

プライベート認証局Gléas ホワイトペーパー

KAMOME SSOを使ったG Suiteへの証明書認証

Ver.1.0 2019 年 3 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

目次

1. はじ	めに	1
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. KAM	10ME SSO の設定	5
2.1	サーバ証明書/秘密鍵の設定	5
2.2	署名用証明書の設定	8
2.3	認証ルールの作成	9
2.4	Apache の証明書認証設定	
2.5	ホストアイデンティティープロバイダの設定	
2.6	G Suite の設定	13
3. G Su	iite での設定	14
3.1	シングルサインオンの設定	14
4. クラ	イアントでの操作	14
4.1	クライアント証明書のインストール	14
4.2	G Suite へのシングルサインオン	
5. 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]で発行した電子証明書を使って、かもめエ ンジニアリング株式会社の提供するシングルサインオン[KAMOME SSO]を経由した、G SuiteへのSAMLを用いたシングルサインオンを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。

- ▶ [シングルサインオン] KAMOME SSO (1.2.2)
- [認証局] JS3 プライベート認証局Gléas (1.16.9)
 ※以後、「Gléas」と記載します
- ▶ [SaaS] G Suite Business ※以後、「G Suite」と記載します
- [クライアント] Windows 10 / Internet Explorer (11.316)
 ※以後、「Windows」と記載します
- [クライアント] iOS 12.1.4 / Safari (12.0.3)
 ※以後、「iOS」と記載します
- [クライアント] macOS Mojave (10.14.3) / Safari (12.0.3)
 ※以後、「macOS」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。

- KAMOME SSOの基本設定
- G Suiteの基本設定
- 各クライアントのネットワーク設定

● Gléasでのアカウント登録、サーバ証明書、クライアント証明書の発行等の基本操作 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、以下の構成で検証します。



- 1. クライアントはGléasからクライアント証明書を取得する
- クライアントのブラウザでG Suite (Gmail) にアクセスすると、KAMOME SSOに転送される
- 3. KAMOME SSOとクライアント間で、Gléasから取得したクライアント証明書による認 証がおこなわれる
- 4. KAMOME SSOでの認証に成功すると、G Suite (Gmail) にログインする

2. KAMOME SSO での設定

2.1 サーバ証明書/秘密鍵の設定

あらかじめGléasでKAMOME SSOのサーバ証明書を発行し、ダウンロードしておきます。

証明書	▶一覧に戻る	l
JCCH-SSS demo CA#11652	E₂2	ł
★ 証明書情報		ļ
▶ kamome	開始日:2019/02/13 11:43 終了日:2030/01/06 11:43	ł
▶ 説明:	最終更新:2019/02/13 11:44 <mark>編集</mark>	ł

OpenSSLを使ってサーバ証明書から秘密鍵を取り出し、以下のファイル名を付けます。

● サーバ証明書 localhost.crt サーバ秘密鍵 localhost.key

※参考

openssl pkcs12 -in kamome.p12 -clcerts -nokeys -out localhost.crt openssl pkcs12 -in kamome.p12 -nocerts -nodes -out localhost.key

Webminで、[その他]→[アップロードとダウンロード]→[Upload to server]と進みます。

යි Webmin 🥢	⊘ ッシュポード		☆ U	pload and Download
検索	٩	Download from web Upload to serve	er Download from server	
Ø Webmin		This page allows you to upload one or more	files from the PC on which your web	browser runs to the system running W
▶ システム	•			Upload files to server
◀ サーバ	•	Files to upload	0 0 0	
◆ その他	•	File or directory to upload to	1	æ
アップロードとダウン 0 カスタム コマンド	/ u -ド	Owned by user	root &	
0 コマンドシェル		Owned by group	● デフォルト ○	22
o システムおよびサー/	〈のステータス	Extract archive or compressed files?	ି Yes, then delete ି ដែល 🖲	いいえ
◎ ネットワーク		Send email when uploads are done?	● ເບເບえ ○ Yes, to address	
€ モジュールをリフレ	ッシュする	⊘ Upload		

[Files to upload]でサーバ秘密鍵を選択します。[File or directory to upload to]に [/etc/pki/tls/private/]と入力して、[Upload]をクリックします。

