SECUREMATRIX

DocuSign との認証連携

- SECUREMATRIX およびマトリクス認証は、株式会社シー・エス・イーの登録商標です。
- その他、記載されている会社名、商品名、ロゴは、各社の商標または登録商標です。
- 記載事項（仕様・デザインなどを含む）は、お断りなく変更することがありますので、あらかじめご了承ください。

ドキュメント改版履歴

版　数	発行年月日	検証年月日	改版内容
第 1 版	2022/7/21	2022/7/5	初版

1. 免責

本書は、弊社で検証した SECUREMATRIX と DocuSign(DocuSign, Inc.)の認証連携に関する実績を記載したドキュメントで、2022 年 7 月 5 日時点の情報です。対象のサービスとの連携やサービス動作を保証するものではありません。

2. 環境

2.1. バージョン

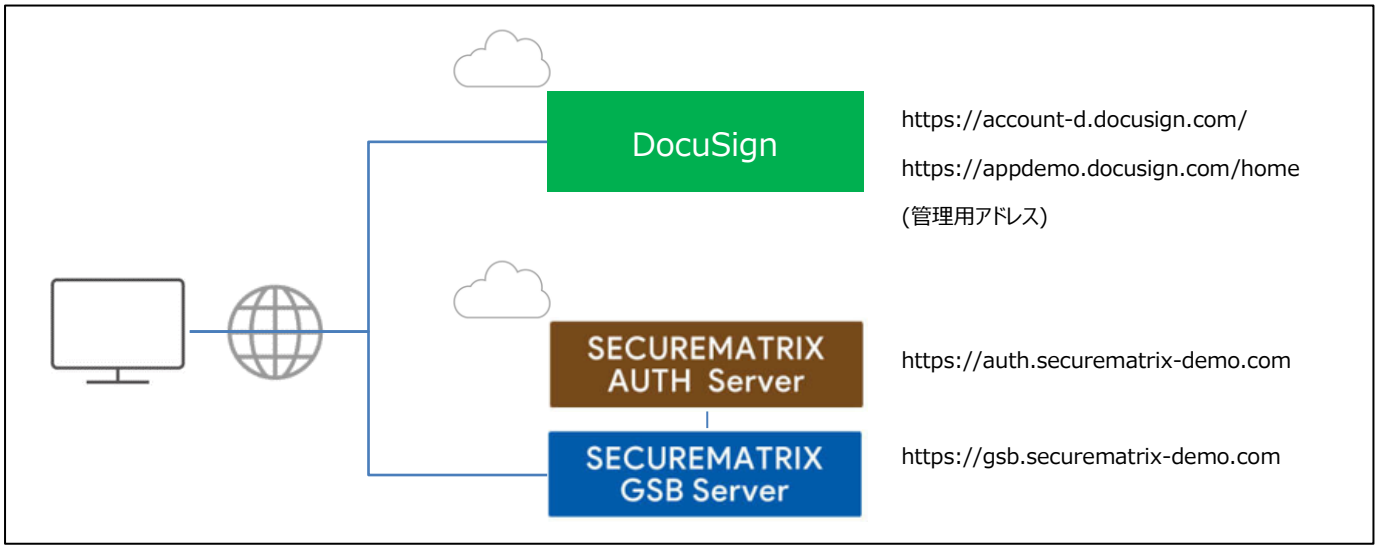
・SECUREMATRIX V12.2
・DocuSign (2022 年 7 月 5 日検証)、DocuSign トライアルライセンス

・Firefox (102.0.1)
・Chrome (103.0.5060.114)
・Microsoft Edge (103.0.1264.49)
・Safari (604.1)

2.2. 連携方式

・SAML2.0

2.3. 構成図



3. 設定

3.1.SECUREMATRIX

SECUREMATRIX 管理コンソールから以下の設定を行います。

1. 管理トップページ画面で、「SAML2.0 認証」→「IdP 署名鍵設定」→発行者に任意の値を登録し「登録」 →「証明書ダウンロード」 →「X509Key.pem」ファイルをダウンロード。
2. 管理トップページ画面で、「SAML2.0 認証」→「クラウドサービス新規登録」→クラウドサービス連携情報新規登録画面を表示し、クラウドサービス連携情報新規登録画面で、以下の設定項目を入力。

