

OpenAMトレーニング

OpenAMでシングルサインオンを実現しよう！

- 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

● 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

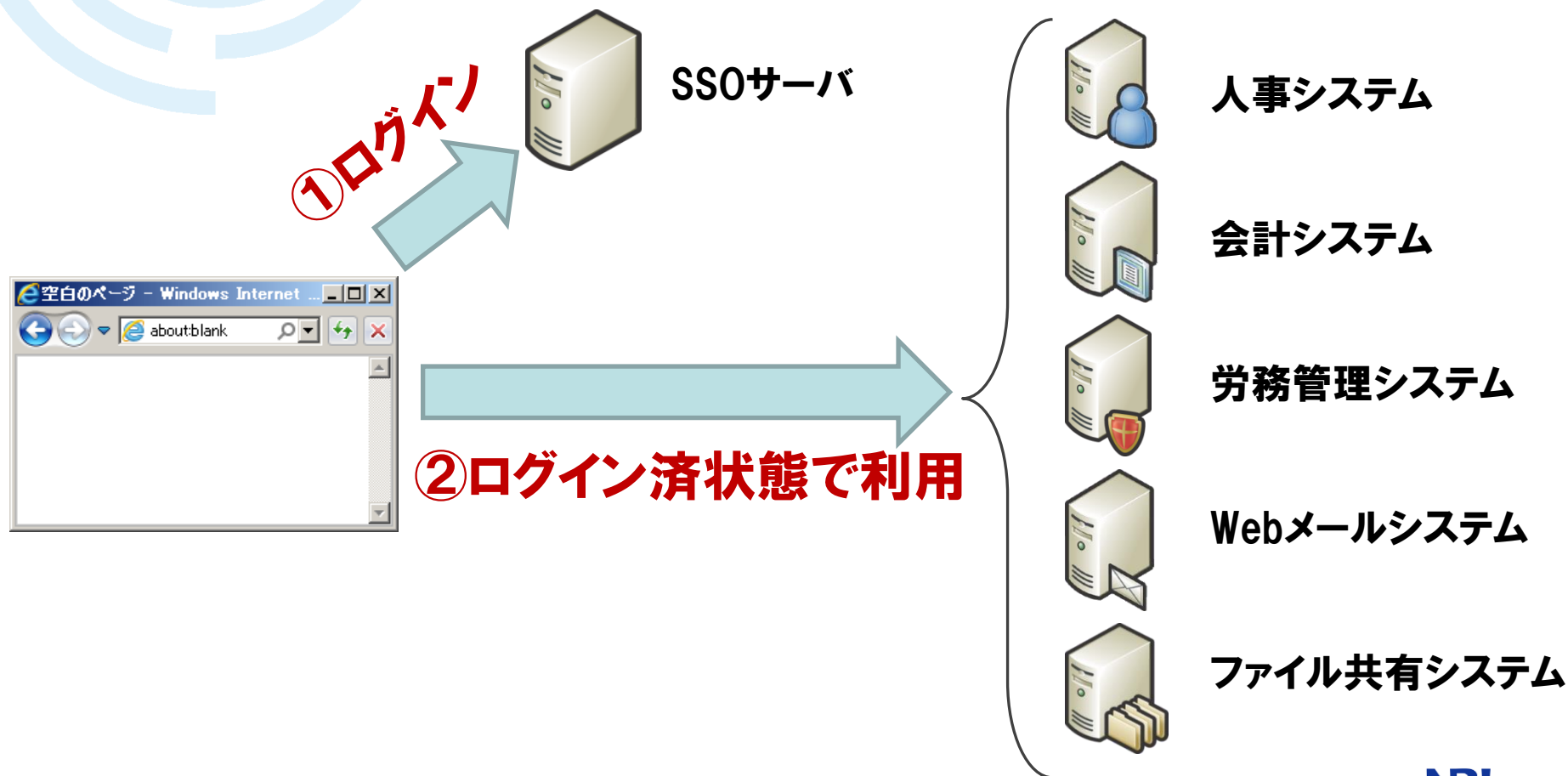
- ▶ SI
- ▶ システム運用維持管理
- ▶ 製品開発

Section 1

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

● 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

● 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



● SSOを実現するためのOSS

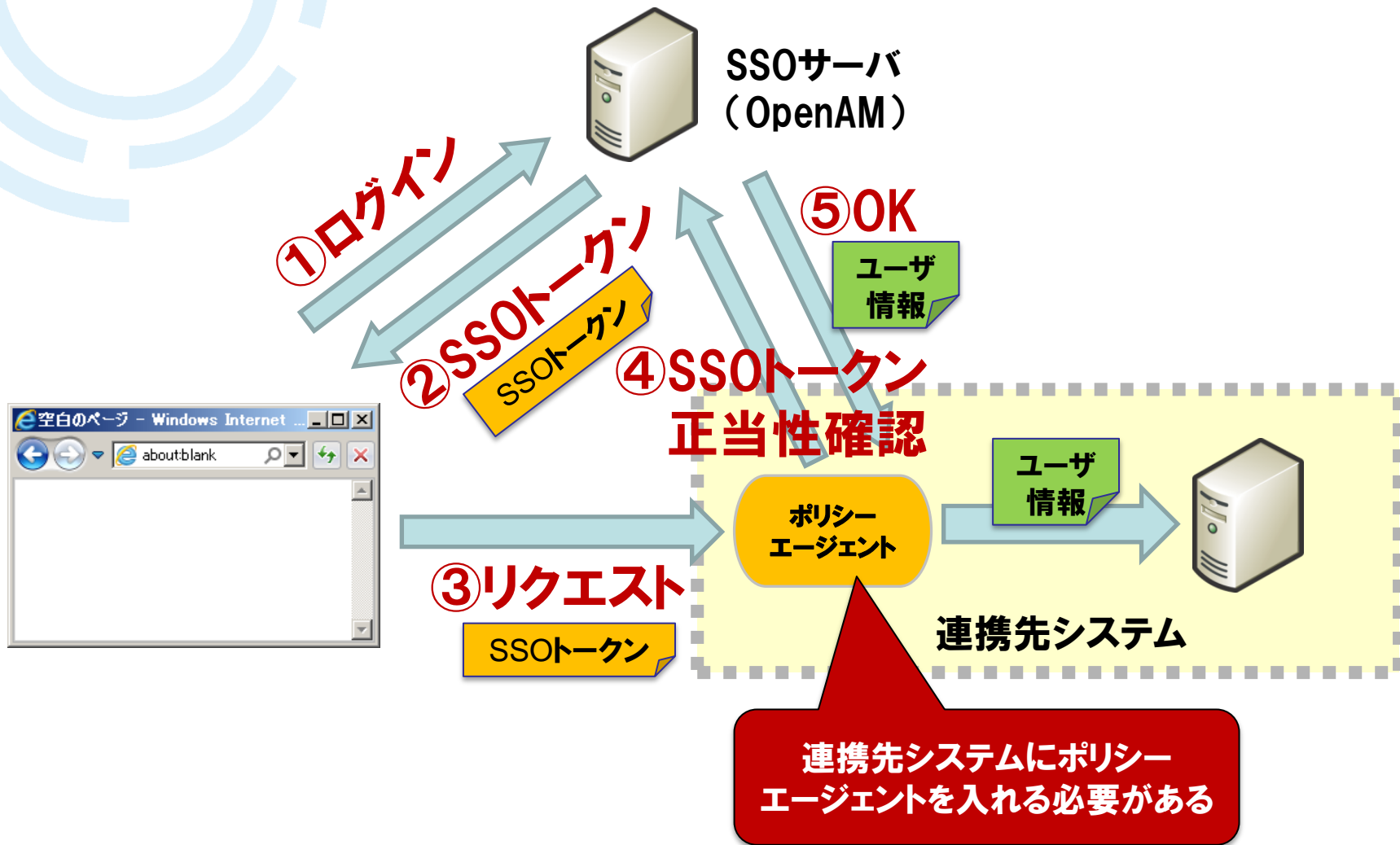
- ▶ 旧Sun Microsystems社の商用製品(OpenSSO)がベースであるため高品質かつ多機能
- ▶ ForgeRock社が継続開発中
- ▶ Javaで実装されたWebアプリケーションでOS非依存
- ▶ CDDL(Common Development and Distribution License)で、ソースコードを無償で使用、改変、再配布可能
- ▶ 最新の安定バージョンは**12.0.0**

