



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 NetScalerでのクライアント証明書認証

Ver.1.0

2016年11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 .....	4
1.1. 本書について .....	4
1.2. 本書における環境 .....	4
1.3. 本書における構成 .....	5
1.4. 証明書発行時における留意事項 .....	6
2. NetScaler の設定 .....	6
2.1. ルート証明書の登録 .....	6
2.2. サーバ証明書の発行と登録 .....	7
2.3. 失効リスト (CRL) の登録 .....	12
2.4. 証明書認証ポリシーの設定 .....	13
2.5. バーチャルサーバの設定 .....	14
3. Gléas の管理者設定 (PC) .....	16
4. PC からの接続操作 .....	17
4.1. クライアント証明書のインポート .....	17
4.2. クライアントからの ICA 接続 .....	18
5. Gléas の管理者設定 (iPad) .....	20
6. iPad からの接続操作 .....	21
6.1. Citrix Receiver のインストール .....	21
6.2. Gléas の UA からの証明書インポートおよび ICA 接続 .....	21
7. 問い合わせ .....	25

## 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 NetScaler を経由した ICA (Independent Computing Architecture) 接続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。

- ICAゲートウェイ：  
Citrix NetScaler VPX 1000 Platinum Edition (NS10.5: Build 56.22.nc)  
※以後、「NetScaler」と記載します
- 認証局：JS3 プライベートCA Gléas (バージョン1.14.6)  
※以後、「Gléas」と記載します
- ハイパーバイザー：XenServer 7 (XS70E004)
- ドメインコントローラ：  
Windows Server 2012 R2 Standard / Active Directory Domain Services  
※以後、「ドメインコントローラ」と記載します
- Delivery Controller 兼 StoreFront：  
Windows Server 2012 R2 Standard / XenDesktop Platinum Edition 7.11  
※以後、「XenDesktop」と記載します
- 仮想デスクトップ：Windows10 Pro / Citrix Virtual Delivery Agent 7.11  
※以後、「仮想デスクトップ」と記載します
- クライアント：Windows10 Pro / Internet Explorer 11 / Citrix Receiver 4.5  
※以後、「Windows」と記載します
- クライアント：iPad Air2 (iOS 10.1.1) / Citrix Receiver for iOS v7.1.1  
※以後、「iPad」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。

- NetScaler 及び XenDesktop の基本設定（ネットワーク設定や基本的な ICA のプロキシ設定）

本書では、以下の環境がすでにあることを前提としています。

- ✓ NetScaler 経由で XenDesktop (StoreFront) にアクセス可能なこと
- ✓ NetScalerの認証がActive Directory (LDAP Authentication) でおこなえること

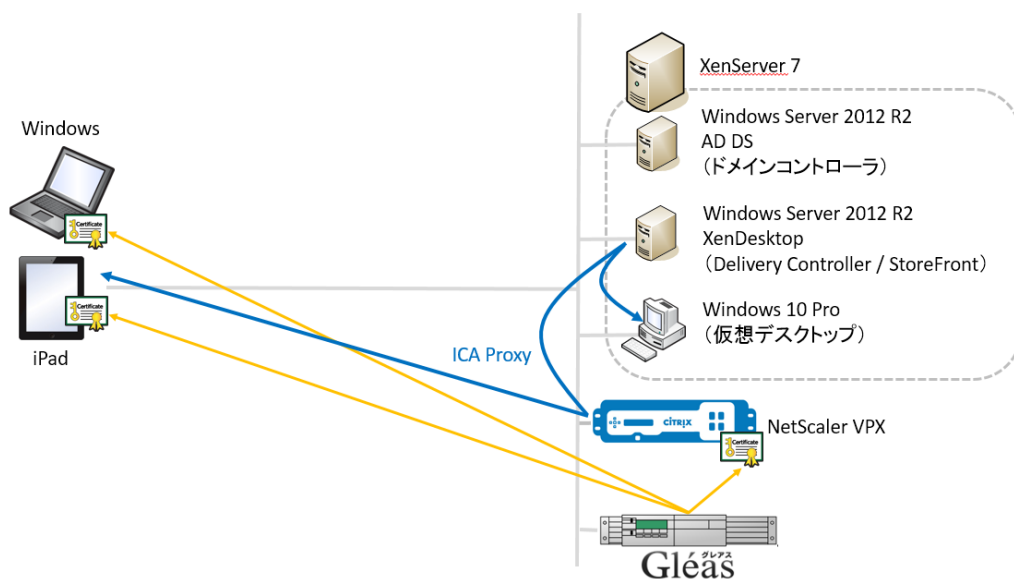
- Gléasでのユーザ登録やクライアント証明書発行などの基本操作

- 各種サーバ・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、NetScalerにサーバ証明書を、PCとiPadにクライアント証明書を発行する。
2. PCとiPadはGléasより証明書をインポートする。
3. PCはブラウザより、iPadはCitrix ReceiverよりNetScalerにアクセスし、NetScalerはクライアント証明書認証をおこなう。

