

# OSSTech OpenAM 11.0.0

## リリースノート



OSSTech

OSSTech(株)

更新日: 2024年5月28日

## 目次

<b>1. はじめに</b>	<b>1</b>
<b>2. osstech-openam11-11.0.0-142 の修正内容</b>	<b>2</b>
2.1 11.0.1／12.0.0 以降に統合される修正(バックポート).....	2
2.2 OSSTech 独自の修正.....	2
2.2.1 機能追加.....	2
2.2.2 設定関連の変更.....	2
2.2.3 問題の修正.....	2
<b>3. コミュニティ版との差異</b>	<b>3</b>
3.1 11.0.1／12.0.0 以降に統合される修正(バックポート).....	3
3.2 OSSTech 独自の修正.....	10
3.2.1 機能追加.....	10
3.2.2 設定関連の変更.....	10
3.2.3 問題の修正.....	11
<b>4. osstech-tomcat パッケージの更新</b>	<b>14</b>
4.1 systemd 対応(RHEL7).....	14
<b>5. 制限事項</b>	<b>15</b>
<b>6. パッケージ更新履歴</b>	<b>16</b>

## 1. はじめに

本ドキュメントは、OSSTech 提供の OpenAM の修正内容について記載しています。本ドキュメントの対象となる OpenAM パッケージは、osstech-openam11-11.0.0-142 です。

このパッケージは ForgeRock コミュニティ版 OpenAM 11.0.0 のソースコードをベースとしています。コミュニティ版のリリースノートについては次のページより確認してください。

<http://docs.forgerock.org/en/openam/11.0.0/release-notes/>

また、ご利用の OpenAM パッケージのバージョンの確認は次のコマンドで確認することができます。

```
$ rpm -qa | grep osstech-openam11
osstech-openam11-11.0.0-142.el7.noarch
```

## 2. osstech-openam11-11.0.0-142 の修正内容

OSSTech 提供の OpenAM 11.0.0-142 では以下の修正を行いました。

### 2.1 11.0.1 / 12.0.0 以降に統合される修正(バックポート)

なし

### 2.2 OSSTech 独自の修正

#### || 2.2.1 機能追加

なし

#### || 2.2.2 設定関連の変更

なし

#### || 2.2.3 問題の修正

- IdP で SAML2 フェイルオーバーが動作しない問題を修正

## 3. コミュニティ版との差異

OSSTech 提供の OpenAM 11.0.0 は ForgeRock コミュニティ版 OpenAM11.0.0 と以下の差異があります。

### 3.1 11.0.1 / 12.0.0 以降に統合される修正(バックポート)

- IdRepo デバッグログに RetryTask のエラーが出つづける問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-688>
- Fedlet の JSP のコンパイルエラーを修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3217>
- シングルログアウト時に RelayState の検証に失敗する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3437>
- データストア認証モジュールを利用する場合にオンメモリのアカウントロックを利用できない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3456>
- デスクトップ SSO の認証レベルが設定されない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3490>
- OpenAM に同梱されている OpenDJ SDK の問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENDJ-1247>
  - <https://bugster.forgerock.org/jira/browse/OPENDJ-1258>
- OpenAM が SAML SP として動作する場合にレルムの設定を正しく扱わない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3698>
- 設定ディレクトリからバージョン情報を取得できない場合に NullPointerException が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3489>
- ポリシー判定処理がリソースの URL からスラッシュを外してしまう問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3509>

- ポリシー判定処理がワイルドカードの判定を正しく処理しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3638>
- デバッグレベルがメッセージである場合にアダプティブリスク認証を利用すると失敗する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3607>
- ssoadm コマンドの create-metadata-templ サブコマンドで NullPointerException が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3172>
- OpenAM の依存ライブラリである Restlet のアップデート
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3694>
- OpenAM を冗長構成としている場合に ClientSDK や ssoadm が動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3528>
- OAuth 認証が Cookie 付加時にサーバー設定の HttpOnly と Secure の設定を反映しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3227>
- エージェントグループをサブレルムで作成できない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3269>
- OAuth Client を設定しているとアップグレードに失敗する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3422>
- OpenID Connect 1.0 クライアントの動的登録機能が動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2865>
- OpenID Connect の”prompt”パラメータが動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3318>
- OAuth 2.0 の同意の保存が動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3315>
- OAuth 2.0 のクライアント登録ページの表示の問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3205>

