海外調査比較表（制度概要）

項目	比較・分析観点	ISMAP	FedRAMP（米国）	G-Cloud（英国）	C5（ドイツ）	IRAP（オーストラリア）
制度の概要	制度概要	政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度	FedRAMP の根拠となる法律は、2002年に制定された、連邦政府機関に対して情報および情報システムのセキュリティを強化するためのプログラムの開発・文書化・実践を義務付けた FISMA：Federal Information Security Management Act（連邦情報セキュリティマネジメント法）である。FedRAMP（Federal Risk and Authorization Management Program）は、政府機関が導入するクラウドサービスに求められるセキュリティを評価・認証するための標準的プロセスを定める。	中央政府向けのクラウドサービスを対象としたセキュリティ評価制度	国家の機密データを処理できるすべてのIT製品及びITサービスを対象としたセキュリティ評価制度	登録セキュリティ評価者プログラム
	制度の根拠	政府情報システムにおけるクラウドサービスのセキュリティ評価制度の基本的枠組みについて	Federal Information Security Management Act(FISMA)	The Technology Code of Practice	Verschlusssachenanweisung(VSA)	Australian Government Cloud Computing Policy
	制度発足時期（運用期間）	2020年6月より開始	2011年より開始	2013年より開始	2016年より開始	2014年より開始（クラウドサービスの認証制度は2020年3月に終了）
	調達先	政府機関	連邦政府機関	中央政府機関	連邦政府機関及び連邦警察のIT製品及びITサービスの調達者	-
	登録件数（サービス名）	令和6年6月現在、69サービスを登録済。	令和6年2月現在、327サービスを登録済。	-	-	-
運営主体	運営主体	内閣サイバーセキュリティセンター、デジタル庁、総務省、経済産業省	General Services Administration(GSA)	The Crown Commercial Service(CCS)	Federal Office for Information Security(BSI)	Australian Signals Directorate(ASD)
	運営主体の役割	・ クラウドサービスが満たすべき統一的なセキュリティ基準の策定 ・ 当該基準が適切に実施されているか監査するプロセスを経たうえでの安全性が評価されたクラウドサービスの登録 ・ 監査機関の登録や監査実務における基準等の策定	・ NIST SP800-53に基づく、クラウドサービスが満たすべき統一的なセキュリティ基準の策定 ・監査機関の登録 ・当該基準に基づく監査(適合性評価)、認証は実施していない（監査(適合性評価)は第三者監査機関が、認証はJABまたは各省庁が実施している） ・ Market Placeへのクラウドサービスの登録は、各省庁による認証プロセスの場合のみ実施している（JAB P-ATOによる認証プロセスの場合は、JABが登録を実施している）	・ クラウドサービスが満たすべき統一的なセキュリティ基準の策定 ・ クラウドサービスプロバイダーの申請情報の内容確認とG-Cloud契約可否の判断・承認・通知 ・ 適合性評価を行う第三者監査機関に対する指示 ・ Digital Market Placeへのクラウドサービスの登録は実施していない（登録主体はGovernment Digital Service）	・ クラウドサービスを含め、IT製品及びITサービスが満たすべき統一的なセキュリティ基準の策定 ・当該基準に基づく監査(適合性評価)、認証、登録は実施していない（監査(適合性評価)や適合証明書の付与は公認会計士が実施している）	・ IRAP評価者の承認
公開情報リスト（URL等）	公開先（URL等）	ISMAPポータル https://www.ismap.go.jp/	FedRAMPポータル https://www.fedramp.gov/	G-Cloudポータル https://www.applytosupply.digitalmarketplace.service.gov.uk/	C5ポータル https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html	IRAPポータル https://www.cyber.gov.au/irap
	公開情報リスト（URL等） 認証クラウドサービスリスト（URL等）	ISMAP登録クラウドサービスリスト https://www.ismap.go.jp/csm?id=cloud_service_list	FEDRAMP MARKETPLACE https://marketplace.fedramp.gov/products	-	-	-
	公開内容	・クラウドサービスリスト ・制度概要 ・規程類 ・PR／研修（動画） ・その他	・ 制度概要 ・認証プロセス ・規程類 ・ FEDRAMP MARKETPLACE ・その他	・ 制度概要 ・申請プロセス ・その他	・ 制度概要 ・規程類 ・その他	・ 制度概要 ・認証プロセス ・規程類 ・その他

