

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

- JCCH・セキュリティ・ソリューション・システムズ、JS3 およびそれらを含むロゴは日本および他の国における株式会社 JCCH・セキュリティ・ソリューション・システムズの商標または登録商標です。Gléas は株式会社 JCCH・セキュリティ・ソリューション・システムズの商標です。
- その他本文中に記載されている製品名および社名は、それぞれ各社の商標または登録商標です。
- Microsoft Corporation のガイドラインに従って画面写真を掲載しています。

目次

1. はじめに	5
1.1. 本書について	5
1.2. 本書における環境	6
1.3. 本書における構成	8
1.4. 留意事項	9
2. AWS の設定	10
2.1. ルート証明書を S3 に登録	10
2.2. サーバ証明書を ACM に登録	12
2.3. ターゲットグループの作成	15
2.4. トラストストアの作成	18
2.5. 失効リスト (CRL) の登録	19
2.6. ロードバランサー(ALB)の作成	31
2.7. 失効リスト (CRL) の自動更新について	35
2.8. DNS 登録	36
3. Gléas の管理者設定 (Windows 向け)	38
4. クライアントの設定 (Windows)	40

4.1. クライアント証明書のインポート	40
4.2. ALB にアクセス.....	42
5. Gléas の管理者設定 (iPhone 向け)	44
6. クライアントの設定 (iPhone)	47
6.1. クライアント証明書のインポート	47
6.2. ALB にアクセス.....	50
7. サーバでクライアント証明書情報を取得	51
8. 問い合わせ	53

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

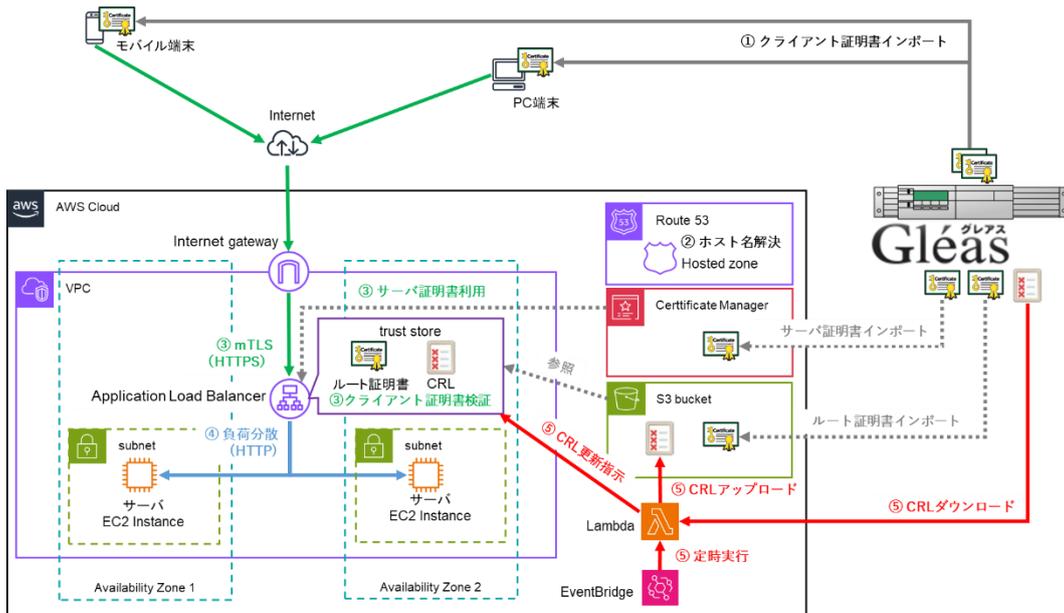
以下については、本書では説明を割愛します。

- 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関数を定期的に行うことで、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 情報

S3 にアップロードするファイルとフォルダを追加します。160 GB を超えるファイルをアップロードするには、AWS CLI、AWS SDK、または Amazon S3 REST API を使用します。 [詳細はこちら](#)

ここにアップロードするファイルとフォルダをドラッグアンドドロップするか、[ファイルを追加] または [フォルダを追加] を選択します。

ファイルとフォルダ (1 合計, 1.5 KB) 削除 ファイルを追加 フォルダの追加

このテーブル内のすべてのファイルとフォルダがアップロードされます。

🔍 名前で検索 < 1 >

<input type="checkbox"/>	名前	フォルダ	タイプ	サイズ
<input type="checkbox"/>	ia1.pem	-	-	1.5 KB