証明書認証後にActive DirectoryでのユーザID・パスワード認証をおこなうが、ユーザIDはクライアント証明書から抽出することで、ユーザIDの詐称がおこなえないようにする。

## 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。

- 本書の構成では、クライアント証明書の発行時に「サブジェクトの代替名 (Subject Alternative Name)」フィールドに、Active Directoryのユーザープリンシパル名 (userPrincipalName) を含める必要があります。  
(Gléasでは、Active Directoryよりアカウント情報をインポートさせることも可能です)
- 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く必要があります。

## 2. NetScaler 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://hostname/crl/ia1.pem>

NetScalerの管理画面にログインし、左ペインから Traffic Management > SSL > Certificates と進み、右ペインより Install ボタン をクリックします。

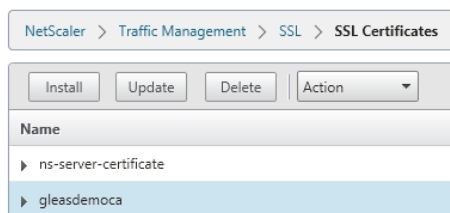
次の画面で 以下を設定します。

- Certificate Key Pair Name には、任意の識別名称を入力
- Certificate File Name は、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ファイルを選択しアップロード
- Certificate Format は、PEM を選択

The screenshot shows the 'Install Certificate' configuration page in NetScaler. The form includes the following fields and options:

- Certificate-Key Pair Name\***: A text input field containing 'gleasdemoca'.
- Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.**: A note indicating the storage location.
- Certificate File Name\***: A text input field containing 'ia1.cer', with a 'Browse' button and a '+' icon to the right.
- Key File Name**: A text input field, with a 'Browse' button and a '+' icon to the right.
- Certificate Format**: Radio buttons for 'PEM' (selected) and 'DER'.
- Password**: A text input field.
- Certificate Bundle**: An unchecked checkbox.
- Notify When Expires**: A checked checkbox.
- Notification Period**: A text input field containing '30'.
- Buttons**: 'Install' and 'Close' buttons at the bottom.

設定後に、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。



## 2.2. サーバ証明書の発行と登録

NetScalerの管理Webの左ペインから Traffic Management > SSL を選択し、右ペインより Create RSA Key をクリックします。

その画面で以下を入力します。

- [Key Filename]に、NetScaler内に保存するファイル名を入力
- 他の項目は、環境に応じて設定

入力後、Create をクリックします。

右図は、トリプル DES 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です。

← Back

### Create RSA Key

Key Filename\*  
ns.js3-test.xen.local.key Browse

Key Size(bits)\*  
2048

Public Exponent Value\*  
F4

Key Format\*  
PEM

PEM Encoding Algorithm  
DES3

PEM Passphrase  
●●●●●●●●

Confirm PEM Passphrase  
●●●●●●●●

Create Close

次に Create Certificate Signing Request (CSR) をクリックします。

次の画面で以下を入力します。

- [Request File Name]に、NetScaler内に保存するファイル名を入力
- [Key Filename]に、Create RSA Keyで作成した秘密鍵を指定
- [Country]、[State or Province]、[Organization Name]（いずれも必須項目）は、任意の名称を入力
- [Common Name]は、サーバのホスト名を入力  
※Gléasに同じ名前のサーバアカウントがあること

入力後、Create をクリックします。

**Create Certificate Signing Request (CSR)**

Request File Name\*  
ns.js3-test-xen.local.req Browse

Key Filename\*  
ns.js3-test-xen.local.key Browse

Key Format  
 PEM  DER

PEM Passphrase (For Encrypted Key)  
●●●●●●●●

**Distinguished Name Fields**

Country\*  
JAPAN

State or Province\*  
Tokyo

Organization Name\*  
JS3

City

Email Address

Organization Unit

Common Name  
ns.js3-test-xen.local

**Attribute Fields**

Challenge Password

Company Name

Create Create and Add New Close

画面に証明書署名リクエスト（CSR）が生成されるので、Click here to view をクリックします。

CSRのテキストデータが表示されるので Save text to a file をクリックし、ファイルを保存します。

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。  
小メニューの[証明書発行]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 NetScaler でのクライアント証明書認証



