米国におけるクラウドサービスのセキュリティ評価に係る手続・評価手法等に関する調査

FedRAMP概要説明資料

株式会社野村総合研究所

コンサルティング事業本部
ICT・コンテンツ産業コンサルティング部

2025年3月21日

NRI

Envision the value,
Empower the change

①制度の概要

FedRAMPの制度の根拠は、「Federal Information Security Modernization Act of 2014」、「Circular A-130 - Managing Information as a Strategic」、「FedRAMP Authorization Act」、「M-24-15：Modernizing the Federal Risk and Authorization Management Program (FedRAMP) 」

2014年に制定された「Federal Information Security Modernization Act of 2014 (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。

連邦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である FedRAMP（Federal Risk and Authorization Management Program）を定めた。

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。

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、第3607条～第3616条として、「FedRAMP Authorization Act」が追加され、2022年12月に公布された。

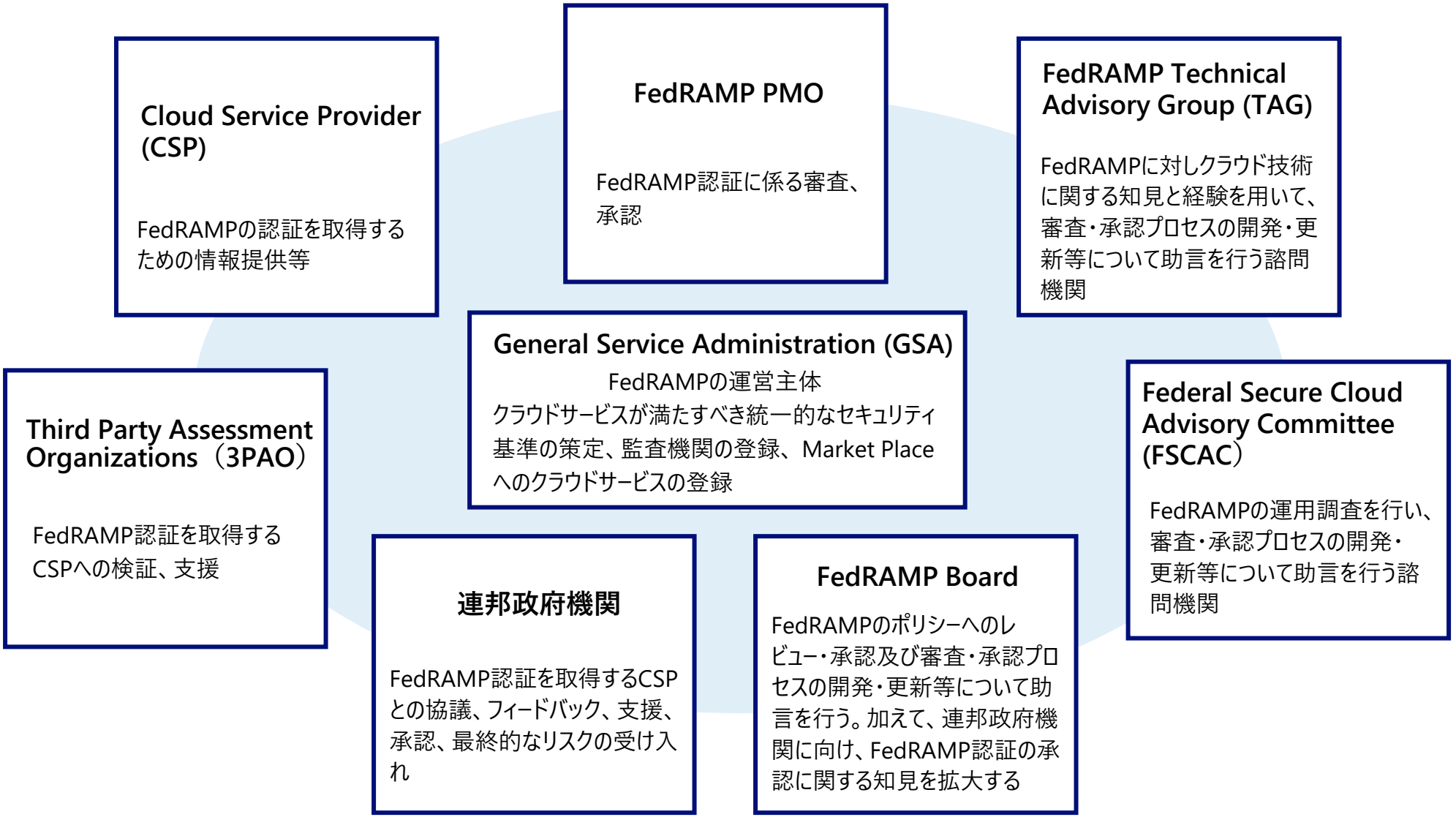
GSAの組織内にFedRAMP PMO (Program Management Office) とFedRAMP Boardが設置されたほか、それぞれの役割と更なる責任が確立された。

