情報通信ネットワーク安全・信頼性基準
（昭和六十二年二月十四日郵政省告示第七十三号）

第１　目的

情報通信ネットワークのうち社会的に重要なもの又はそれに準ずるものを対象とし、その安全・信頼性対策の指標としての基準を定めることにより、安全・信頼性対策の普及を促進し、もつて情報通信ネットワークの健全な発展に寄与することを目的とする。

第２　定義

この基準において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

１　「情報通信ネットワーク」とは、有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けるためのネットワークをいう。

２　「電気通信事業用ネットワーク」とは、電気通信事業法（昭和 59 年法律第 86 号）第２条第４号に規定する電気通信事業の用に供する情報通信ネットワークをいう。

３　「電気通信回線設備事業用ネットワーク」とは、電気通信事業用ネットワークのうち電気通信事業法第 41 条第１項又は第２項に規定する電気通信設備を設置して電気通信役務を提供する電気通信事業の用に供する情報通信ネットワークをいう。

４　「その他の電気通信事業用ネットワーク」とは、電気通信回線設備事業用ネットワーク以外の電気通信事業用ネットワークをいう。

５　「自営情報通信ネットワーク」とは、電気通信事業用ネットワーク以外の情報通信ネットワークのうち電気通信回線設備（送信の場所と受信の場所との間を接続する伝送路設備及びこれと一体として設置される交換設備並びにこれらの附属設備をいう。以下同じ。）を設置する情報通信ネットワークをいう。

６　「ユーザネットワーク」とは、電気通信事業用ネットワーク及び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をいう。

７　「情報セキュリティポリシー」とは、情報資産の損失に対する抑止、予防、検知及び回復について、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及び方向性を定めたものをいう。

第３　安全・信頼性基準

１　設備等基準

情報通信ネットワークを構成する設備及び情報通信ネットワークを構成する設備を設置する環境の基準は、別表第１のとおりとする。

２　管理基準

情報通信ネットワークの設計、施工、維持及び運用の管理の基準は、別表第２のとおりとする。

第４　配慮すべき事項

１　別表第２に基づき、情報セキュリティポリシーを策定するに当たつては、別表第３の「情報セキュリティポリシー策定のための指針」に配慮すること。

２　別表第２に基づき、危機管理計画を策定するに当たつては、別表第４の「危機管理計画策定のための指針」に配慮すること。

第５　他の基準の活用

情報通信ネットワークの安全・信頼性対策を実施するに当たっては、「情報システム安全対策指針」（平成九年国家公安委員会告示第 9 号）の基準も活用することが重要である。

附　則（平成６年 11 月 29 日郵政省告示第 638 号）

１　この告示は、公布の日から施行する。

２　この告示の施行の際現に、昭和六十二年郵政省告示第七十四号（情報通信ネットワーク安全・信頼性対策実施登録規程）第八条の規定による登録を受けている情報通信ネットワークについては、その登録の有効期間までは、なお従前の例による。

附　則（平成８年３月 28 日郵政省告示第 152 号）

１　この告示は、公布の日から施行する。

２　この告示の施行の際現に昭和六十二年郵政省告示第七十四号（情報通信ネットワーク安全・信頼性対策実施登録規程）第八条の規定による登録を受けている情報通信ネットワークについては、その登録の有効期間までは、なお従前の例による。

附　則（平成９年７月 18 日郵政省告示第 364 号）

この告示の施行の際現に昭和六十二年郵政省告示第七十四号（情報通信ネットワーク安全・信頼性対策実施登録規程）第八条の規定による登録を受けている情報通信ネットワークについては、その登録の有効期間までは、なお従前の例による。

附　則（平成９年９月 18 日郵政省告示第 475 号）

この告示は、公布の日から施行する。

附　則（平成 12 年 8 月 29 日郵政省告示第 546 号）

この告示の施行の際現に昭和六十二年郵政省告示第七十四号（情報通信ネットワーク安全・信頼性対策実施登録規程）第八条の規定による登録を受けている情報通信ネットワークについては、その登録の有効期間までは、なお従前の例による。

附　則（平成 12 年 12 月 27 日郵政省告示第 848 号）

この告示の施行の際現に昭和六十二年郵政省告示第七十四号（情報通信ネットワーク安全・信頼性対策実施登録規程）第八条の規定による登録を受けている情報通信ネットワークについては、その登録の有効期間までは、なお従前の例による。

附　則（平成 13 年３月 29 日総務省告示第 188 号）

１　この告示は、公布の日から施行する。ただし、別表第２の表５の項の改正規定は、平成十三年七月一日から施行する。

２　この告示の施行の際現に昭和六十二年郵政省告示第七十四号（情報通信ネットワーク安全・信頼性対策実施登録規程）第八条の規定による登録を受けている情報通信ネットワークについては、その登録の有効期間までは、なお従前の例による。

附　則（平成 14 年３月７日総務省告示第 136 号）

この告示の施行の際現に昭和六十二年郵政省告示第七十四号（情報通信ネットワーク安全・信頼性対策実施登録規程）第八条の規定による登録を受けている情報通信ネットワークについては、その登録の有効期間までは、なお従前の例による。

附　則（平成 16 年３月 25 日総務省告示第 244 号）

１　この告示は、平成十六年四月一日から施行する。

２　この告示の施行の際現に昭和六十二年郵政省告示第七十四号（情報通信ネットワーク安全・信頼性対策実施登録規程）第八条の規定による登録を受けている情報通信ネットワークについては、その登録の有効期間までは、なお従前の例による。

附　則（平成 20 年 3 月 21 日総務省告示第 144 号）

（施行期日）

１　この告示は、平成二十年四月一日から施行する。

（経過措置）

２　この告示の施行の際現に昭和六十二年郵政省告示第七十四号（情報通信ネットワーク安全・信頼性対策実施登録規程）第八条の規定による登録を受けている情報通信ネットワークについては、その登録の有効期間までは、なお従前の例による。

別表第１　設備等基準

項　　目	対　　策	実施指針			
		電気通信回線設備事業用ネットワーク	その他の電気通信事業用ネットワーク	自営情報通信ネットワーク	ユーザネットワーク
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。	○	○	○	○
	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。	○	○	○	○
(2)　代替接続系統の設定	交換網の場合は、二つの重要な通信センター間を結ぶ接続系統の障害に対し、その代替となる他の通信センター経由のう回接続系統を設けること。	○	○	○	○
(3)　異経路伝送路設備の設置	ア　重要な通信センター間を結ぶ伝送路設備は、複数の経路により設置すること。	○	－	○	－
	イ　重要な光加入者伝送路は、ループ化等による２ルート化を促進すること。	○	－	○	－
(4)　電気通信回線の分散収容	重要な通信センター間を結ぶ電気通信回線の収容は、異なる伝送路設備に分散して行うこと。	○	－	○	－
(5)　モバイルインターネット接続サービスにおける設備の分散等	重要な設備の事故等が全国的な又は相当広範囲の利用者に影響する場合は、当該設備について、地域的に分散して設置するとともに分散した設備を複数の経路で接続し、故障等による影響範囲を限定すること。	○	－	－	－
(6)　モバイルインターネット接続サービスにおける設備容量の確保	サーバー及びゲートウェイの設備は、通信の集中を考慮した適切な容量のものを設置すること。	◎＊	－	－	－
(7)　電子メールによる一方的な広告・宣伝等への対策	モバイルインターネット接続サービスにおいては、利用者が指定した特定の条件に該当する電子メールの受信を拒否する等の機能を設けること。	○	－	－	－
(8)　予備の電気通信回線の設定等	ア　重要な伝送路設備には、予備の電気通信回線を設定すること。ただし、他に疎通確保の手段がある場合は、この限りでない。	◎	－	◎	－
	イ　重要な伝送設備には、予備の電気通信回線に速やかに切り換える機能を設けること。	◎	◎	◎	◎
(9)　情報通信ネットワークの動作状況の	ア　重要な伝送路設備の動作状況を監視し、故障等を速やかに検知、通報する機能を設けること。	◎	－	◎＊	－
	イ　重要な電気通信回線の動作状況を監視し、故障等を	－	◎	－	◎＊

監視等	速やかに検知、通報する機能を設けること。				
	ウ　重要な伝送路設備の動作状況を統合的に監視する機能を設けること。	○	－	○	－
	エ　重要な電気通信回線の動作状況を統合的に監視する機能を設けること。	－	○	－	○
	オ　交換設備には、トラヒックの疎通状況を監視し、異常ふくそう等を速やかに検知、通報する機能を設けること。ただし、通信が同時に集中することがないようこれを制御する措置を講ずる場合は、この限りでない。	◎	◎	○	○
	カ　交換設備には、通信の接続規制を行う機能又はこれと同等の機能を設けること。ただし、通信が同時に集中することがないようこれを制御する措置を講ずる場合は、この限りでない。	◎	◎	○	○
	キ　交換設備には、利用者に異常ふくそうを通知する機能を設けること。ただし、通信が同時に集中することがないようこれを制御する措置を講ずる場合は、この限りでない。	◎	○	○	○
	ク　トラヒックの疎通状況を統合的に監視する機能を設けること。	○	○	○	○
(10)　ソフトウェアの信頼性向上対策	ア　ソフトウェアを導入する場合は、品質の検証を行うこと。	◎	◎	◎＊	◎＊
	イ　ソフトウェア及びデータを変更するときは、容易に誤りが混入しないよう措置を講ずること。	◎	◎	◎＊	◎＊
	ウ　システムデータ等の重要データの復元ができること。	◎	◎	◎＊	◎＊
	エ　ソフトウェアには、異常の発生を速やかに検知、通報する機能を設けること。	○	○	○	○
	オ　ソフトウェアには、サイバー攻撃等に対する脆弱性がないように対策を継続的に講ずること。	◎	◎	◎＊	◎＊
	カ　モバイルインターネット接続サービスにおいて、新しいシステムの導入に当たっては、実際に運用する場合と同一の条件や環境を考慮し、ハードウェアの初期故障、ソフトウェアのバグによる障害が可能な限り発生しないよう十分なシミュレーションを実施すること。	◎	◎	－	－
	キ　ＩＰ系接続サービスにおいては、現用及び予備機器の切替えを行うソフトウェアは十分な信頼性を確保すること。	◎	◎	－	－
	ク　ソフトウェアの導入又は更新に当たってはウイルス等の混入を防ぎ、セキュリティを確保すること。	◎	◎	◎＊	◎＊
	ケ　定期的にソフトウェアを点検し、リスク分析を実施すること。	◎	◎	○	○
(11)　情報セキュリティ対策	ア　インターネットへ接続する場合は、ファイアウォールを設置して適切な設定を行うこと。	◎	◎	◎	◎
	イ　インターネットへ接続する場合は、非武装セグメント構成を採用すること。	◎	◎	◎	◎
	ウ　インターネットへ接続する場合は、ｔｅｌｎｅｔやｆｔｐ等サービス提供に不用な通信の接続制限を行うこと。	◎	◎	◎	◎
	エ　インターネットへ接続する場合は、開放網と閉域網とを区別したネットワーク構成を採用すること。	◎	◎	◎	◎
	オ　インターネットへ接続する場合は、サーバー等におけるセキュリティホール対策を講ずること。	◎	◎	◎	◎

	カ　インターネットへ接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されること。	◎	◎	◎	◎
	キ　インターネットへ接続する場合は、ネットワーク上のパケット並びにサーバー及びネットワーク機器の動作に関するログの適切な記録及び保存を行うこと。	◎	◎	◎	◎
	ク　インターネットへ接続する場合は、最新の情報セキュリティ技術を採用すること。	◎	◎	◎	◎
	ケ　コンピュータウイルス及び不正プログラム混入対策を講ずること。	◎	◎	◎	◎
	コ　ネットワークの機能を管理・運営するコンピュータから重要な情報が漏えいしないように、電磁波の低減対策、又は電磁環境に配慮した上で漏えい電磁波をマスクする措置を講ずること。	◎＊	◎＊	◎＊	◎＊
	サ　利用者の識別・確認を要する通信を取り扱う情報通信ネットワークには、正当な利用者の識別・確認を行う機能を設けること。	◎	◎	◎	◎
	シ　アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずること。	◎	◎	◎	◎
	ス　利用者のパスワードの文字列をチェックし、一般的な単語を排除する機能を設けること。	○	○	○	○
	セ　アクセス失敗回数の基準を設定するとともに、基準値を越えたものについては、履歴を残しておく機能を設けること。	○	○	○	○
	ソ　保護することが求められる重要な情報については、その情報に対するアクセス要求を記録し、保存する機能を設けること。	○	○	○	○
	タ　ネットワークへのアクセス履歴の表示あるいは照会が行える機能を設けること。	○	○	○	○
	チ　一定期間以上パスワードを変更していない利用者に対して注意喚起する機能を設けること。	○	○	○	○
	ツ　一定期間以上ネットワークを利用していない利用者がネットワークにアクセスする際に、再開の意思を確認する機能を設けること。	○	○	○	○
	テ　機密度の高い通信には、秘話化又は暗号化の措置を講ずること。	○	○	○	○
	ト　適切な漏話減衰量の基準を設定すること。	◎	◎	◎＊	◎＊
	ナ　ネットワークの不正使用を防止する措置を講ずること。	○	○	○	○
(12)　通信の途絶防止対策	通信の途絶を防止する措置を講ずること。	◎＊	－	◎＊	－
(13)　応急復旧対策	ア　重要な伝送路設備には、応急復旧用ケーブルの配備等の応急復旧対策を講ずること。	◎	－	◎＊	－
	イ　移動用交換設備の配備等の応急復旧対策を講ずること。	○	○	○	○
	ウ　災害時等において、衛星地球局等の無線設備により、臨時電話等の設置が可能であること。	○	－	○	－
	エ　移動体通信基地局と交換局の間の回線に障害が発生した場合等に、無線設備により、臨時に対向の電気通信回線の設定が可能であること。	○	－	○	－
	オ　移動体通信基地局に障害が発生した場合等に、可搬	○	－	○	－

	型無線基地局により、臨時の電気通信回線の設定が可能であること。				
	カ　他の伝送設備の障害時に、通信の疎通が著しく困難となった場合、予備の設備等により臨時の電気通信回線の設定が可能であること。	○	－	○	－
(14)　緊急通報の確保	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。なお、メンテナンス時にサービス停止が必要な場合はユーザに通知する措置を講ずること。	◎	◎	－	－
(15)　バックアップの分散化等	予備電源の設置又は冗長化などの予備機器等の配備基準の明確化を図ること。	◎	◎	○	○
2　屋外設備					
(1)　風害対策	ア　強度の風圧を受けるおそれのある場所に設置する屋外設備には、強風下において故障等の発生を防止する措置を講ずること。	◎	◎	◎	◎
	イ　風による振動に対し、故障等の発生を防止する措置を講ずること。	◎	◎	◎	◎
(2)　振動対策	地震等による振動に対し、故障等の発生を防止する措置を講ずること。	◎	◎	◎	◎
(3)　雷害対策	雷害が発生するおそれのある場所に設置する重要な屋外設備には、雷害による障害の発生を防止する措置を講ずること。	◎＊	◎＊	○	○
(4)　火災対策	火災が発生するおそれのある場所に設置する屋外設備には、不燃化又は難燃化の措置を講ずること。	○	○	○	○
(5)　耐水等の対策	ア　水中に設置する屋外設備には、耐水機能を設けること。	◎	－	◎	－
	イ　水中に設置する屋外設備には、水圧による故障等の発生を防止する措置を講ずること。	◎	－	◎	－
(6)　水害対策	水害のおそれのある場所には、重要な屋外設備を設置しないこと。ただし、やむを得ない場合であって、防水措置等を講ずる場合は、この限りでない。	◎	◎	◎	◎
(7)　凍結対策	凍結のおそれのある場所に設置する屋外設備には、凍結による故障等の発生を防止する措置を講ずること。	◎	◎	◎＊	◎＊
(8)　塩害等対策	塩害、腐食性ガスによる害又は粉塵による害のおそれのある場所に設置する屋外設備には、これらによる故障等の発生を防止する措置を講ずること。	◎	◎	◎＊	◎＊
(9)　高温・低温対策	ア　高温度又は低温度の場所に設置する屋外設備は、当該条件下で安定的に動作するものであること。	◎	◎	◎	◎
	イ　温度差の著しい場所又は温度変化の急激な環境に設置する屋外設備は、当該条件下で安定的に動作するものであること。	◎	◎	◎	◎
(10)　高湿度対策	高湿度となるおそれのある場所に設置する屋外設備には、耐湿度措置、防錆措置等を講ずること。	◎	◎	◎	◎
(11)　高信頼度	海底、宇宙空間等の特殊な場所に設置する重要な屋外設備については、高信頼度部品の使用等による高信頼度化を図ること。	◎	－	◎	－
(12)　第三者の接触防止	ア　設備に第三者が容易に触れることができないような措置を講ずること。	◎	◎	◎	◎
	イ　とう道等には、施錠等の侵入を防止する措置を講ずること。	◎	◎＊	◎＊	◎＊
(13)　故障等の検知、通報	ア　重要な屋外設備には、故障等を速やかに検知、通報する機能を設けること。	◎	◎	◎＊	◎＊

	イ　重要な屋外設備には、故障等の箇所を識別する機能を設けること。	○	○	○	○
(14)　予備機器等の配備	重要な屋外設備には、予備機器等の適切な配備又はこれに準ずる措置を講ずること。	◎	◎	◎	－
(15)　通信ケーブルの地中化	災害時等の建物の倒壊、火災等による通信ケーブルの被災を防ぐため、通信ケーブルの地中化等を促進すること。	○	－	○	－
(16)　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すべての電気通信設備について、設備を設置する事業者が発火・発煙防止等安全・信頼性確保のための所要の措置を講ずること。	◎	◎	◎	◎
3　屋内設備					
(1)　地震対策	ア　通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。	◎	◎	◎	◎
	イ　通常想定される規模の地震による屋内設備の構成部品の接触不良及び脱落を防止する措置を講ずること。	◎	◎	◎	◎
	ウ　重要な屋内設備に関する地震対策は、大規模な地震を考慮すること。	◎	◎	○	○
(2)　雷害対策	雷害が発生するおそれのある場所に設置する重要な屋内設備には、雷害による障害の発生を防止する措置を講ずること。	◎＊	◎＊	○	○
(3)　火災対策	重要な屋内設備には、不燃化又は難燃化の措置を講ずること。	○	○	○	○
(4)　高信頼度	ア　重要な屋内設備の機器等には、冗長構成又はこれに準ずる措置を講ずること。	◎	◎	◎	◎
	イ　重要な屋内設備の機器等は、速やかに予備機器等への切換えができるものであること。	◎	◎	◎	◎
(5)　故障等の検知、通報	ア　重要な屋内設備には、故障等の発生を速やかに検知、通報する機能を設けること。	◎	◎	◎	◎
	イ　無人施設の重要な屋内設備には、遠隔通報機能を設けること。ただし、これに準ずる措置を講ずる場合は、この限りでない。	◎	◎	◎	◎
	ウ　重要な屋内設備には、故障等の箇所を識別する機能を設けること。	○	○	○	○
(6)　試験機器の配備	試験機器の適切な配備又はこれに準ずる措置を講ずること。	◎	◎	◎	◎
(7)　予備機器等の配備	重要な屋内設備には、予備機器等の適切な配備又はこれに準ずる措置を講ずること。	◎	◎	◎	◎
(8)　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すべての電気通信設備には、安全・信頼性を確保する適切な措置を講ずること。	◎	◎	◎	◎
4　電源設備					
(1)　電力の供給条件	ア　情報通信ネットワークの所要電力を安定的に供給できること。	◎	◎	◎	◎
	イ　電圧を許容限度内に維持するための措置を講ずること。	◎	◎	◎	◎
	ウ　周波数を許容限度内に維持するための措置を講ずること。	◎	◎	◎	◎
(2)　地震対策	ア　通常想定される規模の地震による転倒、移動及び故障等の発生を防止する措置を講ずること。	◎	◎	◎	◎

	イ　重要な電源設備に関する地震対策は、大規模な地震を考慮すること。	◎	◎	○	○
(3)　雷害対策	雷害が発生するおそれがある場所に設置する重要な設備に電力を供給する電源設備には、雷害による障害の発生を防止する措置を講ずること。	◎＊	◎＊	○	○
(4)　火災対策	重要な設備に電力を供給する電源設備には、不燃化、難燃化又は保護装置の設置等の措置を講ずること。	◎＊	◎＊	○	○
(5)　高信頼度	重要な設備に電力を供給する電源設備の機器には、冗長構成又はこれに準ずる措置を講ずること。	◎	◎	◎	◎
(6)　故障等の検知、通報	ア　電源設備の故障等、ヒューズ断又は停電の発生を速やかに検知、通報する機能を設けること。	◎	◎	◎	◎
	イ　重要な設備を収容する無人施設の電源設備には、遠隔通報機能を設けること。ただし、これに準ずる措置を講ずる場合は、この限りでない。	◎	◎	◎	◎
(7)　停電対策	ア　次のいずれかの措置を講ずること。 ①　自家用発電機を設置すること。 ②　蓄電池を設置すること。 ③　複数の系統で受電すること。 ④　移動電源設備を配備すること。	◎	◎	◎＊	◎＊
	イ　交換設備については、蓄電池の設置及び、自家用発電機の設置又はこれに準ずる措置を講ずること。	◎	○	○	○
	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。	◎	◎	○	○
第２　環境基準 １　センターの建築物					
(1)　立地条件及び周囲環境への配慮	ア　強固な地盤上の建築物を選定すること。ただし、やむを得ない場合であって、不同沈下を防止する措置を講ずる場合は、この限りでない。	◎	◎	◎＊	◎＊
	イ　風水害等を受けにくい環境の建築物を選定すること。ただし、やむを得ない場合であって、防風、防水等の措置を講ずる場合は、この限りでない。	◎	◎	◎＊	◎＊
	ウ　強力な電磁界による障害のおそれのない環境の建築物を選定すること。ただし、やむを得ない場合であって、通信機械室等に電磁シールド等の措置を講ずる場合は、この限りでない。	◎	◎	◎	◎
	エ　爆発や火災のおそれのある危険物を収容する施設に隣接した建築物は回避すること。	○	○	○	○
(2)　建築物の選定	ア　耐震構造であること。	◎	◎	◎＊	◎＊
	イ　建築基準法（昭和 25 年法律第 201 号）第２条に規定する耐火建築物又は準耐火建築物であること。	◎	◎	◎＊	◎＊
	ウ　床荷重に対し、所要の構造耐力を確保すること。	◎	◎	◎	◎
(3)　入出制限機能	ア　建築物の出入口には、施錠機能を設けること。	◎	◎	◎	◎
	イ　通常利用する出入口には、設備の重要度に応じた適切な入出管理機能を設けること。ただし、これに準ずる措置を講ずる場合は、この限りでない。	◎	◎	◎	◎
	ウ　セキュリティを保つべき領域の具体的な基準を設定し、運用すること。	◎	◎	◎	◎

