

OSSTech OpenAM 13.0.0 リリース ノート



OSSTech

OSSTech(株)

更新日

2024 年 1 月 22 日

目次

1	はじめに	1
2	osstech-openam13-13.0.0-196 の修正内容	2
2.1	コミュニティ版 13.0.0 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
3	コミュニティ版との差異	3
3.1	コミュニティ版 13.0.0 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
4	osstech-tomcat パッケージの更新	13
4.1	systemd 対応	13
5	パッケージ更新履歴	15

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-openam13-13.0.0-196 です。

このパッケージはコミュニティ版 OpenAM 13.0.0 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。

<https://backstage.forgerock.com/#!/docs/openam/13/release-notes>

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

```
$ rpm -qa | grep osstech-openam13
osstech-openam13-13.0.0-196.e17.noarch
```

2 osstech-openam13-13.0.0-196 の修正内容

OSSTech 提供の OpenAM 13.0.0-196 では以下の修正を行いました。

2.1 コミュニティ版 13.0.0 以降に統合される修正 (バックポート)

- 冗長構成の SAML SP として動作している場合にセッションの取得に失敗する場合がある問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-3891>

2.2 OSSTech 独自の修正

- サービス運用妨害 (DoS) の脆弱性を修正
- 認証 REST API の POST パラメーターを改ざんすると Internal Server Error が応答される問題を修正
- 認証 REST API で authId を base64url でデコードできなかった場合に Internal Server Error が応答される問題を修正

3 コミュニティ版との差異

OSSTech 提供の OpenAM 13.0.0 はコミュニティ版 OpenAM 13.0.0 と以下の差異があります。

3.1 コミュニティ版 13.0.0 以降に統合される修正 (バックポート)

- LDAP 認証のパスワード変更画面の表示の問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-4757>
- アップグレード時にバージョン関連のプロパティが削除される問題・更新されない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-7982>
- OAuth のページ (/openam/oauth2/device/user) を表示できない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8371>
- ログを syslog に出力しているとハングする場合がある問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-7864>
- SAML のエンドポイントにアクセスする際に realm パラメーターを付与すると ClassCastException が発生する問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8351>
- アカウントロックの挙動の問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8321>
- セキュリティ脆弱性の修正 (OpenAM Security Advisory #201604)
 - <https://forgerock.org/2016/05/openam-security-advisory-201604/>
- Self Service のトークンを別の号機や再起動後に処理できない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8451>
- ForgeRock Commons ライブラリのアップデート
- セキュリティ脆弱性の修正 (OpenAM Security Advisory #201605)
 - (ただし、Issue #201605-06 を除く)
 - <https://forgerock.org/2016/08/openam-security-advisory-201605/>
- データストアキャッシュの有効期限を設定するとデッドロックが発生する問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8521>
- OpenDJ のエラーログが出力されない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8347>

- セキュリティ脆弱性の修正 (OpenAM Security Advisory #201608)
 - <https://backstage.forgerock.com/#!/knowledge/kb/article/a25759331>
- アップグレード時に OAuth Provider の設定が作成される問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-9043>
- サイト構成時にステートレスセッションが発行されない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-9137>
- Fedlet を作成できない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8218>
- OepnDJ SDK の Trace レベルのログを抑制する
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8696>
- JDK の XML パーサーを利用するように修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-7320>
- OAuth 2.0 の同意画面を表示しないオプションを追加
 - <https://bugster.forgerock.org/jira/browse/OPENAM-5093>
- OAuth 2.0 で同意を保存しない設定の場合に同意ページにチェックボックスを表示しない
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8375>
- OAuth 2.0 でディスプレイモードを指定した場合に同意ができない問題の修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-9507>
- 統計情報ログが出力されない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-6998>
- 認証 REST API 用の署名鍵が冗長構成の各サーバーで異なる問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8269>
- 認証連鎖の途中で認証セッションがタイムアウトした場合にセッションタイムアウトの表示にならない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8433>
- NullPointerException が発生する問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8386>
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8432>
- 一般ユーザーのセッション毎に余分な権限キャッシュを取得していた問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8607>
 - <https://bugster.forgerock.org/jira/browse/OPENAM-9102>
- OpenID Connect id_token bearer 認証の設定ができない問題を修正
- 管理画面で設定項目の順序が崩れる問題を修正

