

# OpenAM 技術 Tips

### Vol.3

## Window デスクトップ SSO の実現手順

執筆者: 和田 広之(株式会社野村総合研究所),

田村 広平(フリーランス)

監修: OpenAM コンソーシアム

当技術 Tips コンテンツは、OpenAM コンソーシアム監修のもと、OpenAM コンソーシアム開発ワーキン ググループに属する各企業の担当者により、執筆、編集されたものであり、各記事の著作権は執筆者に 帰属いたします。

また、当記事のライセンスは、Creative Commons 4.0 の BY-NC-SA (表示、非営利、継承) とし、執筆 者のクレジット(氏名、作品タイトル)を表示し、かつ非営利目的に限り、また改変を行った際には元の記 事と同じ組み合わせの CC ライセンスで公開することを主な条件に、改変したり再配布したりすることが できるものとします。



### 目次

1.	はじめに	3
2.	目的	4
З.	推奨環境	5
4.	事前準備	6
5.	名前解決の設定	7
6.	ファイアウォールの設定	8
7.	OpenAM 連携用ユーザーと一般ユーザーの作成	9
8.	Kerberos 認証用の keytab ファイルの生成	
9.	「データストア」の設定(Active Directory 連携)	
10.	「認証連鎖」の設定(Windows デスクトップ SSO 認証の設定)	
11.	クライアント PC (Windows)の設定	
12.	動作確認	
13.	トラブルシューティングの方法	
14.	付録1 : Active Directory のインストールと設定	
15.	付録 2:DNS サーバーの設定	
16.	付録3:FirefoxとChromeの設定	
17.	参考資料	



#### 1. はじめに

OpenAM は、Active Directory ドメインにログインしているユーザーを、OpenAM と連携する全てのアプリケー ションに、再ログイン無しでシングルサインオンする仕組みを提供しています。この仕組みを「Windows デス クトップ SSO」と言います。

Windows デスクトップ SSO は、OpenAM の認証モジュールの1つであり、「統合 Windows 認証 (Kerberos 認証)」の仕組みを利用しています。Windows デスクトップ SSO の動作原理(シーケンス)は、以下のようになります。



まず、ユーザーは Windows に Active Directory のドメインを指定して、ログインします(①)。ログイン時に 入力したユーザーID とパスワードが正しいと、Active Directory サーバーは TGT (Ticket Granting Ticket: チケット保証チケット)といわれるチケットを発行します(②)。ユーザーは、利用したいサービスがある場合、 このチケットを再度 Active Directory サーバーに提示して(③)、ST(サービスチケット)といわれるチケット を取得します(④)。ST は、利用したいサービス(OpenAM)へのアクセス許可を証明するチケットで、ユーザー はこれを OpenAM に提示する(⑤)ことで OpenAM が連携するアプリケーションへシングルサインオンできるよ うになります(⑥)。 2. 目的

本構築手順を実施することで、Active Directory ドメインに参加する Windows ユーザーであれば、再ログインを要求されることなく、OpenAM にログイン可能な環境を構築することができます。

OpenAM I



今回はこのような OpenAM と Active Directory のみの構成ですが、さらに OpenAM と連携するアプリケーショ ンを追加すれば、以下のように Windows 端末にログインするだけで、社内アプリケーションや Google Apps な どのクラウドサービスにもシングルサインオンができるようになります。





#### 3. 推奨環境

OpenAM をインストールするサーバー環境の推奨環境は以下の通りです。

- ・サーバーOS:Linux、Windows、UNIX
- ・メモリ:2GB 以上 (JVM ヒープサイズ)
- •JDK:1.6以上
- ・アプリケーションコンテナ (例. Apache Tomcat、JBoss、…etc.)

詳細についてはForgeRock 社サイト(OpenAM Release Notes)をご参照下さい。

本構築手順では以下環境を前提としています。

OpenAM サーバー

- ・サーバーOS: CentOS 6.5
- ・メモリ:2GB
- JDK : OpenJDK 1.7.0\_79
- ・アプリケーションコンテナ: Apache Tomcat 6.0.24
- OpenAM : OpenAM-12. 0. 0. war

🔔 ForgeRock 社でビルドされた OpenAM 12.0.0. war を本番環境で利用する場合は、ForgeRock 社のサブスク リプションが必要です。

Active Directory サーバー

- ・サーバーOS: Windows Server 2012 R2 Standard (評価版)
- ・メモリ:2GB



#### 4. 事前準備

本手順書では、以下の OpenAM サーバーが既にインストールされているものと仮定しています。

項目	値
URI	http://sso1.example.com:8080/openam

インストール手順に関しては、技術 Tips Vol.1「OpenAM インストール手順」を参照下さい。

http://www.openam.jp/category/member/techtips

また、以下の Active Directory サーバーが既にインストールされているものと仮定しています。

項目	值
ホスト名	ad.example.local
LDAP ポート	389
LDAP 組織 DN	cn=Users, dc=example, dc=local
LDAP バインド DN	cn=administrator, cn=Users, dc=example, dc=local

インストール手順に関しては、「14. 付録1: Active Directory のインストールと設定」を参照下さい。



#### 5. 名前解決の設定

各 Windows クライアントから OpenAM サーバーの名前解決と、OpenAM - Active Directory 間の相互の名前解 決ができるように DNS サーバーや hosts ファイルを設定する必要があります。

Windows ServerのDNSサービスによりこれを実施する場合は、「15. 付録2:DNSサーバーの設定」を参照 して下さい。

🤣 クライアントが数台しかない場合であれば、hosts ファイルでの運用も可能です。



#### 6. ファイアウォールの設定

OpenAM との通信のためには、88 番ポート(TCP/UDP)を開放しておかなければなりません。また、その他にも Active Directory を利用するにあたって、いくつかの TCP/UDP ポートを解放する必要があります。

起動しているサービスが必要とするポートの解放が自動的に行われるように、Windows ファイアウォールの自動設定を有効化して下さい(デフォルトは有効)。自動設定を有効化できない場合は、手動で見直しが必要です。

🤣 テスト目的であれば、全てのポートを解放しても構いません。

#### 7. OpenAM 連携用ユーザーと一般ユーザーの作成

OpenAM から Kerberos 認証を行うための、ユーザーを作成します。「管理ツール」 > 「Active Directory ユ ーザーとコンピューター」をクリックします。

🔁 l 💽 🔢 = l	ショートカット ツール	管理ツ-	-ル	_	
ファイル ホーム 共有	表示    管理				~ O
<د 🗟 💿 🗉 🖒 🕲	トロール パネル 🕨 システムとセキュリティ 🕨 管理ツール		✓ ℃ 管理ツ	ールの検索	م
☆ お気に入り	名前	更新日時	種類	サイズ	^
🍡 ダウンロード	light Terminal Services	2013/08/23 0:39	ファイル フォルダー		
📰 デスクトップ	📷 Active Directory サイトとサービス	2013/08/22 15:55	ショートカット	2 KB	
🗐 最近表示した場所	🛃 Active Directory ドメインと信頼関係	2013/08/22 15:55	ショートカット	2 KB	
	🛃 Active Directory ユーザーとコンピューター	2013/08/22 15:55	ショートカット	2 KB	
PC	Active Directory 管理センター	2013/08/22 8:50	ショートカット	2 KB	
🛺 ダウンロード	📝 ADSI エディター	2013/08/22 15:55	ショートカット	2 KB	
隆 デスクトップ	式 DNS	2013/08/22 15:55	ショートカット	2 KB	=
אראד+ 📗	🔝 iSCSI イニシェーター	2013/08/22 15:57	ショートカット	2 KB	
📔 ピクチャ	📷 ODBC データ ソース (32 ビット)	2013/08/22 8:56	ショートカット	2 KB	
🍓 ビデオ	📷 ODBC データ ソース (64 ビット)	2013/08/22 15:59	ショートカット	2 KB	
🜗 ミュージック	🛃 Windows PowerShell (x86)	2013/08/23 0:37	ショートカット	3 KB	
🚢 ローカル ディスク (C:)	🗃 Windows PowerShell ISE (x86)	2013/08/22 15:55	ショートカット	2 KB	
🎽 DVD ドライブ (D:) IF	🗃 Windows PowerShell ISE	2013/08/22 15:55	ショートカット	2 KB	
	😿 Windows PowerShell 用の Active Dire	2013/08/22 15:55	ショートカット	2 KB	
📬 ネットワーク	🖄 Windows Server バックアップ	2013/08/22 15:53	ショートカット	2 KB	
	<b>減</b> Windows メモリ診断	2013/08/22 15:52	ショートカット	2 KB	
	🔝 イベント ビューアー	2013/08/22 15:55	ショートカット	2 KB	
	🛃 グループ ポリシーの管理	2013/08/22 15:56	ショートカット	2 KB	
	🛃 コンピューターの管理	2013/08/22 15:54	ショートカット	2 KB	
	🔊 コンポーネント サービス	2013/08/22 15:57	ショートカット	2 KB	
	🔁 サーバー マネージャー	2013/08/22 15:55	ショートカット	2 KB	~
31 個の項目 1 個の項目を	選択 1.13 KB	нр. Си			



2	Active Dire	ectory 1-	ザーとコンピューター	_ 🗆 X	
ファイル(F) 操作(A) 表示(V) ヘル	,プ(H)				
🗢 🏟 🙍 📰 📋 🖾 🐼	🛛 🖬 🗏 💐	🗑 🔻 🖻 🤅	R		
📔 Active Directory ユーザーとコンと 💲	名前 種類	Į.	説明		
▶ 🔤 保存されたクエリ 📔 Builtin builtinE			omain Default container for		
り 制御の委任(E)			Default container for		
検索(I)		-	Default container for		
ドメインの変更(D)			Default container for		
ドメイン コントローラーの変更(C) ドメインの機能レベルの昇格(A) 提供コスター(M)			- Default container for		
操作Fマスター(M)			10 1		
新T规作FDX(N)		<u>·</u> =>	12-9-		
すべてのタスク(K)	)	▶ 	格先		
表示(V)		▶ グル	,ープ		
最新の情報に更	新(F)	Ine	etOrgPerson		
一覧のエクスポー	۲(L)	ms	simaging-PSPs		
プロパティ(R)		細調	mlQ +1- 110/ス 最単位 (OU)		
へルプ(H)		プリ	ンター		
		-ב	-ザ- N		
4		共	ヨフォルダー		
新しいパノンエクトを作成します。					