海外調査比較表（規定類（制度規程、管理策等））

項目	比較・分析観点	ISMAP	FedRAMP（米国）	G-Cloud（英国）	C5（ドイツ）	IRAP（オーストラリア）
管理策名／管理策数	管理策名	クラウドサービスが満たすべき要件・基準として、 ・ガバナンス基準 ・マネジメント基準、 ・管理策基準 の3種類から構成されるISMAP管理基準を策定・公開	・ 連邦政府情報処理規格：FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems ・ NIST SP800-53：Security and Privacy Controls for Federal Information Systems and Organizations ・ NIST SP 800-60 Vol. 2 Rev. 1 Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices	G-Cloudが定める基準（管理策基準）のうちの1つとして、Cloud Security Principlesを定めている。それ以上の詳細な基準（管理策基準）や、クラウドサービスに求める要件についてはクラウドサービスを調達する政府機関側で設定	・2016年に、BSIにおいて、C5におけるIT製品及びITサービスが満たすべき基準を策定・公開 ・その後、FedRAMPとの連携を目的に、2019年から改訂作業を開始し、2020年に改訂版を公開	-
	管理策数	・ガバナンス基準については、4桁管理策レベルで18の管理策がある ・マネジメント基準については、3桁管理策レベルで21の管理策、4桁管理策レベルで64の管理策がある ・管理策基準については、3桁管理策レベルで121の管理策がある。 ※4桁管理策に関しては選択制	FIPS 199 に規定されているセキュリティ影響レベルは、Low（限定的な影響）、Moderate（深刻な影響）、High（経済危機等につながる破滅的な影響）となっており、セキュリティ影響レベル High, Moderate, Low それぞれにおいて規定されているセキュリティ管理策の数は以下の通り High：421 Moderate：325 Low：125	詳細な基準（管理策基準）や、クラウドサービスに求める要件についてはクラウドサービスを調達する政府機関側で設定しているため該当せず。	17の主題分野に分けられた125の基準で構成される。	-
	管理策のレベル分け	クラウドサービスに求めるセキュリティ上の影響度レベルによる基準のレベル分けは実施していない。	FIPS 199 に基づく High、Moderate、Low の3段階のセキュリティ影響レベルが設定されているほか、セキュリティ影響度が低である SaaS = LI-SaaS を対象とする基準も追加されている。	クラウドサービスに求めるセキュリティ上の影響度レベルによる基準のレベル分けは実施していない。	クラウドサービスに求めるセキュリティ上の影響度レベルによる基準のレベル分けは実施していない（なお、C5が定める基準には、クラウドサービスプロバイダーが満たすべき必要最低限の基準を規定した基本的なコモンクライテリアと、より高いレベルの情報セキュリティを求めるクラウドサービスプロバイダーが追加的に実施すべき基準を規定した追加のコモンクライテリアの2種類が存在する）	-