(4) 火災の検知、消火	ア 自動火災報知設備を適切に設置すること。	◎	◎	◎＊	◎＊
	イ 消火設備を適切に設置すること。	◎	◎	◎	◎
2 通信機械室等					
(1) 通信機械室の位置	ア 自然災害等の外部からの影響を受けるおそれの少ない場所に設置すること。	◎	◎	◎	◎
	イ 第三者が侵入するおそれの少ない場所に設置すること。ただし、第三者が容易に侵入できないような措置が講じられている場合は、この限りでない。	◎	◎	◎	◎
	ウ 浸水のおそれの少ない場所に設置すること。ただし、やむを得ない場合であって、床のかさ上げ、防水壁等の措置を講ずる場合又は排水設備を設置する場合は、この限りでない。	◎	◎	◎＊	◎＊
	エ 強力な電磁界による障害のおそれの少ない場所に設置すること。ただし、やむを得ない場合であって、電磁シールド等の措置を講ずる場合は、この限りでない。	◎	◎	◎	◎
(2) 通信機械室内の設備等の設置	ア 保守作業が安全かつ円滑に行える空間を確保すること。	◎	◎	◎	◎
	イ じゅう器等には、通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。	◎	◎	◎	◎
(3) 通信機械室の条件	ア 重要な設備を収容する通信機械室は、専用に設け、十分な強度を持つ扉を設けること。	◎	◎	◎＊	◎＊
	イ 床、内壁、天井等に使用する内装材には、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。	◎	◎＊	◎＊	◎＊
	ウ 床、内壁、天井等に使用する内装材には、建築基準法第２条に規定する不燃材料又は建築基準法施行令（昭和 25 年政令第 338 号）第１条に規定する準不燃材料若しくは難燃材料を使用すること。	◎	◎＊	◎＊	◎＊
	エ 静電気の発生又は帯電を防止する措置を講ずること。	◎＊	◎＊	◎＊	◎＊
	オ 通信機械室に電源設備等を設置する場合は、必要に応じ、電磁界による障害を防止する措置を講ずること。	◎	◎	◎	◎
	カ 通信機械室の貫通孔には、延焼を防止する措置を講ずること。	◎＊	◎＊	◎＊	◎＊
(4) 入出制限機能	ア 出入口には、施錠機能を設けること。	◎	◎	◎	◎
	イ 重要な設備を収容する通信機械室の出入口には、入出管理機能を設けること。また、設備の重要度に応じた適切な入出管理機能を設けること。	◎	◎	◎	◎
	ウ セキュリティを保つべき領域の具体的な基準を設定し、運用すること。	◎	◎	◎	◎
(5) データ類の保管	ア システムデータ等の重要なデータは、データ保管室又は専用のデータ保管庫に収容すること。	◎	◎	◎＊	◎＊
	イ データ保管室及びデータ保管庫には、施錠機能を設けること。	◎	◎	◎＊	◎＊
	ウ データ保管室及びデータ保管庫には、必要に応じ、電磁界による障害を防止する措置を講ずること。	◎	◎	◎	◎
	エ データ保管庫には、通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。	◎	◎	◎＊	◎＊
	オ データ保管室及びデータ保管庫には、必要に応じ、耐火措置を講ずること。	◎	◎	◎＊	◎＊
(6) 火災の検知、消火	ア 自動火災報知設備を適切に設置すること。	◎	◎	◎	◎
	イ 消火設備を適切に設置すること。	◎	◎	◎	◎
3 空気調和設備					

(1) 空気調和設備の設置	ア 通信機械室は、必要に応じ、空気調和を行うこと。	◎	◎	◎	◎
	イ 荷重を十分考慮して設置すること。	◎	◎	◎	◎
	ウ 通常想定される規模の地震による転倒又は移動を防止する措置を講ずること。	◎	◎	◎	◎
(2) 空気調和設備室への入出制限	出入口には、施錠機能を設けること。	◎＊	◎＊	◎＊	◎＊
(3) 空気調和の条件	ア 適切な設備容量とすること。	◎	◎	◎	◎
	イ 温湿度及び空気清浄度を適正な範囲内に維持する機能を設けること。	◎	◎	◎	◎
	ウ 急激な温度変化が生じないよう制御する機能を設けること。	○	○	○	○
	エ 重要な設備を収容する通信機械室の空気調和は、事務室等の空気調和と別系統とすること。ただし、通信機械室の空気調和が損なわれないような措置を講ずる場合は、この限りでない。	◎	◎	◎	◎
	オ 重要な設備を収容する通信機械室の空気調和を行う空気調和設備は、冗長構成とすること。	◎＊	◎＊	○	○
(4) 凍結防止	凍結のおそれのある場所に設置する空気調和設備には、凍結による故障等の発生を防止する措置を講ずること。	◎	◎	◎＊	◎＊
(5) 漏水防止	排水口等の漏水を防止する措置を講ずること。	◎	◎	◎＊	◎＊
(6) 有毒ガス等	腐食性ガス（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。	◎	◎	◎＊	◎＊
(7) 故障等の検知、通報	重要な設備を収容する通信機械室の空気調和を行う空気調和設備には、故障等を速やかに検知、通報する機能を設けること。	◎＊	◎＊	◎＊	◎＊
(8) 火災の検知、消火	ア 空気調和設備室には、自動火災報知設備を適切に設置すること。	◎	◎	◎	◎
	イ 空気調和設備室には、消火設備を適切に設置すること。	◎	◎	◎	◎

注１　「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。ただし、軽微な交換機能、通信処理機能又は情報処理機能を有するものを除く。

２　実施指針の欄中、「◎」、「◎＊」、「○」及び「－」は、それぞれ次のことを示す。

◎　：実施すべきである。

◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

○　：実施が望ましい。

－　：対象外

３　その他の電気通信事業用ネットワーク及びユーザネットワークのそれぞれの集線センター（主として情報通信ネットワークの利用者の端末と通信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をいう。）に係る次の対策についての実施指針は、「○」と読み替える。

(1)　第１の４の(1)のウ及び(7)

(2)　第２の１の(1)のア及びイ、(2)のア及びイ並びに(3)のイ

(3)　第２の２の(1)のア及びウ、(2)のイ並びに(3)のイ及びウ

別表第２　管理基準

項　　目	対　　策	実施指針			
		電気通信回線設備事業用ネットワーク	その他の電気通信事業用ネットワーク	自営情報通信ネットワーク	ユーザネットワーク
１　ネットワーク設計管理					
(1)　体制の明確化	意思決定、作業の分担、責任の範囲等の設計管理体制を明確にすること。	◎	◎	◎	◎
(2)　設計指針の明確化等	ア　情報通信ネットワークの基本的機能を明確にすること。	◎	◎	◎	◎
	イ　将来の規模の拡大、トラヒック増加及び機能の拡充を考慮した設計とすること。	◎	◎	◎	◎
(3)　設計工程の明確化等	設計工程を明確にするとともに、工程間の調整を行うこと。	◎	◎	◎＊	◎＊
(4)　相互接続への対応	ア　相互接続を考慮した設計とすること。	○	○	－	－
	イ　相互接続を行う場合は、接続先との間で設計工程を明確にするとともに、工程間の調整を行うこと。	◎	◎	－	－
(5)　品質・機能検査の充実化	ア　サーバ等機器導入前の機能確認を十分に実施すること。	◎	◎	◎	◎
	イ　機器等の製造・販売等を行う者から提供されるシステムについての検査手法、品質評価手法を事前に確認すること。	◎	◎	◎	◎
	ウ　セキュリティ対策についてその手法及び事前確認を十分行うこと。	◎	◎	◎	◎
	エ　ネットワークふくそうを回避するため、災害時におけるユーザの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。	◎	◎	－	－
２　ネットワーク施工管理					
(1)　体制の明確化	作業の分担、責任の範囲等の施工管理体制を明確にすること。	◎	◎	◎	◎
(2)　作業工程の明確化等	作業工程を明確にするとともに、その管理を行うこと。	◎	◎	◎	◎
(3)　相互接続への対応	相互接続を行う場合は、接続先との間で作業工程を明確にするとともに、その管理を行うこと。	◎	◎	－	－
(4)　委託工事管理	ア　工事を委託する場合は、委託契約により工事及び責任の範囲を明確にすること。	◎	◎	◎	◎
	イ　工事を委託する場合は、作業手順を明確にするとともに、監督を行うこと。	◎	◎	◎	◎
	ウ　外部委託における情報セキュリティ確保のための対策を行うこと。	◎	◎	◎	◎
(5)　検収試験管理	検収試験においては、実データを使用しないこと。ただし、やむを得ない場合であって、通信の秘密の保護及びデータの保護に十分に配慮する場合は、こ	◎	◎	◎	◎

	の限りでない。				
3　ネットワーク保全・運用管理					
(1)　体制の明確化	作業の分担、連絡体系、責任の範囲等の保全・運用管理体制を明確にすること。	◎	◎	◎	◎
(2)　基準の設定	保全・運用基準を設定するとともに、保全・運用に関する各種データの集計管理を行うこと。	◎	◎	◎	◎
(3)　作業の手順化	保全・運用作業の手順化を行い、手順書の作成を行うこと。	◎	◎	◎	◎＊
(4)　監視、保守及び制御	ア　設備の動作状況を監視し、故障等を検知した場合は、必要に応じ、予備設備への切換え又は修理を行うこと。	◎	◎	◎	◎
	イ　情報通信ネットワークの動作状況を監視し、必要に応じ、接続規制等の制御措置を講ずること。	◎	◎	◎＊	◎＊
(5)　相互接続への対応	ア　相互接続を行う場合は、作業の分担、連絡体系、責任の範囲等の保全・運用体制を明確にし、非常時等における事業者間の連携・連絡体制の整備を行うこと。	◎	◎	－	－
	イ　移動体通信において国際間のローミングサービスを行う場合は、外国の電気通信事業者との間の作業の分担、連絡体系、責任の範囲等の保全・運用体制を明確にすること。	◎	－	－	－
	ウ　モバイルインターネット接続サービスにおいて、コンテンツ等の供給を受けるために接続を行う場合は、その条件及び保全・運用体制を明確にすること。	◎	－	－	－
	エ　相互接続性の試験・検証方式を明確にすること。	◎	◎	－	－
(6)　委託保守管理	ア　保守の委託を行う場合は、契約書等により保守作業の範囲及び責任の範囲を明確にすること。	◎	◎	◎	◎
	イ　保守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。	◎	◎	◎	◎
	ウ　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。	◎	◎	◎	◎
	エ　業務委託先の選別の評価要件の設定を行うこと。	◎	◎	◎	◎
(7)　保守試験管理	保守試験においては、実データを使用しないこと。ただし、やむを得ない場合であって、通信の秘密の保護及びデータの保護に十分に配慮する場合は、この限りでない。	◎	◎	◎	◎
(8)　情報の収集	部外工事に係る情報や企画型ふくそうの原因となる情報等、情報通信ネットワークの健全な運用に必要な情報の収集のための措置を講ずること。	◎	○	○	○
(9)　ふくそう対策	ア　情報通信ネットワークのふくそうを防止し、有効活用を図るため、必要に応じて利用者への協力依頼・周知のための措置を講ずること。	◎	◎	－	－
	イ　災害時等において著しいふくそうが発生し、又はふくそうが発生するおそれがある場合に、情報通信ネットワークの有効活用を図るため、相互接続する事業者が協調して通信規制等の措置を講ずるとともに、ふくそうの波及防止手順の整備及び長期的視点の対策に取り組むこと。	◎	◎	－	－
4　設備の更改・移転					

管理					
(1) 体制の明確化	作業の分担、連絡体系、責任の範囲等の管理体制を明確にすること。	◎	◎	◎＊	◎＊
(2) 作業工程の明確化等	作業工程を明確にするとともに、その管理を行うこと。	◎	◎	◎＊	◎＊
5 情報セキュリティ管理					
(1) 情報セキュリティポリシーの策定	情報セキュリティポリシーを策定し、適宜見直しを行うこと。	◎	◎	◎	◎
(2) 危機管理計画の策定	不正アクセス等への対処を定めた危機管理計画を策定し、適宜見直しを行うこと。	◎	◎	◎	◎
(3) 情報セキュリティ監査の実施	監査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。	◎	◎	○	○
(4) コンピュータウイルス情報緊急通報体制の整備	ア 新たなコンピュータウイルスを発見した場合等、コンピュータウイルスに関する情報を広く一般に周知する必要があるときは、電気通信業界で定めた緊急連絡先に、直ちに連絡すること。	◎	◎	－	－
	イ コンピュータウイルスに関する情報を入手したときは、自社内に対して速やかに周知するとともに、利用者に対してウェブへの掲示、メールニュース等適切な方法により速やかに情報提供する等、被害の拡大を防止するための措置を講ずること。	◎	◎	◎	◎
(5) 情報セキュリティに関する情報収集	最新の情報セキュリティに関する技術情報や業界動向を入手し、それらを情報セキュリティ対策に反映させること。	◎	◎	◎	◎
(6) 知識・技能を有する者の配置	情報セキュリティに関する資格の保有者等一定以上の知識・技能を有する者を配置すること。	◎＊	◎＊	◎＊	◎＊
(7) 情報セキュリティに関する利用者への周知	情報通信ネットワークに対して利用者が与える又は情報通信ネットワークの利用者が受ける可能性のある影響とその対策について利用者に周知すること。	◎	◎	－	－
(8) 社内の重要情報の管理	ア ネットワーク内の装置類やサービスの属性に応じた情報を分類すること。	◎	◎	◎	◎
	イ 情報管理に関する内部統制ルールを整備すること。	◎	◎	◎	◎
(9) サイバー攻撃に備えた管理体制	サイバー攻撃発生時の迅速な情報共有方法を確立すること。	◎	◎	－	－
6 データ管理					
(1) 体制の明確化	作業の分担、連絡体系、責任の範囲等のデータ管理体制を明確にすること。	◎	◎	◎	◎
(2) 基準の設定	データ管理基準を設定すること。	◎	◎	◎	◎
(3) 作業の手順化	データ取扱作業の手順化を行うこと。	◎	◎	◎	◎
(4) データの記録物の管理	ア 設備の仕様及び設置場所等のデータ並びに利用者に関するデータの記録物については、重要度による分類及び管理を行うこと。	◎	◎	◎	◎
	イ 設備の仕様及び設置場所等のデータ並びに利用者に関するデータに対する従事者の守秘義務の範囲を明確にするとともに、その周知、徹底を図ること。	◎	◎	◎	◎
	ウ 利用者の暗証番号等の秘密の保護に配慮するこ	◎	◎	◎	◎

	と。				
	エ　記録媒体の性能向上やシステム間の接続の拡充などによるリスク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。	◎	◎	◎	◎
(5)　ファイル等の遠隔地保管	重要なプログラム、システムデータ及び利用者に関するデータのファイル等については、前世代及び現世代のものを地域的に十分隔たった場所に別に保管すること。	○	○	○	○
(6)　重要データの漏えい防止対策	重要な設備情報（特に他社のセキュリティ情報等）の漏えいを防止するための適切な措置を講ずること。	◎	◎	○	○
7　環境管理					
(1)　建築物の保全	保全点検を定期的に行うこと。	◎	◎	◎	◎
(2)　空気調和設備の保全	保全点検を定期的に行うこと。	◎	◎	◎	◎
8　防犯管理					
(1)　体制の明確化	防犯体制を明確にすること。	◎	◎	◎	◎
(2)　管理の手順化	防犯管理の手順化を行うこと。	◎	◎	◎	◎
(3)　建築物、通信機械室等の入出管理	建築物、通信機械室等の入出管理を行うこと。	◎	◎	◎	◎
(4)　かぎ、暗証番号等の管理	出入口のかぎ及び暗証番号等の適切な管理を行うこと。	◎	◎	◎	◎
(5)　防犯装置の管理	防犯装置の保全点検を定期的に行うこと。	◎	◎	◎	◎
(6)　入出管理記録の保管	入出管理記録は、一定の期間保管すること。	○	○	○	○
9　非常事態への対応					
(1)　体制の明確化	ア　連絡体系、権限の範囲等の非常時の体制を明確にすること。	◎	◎	◎	◎
	イ　非常時における社員・職員、復旧に必要な業務委託先などへの連絡手段、社員・職員の参集手段の確保等の体制を整えること。	◎	◎	○	○
	ウ　非常時における広域応援体制を明確にすること。	○	○	○	○
	エ　相互接続を行う事業者等の間において、非常時の連絡体制や連絡内容を明確にすること。	◎	◎	○	○
	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。	◎	◎	○	○
	カ　非常時において、応急活動、復旧活動にかかわる連絡手段を確保するために必要な措置を講ずること。	◎	◎	○	○
(2)　復旧対策の手順化	復旧対策の手順化を行うこと。	◎	◎	◎	◎
10　教育・訓練					
(1)　体制の明確化	教育・訓練に関する計画の策定及び実施を行う体制を明確にすること。	◎	◎	◎＊	◎＊
(2)　教育・訓練の内容	ア　教育・訓練の目的を明確にするとともに、終了後の実施効果により計画の修正を行うこと。	◎	◎	◎＊	◎＊
	イ　情報通信ネットワークの円滑な運用に必要な知識及び判断能力を養うための教育・訓練を行うこと。	◎	◎	◎	◎＊
	ウ　データ投入等における信頼性の高い作業能力を養うための教育・訓練を行うこと。	◎	◎	◎	◎

	エ　設備の保全に関する知識を養うための教育・訓練を行うこと。	◎	◎	◎＊	◎＊
	オ　防災に関する教育・訓練を行うこと。	◎	◎	◎	◎
	カ　防犯に関する教育・訓練を行うこと。	◎	◎	◎	◎
	キ　情報セキュリティに関する教育・訓練を行うこと。	◎	◎	◎	◎
11　現状の調査・分析及び改善					
(1)　体制の明確化	情報通信ネットワークの維持及び運用に関して、現状の調査・分析を行う体制を明確にすること。	◎	◎	◎	◎
(2)　基準の設定	情報通信ネットワークの維持及び運用に関して、現状の調査・分析を行う項目、評価方法等の基準を設定すること。	◎	◎	◎	◎
(3)　作業の手順化	情報通信ネットワークの維持及び運用に関して、現状の調査・分析作業の手順化を行うこと。	◎	◎＊	◎＊	◎
(4)　改善	ア　情報通信ネットワークの維持及び運用に関して、現状の調査・分析結果を、必要に応じ、情報通信ネットワークの維持及び運用体制並びに手順書に反映させること。	◎	◎	◎	◎
	イ　情報通信ネットワークの維持及び運用に関して、現状の調査・分析結果を、必要に応じ、教育・訓練計画に反映させること。	◎	◎	◎＊	◎＊
12　安全・信頼性の確保等の情報公開					
(1)　情報通信ネットワークの安全・信頼性の確保に係る取組状況	情報通信ネットワークの安全・信頼性の確保の取組状況を適切な方法により利用者に対して公開すること。	◎	◎	―	―
(2)　情報通信ネットワークの事故・障害の状況	情報通信ネットワークの事故・障害の状況を適切な方法により利用者に対して公開すること。	◎	◎	―	―
(3)　サービスの特質等の周知	情報通信ネットワークにおいて、サービスを提供できなくなる場合などについて利用者に周知すること。	◎	◎	―	―

注　実施指針の欄中、「◎」、「◎＊」、「〇」及び「－」は、それぞれ次のことを示す。
◎　：実施すべきである。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。
〇　：実施が望ましい。
－　：対象外

別表第３　情報セキュリティポリシー策定のための指針

１　目的

この指針は、情報通信ネットワークの健全な発展に寄与することを目的とし、適正なリスク管理を実現させるための基本となる情報セキュリティポリシー策定のための指針として定めたものである。

２　情報セキュリティの管理

情報セキュリティを適切に管理していくためには、情報セキュリティの「方針立案」、「対策実施」、「運用・監視」及び「監査・診断」の各段階において、以下の対策を行う必要がある。

⑴　方針立案

ア　情報セキュリティポリシー及び実施手順の策定

情報セキュリティを適正に管理していくために、組織における情報セキュリティ対策に関する統一方針として情報セキュリティポリシーを策定する。

また、情報セキュリティポリシーに基づき、実際の業務・作業レベルまで考慮した情報セキュリティ実施手順を策定する。

イ　情報セキュリティ組織体制の整備

情報セキュリティに関して、責任所在の明確化やセキュリティ情報の共有化を行うために、情報セキュリティ組織体制を整備する。

⑵　対策実施

情報セキュリティポリシーの普及・教育

情報セキュリティポリシーが適正に実施されるよう、普及・教育活動を行い、情報セキュリティに対する自覚や意識の向上を目指す。

⑶　運用・監視

ア　情報セキュリティポリシーに沿った運用

情報セキュリティポリシーを理解し、情報セキュリティポリシーに沿った運用を適正に実行する。

イ　例外の管理

業務を遂行する中で、情報セキュリティポリシーが適用できない場合が発生する可能性もある。情報セキュリティポリシーから逸脱した際に、適正に管理する仕組みを確立する。

ウ　情報セキュリティ侵害時の対応の明確化

情報セキュリティ侵害が起きた際、速やかに侵害の事実、状況を伝達できるよう伝達経路を明確化する。

⑷　監査・診断

ア　情報セキュリティ監査

情報セキュリティポリシーが組織内において正しく実行されていることを把握するため定期的に監査する。

イ　情報セキュリティポリシーの見直し

情報セキュリティ監査結果や情報セキュリティを取り巻く環境等を考慮し、情報セキュリティポリシーを定期的に見直し、改訂を行う。

３　情報セキュリティポリシーの構成等

情報セキュリティの環境は技術動向、組織状況により変化することから、次のように情報セキュリティポリシーを目的、原則及び方針の三段階に階層化させることで、下位の方針のみを見直し、時代・環境変化に対応することができる。

⑴　目的

情報セキュリティポリシーにおいて最も基本となるもので、組織としての情報セキュリティへの取組の目的を定めるものである。最高権限者の声明として記述し、組織全体で積極的に情報セキュリティに取り組むことを明確化することが望ましい。

⑵　原則

目的に基づき、情報セキュリティを実現するための組織方針、組織理念等組織の基本的な考え方を定めるものである。利便性とセキュリティのバランスをどのように取るかといった、情報セキュリティ全体の考え方の根幹となる。

⑶　方針

原則に基づき、情報セキュリティを実現するための基本方針をテーマごとに具体化し定めるものである。各方針に対し、責任の所在を明確化する必要がある。

(4)　実施手順

定められた情報セキュリティポリシーを確実に実施するため、情報セキュリティポリシーに基づき、具体的な手順や方法を実施手順として定めることが一般的である。実施手順では、情報システムが最低限備えるべき具体的セキュリティ要件や、各情報システムの利用方法等、各方針に沿い、実際の業務、手順、方法等を記述することとなる。

