FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
制度概要	
制度の概要	FedRAMP の根拠となる法律は、2014年に制定された「Federal Information Security Modernization Act of 2014(FISMA2014)」である。FISMA2014は、2002年に制定された「 Federal Information Security Management Act of 2002 (FISMA) 」を改正し、連邦政府機関の情報セキュリティポリシーとその実践に関するOMB局長の監督権限を再定義したほか、連邦政府機関に対して連邦政府機関の情報を保護することを義務付けた。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た。 その後、2016年7月にOMBが改訂した「Circular A-130 - Managing Information as a Strategic」においては、連邦政府機関が FISMA2014 を実装する場合、米国国立標準技術研究所 (NIST) の標準とガイドラインを使用する必要があることを規定した。 さらに、米国の一般法及び恒久法を主題ごとに統合し、成文化している「United States Code」の第44編（Public Printing And Documents）第36章（Management And Promotion Of Electronic Government Services）の中に、以下に示す条文からなる「FedRAMP Authorization Act」が追加され、2022年12月に公布されている。 第3607条（定義） 第3608条（FedRAMP） 第3609条（GSAの役割と責任） 第3610条（FedRAMP Board） 第3611条（独立した評価） 第3612条（外国の利害関係の申告） 第3613条（政府連邦機関の役割と責任） 第3614条（OMBの役割と責任） 第3615条（議会への報告（GAO報告書）） 第3616条（Federal Secure Cloud Advisory Committee） 「FedRAMP Authorization Act」に基づき、GSAの組織内にFedRAMP PMO（Program Management Office）とFedRAMP Boardが設置されているほか、それぞれの役割と更なる責任が確立されている。 OMBは、2024年7月25日に、「M-24-15：Modernizing the Federal Risk and Authorization Management Program（FedRAMP）」を施行し、この覚書によって連邦CIOが2011年12月8日に施行した覚書「Security Authorization of Information Systems in Cloud Computing Environments」を置き換えるとともに、FedRAMPのビジョンや、FedRAMPの承認を受けるクラウドサービスのスコープ、承認プロセス、FedRAMPを構成するステークホルダーの役割と責任を最新のものに更新している。

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
制度の根拠	Federal Information Security Modernization Act of 2014 (FISMA2014) Circular A-130 - Managing Information as a Strategic FedRAMP Authorization Act M-24-15 : Modernizing the Federal Risk and Authorization Management Program（FedRAMP）
運営主体	General Services Administration(GSA)
運営主体の役割	・ 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、FedRAMP PMOが省庁からの申請を受け実施している。
利害関係者（制度を構成する者）	・運営組織のGeneral Services Administration(GSA) ・FedRAMPプログラムの改善を協議するガバナンス機関のFedRAMP Board（連邦政府の幹部で構成） ・運用的な観点の諮問機関のFSCAC（Federal Secure Cloud Advisory Committee）（連邦政府および民間で構成） ・技術的な観点の諮問機関のFedRAMP Technical Advisory Group (TAG)（連邦政府の技術専門家で構成） ・FedRAMPプログラムの改善を協議するJAB（Joint Authorization Board）（連邦政府のクラウドコンピューティングの専門家で構成） ※以前はJABによる認証プロセスで、暫定承認等を実施していた ・FedRAMP認証の認証プロセスに関わるCSP、Third Party Assessment Organizations（3PAO）、FedRAMP PMO、省庁

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
利害関係者の役割	・FedRAMPの制度運営：General Services Administration(GSA) ・FedRAMPのポリシーへのレビュー・承認、および審査・承認プロセスの開発・更新等について助言を行う。加えて、連邦政府に向け、FedRAMP認証の承認に関する知見を拡大する。：FedRAMP Board ・FedRAMPの運用調査を行い、審査・承認プロセスの開発・更新等について助言を行う諮問機関：FSCAC ・FedRAMPに対しクラウド技術に関する知見と経験を用いて、審査・承認プロセスの開発・更新等について助言を行う諮問機関：TAG ・FedRAMPプログラムの改善について協議する：JAB（Joint Authorization Board） ※以前はJABによる認証プロセスにおいて、FedRAMP認証に関する暫定承認等を実施していた ・FedRAMPの認証を取得するための情報提供等：CSP ・FedRAMP認証を取得するCSPへの検証、支援：Third Party Assessment Organizations（3PAO） ・FedRAMP認証に係る審査、承認：FedRAMP PMO ・FedRAMP認証を取得するCSPとの協議、フィードバック、支援、承認、最終的なリスクの受け入れ：省庁
調達先	連邦政府機関
管理基準	
クラウドサービスが満たすべき要件・基準（管理策）	GSAは、「NIST SP800-53 Security and Privacy Controls for Information Systems and Organizations（以下、NIST SP800-53という。）」で規定された管理策をもとに、High、Moderate、Low、LI-SaaSの各レベルで遵守が求められるベースライン管理策を取りまとめた「FedRAMP Security Controls Baseline」を提供している。 NIST SP800-53が、2020年9月23日にRev.4からRev.5に改訂されたことを受けて、GSAは、2023年5月30日に、これまでの「FedRAMP Security Controls Baseline」にRev.5の改訂内容を反映した「FedRAMP Security Controls Baseline」の改訂版を提供している。
基準のレベル分け	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。

