



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

Citrix ADC でのクライアント証明書認証

Ver.1.0

2023年03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. 証明書発行時における留意事項	9
2. Citrix ADC の設定	10
2.1. ルート証明書の登録	10
2.2. サーバ証明書の発行と登録	12
2.3. 失効リスト (CRL) の登録	19
2.4. SSL プロファイルの登録	22
2.5. バーチャルサーバの設定	24
2.6. リクエストヘッダにクライアント証明書情報を挿入	27
3. Gléas の管理者設定 (Windows 向け)	32
4. クライアントの設定 (Windows)	34
4.1. クライアント証明書のインポート	34
4.2. サーバアクセス	36

5. Gléas の管理者設定 (iPhone 向け)	38
6. クライアントの設定 (iPhone)	41
6.1. クライアント証明書のインポート	41
6.2. サーバアクセス	44
7. Web サーバでクライアント証明書情報を取得	46
8. 問い合わせ	48

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、シトリックス・システムズ・ジャパン株式会社の Citrix ADC で SSLオフロードしたロードバランシング (Web負荷分散) 構成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。

➤ SSLロードバランサー

Citrix ADC VPX Express (NS13.1: Build 37.38.nc)

※以後、「Citrix ADC」と記載します

➤ 認証局 : JS3 プライベートCA Gléas (バージョン2.5.1)

※以後、「Gléas」と記載します

➤ Webサーバ : CentOS7.5.1804 / Apache 2.4.6

※以後、「Webサーバ」と記載します

➤ クライアント : Windows10 Pro 22H2 / Microsoft Edge 108.0.1462.46

※以後、「Windows」と記載します

➤ クライアント : iPhone8 (iOS 15.3.1) / Safari

※以後、「iPhone」と記載します

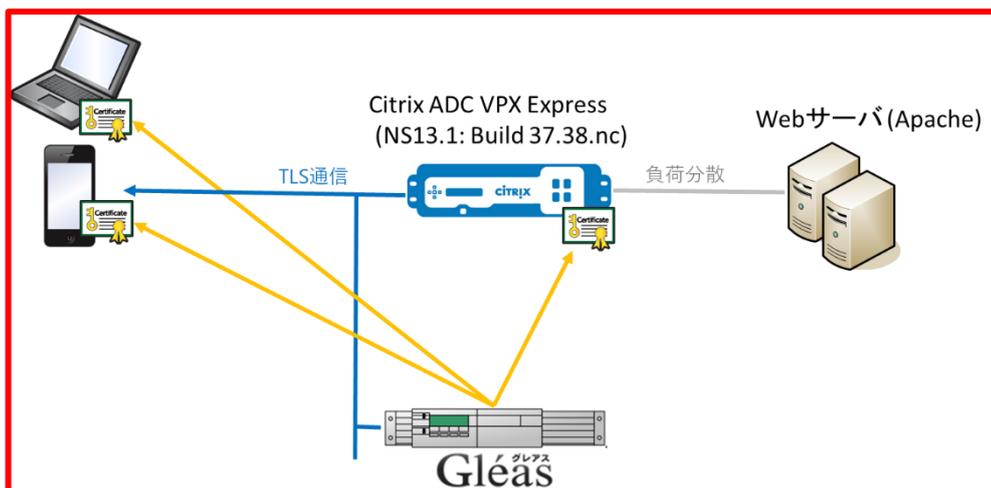
以下については、本書では説明を割愛します。

- Citrix ADC の基本設定 (ネットワークや基本的な負荷分散に関する設定)
- Webサーバの基本設定 (ネットワークや基本的なWebページ公開設定)
- Gléasでのユーザ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。



1. Gléasでは、Citrix ADCにサーバ証明書を、PCとiPhoneにクライアント証明書を発行する。
2. PCとiPhoneはGléasより証明書をインポートする。
3. PCではEdgeブラウザ、iPhoneではSafariブラウザよりCitrix ADCのバーチャルサーバにアクセスし、Citrix ADCはクライアント証明書認証をおこなう。

証明書認証後にロードバランスしているWebページをクライアントに表示。

証明書を提示しない、期限切れ、または失効している、端末はクライアント証明書認証に失敗。

1.4. 証明書発行時における留意事項

Gléasで電子証明書を発行する際に以下の点に留意する必要があります。

- 本書2.2の方法でサーバ証明書を発行する場合は、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。
- Citrix ADC は、以下の基本機能が有効になっている必要があります。
 - SSL Offloading
 - Load Balancing
 - Rewrite

2. Citrix ADC の設定

2.1. ルート証明書の登録

クライアント証明書によるSSL認証を利用するためには、ルート証明書の登録が必要です。これは、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際に利用するためです。

本手順の前にGléasより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`

Citrix ADC の管理画面にログインし、[Configuration]タブを選択、左ペインから [Traffic Management] > [SSL] > [Certificates] > [CA Certificates] と進み、右ペインより [Install] ボタン をクリックします。

次の画面で 以下を設定します。

- [Certificate Key Pair Name]には、任意の識別名称を入力
- [Certificate File Name]には、[Choose File]ボタンをドロップダウンして [Local] を選択、Gléas よりダウンロードしたファイルを選択しアップロード

プライベート CA Gléas ホワイトペーパー
Citrix ADC でのクライアント証明書認証

← Install CA Certificate

Certificate-Key Pair Name*
gleasCA ⓘ

Certificate File Name*
Choose File ▼ ia1.pem ⓘ

Notify When Expires ⓘ

No SNMP Trap destination found. Notification will not be sent until a trap destination is configured.

