旧措置を行うために必要な機材の迅速・有効な展開について、事前に計画を策定することが重要である。

（参考）「大規模地震防災・減災対策大綱」（平成 26 年 3 月、中央防災会議）（P.33）

「国、地方公共団体、関係事業者は、被災した施設の復旧に当たっての優先度を含め、復旧活動の調整方法についてあらかじめ検討しておく。」

（令和６年度告示改正により追加）

２．事故発生時の取組

(1)　報告、記録、措置及び周知
ア　迅速な原因分析のための関連事業者等（接続先、委託先、製造業者等をいう。）との連携を図るよう取り組むこと。
イ　速やかに故障を検知し、事故装置を特定すること（サイレント故障への対処を含む。）。

解説

事故対応については、事故発生がそもそも検知できないサイレント故障や、事故装置の特定に要する時間の増加及び事故対応に必要な関係者数の増加等による長時間化を踏まえ、事故の短期収束・拡大防止に努めることが必要である。

ア　電気通信事業者の設備は、マルチベンダ化やソフトウェアへの比重が大きくなっていることから、関係者間の連携を事前に図っておくことが必要である。
また、事故又は障害発生時に有益な情報共有が行われるよう、直接接続関係にあり、契約を締結している事業者（海外の事業者を含む。）との障害対応時の連絡先を把握しておくことが重要である。

イ　故障検知については、速やかな事故対応のためには必要であるが、ハードウェア故障やソフトウェア故障などにより、故障検知機能そのものが機能しない場合も考えられる。このため、故障検知機能だけではない対策を講じることが必要である。

●措置例１●
１　外部装置からの定期的な試験呼による「外部監視」
２　周辺装置でのトラヒックの傾向監視等によるサイレント故障が発生している装置の特定
３　利用者対応部門での、複数の類似問い合わせに対する速やかな監視部門へのエスカレーション

●措置例２●
ログ情報監視の対象を、通信異常を明らかに引き起こすもののみでなく、その可能性があるものまで拡大するとともに、当該拡大により大容量となったログ情報から直接システムに影響を与えないものを除外するスクリプトを導入し、被疑箇所の切り分け時間の短縮化を図る。

（平成 27 年度告示改正により追加）
（平成 31 年度にアのまた書きを追加）

ウ　障害の最小化対策を講ずること。
エ　事故装置に応じた定型的・類型的な応急復旧措置（一次措置）をあらかじめ準備し、速やかに実施すること。
オ　一次措置が機能しない場合にとるべき措置（二次措置（関連部門や機器等の製造・販売を行う者による措置等））を速やかに実施すること。

解説

ウ　ネットワークや設備構成が複雑化することにより、事故が発生すると影響範囲が大規模化することが考えられる。そのため、障害発生時にその影響ができるだけ最小限となるよう対応することが必要である。

●措置例●
１　利用者への影響を考慮の上、提供中のサービスの一時断
２　通常時の監視結果分析による予兆の発見、対応

３　障害発生による影響を最小化できるネットワーク構成の構築

エ　事故対象装置の特定後は、サービスの復旧が事故原因の特定よりも優先される。そのため、事故対象に応じた応急復旧措置を定型化・類型化し、措置に要する時間をできる限り短縮することが必要である。

●措置例●

１　各装置毎に、警報に応じた措置内容を記載した復旧対応マニュアルを作成し、遠隔からの予備系への切替及びハードウェア故障時には現地での交換作業等を実施

２　一時措置に係る故障復旧の目標時間を定め、その時間を満足するための手順書を作成

オ　事故原因や内容が複雑化することにより、定型的な応急復旧措置では復旧しない場合もあるため、事故の長時間化を回避するためにも保守・運用部門、開発部門又はベンダ等に速やかに情報をエスカレーションし、二次措置を実施することが必要である。

●措置例●

１　エスカレーションの基準や体制を整備し、関係者間で情報共有

２　複数ベンダが関係する場合は、責任範囲を契約において明確化

（平成 27 年度告示改正により追加）

カ　接続電気通信事業者との連携を図るよう取り組むこと。

解説

相互接続及び卸役務を実施している場合、自らの設備で事故が発生することにより、接続先の事業者にも影響を与えてしまう。このため、事故に関する情報の共有及び速やかな復旧のため、接続先の電気通信事業者と情報共有の在り方や復旧体制等について事前の連携を図ることが必要である。

