オージス総研の ThemiStruct Identity Platform が OpenID Certified になった話

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

八幡 孝

自己紹介

八幡 孝 （やはた たかし）

- 株式会社オージス総研
- テミストラクト関連サービス 東日本エリア責任者
- テミストラクト商品開発 リードアーキテクト

- OpenAMコンソーシアム 理事
- OpenIDファウンデーション・ジャパン
  Enterprise Identity WG リーダー

- twitter.com/paoneJP
- facebook.com/takashi.yahata
- https://paonejp.github.io
- OpenID, OAuth, SCIM, Python, OpenAM, OpenIDM, …

統合認証ソリューション ThemiStruct を提供しています

ThemiStruct-WAM

シングルサインオン
認証基盤ソリューション

ThemiStruct-IDM

ID管理ソリューション

ThemiStruct-CM

電子証明書発行・管理
ソリューション

ワンタイムパスワードソリューション

ThemiStruct-OTP

システム監視ソリューション

ThemiStruct-MONITOR

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

クラウド、IoT時代の
“All in one”
認証プラットフォーム

OIDF-J EIWGでガイドライン文書を執筆・公開しています。

OpenID Japan

OIDF-Jについて | お知らせ

News 資料公開

Enterprise Identity WGが『OpenID ConnectとSCIMのエンタープライズ利用ガイドライン』と『(同)実装ガイドライン』を公開

By staff | 2016年03月28日

一般社団法人OpenIDファウンデーション・ジャパン(代表理事:楠 正憲)のワーキンググループであるEnterprise Identity WG「以下、EIWG」は、エンタープライズIT市場において、OpenID Connect(※1)やSCIM(※2)などの仕様をベースとした、IDフェデレーションやIDプロビジョニングの普及を推進し、その過程を通して新たなビジネスの創造・展開を図ることを目的として2012年に発足いたしました。

2013年12月20日に「OpenID ConnectとSCIMのエンタープライズ利用ガイドライン」を公開しましたが、その後もガイドラインの改訂及び検討を続け、利用ガイドラインと実装ガイドラインの2つへと再構成し、本日2016年3月28日に公開いたしました。

ガイドラインのダウンロードはこちら ➡ j.mp/eiwg-guides-2016

https://openid.or.jp/news/2016/03/eiwg-guideline.html

OIDF-J EIWG はフェーズ３の活動へ

OpenID Japan

News

Enterprise Identity WG フェーズ3活動開始と参加企業募集について

By staff | 2016年07月19日

2012年より活動してきたEnterprise Identity WG（EIWG）ですが 、2016年8月1日よりフェーズ3の活動を開始いたします。

活動開始にあたり、WGに参加される会員企業様を募集いたしますので、以下ご確認の上、参加希望の方は本メールにご返信ください。

なお、参加するにはOpenIDファウンデーション・ジャパンの会員企業の従業員であることが条件に含まれております。この機会に会員企業への申し込みについてもご検討いただけると幸いです。

どうぞよろしくお願いします。

- 活動の背景
  - 海外のSaaS, IDaaSを中心にOpenID Connect, SCIMによるID連携の実装、機能提供が始まっており、今後急速に広がると予想されます。そうした動きの下、企業ではクラウドサービスの活用、相互接続のために OpenID Connect, SCIMによるID連携に対応することが必須となるとともに、同技術をAPI活用や、取引先とのシステム連携、社内IT向けのID基盤などにも広く適用していくことが求められるようになると考えられます。

https://openid.or.jp/news/2016/07/enterprise-identity-wg-3.html

エンプラ向けユースケースを対象にプロファイル作りを実施中。

活動の目的

クラウド連携にとどまらず、エンタープライズITでのID連携ユースケースを整理し、それぞれのユースケースにおけるOpenID Connect, SCIMの適用 の考え方、課題、プラクティスを整理する。

特に公開済みの実装ガイドでも議論となったOpenID ConnectとSCIMを相互運用する際の識別子マッピング方式は、各ユースケース毎に検討が必要となると予想され、重点検討課題とする。

今日のお話

OpenID Certified になりました。

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

http://openid.net/certification/

オージス総研の ThemiStruct Identity Platform は OpenID Connect™ プロトコルの OP Basic, OP Implicit, OP Config の3つのプロファイルに適合した OpenID Certified™ 実装です。

ところで
ThemiStruct Identity Platform
って何なん？

統合認証ソリューション ThemiStruct を提供しています

ThemiStruct-WAM

シングルサインオン
認証基盤ソリューション

ThemiStruct-IDM

ID管理ソリューション

ThemiStruct-CM

電子証明書発行・管理
ソリューション

ワンタイムパスワードソリューション

ThemiStruct-OTP

システム監視ソリューション

ThemiStruct-MONITOR

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

クラウド、IoT時代の
“All in one”
認証プラットフォーム

統合認証ソリューションに取り組んで15年

- 2001年ごろから基盤部門で
- セキュリティソリューションの一環として
- 2005年からはオープンソースソフトウェアをベースに開発をし
- 2009年からThemiStructブランドを立ち上げて
- 2013年からは専門部隊として
- 気がつけば今年15周年

認証基盤を作るメリット

① 利用者が便利になる

- 作業効率の向上
- IT活用の促進

② セキュリティレベルのばらつきがなくなる

- 開発者に依存したばらつき
- ユーザーに依存したばらつき

③ システム開発がしやすい

- アプリ毎の認証機能開発は不要
- サブシステムに分割した開発の実現

④ 認証方式の変更がやりやすい

- ID/パスワードを使った認証
- 多要素認証への対応
- 新しい方式への対応

セキュリティのための認証基盤

認証基盤のユースケースが拡大

ユースケース	狙い・特長
社内システム利用のガバナンス強化	認証処理の一元化、人事システム等と連動したタイムリーなIDメンテナンス。
取引先へのシステム提供	取引先ユーザーの確実な認証。IPアドレスや電子証明書の併用。
クラウドサービス利用時、スマホ・タブレット利用時の認証強化	社外からの利用の制限。社外での利用時の追加の認証の実施。社用端末の識別。 クラウドサービスのIDメンテナンス。
顧客（一般消費者）向けの情報提供、サービス提供	SSOによる顧客への利便性の提供。複数アプリへの展開。収集した属性の活用。 他社サービスとの連携。

“Identity is the new perimeter.”

