OSSTech OpenAM 11.0.0

リリースノート

オープンソース・ソリューション・テクノロジ(株)

更新日: 2014 年 11 月 6 日

目次

1. はじめに 1
2. osstech-openam-11.0.0-38 の修正内容 2
2.1 11.0.2／12.0.0 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
3. コミュニティ版との差異 3
3.1 11.0.2／12.0.0 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 6
3.2.1 機能追加 6
3.2.2 設定関連の変更 7
3.2.3 問題の修正 7
4. 制限事項 8
5. パッケージ更新履歴 9

1. はじめに

本ドキュメントは、OSS テクノロジ提供の 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-openam-11.0.0-38 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-openam11-11.0.0-38.el6.noarch
```

2. osstech-openam-11.0.0-38 の修正内容

OSS テクノロジ提供の OpenAM 11.0.0-38 では以下の修正を行いました。

2.1 11.0.2／12.0.0 以降に統合される修正(バックポート)

- 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

2.2 OSSTech 独自の修正

2.2.1 機能追加

- NTLM 向けの WindowsDesktopSSO 認証モジュールの改修

2.2.2 設定関連の変更

なし

2.2.3 問題の修正

- 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

3. コミュニティ版との差異

OSS テクノロジ提供の 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 11.0.2／12.0.0 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
- 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

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

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

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
- 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

4. 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おりません

5. パッケージ更新履歴

- 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