- OpenID Connect のエンドポイントが返却する id\_token\_signing\_alg\_values\_supported 名のスペルミスを修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3534>
- OAuth2.0 クライアントクレデンシャルで作成したトークンの読み込みで NullPointerException が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3506>
- OAuth2.0 の読み込み・削除操作で管理者トークンと読み込み対象トークンのレلمムが一致しない場合に NullPointerException が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3520>
- OpenID Connect Session Management の署名検証処理の修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3620>
- OAuth 2.0 の同意画面の Description をロケール毎に表示できない問題の修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3678>
- クッキーエンコードを有効にしている場合に OAuth 認証が動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4094>
- OpenAM を冗長構成としている場合に OpenAM が発行する Cookie に HttpOnly が付加されない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3740>
- データストア通知の設定が有効である場合に権限情報の書き込みが競合してしまう問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3226>
- データストアに対して不正なサーチが発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3742>
- アダプティブリスク認証が Cookie 付加時にサーバー設定の HttpOnly と Secure の設定を反映しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3632>
- OpenDJ SDK のアップデートにより dsconfig コマンドの結果が正しく表示されない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3465>
- sAMAccountName をネーミング属性に設定した場合に Active Directory データストアが動

作しない問題を修正

- <https://bugster.forgerock.org/jira/browse/OPENAM-3428>
- 組織の DN にルートサフィックスを設定した場合に Active Directory データストアが動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3385>
- LDAP 認証にオペレーションタイムアウトの設定機能がない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3353>
- データストアのエラー出力強化
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3113>
- gotoOnFail URL の検証処理の追加
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2760>
- リモートセッション関連の処理で発生するメモリリークの問題の修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2145>
- コネクションプール内で名前解決後の IP アドレスをキャッシュしてしまい、再接続時に名前解決を行わない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3865>
- OpenAM のアップグレード時にサーバーのデフォルト設定の一部が削除されてしまう問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3947>
- 保護対象の URL が複数の参照ポリシーに合致する場合にポリシー判定処理がハングアップする問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2460>
- SAML リクエストに isPassive 属性が付与されていない場合に NullPointerException が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3542>
- Secure Attribute Exchange (SAE) 用エンドポイントの XSS 脆弱性の修正
- REST API へ JSON リクエストを送る度に RestSecurity インスタンスが作成される問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4044>



- SAML アサーションの NameID に SPNameQualifier 属性が無い場合に SAML エラーとなる問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3573>
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3707>
- DelegationPolicyImpl のキャッシュ更新処理がスレッドセーフではない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4176>
- SAML2 フェイルオーバーが動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4195>
  - <https://bugster.forgerock.org/jira/browse/OPENAM-5614>
- セキュリティ脆弱性の修正(AM20150408-1)
  - <http://www.osstech.co.jp/support/AM20150408-1>
- FRREST のトークン管理エンドポイントで取得できるリフレッシュトークンの tokenName が access\_token である問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3646>
- セッションアップグレードの場合に HOTP 認証が動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4304>
- HOTP 認証で認証画面で OTP コードの要求ボタンを押下すると OTP が 2 回送信される問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2464>
- セキュリティ脆弱性の修正(AM20150527-1)
  - <http://www.osstech.co.jp/support/AM20150527-1>
- LDAP 認証モジュール内の検索で複数のユーザーが見つかった場合に NullPointerException が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-6286>
- データストアの設定がキャッシュとして残る問題の修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-6399>
- データストア設定の削除に連動して参照ポリシーが削除されてしまう問題の修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2532>

- OpenAM のログローテーション機能が実際のログサイズではなく OpenAM が出力したログサイズで実行される問題の修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4072>
- セキュリティ脆弱性の修正(AM20150915-1)
  - <http://www.osstech.co.jp/support/AM20150915-1>
- セキュリティ脆弱性の修正(AM20151027-1)
  - <http://www.osstech.co.jp/support/AM20151027-1>
- セキュリティ脆弱性の修正(AM20151207-1)
  - <http://www.osstech.co.jp/support/AM20151207-1>
- SunQueryParamsString が二重にエンコードされる問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2940>
- SunQueryParamsString のデコードで例外が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-5214>
- CDSSO で SunQueryParamsString がエンコードされない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-8154>
- セキュリティ脆弱性の修正(AM20160308-1)
  - <http://www.osstech.co.jp/support/AM20160308-1>
- セキュリティ脆弱性の修正(AM20160726-1)
  - <http://www.osstech.co.jp/support/am20160726-1>
- Adaptive Risk 認証におけるクッキー値のエンコードおよびデコードに関する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3999>
- REST API 利用時にコールバックが正常に渡らない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2270>
- 認証中に NPE が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3784>
- Java-1.7.0-openjdk 非互換問題の修正(AM20160729-1/AM20160729-2)
  - <http://www.osstech.co.jp/support/am20160729-1>