Files to upload	⊗ localhost	.key 📎	0 0
File or directory to upload to	/etc/pki/tls/priva	ate/	
Owned by user	root	2	
Owned by group	● <i>デ</i> フォルト ○		22
Extract archive or compressed files?	• Yes, then delete	e ⊖ はい ⊛ เ	いいえ
Send email when uploads are done?	●いいえ ○ Yes,	to address	

以下の画面が表示されます。[uploads and downloads from に戻る]をクリックします

ය Webmin	⊘ ダッシュポード	← C Upload Files
校索 Webmin	۹	Saving file /etc/pki/t/s/private//localhost.key wrote 1.81 kB
♪ システム ◀ サーバ	•	← uploads and downloads form に戻る

[Files to upload]でサーバ証明書を選択します。[File or directory to upload to]に [/etc/pki/tls/certs/]と入力して、[Upload]をクリックします。

Download from web	Upload to server	Download	l from	server		
This page allows you to upload one or more files from the PC on which your we					ur web	browser ru
			Uplo	ad file	s to se	erver
Files to upload	Ø	localhost.crt	۲	۲	0	
File or directory to upload	ito /etc/	oki/tls/private/				

[Webmin]→[Webmin設定]→[Webminの再起動]をクリックするとサーバ証明書/秘密鍵の 設定が有効になります。

ی Webmin	の ダッシュポード	0			C Webrin K	nin 設定 ニジョン1.900
60.7%	•	ようしていた。 ドアドレスの アクセス制御	ボートとアド レス	▲ □7	プロキシサー パ	ユーザインタ -フェイス
 く その他 ① ネットワーク ご モジュールをリフ 	・ ・ レッシュする	インデックス ページオブシ ョン	Webmin のア ップグレード	REE.	2 段階認証	そジュールの 再割り当て
• * -< • H	D ₀ å amadmin	管任照会	を 匿名モジュー ルアクセス	ファイルのロ ック	モバイルデパ イスオプショ ン	プロックした ホストとユー ザ
		ウェブサーバ オプション	Webmin 予定 根総	電子メール送信	《 SSL 暗号化	E E E E
		-● 起動時に開 C Webminの利	始する ® は 5記動 このボタ	はい ○ いいえ この でな タンをクリックする	オプションで起動 い場合に はい をJ とWebminを再起動	時にWebminを開 選択すると新しい bします。最近Pei

[サーバ]→[Apache Webサーバ]→[変更を適用]アイコンをクリックして、Apache Webサ ーバを再起動します。

ل Webmin	の ダッシュボード	٥		☆ Apache Webサーバ Apache バージョン 2.4.6	
検索	Q				
 Webmin 		グローバル	設定 存在する仮想ホスト	仮想ホストの作成	
# システル		☞ 全て選択	ピ 選択を反転		
F 2014	•		他のすべての仮想サーバのデ	フォルト設定を定義し、処理されなかった要求をすべて処理します。	
⋞ サーバ		0	アドレス 任意	サーバ名 自動	
L		69	ポート 任意	ドキュメントのルート /var/www/html	
Apache Vebサー/	C.		全てのアドレスで名前ペース	のサーバ を取り扱う	
	.	- 0	アドレス 任意	サーバ名 自動	
< その他	•	60	ポート 10443	ドキュメントのルート /var/www/html	
◎ ネットワーク	•	☞ 全て選択	15 選択を反転		

2.2 署名用証明書の設定

あらかじめ Gléas で SAML の署名用証明書を発行し、ダウンロードしておきます。



ダウンロードした PKCS12 形式の証明書ファイルを、JDK を使ってキーストアファイルに 変換します。

keytool -importkeystore -srckeystore signing.p12 -srcstoretype PKCS12 -srcstorepass xxxxxx -destkeystore signing.jks -deststoretype JKS -deststorepass yyyyyy -destkeypass zzzzz

※srcstorepass には Gléas から署名用証明書をダウンロードする際の保護パスワードを入力します。 deststorepass、destkeypass には任意のパスワード(6 文字以上)を入力します。

