JJUG CCC 2024 Fall

オープンソースKeycloakのハンズオンで理解する認証と認可の基本

raedion

2024年10月27日

NRI

Envision the value,
Empower the change

本セッションの対象者と目標

■対象者

- セキュリティ、特に認証関連に何となく興味がある人

■目標

- 「認証と認可とは何か？」を理解してもらうこと
  - 前半は概念をざっくりと理解
  - 後半はKeycloakで動きを見ながらイメージアップ

■始める前に

- 本発表では時間が限られているため、ハンズオンは発表者の手元で実施させていただきます汗
- ハンズオンの実施手順は後日GitHubページにて公開するため、こちらご参照ください。

自己紹介

■raedion

■株式会社野村総合研究所

■業務では認証認可サービスの構築・維持保守に従事

- KEYCLOAK をメインに扱っています

サムネ：大学時代に食べていた天津麻婆丼

■今後の目標：何かしらのOSSにコントリビューションしたい！

不正アクセスのセキュリティリスクへの関心度が高まっている

情報セキュリティ10大脅威 2024

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	5年連続8回目
インターネット上のサービスへの不正ログイン	2016年	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6回目
不正アプリによるスマートフォン利用者への被害	2016年	9年連続9回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

(出所) https://www.ipa.go.jp/security/10threats/10threats2024.html

攻撃者の主な侵入経路

■認証情報の侵害手法：クレデンシャルスタッフィング、ブルートフォース攻撃、etc

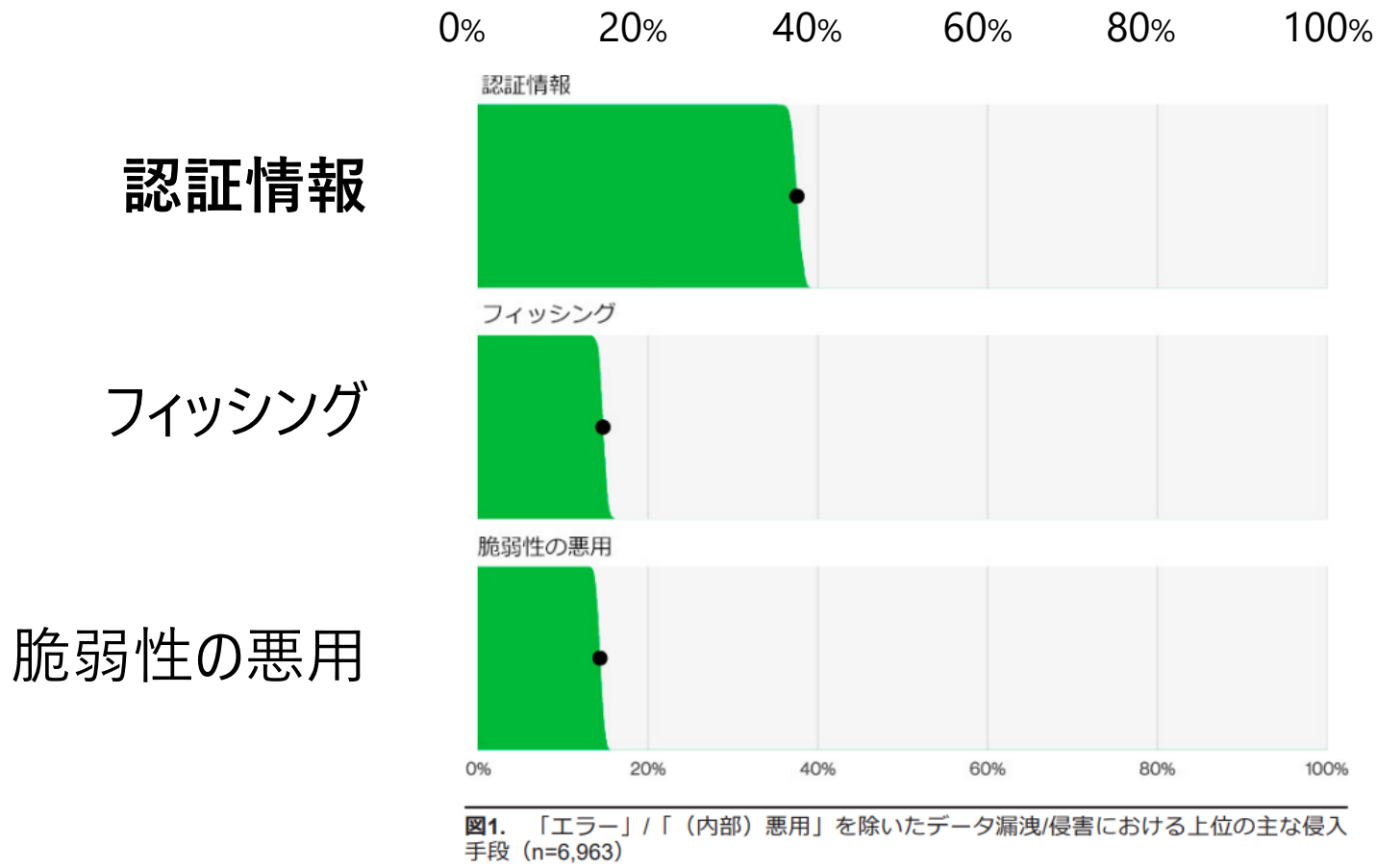


図1. 「エラー」/「（内部）悪用」を除いたデータ漏洩/侵害における上位の主な侵入手段（n=6,963）

(出所) ベライゾン「2024年度 データ漏洩/侵害調査報告書（DBIR）」

アクセス制御が重要

認証と認可について
理解しましょう

認証と認可とは？

認証と認可

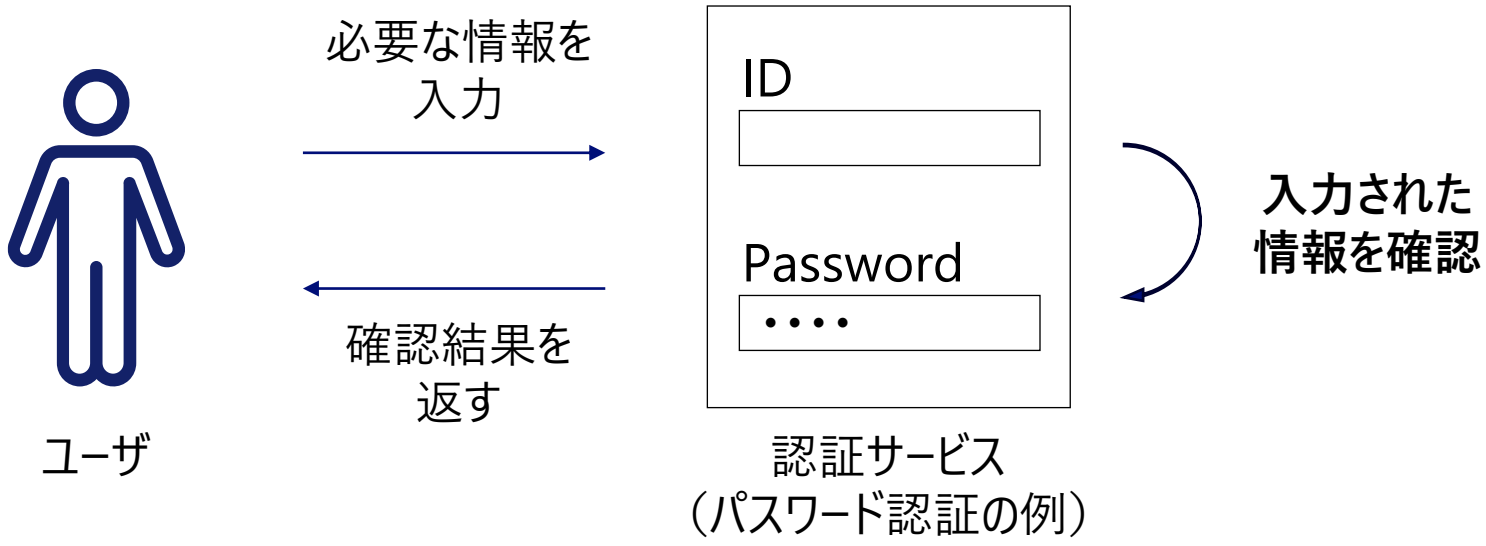
■認証と認可はセットで語られることが多いが別の概念である。

* (出所) https://www.amazon.co.jp/

認証とは。。。

認証：あなたは誰？本当に○○さん？

アクセスした人が本当にその人か確認すること



認証には色々な方法があり、組合せることでセキュリティが向上

■認証の種類

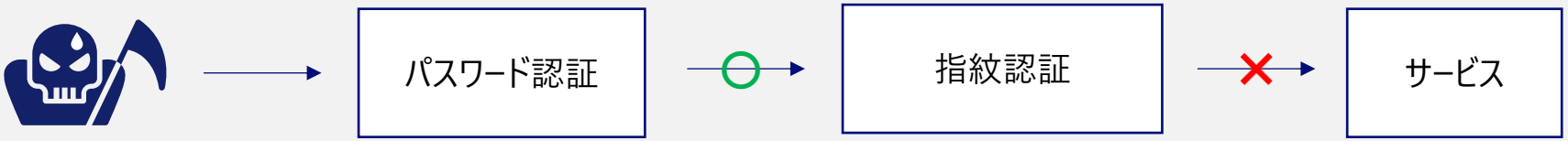
- 知識情報ベース
  - パスワードなど
- 生体情報ベース
  - 指紋や顔判別など
- 所持情報ベース
  - スマホのワンタイムパスワードなど