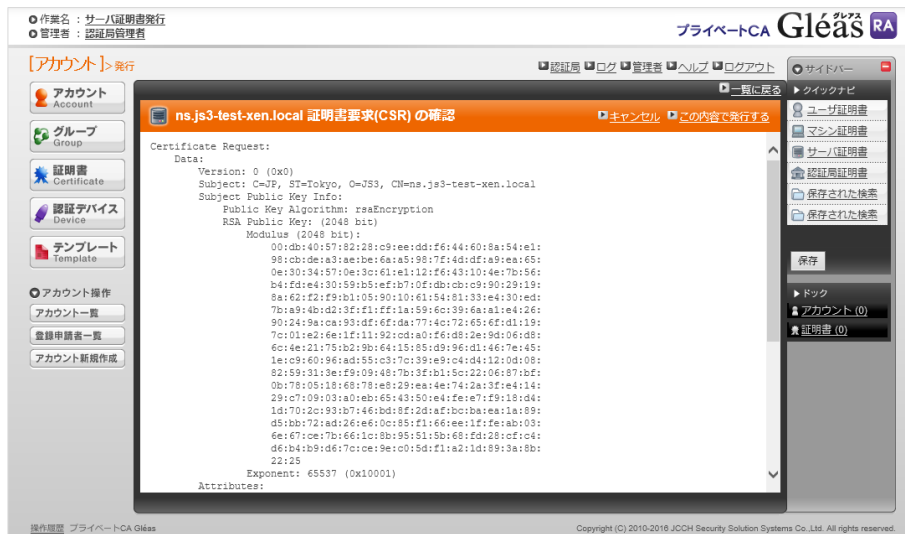
上級者向け設定を展開し、以下の操作をおこないます。

- 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。



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。

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



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。



NetScaler の管理画面に戻り、左ペインから Traffic Management > SSL > 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 は、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ファイルを選択しアップロード
- Key File Nameは、Create RSA Key で生成し、NetScalerのファイルシステムに保存されたファイルを選択
- Certificate Format は、PEM を選択
- Passwordは、Create RSA Key で秘密鍵のパスワードを指定した場合に入力

**Install Certificate**

Certificate-Key Pair Name\*  
ns.js3-test-xen.local

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name\*  
download.crt Browse +

Key File Name  
ns.js3-test-xen.local.key Browse +

Certificate Format  
 PEM  DER

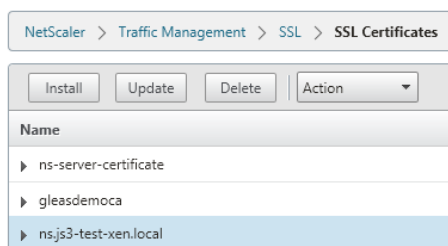
Password  
.....

Certificate Bundle  
 Notify When Expires

Notification Period  
30

Install Close

設定後に、Install ボタンをクリックするとサーバ証明書が追加されます。



## 2.3. 失効リスト (CRL) の登録

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://hostname/crl/ia1.crl

NetScalerの管理Webの左ペインから Traffic Management > SSL > CRL を選択し、右ペインより[Add]をクリックします。

CRL追加画面で以下を設定します。

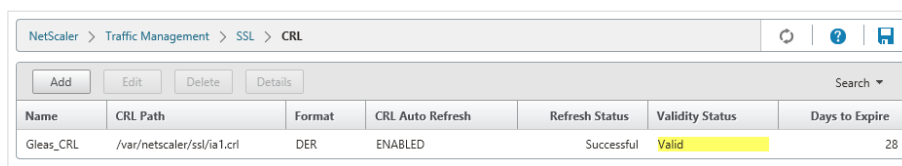
※右図は毎日0時にCRLを自動更新する設定例

- CRL には、任意の名称を入力
- CRL File には、[Browse]をクリックすると File Browser が表示されるので [Upload]をクリックし事前にダウンロードしたCRLをアップロードし、それを選択
- 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 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

The screenshot shows the 'Create CRL' configuration page in NetScaler. The form is divided into several sections:

- Basic Information:** CRL Name\* (Gleas\_CRL), CRL File\* (/var/netscaler/ssl/ia1.crl), Inform (DER selected), CA Certificate (gleasdemoca), and a checked 'Enable CRL Auto Refresh' checkbox.
- CRL Auto Refresh Parameter:** Method\* (HTTP), Scope\* (One), Server IP (empty), Port\* (80), URL (http://demo.jcch-sss.com/crl/ia1.crl), Base DN\* (empty), Bind DN (empty), Password (empty), Interval (Daily), Day(s) (empty), and Time (HH:MM)\* (00:00).
- Additional Options:** An unchecked 'Binary' checkbox.
- Buttons:** 'Create' and 'Close' buttons at the bottom.

