

OpenAMトレーニング

OpenAMでシングルサインオンを実現しよう!



野村総合研究所のOpenStandia(オープン スタンディア)は、おかげさまで、2006年 のサービス開始から2011年までの5年間で 契約数累計が1,000件を突破いたしました!



Mail: ossc@nri.co.jp Web: http://openstandia.jp/

OpenStandia Open Source Technology

オープンソースまるごと







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

З







林田 敦

●所属部署

▶オープンソースソリューション推進室(OSSC)

▶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



►SI

▶システム運用維持管理

▶製品開発

▶0SSサポート







Section1 OpenAM概要



NRIオープンソースソリューションセンター Copyright[©] Nomura Research Institute, Ltd. All rights reserved.

シングルサインオン(SSO)とは



Dream up the future

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





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



シングルサインオン(SSO)とは



● OpenStandiaのSSO導入事例

√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、顧客システムとをシン 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





Open AM

SSOを実現するためのOSS

- In 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)ライセンスで、 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10.0.1





OpenAMの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。
[参考] SAML	SAMLとは認証情報を表現するためのXML仕様。おもにクロス ドメインのサイトやSalesforce、GoogleAppsとSSOする際に採 用する方式。
[参考] 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。







Dream up the future





Dream up the futur

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





14



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用 ✓Microsoft IIS 6.0、7.0 等

▶J2EEポリシー エージェント

15

✓Tomcat 6.0 ✓JBoss v 4.2 & v 5.x 等















Dream up the futur

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





Dream up the future





●ネットワークのセットアップ(FQDNの登録)

/etc/sysconfig/network

HOSTNAME=openam.nriossc.co.jp

/etc/hosts

192.175.204.101 openam.nriossc.co.jp

●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

20

\$ 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
- <u>http://www.oracle.com/technetwork/java/javase/downloads/jdk</u>
 <u>6u37-downloads-1859587.html</u>
 - ✓「Accept License Agreement」をクリックしてから「jdk-6u37-linuxi586-rpm.bin」をクリック

Java SE Development Kit 6 Update 37

0

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	65.43 MB	보 jdk-6u37-linux-i586-rpm.bin
.inux x86	68.44 MB	👤 jdk-6u37-linux-i586.bin
Linux x64	65.65 MB	👤 jdk-6u37-linux-x64-rpm.bin
Linux x64	68.71 MB	👤 jdk-6u37-linux-x64.bin
Linux Intel Itanium	53.95 MB	idk 6u27 linux io64 rom bin





JDKのインストール



chmod 755 jdk-6u37-linux-i586-rpm.bin
./jdk-6u37-linux-i586-rpm.bin
java -version
java version "1.6.0_37"

▶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 Id-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.tsukuba.wide.ad.jp/software/apache/tomcat/tomcat-6/v6.0.37/bin/apache-tomcat-6.0.37.tar.gz

tar zxvf apache-tomcat-6.0.37.tar.gz
mv apache-tomcat-6.0.37 /usr/share/tomcat6

/root/.bash_profile

23

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





▶warファイルをダウンロードしてTomcatにデプロイする

wget

24

http://download.forgerock.org/downloads/openam/openam10/ 10.0.1/openam_10.0.1.war

cp -p openam_10.0.1.war /usr/share/tomcat6/webapps/

▶Tomcatを起動する

/usr/share/tomcat6/bin/startup.sh





OpenAM初期設定:Step1

http://openam.nriossc.co.jp:8080/openam/



25

没定オブションを選択してください。	
フォルト設定	カスタム設定
フォルト管理者とエージェントアクセサのバ フードのみを入力します。ほかのすべての ータはデフォルトバラメータを使用して設定	テータストアのタイプ、暗号化のプロパティ ー、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
れます。このオプションは、主に評価または 略の目的に使用するようにしてください。 フォルト 誤空穴の作成	ョンは、インストールの設定におけるもっとも
ルト設定の作成	新しい設定の作成

Copyright © 2010 ForgeRock AS, Philip Pedersens vei 1, 1366 Lysaker, Norway. All rights reserved. Licensed for use under the Common Development and Distribution License (CDDL), see http://www.forgerock.com/license/CDDLv1.0.html for details. This software is based on the OpenSSO/OpenAM open source project and the source includes the copyright works of other authors, granted for use under the CDDL. This distribution may include other materials developed by third parties. All Copyrights and Trademarks are property of their owners.





