OSSTech版 OpenAM 11紹介

技術力と経験でソースコードを磨いた日本版製品

オープンソース・ソリューション・テクノロジ株式会社

代表取締役 チーフアーキテクト 小田切耕司

お問い合わせ info@osstech.co.jp

OSSTech

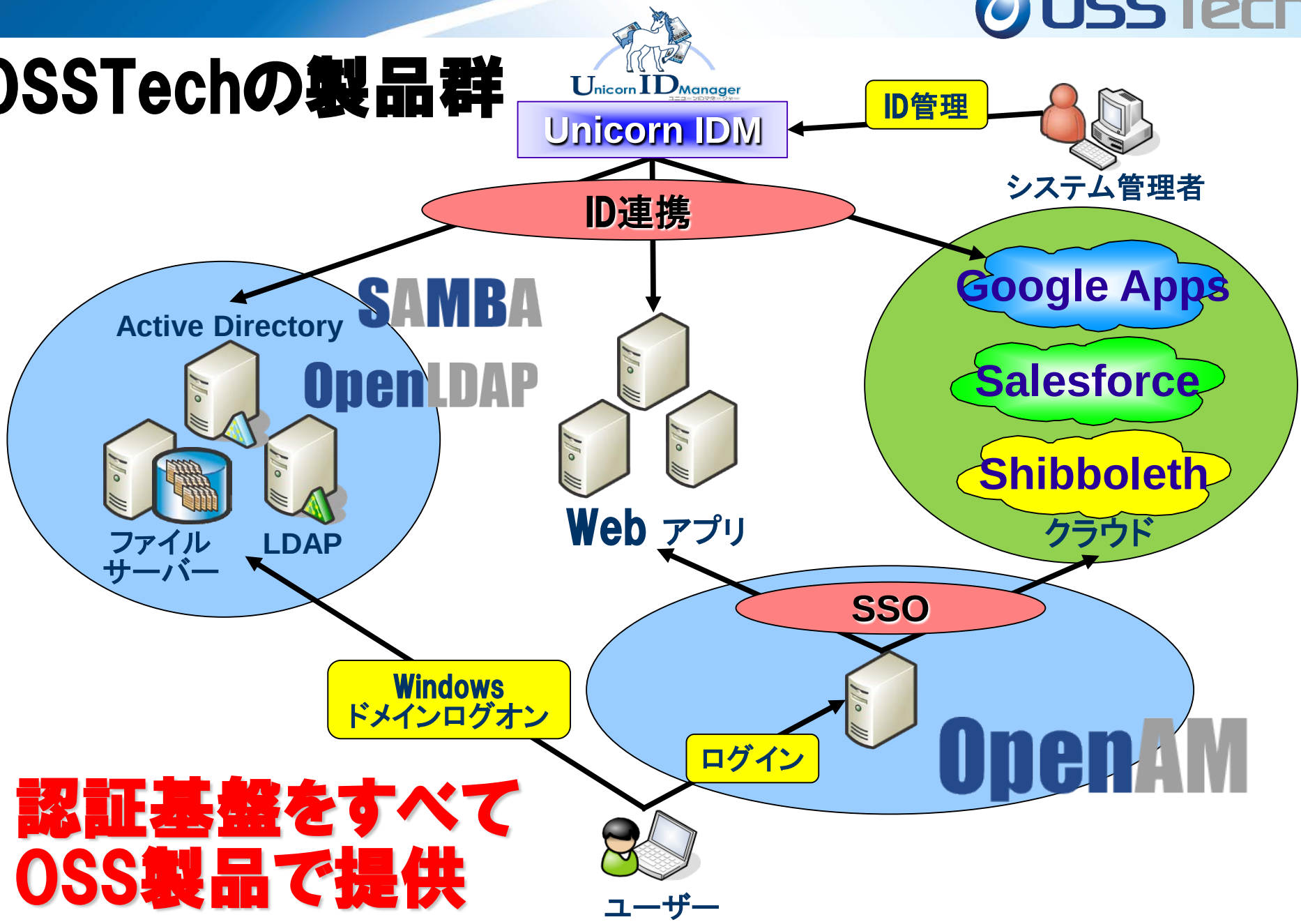
オープンソース・ソリューション・テクノロジ株式会社

「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

- **OSに依存しないOSSのソリューションを中心に提供**
  Linuxだけでなく、AIX, Solaris, Windowsなども対応！
- **OpenAM, OpenLDAP, Sambaによる認証統合／シングル・サイン・オン、ID管理ソリューションを提供**
  - 製品パッケージ提供
    機能証明、定価証明が発行可能
  - 製品サポート提供
    5年以上の長期サポート
    コミュニティでサポートが終わった製品のサポート
  - OSSの改良、機能追加、バグ修正などコンサルティング提供

OSSTechの製品群



認証基盤をすべて
OSS製品で提供

OSSTechの製品群(すべてOSSで提供)
Linux/AIX/Solaris版すべてRPMで提供

- OpenAM
  - Tomcat, OpenLDAP対応で高機能なシングルサインオン製品
- OpenLDAP
  - 認証統合、ディレクトリサービス、シングルサインオンのインフラ
- Samba
  - Active Directoryの代替、高性能NAS(CIFSサーバー)の代替
- Unicorn ID Manager
  - Google Apps, Active Directory, LDAP, Sambaに対応した統合ID管理製品
- ThothLink
  - WebブラウザからのWindowsファイルサーバアクセス機能を提供