NO	設定項目	設定値	備考
1	クラウドサービス名称	DocuSign	ー
2	アクセスパス	/DocuSign/	DocuSign の「ID プロバイダーのログイン URL」と一致させる。
3	メタデータ	ー	ー
4	アサーション有効時間	60 分	ー
5	NameID マッピング値	メールアドレス	本環境では「備考欄 1」で設定。DocuSign で申請したドメインのメールアドレスが必要。
6	NameID 書式	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent	SamlRequest の「NameIDPolicy Format」
7	エンティティ ID	Securematrix	DocuSign の「ID プロバイダーの発行者」と一致させる。
8	SP シングルサインオン URL	https://account-d.docusign.com/organizations/de57ae56-7feb-49ed-a513-ffe1a65e7b67/saml2/login/2f1e46ac-1e37-4369-8124-de8ae0789447	DocuSign の SAML2.0 エンドポイント「サービスプロバイダーのアサーションコンシューマーサービスの URL」を設定。（AssertionConsumerServiceURL）
9	シングルサインオン Binding	Post	ー
10	有効/無効 チェック	チェック OFF（有効にする）	ー

3. 管理トップページ画面で、「SAML2.0 認証」→「クラウドサービス一覧」→「DocuSign」の「アトリビュート設定」→「アトリビュート新規設定」→以下 3 件のアトリビュートを設定。

No	設定項目	設定値 1	設定値 2	設定値 3
1	クラウドサービス名称	DocuSign	DocuSign	DocuSign
2	アトリビュート名	emailaddress	surname	givenname
3	アトリビュート	emailaddress	surname	givenname
4	アトリビュート書式	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	urn:oasis:names:tc:SAML:2.0:attrname-format:basic	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
5	マッピング値	備考欄 1	備考欄 2	備考欄 3
6	固定値	ー	ー	ー
7	有効/無効	チェック OFF（有効にする）	チェック OFF（有効にする）	チェック OFF（有効にする）
※備考（コメント）		マッピング値は本来メールアドレス 本環境ではメールアドレスが DocuSign で登録したものと異なるため備考欄 1 にて設定。	DocuSign で登録してある LastName を設定。	DocuSign で登録してある FirstName を設定。

4. 管理トップページ画面で、「ユーザー管理」→「ユーザー新規登録」→ユーザー情報新規登録画面で以下の設定項目を入力し登録。

NO	設定項目	設定値	備考
1	UserID	test	左記は参考。任意の UserID を登録。
2	メールアドレス	test@securematrix-demo.com	DocuSign で登録しているメールアドレスを登録。
3	登録年月日	登録日	ー
4	GSB アクセスレベル	任意のアクセスレベル	ー
5	ユーザーグループ	任意のユーザーグループ	ー
6	認証方式	任意の認証方式	ー
7	備考欄 1	test@securematrix-demo.com	メールアドレスが DocuSign で登録してメールアドレスであれば不要。
8	備考欄 2	Yamada	DocuSign で登録している LastName を登録。
9	備考欄 3	Tarou	DocuSign で登録している FirstName を登録。

3.2. DocuSign

DocuSign では下記を設定します。

1. ドメイン申請

〈参考サイト〉

https://support.docusign.com/s/document-item?language=ja&bundleId=rrf1583359212854&topicId=bzr1583359141662.html&_LANG=jajp

DocuSign 管理者でログインし、DocuSign Admin ダッシュボードの［ドメイン］ページで、ドメインの予約プロセスを開始します。これにより生成されるトークンを、対象ドメインの DNS（Domain Name System）に追加します。DNS 内のトークンが DocuSign により検証されると、そのドメインが組織に登録されます。

