

OpenIDMの調査

2019.02.06作成 藤澤貴智

OpenIDMの主な機能

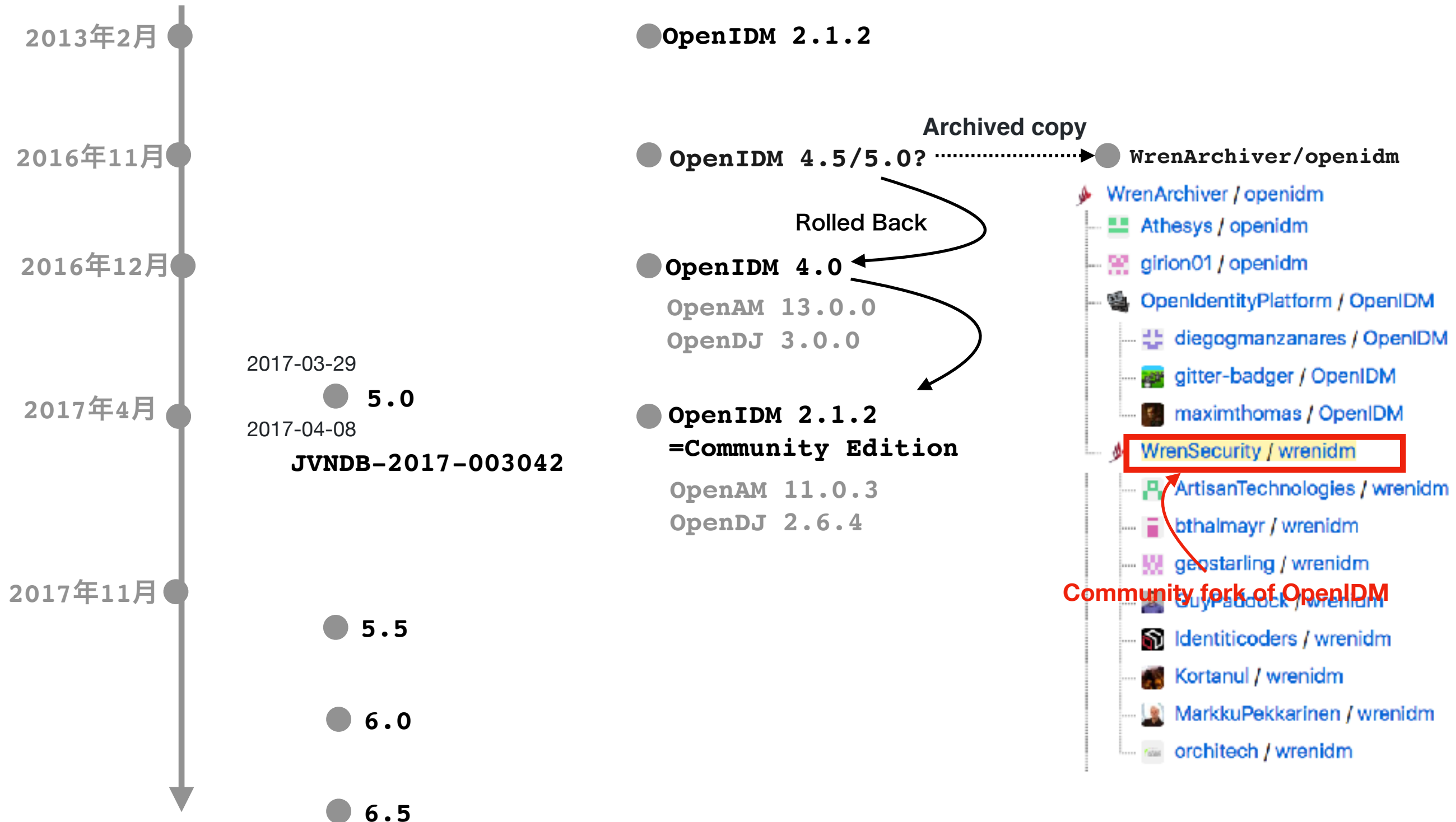
- オンプレミス、クラウド、そのハイブリッド環境に展開できるレスポンシブフレームワーク
- データリポジトリ、ネットワークアプリケーション、およびユーザーデータストアを管理
- ForgeRock Open Connector Frameworkと柔軟なワークフローエンジンでユーザー関係をプロビジョニング
- ユーザー登録およびプロビジョニングの管理