● OpenAMの代表的なSSO方式

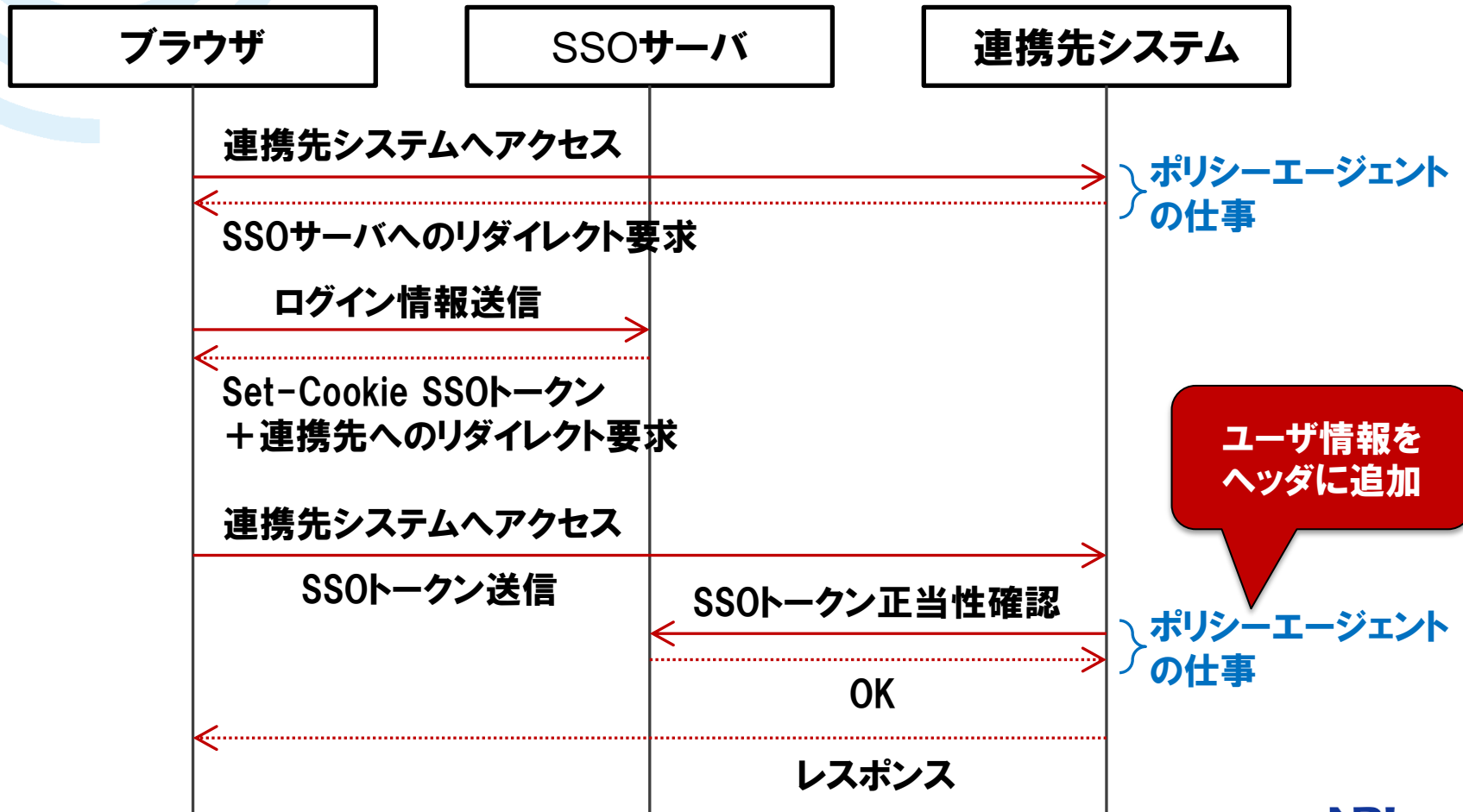
SSO方式	説明
エージェント方式	アプリケーションが動作するサーバに直接エージェントを導入する方式。
リバースプロキシ方式	リバースプロキシサーバ(通常はApache)にエージェントを導入し、バックエンドにいる複数のアプリケーションサーバに対してリバースプロキシする方式。
代理認証方式	代理認証とは、ユーザからのログインリクエストをエミュレートし、認証を代行すること。OpenIGと連携することで、代理認証が可能となる。 連携先システムで、HTTPヘッダから認証情報を取得するカスタマイズが出来ない際に採用する方式。
SAML	SAMLとは認証情報を表現するためのXML仕様。主にSalesforce、GoogleApps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と思われる。

