

Alibaba Cloud 物#网平台

プロダクト紹介

Document Version20191115

目次

1 IoT Platform とは.....	1
2 アーキテクチャ.....	4
3 用語集.....	6
4 利点.....	9
5 制限事項.....	11

1 IoT Platform とは

IoT Platform は、**Alibaba Cloud** 上のデバイス管理プラットフォームであり、**IoT** アプリケーションの開発者が、エンドデバイス (センサー、アクチュエーター、組み込みデバイス、スマート家電など) とクラウド間の双方向通信を、データチャネルにより実現することを可能にします。

IoT Platform の利点は次のとおりです。

デバイス接続

IoT Platform は、ユーザーのデバイスと **Alibaba Cloud** とを接続するデバイス **SDK** を提供します。

- ・ **2G/3G/4G**、**NB-IOT**、または **LoRa** テクノロジーを使用するネットワーク機器を接続するための多様なソリューションを提供し、異機種間ネットワークに接続されたデバイスの管理を合理化します。
- ・ **MQTT** や **CoAP** プロトコルなど、各種のプロトコルをサポートするデバイス **SDK** を提供します。これにより、永続的接続によるリアルタイム同期機能だけでなく、一時的な接続による省エネルギー化も実現します。
- ・ 各種のオープンソースのプログラミング言語をサポートし、所望のプログラミング言語を使用して多様なチップに組み込み可能な **SDK** ガイドを提供します。これにより、企業はさまざまなチップを備えたデバイスを **IoT Platform** に接続できます。

デバイス通信

デバイスは **IoT Platform** を使用して、**IoT Hub** 経由でクラウドとの双方向通信を行います。このプラットフォームにより、デバイスとクラウド間のアップロード/ダウンロードチャネルを実現し、デバイスとクラウドとの間でスムーズかつ信頼性の高い双方向通信を保証します。

デバイス管理

IoT Platform は、デバイス登録、機能定義、スクリプト解析、オンラインデバッグ、リモート設定、ファームウェアアップグレード、リモートメンテナンス、リアルタイムモニタリング、グループ化、デバイス削除など、デバイスのライフサイクル全体を管理します。

- ・ アプリケーション開発を簡素化するための **Thing Specification Language** が用意されています。
- ・ デバイスの状態が変化したときに通知をプッシュします。

- ・ データストレージ機能を提供し、膨大な量のデバイスデータのリアルタイム送受信を簡単に実現します。
- ・ **Over-The-Air (OTA)** 技術に基づくデバイスのリモートアップグレードをサポートします。
- ・ デバイスシャドウ機能によりデバイスとアプリケーションを分離し、ワイヤレス接続が不安定な場合に対処します。

