令和４年度森林吸収源インベントリ情報整備事業

国家森林資源データベース
クラウド移行検討調査
仕様書

林野庁

目次

１　調達案件の概要

（１）調達件名

令和４年度森林吸収源インベントリ情報整備事業　国家森林資源データベースクラウド移行検討調査

（２）調達の背景

我が国は、気候変動に関する国際連合枠組条約（以下「気候変動枠組条約」という。）並びにパリ協定の締約国として森林の温室効果ガスの排出・吸収量（以下「森林吸収量」という。）の算定・報告が義務付けられており、国際的に定められたガイドライン等に基づき、森林による炭素蓄積変化量（吸収・排出量）を算定している。この算定作業を効率的、適切に実施するにあたって、必要なデータを格納する国家森林資源データベース（以下「国家 DB」という。）の整備を随時実施する必要がある。

2018 年６月には、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2021 年３月改訂）が決定された。この中で、「クラウド・バイ・デフォルトの原則」が政府方針として出されている。

また、農林水産省では、政府全体の動向や利用者視点に立った、あるべき農林水産行政の姿を踏まえ、2020 年３月に「農林水産省デジタル・ガバメント中長期計画」を改訂し、情報システムのクラウド化の推進に当たっては、共通基盤となる農林水産省クラウド（以下「MAFF クラウド」という。）を利用することを前提としたパブリック・クラウドへの移行を進めることとしている。

MAFF クラウドでは、パブリック・クラウドへの移行・運用に必要な最小限の共通機能が提供されるとともに、「MAFF クラウド活動」として、パブリック・クラウドへの移行・運用等の一連の工程における、農林水産省デジタル戦略グループ情報管理室による国家森林資源データベースシステム担当者への総合的な支援活動が実施される。なお、総合的な技術支援を行う組織を MAFF クラウド CoE と言う。

これらの状況を踏まえ、本システムの MAFF クラウド利用を前提とした移行について検討する。

（３）目的

国家 DB 運用における現状分析を行い、令和５年度に予定するクラウド移行業務及び移行後の運用・保守業務に必要な条件・事項を整理し、要件定義書を作成する等、国家 DB のクラウド移行に向けた準備を行う。

（４）業務・情報システムの概要

森林吸収量算定業務及び国家 DB の概要は図１に示すとおり、我が国の森林吸収量の算定に必要な全国の森林資源に関する様々な情報を格納、解析、表示及び出力するものである。

令和５年度に現在オンプレミスで構築されている国家 DB の MAFF クラウドへの移行を予定している（図２）。本業務は、国家 DB をクラウドへ移行するにあたり、データベース運用における現状分析を行い、クラウド移行及び移行後の国家 DB（以下「新システム」という。）の運用・保守に必要な条件を整理する。検討した結果をもとに来年度のクラウド移行業務に関する要件定義書を

作成する。

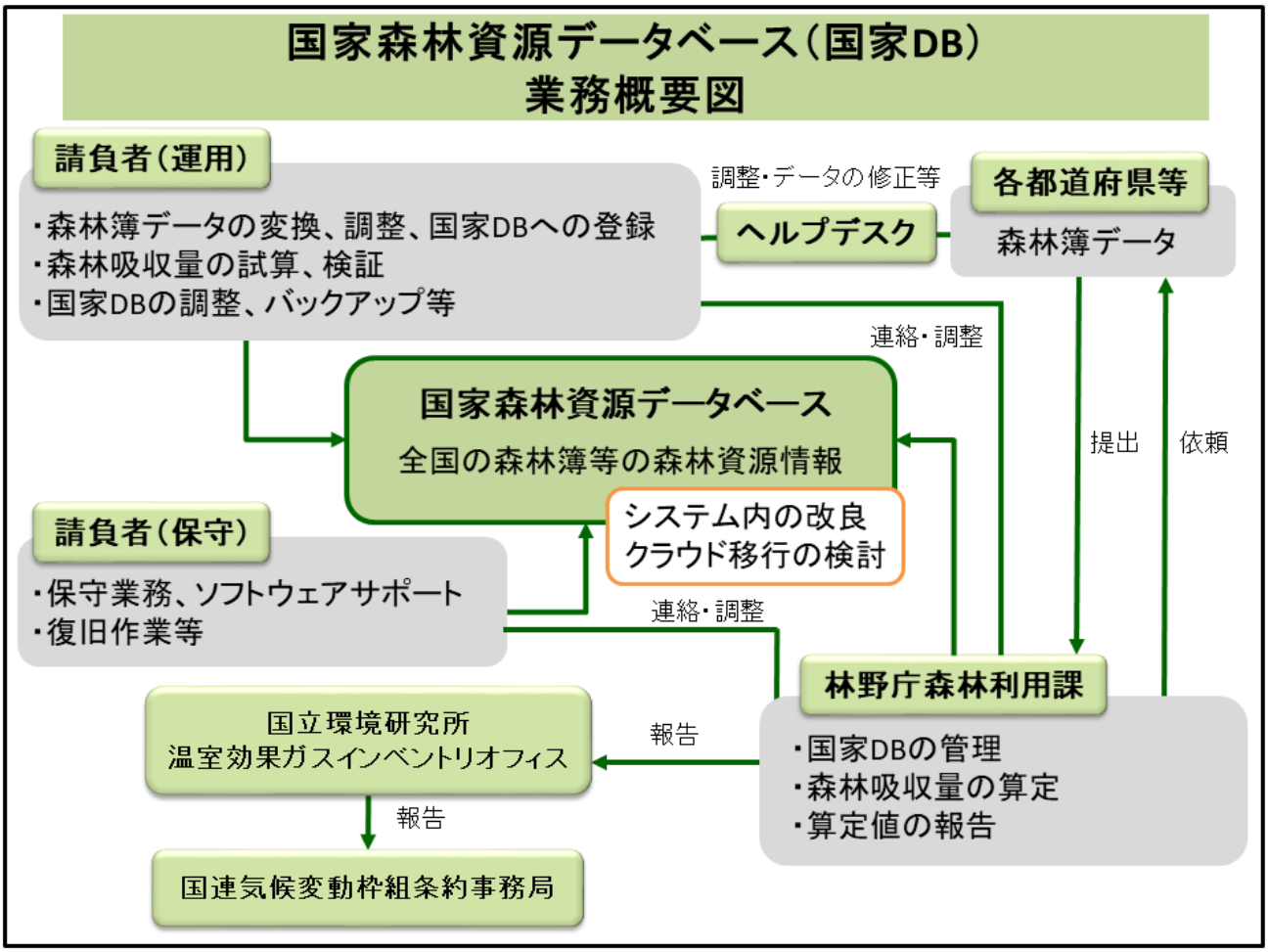


図１　森林吸収量算定業務及び国家森林資源データベースシステムの概要

MAFFクラウド構成イメージ

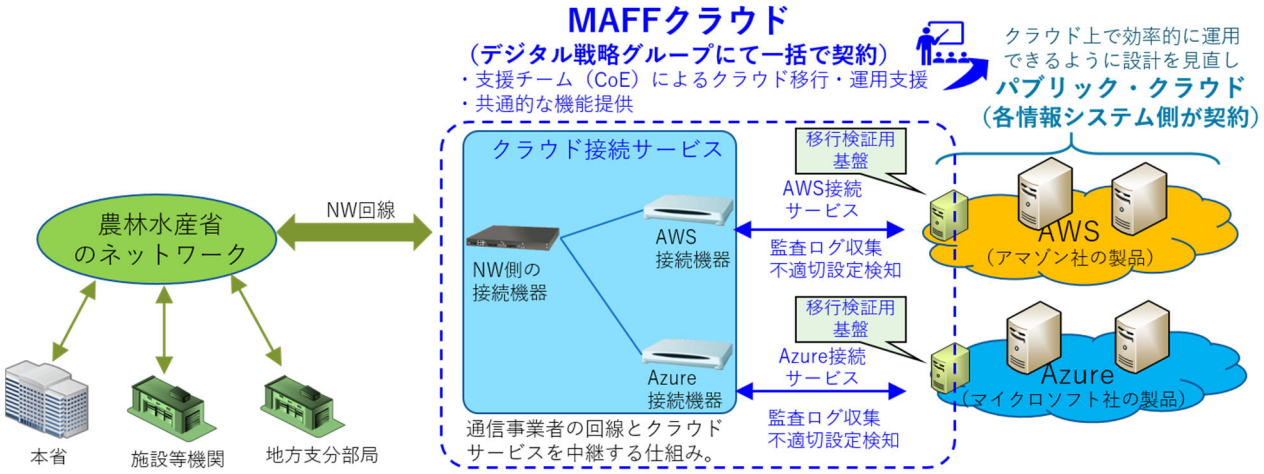


図２　MAFF クラウド構成イメージ

（５）契約期間

契約締結日から令和５年２月 28 日まで

（６）作業スケジュール

主な作業スケジュールは図3のとおり想定している。

作業項目	令和４年									令和５年		
	4	5	6	7	8	9	10	11	12	1	2	3
国家DBクラウド移行検討調査												
							現状分析		要件定義	書作成		

図３　作業スケジュール

（７）関連する調達

関連する調達の単位、調達の方法、実施時期等は図４のとおりである。

図４　関連する調達

２　業務の実施内容

（1）国家 DB クラウド移行に向けた準備

受注者は、国家 DB 運用における現状分析を行い、発注者と協議しながら、令和５年度のクラウド移行及び新システムでの算定作業に向けた、新しいデータベース環境の構築及びデータベース

運用に必要な条件を整理する。この際、現行システム内でデータベースの検索、抽出等を行うＶＢツール（アナライザ）について、新たなデータベース環境に対応した形態を検討する。受注者はこの結果を踏まえて、令和５年度のクラウド移行業務の要件定義書を別添３　「農林水産省クラウド利用ガイドライン」に基づき令和５年２月 28 日までに作成する。要件検討にあたっては、令和 5 年度にガバメントソリューションサービス（GSS）に移行することを踏まえて、必要な検討を行うこと。

なお、要件定義書には、発注者の意見を十分に踏まえるとともに「デジタル・ガバメント推進標準ガイドライン」（デジタル社会推進会議幹事会決定。2022 年４月 20 日最終改訂）の内容を踏まえ、次の事項を実施する。

（ア）現状の把握と分析（利用者の把握と分析、業務の把握と分析、データの把握と分析、情報システム運用の把握と分析等）
（イ）業務要件の定義
（ウ）機能要件の定義（機能（アナライザ機能を含む）、画面、帳票、データ、外部インタフェースに関する事項）
（エ）非機能要件の定義（ユーザビリティ及びアクセシビリティ、システム方式、規模、性能、信頼性、拡張性、上位互換性、中立性、継続性、情報セキュリティ、情報システム稼働環境、テスト、移行、引継ぎ、教育、クラウド移行後の新システムの運用、保守業務要件に関する事項）
（オ）システム方式の決定
（カ）移行経費及び新システム運用・保守経費の見積り

なお、国家 DB 運用・データ整備等事業受託者や国家 DB 賃貸借・保守事業受託者とも連携をとるよう留意すること。

（２）引継ぎ

受注者は、本業務の作業経緯、残存課題等を文書化し、担当部署に対して確実な引継ぎを行うこと。また、本業務における検討結果を当システムのプロジェクト計画書に適宜反映及び内容変更の支援をすること。

（３）作業実施計画の作成及び情報資産管理標準シートの提出

受注者は、プロジェクト計画書及びプロジェクト管理要領と整合をとりつつ、林野庁担当者の指示に基づき、作業実施計画書及び作業実施要領の案を作成し、林野庁担当部署の承認を受けること。

なお、作業実施計画書及び作業実施要領の記載内容は、デジタル・ガバメント推進標準ガイドライン「第７章　設計・開発」で定義されている事項を踏まえたものとする。

受注者は、別添２　「情報システムの経費区分」に基づき区分等した契約金額の内訳を記載した情報資産管理標準シートを契約締結後速やかに提出すること。

受注者は、林野庁担当者から求められた場合は、スケジュールや工数等の計画値及び実績値について記載した情報資産管理標準シートを提出すること。

（４）打合せの実施

ア　受注者は、打合せを毎月開催するとともに、業務の進捗状況を作業実施要領に基づき報告すること。なお、打合せの内容が進捗状況の報告のみで、あらかじめ林野庁担当部署の承認を得た場合は、メール等による進捗状況の報告をもって打合せにかえることができる。

イ　林野庁担当部署から要請があった場合又は受注者が必要と判断した場合は、必要資料を作成の上、打合せを開催すること。

ウ　受注者は、打合せ終了後、林野庁担当部署が議事録の作成を不要と判断した場合を除き、３日以内（行政機関の休日（行政機関の休日に関する法律（昭和 63 年法律第 91 号）第１条第１項各号に掲げる日をいう。）を除く。）に議事録を作成し、林野庁担当部署の承認を受けること。

（５）成果物

ア　成果物名

本業務の成果物一覧を表１に示す。

表１　成果物一覧

項	成果物名	納品期日
２（３）	・作業実施計画書（案）及び 作業実施要領（案） ・契約金額の内訳を記載した情報資産管理標準シート	契約締結日から 20 開庁日以内
２（１）	・クラウド移行業務　要件定義書 ２（１）（ア）～（カ）の内容を含む	令和５年２月 28 日
２（２）	・引継ぎ事項を文書化した資料	令和５年２月 28 日
２（４）	・打合せの議事録	林野庁担当部署が議事録の作成を不要と判断した場合を除き、会議終了後３開庁日以内
３（１）	・作業実施体制図 ・情報セキュリティ対策管理体制図	契約締結日から 20 開庁日以内

ア　成果物の納品方法

- 成果物は、全て日本語で作成すること。
- 用字・用語・記述符号の表記については、「公用文作成の考え方」の周知について（令和４年１月 11 日内閣文第１号内閣官房長官通知）」を参考にすること。
- 情報処理に関する用語の表記については、日本産業規格（JIS）の規定を参考とすること。

・　成果物は紙媒体及び電磁的記録媒体により作成し、林野庁担当部署から特別に示す場合を除き、原則紙媒体を正・副各１部、電磁的記録媒体１部を納品すること。
・　紙媒体により納品する用紙のサイズは、原則として日本産業規格Ａ列４番とするが、必要に応じて日本産業規格Ａ列３番を使用すること。
・　電磁的記録媒体による納品について、Microsoft Office 又は PDF のファイル形式で作成し、CD-R 等の電磁的記録媒体に格納して納品すること。
・　納品後、林野庁担当部署において改変が可能となるよう、図表等の元データも併せて納品すること。
・　成果物の作成に当たって、特別なツールを使用する場合は、林野庁担当部署の承認を得ること。
・　成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。
・　電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう適切に対処すること。なお、対策ソフトウェアに関する情報（対策ソフトウェア名称、定義パターンバージョン、確認年月日）を記載したラベルを貼り付けること。

イ　成果物の納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、林野庁担当部署が納品場所を別途指示する場合はこの限りではない。

〒100－8952　東京都千代田区霞が関 1-2-1

林野庁森林整備部森林利用課吸収源推進班（ドア番号：別 710）

３　作業の実施体制・方法

（１）作業実施体制

本業務の推進体制及び本業務受注者に求める作業実施体制は図５及び表２のとおりである。なお、受注者内の人員構成については想定であり、受注者決定後に林野庁担当部署と協議の上見直しを行う。また、作業実施体制図とは別に、受注者の情報セキュリティ対策管理体制図を作成し提出すること。

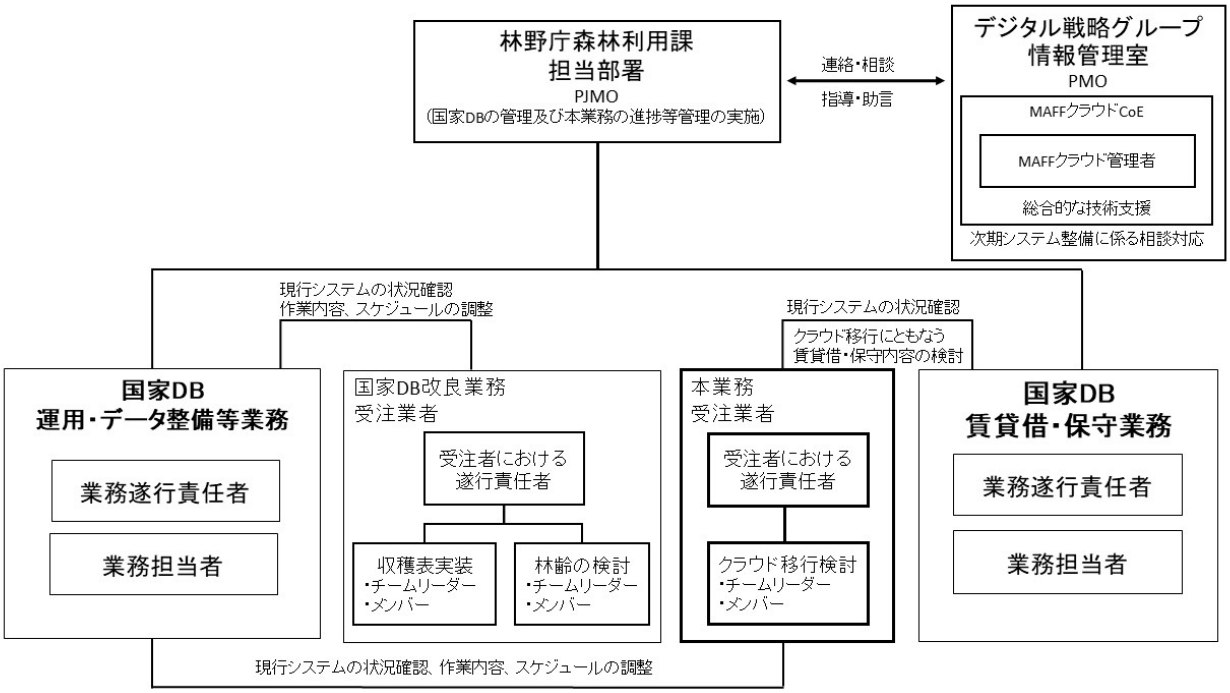


図５　本業務の推進体制及び本業務受注者に求める作業実施体制

組織等	本業務における役割
林野庁森林利用課	国家DBの管理組織として、本業務の進捗等を管理する。
本業務受注業者	本業務を実施する。
国家DB運用・データ整備等事業受託者	国家DBの運用を行う。
国家DB賃貸借・保守事業受託者	国家DBの機器等のリース及び保守を行う。
PMO	担当部署からの次期システム整備に係る相談対応を行う。 また、政府共通プラットフォームに係る農林水産省の連絡窓口としての役割を行う。
MAFFクラウドCoE	担当部署・受注者に対してパブリック・クラウド全般及びMAFFクラウド利用に係る技術的な支援を行う。

表２　本業務における組織等の役割

（２）作業要員に求める資格等の要件

ア　業務遂行責任者を配置すること。

イ　業務に従事する者の中で、林野庁担当部署との連絡・調整を行う者を１人以上配置すること。

ウ　業務に従事する者の中で、オラクルマスター（シルバー以上）の資格保持者を１人以上配置すること。

エ　国家 DB クラウド移行に向けた準備業務を担当するチームの担当メンバーは、パブリック・ク

ラウドに係る全ての技術領域において、当該クラウドサービスプロバイダーの認定技術者として中級資格[※]以上のものを有するものを含めること。

※　例として、以下のような資格が挙げられる。また、クラウドシステムに関する技術的指導の活動実績がある等、ＩＴスキル基準（ＩＴＳＳ）のレベル３相当以上の実績を示すことができる場合も中級資格以上に相当するものとする。

・AWS 認定ソリューションアーキテクト-アソシエイト試験

・マイクロソフト認定ソリューションアソシエイト試験

エ　データベース運用や設計開発等情報処理業務の経験が５年以上の者を１人以上配置すること。

オ　業務責任者及び業務に従事する者が何らかの理由で業務に従事できなくなった場合又はできなくなることが想定される場合は、遅滞なく代わりの者を配置し、林野庁担当部署に報告すること。

※ ウ、エについては該当資格を保有する者に委任し、又は請け負わせる場合も可とする。

※これら従事者の役割は、業務実施可能な範囲において兼務させることを可能とする。

（３）作業場所

本業務の作業場所及び作業に当たり必要となる設備、備品、消耗品等については、受注者の責任において用意すること。また、必要に応じて林野庁担当職員が現地確認を実施することができるものとする。

（４） 作業の管理に関する要領

受注者は、担当部署が承認した作業実施計画書の作業体制、スケジュール、開発形態、開発手法、開発環境、開発ツール等に従い、記載された成果物を作成すること。その際、作業実施要領に従い、コミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

４　作業の実施に当たっての遵守事項

（１）機密保持、資料の取扱い

ア 受注者は、「農林水産省における情報セキュリティの確保に関する規則」（平成 27 年農林水産省訓令第４号。以下「セキュリティ規則」という。）等の説明を受けるとともに、本業務に係る情報セキュリティ要件を遵守すること。なお、セキュリティ規則は、政府機関等の情報セキュリティ対策のための統一基準群（以下「統一基準群」という。）に準拠することとされていることから、受託者は、統一基準群の改定を踏まえてセキュリティ規則が改正された場合には、本業務に関する影響分析を行うこと。

イ 受注者は、別添２　「情報セキュリティの確保に関する共通基本仕様」に基づき作業を行うこと。

（２）標準ガイドラインの遵守

受注者が、本業務を遂行するに当たっては、標準ガイドラインに基づき作業を行うこと。具体的な作業内容及び手順等については、「デジタル・ガバメント推進標準ガイドライン解説書（内閣官

房情報通信技術（IT）総合戦略室)」（以下「解説書」という。）を参考とすること。なお、「標準ガイドライン」及び「解説書」が改定された場合は、最新のものを参照し、その内容に従うこと。

（３）その他文書、標準への準拠

業務遂行に当たっては、林野庁担当部署が定めるプロジェクト計画書との整合を確保して行うこと。

（４）情報システム監査

農林水産省が本調達において整備又は管理を行う情報システムに伴うリスクとその対応状況を客観的に評価するため、情報システム監査の実施を必要と判断した場合に受注者は、農林水産省が定めた実施内容（監査内容、対象範囲、実施者等）に基づく情報システム監査を受け入れること（農林水産省が別途選定した事業者による監査を含む。）。

情報システム監査で問題点の指摘又は改善案の提示を受けた場合に受注者は、林野庁担当部署と対応案を協議し、指示された期間までに是正を図ること。

（５）情報セキュリティ要件への対応

本業務の遂行に当たり、以下の内容を含む情報セキュリティ対策を実施し、情報セキュリティ水準の低下を招かないこと。

ア　提供するアプリケーション・コンテンツに不正プログラムを含めないこと。

イ　提供するアプリケーションにぜい弱性を含めないこと。

ウ　実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

エ　電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。

オ　提供するアプリケーション・コンテンツの利用時に、ぜい弱性が存在するバージョンのＯＳやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、ＯＳやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。

カ　サービス利用に当たって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

キ　「.go.jp」で終わるドメインを使用してアプリケーション・コンテンツを提供すること。

ク　詳細については、担当部署から「アプリケーション・コンテンツの作成及び提供に関する規程」の説明を受けるとともに、それに基づきアプリケーション・コンテンツの作成及び提供を行うこと。

受注者は、情報システムに係る政府調達におけるセキュリティ要件策定マニュアル（2019 年 9 月 24 日 内閣サイバーセキュリティセンター)」の点検を行い、要件定義書に反映すること。

５　成果物の取扱いに関する事項

（１）知的財産権の帰属

ア　本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む。）は、受注者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書にて権利譲渡不可能と示されたもの以外は、全て林野庁に帰属するものとする。

イ　林野庁は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、それらの利用を第三者に許諾すること（以下「複製等」という。）ができるとともに、任意に開示できるものとする。また、受注者は、成果物について、複製等ができるものとする。ただし、複製等により林野庁がその業務を遂行する上で支障が生じるおそれがある旨を契約締結時までに通知したときは、複製等ができる範囲やその方法等について協議するものとする。

ウ　受注者は、納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の受注者は、当該既存著作物の内容について事前に林野庁の承認を得ることとし、林野庁は、既存著作物等について当該許諾条件の範囲で使用するものとする。なお、本仕様に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争の原因が専ら林野庁の責めに帰す場合を除き、受注者の責任及び負担において一切を処理すること。この場合、林野庁は係る紛争等の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講じるものとする。

エ　本調達に係るプログラムに関する権利（著作権法第 21 条から第 28 条に定める全ての権利を含む。）及び成果物の所有権は、林野庁から受注者に対価が完済されたとき受注者から林野庁に移転するものとする。

オ 受注者は林野庁に対し、一切の著作者人格権を行使しないものとし、また、第三者に行使させないものとする。

カ 受注者は、使用する画像、デザイン、表現等に関して他者の著作権を侵害する行為に十分配慮し、これを行わないこと。

（２）契約不適合責任

ア　林野庁は検収完了後、成果物についてシステム仕様書との不一致（バグも含む。以下「契約不適合」という。）が発見された場合、受注者に対して当該契約不適合の修正等の履行の追完（以下「追完」という。）を請求することができ、受注者は、当該追完を行うものとすること。ただし、林野庁が追完の方法についても請求した場合であって、林野庁に不相当な負担を課するものでないときは、受注者は林野庁が請求した方法と異なる方法による追完を行うことができること。

イ　前号にかかわらず、当該契約不適合によっても個別契約の目的を達することができる場合であって、追完に過分の費用を要する場合、受注者は前号に規定された追完に係る義務を負わないものとすること。

ウ　林野庁は、当該契約不適合（受注者の責めに帰すべき事由により生じたものに限る。）により損害を被った場合、受注者に対して損害賠償を請求することができること。

エ　当該契約不適合について、追完の請求にもかかわらず相当期間内に追完がなされない場合又は追完の見込みがない場合で、当該契約不適合により個別契約の目的を達することができないときは、林野庁は本契約及び個別契約の全部又は一部を解除することができること。

オ　受注者が本項に定める責任その他の契約不適合責任を負うのは、検収完了後１年以内に林野庁から当該契約不適合を通知された場合に限るものとすること。ただし、検収完了時において受注者が当該契約不適合を知り若しくは重過失により知らなかったとき、又は当該契約不適合が受注者の故意若しくは重過失に起因するときにはこの限りでない。

カ　前各号の規定は、契約不適合が林野庁の提供した資料等又は農林水産省の与えた指示によって生じたときは適用しないこと。ただし、受注者がその資料等又は指示が不適当であることを知りながら告げなかったときはこの限りでない。

（３）検収

ア　受注者は、成果物等について、納品期日までに林野庁担当部署に内容の説明を実施して検収を受けること。

イ　検収の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について林野庁担当部署に説明を行った上で、指定された日時までに再度納品すること。

６　入札参加資格に関する事項

（１）予算決算及び会計令(昭和 22 年勅令第 165 号）第 70 条各号のいずれかに該当する者でないこと。なお、競争に参加する者が未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者である場合は、同条の特別の理由がある場合に該当する。

（２）予算決算及び会計令第 71 条の規定に該当する者でないこと。

（３）令和４・５・６年度農林水産省競争参加資格（全省庁統一資格）の「役務の提供等」に格付けされ、競争参加資格を有する者であること。

（４）入札書及び提案書等の提出期限の日から、開札の時までの間において林野庁長官から「物品の製造契約、物品の購入契約及び役務等契約指名停止措置要領」に基づく指名停止を受けている期間中でないこと。

（５）本業務を直接担当する農林水産省ＩＴテクニカルアドバイザー（旧農林水産省ＣＩＯ補佐官に相当）、農林水産省全体管理組織（ＰＭＯ）支援スタッフ及び農林水産省最高情報セキュリティアドバイザーが、その現に属する事業者及びこの事業者の「財務諸表等の用語、様式及び作成方法に関する規則」　（昭和 38 年大蔵省令第 59 号）第８条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先等緊密な利害関係を有する事業者は、本書に係る業務に関して入札に参加できないものとする。

（６）複数の団体が本委託事業の受託のために組織した共同事業体（民法（明治 29 年法律第 89 号）上の組合に該当するもの。以下同じ。）による参加も可とする。

この場合において共同事業体は、本委託事業を実施すること等について業務分担及び実施体制等を明確にした、構成する各団体（以下「構成員」という。）の全てから同意を得た規約書、全構成員が交わした協定書又は全構成員間での契約締結書（又はこれに準ずる書類）（以

下「規約書等」という。）を作成する必要があり、全構成員の中から代表者を選定し、代表者は本委託事業に係る競争入札の参加及び事業の委託契約手続を行うとともに、業務の追考に当たっては、代表者を中心に各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。

また、全構成員は、上記（１）から（５）の要件に適合している必要がある。

なお、共同事業体に参加する構成員は、本入札において他の共同事業体の構成員となること又は単独で参加することはできない。

①共同事業体の結成、運営等に関する規約書等を入札書の提出期限までに提出すること。

②規約書等の作成にあたっては、事業分担とその考え方、実施体制及び解散後の契約不適合責任について、明確に記載すること。

７　再委託に関する事項

（１）再委託の制限及び再委託を認める場合の条件

ア　予算決算及び会計令（昭和 22 年勅令第 165 号）第 70 条各号のいずれかに該当する者でないこと。なお、競争に参加する者が未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者である場合は、同条の特別の理由がある場合に該当する。本業務の受注者は、業務を一括して又は主たる部分を再委託してはならない。

イ　受注者における遂行責任者を再委託先事業者の社員や契約社員とすることはできない。

ウ　受注者は再委託先の行為について一切の責任を負うものとする。

エ　再委託先における情報セキュリティの確保については受注者の責任とする。

オ　再委託を行う場合、再委託先が「６　入札参加資格に関する事項」の（1）から（5）に示す要件を満たすこと。

(2)承認手続

ア　本業務の実施の一部を合理的な理由及び必要性により再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性及び契約金額等について記載した別添の再委託承認申請書を林野庁に提出し、あらかじめ承認を受けること。

イ　前項による再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託に関する書面を林野庁に提出し、承認を受けること。

ウ　再委託の相手方が更に委託を行うなど複数の段階で再委託が行われる場合（以下「再々委託」という。）には、当該再々委託の相手方の商号又は名称及び住所並びに再々委託を行う業務の範囲を書面で報告すること。

(3)再委託先の契約違反等

再委託先において、本調達仕様書の遵守事項に定める事項に関する義務違反又は義務を怠った場合には、受注者が一切の責任を負うとともに、林野庁は、当該再委託先への再委託の中止を請求することができる。

８　附属文書

（１）別添１　情報セキュリティの確保に関する共通基本仕様

（２）別添２　情報システムの経費区分

（３）別添３　農林水産省クラウド利用ガイドライン

９　その他特記事項

・MAFF クラウドについて不明点等がある場合は、担当部署及び MAFF クラウド CoE との協議の上、作業を進めること。

・本調達仕様書と契約書の内容に齟齬が生じた場合には、本調達仕様書の内容が優先すること。

・本仕様書について疑義等がある場合は、質問書により質問すること。なお、質問書に対する回答は適宜行うこととする。

・農林水産省は、令和５年度に農林水産省統合ネットワークをガバメントソリューションサービス（GSS）に移行する予定である。当該 GSS についてはデジタル庁において検討されており、詳細について順次検討が進められているところ、担当部署の求めに応じ、移行に必要な情報提供、質疑応答等の協力を行うこと。