[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。

🟢 アップロードに成功しました
詳細については、[ファイルとフォルダ] テーブルを参照してください。

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



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

● [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

証明書の詳細 情報

証明書本文

```
87YcuWRH7a/RYnf2TIWfA1CZg6hUU1KBgfBssTHdlu5tBfDnvCdDUqNByyDvuPNW  
Ce/U/zlEWy5lr7DgC+MTrsjqW877  
-----END CERTIFICATE-----
```

証明書のプライベートキー

```
U5meuxyi6g5JPK14BgbFptOdao0ylMjpXZVHp12y4x8n0lCVzslUKrcR9c8VEi4a  
DAzLqmd6HMa7gATxG2sGxQLi  
-----END PRIVATE KEY-----
```

証明書チェーン - オプション 情報

```
Q3+H3wvcYTIj+fQ/UykElyr1HvWHNXAZluSK/F3Ftn0joCW9ndajo9bip7efiUJ8  
qGyNR1f/y6fn6SeHEVDbl9gH5V7Jn/GrYMv1LQ==  
-----END CERTIFICATE-----
```

タグ 情報

リソースに関連付けられたタグがありません。

[新しいタグを追加](#)

最大 50 個のタグを追加できます。

証明書のステータス

識別子	ステータス
ARN	発行済み
arn:aws:acm:ap-northeast-1:certificate/	
タイプ	
インポート済み	

[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

ターゲットグループの作成
ターゲットグループは、1つ以上のターゲットで構成できます。ロードバランサーは、リクエストをターゲットグループ内のターゲットにルーティングし、ターゲットのヘルスチェックを実行します。

設定 - イミュータブル
ターゲットタイプを選択すると、ロードバランサーとリスナーがトラフィックをターゲットにルーティングします。これらの設定は、ターゲットグループの作成後は変更できません。

ターゲットの種類
ターゲットとするリソースタイプを設定します。選択したリソースタイプのみをこのターゲットグループに登録できます。

- インスタンス**
VPC 内の EC2 インスタンスのロードバランシングをサポートします。Amazon ElastiCache リソースは対応していません。統合して自動管理を有効にします。
次に進みます: [ヘルプ](#) [ヘルプ](#) [ヘルプ](#)
- IP アドレス**
VPC およびオンプレミスのリソースへのロードバランシングをサポートします。統合して自動管理を有効にします。統合して自動管理を有効にします。
次に進みます: [ヘルプ](#) [ヘルプ](#) [ヘルプ](#)
- Lambda 関数**
Amazon Lambda 関数のロードバランシングをサポートします。トラフィックソースとして ALB が必須です。
次に進みます: [ヘルプ](#)
- Application Load Balancer**
Application Load Balancer で提供された IP アドレスと PrivateLink を参照できるようにします。トラフィックソースとして ALB が必須です。
次に進みます: [ヘルプ](#)

ターゲットグループ名
名前は、AWS アカウントごとに、各リージョンで一意である必要があります。

説明可能な文字、数字、およびハイフン()、先頭または末尾にハイフンを使用することはできません。合計 1~32 文字。カラム: 0/32

プロトコル
ロードバランサーとターゲット間の通信用プロトコル。
HTTP

ポート
ターゲットがトラフィックを受け取るポート番号。登録時に他のターゲットのためにオーバーライドできます。
80

IP アドレスタイプ
このターゲットグループに登録できるのは、指定された IP アドレスタイプのターゲットのみです。

- IPv4**
各 EC2 インスタンスには、プライベート IP アドレスが割り当てられ、デフォルトではネットワークインターフェイス (NIC) が割り当てられています。インスタンスの IP アドレスは、この IP アドレスタイプに割り当てられます。
- IPv6**
IPv6 を使用する EC2 インスタンスには、プライベート IPv6 アドレスが割り当てられていない必要があります。これは EC2 インスタンスのデフォルトネットワークインターフェイス (NIC) で設定されます。 [詳しくはこちら](#)

VPC
ターゲットグループに追加する EC2 インスタンスを含む VPC を選択します。上記で選択した IP アドレスタイプをサポートする VPC のみが、このリストに表示されます。

172.31.0.0/16 [VPC の作成](#)

