「情報通信ネットワーク安全・信頼性基準」の見直し案整理表

資料９－３

設備基準

ガイドライン		答申				作業班報告書(案)				
項目	対策	項目		対策	具体的取組	頁	対策	解説	例	備考
1.一般基準 （13項目53対策）	(1)通信センターの分散<2>	5.1.1	バックアップ、分散化等のICT障害対策	ケ　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等	ネットワークのふくそうの事前及び事後の対応策については、有識者を含めて技術的検討を行い、また、予備機器の設置、応急復旧機材の配備、データ等の定常的バックアップ、ネットワーク経路の二重化、オペレーションセンターの分散化、通信経路の迂回措置、ケーブル配線の安全対策、予備電源の設置等、安全・信頼性を確保する観点で対策すべき事項についてガイドラインの充実を行う	38 78		○		
	(2)代替接続系統の設定<1>									
	(3)異経路伝送路設備の設置<2>									
	(4)電気通信回線の分散収容<1>									
	(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<1>	5.1.1	バックアップ、分散化等のICT障害対策	ウ　障害の影響範囲を限定する対策		41	○			
	(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<1>									
	(7)電子メールによる一方的な広告・宣伝等への対策									
	(8)予備の電気通信回線の設定等<2>									
	(9)情報通信ネットワークの動作状況の監視等<8>	4.2.2	ネットワークふくそう対策	カ　アクセス集中時のブロック、負荷分散機構等の機能の実現	アクセス集中時のブロック、負荷分散機構等の機能については、技術検討作業班において、0AB～J番号を使用するIP電話について、「現行のアナログ電話用設備等と同様に、交換設備は、異常ふくそうが発生した場合に、これを検出し、通信の集中を規制する機能又はこれと同等の機能を有することが適当」とされている					1(9)オで対応済
				キ　ふくそう発生のユーザー端末への自動通知	ふくそうの発生をユーザーに通知するための具体的手法（ネットワーク側と端末側双方への機能の実装）					管理基準で対応
		5.1.1	バックアップ、分散化等のICT障害対策	オ　事業者をまたがる標準的網管理インタフェースの検討	各事業者は自らのIPネットワーク上の交換設備に異常ふくそうを検出する機能や通信の集中を規制する機能の具備を検討する					1(9)キで対応済
	(10)ソフトウェアの信頼性向上対策<6>	3.1.2	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	オ　ソフトウェアの導入・更新時の信頼性確保のための体制	ソフトウェア導入・更新時のセキュリティ確保については、OS、ミドルウェアベンダーとベンダー間、ベンダーと事業者間で連携して対策を実施し、現状を整理しながら、両者間で情報共有・改善	47	◎	○		
		4.1.2	開発及びサポートプロセスにおける管理	イ　定期的なソフトウェアのリスク分析とバージョンアップの計画	開発段階で見過ごされた脆弱性を発見するために定期的にソフトウェアを点検し、リスク分析を行う	47	◎	○		
		5.1.2	サイバー攻撃に備えた設備等に関する脆弱性への対策	ウ　出荷前での端末機器の徹底的な脆弱性テストの実施と出荷後の迅速なパッチの適用	端末機器のソフトウェアに脆弱性が存在しないように開発段階でのチェックを各機器ベンダーで徹底することが必要であり、また機器ベンダーが出荷段階での品質検査を徹底する	46	◎	○		
					端末機器が市販された後になって脆弱性が発見された場合は、機器ベンダーが迅速にユーザーにその旨通知し、ソフトウェアパッチの早期適用を徹底することが必要	46	◎	○		
					新たに発見される脆弱性への対策としてソフトウェアの更新が必須であることについて、ユーザーの幅広い理解を得るための啓発活動を国、事業者及び関係団体が連携した上で積極的に行う	46	◎	○		
					技術検討作業班での検討を踏まえ、脆弱性が発見されたソフトウェアについて早期の更新を確実に実施できる仕組み（例えば自動更新機能）を端末に装備させ、普及促進を図っていく					対象外

ガイドライン		答申				作業班報告書(案)				
項目	対策	項目		対策	具体的取組	頁	対策	解説	例	備考
	(11)情報セキュリティ対策<21>	4.3.1	社内の重要情報の管理	ウ　情報の暗号化、アクセス権制御など情報の秘密を確保する対策・手順の明確化	常に最先端の研究開発の成果を取り入れた情報セキュリティ対策を講じることが必要					1(11)ｸで対応済