- OpenDJ が changelogDb を読み込めなくなる問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENDJ-2969>
- UMA Provider のサービス設定をキャッシュするように修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8678>
- ScriptingService の設定をキャッシュするように修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8023>
- OIDC/OAuth2.0 認証モジュールで jwk_url 使用時 OP からの応答に x5c が含まれていると認証に失敗する問題の修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8807>
- CTS の削除スレッドで予期せぬ例外が発生した場合にコネクションをクローズしない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-9947>
- 認証ポストプロセスで設定した認証成功時の URL に遷移しない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8146>
- 秒単位の LDAP タイムアウト設定がミリ秒単位で扱われている問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8459>
- デスクトップ SSO 失敗時に ClassCastException が発生する問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-9893>
- 署名の無い SAML ECP リクエストを許容するように修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-3095>
- 監視の状態が無効の場合、CoreSystem にエラーが出力される問題の修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-3415>
 - <https://bugster.forgerock.org/jira/browse/OPENAM-9814>
- セッションを発行したサーバーにアクセスできない場合に SAML アサーションを発行できない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-6974>
- LDAP フィルター条件でメモリーリークが発生する問題を修正
 - <https://github.com/openam-jp/openam/issues/211>
- OAuth 2.0 デバイスフローのユーザーコードのエントロピーが十分でない問題を修正
 - <https://github.com/openam-jp/openam/issues/278>
- 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>

- 冗長構成の SAML SP として動作している場合にセッションの取得に失敗する場合があります問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-3891>

3.2 OSSTech 独自の修正

- 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
- XUI のロゴの変更
- 旧ログイン画面や初期設定画面を OpenAM 10 系の画面レイアウトに変更
- クッキーエンコードの設定の初期値を false から true に変更
- 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旧バージョン (9.5.5/10.1.0-Xpress) のモードに変更
- 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
- 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
- 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
- NTLM 向けの WindowsDesktopSSO 認証モジュールの改修
- 管理画面の共通タスクでレルムを選択できないように修正
- 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
- 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>
- 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>
 - 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>
 - 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>
 - 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>
 - Host IdP 作成後の完了画面から XUI に戻らない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8537>
 - Google Apps の設定完了画面で終了ボタンを押すと AMUncaughtException が表示される問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8538>
 - 他のレルムに CoT がある場合に、GoogleApps を設定できない問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8540>
 - 共通タスクのいくつかの機能で、キャンセルボタンを押すとダッシュボードではなくレルムの選択画面にもどる問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8546>
 - 未認証状態で encode.jsp にアクセスすると goto が showServerConfig.jsp になる問題を修正
 - <https://bugster.forgerock.org/jira/browse/OPENAM-8572>
 - 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>
 - XUI のログイン画面で発生する XSS の問題を修正
 - OpenJDK のバージョンを 8 に変更
 - Fedlet を従来通りのアーカイブで作成するように修正
 - AuditLog に出力される時刻を JST にするオプションの追加
 - ログイン時の XUI のレルム判定処理で DNS エイリアスを考慮するように修正
 - OpenID Connect の OP である時にセッションアップグレードをすると acr_values の認証連鎖が有効にならない
 - ログイン画面の日本語化
 - 管理画面の日本語化
-