ロ ネットワーク型の境界防御が効かない時代になった

- 守るべき情報資産は壁 (Firewall) の外にある
- アクセスする主体は壁の中にも外にもいる

ロ アイデンティティを用いた情報へのアクセス管理が重要に

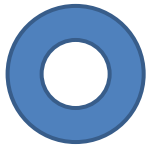
- アイデンティティによるアクセスの制御
- アイデンティティによるアクセスの監視

セキュリティのための認証基盤

ロ 情報セキュリティの3要素（CIA）

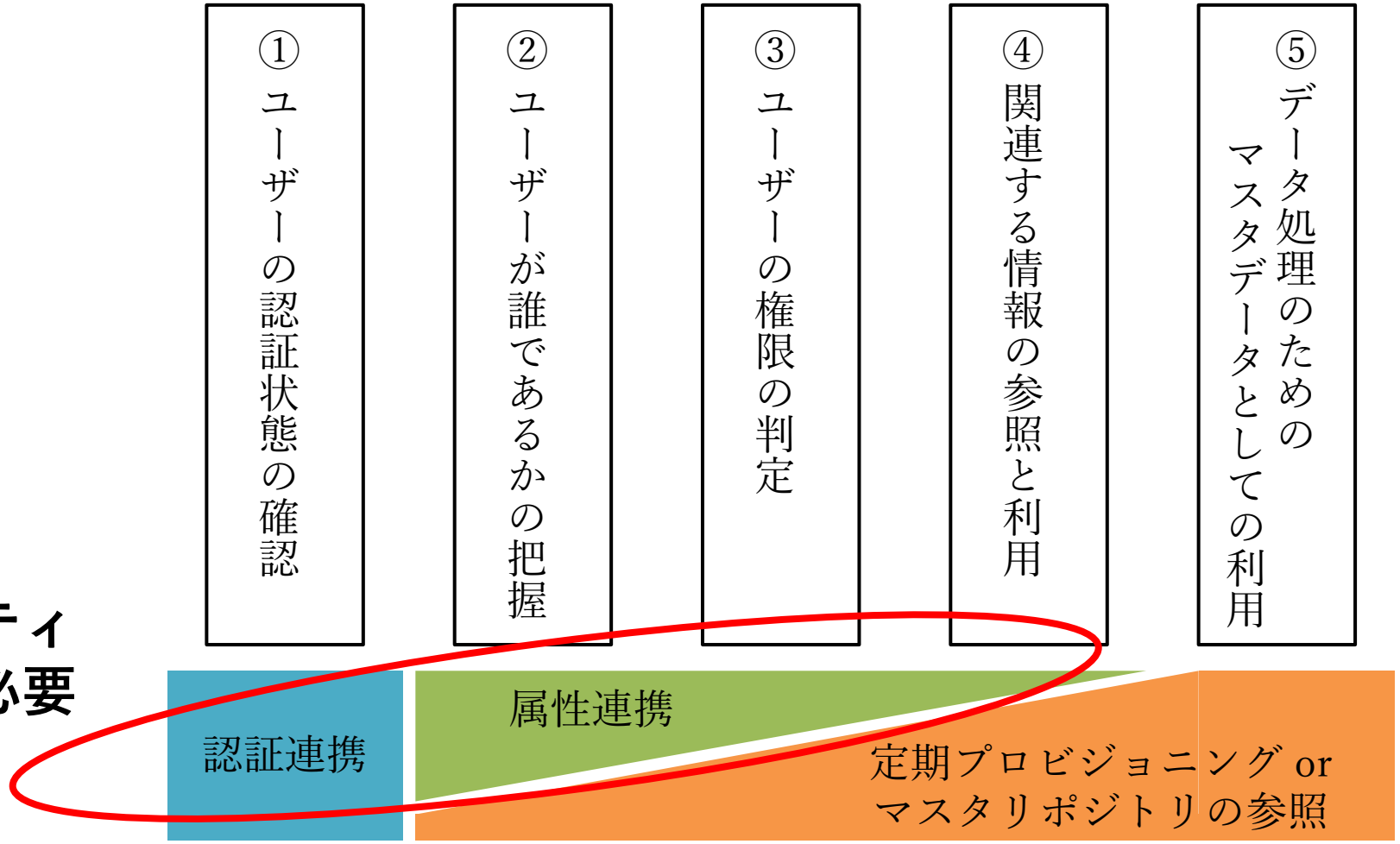
- 機密性: Confidentiality
- 完全性: Integrity
- 可用性: Availability ➡ 本当は最も優先されるべき要素

利用を制限するための認証基盤



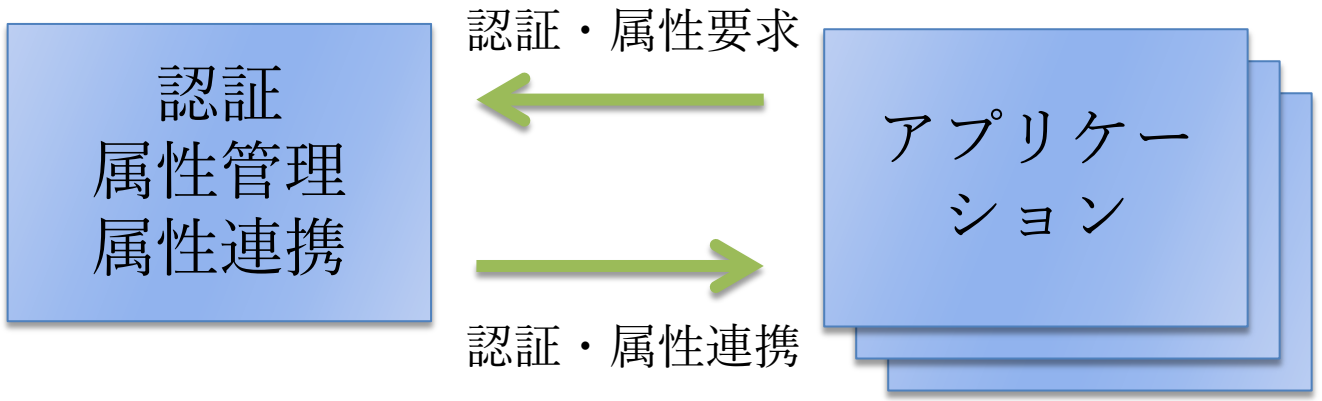
クラウド、デバイス、サービスを活用してもらうための認証基盤

アプリケーションに必要な情報を提供する方法



アイデンティティ連携の技術が必要

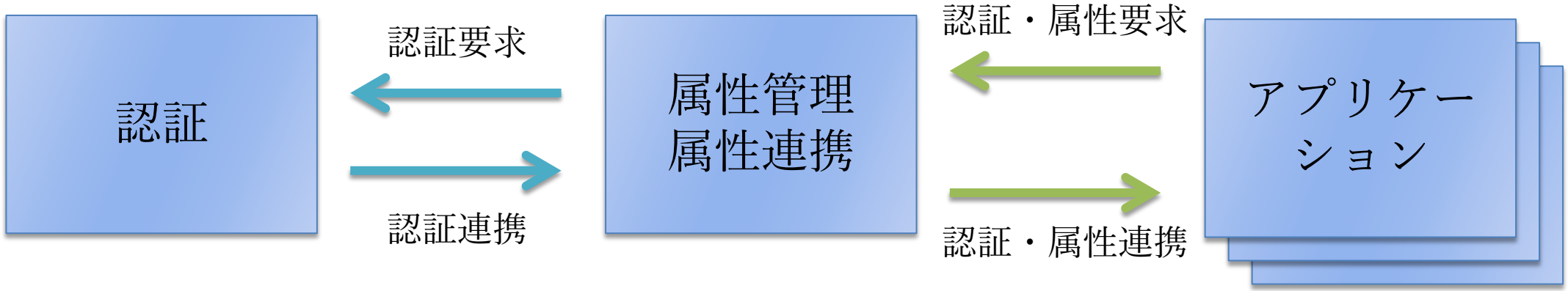
認証基盤を作る・サービスを展開する



ユーザーの認証
アプリが必要とする
属性の管理、提供、記録

ユーザーごとに
最適化された
サービスを提供

外部IdP活用で、より使いやすく、より管理しやすく



外部の信頼できる
認証システム(IdP)を利用

ドメインログオン、
Google, Facebook, Yahoo! JAPAN ID, ...

