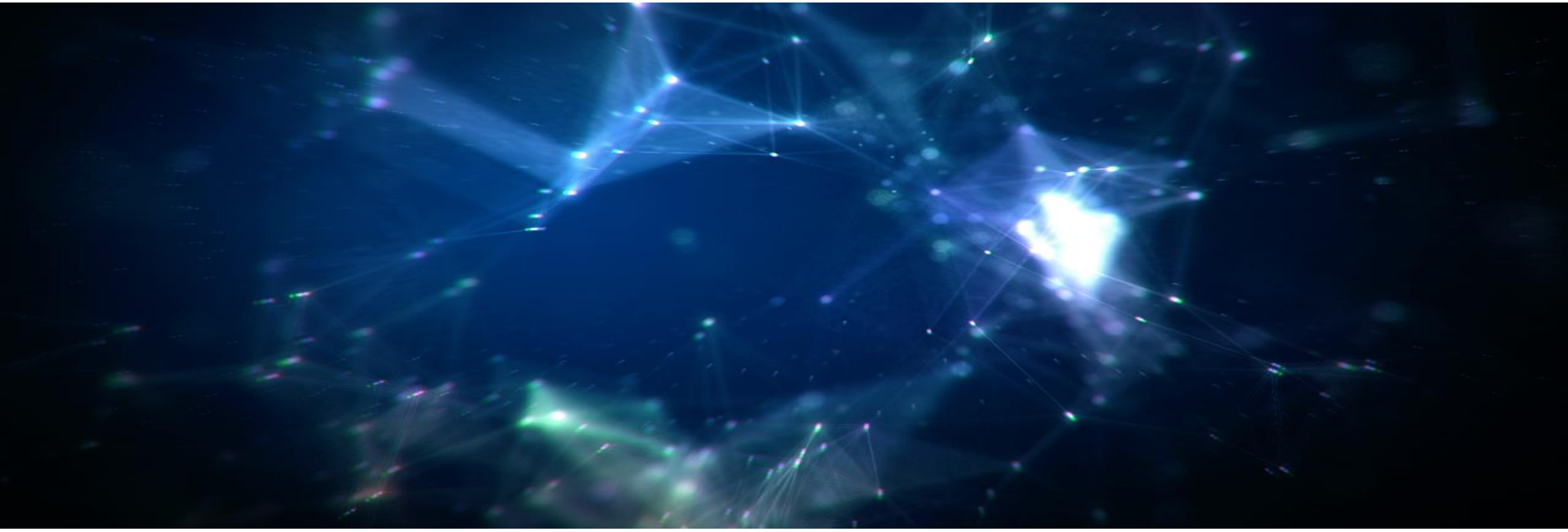
Neural Pocket



AWS IoT Coreを使ったサービスの作り方

IoT技術者向けAWSセミナー| 2022年10月20日

自己紹介

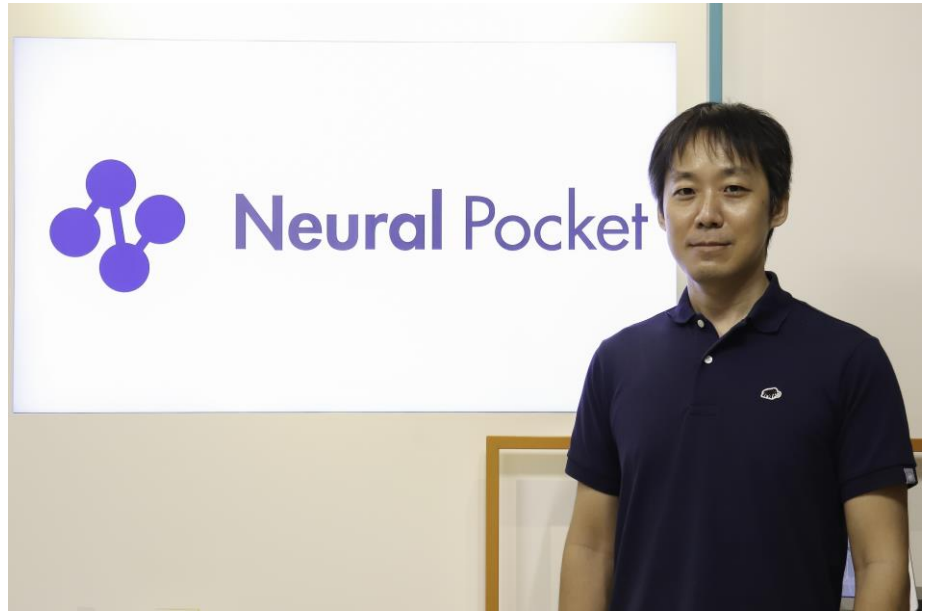
ニューラルポケット株式会社
技術開発本部
プラットフォーム開発部
部長代理

中野　匡洋

2021年5月入社
サイネージ広告の運営基盤を担当

経歴
ECサイトのASP事業、ISPの課金システム、
決済代行システムといった大量トランザクション
が集まるシステムの企画・開発・運用を経験

趣味
ランニング・クライミング・バイク



独自開発の「AIアルゴリズムによる画像・動画解析技術」と「エッジコンピューティング技術」の活用によるソリューション提供

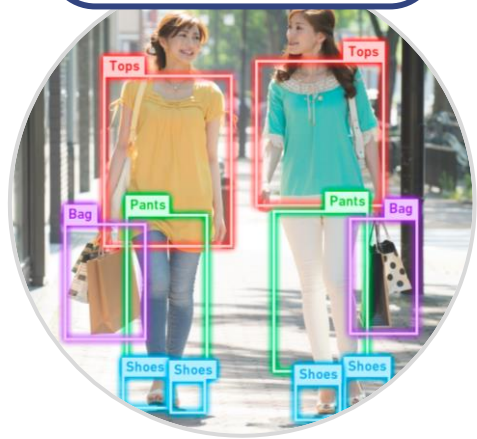
人流・防犯
デジフロー

駐車場・モビリティ*1
デジパーク

サイネージ広告
SIGN DIGI

在宅勤務支援
リモデスク

ファッション解析
AIMD®



AIカメラを活用したスマートパーキング

駐車場・モビリティ*1
デジパーク

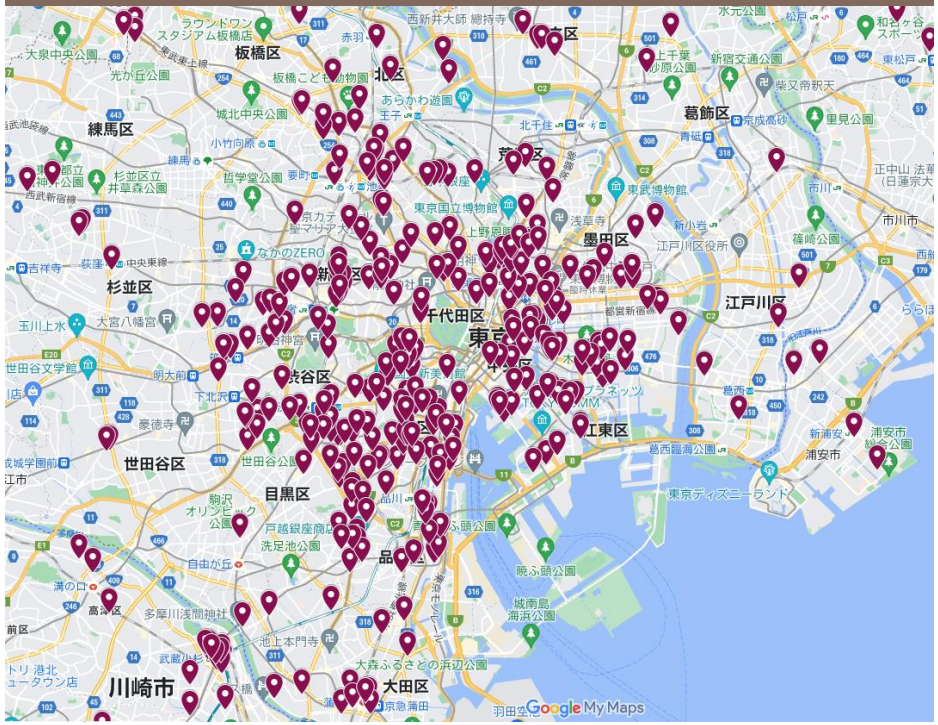
