



JCCH・セキュリティ・ソリューション・システムズ

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

- ・ 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	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. KAMOME 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	11
2.5 ホストアイデンティティプロバイダの設定	12
2.6 G Suite の設定	13
3. G Suite 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	15
5. 問い合わせ	16

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。

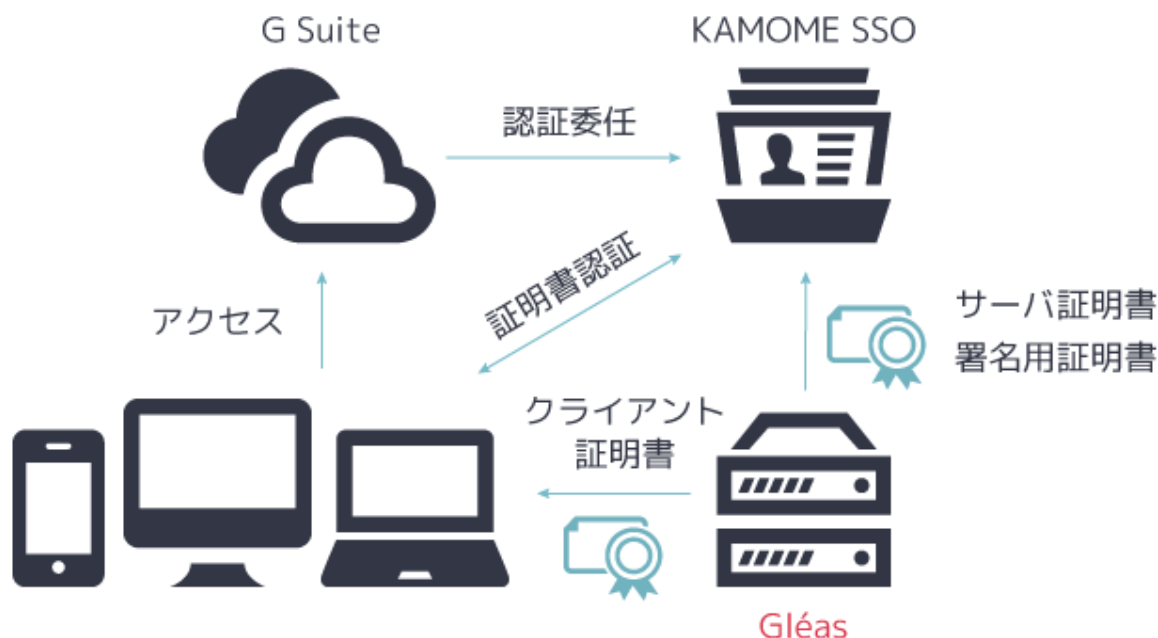
- [シングルサインオン] KAMOME SSO (1.2.2)
- [認証局] JS3 プライベート認証局Gléas (1.16.9)
 - ※以後、「Gléas」と記載します
- [SaaS] G Suite Business
 - ※以後、「G Suite」と記載します
- [クライアント] Windows 10 / Internet Explorer (11.316)
 - ※以後、「Windows」と記載します
- [クライアント] iOS 12.1.4 / Safari (12.0.3)
 - ※以後、「iOS」と記載します
- [クライアント] macOS Mojave (10.14.3) / 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
2. 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。



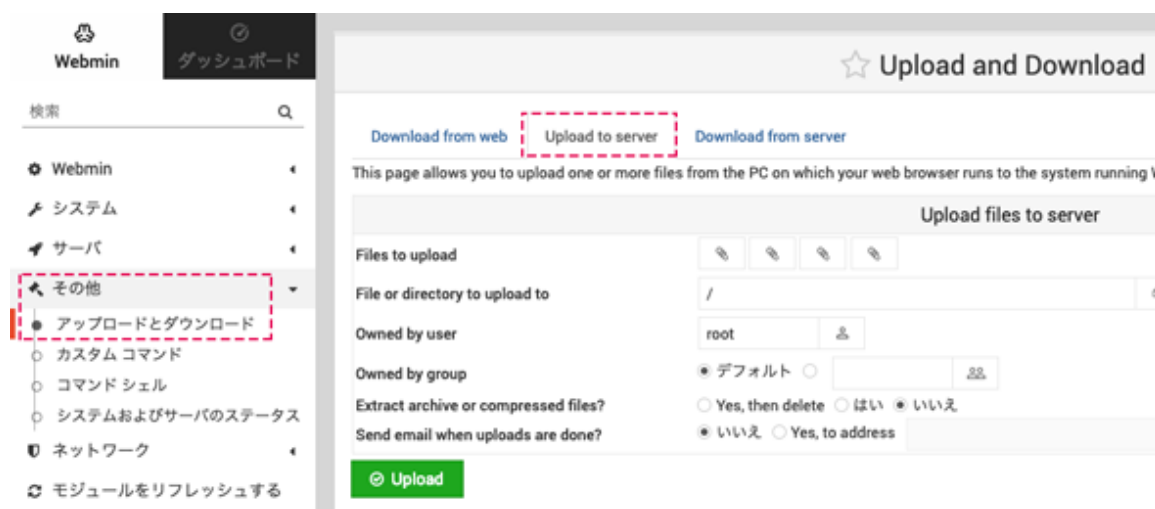
OpenSSLを使ってサーバ証明書から秘密鍵を取り出し、以下のファイル名を付けます。

