インシデント規程比較表

大分類	中分類	小分類	米国FedRAMP	英国G-Cloud※	ドイツC5	豪州IRAP
インシデント対応態勢	インシデント対応のポリシー、計画、手順の作成	インシデント処理能力の確立・実装（自動化プロセス、システム）	IR-4 インシデント対応			
		経営層のコミットメント				
		ポリシーの策定・文書化（目的、適用範囲、役割・責任の明確化）	IR-1 ポリシー及び手順		SIM-01 セキュリティインシデント管理ポリシー	サイバーセキュリティインシデント管理ポリシー
		ポリシーの実行・管理・更新（担当者、頻度の明確化）	IR-1 ポリシー及び手順			サイバーセキュリティインシデント管理ポリシー
		計画の策定・文書化（ミッション、戦略、目標、対応措置の明確化）	IR-8 インシデント対応計画			サイバーセキュリティインシデント管理ポリシー
		計画の実行・管理・更新（担当者、頻度の明確化）	IR-8 インシデント対応計画 IR-9 情報流出対応			サイバーセキュリティインシデント管理ポリシー
		手順の策定・文書化	IR-1 ポリシー及び手順 IR-4 インシデント対応	原則５：運用のセキュリティ／インシデント管理（インシデント管理プロセス）		
		インシデント対応計画の策定・準備手順				
		インシデントの監視・検知・分析・報告手順			SIM-01 セキュリティインシデント管理ポリシー	
		ログの取得手順				
		法的証拠の取扱い手順				
		インシデント・脆弱性の評価・決定手順			OPS-20 脆弱性、誤動作及びエラーの管理 – 測定、分析及び評価手順 SIM-01 セキュリティインシデント管理ポリシー	
		インシデント対応手順				
		手順の管理・更新（担当者、頻度の明確化）	IR-1 ポリシー及び手順		OPS-20 脆弱性、誤動作及びエラーの管理 – 測定、分析及び評価手順	
		外部の関係者との情報共有				
		顧客への対応			OPS-21 インシデント発生時におけるクラウドサービスの顧客の関与 SIM-03 セキュリティインシデントの文書化及び報告	
		マスコミへの対応				
		法執行機関への対応				
		インシデント報告組織への対応				
	インシデント対応組織の編成					
		セキュリティオペレーションセンターの設置			SIM-05 評価及び学習のプロセス	
		チーム構成・対応要員の配置・必要スキル	IR-4(11) 統合インシデント対応チーム		SIM-01 セキュリティインシデント管理ポリシー	
		広報活動体制の構築				
		組織内外との依存関係、連携・連絡体制の構築			SIM-04 セキュリティインシデントを中央の対応組織に報告するユーザーの義務	ASDに対するサイバーセキュリティインシデントの報告
	インシデント対応組織による支援					
		アドバイザリーの提供	IR-7 インシデント対応支援 IR-7(1) 情報及びサポートの可用性のための自動化されたサポート			
		サポートの提供	IR-7 インシデント対応支援 IR-7(1) 情報及びサポートの可用性のための自動化されたサポート			
インシデント処理プロセス、インシデント対応措置の実施						
	準備					
		リソース・ツール・ケイパビリティの確保・実装	IR-4(4) 情報の相互関連付け IR-4(6) インサイダー脅威			信頼できるインサイダープログラム 十分なデータソース及びツールへのアクセス
		インシデントの予防				
		パッチの管理、脆弱性の管理	RA-5 脆弱性の監視及びスキャン RA-5(2) スキャンする脆弱性の更新 RA-5(3) カバレッジの幅及び深さ RA-5(4) 検出可能な情報 RA-5(5) 特権アクセス RA-5(8) 過去の監査ログのレビュー RA-5(11) 公開開示プログラム	原則５：運用のセキュリティ／脆弱性管理（脅威の監視、脆弱性管理プロセス、緩和策を適用するためのタイムスケール）	OPS-18 脆弱性、誤動作及びエラーの管理 – コンセプト OPS-19 脆弱性、誤動作及びエラーの管理 – 侵入テスト OPS-22 既知の脆弱性に対するテスト及び文書化 OPS-19 脆弱性、誤動作及びエラーの管理 – システムの強化	パッチ管理プロセス及び手順 ソフトウェアレジスタ 不足しているパッチまたはアップデートのスキャン 脆弱性にパッチを適用するタイミング サポートの終了
		許可されていない通信トラフィックの拒否				
		不必要なプログラムの無効化、利用制限				
		重要な機能の冗長化				
		定期的なリスク評価				
		意識啓発、トレーニングやテストの実施・更新	IR-2 インシデント対応トレーニング IR-2(1) シミュレーションイベント IR-2(2) 自動化されたトレーニング環境 IR-3 インシデント対応テスト IR-3(2) 関連計画との調整 IR-4 インシデント対応 IR-9(2) トレーニング		SIM-02 セキュリティインシデントの処理	
	検知・分析					
		インシデントの兆候の監視、検知	IR-5 インシデント監視 IR-5(1) 自動化された追跡、データ収集及び分析	原則１３：監査情報と顧客への警告／監査情報（データ形式、記録される情報、基盤サービスから取得されるログ、監査情報の保護）		ASDに対するサイバーセキュリティインシデントの報告
		インシデントの分類			SIM-02 セキュリティインシデントの処理	
		インシデントの分析				
		調査・分析の実施	IR-5(1) 自動化された追跡、データ収集及び分析		SIM-02 セキュリティインシデントの処理	
		インシデントの影響評価				