アプリが必要とする
属性の管理、提供、記録

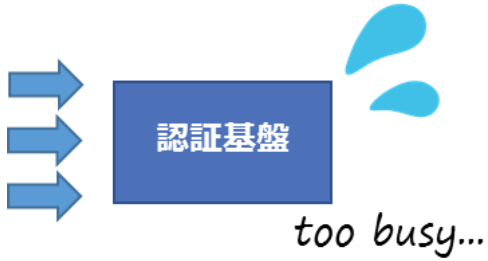
ユーザーごとに
最適化された
サービスを提供

認証基盤 から
アイデンティティプラットフォーム へ

おのずと「非機能要求」のレベルもアップ

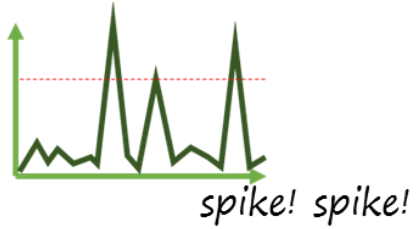
膨大なトラフィック

- 認証基盤の役割増加
- 提供するサービス・システムの増加
- ユーザー数・デバイス数の増加
- API利用の増加



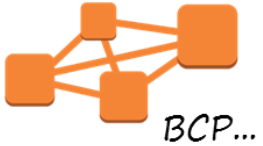
スパイクアクセス

- 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



システム停止を回避

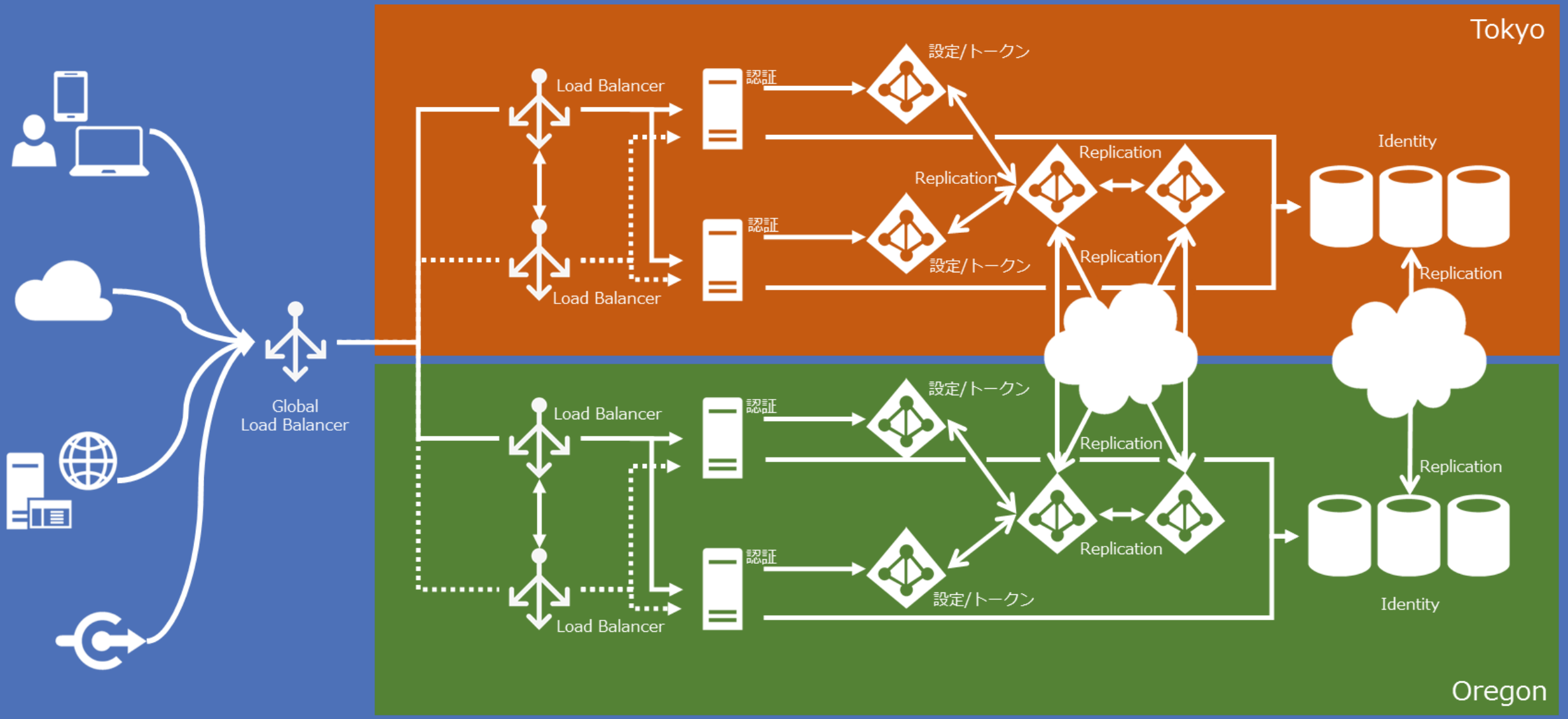
- 認証基盤役割の増加に伴い、システム停止や遅延による機会損失が大きくなり、事業継続性や機会損失回避など可用性要求のレベルが格段にUPした