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、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た。

当該覚書によって連邦CIOが2011年12月8日に施行した覚書「Security Authorization of Information Systems in Cloud Computing Environments」を置き換えた。

①制度の概要

FedRAMPの運営には、運営主体であるGSAのほかに、FedRAMP Board、FSCAC、TAG、CSP、3PAO、FedRAMP PMO、連邦政府機関といったステークホルダーが関わる



②管理基準

GSAは、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

FedRAMP Security Controls Baseline

- ベースライン管理策は、「NIST SP 800-53 Security and Privacy Controls for Information System and Organizations」をもとに規定されている。
  （2020年9月23日にNIST SP 800-53 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、Rev.5 の改訂内容を反映した「FedRAMP Security Controls Baseline」の改訂版を提供 ）

- FIPS 199に基づき、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おり、それぞれのレベルに見合う遵守が求められる管理策は、上記のベースライン管理策の中から選定されている。
  （管理策数） High：410、Moderate：323、Low：156

- その上で、LI-SaaSについては、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（詳細は後述）を参照しつつ、必要となる管理策を選択する。

各レベルの定義

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。

②管理基準

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

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2種類のテンプレートを提供

「FedRAMP High Control Implementation Summary (CIS) Workbook Template」
「FedRAMP Low or Moderate Control Implementation Summary (CIS) Workbook Template」

管理策の言明は、あくまでCSPが、上記のテンプレートの中で、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いる

管理策ごとの実装状況

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

管理策ごとの実装責任

実装責任については、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

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る

※SSPとはSystem Security Planのことを指す。

②管理基準

他のクラウドサービスとの間での相互接続を通じて、連邦政府機関のデータ等が扱われる場合は、他のクラウドサービスについても承認境界内に含める必要がある

FedRAMPの承認を受けるクラウドサービスに接続される他のクラウドサービスの取扱い

- 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。
- 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。

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。

FedRAMPの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の取扱い

- 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はセキュリティ影響度分析結果に基づき、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。

③監査（評価）

FedRAMPは、「3PAO Obligations and Performance Standards Version 3.3」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

（1）監査機関の認定主体	American Association for Laboratory Accreditation（A2LA）
（2）監査機関の認定プロセス	● 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。
（3）監査機関の認定基準	● 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。
3PAOに対するFedRAMP要件及びISO/IEC 17020が定めるQMSの遵守	● 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。
RAR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	● 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。

