

アプリケーションノート

Armadillo-X1 監視カメラシステム

Version 1.0.0
2021/01/22

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-X1 監視カメラシステム

株式会社アットマークテクノ

製作著作 © 2021 Atmark Techno, Inc.

Version 1.0.0
2021/01/22

目次

1. システム概要	4
1.1. システム構成図	4
1.2. Armadillo 上で動作するシステム全体のフロー	5
1.2.1. 各処理のシーケンス図	5
1.2.1.1. Setup	6
1.2.1.2. SystemOperation	6
1.3. Web サーバ上で動作するアプリケーション	7
1.4. データストア仕様	8
2. 用意するもの	9
3. システム利用手順	10
3.1. セットアップ方法	10
3.1.1. EC2 の設定	10
3.1.1.1. インスタンスの作成	10
3.1.1.2. インスタンスへの IAM ロールの追加	11
3.1.1.3. インスタンスへの接続情報の取得	16
3.1.2. S3 の設定	17
3.1.2.1. S3 バケットの作成	17
3.1.2.2. S3 バケットのライフサイクルルールの追加	18
3.1.3. IAM ユーザー作成	21
3.1.3.1. ユーザーを追加	21
3.1.3.2. アクセス許可の設定	22
3.1.3.3. タグの追加(オプション)	22
3.1.3.4. 確認画面	22
3.1.3.5. IAM ユーザー作成完了	23
3.1.4. IDS Software Suite のダウンロード	24
3.1.5. インストールディスクの作成	24
3.1.5.1. Windows の場合	24
3.1.5.2. Linux の場合	25
3.1.6. 設定ファイルの書き込み	25
3.1.6.1. 各種設定ファイルの配置	25
3.1.6.2. 初期設定ファイルの編集	26
3.1.6.3. SD カードの取り外し	28
3.1.7. ソフトウェアのインストール	28
3.2. システムの起動	28
4. 動作の確認	30
4.1. ブラウザから撮影した画像を閲覧	30
4.1.1. Armadillo Camera ページの画面説明	30
4.2. システムの状態と LED	31
5. Appendix	32
5.1. 本アプリケーションの各種ファイル	32

1. システム概要

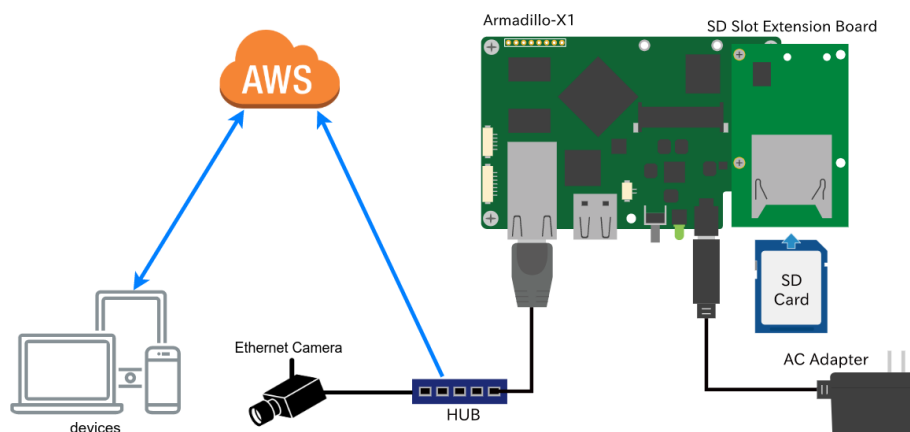
本アプリケーションノートでは、

- ・ Ethernet カメラから画像を取得すること
- ・ 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こと
- ・ 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こと
- ・ 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こと