Notification Period
30

Install Close

入力後、[Install]ボタンをクリックするとルート証明書が追加されます。

CA Certificates 2

Install Update Delete No action ▼

Q Certificate Type: ROOT_CERT|INTM_CERT Click here to search or you can enter Key : Value format ⓘ

<input type="checkbox"/>	NAME	CERTIFICATE TYPE	COMMON NAME	ISSUER NAME	DAYS TO EXPIRE	STATUS	LINK STATUS
<input type="checkbox"/>						Valid	
<input type="checkbox"/>	gleasCA	ROOT_CERT				Valid	

Total 2 25 Per Page Page 1 of 1

2.2. サーバ証明書の発行と登録

バーチャルサーバで使用するサーバ証明書をGléasから発行し、Citrix ADC に登録します。

Citrix ADCの管理画面の[Configuration]タブを選択、左ペインから [Traffic Management] > [SSL] と進み、右ペインから [Server Certificate Wizard] をクリックします。

その画面で以下を入力し、鍵ペアを生成します。

※右図は、AES256で暗号化されたPEMフォーマットの2048bitのRSA秘密鍵を生成する例。

- [Key Filename]には、Citrix ADC内に保存するファイル名を入力
- [PEM Passphrase] および [Confirm PEM Passphrase]に任意のパスワードを入力
- 他の項目は、環境に応じて設定

入力後、[Create]ボタンをクリックします。

The screenshot shows a 'Create Key' dialog box with the following fields and options:

- Algorithm: RSA, ECDSA
- Key Filename*: Choose File (dropdown), adc-testjcch-sss.local.key
- Key Size(bits)*: 2048 (dropdown)
- Public Exponent Value*: F4 (dropdown)
- Key Format*: PEM (dropdown)
- PEM Encoding Algorithm: AES256 (dropdown)
- PEM Passphrase*: [masked]
- Confirm PEM Passphrase*: [masked]
- PKCS8

Buttons: Create, Cancel

続いてCSRを作成します。

- [Key Filename]には、Citrix ADC内に保存するファイル名を入力
- [PEM Passphrase (For Encrypted Key)]には、先に入力したパスフレーズを入力
- [Subject Alternative Name]には、公開するバーチャルサーバのFQDNを入力
- [Common Name]には、Gléas のサーバアカウント名を入力
- 他の項目は、環境に応じて設定

2 Create Certificate Signing Request (CSR)

Request File Name*
Choose File | adc-test.jcch-sss.local.csr

Key Filename*
Choose File | adc-test.jcch-sss.local.key

Key Format*
PEM

PEM Passphrase (For Encrypted Key)
.....

Digest Method*
SHA256

Subject Alternative Name
adc-test.jcch-sss.local

Distinguished Name Fields

Country*
JAPAN

State or Province*
Tokyo

Organization Name*
JCCH Security Solution Systems

City

Email Address

Organization Unit

Common Name*
adc-test.jcch-sss.local

Attribute Fields

Challenge Password

Company Name

Create Cancel

入力後、[Create]ボタンをクリックします。

Confirm

Do you want to download the created CSR file adc-test.jcch-sss.local.csr?

Yes No

確認ダイアログで [Yes]をクリックすると、CSRファイルがダウンロードされます。

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、ホスト名に公開するバーチャルサーバの FQDN を
入力します。

小メニューの[証明書発行]をクリックします。



上級者向け設定を展開し、以下の操作をおこないます。

- 証明書要求 (CSR) ファイルをアップロードする : の[参照...]ボタンよりダウンロードした CSR ファイルを選択
 - [CSR ファイルの内容を確認する]にチェック
- その後、[発行]ボタンをクリックします。

プライベート CA Gléas ホワイトペーパー Citrix ADC でのクライアント証明書認証



証明書の要求内容が表示されるので確認し、**[この内容で発行する]**をクリックし、証明書の発行をおこないます。



証明書発行完了後、証明書詳細画面の証明書ファイル欄の「証明書：あり」をクリックし、発行された証明書をダウンロードします。

プライベート CA Gléas ホワイトペーパー
Citrix ADC でのクライアント証明書認証

The screenshot displays the Gléas RA web interface for a private CA. The main content area shows details for a certificate issued by 'JCCH-SSS demo CA#156' to the subject 'ns.js3.test.xen.local'. The interface is organized into several sections:

- 証明書情報 (Certificate Information):** Displays the subject 'ns.js3.test.xen.local' and the start/end dates: '開始日: 2016/10/24 17:27' and '終了日: 2019/10/24 17:27'.
- サブジェクト (Subject):** Lists attributes: 国: JP, 都道府県: Tokyo, 組織: JS3, 一般名: ns.js3-test-xen.local.
- 基本情報 (Basic Information):** Lists: 作成日: 2016/10/24 17:26, 有効日数: 1095, 失効日: (blank), 失効理由: (blank), 期限終了日: (blank), 状態: 有効な証明書, 処理の状態: 有効な証明書, トークン必要: (blank), バージョン: 4.
- 証明書情報 (Certificate Details):** Lists: 認証局: JCCH-SSS demo CA, 暗号アルゴリズム: rsa, タイグエストアルゴリズム: sha256, 鍵長: 2048, 鍵用途: 電子署名 鍵の暗号化, 拡張鍵用途: SSLサーバ認証 SSLクライアント認証, 別名: DNS名 ns.js3-test-xen.local.
- 証明書ファイル (Certificate File):** Lists: 証明書要求: あり, 作成日時: 2016/10/24 17:26, 証明書: あり, 作成日時: 2016/10/24 17:28, 秘密鍵: なし.

