# 高速化されたOpenLDAPの実力と OpenAMの多要素認証機能の活用

OSSTech

オープンソース・ソリューション・テクノロジ株式会社

2017年9月15日

技術取締役　武田 保真

お問い合わせ info@osstech.co.jp

# 目次

- OpenAM最新動向
- OpenLDAP最新動向

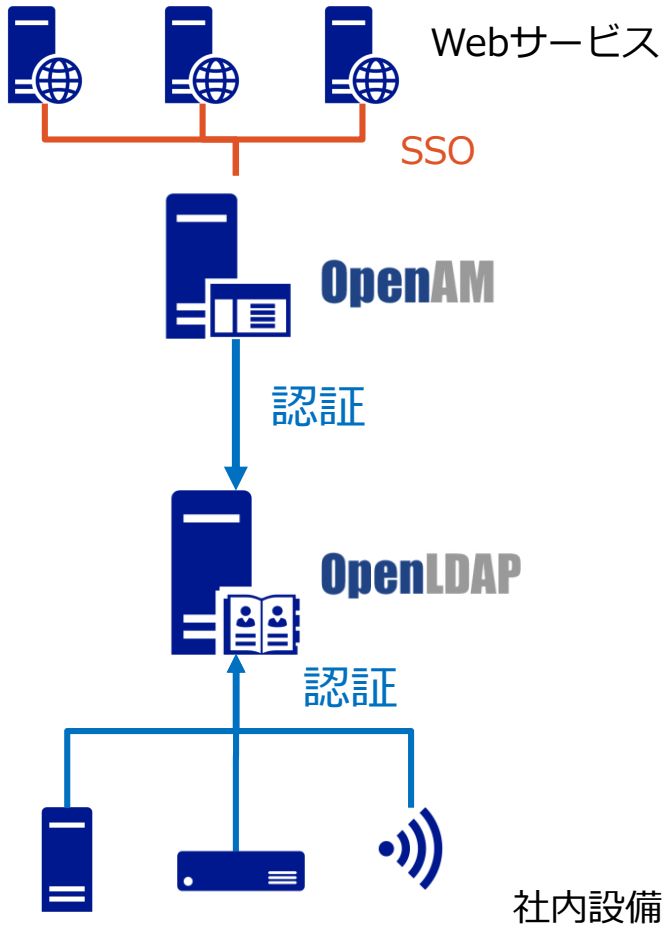
# OpenAMとOpenLDAP

## OpenAM

- OSSのシングルサインオン(SSO)サービス
- Webサービスなどの認証を統合
- SAML や OpenID Connectなどの
  認証連携（フェデレーション）に対応

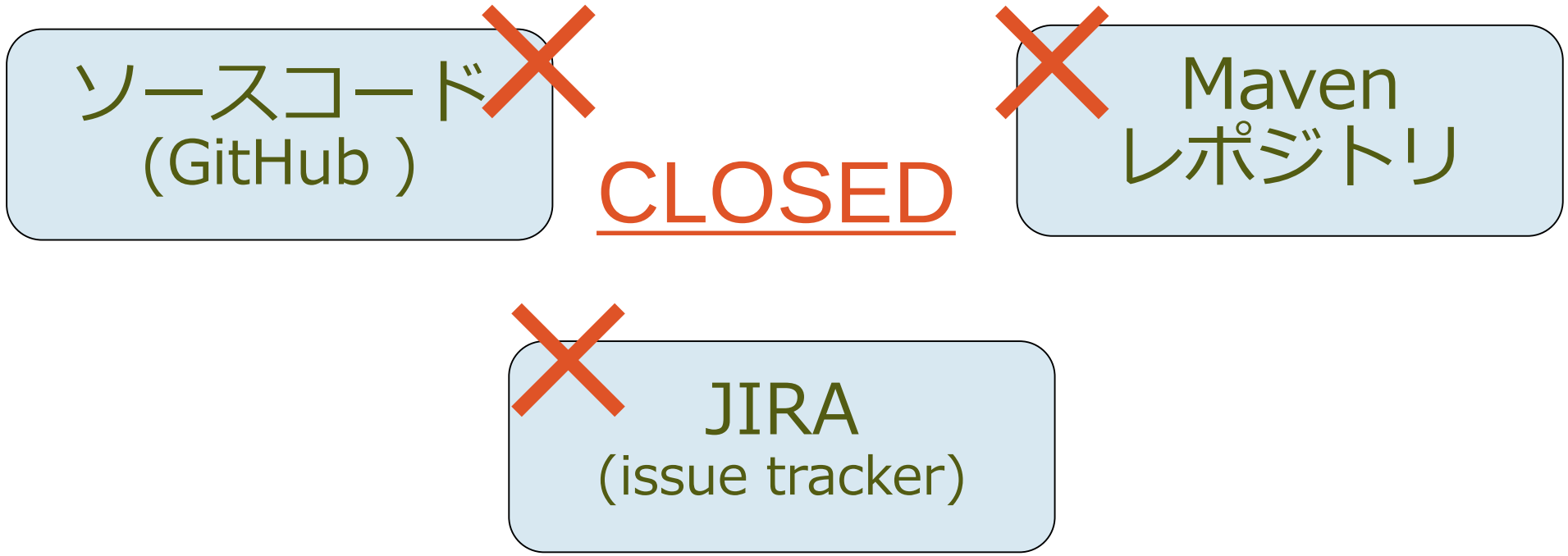
## OpenLDAP

- OSSのLDAPサービス
- ユーザー情報を保管し認証を行う
- LDAPに対応したサービスや機器が多い



# OpenAM 2017 Topics

- ForgeRockがソースコード公開ポリシーを変更
  - EOLの製品ソースコードのみを公開
    - 現在は OpenAM11系が公開対象



# OpenAMのFork

- ForkしたOpenAM
  - http://wrensecurity.org/
  - ソースコード(wren:AM)
    - https://github.com/WrenSecurity/wrenam