スピードスタート・スモールスタート

- 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

これまで： 高度な基盤設計。入念な可用性、性能のテスト。プロジェクトの巨大化。



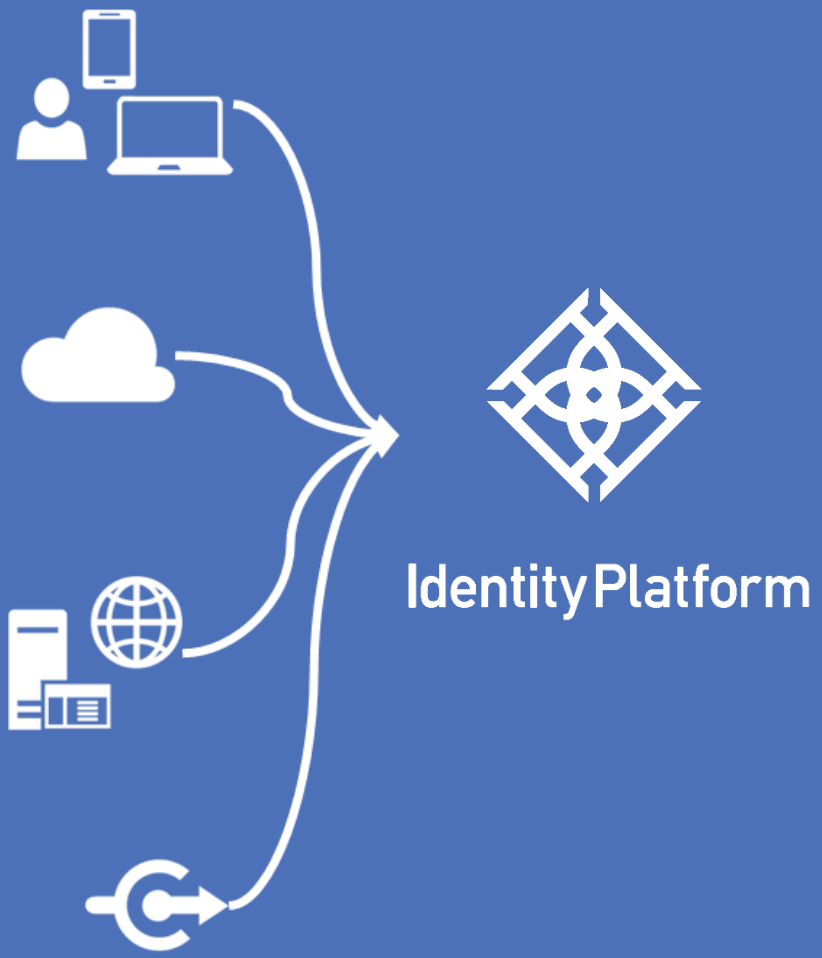
当社のアプローチ

ThemiStruct テミストラクト

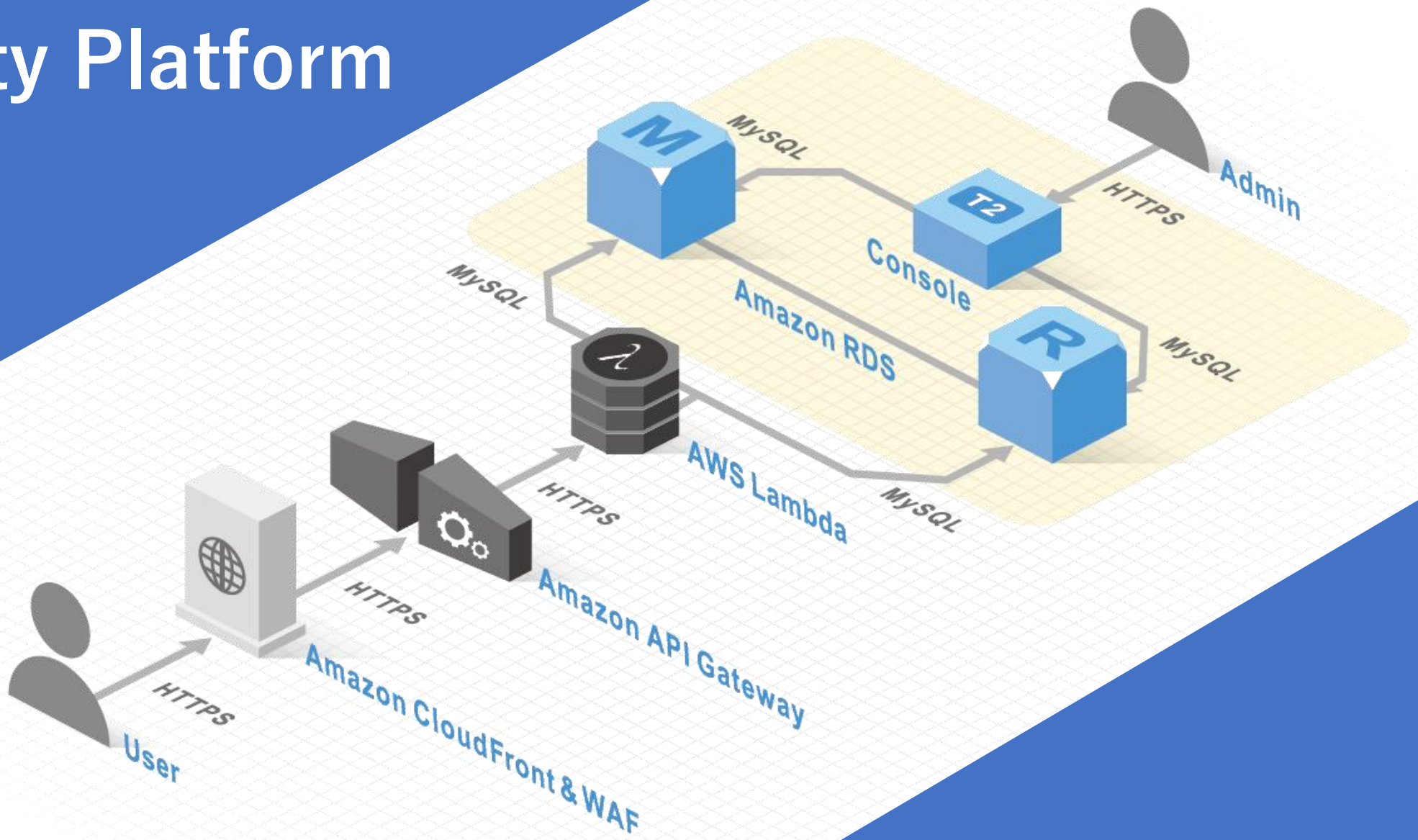
IdentityPlatform AWS対応版

- ✓ AWSのPaaS上で動く
  アイデンティティ連携基盤
- ✓ ≠OpenAM、OpenIDM
- ✓ ≠IDaaS
- ✓ オージス総研自社商品

これから： 基盤の設計、テストは不要。プロジェクトの迅速なスタートアップ。



ThemiStruct Identity Platform



OpenID Certification Program に参加する意味

認証基盤のユースケースが拡大

ユースケース	狙い・特長
クラウドサービス利用時、スマホ・タブレット利用時の認証強化	社外からの利用の制限。社外での利用時の追加の認証の実施。社用端末の識別。クラウドサービスのIDメンテナンス。
顧客（一般消費者）向けの情報提供、サービス提供	SSOによる顧客への利便性の提供。**複数アプリへの展開**。収集した属性の活用。**他社サービスとの連携**。

クラウドサービスと
簡単に繋がる認証基盤
が必要

ID基盤とアプリの
開発の分担のための
明確・安全な仕様が必要

提携先と簡単に繋がる
ビジネスを広げられる
認証基盤が必要

アイデンティティ連携の標準技術への対応が求められる

これらの技術は標準化が進み、製品・サービスへの実装も浸透している。

標準技術に対応できていることを知る

自分達が作ったものが正しく実装されたものなのか？
を知るための信頼できるテストケースが必要

ソリューションを選択するお客さまが
正しく実装されたものであることを知るすべが必要

OpenID Certification Program

OpenID Certified への道

まずは Conformance Test Suite Software を動かす

➡ このあと 当社 氏縄 が解説

Terms and Conditions をよく確認する

ポイント

TERMS AND CONDITIONS FOR CERTIFICATION OF CONFORMANCE TO AN OPENID CONNECT CONFORMANCE PROFILE (Effective February 19, 2015)