インシデント規程比較表

大分類	中分類	小分類		米国FedRAMP	英国G-Cloud※	ドイツC5	豪州IRAP
			インシデントの優先順位付け			SIM-02 セキュリティインシデントの処理	
		インシデントの文書化		IR-5 インシデント監視			サイバーセキュリティインシデント登録台帳
		インシデントの通知・報告		IR-6 インシデント報告 IR-6(1) 自動化された報告 IR-6(3) サプライチェーンとの連携 IR-9 情報流出対応	原則５：運用のセキュリティ／インシデント管理（インシデントの通知） 原則１３：監査情報と顧客への警告／セキュリティ警告（アラートの通知、アラートの文書化、アラート通知の処理）	OPS-21 インシデント発生時におけるクラウドサービスの顧客の関与 SIM-03 セキュリティインシデントの文書化及び報告	サイバーセキュリティインシデントの報告 顧客及び一般の人々に対するサイバーセキュリティインシデントの報告
	封じ込め・根絶・復旧						
		戦略・計画の立案					サイバーセキュリティインシデント対応計画の策定
		段階的取扱いの実行					
		証拠の収集・保全・記録					証拠の完全性の維持
		原因調査					
			フォレンジック調査				
		攻撃、汚染システムの特定		IR-9 情報流出対応			
		インシデントの評価（対応の有効性改善、他の組織への影響最小化）					
		インシデントの封じ込め					
			サーバーのシャットダウン				
			システム・ネットワークの隔離	IR-9 情報流出対応			悪意あるコードの感染に対する処理及び封じ込め
			サービス・接続の無効化・制限				データ流出に対する処理及び封じ込め 悪意あるコードの感染に対する処理及び封じ込め
			悪用可能な脆弱性の修正				
			侵入ルートの除去				システム侵入に対する処理及び封じ込め
		インシデントの根絶		IR-9 情報流出対応			
			悪用された脆弱性の修正				
			悪意のあるコード・不適切データの削除	IR-9 情報流出対応			悪意あるコードの感染に対する処理及び封じ込め
			アクセス権限のリセット	IR-9(4) 認可されていない職員への露出			
			業務運用の継続性確保	IR-9(3) 流出後の運用			
		インシデントの復旧					
			元の良好な状態への回復				悪意あるコードの感染に対する処理及び封じ込め
			侵入・侵害に対する修復				システム侵入に対する処理及び封じ込め
			再発防止策の実装				
			追加の監視の実施				
		インシデント対応活動の記録				SIM-03 セキュリティインシデントの文書化及び報告	
	インシデント後の対応						
		追跡分析、追跡レポートの作成					
		反省会の開催、得られた教訓の学習・活用				SIM-05 評価及び学習のプロセス	

※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。