

シングルサインオンによるGléas UAログイン

(AD FS 連携)

Ver.1.1

2023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。

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

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

目次

1.	はじる	りに
	1.1.	本書について5
	1.2.	本書における環境
	1.3.	本書における構成
2.	AD ወ	設定8
	2.1.	SSL 証明書をインポート8
3.	Gléas	; アカウントの登録11
	3.1.	AD ユーザ情報をインポート 11
4.	SAM	L SP 署名用証明書の発行14
5.	AD F	S の設定16
	5.1.	SAML SP 署名用証明書の信頼16
	5.2.	証明書利用者信頼を追加18
	5.3.	証明書利用者信頼の設定27
	5.4.	SAML IdP 暗号用証明書の取得32
	5.5.	SAML IdP 署名用証明書の取得34

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

6. Gléas の管理者設定 (Windows 向け)
7. クライアントからのアクセス (Windows)
7.1. シングルサインオンで UA にログイン
7.2. クライアント証明書のインポート4
8. Gléas の管理者設定 (iPhone 向け)43
9. クライアントからのアクセス (iPhone)47
9.1. シングルサインオンで UA にログイン47
9.2. クライアント証明書のインポート49
10.Gléas の管理者設定 (Android 向け)52
11. クライアントからのアクセス (Android)57
11.1. シングルサインオンで UA にログイン57
11.2. クライアント証明書のインポート
12.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「プライベート認証局 Gléas」のユーザ申込局 UA を、Active Directory フェデレーション サービス (AD FS) の証明書利用者として登録し、シング ルサインオンで UA にログインする環境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。

- SAML SP: JS3 プライベート認証局 Gléas (バージョン 2.6.0) UA
 ※以後「UA」と記載します
- Active Directory フェデレーション サービス: Microsoft Windows Server 2019
 ※以後「ADFS」と記載します

- ドメインコントローラ: Microsoft Windows Server 2019
 ※以後「AD」と記載します。
- > Web アプリケーション プロキシ: Microsoft Windows Server 2019
 ※以後「WAP」と記載します。
- > JS3 プライベート認証局 Gléas (バージョン 2.6.0)
 ※以後「Gléas」と記載します
- クライアント: Windows 10 Pro (21H1) / Microsoft Edge 104.0.1293.70
 ※以後「Windows」と記載します
- クライアント: iPhone X (iOS 16) / Safari
 ※以後「iPhone」と記載します
- クライアント: Google Pixel5 (Android 13) / Chrome
 ※以後「Android」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。

- AD、ADFS、WAPの基本設定
- 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、iPhone での UA へのログイン方法

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います。



- 1. Windowsでは、EdgeブラウザからUAへアクセス試行する
- 2. 認証連携先のADFSのサインイン画面に画面遷移。ADFSはパスワードを要求し、認 証成功するとUAにログインした状態になる
- 3. iPhoneでは、SafariブラウザからUAへアクセス試行する
- 4. 認証連携先のADFSのログイン画面に画面遷移。ADFSはパスワードを要求し、認証 成功するとUAにログインした状態になる
- 5. Androidでは、ChromeブラウザからUAへアクセス試行する
- 6. 認証連携先のADFSのログイン画面に画面遷移。ADFSはパスワードを要求し、認証 成功するとUAにログインした状態になる

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

- 2. AD の設定
- 2.1. SSL 証明書をインポート

ADにSSL証明書をインポートして、LDAPSを有効化します。

ADサーバのFQDNが記載されたSSL証明書を準備します。

※SSL証明書はGléasから発行することも可能です。詳しくはお問い合わせください。

PKCS#12(.pfx)形式の SSL 証明書を AD サーバにコピーします。

MMC 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、[サービス アカウント(S)]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、

次の「証明書スナップイン」では、[Active Directory Domain Services)]を選択し、

[完了]をクリックします。

証明音スナップイン	×	コンピューターの歴史	×	証明書スナップイン	×
283から70代電源42周曲 C34-5785/H0 第十2375/H0 C3904-5-7800H0		2005/71/71/20世界420/2-3-4世界にくなり、 2017/71/72年9年30/2-3-7 日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	후(1),1,	D-56-2024-0-2018 19-4-201703-14-501 -2-21702/1-00 Test D-straty-Califordia Server Test D-straty-Califordia Server Test D-straty-Califordia Server Test D-straty-Califordia Server Test D-straty-Califordia D-strate Server Ser	
< 36 (3)	さへ(N) > キャンセル	< #3(8)	A(N) > ++>#+>##		< 戻る(お) 完了 キャンセル

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

スナップインが追加されたら左ペインより[証明書-ローカルコンピューター上のサービス] > [NTDS ¥ 個人]と展開し、中央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、SSL 証明書をインポートしま

×

次へ(N) キャンセル

す。

÷ 🦻	証明書のインボート ウィザード
	証明書のインポート ウィザードの開始
	このウィザードでは、証明會、証明會信頼リスト、および証明會失効リストをディスクから証明會ストアにコピー します。
	証明機関によって発行された証明書は、ユーザーIDを確認し、データを保護したり、またはセキュリティで保護 されたネットワーク接続を提供するための情報を合んでいます。証明書かけ、証明書が保留されるシステ ム上の構成です。
	保存場所
	○ 現在のユーザー(C)
	◎ ローカル コンピューター(L)
	統行するには、「次へ」をクリックしてください。

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	SSL 証明書ファイル(拡張子 : p12/pfx)を指定し
	て、[次へ(N)]をクリック
秘密キーの保護	SSL 証明書のパスフレーズを入力して、[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に配置する(P)]を選択
	し、[証明書ストア]に[NTDS¥個人]が指定されて
	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(F)]をクリック

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

中央ペインで右クリックして、[最新の情報に更新(F)]をクリックします。

左ペインより[証明書-ローカルコンピューター上のサービス] > [NTDS ¥ 個人] > [証明

書]と展開すると、インポートされた証明書が確認できます。

※中央ペインにルート証明書がある場合には、ルート証明書を選択し、左ペインの[証明書-ローカルコ ンピューター上のサービス] > [NTDS¥信頼されたルート証明機関] > [証明書] に移動してください。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

3. Gléas アカウントの登録

3.1. AD ユーザ情報をインポート

AD のユーザ情報を LDAPS で Gléas のアカウントとしてインポートします。

GléasのRA (登録局) にログインします。

[アカウント]>[アカウント新規作成]メニューから[上級者向け設定」をクリックします。

▶アカウント情報		■上級者向け設定
>アカウント名 対		
>初期グループ	なし	
	▶ここをクリックしてユーザを参加させるグループを選択	
> その他の設定	☑ 証明書を発行する	
	□ 連続して登録を行う	
▶種類 ○ ユーザ ○	コンピュータ 〇 サーバ 〇 認証局 〇 CSVファイルー括登録 🖲 LDAP	
> 指定方法	○ URL ◉ ホスト名	
> ホスト名	210-000.200-00]
>ポート番号	(Canal)	
> Base DN	OU= ,DC= ,DC= ,DC=]
>管理者DN	CN= ,CN= ,DC= ,DC= ,DC=	
>パスワード]
>検索フィルタ	(objectClass=person)	
>グループメンバー属性		
> 前回のインポート	✓ 前回のインボート以降に作成されたエントリのみ	
> 属性のマッピング	カスタム設定	
Gléasの属性	LDAPの属性	
アカウント名 userF	PrincipalName	
名前(姓) sn		
名前(名) given	Name	
メールアドレス mail		
パスワード		
プリンシバル名 userF	PrincipalName]
	作 E5戈	