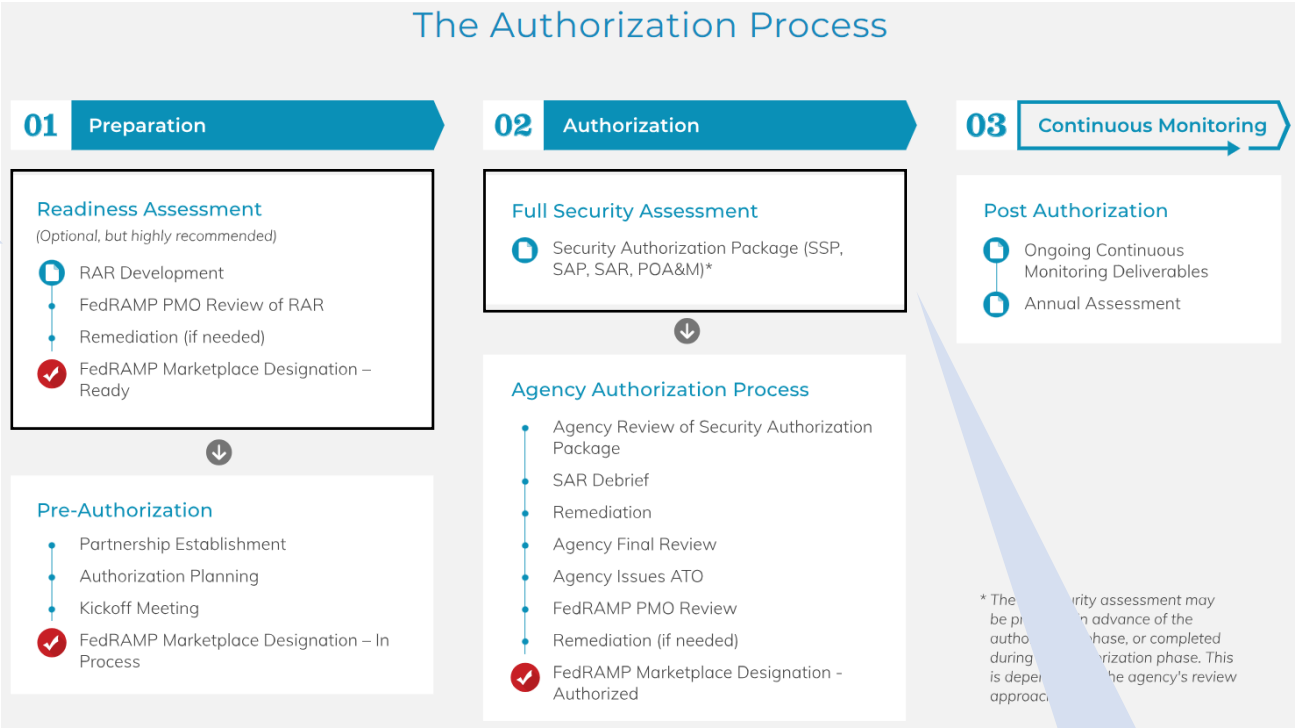
監査機関の独立性の担保

- 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。
- 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。

③監査（評価）

FedRAMPの審査・承認プロセスを以下に示す。監査プロセスには、Readiness AssessmentとFull Security Assessmentの2つのプロセスが存在する

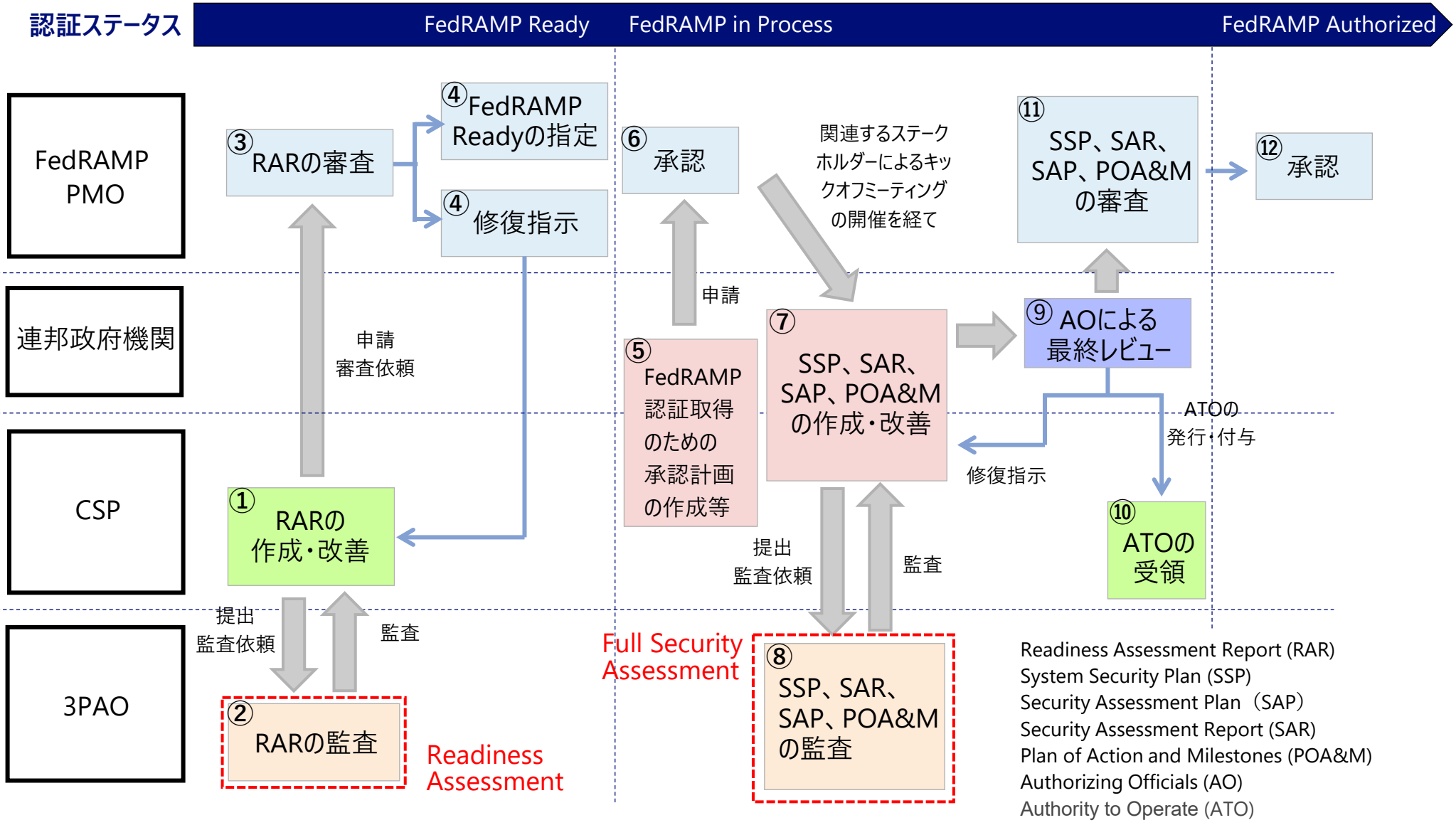
- 監査実施前に、FedRAMP Ready に指定されるためのReadiness Assessmentを実施する.。
- Readiness Assessmentにおいて、監査機関である3PAOは、チェックシート形式の確認を行い、CSPの能力を確認する。
- 確認の結果、CSPがFedRAMP認証プロセスが整ったことを示すReadiness Assessment Report (RAR) をPMOに提出する。
- CSP は、CSP のシステムが、どの程度 FedRAMP のセキュリティコントロールと整合しているかを示す System Security Plan (SSP) を作成し、適宜省庁やFedRAMP PMOのフィードバックを受けて更新する。