セキュリティ

多層セキュリティ戦略により、クラウドに接続されたデバイスのセキュリティを確保します。

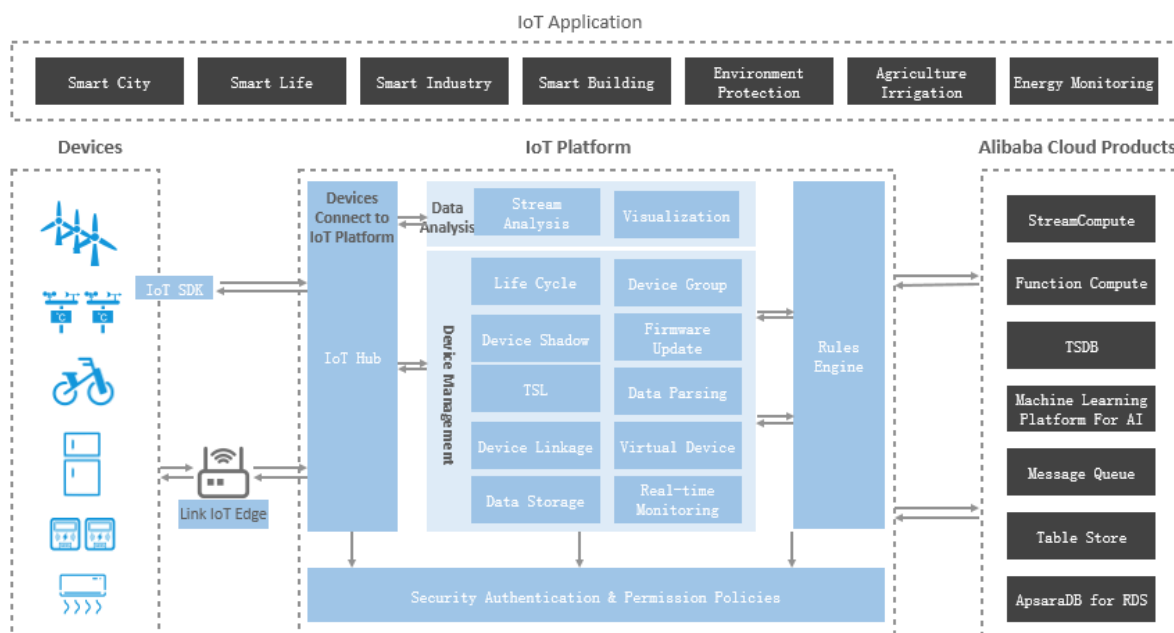
- ・ 認証
 - チップレベルのセキュリティソリューション (**ID²**) と **DeviceSecret** のメカニズムにより、**DeviceSecret** への不正侵入を防止します。セキュリティレベル: 高。
 - デバイス固有証明書による認証メカニズムにより、デバイスに対する攻撃を防止します。このメカニズムは、デバイス証明書 (**ProductKey**、**DeviceName**、および **DeviceSecret** で構成される) のプールが大量生産のデバイスチップにインストールされる場合に適用されます。セキュリティレベル: 高。
 - プロダクト固有証明書による認証メカニズムを提供し、デバイスの攻撃リスクを軽減します。このメカニズムは、デバイス証明書 (**ProductKey**、**DeviceName**、および **DeviceSecret** で構成される) のプールを大量生産のデバイスチップにインストールできない場合に適用されます。セキュリティレベル: 中。
- ・ 通信セキュリティ
 - **TLS (MQTT や HTTP など)** と **DTLS (CoAP など)** プロトコルを使用する各種のデータチャンネルをサポートし、データのプライバシーと整合性を保証します。これは、ハードウェアのリソースが十分であり、デバイスの電力消費が問題にならない場合に適用されます。セキュリティレベル: 高。
 - **TCP (MQTT など)** および **UDP (CoAP など)** プロトコルを使用するカスタムデータ対称暗号化チャンネルをサポートします。これは、ハードウェアのリソースが不十分で、デバイスの電力消費が制限される場合に適用されます。セキュリティレベル: 中。
 - 権限管理を提供し、デバイスとクラウド間の通信が安全であることを保証します。
 - 通信リソースをデバイスレベルで分離し (**Topic など**)、デバイス上での不正な操作を防ぎます。

ルールエンジンを使用した SQL 解析とデータ転送

IoT Platform は、ルールエンジンを使用して他の **Alibaba Cloud** サービスと統合することができます。**Alibaba Cloud** サービスへデバイスデータ転送し、データの保存やコンピューティングを行うための簡単なルールを設定できます。ルールエンジンには以下の機能があります。

- ・ ルールを使用してデバイス間で **M2M** 通信を確立します。
- ・ **MQ (Message Queue)** にデータを転送し、アプリケーションが確実にデバイスデータにアクセスできるようにします。
- ・ **Table Store** にデータを転送し、データ取得と構造化ストレージの統合をサポートします。
- ・ **Function Compute** にデータを転送し、データ取得とイベント駆動型処理の統合をサポートします。

2 アーキテクチャ



IoT Hub

IoT Hub は、デバイスと **Alibaba Cloud IoT Platform** サービスとの接続に使用されます。

IoT Hub は、デバイスとクラウドの間のセキュアな通信のためのデータチャンネルとして働きます。**IoT Hub** は、**Pub/Sub** と **Revert-RPC** の両方の通信モードをサポートしています。**Pub/Sub** モードは、**Topic** に基づくメッセージルーティングモードです。

