

IoT Platform
サービス詳細説明書
(16.0_0 版)

<改版履歴>

版数	説明	日付
1.0 版	初版	2016/10/7
1.1 版	<ul style="list-style-type: none"> 全体：URL の例を修正 (誤記) 図 1.1 および 1.3 のサービス名称を修正 2.10.7、MQTT プロトコル利用時の課金対象メッセージを明記 	2016/11/1
1.2 版	<ul style="list-style-type: none"> (誤記) 2.3.7.1 操作権限の表中、更新 (U:update) の内容に記載の「※ MQTT/MQTTS は非対応」を正しい位置に修正。 2.3.6.2/2.3.6.3 において必要な情報の取得方法を修正 (誤) 開通通知書で通知 → (正) サービス申込み時に通知 3.1 目安を超えた使い方をする場合の対応に、「17 年春以降のエンハンスで目安を越える利用状況の場合システム制限がかかり、すべてのリクエストがエラーまたは破棄されるようになる」ことを追記 	2016/12/1
4_1.0 版	<ul style="list-style-type: none"> 追加機能について追加 (1) 2.3.7、アクセスコードの設定項目に P/G 権限、プロトコル制限、クライアント証明書について追記 (2) 2.4.3、サービスポータル画面の機能に以下を追記 「エラーログ蓄積」「CORS 機能」「クライアント証明書」 (3) 2.3.6.2 と 2.3.6.3 の②の名称についてシステムバージョンから API バージョンに変更 	2017/3/27
4_2.0 版	<ul style="list-style-type: none"> 17 年春のエンハンスに関する記載を削除 2.4.2 サービスポータルの動作確認対象に Windows10 を追加 2.10 「エラーログ蓄積」 2.11 「CORS 対応」 2.12 「クライアント証明書」を追記 本書名称を「Fujitsu Cloud Service K5 IoT Platform サービス詳細説明書」から「IoT Platform サービス詳細説明書」に変更 3.1 サービス利用頻度の目安を変更 	2017/8/1
4_2.1 版	<ul style="list-style-type: none"> 3.8 DoS 攻撃への対処を追記 4.8 「イベント設定の削除」を追記 	2017/10/11
5.0_0 版	<ul style="list-style-type: none"> 用語一覧に「BSON」の説明を追記 2.3.6 にリソースに登録可能なデータ形式に csv、text、256KByte 以下の Binary を追加。 2.13 仕様制限の 2.13.1 「リソースの制限」の記載を、2.5 API の説明部に 2.5.3 「リクエストの制限」として移動。 2.5.3 リクエスト制限の表中「イベント機能で転送されるデータの容量上限を 256Kbyte に修正 2.13.3 「リソースの制限」を「1 リソースに蓄積するデータ量の考え方」として修正 2.3.7.4 「クライアント証明書」にポータルから発行したクライアント証明書に加え、お客様が手配したクライアント証明書も対照であることを追記 	2017/11/18
5.0_1 版	<ul style="list-style-type: none"> 2.3.6.2 SSL 対応から TLS1.1 を削除 	2018/1/9
5.1_0 版	版数を修正	2018/3/17
7.0_0 版	<ul style="list-style-type: none"> 2.10 イベント機能の内部エラーについて検出できない場合があることを追記 	2018/09/15
9.0_0 版	<ul style="list-style-type: none"> 2.2.5 DRC (オンデマンドデータ収集) についての記載を追加 	2019/8/22
11.0_0 版	版数を修正	2021/1/16
14.0_0 版	<ul style="list-style-type: none"> 2.4.2 サポートブラウザの変更 2.4.3 アカウントに紐づくクライアント証明書の操作機能を追加 4.4 クライアント証明書秘密鍵の漏洩に対する注意喚起を追加 	2022/4/1
16.0_0 版	<ul style="list-style-type: none"> DRC (オンデマンドデータ収集) 機能削除に伴い、本記載を削除 	2024/6/3

はじめに

このたびは「IoT Platformサービス（以下、本サービス）」をご検討いただき、誠にありがとうございます。ご紹介します。

この「IoT Platform サービス詳細説明書（以下、本書）」は、本サービスをご契約いただいたお客様、またはご採用いただくお客様のための資料です。下記につきましてご了承くださいませよう、よろしくお願いいたします。

1. ご検討中のお客様は、本書を本サービスご採用可否のご判断のためにのみ、ご参照願います。
2. 本書および本書の内容について、第三者へご開示／ご提供にはならないようお願いいたします。
3. 発行元の許可なく、本書の記載内容を複写／転写することを禁止します。

本書には本サービスをご採用いただくための重要な情報を記載しています。

ご契約いただいたお客様は、ご利用前に本書をよくお読みの上、本サービスをご利用ください。なお、本書は大切に保管してください。

ご採用いただけないお客様は、お客様の責任で本書をすみやかに廃棄願います。

※ *Windows* は、米国 *Microsoft Corporation* の、米国およびその他の国における商標または登録商標です。

Google Chrome は、*Google Inc.* の、米国およびその他の国における商標または登録商標です。

本書は、今後サービス仕様の変更にあわせて、予告なく内容を変更する場合があります。

<用語一覧>

用語	説明	備考
IoT	Internet of Things の略 「モノのインターネット」と言われるが、「モノがインターネットプロトコル（インターネット言語）でネットワークされている状態」のこと。	
REST	REpresentational State Transfer の略 複数のソフトウェア連携に適した設計原則を Web に適用したソフトウェアの設計様式を示す。 ※特定の URL にパラメータを指定して HTTP でアクセスすると XML で記述されたメッセージが送られてくるような、呼び出しインターフェース（「RESTful API」と呼ばれる）。 本サービスでは XML ではなく JSON 形式で返信する。	
MQTT	Message Queuing Telemetry Transport の略 MQTT とは、TCP/IP ネットワーク上の通信プロトコルで、多数の主体の間で短いメッセージを頻繁に送受信する用途に向けた軽量なプロトコル。M2M ネットワークや IoT（Internet of Things）分野での普及が見込まれている。ヘッダ部分が最小で 2 バイトと小さく、HTTP で同様の通信を行う場合より、通信量や CPU 負荷・電力消費量などを数十分の一に抑える。	
DRC	ダイナミックリソースコントローラー(Dynamic Resource Controller) 富士通の広域分散技術を用いた分散制御処理。データ収集においてトラフィックの変動に従い、限られたリソースの中で最適化した収集の実現を補佐する機能。	
BSON	主に MongoDB のデータストレージ及びネットワーク転送フォーマットとして利用されている、データ交換フォーマット。	
リソース	リソースデータの収集単位として定義	
リソースデータ	リソースの中にある 1 つのデータとして定義	
アクセスコード	リソースを対象に設定する認可情報として定義	
エッジ	現場や現場にある装置や PC、デバイスなどの総称	

