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	
エ　サイバーセキュリティ対策	(1)　運用上の対策	
	(2)　マルウェア対策	
	[削る]	
	(3)　不正アクセス対策技術	
	(4)　セキュリティホール対策技術	
	(5)　無線LANセキュリティ対策	
	(6)　アプリケーションセキュリティ対策	
	[(7)　略]	
オ　その他情報セキュリティ対策	(1)　情報漏えい対策	
	[(2)～(4)　略]	
	(5)　個人情報管理	

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、リスク等）	
	(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 2001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]	
エ　ネットワークセキュリティ対策	(1)　マルウェア（コンピュータウィルス、ワーム、ボット等）	
	(2)　マルウェア対策技術（感染防止、検出、駆除等）	
	(3)　不正アクセス（アタック、DoS攻撃等）	
	(4)　不正アクセス対策技術（ファイアウォール、フィルタリング、侵入検知システム、侵入防止システム等）	
	(5)　セキュリティホール対策技術（脆弱性管理、セキュリティパッチ等）	
	[新設]	
	[新設]	
	(6)　[同上]	
オ　その他情報セキュリティ対策	(1)　情報漏洩対策（設備の重要情報、個人情報等）	
	[(2)～(4)　同上]	
	[新設]	