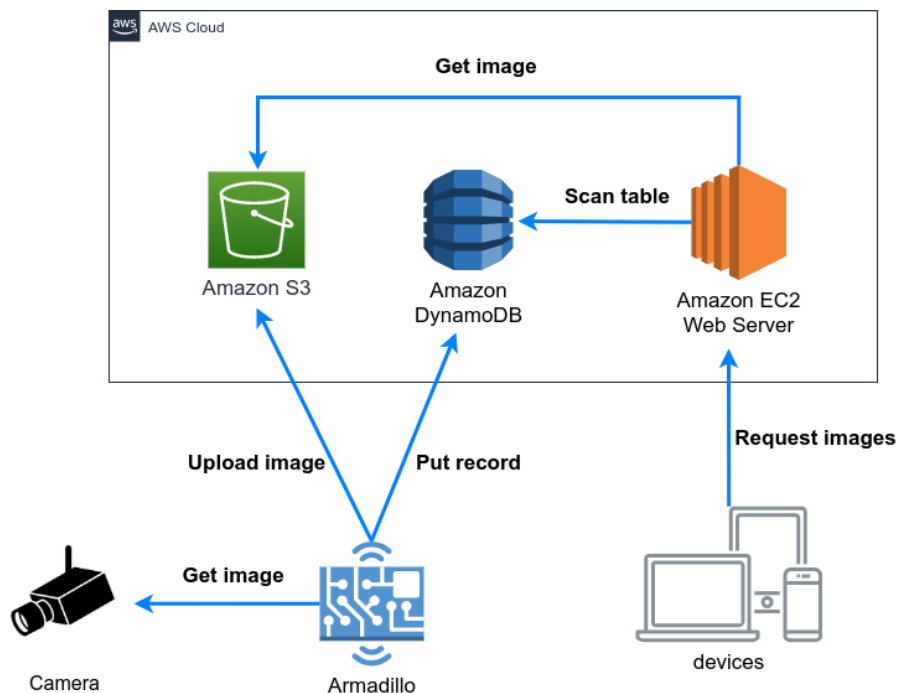
などの開発時に必要になることの多い処理を実装しているシンプルな構成のシステムの例として、Ethernet カメラから取得した画像をクラウドにアップロードして閲覧できる監視カメラシステムのサンプルアプリケーションを紹介します。

1.1. システム構成図

本システムの構成図を以下に示します。



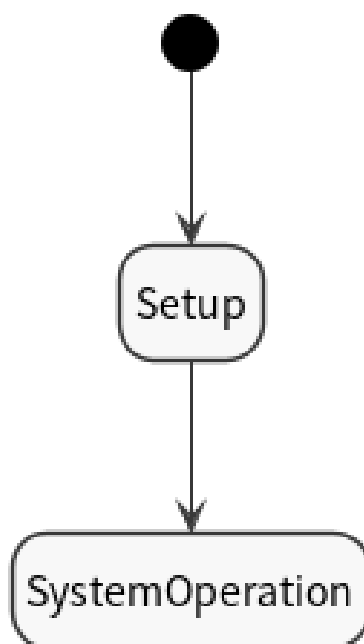
AWS 内のシステム構成図を以下に示します。



1.2. 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「1.2.1. 各処理のシーケンス図」を参照してください。