まずは OpenAM 連携用ユーザーを作成します。ここでは、「openam」というユーザー名にしています。

姓(L):	openam
名(F):	า=ระพา
フル ネーム(A):	openam
ユーザー ログオン名	ζ(U):
openam	@example.local v
- #	ム (Windows 2000 より前)(W):
ユーリー ロクハノモ	



「ユーザーは次回ログオン時にパスワード変更が必要」のチェックは解除し、「パスワードを無期限にする」 にチェックをします。

新しいオブジェクト - ユーザー
修成先: example.local/
パスワード(P): パスワードの確認入力(C): ●●●●●●● □ ユーザーは次回ログオン時にパスワード変更が必要(M) □ ユーザーはパスワードを変更できない(S) ● パスワードを無期限にする(W) □ アカウントは無効(O)
< 戻る(B) 次へ(N) > キャンセル

「パスワードを無期限にする」をチェックしておくことで、パスワードの有効期限が過ぎてもデスクトップ SSOが失敗することが無くなります。



新しいオブジェクト - ユーザー	x
A 作成先: example.local/	
[完了]をクリックすると、次のオブジェクトが作成されます:	
フルネーム: openam ^	6
ユーザー ログオン名: openam@example.local	
パスワードを無期限にする	
	e,
< 戻る(B) 示了 キャンセル	



example. local ドメインに参加する一般ユーザーを作成します。example. local/Users で右クリックし、新規 ユーザーを作成します。

3	Active	Directory ユー	ザーとコンピューター	_ 🗆 X
ファイル(F) 操作(A) 表示(V)	√レプ(H)			
🗢 🏟 🖄 📰 🔏 📋 🗙 🛙	I Q 🔒 🛛 🖬	1 🕺 🐱 🛅 🎙	r 🧕 🖗	
<ul> <li>Active Directory ユーザーとコンと</li> <li>除存されたクエリ</li> <li>解存されたクエリ</li> <li>■ Builtin</li> <li>■ Computers</li> <li>■ Domain Controllers</li> <li>■ ForeignSecurityPrincip</li> <li>■ Managed Service Acco</li> <li>■ Use</li> <li>制御の委任(E).</li> <li>検索(I)</li> <li>新規作成(N)</li> <li>すべてのタスク(K)</li> <li>表示(V)</li> <li>最新の情報に更 一覧のエクスポー プロパティ(R)</li> </ul>	名前 Administra Allowed R Cert Publis Coneable Coneable Denied RO DnsAdmins DnsUpdate       	<ul> <li>種類&lt;</li> <li>説明</li> <li>rra ユーザー</li> <li>コンピューター/ドメインの管</li> <li>R セキュリティ グル このグループのメンバーは、</li> <li>iis セキュリティ グル このグループのメンバーはデ</li> <li>e セキュリティ グル このグループの、ドメイン コ</li> <li>RO セキュリティ グル このグループの、ドメイン コ</li> <li>マキュリティ グル このグループのメンバーは、</li> <li>ロドキュリティ グル このグループの水ンバーは、</li> <li>ロドキュリティ グル このグループの水ンバーは、</li> <li>ロドキュリティ グル このグループの、ドメイン コ</li> <li>マキュリティ グル レキュリティ グル</li> <li>ロドキュリティ グル ドメインの管理者</li> <li>・ セキュリティ グル ドメインの管理者</li> <li>・ セキュリティ グル ドメインのすべてのワークス</li> <li>ロンピューター</li> <li>連絡先</li> <li>グループ</li> <li>InetOrgPerson</li> <li>msDS-ResourcePropertyList</li> <li>msImaging-PSPs</li> </ul>	説明 コンピューター/ドメインの管 このグループのメンバーは、 このグループのメンバーはデ このグループのメンバーはデ このグループのメンバーは、 DNS 管理者グループ DHCP サーバーなどのほか ドメインの管理者 ドメインのすべてのワークス たいたのまたてのだいた SPs こイリアス	
へルプ(H)		プリンター		
< III >	& Schema A. & WinRMRe.	ユーザー 共有フォルダー	×	
新しいオブジェクトを作成します。				



姓(L):	test
名(F):	イニシャル
フル ネーム(A):	test
ユーザー ログオン名	,(U):
test	@example.local
ユーザー ログオン名	(Windows 2000 より前)(W):

ここでは、ユーザー名を「test」としています。



「ユーザーは次回ログオン時にパスワード変更が必要」のチェックは解除します。

新しいオブジェクト - ユーザー
A 作成先: example.local/Users
パスワード(P):       ●●●●●●●         パスワードの確認入力(C):       ●●●●●●●●         □ ユーザーは次回ログオン時にパスワード変更が必要(M)         □ ユーザーはパスワードを変更できない(S)         □ パスワードを無期限にする(W)         □ アカウントは無効(O)
< 戻る(B) 次へ(N) > キャンセル



新しいオブジェクト - ユーザー	x
Ar成先: example.local/Users	
[完了]をクリックすると、次のオブジェクトが作成されます:	
フルネーム: test	
ユーザー ログオン名: test@example.local	
~	•
< 戻る(B) 完了 キャンセル	



#### 8. Kerberos 認証用の keytab ファイルの生成

OpenAM の Windows デスクトップ SSO 認証では、Kerberos 認証用の keytab ファイルが必要になります。keytab ファイルは、Windows の ktpass コマンドにより生成します。Active Directory サーバーでコマンドプロンプ トを起動し、以下のコマンドを実行します。

> ktpass -out desktopsso. HTTP. keytab
 -princ HTTP/sso1. example. com@EXAMPLE. LOCAL
 -ptype KRB5\_NT\_PRINCIPAL
 -pass Password1
 -mapuser openam

各オプションについて説明します。

-out keytab ファイルのファイル名

出力される keytab ファイルのファイル名です。

- princ サービス主体

Kerberos 認証での「サービス主体」を指定します。

HTTP/"OpenAMの FQDN"@"Active Directoryのドメイン名の大文字"で設定します。

-ptype KRB5\_NT\_PRINCIPAL

固定値(KRB5\_NT\_PRINCIPAL)を指定します。

-pass OpenAM 連携用ユーザーのパスワード

OpenAM 連携用ユーザーのパスワードを指定します。

-mapuser OpenAM 連携用ユーザーの ID

OpenAM 連携用ユーザーの ID を指定します。



#### 実行結果は以下のようになります。

> ktpass -out desktopsso. HTTP. keytab -princ HTTP/sso1. example. com@EXAMPLE. LOCAL -ptype
KRB5\_NT\_PRINCIPAL -pass Password1 -mapuser openam
Targeting domain controller: WIN-DTOKQDBDE2J. example. local
Using legacy password setting method
Successfully mapped HTTP/sso1. example. com to openam.
Key created.
Output keytab to desktopsso. HTTP. keytab:
Keytab version: 0x502
keysize 79 HTTP/sso1. example. com@EXAMPLE. LOCAL ptype 1 (KRB5\_NT\_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength 16 (0x64f12cddaa88057e06a81b54e73b949b)

#### 🕢 エラーが出る場合は -Target AD のドメイン名 をオプションに追加して下さい。

出力された desktopsso. HTTP. keytab ファイルは、OpenAM サーバーの任意のディレクトリに転送しておきます。 ここでは、/home/tomcat/desktopsso. HTTP. keytab に配置したと仮定します。

▲ keytab ファイルは任意のパスに配置できますが、Tomcat の実行ユーザーが参照できるディレクトリでな ければなりません。



#### 9. 「データストア」の設定 (Active Directory 連携)

Active Directory を OpenAM のユーザーデータストアとして使用するための設定を行います。 OpenAM の管理コンソールに amadmin でログインして下さい。

0	OpenAM	- Login - M	ozilla F	irefox					-	o x
🕜 OpenAM - Login	× &									
Sso1.example.com	8080/openam/XUI/#	login/	✓ C <sup>i</sup>	् Invalid i	nitial he >	☆	Ê	+	⋒	≡
	FORGEROCK					\				
	OpenAM ^	のサイン	ソイン	,						
	ユーザー名:	amadmin								
	パスワード:	•••••								
	l	Remember	my userna	ame						
					Log in					
	Copyright ©	info@forg 2010-14 Forgel	<u>erock.com</u> Rock AS, a	ll rights reserved	d.					

「アクセス制御」タブをクリックします。

) OpenAM	*	· (+							
⊛ ssol.e	xample.com:808	0/openam	/task/Hom	e 💊	C Q Invalid initial hei → ☆ 6				
ジョン						ログアウ			
FOR	RGEROC	к							
連タスク	<u>アクセス</u> 制御	連携	設定	セッション					
	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~								
SAMLv2 プ	ロバイダを作成				Salesforce CRM の設定				
これらのワー	クフローを使用して、	SAMLv2 連携	りパンドまた		OpenAM と Salesforce CRM を統合して、シン	ノグルサインオ			
します。	)バイナンテイティーC	9-EXJ	コハインを作用	6	ン境現を作成します。最初に、SAMLVZ 小スト ティープロバイダとトラストサークルを設定す	アイテンティ る必要があり			
ホストアー	イデンティティープロバ-	ィダの作成	i		ます。				
ホストサー	-ビスプロバイダの作成		i		Salesforce CRM の設定	i			
リモートン	アイデンティティープロ/	「イダを登録	i						
UE-ht	+ービスプロバイダを発発	3	16		Configure Social Authentication				
2011	, cypuniyed.	ar.			task configures authentication through	third			
OAuth2 の	設定				parties such as Facebook, Google and Mi	icrosoft.			
このタスクは	レルムごとに OAuth2	を設定しま	す。レルム単位	Ω.	Configure Facebook Authentication	i			
に認可サーバ	(として動作することか	べできます。			Configure Google Authentication	(i)			
OAuth2 の	設定		i		Configure Microsoft Authentication	i			
Fodlot &	₩= R <sup>®</sup>				Configure Other Authentication	i			
Fedlet 东作	TFRA 成して OpenAM のこ	のインスタン	ノスでホストさ						
れているアイ	デンティティープロバ	「イダと、連	勢ソリューショ	1	連携の接続性をテスト				
ンのないりも	ートサービスプロバィ	「夕間で、連打	隽を有効にしま くどを記念する		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			
9。最初に、 必要がありま	·ホストアイテンティテ す。	イープロハ・	イタを設定する	)	かとつかを判断し、とこに問題かめるかを確認	します。			
Fedlet &	作成		i		王坊の技術社をアスト				
			100		製品マニュアルを取得				
Google Ap	ps の設定				OpenAM 製品マニュアルのページを起動します。				
Decedul La C	ioogle Apps Web アフ	パリケーショ	ンを統合して、		製品マニュアルを取得	i			
орепам с с						and the second se			



