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

Azure Application Gateway でのクライアント証明書認証

Ver.1.0

2026 年 2 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、MicrosoftがAzure Application Gateway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。

- **Azure Application Gateway**
  ※以後、「App Gateway」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**
  ※Azure Virtual Machine インスタンス
  ※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

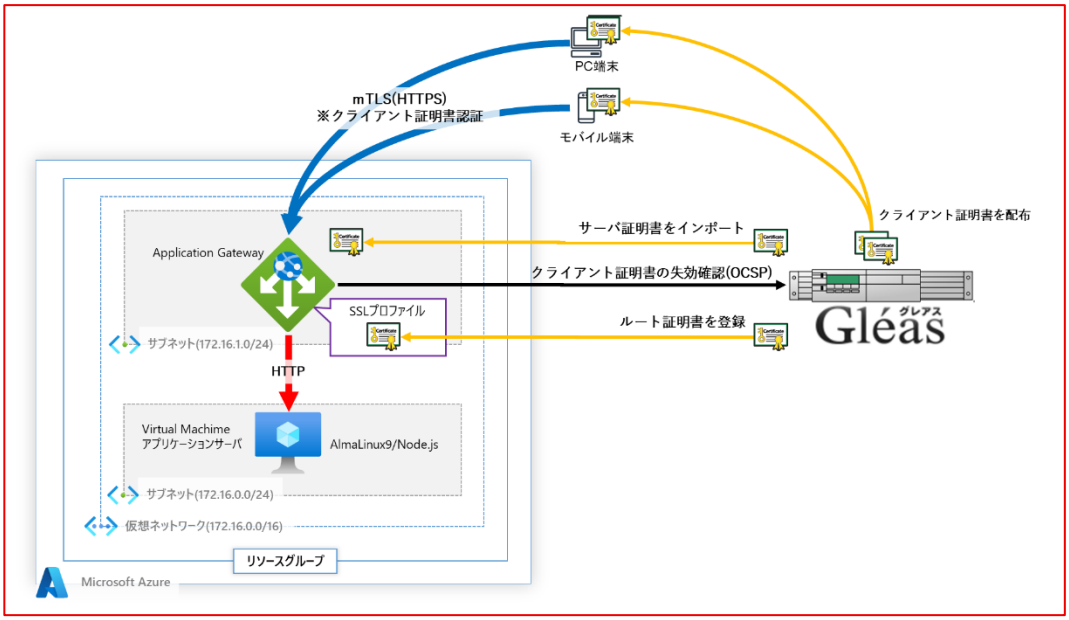
以下については、本書では説明を割愛します。

- **Azure 管理コンソールの基本操作**
- **Azure Virtual Machineの基本設定（デプロイ、基本設定)**
- **Azure PowerShellの基本設定（インストール、基本操作)**
- **アプリケーションサーバの基本設定（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から発行したサーバ証明書をApp Gatewayに登録**
- **GléasのルートCA証明書をApp GatewayのSSLプロファイルに登録**
- **App GatewayのSSLプロファイルにOCSPによる失効確認を設定**
- **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. **PCではEdgeブラウザ、iPhoneではSafariブラウザよりApp Gatewayにアクセス。**
   App Gateway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、提示した証明書が期限切れまたは失効済みの場合、クライアント証明書認証に失敗。
3. **App Gatewayは証明書認証後にアプリケーションサーバにアクセスしてWebページをクライアントに表示。**

1.4. 留意事項

1.4.1. サーバ証明書の発行について

本書2.1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. OCSP による失効確認について

本書2.4の方法で、OCSPによる失効確認を設定する場合、事前に作業PCに Azure PowerShell をインストールする必要があります。

2. Azure の設定

2.1. サーバ証明書を発行

App Gateway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、App Gateway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でサーバ証明書を発行し、ダウンロードします。

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 App Gateway
- 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。

ダウンロードした証明書をファイルは、Azure 管理コンソールからアップロードできるようにファイル名の拡張子を.p12 から.pfx に変更しておきます。

2.2. App Gatewayのデプロイ

App Gatewayを作成します。

Azure 管理コンソールのメニューから [Application gateways]を選択し、

[+create] > [Application Gateway]をクリックします。

次の画面で以下を設定します。

[基本]タブ

- **サブスクリプションを選択**
- **リソースグループに App Gateway を配置するリソースグループを選択**
  ※存在しない場合は[新規作成]をクリックしてリソースグループを作成
- **ゲートウェイ名に任意の名前を入力**
- **リージョンを選択**
- **レベルに [Standard cV2] を選択**
- **最小インスタンス数に 0 を指定**
- **仮想ネットワークにターゲット VM が配置されているネットワークを選択**
- **サブネットの[サブネット構成の管理]をクリック**

