

# アプリケーションノート

## Armadillo-IoT ゲートウェイ A6 省電力画像監視システム

Version 1.0.0  
2022/02/08

株式会社アットマークテクノ [<https://www.atmark-techno.com>]

Armadillo サイト [<https://armadillo.atmark-techno.com>]

---

# アプリケーションノート: Armadillo-IoT ゲートウェイ A6 省電力画像監視システム

株式会社アットマークテクノ

製作著作 © 2022 Atmark Techno, Inc.

Version 1.0.0  
2022/02/08

---

# 目次

1. システム概要	6
1.1. システムの機能	6
1.2. システム構成図	6
1.3. Armadillo 上で動作するシステム全体のフロー	7
1.3.1. 各処理のシーケンス図	8
1.3.1.1. Setup	8
1.3.1.2. SystemOperation	8
1.4. Web サーバ上で動作するアプリケーション	9
1.5. データストア仕様	10
2. 用意するもの	11
3. システム利用手順	12
3.1. セットアップ方法	12
3.1.1. EC2 の設定	12
3.1.1.1. インスタンスの作成	12
3.1.1.2. インスタンスへの IAM ロールの追加	14
3.1.1.3. インスタンスへの接続情報の取得	19
3.1.2. S3 の設定	20
3.1.2.1. S3 バケットの作成	20
3.1.2.2. S3 バケットのライフサイクルルールの追加	22
3.1.3. IAM ユーザー作成	25
3.1.3.1. ユーザーを追加	26
3.1.3.2. アクセス許可の設定	27
3.1.3.3. タグの追加(オプション)	28
3.1.3.4. 確認画面	29
3.1.3.5. IAM ユーザー作成完了	30
3.1.4. インストールディスクの作成	31
3.1.5. 設定ファイルの書き込み	31
3.1.5.1. 各種設定ファイルの配置	31
3.1.5.2. 初期設定ファイルの編集	32
3.1.5.3. LTE 設定ファイル (/etc/aiot-modem-control/startup.conf) の編集	34
3.1.5.4. SD カードの取り外し	34
3.1.6. ソフトウェアのインストール	34
3.2. システムの起動	34
4. 動作の確認	36
4.1. ブラウザから撮影した画像を閲覧	36
4.1.1. Armadillo Camera ページの画面説明	36
5. Appendix	38
5.1. 本アプリケーションの各種ファイル	38

## 目次

1.1. システムの構成図	6
1.2. AWS 内のシステム構成図	7
1.3. システム全体のフロー	7
1.4. 初回起動時のシーケンス図	8
1.5. システム起動後のシーケンス図	9
1.6. Web アプリケーションのシーケンス図	10
3.1. インスタンスの作成	12
3.2. AMI の選択	12
3.3. インスタンスタイプの選択	12
3.4. セキュリティグループの設定	13
3.5. セキュリティグループの設定内容	13
3.6. キーペアの作成	14
3.7. IAM ロールの割当	14
3.8. IAM ロールの作成①	15
3.9. IAM ロールの作成②	15
3.10. ユースケースの選択	16
3.11. IAM ロールへアタッチするポリシーの選択①	16
3.12. IAM ロールへアタッチするポリシーの選択②	16
3.13. タグの設定	17
3.14. ロール名の設定	18
3.15. ロールの選択と保存	19
3.16. インスタンスの再起動	19
3.17. インスタンスの接続	19
3.18. インスタンス接続情報の表示	20
3.19. バケットの作成	20
3.20. バケットの名称設定	21
3.21. ACL の設定	21
3.22. パブリックアクセスの設定	22
3.23. ライフサイクルルールの作成①	23
3.24. ライフサイクルルールの作成②	23
3.25. ライフサイクルルールの設定①	24
3.26. ライフサイクルルールの設定②	25
3.27. IAM ユーザーの追加①	26
3.28. IAM ユーザーの追加②	26
3.29. IAM ユーザーの設定	27
3.30. IAM ユーザーへアタッチするポリシーの選択①	28
3.31. IAM ユーザーへアタッチするポリシーの選択②	28
3.32. IAM ユーザーへのタグの追加	29
3.33. IAM ユーザーの作成	30
3.34. csv のダウンロード	31
3.35. 設定ファイルの配置場所	32
3.36. 設定ファイルの配置	32
3.37. 初期設定ファイルの編集	33
3.38. parameter.json の編集例	34
3.39. システムの接続	35
4.1. Armadillo Camera ページの表示	36
4.2. Armadillo Camera ページ	36
4.3. Armadillo Camera ページの画面説明	37

## 表目次

1.1. データストア仕様 .....	10
3.1. セキュリティグループの設定 .....	13
3.2. 初期設定ファイルの設定項目 .....	33
3.3. インストールの進捗と LED の対応 .....	34

# 1. システム概要

本アプリケーションノートでは、Armadillo-IoT ゲートウェイ A6(以下 Armadillo)を使用した省電力画像監視システムとして汎用的な処理を実装したサンプルアプリケーションについて紹介します。

## 1.1. システムの機能

本システムには以下の機能が実装されています。

- ・ USB カメラから画像を取得する機能
- ・ 取得した画像を Armadillo に接続された USB メモリなどの外部ストレージに保存する機能
- ・ 取得した画像やその他情報をクラウドにアップロードする機能
- ・ 上記を実行後、間欠動作を行い省電力で動作する機能
- ・ 一定間隔または接点出力のセンサによる割り込みで起床し、再び上記の動作を行う機能
- ・ コンテンツサーバ上にある画像を Web ブラウザから閲覧する機能

