

Social Tech Talk #02

日立でOSSにコントリビュートということ

株式会社 日立製作所
Software CoE
OSSソリューションセンタ
田畑 義之



田畑 義之 (たばた よしゆき)

- 株式会社 日立製作所 Software CoE OSSソリューションセンタ
- ソフトウェアエンジニア
- GitHub: [@y-tabata](#), Qiita: [@yo-tabata](#)

• 認証認可スペシャリストとしてのAPI/SSO関連案件の支援

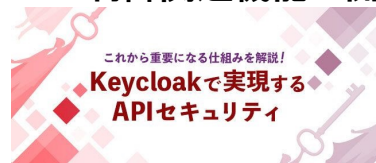
- 銀行用の高セキュリティAPIシステムのコンサル/サポート

• 認証認可・API管理関連のOSSへのコントリビュート

- Keycloak(アイデンティティ管理のOSS)における、OAuth/OIDC/FAPI関連機能の開発
- 3scale(API管理のOSS)における、セキュリティ/アクセス制御関連機能の開発

• OSSの活用事例や検証結果の情報発信

- Qiita/ThinkITでのWeb記事投稿
- Apidays/API Specifications Conference/CloudNative Daysなど、国内外のイベントでの情報発信

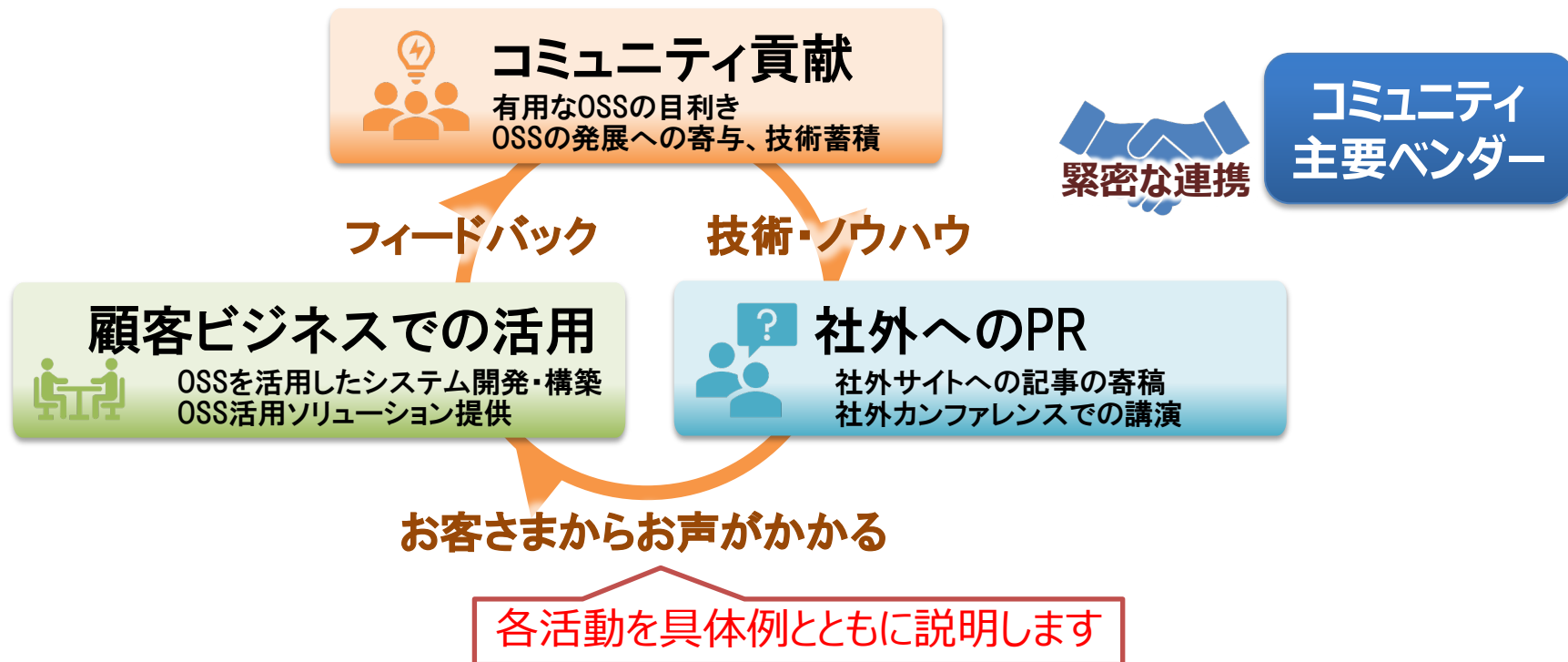


出典: ThinkIT <https://thinkit.co.jp/series/9721>



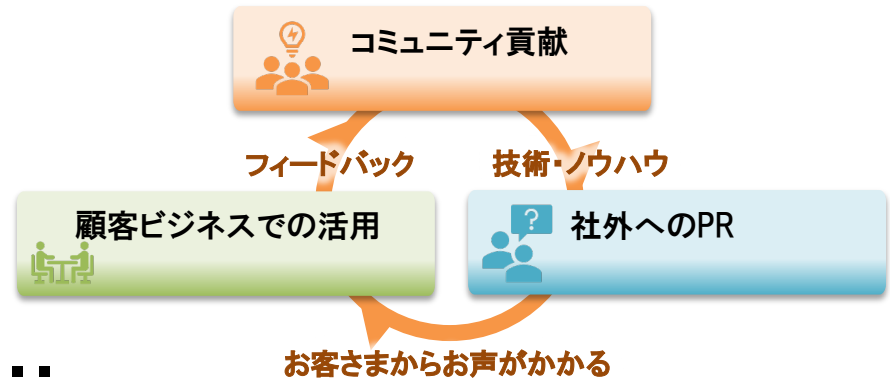
出典: ThinkIT <https://thinkit.co.jp/series/8697>

日立はOSSコミュニティ貢献とOSSの顧客ビジネスでの活用を繋げるスキームを確立しています。そのスキーム(サイクル)を回すことで、継続的にビジネスを拡大しています。