OpenAM 11
新機能紹介

OSSTech

OpenAM 11新機能

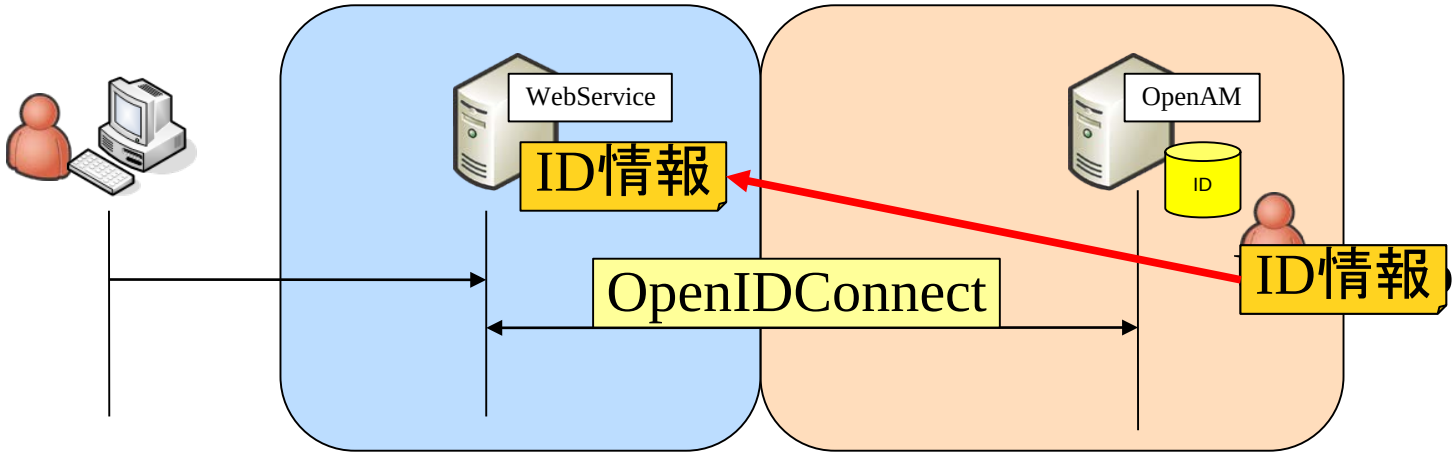
- OpenID Connect 1.0対応
- OAuth 2.0 Client/Resource Server 対応
- コアトークンサービス
  - 新セッションフェイルオーバー
- OATH(Open Authentication)
- Java 7対応
- JSON REST API
- etc.

Federation 認証連携プロトコル対応強化

	OpenAM 10		OpenAM 11	
	SP (RP)	IdP (OP)	SP (RP)	Idp (OP)
OpenID Connect1.0	×	×	×	○
OAuth2.0	○	×	○	○
SAML2.0	○	○	○	○