## 1.2. システム構成図

本システムの構成図を以下に示します。

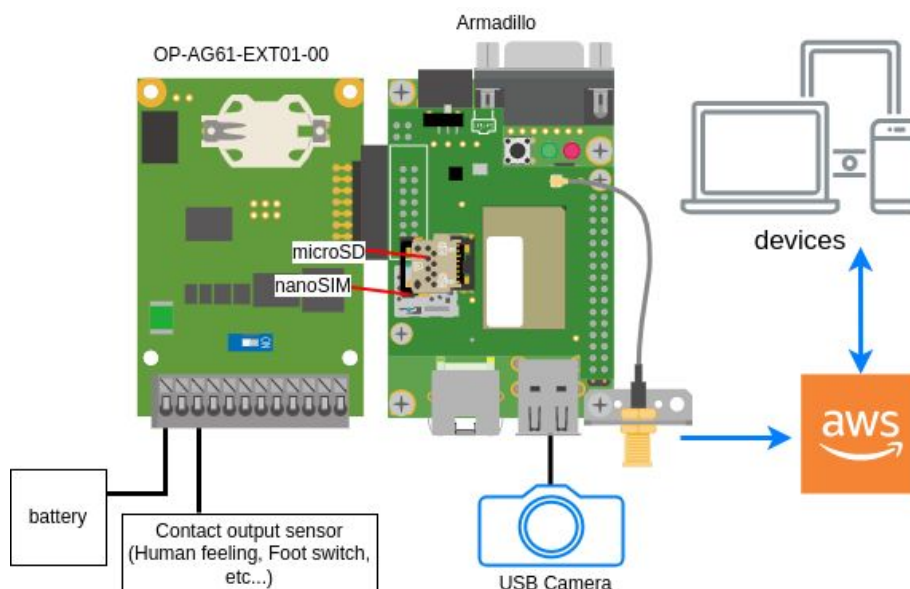


図 1.1 システムの構成図

AWS 内のシステム構成図を以下に示します。

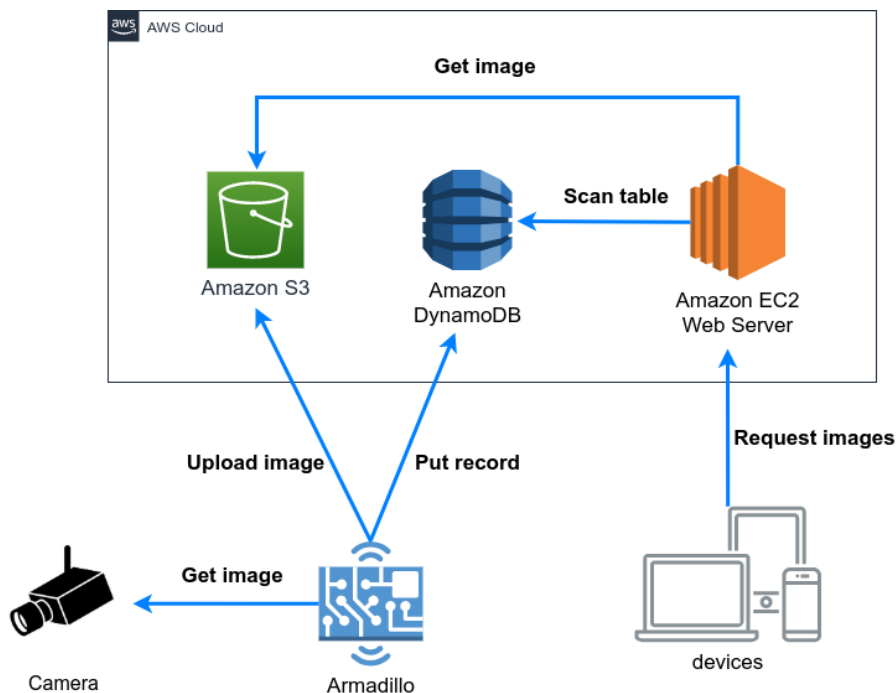


図 1.2 AWS 内のシステム構成図

### 1.3. Armadillo 上で動作するシステム全体のフロー

Armadillo の電源投入後からの状態遷移図を以下に示します。

図中の各処理の内容については「1.3.1. 各処理のシーケンス図」を参照してください。

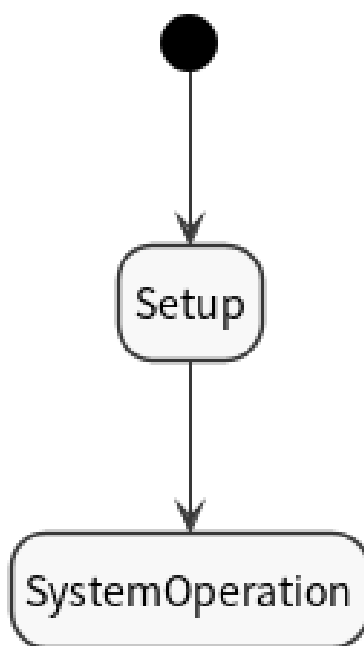


図 1.3 システム全体のフロー

### 1.3.1. 各処理のシーケンス図

「1.3. Armadillo 上で動作するシステム全体のフロー」の状態遷移図中の各処理のシーケンス図を以下に示します。

#### 1.3.1.1. Setup

インストールディスクを使用し、初回起動時のセットアップを行う際のシーケンス図です。

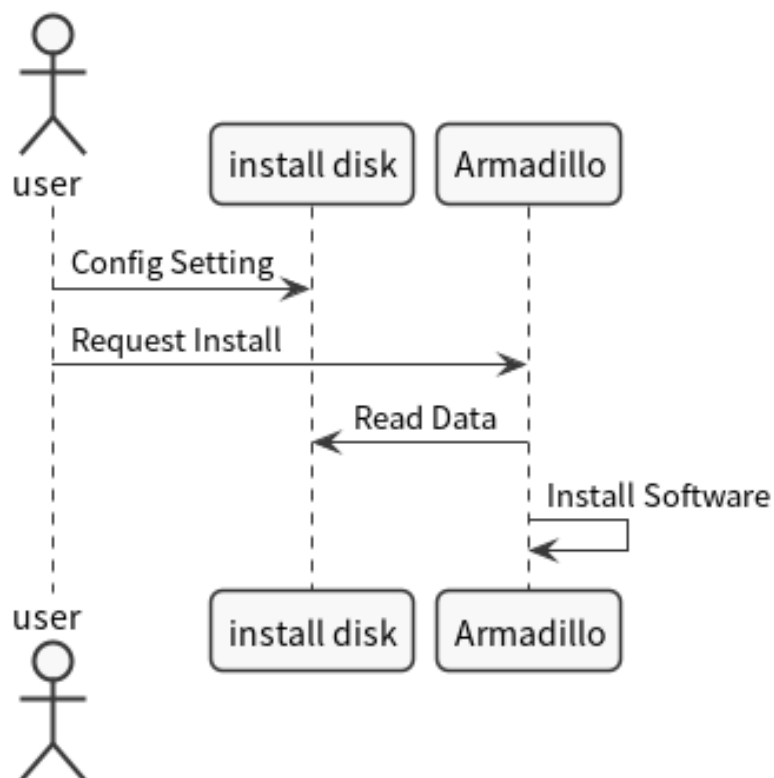


図 1.4 初回起動時のシーケンス図

#### 1.3.1.2. SystemOperation

システム起動後、カメラから取得した画像をクラウドにアップロードするまでのシーケンス図です。



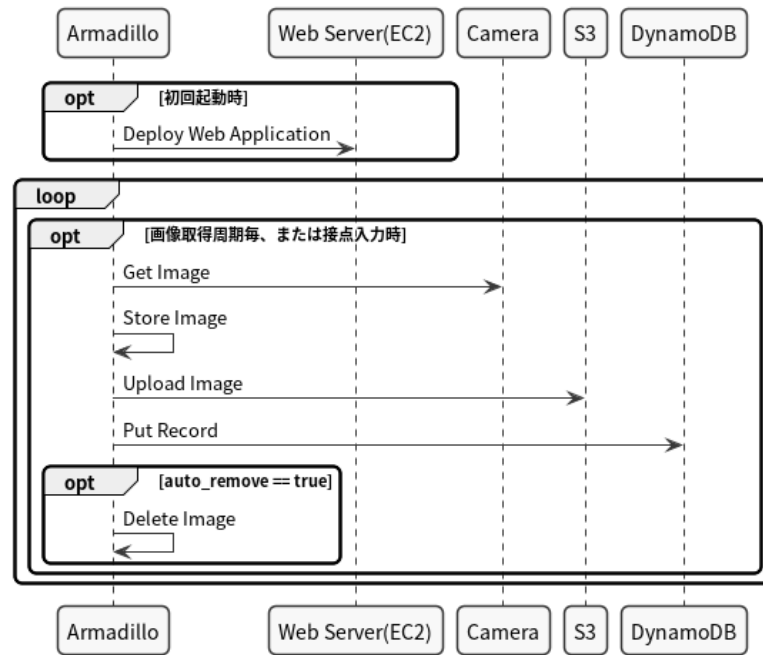


図 1.5 システム起動後のシーケンス図

## 1.4. Web サーバ上で動作するアプリケーション

Amazon Elastic Compute Cloud(EC2)内の Web サーバ上で動作するアプリケーションのシーケンス図です。

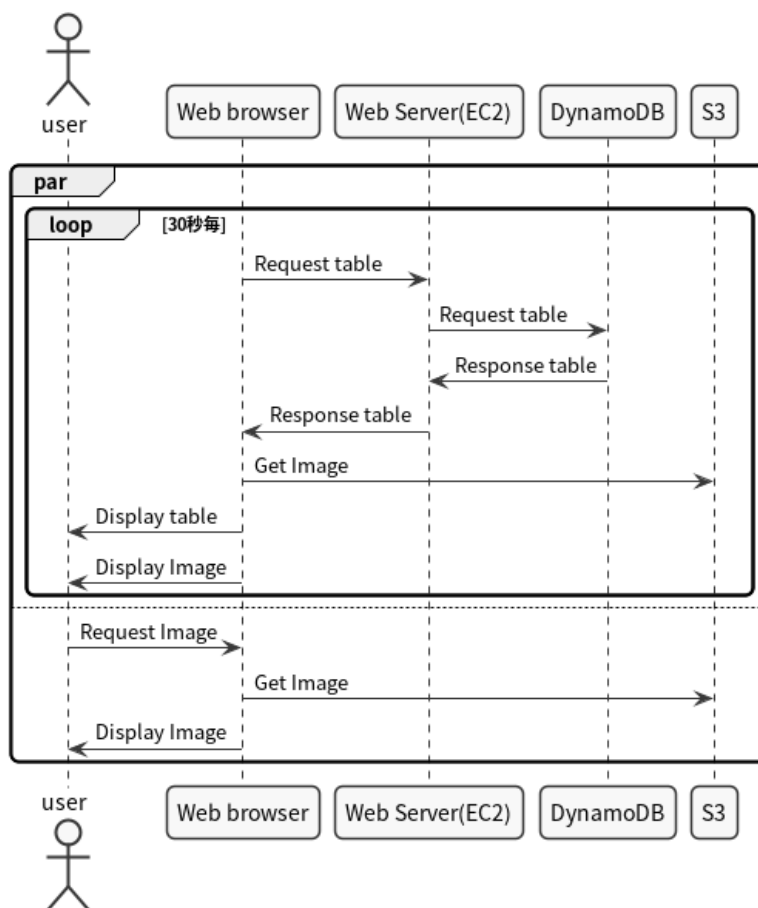


図 1.6 Web アプリケーションのシーケンス図

## 1.5. データストア仕様

本システムのデータストア仕様を以下の表に示します。

表 1.1 データストア仕様

データ内容	生成タイミング	更新タイミング	データ名
画像	画像取得時	更新しない	[画像取得日時]
画像取得・S3 アップロード 周期	ユーザー設定	ユーザー設定	operation_interval_min

## 2. 用意するもの

---

本アプリケーションノートでは以下の物を使用します。

- ・ 以下の条件を満たす PC
  - ・ インターネット接続可能
  - ・ Web ブラウザが利用可能
  - ・ microSD カードへの読み書きが可能
- ・ Armadillo-IoT ゲートウェイ A6 [<https://armadillo.atmark-techno.com/armadillo-iot-a6/models>]
- ・ Armadillo-IoT ゲートウェイ A6 U1 モデル用 拡張 I/O ボード 01 [<https://armadillo.atmark-techno.com/option-products/OP-AG61-EXT01-00>]
- ・ USB カメラ
  - ・ UVC (USB Video Class) に対応している必要があります
- ・ microSD カード (4GB 以上)
- ・ 接点出力が可能なセンサ
- ・ インターネットへの接続が可能な nanoSIM

## 3. システム利用手順

実際に本システムを Armadillo 上で動作させる手順を説明します。

### 3.1. セットアップ方法

以下の手順は、既に AWS のアカウントを作成し、AWS マネジメントコンソールにログインできていることを前提としています。AWS アカウントの作成方法については、こちら [https://aws.amazon.com/jp/register-flow/] を参照してください。

#### 3.1.1. EC2 の設定

後に Armadillo がカメラから取得した画像を閲覧するために、Web サーバーを Amazon Elastic Compute Cloud(EC2)上に構築します。本手順では、EC2 のインスタンスの作成を行います。EC2 のインスタンスの作成を行うことができる IAM ユーザーで作業を行ってください。

##### 3.1.1.1. インスタンスの作成

EC2 インスタンスページ [https://ap-northeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#Instances:] にアクセスし、「インスタンスを起動」をクリックしてください。



図 3.1 インスタンスの作成

「ステップ 1: Amazon マシンイメージ(AMI)」では、無料枠のある「Ubuntu Server 20.04 LTS (HVM)」の 64 ビットを選択してください。



図 3.2 AMI の選択

「ステップ 2: インスタンスタイプの選択」では、無料枠の「t2.micro」を選択し、「確認と作成」をクリックしてください。

現在選択中: t2.micro (- ECU, 1 vCPU, 2.5 GHz, -, 1 GiB メモリ, EBS のみ)

	ファミリー	タイプ	vCPU ①	メモリ (GiB)	インスタンスストレージ (GB) ①	EBS 最適化利用 ①	ネットワークパフォーマンス ①	IPv6 サポート ①
<input type="checkbox"/>	t2	t2.nano	1	0.5	EBS のみ	-	低から中	はい
<input checked="" type="checkbox"/>	t2	t2.micro	1	1	EBS のみ	-	低から中	はい
<input type="checkbox"/>	t2	t2.small	1	2	EBS のみ	-	低から中	はい

図 3.3 インスタンスタイプの選択

「ステップ 7: インスタンス作成の確認」では、「セキュリティグループの編集」をクリックしてください。