- 目次 -

第1章	IoT Platform サービスについて	4
1.1.	概要	4
1.2.	特長	5
1.3.	サービス範囲	5
1.4.	ドキュメント	5
第2章	サービス仕様	6
2.1.	マルチテナント	6
2.2.	機能概要	6
2.2.1.	データ収集	6
2.2.2.	イベント機能	7
2.2.3.	アクセス制限	7
2.2.4.	ダイナミックリソースコントローラー	7
2.3.	定義	8
2.3.1.	テナント ID	8
2.3.2.	管理者アカウント	8
2.3.3.	管理者パスワード	8
2.3.4.	MQTT アカウント	8
2.3.5.	MQTT パスワード	8
2.3.6.	リソース	9
2.3.7.	アクセスコード	11
2.4.	サービスポータル	12
2.4.1.	利用条件	12
2.4.2.	動作確認	12
2.4.3.	管理機能	12
2.5.	API	13
2.5.1.	HTTP REST インターフェース	13
2.5.2.	MQTT インターフェース	14
2.5.3.	リクエストの制限	14
2.5.4.	HTTP-IF におけるリソースデータ登録と MQTT-IF の関係	14
2.5.5.	同時刻のデータの扱い	15
2.6.	データの転送先設定	15
2.7.	イベント機能	15
2.7.1.	対象操作	15
2.7.2.	検出条件設定	16
2.7.3.	イベント発行時の添付データ	17
2.8.	アクセス制限機能	17
2.8.1.	サービスポータルへのアクセス制限	17
2.8.2.	リソースへのアクセス制限	17
2.9.	ダイナミックリソースコントローラー機能（分散機能）	17
2.10.	エラーログ蓄積機能	18
2.11.	CORS 対応	19
2.12.	クライアント証明書発行機能	19
2.13.	注意事項（仕様制限）	19
2.13.1.	API で使用する文字コード	19
2.13.2.	時刻	19
2.13.3.	1 リソースに蓄積するデータ量の考え方（JSON データ）	19
2.13.4.	[MQTT のみ]QoS	19
2.13.5.	[MQTT のみ]コネクション断時の振る舞い	19
2.13.6.	[MQTT のみ]課金対象メッセージ	19
2.13.7.	その他	19
第3章	制限事項	20

3.1.	目安を超えた使い方をする場合の対応	20
3.2.	過度な集中利用の禁止	20
3.3.	イベント機能／転送機能利用時の注意	20
3.4.	データの保障	20
3.5.	データの到達性	20
3.6.	API のクエリー仕様変更の可能性	20
3.7.	データの削除	20
3.8.	DoS 対策	20
第4章	重要事項説明	21
4.1.	サービス提供時間	21
4.1.1.	計画メンテナンス	21
4.1.2.	緊急メンテナンス	21
4.2.	サポート範囲	21
4.2.1.	サポートデスク利用時の必要情報	21
4.3.	蓄積データの正当性について	21
4.4.	アクセスコードの管理	21
4.5.	お客様データの閲覧	21
4.6.	ダイナミックリソースコントローラー利用時の課金について	22
4.7.	蓄積データの利用	22
4.8.	イベント設定の削除	22

第1章 IoT Platform サービスについて

1.1. 概要

本サービスは、IoT 活用で必要となる大量の機器や業務とのデータ送受信～蓄積と、主にリアルタイム系の判断／アクションの実行、および効率的なデータ収集を行う分散機能を含む、IoT 専用クラウドサービスです。

- データ管理機能
データの管理を行う、お客様管理者用の WEB サイト(サービスポータル)を提供します。
- データ収集機能
データを本サービスに蓄積します。データの外部サービスへの転送機能も提供します。
- API の提供
データ管理／収集／活用を実行できる API を提供します。
HTTP REST および MQTT プロトコルに対応します。
- 認可管理
API リクエストに対する認可機能を提供します。リソース単位に認可管理できます。
- イベント機能
本サービスに登録されるデータに対する条件を設定し、条件がマッチした場合にアクションします。
アクションの種類： API 起動、Email 通知
- ダイナミックリソースコントローラー (分散制御)
お客様の限られた IT リソース内で、効率的なデータ収集を実現する機能を提供します。
- アクセス制限機能
お客様の指定の IP アドレスからのみアクセスを許容する機能を提供します。サービスポータル、およびアクセスコードに対して制限できます。

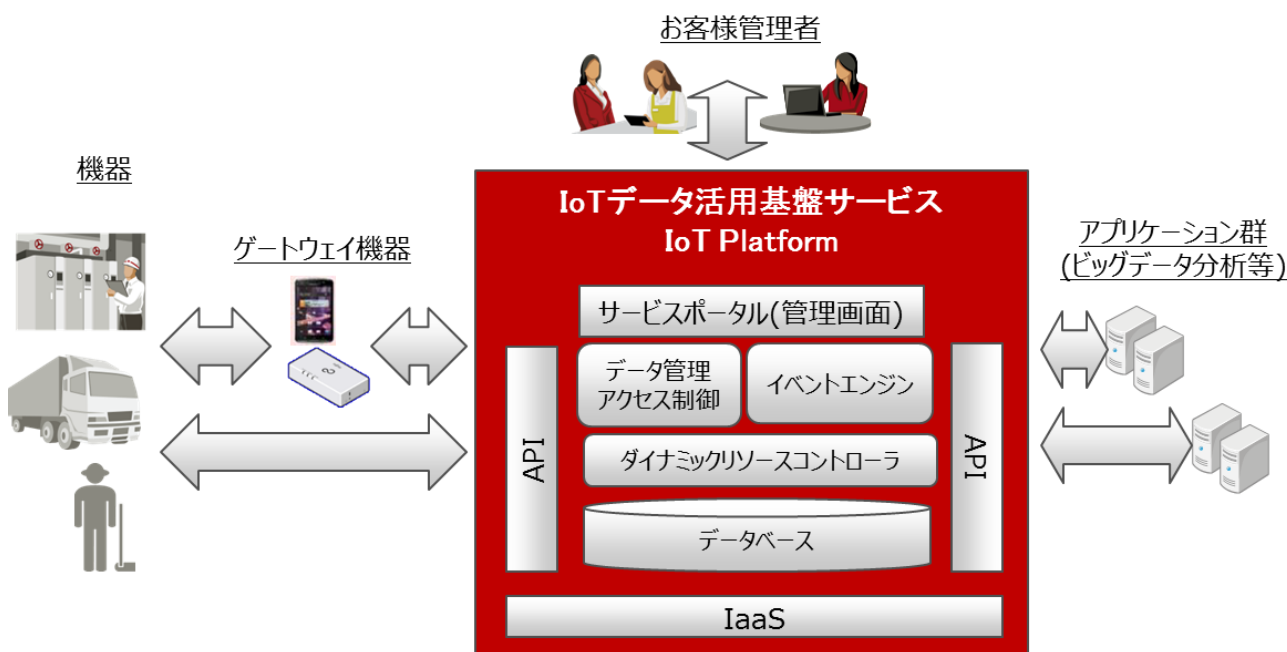


図 1.1 サービス概要

1.2. 特長

- IoT システムを短時間で構築可能
クラウドサービスの活用によりお客様での環境構築作業が不要です。IoT で必要となる基本的な機能群をセット提供しており、お客様は IoT を活用して実現したい業務アプリケーション開発に専念できます。標準的なインターフェースを提供しており、アプリケーション開発も容易です。
- 多様なセンサー／デバイスに対応
通信負荷やバッテリー消費の少ない IoT 向けの軽量プロトコルである「MQTT」を標準でサポートします。従来の HTTP REST にも対応しており、多様なセンサー／デバイスをビジネスに活用できます。
- セキュアなデータ管理
お客様がデータ活用するために蓄積する各データ群（リソース）に対し、アクセス権限を設定出来る為、お客様関連会社等複数社間でのセキュアなデータ活用が可能です。
- 安定したデータ収集を支援
センサー等デバイスから発生するデータの収集に対し、富士通独自の全体最適化技術（広域分散技術）により、データトラフィックの変動等に対して効率的かつ安定したデータ収集が可能です。

1.3. サービス範囲

本サービスにおいて、データの収集元である機器やデバイス・センサー群、データの取得元である「分析基盤」「お客様業務／協業他社アプリケーション」など、およびネットワーク、はサービス範囲外です。

