令和2年度経済産業省デジタルプラットフォーム構築事業

（Gビズスタックに関するUI・UX向上機能調査）

調査報告書

2021 年 3 月 31 日

株式会社日立社会情報サービス

目次

調査研究状況サマリ

(1) 問合せ対応（チャットボット）

① 各システムのＦＡＱデータを一元的管理できる環境設計

② チャットボットサービスの選定調査

③ ＧビズインフォおよびＧビズＩＤへの導入・実証

(2) システム利用状況の見える化とサービス改善のためのデータ分析環境（ダッシュボード）

① 各システムの稼働状況管理機能および指標調査

② 一元化・分析機能に向けたデータ項目整理

③ 各指標を収集・分析できるサービスおよびツールの選定

④ パフォーマンスＡＰＩのサーバー実装

⑤ 適切なアクセスコントロールの実施

1. 事業の概要

1.1. 本事業の概要

(1) 事業目的

我が国のこれまでの電子政府の取組は、紙や押印の機能を電子上で再現することを所与のものとしてきたが、真のデジタル・ガバメントの実現に向けた取組を推進していくに当たっては、行政サービスの利用者と行政機関間のフロント部分だけでなく、行政機関内のバックオフィスを含めたプロセスについても、技術の進展に応じて、デジタル技術の活用を進めていくことが重要である。この点について、今までは制度・業務ごとに個別システムを構築してきたため、同一ユーザに紐づく申請情報や利用履歴などシステム間の連携が取れておらず、多岐に渡る問合せ対応や横断的なサービス誘導等の観点では、必ずしも利用者・運用管理者双方にとって利便であるとは言えず、改善の余地が多分に存在するところである。

経済産業省では、共通認証基盤のＧビズＩＤ、補助金申請基盤のＪグランツ、オープンデータ基盤のＧビズインフォ、中小企業支援基盤のミラサポプラス、など（以下、「Ｇビズスタック」という）の整備およびシステム間連携を通じて、利用者・運用者双方の立場に立った行政手続きのデジタル化及び省内業務の効率化の双方を実現するための方策検討を実践している。他方、システム間連携が進むにつれて、各サービス窓口に他サービス・システムに関する問合せが寄せられ別窓口に再案内する事案等発生しているが、これらは認知度、ユーザ数、連携サービスが増加するごとに共通課題として拡大し、横断的解決策が必要とされるほか、各システムへの更なる可用性・信頼性も求められるところ、システム間連携での運用に関するユーザーインタフェース・エクスペリエンス（以下、ＵＩ・ＵＸという）の向上が急務となっている。

係る観点から、本事業ではＧビズスタックを対象に、共通機能の一元集約や投資抑制の観点を持ちつつ、各システムのサービス効果の可視化、またユーザに対する訴求力を高めることを目的としたＵＩ・ＵＸ向上に資する機能の要件整理および実証調査を行う。

⑵ 事業概要

Ｇビズスタックのサービス改善および運用管理の一元化を目的とし、以下の項目について各システムのＵＩ・ＵＸ向上機能に関する調査と導入にむけた要件整理を実施した。

(ア) 問合せ対応（チャットボット）

システム間連携に伴った各サービス窓口への他サービス・システムに関する問合せに対する機械的処理として、システム間連携するサービス全体で共通利用可能なチャットボットを導入する。

(イ) システム利用状況の見える化とサービス改善のためのデータ分析環境（ダッシュボード）

Ｇビズスタック（本項目では、ＧビズＩＤ、Ｇビズインフォおよびｊグランツ、ミラサポプラスを対象とする）に関して、稼働状況やサービス改善やピーク予測など施策立案運用の評価・分析を目的として、各システム稼働・運用状況の一元管理やカスタマージャーニーを特定・分析できるダッシュボードと抽出項目等について設計・調査する。

1.2. 事業計画

本事業は 2021 年 1 月（令和 3 年 1 月）より開始され、2021 年 3 月まで実施された。

個々の活動状況は次のとおり

(ア)問合せ対応（チャットボット）

図 1-1 チャットボットスケジュール

(イ)システム利用状況の見える化とサービス改善のためのデータ分析環境（ダッシュボード）

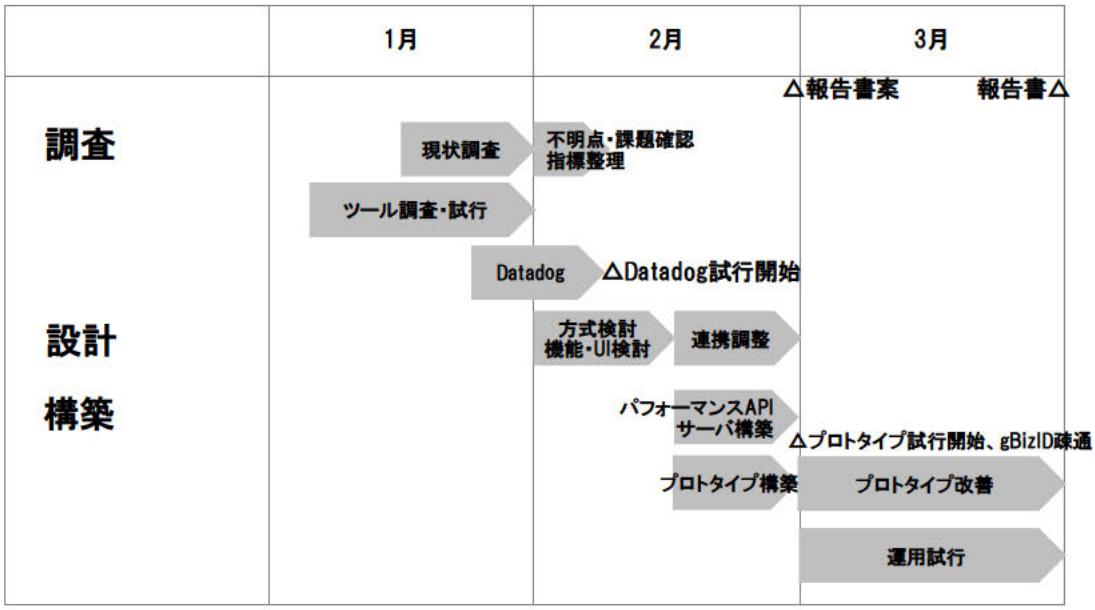

図 1-2 ダッシュボードスケジュール

2.　問合せ対応（チャットボット）

2.1.　チャットボットサービスの選定調査

チャットボットサービスの要件を満たすチャットボットサービスの選定を行った。G ビズスタックでは、共通認証基盤のＧビズＩＤ、補助金申請基盤のＪグランツ、オープンデータ基盤の G ビズインフォ、中小企業支援基盤のミラサポプラス等、複数のシステムが相互に連携しながら一体となってサービスを提供する。そのため、各システムで個別にチャットボットサービスを導入した場合、あるシステムの利用にあたり G ビズスタックの他のシステムの知見が必要になる場合に対応できない場合が想定される。このような課題に対応するためには、複数のサービスに関する FAQ データを一元管理し、連携する他システムの FAQ も必要に応じて回答可能である必要がある。このような機能を実現可能であるサービスとして、CAIWA　Service Viii(以下 CAIWA)を選定した。CAIWA の概要を図 2-1 に示す。

