「ThemiStruct(テミストラクト) Identity Platform」クックブック

株式会社 オージス総研
サービス事業本部 テミストラクトソリューション部
杉野 真士

ある日・・・

「明日までに認証基盤用意してね」
by 某ボス

明日までに認証基盤って・・・

社内のいろんな
アプリケーションを
シングルサインオンでき
るようにしないと・・・

認証基盤が停止したら
アプリケーションが使え
なくなるので、構成考え
ないと・・・

今後利用したいアプリケー
ション増えてくるだろうか
ら、追加時の作業が多いと
運用きつくなりそう

月末月初とかのアクセス
が殺到するピークの時に
遅くなったらダメだよね

すぐに社外からも
セキュアにアクセス
したいとかの要望が
でるだろうな

そんな無茶な・・・

そんなとき

某同僚
「すぎのさん、すぎのさん。
最近こんなの作ってみたんだけど
試してみてよ」

ThemiStruct Identity Platform ?

ThemiStruct Identity Platformは

ブラウザからの操作で短時間で構築できる

AWSのサービスを利用した高い可用性を持ち、
大量ユーザアクセスも対応できる認証基盤に仕上がる

クラウドサービスや業務アプリケーションに
フェデレーション/エージェント/リバースプロキシ方式
で接続できる

アプリケーションへの接続は
少ない作業で簡単に接続できる

IPアドレスによる制御やOTPなどの多要素認証などで
認証強化を行うことができる

という認証基盤です。

これ使ったら・・・

社内のいろいろなアプリケーションをシングルサインオンできるようにしないと・・・

社内やクラウドサービスなどのアプリとも接続できそう

認証基盤が停止したらアプリケーションが使えなくなるので、構成考えないと・・・

AWSのサービスを利用して可用性高い構成みたい

今後利用したいアプリケーション増えてくるだろうから、追加時の作業が多いと運用きつくなりそう

アプリ接続作業も難しくなさそう

月末月初とかのアクセスが殺到するピークの時に遅くなったらダメだよね

突発的なスパイクアクセスにも対応できそう

すぐに社外からもセキュアにアクセスしたいとかの要望がでるだろうな

OTPなどを組み合わせた多要素認証でできそう

これなら明日までに
できるかも！

Let's get cooking.

調理の流れ

- 下ごしらえ
- 認証基盤調理
  - マネジメントコンソール作成
  - Identity Platform作成
- 盛り付け
  - アプリケーション接続
  - Office 365 も接続

調理作業時間目安
１０分

第　１　章

下ごしらえ

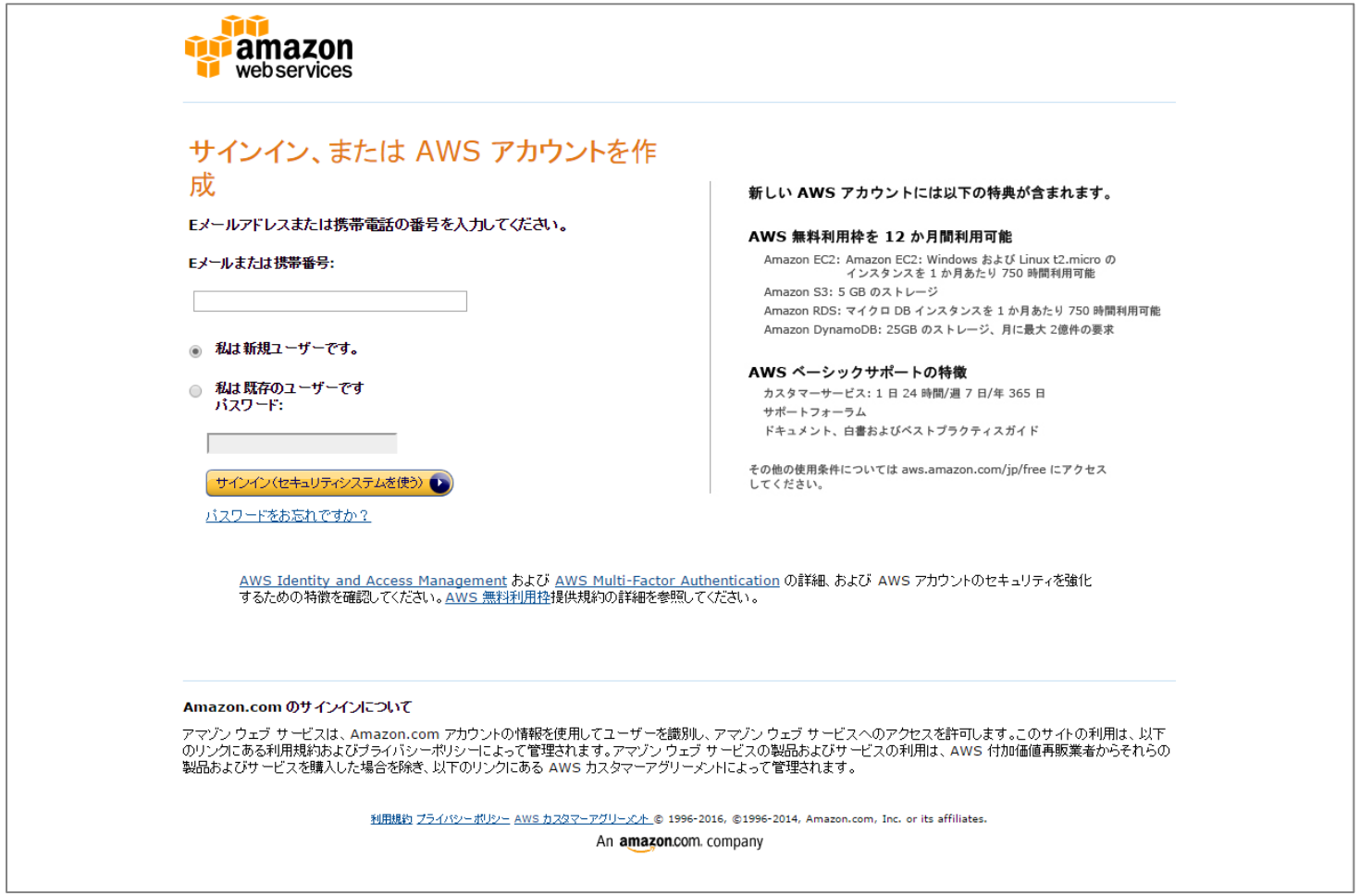
下ごしらえ

- AWSのご契約
- 構築用ユーザの作成
- VPC及びサブネット作成
- 認証基盤用ドメイン登録

etc

AWSのご契約

AWSアカウントの作成



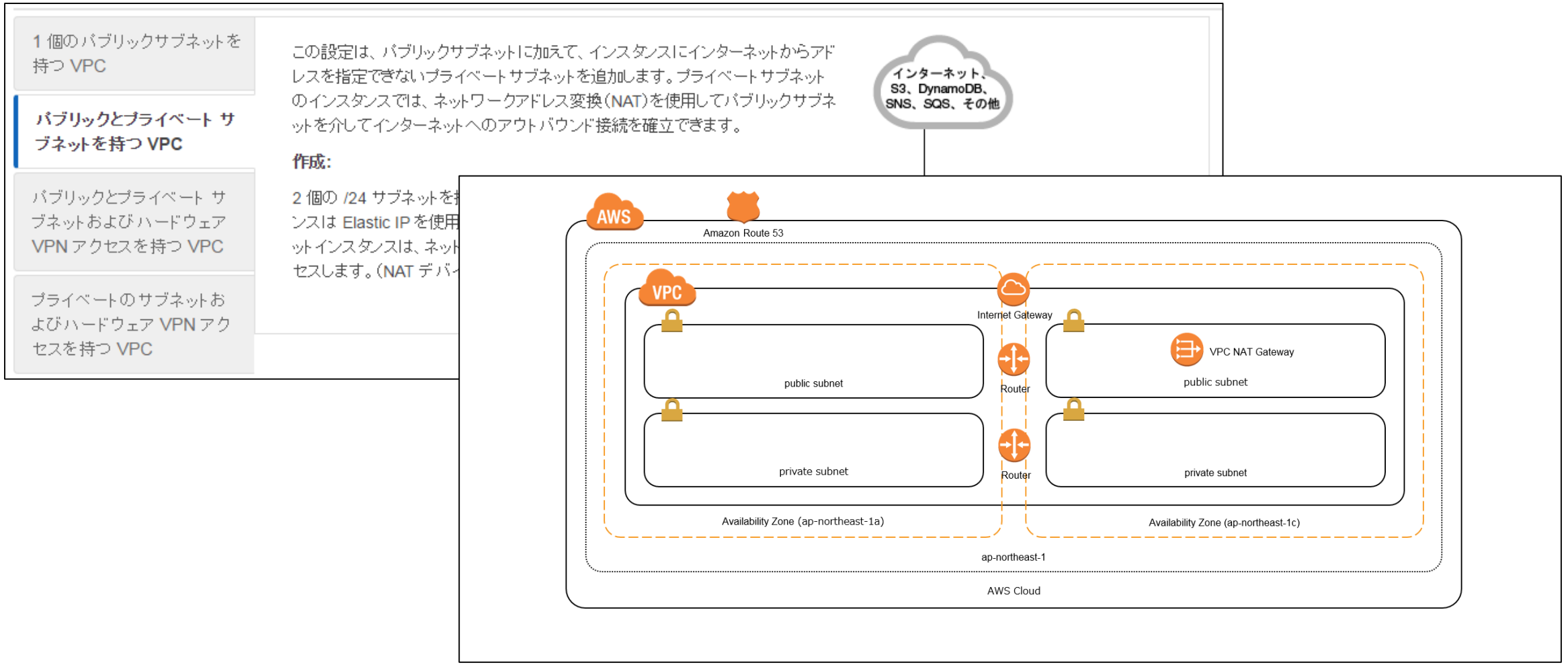
構築用ユーザの作成

IAM画面からユーザを作成

アクセスキーIDとシークレットアクセスキーを取得

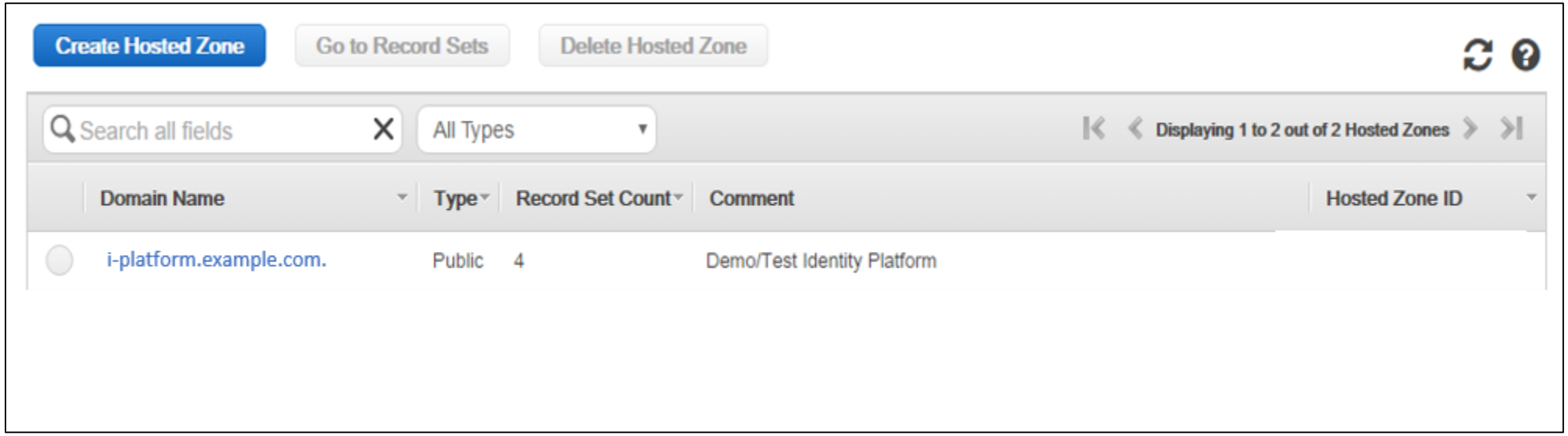
VPCとサブネット作成

ThemiStruct Identity Platformを構築するVPCを作成



DNSへのドメイン設定（Route53）

ThemiStruct Identity Platform用ドメインをRoute53に登録



通知用TOPICの作成

各種通知用のSNS TOPICを作成

次工程のために以下を準備＆メモしておきます

アクセスキーID
シークレットアクセスキー
インストール先のVPCのID
インストール先のサブネットのID
Identity Platform用のドメイン名
通知のためのSNS TOPIC名
Identity Platform用サーバ証明書
マネージメントコンソール用サーバ証明書
メンテナンス通信（SSH）用の公開鍵

