

「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

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



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見たんだけど
試してみてくださいよ」



ThemisStruct 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な

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


下記しえ

- 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アカウントの作成



The screenshot shows the AWS account creation page. At the top left is the Amazon Web Services logo. The main heading is 'サインイン、または AWS アカウントを作成' (Sign in or create an AWS account). Below this, there is a form with a text input field for 'Eメールまたは携帯電話の番号を入力してください。' (Enter your email or mobile phone number). Below the input field are two radio buttons: '私は新規ユーザーです。' (I am a new user) and '私は既存のユーザーです' (I am an existing user). The second option is followed by a password input field and a 'サインイン(セキュリティシステムを使う)' (Sign in) button. A link 'パスワードをお忘れですか?' (Forgot your password?) is located below the button. To the right of the form, there is a section titled '新しい AWS アカウントには以下の特典が含まれます。' (New AWS accounts include the following benefits). This section lists 'AWS 無料利用枠を 12 か月間利用可能' (12 months of AWS Free Tier) with details for Amazon EC2, Amazon S3, Amazon RDS, and Amazon DynamoDB. It also lists 'AWS ベーシックサポートの特徴' (Features of AWS Basic Support) including 24/7 customer service, support forums, and documentation. At the bottom of the page, there is a section titled 'Amazon.com のサインインについて' (About signing in to Amazon.com) and a footer with the text '利用規約 プライバシーポリシー AWS カスタマーアグリーメント © 1996-2016, ©1996-2014, Amazon.com, Inc. or its affiliates. An amazon.com company'.

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

The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like 'ダッシュボード', 'IAM の検索', '詳細', 'グループ', 'ユーザー', 'ロール', 'ポリシー', 'ID プロバイダ', 'アカウント設定', '認証情報レポート', and '暗号化キー'. The main content area is titled 'Identity and Access Management へようこそ' and displays summary statistics for IAM resources: 'ユーザー: 43', 'ロール: 70', 'グループ: 9', 'ID プロバイダ: 2', and 'カスタマー管理ポリシー: 6'. A notification banner at the bottom of the main area states: '1 ユーザーが正常に作成されました。これは、これらのユーザーセキュリティ認証情報をダウンロードできる最後の機会です。これらの認証情報はいつでも管理および再作成できます。' Below this, a dropdown menu is expanded to show 'ユーザーのセキュリティ認証情報を非表示'. The user 'IPUSER' is listed, and their 'アクセスキー ID' and 'シークレットアクセスキー' are displayed in a yellow box, with the secret key field highlighted by a red rectangle.

VPCとサブネット作成

ThemiStruct Identity Platformを構築するVPCを作成

1 個のパブリックサブネットを持つ VPC

パブリックとプライベート サブネットを持つ VPC

パブリックとプライベート サブネットおよびハードウェア VPN アクセスを持つ VPC

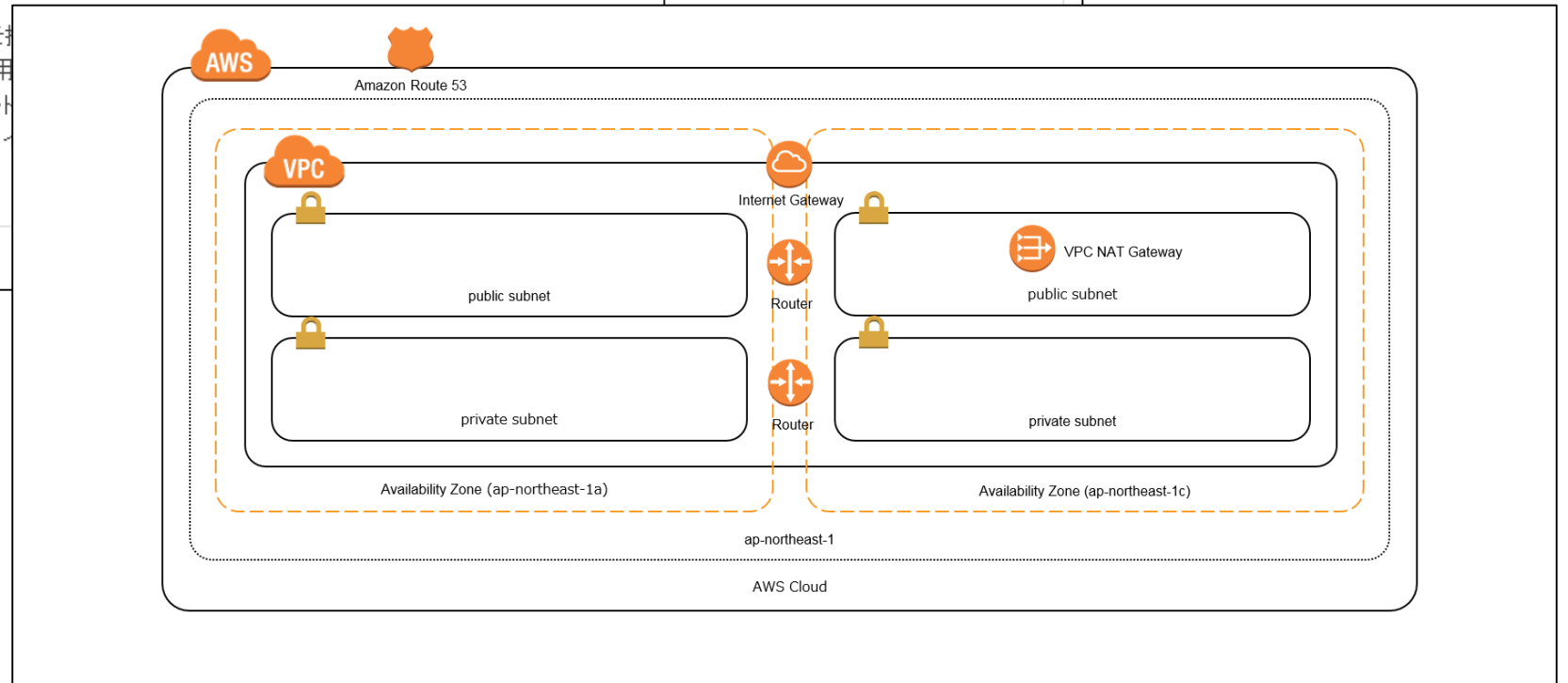
プライベートのサブネットおよびハードウェア VPN アクセスを持つ VPC

この設定は、パブリックサブネットに加えて、インスタンスにインターネットからアドレスを指定できないプライベートサブネットを追加します。プライベートサブネットのインスタンスでは、ネットワークアドレス変換 (NAT) を使用してパブリックサブネットを介してインターネットへのアウトバウンド接続を確立できます。

作成:

