OpenAMトレーニング

OpenAMでシングルサインオンを実現しよう！

株式会社 野村総合研究所 IT基盤イノベーション事業本部 オープンソースソリューション推進室(OSS推進室)
Mail：ossc@nri.co.jp　Web：http://openstandia.jp/

アジェンダ

- Section0：自己紹介
- Section1：OpenAM概要
- Section2：OpenAMインストール
- Section3：連携先システムとのSSO
- Section4：まとめ

Section0

自己紹介

自己紹介

- 盛 慎（Makoto MORI）

- 所属部署
  - オープンソースソリューション推進室
  - OSSを使ったシステム構築から運用までワンストップでサポート
  - 対象OSSは50種類以上

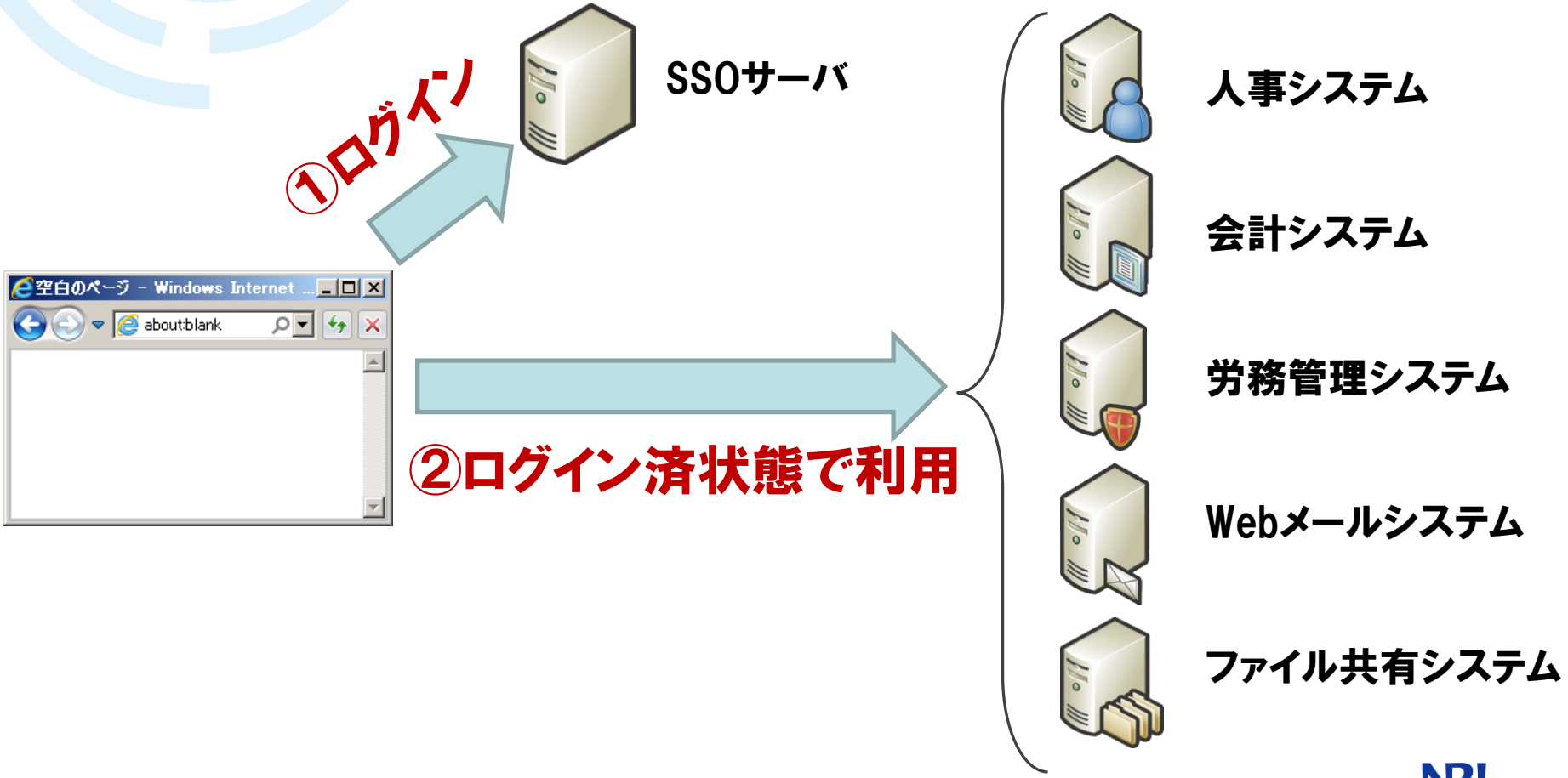
- 担当
  - SI
  - システム運用維持管理
  - 製品開発

Section1

OpenAM概要

シングルサインオン(SSO)とは

- 一度のログイン(サインオン)で複数のアプリケーションがログイン済状態で利用できる仕組み



シングルサインオン(SSO)とは

- ユーザにとってのメリット
  - システムごとの認証が無くなって手間が減る
  - ID/PWの管理(記憶や更新)が楽になる
- システム管理者にとってのメリット
  - アカウント情報の一元化により、運用の手間が減る
  - ユーザの認証方法を変更しやすい(指紋認証機能の追加など)
  - ユーザのID/PW管理一元化に伴うセキュリティの向上

シングルサインオン（SSO）とは

SSO需要の高まり

▶企業内システム数の増加

✓複雑化したシステムをよりスマートに利用／管理したい

▶クラウドサービスの増加

✓salesforceなどのクラウドサービスも企業内システムとシームレスに使いたい

▶求められる企業コンプライアンスの高まり

✓不正ログイン等のセキュリティリスクを低減したい

シングルサインオン（SSO）とは

OpenStandiaのSSO導入事例

ヘルスケア

✓課題

- 顧客の利便性を向上させるため、複数の自社サービスと、顧客システムとでシングルサインオン対応したい。

✓ユーザ数

- 10,000人

大手医療機器メーカー

✓課題

- 様々なアプリケーションに対応でき、将来のサービス追加にも柔軟に対応できる社内認証基盤が欲しい。

✓ユーザ数

- 10,000人

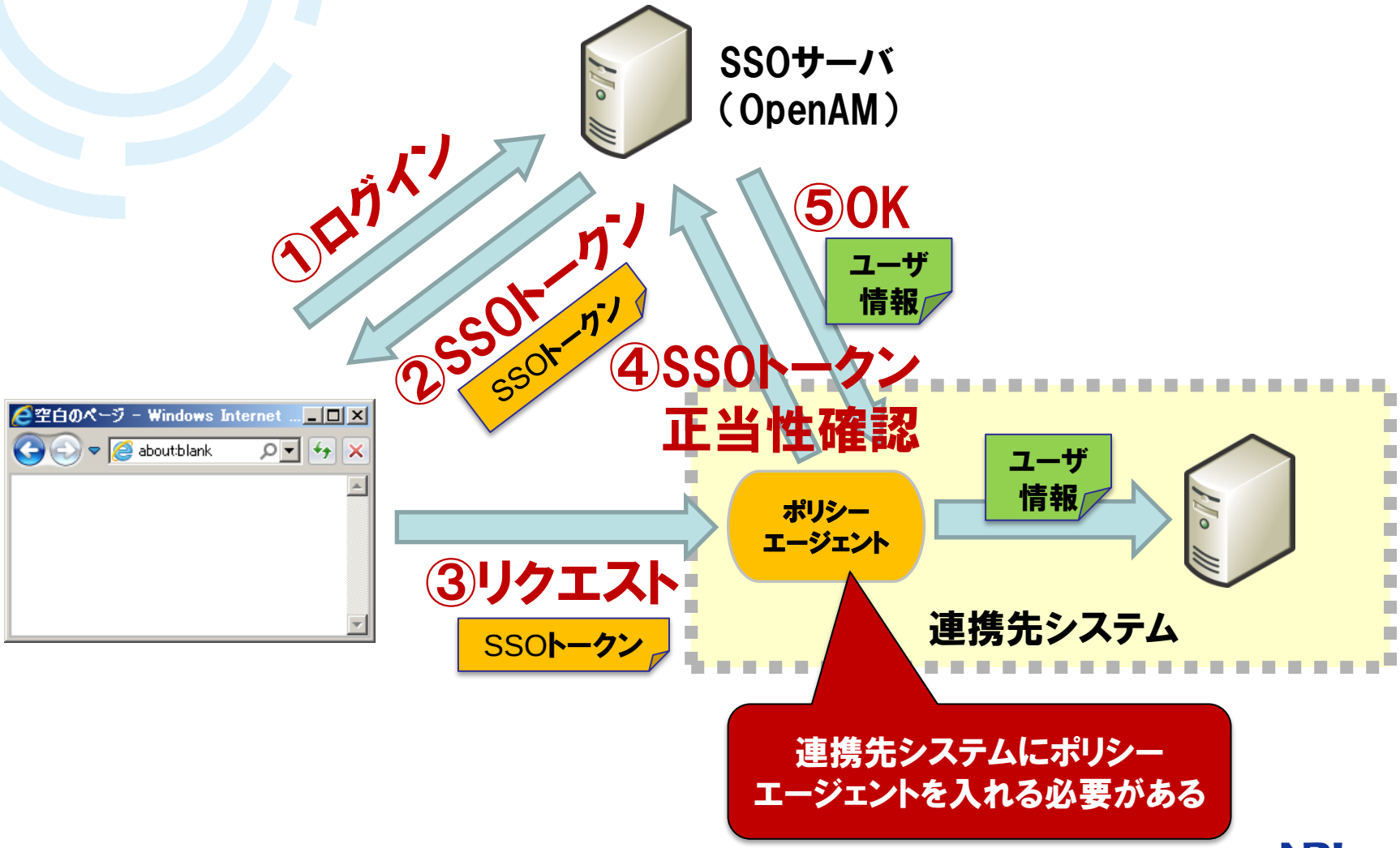
OpenAMとは

- SSOを実現するためのOSS
  - 旧Sun Microsystems社の商用製品(OpenSSO)がベースであるため高品質かつ多機能
  - ForgeRock社が継続開発中
  - Javaで実装されたWebアプリケーションでOS非依存
  - CDDL(Common Development and Distribution License)で、ソースコードを無償で使用、改変、再配布可能
  - 最新の安定バージョンは12.0.0