弊社ウェブサイトのサービス紹介ページで動画をご覧いただけます
https://www.neuralpocket.com/

サイネージ広告事業

都心マンションの感度の高い居住者へ
広告主様のメッセージをお届けします。

FOCUS CHANNEL by Neural Pocket

約20万人の首都圏富裕層にリーチ可能



設置棟数420・世帯数81,000戸
※2022年9月末時点見込み

Impression
情勢に左右されない
安定したリーチ数

No.1
マンション
サイネージ広告
業界1位
*当社調べ

Frequency
生活動線にあり、
居住者全員に繰り返し訴求
(1枠あたり想定視認回数: 150万回/月)

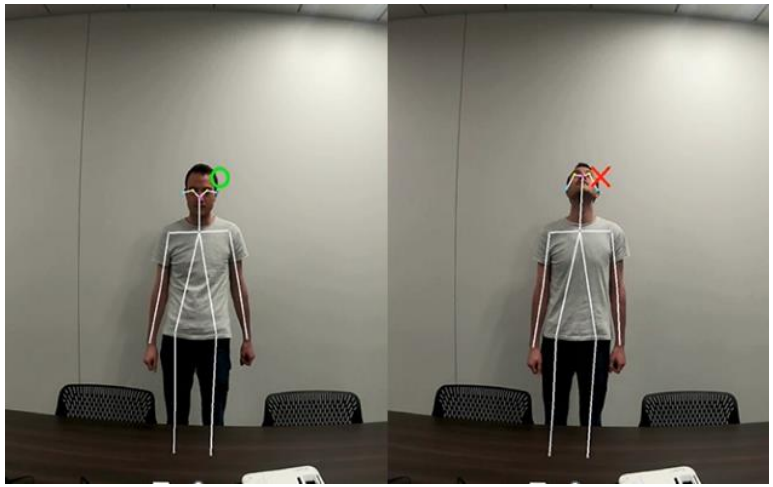
Targeting
ハイグレードマンション居住の
富裕層を中心にターゲティング

One-stop
広告配信とフライヤー設置により、
認知から詳細検討まで一貫して獲得

サイネージ広告事業

サイネージ広告
SIGN DIGI

エッジAIを搭載したサイネージを利用しています。放送しているコンテンツに対して、「何人通過したか」「何秒視聴したか」を計測できます。
デバイス内で計測が完結するエッジAIで、カメラの映像を解析することで、結果データのみを収集し、個人の特定や画像の収集は行ってません。