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	ĸ
カスタム設定オブション		
 → 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。パスワード員は 8 文字以上にする必要があります。この設定な 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【amAdmin】 *パスワード □□□□ *パスワードの確認 □□□□	5
	展る次へ	_

NRI 未来創発



OpenAM初期設定:Step3

- ▶サーバーURL : http://openam.nriossc.co.jp:8080
- ►Cookieドメイン : .nriossc.co.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 設定ツール		×
カスタム設定オブション				
 一分一段 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 祝要 	手順 2: サーバー設定 サーバーで使用する次の設定をす サーバーで使用する次の設定をす *サーバー URL *Cookie ドメイン *ブラットフォームロケール *設定ディレクトリ	翻訳します。 http://openam.nriossc.co.jp:8080 nriossc.co.jp en_US /root/openam	 ☑ 7 ⋈ ☑ 7 ⋈ 	∗必須フィールド
	展る次へ			取消し





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

コスタム設定オブション	OpenAM 設定ツール	3
 一般 サーバー設定 ⇒ 設定ストア ユーザーストア リイト設定 エージェント情報 概要 	手順3:設定データストア設定 環境ごまかの既存の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。 * 必須つ ●最初のインスタンス ● 既存の配備に追加しますか。 * 必須つ ●最初のインスタンス ● 既存の配備に追加しますか。 * 必須つ ●最初のインスタンス ● OpenAM ● Sun Java System Directory Server * 必須つ ●家定ズトアの評組 ● OpenAM ● Sun Java System Directory Server * 必須つ * ホスト名 ● ocalhost * ボート ● S0389 * 私dmin Port 4444 * JMX Port 1689 * 暗号化鍵 ● 定体60WAE2/htWSm/gBbXEXcW/MkgU * ルートサフィックス dc=opensso.dc=java.dc=net	の既存 <i>0</i>
	联 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 X
カスタム設定オブション	
1. 一般	手順 4: ユーザーデータストア設定 🌻
2. サーバー設定	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
3. 設定ストア	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。
→ ユーザーストア	◎ OpenAM のユーザーデータストア
5. サイト設定	◎ その他のユーザーデータストア *必須フィールド
6. エージェント情報	フーザーストアの詳細
7. 概要	
	◎ 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。
	UpenAm ユーリーナーダスドアは、本体的球鬼ではリホードでれません。
	K, o Min



NRI

未来創発

Dream up the future

● OpenAM初期設定:Step6 「いいえ」を選択して次へ

	OpenAM 設定ツール	×
カスタム設定オブション		
 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 	F.照 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パランサの背後に配価されますか? ○ しい え ○ しい え ○ しい え ○ しい え ・ 必須フィールド ・ セイト設定の う 4 ・ セイト 、 な 「 たの 、 新しい サイト 設定 、 な た た 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、 、	
	Rる 次へ	取消し

30



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	×
カスタム設定オブション		
 1. 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 * エージェント情報 7. 概要 	手順 6: デフォルトのボ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ブロパティーを取得するために OpenAM ポリシーエージェントで使用され *必須フィールド ボ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 *パスワードの確認	ます。
	展る二次へ	取消し

NRI 未来創発 Dream up the future



● OpenAM初期設定: Step8 ▶設定内容を確認して「設定の作成」

	OpenAM 設定ツール	×
カスタム設定オブション		
 1. 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 → 概要 	 設定ツールの概要と詳細 下の設定を確認してください。正しくない値がある場合は、設定を行う前に、戻ってその設定を変更できます。 読定ノナの課題編集 SSLが有効 いいえ ホスト名 localhost 待機ポート localhost 待機ポート co-alpostade=net ユーザー名 cn=Directory Manager ディレクトリ名 /root/openam ユーザーストアの詳細編集 設定ストア設定の使用 サイト設定の評編編集 このインスタンスは、ロードバランサの背後には設定されません。 	
	展る 設定の作成	取消し

NRI 未来創発 Dream up the future.



