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

XenDesktopスマートカードログオン

Ver.1.1

2011 年 11 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」で発行した電子証明書とGemalto .NET（ドットネット）製品を利用して、シトリックス・システムズ・ジャパン株式会社のXenDesktopにおけるスマートカードログオンを行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

本書における手順は、以下の環境で動作確認を行っています。

- 【ハイパーバイザ】Citrix XenServer 5.6 FP1
- 【デスクトップ配信コントローラ】
  Citrix XenDesktop 5 SP1 Express Edition / Microsoft Windows Server 2008 Standard SP2 （64bit）
  ※以後、「XenDesktop」或いは「DDC」と記載します
- 【ドメインコントローラ】Microsoft Windows Server 2008 R2 Standard
  ※以後、「ドメインコントローラ」と記載します
- 【仮想デスクトップ】Microsoft Windows 7 Ultimate SP1 （32bit）
  ※以後、「仮想デスクトップ」と記載します
- 【認証局】JS3 プライベートCA Gléas （バージョン1.9）
  ※以後、「Gléas」と記載します
- 【クライアントPC】Microsoft Windows 7 Ultimate SP1 （32bit）
  ※以後、「クライアントPC」と記載します
- 【認証デバイス】Gemalto .NETカード
  ※以後、「認証デバイス」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。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。

- Gléasでのユーザ登録やクライアント証明書発行等の基本操作
- Windows 7でのネットワーク設定等の基本設定
- 認証デバイスのドライバインストールや、パーソナライズ等の基本操作
- Windowsスマートカードログオン環境のセットアップ

  ※弊社のWEBサイトでは、Windowsスマートカードログオン環境を構築するためのホワイトペーパーを公開しておりますので、構築時の参考にしてください

  参考URL：

  http://www.jcch-sss.com/images/Windows_Smartcard_Logon_Gleas_Configuration.pdf
- XenServer環境、及びXenDesktop環境のセットアップ

  以下のインストールや設定は済んでおり、仮想デスクトップへの接続がドメインユーザID・パスワードを利用して可能になっていることを前提としています

  - DDCのインストール・仮想デスクトップの公開設定
  - 仮想マシンに対するVirtual Desktop Agentのインストール
  - クライアントPCへの認証デバイスのドライバインストール
  - クライアントPCに対するOnline Plug-in Webのインストール

  ※上記のXenDesktop環境構築に関しては、シトリックス・システムズ・ジャパン株式会社が公開している「Xen Desktop 5.0 SP1 仮想デスクトップ環境簡易構築ガイド」を参考にしています。

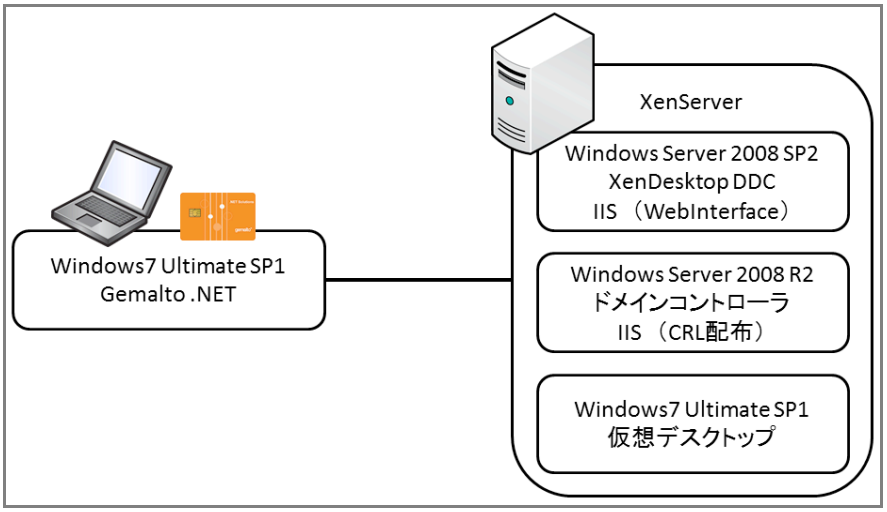
  本ホワイトペーパー作成時では以下URLで配布されています

  参考URL：

  http://www.citrix.co.jp/products/download.html

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おります。



XenDesktopで以下認証方式を用いた認証を行います。

- スマートカード認証（Webサイト・Serviceサイト）
  クライアントPCでのDDCへのログインにスマートカードを利用します。
  仮想デスクトップにログオンする際にもスマートカードを利用します。
  DDCへのアクセスにはWebブラウザを利用する方法と、専用クライアントソフトウェアを利用してログインする方法があります。