視認検知のデモ

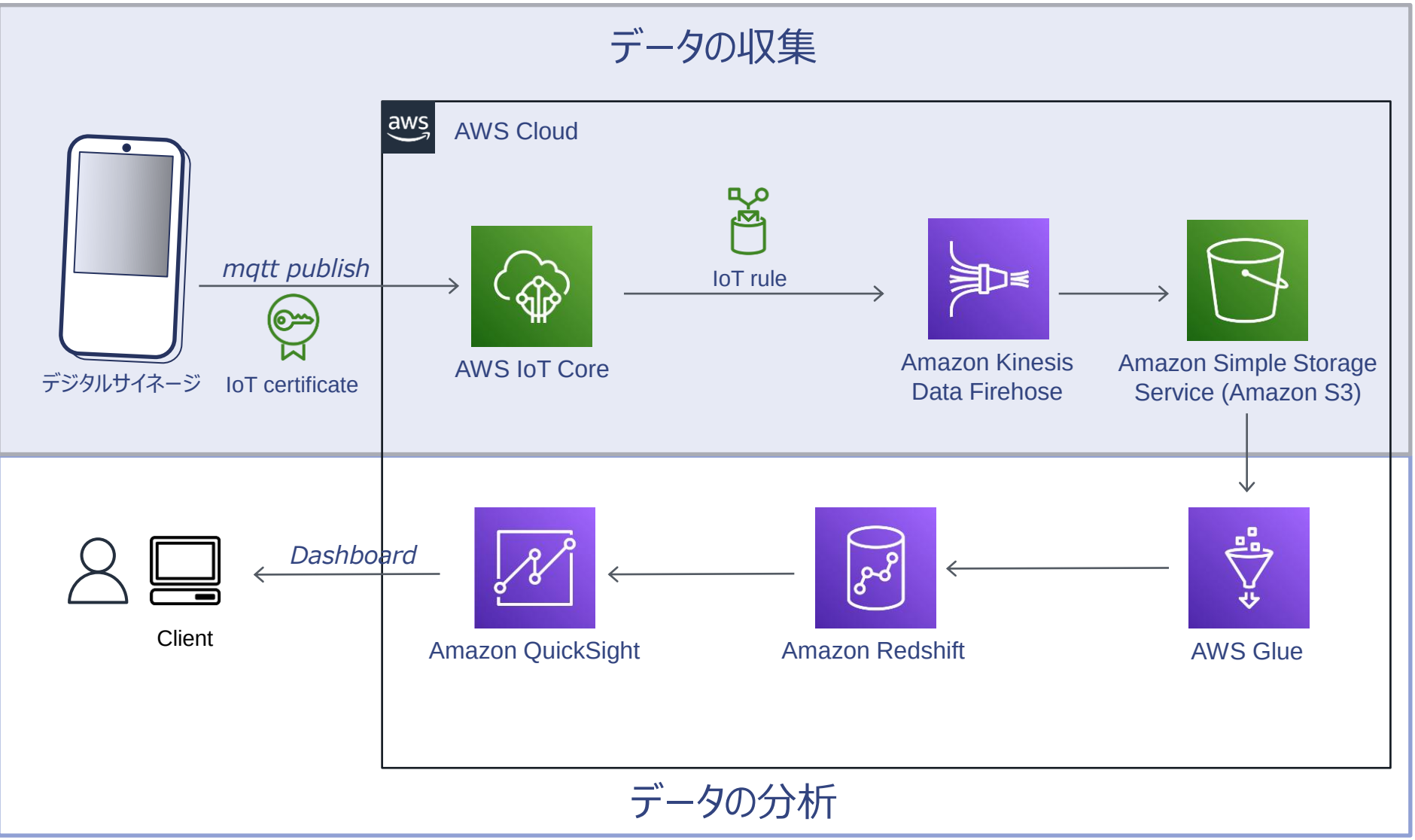
サイネージ広告事業　システム規模

視聴データを取り扱っているため、デバイスからレポートされる情報は多く、

毎月３.９億件

※さらに監視システムにメッセージを複製しているので実際はさらに多いメッセージを扱っています。

アーキテクチャの紹介



サイネージアーキテクチャの紹介

データ収集

AIの検知した視聴データや広告の再生データをAWS IoT Coreを通じて収集しS3に保存という一般的な利用方法を踏襲しています。

ポイント

IoT Coreのドキュメントには受信したデータの保存に関する情報が少ない、そこで連携しているサービスのドキュメントを参照する事をお勧めします。

AWS IoT Coreから iot ruleを介して連携可能なサービスは以下のウェブサイトで確認できます。

https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/iot-rule-actions.html

弊社はバックアップを残す事を視野にS3にデータを保存する事を選択しました他のストレージやデータベースに直接保存することもできるので、目的のサービスをぜひ探してみてください。