出所）FedRAMPの公式ホームページ（https://www.fedramp.gov/）

- 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。管理策毎に評価方法や目的が規定されていて、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。

③監査（評価）
FedRAMPの承認を受けるために必要な申請・審査・監査に関わる基本的な流れを以下に示す



Readiness Assessment Report (RAR)
System Security Plan (SSP)
Security Assessment Plan（SAP）
Security Assessment Report (SAR)
Plan of Action and Milestones (POA&M)
Authorizing Officials (AO)
Authority to Operate (ATO)

③監査（評価）
FedRAMPの承認を受けたクラウドサービスにおける情報システムの変更や、新たなサプライチェーンリスクへの対応は、Continuous Monitoringを通じて確認される

- FedRAMPにおいては、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。

情報システム変更時の監査

- 連邦政府機関は、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ているかどうかの判断を行う。

SaaSの場合の監査

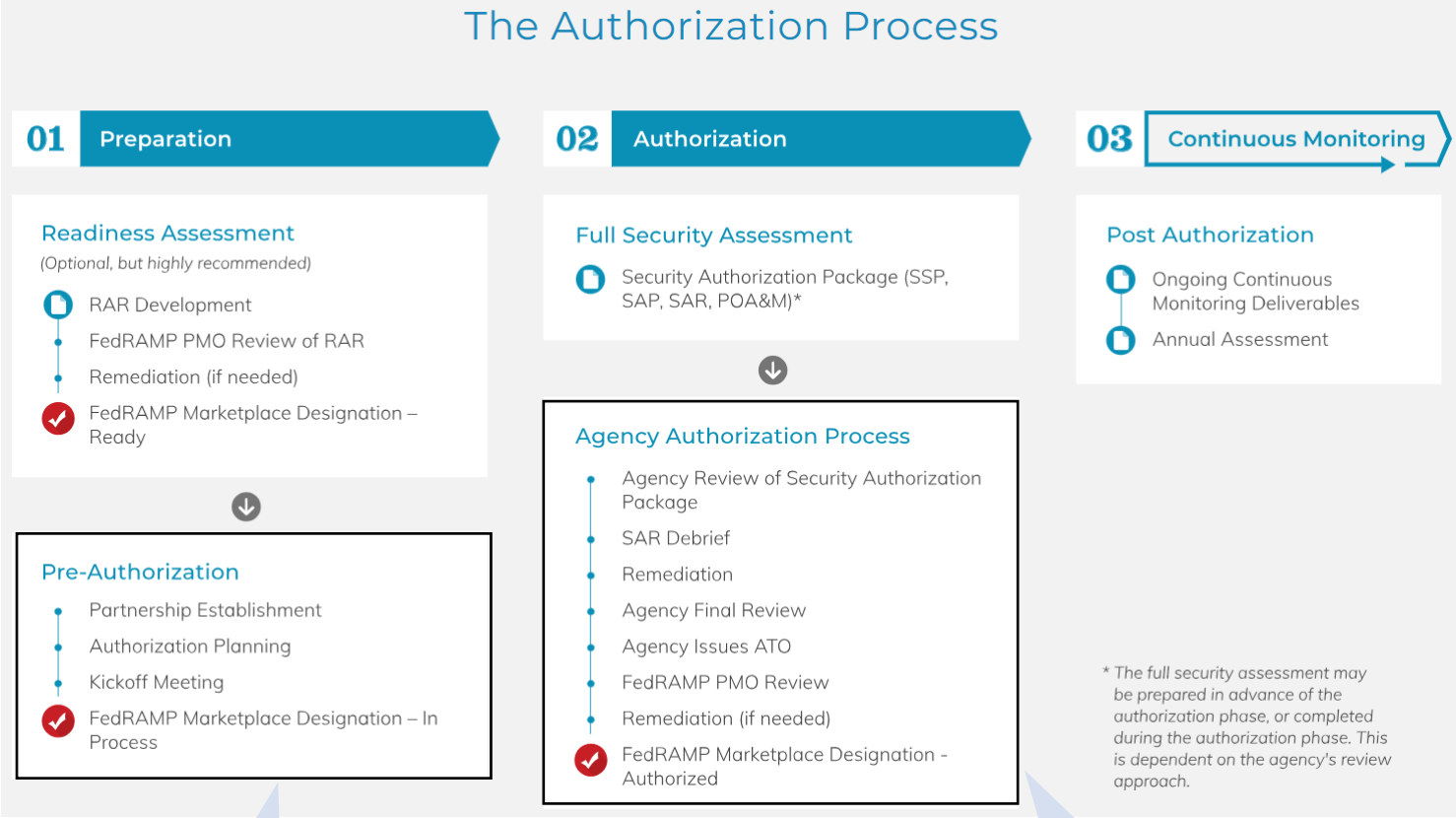
- SaaS、PaaS、IaaS というクラウドサービスの種類ごとに異なる監査範囲・監査方法を策定してしない。
- 一方、前述したLI-SaaSにおいて、CSPが必要となる管理策を選択する際に参照されるカスタマイズ基準では、管理策ごとに以下の分類を行うこととされている。
  - FED(通常、連邦政府機関の責めに帰すもの)
  - NSO（セキュリティに影響を与えないと判断されるもの）
  - Document and Assess（文書化し、独立した評価を受けるもの）
  - Document and Assess（Conditional）（条件付きで文書化し、独立した評価を受けるもの）
  - 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）

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

- クラウドサービス間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。
- 遵守が求められる管理策には、サプライチェーンに関する管理策が含まれており、CSPはその管理策についても対応することが求められる。また、その状況は、連邦政府機関によって継続的にモニタリングされ、確認される。

④審査

CSPは、Pre-Authorizationにおいて、FedRAMP Readyの指定を受けるために、また、Agency Authorization Processにおいて、FedRAMPの承認を受けるために審査される



発見事項があった際の対応

- CSPは3PAO、連邦政府機関、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、以下に示す必要書類一式を更新し、そのレビューを受ける。

