

**Axies2025**

# 認証基盤OSS導入事例と運用について

2025/12/02

**サイオステクノロジー株式会社**



# 本日の説明内容

- これまでのOSSとの関わりを事例を通してご説明します
  - OSS導入事例紹介
  - Shibbolethについて
  - Shibbolethを通して見えるOSS運用の課題とその対策

## ■ 氏名

- 田中 元道

## ■ 所属

- サイオステクノロジー株式会社  
エンジニア入社

## ■ 仕事の割合

- 文教90%：企業10%

---

2008 年	Google Apps導入案件
-----------	-----------------

---

2009 年	統合ID管理システム構築
-----------	--------------

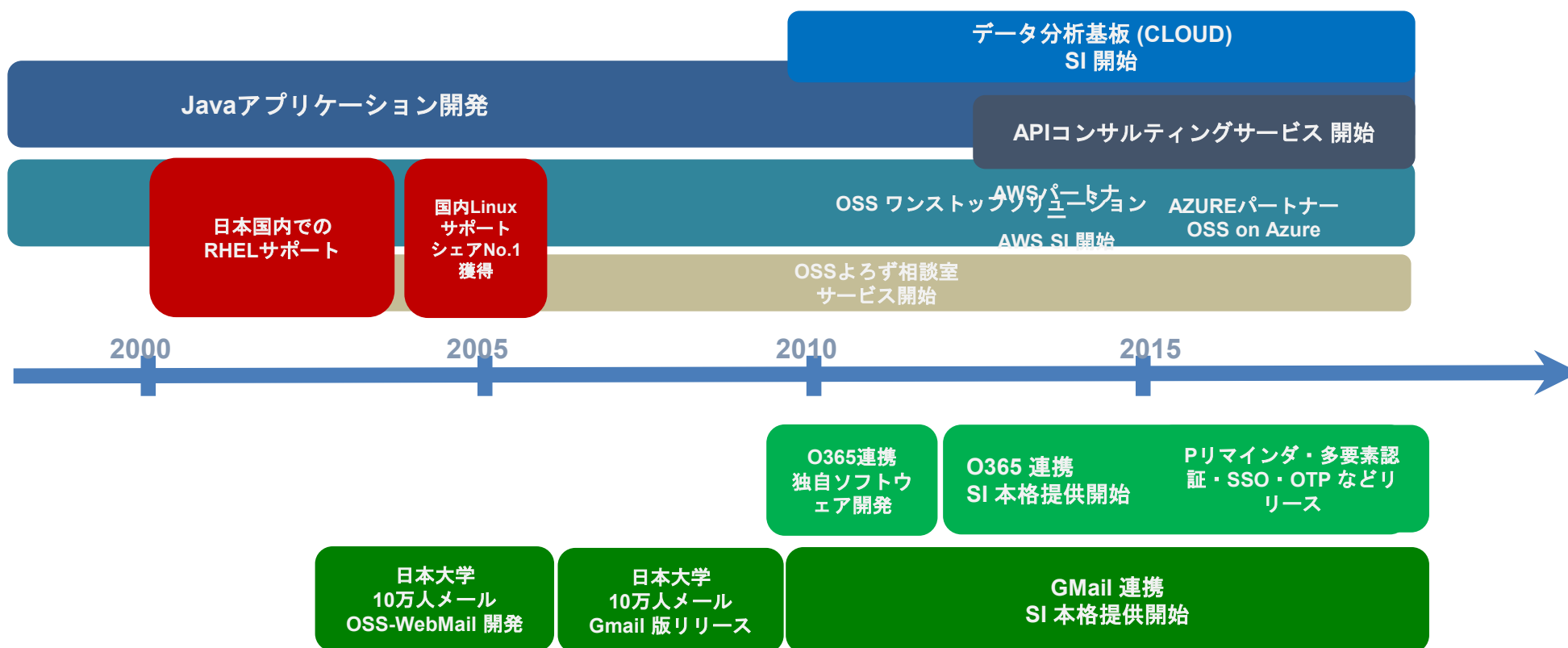
---