				エ　アクセスログの取得、適切な保管						1(11)ｷで対応済
		4.3.2	サイバー攻撃に備えた管理体制	ア　他の利用者へ悪影響等を与えている利用者に対する一時利用停止の						管理基準で対応
		4.3.3	情報漏えい防止対策	イ　メール等を利用した情報交換におけるセキュリティの確保	メール等を利用した情報交換を行う際の手順を具体化して内規等のドキュメントに定める					対象外
				カ　コンピュータウィルス等による情報漏えい対策						管理基準で対応
	(12)通信の途絶防止対策									
	(13)応急復旧対策<6>									
	追加(14)	5.1.1	バックアップ、分散化等のICT障害対策	カ　緊急通報確保のため稼働状態でメンテナンスを可能とするIP電話システムの実現	0AB～J番号を使用するIP電話においては、緊急通報が常に利用できるようにするためにも、稼働状態でのメンテナンスを可能とするようシステムの改善を図る	62	◎	○		
					メンテナンス時にサービスを停止する場合は、多様なメディアを通じて、ユーザーに通知できるようにする	62	◎	○		
2.屋外設備 （15項目20対策）	(1)風害対策<2>									
	(2)振動対策<1>									
	(3)雷害対策<1>									
	(4)火災対策<1>									
	(5)耐水等の対策<2>									
	(6)水害対策<1>									
	(7)凍結対策<1>									
	(8)塩害等対策<1>									
	(9)高温・低温対策<2>									
	(10)高湿度対策<1>									
	(11)高信頼度<1>									
	(12)第三者の接触防止<2>									
	(13)故障等の検知、通報<2>									
	(14)予備機器等の配備<1>									
	(15)通信ケーブルの地中化<1>									

ガイドライン		答申				作業班報告書(案)				
項目	対策	項目		対策	具体的取組	頁	対策	解説	例	備考
3.屋内設備 （7項目12対策）	(1)地震対策<3>									
	(2)雷害対策<1>									
	(3)火災対策<1>									
	(4)高信頼度<2>									
	(5)故障等の検知、通報<3>	5.1.1	バックアップ、分散化等のICT障害対策	エ　障害発生箇所の特定の迅速化を図るため設備構成のシンプル化及び小規模分散化等の検討						管理基準で対応
	(6)試験機器の配備<1>									
	(7)予備機器等の配備<1>									
	追加(8)	5.1.1	バックアップ、分散化等のICT障害対策	キ　コロケーション先の電気通信設備の保護	電源設備について、例えば、異常時電源遮断機能を具備することや、保守点検により正常性を維持すること等、発火・発煙等の防止に関する基準を、電気通信事業法上の技術基準等として設ける					対象外
					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ついて、発火・発煙等の防止等の最低限の安全・信頼性が確保されるよう所要の措置を講じる	78	◎	○		
4.電源設備 （7項目14対策）	(1)電力の供給条件<3>									
	(2)地震対策<2>									
	(3)雷害対策<1>									
	(4)火災対策<1>									
	(5)高信頼度<1>									
	(6)故障等の検知、通報<2>									
	(7)停電対策<4>	5.1.1	バックアップ、分散化等のICT障害対策	ア　設備の規模に応じた予備電源による具体的な動作時間の設定	各事業者が設備の重要度に応じて十分な規模の予備電源が確保できるよう、適切な局舎やハウジングスペースの選定、自前の予備電源の設置などの対策を講じることをガイドライン等において明確化する	86	◎	○		
				イ　地下鉄構内等の携帯電話基地局等の予備電源の確保・充実	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、共同設置など他事業者と積極的に連携をとる	86		○		