OpenAMの代表的なSSO方式

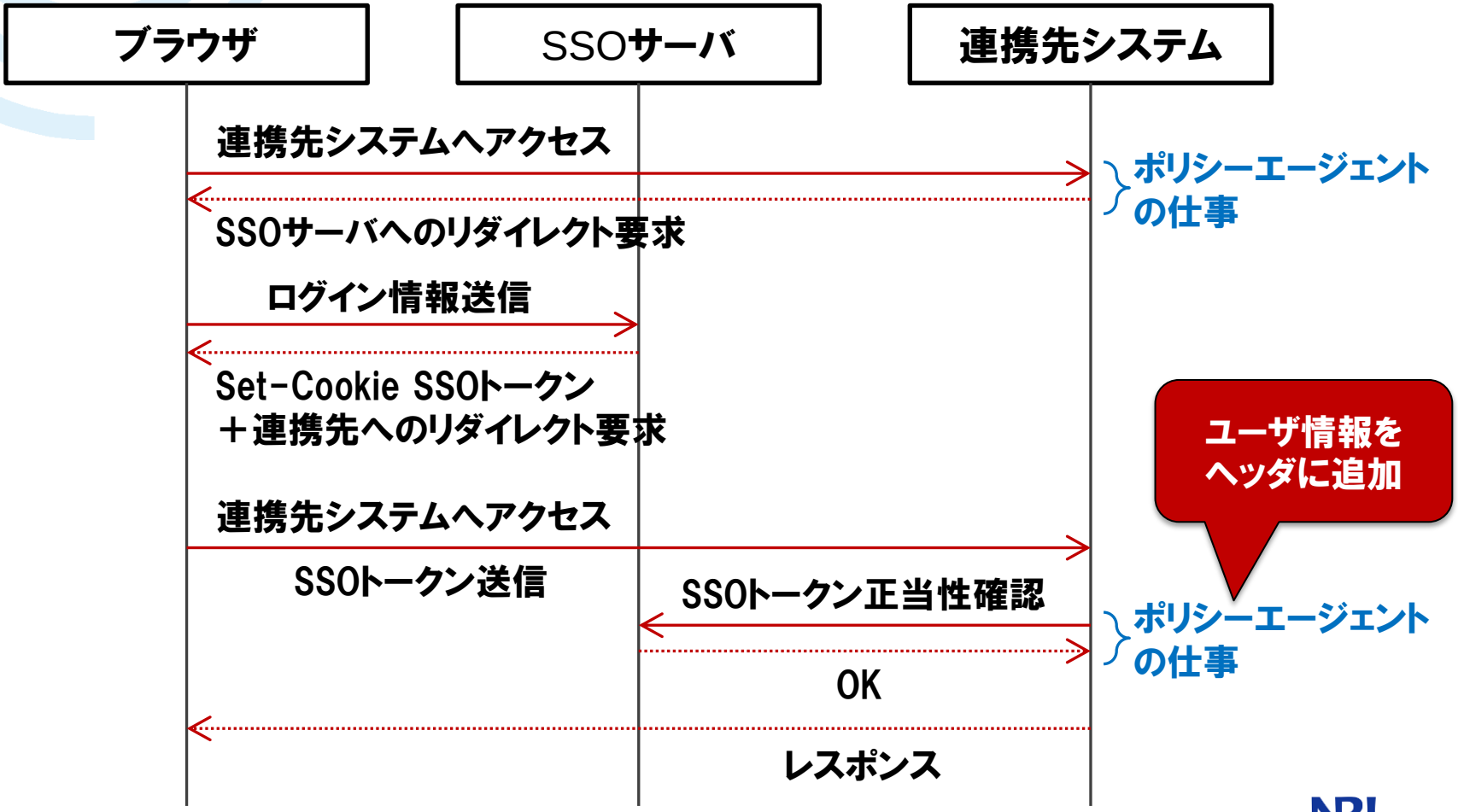
SSO方式	説明
エージェント方式	アプリケーションが動作するサーバに直接エージェントを導入する方式。
リバースプロキシ方式	リバースプロキシサーバ(通常はApache)にエージェントを導入し、バックエンドにいる複数のアプリケーションサーバに対してリバースプロキシする方式。
代理認証方式	代理認証とは、ユーザからのログインリクエストをエミュレートし、認証を代行すること。OpenIGと連携することで、代理認証が可能となる。 連携先システムで、HTTPヘッダから認証情報を取得するカスタマイズが出来ない際に採用する方式。
SAML	SAMLとは認証情報を表現するためのXML仕様。主にSalesforce、GoogleAppsとSSOする際に採用する方式。
OpenID Connect	OAuth2.0をベースとするシンプルな新しいID連携プロトコル。OpenAM11.0から利用可能。主にクラウドサービスとのSSO方式として今後の主流になると思われる。

エージェント方式



SSO方式

- OpenAMでのログインが完了したらSSOトークン（Cookie）を発行します



SSOトークンについて

- SSOトークンの正体
  - 認証トークン、認証クッキーとも呼ばれる
  - 標準では「iPlanetDirectoryPro」という名前のクッキー
- 認証されたユーザの識別方法
  - ポリシーエージェントがHTTPリクエストヘッダにユーザ識別情報(例:ログインID)を付与する
  - アプリケーションはHTTPリクエストヘッダからユーザ識別情報を取得する

```
GET / HTTP/1.1
Accept                          : text/html
Accept-Language                 : ja-JP
Connection                      : Keep-Alive
Cookie :iPlanetDirectoryPro=KU (GKU (#LGSJVUUR749
```

エージェント通過後

```
GET / HTTP/1.1
Accept                          : text/html
Accept-Language                 : ja-JP
Connection                      : Keep-Alive
Cookie : iPlanetDirectoryPro=KU (GKU (#LGSJVUUR749
LOGINID                         : makoto-mori@nri.co.jp
```

ポリシーエージェントについて

ポリシーエージェントとは

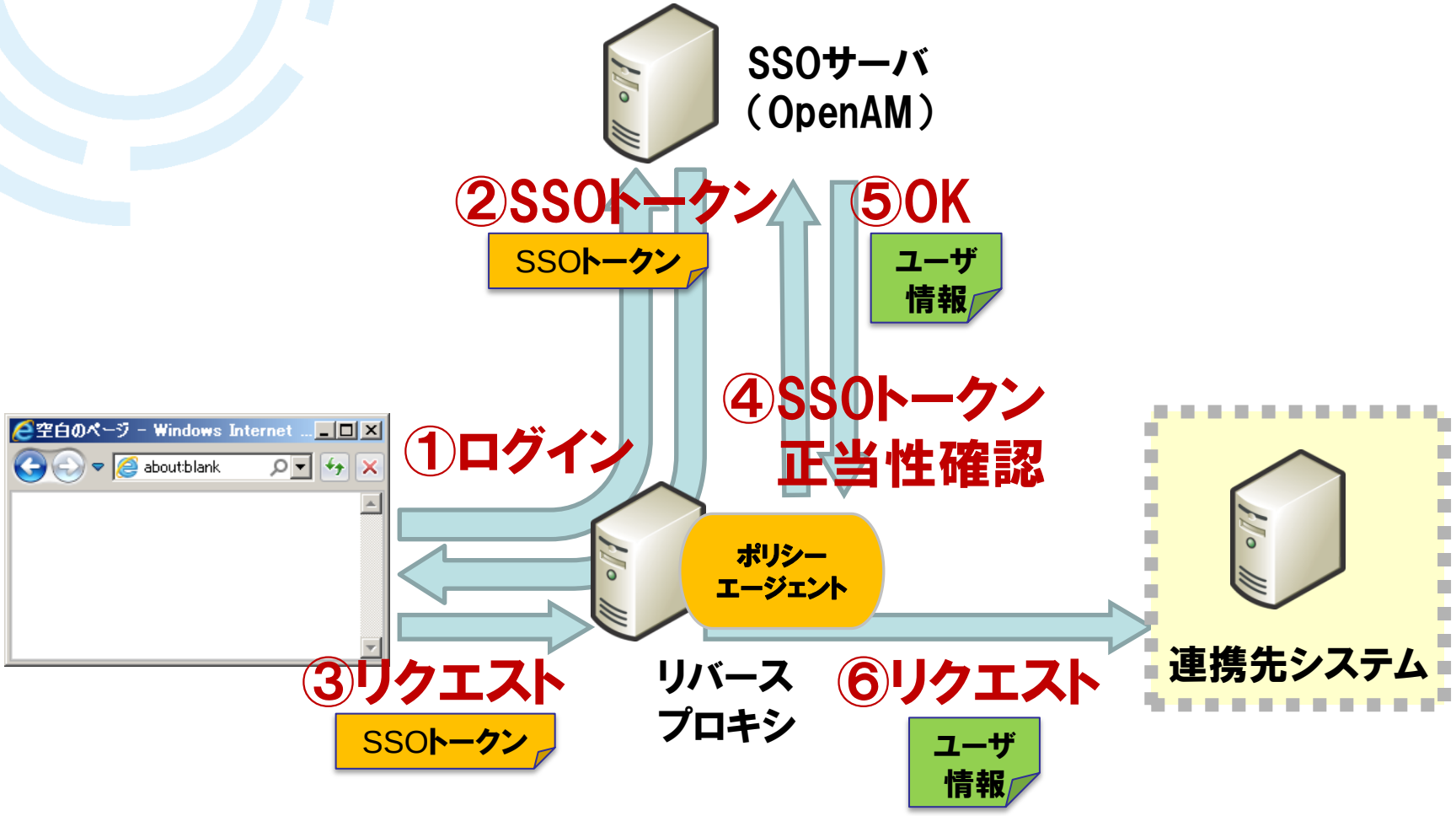
- SSO対象の連携先サーバへインストールするモジュール
- SSOサーバと通信し、認証／認可に必要な情報を取得する
- ユーザからリクエストがあるとそのURLを評価し、拒否／許可を判定する

提供されているエージェントの種類

- Webポリシー エージェント
  - ✓Apache 2.0、2.2、2.4用
  - ✓Microsoft IIS 6.0、 7.0 等
- J2EEポリシー エージェント
  - ✓Tomcat v 6.0 & 7.0用
  - ✓JBoss EAP 5.x、6 用
  - ✓JBoss AS 7 用
  - ✓Jetty 6.1、7 & 8 用 等