2013 年	Shibboleth構築案件
	Office 365案件

---

# OSSでのインテグレーション事業の歴史 SIOS

OSS の経験は20年以上、クラウド技術も多数実績



クラウドメールの導入・ID 連携（統合認証やSSOなど）の経験は15年以上

# 事例：メール中継（Postfix + OpenLDAP）SIOS

## Postfix

メール受信と複数MTAへの並列配送

## OpenLDAP

ユーザ情報、配送ポリシーの一元管理

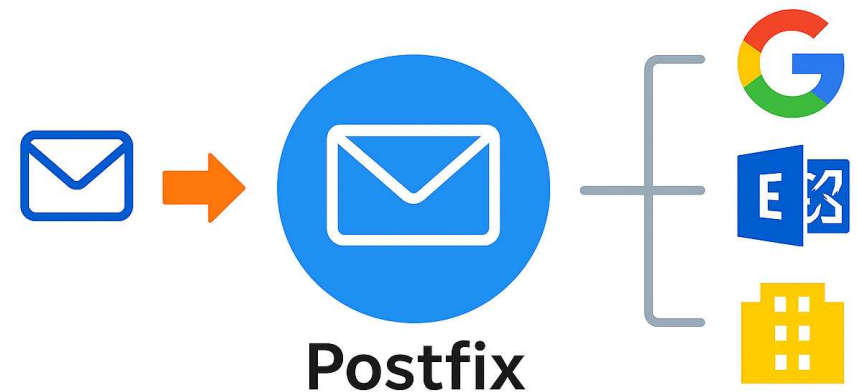
## 3重配送

GoogleWorkspace、ExchangeOnline、  
オンプレメールサーバに同時配送

## 利点

冗長性、ユーザ毎に任意のメールを利用

### Postfixによるマルチ配送構成



# 事例：LDAP移行（商用からOpenLDAPへ）

## コスト削減

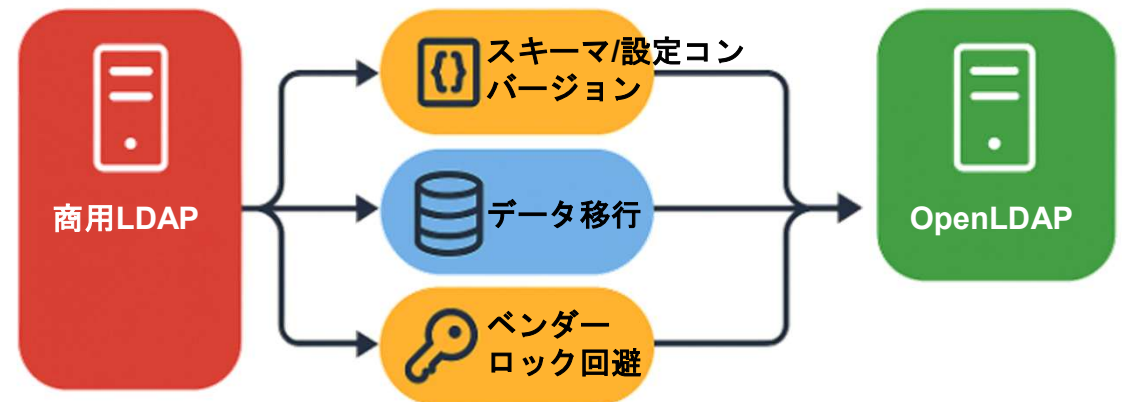