- [▶種類]から[LDAP]を選択
- [指定方法]に[ホスト名]を選択
- [ホスト名]に AD のホスト名を入力

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

- [ポート番号]に "636" を入力
- [BaseDN]にユーザ情報の検索対象となるベース DN を入力
- [管理者 DN]に BaseDN 以下にアクセスできる AD 管理者の DN を入力
- [パスワード]に AD 管理者のパスワードを入力
- [検索フィルタ]に "(objectClass=person)" を入力
- [属性のマッピング]に[カスタム設定]を入力
- [Gléas の属性]に Gléas のアカウントと LDAP 属性の紐づけを入力

Gléas の属性	LDAP の属性
アカウント名	sn
名前 (姓)	sn
名前 (名)	givenName
メールアドレス	mail
パスワード	空欄
プリンシパル名	userPrincipalName

● [作成]をクリック

※[証明書を作成する]をチェックすると、インポートと一緒に証明書の発行が行われます。

されたファイルの最初の4件				
アカウント名	女生	名	メールアドレス	プリンシバル名
and the second second				at the got the last on or
			· · · · · · · · · · · · · · · · · · ·	ŝ

● 内容を確認し[実行]をクリック

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

[アカウント]>[登録申請者一覧]メニューを選択します。

※しばらくするとアップロードしたユーザ情報がアカウント登録申請として登録されます。



- [全て許可する」をクリック
- [実行]をクリック

これで AD のユーザ情報が Gléas のアカウントとしてインポートされました。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

4. SAML SP 署名用証明書の発行

SAML SPとして使用する署名用証明書をGléasから発行します。

※ADFSとの連携に使用するSAML SP署名用証明書には、CRL配布ポイントの記載が必要となりますの でご注意ください。詳しくはお問い合わせください。

GléasのRA (登録局) にログインします。

[アカウント]>[アカウント新規作成]からアカウント saml_sp を作成します。

→ 新規アカウント作成				
2 アカウント情報の入 このページではアカウントの新規(アカウントは証明書を発行する対な ★の付いている項目は入力必須	プ いたを行います。 象(エンドエンティティ)のことで、このページで指定したアカウント名が証明書の発行先となります。 項目です。			
▶アカウント情報	*上級者向け設定			
> アカウント名 対	saml_sp			
> 名前(姓) 🚖	SAML			
> 名前(名) 📩	SPEII明書			
>メールアドレス				
>パスワード				
>バスワード(確認)				
>パスワード(自動生成)	バスワード生成			
> プリンシバル名				
	(fest			

[証明書発行]で saml_sp アカウントに対し証明書を発行します。

saml_sp	D 詳細
≹ 証明書発行	
の画面では証明書要求の作成を行います。	
E側の「サブジェクト」と「属性」の内容で証明書要求を作成します。	
11別のテンフレートの中から必要なものを選択して「先行」を押してくたさい。	
▶証明書発行	- 上級者向了設定
> 下記の内容で証明書を発行します。よろしければ「発行」を押してください。	
	994=
▶サブジェクト	▶選択されているテンプレート ▶ 全て解除
> CN=saml_sp	> 必須 デフォルト設定
> O=JCCH Security Solution Systems	>必須区分CRL
> DC=local, jcch-sss	
	▶選択可能なテンプレート
▶属性	> tal
> 発行局:	
>暗号アルゴリズム:RSA暗号	
▶ 鍵長: 2048bit	
>ダイジェストアルゴリズム:SHA256	
> 有効日数:1年	
> 縺用途:電子署名, 縺の暗号化	
> 拡張鏈用途: SSLクライアント認証	
> Netscape 拡張:有効	
> CRL 配布点:	

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

証明書詳細画面から[ダウンロード]をクリックし証明書をダウンロードします。

sami_sp	開始日: 2022/09/28 10:09 終了日: 2023/09/28 10:09
説明:	最終更新:2022/09/28 10:10 編集
• サブジェクト	▶□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
統名:sami_so 結題:JCCH Security Solution Systems ドッパーンコーネント:local ドッインコンボーネント:jcch-sss	 > fysK日: 2022/0028 10:08 > 為均日表: 3065 > 入丸日: > 入均理由: > 界域地告: > 界域地子日: > 以常認知: 有効な証明書 > 以馬切い就想:: 有効な証明書 > トージン必要:: > パージン: 4
証明書情報 認証局:	
- 暗号アルゴリズム: rsa ダイジェストアルゴリズム: sha256 2提長: 2048 週田途: 電子至名 録の指号化	
#音アルビリズム: rsa タイシュストアルニリズム: sha256 線長: 2048 線用: (# <u>2</u>	
 ·留号アルゴリズム: rsa ダイジェストアルビリズム: sha256 メタイシェストアルビリズム: sha256 メ優用:2: <u>SL/25-77-11/0日</u> ・ ・認用:3: <u>SL/25-77-11/0日</u> ・ ・別名: ゴ明言ファイル ゴ明言ファイル ゴ明言ファイル ゴリコン200022 10.09 ゴリヨークション ブリ ブレ ブリ ジリ ブリ ブリ ブリ ブリ ブリ ブリ ブリ ブリ ブリ ブリ <td>▶先物值程 >COP:</td>	▶先物值程 >COP:

※ダウンロード時に証明書、秘密鍵を取り出す際のパスフレーズを指定します。

ダウンロードした.p12ファイルからPEM形式の証明書を取り出します。

※OpenSSLで行なう例 (パスフレーズの入力が必要となります)

openssl pkcs12 -in saml_sp.p12 -nokeys -clcerts | openssl x509 out saml_sp.crt

※取得した証明書ファイル saml_sp.crt を保存します。

ダウンロードした.p12ファイルからPEM形式の秘密鍵を取り出します。

※OpenSSLで行なう例 (パスフレーズの入力が必要となります)

openssl pkcs12 -in saml_sp.p12 -nodes -nocerts | openssl rsa -out saml_sp.key

※取り出した秘密鍵ファイル saml_sp.key を保存します。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

5. AD FS の設定

5.1. SAML SP 署名用証明書の信頼

SAML SP 署名用証明書を ADFS が信頼できるようにします。

Gléas からルート証明書をダウンロードします。

※ダウンロードURLは、 https://[RAのFQDN]/crl/ia1.pem ※PowerShellで行なう例

Invoke-WebRequest "http://[RA Ø FQDN]/crl/ia1.pem" -OutFile "ia1.cer"

MMC 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

証明書スナップイン	× コンピューターの選択 ×
このスナップインで管理する証明書: () ユーザー アカウンド(M) () サービス アカウンド(S) ④ コンビューター アカウンド(C)	このスオップインで管理するコンビューターを選択してください。 このスオップインで管理するコンビューター: ④ ローカル コンビューター(L): (このコンソールを来行しているコンビューター) 〇 別のコンビューター(A): 参照(R) □ コマンド ラインから起動したときは選択されたコンビューターを表更できるようにする(W) これは、コンソールを保守した場合にのか感用されます。
< 戻る(8) 次へ(N) > キャンセル	< 頁3(8) 発了 キャンセル

します。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

スナップインが追加されたら左ペインより[証明書(ローカルコンピューター)] > [信頼さ れたルート証明機関]と展開し、中央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、ルート証明書をインポートしま