設定後、[Create]をクリックします。以下の通り設定されたCRLが表示されます。



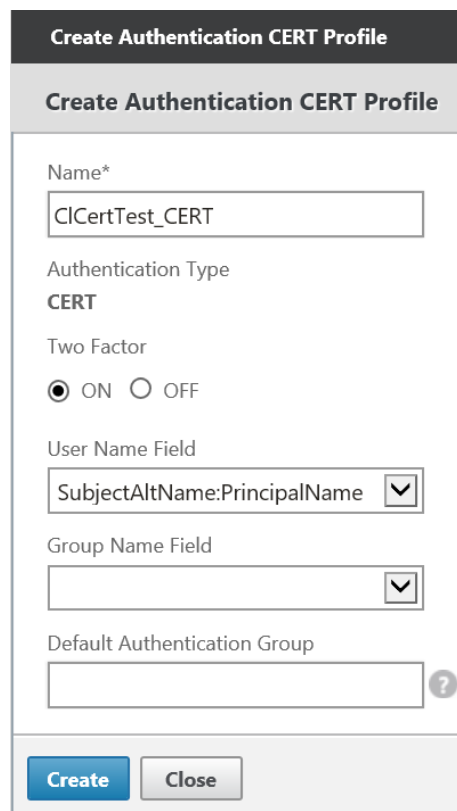
Name	CRL Path	Format	CRL Auto Refresh	Refresh Status	Validity Status	Days to Expire
Gleas_CRL	/var/netscaler/ssl/ia1.crl	DER	ENABLED	Successful	Valid	28

以上で CRL の登録は完了です。

## 2.4. 証明書認証ポリシーの設定

NetScaler の管理 Web の左ペインから Security > AAA-Application Traffic > Policies > Authentication > Basic Policies を選択し、右ペインより [No Authentication Cert Policy] をクリックし、Policies で [Add] を追加します。  
ポリシー設定画面で以下を設定します。

- Name は、任意の識別名称を入力
- Server は、[+] をクリックすると Create Authentication CERT Profile が表示されるので、以下を設定（右図）
  - ✓ Name は、任意の識別名称を入力
  - ✓ Two Factor は、[On] を選択
  - ✓ User Name Field は、  
[SubjectAltName:PrincipalName] を選択
- Expression は、NS-TRUE と入力



**Create Authentication CERT Profile**

**Create Authentication CERT Profile**

Name\*  
CI CertTest\_CERT

Authentication Type  
**CERT**

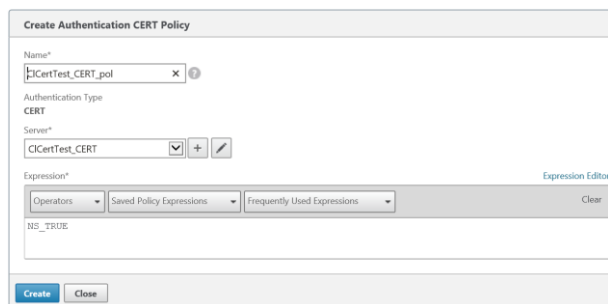
Two Factor  
 ON  OFF

User Name Field  
SubjectAltName:PrincipalName

Group Name Field

Default Authentication Group

**Create** **Close**



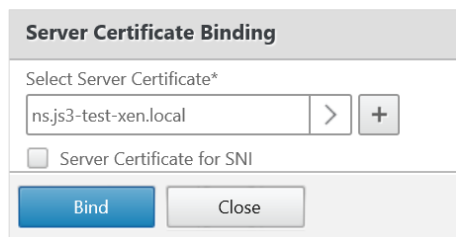
完了後、[Create]をクリックします。

## 2.5. バーチャルサーバの設定

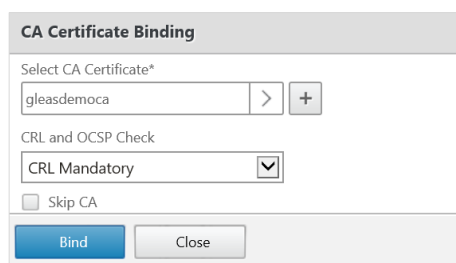
NetScalerの管理Webの左ペインから NetScaler Gateway > Virtual Servers と進み、右ペインよりクライアント証明書認証を追加するバーチャルサーバをクリックし、[Edit]をクリックします。