4　情報セキュリティポリシーの策定

情報セキュリティポリシーは、組織として取り決めた最も重要な規程となるため、組織の幹部の関与により策定することが一般的である。

情報セキュリティポリシーの策定に当たり、各部門の業務に何らかの制約や変更を要請することがあるため、経営企画部門、総務部門といった社内規定を担当する部門が中心となり、各部門よりメンバーを召集して策定の為のチームを設立し、策定を行うことが望ましい。

なお、情報セキュリティポリシーには、情報システム部門、人事部門、監査部門等の部署の役割が非常に大きいため、これらの部門からの積極的参加を要請する。

また、外部コンサルティングサービスを提供する機関を活用し、策定に当たってのスケジュール、策定方法、記述事項等についての助言を得ることが好ましい。

情報セキュリティポリシーを策定する際の実施手順を以下に示す。

(1)　情報セキュリティポリシー策定チームの編成

各部門よりメンバーを召集し策定のためのチームを設立する。

(2)　「目的」及び「原則」の明確化

組織としての情報セキュリティに関する考えの根幹となる「目的」及び「原則」を定める。

(3)　情報セキュリティポリシーの適用範囲の明確化

情報セキュリティポリシーがどの範囲まで適用されるのかを明確化する。

(4)　情報資産の洗い出し

現在、組織が保有する情報資産とその価値を明確化する。

(5)　情報資産を取り巻く脅威とその脅威に対するリスクの分析

保護すべき情報資産を明らかにし、脅威の発生頻度、影響度を基にリスクを分析する。

(6)　「方針」の明確化

各情報資産を保護するために、組織としてどのような方針をもって対策を行うかを明確化する。

5　情報セキュリティポリシーの構成例

情報セキュリティポリシーの構成例と各項目における記述内容を以下に示す。

ここでは、方針を「情報セキュリティ運営に関する方針」と「情報資産に関する方針」に大きく分け、前者では管理の各段階に応じた項目、後者では情報資産の大きな区分である「情報」、「情報システム」、そして、情報資産を保護するための「アクセス制御」という項目立てとしている。

１　総則

(1)　目的

情報セキュリティの必要性と組織としての情報セキュリティの目的を記述する。最高権限者の声明として記述することで、情報セキュリティに対して組織全体で積極的に取り組むことを表明することが望ましい。

(2)　適用範囲

人、組織、場所、情報資産、技術等の切り口で情報セキュリティポリシーが適用される範囲を明確化する。

(3)　用語及び定義

情報セキュリティポリシー内で用いる用語の意味を明確にし、読者が共通の解釈の下、理解・判断できるよう用語の定義を行う。

(4)　原則

組織としての情報セキュリティに対する考え方の根幹となる原則を明確にし記述する。すべての方針、対策等は、ここで記述される原則に準拠しなければならない。例として、法令の遵守を原則として記述した場合、この原則に準拠し各組織員の役割等を方針にて定める。

２　方針

(1)　セキュリティ運営に関する方針

ア　情報セキュリティ組織

組織内の情報資産を管理し、セキュリティを担保する仕組みを確立する。具体的には、経

営陣による情報セキュリティフォーラムの設立と、情報セキュリティに関する責任者の割当てを行う。また、組織内で働く外部業者を適用範囲に含む際は、その管理方法（契約時の必須項目等）を明確化する。

イ　普及・教育

情報セキュリティに対する知識と意識を向上させ、適用範囲内すべての人が情報セキュリティポリシーを理解し、遵守するよう、情報セキュリティポリシーの普及・教育活動を行うことを記述する。

ウ　例外の管理

情報セキュリティポリシーから逸脱する事項を管理・統括する組織・方法を明確にする。費用対効果を分析した結果、情報セキュリティポリシーに準拠することが得策ではない事項等が発生した際の対処方法を明確にすることで、逸脱発見者が迅速に対応を行い、組織として逸脱事項を管理・統括する体制を整備する。

エ　情報セキュリティ侵害時の対応

適用範囲内において、情報セキュリティ侵害が発生した際の対応手順を明確化することで、発生時に迅速に対応できる体制、方法を確立する。また、情報セキュリティポリシー違反者及びその監督責任者に対する罰則についても記述する。

オ　情報セキュリティ監査

情報セキュリティポリシーが組織内において正しく実行されていることを把握するため、定期的に監査する必要がある。監査組織と監査結果を把握する者を明確化する。

カ　情報セキュリティポリシーの改訂

情報セキュリティ監査結果や情報セキュリティを取り巻く環境等を考慮し、情報セキュリティポリシーを定期的に見直し、改訂を行う。改訂手順についても明確化する。

(2)　情報資産に関する方針

ア　情報

適用範囲内の情報についての管理方法を明確化することで、情報の漏えい、破壊、改ざん等を防止する。また、プライバシーにかかわる情報を取り扱う際に遵守すべき事項を明確化する。

(ｱ)　情報管理

情報の漏えい、破壊、改ざん等による被害等に応じて、情報を区分する。情報の区分と情報の取得・生成、保管、流通、利用及び廃棄という各段階における情報の取扱方法を明確にし、組織員による情報の取扱方法を統一化する。

(ｲ)　プライバシー情報

通信の秘密を含むプライバシー情報の漏えいは深刻な権利利益侵害につながるおそれが高いため、電気通信事業者に対しては、「電気通信事業における個人情報保護に関するガイドライン」（平成１６年総務省告示第６９５号）が制定されている。

プライバシー情報の適切な利用と保護が極めて重要であるとの認識により、プライバシー情報の取扱いについては、個別の項目を設け、個人情報の収集、利用・提供、適正管理、責任の明確化等について、遵守すべき方針を明確に記述する。

イ　情報システム

適用範囲内の情報システム上にて取り扱われる電子情報の漏えい、破壊、改ざん等の防止及び情報システム停止による損害の抑止を目的とし、情報システムについての管理方法（設計、構築及び運用方法）を明確化する。

(ｱ)　情報システム設計・構築

情報システムの設計、構築時における管理体制と、情報システムに実装すべきセキュリティ機能（アクセス制御機能、フロー制御機能、暗号化制御機能等）を明確化する。

(ｲ)　情報システム運用・停止

情報システムを適切に運用するための管理体制と実施事項を明確化する。また、情報システム障害時の対応策についても明確化する。

(ｳ)　情報システムの使用権

情報システムの利用資格管理が適切に行われないと、情報システムの不正利用を招く危険がある。そこで、情報システムの使用権を、必要な者に、必要な期間与え、情報システムの利用資格に関する義務・責任を明確化する。また、情報システムの不正利用の定義を明確化する。

(ｴ)　ネットワークセキュリティ

　ネットワークは情報流通の基盤であるとともに、情報侵害の経路ともなり得るため、適切に把握・管理することが必要である。セキュリティ侵害を防止するため、管理体制・実施事項を明確化する。

(ｵ)　コンピュータウイルス

　業務で使用する機器がコンピュータウイルスに感染した場合、多大な被害が発生する可能性があるため、感染の予防及び防止が重要である。そこで、コンピュータウイルスに関しても管理体制を確立し、予防及び防止並びに感染時の対策を明確化する。また、コンピュータウイルス等による情報漏えいの防止対策も明確化する。

　また、コンピュータウイルスによる情報漏えいが懸念されるため、情報漏えいを発生させる懸念のあるソフトウェアの導入を防止する等の予防措置を明確化するとともに、コンピュータウイルスに感染した場合の情報漏えいの防止対策を明確化する。

ウ　アクセス制御

　適用範囲内の情報システムの利用、建物への入館、事務室及び機械室への入室等に際しては、情報資産を保護するため、個人を識別・認証し、情報へアクセスする際に審査することが必要である。そこで、利用者を限定・把握できるよう実施事項を明確化する。

別表第４　危機管理計画策定のための指針

１　目的

危機管理計画は、サイバーテロについてあらかじめ対処方法を定めておくことで、実際にサイバーテロが発生した場合に迅速な対応を可能とし、早期に現状へ復旧し、被害の拡大を防ぐことを目的とするものである。この指針は、電気通信事業用ネットワークにおいてサイバーテロが発生した場合の緊急対応体制を整備するため、危機管理計画策定の指針として定めたものである。

電気通信事業用ネットワーク以外のネットワークにおける危機管理計画についても対象とするネットワーク、想定される攻撃等を考慮し、本指針を参考として策定されることが望ましい。

２　サイバーテロの定義等

⑴　サイバーテロの定義

サイバーテロは、コンピュータウィルスやハッカーによつて個人が被害を受けるものとは異なり、国家等の重要システムを機能不全に陥れるものであることから、この指針におけるサイバーテロの定義は、「ネットワークを通じて各国の国防、治安等をはじめとする各種分野の情報システムに侵入し、データを破壊、改ざんするなどの手段で国家等の重要システムを機能不全に陥れる行為」とする。

⑵　攻撃対象となる重要インフラ

サイバーテロの攻撃対象となつた場合、その産業、企業のみならず、広く国民生活に重大な影響が及ぶこととなる重要インフラとして、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）等が想定される。

⑶　重要インフラの相互依存性

各重要インフラは、他の重要インフラと独立して存立するのではなく、相互に依存し存立しており、ある重要インフラが攻撃を受けた場合、関連する他の重要インフラも影響を受ける場合が多々あることから、重要インフラを保有してサービスを提供する事業者は、他インフラへの影響も考慮した対策が必要である。

⑷　主な攻撃方法

サイバーテロにおける主な攻撃方法の具体例としては、次のものがある。

ア　物理的な攻撃

電気通信施設に不正侵入し、ネットワーク管理センターを占拠する等によりネットワークのコントロールを奪い、これをまひさせるような攻撃

イ　ホームページ改ざん

思想的な意図等により社会に広くアピールするため、ホームページの掲載内容を改ざんするもの

ウ　分散協調型サービス拒否（以下「ＤＤｏｓ」という。）攻撃

複数の場所からサーバーの処理能力を超える大量のデータを送り付けるなどの方法によりサーバーを停止させるもの

エ　コンピュータウィルス

強力な感染力と破壊力を持つウィルスによる攻撃

オ　不正侵入（なりすまし）

他人になりすまして侵入し、データの改ざん、削除を行うほか、他への攻撃にも使用

３　危機管理計画の策定

危機管理計画の策定に当たつて配慮すべき内容を以下に示す。

⑴　対象

ア　攻撃

対象とするべき電気通信ネットワークのぜい弱な部分の具体例は次のとおりである。これを参考として、各電気通信事業者の状況により大規模な影響が出ることを想定し、対象となる攻撃を明確に規定する。

(ｱ)　固定・移動電話網

物理的な攻撃、意図的なふくそうによる攻撃

(ｲ)　移動電話網

電波による不正アクセス、電波による通信妨害

(ｳ)　専用回線網及び中継回線網

電波妨害

(ｴ)　ＩＰネットワーク
　　サーバー等への攻撃、モバイルインターネットアクセスへの攻撃、コンピュータウィルス
(ｵ)　ネットワークの機能を管理・運営するコンピュータ
　　電磁波による情報漏えい

イ　被害規模の対象範囲

各電気通信事業者の状況により大規模な影響が出ることを想定して、被害規模の対象範囲を明確に規定する。

その際には、電気通信事業法施行規則（昭和 60 年郵政省令第 25 号）第 58 条の報告を要する重大事故の基準も参考とする。

(2)　予防

必要に応じて次のハッカー対策、コンピュータウィルス対策等を規定し、サイバーテロに対する予防措置を図る。

ア　インターネットに接続するための機器の配置及び構成

(ｱ)　ファイアウォール等を設置して適切な設定を行う。
(ｲ)　非武装セグメント構成を採用する。
(ｳ)　開放網と閉域網とを区別したネットワーク構成を採用する。
(ｴ)　ｔｅｌｎｅｔやｆｔｐ等サービス提供に不用な通信の接続制限を行う。
(ｵ)　最新の情報セキュリティ技術を採用する。
(ｶ)　攻撃元を特定できる機能と攻撃元のトラヒックを遮断する仕組み等を採用する。

イ　ソフトウェア上の対策

(ｱ)　インターネットに接続する場合は、サーバー等におけるセキュリティホール対策を講ずる。
(ｲ)　コンピュータウィルス及び不正プログラム混入対策を講ずる。

ウ　監視、管理等

(ｱ)　インターネットに接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されるよう措置する。

　　また、ネットワーク上のパケット並びにサーバー及びネットワーク機器の動作に関するログの適切な記録及び保存を行う。

(ｲ)　コンピュータからの漏えい電磁波の低減対策、又は電磁環境に配慮した上で漏えい電磁波をマスクする措置を講ずる。

エ　不正アクセス防止のためのシステム上の設定

(ｱ)　利用者の識別・確認を要する通信を取り扱う情報通信ネットワークには、正当な利用者の識別・確認を行う機能を設ける。
(ｲ)　アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずる。
(ｳ)　利用者のパスワードの文字列をチェックし、一般的な単語を排除する機能を設ける。
(ｴ)　アクセス失敗回数の基準を設定するとともに、基準値を超えたものについては、履歴を残しておく機能を設ける。
(ｵ)　保護することが求められる重要な情報については、その情報に対するアクセス要求を記録し、保存する機能を設ける。
(ｶ)　ネットワークへのアクセス履歴の表示又は照会が行える機能を設ける。
(ｷ)　一定期間以上パスワードを変更していない利用者に対して注意喚起する機能を設ける。
(ｸ)　一定期間以上ネットワークを利用していない利用者がネットワークにアクセスする際に、再開の意思を確認する機能を設ける。
(ｹ)　アクセスにおける本人認証手段には、端末認証（ＭＡＣアドレス、シリアル番号等）や生体認証（指紋、静脈等）など、高度な認証方式の導入を検討する事が望ましい。

オ　通信の秘密の保護

(ｱ)　機密度の高い通信には、秘話化又は暗号化の措置を講ずる。
(ｲ)　適切な漏話減衰量の基準を設定する。

カ　ネットワークの不正使用の防止

ネットワークの不正使用を防止する措置を講ずる。

キ　新たな手法による攻撃に対するハード・ソフト対策の体制強化

ネットワークシステムの脆弱性に対処できるように内部統制や社内ルールを随時見直し、新た

な手法による攻撃に対しても迅速にハード・ソフト両面で対処できる体制を確立・強化する。

ク　他の利用者へ悪影響を与えている利用者に対する一時利用停止の明確化

他の利用者に悪影響を与えている事象を洗い出し、当該事象への対応方針を策定し、利用者の合意形成を図る。

ケ　サーバー等への攻撃が発生した際の迅速な情報共有方法の確立

(3)　発生時の復旧対応

ア　復旧対応としては、必要に応じて次の項目を規定するとともに、既存の障害復旧マニュアル等を活用することも規定する。

(ｱ)　サーバー等への攻撃からの復旧対応

Ａ　ＤＤｏＳ攻撃により通信不能となつた場合、攻撃側サーバーの速やかな停止を依頼する。

Ｂ　サーバーのルート権限を奪われる等により不正な処理を開始した場合、サーバーを停止する又はネットワークから切断し再起動する。

Ｃ　サーバーが何らかの原因により不正な処理を開始した場合、ルート権限で不正な処理のプロセスを排除する。

Ｄ　サーバーへの侵入の痕跡を発見した場合、サーバーをネットワークから隔離する。

Ｅ　サーバー等が通信不能となつた場合、通信不能箇所を特定し再起動などの処置を行う。

(ｲ)　伝送交換設備への攻撃からの復旧対策

Ａ　重要な伝送路設備には、応急復旧用ケーブルの配備等の応急復旧対策を講ずる。

Ｂ　移動用交換設備の配備等の応急復旧対策を講ずる。

Ｃ　災害時等において、衛星地球局等の無線設備により、臨時電話等の設置が可能であること。

Ｄ　移動体通信基地局と交換局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。

Ｅ　移動体通信基地局に障害が発生した場合等に、可搬型無線基地局により、臨時の電気通信回線の設定が可能であること。

Ｆ　他の伝送設備の障害時に、通信の疎通が著しく困難となつた場合、予備の設備等により臨時の電気通信回線の設定が可能であること。

イ　緊急時における対処には、高度な判断を必要とする場合があることから、責任と権限を有する適切な者が速やかに判断を行うことができるように規定する。

ウ　複数の電気通信事業者に障害が発生し、その影響が波及して被害が拡大していくことが想定されることから、障害情報等を交換し被害を最小限に抑えるために、国、電気通信事業者、事業者団体等の関係者間で連絡体制、運用方法を明確に規定する。

(4)　原因判明時の措置

ア　当該障害がサイバーテロによるものであることが判明した場合は、一定のルートで国、電気通信事業者、事業者団体等の関係者に通知することが可能なよう、(3)ウと同様に伝達ルート等をあらかじめ定めておく。

イ　障害の発生状況及び影響の拡大防止に対する協力に関して、電気通信事業者から利用者への周知方法等について規定する。

ウ　障害の発生原因が判明し、再度攻撃にさらされるおそれがある場合における障害の発生防止のため、必要な措置を講じることを規定する。

エ　ネットワークを介して、他分野の重要インフラ事業者と情報システムを相互接続している場合には、サイバーテロ対策に関し互いの連絡・連携体制を必要に応じ構築する。

(5)　危機管理計画の見直し等

ア　技術の進展に伴い、サイバーテロによる攻撃方法等が、変化していくと考えられるため、適宜危機管理計画の見直しを行うことを規定する。

イ　サイバーテロが発生した際の対処を円滑に行えるよう、必要に応じサイバーテロの発生を想定した訓練を実施することを規定する。

設備等基準の対策項目（解説）

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

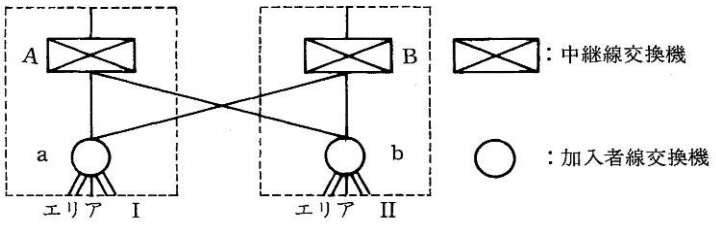
通信を安定的に提供し、災害等の発生時において、疎通の全面的停止を防止するため、通信の取扱いの地理的範囲やネットワーク全体のバランス等を考慮しながら、重要な通信センターを地域的に分散して設置する。

「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、MT 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

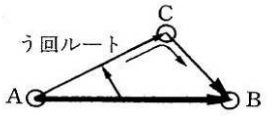
交換網の場合は、二つの重要な通信センター間を結ぶ接続系統の障害に対し、その代替となる他の通信センター経由のう回接続系統を設けること。

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

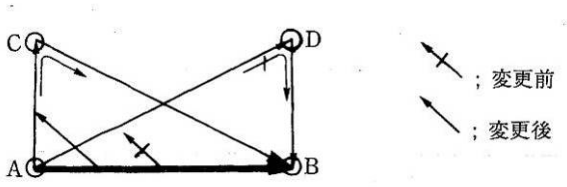
通信センター間回線を他の通信センター経由の回線にう回させる。



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

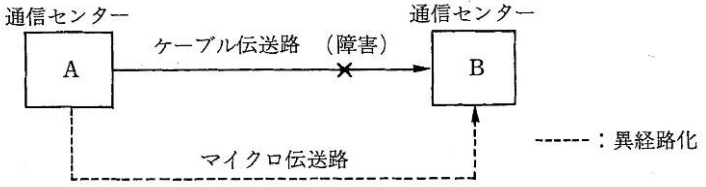
伝送路設備の障害に対処するため、疎通する通信量等を考慮し、重要な通信センター間を結ぶ伝送路設備については、複数の経路に設置する。

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

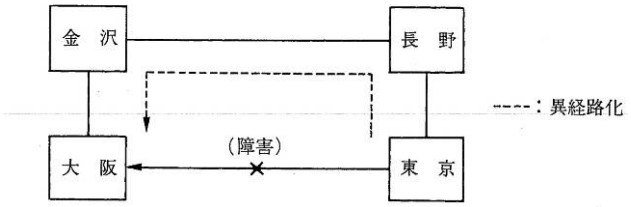
一つの伝送路が故障になった時でも、他の伝送路収容の回線により、通信サービスの一部が維持できるように対地間の伝送路を異なる伝送媒体により複数設置する。



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

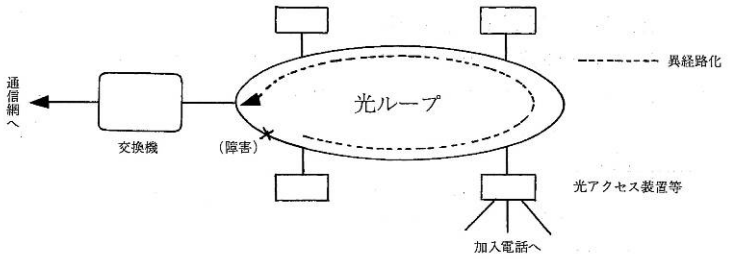
イ　重要な光加入者伝送路は、ループ化等による２ルート化を促進すること。

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

(4)　電気通信回線の分散収容

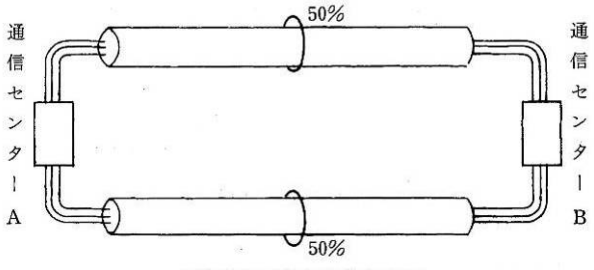
重要な通信センター間を結ぶ電気通信回線の収容は、異なる伝送路設備に分散して行うこと。

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又は相当広範囲の利用者に影響する場合は、当該設備について､地域的に分散して設置するとともに分散した設備を複数の経路で接続し、故障等による影響範囲を限定すること。

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

サーバー及びゲートウェイの設備は、通信の集中を考慮した適切な容量のものを設置すること。

解説

第３世代移動通信システムでは、伝送速度が向上することからメールサーバーやルーター等のゲートウェイの設備への負担が増加することが考えられる。また、第２世代移動通信システムを含むモバイルインターネット接続サービスの利用は今後も増大し、さらに同サービスに新しいコンテンツやアプリケーションが追加された際には加入者の急増も見込まれ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) 電子メールによる一方的な広告・宣伝等への対策

モバイルインターネット接続サービスにおいては、利用者が指定した特定の条件に該当する電子メールの受信を拒否する等の機能を設けること。

解説

モバイルインターネット接続サービスにおけるいわゆる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 利用者に電話番号から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。