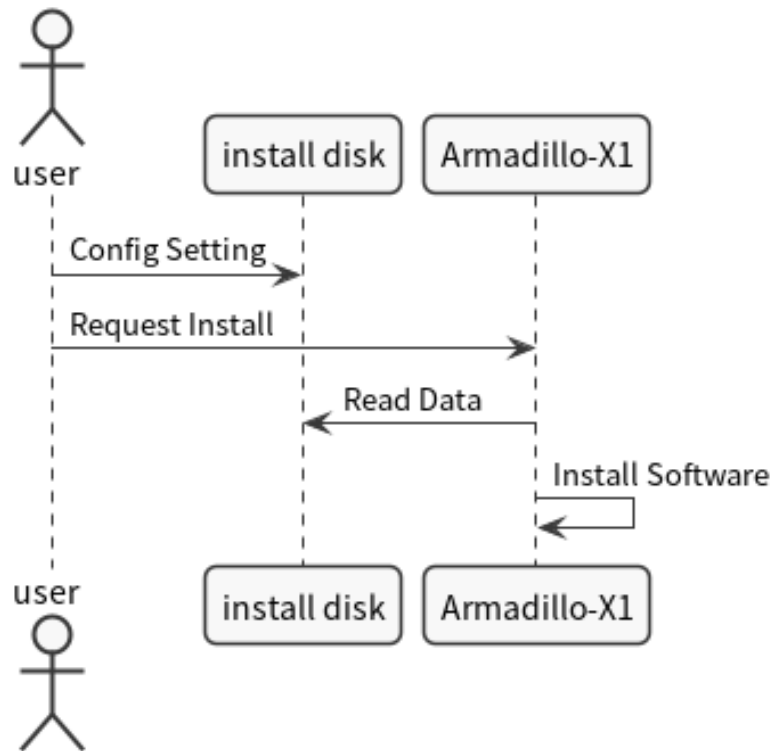


1.2.1. 各処理のシーケンス図

「1.2. 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。

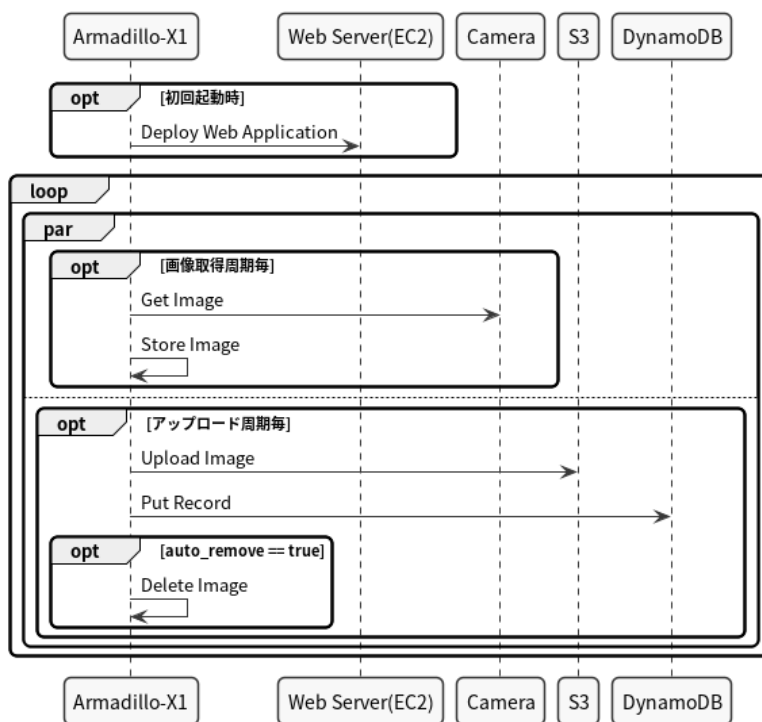
1.2.1.1. Setup

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。



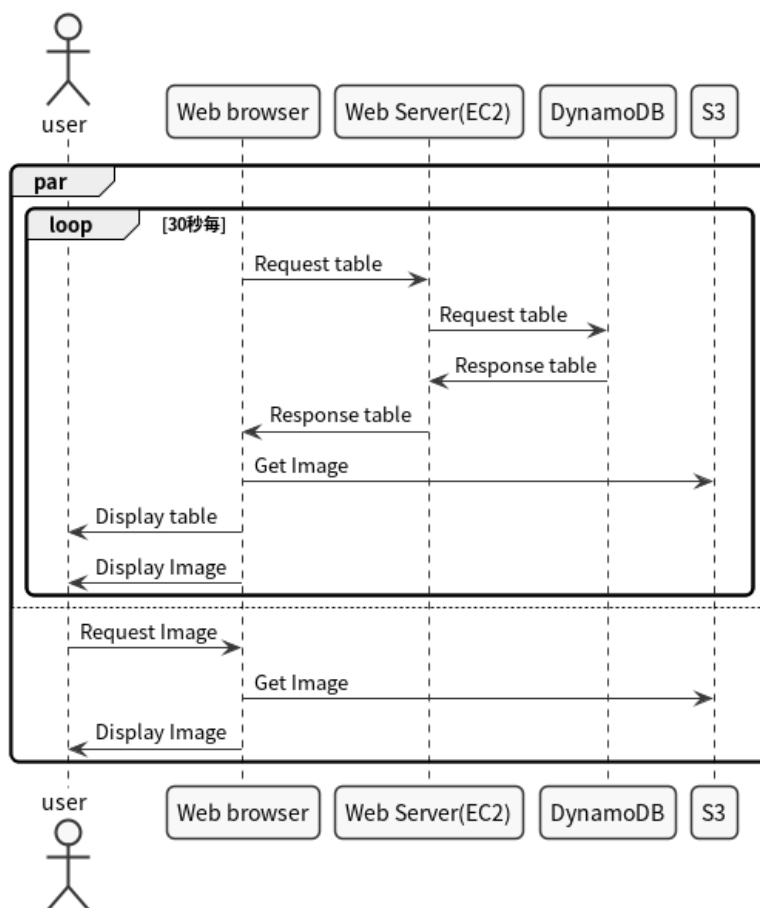
1.2.1.2. SystemOperation

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。



1.3. 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。



1.4. 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。

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]
画像取得周期	ユーザー設定	ユーザー設定	take_pic_period
S3 アップロード周期	ユーザー設定	ユーザー設定	upload_s3_period

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
 - ・ SD カードへの読み書きが可能
- ・ Armadillo-X1 [<https://armadillo.atmark-techno.com/armadillo-x1/models>]
- ・ SD スロット 拡張ボード 00 [<https://armadillo.atmark-techno.com/option-products/OP-AXA-SD00-00>]
- ・ イーサネットカメラ
 - ・ 本アプリケーションでは、 UI-5220SE [<https://jp.ids-imaging.com/store/products/cameras/ui-5220se.html>]を使用
- ・ SD カード (4GB 以上)
- ・ Ethernet ケーブル