・本業務の実施に参考となる過去の類似業務の報告書等に関する資料については、林野庁内にて閲覧可能とする。なお、資料の閲覧に当たっては、必ず事前に担当部署まで連絡の上、閲覧日時を調整すること。

ア　資料閲覧場所

東京都千代田区霞が関 1-2-1　林野庁森林整備部森林利用課（別階７階ドア番号別 710）

イ　閲覧期間及び時間

令和４年９月６日から令和４年 ９ 月 26 日まで

行政機関の休日を除く日の 10 時から 17 時まで。(12 時から 13 時を除く。)

ウ　閲覧手続

最大３名まで。応札希望者の商号、連絡先、閲覧希望者氏名を規定の「閲覧申込書」に記載の上、閲覧希望日の２日前までに提出すること。また、閲覧日当日までに規定の「守秘義務に関する誓約書」に記載の上、提出すること。

エ　閲覧時の注意

閲覧にて知り得た内容については、提案書の作成以外には使用しないこと。また、本調達に関与しない者等に情報が漏えいしないように留意すること。閲覧資料の複写等による閲覧内容の記録は行わないこと。

オ　連絡先

林野庁森林整備部森林利用課森林吸収源推進班　電話 03－3502－8240（直通）

カ　事業者が閲覧できる資料

閲覧に供する資料の例を次に示す。

(ア)プロジェクト計画書

(イ)遵守すべき農林水産省独自の規定類

a 農林水産省における情報セキュリティの確保に関する規則

b 農林水産省における個人情報の適正な取扱いのための措置に関する訓令

(ウ)現行の情報システムの情報システム設計書、操作マニュアル

(エ) 過去のシステム関係資料等

・本事業における人件費の算定に当っては、別添の「委託事業における人件費の算定等の適正化について」に従って行うものとする。なお、発注者は受諾者から提出された人件費の算定について確認す

るため、原則として人件費単価表（受諾者が組織として人件費単価を定めている場合）又は実際に従事する（した）者の給与明細を確認します。

以　上

情報セキュリティの確保に関する共通基本仕様

Ⅰ　情報セキュリティポリシーの遵守

１　受託者は、担当部署から農林水産省における情報セキュリティの確保に関する規則（平成27 年農林水産省訓令第４号。以下「規則」という。）等の説明を受けるとともに、本業務に係る情報セキュリティ要件を遵守すること。

なお、規則は、政府機関等の情報セキュリティ対策のための統一基準群（以下「統一基準群」という。）に準拠することとされていることから、受託者は、統一基準群の改定を踏まえて規則が改正された場合には、本業務に関する影響分析を行うこと。

２　受託者は、規則と同等の情報セキュリティ管理体制を整備していること。

３　受託者は、本業務の従事者に対して、規則と同等の情報セキュリティ対策の教育を実施していること。

Ⅱ　受託者及び業務実施体制に関する情報の提供

１　受託者は、受託者の資本関係・役員等の情報、本業務の実施場所、本業務の従事者（契約社員、派遣社員等の雇用形態は問わず、本業務に従事する全ての要員）の所属・専門性（保有資格、研修受講実績等）・実績（業務実績、経験年数等）及び国籍に関する情報を記載した資料を提出すること。

なお、本業務に従事する全ての要員に関する情報を記載することが困難な場合は、本業務に従事する主要な要員に関する情報を記載するとともに、本業務に従事する部門等における従事者に関する情報（〇〇国籍の者が△名（又は□%）等）を記載すること。また、この場合であっても、担当部署からの要求に応じて、可能な限り要員に関する情報を提供すること。

２　受託者は、本業務を実施する部署、体制等の情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。）

（1）ISO/IEC27001 等の国際規格とそれに基づく認証の証明書等

（2）プライバシーマーク又はそれと同等の認証の証明書等

（3）独立行政法人情報処理推進機構（IPA）が公開する「情報セキュリティ対策ベンチマーク」を利用した自己評価を行い、その評価結果において、全項目に係る平均値が4に達し、かつ各評価項目の成熟度が2以上であることが確認できる確認書

（4）MS 認証信頼性向上イニシアティブに参画し、不祥事への対応や透明性確保に係る取組を実施している実績

Ⅲ　業務の実施における情報セキュリティの確保

１　受託者は、本業務の実施に当たって、以下の措置を講じること。また、以下の措置を講じることを証明する資料を提出すること。

（１）本業務上知り得た情報（公知の情報を除く。）については、契約期間中はもとより契約終了後においても第三者に開示及び本業務以外の目的で利用しないこと。

（２）本業務に従事した要員が異動、退職等をした後においても有効な守秘義務契約を締結すること。

（３）本業務の各工程において、農林水産省の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図、第三者機関による品質保証体制を証明する書類等を提出すること。）。

（４）本業務において、農林水産省の意図しない変更が行われるなどの不正が見つかったときに、追跡調査や立入調査等、農林水産省と連携して原因を調査し、排除するための手順及び体制（例えば、システムの操作ログや作業履歴等を記録し、担当部署から要求された場合には提出するなど）を整備していること。

（５）本業務において、個人情報又は農林水産省における要機密情報を取り扱う場合は、当該情報（複製を含む。以下同じ。）を国内において取り扱うものとし、当該情報の国外への送信・保存や当該情報への国外からのアクセスを行わないこと。

（６）本業務における情報セキュリティ対策の履行状況を定期的に報告すること。

（７）農林水産省が情報セキュリティ監査の実施を必要と判断した場合は、農林水産省又は農林水産省が選定した事業者による立入調査等の情報セキュリティ監査（サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 25 条第１項第２号に基づく監査等を含む。以下同じ。）を受け入れること。また、担当部署からの要求があった場合は、受託者が自ら実施した内部監査及び外部監査の結果を報告すること。

（８）本業務において、要安定情報を取り扱うなど、担当部署が可用性を確保する必要があると認めた場合は、サービスレベルの保証を行うこと。

（９）本業務において、第三者に情報が漏えいするなどの情報セキュリティインシデントが発生した場合は、担当部署に対し、速やかに電話、口頭等で報告するとともに、報告書を提出すること。また、農林水産省の指示に従い、事態の収拾、被害の拡大防止、復旧、再発防止等に全力を挙げること。なお、これらに要する費用の全ては受託者が負担すること。

（10）情報セキュリティ対策の履行が不十分な場合、農林水産省と協議の上、必要な改善策を立案し、速やかに実施するなど、適切に対処すること。

２　受託者は、私物（本業務の従事者個人の所有物等、受託者管理外のものをいう。）の機器等を本業務に用いないこと。

３　受託者は、成果物等を電磁的記録媒体により納品する場合には、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう、適切に対処するとともに、確認結果（確認日時、不正プログラム対策ソフトウェアの製品名、定義ファイルのバージョン等）を成果物等に記載又は添付すること。

４　受託者は、本業務において取り扱われた情報を、担当部署の指示に従い、本業務上不要

となったとき若しくは本業務の終了までに返却又は復元できないよう抹消し、その結果を担当部署に書面で報告すること。

Ⅳ　情報システムの各工程における情報セキュリティの確保

１　受託者は、本業務において情報システムの運用管理機能又は設計・開発に係る企画・要件定義を行う場合には、以下の措置を実施すること。

（１）情報システム運用時のセキュリティ監視等の運用管理機能を明確化し、本業務の成果物へ適切に反映するために、以下を含む措置を実施すること。

ア　情報システム運用時に情報セキュリティ確保のために必要となる管理機能を本業務の成果物に明記すること。

イ　情報セキュリティインシデントの発生を監視する必要がある場合、監視のために必要な機能について、以下を例とする機能を本業務の成果物に明記すること。

（ア）農林水産省外と通信回線で接続している箇所における外部からの不正アクセスを監視する機能

（イ）不正プログラム感染や踏み台に利用されること等による農林水産省外への不正な通信を監視する機能

（ウ）農林水産省内通信回線への端末の接続を監視する機能

（エ）端末への外部電磁的記録媒体の挿入を監視する機能

（オ）サーバ装置等の機器の動作を監視する機能

（２）開発する情報システムに関連する脆（ぜい）弱性への対策が実施されるよう、以下を含む対策を本業務の成果物に明記すること。

ア　既知の脆（ぜい）弱性が存在するソフトウェアや機能モジュールを情報システムの構成要素としないこと。

イ　開発時に情報システムに脆（ぜい）弱性が混入されることを防ぐためのセキュリティ実装方針を定めること。

ウ　セキュリティ侵害につながる脆（ぜい）弱性が情報システムに存在することが発覚した場合に修正が施されること。

エ　ソフトウェアのサポート期間又はサポート打ち切り計画に関する情報を提供すること。

２　受託者は、本業務において情報システムの設計・開発を行う場合には、以下の事項を含む措置を適切に実施すること。

（１）情報システムのセキュリティ要件の適切な実装

ア　主体認証機能

イ　アクセス制御機能

ウ　権限管理機能

エ　識別コード・主体認証情報の付与管理

オ　ログの取得・管理

カ　暗号化機能・電子署名機能

キ　暗号化・電子署名に係る管理

ク　ソフトウェアに関する脆（ぜい）弱性等対策

ケ　不正プログラム対策

コ　サービス不能攻撃対策

サ　標的型攻撃対策

シ　アプリケーション・コンテンツのセキュリティ要件の策定

ス　政府ドメイン名（go.jp）の使用

セ　不正なウェブサイトへの誘導防止

ソ　農林水産省外のアプリケーション・コンテンツの告知

（２）情報セキュリティの観点に基づく試験の実施

ア　ソフトウェアの開発及び試験を行う場合は、運用中の情報システムと分離して実施すること。

イ　試験項目及び試験方法を定め、これに基づいて試験を実施すること。

ウ　試験の実施記録を作成し保存すること。

（３）情報システムの開発環境及び開発工程における情報セキュリティ対策

ア　ソースコードが不正に変更されることを防止するため、ソースコードの変更管理、アクセス制御及びバックアップの取得について適切に管理すること。

イ　調達仕様書等に規定されたセキュリティ実装方針に従うこと。

ウ　セキュリティ機能の適切な実装、セキュリティ実装方針に従った実装が行われていることを確認するために、情報システムの設計及びソースコードを精査する範囲及び方法を定め実施すること。

エ　オフショア開発を実施する場合、試験データとして実データを使用しないこと。

３　受託者は、情報セキュリティの観点から調達仕様書で求める要件以外に必要となる措置がある場合には、担当部署に報告し、協議の上、対策を講ずること。

４　受託者は、本業務において情報システムの運用・保守を行う場合には、情報システムに実装されたセキュリティ機能が適切に運用されるよう、以下の事項を適切に実施すること。

（１）情報システムの運用環境に課せられるべき条件の整備

（２）情報システムのセキュリティ監視を行う場合の監視手順や連絡方法

（３）情報システムの保守における情報セキュリティ対策

（４）運用中の情報システムに脆（ぜい）弱性が存在することが判明した場合の情報セキュリティ対策

（５）利用するソフトウェアのサポート期限等の定期的な情報収集及び報告

（６）「デジタル・ガバメント推進標準ガイドライン」(2019 年 2 月 25 日各府省情報化統括責任者（CIO）連絡会議決定)の別紙3に基づく情報資産管理を行うために必要な事項を記載した情報資産管理標準シートの提出

（7）情報システムの利用者に使用を求めるソフトウェアのバージョンのサポート終了時における、サポート継続中のバージョンでの動作検証及び当該バージョンで正常に動作させるための情報システムの改修等

5　受託者は、本業務において情報システムの運用・保守を行う場合には、運用保守段階へ移行する前に、移行手順及び移行環境に関して、以下を含む情報セキュリティ対策を行うこと。

（1）情報セキュリティに関わる運用保守体制の整備

（2）運用保守要員へのセキュリティ機能の利用方法等に関わる教育の実施

（3）情報セキュリティインシデント（可能性がある事象を含む。以下同じ。）を認知した際の対処方法の確立

6　受託者は、本業務において情報システムのセキュリティ監視を行う場合には、以下の内容を含む監視手順を定め、適切に監視運用すること。

（1）監視するイベントの種類

（2）監視体制

（3）監視状況の報告手順

（4）情報セキュリティインシデントの可能性がある事象を認知した場合の報告手順

（5）監視運用における情報の取扱い（機密性の確保）

7　受託者は、本業務において運用中の情報システムに脆（ぜい）弱性が存在することを発見した場合には、速やかに担当部署に報告し、本業務における運用・保守要件に従って脆（ぜい）弱性の対策を行うこと。

8　受託者は、本業務において本業務の調達範囲外の情報システムを基盤とした情報システムを運用する場合は、運用管理する府省庁等との責任分界に応じた運用管理体制の下、基盤となる情報システムの運用管理規程等に従い、基盤全体の情報セキュリティ水準を低下させることのないよう、適切に情報システムを運用すること。

9　受託者は、本業務において情報システムの運用・保守を行う場合には、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理すること。

10　受託者は、本業務において情報システムの更改又は廃棄を行う場合には、当該情報システムに保存されている情報について、以下の措置を適切に講ずること。

（1）情報システム更改時の情報の移行作業における情報セキュリティ対策

（2）情報システム廃棄時の不要な情報の抹消

Ⅴ　クラウドサービスに関する情報セキュリティの確保

受託者は、本業務において、クラウドサービスを活用する場合には、以下の措置を講じること。また、当該クラウドサービスの活用が本業務の再委託に該当する場合は、当該クラウドサービスに対して、Ⅷの措置を講じること。

1　ISO/IEC27001 又はそれに基づく認証を取得しているクラウドサービスを採用すること。また、

当該認証の証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。）

２　クラウドサービスの情報セキュリティ水準を証明する以下のいずれかの証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。）

（１）ISO/IEC 27017 又は ISMS（情報セキュリティマネジメントシステム）クラウドセキュリティ認証制度に基づく認証

（２）セキュリティに係る内部統制の保証報告書（SOC 報告書（Service Organization Control Report））

（３）情報セキュリティ監査により対策の有効性が適切であることを証明する報告書（クラウド情報セキュリティ監査制度に基づく CS マークが付された CS 言明書等）

３　クラウドサービスにおいて個人情報又は農林水産省における要機密情報が取り扱われる場合には、当該クラウドサービスのデータセンター（バックアップセンターを含む。）は国内に限ること。

４　クラウドサービスの廃止、サービス内容の変更等に伴い契約を終了する場合は、他のクラウドサービス等に円滑に移行できるよう、十分な期間をもって事前（サービス廃止等の１年以上前が望ましい。）に担当部署へ通知すること。

５　クラウドサービスの契約を終了する場合、クラウドサービス上に保存された農林水産省のデータについて、汎用性のあるデータ形式に変換して提供するとともに、クラウドサービス上において復元できないよう抹消し、その結果を担当部署に書面で報告すること。

６　クラウドサービスに係るアクセスログ等の証跡を保存し、担当部署からの要求があった場合は提供すること。なお、証跡は１年間以上保存することが望ましい。

７　インターネット回線とクラウド基盤との接続点の通信を監視すること。

８　クラウドサービスに係る業務の一部がクラウドサービス事業者以外の事業者に外部委託されている場合は、当該クラウドサービス事業者以外の事業者にⅧの措置を講ずること。

９　クラウドサービスにおける脆（ぜい）弱性対策の実施内容を担当部署が確認できること。

10　クラウドサービスの可用性を保証するための十分な冗長性、障害時の円滑な切替等の対策が講じられていること。また、クラウドサービスに障害が発生した場合の復旧時点目標（RPO）等の指標を提示すること。

なお、農林水産省の要安定情報を取り扱う場合は、データセンターを地理的に離れた複数の地域に設置するなどの災害対策が講じられていること。

11　クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。

12　クラウドサービスの利用者が、自らの意思によりクラウドサービス上で取り扱う情報を確実に抹消できること。

13　本業務において、農林水産省に開示することとしているクラウドサービスに係る情報について、業務開始時に開示項目や範囲を明記した資料を提出すること。

14　農林水産省に対して、クラウドサービスに係る機密性の高い情報を開示する場合は、農林

水産省において、当該情報を審査又は本業務以外の目的で利用しないよう適切に取り扱うため、必要に応じて当該情報に取扱制限を明記するなどの措置を講じること。

Ⅵ　機器等に関する情報セキュリティの確保

受託者は、本業務において、農林水産省にサーバ装置、端末、通信回線装置、複合機、特定用途機器、外部電磁的記録媒体、ソフトウェア等（以下「機器等」という。）を納品、賃貸借等をする場合には、以下の措置を講じること。

１　納入する機器等の製造工程において、農林水産省が意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

２　機器等に対して不正な変更があった場合に識別できる構成管理体制を確立していること。また、不正な変更が発見された場合に、農林水産省と受託者が連携して原因を調査・排除できる体制を整備していること。

３　機器等の設置時や保守時に、情報セキュリティの確保に必要なサポートを行うこと。

４　利用マニュアル・ガイダンスが適切に整備された機器等を採用すること。

５　脆（ぜい）弱性検査等のテストが実施されている機器等を採用し、そのテストの結果が確認できること。

６　ISO/IEC 15408 に基づく認証を取得している機器等を採用することが望ましい。なお、当該認証を取得している場合は、証明書等の写しを提出すること。（提出時点で有効期限が切れていないこと。）

７　情報システムを構成するソフトウェアについては、運用中にサポートが終了しないよう、サポート期間が十分に確保されたものを選定し、可能な限り最新版を採用するとともに、ソフトウェアの種類、バージョン及びサポート期限について報告すること。なお、サポート期限が事前に公表されていない場合は、情報システムのライフサイクルを踏まえ、販売からの経過年数や後継ソフトウェアの有無等を考慮して選定すること。

８　機器等の納品時に、以下の事項を書面で報告すること。

（１）調達仕様書に指定されているセキュリティ要件の実装状況（セキュリティ要件に係る試験の実施手順及び結果）

（２）機器等に不正プログラムが混入していないこと（最新の定義ファイル等を適用した不正プログラム対策ソフトウェア等によるスキャン結果、内部監査等により不正な変更が加えられていないことを確認した結果等）

Ⅶ　管轄裁判所及び準拠法

１　本業務に係る全ての契約（クラウドサービスを含む。以下同じ。）に関して訴訟の必要が生じた場合の専属的な合意管轄裁判所は、国内の裁判所とすること。

２　本業務に係る全ての契約の成立、効力、履行及び解釈に関する準拠法は、日本法とする

こと。

Ⅷ　業務の再委託における情報セキュリティの確保

１　受託者は、本業務の一部を再委託（再委託先の事業者が受託した事業の一部を別の事業者に委託する再々委託等、多段階の委託を含む。以下同じ。）する場合には、受託者が上記Ⅱの１、Ⅱの２及びⅢの１において提出することとしている資料等と同等の再委託先に関する資料等並びに再委託対象とする業務の範囲及び再委託の必要性を記載した申請書を提出し、農林水産省の許可を得ること。

２　受託者は、本業務に係る再委託先の行為について全責任を負うものとする。また、再委託先に対して、受託者と同等の義務を負わせるものとし、再委託先との契約においてその旨を定めること。なお、情報セキュリティ監査については、受託者による再委託先への監査のほか、農林水産省又は農林水産省が選定した事業者による再委託先への立入調査等の監査を受け入れるものとすること。

３　受託者は、担当部署からの要求があった場合は、再委託先における情報セキュリティ対策の履行状況を報告すること。

Ⅸ　資料等の提出

上記Ⅱの１、Ⅱの２、Ⅲの１、Ⅴの１、Ⅴの２、Ⅵの１及びⅥの６において提出することとしている資料等については、最低価格落札方式にあっては入札公告及び入札説明書に定める証明書等の提出場所及び提出期限に従って提出し、総合評価落札方式にあっては提案書等の総合評価のための書類に添付して提出すること。

Ⅹ　変更手続

受託者は、上記Ⅱ、Ⅲ、Ⅴ、Ⅵ及びⅧに関して、農林水産省に提示した内容を変更しようとする場合には、変更する事項、理由等を記載した申請書を提出し、農林水産省の許可を得ること。

別添２　情報システムの経費区分

経費区分		摘要
1）整備経費		情報システムの整備（新規開発、機能改修・追加、更改及びこれらに付随する環境の整備をいう。）に要する一時的な経費
	ア　調査研究等経費	情報システムの整備に当たり、業務の設計、要件定義を行う目的で行う現状分析、プロトタイプ作成、ドキュメント作成支援、調査研究等に要する経費（最適化計画の策定に要する経費を含む。）
	イ　設計経費	情報システムの整備に際し、その開発に関する設計書の作成に要する経費
	ウ　開発経費	情報システムの整備に際し、情報システムのプログラミング、パラメータ設定等による情報システムの開発（単体テストを含む。）に要する経費
	エ　据付調整経費	ハードウェアやラックの搬入・据付け、ネットワークケーブルの敷設等、情報システムの物理的な稼働環境の整備に要する経費
	オ　テスト経費	開発する情報システムの結合テスト、総合テスト及び受入テストに要する経費
	カ　移行経費	情報システムのシステム移行及びデータ移行に要する経費
	キ　廃棄経費	情報システムの廃止及び更改に伴う、ハードウェアやラック、ネットワークケーブル等の撤去及び廃棄に要する経費
	ク　プロジェクト管理支援経費	情報システムの整備に伴うプロジェクト管理支援事業者に要する経費
	ケ　施設整備等経費	情報システムを構成するハードウェアを設置する施設、データ等を保管する施設又は運用事業者等が運用・保守等を行うために駐在する施設の整備、改修等に要する経費
	コ　ハードウェア買取経費	情報システムを構成するハードウェアの買取りに要する経費
	サ　ソフトウェア買取経費	情報システムを構成するソフトウェア製品のライセンスの買取り又は更新に要する経費
	シ　その他整備経費	アからサまでのいずれにも該当しない情報システムの整備に要する経費
2）運用等経費		情報システムの運用、保守等に要する経常的な経費
	ア　システム運用経費	情報システムの正常な稼働を保持するために行うハードウェアの状態ファイルの管理、アプリケーションの設定等の管理、障害に対する予防等の措置など、仕様変更や構成変更を伴わない情報システムの技術的及び管理的業務の実施に要する経費
	イ　業務運用支援経費	情報システムの稼働に当たって、業務実施部門が行う業務（データ作成（Web サイトや e ラーニングのコンテンツ作成等）、データ受付・登録等）の運用支援に要する経費
	ウ　操作研修等経費	情報システムの利用に当たって、当該情報システム部門の担当者又は情報システムの利用者に対する操作研修等（教材作成・更新を含む。）に要する経費
	エ　ヘルプデスク経費	職員等の情報システム利用者からの問合せに対応するために行う業務に要する経費
	オ　コールセンター経費	国民や事業者等の情報システム利用者からの問合せに対応するために行う業務に要する経費

経費区分		摘要
	カ　アプリケーション保守経費	開発した情報システムについて、障害や技術革新等の外部環境の変化に対して情報システムの機能を仕様どおり正常な状態に保つために行うアプリケーションプログラムの改修、設定変更等に要する経費
	キ　ハードウェア保守経費	情報システムを構成するハードウェアについて、障害や技術革新等の外部環境の変化に対して情報システムの機能を仕様どおり正常な状態に保つために行う業務に要する経費
	ク　ソフトウェア保守経費	情報システムを構成するソフトウェア製品について、障害や技術革新等の外部環境の変化に対して情報システムの機能を仕様どおり正常な状態に保つために行う業務に要する経費
	ケ　監査経費	情報システムについて、システム監査又は情報セキュリティ監査の実施に要する経費
	コ　情報セキュリティ検査経費	情報システムについて、ペネトレーションテスト、脆弱性診断等の情報セキュリティ検査・診断の実施に要する経費
	サ　ハードウェア借料	情報システムを構成するハードウェアについて、その使用に要する借料
	シ　ソフトウェア借料	情報システムを構成するソフトウェア製品について、その使用に要する借料
	ス　サービス利用料	情報システムの稼働又は利用に当たって、ASP、SaaS、PaaS、ホスティングサービスなど、国の行政機関以外の者が提供するサービスの利用に要する経費
	セ　通信回線料	情報システムを構成するネットワークにおいて必要となる通信回線の利用に要する経費
	ソ　施設利用等経費	情報システムを構成するハードウェアを設置する施設、データ等を保管する施設又は運用事業者等が運用・保守等を行うために駐在する施設の利用等に要する経費
	タ　その他運用等経費	アからソまでのいずれにも該当しない情報システムの運用等に要する経費
3）その他経費		国の行政機関以外の情報システムに関係する経費及びデジタル・ガバメントの推進のための体制整備に要する経費
(1) 情報システム振興等経費		地方公共団体、独立行政法人等に対する情報システムの整備・運用に関する助成金、補助金、交付金等の経費
	ア　地方公共団体情報システム関係経費	地方公共団体に対する情報システムの整備・運用に関する補助金、交付金等の経費
	イ　独立行政法人等情報システム関係経費	独立行政法人、国立大学法人（大学共同利用機関法人を含む。）、特殊法人、公益法人等に対する情報システムの整備・運用に関する助成金、補助金、交付金（法人の運営に関する経費は除く。）等の経費
(2) デジタル・ガバメントの推進のための体制整備関係経費		高度デジタル人材の登用に要する経費、ＰＭＯの支援スタッフ等に要する経費、内部職員の育成に要する経費等、デジタル・ガバメントの推進のための体制整備に要する経費

農林水産省クラウド利用ガイドライン

2022年（令和4年）3月

農林水産省大臣官房デジタル戦略グループ

改定履歴

改定年月	改定頁	改定内容
令和３年11月	全頁	初版として作成
令和３年12月	４頁,13頁,16頁,19頁～22頁	クラウドサービスの名称変更に伴い、Security CenterをMicrosoft Defender for Cloudに変更 名称変更があった際は読み替えて利用する旨追記
令和３年12月	12頁	MAFFクラウドのAzureADのカスタムドメイン「azcloud.maff.go.jp」を追記 Azureを利用する際の留意事項に事業者を含めた打ち合わせを設定する旨を追記
令和３年12月	６頁	関連資料に机上評価チェックシートを追記
令和４年１月	17項,18項	MAFFクラウド利用時のネットワークに関するページを追加
令和４年２月	15頁	マネージド型脅威検出機能・不適切設定検知機能の利用に関する注意事項を追加

目次

1．本ガイドラインの目的

■　農林水産省においては、システムの新規構築や更改を検討するときは、まずはクラウドサービスの利用を検討することとしています。

■　農林水産省PMOでは、省内の情報システムにおけるクラウドサービスの利用を支援するため、「農林水産省クラウド（MAFFクラウド）」として、利用環境の提供及びクラウド利用への支援を行っています。

■　MAFFクラウド共通機能は、現時点ではISMAPに掲載されたクラウドサービスであるAWSおよびAzureに対応しています。今後MAFFクラウド共通機能が対応するクラウドサービスは追加される可能性があります。

■　本ガイドラインは、MAFFクラウドの全体像、MAFFクラウドが提供する機能、その利用方法について、PJMOとその受託事業者（※）の理解を促すことにより、農林水産省内におけるシステムのクラウド化及びMAFFクラウドの利用を推進することを目的としています。

■　システムの新規構築や更改を検討するPJMOは、このガイドラインを必ず御覧ください。

■　なお、PJMO及び事業者からのこれまでの問合せを「FAQ一覧」として整理しています。こちらについても必要に応じて参照してください。

※ 本ガイドラインは、これからPJMOの事業を受託しようとする者にも提供していただくことができます。
MAFFクラウドの利用を予定している又は既に利用している場合は、入札予定者又は受託事業者に
本ガイドラインをお渡しください。

※クラウドサービスの名称変更が生じた場合は順次修正を行いますが、修正されていない場合は適宜
読み替えて利用してください。

2．本ガイドラインの利用方法

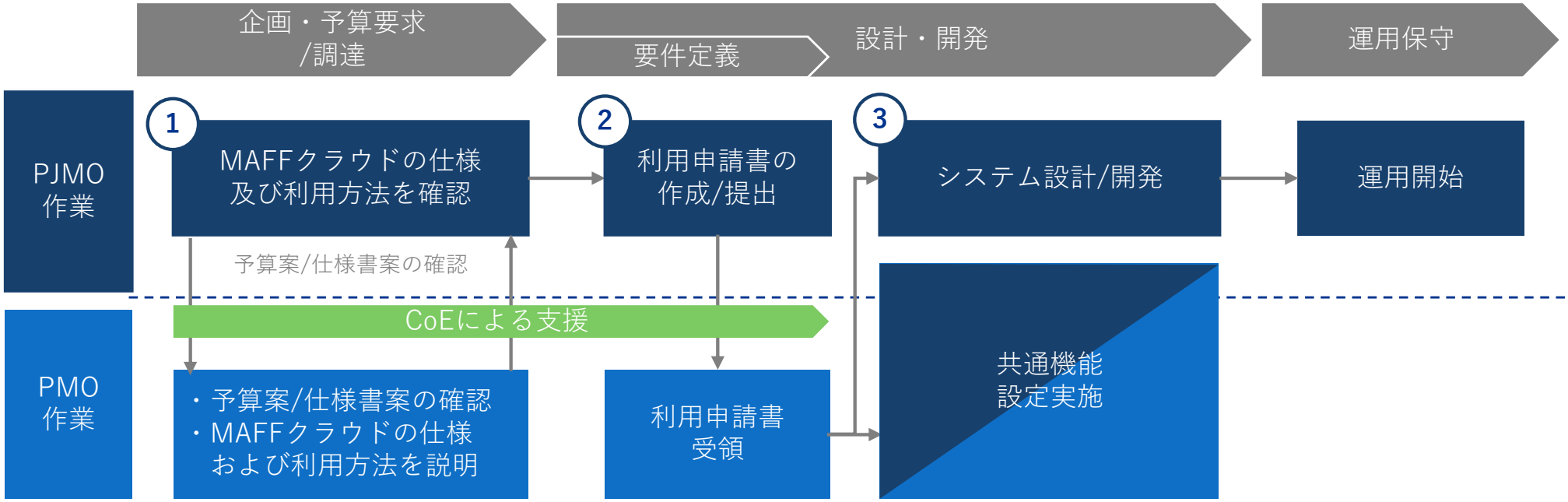
■ PJMOは、その管理する情報システムの以下の開発・作業工程に応じて本ガイドラインの関係箇所を参照してください。

システム開発工程	本資料での参照箇所/想定利用方法
企画・予算要求	• システムのクラウド化検討時には本紙1、3章を参照し、MAFFクラウドの概要及びクラウド移行（MAFFクラウド利用）によるメリット、PoCの実施方法（新規整備システムを除く）を確認ください。 • 予算要求時には本紙2章を参照し、見積依頼先の事業者にMAFFクラウド利用時の調達範囲を明示してください。
調達	• 調達手続き時に本紙2章を参照し利用するMAFFクラウド共通機能の仕様を調達仕様書に記載、または本紙を参考資料として添付し、事業者へMAFFクラウド利用時の調達範囲を明示してください。
設計・開発	• 設計構築前に「農林水産省クラウド利用ガイドライン別紙4_ MAFFクラウド命名規約設計」を事業者へ提示し、規約に沿ったリソースの作成およびタグの設定をするよう依頼してください。 • 設計開始時には本紙1、2章を参照し、MAFFクラウドの利用方法の確認、利用申請を行ってください。
要件定義	• 要件検討時に本紙2章を参照し、MAFFクラウドが提供する共通機能を理解したうえで、MAFFクラウド共通機能を利用する要件、自システムで個別に開発すべき要件の検討を行ってください。

