



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

Wyse シンククライアントでの

XenDesktopスマートカードログオン

Ver.1.0

2011年12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。

プライベート CA Gléas ホワイトペーパー  
Wyse シンククライアントでの Xen Desktop スマートカードログオン

## 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
2. Wyse シンククライアントの設定 .....	6
3. Gléas での認証デバイスの準備 .....	6
4. Wyse シンククライアントからの接続 .....	8
4.1. wnos.ini の取得設定 .....	8
4.2. 仮想デスクトップへの接続 .....	9
5. 問い合わせ .....	11

## 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、ワイズテクノロジー株式会社のシンククライアント端末（Wyse Thin OS）にてシトリックス・システムズ・ジャパン株式会社のXenDesktopで構築した仮想デスクトップへのスマートカードログオン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。

- 【シンククライアント】 Wyse C10LE （Wyse Thin OS (WTOS) 7.1\_033）  
※以後、「Wyseシンククライアント」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
- 【仮想デスクトップ基盤】 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
- 【仮想デスクトップ】 Microsoft Windows 7 Professional SP1  
※以後、「仮想デスクトップ」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。

- 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](http://www.jcch-sss.com/images/Windows_Smartcard_Logon_Gleas_Configuration.pdf)

- XenDesktop環境のセットアップ

※弊社のWEBサイトでは、XenDesktopでの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/service/support/2011/12/citrix-xendesktop-smartcard-logon>

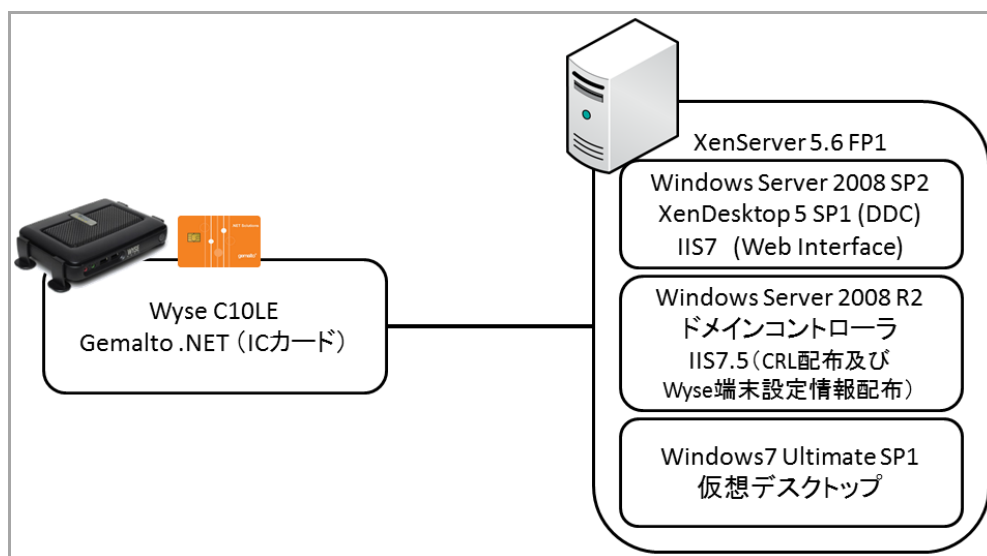
本環境では、上記ホワイトペーパーでのServiceサイトを利用しています

- 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
- WyseシンクライアントやWindowsでのネットワーク設定等の基本設定
- 認証デバイスのパーソナライズ等の基本操作

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. スマートカード証明書は、Gléasより発行して認証デバイスに格納する
2. Wyseシンクライアントは起動時にFTPサーバよりXenDesktopへの接続情報を受信する
3. XenDesktopにスマートカードを用いてログインする
4. 事前指定済みの仮想デスクトップに転送され、その仮想デスクトップへのログオンには認証デバイスを使用する (スマートカードログオン)

## 2. Wyse シンククライアントの設定

以下の記述を含む wnos.ini (Wyse シンククライアントの設定ファイル) を作成します。

```
SignOn=Yes ¥  
SCRemovalBehavior=1  
PNLiteServer=https://hostname/directory/config.xml  
AddCertificate=rootcert.crt
```