下ごしらえ完了

調理の目安
2時間00分

第　2　章

認証基盤の調理

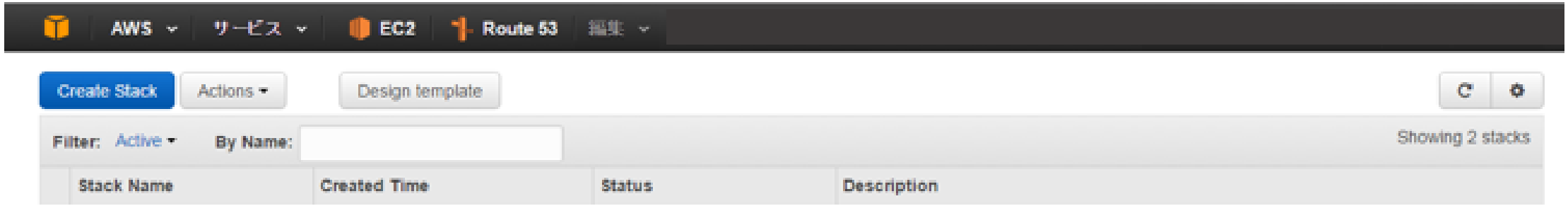
認証基盤の調理の流れ

- マネージメントコンソール作成
- ThemiStruct
  Identity Platform作成

マネージメントコンソール
作成開始！

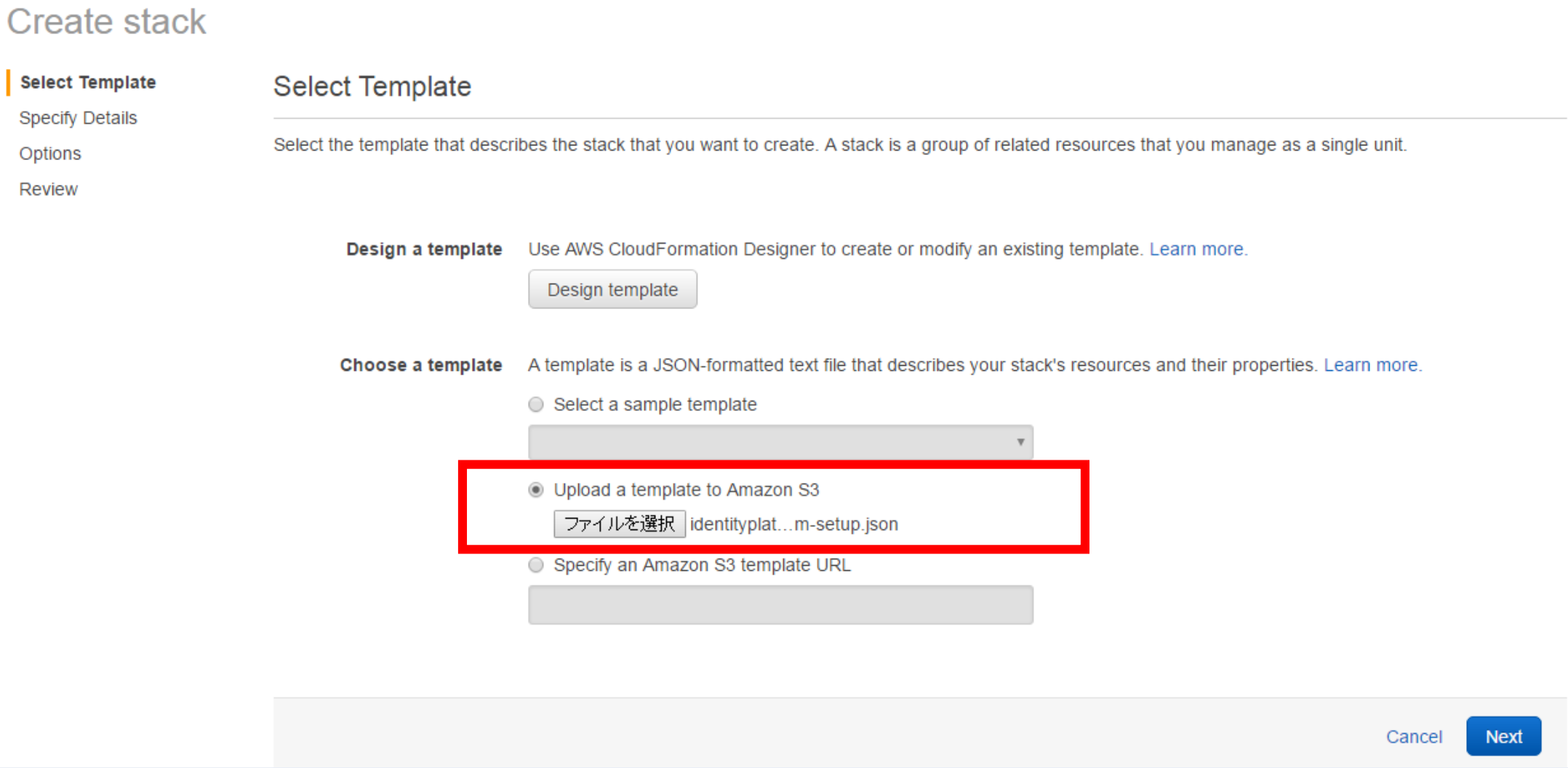
Create Stack

CloudFormationからCreate Stackをクリック



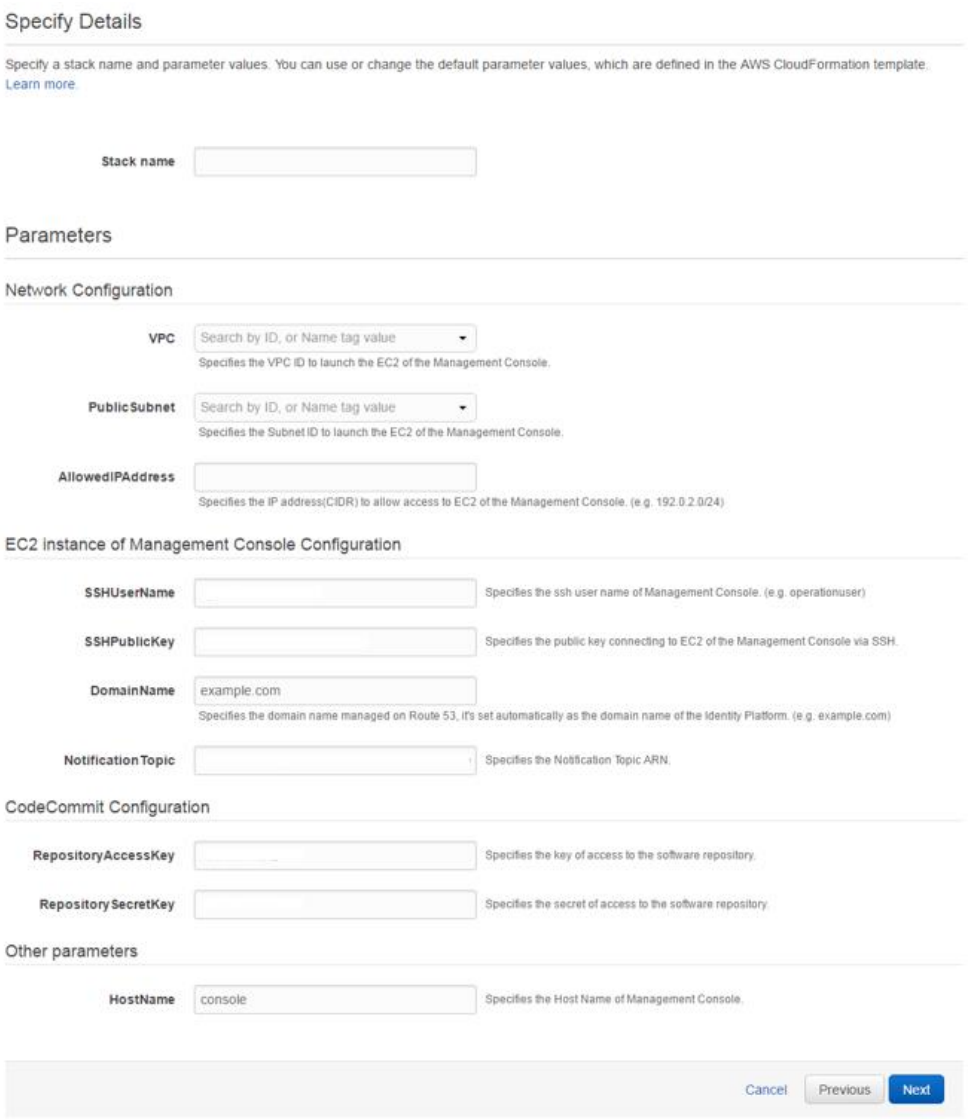
Identity Platformテンプレート選択

ThemiStruct Identity Platform用テンプレートをアップロード



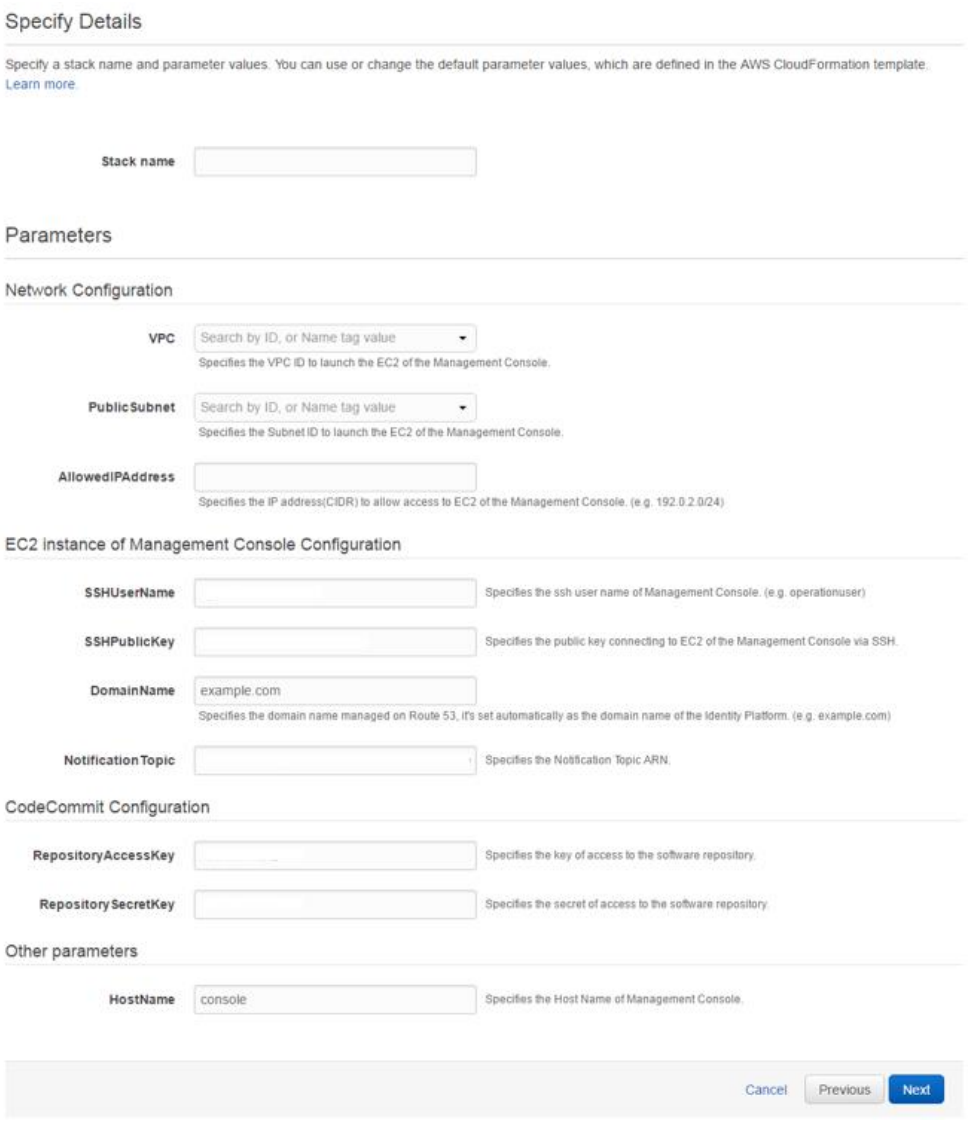
マネジメントコンソール作成時情報入力

- インストールするVPC
- インストールするサブネット
- MCへアクセス可能なIPアドレス
- MCへSSHするためのユーザ名
- MCへSSHするためのSSH公開鍵
- インストールするドメイン名
- 通知のためのSNS TOPIC名
- ThemiStruct Identity Platform用アクセスキー
- ThemiStruct Identity Platform用シークレットキー



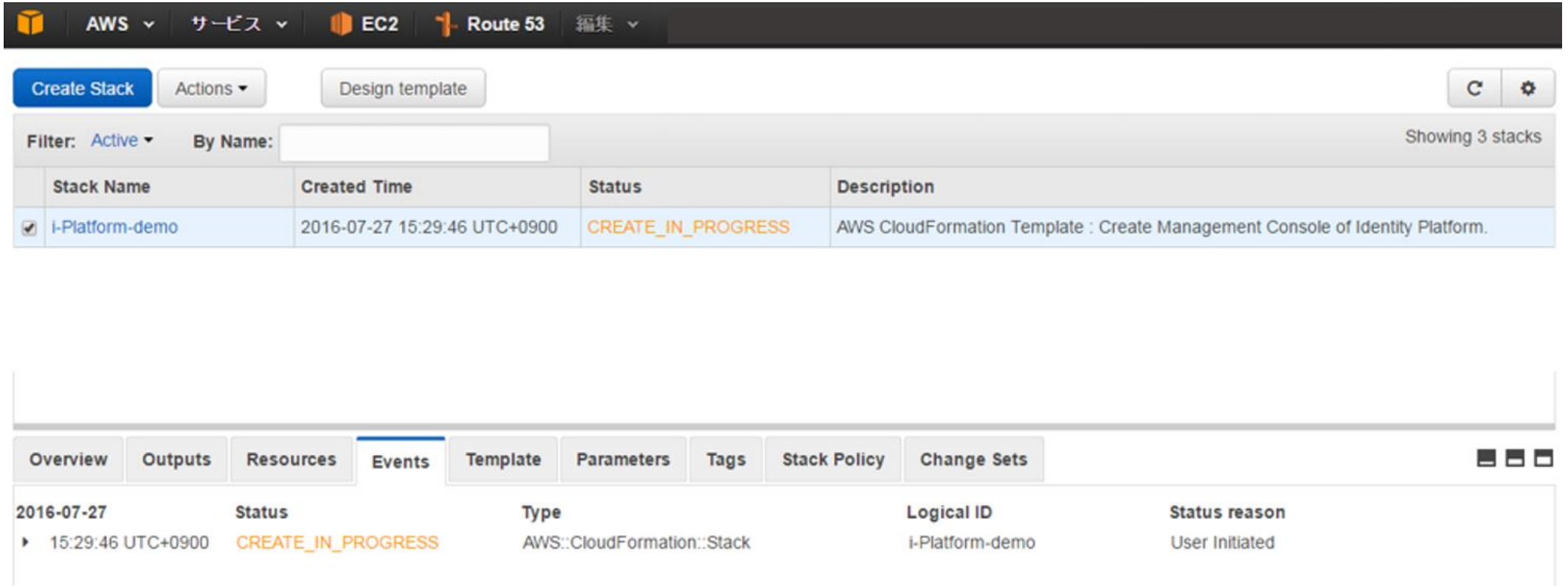
マネジメントコンソール作成時情報入力（ここで考える項目）

- インストールするVPC
- インストールするサブネット
- **MCへアクセス可能なIPアドレス**
- **MCへSSHするためのユーザ名**
- MCへSSHするためのSSH公開鍵
- インストールするドメイン名
- 通知のためのSNS TOPIC名
- ThemiStruct Identity Platform用アクセスキー
- ThemiStruct Identity Platform用シークレットキー



インストール開始

マネージメントコンソールのインストール開始



30分蒸らします

マネージメントコンソール
完成！

Identity Platform
調理開始！

15工程で調理していきます（味付け5分、焼き/蒸らし90分）

Identity Platformインストール時入力項目

アクセスキーID	複数のアベイラビリティゾーンでのレプリケーション