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
管理策の内容 (例：管理策数や管理策の違いに関する考え方)	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)となっている。 最新の「FedRAMP Security Controls Baseline」において規定されている、セキュリティ影響レベル High, Moderate, Low それぞれのセキュリティ管理策の数は以下の通り High：410 Moderate：323 Low：156
クラウドサービスの種類やセキュリティ上の影響レベルごとの異なる基準の策定状況	クラウドサービスの種類(SaaS、PaaS、IaaS)ごとに異なるセキュリティ基準を策定してしない。 セキュリティ上の影響レベルによって求められるセキュリティ管理策の数が異なるが、異なる基準は策定されていない。
IaaS/PaaS/SaaSのレベル分けの考え方	SaaS、PaaS、IaaS というクラウドサービスの種類ごとに異なるセキュリティ基準を策定してしない。 セキュリティ影響度が低である SaaS(LI-SaaS)を対象とする認証プロセスが規定されている。
基準レベルの評価方法	High ： 機密性、完全性、または可用性の損失が、組織活動、組織資産、または個人に致命的または壊滅的な悪影響を及ぼすことが予想されうる。 Moderate ： 機密性、完全性、または可用性の損失が、組織活動、組織資産、または個人に重大な悪影響を及ぼすことが予想されうる。 Low ： 機密性、完全性、または可用性の損失が、組織活動、組織資産、または個人に限定的な悪影響を及ぼすことが予想されうる。

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
管理策の言明の考え方（非言明の考え方）	FedRAMPは、管理策の言明に関して、CSPが管理策の実装状況や実装責任を明らかにし、SSPとその添付書類のレビューを行う3PAOに対して、その要約を提供できるようにするためのテンプレートを2種類（「FedRAMP High Control Implementation Summary (CIS) Workbook Template」と「FedRAMP Low or Moderate Control Implementation Summary (CIS) Workbook Template」の2種類）提供している。 管理策の実装状況については、当該テンプレートにおいて用意されている、①実装済み、②部分的な実装、③予定中、④代替策の実装、⑤未実装という5つの選択肢の中から、CSPが該当する実装状況を選定している。 また併せて、管理策の実装責任についても、当該テンプレートにおいて用意されている、①サービスプロバイダー側の組織、②サービスプロバイダー側のシステム固有、③上記①と②の両者、④ユーザー側のシステム固有（ユーザーによる設定・構成）、⑤ユーザー側のシステム固有（ユーザーによる提供）、⑥サービスプロバイダー側とユーザー側の責任分担、⑦既存の承認からの継承という7つの選択肢の中から、CSPが該当する実装の責任主体を選定している。 このように管理策の言明は、あくまでCSPが自らの判断で管理策ごとの実装状況や実装責任を明確にするという形で行われており、言明及び非言明の定義や判断基準が設けられているわけではない。 なお、当該テンプレート上で要約される管理策ごとの実装状況や実装責任に関する情報は、SSPやSSPに関連するさまざまな添付書類と一緒に3PAOによってレビューされている。
他のクラウドサービス利用時の考え方	FedRAMPの承認を受けるクラウドサービスに接続される外部サービスや外部サービスに関連するシステムに関して、他のクラウドサービスとの間での相互接続を通じて他のクラウドサービスに関連するシステム内で連邦政府機関のデータとそのメタデータが扱われている場合は、それらのデータが適切に保護されるよう、他のクラウドサービスをFedRAMPの承認を受けるクラウドサービスの承認境界内に含める必要がある。Authorizing Officials（AO）は、上記の観点からFedRAMP承認パッケージをレビューし、連邦政府機関のデータとそのメタデータに対する潜在的なリスクが存在しないかどうかを確認する。 なお、他のクラウドサービスが既にFedRAMPの承認を受けている場合、CSPはその情報をFedRAMP承認パッケージに反映する必要があるが、FedRAMPの承認を受けるクラウドサービスの承認境界内に含める必要はない。
重大な統制変更の考え方	FedRAMP承認を受けたクラウドサービスのシステムに関する重大な変更を行う場合の必要となる手続きについては、「FedRAMP Continuous Monitoring Strategy Guide」において規定されており、具体的には、CSPは、計画しているクラウドサービスのシステムの変更を行う前に、セキュリティ影響度分析を実施する必要がある。FedRAMPはその分析結果に基づき、システム変更によってクラウドサービスの承認にマイナス面の影響がないかどうかを確認したうえで、マイナス面の影響があると判断される場合は、当該システム変更を重大な統制変更として扱うこととなっている。
監査	