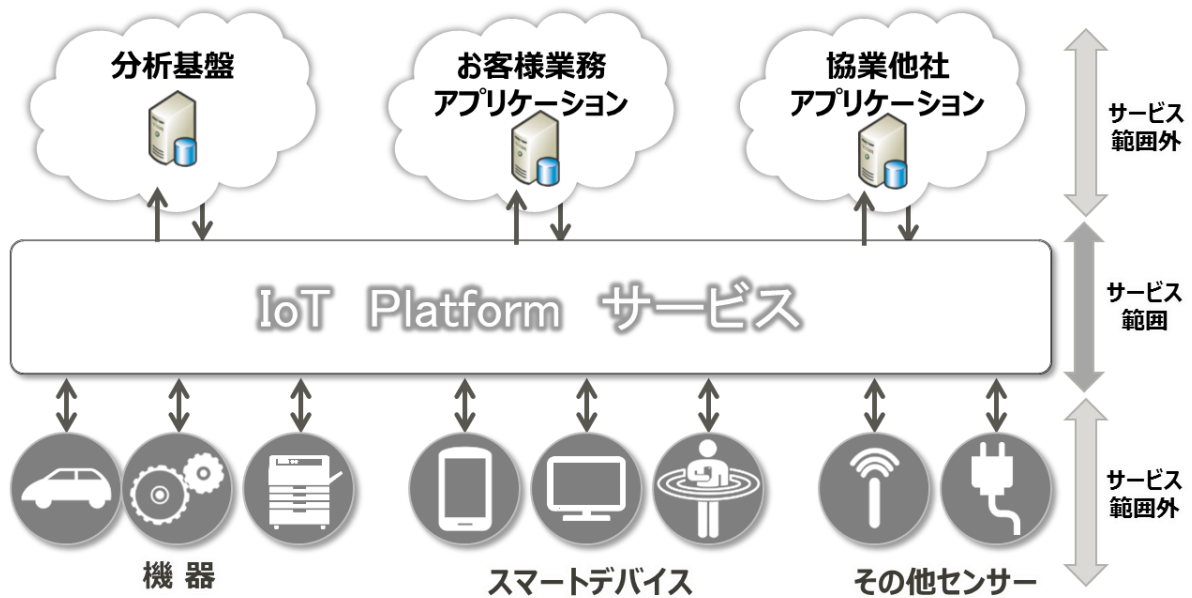


図 1.3 サービス範囲

1.4. ドキュメント

本サービスにおけるドキュメント構成を示します。

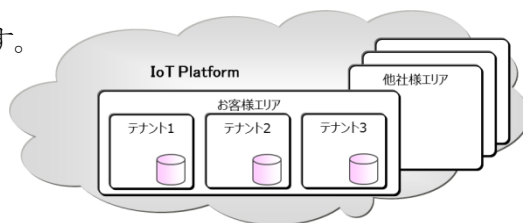
マニュアル名	説明
IoT Platform サービス詳細説明書	本サービスのサービス仕様を説明しています。(本書)
IoT Platform サービスポータル操作マニュアル	WEB インターフェース機能(以下、サービスポータル)に関するマニュアルです。
IoT Platform ユーザーガイド	本サービスを活用するアプリケーション設計・開発を支援するマニュアルです。
IoT Platform API リファレンス	本サービスで提供する API 一覧です。

図 1.4 ドキュメント一覧

第2章 サービス仕様

2.1. マルチテナント

本サービスでは、当社のクラウドにお客様エリアを用意します。
(他お客様との共同利用のベストエフォート型)。
お客様エリアには複数のテナントを作成できます。



2.2. 機能概要

2.2.1. データ収集

お客様テナント内にデータ登録単位である「リソース」を作ります。リソースには、当該リソースに対する権限である「アクセスコード」を作成し、付与する必要があります。

アクセスコードをAPIに付与することにより、該当リクエストは認可され、実行できます。

<権限の種類>

C：リソースやアクセスコードなど、作成できる権限

R：データを参照できる権限

U：データを登録できる権限

D：リソースやアクセスコード、イベントを削除できる権限

L：リソースやアクセスコード、イベントの一覧を取得できる権限

P：リソースの特定ディレクトリ配下に対してデータを登録できる権限

G：リソースの特定ディレクトリ配下に対してデータを参照できる権限

2.2.1.1. データ収集準備

サービスポータルからの操作、およびAPIでの操作が可能です。

※APIでの操作対象は「リソース」「アクセスコード」「イベント」のみ。

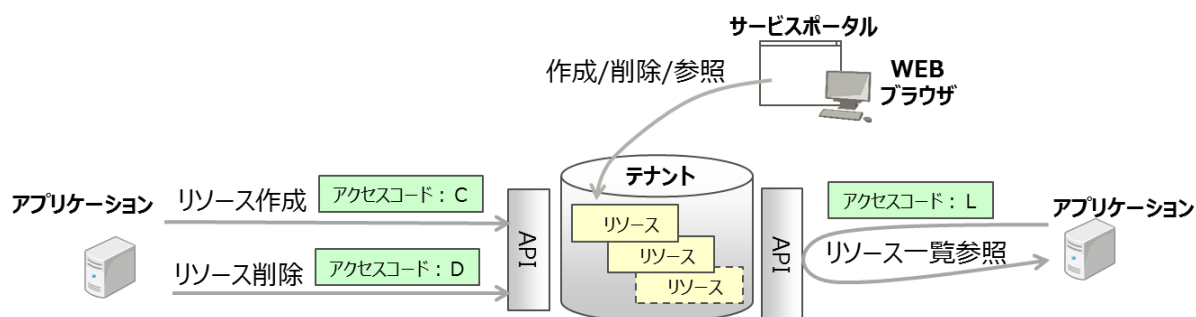


図 2.2.1.1 リソースを管理する

2.2.1.2. データ収集と活用

データの登録や参照はAPIで実行できます。

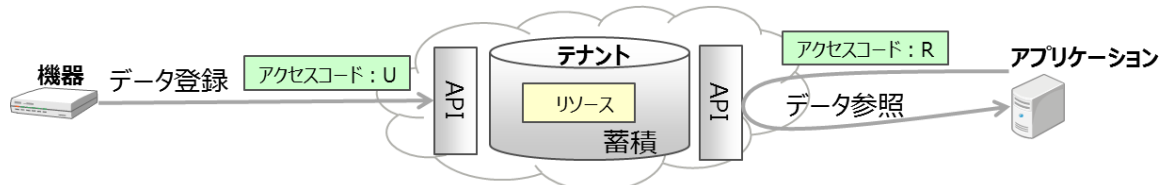


図 2.2.1.2-1 データを蓄積する

本サービス内にデータを蓄積せず、他サービスへ転送することも可能です。

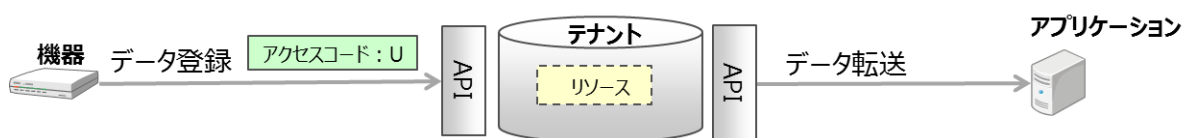


図 2.2.1.2-2 データを転送する

2.2.2. イベント機能

イベントとしてデータの抽出条件を設定することにより、データの登録／更新を契機に抽出条件にマッチする場合にアクションできます。アクションは、Email 通知または指定の API 起動を設定できます。