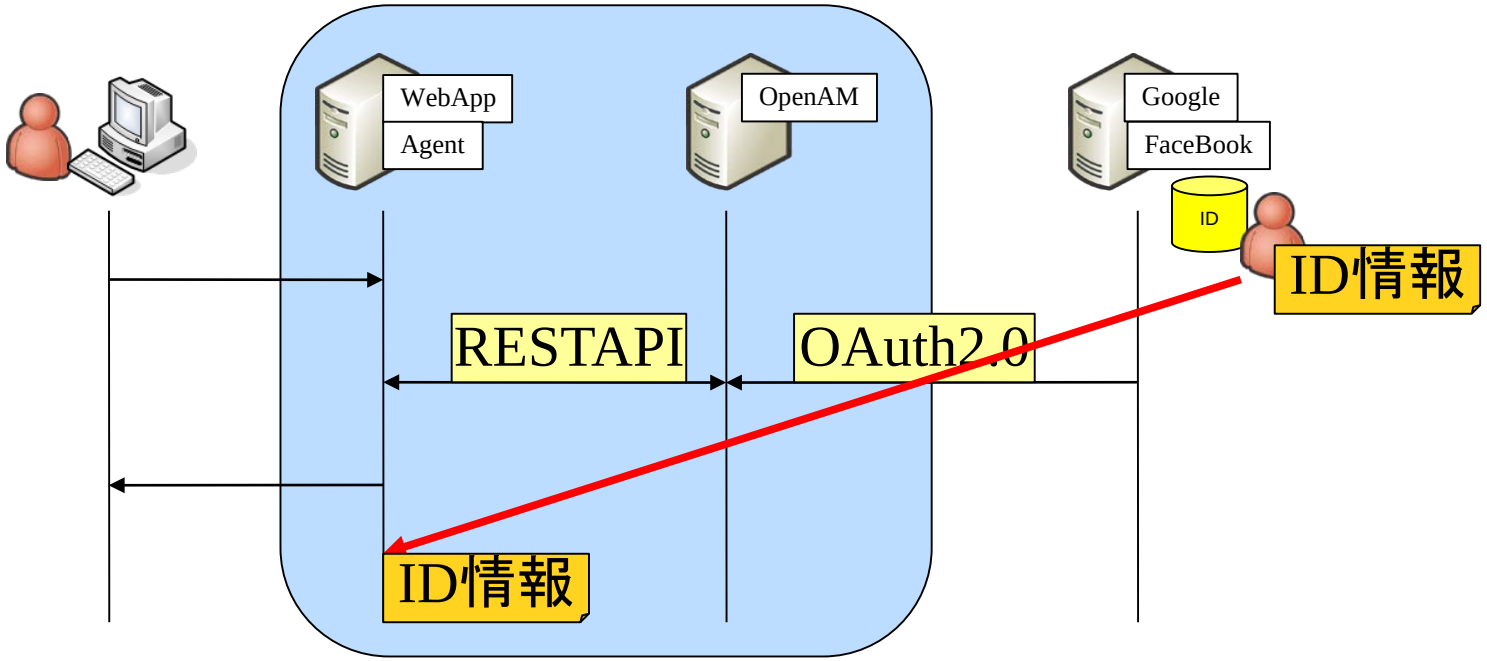
OpenID Connect1.0対応

OpenAMをID情報のエンドポイントとして利用可能
Client(WebService)へOpenAMの ID情報 を提供



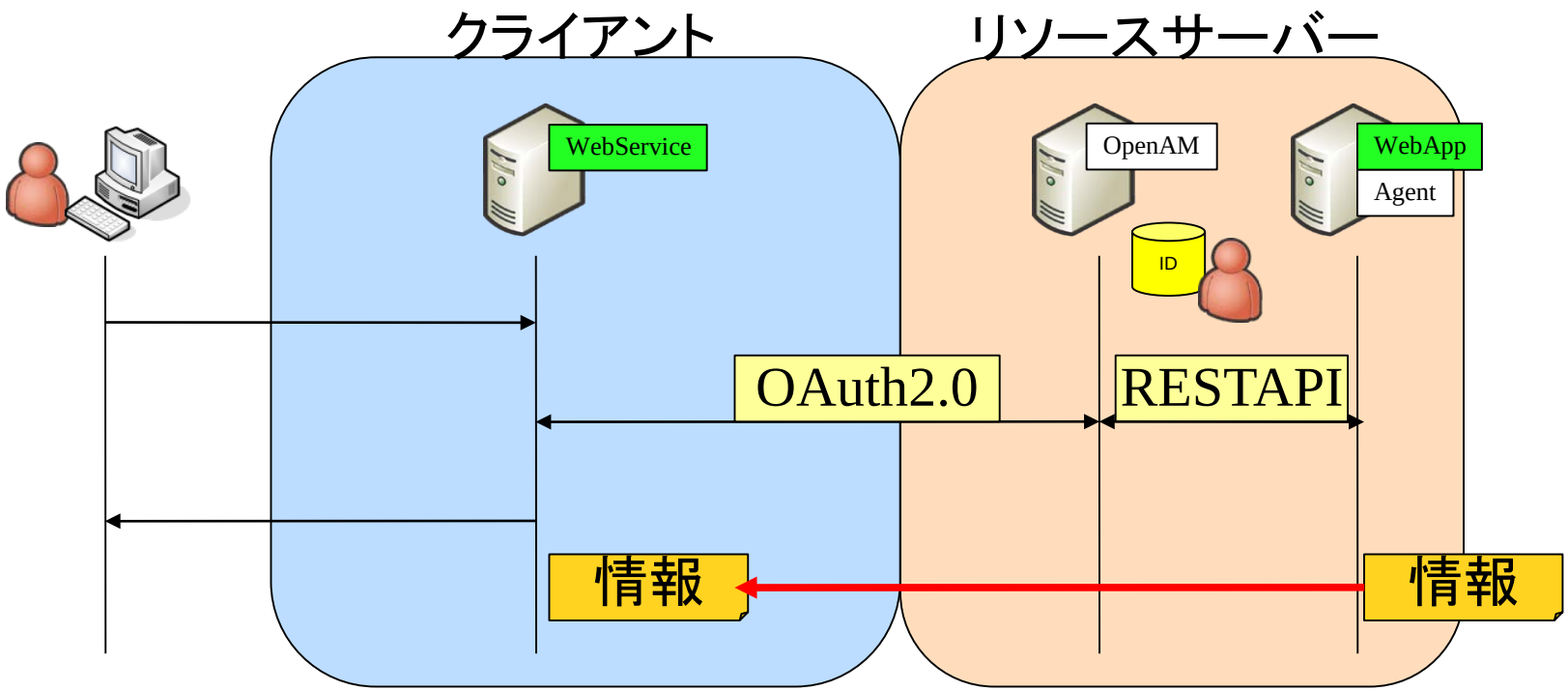
OAuth2.0対応 OpenAM 10

OAuth2.0 クライアントとしてOpenAMを利用例



OAuth2.0対応 OpenAM 11

OAuth2.0 リソースサーバーとしてOpenAMを利用例

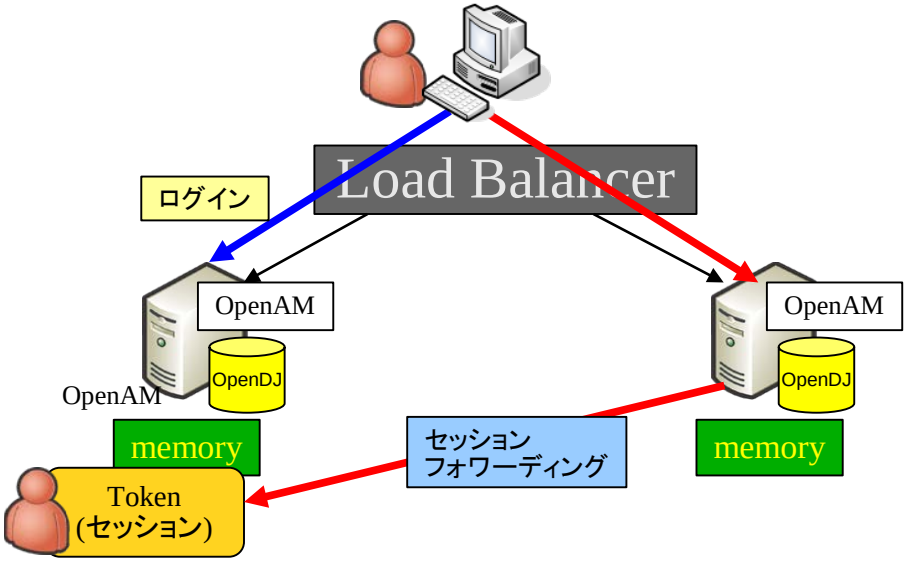


コアトークンサービス

- 内蔵OpenDJにセッション情報（Token）を格納
- 外部OpenDJも利用可能

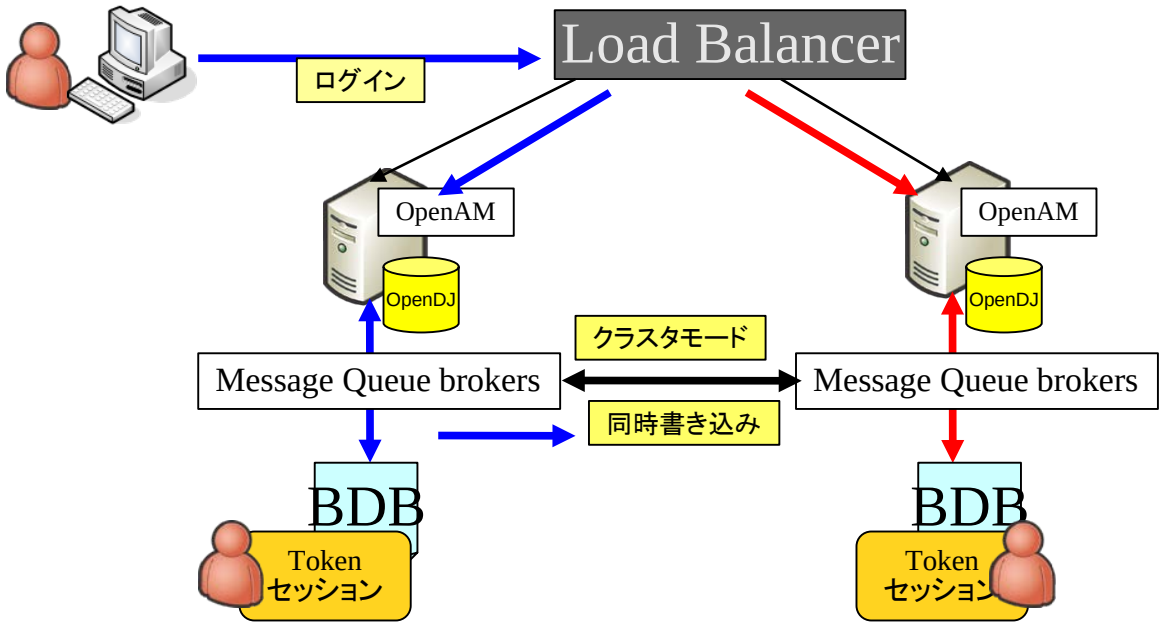
セッションフェイルオーバー

- 9.xまでの非FO構成
- セッションフォワーディングにより実装
- ログインセッション側のOpenAMが再起動すると再ログインが必要



