JCCH・セキュリティ・ソリューション・システムズ

プライベートCA Gléas ホワイトペーパー

AWS ALB でのクライアント証明書認証

Ver.1.0

2026 年 1 月

目次

1. はじめに

1.1. 本書について

本書では、弊社製品プライベートCA Gléasで発行したクライアント証明書を利用して、Amazon Web Service (AWS)が提供するロードバランサーALB (Application Load Balancer)でクライアント証明書認証をおこなう環境を構築するための設定例を記載します。

本書に記載の内容は、弊社の検証環境における動作を確認したものであり、あらゆる環境での動作を保証するものではありません。弊社製品を用いたシステム構築の一例としてご活用いただけますようお願いいたします。

弊社では試験用のクライアント証明書の提供も行っております。検証等で必要な場合は、最終項のお問い合わせ先までお気軽にご連絡ください。

1.2. 本書における環境

本書は、以下の環境で検証をおこなっております。

- **ロードバランサー**
  AWS ALB (Application Load Balancer)
  ※以後、「ALB」と記載します

- **DNS**
  Amazon Route53
  ※以後、「Route53」と記載します

- **オブジェクトストレージ**
  Amazon Simple Storage Service (Amazon S3)
  ※以後、「S3」と記載します

- **証明書マネージドサービス**
  AWS Certificate Manager（ACM)
  ※以後、「ACM」と記載します

- **AWS コマンドラインインターフェイス**
  AWS Command Line Interface（AWS CLI)
  ※以後、「AWS CLI」と記載します

- **認証局：JS3 プライベートCA Gléas（バージョン2.8.0)**
  ※以後、「Gléas」と記載します

- **アプリケーションサーバ：AlmaLinux 9.5 / Node.js 16.20.2**
  ※以後、「サーバ」と記載します

- **クライアント：Windows11 Pro 25H2 / Microsoft Edge 143.0.3650.96**
  ※以後、「Windows」と記載します

- **クライアント：iPhone14（iOS 26.0）/ Safari**
  ※以後、「iPhone」と記載します

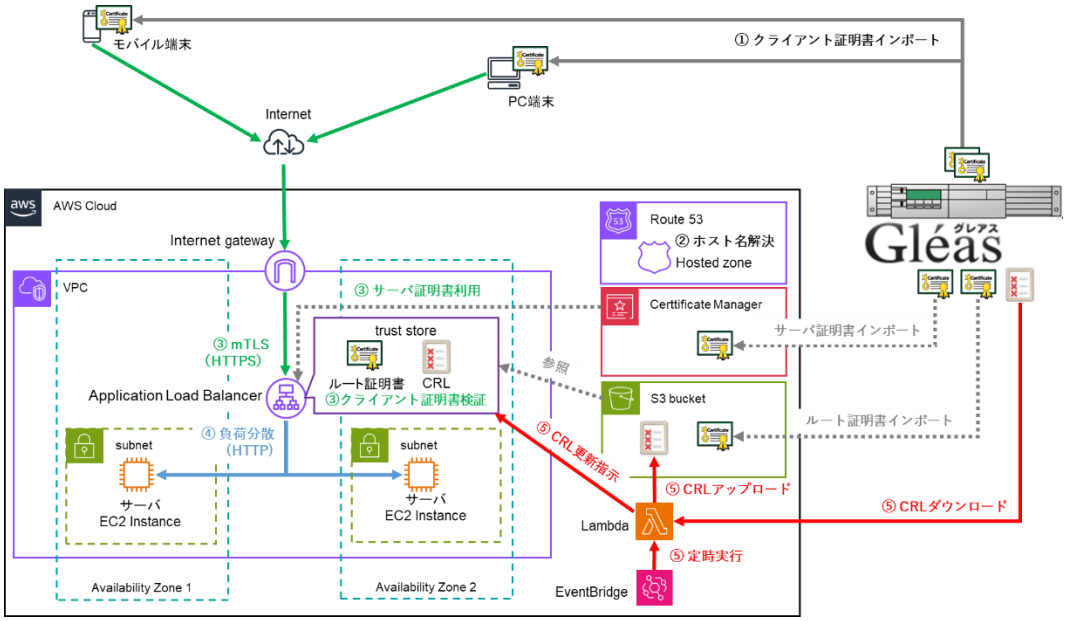
以下については、本書では説明を割愛します。

- **AWSマネジメントコンソールの基本操作**
- **Route53の基本設定（初期設定やホストゾーンに関する設定)**
- **S3の基本設定（オブジェクトやアクセス権限に関する設定)**
- **ACMの基本設定（初期設定や基本操作)**
- **AWS CLIの基本設定（インストールや初期設定)**
- **サーバの基本設定（インストールや初期設定)**
- **Gléasでのアカウント登録やクライアント証明書発行などの基本操作**
- **クライアント端末におけるネットワーク設定など**

これらについては、各製品のマニュアルをご参照いただくか、各製品を取り扱っている販売店にお問い合わせください。

1.3. 本書における構成

本書では、以下の構成で検証を行っています。



準備

- **Gléasのルート証明書、CRLをS3バケットにインポートして、トラストストアを作成**
- **Gléasから発行したサーバ証明書をACMにインポート**
- **Gléasからクライアント証明書を発行**

1. **PC端末とモバイル端末(iPhone)は、Gléasよりクライアント証明書をインポート。**
2. **ALBのFQDNをRoute53 (DNS)で名前解決。**
3. **PCではEdgeブラウザ、iPhoneではSafariブラウザよりALBにアクセス。**
   ALBはクライアント証明書認証をおこなう。
   証明書を提示しない、または提示した証明書が期限切れ、失効している場合、クライアント証明書認証に失敗。
4. **ALBは証明書認証後にサーバにロードバランスしてWebページをクライアントに表示。**
5. **AWS EventBridgeのイベントからAWS Lambda関数を定期的に実行することで、失効リストを自動更新。**