す。

← 憂 証明書のインボート ウィザード	
証明書のインポート ウィザードの開始	
このウィザードでは、証明書、証明書信頼リスト、ま します。	よび証明書失効リストをディスクから証明書ストアにコピー
証明機關によって発行された証明書は、ユーザー されたネットワーク接続を提供するための情報を合, ム上の領域です。	D を確認し、データを保護したり、またはセキュリティで保護 しでいます。証明書ストアは、証明書が保管されるシステ
保存場所 ○現在のユーザー(C) ④ローカルコンピューター(L)	
続行するには、[次へ]をクリックしてください。	
	次へ(N) キャンセル

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	ルート証明書ファイル (拡張子 : pem/der/crt) を
	指定して、[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に配置する(P)]を選択
	し、[証明書ストア]に[信頼されたルート証明機関]
	が指定さ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(F)]をクリック

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

5.2. 証明書利用者信頼を追加

証明書利用者信頼として UA を登録します。

スタートメニューから [ADFS の管理] を起動します。

左ペインの [証明書利用者信頼] を選択します。

右ペインの [証明書利用者信頼の追加...] をクリックします。

AD FS			– 🗆 ×
翰 ファイル(F) 操作(A) 表示(V)	ウィンドウ(W) ヘルプ(H)		_ 6 ×
🗢 🏟 🙇 📰 🔢 🖬			
AD FS	証明書利用者信頼		操作
> 三 サービス 「 アクセス制御ポリシー	表示名	有効 種類	1 証明書利用者信頼
証明書利用者信頼	Record The Wilson's Tables Rela-	(‡t) WS	証明書利用者信頼の追加
三 要求プロバイダー信頼 マプリケーション グリープ			表示
			ここから新しいウィンドウ
			最新の情報に更新
			∧ルプ
	<	>	
L	1		

証明書利用者信頼の追加ウィザードが起動します。

[ようこそ] ページ

● [要求に対応する(C)] を選択

5- <i>z</i>	
ようこ ようこそ テーション-の運訳 アウレス事故がリッレーの運訳 (特別の語かが年後年7 光7	25. 沙定します。 会認道を使用 ます。 社会社

[開始(S)] をクリックします。

[データ ソースの選択] ページ

● [証明書利用者についてのデータを手動で入力する(T)] を選択

翰 証明書利用者信頼の追加ウ	۲۳-۴ ×
データ ソースの選択	
ステナノ - よンご - データソースの建築 - データソースの建築 - ビートンスの物変 - 認知手の構成 - 認知子の構成 - 適知子の構成 - 資格の点別のの準備完了 - 光了	この証明書が明報についてのデーが影响するために使用するオグシューを求用してください ・ つっていためだって、 ・ つっていためだって、 ・ つっていためだって、 ・ つっていためだって、 ・ つっていためだって、 ・ つっていためで、 ・ ついためで、 ・ ついたので、 ・ ついためで、 ・ ついたので、 ・ ついためで、 ・ ついためで、 ・ ついためで、 ・ ついたので、 ・ ついたのでので、 ・ ついたのでいたので、 ・ ついたのでいたので、 ・ ついたので、 ・ ついたので、 ・
	<前へ(P) 次へ(NO > キャンセル

[次へ(N)>] をクリックします。

[表示名の指定] ページ

- [表示名(I)] に任意の名前を入力
- [メモ(C)] に証明書利用者の説明を入力



表示名の指定		
ステップ	この証明書利用者の表示名およびオブションの注意事項を入力してください。	
₀ ಕಿನಿಲಿಕೆ	表示名(D)	
● データソースの選択	The O's Webs	
◎ 表示名の指定	xE(0):	
 証明書の構成 	TORE OF THE OWNER OF	^
 URL の構成 		
 ・ ・ ・		
アクセス制御ホリシーの違択		~
● 1117月(2月11日)(2年1月)元 1		
•元1		

[次へ(N)>] をクリックします。

証明書の構成] ページ

※オプション

証明書の構成		
ステップ - ようこそ - データンコースの成果 - データンコーンの成果 - ジーンスの成果 - 建築明金の構成 - 辺中しの構成 - 連邦人で構成 - 連邦人で構成 - 運動人で構成 - ご知らの定義売了 - ディ	オプションローン/用型(12)(12)(12)(12)(12)(12)(12)(12)(12)(12)	

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

[URL の構成] ページ

- [SAML 2.0 WebSSO プロトコルのサポートを有効にする(A)] をチェック
- [証明書利用者 SAML 2.0 SSO サービスの URL(S)] を入力

※https://[UA の FQDN]/ua/[UA の名前]/saml/acs

URLの構成		
ステップ - シスと モンクシークの確認 - データンークの確認 - データンークの確認 - ジャン・の情感 - ジャン・の構成 - ジャン・の構成 - ジャン・の構成 - ジャン・の構成 - ジャン・の構成 - デモア - 光子 - 光子 - 光子 - 光子 - ジャン・の - ジェーク - ジェーク	A F151 日間時を開催についての GC-Tune いたいないためませい。たけ 544 31 F344 31 F446 31 F446 51 F466 51 F46	-

[次へ(N)>] をクリックします。

[識別子の構成] ページ

● [証明書利用者信頼の識別子(E)] を入力

※https://[UA の FQDN]/ua/[UA の名前]/saml

● [追加(D)] をクリック

書別での提供		
PK 54 T 47 114 DX		
ステップ	証明書利用者は、1つ以上の一意の識別子文字列で識別できます。この証明書利用	者信頼の識別子を指
ようにそ	定してください。	
▶ データソースの選択	証明書利用者信頼の識別子(E):	
表示名の指定		i宣加(D)
■ 証明書の構成	(9) https://fs.contoso.com/adfs/services/trust	
URL の構成	証明書利用者信頼の感別子(Y):	E(E)/(D)
≥ 識別子の構成	nttps://uanarik.awa.test.jccn~sss.jccai/ua/pc/sami	MUDB(R)
。 アクセス制御ポリシーの選択		
自頼の道加の準備完了		
完了		

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

[アクセス制御ポリシーの選択] ページ

● [アクセスポリシーを選択してください] で [すべてのユーザーを許可] を選択

翰 証明書利用者信頼の追加ウ	ィザード	×
アクセス制御ボリシーの選択	R	
ステック ・ ようこそ ・ テーシーンの成果 ・ テーシーンの成果 ・ デーシーンの成果 ・ ビルしの加え ・ ビルしの加え ・ アラセン入動体のシーの変現 ・ アラセン入動体のシーの変現 ・ アラセン入動体のシーの変現 ・ アラセン入動体のシーの変現 ・ アラセン入動体のシーの変現 ・ アラセン入動体のシーの変現 ・ アラセント	アサビス制築的シーも獲用して代えい 名目 マイでのユーサーくに少ら3ット アシビス有計可 日本のロシェーローに30 マイでのユーサーに30 マイでのユーサーに30 マイでのユーサーに30 マイでのユーサーに30 マイでのユーサーに30 マイでのユーサーは30 マイでのユーサーは30 マイでのユーサーは30 マイでのユーサーは30 マイでのユーサーは30 マイでのユーサーは30 マイマン・サイト 第0 ション・ローク 第0 マーク ・10 ・10 ・10 ・10 ・10 ・10 ・10 ・10	29月 イントラネク・ユーザーにアクセス結中で パンパールールのシロシス 4日にして インパースタールールのシロシス 4日にして インパースタール インパースタール インパースタール インパース 2012 インパースタール インパース 2012 インパースタール インパース 2012 インパースタール インパース 2012 インパースタール インパース 2012 インパースタール インパース 2012 インパース 2012 インパー
	<前へ	、(P) 次へ(N) > キャンセル