AWS IoT ルールアクション

ルールアクション	説明	API での名前
CloudWatch アラーム	Amazon CloudWatch アラームの状態を変更します。	cloudwatchAlarm
[CloudWatch Logs]	Amazon CloudWatch Logs にメッセージを送信します。	cloudwatchLogs
CloudWatch メトリクス	CloudWatch メトリクスにメッセージを送信します。	cloudwatchMetric
DynamoDB	DynamoDB テーブルにメッセージを送信します。	dynamoDB
DynamoDBv2	DynamoDB テーブル内の複数の列に、メッセージデータを送信します。	dynamoDBv2
Elasticsearch	Amazon Elasticsearch Service エンドポイントに、メッセージを送信します。	elasticsearch
HTTP	HTTPS エンドポイントに、メッセージをポストします。	http
IoT Analytics	AWS IoT Analytics チャネルにメッセージを送信します。	iotAnalytics
IoT Events	AWS IoT Events 入力にメッセージを送信します。	iotEvents
IoT SiteWise	AWS IoT SiteWise アセットプロパティにメッセージデータを送信します。	iotSiteWise
Kinesis Data Firehose	Kinesis Data Firehose 配信ストリーミングにメッセージを送信します。	firehose
Kinesis Data Streams	Kinesis データストリーミングにメッセージを送信します。	kinesis
Lambda	メッセージデータを入力として Lambda関数を呼び出します。	lambda
OpenSearch	Amazon OpenSearch Service エンドポイントにメッセージを送信します。	OpenSearch
Republish	メッセージを別の MQTT トピックに再発行します。	republish
S3	Amazon Simple Storage Service (Amazon S3) バケットにメッセージを保存します。	s3
Salesforce IoT	Salesforce の IoT 入力ストリーミングにメッセージを送信します。	salesforce
SNS	Amazon Simple Notification Service (Amazon SNS) プッシュ通知としてメッセージを発行します。	sns
SQS	Amazon Simple Queue Service (Amazon SQS) キューにメッセージを送信します。	sqs
Step Functions	AWS Step Functions ステートマシンを始動します。	stepFunctions
Timestream	Amazon Timestream データベーステーブルに、メッセージを送信します。	timestream

https://docs.as.amazon.com/ja_jp/iot/latest/developerguide/iot-rule-actions.html

アーキテクチャを選んだ背景

1. フルマネージドサービスである事
   自ら事業を運営している都合上、コストを明確にする必要がありました。
   オンプレミスや仮想サーバーでは故障や障害といった、不測の事態を含めて計画をしなければならず、比較した場合AWS IoT Coreは使用量に応じて費用が発生するので事業の推進をシンプルにしてくれています。

2. デバイス認証が備わっていた事
   デバイスを不正にネットワークに接続させない仕組みがビルトインされている事は外部に機器を置いている身としては安心感があります。

3. セキュアトンネリングと呼ばれるリモート操作用のツールが用意されている
   万が一障害が発生したとしても、安全な方法でリモートの機器の状態調査が可能な仕組みが用意されている。

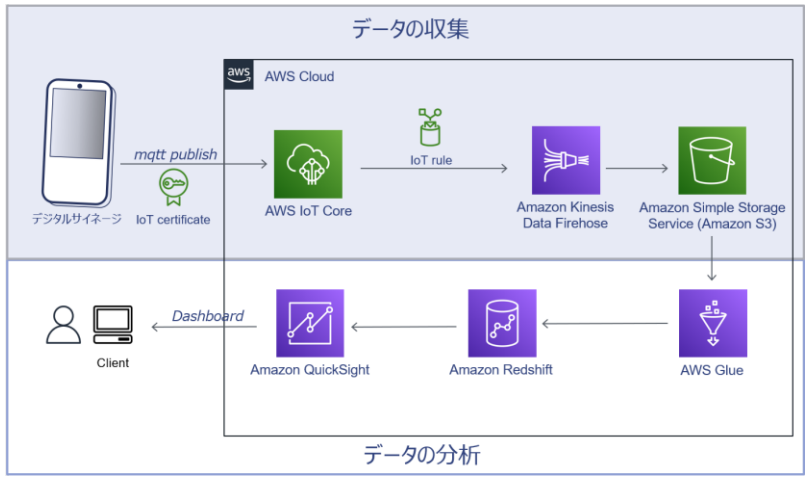
新しいサービスの登場

Amazon Timestream

東京リージョンでも Amazon Timestream の提供が開始されました。
このサービスを使うと弊社のアーキテクチャの「データの分析」にあたる部分を置き換え可能な機能を備えています。

データの保存期限に応じて、アーカイブするティアリング機能も備わっているようですので、長期の運用には非常に有効です。

分析を行う処理は複雑なのでそのまま置き換えに検証が必要ですが、適用できるか評価をしたいと考えています。



AWS IoT Coreを用いたサービスの開発

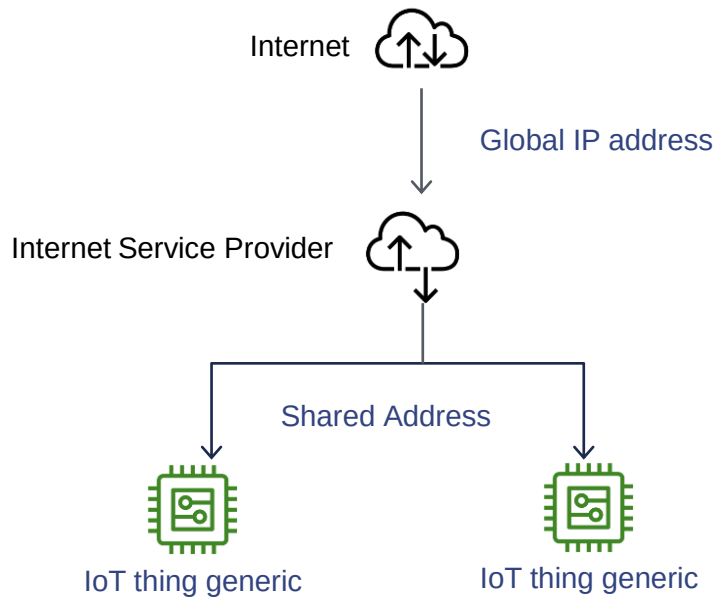
サービスの開発にあたり、注意したいポイントは３つ

1. **IoT機器からメッセージが通る経路の確認**
2. **クォータの条件とモニタリング**
3. **システム開発だけではないサービス開発に必要な事**

1．IoT機器からメッセージが通る経路の確認①

IoT機器はモデムを内蔵した機器があります
「LTE網に繋がっているから外部からアクセスされないだろう」は間違い

LTE回線で機器を接続した際に割り当てられるグローバルIPアドレスは
Shared Address Space「100.64.0.0/10」と呼ばれる予約された領域です。
これは Carrier Grade NAT と呼ばれる、プロバイダ単位でNAT運用をしているイメージです。