「/ (最上位のレルム)」のリンクをクリックします。

🥥 OpenAM - Mozilla Firefox _ 🗆 🗙
OpenAM × ⊕
♦ Sso1.example.com:8080/openam/task/Home?Hor < C
ログアウト
FORGEROCK
共通タスク アクセス制御 連携 設定 セッション
レルムは、OpenAM が設定情報の整理に使用する単位です。レルム内では、認証プロパティー、承認ポリシー、データストア、対象、その他のデータを定義で きます。最上位のレルムは、OpenAM の配備時に作成されます。最上位のレルムは、OpenAM インスタンスの root で OpenAM 設定データを含んでいます。 レルム * 検索 レルム(1 項目) 新規 削除
図 目     レルム名     場所     △



「データストア」をクリックします。

0	OpenAM	I - Mozilla Firefo	x		_ = ×
🔗 OpenAM	× &				
Ssol.example.com:	8080/openam/realm/RM	IRealm?R№ <b>~ C</b>	् Invalid initi	al he; → 🟠	<b>≜ ∔ ☆ ≡</b>
パージョン					ログアウト
	sol.example.com				
<b>FORGERC</b>	ОСК	_	_	_	_
一般 認証 サービ	ス <u>データストア</u>	権限 ポリシー	対象	エージェント	STS
( (量上位のレルム)					
(最上位のレルム) - プロ	パティー		6	存 リセット	アクセス制御 へ戻る
レルム属性					
レルムの状態: ④ アクティブ	_				
○ 非アクティ 1 このレルムを	フ ご有効または無効にします。				
レルムまたは DNS のエイリアン	z				
現在の値 sso1.examp	le.com _ 削除				
	~				
新しい値	追加				
し このレルムに関連付け	られた いい トスインのリスト。				
ssol.example.com:8080/one	enam/realm/RealmProp	ertiYklkcOB-AAN(	)ABIDdXIv7WF	50UHIv7mls7\	/ZpZXdxAH4AHna\$
ere restanding and the second of the	in and it contribution in the pro-	and the second			-p=::::::::::::::::::::::::::::::::::::



#### 「新規」ボタンをクリックします。

٩			Open	AM - Moz	illa Firefox				×
🕜 Oper	nAM	×	4						
🗲 🕲 ss	ol.exam	ple.com:8080	)/openam/realm/	RealmPro	pert <b>~ C</b>	Invalid i	nitial he > 🏠	ê <b>+</b>	⋒ ≡
バージョン		+ 1° 1 -							ログアウト
			xample.com						_
	JIEG	EROC	n	_	_	_	_	_	_
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	STS	_
/ (最上位の)									
(最上位の	レルム)	- データス	トア					アクセ	2ス制御 へ戻る
データス	トア (1	項目)	_	_	_	_	_		
新規	削除								
I → 日 名	前				▲ タイプ OpenD1				<u>م</u>
	bedded				openos				

任意の名前(本書では ActiveDirectory)を入力し、タイプは「Active Directory」を選択して、「次へ」ボタンをクリックします。

OpenAM - Mozil	lla Firefox	_ = ×
🔇 OpenAM 🗙 🕀		
Sso1.example.com:8080/openam/realm/IDRepo	✓ C Q Invalid initial hei → ☆ 自 ↓	▶ <b>⋒</b>
パージョン		ログアウト
ユーザー: amAdmin サーバー: sso1.example.com		
V FORGEROCK		
ステップ 1/2: データストアのタイプを選択 * 名前: ActiveDirectory ○ Active Directory アプリケーションモード (ADAM) ○ OpenAM スキーマを含んだ Sun Directory Server ○ OpenDJ ○ Tivoli Directory Server ○ データペースリボジトリ (アーリーアクセス) ○ 汎用 LDAPv3		■ 取消し 対策 入力フィールド



Active Directory をデータストアとして利用するための設定画面が表示されます。

OpenAM - Mozilla Firefox _ □ ×
OpenAM ★ 문
< 🕙 sso1.example.com:8080/openam/realm/IDRepoSelect 🗸 🖒 🔍 Invalid initial hei 🗲 🏠 🗎 🖶 🏠
バージョン ログアウト
ユーザー: amAdmin サーバー: ssol.example.com
S FORGEROCK
   ステップ 2/2: 新規データストア - Active Directory
* 必須入力フィールド
* 名前: ActiveDirectory
完了時にスキーマを読み込み: 🖌
現在の値 ad.example.local:389 削除
新しい値
形式: LDAP サーバーのホスト名:ポート   server_ID   site_ID
LDAP バインド DN: CN=Administrator,CN=Users,dc=openam,dc=for
サポートされる操作を実行できる適切なアクセス権を持つユーザーまたは管理者。
LDAP バインドパスワード (確認):
* LDAP 組織 DN: dc=openam,dc=forgerock,dc=org
LDAP SSL: □有効

OpenAM コンソーシアム

以下の設定を行います。

項目	値
LDAP サーバー	ad.example.local:389
	※デフォルトで設定されている値は削除して、上記値を追加し
	て下さい。
LDAP バインド DN	cn=administrator, cn=Users, dc=example, dc=local
LDAP バインドパスワード	[administrator のパスワード]
LDAP バインドパスワード(確認)	[administrator のパスワード]
LDAP 組織 DN	cn=Users,dc=example,dc=local
LDAPv3 プラグイン検索範囲	SCOPE_SUB
LDAP ユーザー検索属性	sAMAccountName
LDAP ピープルコンテナネーミング属性	(空にする)
LDAP ピープルコンテナ値	(空にする)
グループメンバーシップの属性名	memberOf
持続検索ベース DN	dc=example, dc=local



#### データストア「ActiveDirectory」を作成したら、デフォルトの embedded データストアは削除して下さい。

OpenAM - Mozilla Firefox								. <b></b>
🖉 🕼 OpenAM 🛛 🗙	4							
Ssol.example.com:8080	)/openam/realm/I	DRepoAdd	✓ C Q	Invalid	initial he >	☆ 🖻	∔ ก	
	vamolo com						C	コグアウト
	example.com							
FORGEROC	N	_	_	_	_	_	_	_
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	STS		
/ (景上位のレルム)								
(最上位のレルム) - データス	トア					7	7クヤス制御	へ戻る
(最上位のレルム) - リーノス	1-2	_	_	_	_	-		
新規 削除							_	
☑ 圖 名前			タイプ					<u> </u>
ActiveDirectory			Active Di	rectory				_
			openos					



対象タブをクリックし、Active Directory サーバー上のユーザーアカウントが表示されていることを確認します。

٢	OpenAM - Mozilla	Firefox	_ 0 ×					
🕼 O	penAM × 中							
	ssoriekample.com.sooo/openam/aathenaeaton/Aath							
バージョン	✓		ログアウト					
- 📣 F	FORGEROCK							
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	STS					
+	f- グループ							
/ (最上位	のレルム)							
	, , , , , , , , , , , , , , , , , , ,							
ש-ב	_	アクサ	セス制御 へ戻る					
*	検索							
7-#	デー (7 ユーザー)							
±_+8								
初况								
	名前	汎用 ID						
	Administrator	Administrator						
	amAdmin	amAdmin						
	anonymous	anonymous						
	demo	demo						
	Guest	Guest						
	krbtgt	krbtgt						
	test	test						



#### 10. 「認証連鎖」の設定(Windows デスクトップ SSO 認証の設定)

OpenAMの認証の方式を Windows デスクトップ SSO 認証に変更します。

「認証」タブをクリックして、認証画面を表示します。

0		OpenA	M - Mo	zilla Firefox	(			_ 🗆 ×
🚷 OpenAM	×	4						
🗲 🖉 🕲 sso1	.example.com	:8080/openam/au	thentica	tion, 🗸 C	🔾 Invalid i	initial he 🔶 🏠	≜ ∔	⋒ ≡
バージョン								ログアウト
ユーサー: amAdmin	サーハー: ssol.e	example.com						
FOR (	GEROC	K	_	_	_	_	_	_
-#2 2027	サービス	データストア	権限	ポリシー	対象	エージェント	STS	_
	\ <b></b>						704	ったり、ラフ
(最上位のレルム	() - JUN <del>,</del>	<b>イ</b> −				保存 リセット	- roe.	人利御 へ戻る
レルム属性								
レルムの状態: (	◉ アクティブ							
(	非アクティブ このレルムを有効?	または毎効にします。						
レルムまたは DNS 現在の値	SSO1.example.co		1					
370 LL 07 188	openam	H31K5A						
		~						
新しい値		追加						
(i) このレ	ルムに関連付けられた	DNS ドメインのリスト。						
sso1.example.com	n:8080/openan	n/realm/RealmPro	pertiE	FCUXRPRGsx	T0RZeE50	qa3pNekF3TkRRM	IU5ETXIOU	S4uKng\$



モジュールインスタンスのセクションにある「新規」ボタンをクリックします。

OpenAM - Mozilla	Firefox _ 🗆	x
🚷 OpenAM 🗙 문		
♦ ♦ @ sso1.example.com:8080/openam/realm/RealmPro	✓ C Q Invalid initial hei⇒ ☆ 自 ↓ 合	
コア		^
すべてのコア設定		
組織認証設定: ldapService ▼		
管理者認証設定: ldapService ▼		
ログイン成功時に返すデフォルトの URL		
現在の値 /openam/console / 削除		
		-
👔 ログイン成功後にこの URL ヘ転送します。		
モジュールインスタンス		
モジュールインスタンス (7 項目)		
新規 削除		
☑ 图 名前	▲ タイプ △	
НОТР	НОТР	
LDAP	LDAP	
	OATH	
SAE MSCAuthModulo	SAE	
	U10ACC#	Ŭ