IoT Hub には次の機能があります。

- ・ **高いスケーラビリティ:** 線形の動的スケーリングをサポートし、**10 億台**のデバイスを同時に接続できます。
- ・ **エンドツーエンドの暗号化:** 通信リンク全体が **RSA** と **AES** で暗号化され、データ伝送がセキュアであることが保証されます。
- ・ **リアルタイムメッセージ:** デバイスと **IoT Hub** との間のデータチャンネルを確立後、永続的接続となり、ハンドシェイク時間を短縮し、メッセージがリアルタイムで到着することを保証します。
- ・ **データパススルーのサポート:** **IoT Hub** は、サーバーへのバイナリ形式のデータパススルーをサポートしています。データをセキュアかつ制御可能に保つために、**IoT Hub** はデバイスデータを保存しません。
- ・ **さまざまな通信モード:** **IoT Hub** は、さまざまな利用形態における通信のニーズを満たすために、**Pub/Sub** と **Revert-RPC** の両方の通信モードをサポートしています。

- ・ 複数プロトコルのサポート: **CoAP**、**MQTT**、および **HTTPS** プロトコルを使用してデバイスを **IoT Platform** に接続できます。

デバイス管理

IoT プラットフォームには次のような複数のデバイス管理サービスを提供します。ライフサイクル、[デバイスグループ](#)、[デバイスシャドウ](#)、[TSL モデル](#)、[#unique_6](#)、[#unique_7](#)、[ファームウェアの更新](#)、[リモート設定](#)、及びリアルタイムモニタリング。詳細は、関連文書をご参照ください。

ルールエンジン

デバイスが **Topic** を使用して **IoT Platform** と通信する場合、**Topic** 内のデータを処理する **SQL** 式を記述できます。その後、データを他の **Topic** または **Alibaba Cloud** サービスに転送するようにルールを設定できます。以下に例を示します。

- ・ **RDS**、**Table Store**、および **HiTSDB** にデータを転送して保存することができます。
- ・ **DataHub** にデータを転送し、**StreamCompute** をストリームコンピューティングに使用するか、**MaxCompute** を大規模データセットのオフラインコンピューティングに使用することができます。また、イベント駆動型処理のために **Function Compute** にデータを転送することもできます。
- ・ 高信頼性データ消費のために、**MQ (Message Queue)** にデータを転送することができます。
- ・ ある **Topic** のデータを別の **Topic** に転送して、デバイス間で **M2M** 通信を確立することができます。

セキュリティ認証ポリシーと権限付与ポリシー

セキュリティは **IoT** にとって非常に重要です。 **Alibaba Cloud IoT Platform** は、デバイスとクラウドの間の接続がセキュアであることを保証するための多層的なセキュリティ戦略を提供します。

- ・ **IoT Platform** は各デバイスに固有の証明書を発行し、各デバイスは **IoT Hub** に接続している間にその固有の証明書を認証に使用します。
- ・ **IoT Platform** は、開発者が多様なセキュリティ要件と生産ライン要件に対処するための、さまざまなデバイス認証方法を提供します。
- ・ 権限はデバイスレベルで付与されます。デバイスは、特定のデバイスに関連付けられた **Topic** のみをパブリッシュまたはサブスクライブすることができます。サーバーは **AccessKey** を使用して、**Alibaba Cloud** アカウントの **Topic** を介してデータを処理します。

