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

NetWiser でのクライアント証明書認証

Ver.1.0

2024 年 05 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、セイコーソリューションズ株式会社の NetWiser 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**

  Netwiser Virtual Edition SX-3990（v8.4.10)

  ※以後、「NetWiser」と記載します

- **認証局：JS3 プライベートCA Gléas（バージョン2.7.1)**

  ※以後、「Gléas」と記載します

- **Webサーバ：AlmaLinux release 9.2 / Apache 2.4.53**

  ※以後、「Webサーバ」と記載します

- **クライアント：Windows10 Pro 22H2 / Microsoft Edge 124.0.2478.9**

  ※以後、「Windows」と記載します

- **クライアント：iPhone14（iOS 16.3）/ Safari**

  ※以後、「iPhone」と記載します

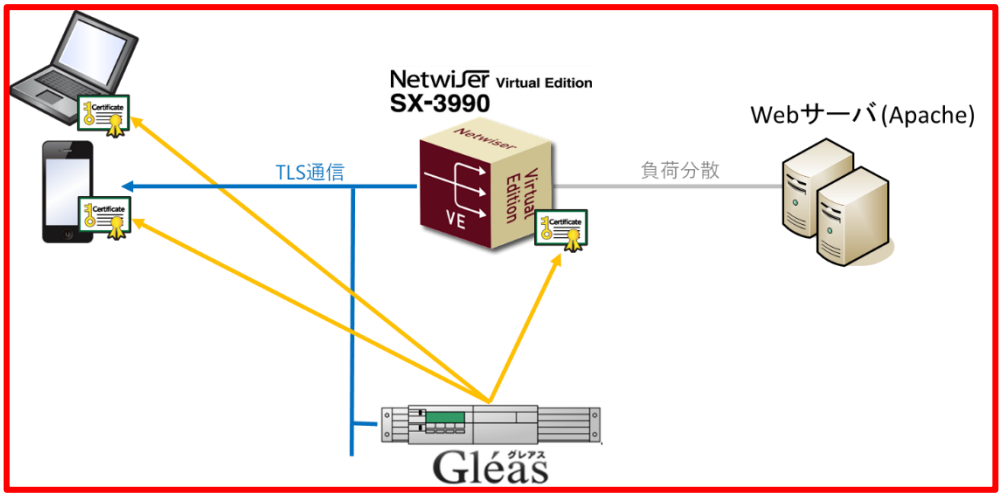
以下については、本書では説明を割愛します。

- **NetWiser 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、NetWiser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NetWiserの仮想サーバーにアクセスし、NetWiser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2.1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。**

2. NetWiser の設定

2.1. サーバ証明書の発行と登録

仮想サーバーで使用するサーバ証明書をGléasから発行し、NetWiser に登録します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [SSL] の [SSL証明書] をクリックします。

[SSL証明書]画面で以下を入力し、SSLポリシーを作成します。

- [SSLポリシー]には、任意の名前を入力

入力後、[設定内容を変更する]ボタンをクリックするとSSLポリシーが作成されます。

続いてCSRを作成します。

メニュー [SSL] の [SSL証明書署名要求作成] をクリックします。

[SSL証明書署名要求作成]画面で以下を入力し、CSRを作成します。

※以下はRSA 2048 ビット長の鍵を使用してCSRを作成する例です。

- **[SSLポリシー名]に、先に作成したSSLポリシーを選択**
- **[ECC証明書]のチェックを外す**
- **[公開鍵長]に、[2048] を選択**
- **[サーバーのFQDN]に、公開する仮想サーバーのFQDNを入力**
- **[国名 (Country)]を入力**
- **[都道府県名 (State)]を入力**
- **[組織名 (Organization)]を入力**
- **他の項目は、環境に応じて設定**

入力後、[設定内容を変更する]ボタンをクリックするとCSRが作成されます。

続いて作成したCSRをダウンロードします。

メニュー [SSL] の [SSLエクスポート] をクリックします。

[SSLエクスポート]画面で[csr]リンクをクリックして、CSRをPCに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、ホスト名に公開する仮想サーバーの 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[ファイルの選択]ボタンより**

  ダウンロードした CSR ファイルを選択

その後、[発行]ボタンをクリックします。

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」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。