- Cookie ドメインが設定されていない場合でも動作するように修正
- URL 比較処理の結果を OSSTech OpenAM 11 に合わせる
- OpenID Connect の RP である時に client_secret_post のみに対応するよう修正
- カスタム認証モジュールで RedirectCallback を複数回利用できない問題を修正
- OpenID Connect の OP である時にリクエストの acr_values にマップされる認証連鎖が存在しない場合、エラーを応答するように修正
- RPM アップデート後に XUI のコンテンツをブラウザに更新させるように修正
- IE で画面が日本語化されない問題を修正
- ポリシー条件によりアクセスが拒否される場合にポリシーサービスの結果が欠落する問題を修正
- authId クッキーがタイムアウトしている場合に認証を継続できない問題を修正
- SAML2 認証の内部で呼び出す認証連鎖が失敗すると認証を継続できない問題を修正
- SAML2 認証の内部で呼び出す認証にフォーカスが当たらない問題を修正
- アダプティブリクス認証の設定画面でタブを切り替えた際に更新前の設定が表示される問題を修正
- favicon を変更
- ログイン失敗画面のリンクのクエリーがエンコードされていない問題を修正
- 認証成功時に sharedState のユーザー名を上書きする機能を OpenLDAP 認証に追加
- 最初のコールバックが RedirectCallback の場合はセッションタイムアウトで認証失敗画面に遷移するように修正
- OAuth2/OIDC 認証モジュールで署名にクライアントアントシークレットを使う場合二箇所を設定する必要がある問題を修正
- デフォルトで登録されている認証モジュールのインスタンスを削除すると後から作成した同じ認証モジュールのインスタンスも削除される問題を修正
- OAuth2.0/OIDC 認証モジュールで jwk_url に応答される json に楕円暗号方式があると認証に失敗する問題を修正
- ログイン成功 URL へ遷移しない問題を修正
- 管理画面で作成した認証モジュールと同じ名称のインスタンスを ssoadm から削除できない問題を修正
- XUI アクセス時のクエリーパラメーターをバージョン情報からハッシュに変更
- ssoadm/ampassword の java オプションを追加
- CTS に不正なエントリが存在した場合に削除処理として当該エントリを無視するように修正
- Client Configuration Endpoint の応答が仕様に準拠していない問題の修正

- SAML の認証コンテキストクラスの問題を修正
- OAuth クライアントに関するログ出力の問題を修正
- ログローテーション用 logrotate 設定の組込み
- セッションプロパティのポリシー条件でドットを含むプロパティ名を管理画面から設定できない問題の修正
- LDAP フィルター条件で Time Limit/Size Limit を適切に利用するように修正
- ForgeRock Authenticator 認証をセッションアップグレードで利用できない問題を修正
- ForgeRock Authenticator 認証の日本語化
- ForgeRock Authenticator 認証で生成する QR コードのフォーマットの変更
- Groovy 及び Groovy Sandbox ライブラリのアップデート
- IE11 で管理画面からポリシーを編集できない問題の修正
- ssoadm の認証にアダプティブリスクの IP アドレスレンジを利用できない問題を修正
- OAuth 2.0 Introspection Endpoint のレスポンスに含まれる exp がトークンの有効期限切れとなる時刻を示す値となるよう修正
- 認証ポストプロセスクラスで設定した認証成功時のリダイレクト先がクエリーパラメータで指定したものよりも優先されるように修正
- ForgeRock Authenticator 認証でリカバリーコードを発行しないオプションを追加
- アダプティブリクス認証のにユーザー属性の存在チェック機能を追加
- XUI のキャッシュ防止用クエリーパラメーターを修正
- セッションアップグレード時の認証に失敗すると既存のセッションが破棄される問題を修正
- デスクトップ SSO が認証連鎖に含まれるときに後続の認証が失敗する問題を修正
- osstech-openam13-tools パッケージに管理者コマンドを追加
- 冗長構成の場合に OpenDJ に書き込みできなくなる問題を修正
- SAML2 認証が出力するデバッグログの一部を抑制
- SAML2 認証で NullPointerException が発生する問題を修正
- goto 及び gotoOnFail パラメーターに関する問題を修正
- ログアウト URL アクセス時に unknown エラーが表示される問題を修正
- IE11 で発生する JavaScript のエラーを修正
- goto パラメーターに特定の文字が含まれていると意図したページに遷移しない問題を修正
- セッションアップグレード中に認証セッションのタイムアウトが発生すると認証を継続できない問題を修正
- XUI の挙動を変更するオプションの追加