▼ セキュリティグループ セキュリティグループの編集

セキュリティグループ名 launch-wizard-11  
 説明 launch-wizard-11 created 2022-01-26T11:22:19.323+09:00

タイプ ⓘ	プロトコル ⓘ	ポート範囲 ⓘ	ソース ⓘ	説明 ⓘ
SSH	TCP	22	0.0.0.0/0	

図 3.4 セキュリティグループの設定

「ステップ 6: セキュリティグループの設定」では、「ルールの追加」をクリックし、以下の様に設定して「確認と作成」をクリックしてください。

表 3.1 セキュリティグループの設定

タイプ	プロトコル	ポート範囲	ソース	説明
HTTP	TCP	80	0.0.0.0/0	空白

タイプ ⓘ	プロトコル ⓘ	ポート範囲 ⓘ	ソース ⓘ	説明 ⓘ
SSH	TCP	22	カスタム 0.0.0.0/0	例: SSH for Admin Desktop
HTTP	TCP	80	カスタム 0.0.0.0, ::0	例: SSH for Admin Desktop

ルールの追加

図 3.5 セキュリティグループの設定内容

再度「ステップ 7: インスタンス作成の確認」に戻りますので、右下の「起動」をクリックしてください。クリックすると、以下のポップアップが出るので、「新しいキーペアの作成」を選択し、キーペアのタイプを「RSA」、キーペア名に任意の文字列を入力して「キーペアのダウンロード」を行ってください。以下の例ではキーペア名を「aiota6\_monitoring\_camera」として行っています。

**既存のキーペアを選択するか、新しいキーペアを作成します。**
×

キーペアは、AWS が保存するパブリックキーとユーザーが保存するプライベートキーファイルで構成されます。組み合わせて使用することで、インスタンスに安全に接続できます。Windows AMI の場合、プライベートキーファイルは、インスタンスへのログインに使用されるパスワードを取得するために必要です。Linux AMI の場合、プライベートキーファイルを使用してインスタンスに SSH で安全に接続できます。Amazon EC2 は ED25519 および RSA キーペアタイプをサポートしています。

注: 選択したキーペアは、このインスタンスに対して権限がある一連のキーに追加されます。「パブリック AMI から既存のキーペアを削除する」の詳細情報をご覧ください。

新しいキーペアの作成

キーペアのタイプ

RSA  ED25519

キーペア名

続行するには、事前にプライベートキーファイル (\*.pem ファイル) をダウンロードする必要があります。それを、安全でアクセス可能な場所に保存します。一度作成されたファイルは再度ダウンロードすることはできなくなります。

図 3.6 キーペアの作成

「[キーペア名].pem」を任意の場所に保存しておいてください。その後、「インスタンスの作成」をクリックしてください。しばらくするとインスタンスの起動が完了します。

### 3.1.1.2. インスタンスへの IAM ロールの追加

作成した EC2 インスタンスは、S3 と DynamoDB への読み込みアクセスが可能である必要があります。本手順では、作成した EC2 インスタンスに適切な IAM ロールを割り当てます。

EC2 インスタンスページ [<https://ap-northeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#Instances:>]から先程作成したインスタンスを選択し、「アクション」→「セキュリティ」→「IAM ロールを変更」をクリックしてください。



図 3.7 IAM ロールの割当

「新しい IAM ロールを作成」をクリックしてください。

**IAM ロールを変更** 情報

IAM ロールをインスタンスにアタッチします。

インスタンス ID

**IAM ロール**

インスタンスにアタッチする IAM ロールを選択するか、まだ作成していない場合は新しいロールを作成します。選択したロールによって、現在インスタンスにアタッチされているロールが置き換えられます。

IAM ロールを選択

**⚠ IAM ロールがありません** を選択すると、インスタンスに現在アタッチされている IAM ロールが削除されます。選択したインスタンスから を削除してよろしいですか?

キャンセル

図 3.8 IAM ロールの作成①

新しいタブでページが開かれるので、「ロールを作成」をクリックしてください。

IAM > ロール

**ロール (95) 情報**

IAM ロールは、短期間有効な認証情報を持つアクセス権を持つアカウント作成できるアイデンティティです。信頼するエンティティにロールを委任することもできます。

< 1 2 3 4 5 >

**ロール名**  **信頼されたエンティティ**  **最後のアクティビティ**

図 3.9 IAM ロールの作成②

「一般的なユースケース」、もしくは「または、サービスを選択してユースケースを表示します」から「EC2」を選択して、「次のステップ: アクセス権限」をクリックしてください。

## ロールの作成



### 信頼されたエンティティの種類を選択

<b>AWS サービス</b> EC2、Lambda、およびその他	<b>別の AWS アカウント</b> お客様またはサードパーティーに属しています	<b>ウェブ ID</b> Cognito または任意の OpenID プロバイダ	<b>SAML 2.0 フェデレーション</b> 企業ディレクトリ
--------------------------------------	--	--	--------------------------------------

AWS のサービスによるアクションの代行を許可します。 [詳細はこちら](#)

### ユースケースの選択

#### 一般的なユースケース

##### EC2

Allows EC2 instances to call AWS services on your behalf.