OpenIDM関連リリース

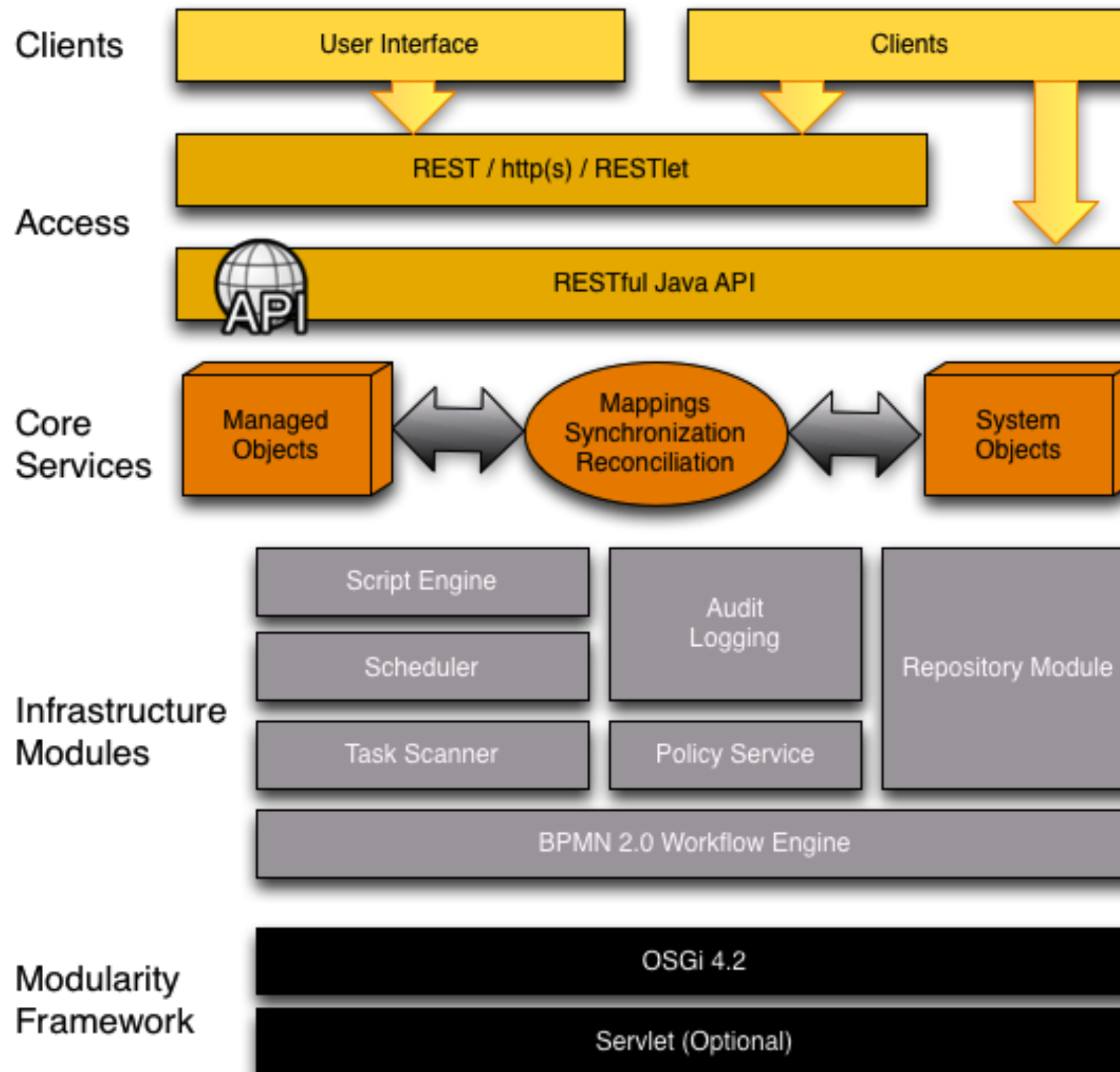
ForgeRock/
Identity Management

ForgeRock/
Public repository








GitHub



OpenIDM Community Edition



開発項目の対応

開発項目	OpenIDM Community Edition	
(1) ユーザアカウント統合管理システムのユーザ登録画面およびユーザ管理 DB の作成		
登録画面(ユーザ登録 Web UI)		
ユーザ管理 DB		
(2) データ登録系システム((ii)D-way)へのデータ登録スクリプトの作成		
OpenDJ ディレクトリサービスに登録するデータを生成するスクリプト		
メール承認機能		?
OpenDJとの自動的な連動		
(3) スパコン LDAP へのデータ登録スクリプトの作成		
LDAP ディレクトリサービスに登録するデータを生成するスクリプトを作成		
LDAP へのデータ登録スクリプトはスパコン SE が手動		

OpenIDM利用判断のポイント

- 本開発の仕様はおおよそ満たしている
- 製品版は高い（らしい）／OSSは筋が悪い
- OSSカスタマイズへの対応（技術力、コスト）
- SCIM（System for Cross-domain Identity Management）-like仕様

参考

ForgeRock Open Source Projects

Welcome to the ForgeRock open source repositories for our identity and access management projects. Here you can download, modify, and contribute code to these projects.

ForgeRock Commercial Engagements

In addition to these open source projects, ForgeRock offers a commercial subscription offering with the most advanced identity solutions including with comprehensive support, maintenance, and training offerings, ideally suited for organizations looking to implement mission critical identity solutions. [Learn more here.](#)

[ForgeRock.com](#)



The OpenAM project is an access management solution that includes Authentication, SSO, Authorization, Federation, Entitlements and Web Services Security.

[Project Home Page](#)

[On GitHub](#)



OpenIDM is an identity management system that provides simple management and synchronization of identity

[Project Home Page](#)

[On GitHub](#)



The OpenDJ project is a REST & LDAP Directory, including a secure directory server, built-in data replication, client tools, and an LDAP SDK.

[Project Home Page](#)

[On GitHub](#)



The OpenIG project is an identity gateway with high-performance reverse proxy with specialized session management and credential replay functionality.

[Project Home Page](#)

[On GitHub](#)

<https://forgerock.github.io>

Welcome to Open Identity Platform Community

Open-source community organization, hosted on [GitHub](#)

