

プライベートCA Gléas ホワイトペーパー

~Windows Server (ネットワークポリシーサーバー) ~

スマートデバイスでの802.1x EAP-TLS設定手順

Ver.1.0 2012 年 8 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. はじる	めに4
1.1.	本書について
1.2.	本書における環境4
1.3.	本書における構成
1.4.	電子証明書の発行時における留意事項5
2. ドメ・	インコントローラでの設定6
2.1.	ルート証明書の NTauth ストアへのインポート6
2.2.	グループポリシーの設定7
2.3.	Active Directory でのアカウント設定7
3. NPS	サーバでの設定
3.1.	サーバ証明書のインポート8
3.2.	NPSのActive Directoryとの連携10
3.3.	RADIUS クライアントの設定11
3.4.	認証ポリシの設定
4. Gléa	s の管理者設定(iPad)14
4.1.	UA(ユーザ申込局)設定14
5. iPad	での構成プロファイル・証明書のインストール16
5.1.	Gléas の UA からのインストール16
5.2.	OTA エンロールメントを利用した証明書発行について18
6. 無線	LAN の利用19
7. Andr	oid でのクライアント証明書取得・EAP-TLS 設定20
8. 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を利用して、 Microsoft CorporationのWindows Serverにおける802.1x(EAP-TLS)認証を行う 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
- 【RADIUSサーバ】Microsoft Windows Server 2008 R2 Standard SP1

 ホットワークポリシーサーバー 6.1.7601.17514
 ※以後、「NPS」と記載します
- > 【認証局】JS3 プライベートCA Gléas (バージョン1.10)
 ※以後、「Gléas」と記載します
- 【アクセスポイント】AirMac Extreme (バージョン7.6.1)
 ※以後、「アクセスポイント」と記載します
 ※本書では、無線LANアクセスポイントが802.1xにおけるオーセンティケータとなります
- 【クライアント】iPad (iOS5.1.1)
 ※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。

- Windows Server及びActive Directoryのセットアップ
 RADIUS認証用のユーザ及びグループは既に作成されているものとします
- 「ネットワークポリシーとアクセスサービス」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

- 各機器におけるネットワーク設定
- 無線LAN装置におけるRADIUSサーバの指定方法 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おります。



- ▶ スマートデバイス (iPad) からのWiFiアクセスをおこなう
- ▶ ユーザ認証にはEAP-TLSを利用する
- ▶ RADIUSサーバ証明書、及びクライアント証明書はGléasより発行されたものを利用する
- > NPSはActive Directoryのグループ及びユーザ情報を参照して認証をおこなう (ログインユーザ情報はクライアント証明書のサブジェクトの別名に記載されて いるUPNを用いる)

1.4. 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。

 クライアント証明書の発行には、「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。 「username@Windowsドメイン名」の形式のもの)と、CRL配布ポイントを 正しく設定する必要があります

※CRL配布ポイントが含まれていない証明書を用いる場合は、NPSサーバで以下のレジストリ エントリを設定すればクライアント証明書認証が可能となります HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥RasMan¥PPP¥EAP¥13 IgnoreNoRevocationCheck (存在しない場合は追加する)のDWARD値を1に設定する

2. ドメインコントローラでの設定

2.1. ルート証明書の NTauth ストアへのインポート

ルート証明書を Gléas よりダウンロードし、Windows ドメインの NTauth ストアと 呼ばれる格納領域にインポートします。 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。



明書	د
ま示(S): <すべて>	•
77-11-15	
テー使用法 Netscape 証明書の種類	Digital Signature, Certificate Signing, Off-line SSL CA, SMIME CA (06)
 The scape コメント 基本制限 提印アルゴリズム 	Subject Type=CA, Path Length Constraint=0 sha1
■拇印	614a68c8aed89b800d1cb1ed57c7
61 4a 68 c8 ae d8 9b 80 0d 1c	b1 ed 57 c7 03 b7 c8 44 5e 9b
証明書の詳細について表示します。	ファイルにコピー(C) -
	ОК

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

■ グループボリシーの管理 回 A フォレスト: js3-test.local	Defau スコープ	lt Domain Policy 詳細 設定 委任		
E ∰ js3-test.local	リンク		is 3-test local	
⊞	・ 通来(L)… ・ 強制(N) ・ リンクの有効化(L)	、ドメイン、および OU がこの GPC) についたいしています(T):	
	レポートの保存(S) 表示いか	test.local	<u> 強制 リンクの有効</u> い はい	化 パス js3-test.local
■ ■ サイト 「「」」 ポリシーのモデル作 ■ グループ ポリシーのモデル作	までパペップ ここから新しいウィンドウ(W)	_		
	削除(D) 名前の変更(M) 最新の情報に更新(F)			
	ヘルプ(H)			