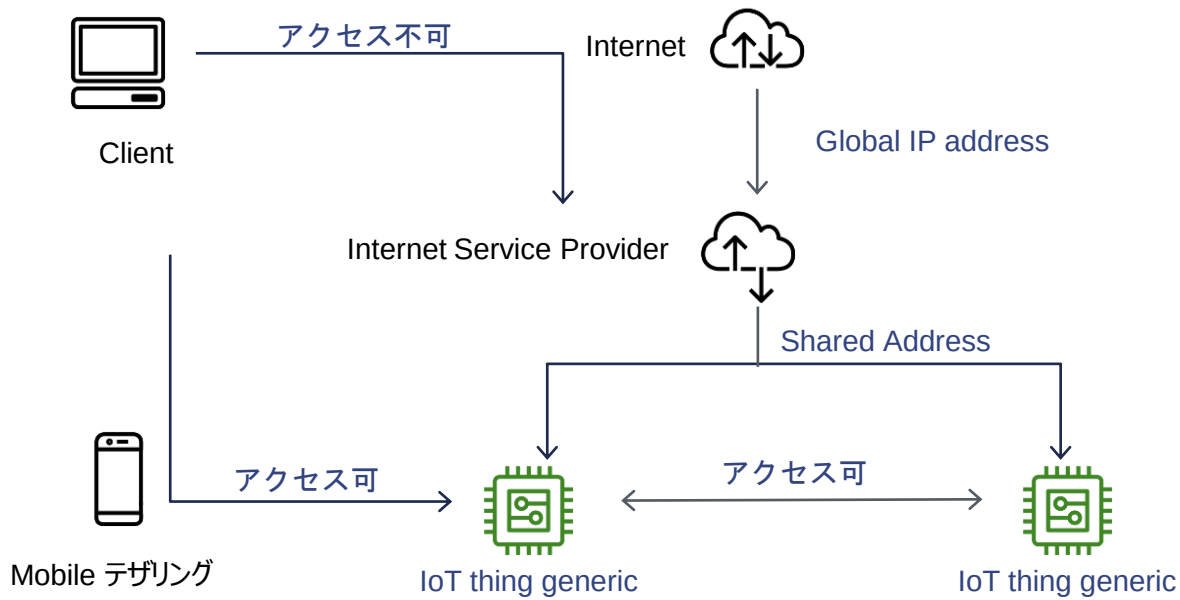


CGNとは
https://www.nic.ad.jp/ja/basics/terms/cgn.html
一般社団法人日本ネットワークインフォメーションセンター(JPNIC)

1．IoT機器からメッセージが通る経路の確認①

CGNの場合、他のネットワークからはNATに阻まれて通信できません。
これは**「開発用のPCから、IoT機器にインターネット経由でアクセスできない」**状態を作ります。しかし、同じキャリア・MVNOのLTEのネットワーク同士だと接続するケースがあります。つまりIoT機器同士やスマートフォンからテザリング通信では接続できるという状態になります。

ポイント　**「必ずファイアウォールを設定し、不必要なポートは開放しない」**

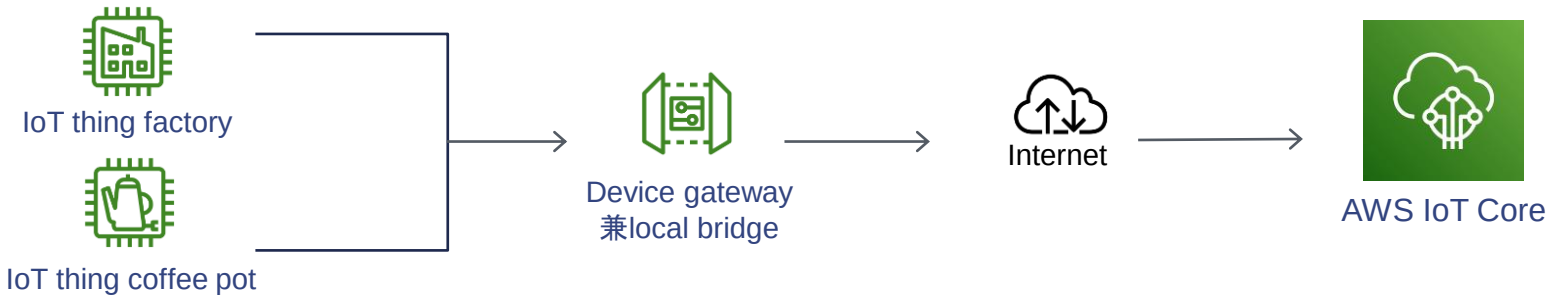


1．IoT機器からメッセージが通る経路の確認②

ローカルブリッジの使用

IoT機器からの通信は、設置場所の電波状況により通信が不安定になることがあります。
MQTTプロトコルでメッセージのプーリングは規定されていませんが、ローカルブリッジと呼ばれるMQTTサーバーをデバイス内に起動しておくことがあります。