等

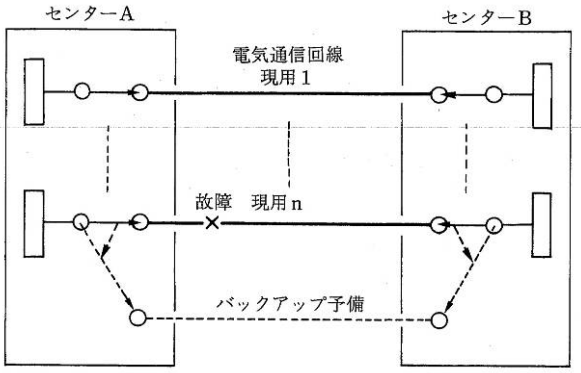
(8)　予備の電気通信回線の設定等

ア　重要な伝送路設備には、予備の電気通信回線を設定すること。ただし、他に疎通確保の手段がある場合は、この限りでない。

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

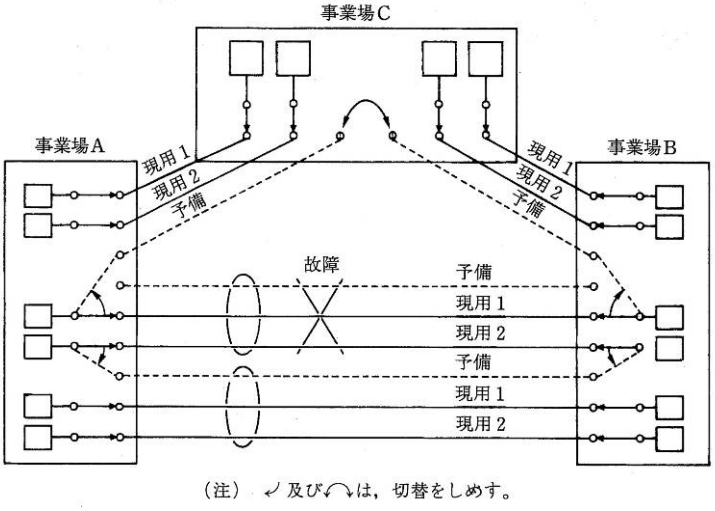
イ　重要な伝送設備には、予備の電気通信回線に速やかに切り換える機能を設けること。

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。



回線切り替えの例

(9) 情報通信ネットワークの動作状況の監視等

ア　重要な伝送路設備の動作状況を監視し、故障等を速やかに検知、通報する機能を設けること。

イ　重要な電気通信回線の動作状況を監視し、故障等を速やかに検知、通報する機能を設けること。

ウ　重要な伝送路設備の動作状況を統合的に監視する機能を設けること。

エ　重要な電気通信回線の動作状況を統合的に監視する機能を設けること。

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。

なお、事業用電気通信設備のうちアナログ電話用設備等については、技術基準（事業用電気通信設備規制(昭和 60 年郵政省令第 30 号)第５条及び第 39 条により、電源停止、共通制御機器の動作停止その他電気通信役務の提供に直接係る機能に重大な支障を及ぼす故障等の発生時には、これを直ちに検出し、通知する機能を備える旨定められている。

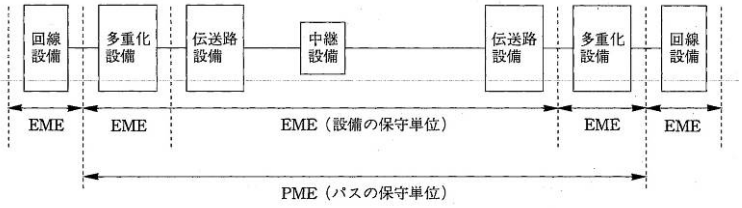
●措置例●

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、通報する機能を設けること。ただし、通信が同時に集中することがないようこれを制御する措置を講ずる場合は、この限りでない。

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。

カ　交換設備には、通信の接続規制を行う機能又はこれと同等の機能を設けること。ただし、通信が同時に集中することがないようこれを制御する措置を講ずる場合は、この限りでない。

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出接続規制を行う。

「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。

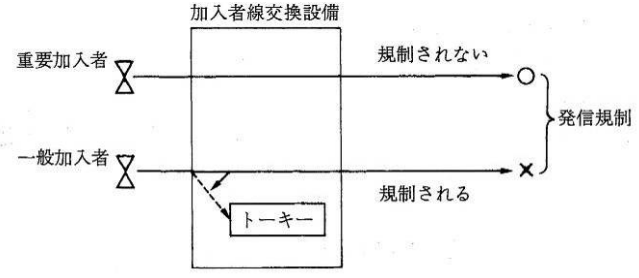
なお、データ通信用のネットワーク等では、交換設備から端末設備等の発信機能を制御する通信方式を採用している場合のように、原理的に異常ふくそうが発生するおそれがないものがあるので、この場合は適用しないことをただし書により定めている。

●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共通機器能率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。

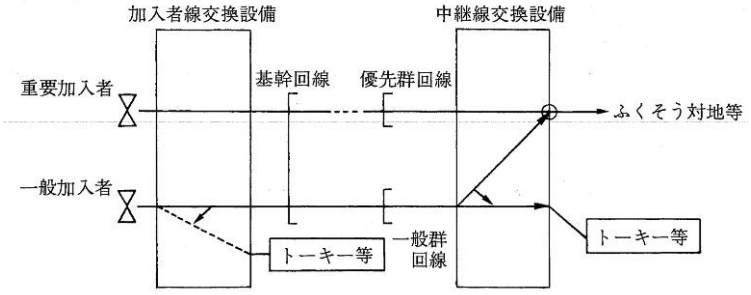
発信規制時は、重要加入者以外の一般加入者を規制し、着信については規制しない。



発信規制

２　出接続規制

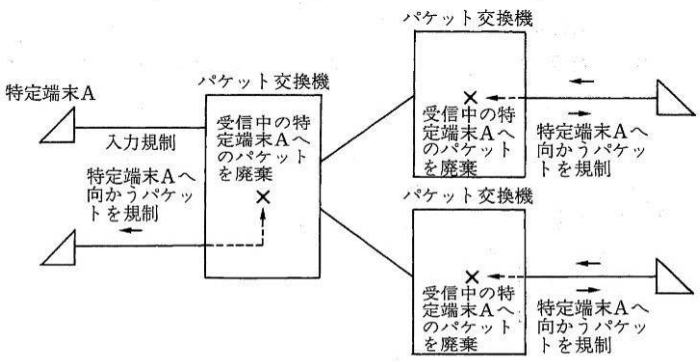
特定対地、特定加入者への接続を制限する。



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これを制御する措置を講ずる場合は、この限りでない。

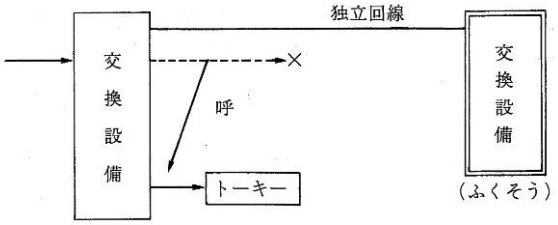
解説

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

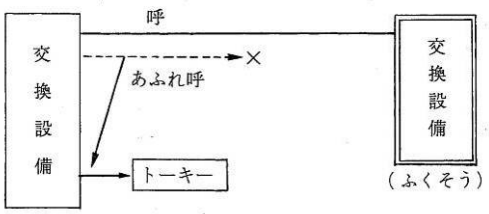
交換設備の、ある方路への接続に際して、その方路への接続動作を行わず、直ちに案内トーキーに接続する。



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。

(10)　ソフトウェアの信頼性向上対策

ア　ソフトウェアを導入する場合は、品質の検証を行うこと。

イ　ソフトウェア及びデータを変更するときは、容易に誤りが混入しないよう措置を講ずること。

ウ　システムデータ等の重要データの復元ができること。

エ　ソフトウェアには、異常の発生を速やかに検知、通報する機能を設けること。

オ　ソフトウェアには、サイバー攻撃等に対する脆弱性が無いように対策を継続的に講ずること。

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　重要なデータ等は磁気ディスク等の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　モバイルインターネット接続サービスにおいて、新しいシステムの導入に当たっては、実際に運用する場合と同一の条件や環境を考慮し、ハードウェアの初期故障、ソフトウェアのバグによる障害が可能な限り発生しないよう十分なシミュレーションを実施すること。

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。

キ　IP 系接続サービスにおいては、現用及び予備機器の切替えを行うソフトウェアは十分な信頼性を確保すること。

解説

IP 系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、更新にあたってはウイルス等の混入を防ぎ、セキュリティを確保すること。

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　定期的なソフトウェアの点検及び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。

(11)　情報セキュリティ対策

ア　インターネットへ接続する場合は、ファイアウォールを設置して適切な設定を行うこと。

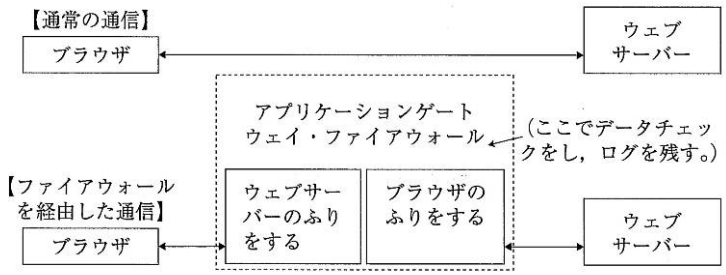
解説

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

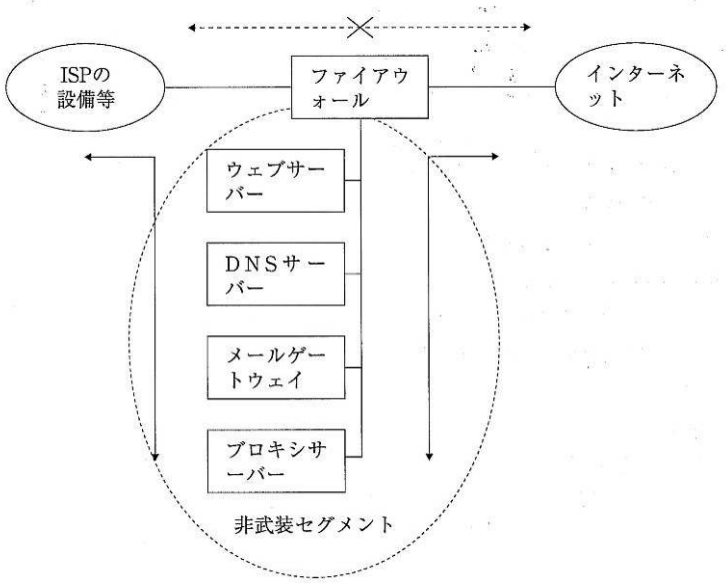
イ　インターネットへ接続する場合は、非武装セグメント構成を採用すること。

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ー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 サーバー、メールサーバー等を配置する。



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 や ftp 等サービス提供に不用な通信の接続制限を行うこと。

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、サーバー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、サーバー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●

具体的な措置例は次のとおりである。

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 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 下記参照

(参考)UNIX 上でシステムに関係したサービスを提供するバックグランドプロセス(例 routed 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ー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されること。

解説

ネットワークやサーバー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）の導入が上げられるが、このシステムは、急速な発展を遂げてきているものであるところであり、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ー及びネットワーク機器の動作に関するログの適切な記録及び保存を行うこと。

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ー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、原則として取扱規定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、被害の拡大も危惧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 サーバー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、そのサーバーなどをダウンさせる攻撃である。

●措置例●

具体的な措置例は次のとおりである。

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、ファイルサーバー、メールサーバー等について、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マスク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●

①CRT ディスプレイに代えて液晶ディスプレイを使用すること。

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すること。

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すること。

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すること。

⑤CRT 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すること。

サ　利用者の識別・確認を要する通信を取り扱う情報通信ネットワークには、正当な利用者の識別・確認を行う機能を設けること。

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天性とし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。

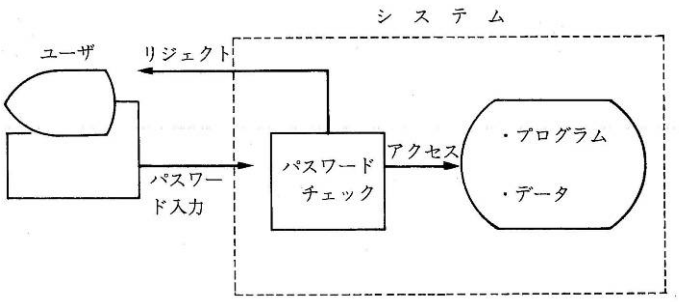
●措置例●

<u>１　パスワードによる識別、確認方法</u>

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。



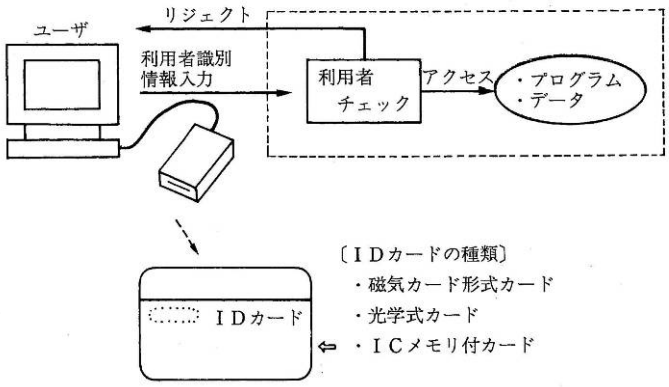
パスワードによる識別

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ー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

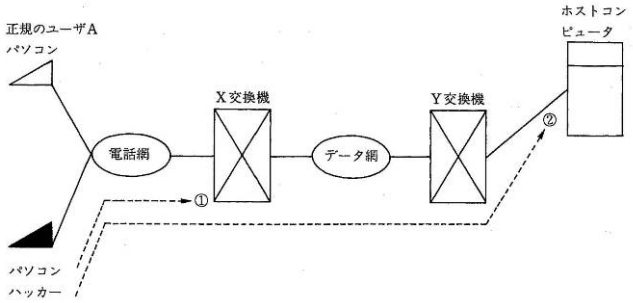
手の大きさ、指の太さ、長さなどの特徴を識別し、使用者を確認する。

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。

（参考）情報通信の高度化に伴う新たな問題：ハッカー

ハッカーとは、他人のパスワード（暗証番号）を何らかの方法（試行錯誤等）で捜し当て、他人になりすましてネットワークやホストコンピュータに侵入し、情報の盗用、データやプログラムの改ざん等を行うコンピュータ侵入者のことである。ハッカー行為は、知的な遊びとしてとらえられ、犯罪意識が薄いといった傾向がある。ハッカーは、捜し当てたパスワードを不正使用すること等によって、次図のように侵入する。



ハッカーの侵入経路

①ネットワークへの侵入
　ネットワーク利用パスワードの入力
　→X交換機は契約者Aと確認。ネットワークを利用して通信が可能となる。
②ホストコンピュータへの侵入
　ホストコンピュータ利用パスワードの入力
　→ホストコンピュータは契約者Aと確認。ホストコンピュータを利用してデータの検索等が可能となる。
　ハッカーは、以上二種類のパスワードを知る必要がある。
　主なハッカー対策を次表に示す。

ネットワークコンピュータサイド	① アクセスの制限・監視の強化 ・アクセス領域及び使用可能命令の範囲の制限 ・アクセス失敗の監視 ・履歴の記録等 ② コールバック方式の採用 ・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。 ③ パスワード以外の認証方式の採用 ・天性の特徴（声紋、指紋、手形、署名等）によるもの ・IDカード、ICカード等 ・ディジタル署名
ユーザサイド	① セキュリティ意識の向上 ② パスワードの厳重な管理 ・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。 ・パスワードを頻繁に変更する。 ③ データの暗号化（暗号装置、暗号ソフトウェアの付加等）

主なハッカー対策

シ　アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずること。

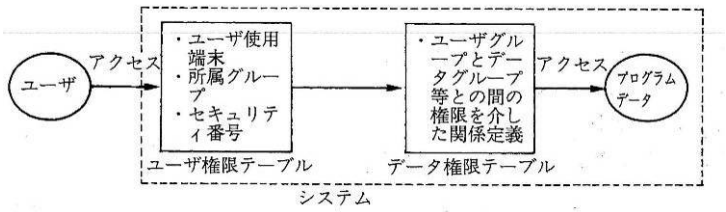
解説

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。

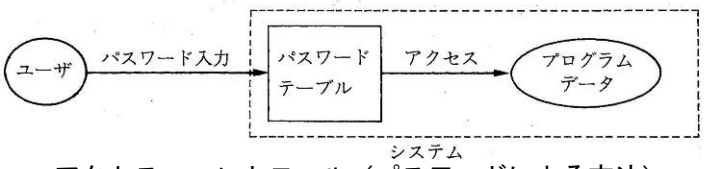
●措置例●

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。

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 種類の文字を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、基準値を越えたものについては、履歴を残しておく機能を設けること。

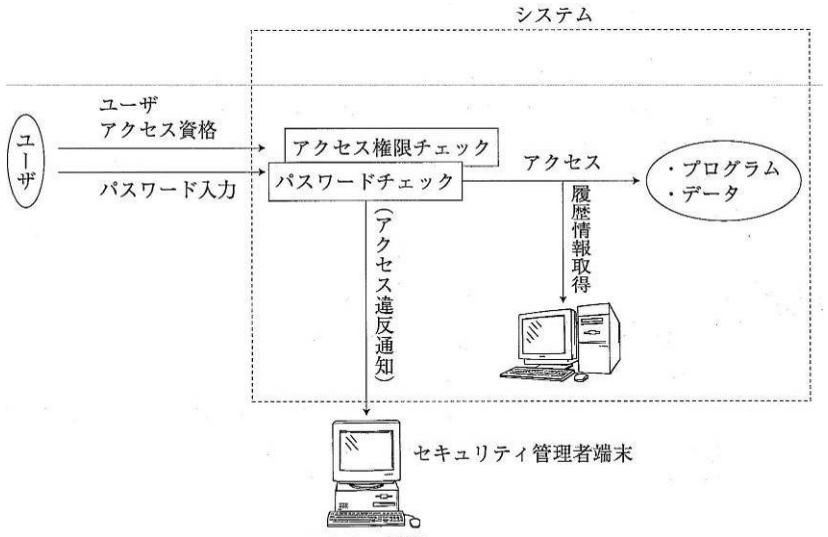
ソ　保護することが求められる重要な情報については、その情報に対するアクセス要求を記録し、保存する機能を設けること。

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。

●措置例●

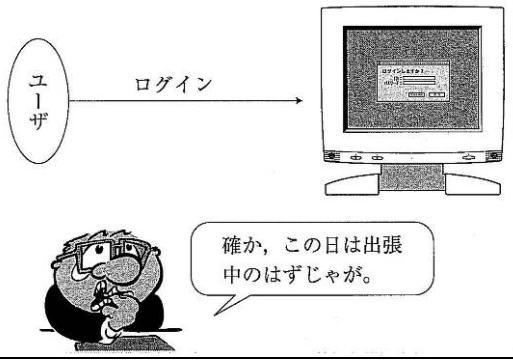


アクセス監視

タ　ネットワークへのアクセス履歴の表示あるいは照会が行える機能を設けること。

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アクセスする際に、再開の意思を確認する機能を設けること。

解説

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を探したり、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。

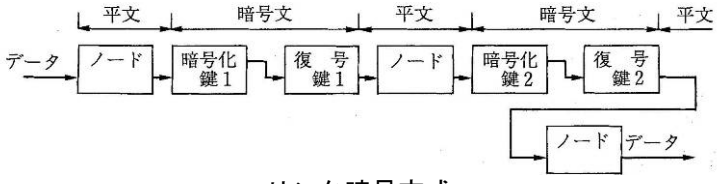
2　暗号化措置

暗号の目的は、正当な送受信間でのみ意味を理解できるメッセージ交換を可能にし、不当な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

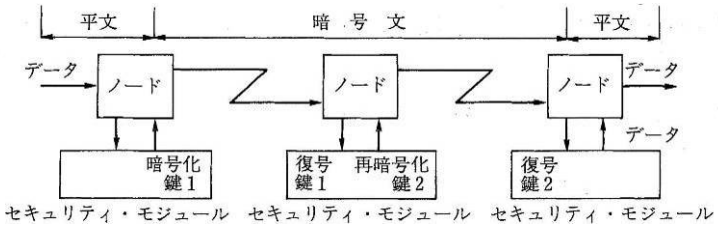
ネットワーク内で隣接するノードとノードを接続するリンク上でのみ暗号されているがノードで処理されている間は平文となっている方式である。情報の行先を示す経路情報を暗号化することも可能である。



リンク暗号方式

(2) ノード暗号方式

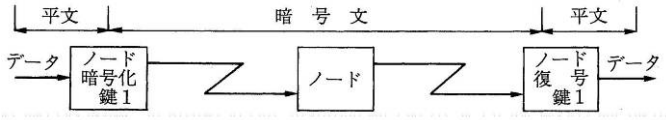
この方式は、リンク方式の弱点（ノードで処理されている間は平文となっている）を補うもので、データはノード内のセキュリティ・モジュールにより暗号化、復号及び再暗号化が行われる方式である。経路情報は平文のままである（暗号化してはならない）。



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、端点間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

(4)三つの方式の比較

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第一種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などの措置を行う。

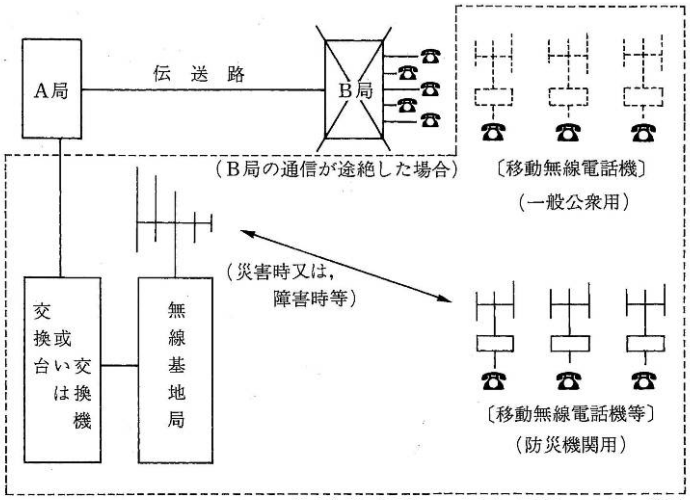
(12)　通信の途絶防止対策
通信の途絶を防止する措置を講ずること。

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。

●措置例●

図に、非常通信設備として、移動無線電話機を用いた場合の回線構成例を示す。この場合の移動無線電話機の所要数は、当該地域の防災関係機関等の公共機関並びに被災時に必要な一般公衆回線の数を勘案して配備する。