SSO方式

● エージェント方式



● 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

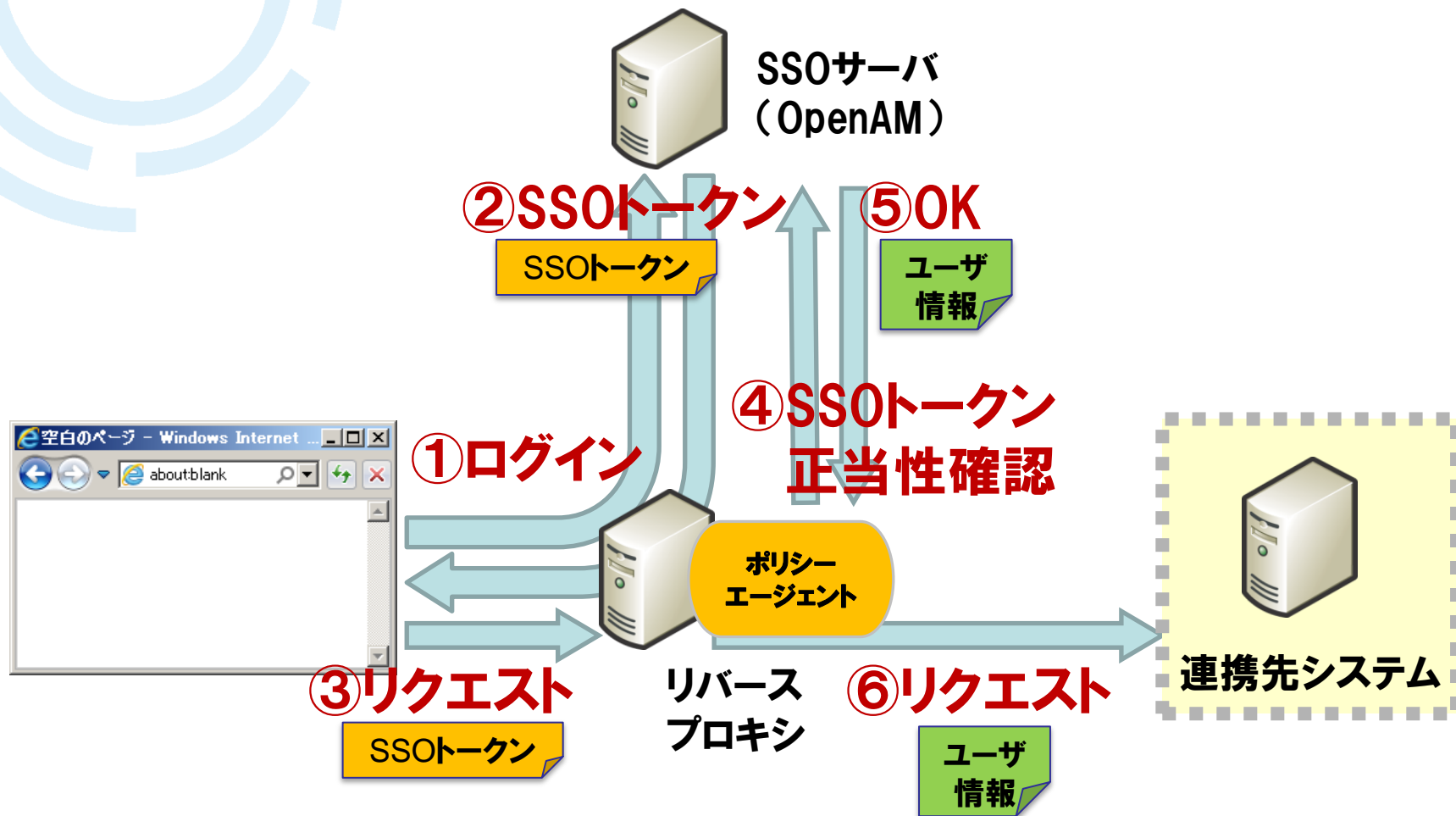
● ポリシーエージェントとは

- ▶ 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

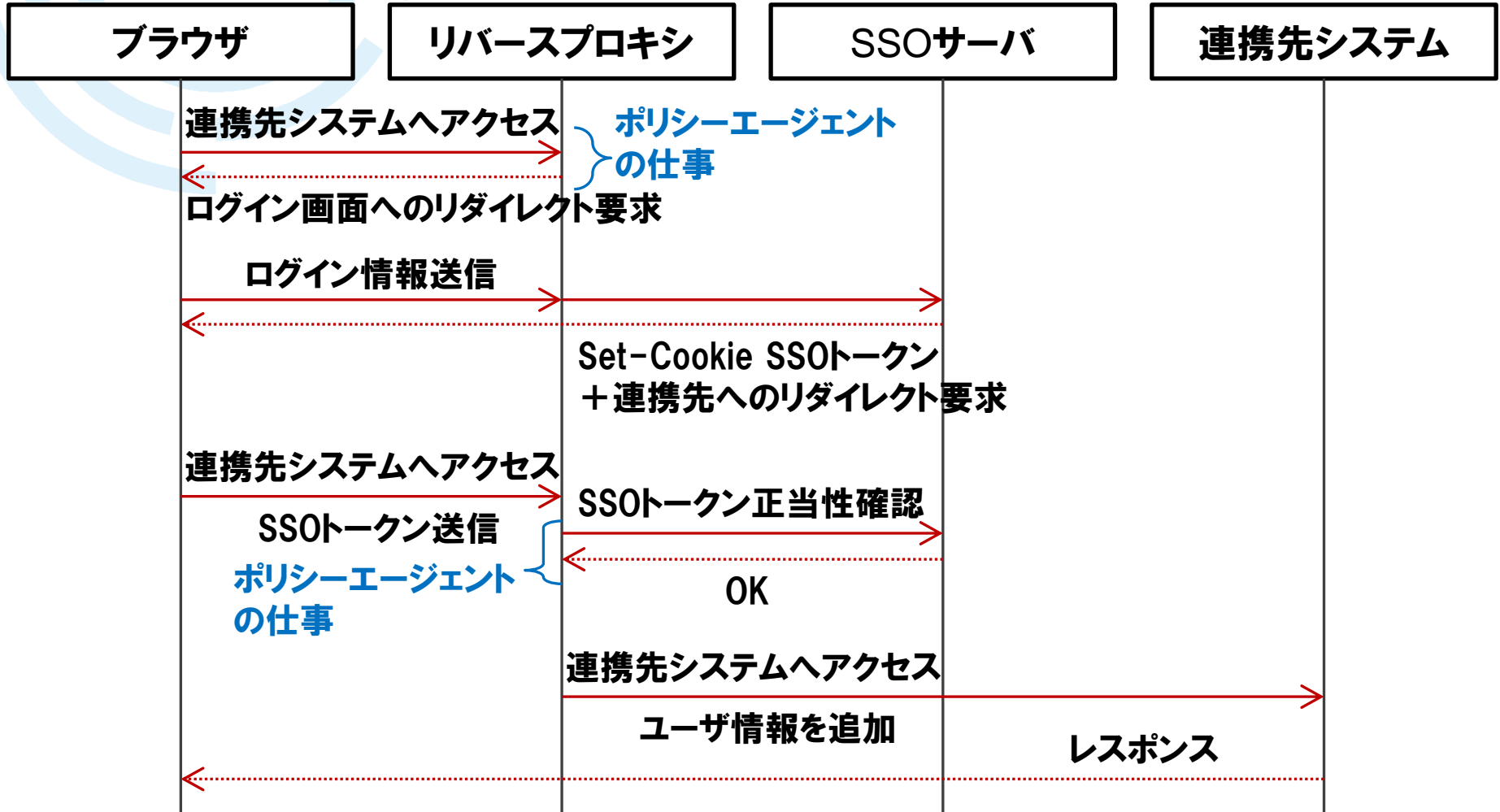
● 提供されているエージェントの種類

- ▶ 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

●リバーズプロキシ方式



●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

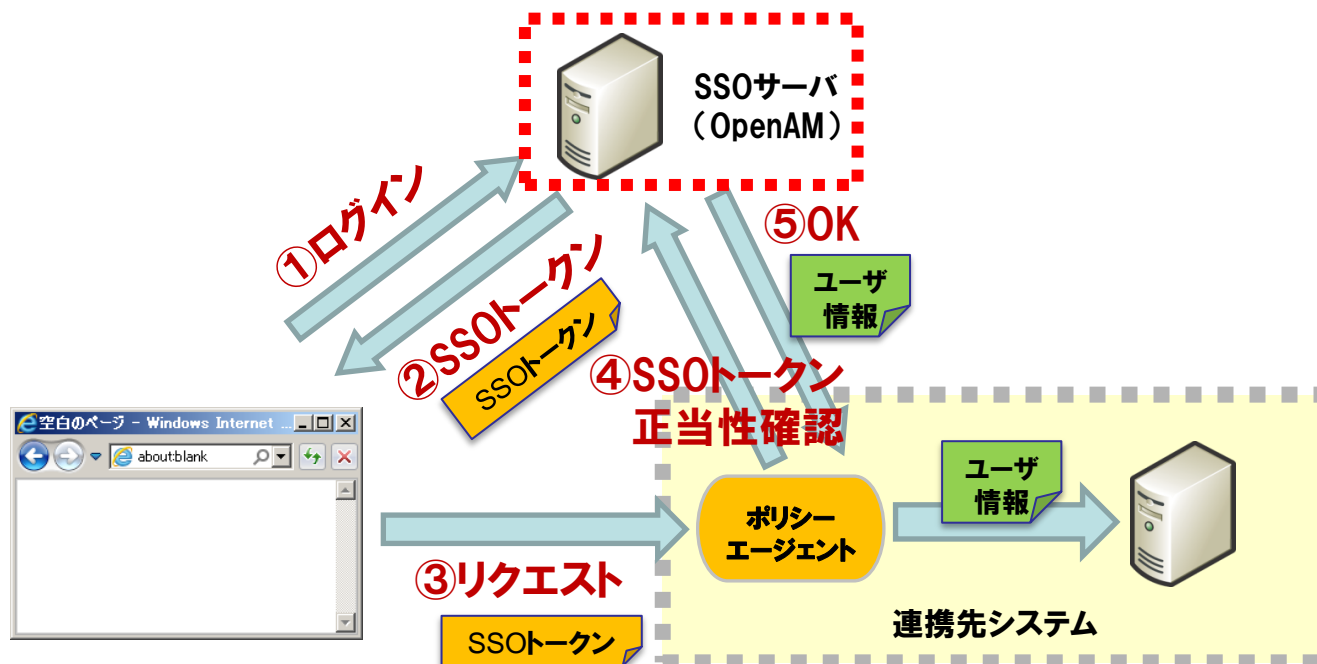
▶ OS

✓ CentOS6

▶ OpenAM

✓ 11.0.0

✓ ダウンロード元: <http://forgerock.org/openam-archive.html>



● 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

OpenAM
Download our OpenAM software, policy agents, Open Identity Gateway and documentation here.

OpenAM Enterprise

11.0.0 **latest** ▼

Title	Files
OpenAM 11	zip sha war tools configurator
10.1.0 EOSL	▶
10.0.1	▶

Web Policy Agents

3.3.0 ▼

● 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初期設定: Step 1

▶ <http://openam.nri.jp:8080/openam/>



設定オプション

設定オプションを選択してください。

デフォルト設定

デフォルト管理者とエージェントアクセサのパスワードのみを入力します。ほかのすべてのデータはデフォルトパラメータを使用して設定されます。このオプションは、主に評価または開発の目的に使用するようにしてください。

デフォルト設定の作成

カスタム設定

データストアのタイプ、暗号化のプロパティ、ユーザーデータストアなどを含む、すべての設定パラメータを指定できます。このオプションは、インストールの設定におけるもっとも高い柔軟性を備えています。

新しい設定の作成

● OpenAM初期設定: Step2

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

OpenAM 設定ツール

カスタム設定オプション

- 一般
- 2. サーバー設定
- 3. 設定ストア
- 4. ユーザーストア
- 5. サイト設定
- 6. エージェント情報
- 7. 概要

手順 1: 一般 ⓘ

デフォルトユーザー amAdmin のパスワードを入力します。パスワード長は 8 文字以上にする必要があります。この設定が既存の配備の一部になる場合は、入力するパスワードを元の配備のパスワードと一致させてください。

*必須フィールド

デフォルトユーザーパスワード

デフォルトユーザー [amAdmin]

*パスワード 了解

*パスワードの確認

戻る 次へ 取消し

● 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OK