シークレットアクセスキー	RDSのインスタンスクラス
Availability-Zone-1aのサブネットID	データベースの名称
Availability-Zone-1cのサブネットID	データベースのユーザー
Identity Platformのホスト名	ユーザーのパスワード
DNSのHosted Zone	バックアップの保存期間
セットアップするステージ	Identity Platformのサーバ証明書
管理者のパスワード	Identity Platformの証明書の秘密鍵
踏み台として作成するEC2のAMIのID	Identity Platformの中間証明書
踏み台のホスト名	CloudFrontのログを格納するS3のバケット名
踏み台のログインユーザ名	各種コンテンツを格納するS3のバケット名
SSH接続を行う公開鍵	Management Consoleのサーバ証明書
接続を許可するCIDR IPアドレス	Management Consoleの証明書の秘密鍵
	Management Consoleの中間証明書

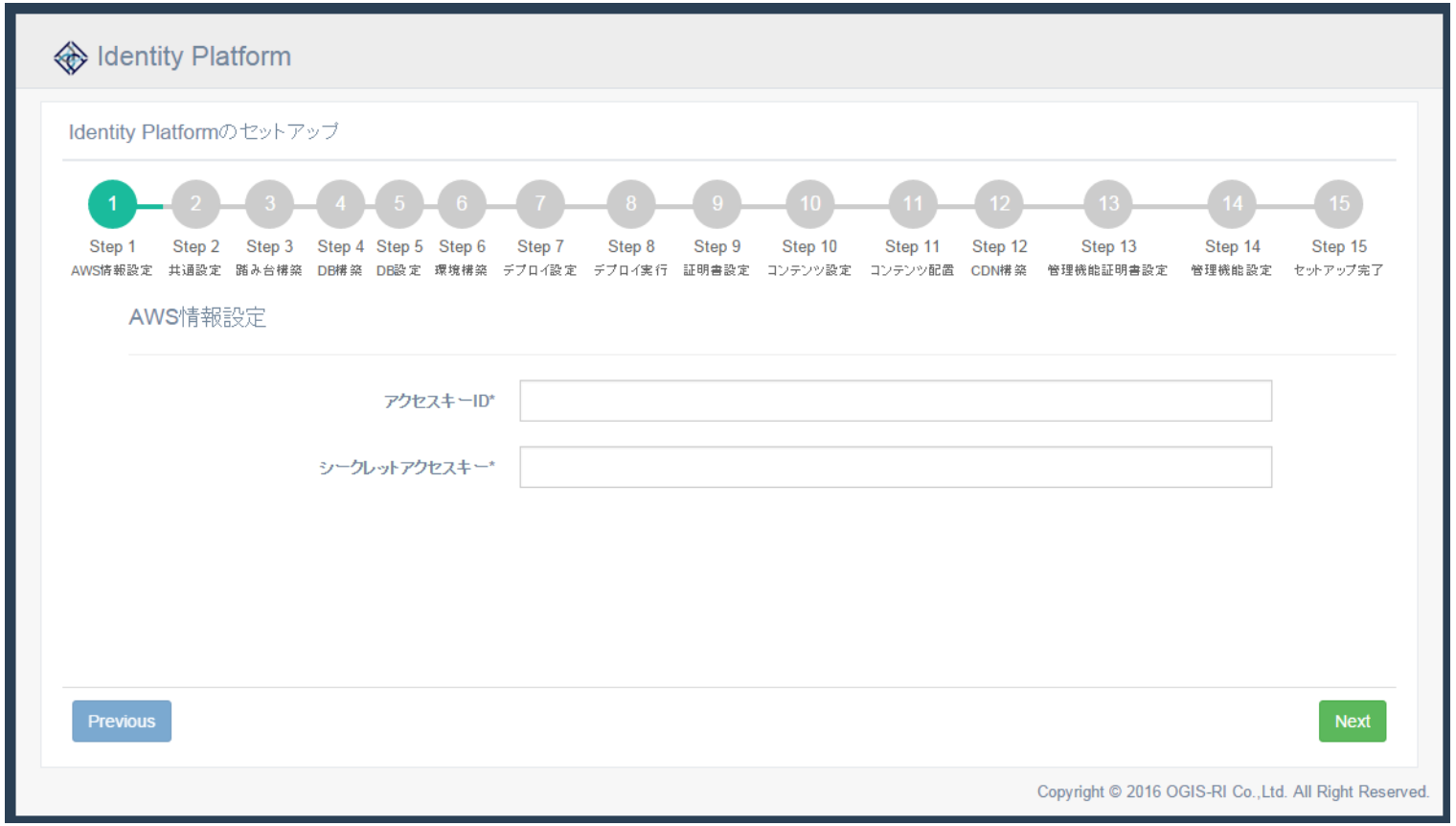
Identity Platformインストール時入力項目（ここで考える項目）

アクセスキーID	**複数のアベイラビリティゾーンでのレプリケーション**
シークレットアクセスキー	**RDSのインスタンスクラス**
Availability-Zone-1aのサブネットID	**データベースの名称**
Availability-Zone-1cのサブネットID	**データベースのユーザー**
Identity Platformのホスト名	**ユーザーのパスワード**
DNSのHosted Zone	**バックアップの保存期間**
セットアップするステージ	Identity Platformのサーバ証明書
管理者のパスワード	Identity Platformの証明書の秘密鍵
踏み台として作成するEC2のAMIのID	Identity Platformの中間証明書
踏み台のホスト名	**CloudFrontのログを格納するS3のバケット名**
踏み台のログインユーザ名	**各種コンテンツを格納するS3のバケット名**
SSH接続を行う公開鍵	Management Consoleのサーバ証明書
接続を許可するCIDR IPアドレス	Management Consoleの証明書の秘密鍵
	Management Consoleの中間証明書