1.4. 留意事項

1.4.1. サーバ証明書の発行について

本書2.2の方法で、Gléasからサーバ証明書を発行する場合、事前にサーバアカウントを作成しておき、[SSLサーバ証明書]ロールグループに参加させる必要があります。

1.4.2. 失効リストの登録について

本書2.5の方法で、Gléasで発行された失効リストをトラストストアに登録する際、事前に作業端末にcurlコマンド、およびAWS CLIをインストールする必要があります。

2. AWS の設定

2.1. ルート証明書をS3に登録

クライアント証明書認証を利用するためには、AWSにルート証明書の登録が必要です。

ルート証明書は、クライアントから提示される証明書が正しいことを検証するために利用されます。

ルート証明書をS3に登録し、ALBが利用できるようにします。

Gléasからルート証明書をダウンロードします。

※GléasのデフォルトCAのルート証明書（PEM形式）のダウンロードURLは以下となります
http://[GléasのFQDN]/crl/ia1.pem

S3 コンソールでルート証明書を登録するバケットを作成し、バケット情報を開きます。

[アップロード] をクリックし、次の画面で以下を設定します。

アップロード

- **ルート証明書をドラッグアンドドロップ**

[アップロード] をクリックすると、ルート証明書が登録されます。

登録後、ルート証明書のS3 URIをメモしておきます。

2.2. サーバ証明書をACMに登録

ALBがTLS通信を行うためにはサーバ証明書が必要です。

サーバ証明書は、ALBが正しいサーバであることをクライアントに提示するために利用されます。

Gléasで発行したサーバ証明書をACMに登録することでALBが利用できるようにします。

Gléas（RA）にログインし、該当のサーバアカウントのページへ移動します。

- サーバ属性の [編集] をクリックし、ホスト名に ALB の FQDN を入力
- 小メニューの [証明書発行] をクリック

- **[発行]ボタンをクリックし、証明書を発行**

証明書発行完了後、[ダウンロード] リンクをクリックし、発行された証明書をダウンロードします。

ダウンロードしたサーバ証明書(.p12)から PEM 形式の証明書、秘密鍵、ルート証明書を取り出します。

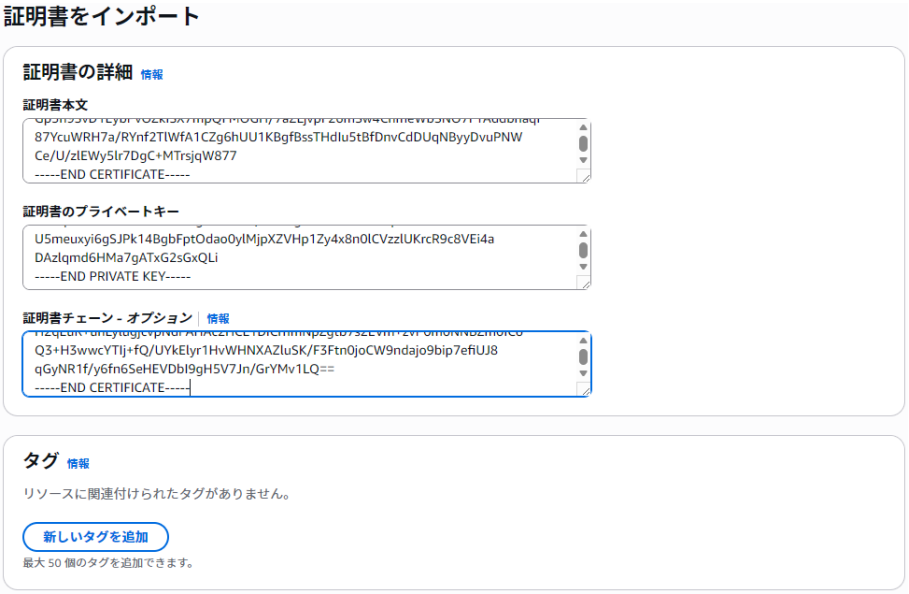
※証明書、秘密鍵、ルート証明書の取り出しはOpenSSL等のツールで行うことができます。

ACM コンソールの［証明書をインポート］メニューを開きます。

次の画面で以下を設定します。

証明書をインポート

- **証明書本文にサーバ証明書の内容（PEM 形式）を入力**
- **証明書のプライベートキーにサーバ証明書の秘密鍵（PEM 形式）を入力**
- **証明書チェーンにサーバ証明書の発行元ルート証明書（PEM 形式）を入力**



[証明書をインポート] をクリックすると、ACMにサーバ証明書が登録されます。

2.3. ターゲットグループの作成

トラフィックを分散するターゲットをグループ化します。

本書ではEC2インスタンスをターゲットとします。

EC2 コンソールの［ターゲットグループ］メニューから［ターゲットグループの作成］

をクリックします。

次の画面で以下を設定します。

設定

- **ターゲットの種類に［インスタンス］を選択**
- **ターゲットグループ名に任意の名称を入力**
- **プロトコルに［HTTP]、ポートにポート番号を指定**
- **IP アドレスタイプに［IPv4］を選択**
- **VPC にターゲットとなる EC2 インスタンスが配置されている VPC を選択**
- **プロトコルバージョンに［HTTP1］を選択**