# OSSTechのOpenAMへの取り組み

- OSSTech版 OpenAMソース公開
  - OpenAM 13.0をベース
  - OSSTech版に適用しているパッチ込み

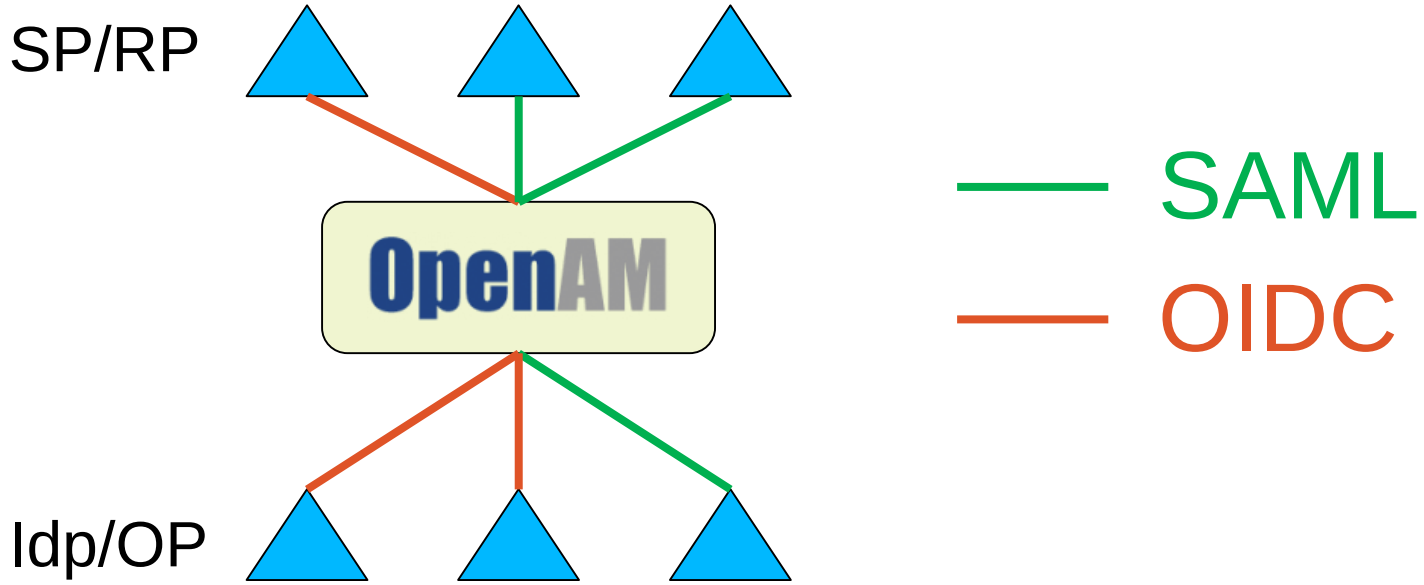
https://github.com/osstech-jp/openam

- OSSTech版 OpenAM評価版

お問合せ先：**info@osstech.co.jp**

# OSSTech の OpenAM最近のトレンド

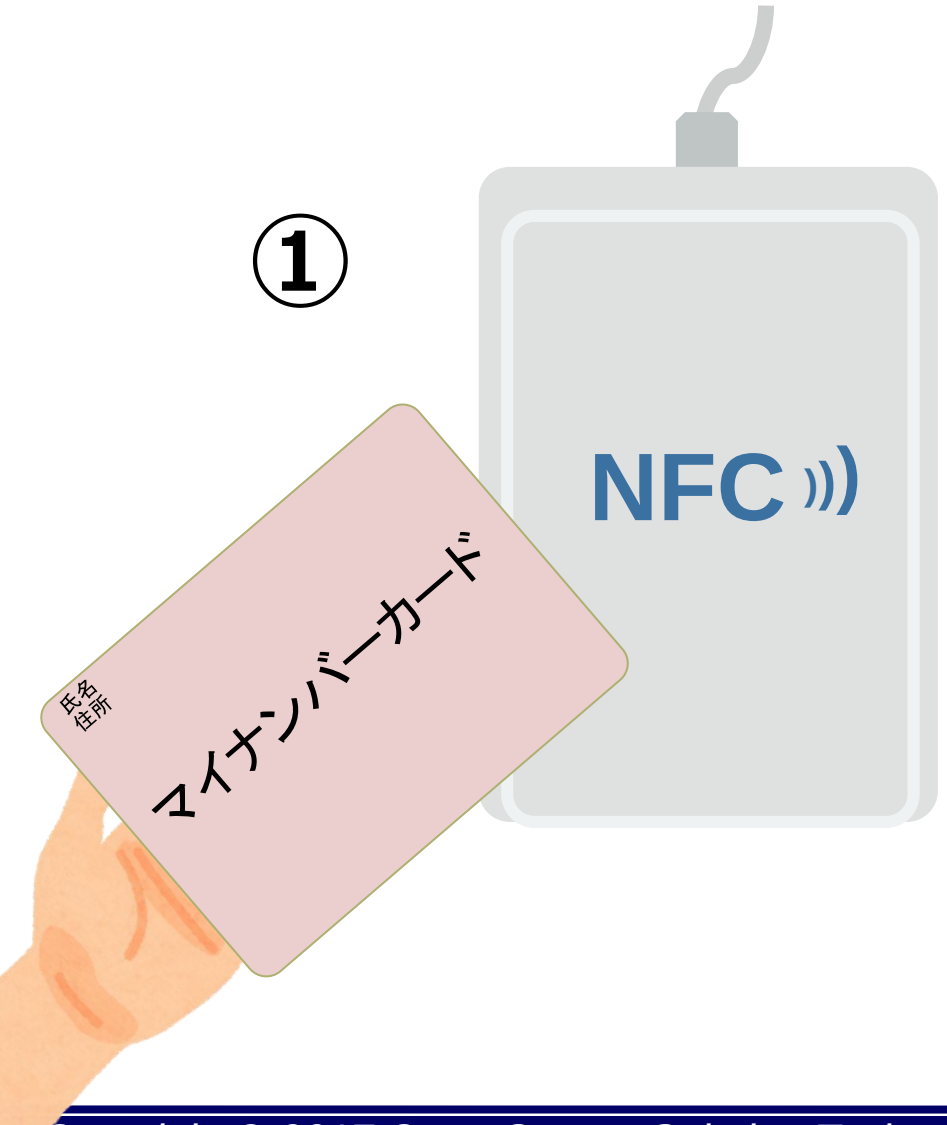
- 認証モジュールのカスタマイズ
  - ユーザーやシステムの要望に合わせた認証フロー
- プロトコルハブとしての利用形態

