

プライベートCA Gléas ホワイトペーパー

Windowsスマートカードログオン

Ver.1.2 2011 年 9 月

Copyright by JCCH Security Solution Systems Co., Ltd., All Rights reserved

- 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. はじる	めに4
1.1.	本書について
1.2. 1.3.	本書における環境
2. ドメ-	インコントローラでの設定5
2.1.	サーバ証明書のインポート5
2.2.	ルート証明書のエクスポート8
2.3.	NTauth ストアへのインポート8
2.4.	グループポリシーの設定9
3. Gléas	s での認証デバイスの準備10
3.1.	認証デバイスへの電子証明書インポート10
4. クライ	イアント PC での作業12
4.1.	認証デバイスのセットアップ12
4.2.	スマートカードログオンの利用12
5. その(也設定13
5.1.	クライアント PC のログオンをスマートカードに限定する設定
5.2.	スマートカード取り出し時の動作の設定14
5.3.	スマートカードログオンが有効な PC にリモートデスクトップをする設定15
5.4.	特定のユーザに対しスマートカードログオンを強制する設定
6. 問い	合わせ

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、Microsoft CorporationのWindows 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。

- 【ドメインコントローラ】Microsoft Windows Server 2008 R2 Standard SP1
 ※以後、「ドメインコントローラ」と記載します
- 【認証局】JS3 プライベートCA Gléas (バージョン1.7)
 ※以後、「Gléas」と記載します
- 【クライアントPC】Microsoft Windows 7 Professional SP1
 ※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
 ※.NET製品には、ICカードタイプとUSBトークンタイプがあり、どちらでも同様の動作となります(サードパーティのICカードリーダのインストールを除く)
 ※本環境では、ICカードリーダにGemalto PC Twin Reader (USB接続)を利用しています

以下については、本書では説明を割愛します。

- ・ドメインコントローラのセットアップ
- 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. 電子証明書の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。

 ドメインコントローラ証明書の発行には、「Microsoftドメインコントローラ」 テンプレートを用います。その際には、ドメインコントローラのホスト名、 CRL配布ポイント、GUID(Global Unique Identifier)を正しく設定する必要 があります

以下は「dc01.js3-test.local」という名前のドメインコントローラ上でGUIDを取得するVBスクリプト サンプルです。

Set objUser = GetObject("LDAP://CN=dc01,OU=Domain Controllers,DC=js3-test,DC=local") Wscript.Echo objUser.GUID

スマートカード用証明書の発行には、「スマートカードログオン」テンプレートを用いて証明書を発行します。その際には、UPN(ユーザプリンシパル名)、CRL配布ポイントを正しく設定する必要があります

2. ドメインコントローラでの設定

2.1. サーバ証明書のインポート

ドメインコントローラにドメインコントローラ証明書と、今回利用するクライアン ト証明書のトラストアンカとなるルート証明書をインポートします。

ドメインコントローラで 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。

このスナップインで管理する証明書: ① ユーザー アカウンド(M) ① サービス アカウンド(S) ④ コンピューター アカウンド(C)		
○ ユーザー アカウンド(M) ○ サービス アカウンド(S) ⓒ コンピューター アカウンド(O)		
○ サービス アカウント(S) ◎ コンピューター アカウント(O)		
○ ユンピューター アカウント(C)		
_	< 戻る(8) 次へ(N) 2	キャンセル
レビューターの選択		
この人ナッノインに管理するコンピューターを選択してくたさい。		
○ ローカル コンピューター(1) (2のコンノールを実行しているコ	/ピューター)	
		会昭(中)
		3-4601A
コマンド ラインから起動したときは選択されたコンピューター これは、コンソールを保存した場合にのみ適用されます。	E変更できるようにする(W)	
	/ 百支(1) 「一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	الطرديط

スナップインが追加されたら左側のペインより[証明書] > [個人]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、サーバ証明書とルート証明 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
	<i>7</i>
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	[証明書をすべて次のストアへ配置する(P)]を選
	択し、[証明書ストア]で[個人]が選ばれているこ
	とを確認し、[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ドメインコントローラ用証明書と、 Gléas のルート証明書(発行元と発行先とが同じ名前の証明書)がインポートされ ていることを確認します。