バーチャルサーバの設定画面で以下を設定します。

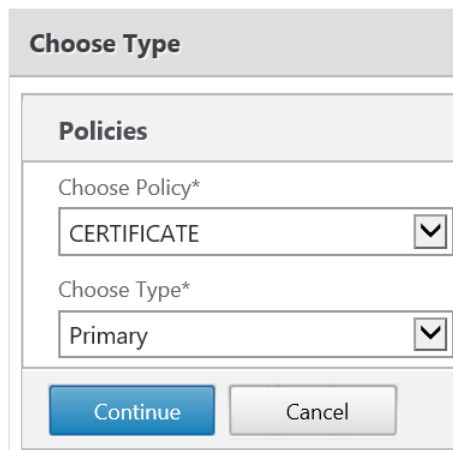
- Certificates 欄の No Server Certificate をクリックし、2.2 項で設定したサーバ証明書を設定



- Certificates 欄の No CA Certificate と進み、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

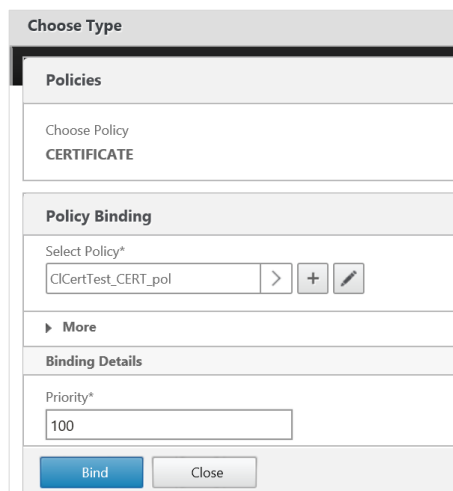


- Authentication 欄の[+]をクリックし証明書認証を追加します。
  - ✓ Choose Policy は、[Certificate]を選択
  - ✓ Choose Type は、[Primary]を選択



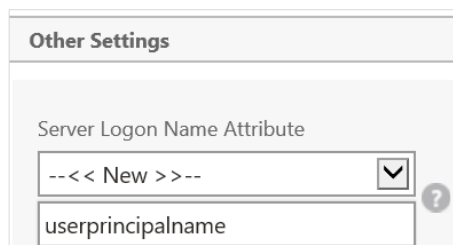
[Continue]をクリックし、

- ✓ Policy Binding は、2.4 後で設定したポリシーを選択
- ✓ Priority は、100 を入力（デフォルト）



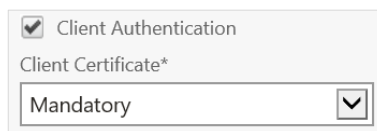
[Bind]をクリック

- (LDAP 認証ポリシーで、userPrincipalName によるログインが設定されていない場合) Authentication 欄の Active Directory の認証設定 (LDAP Policy) をクリックし、対象のポリシーを選択し[Edit Action]をドロップダウンより選択。Configure Authentication LDAP Server 画面で、Server Logon Name Attribute に"userprincipalname"を設定

