

Press Release

「Shibboleth IdP オプション」をバージョンアップした「AXIOLE v1.14.1」をリリース

Shibboleth IdP の最新版 IdP V3 に対応

uApprove・FPSP や Office365 の IdP 関連機能も再実装

株式会社ネットスプリング（本社：東京都港区、代表取締役社長：西武 進）は、LDAP ベースの認証アプリケーションサーバ「AXIOLE（アクシオレ）」の新バージョン「AXIOLE v1.14.0」を開発し、出荷を開始します。本バージョンでは、学術教育研究機関向けのオプションである「AXIOLE IdP オプション」を、Shibboleth IdP V3 に準拠した IdP V3 対応版として提供します。バージョンアップした AXIOLE IdP オプションでは、Shibboleth IdP の条件同意機能（uApprove 相当）や、特定の SP（サービスプロバイダー）へのアクセスポリシー設定を可能にする「FPSP 機能（SP アクセスポリシー）」も旧バージョン同様に標準実装しています。新バージョンは 4 月 21 日からファームウェアの提供を開始。既存の IdP オプションライセンス購入済みのユーザは、無償で IdP V3 へのバージョンアップが可能です。なお、Java の脆弱性対応を実施した AXIOLE v1.14.1 を 5 月 12 日にリリース済みです。

AXIOLE IdP オプションは、全国の大学等と国立情報学研究所（NII）が連携して運用する学術認証フェデレーション「学認：GakuNin」の相互認証連携システム「Shibboleth」に対応し、異なる組織間でのシングルサインオンを可能にする IdP 機能を提供します。

Shibboleth IdP の最新版である IdP V3 をベースに開発した AXIOLE IdP オプションの IdP V3 対応版は、AXIOLE の新バージョンのオプション機能として提供され、旧バージョンで実装済みの uApprove 機能や FPSP 機能は、Shibboleth IdP V3 をベースに再実装しています。uApprove 機能については、Shibboleth IdP V3 に標準実装された条件同意機能をベースに実装しています。

FPSP（Filter Per SP：SP アクセスポリシー）機能は、エンドユーザが内外のさまざまなサービス提供者による Web アプリケーション（SP）にアクセスする際、SP から入る IdP への認証要求に対し、そのユーザの利用可否を SP 側でなく、IdP 側で設定できる Shibboleth の機能です。各 SP との利用ライセンス数や、ユーザの所属や役職などの属性（資格）により、利用可否を IdP 側で設定することが可能となり、例えば、特定 SP に対して、一般学部生は使用不可だが院生や教職員は利用可能といった設定ができるようになります。

FPSP 機能は、Shibboleth IdP V3 の標準機能として提供されていますが、導入利用には XML の作成編集などかなりの技術力が必要となります。ネットスプリングでは導入運用上の使いやすさを追求した FPSP 機能「SP アクセスポリシー」を独自に開発し、AXIOLE 各設定画面と共通の使いやすい Web GUI ベースで実装。編集画面からの設定ができ、コーディング技術などを必要とすることなく、専門技術を持たない事務担当者による運用操作も可能です。本機能は、利便性を考慮し、IdP V3 において再実装しています。

AXIOLE は、新装なった Shibboleth IdP オプションにより、本格的な普及期に入りつつある学認への参加や、地域大学間連携機能の本格運用など、学術教育研究機関が相互認証で連携するシステムを構築しようとする際に、セキュリティ面においてより安心して導入できるオールインワンの認証アプリケーションサーバとして、今後も顧客の期待に応えていきます。

本バージョンのリリースと同時に、AXIOLE の IdP 機能のみに限定した「IdP 専用アプリケーションモデル」（外部認証参照のみ）および仮想アプリケーション版「AXIOLE-i」にも、本機能が提供されます。

なお、AXIOLE の IdP オプション (V1.13 以前) をご利用の組織においては、バージョンアップに際しては、IdP に関連する設定変更その他の作業が必須となりますが、IdP オプション機能以外の設定については、設定変更その他の作業は必要ありません。また、IdP V3 の導入に際して、SP 側の変更作業その他は一般的に不要です。

●AXIOLE-IdP と条件同意機能 (uApprove 相当) 各画面



AXIOLE

Webログインサービス

Login to Sample SP-1

ユーザ名とパスワードを入力して"ログイン"ボタンを押下してください。

ユーザ名

パスワード

ログイン状態を記憶しない

ユーザ情報送信の同意を解除する

ログイン



AXIOLE

サンプルフェデレーション使用条件

2016/xx/xx

第1.0版

サンプルフェデレーションを利用する際には、利用するサービスに対して利用者のユーザ情報が送信されます。サンプルフェデレーション内のサービスには、外部の機関が運用するものも含まれています。ユーザ情報は、あらかじめ利用者から提供された情報を蓄積したものであり、利用するサービスに応じてその中から必要なものが送信され、ユーザの認証、サービス利用のために使用されます。利用者は、このユーザ情報の利用についてここに同意するものとします。この同意は、クッキー、キャッシュ等からユーザ情報が送信される場合も含まれます。