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

2.3. Active Directory でのアカウント設定

[管理ツール]より[Active Directoryユーザーとコンピューター]を開始し、無線LAN アクセスを許可するユーザアカウントのプロパティを開き、[所属するグループ] タブを開き、無線LANを利用するグループに所属していることを確認します。 (本書では「wlan」セキュリティグループとします)

יב	-ザ 01のプロパティ	? ×
	リモート デスクトップ 5 ダイヤルイン 全般 住所 アオ 所属するグループ(<u>M</u>)	トービスのプロファイル 個人用仮想デスクトップ COM+ フリガナ 環境 セッション リモート制御 コウント プロファイル 電話 所属されている組織 所属するグループ
		Active Directory ドメイン サービス フォルダー
	Domain Users	js3-test.local/Users
	 追加(<u>D</u>)	削除(12)

3. NPS サーバでの設定

3.1. サーバ証明書のインポート

NPS を動かしているサーバ上で 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。

証明書スナップイン	1
このスナップインで管理する証明書:	
〇 ユーザー アカウンド(M)	
○ サービス アカウント(S)	
・ コンピューター アカウント(C)	
	< 戻る(B) 次へ(N) > キャンセル

コンピューターの選択 このスナップインで管理するコンピューターを選択してください。 このスナップインで管理するコンピューター:	
 ローカル コンピューター(L): (このコンソールを実行しているコンピュー 別のコンピューター(A): ロマンド ラインから起動したときは実現されたコンピューターを変更で 	ター) 参照(R)
これば、コンジールを保存した場合にのみ適用されます。	

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
	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	[証明書の種類に基づいて、自動的に証明書スト
	アを選択する(U)]を選択し、[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 RADIUS サーバ用の証明書がインポートされていることを確認します。

👼コンソール1 - 「コンソール 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)	へルプ(F) ちょうドウ(W) ヘルプ(F	0		
🗢 🔿 💋 🖬 📋 🧟 🗟 🖬				
📔 בעער אירא	発行先 -	発行者	有効期限	目的
🖂 🔜 証明書 (ローカル コンピューター)	🛐 radius.jcch-sss.local	JCCH-SSS demo CA	2015/07/13	サーバー認証、クライアン
🔁 🚞 個人				1
🦳 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				
Ξ				
⊞ Remote Desktop				
田 □□ 証明書の登録要求				
■ ■ スマートカードの信頼されたルート	1			
Ⅲ 1言頼されたデバイス	1			
1				

3.2. NPS の Active Directory との連携

[管理ツール]から[ネットワーク ポリシー サーバー]を開きます。

左ペインの[NPS(ローカル)]を右クリックして、[Active Directory にサーバーを登録(G)]をクリックします。

- 🌍 ネットワーク ፣	初シー サーバー	
ファイル(F) 操	作(A) 表示(V) ヘルプ(H)	
🗢 🔿 🖬	?	
● NPS (ローカ 団 一 RADIUS 団 目 ポリシー	構成のインボート(1) 構成のエクスボート(E)	
田 ■ ネットワ・ ■ アカウン: ■ ■ アンプレ・	NPS サービスの開始(S) NPS サービスの停止(O) Active Directory (こサーバン	リシー サーバー (NPS) を使用すると、クライアントの 5組織全体のネットワーク アクセス ポリシーを作成 た容皝(G)
	プロパティ(R)	C.32.99(\\)
	表示(V)	▶ すを選択し、下のリンクをクリックしてシナリオ ウィザー
	ヘルプ(H)	
	ネッ ネッ トーマ ト ト ト ト ト ト ト ト ト ト	トワーク アクセス(保護 (NAP) トワーク アクセス(保護 (NAP) 5 を NAP 正常性ポリシー サーバーとして構成する場合、正常性ポ ーターがネットワークに接続する際には NPS でそのコンピューターの都 準拠していない場合はそのクライアントを制限付きネットワークに移動 ことができます。

その後、確認メッセージが表示されるので[OK]をクリックします。

3.3. RADIUS クライアントの設定

[ネットワーク ポリシー サーバー]の左ペインから[NPS(ローカル)] > [RADIUSク ライアントとサーバー] > [RADIUSクライアント]を展開し右クリックし、[新規]を選 択します。