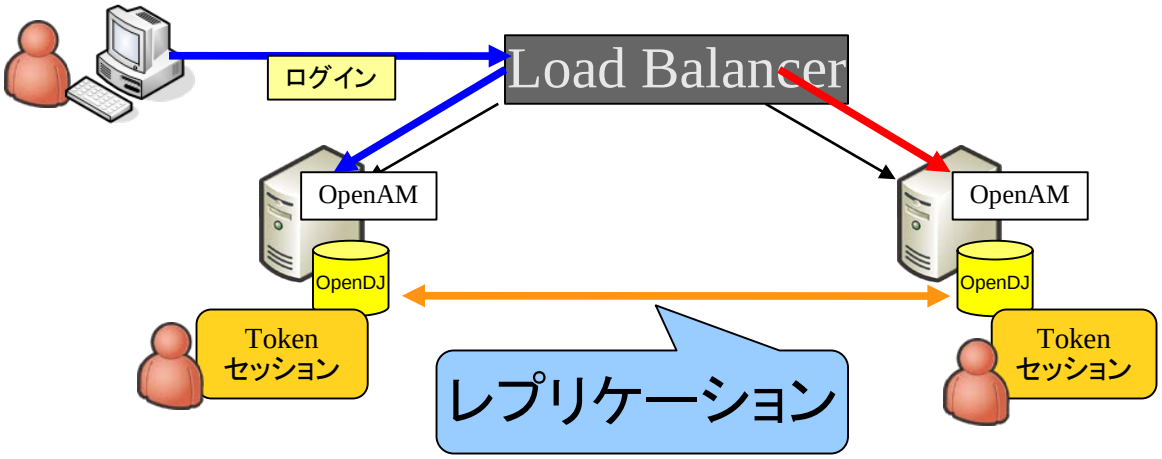
セッションフェイルオーバー

- 9.xまでのFO構成
- MQBとBDBによるセッションの共有化
- セットアップが煩雑で障害ポイントも多い



セッションフェイルオーバー

- コアトークンサービスを利用
- セッションはOpenDJに格納、レプリケーション
- セットアップの容易さと確実性



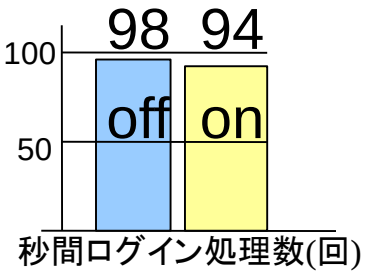
セッションフェイルオーバー

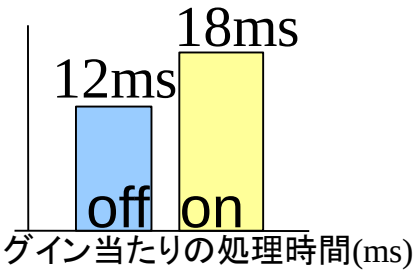
- 長時間（24hr）の負荷検証を実施
- OpenDJへの書き込みオーバーヘッドは？
- 処理遅延は？

CPU 3.2GHz 2core Memory 4GB 15,000ユーザーをランダムにログインさ
処理遅延は6ms程度。約5%の処理低下に抑えられてる。

FailOver On

FailOver Off



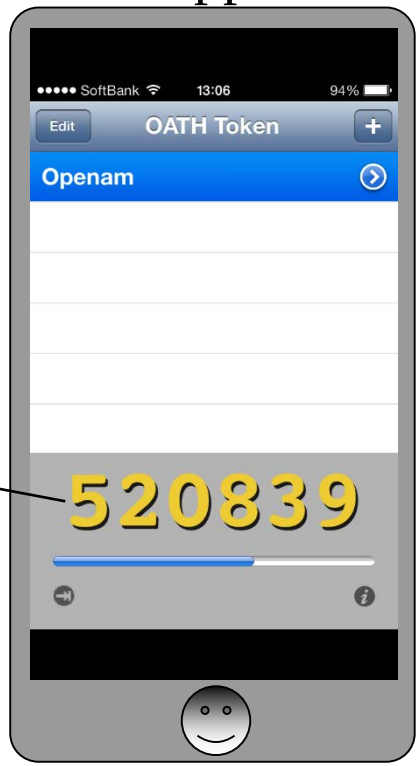


	秒間処理数	処理時間	CPU利用率	MEM利用率	I/O利用率