##### Lambda

Allows Lambda functions to call AWS services on your behalf.

または、サービスを選択してユースケースを表示します

[API Gateway](#)
[CloudWatch Events](#)
[EKS](#)
[IoT SiteWise](#)
[DNS](#)

図 3.10 ユースケースの選択

以下の 2 つのポリシーをアタッチし、「次のステップ： タグ」に進みます。

- ・ AmazonDynamoDBReadOnlyAccess
- ・ AmazonS3ReadOnlyAccess

## ロールの作成



### ▼ Attach アクセス権限ポリシー

新しいロールにアタッチするポリシーを 1 つ以上選択します。

ポリシーの作成 🔄

---

ポリシーのフィルタ 
1 件の結果を表示中

	ポリシー名	次として使用
<input checked="" type="checkbox"/>	AmazonDynamoDBReadOnlyAccess	Permissions policy (4)

図 3.11 IAM ロールへアタッチするポリシーの選択①

ポリシーのフィルタ 
1 件の結果を表示中

	ポリシー名	次として使用
<input checked="" type="checkbox"/>	AmazonS3ReadOnlyAccess	Permissions policy (4)

図 3.12 IAM ロールへアタッチするポリシーの選択②

タグは設定不要です。「次のステップ： 確認」に進みます。



## ロールの作成



### タグの追加 (オプション)

IAM タグは、ロール に追加できるキーと値のペアです。タグには、E メールアドレスなどのユーザー情報を含めるか、役職などの説明文とすることができます。タグを使用して、この ロール のアクセスを整理、追跡、制御できます。 [詳細はこちら](#)

キー	値 (オプション)	削除
<input type="text" value="新しいキーを追加"/>	<input type="text"/>	

さらに 50 個のタグを追加できます。

[キャンセル](#)[戻る](#)[次のステップ: 確認](#)

### 図 3.13 タグの設定

「ロール名」に任意の文字列を設定してください。以下の例では「EC2WebServer」としています。ロール名が決まったら「ロールの作成」をクリックしてください。

## ロールの作成

1 2 3 4

## 確認

以下に必要な情報を指定してこのロールを見直してから、作成してください。





ロール名\*

英数字と「+,.@-」を使用します。最大 64 文字。

ロールの説明

最大 1000 文字。英数字と「+,.@-」を使用します。

信頼されたエンティティ AWS のサービス: ec2.amazonaws.com

ポリシー  [AmazonDynamoDBReadOnlyAccess](#)   
 [AmazonS3ReadOnlyAccess](#) 

アクセス権限の境界 アクセス権限の境界が設定されていません

追加されたタグはありません。

\* 必須

キャンセル

戻る

ロールの作成

## 図 3.14 ロール名の設定

「IAM ロールを変更」の画面に戻り、更新ボタンをクリックし、プルダウンメニューから作成した IAM ロールを選択してください。選択したら、「保存」をクリックしてください。



図 3.15 ロールの選択と保存

EC2 インスタンスページ [https://ap-northeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#Instances:]に戻り、作成したインスタンスを選択してインスタンスの再起動を行ってください。しばらくすると再起動が完了します。



図 3.16 インスタンスの再起動

### 3.1.1.3. インスタンスへの接続情報の取得

EC2 インスタンスページ [https://ap-northeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#Instances:]から先程作成したインスタンスを選択し、「接続」をクリックしてください。



図 3.17 インスタンスの接続

「インスタンスに接続」の「SSH クライアント」タブを開き、「4. ご使用中のインスタンスのパブリック DNS を使用してインスタンスに接続」の下にある文字列をメモしてください。

### インスタンスに接続 情報

これらのオプションのいずれかを使用してインスタンス ID [REDACTED] に接続する

EC2 Instance Connect
セッションマネージャー
SSH クライアント
EC2 シリアルコンソール

インスタンス ID

- SSH クライアントを開きます。
- プライベートキーファイルを見つけます。このインスタンスの起動に使用されるキーは `keshite_iiyatu.pem` です。
- 必要に応じて、このコマンドを実行して、キーが公開されていないことを確認します。
 

```
chmod 400 [REDACTED].pem
```
- ご使用のインスタンスのパブリック DNS を使用してインスタンスに接続:
 

```
ec2-[REDACTED].ap-northeast-1.compute.amazonaws.com
```

例:

```
ssh -i "[REDACTED].pem" ubuntu@[REDACTED].ap-northeast-1.compute.amazonaws.com
```

**注意:** ほとんどの場合、推測されたユーザー名に間違いはありませんが、AMI の使用手順を読んで AMI の所有者がデフォルトの AMI ユーザー名を変更していないか確認してください。

図 3.18 インスタンス接続情報の表示

以上で EC2 の設定は完了です。

## 3.1.2. S3 の設定

次に Amazon Simple Storage Service(S3)上にバケットを作成します。S3 のバケット作成を行うことができる IAM ユーザーで作業を行ってください。

### 3.1.2.1. S3 バケットの作成

S3 バケットページ [<https://s3.console.aws.amazon.com/s3/home?region=ap-northeast-1>]にアクセスし、「バケットを作成」をクリックしてください。

図 3.19 バケットの作成

「バケット名」は任意の文字列、リージョンは「アジアパシフィック(東京) ap-northeast-1」を選択します。

### 一般的な設定

バケット名

s3bucket

バケット名は一意である必要があり、スペース、または大文字を含めることはできません。[バケットの命名規則をご参照ください](#)

AWS リージョン

アジアパシフィック (東京) ap-northeast-1 ▼

既存のバケットから設定をコピー - オプション  
次の設定のバケット設定のみがコピーされます。

バケットを選択する

図 3.20 バケットの名称設定

「オブジェクト所有者」では「ACL 有効」と「希望するバケット所有者」を選択します。

### オブジェクト所有者 Info

他の AWS アカウントからこのバケットに書き込まれたオブジェクトの所有権と、アクセスコントロールリスト (ACL) の使用を管理します。オブジェクトの所有権は、オブジェクトへのアクセスを指定できるユーザーを決定します。

ACL 無効 (推奨)

このバケット内のすべてのオブジェクトは、このアカウントによって所有されます。このバケットとそのオブジェクトへのアクセスは、ポリシーのみを使用して指定されません。

ACL 有効

他の AWS アカウントがこのバケット内のオブジェクトの所有者となることができます。このバケットとそのオブジェクトへのアクセスは、ACL を使用して指定できます。

オブジェクト所有者

希望するバケット所有者  
このバケットに書き込まれた新しいオブジェクトが bucket-owner-full-control 既定 ACL を指定する場合、その所有者はバケット所有者となります。それ以外の場合は、オブジェクトライターが所有者となります。

オブジェクトライター  
オブジェクトライターが引き続きオブジェクト所有者となります。

新しいオブジェクトにのみオブジェクトの所有権を強制する場合、バケットポリシーは、オブジェクトのアップロードに bucket-owner-full-control 既定 ACL が必須であることを指定する必要があります。[詳細はこちら](#)