PNLiteServer パラメータでは、Web Interface の Service サイトの config.xml のパスを指定します。

AddCertificate パラメータでは、Gléas のルート証明書ファイル名を指定します。ルート証明書ファイルの拡張子は.crt である必要があるため、拡張子が.cer の場合は変更しておきます。

※本ホワイトペーパーでは、wnos.ini の詳細は説明しません。詳細に関してはワイズテクノロジー株式会社のサポートサイトをご参照ください

参考 URL : <http://www.wyse.com/kb>

wnos.ini を FTP サーバに以下の通りに配置します。

```
ftproot  
├─wnos  
│   └─wnos.ini  
└─cacerts  
    └─rootcert.crt
```

以上で、Wyse シンククライアントの設定は終了です。

## 3. Gléasでの認証デバイスの準備

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。

プライベート CA Gléas ホワイトペーパー  
Wyse シンククライアントでの Xen Desktop スマートカードログイン

✦ 証明書情報 ..... [トークンへのインポート](#) [ダウンロード](#) [タイムライン](#)

▶ [user01@is3-test.local](#) 開始日 : 2011/04/05 20:23 終了日 : 2014/04/05 20:23

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。

✦ 証明書のインポート .....

▶ 認証デバイスへの証明書インポート

▶ ICカード(スマートカード)やUSBトークン等の認証デバイスを挿入してください。PINコードは認証デバイスのユーザーPINを入力してください。このデバイスでは「書き込み」ボタンを押してしばらくした後で、もう一度 PIN の入力を求められます。

PIN:

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。

▶ 認証デバイス .NETキー

- ▶ ラベル名 : [CF.NET P11](#)
- ▶ ベンダ名 : Gemalto
- ▶ 製品説明 : .NETキー
- ▶ シリアル : E429DEAD97FC3EDB
- ▶ 格納日時 : 2011/04/05 20:34

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。

認証デバイス 二覧に戻る

✦ CF.NET P11

✦ トークン情報 ..... [設定履歴](#)

▶ .NETキー トークン初期化日時 : 2011/08/24 15:47

- ▶ 製造元 : Gemalto
- ▶ セキュリティ認定 : FIPS140-2 Level3
- ▶ サポートするアルゴリズム : RSA 1024bit SHA1, RSA 2048bit SHA1, RSA 1024bit SHA256, RSA 2048bit SHA256



✦ 証明書情報 .....

▶ 格納されている証明書

証明書	アカウント	インポート日時
✦ JCOH-SSS_demo_CA#9621	user01	2011/08/24 17:13

以上で、認証デバイスの準備は終了です。

プライベート CA Gléas ホワイトペーパー  
Wyse シンククライアントでの Xen Desktop スマートカードログオン

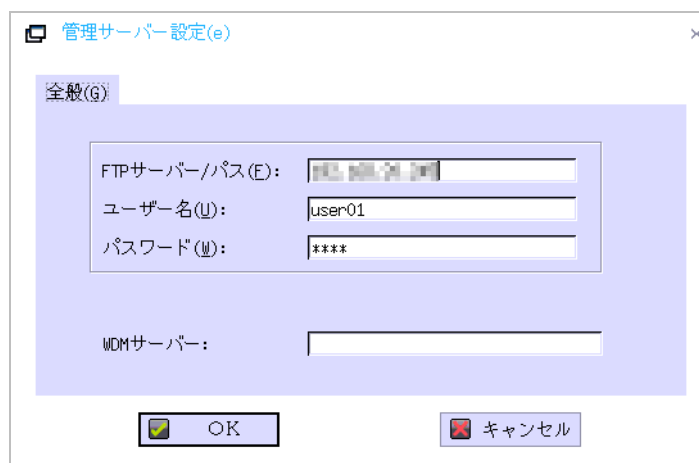
※Gléasでは、パーソナライズした認証デバイスをエンドユーザに配布し、エンドユーザに証明書のインポートを行わせることも可能です。詳細はJS3までお問い合わせください