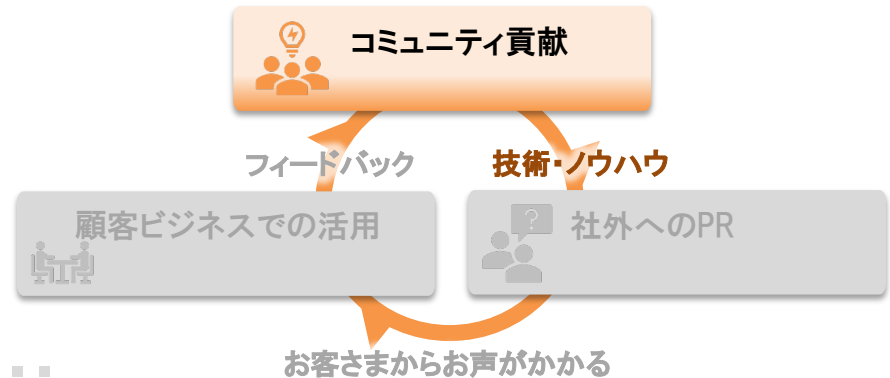
Contents

1. コミュニティ貢献
2. 社外へのPR
3. 顧客ビジネスでの活用
4. このサイクルを回していくと・・・



Contents

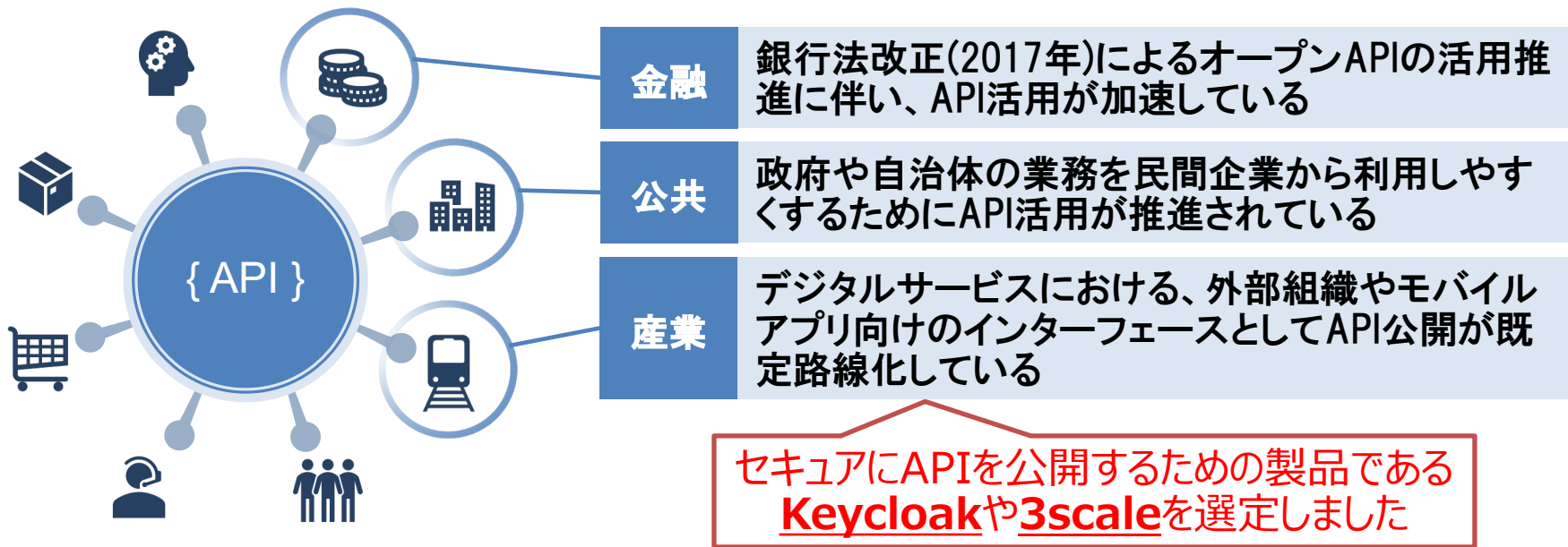
1. コミュニティ貢献
2. 社外へのPR
3. 顧客ビジネスでの活用
4. このサイクルを回していくと・・・



1. コミュニティ貢献 (1/9) ~コミュニティの選定~

コミュニティ貢献をする際、まずはどのコミュニティに貢献するかが目利きが非常に重要です。「顧客のニーズが大きく、かつ自社(日立)の強みを出せる技術分野を選定すること」が重要な目利きポイントです。

たとえば…



Keycloakは、Red Hat社を中心に開発されるID管理のOSSです。
Webシングルサインオンや、認証認可サーバの機能を提供します。

主要標準に対応したID連携
(OAuth 2.0認可サーバ含む)

OpenID Connect SAML

Keycloak

GitHub

Twitter

Facebook

RDB

LDAP

Active Directory

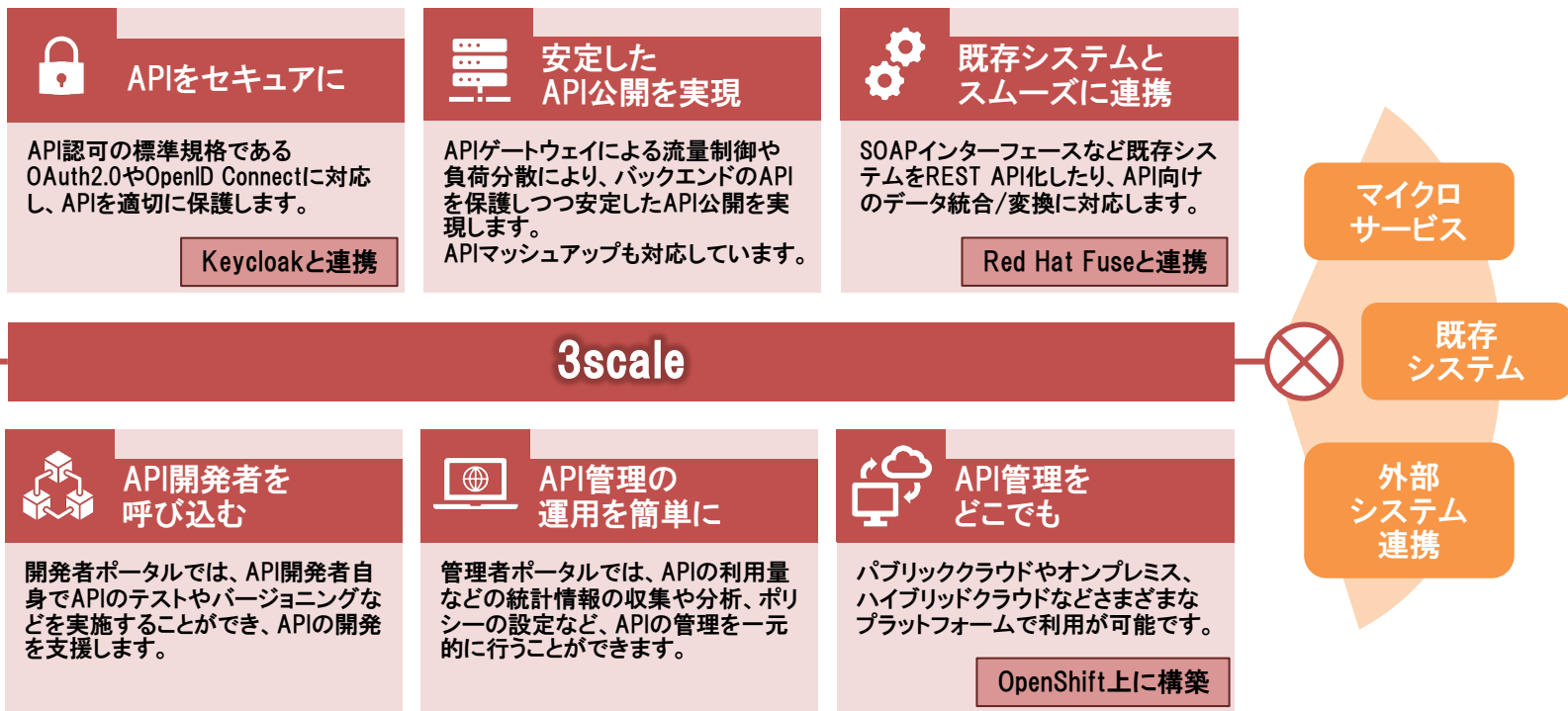
ソーシャルログイン
(Identity Brokering)

