供給者管理規程比較表

大分類	中分類	小分類	米国FedRAMP	英国G-Cloud※	ドイツC5	豪州IRAP
供給者関係における情報セキュリティ	供給者関係のための情報セキュリティの方針					
		サプライチェーンのリスクマネジメントポリシーの策定・文書化	SR-1 ポリシー及び手順		SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	供給者関係の管理
		調達により生じるリスク評価の要件			SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	
		リスク評価の要件・サードパーティの分類要件			SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	
		情報の処理・保存・送信に関する情報セキュリティ要件			SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	
		従業員に対する情報セキュリティに関する意識啓発・トレーニング要件			SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	
		適用される法規制上の要件			SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	
		脆弱性・インシデント・誤動作への対処要件			SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	
		契約上の合意に関する仕様			SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	
		要件を監視するための仕様			SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	
		サードパーティが利用するサービスプロバイダに対して要件を適用するための仕様			SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	
		サプライチェーンのリスクマネジメントポリシーの評価・更新	SR-1 ポリシー及び手順			
		サプライチェーンのリスクマネジメントの管理策の実装を促進するための手順の策定・文書化	SR-1 ポリシー及び手順		SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	
		サプライチェーンのリスクマネジメントの管理策の実装を促進するための手順の評価・更新	SR-1 ポリシー及び手順			
		サプライチェーンのリスクマネジメントの担当者の指定	SR-1 ポリシー及び手順			
		サプライチェーンのリスクマネジメント計画の策定	SR-2 サプライチェーンのリスクマネジメント計画			
		サプライチェーンのリスクマネジメント計画の評価・更新	SR-2 サプライチェーンのリスクマネジメント計画			
		サプライチェーンのリスクマネジメント計画の認可されていない開示や変更からの保護	SR-2 サプライチェーンのリスクマネジメント計画			
		サプライチェーンのリスクマネジメントチームの設置	SR-2(1) SCRMチームの確立			
		サプライチェーンのリスクマネジメント活動の主導・サポート	SR-2(1) SCRMチームの確立			サイバーサプライチェーンのリスク管理活動
		サプライチェーンの脆弱性管理プロセスの確立	SR-3 サプライチェーンの管理策及びプロセス			
		サプライチェーンの管理策の実装	SR-3 サプライチェーンの管理策及びプロセス			
		供給源の多様化				
		損害の限定				
		下請業者との契約への主契約事業者の契約内容（管理策）の適用				
		分離制御（ユーザー分離、ハードウェア分離）		原則 8 ：サプライチェーンのセキュリティ／分離		
		リスク評価・評価結果の定期的なレビュー			SSO-02 サービスプロバイダ及びサプライヤーのリスク評価	サイバーサプライチェーンのリスク管理活動 マネージドサービスプロバイダの評価 外部委託されたクラウドサービスプロバイダの評価
		登録台帳の作成・維持			SSO-03 サービスプロバイダ及びサプライヤーの登録台帳	サイバーサプライチェーンのリスク管理活動 供給者関係の管理 マネージドサービス 外部委託されたクラウドサービス
		セキュリティ責任の明確化				サイバーサプライチェーンのリスク管理活動
		来歴の文書化・監視・維持				
		サプライチェーンの要素・プロセス・職員の一意の識別の確立・維持（可視化）				
		開発中・移送中のシステム・システムコンポーネントの一意の識別の追跡				
		取得したシステム・システムコンポーネントの真正性・改変有無の確認				アプリケーション、ICT機器・サービスの提供
		製品・サービスの内部構成・来歴の検証によるシステム・システムコンポーネントの完全性確保				アプリケーション、ICT機器・サービスの提供
		サプライチェーンリスクからの保護・特定・軽減のための取得戦略・ツール・方法	SR-5 取得戦略、ツール及び方法			
		重要なシステムコンポーネントの適切な供給の確保				アプリケーション、ICT機器・サービスの調達
		システム・システムコンポーネント・サービスのアセスメントの実施				
		代替サービスプロバイダ・サプライヤーへの移行に向けた分析・出口戦略			SSO-05 ベネフィットを得るための出口戦略	
供給者との合意における情報セキュリティの取扱い	各供給者との間の情報セキュリティ要求事項の確立・合意					
		通知協定	SR-8 通知協定			
		サプライチェーンの侵害の通知	SR-8 通知協定			サービスプロバイダとの契約上のセキュリティ要件
		アセスメント・監査結果の通知	SR-8 通知協定			
		内部統制システムの設計の適合性・運用効率性に関する定期的な報告	SR-8 通知協定		SSO-01 サードパーティを管理及び監視するためのポリシー及び指示	