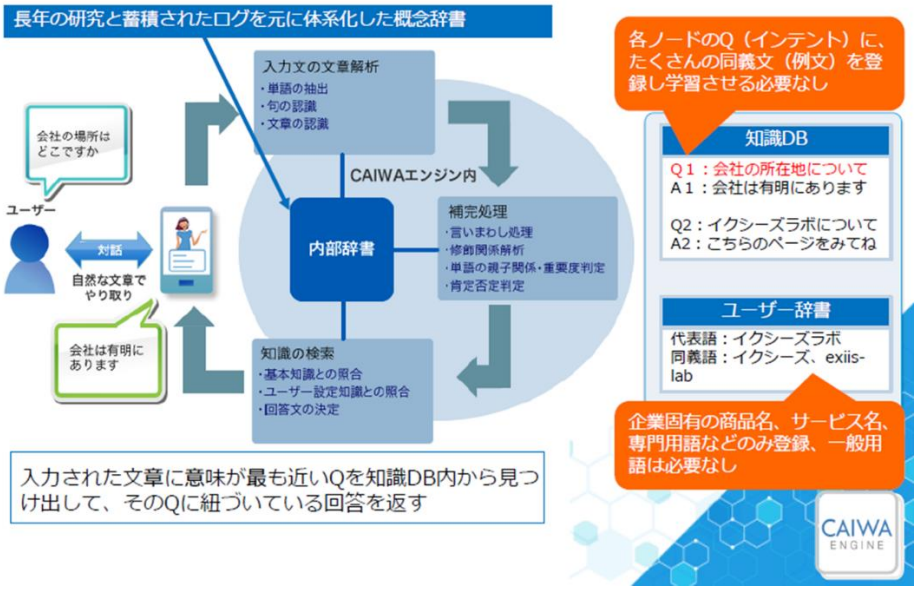

図 2-1 CAIWA の概要

CAIWA は以下のような特徴を持つ。

- Q&A を 1 問 1 答式で登録可能
- カテゴリ設定が可能
- 簡易シナリオが登録可能
- ユーザ辞書による認識精度の向上が可能
- 質問に対し回答がない場合の例外メッセージの管理が可能
- その他回答時のアクション設定が可能
- チャットボットの対話ログ情報に基づき、利用傾向を分析し、知識の構築育成が可能
- 無ヒット(回答できなかった)質問文の一覧を出力し、クリックするとその場で対応する回答文の作成が可能

2.2.　各システムの FAQ データを一元的管理できる環境設計

選定したチャットボットサービスにより、FAQ データを一元的管理し利用するチャットボット環境を構築した。FAQ の管理画面を図 2-2 に示す。本事業において、複数のサービスに関する FAQ データを一元管理し、連携する他システムの FAQ も必要に応じて回答可能とするために、カテゴリ機能を軸に環境設計を行った。カテゴリを指定した上で問い合わせを行うとカテゴリ内で回答をマッチングするが、そうでない場合は複数のカテゴリを横断して回答をマッチングすることができるため、各システム固有の FAQ と他システムで参照する必要がある FAQ を一元的に管理しながら、複数のシステムでの横断的な利用を可能とした。

図 2-2 FAQ の管理画面

2.3. ＧビズインフォおよびＧビズＩＤへの導入・実証

2.3.1. システム概要

今回導入したチャットボットサービスの CAIWA は、ユーザが入力した質問文を対話形式で回答するシステムである。FAQ の管理やサービスの設定は Web 画面により行い、規定された Javascript を対象サイトの Web ページに記載してチャットボットサービスを呼び出す。システム概要を図 2-3 に示す。呼び出すチャットボットサービスは、導入先システム内のリンクからチャットボットサービス専用の Web ページに遷移したり、導入先システムの画面上にフローティング形式として表示するなど用途に応じていくつかの表示パターンを選択可能である。

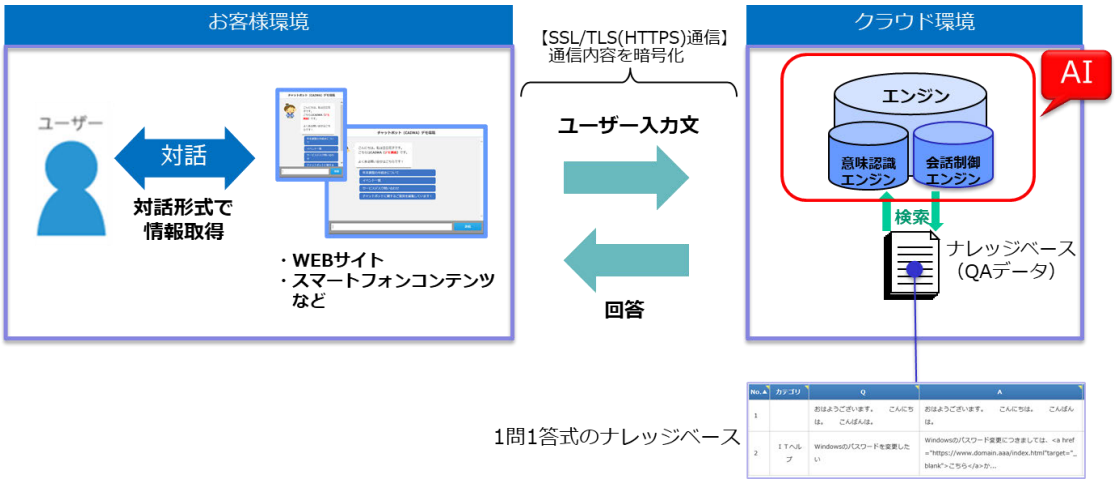

図 2-3 システム概要

2.3.2. G ビスインフォ・G ビズインフォへの導入

環境設計したチャットボットを G ビズ ID の検証環境および G ビズインフォの検証環境へ導入し実証を行った。G ビズインフォの画面を図 2-4 および図 2-5 に示す。それぞれ既存の FAQ をベースにチャットボットへ知識登録を行い、適切に回答が得られることを確認できた。

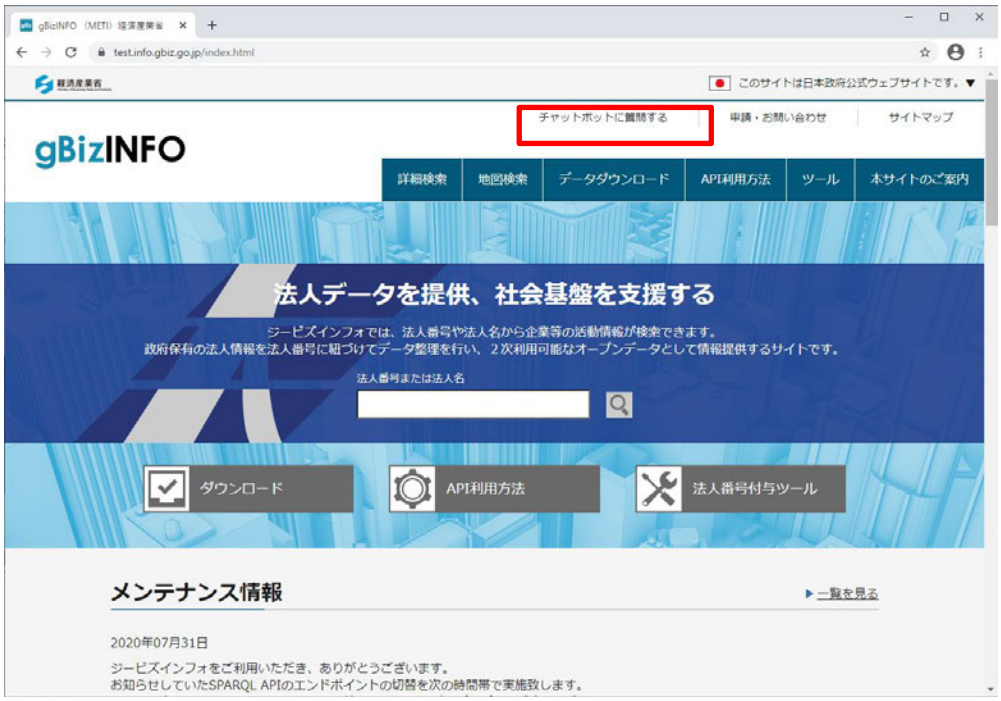

図 2-4 G ビズインフォのチャットボット（Top ページ）

図 2-5 ビズインフォのチャットボット（チャットページ）

3. システム利用状況の見える化とサービス改善のためのデータ分析環境（ダッシュボード）

3.1. 各システムの稼働状況管理機能および指標調査

ダッシュボードの検討にあたり、現在、各システムで集計している指標およびその収集方法等について調査を行った（調査結果の詳細は別添資料参照）。各システムで集計している指標の共通項についてのサマリーを表 3-1 に示す。