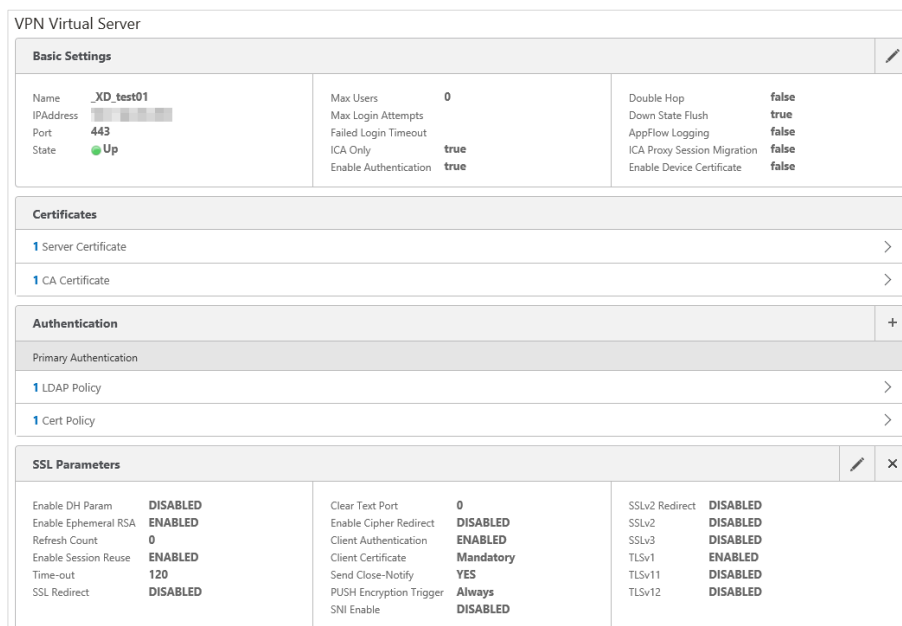


- SSL Parameters 欄の設定を以下の通り編集します

- ✓ Client Authentication をチェック
- ✓ Client Certificate に、[Mandatory]を選択



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。



Basic Settings					
Name	_XD_test01	Max Users	0	Double Hop	false
IP Address	[REDACTED]	Max Login Attempts		Down State Flush	true
Port	443	Failed Login Timeout		AppFlow Logging	false
State	Up	ICA Only	true	ICA Proxy Session Migration	false
		Enable Authentication	true	Enable Device Certificate	false

Certificates		
1	Server Certificate	>
1	CA Certificate	>

Authentication		
Primary Authentication		
1	LDAP Policy	>
1	Cert Policy	>

SSL Parameters					
Enable DH Param	DISABLED	Clear Text Port	0	SSLv2 Redirect	DISABLED
Enable Ephemeral RSA	ENABLED	Enable Cipher Redirect	DISABLED	SSLv2	DISABLED
Refresh Count	0	Client Authentication	ENABLED	SSLv3	DISABLED
Enable Session Reuse	ENABLED	Client Certificate	Mandatory	TLsv1	ENABLED
Time-out	120	Send Close-Notify	YES	TLsv11	DISABLED
SSL Redirect	DISABLED	PUSH Encryption Trigger	Always	TLsv12	DISABLED
		SNI Enable	DISABLED		

以上でNetScalerの設定は終了です。

### 3. Gléas の管理者設定 (PC)

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の納品時に弊社で設定をおこなっている場合があります

GléasのRA (登録局) にログインし、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をクリックします。



[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。

- [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

<input checked="" type="checkbox"/> 証明書ストアへのインポート	証明書ストアの種類	ユーザストア
<input type="checkbox"/> ダウンロードを許可	<input checked="" type="checkbox"/> インポートワンスを利用する	

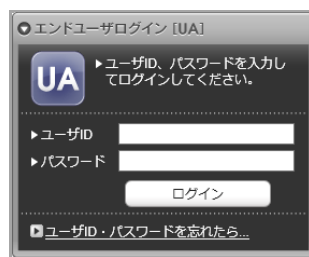
設定終了後、[保存]をクリックし設定を保存します。

## 4. PC からの接続操作

### 4.1. クライアント証明書のインポート

Internet Explorer で Gléas の UA にアクセスします。

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。



End User Login [UA]

ユーザID、パスワードを入力してログインしてください。

ユーザID:

パスワード:

ログイン

ユーザID・パスワードを忘れたら...

ログインすると、ユーザ専用ページが表示されます。



プライベートCA Gléas UA

[user01@js3-test-xen.local さんのページ] ログアウト

ユーザ情報

user01@js3-test-xen.local さんのページ ヘルプ

ユーザ情報

ユーザ 登録日時: 2016/10/15 09:28

姓: XenD 名: test  
ユーザID: user01@js3-test-xen.local  
メールアドレス:  
パスワード: \*\*\*\*\*

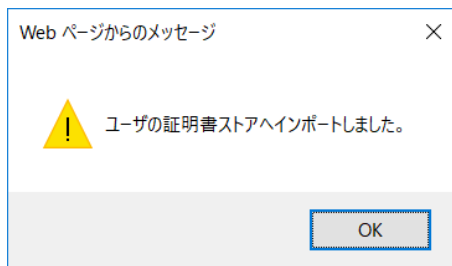
証明書情報

発行済み証明書

#	発行局	シリアル	有効期限	証明書ストアへインポート
1	JCCH-SSS demo CA	#11251	2019/10/15	証明書のインポート

プライベートCA Gléas Copyright (C) 2010-2016 JCCH Security Solution Systems Co., Ltd. All rights reserved.