本環境では以下操作を行いました。

1-1. ［ドメイン]ページで「ドメインの申請」を押下し「securematrix-demo.com」を申請。

1-2. 登録したドメインの「アクション」→「トークンを取得」を押下し「テキストトークン」を取得（コピー)。

1-3. 「securematrix-demo.com」ドメインの DNS サーバーに取得したテキストトークンを TXT レコードとして登録。本環境では以下のテキストトークンを登録。
docusign=19dfdabf-cd56-4722-810a-65eae489665f

1-4. ［ドメイン]ページで「securematrix-demo.com」ドメインの「アクション」→「検証」を押下しステータスが「保留中」から「アクティブ」になることを確認。

2. ID プロバイダーのセットアップ

〈参考サイト〉

https://support.docusign.com/s/document-item?language=ja&bundleId=rrf1583359212854&topicId=vhh1583359145046.html&_LANG=jajp

DocuSign Admin のダッシュボードで、[ID プロバイダー] を選択し「ID プロバイダーの追加」を押下し以下の設定を実施。

No	設定項目	設定値	備考
1	カスタム名		
1-1	カスタム名	SECUREMATRIX	任意の名前、本環境では左記で設定
2	ID プロバイダーの設定		
2-1	ID プロバイダーの発行者	Securematrix	SECUREMATRIX の「エンティティ ID」
2-2	ID プロバイダーのログイン URL	https://gsb.securematrix-demo.com/smx_cloud/DocuSign	SECUREMATRIX の「アクセスパス」
2-3	ID プロバイダーのメタデータ URL	ー	ー
2-4	カスタム属性	属性:emailaddress、カスタムの属性名:emailaddress	SECUREMATRIX の「アトリビュート：emailaddress」

2-5		属性：surname、カスタムの属性名：surname	SECUREMATRIX の「アトリビュート：surname」
2-6		属性：givenname、カスタムの属性名：givenname	SECUREMATRIX の「アトリビュート：givenname」
3	シングルサインオン（SSO）設定の編集		
3-1	サードパーティログイン	チェック ON（有効）	ー
3-2	シングルログアウト（SLO）	チェック OFF（無効）	ー
	HTTP 要求		
3-3	認証要求に署名する	チェック OFF（無効）	ー
3-4	ログアウト要求に署名する	チェック OFF（無効）	ー
3-5	認証要求の送信:	POST	SECUREMATRIX の「シングルサインオン Binding」
3-6	ログアウト要求の送信:	POST	ー

ID プロバイダーが登録されると以下のエンドポイントが発行されるので、必要な値を SECUREMATRIX へ登録する。エンドポイントの値は ID プロバイダー毎に発行されます、以下は本環境の値となります。

No	URL	値	設定
1	サービスプロバイダーの発行元 URL	https://account-d.docusign.com/organizations/de57ae56-7feb-49ed-a513-ffe1a65e7b67/saml2	IdP initiated 時に spEntityID に使用。
2	サービスプロバイダーのログイン URL	https://account-d.docusign.com/organizations/de57ae56-7feb-49ed-a513-ffe1a65e7b67/saml2/login/sp/2f1e46ac-1e37-4369-8124-de8ae0789447	SECUREMATRIX では使用しない。
3	サービスプロバイダーのアサーションコンシューマーサービスの URL	https://account-d.docusign.com/organizations/de57ae56-7feb-49ed-a513-ffe1a65e7b67/saml2/login/2f1e46ac-1e37-4369-8124-de8ae0789447	SECUREMATRIX の「SP シングルサインオン URL」に設定。
4	サービスプロバイダーのメタデータ URL	https://account-d.docusign.com/organizations/de57ae56-7feb-49ed-a513-ffe1a65e7b67/saml2/metadata/2f1e46ac-1e37-4369-8124-de8ae0789447	SECUREMATRIX では使用しない。