3 用語集

このセクションでは、**Alibaba Cloud IoT Platform** で使用されている用語について説明します。

用語集

用語	説明
プロダクト	プロダクトとは、同じ機能を共有するデバイスのグループです。 IoT Platform は、各プロダクトに固有の ProductKey を発行します。1 つのプロダクトに、数千台のデバイスが含まれる場合があります。
デバイス	プロダクトを構成する物理デバイス。 IoT Platform は、各デバイスに対して同じプロダクト内で一意の DeviceName を発行します。デバイスは、 IoT Platform に直接接続することも、 IoT Platform に接続されているゲートウェイにサブデバイスとしてマウントすることもできます。
ゲートウェイ	ゲートウェイは IoT Platform に直接接続でき、サブデバイス管理機能を提供します。サブデバイスは、ゲートウェイ経由でのみ IoT Platform と通信できます。
サブデバイス	サブデバイスは基本的にデバイスです。サブデバイスは IoT Platform に直接接続することはできず、ゲートウェイ経由でのみ接続可能です。
3 つのキーフィールド	3 つのキーフィールドとは ProductKey、DeviceName、および DeviceSecret です。 • ProductKey は、IoT Platform 内で一意のプロダクト識別子です。このパラメーターは非常に重要であり、デバイスの認証と通信に使用されます。このパラメーターは、安全な場所に保存してください。 • DeviceName は、デバイス登録時に自動生成されるか、ユーザーによって定義されるデバイス名です。各デバイスには、同じプロダクト内で一意の DeviceName が割り当てられます。このパラメーターは非常に重要であり、デバイスの認証と通信に使用されます。このパラメーターは、安全な場所に保存してください。 • DeviceSecret は、デバイスごとに IoT Platform が発行する秘密鍵です。DeviceSecret は DeviceName と組み合わせて使用します。このパラメーターは非常に重要であり、デバイス認証に使用されます。このパラメーターは、安全な場所に保存して、決して他人に明かさなideてください。

用語	説明
ProductSecret	ProductSecret は、プロダクトごとに IoT Platform が発行する秘密鍵です。 ProductSecret は通常、 ProductKey と組み合わせて、プロダクト固有証明書による認証に使用されます。 このパラメーターは非常に重要です。 このパラメーターは、安全な場所に保存して、決して他人に明かさなてください。
Topic	Topic は、 Pub/Sub 通信時の伝送媒体として使用される UTF-8 文字列です。 デバイスは Topic にメッセージを公開したり、 Topic からのメッセージをサブスクライブしたりできます。
Topic カテゴリ	Topic カテゴリは、同じプロダクト内のさまざまなデバイスに関連付けられている Topic のセットです。 \${productKey} と \${deviceName} を組み合わせて一意のデバイスを指定できます。 Topic カテゴリは、同じプロダクト内のすべてのデバイスに適用できます。
パブリッシュ	デバイスが Topic にメッセージを公開することを許可する操作権限。
サブスクライブ	デバイスが Topic からのメッセージをサブスクライブすることを許可する操作権限。
RRPC	RRPC は Revert-RPC の略です。 RPC (Remote Procedure Call) は、クライアントとサーバー間の対話形式を使用しており、リモート対話に詳しくなくても、遠隔地でプロシージャを実行できます。 RRPC を使用すると、指定したデバイスにリクエストを送信したり、そのデバイスからレスポンスを受信したりできます。
タグ	タグには、プロダクトタグとデバイスタグがあります。 ・ プロダクトタグには、通常、同じプロダクト内のすべてのデバイスに共通する情報を設定します。 ・ デバイスタグには、デバイス固有の機能を設定します。 必要に応じて、カスタムタグを追加することができます。
Alink	デバイスと IoT Platform との通信用プロトコル。
TSL モデル	IoT Platform は、 TSL (Thing Specification Language) を使用してデバイスを記述します。 TSL モデルには、プロパティ、サービス、およびイベントが含まれます。 TSL モデルは JSON 形式を使用します。 TSL に基づいてデータを編成し、データをクラウドに報告することができます。
プロパティ	環境モニタリング装置によって収集された温度情報など、デバイスの実行ステータスを設定する機能。 プロパティは、 GET および SET のリクエストメソッドをサポートしています。 アプリケーションシステムは、プロパティを取得および設定するリクエストを送信できます。