海外調査比較表（認証プロセス）

項目	比較・分析観点	ISMAP	FedRAMP（米国）	G-Cloud（英国）	C5（ドイツ）	IRAP（オーストラリア）
認証機関	認証に関係する組織・機関	ISMAPの最高意思決定機関で、有識者と制度所管省庁（内閣サイバーセキュリティセンター、デジタル庁、総務省、経済産業省）より構成されるISMAP運営委員会	GSA 内の FedRAMP PMO、JAB(Joint Authorization Board：国土安全保障省(DHS)、一般調達局(GSA)、国防総省(DOD)の最高情報責任者により構成される組織)、連邦政府機関、認証担当者(Authorizing Official (AO))、第三者評価機関(3PAO : Third Party Assessment Organizations)	The Crown Commercial Service (CCS)。CCSの指示のもと活動する第三者監査機関。Government Digital Service（GDS）。	公認会計士（C5が定める基準に基づく監査を行う公認会計士は、業務を行うにあたりC5に特化した資格の認定を受ける必要はない）	-
	認証に関係する組織・機関の役割	・ISMAP運営委員会は、実施結果報告書を含むサービス登録に必要となる申請書類をクラウドサービスプロバイダーから受領し、ISMAP クラウドサービス登録規則に基づいて ISMAP クラウドサービスリストへのクラウドサービスの登録審査を行う責任を負う。	JAB による認証では、クラウドサービスプロバイダーが提供するクラウドサービスのセキュリティに対する第三者評価機関による評価結果に基づいて、JAB が、クラウドサービスプロバイダーに対して運用許可(P-ATO(Provisional Authority to Operate))を発行する。 各省庁による認証では、各省庁が個別に、クラウドサービスプロバイダーが提供するクラウドサービスのセキュリティに対する評価を実施する。 セキュリティ評価は、クラウドサービスプロバイダーが契約した第三者評価機関(3PAO : Third Party Assessment Organizations)により実施され、評価結果に基づいて、クラウドサービスプロバイダーに対して運用許可(ATO(Authority to Operate))が発行される。	The Crown Commercial Service (CCS)がG-Cloudの運営主体。Government Digital Service（GDS）が政府全体のクラウドへの移行やデジタル化の推進を実施。第三者監査機関がCCSの指示のもと監査を実施。	公認会計士は、すべての基準を満たしているIT製品およびITサービスのプロバイダーに対して、適合証明書を付与している。	-
認証プロセス	認証プロセス内容	ISMAP運営委員会における審査を実施し、登録が決定したクラウドサービスについては、ISMAPクラウドサービスリストに登録し、Webサイトを通じて公開する。	JABによる認証と省庁による認証の違い ＊ JAB(Joint Authorization Board) による認証 フェーズ１：FedRAMP Readiness 認証 フェーズ２：Full Security Assessment フェーズ３：Authorization Process ＊ 省庁による認証 フェーズ 1： Partnership Establishment フェーズ 2： Full Security Assessment フェーズ 3： Authorization Process	クラウドサービスプロバイダーがDigital Market Placeに登録する際に自己申告する内容を、CCSが確認する。	BSIは、C5の運営において、C5が定める基準に基づく監査や、監査結果に基づくIT製品およびITサービスの認証・認定を行っていない。	-