「Windows デスクトップ SSO」を選択し、任意の名前(本書ではDesktopSSO)を付けて「了解」ボタンをクリ ックして下さい。

OpenAM - Mozilla Firefox		>	ĸ
🕼 OpenAM 🗙 🕀			
♦ 🛞 sso1.example.com:8080/openam/authentication/Auth 🗸 😋 🔍 Invalid initial he; →	☆ 自	+ ☆ =	
パージョン		ログアウト	1
ユーザー: amAdmin サーバー: ssol.example.com			
<b>W</b> FORGEROCK			
新規モジュールインスタンス		了解 取消し	
		必須入力フィールト	2
* 名前: DesktopSS0			
* タイプ: O Active Directory			
O Device Id (Match) O Device Id (Save)			
O HOTP			
○ HTTP 基本			
O JDBC			
O DATH			
OAuth 2.0			
OpenID Connect id_token bearer			
O RADIUS			
SAE			
Securit			
Windows NT			
● Windows デスクトップ SSO			
○ WSSAuth			
○ 法続 Cookie			
○ ○ 匿名			
○ 連携			



モジュールインスタンスの一覧から、作成された Windows デスクトップ SSO 認証モジュールを選択します。

	OpenAM - Mozilla Firefox	- ×			
🚯 OpenAM 🗙 🕂					
♦ ♦ ♦ sso1.example.com:8080/op	enam/realm/RealmPrc 🗸 😋 🔍 Invalid initial hei 🔶 🏠 📋 🖡 🏫	≡			
コア		^			
すべてのコア設定					
組織認証設定: ldapService ▼					
(1) ユーザーのデフォルト認証	連鎖。				
管理者認証設定: ldapService ▼					
[1] 管理者のデフォルトの認証	連鎖。				
ログイン成功時に返すデフォルトの URL					
現在の値 /openam/console 🔼	削除				
		=			
~					
新しい値	追加				
🪺 ログイン成功後にこの URL ヘ転送しま	👔 ログイン成功後にこの URL ヘ転送します。				
。					
* 元頃に戻る					
モジュールインスタンス					
モジュールインスタンス (8 項目)					
新規削除					
図 圓 名前	▲ タイプ				
DataStore	データストア				
DesktopSS0	Windows デスクトップ SSO				
Federation	連携				
НОТР	НОТР				
II I LDAP	LDAP	Ľ			



#### Windows デスクトップ SSO 認証モジュールに、以下の設定を行います。

0	OpenAM - Mozilla Firefox	_ 0 ×
🚷 OpenAM	× ₽	
Ssol.example.com	8080/openam/authentication/Auth 🗸 🕑 🔍 Invalid initial he; 🔶 🏠 自 🛛 🕂	⋒
バージョン		ログアウト
ユーザー: amAdmin サーバー: s		
W FORGERO	DCK	
Windows デスクトップ SS	() 保存 リセット 語	認証 へ戻る
レルム属性	*	
サービス主体:	HTTP/sso1.example.com@EXAMPLE.LOCAL	
	i) 認証時に使用される Kerberos 主体の名前	
Keytab ファイル名:	/home/tomcat/desktopsso.HTTP.keytab	
	▲ AD の keytab ファイルのパス	
Kerberos レルム:	EXAMPLE.LOCAL	
	認証に使用される Kerberos (Active Directory) のレルムの名前。	
Kerberos サーバー名:	ad.example.local	
は ノンカナ みれ みば ナ に ナ・	Kerberos (Active Directory) サーバーのホスト名/ IP アドレス。	
トメイン名を言む主体を返9:	□ 月辺	
認証レベル:		
BUT INT D	■ この認証モジュールで認証成功時に設定される認証レベルです。	
レルム内のユーザー検索:		
	ー 」 ユーザーがデータストアで構成されたユーザープロファイルと一致していることを検証します。	
	保存リセット	認証 へ戻る

項目	值
サービス主体	HTTP/sso1. example. com@EXAMPLE. LOCAL
Keytab ファイル名	/home/tomcat/desktopsso.HTTP.keytab
Kerberos レルム	EXAMPLE. LOCAL
Kerberos サーバー名	ad.example.local
ドメイン名を含む主体を返す	チェックなし
認証レベル	0
レルム内のユーザー検索	チェックなし

この例では、Keytab ファイル(desktopsso.HTTP.keytab)を/home/tomcat/に配置しています。

次に、Windows デスクトップ SSO 認証モジュールを含む認証連鎖を作成します。 認証連鎖のセクションにある「新規」ボタンをクリックして下さい。

٢	OpenAM - Mozilla Firefox _ d				×
5	🚷 Op	enAM × 守			
	÷) >	Ssol.example.com:8080/openam/au	thentication/E 🗸 C Invalid initial her > 🟠 🗈 🖡	⋒	≡
		👔 ログイン成功後にこの URL ヘ転送します。			^
	+ == (- ==	-			
~	光頭(こ戻	ବ			
Ŧ	ジュー	-ルインスタンス			
	エジー	ュールインスタンス (8 頂日)		_	. 17
	レノ - 新田			_	
	新規				
		名削 🔺		~	
	븝	DesktopSSU	Windows テスクトップ SSO		
	븝		建绣 HOTD		
	H	OATH	OATH		
		SAE	SAF		
		WSSAuthModule	WSSAuth		
		DataStore	データストア		
<u>。</u> 認		レルムに使用可能な認証モジュールのリスト る			
	A DARGE DR	<u> </u>			~


任意の名称(本書では desktopssochain)で認証連鎖を作成します。

・ OpenAM       ・ ●         ・ Ssol.example.com:8080/openam/authentication/Auth * C       ・ Invalid initial he: + ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●       ●
Solexample.com:8080/openam/authentication/Auth 、
パージョン ユーザー: amAdmin サーバー: ssol.example.com 新規認証連鎖 * 名前: desktopssochain
ユーザー: waAdmin サーバー: ssol.example.com <b>FORGEROCK</b> 新規認証連鎖 * 名前: desktopssochain
★ FORGEROCK 新規認証連鎖 * 名前: @esktopssochain
新規認証連鎖 * 述 <sub>知入力フィール</sub> ド
新規認証連鎖 * 公園入力フィールド
* 名前: desktopssochain
Han Deskrobszoruari



認証連鎖は以下のようなモジュール構成にします。

インスタンス	条件	オプション
DesktopSS0	十分	

<b>e</b> o	penAM - Mozilla Firefox			_ = ×	
🚷 OpenAM 🛛 🗙 🕂					
Sso1.example.com:8080/openam/a	uthentication/Auth 🛩 C	、Invalid initial he; →	☆ 自 ┨	- ⋒ ≡	
パージョン					
ユーザー: amAdmin サーバー: sso1.example.com					
V FORGEROCK	_	_	_	_	
desktonssochain - プロパティー		保友	11471116	認証 へ戻る	
			Jeji	BUAL YOR OF	
(1 項目)			_		
追加削除並べ替え					
	条件	オプション	1		
このテーブルには、この認証連鎖を構成する認証モジ:	ュールのリストを表示します。				
ログイン成功時に返す URL					
現在の値	削除				
新しい値	追加				
👔 ログイン成功後、次のURLに転送されます。					
ログイン失敗時に返す URL					
現在の値	削除			~	



この設定の場合、OpenAM は Windows デスクトップ SSO 認証が成功すれば、ログインを許可します。つまり、 Active Directory ドメインに参加している Windows にログインしているユーザーは、ログイン画面で ID とパ スワードを入力することなく、OpenAM にシングルサインオンできることになります。 最後に作成した認証連鎖を有効にします。「認証タブ」の「コア」セクションにある「組織認証設定」をデフ オルトの Idapservice から作成した認証連鎖(desktopssochain)に変更し、「保存」をクリックします。

OpenAM コンリーシアム

0		Open/	AM - Moz	zilla Firefox	(			_ o ×	ĸ
🚷 OpenAM	×	4-							
♦ Ssol.exa	mple.com:808	)/openam/authen	tication/#	Auth 🗸 🥑 🖸	🔍 Invalid	initial he 🔶 🏠	ê - 1	▶ ♠ ≡	:
バージョン								ログアウト	~
ユーザー: amAdmin									
FOR	GEROC	K	_	_	_	_	_		
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	STS		
/ (最上位のレルム)	)						7.0.14		Ξ
	ム) - 認証	10.014				保存リセット	100	〈制御 へ戻る	
◎ コア ◎ モジュールインス	◎ 認証: タンス	建頻							
コア									
すべてのコア設定	Ē								
組織認証設定:	desktopssochair	1 -							
截烟去砌红砂中。	ユーザーのデフ	ォルト認証連鎖。							
<b>官</b> 建自路証設定:	ldapservice 〔〕管理者のデフォ	 ルトの認証連鎖。							
ログイン成功時に	返すデフォルトの	URL							
現在の値	/openam/console	_ 削除							
		~							
新しい値		追加							
👔 อวีส	ン成功後にこの URL /	へ転送します。							~

以上で、OpenAMの設定は終了です。完了したら、アプリケーションコンテナを再起動して下さい。



🦺 「組織認証設定」の認証を変更したため、OpenAM サーバーヘアクセスすると Windows 統合認証となり OpenAM のログイン画面が表示されなくなります。

OpenAM 管理コンソールを操作するために amAdmin でログインする場合は、OpenAM ヘアクセスする URL のクエ リストリングに service=adminconsoleservice を付けてアクセスするようにして下さい 。

http://sso1.example.com:8080/openam/UI/Login?service=adminconsoleservice



通常は、Active Directory のグループポリシーのブラウザの設定テンプレートにクライアント PC の共通設定 を行いますが、本手順書では動作検証用のクライアント PC の設定を変更します。Active Directory の設定を 変更している場合は、このセクションを読み飛ばして下さい。

OpenAM コンソーシアム

ドメインに参加していない端末は、DNS 設定とドメインへの参加設定が必要です。TCP/IP の設定で、Active Directory サーバーの IP アドレスを DNS サーバーとして指定します。