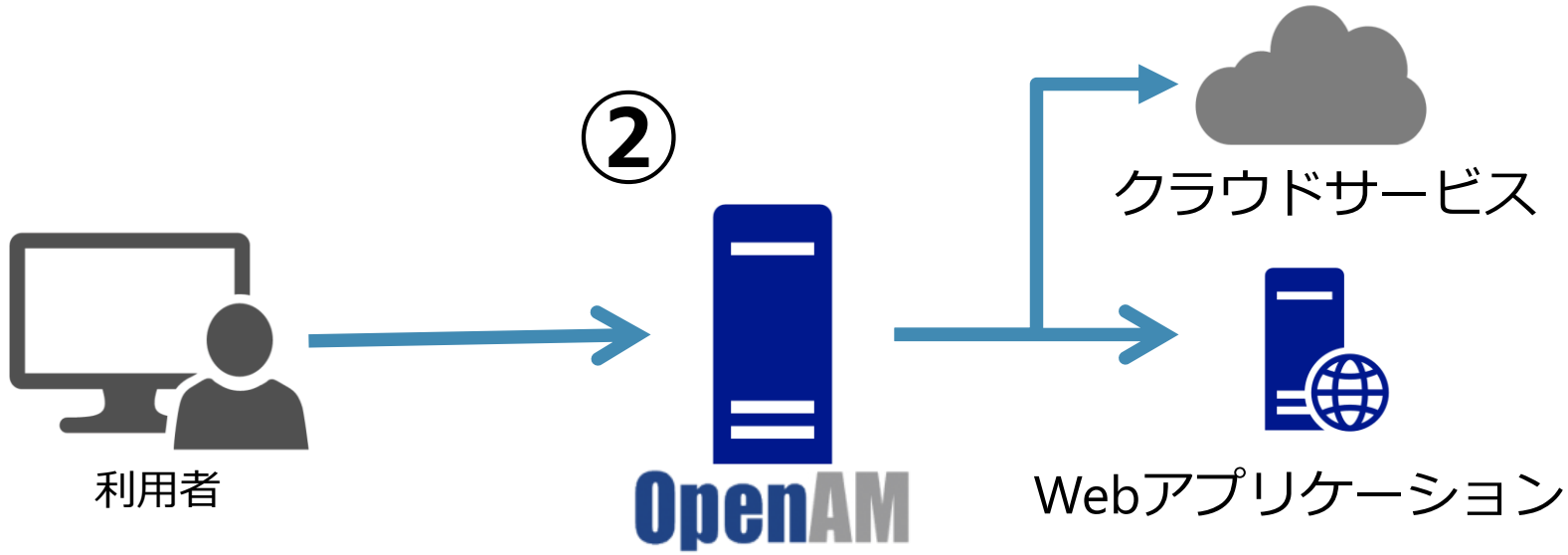


# JICS 2017 展示内容

- OpenAMデモ (技術検証内容を展示)
  - マイナンバーカードでクライアント証明書認証
  - OTPコードの通知をLINEで行おう

# デモ概要１：マイナンバーカードでクライアント認証




**事前準備：マイナンバーカードの認証用証明書の情報をOpenLDAPに登録＊**
**①ユーザーがNFCデバイスにマイナンバーカードをタッチ**
**②OpenAMで認証完了！**

**＊保存されている情報にマイナンバー情報は含まれません**

# マイナンバーカードでクライアント認証

- マイナンバーカードの構成
  - 署名用証明書 / **認証用証明書**
- OpenSCドライバによるマイナンバーカード対応
  - ブラウザの認証にマイナンバーカードを利用可能