	追加	5.1.3	端末等に対する対策	ウ　停電後の地域単位のセッションリクエストによるネットワーク負荷の分散	IP電話端末については技術検討作業班で一斉登録に伴うふくそうを回避する機能、端末の無効呼抑止機能、自動発信回数制限などについて検討を実施し、その結果「ネットワークが端末からの登録を受付できない場合に、ネットワークから再登録要求の送信タイミングについて指示があった場合は、端末はその指示に従い送信タイミングを調整し、また、ネットワークから再登録要求の送信タイミングについて指示が無い場合は、端末が送信タイミングを調整し、再登録要求を行う機能を有することが適当」とされている。将来に向けて改善すべき事項として、IP電話以外の端末についても同様の検討が必要	117		○		管理基準に追加

環境基準

ガイドライン		答申				作業班報告書(案)				
項目	対策	項目		対策	具体的取組	頁	対策	解説	例	備考
1.センターの建築物 （4項目11対策）	(1)立地条件及び周囲環境への配慮<4>									
	(2)建築物の選定<3>									
	(3)入出制限機能<2>	5.1.1	バックアップ、分散化等のICT障害対策	ク　セキュリティを保つべき領域の基準の明確化と重要度に応じた入出管理の導入	電気通信設備を工事・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にセキュリティを保つべき領域の具体的な基準を設定	90	◎	○		
					次世代IPネットワーク等新たなネットワークやサービス形態へ移行していく中で、電気通信事業法等の法令や現行のガイドラインを適宜見直し、それらに基づき、各事業者がそれぞれのサービスに適した形で、取り組んでいく					対象外
					重要度に応じた適切な入出管理を導入していく	90	○			
					生体認証など新しい認証技術の入出管理システムが開発されていることなどから、技術の進展に沿ってシステムを見直していくことが必要	90			○	
					定期的に取り組み状況等を相互接続している事業者間で情報共有する 模範的な導入事例等を事業者間で共有するなど、各事業者における入					対象外
	(4)火災の検知、消火<2>									
2.通信機器室等 （6項目21対策）	(1)通信機械室の位置<4>									
	(2)通信機械室内の設備等の設置<2>									
	(3)通信機械室の条件<6>									
	(4)入出制限機能<2>	5.1.1	バックアップ、分散化等のICT障害対策	ク　セキュリティを保つべき領域の基準の明確化と重要度に応じた入出管理の導入	電気通信設備を工事・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にセキュリティを保つべき領域の具体的な基準を設定	95	◎	○		
					次世代IPネットワーク等新たなネットワークやサービス形態へ移行していく中で、電気通信事業法等の法令や現行のガイドラインを適宜見直し、それらに基づき、各事業者がそれぞれのサービスに適した形で、取り組んでいく					対象外
					重要度に応じた適切な入出管理を導入していく	95	○			
					生体認証など新しい認証技術の入出管理システムが開発されていることなどから、技術の進展に沿ってシステムを見直していくことが必要	95			○	
					定期的に取り組み状況等を相互接続している事業者間で情報共有する 模範的な導入事例等を事業者間で共有するなど、各事業者における入					対象外
	(5)データ類の保管<5>									
	(6)火災の検知、消火<2>									
3.空気調和設備 （8項目15対策）	(1)空気調和設備の設置<3>									
	(2)空気調和設備室への入出制限<1>									
	(3)空気調和の条件<5>									
	(4)凍結防止<1>									
	(5)漏水防止<1>									
	(6)有毒ガス等<1>									
	(7)故障等の検知、通報<1>									
	(8)火災の検知、消火<2>									

管理基準

ガイドライン		答申				作業班報告書(案)				
項目	対策	項目		対策	具体的取組	頁	対策	解説	例	備考
1.ネットワーク設計管理 （4項目6対策）	(1)体制の明確化<1>	4.1.1	ネットワークシステムの容量の適切な計画・設計	エ　サーバ等機器の事前機能確認の充実	サービスの安定的な提供のために、事前に確認することが必要な最低限の事項について事業者、ベンダーなど関係者でガイドライン化することについて検討	102 (1)		○		
	(2)設計指針の明確化等<2>	4.2.2	ネットワークふくそう対策	ア　ふくそう監視手法や事業者間連携	トラヒックの増加に対応した設備設計手法については、各事業者が自らのネットワーク構成等を踏まえて検討	102 (2)	○	○	○	
	(3)設計工程の明確化等<1>									