インターネット プロトコル バージョン 4 (TCP/IPv4)のプロパティ 🛛 🤗 🔀				
全般(代替の構成)				
ネットワークでこの機能がサポートされている場合 きます。サポートされていない場合は、ネットワー てください。	は、IP 設定を自動的に取得することがで ク管理者に適切な IP 設定を問い合わせ			
<ul> <li>IP アドレスを自動的に取得する(Q)</li> </ul>				
○ 次の IP アドレスを使う( <u>S</u> ):				
IP アドレス(D:				
サブネット マスク(山):				
デフォルト・ゲートウェイ( <u>D</u> ):				
<ul> <li>DNS サーバーのアドレスを自動的に取得</li> </ul>	!する( <u>B</u> )			
○ 次の DNS サーバーのアドレスを使う(E):				
優先 DNS サーバー( <u>P</u> ):				
代替 DNS サーバー( <u>A</u> ):	· · ·			
□ 終了時(ご設定を検証する( <u>し</u> )				
	OK キャンセル			

次にドメイン参加の設定を行います。コンピュータ名変更のダイアログより、ドメインを入力して「OK」ボタ ンをクリックして下さい。

OpenAM コンソーシアム

システムのプロパティ	×
コンピューター名/ドメイン名の変更	
このコンピューターの名前とメンバーシップを変更できます。変更により、ネット ワークリソースへのアクセスに影響する場合があります。 <u>詳細情報</u>	使われます。
コンピューター名( <u>C</u> ): CLIENT] フル コンピューター名: CLIENT.example.local	ユーター"
詳細( <u>M</u> ) 「所属するグループ ● ドメイン( <u>D</u> ): example.local ● ワークグループ( <u>W</u> ):	-ウ id(N) E(C)
OK キャンセル	
OK キャンセル	適用(A)

以下の認証ダイアログが表示されるので、Active Directory に登録したユーザーID とパスワードを入力します。



最後にブラウザの設定を変更します。通常は、Active Directoryのグループポリシーのブラウザの設定テン プレートにクライアント PCの共通設定を行いますが、本手順書では動作検証用のクライアント PCの設定を変 更します。Active Directoryの設定を変更している場合は、このセクションを読み飛ばして下さい。

OpenAM コンソーシアム

以下は Internet Explorer 11 の場合ですが、Microsoft Edge でも同様です。それ以外のブラウザの設定については、「16. 付録3: Firefox と Chrome の設定」を参照して下さい。

インターネットオプションの「セキュリティ」タブをクリックし、「ローカル イントラネット」を選択して下 さい。

インターネット オブション <b>?</b> 🗙					
全般 セキュリティ フライバシー コンテンツ 接続 フログラム 詳細設定					
セキュリティ設定を表示または変更するソーンを選択してください。					
インターネット ローカル イントラネッ 信頼済みサイト 制限付きサイト ト					
ローカル イントラネット サイト/C2					
イントラネットにあるすべての Web サイトには、このソーン					
このジーンのセキュリティのレベル(L)					
ክスタム					
カスタム設定 - 設定を変更するには「レベルのカフタマイプ」ボタンをクロックします。					
- 推奨設定を使用するには、[肌定のレベル]ボタンをクリックします。					
□ 保護モードを有効にする (Internet Explorer の再起動が必要)(P)					
すべてのソーンを既定のレベルにリセットする(R)					
して、 キャンセル 道用(日)					

「サイト」ボタンをクリックして開いたダイアログの「詳細設定」ボタンをクリックすると、以下のようなダ イアログが表示されます。



ここに OpenAM サーバーの URL を追加して下さい。

ローカル イントラネット	×
このゾーンの Web サイトの追加と削除ができます。このゾー べてに、ゾーンのセキュリティ設定が適用されます。	-ンの Web サイトす
この Web サイトをゾーン(ご追加する( <u>D</u> ):	追加( <u>A</u> )
http://sso1.example.com	<u>肖</u> 『除余( <u>R</u> )
🔲 このゾーンのサイトにはすべてサーバーの確認 (https:) を必要とす	TB( <u>S</u> )
	閉じる( <u>C</u> )

「詳細設定」タブをクリックし、「統合 Windows 認証を使用する」にチェックが入っていることを確認して下 さい。

OpenAM コンソーシアム

インターネット オブション ? 🗙
全般   セキュリティ   プライバシー   コンテンツ   接続   プログラム   詳細設定   設定
<ul> <li>● 厳密な P3P 検証を有効にする*</li> <li>● 署名が無効な場合でもソフトウェアの実行またはインストールを許可する</li> <li>● 証明書のアドレスの不一致について警告する*</li> <li>● 他の混在したコンテンツを持つセキュリティで保護されていないイメージをフ</li> <li>● 統合 Windows 認証を使用する*</li> <li>● 発行元証明書の取り消しを確認する</li> <li>■ 保護付き/保護なしのサイト間を移動する場合に警告する</li> <li>● ブラウズ</li> <li>■ Ctrl+Tab でタブを切り替えるときに、最新のページの順で切り替える</li> <li>● FTP フォルダー ビューを有効にする (Internet Explorer 外)</li> <li>● HTTP エラー メッセージを簡易表示する</li> <li>● Internet Explorer アドレス パーと [ファイルを開く] ダイアログでインラ-</li> <li>● Web ページのボタンとコントロールで視覚スタイルを有効にする</li> <li>▼ マド・コンピューターの再起動後に有効になります</li> </ul>
詳細設定を復元(民)
Internet Explorer の設定をリセット Internet Explorer の設定を既定の状態にリセットします。 リセット(S) ブラウザーが不安定な状態になった場合にのみ、この設定を使ってください。
OK キャンセル 適用(A)

以上で、クライアントの設定は完了です。

<46>



## 12. 動作確認

## それでは実際に動作確認をしてみましょう。

Active Directory に作成した一般ユーザー「test」で、Windows にログインします。その際のドメインは「example.local」になるので、ユーザーID は「test¥example.local」になります。Windows にログインしたら、OpenAM(http://sso1.example.com:8080/openam)の URI にアクセスします。全ての設定に問題が無ければ、 ログイン画面は表示されず、以下のようなユーザープロファイル画面が表示されます。

0	OpenAM - Profil	e - Mozilla Firefox		_
🔗 OpenAM - Profile	× ₽			
Sso1.example.co	om:8080/openam/XUI/#profile/	✓ ♂	→ ☆ 自 🛡	★ =
FORGEROCK			test   <u>Profile</u>   <u>Change Password</u>	d   <u>Log out</u>
<b>∷</b> Dashboard				
User profile	test		Change Passw	vord
First Name		Last Name	test	
Email address		Phone number		
			Update	Reset
	infc Copyright © 2010-14	<u>)@forgerock.com</u> ForgeRock AS, all rights reserved.		



<47>

## 13. トラブルシューティングの方法

Windows デスクトップ認証が正常に動作しない場合、まずは OpenAM のデバッグログを確認して下さい。デバ ッグログの出力先は、管理コンソールの 設定 > サーバーおよびサイト > [サーバー名] > 一般 の「デバッ グ」セクションで確認できます。

0	OpenAM - Mozilla Firefox _ 🛛 🛛	x
🚷 OpenAM	× ₽	
🗲 🕲 ssol.example	e.com:8080/openam/service/ServerSite?: 🗸 🕻 🔍 Invalid initial he: 🗲 🏠 📋 🖡 🏠	
親サイト:なし		^
☆先頭に戻る		
システム		
ペースインストール ディレクトリ:	/usr/share/tomcat6/openam 製品のデータが存在するペースディレクトリ。(プロパティー名: com.iplanet.services.configpath)	
デフォルトのロケール:	en_US 製品のデフォルトのロケール。(プロパティー名: com.iplanet.am.locale)	
通知 URL:	通知サービスエンドポイントの場所。これは、通常、製品の配備 URI または notificationservice です。 (プロパティー名: com sun identity client potification url)	
XML 検証:	off XML 文書の解析時に検証が必要かどうかを指定します。(プロパティー名: com.iplanet.am.util.xml.validating)	
≪ 先頭に戻る		
デバッグ		
デバッグレベル: I 製	ラー - 品類すべてのコンポーネントのデバッグレベル。(プロパティー名: com.iplanet.services.debug.level)	
デバッグファイル オ のマージ: オ し	「フ ▼ ン: デバッグデータをすべて 1 つのファイル (debug.out) に転送します。オフ: コンポーネントごとに個別のデバッグファイルを作成 ます (プロパティ名: com.sun.services.debug.mergeall)	
デバッグディレク %B トリ: デ	ASE_DIR%/%SERVER_URI%/debug バッグファイルが存在するディレクトリ。(プロパティー名: com.iplanet.services.debug.directory)	Ξ
≪ 先頭に戻る		
メールサーバー		
メールサーバーのホスト	≻名: localhost (プロパティー名: com.iplanet.am.smtphost)	
メールサーバーのポート	└番号: 25 (プロパティー名: com.iplanet.am.smtpport)	
☆ 先頭に戻る		~

デバッグログから詳細な情報が得られない場合は、デバッグレベルをメッセージに変更して下さい。

<48>



Windows デスクトップ認証に関するログは、主に以下のファイルに出力されます。

debug/Authentication

このログを参照しても、原因が分からない場合は Wireshark などのパケット解析ツールで Kerberos 通信の内 容を確認して下さい。



14. 付録1: Active Directory のインストールと設定

このセクションでは、Windows Server に Active Directory をインストールする手順を説明します。

🤣 ここで記載されているのは、動作確認用の最小限のインストール、設定手順です。

画面右下のサーバーマネージャーをクリックします。



次のような画面が表示されるので、「② 役割と機能の追加」を選択します。

2	<del>ታ</del> -	-バー マネージャー	Ŀ	- 🗆 X
€ → サーバー 、	マネージャー・ダッシュボー	۴ 🕄 ۲	管理(M) ツ−ル(T) 表示(V	) へルプ(H)
<ul> <li>■ クッシュポード</li> <li>■ ローカル サーバー</li> <li>■ すべてのサーバー</li> <li>■ ファイル サービスと記憶域… ▶</li> </ul>	サーバーマネージャーへようこそ         グ(ックスタート (2)         2         3         最新情報(W)         4         詳細情報(L) <b>役割とサーバーグループ 役割とサーバーグループ 役割</b> の数:1 <b>役割</b> の数:1 <b>役割</b> の数:1 <b>役割</b> の数:1 <b>役割</b> の数:1 <b>び 役割</b> し、 <b>〇 〇</b>	ローカル サーバーの構成 空割と機能の追加 管理するサーバーの追加 サーバー グループの作成 1 サ−バーの合計数: 1 ■ ローカルサーバー 1 ● 管理状態 イベント サービス パフォーマンス BPA 結果	Ξ	► 表示 ▼