表 3-1 各システムで集計している指標の概要

	メトリクス			システム別					
	大分類		項目	gBizINFO	gBizID	ミラサポ	Jグランツ	石油流通システム	保安ネット
1	リソース		CPU使用率	○			○		○
2			メモリ使用率	○			○		○
3			ディスク使用率	○			○	○	○
4			JVMメモリ使用率	○					○
5			ファイルの使用ディスク量					○	
6			ストリーミング API イベント数（24 時間以内）					○	
7			使用ライセンス					○	
8	Webアクセス	PV	Web画面 PV数	○		○		○	
9			アクセス元別Web画面 PV数	○		○			
10			アクセス元別Web画面 訪問数	○		○			
11			Web画面 ページアクセス数	○		○			
12		ユーザ数	ユーザ数					○	
13			Web画面 訪問数	○		○		○	
14		セッション	平均セッション時間					○	
15			新規セッション率					○	
16			ページ/セッション					○	
17			アクセス元別アクセス数	○		○			
18		APIアクセス	WebAPI PV数	○					
19			WebAPI 訪問数	○				○	
20			アクセス元別WebAPI PV数	○					
21			アクセス元別WebAPI 訪問数	○					
22		検索キーワード	検索キーワード　検索数	○		○			
23			検索キーワード　クリック率			○			
24			ランディングページ別検索ワード　検索数			○			
25		メールクリック	お知らせメールクリック数			○			
26		コンバージョン	コンバージョンレート(CVR)						○
27		ユーザの遷移	直帰率					○	○
28			離脱率						○
29			手続き未完了者の再来訪率						○
30		メールログ	メールログファイル	○				○	
31		ログイン数（認証要求・成功・失敗	ログイン者数				○	○	○
32			ログイン数（成功）:件数		○			○	○
33			ログイン数（失敗）:件数		○			○	
34	セキュリティ		WAF監視	○					
35			アンチウイルス監視	○					
36			セキュリティ状態チェック					○	
37			設定変更履歴					○	
38	サービス・システム管理		サービスレベル・稼働率・サーバ稼働状況	○			○	○	○
39			イベントモニタリング					○	
40			デバッグログ					○	
41	業務固有	アカウント数	全会員数			○			
42			アカウント発行数		○	○（Webアクセス）			
43			アカウント変更数		○				
44			ステータス＆事業形態		○				
45		情報数	法人活動情報の掲載件数	○					
46			補助金掲載件数				○		
47			揮発油販売業者数					○	
48			給油所数					○	
49			揮発油貯蓄状況					○	
50			補助金累計ごとの事業数				○		
51			所管組織単位の事業数				○		
56			事業総数				○		
57			RP数		○				
52		申請数	電子申請件数					○	
53			手続件数						○
54		情報ダウンロード数	法人データダウンロード件数	○					
55		APIキー発行数	APIキー発行数	○					
58		手続き関連指標	手続きにおける滞在時間						○
59			審査所要時間比（電子/紙）						○
60			1件あたりの申請工数						○
61			差し戻し発生率						○
62			審査時間						○
63			紙申請の手続きにおける提出時間						○
64			電子化率						○
65		問い合わせ関連指標	平均応答時間						○
66			電話応答率						○
67			問合せ件数						○
68			問合せ発生率						○
69			簡易申請手続数						○
70		トランザクション数	userinfoリクエスト数：件数		○				
71		ユーザ評価	ユーザ評価・アンケート	○		○			

3.2. 一元化・分析機能に向けたデータ項目整理

3.1 節の調査結果と、表 3-2 に示す一元化により実現するシナリオ・期待する効果により、一元化・分析機能に向けたデータ項目の整理について検討を行った。各システムの現状では、リソースや Web アクセスに関する指標は共通項が多いが、業務固有の指標については共通項が少ない。また、集計方法や可視化方法はシステムごとに個別となっている。

このような現状から、業務固有の指標について各システムに共通的なデータ項目を指標として定義し一元的に集計することは、各システムの対応の負担が大きいと考えられる。そのため、本事業で検討するダッシュボードにおいては、様々なシステムから共通的に利用可能な汎用的なデータ集計方法と、取り扱う指標に応じて柔軟に可視化・分析の定義を行うことができる仕組みを構築する必要があると考えられる。一方で、リソースや Web アクセスの指標については業務固有の指標と比較して共通項が多いため一元化は可能であり、集計・可視化のツールやサービスも多く存在するため、それらのツールやサービスを活用することがコストや使い勝手の面で有効であると考えられる。

表 3-2 一元化により実現するシナリオ・期待する効果

#.	実施ロール	シナリオ	期待する効果・考慮事項等	必要メトリクス
1	運用ベンダ、職員	リソースの監視・可視化	一元化した場合、監視ツール・ロジックの共通化によるコスト・体制の効率化、監視レベルの均質化が見込めると考えられるが、比較することのメリットは少ない。	CPU,メモリ,ディスク,ネットワーク等
2	運営ベンダ、職員	Web ページのアクセス数の分析	アクセス数等の基本的なメトリクスについては、それ自体の分析や比較に加えて、分析にあたっての基礎値として使用できるため一元化すると有用である（例えば、アクセス数あたりの運営コスト費などを算出する等）。	サイトへのアクセス数・ユーザ数（Web サーバのログより集計）等
3	運営ベンダ、職員	Web ページのアクセスユーザの詳細分析、クロスドメイントラッキング	Google Analytics のようなサービスを想定。各サイト間の移動や、サイトごとのアクセスユーザの重複など、各サイト間のシナジーを分析するために必要。利用にあたっては、プライバシーポリシーや利用規約上の考慮が必要であるため、すべてのシステムに導入することは困難である可能性がある。	Google Analytics によるメトリクス等
4	運営ベンダ、職員	業務固有のメトリクスの可視化、推移分析	情報の掲載数や手続き数など、業務固有で定義・集計している数値の可視化、分析。基本的には、各システムで業務が異なるため、システム間で比較する場合は比較基準の整理が必要だが、情報掲載システム・申請システム等のカテゴリ内では共通的な指標を定義することは可能。	業務固有のログ（ログイン数、情報掲載数、申請数等）
5	職員	パフォーマンス API メトリクスの可視化、分析	行政内における施策評価やシステム改善。メトリクスの定義、フォーマットや収集方式を共通化しているため、可視化・分析の共通化も容易で、比較に意味があるためダッシュボードとして取り組む効果が高い。	パフォーマンス API メトリクス
6	一般利用者	パフォーマンス API メトリクスの公開	外部公開による透明性向上。メトリクスの定義、フォーマットや収集方式を共通化しているため、可視化・分析の共通化も容易で、比較に意味があるためダッシュボードとして取り組む効果が高い。	パフォーマンス API メトリクス

3.3. 各指標を収集・分析できるサービスおよびツールの選定

各システムからデータを収集し、可視化分析するにはテータの転送、加工、保存、可視化するためのツー

ル・サービスが必要になる。以下に主なサービス・ツールを示す。

表 3-3 ツールの整理

#	カテゴリ	ツール・サービス	説明
1	データ転送	FTP	File Transfer Protocol
2		SSH/SCP	Secure Copy Protocol
3		td-agent/fluentd	ログ収集サービス
4		AWS CLI	AWS コマンドラインインターフェイス（CLI）は、AWS サービスを管理するための統合ツール aws s3 コマンドを用いて他アカウントや AWS 以外の環境から S3 へアップロードが可能。
5	保存	Amazon S3	オブジェクトストレージサービス
6		Amazon Elasticsearch Service	検索および分析エンジン 大規模なデータコレクションをインデックス化、管理、検索、視覚化し、ログ分析、リアルタイムのアプリケーションモニタリング、クリックストリーム分析が可能。
7	データ処理・加工	Amazon Athena	クエリサービス Amazon S3 にあるデータを直接、標準 SQL にてデータ抽出することが可能なクエリサービス。
8		AWS Glue	サーバレス ETL サービス 各サービスとの間で動作しデータを抽出し、変換し、出力する。
9		Redshift	フル機能のエンタープライズデータウェアハウスサービス データを収集して蓄積し 1 つにまとめ、データ抽出やデータ分析などを行う。 大規模・パフォーマンス・複雑なクエリー対応。
10	可視化	Amazon Elasticsearch Service/ Kibana	検索および分析エンジン Kibana を用いて視覚化することが可能。
11		Amazon QuickSight	BI ツール AWS 上で利用できることが利点。
12		Tableau	BI ツール 低コストで導入できるノンプログラミングで誰でも簡単にデータ分析できるビジネスインテリジェンス(BI)ツール。
13		DataDog	システム・アプリケーションの運用監視プラットフォーム BI ツールとしても利用可能。
14	データレイク	AWS Lake Formation	データレイクサービス S3, KMS, Glu 各種サービスの組み合わせ。
15	データウェアハウス(保存・データ処理・加工・分析)	Amazon Redshift	フル機能のエンタープライズデータウェアハウスサービス データを収集して蓄積し 1 つにまとめ、データ抽出やデータ分析などを行う。 大規模・パフォーマンス・複雑なクエリー対応。