注：一般公衆用の移動無線電話機は，B局に保管しておき，通信途絶時に使用する。また，衛星通信を利用する場合もありうる。

通信の途絶防止対策

(13)　応急復旧対策
ア　重要な伝送路設備には､応急復旧用ケーブルの配備等の応急復旧対策を講ずること。

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。

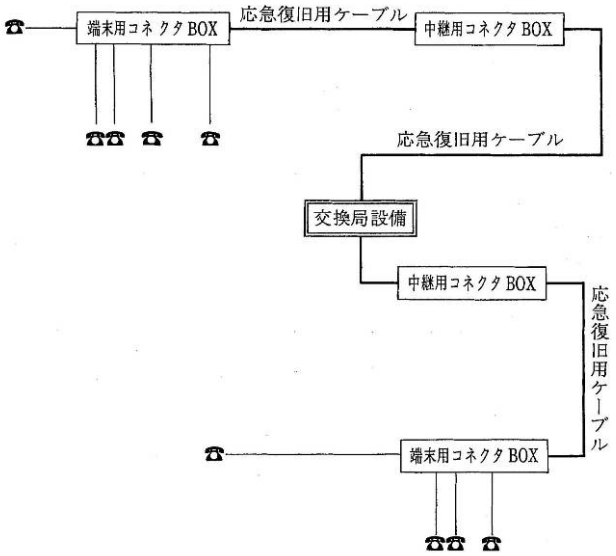
●措置例●

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、復旧範囲を余裕を持って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。)

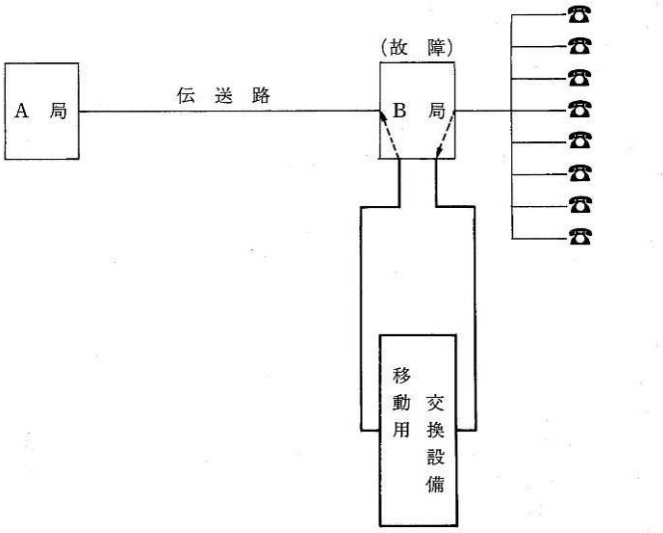


応急復旧対策（応急復旧ケーブルの配備）

イ　移動用交換設備の配備等の応急復旧対策を講ずること。

解説

交換設備の全面的な損壊等の大規模災害に対処するため、移動用交換設備を配備する等、交換設備の障害時に交換機能の確保を行う。



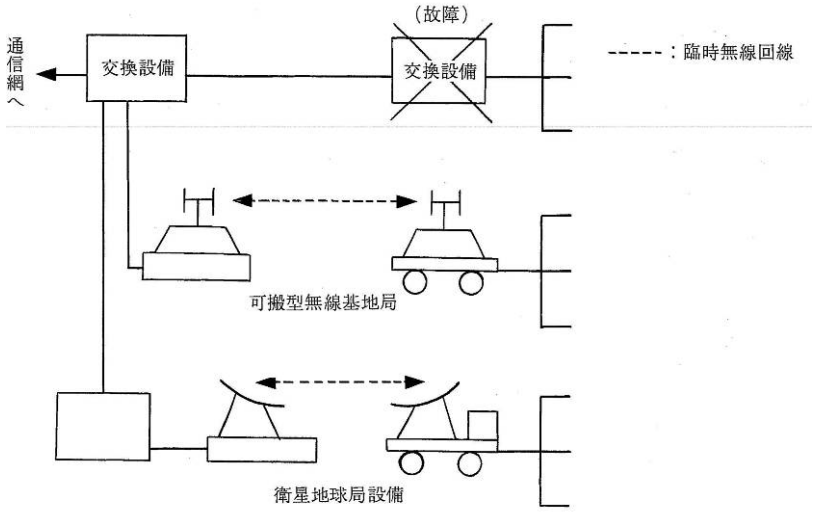
（注）伝送路も被災している場合は，可搬形無線装置等と組み合わせて使用する。

応急復旧対策（移動用交換設備の配備）

ウ　災害時等において、衛星地球局等の無線設備により、臨時電話等の設置が可能であること。

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。

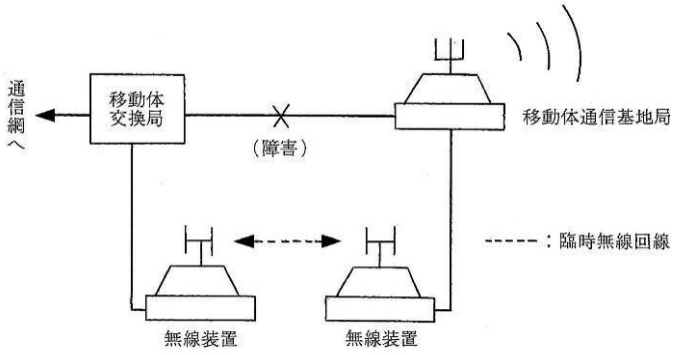


臨時の電気通信回線の設定

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

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。

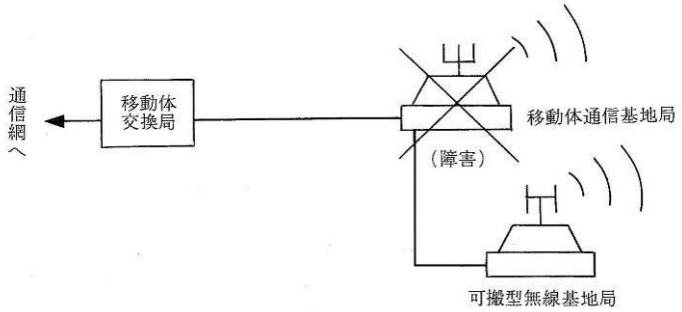


臨時対向回線の設定

オ　移動体通信基地局に障害が発生した場合等に、可搬型無線基地局により、臨時の電気通信回線の設定が可能であること。

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

カ　他の伝送設備の障害時に、通信の疎通が著しく困難となった場合、予備の設備等により臨時の電気通信回線の設定が可能であること。

解説

自然災害等が発生すると、見舞い呼等により定常時よりトラヒックも増加する傾向にあり、迂回ルートのトラヒックも増加することになる。こうした場合、既存の伝送路設備の予備パネルや予備のケーブル心線を利用して回線を増設することにより、通信の疎通の向上を図ることができる場合がある。

このため、迂回ルートでの回線増設等の二次対策を行うため、予備装置、予備パネルの手配を行う。

(14)　緊急通報の確保

緊急通報手段を提供するサービスは、メンテナンス時にもできるだけ緊急通報が利用できるよう適切な措置を講ずること。なおメンテナンス時にサービス停止時が必要な場合はユーザに通知する措置を講じること。

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。

(15)　バックアップの分散化等

予備電源設置・冗長化などの予備機器等の配備基準の明確化を図ること。

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。

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

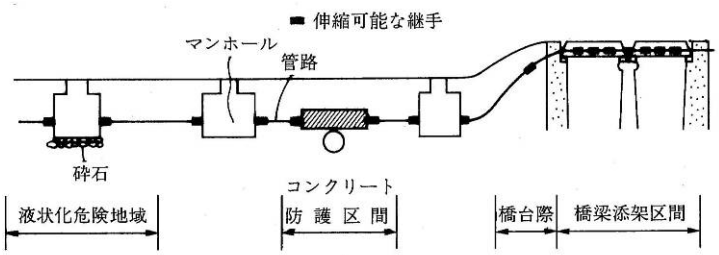
地震等による強力な振動（震度５程度）や道路、架橋等にみられる定常的な振動に対して、安定的に所定の機能を維持できるような措置を講ずる。

●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。

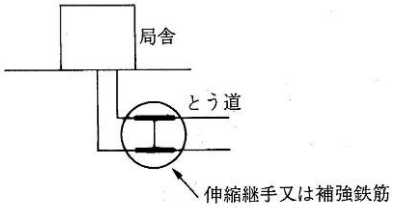
橋梁添架管路では、橋台際、橋げたの不連続箇所、所定の間隔の箇所に伸縮可能な継手を入れるなどして耐震性の向上を図る。



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する。

(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させる。

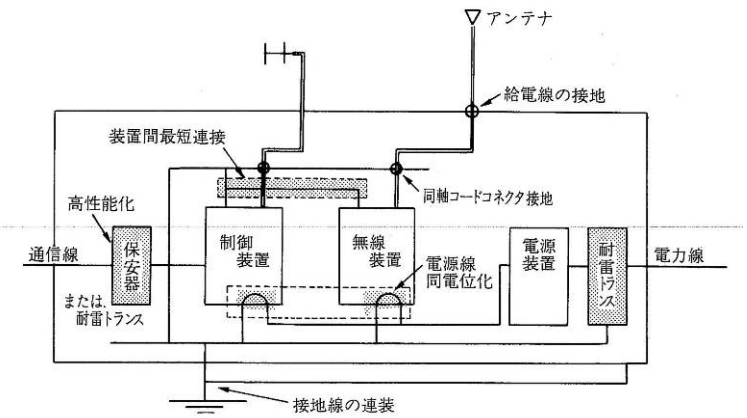
(3)アレスタ等の保護素子を挿入し、電位差を機器の耐力以下に抑圧する。

(4)装置間の接地端子を連接し、装置間の同電位化を図る。

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

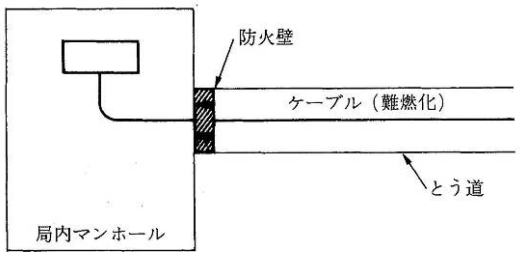
(2) シート状の耐火材料等による、ケーブルの難燃化の実施

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

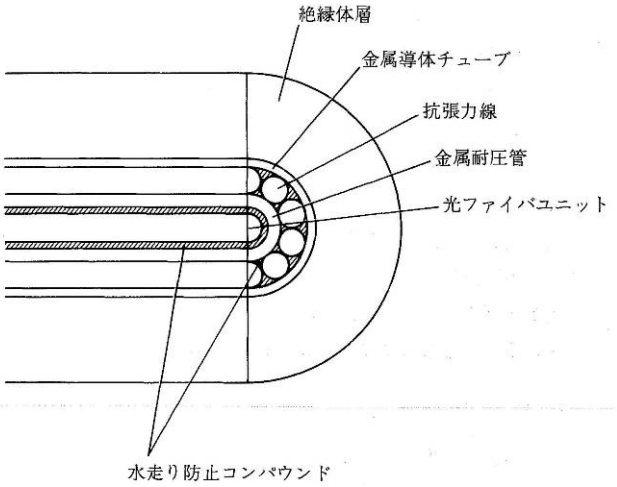
水中に設置する設備においては、設備を構成する素材及び設備構造上、耐水機能を持つようにする。

●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

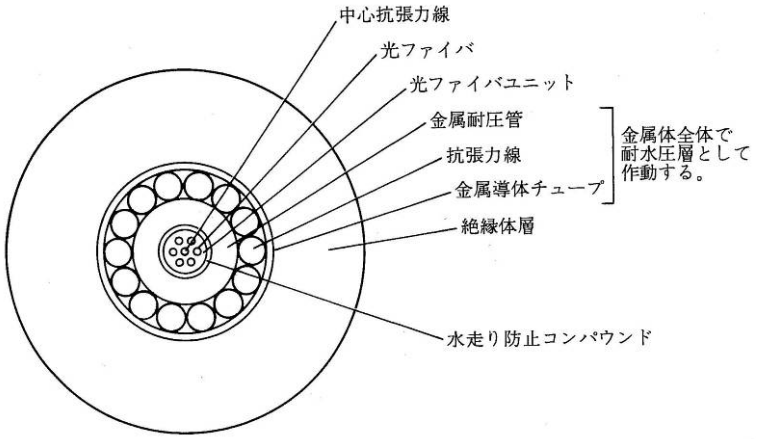
イ　水中に設置する屋外設備には、水圧による故障等の発生を防止する措置を講ずること。

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

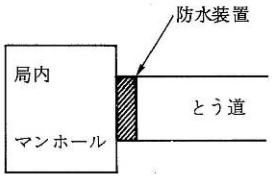
水害のおそれのある場所には、重要な屋外設備を設置しないこと。ただし、やむを得ない場合であって、防水措置等を講ずる場合は、この限りでない。

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。

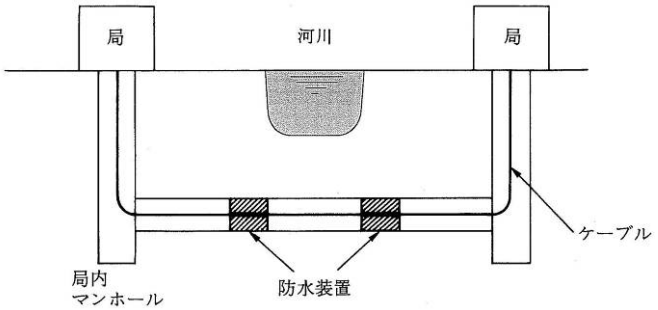
●措置例●

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。



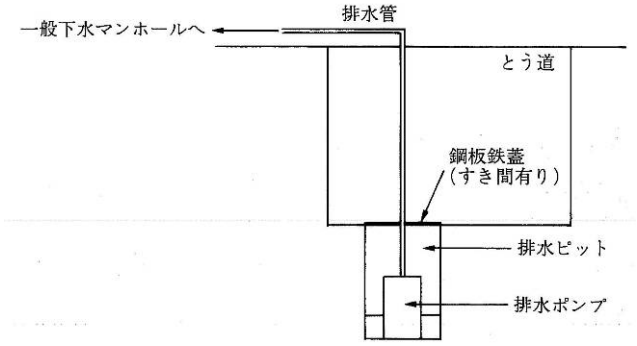
とう道の水害対策例１

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)　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。

(8)　塩害等対策

塩害、腐食性ガスによる害又は粉塵による害のおそれのある場所に設置する屋外設備には、これらによる故障等の発生を防止する措置を講ずること。

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。

(9) 高温・低温対策

ア 高温度又は低温度の場所に設置する屋外設備は、当該条件下で安定的に動作するものであること。

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

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。

(10) 高湿度対策

高湿度となるおそれのある場所に設置する屋外設備には、耐湿度措置、防錆措置等を講ずること。

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。

(11) 高信頼度

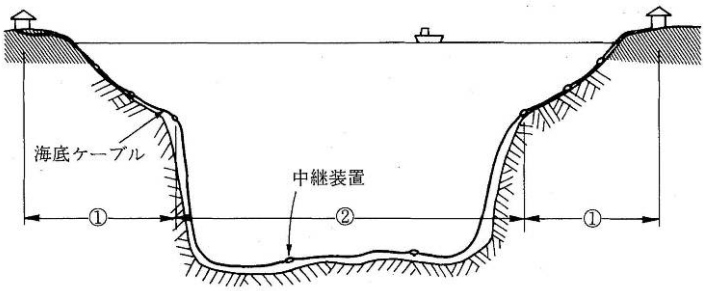
海底、宇宙空間等の特殊な場所に設置する重要な屋外設備については、高信頼度部品の使用等による高信頼度化を図ること。

解説

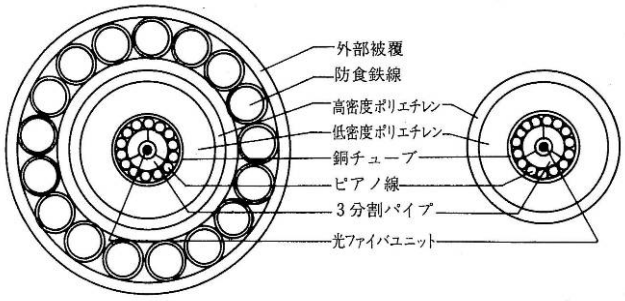
海底や宇宙空間等の特殊な場所に設置する重要な屋外設備においては、それを構成する装置の高信頼度化を図り、設備としての信頼性を確保する。

●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、電気回路の I.C 化、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。

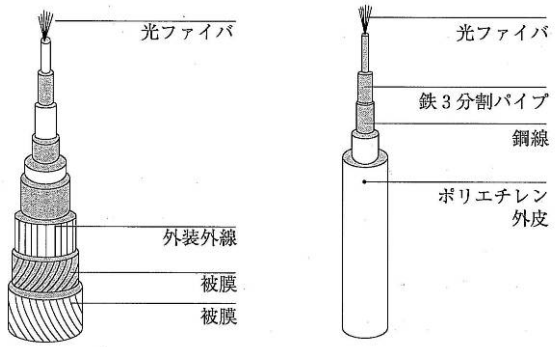


ケーブル敷設図



①の区間に使用する海底光ケーブル　　②の区間に使用する海底光ケーブル

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

(12)　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。

●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。

(13)　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、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。

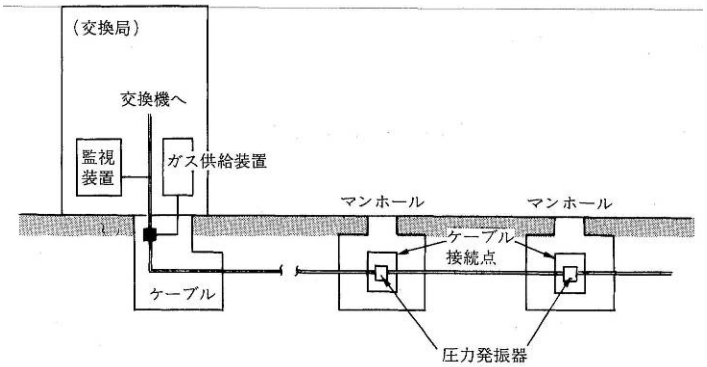
●措置例●

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測定用回線を通じてビル内に設置されている監視装置に転送し、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恐れがあるため、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。

(14) 予備機器等の配備

重要な屋外設備には、予備機器等の適切な配備又はこれに準ずる措置を講ずること。

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……使用額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　専用常備……保全・運用エリア単位で専用して使用するもの。

3　共通常備……近隣の保全・運用エリア間で共用して使用するもの。

(15) 通信ケーブルの地中化

災害時等の建物の倒壊、火災等による通信ケーブルの被災を防ぐため、通信ケーブルの地中化等を促進すること。

解説

災害時等の建物の倒壊、大規模な火災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。

(16) 発火・発煙防止

他事業者の屋外設備にコロケーションしているすべての電気通信設備について、設備を設置する事業者が発火・発煙防止等安全・信頼性確保のための所要の措置を講じること。

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。

3　屋内設備

(1)　地震対策

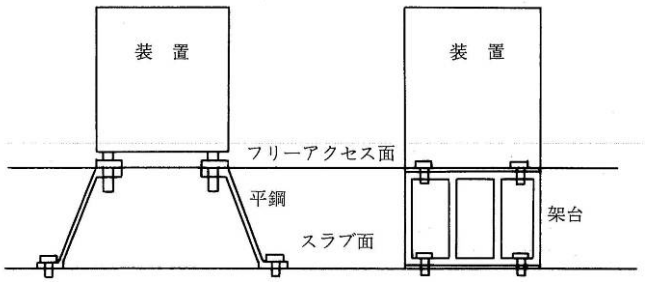
ア　通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。

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。

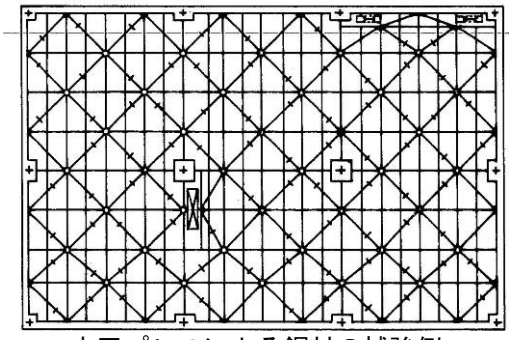
●措置例●

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。

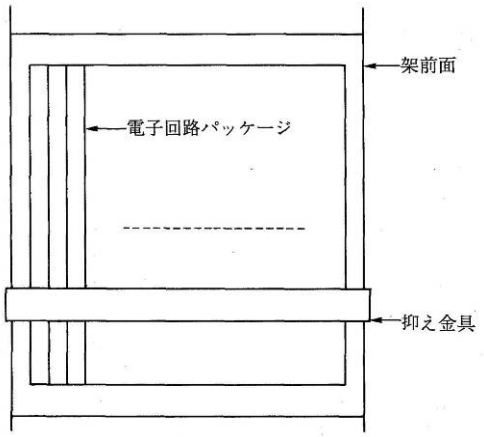
イ　通常想定される規模の地震による屋内設備の構成部品の接触不良及び脱落を防止する措置を講ずること。

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。

●措置例●

地震等により、設備の構成部品（比較的重量の大きい電子回路のパッケージ）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に重大な影響を及ぼす恐れのある電気通信設備については、発生確率は低いが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等には、冗長構成又はこれに準ずる措置を講ずること。

解説

重要な屋内設備の機器等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重化構成又は複数の現用機器に対しては１つの予備を持つｎ＋１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。

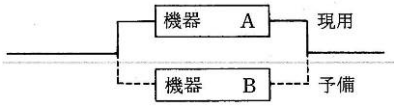
●措置例●

重要な設備では障害による処理の中段を防止するため、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。

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、大別して次の２種がある。

1　２重化方式

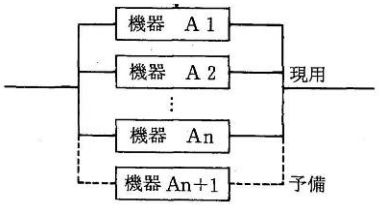
同じ機器を２組用意する方式で、一方が障害になっても、もう一方を使用して正常運転を続行できる。



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

イ　重要な屋内設備の機器等は、速やかに予備機器等への切換えができるものであること。

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）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。

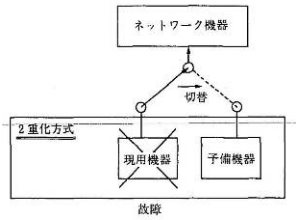
②　機器の定期試験などのために、正常運転系から被試験機器を取り外す。

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

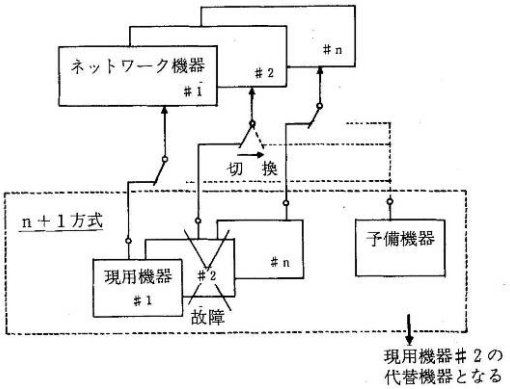
一つの現用機器に対して、現用と同一の予備機器を一つ設置し、現用機器が故障時、プログラム制御で速やかに予備機器に切り替えるとともに警報、ベル鳴動、ランプ表示、メッセージ出力により故障発生を保守者に通知する。