**マイナンバーカードをクライアント証明書のインフラとして活用**

# OpenSCとは

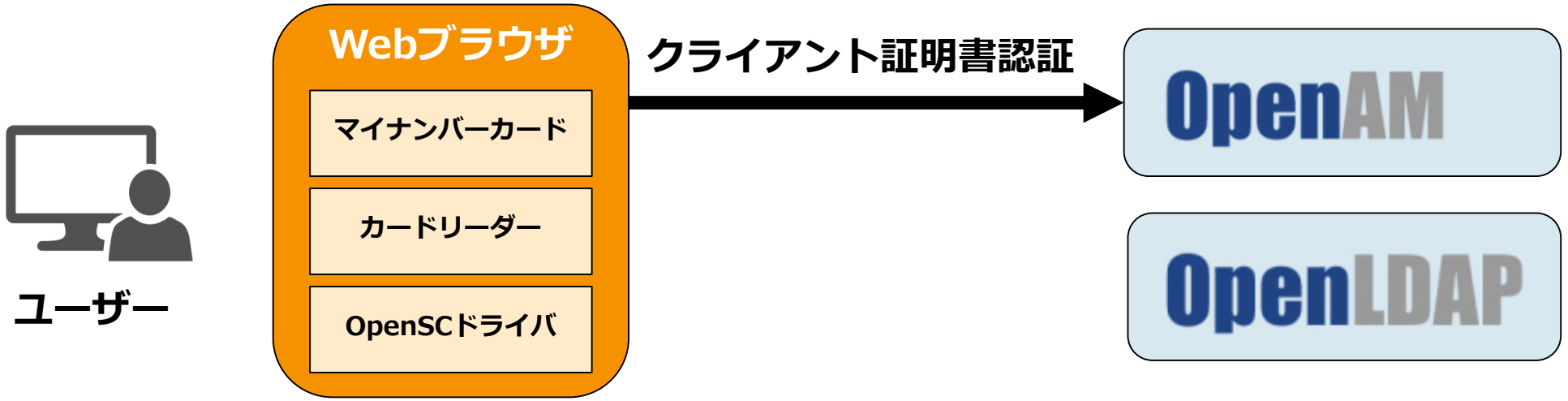
- クロスプラットホームで動作するスマートカード用の
  ツール・ライブラリ群
  - Windows / Mac / Linux など
  - Edge / Safari / Chrome / Firefox など

バージョン 0.17 にて JPKI ドライバとしてマイナンバーカードに対応済み

https://github.com/OpenSC/OpenSC/wiki

https://www.osstech.co.jp/~hamano/

# マイナンバーカードによる認証(構成)




**オープンソースのソフトウェアのみで構成可能**

# 認証の準備

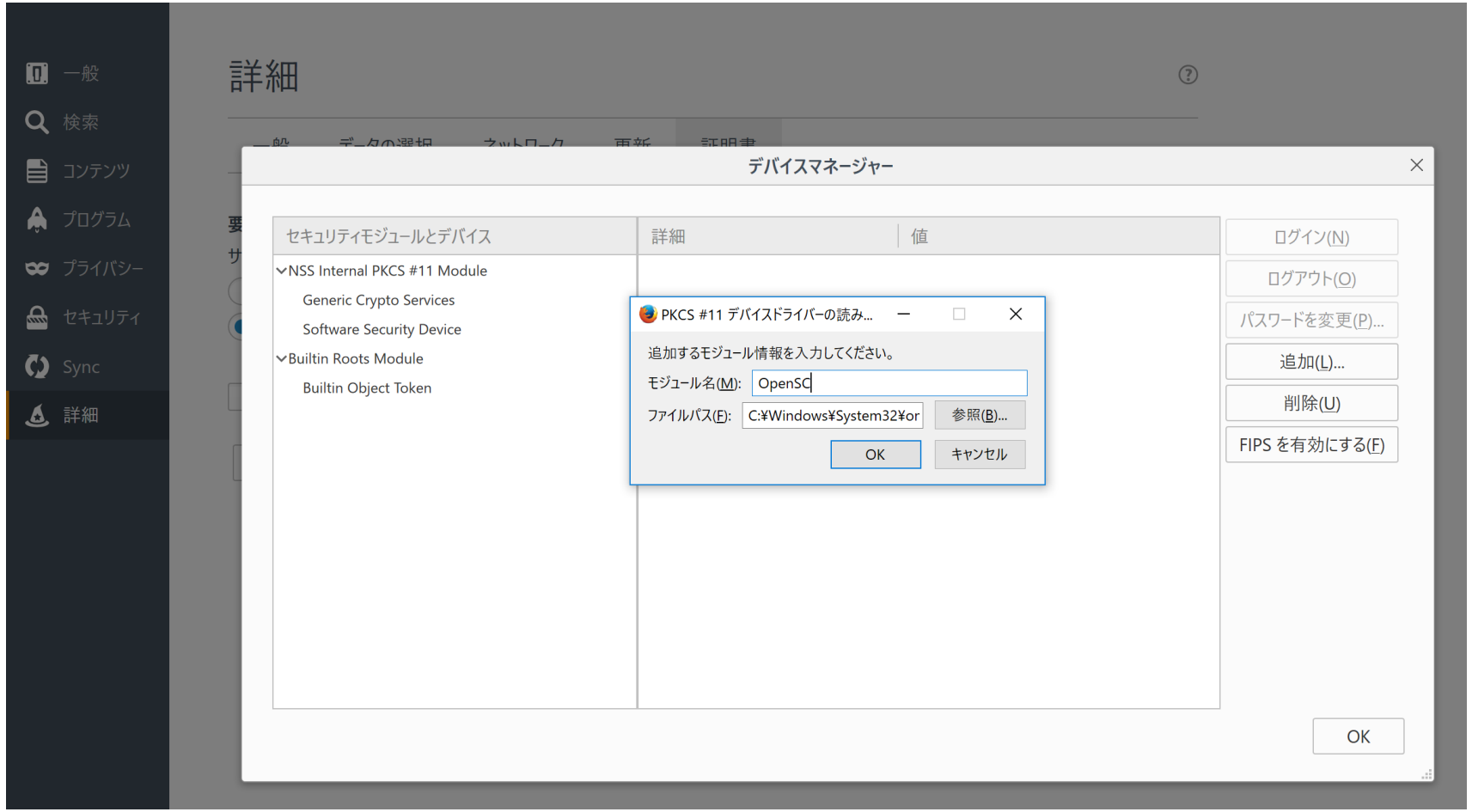
- マイナンバーカードに保存されている情報を事前登録
- 認証用証明書の登録、もしくはCNを事前登録
  - 保存されている情報にマイナンバーは含まれていません