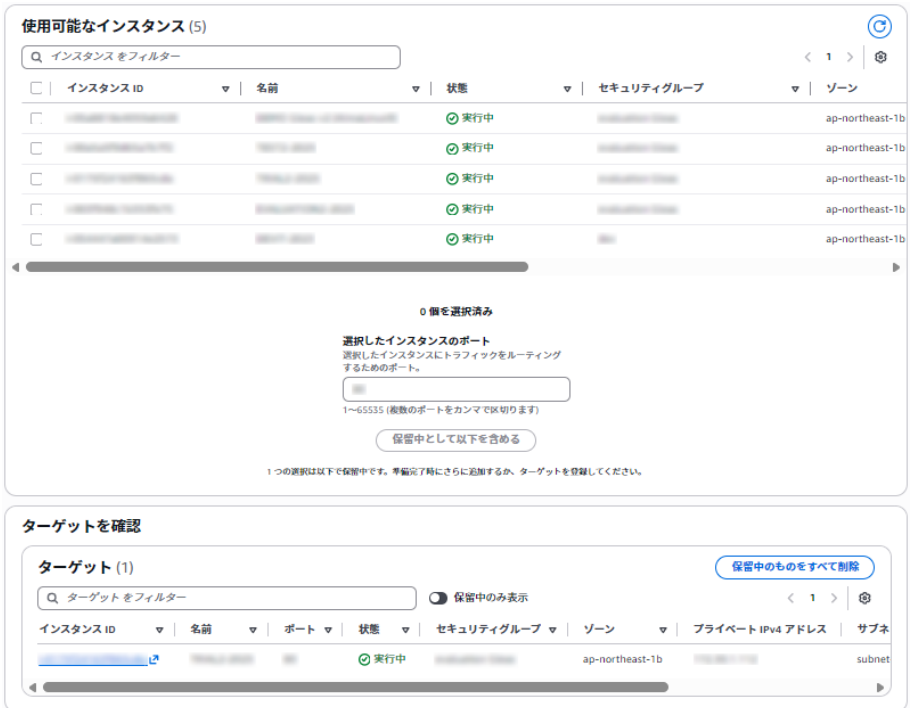
ヘルスチェック

- **ヘルスチェックプロトコルに [HTTP] を選択**
- **ヘルスチェックパスに [/] を入力**

入力後、[次へ] をクリック

使用可能なインスタンス

- **使用可能なインスタンスの一覧からターゲット EC2 インスタンスをチェック**
- **[保留中として以下を含める] をクリック**
- **ターゲットとなるインスタンス、ポートが指定されたことを確認**
  ※ターゲットの数は 1 つでも指定可能です

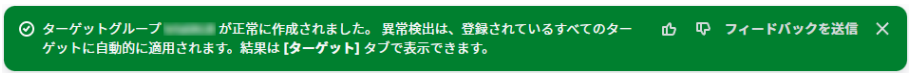


入力後、[次へ] をクリック

作成と確認

- **入力内容が正しいことを確認**

[ターゲットグループの作成] をクリックすると、ターゲットグループが作成されます。



2.4. トラストストアの作成

ALBがクライアント証明書認証を行う際に使用するルート証明書、失効リスト（CRL）を格納するトラストストアを作成します。

EC2 コンソールの［トラストストア］メニューから［トラストストアを作成］をクリックします。

次の画面で以下を設定します。

トラストストアの設定

- トラストストアの名前に任意の名称を入力
- 認証局バンドルに本書 2.1 で登録したルート証明書を S3 URI 形式で指定

※S3 URIは以下の形式

S3://[S3バケット名]/[ディレクトリ]/[ファイル]