The screenshot shows the 'OpenAM 設定ツール' (OpenAM Configuration Tool) window. The title bar reads 'OpenAM 設定ツール'. The main content area is titled 'カスタム設定オプション' (Custom Setting Options). On the left, a navigation menu lists steps: 1. 一般, 2. サーバー設定 (selected), 3. 設定ストア, 4. ユーザーストア, 5. サイト設定, 6. エージェント情報, 7. 概要. The main panel is titled '手順 2: サーバー設定' (Step 2: Server Settings) and includes the instruction 'サーバーで使用する次の設定を確認します。' (Check the following settings to be used on the server.) and a note '*必須フィールド' (Required field). Below this, the 'サーバー設定' (Server Settings) section contains four fields: '*サーバー URL' (http://openam.nri.jp:8080), '*Cookieドメイン' (.nri.jp) with a checked '了解' (I understand) checkbox, '*プラットフォームロケール' (en_US), and '*設定ディレクトリ' (/root/OpenAM-11.0.0). At the bottom, there are three buttons: '戻る' (Back), '次へ' (Next), and '取消し' (Cancel).

● OpenAM初期設定: Step4 ▶ 「最初のインスタンス」を選択して次へ

OpenAM 設定ツール

カスタム設定オプション

- 一般
- サーバー設定
- 設定ストア
- ユーザーストア
- サイト設定
- エージェント情報
- 概要

手順 3: 設定データストア設定

環境にほかの既存の OpenAM インスタンスがなければ、「最初のインスタンス」を選択します。環境に 1 つ以上の既存の OpenAM インスタンスがあれば、「既存の配備に追加しますか。」を選択します。

最初のインスタンス 既存の配備に追加しますか。 * 必須フィールド

設定ストアの詳細

設定データストア OpenAM OpenDJ or Oracle Directory Server Enterprise Edition

* SSL が有効

* ホスト名

* ポート

* Admin Port

* JMX Port

* 暗号化鍵

* ルートサフィックス

戻る 次へ 取消し

● 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 設定ツール

カスタム設定オプション

1. 一般
2. サーバー設定
3. 設定ストア
- ユーザーストア
5. サイト設定
6. エージェント情報
7. 概要

手順 4: ユーザーデータストア設定

OpenAM 設定データストアに付属のデータストアを使用することも、別のユーザーデータストアを使用することもできます。本稼働環境を設定する際には、OpenAM ユーザーデータストアとは異なる外部のユーザーデータストアを使用することをお勧めします。ここで指定したディレクトリ管理者 DN とパスワードを使用するようポリシーサービスと LDAP 認証モジュールが設定されることに注意してください。

OpenAM のユーザーデータストア
 その他のユーザーデータストア

*必須フィールド

ユーザーストアの詳細

❌ OpenAM ユーザーデータストアの使用は、デモ目的または開発環境内でのみサポートされます。OpenAM ユーザーデータストアは、本稼働環境ではサポートされません。