[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が証明書ストアにインポートされます。



※初回ログインの際は、ActiveX コントロールのインストールを求められるので、画面の指示に従いインストールを完了してください。

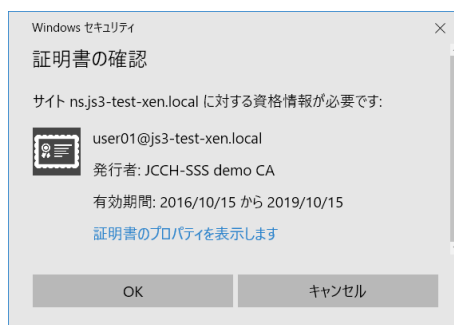
「インポートワンス」を有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度のインポートを行うことはできません。



## 4.2. クライアントからのICA接続

WebブラウザでNetScalerのバーチャルサーバに接続すると、クライアント証明書の提示を求められます。

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



証明書認証がおこなわれるとログイン画面に遷移しますが、ユーザIDはクライアント証明書より抽出されていて変更することはできません。パスワードのみ入力します。



パスワード認証に成功するとStoreFrontのトップ画面に遷移します。



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接続に失敗しま

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場合です。



## 5. Gléas の管理者設定 (iPad)

Gléas で、発行済みのクライアント証明書を Citrix Receiver 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、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。

[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、クライアント証明書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iOSデバイスへのクライアント証明書のインストールを制限することができます。



設定終了後、[保存]をクリックし設定を保存します。

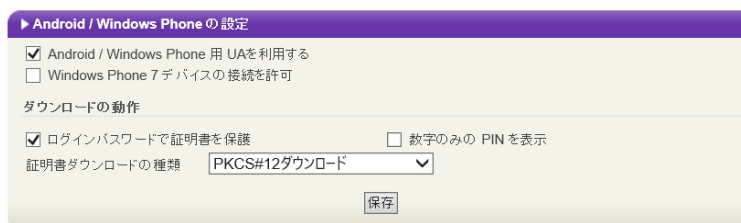
[認証デバイス情報]の[Android / Windows Phone の設定]までスクロールし、[Android/Windows Phone用UAを利用する]をチェックします。

※iPadに証明書をインポートしますが、GléasのAndroid向け機能を利用するため



Androidからの接続に必要な情報を入力する画面が展開されるので、以下設定を行います。

- ログインパスワードで証明書を保護：チェック
- 証明書ダウンロードの種類：[PKCS#12ダウンロード]を選択



設定終了後、[保存]をクリックし設定を保存します。  
以上でGléasの設定は終了です。

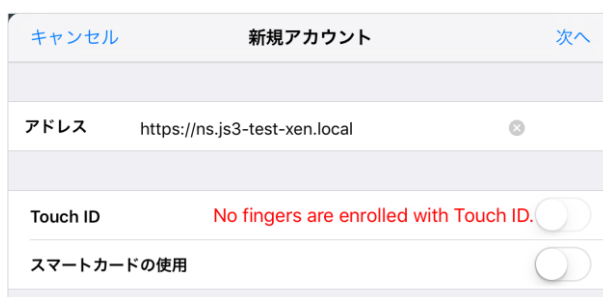
## 6. iPad からの接続操作

### 6.1. Citrix Receiverのインストール

iPhoneでCitrix Receiverを利用する場合は、クライアントソフトウェアのダウンロードが必要です。App Store より事前にインストールを行ってください。  
本書ではCitrix Receiverのインストール方法については割愛します。

### 6.2. GléasのUAからの証明書インポートおよびICA接続

Citrix Receiverを起動し、[アカウントの追加]をタップします。  
新規アカウントの画面で、2.5項で設定したNetScalerのバーチャルホストのURLを入力します。

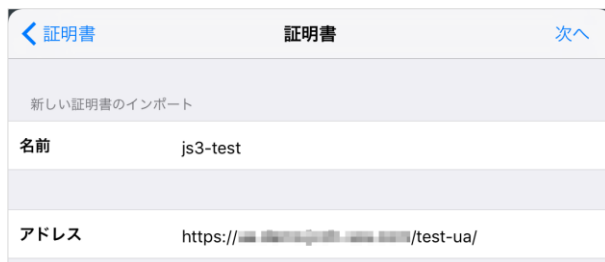


[新しい証明書のインポート]をタップします。

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



名前は、任意の識別名称を入力します。  
アドレスは、5.1項で設定したGléasのUAのアドレスを入力します。



UAのトップ画面が開きます。  
IDとパスワードを入力し、ログインします。  
※2016年11月現在、GléasはCitrix Receiverの内蔵ブラウザに正式対応していないため、UAの画面上に警告が表示されますが、以下に記載する証明書のインポート動作は正常におこなえることを弊社では確認しています