- <http://www.osstech.co.jp/support/am20160729-2>
- <https://bugster.forgerock.org/jira/browse/OPENDJ-2247>
- セキュリティ脆弱性の修正(AM20160907-1)
  - <http://www.osstech.co.jp/support/am20160907-1>
- セキュリティ脆弱性の修正(AM20161109-1)
  - <http://www.osstech.co.jp/support/am20161109-1>
- CTS の削除スレッドが例外により停止してしまう問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3283>
- 認証レベルにレルム名が含まれていた場合に SAML の認証処理で NumberFormatException が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-6776>
- サーバー間死活監視にコネクションタイムアウト・リードタイムアウトを設定する修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2920>
- サーバー間死活監視のコネクションが適切にクローズされていない問題の修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-5040>
- Java8 を利用した場合に証明書認証で NoClassDefFoundError が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-141>
- Java8 でユニットテストが失敗する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3766>
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4511>
- ログインページに入力したユーザー名/パスワードを認証ポストプロセスに渡すしくみを追加
  - <https://bugster.forgerock.org/jira/browse/OPENAM-5921>
- サービス運用妨害 (DoS) の脆弱性を修正
  - <https://github.com/openam-jp/openam/issues/280>
- アクセス制御の不備の脆弱性を修正
  - <https://github.com/openam-jp/openam/issues/283>

## 3.2 OSSTech 独自の修正

---

### || 3.2.1 機能追加

- OpenLDAP 用のデータストアを追加
- OpenLDAP 用のデータストアにパーシステントサーチ機能を追加
- OpenLDAP 用の認証モジュールを追加
- Yubikey 認証モジュールを追加
- OpenAM 10 系の画面レイアウトに変更
- スマートフォン向け CSS を追加
- エージェントの設定を OpenLDAP に保存するための拡張
- NTLM 向けの WindowsDesktopSSO 認証モジュールの改修
- レルムに最大セッション時間及び最大アイドル時間を設定するためのサービス定義を追加
- レルムに最大セッション数を設定するためのサービス拡張
- レルム作成時に権限の複製を省略するためのプロパティを追加
- レルム削除時に参照ポリシーの削除をスキップするプロパティの追加
- 通知サーバーリストのキャッシュを削除するためのメソッドの追加
- SAML2 の RelayState パラメータの文字列長の制限 2,000 文字を設定で変更できるように変更

### || 3.2.2 設定関連の変更

- クッキーエンコードの設定の初期値を false から true に変更
- 統計情報ログのデフォルト無効化
- デフォルトのルートサフィックスを OSSTech 独自のものに変更
- ポリシーエージェントのデフォルトの動作モードを従来 (9.5.5/10.1.0-Xpress) のモードに変更
- データストア通知の設定をデフォルトで有効に変更
- 利用していない Distributed Authentication Service(DAS) パッケージを削除

- OS 標準 OpenJDK8 上で動作するようにパッケージを変更
- OpenAM が発行する Cookie に SameSite=None を付与するオプションを追加

### || 3.2.3 問題の修正

- ログアウト時にエラーが発生する問題を修正
- フェデレーションのシーケンスでフォワード先の URL からコンテキスト名までを削除するように修正
- ログインエラー時の画面のリンクに不要な SAML リクエストが含まれる問題を修正
- 証明書認証モジュールのログ出力のレベルを修正
- CRL 取得処理の不具合を修正
- マルチサーバーモードでのユーザー毎のセッション数チェックの有効化
- ログイン／ログアウトのリクエストをキャッシュしないように HTTP キャッシュヘッダに no-store を設定するように修正
- SAML2.0／OAtuth2.0 関連の画面の文字化けを修正
- データストアが利用するハートビートタイムアウトのデフォルト値を変更
- データストアのパージメントサーチのフィルタに不正な文字列を設定した場合に復旧できなくなる問題を修正
- ユーザーの DN を変更した場合に古い DN が利用されてしまう問題を修正
- OpenLDAP をデータストアとして利用した場合に objectClass の調整機能が動作しない問題を修正
- OAuth 2.0 認可コードグラントでスコープの取扱いに関する問題を修正
- REST API によるエントリ（ユーザー／グループ）作成処理を修正
- セッションフォワーディングの DoS 脆弱性の修正
- セッションフォワーディング時に不正な HTTP ヘッダのリクエストを生成する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4705>
- OpenLDAP をデータストアとして利用する場合に、ユーザーにサービスを追加できない問題を修正
- Agent のセッションが無効な場合に正しくハンドリングされない問題を修正