1.4. Gléas で事前発行する電子証明書

Windowsスマートカードログオン環境で必要となるもの以外で、事前準備が必要となる証明書は以下の通りです。

- Web Interface用サーバ証明書（SSLサーバ証明書）

2. 仮想デスクトップでの設定

2.1. スマートカードドライバのインストール

仮想デスクトップに.NETカードのミニドライバをインストールします。

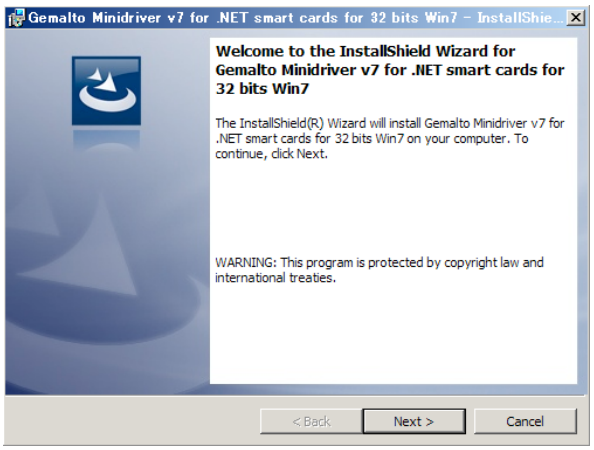
※本ホワイトペーパー作成時点では以下URLでミニドライバが配布されています

参考URL：

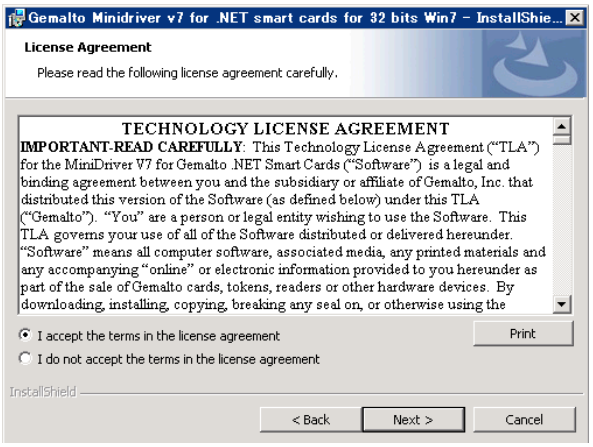
http://www.gemalto.com/products/dotnet_card/resources/libraries.html

*.NET card minidriver dll installation software*がミニドライバのインストーラになります

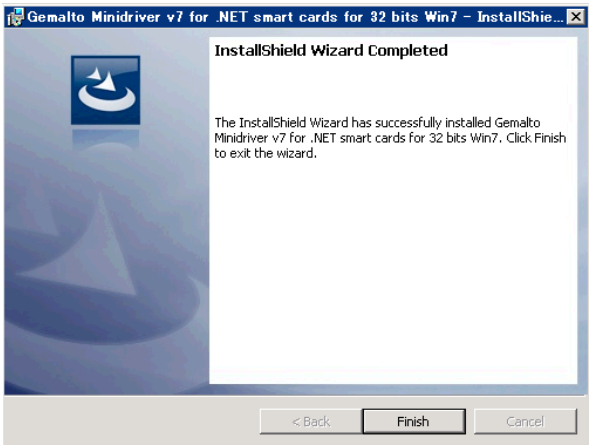
ダウンロードしたファイルを解凍して、Windows7（32bit）用のインストーラファイルを実行してインストールを開始します。



ライセンス使用許諾を受諾する場合は、[I accept the term in the license agreement]を選択し、[Next >]をクリックしてインストールを進めます。



インストールウィザードに従いインストールを終了します。



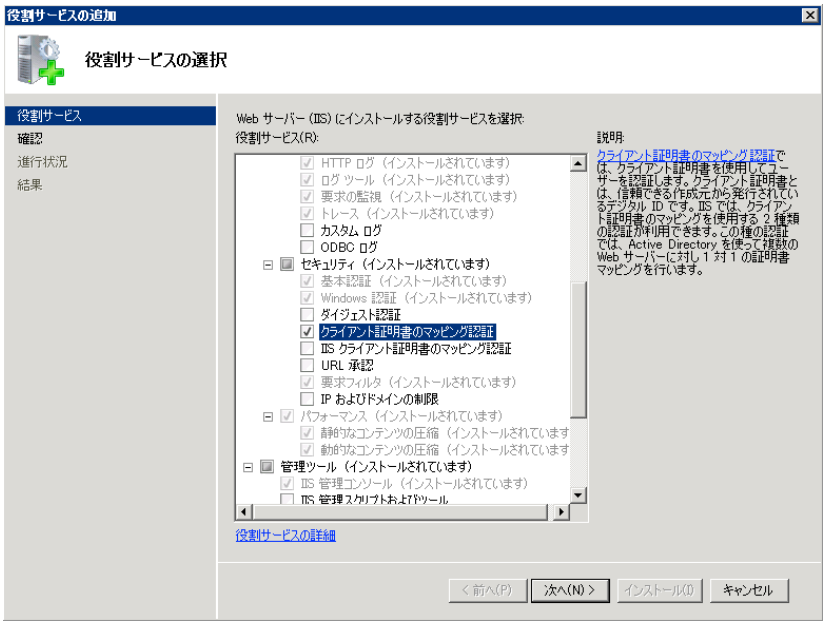
インストールが完了した段階で、仮想デスクトップへのリモートデスクトップ接続にスマートカードログオンができるようになります。

※Virtual Desktop Agent が未インストールである必要があります

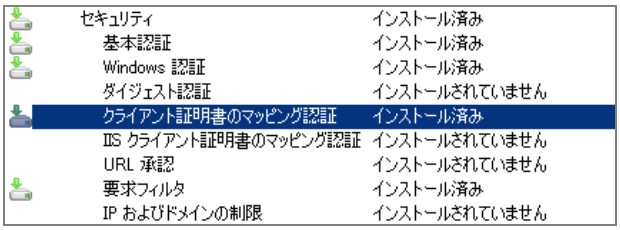
3. DDC での設定

3.1. IIS への役割の追加

管理メニューの [サーバーマネージャ]を開き、左ペインの[役割]を展開します。
右ペインの[WEB サーバー（IIS）]欄で[役割サービスの追加]をクリックすると、[役割サービスの追加]ウィンドウが表示されるので、[クライアント証明書のマッピング認証]を選択し[次へ(N) >]をクリックし 、インストールします。