図 3.21 ACL の設定

「このバケットのブロックパブリックアクセス設定」では「パブリックアクセスをすべてブロック」のチェックを外し、「現在の設定により、このバケットとバケット内のオブジェクトが公開される可能性があることを承認します。」にチェックを入れて「バケットの作成」をクリックしてください。



## このバケットのブロックパブリックアクセス設定

パブリックアクセスは、アクセスコントロールリスト (ACL、Access Control List)、バケットポリシー、アクセスポイントポリシー、またはそのすべてを介してバケットとオブジェクトに許可されます。このバケットとそのオブジェクトへの公開アクセスが確実にブロックされるようにするには、[パブリックアクセスをすべてブロック] を有効にします。これらの設定はこのバケットとそのアクセスポイントにのみ適用されます。AWS では [パブリックアクセスをすべてブロック] を有効にすることをお勧めしますが、これらの設定を適用する前に、アプリケーションが公開アクセスなしで正しく機能することをご確認ください。このバケットやオブジェクトへのある程度の公開アクセスが必要な場合は、各ストレージユースケースに合わせて以下にある個々の設定をカスタマイズできます。 [詳細](#)

### パブリックアクセスをすべてブロック

この設定をオンにすることは、以下の 4 つの設定をすべてオンにすることと同じです。次の各設定は互いに独立しています。

- 新しいアクセスコントロールリスト (ACL) を介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする**  
S3 は、新しく追加されたバケットまたはオブジェクトに適用されたパブリックアクセス許可をブロックし、既存のバケットおよびオブジェクトに対する新しいパブリックアクセス ACL が作成されないようにします。この設定では、ACL を使用して S3 リソースへのパブリックアクセスを許可する既存のアクセス許可は変更されません。
- 任意のアクセスコントロールリスト (ACL) を介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする**  
S3 はバケットとオブジェクトへのパブリックアクセスを付与するすべての ACL を無視します。
- 新しいパブリックバケットポリシーまたはアクセスポイントポリシーを介して付与されたバケットとオブジェクトへのパブリックアクセスをブロックする**  
S3 は、バケットとオブジェクトへのパブリックアクセスを許可する新しいバケットポリシーおよびアクセスポイントポリシーをブロックします。この設定は、S3 リソースへのパブリックアクセスを許可する既存のポリシーを変更しません。
- 任意のパブリックバケットポリシーまたはアクセスポイントポリシーを介したバケットとオブジェクトへのパブリックアクセスとクロスアカウントアクセスをブロックする**  
S3 は、バケットとオブジェクトへのパブリックアクセスを付与するポリシーを使用したバケットまたはアクセスポイントへのパブリックアクセスとクロスアカウントアクセスを無視します。



**パブリックアクセスのブロックをすべてオフにすると、このバケットとバケット内のオブジェクトが公開される可能性があります。**

AWS では、静的ウェブサイトホスティングなど、特定の検証済みのユースケースでパブリックアクセスが必要な場合を除き、すべてのパブリックアクセスをブロックすることをお勧めします。

現在の設定により、このバケットとバケット内のオブジェクトが公開される可能性があることを承認します。

図 3.22 パブリックアクセスの設定

バケット一覧に作成したバケットが表示されたら完了です。

### 3.1.2.2. S3 バケットのライフサイクルルールの追加

「3.1.2.1. S3 バケットの作成」で作成したバケットをそのまま使用しても問題ありませんが、現状の設定ではバケットに保存された画像は手動で削除しない限り永遠に残り続けます。S3 は保存容量による課金がありますので、このままの運用では料金が膨れ上がっていきます。

本手順では、作成した S3 バケットにライフサイクルルールを追加し、保存から 2 週間で自動的に削除されるように設定します。

作成した S3 のバケットページから、「管理」タブをクリックします。



図 3.23 ライフサイクルルールの作成①

管理タブから「ライフサイクルルールを作成する」をクリックしてください。



図 3.24 ライフサイクルルールの作成②

「ライフサイクルルールを作成する」ページに遷移するので、以下の様に設定します。

1. 「ライフサイクルルール名」：S3\_lifecycle
2. 「ルールスコープを選択」：「バケット内のすべてのオブジェクトに適用」を選択
3. 「このルールがバケット内のすべてのオブジェクトに適用されることを了承します。」にチェック
4. 「ライフサイクルルールのアクション」は以下の 2 つにチェック
  - a. 「オブジェクトの現行バージョンを有効期限にする」
  - b. 「オブジェクトの非現行バージョンを完全に削除」
5. 「オブジェクトの現行バージョンの有効期限が切れる」の「オブジェクト作成後の日数」を 7 に設定
6. 「オブジェクトの以前のバージョンを完全に削除する」の「オブジェクトが以前のバージョンになってからの日数」を 7 に設定

## ライフサイクルルールを作成する

### ライフサイクルルールの設定

ライフサイクルルール名

S3\_lifecycle

最大 255 文字

ルールスコープを選択

1つ以上のフィルターを使用してこのルールのスコープを制限する

**バケット内のすべてのオブジェクトに適用**



#### バケット内のすべてのオブジェクトに適用

ルールを特定のオブジェクトに適用する場合は、フィルターを使用してそれらのオブジェクトを識別する必要があります。[Limit the scope of this rule using one or more filters] を選択します。詳細 [🔗](#)

**このルールがバケット内のすべてのオブジェクトに適用されることを了承します。**

### ライフサイクルルールのアクション

このルールで実行するアクションを選択します。リクエストごとの料金が適用されます。詳細 [🔗](#) または [Amazon S3 の料金](#) [🔗](#) を参照してください

- オブジェクトの最新バージョンをストレージクラス間で移動
- オブジェクトの非現行バージョンをストレージクラス間で移動

**オブジェクトの現行バージョンを有効期限切れにする**

**オブジェクトの非現行バージョンを完全に削除**

- 有効期限切れのオブジェクト削除マーカーまたは不完全なマルチパートアップロードを削除  
オブジェクトタグまたはオブジェクトサイズでフィルタリングする場合、これらのアクションはサポートされません。

図 3.25 ライフサイクルルールの設定①



### オブジェクトの現行バージョンの有効期限が切れる

バージョン対応バケットの場合、Amazon S3 は削除マーカを追加し、オブジェクトの現行バージョンは非現行バージョンとして保持されます。バージョン非対応バケットの場合、Amazon S3 はオブジェクトを完全に削除します。[詳細はこちら](#)

オブジェクト作成後の日数

### オブジェクトの非現行バージョンを完全に削除

Amazon S3 がオブジェクトの指定された非現行バージョンを完全に削除するタイミングを選択します。[詳細はこちら](#)

オブジェクトが現行バージョンでなくなってからの日数

保持する新しいバージョンの数 - オプション

最大 100 バージョンにすることができます。他のすべての非現行バージョンは移動されます。

### 移行と有効期限切れのアクションを確認

最新バージョンのアクション	非現行バージョンのアクション
0 日	0 日
<ul style="list-style-type: none"><li>アップロードされたオブジェクト</li></ul>	<ul style="list-style-type: none"><li>オブジェクトが最新バージョンでなくなる</li></ul>
↓	↓
7 日	7 日
<ul style="list-style-type: none"><li>オブジェクトの有効期限切れ</li></ul>	<ul style="list-style-type: none"><li>最新の 0 個の非現行バージョンは保持されます。</li><li>他の非現行バージョンはすべて完全に削除されます</li></ul>

キャンセル **ルールの作成**

図 3.26 ライフサイクルルールの設定②

設定後、「ルールの作成」をクリックしてください。

以上で S3 の設定は完了です。

### 3.1.3. IAM ユーザー作成

IAM マネジメントコンソール [<https://console.aws.amazon.com/iam/home>]へログインしてください。その後、ユーザータブを開き、「ユーザーを追加」をクリックします。



図 3.27 IAM ユーザーの追加①



図 3.28 IAM ユーザーの追加②

### 3.1.3.1. ユーザーを追加

下記の通り入力、選択し「次のステップ：アクセス権限」に進みます。

- ・ ユーザー名
- ・ AWS アクセスの種類を両方選択
- ・ コンソールのパスワードは自動生成パスワードを選択
- ・ 「パスワードのリセットが必要」にチェックを入れる