16	ストリーミング	Amazon MSK	ストリーミングサービス リアルタイムに大容量データを大量に取り込むことができるサービス。
17		Amazon Kinesis	ストリーミングキューサービス リアルタイムに大容量データを大量に取り込むことができるサービス。

ダッシュボードおよび、ダッシュボードにて収集するデータを保持するシステムはパブリッククラウド上で稼働しているため、コスト最適化を考慮し、サーバレス、フルマネージドサービスを優先的に検討、選択した。

また、ツール、サービスを選定するにはリクエスト数、データの規模、リアルタイム性、クエリの複雑性等を考慮する必要がある。本事業で検討するダッシュボードでは現状限定的なリクエスト数、小～中規模、日次程度の更新頻度のデータ、複雑性の高いクエリは存在しないため、データ保存に S3、データ処理に Amazon Athena、可視化に Tableau、Amazon QuickSight、DataDog を検討した。今後、より大量リクエスト、大規模、リアルタイム性のある分析が必要になる場合は Redshift 等のデータウェアハウス、Amazon Kinesis 等ストリーミングサービスを検討する必要がある。

ダッシュボードに使用したツール・サービスを以下に示す。

表 3-4 ダッシュボードに使用したツール・サービス

指標	ツール・サービス		
	データ転送	保存・データ処理	可視化
サーバリソースメトリクス	AWS CloudWatch API	—	DataDog
業務固有データ	AWS Lambda AWS CLI	Amazon S3, Athena	Amazon QuickSight Tableau
パフォーマンス指標	独自 API(パフォーマンス API)	Amazon API Gateway , Lambda, S3, Athena	パフォーマンスダッシュボード Tableau

本事業では、以上の構成により DataDog によるサーバメトリクスの可視化、業務固有データの収集・可視化、パフォーマンス API の収集・可視化を実装した。

3.4. アクターとロール

本事業で構築した業務固有データの収集・可視化とパフォーマンスＡＰＩのアクターとロールを以下のようにまとめた。

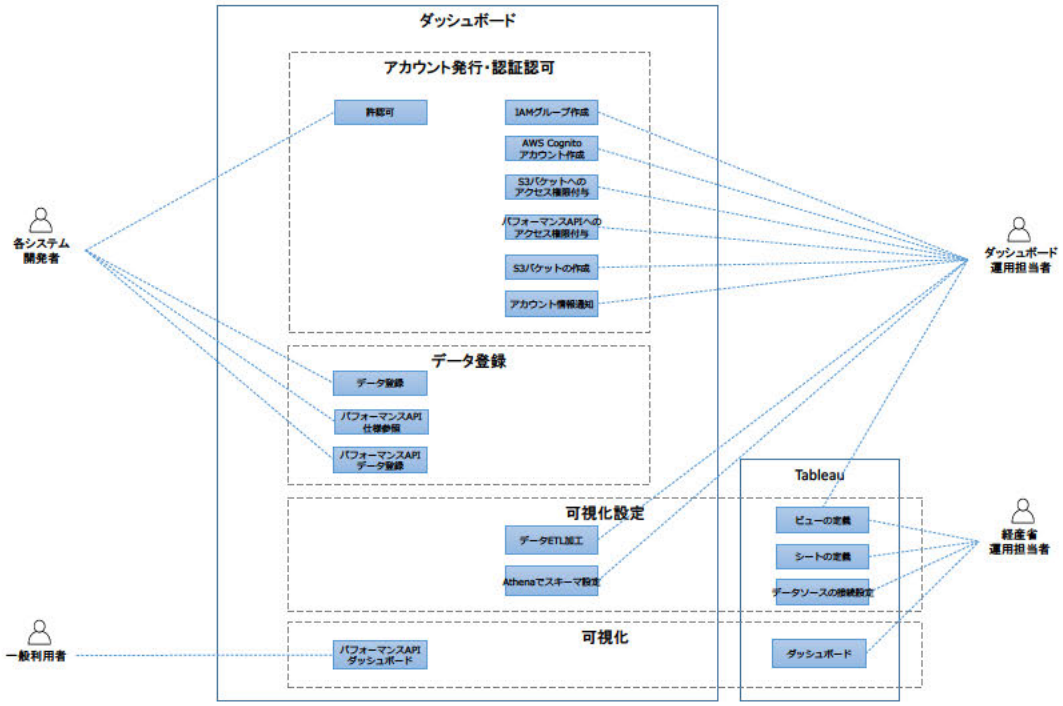

図 3-1 アクターとロール

表 3-5 アクターとロール

#	アクター	ロール
1	経済産業省運用担当者	可視化されたデータを Tableau/Amazon QuickSight 等で参照する。 Tableau を使用する場合はデータソースの接続設定、ビュー、シート等の設定をする必要がある。
2	ダッシュボード運用担当者	アカウントの払い出し、データの収集・加工を行う。
3	各システム開発者	データをダッシュボードへ登録する。 ダッシュボード運用担当者から払い出されたアカウントによる認証・認可が必要になる。
4	一般利用者	パフォーマンス API ダッシュボードを参照する。認証・認可は不要。

3.5.　サーバメトリクスの収集・可視化

本事業では DataDag を用いた G ビズインフォのサーバメトリクスの可視化を実施した。

3.5.1.　システム構成

システム構成を以下に示す。

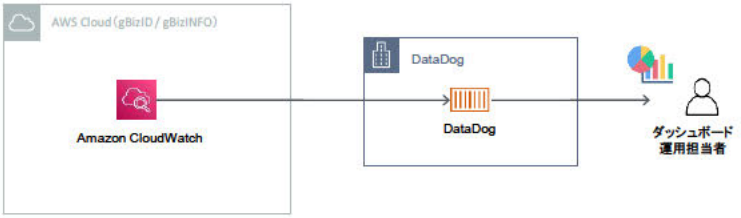

図 3-2DataDog によるシステムメトリクスの収集・可視化

3.5.2.　G ビズインフォでのダッシュボード例

ダッシュボードの例を以下に示す。以下ダッシュボードは G ビズインドの EC2 および Aurora の CPU 使用率、Web サーバへのリクエスト数/秒、レスポンスタイム、S3 バケットの使用量(GB)を表示した例。