[次へ(N)>] をクリックします。

[信頼の追加の準備完了] ページ



[完了] ページ

● [このアプリケーションの要求発行ポリシーを構成する(C)] をチェック

完了		
ステラ ● シテミ ● シテミ ● クータンースの確保 ● データの加速(■ の用いる構成 ■ 0年(の構成 ■ 0年(の構成 ■ 0年(の構成 ■ 0年(の構成) ● 2702.3%時かか)-の確保 ● 2年前の出版の準備化? ● 光子 ● 二 ● 二 ● 二 ● 二 ● 二 ● 二 ● 二 ● 二	田明春中周希信報所工がに300c1よし。 2 この7フウォーシェムの東京電行ポウシーを構成する(C)	

[閉じる(C)] をクリックします。

自動的に [要求発行ポリシーの編集] ダイアログボックスが表示されます。

			の事	[求発行	ポリシーの)編集						×
発行	変換規	IJ										
	次の変換	奥規則は、	証明	書利用:	皆へ送信	する要求	を指定しま	ŧŧ.				
	順序	規則名					発行	済み要求				
											T	
											•	
										>		
	規則)追加(A).		規則の	扁集(E)	規則	りの削り除()	R)		-		
							OK	キャン	セル		適用(P)	1

[規則の追加(A)...] をクリックします。

変換要求規則の追加ウィザードが表示されます。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

[規則テンプレートの選択] ページ

● [要求規則テンプレート(C)] に [入力方向の要求を変換] を選択

規則テンプレートの選択	R
ステ ッ プ ・ 規則の種類の選択	作成する要求規則のテンプレートを次の一覧から選択してください。各要求規則テンプレートの詳細は説明に記 載されています。
●要求規則の構成	要求規則テンプレート(C):
	入力方向の要求を実換
	要求規則テンプレートの説明
	しい方が高い使きなど見て、機能にない、もないます。ここでは、ないないないないである。 「いっかからい」では、「いっか」では、「いっか」では、「いっか」では、「いっか」では、「いっか」では、「いっか」では、 「いっか」では、「いっか」では、「いっか」では、「いっか」では、「いっか」では、「いっか」では、 「いっか」では、「いっか」では、「いっか」では、「いっか」では、「いっか」では、 「いっか」では、「いっか」では、「いっか」では、「いっか」では、 「いっか」では、「いっか」では、「いっか」では、「いっか」では、 「いっか」では、「いっか」では、「いっか」では、 「いっか」では、「いっか」では、「いっか」では、 「いっか」では、「いっか」では、 「いっか」では、「いっか」では、 「いっか」では、「いっか」では、 「いっか」でする。 「いっか」 「いっか」、 「いっか」、 「いっか」、 「いっか」 「いっか
	<約へ(P) 次へ(N0 > キャンセル

[次へ(N)>] をクリックします。

[規則の構成] ページ

- [要求規則名(C)] に "NameID"と入力
- [入力方向の要求の種類]に[UPN]を選択
- [出力方向の要求の種類]に[名前 ID]を選択
- [出力方向の名前 ID の形式]に[指定なし]を選択
- [すべての要求値をパススルーする]を選択

ステ ップ - 周辺の新聞の深祝	この規則を構成することにより、入ナ す。オブションとして、入力方向の要	1方向の要求の種類を出力方向の要求の種類に関連付けることができ 求の値を出力方向の要求の値に要連付けることもできます。出力方向	は初期			
● 要求規則の構成	求の種類に関連付ける人力方向のす。)要求の種類と、要求値を新しい要求値に関連付けるかどうかを指定!	<i>,</i> ‡,			
	要求規則名(C):					
	NameID					
	規則テンプレート: 入力方向の要求	を変換				
	入力方向の要求の種類(1)	UPN	-			
	入力方向の名前 ID の形式(M):	No. of Concession, Name				
	出力方向の要求の種類(0):	名前D				
	出力方向の名前 ID の形式(E):	指定なし				
	 すべての要求値をパス スルーする(S) 					
	○ 入力方向の要求の値を異なる出力方向の要求の値に置き換える(R)					
	入力方向の要求の値(V):					
	出力方向の要求の値(U):	参照(B)_			
	○ 入力方向の電子メール サフィッ	りス要求を新しい電子メールサフィックスに置き換える(X)				
	新しい電子メール サフィックス(W					
		例: fabrikam.com				

[完了] をクリックします。

1 NameID 名前 ID	1 N	lameID	名前 ID	
				4

[規則の追加(A)] をクリックします。

変換要求規則の追加ウィザードが表示されます。

[規則テンプレートの選択] ページ

● [要求規則テンプレート(C)] に [LDAP 属性を要求として送信] を選択

🧌 変換要求規則の追加ウィ	<i>ザ</i> -ド	×
規則テンプレートの選択		
ステ ップ 	作成する要求規則のテンプレートを次の一覧から違訳してください。各要求規則テンプレートの詳細は説明に記 載されています。	
要求規則の構成	要求規則テンプレート(C): 1.040 原始を要求として送付金	
	■活動(サンプレートは転用) ■ ため用 開きままでした。(1981) 開きロンゴレートを使用なた。Antion Directory ACO 1000 開きに上 他の目的である。 の目的である。 したい、「したい」、「したい」、「したい」、Antion Directory ACO 1000 開きに上 の目的である。 したい、「したい」、「したい」、「したい」、Antion Directory ACO 1000 目前に、 したい、 の目的である。 したい、 したい、 の目的である。 したい、 の一のである。 したい、 の一のである。 したい、 の一のである。 したい、 の一のである。 したい、 の一のである。 ののである。 したい、 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 のののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 ののである。 のののである。 ののでのである。 ののでのである。 ののでのである。 ののでのである。 ののでのである。 ののでのである。 ののでののでのである。 ののでのである。 ののでのでのである。 ののでのである。 ののでのでのでのである。 ののでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでの]
	<約へ(?) 次へ00> キャンセル	

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

[規則の構成] ページ

- [要求規則名(C)] に "ユーザ情報属性"と入力
- [属性ストア(S)] に [Active Directory] を選択
- [LDAP 属性の出力方向の要求の種類への関連付け(M)] を以下のように入力

[LDAP 属性]	[出力方向の要求の種類]
[User-Principal-Name]	"cn"
[Suname]	"sn"
[Given-Name]	"givenname"
[E-Mail-Addresses]	"mail"

ステップ ● 規則の種類の選択	この規 性スト	則を構成することにより、 LDAP 腐性の値 Pを選択します。 次に、規則から発行する	を悪力	まとして送信できます。まず、LDAP 腐性の抽出元となる暴 う方向の要求の種類に腐性を関連付ける方法を指定しま			
● 要求規則の構成	要求制	要求規則名(C):					
	ユーザ情報開注						
	規則テンプレート LDAP 属性を要求として送信						
	原14-7	1F7(S)					
	Activ	Active Directory					
	LDAP	居住の出力方向の要求の種類への開き	町	±(M):			
		LDAP 腐性(さらに追加する場合は 選択または入力してください)		出力方向の要求の種類(さらに追加する場合は ない)			
		User-Principal-Name	×	on 🗸			
		Sumame	\sim	an 🗸			
	×	Given-Name	×	givenname ~			
		E-Mail-Addresses	\vee	mai 🗸 🗸			
			\sim	× *			

