



OSSTech

Samba LDAP  
統合認証,SSOなら  
OSSTechへ

オープンソース・  
ソリューション・  
テクノロジー株式会社

<http://www.osstech.co.jp>

〒141-0022

品川区東五反田1-21-10  
三井住友海上五反田ビル6F

電話 & Fax : 03-5422-9373

Email: [info@osstech.co.jp](mailto:info@osstech.co.jp)



OpenAM

for Linux/Solaris/Windows/AIX

製品情報



OpenAM for Linux/Solaris/Windows/AIX 製品機能概要

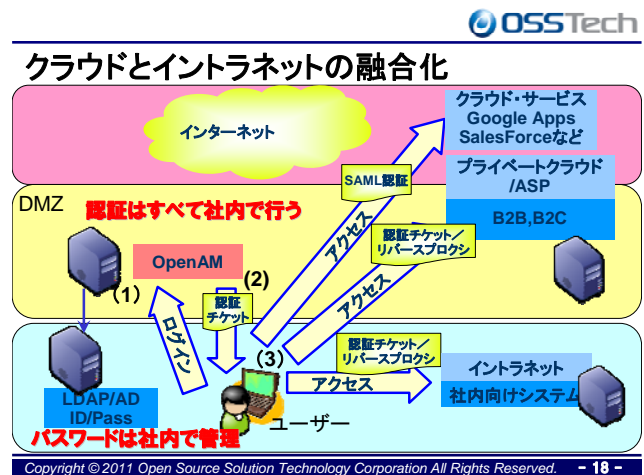
- シングルサインオン (SSO) 機能
  - ◆ 従来製品OpenSSO,Sun AccessManagerの後継製品で互換性あり
  - ◆ OpenAMで一度認証されたユーザは、OpenAMで管理したリソースに再度認証することなくアクセス可能
  - ◆ SSOの方式としてエージェント方式、リバースプロキシ方式に対応
  - ◆ 代理認証によるSSO : Form認証およびBasic認証を備えたアプリケーションに対して、OpenAMが擬似サインオンを実現
  - ◆ Windows Desktop SSO : Windowsドメイン認証により認証を受けたユーザは、その端末上でウェブブラウザを起動すると、パスワードを入力することなくウェブアプリケーションに即座にアクセス可能
  - ◆ OpenAMの認証バックエンドとしてWindows Active DirectoryやOpenLDAPなどのディレクトリサーバーとMySQLやOracleなどのRDBを利用可能
  - ◆ 多要素認証  
IDとパスワードだけでなく、社員証 (フェリカなどのICカード) や生体認証 (指紋認証や静脈認証)、OTP (ワンタイムパスワード) などの認証も併せて行うことでセキュリティレベルを上げることが可能
- アクセス制御機能
  - ◆ ユーザが利用できるアプリケーションをレルムというグルーピング機能を使って制御することができます。
- フェデレーション機能
  - ◆ Google AppsやSalesforceと連携可能なSAML認証をサポート
  - ◆ 独自認証しているアプリをSAML対応にさせるFedletを提供  
Javaや.Net , PHPアプリを容易にSAML対応に改造可能