1．AWS情報設定

入力項目

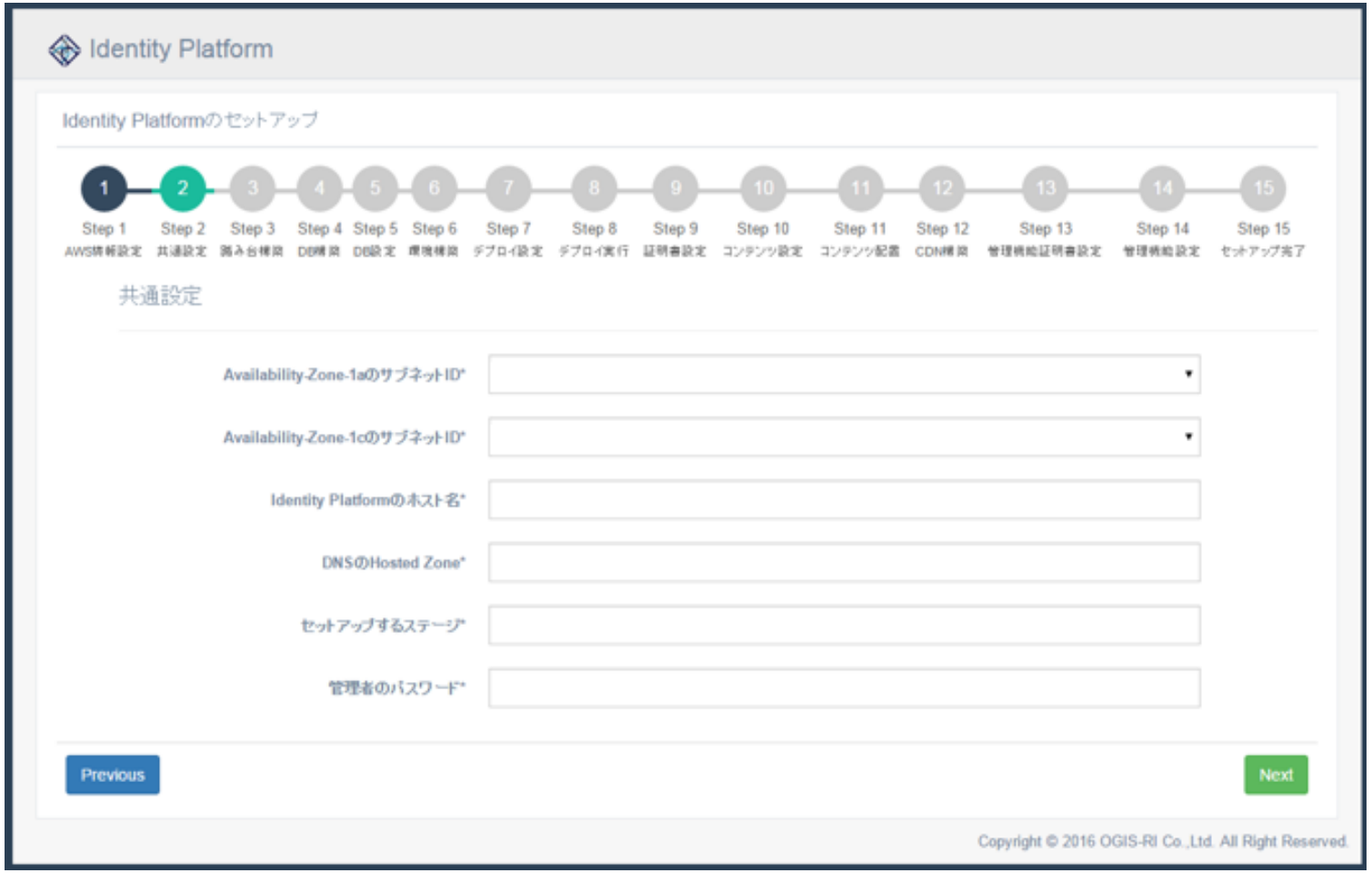
・アクセスキーID
・シークレットアクセスキー



2．共通設定

入力項目

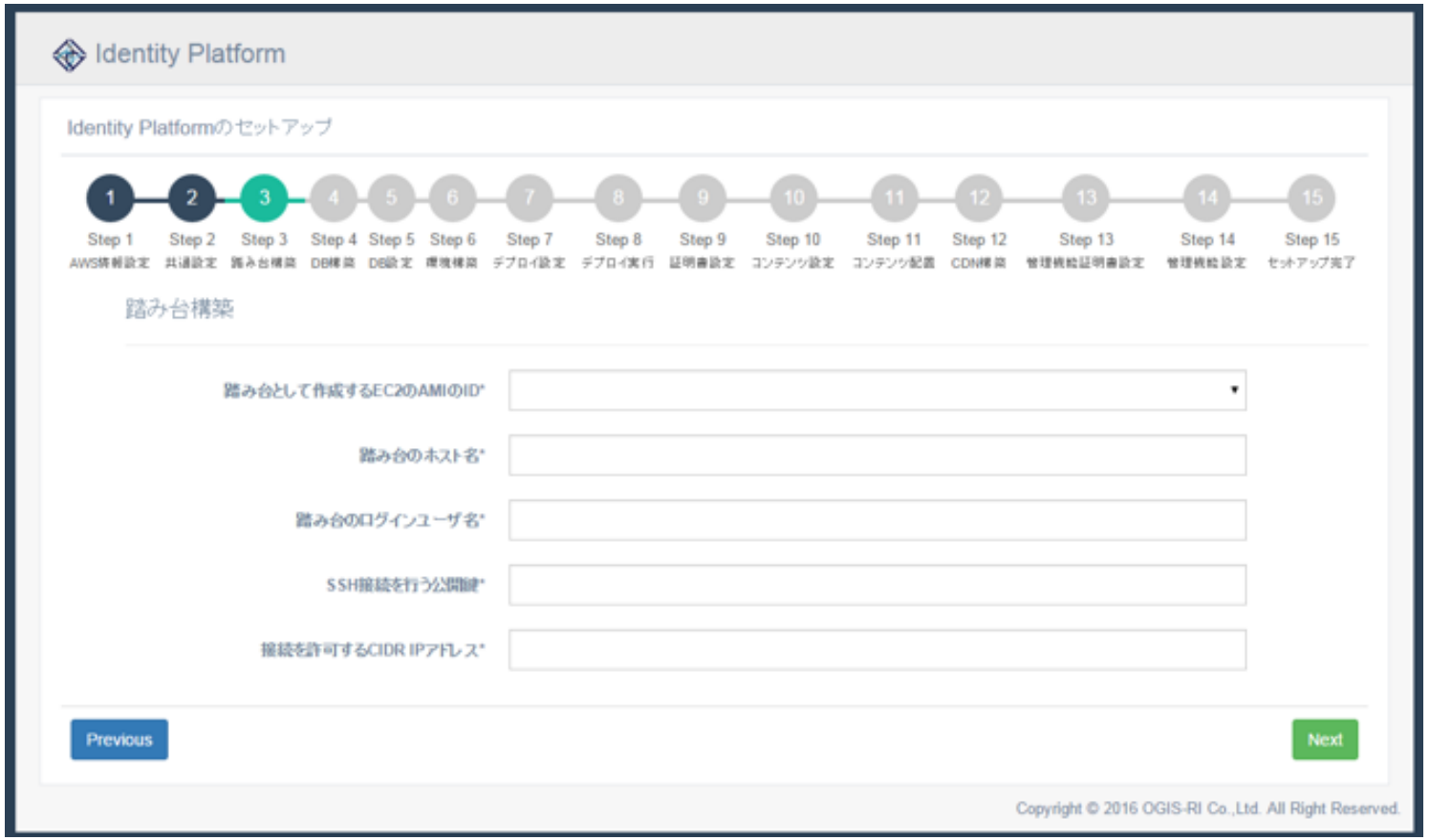
・サブネットID情報
・Identity Platformホスト名
・ドメイン名
・ステージ名
・管理者のパスワード



3．踏み台構築

入力項目

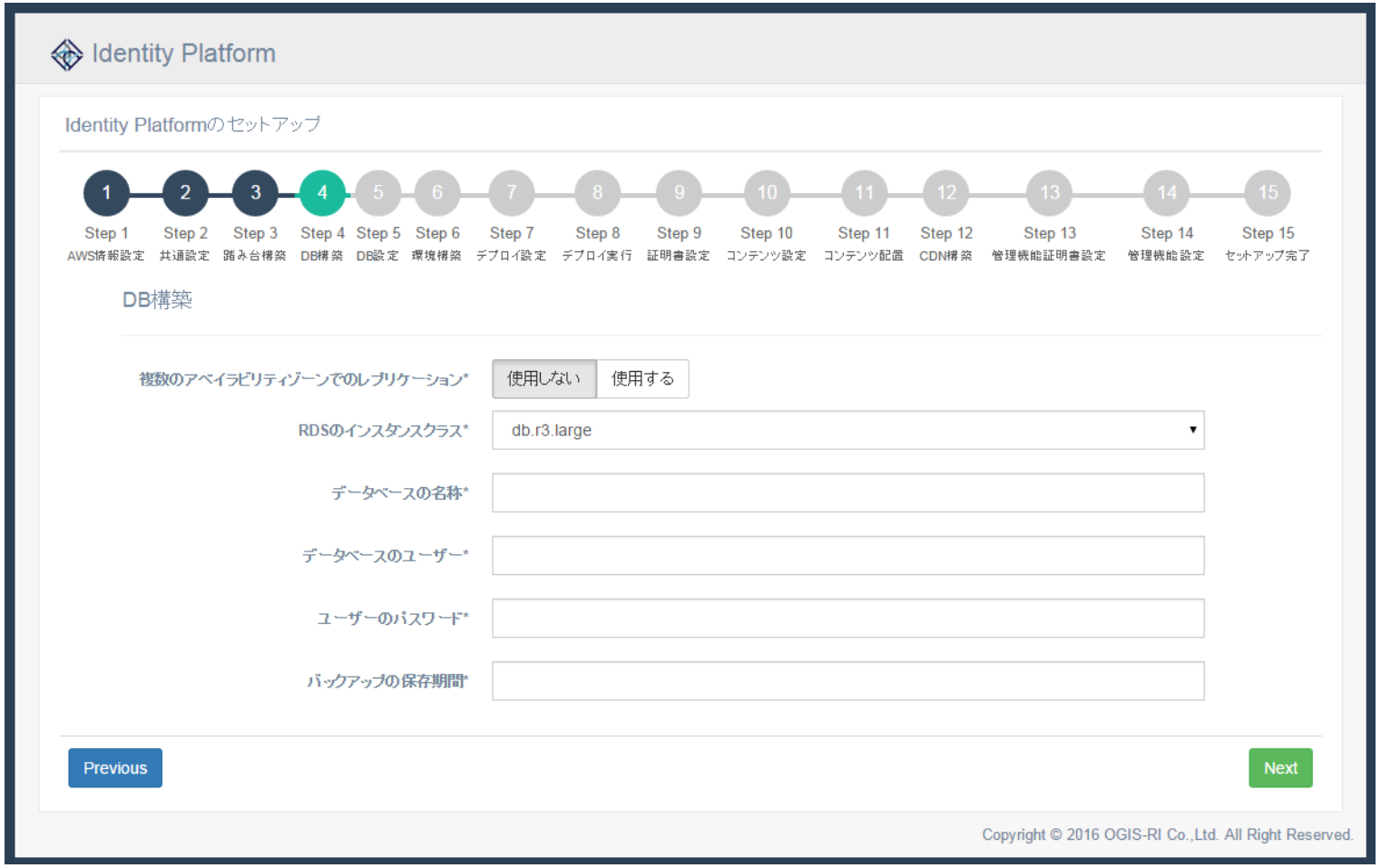
・踏み台サーバのホスト名
・踏み台サーバのユーザ名
・踏み台サーバの
　　SSH接続公開鍵
・踏み台サーバへの
　　アクセス許可IP