キーストアファイルを KAMOME SSO の以下のフォルダに配置します。 /usr/share/tomcat/openam/openam/private/

Tomcat プロセスの実行ユーザである"tomcat"のみがキーストアファイルを読み込めるようにパーミッションを設定します。

OpenAM に管理者ログインして以下の URL を開き、キーストアファイルに設定した deststorepass を符号化します。

https://hostname:10443/openam/encode.jsp





符号化されたパスワードは

別のパスワードを符号化する

符号化したパスワードを以下のファイルに保存します。 /usr/share/tomcat/openam/openam/private/.storepass

Tomcat プロセスの実行ユーザである"tomcat"のみがファイルを読み込めるようにパーミッションを設定します。

destkeypass も同様に符号化し以下のファイルに保存します。 /usr/share/tomcat/openam/openam/private/.keypass

Tomcat プロセスの実行ユーザである"tomcat"のみがファイルを読み込めるようにパーミ ッションを設定します。

OpenAM で、[設定]→[サーバーおよびサイト]→[デフォルトのサーバー設定値]→[セキュ リティ]→[キーストア]と進み、下記の項目を設定し、[保存]をクリックします。

キーストアファイル /usr/share/tomcat/openam/openam/private/signing.keystore キーストアパスワードファイル

/usr/share/tomcat/openam/openam/private/.storepass 非公開鍵パスワードファイル /usr/share/tomcat/openam/openam/private/.keypass 証明書エイリアス 署名用証明書のサブジェクト名

設定を反映させるため、Webminで、[システム]→[起動およびシャットダウン]と進み、 [tomcat.service]にチェックを入れて[選択したものを再起動]をクリックし、Tomcatを再 起動します。

2.3 認証ルールの作成

OpenAM で、[アクセス制御]→[最上位のレルム]をクリックします。

KAMOMES	SO 🛔			-
共通タスク	アクセス制御	連携	設定	セッション

レルムは、OpenAM が設定情報の整理に使用する単位です。レルム内では、認証プに 最上位のレルムは、OpenAM の配備時に作成されます。最上位のレルムは、OpenAI

レルム	
•	検索
レルム	(1項目)
新規	削除
28	レルム名
	/ (最上位のレルム)

[認証]→[モジュールインスタンス]→[新規]をクリックします。

モジュールインスタンス

_		
l	モジュ	ールインスタンス (5 項目)
l	新規	N IR
	28	名約
		DataStore
	0	HOTP
	0	LDAP
	0	OATH
	0	UserId

任意の[名前]をつけ、[タイプ]の[証明書]を選択し、[了解]をクリックします。 新規モジュールインスタンス

* 名前:	CertModule
* タイプ:	 Active Directory
	O Device Print
	OHOTP
	○ HTTP 基本
	OJDBC
	OLDAP
	MSISDN
	OATH
	OAuth 2.0
	Persistent Cookie
	RADIUS
	○ SAE
	 Scripted Module
	Windows NT
	○Windows デスクトップ SSO
	WSSAuth
	○ アダプティブリスク
	○ データストア
	○ メンバーシップ
	○ユーザーID
	 証明書
	○匿名
	○連携

[アクセス制御]で最上位のレルムを開き、[認証]→[認証連鎖]→[新規]をクリックします。

100 007 140 444

80	ALC NO. 304	I
	12150	續 (1項目)
1	新規	WL Risk
1	38	名前
	0	IdapService

任意の[名前]を入力して、[了解]をクリックします。インスタンスの[追加]をクリックし、 [インスタンス]に作成したモジュール名を選択し、[条件]に[必要]を選択して、[保存]をク リックします。

追加	削除	並べ替え		
インスタン	/ X			
この連続に	は定義され	った値がありません。	GBM	ボタンを押して作り

(1 項目)				
<u>追加</u> 削除 並べ替え				
🗵 🔠 インスタンス	条件	オプション		
CertModule \$	<u>必要 </u> \$			

[アクセス制御]で最上位のレルムを開き、[認証]→[コア]→[組織認証設定]で、作成した認 証連鎖を選択し、[保存]をクリックします。

3 <i>7</i>	
すべてのコア	设定
組織認証設定:	CertAuthChain ・ ユーザーのデフォルト認証連鎖。

[コア]→[すべてのコア設定]を開き、[ユーザープロファイル]で[必須]を選択して、[保存] をクリックします。

コア		保存	リセット	認証へ戻る
レルム属性				
ユーザープロファイ	r JL			
ユーザーブロファイル:	 ユーザーエイリア 動的 必須 無視 	スを使用して	〔動的に	