	(4)相互接続への対応<2>	4.1.1	ネットワークシステムの容量の適切な計画・設計	ウ　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	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ルール化を図る	103 (4) 114 エ		○	○	
	追加(5)	4.1.1	ネットワークシステムの容量の適切な計画・設計	エ　サーバ等機器の事前機能確認の充実	サーバ等機器の事前機能確認を十分に実施する	104 (5)	◎	○	○	
				キ　ベンダーから提供されるシステムについての事業者における検査手法、品質評価手法の確立	情報通信ネットワークの安全・信頼性の確保のために、必要最低限行うべき共通的な検査・品質測定手法の確立について事業者及びベンダーが連携して検討する	104 (5)	◎	○	○	
		4.1.2	開発及びサポートプロセスにおける管理	ウ　セキュリティチェックのための体制		104 (5)	◎	○	○	
		4.2.2	ネットワークふくそう対策	ケ　災害時におけるユーザーの振る舞いや端末の挙動がネットワークに与える影響の事前検証		104 (5)	◎	○	○	
2.ネットワーク施工管理 （5項目6対策）	(1)体制の明確化<1>									
	(2)作業工程の明確化等<1>	4.1.2	開発及びサポートプロセスにおける管理	カ　安全かつ容易な設備増強、拡張性確保手法の確立	各事業者が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	105 (2)		○	○	
					作業の自動化及び作業確認の強化を実施することにより人為的要因によるサービス中断を回避するとともに、工事ミス時のリカバリー手順を確立する	105 (2)		○	○	
	(3)相互接続への対応<1>									
	(4)委託工事管理<2>	4.1.2	開発及びサポートプロセスにおける管理	オ　工事実施者とネットワーク運用者による工事実施体制の確認や工事手順の策定	工事ミスが発生した場合のリカバリー手法の確認を工事前に実施する	107		○	○	
					工事手順について工事業者から意見を募り、安全性の観点から製品に反映すべき事項、工事計画に反映すべき事項等をまとめたガイドラインを作成することや、遵守状況のチェック体制を確立する	107		○	○	
		4.3.4	外部委託における情報セキュリティ確保のための対策	イ　守秘義務契約、誓約書、情報管理規定の保持	自社の社員と守秘義務契約等を結ぶのと同様に、業務を外部委託する場合には、守秘義務・保持契約を義務化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等を定めた情報管理規定の策定等、委託先の取組みを明確化していく	106 (4) 107 ウ	◎	○	○	
	(5)検収試験管理<1>									

ガイドライン		答申				作業班報告書(案)				
項目	対策	項目		対策	具体的取組	頁	対策	解説	例	備考
3.ネットワーク保全・運用管理 （9項目14対策）	(1)体制の明確化<1>	3.1.2	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	ウ　非常時等の事業者間の連携・連絡体制の整備	ICT障害に限らず、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、ベンダー、施工業者、行政機関などの連絡体制の一元管理、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っておく	109 (1)		○	○	
		4.2.1	故障検知・解析	ア　運用監視体制の充実						3(1)対応済
	(2)基準の設定<1>	4.1.1	ネットワークシステムの容量の適切な計画・設計	ア　ルータ等の重要な設備の安全・信頼性基準・指標及び定期点検等の実施方法の策定と適切な見直し	ルータ等の重要な設備の安全・信頼性基準・指標及び定期点検等の実施方法を策定するとともに適切に見直す	102 (2) 110		○	○	
				イ　将来の利用動向に対応できる設備計画の策定及び障害の極小化対策等に関する設計指針等の策定	装置の処理能力を適切に把握するとともに通信需要を適切に予測し、将来の設備増強計画に反映していくことが必要	102 (2) 110		○	○	
					導入前の装置等の処理能力の確認方法、将来の需要予測に基づく適切な設備増強計画、障害の拡大防止・極小化対策等をネットワークの設計指針に反映していくことが必要	102 (2) 110		○	○	