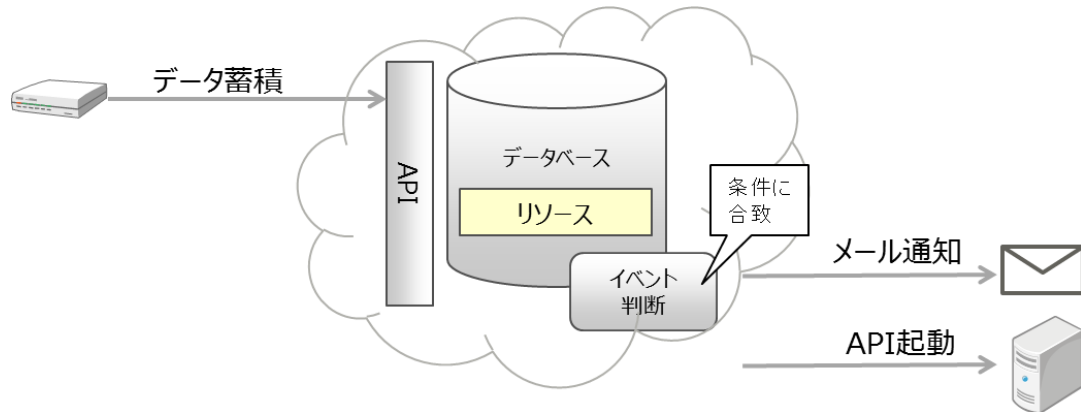


図 2.2.2 イベント機能

2.2.3. アクセス制限

本サービスに対するアクセスに IP アドレスの制限をかけることができます。サービスポータルに対するアクセスおよび、アクセスコードに対して制限を設けることによりリソースに対するアクセスを制限できます。

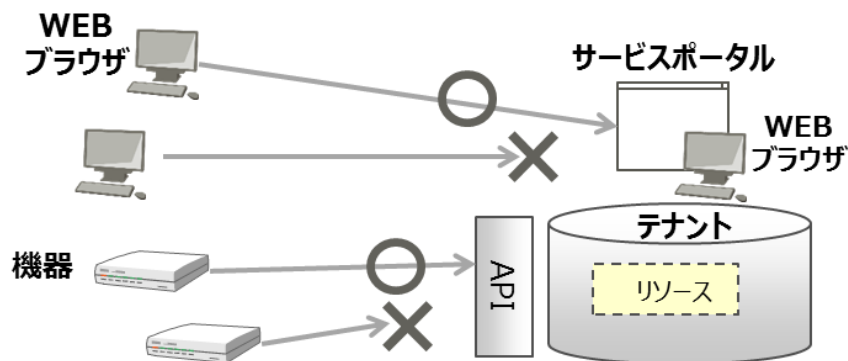


図 2.2.3 アクセス制限

2.2.4. ダイナミックリソースコントローラー

データ収集において、クラウドにかかる負荷によってデータ収集を制御する指針として利用できるリコメンドリソースを提供します。これによってお客様 IT リソースに合わせたデータ収集を可能とします。

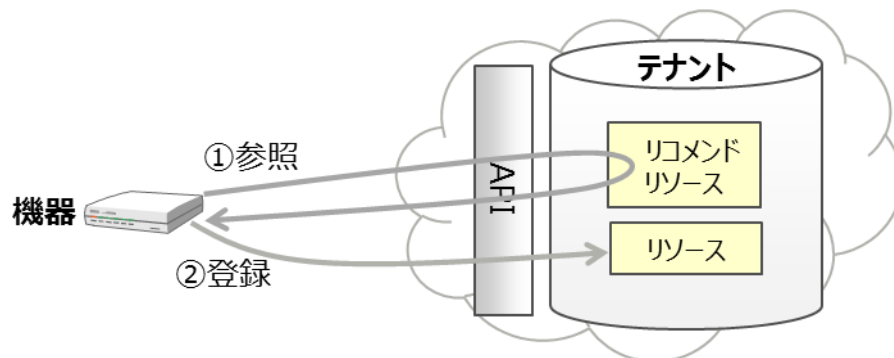


図 2.2.4 ダイナミックリソースコントローラー

2.3. 定義

2.3.1. テナント ID

お客様エリア内のテナントを識別するコードで、本サービス内で一意です。

<定義>

形式	半角英数字
桁数	10(固定)

2.3.2. 管理者アカウント

お客様単位に提供されるデータの管理を行う WEB サイト (以下、サービスポータル) のアカウントです。

<定義> E メールアドレス

形式	E メールアドレス
登録数	制限なし

(補足) 管理者アカウントは、お客様エリア内のすべてのテナントに対する操作権があります。
テナント単位に管理者アカウントを分けたい場合は、別の顧客としてでご契約下さい。

2.3.3. 管理者パスワード

管理者アカウントのパスワードポリシーを以下に示します。

<定義>

使用可能文字種別	以下の4つの文字種別から最低1つずつ使用しなければならない。 英大文字、英小文字、数字、記号 (#, @, -, (,), :, ., _ の8個)
文字数	8~15
初期パスワードの有効期限	制限なし
パスワード有効期限	制限なし

2.3.4. MQTT アカウント

MQTT を利用する場合のアカウントは、テナント ID です。

2.3.5. MQTT パスワード

MQTT パスワードのポリシーを以下に示します。

<定義>

使用可能文字種別	以下の4つの文字種別から最低1つずつ使用しなければならない。 英大文字、英小文字、数字、記号 (#, @, -, (,), :, ., _ の8個)
文字数	8~12
初期パスワードの有効期限	制限なし
パスワード有効期限	制限なし

2.3.6. リソース

データの格納単位を「リソース」、1つ1つのデータを「リソースデータ」、と定義します。

2.3.6.1. リソースの種類と対応データ形式

リソースの種類とその扱いについて以下に示します。

	リソースの種類	登録可能なデータ形式	本サービスでの扱い	
			登録時の処理	参照時の処理
1	リソース_JSON	JSON	BSON形式で保持	JSON形式で出力(注2)
		Csv	JSON形式に変換後(注1)、 BSON形式で保持	JSON形式で出力
		text		
	Binary (256Kbyte以下)			
2	リソース_Binary	Binary	Binary形式で保持	Binary形式で出力
3	リソース(転送)_JSON	JSON	JSON形式で転送	—
		Csv	JSON形式に変換後(注1)、 転送	
		Text		
	Binary (256Kbyte以下)			

表 2.3.6.1 リソースの種類

(注1)各データ形式のJSON形式への変換方法

	データ形式	変換ロジック
1	csv	csvを1つのJSONデータとして変換 ※フォーマットに規定無し (csv自体はRFC4180に従う) ※上部N行削除可
2	text	textデータを1つのJSONデータとして変換
3	Binary (256Kbyte以下)	BinaryデータをBase64エンコードして、1つのJSONデータとして変換

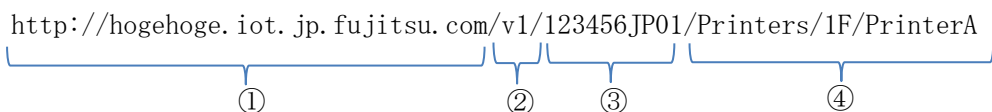
表 2.3.6.1 各データのJSON形式への変換方法

(注2)JSON形式におけるネームの重複利用(コメントの代用)は削除されます。

2.3.6.2. REST API の URI

<定義>

http://hoge.hoge.iot.jp.fujitsu.com/v1/123456JP01/Printers/1F/PrinterA



HTTP におけるリソースの表記は、下記の 4 項目を「/ (スラッシュ)」でつないだ文字列です。

- ① baseURI
サービス申込み時に通知されます。
※SSL 利用の場合は https~となります。 ※SSL は TLS1.2 に対応
- ② APIバージョン
サービス申込み時に通知されます。
- ③ テナント ID
サービス申込み時に通知されます。
- ④ リソースパス
お客様が命名可能な文字列です。階層構造で記載できます。

