参考資料 21－3

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。

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。

⑺　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

⑴　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

⑼　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。