				エ　サーバ等機器の事前機能確認の充実	サービスの安定的な提供のために、事前に確認することが必要な最低限の事項について事業者、ベンダーなど関係者でガイドライン化することについて検討	102 (2) 110		○	○	
	(3)作業の手順化<1>	4.1.1	ネットワークシステムの容量の適切な計画・設計	ア　ルータ等の重要な設備の安全・信頼性基準・指標及び定期点検等の実施方法の策定と適切な見直し	ルータ等の重要な設備の安全・信頼性基準・指標及び定期点検等の実施方法を策定するとともに適切に見直す	111 (3)		○	○	
		4.1.2	開発及びサポートプロセスにおける管理	ア　保守点検の手順書の作成		111 (3)	○			
		4.2.1	故障検知・解析	オ　故障箇所特定のためのデータ取得手順、切り分け手順等の整備	故障箇所を特定するためのデータの取得手順や切り分け手順等を整備しておくことが必要	111 (3)			○	
				カ　故障箇所の特定及び故障原因の特定の迅速化対策	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	111 (3)			○	
		4.2.2	ネットワークふくそう対策	ア　ふくそう監視手法や事業者間連携	具体的なふくそうの検出手法やふくそう制御手法を検討し、各事業者に共通的な事項については制度化やガイドライン化	112		○	○	P109にも追加
					トラヒックの増加に対応した設備設計手法については、各事業者が自らのネットワーク構成等を踏まえて検討	112		○	○	P109にも追加
	(4)監視、保守及び制御<2>	4.2.1	故障検知・解析	エ　問題発生時に検知、通報させる機能や体制の確立						3(4)対応済
	(5)相互接続への対応<3>	3.1.2	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	ウ　非常時等の事業者間の連携・連絡体制の整備	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）が必要	114 (5)	○		○	
					連携にあたっては、相互接続を意識して、事業者とベンダー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の検討が必要	114 (5)		○	○	
		4.2.1	故障検知・解析	イ　相互接続時のネットワーク管理体制の強化等	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	114 (5)			○	
					適切なオペレーションの実現に向けた事業者間のやり取りに必要な情報の抽出について検討。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、VoIPなどのサービス別に協議し、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の具体的な検討	114 (5)		○	○	
				オ　故障箇所特定のためのデータ取得手順、切り分け手順等の整備	事業者共同で検討 ·事業者間の網運用・管理情報交換に関する方針、情報項· 故障特定方法に関して共通化できる項目の抽出 ·ベンダーによるネットワーク切り分け手順作成や実技講習の積極的な開催	114 (5)			○	

ガイドライン		答申				作業班報告書(案)				
項目	対策	項目		対策	具体的取組	頁	対策	解説	例	備考
	(6)委託保守管理<2>	3.1.2	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	エ　迅速な原因分析のための事業者とベンダーの連携体制の確立	ベンダーの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ベンダーとの保守契約などに盛り込む	115 (6)	◎	○	○	
					ベンダーに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	115 (6)	◎	○	○	
					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ーと適切な対策を立てる	115 (6)	◎	○	○	
					ベンダーとの共同訓練を実施する	115 (6)	◎	○	○	
		4.3.4	外部委託における情報セキュリティ確保のための対策	ア　業務委託先の選別の評価要件の設定	事業者は、外部委託先の要件として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取り入れる等、外部委託先の情報セキュリティを確保していくことが適当	115 (6)	◎	○	○	