サンプルフェデレーション運用部
問い合わせ: exfedadmin@example.com

使用条件に同意します



アクセスしようとしているサービス:
sp-1.example.com

サービスに送信される情報

commonName	yamada
姓	yamada
名	taro
組織名	Example Inc,
部署名	Sales
メールアドレス	yamada@example.com

上記の情報がサービスに送信されます

次回の情報送信確認について:

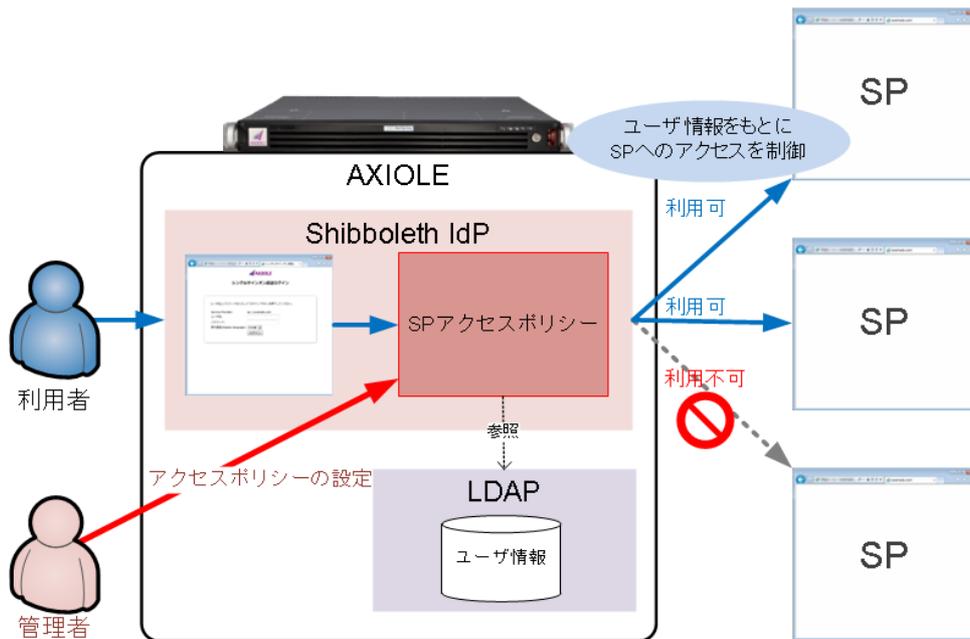
- 次回ログイン時に再確認する
 - 送信先サービス、送信内容にかかわらず、再度この確認画面が表示されます。
- 送信先のサービス、または送信される情報に変更があった場合に再確認する
 - 上記と同じサービスに同じ内容の情報が送信される場合は、この確認画面は表示されず、情報が自動的に送信されます。
- 次回以降確認しない
 - 送信先サービス、送信内容にかかわらず、この確認画面は表示されず、情報が自動的に送信されます。

この設定はログインページのチェックボックスでいつでも取り消すことができます。

拒否する

同意する

●AXIOLE-IdP と FPSP (SP アクセスポリシー) 機能概略図



● SP アクセスポリシー設定画面

SPアクセスポリシー - 追加

SPアクセスポリシーの追加を行います。

"保存"した場合、IdP機能が一時的に停止します。

IdP属性定義IDは、IdP属性定義のAttribute要素のid属性に指定した値を指定してください。
IdP属性定義ID、値、いずれも大文字/小文字を区別します。
IdP属性フィルタポリシー適用前の値をチェックします。また、type="Scoped"のIdP属性はスコープが付与される前の値をチェックします。
IdP属性を指定しない場合、送信するIdP属性値にかかわらず、SPエンティティIDに指定したSPへのアクセスがすべて本条件に適合します。

* SPアクセスポリシー設定名:

* SPエンティティID:

* アクセス: 許可 拒否

* IdP属性条件: 以下のいずれかの条件を満たす 以下のすべての条件を満たす

	IdP属性定義ID	判定方法	値	追加/削除
1	eduPersonAffiliation	一致する	faculty	削除
2	eduPersonAffiliation	一致する	student	削除
3	eduPersonPrincipalName	始まる	Stu	削除
				追加