「次へ」ボタンをクリックします。

à	役割と機能の追加ウィザード
開始する前に	対象サーバー WIN-91JSAEGHVAC
開始する前に インストールの種類 サーバーの選択 サーバーの役割 機能 確認 結果	このウィザードを使用すると、役割、役割サービス、または機能をインストールできます。ドキュメントの共有や Web サイト のホストなどの組織のコンピューティング ニーズに応じて、インストールする役割、役割サービス、または機能を決定しま す。 役割、役割サービス、または機能を削除するには、次の手順を実行します: 役割と機能の削除ウィザードの起動 続行する前に、次のタスクが完了していることを確認してください。 ・管理者アカウントに強力なパスワードが設定されている ・静的 IP アドレスなどのネットワークの設定が構成されている ・Windows Update から最新のセキュリティ更新プログラムがインストールされている 前提各件が完了していることを確認する必要がある場合は、ウィザードを閉じて、それらの作業を完了してから、ウィザー
	<ul> <li>▶ 「たを再度実行してください。</li> <li>         ・続行するには、[次へ]をクリックしてください。     </li> <li>□ 既定でこのページを表示しない(S)     </li> </ul>
	<前へ(P) 次へ(N)> インストール(I) キャンセル



à	役割と機能の追加ウィザード	_ <b>D</b> X
トレンストールの種类 開始する前に インストールの種類 サーバーの選択 サーバーの役割 機能 確認 結果	役割と機能の追加ウィザード 算の選択 インストールの種類を選択します。役割および機能は、実行中に ンの仮想ハード ディスク (VHD) にインストールできます。	
	< 前へ(P)	次へ(N) > インストール(I) キャンセル



<b>b</b>	役割と	機能の追加ウィザ・	-  *	_ <b>D</b> X
対象サーバーの注	選択			対象サーバー WIN-91JSAEGHVAC
開始する前に インストールの種類 サーバーの選択 サーバーの役割 機能	役割と機能をインストールする ● サーバー プールからサーノ ○ 仮想ハード ディスクから選 サーバー プール フィルター:	5サーバーまたは仮想ハ (ーを選択 選択	ード ディスクを選択します。	
確認 結果	名前 WIN-91JSAEGHVAC	IP アドレス 192.168.1.8	オペレーティング システム Microsoft Windows Server 2	2012 R2 Standard 評価
	< 1 台のコンピューターが見つか このページには、Windows 用して追加されたサーバーが サーバーは表示されません。	りました Server 2012 を実行 表示されます。オフライン	III しており、サーバー マネージャーの [サ ノ サーバーや、データ収集が完了してい	ーバーの追加] コマンドを使 いない、新たに追加された
		<前/	(P) X~(N) > 12	ストール(I) <b>キャンセル</b>

「Active Directory ドメインサービス」を選択します。



「役割と機能の追加ウィザード」が表示されるので、「管理ツールを含める(存在する場合)」にチェックした 状態で、「機能の追加」ボタンをクリックします。

<b>b</b>	役割と機能の追加ウィザード
Ac ま	ctive Directory ドメイン サービス に必要な機能を追加し すか?
Act スま	tive Directory ドメイン サービス をインストールする前に、次の役割サービ たは機能もインストールする必要があります。
	[ツール] グループ ポリシーの管理
⊿	リモート サーバー管理ツール
	▲ 役割管理ツール
	▲ AD DS および AD LDS ツール
	Windows PowerShell の Active Directory モジュール
	▲ AD DS ツール
	[ツール] Active Directory 管理センター
	[ツール] AD DS スナップインおよびコマンドライン ツール
7	管理ツールを含める (存在する場合) 機能の认知 キャンセル







OpenAM コンソーシアム

<56>





内容を確認して、「次へ」ボタンをクリックします。



OpenAM JUJ-STI

<58>

完了と同時に再起動する場合は「必要に応じて対象サーバーを自動的に再起動する」のチェックをクリックします。

OpenAM コンリーシアム

2	役割と機能の追加ウィザード	- 0 X
<b>インストール オブ</b> 開始する前に インストールの種類 サーバーの選択 サーバーの役割 機能 AD DS 殖認 結果	<ul> <li>ションの確認</li> <li>選択したサーバーに次の役割、役割サービス、または機能をインストールするには、</li> <li>必要に応じて対象サーバーを自動的に再起動する</li> <li>かうきつの機能(管理ツールなど)は、自動的に選択されるため、このページに表 らのオブションの機能をインストールしない場合は、[前へ] をクリックして、チェックオ</li> <li>Active Directory ドメイン サービス</li> <li>グループ ポリシーの管理</li> <li>リモート サーバー管理ツール</li> <li>役割管理ツール</li> <li>AD DS および AD LDS ツール</li> <li>Mindows PowerShell の Active Directory モジュール</li> <li>AD DS ツール</li> <li>Active Directory 管理センター</li> <li>AD DS スナップインおよびコマンドライン ツール</li> <li>構成設定のエクスポート</li> <li>代替ソース バスの指定</li> </ul>	対象サーバー WIN-91JSAEGHVAC [インストール] をクリックしてください。 示されている可能性があります。これ ックスをオフにしてください。
	<前へ(P) 次へ(N) >	インストール(I) キャンセル

確認のダイアログが表示されますので、「はい」ボタンをクリックしてチェックを有効にします。

役割と機	態能の追加ウィザード
必要に応じて、このサーバーは     起動しますか?	通知なしで自動的に再起動されます。自動的に
	1411/04 11113

<59>

「インストール」ボタンをクリックして、インストールを開始します。

<b>b</b>	役割と機能の追加ウィザード	_ <b>D</b> X
▲      A ンストール オブ       開始する前に     インストールの種類     サーバーの選択     サーバーの役割     機能     AD DS     7な記	役割と機能の追加ウィザード ションの確認 選択したサーバーに次の役割、役割サービス、または機能をインストールする( ✓ 必要に応じて対象サーバーを自動的に再起動する オプションの機能(管理ツールなど)は、自動的に選択されるため、このページ らのオプションの機能をインストールしない場合は、[前へ]をクリックして、チェッ Active Directory ドメイン サービス グループポリシーの管理 リモート サーバー管理ツール	メオネサーバー WIN-91JSAEGHVAC には、「インストール」をクリックしてください。 にま示されている可能性があります。これ ック ボックスをオフにしてください。
結果	役割管理ツール AD DS および AD LDS ツール Windows PowerShell の Active Directory モジュー AD DS ツール Active Directory 管理センター AD DS スナップインおよびコマンドライン ツール 構成設定のエクスポート 代替ソース パスの指定	-JL
	<前へ(P) 次へ(N) >	インストール(I) キャンセル



完了したら、「閉じる」ボタンをクリックします。インストール時に「必要に応じて対象サーバーを自動的に 再起動する」をチェックしていた場合は自動的に再起動します。

<b>a</b>	役割と機能の追加ウィザード	_ <b>D</b> X
▲ <b>インストールの進行</b> 開始する前に   インストールの種類   サーバーの選択    サーバーの役割   機能   AD DS   確認 <b> <b> 拾果</b> </b>	役割と機能の追加ウィザード	文録サーバー WIN-91JSAEGHVAC
	このウィザードを閉じても、実行中の処理が中断されることはありません。処理の進行 ページを再度開いたりするには、コマンド バーの [通知] をクリックし、 [タスクの詳細 構成設定のエクスポート	う状況を表示したり、この ] をクリックします。
	<前へ(P) 次へ(N) > 目	1173 キャンセル

再起動したら、再度「サーバーマネージャー」を起動して下さい。画面上部の旗のマークのところに警告マー クがあるので、この中の「このサーバーをドメインコントローラーに昇格する」のリンクをクリックすると、 Active Directory ドメインサービスの設定画面が表示されます。

OpenAM コンソーシアム

<b>b</b>		サーバー マネージャー	_ <b>D</b> X
€. サーバー	マネージャー・ダッシュブ	ボード ・ ②   🍢	管理(M) ツ−ル(T) 表示(V) ヘルプ(H)
III クッシュボード     I ローカル サーバー     III すべてのサーバー     III AD DS     IIII ファイル サービスと記憶域… ▶	サーバー マネージャーへようこそ クイック スタート (Q) 最新情報(W)	<ul> <li>▲ 展開後構成 タスク ▼ ×</li> <li>WIN-91JSAEGHVAC で Active Directory ドメイン サービス の構成が必要です</li> <li>このサーバーをドメイン コントローラーに昇格する</li> <li>① 機能のインストール</li> <li>構成が必要です。WIN-91JSAEGHVAC でインストール が正常に完了しました。</li> <li>役割と機能の追加</li> <li>タスクの詳細</li> </ul>	
	詳細情報(L) 役割とサーバー グループ		非表示
	<ul> <li>役割の数: 2 ↓ サーバー グループの</li> <li>役割の数: 2 ↓ サーバー グループの</li> <li>● 管理状態 イベント サービス パフォーマンス BPA 結果</li> </ul>	数:1   サーバーの合計数:1 1 1 ① デイル サービスと記憶 1 域サービス 1 ① 管理状態 イベント パフォーマンス BPA 結果	Y

OpenAM コンソーシアム

<62>

「新しいフォレストを追加する」を選択して、「ルートドメイン名」に適切なドメイン名(本書の構成の場合は example.local)を入力します。完了したら、「次へ」ボタンをクリックして下さい。

OpenAM コンソーシアム

2	Active Directory ドメインサ	ービス構成ウィザード	_ <b>_</b> X
配置構成          配置構成         ドメイン コントローラー オブ・・・         追加オプション         パス         オプションの確認         前提条件のチェック         インストール         結果	配置操作を選択してください <ul> <li>既存のドメインにドメイン コントローラー・</li> <li>新しいドメインを既存のフォレストに追加</li> <li>新しいフォレストを追加する(F)</li> </ul> この操作のドメイン情報を指定してください ルートドメイン名(R): 詳細 配置構成	を追加する(D) Iする(E) example.loca	<u>ዎ-ሾቃኑ サ-ሾ- WIN-91JSAEGHVAC</u>
	<	前へ(P) 次へ(N) >	インストール(I) <b>キャンセル</b>