- **[+サブネット]をクリックしてウィンドウを開く**
  ※App Gateway のみが配置されたサブネットを作成

  [サブネットの追加]ウィンドウ
  - **名前に任意の名前を入力**
  - **アドレス空間を指定**
  - **開始アドレスを指定**
  - **サイズを指定**

- **[追加]をクリックしてウィンドウを閉じる**

- **サブネットに作成した仮想ネットワークのサブネットを選択**

- **[次： フロントエンド >]をクリック**

[フロントエンド]タブ

- **フロントエンド IP の種類に[パブリック]を選択**
- **パブリック IPv4 アドレスの[新規追加]をクリックしてウィンドウを開く**

[パブリック IP の追加]ウィンドウ

- **名前に任意の名前を入力**

- **[OK]をクリックしてウインドウを閉じる**

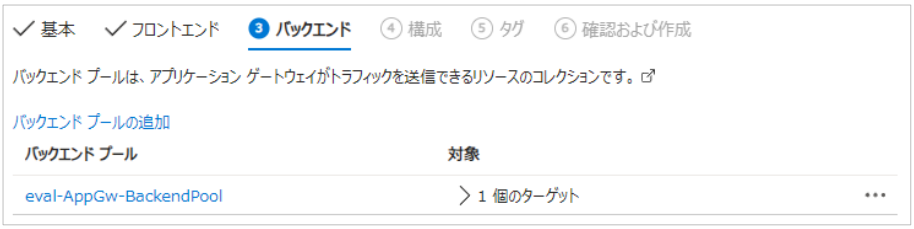
- **[次： バックエンド >]をクリック**

[バックエンド]タブ

- **[バックエンドプールの追加]をクリックし、ウィンドウを開く**

  [バックエンドプールの追加]ウィンドウ
  - **名前に任意の名前を指定**
  - **ターゲットの種類に[仮想マシン]を選択**
  - **ターゲットに対象の仮想マシンを選択**

  - **[追加を]クリックし、ウィンドウを閉じる**



- **[次： 構成 >]をクリック**

[構成]タブ

- **[ルーティング規則の追加]をクリックしてウィンドウを開く**
  [ルーティング規則の追加]ウィンドウ
  - **ルール名に任意の名前を指定**
  - **優先度に 100 を入力**
    ※1～20000 を指定可能。1 は最も高い優先度

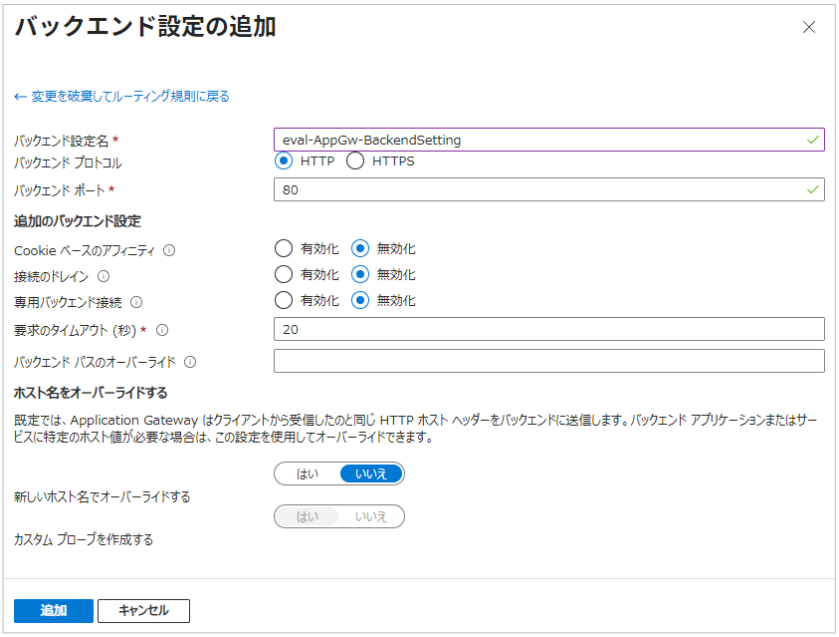
  [リスナー]タブ
  - **リスナー名に任意の名前を入力**
  - **フロントエンド IP に[パブリック IPv4]を選択**
  - **プロトコルに[HTTPS]を選択**
  - **ポートに 443 を入力**
  - **証明書の選択に[証明書のアップロード]を選択**
  - **証明書名に任意の名前を入力**
  - **PFX 証明書ファイルに本書 2.1 でダウンロードしたサーバ証明書を指定**
  - **パスワードにサーバ証明書のパスワードを入力**