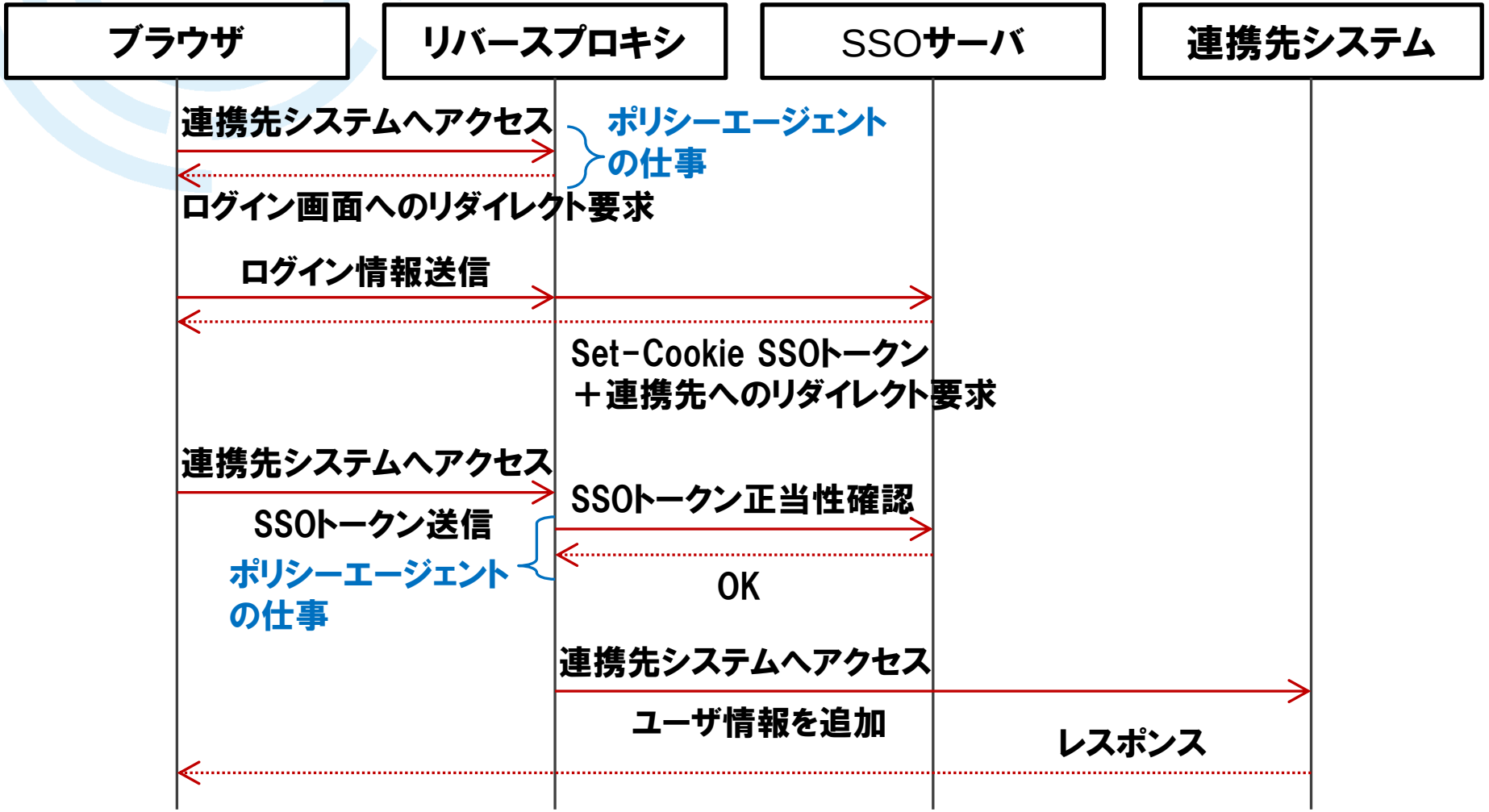
SSO方式

リバースプロキシ方式



SSO方式

リバースプロキシがSSOをドライブします



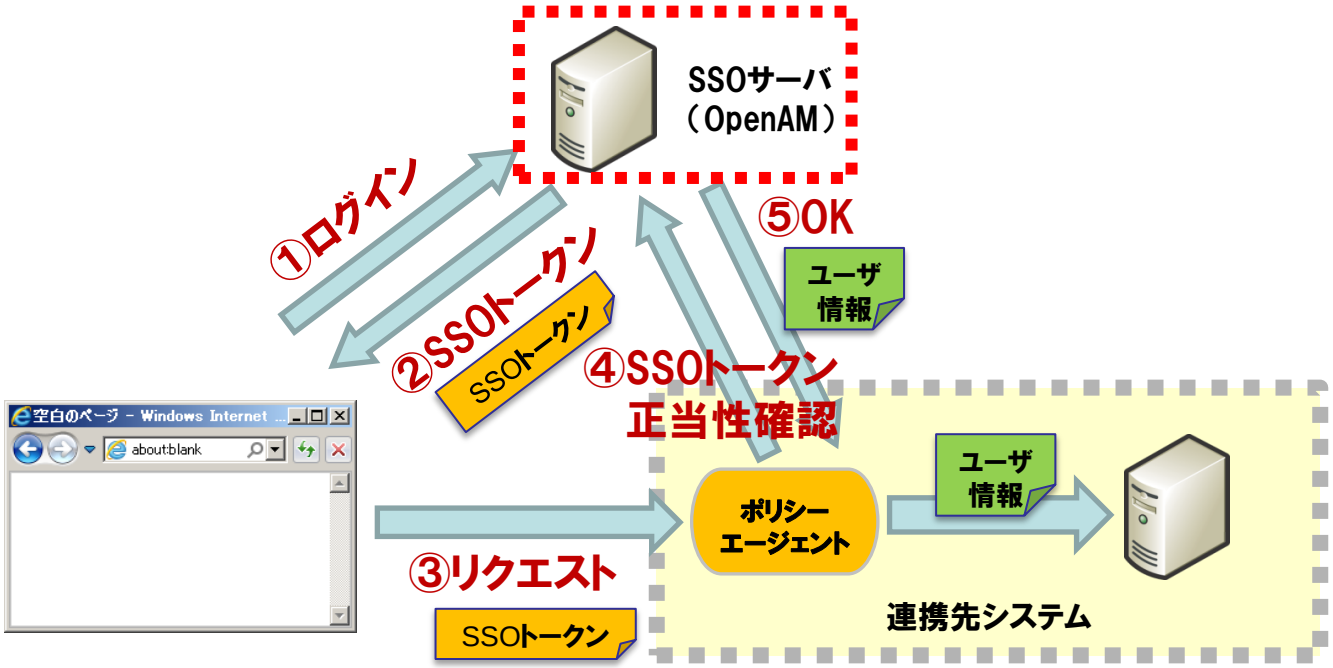
Section2

OpenAMインストール

OpenAMインストール

概要

- OS
  - ✓CentOS6
- OpenAM
  - ✓11.0.0
  - ✓ダウンロード元：http://forgerock.org/openam-archive.html



OpenAMインストール

ネットワークのセットアップ（FQDNの登録）

- /etc/sysconfig/network

```
HOSTNAME=openam.nri.jp
```

- /etc/hosts

```
192.175.204.251 openam.nri.jp
192.175.204.192 openam-app.nri.jp ←出番は後ほど
```

環境整備（動作検証のため）

- /etc/sysconfig/selinux

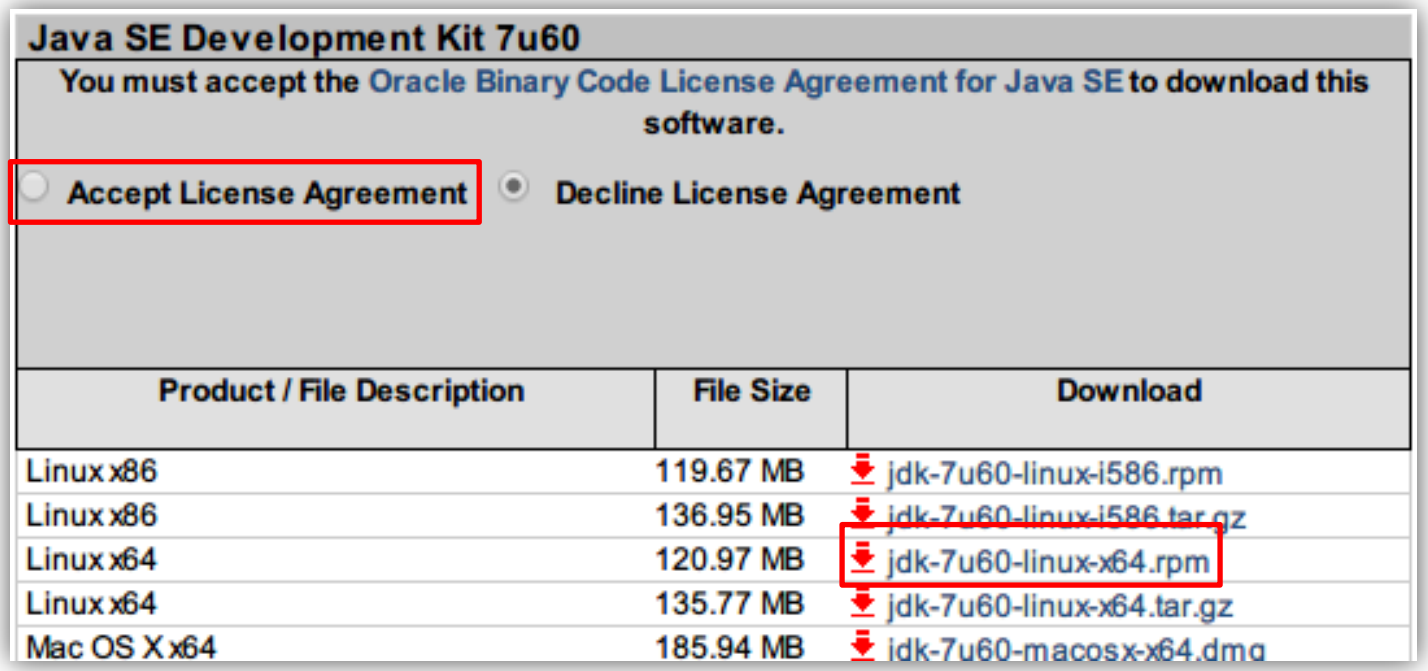
```
#SELINUX=enforcing
SELINUX=disabled
```

- ファイアウォールをOFF

```
$ service iptables stop
$ chkconfig iptables off
```

JDKのダウンロード

- ORACLE公式サイトからJDKをダウンロード
- http://download.oracle.com/otn-pub/java/jdk/7u60-b19/jdk-7u60-linux-x64.rpm?AuthParam=1404214955_1502d8aa0b24bce9ad8fbca7bc8fde11
- 「Accept License Agreement」をクリックしてから「jdk-7u60-linux-x64-rpm」をクリック



Java SE Development Kit 7u60

You must accept the Oracle Binary Code License Agreement for Java SE to download this software.

Accept License Agreement　Decline License Agreement

Product / File Description	File Size	Download
Linux x86	119.67 MB	jdk-7u60-linux-i586.rpm
Linux x86	136.95 MB	jdk-7u60-linux-i586.tar.gz
Linux x64	120.97 MB	jdk-7u60-linux-x64.rpm
Linux x64	135.77 MB	jdk-7u60-linux-x64.tar.gz
Mac OS X x64	185.94 MB	jdk-7u60-macosx-x64.dmg

JDKのインストール

インストール

```
# rpm -ivh jdk-7u60-linux-x64.rpm
# java -version
java version "1.7.0_60"
Java(TM) SE Runtime Environment (build 1.7.0_60-b19)
Java HotSpot(TM) 64-Bit Server VM (build 24.60-b09, mixed
mode)
```

以下のようなエラーが出た場合は、ld-linux.so.2をインストールする

```
/lib/ld-linux.so.2: bad ELF interpreter: No such file or directory

# yum install ld-linux.so.2
```

Tomcatのインストール

Tomcatをダウンロードしてインストール

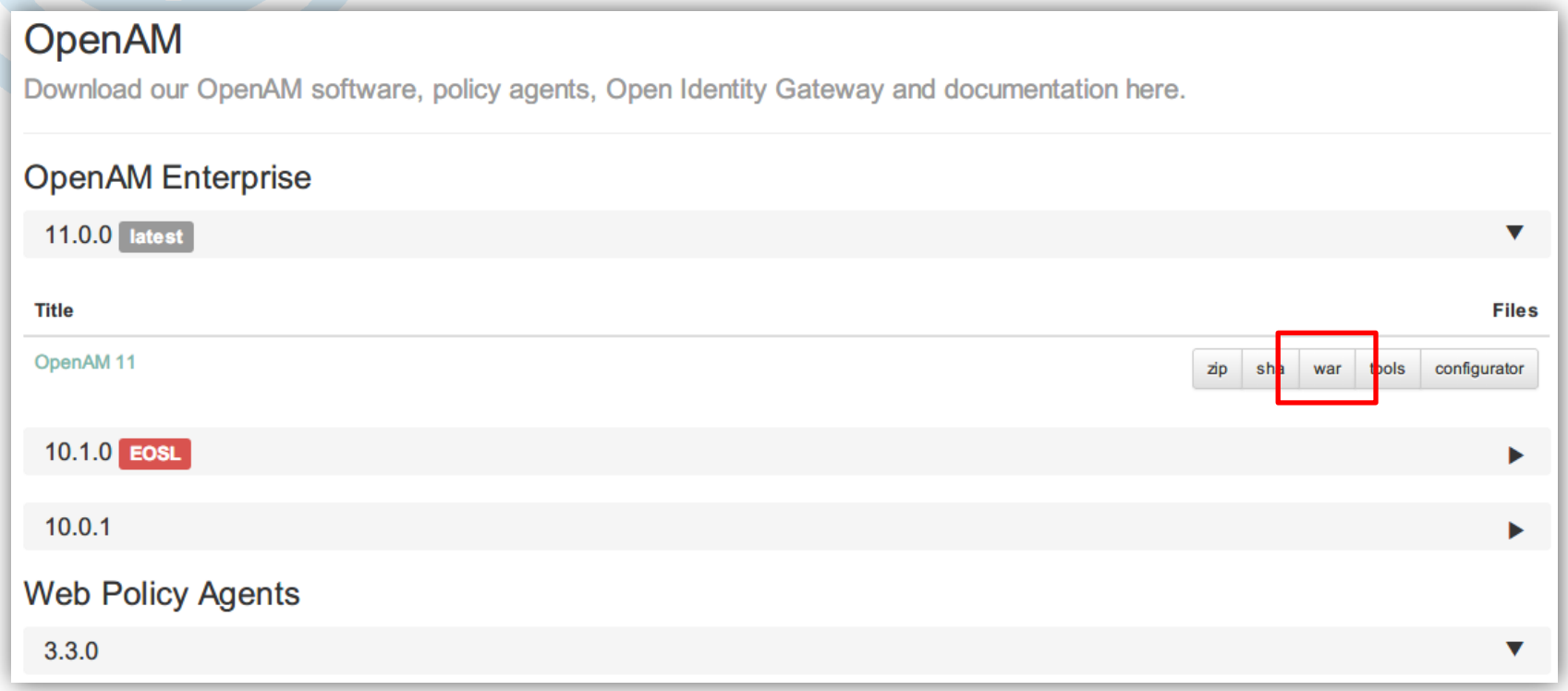
```
# wget
http://ftp.yz.yamagata-u.ac.jp/pub/network/apache/tomcat/tomcat-8/v8.0.9/bin/apache-tomcat-8.0.9.tar.gz

# tar zxvf apache-tomcat-8.0.9.tar.gz
# mv apache-tomcat-8.0.9 /usr/share/tomcat8
```