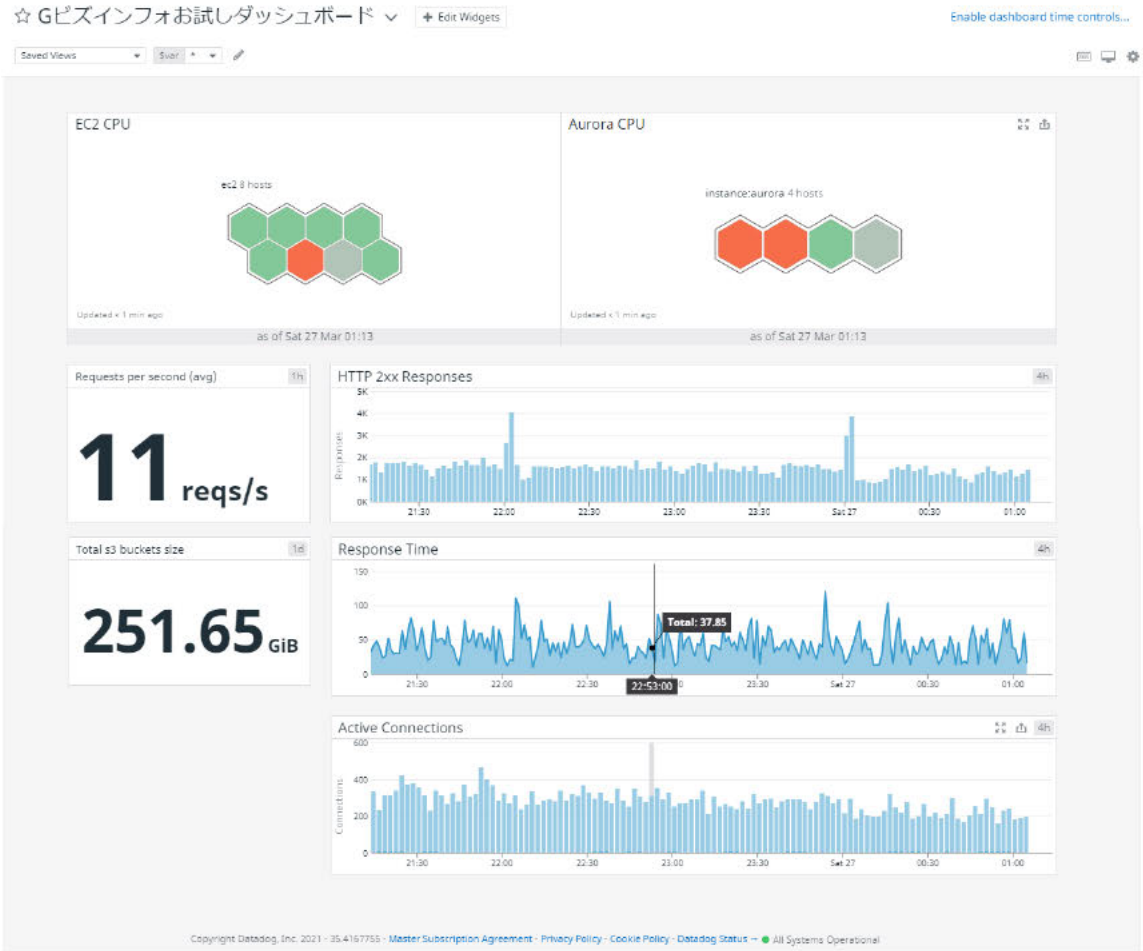

図 3-3DataDog によるサーバメトリクスの可視化

3.6. 業務固有メトリクスの収集・可視化

3.6.1. システム構成

システム構成を以下に示す。

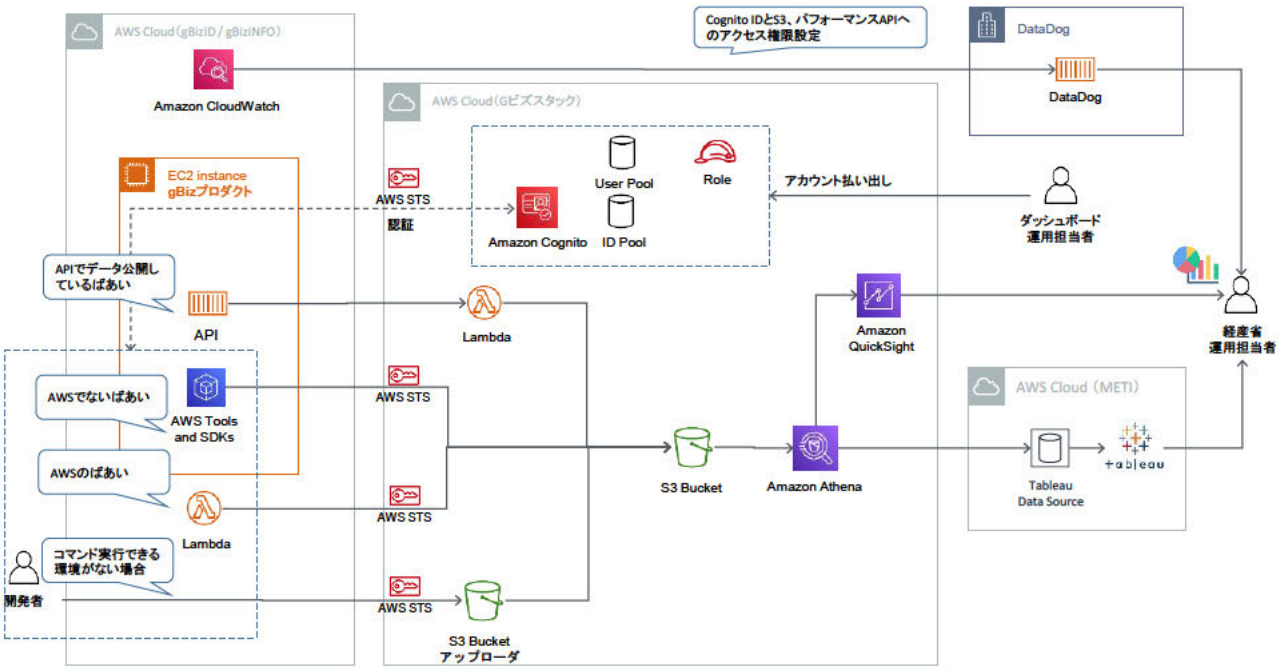

図 3-4 業務固有のメトリクスの収集・可視化

Amazon Cognito を使用した認証を行い、業務固有のメトリクスを S3 Bucket に送信、保存する。ダッシュボードで Athena を使ってスキーマを定義し、BI ツール(Amazon QuickSight / Tableau)からは Athena に接続し、データを可視化する。認証・認可は Amazon Cognito で行う。

また、S3 バケットへのデータ登録は各システム開発者の保有する環境条件や要件に応じて以下 3 パターンの登録方法が考えられる。

表 3-6 S3 バケットへの登録方法

#	登録方法	環境条件や要件
1	AWS CLI コマンドを用いて登録する。	AWS CLI コマンドを実行できる環境がある場合
2	Lambda を用いて登録する。	AWS CLI コマンドを実行できる環境がなく、AWS の環境が利用できる場合
3	S3 バケットへのアップローダを用いて登録する。	AWS CLI コマンドを実行できる環境、Lambda を実行する環境が無い場合。

本事業では AWS CLI コマンドを実行できる環境、Lambda を実行する環境が無い場合を考慮し、 S3 バケットへのアップローダを実装した。

3.6.2. 業務フロー

業務フローを以下に示す。

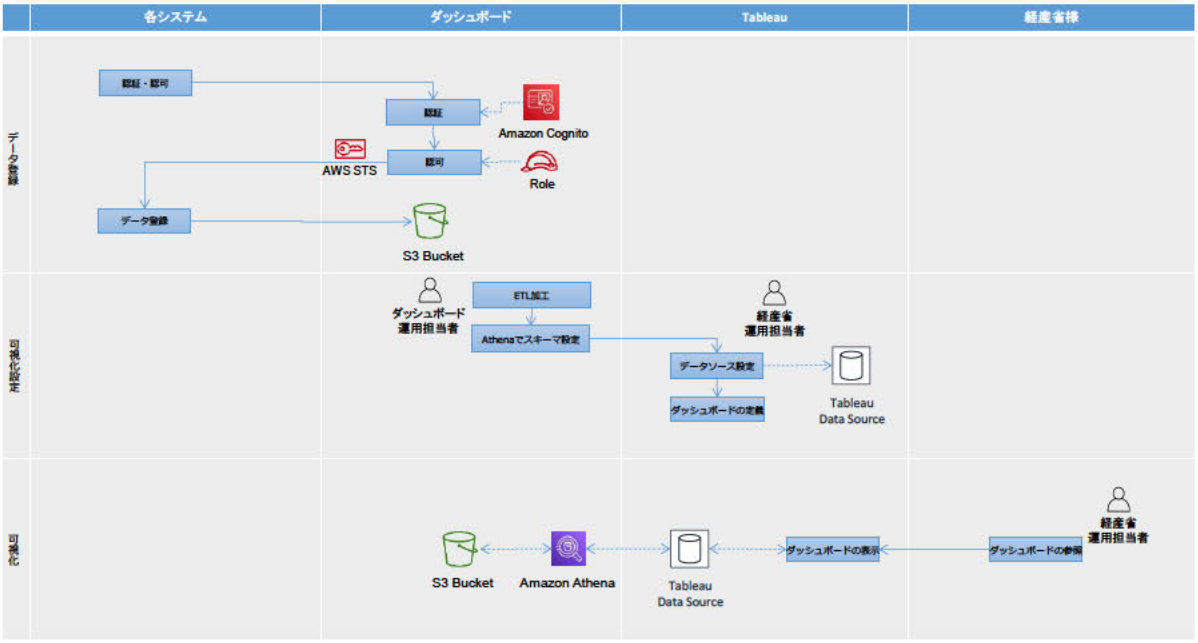

図 3-5 業務固有メトリクスのデータ登録・可視化

- 事前準備（3.9 事前の準備と運用に係る作業参照）
- データ登録
  - 各システムで作成したプログラム（シェルスクリプトやバッチ）もしくはアップローダでダッシュボードの Amazon Cognito により認証・認可を実施
  - プログラム（シェルスクリプトやバッチ）もしくはアップローダを用いて S3 バケットへ該当ファイルアップロードする
- 可視化設定
  - ダッシュボード運用担当者が ELT 加工を実施
  - Athena でスキーマを定義する
- 可視化
  - 経済産業省運用担当者はダッシュボードを表示・参照