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）

(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、通報する機能を設けること。

解説

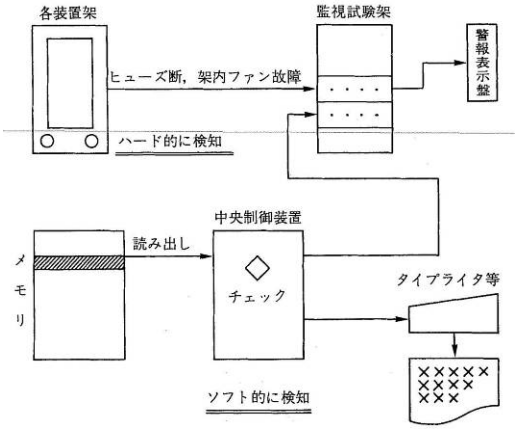
重要な設備の故障及び設備の機能障害が発生した場合、その故障等の発生を速やかに検知、通報する機能を設ける。

●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：供給電源断の検札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

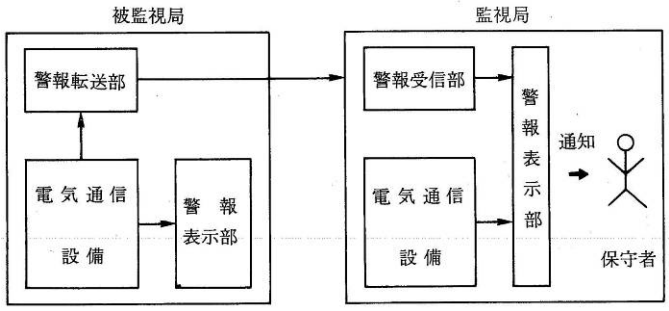
無人施設の重要な設備においては、設備の故障等を検知した場合、速やかに通報する遠隔通報機能を設ける。

「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。

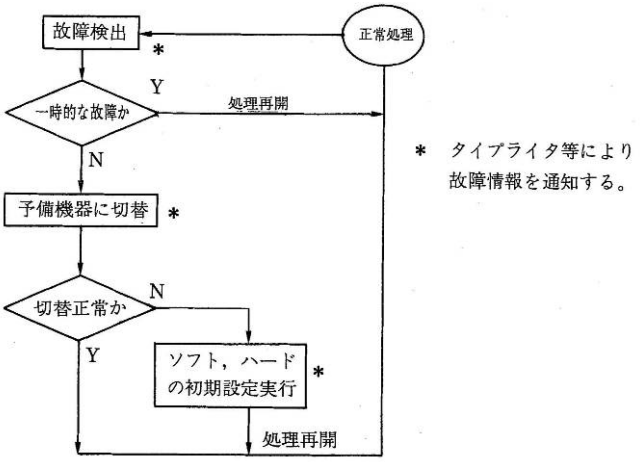
●措置例●

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。

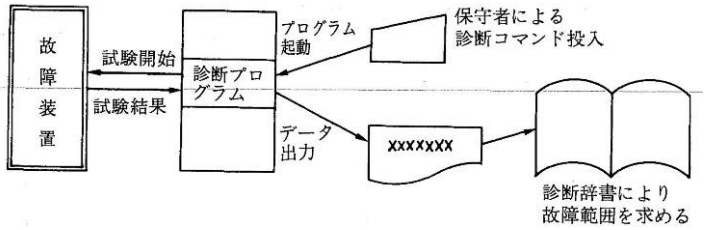
(1)　故障検出時の処理の流れ



故障検出時の処理の流れ

(2) 手動診断

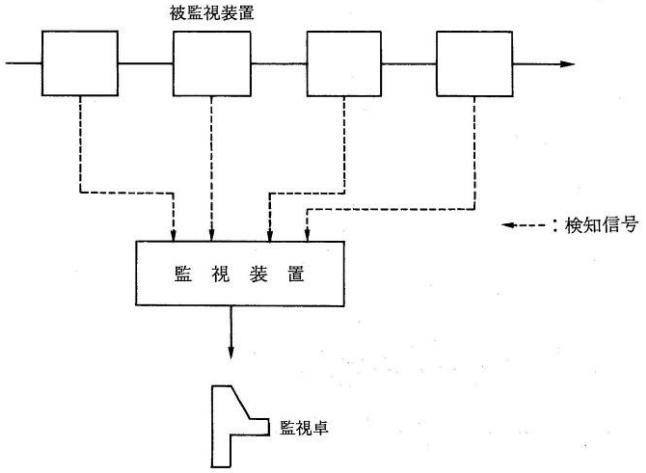
故障情報により故障装置を判定し、保守者の診断コマンド投入操作で故障装置内部の故障位置を限定する。さらに、この故障位置を限定するために診断辞書（診断コマンド投入後の出力データに基づいて故障位置を求めるためのマニュアル）を用意する。



手動式診断概念図

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、試験機器の使用額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ーは、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　集中常備……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　専用常備……各交換局所等で専用して使用するもの。

3　共用常備……各交換局所等で共用して使用するもの。

(8) コロケーション先の電気通信設備の保護

他の事業者のビルにコロケーションしているすべての電気通信設備には、安全・信頼性を確保する適切な措置を講ずること。

解説

電気通信事業法第 41 条では、電気通信回線設備を設置する電気通信事業者は、事業用電気通信設備を一定の技術基準に適合するよう維持しなければならないとしている。

これを受けて、事業用電気通信設備規則では、事業用電気通信回線設備を収容し、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所要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、移動及び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。

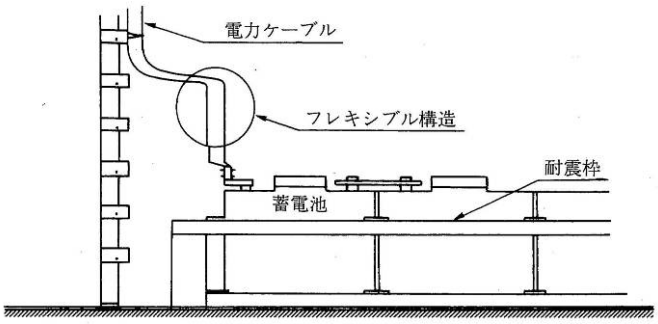
●措置例●

1　給電系統

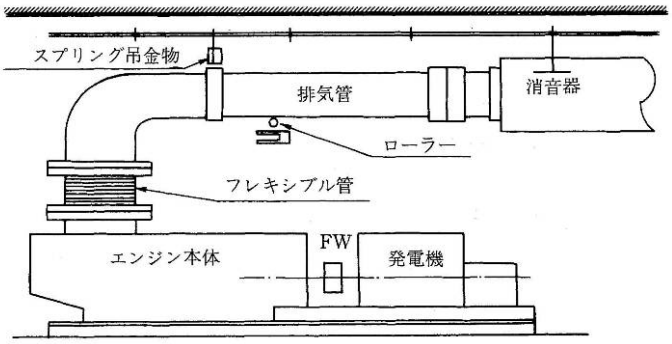
振動系の異なる装置を結ぶ給電系統は、適切な箇所で余長又はフレキシブルな構造を採用し、振動を吸収する。

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、発生確率は低いが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、難燃化又は保護装置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

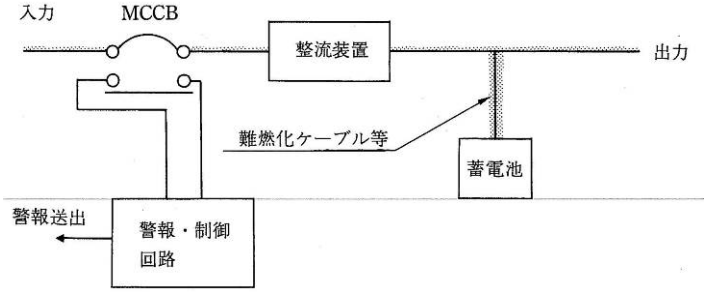
(1)商用電源の受変電設備等は、万一、発火した場合でも他の設備への延焼を防止するため、キュービクル等安全性の高い構造のものを使用する。

(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。

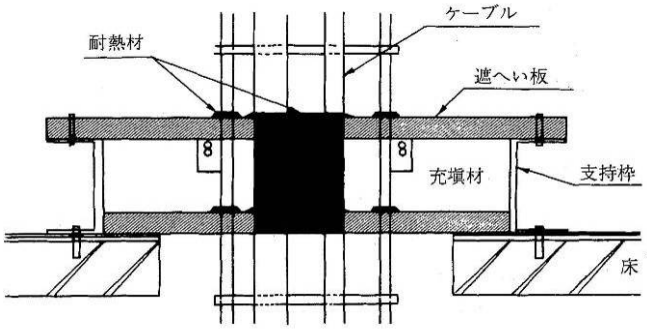
例 とう道配電設備

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。

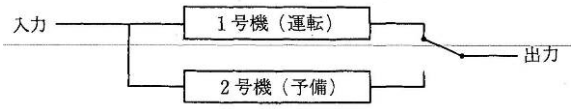
解説

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

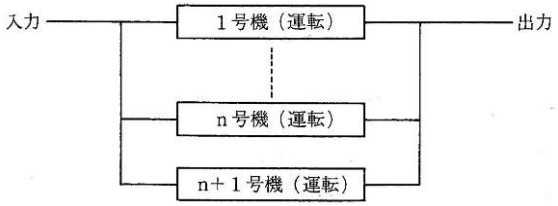
常時は現用機から負荷に電力を供給し、現用機が故障のときは、予備機に切替える方式である。



待機冗長運転方式

２　並列常用冗長運転方式

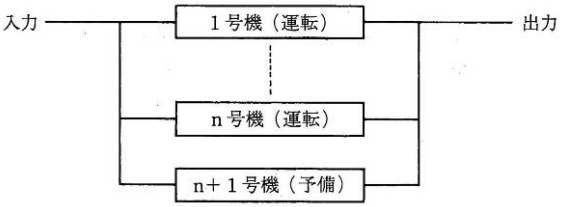
本方式は、ｎ台分の装置の容量を必要とする負荷に対し、（ｎ＋１）台で運転し、いずれか１台が故障しても電力供給を可能とする方式である。



並列常用冗長運転方式

３　待機形並列常用冗長運転方式

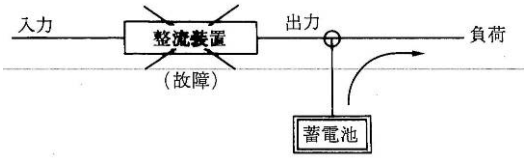
本方式は、ｎ台分の装置の容量を必要とする負荷に対し、（ｎ＋１）台分の装置構成で、常時はｎ台で運転しており、故障時には予備機が運転を開始する方式である。



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

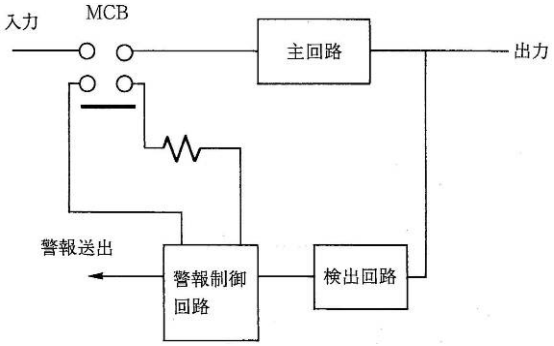
ア　電源設備の故障等、ヒューズ断又は停電の発生を速やかに検知、通報する機能を設けること。

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。

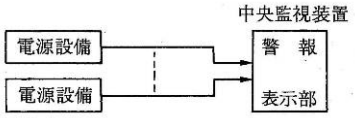
●措置例●

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。

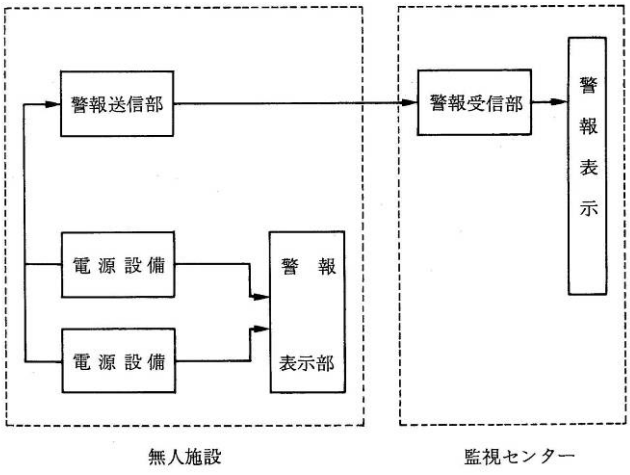
解説

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。

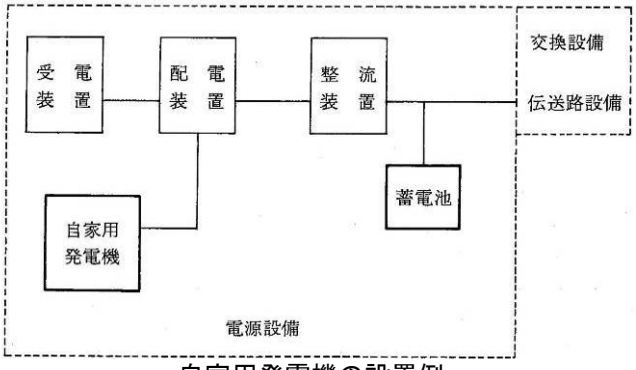
①　停電時に電源を確保するため、自家用発電機を設置する。また自家用発電機の容量は、空気調和設備等の負荷を考慮した容量とする。自家用発電機の燃料については、十分な量を備蓄しておくか、補給手段を明確にしておく。

●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。



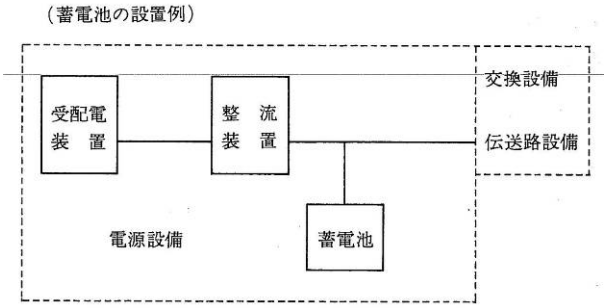
自家用発電機の設置例

② 停電時に電源を確保するため、蓄電池を設置する。また自家用発電機での給電又は異系列電源からの受電が可能となるまでの間、電源を確保する。

●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、蓄電池の設置及び、自家用発電機の設置又はこれに準ずる措置を講ずること。
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　移動体通信基地局の広域・長時間の停電対策として、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。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を備蓄し、又はその供給体制を予め確保する。

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。

第２　環境基準

１　センターの建築物

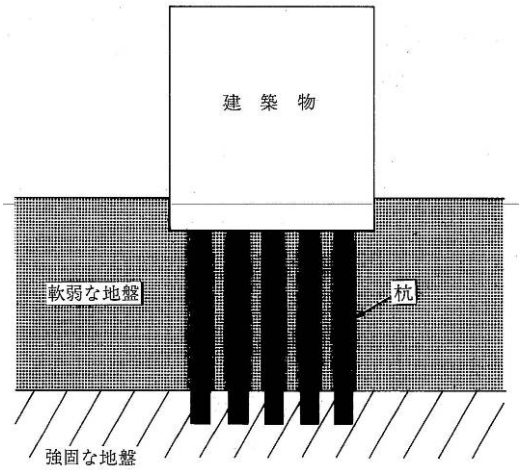
(1)　立地条件及び周囲環境への配慮
ア　強固な地盤上の建築物を選定すること。ただし、やむを得ない場合であって、不同沈下を防止する措置を講ずる場合は、この限りでない。

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

イ　風水害等を受けにくい環境の建築物を選定すること。ただし、やむを得ない場合であって、防風、防水等の措置を講ずる場合は、この限りでない。

解説

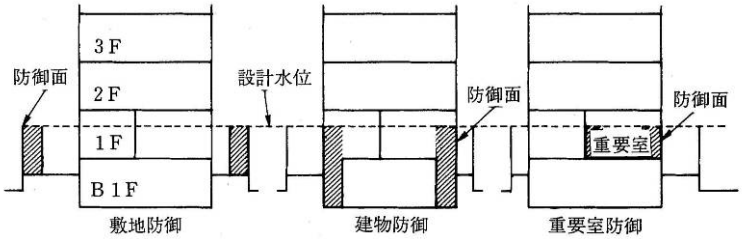
風水害等の被害を受けにくい場所を選定する。やむを得ず当該地区に建築物を設置又は既存建築物を利用する場合は防風措置や防水措置を講じる。

●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。

ウ　強力な電磁界による障害のおそれのない環境の建築物を選定すること。ただし、やむを得ない場合であって、通信機械室等に電磁シールド等の措置を講ずる場合は、この限りでない。

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。

エ　爆発や火災のおそれのある危険物を収容する施設に隣接した建築物は回避すること。

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●

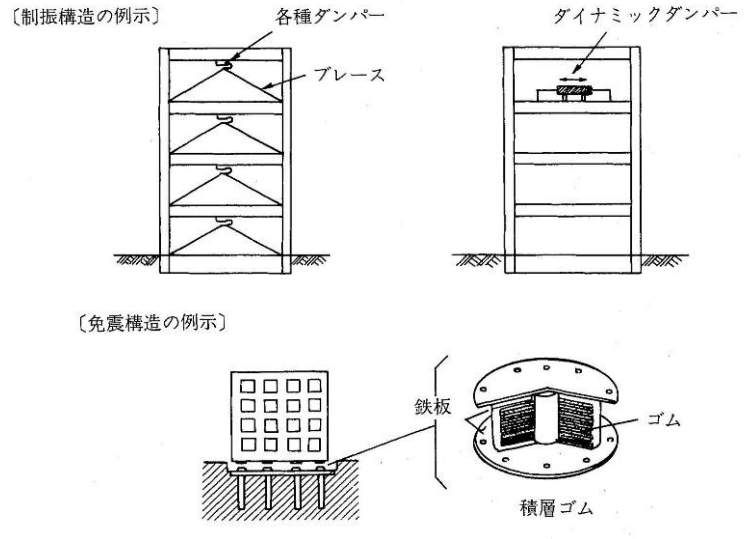
1　耐震構造

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なように設計する。

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、フ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。

・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。

・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、みだりに事業用電気通信回線設備を操作して、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

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 10 条～第 19 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し、第三者が容易に侵入できないようにすること等をいう。

●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って、床のかさ上げ、防水壁等の措置を講ずる場合又は排水設備を設置する場合は、この限りでない。

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、土壌、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って、電磁シールド等の措置を講ずる場合は、この限りでない。

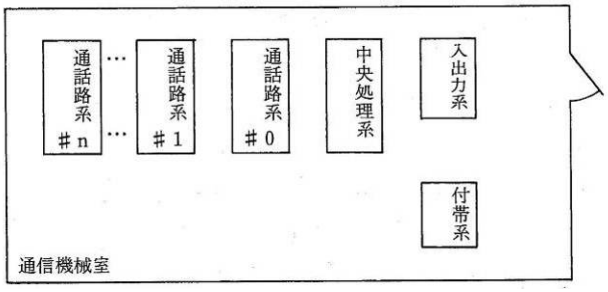
解説

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　保守作業が安全かつ円滑に行え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。

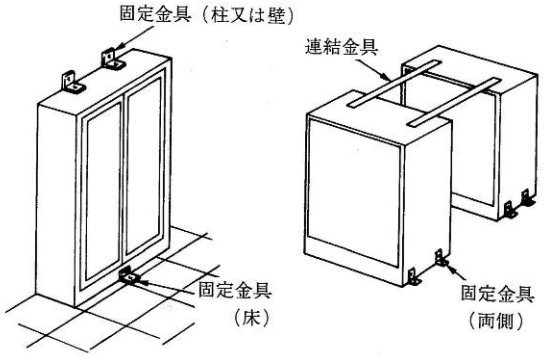
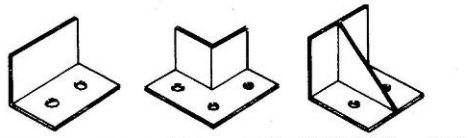


図　じゅう器類の転倒，移動防止装置



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科を使用する。

●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

出入口には、施錠機能を設ける。

（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

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。

（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

電気通信設備を保守・維持・運用する者以外の者が、みだりに事業用電気通信回線設備を操作して、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を保つべき適切な基準を設定し、運用することが必要である。

(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。

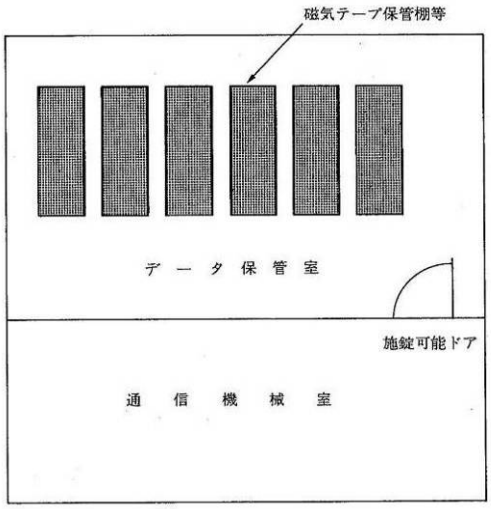
２　出入口の扉は十分な強度を持たせ、施錠機能を備える。

３　出入口は１か所とし、前室を設ける。

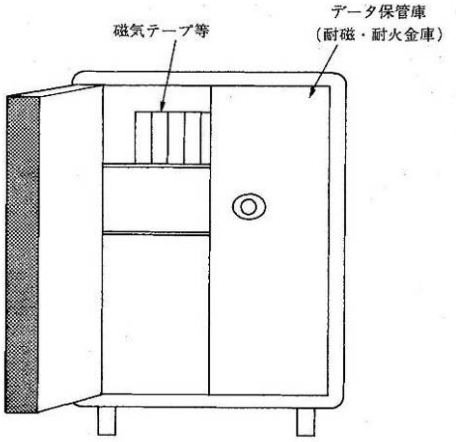
４　耐磁気措置を必要とする場合は、耐磁気保管庫を設置する。

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、火災発生時に水損の被害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、７、10～24条