[バックエンドターゲット]タブ

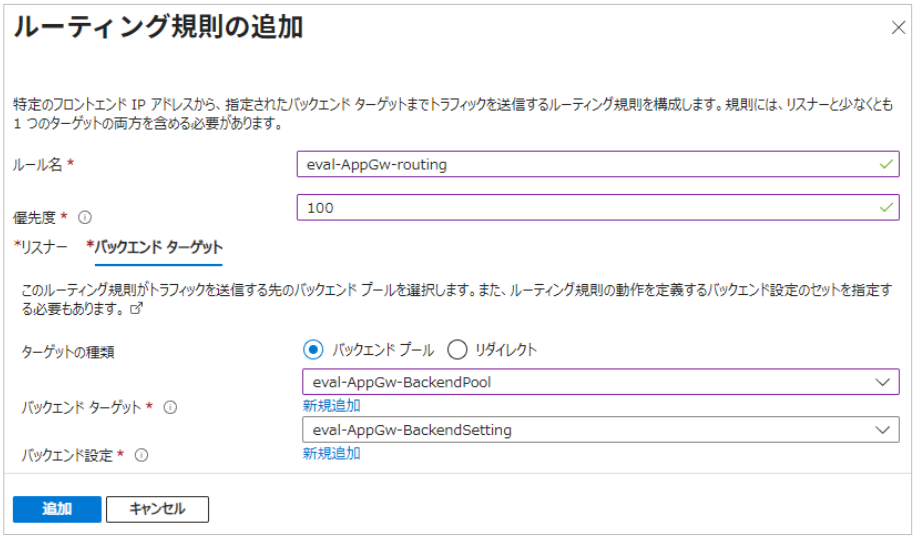
- **ターゲットの種類に[バックエンドプール]を選択**
- **バックエンドターゲットに作成したバックエンドプールを選択**
- **バックエンド設定の[新規追加]をクリックしてウィンドウを開く**

[バックエンド設定の追加]ウィンドウ

- **バックエンド設定名に任意の名前を設定**
- **バックエンドプロトコルに[HTTP]を設定**
- **バックエンドポートに 80 を入力**
- **要求のタイムアウト(秒) に 20 を入力**