※ 既にAWS/Azureを利用中のシステムにおいては、MAFFクラウド利用検討時に本紙1、2章を参照し、MAFFクラウドの仕様、AWS/Azureを利用中のシステムにおける考慮事項を確認の上、検討してください。

3．本ガイドラインの利用フロー

MAFFクラウド利用フロー



関連資料

1
- 「農林水産省クラウド利用ガイドライン」（本紙）
- 「農林水産省クラウド利用ガイドライン別紙5_FAQ一覧」
- 「机上評価チェックシート」

2
- 「農林水産省クラウド利用ガイドライン別紙1_【システム名】共通機能_利用申請書」

3
- 「農林水産省クラウド利用ガイドライン別紙2_共通機能_設定手順書(AWS)」
- 「農林水産省クラウド利用ガイドライン別紙3_共通機能_設定手順書(Azure)」
- 「農林水産省クラウド利用ガイドライン別紙4_ MAFFクラウド命名規約設計」（※）

※MAFFクラウドにおけるリソースの命名規約およびタグのキー・値の規約について記載したドキュメントです。
MAFFクラウド利用時はタグの登録が必須です。システム設計/構築前に必ずご確認いただき、リソース作成後速やかにタグを設定してください。

1. MAFFクラウドの概要

1-1. MAFFクラウドとは　－基本方針－

1-2. MAFFクラウドの構成

1-3. MAFFクラウドを利用するメリット

1-4. MAFFクラウドの構成要素

1-5. MAFFクラウド利用時の留意事項

1-6. 既にAWS/Azureを利用中のシステムについて

1-1. MAFFクラウドとは　ー基本方針－

MAFFクラウド整備の背景と基本的な考え方

■ 農林水産省の個別システム（PJMO）の抱える課題

- 農林水産省には、比較的小規模な情報システムが多数存在します。このため、PJMOが他業務と情報システム関連業務とを兼務して、システムの整備、運用を行っている場合が多くみられます。情報システム整備・運用業務の中でも技術的な知見を要するクラウド化の検討は、PJMO担当者にとって負荷が高い作業となっています。
- 既存の受託事業者が提供するクラウドサービスを利用している場合であっても、クラウド化を進めた情報システムにおいて、運用メニューやセキュリティレベルが統一されておらず、 クラウド化のメリットを十分に享受できていない状況がみられます。

■ 農林水産省PMOの対応方針

- 農林水産省の情報システムが利用する共通のクラウドサービス利用環境を整えます。その際、共通機能を最小限とし、追加で必要となる機能はPJMOシステム毎に構築を行うことで、PJMOに過剰な制約や省内での重複投資を防ぎます。
- クラウドへの移行を専門的に支援する機能チーム（MAFFクラウドCoE）を立ち上げ、各システムが個別の課題に対応しつつ、クラウド移行できるように支援します。
- **検討を支援する活動と共通機能の提供、これらの総称を「MAFFクラウド」と呼び、取組を行っています。**

MAFFクラウドの基本方針

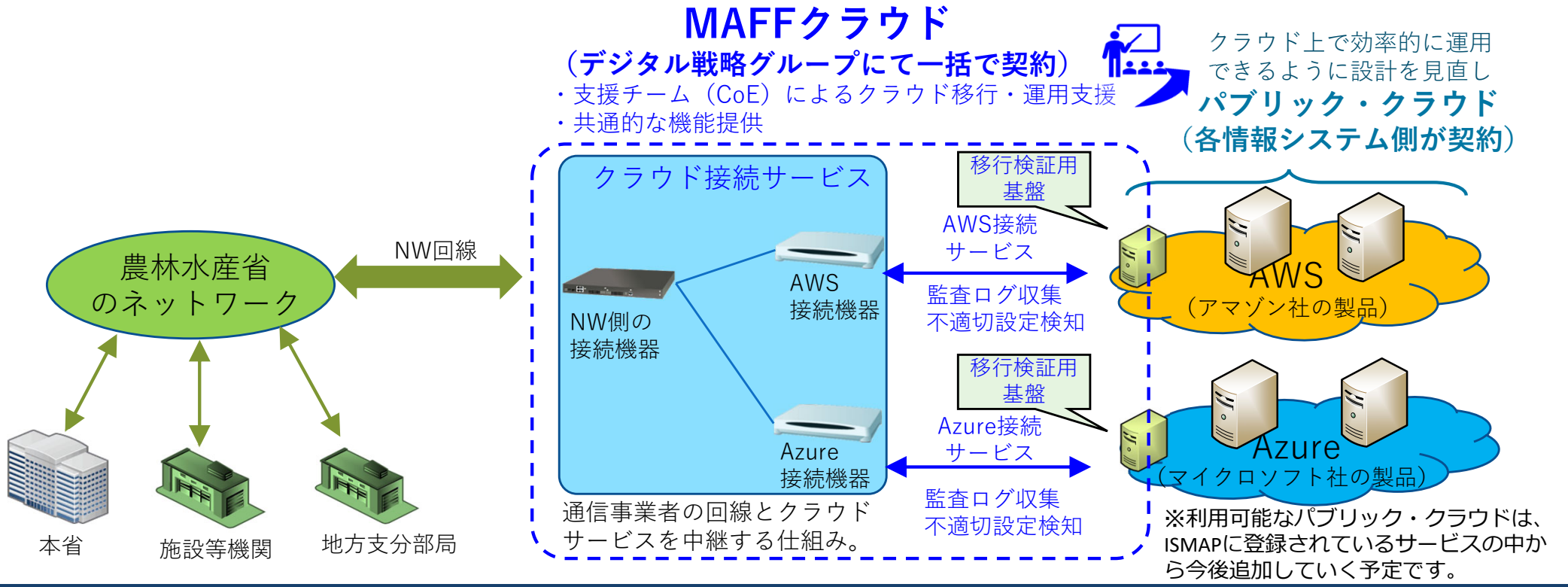
・ 共通機能は最小限とし、MAFFクラウドCoE支援の下、PJMOが柔軟且つ迅速にクラウドサービスを利用可能となることを目的とします。
・ ベンダーロックインが防がれることで、システムベンダー及びクラウドサービス利用の自由度が高まり、ベンダーの得意技術や先端技術の恩恵を享受できるようにします。

1-2. MAFFクラウドの取組及び全体の構成

■　政府機関が整備・運用する情報システムについては、オンプレミス（個別の動作環境（データセンター、ハードウェア、サーバ等）を自ら整備・運用すること）に比べて、運用負荷の低減等が期待されるクラウドサービス（ソフトウェア、データベース等を提供する技術基盤を、サーバ等ではなくインターネット等のネットワークにより行うもの）の採用が適当との考え方により、平成30年１月に閣議決定された「デジタル・ガバメント実行計画」において、クラウド・バイ・デフォルトの原則（政府情報システムは、クラウドサービスの利用を第一候補として検討すること）が明記されました。

■　これに基づき、農林水産省においては、オンプレミスで運用してきた情報システムを、パブリック・クラウド（任意の組織において利用可能なクラウドサービス）に移行させることとし、令和２年度にＭＡＦＦクラウドの取組を開始しました。その一環として、共通的な機能を整備し、運用を始めています。（農林水産省の情報システム数は約70）。

MAFFクラウド構成イメージ



1-3. MAFFクラウドを利用するメリット

■ MAFFクラウドは農林水産省の情報システムのうちクラウドサービスを利用するものに対して、クラウドサービス利用のために必要となる共通の基盤及びサービスを提供するものです。

■ MAFFクラウドを利用することで、個別システム側では、ISMAP(※)に準拠したクラウドサービスの利用、MAFFクラウドCoE（農林水産省PMOが提携するコンサル機能）による技術支援、MAFFクラウド共通機能の適用による当省として定めるセキュリティ基準への準拠が可能となります。

MAFFクラウドを利用するメリット

1	信頼できるクラウドの利用	• MAFFクラウドで利用可能なAWS/AzureはISMAPに準拠しており、安心・安全にクラウドを利用できます。 • PJMOが各クラウドサービスのセキュリティ基準について個別にチェックし選定する必要がなく、工数の削減が可能です。
2	MAFFクラウドCoEによる技術支援	• クラウド化の検討から運用に至るまでMAFFクラウドCoEが支援を行い、PJMOの負荷を軽減します。 • クラウドに関する知見を集約しているMAFFクラウドCoEより、政府のクラウド施策やクラウドサービスの最新動向を踏まえた情報を取得することができます。
3	共通機能の利用によるセキュリティ基準への準拠	• セキュリティに係る共通機能を利用することで、当省として定めるセキュリティ基準への準拠が可能です。また、要件に応じた追加でのセキュリティ対策機能の整備も可能です。 • MAFFクラウドで提供されている共通機能を使用することで、該当機能の整備期間の短縮と整備・運用費用の削減が可能です。

※ ISMAP：「政府情報システムのためのセキュリティ評価制度」 令和２年６月30日（令和３年７月最終改定）（サイバーセキュリティ対策推進会議・各府省情報化総括責任者（CIO）連絡会議）

1-4. MAFFクラウドの構成要素

- MAFFクラウドは、「MAFFクラウド共通機能」「MAFFクラウドCoE」「PoC環境」をPJMOに提供します。
- 各構成要素の概要は以下のとおりです。

MAFFクラウドの構成要素

構成要素	概要
1 MAFFクラウド共通機能	• MAFFクラウドはAWS/Azureを対象に以下の機能を共通機能として提供します。 ➢ 農林水産省統合ネットワーク（以降、統合NW）閉域網接続機能 ➢ 監査ログ収集機能 ➢ マネージド型脅威検出策機能 ➢ 不適切設定検知機能
2 MAFFクラウドCoE	• MAFFクラウドのコンセプトを理解し、クラウド移行・運用の知見を集約したPJMOへの総合的な技術支援を行うMAFFクラウドCoEを当省内に設置します。 • MAFFクラウドCoEはクラウド移行を検討しているPJMOに、検討、企画・予算要求、調達、設計・構築、運用保守の各段階において技術支援を行います。
3 PoC環境	• クラウド化に向けた網羅的な評価を机上で実施する「机上評価チェックシート」をPJMOに提供し、リスクや課題等洗い出しをご支援します。 • 必要に応じて、実機検証が可能なクラウド環境をPJMOに提供します。なお、検証によって発生するクラウドサービス利用料はMAFFクラウドCoEにて負担します。

1-5. MAFFクラウド利用時の留意事項

■　MAFFクラウドを利用する情報システム担当課室（以下「MAFFクラウドPJMO」という。）においては、CSP（クラウドサービスプロバイダー）（※）に関連する以下の点に留意してください。

クラウドサービスプロバイダーに関する留意事項

CSPとの契約	• クラウドサービスプロバイダー（CSP）との契約は、PJMOシステム側で実施してください。 • MAFFクラウドCoE/PMOでは包括的な契約は行っておりません。
クラウドサービスの利用	• MAFFクラウドではPJMOシステムが自由にクラウドサービスを利用可能です。自システムで必要となるクラウドサービスを選択し、設計、構築、運用を実施してください。 • MAFFクラウド共通機能の利用に当たっては、MAFFクラウドが指定するクラウドサービスを利用いただく必要があります。→P３参照
クラウドサービス利用料	• PJMOシステムのアカウントに関するクラウドサービス利用料は、MAFFクラウドが指定したクラウドサービス分も含めてPJMOシステムにて負担いただきます。
CSPへの技術問合せ	• AWS、Azureの技術仕様に関する問い合わせは、各PJMOシステムの構築事業者経由でAWS、Azureのサポートに直接お問い合わせください。 • 問い合わせ内容作成に関する支援はMAFFクラウドCoEでも可能です。
AWS関連（※※）	• MAFFクラウドではAWS Organizationsを利用していませんので、事業者は請求等におけるAWS Organizationsの利用が可能です。
Azure関連（※※）	• MAFFクラウド共通機能の利用にあたって、各PJMOシステムサブスクリプションの紐づけ先AzureADテナントは、MAFFクラウドが用意するカスタムドメイン「azcloud.maff.go.jp」を利用していただくことが必須です。 • サブスクリプションを契約する際の形態は、原則としてCSP契約としてください。 • 留意事項が多数あるため、Azureを利用する際は事業者が決定次第打ち合わせを設定してください。

※　CSP(クラウドサービスプロバイダー)：クラウドベースのプラットフォーム、インフラストラクチャ、アプリケーション、またはストレージ サービスを提供するIT企業（Amazon、Google等）のこと。

※※　利用可能なパブリック・クラウドは現時点ではこの２つですが、ISMAPに登録されているサービスの中から今後追加していく予定です。

1-6.既にAWS/Azureを利用中のシステムについて

■ 既にAWS/Azureを利用中のシステムは、以下に記載する考慮事項、本ガイドラインの目的及び利用方法（2,3ページ）の内容を踏まえてMAFFクラウドの利用が可能か検討してください。

■ 検討に当たってはMAFFクラウドCoEにご相談ください。

既にAWS/Azureを利用中のシステムにおける考慮事項

利用共通機能の利用に当たっての考慮すべき事項	統合NW閉域網接続機能	• IaaS等に割り当てているIPアドレスの変更が発生する可能性があります。（MAFFクラウドにて取得している統合ネットワーク接続用IPアドレスへの変更）
	脅威検出機能	• Amazon GuardDuty/Microsoft Defender for Cloud等を利用していない場合には新規に利用が必要であり、利用済みの場合でも設定変更が必要となります。
	監査ログ収集機能	• AWS S3/Azure Blob Storageへログを出力していない場合には、出力先の変更が必要となります。
	不適切設定検知機能	• AWS Config/Azure Policy等を利用していない場合には新規に利用が必要であり、利用済みの場合でも設定変更が必要となります。
利用クラウド別に考慮すべき事項	AWS	• 特にありません。
	Azure	• サブスクリプションの紐づけ先をMAFFクラウド管理のAzure ADに変更する必要があります。 • 利用しているクラウドリソース、契約形態によって紐づけ先Azure AD変更時の移行難易度が変動するため、MAFFクラウドCoEと協議を実施しMAFFクラウドの利用是非を検討してください。

2. MAFFクラウド共通機能の仕様

2-1. MAFFクラウド共通機能の概要

2-2. MAFFクラウド共通機能の全体構成

2-3. MAFFクラウド利用時のネットワーク

2-4. MAFFクラウド利用時のネットワーク構成例

2-5. MAFFクラウド共通機能　ー統合NW閉域網接続ー

2-6. MAFFクラウド共通機能　ーマネージド型脅威検出ー

2-7. MAFFクラウド共通機能　ー監査ログ収集ー

2-8. MAFFクラウド共通機能　ー不適切設定検知機能ー

2-1. MAFFクラウド共通機能の概要

■ MAFFクラウドは、統合NWとの閉域網接続機能及びセキュリティ関連分野における３つの機能、計４つの機能を提供します。
- 閉域網接続機能は、省内から統合NWを経由しMAFFクラウドを利用するシステム（以下「PJMOシステム」という。）に接続する場合には利用してください。
- セキュリティ関連機能は、AWS/Azure上にシステムを構築する場合にはその利用が必須とされています。

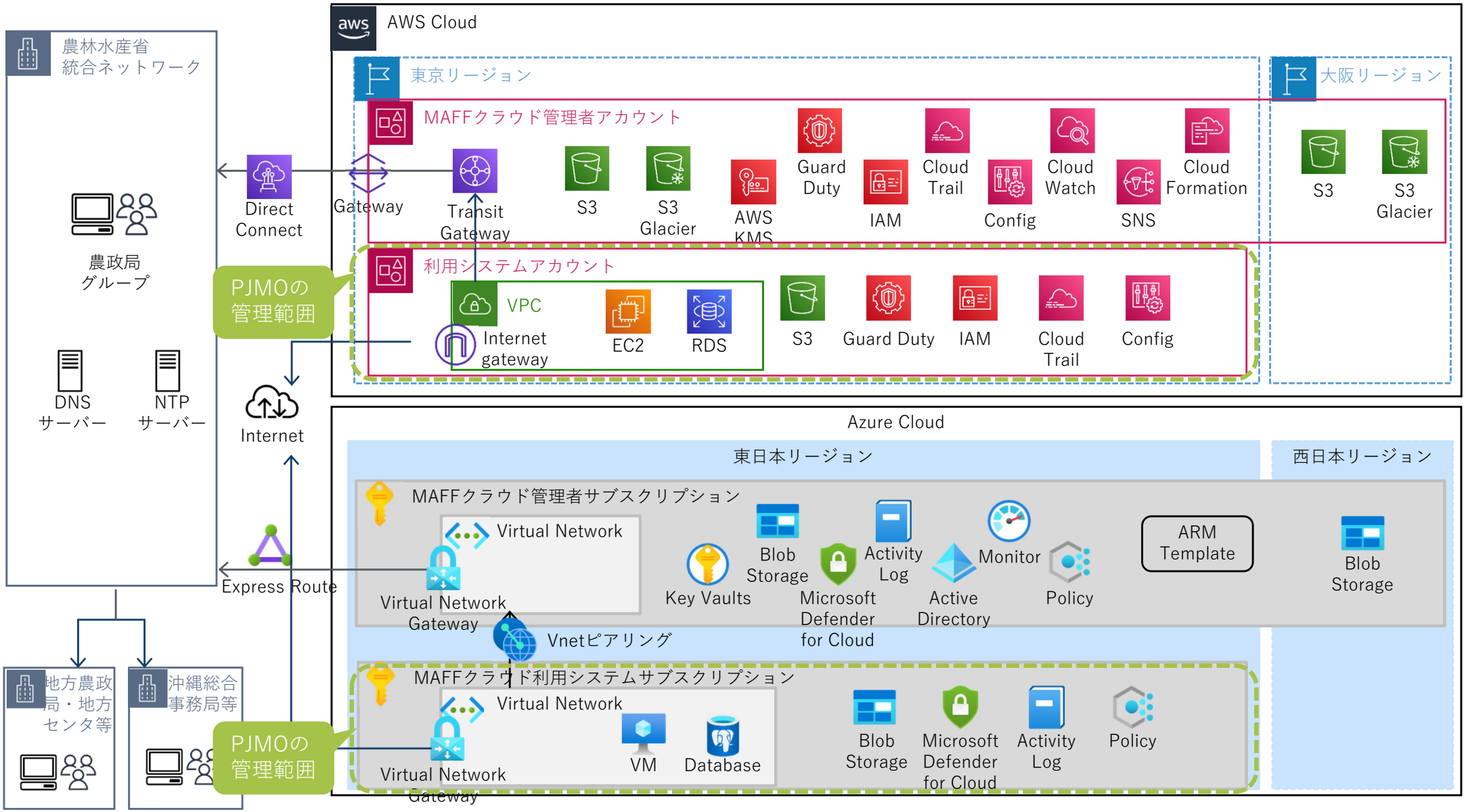
MAFFクラウド共通機能一覧

統合NW 閉域網接続機能	• 統合NWとクラウドサービスプロバイダを閉域網接続し、PJMOシステムにクラウドとの接続機能を提供します。 • PJMOシステムは統合NWとの接続要否に応じて、本機能の利用を検討してください。 （統合NWと接続が必要となる場合には、原則として本機能を利用してください。）
セキュリティ 関連機能	• 以下3機能は当省として定めるセキュリティ基準への準拠を目的とした機能であるため、原則として利用が必須です。 • なお、PJMOシステムは自身のセキュリティに関する要件に応じてセキュリティ機能の追加を検討してください。
マネージド型 脅威検出機能 （※）	• 各クラウドサービスプロバイダ上の脅威を検出し、検出時にPJMOシステムの管理者及びMAFFクラウド管理者へ通知を行います。
監査ログ 収集機能	• システム監査等の必要時にMAFFクラウドCoEがログの取り出し及び確認を行えるよう、PJMOシステム監査ログの収集・アーカイブを行います。 • 本機能で収集したログはあくまでMAFFクラウドCoEが確認する用途であるため、各システムにて適宜ログの管理を行います。
不適切設定 検知機能（※）	• 順守すべきポリシーと異なるPJMOシステムの設定及び設定の変更を検知し、PJMOとMAFFクラウド管理者へ通知を行います。

※ マネージド型脅威検出機能・不適切設定検知機能にて検知されるテストを行う場合は、MAFFクラウドCoEへ事前に通知をお願いいたします。

2-2. MAFFクラウド共通機能の全体構成

■　MAFFクラウド共通機能の全体構成を以下に示します。PJMO管理範囲内のクラウドサービスは例です。



2-3. MAFFクラウド利用時のネットワーク

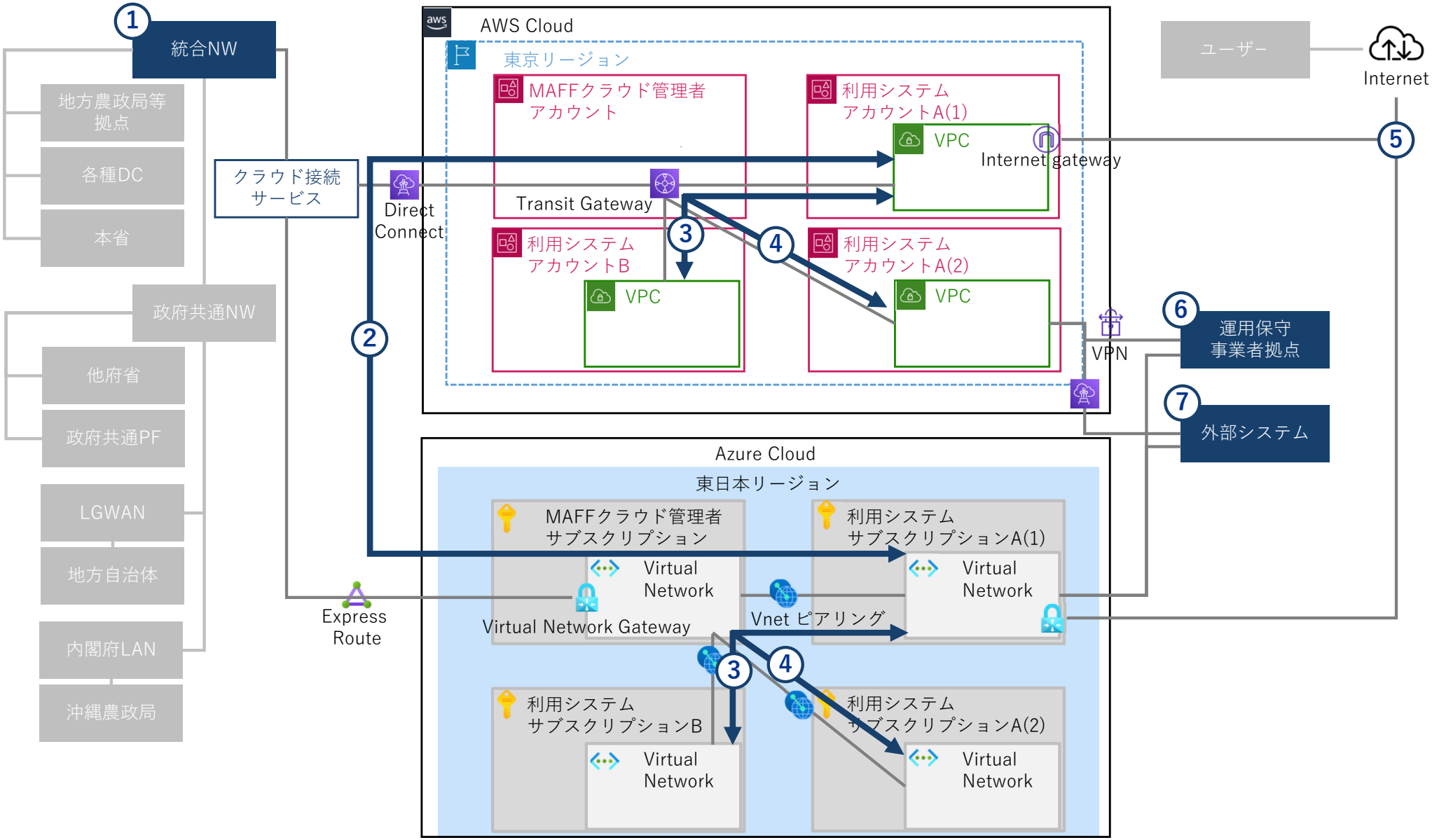
- 接続先によりMAFFクラウドが接続機能を提供する場合と、利用システム個別に用意いただく場合が存在します。
- 以下に接続先ごとの利用システムによる設計/構築要否、接続方式等を示します。
- 下記の他に通信要件がある場合には個別にお問い合わせください。

MAFFクラウド利用時に想定される通信一覧

	接続先	利用システムが個別に設計/構築	接続方式等
1	統合ネットワーク	―	• MAFFクラウドが提供する「統合NW閉域網接続機能」を利用し接続してください。 • 利用にあたってはPMOへ利用申請書の提出をお願いいたします。
2	クラウドを跨いだ他システム	○ （場合によるため、右記を要参照）	• MAFFクラウドが提供する「統合NW閉域網接続機能」を利用する場合は、利用システムで作業を行うことなく接続可能です。 • 「統合NW閉域網接続機能」を利用しない場合は、利用システムにて個別に通信経路の設計、構築、運用保守を行ってください。
3	同一クラウド内の他システム	―	• MAFFクラウド管理者アカウント/サブスクリプション経由で接続してください。 • 本通信の要件がある場合にはPMOへ連絡を行ってください。（MAFFクラウド側での作業が必要なためです。） • 他システムと接続する際には、接続先システムのPJMOから接続の承認を受けてください。
4	アカウントを跨いだ自システム	―	
5	インターネット	○	• 利用システムにて個別に通信経路の設計、構築、運用保守を行ってください。 • インターネットとの接続にあたっては、接続先を必要最小限に限定する、WAFを導入する等のセキュリティ対策を実施してください。
6	運用保守事業者拠点	○	• 利用システムにて個別に通信経路の設計、構築、運用保守を行ってください。 • 拠点から接続する際は、VPNによる通信暗号化、踏み台サーバやAWS Systems Manager等を利用した間接的な接続等のセキュリティ対策を実施してください。
7	外部システム	○	• 外部システムとは、セキュリティ要件上専用線での接続が必須である政府システムや、民間事業者のシステムを想定しています。 • 利用システムにて個別に通信経路の設計、構築、運用保守を行ってください。

2-4. MAFFクラウド利用時のネットワーク構成例

■　MAFFクラウド利用時のネットワーク構成例を以下に示します。



2-5. MAFFクラウド共通機能　　ー統合NW閉域網接続ー（1/2）

仕様

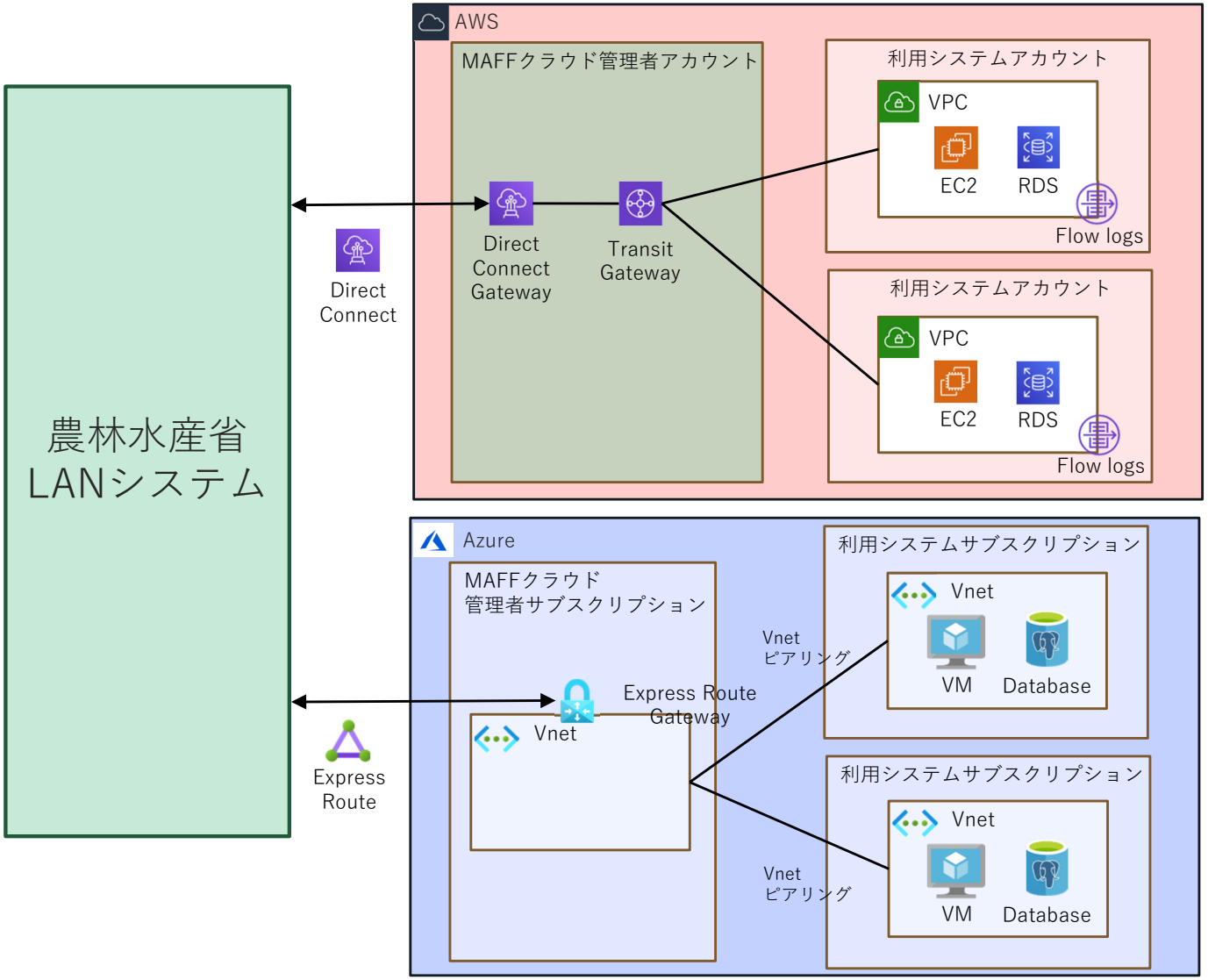
各クラウド共通	• 各クラウドと統合NWとの接続はNTT Com社が提供するFlexible InterConnectサービス（以降FIC）を利用し、帯域幅1Gbpsの回線が2本(act/stb)で構成されています。 • 各クラウド及びFICは東日本の拠点を利用しており、西日本拠点とのDR構成は現状不可能です。
AWS	• MAFFクラウド管理者アカウント内のTransitGatewayを、ResourceAccessManagerを活用することで各PJMOシステムカウントへ共有を行います。 • 共有を行ったTransitGatewayとそれに紐づくルートテーブルを活用し、各PJMOシステムとの接続をMAFFクラウド管理者アカウントで一元管理を行います。
Azure	• MAFFクラウド管理者サブスクリプションとPJMOシステムサブスクリプション間の接続についてはVNetピアリングによってハブアンドスポーク構成をとっており、各PJMOシステムサブスクリプション間での通信を制御します。 • VNetピアリングの接続によって、各PJMOシステムとの接続をMAFFクラウド管理者サブスクリプションで一元管理を行います。PJMOシステムサブスクリプション側での制御は、各PJMOシステムのNSGによって行ってください。