［必要書類一式］

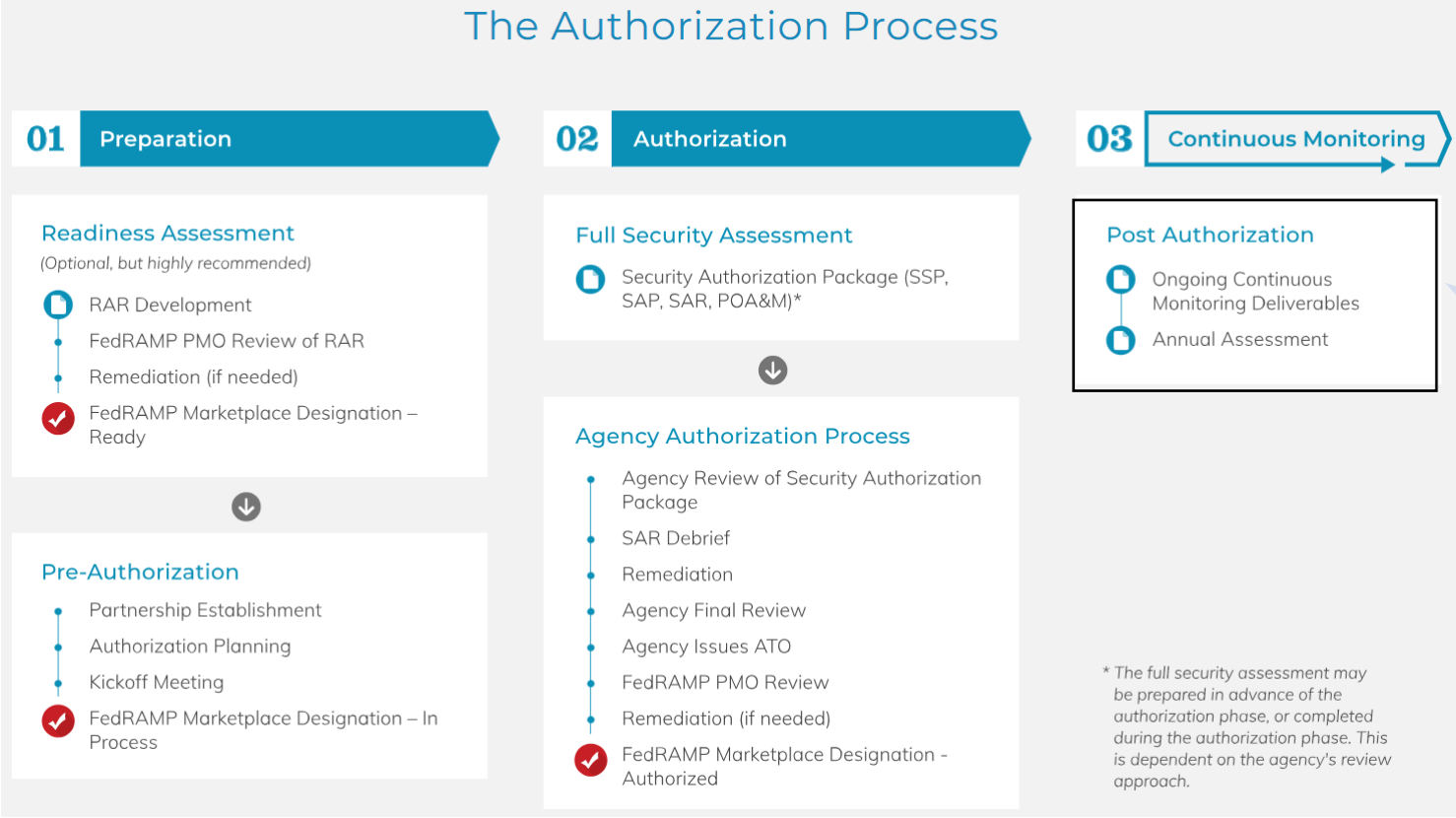
System Security Plan (SSP)
Security Assessment Plan（SAP）
Security Assessment Report (SAR)
Plan of Action and Milestones (POA&M)

出所）FedRAMPの公式ホームページ（https://www.fedramp.gov/）

- CSPに対して、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が求められる。
- CSPは、そのような審査プロセスを経て、FedRAMP Readyの指定を受けることができる。

- CSPに対して、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が求められる。
- CSPは、そのような審査プロセスを経て、FedRAMPの承認を受けることができる。

④審査
CSPは、Post Authorizationにおいて、実装しているセキュリティ管理策の有効性を審査される



出所）FedRAMPの公式ホームページ（https://www.fedramp.gov/）

- CSPは、管理策毎にきめ細かく設定された評価の頻度（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）に従い、対象となる管理策の有効性評価結果を連邦政府機関の認証担当者に報告しなくてはならない。
- その他に該当する場合は、システム環境や運用環境の変更や、その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も、連邦政府機関の認証担当者に報告しなくてはならない。
- 連邦政府機関は、CSPより提出されたそれらの報告書をレビューする。