多要素認証

ID・パスワードなどの**知識情報**および、**所持情報**や**生体情報**という認証の3要素から、2つ以上の異なる認証要素を用いて認証する方法。

■認証を**多要素**にすることでセキュリティが向上する

ex. パスワードと指紋認証の多要素認証

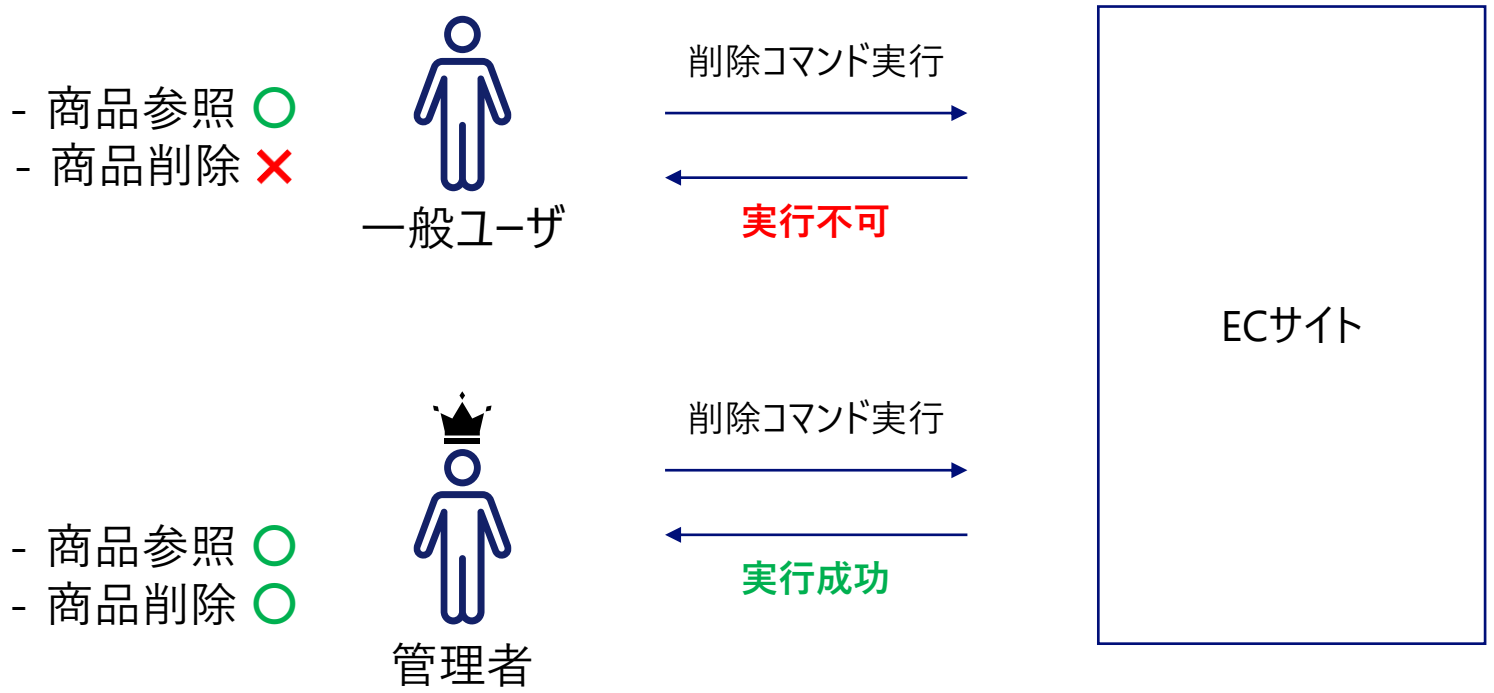


パスワードが漏れても指紋認証があるので不正アクセスを防ぐことが可能

認可とは。。。

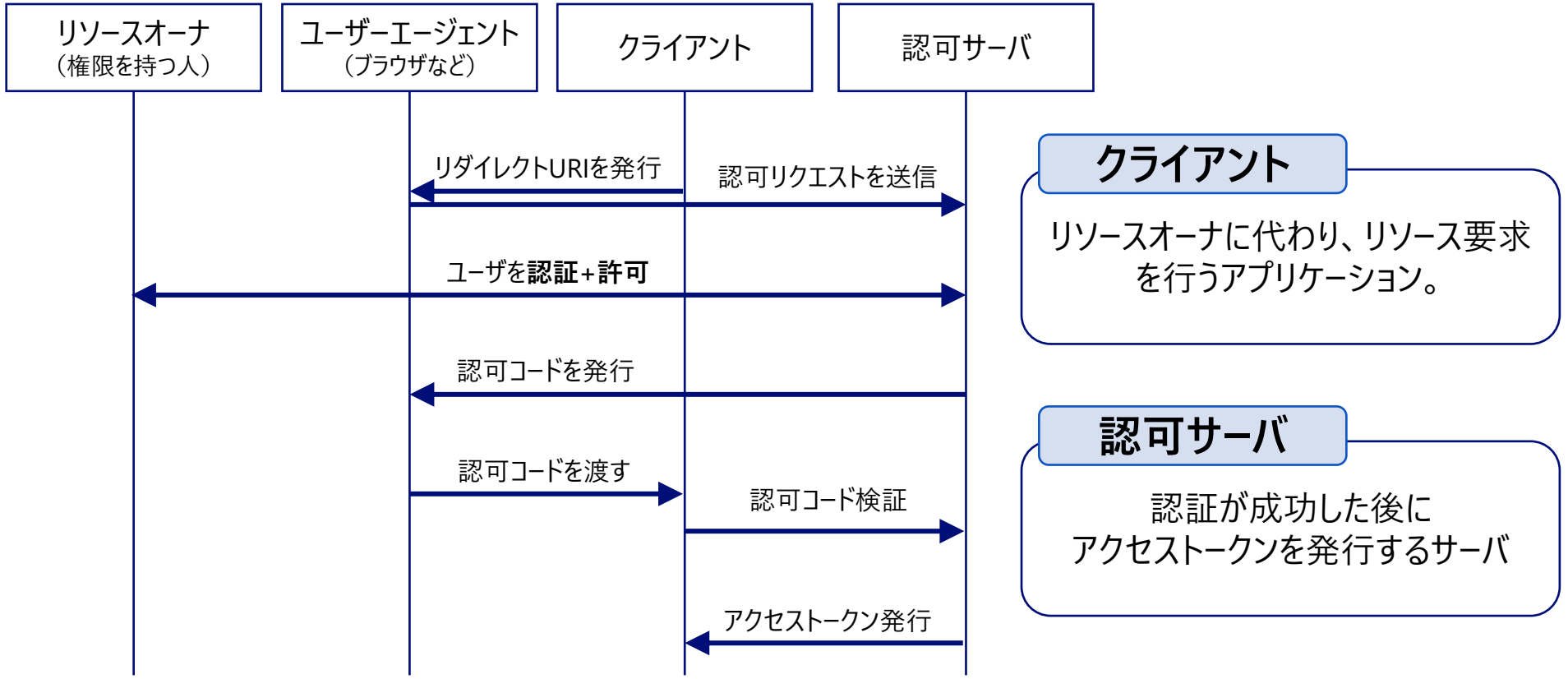
認可：○○さんはこのシステムで何ができる？

権限を持つ人だけがリソースを利用できるよう制御すること



認可の代表的な規格としてOAuth2.0がある。