MAFFクラウド及びPJMOシステムの役割分担

MAFFクラウド	• FICを利用した統合NWと各クラウドとの閉域網接続回線、クラウドサービス及び利用料を負担します。 • 統合NW内で利用可能なIPアドレス（原則/24~/20の範囲で提供）の払い出しを行います。 • 各PJMOシステム向けの設定手順を作成します。
PJMOシステム	• MAFFクラウドが提供するIPアドレスを用いたVPC、vNetの構築及び利用料を負担してください。 • TransitGateway、MAFFクラウド管理者vNetへの接続設定及び疎通確認作業を行ってください。 • 開発、運用管理用等の事業者接続環境を構築してください。

2-5. MAFFクラウド共通機能　　ー統合NW閉域網接続ー（2/2）

提供イメージ



2-6. MAFFクラウド共通機能　　ーマネージド型脅威検出ー（1/2）

仕様

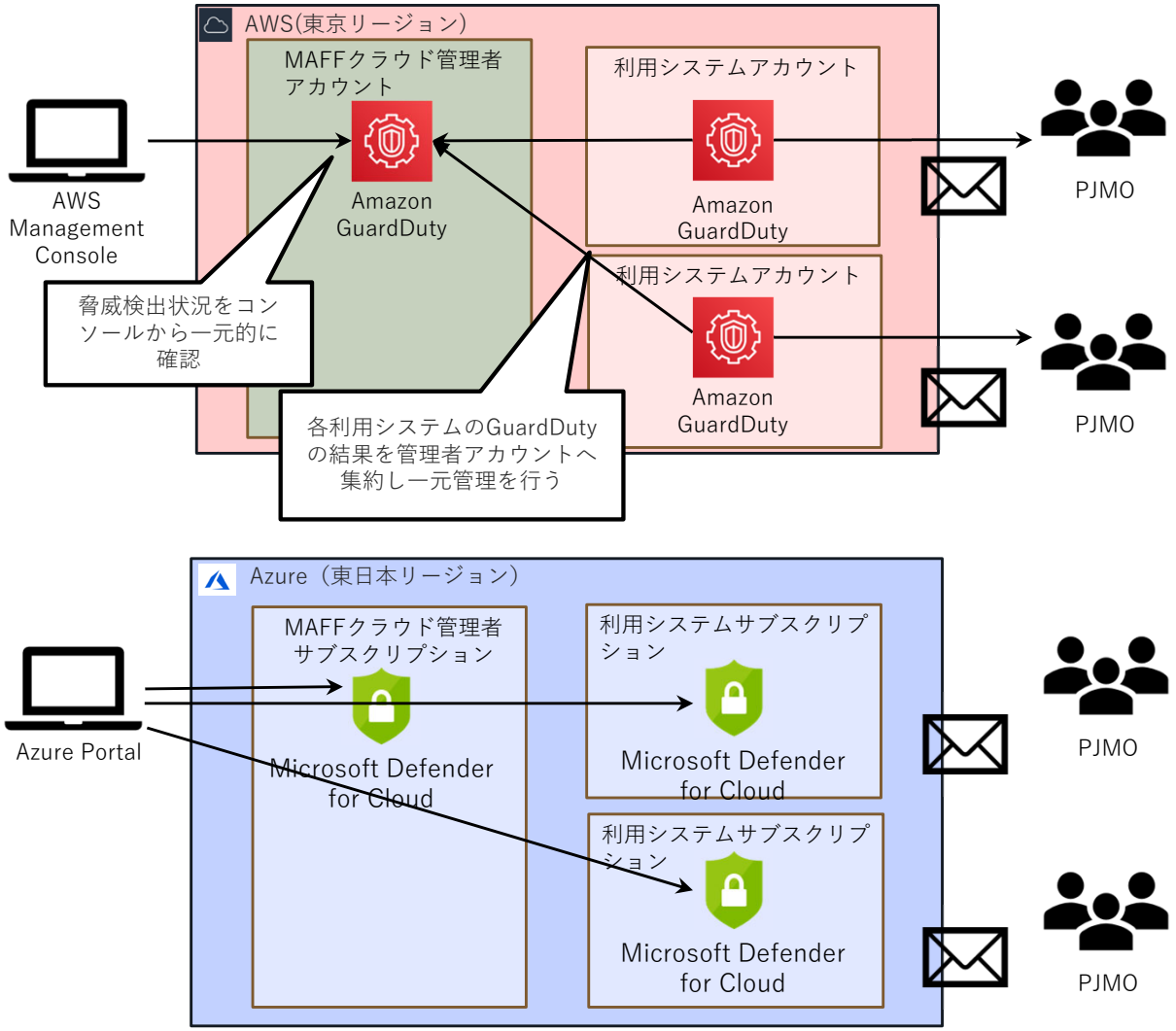
AWS	• マネージド脅威検出機能を実現するための方法として「GuardDuty」、「EventBridge」、「Simple Notification Service」を活用します。 • MAFFクラウド管理者アカウントは検出対象を原則全16リージョンでの適用としますが、PJMOシステムアカウントには東京リージョンのみの適用もしくは全16リージョンでの適用のいずれかを選択いただきます。
Azure	• マネージド脅威検出機能を実現するための方法として「Microsoft Defender for Cloud」、「Log Analytics ワークスペース」、「Azure Logic Apps」を活用します。 • Microsoft Defender for Cloudはサブスクリプション全体に適用されるため、MAFFクラウド管理者及びPJMOシステムともに全リージョンのリソースを検出対象としてセキュリティ評価を実施します。 • Microsoft Defender for Cloudを利用することで、仮想マシン、SQLデータベース、コンテナ、Webアプリケーション、ネットワークなどに対して、セキュリティアラートと高度な脅威保護の提供が可能となりますが、利用要否は各PJMOシステムにて判断してください。

MAFFクラウド及びPJMOシステムの役割分担

MAFFクラウド	• 管理者用アカウントにおいて、統合的な脅威検出を行うための以下クラウドサービス及び利用料を負担します。 ➢ AWS：「GuardDuty」、「EventBridge」、「Simple Notification Service」 ➢ Azure：「Microsoft Defender for Cloud」、「Log Analytics ワークスペース」、「Azure Logic Apps」 • 各PJMOシステム向けの設定手順を作成します。
PJMOシステム	• PJMOシステムアカウントにおいて、脅威検出とMAFFクラウド管理者への検出結果の連携を行うための以下クラウドサービス及び利用料を負担してください。 ➢ AWS：「GuardDuty」、「EventBridge」、「Simple Notification Service」 ➢ Azure：「Microsoft Defender for Cloud」、「Log Analytics ワークスペース」、「Azure Logic Apps」 • MAFFクラウド管理者より提供された手順に基づく設定作業を実施してください。

2-6. MAFFクラウド共通機能　　ーマネージド型脅威検出ー（2/2）

提供イメージ



2-7. MAFFクラウド共通機能　　ー監査ログ収集ー（1/2）

仕様

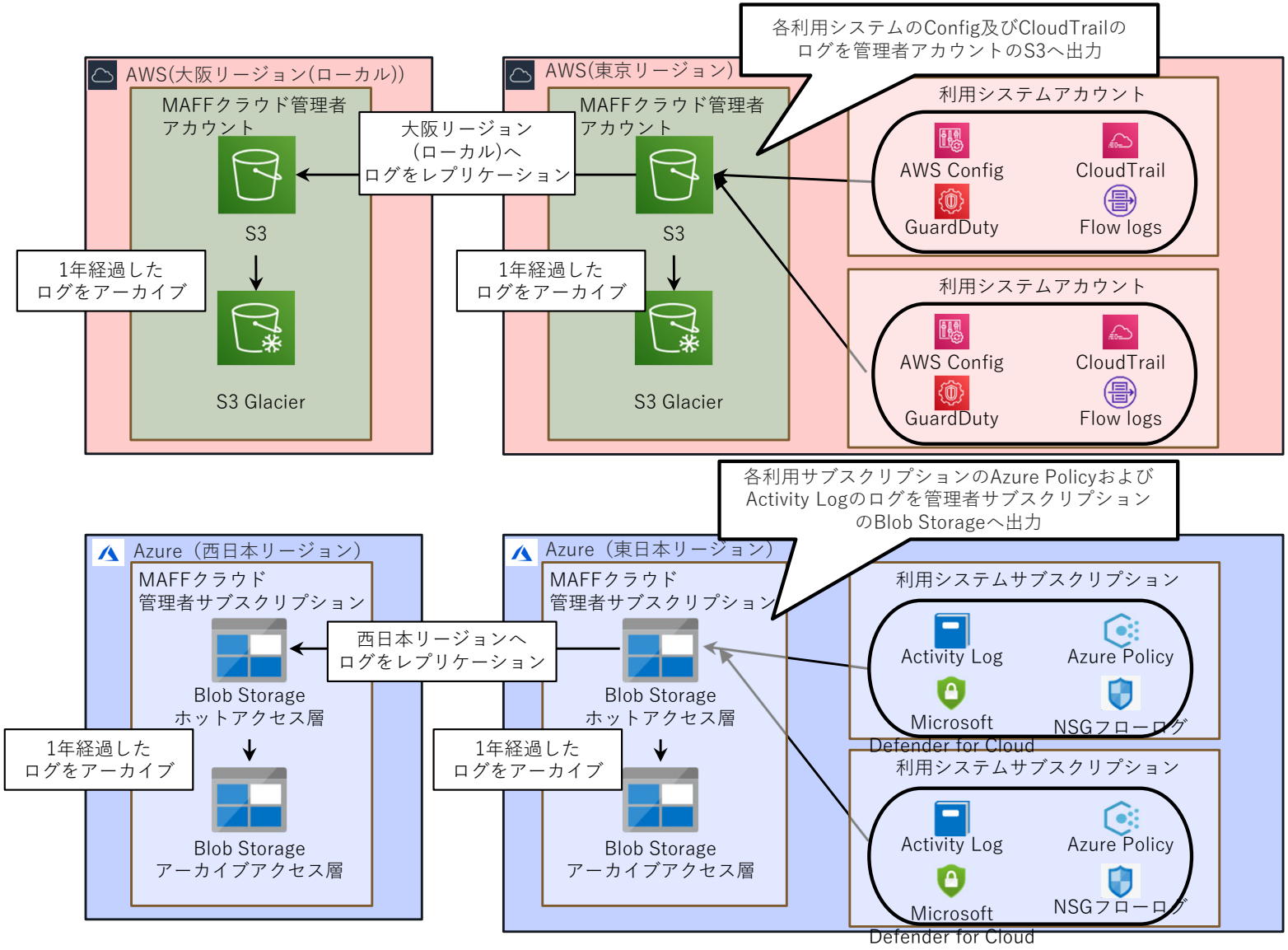
AWS	• PJMOシステムアカウントが各リージョンで出力するログをMAFFクラウド管理者アカウントのS3バケットへ集約します。 • 「AWS Config」「Amazon Guard Duty」「AWS Cloudtrail」「Amazon VPC Flow Logs」を収集対象ログとしています。 • 収集対象リージョンは、原則デフォルトで有効となっている16リージョンですが、「Amazon VPC Flow Logs」のみ“アジアパシフィック (東京)”が対象です。
Azure	• 各PJMOシステムサブスクリプションの各リージョンで出力されるログをMAFFクラウド管理者サブスクリプションのAzure Storageへ集約を行います。 • 「Azure Policy」「Microsoft Defender for Cloud」「Activity Log」「NSGフローログ」を収集対象ログとしています。 • 収集対象リージョンは、原則全リージョンですが、「NSGフローログ」のみ“東日本リージョン”が対象です。

MAFFクラウド及びPJMOシステムの役割分担

MAFFクラウド	• MAFFクラウド管理者及びMAFFクラウドCoEがPJMOシステムの監査ログを集約、確認を行うためのクラウドサービス（S3、Azure Storage）及び利用料を負担します。 • 各PJMOシステム向けの設定手順を作成します。
PJMOシステム	• 自身のログを保管・管理するためのクラウドサービス（S3、Azure Storage）及び利用料を負担してください。 ※　MAFFクラウドにて集約する監査ログは、S3またはAzure Storageへの保管・管理が前提となります。 • MAFFクラウド管理者より提供された手順に基づく設定作業を実施してください。

2-7. MAFFクラウド共通機能　　ー監査ログ収集ー（2/2）

提供イメージ



2-8. MAFFクラウド共通機能　　ー不適切設定検知ー（1/2）

仕様

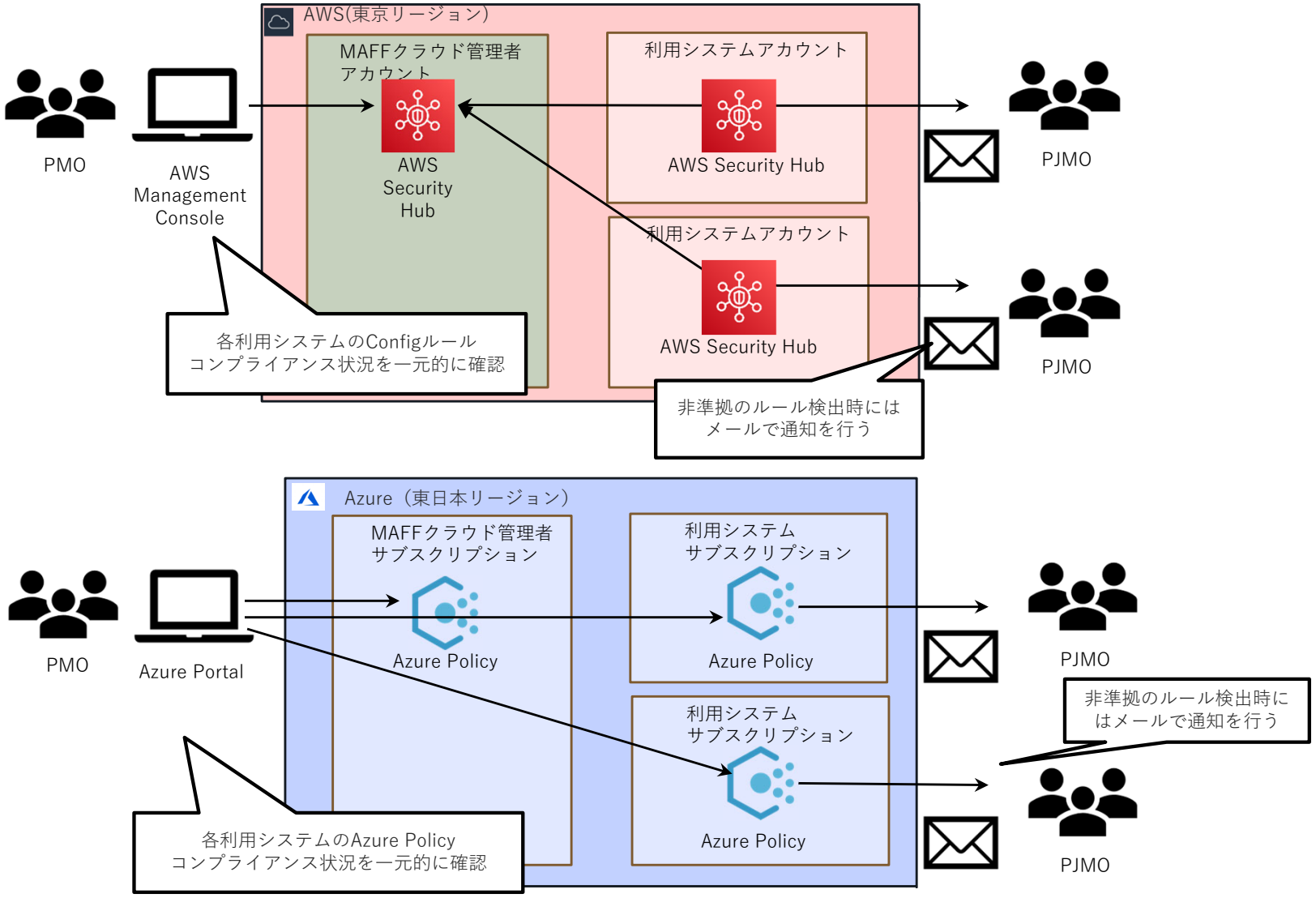
AWS	• 不適切設定検知機能を実現するための方法として「Config」、「Security Hub」、「EventBridge」、「Simple Notification Service」を活用します。 • 「CIS AWS Foundations Benchmark v1.2.0」及び「AWS 基礎セキュリティのベストプラクティス v1.0.0」のベストプラクティス基準に準拠した項目を対象に検知を行います。 • デフォルトで有効となっている16リージョンを対象リージョンとしています。
Azure	• 不適切設定検知機能を実現するための方法として「Azure Policy」、「Azure monitorアラート」を活用します。 • 「CIS Microsoft Azure Foundations Benchmark 1.1.0」及び「Azure セキュリティ ベンチマーク」の推奨事項に準拠した項目を対象に検知を行います。 • 全リージョンを対象リージョンとしています。

MAFFクラウド及びPJMOシステムの役割分担

MAFFクラウド	• 不適切な設定の検知を統合的に行うための以下クラウドサービス及び利用料を負担します。 ➢ AWS：「Config」、「Security Hub」、「EventBridge」、「Simple Notification Service」 ➢ Azure：「Azure Policy」、「Azure monitorアラート」 • 各PJMOシステム向けの設定手順を作成します。
PJMOシステム	• PJMOシステムアカウントでの不適切設定検知及びMAFFクラウド管理者への検知結果の連携を行うための、以下クラウドサービス及び利用料を負担してください。 ➢ AWS：「Config」、「Security Hub」、「EventBridge」、「Simple Notification Service」 ➢ Azure：「Azure Policy」、「Azure monitorアラート」 • MAFFクラウド管理者より提供された手順に基づく設定作業を実施してください。

2-8. MAFFクラウド共通機能　　ー不適切設定検知ー（2/2）

提供イメージ



3. PoCの概要

3-1. PoCの目的

3-2. PoCの実施方針

3-3. 机上評価と実機検証の実施方法

3-4. PoCの進め方

3-5. PoCの検証対象スコープ

3-1. PoCの目的

■ PoC（Proof of Concept）とは、新しいプロジェクトが本当に実現可能かどうか、効果や効用、技術的な観点から検証する行程をいいます。MAFFクラウドにおいては、クラウド移行に関する課題の事前検証・評価であり、業務アプリケーション見直しに関する評価、クラウドに適したアーキテクチャの評価、システム運用に対する評価の3つの観点で評価することで、PoEが、クラウド移行に係る移行経費抑制やリスク抑制等を目的として、以下の観点から、クラウド移行に関する課題の事前検証・評価を行います。

- 移行対象システムが想定どおりクラウドに移行できるか。
- クラウド標準サービスを活用して運用負荷の低減が可能か。

■ PJMOは、クラウド移行に向けた企画・予算要求時にPoCの実施を検討してください。なお、検討に当たってはMAFFクラウドCoEへ事前に相談をしてください。

PoCにおける評価の観点

1	2	3
業務アプリケーション見直しに関する評価	**クラウドに適したアーキテクチャの評価**	**システム運用に対する評価**
● 業務アプリケーションの移行観点を評価 ● リファクタリングの移行方法について評価 ※リビルドは再構築が前提であることから、本評価は行いません。	● クラウドアーキテクチャへの移行観点を評価 ● OS／ミドルウェアの対応バージョン、サードパーティー製品、移行ツール、等の検証要素を抽出し評価	● PJMOの運用観点を評価 ● クラウド化で変更となる運用項目を抽出し評価

3-2. PoCの実施方針

■ PoCはPJMO及び運用保守事業者が中心となり実施していただき、MAFFクラウドCoEが支援します。

■ 対象システム
- 原則として、AWS・Azureへ移行予定のシステムが対象です。
- PJMOとMAFFクラウドCoEで各システムのPoC実施について検討を実施します。

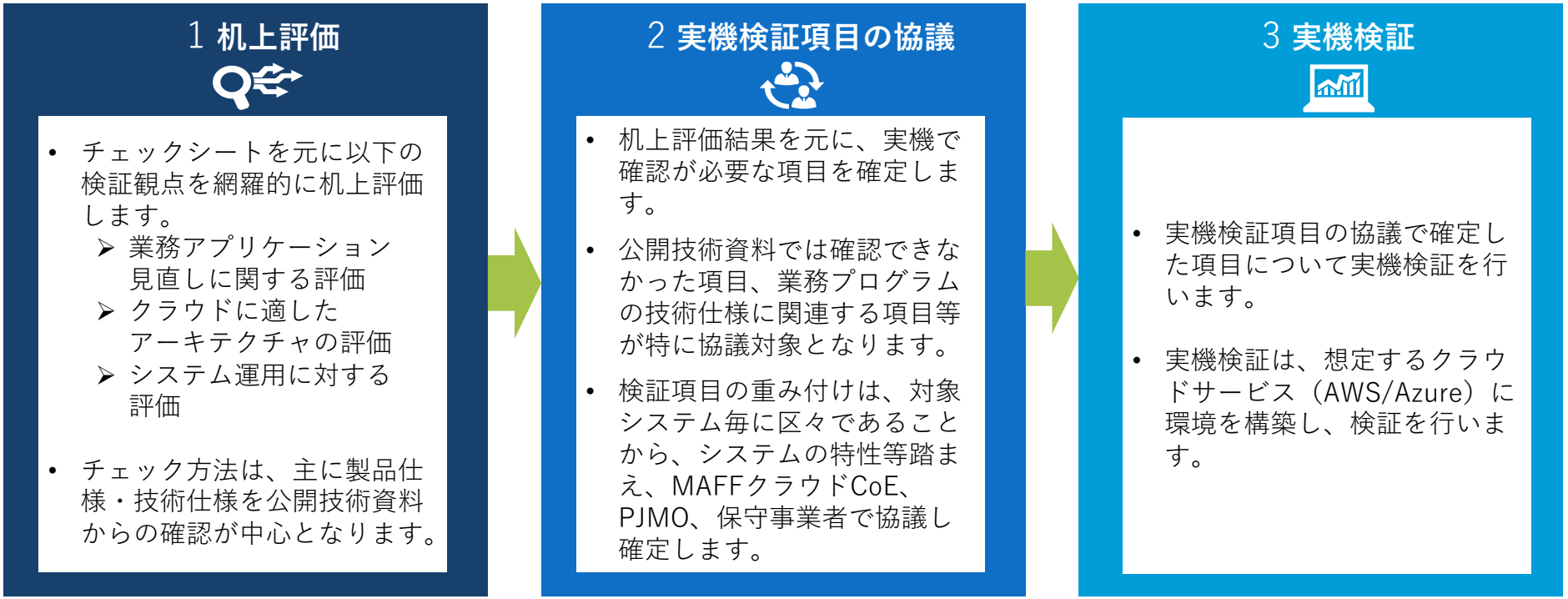
■ 実施内容
- 机上評価チェックシートを利用し、網羅的にクラウド移行に係る課題を抽出（机上評価）します。
- 実際に簡易的なAWS、Azureの環境を構築し、実機での課題検証を実施（実機検証）します。

3-3. 机上評価と実機検証の実施方法

■ 机上評価
- 机上評価チェックシートをPJMOにて記入いただき、MAFFクラウドCoEにて内容を精査します。
- 対象システムが想定する製品仕様とクラウドサービスの技術仕様、クラウド利用上の制限事項について、公開技術資料等を元に課題がないか確認を行います。

■ 実機検証方法
- 机上評価の結果から実機で検証が必要な項目をPJMOとMAFFクラウドCoEで検討し、必要と判断された場合には実環境を使った検証を行います。

■ 実機検証環境
- MAFFクラウドCoEにてAWS、Azureの検証環境を用意します。
- 検証環境のクラウドサービス利用料はMAFFクラウドCoE（PMO）にて負担します。



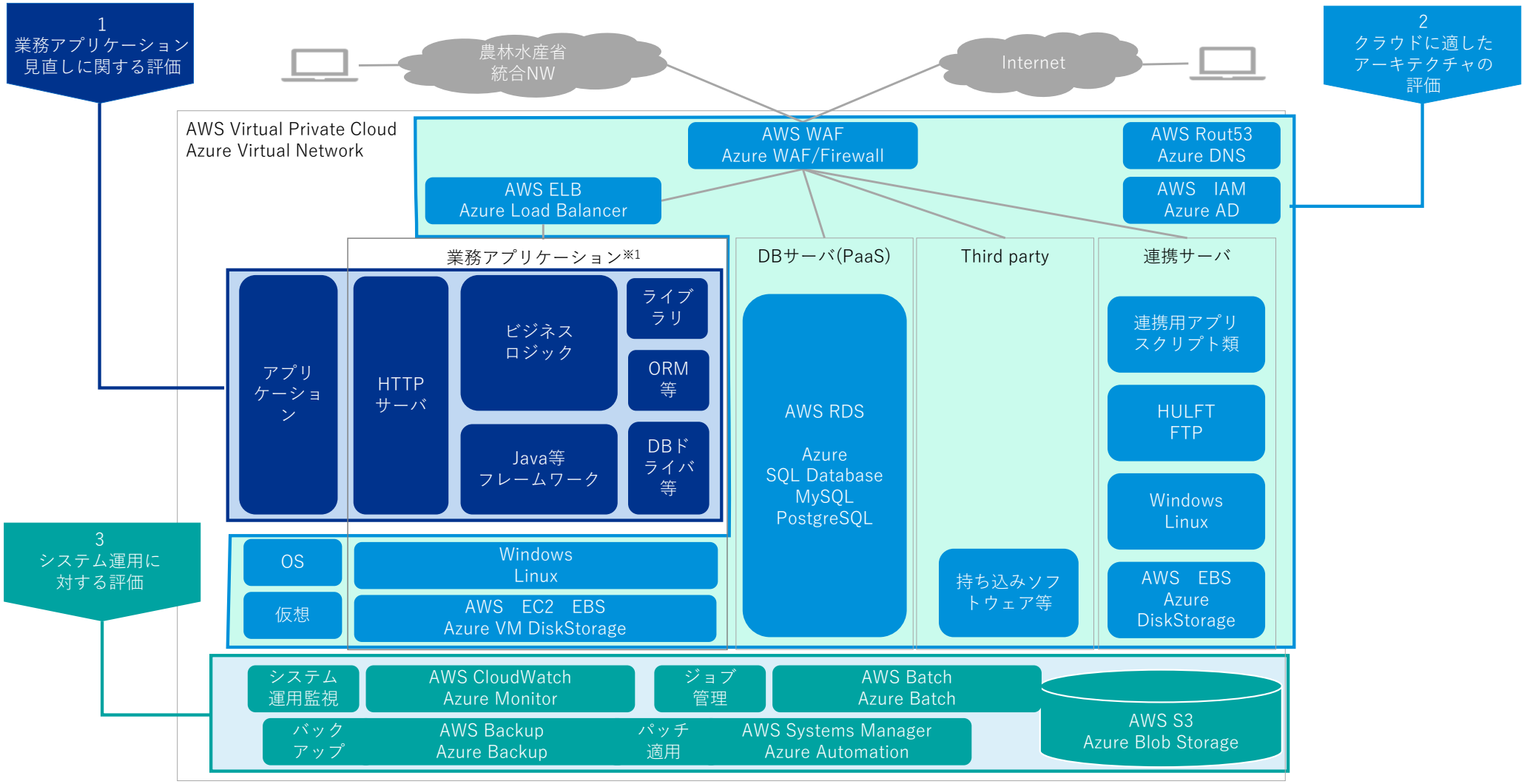
3-4. PoCの進め方

■　PoCの進め方は、以下のフローのとおりです。

PoC実施フロー	業務内容
実施計画の立案・作成	• MAFFクラウドCoE・PJMO間で協議の上、スケジュール・実施体制を整理し、PJMOにてPoC実施計画書を作成してください。
机上評価	• PJMOにて机上評価チェックシートを記載してください。 • ミドルウェア、ライブラリ、OS等のバージョン組み合わせ仕様や、業務アプリケーションの技術仕様との整合等、机上評価での確認が非効率な項目や、確認が難しい項目等を実機検証候補として特定してください。
実機検証項目の整理・確定	• 机上評価の結果を元に、実機で検証が必要な項目をPJMO・MAFFクラウドCoEにて検討します。 • 本番と同規模の環境が必要なものや、外部ネットワーク接続など本番環境でないと検証できない項目については、項目の検証重要度に応じて、確認方法を整理してください。
実機検証設計	• PJMO及び運用保守事業者にて、実機検証に必要な、業務アプリケーションの改修設計、クラウド基盤の環境設計、検証に必要なデータベース等のテストデータ設計を行ってください。
実機検証構築	• PJMO及び運用保守事業者にて、業務アプリケーションの改修、基盤の構築、検証に必要なデータベース等のテストデータの作成を行ってください。
実機検証	• 上記にて構築した検証環境下において、 PJMO及び運用保守事業者にて実機検証を実施してください。 • 実機検証では想定する結果と異なる結果になる可能性があることから、検証は繰り返し行う前提とします。
検証結果報告	• 上記の机上評価、実機検証を元にPJMOにて検証結果を報告してください。 • 検証結果を元にクラウド移行について想定と異なる点や、注意すべき点、改修箇所、対応策等についてPJMOとMAFFクラウドCoEにて取りまとめます。

3-5. PoCの対象例

- PoCの対象となるクラウドサービスやシステム構成要素例を以下に示します。
- システムの構成によりPoCの対象は異なるため、MAFFクラウドCoEに相談してください。



別表

別表 1-1. 用語集（一般用語）

■　本資料で登場する一般的な用語について、以下に示します。

	用語	説明
1	AWS	• Amazon Web Servicesの略称。 Amazon.comが提供するクラウドコンピューティングサービスであり、ISMAPに準拠している。クラウドの世界的シェアNo.1（2021年4月現在）。
2	Azure	• Microsoft Azureの略称。 マイクロソフトが提供するクラウドコンピューティングサービスであり、 ISMAPに準拠している。クラウドの世界的シェアNo.2（2021年4月現在）
3	リホスト	• 既存のシステム構成に大きな変更を加えずにクラウドへ移行する移行方式。クラウドサービスは主にIaaSを利用する。
4	リファクタリング	• 業務アプリケーションの改修は最低限に留め、マネージドDB等のPaaS、クラウド標準の運用サービスを活用しすることでクラウドに適したシステム構成を可能な限り採用する移行方式。MAFFクラウドとして推奨する移行方式。
5	リビルド	• 既存のシステム構成の抜本的な刷新、再構築を行い、全面的にクラウドに適したシステム構成を採用する移行方式。
6	CSP契約	• Azureにおける契約形態の一つ。MAFFクラウドではCSP契約を採用しており、PJMOシステムもCSP契約を採用することが求められる。その他の契約形態として、Web直販、Open契約、EA契約が存在する。
7	サブスクリプション	• Azureにおける契約の単位。AWSのアカウントに近い存在。MAFFクラウドでは原則CSP契約でサブスクリプションを作成し、サブスクリプション内にリソースの配置及びシステム構築を行う。また、クラウドリソースの利用料金はサブスクリプション毎に請求される。
8	CoE	• Center of Excellenceの略称。組織横断的な取組を行う際に中核的な役割を担う。一般的に取組に精通する人材やノウハウ、ツール等が集結した組織。