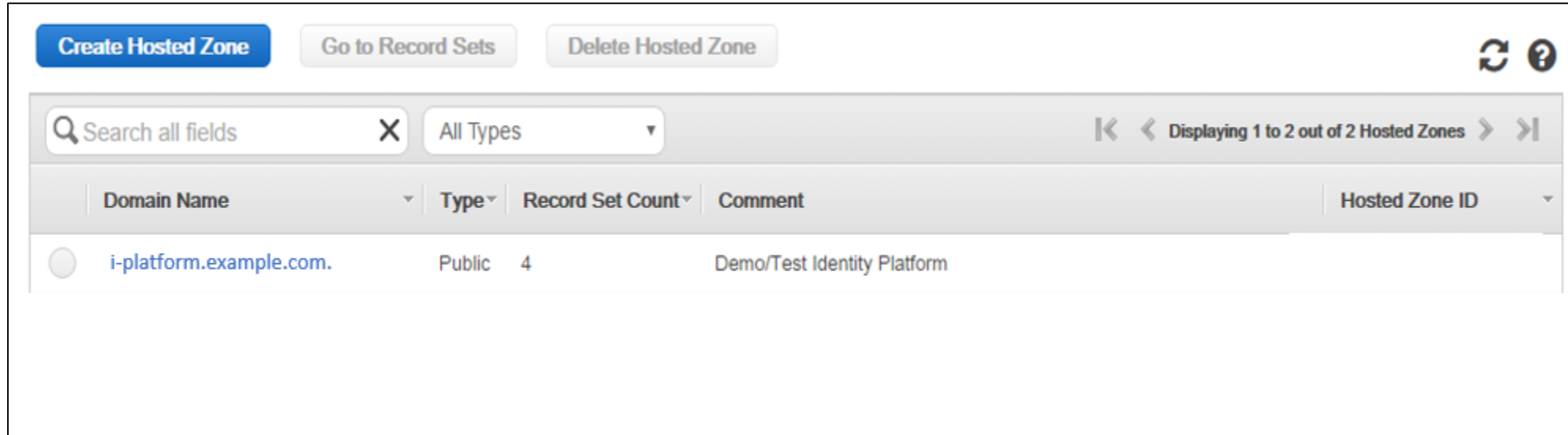
2 個の /24 サブネットを持つインスタンスは Elastic IP を使用してインターネットに接続し、ネットワークインスタンスは、ネットワークアクセスします。(NAT デバイス)

インターネット、S3、DynamoDB、SNS、SQS、その他



DNSへのドメイン設定 (Route53)

ThemiStruct Identity Platform用ドメインをRoute53に登録



The screenshot shows the AWS Route 53 console interface. At the top, there are three buttons: 'Create Hosted Zone' (highlighted in blue), 'Go to Record Sets', and 'Delete Hosted Zone'. To the right are refresh and help icons. Below the buttons is a search bar with the text 'Search all fields' and a dropdown menu set to 'All Types'. A pagination indicator shows 'Displaying 1 to 2 out of 2 Hosted Zones'. The main content is a table with the following columns: Domain Name, Type, Record Set Count, Comment, and Hosted Zone ID. One row is visible with the following data:

Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
i-platform.example.com.	Public	4	Demo/Test Identity Platform	

通知用TOPICの作成

各種通知用のSNS TOPICを作成



Amazon Simple Notific

Create new topic

A topic name will be used to create a permanent unique identifier called an Amazon Resource Name (ARN).

Topic name ⓘ

Display name ⓘ

Cancel

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
- ThemisStruct

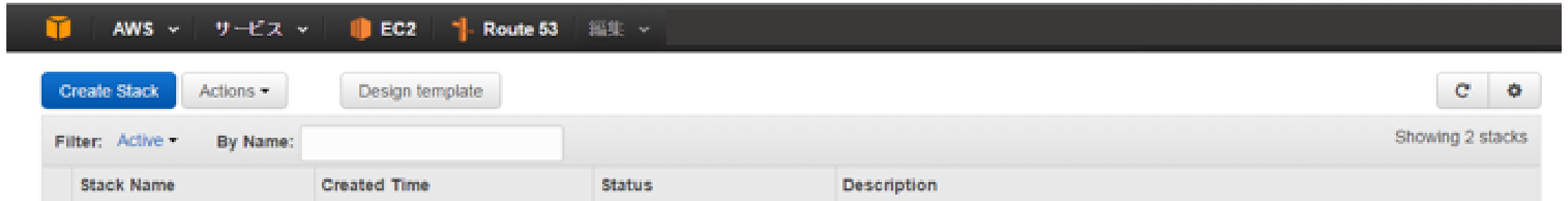
Identity Platform作成



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

Create stack

Select Template

Specify Details

Options

Review

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)

Design template

Choose a template A template is a JSON-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

Select a sample template

Upload a template to Amazon S3

ファイルを選択 identityplat...m-setup.json

Specify an Amazon S3 template URL

Cancel

Next

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

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more.](#)

Stack name

Parameters

Network Configuration

VPC

Specifies the VPC ID to launch the EC2 of the Management Console.

PublicSubnet

Specifies the Subnet ID to launch the EC2 of the Management Console.

AllowedIPAddress

Specifies the IP address(CIDR) to allow access to EC2 of the Management Console. (e.g. 192.0.2.0/24)

EC2 Instance of Management Console Configuration

SSHUserName

Specifies the ssh user name of Management Console. (e.g. operationuser)

SSHPublicKey

Specifies the public key connecting to EC2 of the Management Console via SSH.

DomainName

Specifies the domain name managed on Route 53. It's set automatically as the domain name of the Identity Platform. (e.g. example.com)

Notification Topic

Specifies the Notification Topic ARN.

CodeCommit Configuration

RepositoryAccessKey

Specifies the key of access to the software repository.

RepositorySecretKey

Specifies the secret of access to the software repository.

Other parameters

HostName

Specifies the Host Name of Management Console.

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

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more.](#)

Stack name

Parameters

Network Configuration

VPC

Specifies the VPC ID to launch the EC2 of the Management Console.

Public Subnet

Specifies the Subnet ID to launch the EC2 of the Management Console.

Allowed IP Address

Specifies the IP address(CIDR) to allow access to EC2 of the Management Console. (e.g. 192.0.2.0/24)

EC2 Instance of Management Console Configuration

SSHUserName

Specifies the ssh user name of Management Console. (e.g. operationuser)

SSHPublicKey

Specifies the public key connecting to EC2 of the Management Console via SSH.

DomainName

Specifies the domain name managed on Route 53. It's set automatically as the domain name of the Identity Platform. (e.g. example.com)

Notification Topic

Specifies the Notification Topic ARN.

CodeCommit Configuration

RepositoryAccessKey

Specifies the key of access to the software repository.

RepositorySecretKey

Specifies the secret of access to the software repository.

Other parameters

HostName

Specifies the Host Name of Management Console.

Cancel

Previous

Next

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

The screenshot shows the AWS CloudFormation console interface. At the top, there are navigation tabs for 'AWS', 'サービス', 'EC2', and 'Route 53'. Below this, there are buttons for 'Create Stack', 'Actions', and 'Design template'. A filter section shows 'Filter: Active' and 'By Name:'. The main table displays one stack: 'i-Platform-demo', created on '2016-07-27 15:29:46 UTC+0900', with a status of 'CREATE_IN_PROGRESS'. The description is 'AWS CloudFormation Template : Create Management Console of Identity Platform.'. Below the table, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', 'Stack Policy', and 'Change Sets'. The 'Events' tab is selected, showing a log entry for the stack creation event on '2016-07-27' at '15:29:46 UTC+0900' with a status of 'CREATE_IN_PROGRESS', type 'AWS::CloudFormation::Stack', logical ID 'i-Platform-demo', and status reason 'User Initiated'.

Stack Name	Created Time	Status	Description
<input checked="" type="checkbox"/> i-Platform-demo	2016-07-27 15:29:46 UTC+0900	CREATE_IN_PROGRESS	AWS CloudFormation Template : Create Management Console of Identity Platform.