（平成 27 年度告示改正により追加）

キ　サービス復旧のための手順及びとるべき措置を講ずること。

解説

別表第２ 第３ ２．(1)エ、オ参照。

ソフトウェア化・仮想化の進展により電気通信事業者の通信ネットワークが複雑化することや、電気通信事業者の通信ネットワークにおいて、物理的な設備の設置場所にかかわらず、インターネット等の外部回線経由で、必要に応じてネットワーク資源を提供可能なクラウドの利用が進展することに伴い、障害発生時において、故障箇所の特定やサービス維持、復旧作業等が従来以上に困難となることが想定される。こうした状況において、サービスの早期復旧に向けた対応を適切に行うことが必要である。

●措置例●

１．警報に応じた対応手順を予め定め、その手順に基づき対処すること

２．仮想化基盤の定常的な監視によりソフトウェアで構成されるノードにおいて処理時のログを適切に取得・保存すること

３．トラヒックの状況や周辺装置のリソース利用状況から故障箇所を特定できるよう努めること

４.故障箇所の特定に時間を要する場合に備え､正常稼働していた旧世代ソフトウェアを保管し復元可能にすること

５．ハードウェア故障を検知することで物理的に切り離しを行うことも考慮するこ

と

（平成 27 年度告示改正により追加）
（令和２年度告示改正により「ソフトウェア化」以降追加）

ク　ふくそう発生時には必要最小限の通信規制を実施すること。
ケ　重要通信を扱う場合は、ふくそう発生時等に当該重要通信を優先的に取り扱うこと。

解説

ふくそうの発生により、緊急通報や重要通信の確保に支障が生じることのないよう、最小限の通信規制の実施と、重要通信の優先的取り扱いについて予め対応を講じておく必要がある。

（平成 27 年度告示改正により追加）

コ　事故又は障害発生時に迅速な原因分析、状況把握及び復旧対応等のため、電気通信事業者間での情報共有を含め、複数のルートを活用し幅広く情報収集に努めること。

解説

インターネットにおける障害においては、まず、発生した事象が自社単独で起きている事象なのか、他の電気通信事業者でも同様に起きている事象なのか、あるいは、他の電気通信事業者がどのように復旧対応したかを把握することが、自らの対応策を検討する上で大変重要である。

そのため、自社内の状況確認に加え、必要に応じて契約関係等がある電気通信事業者との状況確認や、ネットワーク技術者間の情報交換など複数のルートを活用し幅広く情報収集に努めることが必要である。

特に、誤った経路制御情報やサイバー攻撃による障害等、ネットワークを跨がって発生する障害については、障害の発生状況や影響範囲、収束状況などの把握が困難な場合があることから、報道や SNS、総務省への確認等を通じて幅広く情報収集を行うことが有効である。

（平成 31 年度告示改正により新規追加）

(2)　情報提供
ア　事故・ふくそうが発生した場合又は利用者の混乱が懸念される障害が発生した場合には、その状況を速やかに利用者に対して公開すること。

解説

不測の要因による事故及び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、ネットワークの負荷軽減に有効と考えられることから、当該情報を公開する。

なお、第一報の提供は、事故・ふくそう等の発生を認知してから３０分～１時間以内を目途に公開するよう努める。

また､インターネットにつながりにくい障害であって､接続先や他の事業者のネットワークに起因するものの場合、自社に原因がないもの又は自社に原因があるか不明なものについては、迅速な原因分析や状況把握が困難である可能性がある。そのため利用者への情報提供に時間を要する可能性があるが、情報提供の遅れが利用者の混乱を拡大させる恐れがある。法人ユーザーの顧客が多数存在する場合は混乱が相当規模に発展する恐れもある。

そのため、利用者の混乱を防止する観点から、発生事実のみであっても利用者に

公開することが重要である。また、あらかじめその周知内容を決めておくことが重要とである。

なお､対象が特定の法人ユーザー等限定的な場合は､無用な混乱を防ぐ観点から、個別に情報提供する方が適当と考えられる。

●措置例●

障害を検知した後､予め用意してある定型文をシステムにより第一報として自動掲載する。その際の内容は､障害の影響を受ける主要サービスや概ねの発生時刻等の重要情報を優先し､発生原因､復旧見込み等の情報の早期把握が困難な場合は、第二報以降に掲載する。