■**アクセストークン**（チケットみたいなもの）をクライアントに対して発行する。
＝リソースオーナはクライアントに対してリソースアクセスを**認可**する。

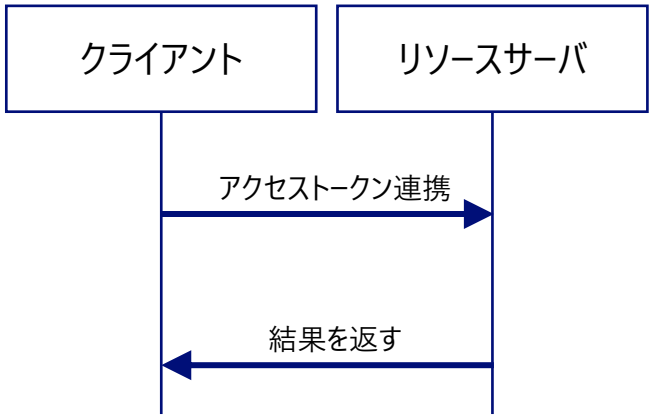


OAuth2.0の実行フロー（認可コードフローの場合）

認可の代表的な規格としてOAuth2.0がある。

■アクセストークンを受け取ったクライアントはリソースサーバにアクセス

■アクセスされたリソースサーバでアクセストークンを検証してクライアントを許可する。



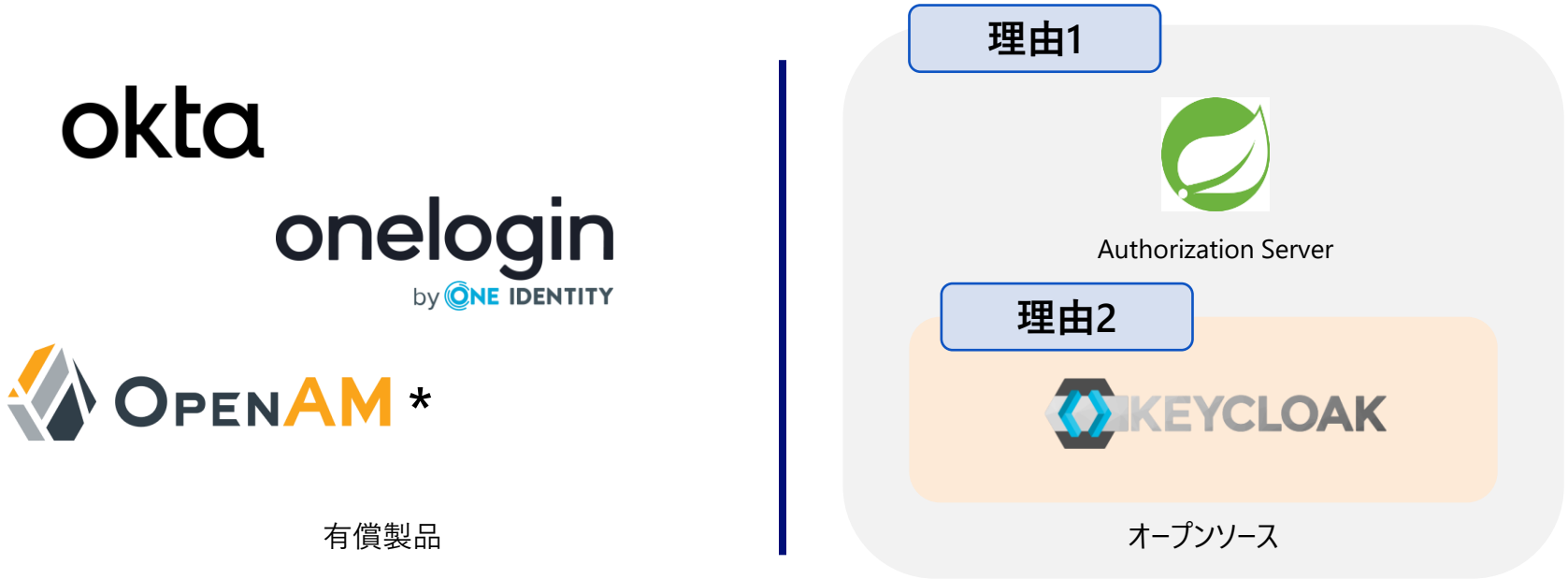
クライアントとリソースサーバ間のやり取り

Keycloakについて

認証認可を実現するサービスの中でもKeycloakは柔軟性や安定性に優れている