[新しいRADIUSクライアント]画面にて、本件章においてのRADIUSクライアントとなるアクセスポイントの情報を入力します。

- ▶ [フレンドリ名(F):]には、任意の名称を入力
- [アドレス(IPまたはDNS)(D):]には、アクセスポイントのIPアドレスか、ホスト名を入力(名前解決できるようになっている必要があります)
- ▷ [共有シークレット(S):]には、アクセスポイントとの通信に利用するパスワード (シークレット)を入力

UU R	ADIUS クライア	ント					
設定	詳細設定						
			-+7/5)				
I ⊻ C00	RADI03 994	アントを有効ル	699(<u>F</u>)				
□ 既	存のテンプレート	E選択する(工):				
							-
	- 						
フレン	/U/A (F):						
test-	-ap						
7	.7 (TD ±5/1 DM	ie)(D).					
test-	-an is 2-test los	63/(<u>D</u>).				祒	2000 L
liest	ap.jso test.ioc	JI					560 Y
一共有资	シークレットーー		1.5771-7.5				
既存(の共有シークレッ	トテンプレート	、を選択(<u>M</u>):				
ねし							•
共有: 住成 成時(ます。	シークレットを直持 1] をクリックします にも指定する必要	度入力する場。 。ここに指定し 見があります。	合は [手動] 走共有シー 共有シーク] をクリック ・クレットを、 ・ットではフ	し、自動で 、RADIUS 大文字と小	生成す クライア 文字が	る場合は シトの構 区別され
⊙₹	≞動(∐)	〇 生ೂ	t‰(<u>G</u>)				
共有:	シークレット(<u>S</u>):						
	•••••	••					
共有:	シークレットの確認	2入力(0):				-	
					OK		キャンセル

以上を設定したら[OK]をクリックします。

3.4. 認証ポリシの設定

[ネットワーク ポリシー サーバー]の左ペインから[NPS (ローカル)]>[ポリシー]> [ネットワーク ポリシー]を展開し右クリックし、[新規]を選択します。 [新しいネットワーク ポリシー]ウィザードが開始されますので、以下の通り設定を おこないます。

新しいネットワー	-b #J>-
	ネットワークボリシー名と接続の種類の指定 ネットワークポリシーの名前およびポリシーを適用する接続の種類を指定できます。
ポリシー名(A	y):
「 ネットワーク接 NPS (ご接続専 べンダー固有] 802.1X ワイヤ	続の方法 夏求を送信するネットワーク アクセス サーバーの種類を選択してください。ネットワーク アクセス サーバーの種類を選択するが、 【を指定することができますが、どちらも必須ではありません。ネットワーク アクセス サーバーが 802.1× 認証スイッチまたは 「レス アクセス ポイントの場合は、【未指定】を選択してください。
 ネットワーク Unspecif ベンダー国 	ケアクセスサーバーの種類(S): fied ▼ 初報(V):
10	Ξ
	前へ(2) 次へ(N) 完了(2) キャンセル



	は wlan)を選択
	7.[OK]をクリックし元の画面まで戻り、[次へ(P)]
	をクリック
Windows ガループ	X
このポリシーに一致するために必要な	デー
JS3-TEST¥wlan	
グループの追加()	〕 前耶余(<u>M</u>)
	OK キャンセル
	「/.[OK]をクリックし元の画面まで戻り、[次へ(N)]
	をクリック
アクセス許可の指定 	[アクセスを許可する(A)]を選択し、[次へ(N)]をク
	リック
認証方法の構成	1. [EAP の種類(T)]にて、[追加(D)]をクリック
	2. [EAP の追加]画面で、[Microsoft:スマートカ
	ードまたはその他の証明書]を選択し[OK]を
	クリック
	3. [セキュリティレベルの低い認証方法]のチェ
	ックをすべて外す
新しいネットワーク ポリシー	X
認証方法の構成 接続要求がこのポリシーの条件を満たすために必	要な認証方法を、1 つ以上指定してください。EAP 認証には、EAP の
種類を指定する必要があります。NAP を使用す た EAP を指定する必要があります。接続要求ポ	5 802.1Xまたは VPN を展開する場合は、接続要求ポリシーに保護され リシーは、ネットワーク ポリシーの認証設定 よりも優先されます。
EAP の種類は、NPS とクライアントとの間で、表示されている順序で	ネゴシェートされます。
EAP の種類(1): Microsoft: スマートカードまたはその他の証明書	上へ移動(山)
	下八移動(199)
セキュリティ レベルの低い翌証方法 : □ Microsoft 暗号化認証バージョン 2 (MS-CHAP v2)(<u>V</u>)	
□ パスワードの邦駅が切れた後も、ユーザーにパスワードの変更 □ Microsoft 音号化認証 (MS-CHAP)()	
□ TXAS + TO MANAGEMENT (CONTRACT + CONTRACT □ 暗号化認証(CHAP)(C) □ 暗号化されていない認証(PAP, SPAP)(S)	(21年1,3,997年)
 □ 認証方法をネゴシエートせずにクライアンドに接続を許可する(L) □ コンピューターの正常性チェックのみを実行する(M) 	
	前へ(P) 次へ(D) 完了(E) キャンセル