/root/.bash_profile

```
export JAVA_HOME=/usr/java/default/
export JAVA_OPTS="-Xmx1024m -XX:MaxPermSize=256m"
```

OpenAMのインストール

- ForgeRock公式サイトからwarファイルをダウンロード



Tomcatへのデプロイ

- ダウンロードしたwarファイルをリネームする

```
# mv OpenAM-11.0.0.war openam.war
```

- Tomcatにデプロイする

```
# mv openam.war /usr/share/tomcat8/webapps/
```

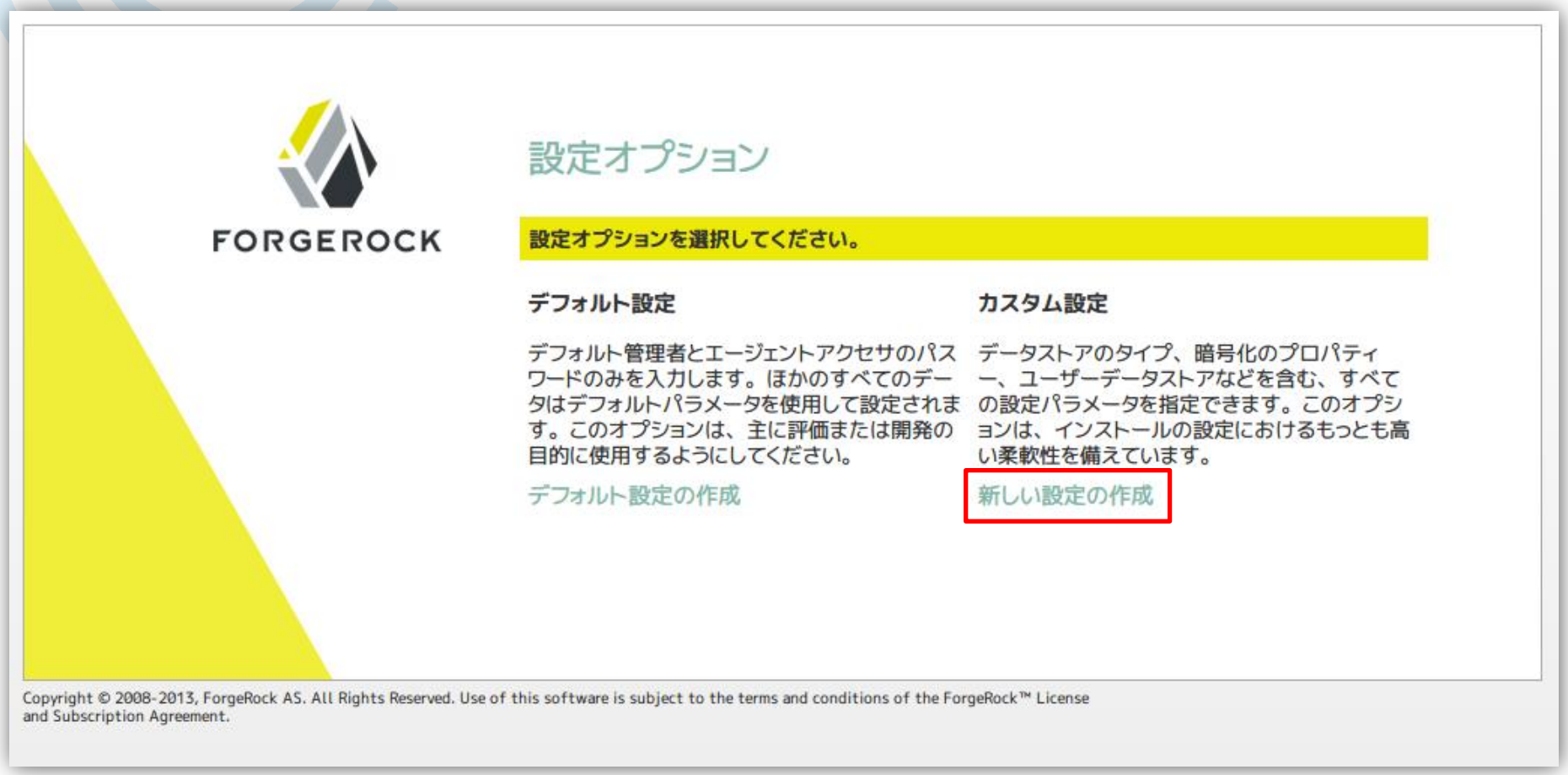
- Tomcatを起動する

```
# /usr/share/tomcat8/bin/startup.sh
```

OpenAMインストール

OpenAM初期設定：Step 1

- http://openam.nri.jp:8080/openam/



OpenAMインストール

OpenAM初期設定：Step2

- amAdmin（OpenAM管理者）のパスワードを設定（例：adminpassword）

OpenAMインストール

OpenAM初期設定：Step3

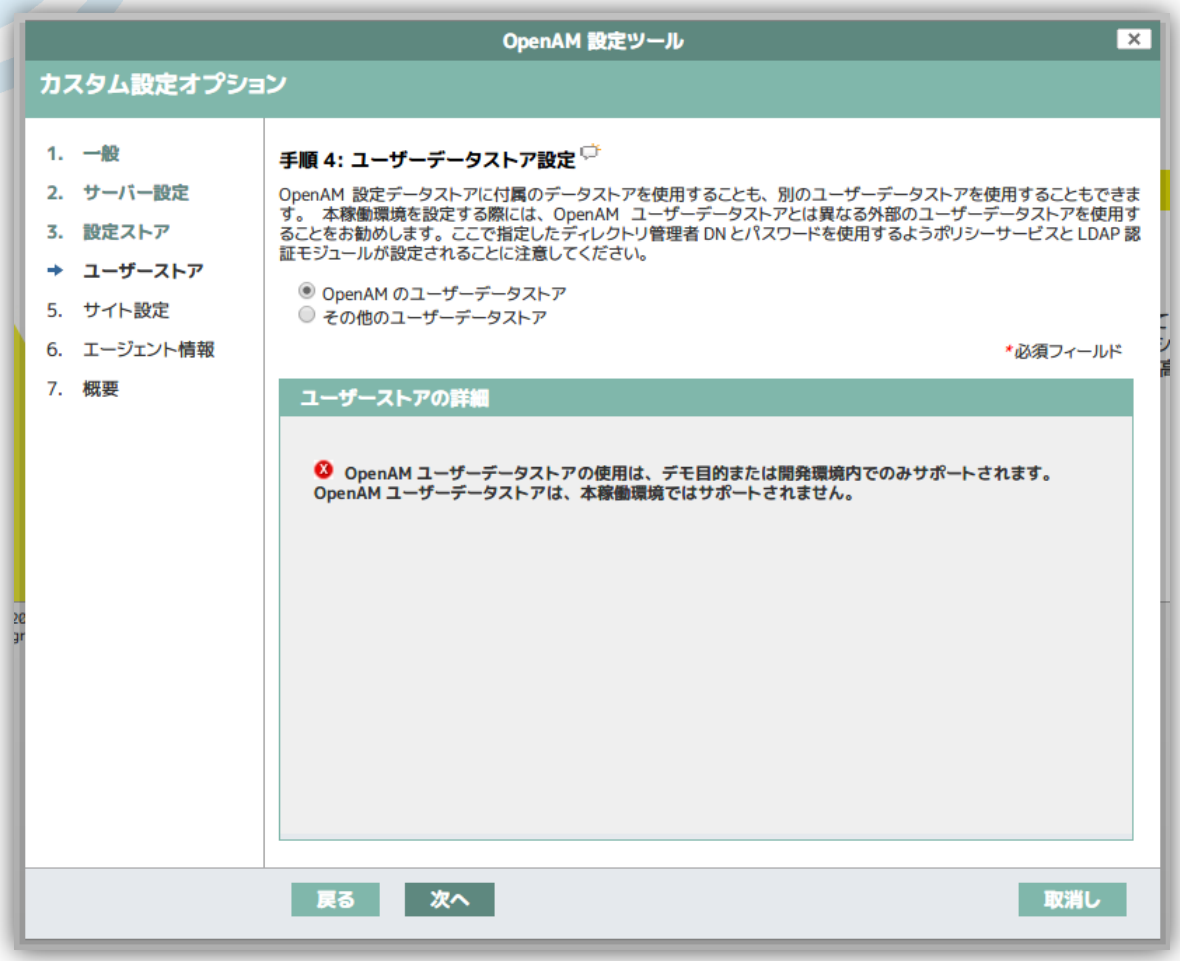
- サーバーURL　：http://openam.nri.jp:8080
- Cookieドメイン　：.nri.jp
- プラットフォームロケール、設定ディレクトリはそのままでOK

OpenAM初期設定：Step4

- 「最初のインスタンス」を選択して次へ

OpenAM初期設定：Step5

- 「OpenAMのユーザーデータストア」を選択して次へ



OpenAM初期設定：Step6

- 「いいえ」を選択して次へ

OpenAM初期設定：Step7

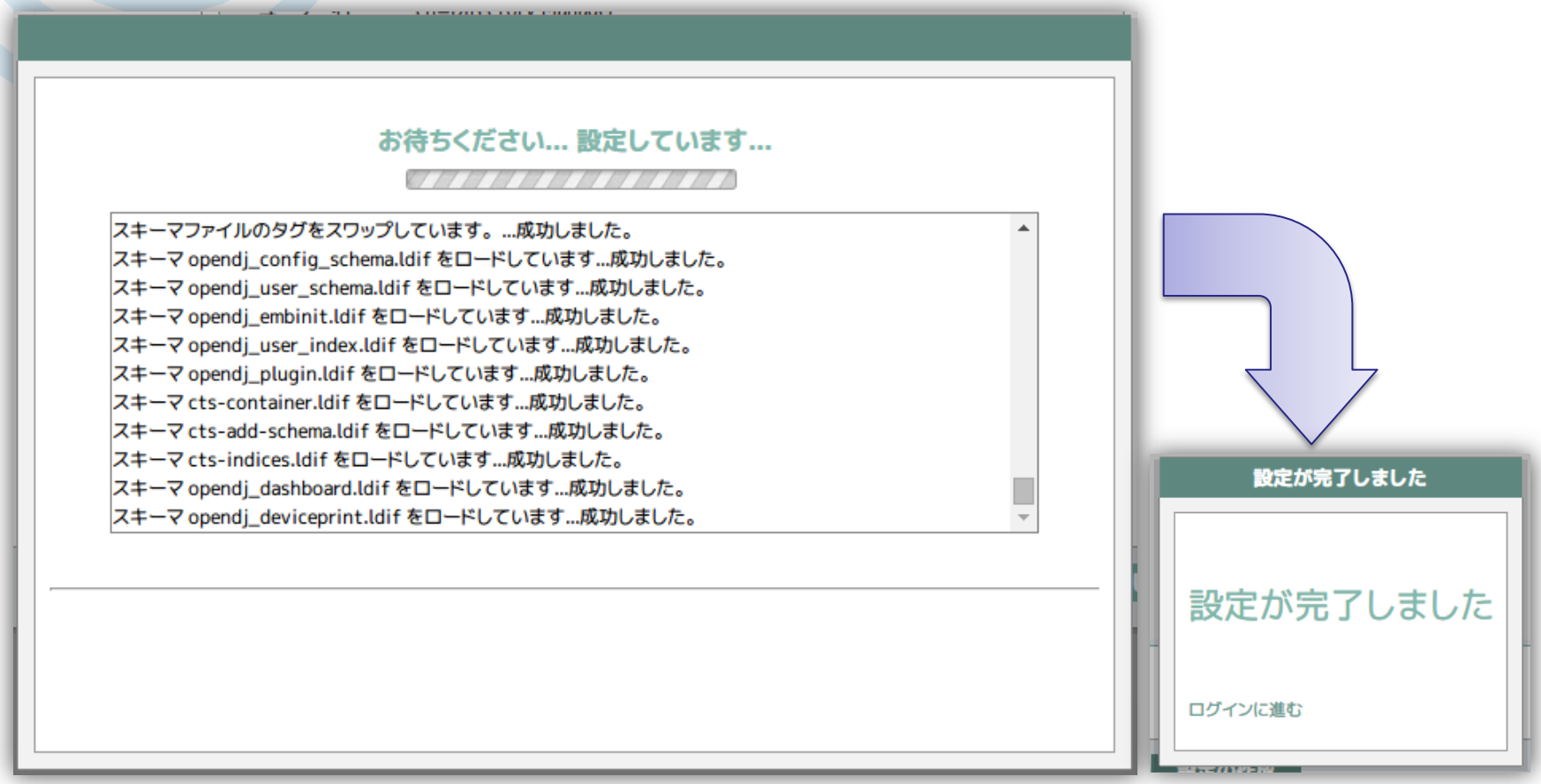
- デフォルトポリシーエージェントのパスワードを設定（例：agentpassword）