4．DB構築

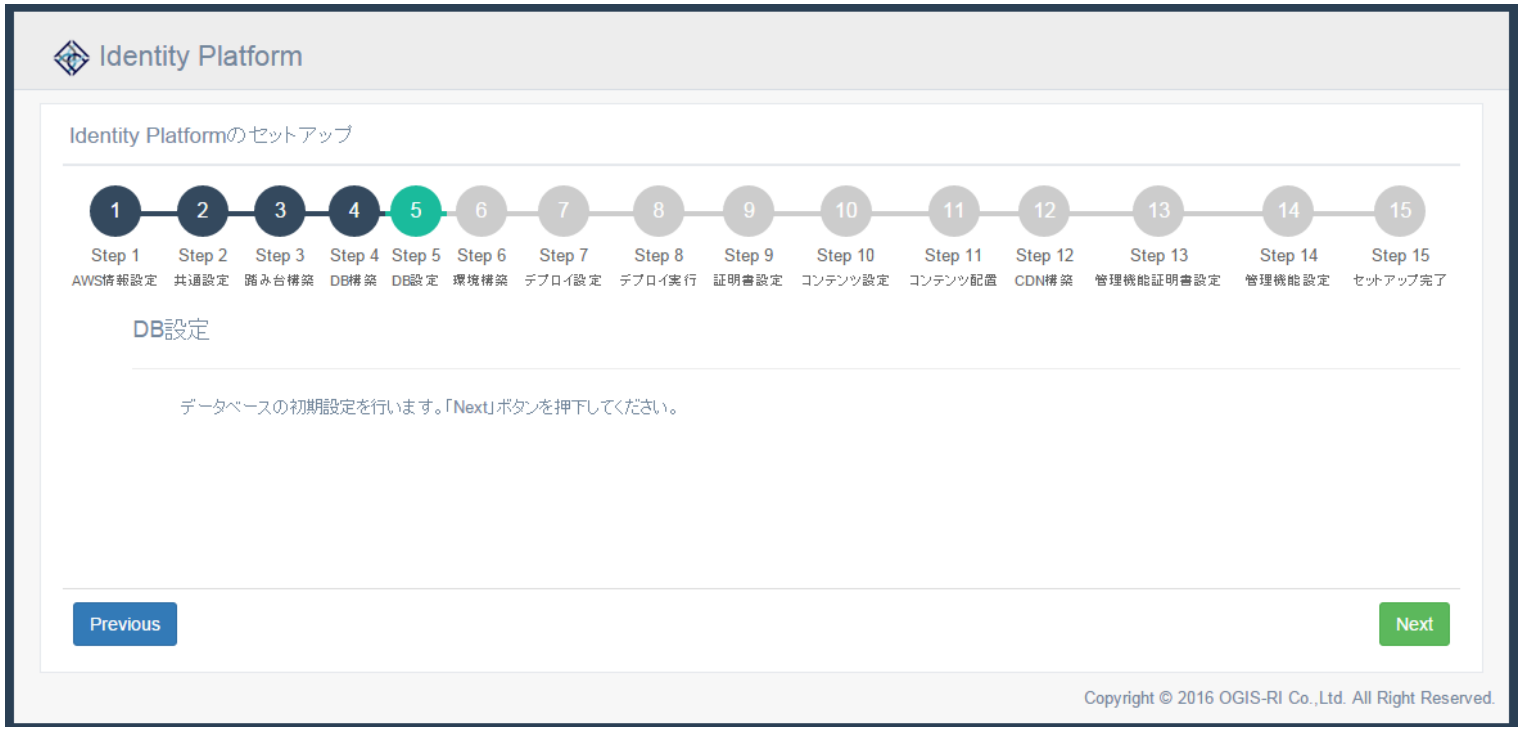
入力項目

・データベースの
　レプリケーション有無
・データベースの
　インスタンスサイズ
・データベースの名前
・データベースの
　ユーザー名
・データベースの
　ユーザパスワード
・バックアップの保存期間