- OAuth2.0 のトークン情報エンドポイントで発生するメモリーリークを修正
- OAuth2.0 のアクセストークン及びリフレッシュトークンの取得処理にレルムのチェックを追加
- SAML SP でエラーが発生した場合に転送する URL に誤りがある問題を修正
- SecurID 認証をデフォルトから削除
- SAML アサーションの属性として実体参照文字を SP に渡すと、SP 側で期待通りに受け取れない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-5988>
- OAuth2.0 アクセストークン発行時のトークン名検証の不備を修正
- OpenAM が SAML SP である場合、条件によりセッションが正常に更新されない問題を修正
- セッションアップグレード時に AMAuthCookie がタイムアウトすると認証フローが正常に遷移しない問題を修正
- セッションフォワーディング時の文字エンコードの問題を修正
- Apache Commons FileUpload におけるサービス運用妨害 (DoS) の脆弱性を修正 (CVE-2016-3092)
  - <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3092>
- リソースベース認証でポリシーキャッシュを利用できない問題を修正
- リソースベース認証で LDAP フィルター条件を利用できない問題を修正
- Java-1.7.0-openjdk 非互換問題の修正(AM20170216-1/AM20170216-2)
  - <http://www.osstech.co.jp/support/am20170216-1>
  - <http://www.osstech.co.jp/support/am20170216-2>
- SAML の認証コンテキストクラスの問題を修正
- OpenDJ Server のビルドの問題を修正
- ユーザー ID の大文字・小文字を区別するために SAML SP アカウントマッパークラスを追加
- Java8 利用時に監査ログのフォーマットが変わる問題を修正
- WS-Federation のエンティティをトラストサークルに追加できない問題を修正
- セキュリティ脆弱性の修正(AM20180604-1)

- <https://www.osstech.co.jp/support/am2018-3-1>
- Fedlet で NoClassDefFoundError が発生する問題を修正
- セキュリティ脆弱性の修正(AM20190722-1)
  - <https://www.osstech.co.jp/support/am2019-2-1>
- メモリーリークの問題により、レルム単位で最大セッション数を設定するためのサービスを廃止
- OpenJDK 8 非互換問題の修正(AM20201118-1/AM20201118-2)
  - <https://www.osstech.co.jp/serviceinfo/am2020-4-1/>
  - <https://www.osstech.co.jp/serviceinfo/am2020-4-2/>
- WebFinger の脆弱性(CVE-2021-29156)を修正
- LDAPS の TLS バージョンを指定するオプションを追加
- OpenLDAP データストアの持続検索によりヒープの逼迫が発生する問題を修正
- リモートコード実行の脆弱性(CVE-2021-35464)を修正
- SAML における XML インジェクションの脆弱性を修正
- アクセス制御の不備の脆弱性を修正
  - <https://www.osstech.co.jp/support/am2021-7-1/>
- アップグレード処理の修正
- Apache Commons FileUpload の脆弱性 (CVE-2023-24998) によるサービス運用妨害 (DoS) の脆弱性を修正
- サービス運用妨害 (DoS) の脆弱性を修正
- IdP で SAML2 フェイルオーバーが動作しない問題を修正

## 4. osstech-tomcat パッケージの更新

OSSTech 提供の OpenAM 11.0.0 は osstech-tomcat(RHEL7)/osstech-tomcat7(RHEL6)を同梱しています。本章ではこれらのパッケージの更新について記載します。

### 4.1 systemd 対応(RHEL7)

Osstech-tomcat 1.0.0-18(osstech-openam11-11.0.0-120 に同梱)で systemd に対応しました。以前のバージョンでは service コマンドで起動・停止を行っていましたが、1.0.0-18 以降では systemctl コマンドを利用できます。

- 起動

```
# /usr/bin/systemctl start osstech-tomcat.service
```

- 停止

```
# /usr/bin/systemctl stop osstech-tomcat.service
```

また、従来どおり service コマンドで起動・停止を行うことも可能です。ただし、コマンドの出力が従来とは異なる点に注意してください。

- service コマンドによる起動

```
# /usr/sbin/service osstech-tomcat start  
Redirecting to /bin/systemctl start osstech-tomcat.service
```

