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

Amazon WorkSpacesでのクライアント証明書認証

Ver. 1.0
2021 年 8 月

目次

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で発行したクライアント証明書を用いて、Amazon AWSのクラウドデスクトップサービスであるAmazon WorkSpacesのログイン認証をおこな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

本書は、以下の環境で検証をおこなっております。

- クラウドデスクトップサービス：Amazon WorkSpaces

※以後、「WorkSpaces」と記載します

- 認証局：JS3 プライベート認証局Gléas（バージョン2.2.8）

※以後、「Gléas」と記載します

- クライアント：Windows 10 Pro （バージョン20H2）
  / WorkSpacesクライアント（バージョン 4.0.1.2262）

※以後、「Windows」と記載します

- クライアント：macOS 11.5.2 / Gléas CertImporter (バージョン 1.3.1)
  / WorkSpacesクライアント（バージョン 4.0.1.2036）

※以後、「Mac」と記載します

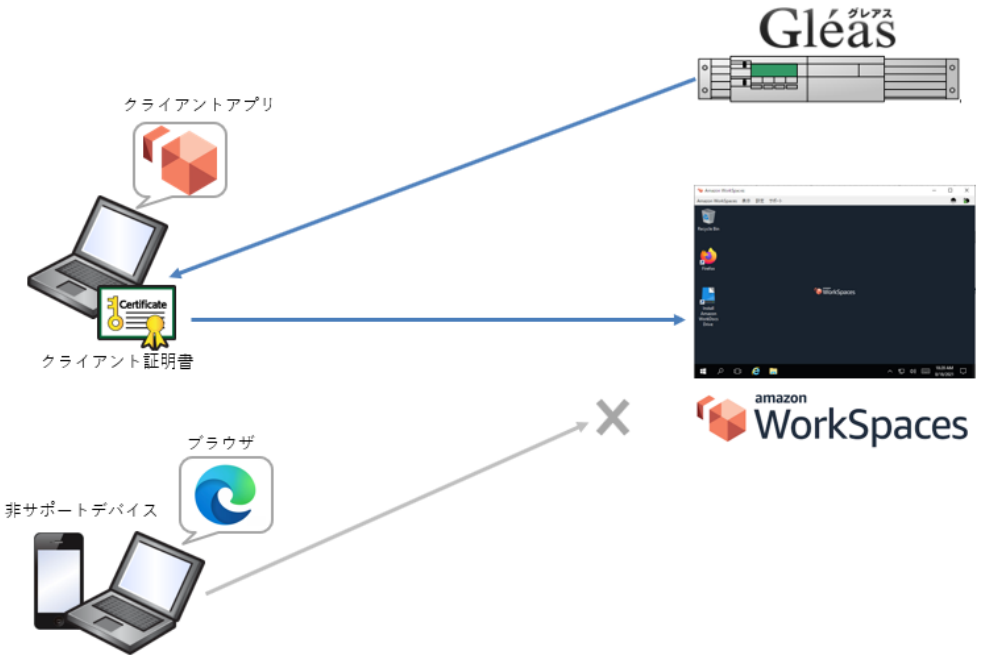
以下については、本書では説明を割愛します。

- WorkSpacesでのワークスペース（仮想デスクトップ）やディレクトリ作成などの基本操作
- WorkSpacesクライアントのインストールなど利用者側の操作
- Gléasの基本的な操作

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. 本書における環境

本書では、以下の構成で検証を行っています。



1. WorkSpacesアプリをインストールしたWindowsおよびMacに対して、Gléasはクライアント証明書を発行し、デバイスに配布する。
2. WindowsおよびMacはWorkSpacesクライアントアプリを使ってAmazon WorkSpacesにアクセスし、仮想デスクトップを利用する。
3. 2以外の環境（他のデバイスや、証明書がインポートされたWindowsやMacであってもブラウザからのアクセス）は認証を拒否する。