別表 1-2. 用語集（MAFFクラウド関連用語）

■　本資料で登場する一般的な用語について、以下に示します。

	用語	説明
1	MAFFクラウド	• 農林水産省クラウドの略称。MAFFクラウドCoEによるPJMOへの総合的なクラウドに関する支援活動及びクラウド移行・運用時に必要となる最小限の共通機能を提供する。
2	MAFFクラウド管理者	• MAFFクラウドの管理を担い、各種共通機能の設定を行う事業者。MAFFクラウド利用時に提出する申請書は、MAFFクラウド管理者に提出する。
3	MAFFクラウドCoE	• MAFFクラウドのコンセプトを理解し、クラウド移行・運用の知見を集約したPJMOへの総合的な技術支援を行う組織。クラウド移行を検討しているPJMOに、検討、企画・予算要求、調達、設計・構築、運用保守の各段階において技術支援を行う。
4	PMO	• Portfolio Management Officeの略称。農林水産省内のシステム全体を管理する組織。MAFFクラウドの利用有無に関わらず、各業務システムのPJMOを横断的に管理している。 MAFFクラウド共通機能のクラウドサービス利用料を負担する。
5	PJMO	• Project Management Officeの略称。省内個別業務システムを所管し、当該システムに関するプロジェクトマネジメントを実施する。当該システムに関するクラウドサービス利用料、設計・構築、運用・保守、移行経費等負担する。
6	事業者	• PJMOと結んだ契約に基づいてシステムの設計・開発・運用作業を行う会社。（SIer、ベンダー）
7	PoC	• Proof of Conceptの略称。クラウド移行に関する課題の事前検証・評価であり、業務アプリケーション見直しに関する評価、クラウドに適したアーキテクチャの評価、システム運用に対する評価の3つの観点で評価する。

農林水産省クラウド
共通機能利用申請書

2022年2月4日版

改版履歴

改訂日	対象シート	改訂内容
2022/02/04	改訂履歴	改訂履歴シートを新規作成
2022/02/04	利用申請書	「利用するMAFFクラウド共通機能」欄、「統合NW経由での接続先拠点」欄および沖縄総合事務局と接続する場合の注意点を追加

0.はじめに

0.1.本書の内容と目的

本書は、農林水産省クラウドの運用業務における共通機能の申請を行うための利用申請書を記載したものである。
PJMOから利用申請を行い、PMOより本書に必要事項を記載し返却を行う。

【利用申請書】

利用システム担当者が記載

1.申請者	申請日	XXXX年XX月XX日
	所属	
	氏名	
2.利用情報	システム名称	
	システム略称（英小文字/数字20字以内） ※AWS、Azureのタグに設定しシステムを識別します。 ※システム略称はPJMOにて検討の上、記載してください。	
	システムID	
	緊急時連絡先メーリングリスト ※PJMO、保守事業者を含めたメーリングリストの作成をお願いします。	
	必要なIP数 /24～/20の範囲で選択してください。 ※足りない場合は「3.補足・追記」へ記入をお願いします。	/24(最大IP数:251)
	利用するクラウド	AWS
	「AWS アカウントID」　もしくは 「Azure サブスクリプションID」 **Azureの場合、以下注意事項がございます。** **※原則、CSP契約で作成をお願いします。** **※MAFFクラウドのAzureADのカスタムドメイン「azcloud.maff.go.jp」に関連付けを行い作成をお願いします。**	
	AWS アカウントのルートユーザー	
	利用ポートとプロトコル (記入例：80/TCP、443/TCP、53/UDP) **※PMO側ではFWの開放申請は行いません。** **統合NW,各拠点へのFWの開放申請に関しては、PJMO側で対応をお願いします。**	
	利用するサービス (記入例(AWS)：EC2,RDS,S3)	
	利用するMAFFクラウド共通機能 ※利用する共通機能を以下から全て記載してください。 ・統合NW閉域網接続 ・監査ログ収集 ・不適切設定検知 ・脅威検出	
	統合NW経由での接続先拠点 **※沖縄総合事務局と通信を行う場合はネットワーク機器の設定が必要となりますので、農林水産省システム運営チームへ依頼をお願いします。**	
	共通セキュリティ機能を適用するリージョン MAFFクラウドで提供している以下の共通セキュリティ機能を適用するリージョンについて「東京リージョンのみ」、「全リージョン」のいずれかから選択してください。 ・不適切設定検知 ・脅威検出 **※AWSのみ**	東京リージョンのみ
	システム構成図	※「システム構成図」シートにご記入ください
3.他利用システムとの連携 ※連携しない場合は記載不要	連携先利用システム名	
	連携先システムID	
	連携先システム種別 (例：MAFFクラウド内の他システム、MAFFクラウド以外のクラウドを利用しているシステム、他府省のシステム、農林水産省NW内の他利用システム 等)	
4.補足・追記		

以下は設定完了後にPMO(MAFFクラウド管理者)が記載

・AWS

1.接続情報	管理者AWSアカウントID	021272315908
2.利用情報	払い出しIPアドレス	
3.補足・追記		

・Azure

1.接続情報	管理者Azureサブスクリプション ID	
	ExpressRoute 回線名称	
2.補足・追記		

１．システム構成図

利用システム担当者が記載

農林水産省クラウド
共通機能設定手順書(AWS)

2022年6月17日版

改版履歴

改訂日	対象シート	改訂内容
2022/02/04	改訂履歴	改訂履歴シートを新規作成
2022/06/06	目次と作業分担	シート名を「目次」から「目次と作業分担」に変更、MAFFクラウド・利用システム側アカウントの作業分担について表を追加
2022/06/17	目次と作業分担	シートを目立たせるため、色付け

0.はじめに

0.1.本書の内容と目的

本書は、農林水産省クラウドの運用業務における共通機能の設定方法を記載したものである。
PJMOから提出された利用申請書を元にPMO及びPJMO双方で設定を行う。

【要確認】

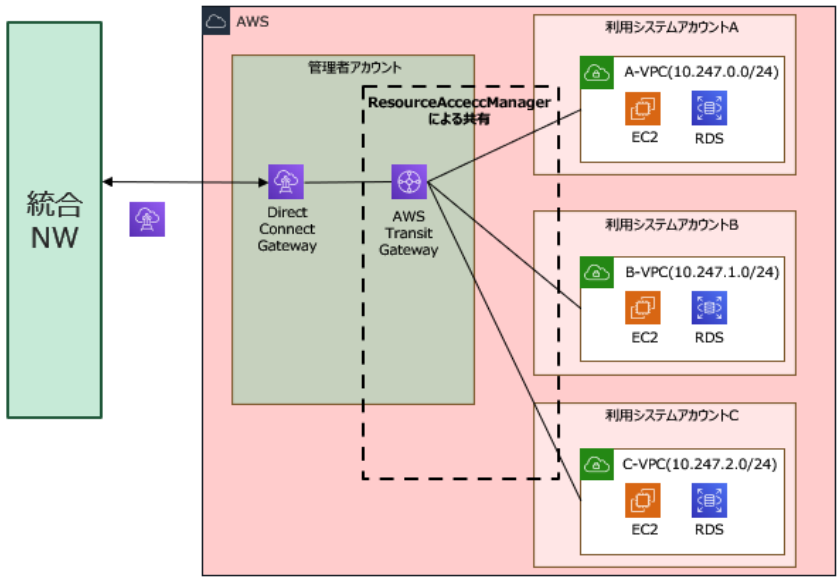
■目次

■MAFFクラウド・利用システム側アカウントの作業分担

作業内容	担当
1.統合NW閉域網接続機能	
手順①RAMの共有申請	MAFFクラウド
手順②RAMの承認	**利用システムアカウント側作業**
手順③TransitGWにVPCを接続	**利用システムアカウント側作業**
手順④VPC側のルーティング設定	**利用システムアカウント側作業**
手順⑤TransitGW側のルーティング設定	MAFFクラウド
2.マネージド型脅威検出機能	
事前作業 GuardDutyの有効化	**利用システムアカウント側作業**
手順①GuardDutyの招待	MAFFクラウド
手順②承諾	**利用システムアカウント側作業**
手順③EventBrigeの設定	**利用システムアカウント側作業**
3.監査ログ収集機能	
手順①S3バケットポリシー設定	MAFFクラウド
手順②ログ転送設定(Config)	**利用システムアカウント側作業**
手順③ログ転送設定(GuardDuty)	**利用システムアカウント側作業**
手順④ログ転送設定(CloudTrail)	**利用システムアカウント側作業**
手順⑤ログ転送設定(VPCフローログ)	**利用システムアカウント側作業**
4.不適切設定検知機能	
事前作業 Config・Security Hubの有効化	**利用システムアカウント側作業**
手順①メンバーアカウントの招待(Configアグリゲータ)	MAFFクラウド
手順②承諾	**利用システムアカウント側作業**
手順③メンバーアカウントの招待(SecurityHub)	MAFFクラウド
手順④承諾	**利用システムアカウント側作業**
手順⑤ConfigRulesの設定	**利用システムアカウント側作業**
手順⑥EventBridgeの設定	**利用システムアカウント側作業**

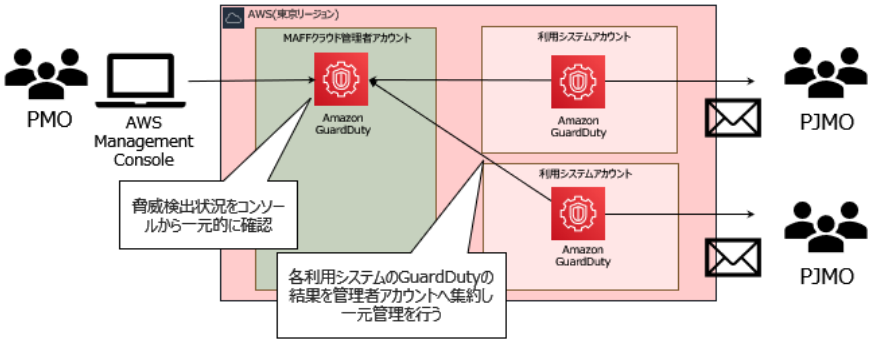
1.統合NW閉域網接続機能

1）統合NWと各利用システム間をDirectConnect Gatewayを経由して接続を行う。
2）MAFFクラウド管理者システム内のTransitGatewayをResourceAccecCManagerを活用し各利用システムカウントへ共有を行う。
3）MAFFクラウド管理者システム内のTransitGatewayで各利用システムカウントとの接続の一元管理を行う。



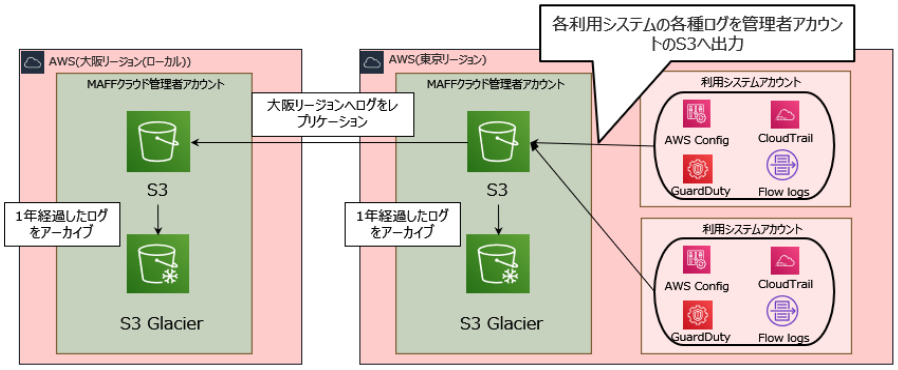
2.マネージド型脅威検出機能

1）MAFFクラウド管理者アカウントのGuardDutyで各利用システムのGuardDutyの一元管理を行う。
2）利用システム側で検知した脅威はMAFFクラウド管理者アカウントへも通知が行われる。
3）利用システムアカウント側でGuardDutyを適用するリージョンを「東京リージョンのみ」、「全リージョン」から選択することが可能。
※セキュリティの観点から「全リージョン」への適用を推奨しているがコスト増大につながるため「東京リージョンのみ」も選択可能としている。
東京リージョン以外の能動的に利用していないリージョンでの許可されていないアクティビティを検知し、リソースの盗用といったセキュリティ脅威への対策という
観点からデフォルトで有効になっているリージョンについて全てのリージョンを対象に検知を行うことがベストプラクティスとなっている。
(例：管理者アカウント情報が意図せず漏洩し、攻撃者により東京リージョン以外の普段利用していないリージョンにリソースを作成された場合等に検知を行うことができる)



3.監査ログ収集機能

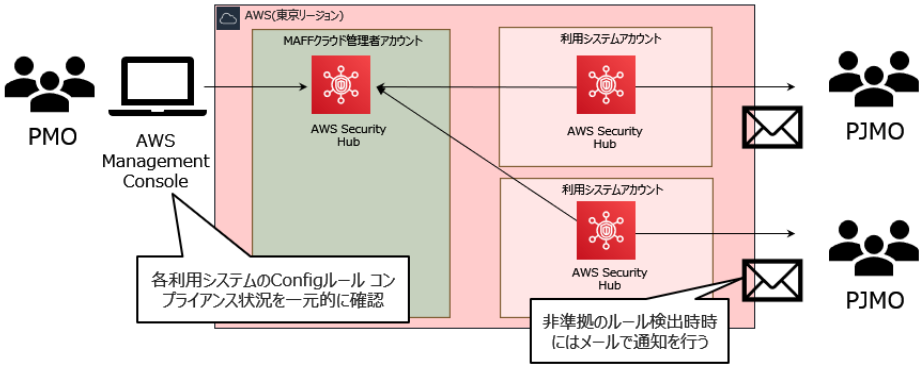
1）各利用システムアカウントの以下ログをMAFFクラウド管理者アカウント内のS3バケットに出力する。
・Configの「Configsnapshot」、「Confighistory」
・CloudTrailの証跡ログ
・VPCフローログ
・GuardDutyの検出結果
2）MAFFクラウド管理者アカウントではS3のライフサイクルポリシーにより1年経過したログはS3 Glacierにアーカイブを行いその後３年間保存を行う。
バックアップ先とて大阪リージョンのS3バケットへレプリケーションを行う。
3）MAFFクラウド管理者アカウントのS3バケットにはバケットポリシーにより以下AWSサービスとAWSアカウントでアクセス制限を行っている。
■許可するAWSサービス
Config
CloudTrail
GuardDuty
VPCフローログ
■許可するAWSアカウント
※利用システムのAWSアカウント



4.不適切設定検知機能

1）MAFFクラウド管理者アカウントのConfigで各利用システムのConfigの一元管理を行う。
2）MAFFクラウド管理者アカウントのSecurityHubで各利用システムのSecurityHubの一元管理を行う。
3）利用システム側で検知した不適切設定はMAFFクラウド管理者アカウントへも通知が行われる。
4）利用システムアカウント側でConfig、SecurityHubを適用するリージョンを「東京リージョンのみ」、「全リージョン」から選択することが可能。
※セキュリティの観点から「全リージョン」への適用を推奨しているがコスト増大につながるため「東京リージョンのみ」も選択可能としている。
東京リージョン以外の能動的に利用していないリージョンでの許可されていないアクティビティを検知し、リソースの盗用といったセキュリティ脅威への対策という観点からデフォルトで有効になっているリージョンについて全てのリージョンを対象に検知を行うことがベストプラクティスとなっている。
(例：管理者アカウント情報が意図せず漏洩し、攻撃者により東京リージョン以外の普段利用していないリージョンにリソースを作成された場合等に検知を行うことができる)
5）以下を対象によりConfigRules自動修復アクションを実施する。

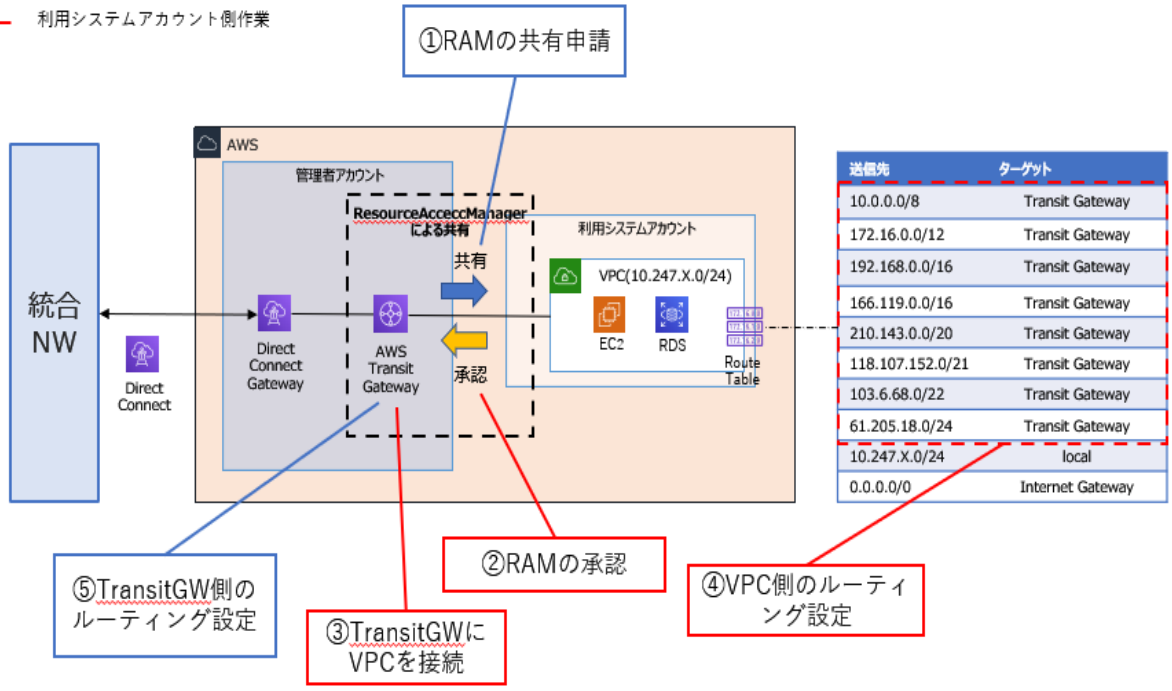
項番	実施方法	実施項目	実施アクション
1	AWSマネージドルール	RDSスナップショットがパブリックに公開されている	パブリック公開されているスナップショットを削除
2	カスタムルール	EBSスナップショットがパブリックに公開されている	EBSスナップショットのパブリック公開権限の削除 (AMIに紐づいているEBSスナップショットの削除が行えないためパブリック公開権限の削除を行う)



■閉域網接続の流れ

MAFFクラウド管理者アカウント側作業

利用システムアカウント側作業



手順①RAMの共有申請

以下のドキュメントを参考にMAFFクラウドアカウント内に作成したTransitGatewayを利用システムアカウントへ共有を行う。
※利用システムアカウントの「AWSアカウントID」の情報を元に共有を行う。
https://docs.aws.amazon.com/ja_jp/ram/latest/userguide/getting-started-sharing.html

手順②RAMの承認　※利用システムアカウント側作業

以下のドキュメントを参考にAWS Resource Access Managerから手順①で共有された共有申請の承認を行う。
https://docs.aws.amazon.com/ja_jp/ram/latest/userguide/working-with-shared.html#working-with-shared-invitation
※以下のリソースに対して共有を行う。
名前：「maff-prod-ram」
所有者：「021272315908」

手順③TransitGWにVPCを接続　※利用システムアカウント側作業

以下のドキュメントを参考に手順②で共有したTransitGatewayに閉域網接続を行いたいVPCを接続する。
https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/tgw-vpc-attachments.html
※以下のTransitGatewayに対して接続を行う。
Transit Gateway ID：「tgw-0a858388cccaf937c」
OwnerID：「021272315908」

手順④VPC側のルーティング設定　※利用システムアカウント側作業

VPC側のルートテーブルに農林水産省内宛の経路を追加する。ターゲットとして手順③で接続しTransitGatewayを指定する。
※以下、農林水産省内で利用されているIPアドレスとなりますが、全てを指定すると範囲が広すぎるため実際にアクセスする対象に絞って設定を行ってください。

＜農水省内でプライベートアドレスとして使用しているIPアドレス＞
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

＜グローバルアドレス＞
166.119.0.0/16
※うち166.119.78.0/23はインターネット側からもアクセスできるDMZ

＜政府共通ネットワークで利用しているIPアドレス＞
210.143.0.0/20
118.107.152.0/21
103.6.68.0/22
61.205.18.0/24

手順⑤TransitGW側のルーティング設定

以下のドキュメントを参考に手順③でTransitGWに接続したVPCのルーティング設定を行う。
https://docs.aws.amazon.com/ja_jp/vpc/latest/tgw/tgw-route-tables.html

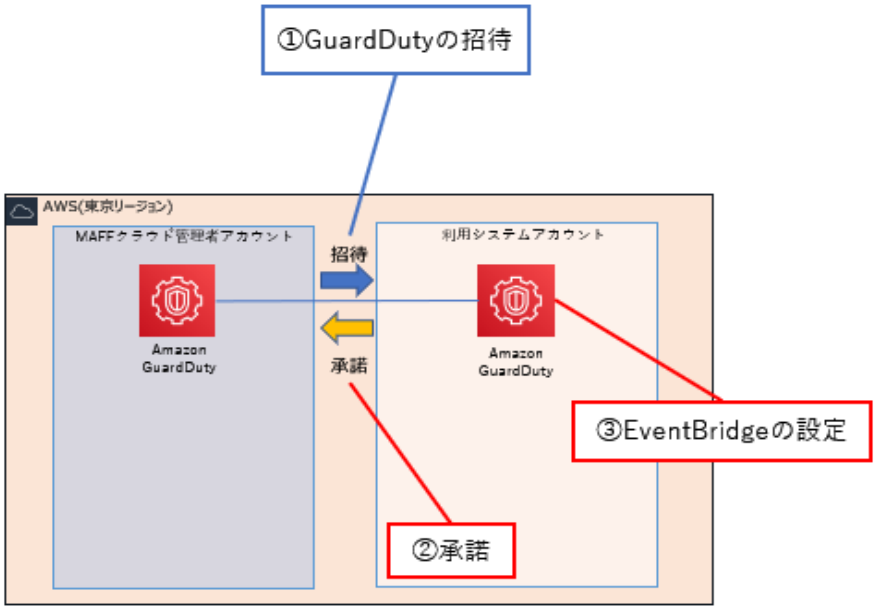
疎通確認

アプリケーションの疎通確認方法についてはPJMOと調整のうえ実施してください。

■マネージド型脅威検出機能設定の流れ

MAFFクラウド管理者アカウント側作業

利用システムアカウント側作業



事前作業　※利用システムアカウント側作業

GuardDutyが有効化されていない場合は以下ドキュメントを参考に有効化を行ってください。

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_settingup.html

手順①GuardDutyの招待

以下のドキュメントを参考にMAFFクラウドアカウント内のGuardDutyに利用システムアカウントをメンバーアカウントとして招待を行う。

※利用システムアカウントの「AWSアカウントID」、「AWS アカウントのルートユーザー」の情報を元に招待を行う。

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_invitations.html

手順②承諾　※利用システムアカウント側作業

以下のドキュメントのステップ３を参考に招待を承諾する。

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_invitations.html

手順③EventBrigeの設定　※利用システムアカウント側作業

以下のドキュメントを参考にGuardDutyでの検出結果の通知設定を行う。

https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_findings_cloudwatch.html#guardduty_cloudwatch_severity_notification

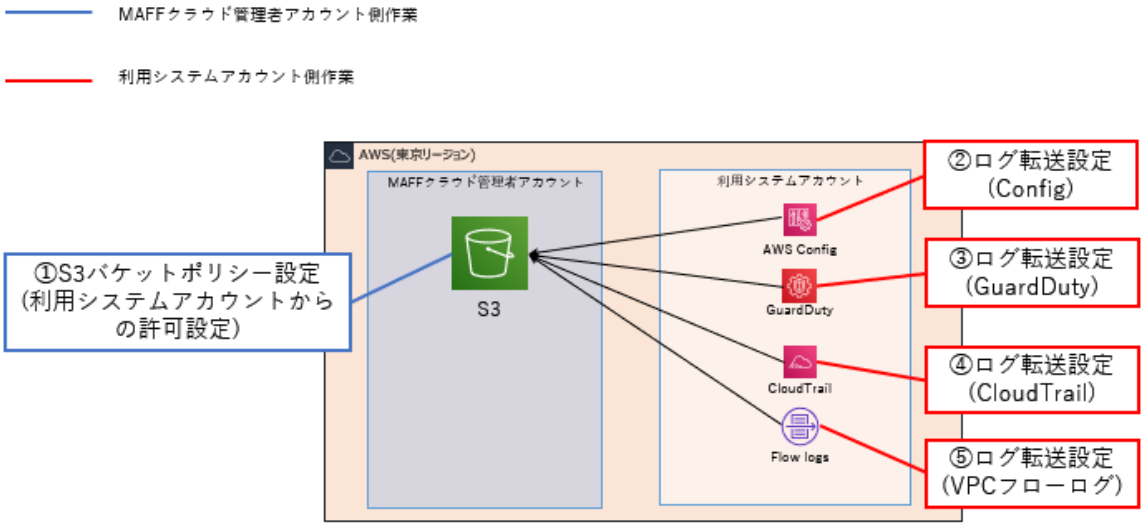
※MAFFクラウドでは重要度Medium以上を対象に検知を行うことを推奨。

Event Bridgeで重要度Medium以上(Severity >= 4.0)でフィルタリングを行う際のイベントパターンを以下に示す。

■イベントパターン

```
{
  "detail-type": ["GuardDuty Finding"],
  "source": ["aws.guardduty"],
  "detail": {
    "severity": [{
      "numeric": [">=", 4]
    }]
  }
}
```

■監査ログ収集機能設定の流れ



手順①S3バケットポリシー設定

以下のドキュメントを参考にMAFFクラウドアカウント内の監査ログ収集用S3バケットに利用システムアカウントからのアクセス許可設定を行う。
※利用システムアカウントの「AWSアカウントID」の情報を元に招待を行う。
https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/dev/access-policy-language-overview.html

手順②ログ転送設定(Config) ※利用システムアカウント側作業

以下のドキュメントを参考に設定履歴と設定スナップショットファイルを送信する先の Amazon S3 バケットをMAFF管理者アカウントの監査ログ収集用S3バケットに変更する。
https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/gs-console.html
※以下のS3バケット名を指定してください。
監査ログ収集用S3バケット：maff-prod-audit-logs

手順③ログ転送設定(GuardDuty) ※利用システムアカウント側作業

以下のドキュメントを参考にGuardDutyでの検出結果の出力先設定を行う。
https://docs.aws.amazon.com/ja_jp/guardduty/latest/ug/guardduty_exportfindings.html
※以下のバケットARNとキーARNを指定してください。
バケットARN：　arn:aws:s3:::maff-prod-audit-logs/guardduty
キーARN:　arn:aws:kms:ap-northeast-1:021272315908:key/f33c2829-51bd-41f2-9615-81ac6b6ab586

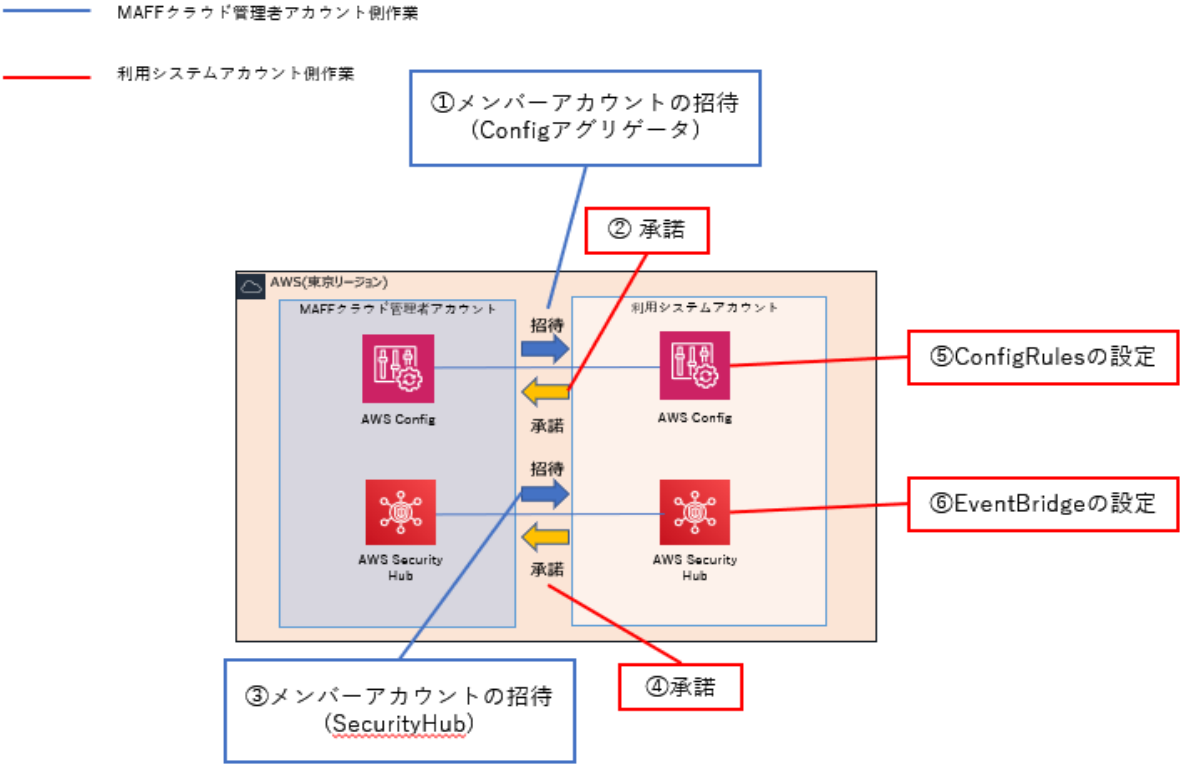
手順④ログ転送設定(CloudTrail) ※利用システムアカウント側作業

事前に用意するファイル
　CloudFormation用テンプレート：010_cloudtrail.yml
以下のドキュメントを参考にCloudFormationでCloudTrailの証跡の作成を行う。
https://docs.aws.amazon.com/ja_jp/AWSCloudFormation/latest/UserGuide/GettingStarted.Walkthrough.html
　・パラメータには以下を入力
　ProjectCode：（任意のシステム名）
　RetentionInDays：　90　　※Cloudwatchログのデータ保存期間
　S3BucketName：　maff-prod-audit-logs