The interface includes a left sidebar with navigation options like 'アカウント', 'グループ', '証明書', '認証デバイス', and 'テンプレート'. The top right shows the user is logged in as 'サイドバー' and provides links for 'ログアウト' and 'ヘルプ'. The bottom of the page contains the text '著作権 © 2010-2016 JCCH Security Solution Systems Co., Ltd. All rights reserved.'

Citrix ADC の管理画面に戻り、右ペインの「4 Install Certificate」を開きます。

※Gléas で証明書を発行するため「3 Certificate」はスキップします。

次の画面で 以下を設定します。

- [Certificate Key Pair Name] には、任意の識別名称を入力
- [Certificate File Name] の [Browse] ボタンをドロップダウンして [Local] を選択、Gléas よりダウンロードした証明書ファイルを選択しアップロード
- [Key File Name] には、鍵ペアの生成で作成した Citrix ADCのファイルシステムに保存されたファイルを選択
- [Password] には、鍵ペアの生成時に指定した秘密鍵のパスワードを指定した場合に入力

4 Install Certificate

Certificate-Key Pair Name*
adc-test-jcch-sss.local.crt ⓘ

Certificate File Name*
Choose File ▾ download.crt ⓘ

Key File Name
Choose File ▾ adc-test-jcch-sss.local.key ⓘ

Password*
..... ⓘ

Notify When Expires

No SNMP Trap destination found. Notification will not be sent until a trap destination is configured.

Notification Period
30

Create Cancel

Done

入力後、[Create]ボタンをクリックするとサーバ証明書が追加されます。

プライベート CA Gléas ホワイトペーパー
Citrix ADC でのクライアント証明書認証

[Done]ボタンをクリックして Server Certificate Wizard を終了します。

SSL Certificate-Key pair adc-test_jcch-sss.local.crt installed successfully			
1 SSL RSA/DSA/ECDSA Keys			
Key Type RSA	Key Filename adc-test_jcch-sss.local.key	Key Size(bits) 2048	Key Format PEM
2 SSL Certificate			
Request File Name adc-test_jcch-sss.local.csr	Country JAPAN	State or Province Tokyo	Organization Name JCCH Security Solution Systems
3 Certificate			
4 SSL Install Certificate			
Certificate-Key Pair Name adc-test_jcch-sss.local.crt		Certificate File Name download.crt	

Done

2.3. 失効リスト (CRL) の登録

クライアント証明書によるSSL認証を利用するためには、失効リストの登録が必要です。

これは、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際に利用するためです。

本手順の前にGléasより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CRLのダウンロードURLは以下となります。

`http://[GléasのFQDN]/crl/ia1.crl`

Citrix ADC の管理画面の[Configuration]タブを選択、左ペインから [Traffic

Management] > [SSL] > [CRL] と進み、右ペインより[Add]ボタンをクリックします。

次の画面で以下を設定します。

※右図は毎日 0 時 10 分に CRL を自動更新する設定例

- [CRL]には、任意の名称を入力
- [CRL File]には、Choose File ボタンをドロップダウンして Local を選択、Gléas よりダウンロードした CRL ファイルを選択しアップロード
- [Inform]は、[DER]を選択
- [CA Certificate]は、2.1 で作成したルート CA 名を選択
- [Enable CRL Auto Refresh]をチェック

CRL Name*
gleasCRL ⓘ

CRL File*
Choose File ▼ ia1.crl ⓘ

Inform
 PEM DER

CA Certificate
gleasCA ▼ ⓘ

Enable CRL Auto Refresh ⓘ

CRL Auto Refresh Parameter

Method*
HTTP ▼

Scope*
One

Server IP
ⓘ

Port*
80 ⓘ

URL
http://.../cr/ia1.crl ⓘ

Base DN*
ⓘ

Bind DN
ⓘ

Password
ⓘ

Interval
Daily ▼ ⓘ

Day(s)
ⓘ

Time (HH:MM)*
00 10 ⓘ

Binary

Create Close

[CRL Auto Refresh Parameter]が追加表示されるので、以下を設定

- [Method]は、http を選択
- [Port]は、80 を入力
- [URL]は、上記の Gléas の CRL ダウンロード URL を入力
- [Interval] と [Time] は、CRL の更新間隔を設定

入力後、[Create]ボタンをクリックします。

プライベート CA Gléas ホワイトペーパー
Citrix ADC でのクライアント証明書認証

以下のように設定された CRL が表示されます。

CRL 2  

[Add](#) [Edit](#) [Delete](#) [Details](#)

🔍 Click here to search or you can enter Key : Value format ⓘ

<input type="checkbox"/>	NAME	CRL PATH	FORMAT	CRL AUTO REFRESH	REFRESH STATUS	VALIDITY STATUS	DAYS TO EXPIRE
<input type="checkbox"/>							
<input type="checkbox"/>	gleasCRL	ia1.crl	DER	ENABLED	Successful	Valid	29

Total 2 25 Per Page Page 1 of 1

2.4. SSLプロファイルの登録

バーチャルサーバのSSLでクライアント証明書認証を行うためのSSLプロファイルを作成します。

Citrix ADC の管理画面の[Configuration]タブを選択、左ペインから [System] > [Profiles]と進み、右ペインの[SSL Profile]タブを選択、[Add]ボタン をクリックします。

次の画面で以下を設定します。

- [Name]には、任意の識別名称を入力
- [Client Authentication]をチェックすると [Create Certificate]が表示されるので、[MANDATORY]を選択
- [Skip Client Certificate Policy Check] をチェック
- [Enable Client Authentication Using bound CA Chain] をチェック
- 他の項目は、環境に応じて設定

The screenshot displays the configuration interface for an SSL Profile in Citrix ADC. It is divided into two main sections: 'Basic Settings' and a list of options.