④審査
参考：審査・承認プロセスのPreparationの段階におけるステークホルダーの役割概要

フェーズ	役割			
	CSP	3PAO	省庁	FedRAMP PMO
Readiness Assessment	・ SSPの作成 ・ 3PAOからReadiness Assessmentを受ける ・ 3PAOとRARを作成	・ CSPにReadiness Assessmentを実施 ・ CSPとRARを作成	・ FedRAMP Marketplaceでクラウドサービスを検討	・ RARを確認 ・ RARの承認後、FedRAMP MarketplaceにおけるCSPの当該クラウドサービスのステータスを"FedRAMP Ready"に変更
Pre-Authorization	・ パートナーシップの締結に向け、省庁からの質問対応 ・ 承認計画の作成 ・ キックオフミーティングの開催に向け、WBSおよび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	－	・ パートナーシップの締結に向け、CSPへ確認 ・ 承認計画の作成 ・ 必要書類一式の確認の際のアプローチ方法の決定 ・ キックオフミーティングの開催に向け、WBSの作成、およびCSPへのキックオフミーティング資料の作成指示 ・ WBSの承認後、FedRAMP PMOへIn-Processリクエスト ・ キックオフミーティングへの参加	・ WBSおよびキックオフミーティング資料の承認 ・ 省庁からのIn-Processリクエストを承認後、FedRAMP MarketplaceにおけるCSPの当該クラウドサービスのステータスを"FedRAMP in Process"に変更

出所）これまでの調査結果、および「FedRAMP Agency Authorization Playbook Version 4.0」（https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook.pdf）、ならびに「M-24-15 Modernizing the Federal Risk and Authorization Management Program (FedRAMP)」（https://bidenwhitehouse.archives.gov/omb/management/ofcio/m-24-15-modernizing-the-federal-risk-and-authorization-management-program-fedramp/）

④審査
参考：審査・承認プロセスのAuthorizationの段階におけるステークホルダーの役割概要

フェーズ	役割			
	CSP	3PAO	省庁	FedRAMP PMO
Full Security Assessment	・完全なセキュリティ評価用の必要書類一式を作成、フィードバックを受け、適宜修正 ・3PAOのSARに基づき、POA&Mを作成 ・省庁にSARとPOA&Mを提出し、フィードバックを受け、適宜修正	・完全なセキュリティ評価用の必要書類一式について検証 ・検証結果に基づき、SARを作成 ・省庁にSARとPOA&Mを提出し、フィードバックを受け、適宜修正	・完全なセキュリティ評価の前に必要書類一式を確認し、CSPに対しフィードバック ・SARとPOA&Mについてフィードバック	－
Agency Authorization Process	・SAR確認用のプレゼンテーション資料の作成 ・SAR確認用のプレゼンテーションの実施 ・省庁からの必要書類一式へのフィードバックを受け、適宜修正 ・省庁のAOが発行したATOを受領 ・FedRAMP PMOからの必要書類一式へのフィードバックを受け、適宜修正	・SAR確認用のプレゼンテーション資料の作成 ・SAR確認用のプレゼンテーションの実施 ・省庁からの必要書類一式へのフィードバックを受け、適宜修正 ・FedRAMP PMOからの必要書類一式へのフィードバックを受け、適宜修正	・SAR確認用のプレゼンテーションの質問 ・必要書類一式へのフィードバック ・AOがATOを発行	・SAR確認用のプレゼンテーション資料のフォーマット提供 ・SAR確認用のプレゼンテーション資料の事前確認とフィードバック ・省庁のAOが発行したATOを受領 ・必要書類一式についてフィードバック ・必要書類一式についてドラフトレポートを発行 ・CSPと3PAOの修正内容を確認 ・更新された必要書類一式を確認し、承認後、FedRAMP MarketplaceにおけるCSPの当該クラウドサービスのステータスを"FedRAMP Authorized"に変更

出所）これまでの調査結果、および「FedRAMP Agency Authorization Playbook Version 4.0」（https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook.pdf）、ならびに「M-24-15 Modernizing the Federal Risk and Authorization Management Program (FedRAMP)」（https://bidenwhitehouse.archives.gov/omb/management/ofcio/m-24-15-modernizing-the-federal-risk-and-authorization-management-program-fedramp/）

④審査
参考：審査・承認プロセスのContinuous Monitoringの段階におけるステークホルダーの役割概要

フェーズ	役割			
	CSP	3PAO	省庁	FedRAMP PMO
–	・ 当該クラウドサービスのセキュリティ体制を継続的に監視 ・ 省庁に当該クラウドサービスに関する必要情報を提供	・ 当該クラウドサービスのセキュリティ体制を継続的に監視 ・ 省庁に当該クラウドサービスに関する必要情報を提供 ・ 作成するすべての文章について真正性を保証	・ CSPおよび当該クラウドサービスのセキュリティ体制やFedRAMP要件の遵守を確認	・ プロセスの改善のために検討が必要なケースがある場合や、重大な脆弱性を認識した場合、CSPや3PAOに報告を求める