3.6.3. 実装例

(1) アップローダ

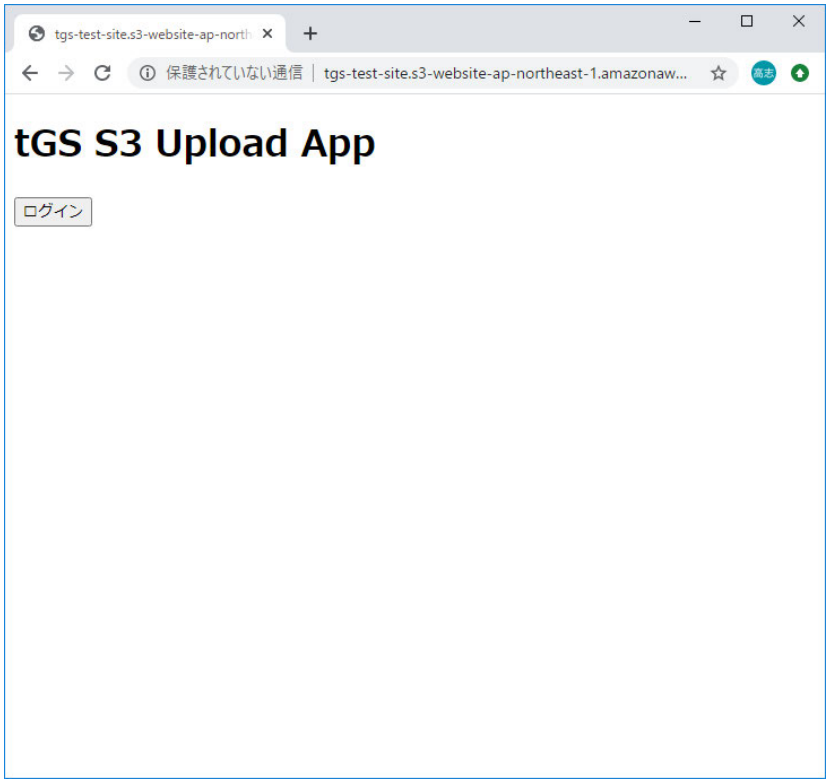

図 3-6 アップローダ(未ログイン)

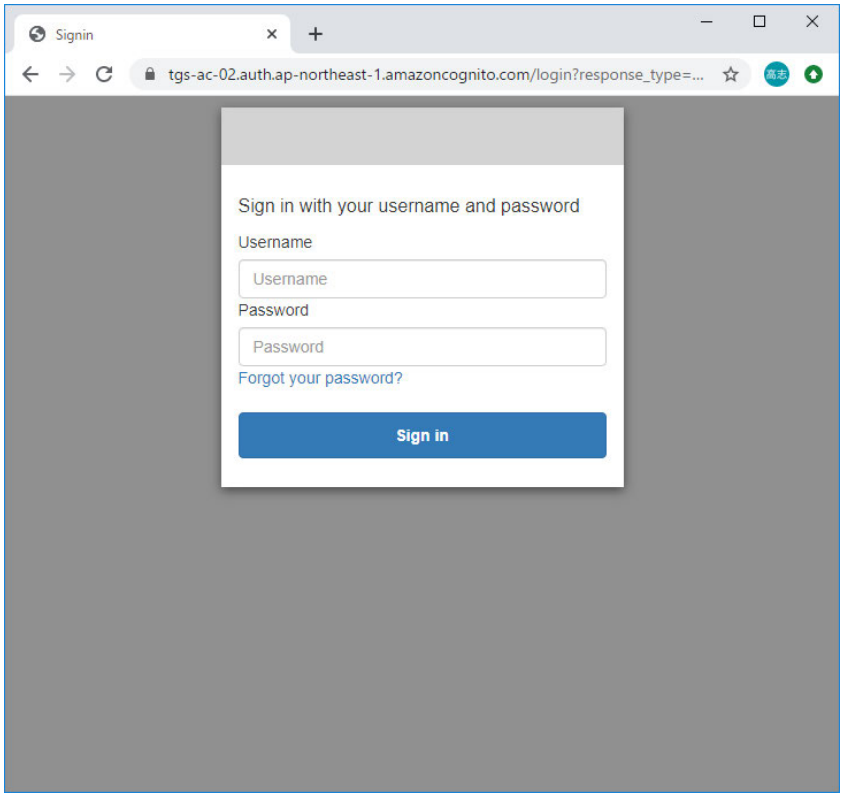

図 3-7Cognito による認証

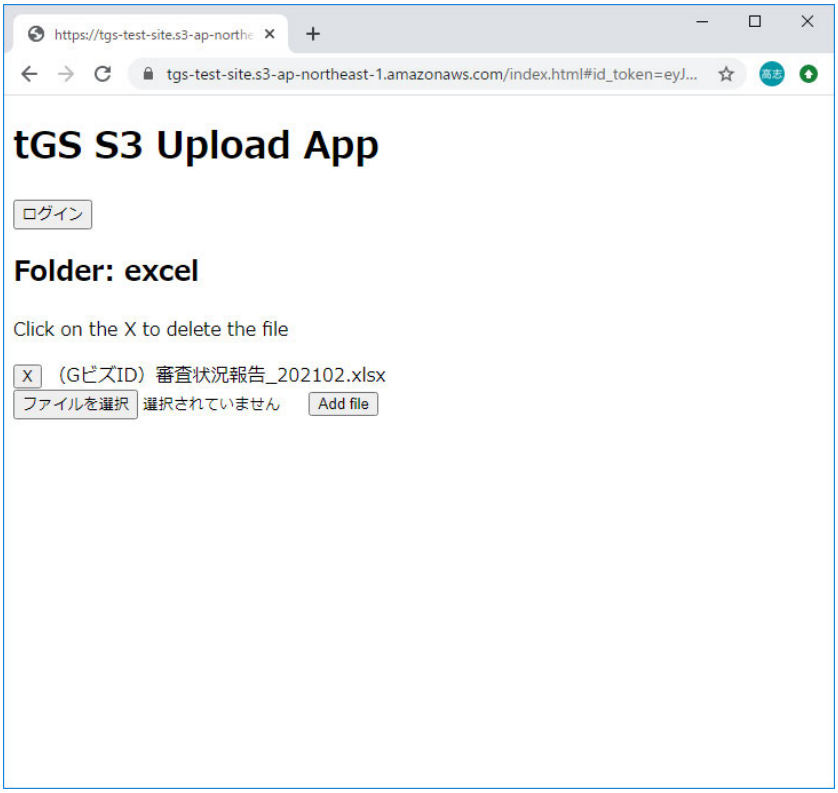

図 3-8 アップローダ(認証後)