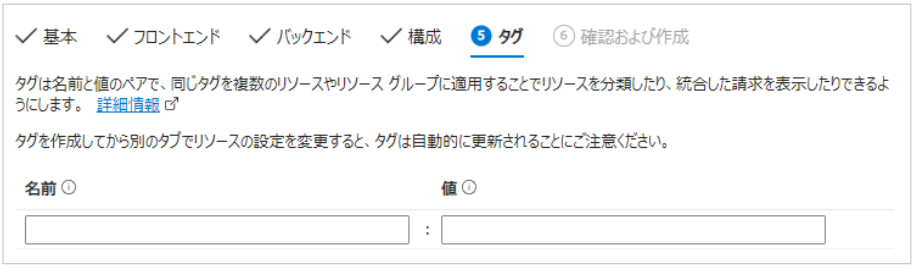
- **[追加]クリックし、ウィンドウを閉じる**



- **[追加]をクリックし、ウィンドウを閉じる**

- **[次： タグ >]をクリック**

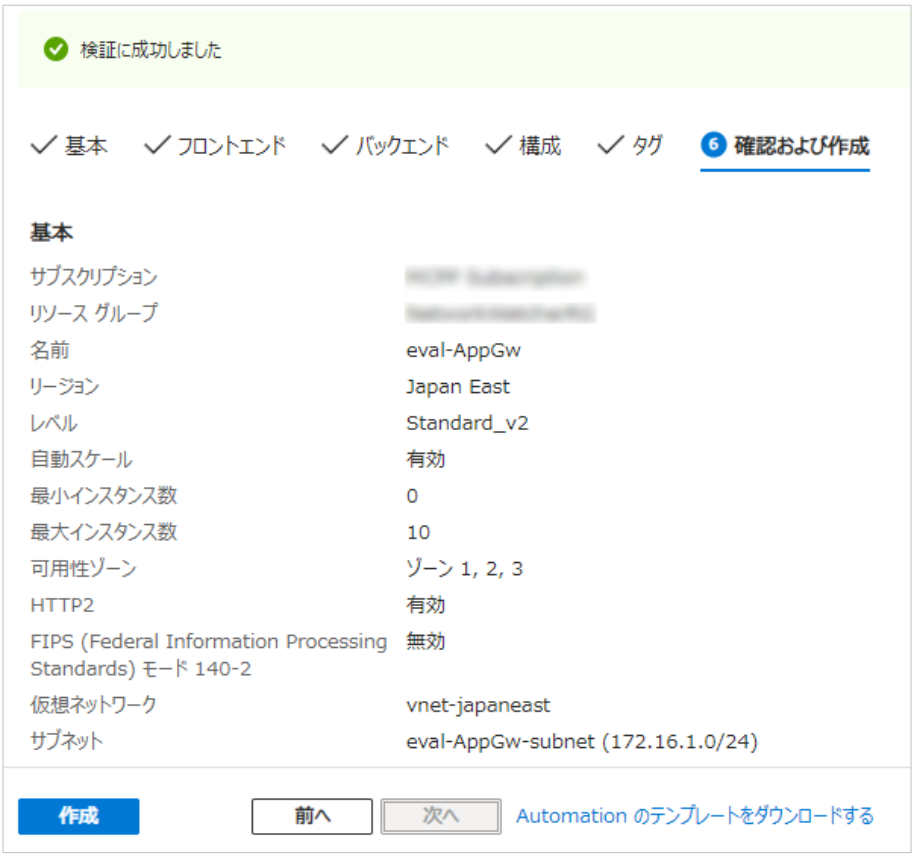
[タグ]タブ



- **[次： 構成および作成 >]をクリック**

[構成および作成]タブ

- **設定を確認**



- **[作成]をクリック**

しばらくすると App Gateway が作成されます。

2.3. クライアント証明書認証を有効化

クライアント証明書認証を利用するためには、App Gateway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。

App Gatewayにクライアント証明書認証を行うためのSSLプロファイルを設定します。

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

Azure 管理コンソールのメニューから [Application gateways]を選択し、一覧から対象の App Gateway を選択します。

メニュー[SSL 設定]を開き、[+SSL プロファイル]をクリックします。

次の画面で以下を設定します。

SSLプロファイルの作成

- **SSL プロファイル名に任意の名前を入力**
- **[Client Authentication]タブを選択**
- **[新しい証明書のアップロード]をクリックしてウィンドウを開く**

[クライアント CA 証明書のアップロード]ウィンドウ

- **証明書名に任意の名前を入力**
- **CER または PEM ファイルにルート証明書を指定**

- **[OK]をクリックしてウィンドウを閉じる**

- **クライアント証明書の発行者の DN を検証します をチェック**

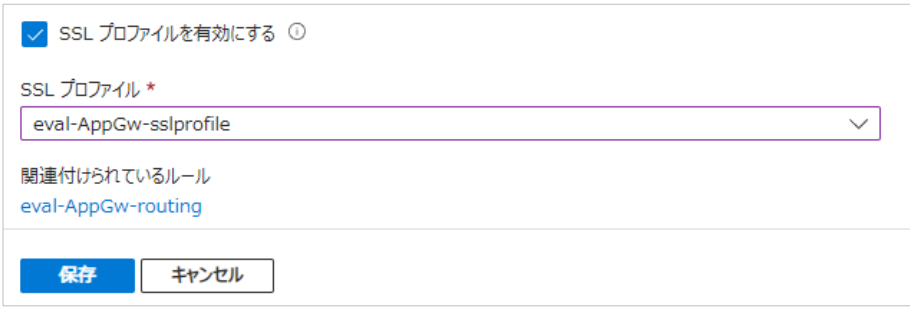
- **[追加]をクリック**

続いて App Gateway のリスナーに作成した SSL プロファイルを割り当てます。

メニュー[リスナー]を開き、[リスナー]タブを選択、対象のリスナーを選択します。

リスナーの設定画面で以下を設定します。

- **SSL プロファイルを有効にする をチェック**
- **SSL プロファイルに作成した SSL プロファイルを選択**



- **[保存]をクリック**

設定が反映され、クライアント証明書認証が有効化されます。

2.4. 失効確認を有効化

App Gateway はOCSPによる失効確認がサポートされています。

※失効リスト (CRL) による失効確認はサポートされていません。

App GatewayのSSLプロファイルを設定し、OCSPによる失効確認を有効化します。

※本操作は、Azure PowerShell を用いて行います。

- **Azure にサインイン**

```
  Connect-AzAccount `
    -Subscription  【サブスクリプション ID】
```

- **App Gateway のSSLプロファイルを取得**

```
$AppGw = Get-AzApplicationGateway `
  -Name 【本書 2.2 で作成した App Gateway のゲートウェイ名】 `
  -ResourceGroupName 【リソースグループ名】

$profile = Get-AzApplicationGatewaySslProfile `
  -Name 【本書 2.3 で作成した SSL プロファイル名】 `
  -ApplicationGateway $AppGw
```