- service コマンドによる停止

```
# /usr/sbin/service osstech-tomcat stop  
Redirecting to /bin/systemctl stop osstech-tomcat.service
```

- 以前のバージョンの起動

```
# service osstech-tomcat start  
Starting /opt/osstech/etc/svscan/tomcat: [OK]
```

- 以前のバージョンの停止

```
# service osstech-tomcat stop  
Stopping /opt/osstech/etc/svscan/tomcat: .....[OK]
```



## 5. 制限事項

- 異なるバージョンの OpenAM を同一の OpenAM サイトに利用することはできません
- データストアのデータベースリポジトリは試験的実装であり本稼働環境での利用を推奨していません

## 6. パッケージ更新履歴

- 2024年5月28日 osstech-openam-11.0.0-142
  - IdPでSAML2 フェイルオーバーが動作しない問題を修正
- 2023年12月7日 osstech-openam-11.0.0-141
  - サービス運用妨害 (DoS) の脆弱性を修正
- 2023年3月29日 osstech-openam-11.0.0-140
  - サービス運用妨害 (DoS) の脆弱性を修正
  - アクセス制御の不備の脆弱性を修正
  - アップグレード処理の修正
  - Apache Commons FileUpload の脆弱性 (CVE-2023-24998) によるサービス運用妨害 (DoS) の脆弱性を修正
- 2021年12月23日 osstech-openam-11.0.0-136
  - アクセス制御の不備の脆弱性を修正
- 2021年8月20日 osstech-openam-11.0.0-135
  - SAML における XML インジェクションの脆弱性を修正
- 2021年8月4日 osstech-openam-11.0.0-134
  - リモートコード実行の脆弱性 (CVE-2021-35464) を修正
- 2021年7月19日 osstech-openam-11.0.0-133
  - OpenLDAP データストアの持続検索によりヒープの逼迫が発生する問題を修正
- 2021年4月28日 osstech-openam-11.0.0-132
  - WebFinger の脆弱性 (CVE-2021-29156) を修正
  - LDAPS の TLS バージョンを指定するオプションを追加
- 2020年11月25日 osstech-openam-11.0.0-130
  - OpenJDK 8 非互換問題の修正 (AM20201118-1/AM20201118-2)

- <https://www.osstech.co.jp/serviceinfo/am2020-4-1/>
- <https://www.osstech.co.jp/serviceinfo/am2020-4-2/>
- 2020年5月18日 osstech-openam-11.0.0-129
  - メモリーリークの問題により、レルム単位で最大セッション数を設定するためのサービスを廃止
- 2020年1月20日 osstech-openam-11.0.0-128
  - OpenAM が発行する Cookie に SameSite=None を付与するオプションを追加
- 2019年7月8日 osstech-openam-11.0.0-126
  - セキュリティ脆弱性の修正(AM20190722-1)
    - <https://www.osstech.co.jp/support/am2019-2-1>
- 2018年10月11日 osstech-openam-11.0.0-124
  - Fedlet で NoClassDefFoundError が発生する問題を修正
- 2018年5月2日 osstech-openam-11.0.0-123
  - セキュリティ脆弱性の修正(AM20180604-1)
    - <https://www.osstech.co.jp/support/am2018-3-1>
- 2018年4月24日 osstech-openam-11.0.0-122
  - ログインページに入力したユーザー名/パスワードを認証ポストプロセスに渡すしくみを追加
    - <https://bugster.forgerock.org/jira/browse/OPENAM-5921>
  - WS-Federation のエンティティをトラストサークルに追加できない問題を修正
- 2018年1月31日 osstech-openam-11.0.0-120
  - Java8 を利用した場合に証明書認証で NoClassDefFoundError が発生する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-141>
  - Java8 でユニットテストが失敗する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3766>
    - <https://bugster.forgerock.org/jira/browse/OPENAM-4511>
  - OS 標準 OpenJDK8 上で動作するようにパッケージを変更