<定義>

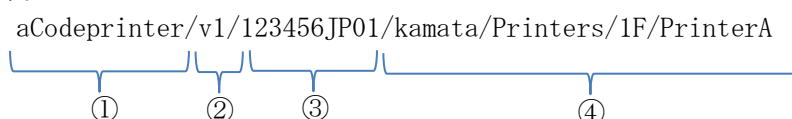
使用可能文字	英大文字、英小文字、数字、 記号 (-(ハイフン), _(アンダー), /(スラッシュ) の 3 個) ※すべて半角のみ。 ※使用可能記号は先頭には使用できない。 ※「/-」、「/_」のように、「/」の後に「-」と「_」と「/」は指定不可。 ※転送リソース作成時は自動で _fwd/ が先頭に付与される。 ※バイナリデータ選択時は自動で _bin/ が先頭に付与される。
文字数	1~128 文字 ※転送リソースの場合、_fwd/ を含めて最大 128 文字。 ※バイナリデータの場合、_bin/ を含めて最大 128 文字。
制限	テナント内で一意

(補足) HTTP においてはヘッダ部にアクセスコードを設定する必要があります。

2.3.6.3. MQTT のトピック

<定義>

aCodeprinter/v1/123456JP01/kamata/Printers/1F/PrinterA



MQTT におけるリソースの表記は、以下の 3 項目を「/ (スラッシュ)」でつないだ文字列です。

- ① アクセスコード
2.3.7 章を参照 (後述)
- ② APIバージョン
2.3.6.2②を参照
- ③ テナント ID
2.3.6.2③を参照
- ④ リソースパス
2.3.6.2④を参照

2.3.7. アクセスコード

アクセスコードとは、リソースやアクセスコード、イベント設定に対する操作権限を示すコードです。サービスポータルと API で作成できますが、最初の1つはサービスポータルから設定が必要です。

〈定義〉

使用可能文字	英大文字、英小文字、数字 ※すべて半角のみ
文字数	3~48 文字
制限	テナント内で一意

アクセスコードはリソースを指定して設定しますが、その他の設定内容を以下に示します。

2.3.7.1. 操作権限

操作権限の種類と内容を以下に示します。

操作権限	内容	操作対象	対応プロトコル
作成 (C:Create)	<ul style="list-style-type: none"> 作成権限 指定リソース<u>配下</u>に対して有効 (注 1) 	リソース アクセスコード イベント	HTTP/HTTPS
参照 (R:read)	<ul style="list-style-type: none"> リソースに蓄積されたデータを参照する権限 指定リソースのみに対して有効 	リソースデータ	HTTP/HTTPS MQTT/MQTTS (注 2)
更新 (U:update)	<ul style="list-style-type: none"> リソースにデータを登録する権限 リソースに蓄積されたデータを更新する権限 (MQTT/MQTTS は非対応) リソースに蓄積されたデータを削除する権限 (MQTT/MQTTS は非対応) 指定リソースのみに対して有効 	リソースデータ	HTTP/HTTPS MQTT/MQTTS
削除 (D:delete)	<ul style="list-style-type: none"> 削除権限 指定リソース<u>配下</u>に対して有効 (注 1) 	リソース アクセスコード イベント	HTTP/HTTPS
リスト取得 (L:list)	<ul style="list-style-type: none"> 指定リソース配下のリソース一覧の取得権限 指定リソース<u>配下</u>に対して有効 (注 1) 	リソース アクセスコード イベント	HTTP/HTTPS
複数更新 (P:put)	<ul style="list-style-type: none"> U権限を指定したリソースURL (ディレクトリ) 配下の複数のリソースに与える権限 	リソースデータ	HTTP/HTTPS MQTT/MQTTS
複数参照 (G:get)	<ul style="list-style-type: none"> R権限を指定したリソースURL (ディレクトリ) 配下の複数のリソースに与える権限 	リソースデータ	HTTP/HTTPS MQTT/MQTTS

(注 1) 矛盾のある権限が設定された場合、権限の強い方が適用されます。

(注 2) バイナリデータに対する更新時刻指定のデータ一覧取得は MQTT/MQTTS 非対応です。

表 2.3.7.1 操作権限一覧

2.3.7.2. 操作権限の組み合わせ

「CDL」「L」「R」「U」「P」「G」単位で権限を組み合わせることができます。

2.3.7.3. プロトコル制限

アクセスを許可するプロトコルを設定することができます。

プロトコルを制限しない	プロトコルを制限しない設定
プロトコルを制限する	HTTP/HTTPS/MQTT/MQTTS を組み合わせて設定可

2.3.7.4. クライアント証明書

サービスポータルから発行／またはお客様が手配したクライアント証明書を、アクセスコードに登録することによりクライアント認証を行うことができます。

クライアント認証は HTTPS プロトコルのみ利用できます (HTTP/MQTT/MQTTS 非対応)。

2.4. サービスポータル

本サービスの利用に必要な設定をサービスポータル画面(WEB-IF)から実行できます。

※詳細は「IoT Platform サービスポータル操作マニュアル」を参照ください。

※複数テナント契約時、サービスポータルの URL が同一であればテナントを切替えて利用できますが、異なる場合はできません。

2.4.1. 利用条件

サービスポータルの利用条件を以下に示します。

	項目	条件	備考
1	利用手段	WEBブラウザ	—
2	アクセス	インターネット	—
3	対応言語	日本語/英語	デフォルト言語はRegionによる。 ログイン後に設定可。

表 2.4.1 サービスポータルの利用条件

2.4.2. 動作確認

サービスポータルの動作確認は以下で実施しており、記載以外の条件における動作保証はありません。

	対応OS	ブラウザ	備考
1	Windows 10/11	Google Chrome	バージョン 123以降

表 2.4.2 サービスポータルの動作確認

2.4.3. 管理機能

サービスポータルで提供する機能を以下に示します。

	管理機能	内容	備考
1	アカウント	・サービスポータル利用のためのアカウントの作成・削除 ・パスワードの再発行 ・アカウントに紐づくクライアント証明書の追加・変更・削除	—
2	リソース	・リソースの作成/変更/削除、一括登録 ・リソース内データの自動削除設定 (1~9999日設定可) ※設定日時+最大1日のデータが参照できる ・リソース一覧の表示/検索/ダウンロード	—
3	アクセスコード	・アクセスコードの作成/変更/削除、一括登録 ・アクセスコード一覧の表示/検索/ダウンロード ・クライアント証明書の登録	—
4	イベント	・イベントの作成/変更/削除 ・イベント一覧の表示/検索	—
5	ログ	・サービスポータルの操作履歴の表示/検索/ダウンロード ・月次の利用実績サマリの表示 ・月次の利用実績の画面表示 ・日時の利用実績のログファイルダウンロード(課金確認用) ・システムログの画面表示 (本システム内部でエラー終了する可能性のあるリクエストの確認用)	—
6	アクセス制限	・サービスポータルアクセス制限条件の作成/変更/削除 ・アクセスコードアクセス制限条件の作成/変更/削除	—
7	分散設定	・ダイナミックリソースコントローラーを利用するための設定/変更/削除 ・分散ポリシーの有効/無効の設定	—
8	共通設定	・MQTTパスワードの表示/変更 ・エラーログ蓄積ON/OFFの切替 ・CORS機能ON/OFFの切替 ※CORS: サーバを経由したアクセスを許容する仕様 (CORSへの対応可否はブラウザに依存)	—
9	クライアント証明書	・クライアント証明書の発行	—