（平成 31 年度告示改正によりまた書き以降（措置例を除く）を追加）

イ　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速やかに利用者に対して公開すること。

解説

情報通信ネットワークの事故・障害の発生時には、サービス状況（停止、接続し難い等）やサービスの影響範囲（地域、サービス範囲等）を、速やかにホームページ等を用いて利用者が容易に知りえる方法によって公表するように努めること。また､障害の状況によってはホームページによる掲載では利用者が情報を把握することが困難な場合や､ホームページ掲載システム自体が使用できないことがあるため、メールや報道機関等の各種メディアを活用する等多様な媒体によって利用者に通知することを検討すること。

さらに、障害発生により、他社ユーザにも影響を与えている場合は、他社ユーザに対しても自社ユーザと同等レベルの情報提供ができるよう、T-CEPTOAR 等を活用して障害内容を利用者へ提供する。

●他の公表内容の例●

１　故障・事故等の情報を印刷して店頭に提示

２　利用者に影響のある工事を行う場合､影響エリアの地図を事前にホームページに掲載

３　ソーシャルメディアを用いた情報提供

ウ　事故情報の利用者への提供窓口、方法、場所等に関する情報はあらかじめ利用者に周知すること。

解説

利用者が情報通信ネットワークの事故・障害に関する情報をどのような状況（場所、時間等）でも取得することができるよう、情報提供の窓口、方法、場所等に関する情報はサービス提供前から周知することが必要である。

●措置例●

障害発生時の偽情報の拡散防止策の一環として、事前に公式の Web サイトやアカウントの周知の徹底等を行い､公式情報と偽情報の差別化を行うことにより、利用者が正しい情報に容易にアクセスできる環境を整える。

（平成 27 年度告示改正により追加）

エ　情報の提供方法については利用者が理解しやすいように工夫すること。

解説

事故発生時に利用者へ提供する情報は、利用者のＩＣＴ分野に対する認知の度合いが様々であるため、できるだけ専門的な用語は用いず平易な表現を用いることが

必要である。また、その内容も利用者のニーズが高いと思われる内容（影響サービス、復旧見込みの日時、障害原因等）を提供することが必要である。

●措置例１●

１　第一報は事故発生の事実とともに、「影響サービス」、「障害復旧の見込み」等の利用者ニーズが高いものを伝える。

２　続報は、第一報で伝えられなかった内容の他に、最新情報を提供する観点から、情報提供の日時を明確に示す。

３　第一報及び続報では、可能な限り最新の「復旧見込みの日時」についても伝えるようにする。

４　復旧報については、利用者ニーズを考慮し「復旧時刻」、「障害原因」及び「影響地域及びサービス」について伝える。

５　情報は、第一報から復旧報までの履歴を保持し、復旧後も当面の間は掲載し続ける。

●措置例２●

設備を復旧させる各過程において、利用者体感としてどのような影響が生じているのかを正確に周知することを目的に、事故を生じさせた事業者に所属する職員を一般のユーザと見なして、当該職員から利用体感についてアンケートを実施し、その結果から全体の利用者体感を模擬的に把握する。把握した情報は、利用者体感の一例として、ホームページ等に掲載する。

●措置例３●

長時間障害は収まっているが原因が特定できていないような場合、その時点の事実を正確に周知することが望まれるが、そのような状況下でも「復旧」として周知する場合は、そう判断した理由を具体的にホームページ等に記載する。

（平成 27 年度告示改正により追加）

オ　情報提供の手段を多様化すること。

解説

別表第２ 第３ ２．(2) イ参照

（平成 27 年度告示改正により追加）

カ　利用者と直接対応する販売代理店等に事故の詳細を周知すること。

キ　仮想移動電気通信サービスを提供する電気通信事業者に対してサービスを提供している場合は、迅速に障害情報を通知すること。

解説

カ　サービスが利用不可又は利用困難となった場合、利用者は電気通信事業者ではなく、最寄りの販売代理店に問い合わせ・相談を行うことが考えられる。そのため、電気通信事業者は、自社内だけでなく販売代理店に対しても、現在発生している事故の概要等について幅広く情報共有することが必要である。