[完了] をクリックします。

の要求発行ポリシーの第 発行変換規則	編集	×
次の変換規則は、証明書利用者へ送信す	る要求を指定します。	
順序 規則名	発行済み要求	
1 NameID	名前 ID	
2 ユーザ情報時1住	cn,sn,givenname,mail	
		_
<	>	
相則(小)合加(A) 相則(小)合集(F)	相目山の肖明金(R)	
PER MUMBER LT	Ches Port Prov V-	
	OK キャンセル	適用(P)

[OK] をクリックします。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

5.3. 証明書利用者信頼の設定

証明書利用者信頼のその他設定を行います。

SAML SP 署名用証明書ファイルを ADFS サーバにコピーします。

スタートメニューから [ADFS の管理] を起動します。



左ペインの[証明書利用者信頼] を選択します。

中央ペインの [表示名] から 追加した証明書利用者信頼 を選択します。

右ペインの[プロパティ]をクリックします。

[プロパティ]ダイアログが表示されます。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

[署名]タブを選択します。

- [追加 (D)]をクリック
- SPの署名用証明書ファイルを選択

-	のプロパティ		×
エンドポイント 監視 識別子 この証明書利用者:	プロキシ エンドポイント - 暗号化 署名 からの要求の署名検証証	注意事項 受け付ける要: 明書を指定してくた	詳細設定 求 組織 ざい。
サブジェクト	発行者	有効開始日	有効期
<			>
追加.(D)	表示(W) 削	除(R)	
	ОК	キャンセル	適用(A)

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

[エンドポイント]タブを選択します。

[SAML の追加(D)...]をクリックします。

[エンドポイントの追加] ダイアログボックスが表示されます。

		のプロパティ	r			×
監視 エンドポイ SAML プロ イントを指	識別子 (ント フ コトコルおよび	暗号化 プロキシ エンド WS-Federa	署名 ボイント ationPassin	受け付ける 注意事項 /e プロトコル(2	要求 詳細 使用する	組織 田設定 エンドポ
URL	. アサーション	יי ד-בפֿעב-	イン - エンドポイ	バインデ	既定	応
http	s://		0	POST	いいえ	
<				_		>
SAML WS-Fe	の追加(D)… deration のう			削除(R)	編集	(E)
	[OK		キャンセル	適	用(A)

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

- [エンドポイントの種類(E)] に [SAML ログアウト]を選択
- [バインディング]に[POST]を選択
- [信頼された URL]に UA のログアウト URL を入力
 ※https://[UA の FQDN]/ua/[UA の名前]/saml/logout
- [応答 URL]に UA のログアウト URL を入力

※https://[UA の FQDN]/ua/[UA の名前]/saml/logout

● [OK(O)] をクリック

	のプロパティ	>
エンドポイントの追加		×
エンドポイントの種类	頁(E):	
SAML ログアウト	~	
バインディング(B):		
POST	~	
 □ 信頼された URL インデックス(N): □ (信頼された UBL(T) 	- を既定として設定する(S)	
https://	/ua/ /saml/logout	
例: https://sts.cor 応答 URL(R):	itoso.com/adfs/ls	
https://	/ua/ /saml/logout	
例: https://sts.com	ntoso.com/logout	
	OK(0) キャンセ	JI -
	OK キャンセル 適用	(<u>A</u>)

[詳細設定]タブを選択します。

● [セキュアハッシュアルゴリズム(S)] に [SHA-256]を選択

		のプロパティ			×
監視 エンドポイ	識別子	暗号化 プロキシ エンド	署名 ポイント	受け付ける要注意事項	「求 組織 詳細設定
この証明 してくだ	明書利用者(ざい。	信頼に使用す	ねセキュア、	ハッシュ アルゴリ	ズムを指定
セキュア	7 ハッシュ アル	レゴリズム(S):	SHA-256		~
	[ОК	+	ャンセル	適用(A)

[OK] をクリックします。

※証明書利用者信頼の追加、設定は、UA 毎に登録する必要があります。PC と iOS などデバイス種類 ごとに複数の UA を利用している場合などは、それぞれ証明書利用者信頼の追加を行う必要がありま す。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

5.4. SAML IdP 暗号用証明書の取得

Gléas に設定する SAML IdP の暗号用証明書を ADFS から取得します。

スタートメニューから [ADFS の管理] を起動します。

左ペインの [サービス] > [証明書] を選択します。

中央ペインの [トークン暗号化解除] の証明書を右クリックしてメニューを表示します。

[証明書の表示(V)]をクリックすると[証明書]ダイアログボックスが表示されます。

砩 証明書		×
全般 詳細 証明のパス		
表示(S): <すべて>	~	
フィールド	值 ^	
■ バージョン	V3	
回 シリアル番号 回 黒タマルゴリズム	cha256RSA	
国家名ハッシュアルゴリズム	sha256	
🛄 発行者	and the second sec	
有効期間の開始 方効期間の終了	and the second second	
(回) サブジェクト	· · · · · · · · · · · · · · · · · · ·	
V3		
	プロパティの編集(E) ファイルにコピー(C)	
	ОК	

[詳細]タブで[ファイルにコピー(C)...] をクリックします。

[証明書のエクスポートウィザードが起動します。



← ● 疑明書のエクスポート ウィザード	×
証明書のエクスポート ウィザードの開始	
このウィザードでは、証明音、証明音信頼リストおよび証明音失効リストを証明音ストアからディスクにコピ ーします。	
証明機関によって進行された証明書は、ユーザーDを確認し、データを使調したり、またはセキュリティで停請 されたネットワーク環境を提供するための情報を含んでいます。証明書ストアは、証明書が保留されるシステ 人上の模式です。	
続行するには、 (次へ) をクリックしてください。	

次へ(N) キャンセル

- [次へ(N)] をクリック
- [Base 64 Encoded X.509 (.CERT)(s)] を選択
- [次へ(N)] をクリック
- [参照(R)...] をクリックして出力先を選択
- [次へ(N)] をクリック
- [完了] をクリック

エクスポートしたSAML IdP暗号用証明書をローカルPCに保存します。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

5.5. SAML IdP 署名用証明書の取得

Gléas に設定する SAML IdP の署名用証明書を ADFS から取得します。

スタートメニューから [ADFS の管理] を起動します。

左ペインの [サービス] > [証明書] を選択します。

中央ペインの [トークン暗号化解除] の証明書を右クリックしてメニューを表示します。

[証明書の表示(V)]をクリックすると[証明書]ダイアログボックスが表示されます。

砩 証明書		×
全般 詳細 証明のパス		
表示(S): <すべて>	~	
フィールド	值 ^	
■ バージョン	V3	
回 シリアル番号 回 黒タマルゴリズム	cha256RSA	
国家名ハッシュアルゴリズム	sha256	
🛄 発行者	AND INCOME.	
有効期間の開始 方効期間の終了	and the second second	
(回) サブジェクト	· · · · · · · · · · · · · · · · · · ·	
V3		
	プロパティの編集(E) ファイルにコピー(C)	
	ОК	

[詳細]タブで[ファイルにコピー(C)...] をクリックします。

[証明書のエクスポートウィザードが起動します。



← ● 疑明書のエクスポート ウィザード	×
証明書のエクスポート ウィザードの開始	
このウィザードでは、証明音、証明音信頼リストおよび証明音失効リストを証明音ストアからディスクにコピ ーします。	
証明機関によって進行された証明書は、ユーザーDを確認し、データを使調したり、またはセキュリティで停請 されたネットワーク環境を提供するための情報を含んでいます。証明書ストアは、証明書が保留されるシステ 人上の模式です。	
続行するには、 (次へ) をクリックしてください。	