FailOver On	93.8/s	18ms	18%	46%	4%
FailOver Off	97.9/s	12ms	10%	26%	1%

OATH 認証モジュール

- Open Authentication
  - オープンなワンタイムパスワード認証
  - HOTPとTOTP

iPhone Appを利用した例



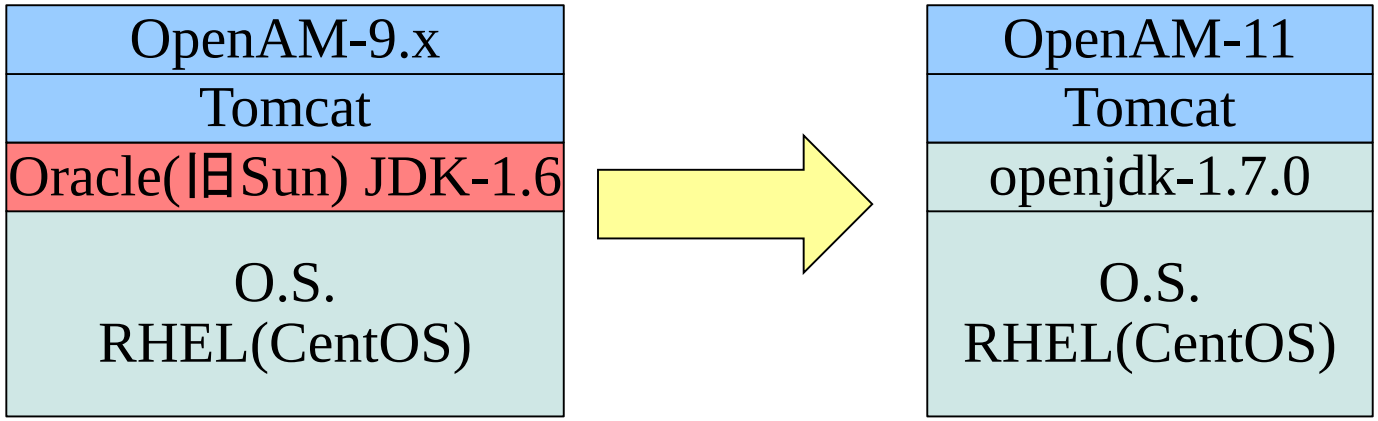
OATH 認証モジュール

- YubiKey authentication
  - トークン入力を代替え、より長いトークンが使える
  - USBポートに刺すことによりキーボードとして動作
  - ボタンを押せばトークンを送信

YubiKey

Java 7 完全対応

- OSSTech版ではopenjdk-1.7.0で検証し、対応



その他

- JSON RESTAPI
- IPv6フル対応
- OpenDJ 2.6同梱
- セキュリティ向上
  - ゼロページログインの無効化
- 運用性向上
  - 持続性Cookie
  - ssoadm コマンドでの設定・運用を自動化