Dream up the future

● OpenAM初期設定:Step9 ▶設定が実行されます



34



OpenAMにログイン

▶<u>http://openam.nriossc.co.jp:8080/openam</u> にアクセスし、amadmin ユーザーでログインします

Open AM O	OpenAM へ ユーザー名: パスワード:	・のサインイン amadmin
Copyright © 2010 ForgeRock AS, Philip Pedersen reserved. Licensed for use under the Common Dev http://www.forgerock.com/license/CDDLv1.0.html f OpenSSO/OpenAM open source project and the s authors, granted for use under the CDL. This dist by third parties. All Copyrights and Trademarks are	s vei 1, 1368 Lysaker, Norws velopment and Distribution or details. This software is b ource includes the copyrigh ribution may include property of their owners.	ay. All rights License (CDDL), see based on the ht works of other materials developed



35



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

amAdmin	サーバー: openamn	riossc.co.jp			-		H
通タスク	アクセス制御	連携	Web サービス	設定	セッション		
SAMLv2 これらの5 とサービス ホスト・ リモー リモー Fedlet ³	・プロバイダを作成 フークフローを使用して、 ブロバイダを作成しまっ アイデンティティープロバ サービスプロバイダの作り トサービスプロバイダを強 トサービスプロバイダを強 を作成	、SAMLv2 連 す。 イダの作成 成 バイダを登録 S録	携のホストまたはリモ	ートのアイデ	ンティティー 1 1 1	Salesforce CRM の設定 OpenAM と Salesforce CRM を統合して、シングルサインオン環境を作成します。最初に、 SAMLv2 ホストアイデンティティーブロバイダとトラストサークルを設定する必要がありま す。 Salesforce CRM の設定 i 連携の接続性をテスト この自動化されたテストを使用して、連携の接続が成功するかどうかを判断し、どこに問題 があるかを確認します。 連携の接続性をテスト	
Fedlet をf イダと、連 初に、ホス Fedlet Google OpenAM ます。最新 す。	乍成して、OpenAM のご 携リリューションのない トアイデンティティープ を作成 Apps の設定 E Google Apps Web ア DIC、ホストアイデンティ	のインスタン リモートサー ロバイダを設 プリケーショ (ティープロバ	スでホストされている7 ビスブロバイダ間で、う 定する必要があります ンを統合して、シングル イダとトラストサークル	アイデンティテ 連携を有効して 「。 ノサインオン様 ノを設定する。	プロバ します。最	<mark>製品マニュアルを取得</mark> Launch the OpenAM product documentation page. 製品マニュアルを取得	I







Section3 連携先システムとのSSO



連携先システムとのSSO



Dream up the future





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_CHARSET = Shift_JIS,utf=8;q=0.7,*;q=0.3 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 --------------------------



38-



● 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)

<u>http://www.oracle.com/technetwork/java/javase/downloads/jre7</u> <u>-downloads-1880261.html</u>