NetWiserのWeb管理画面に戻り、メニュー [SSL] の [SSLインポート] をクリックします。

[SSLインポート]画面で以下を入力し、サーバ証明書をインポートします。

- [SSLポリシー名] に作成したSSLポリシーを選択
- [サーバ証明書] の[ファイルの選択] をクリックし、先に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

入力後、[ファイルをインポートする]ボタンをクリックすると、SSL ポリシーに紐づくサーバ証明書がインポートされます。

サーバ証明書がインポートされると、[SSL インポート]画面の[サーバ証明書]欄に

[valid]と表示されます。

2.2. 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

NetWiserのWeb管理画面にログインし、[設定]タブを選択、メニュー [SSL] の [SSLインポート] をクリックします。

[SSLインポート]画面で以下を入力し、サーバ証明書をインポートします。

- [SSLポリシー名] に2.1章で作成したSSLポリシーを選択
- [CA証明書 (クライアント認証)] の[ファイルの選択] をクリックし、Gléas よりダウンロードしたルート証明書ファイルを選択しアップロード

入力後、[ファイルをインポートする]ボタンをクリックすると、SSL ポリシーに紐づくルート証明書がインポートされます。

ルート証明書がインポートされると、[SSL インポート]画面の[CA 証明書]欄に[valid]と表示されます。

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。

NetWiserのWeb管理画面にログインし、[設定]タブを選択、メニュー［SSL］の［証明書失効リスト］をクリックします。

[証明書失効リスト]画面で以下を入力し、サーバ証明書をインポートします。

- ［SSLポリシー名］に2.1章で作成したSSLポリシーを選択
- ［証明書失効リストダウンロードURL］に、Gléas のCRLダウンロードURLを入力。

  ※Gléasのデフォルト発行局の失効リスト（DER形式）のダウンロードURLは以下となります

  http://[GléasのFQDN]/crl/ia1.crl
- [更新間隔]に失効リストを自動更新する間隔を入力

入力後、[設定内容を変更する]ボタンをクリックすると、SSL ポリシーに紐づく失効リストがインポートされます。

※この設定により、[更新間隔]で指定した間隔で[証明書失効リストダウンロードURL]から失効リストを自動取得されます。
※失効リストの登録を行わない場合、クライアント証明書認証時に証明書の失効確認が行われなくなります。

登録されている失効リストは以下の方法で確認できます。

NetWiserのWeb管理画面にログインし、[設定]タブを選択、メニュー [SSL] の [SSLエクスポート] をクリックします。

[SSL エクスポート]画面で SSL ポリシー名に対応する[crl]ボタンをクリックすると、登録されている失効リストがダウンロードされます。

2.4. 実サーバーの登録

ロードバランス先のWebサーバの情報をNetWiserに登録します。

まず、WebサーバのIPアドレスに名前を付与します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [システム] > [ネットワーク] の [IPアドレス名の定義] をクリックします。

[IPアドレス名の定義]画面で以下を入力します。

- [IPアドレス名]には、任意の名前を入力
- [IPアドレス名]には、WebサーバのIPアドレスを入力
- 複数のIPアドレスを登録する際は、[行追加]ボタンをクリックして入力

入力後、[設定内容を変更する]ボタンをクリックするとIPアドレスに名前が付与されます。

次に、WebサーバのListenアドレス、ポートを登録します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [バランシング] > [実サーバー]の [実サーバー設定] をクリックします。

[実サーバー設定]画面で以下を入力しします。

- **[実サーバーIP]に、先に定義したWebサーバのIPアドレスの名前を入力**
- **[ポート]には、Webサーバの待ち受けポート番号を入力**
- **[プロトコル]は、[tcp]を選択**
- **[有効]をチェック**
- **他の項目は、環境に応じて設定**
- **複数のWebサーバを登録する際は、[行追加]ボタンをクリックして入力**

入力後、[設定内容を変更する]ボタンをクリックすると実サーバーが登録されます。

続いて、登録した実サーバーを監視する設定を行います。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [ヘルスチェック] の [ヘルスチェック設定] をクリックします。