2.4 Apache の証明書認証設定

Gléas から PEM 形式のルート証明書と CRL をダウンロードし、KAMOME SSO の下記のフ ォルダに配置します。

ルート証明書:http://hostname/crl/ia1.pem CRL:http://hostname/crl/crl_ia1.pem /etc/pki/tls/certs/

Webmin で、[サーバ]→[Apache Web サーバ]→[グローバル設定]→[設定ファイルの編集]と 進み、[ファイルのディレクティブを編集する:]で[/etc/httpd/conf.d/ssl.conf]を選択し、下 記項目を編集し、[セーブ]をクリックします。

SSLCACertificateFile /etc/pki/tls/certs/ia1.cer(PEM 形式:証明書名は各環境による) SSLCARevocationCheck chain SSLCARevocationFIle /etc/pki/tls/certs/ia1.crl (PEM 形式:CRL 名は各環境による) SSLVerifyClient optional SSLVerifyDepth 1



設定を反映させるため、[システム]→[起動およびシャットダウン]と進み、[httpd.service] にチェックを入れて[選択したものを再起動]をクリックし、Apacheを再起動します。

2.5 ホストアイデンティティープロバイダの設定

OpenAM で、[共通タスク]→[ホストアイデンティティープロバイダの作成]と進み、[署名 鍵]で、設定した署名用証明書を選択し、[新しいトラストサークル]で任意の名前を入力し、 [設定]をクリックします。

メタデータ

* * * *					
* 名前: h	* 名前: https://kamome.jcch-sss.local:10443/openam				
署名鍵:	camome 🕈 🕕				
トラストサークル					
表示されて	いる既存のトラストサークルから選択するか、またはこの IDP を含む,				
トラストサ	ー クル: 🔘 既存のトラストサークルに追加します 💿 新しいトラスト				
* 新しいト・	ラストサークル:				

2.6 G Suite の設定

OpenAM で、[共通タスク]→[Google Apps の設定]と進み、[新しい値]に、G Suite で使用す るドメインを入力し、[追加]と[作成]をクリックします。

Google の管理者画面に設定する [サインインページの URL][サインアウトページの URL][パスワード変更の URL]が表示されます。各項目のテキストをコピーします。

[検証用証明書]の[ダウンロードするには、ここをクリックします。]をクリックして、署名 用証明書をダウンロードします。

URL

サインインペー	https://kamome.jcch-sss.local:10443/openam/SSORedirect/metaAlias/idp
ジの URL:	OpenAM および Google Apps にサインインするための URL
サインアウトペ	https://kamome.jcch-sss.local:10443/openam/UI/Logout?goto=https://kamome.jcch-sss.local:10443/openar
ーシの URL:	サインアウト時のユーザーのリダイレクト先 URL
パスワード変更	https://kamome.jcch-sss.local:10443/openam/idm/EndUser
の URL:	ユーザーが OpenAM のパスワードを変更できる URL