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
監査機関への要求事項	FedRAMPは、2023年4月6日に、「3PAO Obligations and Performance Standards Version 3.3」を作成し公表しており、その中で3PAOを認定するための適合性評価プロセスを規定している。なお、3PAOを認定する主体は、American Association for Laboratory Accreditation（以下「A2LA」という。）である。 適合性評価プロセスでは、①3PAOに対するFedRAMP要件及び「ISO/IEC 17020：2012 Conformity assessment－Requirements for the operation of various types of bodies performing inspection」が定めるQMSの遵守と、②RARまたはFedRAMPのセキュリティ承認パッケージを作成する担当者に対するパフォーマンス基準の遵守の双方が求められている。 FedRAMP要件については、A2LA が作成し公表する「R311－Specific Requirements：Federal Risk and Authorization Management Program（FedRAMP）」の中で、FedRAMPにおいて、A2LAの認定を求める3PAOが満たすべき要件を規定している。 パフォーマンス基準については、「3PAO Obligations and Performance Standards Version 3.3」の中で、完全なパッケージ、ドキュメントの品質、応答の適時性、テストの正確性と完全性、評価の完全性、担当者の資格という6つの観点に基づく基準を規定している。
監査機関の独立性	3PAOの独立性については、評価対象であるCSPから独立していることや、ISO/IEC 17020が定めるType Aの検査機関またはType Cの検査機関であることが求められている。 A2LAは、FedRAMPの認定を受ける3PAOに対して、ISO/IEC 17020やR311を含む自らが求める要件への適合性評価を行っている。 また、FedRAMPの認定後においても、その3PAOの認定を維持するために、A2LAは、年に1回の自らが求める要件への適合性のレビューと、2年に1回の再審査（初回審査と同じ内容での審査）を行っている。 3PAOの独立性について、A2LAは、適合性評価・レビューの中で、ISO/IEC 17020における検査機関の独立性に関する要求事項の中に規定されているType Aの検査機関に対する要求事項や、Type Cの検査機関に対する要求事項を確認している。
監査概要	クラウドサービスの認証各省庁による認証により行われる。

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
監査方法	一般的には、以下の通り。 ・ 監査実施前に、FedRAMP Ready に指定されるためのReadiness Assessmentを実施する、Readiness Assessmentにおいて、監査機関である3PAOは、チェックシート形式の確認を行い、CSPの能力を確認する。確認の結果、CSPがFedRAMP認証プロセスが整ったことを示すReadiness Assessment Report (RAR) をPMOに提出する。同Readiness Assessmentは必須ではないが、FedRAMP PMOは実施を強く推奨している。 ・ 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)を作成し、適宜省庁やFedRAMP PMOのフィードバックを受けて更新する。 ・ 3PAOが、SSPに基づいてシステムのテスト（セキュリティコントロールの実装テスト及び検証、脆弱性スキャンの検証、ペネトレーションテストの実行）を含むFull Security Assessmentを実施する。Full Security Assessmentでは、管理策毎に評価方法や目的が規定されている。Full Security Assessmentの評価方法として、検証(Examine)、インタビュー調査(Interview)、テスト(Test)、観察と証拠(Observations and Evidence）ごとに実施すべき作業や記載すべき事項が、Security Requirements Traceability Matrix Templateにおいて規定されている。 ・3PAOは、Full Security Assessment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。
初回審査に要する監査期間	監査に要する期間は、クラウドサービスに求められるセキュリティレベルや、監査実施機関によって異なる。 FedRAMPにおけるクラウドサービスの審査・承認に要する期間は、FedRAMPからは公開されていない。3PAOであるDeloitte & Touche LLP社、およびSchellman Compliance, LLC社、FedRAMP認証を取得済のCSPであるBox Enterprise社のウェブサイトから収集した情報によると、審査・承認プロセスにおける各工程のおおよその所要期間は以下の通りである。 ・フェーズ１：Preparationは１～３か月程度 ・フェーズ２：Authorizationは５～８か月程度（１書類につき約２か月のレビュー期間） ・フェーズ３：Continuous Monitoringは毎月継続的に実施

