

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

- 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.	Gléas で事前発行する電子証明書	6
2. 仮想	デスクトップでの設定	6
2.1.	スマートカードドライバのインストール	6
3. DDC	こでの設定	7
3.1.	IIS への役割の追加	7
3.2.	サーバ証明書のインポート	8
3.3.	Web サイトの作成	10
3.4.	XML の信頼ポリシーの構成	11
3.5.	Web Interface サイトの作成	11
3.5.	1. Web サイトの作成	11
3.5.	2. Service サイトの作成	13
4. クラ	イアント PC での設定	
4.1.	Online Plug-in のインストール	15
5. ドメ	インコントローラでの設定	15
5.1.	グループポリシオブジェクト(GPO)の追加	15
5.2.	スマートカード認証の設定	16
6. Gléa	as での認証デバイスの準備	17
6.1.	認証デバイスへの電子証明書インポート	17
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	
7.1.	1. Web サイト	19
7.1.	2. Services サイト	20
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	22
8.2.	スマートカード取り出し時の動作の設定	23
9. 問い	合わせ	24

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。

	👆 🛃	キュリティ	インストール済み
i	₽	基本認証	インストール済み
	₽	Windows 認証	インストール済み
Γ		ダイジェスト認証	インストールされていません
li	L	クライアント証明書のマッピング認証	インストール済み
		IIS クライアント証明書のマッピング認証	インストールされていません
		URL 承認	インストールされていません
l	_	要求フィルタ	インストール済み
Ľ		IP およびドメインの制限	インストールされていません

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。

1 認証		
グループ化: グループ化なし 🔹		
名前 ^	状態	応答の種類
Active Directory クライアント証明書の認証	有効	HTTP 401 チャレンジ
ASP.NET 偽装	無効	
Windows 認証	無効	HTTP 401 チャレンジ
フォーム認証	無効	HTTP 302 ログイン/リダイレクト
基本認証	無効	HTTP 401 チャレンジ
匿名認証	無効	

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。

5(B)	<u>;</u> ≵∧(N)>	<u>++>>t01</u>
5(B)	· 法へ(N) >	<u>キャンセル</u>
5(B)	·汝へ(N) >	<u>キャンセル</u>
5(B)	<u>沐へ(N) 〉</u>	+++>\textrm{ten}
5(B)	·法へ(N) >	<u>++v\tzu</u>
5(B)		*#21214
δ(B)	· 次へ(N) >	
δ(B))次へ(N) >	
5(B)	·次へ(N) >	キャンセル
5(B)	· 次へ(N) >	++>\t11
5(B)	`次へ(N) >	キャンセル
5(B)	`;≿^(N)>	+++>>DUI
5(B)	法へ(N) >	キャンセル
5(B))次へ(N) >	++>UUI
-/2)		
-/2)		
-&-)		
-/2)		
-x-)		
- · ·		
		参照(R)
できるようにす	する(W)	
Ċ	きるように	きるようにする(W)

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
	2
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

発行先 🔺	発行者	有効期限	目的	フレンドリ名
🔄 ddc.js3-test-xd5.local	JCCH-SSS demo CA	2014/09/03	サーバー認証、クライア	ddc.js3-test-xd5.local
🛱 WMSvc-DDC	WMSvc-DDC	2021/08/30	サーバー認証	〈なし〉