(2) 可視化

図 3-9 可視化の例

図 3-10 可視化の例 2

3.7. パフォーマンス API の実装と可視化

3.7.1. システム構成

システム構成を以下に示す。

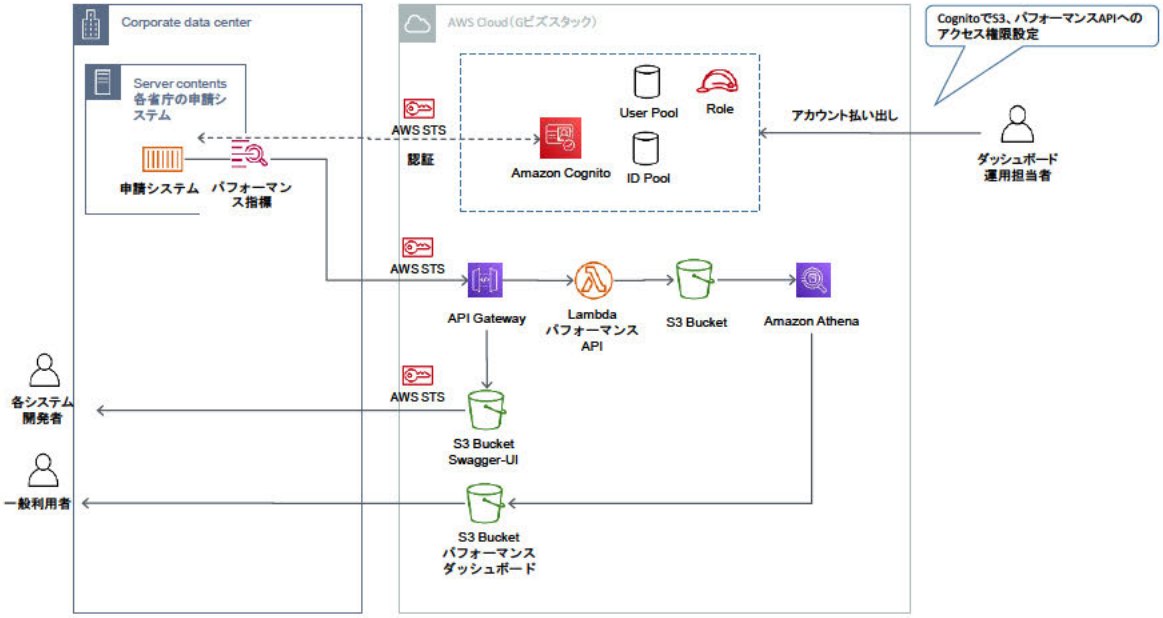

図 3-11 システム構成

Amazon Cognito を使用した認証を行い、パフォーマンス指標をパフォーマンス API へ POST する。

パフォーマンス API は API Gateway と Lambda で実装されており、受け取った指標を S3 Bucket に送信、保存する。ダッシュボードで Athena を使ってスキーマを定義し、BI ツール(Amazon QuickSight / Tableau)からは Athena に接続し、データを可視化する。

3.7.2. 業務フロー

業務フローを以下に示す。

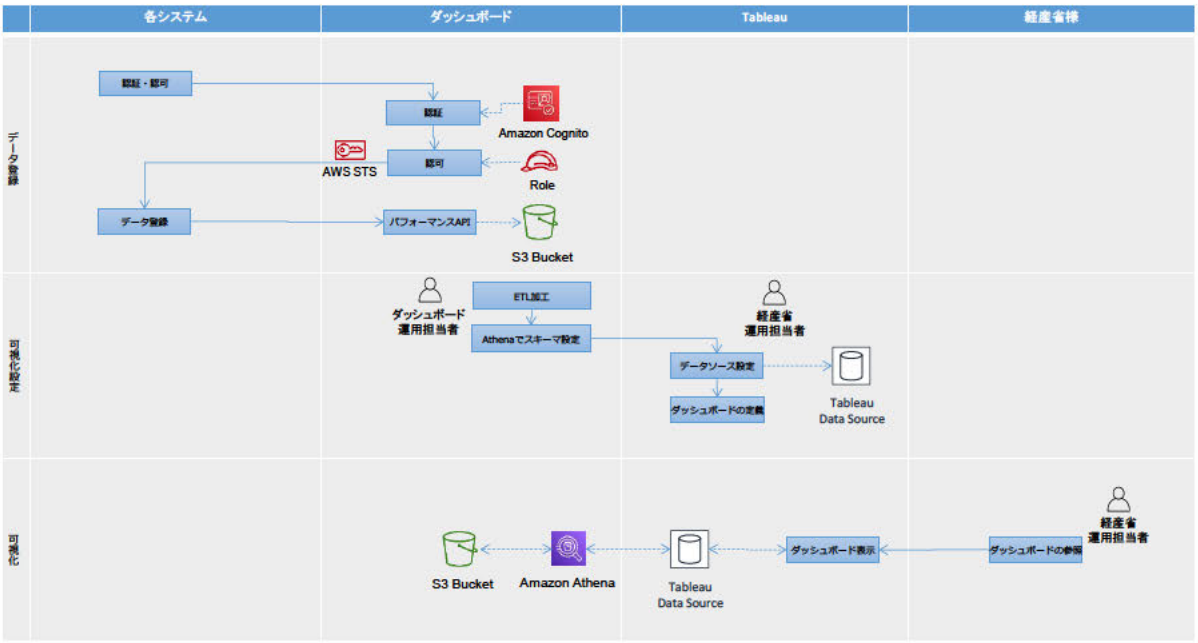

図 3-12 業務フロー

- 事前準備（3.9 事前の準備と運用に係る作業参照）
- データ登録
  - 各システムで作成したプログラムでダッシュボードの Amazon Cognito により認証・認可を実施
  - パフォーマンス API へパフォーマンス指標を POST する
- 可視化設定
  - ダッシュボード運用担当者が ELT 加工を実施
  - Athena でスキーマを定義する
- 可視化
  - 経済産業省運用担当者はダッシュボードを表示・参照

3.7.3. 実装例

(1) Swagger-UI（パフォーマンス API の仕様とシミュレータ）

図 3-13 パフォーマンス API Swagger-UI

(2) パフォーマンスダッシュボード

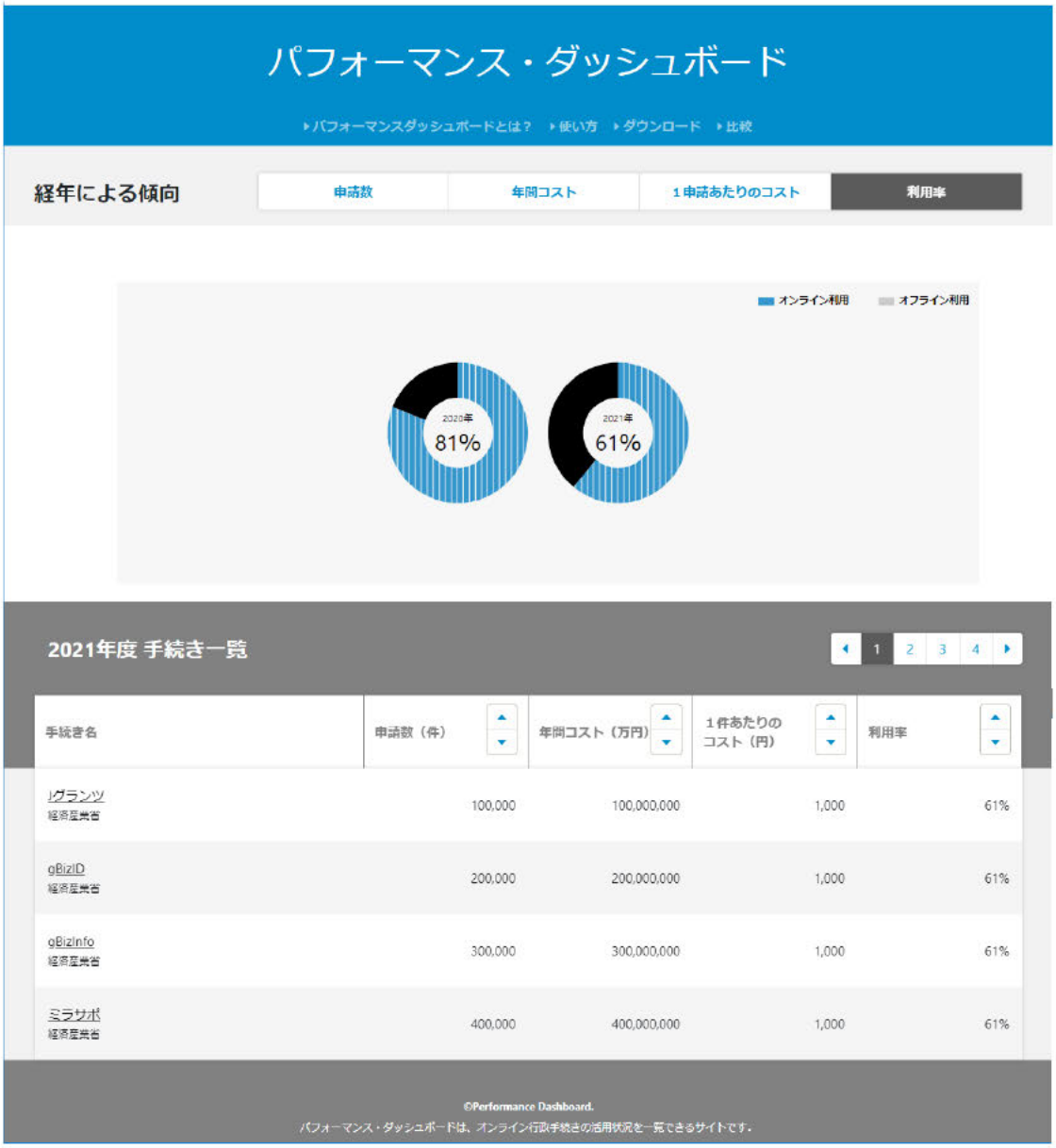

図 3-14 パフォーマンスダッシュボード

3.8. 適切なアクセスコントロールの実施

本業務では Amazon Cognito を使用したアクセスコントロールを行った。

Amazon Cognito はウェブアプリケーションやモバイルアプリケーションの認証、許可、ユーザ管理をサポートしている。ユーザは、ユーザ名とパスワードを使用して直接サインインするもしくは、Facebook、Amazon、Google、Apple などのサードパーティーを通じてサインインできる。