OpenAM コンソーシアム

<63>

パスワードを入力して、「次へ」ボタンをクリックします。

<b>B</b>	Active Directory ドメイン	> サービス構成ウィザード	_ 0 X
ド <b>メイ</b> ン コントロー	ラー オプション		ターゲット サーバー WIN-91JSAEGHVAC
配置構成 トメイン コントローラー オプ・・・ DNS オプション 追加オプション パス オプションの確認 前提条件のチェック インストール 結果	新しいフォレストおよびルート ドメインの フォレストの機能レベル: ドメインの機能レベル: ドメイン コントローラーの機能を指定し 「ドメイン ネーム システム (DNS) 「ゲローバル カタログ (GC)(G) 「読み取り専用ドメイン コントローラ ディレクトリ サービス復元モード (DSF パスワード(D): パスワードの確認入力(C):	D機能レベルを選択してください Windows Server 2012 R2 Windows Server 2012 R2 VTください サーバー(O) iー (RODC)(R) XM) のパスワードを入力してください ●●●●●●●●	
	詳細 ドメイン コントローラー オプション	ć	
		<前へ(P) 次へ(N) > 化	ンストール(I) <b>キャンセル</b>



そのまま「次へ」ボタンをクリックします。

2	Active Directory ドメイン t	ナービス構成ウィザード	_ <b>_</b> X
DNS オプション	ないか Windows DNS サーバーが実行さ		ターゲット サーバー WIN-91JSAEGHVAC 季任を作… 詳細主テ 🖌
配置構成 ドメイン コントローラー オブ… DNS オプション 追加オプション パス オプションの確認 前提条件のチェック インストール 結果	DNS 委任オプションの指定 □ DNS 委任の作成(D)		
	詳細 DNS 委任		
		<前へ(P) 次个(N) >	インストール(I) <b>キャンセル</b>



デフォルトのまま(本書の構成の場合は EXAMPLE)、「次へ」ボタンをクリックします。

<b>b</b>	Active Directory ドメ	イン サービス構成ウィザード	_ <b>_</b> ×
追加オプション			ターゲット サーバー WIN-91JSAEGHVAC
配置構成	ドメインに割り当てられている NetF	1	
ドメイン コントローラー オブ…	NetBIOS ドメイン名:		
DNS オノション 追加オプション			
パス			
オプションの確認			
前提条件のチェック			
インストール 総由			
和未			
	詳細 追加オプション		
		<前へ(P) 次へ(N)> イン	ストール(I) <b>キャンセル</b>

データベースファイルなどの出力先を変更する場合は、変更して「次へ」ボタンをクリックして下さい。



内容を確認して、「次へ」ボタンをクリックします。

<b>b</b>	Active Directory ドメイン サービス構成ウィザード	D X
オプションの確認	ターゲット WIN-91JSAE(	サーバー GHVAC
配置構成 ドメイン コントローラー オブ… DNS オプション 追加オプション パス オプションの確認 前提条件のチェック インストール 結果	次の選択を確認してください: 新しいフォレストの最初の Active Directory ドメイン コントローラーとしてこのサーバーを構成します。 新しいドメイン名は "example.local" です。これは新しいフォレスト名にもなります。 ドメインの NetBIOS 名: EXAMPLE フォレストの機能レベル: Windows Server 2012 R2 ドメインの機能レベル: Windows Server 2012 R2 追加オプション: グローバル カタログ: はい DNS サーバー: はい DNS サーバー: はい DNS 委任の作成: いいえ これらの設定は、追加のインストールを自動化する Windows PowerShell スクリプトに エクスポートできます スクリプトの表	▲
	<前へ(P) 次へ(N) > インストール(I) キャ	ンセル





OpenAM JV

完了すると自動的に Windows Server が再起動します。

以上で、Active Directory サーバーの設定は完了です。

15. 付録 2: DNS サーバーの設定

各 Windows クライアントから、OpenAM サーバーの名前解決ができるように、前方参照ゾーンに Host (A) レコードを、逆引き参照ゾーンに Pointer (PTR) レコードを追加します。

まずは、前方参照ゾーンに A レコードを追加します。「管理ツール」 > 「DNS」より、DNS マネージャーを起動して下さい。

🕲 I 🖸 🖪 🖛 I	管理ツ-	-11		-	
ファイル ホーム 共有	表示				~ <b>(</b> )
ا<⊏ • 🗟 → 👌		▼ ♂ 管理ツ	ールの検索	Q	
☆ お気に入り	名前	更新日時	種類	サイズ	^
🎉 ダウンロード	\mu Terminal Services	2013/08/23 0:39	ファイル フォルダー		
📰 デスクトップ	🛃 Active Directory サイトとサービス	2013/08/22 15:55	ショートカット	2 KB	
🗐 最近表示した場所	🛃 Active Directory ドメインと信頼関係	2013/08/22 15:55	ショートカット	2 KB	
	<u>え</u> Active Directory ユーザーとコンピューター	2013/08/22 15:55	ショートカット	2 KB	
PC	🛃 Active Directory 管理センター	2013/08/22 8:50	ショートカット	2 KB	
🍡 ダウンロード	📝 ADSI エディター	2013/08/22 15:55	ショートカット	2 KB	
灄 デスクトップ	B DNS	2013/08/22 15:55	ショートカット	2 KB	=
אראב+ז 📗	15CST イニシェーター	2013/08/22 15:57	ショートカット	2 KB	
📔 ピクチャ	📷 ODBC データ ソース (32 ビット)	2013/08/22 8:56	ショートカット	2 KB	
📓 ビデオ	📷 ODBC データ ソース (64 ビット)	2013/08/22 15:59	ショートカット	2 KB	
🜗 ミュージック	🔝 Windows PowerShell (x86)	2013/08/23 0:37	ショートカット	3 KB	
🏭 ローカル ディスク (C:)	📷 Windows PowerShell ISE (x86)	2013/08/22 15:55	ショートカット	2 KB	
🎽 DVD ドライブ (D:) IF	🗃 Windows PowerShell ISE	2013/08/22 15:55	ショートカット	2 KB	
	😿 Windows PowerShell 用の Active Dire	2013/08/22 15:55	ショートカット	2 KB	
📬 ネットワーク	🖄 Windows Server バックアップ	2013/08/22 15:53	ショートカット	2 KB	
	Nindows メモリ診断	2013/08/22 15:52	ショートカット	2 KB	
	🔝 イベント ビューアー	2013/08/22 15:55	ショートカット	2 KB	
	🛃 グループ ポリシーの管理	2013/08/22 15:56	ショートカット	2 KB	
	🛃 コンピューターの管理	2013/08/22 15:54	ショートカット	2 KB	
	🔊 コンポーネント サービス	2013/08/22 15:57	ショートカット	2 KB	
	🛃 サーバー マネージャー	2013/08/22 15:55	ショートカット	2 KB	×
31 個の項目		16° CP			



起動したら、「前方参照ゾーン」を右クリックして、新しいゾーンを追加します。





「次へ」ボタンをクリックします。






新しいゾーン ウィザード	×
<mark>ゾーンの種類</mark> DNS サーバーは各種のゾーンと記憶域をサポートします。	The second second
作成するゾーンの種類を指定してください:	
● プライマリ ゾーン(P)	
このサーバーで直接更新ができるゾーンのコピーを作成します。	
○ セカンダリ ゾーン(S) ほかのサーバーに存在するゾーンのコピーを作成します。このオプションは、プライマリ サーバーの処理 負荷の均衡化を助け、フォールト トレランスを提供します。	1
○ スタブ ゾーン(U) ネーム サーバー (NS) 及び、SOA (Start of Authority) のみを含むゾーンのコピーを作成しま す (グルー ホスト (A) レコードも含めることが可能です)。 スタブ ゾーンを含むサーバーは、そのゾーン に対して権威を持っていません。	×
✓ Active Directory にゾーンを格納する(A) (DNS サーバーが書き込み可能ドメイン コントローラーの場合のみ利用可能です)	
< 戻る(B) 次へ(N) > キャン	12IL



「このドメインのドメインコントローラー上で実行しているすべての DNS サーバー: example.local」を選 択して、「次へ」ボタンをクリックします。

OpenAM コンソーシアム

新し	ノいゾーン ウィザード	x
Active Directory ゾーン レプリケーション ス DNS データがネットワーク全体でどのように	スコープ レプリケートされるかを選択できます。	1 TH 100
ソーン データのレプリケート方法を選択して	てください。	
○ このフォレストのドメイン コントローラー上	で実行しているすべての DNS サーバー(A): ex	ample.local
◎ このドメインのドメイン コントローラー上で	を実行しているすべての DNS サーバー(D): exa	mple.local
○ このドメインのすべてのドメイン コントロー (Windows 2000 との互換性維持の)	-ラー(O): example.local Dため)	
○ このディレクトリ パーティションのスコープ	で指定されたすべてのドメイン コントローラー(C):	
		~
	< 戻る(B) 次へ(N) >	キャンセル



「ゾーン名」に OpenAM の Cookie ドメインから先頭の「.」を除いた値を入力して、「次へ」ボタンをクリック します。

新しいゾーン ウィザード	×
<b>ゾーン名</b> 新しいゾーンの名前を指定してください。	
ゾーン名は、このサーバーが権限を持っている DNS 名前空間の一部を指定します。 組織 microsoft.com) やドメイン名の一部 (例: newzone.microsoft.com) などがありま DNS サーバーの名前ではありません。 ゾーン名(Z):	飯のドメイン名 (例: ます。ゾーン名は
example.com	
< 戻る(B) 次へ(N) >	キャンセル