	(7)保守試験管理<1>									
	(8)情報の収集<1>	3.1.2	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	ウ　非常時等の事業者間の連携・連絡体制の整備	災害発生初期における電気通信設備の復旧にあたり必要となる、道路状況など重要インフラ各分野を越えた情報交換については、CEPTOAR-Councilの場での検討を見守る					9(1)オ対応済
		4.2.2	ネットワークふくそう対策	ウ　企画型ふくそうを防止するための情報収集の仕組み		116 (8)	○	○	○	
	(9)ふくそう対策<2>	4.2.2	ネットワークふくそう対策	ア　ふくそう監視手法や事業者間連携	具体的なふくそうの検出手法やふくそう制御手法を検討し、各事業者に共通的な事項については制度化やガイドライン化	117 (9)		○	○	
				イ　ふくそう時のユーザー間の公平性の確保	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共に、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	117 (9)		○	○	
					重大なネットワークふくそうにより他事業者にも影響を及ぼす場合を想定した事業者間連携、そのための事業者間での共通用語の定義、連絡基準・連絡体制、さらにユーザー(消費者)への周知の基準・内容について業界団体でガイドライン化の検討	117 (9)		○	○	
				エ　ふくそうの波及防止手順の整備及び長期的視点の対策		117 (9)	○	○	○	
				オ　ノードが具備すべきふくそう対策		117 (9)			○	
				キ　ふくそう発生のユーザー端末への自動通知		117 (9)			○	
				ク　災害用伝言ダイヤル等の利用促進によるふくそう軽減	引き続き周知徹底に努める	117 (9)			○	
				シ　障害時の集中呼のパターンを再現できる試験方法の確立	イベントなどトラヒック急増時のふくそう対策などの措置手順、連絡体制の整備	117 (9)			○	
					開発・試験環境の充実、具体的障害事例を用いた、分析と改善策の情報交換・検討	117 (9)			○	
		5.1.1	バックアップ、分散化等のICT障害対策	オ　事業者をまたがる標準的網管理インタフェースの検討	技術検討作業班の今後の検討状況に合わせて、必要に応じて通信事業者間で障害情報やふくそう情報を伝達できるプロトコルの開発・標準化等を検討する	117 (9)			○	
4.設備の更改・移転管理(2項目2対策)	(1)体制の明確化<1>									
	(2)作業工程の明確化等<1>									

ガイドライン		答申				作業班報告書(案)				
項目	対策	項目		対策	具体的取組	頁	対策	解説	例	備考
5.情報セキュリティ管理（7項目8対策）	(1)情報セキュリティポリシーの策定<1>	4.3.3	情報漏えい防止対策	カ コンピュータウィルス等による情報漏えい対策		123 (8)			○	
	(2)危機管理計画の策定<1>	3.1.2	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	ア 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	120 (2)			○	
		4.3.2	サイバー攻撃に備えた管理体制	ア 他の利用者へ悪影響等を与えている利用者に対する一時利用停止の明確化	技術革新や社会の変化に伴い、他の利用者に悪影響を与えている事象も変化していくと考えられるが、そのような事例を洗い出し、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	120 (2)			○	
				ウ サイバー攻撃発生時の迅速な情報共有方法の確立	T-CEPTOAR等において、例えば、サイバー攻撃の危険度の考え方、事業者間での情報共有のあり方について検討	120 (2)			○	
		5.1.2	サイバー攻撃に備えた設備等に関する脆弱性への対策	イ 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	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）を導入するなど、より高度な認証方式の導入の検討	120 (2)			○	
				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		120 (2)			○	