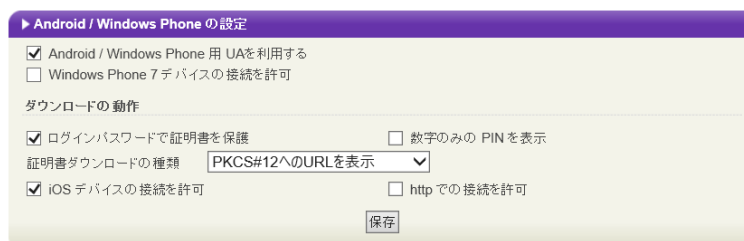


ログイン後、証明書のダウンロードページが表示されます。



※ログイン後に「お使いのブラウザはサポートしておりません」という表示が出現する場合は、5.1項のUAの設定において以下の操作をおこなうことで対処可能です

1. Android / Windows Phone の設定で、証明書ダウンロードの種類を[PKCS#12ダウンロード]から[PKCS#12へのURLを表示]に変更
2. [iOSデバイスの接続を許可]をチェック
3. いったん保存し、再度証明書ダウンロードの種類を[PKCS#12ダウンロード]に変更して再度保存



パスワードを要求されるので、ログイン時と同じパスワードを入力します。

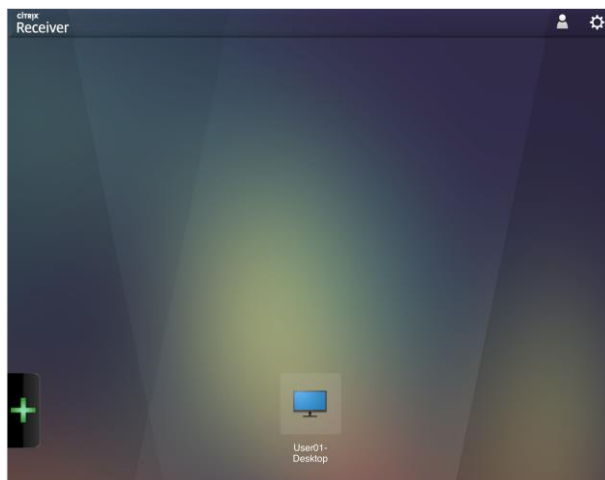


証明書のインポートと同時に証明書認証が完了し、パスワード認証画面が表示されます。ユーザ名とドメイン名は、証明書より抽出されたものが表示され、変更はできません。

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

Citrix Receiver へのログイン	
キャンセル	ログイン
ユーザ名	user01
パスワード	パスワード
ドメイン	js3-test-xen.local

ログインが完了すると、ユーザに割り当てられたリソースが表示されます。

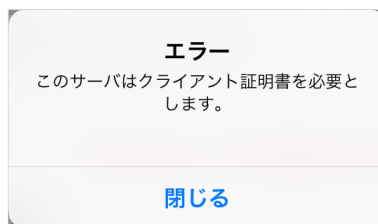


なお、インポートロックを有効にしている場合、UAで[ダウンロード]をタップした時点より管理者の指定した時間（分）を経過した後にUAに再ログインすると、以下の通り「ダウンロード済み」という表記に変わり、以後のダウンロードは一切不可となります。

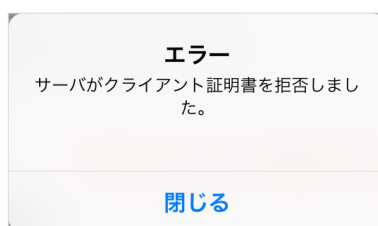
証明書	
プライベートCA Gléas UA	
XenD test さんのページ	
ユーザID	user01@js3-test-xen.local
姓	XenD
名	test
メール	
JCCH-SSS demo CA	
有効期限 2019/10/27	ダウンロード済み
ログアウト	



証明書をインポートせずに NetScaler にアクセスしようとするると以下のメッセージが表示されます。



失効された証明書で NetScaler にアクセスすると、以下のメッセージが表示されま



## 7. 問い合わせ

### ■Gléasに関するお問い合わせ先

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