# 1. OpenAM詳細機能

## (1) シングルサインオン (SSO) 機能

- ① OpenAM で認証されたユーザは、OpenAM で管理したリソースに再度認証 (パスワードを再入力する) 必要なくアクセスできます。
- ② SSO の方式としてエージェント方式、リバースプロキシ方式をサポートしています。
- ③ 代理認証による SSO  
独自の認証機構を持つパッケージ製品に対して、アプリケーションの改修を加えることなく、代理認証と呼ばれる仕組みを用いて擬似的にシングル・サインオンを実現することができます。代理認証の仕組みでは、OpenAM がエンドユーザに成り代わり、Form 認証及び Basic 認証を備えたアプリケーションへの擬似シングル・サインオンを実現します。
- ④ Windows Desktop SSO  
Kerberos 認証の仕組みを使い、Windows の AD ドメイン認証と OpenAM の認証の仕組みを連携させる方法です。Windows ドメイン認証により認証を受けたユーザは、その端末上でウェブブラウザを起動すると、再度パスワードを入力することなくウェブアプリケーションに即座にアクセスできるようになります。
- ⑤ 複数の認証ディレクトリと RDB に対応  
OpenAM は標準でディレクトリサーバー OpenDS を組み込んでおり、設定情報を格納するだけでなく、ユーザ情報 (認証情報) を保持することが可能です。加えて OpenAM の認証バックエンドとして Windows Active Directory や OpenLDAP などの一般的なディレクトリサーバーと MySQL や Oracle といった RDB を利用でき、ID (パスワード) 情報を一元管理することが可能です。
- ⑥ 多要素認証  
ID とパスワードだけでなく、社員証 (フェリカなどの IC カード) や生体認証 (指紋認証や静脈認証)、OTP (ワンタイムパスワード) などの認証も併せて行うことでセキュリティレベルを上げることができます。
- ⑦ クロスドメイン・シングル・サインオン  
複数の DNS ドメインをまたがるシングル・サインオンであるクロスドメイン・

シングル・サインオンに対応しています。



## (2) アクセス制御機能

- ① ユーザが利用できるアプリケーションをレールムというグルーピング機能を使って制御することができます。
- ② 管理者は1つの集中管理コンソールから、エージェントとサーバの構成およびエージェントが適用するポリシーを設定することができます。
- ③ 開発者は様々な統合開発環境やアイデンティティ・サービスを介し、OpenAM のサービスへ直接アクセス可能できます。
- ④ ポリシーを定義して企業/組織全体に適用できる業界規格のフレームワークである XACML ベースのポリシー管理を適用できます。
- ⑤ アクセス制御対象は URL で指定することができるため、ドメインやサーバレベルだけでなくフォルダやファイル単位で細かく制御できます。さらに、認証方式、クライアントアドレス等の認証コンテキストによっても制御可能です。
- ⑥ 自動ログオフ機能  
一定時間ユーザからのアクセスがなかった場合に自動的に接続を切断することが可能です。
- ⑦ アクセスログ  
OpenAM では認証ログや代理認証やリバースプロキシ型の認証時などユーザのログイン、ログアウト時刻、アイドルタイムアウト後の自動ログオフ時、アクセス元、アクセス先のログなど様々な事象のログを採取可能です。(ただし、ログアウトのログに関してはログアウト処理をせずにブラウザを終了すると記録されないことがあります)

### (3) フェデレーション機能

- ① OpenAM は、フェデレーションを実現するための軽量なパッケージである Fedlet を提供します。
- ② 軽量な Fedlet をアイデンティティ・プロバイダーからサービス・プロバイダーへ提供することで、他のフェデレーション製品を追加することなく、容易に企業へのフェデレート・バックが行えます。
- ③ サービス・プロバイダーは、Fedlet をアプリケーションに追加し、アプリケーションを実装するだけでフェデレーションを有効にすることができます。
- ④ Fedlet は Java と .NET の両方のアプリケーションで利用可能です。  
加えて PHP アプリケーションなどとの連携も可能です。
- ⑤ フェデレーションでサポートされる機能には以下が含まれます。
  - ・ SAML 1.0/1.1/2.0  
(OASIS Security Assertion Markup Language)  
Google Apps や Salesforce と連携可能です
  - ・ Liberty ID-FF 1.1/1.2 (Liberty Alliance Project Identity Federation Framework )
  - ・ WS-Federation (Passive Requestor Profile)
  - ・ WS-Trust
  - ・ WS-Security
  - ・ WS-Policy
  - ・ WS-I BSP などに対応
- ⑥ フェデレーションでは、シングル・サインオンだけでなく、ユーザの属性情報(アイデンティティ)や認証コンテキスト(認証方法や認証日時等)も受け渡すことが可能です。従って、フェデレーション環境下のアプリケーションではアクセスするユーザに応じたコンテンツを配信できます。
- ⑦ マルチ・プロトコル・フェデレーション・ハブ異なるフェデレーション・プロトコルを「翻訳」し、アイデンティティ・プロバイダーとサービス・プロバイダーは複数のプロトコルを利用して SSO の確立が可能です。
- ⑧ 集中化された Federation Validator 管理者は、フェデレーションの通信が稼動しているかどうかをシステム動作中に素早くテストすることが可能です。