	(3)情報セキュリティ監査の実施<1>	4.3.3	情報漏えい防止対策	ウ 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		121 (3)		○	○	
				カ コンピュータウィルス等による情報漏えい対策		123 (8)			○	
	(4)コンピュータウィルス情報緊急通報体制の整備<2>	4.3.2	サイバー攻撃に備えた管理体制	ア 他の利用者へ悪影響等を与えている利用者に対する一時利用停止の明確化	技術革新や社会の変化に伴い、他の利用者に悪影響を与えている事象も変化していくと考えられるが、そのような事例を洗い出し、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	120 (2)			○	
				ウ サイバー攻撃発生時の迅速な情報共有方法の確立	T-CEPTOAR等において、例えば、サイバー攻撃の危険度の考え方、事業者間での情報共有のあり方について検討	122 (4)		○	○	
	(5)情報セキュリティに関する情報収集<1>	3.1.1	基本指針、責任の明確化など組織・体制の整備	エ システム管理のガイドラインの国際的な基準への反映と整合性の確保	ネットワークの高度化や技術革新により生まれる新しい電気通信サービスに関する情報セキュリティ対策等について、ネットワーク環境や市場、国際動向等の変化に応じて、随時対応する	122 (5)		○		
	(6)知識・技能を有する者の配置<1>									
	(7)情報セキュリティに関する利用者への周知<1>									
	追加(8)	4.3.1	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の分類		123 (8)	◎	○		
				イ 情報の管理に関する内部統制ルールの整備	内部統制ルールに関する事項の整備を行う	123 (8)	◎	○		
	追加(9)	4.3.2	サイバー攻撃に備えた管理体制	イ セキュリティ情報管理レベルの規定及び攻撃者への対処	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事業者間の協力体制について検討を行い、情報共有する体制の整備、他社へ協力を依頼するルートの整備、情報共有を行う上での情報管理基準、秘密保持契約等の締結方法等について検討	123 (9)	◎	○	○	
				ウ サイバー攻撃発生時の迅速な情報共有方法の確立	サイバー攻撃発生時に、国に提供する情報について検討	123 (9)	◎	○	○	

ガイドライン		答申				作業班報告書(案)				
項目	対策	項目		対策	具体的取組	頁	対策	解説	例	備考
6.データ管理 （5項目7対策）	(1)体制の明確化<1>									
	(2)基準の設定<1>	4.3.4	外部委託における情報セキュリティ確保のための対策	事業者からベンダーに送付される故障物品内に格納された情報の漏えい防止対策	事業者からベンダー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	126 (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	126 (2)		○	○	
	(3)作業の手順化<1>									
	(4)データの記録物の管理<3>	3.1.1	基本指針、責任の明確化など組織・体制の整備	イ　記録媒体の性能向上やシステム間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		128 エ	◎	○		
		4.3.3	情報漏えい防止対策	ア　媒体の種類に応じた廃棄処分方法の明確化	媒体廃棄の際の手順を具体化して内規等のドキュメントに定める	127 (4)			○	
		4.3.4	外部委託における情報セキュリティ確保のための対策	事業者からベンダーに送付される故障物品内に格納された情報の漏えい防止対策	事業者からベンダー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	127 (4)		○	○	P126(2)にも追加
					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	127 (4)		○	○	P126(2)にも追加
	(5)ファイル等の遠隔地保管<1>									
	追加(6)	4.3.3	情報漏えい防止対策	エ　情報漏えい対策についての事業者間の情報・意見交換の場の設定	電気通信分野における情報セキュリティ対策協議会などの場を活用しながら、技術的・人的な対策等について事業者間の意見交換を行うことにより、すべての事業者がレベルの高い情報セキュリティ対策を講じる	129 (6)	◎	○		