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



サイトを(S): アブリケーション ブール(L): VDI Web Site VDI Web Site 選択(E) コンテンツ ディレクトリー 物理パス(P): C:*inetpub#wwwroot2 パススルー経証 接続(C) テスト設定(G) ディンド 種類(T): IP アドレスロン: ポート(O): https ▼ 床使用の IP アドレスすべて ▼ [443 ホストを(H): SSL 証明書(S): ddc.js3-test-xd5.local ▼ 表示(V) ▼ Web サイトを直ち(C開始する(M)	Web サイトの追加 ?×			
VDI Web Site 図訳(E) コンテンツ ディレクトリー 物理パス(P): 「シオージンジー 「C-¥inetpubЧwwwroot2 パイスルー認証 接続(C) テスト設定(G) パインド 「指気(T): IP アドレス(D): ボート(O): 「https: 「未使用の IP アドレスすべて ▼ SSL 証明書(S): ddc.js3-test-xd5.local ▼ ▼ ▼ Web サイトを直ち(こ開始する(M)	サイト名(S): アプリケーション ブール(L):			
コンテンツ ディレクトリ 物理パス(P): ○¥imetpub¥wwwroot2 パススルー記証 接続(C)	VDI Web Site			
C:¥inetpub¥wwwroot2 パススルー起証 接続(C)_ テスト設定(G)_ 「バインド 種類(T): IP アドレス(D: ポート(O): https ▼ 床使用の IP アドレスすべて ▼ 443 ホスト名(H) SSL 証明書(S): ddc js3-test-xd5 local ▼ 表示(V)_ ▼ Web サイトを直ち(C開始する(M)	コンテンツ ディレクトリー			
/パススルー認証 接続(C) テスト設定(G) -/パンド 種類(T): IP アドレス(D: ボート(O): https ▼ 床使用の IP アドレスすべて ▼ 443 ホスト-8(H). SSL 証明書(S): ddc.js3-test-xd5.local ▼ 表示(V) ▼ Web サイトを直ち(c間始する(M)	C:¥inetpub¥wwwroot2			
接続(C) テスト設定(G)	パススルー記証			
バインド アドレス(D): ボート(O): https 床使用の IP アドレスすべて [443] ホスト名(H): SSL 証明書(S): [ddc.js3-test-xd5.local] 夏元(V) 「Web サイトを直ち(ご開始する(M) [4] [4] [4]	接続(C) テスト設定(G)			
種類(T): IP アドレス(D): ポート(O): https ▼ 床使用の IP アドレスすべて ▼ 443 ホスト名(H) SSL 証明書(S): ddc js3-test-xd5.local ▼ 表示(V) ▼ Web サイトを直ち(C開始する(M)	バインド			
https 床使用の IP アドレスすべて [443] ホスト名(H)	種類(T): IP アドレス(I): ポート(O):			
ホスト名(H): SSL 証明書(S): ddc js3-test-xd5 Jocal ▼ 表示(V)	https 💌 未使用の IP アドレスすべて 💌 443			
SSL 証明書(S): ddc.js3-test-xd5.local マ Web サイトを直ちに開始する(M)	ホスト名(H):			
SSL 証明書(S): ddc.js3-test-xd5.local 支示(V) マ Web サイトを直ちに開始する(M)				
ddc.js3-test-xd5.local ▼ Web サイトを直ちに開始する(M)	SSL 証明書(S):			
· · · · · · · · · · · · · · · · · · ·	ddc.js3-test-xd5.local			
✓ Web サイトを直ちに開始する(M)				
	✓ Web サイトを直ちに開始する(M)			
OK キャンセル	OK キャンセル			

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。

		CİTRI
ട്ര ത:	場所の指定	
サイトをホン	マリアルマリコース」 ストする IIS の場所を指定します。これにより、サイトにアクセスする URL が決定します。	
us サイト(I	VDI Web Site	
パス(P):	/Citrix/SCWeb/	
名前(M):	SCWeb	
	□ IS サイトのデフォルトのページとして設定する(S)	

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]))]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。

ና トの作成	
	CİTRİX
IIS の提所の指定	
サイトをホストする IIS の場所を指定します。これにより、サ	イトにアクセスする URL が決定します。
M2(P): //Citrix/SCServices	<u> </u>
名前(M): SCServices	
	次へ(N) > キャンセル