- セキュリティ脆弱性の修正 (AM20180604-1)
 - <https://www.osstech.co.jp/support/am2018-3-1>
- REST API の users エンドポイントの改善
- ログイン画面にエラーメッセージが 2 回表示される問題を修正
- OpenDJ がレプリケーション先と接続できない場合のログ出力を改善
- Office 365 向けの SAML IdP アダプターを追加
- REST API のユーザーセルフサービスエンドポイントの改善
- ユーザーセルフサービスに関する修正
- ForceAuth によるセッションアップグレードに失敗する問題を修正
- Agent のログアウトにより Active Session 数に実際の値との差が生じる問題を修正
- SAML IdP として動作している場合にレルムの設定に依存してログインに失敗する問題を修正
- ForgeRock Authenticator 認証のログ出力の改善
- JavaMail のデバッグログの抑制
- SAML のアサーション暗号化に RSA_OAEP を利用するオプションを追加
- OAuth 2.0 同意画面の日本語化
- REST API のセッションエンドポイントの改善
- Apache Commons FileUpload を 1.3.3 にアップデート (CVE-2016-1000031)
- OpenID Connect OP の署名アルゴリズムとして RS384/RS512 をサポート
- セキュリティ脆弱性の修正 (AM20190206-1)
 - <https://www.osstech.co.jp/support/am2019-1-1>
- SAML2 フェイルオーバー有効時にシングルログアウト用の情報を更新できない問題を修正
- 認可コード/アクセストークンを CTS から読み込めない場合にリトライを行うオプションを追加
- 認証 REST API が HTML 応答を返却した場合にログイン画面でエラーメッセージが表示されない問題を修正
- SAML2 IdP/OAuth2 認可サーバーをポリシーで保護する機能を追加
- セキュリティ脆弱性の修正 (AM20190722-1)
 - <https://www.osstech.co.jp/support/am2019-2-1>
- HTML ファイル取得の遅延によりログイン画面が表示できなくなる問題を修正
- SAML2 IdP のポリシー保護機能で LDAP フィルター条件を利用できない問題を修正
- SAML2 IdP のポリシー保護機能でリソースが正しく表示されない問題を修正
- OAuth2 認可サーバーのポリシー保護機能で LDAP フィルター条件を利用できない問題

題を修正

- メンバーシップポリシー条件の設定画面を修正
- SAML2 IdP/OAuth2 認可サーバーのポリシー保護機能でメンバーシップ条件を利用できない問題を修正
- Client Configuration Endpoint のエラー処理の修正
- SAML2 フェイルオーバーを有効にした場合に SAML2 認証が動作しない問題を修正
- OpenAM が発行する Cookie に SameSite=None を付与するオプションを追加
- ポリシー設定サービスでハートビートを利用するためのオプションを追加
- 非アクティブユーザーのエラーが正常に表示されない問題の修正
- ログイン画面のユーザー名を記憶する機能で Cookie に Base64 エンコードした値を保存するように修正
- パーシステント Cookie 認証を多要素認証の判定に利用できるように拡張
- SAML でメモリーリークが発生する問題を修正
- 生成した Fedlet が動作しない問題を修正
- 冗長構成セットアップ時の LDAPS 接続に TLSv1.2 を利用するように変更
- LDAPS の TLS バージョンを指定するオプションを追加
- JBoss にデプロイした際に MANIFEST Class-Path の警告が多発する問題を修正
- dsconfig コマンドの LDAPS 接続に TLSv1.2 を利用するように変更
- iOS 版 Safari 14 でユーザー名を記録しているとログイン画面が表示できなくなる問題を修正
- WebFinger の脆弱性 (CVE-2021-29156) を修正
- パーシステントサーチにおける TLS バージョンの指定が適用されない問題を修正
- ユーザー REST API で返却する属性の調整
- リモートコード実行の脆弱性 (CVE-2021-35464) を修正
- Microsoft 365 向け IdP アダプターで発生する NullPointerException を修正
- 証明書認証で証明書や CRL 取得時の LDAPS 接続に TLS 1.2 を利用できない問題を修正
- SAML における XML インジェクションの脆弱性を修正
- クロスサイトスクリプティングの脆弱性を修正
- 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/>
- OpenDJ が changelogDb に書き込む際の同期制御を修正
- アカウントロック有効時のメッセージを調整
- REST API のエラー応答を調整

- 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
- ログアウト URL におけるパラメーターの処理を修正
- 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
- メール送信に TLS 1.2 を利用できない問題を修正
- サービス運用妨害 (DoS) の脆弱性を修正
- 認証 REST API の POST パラメーターを改ざんすると Internal Server Error が応答される問題を修正
- 認証 REST API で authId を base64url でデコードできなかった場合に Internal Server Error が応答される問題を修正