1.4. 本書記載時における留意事項

本ドキュメント作成時点において、WorkSpacesでは証明書の失効確認はサポートされておりません。

参考URL: https://docs.aws.amazon.com/workspaces/latest/adminguide/trusted-devices.html

2. WorkSpaces への信頼する認証局の設定

2.1. ルート証明書のダウンロード

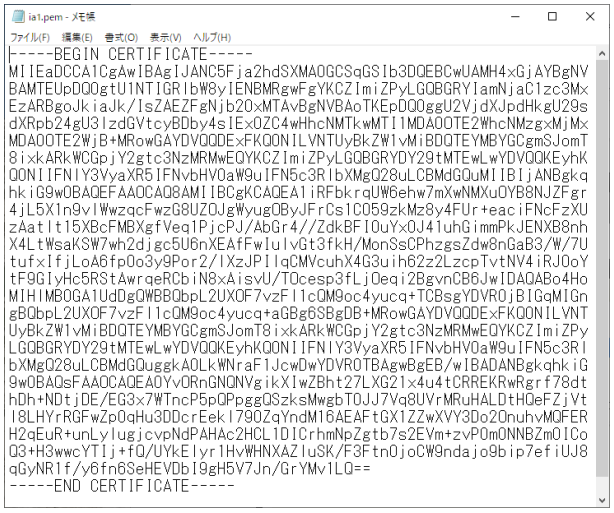
Gléas の RA にログインし、画面上部の[認証局]リンクをクリックします。

該当する IA（発行局）のリンクをクリックすると、ルート証明書のダウンロードが可能なので、「PEM 形式」のものをダウンロードしておきます。

2.2. WorkSpacesでの設定

WorkSpaces 管理コンソールに移動して左側ペインの[ディレクトリ]をクリックし、対象のディレクトリを選択し[アクション] > [詳細の更新]をクリックします。
[アクセス制御のオプション]を展開し、以下の設定をおこないます。

- Windows と Mac（macOS）は、[信頼されたデバイスのみ]を選択
- Android/ChromeOS は、[すべてブロック]を選択
- ルート証明書 1 の[インポート]ボタンをクリックし、2.1 項でダウンロードしたルート証明書をアップロードします。
  テキストデータでのアップロードが必要なので、2.1 項でダウンロードしたファイルをテキストエディタで開き、それをコピー＆ペーストして[インポート]ボタンをクリックします。



テキストをコピー

テキストボックスにペースト

- その他のプラットフォームは、[ブロック]を選択

以下の表示がされたら、[更新と終了]をクリックして保存します。

3. Gléas UAの管理者設定（Windows用）

GléasのUA（申込局）より発行済み証明書をWindowsクライアントにインポートできるよう設定します。

※ 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、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

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
- 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

設定終了後、[保存]をクリックし設定を保存します。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/Windows Phone の設定の、[Android / Windows Phone 用 UA を利用する]
- 証明書インポートアプリ連携の設定の、[証明書インポートアプリを利用する]

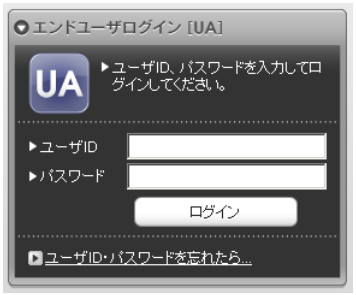
以上でGléasの設定は終了です。

4. クライアントからのアクセス（Windows）

4.1. クライアント証明書のインポート

IEモードが設定されたEdge、あるいはInternet Explorer（IE）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、Gléasでのユーザ IDとパスワードを入力しログインします。