1. 自己認証型のプログラムである。
2. OIDFと関連団体は完全免責である。
3. OIDFはTerms and Conditionsをいつでも変更できる。
4. 現在は有料である。
5. 認証結果の表示方法等に指定がある。

✓ テスト結果（認証結果）の提出により、Terms and Conditionsに合意したことになる。

ポイント

TERMS AND CONDITIONS FOR CERTIFICATION OF CONFORMANCE TO AN OPENID CONNECT CONFORMANCE PROFILE (Effective February 19, 2015)

1. 自己認証型のプログラムである。

- 認証を行なうのは実装者である。
- 認証の根拠となるテスト結果の妥当性は、実装者が責任をもつ。
- OIDFと関連団体が第三者的にテスト結果を検証・認証するものではない。
- 認証結果に変更がある場合は、実装者はOIDFに通知し、更新された認証結果を再提出する必要がある。
- 認証結果の妥当性に影響がある誤りが見つかった場合は、実装者が自ら取消を申請しなければならない。

2. OIDFと関連団体は完全免責である。

- 認証により生じるいかなることも実装者の責任。
- OIDFと関連団体は、実装者の損害に責任は負わない。
- 損害賠償額の上限も$1である。

ポイント

TERMS AND CONDITIONS FOR CERTIFICATION OF CONFORMANCE TO AN OPENID CONNECT CONFORMANCE PROFILE (Effective February 19, 2015)

3. OIDFはTerms and Conditionsをいつでも変更できる。

- 認証済みの実装については、変更の30日前までに通知がある。
- 新しいTerms and Conditionsに合意できない場合は認証を取消す申請を行なう必要がある。

4. 現在は有料である。

- FAQに記載がある。
- 2016/12/1現在の費用は以下のとおり。
  - OIDF会員は、Deployment毎に US$ 200
  - OIDF非会員は、新規のDeploymentが US$ 999
    認証済み実装の新しいDeploymentが US$ 499

5. 認証結果の表示方法等に指定がある。

- “[Implementer Name] has certified that [Deployment name and version] conforms to the [specify Conformance Profile] of the OpenID Connect™ protocol.” という。
- タグラインには “OpenID Certified™ by [Implementer Name] to the [specify Conformance Profile] of the OpenID Connect™ protocol” もしくは類似の表示を使う。
- 適切な翻訳はOK
- ロゴマークは、OIDFが提供するものを使う。

テスト結果（認証結果）を提出する

テスト結果（認証結果）を提出する

ロ 提出物

- 記入、署名された “CERTIFICATION OF CONFORMANCE TO OPENID CONNECT CONFORMANCE PROFILE” をPDF化したファイル

認証を宣言

- Conformance Test Suite Software のすべてのテスト結果
- その他、Conformance Profile Definitionsに指定されているもの

