SECUREMATRIX

Kintone との認証連携

CAR12-22136

- 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	2022/7/13	初版

1. 免責

本書は、弊社で検証した SECUREMATRIX と Kintone (Cybozu, 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 13 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

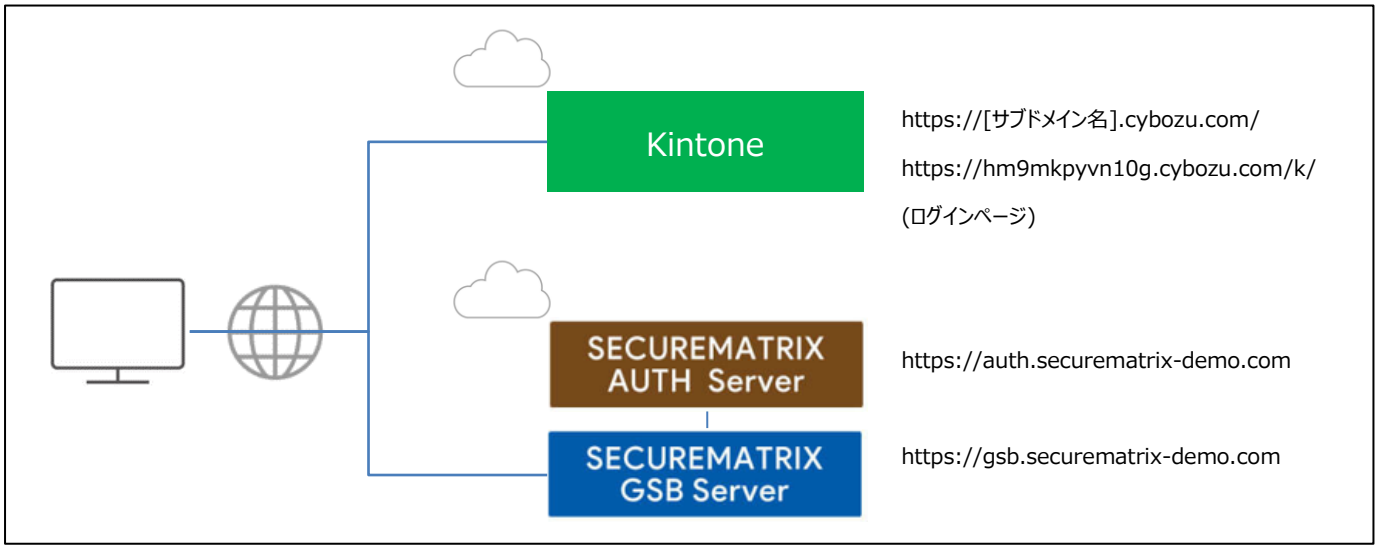
・SECUREMATRIX V12.2
・Kintone (2022 年 7 月 13 日検証)、無料トライアルライセンス

・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	Kintone	ー
2	アクセスパス	/Kintone/	Kintone の「Identity Provider の SSO エンドポイント URL（HTTP-Redirect）」と一致させる。
3	メタデータ	spmetadata.xml	「3.2.Kintone」の「8.Service Provider メタデータのダウンロード」でダウンロードした「spmetadata.xml」ファイルを登録する。
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	Kintone のログイン名と NameID を一致させる、本環境ではメールアドレスをログイン名としていますがメールアドレスが必須ではない。 〈参考サイト〉 https://get.kintone.help/general/ja/admin/list_useradmin/pw_limitations.html
6	NameID 書式	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified	SamlRequest の「NameIDPolicy Format」
7	エンティティ ID	Securematrix	Kintone では設定箇所無し。
8	SP シングルサインオン URL	ー	メタデータに登録されているため設定不要。
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. アトリビュート設定は不要です。

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する。

NO	設定項目	設定値	備考
1	UserID	test	左記は参考です。任意の UserID を登録。
2	メールアドレス	test@securematrix-demo.com	Kintone でログイン名として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	ー	ー
8	備考欄 2	ー	ー
9	備考欄 3	ー	ー

3.2. Kintone

Kintone では下記を設定します。
〈参考サイト〉
https://blog.cybozu.io/entry/4224

1. 管理者アカウントで Kintone にログイン。
2. ［cybozu.com 共通管理］へ遷移。
3. サイドバーの［ログイン］を押下。
4. ［SAML 認証を有効にする］をチェック。
5. ［Identity Provider の SSO エンドポイント URL (HTTP-Redirect)］に以下 URL を設定。
   https://gsb.securematrix-demo.com/smx_cloud/Kintone
6. ［cybozu.com からのログアウト後に遷移する URL］に以下 URL を設定。
   本環境では Kintone ログイン画面を指定していますが IdP へ遷移してしまうのでログアウト画面が望ましい。
   https://hm9mkpyvn10g.cybozu.com/k/
7. ［Identity Provider が署名に使用する公開鍵の証明書］に SECUREMATRIX でダウンロードした「X509Key.pem」ファイルを登録。
8. ［Service Provider メタデータのダウンロード]を押下してメタデータ「spmetadata.xml」をダウンロード。
   ダウンロードしたメタデータはエディタにて以下を追記。
   〈md:SPSSODescriptor

protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
↓
<md:SPSSODescriptor
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
WantAssertionsSigned="true">