もとの画面で、クライアント証明書のマッピング認証がインストール済みであることを確認します。

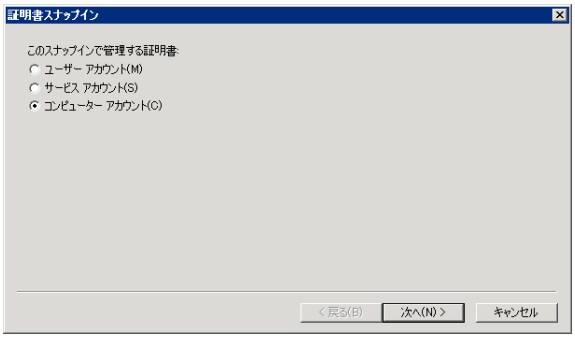


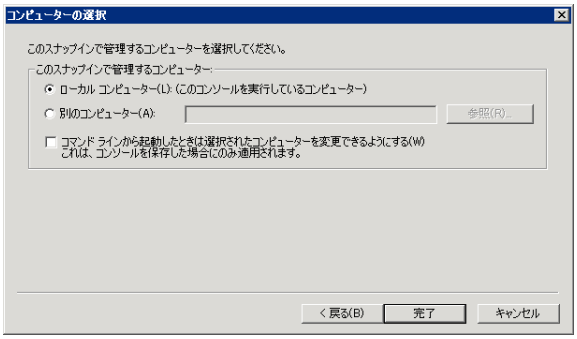
スタートメニューより[インターネット インフォメーション サービス（IIS）マネージャー]を開き、左ペインからホスト名を選択し、右ペインより[認証]オプションを開きます。[Active Directory クライアント証明書の認証]を有効にし、他のものを全て無効にします。

3.2. サーバ証明書のインポート

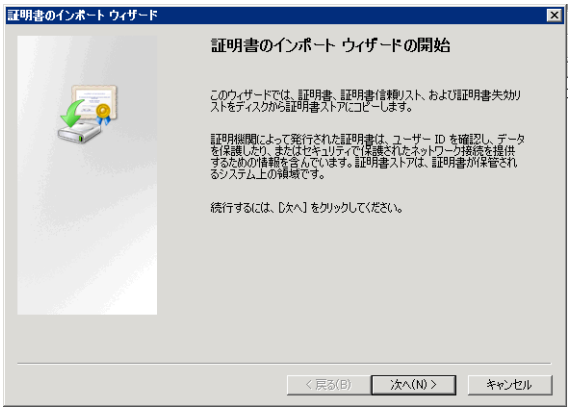
MMC（Microsoft Management Console）を開き、メニューの[ファイル(F)] > [スナップインの追加と削除(N)]より[証明書]を追加します。

「証明書のスナップイン」では、[コンピューター アカウント(C)]を選択し、次の「コンピューターの選択」では、[ローカルコンピューター(L)]を選択し、[完了]をクリックします。





スナップインが追加されたら左側のペインより[個人] > [証明書]と展開し、右側のペインで右クリックして、[すべてのタスク(K)] > [インポート(I)]をクリックします。「証明書のインポートウィザード」が開始されるので、サーバ証明書をインポートします。



ページ	設定
証明書のインポートウィザードの開始	[次へ(N)]をクリック
インポートする証明書ファイル	Gléas よりダウンロードした PKCS#12 ファイル

	（拡張子：p12）を指定して、[次へ(N)]をクリック
パスワード	Gléas から PKCS#12 ファイルをダウンロードする際に設定したパスワードを入力して、[次へ(N)]をクリック
証明書ストア	[証明書を次のストアへ配置する]を選択し、証明書ストアが[個人]となっている状態で、[次へ(N)]をクリック
証明書インポートウィザードの終了	[完了]をクリック

完了後、[個人]に Gléas よりダウンロードしたサーバ証明書がインポートされていることを確認します。もしここにルート証明書（発行先と発行者が同じ証明書）も追加されている場合は削除します。

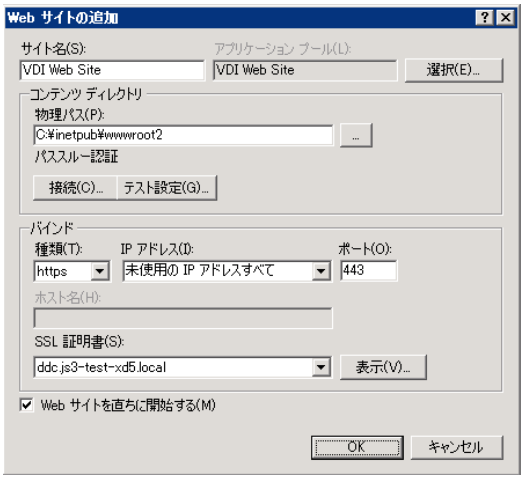
※以下で「WMsvc-…」という名前の証明書は Windows の WMSVC サービス（Web 管理サービス）により自動発行された自己署名証明書となりますが、今回は使用しません

3.3. Web サイトの作成

スマートカード認証・スマートカードパススルー認証のための Web サイトの作成を行います。

[インターネット インフォメーション サービス（IIS）マネージャー]を開き、左ペインで[サイト]を右クリックし、[WEB サイトの追加]を選択し、以下を設定します。

- [サイト名]には任意の名前を入力
- [物理パス]には作成する WEB サイトが利用する任意のディレクトリパスを入力
- [バインド]には、[種類(T):]に https を選択し、[利用する証明書(S):]に 3.2 項でインポートしたサーバ証明書を選択
- 他の項目は必要に応じ設定