表 2.4.3 管理機能概要

2.4.3.1. システムログの用途

システムログは主に、お客様アプリケーション開発時に本サービス内部の処理によってリクエストが破棄されていないか確認することを目的として提供する、本サービスシステムのログです。

項目	内容
1 用途	以下の確認 ・ イベント転送結果 (API/Email) ・ MQTT結果
2 参照条件	画面表示のみ
3 ログ表示条件	参照日を含む 2 日間のうち、該当テナントに関するログで、システム内に存在しているものの中から、最新の 5000 件まで ※2日間のログを保障するものではない。

表 2.4.3.1 管理機能概要

2.5. API

リソースやアクセスコード、イベント設定に対する操作を API で実行できます。

リクエストの認可は、リソースに対して権限をもつアクセスコードを API に組み込むことによって実現します。

2.5.1. HTTP REST インターフェース

HTTP および HTTPS に対応しています。提供インターフェースを以下に示します。

	操作	Method名	アクセスコードとの関連性
管理系	リソース作成	POST	Cで許可
	リソース更新	PUT	Cで許可
	リソース削除	DELETE	Dで許可
	アクセスコード作成	POST	Cで許可
	アクセスコード更新	PUT	Cで許可
	アクセスコード削除	DELETE	Dで許可
	イベント作成	POST	Cで許可
	イベント更新	PUT	Cで許可
	イベント削除	DELETE	Dで許可
	リソース一覧参照	GET	Lで許可
	アクセスコード一覧参照	GET	Lで許可
	イベント一覧参照	GET	Lで許可
データ系	リソースデータ登録 (JSON)	PUT	UまたはPで許可
	リソースデータ参照 (JSON)	GET	RまたはGで許可
	リソースデータ更新 (JSON)	PUT	UまたはPで許可 (注)
	リソースデータ削除 (JSON)	DELETE	Dで許可
	リソースデータ転送 (JSON)	PUT	Uで許可
	リソースデータ登録 (Binary)	PUT	UまたはPで許可 (注)
	リソースデータ参照 (Binary)	GET	RまたはGで許可
	リソースデータ一覧参照 (Binary)	GET	RまたはGで許可
リソースデータ削除 (Binary)	DELETE	Dで許可	

(注) 同一時刻に対する更新について、JSON データは複数データとして/Binary データは上書きして、蓄積されます。

表 2.5.1 REST IF 一覧

2.5.2. MQTT インターフェース

MQTT および MQTTS に対応しています。提供インターフェースを以下に示します。

	操作	Control Packet名	アクセスコードとの関連性
データ系	リソースデータ登録 (JSON)	PUBLISH	UまたはPで許可
	リソースデータ参照 (JSON)	SUBSCRIBE +PUBLISH(注)	RまたはGで許可
	リソースデータ削除 (JSON)	非対応	
	リソースデータ転送 (JSON)	PUBLISH	Uで許可
	リソースデータ登録 (Binary)	PUBLISH	UまたはPで許可
	リソースデータ参照 (Binary)	SUBSCRIBE +PUBLISH(注)	RまたはGで許可
	リソースデータ削除 (Binary)	非対応	

(注) クライアントからの SUBSCRIBE を経た本サービスからの PUBLISH

表 2.5.2 MQTT IF 一覧

2.5.3. リクエストの制限

リクエストに関する制限について以下に示します。

	リクエストの種類	データサイズ上限	その他の制限
1	リソース一覧(リスト)参照	—	1 回のリクエストで 1000 件まで
2	リソースデータ登録 (JSON)	JSON 形式で 256Kbyte かつ BSON 形式で 256Kbyte	—
3	リソースデータ参照 (JSON)	JSON 形式で 16Mbyte	1 回のリクエストでデータサイズ上限、または 1000 件まで
4	リソースデータ登録 (転送_JSON)	JSON 形式で 256Kbyte	—
5	リソースデータ登録 (Binary)	Binary 形式で 100Mbyte	—
6	リソースデータ参照 (Binary)	Binary 形式で 100Mbyte	1 回のリクエストで 1 データのみ取得可
7	リソースデータ一覧参照 (Binary)	—	1 回のリクエストで 1000 件まで
8	イベント機能での API 起動または Email 通知 (JSON)	JSON 形式で 256Kbyte	—

表 2.5.3 リクエストの制限

2.5.4. HTTP-IF におけるリソースデータ登録と MQTT-IF の関係

本サービスでは、HTTP-IF で当該リソースにデータ登録時、当該リソースに対して MQTT-IF で subscribes しているクライアントに対して publish されます。

但し、HTTP-IF の一括登録 API (=bulk) / binary データの登録は対象外です。

※機能エンハンスによって binary データが対象になる可能性があります。

2.5.5. 同時刻のデータの扱い

時刻はミリ秒(3桁)まで区別します。

(1) リソース_JSON

同一リソースに対して同じ時間にデータ登録が実行された場合、複数登録されます。同一時刻のデータが複数存在する場合、時刻指定の操作について以下ようになります。

	操作	動作	備考
1	更新	指定時刻のデータのうちのどれか1つが更新対象となる	対象となるデータは不定
2	参照	指定時刻のデータすべて返却	—
3	削除	指定時刻のデータすべて削除	—

表 2.5.5(1) 同時刻のデータの扱い(JSON)

(2) リソース_Binary

同一リソースに対して同じ時間にデータ登録が実行された場合、上書きされます

2.6. データの転送先設定

リソース作成時に「リソース(転送)」のリソース種別を選択することで、本サービス内にデータを蓄積せず、他サービスに転送することができます(転送先 IF は HTTP/HTTPS のみに対応)。データ転送先の設定項目を以下に示します。

※本項目を設定せず(転送をせず)に MQTT の Subscribe でデータ取得する方法も可能です(2.5.4 参照)。

	項目	設定方法	備考
1	URI	自由入力	半角のみ、最大254文字
2	メソッド	画面から選択	空/POST/PUT/GET/DELETE/HEAD/ OPTIONS/TRACE
3	認証ID	自由入力	半角のみ、最大20文字 ※Basic認証のみ対応
4	認証パスワード	自由入力	半角のみ、最大20文字 ※Basic認証のみ対応
5	ヘッダ名	自由入力	半角のみ、最大20文字。最大10個。
6	ヘッダ値	自由入力	半角のみ、最大512文字。最大10個。

表 2.6 転送先 API の設定項目

2.7. イベント機能

リソースの中のデータに対する検出条件の設定、および、検出時のアクションを設定します。

2.7.1. 対象操作

イベント機能の対象になるリソースへの操作を以下に示します。

※リソース(転送)_JSON にイベントは設定できません。

	操作	イベントの対象操作	備考
1	リソースデータ登録	対象	—
2	リソースデータ参照	対象外	—
3	リソースデータ更新	対象	—
4	リソースデータ削除	対象外	—

表 2.7.1 イベント機能の対象操作

2.7.2. 検出条件設定

検出条件として、以下の項目が設定できます。

※検出解除とは、1回検出後、同じイベントでアクションを実行しない機能です。

この条件が未設定の場合は、検出の都度、定められたアクションを実施します。

※リソース_Binary に対する検出条件設定はできません。

	項目	設定方法	備考
1	対象リソース	画面の検索機能による選択	最大1個
2	対象時間	年月日時間分秒を画面で選択／自由入力	—
3	データ位置	データの中の対象となる位置を自由入力	JSONPath形式で入力
4	検出の文字種別	データが数字か文字列かを選択	—
5	検出の値	自由入力	(注1)
6	検出の判定条件	画面で選択	(注2)
4	検出解除の文字種別	データが数字か文字列かを選択	—
5	検出解除の値	自由入力	(注1)
6	検出解除の判定条件	画面で選択	(注2)