## ユーザーを追加



### ユーザー詳細の設定

同じアクセスの種類とアクセス権限を使用して複数のユーザーを一度に追加できます。 [詳細はこちら](#)

ユーザー名\*

[+ 別のユーザーの追加](#)

### AWS アクセスの種類を選択

これらのユーザーが主に AWS にアクセスする方法を選択します。プログラムによるアクセスのみを選択しても、ユーザーは引き受けたロールを使用してコンソールにアクセスすることはできません。アクセスキーと自動生成されたパスワードは、最後のステップで提供されます。 [詳細はこちら](#)

AWS 認証情報タイプを選択\*  **アクセスキー - プログラムによるアクセス**  
AWS API、CLI、SDK などの開発ツールの **アクセスキー ID** と **シークレットアクセスキー** を有効にします。

**パスワード - AWS マネジメントコンソールへのアクセス**  
ユーザーに AWS マネジメントコンソールへのサインインを許可するための **パスワード** を有効にします。

コンソールのパスワード\*  自動生成パスワード  
 カスタムパスワード

パスワードのリセットが必要  ユーザーは次回のサインインで新しいパスワードを作成する必要があります  
ユーザーは、自動的に `IAMUserChangePassword` ポリシーを取得し、自分のパスワードを変更できるようにします。

図 3.29 IAM ユーザーの設定

### 3.1.3.2. アクセス許可の設定


下記の手順でポリシーをアタッチし、「次のステップ： タグ」に進みます。


- ・ 「既存のポリシーを直接アタッチ」を選択
- ・ 表示された中から以下にチェック
  - ・ AmazonS3FullAccess
  - ・ AmazonDynamoDBFullAccess


## ユーザーを追加



## ▼ アクセス許可の設定

 ユーザーをグループに追加

 アクセス権限を既存のユーザーからコピー

 既存のポリシーを直接アタッチ

ポリシーの作成

↻

ポリシーのフィルタ

1件の結果を表示中

	ポリシー名	タイプ	次として使用
<input checked="" type="checkbox"/>	▶ AmazonS3FullAccess	AWS による管理	Permissions policy (8)

図 3.30 IAM ユーザーへアタッチするポリシーの選択①

ポリシーのフィルタ

1件の結果を表示中

	ポリシー名	タイプ	次として使用
<input checked="" type="checkbox"/>	▶ AmazonDynamoDBFullAccess	AWS による管理	Permissions policy (8)

図 3.31 IAM ユーザーへアタッチするポリシーの選択②

## 3.1.3.3. タグの追加(オプション)

今回は設定不要です。「次のステップ：確認」に進みます。

## ユーザーを追加



### タグの追加 (オプション)

IAM タグは、ユーザー に追加できるキーと値のペアです。タグには、E メールアドレスなどのユーザー情報を含めるか、役職などの説明文とすることができます。タグを使用して、このユーザー のアクセスを整理、追跡、制御できます。 [詳細はこちら](#)

キー	値 (オプション)	削除
<input type="text" value="新しいキーを追加"/>	<input type="text"/>	

さらに 50 個のタグを追加できます。

[キャンセル](#)[戻る](#)[次のステップ: 確認](#)

図 3.32 IAM ユーザーへのタグの追加

#### 3.1.3.4. 確認画面

確認画面が表示されます。設定した通りの内容になっていることを確認し、「ユーザーの作成」をクリックしてください。

## ユーザーを追加



### 確認

選択内容を確認します。ユーザーを作成した後で、自動生成パスワードとアクセスキーを確認してダウンロードできます。

### ユーザー詳細

ユーザー名	monitoring_camera
AWS アクセスの種類	プログラムによるアクセスと AWS マネジメントコンソールへのアクセス
コンソールのパスワードの種類	自動生成
パスワードのリセットが必要	はい
アクセス権限の境界	アクセス権限の境界が設定されていません

### アクセス権限の概要

次のポリシー例は、上記のユーザーにアタッチされます。

タイプ	名前
管理ポリシー	AmazonS3FullAccess
管理ポリシー	AmazonDynamoDBFullAccess
管理ポリシー	IAMUserChangePassword

### タグ

追加されたタグはありません。

キャンセル 戻る ユーザーの作成

図 3.33 IAM ユーザーの作成

### 3.1.3.5. IAM ユーザー作成完了

成功すると下記のような画面が表示されます。後ほど Armadillo の設定で使用するため、ここでは必ず csv のダウンロードを忘れずに行ってください。行わなかった場合、再度 IAM ユーザーを作成する必要があります。

## ユーザーを追加

1 2 3 4 5

**成功**  
以下に示すユーザーを正常に作成しました。ユーザーのセキュリティ認証情報を確認してダウンロードできます。AWS マネジメントコンソールへのサインイン手順を E メールでユーザーに送信することもできます。今回が、これらの認証情報をダウンロードできる最後の機会です。ただし、新しい認証情報はいつでも作成できます。

AWS マネジメントコンソールへのアクセス権を持つユーザーは「[https://\[redacted\].signin.aws.amazon.com/console](https://[redacted].signin.aws.amazon.com/console)」でサインインできます

[.csv のダウンロード](#)

	ユーザー	アクセスキー ID	シークレットアクセスキー	パスワード	ログイン手順を Eメールで送信
▶	aiota6_monit...	[redacted]	***** 表示	***** 表示	Eメールの送信 <a href="#">🔗</a>

図 3.34 csv のダウンロード

ダウンロードしたファイル( `new_user_credentials.csv` )の内容は、以下のようなカンマ区切りの文字列になります。

```
User name,Password,Access key ID,Secret access key,Console login link
user,pass,AWS123,asdfghjkl,https://***.signin.aws.amazon.com/console
```

この例の場合、Access key ID の値は AWS123 で、Secret access key の値は asdfghjkl です。

### 3.1.4. インストールディスクの作成

監視カメラシステムのインストールディスクイメージをダウンロードしてください。

次にダウンロードしたインストールディスクイメージを SD カードに書き込みます。インストールディスクイメージは zip 圧縮されていますので、書き込み前に展開してください。

Armadillo-IoT ゲートウェイ A6 製品マニュアル 「インストールディスクの作成」 [[https://manual.atmark-techno.com/armadillo-iot-a6/armadillo-iota6\\_product\\_manual\\_ja-1.4.1/ch12.html#idm6175](https://manual.atmark-techno.com/armadillo-iot-a6/armadillo-iota6_product_manual_ja-1.4.1/ch12.html#idm6175)]の手順を参考に SD カードにインストールディスクイメージを書き込んでください。

### 3.1.5. 設定ファイルの書き込み

インストールディスクの第 1 パーティションには、本アプリケーションが動作するための設定を記入するファイルが格納されています。本手順ではそれらの設定ファイルの編集方法について説明します。

#### 3.1.5.1. 各種設定ファイルの配置

Armadillo が動作するための各種ファイルを配置します。

1. インストールディスクイメージが書き込まれた SD カードを PC に接続
2. 「ファイル」から「2.1MB ボリューム」をクリック

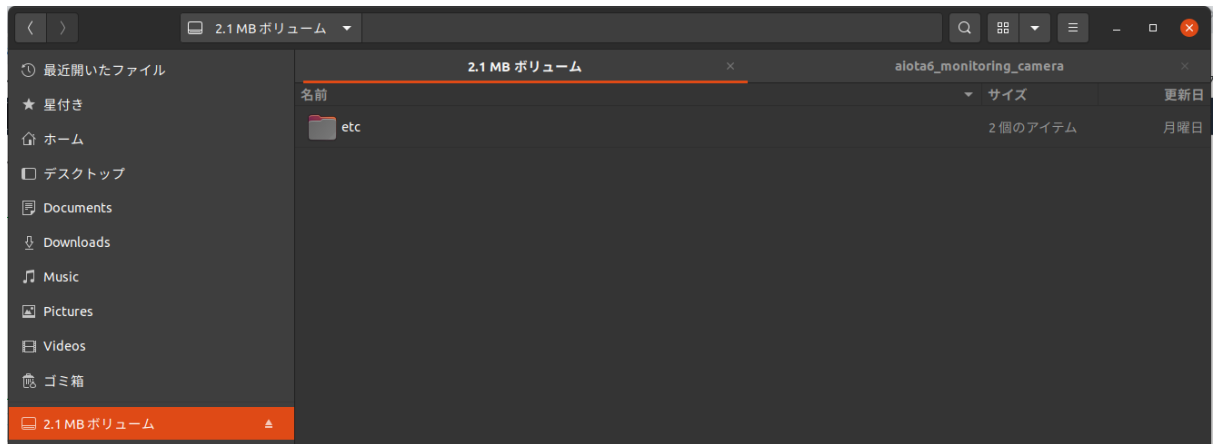


図 3.35 設定ファイルの配置場所

3. 下記のファイルを `etc/aiota6_monitoring_camera/` 以下に配置してください。
  - a. 「3.1.3.5. IAM ユーザー作成完了」でダウンロードした `new_user_credentials.csv` を `credentials.csv` にリネームして配置
  - b. 「3.1.1.1. インスタンスの作成」でダウンロードした `[キーペア名].pem`