3.4. XML の信頼ポリシーの構成

[Windows PowerShell]を開き、以下のコマンドレットを実行し、シトリックス用の Power Shell モジュールをロードします。

```
Asnp Citrix.*
```

※ロード完了後に以下コマンドレットを実行することで有効なコマンドレット一覧を参照可能なので、正しくロードされたかの確認ができます

```
Get-Command -Module Citrix.*
```

ロード完了後に以下のコマンドレットを実行します。

```
Set-BrokerSite -trustrequestssenttothexmlserviceport $true
```

正常終了を確認するためには以下のコマンドレットを実行します。

```
Get-BrokerSite
```

出力される結果に以下が含まれていることを確認します。

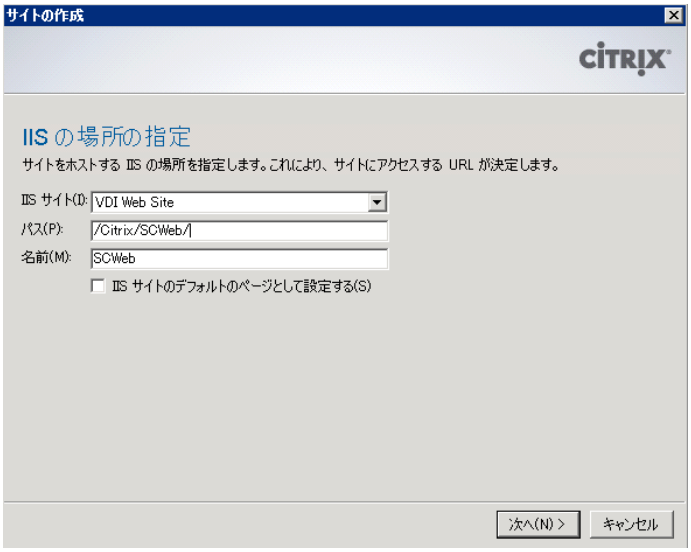
```
TrustRequestsSentToTheXmlServicePort     : True
```

3.5. Web Interface サイトの作成

3.5.1. Web サイトの作成

[Desktop Studio]を開いて、左ペインより[Access] > [Citrix Web Interface]を展開し、[XenApp Web サイト]を右クリック>[サイトの作成(C)]をクリックします。

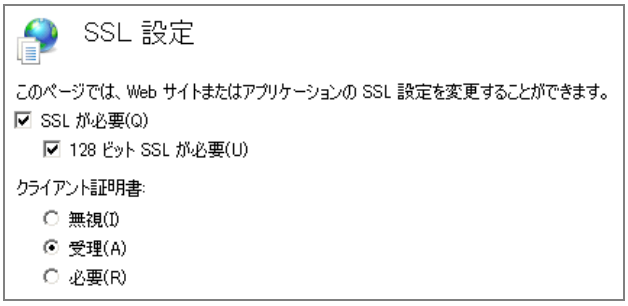
[サイトの作成]ウィザードが起動しますので、以下を設定します。



ページ	設定
IIS の場所の指定	1) [IIS サイト(I):]に 3.3 項で作成した Web サイト名を選択 2) [パス(P)]に任意のパス（例 : /Citrix/SCWeb/）を設定 上記を設定後、[次へ(N)]をクリック
認証ポイントの指定	[Web Interface]を選択し、[次へ(N)]をクリック
新しいサイトの設定の確認	設定内容を確認し、[次へ(N)]をクリック
サイトの作成	サイトの作成終了後、[すぐにこの Web サイトを設定する(C):]にチェックが入っていることを確認して、[次へ(N)]をクリック
サーバファームの指定	[サーバー（フェイルオーバー順）:(S)]欄で[追加(A)…]をクリックして、DDC のホスト名（今回は localhost）を追加し、[次へ(N)]をクリック
認証方法の設定	[スマートカード認証]を選択し、[次へ(N)]をクリック
ログオン画面の外観の指定	[完全(U):]を選択し（任意）、[次へ(N)]をクリック
公開リソースの種類の選択	[オンライン(O):]を選択し、[次へ(N)]をクリック
設定の確認	設定内容を確認し、[完了]をクリック

作成したサイトに対する SSL 設定を行います。
[インターネット インフォメーション サービス（IIS）マネージャー]の左ペインで、[Web サイト] > [（3.3 項で作成したサイト名）] > [（上記で作成したパス（例 : [Citrix] > [SCWeb]））]と展開し、右ペインで[SSL 認証]を開き、以下を設定します。

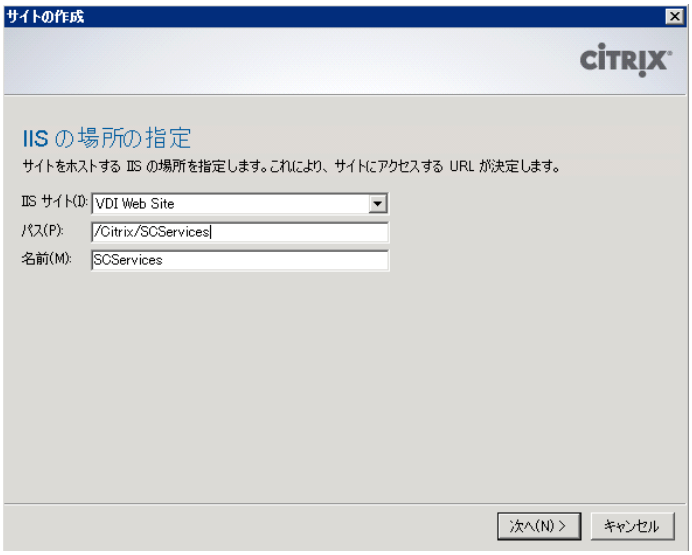
- [SSL が必要]にチェック。さらに[128 ビット SSL が必要]にもチェック
- [クライアント証明書]は[受理(A)]を選択