3. システム利用手順

実際に本システムを Armadillo-X1 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。



「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。

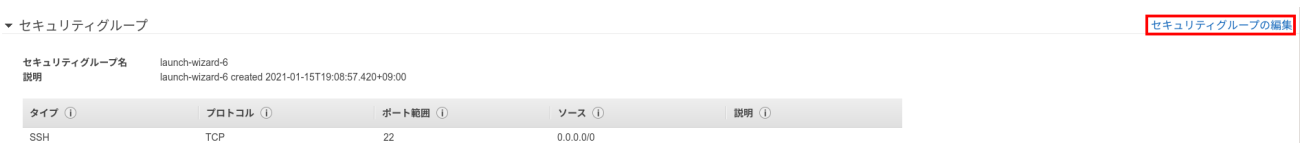


「ステップ 2: インスタンスタイプの選択」では、無料枠の「t2.micro」を選択し、「確認と作成」をクリックしてください。

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	メモリ (GiB)	インスタンスストレージ (GiB)	EBS 最適化利用	ネットワークパフォーマンス	IPv6 サポート
<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

「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。



「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。

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 ①	プロトコル ①	ポート範囲 ①	ソース ①	説明 ①
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

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、キーペア名は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「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。

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 ▼

キーペア名

monitoring_camera

キーペアのダウンロード

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。

キャンセル

インスタンスの作成

「[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。



「新しい IAM ロールを作成」をクリックしてください。



新しいタブでページが開かれるので、「ロールの作成」をクリックしてください。「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」をクリックし、画面下部に表示された「ユースケースの選択」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。

Category	Category	Category	Category	Category
Certificate Manager	Directory Service	Health Organizational View	OpsWorks	Transfer
Chime	DynamoDB	Honeycode	Personalize	Trusted Advisor
CloudFormation	EC2	IAM Access Analyzer	Purchase Orders	VPC
CloudHSM	EC2 - Fleet	Inspector	QLDB	WorkLink
CloudTrail	EC2 Auto Scaling	IoT	RAM	WorkMail
CloudWatch Alarms	EC2 Image Builder	IoT SiteWise	RDS	
CloudWatch Application Insights				

ユースケースの選択

EC2

Allows EC2 instances to call AWS services on your behalf.

EC2 - Scheduled Instances

Allows EC2 Scheduled Instances to manage instances on your behalf.

EC2 - Spot Fleet

Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

EC2 - Spot Fleet Auto Scaling

Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

EC2 - Spot Fleet Tagging

Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

EC2 - Spot Instances

Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

* 必須

キャンセル

次のステップ: アクセス権限

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

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](#)

「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

「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。

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
I-██████████

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。

EC2WebServer ▼ ①更新 新しい IAM ロールを作成

②選択

キャンセル ③保存 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。

インスタンス (1/1) 情報

検索: running x フィルターをクリア

接続 ①更新 インスタンスの状態 ▲ アクション ▼ インスタンスを起動 ▼

②再起動

インスタンスの状態 ▲
 インスタンスを停止
 インスタンスを開始
 インスタンスを再起動
 インスタンスを停止
 インスタンスを終了

選択	Name	インスタンス ID	インスタンスの状態	インスタン...	ステータスチ...	アラームの...	パブリック IPv4 DNS	パブリック I...	Elas
<input checked="" type="checkbox"/>	-	I-██████████	実行中	t2.micro	2/2 のチエ...	アラーム... +	ap-northeast-1a	ec2-██████████ ap-...	-

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。

インスタンス (1/1) 情報

検索: running x フィルターをクリア

接続 ②クリック インスタンスの状態 ▼ アクション ▼ インスタンスを起動 ▼

選択	Name	インスタンス ID	インスタンスの状態	インスタン...	ステータスチ...	アラームの...	アベイラビリティ...	パブリック IPv4 DNS	パブリック I...	Elas
<input checked="" type="checkbox"/>	-	I-██████████	実行中	t2.micro	2/2 のチエ...	アラーム... +	ap-northeast-1a	ec2-██████████ ap-...	-	-

「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 i-XXXXXXXXXX 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


インスタンス ID

 i-XXXXXXXXXX

1. SSH クライアントを開きます。
2. 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 `monitoring_camera.pem` です。
3. 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 monitoring_camera.pem`

4. 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-XXXXXXXXXX.ap-northeast-1.compute.amazonaws.com` この文字列をメモ

例:

 `ssh -i "monitoring_camera.pem" ubuntu@ec2-XXXXXXXXXX.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。

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。



「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」を選択して、「ブロックパブリックアクセスのバケット設定」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パブリックにな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。

ブロックパブリックアクセスのバケット設定

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](#)

チェックを外す

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パブリックにな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。

チェックを入れる

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パブリックになる可能性があることを承認します。

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 日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。



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。



「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」：「このルールは、バケット内のすべてのオブジェクトに適用されます」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の有効期限が切れる」
 - b. 「オブジェクトの以前のバージョンを完全に削除する」
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1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1に設定

設定後、「ルールの作成」をクリックしてください。

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

最大文字数は 255 文字です。

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
- このルールは、バケット内のすべてのオブジェクトに適用されます