エビデンス

- Terms and Conditions のPDFファイルのコピー

T&Csへの合意

ロ 注意点

- 実装者が提出したものは、そのままの形でWebサイトに掲載される。
- Confidentialな情報が含まれないように提出する前によく確認する。

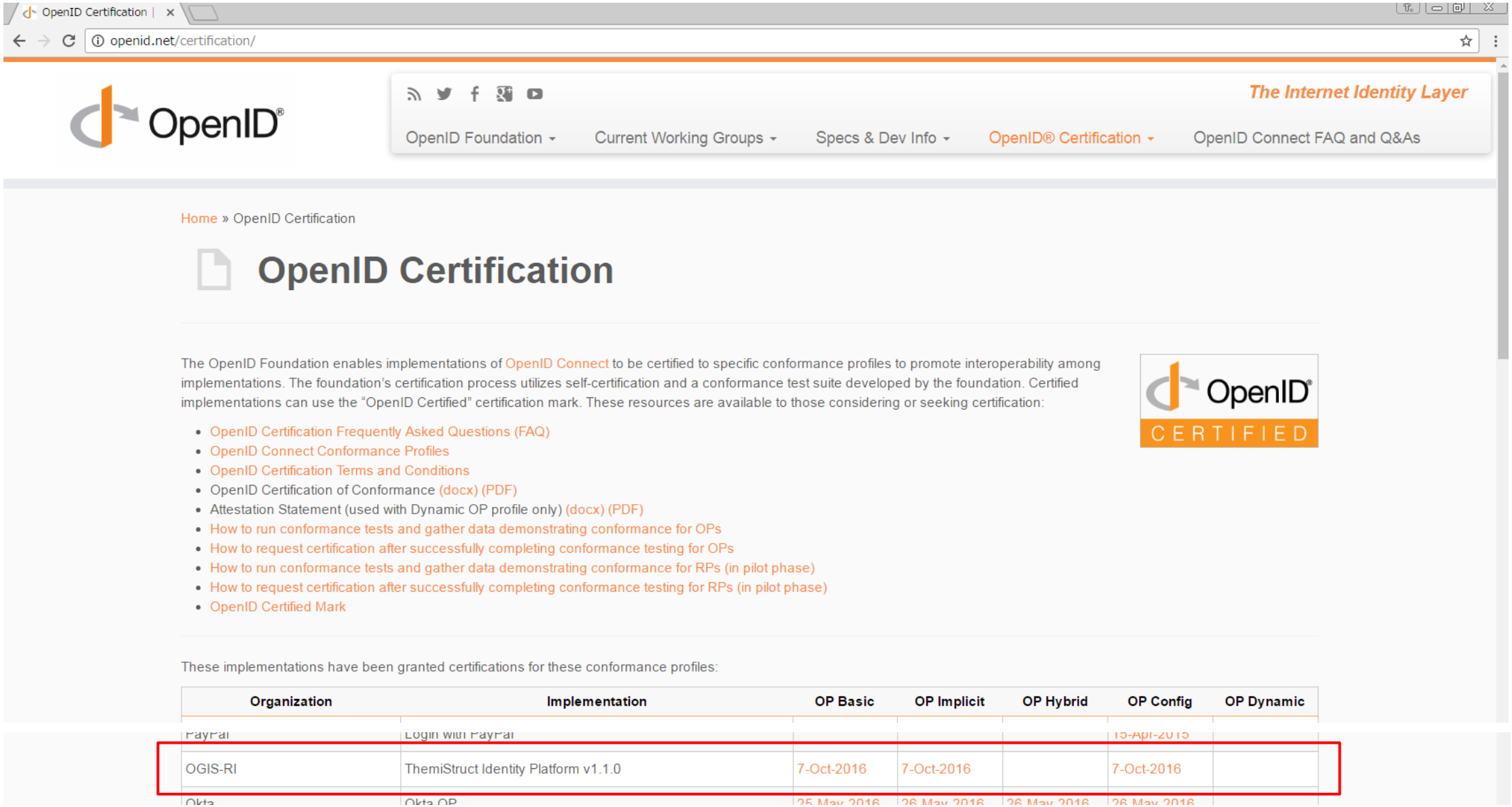
支払いは PayPal で

OpenID Certified になりました。

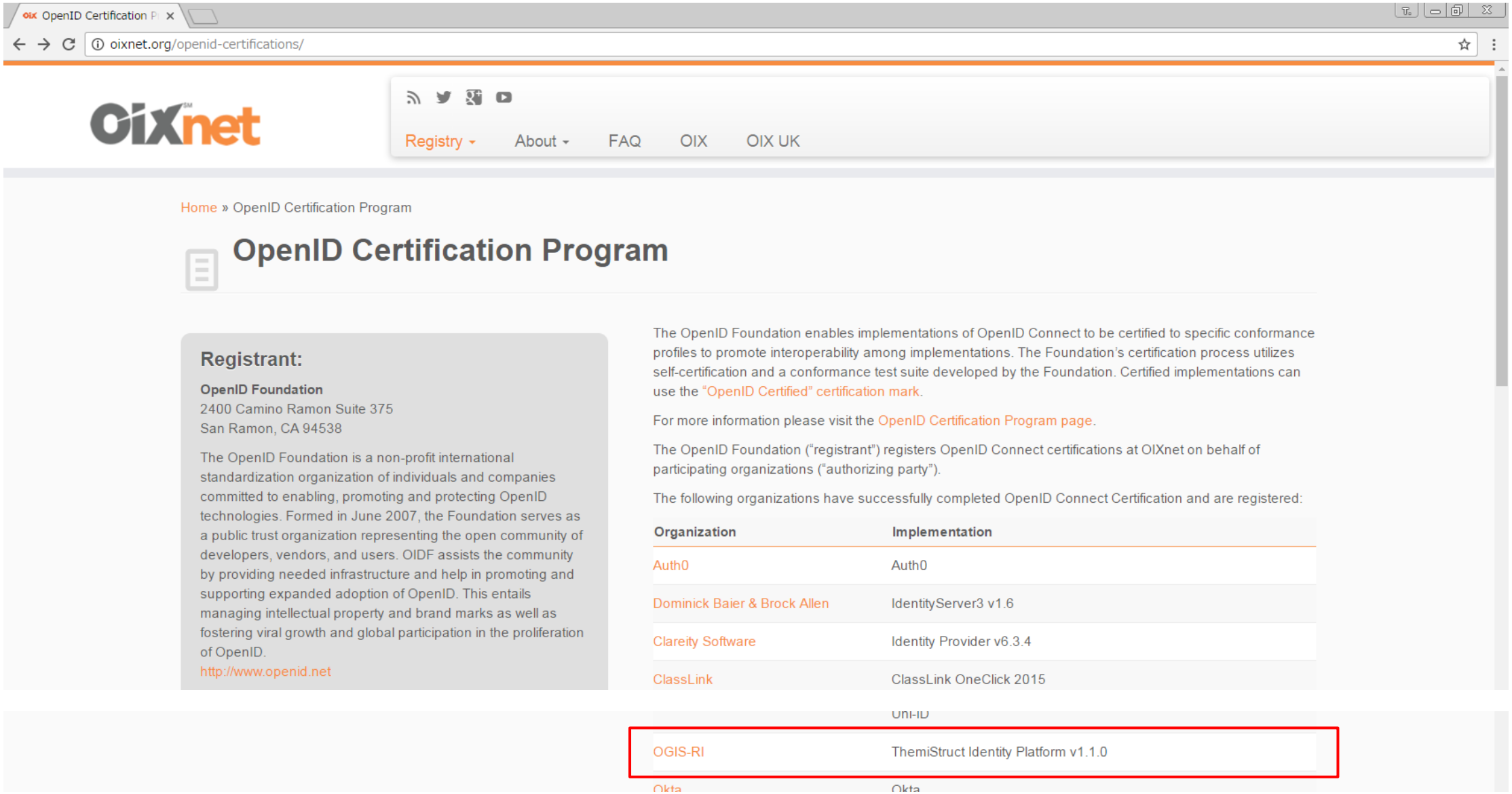
ThemiStruct（テミストラクト）
Identity Platform AWS対応版

http://openid.net/certification/

オージス総研の ThemiStruct Identity Platform は OpenID Connect™ プロトコルの OP Basic, OP Implicit, OP Config の3つのプロファイルに適合した OpenID Certified™ 実装です。



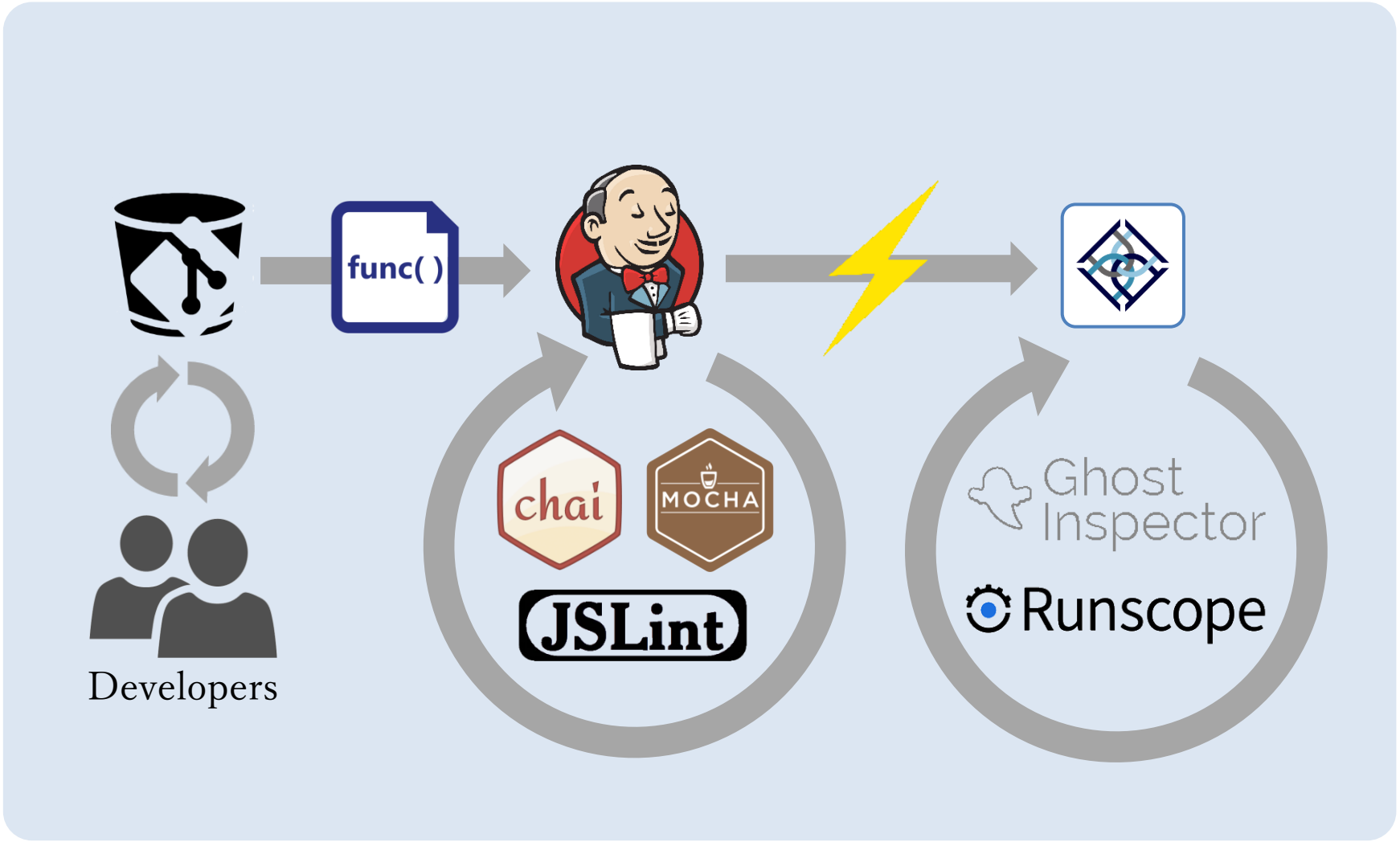
http://openid.net/certification/ （2016年12月15日現在）