ORACLE	Welcome 教 Account Si	gn Out Help Sele	ct Country/Region 👻 Communities 👻 I am a 😒	I want to Search			
PRODUCTS AND SERVICES	SOLUTIONS DOWNLOADS STO	RE SUPPOR	T TRAINING PARTNERS ABOUT	Oracle Technology Network			
Oracle Technology Network >	Java > Java SE > Downloads						
Java SE	Overview Downloads Docum	entation Con	munity Technologies Training	Java SDKs and Tools			
Java EE				🛃 Java SE			
Java ME	Java SE Runtime Env	ironment 7	Downloads	星 Java EE and Glassfish			
Java SE Support	TM I TM			差 Java ME			
Java SE Advanced & Suite	Lava programs, but not develop the	ns, or do you wa m. download th	nt to develop Java programs? If you want to rur a Java Runtime Environment or IRE TM	1 <u> </u>			
Java Embedded				差 Java Card			
JavaFX	JDK includes the JRE, so you do n	If you want to develop applications for Java, download the Java Development Kit, or JDK TM . The					
Java DB				Java Resources			
Web Tier				New to Java?			
Java Card	Java SE Runtime Environm	nent 7u21 nary Code Licer	se Agreement for Java SE to download this	APIs			
Java TV		softw	are.	👱 Code Samples & Apps			
New to Java	Accept License Agreement	Accept License Agreement Decline License Agreement					
Community				Documentation			
Java Magazine				Java.com			
Java Advanced	Product / File Description	File Size	Download	 <u> </u>			
	Linux x86	35.77 MB		Student Developers			
	Linux x86	46 MB	ire-7u21-linux-i586 tar oz	. Tutoriala			
	Linux x64	36.3 MB					
	Linux x64	44.76 MB	🛓 jre-7u21-linux-x64.tar.gz	NEW			
	Mac OS X x64	50.45 MB	jre-7u21-macosx-x64.dmg				
	Mac OS X x64	46.76 MB	差 jre-7u21-macosx-x64.tar.gz	dVd Catit agu			
	Solaris x86	45.56 MB	보 jre-7u21-solaris-i586.tar.gz	magazine Get It NOW			
	Colorio v64	44.06 MD	in 7004 selecte of the se	TO 12 21 22			





●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-7u21-linux-i586.gz
```

```
# tar zxvf jre-7u21-linux-i586.gz
# ls -l
jre1.7.0_21
```



●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_21←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 Id-linux.so.2
# java -version
java version "1.7.0_21"
Java (TM) SE Runtime Environment (build 1.7.0_21-b11)
```

Java HotSpot (TM) Client VM (build 23.21-b01, mixed mode)





ネットワーク設定

▶SSOサーバの/etc/hostsファイルに連携先サーバを追記する

172.105.126.67 openam-traning-app.nriossc.co.jp

▶連携先サーバの/etc/hostsファイルにSSOサーバを追記する

192.175.204.101 openam.nriossc.co.jp



連携先システムの構築

43



ポリシーエージェントをダウンロード

Forge Rock Com		eloper Comm	unity	
OpenAM OpenDJ OpenID	DM OpenICF OpenIG Humanoit - 2012	≢9月29日		
Community • The Community • Dev Principles • Dev Process • Get involved • FAQ • Enterprise License FAQ	Enterprise	OpenAN Authenticate - Authorise - Feder Release Downloads Archive of	ate community releases	
Projects OpenAM • Home	OpenAM Nightly Bu	ilds		
Security advisoryWiki	Release	Built from	Notes	Build Date
Bugster Source Builds Archives Enternrise Downloads	[Nightly Build][SHA][WAR][TOOLS]	trunk	Latest nightly build	20130523
• Enterprise Downloads OpenDJ • Home • Wiki	Web Policy Agents	Operating System Type	32/64 bits Build Date	
 Bugster Source Builds Archives Enterprise Downloads 	Apache 2.2	Linux	64 bits 💌 20130523	Download SHA
OpenIDM Home 	Java EE Policy Agents			
WIKI Bugster Source	Container	Version	Policy Agent version	Build Date
 Builds Archives Enterprise Downloads 	Glassfish [SHA] Web Logic [SHA]	2.x & 3.x v10	3.1.0-Xpress 3.1.0-Xpress	20130522 20130522
OpenICF	JBoss [SHA] Jothy [SHA]	4.2 & 5.x	3.1.0-Xpress	20130522





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

Is -I
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

44

/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 [デフォルトポリシーエージェントのパスワード] > 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]: /opt/OpenStandia/apache-2.2/conf OpenAM server URL: http://openam.nriossc.co.jp:8080/openam Agent URL: http://openam-traning-app.nriossc.co.jp:80 Enter the Agent Profile name: openam-traning 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