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

認証方法の構成 - SCServices	×
Citrix Online Plue-in を使用する場合にユーザーがどのよう す。 ユーザーに許可する認証方法(A):	に認証するかを指定しま
□ 指定ユーザーとしてログオン	既定値として設定(S)
□ パススルー認証 □ スマート カード パススルー認証	プロパティ(P)
 ✓ スマートカード (デフォルト) ■ 匿名ユーザーとしてログオン* 	
* XenDesktop ではサポートされていません。	
注: 選択した認証方法を有効にする前に、それをサポートす る必要があります。 <mark>詳細</mark> .	るようにシステムを構成す
	OK キャンセル

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)

Citrix Online Plug-in のインストール	
インストールしています	キャンセル
Citrix Online Plug-in のイン	ンストール × 正常に完了しました。
	ОК

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。

プライベート CA Gléa	as ホワイ	トペーパー
XenDesktop スマー	トカード	ログオン

新しい GPO	X
名前(N):	
Smard Card LogOn	
(なし)	•
	OK キャンセル

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。

テンプレートの追加と削除 現在のポリシー テンプレート(C):	×
名前 a icaclient	サイズ 変更 19KE 2010/08/02 2241
送加(A)	開じる(L)

[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。

-	Ē	従来の管理用テンプレート (ADM)	
	-	🧮 Citrix Components	
		🖃 🚞 Citrix on line plug-in	
	🕀 🚞 Network routing		
	🧮 User authentication		
	🦳 Remoting client devices		
		🧮 User experience	
		🧮 Client Engine	
_			

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



Smart card authentication	
Smart card authentication	前の設定(P) 次の設定(N)
○ 末機成(C) コメント: ○ 有効(E) ○ 預効(D) サポートされるパージョン:	* * * *
オプション:	ヘレプ:
₩ Allow smart card authentication □ Use pass-through authentication for PIN	Use this policy to control how the dient uses smart cards attached to the client device. When enabled, this policy allows the remote server to access smart cards attached to the dient device for authentication and other purposes. When disabled, the server cannot access smart cards attached to the client device. Troubleshooting: When using smart cards in a Citrix environment, the smart card device driver must be installed on the server. When using a different operating system on the client machine, it may be necessary to ensure that the smart card device drivers in use interoperate correctly.
	OK キャンセル 適用(A)

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。

★ 証明書情報 ······	
▶ <u>user01@js3-test.local</u>	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ボート
> 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□コは認証デバイスのユーザ 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。 す。
PIN: e書き込み

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: <u>CF.NET P11</u>
> 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		D <u>一覧に戻る</u>
🔗 CF.NET P11		
▶ <u>.NET+</u>		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 > サポートするアルニリズム: RSA 1024bit SHA1, RSA 2048bit SHA1, RSA 1024bit SHA256, RSA 2048bit SHA256 業 証明書情報		Gemalto .NET Anderson Jane Anderson gemaltor we geneticon
▶格納されている証明書		
証明書	アカウント	インボート日時
R JCCH-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。

※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。

Windows セキュ	IJティ Х
Microsoft ス국 暗証番号 (PIN	マート カード プロバイダー)) を入力してください。
	暗証番号 (PIN) ●●●● 詳細情報
	OK キャンセル

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。

ログオン		
ログオンの種類:	スマート カード認証	-
🗙 認証エラーカ		
		ログオン

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。

Citrix Online Plug-in
ジ サーバーへのアクセスが禁止されています。
ок

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。

対話型ログオン: スマート カードが必要のブロパティ	? ×
セキュリティポリシーの設定 説明	
対話型ログオン: スマート カードが必要	
☑ このポリシーの設定を定義する(D):	
● 有効(E)	
○ 無効(S)	

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。

20コンピューターにログオン	するにはスマート カードを使う必要があります。
	ОК

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。

対話型ログオン: スマート カード取り出し時の動作のプロパティ	? ×
セキュリティ ポリシーの設定 説明	
対話型ログオン・スマート カード取り出し時の動作	
☑ このポリシーの設定を定義する(D)	
リモート デスクトップ サービスのセッションである場合に切断する	
何もしない	
ログオフを強制する リモート デスクトップ サービスのセッションである場合に切断する	

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