- **OCSPで失効状態を確認するようにSSLプロファイル設定**

```
Set-AzApplicationGatewayClientAuthConfiguration `
  -SslProfile $profile `
  -VerifyClientRevocation OCSP
```

- **App Gatewayに SSLプロファイルを反映**

```
Set-AzApplicationGateway `
  -ApplicationGateway $AppGw
```

以上でApp GatewayがOCSPによる失効確認が行われるようになります。

※失効確認が有効な場合、クライアント証明書には機関情報アクセス(AIA)拡張にOCSPレスポンダURLが記載されている必要があります。

※App Gatewayは、OCSP応答のnextUpdate時刻に基づいてOCSP応答をキャッシュし、このOCSPキャッシュを介して失効確認を行う仕様となっています。

2.5. 書き換えセットの登録

App Gatewayが検証したクライアント証明書情報をアプリケーションサーバへ送信することでアプリケーションがクライアント証明書のチェックを行うことができます。

App Gateway に書き換えセットを登録し、アプリケーションサーバへのリクエストヘッダにクライアント証明書を追加します。

Azure 管理コンソールのメニューから [Application gateways]を選択し、一覧から対象の App Gateway を選びます。

メニュー[書き換え]を開き、[+書き換えセット]をクリックします。

次の画面で以下を設定します。

書き換えセットの作成

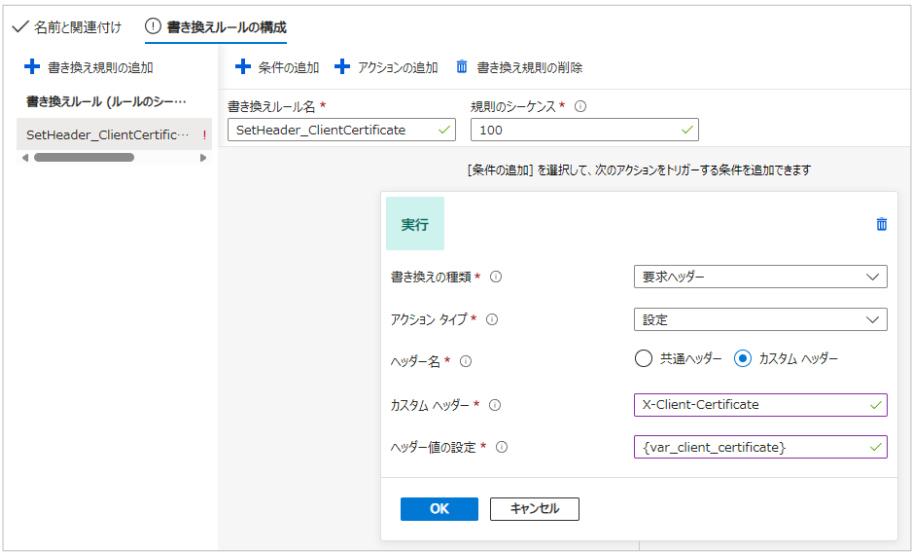
[名前と関連付け]タブ

- 名前に任意の名前を入力
- App Gateway に関連付けられているルーティング規則をチェック

- [次へ]をクリック

[書き換えルールの構成]タブ

- **[+書き換え規則の追加]をクリック**
- **書き換えルール名に任意の名前を入力**
- **規則のシーケンスに 100 を入力**
  ※書き換えルールを実行する
- **[クリックしてこのアクションを構成]をクリックして入力フォームを開く**
  - **書き換えの種類に[要求ヘッダー]を選択**
  - **アクションタイプに[設定]を選択**
  - **ヘッダー名に[カスタムヘッダーを選択**
  - **カスタムヘッダー名 に任意のリクエストヘッダ名を入力**
  - **ヘッダー値の設定 にクライアント証明書情報を表す識別子を入力**



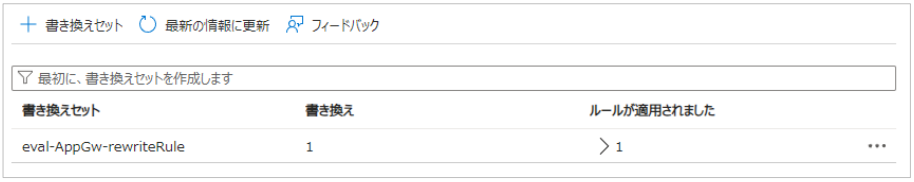
- **[アクションの追加]をクリックしてリクエストヘッダの設定を追加を繰り返す**