# 事前準備 －Firefox－(1)

- 「セキュリティデバイス」の設定

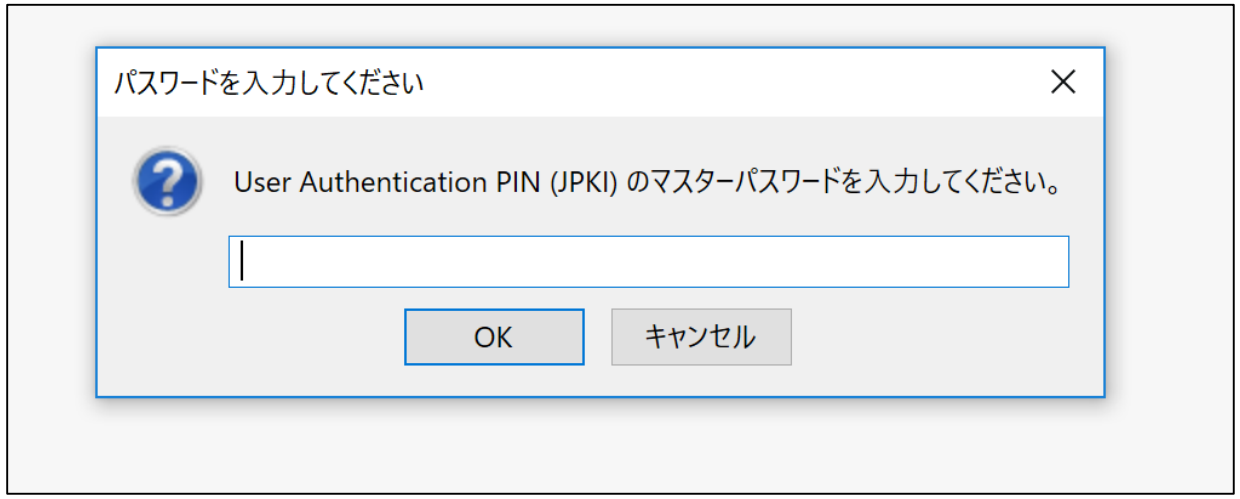
# 事前準備 – Firefox – (2)