- ⑨ バーチャル・フェデレーション・プロキシ機能  
サービス・プロバイダーに対するフェデレーションを実現するために、既存の認証アプリケーションを利用して企業/組織内で既に確立されている SSO を有効に利用でき、Web サービスのセキュリティを向上させます。

## 2. OSSTech社独自の改良点

OSSTech 社製 OpenLDAP において専用スキーマを拡張し、OpenLDAP および Tomcat, Linux との親和性を向上させています。

## 3. 最新製品名およびバージョン

- OpenAM 9.5

## 4. システム要求仕様

- (1) オペレーティングシステム
  - Red Hat Enterprise Linux 5 以降
  - CentOS 5 以降
  - Solaris 10 Sparc 版および Intel 版
  - その他、Java が動作する OS (64 ビット OS を推奨)
- (2) アプリケーションサーバー
  - Apache Tomcat 6 以降
  - Oracle Application Server
  - BEA Weblogic
  - IBM WebSphere
  - JBoss Application Server など
- (3) ディレクトリサーバー
  - OpenLDAP 2.4 以降
  - OpenDS (標準で内蔵しています)
  - Microsoft Windows Active Directory
  - Oracle Directory Server Enterprise Edition
- (4) 対応 Web クライアント
  - オペレーティングシステム
    - WindowsXP 以降を推奨
    - Mac OS X (Tiger 以降を推奨)
    - Linux, UNIX
  - Web ブラウザ
    - Microsoft Internet Explorer 7 以降
    - Firefox 3.0 以降
    - Safari 3.0 以降

## OSSTech OpenAM製品エディション比較

項目		OSSTech OpenAM	
		Standard Edition	Enterprise Edition
価格	パッケージ価格	¥500,000/ノード	¥3,000,000/ノード
	サポート料金	¥960,000/年・システム	¥1,200,000/年・システム
	各種Agent/パッケージ価格	¥100,000/ノード	¥100,000/ノード
	各種Agentサポート料金	¥240,000/年・システム	¥240,000/年・システム
サーバー動作対応 オペレーティングシステム	Linux(RHEL,CentOS)	○	○
	Windowsサーバー	×	○
	Solaris x86	×	○
	Solaris SPARC	×	○
	その他	×	○
サーバー動作対応 アプリケーションサーバー	Tomcat 6以降	○	○
	JBoss Application Server	×	○
	その他	×	○
SSO対象 アプリケーション	アプリの種類	3種類	無制限
	Apache Agent	○	○
	IIS Agent	×	○
	Sun Web Server Agent	×	○
	Sun Proxy Server Agent	×	○
	Tomcat Agent	○	○
	JBoss Agent	×	○
	Web Logic Agent	×	○
	Glassfish Agent	×	○
	Websphere Agent	×	○
	Fedlet	×	○
	代理認証	○	○
	Google Apps,Salesforceなどとの SAML連携	○	○
認証方式	Desktop SSO	×	○
	ICカードやOTPなどの 認証デバイス対応	×	○
冗長化	サイト構成	○2ノードまで	○台数無制限
	セッションフェイルオーバー	×	○
ユーザーリポジトリとして 利用可能な ディレクトリサーバー	OSSTech製OpenLDAP	○	○
	一般OpenLDAP	×	×
	ActiveDirectory	○認証のみ※1	○
	OpenDS/OpenDJ	○※2	○※2
	Oracle DSEE / Sun JDS	×	○
	その他LDAP	×	○
RDMS (JDBC接続)	×	○	

※1：ADは認証用として利用し、スキーマ拡張には対応しない

※2：OpenAM内蔵のOpenDSのみ対応、OpenAM以外の用途としてのLDAP機能はサポートしない