用語	説明
サービス	外部のリクエスターから使用できるデバイスで提供される機能またはメソッドを設定する機能。入力パラメーターと出力パラメーターを指定できます。プロパティと比較して、サービスは 1 つのコマンドを使用して複雑なビジネスロジックを実装することができます (特定のタスクを実行するなど)。
イベント	デバイスの実行中に生成されるイベントを設定する機能。イベントには通常、対処または注意を必要とする通知が含まれ、複数の出力パラメーターが含まれている場合があります。たとえば、タスクの完了通知、デバイス障害の発生、温度アラートなどのイベントがあります。イベントをサブスクライブすることも、プッシュすることもできます。
データ解析スクリプト	IoT Platform Pro で作成されたプロダクト内のデバイスでは、パススルーモードまたはカスタムモードを使用して IoT Platform にデータを送信する場合、データ解析スクリプトを作成して、デバイスから送信されたバイナリデータまたはカスタム JSON データを Alink に変換する必要があります。
デバイスシャドウ	デバイスシャドウは、デバイスまたはアプリケーションのステータス情報を保存するための JSON ファイルです。各デバイスには、 IoT Platform 内で固有のデバイスシャドウが割り当てられます。デバイスがインターネットに接続されているかどうかに関係なく、デバイスシャドウを使用して、 MQTT や HTTP 経由でデバイスのステータスを取得および設定できます。
ルールエンジン	ルールエンジンは、 SQL ベースの言語を提供し、 Topic からデータをフィルタリングし、処理したデータを Message Service や Table Store など、他の Alibaba Cloud サービスに送信できます。

4 利点

ますます多くの企業が **IoT (Internet of Things)** ソリューションを利用して、デバイスからデータを収集、管理し、収益を向上させています。しかし、**IoT** エコシステムを変革し、強力な **IoT** プラットフォームを構築する作業は困難に直面しています。**Alibaba Cloud IoT Platform** は、これらの問題に対するソリューションを提供します。

次の表は、従来の **IoT** 開発と、**Alibaba Cloud IoT Platform** に基づく **IoT** 開発の違いを示しています。

	従来の IoT 開発	Alibaba Cloud IoT Platform に基づく開発
IoT プラットフォームへのデバイスの接続	インフラストラクチャと、組み込みシステム開発者およびクラウド開発者のサポートが必要です。 開発は難しく、非効率的です。	デバイスとクラウドの間を短期間で接続するための SDK (ソフトウェア開発キット) を提供します。 IoT Platform は、世界中のデバイス、異種ネットワークのデバイス、多環境下で実行されているデバイス、および複数プロトコルに基づいて動作するデバイスへの接続をサポートします。
パフォーマンス	アーキテクチャの手動スケーリングが必要です。その結果、サーバーやロードバランサーなどのインフラストラクチャを、デバイスレベルの粒度で実装することが困難になります。	1 億台以上のデバイスの永続的接続と数百万台の同時接続をサポートし、アーキテクチャの水平スケーリングを可能にします。
セキュリティ	セキュリティ対策の策定とデプロイメントが別途必要です。デバイスデータのセキュリティ確保には困難が予想されます。	クラウド内のデータを保護する手段が、複数あります。 ・ デバイス認証によるデバイスのセキュリティと一意性の保証 ・ 通信暗号化によるデータ改ざん防止 ・ Alibaba Cloud Security と権限チェックによるクラウドセキュリティの保護
安定性	手動によるサーバー障害検出とサービス移行が必要で、移行中のサービス中断によりサービスが不安定になります。	最大 99.9% のサービス可用性を保証し、単一障害点での自動移行を可能にします。

	従来の IoT 開発	Alibaba Cloud IoT Platform に基づく開発
使いやすさ	ロードバランシングのための分散アーキテクチャ構築に追加のサーバーを必要とし、接続、コンピューティング、ストレージを処理する完全な IoT システム開発が必要で、費用がかかります。	同一プラットフォームでのデバイス管理、デバイスのリアルタイムモニタリング、および Alibaba Cloud サービスへのシームレスな接続をサポートし、複雑な IoT アプリケーションの柔軟で容易な実装を可能にします。