カスタムヘッダー名とヘッダー値は、以下のように指定可能

※カスタムヘッダー名には任意の名前で指定

カスタムヘッダー名(例)	ヘッダー値の設定	意味
X-Client-Certificate	{var_client_certificate}	証明書（PEM 形式）
X-Client-Certificate-Issuer	{var_client_certificate_issuer}	証明書の発行元
X-Client-Certificate-Subject	{var_client_certificate_subject}	証明書サブジェクト
X-Client-Certificate-Serial	{var_client_certificate_serial}	証明書シリアル
X-Client-Certificate-Start-Date	{var_client_certificate_start_date}	証明書の開始日
X-Client-Certificate-End-Date	{var_client_certificate_end_date}	証明書の終了日
X-Client-Certificate-Fingerprint	{var_client_certificate_fingerprint}	証明書フィンガープリント

- **[作成]をクリックして書き換えセットを作成**



2.6. DNS登録

FQDNでApp Gatewayを参照できるようにDNS登録します。

DNSにAレコードを登録し、App Gatewayを名前解決できるようにします。

App Gateway に割当てられているパブリックIPアドレスを確認し、DNSに登録します。

Azure 管理コンソールのメニューから [Application gateways]を選択し、一覧から対象の App Gateway を選びます。

- メニュー[フロントエンド IP 構成]を選択

パブリックIPアドレスが確認できるので、このアドレスをDNSに登録します。

以上でAzure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。

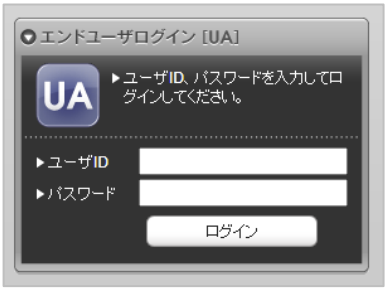
4. クライアントの設定 (Windows)

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。

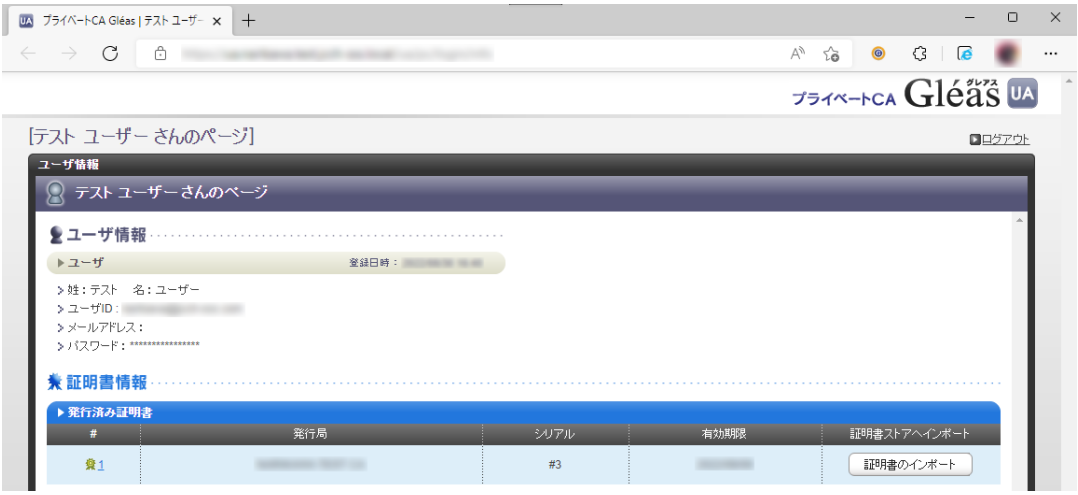
※URL https://[UA の FQDN]/[UA の名前]/ua

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。

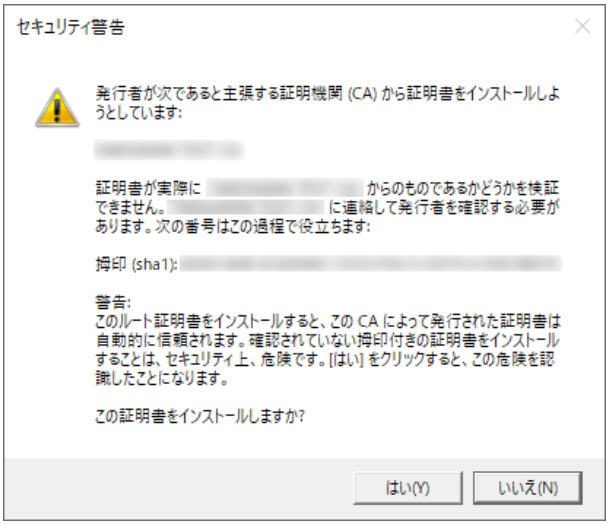


ログインすると、ユーザ専用ページが表示されます。

[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。



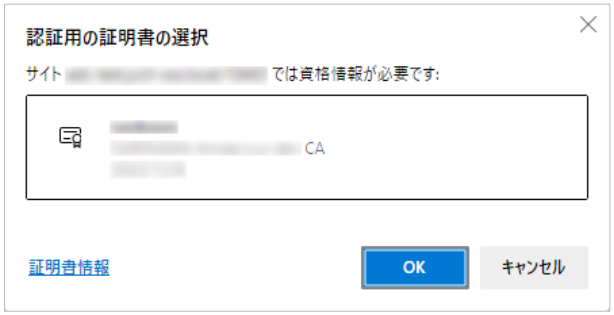
※証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印を確認するなど正当性を確認してから[はい]をクリックします