2016-07-27	Status	Type	Logical ID	Status reason
▶ 15:29:46 UTC+0900	CREATE_IN_PROGRESS	AWS::CloudFormation::Stack	i-Platform-demo	User Initiated

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

The screenshot shows the 'Identity Platform' setup wizard. At the top, it says 'Identity Platform' with a logo. Below that, it says 'Identity Platformのセットアップ'. A progress bar shows 15 steps, with Step 1 highlighted in green. The steps are: Step 1: AWS情報設定, Step 2: 共通設定, Step 3: 踏み台構築, Step 4: DB構築, Step 5: DB設定, Step 6: 環境構築, Step 7: デプロイ設定, Step 8: デプロイ実行, Step 9: 証明書設定, Step 10: コンテンツ設定, Step 11: コンテンツ配置, Step 12: CDN構築, Step 13: 管理機能証明書設定, Step 14: 管理機能設定, Step 15: セットアップ完了.

Below the progress bar, the section 'AWS情報設定' is shown. It contains two input fields: 'アクセスキーID*' and 'シークレットアクセスキー*'. At the bottom, there are 'Previous' and 'Next' buttons. The footer says 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

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

The screenshot shows the 'Identity Platform' setup wizard. At the top, there is a progress bar with 15 steps. Step 2, '共通設定' (Common Settings), is highlighted in green. Below the progress bar, the title 'Identity Platformのセットアップ' is displayed. The main content area is titled '共通設定' and contains several input fields:

- 'Availability-Zone-1aのサブネットID*' (Availability-Zone-1a Subnet ID): A dropdown menu.
- 'Availability-Zone-1cのサブネットID*' (Availability-Zone-1c Subnet ID): A dropdown menu.
- 'Identity Platformのホスト名*' (Identity Platform Hostname): A text input field.
- 'DNSのHosted Zone*' (DNS Hosted Zone): A text input field.
- 'セットアップするステージ*' (Setup Stage): A text input field.
- '管理者のパスワード*' (Admin Password): A password input field.

At the bottom of the form, there are 'Previous' and 'Next' buttons. The footer contains the copyright notice: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

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

The screenshot displays the 'Identity Platform' console interface. At the top, a progress bar shows 15 steps, with Step 3, '踏み台構築' (Stepping Stone Construction), highlighted in green. Below the progress bar, the '踏み台構築' section contains several input fields:

- 踏み台として作成するEC2のAMIのID* (AMI ID for EC2 to be created as the stepping stone)
- 踏み台のホスト名* (Stepping stone host name)
- 踏み台のログインユーザ名* (Stepping stone login user name)
- SSH接続を行う公開鍵* (Public key for SSH connection)
- 接続を許可するCIDR IPアドレス* (CIDR IP address to allow connection)

Navigation buttons 'Previous' and 'Next' are visible at the bottom of the form. A copyright notice 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.' is located at the bottom right of the console.

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

Identity Platform

Identity Platformのセットアップ

1 Step 1 Step 2 Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 Step 10 Step 11 Step 12 Step 13 Step 14 Step 15

AWS情報設定 共通設定 踏み台構築 DB構築 DB設定 環境構築 デプロイ設定 デプロイ実行 証明書設定 コンテンツ設定 コンテンツ配置 CDN構築 管理機能証明書設定 管理機能設定 セットアップ完了

DB構築

複数のアベイラビリティゾーンでのレプリケーション* 使用しない 使用する

RDSのインスタンスクラス* db.r3.large

データベースの名称*

データベースのユーザー*

ユーザーのパスワード*

バックアップの保存期間*

Previous Next

Copyright © 2016 OGIS-RI Co.,Ltd. All Right Reserved.

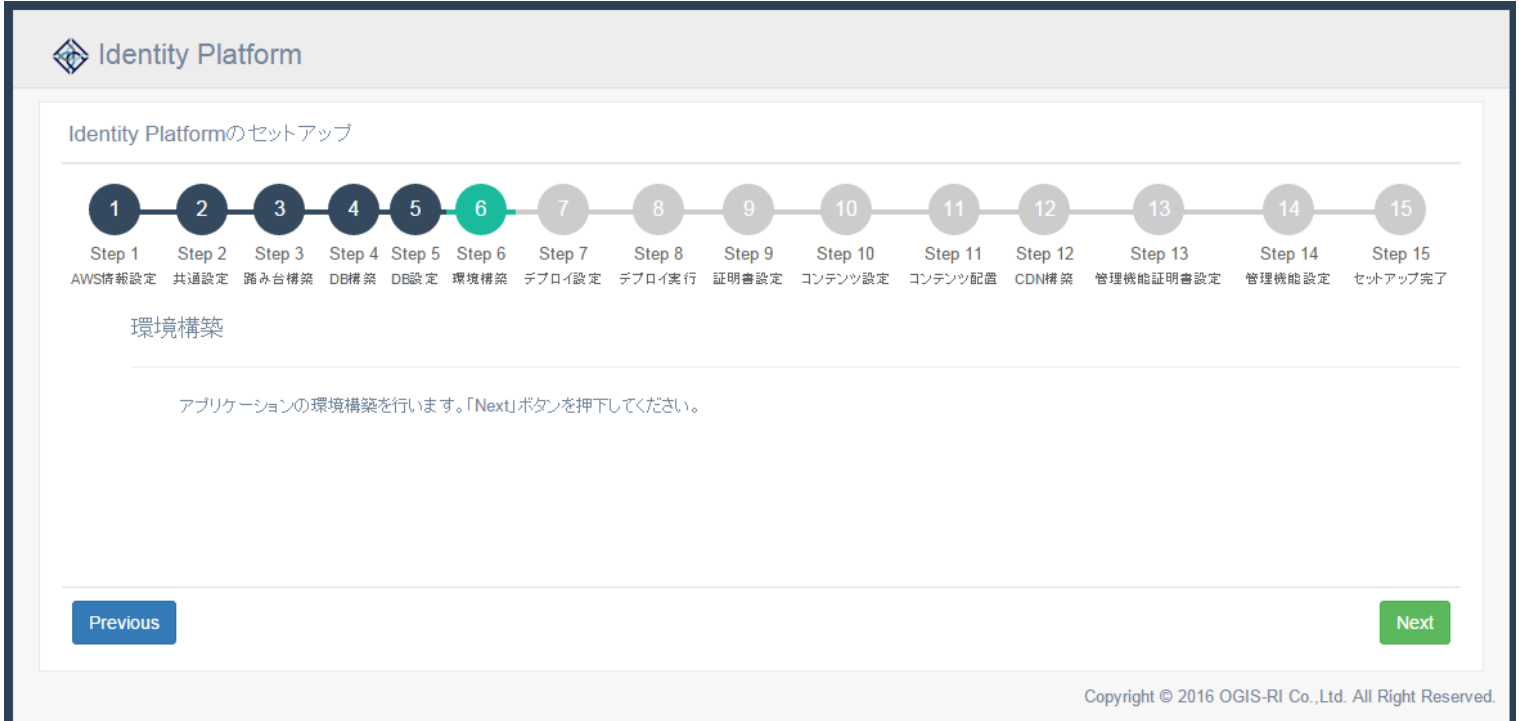
5. DB設定

「Next」をクリックするだけ

The screenshot shows the 'Identity Platform' setup wizard. At the top, it says 'Identity Platform' with a logo. Below that, it says 'Identity Platformのセットアップ'. A progress bar shows 15 steps, with Step 5 'DB設定' highlighted in green. Below the progress bar, the steps are listed: Step 1 (AWS情報設定), Step 2 (共通設定), Step 3 (踏み台構築), Step 4 (DB構築), Step 5 (DB設定), Step 6 (環境構築), Step 7 (デプロイ設定), Step 8 (デプロイ実行), Step 9 (証明書設定), Step 10 (コンテンツ設定), Step 11 (コンテンツ配置), Step 12 (CDN構築), Step 13 (管理機能証明書設定), Step 14 (管理機能設定), and Step 15 (セットアップ完了). Below the progress bar, the current step is 'DB設定'. The main content area says 'データベースの初期設定を行います。「Next」ボタンを押下してください。'. At the bottom, there are 'Previous' and 'Next' buttons. The footer says 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

6. 環境構築

「Next」をクリックするだけ



Identity Platform

Identity Platformのセットアップ

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6 Step 7 Step 8 Step 9 Step 10 Step 11 Step 12 Step 13 Step 14 Step 15

AWS情報設定 共通設定 読み台構築 DB構築 DB設定 環境構築 デプロイ設定 デプロイ実行 証明書設定 コンテンツ設定 コンテンツ配置 CDN構築 管理機能証明書設定 管理機能設定 セットアップ完了

環境構築

アプリケーションの環境構築を行います。「Next」ボタンを押下してください。

Previous Next

Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.