Basic Settings:

- Name*:** A text input field containing 'gleasClientCertAuth'.
- SSL Profile Type*:** A dropdown menu set to 'FrontEnd'.

Options:

- Enable Cipher Redirect
- Client Authentication ⓘ
- Client Certificate*:** A dropdown menu set to 'MANDATORY' ⓘ
- Skip Client Certificate Policy Check ⓘ
- OCSP Stapling
- SSL Redirect
- SNI Enable
- Send Close-Notify
- Non-FIPS Ciphers
- Strict CA checks
- Drop requests for SNI enabled SSL sessions if host header is absent
- Enable Client Authentication using bound CA Chain ⓘ

プライベート CA Gléas ホワイトペーパー
Citrix ADC でのクライアント証明書認証

入力後に、[OK]ボタンをクリックするとSSLプロファイルが追加されます。

Basic Settings	
Name	gleasClientCertAuth
SSL Profile Type	FrontEnd
PUSH Encryption Trigger	Always
Encryption trigger packet count	45
Push Flag	Auto (PUSH flag is not set)
PUSH encryption trigger timeout (ms)	1
Encryption trigger timeout (10 ms ticks)	100
Encoding type	Unicode
Deny SSL Renegotiation	ALL
ALPN Protocol	NONE
SSL quantum size (KBytes)	8192
Clear Text Port	0
DH Param	DISABLED
DH Key Expire Size Limit	DISABLED
Ephemeral RSA	ENABLED
Refresh Count	0
SSL Log Profile	-
Strict Signature Digest Check	DISABLED
HSTS	DISABLED
Max Age	0
Include Subdomains	NO
SNI HTTP Host Match	CERT
Preload	NO
SSL Sessions Interception	DISABLED
Verify Server Certificate For Reuse On SSL Interception	ENABLED
SSL Interception Client Renegotiation	ENABLED
SSL Interception OCSP Check	ENABLED
Maximum SSL Sessions Per Server On SSL Interception	10
TLS13 Session Tickets Per Authcontext	1
Session Reuse	ENABLED
Session Timeout	120
Cipher Redirect	DISABLED
Client Authentication	ENABLED
Client Certificate	Mandatory
OCSP Stapling	DISABLED
SSL Redirect	DISABLED
SNI Enable	DISABLED
Send Close-Notify	YES
Non-FIPS Ciphers	DISABLED
Strict CA checks	NO
Drop requests for SNI enabled SSL sessions	NO
Enable Client Authentication using bound CA Chain	ENABLED
Session Ticket	DISABLED
Session Ticket Life Time (secs)	300
Session Key Auto Refresh	ENABLED
Session Key Lifetime (secs)	3000
Previous Session Key Lifetime (secs)	0
SSLv3	DISABLED
TLSv1	ENABLED
TLSv11	ENABLED
TLSv12	ENABLED
TLSv13	DISABLED
Zero RTT Early Data	DISABLED
DHE Key Exchange with PSK	NO
Allow Extended Master Secret	NO
Skip Client Certificate Policy Check	ENABLED

Done

2.5. バーチャルサーバの設定

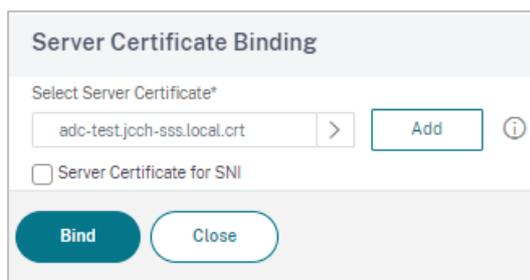
バーチャルサーバにSSLプロファイルをバインドしてクライアント証明書認証を行うように設定します。

本手順の前にSSLプロトコルのバーチャルサーバを作成し、サービスをバインドして構成しておきます。

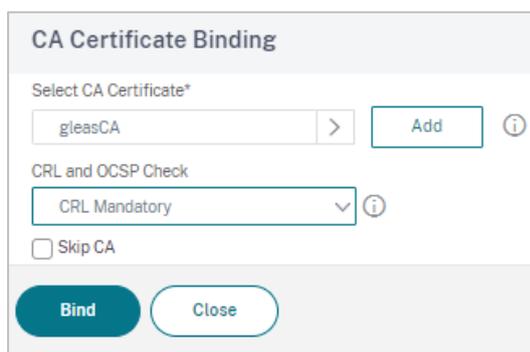
Citrix ADC の管理画面の [Configuration] タブを選択、左ペインから [Traffic Management] > [Load Balancing] > [Virtual Servers] 進み、右ペインよりクライアント証明書認証を追加するバーチャルサーバをチェックして、[Edit] ボタンをクリックします。

