別表第2　管理基準

参考資料1

情報通信ネットワーク　安全・信頼性基準（現行）						
項目		対策		実施指針		
				事業用	その他	自営	ユーザ
1.ネットワーク設計管理							
	(1)体制の明確化	ア	意思決定、作業の分担、責任の範囲等の設計管理体制を明確にすること。	◎	◎	◎	◎
		イ	重要な設備に関する設計については、関連部門間での連携を図ること。	◎	◎	◎	◎
	(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（端末の挙動によるものを含む。）及び機能の拡充を考慮した設計とすること。	◎	◎	◎	◎
		ウ	トラヒックの瞬間的かつ急激な増加及び制御信号の増加の対策を講じた設計とすること。	◎	－	－	－
	(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	重要な機器を導入する場合は、導入判定の統一基準を策定し、その基準に基づき品質の検証を行うこと。	◎	◎	◎	◎
		イ	サーバ等機器導入前の機能確認を十分に実施すること。	◎	◎	◎	◎
		ウ	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。	◎	◎	◎	◎
		エ	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。	◎	◎	◎	◎
		オ	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。	◎	◎	－	－
		カ	冗長構成をとる機器は、その切替動作が確実に行われることを確認すること。	◎	◎	○	○
		キ	トラヒックの瞬間的かつ急激な増加への対策として、各装置の最大処理能力を超える負荷試験を実施すること。その際、実環境でのトラヒックパターンを参考に、複数のトラヒック条件での試験を実施すること。	○	－	－	－
2.ネットワーク施工管理							
	(1)体制の明確化	ア	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。	◎	◎	◎	◎
		イ	重要な設備の施工、新設備等の導入に際しては、関連部門間での連携を図ること。	◎	◎	◎	◎
	(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。	◎	◎	◎	◎

別表第2 管理基準

参考資料1

情報通信ネットワーク 安全・信頼性基準（現行）							
項目		対策		実施指針			
				事業用	その他	自営	ユーザ
		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つて、通信の秘密の保護及びデータの保護に十分に配慮する場合は、この限りでない。	◎	◎	◎	◎
3.ネットワーク保全・運用管理							
	(1)体制の明確化	ア	作業の分担、連絡体系、責任の範囲等の保全・運用管理体制を明確にすること。	◎	◎	◎	◎
		イ	重要な設備の保全・運用については、関連部門間での連携を図ること。	◎	◎	◎	◎
	(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。	◎＊	◎＊	◎＊	◎＊
		ウ	災害時優先通信の機能により他の通信の制限又は停止を行つた場合には、災害時優先通信及び他の通信の疎通の状況を記録・分析すること。	◎	－	－	－
	(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	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つて、通信の秘密の保護及びデータの保護に十分に配慮する場合は、この限りでない。	◎	◎	◎	◎
	(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。	◎	○	○	○

別表第2　管理基準

参考資料1

情報通信ネットワーク　安全・信頼性基準（現行）							
項目		対策		実施指針			
				事業用	その他	自営	ユーザ
	(9)ふくそう対策	ア	情報通信ネットワークのふくそうを防止し、有効活用を図るため、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	ア	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。	◎	◎	◎＊	◎＊
		イ	重要な設備の更改・移転については、関連部門間での連携を図ること。	◎	◎	◎	◎
	(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)コンピュータウィルス情報緊急通報体制の整備	ア	コンピュータウィルス並びに端末及びソフトウェアの脆弱性に関する情報を入手したときは、必要に応じて、電気通信業界で定めた緊急連絡先に、直ちに連絡すること。	◎	◎	－	－
		イ	コンピュータウィルス並びに端末及びソフトウェアの脆弱性に関する情報を入手したときは、必要に応じて、自社内に対して速やかに周知するとともに、利用者に対してウェブサイトへの掲示、メールニュース等適切な方法により速やかに情報提供する等、被害の拡大を防止するための措置を講ずること。	◎	◎	◎	◎
	(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		コンピュータウィルス又は不正プログラムが混入した際に、情報通信ネットワークに対して利用者が与え、又は情報通信ネットワークの利用者が受ける可能性のある影響とその対策について利用者に周知すること。	◎	◎	－	－
	(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。	◎	◎	◎	◎