- OpenSCデバイスを設定

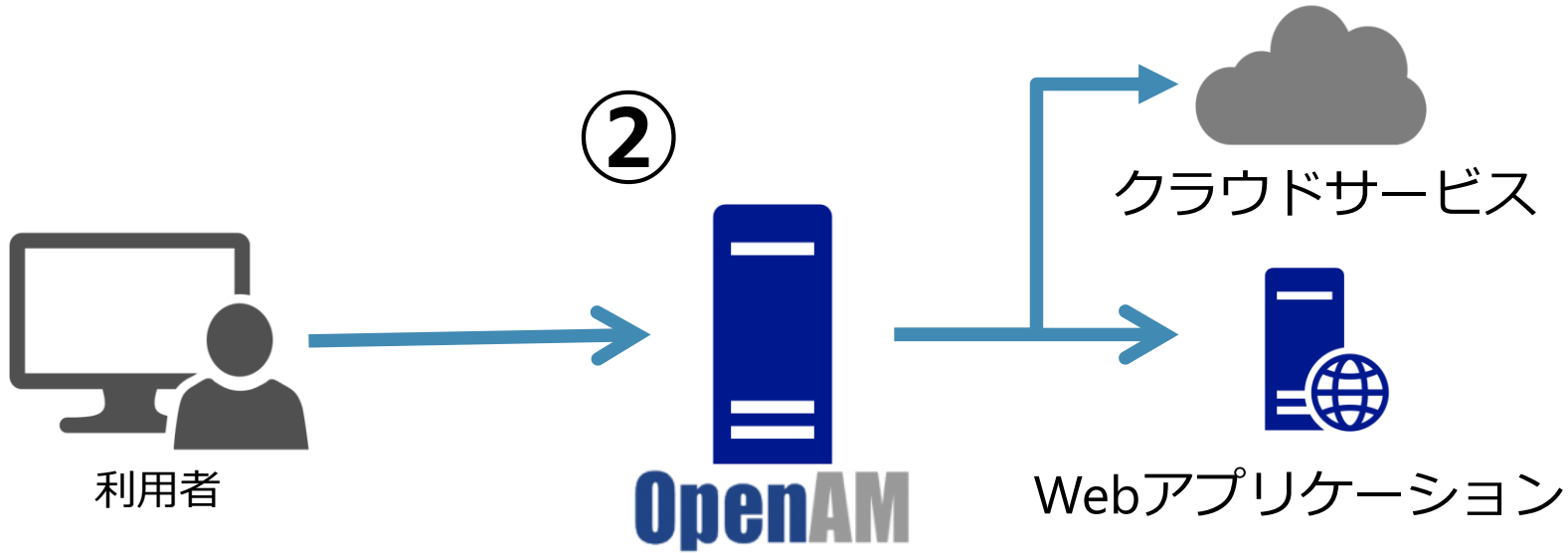


# マイナンバーカードによる認証

- 証明書認証が必要なサイトへのアクセス
  - PINコードの入力
  - 失敗は連続3回まで
    - 正しいPINコード入力でカウントクリア
    - ロックされた場合は役所で再設定手続き必要



# デモ概要２：LINE OTPモジュールで認証


**事前準備：初回ログイン時にLINE Notifyに連携登録**
**①ユーザーがID/パスワードで認証後、LINEにOTPを通知**
**②OpenAMで多要素認証完了！**

# OpenAM - LINE OTPモジュール -

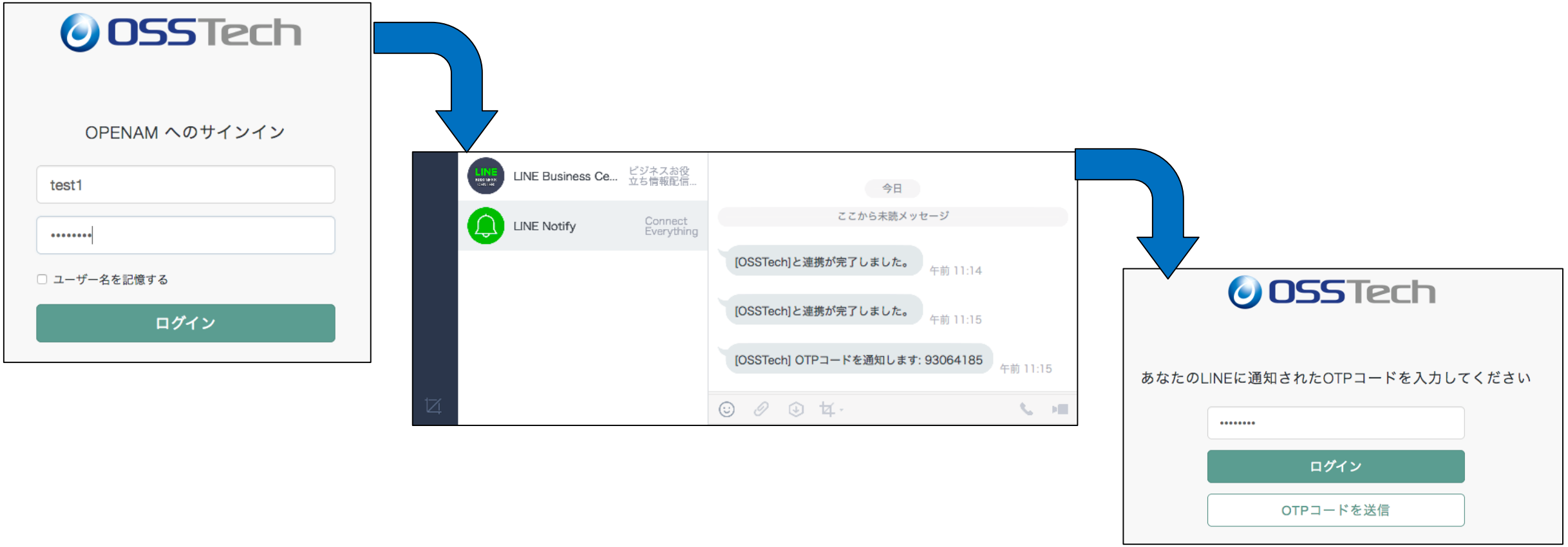
- 多要素認証
  - 低コストで利便性の高い方式
  - LINEによるOTPコードのユーザーへの通知
- LINE notify APIを利用
  - ユーザー単位のアクセストークン制限(1000回/h)

# OpenAM - LINE OTPモジュール (2) -

初回ログイン時にLINE notifyに登録

# OpenAM - LINE OTPモジュール(3) -

2回目以降のログインはLINE にOTPコード通知



# OpenLDAP 2017 Topics

OpenLDAP

- OpenLDAPの開発状況
  - OpenLDAP 2.4 (安定版)
  - OpenLDAP 2.5 (開発版)　…　リリースプランは未定

- 最近のお客様の傾向
  - SHA2/PBKDF2利用の増加　……　パスワード漏洩対策
  - 商用LDAPサービスからの移行　……　機能・性能・コストで比較

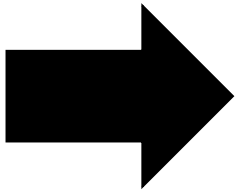
- RHEL7.4 openldap-serversパッケージが deprecated
  - OSSTech版OpenLDAPへ**移行可能**

# OSSTech版OpenLDAPの改良

- 課題
  - BerkleyDB(BDB)のライセンス問題
  - 大規模環境におけるBDB(更新系)の限界
- Community
  - LMDBの開発
- OSSTech
  - WiredTigerバックエンドの開発
    - OpenLDAP 2.5への**取り込み完了**