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
監査対象期間	初回監査に要する期間は、クラウドサービスに求められるセキュリティレベルや、監査実施機関によって異なるが、おおよそ６～１１か月程度となる。（フェーズ１：Preparationは１～３か月程度、フェーズ２：Authorizationは５～８か月程度） 初回監査実施後のセキュリティ対策の実施状況を監視するための仕組みとして、Continuous Monitoring と呼ばれる仕組みがあり、１か月ごとや３か月ごと等、個別管理策ごとに継続的に評価・報告を行うことが求められている。
情報システム変更時の監査範囲・監査方法	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。
SaaSの場合の監査範囲・監査方法	SaaS、PaaS、IaaS というクラウドサービスの種類ごとに異なる監査範囲・監査方法を策定してしない。 セキュリティ影響度が低である SaaS(LI-SaaS)を対象とする認証プロセスが規定されている。 LI-SaaSの場合、CSPが「FedRAMP Security Controls Baseline」のLowレベルに求められる管理策の中から、カスタマイズ基準を参照しつつ、必要となる管理策を選択する。カスタマイズ基準では、管理策ごとに、FED(通常、連邦政府機関の責めに帰すもの)、NSO（セキュリティに影響を与えないと判断されるもの）、Document and Assess（文書化し、独立した評価を受けるもの）、Document and Assess（Conditional）（条件付きで文書化し、独立した評価を受けるもの）、Inherited（管理策が継承されるもの）、Attest（管理策としては必要だが、文書化や独立した評価は不要となるもの）の分類結果が示されている。
サプライチェーンリスクが想定されるクラウドサービスの監査範囲・監査方法	FedRAMPの承認を受けるクラウドサービスに接続される外部サービスや外部サービスに関連するシステムについては、「他のクラウドサービス」と「外部サービスや外部サービスに関連するシステム、コンポーネント」の2つに分類されている。 前者は、クラウドサービス間で相互接続 を行っている場合が対象となっており、相互接続を通じて他のクラウドサービスに関連するシステム内で連邦政府機関のデータとそのメタデータが扱われている場合は、それらのデータが適切に保護されるよう、他のクラウドサービスをFedRAMPの承認を受けるクラウドサービスの承認境界内に含める必要がある。 FedRAMP認証には、サプライチェーンに関する管理策が含まれており、CSPがその管理策についても対応することでサプライチェーンリスクに対応し、Continuous Monitoring等を通して継続的に対応状況を確認することができる。 上記を踏まえ、FedRAMP認証には、サプライチェーンに関する管理策が含まれており、CSPは管理策への対応を求められることから、実質的にCSPの責任の範囲はサプライチェーン全体のスコープ内となる。