手順⑤ログ転送設定(VPCフローログ) ※利用システムアカウント側作業

事前に用意するファイル
　CloudFormation用テンプレート：010_vpcFlowLog.yml
以下のドキュメントを参考にCloudFormationでVPCフローログの設定を行う。
https://docs.aws.amazon.com/ja_jp/AWSCloudFormation/latest/UserGuide/GettingStarted.Walkthrough.html
　・パラメータには以下を入力
　BucketName：　maff-prod-audit-logs
　FlowLogsFilter：　ALL
　VPCID：（対象のVPC）

■不適切設定検知機能設定の流れ



事前作業　※利用システムアカウント側作業

Config、SecurityHubが有効化されていない場合は以下ドキュメントを参考に有効化を行ってください。

・Config

https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/gs-console.html

・SecurityHub

※デフォルトの設定で有効化を行ってください。

AWS 基礎セキュリティのベストプラクティス v1.0.0 を有効化：チェックあり

CIS AWS Foundations Benchmark v1.2.0 を有効化：チェックあり

PCI DSS v3.2.1 を有効化：チェックなし

https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-enable.html#securityhub-enable-console

手順①メンバーアカウントの招待(Configアグリゲータ)

以下のドキュメントを参考にConfigアグリゲータに利用システムアカウントをメンバーアカウントとして招待を行う。

https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/setup-aggregator-console.html

手順②承諾　※利用システムアカウント側作業

以下のドキュメントを参考にConfigアグリゲータのメンバーアカウントの招待を承諾する。

https://docs.aws.amazon.com/ja_jp/config/latest/developerguide/authorize-aggregator-account-console.html

手順③メンバーアカウントの招待(SecurityHub)

以下のドキュメントを参考にConfigアグリゲータに利用システムアカウントをメンバーアカウントとして招待を行う。

https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-accounts-add-invite.html

手順④承諾　※利用システムアカウント側作業

以下のドキュメントを参考にSecurityHubのメンバーアカウントの招待を承諾する。

https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-accounts-add-invite.html

手順⑤ConfigRulesの設定　※利用システムアカウント側作業

事前に用意するファイル

CloudFormation用テンプレート：010_config_rules.yml

Lambda用コード：lambda_function.zip　※事前に任意のS3バケットに配置してください

以下ドキュメントを参考にCloudFormationより「010_config_rules.yml」を実施。

https://docs.aws.amazon.com/ja_jp/AWSCloudFormation/latest/UserGuide/GettingStarted.Walkthrough.html

・パラメータには以下を入力

LambdaSourceKey：lambda_function.zip

LambdaSourceS3BucketName：（「lambda_function.zip」を格納したS3バケット名）

ProjectCode：(任意のシステム名)

手順⑥EventBridgeの設定　※利用システムアカウント側作業

以下のドキュメントを参考にSecurityHubでの検出結果の通知設定を行う。

https://docs.aws.amazon.com/ja_jp/securityhub/latest/userguide/securityhub-cwe-all-findings.html

※MAFFクラウドでは新規の通知かつ重要度がMedium 以上の脅威を対象に検知を行うことを推奨。

Event Bridgeでs新規の通知かつ重要度Medium以上でフィルタリングを行う際のイベントパターンを以下に示す。

■イベントパターン

```
{
  "detail-type": ["Security Hub Findings - Imported"],
 "source": ["aws.securityhub"],
 "detail": {
   "findings": {
    "Compliance": {
     "Status": ["FAILED"]
    },
    "Workflow": {
      "Status": ["NEW"]
    },
    "Severity": {
     "Label": ["CRITICAL", "HIGH", "MEDIUM"]
    }
   }
 }
}
```

農林水産省クラウド
共通機能設定手順書(Azure)

2022年6月17日版

改版履歴

改訂日	対象シート	改訂内容
2022/02/04	改訂履歴	改訂履歴シートを新規作成
2022/06/06	目次と作業分担	シート名を「目次」から「目次と作業分担」に変更、MAFFクラウド・利用システム側アカウントの作業分担について表を追加
2022/06/06	1.統合NW閉域網接続機能	疎通確認部分に「※利用システムアカウント側作業」を追加
2022/06/17	目次と作業分担	シートを目立たせるため、色付け

0.はじめに

0.1.本書の内容と目的

本書は、農林水産省クラウドの運用業務における共通機能の設定方法を記載したものである。
PJMOから提出された利用申請書を元にPMO及びPJMO双方で設定を行う。
※ただし、疎通確認時以外はPJMOの作業は発生しない。

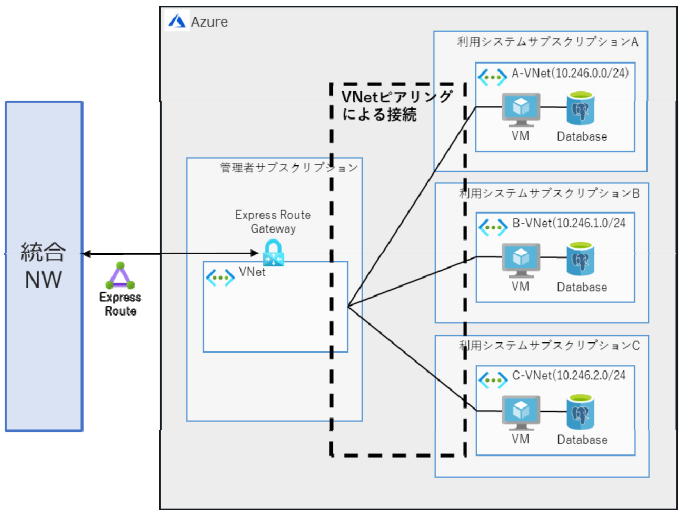
■目次

■MAFFクラウド・利用システム側アカウントの作業分担

作業内容	担当
0.5.ARMテンプレートによる自動設定	
手順①リソースグループの作成	MAFFクラウド
手順②管理グループの作成とサブスクリプションの移動	MAFFクラウド
手順③カスタムテンプレートのデプロイ	MAFFクラウド
手順④デプロイの確認	MAFFクラウド
1.統合NW閉域網接続機能	
手順①Vnetピアリングの作成	MAFFクラウド
疎通確認	**利用システムアカウント側作業**
2.マネージド型脅威検出機能	
手順①自動プロビジョニング設定	MAFFクラウド
手順②電子メールの通知設定	MAFFクラウド
手順③ワークフローの自動化設定	MAFFクラウド
手順④連続エクスポート設定	MAFFクラウド
手順⑤メール通知設定	MAFFクラウド
3.監査ログ収集機能	
手順①Activity Log診断結果ログのエクスポート設定	MAFFクラウド
手順②Microsoft Defender for Cloudのストレージアカウントへのログエクスポート設定	MAFFクラウド
4.不適切設定検知機能	
手順①Azure Policyブループリントの割り当て	MAFFクラウド

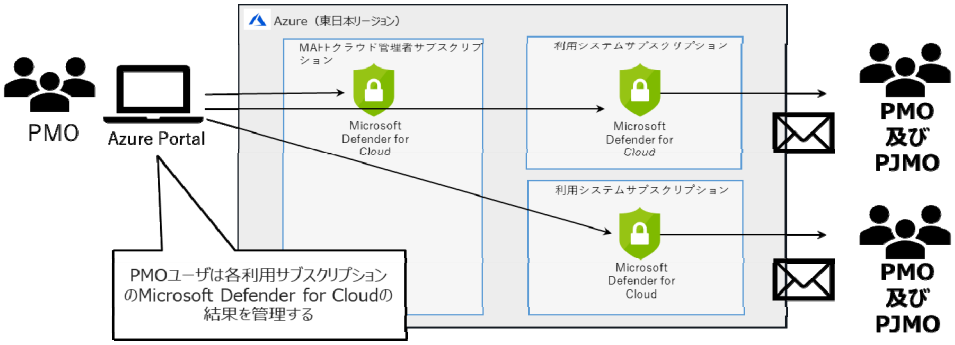
1.統合NW閉域網接続機能

1）統合NWと各利用システム間をExpressRoute Gatewayを経由して接続を行う。
2）MAFFクラウド管理者システムと各利用システム間をVNetピアリングにより接続を行う。
3）MAFFクラウド管理者システム内のVnetピアリングで各利用システムサブスクリプションとの接続の一元管理を行う。



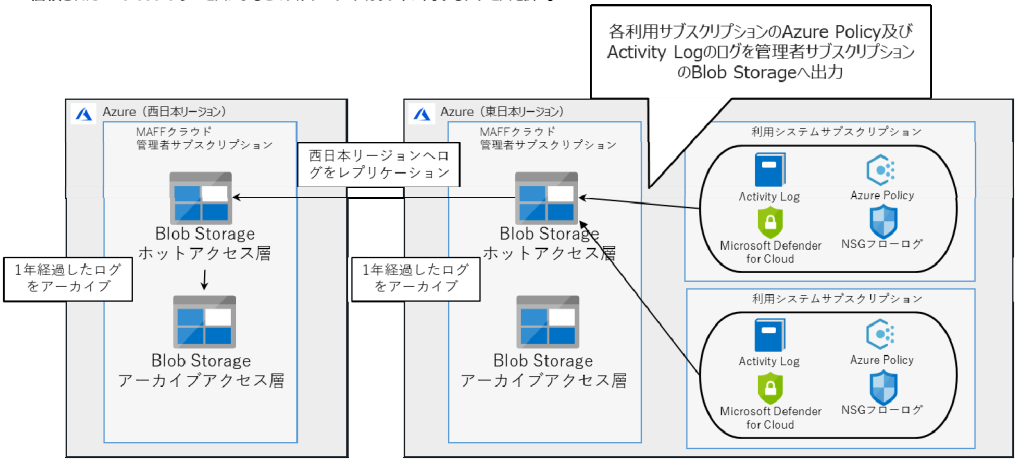
2.マネージド型脅威検出機能

1）各サブスクリプションのMicrosoft Defender for Cloudの評価結果を管理者ユーザでAzure Portalから一括表示することで
　各利用システムのMicrosoft Defender for Cloudの一元管理を行う。
2）利用システム側で検知した脅威はMAFFクラウド管理者サブスクリプションへも通知が行われる。
3）利用システムサブスクリプション側でのMicrosoft Defender for Cloudの適用範囲については、自動的にサブスクリプション全体が対象となる。



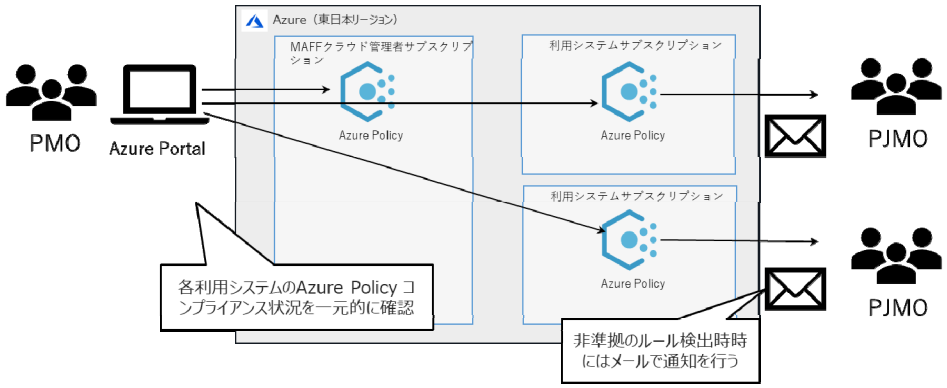
3.監査ログ収集機能

1）各利用システムサブスクリプションの以下ログをMAFFクラウド管理者サブスクリプション内のAzure Storage（ホットアクセス層）に出力する。
・Microsoft Defender for Cloudの評価結果
・Activity Log
・NSGフローログ
・Azure Policyの評価結果
2）MAFFクラウド管理者サブスクリプションではAzure Storageのライフサイクルポリシーにより、1年にわたってアクセスも変更もされていないログはアーカイブアクセス層に移動し、
4年にわたってアクセスも変更もされていないログは削除する。
バックアップ先として西日本リージョンのAzure StorageへGeoレプリケーションを行う。
3）MAFFクラウド管理者サブスクリプションのAzure Storageではネットワーク設定によりアクセス元の制限を行っている。
■許可するアクセス元
<Azure Storageのログにアクセスする運用者のネットワークのアドレス範囲>
■例外
信頼された Microsoft サービスによるこのストレージ アカウントに対するアクセスを許可



4.不適切設定検知機能

1）各サブスクリプションのAzure Policyの評価結果を管理者ユーザでAzure Portalから一括表示することで、各利用システムのAzure Policyの一元管理を行う。
2）利用システム側で検知した不適切設定はMAFFクラウド管理者サブスクリプションへも通知が行われる。
3）利用システムサブスクリプション側でのAzure Policyの適用範囲については、自動的にサブスクリプション全体が対象となる。



■インフラリソース自動デプロイの流れ

手順①リソースグループの作成

以下のドキュメントを参考に新規で契約した利用システムサブスクリプション内にリソースグループを作成する。
https://docs.microsoft.com/ja-jp/azure/azure-resource-manager/management/manage-resource-groups-portal
※設定値は以下の通り。
サブスクリプション：＜対象のサブスクリプションを選択＞
リソースグループ：「maff-prod-rg-infra」
リージョン：「（Asia Pacific）東日本」

手順②管理グループの作成とサブスクリプションの移動

以下のドキュメントを参考に新規で契約した利用システムサブスクリプションを本手順で作成する管理グループに所属させる。
https://docs.microsoft.com/ja-jp/azure/governance/management-groups/overview
※新規作成する管理グループの情報は以下の通り。
親管理グループ：「MAFFクラウド（利用システムサブスクリプション）」
管理グループID：＜下記のパスワード生成サイトから生成した12桁英数字の文字列＞
https://www.luft.co.jp/cgi/randam.php
管理グループの表示名：＜利用システム名＞

手順③カスタムテンプレートのデプロイ

以下のドキュメントの「カスタム テンプレートからリソースをデプロイする」を参考に手順①で作成したリソースグループにリソース群をデプロイする。
https://docs.microsoft.com/ja-jp/azure/azure-resource-manager/templates/deploy-portal
※設定値は以下の通り。
サブスクリプション：＜対象のサブスクリプションを選択＞
リソースグループ：「maff-prod-rg-infra」
リージョン：「東日本」（固定）
Maff_spoke_vnet_cidr：「10.246.xxx.0/24」（新利用システムに割り当てるアドレス範囲）
Maff_spoke_subnet_ip：「10.246.xxx.0」（新利用システムに割り当てるアドレス範囲から/24を除いた部分）
From Email Address：「ml_maffcloud@maff.go.jp」（アラート発報時の送信元ML）
To Email Address：＜利用システム側のML＞

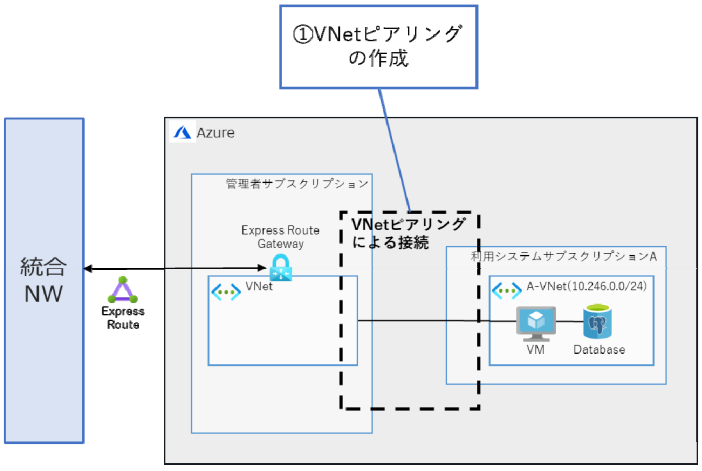
手順④デプロイの確認

手順①で作成したリソースグループに移動し、リソースのレコードが8件となっていることを確認する。
リソースのデプロイに2~3分かかる場合もあるため、8件になっていない場合は時間をおいて「更新」して再度確認する。

■閉域網接続の流れ

MAFFクラウド管理者アカウント側作業

利用システムアカウント側作業



手順①Vnetピアリングの作成

以下のドキュメントを参考にMAFFサブスクリプション内にVnetピアリングを作成し、MAFFクラウド管理者システムと利用システム間をVNetピアリングにより接続を行う。
https://docs.microsoft.com/ja-jp/azure/virtual-network/virtual-network-manage-peering
※VnetピアリングはMAFFクラウド管理者サブスクリプションのVnet「maff-prod-vnet」から作成する。
※新規作成する「この仮想ネットワーク」のピアリングの情報は以下の通り。
ピアリングリンク名：「maff-prod-prlink- ＜利用システムのIPアドレス範囲から/24を除外した部分＞」
リモート仮想ネットワークへのトラフィック：「許可（規定）」
リモート仮想ネットワークから転送されたトラフィック：「許可（規定）」
仮想ネットワーク ゲートウェイまたはルート サーバー：「この仮想ネットワークのゲートウェイまたはルート サーバーを使用する」

※新規作成する「リモート仮想ネットワーク」のピアリングの情報は以下の通り。
ピアリングリンク名：「maff-prod-prlink- ＜利用システムのIPアドレス範囲から/24を除外した部分＞」
仮想ネットワークのデプロイ モデル：「Resource Manager」
サブスクリプション：「＜利用システムのサブスクリプション＞」
仮想ネットワーク：「maff-prod-vnet」
リモート仮想ネットワークへのトラフィック：「許可（規定）」
リモート仮想ネットワークから転送されたトラフィック：「許可（規定）」
仮想ネットワーク ゲートウェイまたはルート サーバー：「リモート仮想ネットワークのゲートウェイまたはルート サーバーを使用する」

疎通確認　※利用システムアカウント側作業

アプリケーションの疎通確認方法については、シート1~4の設定完了後、PJMOと調整のうえ実施してください。
Azure側の利用システム間の通信制御は、**MAFFクラウド管理者サブスクリプションでは行わず、利用システムサブスクリプション内でのNSGによって実装します。**
NSGの受信設定をホワイトリスト形式で管理し、他のシステムとの通信が必要な場合は以下のIPアドレス範囲や、他のAWS/Azureの利用システムのIPアドレス範囲からの通信を許可します。
※以下、農林水産省内で利用されているIPアドレスとなりますが、全てを指定すると範囲が広すぎるため実際にアクセスする対象に絞って設定を行ってください。

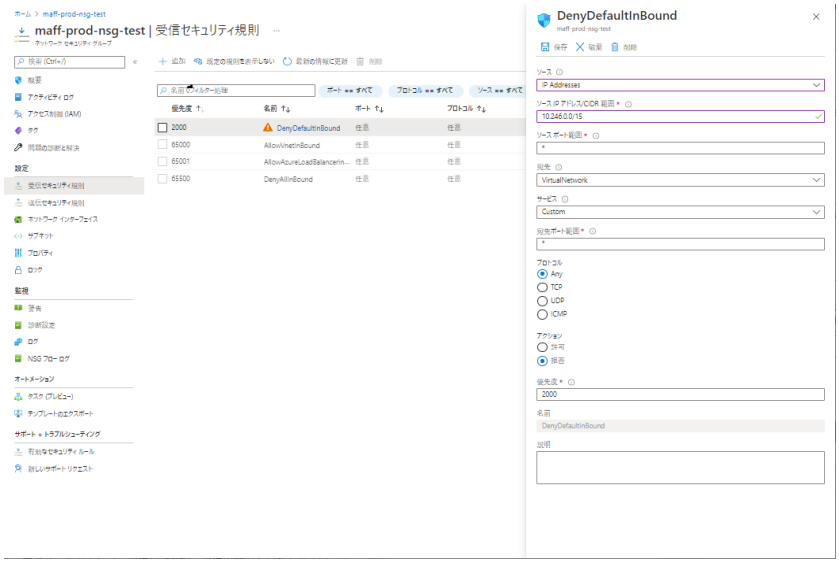
統合NW側で使用されているIPアドレス範囲は以下の通りです。
＜農水省内でプライベートアドレスとして使用しているIPアドレス＞
10.0.0.0/8
172.16.0.0/12
192.168.0.0/16

＜グローバルアドレス＞
166.119.0.0/16
※うち166.119.78.0/23はインターネット側からもアクセスできるDMZ

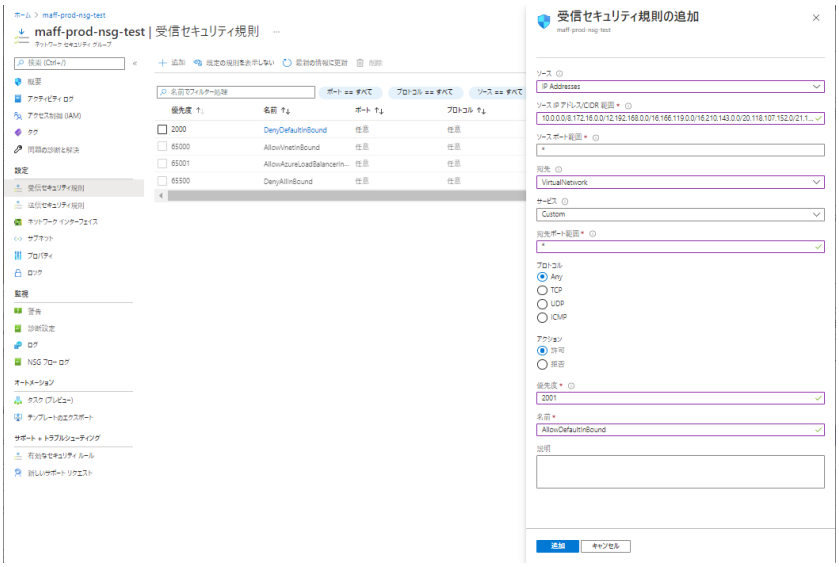
＜政府共通ネットワークで利用しているIPアドレス＞
210.143.0.0/20
118.107.152.0/21
103.6.68.0/22
61.205.18.0/24

各利用システム側のアクセス制御として、NSGには以下の①、②の規則をデフォルトルールとして作成してもらい、③のようにホワイトリスト形式で許可対象のIPアドレスを指定する形になります。

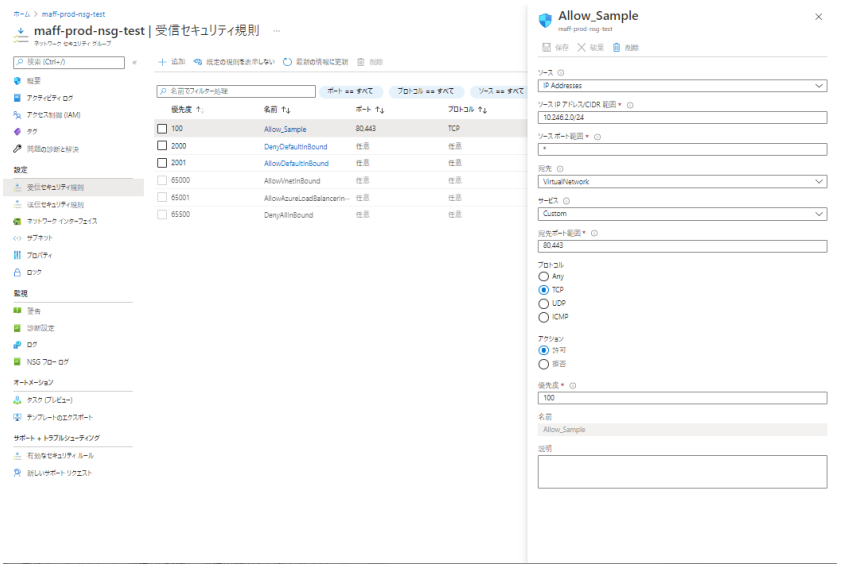
①VNetに対するMAFFクラウド（10.246.0.0/15）からの全ての通信をDenyするNSG規則



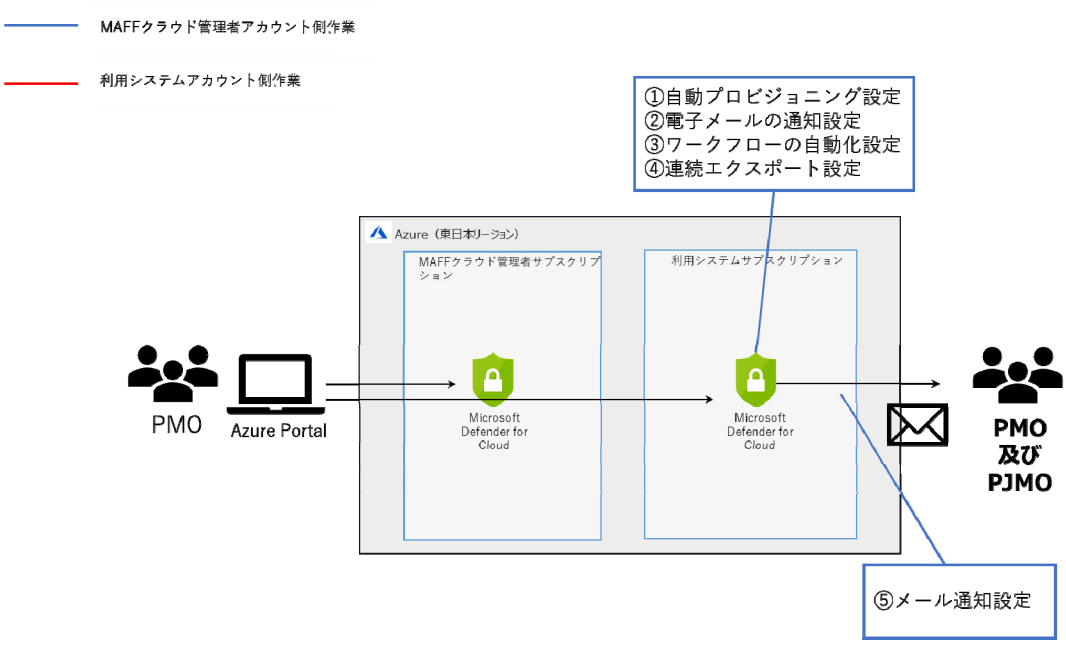
②VNetに対するMAFFクラウドと農水省NWからの全ての通信（上記のすべてのIPアドレス範囲）をAllowするNSG規則



③上記の2つのルールを決まりとして作成し、あとは「2000」より優先度の高いレコードとして、通信を許可したい特定のNWからの通信をAllowするNSGを作成していきます。（以下はサンプルです。）



■マネージド型脅威検出機能設定の流れ



手順①自動プロビジョニング設定

以下のドキュメントを参考に拡張機能の自動プロビジョニング設定を行う。
https://docs.microsoft.com/ja-jp/azure/security-center/security-center-enable-data-collection
※自動プロビジョニング設定の情報は以下の通り。
※個別の設定はせず、「すべての拡張機能を有効にする」を選択する。
ワークスペースの構成：「Azure VMを別のワークスペースに接続する」
ワークスペース名：「maff-prod-laws-security-＜新規利用システムのサブスクリプションID＞」
既存のVMへの適用：「既存および新しいVM」
※忘れずに「保存」を押下すること。

手順②電子メールの通知設定

以下のドキュメントを参考に電子メールの通知設定を行う。
https://docs.microsoft.com/ja-jp/azure/security-center/security-center-provide-security-contact-details
※電子メールの通知設定の情報は以下の通り。
メールの受信者：「ml_maffcloud@maff.go.jp,＜利用システム側のML＞」
通知の種類：「次の重要度（以上）のアラートについて通知します。：中」
※忘れずに「保存」を押下すること。

手順③ワークフローの自動化設定

以下のドキュメントを参考にワークフローの自動化設定を2件行う。「ロジックアプリ」の作成は済んでいるため、ここでは選択するのみでよい。
https://docs.microsoft.com/ja-jp/azure/security-center/workflow-automation
※ワークフローの自動化設定（推奨事項）の情報は以下の通り。
名前：「maff-prod-wf-sc-recommendation」
リソースグループ：「maff-prod-rg-infra」
Defender for Cloudのデータ型の選択：「推奨事項」
推奨事項の名前：「すべての推奨事項が選択されています」
推奨事項の重要度：「中,高」
推奨事項の状態：「異常」
次のサブスクリプションからロジックアプリのインスタンスを表示します：「＜新規の利用システムサブスクリプション＞」
ロジックアプリ名：「maff-prod-logic-apps-sc-recommendation」

※ワークフローの自動化設定（規制コンプライアンス）の情報は以下の通り。
名前：「maff-prod-wf-sc-compliance」
リソースグループ：「maff-prod-rg-infra」
Defender for Cloudのデータ型の選択：「規制コンプライアンス標準」
コンプライアンス標準：「すべての標準が選択されました」
コンプライアンス コントロールの状態：「失敗」
次のサブスクリプションからロジックアプリのインスタンスを表示します：「＜新規の利用システムサブスクリプション＞」
ロジックアプリ名：「maff-prod-logic-apps-sc-compliance」

手順④連続エクスポート設定

以下のドキュメントを参考にLog Analyticsワークスペースへの連続エクスポート設定を行う。（イベントハブの設定は変更しない。）
https://docs.microsoft.com/ja-jp/azure/security-center/continuous-export?tabs=azure-portal
※連続エクスポート設定の情報は以下の通り。
エクスポートが有効です：「オン」
セキュリティに関する推奨事項：「チェック」（内容は変更しない。）
セキュアスコア：「チェック」（内容は変更しない。）
セキュリティ警告：「チェック」（内容は変更しない。）
リソースグループ：「maff-prod-rg-infra」
サブスクリプション：「＜新規のサブスクリプション＞」
ターゲットワークスペースの選択：「maff-prod-laws-security-＜新規のサブスクリプションID＞」
※忘れずに「保存」を押下すること。

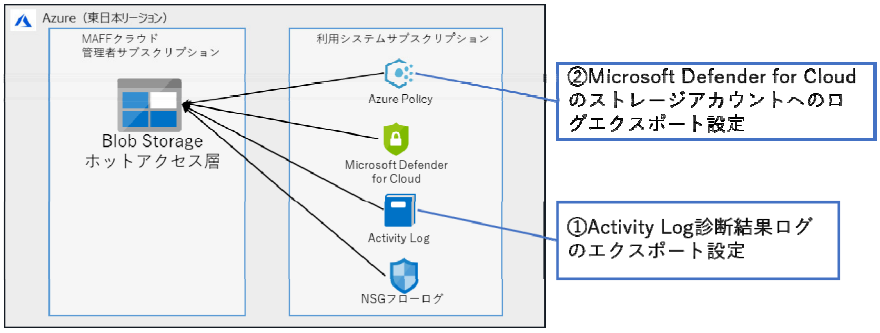
手順⑤メール通知設定

以下のドキュメントを参考にLog Analyticsワークスペースへの連続エクスポート設定を行う。（イベントハブの設定は変更しない。）
https://docs.microsoft.com/ja-jp/azure/security-center/continuous-export?tabs=azure-portal
※メール通知設定の情報は以下の通り。既存の接続が選択肢として表示されている場合は、それを選択する。
接続名：「maff-prod-logicapps-connection-sc」
SendGrid APIキー：「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」
※件名、本文、宛先などを確認し、忘れずに「保存」を押下すること。