3.5.2. Service サイトの作成

[Desktop Studio]を開いて、左ペインより[Access] > [Citrix Web Interface]を展開し、[XenApp Service サイト]を右クリック>[サイトの作成(C)]をクリックします。

[サイトの作成]ウィザードが起動しますので、以下を設定します。

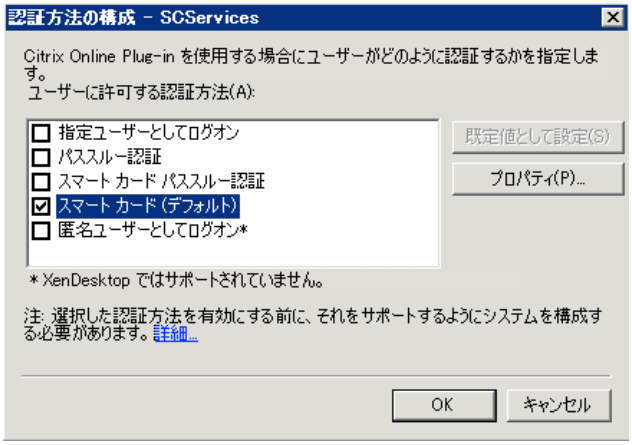


ページ	設定
IIS の場所の指定	1) [IIS サイト(I):]に 2.2 項で作成した Web サイト名を選択 2) [パス(P)]に任意のパス（例：/Citrix/SCServices/）を設定 上記を設定後、[次へ(N)]をクリック
新しいサイトの設定の確認	設定内容を確認し、[次へ(N)]をクリック
サイトの作成	サイトの作成終了後、[すぐにこの Web サイトを設定する(C):]にチェックが入っていることを確認して、[次へ(N)]をクリック

サーバファームの指定	[サーバー（フェイルオーバー順）:(S)]欄で[追加(A)…]をクリックして、DDC のホスト名（今回は localhost）を追加し、[次へ(N)]をクリック
公開リソースの種類の選択	[オンライン(O):]を選択し、[次へ(N)]をクリック
設定の確認	設定内容を確認し、[完了]をクリック

設定終了後、中央ペインに Service サイトが作成されたことを確認し、それを選択し、右ペインから[認証方法]をクリックします。
[認証方法の設定]ウィンドウが開きますので、以下を設定します。

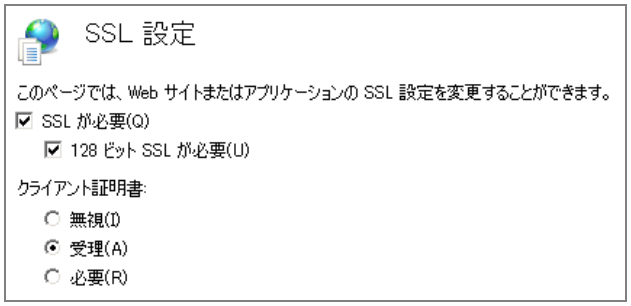
- [スマートカード認証]をチェック



設定完了後[OK]をクリックし、元の画面までに戻ります。

作成したサイトに対する SSL 設定を行います。
[インターネット インフォメーション サービス（IIS）マネージャー]の左ペインで、[Web サイト] > [（3.3 項で作成したサイト名）] > [（2.3.1 で作成したディレクトリ名（例：[Citrix] > [SCServices]））]と展開し、右ペインで[SSL 認証]を開き、以下を設定します。

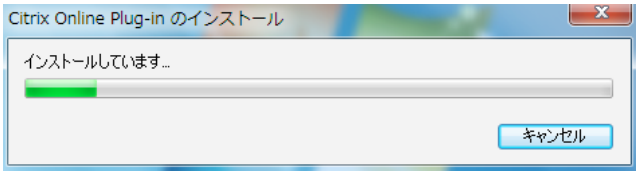
- [SSL が必要]にチェック。さらに[128 ビット SSL が必要]にもチェック
- [クライアント証明書]は[受理]を選択

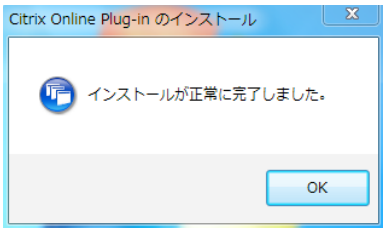


4. クライアントPCでの設定

4.1. Online Plug-in のインストール

*CitrixOnlinePluginFull.exe*を実行しインストールを行います。（Webブラウザのみを利用する場合は不要）





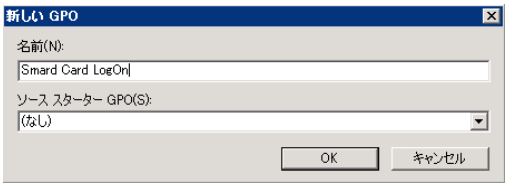
インストール終了後にサーバのURL入力を促すウィンドウが出現しますが、ここでは何も設定せずにウィンドウを閉じます。