検証証明書

検証証	BEGIN CERTIFICATE
明書:	MIID0jCCArqgAwlBAglCLYYwDQYJKoZlhvcNAQELBQAwSjEZMBcGA1UEAxMQSkNDSC1TU1MgZGVt
	byBDQTETMBEGCgmSJomT8ixkARkWA0NPTTEYMBYGCgmSJomT8ixkARkWCEpDQ0gtU1NTMB4XDTE5
	MDlyMjA4Mzk0NVoXDTlwMDlyMjA4Mzk0NVowQDEPMA0GA1UEAwwGa2Ftb21lMRMwEQYKCZImiZPy
	LGQBGRYDQ09NMRgwFgYKCZImiZPyLGQBGRYISkNDSC1TU1MwggEiMA0GCSqGSlb3DQEBAQUAA4IB
	DwAwggEKAolBAQD2Sqc9WPzH/+s3Tg/7CEY4EUbqmZS32fjUq2RPqi8EKowxnfCw0EnpqpRS09d+
	+pF0zXY8+HIWbjRwjaVYt3/k1a26jFi1+yukgwFvIXVTBZrCnEQy13H8vwg95nZ1AluAv0c0Jly3
	MWy7isOelAewEGz8ITGj6TJYGvqjHRFoRNt7Ki9wE+3GZg0lp+ZPNxck/hMeybvxa0y0Y7a6qCQF
	LobFeX7mnERp8N+kFqr8ljV3mQgwm0PwZvllveSZUyfZzZ7OuNEJWb3ONaSe+czP2Fpx3hx8kein
	/iJX2d5xpVh7cGmdZ68rrV3VKgqNfYv6vxZHD0SrFNF6mj/Rf67dAgMBAAGjgcswgcgwCQYDVR0T
	BAlwADAdBgNVHQ4EFgQU3cRNTBwUNghaTGgPPLL+Bf3QM58wegYDVR0jBHMwcYAU6kq9SbJKl7aJ
	jdbwB8LMdEpDp9KhTqRMMEoxGTAXBgNVBAMTEEpDQ0gtU1NTIGRlbW8gQ0ExEzARBgoJkiaJk/ls
	ZAEZFgNDT00xGDAWBgoJkiaJk/IsZAEZFghKQ0NILVNTU4IJAMrWseop2Gk0MBMGA1UdJQQMMAoG
	CCsGAQUFBwMCMAsGA1UdDwQEAwlFoDANBgkqhkiG9w0BAQsFAAOCAQEASPdqRcpybo9Oz1FNhpU8
	ダウンロードするには、ここをクリックします。

3. G Suite での設定

3.1 シングルサインオンの設定

G SuiteのAdmin画面で、[セキュリティ]→[シングル サインオン(SSO

)の設定]と進みます。

[サードパーティのIDプロバイダでSSOを設定する]にチェックを入れ、[ログイン ページのURL]、[ログアウト ページのURL]、[パスワード変更URL]に2.6項でコピーしたテキストを入力します。

[認証の確認]には2.6項でダウンロードした証明書ファイルをアップロードします。



[ドメイン固有の発行元を使用]にチェックを入れて[保存]をクリックします。

4. クライアントでの操作

4.1 クライアント証明書のインストール

クライアントのブラウザでGléasのユーザ用ウェブ画面にアクセスし、GléasでのユーザID とパスワードを入力しログインします。

●エンドユーザログイン [UA]				
・ユーザロ、パスワードを入力してロ ダイルてください。				
▶ユーザID				
▶パスワード				
	ロダイン			
<u>□</u>	スワードを忘れたら			

ログインすると、ユーザ専用ページが表示されます。

[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。

★ 証明書情報 · · · · · · · · · · · · · · · · · · ·								
▶ 発行済	▶発行済み証明書							
#	発行局	シリアル	有効期限	証明書ストアヘインボート				
² 1	JCCH-SSS demo CA	#11472	2030/01/06	証明書のインボート				

※スクリーンショットはWindows / Internet Explorerの場合

4.2 G Suite へのシングルサインオン

ブラウザで下記のURLにアクセスすると、KAMOME SSOに転送されます。 https://mail.google.com/a/ < ドメイン名 >

クライアント証明書の選択ダイアログが出現します。証明書を確認して[OK]をクリックします。

※ブラウザの設定によっては、クライアント証明書の選択ダイアログが出ない場合もあります



証明書のサブジェクト名は、Googleのユーザ名と一致している必要があります。Googleの ユーザー覧に存在しないサブジェクト名を持つ証明書では、Googleにログインできません。

また、証明書の発行者が2.4項で設定したルート証明書と違う場合は、KAMOME SSOによって接続が拒否されます。



Authentication failed.

ログインページに戻る

また、失効された証明書を選択した場合も、KAMOME SSOによって接続が拒否されます。 ※ApacheのCRLに証明書のシリアル番号が記載されている場合

証明書のサブジェクト名がGoogleのユーザ名と一致しているが、KAMOME SSOにユーザ がない場合も、KAMOME SSOによって接続が拒否されます。

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:050-3821-2195 Mail:sales@jcch-sss.com

■KAMOME SSOに関するお問い合わせ

かもめエンジニアリング株式会社 Tel: 03-6457-5237 Mail: sales@kamome-e.com Webフォーム: https://kfep.jp/contact