(注1) 文字種別を[数値]にした場合、半角数字のみ入力可

※ 文字種別を[数値]にした場合[一致/不一致/以上/以下/未満/超え]、文字種別を[文字列]にした場合[完全一致/部分一致]の利用が可能。

表 2.7.2 検出条件の設定項目

2.7.2.1. Email 通知の設定

Email アクションに対して、以下の項目が設定できます。

	項目	設定方法	備考
1	Emailアドレス	自由入力	メールアドレス形式のみ可 半角のみ、最大254文字
2	件名	自由入力	半角／全角、0～256文字
3	本文	自由入力	半角／全角、1～140文字

表 2.7.2.1 Email 通知の設定項目

(補足) Email での通知時は以下の情報が添付ファイル(JSON形式の text)で付加されます。

イベント ID/イベントが発生したリソースパス/リソースの更新時刻/データの実体

※但しデータサイズが 10Mbyte を超えた場合は Email 送信されません。

2.7.2.2. API 起動の設定

API 起動のアクションに対して、以下の項目が設定できます(起動の IF は HTTP/HTTPS のみに対応)。

	項目	設定方法	備考
1	URI	自由入力	半角のみ、最大254文字
2	メソッド	画面から選択	POST/PUT/GET/DELETE/HEAD/OPTIONS/TRACE
3	認証ID	自由入力	半角のみ、最大20文字 ※Basic認証のみ対応
4	認証パスワード	自由入力	半角のみ、最大20文字 ※Basic認証のみ対応
5	ヘッダ名	自由入力	半角のみ、最大20文字。最大10個。
6	ヘッダ値	自由入力	半角のみ、最大512文字。最大10個。
7	ボディ一部	自由入力	半角／全角、最大1024文字、日本語入力可

表 2.7.2.2 API 起動の設定項目

2.7.3. イベント発行時の添付データ

イベント条件に合致した場合、イベント発行の契機となったリソースデータの添付有無を示します。

	イベント発行の契機	アクション	動作
1	リソースデータ登録 (リソース_JSON)	E-mail通知	リソースデータをファイル添付
		API起動	リソースデータをボディー部に追加。
2	リソースデータ登録 (リソース_Binary)	E-mail通知	リソースデータのファイル添付無し。
		API起動	リソースデータのボディー部への追加無し。

表 2.7.3 イベント発行時のリソースデータ添付有無

2.8. アクセス制限機能

アクセスを許可する IP アドレスの範囲（単体含む）を設定できます。

設定できる項目を以下に示します。

2.8.1. サービスポータルへのアクセス制限

ユーザーに対して許可する IP アドレスを設定できます。

	項目	設定方法	備考
1	許可IPアドレス	自由入力	開始IPアドレス～終了IPアドレス
2	IP範囲設定個数	最大5個	—
3	対象ユーザー	画面から選択	—

表 2.8.1 サービスポータルへのアクセス制限設定項目

2.8.2. リソースへのアクセス制限

リソースへのアクセスを制限する方法として、アクセスコードに対して許可する IP アドレスを設定できます。※但し MQTTS IF には非対応で、MQTTS リクエストで該当アクセスコードを使うと切断されます。

	項目	設定方法	備考
1	許可IPアドレス	自由入力	開始IPアドレス～終了IPアドレス
2	IP範囲設定個数	最大5個	—
3	対象アクセスコード	画面から選択	—

表 2.8.2 アクセスコードへのアクセス制限設定項目

2.9. ダイナミックリソースコントローラー機能（分散機能）

本サービスでは、本サービスに対する負荷情報を計測種別として集計し、その値をお客様が設定した条件（エッジコンピューティング条件）と比較してリコメンドとして提供します。お客様はリコメンドを利用することにより、お客様の IT リソース内で最適なデータ収集を行うアプリケーションを開発できます。

お客様の分散条件は分散ポリシーとして設定でき、設定項目を以下に示します。

なお、分散ポリシーはテナントに1つであり、リコメンドを格納するリコメンドリソースは分散ポリシー内に3つ設定できます。エッジコンピューティング条件はリコメンドリソース毎に設定できます。

	項目	設定方法	備考
1	有効/無効	画面から選択	分散ポリシーの有効/無効を切り替えることができます。 [注意]リコメンドや測定負荷情報をリソースに書き込むため、API課金が発生します。利用しない場合は分散ポリシーを無効にすることで稼働しないようにできます。 なお、負荷リソースおよびリコメンドリソースへの書き込みはリコメンド周期で実施しますが、リコメンドリソースへの書き込みは、リコメンドおよび通知文字列に変更があった場合のみ実施します。
2	リコメンド周期	自由入力	1~1440分
3	算出期間	自由入力	1~1440分 ※リコメンド周期以上の値
4	負荷リソース	画面から選択 または 自由入力	お客様テナントに対する負荷を書きこむリソースやアクセスコードを設定。

表 2.9-1 分散ポリシーの設定項目

	項目	設定方法	備考
1	有効/無効	画面から選択	分散ポリシーの中のリコメンドリソース単位に有効/無効を切り替えることができます。
2	リコメンドリソース	画面から選択 または 自由入力	お客様テナントに対するリコメンドを書きこむリソースやアクセスコードを設定。
3	計測種別	画面から選択	TPS(transaction/second) /BPS(bit/second)
4	エッジコンピューティング条件、またその解除条件の文字種別	固定	数値のみ
5	エッジコンピューティング条件、またその解除条件	自由入力	半角数字、最大10桁。
6	エッジコンピューティング条件検出判定の不等号、またその解除条件検出判定の不等号	画面から選択	空/一致/不一致/以上/以下/未満/超え
7	エッジコンピューティング条件合致時、またその解除条件合致時の通知文字列	自由入力	最大 10 文字、日本語可。

表 2.9-2 リコメンドリソースの設定項目

2.10. エラーログ蓄積機能

本サービス内および通信先の影響でリクエストが欠損した場合、エラー情報としてエラー収集用リソース「_error」に蓄積します。該当リソースを参照することによりエラーの発生を確認できます。

<対象>

- ・ イベント機能 (E-Mail 送信エラー、API 起動エラー)
※内部エラーは検出できない場合があります。
- ・ MQTTS/MQTTSの内部エラー
- ・ 転送エラー

2.11. CORS対応

通常、Javascript はダウンロード元の Web サーバ以外とは通信できないため、ブラウザから直接本サービスの API にアクセスできません。それを可能にする仕組みである CORS (Cross-Origin Resource Sharing) に対応しています。以下に、CORS機能の設定項目を示します。

	項目	設定方法	備考
1	有効/無効	画面から選択	—

表 2.11 CORS の設定項目

2.12. クライアント証明書発行機能

本サービスでクライアント証明書を発行できます。

2.13. 注意事項 (仕様制限)

2.13.1. API で使用する文字コード

UTF-8 のみサポートしています。

2.13.2. 時刻

世界標準時 +00:00 (UTC) を採用しています。

2.13.3. 1 リソースに蓄積するデータ量の考え方 (JSON データ)