※　UAのログイン認証をActive Directoryで行うことも可能です。詳細は最終項のお問い合わせ先までご連絡ください

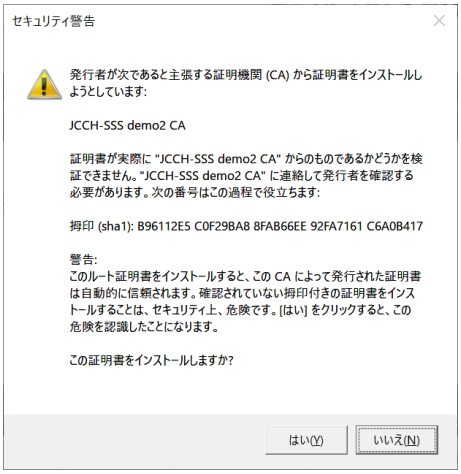


ログインすると、ユーザ専用ページが表示されます。
[証明書のインポート]ボタンをクリックすると、クライアント証明書のインポートが行われます。

※　初回ログイン時にはActiveXコントロールのインストールを求められるので、画面の指示に従いインストールを完了します

※　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

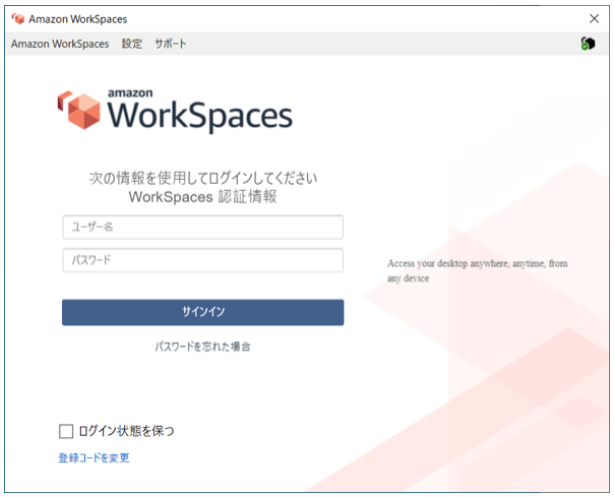
を確認するなど正当性を確認してから[はい]をクリックします

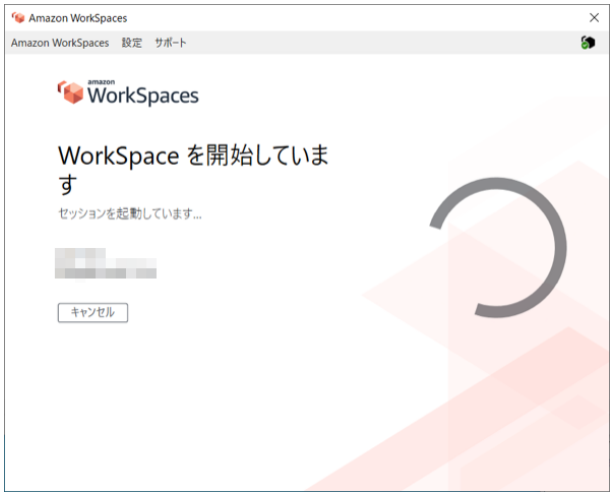


インポートワンスを有効にしている場合は、インポート完了後に強制的にログアウトさせられます。再ログインしても[証明書のインポート]ボタンは表示されず、再度ログインしてインポートをおこなうことはできません。