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
運用状況評価と整備状況評価の有無及び内容	FedRAMPは、CSPがFedRAMP承認のプロセスを開始した段階から、3PAOにより管理策の対応状況を評価し、必要な対応を行うため、省庁やFedRAMP PMOからのフィードバックを受け、協議と対応繰り返したうえで、対応が十分である（残存リスクがあった場合は責任の所在等を明らかにする）ことについて、ステークホルダーから合意を得た場合、FedRAMPの承認を取得できる。 FedRAMPの承認取得後は、Continuous Monitoringを通して、CSPにおいて管理策ごとに適切な対応が行われているか、継続的に確認を行う。 そのため、FedRAMPは、ISMAPの運用状況評価と整備状況評価と同様の位置づけの取り組みを設けていない。
基準レベルの差異による監査内容	セキュリティ上の影響レベルによって、監査対象となるセキュリティ要件の数が異なる。監査内容については、セキュリティ要件の数が増えれば、監査項目も増えるが、セキュリティ要件としては統一されている。 セキュリティレベルが、High、Moderate の場合、ペネトレーションテストの実施が義務付けられている。
監査の省力化に向けた取組	OMBが2024年7月25日に施行した「M-24-15：Modernizing the Federal Risk and Authorization Management Program（FedRAMP）」においては、承認プロセスの効率化の一環として、特定の外部のセキュリティ認証を取得しているクラウドサービスについて、認証取得時のセキュリティ評価が適切である場合に、FedRAMP承認を受けられるようにする基準を作成することを目標して掲げている。 先ずはFIPS 199の影響レベルが低いクラウドサービスを対象として、FedRAMPにおいて実施されるセキュリティ評価と、特定の外部のセキュリティ認証の取得時に実施されるセキュリティ評価の間で双方の評価手法の整合性確保や基準・リスク間の調整が可能であるかについて検討し、可能である場合には、適用対象をさらにより高い影響レベルのクラウドサービスにも拡大していく可能性があることが謳われている。また、双方の評価手法の整合性確保や基準・リスク間の調整が難しい場合に、それらを補完するために、特定の種類のクラウドサービスに対して追加の管理策を求めたり、リスクを許容したりするといった対応についても上記の検討範囲に含まれる可能性がある。

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
他国の制度との相互運用性	相互運用性については、明示的には記載されていないが、FedRAMPの基準は NIST の基準・標準に基づいて策定されているので、他国における認証制度への落とし込みは、制度の基準を策定するそれぞれの国において実施する必要がある。
他の基準の流用・活用	他の基準の流用・活用については、明示的には記載されていないが、クラウドサービスプロバイダーは、FedRAMP 以外の複数のセキュリティ・フレームワークに基づく監査または評価を実施しているケースがある。FedRAMP システムでは、3PAOが監査・評価を実施するが、FedRAMP 以外のセキュリティ・フレームワークに基づく監査または評価がテスト・ケースの要件を満たしており、また、実施時期が十分に新しいものであれば、それらの監査・評価による証拠を受け入れる可能性は大いにある。さらに、異なる評価システムへの準拠に特化し、成果物の収集と準拠を自動で管理するツールも数多く存在する。 FedRAMP の Moderate は、DoDのクラウドサービス向け評価システムのレベル２と相互補完関係にあり、双方の結果を援用できる。 クラウドサービスプロバイダーによっては、FedRAMP の管理策と ISO 基準とのマッピングを実施して、監査の効率化を図っている。
リアルタイム監査の取り組み	FedRAMPにおいては、リアルタイム監査の観点からの取組は実施されていない。一方で、FedRAMPにおいては、FedRAMP Continuous Monitoringの中で、評価対象となるセキュリティ管理策毎に、評価の頻度（都度、1週間に1度、10日に1度、1か月に1度、3か月に1度、1年に1度、2年に1度、3年に1度、5年に1度）をきめ細かく設定している。 その他にも、FedRAMPにおいては、Full Security Assessmentプロセスや、そのプロセスを実行するためのPreparationプロセスを含め、承認プロセスの効率化が目指され、その中でレビュープロセスの合理化や、承認パッケージのデジタル化が進められている。 具体的には、FedRAMPにおいては、承認プロセスの効率化を目的として、NISTと協力し、2018年より、コンピュータで共通的に自動処理可能な言語であるOpen Secure Control Assessment Language（以下「OSCAL」という。）を開発し、承認パッケージのデジタル化が進められてきた。その成果をもとに、FedRAMPは、CSPと3PAOが、FedRAMPに対して承認パッケージを提出する際にOSCALを利用することを推奨している。 加えて、OSCALを使用して、レビュープロセスの合理化やデジタル承認パッケージの自動検証を行う方法についても検討が開始されている。