OpenAM初期設定：Step8

▶設定内容を確認して「設定の作成」

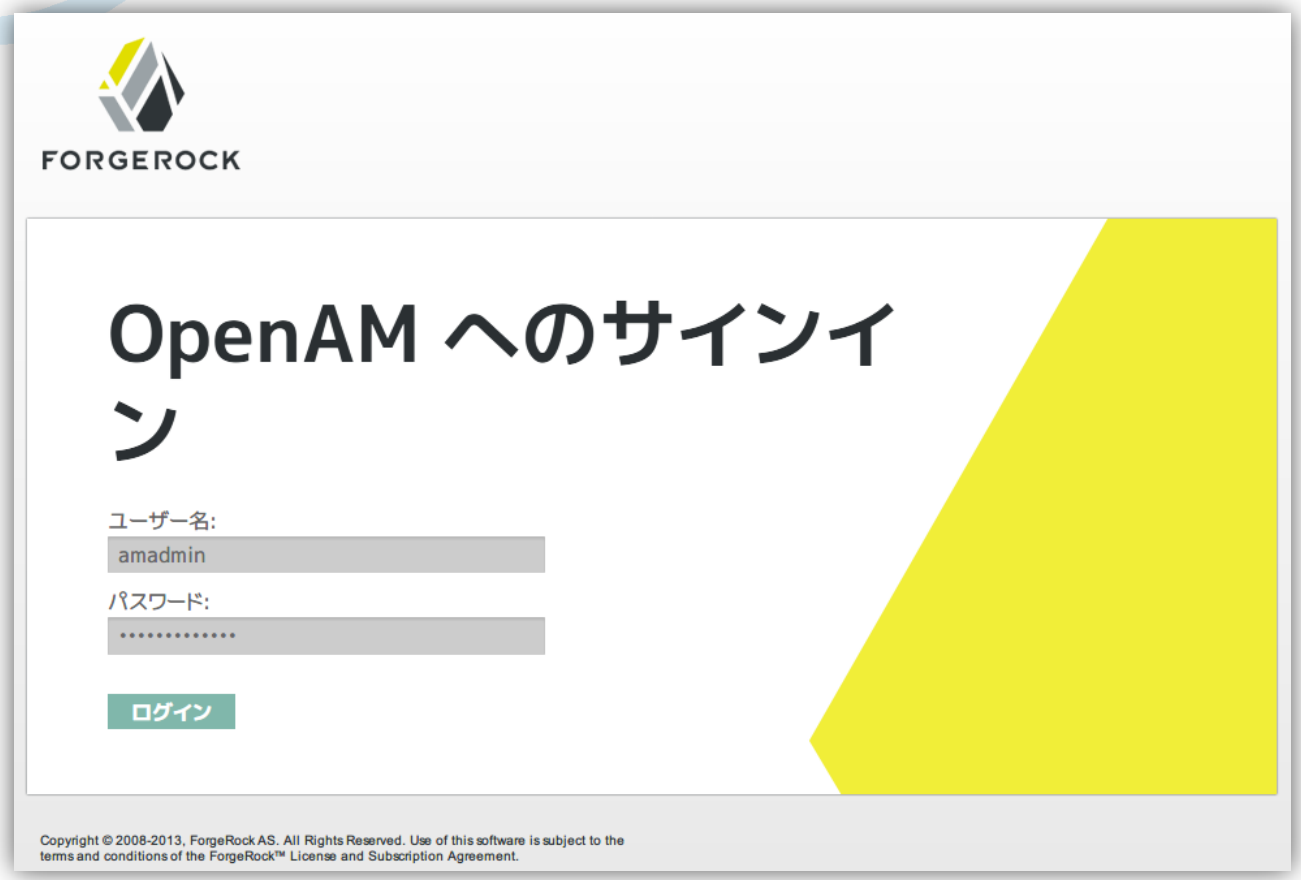
OpenAM初期設定：Step9

- 設定が実行されます



OpenAMにログイン

- http://openam.nri.jp:8080/openam にアクセスし、amadminユーザーでログインします



OpenAMインストール

OpenAMにログイン

- OpenAM管理コンソールのメインメニュー画面が表示されます

Section3

連携先システムとのSSO

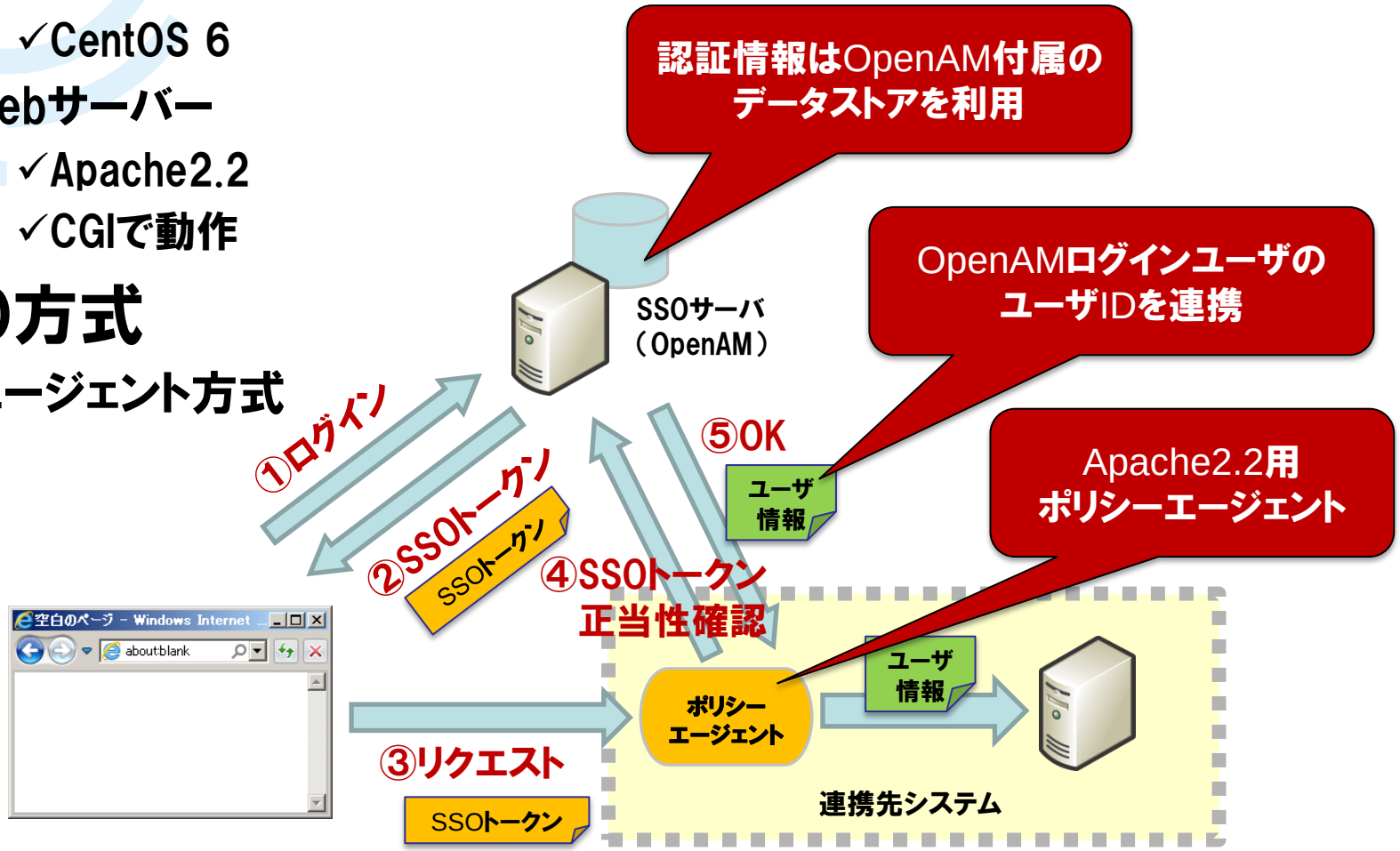
連携先システムとのSSO

連携先システム概要

- OS
  - ✓CentOS 6
- Webサーバー
  - ✓Apache2.2
  - ✓CGIで動作

SSO方式

- エージェント方式



連携先システムとのSSO

連携先システム

- クライアントからのリクエストヘッダの内容を表示するだけのアプリケーション

管理者ユーザー向けサイト HTTPヘッダ SSO実行結果

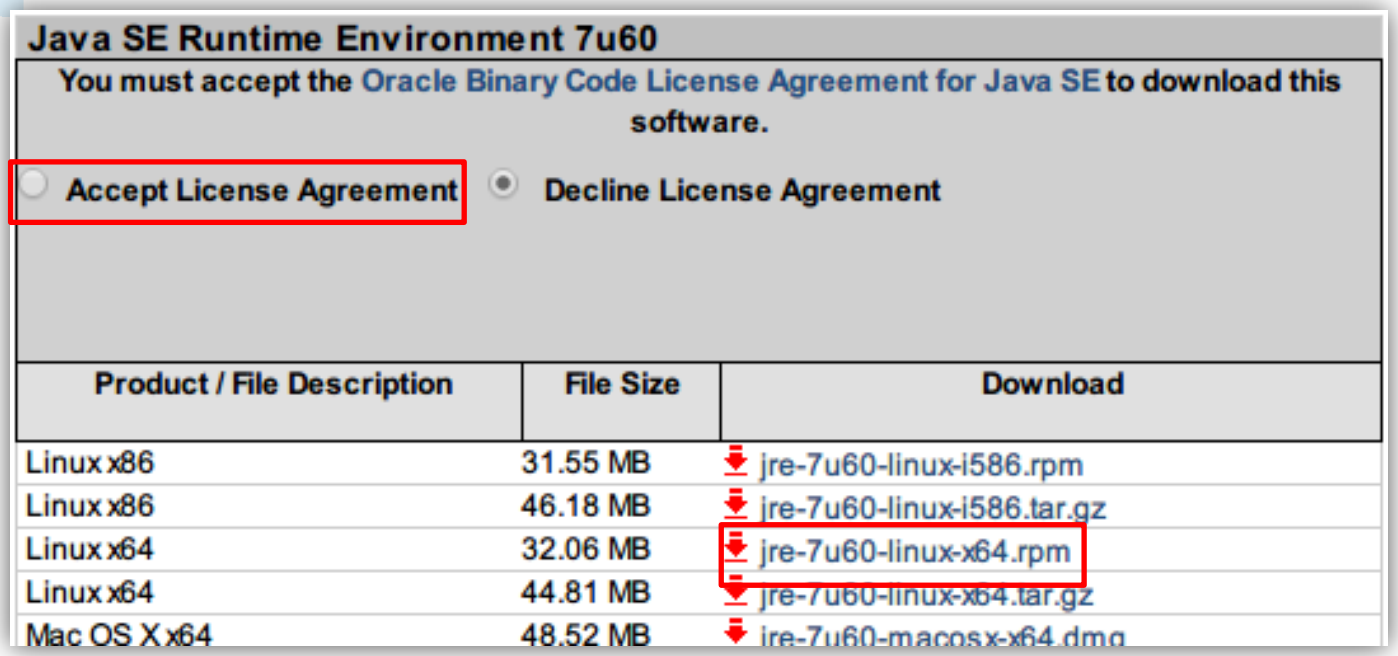
想定通りのパラメータが送信されていることを確認してください。

---------- HTTPヘッダ ----------
ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ACCEPT_CHARSET = Shift_JIS,utf-8;q=0.7,*;q=0.3
ACCEPT_ENCODING = gzip,deflate,sdch
ACCEPT_LANGUAGE = ja,en-US;q=0.8,en;q=0.6
CONNECTION = keep-alive
HOST = openam-traning-app.nriossc.co.jp
USER_AGENT = Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31