9. ［保存］を押下し設定を反映。

10. ID プロバイダー用のユーザーアカウントを作成。
SECUREMATRIX に登録したメールアドレスのユーザーアカウントを作成。

10-1. サイドバーの［組織/ユーザー］を押下。
10-2. ［ユーザーの追加］を押下し SECUREMATRIX に登録したメールアドレスを［ログイン名］としてユーザーを作成。

3.3. 設定値紐づけ参考

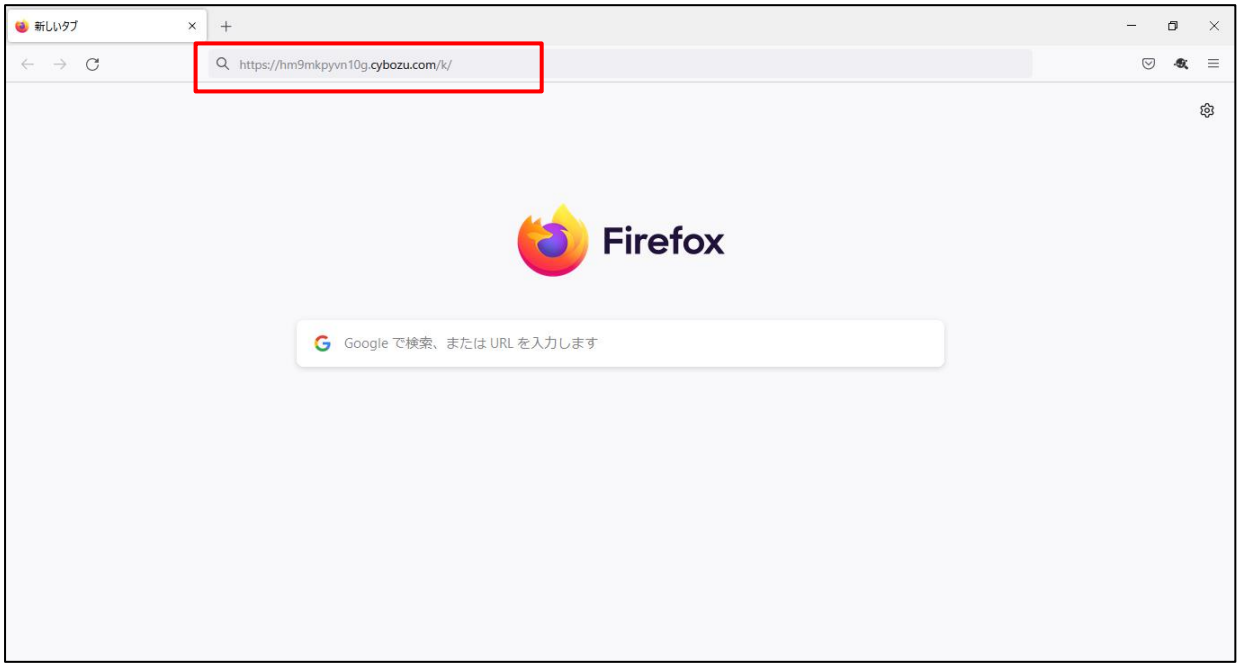
SP（Kintone）と IdP（SECUREMATRIX）では SAML 認証連携するために設定値が一致していることが重要です。参考として、下表にて一致させる設定値の紐づけを示します。

NO	SECUREMATRIX 設定値名	Kintone 設定値名	本資料での設定値	備考
1	アクセスパス	Identity Provider の SSO エンドポイント URL（HTTP-Redirect）	SMX：/Kintone/ Kintone：https://gsb.securematrix-demo.com/smx_cloud/Kintone	Identity Provider の SSO エンドポイント URL のパス部分と一致させる。