帰コンソール1 - ロンソール ルート¥証明書 (ローカルコンピューター)¥個人¥証明書]							
🚘 ファイル(F) 操作(A) 表示(V) お気に入り(O) ウィンドウ(W) ヘルプ(H)							
🗢 🔿 🙍 🖬 📋 🙆 😹 👔							
📔 コンソール ルート	発行先 🔺	発行者	有効期限	目的	フレンドリ名	状態	証明書テンプレート
🖂 🔜 証明書 (ローカル コンピューター)	😨 dc01.js3-test.local	Gleas Generic CA	2013/07/02	クライアント認証、サー	dc01.js3-test.local		DomainController
🗉 🚞 個人	🗒 Gleas Generic CA	Gleas Generic CA	2013/07/03	〈すべて〉	<なし>		
🧰 証明書							
🗉 🚞 信頼されたルート証明機関							
⊡ エンタープライズの信頼							
🗉 🚞 中間証明機関							
🗉 🚞 信頼された発行元							
🗉 🚞 信頼されていない証明書							
🗉 🚞 サード パーティ ルート証明機関							
🗉 🚞 信頼されたユーザー							
표 🚞 Remote Desktop							
🗉 🚞 証明書の登録要求							
🗉 🚞 スマート カードの信頼されたルー							
🗉 🚞 信頼されたデバイス							

2.2. ルート証明書のエクスポート

次に、ルート証明書をファイルとして取得します。 ※既に Gléas よりルート証明書をダウンロードしてある場合は、エクスポートを行う必要はあり ません。この場合はルート証明書を削除して 2.3 に進んでください。

インポートされた Gléas のルート証明書を右クリックし、[すべてのタスク(K)] > [エ クスポート(E)]をクリックします。「証明書のエクスポートウィザード」が開始され るので、ルート証明書をエクスポートします。



ページ	設定
証明書のエクスポートウィザードの開始	[次へ(N)]をクリック
エクスポートファイルの形式	DER encoded binary X.509(.CER)か、Base64
	encoded X.509(.CER)を選択し、[次へ(N)]をクリ
	ック
エクスポートするファイル	保存先を指定して、[次へ(N)]をクリック
証明書エクスポートウィザードの終了	[完了]をクリック

エクスポートが終了したら、[個人]に入っているルート証明書は不要なため削除します。

2.3. NTauth ストアへのインポート

次に、Windows ドメインとして信頼するルート認証局の証明書を NTauth ストアと

呼ばれる格納領域に登録します。

コマンドプロンプトを開き、以下のコマンドを入力し NTauth ストアにルート証明 書を格納します。

certutil -dspublish -f [filename] NTAuthCA

※[filename]には、エクスポートしたルート証明書を指定します。

コマンド実行後、以下のレジストリにルート証明書の拇印と同じ名前のレジストリ キーが追加されます。

HKLM¥SOFTWARE¥Microsoft¥EnterpriseCertificates¥NTAuth¥Certificates ※追加されない場合は、gpupdate コマンドでポリシーの更新を行ってください。

🖃 🌗 EnterpriseCertificates
🕀 📲 CA
🕀 🎴 Disallowed
🖃 🎴 NTAuth
🗄 📲 Certificates
614A68C8AED89B800D1CB1ED57C703B7C8445E9B
CRLs
CTLs

E明書	Б
全般 詳細 証明のパス	
表示(S): <すべて>	•
,	
フィールド	
■■「「「」」を一使用法	Digital Signature, Certificate Signing, Off-lin
🛐 Netscape 証明書の種類	SSL CA, SMIME CA (06)
🐻 Netscape コメント	Private CA Gleas
	Subject Type=CA, Path Length Constraint=0
■ 1月60アルゴリズム	sha1
画 拇印	61 4a 68 c8 ae d8 9b 80 0d 1c b1 ed 57 c7 (—
	V
	<u>•</u>
61 4a 60 a0 aa d0 0b 00 0d 1a	h1 ad E2 a7 00 b7 a0 44 Ea 0b
	D1 EG 37 C7 03 D7 C8 44 3E 3D
,	
	プロパティの編集(E) ファイルにコピー(C)
証明書の詳細について表示します。	
	OK

2.4. グループポリシーの設定

ドメインに参加しているコンピューターに対して信頼するルート認証機関を追加す る設定を行います。

[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 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。

III グループ ポリシーの管理 □ A フォレスト: js3-test.local	Default スコープ	:Domain Policy 詳細 設定 委任		
□ 🙀 js3-test.local	リンク			
厨 Default Domain P ⁺⁺ 編集(E)	1	リンクの場所(L):	js3-test.local	
■ ご じのの間に Controller 強制(N) ■ ご グループ ポリシー オ 、 いっかの有効(F(1)))	、ドメイン、および OU がこの GPO	にリンクされています(T)	t
田 📑 WMI フィルター レポートの保存(S	, .)		強制 リンク	の有効化パス
田 福 サイト 酸 グループ ポリシーのモデル作 ここから新しいウィ	▶ ンドウ(W)	test.local	() (J()	js3-test.local
ろ グループ ポリシーの結果 育明余(D) 名前の変更(M) 最新の情報に更	新(F)			
ヘノレプ(H)				