プロトコルバージョン

- HTTP1**
HTTP1.1 を使用してターゲットにリクエストを送信します。これはリクエストプロトコルが HTTP1.1 または HTTP2 の場合にサポートされます。
- HTTP2**
HTTP2 を使用してターゲットにリクエストを送信します。これはリクエストプロトコルが HTTP2 または gRPC の場合にサポートされますが、gRPC 両方の機能は使用できません。
- gRPC**
gRPC を使用してターゲットにリクエストを送信します。これはリクエストプロトコルが gRPC の場合にサポートされます。

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

ヘルスチェック
関連付けられたロードバランサーは、以下の設定ごとに、登録済みターゲットのステータスをテストするため、登録済みターゲットに対して定期的にリクエストを送信します。

ヘルスチェックプロトコル
HTTP

ヘルスチェックパス
デフォルトパス「/」を使用してルートに対してヘルスチェックを実行するか、または必要に応じてカスタムパスを指定します。
/
最大文字数は 1024 です。

▶ ヘルスチェックの詳細設定

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

使用可能なインスタンス (5)

インスタンスをフィルター

インスタンス ID	名前	状態	セキュリティグループ	ゾーン
i-01234567890123456	my-instance-1	実行中	sg-12345678	ap-northeast-1b
i-01234567890123456	my-instance-2	実行中	sg-12345678	ap-northeast-1b
i-01234567890123456	my-instance-3	実行中	sg-12345678	ap-northeast-1b
i-01234567890123456	my-instance-4	実行中	sg-12345678	ap-northeast-1b
i-01234567890123456	my-instance-5	実行中	sg-12345678	ap-northeast-1b

0 個を選択済み

選択したインスタンスのポート
選択したインスタンスにトラフィックをルーティングするためのポート。
1-65535 (最後のポートをカンマで区切ります)

保留中として以下を含める

1つの選択は以下で保留中です。準備完了時にさらに追加するか、ターゲットを登録してください。

ターゲットを確認

ターゲット (1) 保留中のみ表示 保留中のみをすべて削除

ターゲットをフィルター

インスタンス ID	名前	ポート	状態	セキュリティグループ	ゾーン	プライベート IPv4 アドレス	サブネ
i-01234567890123456	my-instance-1	80	実行中	sg-12345678	ap-northeast-1b	10.0.1.10	subnet

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詳細			
名前	ターゲットの種類 インスタンス	プロトコル: ポート HTTP: 80	プロトコルバージョン HTTP1
VPC	IP アドレスタイプ IPv4		

ヘルスチェックの詳細			
ヘルスチェックプロトコル HTTP	ヘルスチェックパス /	ヘルスチェックポート traffic-port	間隔 30 秒
タイムアウト 5 秒	正常のしきい値 5	非正常のしきい値 2	成功コード 200

ステップ 2: ターゲットを登録する 編集

ターゲット (1)			
インスタンス ID	名前	ポート	ゾーン
			ap-northeast-1b

[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。

👍 ターゲットグループ [] が正常に作成されました。異常検出は、登録されているすべてのターゲットに自動的に適用されます。結果は【ターゲット】タブで表示できます。 🗨️ フィードバックを送信 ✕

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を行うため、ここでは省略します。

トラストストアの設定

トラストストアの名前
名前は各リージョン内で一意である必要があります。トラストストアの作成後に変更することはできません。

ハイフンを含む最大 32 文字の英数字を使用できます。名前の先頭または末尾にハイフンを使用することはできません。

認証局バンドル
認証局 (CA) PEM 形式のファイルが現在保存されている場所を選択します。ELB サービスはファイルを 1 回取得します。この URI はトラストストア設定には保存されません。 [S3 バケットを作成](#)

S3 URI オブジェクトのバージョン

s3://.../ia1.pem 2026年1月13日, 1... 表示 S3 を参照

形式: s3://bucket/prefix/object

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。

🟢 トラストストア [] が正常に作成されました。 ✕

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に利用サービス进行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

ポリシーの詳細

ポリシー名
このポリシーを識別するためのわかりやすい名前を入力します。

最大 128 文字です。英数字と「+','=','@','-」の文字を使用してください。

説明 - オプション
このポリシーの簡単な説明を追加します。

最大 1000 文字です。英数字と「+','=','@','-」の文字を使用してください。

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。

🔔 ポリシー `gléas-policy` が作成されました。

ポリシーを表示 ×

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

ユーザーの詳細

ユーザー名

ユーザー名には最大 64 文字を使用できます。有効な文字: A~Z、a~z、0~9、+、=、.、@、_、- (ハイフン)