7. デプロイ設定

「Next」をクリックするだけ

The screenshot displays the 'Identity Platform' setup wizard. At the top, it says 'Identity Platform' with a logo. Below that, it indicates 'Identity Platformのセットアップ'. A progress bar shows 15 steps, with Step 7, 'デプロイ設定', highlighted in green. Below the progress bar, the steps are listed: Step 1 (AWS情報設定), Step 2 (共通設定), Step 3 (踏み台構築), Step 4 (DB構築), Step 5 (DB設定), Step 6 (環境構築), Step 7 (デプロイ設定), Step 8 (デプロイ実行), Step 9 (証明書設定), Step 10 (コンテンツ設定), Step 11 (コンテンツ配置), Step 12 (CDN構築), Step 13 (管理機能証明書設定), Step 14 (管理機能設定), and Step 15 (セットアップ完了). The current step, 'デプロイ設定', is expanded to show the instruction: 'アプリケーションのデプロイ設定を実施します。「Next」ボタンを押下してください。' At the bottom, there are 'Previous' and 'Next' buttons. The footer contains the copyright notice: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

8. デプロイ実行

「Next」をクリックするだけ

The screenshot displays the 'Identity Platform' setup wizard. At the top, it says 'Identity Platform' with a logo. Below that, the title is 'Identity Platformのセットアップ'. A progress bar shows 15 steps, with Step 8, 'デプロイ実行', highlighted in green. The steps are: Step 1 (AWS情報設定), Step 2 (共通設定), Step 3 (踏み台構築), Step 4 (DB構築), Step 5 (DB設定), Step 6 (環境構築), Step 7 (デプロイ設定), Step 8 (デプロイ実行), Step 9 (証明書設定), Step 10 (コンテンツ設定), Step 11 (コンテンツ配置), Step 12 (CDN構築), Step 13 (管理機能証明書設定), Step 14 (管理機能設定), and Step 15 (セットアップ完了). Below the progress bar, the section is titled 'デプロイ実行' and contains the instruction: 'アプリケーションのデプロイを実施します。「Next」ボタンを押下してください。'. At the bottom, there are 'Previous' and 'Next' buttons. The footer of the wizard says 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

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

The screenshot displays the 'Identity Platform' setup wizard. At the top, a progress bar shows 15 steps, with Step 9, '証明書設定' (Certificate Configuration), highlighted in green. Below the progress bar, the steps are listed: Step 1 (AWS情報設定), Step 2 (共通設定), Step 3 (踏み台構築), Step 4 (DB構築), Step 5 (DB設定), Step 6 (環境構築), Step 7 (デプロイ設定), Step 8 (デプロイ実行), Step 9 (証明書設定), Step 10 (コンテンツ設定), Step 11 (コンテンツ配置), Step 12 (CDN構築), Step 13 (管理機能証明書設定), Step 14 (管理機能設定), and Step 15 (セットアップ完了).

The main section is titled '証明書設定' (Certificate Configuration) and contains three file selection fields:

- Identity Platformのサーバ証明書* (select file)
- Identity Platformの証明書の秘密鍵* (select file)
- Identity Platformの中間証明書* (select file)

At the bottom, there are 'Previous' and 'Next' navigation buttons. A copyright notice at the bottom right reads: 'Copyright © 2016 OGIS-RI Co.,Ltd. All Right Reserved.'

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

The screenshot shows the 'Identity Platform' setup wizard. At the top, there is a progress bar with 15 steps. Step 10, 'コンテンツ設定' (Content Settings), is highlighted in green. Below the progress bar, the current step is titled 'コンテンツ設定'. There are two input fields: 'CloudFrontのログを格納するS3のバケット名*' and '各種コンテンツを格納するS3のバケット名*'. At the bottom, there are 'Previous' and 'Next' buttons. The footer contains the text 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

Identity Platform

Identity Platformのセットアップ

1 Step 1 AWS情報設定 2 Step 2 共通設定 3 Step 3 踏み台構築 4 Step 4 DB構築 5 Step 5 DB設定 6 Step 6 環境構築 7 Step 7 デプロイ設定 8 Step 8 デプロイ実行 9 Step 9 証明書設定 10 Step 10 コンテンツ設定 11 Step 11 コンテンツ配置 12 Step 12 CDN構築 13 Step 13 管理機能証明書設定 14 Step 14 管理機能設定 15 Step 15 セットアップ完了

コンテンツ設定

CloudFrontのログを格納するS3のバケット名*

各種コンテンツを格納するS3のバケット名*

Previous Next

Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.

11. コンテンツ配置

「Next」をクリックするだけ

The screenshot displays the 'Identity Platform' setup wizard. At the top, it says 'Identity Platformのセットアップ'. Below this is a progress bar with 15 steps. Step 11, 'コンテンツ配置', is highlighted in green, indicating the current step. The steps are: Step 1 (AWS情報設定), Step 2 (共通設定), Step 3 (踏み台構築), Step 4 (DB構築), Step 5 (DB設定), Step 6 (環境構築), Step 7 (デプロイ設定), Step 8 (デプロイ実行), Step 9 (証明書設定), Step 10 (コンテンツ設定), Step 11 (コンテンツ配置), Step 12 (CDN構築), Step 13 (管理機能証明書設定), Step 14 (管理機能設定), and Step 15 (セットアップ完了). Below the progress bar, the section is titled 'コンテンツ配置' and contains the instruction: 'コンテンツのアップロードを実施します。「Next」ボタンを押下してください。'. At the bottom, there are 'Previous' and 'Next' buttons. The footer of the wizard reads 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

12. CDN構築

「Next」をクリックするだけ

The screenshot shows the 'Identity Platform' setup wizard. At the top, it says 'Identity Platformのセットアップ'. Below this is a progress bar with 15 steps. Step 12, 'CDN構築', is highlighted in green. The steps are: Step 1 (AWS情報設定), Step 2 (共通設定), Step 3 (踏み台構築), Step 4 (DB構築), Step 5 (DB設定), Step 6 (環境構築), Step 7 (デプロイ設定), Step 8 (デプロイ実行), Step 9 (証明書設定), Step 10 (コンテンツ設定), Step 11 (コンテンツ配置), Step 12 (CDN構築), Step 13 (管理機能証明書設定), Step 14 (管理機能設定), and Step 15 (セットアップ完了). Below the progress bar, the title 'CDN構築' is displayed. The main content area contains the instruction: 'コンテンツデリバリーネットワークの構築を行います。「Next」ボタンを押下してください。' At the bottom, there are 'Previous' and 'Next' buttons. The footer of the wizard says 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

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

The screenshot displays the 'Identity Platform' setup wizard. At the top, there is a progress bar with 15 steps. Step 13, '管理機能証明書設定' (Management Console Certificate Configuration), is highlighted in green. Below the progress bar, the title '管理機能証明書設定' is shown. The main content area contains three file selection fields, each with a 'select file' button and a folder icon:

- Management Consoleのサーバ証明書
- Management Consoleの証明書の秘密鍵
- Management Consoleの中間証明書

At the bottom of the wizard, there are 'Previous' and 'Next' buttons. The footer contains the text: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

14. 管理機能設定

「Next」をクリックするだけ



The screenshot shows the Identity Platform setup wizard interface. At the top, it says "Identity Platform" with a logo. Below that, it says "Identity Platformのセットアップ". A progress bar consists of 15 numbered steps. Step 14, "管理機能設定", is highlighted in green, indicating the current step. The other steps are: Step 1 (AWS情報設定), Step 2 (共通設定), Step 3 (踏み台構築), Step 4 (DB構築), Step 5 (DB設定), Step 6 (環境構築), Step 7 (デプロイ設定), Step 8 (デプロイ実行), Step 9 (証明書設定), Step 10 (コンテンツ設定), Step 11 (コンテンツ配置), Step 12 (CDN構築), Step 13 (管理機能証明書設定), and Step 15 (セットアップ完了). Below the progress bar, the title "管理機能設定" is displayed. Underneath, there is a text instruction: "管理コンソールの設定を行います。「Next」ボタンを押下してください。". At the bottom of the wizard, there are two buttons: "Previous" (disabled) and "Next" (active). The footer of the page contains the text "Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved."

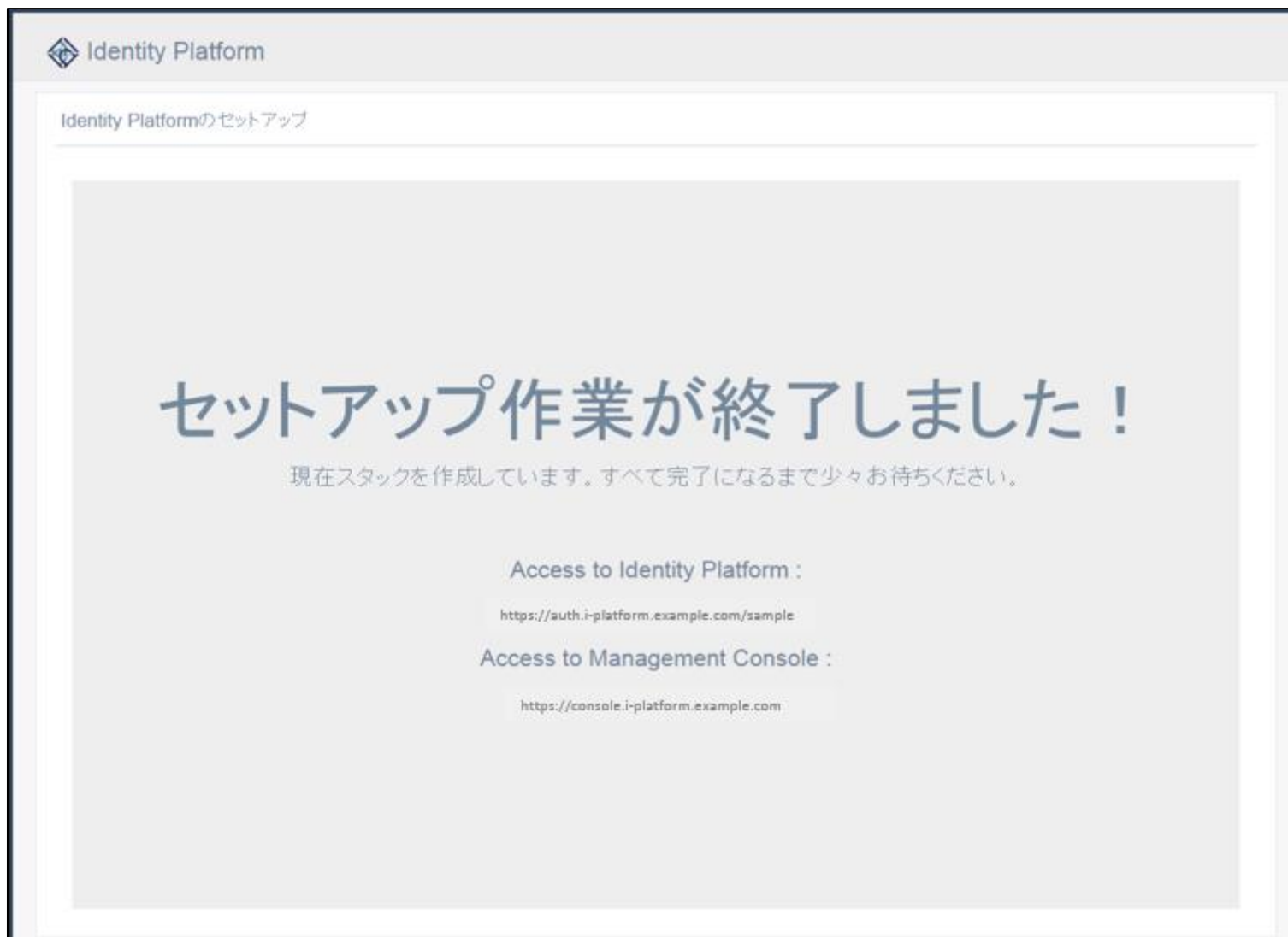
15. 管理コンソールの再起動

「再起動」をクリックするだけ

The screenshot shows the 'Identity Platform' setup progress bar. It consists of 15 numbered steps, each with a corresponding label below it. Step 15, 'セットアップ完了' (Setup Complete), is highlighted in green, indicating that the setup is finished. Below the progress bar, the text 'セットアップ完了' (Setup Complete) is displayed. A large red button labeled '再起動' (Restart) is centered on the screen, with the instruction '管理コンソールを再起動します。' (Restart the management console.) above it. A 'Previous' button is visible at the bottom left of the progress bar area. The footer of the screenshot contains the copyright notice: 'Copyright © 2016 OGIS-RI Co., Ltd. All Right Reserved.'

Step	Label
1	Step 1 AWS情報設定
2	Step 2 共通設定
3	Step 3 読み台構築
4	Step 4 DB構築
5	Step 5 DB設定
6	Step 6 環境構築
7	Step 7 デプロイ設定
8	Step 8 デプロイ実行
9	Step 9 証明書設定
10	Step 10 コンテンツ設定
11	Step 11 コンテンツ配置
12	Step 12 CDN構築
13	Step 13 管理機能証明書設定
14	Step 14 管理機能設定
15	Step 15 セットアップ完了