ID管理と認証

主な特徴

- OAuth 2.0/OpenID ConnectやSAMLに対応
- LDAPサーバやActive Directoryと連携可能
- GitHubなどのユーザーIDを利用したソーシャルログインにも対応

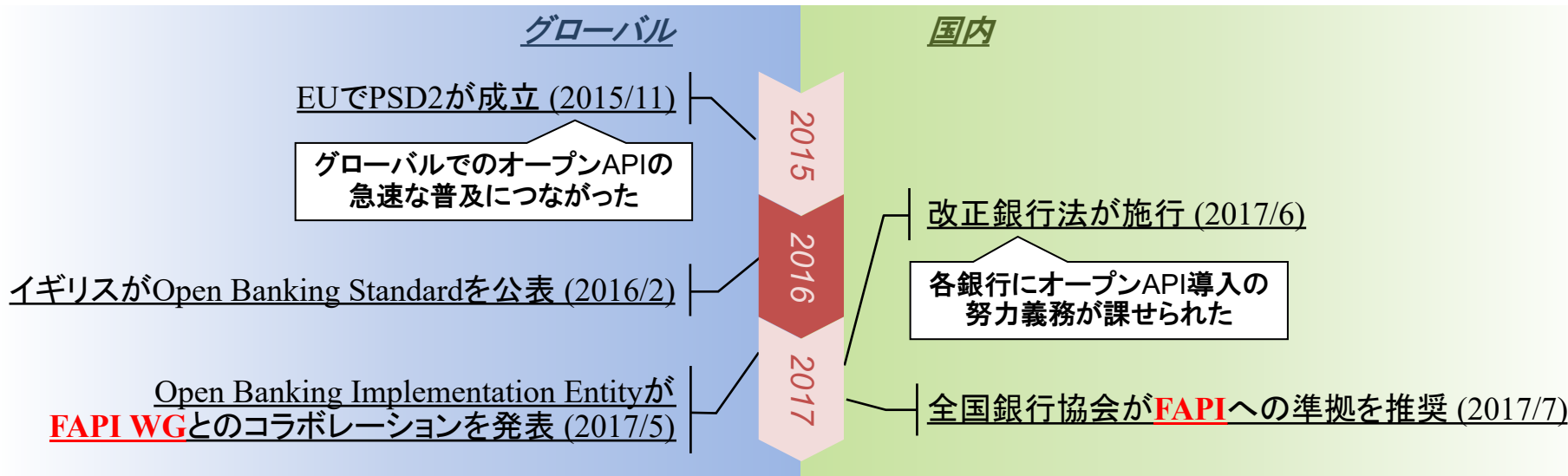
3scaleは、統合型のAPI管理ソフトウェアです。マイクロサービスにおける多数のAPI管理や、APIエコノミーの実現のための組織内外のAPI連携に適しています。