AWS マネジメントコンソールへのユーザーアクセスを提供する - オプション
コンソールへのアクセスに加えて、SignInLocalDevelopmentAccess 権限を持つユーザーは、アクセスキーを必要とせずに、同じコンソール認証情報を使用してプログラムによるアクセスを行うことができます。

① アクセスキー、または AWS CodeCommit や Amazon Keyspaces のサービス固有の認証情報を使用してプログラムによるアクセスを作成する場合は、この IAM ユーザーの作成後に生成できます。 [詳細はこちら](#)

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

許可のオプション

ユーザーをグループに追加
ユーザーを既存のグループに追加するか、新しいグループを作成します。グループを使用して、職務別にユーザーの許可を管理することをお勧めします。

許可のコピー
既存のユーザーから、すべてのグループメンバーシップ、アタッチされた管理ポリシー、およびインラインポリシーをコピーします。

ポリシーを直接アタッチする
ユーザーにマネージドポリシーを直接アタッチします。ベストプラクティスとして、代わりにグループにポリシーをアタッチすることをお勧めします。次に、ユーザーを適切なグループに追加します。

許可ポリシー

- 本書2.5.1で作成したIAMポリシーを選択

許可ポリシー (1/1451)

新しいロールにアタッチする 1 つまたは複数のポリシーを選択します。

絞り込み タイプ

すべてのタイプ ▼ 2一致

< 1 > ⚙

ポリシー名	タイプ	アタッチされ...
<input checked="" type="checkbox"/> customer-management-policy	カスタマー管理	0

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

ユーザーの詳細

ユーザー名 XXXXXXXXXXXX | コンソールパスワードのタイプ
None

パスワードのリセットが必要
いいえ

許可の概要

< 1 >

名前	▲	タイプ	▼	次として使用:	▼
XXXXXXXXXXXX		カスタマー管理		許可ポリシー	

タグ - オプション

タグは AWS リソースに追加できるキーと値のペアで、リソースの特定、整理、検索に役立ちます。このユーザーに関連付けるタグを選択します。

リソースに関連付けられたタグはありません。

[新しいタグを追加する](#)

最大 50 個のタグを追加できます。

[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。

🟢 ユーザーが正常に作成されました

ユーザーのパスワードと、AWS マネジメントコンソールにサインインするための手順が記載された E メールを表示してダウンロードできます。

[ユーザーを表示](#)

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

ユースケース

コマンドラインインターフェイス (CLI)
このアクセスキーを使用して、AWS CLI から AWS アカウントへのアクセスを有効化しようとしています。

ローカルコード
このアクセスキーを使用して、ローカル開発環境のアプリケーションコードから AWS アカウントへのアクセスを有効化しようとしています。

AWS コンピューティングサービスで実行されるアプリケーション
このアクセスキーを使用して、Amazon EC2、Amazon ECS、AWS Lambda などの AWS コンピューティングサービスで実行されるアプリケーションコードから AWS アカウントへのアクセスを有効化しようとしています。

サードパーティーサービス
このアクセスキーを使用して、AWS リソースをモニタリングまたは管理するサードパーティーアプリケーションまたはサービスへのアクセスを有効化しようとしています。

AWS の外部で実行されるアプリケーション
このアクセスキーを使用して、AWS リソースへのアクセスが必要な AWS 外部のデータセンターやその他のインフラストラクチャで実行されているワークロードを認証する予定です。

その他
ここにはユーザーのユースケースがリストされていません。

推奨された代替案

- AWS CLI V2 と `aws login` コマンドを使用して、CLI の既存のコンソール認証情報を使用します。 [詳細はこちら](#)
- ブラウザベースの CLI である AWS CloudShell を使用してコマンドを実行します。 [詳細はこちら](#)

確認

上記の推奨事項を理解し、アクセスキーを作成します。

[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

説明タグ値
このアクセスキーの目的と使用場所を説明します。わかりやすい説明は、後でこのアクセスキーを確実にローテーションするのに役立ちます。

最大 256 文字です。使用できる文字は、UTF-8 で表現できる文字、数字、スペース、および `_./=+-@` です。

[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。

◎ これは、シークレットアクセスキーを表示またはダウンロードできる唯一の機会です。後で復元することはできません。ただし、新しいアクセスキーはいつでも作成できます。 ×