セットアップ完了



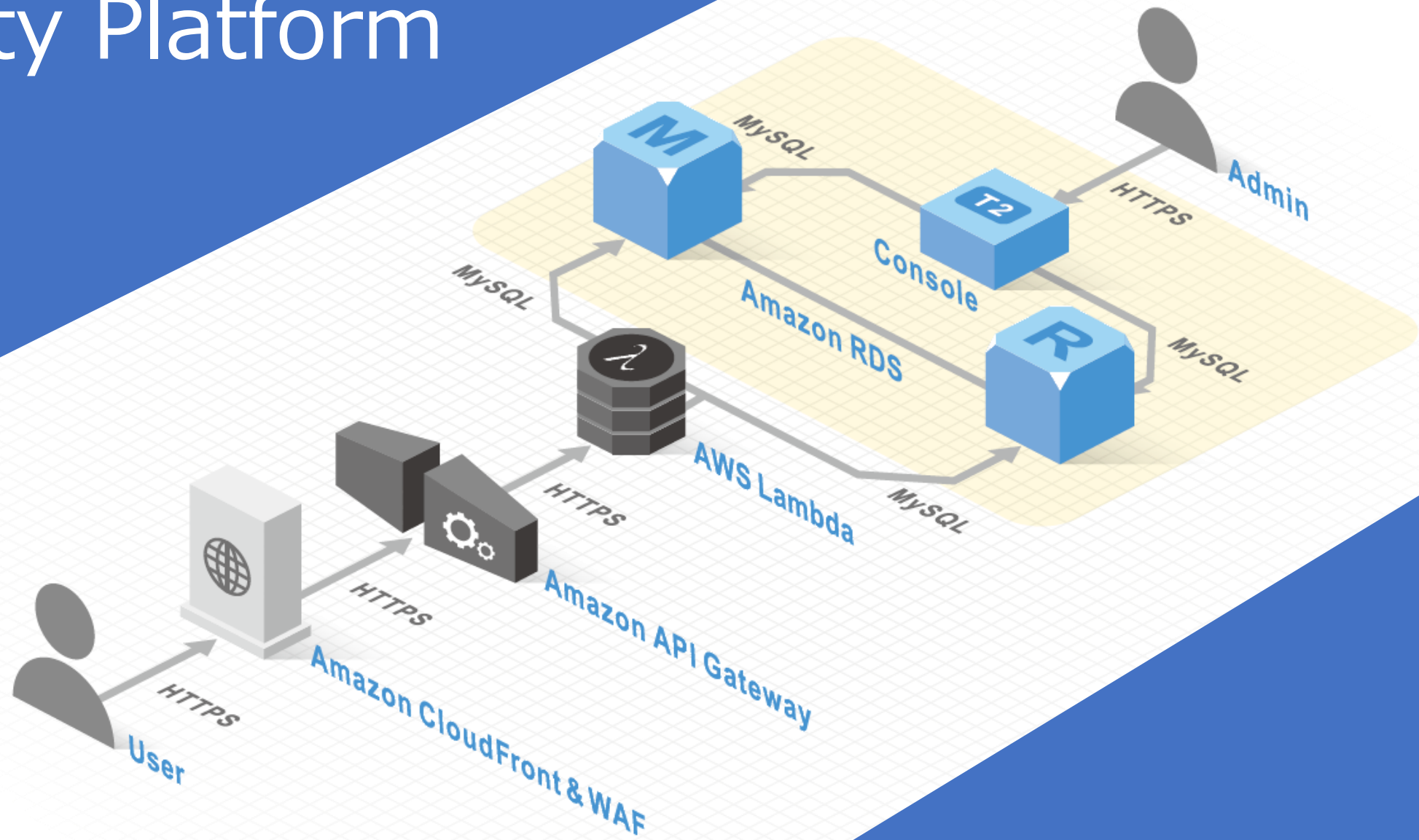
The screenshot shows a web interface for Identity Platform. At the top left, there is a logo and the text "Identity Platform". Below that, the page title is "Identity Platformのセットアップ". The main content area has a large heading "セットアップ作業が終了しました！" (Setup work is completed!) and a sub-heading "現在スタックを作成しています。すべて完了になるまで少々お待ちください。" (We are currently creating the stack. Please wait a little while until everything is completed). Below this, there are two sections: "Access to Identity Platform :" with the URL <https://auth.i-platform.example.com/sample>, and "Access to Management Console :" with the URL <https://console.i-platform.example.com>.