供給者管理規程比較表

大分類	中分類	小分類	米国FedRAMP	英国G-Cloud※	ドイツC5	豪州IRAP
		契約上の取決めに対する重大な変更の通知	SR-8 通知協定			サービスプロバイダとの契約上のセキュリティ要件
		サービス提供停止の通知	SR-8 通知協定			サービスプロバイダとの契約上のセキュリティ要件
		システム・システムコンポーネント・サービスへのタンパープロテクションプログラムの実装	SR-9 耐タンパー性及び検知			
		改ざん防止技術・ツール・技法の実装	SR-9(1) システム開発ライフサイクルの複数の段階			
		組織の資産に対する供給者のアクセスへの対処プロセス・手順				サービスプロバイダとの契約上のセキュリティ要件 サービスプロバイダによるシステム及びデータへのアクセス
		組織の情報を扱う供給者・IT 基盤を提供する可能性のある供給者との合意の確立方法				サービスプロバイダとの契約上のセキュリティ要件
		ICTサービス・製品のサプライチェーンに関連する供給者との合意の確立方法				
ICTサプライチェーンにおける情報セキュリティの取扱い	ICTサプライチェーンに関連する情報セキュリティリスクを管理するためのプロセス及び手順					
		サプライチェーン関連リスクの評価・レビュー	SR-6 サプライヤのアセスメント及びレビュー	原則 8 ：サプライチェーンのセキュリティ／機密データ		
		システム・システムコンポーネント・サービスに関連するサプライチェーン要素・プロセス・行為者に対するテスト・分析		原則 8 ：サプライチェーンのセキュリティ／データ共有		
		システム・システムコンポーネント・サービスのサプライチェーン関連情報の保護				
		システム・システムコンポーネントの検査・改ざん検知	SR-10 システムまたはコンポーネントの検査		SSO-04 要件に準拠しているかどうかの監視	
		偽造コンポーネントの検知・システム侵入防止ポリシー・手順の策定・実装	SR-11 コンポーネントの真正性			
		偽造コンポーネントを検知するためのトレーニング	SR-11(1) 偽造防止トレーニング			
		修理・サービス復帰を控えるコンポーネント・修理されたコンポーネントの構成管理の維持	SR-11(2) コンポーネントのサービス及び修理のための構成管理			
		偽造コンポーネントの精査				
		偽造コンポーネントの供給源の外部報告組織への報告	SR-11 コンポーネントの真正性			
		組織のシステム・データへの不正アクセスの外部報告組織への報告				サービスプロバイダによるシステム及びデータへのアクセス
		コンポーネントの廃棄	SR-12 コンポーネントの廃棄			
		クラウドサービス利用者に対する情報セキュリティ水準の維持・向上のための仕組みの整備				
		クラウドサービスのサプライチェーンに関わる各供給者に対する情報セキュリティの目的を達成するためのリスク管理活動の実施の要求				
供給者のサービス提供の監視・レビュー・変更管理	供給者の管理・監視					
		供給者に対する組織のセキュリティ要求事項の遵守の要求	SA-9 外部システムサービス	原則 8 ：サプライチェーンのセキュリティ		
		ユーザーの役割・責任の明確化・文書化	SA-9 外部システムサービス			
		供給者の情報セキュリティの実践の監視・レビュー・評価・管理	SA-9 外部システムサービス SR-8 通知協定			
		供給者に対する組織のリスクアセスメントの実施	SA-9(1) リスクアセスメント及び組織承認 SR-8 通知協定		SSO-02 サービスプロバイダ及びサプライヤーのリスク評価	サイバーサプライチェーンのリスク管理活動 マネージドサービスプロバイダの評価 外部委託されたクラウドサービスプロバイダの評価
		供給者との信頼関係の確立・維持				
		供給者の利益と組織の利益の一致性確認				
	供給者のサービス提供の管理・監視					
		供給者のサービス提供の監視・レビュー・監査				
		サービス取得・アウトソーシングの承認状況の確認	SA-9(1) リスクアセスメント及び組織承認			アプリケーション、ICT機器・サービスの調達
		機能・ポート・プロトコル・サービスの特定	SA-9(2) 機能、ポート、プロトコル及びサービスの特定			
		処理・保管・サービスの場所の制限	SA-9(5) 処理、保管及びサービスの場所			
		暗号鍵の排他的管理の維持				
		保存された情報の完全性をチェックする機能の提供				
	供給者のサービス提供の変更に対する管理					
		供給者のサービス提供の変更の監視・レビュー・評価・管理				

※英国G-Cloudは、クラウドサービスプロバイダーに対して、「Cloud Security Guidance」が定めるクラウドセキュリティ原則を守ることを求めており、クラウドサービスプロバイダーが遵守すべき管理策を定めていないことに留意する必要がある。表中の記載は、クラウドセキュリティ原則の目標や推奨される実装アプローチをもとにした記載となっている。