戻る 次へ 取消し

● OpenAM初期設定: Step6

▶ 「いいえ」を選択して次へ

OpenAM 設定ツール

カスタム設定オプション

1. 一般
2. サーバー設定
3. 設定ストア
4. ユーザストア
- **5. サイト設定**
6. エージェント情報
7. 概要

手順 5: サイト設定

このインスタンスは、サイト設定の一部としてロードバランサの背後に配備されますか？

いいえ
 はい

*必須フィールド

サイト設定の詳細

これは OpenAM の最初のインスタンスで、現在、サイト設定は存在しません。新しいサイト設定を作成するには、次の情報を入力します

*サイト名

*ロードバランサの URL

Enable Session HA Persistence and Failover

戻る 次へ 取消し

● 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 設定ツール

カスタム設定オプション

- 一般
- サーバー設定
- 設定ストア
- ユーザーストア
- サイト設定
- エージェント情報
- 概要

手順 6: デフォルトのポリシーエージェントユーザー ⚠

これらの設定は、ポリシーエージェントのプロパティを取得するために OpenAM ポリシーエージェントで使用されます。

*必須フィールド

ポリシーエージェントユーザー

デフォルトポリシーエージェント [UrlAccessAgent]

*パスワード 了解

*パスワードの確認

戻る 次へ 取消し

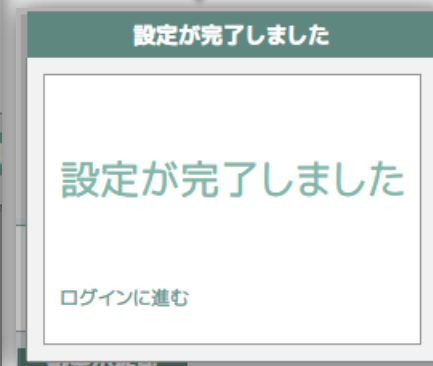
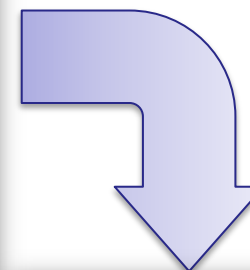
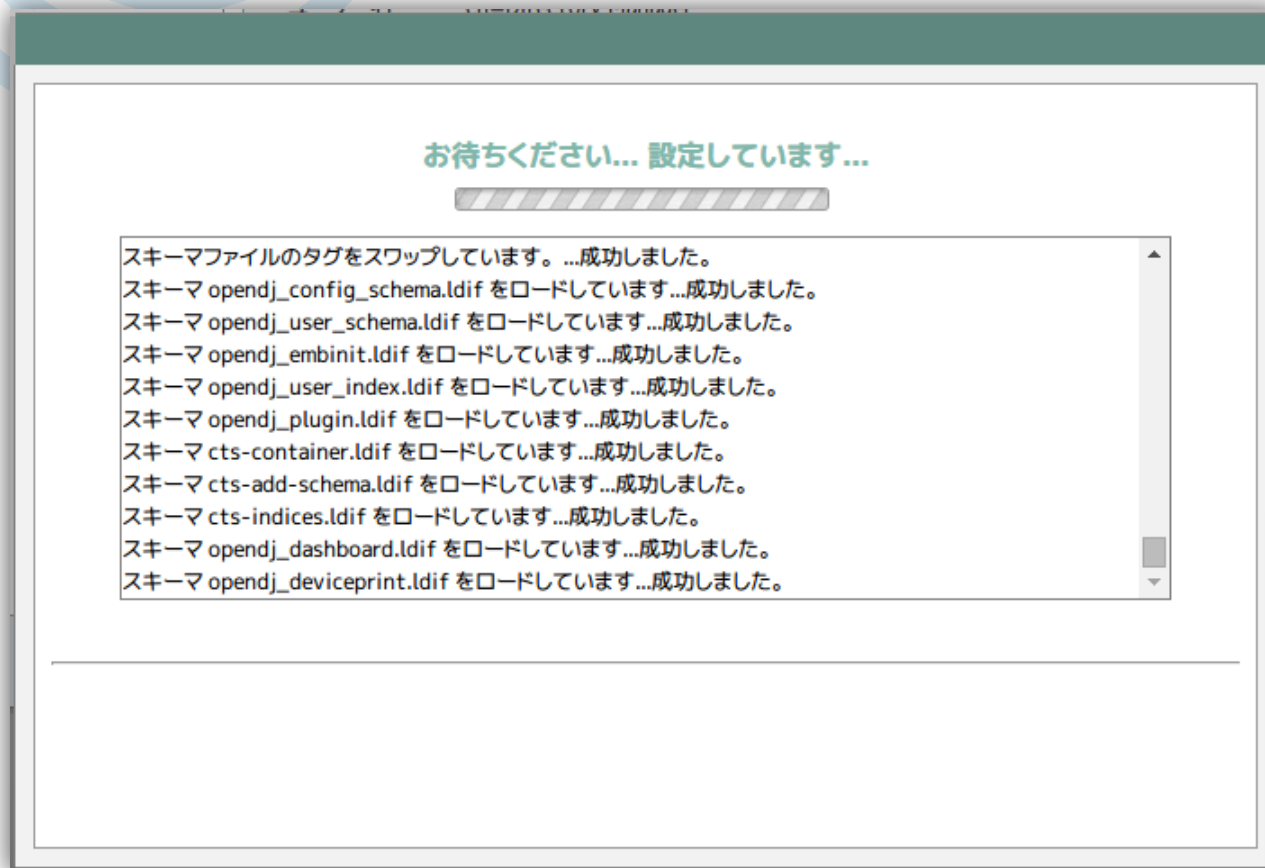
● OpenAM初期設定: Step8

▶ 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

FORGEROCK

OpenAM へのサインイン

ユーザー名:
amadmin

パスワード:
.....

ログイン

Copyright © 2008-2013, ForgeRock AS. All Rights Reserved. Use of this software is subject to the terms and conditions of the ForgeRock™ License and Subscription Agreement.

● 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

The screenshot shows the OpenAM management console interface. At the top, it displays the user 'amAdmin' and server 'openam.nri.jp'. The main navigation bar includes '共通タスク', 'アクセス制御', '連携', '設定', and 'セッション'. The '設定' (Settings) tab is active, showing several configuration tasks:

- SAMLv2 プロバイダを作成**: Instructions to create SAMLv2 providers. Tasks include: 'ホストアイデンティティプロバイダの作成', 'ホストサービスプロバイダの作成', 'リモートアイデンティティプロバイダを登録', and 'リモートサービスプロバイダを登録'.
- Configure OAuth2**: A task to configure OAuth2 per realm.
- Fedlet を作成**: Instructions to create Fedlets for integration with external identity providers.
- Google Apps の設定**: Instructions to configure Google Apps Web applications for single sign-on.
- Salesforce CRM の設定**: Instructions to integrate OpenAM with Salesforce CRM.
- 連携の接続性をテスト**: A task to test the connectivity of integrations.
- 製品マニュアルを取得**: A task to retrieve the product manual.