---------- リクエストパラメータ ----------

JREをダウンロード

- ORACLE公式サイトからJREをダウンロード（エージェントインストール用）
- http://download.oracle.com/otn-pub/java/jdk/7u60-b19/jre-7u60-linux-x64.rpm?AuthParam=1404279220_20255c368d3e0d87f37c3af323bec95f



Java SE Runtime Environment 7u60

You must accept the Oracle Binary Code License Agreement for Java SE to download this software.

Accept License Agreement　Decline License Agreement

Product / File Description	File Size	Download
Linux x86	31.55 MB	jre-7u60-linux-i586.rpm
Linux x86	46.18 MB	jre-7u60-linux-i586.tar.gz
Linux x64	32.06 MB	jre-7u60-linux-x64.rpm
Linux x64	44.81 MB	jre-7u60-linux-x64.tar.gz
Mac OS X x64	48.52 MB	jre-7u60-macosx-x64.dmg

JREを連携先サーバにインストール

ファイルを展開

```
# ls -l
jre-7u60-linux-x64.rpm

# rpm -ivh jre-7u60-linux-x64.rpm
# ls -l /usr/java
jre1.7.0_60
```

JREを連携先サーバにインストール

JREにPATHを通す

```
# vi ~/.bash_profile
export JAVA_HOME=/ [jreを展開したフルパス] /jre1.7.0_60←追記
export PATH=$PATH:$JAVA_HOME/bin←追記

# source ~/.bash_profile
# java -version
/lib/ld-linux.so.2: bad ELF interpreter←ld-linux.so.2が無くエラー
# yum install ld-linux.so.2

# java -version
java version "1.7.0_60"
Java (TM) SE Runtime Environment (build 1.7.0_60-b19)
Java HotSpot (TM) 64-Bit Server VM (build 24.60-b09, mixed
mode)
```

ネットワーク設定

連携先サーバの /etc/sysconfig/network に追記する

```
HOSTNAME=openam-app.nri.jp
```

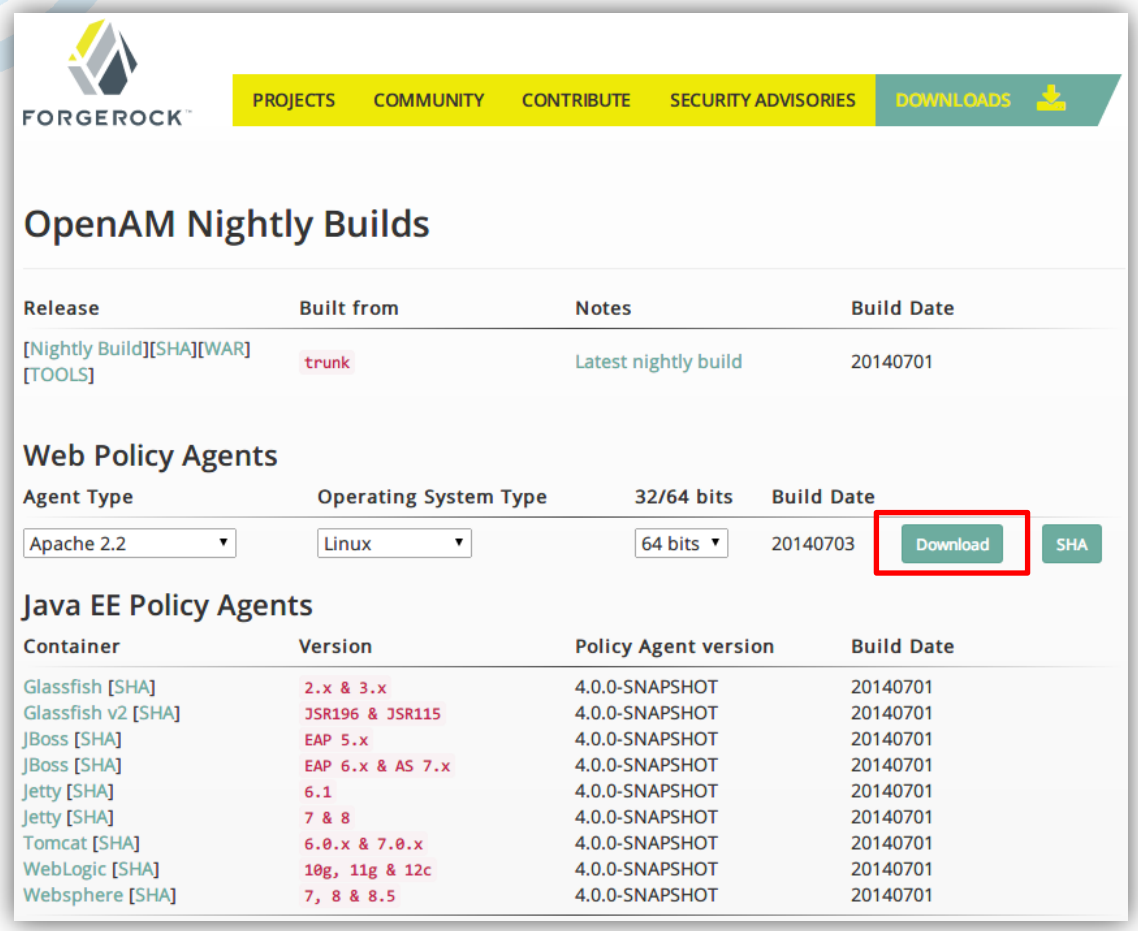
連携先サーバの /etc/hosts に追記する

```
192.175.204.251 openam.nri.jp      ←先ほどのSSOサーバ
192.175.204.192 openam-app.nri.jp
```

連携先システムの構築

ポリシーエージェントをダウンロード

- http://forgerock.org/downloads/openam-builds/



ポリシーエージェントを連携先サーバにインストール

ファイルを解凍

```
# ls -l
apache_v22_Linux_64_agent_3.1.0-Xpress.zip

# unzip apache_v22_Linux_64_agent_3.1.0-Xpress.zip
# ls web_agents
apache22_agent
```

Apacheを止める

```
# /etc/init.d/httpd stop
```

パスワードファイルを作成する

```
# cd web_agents/apache22_agent/bin
# echo [ポリシーエージェントのパスワード] > /tmp/password.txt
```

ポリシーエージェントを連携先サーバにインストール

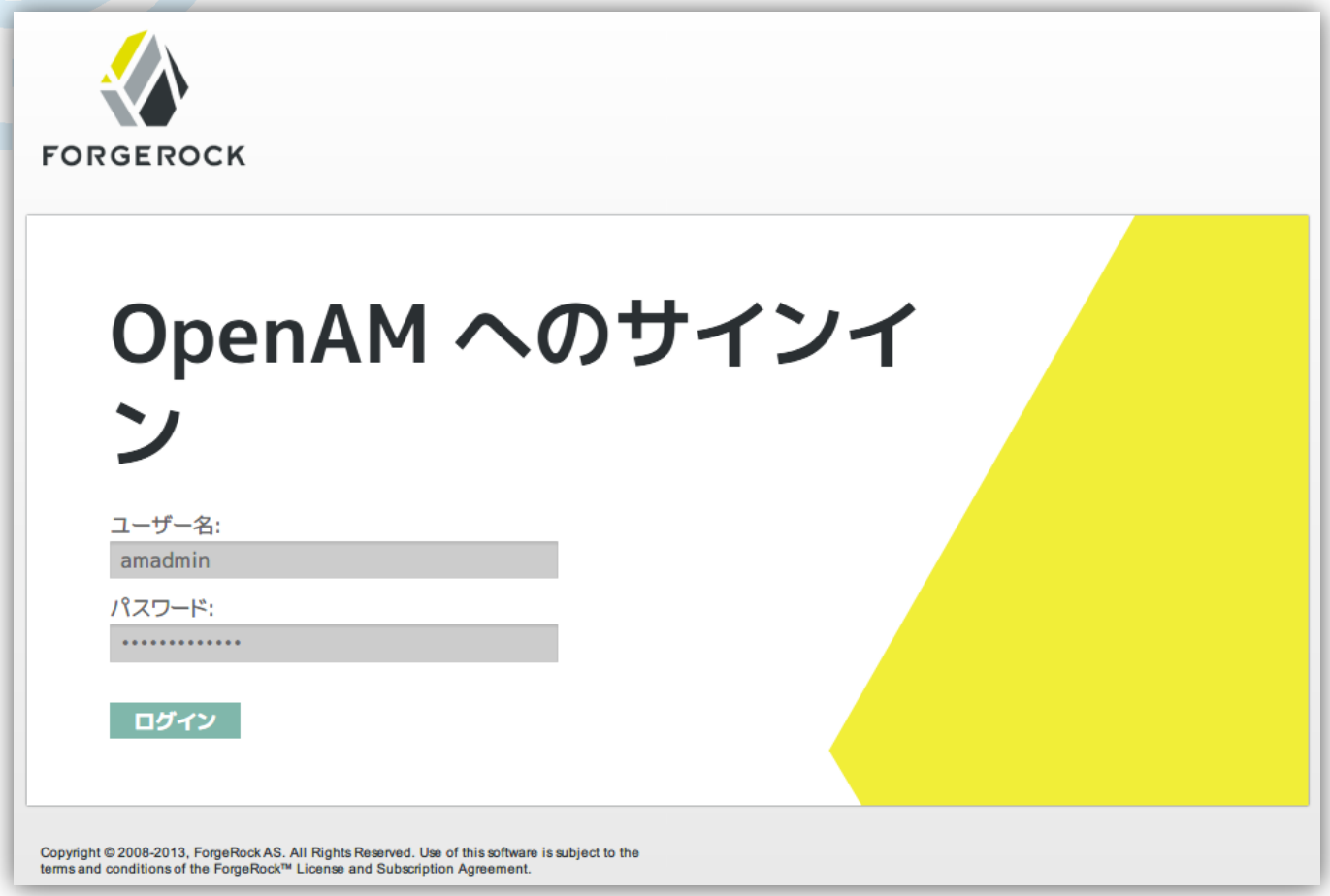
ポリシーエージェントをインストール

```
# ./agentadmin --install
Please read the following License Agreement carefully:
 [Press <Enter> to continue...] or [Enter n To Finish]
（ライセンスが表示されるので、Enterかnで読み進める）
Agreement (yes/no): [no]: yes ←入力

Enter the Apache Server Config Directory Path
 [/opt/apache22/conf]: /etc/httpd/conf
OpenAM server URL: http://openam.nri.jp:8080/openam
Agent URL: http://openam-app.nri.jp:80
Enter the Agent Profile name: openam-app
Enter the path to the password file: [password.txtへのフルパス]

Please make your selection [1]: ←Enter
```