- Java8 利用時に監査ログのフォーマットが変わる問題を修正
- 同梱 osstech-tomcat パッケージの systemd 対応(RHEL7)
- 2017 年 9 月 25 日 osstech-openam-11.0.0-116
  - サーバー間死活監視にコネクションタイムアウト・リードタイムアウトを設定する修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-2920>
  - サーバー間死活監視のコネクションが適切にクローズされていない問題の修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-5040>
- 2017 年 8 月 30 日 osstech-openam-11.0.0-115
  - ユーザー ID の大文字・小文字を区別するために SAML SP アカウントマッパークラスを追加
- 2017 年 7 月 12 日 osstech-openam-11.0.0-114
  - SAML の認証コンテキストクラスの問題を修正
  - OpenDJ Server のビルドの問題を修正
- 2017 年 2 月 16 日 osstech-openam-11.0.0-112
  - CTS の削除スレッドが例外により停止してしまう問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3283>
  - 認証レベルにレルム名が含まれていた場合に SAML の認証処理で NumberFormatException が発生する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-6776>
  - リソースベース認証でポリシーキャッシュを利用できない問題を修正
  - リソースベース認証で LDAP フィルター条件を利用できない問題を修正
  - Java-1.7.0-openjdk 非互換問題の修正(AM20170216-1/AM20170216-2)
    - <http://www.osstech.co.jp/support/am20170216-1>
    - <http://www.osstech.co.jp/support/am20170216-2>
- 2016 年 11 月 9 日 osstech-openam-11.0.0-108
  - セキュリティ脆弱性の修正(AM20161109-1)

- <http://www.osstech.co.jp/support/am20161109-1>
- 2016年9月7日 osstech-openam-11.0.0-106
  - セキュリティ脆弱性の修正(AM20160907-1)
    - <http://www.osstech.co.jp/support/am20160907-1>
- 2016年8月2日 osstech-openam-11.0.0-102
  - Java-1.7.0-openjdk 非互換問題の修正(AM20160729-1/AM20160729-2)
    - <http://www.osstech.co.jp/support/am20160729-1>
    - <http://www.osstech.co.jp/support/am20160729-2>
    - <https://bugster.forgerock.org/jira/browse/OPENDJ-2247>
- 2016年7月26日 osstech-openam-11.0.0-99
  - セキュリティ脆弱性の修正(AM20160726-1)
    - <http://www.osstech.co.jp/support/am20160726-1>
  - Adaptive Risk 認証におけるクッキー値のエンコードおよびデコードに関する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3999>
  - REST API 利用時にコールバックが正常に渡らない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-2270>
  - 認証中に NPE が発生する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3784>
  - SAML2 の RelayState パラメータの文字列長の制限 2,000 文字を設定で変更できるように変更
  - 利用していない Distributed Authentication Service(DAS) パッケージを削除
  - セッションフォワーディング時の文字エンコードの問題を修正
  - Apache Commons FileUpload におけるサービス運用妨害 (DoS) の脆弱性を修正 (CVE-2016-3092)
    - <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3092>
- 2016年3月8日 osstech-openam-11.0.0-85
  - SunQueryParamsString が二重にエンコードされる問題を修正

- <https://bugster.forgerock.org/jira/browse/OPENAM-2940>
- SunQueryParamsString のデコードで例外が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-5214>
- CDSSO で SunQueryParamsString がエンコードされない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-8154>
- セキュリティ脆弱性の修正(AM20160308-1)
  - <http://www.osstech.co.jp/support/AM20160308-1>
- OpenAM が SAML SP である場合、条件によりセッションが正常に更新されない問題を修正
- セッションアップグレード時に AMAuthCookie がタイムアウトすると認証フローが正常に遷移しない問題を修正
- 2015 年 12 月 7 日 osstech-openam-11.0.0-78
  - セキュリティ脆弱性の修正(AM20151207-1)
    - <http://www.osstech.co.jp/support/AM20151207-1>
- 2015 年 9 月 15 日 osstech-openam-11.0.0-77
  - セキュリティ脆弱性の修正(AM20151027-1)
    - <http://www.osstech.co.jp/support/AM20151027-1>
- 2015 年 9 月 15 日 osstech-openam-11.0.0-76
  - LDAP 認証モジュール内の検索で複数のユーザーが見つかった場合に NullPointerException が発生する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-6286>
  - データストアの設定がキャッシュとして残る問題の修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-6399>
  - データストア設定の削除に連動して参照ポリシーが削除されてしまう問題の修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-2532>
  - OpenAM のログローテーション機能が実際のログサイズではなく OpenAM が出力したログサイズで実行される問題の修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-4072>