エントリ数毎のライセンス費用とサポートコストを抑えて

## 柔軟性とカスタマイズ

スキーマ設定の自由度、特定要件に合わせた設定移行

## 長期的な運用

特定ベンダーによるロックインを回避



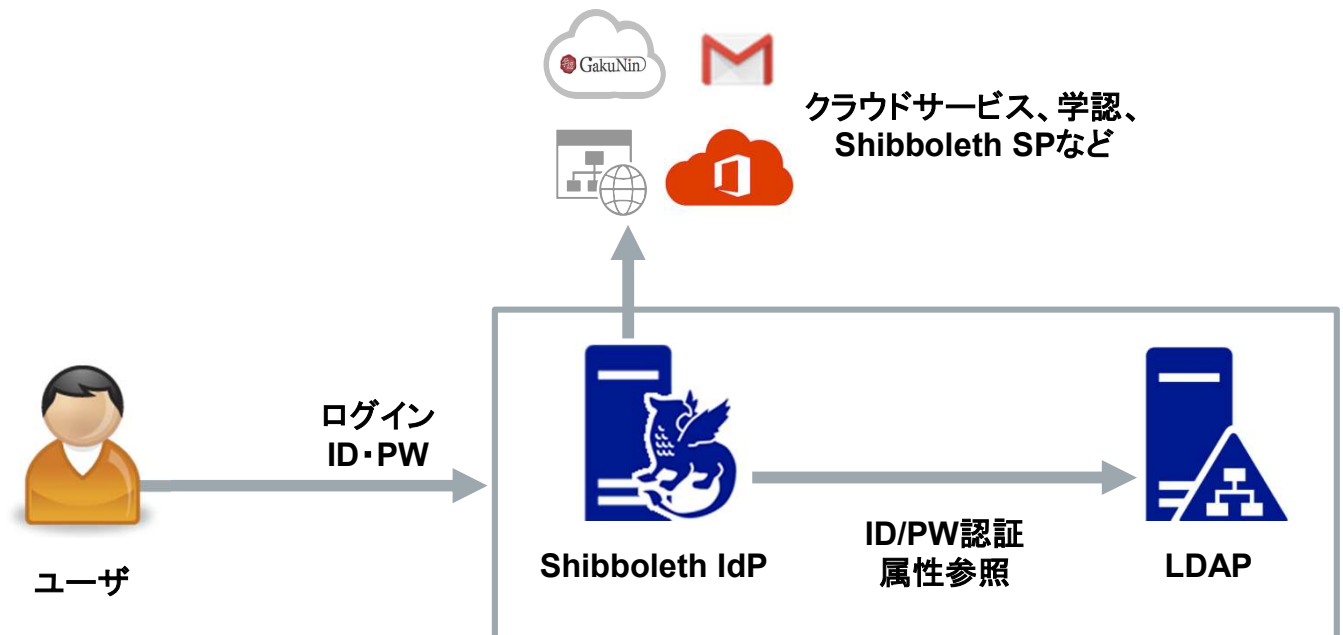
# 事例：Shibboleth

## SSO

一度の認証で複数システムへログイン可能にする。Google、M365、学認SP、学内WEBサービスなども連携可

## Shibboleth

SSOを実現するOSS



# 事例：Shibboleth + OTP認証



## SSO

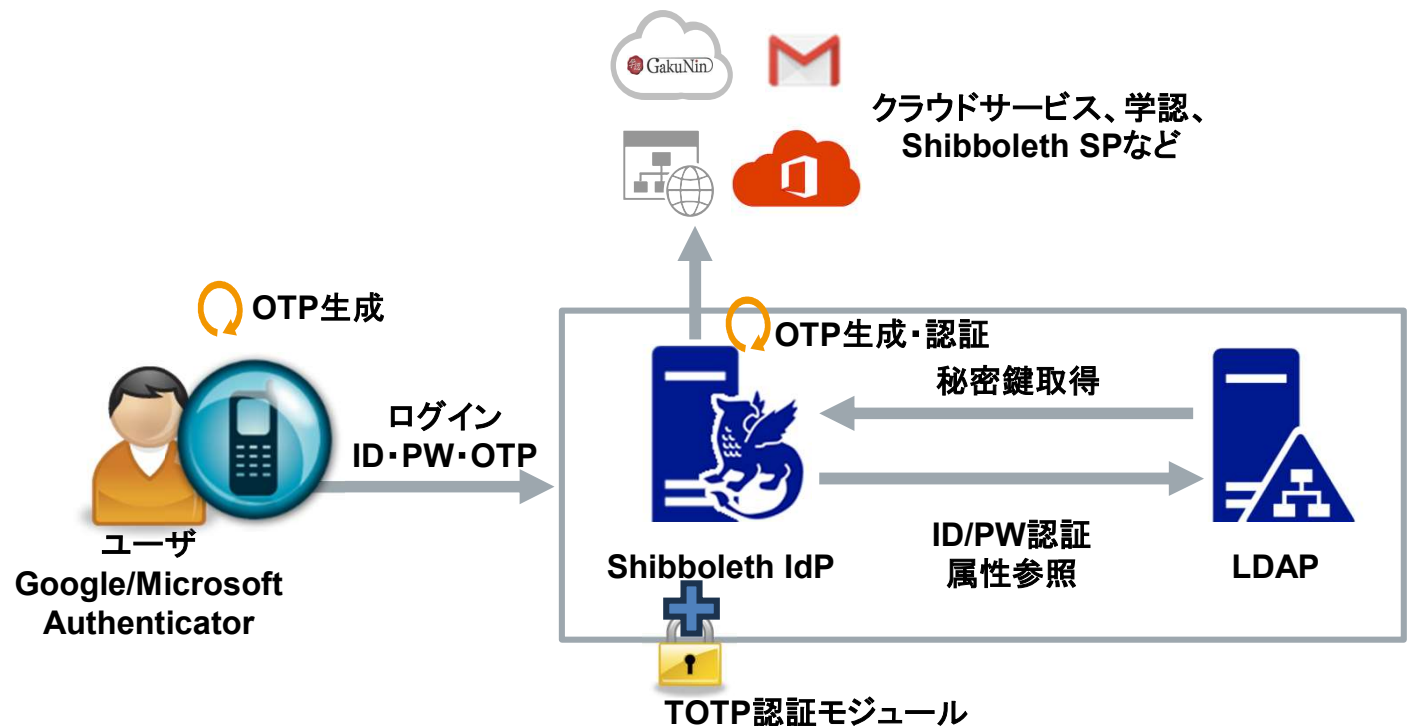
一度の認証で複数システムへログイン可能にする。Google、M365、学認SP、学内WEBサービスなども連携可