	スマート カードまたはその	抱の証明書のプロ/	 4. 追加した[Microsoft:スマートカードまたはその他の証明書]を選択し[編集]をクリック 5. [スマートカードまたはその他の証明書プロパティ]画面にて、[証明書の発行先]に 3.1 項でインポートしたサーバ証明書が選択されていることを確認して[OK]をクリック
	このサーバーは、接続が完 書を選択してください。 証明書の発行先(D: フレンドロタ・	:アする前に呼び出し <mark> radius.jcch-</mark> radius.icch-	/側に識別されます。識別の証拠として使う証明 -sss.local ▼
	発行者:	JCCH-SSS	demo CA
	有効期限:	2015/07/13	9.58:45
			トレン (K)
			6.[次へ(N)]をクリック
			追加の制約条件などを必要に応じ設定し、[次へ
			(N)]をクリック
設定の構成			RADIUS 属性(VLAN ID など)を必要に応じ設定
			し、[次へ(N)]をクリック
新しいネットワークポリシーの完了			[完了(F)]をクリック

4. 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含む無線 LAN 接続設定(構成プロファ イル)を iPad にインポートするための設定を本章では記載します。 ※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

4.1. UA (ユーザ申込局) 設定

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、設定をおこなうUA(申込局)をクリックします。

UA 申込局
▶ <u>Gleas Generic UA</u> Gleas デフォルト申込局

[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

この設定を行うと、GléasのUAからダウンロードしてから、指定した時間(分) を経過した後に、構成プロファイル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)。このインポートロックにより複数台のiPadへの構成 プロファイルのインストールを制限することができます。

▶基本設定
□ トークンへのインボート
□ 証明書ストアへのインボート
☑ ダウンロードを許可
ダウンロード可能時間(分) 1

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

構成プロファイル生成に必要となる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。

- [iPhone用レイアウトを利用する]にチェック
- [ログインパスワードで証明書を保護]をチェック
- [OTA(Over-The-Air)]を利用する場合はチェック(下述参照)
- [iPhone構成プロファイル基本設定]の各項目を入力 ※[名前]、[識別子]は必須項目となります ※[削除パスワード]を設定すると、iPadユーザが設定プロファイルを削除する際 に管理者が定めたパスワードが必要となります(iPadユーザの誤操作等による 構成プロファイルの削除を防止できます)

▶iPhone / iPadの設定		
🔽 iPhone/iPad 用 UA を利用	する	
画面レイアウト		
✓ iPhone 用レイアウトを使用する ✓ Mac OS X 10.7以降の接続を許可		▶ ログインパスワードで証明書を保護
OTA(Over-the-air)		
🔲 OTAエンロールメントを利用	する	🥅 接続する iOS デバイスを認証する
OTA用SCEP URL		
OTA用認証局	デフォルトを利用	-
iPhone 構成ブロファイル基本	設定	
名前(デバイス上に表示)	プライベートCA Gleas	
識別子(例: com.jcch- sss.profile)	com.jcch-sss.demo-mdn	n
プロファイルの組織名	JCCH・セキュリティ・ソリュ	ーション・システムズ
記日月	テスト用の構成プロファイル	,
削除バスワード		

入力が終わったら、 [無線LAN(802.1x)の設定]項目まで移動し以下を設定します。

- [SSID]に、無線LANアクセスポイントのSSIDを入力
- SSIDをブロードキャストしていない場合は、[非公開ネットワーク]をチェック 無線LAN(802.1x)の設定

SSID	js3test
□ 非公開ネットワーク	

他項目の設定も終了したら、[保存]をクリックして設定を保存します。

以上でGléasの設定は終了です。

5. iPad での構成プロファイル・証明書のインストール

GléasのUAに接続し、発行済みのクライアント証明書・構成プロファイルのインポ ートを行います。 ※本ケースではUAに接続するためのネットワーク接続が必要となります(3G回線や、証明書認証 を必要としない無線LAN接続等)

5.1. Gléas の UA からのインストール

iPadのブラウザ(Safari)でGléasのUAサイトにアクセスします。 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。



ログインすると、そのユーザ専用ページが表示されるので、[構成プロファイルのダ ウンロード]をタップし、ダウンロードを開始します。 ※インポートロックを有効にしている場合は、この時点からカウントが開始されます