●措置例●

障害情報を Q&A 形式で販売代理店に展開させることで、電気通信事業者と販売代理店の障害時対応の統一を図る。

キ　仮想移動電気通信サービス（MVNO）では、回線提供元である MNO から情報が提供されないと、自社が提供するサービスで事故が発生した場合に、利用者への説明が不十分になることが考えられる。このため、MNO になる電気通信事業者は、自らの設備で障害等が発生した場合には、MVNO に対して速やかに情報提供するこ

とが必要である。

なお、MVNO における事故が発生した場合に、利用者が MVNO と MNO のどちらから情報を得ればよいか分からないといったことが生じないように、MVNO はサービスの開始前に、事故に関する情報提供の実施主体や方法について、MNO と調整を行い明確にすることが重要である。

（平成 27 年度告示改正により追加）

ク　利用者への周知・広報に関する国のガイドライン等を踏まえた取組を行うこと。

解説

電気通信事故の発生時に、電気通信事業者による利用者への周知・広報に多くの課題が見られたことから、「電気通信事故検証会議 周知広報・連絡体制ワーキンググループ」において周知・広報の在り方について検討がなされ、令和５年１月にとりまとめ報告書が策定された。これを踏まえ、総務省において、令和５年３月に「電気通信サービスにおける障害発生時の周知・広報に関するガイドライン」を策定したこと等を踏まえ、本対策を規定した。

利用者への修理・広報に求められる取組の内容については、「電気通信サービスにおける障害発生時の周知・広報に関するガイドライン」に規定されていることから、当該ガイドライン等を踏まえ、周知・広報の取組を確実に行うことが必要である。

●措置例●

１　事故等の発生後、原則 30 分以内に HP で初報を公表。総務省にも原則 30 分以内に連絡、緊急通報受理機関等には、初報の公表後速やかに連絡。

２　事故の発生日時、影響を受ける地域・サービス、原因、復旧見通し等に加え、「代替的に利用可能な通信手段とその利用方法」等についても周知。

３　災害時等においては、障害発生後、遅くとも数日以内に復旧見通しを示す。

４　通信障害情報等は、トップページのわかりやすい位置で常時掲載。障害時は少なくとも１時間ごとを目安に情報更新。

５　ホームページ、SNS、デジタルサイネージ、報道機関との連携等、多様な媒体で情報提供を行う。

６　周知・広報で使用する用語については、用語集を踏まえて記載。利用者の体感に基づく平易な言葉を使い、利用者目線の丁寧な説明及び情報発信を徹底する。

（令和５年度告示改正により追加）

３．事故収束後

再発防止策
ア　事故の規模にかかわらず、事故発生時の記録等に基づく原因の分析・検証を行い、再発防止策を策定すること。
イ　事故の分析・検証を開始してから再発防止策を講じるまでのスケジュールを構築すること。

解説

電気通信事故の収束後には、事故内容や原因を分析･検証することで適切な再発防止策を策定することができる。再発防止策の策定に当たっては、事故の規模によらず分析・検証を行い、一定期間で防止策を講じることができるよう、スケジュールを講じることが必要である。

（平成 27 年度告示改正により追加）

ウ　事故の分析・検証の結果、必要に応じて設備容量や委託先等との契約内容の見直しを行うこと。
エ　事故の内容・原因等が明らかになったとき、利用者に対してその情報を周知すること。

解説

上記分析･検証の結果、現行の設備に原因があることが判明した場合には、設備容量の見直しや、機器やソフトウェアの開発等を委託している委託先との契約内容の見直し（瑕疵担保期間の再設定、納入に係る判定基準の変更等）を行うことが求められる。

また、事故の原因が明らかになった際には、利用者に対して事故内容及びその原因について情報提供することが必要である。（別表第２ 第３ ２．(2) エ参照）

（平成 27 年度告示改正により追加）

オ　事故の内容・原因・再発防止策に関して、機密情報の取り扱いに留意して第三者による検証を受けること。

解説

電気通信事故を発生させた電気通信事業者自らが、事故の内容・原因を自ら分析・検証し、適切な再発防止策を策定することは重要であるが、当事者の自己チェックだけでは、今後の取組として不十分な部分もあると考えられるため、第三者たる国が、電気通信事業の監督者としての観点から、事故報告内容の適切性を分析・検証することも必要である。