出所）これまでの調査結果、および「FedRAMP Agency Authorization Playbook Version 4.0」（https://www.fedramp.gov/assets/resources/documents/Agency_Authorization_Playbook.pdf）、ならびに「M-24-15 Modernizing the Federal Risk and Authorization Management Program (FedRAMP)」（https://bidenwhitehouse.archives.gov/omb/management/ofcio/m-24-15-modernizing-the-federal-risk-and-authorization-management-program-fedramp/）

④審査
参考：審査・承認プロセスの改善におけるステークホルダーの役割概要

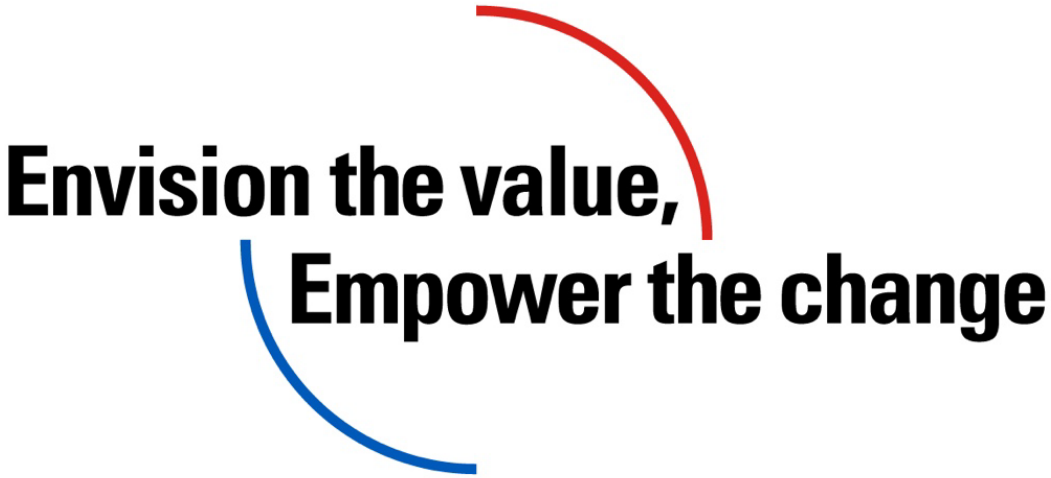
役割				
CSP、3PAO、省庁	FedRAMP PMO	FedRAMP Board	FSCAC	TAG
・ 通常のContinuous Monitoringにおけるタスクを実行する ・ 同タスクにおける情報を審査・承認プロセスの改善のために提供する	・ プロセスの改善のために検討が必要なケースがある場合や、重大な脆弱性を認識した場合、FedRAMP Boardに対して特別なレビューを申請する ・ 報告書の内容を元に、プロセスの改善に伴う変更内容を決定する	・ FedRAMP PMOからの特別なレビュー申請を確認し、検討期限を設定した上で承認する ・ 特別なレビューを行うWGに参加し、Continuous Monitoringの内容を監督し、プロセスの改善について検討する ・ WGの検討結果を報告書にとりまとめる	・ 特別なレビューを行うWGに参加し、Continuous Monitoringの内容を監督し、プロセスの改善について検討する ・ WGの検討結果を報告書にとりまとめる	・ 特別なレビューを行うWGに参加し、Continuous Monitoringの内容を監督し、プロセスの改善について検討する ・ WGの検討結果を報告書にとりまとめる

出所）「M-24-15 Modernizing the Federal Risk and Authorization Management Program (FedRAMP)」（https://bidenwhitehouse.archives.gov/omb/management/ofcio/m-24-15-modernizing-the-federal-risk-and-authorization-management-program-fedramp/）

⑤インシデント発生時の対応

セキュリティインシデント発生時に必要となる対応は、「FedRAMP Incident Communications Procedures」と「FedRAMP Continuous Monitoring Performance Management Guide」に規定されている

（1）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
（2）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がある。 ● インシデントの発生を認知してから1時間以内の報告が求められる。 ● 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となり、合意した期限内に是正措置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。
（3）セキュリティ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する。 ● 連邦政府機関のAOが、連邦政府機関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する。


Envision the value,
Empower the change