正規表現簡易リファレンス
 定義済みの属性定義IDはこちら

■ AXIOLE v1.14.1 のその他修正

- その他 IdP 関連 (Java 脆弱性対応含む) および OSS 関連の修正

■ AXIOLE v1.14.1 販売価格

- AXIOLE 500 ユーザ エントリーモデル 90 万円 (メーカー希望価格) より
本体および初年度のライセンス費用ならびに保守費用を含む
- AXIOLE IdP オプション機能 ライセンス料金 60 万円より (エントリーモデル: 一括払いのみ)
 - Shibboleth IdP 機能
 - ・ Shibboleth IdP V3 対応
 - ・ 条件同意機能 (uApprove 相当)
 - ・ SP 簡易ポータルサーバ機能
 - ・ FPSP 機能 (SP アクセスポリシー)
 - ・ Office365 対応 (SAML 連携機能による SSO や ECP 対応)
 - AXIOLE IdP 専用アプライアンス 本体価格: 167 万円 (メーカー希望価格) より
本体および初年度のライセンス費用ならびに保守費用を含む
 - Shibboleth IdP 機能限定 (条件同意/SP 簡易ポータル/FPSP 機能含む)
 - ・ 外部認証データベース利用前提 (AXIOLE アカウントなし)
 - 仮想化アプライアンス版 (VMware vSphere 版) も提供中
※価格はすべて税別

AXIOLE 製品専用サイト: <http://www.axiole.jp/>

以上

【参考 1】 AXIOLE 「IdP オプション」 の主な機能



- 連盟“フェデレーション”内での Web 認証機能と Web アプリケーション間シングルサインオン機能
フェデレーションに参加することで、フェデレーション内の複数の Web アプリケーション (SP) をシングルサインオンで安全に利用できるようになります。
- Shibboleth 向け (GakuNin 推奨) 属性等の定義を標準提供
学術機関向けに、Shibboleth (GakuNin) 環境で利用されることの多い属性等を予め定義しており、職種、利用資格等の属性を AXIOLE の WebUI から編集することが可能になります。必要なメタデータ等のテンプレートが標準提供されます。

- 利用可能な Web アプリケーションの自動更新機能
フェデレーション内の Web アプリケーションが追加された場合、その情報は定期的に AXIOLE 内に取り込まれるため、自動的に新しい Web アプリケーションの利用が可能になります。
- Stored ID (persistent-id) の利用および管理
どこの Web アプリケーションからどのユーザが IdP の認証を受けたかという識別情報を AXIOLE 内部で持続的に保持。IdP 認証時にこの Stored ID を送信することで、Web アプリケーション側においてユーザ単位で前回の情報を参照・自動復元等が可能です。また Stored ID の検索・ダウンロード・削除等の管理機能が提供されます。
- IdP ログ管理
AXIOLE の管理 WebUI で IdP ログの管理が可能。IdP による認証を受けたユーザ、Web アプリケーション、要求・応答の内容の参照や保存・転送等の管理が容易に行えます。
- IdP 機能の冗長化が可能
AXIOLE の冗長構成 (AXIOLE リダンダンシ構成) により IdP の冗長構成も可能に。

【参考 2】AXIOLE の特長・機能、およびオプション機能について

- ・LDAP ベースの認証基盤を 1U のアプライアンス形態で提供
- ・スキーマ属性等 DB 設計が不要
- ・日本語 WebUI ベースの管理システムおよびエンドユーザ向け機能を提供
- ・RADIUS プロトコル (RADIUS プロキシ/eduroam) にも対応
- ・ActiveDirectory (AD) と ID 同期が可能
- ・AXIOLE 2 台による冗長構成が可能
- ・「LDAP スキーマオプション」
汎用的な LDAP 機能を提供 (有償)
- ・「Google Apps 連携オプション」
AXIOLE と Google Apps 間の ID 同期機能を提供 (有償)
- ・「Shibboleth IdP オプション」
AXIOLE と Shibboleth の IdP 連携機能を組込提供 (有償)

【参考 3】ネットスプリングのその他の主な製品

- ・FEREC520 / FEREC720 / Center2 (Web 認証ゲートウェイ製品群) 全モデル生産終了
FEREC 製品専用サイト : <http://www.ferec.jp/>
- ・SmartSignOn for FEREC (スマートサインオン) iPhone/iPad 版および Android 版アプリ
SSO4F 専用サイト : <http://www.SmartSignOn.jp>
- ・SSOcube (汎用型シングルサインオンアプライアンス)
SSOcube 製品専用サイト : <http://www.SSOcube.jp/>

※記載された会社名および製品名などは、該当する各社の商標または登録商標です。

【株式会社ネットスプリング 会社概要】

- ・本社所在地：東京都港区三田 3-12-16 山光ビル 2F
- ・代表者：代表取締役社長 兼 最高経営責任者 西武 進 (にしたけすすむ)
- ・設立：2000 年 3 月
- ・資本金：8,075 万円
- ・事業内容：ネットワーク関連製品の企画・開発・販売
コンピュータネットワークに関するコンサルティング
- ・URL：<http://www.netspring.co.jp/>

※記載された会社名および製品名などは、該当する各社の商標または登録商標です。

一般読者からのお問い合わせ先：
株式会社ネットスプリング マーケティング部
TEL : 03-5440-7337 E-mail : info@netspring.co.jp

報道関係のお問い合わせ先：
株式会社ネットスプリング広報事務局 アルサープ内 担当：河端、川口
TEL : 03-4405-8773 E-mail : netspring-pr@alsarpp.co.jp