次の画面で以下を設定します。

- Certificates 欄の[No Server Certificate]をクリックし、2.2 項で設定したサーバ証明書を設定

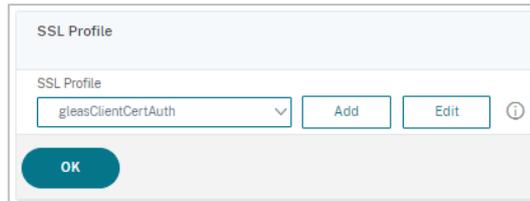


- [Bind]ボタンをクリックして、バーチャルサーバにサーバ証明書をバインド
- Certificates 欄の[No CA Certificate]をクリックし、2.1 項で設定したルート証明書を設定
- CRL and OCSP Check は[CRL Mandatory]を選択



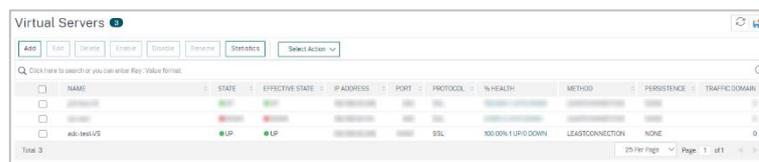
- Bind をクリックして、バーチャルサーバに CA 証明書、CRL をバインド

- 右ペインの Advanced Settings 欄の[SSL Profile]の[+]をクリックし証明書認証を追加します。
- 2.4 項で作成した SSL プロファイルを設定

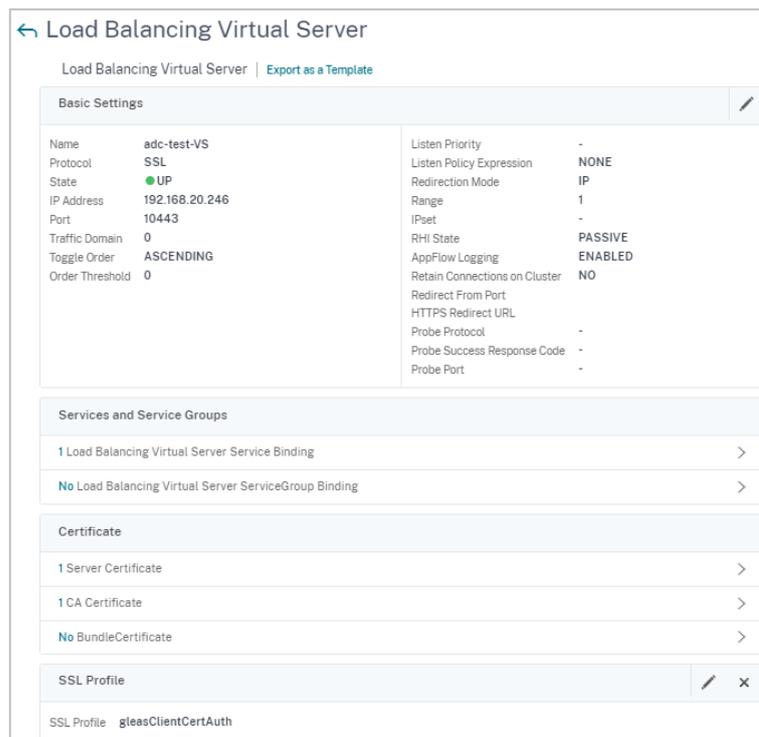


- OK をクリックして、バーチャルサーバに SSL プロファイルをバインド

設定終了後、[Done]をクリックしてバーチャルサーバに反映させます。



NAME	STATE	EFFECTIVE STATE	IP ADDRESS	PORT	PROTOCOL	% HEALTH	METHOD	PERSISTENCE	TRAFFIC DOMAIN
adc-test-VS	UP	UP			SSL	100.00% UP/DOWN	LEASTCONNECTION	NONE	



Load Balancing Virtual Server | Export as a Template

Basic Settings

Name	adc-test-VS	Listen Priority	-
Protocol	SSL	Listen Policy Expression	NONE
State	UP	Redirection Mode	IP
IP Address	192.168.20.246	Range	1
Port	10443	IPset	-
Traffic Domain	0	RHI State	PASSIVE
Toggle Order	ASCENDING	AppFlow Logging	ENABLED
Order Threshold	0	Retain Connections on Cluster	NO
		Redirect From Port	
		HTTPS Redirect URL	
		Probe Protocol	-
		Probe Success Response Code	-
		Probe Port	-

Services and Service Groups

- 1 Load Balancing Virtual Server Service Binding >
- No Load Balancing Virtual Server ServiceGroup Binding >

Certificate

- 1 Server Certificate >
- 1 CA Certificate >
- No BundleCertificate >

SSL Profile

SSL Profile: gleasClientCertAuth

2.6. リクエストヘッダにクライアント証明書情報を挿入

バーチャルサーバでSSLオフロードした場合、ロードバランスしているサーバはクライアント証明書の情報を受け取ることができないため、Citrix ADC の Rewrite 機能を使ってリクエストヘッダを書き換え、サーバにクライアント証明書の情報を送信するように設定します。

まず、Rewriteアクションを設定します。

Citrix ADCの管理画面の[Configuration]タブを選択、左ペインから [AppExpert] > [Rewrite] > [Actions] と進み、右ペインより[Add]ボタンをクリックします。

次の画面で以下を設定します。

- [Name] には、任意の識別名を設定
- [Type] には、[INSERT_HTTP_HEADER]を設定
- [Header Name]には、サーバに送信する任意のヘッダ名を設定
※ここでは、X-client-cert-cn とする
- [Expression]には、送信する証明書情報を設定
※ここでは、証明書のサブジェクト一般名(CN)を送信するように以下とする
CLIENT.SSL.CLIENT_CERT.SUBJECT.VALUE("CN")

プライベート CA Gléas ホワイトペーパー
Citrix ADC でのクライアント証明書認証

← Create Rewrite Action

Name*
sendCertCnRewriteAction ⓘ

Type*
INSERT_HTTP_HEADER ⓘ

Use this action type to insert a header.