成功すると、apache22_agentディレクトリにAgent_001が作成される

エージェントプロファイルの作成

- http://openam.nri.jp:8080/openam からOpenAMにログイン



エージェントプロファイルの作成

- アクセス制御＞(最上位のレルム)＞エージェント と遷移
- エージェントの新規ボタンをクリック

エージェントプロファイルの作成

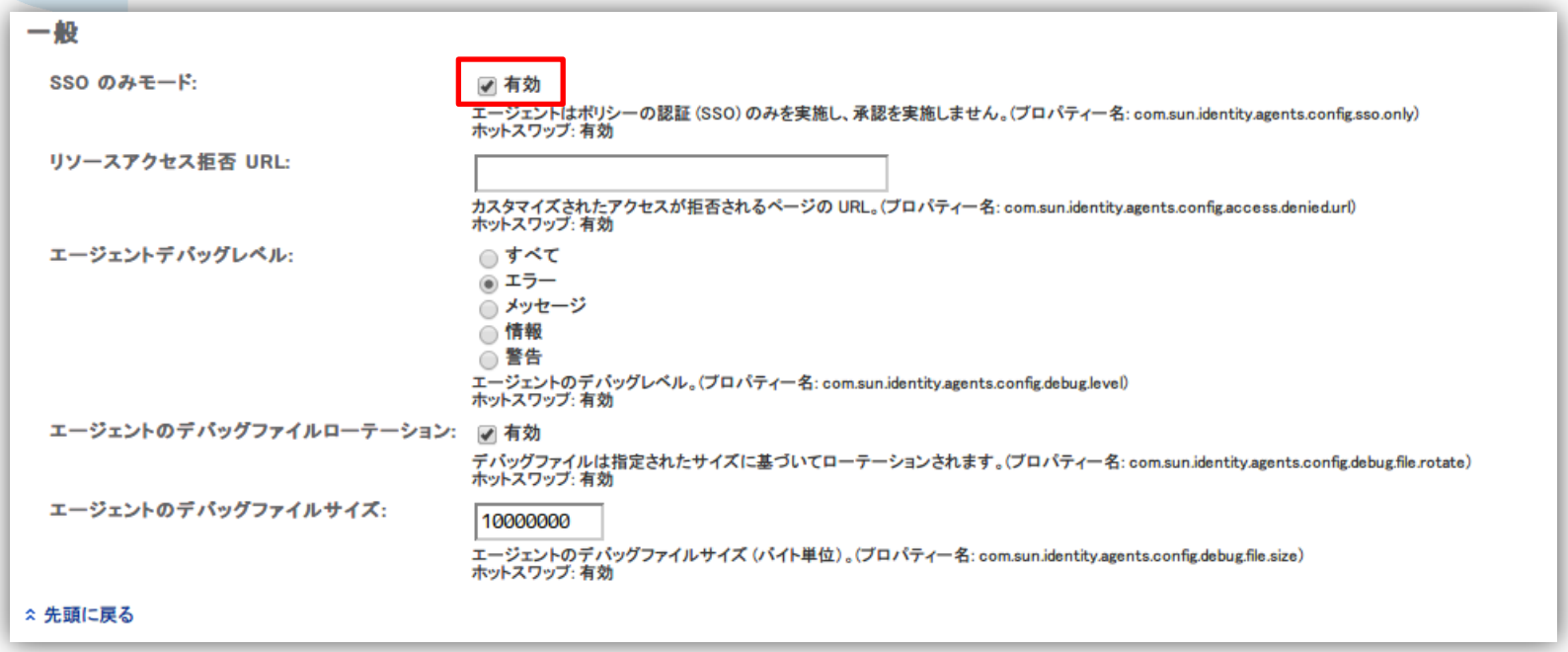
- エージェントの情報を入力して「作成」ボタンをクリック

エージェントプロファイルの作成

- 作成されたエージェント名をクリック

エージェントプロファイルの作成

- 「SSOのみモード」の「有効」にチェックを入れて「保存」ボタンをクリック
- その後ログアウト



連携確認

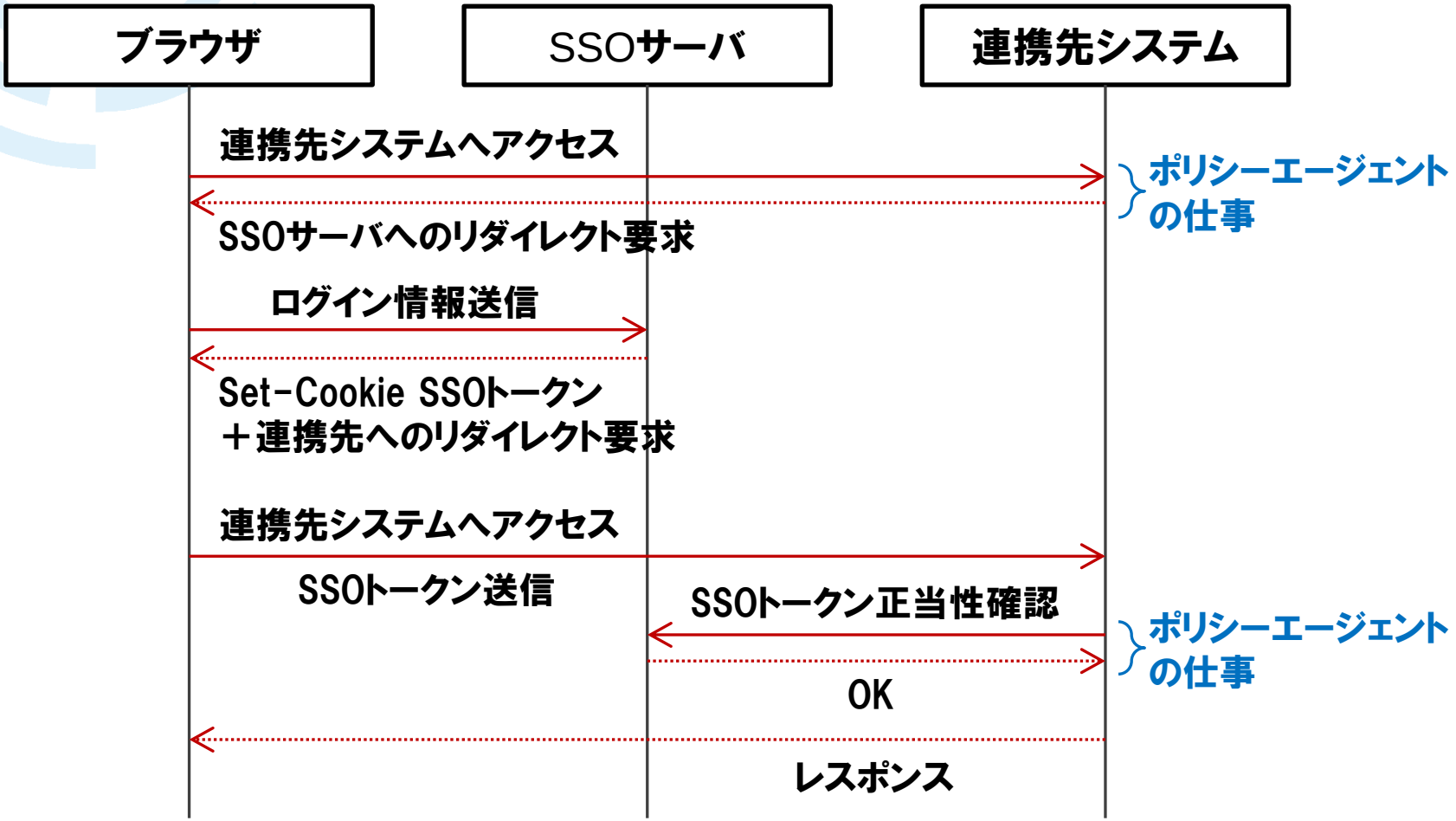
- 連携先システムにアクセス
  - ✓http://openam-app.nri.jp/app01
- OpenAMのログインページにリダイレクトされることを確認
  - ✓http://openam.nri.jp:8080/openam/UI/Login?goto=http%3A%2F%2Fopenam-app.nri.jp%2Fapp01

連携確認

- OpenAMのユーザでログイン（amadmin/adminpassword）すると、app01の画面が表示される
- このとき、HTTPヘッダに「iPlanetDirectoryPro」というSSOトークン（Cookie）が追加されていることを確認

```
管理者ユーザー向けサイト HTTPヘッダ SSO実行結果

想定通りのパラメータが送信されていることを確認してください。

---------- HTTPヘッダ ----------
ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ACCEPT_CHARSET = Shift_JIS,utf-8;q=0.7,*;q=0.3
ACCEPT_ENCODING = gzip,deflate,sdch
ACCEPT_LANGUAGE = ja,en-US;q=0.8,en;q=0.6
CACHE_CONTROL = max-age=0
CONNECTION = keep-alive
COOKIE = amlbcookie=01; iPlanetDirectoryPro=AQIC5wM2LY4SfcwtvDqwLv93UI9Q8wnkEsWboMzyjXA5tTM.*AAJTSQACMDE.*
HOST = openam-traning-app.nriossc.co.jp
REFERER = http://openam.nriossc.co.jp:8080/openam/UI/Login?goto=http%3A%2F%2Fopenam-traning-app.nriossc.co.jp%2Fapp01&gx_charset=UTF-8
USER_AGENT = Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31

---------- リクエストパラメータ ----------
```

構築したシステムは、以下のような動作をしています



ログインユーザのIDを連携

オープンソースまるごと
OpenStandia™
Open Source Technology

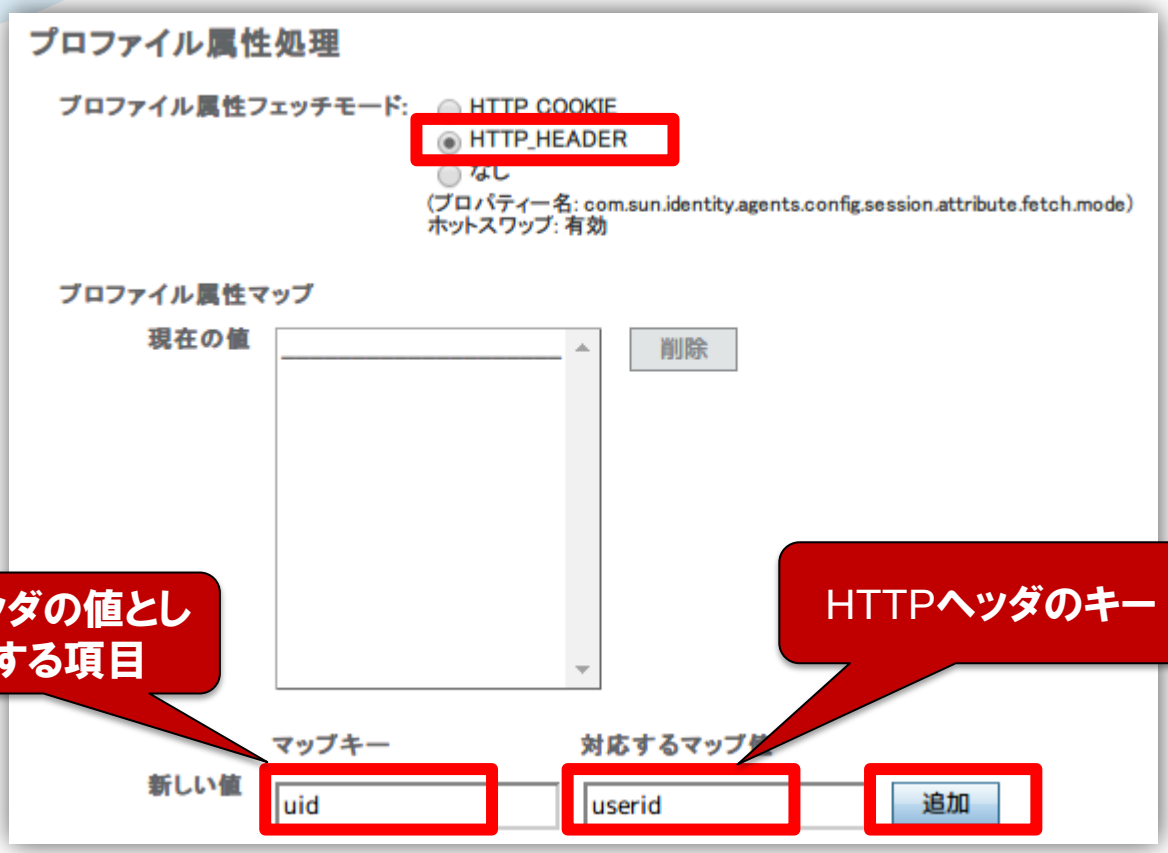
- HTTPヘッダにユーザIDを追加して連携する
  - アクセス制御＞(最上位のレルム)＞エージェント と遷移
  - エージェントの名前をクリックしてアプリケーションタブを開く

NRI 未来創発
Dream up the future.

