	(4)　事故報告制度 (5)　事業継続マネジメントシステム 委託の管理 (6)　利用者への連絡 (7)　利用者への連絡
イ　保全	(1)　予防保全の手順 (2)　設備のライフサイクルの管理
ウ　安全・信頼性対策	(1)　冗長構成 ［(2)・(3)　略］ (4)　設備異常の分析 (5)　災害対策 (6)　情報通信ネットワーク安全・信頼性基準（昭和六十二年郵政省告示第七十三号）
五　サイバーセキュリティ管理・対策	
ア　サイバーセキュリティ管理手法	(1)　サイバー攻撃の脅威・対象・手法・対策 (2)　サイバーセキュリティポリシー ［(3)　略］ (4)　情報セキュリティマネジメントシステム
イ　サイバーセキュリティ管理技術	(1)　暗号化技術 (2)　PKI (3)　暗号化通信 (4)　認証技術 ［(5)　略］
ウ　物理的な対策	(1)　不正侵入対策 ［(2)　略］ (3)　可用性の確保 (4)　シンクライアント

	［新設］ ［新設］ ［新設］ ［新設］
イ　予防保全	(1)　予防保全の手順（保守計画の策定・実施、実績評価・分析等） (2)　設備のライフサイクルの管理（設備寿命・ベンダ保守限界を考慮した設備更改計画・保守計画等）
ウ　安全・信頼性対策	(1)　冗長構成（二重化／N＋1構成、2ルート化、ホットスタンバイ／コールドスタンバイ等） ［(2)・(3)　同上］ (4)　故障分析（課題抽出、再発防止策の策定・実施等） (5)　災害対策（停電対策、自然災害対策等） (6)　情報通信ネットワーク安全・信頼性基準
五　セキュリティ管理・対策	
ア　セキュリティ管理手法	(1)　脅威の分類（攻撃の対象・手法、リスク） (2)　セキュリティポリシー ［(3)　同上］ (4)　情報セキュリティマネジメントシステム（ISO／IEC27001、JIS　Q　27001等）
イ　セキュリティ管理技術	(1)　暗号化方式（共通鍵、公開鍵等） (2)　暗号鍵管理（PKI等） (3)　データ転送の暗号化（TLS等） (4)　認証技術（パスワード認証、チャレンジレスポンス認証、電子署名、電子証明書、CA、ハッシュ関数、認証サーバ、完全性保証等） ［(5)　同上］
ウ　物理的セキュリティ対策	(1)　不正侵入対策（入出管理、鍵の管理、生体認証等） ［(2)　同上］ ［新設］ ［新設］