まず認証基盤できた！



 ThemisStruct デモストラクト
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

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/>

tsipadmin

Administrator

 Home

 User

 Authentication 

 Federation 

 Application 

 Global Config 

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

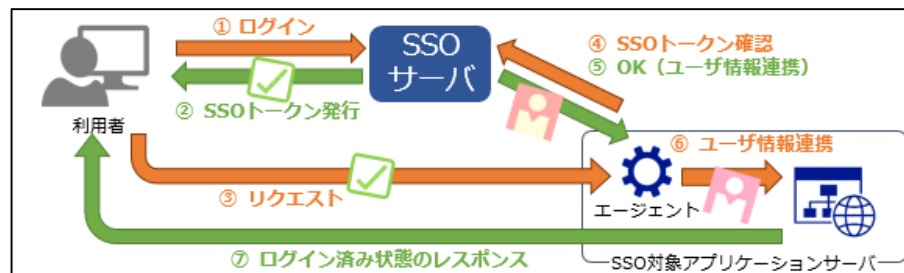


クラウドサービス

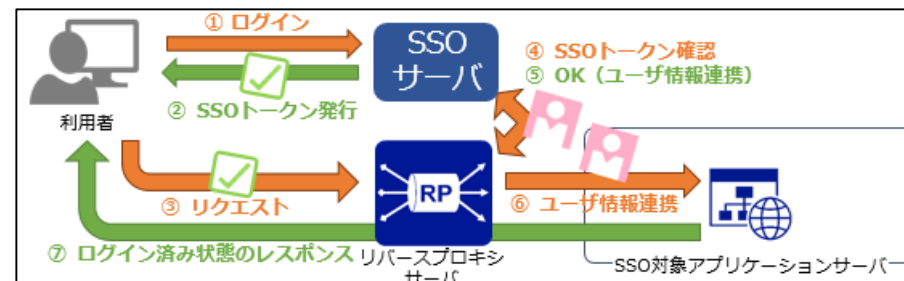
Office 365

盛り付け方は3パターンをご用意

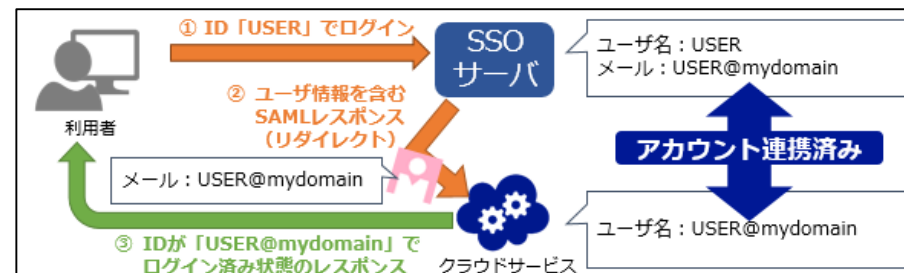
□ エージェントによる接続



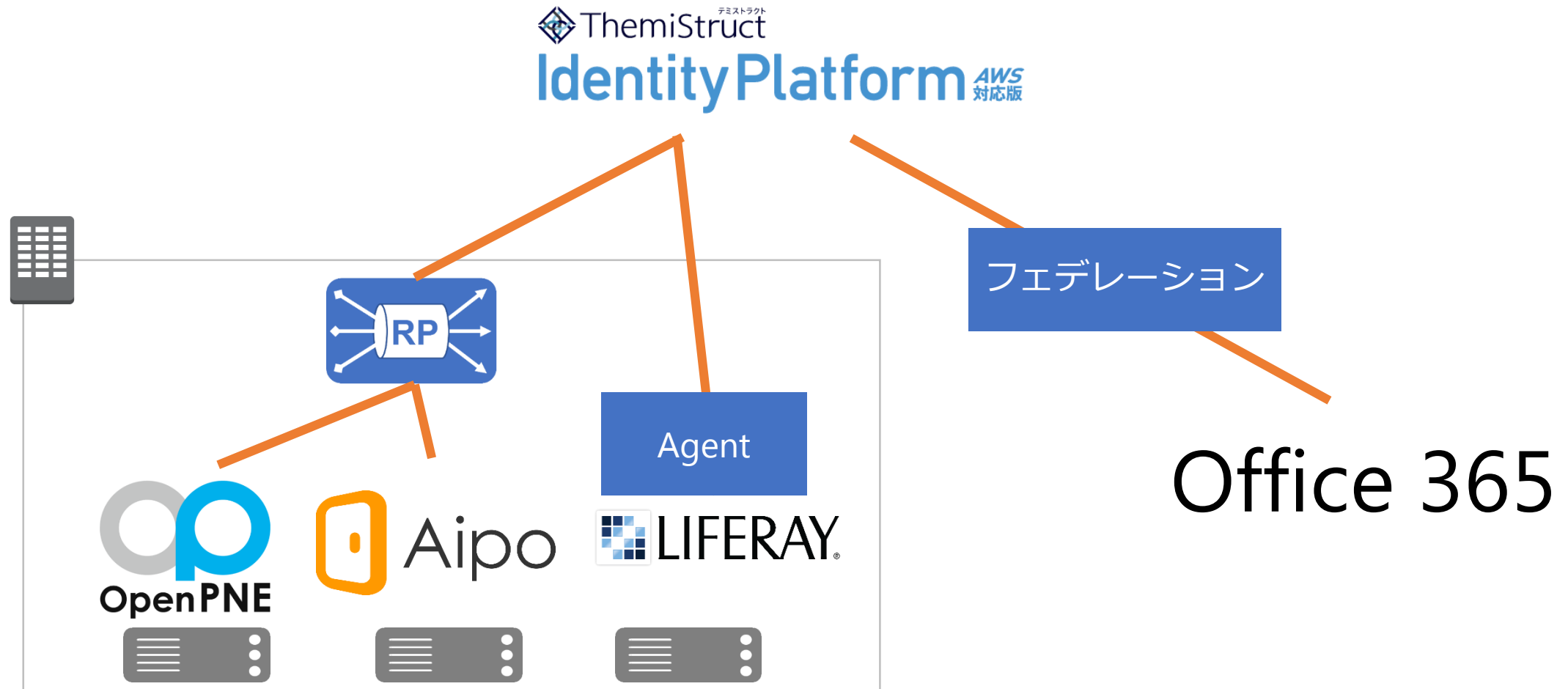
□ リバースプロキシによる接続



□ 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. ThemisStruct Identity Platformへのアプリ登録

The image displays two screenshots of the ThemisStruct Identity Platform client registration interface. The top screenshot shows the 'Client Registration' progress bar with step 1 (Client) active and step 2 (Response) pending. Below it, the 'Client Info' form is visible, containing fields for 'Application Name*' (Name of Application) and 'Description'. The bottom screenshot shows the 'Client Registration' progress bar with step 1 (Client) completed and step 2 (Response) active. Below it, the 'Response Info' form is visible, containing fields for 'Redirect URI*' (https://ipdev.example.com) and 'Application URI*' (https://ipdev.example.com).

Client Registration

1 Client Step 1 : Client Info

2 Response Step 2 : Response Info

Client Info

Application Name*

Description

Client Registration

1 Client Step 1 : Client Info

2 Response Step 2 : Response Info

Response Info

Redirect URI*

Application URI*

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、

The screenshot displays the ThemiStruct Identity Platform management interface. On the left is a navigation menu with the following items: Administrator, Home, User, Authentication, Federation, Application, and Global Config. The main content area is titled 'Application' and shows a list of SaaS applications, with 'Office 365' selected. Below the application list, a progress indicator shows three steps: 1 (ID), 2 (SP Information), and 3 (Application Setting). The 'ID' step is highlighted in green, and the 'SP Information' step is also highlighted in green. The 'Application Setting' step is currently greyed out. Below the progress indicator, the 'ID' field is set to 'o365'. The 'Key and Certificate' section is visible, showing the following configuration:

Field	Value
Audience	urn:federation:MicrosoftOnline
Destination	https://login.microsoftonline.com/login.srf
Name ID Format	urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
ACR	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordP
Attribute	{"IDPEmail": "email"}

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。

The screenshot shows a three-step wizard for Office 365 connection. Step 1 (ID) and Step 2 (SP Information) are completed. Step 3 (Application Setting) is the current step, titled "Office 365の連携設定を続けて下さい".

Office 365の連携設定を続けて下さい

Windowsクライアントに以下の4つのプログラムをインストール

- Microsoft Online Services Sign-In Assistant for IT Professionals
- Azure Active Directory Module for Windows PowerShell
- SharePoint Online Management Shell
- Windows PowerShell Module for Skype for Business Online

PowerShellコマンドプロンプト上で、以下のコマンドを実行促されますので、Office 365の管理者アカウントのIDとパスワードを入力してください。

```
$msolcred = get-credential
connect-msolservice -credential $msolcred
```

続いて、以下のコマンドを実行し、Office 365との連携設定を有効化します。

```
$dom = "demo.example.com" //Office 365に登録しているドメイン名
$entity = "https://themistruct.example.com:443/prod" //Office 365のエンティティ (必ず https:// を含む)
$url = "https://themistruct.example.com:443/prod/saml" //Office 365のSAML認可エンドポイント
$logon = "https://themistruct.example.com:443/v1/saml" //Office 365のSAMLサインアウトエンドポイント (未対応)
$secp = "https://themistruct.example.com:443/v1/saml" //Office 365のSAMLサインアウトエンドポイント (未対応)
$scert = "MII ... (省略) ... Q=" //Identity Platformの証明書
```

以下のコマンドを実行し、Office 365との連携設定を有効化します。

```
Set-MsolDomainAuthentication -DomainName $dom -FederationBrandName $dom -Authentication Federated
-PassiveLogonUri $url -SigningCertificate $cert -IssuerUri $entity -ActiveLogonUri $secp -LogOffUri $logon -PreferredAuthenticationProtocol SAML
```

各種Officeクライアントアプリケーションを使用する場合、以下のコマンドを実行し、連携設定を有効化します。

```
$sessionEO = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $msolcred -Authentication Basic -AllowRedirection
Import-PSSession $sessionEO
Set-OrganizationConfig -OAuth2ClientProfileEnabled:$true
$sessionS48 = New-CsOnlineSession -Credential $credential
Import-PSSession $sessionS48
Set-CsOauthConfiguration -ClientAdalAuthOverride Allowed
```

最後に以下のコマンドを実行し、サンプルユーザーを作成します。事前にIdentity Platform上に「UserID」が「testuser」、メールアドレスが「testuser@demo.example.com」のプロフィール情報を持ったユーザーアカウントが作成されているとします。

```
$mail = "testuser@demo.example.com"
$uid = "testuser"
New-MsolUser -UserPrincipalName $mail -DisplayName $uid -ImmutableId $uid
Set-MsolUser -UserPrincipalName $mail -UsageLocation JP
Set-MsolUserLicense -UserPrincipalName $mail -AddLicenses tsipstest:0365_BUSINESS_PREMIUM
```

以上で、Office 365との連携設定が完了となります。

Buttons: Previous, Finish, Cancel

できた！

Office 365

 ThemisStruct デミストラクト

Identity Platform AWS 対応版


OpenPNE

 Aipo

 LIFERAY®

第 4 章

見味の基盤認証

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SSSO

味見 2

Office 365 利用

お召し上がりください



ThemiStruct Identity Platformご紹介



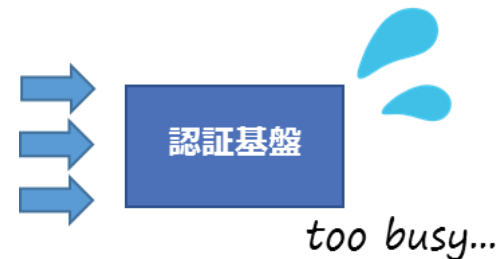
- ✓ AWSネイティブな
アイデンティティ連携基盤
- ✓ ≠OpenAM
- ✓ ≠OpenIDM
- ✓ オージス総研自社商品