■監査ログ収集機能設定の流れ

MAFFクラウド管理者アカウント側作業

利用システムアカウント側作業



手順①Activity Log診断結果ログのエクスポート設定

以下のドキュメントを参考にMAFFクラウドサブスクリプション内の監査ログ収集用Azure Storageと利用システムサブスクリプション内のLog Analyticsワークスペースに
Activity Logのエクスポート設定を行う。
https://docs.microsoft.com/ja-jp/azure/azure-monitor/essentials/activity-log
※Activity Log診断結果ログのエクスポート設定の情報は以下の通り。
サブスクリプション：「＜新規のサブスクリプション＞」
診断設定の名前：「maff-prod-diag-security」
log：「すべてにチェック」
Log Analyticsワークスペースへの送信：「チェック」
サブスクリプション：「＜新規のサブスクリプション＞」
Log Analyticsワークスペース：「maff-prod-laws-security-＜新規のサブスクリプションID＞」
ストレージアカウントへのアーカイブ：「チェック」
サブスクリプション：「SUB21012799299」
ストレージアカウント：「maffprodsasecurity」
※忘れずに「保存」を押下すること。

手順②Microsoft Defender for Cloudのストレージアカウントへのログエクスポート設定

以下のドキュメントを参考にCloud Shellを利用し、Microsoft Defender for Cloud関連のログを利用システムサブスクリプションのLog Analyticsワークスペースから
MAFFクラウド管理者サブスクリプションのAzure Storageへのエクスポート設定を行う。
https://docs.microsoft.com/ja-jp/azure/cloud-shell/overview
※Cloud Shell起動時の情報は以下の通り。ストレージアカウントが自動で作成される。
サブスクリプション：「SUB21012799299」

※Cloud Shellでのコマンド実行内容は以下の通り。
以下のコマンド実行により、「IsDefault」が「True」となっているサブスクリプションが現在のコマンド実行対象となっている。
$ az account list --output table --all

以下のコマンドで、新規のサブスクリプションIDに切り替える。
$ az account set --subscription XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

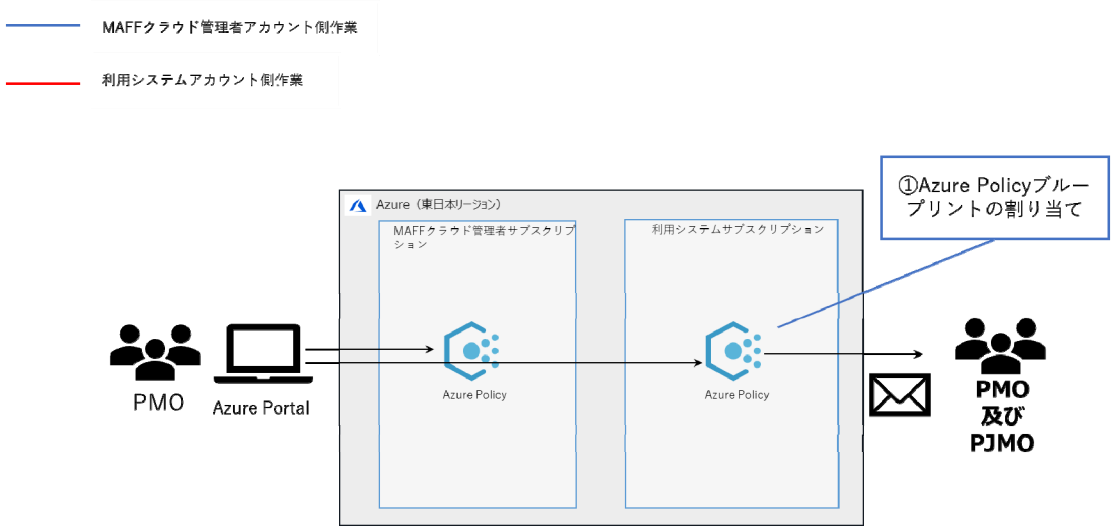
以下のコマンドで、Microsoft Defender for CloudからLog Analyticsワークスペースへのログ出力テーブルを確認する。（赤字箇所は適切な値に変更）
「SecureScores、SecurityAlert、SecurityRecommendation」の3テーブルが表示されるが、現時点で存在しない場合でも次のコマンドに進む。
$ az monitor log-analytics workspace table list --resource-group maff-prod-rg-infra --workspace-name maff-prod-laws-security-＜新規のサブスクリプションID＞ --query [].name --output table

以下のコマンドで、Log AnalyticsワークスペースからAzure Storageへのログ出力ルールを作成する。（赤字箇所は適切な値に変更）
$ az monitor log-analytics workspace data-export create --resource-group maff-prod-rg-infra --workspace-name maff-prod-laws-security-＜新規のサブスクリプションID＞
--name maff-prod-exportrule-laws-to-blob --tables SecureScores SecurityAlert SecurityRecommendation --destination '/subscriptions/3c9a9f4a-cec2-44ef-8528-6a6ee992bfe0/resourceGroups/maff-prod-rg-infra/providers/Microsoft.Storage/storageAccounts/maffprodsasecurity'

ここで、対象テーブルが存在しない場合は「SecureScoresはテーブルが存在しない」というようなメッセージが表示されるが、現時点ではルールの作成のみでよいため、
次のコマンドでSecureScores、SecurityAlert、SecurityRecommendationがルール内（tableNamesのリスト）に入っていれば問題ない。（赤字箇所は適切な値に変更）
$ az monitor log-analytics workspace data-export list --resource-group maff-prod-rg-infra --workspace-name maff-prod-laws-security-＜新規のサブスクリプションID＞

※本作業で自動作成されるストレージアカウントは削除する。
Cloud Shellで自動作成されるストレージアカウントは、サブスクリプション「SUB21012799299」のリソースグループ「cloud-shell-storage-southeastasia」内のすべてであるため、
上記のリソースグループごと削除する。

■不適切設定検知機能設定の流れ



手順①Azure Policyブループリントの割り当て

以下のドキュメントの「ブループリントを割り当てる」を参考に利用システムサブスクリプションにAzure Policyブループリントの割り当てを行う。

https://docs.microsoft.com/ja-jp/azure/governance/blueprints/create-blueprint-portal

※ブループリントの割り当て情報は以下の通り。（ブループリント自体は作成済み）

割り当てるブループリント名：「CommonRule」

サブスクリプション：「＜新規のサブスクリプション＞」

割り当て名：「Assignment-CommonRule」

リージョン：「東日本」

ブループリント定義ラベル：「ver1.0」

ロックの割り当て：「読み取り専用」

マネージドID：「システム割り当て済み」

アーティファクト/パラメーター：以下の表に沿って入力。

成果物	パラメーター値	備考
[プレビュー]: ストレージ アカウントのパブリック アクセスを禁止する必要がある		
[プレビュー]: 効果 (ポリシー: [プレビュー]: ストレージ アカウントのパブリック アクセスを禁止する必要がある)	Audit	
[プレビュー]: デプロイ - Azure Security エージェントを自動的にインストールするように Linux マシンを構成する		
[プレビュー]: デプロイ - Azure Security エージェントを自動的にインストールするように、Windows マシンを構成する		
[プレビュー]: デプロイ - Azure Security エージェントを自動的にインストールするように、Windows マシンを構成する		
リソース グループ名 (ポリシー: Microsoft Defender for Cloud データの Log Analytics ワークスペースへのエクスポートをデプロイする)	maff-prod-rg-infra	
リソース グループの場所 (ポリシー: Microsoft Defender for Cloud データの Log Analytics ワークスペースへのエクスポートをデプロイする)	東日本	
エクスポートされるデータ型 (ポリシー: Microsoft Defender for Cloud データの Log Analytics ワークスペースへのエクスポートをデプロイする)	全項目	
推奨事項 ID (ポリシー: Microsoft Defender for Cloud データの Log Analytics ワークスペースへのエクスポートをデプロイする)	[]	
推奨事項の重要度 (ポリシー: Microsoft Defender for Cloud データの Log Analytics ワークスペースへのエクスポートをデプロイする)	全項目	
セキュリティに関する調査結果を含める (ポリシー: Microsoft Defender for Cloud データの Log Analytics ワークスペースへのエクスポートをデプロイする)	true	
セキュリティ スコア コントロール ID (ポリシー: Microsoft Defender for Cloud データの Log Analytics ワークスペースへのエクスポートをデプロイする)	[]	
アラートの重要度 (ポリシー: Microsoft Defender for Cloud データの Log Analytics ワークスペースへのエクスポートをデプロイする)	全項目	
Regulatory compliance standards names (ポリシー: Microsoft Defender for Cloud データの Log Analytics ワークスペースへのエクスポートをデプロイする)	[]	
Log Analytics ワークスペース (ポリシー: Microsoft Defender for Cloud データの Log Analytics ワークスペースへのエクスポートをデプロイする)	maff-prod-laws-security-<サブスクリプションID>	
Microsoft Defender for Cloud での監視のために、仮想マシン スケール セットに Log Analytics エージェントをインストールする必要がある		
効果 (ポリシー: Microsoft Defender for Cloud での監視のために、仮想マシン スケール セットに Log Analytics エージェントをインストールする必要がある)	AuditIfNotExists	
Microsoft Defender for Cloud での監視のために、仮想マシンに Log Analytics エージェントをインストールする必要がある		
効果 (ポリシー: Microsoft Defender for Cloud での監視のために、仮想マシン スケール セットに Log Analytics エージェントをインストールする必要がある)	AuditIfNotExists	
Azure セキュリティ ベンチマーク		

Windows VM の Administrators グループから除外されたユーザーの一覧	;	
Windows VM の Administrators グループに含める必要があるユーザーの一覧	;	
Windows VM の Administrators グループに含める必要があるユーザー*だけ*の一覧	;	
Network Watcher を有効にする必要があるリージョンの一覧	japaneast	
VM の接続先となる仮想ネットワーク	;	
仮想ネットワークで使用する必要があるネットワーク ゲートウェイ	;	
Log Analytics エージェントが接続する必要のあるワークスペース ID の一覧	;	
診断ログを有効にする必要のあるリソースの種類の一覧	全項目	
最新の PHP バージョン	7.3	
最新の Java バージョン	11	
最新の Windows Python バージョン	3.6	
最新の Linux Python バージョン	3.8	
CIS Microsoft Azure Foundations Benchmark 1.1.0		
Network Watcher を有効にする必要があるリージョンの一覧 (ポリシー: CIS Microsoft Azure Foundations Benchmark 1.1.0)	東日本	
NetworkWatcher リソース グループ名 (ポリシー: CIS Microsoft Azure Foundations Benchmark 1.1.0)	NetworkWatcherRG	
使用が承認されている仮想マシン拡張機能の一覧 (ポリシー: CIS Microsoft Azure Foundations Benchmark 1.1.0)	["AzureDiskEncryption","AzureDiskEncryptionForLinux","DependencyAgentWindows","DependencyAgentLinux","IaaSAntimalware","IaaSDiagnostics","LinuxDiagnostic","MicrosoftMonitoringAgent","NetworkWatcherAgentLinux","NetworkWatcherAgentWindows","OmsAgentForLinux","VMSnapshot","VMSnapshotLinux"]	
MariaDB サーバーに対して公衆ネットワーク アクセスを無効にする必要がある		
結果 (ポリシー: MariaDB サーバーに対して公衆ネットワーク アクセスを無効にする必要がある)	Audit	
MySQL サーバーに対して公衆ネットワーク アクセスを無効にする必要がある		
結果 (ポリシー: MySQL サーバーに対して公衆ネットワーク アクセスを無効にする必要がある)	Audit	
PostgreSQL サーバーに対して公衆ネットワーク アクセスを無効にする必要がある		
結果 (ポリシー: PostgreSQL サーバーに対して公衆ネットワーク アクセスを無効にする必要がある)	Audit	
サブスクリプションで Microsoft Defender for Cloud を有効にする		
すべてのネットワーク セキュリティ グループに対してフロー ログを構成する必要がある		
ターゲット ネットワーク セキュリティ グループを使用してフロー ログ リソースをデプロイする		
NSG リージョン (ポリシー: ターゲット ネットワーク セキュリティ グループを使用してフロー ログ リソースをデプロイする)	東日本	
ストレージ ID (ポリシー: ターゲット ネットワーク セキュリティ グループを使用してフロー ログ リソースをデプロイする)	/subscriptions/3c9a9f4a-cec2-44ef-8528-6a6ee992bfe0/resourceGroups/maff-prod-rg-infra/providers/Microsoft.Storage/storageAccounts/maffprodsasecurity	
Network Watcher RG (ポリシー: ターゲット ネットワーク セキュリティ グループを使用してフロー ログ リソースをデプロイする)	NetworkWatcherRG	
Network Watcher 名 (ポリシー: ターゲット ネットワーク セキュリティ グループを使用してフロー ログ リソースをデプロイする)	NetworkWatcher_japaneast	

割り当てたブループリントのマネージドリソースを確認し、最上部の「共同作成者」となっているクライアントIDをもとに、PMO運用担当者グループに所属させる。
グループへの追加時は「クライアントID」で検索して設定する。

令和4年度
農林水産省クラウド運用及び移行支援業務

MAFFクラウド利用システム向け命名規約

2022年4月13日版

改版履歴

改訂日	対象シート	改訂内容
2022/02/04	改訂履歴	改訂履歴シートを新規作成
2022/04/06	2.AWS_規約設計	37行目 Security Groupの命名ルールについて変更
2022/05/25	1.AWS_タグ設計	83-88行目 ElasticIPの規約を追加 89-106行目 NetworkFirewallの規約を追加 248-254行目 Systems Managerの規約を追加 269行目 Elasticsearch→OpenSearchに変更 312-317行目 DataPipelineの規約を追加 337行目 AWS BackupについてOrganizations利用時の備考を追記 379-384行目 CertificateManagerの規約を追加 391行目 Cloudfrontの規約を追加
2022/05/25	2.AWS_規約設計	29行目 ElasticIPの規約を追加 30-32行目 NetworkFirewallの規約を追加 66行目 RDS(Oracle)に関する規約追加 85行目 CloudWatchルール規約廃止 95,96行目 Systems Managerの規約を追加 109行目 Budgetsの規約を追加 115行目 Athenaの規約を追加 116行目 Elasticsearch→OpenSearchに変更 139行目 DataPipelineの規約を追加 148行目 AWS Backupについて備考を追記 157行目 CertificateManagerの規約を追加

◆本書の目的

CoEによるMAFFクラウド利用システムの横断的な管理が容易となるよう、AWS/Azureが提供している各サービスの命名に一貫したルールを定める。
統一的な命名規約を定めることで、命名規約検討に係るPJMO負荷および設計工数を低減する。

◆利用方法

各システムのPJMOは自システムの設計・開発業務時に本資料を事業者へ提供し、本規約を基に設計を行うよう依頼する。
特別な事情がない限り本規約の通りに設計を行うこと。

◆目次

1.AWS タグ設計 タグ一覧

前提
・本規約は、各リソースに設定するタグの記載ルールを定義する。
・改定により更新された規約については、原則遡って適用しない。
・タグの値は規約設計にあわせて英小文字もしくは数字で記載する。日本語のローマ字書きではなく英訳を記載すること。
・{本番／検証／ステージング／開発}については、prod／test／stg／devを代入する。必要な環境のみを作成し、不必要なものは作成しないこと。
・{サブシステムコード}については、システムに複数のサブシステムを内包している場合に各システムにて決定する。サブシステムがない場合、「SubSystem」のタグは設定不要。例（F列）に示す"xq"はサブシステムコードの一例である。
・{リージョン}については、ap-northeast-1（東京）を利用する場合にはapn1、ap-northeast-3（大阪）を利用する場合にはapn3を設定する。
・{システム略称}については、農林水産省クラウド共通機能利用申請書の「システム略称（英小文字/数字20字以内）」欄に記載したものを設定する。
・本規約に記載されていないサービスについては、定義済の規約を参照しタグを設定すること。
・個別システムにて必要があれば本規約に記載されていないタグについても追加可能。

カテゴリ	内容	タグ	規約	例	備考
IAM	USER	設定不可	-	-	
	Group	設定不可	-	-	
	Role	Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	Policy	設定不可	-	-	
VPC	VPC	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	subnet	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	RouteTable	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	DHCPオプションセット	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	VPCピアリング	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	InternetGateway	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	VPNGateway	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	CustomerGateway	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	NATGateway	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	VPCEndpoint	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	ElasticIP	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	NetworkFirewall ファイアウォール	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	NetworkFirewall ファイアウォールポリシー	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	NetworkFirewall ルールグループ	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
EC2	EC2	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	

カテゴリ	内容	タグ	規約	例	備考
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	AMI	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	KeyPair	設定不可	-	-	
	起動テンプレート名	Name	規約設計を参照	規約設計を参照	
EBS	EBS	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	Snapshot	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
ENI	ENI	Name	規約設計を参照	規約設計を参照	
Security Group	SecurityGroup	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
S3	バケット	Name	規約設計のバケット名を参照	規約設計のバケット名を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	イベント	設定不可	-	-	
	ライフサイクルルール	設定不可	-	-	
	ストレージクラス分析	設定不可	-	-	
	メトリクスフィルタ	設定不可	-	-	
	インベントリ	設定不可	-	-	
EFS	ファイルシステム	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Glacier	ボールト	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Redshift	クラスター	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	Snapshot	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	クラスターパラメータグループ	Name	規約設計を参照	規約設計を参照	
	イベントサブスクリプション	設定不可	-	-	
ELB	ロードバランサー	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	ターゲットグループ	Name	規約設計を参照	規約設計を参照	
AutoScaling	起動設定	設定不可	-	-	
	グループ	Name	規約設計を参照	規約設計を参照	
	スケールポリシー	設定不可	-	-	
	ライフサイクルフック名	設定不可	-	-	
RDS / Aurora	DBインスタンス	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	DBサブネットグループ	Name	規約設計を参照	規約設計を参照	
	DBクラスター	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	DBパラメータグループ	Name	規約設計を参照	規約設計を参照	
	DBオプショングループ	Name	規約設計を参照	規約設計を参照	
	DBスナップショット	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	サブスクリプション	Name	規約設計を参照	規約設計を参照	
DynamoDB	テーブル	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	バックアップ	設定不可	-	-	
	DynamoDB Accelerator ク	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	

カテゴリ	内容	タグ	規約	例	備考
	サブネットグループ	設定不可	-	-	
	パラメータグループ	設定不可	-	-	
ElastiCache	クラスタ名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	サブネットグループ名	設定不可	-	-	
	パラメータグループ名	設定不可	-	-	
DMS	タスク名	設定不可	-	-	
	エンドポイント名	設定不可	-	-	
	サブネットグループ識別子	設定不可	-	-	
	イベントサブスクリプション名	設定不可	-	-	
CloudWatch	アラーム名	設定不可	-	-	
	ルール名	設定不可	-	-	
	ロググループ名	設定不可	-	-	
	ログストリーム名	設定不可	-	-	
	フィルタの名前	設定不可	-	-	
	メトリクスの名前空間	設定不可	-	-	
	メトリクス名	設定不可	-	-	
	ダッシュボード名	設定不可	-	-	
SystemsManager	メンテナンスウィンドウ名	設定不可	-	-	
	タスク名	設定不可	-	-	
	ターゲット名	設定不可	-	-	
	パラメータストア名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	インベントリ名	設定不可	-	-	
Lambda	関数	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
APIGateway	API	設定不可	-	-	
CloudFormation	スタック	設定不可	-	-	
	スタックセット	設定不可	-	-	
CloudTrail	証跡名	設定不可	-	-	
Config	ルール名（マネージドルール）	設定不可	-	-	
	ルール名（カスタムルール）	設定不可	-	-	
	アグリゲータ名	設定不可	-	-	
Athena	データベース名	設定不可	-	-	
OpenSearch	ドメイン	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Kinesis	ストリーム	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Glue	テーブル名	設定不可	-	-	
	接続名	設定不可	-	-	
	クローラ名	設定不可	-	-	
	分類子名	設定不可	-	-	
	ジョブ名	設定不可	-	-	
	トリガー名	設定不可	-	-	
	開発エンドポイント名	設定不可	-	-	
	セキュリティ設定名	設定不可	-	-	
StepFunctions	ステートマシン名	設定不可	-	-	
	アクティビティ名	設定不可	-	-	
SNS	トピック名	設定不可	-	-	
	表示名	設定不可	-	-	
	アプリケーション名	設定不可	-	-	
SQS	キュー名	Name	規約設計を参照	規約設計を参照	
QuickSight	パラメータ名	設定不可	-	-	
CodeCommit	リポジトリ名	設定不可	-	-	
CodeBuild	プロジェクト名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
CodePipeline	パイプライン名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
CodeBuild	アプリケーション名	設定不可	-	-	
	デプロイグループ名	設定不可	-	-	
	デプロイ設定名	設定不可	-	-	
DataPipeline	パイプライン名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
ECS	クラスター名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	タスク定義名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	サービス名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	

カテゴリ	内容	タグ	規約	例	備考
		SubSystem	{サブシステムコード}	xq	
AWS Backup	バックアッププラン名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	Organizationsを利用する場合は省略可 prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	ルール名	設定不可	-	-	
	バックアップボールト名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	ルール名	設定不可	-	-	
	サービス名	設定不可	-	-	
Cloud9	名前	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
SecurityHub	アクション名	設定不可	-	-	
AccessAnalyzer	アナライザー名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	アーカイブルール名	設定不可	-	-	
Inspector	評価ターゲット名	設定不可	-	-	
	評価テンプレート名	設定不可	-	-	
KMS	カスタマー管理型のキーエイリア	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
EventBridge	名前	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
CertificateManager	名前	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
CloudFront	名前	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	cache policy	設定不可	-	-	
	関数	設定不可	-	-	
Route53	ドメイン名	Name	規約は設定しない	-	ドメイン名は農水省担当者と相談の上決定するこ
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	apn1	apn1／apn3
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
WAF	web ACL	設定不可	-	-	
	IP set	設定不可	-	-	
	rule group	設定不可	-	-	
	Regex pattern sets	設定不可	-	-	
Lex	ボット	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	環境ごとにエイリアスを作成する場合は設定不要 prod／test／stg／dev
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	インテント	設定不可	-	-	
	スロットタイプ	設定不可	-	-	
	チャネル	設定不可	-	-	
	エイリアス	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	

2.AWS 規約設計 規約一覧

前提
・本規約は、各リソースのリソース名（Nameタグ）の記載ルールを定義する。
・改定により更新された命名規約については、遡って適用しない。
・リソース名の値は規約にあわせて英数字もしくはハイフン（-）で記載する。日本語のローマ字書きではなく英訳を記載すること。
・{本番／検証／ステージング／開発}については、prod／test／stg／devを代入する。必要な環境のみを作成し、不必要なものは作成しないこと。
・{サブシステムコード}については、システムに複数のサブシステムを内包している場合に各システムにて決定する。サブシステムがない場合は省略可能。例（E列）に示す"xt"や"nf"はサブシステムコードの一例である。
・{リージョン}については、ap-northeast-1（東京）を利用する場合にはapn1、ap-northeast-3（大阪）を利用する場合にはapn3を設定する。
・{システム略称}については、農林水産省クラウド共通機能利用申請書の「システム略称（英小文字/数字20字以内）」欄に記載したものを設定する。
・本規約に記載されていないサービスについては、定義済の規約を参照しリソース名を設定すること。

カテゴリ	内容	規約	例	備考
IAM	USER	{名の先頭小文字}{姓のフル小文字} ・システム用IAMユーザ名 sysuser-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{任意文字列（用途）}	thibiya sysuser-A008263-xq-test-{任意文字列（用途）}	
	Group	group-{システムコード（7桁）}-{サブシステムコード}-{任意文字列}	group-A008263-nf-{任意文字列}	
	Role	role-{任意文字列}	role-{任意文字列}	
	Policy	policy-{任意文字列}	policy-{任意文字列}	
VPC	VPC	vpc-{任意文字列}	vpc-{任意文字列}	
	subnet	sub-{連番2桁}-{public/private}-{availability-zone}-{任意文字列}	sub-01-public-a-{任意文字列} sub-01-public-c-{任意文字列} sub-01-private-a-{任意文字列} sub-01-private-c-{任意文字列}	
	RouteTable	route-{連番2桁}-{public/private}-{availability-zone}-{任意文字列}	route-01-public-a-{任意文字列} route-01-public-c-{任意文字列} route-01-private-a-{任意文字列} route-01-private-c-{任意文字列}	
	DHCPオプションセット	dhcpoption-{任意文字列}	dhcpoption-{任意文字列}	
	VPCピアリング	peer-{VPC名}-{対向先VPC名}	peer-vpc-{任意文字列}-vpc-{任意文字列}	
	InternetGateway	igw-{任意文字列}	igw-{任意文字列}	
	VPNGateway	vgw-{任意文字列}	vgw-{任意文字列}	
	CustomerGateway	cgw-{任意文字列}	cgw-{任意文字列}	
	NATGateway	natgw-{availability-zone}-{任意文字列}	natgw-a-{任意文字列} natgw-c-{任意文字列}	
	VPCEndpoint	vpce-{サービス名}-{任意文字列}	vpce-s3-{任意文字列} vpce-ssm-{任意文字列} vpce-ec2-{任意文字列}	
	ElasticIP	eip-{任意文字列}	eip-{任意文字列}	
	NetworkFirewall ファイアウォール	nfw-{任意文字列}	nfw-{任意文字列}	
	NetworkFirewall ファイアウォールポリシー	nfw-policy-{任意文字列}	nfw-policy-{任意文字列}	
	NetworkFirewall ルールグループ	nfw-rule-group-{任意文字列}	nfw-rule-group-{任意文字列}	
EC2	Nameタグ	{任意文字列（サーバー名）}	{任意文字列（サーバー名）}	
	AMI名	ami-{任意文字列（サーバー名）}-{yyyymmddhhmm}	ami-{任意文字列（サーバー名）}-201805281418	
	Snapshot名	ss-{任意文字列（サーバー名）}-{volume名}-{yyyymmddhhmm}	ss-{任意文字列（サーバー名）}-vol01-201805281418	
	KeyPair名	規約は作成しない	-	
	起動テンプレート名	ec2-lt-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	ec2-lt-A008263-nf-prod-apn1-{任意文字列}	
EBS	Nameタグ	ebs-{任意文字列（サーバー名）}-{任意文字列}	ebs-{任意文字列（サーバー名）}-01	
ENI	Nameタグ	eni-{任意文字列（サーバー名）}-{任意文字列}	eni-{任意文字列（サーバー名）}-01	
Security Group	Group名	secg-{任意文字列}	secg-{任意文字列}	
	Nameタグ	・EC2 EC2名と同様：{任意文字列（サーバー名）} ・その他 Group名と同様：secg-{任意文字列} ※同じ用途の複数のEC2に同一のSecurity Groupを適用する場合等	secg-{任意文字列（サーバーの種類）} secg-web secg-api	
S3	バケット名	s3-{任意文字列}	s3-{任意文字列}	
	イベント名	s3-event-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	s3-event-A008263-nf-prod-apn1-{任意文字列}	
	ライフサイクルルール名	s3-lc-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	s3-lc-A008263-nf-prod-apn1-{任意文字列}	
	ストレージクラス分析名	s3-sc-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	s3-sc-A008263-nf-prod-apn1-{任意文字列}	
	メトリクスフィルタ名	s3-metrics-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	s3-metrics-A008263-nf-prod-apn1-{任意文字列}	
	インベントリ名	s3-inventory-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	s3-inventory-A008263-nf-prod-apn1-{任意文字列}	
EFS	Nameタグ	efs-{任意文字列}	efs-{任意文字列}	
Glacier	ボールト名	glacier-{任意文字列}	glacier-{任意文字列}	
Redshift	クラスター名	rs-{任意文字列}	rs-{任意文字列}	
	データベース名	{本番／検証／ステージング／開発}{システムコード（7桁）}{サブシステムコード}{リージョン}{連番3桁 or all}	prodA008263nfapn1all	データベースが1つの場合は連番は「all」
	Snapshot名	ss-{クラスター名}-{yyyymmddhhmm}	ss-rs-{任意文字列}-201805281418	
	クラスターパラメータグループ名	rs-parameter-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	rs-parameter-A008263-nf-prod-apn1-01	
	イベントサブスクリプション名	rs-subscription-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	rs-subscription-A008263-nf-prod-apn1-01	
ELB	ロードバランサー名	{clb／alb／nlb}-{任意文字列}	clb-{任意文字列} alb-{任意文字列} nlb-{任意文字列}	
	Nameタグ	ロードバランサー名と同様	-	
	ターゲットグループ名	elb-tg-{ロードバランサー名}-{任意文字列}	elb-tg-clb-{任意文字列}-{任意文字列} elb-tg-alb-{任意文字列}-{任意文字列} elb-tg-nlb-{任意文字列}-{任意文字列}	
AutoScaling	起動設定名	as-lc-EC2名-{任意文字列}	as-lc-{任意文字列（サーバー名）}-{任意文字列}	
	グループ名	as-asg-EC2名-{任意文字列}	as-asg-{任意文字列（サーバー名）}-{任意文字列}	
	Nameタグ	グループ名と同様	-	
	スケールポリシー名	as-sp-{グループ名}-{用途}	as-sp-as-asg-{任意文字列（サーバー名）}-{任意文字列}-scaleout as-sp-as-asg-{任意文字列（サーバー名）}-{任意文字列}-scalein	
	ライフサイクルフック名	as-lch-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-EC2名-{任意文字列}	as-lch-A008263-xt-prod-apn1-{任意文字列（サーバー名）}-01	
RDS / Aurora	DBインスタンス識別子	rds-{任意文字列}	rds-{任意文字列}	
	DBサブネットグループ名	rds-sub-{任意文字列}	rds-sub-{任意文字列}	
	データベース名	{本番／検証／ステージング／開発}{システムコード（7桁）}{サブシステムコード}{リージョン}{連番3桁 or all}	prodA008263nfapn1001	データベースが1つの場合は連番は「all」
	データベース名（Oracle）	規約は作成しない	-	デフォルトはORCL、最大８文字
	DBクラスター 識別子	rds-cluster-{任意文字列}	rds-cluster-{任意文字列}	Auroraのみ
	DBパラメータグループ名	rds-parameter-{任意文字列}	rds-parameter-{任意文字列}	
	DBオプショングループ名	rds-option-{任意文字列}	rds-option-{任意文字列}	
	DBスナップショット名	ss-{DBインスタンス識別子}-{yyyymmddhhmm}	ss-rds-{任意文字列}-201808021446	
	サブスクリプション名	rds-subscription-{DBインスタンス識別子 or DBクラスター識別子 or all}-{イベント名 or all}	rds-subscription-rds-{任意文字列}-all rds-subscription-rds-cluster-{任意文字列}-all	通知するイベント内容が把握できるように、対象とイベント名を明記
DynamoDB	テーブル名	dynamo-{任意文字列}	dynamo-{任意文字列}	
	バックアップ名	dynamo-bk-{テーブル名}-{yyyymmddhhmm}	dynamo-bk-dynamo-{任意文字列}-201808311015	