## Shibboleth

SSOを実現するOSS

## TOPT認証モジュール

ID/PWに加えてワンタイムパスワードで認証することでセキュリティ強化をするOSS





# SSOとShibboleth

項目	SSOとは	Shibboleth	学認
概要	1回の認証で複数サービスにアクセス可能。利便性向上（ログイン回数削減）	SAMLを利用した認証・属性連携のOSS	学術認証フェデレーション
目的	認証情報を一元管理。セキュリティ強化	IdPとSP間で連携通信の暗号化、署名検証で認証情報の漏洩、改ざんを防止	大学・研究機関間で認証連携
役割	1回の認証で複数のシステムと認証情報、属性情報の共有	SSOを実現する仕組み	Shibbolethで大学・研究機関間で認証情報共有、学術サービス利用促進
標準化	標準プロトコルでSAML/OIDC など	SAML標準に準拠	国内外の学術サービスと連携

# Shibbolethを通して見えるOSS運用の課題os

## バージョンアップしていますか？

セキュリティ対応や機能改善のため頻繁なアップデートが必要

## Shibbolethでの現実的な課題

依存関係の複雑さ：Java、Jetty、ライブラリなど複数コンポーネントの整合性確認が必須

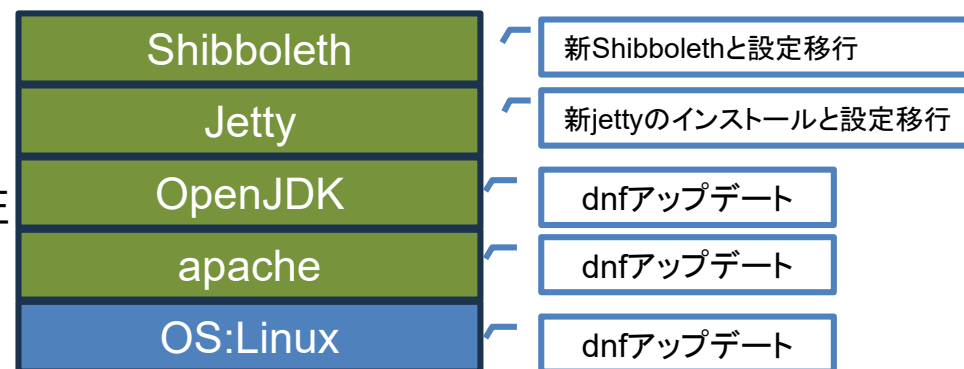
設定ファイルの互換性：バージョン間で仕様変更があり、移行時に手作業が発生

テスト工数の増大：認証基盤のため影響範囲が広く、検証に時間がかかる

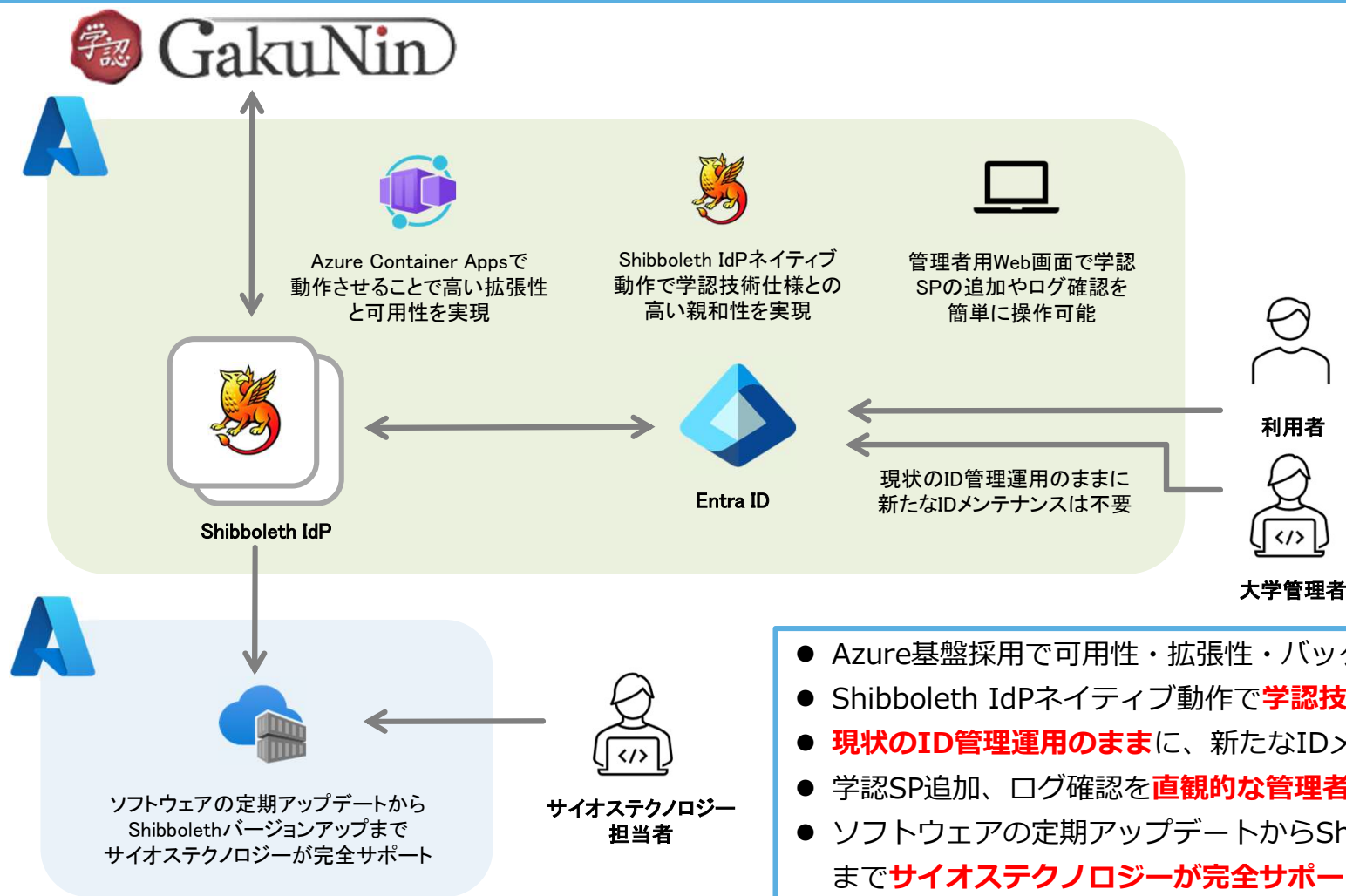
## 運用への影響

アップデート遅延によるセキュリティリスク

長期的にはサポート切れによる重大障害の可能性



# SIOS Shibboleth IdPサービス SIOS



# Shibbolethを通して見えるOSS運用の課題os

## 管理者の負担軽減できていますか？

運用・障害対応は属人化しやすい

### 軽減できている

- ✓ IdP/SP連携の標準化により初期構築は容易化
- ✓ コミュニティ情報やドキュメントの充実

### 依然残る負担

- サーバ証明書更新（証明書最大有効期間の短縮対応）
- 連携するWEBサービスの追加
- 問い合わせからのログ解析

# 証明書自動更新ソリューション



- 証明書更新サーバを構築（OSSのCertbotを使用）
- WEBで更新状況を確認できるダッシュボードを提供

リリース計画中

認証局（ACME）

② 証明書取得/  
ドメイン検証

（学外）

（学内）



証明書更新サーバ