46



● エージェントプロファイルの作成

▶<u>http://openam.nriossc.co.jp:8080/openam</u> から0penAMにログイン

OpenAM O	OpenAM へ ューザー名:	へのサインイン amadmin
	パスワード:	
Copyright © 2010 ForgeRock AS, Philip Pedersen reserved. Licensed for use under the Common De http://www.forgerock.com/license/CDDLv1.0.html f OpenSSO/OpenAM open source project and the authors, granted for use under the CDDL. This dis by third parties. All Copyrights and Trademarks and	s vei 1, 1386 Lysaker, Norw velopment and Distribution or details. This software is b source includes the copyrig! ribution may include other e property of their owners.	way. All rights n License (CDDL), see based on the ght works of other er materials developed





Dream up the future

▶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

ユーザー: amAdmin サーバー: openam <i>u</i> rio OpenAM	pssc.co.jp										
共通タスク アクセス制御 レルムは、OpenAM が設定情報の整理に使用 配備時に作成されます。最上位のレルムは、	連携 Web サ ユーザー: amAdmin サー Open AM	ービス リバー: openaminrios	設定 セ: sccojp	ッション]						
レルム * 検索 レルム (1 項目)	 一般 認証 /(最上位のレルム) (最上位のレルム) 	サービス - ブロバティー	データストア ューザー: amAdmir <mark>Open AM</mark>	権限 n サーバー:	ポリシー openam <i>i</i> nriossci	対象 co.jp	エージュ			-	
新規 ぎ 目 /(最上位のレルム)	レルム属性 レルムの状態: @ア の別 1 E	'クティブ Fアクティブ nable or Disable this r	 →般 Web J2 	2표 サ EE Web	ービス ====================================	データストア イダ Web	権限 サービスクライ	ポリシー アント STS	対象 クライアント	エージェント 22 エージェント	エージェント認証
	レルムまたは DNS の 現在の値 ー)エイリアス pensso penamnriossc.co.jp	Web Web エージェントは	/ 、Apache Web) Server †⊃ Micr	osoft IIS などの	Web サーバー	-を保護します。			
			 新規< 新規 7.0 8.0 エンティティーが 	0 エージェご 涂 ありません。	∠F)	<u>ן</u> אַר	ジトリの場所				
1											IN ≤I _{未来創発}

48



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

ユーザー: amAdmin サーバ OpenAM	-: openamnriossc.co.jp
新しいエージェント	
* 名前:	openam-traning
*パスワード:	100000
*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ー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、Open AM サーバーです。
*サーバー URL:	http://openam.nriossc.co.jp:8080/openam
	プロトコル://ホスト:ボート/deploymentUri (たとえば、http://opensso.sample.com:58080/opensso)
*エージェント URL:	http://openam-traning-app.nriossc.co.jp:80
	プロトコル://ホスト:ボート (たとえば、http://agent1.sample.com:1234)



49



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

		_	_	_	_	_	_	_
一般	認証	サービス	データストア	権限	ポリシー	対象	エージェント	
Web	J2EE	Web サービスブ	ロバイダ Web	サービスクライア	ント STS :	クライアント	2.2 エージェント	エージェント認証
* 検索 エージェント (1 エージェント)								
エージェン	パ (1 エー	検索 ジェント)	_	_	_	_	_	_
エージェン 新規	<mark>小(1 エー</mark> 削除	検索 ジェント) □+©	-	-	-	-		-



50



■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 オーラームポリシーの認証 (SSO)のみを実施し、承認を実施しません。(プロパティー名: 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。(プロパティー名: comisunidentityagents.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。(プロパティー名: 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。(プロパティー名: comisunidentityagents.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:	10000000 エージェントのデバッグファイルサイズ (バイト単位)。(プロパティー名: comisun identity agents configidebug file size) ホットスワップ: 有効