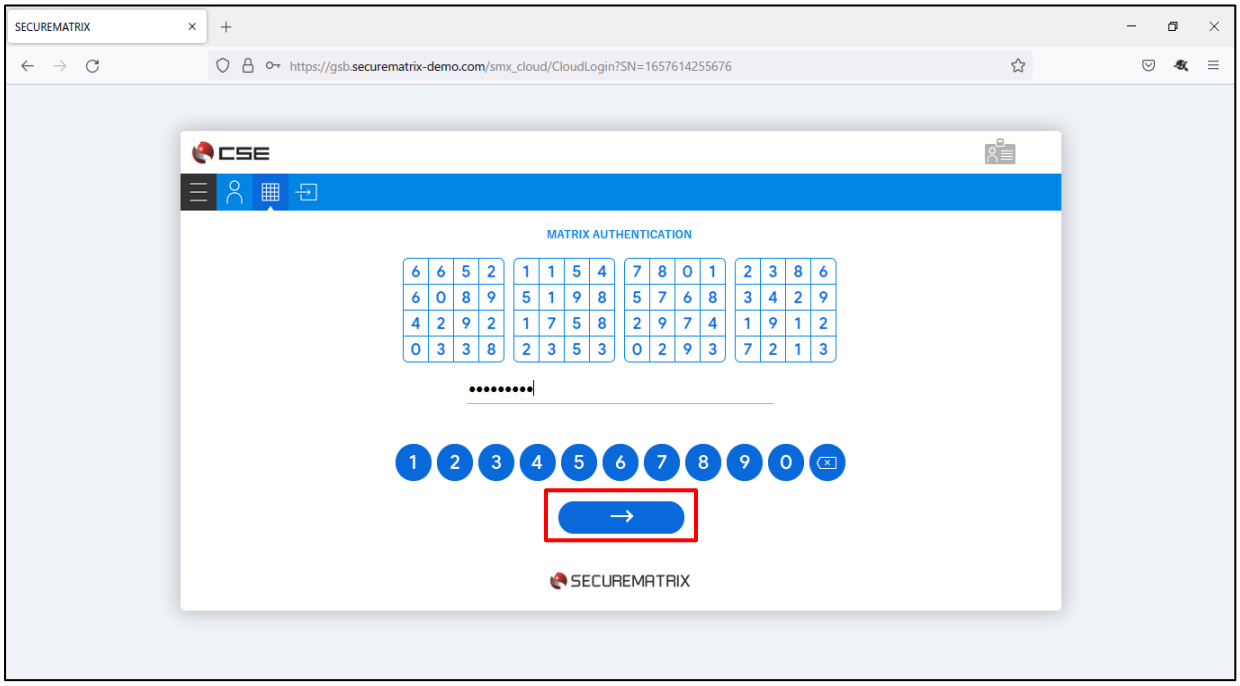
4. 画面遷移

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。

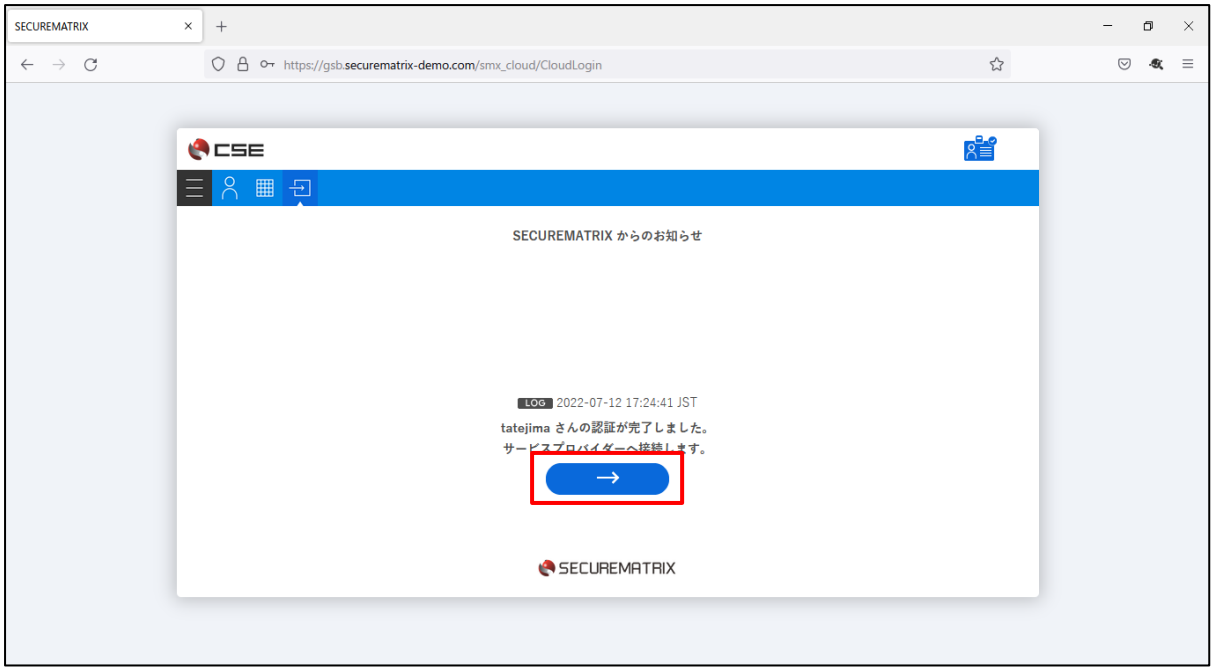
1. ブラウザを起動し以下 URL にアクセス。（サブドメインは契約社毎に異なる）
   https://hm9mkpyvn10g.cybozu.com/k/