■認証と認可を実現するサービスの中でもKeycloakをハンズオンで採用する。

- 理由１：オープンソース（Apache Licence 2.0）であるため、カスタマイズ性が高い
- 理由２：長くメンテされているため安定している

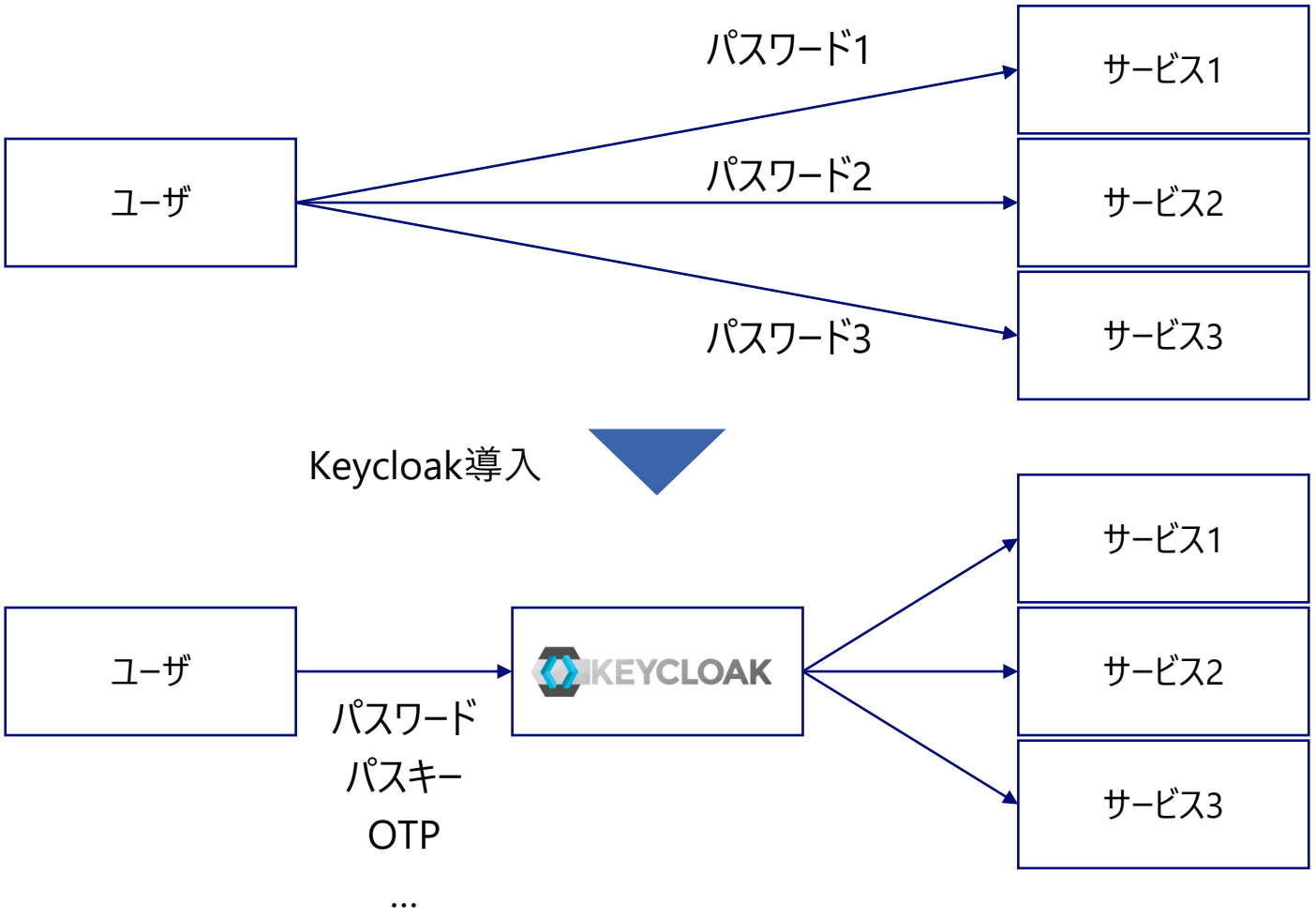


代表的な認証認可プロダクトの例

* 元はオープンソースだったが、ForgeRock社の方針で現在は有償

Keycloak：認証認可の機能を提供するオープンソースソフトウェア

■Keycloakは、**ID連携**や**アクセス制御**などの機能を実現できるJavaベースのオープンソースソフトウェア。



Keycloakのいいところ

- ID連携によるシングルサインオンが可能
- オープンソースソフトウェアでカスタマイズ性が高い
  - SPI（Service Provider Interface）の仕組みを利用
- 様々な認証方式に対応
  - パスワード認証、WebAuthn認証など。。
- マルチプラットフォーム対応
- CNCF傘下＝ベンダー中立なプロジェクト
- OAuth2.0やOpenID Connect、SAMLに対応

Keycloakのハンズオン

ハンズオンの流れ

- Keycloakのインストール
- Keycloakの管理者コンソール上で設定
  - レルム作成、クライアント追加、ユーザ追加
  - 認証フロー設定（多要素認証）
- OAuth2.0の挙動を確認してみる

ハンズオン

実演します

ハンズオンの全体感