※失効リストの登録は以降の操作行うため、ここでは省略します。

入力後、［トラストストアを作成］をクリックすると、トラストストアが作成されます。

作成後、トラストストアのARNをメモしておきます。

2.5. 失効リスト（CRL）の登録

クライアント証明書認証を利用するためには、失効リストの登録が必要です。

失効リストは、クライアントから提示される証明書が失効されていないことを検証するために利用されます。

トラストストアに失効リストを登録します。

本書では AWS CLI を使用してコマンドライン操作で失効リストの登録を行います。

2.5.1. IAM ポリシーを作成

AWS CLIを使ってコマンドライン操作を行うためにIAMに利用サービスを操作するため

に必要なポリシーを作成します。

IAM コンソールの [ポリシー] メニューから [ポリシーの作成] をクリックします。

次の画面で以下を設定します。

アクセス許可を指定

- **ポリシーエディタに [JSON] を指定**

※JSON形式でポリシーを入力

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3access",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::【S3 バケット】/【ディレクトリ】/*"
      ]
    },
    {
      "Sid": "TrustStoreaccess",
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:AddTrustStoreRevocations",
        "elasticloadbalancing:RemoveTrustStoreRevocations"
      ],
      "Resource": [
        "【トラストストア ARN】"
      ]
```

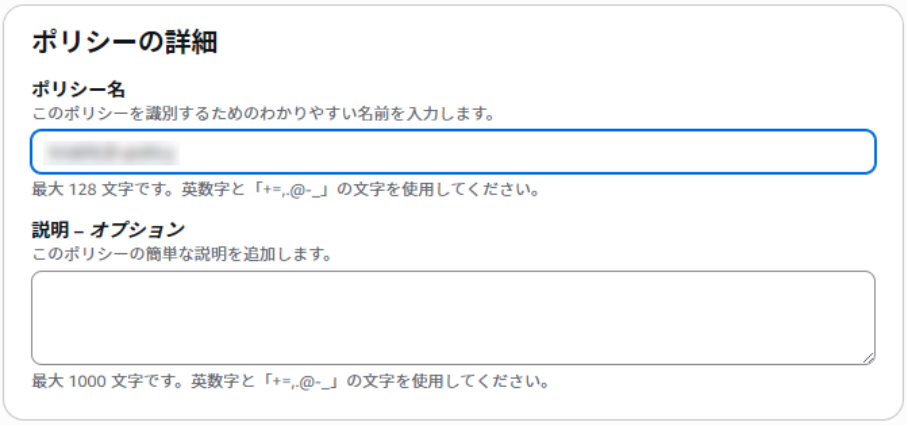
※許可ポリシーの詳細

アクション	リソース	ポリシー
s3:PutObject	S3 バケット	ファイルアップロードを許可
s3:GetObject	S3 バケット	ファイルダウンロードを許可
elasticloadbalancing:AddTrustStoreRevocations	トラストストア	失効リスト追加を許可
elasticloadbalancing:RemoveTrustStoreRevocations	トラストストア	失効リスト削除を許可

入力後、[次へ] をクリック

ポリシーの詳細

- **ポリシー名に任意の名称を指定**



入力後、[ポリシーの作成] をクリックすると、IAMポリシーが作成されます。

2.5.2. IAM ユーザーを作成

作成したIAMポリシーをアタッチしたIAMユーザーを作成します。

IAM コンソールの［ユーザー］メニューから［ユーザーの作成］をクリックします。

次の画面で以下を設定します。

ユーザーの詳細

- **ユーザー名に任意の名称を指定**

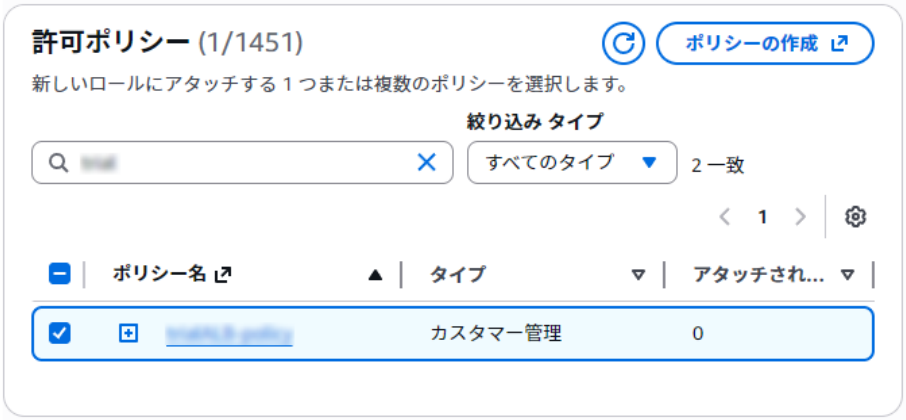
入力後、[次へ] をクリック

許可のオプション

- **[ポリシーを直接アタッチする] を選択**

許可ポリシー

- **本書2.5.1で作成したIAMポリシーを選択**

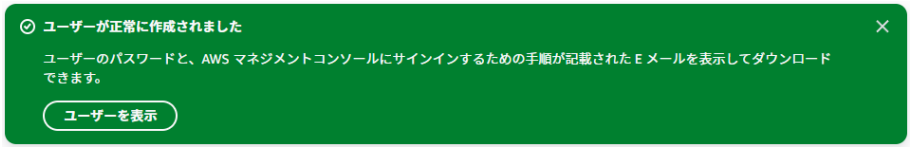


入力後、[次へ] をクリック

確認して作成

- **許可の概要に本書2.5.1で作成したIAMポリシーが指定されていることを確認**

[ユーザーの作成] をクリックすると、IAMユーザーが作成されます。



2.5.3. アクセスキーを作成

作成したIAMユーザでAWS CLIを利用できるようにアクセスキーを作成します。

作成したアクセスキー、シークレットアクセスキーは、AWS CLIのクレデンシャル情報として使用します。

IAM コンソールの [ユーザー] メニューから作成した IAM ユーザを選択します。

次の画面で以下を設定します。

IAMユーザー情報

- [セキュリティ認証情報] タブを選択
- [アクセスキーを作成] をクリック

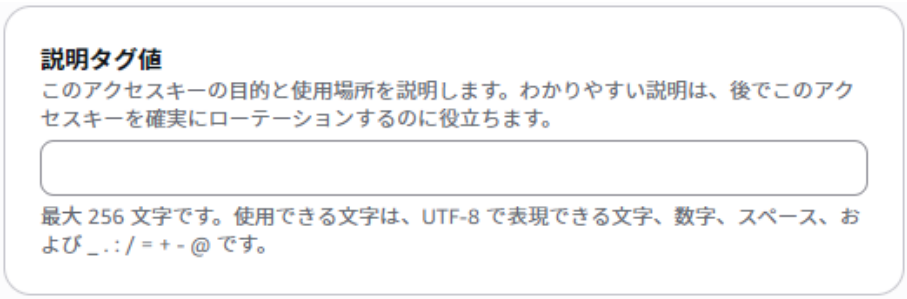
主要なベストプラクティスと代替案にアクセスする

- **ユースケースに[コマンドラインインターフェイス (CLI)]を選択**
- **[・・・を理解し、アクセスキーを作成します。] をチェック**

[次へ] をクリック

説明タグを設定 – オプション

- **必要に応じて任意の説明タグ値を入力**



[アクセスキーを作成] をクリックすると、アクセスキーが作成されます。

表示された [アクセスキー] および [シークレットアクセスキー] は大切に保管します。

[完了] クリック以降、シークレットアクセスキーは表示されなくなります。

2.5.4. 最新の失効リストをダウンロード

Gléasが発行した最新の失効リストをダウンロードします。

- curl コマンドを用いて以下のコマンドを実行

```
curl http://【CRL ファイルの URL】 -o 【CRL ファイル名】
```

※Gléas のデフォルトCAの失効リスト (PEM形式) のダウンロードURLは以下
http://[GléasのFQDN]/crl/ia1_crl.pem

2.5.5. S3 バケットに失効リストをアップロード

トラストストアはS3に登録された失効リストを参照するため、ダウンロードした失効リストをS3にアップロードします。

- AWS CLI を用いて以下のコマンドを実行