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。

なお、空気調和設備の項に関する以下の規定は、空気調和設備を設置する必要がない場合は該当しない。

ウ　通常想定される規模の地震による転倒又は移動を防止する措置を講ずること。

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。

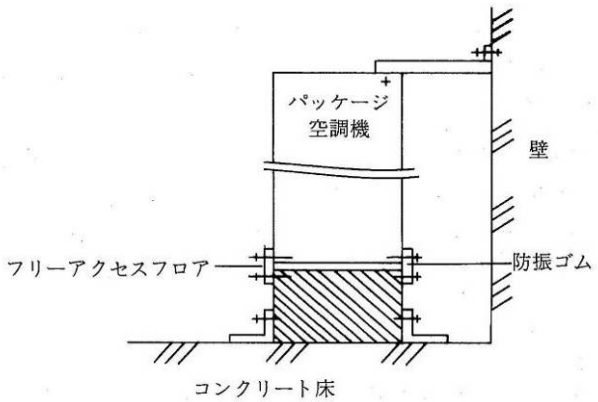
(2)冷却塔の支柱は、十分な強度を有する。

(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室内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。これらにより室内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は寒冷地の場合、冬季に循環するが、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

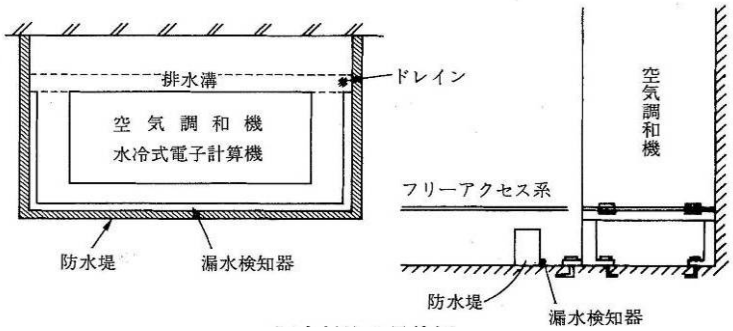
排水口等の漏水を防止する措置を講ずること。

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、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。

管理基準の対策項目
（解説）

1　ネットワーク設計管理

(1)　体制の明確化
意思決定、作業の分担、責任の範囲等の設計管理体制を明確にすること。

解説

システム設計のために、意志決定、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。

●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。

(2)　設計指針の明確化等
ア　情報通信ネットワークの基本的機能を明確にすること。
イ　将来の規模の拡大、トラヒック増加及び機能の拡充を考慮した設計とすること。

解説

運用時の作業の容易さや事業者間の連携等も考慮しながら、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、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。

(3) 設計工程の明確化等
設計工程を明確にするとともに、工程間の調整を行うこと。

解説

設計工程を明確にし、工程間の調整を十分に行う。

●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

(4) 相互接続への対応
ア 相互接続を考慮した設計とすること。
イ 相互接続を行う場合は、接続先との間で設計工程を明確にするとともに、工程間の調整を行うこと。

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●

・接続形態
・番号方式
・信号方式
・接続シーケンス
・課金方式
・試験方式
・認証方式
・IPルーティング
・QOS等品質条件
・IPパケットデータコーディング等各種パラメーター情報等

(5)　品質・機能検査の充実化

ア　サーバ等機器導入前の機能確認を十分に実施すること。

イ　ベンダーから提供されるシステムについての検査手法、品質評価手法を事前確認すること。

ウ　セキュリティ対策の手法の事前確認を十分行うこと。

エ　ネットワークふくそうを回避するため、災害時におけるユーザの振舞いや端末の挙動がネットワークに与える影響を事前確認すること。

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。

２　ネットワーク施工管理

(1)　体制の明確化
作業の分担、責任の範囲等の施工管理体制を明確にすること。

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。

●例●

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。

また、事故は、設備、環境などが整備されていなかったり、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。

(2)　作業工程の明確化等
作業工程を明確にするとともに、その管理を行うこと。

解説

作業方法及び日程等の工程を明確にするとともにその管理を行う。

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、安全に作業を行うべく手順書の作成を行うことや、工事による不具合が発生した時のリカバリー手順を用意することが必要であり、安全且つ容易な設備増設、拡張性確保の手法を確立することが必要である。

●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。

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。

工事ミス時のリカバリー手順を作成する。

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。

(3) 相互接続への対応

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

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

(4) 委託工事管理

ア 工事を委託する場合は、委託契約により工事及び責任の範囲を明確にすること。

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、甲乙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
- 情報管理規定の策定
- 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）

イ　工事を委託する場合は、作業手順を明確にするとともに、監督を行うこと。

解説

委託工事においては、その作業手順を明確にし、所要の監督を行う。

委託工事の施工に先立って、必ず乙から「施工計画書」又は「工程表」の提出を求めるよう契約に際し注意すると共に、「施工計画書」又は「工程表」の内容について甲乙間で十分討議し、設備障害及び作業者の安全確保に務める。

また､工事実施者とネットワーク運用者による工事実施体制や工事手順の確認を行う。

●例●

1　施工計画書に記載される内容

(1)設備品質確保のため特に必要な事項

(2)安全確保及び設備事故防止のため特に必要な事項

(3)工程管理のため特に必要な事項

(4)地域及び第三者に対する配慮が必要な事項

(5)問題発生時のリカバリー等対応に必要な事項

2　施工計画書による工事実施状況の確認

工事が施工計画書に基づいて行われていることの確認を監督者等が行う。監督に当たっては、遵守状況のチェック・監査体制を確保する。また、工事委託先からの安全性の観点での要望・意見を計画や製品に反映する。

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定の策定等、委託先の取組を明確化する。

(5)　検収試験管理

検収試験においては、実データを使用しないこと。ただし、やむを得ない場合であって、通信の秘密の保護及びデータの保護に十分に配慮する場合は、この限りでない。

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、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。

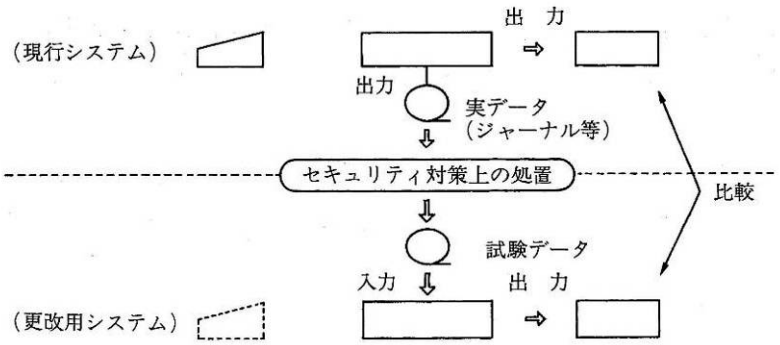
●例●

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

3　ネットワーク保全・運用

(1)　体制の明確化
作業の分担、連絡体系、責任の範囲等の保全・運用管理体制を明確にすること。

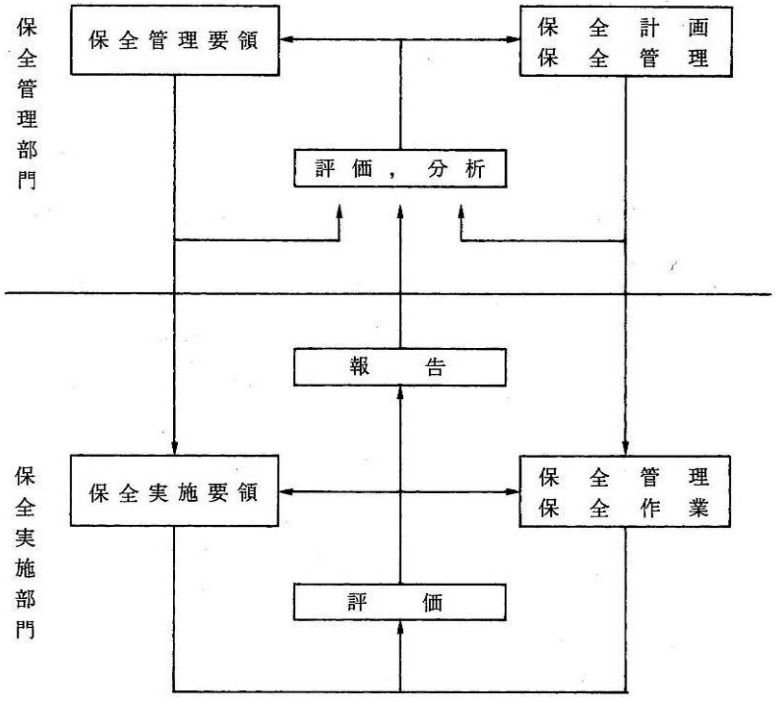
解説

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。

●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

●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

●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。

(2)　基準の設定

保全・運用基準を設定するとともに、保全・運用に関する各種データの集計管理を行うこと。

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務める。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。

●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

●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、ルータに代表される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。

(3)　作業の手順化
保全・運用作業の手順化を行い、保守点検の手順書の作成を行うこと。

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。

●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、障害発生時の対応や定期試験等の保全作業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
　システム構成や処理能力及び基本仕様等

２　システムの運転管理
　定期的な運転管理機能の概要と実施方法及びその手順等

３　定期試験・点検
　定期試験・点検の概要と実施方法及びその手順等

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、対応措置の概要と実施方法及びその手順等

５　その他
　保全作業を実施する上で必要な機能とその実施方法及びその手順等

●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、代替復旧続制局、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~~変換~~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。

(4) 監視、保守及び制御

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

イ 情報通信ネットワークの動作状況を監視し、必要に応じ、接続規制等の制御措置を講ずること。

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。

ア 設備の動作状況を監視し、故障等を検出した場合、必要に応じて予備設備への切替え又は故障設備の修理を行う。

●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。

●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 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。

●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、羅障箇所及びメディアを即座に発見する。

●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。

●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、網管理センタを設け、ネットワークの運用保守に係る事業所を続括する。

(5)　相互接続への対応

ア　相互接続を行う場合は、作業の分担、連絡体系、責任の範囲等の保全・運用体制を明確にし、非常時等の事業者間の連携・連絡体制の整備を行うこと。

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。

●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。

イ　移動体通信において国際間のローミングサービスを行う場合は、外国の電気通信事業者との間の作業の分担、連絡体系、責任の範囲等の保全・運用体制を明確にすること。

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。

ウ　モバイルインターネット接続サービスにおいて、コンテンツ等の供給を受けるために接続を行う場合は、その条件及び保全・運用体制を明確にすること。

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。

エ　相互接続性の試験・検証方式を明確にすること。

解説

IP 網における相互接続性を十分に確保するための試験・検証を行う。

●例●

既存の電話交換網レベルのように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。

(6)　委託保守運用管理

ア　保守の委託を行う場合、契約書により保守作業の範囲及び責任の範囲を明確にすること。

●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
・金額
・情報セキュリティの確保
・障害時の対応、及び報告

イ　保守を委託する場合は、作業手順を明確にするとともに、監督を行うこと。

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。

●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。

ウ　故障、障害等における迅速な原因分析のための事業者とベンダや業務委託先との連携体制を確立すること。

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。

●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。

エ　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。

(7) 保守試験管理

保守試験においては、実データを使用しないこと。ただし、やむを得ない場合であって、通信の秘密の保護及びデータの保護に十分に配意する場合は、この限りでない。

解説

保守作業後の検収試験において、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。

(8) 情報の収集

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

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●

- 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
- 道路管理者、警察からの入手
- 道路パトロールからの入手
- CEPTOAR-Councilからの入手の検討

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。

なお、通信ケーブル埋設箇所での工事においては、試掘、危険工程の停止の依頼、掘削工事への注意喚起、工事立ち会い等により、障害の回避を図る。

(9) ふくそう対策

ア 情報通信ネットワークのふくそうを防止し、有効活用を図るため、必要に応じて利用者への協力依頼・周知のための措置を講ずること。

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。

●例●

地震、豪雨、台風等の災害時に一般の利用者の見舞い呼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

イ 災害時等において著しいふくそうが発生し、又はふくそうが発生するおそれがある場合に、情報通信ネットワークの有効活用を図るため、相互接続する事業者が協調して通信規制等の措置を講ずるとともに、ふくそうの波及防止手順の整備及び長期的視点の対策に取り組むこと。

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､緊急通話等重要通信の確保など情報通信ネットワークの有効活用を図るため、相互接続する事業者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、ＩＰ電話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。

●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

4　設備の更改、移転管理

(1)　体制の明確化
作業の分担、連絡体系、責任の範囲等の管理体制を明確にすること。
(2)　作業工程の明確化等
作業工程を明確にするとともに、その管理を行うこと。

解説

(1)　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。

(2)　作業の方法及び工程を明確にし、その管理を行う。

●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)センタ移転先の選定
(3)新センタの設備
(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
- 新センタの運用方式
- 新センタでの運用訓練計画

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

旧センタから新センタ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

新センタが安定して稼働していることを確認した後、旧センタ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。

５　情報セキュリティ管理

(1)　情報セキュリティポリシーの策定
情報セキュリティポリシーを策定し、適宜見直しを行うこと。

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)　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。

●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。

●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

●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。

●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。

(3) 情報セキュリティ監査の実施

監査のチェック項目の策定と定期的な内部･外部セキュリティ監査を実施し、その結果を踏まえ情報セキュリティ対策全体の見直しを行うこと。

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。

●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。

●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。

(4) コンピュータウイルス情報緊急通報体制の整備

ア 新たなコンピュータウイルスを発見した場合等、コンピュータウイルスに関する情報を広く一般に周知する必要があるときは、電気通信業界で定めた緊急連絡先に、直ちに連絡すること。

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。

イ コンピュータウイルスに関する情報を入手したときは、自社内に対して速やかに周知するとともに、利用者に対してウェブへの掲示、メールニュース等適切な方法により速やかに情報提供する等、被害の拡大を防止するための措置を講ずること。

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。

(5) 情報セキュリティに関する情報収集

最新の情報セキュリティに関する技術情報や業界動向を入手し､それらを情報セキュリティ対策に反映させること。

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。

(6)　知識・技能を有する者の配置

情報セキュリティに関する資格の保有者等一定以上の知識・技能を有する者を配置すること。

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。

(7)　情報セキュリティに関する利用者への周知

情報通信ネットワークに対して利用者が与える又は情報通信ネットワークの利用者が受ける可能性のある影響とその対策について利用者に周知すること。

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。

(8) 社内の重要情報の管理

ア　ネットワーク内の装置類やサービスの属性に応じた情報を分類すること。

イ　情報管理に関する内部統制ルールを整備すること。

解説

取扱規定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　コンピュータウイルス等による情報漏えい対策●

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。

(9) サイバー攻撃に備えた管理体制
サイバー攻撃発生時の迅速な情報共有方法を確立すること。

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。

●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

６　データ管理

(1)　体制の明確化
作業の分担、連絡体系、責任の範囲等のデータ管理体制を明確にすること。

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。

●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

(2) 基準の設定
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。

●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。

・対象データの指定方法
・データ取扱いの優先度、重要度の分類方法
・分類された重要度による取扱い方法
・データの保管方法
・データ運用・管理の記録方法
・データの正確性、正当性、妥当性の確認方法
・データ移転時の処理方法
・パスワード等の管理方法
・データ管理の責任者の責務
・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

(3) 作業の手順化
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い手順書を作成し、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。

(4)　データの記録物の管理

ア　設備の仕様及び設置場所等のデータ並びに利用者に関するデータの記録物については、重要度による分類及び管理を行うこと。

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。

●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。

●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。

イ　設備の仕様及び設置場所等のデータ並びに利用者に関するデータに対する従事者の守秘義務の範囲を明確にするとともに、その周知、徹底を図ること。

ウ　利用者の暗証番号等の秘密の保護に配慮すること。

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。

●例●

1　社会における範囲

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積極的に漏らすことはもちろん、窃用した第三者の照会に回答してはならない。

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間接的に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。また、
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間接的に大きな響をえるもの	管理責任者の元に管理され、業務遂行上必要と認められる場合は、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

エ　記録媒体の性能向上やシステム間の接続の拡充などによるリスク・脅威の拡大に応じた適時の点検・見直しを行うこと。

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。

(5)　ファイル等の遠隔地保管

重要なプログラム、システムデータ及び利用者に関するデータのファイル等については、前世代及び現世代のものを地域的に十分隔たった場所に別に保管すること。

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。

●例●

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。

(6) 重要データの漏えい防止対策

個人情報以外の重要な設備情報（特に他社のセキュリティ情報等）の漏えいを防止するための適切な措置を講ずること。

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。

7　環境管理

(1)　建築物の保全
保全点検を定期的に行うこと。

解説

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。）

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被り、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。

●例●

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。

(2)　空気調和設備の保全
保全点検を定期的に行うこと。

解説

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。）

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。

●例●

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。

8　防犯管理

(1)　体制の明確化
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、その手投、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。

(2)　管理の手順化
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。

(3)　建築物、通信機械室等の入出管理
建築物、通信機械室等の入出管理を行うこと。

解説

監視装置や受付等により入出管理を行う。

●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。

(4) かぎ、暗証番号等の管理
出入口のかぎ及び暗証番号等の適切な管理を行うこと。

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、現状の把捉を行い適切に管理する。

●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。

(5) 防犯装置の管理
防犯装置の保全点検を定期的に行うこと。

解説

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。

●例●

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定を明確にし、遵守状況を管理する。

(6) 入出管理記録の保管
入出管理記録は、一定の期間保管すること。

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。

●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。

９　非常事態への対応

(1)　体制の明確化
ア　連絡体系、権限の範囲等の非常事態時の体制を明確にすること。

解説

大規模な災害や重大事故等、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。

●例●

次のような内容を含んだ災害対策規定を作成し、組織・体制を予め定めておく。

1　災害予防と事前措置
2　災害応急対策
(1)災害情報
(2)準備警戒
(3)通信設備に対する応急措置
(4)通信疎通に対する応急措置
(5)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　非常事態時における社員・職員、復旧に必要な業務依託先などへの連絡手段、社員・職員の参集手段の確保等の体制を整えること。
ウ　非常事態時における広域応援体制を明確にすること。
エ　相互接続を行う事業者等の間において、非常災害時の連絡体制や連絡内容を明確にすること。
オ　非常事態時における応急活動、復旧活動に際しては国等の関係機関との連絡体制を明確にすること。
カ　非常事態時において、応急活動、復旧活動にかかわる連絡手段を確保するために必要な措置を講ずること。

解説

イ　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、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。

エ　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。

●例●

・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）
・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
・緊急通信や重要通信確保、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
・疎通状況の共有・公開などによる障害の影響拡大防止

オ　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。

・災害時優先電話の設置
・携帯電話・PHS、パソコン通信など多様な通信手段の整備
・被災地への着信を極力さける連絡方法（運用ルール）の確立など

(2)　復旧対策の手順化
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、ネットワークの縮退計画等について、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。

●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

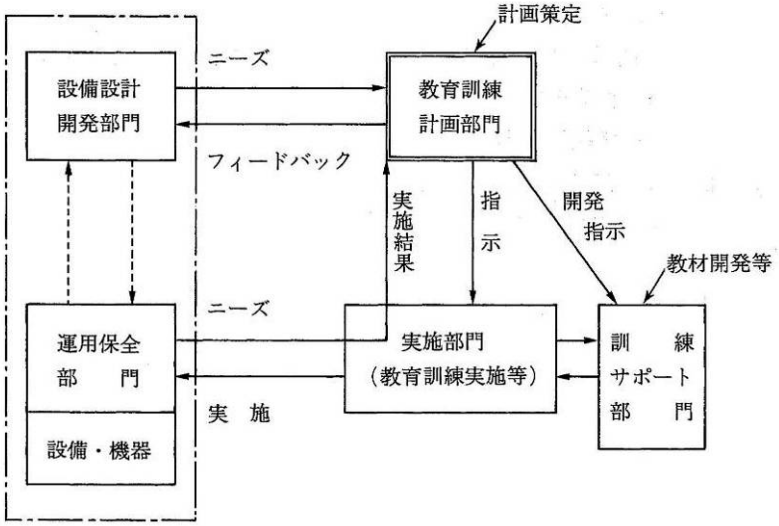
10　教育・訓練

(1)　体制の明確化
教育・訓練に関する計画の策定及び実施を行う体制を明確にすること。

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。

●例●



教育・訓練体制の例

(2)　教育・訓練の内容
ア　教育・訓練の目的を明確にするとともに、終了後の実施効果により計画の修正を行うこと。

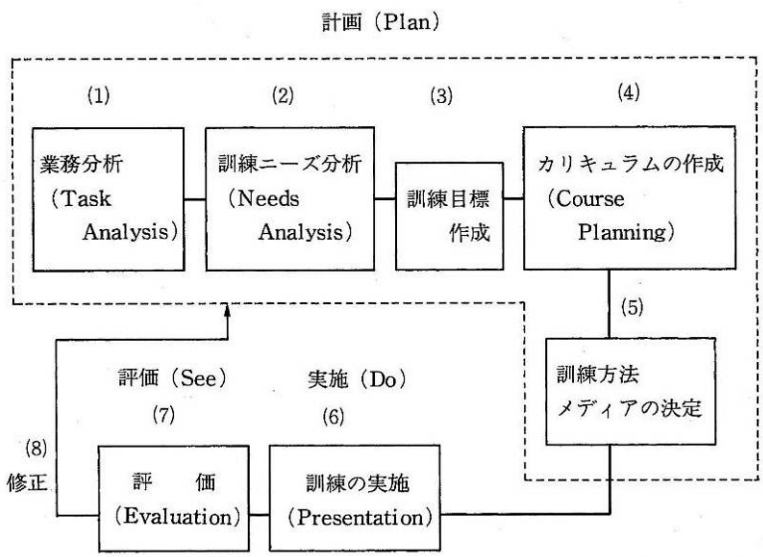
解説

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。

●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。

イ　情報通信ネットワークの円滑な運用に必要な知識及び判断能力を養うための教育・訓練を行うこと。

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。

●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、伝統的な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。

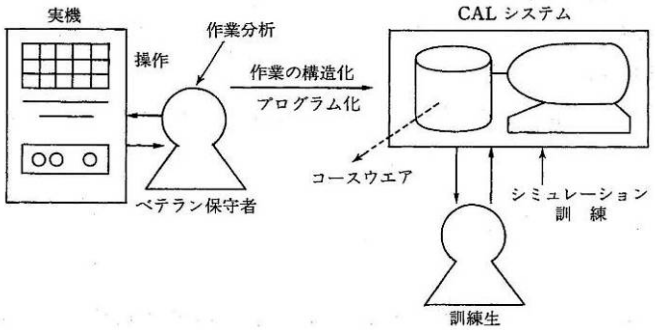
３　CAL（Computer Assisted Leaning）システムによる模擬演習訓練

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

ウ　データ投入等における信頼性の高い作業能力を養うための教育・訓練を行うこと。

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。

●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（0JT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

エ　設備の保全に関する知識を養うための教育・訓練を行うこと。

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。

●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0JTの実施がある。

オ　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。

●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。

カ　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。

●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　0JT

このうち、0JT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0JTによる方法は特に有効である。

なお、0JT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、0JTの前提として１および２による訓練が必要である。