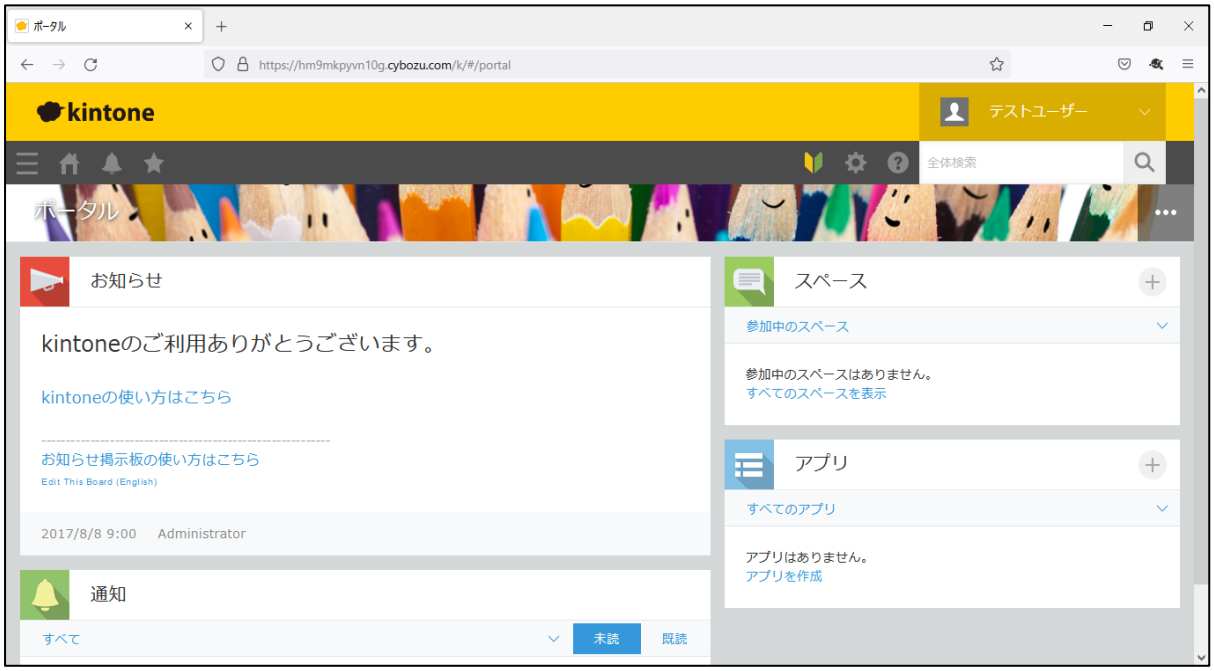
2. パスワードを入力後、「→」を押下。



3. サービスプロバイダー接続画面で「→」を押下。



4. Kintone にログイン。



5. その他

5.1. IdP initiated

Kintone は IdP initiated に対応していません。
〈参考サイト〉
https://jp.cybozu.help/general/ja/admin/list_saml/saml_errors.html

5.2. クライアントアプリ

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

- iOS 15.1
- Kintone モバイル版（2.22）

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. サイボウズから連携されているサブドメインを入力。
3. 「次へ」を押下。
4. 確認メッセージが表示されるので「続ける」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. Kintone にログイン。

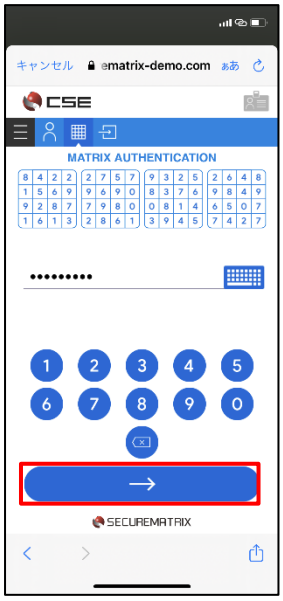
1.

2.

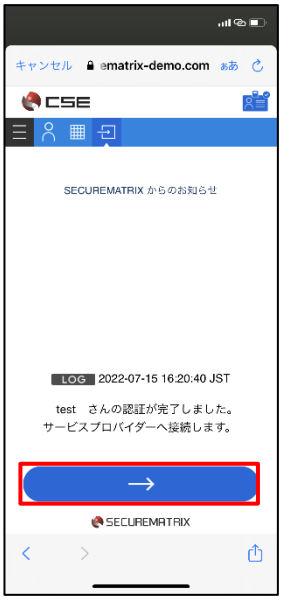
3.

4.

5.



6.



7.

以上