We develop and support Access Management, Identity Management, User-Managed Access, Directory Services and Identity Gateway, designed and built as a single, unified platform

[Join Us on GitHub](#)

Open Identity Platform Ecosystem:



OpenAM

Open Access Management (OpenAM) is an access management solution that includes Authentication, SSO, Authorization, Federation, Entitlements and Web Services Security.

OpenDJ

OpenDJ is an LDAPv3 compliant directory service, which has been developed for the Java platform, provides a high performance, highly available, and secure store for identities, that managed by your organization. Its easy installation process, combined with the power of the Java platform makes OpenDJ the simplest, fastest directory to deploy and manage.

OpenIG

Open Identity Gateway (OpenIG) is a high-performance reverse proxy server with specialized session management and credential replay functionality.

WHY IS A FORK NECESSARY?

Simply put, FORGEROCK no longer works with the community to develop software. Consider the evidence:



Trunk access closed off

November 2016

Without prior notice, all of the "trunk" GIT repos on the FORGEROCK Stash server were switched to requiring commercial subscriptions to access.

No official public statement was provided after the fact about this change.

Public repositories rolled back

December 2016

After having closed off the main trunk, FORGEROCK moved forward by rolling all of the source code copies they had under the ForgeRock GitHub account to code from the last stable release, effectively erasing 8 to 12 months of code from public history.



Maven access closed off

March 2017

Once again proceeding without any prior notice to the community, FORGEROCK switched the ForgeRock Maven repository to deny access to anyone other than paid commercial subscribers.

The Maven repository previously hosted all of the artifacts required to build open-source copies of OpenAM, OpenDJ, and OpenIDM. Without Maven access, users who did not already have a local copy of these artifacts could no longer build these projects.