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
監査機関の提出書類	3PAOを認定する主体は、American Association for Laboratory Accreditation（以下「A2LA」という。）であり、初回の認定の準備として、3PAOは、A2LAより提供される認定見積もり依頼フォームを通じて、認定を希望するプログラムと認定範囲の草案を入力しなければならない。 その後、初回の認定に係る申請において、3PAOは、A2LAに対して、以下のサポート文書を提出しなければならない。 ・該当する適合性評価規格とA2LA要件を満たすためのポリシーと手順、それらを備えた管理システムに関する書類 ・内部監査結果 ・マネジメントレビューの結果 さらに、A2LAが申請を受け付けた後においても、3PAOは、A2LAに対して、裏づけに必要となる文書を提出しなければならない。
審査	
認証プロセス内容	これまでは、JABによる認証と省庁による認証があったが、省庁による認証に一本化された。 ＊ 省庁による認証プロセス フェーズ 1： Preparation（Readiness Assessment、Pre-Authorization） フェーズ 2： Authorization（Full Security Assessment、Agency Authorization Process） フェーズ 3： Continuous Monitoring その他：審査・承認プロセスの改善 省庁による認証方式に一本化されたことによる生じた変更点は、これまで省庁における認証方式では明示化されていなかったReadiness Assessmentが、認証プロセスに組み込まれた点のみである。Readiness Assessmentの実施は必須ではないが、FedRAMP認証を取得する上で必要な準備を整えることができるため、強く推奨されている。

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
CSPへの要求事項	CPSへの要求事項の概要を、省庁による認証プロセスのフェーズごとに示す。 フェーズ 1： Preparation ・Readiness Assessment時点での、Readiness Assessmentの実施、SSP・RARの作成 ・Pre-Authorization時点での、パートナーシップ締結可能性のある省庁からの質問対応、承認計画・WBS・キックオフミーティング資料の作成、キックオフミーティングへの参加 フェーズ 2： Authorization ・Full Security Assessment時点での、完全なセキュリティ評価用の必要書類・POA&Mの作成、フィードバックに基づく修正 ・Agency Authorization Process時点での、SAR確認用プレゼンテーション資料の作成とプレゼンテーション実施、フィードバックに基づく修正 フェーズ 3： Continuous Monitoring ・当該クラウドサービスのセキュリティ体制の継続的な監視、当該クラウドサービスに関する情報提供 その他：審査・承認プロセスの改善 ・CSPに求める内容は特にないが、Continuous Monitoringの結果が、FedRAMP Board、FSCAC、TAG等にも共有され、審査・承認プロセスの改善の参考情報となる
申請に必要な書類	System Security Plan (SSP)、Security Assessment Plan（SAP）、Security Assessment Report (SAR)、 Plan of Action and Milestones （POA&M）の４点
認証に関係する組織・機関	審査・承認プロセスのうち、フェーズ１～３の認証に関連する利害関係者は、CSP、Third Party Assessment Organizations（3PAO）、FedRAMP PMO、省庁の４者である。 審査・承認プロセスの後、必要に応じて行われる審査・承認プロセスの改善に関連する利害関係者は、上記に加え、FedRAMP Board、FSCAC、TAGの３者である。
認証に関係する組織・機関の役割	FedRAMPの認証を取得するための情報提供等：CSP FedRAMP認証を取得するCSPへの検証、支援：Third Party Assessment Organizations（3PAO） FedRAMP認証に係る審査、承認：FedRAMP PMO FedRAMP認証を取得するCSPとの協議。フィードバック、支援：省庁 審査・承認プロセスの改善（※個々のCSPの審査・承認プロセスには関与しない）：FedRAMP Board、FSCAC、TAG

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
発見事項があった際の対応に関して	省庁による認証プロセスの間、CSPは3PAO、省庁、FedRAMP PMOからフィードバックを継続的に受け、発見事項があった際に、詳細を確認した上で修正を行うとともに、必要書類一式を更新し、そのレビューを受ける 脆弱性等の発見事項について、CSPはPOA&Mにその情報を記載し、是正対応を管理しなければならない。POA&Mには、既知の脆弱性、脆弱性により影響を受ける管理策、脆弱性の概要、脆弱性が発見された時点でのリスク（High、Moderate、Low）、脆弱性対応の責任者、脆弱性の是正状況等が記載される
認証後の評価・復旧方法	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。
監査モニタリング方法	一定期間における個別管理策の運用状況を確認する運用状況評価の仕組みとして「Continuous Monitoring」(継続モニタリング)があり、クラウドサービスプロバイダーが、１か月ごとや３か月ごと等、個別管理策ごとに継続的に評価・報告しなくてはならない項目が規定されている。 クラウドサービスプロバイダーは、継続モニタリングプログラムを導入し、セキュリティコントロールの有効性評価、システムや運用環境に関する変更の文書化、変更に関連するセキュリティ影響評価、システムのセキュリティ状態について、省庁の認証担当者に報告することが規定されている。