5．DB設定

「Next」をクリックするだけ



6．環境構築

「Next」をクリックするだけ

7．デプロイ設定

「Next」をクリックするだけ

8．デプロイ実行

「Next」をクリックするだけ

9．Identity Platform用サーバ証明書設定

入力項目

・Identity Platform用の
　サーバ証明書
　秘密鍵
　中間証明書

１０．コンテンツ設定

入力項目

・ログの格納先バケット名
・コンテンツ格納先バケット名

１１．コンテンツ配置

「Next」をクリックするだけ

１２．CDN構築

「Next」をクリックするだけ

１３．管理機能証明書設定

入力項目

・マネジメントコンソール用の
　サーバ証明書
　秘密鍵
　中間証明書

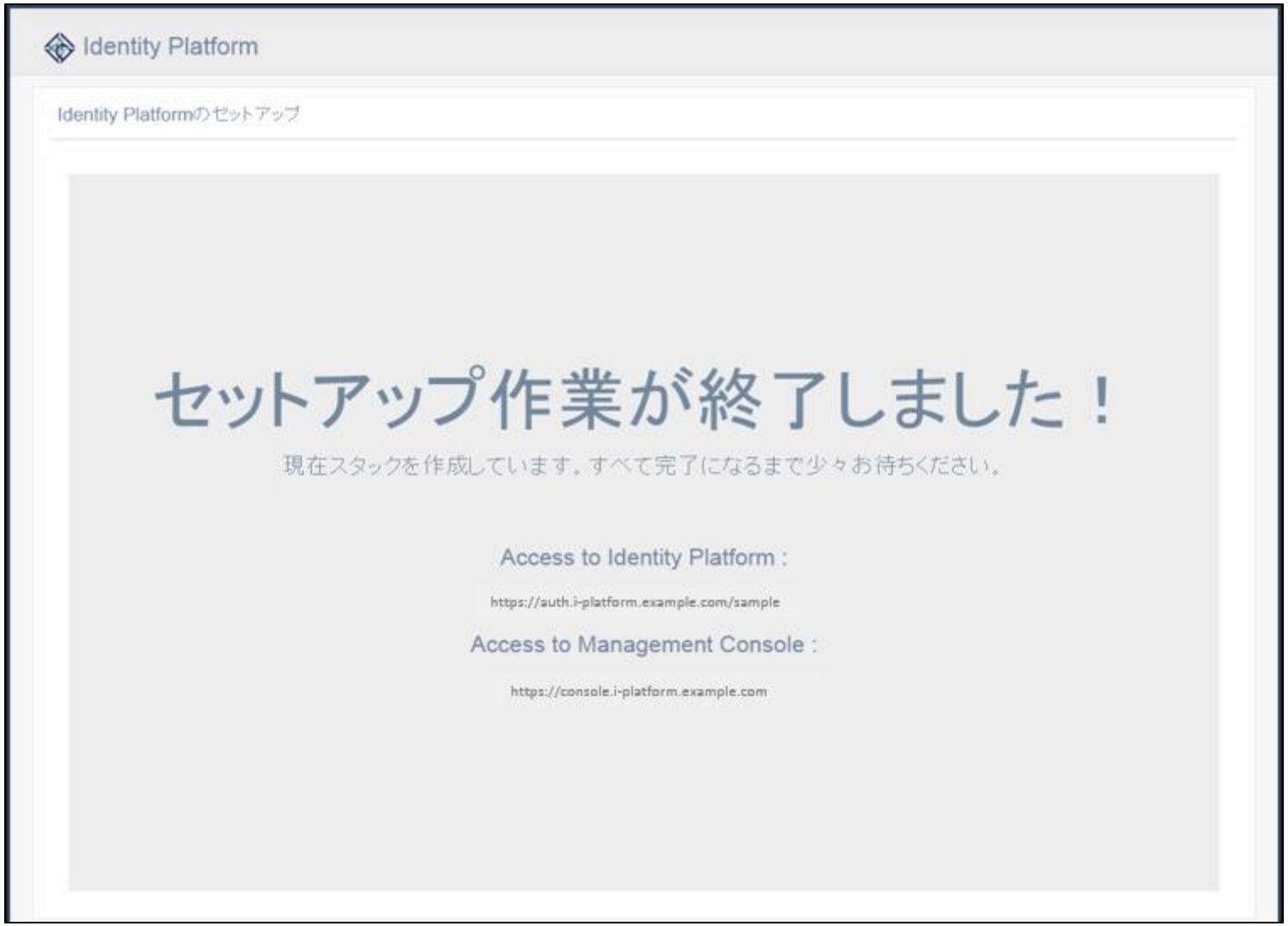
１４．管理機能設定

「Next」をクリックするだけ

１５．管理コンソールの再起動

「再起動」をクリックするだけ

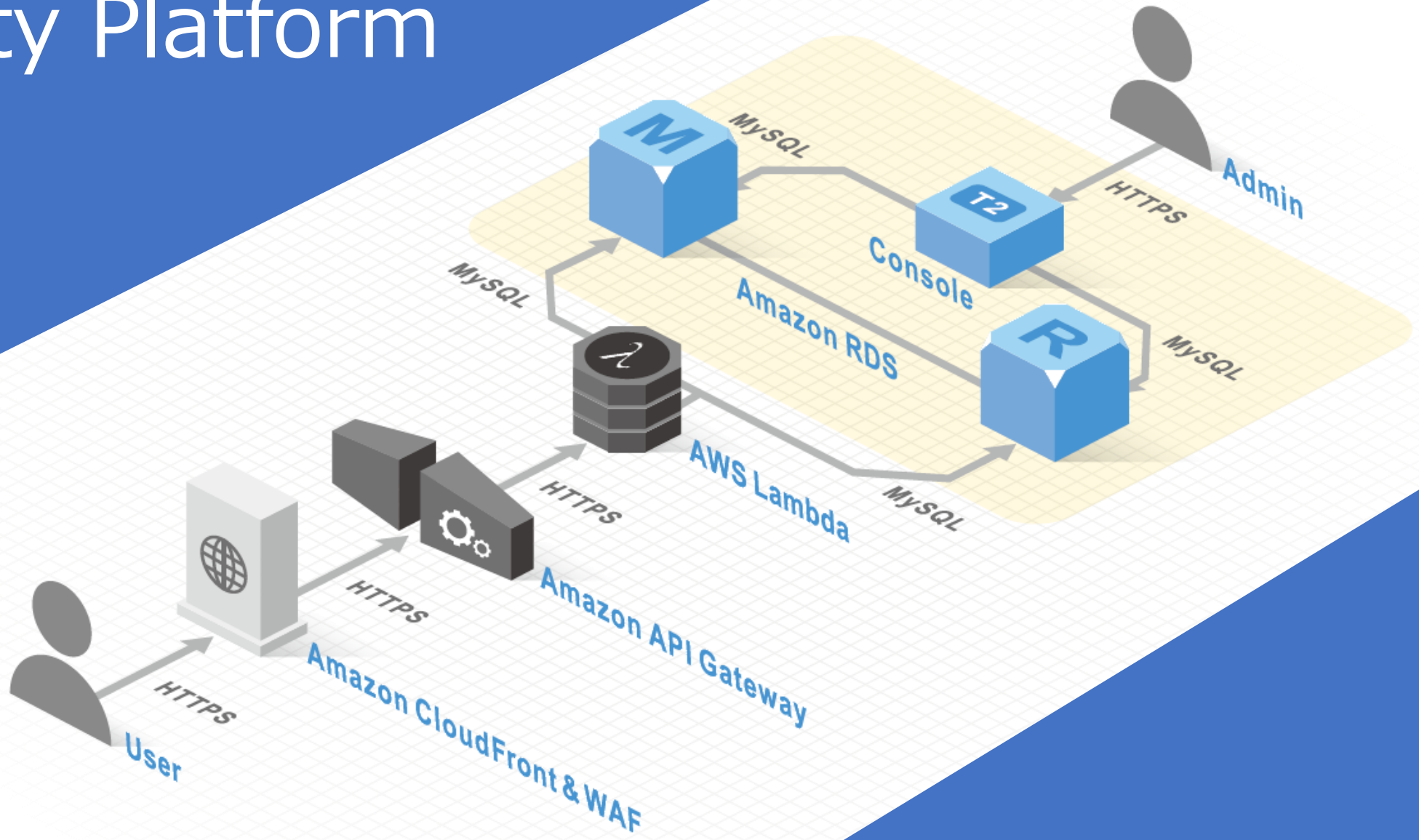
セットアップ完了

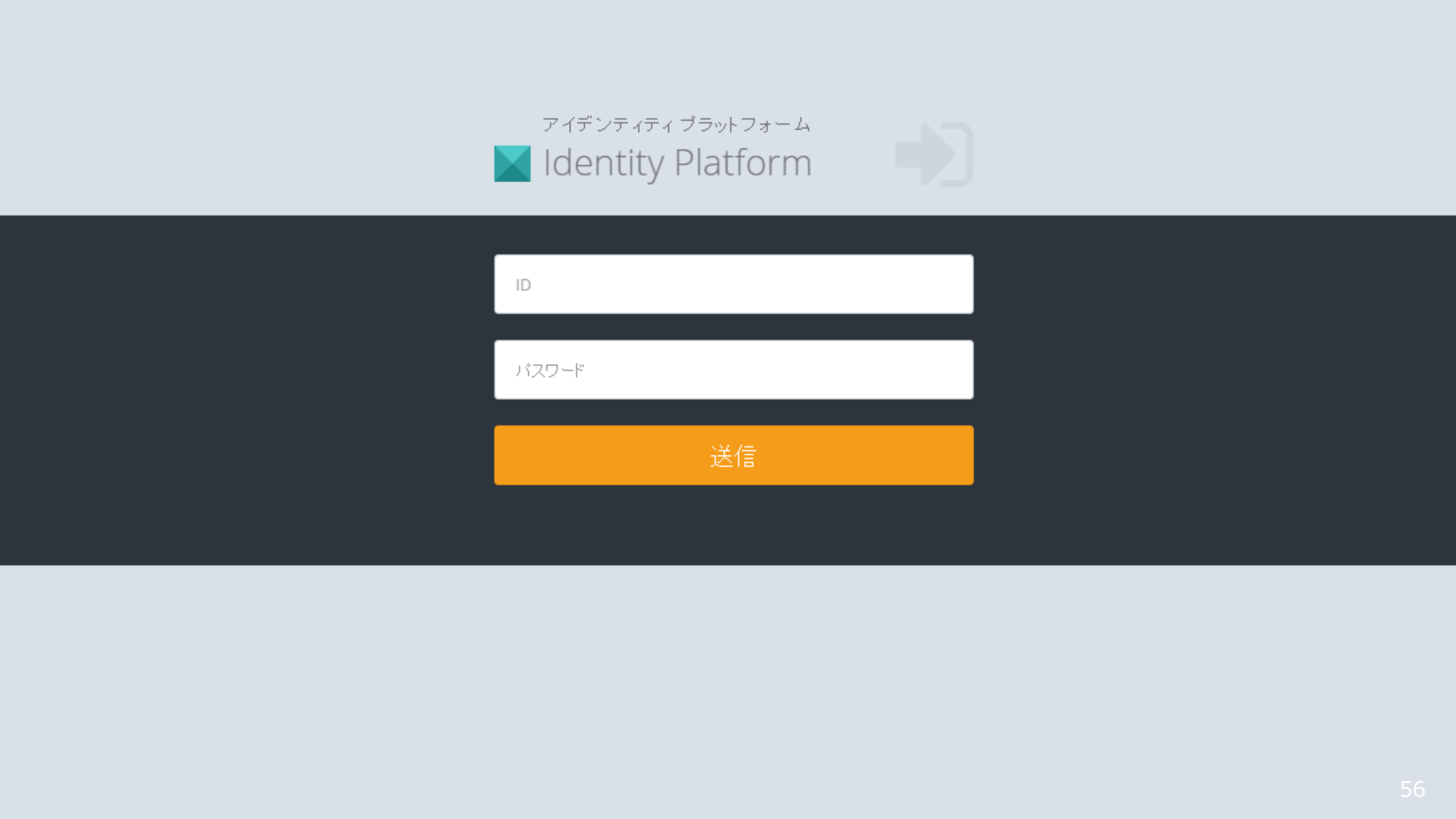


まず認証基盤できた！


ThemiStruct
デミストラクト
Identity Platform
AWS
対応版

ThemiStruct Identity Platform




アイデンティティ プラットフォーム
Identity Platform
ID
パスワード
送信

Identity Platform

tsipadmin
Administrator

- Home
- User
- Authentication
- Federation
- Application
- Global Config

Identity Platform Admin Page you can configure some of parameters.

Administrator Management Console Page

Page Description

Index
This page.

User Setting
User CRUD.

Authentication Setting
Authentication configuration CRUD.

OpenID Connect Setting
OpenID Connect configuration CRUD.