[ヘルスチェック選択]画面で[新規]ボタンをクリックします。

[ヘルスチェック設定]画面で以下を入力しします。

- **[ヘルスチェック方法]に、[L4-7ヘルスチェック]を選択**
- **[ヘルスチェック名]には、任意の名前を入力**
- **[有効]をチェック**
- **他の項目は、監視方法に応じて設定**
- **複数の実サーバーを監視する際は、[行追加]ボタンをクリックして入力**

入力後、[設定内容を変更する]ボタンをクリックするとヘルスチェックが開始されます。

[ヘルスチェック選択]画面に戻り、登録状況が確認できます。

2.5. NATプールの登録

NetWiserがWebサーバにアクセスする際の送信元となるソースNAT用IPアドレスを登録します。

まず、ソースNAT用のIPアドレスに名前を付与します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [システム] > [ネットワーク]の [IPアドレス名の定義] をクリックします。

[IPアドレス名の定義]画面で以下を入力します。

- [IPアドレス名]には、任意の名前を入力
- [IPアドレス]には、ソースNAT用のIPアドレスを入力

入力後、[設定内容を変更する]ボタンをクリックするとIPアドレスに名前が付与されます。

次に、NATプールをWebサーバのListenアドレス、ポートを登録します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [バランシング] > [NATプール]の [NATプール] をクリックします。

[NATプール選択]画面で[新規]ボタンをクリックします。

[NATプール設定]画面で以下を入力します。

- [NATプール名]には、任意の名前を入力
- [開始IPアドレス]には、先に定義したソースNAT用のIPアドレスの名前を入力

入力後、[設定内容を変更する]ボタンをクリックするとNATプールが登録されます。

[NATプール選択]画面に戻り、登録状況が確認できます。

2.6. 仮想サーバーの登録

NetWiserが公開する仮想サーバーを登録します。

まず、公開する仮想サーバーのIPアドレスに名前を付与します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [システム] > [ネットワーク] の [IPアドレス名の定義] をクリックします。

[IPアドレス名の定義]画面で以下を入力します。

- [IPアドレス名]には、任意の名前を入力
- [IPアドレス名]には、仮想サーバーのIPアドレスを入力

入力後、[設定内容を変更する]ボタンをクリックするとIPアドレスに名前が付与されます。

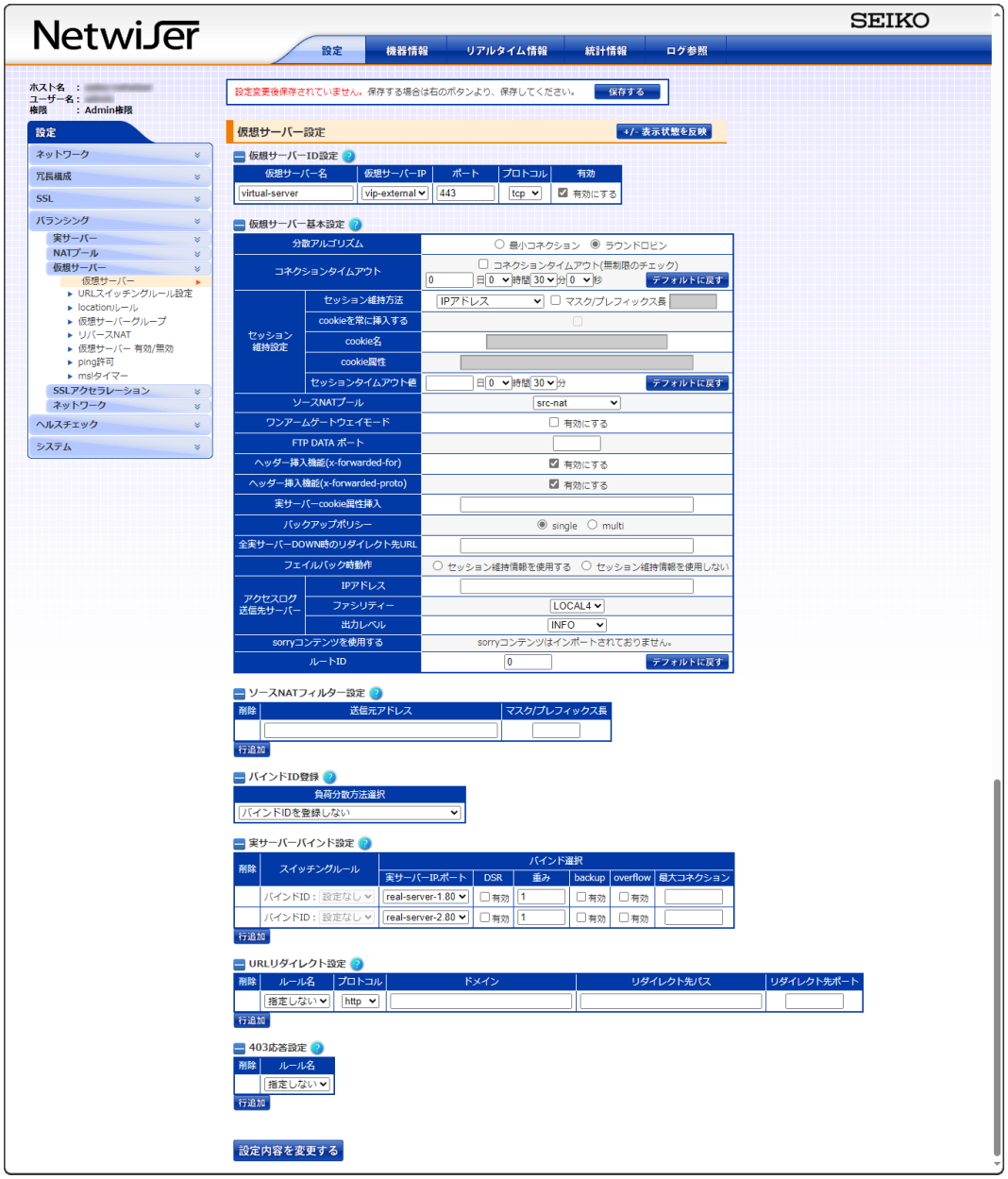
次に、仮想サーバーを登録します。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [バランシング] > [仮想サーバー] の [仮想サーバー] をクリックします。