3. 証明書の登録

SECUREMATRIX でダウンロードした「X509Key.pem」ファイルを DocuSign で登録した ID プロバイダーに登録します。

3-1. DocuSign Admin のダッシュボードで、[ID プロバイダー] を選択し登録した ID プロバイダーの「アクション」→「設定の管理」を押下。

3-2. 「証明書」タブを選択し「証明書の追加」を押下し「X509Key.pem」ファイルを選択。

4. ID プロバイダー用のユーザーアカウント作成

登録したドメインのユーザーアカウントを作成します。

4-1. DocuSign Admin のダッシュボードで、[ユーザー] を選択し「ユーザーの追加」を押下。

4-2. 以下の内容でユーザーを登録。

NO	設定項目	設定値	備考
1	氏名	Yamada Tarou	SECUREMATRIX の「LastName FirstName」
2	メールアドレス	test@securematrix-demo.com	登録したドメインのメールアドレス かつ受信可能であること（2 段階認証のため）
3	会社名	CSE	任意の値
4	役職	なし	任意の値
5	言語	日本語	任意の値
6	住所と電話番号	なし	任意の値

3.3. 設定値紐づけ参考

SP（DocuSign）と IdP（SECUREMATRIX）では SAML 認証するために設定値が一致していることが重要です。参考として、下表にて一致させる設定値の紐づけを示します。

NO	SECUREMATRIX 設定値名	DocuSign 設定値名	本資料での設定値	備考
1	アクセスパス	ID プロバイダーのログイン URL	SMX：/DocuSign/ DocuSign： https://gsb.securematrix-demo.com/smx_cloud/DocuSign	ID プロバイダーのログイン URL のパス部分と一致させる。
2	エンティティ ID	ID プロバイダーの発行者	Securematrix	ー
3	SP シングルサインオン URL	SAML2.0 エンドポイント 「サービスプロバイダーのアサーションコンシューマーサービスの URL」	https://account-d.docusign.com/organizations/de57ae56-7feb-49ed-a513-ffe1a65e7b67/saml2/login/2f1e46ac-1e37-4369-8124-de8ae0789447	ー
4	アトリビュート ・emailaddress ・surname ・givenname	カスタム属性 ・emailaddress ・surname ・givenname	・test@securematrix-demo.com ・Yamada ・Tarou	ー