THANK YOU FOR YOUR BUSINESS

http://www.ogis-ri.co.jp/

第　3　章

盛り付け
～アプリケーション接続～

本日盛り付けるアプリケーション

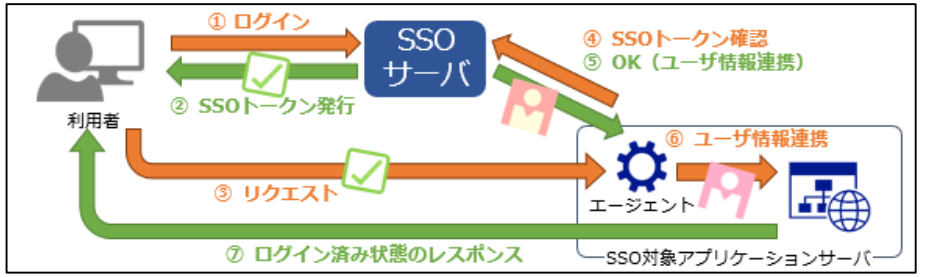
オンプレミスのデータセンターに配置されたアプリケーション

クラウドサービス

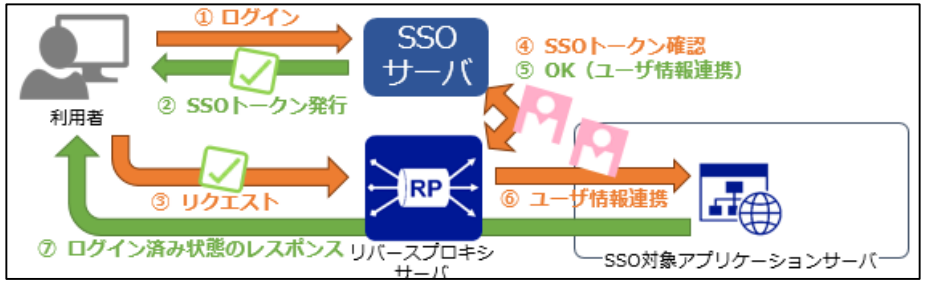
Office 365

盛り付け方は３パターンをご用意

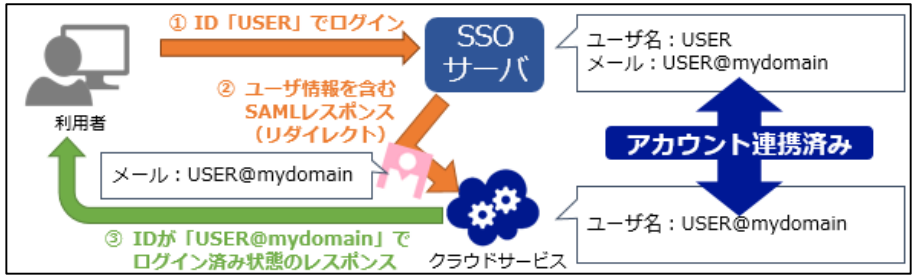
- エージェントによる接続



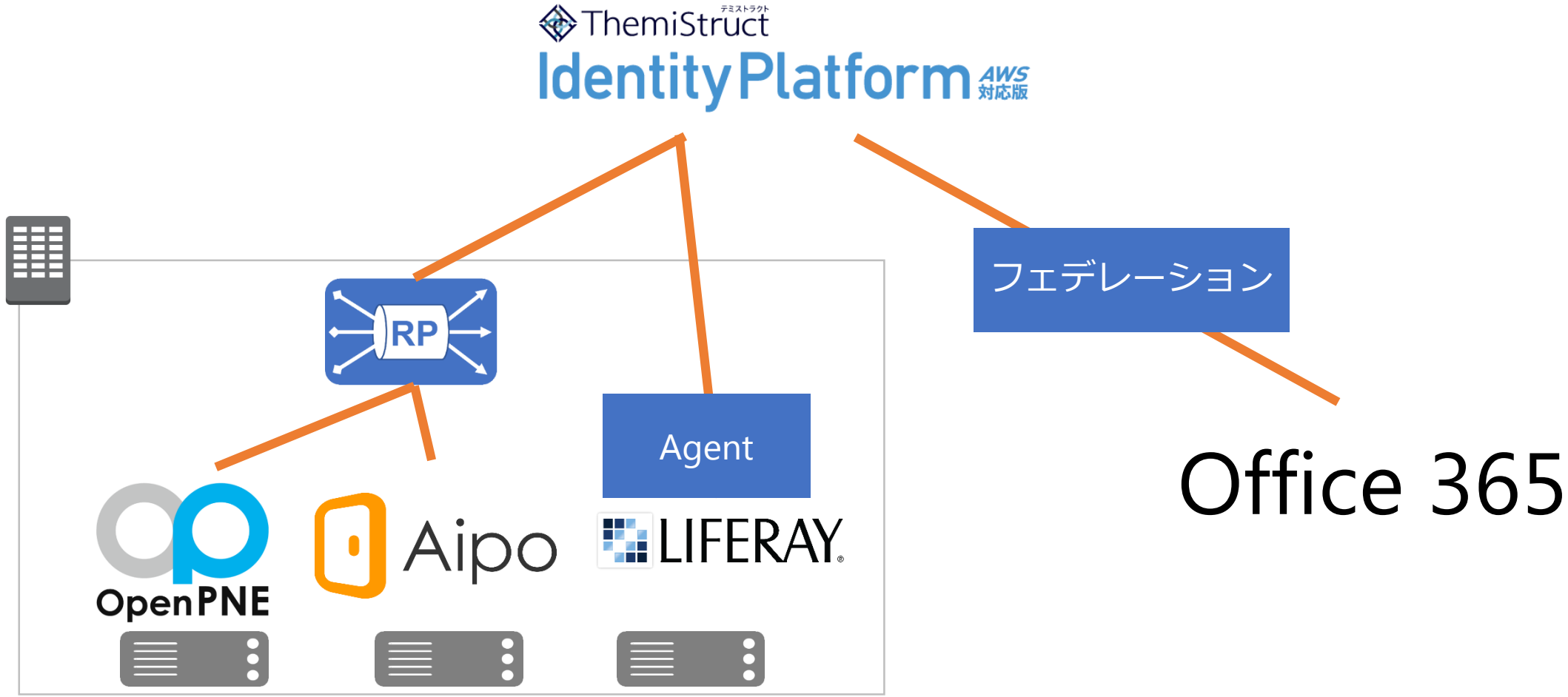
- リバースプロキシによる接続



- フェデレーションによる接続



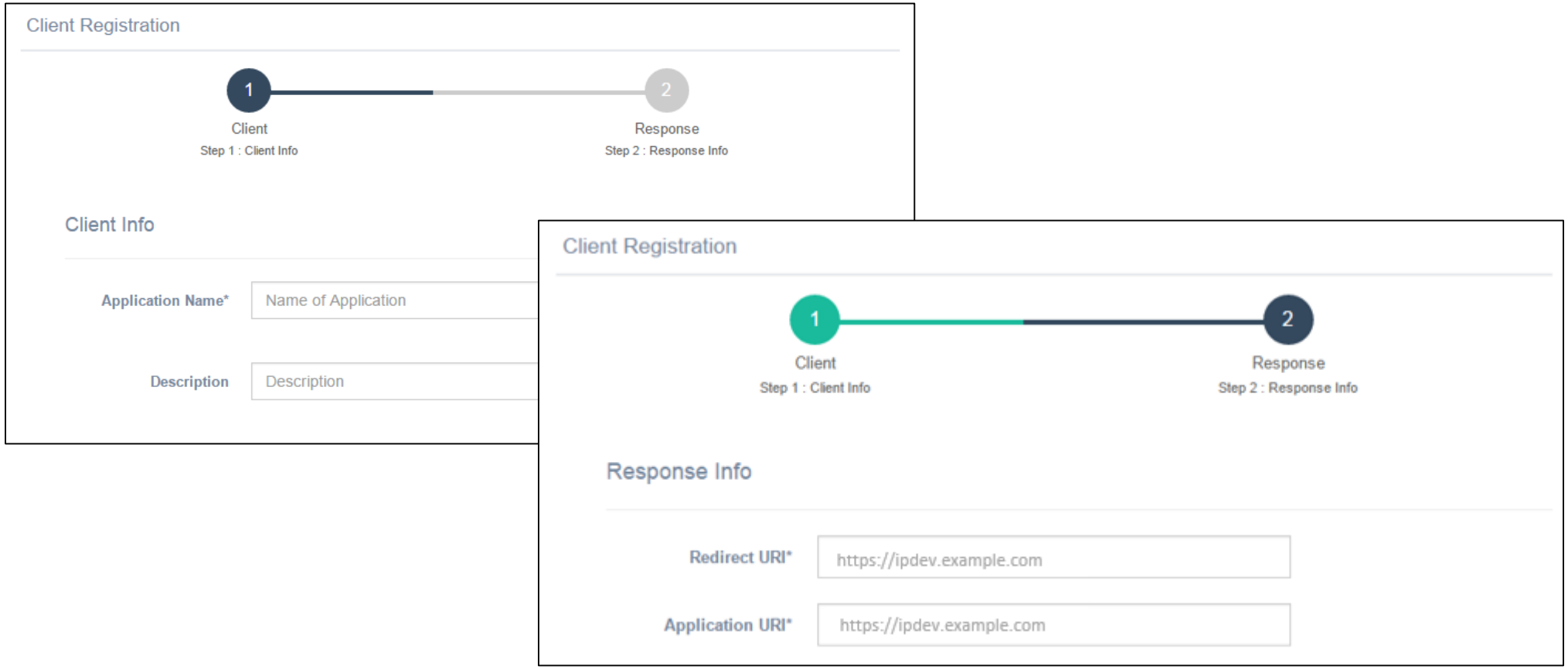
盛り付け例



参考｜リバースプロキシでの接続①

リバースプロキシでアプリケーションに接続する場合

1. ThemiStruct Identity Platformへのアプリ登録



参考｜リバースプロキシでの接続②

リバースプロキシでアプリケーションに接続する場合

2. フェデレーションプロキシ構築キットでアプリ接続

1.フェデレーションプロキシのインストールを実行

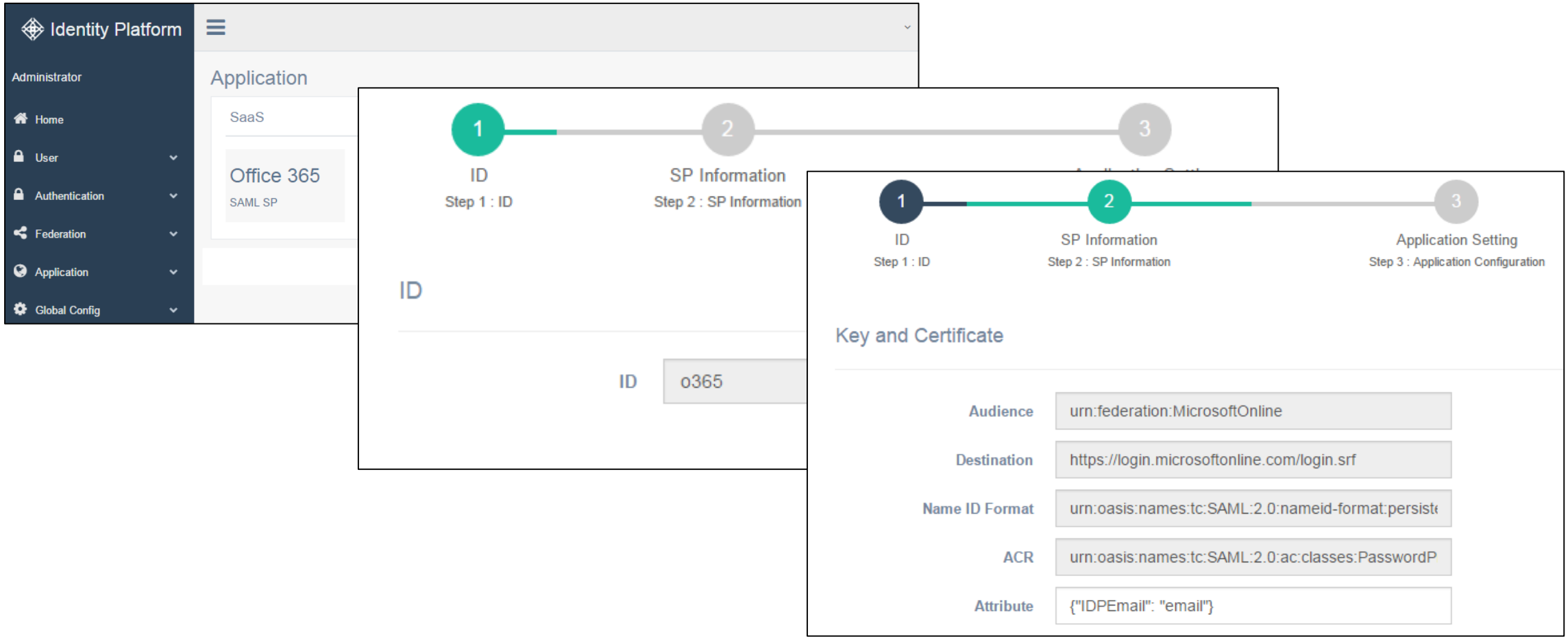
```
# /opt/federationproxy/install.sh
```

2.addappコマンドを実行

```
# /opt/federationproxy/addapp.sh ¥
    -p openpne ¥
    -v https://openpne.example.com:443 ¥
    -d https://dest.example.com:443 ¥
    -o https://op.example.com:443/prod ¥
    -c /etc/pki/tls/certs/openpne.crt ¥
    -k /etc/pki/tls/private/openpne.key ¥
    -I openpne.jNuaTZ3B ¥
    -s sX79zi3Y
```