このルールは、バケット内のすべてのオブジェクトに適用されます

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

- オブジェクトの現行バージョンをストレージクラス間で移行する
- ストレージクラス間でオブジェクトの以前のバージョンを移行する
- オブジェクトの現行バージョンの有効期限が切れる
- オブジェクトの以前のバージョンを完全に削除する
- 期限切れの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する
ライフサイクルルールのスコープがタグである場合、これらのアクションは利用できません。

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ingが有効なバケットの場合、Amazon S3 は削除マーカーを追加し、オブジェクトの現行バージョンは以前のバージョンとして保持されます。バージョンingされていないバケットの場合、Amazon S3 はオブジェクトを完全に削除します。 [詳細](#)

オブジェクト作成後の日数

1

オブジェクトの以前のバージョンを完全に削除する

オブジェクトが以前のバージョンになってからの日数

1

タイムラインの概要

最新バージョンのアクション

0日

アップロードされたオブジェクト



20日以前のバージョンのアクション

0日

オブジェクトが最新バージョンでなくなる



以上で S3 の設定は完了です。

3.1.3. IAM ユーザー作成

AWS マネジメントコンソールへログインし、サービス一覧から IAM を選択してください。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。

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

これらのユーザーから AWS にアクセスする方法を選択します。アクセスキーと自動生成パスワードは前のステップで提供されています。 [詳細はこちら](#)

- アクセスの種類* **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。
- 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。

* 必須

[キャンセル](#)

[次のステップ: アクセス権限](#)

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

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](#)

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](#)

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-X1 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



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
▶	✓ monitoring_c...	[redacted]	***** 表示	***** 表示	Eメールの送信

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. IDS Software Suite のダウンロード

本アプリケーションノートで使用するカメラのドライバを含むソフトウェアのダウンロードを行います。ダウンロードページ [<https://jp.ids-imaging.com/downloads.html>]から、対応するソフトウェアをダウンロードしてください。今回ダウンロードするソフトウェアは、ダウンロードするためにサイトへの登録が必要となっていますので、登録後にダウンロードを行ってください。

例として本アプリケーションノートで使用する UI-5220SE のダウンロードページは [こちら](https://jp.ids-imaging.com/download-details/AB.0010.1.36702.24.html?os=linux_arm&version=v7&bus=32&floatcalc=hard) [https://jp.ids-imaging.com/download-details/AB.0010.1.36702.24.html?os=linux_arm&version=v7&bus=32&floatcalc=hard] です。ダウンロードページから、「ids-software-suite-linux-armhf-[VERSION].tgz」をダウンロードしてください。

3.1.5. 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。SD カードを PC に接続してください。PC の OS 毎に書き込み方法が異なりますので、該当の項目を参考に書き込んでください。

3.1.5.1. Windows の場合

Armadillo-IoT(G3/G3L)/X1: Windows 上でのインストールディスクの作成方法 [<https://armadillo.atmark-techno.com/blog/1913/2400>]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。

3.1.5.2. Linux の場合

Armadillo-X1 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-x1/armadillo-x1_product_manual_ja-3.0.0/ch11.html#sct.install_base_software.with_install_disk.create_disk]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。