5. ドメインコントローラでの設定

5.1. グループポリシオブジェクト（GPO）の追加

グループポリシのテンプレートファイル（icaclient.adm）により、設定を行います。icaclient.adm は Online Plug-in のインストールフォルダ配下の Configuration フォルダ配下に含まれます。
%SystemDrive%¥Program Files¥Citrix¥ICA Client¥Configuration¥icaclient.adm

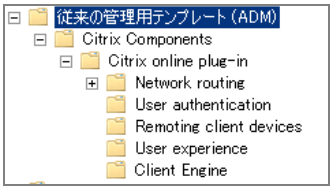
以下手順によりテンプレートを追加します。
[グループポリシー管理コンソール]を開き、左ペインでドメインの[グループポリシーオブジェクト]を選択し右クリックし、[新規(N)]を選択します。[新しい GPO]ウィンドウで新規作成する GPO の名前を任意に設定し、[OK]をクリックします。



作成した GPO を選択し、右クリックで[編集(E)...]を選択します。[グループポリシー管理エディター]が起動するので、左ペインで[ユーザーの構成] > [ポリシー] > [管理用テンプレート]と展開し右クリックし、[テンプレートの追加と削除(A)...]を選択します。

[テンプレートの追加と削除]ウィンドウで[開く(O)]をクリックし、icaclient.adm を指定します。

[管理用テンプレート]配下に以下のテンプレートが追加されます。



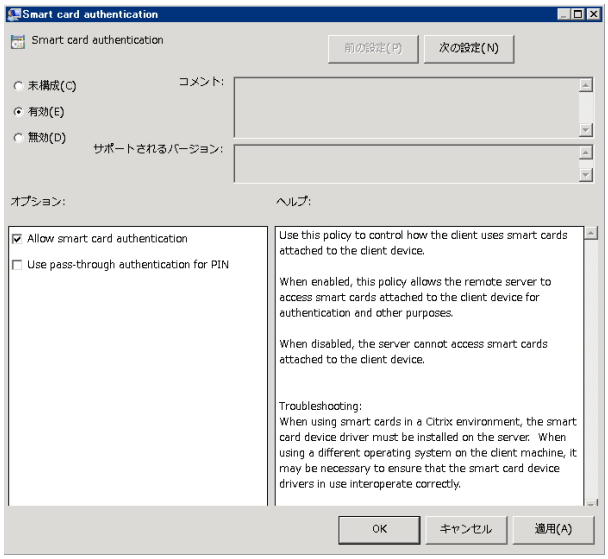
作成した GPO を選択し、今回の認証対象となるユーザが属する組織単位（OU）に適用（ドラッグアンドドロップ）します。

5.2. スマートカード認証の設定

作成した GPO を選択し、右クリックで[編集(E)...]を選択します。[グループポリシー管理エディター]が起動するので、左ペインで[ユーザーの構成] > [ポリシー] > [管理用テンプレート] > [従来の管理用テンプレート（ADM）] > [Citrix Components] > [Citrix online plug-in] > [User authentication]を展開し、右ペインで[Smart Card Authentication]を選択してダブルクリックします。

当該ポリシの編集画面が開くので以下の設定を行い、[適用(A)]をクリックします。

- [有効(E)]をチェック
- [Allow smart card authentication]を選択



6. Gléasでの認証デバイスの準備

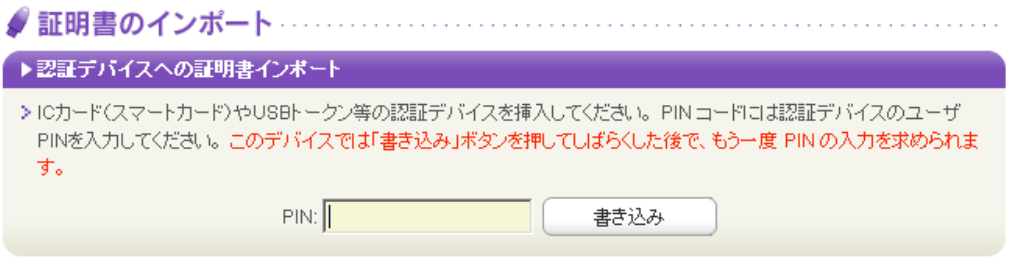
※Windowsスマートカードログオン構成時に認証デバイスを準備済みの場合は、本項目は不要

6.1. 認証デバイスへの電子証明書インポート

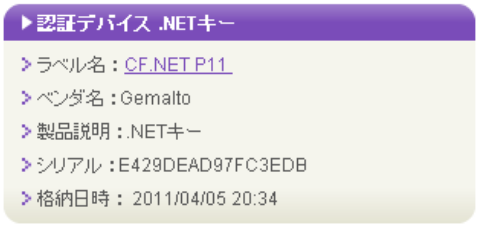
GléasのRAにログインし、スマートカード用に発行した証明書の詳細画面まで移動します。
エンドユーザ用の認証デバイスを管理者端末に接続し、画面上部の[トークンへのインポート]をクリックします。