[仮想サーバー選択]画面で[新規]ボタンをクリックします。

[仮想サーバー設定]画面で以下を入力します。

項目名		値
仮想サーバーID設定	仮想サーバー名	任意の名前
	仮想サーバーIP	仮想サーバーのIPアドレスの名前
	ポート	待ち受けポート(443)
	プロトコル	[tcp]
	有効にする	チェック
仮想サーバー基本設定	分散アルゴリズム	[ラウンドロビン]
	セッション維持方法	[IPアドレス]
	セッションタイムアウト値	30分
	ソースNATプール	2.5章で作成したNATプール
	ヘッダー挿入機能(x-forwarded-for)	チェック
	ヘッダー挿入機能(x-forwarded-proto)	チェック
実サーバーバインド設定	実サーバーIP.ポート	2.4章で登録した実サーバー ※複数ある場合は[行追加]をクリックして登録
	重み	1



入力後、[設定内容を変更する]ボタンをクリックすると仮想サーバーが登録されます。

[仮想サーバー選択]画面に戻り、登録状況が確認できます。

2.7. SSLアクセラレーション設定

2.6章で登録した仮想サーバーに対し、

- サーバ証明書の適用
- 許可する暗号スイート
- クライアント証明書認証
- クライアント証明書情報のWebサーバへの送信

といった設定を行います。

NetWiserのWeb管理画面の[設定]タブを選択、メニュー [バランシング] > [SSLアクセラレーション] の [SSLアクセラレーション] をクリックします。

[SSLアクセラレーション選択]画面で2.6章で登録した仮想サーバーのリンクをクリックして選択します。

[SSLアクセラレーション設定]画面で以下を入力します。

SSL証明書の割り当て

- **[追加元] に 2.1 章で登録したサーバ証明書を選択**
- **[追加]ボタンをクリック ([追加先]に反映される)**

SSL アクセラレーション詳細設定

- **クライアント証明書の[ヘッダー] に、"X-CLIENT-CERT"と入力**
- **クライアント証明書の[形式] に、[Base64]を選択**

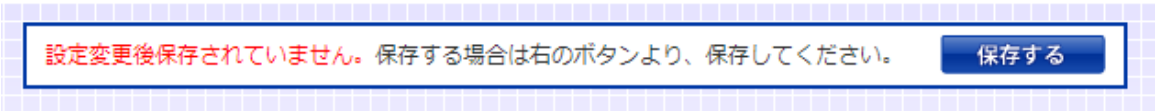
  ※この設定により、実サーバーへの HTTP リクエストの HTTP-X-CLIENT-CERT ヘッダに Base64 形式のクライアント証明書が送信されるようになる
- **SSL セッション ID ヘッダーの[ヘッダー]に"X-SSL-SESSION-ID"と入力**