AWSのガイドにも案内があり、アプリケーション毎にコネクションを確立・維持しなくて良くなるといったメリットがあります。



1．IoT機器からメッセージが通る経路の確認②

ローカルのMosquitto MQTT BrokerをブリッジにAWS IoTを使う
https://aws.amazon.com/jp/blogs/news/how-to-bridge-mosquitto-mqtt-broker-to-aws-iot/

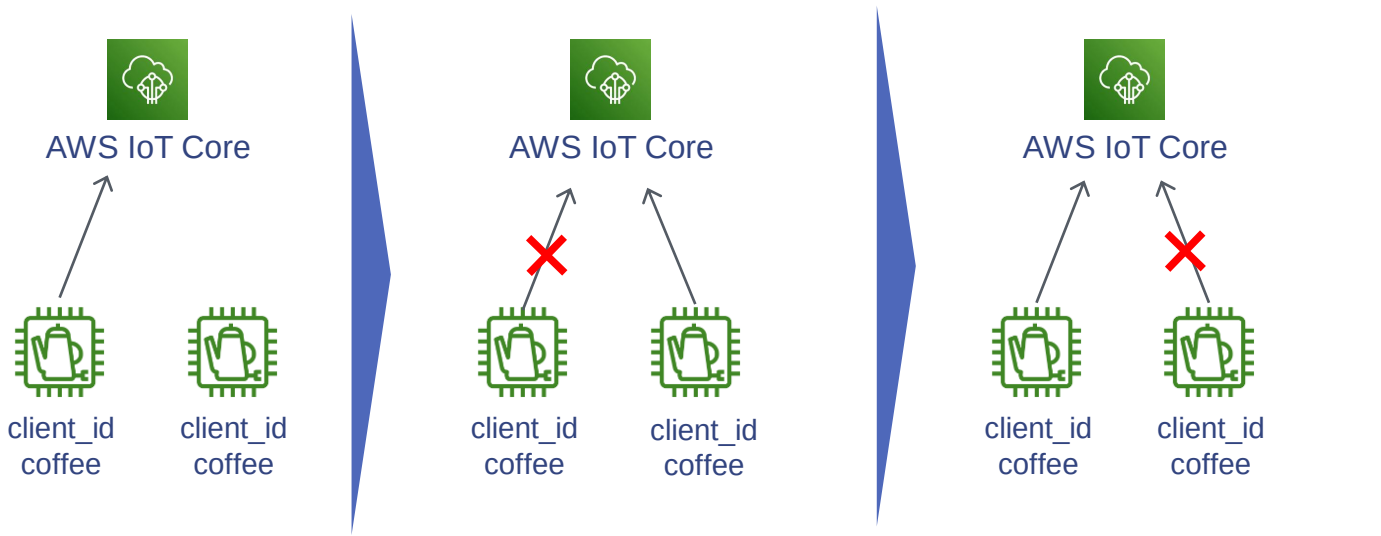
実はこのガイドの通り実装した機材を2台以上稼働させると、
AWS IoT Coreのクォータ制限を受けます。

1．IoT機器からメッセージが通る経路の確認②

AWS IoT CoreではMQTTの接続毎にクライアントIDを変更することを推奨しています。

クライアント ID は、各 AWS アカウント および各 AWS リージョン 内で一意である必要があります。
https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/security-best-practices.html

ポイント
必ず接続単位でユニークなIDを設定しましょう。



コーヒーポット（左）が空になった事を通知

コーヒーポット（右）が空になった事を通知
コーヒーポット（左）は接続断

コーヒーポット（左）がドリップ完了を通知
コーヒーポット（右）は接続断

2．クォータの条件とモニタリング

「ローカルのMosquitto MQTT BrokerをブリッジにAWS IoTを使う」に記載されたサンプルコードに戻ります

ローカルブリッジの設定にクライアントIDが以下の通り固定で書かれています。

```
# Bridge connection name and MQTT client Id,
# enabling the connection automatically when the broker starts.
cleansession true
clientid bridgeawsiot
start_type automatic
notifications false log_type all
```

この bridgeawsiot が2**台以上同時に接続するとスロットリングがかかります。**
すでに接続されている機器は切断、新しく接続を試みた機器に接続を譲ります。メッセージが送信される都度、クオータが評価され切断と接続を交互に繰り返します。
※実際はローカルブリッジサーバーがclientidの後にホスト名を付与してくれるケースも場合もあるのですが、ホスト名がlocalhost.localdomainだと同じ条件になり、接続と切断が繰り返されます。

2．クォータの条件とモニタリング

AWS IoT Core クォータの注意するポイント

まずは条件をチェック！

AWS IoT Core エンドポイントとクォータ
https://docs.aws.amazon.com/ja_jp/general/latest/gr/iot-core.html#limits_iot

特に以下の条件をチェック！
- 「破棄」されます
- 「拒否」されます
- 「デフォルト値」が１桁
- 調整可能が「不可能」

2．クォータの条件とモニタリング

破棄される例

Maximum retry interval for delivering QoS 1 messages	AWS IoT Core では、未確認の quality-of-service 1 (QoS 1) パブリッシュリクエストの再配信を最大 1 時間試行します。1 時間経過してもクライアントから PUBACK メッセージが AWS IoT Core に送信されない場合、パブリッシュリクエストは破棄されます。	3600 秒	3600 秒	いいえ