「セキュリティで保護された動的更新のみを許可する」を選択して、「次へ」ボタンをクリックします。

OpenAM コンソーシアム

	新しいゾーン ウイザード	×
動的更新 この DNS 更新を受(	ゾーンがセキュリティで保護された更新、セキュリティで保護されていない更新、または動的 ナ入れるかどうかを指定できます。	
動的更新 サーバー(	fiにより、DNS クライアント コンピューターのリソース レコードに変更があればいつでも DNS こ対して登録や動的な更新を行うことができます。	
<mark>許可する</mark>	動的な更新の種類を選択してください:	
ב≠ء 207	リティで保護された動的更新のみを許可する (Active Directory 用に推奨)(S) ヤプションは Active Directory を統合しているソーンでのみ利用できます。	
○ 非セ= どのり <u>へ</u>	Fユリティ保護およびセキュリティ保護の両方による動的更新を許可する(A) フライアントからもリソース レコードの動的更新が受け付けられます。 このオプションを選択すると、信頼されていないソースからの更新も受け付けるようになるため、 セキュリティによる保護が脆弱になります。	
○ 動的見 このり ばなり	更新を許可しない(D) 『ーンはリソース レコードの動的更新を受け付けません。これらのレコードを手動で更新しなけれ Dません。	
	< 戻る(B) 次へ(N) > キャンセ	IL



<76>

内容を確認して、「完了」ボタンをクリックします。



OpenAM コンリーシアム



<77>



次に、作成された「example.com」を右クリックして、新しいホストを作成します。

å	DNS マ	ネージャ	2 775	_	D X
ファイル(F) 操作(A) 表示(V)	へルプ(H)				
🗢 🄿 🙍 🖬 🗶 🖬 🧟 🖻					
🛔 DNS	名前	種類		データ	タイムスタン
▲ WIN-91JSAEGHVAC ▶ 創 グローバル ログ ▲ 値 前方参照ゾーン ▶ 『 _msdcs.example.local ▶ ◎ example.local	<ul> <li>(親フォルダーと同じ)</li> <li>(親フォルダーと同じ)</li> </ul>	Start Name	of Authority (S Server (NS)	[1], win-91jsaeghvac.e win-91jsaeghvac.exam	静的 静的
Compare サーバー	'' · データファイルの更新(U)				
▶ 🔜 逆りき参照 ▶ 🎬 トラスト ポイ 再読み	込み(E)				
▶ 🧰 条件付フォワ 新しいす	スト (A または AAAA)(S)				
新しいエ	イリアス (CNAME)(A)	10			
新しいメ	ール エクスチェンジャー (MX)(M)				
新しいド	ジイン(0)				
新しい書	ē任(G)				
その他の	)新しいレコード(C)				
DNSSE	EC(D)	•			
すべての	920(K)	•			
表示(V	)	•			
削除(D	)				
く III 最新の	青報に更新(F)		Ш		>
新しいホストリソースレコ 一覧のこ	エクスポート(L)				
プロパテ	۲(R)				
ヘルプ(ト	H)				

OpenAM サーバーのホスト名と IP アドレスを入力して、「ホストの追加」ボタンをクリックします。

新しいホスト
名前 (空欄の場合は親ドメインを使用)(N):
sso1
完全修飾ドメイン名 (FQDN):
sso1.example.com.
IP アドレス(P):
192.168.0.2
<ul> <li>□ 関連付けられたポインター (PTR) レコードを作成する(C)</li> <li>□ 同じ所有者名の DNS レコードの更新を認証されたユーザーに許可する(O)</li> </ul>
ホストの追加(H) キャンセル



最後に、逆引き参照ゾーンに PTR レコードを追加します。

「逆引き参照ゾーン」を右クリックして、新規ゾーンを追加して下さい。







「次へ」ボタンをクリックします。









OpenAM コンリーシアム

OpenAM コンソーシアム

<82>

「このドメインのドメインコントローラー上で実行しているすべての DNS サーバー: example.local」を選 択して、「次へ」ボタンをクリックします。

新しいゾーン ウイザード	x
Active Directory ゾーン レプリケーション スコープ DNS データがネットワーク全体でどのようにレプリケートされるかを選択できます。	I THE REAL PROPERTY OF
ゾーン データのレプリケート方法を選択してください。	
○ このフォレストのドメイン コントローラー上で実行しているすべての DNS サーバー(A): e	xample.local
● このドメインのドメイン コントローラー上で実行しているすべての DNS サーバー(D): ex	ample.local
○ このドメインのすべてのドメイン コントローラー(O): example.local (Windows 2000 との互換性維持のため)	
○ このディレクトリ パーティションのスコープで指定されたすべてのドメイン コントローラー(C):	
	v
	1
< 戻る(B) 次へ(N) >	キャンセル



「IPv4 逆引き参照ゾーン」を選択して、「次へ」ボタンをクリックします。

新しいゾーン ウィザード	x
<mark>逆引き参照ゾーン名</mark> 逆引き参照ゾーンは、IP アドレスを DNS 名に変換します。	
IPv4 アドレスまたは IPv6 アドレスのための逆引き参照ゾーンを作成するかどうかを選択してください。	
● IPv4 逆引き参照ゾーン(4)	
○ IPv6 逆引き参照ゾーン(6)	
< 戻る(B) 次へ(N <u>)</u> > キャン	til 🛛



「ネットワーク ID」に IP アドレス範囲のネットワーク ID を入力します。例えば、OpenAM サーバーの IP アド レスが「192.168.0.11」の場合は「192.168.0」を入力して、「次へ」ボタンをクリックします。

OpenAM コンソーシアム

新しいゾー	-ン ウイザード	x
<b>逆引き参照ゾーン名</b> 逆引き参照ゾーンは、IP アドレスを DNS 名に変掛	奥します。	
<ul> <li>逆引き参照ソーンを識別するには、ネットワーク ID</li> <li>● ネットワーク ID(E):         <ul> <li>192 .168 .0</li> <li>ネットワーク ID は、このゾーンに属する IP アレてください。</li> <li>ネットワーク ID に 0 を使うと、ゾーン名に表示 10.in-addr.arpa を作成し、ネットワーク ID</li> <li>○ 逆引き参照ゾーンの名前(V):</li></ul></li></ul>	)またはゾーン名を入力してください。 ドレスの一部です。通常の順序でネットワーク ID を入力し 示されます。たとえば、ネットワーク ID 10 は、ゾーン 10.0 はゾーン 0.10.in-addr.arpa を作成します。	
	< 戻る(B) 次へ(N) > キャンセル	

<85>

「セキュリティで保護された動的更新のみを許可する」を選択して、「次へ」ボタンをクリックします。

動	的更新 この DNS ゾーンがセキュリティで保護された更新、セキュリティで保護されていない更新、または動的 更新を受け入れるかどうかを指定できます。
	動的更新により、DNS クライアント コンピューターのリソース レコードに変更があればいつでも DNS サーバーに対して登録や動的な更新を行うことができます。
	許可する動的な更新の種類を選択してください:
	● セキュリティで保護された動的更新のみを許可する (Active Directory 用に推奨)(S) このオプションは Active Directory を統合しているゾーンでのみ利用できます。
	<ul> <li>○ 非セキュリティ保護およびセキュリティ保護の両方による動的更新を許可する(A) どのクライアントからもリソース レコードの動的更新が受け付けられます。</li> <li>▲ このオプションを選択すると、信頼されていないソースからの更新も受け付けるようになるため、 セキュリティによる保護が脆弱になります。</li> </ul>
	○ 動的更新を許可しない(D) このゾーンはリソース レコードの動的更新を受け付けません。これらのレコードを手動で更新しなけれ ばなりません。
	< 戻る(B) 次へ(N) > キャンセル



最後に、「完了」ボタンをクリックします。

新しいゾーン ウィザード
新しいゾーン ウィザードの完了 新しいゾーン ウィザードが完了しました。指定された設定は次のとおりで す: 名前: 192.168.0.in-addr.arpa 種類: Active Directory 統合プライマリ 参照の種類: 逆引き
注意: ゾーンにレコードを追加するか、またはレコードが動的に更新され ることを確認してください。その後、nslookupを使って名前の解決を検 証してください。 このウィザードを閉じて新しいゾーンを作成するには、[完了]をクリックしてく ださい。 < 戻る(B) 完了 キャンセル

OpenAM コンソーシアム

以上で、DNS サーバーの設定は完了です。

<87>



## 16. 付録3: FirefoxとChromeの設定

FireFox を使用して、Windows デスクトップ SSO 行う場合は以下の設定が必要です。

FireFox を起動して、アドレスバーに "about: config" を入力します。次に、フィルタに "negotiate" と入 力して絞り込みを行い、次の2つの属性に OpenAM の Cookie ドメインを設定します。

network.negotiate-auth.delegation-uris 属性: .example.com network.negotiate-auth.trusted-uris 属性: .example.com

ファイル(E) 編集(E) 表示(V) 履歴(S) ブックマーク(B)	ツール(I)	ヘルプ(圧)						
aboutconfig × +								
Fire fox about config		⊽ C 😫	+ Google	٩	☆自	÷	♠	≡
検索(R): negotiate								×
設定名	状態	型	値					E.
network negotiate-auth gsslib	初期設定値	文字列						
network.negotiate-auth.delegation-uris	ユーザ設定	文字列	.example.com					
network.negotiate-auth.trusted-uris	ユーザ設定	文字列	.example.com					
network negotiate-auth.allow-insecure-ntlm-v1	初期設定値	真偽値	false					
network negotiate-auth.allow-non-fqdn	初期設定値	真偽値	false					
network negotiate-auth.allow-insecure-ntlm-v1-https	初期設定値	真偽値	true					
network negotiate-auth.allow-proxies	初期設定値	<b>真偽値</b>	true					
network negotiate-authusing-native-gsslib	初期設定値	真偽値	true					

Chrome を使用して Windows デスクトップ SSO 行う場合は、「11. クライアント PC (Windows)の設定」で説 明した Internet Explorer の設定があれば十分です。



## 17. 参考資料

OpenAM Release Notes

<u>http://OpenAM.forgerock.org/OpenAM-documentation/OpenAM-doc-source/doc/release-</u> notes/index.html

OpenAM Wiki - How does OpenAM work with Windows Desktop SSO <u>https://wikis.forgerock.org/confluence/display/OpenAM/How+does+OpenAM+work+with+Windows+Desktop+S</u> <u>SO</u>

OpenAM 12.0.0 Administration Guide - Hints for the Windows Desktop SSO Authentication Module <u>http://docs.forgerock.org/en/openam/12.0.0/admin-guide/index/chap-auth-services.html#desktop-module-conf-hints</u>

OpenAM Nightly Builds http://forgerock.org/downloads/OpenAM-builds/

OpenAM コンソーシアム OpenAM インストール手順 http://www.OpenAM.jp/category/member/techtips