海外調査比較表（監査体制）

項目	比較・分析観点	ISMAP	FedRAMP（米国）	G-Cloud（英国）	C5（ドイツ）	IRAP（オーストラリア）
監査概要	監査の概要	・ISMAP運営委員会が審査を実施し、その結果、登録が認められた監査機関が、監査基準等に準拠して本制度における監査業務を実施し、その実施結果を業務依頼者に報告する責任を負う。	クラウドサービスの認証には、JAB(Joint Authorization Board：国土安全保障省(DHS)、一般調達局(GSA)、国防総省(DOD)の最高情報責任者により構成される組織)による認証と各省庁による認証がある。	G-Cloudが定める基準に基づく監査は、クラウドサービスプロバイダーがサービスごとに自己申告するセキュリティの取組等について、サプライヤーの信用スコア調査、サプライヤーに対して直接の問い合わせ調査、サプライヤーの申請書に記載されている情報が正しいかを確認するための、サービスのランダムな抜き打ち検査。	C5が定める基準に基づく監査は、公認会計士が、IT製品およびITサービスのプロバイダーから提出された言明書をもとに、ISAE 3000（国際保証業務基準3000）に基づき行っている。	-
監査手法	監査方法	・監査機関は、標準監査手続に準拠して自ら手続を実施する。 ・監査の内容においては、ある時点における個別管理策の実装状況を確認する整備状況評価、一定期間における個別管理策の運用状況を、サンプリング等により確認する運用状況評価の双方が含まれる。 ガバナンス基準及びマネジメント基準に対応する標準監査手続は整備状況評価 に関する手続 のみ、管理策基準に対応する標準監査手続は原則、整備状況評価及び運用状況評価 に関する 手続から構成される。 業務実施者が監査証拠を入手するための手段をいい、標準監査手続においては、 ISMAP 管理基準の性質を踏まえて、 質問、閲覧、観察の 3 つの技法を想定。	監査方法に関する規定はなく、監査を実施する機関によって異なる。 一般的には、以下の通り。 ➢ JAB(Joint Authorization Board) による認証の場合 ✓ 監査実施前に、FedRAMP Ready に指定されるためのアセスメントを実施し、監査機関が PMO に Readiness Assessment Report (RAR) を提出する。 ✓ PMO によるレビューの結果、何らかの問題が見つかった場合、関係者によるミーティングを開催して、CSP が FedRAMP Ready になるために何が必要であるかについて議論する。 ✓ Readiness Assessment Report が承認された場合、対象となるクラウドサービスは FedRAMP Ready に指定され、FedRAMP Marketplace において広告される。 ✓ 監査機関は、Security Assessment Plan (SAP) を作成し、対象となるクラウドサービスに対して完全なセキュリティアセスメントを実施するとともに、Security Assessment Report (SAR) を作成する。 ➢ 省庁による認証の場合 ✓ CSP は、CSP のシステムが、どの程度 FedRAMP のセキュリティコントロールと整合しているかを示す System Security Plan (SSP)を作成する。 ✓ 監査機関が、SSP に基づいてシステムのテストを実施し、テストで発見された事項の詳細や、FedRAMP 認証に向けた勧告が記載された Security Assessment Report (SAR)を作成する。 ✓ CSP は、Security Assessment Report に基づいて、監査機関によるインプットが反映された、テストで発見された事項に対処するための計画が記載された POA&M を作成する。	CCSの指示のもと活動する第三者監査機関がクラウドサービスプロバイダーがサービスごとに自己申告するセキュリティの取組等について、サプライヤーの信用スコア調査、サプライヤーに対して直接の問い合わせ調査、サプライヤーの申請書に記載されている情報が正しいかを確認し、The Technology Code of Practiceの5つの要求項目を満たすかどうかの適合性を評価・検証を実施する。	・C5が定める基準に基づく監査には、タイプⅠの監査とタイプⅡの監査の2種類がある。タイプⅠの監査は、監査時点において管理策が特定の基準を満たすように適切に設計・実装されているかどうかを監査するものである ・他方、タイプⅡの監査は、タイプⅠの監査をサブセットとし、加えて管理策が、過去の特定の期間にわたって、適切に運用されていたかどうかを監査するものである。	-
	情報システム変更時の監査範囲・監査方法	クラウドサービスについて重大な統制変更または重大な統制変更につながり得る事象が発生した場合、「重大な統制変更届出書」による変更届けを行い、ISMAP運営委員会による審査、判断を行う。	省庁は、運用が許可されたクラウドサービスを継続的にモニタリングし、クラウドサービス事業者が提供する月次および年次の報告書をレビューすることにより、情報システムに変更があった場合に、セキュリティ要件が満たされるかどうかの判断を行う。	G-Cloudの適合性証明に関する契約を締結した後に、サービスの追加を行うことは出来ず、次回のG-Cloudフレームワークの更新の際、新規申請を行わなければならない。そのため、原則として情報システム変更時の監査は実施されない。（G-Cloudの適合性証明に関する契約を締結した後の契約期間中に変更できるのは、サービス名、サービスの説明等の概要情報と、サービスの削除のみ。CCSに申請が必須だが、価格情報とその根拠文章を更新することが出来る。）	・公認会計士がタイプⅡの監査を行った後で、クラウドサービスプロバイダー側で情報システムが変更された場合、公認会計士は、次回のタイプⅡの監査において、変更された部分がC5が定める基準を満たしているかを含め、すべての基準について適合性を評価している ・タイプⅡの監査は、管理策が、過去の特定の期間にわたって、適切に運用されていたかどうかを監査するものであるため、情報システムが変更された場合にその都度再監査を行うことまでは必要はない	-

海外調査比較表（直近の制度の状況変化）

項目	比較・分析観点	ISMAP	FedRAMP（米国）	G-Cloud（英国）	C5（ドイツ）	IRAP（オーストラリア）
規定類の更改	規定類の更改	–	・覚書M21-31、覚書M22-09に対応した要件の追加 ・NIST SP800-53のRev.4からRev.5への改訂に伴うFedRAMP Security Controls Baselineの改訂 ・3PAO Obligations and Performance Guideの改訂 ・FedRAMP Collaborative ConMon Quick Guide ・FedRAMP Incident Communications Proceduresの改訂	–	–	–
組織体制の見直し	組織体制の見直し	–	–	・Digital Marketplaceを使用したクラウドサービスの政府調達の終了 ・政府のデジタル調達の手段としてのPublic Procurement Gatewayの新設	–	–
登録クラウドサービスの増減	登録クラウドサービスの増減	–	・2020年9月に登録サービスが200に達してから登録サービスが増加し、2024年2月の登録サービスは327。	–	–	–