1. コミュニティ貢献 (2/9) ~戦略決め (市場ニーズ調査)~

コントリビュート対象が決まったら、次は何を作りこむかを決めます。
市場にとって有益な機能を作らないと意味がないので、まずは市場ニーズを調査します。

たとえば…

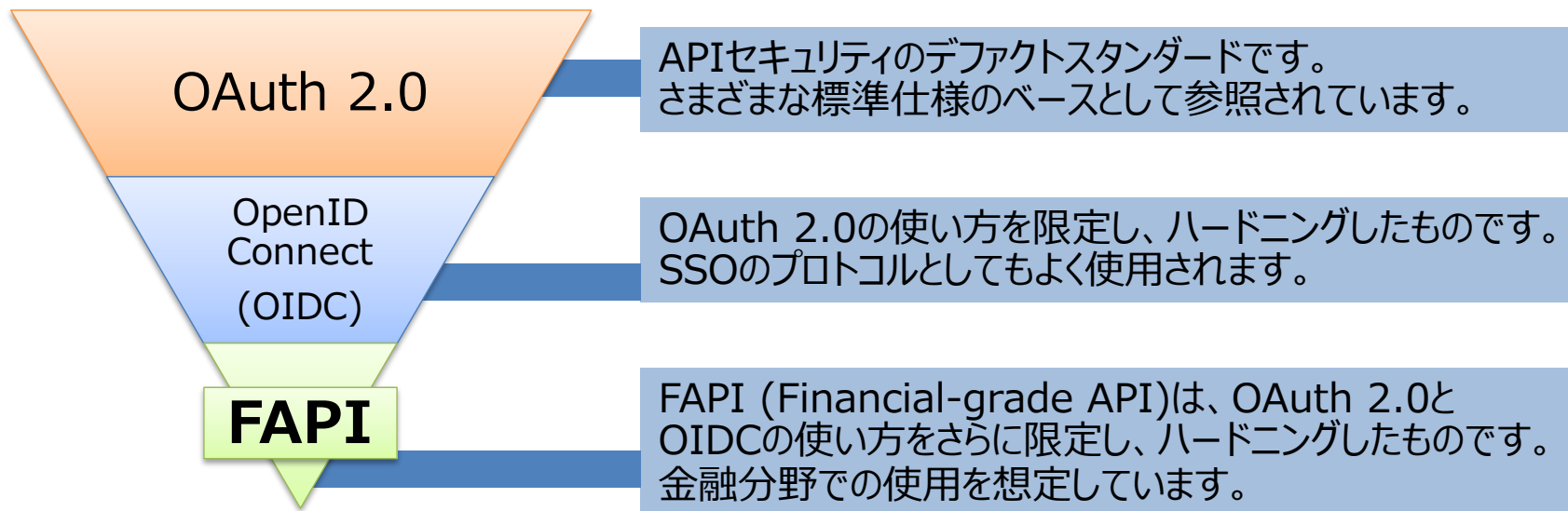


市場ニーズ調査により、国内外問わずFAPIへの注目度が上がっていることがわかります

1. コミュニティ貢献 (3/9) ~戦略決め (標準仕様調査)~

市場ニーズの実現方法を考えるには標準仕様の調査が欠かせません。
標準仕様によっては解釈のわかるものもあるため、和訳ではなく原文を調査することが重要です。

たとえば…



標準仕様調査により、FAPI周辺の標準仕様やその実現方法への理解が深まります

1. コミュニティ貢献 (4/9) ~戦略決め (製品調査)~

標準仕様の調査によって、市場ニーズの実現方法を把握したのち、実際に現状の実現度合いを確認するために製品を調査します。

たとえば…

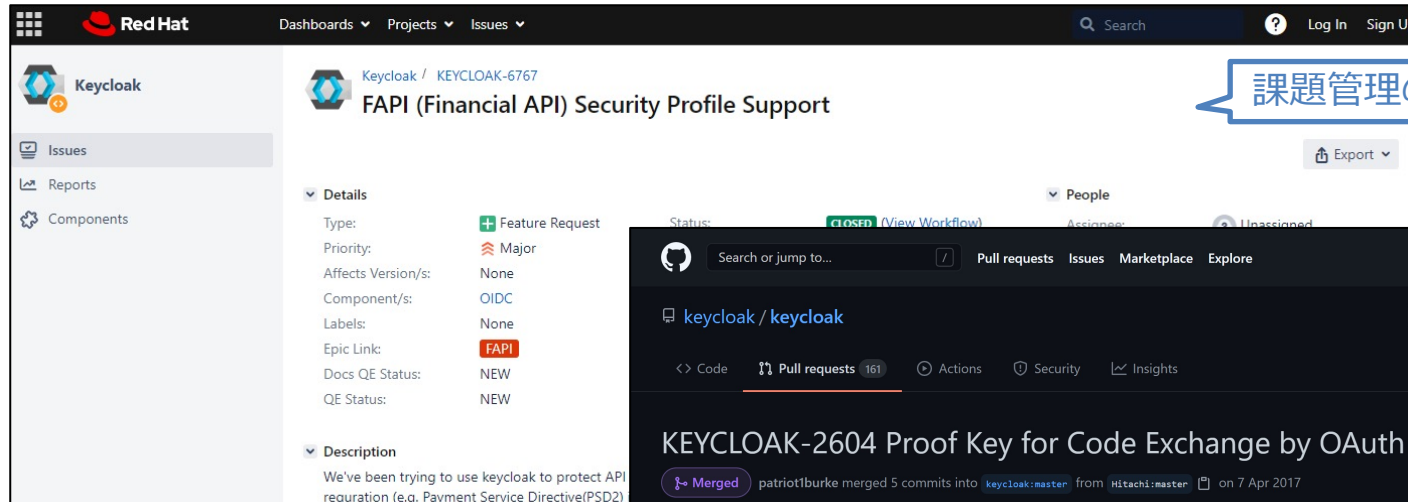
番号	小見出し	内容	準拠状況	備考
#1	認可コード要求の保護	認可サーバーは、クライアントが[OIDC]の第6章に従い署名したJWTを、requestあるいはrequest_uriパラメータの値として送信してきた場合、これを処理できること。	○(*1)	RH-SSO および keycloak のマニュアルではどこにも Request Object については触れていない。ソースコードを調べた結果、サポートされている、といえる。但し、署名アルゴリズムはRS256のみである。
#2	認可コード応答の保護	認可サーバーは、response_type パラメータの値がcode id_token あるいは code id_token token の場合に対応すること。	○	OIDC の Hybrid Flow をサポートしているかどうかとほぼ同義である。OID-F の Open ID Certificate (Hybrid OP)を取っていることから明らかなように、OIDC の Hybrid Flow はサポートしている。
#3	認可コード応答の保護	認可サーバーは、認可要求の応答に対する「切り離された署名」としてIDトークンを返すこと。	△(*1)	#3 で c_hash が返せることは明らかであるが、#5 にあるとおり、s_hash が実装されていない。また、この署名入りハッシュはデジタル署名アルゴリズムを使用するが、現状RS256のみである。
#4	認可コード応答の保護	認可サーバーは、state パラメータの値を保護する為に、IDトークン内にstateパラメータの値のハッシュ値であるs_hashフィールドを含めること。	×	FAPI Part 2 で出てきた概念であり、OIDCにはない。ソースコードをs_hashで検索したが、引っかからず。
#5	トークンの所持者証明	リソースサーバーが提供するWrite操作可能なリソースへのアクセス要求に対し、認可サーバーは認可コード、アクセストークン、リフレッシュトークンを所持者証明が行える形式で発行すること。	×	マニュアルに記載なし。ソースコードにも実装はない。

製品調査により、FAPI準拠に向けて製品の不足している機能を把握します

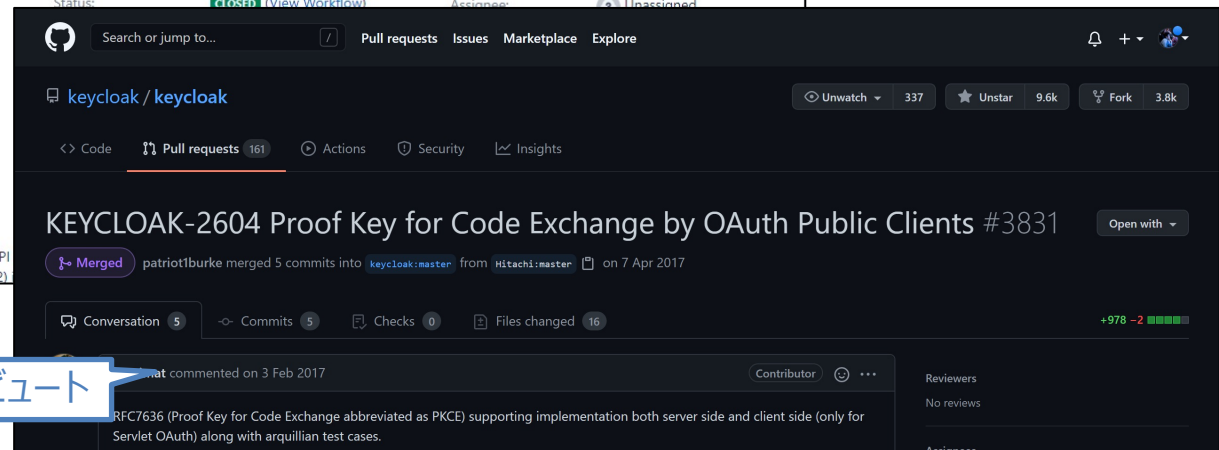
1. コミュニティ貢献 (5/9) ~コントリビュート~

不足機能を把握し、コントリビュート戦略が決まったら、実際にコントリビュートします。
コントリビュートのお作法はコミュニティによってバラバラです。お作法に則ることが大切です。