```
aws s3 cp ¥
  ${CRL_FILE} ¥
  【S3 URI】 ¥
  --region 【AWS リージョン】
```

※S3 URIの形式
s3://[S3バケット]/[ディレクトリ]/[ファイル]

※AWSリージョンの形式
ap-northeast-1　　(アジアパシフィック (東京) リージョン)

2.5.6. トラストストアに失効リストを追加

S3にある失効リストをトラストストアに追加して、最新の失効リストを反映します。

- **AWS CLIを用いて以下のコマンドを実行**

```
aws elbv2 add-trust-store-revocations ¥
  --trust-store-arn 【トラストストア ARN】 ¥
  --revocation-contents S3Bucket=【S3 バケット】,S3Key=【ディレクトリ】/【ファイル】,RevocationType=CRL ¥
  --region 【AWS リージョン】
```

※トラストストアARNの形式

arn:aws:elasticloadbalancing:[AWSリージョン]:[アカウントID]:truststore/[トラストストア名]/XXXXXXXXXX

※AWSリージョンの形式

ap-northeast-1　　(アジアパシフィック (東京) リージョン)

トラストストアに登録された失効リスト情報が出力される

```
{
  "TrustStoreRevocations": [
    {
      "TrustStoreArn":"【トラストストア ARN】",
      "RevocationId": 1,
      "RevocationType": "CRL",
      "NumberOfRevokedEntries": 10
    }
  ]
}
```

※失効リストはトラストストアに追加される

※RevocationId は登録された失効リストの識別子。登録毎に1増加してゆく

※NumberOfRevokedEntriesは失効リストに記録された失効済み証明書数。

2.5.7. トラストストアから古い失効リストを削除

トラストストアに失効リストが追加されたら、以前の古い失効リストは不要となるため削除します。

- **AWS CLI を用いて以下のコマンドを実行**