				オ　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）の漏えいについての報告	重要なシステム情報の流出についても監督官庁へ報告を行う	129 (6)	◎	○		
7.環境管理 （2項目2対策）	(1)建築物の保全<1>									
	(2)空気調和設備の保全<1>									
8.防犯管理 （6項目6対策）	(1)体制の明確化<1>									
	(2)管理の手順化<1>									
	(3)建築物、通信機械室等の入出管理<1>									
	(4)かぎ、暗証番号等の管理<1>									
	(5)防犯装置の管理<1>									
	(6)入出管理記録の保管<1>									
9.非常事態への対応 （2項目7対策）	(1)体制の明確化<6> (2)復旧対策の手順化<1>	3.1.2	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	イ　非常時等のサービス復旧のための緊急対応の手順や管理体制の整備	障害の対応マニュアルの整備や、災害時、重大故障時のサービス復旧のための緊急対応の手順や管理体制の整備を行うことが必要	133 134	○	○	○	
					具体的な対策などは各事業者が主体的に実施	133 134		○		
					相互接続している事業者間の連携、緊急通報や重要通信の確保、故障状況の広報などの在り方については、事業者間で共通に運用可能なマニュアルの策定について検討を行う	133 134		○	○	
					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が必要 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	133 134		○		

ガイドライン		答申				作業班報告書(案)				
項目	対策	項目		対策	具体的取組	頁	対策	解説	例	備考
10.教育・訓練 （2項目8対策）	(1)体制の明確化<1>									
	(2)教育・訓練の内容<7>	3.2.1	人材の育成など人的資源のセキュリティ確保	ア　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機関の整備等	将来に向けて、業界団体による研修コースの開発や大学における情報セキュリティや情報リスク管理を扱うカリキュラムの強化等、訓練機関の整備に取り組むことについて検討する	140		○		
11.現状の調査・分析及び改善 （4項目5対策）	(1)体制の明確化<1>									
	(2)基準の設定<1>									
	(3)作業の手順化<1>									
	(4)改善<2>									
12.安全・信頼性の確保等の情報公開 （2項目2対策）	(1)ネットワークの安全・信頼性の確保に係る取組状況	3.1.1	基本指針、責任の明確化など組織・体制の整備	ア　各事業者における情報セキュリティ確保に関する基本指針の公表	セキュリティ確保の基本指針や体制、その実施状況などをホームページや配布物などを通じて公表に努める	143 (1)		○		
	(2)ネットワークの事故・障害の状況<1>	4.2.3	緊急時の情報連絡（迅速な連絡・対応・報告体制）及び連携	イ　多様なメディアによる障害内容の利用者への提供	サービスの停止等のトラブルが発生した場合に障害内容や復旧状況を利用者や関係者に適切に提供する	143 (1)		○		
					現在、主に用いられているホームページの掲載のみならず、多様な情報提供媒体を通して、利用者に通知する	143 (2)		○		
					複数事業者が同一の要因でICT障害を発生させている場合等には、T-CEPTOAR等を活用して障害内容を利用者へ情報提供するための具体的な手法等を検討する	143 (2)		○		
				ウ　他社ユーザーへの障害情報等の提供	障害発生により、他社ユーザーにも影響を与えている場合は、他社ユーザーに対しても、自社ユーザーと同等レベルの情報提供ができる仕組みをT-CEPTOAR等の場を利用して構築していく	143 (2)		○		
	追加	5.1.1	バックアップ、分散化等のICT障害対策	ケ　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等	サービス稼働率・故障など品質の定義の明確化と一般への公開を行う	62	◎	○	○	設備基準 1 一般基準(15)に追加
	追加(3)	5.1.3	端末等に対する対策	エ　端末の電力確保、バッテリー寿命延長の技術開発等	サービスの欠点等をあらかじめ広く利用者に理解してもらう取組み	143 (3)	◎	○	○	