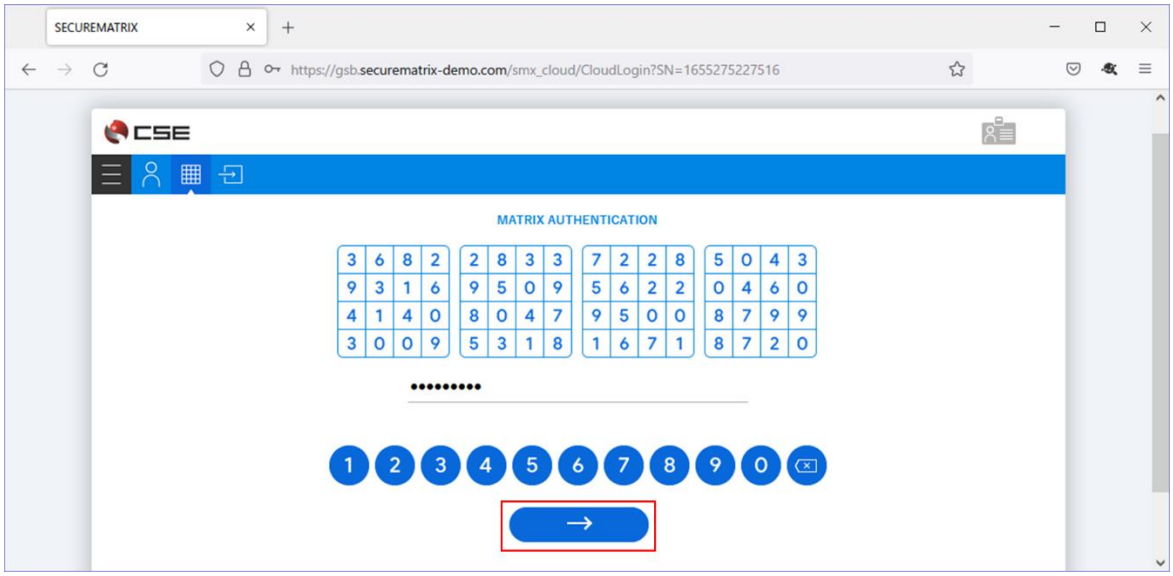
4. 画面遷移

SP Initiated の画面遷移は下記の通りです。IdP Initiated については 5.その他をご覧ください。

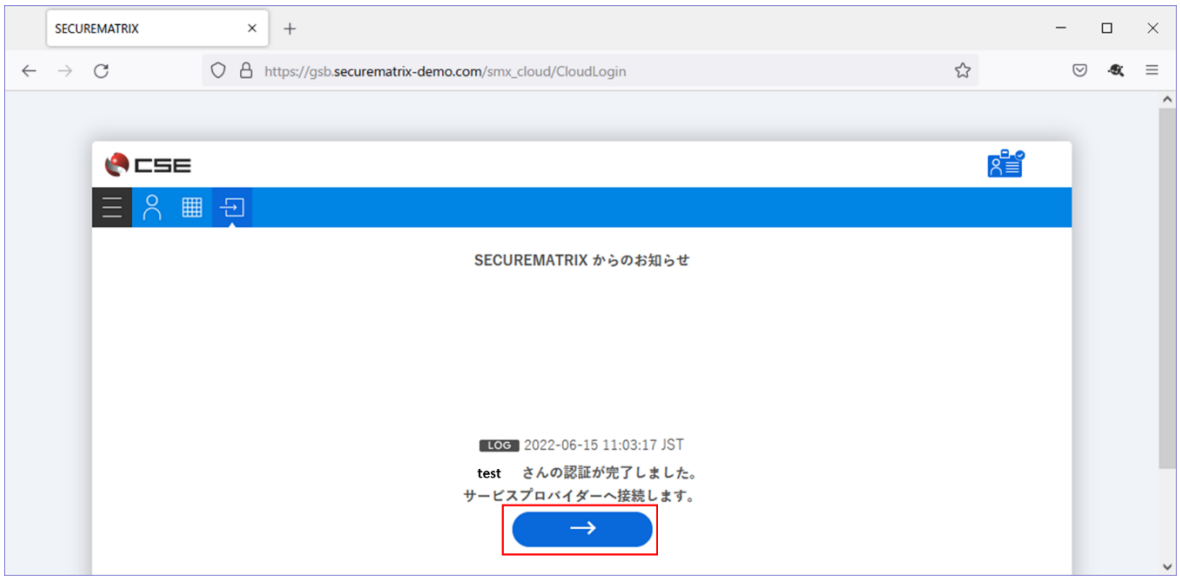
1. ブラウザを起動し以下 URL にアクセス、DocuSign にて登録済みのユーザーアカウントのメールアドレスを入力して「次へ」を押下。
   https://account-d.docusign.com/