```
aws elbv2 remove-trust-store-revocations ¥
   --trust-store-arn 【トラストストア ARN】 ¥
   --revocation-ids 【削除する RevocationId】 ¥
   --region 【AWS リージョン】
```

※トラストストアARNの形式

arn:aws:elasticloadbalancing:[AWSリージョン]:[アカウントID]:truststore/[トラストストア名]/XXXXXXXXXX

※--revocation-idオプションに削除したい失効リストのRevocationIdを指定

※AWSリージョンの形式

ap-northeast-1　　(アジアパシフィック (東京) リージョン)

2.6. ロードバランサー(ALB)の作成

ALBを作成します。

EC2 コンソールの［ロードバランサー］メニューから［ロードバランサーの作成］>

[Application Load Balancer を作成］をクリックします。

次の画面で以下を設定します。

基本的な設定

- **ロードバランサーに任意の名称を入力**
- **スキームに［インターネット向け］を選択**
- **ロードバランサーの IP アドレスタイプに［IPv4］を選択**

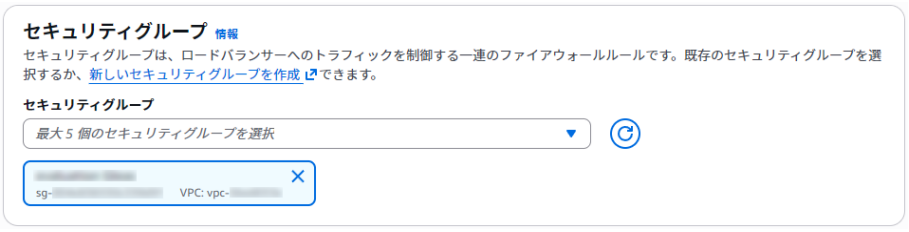
ネットワークマッピング

- **VPC に ALB を配置先となる VPC を選択**
- **アベイラビリティーゾーンとサブネットにターゲットが所属するアベイラビリティーゾーンをチェックし、サブネットを選択**

※サブネットは少なくとも 2 つ指定する必要があります。

セキュリティグループ

- **セキュリティグループに ALB に適用するファイアウォールルールを選択**



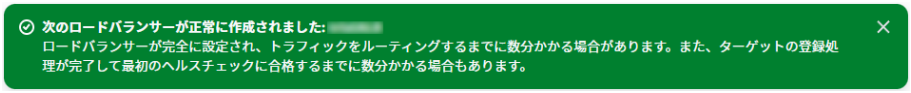
リスナーとルーティング

- **リスナーのプロトコルに [HTTPS]、ポートに [443] を指定**
- **事前ルーティングアクションは [なし] を選択**
- **アクションのルーティングに [ターゲットグループへ転送] を選択**
- **ターゲットグループに本書 2.3 で作成したターゲットグループを選択**

セキュアリスナーの設定

- **セキュリティカテゴリに [すべてのセキュリティポリシー] を選択**
- **ポリシー名に [推奨] のポリシーを選択**
- **証明書の取得先 に [ACM から] を選択**
- **証明書 (ACM から) に本書 2.2 で ACM に登録した証明書を選択**
- **相互認証 (mTLS)をチェックし、[トラストストアで検証] を選択**
- **クライアント証明書の処理に[期限切れのクライアント証明書を許可しない] を選択**
- **トラストストアの CA サブジェクト名をアドバタイズに [オン] を選択**

入力後、[ロードバランサーの作成] をクリックすると、ALB が作成されます。



2.7. 失効リスト（CRL）の自動更新について

失効リストには有効期限があり、Gléasは定期的に失効リストを発行しています。

ALBが利用するトラストストアは、最新の失効リストを参照する必要があります。

本書2.5.4～2.5.7の操作を定期的に行うことで、トラストストアを自動更新することができます。

crontab、タスクスケジューラ、AWS Event Bridgeなどのスケジューラを利用して、定期的な自動更新を行います。

本書ではAWS Lambda関数を実装し、AWS Event Bridgeから定期的に実行する方法で検証を行いました。

※シェルスクリプトやLambda関数の詳細につきましては、弊社までお問い合わせください。

2.8. DNS登録

FQDNでALBを参照できるようにDNS登録します。

Route53のホストゾーンにAレコード（エイリアス）を登録し、ALBを名前解決できるようにします。

Route53 コンソールの［ホストゾーン］メニューから対象となるホストゾーンを選択し、[レコードを作成] をクリックします。

次の画面で以下を設定します。

レコードを作成

- レコード名に ALB に割当てるホスト名を入力
- レコードタイプに［A – IPv4 アドレス…］を選択
- エイリアスを有効化
- トラフィックのルーティング先に作成した ALB を選択
- ルーティングポリシーに［シンプルルーティング］を選択

入力後、[レコードを作成]をクリックするとDNSレコードが作成されます。

以上でAWSの設定は終了です。

3. Gléas の管理者設定（Windows 向け）

GléasのUA（申込局）より発行済み証明書をPCにインポートできるよう設定します。

※下記設定は、Gléas納品時等に弊社で設定を既に行っている場合があります

GléasのRA（登録局）にログインします。

画面上部より[認証局]をクリックし認証局一覧画面に移動し、設定を行うUA（申込局）をクリックします。

※実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

申込局詳細画面が開くので、基本設定で以下の設定を行います。