拒否される例

Message size	すべてのパブリッシュリクエストのペイロードは 128 KB を超えることができません。AWS IoT Core は、このサイズより大きい発行リクエストや接続リクエストを拒否します。	128 KB	128 KB	いいえ

デフォルト値が 1 桁の例

Connect requests per second per client ID	AWS IoT Core では、accountId と clientId が同一の MQTT CONNECT リクエストは、1 秒あたり 1 MQTT CONNECT オペレーションに制限されます。	1	1	いいえ

2．クォータの条件とモニタリング

AWSのドキュメントには一連の接続・送信・切断ライフサイクルを確認する方法が用意されているので紹介します。

ライフサイクルイベント
https://docs.aws.amazon.com/ja_jp/iot/latest/developerguide/life-cycle-events.html

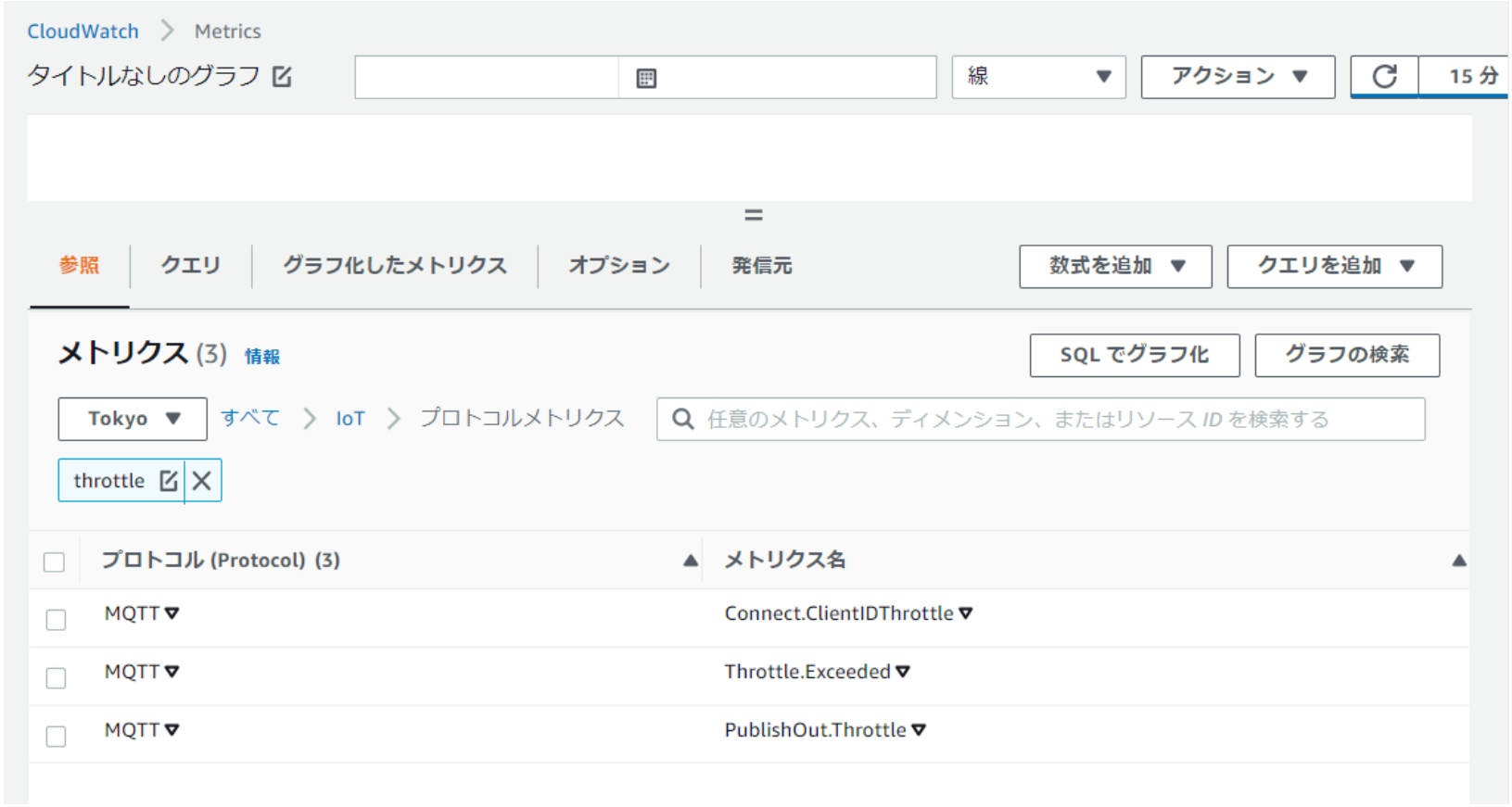
以下のトピックスを購読する事で、クライアントID単位で切断と接続の状態が確認できます。