このため、総務省において設ける第三者検証の仕組みを通じ、事故報告内容について検証を受けることが重要である。

１　対象となる重大事故を発生させた電気通信事業者の出席を求めた上で、当該電気通信事業者より報告に沿って事故の概要の説明を行い、総務省より過去の事故との類似性等について補足説明を行った後、構成員から質問・コメント等をいただくという流れにより検証を行う。

２　構成員には、特に事故発生原因の事前予見性、事故発生後の対応や再発防止策の適切性、報告内容の十分性等についてチェックいただくとともに、必要に応じ、業界全体での再発防止につながる取組等の提案をいただく。

３　検証の対象には電気通信事業者の機密事項等が含まれることが想定されるため、会合は非公開とするとともに、開催要綱において構成員に対して守秘義務

を課す。

（平成 27 年度告示改正により追加）

第４．点検及び見直し

１．経営の責任者による点検等

(1)　管理規程の遵守状況の点検及び評価
　　経営の責任者により、一年に一回以上、管理規程の遵守状況に係る点検及び評価（設備の設計、工事、維持又は運用を委託する場合にあつては、当該委託先の当該管理規程の遵守状況に係る点検及び評価を含む。）を実施すること。

解説

重大な事故の多発を踏まえ、令和５年度に電気通信事業規則の改正を行い、電気通信事業者自身によるガバナンスの強化を図るため､管理規程に記載すべき内容に、管理規程の遵守状況の点検及び評価等を規定した。

重大な事故の未然防止や事故発生時の影響の最小化等を図るには、「第３．方法１．平常時の取組 (14)リスク管理」において記載した、発生リスクの調査・分析、発生リスクに対する対応措置等の整備、想定復旧時間を含む電気通信役務に与える影響評価の実施など、管理規程の遵守状況に係る点検及び評価を確実に行うことが重要である。

経営の責任者は、一年に一回以上、管理規程の遵守状況に係る点検及び評価を実施する。また、設備の設備の設計、工事、維持又は運用を委託する場合は、当該委託先と自らの管理規程に基づく電気通信設備の障害対策及び安全対策等に関する項目を盛り込んだ契約を締結するとともに、当該契約の遵守状況に係る点検及び評価を実施する。

（令和５年度施行規則改正により追加）

(2)　経営資源の点検、評価及び見直し
　　経営の責任者により、一年に一回以上、人材、設備、資金、組織その他の経営資源が十分であることについて点検及び評価並びに経営資源の配分の見直しを行うこと。

解説

重大な事故の未然防止や事故発生時の影響の最小化等を図るには、前項の管理規程の遵守状況に係る点検及び評価の確実な実施に加え、当該点検等の結果を踏まえて、人材、設備、資金、組織等の経営資源が十分であるか等を含め、経営の責任者等が定期的に点検・評価を行い、必要に応じて、経営資源の配分の見直しを行うことが重要である。

経営の責任者は、一年に一回以上、人材、設備、資金、組織その他の経営資源が十分であることについて点検及び評価を行うとともに、その結果を踏まえ、必要に応じて経営資源の配分の見直しを行う。

（令和５年度施行規則改正により追加）

(3)　管理規程の見直し
　　管理規程の遵守状況の点検及び評価、経営資源の点検及び評価の結果その他の事由に基づく当該管理規程の見直しに関すること

解説

管理規程の遵守状況の点検及び評価や経営資源の点検及び評価の結果を踏まえ、電気通信設備の管理の方針・体制・方法等の見直しを実施した場合は、当該内容を管理規程に反映する。また、事故の発生を踏まえて策定した再発防止策、他事業者

の事故の報告を踏まえて実施する対策等、今後、継続的に取り組む内容について管理規程に追記することは、サービス全体への電気通信事故防止の観点からも有効であることから、必要に応じて、再発防止策等を管理規程に適宜反映する。

（令和５年度施行規則改正により追加）