- **[証明書ストアへのインポート]をチェック**
- **証明書ストアの選択で、[ユーザストア]を選択**
- **証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]にチェック**

設定完了後、[保存]をクリックし保存します。

また、認証デバイス設定の以下項目にチェックがないことを確認します。

- **iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]**
- **Android の設定の、[Android 用 UA を利用する]**

以上でGléasの設定は終了です。

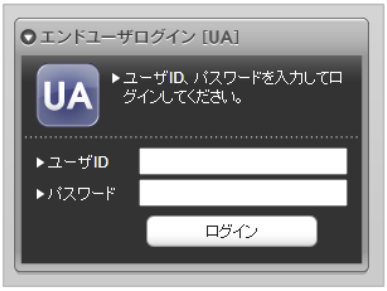
4. クライアントの設定 (Windows)

4.1. クライアント証明書のインポート

PC のブラウザ (Edge) で、UA にアクセスします。

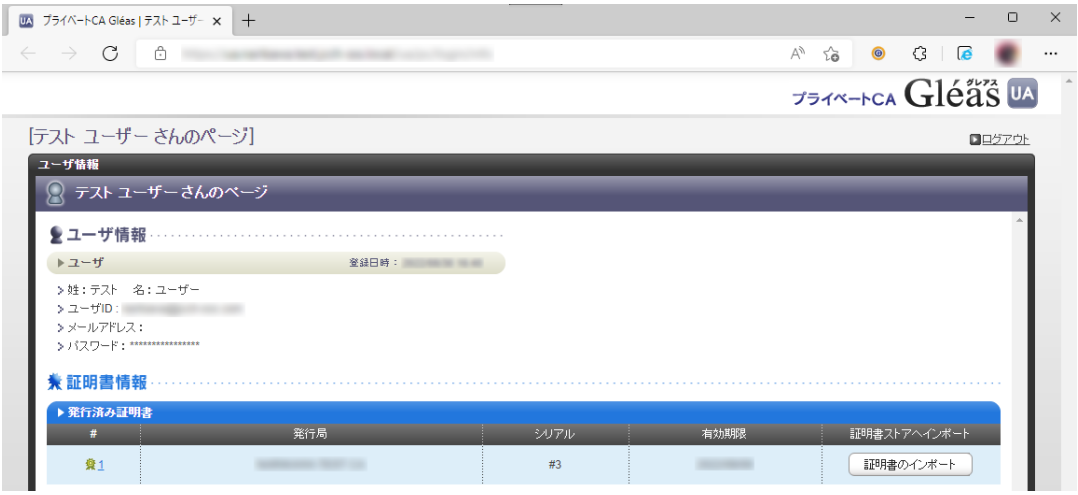
※URL https://[UA の FQDN]/[UA の名前]/ua

ログイン画面が表示されるので、ユーザ ID とパスワードを入力しログインします。

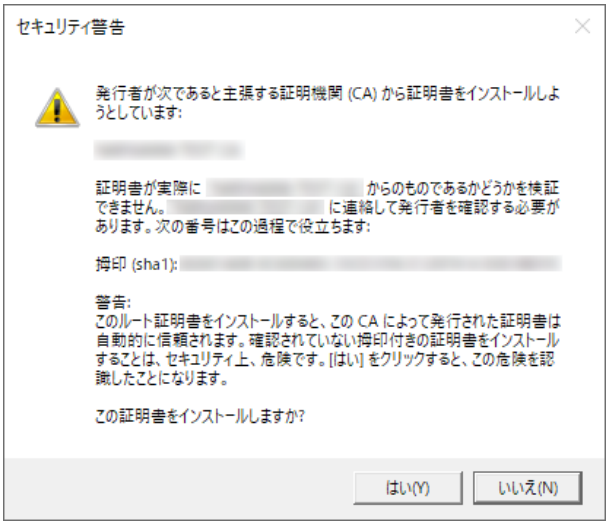


ログインすると、ユーザ専用ページが表示されます。

[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。



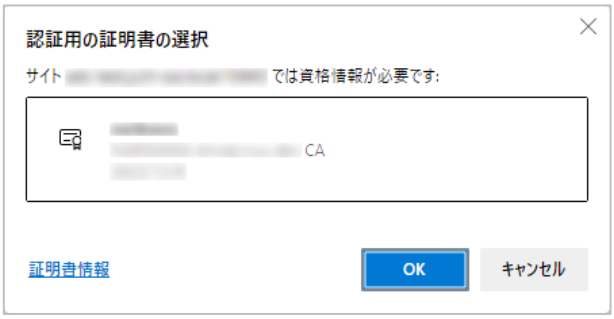
※証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を確認するなど正当性を確認してから[はい]をクリックします



インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ログインしてインポートを行うことはできません。

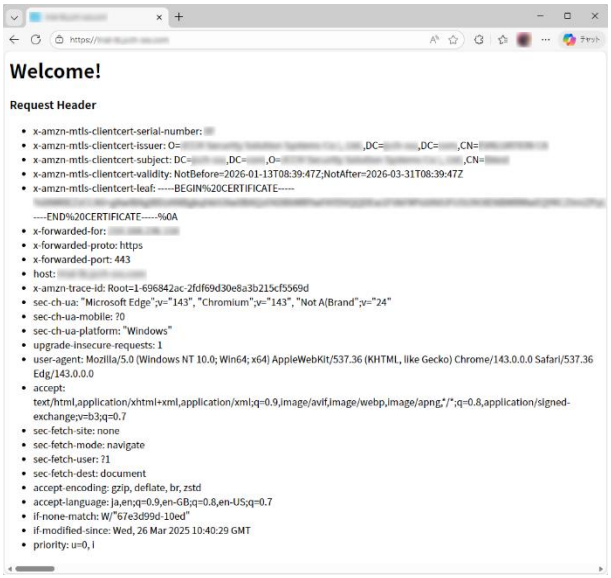
4.2. ALBにアクセス

PCのブラウザ（Edge）でALBにアクセスすると、クライアント証明書の提示を求められます。



[OK]ボタンをクリックし、クライアント証明書認証がおこなわれるとページが表示されます。

※以下は本書 7 章のサーバにアクセスしている例



証明書を持っていない場合や、失効された証明書を提示した場合はアクセスに失敗します。

※以下は失効されたクライアント証明書でアクセスした例

5. Gléas の管理者設定（iPhone 向け）

Gléas で、発行済みのクライアント証明書を iOS にインポートするための設定を本書では記載します。

※下記設定は、Gléas 納品時等に弊社で設定を既に行っている場合があります

GléasのRA（登録局）にログインします。

画面上部より[認証局]をクリックし[認証局一覧]画面に移動し、設定を行うUA (申込局)をクリックします。

※実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- **[ダウンロードを許可]をチェック**
- **[ダウンロード可能時間(分)]の設定・[インポートワンスを利用する]にチェック**

  この設定を行うと、GléasのUAからインポートから指定した時間（分）を経過した後は、構成プロファイルのダウンロードが不可能になります（インポートロック機能）。これにより複数台のデバイスへの構成プロファイルのインストールを制限することができます。

設定完了後、[保存]をクリックし保存します。

[認証デバイス情報]の[iPhone/iPadの設定]までスクロールし、[iPhone/iPad用UAを利用する]をチェックします。

構成プロファイルに必要となる情報の入力画面が展開されるので、以下設定を行います。

【画面レイアウト】

- **[iPhone用レイアウトを利用する]をチェック**
- **[ログインパスワードで証明書を保護]をチェック**

【iPhone構成プロファイル基本設定】

- **[名前]、[識別子]に任意の文字を入力（必須項目）**

各項目の入力が終わったら、 [保存] をクリックします。

以上でGléasの設定は終了です。

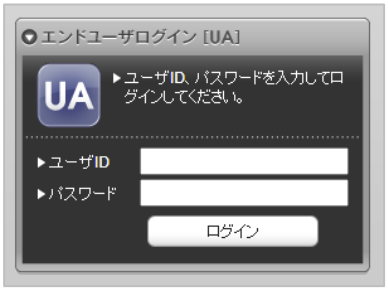
6. クライアントの設定（iPhone)

6.1. クライアント証明書のインポート

iPhoneのブラウザ（Safari）で、UAにアクセスします。

※URL https://[UA の FQDN]/[UA の名前]/ua

ログイン画面が表示されるので、ユーザ ID とパスワードを入力しログインします。

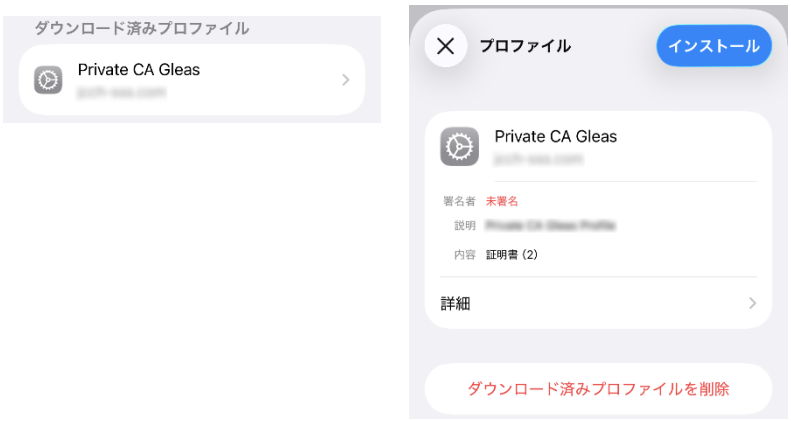


ログインすると、ユーザ専用ページが表示されます。

[ダウンロード]をタップし、構成プロファイルのダウンロードをおこないます。

※　インポートロックを有効にしている場合は、この時点からカウントが開始されます

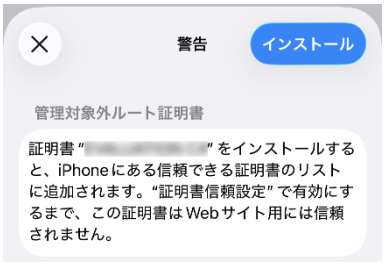
画面の表示にしたがい設定アプリから [一般] > [VPNとデバイス管理] を開き、ダウンロード済みのプロファイルが表示されるので、インストールをおこないます。