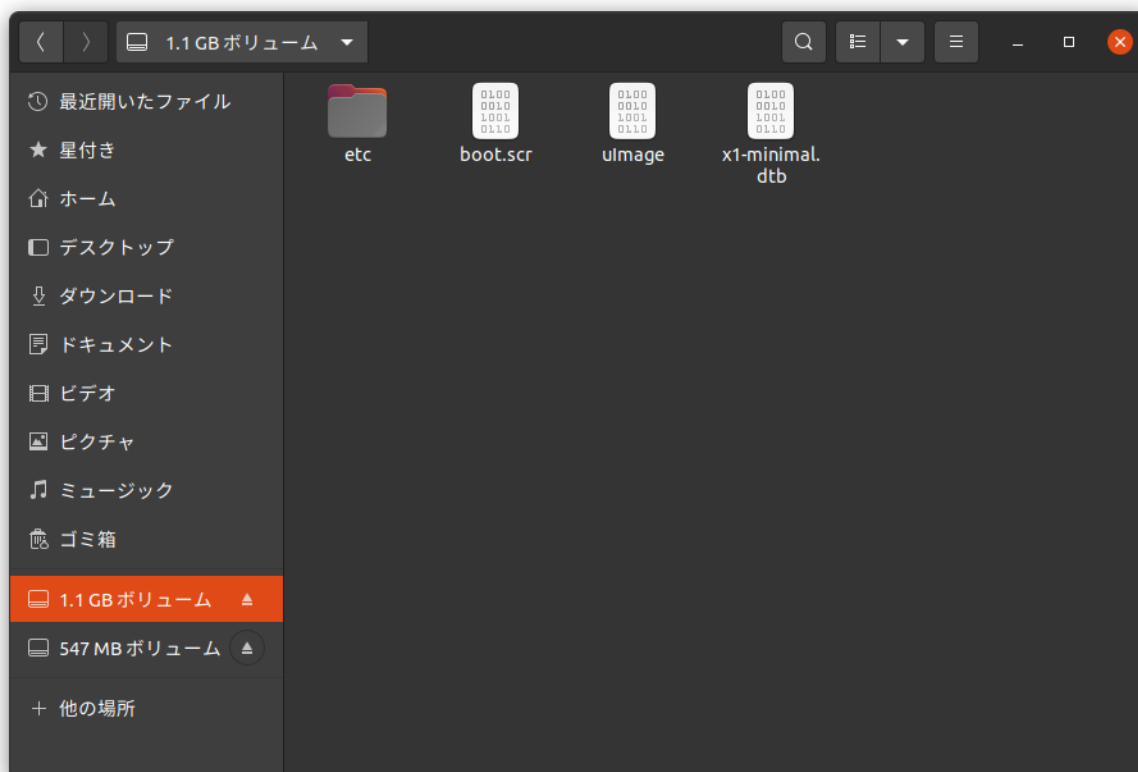
3.1.6. 設定ファイルの書き込み

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。

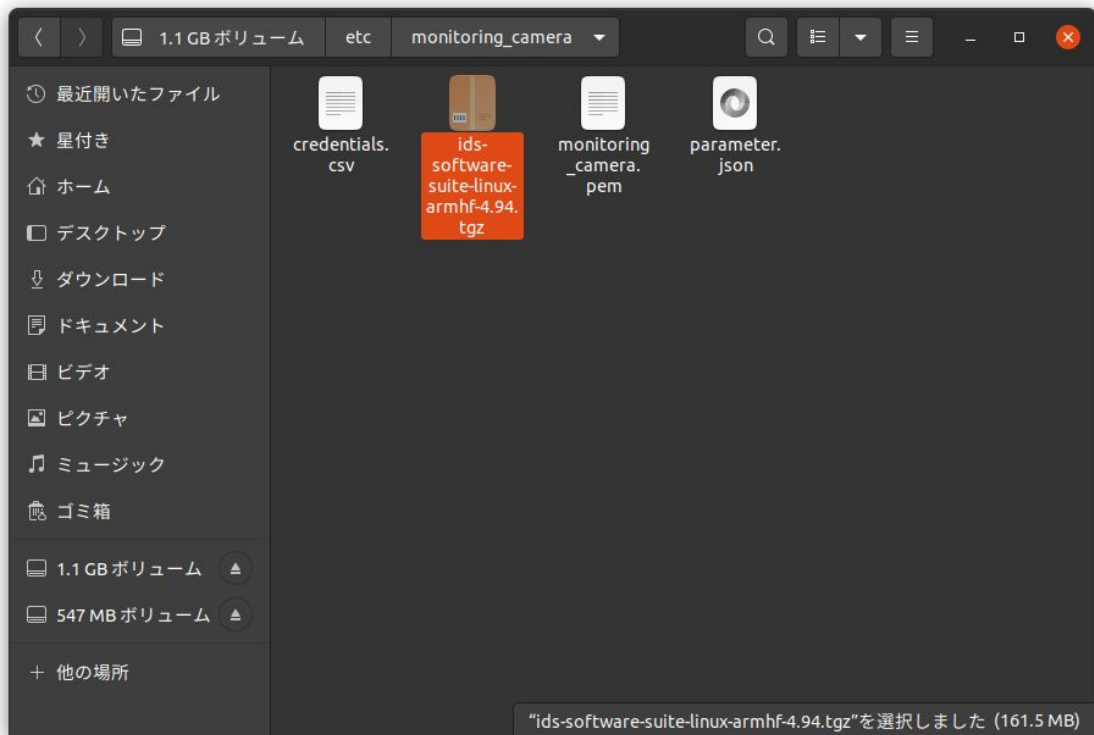
3.1.6.1. 各種設定ファイルの配置

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「1.1GB ボリューム」をクリック



3. 下記のファイルを `etc/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`
 - c. 「3.1.4. IDS Software Suite のダウンロード」でダウンロードした `ids-software-suite-linux-armhf-[VERSION].tgz`



3.1.6.2. 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「1.1GB ボリューム」をクリック
2. `etc/monitoring_camera/parameter.json` をテキストエディタで開きます

```
1 {
2   "take_pic_period": 30,
3   "upload_period": 60,
4   "s3_bucket_name": "",
5   "save_path": "",
6   "auto_remove": "true",
7   "ec2_public_dns": "",
8   "ec2_user_name": "ubuntu"
9 }
```