たとえば…



出典: Red Hat Jira <https://issues.redhat.com/browse/KEYCLOAK-6767>



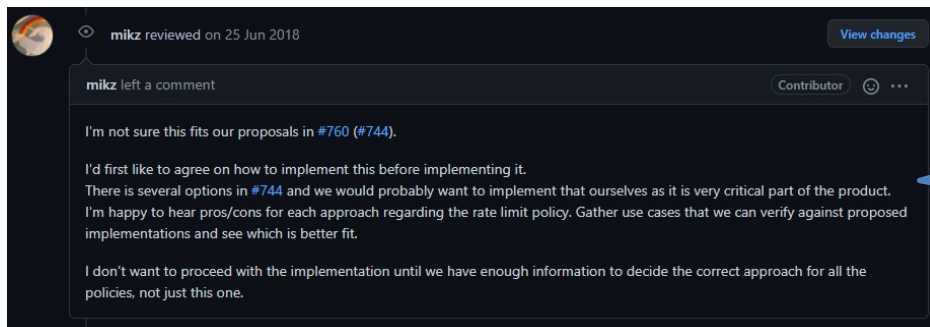
GitHubでプルリクエストを送ってコントリビュート

出典: GitHub <https://github.com/keycloak/keycloak/pull/3831>

1. コミュニティ貢献 (6/9) ~コントリビュートの失敗談 その1~

最初はコミュニティのお作法もわからず探り探りで、色々な失敗もありました。

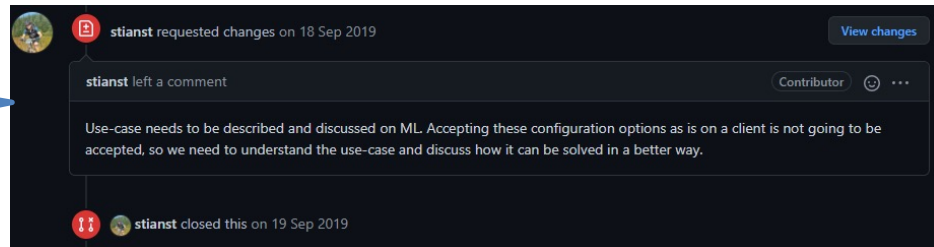
たとえば…



出典: GitHub <https://github.com/3scale/APLcast/pull/781>

プルリクエストを出してそこで議論を始めたところ、GitHubのIssueを作成して、まずはそこで議論してからコードを投稿しろと怒られたケース

プルリクエストを出したところ、ユースケースがわからないから、まずはメーリングリストで議論しろと怒られたケース



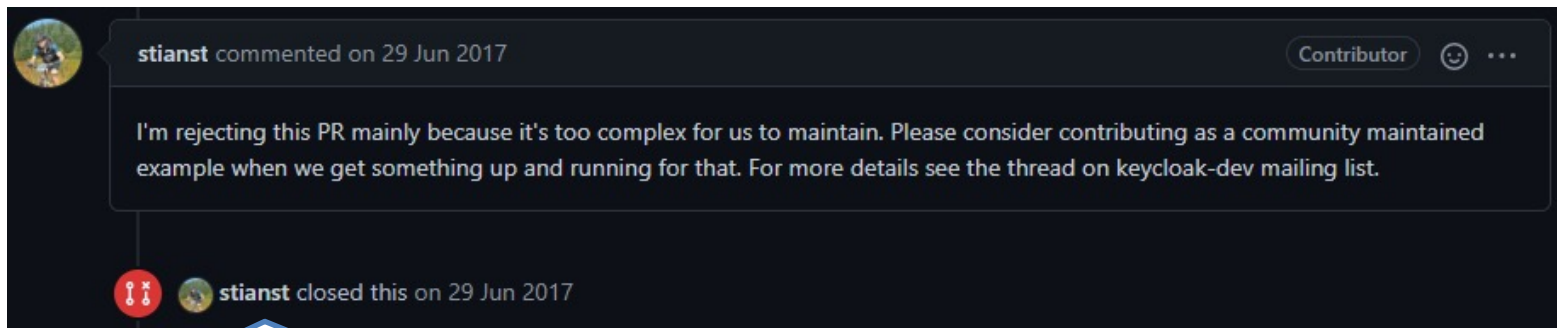
出典: GitHub <https://github.com/kevloak/kevloak/pull/6309>

そのうちマージされるコツなどがわかってくるので、根気強くチャレンジすることが大事です

1. コミュニティ貢献 (7/9) ~コントリビュートの失敗談 その2~

製品仕様やソースコードの生い立ちを知らなかったために失敗したケースもあります。

たとえば…



出典: GitHub <https://github.com/keycloak/keycloak/pull/4260>

製品のコアの部分で、できれば触りたくないコードに手を入れるようなプルリクエストを出してリジェクトされたケース

製品仕様に反する機能を追加するためのJIRAチケットを作成してリジェクトされたケース

Stian Thorgersen added a comment - 2019/Feb/13 1:24 AM

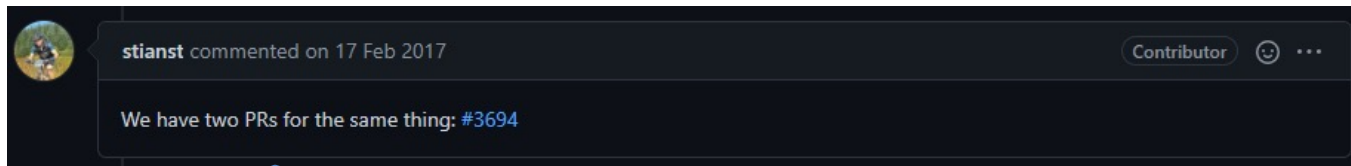
Keycloak does not currently support being logged-in from multiple accounts at the same time so adding this option doesn't make sense at this point

出典: Red Hat Jira <https://issues.redhat.com/browse/KEYCLOAK-8712>

1. コミュニティ貢献 (8/9) ~コントリビュートの失敗談 その3~

単純にプルリクエストを出すタイミングが悪くて失敗したケースもあります。

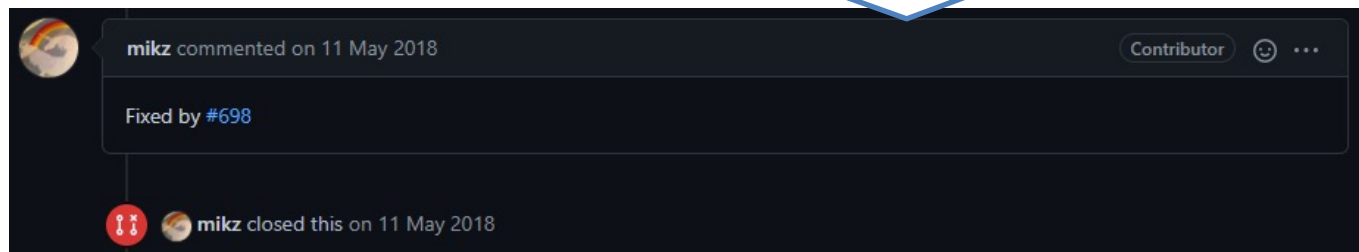
たとえば…



出典: GitHub <https://github.com/keycloak/keycloak/pull/3831>

似たようなタイミングで他の人もプルリクエストを出していたケース

他の機能追加用のプルリクエストによって、バグが修正されてしまったケース



出典: GitHub <https://github.com/3scale/APICast/pull/697>

同じことを考えている開発者がいるので、タイムリーにプルリクエストを出すことが大事です

1. コミュニティ貢献 (9/9) ~コントリビュートの失敗を乗り越えて~

こうした数々の失敗を乗り越え、コントリビュータとしての信頼を勝ち取り、機能追加にこぎつけます。大きい開発項目も、小機能に分けてコントリビュートすることが、最終的な機能追加への近道です。

たとえば…

FAPIサポートに向けてコツコツとコントリビュートを継続

Release Notes

Keycloak 14.0.0

Highlights

Client Policies and Financial-grade API (FAPI) Support

The Keycloak server has now official support for client policies and Financial-grade API (FAPI). This capability was previewed in earlier versions, but now it is more polished and properly documented. Thanks to Takashi Norimatsu who did most of the work on this. Also thanks to Andrii Murashkin and Hryhorii Hevorkian, who did a great deal of the work on this feature as well. Finally thanks to all the members of the FAPI Special interest group for their help and feedback.