				วราง-rca Gléäs u
ューザ 0 1	さんのページ]			□□グアウ
ユーザ情報		_	_	
🙎 ユーザ 0	1 さんのページ			D <u>ヘルプ</u>
🖢 ユーザ情幸	暇の確認・変更			
▶ユーザ	登録日日	寺 : 2011/07/19 13:48		
≫ 姓 : ユーザ 名 : 0 1 ≫ ユーザD : user01 ≫ メール : user01@js3-lest.local				
★ 証明書情幸	£			
▶発行済み証明				
#	発行局	シリアル	有効期限	ダウンロード
#1	JCCH-SSS demo CA	#9850	2015/07/13	構成プロファイルのダウンロード

ダウンロードが終了すると、自動的にプロファイル画面に遷移するので、[インスト ール]をタップします。

なお、[詳細]をタップすると、インストールされる証明書情報を見ることが可能ですので、必要に応じ確認してください。



インストール途中に、以下のようなルート証明書のインストール確認画面が現れま すので、[インストール]をクリックして続行してください。

※ここでインストールされるルート証明書は、通常のケースではGléasのルート認証局証明書になります



パスコードロックを有効にしている場合(或いは構成プロファイルでパスコードロックを強制する場合)はパスコードを入力し、インストール完了画面になりますので、[完了]をタップしてください。



元のUA画面に戻りますので、[ログアウト]をタップしてUAからログアウトしてくだ さい。

以上で、iPadでの構成プロファイルのインストールは終了です。

なお、インポートロックを有効にしている場合、[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能となります。

				プライベートCA Gléäs U
ユーザ 0 1	さんのページ]			▶□グアウ
ユーザ情報			_	
🙎 ユーザ 0	1 さんのページ	_	_	▶ <u>ヘルプ</u>
🖢 ユーザ情幸	服の確認・変更			
▶ ユーザ	登録日時 : 2	011/07/19 13:48		
> 姓 : ユーザ 名 : 0 1 > ユーザID : user01 > メール : user01@js3-test.local				
鮝 証明書情幸	R			
▶ 発行済み証明				
#	発行局	シリアル	有効期限	ダウンロード
章1	JCCH-SSS demo CA	#9850	2015/07/13	ダウンロード済み

5.2. OTA エンロールメントを利用した証明書発行について

Gléasでは、iOSデバイスに対するOver The Air(OTA)エンロールメントを利用した証明書の発行・構成プロファイルの配布も可能です。

OTAを利用すると事前に指定した端末識別番号を持つ端末だけに証明書の発行を限

定することも可能になります。



※端末識別情報:UDID、IMEI、ICCID、MACアドレス

詳細は7項のお問い合わせ先までお問い合わせください。

6. 無線 LAN の利用

インストールした構成プロファイルにより、アクセスポイントの設定や、EAP-TLS 認証に利用するクライアント証明書は既にiPadにインストールされているので、接 続したいワイヤレスネットワークを選択する等で、クライアント証明書によるセキ ュアな接続をお試しください。

無線LANアクセス成功時には、Windows Serverのセキュリティログに以下のメッセ ージが表示されます(一部の抜粋)。

イベント ID:	6272
タスクのカテゴリ:	ネットワーク ポリシー サーバー
レベル:	情報
キーワード:	成功の監査
<i>説明</i> :	ネットワーク ポリシー サーバーがユーザーにアクセスを許可しました。
認証の詳細:	
認証の種	類: EAP

EAP の種類: Microsoft: スマート カードまたはその他の証明書

失効済みの証明書を利用すると、アクセスに失敗しWindows Serverのセキュリティ ログに以下のメッセージが表示されます(一部の抜粋)。

※失効情報がNPSに伝播されている必要があります

イベント ID:	6273	

タスクのカテゴリ: ネットワーク ポリシー サーバー

レベル: 情報

- キーワード: 失敗の監査
- 説明: ネットワーク ポリシー サーバーがユーザーのアクセスを拒否しました。

詳細については、ネットワーク ポリシー サーバーの管理者に問い合わせて ください。

認証の詳細:

認証の種類:	EAP
EAP の種類:	Microsoft: スマート カードまたはその他の証明
理由コード:	256
理由:	この証明書は失効しています。

7. Android でのクライアント証明書取得・EAP-TLS 設定

弊社ホワイトペーパー「Android での無線LAN (802.1X EAP-TLS) 設定」をご参照ください。公開URLは以下の通りとなります。 http://www.jcch-sss.com/service/support/2011/06/wifi-eap-tls-android

8. 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