接続イベント
$aws/events/presence/connected/{クライアントID}

切断イベント
$aws/events/presence/disconnected/{クライアントID}

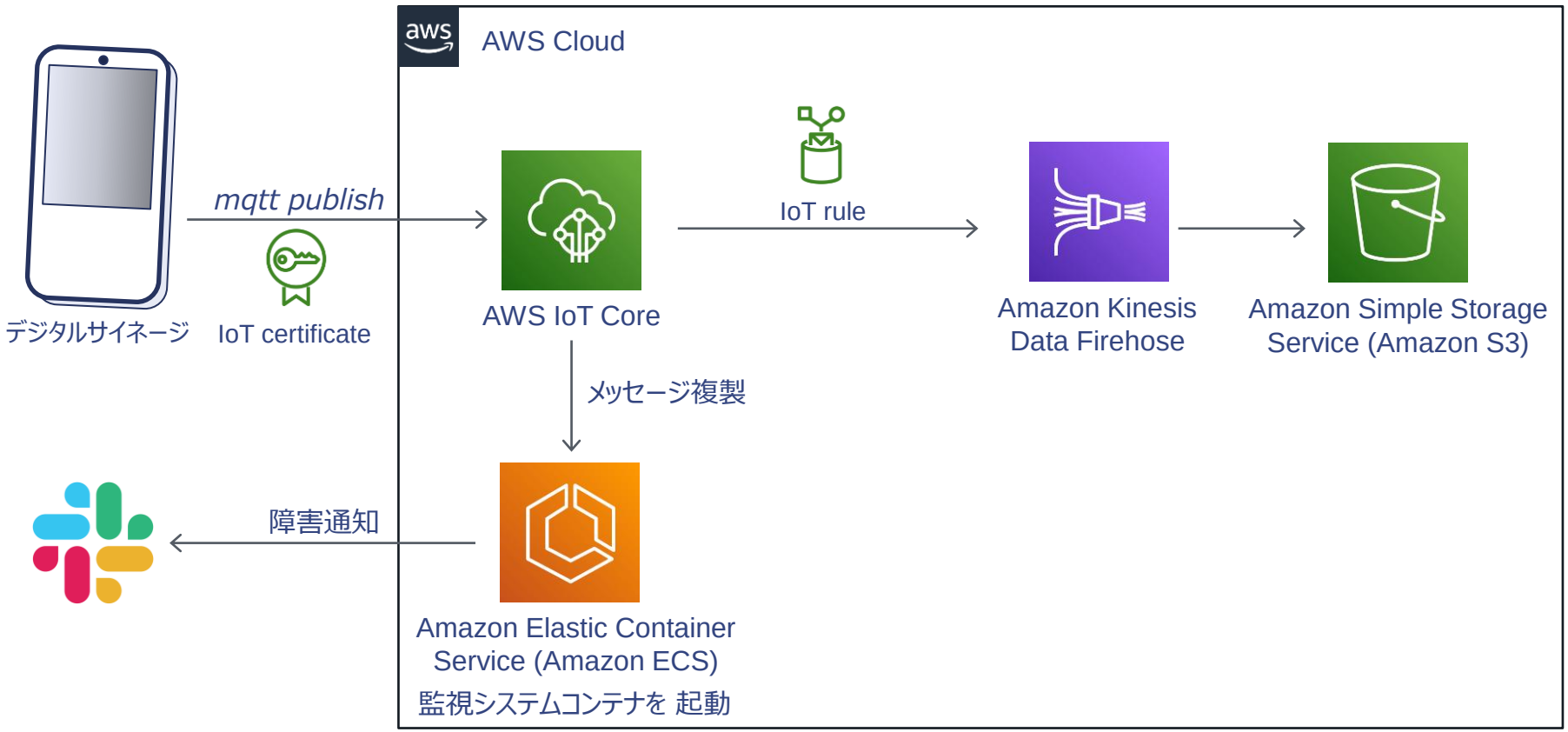
カスタムダッシュボードの作成

もう一つは、CloudWatchのダッシュボードを利用する事です。
特に、Throttle、Errorキーワードを含んだメトリクスを選んで、ダッシュボードを作成する事を推奨します。



業務監視システムの活用

ポイント
LTE接続を使用している場合は、現地の電波状況で接続・切断が発生しますので切断イベントをもって当該機器の故障を判断できません。独自に監視システムを構築し一定時間イベントが送信されなかった場合故障を通知する、といった業務監視システムを構築しています。



3．システム開発だけではないサービス開発に必要な事

ポイント
システム開発だけで解決できない問題がある事を認識する。
AWSのサンプルクライアントIDを一意の値にするのは一例でありますが、機器に設定していく、キッティング、出荷等の業務フローで解決することもあります。

ポイント
機材の盗難や、通信のただ乗りに注意する。
通信回線の利用状況をモニタリングし、盗難された場合は停止する手順を確認・確立しておきましょう。

最後におしらせ

マンションサイネージからのプレゼント

FOCUS CHANNEL by Neural Pocket

サーティワン アイスクリーム プレゼントキャンペーン!!

応募期間：2022年10月15日～2022年10月31日23:59まで

応募方法

①マンションサイネージのTwitter公式アカウント「@mansionsignage」をフォロー

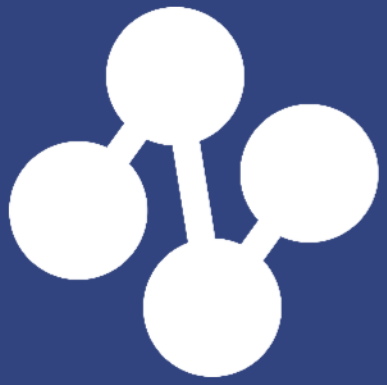
②対象のキャンペーンツイートをRT

③フォロー＆RTしてくれた方の中から抽選で100名様に「サーティワン アイスクリーム 500円ギフト券」をプレゼント!!

マンションサイネージの公式TwitterQRコード

注意事項

※画像はイメージです。
※当選者にはTwitterのDMでお知らせします。
※当社公式アカウントをブロックしていたり、Twitterアカウントを削除した等の理由により当社公式アカウントからのDMを受信できない場合、当選は無効となります。
※当選の有無のお問い合わせにはご回答いたしません。



Neural Pocket