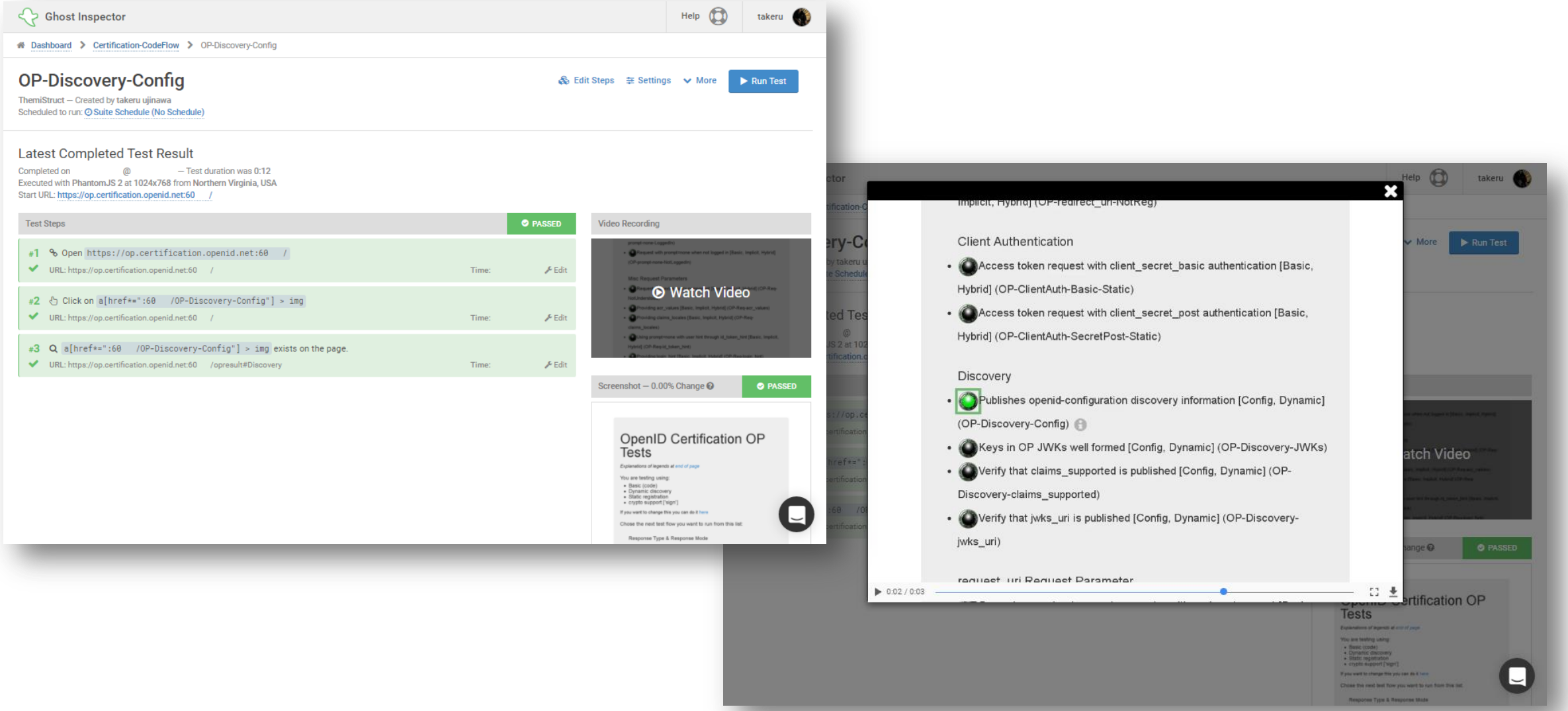
http://oixnet.org/openid-certifications/ （2016年12月15日現在）