OSSTech版 OpenAM 11の特長

OSSTech

OSSTech版の特長

- RPMパッケージ化
- OpenLDAP対応強化
  - 専用データストア設定
  - 持続検索(パーシステントサーチ)
  - パスワードポリシー
- マトリックス型認証
- 携帯端末用CSS
- 不具合修正

RPMパッケージ化

- Tomcat-7を含めたRPMパッケージ群
- rpmコマンドでだけでインストール可能

```
# yum install java-1.7.0-openjdk
# rpm -ivh osstech-tomcat7-*.el6.noarch.rpm
# rpm -ivh osstech-openam11-*.el6.noarch.rpm
```

- あとは、serviceコマンドでTomcatを起動するだけ

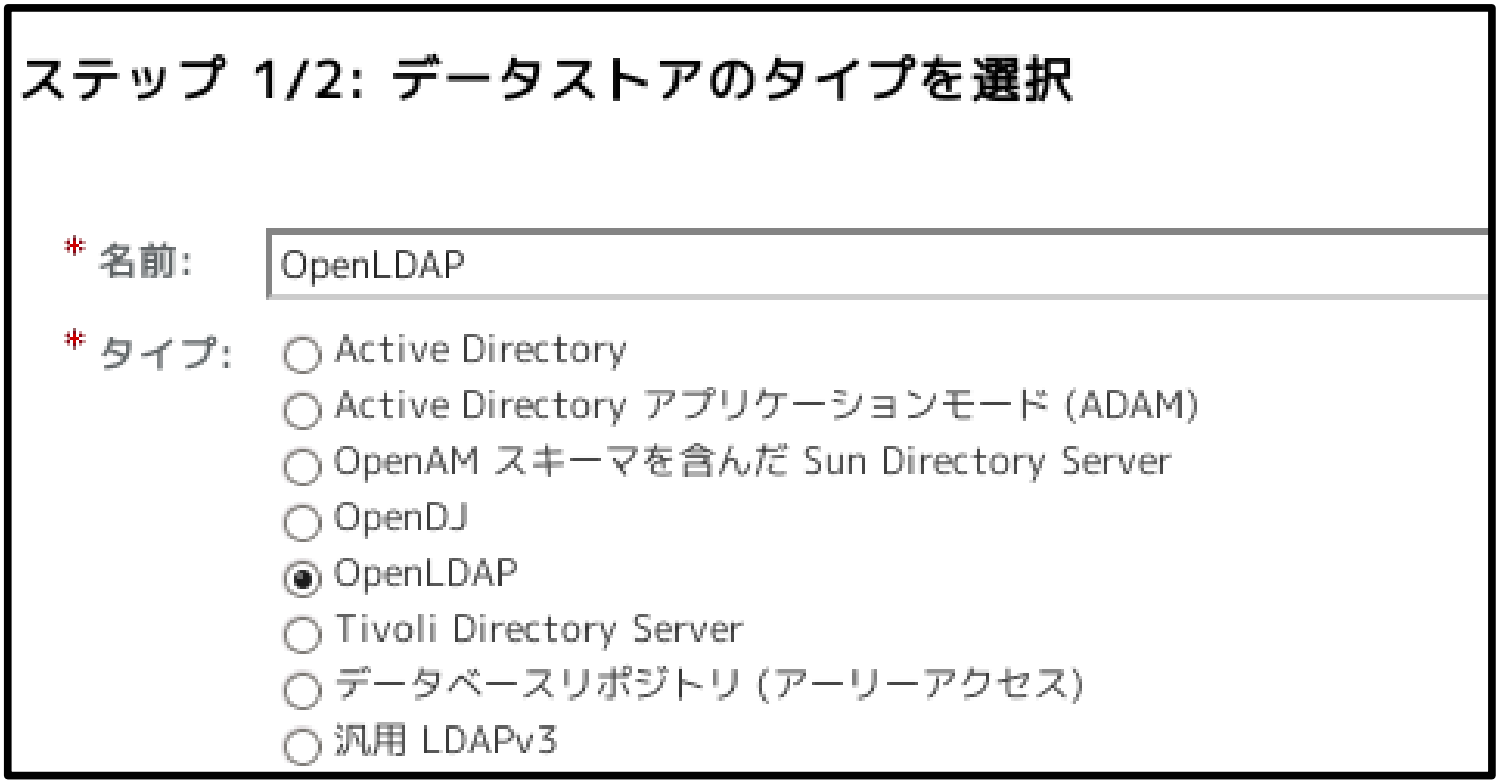
```
# service osstech-tomcat7 start
```

- rpmコマンドでアップデート

```
# rpm -Fvh osstech-openam11-*.el6.noarch.rpm
```

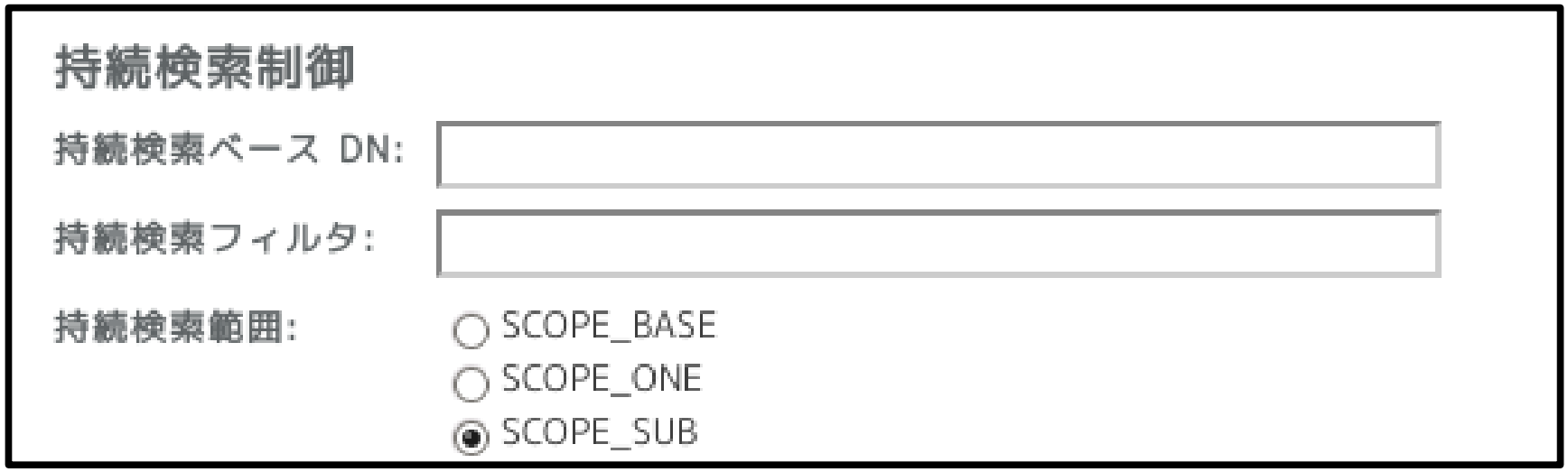
OpenLDAPデータストア

- データストア選択肢にOpenLDAPを追加



OpenLDAP持続検索

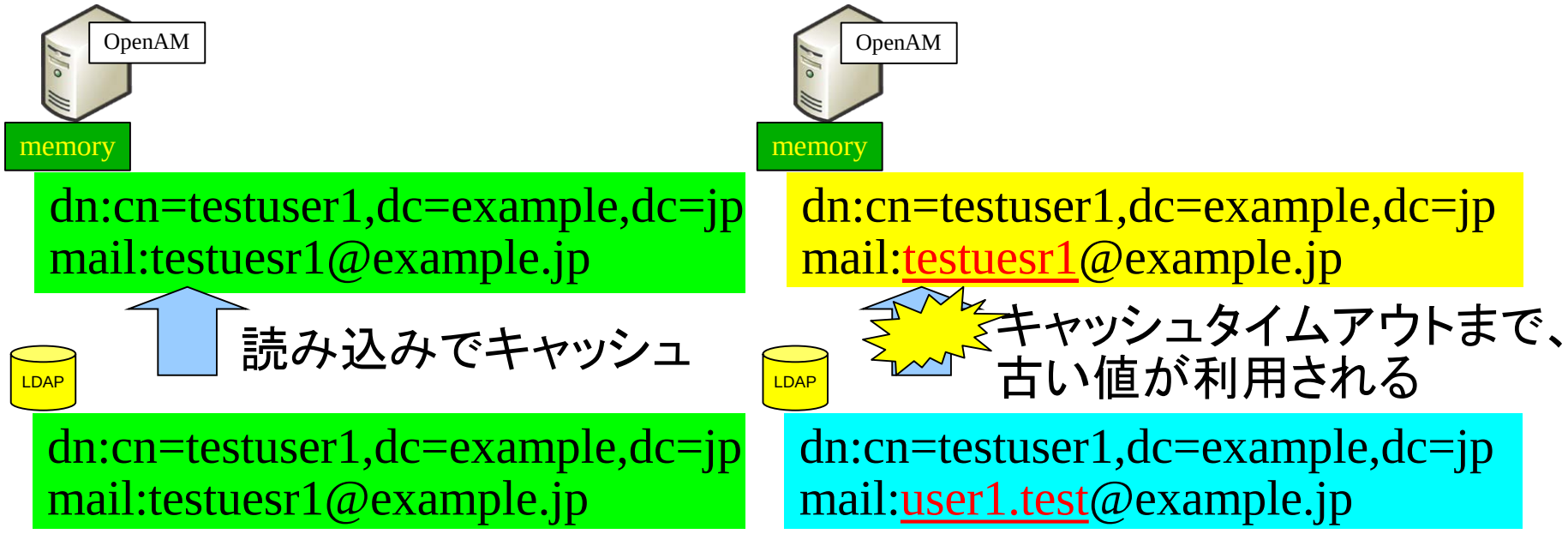
- OpenLDAP上のデータ変更を即座に利用可能
- OpenLDAP内のデータ変更を受け、OpenAM内のLDAPキャッシュをクリア
- 設定はデータストア設定に追加するだけ。