※事前に認証デバイスのパーソナライズを行っている必要があります。

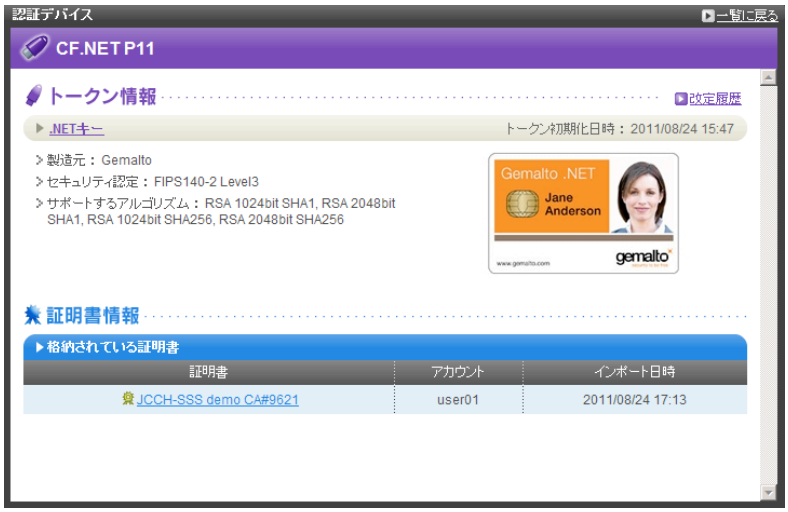
認証デバイスに事前に設定したPIN（暗証番号）を入力し、証明書のインポートを行います。



元の画面に戻ればインポートは成功です。
この時に画面を下にスクロールしていくと、インポート先のデバイス情報が付加されています。



また[認証デバイス]メニューでは、この認証デバイスにインポートした証明書を確認することが可能となります。



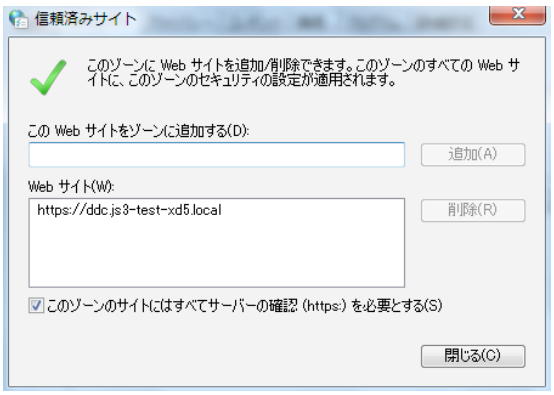
以上で、認証デバイスの準備は終了です。

※Gléasでは、パーソナライズした認証デバイスをエンドユーザに配布し、エンドユーザに証明書のインポートを行わせることも可能です。詳細はJS3までお問い合わせください

7. クライアントPCからのスマートカードログオン

7.1. スマートカード認証

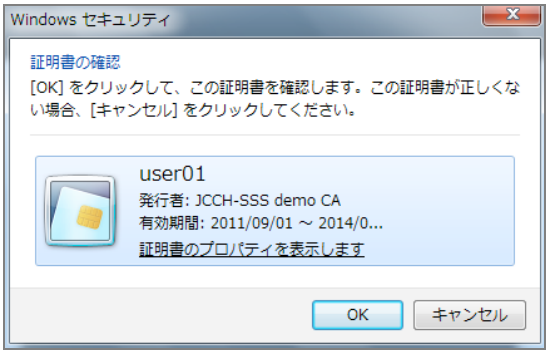
クライアント PC へのログイン後、コントロールパネル（或いは Internet Explorer）より[インターネットオプション]を開き、[セキュリティ]タブ > [信頼済みサイト] > [サイト(S)]をクリックし、信頼済みサイトに DDC のアドレス（FQDN）を追加します。



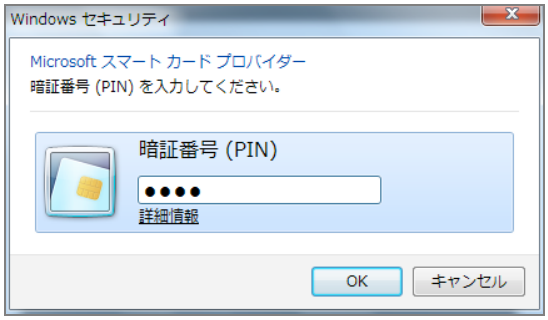
7.1.1. Web サイト

認証デバイスを PC にセットして、Internet Explorer から 3.5.3 項で設定した DDC のアドレスを入力します。

[証明書の確認]ウィンドウが表示されるので、認証デバイスにインポートされたクライアント証明書であることを確認して[OK]をクリックします。



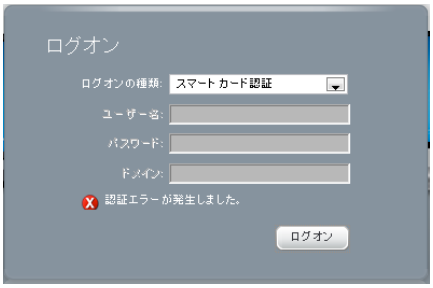
認証デバイスの PIN（暗証番号）を入力します。



DDC へのログインが完了するので、仮想デスクトップにアクセスします。

仮想デスクトップ上でスマートカードログオンを行います。再度 PIN を入力します。

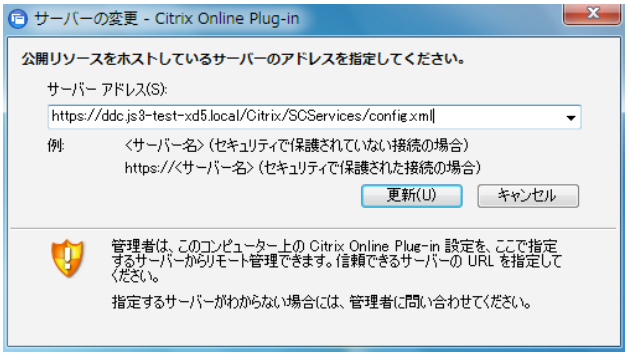
なお失効した証明書や、認証デバイスなしで DDC にログインしようとすると以下の画面になります。