  ※この設定により、実サーバーへの HTTP リクエストの HTTP-X-SSL-SESSION-ID ヘッダに NetWiser の SSL セッションを識別する文字列が送信されるようになる
- **クライアント認証失敗時処理の[動作]に[403 レスポンス返送]を選択**

  ※この設定により、クライアント証明書認証が失敗した場合に NetWiser はステータスコード 403 を応答するようになる

入力後、[設定内容を変更する]ボタンをクリックすると仮想サーバーにSSLアクセラレーション設定が反映されます。

すべての設定変更が終わったら、[保存する]をクリックして、NetWiserに設定を保存します。



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。

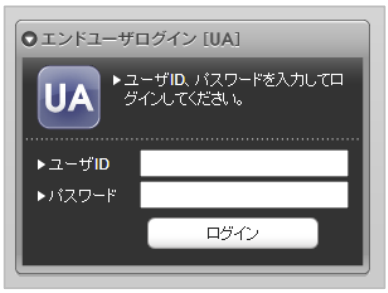
4. クライアントの設定 (Windows)

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。

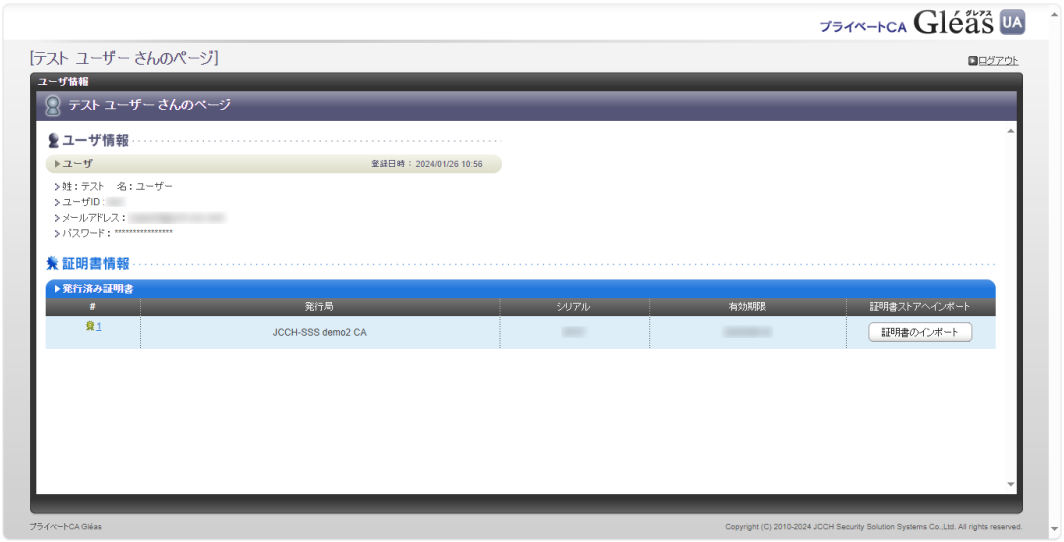