## 4. Wyseシンククライアントからの接続

### 4.1. wnos.ini の取得設定

Wyseシンククライアントのメニューより、[システム情報(S)] > [管理サーバ設定(e)] を選択します。

FTPサーバへの接続情報を設定します。



管理サーバ設定(e)

全般(G)

FTPサーバ/パス(E): [masked]

ユーザー名(U): user01

パスワード(P): \*\*\*\*

WDMサーバ: [empty]

OK キャンセル

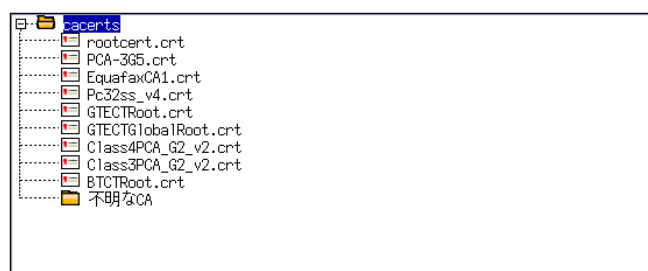
Wyseシンククライアントの起動後に、自動的にwnos.iniを読み込み設定が反映されます。

※XenDesktopへの接続設定は、wnos.iniよりおこなわれています。メニューより、[システム設定] > [リモート接続設定] > [ブローカー(B)]タブより確認できます。

## プライベート CA Gléas ホワイトペーパー Wyse シンククライアントでの Xen Desktop スマートカードログオン



※メニューより[システム設定] > [ネットワーク設定] > [認証(e)]タグ > [証明書管理(f)]より証明書ブラウザを開くと、ルート証明書（下の図ではrootcert.crt）もインポートされていることがわかります。