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

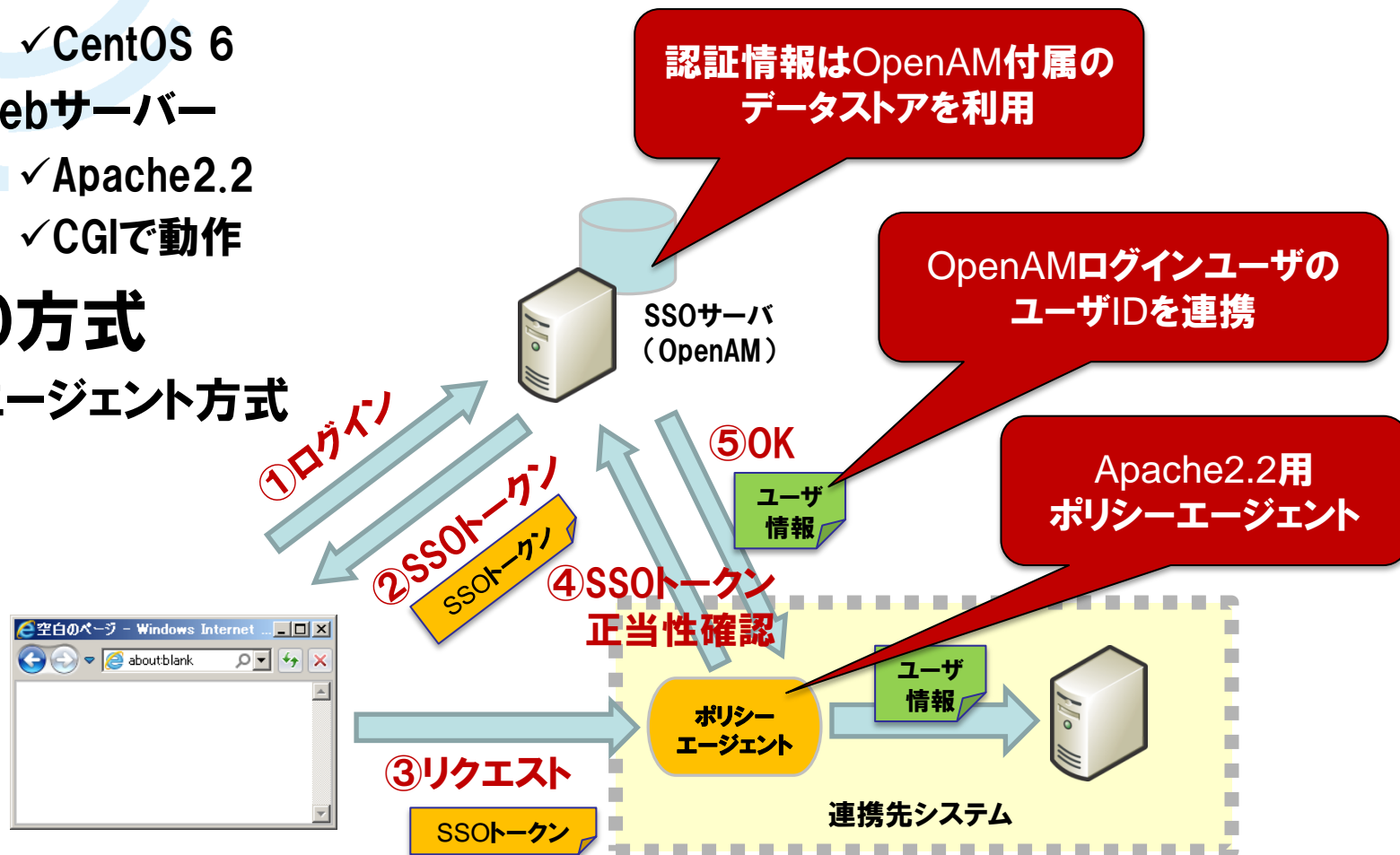
▶ Webサーバー

✓ 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-training-app.nrioss.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 -----