JSON ▾ タブ幅: 8 ▾ (8行、30列) ▾ [挿入]

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)

項目	説明	初期値(単位)
<code>take_pic_period</code>	Armadillo がカメラから画像を取得する周期です。	30(秒)
<code>upload_period</code>	Armadillo が AWS に画像を含むデータをアップロードする周期です。	60(秒)
<code>s3_bucket_name</code>	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
<code>save_path</code>	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 <code>/dev/sda1</code> を、SD カードに保存する際は <code>/dev/mmcblk0p1</code> を指定してください。何も指定しない場合は <code>/opt/monitoring_camera/pictures</code> に保存されます。	なし
<code>auto_remove</code>	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。 <code>true</code> 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、 <code>save_path</code> 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 <code>true</code> になります。	<code>true</code>
<code>ec2_public_dns</code>	「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
<code>ec2_user_name</code>	「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 <code>ubuntu</code> のままで問題ありません。	<code>ubuntu</code>

4. 以下は編集例です

```

1 {
2   "take_pic_period": 30,
3   "upload_period": 60,
4   "s3_bucket_name": "s3bucket",
5   "save_path": "",
6   "auto_remove": "true",
7   "ec2_public_dns": "ec2-255-255-255-255.ap-northeast-1.compute.amazonaws.com",
8   "ec2_user_name": "ubuntu"
9 }

```

JSON ▼ タブ幅: 8 ▼ (8行、30列) ▼ [挿入]

3.1.6.3. 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。

3.1.7. ソフトウェアのインストール

SD スロット拡張ボード上のスライドスイッチを「SD BOOT」に設定し、Armadillo-X1 に取り付けてください。作成したインストールディスクを SD スロット拡張ボードに挿入し、Armadillo-X1 上のユーザスイッチを押しながら電源を投入してください。

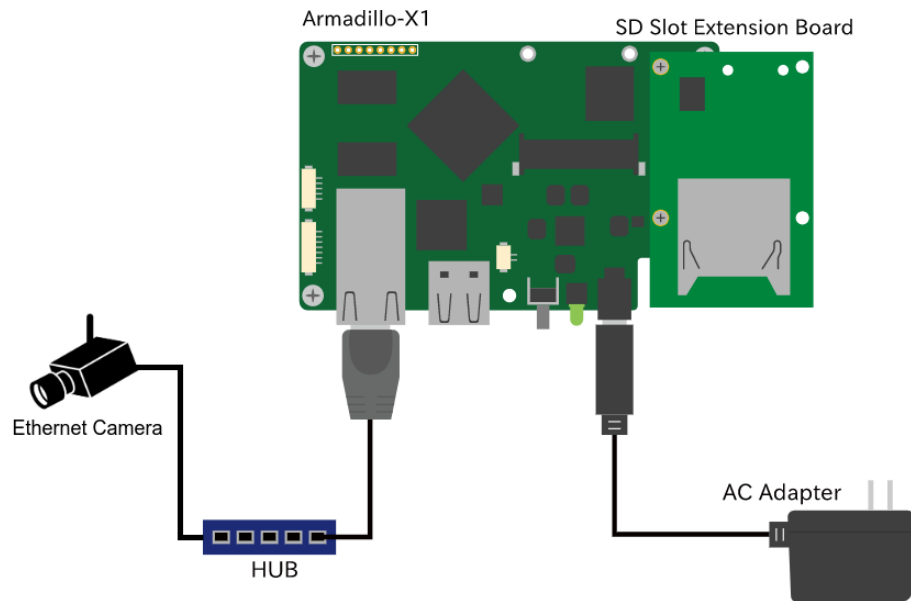
Armadillo-X1 へのソフトウェアのインストールが開始されます。インストールには数分間かかります。インストールの進捗は、Armadillo-X1 の緑色 LED の状態で確認することが出来ます。インストールの進捗と LED の状態の関係は以下の表の通りです。

進捗	ユーザー LED 緑
実行中	点滅
正常終了	点灯
異常終了	消灯

緑色 LED が点滅から点灯に変わり、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。LAN インターフェース(CON1)に Ethernet ケーブルを接続し、同一 LAN 内に Ethernet カメラを接続してください。その後、Armadillo-X1 に電源を投入してください。



電源投入後、初回起動時は Ethernet カメラのドライバのインストールのため、一度自動的に再起動します。再起動時に Linux の起動が完了するまで 30 秒ほどかかります。その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。これは初回起動時は 5~10 分程度、2 回目以降は 30 秒程度で完了します。

AWS のセットアップ完了後に、「3.1.6.2. 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を取得し、AWS へアップロードを始めます。