Community site replaced with static page and JIRA write access discontinued

April 2017

Previously, the page at ForgeRock.org provided a wealth of information about where to find each project, how to get involved in the community, and how to contribute patches and bug reports back. Now, the page is [merely a single static page](#) designed to advertise the new platform, and then point to old copies of source code on GitHub.

In addition, users who could previously log-in to the FORGEROCK JIRA issue tracker ("Bugster") can no longer log-in without a paid subscription, further shutting-out community members from contributing bug reports and commenting on tickets.



Public repositories rolled back even further

April 2017

Initially, in December 2016, the GitHub repository for OpenAM was rolled back to code from version 13; OpenDJ to version 3.0; and OpenIDM version 4.

Now, the copies that FORGEROCK links to from the static ForgeRock.org page are even older – OpenAM 11.0.3, OpenDJ 2.6.4, and OpenIDM 2.1.2.



JVNDB-2017-003042

OpenIDM におけるクロスサイトスクリプティングの脆弱性

概要

OpenIDM には、クロスサイトスクリプティングの脆弱性が存在します。

CVSS による深刻度 (CVSS とは?)

CVSS v3 による深刻度

基本値: **6.1** (警告) [NVD値]

- 攻撃元区分: ネットワーク
- 攻撃条件の複雑さ: 低
- 攻撃に必要な特権レベル: 不要
- 利用者の関与: 要
- 影響の想定範囲: 変更あり
- 機密性への影響(C): 低
- 完全性への影響(I): 低
- 可用性への影響(A): なし

CVSS v2 による深刻度

基本値: **4.3** (警告) [NVD値]

- 攻撃元区分: ネットワーク
- 攻撃条件の複雑さ: 中
- 攻撃前の認証要否: 不要
- 機密性への影響(C): なし
- 完全性への影響(I): 部分的
- 可用性への影響(A): なし

影響を受けるシステム

ForgeRock

- OpenIDM 4.0.0 まで
- OpenIDM 4.5.0

想定される影響

JVN

HOME



JVNとは



脆弱性レポートの読み方



脆弱性レポート一覧



VN-JP

VN-JP (連絡不能)

VN-VU

TA

TRnotes



JVN iPedia

脆弱性対策情報データベース



検索

JVN iPediaとは

使い方

MyJVN

JVNJS/RSS



ベンダ情報一覧



連絡不能開発者一覧



脆弱性情報の届出



お問合せ先



起動&停止

```
[水  2 06 05:55] tf@~/idm/openidm
```

```
%./startup.sh
```

```
Executing ./startup.sh...
```

```
Using OPENIDM_HOME:    /Users/tf/idm/openidm
```

```
Using OPENIDM_OPTS:    -Xmx1024m
```

```
Using LOGGING_CONFIG: -Djava.util.logging.config.file=/Users/tf/idm/openidm/conf/logging.properties
```

```
Using boot properties at /Users/tf/idm/openidm/conf/boot/boot.properties
```

```
OpenIDM version "2.1.2" (revision: c923d153)
```

```
-> OpenIDM ready
```

```
[水  2 06 09:27] tf@~/project/idm/openidm
```

```
%./shutdown.sh
```

```
./shutdown.sh
```

```
Stopping OpenIDM (75907)
```

Common Development and Distribution License (CDDL)

- サン・マイクロシステムズが Mozilla Public License(MPL) version 1.1 をベースとして策定したフリーソフトウェア向けライセンス規定
- CDDLでライセンスされたソフトウェアは、使用料が無料であり、無保証で非独占的な利用が可能
- 対象ソフトウェアの品質、及び性能に関するリスクは、すべて利用者が負う
- 頒布にあたり、ソフトウェアを実行可能なコード形式で提供する場合は、CDDLに従ってソースコードの提供が義務づけられている
- ソフトウェアを修正した場合もCDDLが適用され、自分が修正したコードのコントリビュータであることを明記しなくてはならない
- 全く別のライセンスのコードを組み合わせることで拡大配布物を作成し、それを単一のライセンスとして頒布することも可能