連携先システムの構築






● 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
```

● ポリシーエージェントをダウンロード

▶ <http://forgerock.org/downloads/openam-builds/>

FORGEROCK™ PROJECTS COMMUNITY CONTRIBUTE SECURITY ADVISORIES **DOWNLOADS**

OpenAM Nightly Builds

Release	Built from	Notes	Build Date
[Nightly Build][SHA][WAR][TOOLS]	trunk	Latest nightly build	20140701

Web Policy Agents

Agent Type	Operating System Type	32/64 bits	Build Date	
Apache 2.2	Linux	64 bits	20140703	Download SHA

Java EE Policy Agents

Container	Version	Policy Agent version	Build Date
Glassfish [SHA]	2.x & 3.x	4.0.0-SNAPSHOT	20140701
Glassfish v2 [SHA]	JSR196 & JSR115	4.0.0-SNAPSHOT	20140701
JBoss [SHA]	EAP 5.x	4.0.0-SNAPSHOT	20140701
JBoss [SHA]	EAP 6.x & AS 7.x	4.0.0-SNAPSHOT	20140701
Jetty [SHA]	6.1	4.0.0-SNAPSHOT	20140701
Jetty [SHA]	7 & 8	4.0.0-SNAPSHOT	20140701
Tomcat [SHA]	6.0.x & 7.0.x	4.0.0-SNAPSHOT	20140701
WebLogic [SHA]	10g, 11g & 12c	4.0.0-SNAPSHOT	20140701
Websphere [SHA]	7, 8 & 8.5	4.0.0-SNAPSHOT	20140701

● 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

FORGEROCK

OpenAM へのサインイン

ユーザー名:
amadmin

パスワード:
.....

ログイン

Copyright © 2008-2013, ForgeRock AS. All Rights Reserved. Use of this software is subject to the terms and conditions of the ForgeRock™ License and Subscription Agreement.

● 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

The image shows three overlapping screenshots of the ForgeRock OpenAM web interface, illustrating the steps to create an agent profile:

- Top Screenshot:** The 'アクセス制御' (Access Control) menu item is highlighted with a red box. The breadcrumb path is 'ホーム > アクセス制御 > (最上位のレルム) > エージェント'.
- Middle Screenshot:** The 'エージェント' (Agents) tab is highlighted with a red box. The breadcrumb path is 'ホーム > アクセス制御 > (最上位のレルム) > エージェント'.
- Bottom Screenshot:** The '新規...' (New) button is highlighted with a red box. The breadcrumb path is 'ホーム > アクセス制御 > (最上位のレルム) > エージェント > エージェント (0 エージェント)'.

● 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

バージョン

ユーザー: amAdmin サーバー: openam.nri.jp

 FORGEROCK

新しい Web

* 名前:

* パスワード:

* パスワードの再入力:

設定: ローカル 集中
エージェントプロパティが格納されている場所。「ローカル」は、エージェントが実行されているサーバーです。「集中」は、OpenAM サーバーです。

* サーバー URL:
プロトコル//ホスト:ポート/deploymentUri (たとえば、<http://opensso.sample.com:58080/opensso>)

* エージェント URL:
プロトコル//ホスト:ポート (たとえば、<http://agent1.sample.com:1234>)

● 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

The screenshot shows the ForgeRock OpenAM administration console. At the top, it displays the user 'amAdmin' and server 'openam.nri.jp'. The main navigation bar includes tabs for '一般', '認証', 'サービス', 'データストア', '権限', 'ポリシー', '対象', and 'エージェント'. The 'エージェント' tab is selected, and the 'Web' sub-tab is active. Below the navigation, there is a breadcrumb path '/ (最上位のレルム)' and a section titled 'Web' with a description: 'Web エージェントは、Apache Web Server や Microsoft IIS などの Web サーバーを保護します。' A search input field with a '検索' button is present. The main content area is titled 'エージェント (1 エージェント)' and contains a table with one entry: 'openam-app'. The '名前' column header and the 'openam-app' text are highlighted with a red box. Action buttons for '新規...', '削除', and a refresh icon are visible above and below the table.

OpenAMの設定

● 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

一般

SSO のみモード: 有効
エージェントはポリシーの認証 (SSO) のみを実施し、承認を実施しません。(プロパティ名: com.sun.identity.agents.config.sso.only)
ホットスワップ: 有効

リソースアクセス拒否 URL:
カスタマイズされたアクセスが拒否されるページの URL。(プロパティ名: com.sun.identity.agents.config.access.denied.url)
ホットスワップ: 有効

エージェントデバッグレベル:
 すべて
 エラー
 メッセージ
 情報
 警告
エージェントのデバッグレベル。(プロパティ名: com.sun.identity.agents.config.debug.level)
ホットスワップ: 有効

エージェントのデバッグファイルローテーション: 有効
デバッグファイルは指定されたサイズに基づいてローテーションされます。(プロパティ名: com.sun.identity.agents.config.debug.file.rotate)
ホットスワップ: 有効

エージェントのデバッグファイルサイズ:
エージェントのデバッグファイルサイズ (バイト単位)。(プロパティ名: com.sun.identity.agents.config.debug.file.size)
ホットスワップ: 有効

※ 先頭に戻る

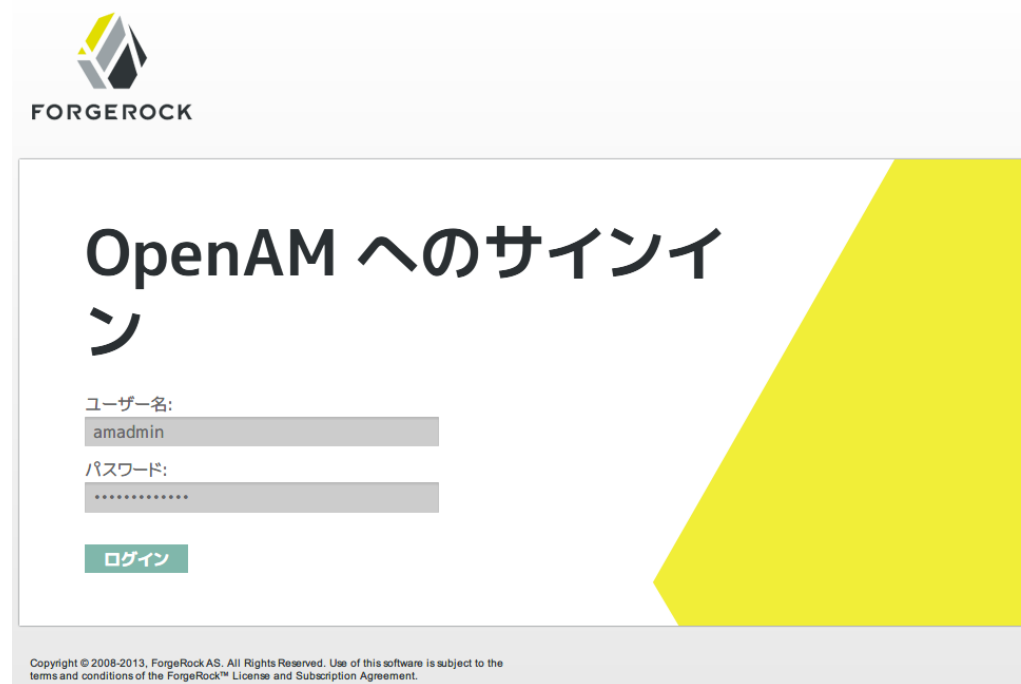
● 連携確認

▶ 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>



FORGEROCK

OpenAM へのサインイン

ユーザー名:
amadmin

パスワード:
.....

ログイン

Copyright © 2008-2013, ForgeRock AS. All Rights Reserved. Use of this software is subject to the terms and conditions of the ForgeRock™ License and Subscription Agreement.

連携確認

● 連携確認

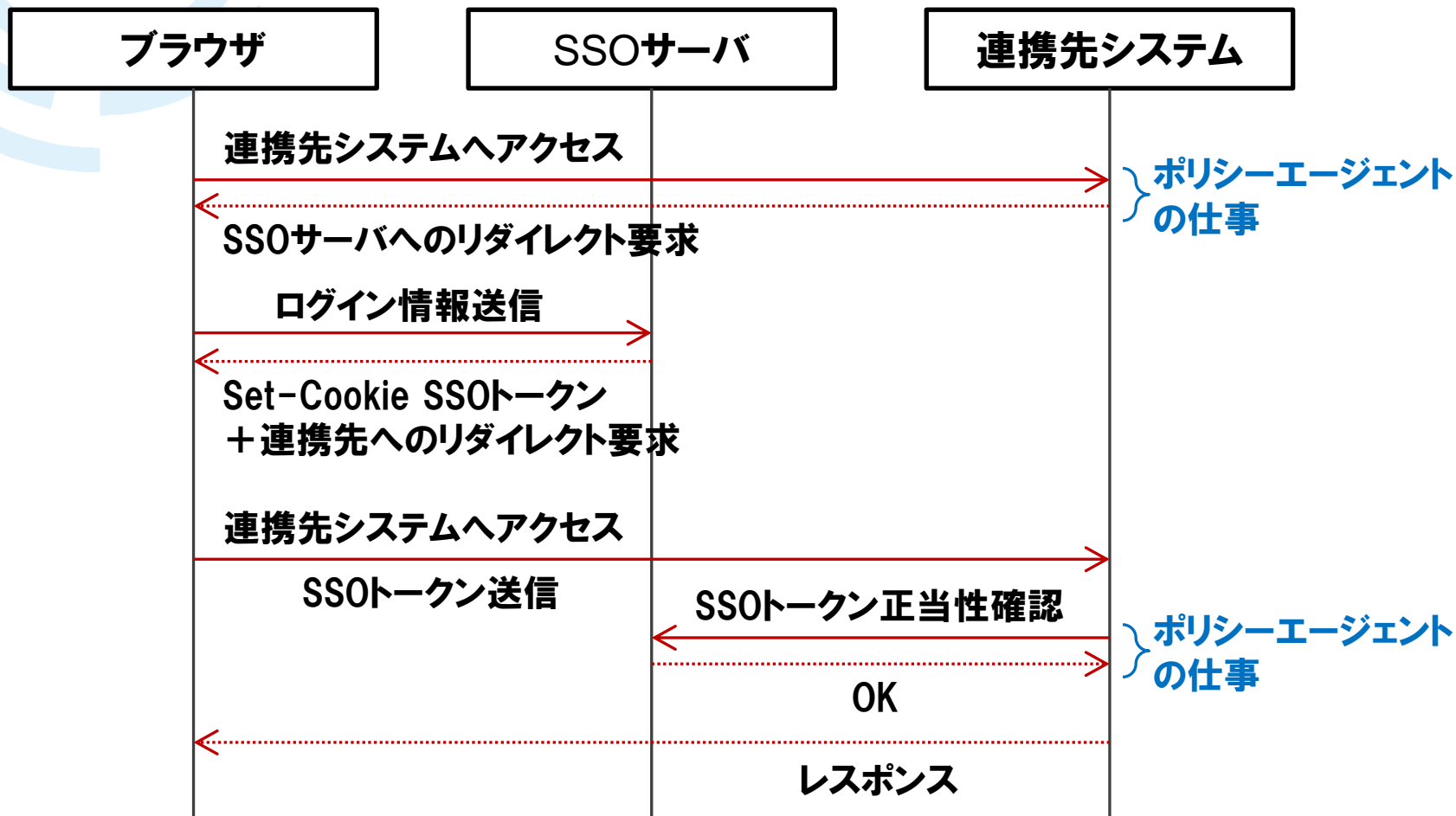
- ▶ OpenAMのユーザでログイン(amadmin/ adminpassword)すると、 app01の画面が表示される
- ▶ このとき、HTTPヘッダに「 iPlanetDirectoryPro 」というSSOトークン(Cookie)が追加されていることを確認

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-a  
REFERER = http://openam.nriossco.jp:8080/openam/UI/Login?goto=http%3A%2F%2Fopenam-traning-app.nriossco.jp%2Fapp01&gx_charset=UTF-8  
USER_AGENT = Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.84 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

- 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



The screenshots illustrate the following steps in the ForgeRock OpenAM administration interface:

- Access Control > Policies > Agents:** The 'Agents' tab is selected in the top navigation bar.
- Realm Selection:** The '(最上位のレルム) - プロパティ' (Top-level realm - Properties) page is shown, with the '(最上位のレルム)' (Top-level realm) selected in the list.
- Agent Configuration:** The 'エージェント (1 エージェント)' (Agents) list shows 'openam-app' selected.
- Application Tab:** The 'アプリケーション' (Application) tab is selected, showing configuration options for 'openam-app' such as '適用されない URL 処理' (Inapplicable URL processing).

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

プロフィール属性処理

プロフィール属性フェッチモード: HTTP_COOKIE HTTP_HEADER なし
(プロパティ名: com.sun.identity.agents.config.session.attribute.fetch.mode)
ホットスワップ: 有効

プロフィール属性マップ

現在の値

	削除
--	----

新しい値

マップキー	対応するマップ値	
uid	userid	追加

HTTPヘッダの値として表示する項目

HTTPヘッダのキー

● 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



FORGEROCK

OpenAM へのサインイン

ユーザー名:
demo

パスワード:
.....

ログイン

Copyright © 2008-2013, ForgeRock AS. All Rights Reserved. Use of this software is subject to the terms and conditions of the ForgeRock™ License and Subscription Agreement.

ログインユーザのIDを連携

● 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。

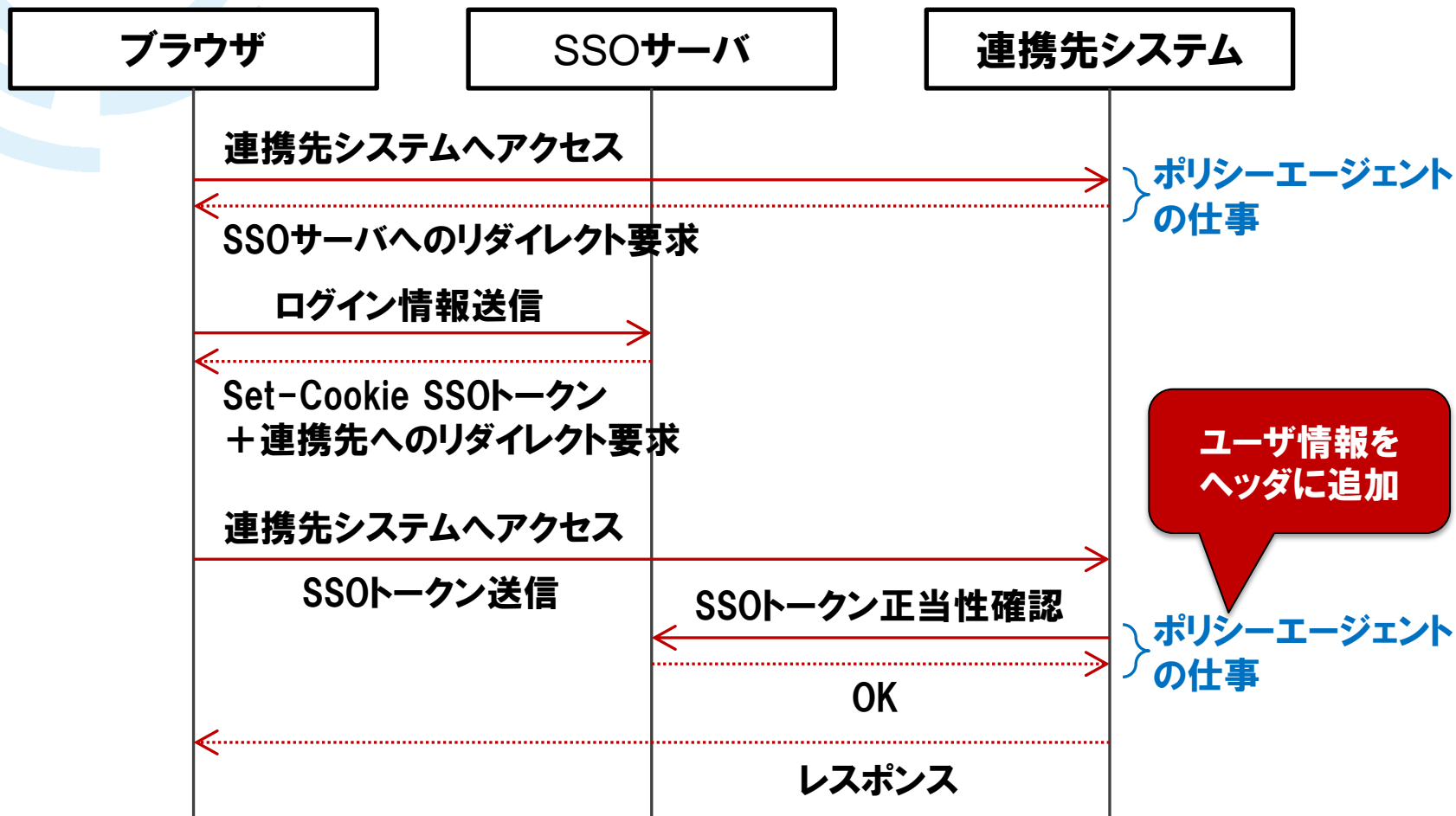
----- HTTPヘッダ -----

```
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.nriossco.jp
REFERER = http://openam.nriossco.jp:8080/openam/UI/Login?goto=http%3A%2F%2Fopenam-traning-app.nriossco.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

●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

● Section 1 : 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

● Section 2 : 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

● Section 3 : 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



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/>

本資料に掲載されている会社名、製品名、サービス名は各社の登録 商標、又は商標です。

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



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/>

本資料に掲載されている会社名、製品名、サービス名は各社の登録 商標、又は商標です。