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
クラウドサービスプロバイダーの評価	特定のCSPへのヒアリングによって、以下の評価を確認している。 ・ 提供するクラウドサービスのセキュリティを適切に評価してもらえるという点についてはよいと考えている。 ・ 確認・評価の方法については満足している。 ・ 監査人の人件費を含む認証取得コストと認証取得により得られるリターン（評価・認定を受けることで得られるメリット）を天秤にかけると、満足のいくリターンが得られている。 ・ 提出しなければいけない書類が何千枚となり、書類作成のための作業量が大きいことが負担となっている。 ・ FedRAMP 制度が受け入れられるものになる上で重要となるのは、クラウドサービスプロバイダーおよび監査機関といかにうまくコミュニケーションをとりながら、制度を運用・改善していくかということである。コミュニケーションにコストをかけないと、クラウドサービスプロバイダーに受け入れられない制度になってしまう恐れがある。 ・ FedRAMP 認証で提出しなければいけない書類が何千枚と量が大きいことが負担。その他の確認、評価の方法や、コストをかけたことによるリターンについては満足している。
普及方策	FedRAMP運営主体が、メーリングリスト、プレスリリース、ブログ等による情報発信を行っている。また、FedRAMP 運営主体が、政府機関にクラウドサービスの利用を推奨する等の活動を通じて、利用者の確保に努めている。 クラウドサービスを利用することによるメリット等の紹介にも注力している。

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
認証取得に要するコスト	CSPへのヒアリングに基づき、以下に示す米国政府の試算が存在することを確認している。 2016年に公表された米国政府の試算によると、FedRAMP認証取得に要するコストは、以下のようになる。 ・ エンジニアリングコスト：平均 $1,100,000 インパクトレベルが中のクラウドシステムについて、連邦政府要件を満たすためにシステムに技術的な変更にかかるコスト ・ 文書整備コスト：$400,000 システムのセキュリティポリシーおよび手続きに関する文書、システムセキュリティ計画、インシデント対応計画を整備するためのコスト ・ 第三者評価機関によるアセスメントコスト：$500,000 FedRAMP 認定第三者評価機関による独立のアセスメントの実施コスト これには、テスト計画の作成、オンサイトでのアセスメント、セキュリティアセスメント報告書の作成、認証担当者 (authorizing officials)に対する説明が含まれる。 ・ JAB によるレビューコスト：$250,000 JAB の要件を満たすために必要となるアップデートにかかるコスト たとえば、クラウドサービスプロバイダーが、アセスメントプロセスに入る前にFedRAMP要件を十分に満たすことができない場合にセキュリティ対策のアップデートを実施するためのコスト ・ 継続モニタリングコスト：$1,000,000 毎月の脆弱性スキャン、活動計画・マイルストーン管理、重大な変更(への対応)、年次アセスメント等、毎年必要となるコスト
審査に要する期間	FedRAMPにおけるクラウドサービスの審査・承認に要する期間は、FedRAMPからは公開されていない。 一部の3PAOおよびCSPのウェブサイトにおいて、参考情報として記載されている所要期間を以下記載する。 フェーズ 1： Preparation（Readiness Assessment、Pre-Authorization）は、1～2か月程度 フェーズ 2： Authorization（Full Security Assessment、Agency Authorization Process）は、6～8か月程度 フェーズ 3： Continuous Monitoringは、毎月継続的に実施
インシデント発生時の対応	

FedRAMP基礎情報表

比較・分析観点	FedRAMP（米国）
セキュリティインシデントに関する規程	FedRAMP Incident Communications Procedures FedRAMP Continuous Monitoring Performance Management Guide
セキュリティインシデント報告/処分の基準	・クラウドサービスに重大な影響を及ぼしうるインシデントが発生した場合の報告義務 ・インシデントの発生を認知してから1時間以内の報告 ・インシデント発生時の報告に遅れが生じた場合には是正措置計画の作成が必要。合意した期限内に対応しない場合は、承認の一時停止または取り消しとなる場合がある
インシデント発覚後の対応	・CISAが必要に応じてCSPのインシデント対応を支援 ・省庁AOが省庁側で策定されたインシデント対応計画の要件が確実に満たされていることを確認