[インストール]をタップして続行してください。

インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し[インストール]をタップして続行してください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります



インストール完了画面になりますので、終了します。

なお [詳細]をタップすると、インストールされた証明書情報を見ることができます。

必要に応じて確認してください。

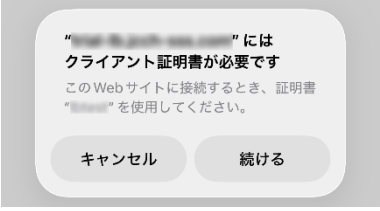
Safariに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、iPhoneでの構成プロファイルのインストールは終了です。

なお、インポートロックを有効にしている場合、[ダウンロード]をタップした時点より管理者の指定した時間を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可となります。

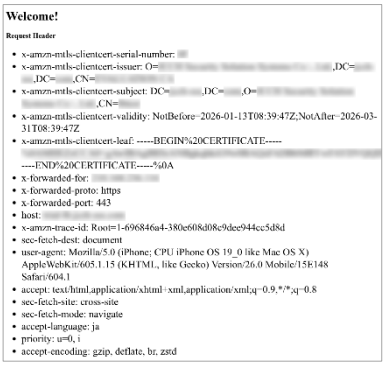
6.2. ALBにアクセス

iPhoneのブラウザ（Safari）でALBにアクセスすると、構成プロファイルにあるクライアント証明書の提示を求められます。



[続ける] をタップするとページが表示されます。

※以下は本書 7 章のサーバにアクセスしている例



証明書を持っていない場合や、失効された証明書を提示した場合はアクセスに失敗します。

※以下はクライアント証明書を持っていない状態でアクセスした例

7. サーバでクライアント証明書情報を取得

ALBによってHTTPリクエストヘッダに挿入されたクライアント証明書情報をサーバが受信していることを確認します。

※以下は、Node.jsで作成したWebサーバをtcp 6000ポートでListenする例

- **サーバを実装**

  ※リクエストヘッダを取得して出力

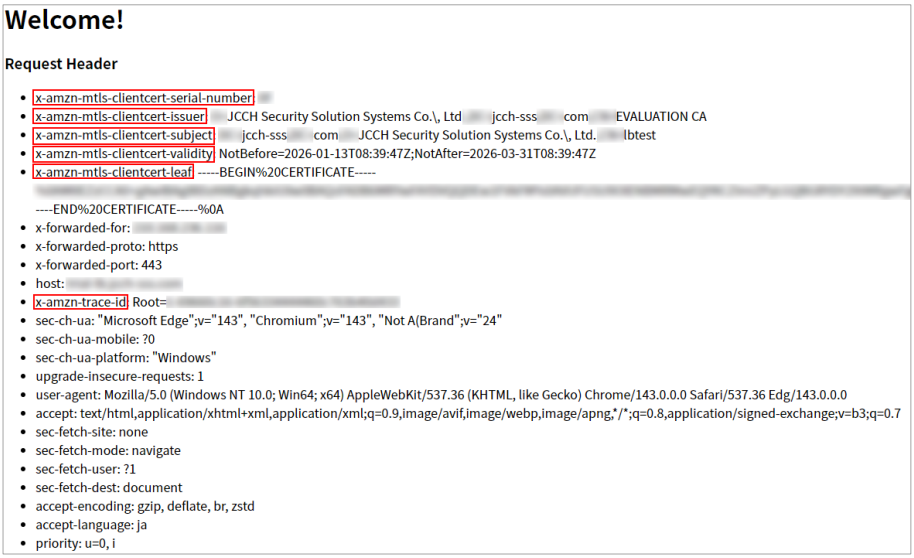
```
tee /usr/local/src/demo_app.js << 'EOS'
"use strict";
const http = require("http");
const listen_port = 6000;
const server = http.createServer((request, response) => {
  var headers = "";
  Object.keys(request.headers).forEach((key) => {
    headers = headers + `<li>${key}: ${request.headers[key]}</li>¥n`
  });
  response.writeHead(200, {"Content-Type": "text/html; charset=UTF-8", "Cache-Control": "no-cache"});
  response.write(`¥
<html><body>¥n¥
  <h1>Welcome! </h1>¥n¥
  <h3>Request Header</h3>
  <ul>¥
    ${headers}¥
  </ul>¥n¥
</body></html>¥n¥
`);
  response.end();
});
server.listen(listen_port);
console.log(`The server has started and is listening on port : ${listen_port}`);
EOS

chmod 644 /usr/local/src/demo_app.js
```

- **サーバを起動**

```
node /usr/local/src/demo_app.js
```

Web ブラウザから ALB 経由でサーバにアクセスすると、リクエストヘッダにクライアント証明書の内容が記録されていることが確認できます。

※以下はPCからEdgeブラウザでアクセスした場合の例



※リクエストヘッダの内容

リクエストヘッダ	値
X-Amzn-Mtls-Clientcert-Serial-Number	クライアント証明書のシリアル番号
X-Amzn-Mtls-Clienrcert-Issuer	クライアント証明書の発行者
X-Amzn-Mtls-Clientcert-Subject	クライアント証明書のサブジェクト
X-Amzn-Mtls-ClientcertT-Validity	クライアント証明書の有効期間
X-Amzn-Mtls-Clientcert-Leaf	クライアント証明書(PEM 形式)
X-Amzn-Trace-Id	ALB が付与するトレース情報

8. 問い合わせ

ご不明な点がございましたら、以下にお問い合わせください。

■Gléasや本検証内容、テスト用証明書の提供に関するお問い合わせ

株式会社JCCH・セキュリティ・ソリューション・システムズ

Tel: 050-3821-2195

Mail: sales@jcch-sss.com