ステップ 1
● 主要なベストプラクティスと代替案にアクセスする

ステップ 2 - オプション
● 説明タグを設定

ステップ 3
● **アクセスキーを取得**

アクセスキーを取得 情報

アクセスキー
シークレットアクセスキーを紛失または失念した場合、それを取得することはできません。代わりに、新しいアクセスキーを作成し、古いキーを非アクティブにします。

アクセスキー		シークレットアクセスキー
 <code>AKIAI44QH8DHBEXAMPLE</code>		 表示

アクセスキーのベストプラクティス

- アクセスキーをプレーンテキストもしくはコードリポジトリで、またはコードに保存しないでください。
- 不要になったアクセスキーを無効化または削除します。
- 最小権限の許可を有効にします。
- アクセスキーを定期的にローテーションします。

アクセスキーの管理の詳細については、「[AWS アクセスキーを管理するためのベストプラクティス](#)」を参照してください。

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

基本的な設定

ロードバランサー名
名前は AWS アカウント内で一意である必要があり、ロードバランサーの作成後に変更することはできません。

ハイフンを含む最大 32 文字の英数字を使用できますが、名前の先頭または末尾にハイフンを使用することはできません。

スキーム | 情報
ロードバランサーの作成後にスキームを変更することはできません。

<input checked="" type="radio"/> インターネット向け <ul style="list-style-type: none">インターネット向けトラフィックを処理します。パブリック IP アドレスがあります。DNS 名はパブリック IP に解決されます。パブリックサブネットが必要です。	<input type="radio"/> 内部 <ul style="list-style-type: none">内部トラフィックを処理します。プライベート IP アドレスがあります。DNS 名はプライベート IP に解決されます。IPv4 および Dualstack の IP アドレスタイプと互換性があります。
---	---

ロードバランサーの IP アドレスタイプ | 情報
ロードバランサーに割り当てるフロントエンド IP アドレスタイプを選択します。このロードバランサーにマッピングされる VPC とサブネットには、選択した IP アドレスタイプを含める必要があります。パブリック IPv4 アドレスには追加料金がかかります。

- IPv4**
IPv4 アドレスのみが含まれます。
- Dualstack**
IPv4 と IPv6 アドレスが含まれます。
- パブリック IPv4 のない Dualstack**
パブリック IPv6 アドレスとプライベートの IPv4 アドレスと IPv6 アドレスが含まれます。インターネットに接続しているロードバランサーとのみ互換性があります。

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。

ネットワークマッピング 情報

ロードバランサーは、IP アドレス設定に従って、選択したサブネットのターゲットにトラフィックをルーティングします。

VPC | 情報
ロードバランサーは、選択した VPC 内に存在し、その中でスケールします。Lambda またはオンプレミスのターゲットにルーティングする場合や VPC ピアリングを使用する場合を除き、選択した VPC はロードバランサーのターゲットをホストしなければならない場所でもあります。ターゲットの VPC を確認するには、[ターゲットグループ](#) を表示します。

vpc- ()
172.30.0.0/16 🔄 [VPC の作成](#)

IP プール | 情報
オプションで、ロードバランサーの IP アドレスの優先ソースとして IPAM プールを設定することもできます。[Amazon VPC IP Address Manager コンソール](#) でプールを作成または表示してください。

パブリック IPv4 アドレスに IPAM プールを使用
選択した IPAM プールが、パブリック IPv4 アドレスの優先ソースになります。プールが枯渇した場合、IPv4 アドレスは AWS によって割り当てられます。

アベイラビリティゾーンとサブネット | 情報
少なくとも 2 つのアベイラビリティゾーンと、各ゾーンのサブネットを 1 つ選択します。選択した各ゾーンにロードバランサーノードが配置され、トラフィックに応じて自動的にスケールアップされます。ロードバランサーは、選択したアベイラビリティゾーンのターゲットにのみトラフィックをルーティングします。

ap-northeast-1b (apne1-az4)
サブネット
ロードバランサーの IP アドレスタイプに対応する CIDR ブロックのみが使用されます。ロードバランサーの効率的なスケールアップには、使用可能な IP アドレスが 8 つ以上必要です。

subnet-
IPv4 サブネット CIDR: 172.30.1.0/24 🔄

ap-northeast-1c (apne1-az1)
サブネット
ロードバランサーの IP アドレスタイプに対応する CIDR ブロックのみが使用されます。ロードバランサーの効率的なスケールアップには、使用可能な IP アドレスが 8 つ以上必要です。

subnet-
IPv4 サブネット CIDR: 172.30.2.0/24 🔄

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

セキュリティグループ 情報

セキュリティグループは、ロードバランサーへのトラフィックを制御する一連のファイアウォールルールです。既存のセキュリティグループを選択するか、[新しいセキュリティグループを作成](#) できます。