以下は Default Domain Policy を編集する場合の例です。

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] > [公開キーのポリ シー] > [信頼されたルート証明機関]を開きます。

次にメニューより[操作(A)] > [インポート(I)]を選択すると、証明書のインポートウ ィザードが起動するので、ルート証明書を登録します。

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	エクスポートしたルート証明書ファイルをを選		
	択し、[次へ(N)]をクリック		
証明書ストア	[証明書をすべて次のストアへ配置する(P)]を選		
	択し、[証明書ストア]で[信頼するルート認証機		
	関]が選ばれていることを確認し、[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		

以上でWindows Serverの設定は完了です。

3. Gléasでの認証デバイスの準備

3.1. 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 コードに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。
PIN: 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		▶ <u>一覧に戻る</u>
CF.NET P11		
		▲ ····· <u>] 改定履歴</u>
▶ <u>.NETキー</u>	トークン初	期化日時:2010/12/10 09:36
> 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, SHA256, RSA 2048bit SHA256 業 証明書情報	, RSA 2048bit SHA1, RSA 1024bit	Gemalto .NET Jane Anderson we genetico
▶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
😤 JCCH-SSS demo CA#9326	user01@js3-test.local	2011/04/05 20:34
		v

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

4. クライアントPCでの作業

4.1. 認証デバイスのセットアップ

認証デバイスのドライバインストールを行います。 詳細は弊社提供のマニュアル等を参照してください。

なお、Widnows7では認証デバイスを挿した状態でクライアントPCを起動するとロ グオン前に自動的にドライバ類のインストールが行われます(要インターネット接 続)。



4.2. スマートカードログオンの利用

ドライバがインストールされた状態でクライアントPCを起動すると、認証デバイス が自動的に読み込まれログオンユーザ名が表示されるのでクリックします。 ※これまでログオンしていたユーザでのログオン画面が表示される場合は、[ユーザの切り替え (W)]をクリックし、スマートカードログオンするユーザを選択します(この時、認証デバイスは クライアントPCに挿しておきます)。



ログオン画面が表示されるので、認証デバイスに予め設定しているPINを入力して ログオンします。



失効しているスマートカード証明書でログオンしようとすると、以下のメッセージ が表示されエラーとなります。



5. その他設定

5.1. クライアント PC 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 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 カードが必要のフロバティ	? ×
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(3)	

このポリシーが適用されたクライアントPC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

5.2. 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 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	? ×
セキュリティボリシーの設定 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5年制する 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	

このポリシーはSmart Card Removal Policyサービスが起動していないと動作しな いので、このサービスも自動起動するようにします。 グループポリシー管理エディターで、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] > [システム サービス]と展開し、右側ペインでSmart Card Removal Policyを自動起動するよう定義します。

Smart Card Removal Policyのプロパティ	? ×
セキュリティポリシーの設定	
Smart Card Removal Policy	
☑ このポリシーの設定を定義する(D)	
サービスのスタートアップ モードを選択してください:	
€ 自動(1)	
○ 手動(<u>M</u>)	
○ 無効(S)	
セキュリティの編集(<u>E</u>)	

このポリシーをクライアントPCに適用すると、定義した通りの動作を行います。

5.3. スマートカードログオンが有効な PC にリモートデスクトップを

する設定

※同じドメインに参加しているPCより行ってください

リモートデスクトップ接続を起動し、[オプション] > [ローカルリソース]タブ > ロ ーカルリソースとデバイスの[詳細]をクリックし、開いた画面で[スマートカード(M)] にチェックを入れ、接続します。



「資格情報を入力して下さい」というダイアログボックスが表示されたらスマート カードを選択し、PINを入力しログオンします。



5.4. 特定のユーザに対しスマートカードログオンを強制する設定

[スタートメニュー] > [管理ツール] > [Active Directory ユーザーとコンピューター]を開き、 対象となるユーザオブジェクトを選択し右クリックし、[プロパティ(R)]をクリックしま す。

そのユーザのプロパティが開きますので、 [アカウント]タブをクリックし [アカウント オプション(O):]項目の[対話型ログオンにはスマートカードが必要]にチェックを入れま す。

アカウント オプション(0):	
□ 暗号化を元に戻せる状態でパスワードを保存する	
「 アカウントは無効	
▼ 対話型ログオンにはスマート カードが必要	
□ アカウントは重要なので委任できない	-
 ✓ 対話型ログオンにはスマート カードが必要 ✓ アカウントは重要なので委任できない 	-

この設定がされたユーザアカウントでは、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。



6. 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