これからの認証プラットフォームに求められること

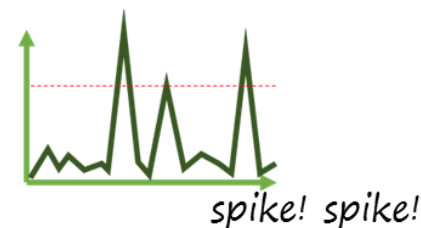
膨大なトラフィック量への対応

- 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



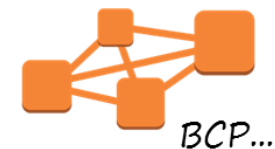
スパイクアクセスへの対応

- 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

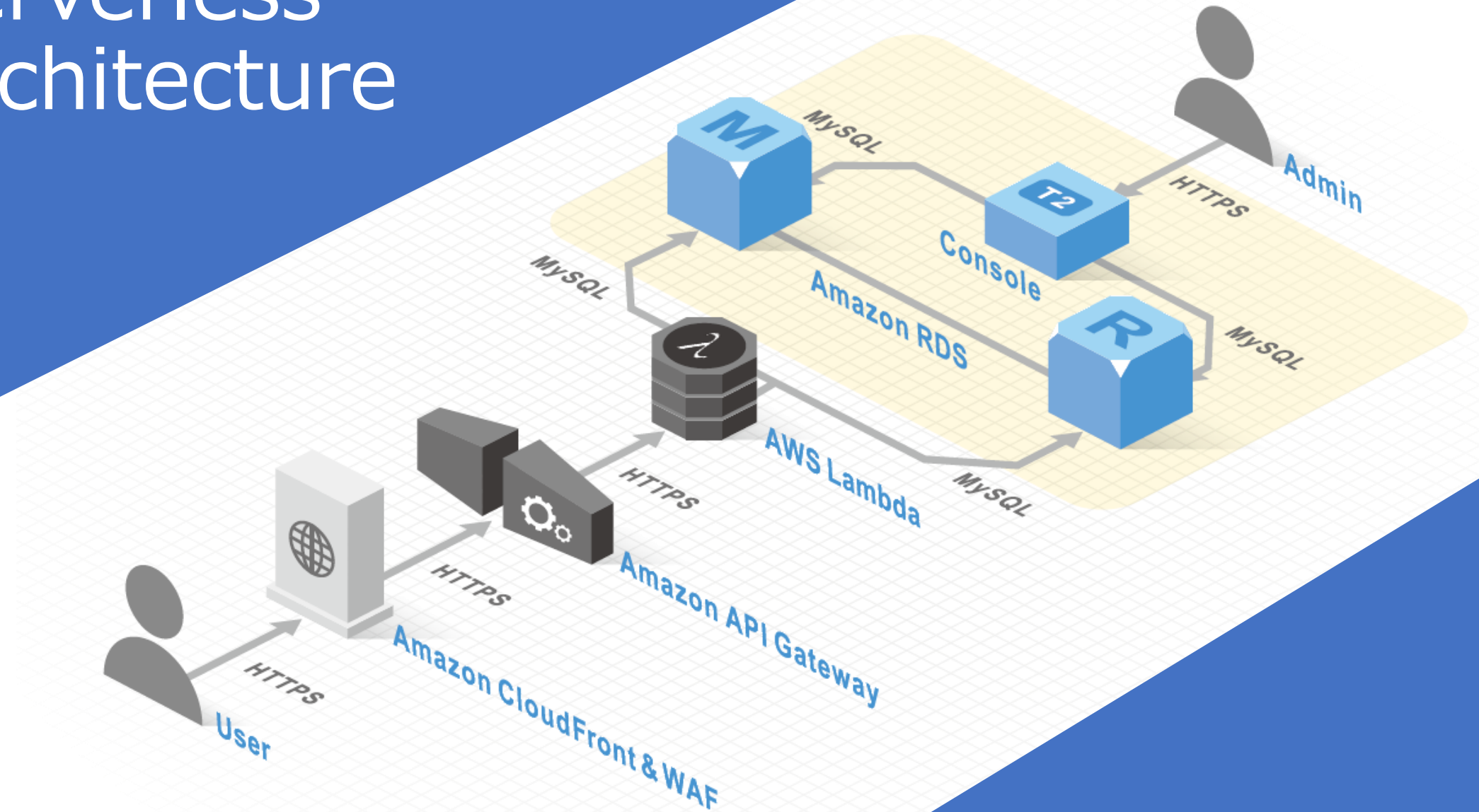
AWSネイティブなアーキテクチャにより下記の恩恵を享受

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

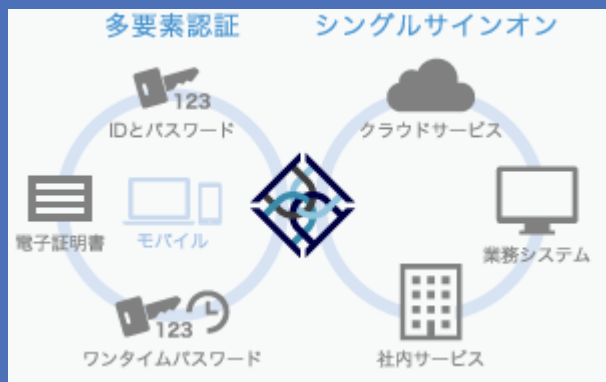


ThemiStruct Identity Platformの特徴



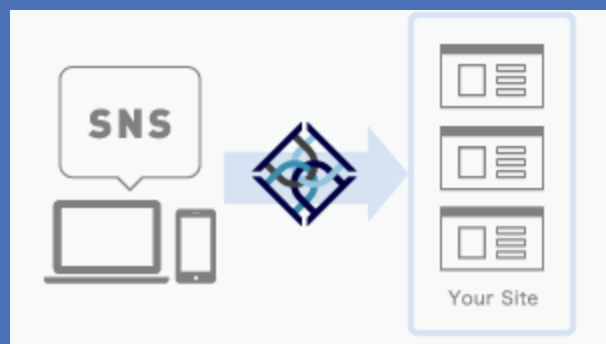
認証システムの短期導入が可能

ThemiStruct Identity Platformはクラウド上に設置され、短時間で従業員、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

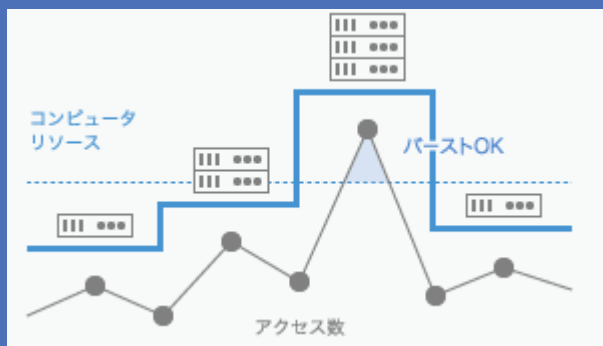
FacebookやGoogleなどのユーザが普段使っているSNSやWebサービスのアカウントを利用して、気軽にユーザ登録が可能です。サイトへの新規ユーザ登録率、ユーザビリティ、コンバージョン率を向上させます。ユーザ自身による登録や、管理者による一括登録も可能です。

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上にパッと作ってサッ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

ASK US



ThemisStruct
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



本資料に掲載されている会社名、製品名は各社の登録商標または商標です。