JIRA	Description	PR
KEYCLOAK-2604	Support PKCE (RFC7636)	3831
KEYCLOAK-6768	Support signed and encrypted ID token	5779
KEYCLOAK-6771	Support holder of key (RFC8705)	5083
...

FAPIがサポートされました！
リリースノートには謝辞が掲載されます

Contents

1. コミュニティ貢献
2. 社外へのPR
3. 顧客ビジネスでの活用
4. このサイクルを回していくと・・・



2. 社外へのPR (1/2) ~社外寄稿~

行ったコントリビュートを社外寄稿や社外講演を通じてアピールし、プレゼンス向上を図ります。
コントリビュートに関することのみではなく、検証結果やイベントレポートを投稿することもあります。

たとえば…

The screenshot shows a Qiiita article page. At the top, there is a search bar with the text 'キーワードを入力'. Below it, a notification banner reads 'Amazonギフト券3,000円分の謝礼を進呈中！プロフィール入力＆アンケート回答してQiiita Jobsをアップデート！'. The article title is 'OSSベースのAPI管理製品 3scale 2.2を試してみた' by @yo-tabata, updated on January 29, 2019, with 10349 views. The article tags include 'api, openshift, APIGateway, Keycloak, 3scale'. The publication date is '初版: 2018/7/10' and the author is '著者: 田畑義之, 株式会社日立製作所 (GitHubアカウント: @y-tabata)'. A disclaimer states: '本記事は、あくまで執筆者の見解であり、所属企業及びRed Hatの公式なドキュメントではありません。' The source is cited as '出典: Qiiita <https://qiiita.com/vo-tabata/items/eb81c5cb324cefa87efc>'.

これらの課題に対して、筆者は、APIcast側での流量制御をポリシーとしてパッチ投稿しました。基本的な機能についてはPR #648で提案し、採用されました。テクノロジレビューながら3scale 2.2から取り込まれています。

APIcast側でトークンイントロスペクションを行うトークンイントロスペクションポリシー(PR #619)を提案し、採用されました。テクノロジレビューながら3scale 2.2から取り込まれています。

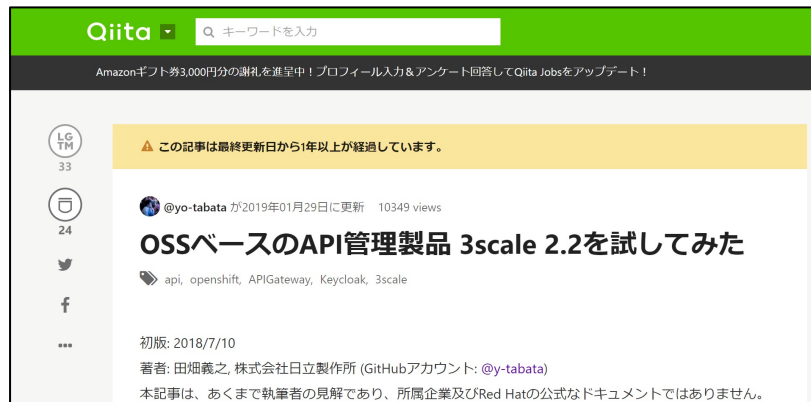
「APIcastでのスコープチェック」という選択肢を実現し、より幅広いユースケースに対応できるように、筆者はPR #773でパッチ提案し、採用されました。

製品について詳しく知っていることのみではなく、実際に製品を作っていることもアピールします

2. 社外へのPR (1/2) ~社外寄稿~

行ったコントリビュートを社外寄稿や社外講演を通じてアピールし、プレゼンス向上を図ります。コントリビュートに関することのみではなく、検証結果やイベントレポートを投稿することもあります。

たとえば…



出典: Qiita <https://qiita.com/yo-tabata/items/eb81c5cb324cefa87efc>



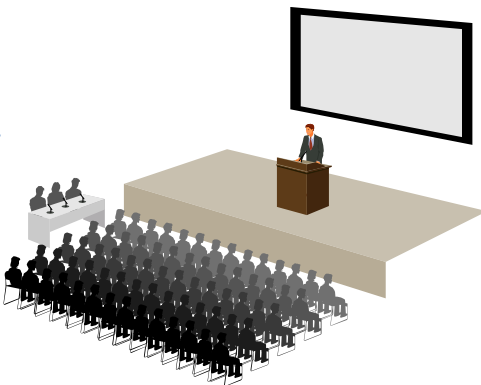
出典: Facebook <https://www.facebook.com/RedHatJapan/posts/1731686740202008>

良い記事を書くとコミュニティ主要ベンダーがPRしてくれることもあります

2. 社外へのPR (2/2) ~社外講演~

社外カンファレンスでの講演も、コントリビュートなどをアピールする絶好の機会です。
カンファレンスに参加しているコミュニティ主要人物とパイプを作ることも大切です。

講演によるプレゼンス向上のみではなく
質疑応答や会食などで高い技術力に
触れることで良い刺激をもらえます



実際の講演の様子:
Open Source Summit Japan 2019



コミュニティ主要人物と直接会うことで新しい情報を仕入れたり
その後のコントリビュートを円滑に進めたりできます



2'. お客様からお声がかかる (1/2)

社外へのPRをすることで、我々のOSSコミュニティ貢献がお客様の目にとまるようになります。OSSへのコントリビュート数や国内外カンファレンスの講演数が、OSSを用いた顧客協創ビジネスにおけるパートナー選定時の指標として使われることもあります。

たとえば…



この記事を書いた〇〇という方と話をしてみたい。

〇〇さんのいる日立に支援いただきたい。



この流れから案件獲得につながることも多々あります

OSSは誰でも自由に使えるという特徴がありますが、何か問題が発生したときのサポートは必要です。いざというときにソースコードレベルの調査ができたり、パッチを投稿できたりするため、**“製品について知っている人がいる”**だけでなく、**“実際に作っている人がいる”**ほうがパートナーとして選定されやすい傾向にあります。



2'. お客様からお声がかかる (2/2)

実際に、金融(銀行、保険など)、公共、社会、産業などさまざまな分野の案件を支援しています。社外でも認証認可の専門家として認知され、お客様の指名で案件対応をした実績もあります。