Header Name*
X-client-cert-cn

Expression [Expression Editor](#)
Select Select Select ⓘ
CLIENTSSLCLIENT_CERTSUBJECTVALUE("CN") ⓘ
[Evaluate](#)

In string expressions, string constants and expressions can be concatenated with "*" operator. Please make sure that string constants are enclosed in double quotes.

Comments

[Create](#) [Close](#)

入力後に、[Create] ボタンをクリックすると[Rewrite]アクションが追加されます。

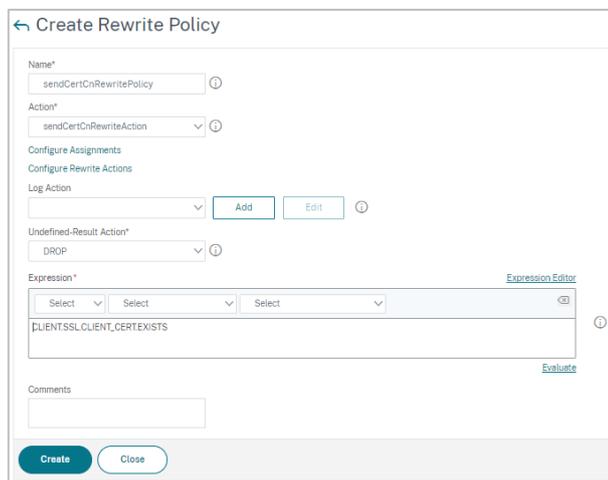
次に、Rewriteポリシーを設定します。

Citrix ADCの管理画面の[Configuration]タブを選択、左ペインから [AppExpert] > [Rewrite] > [Policy] と進み、右ペインより Add ボタン をクリックします。

次の画面で以下を設定します。

- [Name] には、任意の識別名を設定
- [Action] には、先に登録した Rewrite アクションを選択
- [Undefined-Result Action] に[DROP]を選択
- [Expression] には、Rewrite ポリシーが動作する条件を設定

※ここでは、クライアント証明書が存在した場合に動作するように以下とする
CLIENT.SSL.CLIENT_CERT.EXISTS



The screenshot shows the 'Create Rewrite Policy' dialog box. It has the following fields and controls:

- Name***: Input field containing 'sendCertCnRewritePolicy'.
- Action***: Dropdown menu containing 'sendCertCnRewriteAction'.
- Configure Assignments**: Section header.
- Configure Rewrite Actions**: Section header.
- Log Action**: Dropdown menu with 'Add' and 'Edit' buttons.
- Undefined-Result Action***: Dropdown menu containing 'DROP'.
- Expression***: Input field containing 'CLIENT.SSL.CLIENT_CERT.EXISTS'. There is an 'Expression Editor' link and an 'Evaluate' button.
- Comments**: Text area.
- Buttons**: 'Create' and 'Close' buttons at the bottom.

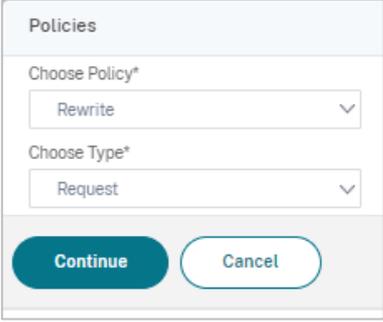
入力後に、[Create]ボタンをクリックするとRewriteアクションが追加されます。

次にRewriteポリシーをバーチャルサーバにバインドします。

Citrix ADC の管理画面の [Configuration] タブを選択、左ペインから [Traffic Management] > [Load Balancing] > [Virtual Servers] 進み、右ペインより クライアント証明書認証を追加するバーチャルサーバをチェックして、[Edit] ボタンをクリックします。

次の画面で以下を設定します。

- Advanced Settings 欄の[Policies]の[+]をクリック
- [Choose Policy]には、[Rewrite]を選択
- [Choose Type]には、[Request]を選択



The screenshot shows a dialog box titled "Policies". It contains two dropdown menus. The first is labeled "Choose Policy*" and has "Rewrite" selected. The second is labeled "Choose Type*" and has "Request" selected. At the bottom of the dialog, there are two buttons: "Continue" (which is highlighted in blue) and "Cancel".

- [Continue]ボタンをクリック
- [Select Policy] に作成した Rewrite ポリシーを選択

プライベート CA Gléas ホワイトペーパー
Citrix ADC でのクライアント証明書認証

The screenshot shows a 'Policy Binding' configuration window. At the top, there's a 'Select Policy*' field containing 'sendCertOnRewritePolicy', with 'Add', 'Edit', and 'Info' buttons to its right. Below this is a 'More' section with a downward arrow. The 'Binding Details' section contains three fields: 'Priority*' with the value '100', 'Goto Expression*' with a dropdown menu showing 'END', and 'Invoke LabelType*' with a dropdown menu showing 'None'. At the bottom of the window are two buttons: 'Bind' and 'Close'.