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。

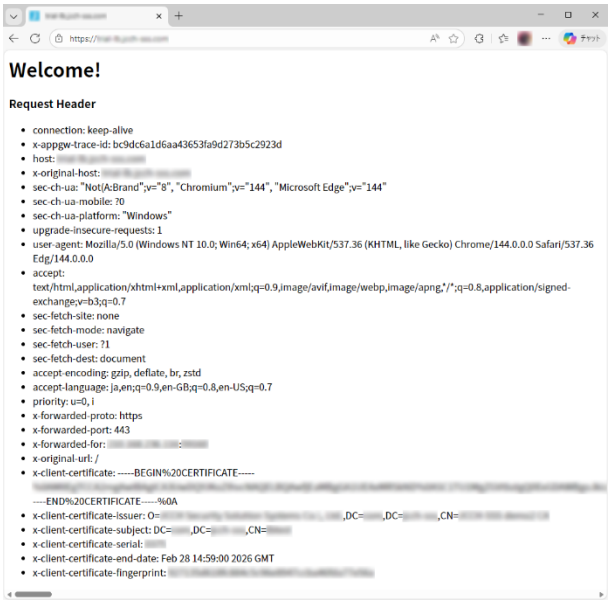
4.2. App Gatewayにアクセス

PCのブラウザ（Edge）でApp Gateway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。



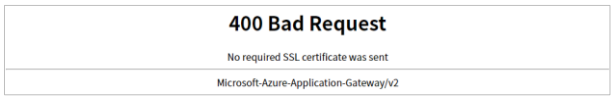
[OK]ボタンをクリックし、クライアント証明書認証がおこなわれるとページが表示されます。

※以下は本書 7 章のサーバにアクセスしている例



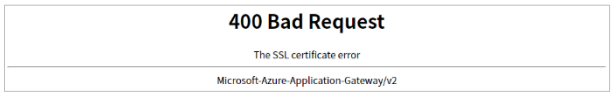
証明書を持っていない場合、アクセスに失敗します。

※以下はクライアント証明書を提示せずにアクセスした例



失効された証明書を提示した場合も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を使用してアクセスした例



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。

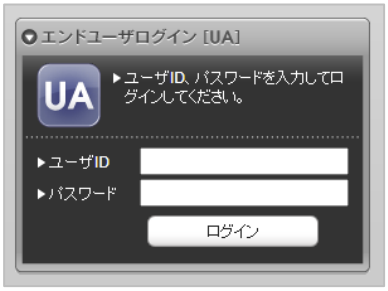
6. クライアントの設定（iPhone)

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。

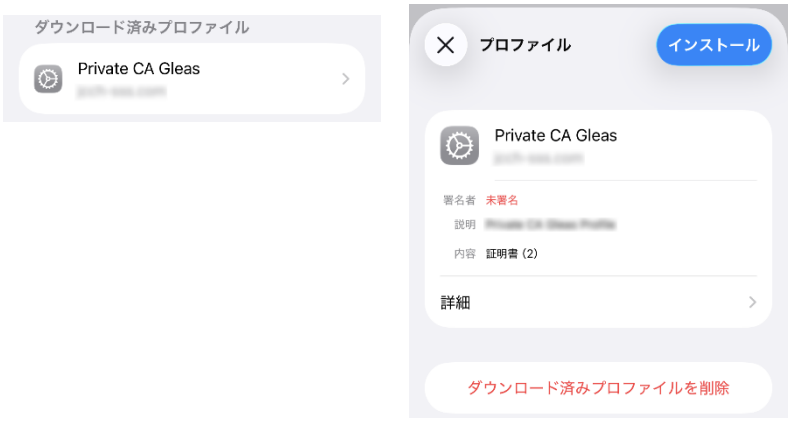


ログインすると、ユーザ専用ページが表示されます。

[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

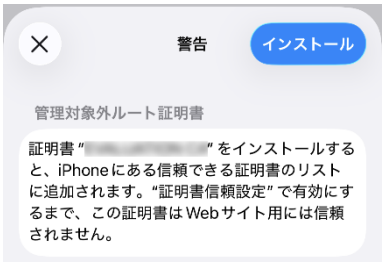
画面の表示にしたがい設定アプリから [一般] > [VPNとデバイス管理] を開き、ダウンロード済みのプロファイルが表示されるので、インストールをおこないます。