5 制限事項

IoT Platform には次の制限があります。

プロダクトとデバイス

項目	説明	制限
タグ総数	1つのプロダクト、デバイス、またはデバイスグループが保持できるタグの最大数。	100
プロダクト総数	1つのアカウントが保持できるプロダクトの最大数。	1,000
デバイス総数	1つのプロダクトが保持できるデバイスの最大数。  注： ビジネスでさらにデバイスが必要な場合は、コンソールでチケットを起票し、サポートセンターへお問い合わせください。	500,000
	1つのアカウントが保持できるデバイスの最大数。  注： ビジネスでさらにデバイスが必要な場合は、コンソールでチケットを起票し、サポートセンターへお問い合わせください。	10,000,000
ゲートウェイとサブデバイス	1つのゲートウェイが保持できるサブデバイスの最大数。	1,500
TSL モデルの機能	1つのプロダクトが保持できる機能の最大数。	200
	struct プロパティに定義できるパラメーターの最大数。	10
	データ型に依存する制限事項 - enum：列挙項目の数が 100 を超えてはいけません。 - text：データが 2,048 バイトを超えてはいけません。 - array：配列要素の数が 128 を超えてはいけません。	—
	1つのサービスに指定できる入力または出力パラメーターの最大数。	20
	1つのイベントに指定できる出力パラメーターの最大数。	50

項目	説明	制限
デバイスグループ	1つのアカウントが保持できるグループ (ペアレントグループとサブグループを含む) の最大数。	1,000
	1つのグループに追加できるデバイスの最大数。	20,000
	1つのデバイスが所属できるグループの最大数。	10
データ解析	データ解析のためにアップロードできるスクリプトファイルの最大サイズ。	48 KB
リモート設定	リモート設定ファイルは JSON 形式のみをサポートします。ファイルサイズは 64 KB を超えてはいけません。	64 KB
データストレージ	プロパティ、イベント、およびサービスのデータは 30 日間保存されます。	30 日間

通信

項目	制限
1つのアカウントが1秒間に送信できる MQTT リクエストの最大数。	500
1つのデバイスが1分間に送信できる接続リクエストの最大数。	5
1つのデバイスがサブスクライブできる Topic の最大数。 最大数に達すると、新しいサブスクリプションリクエストは拒否されます。デバイスは、受信した SUBACK メッセージからリクエストが成功したかどうか確認できます。	100
1つのアカウントが、1秒間にデバイスから IoT Platform に送信できるリクエストの最大数。	10,000
1つのアカウントが、1秒間に IoT Platform からデバイスに送信できるリクエストの最大数。	2,000
1つのアカウントが、1秒間にルールエンジンのデータ転送モジュールに送信できるメッセージの最大数。	1,000
1つのアカウントが、1秒間にサブスクライブできるメッセージの最大数。	1,000
1つのデバイスが IoT Platform にメッセージを送信できる最大頻度。	QoS 0 : 30 メッセージ/秒。 QoS 1 : 10 メッセージ/秒。

項目	制限
デバイスは、最大 50 メッセージ/秒で受信できます。パフォーマンスはネットワークの状態にも左右されます。 TCP 書き込みバッファサイズの上限を超過すると、エラーが返されます。たとえば、Pub 操作を使用してリクエストをデバイスに送信するときに、デバイスがすべてのリクエストを処理できない場合は、スロットルエラーが返されます。  注： MQTT プロトコルを使用してデバイスを IoT Platform に接続する場合、スロットルエラーメッセージは返されません。ただし、ログを閲覧して、スロットルされているデバイスを探し出すことはできません。	50 メッセージ/秒
接続ごとの最大スループット (帯域幅)。	1,024 KB
IoT Platform は、1 つのデバイスに対する応答待ちのメッセージパブリッシュリクエストの数を制限します。 最大数に達すると、IoT Platform は、PUBACK メッセージが返されない限り、そのデバイスに対する新しいメッセージパブリッシュリクエストを受け付けません。	100
QoS 1 の送信方式で送信されたメッセージの最大保存期間。 最大保存期間が経過しても PUBACK メッセージが受信されない場合、リクエストは破棄されます。	7 日
MQTT を使用して送信されるメッセージの最大サイズ。この制限を超えるメッセージは拒否されます。	256 KB
CoAP を使用して送信されるメッセージの最大サイズ。この制限を超えるメッセージは拒否されます。	1 KB