3.8.1. Amazon Cognito を用いた認証・認可

ダッシュボードの S3 へ業務固有のログ、メトリクスをアップロード、パフォーマンス API でパフォーマンス指標を POST する際は認証・認可が必要になる。G ビズスタックでは認証・認可を実現するために Amazon Cognito を利用した認証・認可を実現した。

Amazon Cognito を利用することにより、各機能への認証・認可するためのユーザ情報、ロール情報の一元管理を実現した。

Amazon Cognito はユーザプールと ID プールで構成されている。ユーザプールはグループ、ロール、ユーザの管理、認証を行う。ID プールはユーザプールで認証したユーザに対して一時的な AWS 認証情報を与え、S3 やパフォーマンス API へのアクセスを認可する。

ユーザプールに認証情報（ユーザー名とパスワード）を渡すことで、ロール情報やユーザ情報を含むアクセストークンを取得し、取得したアクセストークンを ID プールに渡してユーザプールに設定したロールを使用できる一時クレデンシャルを取得する。

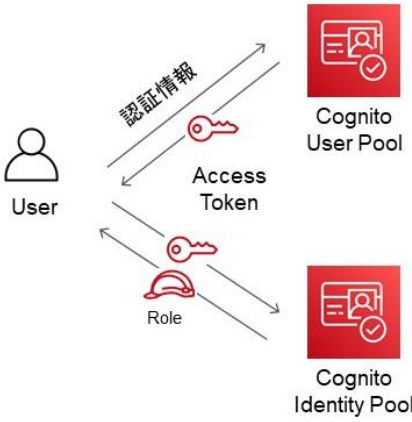

図 3-15Cognito を用いたアクセスコントロール

3.8.2. グループ、ロール、ユーザの管理

各システム（G ビズ ID,G ビズインフォ）毎にグループを作成し、各 S3 バケットへアクセスするロールを作成しグループに紐づけた。

3.8.3. 業務固有のメトリクスをアップロードするときの認証・認可

業務固有のメトリクスのアップロード用のバッチや Lambda から Cognito へ認証情報を渡し、認可を

受ける。S3 アップローダはログイン画面から認証情報を入力し、サーバサイドで Cognito へ認証認可を行う。Cognito で認証された場合、Cognito から S3 にデータをアップロードするロールを取得する。

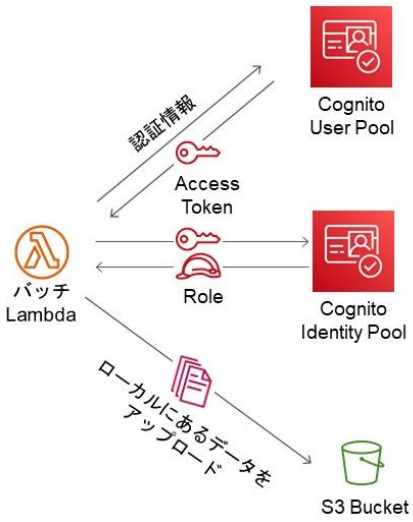

図 3-16 業務固有のメトリクスのアップロード時の認証・認可

3.8.4. パフォーマンス API の認証

ユーザは Cognito ユーザプールに認証情報を渡し、アクセストークンを取得する。パフォーマンス API のヘッダーにアクセストークンを追加してリクエストを送ると、Cognito と連携しているパフォーマンス API が認証し、レスポンスを返す。

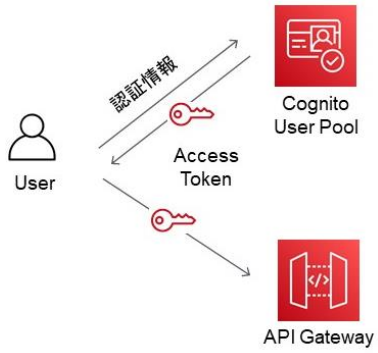

図 3-17 パフォーマンス API の認証

3.9. 事前の準備と運用に係る作業

本事業で検討したダッシュボード環境を使用するにはダッシュボード運用担当者が各システムの開発者・利用者のアカウントを払い出す必要がある。以下にアカウント払い出しのフローを示す。

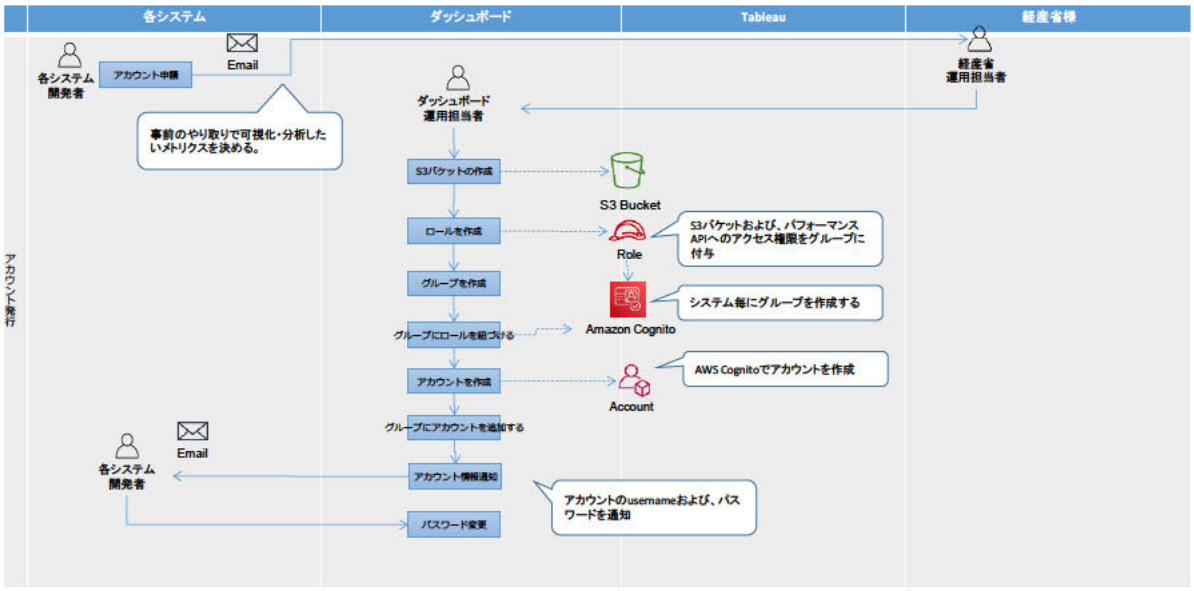

図 3-18 アカウント払い出しのフロー

アカウントの払い出しは以下の方法で行う。

① 追加するプロジェクトのロールを作成
S3 バケットおよび、必要な場合はパフォーマンス API へデータの権限を付与するロールを作成する。

② 追加するプロジェクトのグループを作成

③ グループにロールを紐づける

④ 追加するプロジェクトメンバーのアカウントを作成

⑤ グループにアカウントを追加する

⑥ プロジェクト用の S3 バケットを作成する
本事業においては以上の処理を手動で実施したが、運用を考慮すると、サインアップおよび上記一連の作業を AWS CLI 等により自動化する必要があると考える。

以上