# OpenLDAP大規模環境における問題点

- エントリ数の増加に対する更新時間の増大
- 一括データ投入時間
  - 初期投入、リストア時
- 更新頻度の高い環境
  - ログイン時刻の記録など



更新性能に起因する
設計・運用上の制約

# WiredTiger DBの特長

- ファイルベース Database
- マルチコア、大容量メモリ対応
- ロックフリーのアルゴリズム
  - Core数の増加に応じた更新性能向上
- コア開発者は元BDB開発者
  - BDBの問題点を解消

# WiredTigerバックエンドの制約

- slapd実行中のslapcat 不可
  - データエクスポートはldapsearchを利用
- OpenLDAP 2.5の開発ソースのみで利用可能

# OpenLDAPベンチマーク

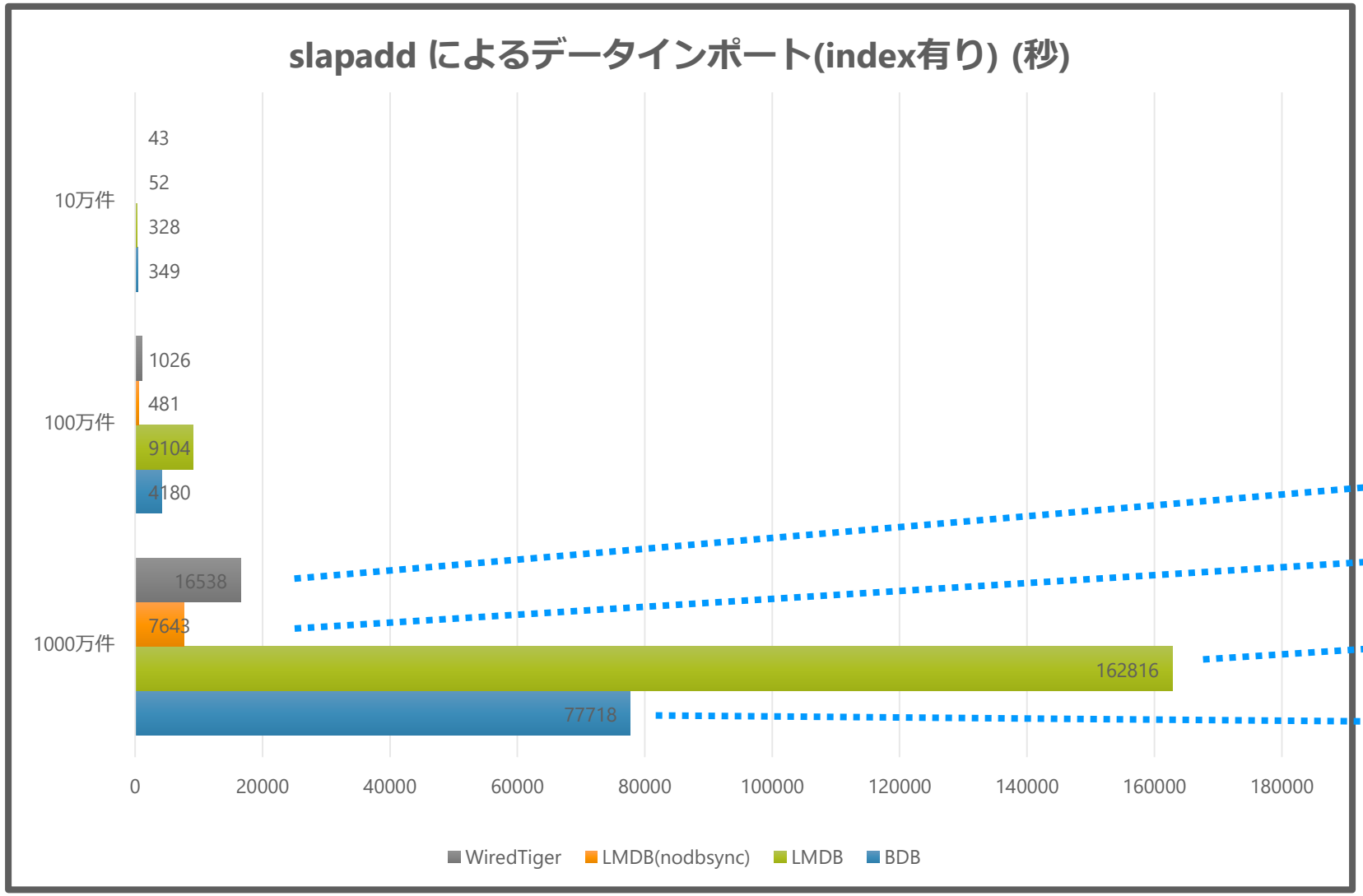
## 測定環境

- CentOS 7 / OSSTech版 OpenLDAP 2.4.45
- CPU 24core / メモリ 10GB / SAS HDD (KVM 仮想ゲストOS)

## LDAPサンプルエントリ

```
dn: uid=user1,ou=Users,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: inetOrgPerson
objectClass: posixAccount
uid: user1
cn: user1
sn: testuser
givenName: user1
uidNumber: 100000
gidNumber: 1000
userPassword: {SSHA}u9sXy3bV21JWPwyfysqdDEkXfO/uuPAE
homeDirectory: /home/user1
loginShell: /bin/bash
```