項目	制限
MQTT 接続のハートビート間隔は、30～1,200 秒です。ハートビート間隔がこの範囲外の場合、IoT Platform は接続リクエストを拒否します。 300 秒を超える値を設定することをお勧めします。 IoT Platform が、CONNECT メッセージに対するレスポンスとして CONNACK メッセージを送信すると、タイマーがスタートします。 PUBLISH、SUBSCRIBE、PING、または PUBACK メッセージを受信すると、タイマーがリセットされます。タイマーは、ハートビート間隔の 1.5 倍の時間にセットされます。タイマーが時間切れになってもメッセージが受信されない場合、接続は切断されます。	30～1,200 秒

Topic

項目	制限
1 つ のプロダクトは、最大 50 個 の Topic カテゴリを定義できます。	50
デバイスは、自分自身の Topic に対するメッセージのパブリッシュとサブスクライブだけが可能です。	なし
Topic は UTF-8 でエンコードされた文字列で、 128 バイト を超えることはできません。	128 バイト
1 つ の Topic に指定できるスラッシュ (/) の最大数。	7
1 つ のサブスクリプションリクエストに指定できる Topic の最大数。	8
Topic のサブスクライブまたはサブスクライブ解除後、変更は約 10 秒で有効になります。サブスクリプションは、Topic をサブスクライブ解除するまで有効です。データの損失を防ぐため、事前に Topic をサブスクライブすることをお勧めします。 例：あるデバイスが Sub リクエストを Topic A に送信したとします。10 秒後、サブスクリプションが有効になり、そのデバイスは Topic A からリアルタイムでメッセージの受信を開始します。サブスクリプションを解除しない限り、そのデバイスは Topic A からのメッセージを受信し続けます。	10 秒
1 つ のブロードキャスト Topic を、最大 1,000 台 のデバイスがサブスクライブできます。サーバー SDK は、 1 秒間 に 1 つ のブロードキャストメッセージを送信可能です。	1,000

デバイスシャドウ

項目	制限
デバイスシャドウ JSON ファイルの最大入れ子レベル。	5
デバイスシャドウ JSON ファイルの最大サイズ。	16 KB
デバイスシャドウ JSON ファイル内のプロパティの最大数。	128
デバイスが 1 秒間に送信できるリクエストの最大数。	20

データ転送

項目	制限
1 つのアカウントは最大 1,000 個のルールを設定できます。	1,000
1 つのルールには、最大 10 個のデータ転送操作 (10 個のデータ転送先) を指定できます。	10
データ転送のパフォーマンスは、転送先クラウドサービスのインスタンスに依存します。転送先インスタンスに十分なパフォーマンスリソースがある場合、ルールエンジンは 1 つのアカウントに対して 1,000 QPS のデータ転送能力を発揮できます。 RAM ユーザーは、対応する Alibaba Cloud アカウントのクォータを共有します。リクエスト数が最大数を超える場合、または転送先インスタンスに対する受信データの書き込みに 1 秒以上かかる場合、データ転送は制限されます。	1,000 QPS
転送先クラウドサービスのインスタンスが正常動作していることを確認してください。転送先インスタンスのクラッシュ、料金滞納、無効なパラメーター (無効な値や権限の変更など)、設定の間違いなどがある場合、データ転送は失敗します。	—
ルールエンジンは、メッセージを複数回転送する場合があります。分散環境では、リアルタイムのメッセージのバランス調整により、単一メッセージの複数回転送が発生します。転送先アプリケーションには、重複したメッセージを無視するメカニズムが必要です。	なし

クラウド API の制限

操作名	QPS/アカウント	QPS/IPアドレス
Pub	1,600	100
RRpc	1,000	100
PubBroadcast	1	100
その他の操作	50	100

操作の呼び出しがスロットルエラーになった場合は、呼び出しを再試行してください。スロットルエラーには、[共通エラーコード](#)の **29～31** のエラーが含まれます。



注：

- ・ **QPS/アカウント** は、**1** つの **Alibaba Cloud** アカウントの **1** 秒間の呼び出し回数を指します。**RAM** ユーザーは、対応する **Alibaba Cloud** アカウントのクォータを共有します。
- ・ **QPS/IP アドレス** は、**IP** アドレスによって識別される **1** つのサーバーの **1** 秒間の呼び出し回数を指します。