入力後、[Bind]をクリックして Rewrite ポリシーをバーチャルサーバにバインドさせます。

以上でサーバへのHTTPリクエストヘッダにクライアント証明書情報が挿入されるようにする設定が完了です。

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。

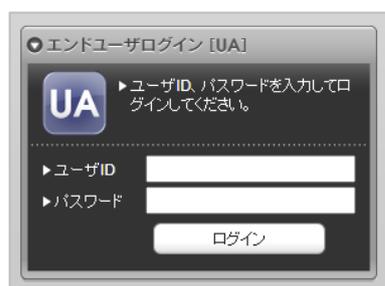
4. クライアントの設定 (Windows)

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。

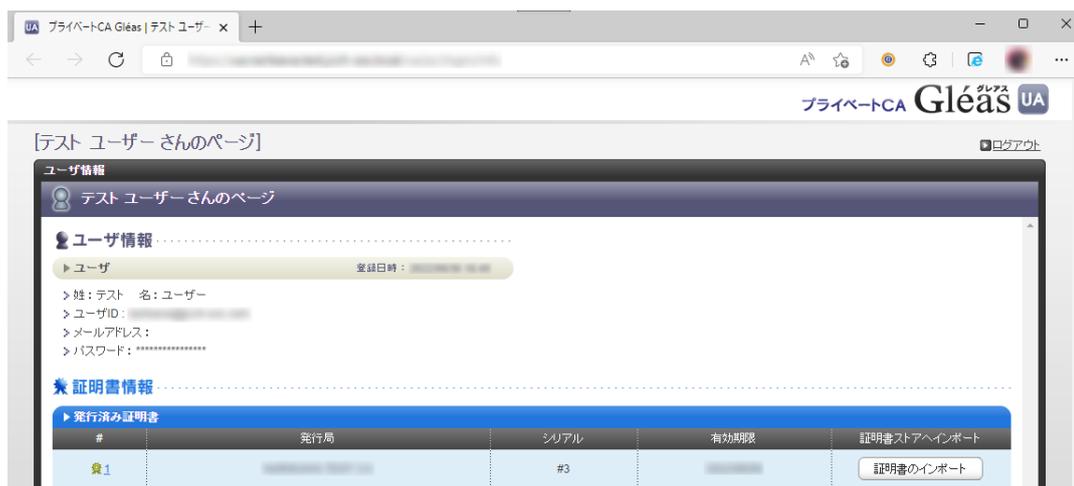
※URL https://[UA の FQDN]/[UA の名前]/ua

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。

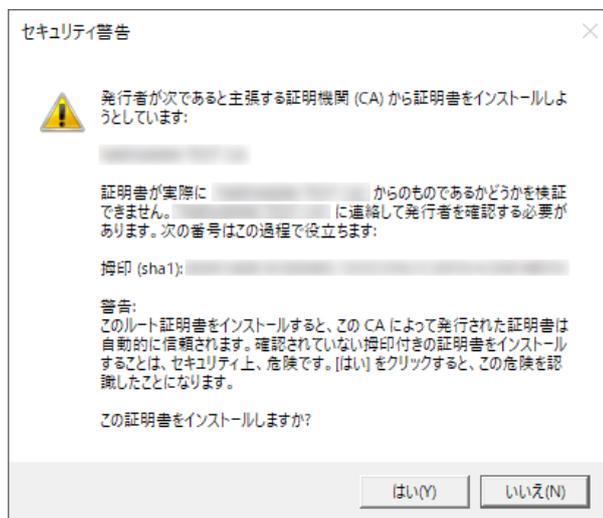


ログインすると、ユーザ専用ページが表示されます。

[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

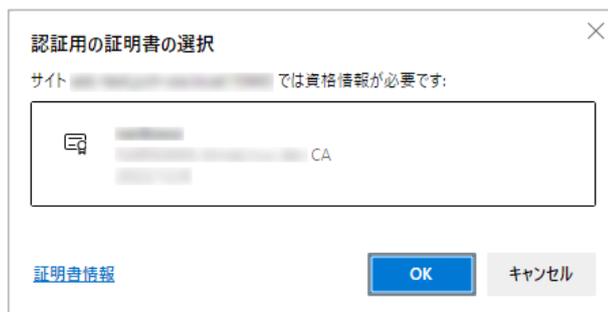


インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ログインしてインポートを行うことはできません。



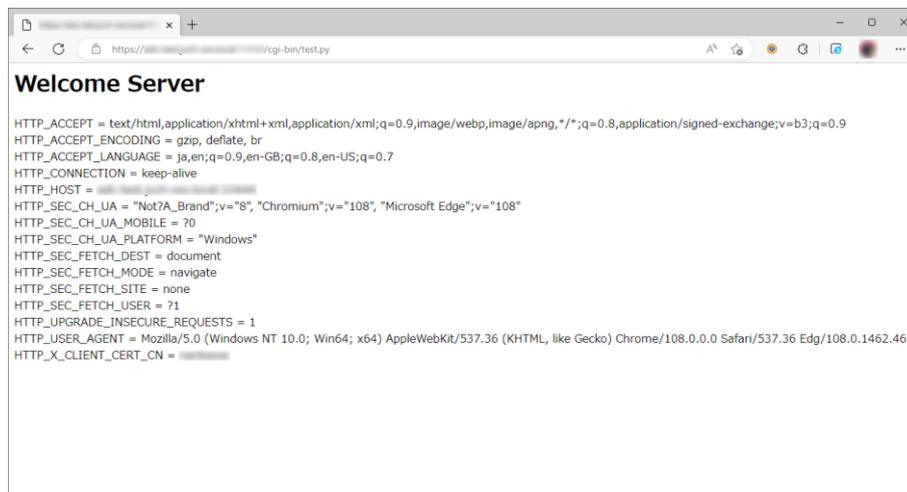
4.2. サーバアクセス

PCのブラウザ (Edge) でCitrix ADCのバーチャルサーバのURL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7項の CGI を実行する Web ページ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。