- セキュリティ脆弱性の修正(AM20150915-1)
  - <http://www.osstech.co.jp/support/AM20150915-1>
- レルム削除時に参照ポリシーの削除をスキップするプロパティの追加
- 通知サーバーリストのキャッシュを削除するためのメソッドの追加
- 2015年5月27日 osstech-openam-11.0.0-66
  - FRREST のトークン管理エンドポイントで取得できるリフレッシュトークンの tokenName が access\_token である問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3646>
  - セッションアップグレードの場合に HOTP 認証が動作しない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-4304>
  - HOTP 認証で認証画面で OTP コードの要求ボタンを押下すると OTP が 2 回送信される問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-2464>
  - セキュリティ脆弱性の修正(AM20150527-1)
    - <http://www.osstech.co.jp/support/AM20150527-1>
  - レルムに最大セッション数を設定するためのサービス拡張
  - レルム作成時に権限の複製を省略するためのプロパティを追加
  - SecurID 認証をデフォルトから削除
  - SAML アサーションの属性として実体参照文字を SP に渡すと、SP 側で期待通りに受け取れない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-5988>
  - OAuth2.0 アクセストークン発行時のトークン名検証の不備を修正
- 2015年4月8日 osstech-openam-11.0.0-55
  - SAML アサーションの NameID に SPNameQualifier 属性が無い場合に SAML エラーとなる問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3573>
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3707>

- DelegationPolicyImpl のキャッシュ更新処理がスレッドセーフではない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4176>
- SAML2 フェイルオーバーが動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4195>
  - <https://bugster.forgerock.org/jira/browse/OPENAM-5614>
- セキュリティ脆弱性の修正(AM20150408-1)
  - <http://www.osstech.co.jp/support/AM20150408-1>
- レルムに最大セッション時間及び最大アイドル時間を設定するためのサービス定義を追加
- OpenLDAP をデータストアとして利用する場合に、ユーザーにサービスを追加できない問題を修正
- Agent のセッションが無効な場合に正しくハンドリングされない問題を修正
- OAuth2.0 のトークン情報エンドポイントで発生するメモリーリークを修正
- OAuth2.0 のアクセストークン及びリフレッシュトークンの取得処理にレルムのチェックを追加
- SAML SP でエラーが発生した場合に転送する URL に誤りがある問題を修正
- 2014 年 11 月 6 日 osstech-openam-11.0.0-38
  - NTLM 向けの WindowsDesktopSSO 認証モジュールの改修
  - セッションフォワーディングの DoS 脆弱性の修正
  - セッションフォワーディング時に不正な HTTP ヘッダのリクエストを生成する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-4705>
  - Secure Attribute Exchange (SAE) 用エンドポイントの XSS 脆弱性の修正
  - REST API へ JSON リクエストを送る度に RestSecurity インスタンスが作成される問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-4044>
- 2014 年 8 月 28 日 osstech-openam-11.0.0-33
  - 保護対象の URL が複数の参照ポリシーに合致する場合にポリシー判定処理がハングアップする問題を修正



- <https://bugster.forgerock.org/jira/browse/OPENAM-2460>
- SAML リクエストに isPassive 属性が付与されていない場合に NullPointerException が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3542>
- REST API によるエントリ（ユーザー／グループ）作成処理を修正
- 2014 年 7 月 22 日 osstech-openam-11.0.0-30
  - デバッグレベルがメッセージである場合にアダプティブリスク認証を利用すると失敗する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3607>
  - ssoadm コマンドの create-metadata-templ サブコマンドで NullPointerException が発生する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3172>
  - OpenAM の依存ライブラリである Restlet のアップデート
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3694>
  - OpenAM を冗長構成としている場合に ClientSDK や ssoadm が動作しない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3528>
  - OAuth 認証が Cookie 付加時にサーバー設定の HttpOnly と Secure の設定を反映しない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3227>
  - エージェントグループをサブレルムで作成できない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3269>
  - OAuth Client を設定しているとアップグレードに失敗する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3422>
  - OpenID Connect 1.0 クライアントの動的登録機能が動作しない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-2865>
  - OpenID Connect の”prompt”パラメータが動作しない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3318>
  - OAuth 2.0 の同意の保存が動作しない問題を修正

- <https://bugster.forgerock.org/jira/browse/OPENAM-3315>
- OAuth 2.0 のクライアント登録ページの表示の問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3205>
- OpenID Connect のエンドポイントが返却する id\_token\_signing\_alg\_values\_supported 名のスペルミスを修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3534>
- OAuth2.0 クライアントクレデンシャルで作成したトークンの読み込みで NullPointerException が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3506>
- OAuth2.0 の読み込み・削除操作で管理者トークンと読み込み対象トークンのレルムが一致しない場合に NullPointerException が発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3520>
- OpenID Connect Session Management の署名検証処理の修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3620>
- OAuth 2.0 の同意画面の Description をロケール毎に表示できない問題の修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3678>
- クッキーエンコードを有効にしている場合に OAuth 認証が動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-4094>
- OpenAM を冗長構成としている場合に OpenAM が発行する Cookie に HttpOnly が付加されない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3740>
- データストア通知の設定が有効である場合に権限情報の書き込みが競合してしまう問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3226>
- データストアに対して不正なサーチが発生する問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3742>
- アダプティブリスク認証が Cookie 付加時にサーバー設定の HttpOnly と Secure の設定を反映しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3632>