★重要★ 1 リソースに蓄積するデータ量に上限は設けておりませんが、JSON データの検索性能は 1 リソース内の蓄積データ量に反比例しますので、利活用に必要な性能を考慮してリソース設計いただく必要があります。基本的にリソースはデバイス (1 つの連続したデータ) 毎に作成することを想定しておりますが、データ蓄積日数を考慮の上 1 デバイスから収集されるデータ量が多く見込まれる場合はリソースを分けるようにしてください (蓄積日数も考慮して 1 リソース当り 100MByte 以下を推奨)。なお、例えば複数のデバイスから収集されるデータを 1 つのリソースに蓄積し検索母体が大きくなるとタイムアウトでデータが取得できなくなります。詳細は「IoT Platform ユーザーガイド」を参照してください。

2.13.4. [MQTT のみ] QoS

MQTT の QoS について、0/1/2 いずれでも受け付けますが、セッション切断時には保障されません。また、受信後のシステム内処理中のエラーによっても、保障されないことがあります。

2.13.5. [MQTT のみ] コネクション断時の振る舞い

MQTT コネクションはサーバの保守等で切れた場合、retain が消える場合があることを考慮してください。

2.13.6. [MQTT のみ] 課金対象メッセージ

MQTT における API 利用回数及び SSL 利用回数は、以下のメッセージが課金対象です。

- CONNECT
- PUBLISH
(クライアントから IoT-PF に向けたメッセージ、または IoT-PF からクライアントに向けたメッセージ)
- SUBSCRIBE
- PINGREQ

2.13.7. その他

本誌に記載がない場合、現状仕様が優先されます。

第3章 制限事項

3.1. 目安を超えた使い方をする場合の対応

データの登録や参照頻度について、以下の各要素に対する目安を1つでも超えた使い方を想定される場合は、お客様の利用シーンが実現できずご利用いただけない場合があります。当社営業経由で事前にご相談ください。

なお、通信頻度についてシステム制限がかかります。通信頻度が一定時間目安を超えた場合すべてのリクエストがエラー返却(HTTP/HTTPS)またはデータ破棄(MQTT/MQTTS)されますのでご注意ください。

<目安>

1 通信におけるデータ量	256kByte	
通信頻度 (ピーク)	データ系 API	契約に依る
	管理系 API※	1 回/秒
登録リソース数	10,000 個	
1 リソース内データ蓄積容量	100Mbyte	
同時接続数	1000	

※リソースやアクセスコード、イベントを作成・更新・削除・参照する API を指します。

3.2. 過度な集中利用の禁止

過度な集中利用を禁止します。本サービスに深刻なダメージを与えるような集中利用があった場合アクセスを拒否する場合があります (3.1 に記載の目安を定常的に超える場合も含む)。

3.3. イベント機能/転送機能利用時の注意

データ登録を契機として発生するイベントまたは転送について、以下の制限があります

<イベント>

- 送信先に設定する API の応答性能によって、イベントリクエストが破棄される場合があります。

<転送>

- 転送先に設定する API の応答性能によって、リクエストが破棄される場合があります。

※データ登録リクエスト数が、イベントの設定先の応答性能を上回る場合など。

※特に SSL で通信を行う場合は性能劣化にご注意ください。

3.4. データの保障

本サービスではデータのバックアップや災害対策など行っておりません。万一お客様のデータが消失した場合保障できかねますのでご了承ください。データ保全をしたい場合は、お客様アプリケーション等にて適切な対処をお願いします。また、いかなる場合においてもデータの移行は実施いたしかねます。

3.5. データの到達性

本サービスではリクエスト受信応答を返した後に、サービス内で欠損する場合があります。特に転送やイベント送信は設定した送信先に送信を試みますが、リクエスト送信元に成功/失敗はわかりません。

3.6. API のクエリー仕様変更の可能性

大量に蓄積されたデータのフルテキストを対象とするようなクエリーは、今後課金単価があがったり制限がかかる (インデックス指定で1万レコードに絞ってから実行する等) 可能性があります。アプリケーション開発においてご注意ください。※現在インデックスは時刻とリソースのみにかかり、アプリケーションでインデックスの指定はできません。

3.7. データの削除

解約後、すべてのデータは当社が適宜削除します。

確実に削除したい場合は解約前に削除してください。

3.8. DoS 対策

同一ネットワーク (/24) からのアクセスは 300 リクエスト/秒に制限しています。

第4章 重要事項説明

4.1. サービス提供時間

本サービスは24時間365日稼動しておりますが、計画メンテナンスや緊急メンテナンス実施時間帯はサービス停止する場合があります。数時間かかる場合もありその間サービスをご利用いただけません（データが蓄積できない場合があります）。なお、お客様のご事情でメンテナンス時間の変更はできません。

4.1.1. 計画メンテナンス

基本的に2週間前までに計画停止をご連絡します。

4.1.2. 緊急メンテナンス

障害発生などの要因により緊急でメンテナンス作業を実施させていただく場合があります、直前または事後の報告になります。この場合、障害報告書を提出することはできません。

4.2. サポート範囲

お客様が用意された通信機器や情報収集端末の問題に関しては弊社ではサポートできませんのでご注意ください。ご購入された窓口でサポートをお受けください。

4.2.1. サポートデスク利用時の必要情報

サポートデスクに連絡いただく際は、以下情報をご準備ください。

	項目	情報
1	契約サービス名	IoT Platformサービス
2	テナントID	お客様テナントを識別する10文字の識別子
3	お客様企業名	お客様企業名称
4	お客様担当者氏名	お客様担当者氏名
5	ご連絡先電話番号	お客様に連絡可能な電話番号
6	お問合せ内容	①ご利用種別（問い合わせ または 障害のご連絡） ②内容 ※障害のご連絡の場合は可能な限り詳しい情報をお伝えください 「発生日時」「テナントID」「対象のリソース」「操作手順」など。

4.3. 蓄積データの正当性について

本サービスで収集蓄積される情報の内容はお客様にて選定するものですので、情報収集にあたってのエンドユーザへの必要な許可等はお客様にて実施いただくものとします。

また、近年、諸外国では個人情報を中心としてデータの域外移動を禁止する法令等の制定の動きがありますが、該当法令の確認、遵守等はおお客様の責任において対応されるものとします。

（本サービスでは個人情報、秘密情報の保存は推奨しません）

4.4. アクセスコードの管理

アクセスコード、管理者アカウントパスワード、クライアント証明書秘密鍵が漏洩すると、意図しないアクセスによる課金やデータ流出が発生する恐れがあるため、お客様の責任で管理を行ってください。

4.5. お客様データの閲覧

本サービスではデータ操作のAPI実行やイベント機能の実現においてお客様データ中身を参照しますが、本機能を実現する用途のみに使用し他の用途には用いません。

4.6. ダイナミックリソースコントローラー利用時の課金について

ダイナミックリソースコントローラーを利用するとリコメンドリソースおよび負荷リソースへの書き込みに対して API 課金が発生します。課金量はお客様が設定する分散ポリシーに依存しますのでご注意ください。なお本機能を利用しない場合は分散ポリシーを無効にすることによって課金停止できます。

4.7. 蓄積データの利用

本サービスの実施期間中に取得した各種情報については、サービス品質および提供機能の改善、統計化した実績の公表を目的として、お客様の承諾および対価の支払なしに利用いたします。なお、お客様データそのものを無断で利活用することはありません。

情報取得箇所	対象データ
サーバ 通信機器	通信情報（時刻、アクセス回数、通信量） サーバ性能情報（負荷、リソース利用状況） サーバシステムログ 本サービスを構成するアプリケーション／ミドルウェアログ サービスポータル利用頻度および内容／API（内部的なものを含む）利用回数および種別・パラメータ／ディスク使用量、など

4.8. イベント設定の削除

イベント機能に実在しないメールアドレスを登録しないでください。その場合、イベント設定が削除されますのでご注意ください。

以上