たとえば…



専門家としての技術力を評価され
対応した案件の一例

[公共] 某省庁様 国民向け申請システム



監査説明ができるセキュリティ専門家として
要望を受け対応。
認証認可のフロー設計やAPI管理基盤構築の
支援を実施。

[金融] 某金融機関様 デジタル決済プラットフォーム



お客様へOAuthやAPI管理について説明できる
セキュリティ専門家としての要望を受け対応。
APIゲートウェイや認証認可サーバの構築支援
を実施。



お客様のご指名で対応した
対応した案件の一例

[金融] 某金融機関様 API管理基盤構築



Red Hat主催のセミナーの日立講演をきっかけ
に日立のセキュリティ技術力の高さを評価いた
だき、日立をご指名頂いた。

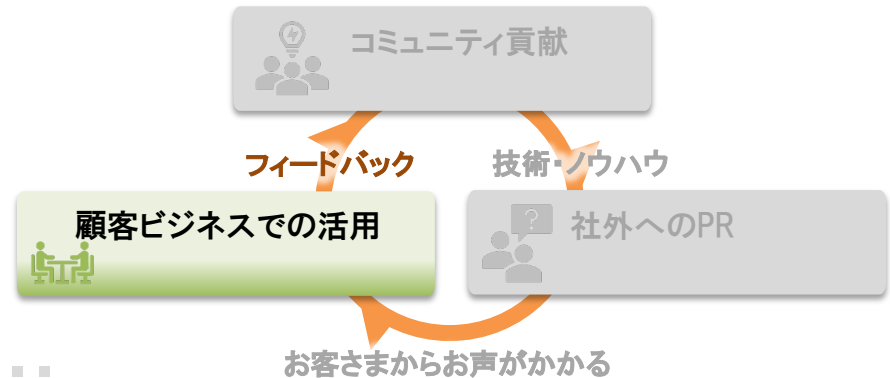
[金融] 某金融機関様 認証認可システムのトラブル対応



日立の社外著作物で日立のセキュリティ技術
の高さを認知。
お客様のご指名で案件を対応。

Contents

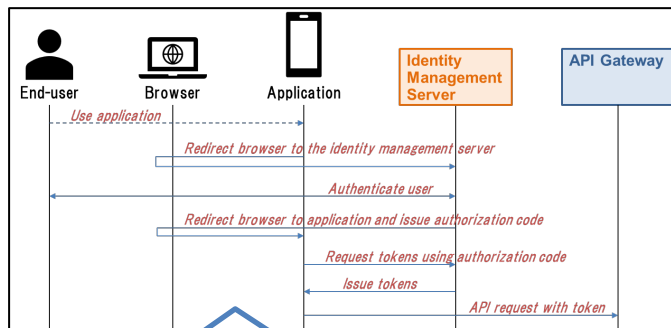
1. コミュニティ貢献
2. 社外へのPR
3. **顧客ビジネスでの活用**
4. このサイクルを回していくと・・・



3. 顧客ビジネスでの活用

コミュニティ貢献で培った知識(製品知識のみならず、標準仕様に関する高度な専門知識)や国内外カンファレンスで仕入れた最先端のグローバル動向を駆使して案件を支援しています。

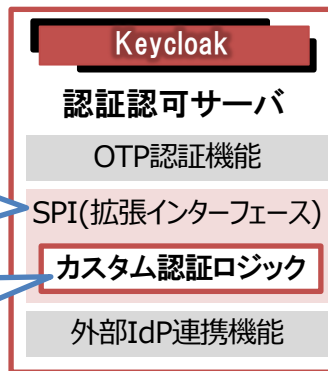
たとえば…



セキュリティ要件を満たすための認証認可周りの複雑なフローの設計を支援しています

機能を追加/拡張できるインターフェースがありますが、実装方法に関する情報はソースコードのみです

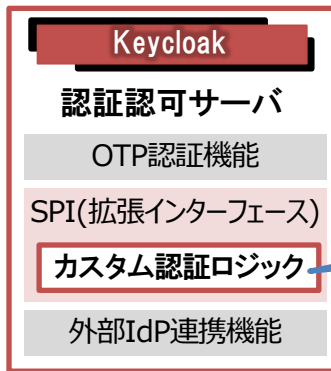
顧客要件を機能に落とし込み、それを実現するモジュールのプロトタイプを提供しています



コミュニティ主要ベンダーとの強固な連携を構築し、いざというときに総力を結集してサポートできる体制を構築しています

実際にOSSを顧客ビジネスで活用すると、OSSのさまざまな課題が見えてきます。それら課題をコントリビュートという形でOSSにフィードバックします。

たとえば…



将来のカスタマイズを不要とするために、案件用に作成したプロトタイプを汎用化してコミュニティにアップストリームしています

実際に顧客が使ったうえでのフィードバックのため、マージに持っていくやすい傾向があります

Keycloak

トークンの有効期限設定機能、トークン無効化機能、性能改善、...

3scale

流量制御機能、RBAC機能、プロキシプロトコル機能、...

実際に何か問題が発生したときに、パッチを投稿した実績も多々あります。

たとえば…



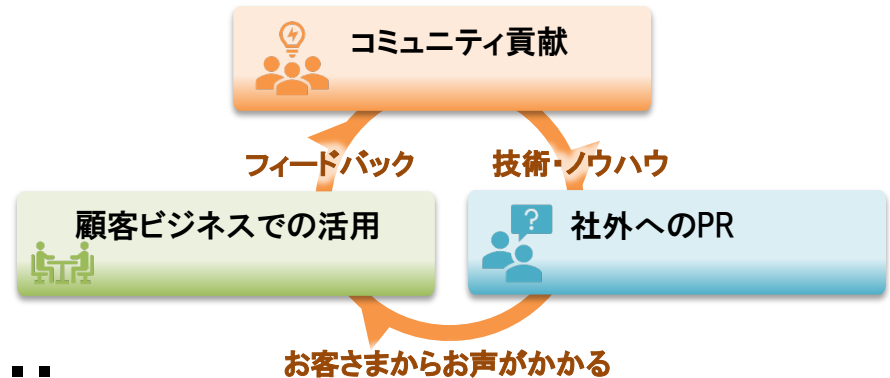
ソースコードやコントリビュートの勝手を知っているので、パッチ投稿までのスピード感が早いことが特徴です

標準仕様寄りの“**理論派**”の視点を持つコミュニティと、実際に製品を使っている“**現実派**”の視点を持つ顧客の、両者と接点があり、両者の視点を持ちつつ両者にフィードバックできるという点が強みとなります。



Contents

1. コミュニティ貢献
2. 社外へのPR
3. 顧客ビジネスでの活用
4. このサイクルを回していくと・・・



4. このサイクルを回していくと・・・ (1/5) ~コミュニティ貢献~

より高い効果を発揮できる活動ができるようになります。

たとえば・・・

機能追加時に、過去実績による信頼とノウハウを活用した効果的な必要性アピールによって、多くの協力者/賛同者を巻き込みつつ、スムーズにマージまでこぎつけたケース

Hi everybody,

we are VERY interested in this is really causing us a lot of headache currently. We are definitely willing to contribute here!

Best regards,

Glad to see this coming. Indeed, it is a critical issue for large-scale deployments.

I've started with an initial comment on your proposal.

