	ケ　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う場合は、災害時優先通信及び他の通信の疎通の状況を記録する機能を設けること。	◎	◎	—	—	—
⑼　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し、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　新しいシステムの導入に当たつては、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、ソフトウェアの不具合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　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つては、ウィ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。	◎	◎	◎	○	○
⑽　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、ftp等サービス提供に不要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機能を設けること。	◎	◎	◎	◎	◎
	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　コンピュータウィ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抑圧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。	◎	◎	◎	◎	◎