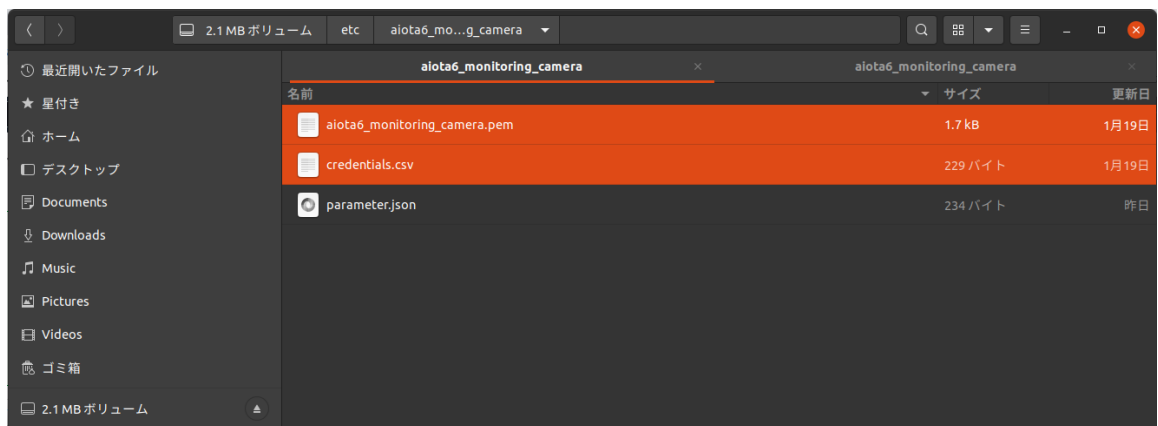


図 3.36 設定ファイルの配置

### 3.1.5.2. 初期設定ファイルの編集

本アプリケーションが動作する際の初期設定値の編集を行います。

1. 「ファイル」から「2.1MB ボリューム」をクリック
2. `etc/aiota6_monitoring_camera/parameter.json` をテキストエディタで開きます



```

1 {
2   "operation_interval_min": 60,
3   "s3_bucket_name": "",
4   "save_path": "",
5   "auto_remove": "true",
6   "ec2_public_dns": "",
7   "ec2_user_name": "ubuntu"
8 }

```

図 3.37 初期設定ファイルの編集

3. 以下の 7 項目を編集します ( s3\_bucket\_name と ec2\_public\_dns は必ず編集してください )

表 3.2 初期設定ファイルの設定項目

項目	説明	初期値(単位)
operation_interval_min	Armadillo が sleep モードから復帰するまでの時間です	60(分)
s3_bucket_name	Armadillo のデータアップロード先となる S3 のバケット名です。「3.1.2.1. S3 バケットの作成」で作成したバケットの名前を指定してください。	なし
save_path	Armadillo がカメラから取得した画像データを保存するディレクトリを絶対パスで指定します。USB メモリに保存する際は /dev/sda1 を、SD カードに保存する際は /dev/mmcblk1p1 を指定してください。何も指定しない場合は /opt/aiota6_monitoring_camera/pictures に保存されます。	なし
auto_remove	Armadillo がカメラから取得した画像データを AWS へのアップロード後に削除するかどうかを指定するオプションです。true なら削除され、それ以外の文字列の場合は削除されません。また、save_path に指定されたパスが不正であったり、何も指定しない場合にはこのオプションは自動的に true になります。	true
ec2_public_dns	「3.1.1.3. インスタンスへの接続情報の取得」でメモした「4. ご使用中のインスタンスのパブリック DNS を使用してインスタンスに接続」の下にある文字列をここに記入してください。	なし
ec2_user_name	「3.1.1.1. インスタンスの作成」で作成した EC2 インスタンス内のユーザー名です。本ドキュメントどおりに設定を進めた場合は初期値である ubuntu のままで問題ありません。	ubuntu

4. 以下は編集例です

```

1 {
2   "operation_interval_min": 60,
3   "s3_bucket_name": "s3bucket",
4   "save_path": "",
5   "auto_remove": "true",
6   "ec2_public_dns": "ec2-255-255-255-255.ap-northeast-1.compute.amazonaws.com",
7   "ec2_user_name": "ubuntu"
8 }

```

図 3.38 parameter.json の編集例

### 3.1.5.3. LTE 設定ファイル (/etc/aiot-modem-control/startup.conf) の編集

Armadillo-IoT ゲートウェイ A6 製品マニュアル 「6.2.4.2. LTE 設定ファイル (/etc/aiot-modem-control/startup.conf) の編集」 [[https://manual.atmark-techno.com/armadillo-iot-a6/armadillo-iota6\\_product\\_manual\\_ja-1.4.1/ch06.html#sec.lte\\_startup\\_conf](https://manual.atmark-techno.com/armadillo-iot-a6/armadillo-iota6_product_manual_ja-1.4.1/ch06.html#sec.lte_startup_conf)]を参照し、LTE 設定ファイルを編集してください

### 3.1.5.4. SD カードの取り外し

SD カードの 2 つのボリュームをアンマウントしてから、PC から SD カードを抜いてください。

以上で起動前の設定ファイルの書き込みは完了です。

## 3.1.6. ソフトウェアのインストール

作成したインストールディスクを microSD ユニットに装着し、サブユニット SW1(ユーザースイッチ)のスライドスイッチを microSD 側に設定して電源を投入してください。

Armadillo へのソフトウェアのインストールが開始されます。インストールには数分かかります。インストールの進捗は、Armadillo のユーザー LED の状態で確認することが出来ます。インストールの進捗と LED の状態の関係は以下の表の通りです。

表 3.3 インストールの進捗と LED の対応

進捗	ユーザー LED 赤	ユーザー LED 緑
実行中	消灯	点滅
正常終了	点灯	点灯
異常終了	消灯	点滅

LED が点灯に変わり、インストールが完了したら AC アダプタを抜いてください。

## 3.2. システムの起動

下記の図のように接続してください。SD カードを抜いてください。メインユニット CON5(USB ホストインターフェース)に USB カメラを接続してください。その後、Armadillo に電源を投入してください。