ログインユーザのIDを連携

エージェントの設定を変更

- プロファイル属性処理を以下のように変更
- 「追加」をクリックした後、ページ上部の「保存」をクリック



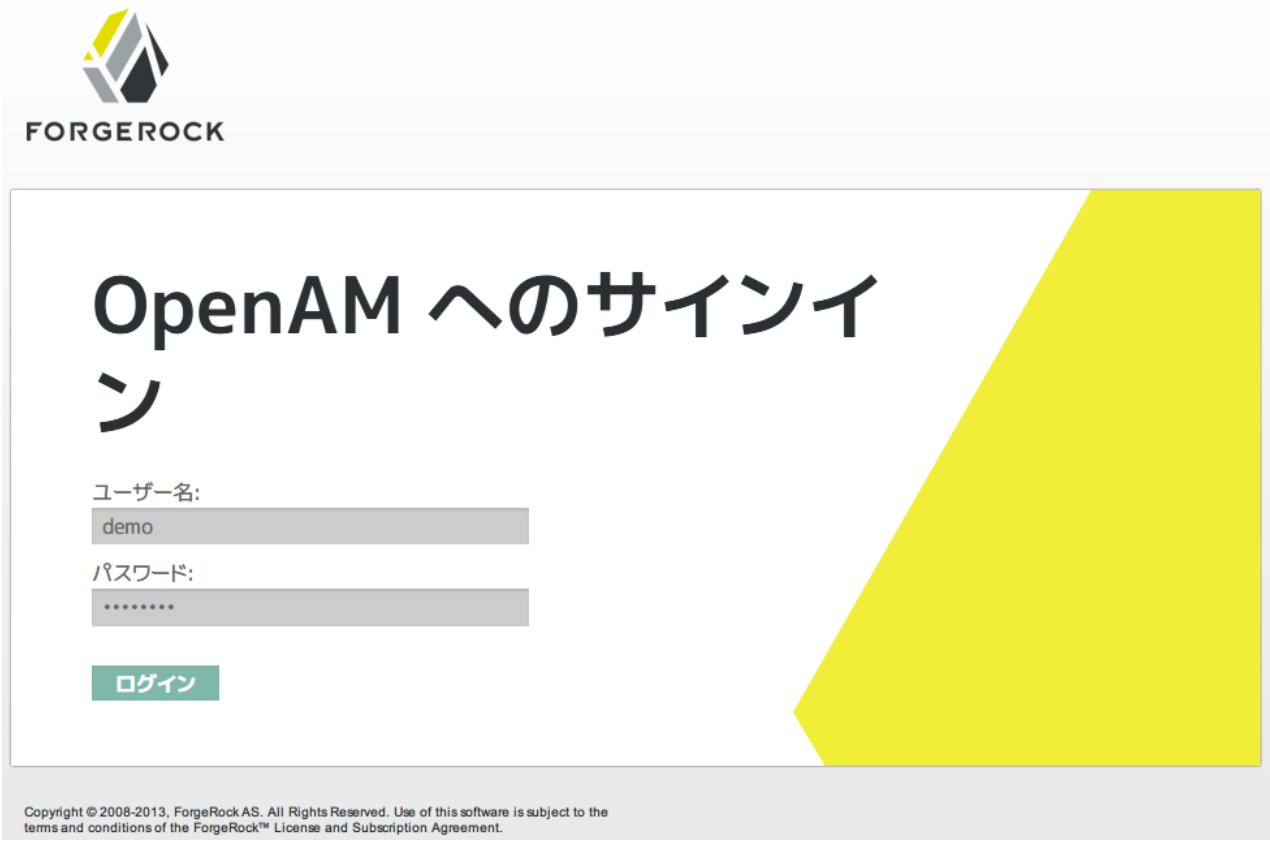
エージェントを再起動

連携先システムのApacheを再起動

```
# /etc/init.d/v-httpd restart
httpd を停止中:                                            [  OK  ]
httpd を起動中:                                            [  OK  ]
```

ログインユーザのIDを連携

- 連携先システムにアクセス
  - http://openam-app.nri.jp/app01
  - ID/PWを入力
    - ✓デフォルトで用意されているdemoユーザ（demo / changeit）でログイン



ログインユーザIDの連携を確認

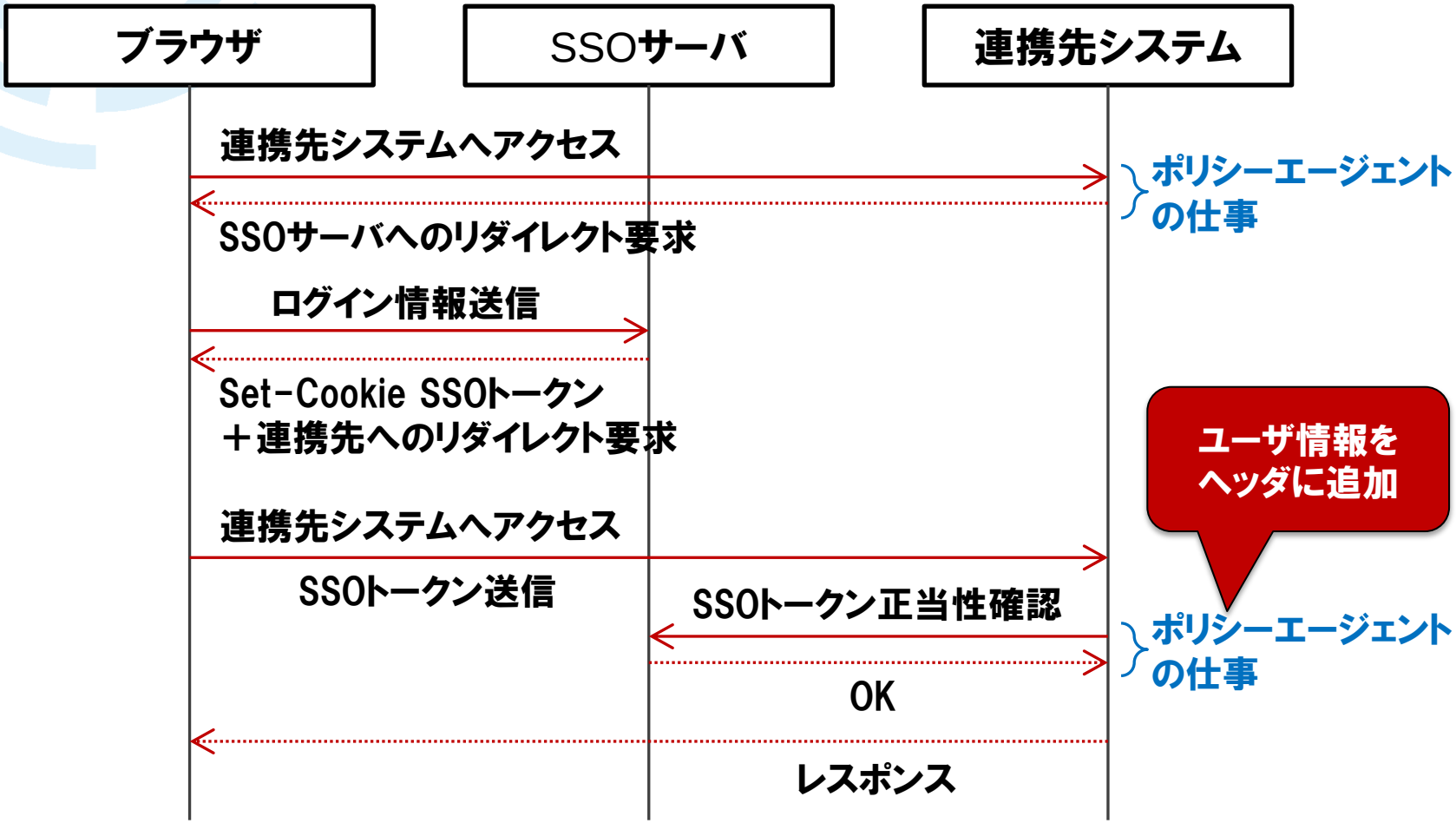
- HTTPヘッダに「USERID=demo」が追加されていることを確認

```
管理者ユーザー向けサイト HTTPヘッダ SSO実行結果

想定通りのパラメータが送信されていることを確認してください。

---------- HTTPヘッダ ----------
ACCEPT = text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
ACCEPT_CHARSET = Shift_JIS,utf-8;q=0.7,*;q=0.3
ACCEPT_ENCODING = gzip,deflate,sdch
ACCEPT_LANGUAGE = ja,en-US;q=0.8,en;q=0.6
CACHE_CONTROL = max-age=0
CONNECTION = keep-alive
COOKIE = amlbcookie=01; iPlanetDirectoryPro=AQIC5wM2LY4SfcxTaMZufuR6YGssjuid9PZdXud6ZFZxsAw.*AAJTSQACMDE.*
HOST = openam-traning-app.nriossc.co.jp
REFERER = http://openam.nriossc.co.jp:8080/openam/UI/Login?goto=http%3A%2F%2Fopenam-traning-app.nriossc.co.jp%2Fapp01
USERID = demo
USER_AGENT = Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.64 Safari/537.31

---------- リクエストパラメータ ----------
```

- これで、連携先システムがHTTPヘッダのUSERIDを参照してログインできる仕組みであれば、該当ユーザとしてログイン可能

連携確認

構築したシステムは、以下のような動作をしています



Section4

まとめ

まとめ

- **Section1：OpenAM概要**
  - SSOのメリットについて説明しました
  - OpenAMで実現可能なSSO方式をまとめました
- **Section2：OpenAMインストール**
  - OpenAMのインストールの流れを説明しました
- **Section3：連携先システムとのSSO**
  - エージェント方式のSSOの設定の流れを説明しました
  - ユーザIDを連携先システムに連携する方法を説明しました

- OpenStandiaは、「攻めのIT」を支援します。
- オープンソースのことなら、なんでもご相談ください！

オープンソースまるごと

OpenStandia™

Open Source Technology

お問い合わせは、NRIオープンソースソリューション推進室へ

ossc@nri.co.jp

http://openstandia.jp/

NRI 未来創発 Dream up the future.

- この後は「OpenStandia/SSO＆IDMソリューションのご紹介」です。

オープンソースまるごと

OpenStandia™

Open Source Technology

お問い合わせは、NRIオープンソースソリューション推進室へ

ossc@nri.co.jp

http://openstandia.jp/

NRI 未来創発 Dream up the future.