セキュリティグループ
最大 5 個のセキュリティグループを選択 🔄

sg- VPC: vpc- ✕

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

セキュアリスナーの設定 [情報](#)
これらの設定は、すべてのセキュアリスナーに適用されます。作成後は、リスナーごとにこれらの設定を管理できます。

セキュリティポリシー [情報](#)
ロードバランサーは、セキュリティポリシーと呼ばれる Secure Socket Layer (SSL) ネゴシエーション設定を使用して、クライアントと SSL 接続を管理します。 [セキュリティポリシーの比較](#)

セキュリティカテゴリ [ポリシー名](#) [参照](#)
すべてのセキュリティポリシー

デフォルト SSL/TLS サーバー証明書
クライアントが SNI プロトコルなしで接続した場合、または一致する証明書がない場合に使用される証明書。この証明書は、AWS Certificate Manager (ACM)、Amazon Identity and Access Management (IAM) から入手するか、証明書をインポートできます。この証明書はリスナー証明書リストに自動的に追加されます。

証明書の取得先
 ACM から IAM から 証明書をインポート

証明書 (ACM から)
選択した証明書が、このロードバランサーのセキュアリスナーのデフォルト SSL/TLS サーバー証明書として適用されます。
 [新しい ACM 証明書をリクエスト](#)

クライアント証明書の処理 [情報](#)
クライアント証明書は、リモートサーバーに監禁されたリクエストを行うために使用されます。 [詳細はこちら](#)

相互認証 (mTLS)
相互 TLS (トランスポートレイヤーセキュリティ) 認証は、双方向の ID 認証を提供します。TLS 経由のセキュリティのレイヤーを追加し、接続しているクライアントをサービスが検証するのを許可します。

パススルー
証明書全体が HTTP ヘッダーとしてバックエンドターゲットに送信され、クライアント証明書が信頼できるかどうか検証されます。

トラストストアで検証
ロードバランサーとクライアントは互いの ID を検証し、TLS 接続を確立して互いの間の通信を暗号化します。

トラストストア [情報](#)
トラストストアには、クライアントを識別するために信頼する証明書と期限切れが含まれています。追加の証明書失効リスト (CRL) をトラストストアの詳細ページにアップロードできます。
 [新しい](#)

mTLS リスナーの高度な設定

クライアント証明書の処理 [情報](#)
クライアント証明書の期限が切れたときのロードバランサーの応答方法を決定します。デフォルトオプションはほとんどのお客様のニーズに対応します。

期限切れのクライアント証明書を許可しない - 推奨
証明書の期限が切れたときに接続を拒否します。これが最も安全な設定です。

期限切れのクライアント証明書を許可する
期限が切れた証明書を含む接続でも、ネットワークに到達することを許可します。

トラストストアの CA サブジェクト名をアドバタイズ [情報](#)
リスナーがトラストストアの信頼する期限切れ (CA) サブジェクト名をアドバタイズするかどうかを決定します。

オフ - デフォルト

オン

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。

🟢 次のロードバランサーが正常に作成されました: ×
ロードバランサーが完全に設定され、トラフィックをルーティングするまでに数分かかる場合があります。また、ターゲットの登録処理が完了して最初のヘルスチェックに合格するまでに数分かかる場合もあります。

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から定期的に行う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。

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に設定します。

※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。

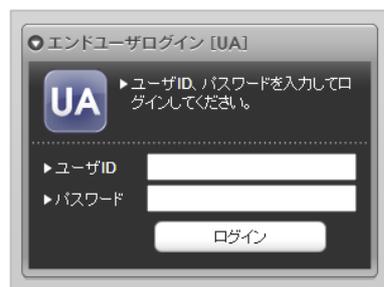
4. クライアントの設定 (Windows)