① 証明書期限チェック  
③ 証明書更新

④ 証明書配置  
⑤ サービス再起動



Webサーバ



リバースプロキシ

...



LDAPサーバ



メールサーバ

...

# Shibboleth Management Portal



## Shibboleth Management Portalは SP管理・Metadataファイル管理を行えるWebアプリケーションです

### SP管理

- SP の新規登録・変更・削除
- SP の一覧表示

### Metadataファイル管理

- Metadata ファイルの新規登録・変更・削除
- Metadata ファイルの一覧表示

The screenshot shows the 'SP 管理' (SP Management) page. The left sidebar has a dark theme with a home icon and three menu items: 'HOME', 'SP 管理' (selected), and 'Metadata 管理'. The main content area has a dark header with the SIOS logo, 'Shibboleth Management Portal', and a user dropdown 'user001'. Below the header is a breadcrumb 'Home / SP 管理'. The main title is 'SP 管理'. There is a search bar with a magnifying glass icon, a blue button 'SP 新規登録', and a blue button 'デプロイ画面へ'. Below this is a table with three columns: 'Id', 'Entity ID', and '送信属性'. The table contains six rows of data.

Id	Entity ID	送信属性
<a href="#">example1</a>	<a href="https://sp.example1.org/shibboleth">https://sp.example1.org/shibboleth</a>	uid
<a href="#">example2</a>	<a href="https://sp.example2.org/shibboleth">https://sp.example2.org/shibboleth</a>	uid