キ　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。

●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。

11　現状の調査・分析及び改善

(1)　体制の明確化
情報通信ネットワークの維持及び運用に関して、現状の調査・分析を行う体制を明確にすること。

解説

情報通信ネットワークの維持及び連用に関して、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。

●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な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。

(2)　基準の設定
情報通信ネットワークの維持及び運用に関して、現状の調査・分析を行う項目、評価方法等の基準を設定すること。

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。

●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。

(3)　作業の手順化
情報通信ネットワークの維持及び運用に関して、現状の調査・分析作業の手順化を行うこと。

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。

(4)　改善

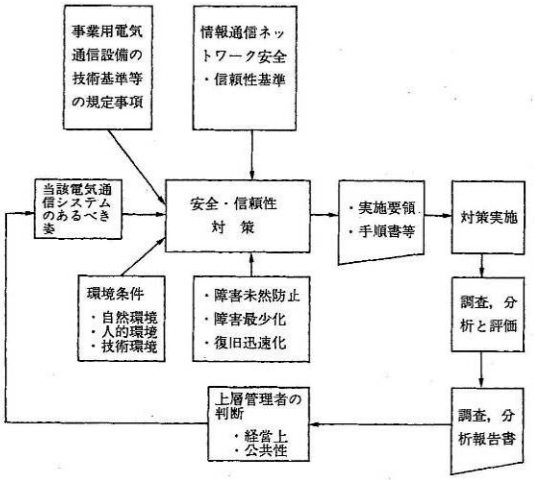
ア　情報通信ネットワークの維持及び運用に関して、現状の調査・分析結果を、必要に応じ、情報通信ネットワークの維持及び運用体制並びに手順書に反映させること。

解説

調査・分析結果に基づき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。

●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

イ　情報通信ネットワークの維持及び運用に関して、現状の調査・分析結果を、必要に応じ、教育・訓練計画に反映させること。

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

12　安全・信頼性の確保等の情報公開

(1)　情報通信ネットワークの安全・信頼性の確保に係る取組状況
情報通信ネットワークの安全・信頼性の確保の取組状況を適切な方法により利用者に対して公開すること。

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　緊急通信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

(2)　情報通信ネットワークの事故・障害の状況
情報通信ネットワークの事故・障害の状況を適切な方法により利用者に対して公開すること。

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、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があるため、メールを併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。

(3)　サービス提供不可に陥るケース等の周知
情報通信ネットワークにおいて、従来サービスとの違いを広く利用者に周知すること。

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。

●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。

別添５

情報セキュリティポリシー策定のための指針

1　目的

この指針は、情報通信ネットワークの健全な発展に寄与することを目的とし、適正なリスク管理を実現させるための基本となる情報セキュリティポリシー策定のための指針として定めたものである。

2　情報セキュリティの管理

情報セキュリティを適切に管理していくためには、情報セキュリティの「方針立案」、「対策実施」、「運用・監視」及び「監査・診断」の各段階において、以下の対策を行う必要がある。

⑴　方針立案

ア　情報セキュリティポリシー及び実施手順の策定

情報セキュリティを適正に管理していくために、組織における情報セキュリティ対策に関する統一方針として情報セキュリティポリシーを策定する。

また、情報セキュリティポリシーに基づき、実際の業務・作業レベルまで考慮した情報セキュリティ実施手順を策定する。

イ　情報セキュリティ組織体制の整備

情報セキュリティに関して、責任所在の明確化やセキュリティ情報の共有化を行うために、情報セキュリティ組織体制を整備する。

⑵　対策実施

情報セキュリティポリシーの普及・教育

情報セキュリティポリシーが適正に実施されるよう、普及・教育活動を行い、情報セキュリティに対する自覚や意識の向上を目指す。

⑶　運用・監視

ア　情報セキュリティポリシーに沿った運用

情報セキュリティポリシーを理解し、情報セキュリティポリシーに沿った運用を適正に実行する。

イ　例外の管理

業務を遂行する中で、情報セキュリティポリシーが適用できない場合が発生する可能性もある。情報セキュリティポリシーから逸脱した際に、適正に管理する仕組みを確立する。

ウ　情報セキュリティ侵害時の対応の明確化

情報セキュリティ侵害が起きた際、速やかに侵害の事実、状況を伝達できるよう伝達経路を明確化する。

⑷　監査・診断

ア　情報セキュリティ監査

情報セキュリティポリシーが組織内において正しく実行されていることを把握するため定期的に監査する。

イ　情報セキュリティポリシーの見直し

情報セキュリティ監査結果や情報セキュリティを取り巻く環境等を考慮し、情報セキュリティポリシーを定期的に見直し、改訂を行う。

3　情報セキュリティポリシーの構成等

情報セキュリティの環境は技術動向、組織状況により変化することから、次のように情報セキュリティポリシーを目的、原則及び方針の三段階に階層化させることで、下位の方針のみを見直し、時代・環境変化に対応することができる。

⑴　目的

情報セキュリティポリシーにおいて最も基本となるもので､組織としての情報セキュリティへの取組の目的を定めるものである。最高権限者の声明として記述し、組織全体で積極的に情報セキュリティに取り組むことを明確化することが望ましい。

⑵ 原則

目的に基づき､情報セキュリティを実現するための組織方針､組織理念等組織の基本的な考え方を定めるものである｡利便性とセキュリティのバランスをどのように取るかといった、情報セキュリティ全体の考え方の根幹となる。

⑶ 方針

原則に基づき、情報セキュリティを実現するための基本方針をテーマごとに具体化し定めるものである。各方針に対し、責任の所在を明確化する必要がある。

⑷ 実施手順

定められた情報セキュリティポリシーを確実に実施するため、情報セキュリティポリシーに基づき、具体的な手順や方法を実施手順として定めることが一般的である。実施手順では、情報システムが最低限備えるべき具体的セキュリティ要件や、各情報システムの利用方法等、各方針に沿い、実際の業務、手順、方法等を記述することとなる。

４ 情報セキュリティポリシーの策定

情報セキュリティポリシーは、組織として取り決めた最も重要な規程となるため、組織の幹部の関与により策定することが一般的である。

情報セキュリティポリシーの策定に当たり、各部門の業務に何らかの制約や変更を要請することがあるため、経営企画部門、総務部門といった社内規定を担当する部門が中心となり、各部門よりメンバーを召集して策定の為のチームを設立し、策定を行うことが望ましい。

なお、情報セキュリティポリシーには、情報システム部門、人事部門、監査部門等の部署の役割が非常に大きいため、これらの部門からの積極的参加を要請する。

また、外部コンサルティングサービスを提供する機関を活用し、策定に当たってのスケジュール、策定方法、記述事項等についての助言を得ることが好ましい。

情報セキュリティポリシーを策定する際の実施手順を以下に示す。

⑴ 情報セキュリティポリシー策定チームの編成

各部門よりメンバーを召集し策定のためのチームを設立する。

⑵ 「目的」及び「原則」の明確化

組織としての情報セキュリティに関する考えの根幹となる「目的」及び「原則」を定める。

⑶ 情報セキュリティポリシーの適用範囲の明確化

情報セキュリティポリシーがどの範囲まで適用されるのかを明確化する。

⑷ 情報資産の洗い出し

現在、組織が保有する情報資産とその価値を明確化する。

⑸ 情報資産を取り巻く脅威とその脅威に対するリスクの分析

保護すべき情報資産を明らかにし､脅威の発生頻度､影響度を基にリスクを分析する。

⑹ 「方針」の明確化

各情報資産を保護するために､組織としてどのような方針をもって対策を行うかを明確化する。

５ 情報セキュリティポリシーの構成例

情報セキュリティポリシーの構成例と各項目における記述内容を以下に示す。

ここでは、方針を「情報セキュリティ運営に関する方針」と「情報資産に関する方針」に大きく分け、前者では管理の各段階に応じた項目、後者では情報資産の大きな区分である「情報」、「情報システム」、そして、情報資産を保護するための「アクセス制御」という項目立てとしている。

1　総則

⑴　目的

情報セキュリティの必要性と組織としての情報セキュリティの目的を記述する。最高権限者の声明として記述することで、情報セキュリティに対して組織全体で積極的に取り組むことを表明することが望ましい。

⑵　適用範囲

人、組織、場所、情報資産、技術等の切り口で情報セキュリティポリシーが適用される範囲を明確化する。

⑶　用語及び定義

情報セキュリティポリシー内で用いる用語の意味を明確にし、読者が共通の解釈の下、理解・判断できるよう用語の定義を行う。

⑷　原則

組織としての情報セキュリティに対する考え方の根幹となる原則を明確にし記述する。すべての方針、対策等は、ここで記述される原則に準拠しなければならない。例として、法令の遵守を原則として記述した場合、この原則に準拠し各組織員の役割等を方針にて定める。

2　方針

⑴　セキュリティ運営に関する方針

ア　情報セキュリティ組織

組織内の情報資産を管理し、セキュリティを担保する仕組みを確立する。具体的には、経営陣による情報セキュリティフォーラムの設立と、情報セキュリティに関する責任者の割当てを行う。また、組織内で働く外部業者を適用範囲に含む際は、その管理方法（契約時の必須項目等）を明確化する。

イ　普及・教育

情報セキュリティに対する知識と意識を向上させ、適用範囲内すべての人が情報セキュリティポリシーを理解し、遵守するよう、情報セキュリティポリシーの普及・教育活動を行うことを記述する。

ウ　例外の管理

情報セキュリティポリシーから逸脱する事項を管理・統括する組織・方法を明確にする。費用対効果を分析した結果、情報セキュリティポリシーに準拠することが得策ではない事項等が発生した際の対処方法を明確にすることで、逸脱発見者が迅速に対応を行い、組織として逸脱事項を管理・統括する体制を整備する。

エ　情報セキュリティ侵害時の対応

適用範囲内において、情報セキュリティ侵害が発生した際の対応手順を明確化することで、発生時に迅速に対応できる体制、方法を確立する。また、情報セキュリティポリシー違反者及びその監督責任者に対する罰則についても記述する。

オ　情報セキュリティ監査

情報セキュリティポリシーが組織内において正しく実行されていることを把握するため、定期的に監査する必要がある。監査組織と監査結果を把握する者を明確化する。

カ　情報セキュリティポリシーの改訂

情報セキュリティ監査結果や情報セキュリティを取り巻く環境等を考慮し、情報セキュリティポリシーを定期的に見直し、改訂を行う。改訂手順についても明確化する。

⑵ 情報資産に関する方針

ア　情報

適用範囲内の情報についての管理方法を明確化することで、情報の漏えい、破壊、改ざん等を防止する。また、プライバシーにかかわる情報を取り扱う際に遵守すべき事項を明確化する。

⑺　情報管理

情報の漏えい、破壊、改ざん等による被害等に応じて、情報を区分する。情報の区分と情報の取得・生成、保管、流通、利用及び廃棄という各段階における情報の取扱方法を明確にし、組織員による情報の取扱方法を統一化する。

⑴　プライバシー情報

通信の秘密を含むプライバシー情報の漏えいは深刻な権利利益侵害につながるおそれが高いため、電気通信事業者に対しては、「電気通信事業における個人情報保護に関するガイドライン」（平成 16 年総務省告示第 695 号）が制定されている。

プライバシー情報の適切な利用と保護が極めて重要であるとの認識により、プライバシー情報の取扱いについては、個別の項目を設け、個人情報の収集、利用・提供、適正管理、責任の明確化等について、遵守すべき方針を明確に記述する。

イ　情報システム

適用範囲内の情報システム上にて取り扱われる電子情報の漏えい、破壊、改ざん等の防止及び情報システム停止による損害の抑止を目的とし、情報システムについての管理方法（設計、構築及び運用方法）を明確化する。

⑺　情報システム設計・構築

情報システムの設計、構築時における管理体制と、情報システムに実装すべきセキュリティ機能（アクセス制御機能、フロー制御機能、暗号化制御機能等）を明確化する。

⑴　情報システム運用・停止

情報システムを適切に運用するための管理体制と実施事項を明確化する。また、情報システム障害時の対応策についても明確化する。

⑼　情報システムの使用権

情報システムの利用資格管理が適切に行われないと、情報システムの不正利用を招く危険がある。そこで、情報システムの使用権を、必要な者に、必要な期間与え、情報システムの利用資格に関する義務・責任を明確化する。また、情報システムの不正利用の定義を明確化する。

⑽　ネットワークセキュリティ

ネットワークは情報流通の基盤であるとともに、情報侵害の経路ともなり得るため、適切に把握・管理することが必要である。セキュリティ侵害を防止するため、管理体制・実施事項を明確化する。

⑾　コンピュータウイルス

業務で使用する機器がコンピュータウイルスに感染した場合、多大な被害が発生する可能性があるため、感染の予防及び防止が重要である。そこで、コンピュータウイルスに関しても管理体制を確立し、予防及び防止並びに感染時の対策を明確化する。また、コンピュータウイルス等による情報漏えいの防止対策も明確化する。

また、コンピュータウイルスによる情報漏えいが懸念される為、情報漏えいを発生させる懸念のあるソフトウェアの導入防止等の予防措置を明確化する。

ウ　アクセス制御

適用範囲内の情報システムの利用、建物への入館、事務室及び機械室への入室等に際しては、情報資産を保護するため、個人を識別・認証し、情報へアクセスする際に審査することが必要である。そこで、利用者を限定・把握できるよう実施事項を明確化する。

危機管理計画
策定のための指針

1　目的

危機管理計画は、サイバーテロについてあらかじめ対処方法を定めておくことで、実際にサイバーテロが発生した場合に迅速な対応を可能とし、早期に現状へ復旧し、被害の拡大を防ぐことを目的とするものである。この指針は、電気通信事業用ネットワークにおいてサイバーテロが発生した場合の緊急対応体制を整備するため、危機管理計画策定の指針として定めたものである。電気通信事業用ネットワーク以外のネットワークにおける危機管理計画についても対象とするネットワーク、想定される攻撃等を考慮し、本指針を参考として策定されることが望ましい。

2　サイバーテロの定義等

⑴　サイバーテロの定義

サイバーテロは、コンピュータウイルスやハッカーによって個人が被害を受けるものとは異なり、国家等の重要システムを機能不全に陥れるものであることから、この指針におけるサイバーテロの定義は、「ネットワークを通じて各国の国防、治安等をはじめとする各種分野の情報システムに侵入し、データを破壊、改ざんするなどの手段で国家等の重要システムを機能不全に陥れる行為」とする。

⑵　攻撃対象となる重要インフラ

サイバーテロの攻撃対象となった場合、その産業、企業のみならず、広く国民生活に重大な影響が及ぶこととなる重要インフラとして、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）等が想定される。

⑶　重要インフラの相互依存性

各重要インフラは、他の重要インフラと独立して存立するのではなく、相互に依存し存立しており、ある重要インフラが攻撃を受けた場合、関連する他の重要インフラも影響を受ける場合が多々あることから、重要インフラを保有してサービスを提供する事業者は、他インフラへの影響も考慮した対策が必要である。

⑷　主な攻撃方法

サイバーテロにおける主な攻撃方法の具体例としては、次のものがある。

ア　物理的な攻撃

電気通信施設に不正侵入し、ネットワーク管理センターを占拠する等によりネットワークのコントロールを奪い、これをまひさせるような攻撃

イ　ホームページ改ざん

思想的な意図等により社会に広くアピールするため、ホームページの掲載内容を改ざんするもの

ウ　分散協調型サービス拒否（以下「DDos」という。）攻撃

複数の場所からサーバの処理能力を超える大量のデータを送り付けるなどの方法によりサーバを停止させるもの

エ　コンピュータウイルス

強力な感染力と破壊力を持つウイルスによる攻撃

オ　不正侵入（なりすまし）

他人になりすまして侵入し、データの改ざん、削除を行うほか、他への攻撃にも使用

3　危機管理計画の策定

危機管理計画の策定に当たって配慮すべき内容を以下に示す。

⑴　対象

ア　攻撃

対象とするべき電気通信ネットワークのぜい弱な部分の具体例は次のとおりである。これを参考として、各電気通信事業者の状況により大規模な影響が出ることを想定し、対象となる攻撃を明確に規定する。

(ｱ) 固定・移動電話網
物理的な攻撃、意図的なふくそうによる攻撃

(ｲ) 移動電話網
電波による不正アクセス、電波による通信妨害

(ｳ) 専用回線網及び中継回線網
電波妨害

(ｴ) IP ネットワーク
サーバ等への攻撃、モバイルインターネットアクセスへの攻撃、コンピュータウイルス

(ｵ) ネットワークの機能を管理・運営するコンピュータ
電磁波による情報漏えい

イ　被害規模の対象範囲

各電気通信事業者の状況により大規模な影響が出ることを想定して、被害規模の対象範囲を明確に規定する。

その際には、電気通信事業法施行規則（昭和 60 年郵政省令第 25 号）第 58 条の報告を要する重大な事故の基準も参考とする。

⑵　予防

必要に応じて次のハッカー対策、コンピュータウイルス対策等を規定し、サイバーテロに対する予防措置を図る。

ア　インターネットに接続するための機器の配置及び構成

(ｱ) ファイアウォール等を設置して適切な設定を行う。

(ｲ) 非武装セグメント構成を採用する。

(ｳ) 開放網と閉域網とを区別したネットワーク構成を採用する。

(ｴ) telnet や ftp 等サービス提供に不用な通信の接続制限を行う。

(ｵ) 最新の情報セキュリティ技術を採用する。

(ｶ) 攻撃元を特定できる機能と攻撃元のトラヒックを遮断する仕組み等を採用する。

イ　ソフトウェア上の対策

(ｱ) インターネットに接続する場合は、サーバ等におけるセキュリティホール対策を講ずる。

(ｲ) コンピュータウイルス及び不正プログラム混入対策を講ずる。

(ｳ) 高度な端末認証、生体認証などについて、広く普及させていくことにより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。

ウ　監視、管理等

(ｱ) インターネットに接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバ及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されるよう措置する。

また、ネットワーク上のパケット並びにサーバ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。

(ｲ) コンピュータからの漏えい電磁波の低減対策、又は電磁環境に配慮した上で漏えい電磁波をマスクする措置を講ずる。

エ　不正アクセス防止のためのシステム上の設定

(ｱ) 利用者の識別・確認を要する通信を取り扱う情報通信ネットワークには、正

当な利用者の識別・確認を行う機能を設ける。

(ｲ) アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃取を防止する措置を講ずる。

(ｳ) 利用者のパスワードの文字列をチェックし、一般的な単語を排除する機能を設ける。

(ｴ) アクセス失敗回数の基準を設定するとともに、基準値を超えたものについては、履歴を残しておく機能を設ける。

(ｵ) 保護することが求められる重要な情報については、その情報に対するアクセス要求を記録し、保存する機能を設ける。

(ｶ) ネットワークへのアクセス履歴の表示又は照会が行える機能を設ける。

(ｷ) 一定期間以上パスワードを変更していない利用者に対して注意喚起する機能を設ける。

(ｸ) 一定期間以上ネットワークを利用していない利用者がネットワークにアクセスする際に、再開の意思を確認する機能を設ける。

(ｹ) アクセスにおける本人認証手段には、端末認証（ＭＡＣアドレス、シリアル番号等）や生体認証（指紋、静脈等）など、より高度な認証方式の導入を検討する事が望ましい。

オ　通信の秘密の保護

(ｱ) 機密度の高い通信には、秘話化又は暗号化の措置を講ずる。

(ｲ) 適切な漏話減衰量の基準を設定する。

カ　ネットワークの不正使用の防止

ネットワークの不正使用を防止する措置を講ずる。

キ　新手の攻撃に対するハード・ソフト対策の体制強化

ネットワークシステムの脆弱性に対処できるように内部統制や社内ルールを随時見直し、新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。

ク　他の利用者へ悪影響を与えている利用者に対する一時利用停止の明確化

他の利用者に悪影響を与えている事象を洗い出し、当該事象への対応方針を策定し、利用者の合意形成を図る。

ケ　サーバー攻撃発生時の迅速な情報共有方法の確立

⑶　発生時の復旧対応

ア　復旧対応としては、必要に応じて次の項目を規定するとともに、既存の障害復旧マニュアル等を活用することも規定する。

(ｱ) サーバ等への攻撃からの復旧対応

Ａ　DDoＳ攻撃により通信不能となった場合、攻撃側サーバの速やかな停止を依頼する。

Ｂ　サーバのルート権限を奪われる等により不正な処理を開始した場合、サーバを停止する又はネットワークから切断し再起動する。

Ｃ　サーバが何らかの原因により不正な処理を開始した場合、ルート権限で不正な処理のプロセスを排除する。

Ｄ　サーバへの侵入の痕跡を発見した場合、サーバをネットワークから隔離する。

Ｅ　サーバ等が通信不能となつた場合、通信不能箇所を特定し再起動などの処

置を行う。

(ｲ) 伝送交換設備への攻撃からの復旧対策

A　重要な伝送路設備には、応急復旧用ケーブルの配備等の応急復旧対策を講ずる。

B　移動用交換設備の配備等の応急復旧対策を講ずる。

C　災害時等において、衛星地球局等の無線設備により、臨時電話等の設置が可能であること。

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

E　移動体通信基地局に障害が発生した場合等に、可搬型無線基地局により、臨時の電気通信回線の設定が可能であること。

F　他の伝送設備の障害時に、通信の疎通が著しく困難となった場合、予備の設備等により臨時の電気通信回線の設定が可能であること。

イ　緊急時における対処には、高度な判断を必要とする場合があることから、責任と権限を有する適切な者が速やかに判断を行うことができるように規定する。

ウ　複数の電気通信事業者に障害が発生し、その影響が波及して被害が拡大していくことが想定されることから、障害情報等を交換し被害を最小限に抑えるために、国、電気通信事業者、事業者団体等の関係者間で連絡体制、運用方法を明確に規定する。

⑷　原因判明時の措置

ア　当該障害がサイバーテロによるものであることが判明した場合は、一定のルートで国、電気通信事業者、事業者団体等の関係者に通知することが可能なよう、(3)ウと同様に伝達ルート等をあらかじめ定めておく。

イ　障害の発生状況及び影響の拡大防止に対する協力に関して、電気通信事業者から利用者への周知方法等について規定する。

ウ　障害の発生原因が判明し、再度攻撃にさらされるおそれがある場合における障害の発生防止のため、必要な措置を講じることを規定する。

エ　ネットワークを介して、他分野の重要インフラ事業者と情報システムを相互接続している場合には、サイバーテロ対策に関し互いの連絡・連携体制を必要に応じ構築する。

⑸　危機管理計画の見直し等

ア　技術の進展に伴い、サイバーテロによる攻撃方法等が、変化していくと考えられるため、適宜危機管理計画の見直しを行うことを規定する。

イ　サイバーテロが発生した際の対処を円滑に行えるよう、必要に応じサイバーテロの発生を想定した訓練を実施することを規定する。