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。

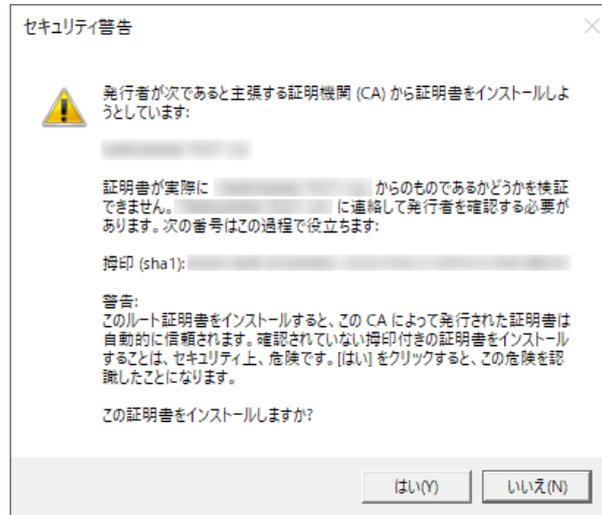


ログインすると、ユーザ専用ページが表示されます。

[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

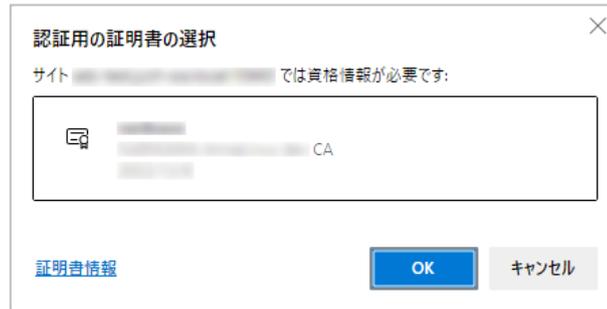


インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ログインしてインポートを行うことはできません。



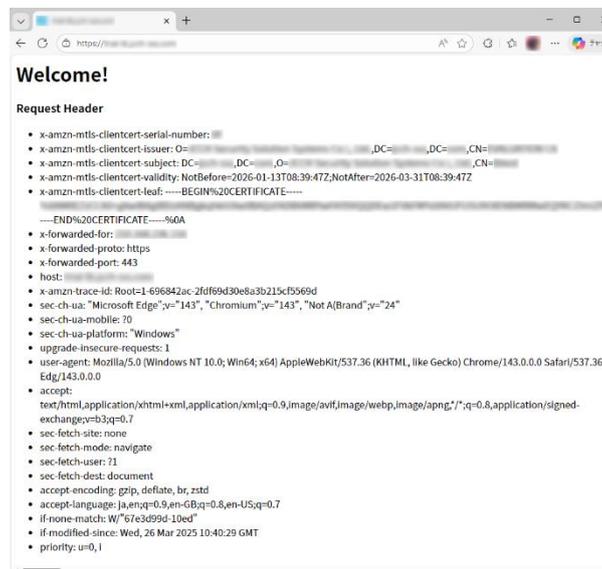
4.2. ALBにアクセス

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な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）

認証デバイス情報

▶ iPhone / iPad の設定

iPhone/iPad 用 UA を利用する

画面レイアウト

iPhone 用レイアウトを使用する ログインパスワードで証明書を保護

Mac OS X 10.7以降の接続を許可

OTA(Over-the-air)

OTAエンロールメントを利用する 接続する iOS デバイスを認証する

OTA用SCEP URL

OTA用認証局

iPhone 構成プロファイル基本設定

名前(デバイス上に表示)

識別子(例: com.jcch-sss.profile)

プロファイルの組織名

説明

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。

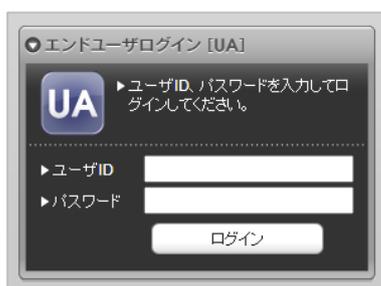
6. クライアントの設定 (iPhone)