4.2. クラウドデスクトップへの接続

証明書インポート後に、WorkSpacesクライアントを起動し接続が正常におこなえることを確認します。

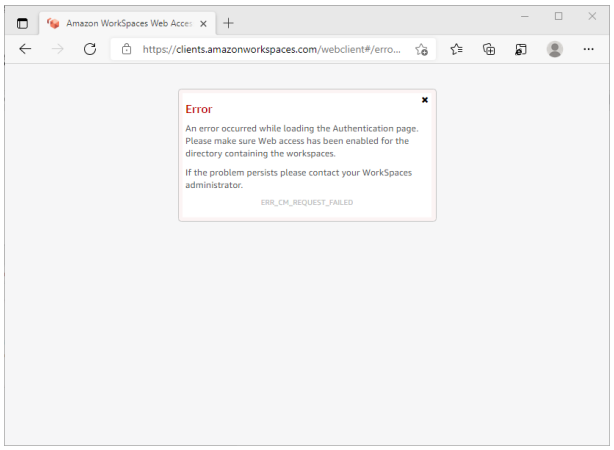




なお、クライアント証明書がない状態でアクセスすると以下のエラーが表示されます。

クライアント証明書がインポートされている状態でも、ブラウザからアクセスした場合

は接続を拒否されます（Macでも同様になります）。



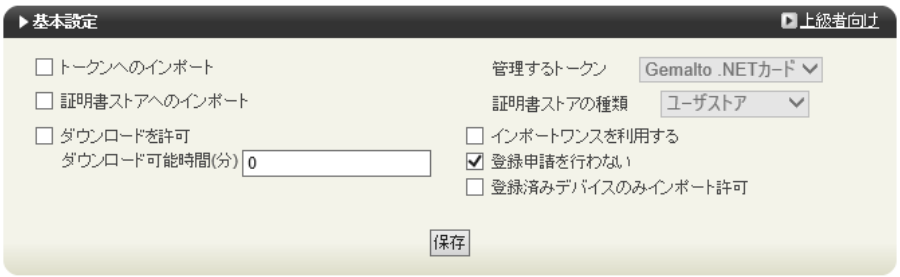
5. Gléas UAの管理者設定（Mac用）

GléasのUA（申込局）より発行済み証明書をMacにインポートできるよう設定します。
※下記設定は、Gléas納品時などに弊社で設定を既に行っている場合があります

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、設定を行うUA（申込局）をクリックします。

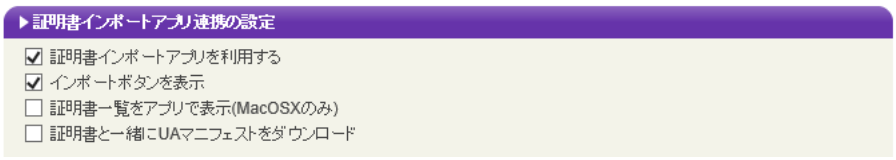
[申込局詳細]画面が開くので、[基本設定]部分で以下の設定を行います。

- [登録申請を行わない]以外のチェックをすべて外す
- 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



設定終了後、[保存]をクリックし設定を保存します。
同じ画面下部の[証明書インポートアプリ連携の設定]で以下を設定します。

- [証明書インポートアプリを利用する]にチェック
- [インポートボタンを表示]にチェック



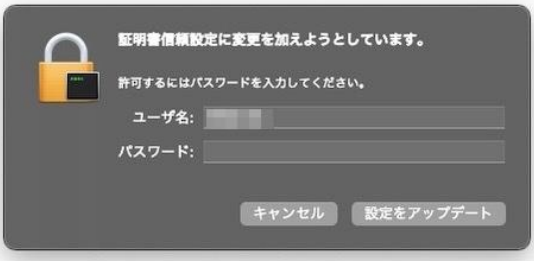
設定終了後、下部の[保存]をクリックし設定を保存します。

6. クライアントからのアクセス（Mac）

6.1. クライアント証明書のインポート

事前にGléas CertImporterをインストールして、SafariでGléasのUAにアクセスします。ログイン画面が表示されるので、GléasでのユーザIDとパスワードを入力しログインすると、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、Gléas CertImporterが呼び出され、クライアント証明書のインポートが行われます。



インポートワンスついてもWindowsとほぼ同様になり、一度インポートした証明書を再度ログインしてインポートすることはできません。

6.2. クラウドデスクトップへの接続

証明書インポート後に、WorkSpacesクライアントを起動し接続が正常におこなえることを確認します。

なお、クライアント証明書がない状態でアクセスすると以下のエラーが表示されます。

7. 問い合わせ

■Gléasに関するお問い合わせ先

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