# OpenLDAPベンチマーク(１)



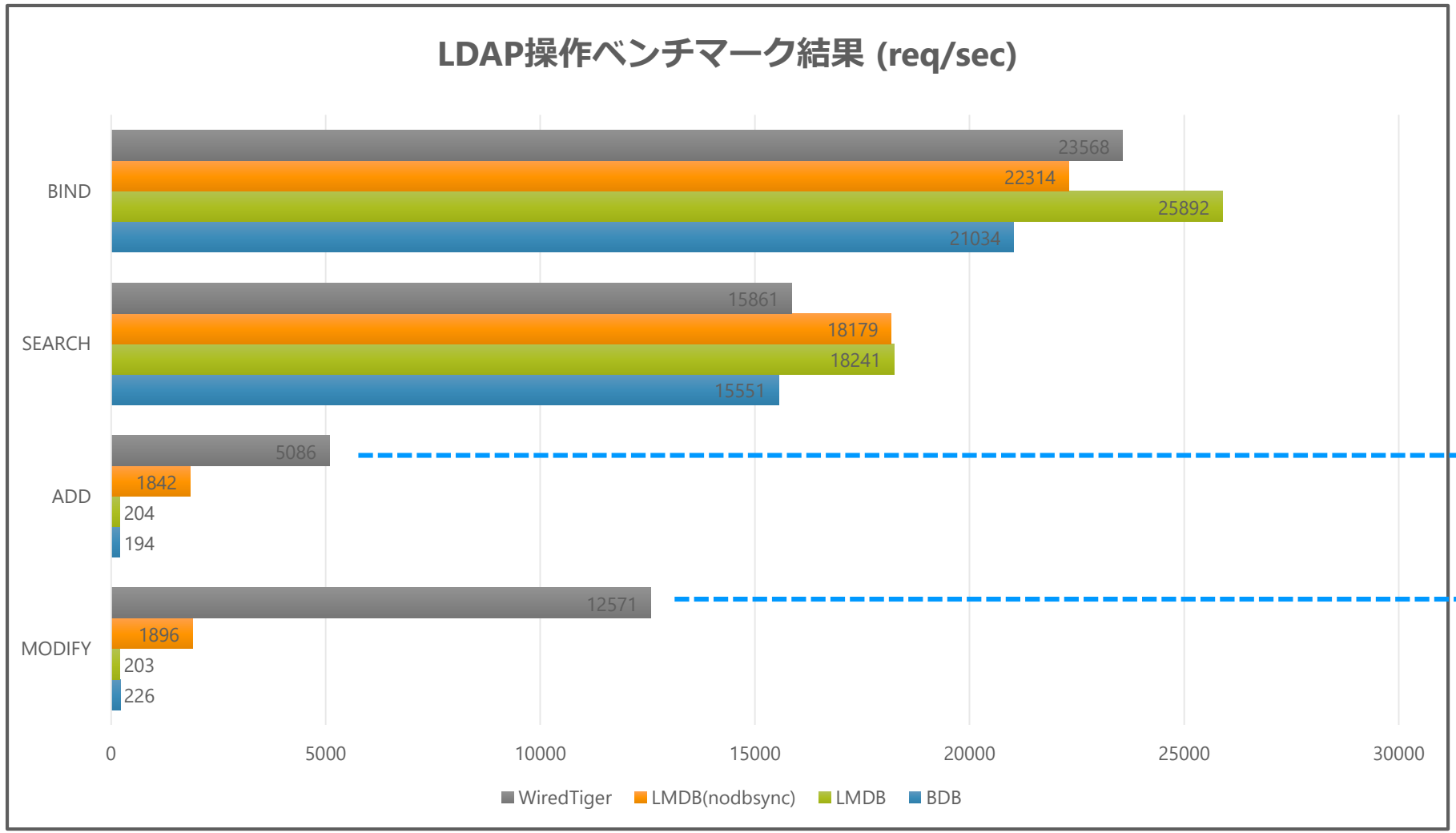

WiredTiger　　：4時間

LMDB(nodbsync)：2時間

LMDB(default)　：45時間

BDB　　：21時間

# OpenLDAPベンチマーク(2)




5086件/sec

12571件/sec

# ベンチマーク結果 サマリー

- 参照性能
  - どのデータベースを選択しても大差はない
- 更新性能
  - WiredTigerバックエンドが優秀
    - 更新が多いシステム
    - 大量エントリ(100万件以上)を管理するシステム

# OSSTech版 OpenLDAP 2.4

- WiredTigerバックエンド対応版の提供開始
  - 対応OS: RHEL7 / CentOS 7
  - OSSTech版 OpenLDAP2.4パッケージに機能追加
  - BDBからエクスポート・インポートで切り替え可
  - パートナーサイトから評価版提供開始
    - 評価版希望の場合は、お申込みを

# LDAPcon2017への参加

- ベルギー ブリュッセルで 10月に開催
- OpenLDAPのmrubyバックエンドについて発表予定

https://ldapcon.org/2017/

# 協業パートナー募集のお知らせ

- ユーザーフレンドリーな認証フローや、多要素認証の実現をお手伝いします
- IDaaSやSaaSといったOSSTech社のサービス提供予定はございませんので、パートナーの皆様のサービスの実現に弊社製品をご活用ください

お問合せ先：info@osstech.co.jp

# 告知：11/1にプライベートセミナーを開催します


先着30名様のプライベートセミナー！

OpenAM/OpenLDAPの最新情報をお伝えします。

お申込みはお手元のチラシに記載のメールアドレス

もしくは展示会場でも受付いたします。

OSSTech

「オープンソースソフトウェア」の新しい価値を創造し、高機能・高品質を追求する

統合認証　シングルサインオン　アイデンティティ管理ソリューション