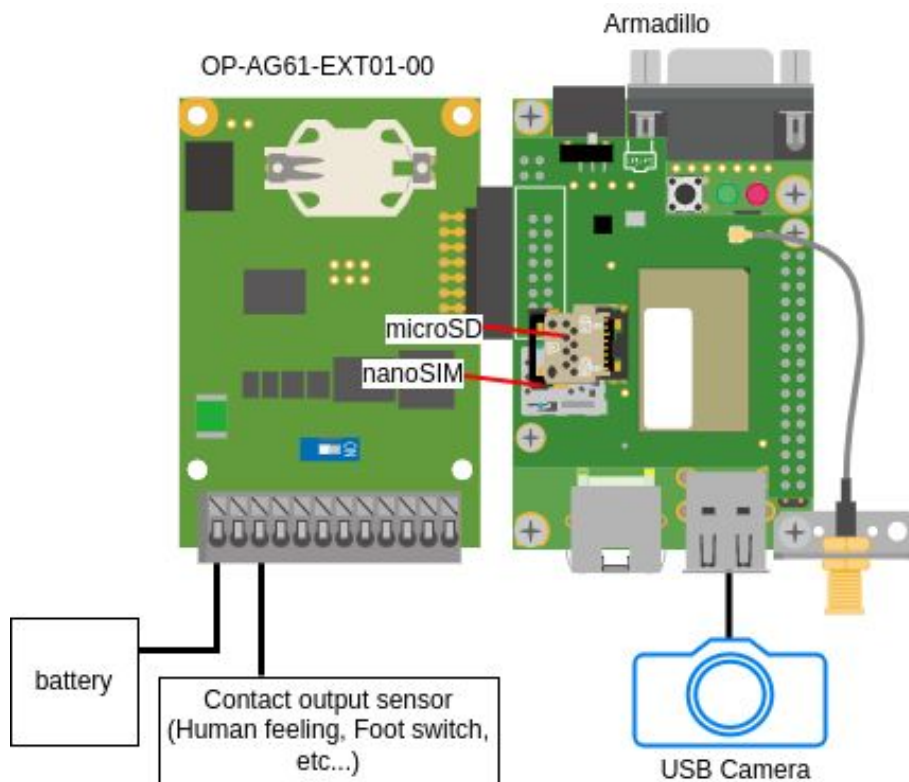


図 3.39 システムの接続

電源投入後、自動的にアプリケーションが起動し、AWS のセットアップを行います。AWS のセットアップ完了後に、「3.1.5.2. 初期設定ファイルの編集」で設定した周期の通りにカメラから画像の取得と、AWS へアップロードを行います。

## 4. 動作の確認

### 4.1. ブラウザから撮影した画像を閲覧

EC2 インスタンスページ [https://ap-northeast-1.console.aws.amazon.com/ec2/v2/home?region=ap-northeast-1#Instances:]から「3.1.1.1. インスタンスの作成」で作成した EC2 インスタンスのインスタンス ID をクリックしてください。「[インスタンス ID]のインスタンス概要」のページで「パブリック IPv4 DNS」の「オープンアドレス」をクリックすると、新規タブでページが開かれます。



図 4.1 Armadillo Camera ページの表示

サンプルアプリケーションでは https アクセスに対応していないため、URL の「https」を「http」に書き換えてアクセスしてください。

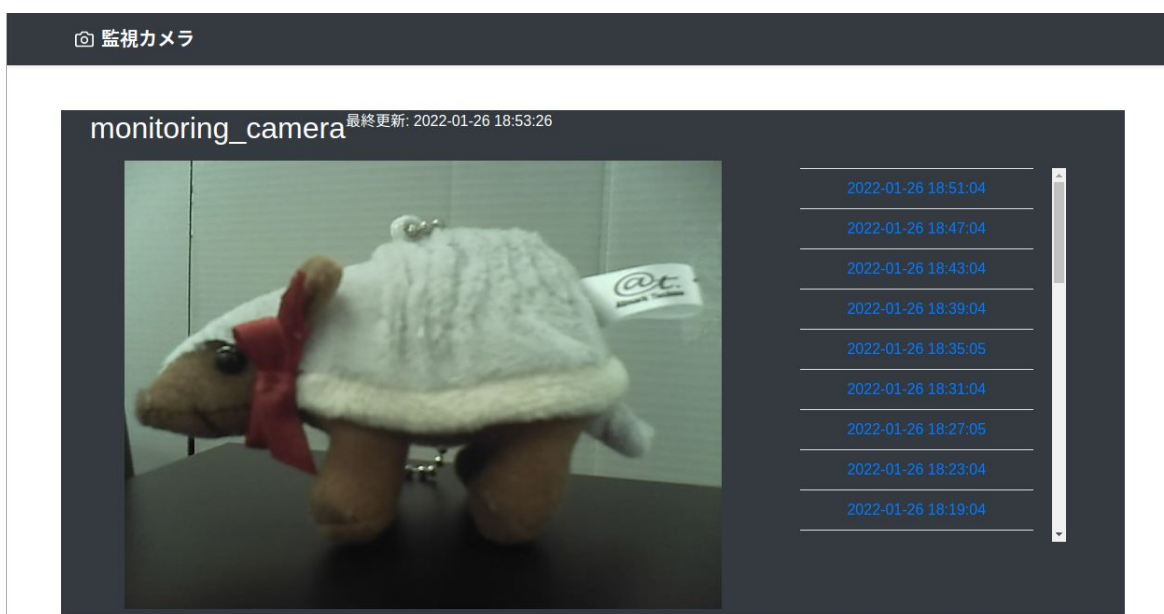


図 4.2 Armadillo Camera ページ

#### 4.1.1. Armadillo Camera ページの画面説明

Armadillo Camera ページの構成とそれぞれの動作について説明します。

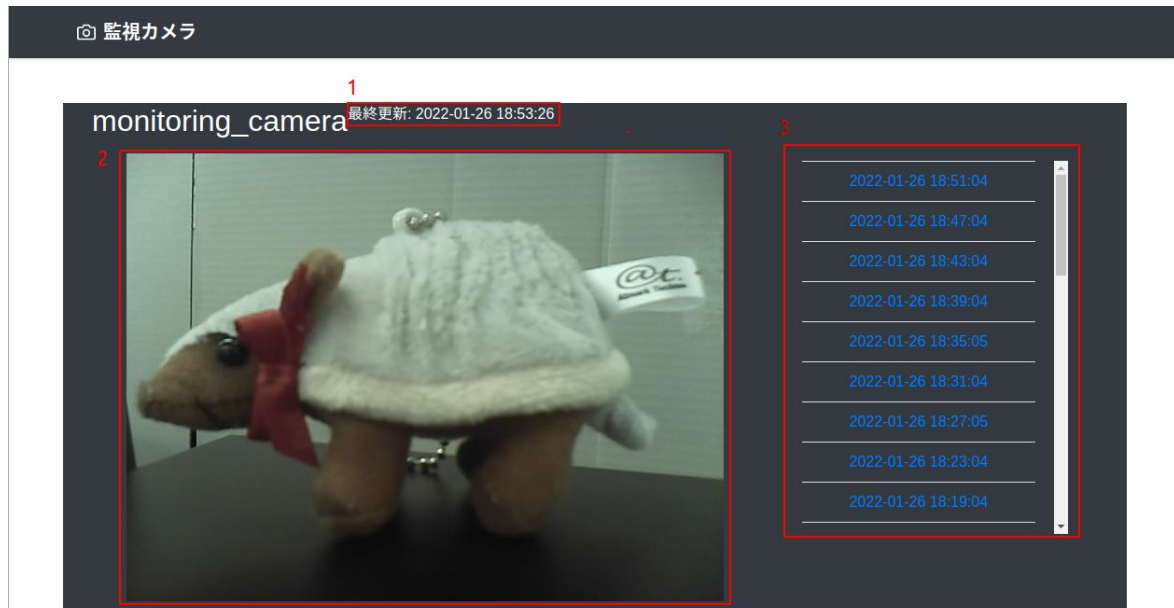


図 4.3 Armadillo Camera ページの画面説明

1. 最後に表示されるコンテンツをリロードした時刻です。
2. 現在選択されている画像が表示されます。ページ読み込み直後は S3 に保存されている最新の画像が表示されます。
3. S3 に保存されている画像のリストです。日付をクリックすると、③の領域にその画像が表示されます。

Armadillo Camera ページは、30 秒に一度自動更新します。

# 5. Appendix

---

## 5.1. 本アプリケーションの各種ファイル

本アプリケーションノートで使用したソースコード、設定ファイル等は以下のリンクよりダウンロード可能です。

各種ファイルのダウンロード [[https://download.atmark-techno.com/application-note/aiota6\\_monitoring\\_camera/](https://download.atmark-techno.com/application-note/aiota6_monitoring_camera/)]

**改訂履歴**

バージョン	年月日	改訂内容
1.0.0	2022/02/01	・ 初版発行

アプリケーションノート  
Version 1.0.0  
2022/02/08