2. 「会社の資格情報でログインする」を押下。

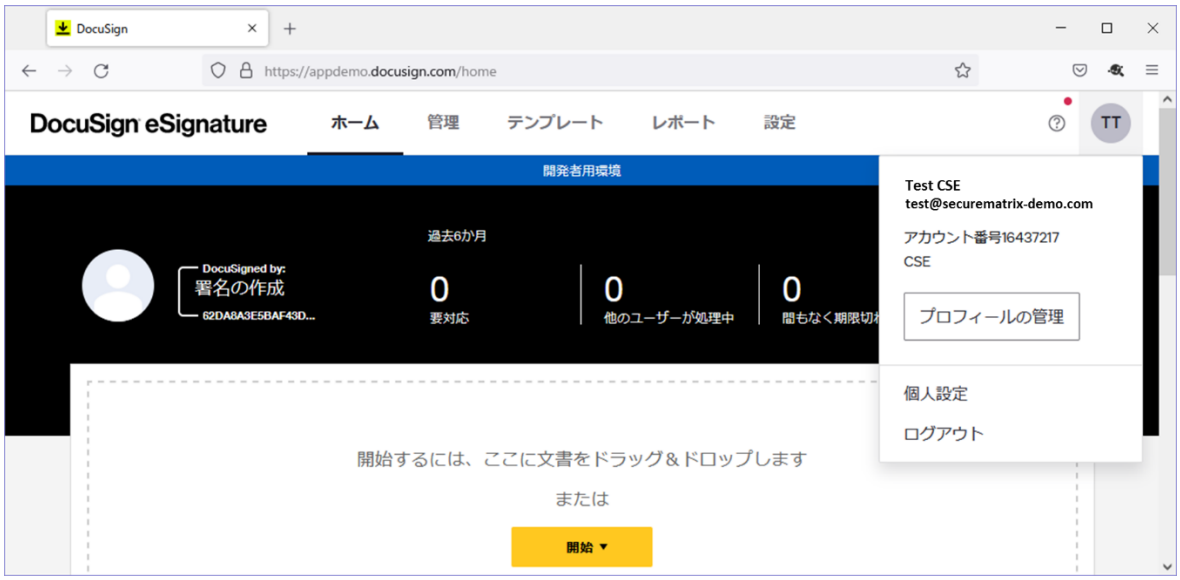
3. パスワードを入力後、「→」を押下。



4. サービスプロバイダー接続画面で「→」を押下。



5. DocuSign にログイン。



5. その他

5.1. IdP initiated

IdP initiated の場合は、以下の URL にてアクセスします。

https://[GSB サーバーURL]/smx_cloud/DocuSign/?spEntityID=[サービスプロバイダーの発行元URL]&RelayState=[ログイン後に遷移させたいサービスの URL]
サービスプロバイダーの発行元 URL は DocuSign の管理コンソールからリンクをコピーします。

例)
https://gsb.securematrix-demo.com/smx_cloud/DocuSign/?spEntityID=https://account-d.docusign.com/organizations/de57ae56-7feb-49ed-a513-ffe1a65e7b67/saml2&RelayState=https://appdemo.docusign.com/home

5.2. クライアントアプリ

3 章の設定が完了していれば DocuSign のモバイルアプリでも認証連携可能です。

- iOS 15.1
- DocuSign モバイル版 (3.9.0)

動作イメージ

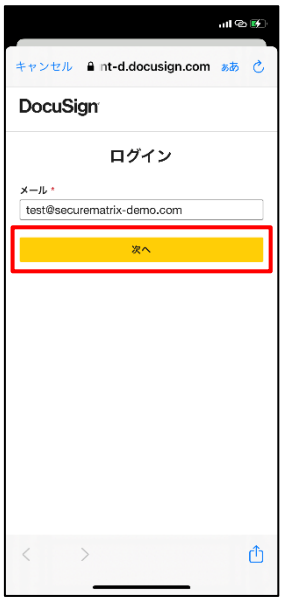
1. ホーム画面からモバイルアプリを起動。
2. 「ログイン」を押下。

3. メールアドレスを入力し「次へ」を押下。
4. 「会社の資格情報でログインする」を押下。
5. パスワードを入力し「→」を押下。
6. サービスプロバイダー接続画面で「→」を押下。
7. DocuSign にログイン。

1.

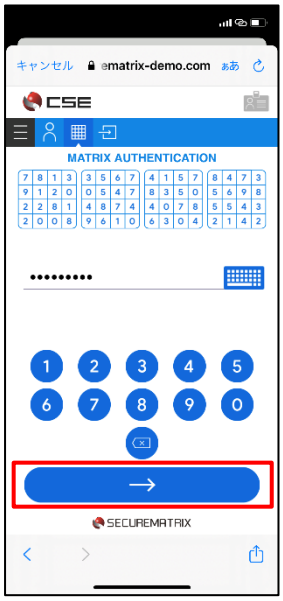
2.

3.

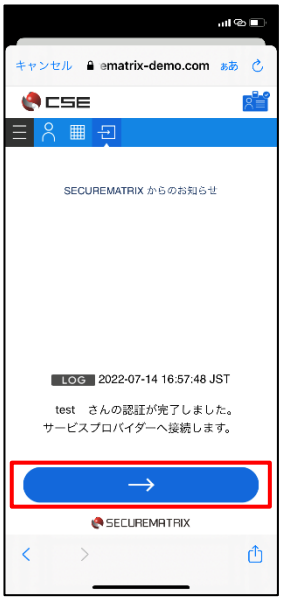


4.

5.



6.



7.

以上