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

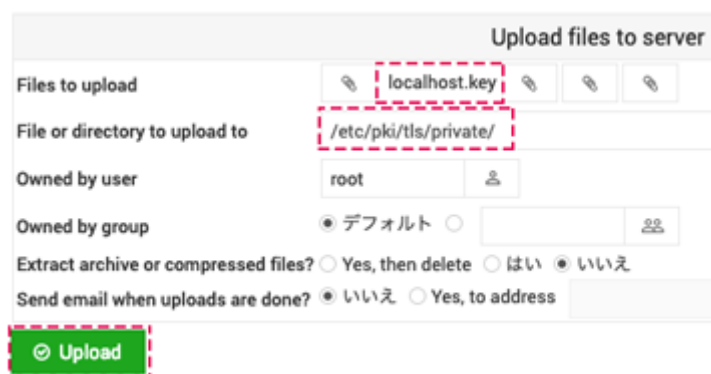
※参考

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

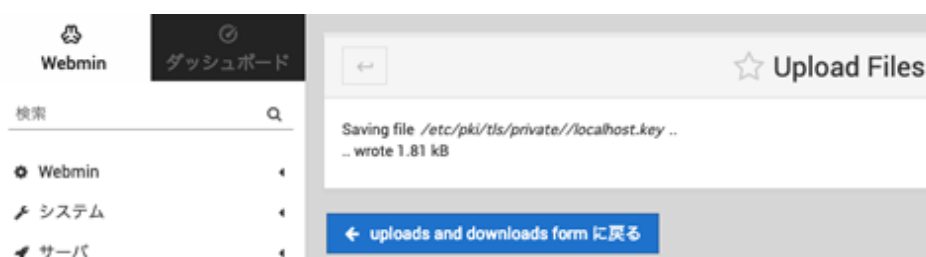
Webminで、[その他]→[アップロードとダウンロード]→[Upload to server]と進みます。



[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。

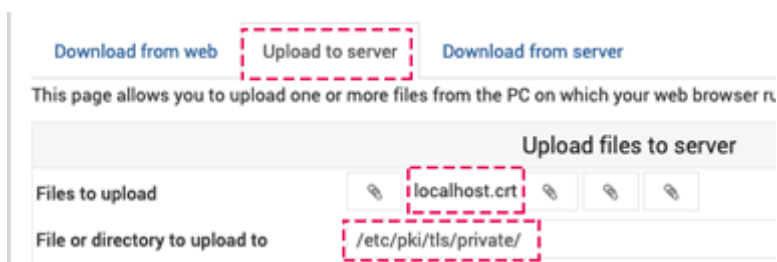


以下の画面が表示されます。[uploads and downloads from に戻る]をクリックします



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

[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。



[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。



[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。



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 zzzzzz
```

※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`

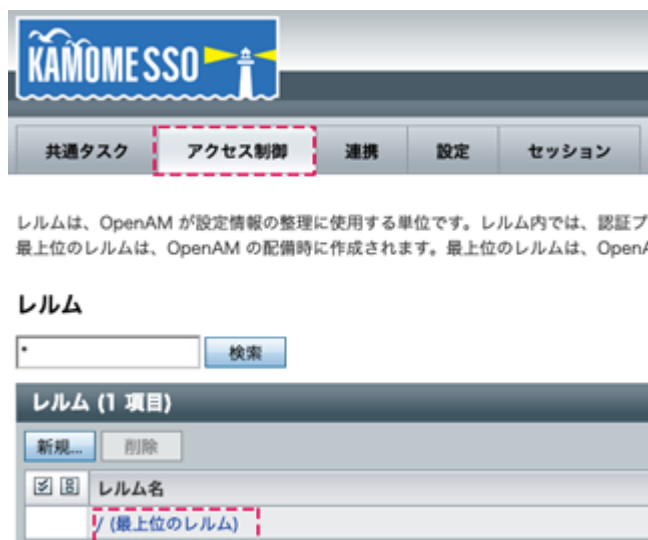
証明書エイリアス 署名用証明書のサブジェクト名

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。

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



[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



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:
- * タイプ:
- Active Directory
 - Device Print
 - HOTP
 - HTTP 基本
 - JDBC
 - LDAP
 - 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。



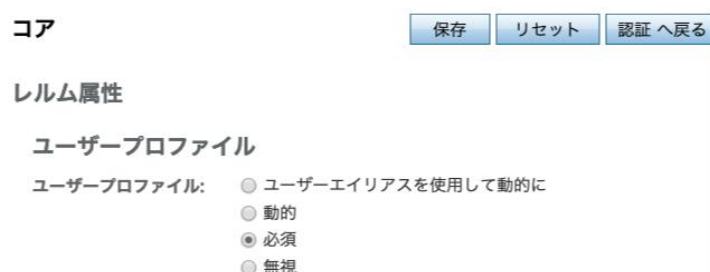
任意の[名前]を入力して、[了解]をクリックします。インスタンスの[追加]をクリックし、[インスタンス]に作成したモジュール名を選択し、[条件]に[必要]を選択して、[保存]をクリックします。



[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。



[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。



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:

署名鍵: ⓘ

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

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

検証証明書

検証証明書:

```
-----BEGIN CERTIFICATE-----
MIID0jCCArqgAwIBAgICLYYwDQYJKoZIhvcNAQELBQAwSjEZMBCGA1UEAxMQSkNDSC1TU1MgZGVt
byBDQTEtMBEGCgMjSjE4MzYwMDYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYy
MDIyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYy
LGMjSjE4MzYwMDYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYyMjYy
DwAwggEKAoIBAQD2Sqc9WPzH/+s3Tg/7CEY4EUbqmZS32fjUq2RPa8EKowxfCw0EnpqrRSO9d+
+pF0zXY8+HIWbjRwjaVYt3/k1a26jFi1+yukgwFvIXVTBZrCnEQy13H8vvg95nZ1AluAv0c0Jly3
MWy7isOelAewEGz8ITGj6TJYgVqjHRFoRnt7Ki9wE+3GZg0lp+ZPNxck/hMeybvxa0y0Y7a6qCQF
LobFeX7mnERp8N+kFqr8jV3mQgwmOPwZvlveSZUyfZzZ7OuNEJWb3ONaSe+czP2Fpx3hx8kein
/iJX2d5xpVh7cGmdZ68rrV3VKgqNFYv6vxZHD0SrFNF6mj/Rf67dAgMBAAQgJscswgCgwCQYDVR0T
BALwADAAdBgNVHQ4EFgQU3cRNTBwUNghaTGgPPLL+Bf3QM58wegYDVR0jBHMwCwYAU6kq9SbJKI7aJ
jdbwB8LMdEpDp9KhTqRMMEoxGTAXBgNVBAMTEEpDQ0gtU1NTIGRlW8gQ0ExEzARBgoJkiaJk/ls
ZAEZFgNDT00xGDAWBgoJkiaJk/lsZAEZFgkQ0NlLVNTU4lUAMrWseop2GkOMBMGAlUdJQMMMAoG
CCsGAQUFBwMCAAsGA1UdDwQEAwIFoDANBgkqhkiG9w0BAQsFAAOCAQEASpDqRcypybo9Oz1FNhpU8

```

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。

サードパーティの ID プロバイダで SSO を設定する

サードパーティを ID プロバイダとして設定するには、次の情報を入力してください。

ログイン ページの URL `//kamome.jcch-sss.local:10443/openam/SSORedirect/metaAlias/idp`
システムと G Suite へのログイン用 URL

ログアウト ページ URL `snam/UI/Logout?goto=https://kamome.jcch-sss.local:10443/openam`
ユーザーがログアウトするときにリダイレクトする URL

パスワード変更 URL `https://kamome.jcch-sss.local:10443/openam/idm/EndUser`
ユーザーがシステムでパスワードを変更する際にアクセスする URL です。定義すると、この URL はシングルサインオンが有効になっていない場合でも表示されます

認証の確認

ファイルを選択 ファイルが選択されていません アップロード

認証ファイルには、ログインリクエストを認証するための Google 公開キーが含まれている必要があります。

破棄 保存

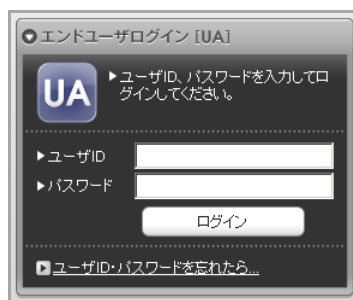
[ドメイン固有の発行元を使用]にチェックを入れて[保存]をクリックします。

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。

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



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

#	発行局	シリアル	有効期限	証明書ストアへインポート
1	JCCH-SSS demo CA	#11472	2030/01/06	証明書のインポート

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

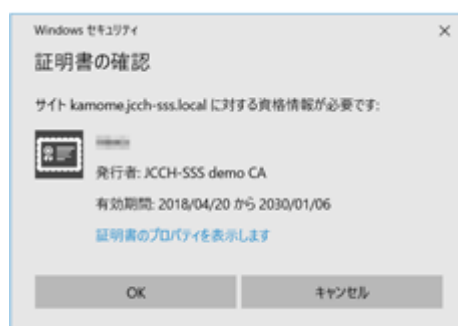
4.2 G Suite へのシングルサインオン

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のユーザー一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>