FAPI-SIG (Financial-grade API Security : Special Interest Group)

Overview

FAPI-SIG is a group whose activity is mainly supporting **Financial-grade API (FAPI)** and its related specifications to keycloak.

FAPI-SIG is open to everybody so that anyone can join it anytime. Nothing special need not to be done to join it. Who want to join it can only access to the communication channels shown below. All of its activities and outputs are public so that anyone can access them.

FAPI-SIG mainly treats FAPI and its related specifications but not limited to. E.g., Ecosystems employing FAPI for their API Security like UK OpenBanking and Australia Consumer Data Right (CDR).

コミュニティへの貢献で信頼を勝ち取り、メンテナに就任したり、標準仕様の策定に一役買ったりした方もいます

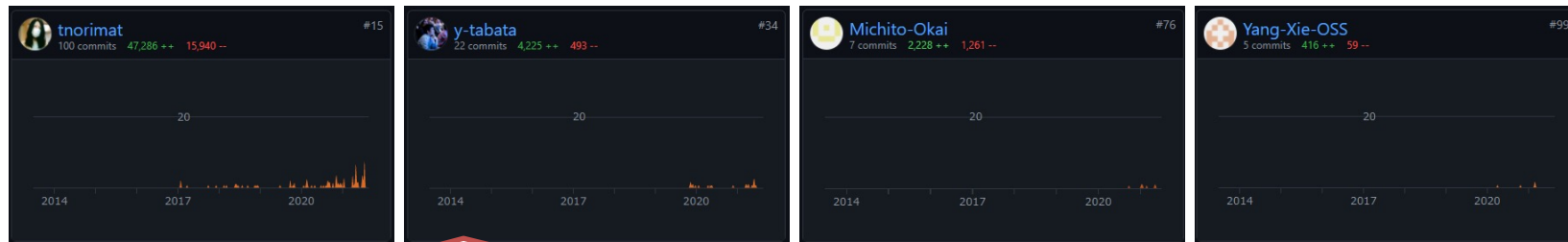
定期的にコミュニティの主要人物とのミーティングを開催し、製品に関する情報交換を実施しています

出典: GitHub <https://github.com/keycloak/kc-sig-fapi>

実際に日立のエンジニアがメンテナに就任した
FAPI関連の標準仕様をサポートするためのKeycloakリポジトリ

4. このサイクルを回していくと・・・ (2/5) ~コミュニティ貢献~

コミュニティ貢献で得たノウハウをもとに、後継の育成も進んでいます。
また、ノウハウの横展開により、他分野のOSSを効率的に開拓しています。



出典: GitHub <https://github.com/kevcloak/kevcloak/graphs/contributors>

コントリビューションのランキングにランクインする日立のコントリビュータも増えています

4. このサイクルを回していくと・・・ (3/5) ~社外寄稿~

単体の記事を寄稿するだけでなく、連載記事を書く機会も増えています。

たとえば・・・



出典: ThinkIT <https://thinkit.co.jp/article/15729>

コミュニティ主要ベンダーの方と共著する機会もありました



出典: ThinkIT <https://thinkit.co.jp/article/17621>

コミュニティ主要ベンダーの方にコミュニティ貢献をアピールしてもらい、よりプレゼンスが向上しました

おわりに

次回は3scaleのコミッターとしても活躍している日立製作所の田畑さんより、3scaleの基本機能や一般的な使い方を紹介します。

出典: ThinkIT <https://thinkit.co.jp/article/16075>

4. このサイクルを回していくと・・・ (4/5) ~社外寄稿~

社外寄稿をする方も増え、QiitaでOrganizationを設立できるようにもなりました。組織全体としてのプレゼンス向上が期待できます。

The screenshot shows the Qiita organization page for Hitachi. The header is green with the Qiita logo and a search bar. The main content area is white and features the Hitachi logo and the text "株式会社 日立製作所 OSSソリューションセンター". Below this, there is a description of the organization's activities and statistics: 203 articles and 4917 LGTM. A list of popular tags is shown, including Keycloak (27 articles, 535 LGTM), GraphQL (26 articles, 248 LGTM), ML 機械学習 (25 articles, 438 LGTM), Python, and node-red. The "人気の記事" (Popular Articles) section lists "日立社員「社内からQiitaに投稿?できるのそれ」" by dracuttimeout and "Apache Kafkaの概要とアーキテクチャ" by sigmalist.

出典: Qiita <https://qiita.com/organizations/hitachi-oss>

The screenshot shows the Qiita Advent Calendar 2020 page for Hitachi. The header is green with the Qiita logo and a search bar. The main content area is white and features the text "日立グループ OSS Advent Calendar 2020". Below this, there is a list of sponsors including Microsoft Azure, DataRobot, Lenovo, free, Udemy, PASONA TECH, and metaps. The page also includes a section for "日立グループのエンジニアによるAdvent Calendarです。" and a list of articles related to the calendar.

出典: Qiita <https://qiita.com/advent-calendar/2020/hitachi-oss>

Advent Calendarにも積極的に取り組んでいます

4. このサイクルを回していくと・・・ (5/5) ~社外講演~

コミュニティ貢献による技術力の向上や案件採用数の増加に伴い、顧客事例の紹介や、複数OSSを絡めたソリューションの紹介など、採択されやすい講演ネタを提案することができるようになり、カンファレンスに登壇する機会も増えています。



実際の講演の様子：
API Specifications Conference 2019

他にも、Apidays、DevConfなど多岐にわたり、講演するカンファレンス数も増えています

日立がOSSコミュニティ貢献とOSSの顧客ビジネスでの活用を繋げ、継続的にビジネスを拡大するスキームを具体例とともにご紹介しました。

日立でOSSコミュニティ貢献を推進するメリットには以下のような点があります。

- コミュニティと顧客の両者と接点があり、両者の視点を持ちつつ両者にフィードバックできる。
- 多様な事業があるため、1つのOSSを色々なユースケースで活用することができ、それに対応していくことでエンジニアとしての幅が広がる。
- 実際にコントリビュートやアウトプット(社外寄稿/社外講演)をしているエンジニア仲間と、ノウハウを共有しつつ切磋琢磨しながらともに成長することができる。
- コミュニティ主要ベンダーとも良好な関係を築いており、OSSの顧客ビジネス活用を推進するための環境が整っている。

- OpenID is a trademark or registered trademark of OpenID Foundation in the United States and other countries.
- GitHub is a trademark or registered trademark of GitHub, Inc. in the United States and other countries.
- Red Hat, the Shadowman logo, and OpenShift are registered trademarks of Red Hat, Inc. in the United States and other countries.
- Other brand names and product names used in this material are trademarks, registered trademarks, or trade names of their respective holders.

HITACHI
Inspire the Next 

日立のOSSへの取り組みをより詳しく知りたい方におススメのイベントです。

今回はオープンソースのポリシーエンジンであるOpen Policy Agent(OPA) について、概要やユースケース、実際に検証した内容などをお話します。

ぜひお気軽にご参加ください！



以下のURLまたはQRコードから参加登録できます

<https://hitachi.comnpass.com/event/220865/>