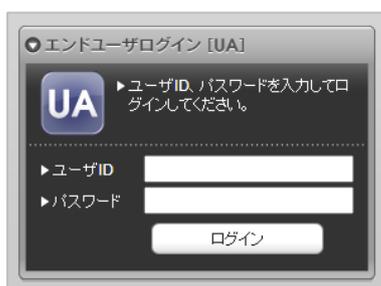
6. クライアントの設定 (iPhone)

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。



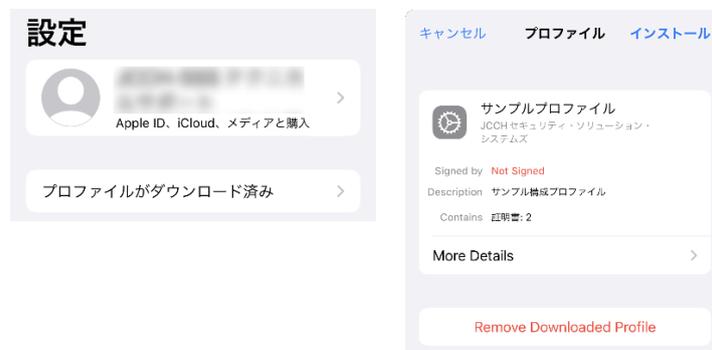
ログインすると、ユーザ専用ページが表示されます。

[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を開くと、プロフィールがダウンロードされた旨が表示されるので、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。

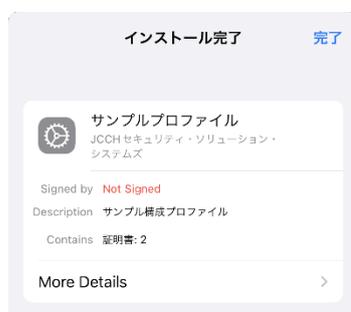
インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[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、[完了]をタップして終了します。



なお [More Details]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. サーバアクセス

iPhoneのブラウザ (Safari) でCitrix ADCのバーチャルサーバのURL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が自動的に提示されます。

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7項の CGI を実行する Web ページにアクセスしている例

```
Welcome Server
HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
HTTP_ACCEPT_ENCODING = gzip, deflate, br
HTTP_ACCEPT_LANGUAGE = ja
HTTP_CONNECTION = keep-alive
HTTP_HOST = ██████████
HTTP_USER_AGENT = Mozilla/5.0 (iPhone; CPU iPhone OS 15_3_1 like Mac OS X)
AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.3 Mobile/15E148 Safari/604.1
HTTP_X_CLIENT_CERT_CN = ██████████
```

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

ページを開けません。Safariはサーバにセキュリティ保護された接続を確立できませんでした。

プライベート CA Gléas ホワイトペーパー
Citrix ADC でのクライアント証明書認証

7. Web サーバでクライアント証明書情報を取得

Citrix ADC の ReWrite 機能によって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Webサーバが受信していることを確認します。

※以下は、Python で作成した CGI を Apache で公開する例

- http.conf に以下を追加

```
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options +ExecCGI
    Require all granted
    AddHandler cgi-script .py
</Directory>
```

- CGI を作成

```
vi /var/www/cgi-bin/test.py
chmod 755 /var/www/cgi-bin/test.py
```

※スクリプトの内容は以下。環境変数からリクエストヘッダを取得して出力

```
#!/usr/bin/env python

import os
print "Content-Type: text/html"
print "Cache-Control: no-cache"
print

print "<html><body>"
print "<h1>Welcome Server</h1>"

for headername, headervalue in sorted(os.environ.iteritems()):
    if headername.startswith("HTTP_"):
        print "{0} = {1}<br>".format(headername, headervalue)
print "</html></body>"
```

- Apache を再起動

```
systemctl restart httpd
```

Web ブラウザから CGI にアクセスすると、環境変数 HTTP_X_CLIENT_CERT_CN にクライアント証明書のサブジェクト一般名(CommonName)が取得でき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 Server

HTTP_ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
HTTP_ACCEPT_ENCODING = gzip, deflate, br
HTTP_ACCEPT_LANGUAGE = ja
HTTP_CONNECTION = keep-alive
HTTP_HOST = ██████████
HTTP_SEC_CH-UA = "Not?A_Brand";v="8", "Chromium";v="108", "Microsoft Edge";v="108"
HTTP_SEC_CH-UA_MOBILE = ?0
HTTP_SEC_CH-UA_PLATFORM = "Windows"
HTTP_SEC_FETCH_DEST = document
HTTP_SEC_FETCH_MODE = navigate
HTTP_SEC_FETCH_SITE = none
HTTP_SEC_FETCH_USER = ?1
HTTP_UPGRADE_INSECURE_REQUESTS = 1
HTTP_USER_AGENT = Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0 Safari/537.36 Edg/108.0.1462.46
HTTP_X_CLIENT_CERT_CN = ██████████
```

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