カテゴリ	内容	規約	例	備考
	DynamoDB Accelerator クラスタ名	dynamo-cl-{連番2桁}-{任意文字列}	dynamo-cl-01-{任意文字列}	最大20文字
	サブネットグループ名	dynamo-subnet-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	dynamo-subnet-A008263-xt-prod-apn1-{任意文字列}	
	パラメータグループ名	dynamo-parameter-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	dynamo-parameter-A008263-xt-prod-apn1-{任意文字列}	
ElastiCache	クラスタ名	ec-{任意文字列}	ec-{任意文字列}	最大20文字
	サブネットグループ名	ec-subnet-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	ec-subnet-A008263-xt-prod-apn1-{任意文字列}	
	パラメータグループ名	ec-parameter-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	ec-parameter-A008263-xt-prod-apn1-{任意文字列}	
DMS	タスク名	dms-task-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	dms-task-A008263-xt-prod-apn1-{任意文字列}	
	エンドポイント名	dms-endpoint-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	dms-endpoint-A008263-xt-prod-apn1-{任意文字列}	
	サブネットグループ識別子	dms-subnet-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	dms-subnet-A008263-xt-prod-apn1-{任意文字列}	
	イベントサブスクリプション名	dms-subscription-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	dms-subscription-A008263-xt-prod-apn1-{任意文字列}	
CloudWatch	アラーム名	cw-alarm-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{メトリクス名}-{監視対象}	cw-alarm-A008263-nf-prod-apn1-StatusCheckFailed_Instance-{監視対象}	アラート名から状況を把握できるようメトリクス名、監視対象を明記
	ルール名	cw-rule-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{ターゲット}-{ターゲット名}	cw-rule-A008263-nf-prod-apn1-lambda-EC2_backup	EventBridgeにサービス変更されたため規約廃止
	ロググループ名	規約は作成しない	-	
	ログストリーム名	規約は作成しない	-	
	フィルタの名前	規約は作成しない	-	
	メトリクスの名前空間	規約は作成しない	-	
	メトリクス名	規約は作成しない	-	
	ダッシュボード名	cw-dashboard-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{用途}	cw-dashboard-A008263-nf-prod-apn1-webserver	
SystemsManager	メンテナンスウィンドウ名	ssm-mw-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	ssm-mw-A008263-xt-prod-apn1-{任意文字列}	
	タスク名	ssm-task-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	ssm-task-A008263-xt-prod-apn1-{任意文字列}	
	ターゲット名	ssm-target-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	ssm-target-A008263-xt-prod-apn1-{任意文字列}	
	パラメータストア名	parameter-store-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	parameter-store-A008263-xt-prod-apn1-{任意文字列}	プレフィクスに「aws」や「ssm」は指定できない
	インベントリ名	ssm-inventory-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	ssm-inventory-A008263-xt-prod-apn1-{任意文字列}	
Lambda	関数名	lambda-{任意文字列}	lambda-{任意文字列}	
APIGateway	API名	apigw-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	apigw-A008263-xt-prod-apn1-{任意文字列}	
	ステージ名	{本番／検証／ステージング／開発}-{リージョン}-{連番2桁}	prod-apn1-01 test-apn1-01 dev-apn1-01	
	オーソライザー名	apigw-auth-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	apigw-auth-A008263-xt-prod-apn1-{任意文字列}	
	モデル名	規約は作成しない	-	
	使用料プラン名	apigw-plan-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	apigw-plan-A008263-xt-prod-apn1-{任意文字列}	
	APIキー名	apigw-key-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	apigw-key-A008263-xt-prod-apn1-{任意文字列}	
	VPCリンク名	apigw-vpclink-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	apigw-vpclink-A008263-xt-prod-apn1-{任意文字列}	
CloudFormation	スタック名	cfn-stack-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{任意文字	cfn-stack-A008263-xt-prod-{任意文字列}	
	スタックセット名	cfn-stacksets-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{任意文字列}	cfn-stacksets-A008263-xt-prod-{任意文字列}	
	テンプレート名	cfn-template-{システムコード（7桁）}-{サブシステムコード}-{任意文字列}	cfn-template-A008263-xt-{任意文字列}	AWSリソースではないものの、判別しやすくするため定義しておく。
	対象アカウントIDの一覧（csv）	cfn-stacksets-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{任意文字列}.csv	cfn-stacksets-A008263-xt-prod-{任意文字列}.csv	AWSリソースではないものの、判別しやすくするため定義しておく。
Budgets	予算名	budgets-{任意文字列}	budgets-{任意文字列}	
CloudTrail	証跡名	traillog-{s3バケット名}	traillog-s3-{任意文字列}	
Config	ルール名（マネージドルール）	マネージドルール名をそのまま設定	iam-password-policy	
	ルール名（カスタムルール）	規約は作成しない	-	対象のサービスおよび検査内容がわかるように命名する
	アグリゲータ名	config-aggregator-{接続先アカウント（数字12桁）}-{リージョン}	config-aggregator-111111111111-apn1	
Athena	データベース名	{本番／検証／ステージング／開発}{システムコード（7桁）}{サブシステムコード}{リージョン}{連番3桁 or all}	prodA008263nfapn1001	データベースが1つの場合は連番は「all」
	クエリ名	athena-query-{任意文字列}	athena-query-{任意文字列}	
OpenSearch	ドメイン名	os-{任意文字列}	os-{任意文字列}	最大28文字
Kinesis	ストリーム名	kinesis-stream-{任意文字列}	kinesis-stream-{任意文字列}	
Glue	テーブル名	glue_table_{システムコード（7桁）}-{サブシステムコード}_{本番／検証／ステージング／開発}_{リージョン}_{任意文字列}	glue_table_A008263_xt_prod_apn1_{任意文字列}	Glueを利用したシステムにてエラーが発生したため、「-」ではなく「_」を利用
	接続名	glue-connect-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	glue-connect-A008263-xt-prod-apn1-{任意文字列}	
	クローラ名	glue-crawler-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	glue-crawler-A008263-xt-prod-apn1-{任意文字列}	
	分類子名	glue-classfier-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	glue-classfier-A008263-xt-prod-apn1-{任意文字列}	
	ジョブ名	glue-job-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	glue-job-A008263-xt-prod-apn1-{任意文字列}	
	トリガー名	glue-trigger-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	glue-trigger-A008263-xt-prod-apn1-{任意文字列}	
	開発エンドポイント名	glue-endpoint-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	glue-endpoint-A008263-xt-prod-apn1-{任意文字列}	
	セキュリティ設定名	glue-security-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	glue-security-A008263-xt-prod-apn1-{任意文字列}	
StepFunctions	ステートマシン名	step-state-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	step-state-A008263-xt-prod-apn1-{任意文字列}	
	アクティビティ名	step-activity-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	step-activity-A008263-xt-prod-apn1-{任意文字列}	
SNS	トピック名	sns-topic-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	sns-topic-A008263-xt-prod-apn1-{任意文字列}	
	表示名	規約は作成しない	-	
	アプリケーション名	sns-app-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	sns-app-A008263-xt-prod-apn1-{任意文字列}	
SQS	キュー名	sqs-{任意文字列}	sqs-{任意文字列}	
QuickSight	パラメータ名	規約は作成しない	-	
CodeCommit	リポジトリ名	commit-{システムコード（7桁）}-{サブシステムコード}-{リージョン}-{任意文字列}	commit-A008263-xt-apn1-{任意文字列}	本番、機能検証、性能検証、開発でリポジトリは共用
CodeBuild	プロジェクト名	build-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	build-A008263-xt-test-apn1-{任意文字列}	
CodePipeline	パイプライン名	pipeline-{任意文字列}	pipeline-{任意文字列}	
CodeDeploy	アプリケーション名	deploy-app-{任意文字列}	deploy-app-{任意文字列}	
	デプロイグループ名	deploy-depgrp-{任意文字列}	deploy-depgrp-{任意文字列}	
	デプロイ設定名	deploy-depconfig-{任意文字列}	deploy-depconfig-{任意文字列}	
DataPipeline	パイプライン名	datapipeline-{任意文字列}	datapipeline-{任意文字列}	
ECS	クラスター名	ecs-cluster-{任意文字列}	ecs-cluster-{任意文字列}	
	タスク定義名	ecs-task-{任意文字列}	ecs-task-{任意文字列}	
	サービス名	ecs-service-{任意文字列}	ecs-service-{任意文字列}	
AWS backup	バックアッププラン名	backup-plan-{任意文字列}	backup-plan-{任意文字列}	
	ルール名	backup-rule-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{任意文	backup-rule-A008263-xt-test-{任意文字	
	バックアップボールト名	backup-vault-{任意文字列}	backup-vault-{任意文字列}	
	ポリシー名	backup-policy-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{任意文字列}	backup-policy-A008263-xt-test-{任意文字列}	

カテゴリ	内容	規約	例	備考
	リソース割り当て名	backup-resource-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{任意文字列}	backup-resource-A008263-xt-test-{任意文字列}	
	バックアップされたリソース名	タグ設計や規約設計に沿わないことを許容する。（AWS Backup側で自動で定義されるため） 例ではEC2をリソースに割り当ててAMIを作成した場合に作成されるAMI名を示す。	AwsBackup_＜インスタンスID＞	
Cloud9	名前	cloud9-{任意文字列}	cloud9-{任意文字列}	本番、機能検証、性能検証、開発でポジトリは共用
SecurityHub	アクション名	sec-custom-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{任意文字列}	sec-custom-A008263-xt-prod-{任意文字列}	本番、機能検証、性能検証、開発でポジトリは共用
AccessAnalyzer	アナライザー名	iam-aa-analyzer-{任意文字列}	iam-aa-analyzer-{任意文字列}	
	アーカイブルール名	iam-aa-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-rule-{任意文	iam-aa-A008263-xt-test-rule-{任意文字	
Inspector	評価ターゲット名	inspector-target-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	inspector-target-A008263-xt-test-apn1-{任意文字列}	
	評価テンプレート名	inspector-template-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	inspector-template-A008263-xt-test-apn1-{任意文字列}	
KMS	カスタマー管理型のキーエイリアス	kms-cmk-{任意文字列}	kms-cmk-{任意文字列}	本番、機能検証、性能検証、開発でポジトリは共用
EventBridge	ルール名	bridge-{任意文字列}	bridge-{任意文字列}	
CertificateManager	名前	acm-{任意文字列}	bridge-{任意文字列}	
CloudFront	名前	cfront-{任意文字列}	cfront-{任意文字列}	
	cache policy	cfront-cache-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{任意文字列}	cfront-cache-A008263-xt-prod-{任意文字列}	
	関数名	cfront-function-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{任意文字列}	cfront-function-A008263-xt-prod-{任意文字列}	
Route 53	ドメイン名	規約は作成しない	-	ドメイン名は農水省担当者と相談の上決定すること
WAF	web ACL	waf-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	waf-A008263-xt-prod-apn1-{任意文字列}	CloudFrontにアタッチする場合はリージョン名を「cfront」にする
	IP set	waf-ip-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	waf-ip-A008263-xt-prod-cfront-{任意文字列}	
	rule group	waf-rule-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	waf-rule-A008263-xt-prod-apn1-{任意文字列}	
	Regex pattern sets	waf-regex-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	waf-regex-A008263-xt-prod-apn1-{任意文字列}	
Lex	ボット名	lex-bot-{任意文字列}	lex-bot-{任意文字列}	
	インテント	lex-intent-{ボット名}-{任意文字列}	lex-intent-lex-bot-{任意文字列}-{任意文字列}	
	スロットタイプ	lex-slot-{ボット名}-{任意文字列}	lex-slot-lex-bot-{任意文字列}-{任意文字	
	チャネル	lex-channel-{ボット名}-{任意文字列}	lex-channel-lex-bot-{任意文字列}-{任意文字列}	
	エイリアス	lex-alias-{ボット名}-{任意文字列}	lex-alias-lex-bot-{任意文字列}-{任意文字	

3.Azure タグ設計 タグ一覧

前提
・本規約は、各リソースに設定するタグの記載ルールを定義する。
・改定により更新された規約については、原則遡って適用しない。
・タグの値は規約設計にあわせて英小文字もしくは数字で記載する。日本語のローマ字書きではなく英訳を記載すること。
・{本番／検証／ステージング／開発}については、prod／test／stg／devを代入する。必要な環境のみを作成し、不必要なものは作成しないこと。
・{サブシステムコード}については、システムに複数のサブシステムを内包している場合に各システムにて決定する。サブシステムがない場合、「SubSystem」のタグは設定不要。
・{リージョン}については、東日本を利用する場合にはjpe、西日本を利用する場合にはjpwを設定する。
・{システム略称}については、農林水産省クラウド共通機能利用申請書の「システム略称（英小文字/数字20字以内）」欄に記載したものを設定する。
・本規約に記載されていないサービスについては、定義済の規約を参照しタグを設定すること。
・個別システムにて必要があれば本規約に記載されていないタグについても追加可能。

カテゴリ	内容	タグ	規約	例	備考
サブスクリプション	サブスクリプション	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod-test	prod／test／stg／dev 同サブスクリプションで複数の環境を利用する場合は、ハイフンで繋げて記載する
		Region	{リージョン}	jpe-jpw	同サブスクリプションで複数のリージョンを利用する場合は、ハイフンで繋げて記載する
		SubSystem	{サブシステムコード}	xq	
Active Directory	名前	設定不可	-	-	
	ユーザー名	設定不可	-	-	
	グループ	設定不可	-	-	
	カスタムロール	設定不可	-	-	
	管理単位	設定不可	-	-	
	カスタムドメイン	設定不可	-	-	
	ディレクトリ	設定不可	-	-	
管理グループ	管理グループID	設定不可	-	-	
	管理グループ表示名	設定不可	-	-	
	子管理グループID	設定不可	-	-	
	子管理グループ表示名	設定不可	-	-	
リソースグループ	リソースグループ	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	予算	設定不可	-	-	
仮想ネットワーク	仮想ネットワーク	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	サブネット	設定不可	-	-	
	ピアリング リンク	設定不可	-	-	
パブリックIPアドレス	パブリックIPアドレス	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
パブリックIPプレフィックス	パブリックIPプレフィックス	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
仮想ネットワークゲートウェイ	名前（VPN）	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	IPアドレス名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	接続	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
NATゲートウェイ	NAT ゲートウェイ名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
アプリケーションゲートウェイ	ゲートウェイ名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	バックエンドプール	設定不可	-	-	
	ルーティングルール	設定不可	-	-	
	リスナー	設定不可	-	-	
	HTTP設定	設定不可	-	-	
ネットワークセキュリティグループ	ネットワークセキュリティグループ	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	受信セキュリティ規則	設定不可	-	-	
	送信セキュリティ規則	設定不可	-	-	
ルートテーブル	ルートテーブル	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	ルート	設定不可	-	-	
Private Link	プライベートエンドポイント	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	

カテゴリ	内容	タグ	規約	例	備考
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
ファイアウォール	インスタンス名	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	ポリシー名	設定不可	-	-	
Virtual Machines	Virtual Machines	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	キーの組名	設定不可	-	-	
	キャプチャイメージ名	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	ブック名	設定不可	-	-	
ディスク	ディスク	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	スナップショット名	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
ストレージアカウント	ストレージアカウント	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	BLOBコンテナー	設定不可	-	-	
	BLOBインベントリ	設定不可	-	-	
ストレージアカウント	ライフサイクル管理	cm-{任意文字列	-	-	
	メトリクスフィルタ名	設定不可	-	-	
	ブック名	設定不可	-	-	
Azure NetApp Files	NetApp アカウント	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	容量プール	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	ボリューム	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Load balancer	ロードバランサー	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	フロントエンドIP名	設定不可	-	-	
	バックエンドプール名	設定不可	-	-	
	負荷分散規則名	設定不可	-	-	
	インバウンド NAT 規則名	設定不可	-	-	
	アウトバウンド規則名	設定不可	-	-	
	キーの組名	設定不可	-	-	
Database for PostgreSQL	PostgreSQLサーバー名	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	レプリカ名	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Azure Database for	サーバー名	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	レプリカ名	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
SQL データベース	データベース	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	同期グループ名	設定不可	-	-	
SQL サーバー	サーバー	Name	規約設計書を参照	規約設計書を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	

カテゴリ	内容	タグ	規約	例	備考
		SubSystem	{サブシステムコード}	xq	
	ロック	設定不可	-	-	
	フェールオーバーグループ名	設定不可	-	-	
モニター	アラートルール	設定不可	-	-	
	アプリケーション	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	データ収集ルール	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	Private Link スコープ	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Event Grid	イベントサブスクリプション	設定不可	-	-	
	システムトピック	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	トピック	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	ドメイン	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
セキュリティセンター	ブック名	設定不可	-	-	
ポリシー	イベント	設定不可	-	-	
	ポリシー定義	設定不可	-	-	
	イニシアティブ定義	設定不可	-	-	
	グループ名	設定不可	-	-	
	イニシアティブパラメータ名	設定不可	-	-	
	イニシアティブパラメータ表示名	設定不可	-	-	
	割り当て名	設定不可	-	-	
App Service	webアプリ	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	FTP/デプロイ ユーザー名	設定不可	-	-	
	スロット	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Azure Cache for Redis	DNS	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Azure 関数アプリ	関数アプリ	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	関数	設定不可	-	-	
データ ファクトリ	データファクトリ名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Kubernetes サービス	Kubernetes クラスター名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	ノードプール名	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Traffic Manager プロファイル	プロファイル	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	エンドポイント	設定不可	-	-	
コンテナレジストリ	コンテナレジストリ	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	イベントサブスクリプション	設定不可	-	-	
キー コンテナー	キー コンテナー	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	

カテゴリ	内容	タグ	規約	例	備考
		SubSystem	{サブシステムコード}	xq	
	イベントサブスクリプション	設定不可	-	-	
	キー	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	シークレット	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	証明書	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Log Analytics ワークスペース	Log Analytics ワークスペース	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
Azure Sentinel	ブック名	設定不可	-	-	
	カスタムクエリ	設定不可	-	-	
	分析	設定不可	-	-	
	ウォッチリスト名	設定不可	-	-	
	ウォッチリストエイリアス	設定不可	-	-	
	オートメーションルール	設定不可	-	-	
Application Insights	Application Insights	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
	可用性テスト	設定不可	-	-	
	コーホート	設定不可	-	-	
Recovery Services コンテ	Recovery Services コンテ	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
可用性セット	可用性セット	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
DDoS 保護プラン	DDoS 保護プラン	Name	規約設計を参照	規約設計を参照	
		Environment	{本番／検証／ステージング／開発}	prod	prod／test／stg／dev
		Region	{リージョン}	jpe	
		SystemName	{システム略称}	maffcloud	
		SystemCode	{システムコード}	a022621	
		SubSystem	{サブシステムコード}	xq	
カテゴリ共通	ロック	設定不可	-	-	

4.Azure_規約設計_規約一覧

前提
・本規約は、各リソースのリソース名（Nameタグ）の記載ルールを定義する。
・改定により更新された命名規約については、遡って適用しない。
・リソース名の値は規約にあわせて英数字もしくはハイフン（-）で記載する。日本語のローマ字書きではなく英訳を記載すること。
・{本番／検証／ステージング／開発}については、prod／test／stg／devを代入する。必要な環境のみを作成し、不必要なものは作成しないこと。
・{サブシステムコード}については、システムに複数のサブシステムを内包している場合に各システムにて決定する。サブシステムがない場合は省略可能。例（E列）に示す"xt"や"nf"はサブシステムコードの一例である。
・{リージョン}については、東日本を利用する場合にはjpe、西日本を利用する場合にはjpwを設定する。
・{システム略称}については、農林水産省クラウド共通機能利用申請書の「システム略称（英小文字/数字20字以内）」欄に記載したものを設定する。
・本規約に記載されていないサービスについては、定義済の規約を参照しリソース名を設定すること。

カテゴリ	内容	規約	例	備考
サブスクリプション	サブスクリプション名	SUB-{システムコード（7桁）}-{システム略称}	SUB-A008263-yakujihoudaityou	
Azure Active Directory	名前	{名の先頭小文字}{姓のフル小文字}	thibiya	
	ユーザー名	・作成の場合 {名の先頭小文字}{姓のフル小文字}@azcloud.maff.go.jp ・招待の場合 規約は作成しない	thibiya@azcloud.maff.go.jp	
	グループ	group-{システムコード（7桁）}-{サブシステムコード}-{任意文字列}	group-A008263-nf-{任意文字列}	
	カスタムロール	role-{任意文字列}	role-{任意文字列}	
	管理単位	au-{任意文字列}	au-{任意文字列}	
	カスタムドメイン	規約は作成しない	-	
	ディレクトリ	規約は作成しない	-	
管理グループ	管理グループID	mg-{システムコード（7桁）}-{サブシステムコード}-{任意文字列}	mg-A008263-nf-{任意文字列}	
	管理グループ表示名	規約は作成しない	-	
	子管理グループID	{任意文字列（親管理グループID）}-{任意文字列}	mg-A008263-nf-{任意文字列}-{任意文字	
	子管理グループ表示名	規約は作成しない	-	
リソースグループ	リソースグループ	rg-{任意文字列}	rg-{任意文字列}	
	予算	規約は作成しない	-	
仮想ネットワーク	仮想ネットワーク	vnet-{任意文字列}	vnet-{任意文字列}	
	サブネット	sub-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意	sub-A008263-nf-prod-jpe-{任意文字列}	
	ピアリング リンク	・ピアリング元仮想ネットワーク pl-{仮想ネットワーク名}-{対向先仮想ネットワーク名} ・ピアリング先仮想ネットワーク pl-{対向先仮想ネットワーク名}-{仮想ネットワーク名}	pl-vnet-{任意文字列}-vnet-{任意文字列}	
パブリックIPアドレス	パブリックIPアドレス名	pip-{任意文字列}	pip-{任意文字列}	
パブリックIPプレフィックス	パブリックIPプレフィックス名	ippre-{任意文字列}	ippre-{任意文字列}	
仮想ネットワークゲートウェイ	名前（VPN）	vgw-vpn-{任意文字列}	vgw-vpn-{任意文字列}	
	IPアドレス名	vgw-ip-{任意文字列}	vgw-ip-{任意文字列}	
	接続	vgw-con-{任意文字列}	vgw-con-{任意文字列}	
NATゲートウェイ	NAT ゲートウェイ名	ng-{任意文字列}	ng-{任意文字列}	
アプリケーションゲートウェイ	ゲートウェイ名	agw-{任意文字列}	agw-{任意文字列}	
	バックエンドプール	agw-bep-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	agw-bep-A008263-nf-prod-apn1-{任意文字列}	
	ルーティングルール	agw-rule-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	agw-rule-A008263-nf-prod-apn1-{任意文字列}	
	リスナー	規約は作成しない	-	
	HTTP設定	規約は作成しない	-	
ネットワークセキュリティグループ	ネットワークセキュリティグループ	nsg-{任意文字列}	nsg-{任意文字列}	
	受信セキュリティ規則	規約は作成しない	-	
	送信セキュリティ規則	規約は作成しない	-	
ルートテーブル	ルートテーブル	route-rt-{任意文字列}	route-rt-{任意文字列}	
	ルート	route-rn-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	route-rn-A008263-nf-prod-jpe-{任意文字列}	
Private Link	プライベートエンドポイント	pe-{任意文字列}	pe-{任意文字列}	
ファイアウォール	インスタンス名	afw-{任意文字列}	afw-{任意文字列}	
	ポリシー名	afwp-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	afwp-A008263-nf-prod-jpe-{任意文字列}	
Virtual Machines	Virtual Machines	{任意文字列（サーバー名）}	{任意文字列（サーバー名）}	
	キーの組名	規約は作成しない	-	
	キャプチャイメージ名	image-{任意文字列（サーバー名）}-{yyyymmddhhmm}	image-{任意文字列（サーバー名）}-202101011111	
	ブック名	規約は作成しない	-	
ディスク	ディスク	disk-{任意文字列}	disk-{任意文字列}	
	スナップショット名	ss-{任意文字列（サーバー名）}-{ディスク名}-{yyyymmddhhmm}	ss-{任意文字列（サーバー名）}-disk-{任意文字列}-202101011111	
ストレージアカウント	ストレージアカウント	st{任意文字列}	st{任意文字列}	ハイフンは入力不可
	BLOBコンテナー	blob-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	blob-A008263-nf-prod-jpe-{任意文字列}	
	BLOBインベントリ	blob-inventory-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	blob-inventory-A008263-nf-prod-jpe-{任意文字列}	
	ライフサイクル管理	blob-lc-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	blob-inventory-A008263-nf-prod-jpe-{任意文字列}	
	メトリクスフィルタ名	st-metrics-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	st-metrics-A008263-nf-prod-jpe-{任意文字列}	
	ブック名	規約は作成しない	-	
Azure NetApp Files	NetApp アカウント	anf-{任意文字列}	anf-{任意文字列}	
	容量プール	cap-{任意文字列}	cap-{任意文字列}	
	ボリューム	vol-{任意文字列}	vol-{任意文字列}	
Load balancer	ロードバランサー名	・内部 lbi-{任意文字列} ・外部 lbe-{任意文字列}	・内部 lbi-{任意文字列} ・外部 lbe-{任意文字列}	
	フロントエンドIP名	lb-fip-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	lb-fip-A008263-nf-prod-jpe-{任意文字列}	
	バックエンドプール名	lb-bep-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	lb-bep-A008263-nf-prod-jpe-{任意文字列}	
	負荷分散規則名	lb-lbrule-{任意文字列}	lb-lbrule-{任意文字列}	
	インバウンド NAT 規則名	lb-ibrule-{任意文字列}	lb-ibrule-{任意文字列}	
	アウトバウンド規則名	lb-obrule-{任意文字列}	lb-obrule-{任意文字列}	
	キーの組名	規約は作成しない	-	
Database for PostgreSQL	サーバー名	psql-{任意文字列}	psql-{任意文字列}	
	レプリカ名	psql-replica-{マスターとなるPostgreDQLサーバー名}	psql-replica-psql-{任意文字列}	
Azure Database for MySQL	サーバー名	mysql-{任意文字列}	mysql-{任意文字列}	
	レプリカ名	mysql-replica-{マスターとなるMySQLサーバー名}	mysql-replica-mysql-{任意文字列}	

カテゴリ	内容	規約	例	備考
SQL データベース	データベース名	sqldb-{任意文字列}	sqldb-{任意文字列}	
	同期グループ名	sqldb-group-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	sqldb-group-A008263-nf-prod-jpe-{任意文字列}	
SQL サーバー	サーバー名	sqlsv-{任意文字列}	sqlsv-{任意文字列}	
	フェールオーバーグループ名	sqlsv-group-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	sqlsv-group-A008263-nf-prod-jpe-{任意文字列}	
モニター	アラートルール名	monitor-alrule-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	monitor-alrule-{任意文字列}	
	アプリケーション名	monitor-apl-{任意文字列}	monitor-apl-{任意文字列}	
	データ収集ルール名	monitor-dtrule-{任意文字列}	monitor-dtrule-{任意文字列}	
	Private Link スコープ名	monitor-pl-{任意文字列}	monitor-pl-{任意文字列}	
Event Grid	イベントサブスクリプション	evg-subscription-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	evg-subscription-A008263-nf-prod-jpe-{任意文字列}	
	システムトピック名	evg-systopic-{任意文字列}	evg-systopic-{任意文字列}	
	トピック名	evg-topic-{任意文字列}	evg-topic-{任意文字列}	
	ドメイン名	evg-domain-{任意文字列}	evg-domain-{任意文字列}	
セキュリティ センター	ブック名	規約は作成しない	-	
ポリシー	イベント	イベントグリッド システムトピックを参照	-	
	ポリシー定義	policy-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	policy-A008263-nf-prod-jpe-{任意文字列}	規定のポリシーを選択する場合は設定不可
	イニシアティブ定義	ini-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文	ini-A008263-nf-prod-jpe-{任意文字列}	
	グループ名	policy-group-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	policy-group-A008263-nf-prod-jpe-{任意文字列}	
	イニシアティブパラメータ名	規約は作成しない	-	
	イニシアティブパラメータ表示名	ini-param-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	ini-param-A008263-nf-prod-jpe-{任意文字列}	
	割り当て名	ポリシー定義、イニシアティブ定義をそのまま設定	-	
App Service	Webアプリ	as-{任意文字列}	-	
	FTP/デプロイ ユーザー名	as-user-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	-	
	スロット	as-slot-{任意文字列}	as-slot-{任意文字列}	
Azure Cache for Redis	DNS	規約は作成しない	-	ドメイン名は農水省担当者と相談の上決定すること
Azure 関数アプリ	関数アプリ	func-app-{任意文字列}	func-{任意文字列}	
	関数	func-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	func-A008263-nf-prod-jpe-{任意文字列}	
データ ファクトリ	データファクトリ名	df-{任意文字列}	df-{任意文字列}	
Kubernetes サービス	Kubernetes クラスター名	aks-{任意文字列}	aks-{任意文字列}	
	ノードプール名	np{任意文字列}	np{任意文字列}	ハイフン(-)は入力不可。Linuxの場合は英小文字・数字12文字以内、Windowsの場合は英小文字・数字6文字以内。
Traffic Manager プロファイル	プロファイル	traf-{任意文字列}	traf-{任意文字列}	
	エンドポイント	traf-end-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	traf-end-A008263-nf-prod-jpe-{任意文字列}	
コンテナレジストリ	コンテナレジストリ	cr-{任意文字列}	cr-{任意文字列}	
	イベントサブスクリプション	Event Gridカテゴリに記載	-	
キー コンテナー	キーコンテナー	kv-{任意文字列}	kv-{任意文字列}	
	イベントサブスクリプション	Event Gridカテゴリに記載	-	
	キー	kv-key-{任意文字列}	kv-key-{任意文字列}	
	シークレット	kv-sec-{任意文字列}	kv-sec-{任意文字列}	
	証明書	kv-cert-{任意文字列}	kv-cert-{任意文字列}	
Log Analytics ワークスペース	Log Analytics ワークスペース	log-{任意文字列}	log-{任意文字列}	
Azure Sentinel	ブック名	規約は作成しない	-	
	カスタムクエリ	stn-que-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	stn-que-A008263-nf-prod-jpe-{任意文字列}	
	分析	stn-ana-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	stn-ana-A008263-nf-prod-jpe-{任意文字列}	
	ウォッチリスト名	stn-watch-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	stn-watch-A008263-nf-prod-jpe-{任意文字列}	
	ウォッチリストエイリアス	規約は作成しない	-	
	オートメーションルール	stn-auto-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	stn-auto-A008263-nf-prod-jpe-{任意文字列}	
Application Insights	Application Insights	appi-{任意文字列}	appi-{任意文字列}	
	可用性テスト	appi-test-{システムコード（7桁）}-{サブシステムコード}-{本番／検証／ステージング／開発}-{リージョン}-{任意文字列}	appi-test-A008263-nf-prod-jpe-{任意文字列}	
	コーホート	規約は作成しない	-	
Recovery Services コンテナー	Recovery Services コンテナー	rsv-{任意文字列}	rsv-{任意文字列}	
可用性セット	可用性セット名	avail-{任意文字列}	avail-{任意文字列}	
DDoS 保護プラン	DDoS 保護プラン名	ddos-{任意文字列}	ddos-{任意文字列}	
カテゴリ共通	ロック	・読み取り専用 lock-ro-{任意文字列（対象リソース名）} ・削除 lock-cd-{任意文字列（対象リソース名）}	lock-ro-rg-{任意文字列} lock-cd-rg-{任意文字列}	例はリソースグループでロックを設定した場合