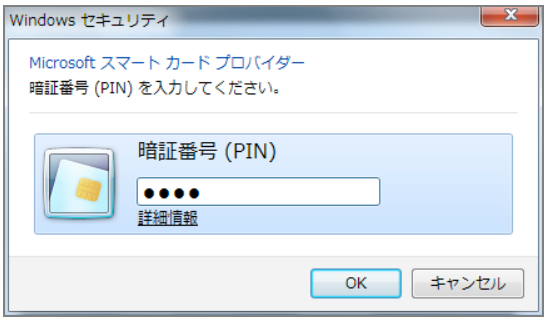
7.1.2. Services サイト

Citrix Online Plug-inを起動するとDDCのURLを求めるウィンドウが表示されるので、[今すぐにURLを入力します。(E)]をクリックします。

DDCのURLを入力し、[更新(U)]をクリックします。
https://（ホスト名）/（3.5.2で設定したパス）/config.xml



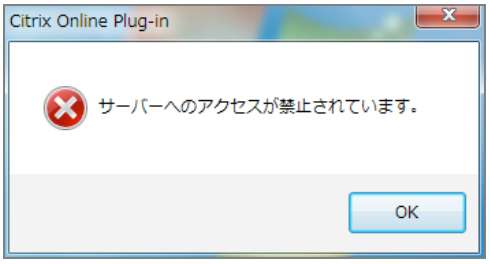
認証デバイスのPIN（暗証番号）を求められますので、PINを入力します。



タスクトレイ上のCitrix Online Plug-inアイコンを右クリックし、[デスクトップ] > [（デスクトップ名）]をクリックして、仮想デスクトップにアクセスします。

仮想デスクトップ上でスマートカードログオンを行います。再度 PIN を入力します。

なお、失効した証明書を格納する認証デバイスを用いて仮想デスクトップにアクセスすると以下メッセージが出現します。

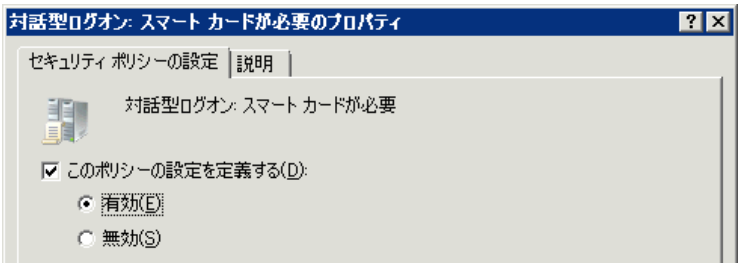


8. その他設定

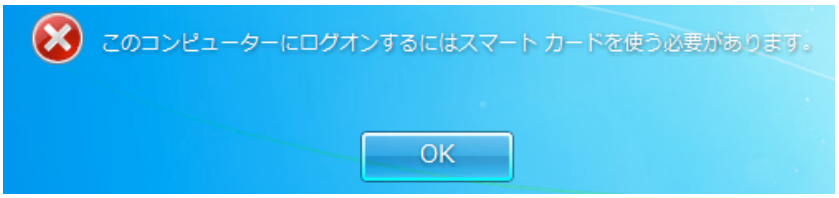
8.1. 仮想デスクトップのログオンをスマートカードに限定する設定

[スタートメニュー] > [管理ツール] > [グループポリシーの管理]を開き、対象となる仮想デスクトップに適用されるグループポリシーオブジェクトを選択し右クリックし、[編集]をクリックします。

グループポリシー管理エディターが開きますので、左側ペインより[コンピューターの構成] > [ポリシー] > [Windowsの設定] > [セキュリティの設定] > [ローカルポリシー] > [セキュリティオプション]を展開し、右側ペインの[対話型ログオン：スマートカードが必要]を有効に定義します。



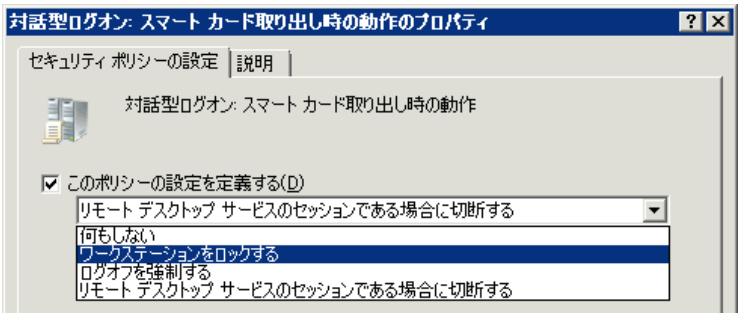
このポリシーが適用された仮想デスクトップでは、ユーザID・パスワードによるログオンが拒否されるようになります。



8.2. スマートカード取り出し時の動作の設定

[スタートメニュー] > [管理ツール] > [グループポリシーの管理]を開き、対象となる仮想デスクトップに適用されるグループポリシーオブジェクトを選択し右クリックし、[編集]をクリックします。

グループポリシー管理エディターが開きますので、左側ペインより[コンピューターの構成] > [ポリシー] > [Windowsの設定] > [セキュリティの設定] > [ローカルポリシー] > [セキュリティオプション]を展開し、右側ペインの[対話型ログオン：スマートカード取り出し時の操作]を以下のどれかに定義します。



ICカードの場合は、カードを抜いた際に設定した動作となります。
USBトークン（リーダー体型）のものには適用されないので、ご注意ください。

9. 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や検証用の証明書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