| | | | | | | |
|---|---|---|---|---|---|---|
| | ツ　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。 | ◎ | ◎ | ◎ | — | — |
| (7)　ソフトウェアの信頼性確保 | ア　ソフトウェアの要求仕様は、サービス内容及び通信需要予測を踏まえて策定すること。 | ◎ | ◎ | ◎ | ◎ | ◎ |
| | イ　ソフトウェア開発を委託する場合は、委託業者との連携により仕様誤認・設計開発面での誤認を防止すること。 | ◎ | ◎ | ◎ | ○ | ○ |
| | ウ　ソフトウェアの不具合による動作不良等を防止するための監視項目・方法を事前に確認すること。 | ◎ | ◎ | ◎ | ○ | ○ |
| | エ　ソフトウェアの試験は、商用環境に近い環境で試験を実施すること。 | ◎ | ◎ | ◎ | ○ | ○ |
| | オ　定期的にソフトウェアのリスク分析を行うとともに、更新の必要性を確認すること。 | ◎ | ◎ | ◎ | ○ | ○ |
| | カ　使用しているソフトウェアの安全・信頼性の基準及び指標を策定すること。 | ◎ | ◎＊ | ◎＊ | ○ | ○ |
| (8)　重要通信の確保 | 重要通信を扱う場合は、その通信の確保に関する取組を実施すること。 | ◎ | ◎ | ◎ | — | — |
| (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。 | ◎ | ◎ | ◎ | — | — |
| | 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、利用者への協力依頼・周知のための措置を講ずること。 | ◎ | ◎ | ◎ | — | — |

| | | | | | | |
|---|---|---|---|---|---|---|
| | キ　データ管理基準を設定すること。 | ◎ | ◎ | ◎ | ◎ | ◎ |
| | ク　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。 | ◎ | ◎ | ◎ | ◎ | ◎ |
| | ケ　データ取扱作業の手順化を行うこと。 | ◎ | ◎ | ◎ | ◎ | ◎ |
| | コ　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。 | ◎ | ◎ | ◎ | ◎ | ◎ |
| | サ　利用者の暗証番号等の秘密の保護に配慮すること。 | ◎ | ◎ | ◎ | ◎ | ◎ |
| | シ　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。 | ◎ | ◎ | ◎ | ◎ | ◎ |
| | ス　情報管理に関する内部統制ルールを整備すること。 | ◎ | ◎ | ◎ | ◎ | ◎ |
| | セ　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。 | ◎ | ◎ | ◎ | ○ | ○ |
| | ソ　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。 | ◎ | ◎ | ◎ | ○ | ○ |
| | タ　サイバー攻撃への対策を講ずるとともに、発生時には迅速に情報共有する方法を確立すること。 | ◎ | ◎ | ◎ | — | — |
| | チ　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。 | ○ | ○ | ○ | ○ | ○ |