<a href="#">spuserapp</a>	<a href="https://spuserapp.example.org/shibboleth">https://spuserapp.example.org/shibboleth</a>	uid, mail
<a href="#">ssms</a>	<a href="https://ssms.test.org/shibboleth">https://ssms.test.org/shibboleth</a>	uid
<a href="#">sp1</a>	<a href="https://sp.example.org/shibboleth">https://sp.example.org/shibboleth</a>	uid, mail

The screenshot shows the 'Metadata 管理' (Metadata Management) page. The left sidebar is the same as the previous screenshot. The main content area has a dark header with the SIOS logo, 'Shibboleth Management Portal', and a user dropdown 'user001'. Below the header is a breadcrumb 'Home / Metadata 管理'. The main title is 'Metadata 管理'. There is a search bar with a magnifying glass icon, a blue button 'Metadata 新規登録', and a blue button 'デプロイ画面へ'. Below this is a table with one column: 'Entity ID'. The table contains three rows of data.

Entity ID
<a href="https://ssms.test.org/shibboleth">https://ssms.test.org/shibboleth</a>
<a href="https://spuserapp.example.org/shibboleth">https://spuserapp.example.org/shibboleth</a>
<a href="https://sp.example.org/shibboleth">https://sp.example.org/shibboleth</a>