連携確認

51



NRI

Dream up the future



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

	OpenAM 个	のサインイン
OpenAIM	ユーザー名: パスワード:	amadmin
Convright @ 2010 ForgeRock AS, Phillip Pedersen	s vei 1. 1388 Lysaker. Nonva	ログイン w. All rights
reserved. Licensed for use under the Common Der http://www.forgerook.com/license/CDDLv1.0.html f OpenSSO/OpenAM open source project and the s authors, granted for use under the CDDL. This dist by third parties. All Copyrights and Trademarks are	velopment and Distribution I or details. This software is b ource includes the copyrigh ribution may include other n a property of their owners.	License (CDDL), see ased on the t works of other naterials developed



連携確認

52





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





Dream up the futur

構築したシステムは、以下のような動作をしています



54



●HTTPへッダにユーザ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

ユーザー: amAdmin サーバー: openam <i>n</i> riossc.co.jp OpenAM	ユーザー: am.Admin - サーバー: openam.nriossc.co.jp	
共通タスク アクセス制御 連携 レルムは、OpenAM が設定情報の整理に使用する単配備時に作成されます。最上位のレルムは、OpenAM レルム * 検索 レルム(1 項目) 新規 削除 図 目 フルスロ /(最上位のレルム)	・皮 U リービス データストア 確果 ポリシー 対集 エージェント パ像上位のレルム) ・	
	Copenam-trains ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	



55



● 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





56



OK]

OK

●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: httpd を起動中:



57



Dream up the future

ー般ユーザの確認

▶アクセス制御>(最上位のレルム)>対象と遷移

▶今回はdemoユーザを使うので、demoをクリックしてパスワードを編集

ユーザー: amAdmin サーバー: openamoriossc.co OpenAM	ыjp						
共通タスク アクセス制御 連邦	ユーザー: amAdm OpenAM	in サーバー∶open≀	amnriossc.co.jp		-		
レルムは、OpenAM が設定情報の整理に使用する 配備時に作成されます。最上位のレルムは、OpenA	一般	認証 サービ	スデータストア	権限 ポリシー	対象 エージェ	ント	
レルム * 検索	ユーザー	グループ	ユーザー:amAdmin サー	・パー: openamnriossc.co.jp		_	
レルム (1 項目) 新規 「削除	7(最上位のレルル ユーザー	~		_	_	_	
図 ほ レルエロ / (最上位のレルム)	* ユーザー (3	<u>検索</u> ユーザー)	一般 サービス	グループ			
	新規 削 図 目 名前 amAdn	nin	ユーザー「demo」の	の編集		保	字 リセット 対象 へ戻る * 必須入力フィールド
	demo	mous	名: * 姓:	demo			
			* フルネーム: バスワード:	demo 編集			
			電子メールアドレス.				
		L	電話番号:				NXI _{**}

58



一般ユーザのパスワード設定 ▶新しいパスワード(demodemo)を設定して「了解」をクリック ▶その後ログアウト

ユーザー: amAdmin サーバー: openamnriosso OpenAM	cojp
demo のパスワードを変更	7解 リセット 閉じる * 必須入力フィールド
古いバスワードを入力します。	
* 古いバスワード:	
新しいバスワードを入力し、再入力します。	
*新しいパスワード:	
* パスワードの再入力:	



59





▶<u>http://openam-traning-app.nriossc.co.jp/app01</u>

▶demoユーザ(demo / demodemo)でログイン

OpenAM	OpenAM 个	のサインイン	
	ユーザー名: パスワード:	demo	
Copyright @ 2010 ForgeRook AS, Philip Pedersen	s vei 1, 1366 Lysaker, Nonwa	、All rights	
reserved. Licensed for use under the Common Der http://www.forgerock.com/license/CDDL/1.0.html f OpenSSO/OpenAM open source project and the s authors, granted for use under the CDDL. This dist by third parties. All Copyrights and Trademarks are	relopment and Distribution L or details. This software is be ource includes the copyright ribution may include other n property of their owners.	.icense (CDDL), see sed on the : works of other naterials developed	



60



●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

▶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





Dream up the futur

構築したシステムは、以下のような動作をしています







Section4

62









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!







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。