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。



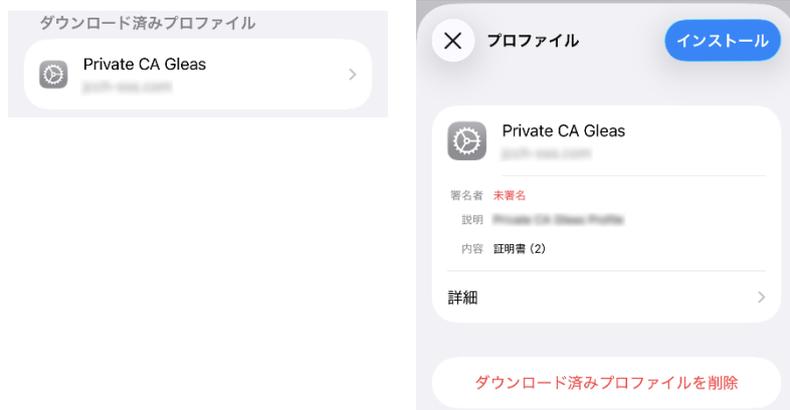
ログインすると、ユーザ専用ページが表示されます。

[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。

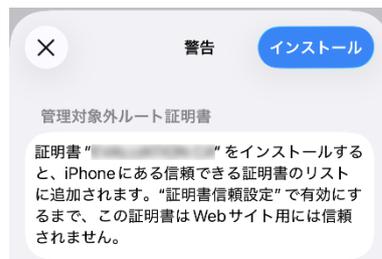


[インストール]をタップして続行してください。

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Gleas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。

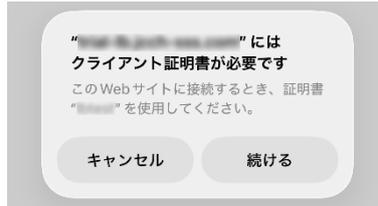
以上で、iPhoneでの構成プロファイルのインストールは終了です。

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

```
Welcome!
Request Header
• x-amzn-mtls-clientcert-serial-number: [redacted]
• x-amzn-mtls-clientcert-issuer: O=[redacted], DC=[redacted]
• x-amzn-mtls-clientcert-subject: DC=[redacted], O=[redacted], CN=[redacted]
• x-amzn-mtls-clientcert-validity: NotBefore: 2026-01-13T08:39:47Z, NotAfter: 2026-03-31T08:39:47Z
• x-amzn-mtls-clientcert-leaf: -----BEGIN%20CERTIFICATE-----
-----END%20CERTIFICATE-----%3d0A
• x-forwarded-for: [redacted]
• x-forwarded-proto: https
• x-forwarded-port: 443
• host: [redacted]
• x-amzn-trace-id: Root=1-696846a4-380e608d08c9dec944cc5d8d
• sec-fetch-dest: document
• user-agent: Mozilla/5.0 (iPhone; CPU iPhone OS 19_0 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/26.0 Mobile/15E148 Safari/604.1
• accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
• sec-fetch-site: cross-site
• sec-fetch-mode: navigate
• accept-language: ja
• priority: u=0, i
• accept-encoding: gzip, deflate, br, zstd
```

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>`+`n`
    ${headers}`+`n`
  </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

```
Welcome!
Request Header
• x-amzn-mtls-clientcert-serial-number
• x-amzn-mtls-clientcert-issuer Jcch Security Solution Systems Co., Ltd jcch-sss.com EVALUATION CA
• x-amzn-mtls-clientcert-subject jcch-sss.com Jcch Security Solution Systems Co., Ltd. lbtest
• x-amzn-mtls-clientcert-validity NotBefore=2026-01-13T08:39:47Z;NotAfter=2026-03-31T08:39:47Z
• x-amzn-mtls-clientcert-leaf -----BEGIN%20CERTIFICATE-----
-----END%20CERTIFICATE-----%0A
• x-forwarded-for:
• x-forwarded-proto: https
• x-forwarded-port: 443
• host:
• x-amzn-trace-id Root=
• sec-ch-ua: "Microsoft Edge";v="143", "Chromium";v="143", "Not A(Brand";v="24"
• sec-ch-ua-mobile: ?0
• sec-ch-ua-platform: "Windows"
• upgrade-insecure-requests: 1
• user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/143.0.0.0 Safari/537.36 Edg/143.0.0.0
• accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
• sec-fetch-site: none
• sec-fetch-mode: navigate
• sec-fetch-user: ?1
• sec-fetch-dest: document
• accept-encoding: gzip, deflate, br, zstd
• accept-language: ja
• priority: u=0, i
```

※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-Clientcert-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