別表第2　管理基準

参考資料1

情報通信ネットワーク　安全・信頼性基準（現行）							
項目		対策		実施指針			
				事業用	その他	自営	ユーザ
	(2)基準の設定		データ管理基準を設定すること。	◎	◎	◎	◎
	(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。	◎	◎	○	○

別表第2 管理基準

参考資料1

情報通信ネットワーク 安全・信頼性基準（現行）						
項目		対策	実施指針			
			事業用	その他	自営	ユーザ
		キ 非常時における対応体制の検証・見直しを必要に応じて行うこと。	◎	○	◎	○
	(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、電気通信事業者の取組等						
	(1)ネットワークの安全・信頼性の確保に係る取組状況	ア 情報通信ネットワークの安全・信頼性の確保の取組状況を適切な方法により利用者に対して公開すること。	◎	◎	－	－
		イ 電気通信設備の安全・信頼性の確保の取組に関する次の情報を適切な方法により利用者に対して公開すること。 ① 停電対策に関する情報 ② ネットワークの通信容量の設計に関する基本的考え方、通信規制や重要通信の優先的取扱いに係る手法等に関する情報 ③ 災害時における被災エリアの通信の確保に関する情報	◎	－	－	－
	(2)ネットワークの事故・障害の状況	ア 情報通信ネットワークの事故・障害の状況を適切な方法により速やかに利用者に対して公開すること。	◎	◎	－	－
		イ ふくそうが発生した場合には、その状況及び通信規制の実施状況を速やかに利用者に対して公開すること。	◎	◎	－	－

別表第2　管理基準

参考資料1

情報通信ネットワーク　安全・信頼性基準（現行）						
項目		対策	実施指針			
			事業用	その他	自営	ユーザ
	(3)サービス提供不可に陥るケース等の周知	ア 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。	◎	◎	－	－
		イ 情報通信ネットワークのふくそうを防止し、有効活用を図るため、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。	◎	◎	－	－
		ウ 災害時においては、不要不急の電話を控えること及び通話時間をできるだけ短くすることについて、周知・要請し、災害用伝言サービスを含めた音声通話以外の通信手段の利用等を平常時から呼びかけること。	◎	－	－	－
		エ 緊急通報手段を提供するサービスは、メンテナンス時にもできるだけ緊急通報が利用できるよう適切な措置を講ずること。また、メンテナンス時にサービス停止が必要な場合は、ユーザに通知する措置を講ずること。	◎	◎	－	－
	(4)情報セキュリティに関する取組	ア 情報セキュリティポリシーを公表すること。	◎	◎	－	－
	(4)情報セキュリティに関する取組	イ コンピュータウィルス並びに端末及びソフトウェアの脆弱性に関する情報を入手したときは、必要に応じて、自社内に対して速やかに周知するとともに、利用者に対してウェブサイトへの掲示、メールニュース等適切な方法により速やかに情報提供する等、被害の拡大を防止するための措置を講ずること。	◎	◎	◎	◎
	(5)電気通信サービスの不適正利用の防止に関する周知・取組	ア 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。	○	○	－	－
		イ 携帯電話インターネット接続役務提供事業者は、青少年有害情報フィルタリングサービスを提供できる体制を整えること。また、インターネット接続役務提供事業者は、青少年有害情報フィルタリングソフトウェア又は青少年有害情報フィルタリングサービスを提供できる体制を整えること。	◎	◎	－	－
		ウ インターネット上の児童ポルノ画像等の流通・閲覧防止対策を講じている事業者においては、その旨を周知すること。	◎＊	◎＊	－	－
	(6)電気通信事業者間等の情報共有	ア 電気通信事業者及びその業界団体は、電気通信事故に係る情報や再発防止策を業界で共有し、事故防止に向けた体制を整えること。	◎＊	－	－	－
		イ 電気通信事業者は、アプリケーション開発者との間で、ネットワークの負荷を考慮したアプリケーションの開発手法等について情報共有すること。	○	－	－	－