OpenLDAP持続検索

- OpenLDAP内のデータ変更を受け、OpenAM内のLDAPキャッシュをクリア

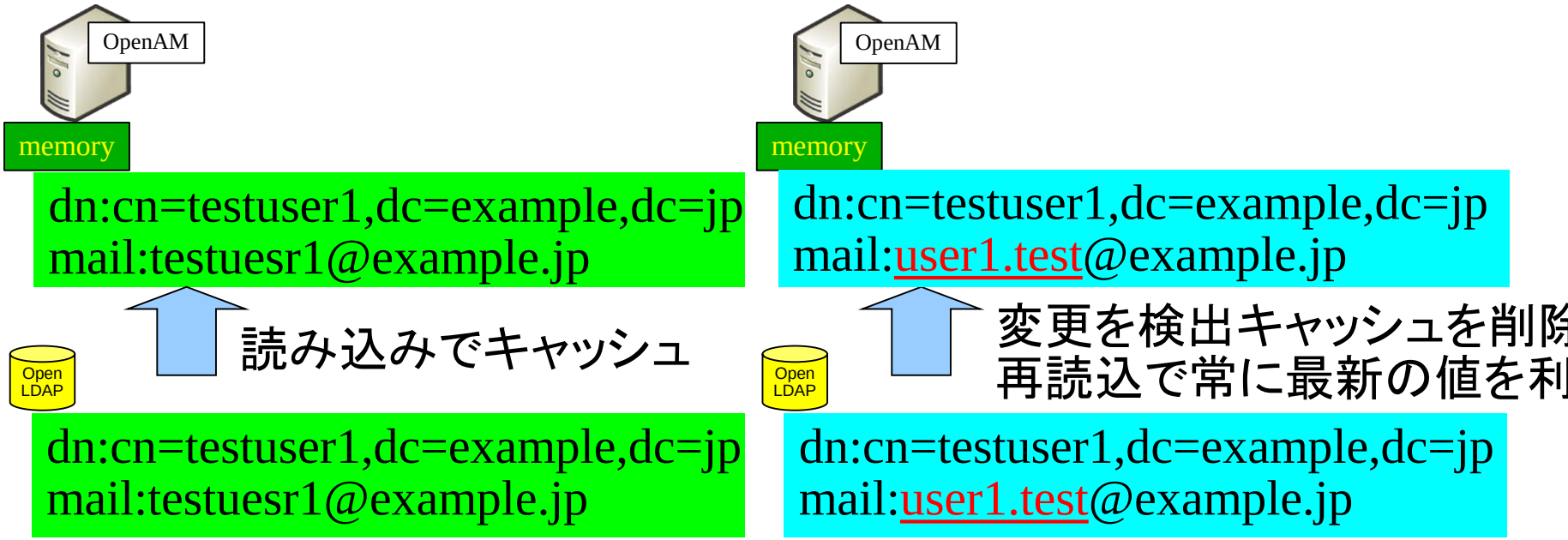
持続検索（パーシステントサーチ）未対応の場合



OpenLDAP持続検索

- OpenLDAP内のデータ変更を受け、OpenAM内のLDAPキャッシュをクリア

持続検索（パーシステントサーチ）対応の場合



マトリックス型認証モジュール

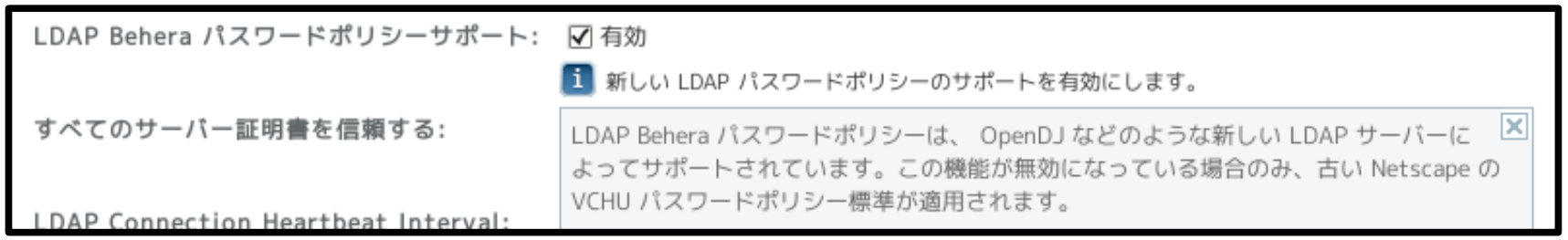
- ワンタイムパスワード用モジュール追加
- ログイン画面にはIDを入力するフィールドのみ

マトリックス型認証モジュール

- 自分の形状パターンに重なるマス目の数値を入力してログイン
- 数値の配置は毎回変化する
- ワンタイムパスワードによりパスワード漏洩を防ぐ

パスワードポリシー調整

- LDAP Beheraパスワードポリシーで対応
  - Beheraポリシー以前はSunJDS認証のみ対応



- 有効期限最終日（残0日）でのパスワード変更

iOS、Android向けCSS

- 携帯端末の画面からログイン入力がはみ出るなど、使い勝手の面を修正。カスタマイズ不要でスマートフォンから利用可能。

不具合修正

- OPENAM-688
  - IdRepo デバッグログに RetryTask のエラーが出つづける問題を修正
- OPENAM-3217
  - Fedlet の JSP のコンパイルエラーを修正
- OPENAM-3437
  - シングルログアウト時に RelayState の検証に失敗する問題を修正
- OPENAM-3456
  - データストア認証モジュールを利用する場合にオンメモリのアカウントロックを利用できない問題を修正
- OPENAM-3490
  - デスクトップ SSO の認証レベルが設定されない問題を修正
- OPENDJ-1247、OPENDJ-1258
  - OpenAM に同梱されている OpenDJ SDK の問題を修正

「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

OSSTech オープンソース・ソリューション・テクノロジ株式会社 Open Source Solution Technology Corporation
〒141-0031 東京都品川区西五反田1-29-1 コイズミビル 8F Tel:03-6417-0753 Fax:03-6417-0754 Mail:info@osstech.co.jp