4. 動作の確認

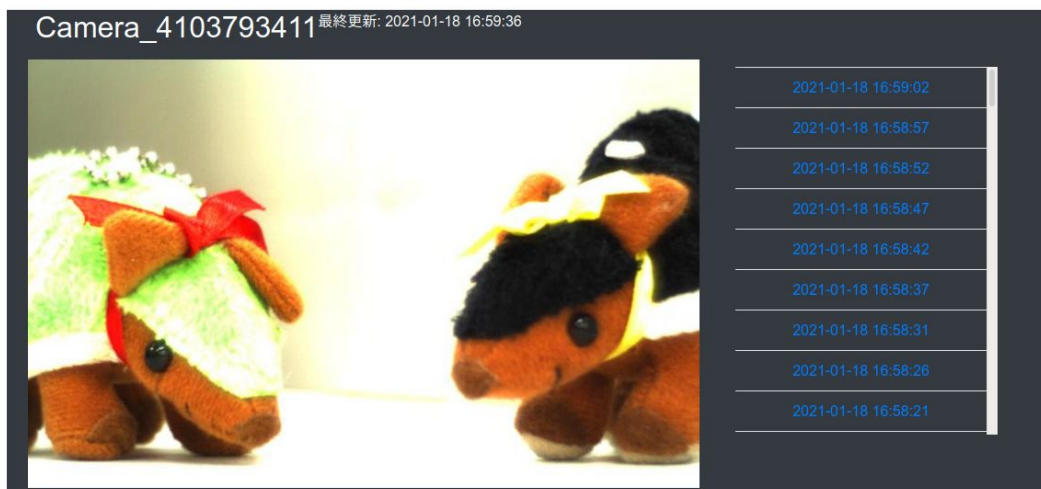
4.1. ブラウザから撮影した画像を閲覧

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。



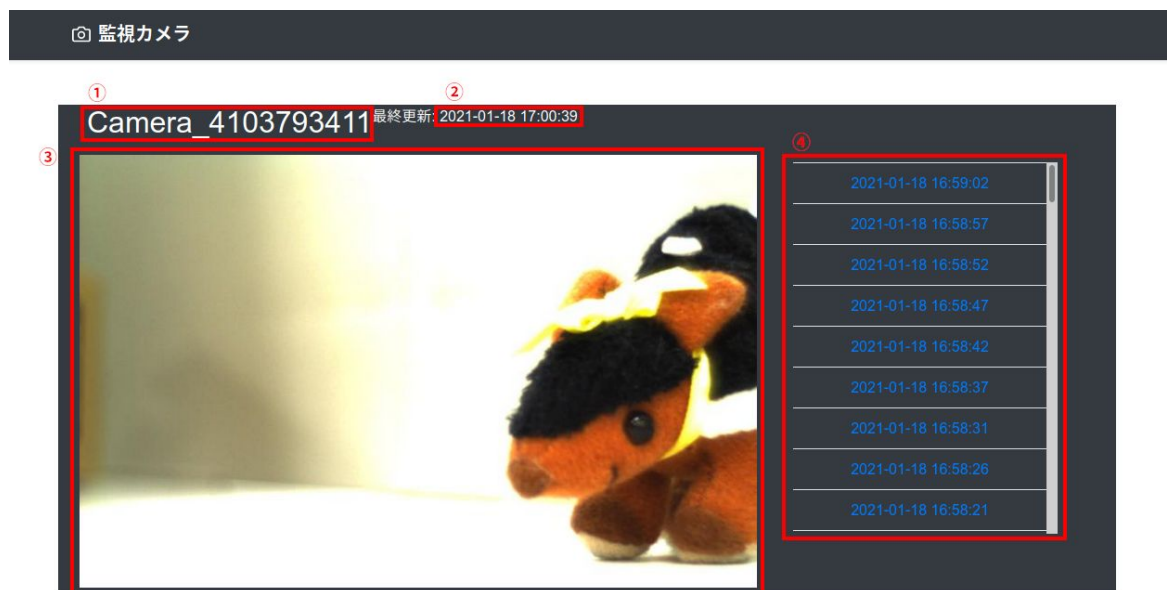
サンプルアプリケーションでは https アクセスに対応していないため、URL の「https」を「http」に書き換えてアクセスしてください。

📷 監視カメラ



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。



1. カメラの名前です。
2. 最後に表示されるコンテンツをリロードした時刻です。
3. 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。
4. 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。

4.2. システムの状態と LED

本アプリケーションはシステム内で何らかのエラーが起こった場合、LED でそれを知らせます。起こったエラーと LED の状態の関係は以下の表の通りです。

システムの状態	ユーザー LED 緑
正常動作中	点灯
カメラ関連の不具合	2 回の短点灯
クラウドとの通信失敗	点滅

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/monitoring_camera/]

改訂履歴

バージョン	年月日	改訂内容
1.0.0	2021/01/22	・ 初版発行

アプリケーションノート
Version 1.0.0
2021/01/22