- OpenDJ SDK のアップデートにより dsconfig コマンドの結果が正しく表示されない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3465>
- sAMAccountName をネーミング属性に設定した場合に Active Directory データストアが動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3428>
- 組織の DN にルートサフィックスを設定した場合に Active Directory データストアが動作しない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3385>
- LDAP 認証にオペレーションタイムアウトの設定機能がない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3353>
- データストアのエラー出力強化
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3113>
- gotoOnFail URL の検証処理の追加
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2760>
- リモートセッション関連の処理で発生するメモリリークの問題の修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-2145>
- コネクションプール内で名前解決後の IP アドレスをキャッシュしてしまい、再接続時に名前解決を行わない問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3865>
- OpenAM のアップグレード時にサーバーのデフォルト設定の一部が削除されてしまう問題を修正
  - <https://bugster.forgerock.org/jira/browse/OPENAM-3947>
- エージェントの設定を OpenLDAP に保存するための拡張
- データストア通知の設定をデフォルトで有効に変更
- OpenLDAP をデータストアとして利用した場合に objectClass の調整機能が動作しない問題を修正
- OAuth 2.0 認可コードグラントでスコープの取扱いに関する問題を修正

- 2014年3月27日 osstech-openam-11.0.0-13
  - ユーザーの DN を変更した場合に古い DN が利用されてしまう問題を修正
- 2014年3月18日 osstech-openam-11.0.0-12
  - OpenAM が SAML SP として動作する場合にレルムの設定を正しく扱わない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3698>
  - 設定ディレクトリからバージョン情報を取得できない場合に NullPointerException が発生する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3489>
  - ポリシー判定処理がリソースの URL からスラッシュを外してしまう問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3509>
  - ポリシー判定処理がワイルドカードの判定を正しく処理しない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3638>
  - ポリシーエージェントのデフォルトの動作モードを従来 (9.5.5/10.1.0-Xpress) のモードに変更
- 2014年1月27日 osstech-openam-11.0.0-7
  - IdRepo デバッグログに RetryTask のエラーが出つづける問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-688>
  - Fedlet の JSP のコンパイルエラーを修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3217>
  - シングルログアウト時に RelayState の検証に失敗する問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3437>
  - データストア認証モジュールを利用する場合にオンメモリのアカウントロックを利用できない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3456>
  - デスクトップ SSO の認証レベルが設定されない問題を修正
    - <https://bugster.forgerock.org/jira/browse/OPENAM-3490>
  - OpenAM に同梱されている OpenDJ SDK の問題を修正

- <https://bugster.forgerock.org/jira/browse/OPENDJ-1247>
- <https://bugster.forgerock.org/jira/browse/OPENDJ-1258>
- OpenLDAP 用のデータストアを追加
- OpenLDAP 用のデータストアにパーシステントサーチ機能を追加
- OpenLDAP 用の認証モジュールを追加
- Yubikey 認証モジュールを追加
- OpenAM 10 系の画面レイアウトに変更
- スマートフォン向け CSS を追加
- クッキーエンコードの設定の初期値を false から true に変更
- 統計情報ログのデフォルト無効化
- デフォルトのルートサフィックスを OSSTech 独自のものに変更
- ログアウト時にエラーが発生する問題を修正
- フェデレーションのシークエンスでフォワード先の URL からコンテキスト名までを削除するように修正
- ログインエラー時の画面のリンクに不要な SAML リクエストが含まれる問題を修正
- 証明書認証モジュールのログ出力のレベルを修正
- CRL 取得処理の不具合を修正
- マルチサーバーモードでのユーザー毎のセッション数チェックの有効化
- ログイン／ログアウトのリクエストをキャッシュしないように HTTP キャッシュヘッダに no-store を設定するように修正
- SAML2.0／OAtuth2.0 関連の画面の文字化けを修正
- データストアが利用するハートビートタイムアウトのデフォルト値を変更
- データストアのパーシステントサーチのフィルタに不正な文字列を設定した場合に復旧できなくなる問題を修正