[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。

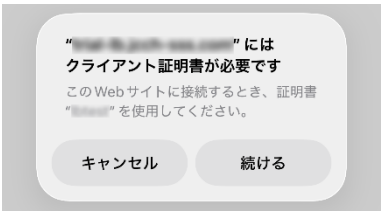
Safariに戻り、[ログアウト]をタップしてUAからログアウトします。

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. App Gatewayにアクセス

iPhoneのブラウザ（Safari）でApp Gateway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。

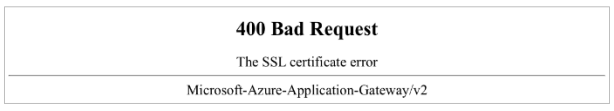
※以下は本書 7 章のサーバにアクセスしている例

証明書を持っていない場合、アクセスに失敗します。

※以下はクライアント証明書を提示せずにアクセスした例

失効された証明書を提示した場合も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を使用してアクセスした例



7. サーバでクライアント証明書情報を取得

App Gateway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 80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

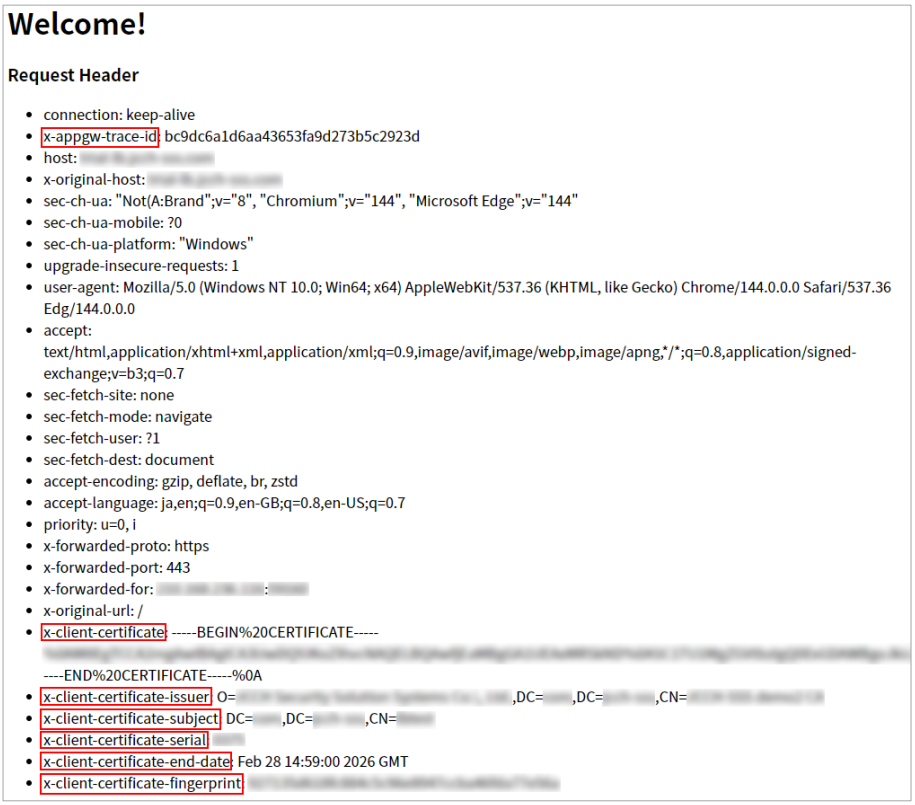
```
tee /usr/local/src/demo_app.js << 'EOS'
"use strict";
const http = require("http");
const listen_port = 80;
const server = http.createServer((request, response) => {
  var headers = "";
  Object.keys(request.headers).forEach((key) => {
    headers = headers + `<li>${key}: ${request.headers[key]}</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 App Gateway 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-AppGw-Trace-Id	App Gateway がリクエスト毎に生成する一意の GUID
X-Client-Certificate	クライアント証明書(PEM 形式)
X-Client-Certificate-Issuer	クライアント証明書の発行者
X-Client-Certificate-Subject	クライアント証明書サブジェクト
X-Client-Certificate-Serial	クライアント証明書シリアル
X-Client-Certificate-End-Date	クライアント証明書有効期限
X-Client-Certificate-Fingerprint	クライアント証明書フィンガープリント

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