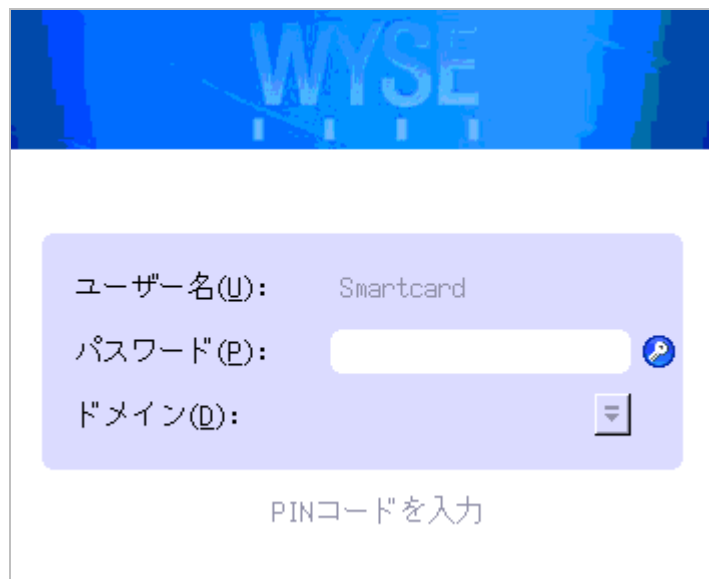


### 4.2. 仮想デスクトップへの接続

Wyseシンククライアントを起動し、認証デバイスをセットしておくことでXen Desktopへのログオン画面が表示されます。

[パスワード(P) : ]に、認証デバイスのPINを入力します。

プライベート CA Gléas ホワイトペーパー  
Wyse シンククライアントでの Xen Desktop スマートカードログオン



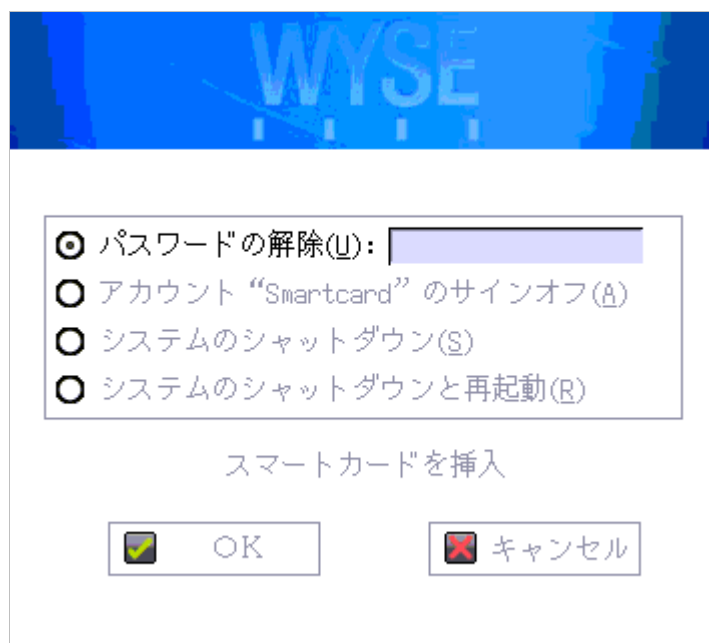
The image shows a login window with a blue header containing the 'WYSE' logo. Below the header is a light purple rounded rectangle containing the following fields:

- ユーザー名(U): Smartcard
- パスワード(P): [Redacted] with a blue key icon to the right.
- ドメイン(D): [Redacted] with a dropdown arrow icon to the right.

Below these fields, the text 'PINコードを入力' (Enter PIN code) is displayed.

ログインに成功すると、そのまま仮想デスクトップに転送され、自動的にスマートカードによるログオンがおこなわれます。

認証デバイスを外すと仮想デスクトップとのセッションが切断され、以下の画面が表示されます。



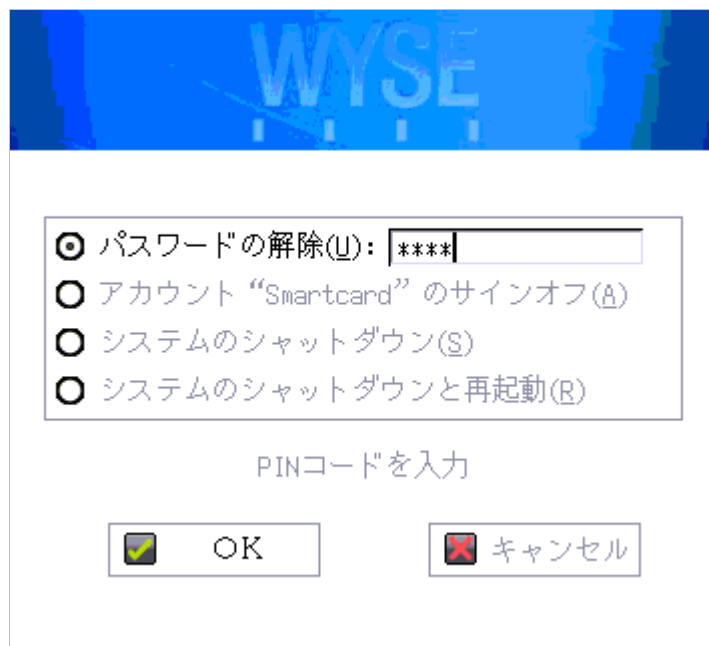
The image shows a dialog box with a blue header containing the 'WYSE' logo. Below the header is a white rounded rectangle containing the following options:

- パスワードの解除(U): [Redacted]
- アカウント "Smartcard" のサインオフ(A)
- システムのシャットダウン(S)
- システムのシャットダウンと再起動(R)

Below these options, the text 'スマートカードを挿入' (Insert smartcard) is displayed.

At the bottom, there are two buttons: 'OK' with a checkmark icon and 'キャンセル' (Cancel) with a red X icon.

再度認証デバイスをセットすると、PIN入力を求められます。  
PINを入力すると直前のセッションが再開されます。



※Windowsのグループポリシーの[対話型ログオン: スマートカード取り出し時の操作]は、何もしていない状態になっている必要があります

## 5. 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: 03-5615-1020

Mail: support@jcch-sss.com