※URL https://[UA の FQDN]/[UA の名前]/ua

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。

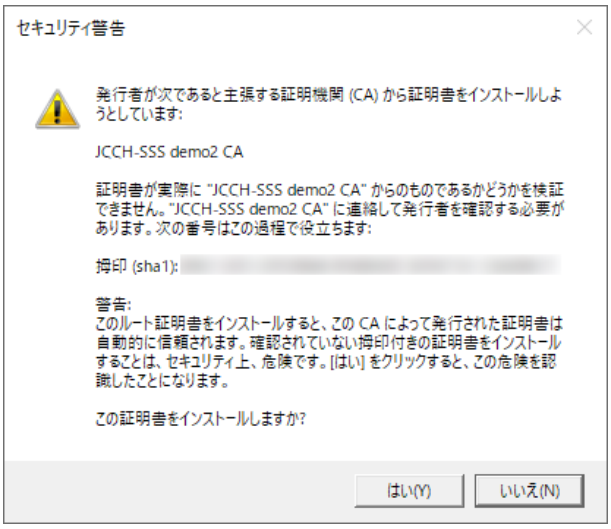


ログインすると、ユーザ専用ページが表示されます。

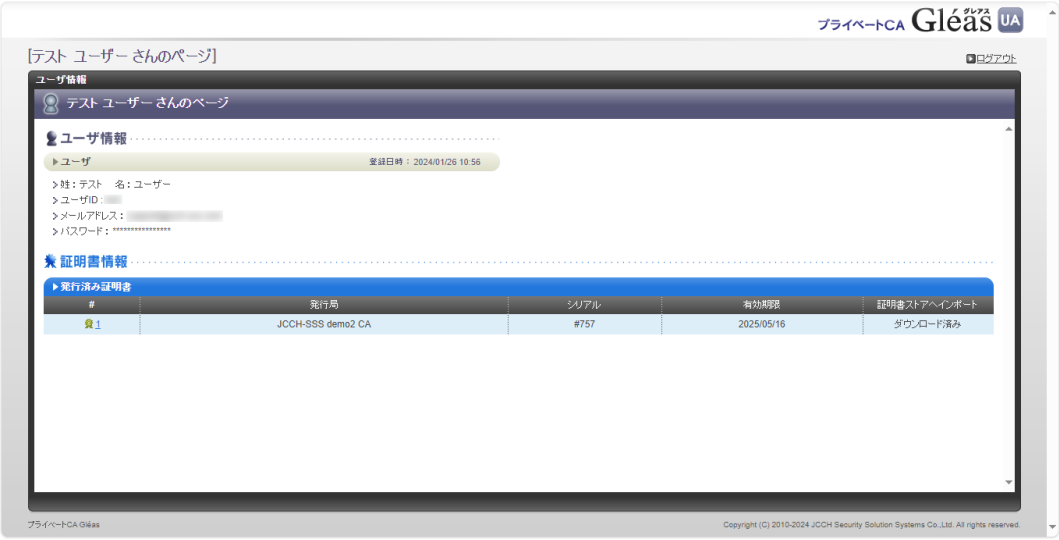
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。



※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

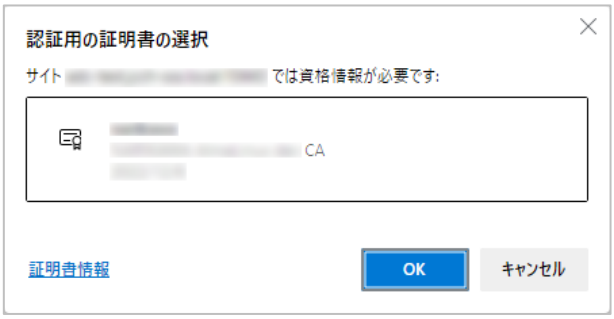


インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ログインしてインポートを行うことはできません。



4.2. Webサーバアクセス

PCのブラウザ（Edge）でNetWiserの仮想サーバーの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。