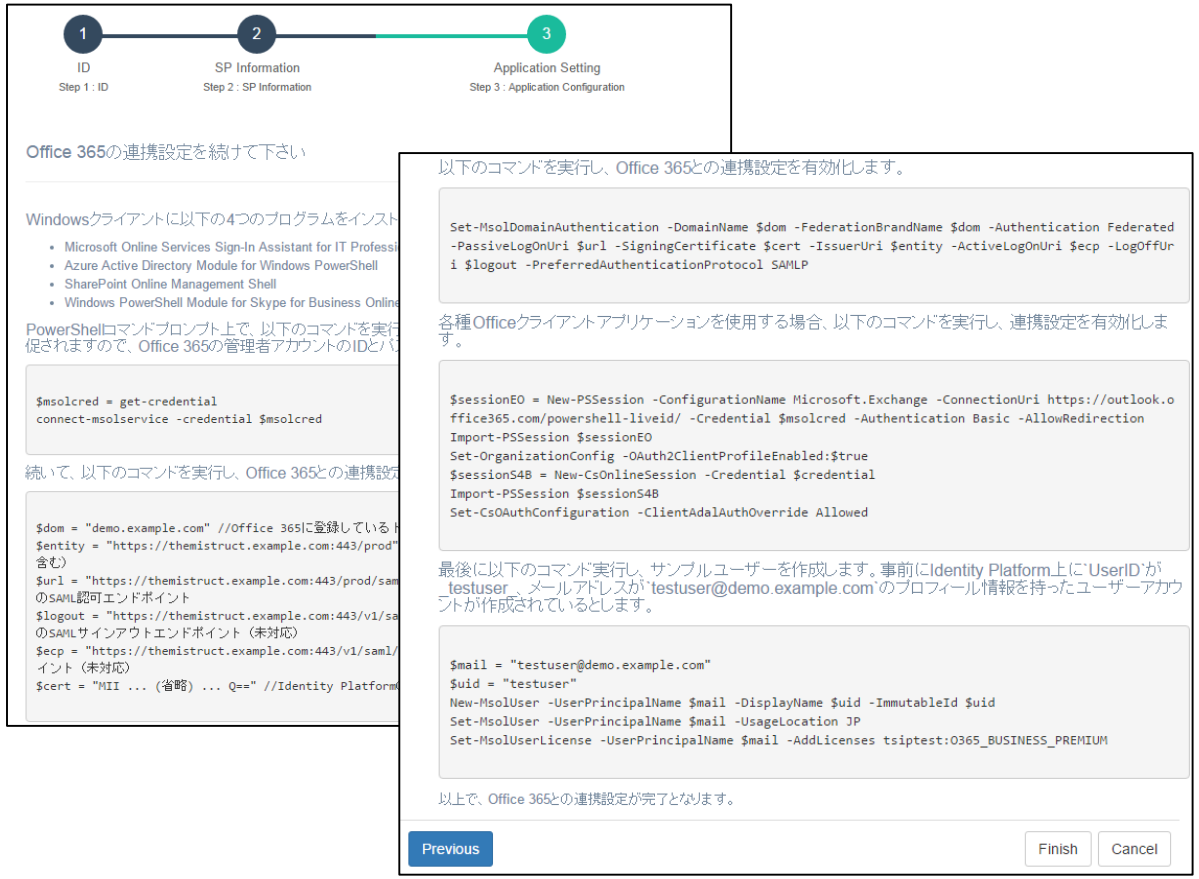
参考｜Office 365 の接続①

Office 365 と接続する場合は、ThemiStruct Identity Platform側は管理画面で以下の設定し、



参考｜Office 365 の接続②

完了画面に表示されるとおりに、PowerShellを実行することで
Office 365 との接続は完了します。



できた！


Office 365
ThemiStruct
デミストラクト
Identity Platform
AWS
対応版
OpenPNE
Aipo
LIFERAY

第　4　章

認証基盤の味見

味見

味見１
　アプリケーションのSSO
味見２
　Office 365 利用

味見１

アプリケーションのSSO

味見 2

Office 365 利用

お召し上がりください

ThemiStruct Identity Platformご紹介

ThemiStruct（テミストラクト）
Identity Platform AWS対応版

- ✓AWSネイティブな
  アイデンティティ連携基盤
- ✓≠OpenAM
- ✓≠OpenIDM
- ✓オージス総研自社商品

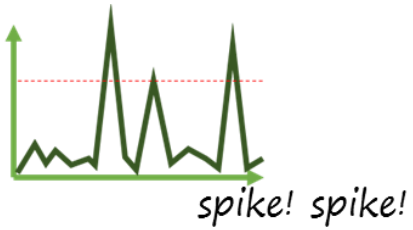
これからの認証プラットフォームに求められること

膨大なトラフィック量への対応

- 認証基盤の役割増加
- 事業者が提供するサービスの増加
- ユーザ数・デバイス数の増加
- API利用の増加

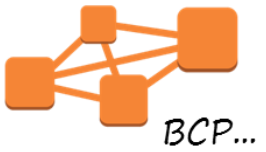
スパイクアクセスへの対応

- キャンペーンやニュースサイト掲載などにより定常的なアクセスと比較し、予想不可な大量のアクセスが発生する



システム停止回避への対応

- 認証基盤役割の増加に伴い、システム停止や遅延による機会損失が大きくなり、事業継続性や機会損失回避など可用性要求のレベルが格段にUPした



スピードスタート・スモールスタートへの対応

- 短期間でビジネスをスタートさせたり、事業規模に応じてスタート、柔軟にスケールできる必要がある

ネイティブなアーキテクチャで高い可用性、成長と共に変化する拡張性を確保

仮想サーバーを極力使用しないアーキテクチャで実装

Amazon
API
Gateway

AWS
Lambda

Amazon
RDS
for Aurora

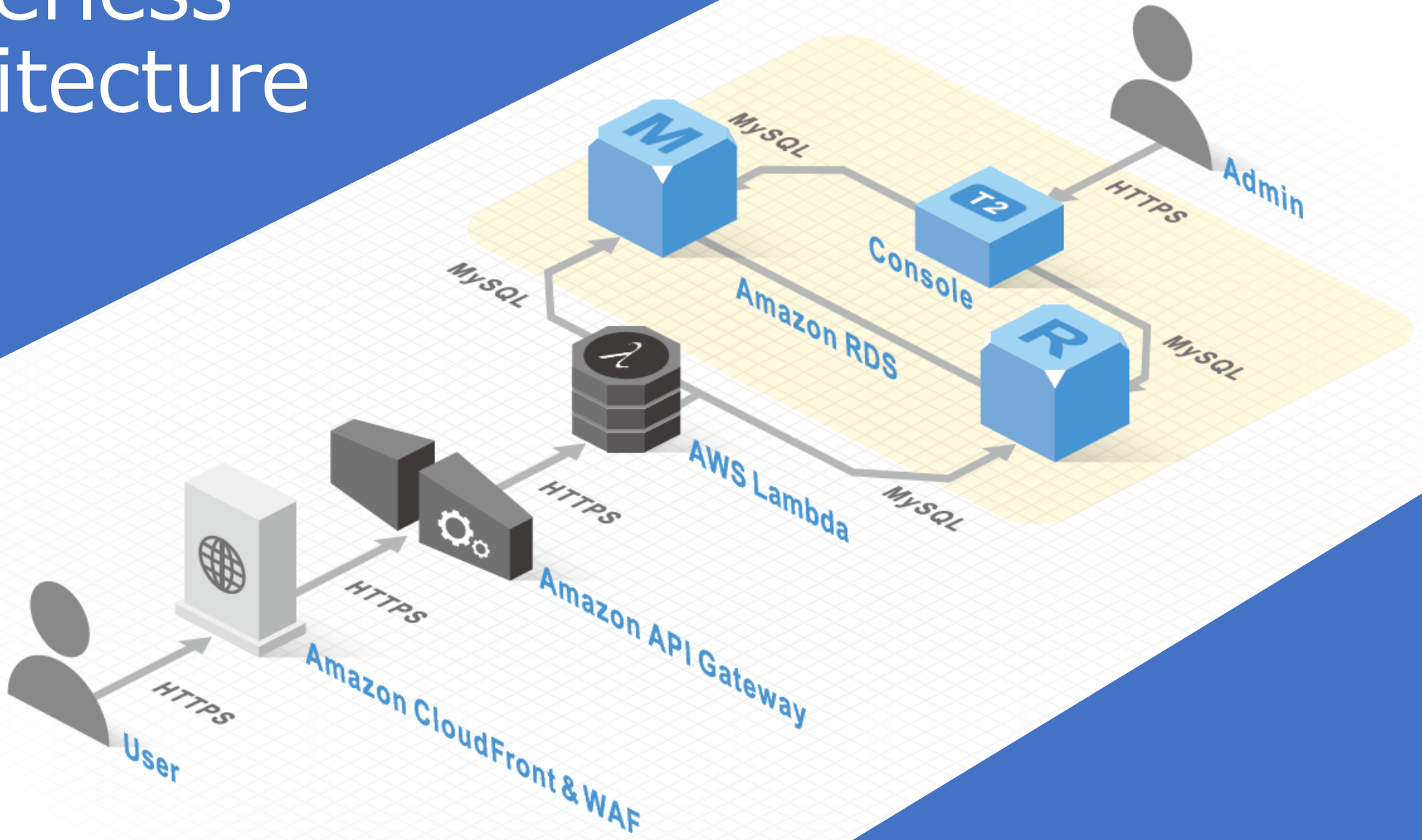
AWSネイティブなアーキテクチャにより下記の恩恵を享受

リクエストに応じた伸縮が可能

一定の可用性確保と自動復旧の実現

プロジェクトの短期間化

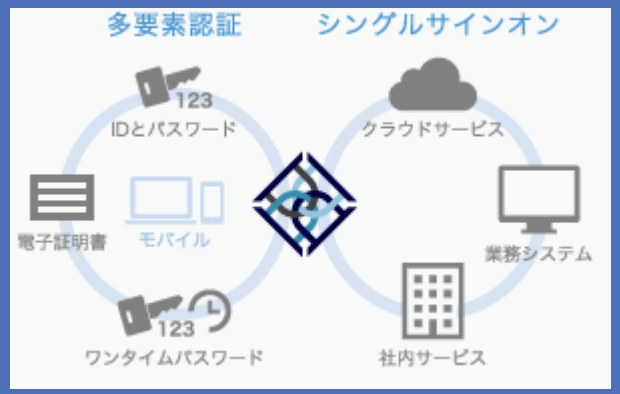
Serverless Architecture



ThemiStruct Identity Platformの特徴

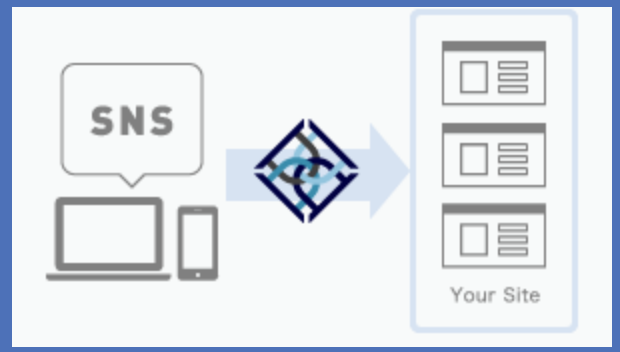
認証システムの短期導入が可能

ThemiStruct Identity Platformはクラウド上に設置され、短期間で従業員、カスタマー、ビジネスパートナーに認証サービスを提供できます。また、APIを利用し既設サイトへの組み込みも容易です。



ログインを1回に、認証方法も組合せ自由

ThemiStruct Identity Platformに一度ログインを行うことで、ユーザが利用したい各サイトへシングルサインオンすることができます。その際のログインではIDとパスワードによる認証だけでなく、ワンタイムパスワード・電子証明書、指紋・指静脈情報やインベントリー認証などを利用することができます。また利用システムごとの設定により、各サイトやコンテンツのセキュリティ、ユーザビリティ要件に応じた認証を行うことができます。



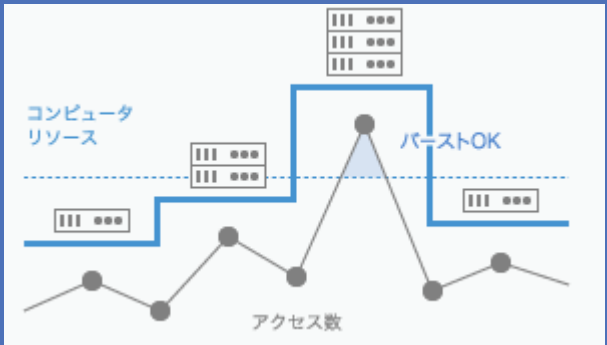
ユーザ登録のハードルを下げ、新規ユーザ登録率をアップ

FacebookやGoogleなどのユーザが普段使っているSNSやWebサービスのアカウントを利用して、気軽にユーザ登録が可能です。サイトへの新規ユーザ登録率、ユーザビリティ、コンバージョン率を向上させます。ユーザ自身による登録や、管理者による一括登録も可能です。

ThemiStruct Identity Platformの特徴

各システムへ必要なときに、必要な情報を連携できます

ThemiStruct Identity Platformから各システムへ必要なタイミングで、必要なユーザ情報を連携することができます。各システムでユーザ情報の管理が不要になります。



事業成長に合わせたスケーリング、突発的アクセス集中への対応

サーバレスアーキテクチャにより、事業環境の変化や突発的アクセス集中に合わせて、自由にかつ自動でコンピュータリソースの拡張・縮小を行えます。

本日のまとめ

1. 「ThemiStruct Identity Platform」なら
認証プラットフォームはすぐ建てられる

2. 「ThemiStruct Identity Platform」なら
アプリケーションもすぐにつながる

AWS上にパっと作ってサっと使える統合認証プラットフォーム

「ThemiStruct（テミストラクト）Identity Platform」

ご清聴ありがとうございました

ThemiStruct
テミストラクト

【お問い合わせ先】
株式会社オージス総研
TEL: 03-6712-1201 / 06-6871-7998
mail: info@ogis-ri.co.jp

OGIS-RI