	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					
⑴　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。	◎	◎	◎	◎
⑵　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					
⑴　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。	◎	◎	◎	◎
⑵　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。	◎	◎	◎	◎
⑶　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。	◎	◎	○	○
⑷　コンピュータウィルス情報等の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。	◎	◎	◎	◎
⑸　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。	◎	◎	◎	◎
⑹　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。	◎＊	◎＊	◎＊	◎＊
⑺　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。	◎	◎	—	—
⑻　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。	◎	◎	◎	◎
⑼　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					
⑴　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。	◎	◎	◎	◎
⑵　基準の設定	データ管理基準を設定すること。	◎	◎	◎	◎
⑶　作業の手順化	データ取扱作業の手順化を行うこと。	◎	◎	◎	◎
⑷　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。	◎	◎	◎	◎
⑸　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つた場所に別に保管すること。	○	○	○	○