# Shibbolethを通して見えるOSS運用の課題os

脆弱性回避していますか？

運用・障害対応は属人化しやすい

**軽減できている**

- ✓ 脆弱性情報の監視（メール、リリースノートでの確認）

**依然残る負担**

- 脆弱性が自システムに該当するか

# サイオステクノロジー / OSSよろず相談室<sub>IOS</sub>

## OSSサポートの歴史



### 専門性

OSSの  
プロフェッ  
ショナル

### 実績

国内Linuxサ  
ポートNo1

### 技術力

OSS 150種類  
の対応力

**OSSよろず相談室**：オープンソースソフトウェアの専門家がお客様の課題に対して、課題解決のお手伝いをするサービスです。

150種類のOSSに対応

150

台数契約ではなく  
エンジニアの調査時間で契約



選べるメニューとカスタマイズ



エンジニア1名を雇用するよりも  
高い費用対効果



メニュー		Light	Basic	Standard	Premium
		限定的な利用	基本サービス	積極的なOSS利用を支援	カスタムメニュー
サポートOSS数		2※	5	無制限	カスタム
対象サーバー数		1	無制限	無制限	
精算	チケット制	チケット5回	—	—	
	時間制	—	月10時間 年60時間	月30時間 年240時間	
Q&Aサービス		○	○	○	
ソースコード解析サービス		—	—	○	カスタム
Errata情報レポートサービス		—	Option	Option	



# サイオステクノロジー / OSSよろず相談室・新サービスIOS

## OSSの導入・運用をもっと安心に サイオスOSS検証サービス

お客様の課題やご要望に応じて **OSS の 技術検証** を実施します結果は  
レポートや説明会ご提供します

### 検証内容

- アップグレード検証
- マイグレーション検証
- OSアップグレードに伴うOSS動作検証



### こんな方にオススメ

- OSSを自社の基幹システムに段階的に導入したい
- OSSを活用したシステムのバージョンアップを進めたい
- 外部の専門家による技術的な裏付けが欲しい

## OSSの導入・運用をもっと安心に サイオス脆弱性レポートサービス

対象OSSの **脆弱性レポート** を月1回ご提供します

- 公式リリースノートをもとに  
最新の脆弱性を定期的にチェック
- 弊社の専門知見から脆弱性の対処方法をご提案

### こんな方にオススメ

- 更新が頻繁な脆弱性情報の収集に時間がかかる
- 利用中のOSSの脆弱性情報を定期的に把握したい



### 対象OSS

コミュニティ版/RHEL(AlmaLinux/Rocky Linux)同梱版  
Apache / Tomcat / PostgreSQL / MariaDB / Zabbix / MySQL / squid /  
samba / nginx / OpenSSL / bind / FreeRADIUS / OpenLDAP / OpenSSH / Postfix

# サイオステクノロジー / SCANOSS SIOS

## SCANOSS はソフトウェアに潜むライセンスを検出します

AI が生成したコードや他社から納入されたコードに OSS などが混入した結果意図せずライセンス違反をしている可能性があります

SCANOSS はソフトウェアに潜むライセンスや利用している OSS を報告します



サイオステクノロジーは、OSS サポートの20年以上の実績と経験に基づくノウハウを活かし、OSS 管理の効率化とコンプライアンス強化を支援します。

## SBOM 導入のメリット

SBOM (Software Bill of Materials) は、ソフトウェアを構成するライブラリやコンポーネントの一覧を記録した「部品表」です。含まれるコンポーネントがどのようなライセンスで提供されているかを明確にし、管理を容易にします。

### ライセンス管理

ライセンスの可視化による  
コンプライアンスの向上



### 脆弱性管理

ソフトウェアに含まれる既知脆弱性の可視化と新規脆弱性時の対応迅速化



### 生産性向上



OSS が含まれるシステムの SBOM を手動管理するには課題が多く、更新作業のコストも大きくなります

SCANOSS を活用でソフトウェアコンポーネントの特定から SBOM の作成・更新までを自動化し、管理の手間を大幅に削減できます

## SCANOSS は4つのデータセットからコードを見える化します

### ・ライセンスデータセット



コードに含まれるライセンスを検出

著作権表示、帰属などの実用的な情報を提供します  
全てを明らかにすることで、ライセンス義務の遵守が可能となります

### ・セキュリティデータセット



コードに含まれる脆弱性を検出

National Vulnerability Database (NVD)、OSV、GitHub Advisories などの信頼できるソースから対象のコードに含まれる脆弱性を表示します

### ・暗号化データセット



コードが利用する暗号化方式を検出

オープンソースおよびプロプライエタリコードの暗号アルゴリズムの一覧表を提供します

### ・地理由来データセット



OSS の作成者の地理情報を取得

オープンソースソフトウェアの開発者の地理的な出所を表示します