次へ(N) キャンセル

- [次へ(N)] をクリック
- [Base 64 Encoded X.509 (.CERT)(s)] を選択
- [次へ(N)] をクリック
- [参照(R)...] をクリックして出力先を選択
- [次へ(N)] をクリック
- [完了] をクリック

エクスポートしたSAML IdP署名用証明書をローカルPCに保存します。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

6. Gléas の管理者設定 (Windows 向け)

GléasのWindows向けUA(申込局)をSAML SPとして動作するように設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

GléasのRA (登録局) にログインします。

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、設定を行うUA (申込局)

をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

▶<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、基本設定で以下の設定を行います。

● [証明書ストアへのインポート]をチェック

UA 申込局

- 証明書ストアの選択で、[ユーザストア]を選択
- 証明書のインポートを一度のみに制限する場合は、[インポートワンスを利用する]に

チェック

▶基本設定	
 トークンへのインボート Ш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) CA証明書を含めない	 管理するトークン Gemalto.NETカード ▼ 証明書ストアの種類 ユーザストア ▼ インボートワンスを利用する 全 登録申請を行わない 登録読済みデバイスのみインボート許可 存

[上級者向け]をクリックします。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力

※ https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx

● [ログアウト URL]を入力

※ https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx

- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID] を入力

※ http://[フェデレーションサービス名]/adfs/services/trust※https ではなく、http であることに注意

● [IdP SSO URL] を入力

※ https://[フェデレーションサービス名]/adfs/ls

● [IdP SLO URL] を入力

※ https://[フェデレーションサービス名]/adfs/ls

- [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定
- [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定
- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択
- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]をチェック
- [ログアウトレスポンスに署名]をチェック

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

https://	/adfs/ls/ldpInitiatedSignOr	n.aspx
https://	/adfs/ls/ldplnitiatedSignOr	n.aspx
https://	/ua/ /saml	
□ 削除する		
★ saml_sp 有効期限:		
□ 削除する		
兼 あり		
https://	/ua/ /saml/acs	
https://	/ua/ /saml/logout	
urn:oasis:names:tc:SAML:1.1:	nameid-format:unspecified	
http://	/adfs/services/trust	
https://	/adfs/ls	
https://	/adfs/ls	
□ 削除する		
★ ADFS Signing - 有効期限:		
□ 削除する		
ADFS Encryption -		
有効期限:		
有効期限: -256 ▼		
有刘典卿侯: -256 ✔ 256 ✔		
有双角PBE: -256 ▼ 256 ▼		✓ ログアウトリクエストに署名
	https:// https:// 前原除する 素 samL sp 有効期形限: 前原除する 黄 あり https:// https:// https:// https:// https:// https:// 前即除する 資源除する	https:///////////////////////////////////

設定完了後、[保存]をクリックし保存します。

また、認証デバイス設定の以下項目にチェックがないことを確認します。

- iPhone/iPad の設定の、[iPhone / iPad 用 UA を利用する]
- Android の設定の、[Android 用 UA を利用する]

以上でGléasの設定は終了です。

7. クライアントからのアクセス (Windows)

7.1. シングルサインオンで UA にログイン

PCのブラウザ (Edge) で、ADFSのサインインページにアクセスします。

※URL https://[UAのFQDN]/ua/[UAの名前]/saml/sso

アクセスするとADFSのサインインページに遷移します。



[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

ADFSのサインインページからUAにログインすることもできます。

※URL https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx



サイトを選択してサインインします。



[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

7.2. クライアント証明書のインポート

[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行

われます。

	· []						U
\rightarrow C =	-				A" to 💿	¢ 🧔	٠
					プライベートC	₄ Gléå	Š UA
テスト ユーザー さんのぺ・	ージ]						ログアウト
ユーザ情報	_	_	_		_	_	_
🔍 テスト ユーザー さんの	マージ						
🖢 ユーザ情報							
シューザ情報		※3日岐 ·					
 2-ザ情報・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		登録目時:					
 ▲ ユーザ情報・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		登録日時:					
▲ ユーザ情報 ·······・ > ユーザ > 姓: テスト 名: ユーザー > ユーザD: > メールアドレス:	-	登録日時:					
シューザ情報 シューザ シューザ シューザ ンーガロ: シールアドレス: パスワード:		登録日時:					
 ユーザ情報 シーザ メロッサ メロッサ メールアドレス: メロットアドレス: メロットアドレス: メロットアドレス: 		堂録日時:					
 ユーザ情報・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		室結日時:	D				
 ▲ ーザ情報 ▶ ユーザ ▶ ユーザ > ☆: デスト 名: ユーザ- > ユーザD: > メールアドレス: > パスワード: ※ 証明書情報 ※ 変行済み証明者 * 	発行局	登却日時:	 ביישור שלי	有効期限	証明書	Z⊦アヘインポート	

※ 証明書インポート時にルート証明書のインポート警告が出現する場合は、システム管理者に拇印 を確認するなど正当性を確認してから[はい]をクリックします

セキュリテ	1 普告	\times
4	発行者が次であると主張する証明機関 (CA) から証明書をインストールしよ うとしています:	
	証明書が実際に からのものであるかどうかを検証 できません。 に連絡して発行者を確認する必要が あります。次の番号はこの過程で役立ちます:	
	拇印 (sha1):	
	警告: このルート証明書をインストールすると、このCAによって発行された証明書は 自動的には預されます。確認されていない毎印付きの証明書をインストール することは、セキュリティ上、危険です。[はい]をクリックすると、この危険を認 識したことになります。 2の証明書をインストールしますか?	
	はい(Y) しいえ(N)	

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

インポートワンス機能を有効にしている場合は、インポート完了後に強制的にログアウ

トさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ロ

Google	× 🛛 プライベートCA Gléas	テストユーザー × +				-	
\rightarrow C \ominus	The state being the	100 C		Aø -	ia 🐵 {	3 🧔	٠
				プライ	r«-ьса (Gléå	Ŝ UA
テスト ユーザー さ	んのページ]						<u>コグアウト</u>
ユーザ情報							
🙎 テスト ユーザ・	ーさんのページ						
●ユーザ情報・・・							*
▶ユーザ	절양	日時:					
>姓:굿자 名:그	.ーザー						
> ユーザID :							
> ユーザID : > メールアドレス : > パスワード : *******	*****						
> ユーザロ : > メールアドレス : > パスワード : ***********************************	*****						
> ユーザロ: > メールアドレス: > パスワード: ************************************	*****						
> ユーザD: > メールアドレス: > パスワード: ************************************	****** 発行局		シリアル	有幼期限	証明書ストラ	アヘインポート	

グインしてインポートを行うことはできません。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

8. Gléas の管理者設定 (iPhone 向け)

GléasのiPhone向けUA(申込局)をSAML SPとして動作するように設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

GléasのRA (登録局) にログインします。

UA 申込局

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、設定を行うUA (申込局)

をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

▶ <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・[インポートワンスを利用する]にチェック

この設定を行うと、GléasのUAからインポートから指定した時間(分)を経過した後

は、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)。

これにより複数台のデバイス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	
 トーケンへのインボート 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) CA証明書を含めない 	 管理するトークン Gemalto.NETカード▼ 証明書ストアの種類 ユーザストア マ ひボートワンスを利用する 登録申請を行われい 登録泳みデバイスのみインボート許可
	保存