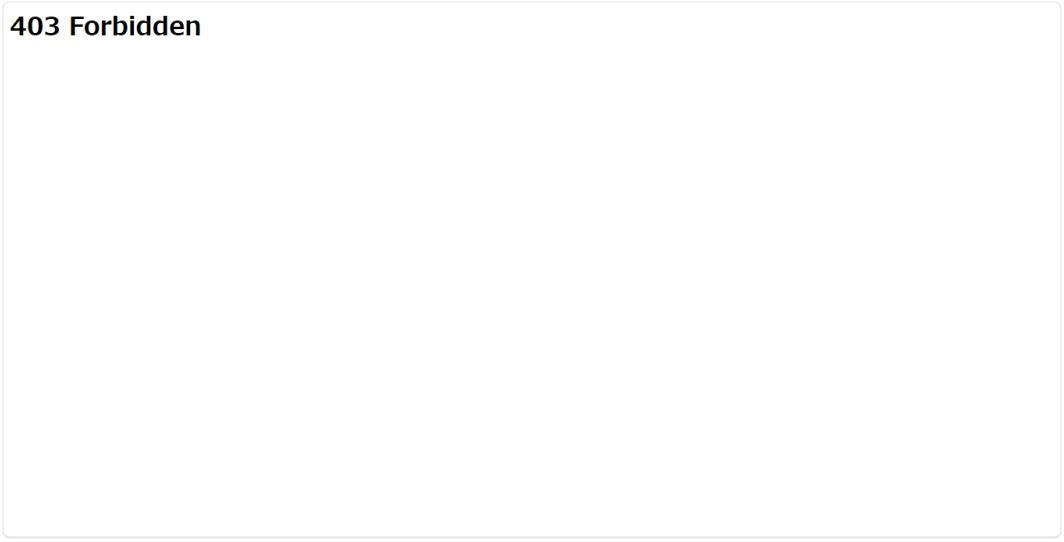


[OK]ボタンをクリックし、クライアント証明書認証がおこなわれるとページが表示されます。

※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。

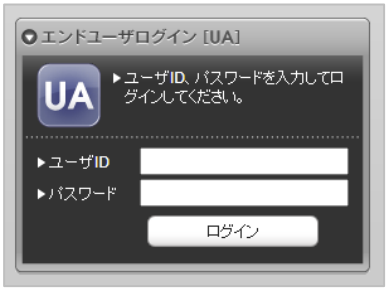
6. クライアントの設定（iPhone)

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。

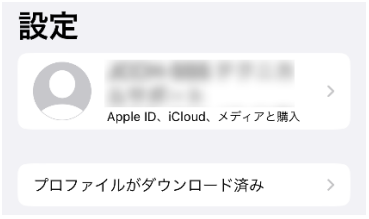


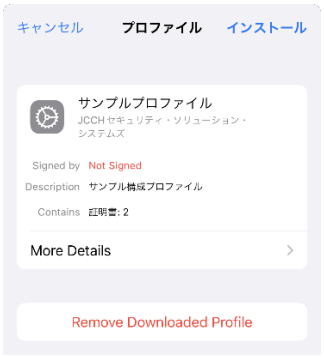
ログインすると、ユーザ専用ページが表示されます。

[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を開くと、プロファイ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。

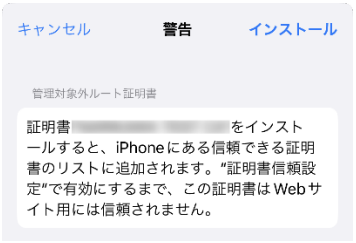




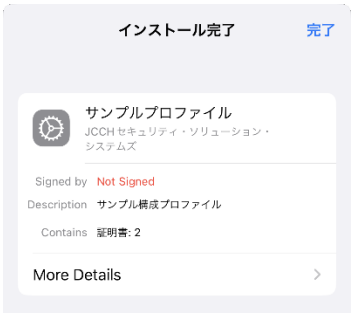
[インストール]をタップして続行してください。

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. Webサーバアクセス

iPhoneのブラウザ（Safari）でNetWiserの仮想サーバーの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

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. Web サーバでクライアント証明書情報を取得

NetWiser 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>
```

- **Apache を再起動**

```
systemctl restart httpd
```

- **CGI を作成**

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

スクリプトの内容は以下。

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

import os
import base64
import OpenSSL
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.items()):
  if headername.startswith("HTTP_"):
    print("{0} = {1}<br>".format(headername, headervalue))

  if headername.startswith("HTTP_X_CLIENT_CERT"):
    der = base64.b64decode(headervalue)
    cert = OpenSSL.crypto.load_certificate(OpenSSL.crypto.FILETYPE_ASN1, der)
    print(" {0}: {1}<br>".format("Issuer", cert.get_issuer().commonName))
    print(" {0}: {1}<br>".format("SerialNo", cert.get_serial_number()))
    print(" {0}: {1}<br>".format("Subject CN", cert.get_subject().commonName))

print("</html></body>")
```

ファイルパーミッションを設定

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

Web ブラウザから CGI にアクセスすると、環境変数 HTTP_X_CLIENT_CERT に Base64 エンコードされたクライアント証明書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

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