ビルド&テストプロセスに組み込む

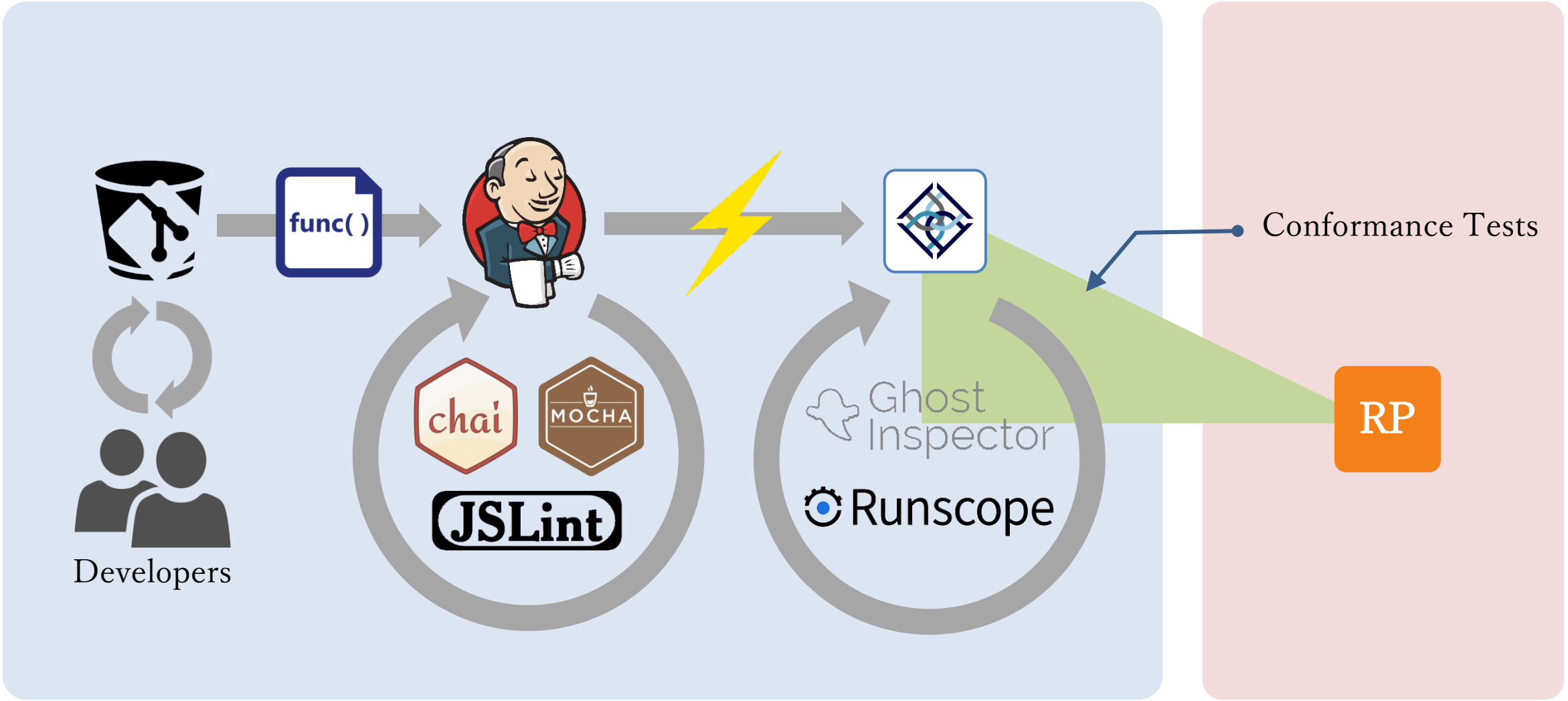
ThemiStruct Identity Platform の開発＆テスト環境



Conformance Tests の実行を自動化



ビルド&テストプロセスに組み込む



まとめ

まとめ

- 認証基盤のユースケースが広がってきた。
- 認証だけではなく、利用者のアイデンティティを管理、提供するプラットフォームが重要となる。
- 標準技術に適合した実装を行なうことで、相互接続が容易にできる認証基盤、アプリケーション、サービスが実現される。
- OpenID Certification Program はその有効な手段を提供してくれる。
- 継続していくことが大事。

ご清聴ありがとうございました

【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

参考資料

統合認証ソリューション ThemiStruct

ThemiStruct-WAM

シングルサインオン
認証基盤ソリューション

ThemiStruct-IDM

ID管理ソリューション

ThemiStruct-CM

電子証明書発行・管理
ソリューション

ワンタイムパスワードソリューション

ThemiStruct-OTP

システム監視ソリューション

ThemiStruct-MONITOR

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

クラウド、IoT時代の
“All in one”
認証プラットフォーム

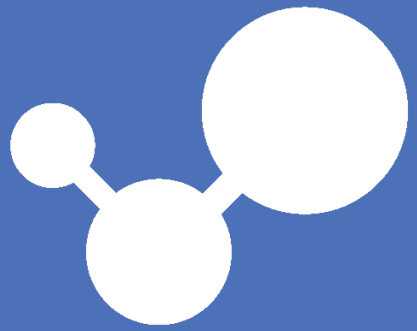
ThemiStruct Identity Platform

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

- ✓ AWSのPaaS上で動く
  アイデンティティ連携基盤
- ✓ ≠OpenAM、OpenIDM
- ✓ ≠IDaaS
- ✓ オージス総研自社商品

あなたの Identity Platform が すぐ構築可能

アイデンティティ連携



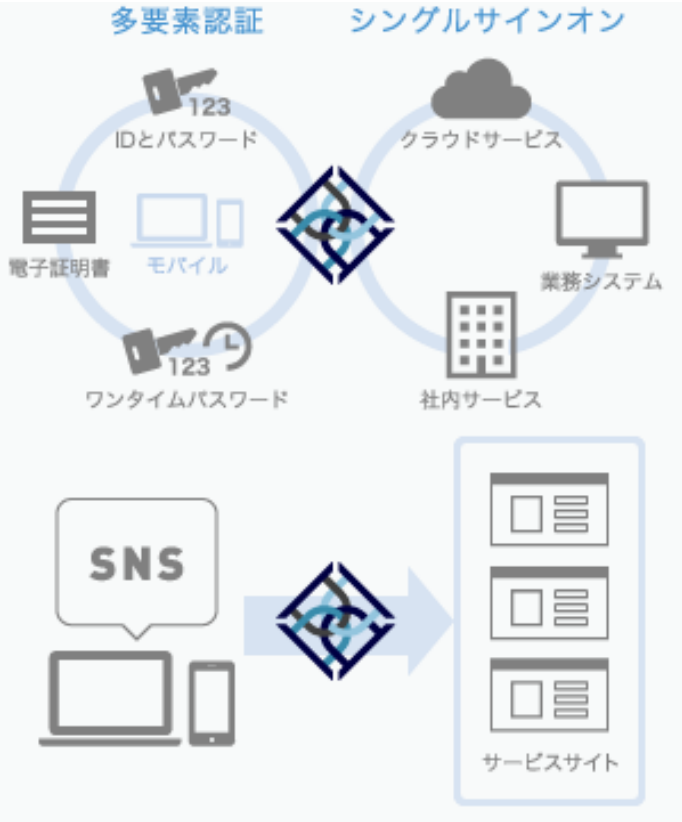
事業成長や突発的アクセスに 合わせたスケーリング

アクセスセキュリティ強化

ThemiStruct Identity Platform の特徴 (1)

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、ユーザー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。

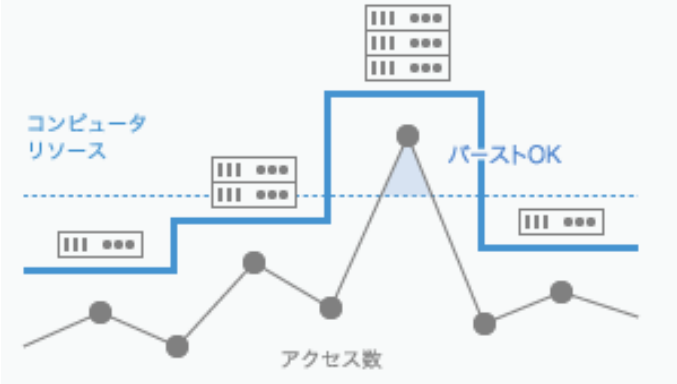
ユーザー登録のハードルを下げ、新規ユーザー登録率をアップ

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

ThemiStruct Identity Platform の特徴 (2)

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、必要なユーザー情報を連携することができます。各システムでユーザー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。