[上級者向け]をクリックします。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力

※ https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx

● [ログアウト URL]を入力

※ https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx

- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID] を入力

※ http://[フェデレーションサービス名]/adfs/services/trust※https ではなく、http であることに注意

● [IdP SSO URL] を入力

※ https://[フェデレーションサービス名]/adfs/ls

● [IdP SLO URL] を入力

※ https://[フェデレーションサービス名]/adfs/ls

- [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定
- [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定
- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択
- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]をチェック
- [ログアウトレスポンスに署名]をチェック

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

✓ SAML2.0で外部認証する			
ホームURL	https://	/adfs/ls/ldplnitiatedSignOn	1.aspx
ログアウトURL	https://	/adfs/ls/ldplnitiatedSignOn	1.aspx
SP Issuer	https://	/ua/ /saml	
SP証明書	□ 削除する		
	★ saml_sp 有効期限:		
SP 秘密鍵	□ 削除する		
	兼 あり		
SP ACS URL	https://	/ua/ /saml/acs	
SP SLO URL	https://	/ua/ /saml/logout	
名前ID形式	urn:oasis:names:tc:SAML:1.1	nameid-format:unspecified	
IdP エンティティID	http://	/adfs/services/trust	
IdP SSO URL	https://	/adfs/ls	
IdP SLO URL	https://	/adfs/ls	
IdP 署名用証明書	□ 削除する		
	★ ADFS Signing - 有効期限:		
ldP 暗号用証明書	□ 削除する		
	★ ADFS Encryption - 有効期限:		
	-256 🗸		
『イジェストアルゴリズム <mark>SHA</mark>			
『イジェストアルゴリズム <mark>SHA</mark> ใ名アルゴリズム <mark>RSA SHA-</mark>	256 🗸		
ぎイジェストアルゴリズム SHA 署名アルゴリズム RSA SHA- ✔ 認証リクエストに署名	256 🗸		✓ ログアウトリクエストに署名

設定完了後、[保存]をクリックし保存します。

[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。

🦸 認証デバイス情報	
▶iPhone / iPadの設定	
□ iPhone/iPad 用 UA を利用する	
保存	

構成プロファイルに必要となる情報の入力画面が展開されるので、以下設定を行います。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

【画面レイアウト】

- [iPhone用レイアウトを利用する]をチェック
- [ログインパスワードで証明書を保護]をチェック

【iPhone構成プロファイル基本設定】

● [名前]、[識別子]に任意の文字を入力 (必須項目)

🦸 認証デバイス情報-		
▶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 ○ Mac OS X 10.7以降の接続	引する 売を許可	✓ 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	月する	 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	Y
iPhone 構成プロファイル基準	本設定	
名前(デバイス上に表示)	サンブルプロファイル	
識別子(例: com.jcch- sss.profile)	local.jcch-sss.profile	
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
	サンプル構成プロファイル	

各項目の入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

9. クライアントからのアクセス (iPhone)

9.1. シングルサインオンで UA にログイン

iPhoneのブラウザ (Safari) で、ADFSのサインインページにアクセスします。

※URL https://[UAのFQDN]/ua/[UAの名前]/saml/sso

アクセスするとADFSのサインインページに遷移します。

JS3 ADFS連携デモ
サインイン
•••••
サインイン

[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

ADFSのサインインページからUAにログインすることもできます。

※URL https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx



サイトを選択してサインインします。

JS3 ADFS連携デモ
サインイン
•••••
サインイン

[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

9.2. クライアント証明書のインポート

[ダウンロード]をタップし、構成プロファイルのダウンロードをおこないます。

プライベー	-eca Gléäs 🔼	プラ	۶イベートca Gléäs 🛯		JライベートCA Gléä	Ŝ UA
テスト ユーザー さん	のページ	テスト ユーザー	- さんのページ	テスト	ユーザー さんのページ	
ユーザロ	advance/light one cost	ユーザID	Inflamation on our	ユーザ	D Inclusion Inclusion	
姓	テスト	姓	テスト	姓		テスト
名	ユーザー	名	ユーザー	名	۲	ーザー
メール		メール		メール		
有効期限	ダウンロード済み	このWebサー ウンロードし ますか?	イトは構成プロファイルをダ ようとしています。許可し	有効	プロファイルがダウンロードさ れました	:済み
有効期限	ダウンロード		無視 許可	有効期	プロファイルをインストールするには設定 Appで再確認してください。	3-6
Copyright (C) 2010-2022 JCCH Security	ログアウト Solution Systems Co.,Ltd. All rights reserved.	Copyright (C) 2010-2022 ICC	ロダアクト 11 Security Solution Systems Co.J.d. All rights reserved.	Copyright	閉じる	アプリウト s reserved.

※ 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

画面の表示にしたがい設定を開くと、プロファイルがダウンロードされた旨が表示され

るので、インストールをおこないます。

設定		キャンセル プロファイル インストー	- <i>n</i>
Apple ID、iCloud、メディアと購入	>	サンブルブロファイル JCCH セキュリティ・ソリューション・ システムズ	
プロファイルがダウンロード済み	>	Signed by Not Signed Description サンプル情感プロファイル	
		More Details	>
		Remove Downloaded Profile	

[インストール]をタップして続行してください。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

インストール中にルート証明書のインストール確認画面が現れるので、内容を確認し

[インストール]をタップ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

キャンセル	警告	インストール
管理対象外ルート 証明書 ールすると、if 書のリストに減 定"で有効にす イト用には信頼	^{証明書} Phone にある信 追加されます。 るまで、この記 頁されません。	をインスト 頼できる証明 "証明書信頼設 E明書は Web サ

インストール完了画面になりますので、[完了]をタップして終了します。

	インストール完了	完了
Ø	ナンプルプロファイル CCHセキュリティ・ソリューション・ バテムズ	
Signed by Description Contains	Not Signed サンプル構成プロファイル 証明書: 2	
More De	tails	>

なお [More Details]をタップすると、インストールされた証明書情報を見ることがで

きます。必要に応じて確認してください。

く 戻	3	サンプルプロファイル	
11	[明書	(2)	
1	⊗		>
1	0	発行元: 有効期限:	>

Safariに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、iPhoneでの構成プロファイルのインストールは終了です。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

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となります。

プライ	«-pca Gléäs 🛯
テスト ユーザー さ	きんのページ
ユーザID	
姓	テスト
名	ユーザー
メール	
有効期限	ダウンロード済み
有効期限	ダウンロード済み
Copyright (C) 2010-2022 JCCH Se	ログアウト curity Solution Systems Co.,Ltd. All rights reserved.

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

10.Gléas の管理者設定 (Android 向け)

GléasのAndroid向けUA(申込局)をSAML SPとして動作するように設定します。

※ 下記設定は、Gléas納品時等に弊社で設定を既におこなっている場合があります

GléasのRA (登録局) にログインします。

UA 申込局

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、設定を行うUA (申込局)

をクリックします。

※ 実際はデフォルト申込局ではなく、その他の申込局の設定を編集します

▶ <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・[インポートワンスを利用する]にチェック

この設定を行うと、GléasのUAからインポートから指定した時間(分)を経過した後

は、証明書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

れにより複数台のデバイスへの証明書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	
 トーグンへのインボート □ 証明書ストアへのインボート ☑ ダウンロードを許可 ダウンロードで総特間(分) □ ローズのロードのにはいいいいい 	 管理するトークン Gemaito NETカード ▼ 証明書ストアの種類 ユーザストア ▼ マ ペンボートワンスを利用する ご 登録申請ざ行わない □ 登録済みデバイスのみインボート許可
□ CAELUH書を含めない	保存

[上級者向け]をクリックします。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

- [SAML2.0 で外部認証する]をチェック
- [ホーム URL]を入力

※ https:// [フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx

● [ログアウト URL]を入力

※ https:// [フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx

- [SP 証明書]に SAML SP 署名用証明書ファイルを指定
- [SP 秘密鍵]に SAML SP 署名用証明書の秘密鍵ファイルを指定
- [IdP エンティティ ID] を入力

※ http://[フェデレーションサービス名]/adfs/services/trust※https ではなく、http であることに注意

● [IdP SSO URL] を入力

※ https://[フェデレーションサービス名]/adfs/ls

● [IdP SLO URL] を入力

※ https://[フェデレーションサービス名]/adfs/ls

- [IdP 署名用証明書]に IdP 署名用証明書ファイルを指定
- [IdP 暗号用証明書]に IdP 暗号用証明書ファイルを指定
- [ダイジェストアルゴリズム]に「SHA-256」を選択
- [署名アルゴリズム]に「RSA SHA-256」を選択
- [署名リクエストに署名]をチェック
- [ログアウトリクエストに署名]をチェック
- [ログアウトレスポンスに署名]をチェック

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

- [メタデータに署名する]をチェック
- [署名をメッセージに埋め込む]はチェックしない

ログイン方法			
☑ SAML2.0で外部認証する			
ホームURL	https://	/adfs/ls/ldplnitiatedSignO	n.aspx
ログアウトURL	https://	/adfs/ls/ldplnitiatedSignO	n.aspx
SP Issuer	https://	/ua/ /saml	
SP証明書	□ 削除する		
	★ saml_sp 有効期限:		
SP 秘密鍵	□ 削除する		
	🌻 あり		
SP ACS URL	https://	/ua/ /saml/acs	
SP SLO URL	https://	/ua/ /saml/logout	
名前ID形式	urn:oasis:names:tc:SAML:1.1	nameid-format:unspecified	
IdP エンティティID	http://	/adfs/services/trust	
IdP SSO URL	https://	/adfs/ls	
IdP SLO URL	https://	/adfs/ls	
IdP 署名用証明書	□ 削除する		
	★ ADFS Signing - 有効期限:		
IdP 暗号用証明書	□ 削除する		
	★ ADFS Encryption - 有効期限:		
ダイジェストアルゴリズム SHA	-256 🗸		
署名アルゴリズム RSA SHA	-256 🗸		
☑ 認証リクエストに署名			☑ ログアウトリクエストに署名
☑ ログアウトレスボンスに署名	2		☑ メタデータに署名
□ 署名をメッセージに埋め込	む		

設定完了後、[保存]をクリックし保存します。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

[認証デバイス情報]の[Androidの設定]までスクロールし、[Android用UAを利用する]を

チェックします。

▶ Android の設定	
Android 用 UAを利用する	
ダウンロードの動作	
 □ ログインパスワードで証明書を保護 ☑ 数字のみの PIN 7 証明書ダウンロードの種類 ○ PKCS#12ダウンロード 	送表示

証明書のダウンロードに必要となる情報の入力画面が展開されるので、以下設定を行い

ます。

- [数字のみのPINを表示]をチェック
- [証明書ダウンロードの種類]]を[PKCS#12ダウンロード]を選択

各項目の入力が終わったら、 [保存]をクリックします。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

証明書インポートアプリ CertImporter for Android を使用する場合は、[証明書インポ

ートアプリ連携の設定]までスクロールし、[証明書インポートアプリを利用する]をチェ

ックします。

▶証明書インボートアブリ連打	携の設定	
 ☑ 証明書インボートアブリを計 インボートボタンを表示 証明書一覧をアブリで表示 証明書と一緒こUAマニフっ 証明書と一緒こUAマニフっ 証明書PINをGléasで生成 	川用する (MacOSXのみ) ・ストをダウンロード	
UAマニフェスト		
ログインURL		
信頼するCA証明書	ファイルの選択ファイルが選択されていません	
証明書PIN生成シード		
<u>UAマニフェスト要求ファイル</u> を	ダウンロードして、弊社サポートに送付してください	
UAマニフェストのアップロード	ファイルが選択されていません	
	保存	

入力が終わったら、 [保存]をクリックします。

以上でGléasの設定は終了です。

11. クライアントからのアクセス (Android)

11.1. シングルサインオンで UA にログイン

Androidのブラウザ (Chrome) で、UAのシングルサインオンURLにアクセスします。

※URL https://[UAのFQDN]/ua/[UAの名前]/saml/sso

アクセスするとADFSのサインインページに遷移します。



[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

ADFSのサインインページからUAにログインすることもできます。

※URL https://[フェデレーションサービス名]/adfs/ls/IdpInitiatedSignOn.aspx

	+	1	0
203 ADFS連携771			
サインインしていません。			
○ このサイトにサインインしてくださ	い。		
● 次のいずれかのサイトにサインイン	してくだ	さい:	
		\sim	
サインイン			

サイトを選択してサインインします。

<u>۵</u>	+	1	0
/12 AD7128771			
サインイン			
サインイン			

[サインイン]をクリックします。

UAにログインし、ユーザ専用ページが表示されます。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

11.2.クライアント証明書のインポート

[ダウンロード]をタップし、証明書ファイルのダウンロードをおこないます。

	JETA-PCA Gléäs UA	プライベー	-pca Gléäs 💵	プライ	«-pca Gléäš 🛯
テストユー	ザー さんのページ	テスト ユーザー さんの	ページ	デ証明書を抽出	
ユーザID		ユーザID		証明書を抽出するため	n かのパスワードを入力しま
姓	テスト	姓	テスト	\$ 5.	
名	ユーザー	名	ユーザー	4	
メール		メール		3	
				NA	キャンセル OK
有効期限	ダウンロード	証明書 PIN:	決定 キャンセル	有効期限	ダウンロード
	ログアウト		ログアウト		ログアウト
Copyright (C) 2010-21 reserved.	022 JCCH Security Solution Systems Co.,Ltd. All rights	Copyright (C) 2010-2022 JCCH Security reserved.	Solution Systems Co., I.td. All rights		

※ 「証明書 PIN」の値を「証明書を抽出」のパスワードとして入力します。

※ 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

[OK]をタップして続行してください。

「証明書の種類の用途」のダイアログが出るので、用途を選択します。

×	証明書の種類の選択		
A	 VPN とアプリユーザー証明書 Wi-Fi 証明書 		1 1 1
Cor rese	キャンセル	ОК	

[OK]をタップして続行してください。

N	この証明書の名前で い	を指定してく	ださ	
¥	証明書名 			۲ ۲
Cor rest		キャンセル	ОК	

[OK]をタップします。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

Chromeに戻り、[ログアウト]をタップしてUAからログアウトします。

以上で、Androidでの証明書ファイルのインストールは終了です。

シングルサインオンによる Gléas UA ログイン (AD FS 連携)

[設定]>[セキュリティ]>[詳細設定]>[暗号化と認証情報]>[ユーザー認証情報]>[証明書 の名前]とタップすると、インストールされた証明書情報を見ることができます。必要 に応じて確認してください。



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となります。

プライグ	K-PCA Gléäš UA
テスト ユーザー さ	んのページ
ユーザID	
姓	テスト
名	ユーザー
メール	
有効期限	ダウンロード済み
有効期限	ダウンロード済み
Copyright (C) 2010-2022 JCCH Sect	ログアウト rity Solution Systems Co.,Ltd. All rights reserved.

12. 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や本検証内容、テスト用証明書の提供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