4 osstech-tomcat パッケージの更新

OSSTech 提供の OpenAM 13.0.0 は osstech-tomcat パッケージを同梱しています。本章では osstech-tomcat パッケージの更新について記載します。

4.1 systemd 対応

osstech-tomcat 1.0.0-18(osstech-openam13-13.0.0-94 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 パッケージ更新履歴

- 2024 年 01 月 22 日 osstech-openam13-13.0.0-196
 - サービス運用妨害 (DoS) の脆弱性を修正
 - 冗長構成の SAML SP として動作している場合にセッションの取得に失敗する場合がある問題を修正
 - 認証 REST API の POST パラメーターを改ざんすると Internal Server Error が応答される問題を修正
 - 認証 REST API で authId を base64url でデコードできなかった場合に Internal Server Error が応答される問題を修正
- 2023 年 06 月 08 日 osstech-openam13-13.0.0-192
 - メール送信に TLS 1.2 を利用できない問題を修正
- 2023 年 03 月 30 日 osstech-openam13-13.0.0-191
 - OAuth 2.0 デバイスフローのユーザーコードのエントロピーが十分でない問題を修正
 - 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
- 2022 年 08 月 22 日 osstech-openam13-13.0.0-186
 - 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
 - ログアウト URL におけるパラメーターの処理を修正
- 2022 年 03 月 07 日 osstech-openam13-13.0.0-183
 - OpenDJ が changelogDb に書き込む際の同期制御を修正
 - アカウントロック有効時のメッセージを調整
 - REST API のエラー応答を調整
- 2021 年 12 月 23 日 osstech-openam13-13.0.0-180
 - アクセス制御の不備の脆弱性を修正
- 2021 年 09 月 28 日 osstech-openam13-13.0.0-179
 - クロスサイトスクリプティングの脆弱性を修正
- 2021 年 08 月 20 日 osstech-openam13-13.0.0-177
 - SAML における XML インジェクションの脆弱性を修正

- 2021年08月06日 osstech-openam13-13.0.0-176
 - ユーザー REST API で返却する属性の調整
 - リモートコード実行の脆弱性 (CVE-2021-35464) を修正
 - Microsoft 365 向け IdP アダプターで発生する NullPointerException を修正
 - 証明書認証で証明書や CRL 取得時の LDAPS 接続に TLS 1.2 を利用できない問題を修正
- 2021年04月30日 osstech-openam13-13.0.0-172
 - WebFinger の脆弱性 (CVE-2021-29156) を修正
 - パーシステントサーチにおける TLS バージョンの指定が適用されない問題を修正
- 2020年09月23日 osstech-openam13-13.0.0-170
 - iOS 版 Safari 14 でユーザー名を記録しているとログイン画面が表示できなくなる問題を修正
- 2020年08月27日 osstech-openam13-13.0.0-169
 - dsconfig コマンドの LDAPS 接続に TLSv1.2 を利用するように変更
- 2020年08月25日 osstech-openam13-13.0.0-168
 - 生成した Fedlet が動作しない問題を修正
 - 冗長構成セットアップ時の LDAPS 接続に TLSv1.2 を利用するように変更
 - LDAPS の TLS バージョンを指定するオプションを追加
 - JBoss にデプロイした際に MANIFEST Class-Path の警告が多発する問題を修正
- 2020年07月02日 osstech-openam13-13.0.0-165
 - SAML でメモリーリークが発生する問題を修正
- 2020年05月12日 osstech-openam13-13.0.0-164
 - LDAP フィルター条件でメモリーリークが発生する問題を修正
 - ログイン画面のユーザー名を記憶する機能で Cookie に Base64 エンコードした値を保存するように修正
 - パーシステント Cookie 認証を多要素認証の判定に利用できるように拡張
- 2020年03月31日 osstech-openam13-13.0.0-161
 - ポリシー設定サービスでハートビートを利用するためのオプションを追加
 - 非アクティブユーザーのエラーが正常に表示されない問題の修正
- 2020年01月20日 osstech-openam13-13.0.0-159
 - OAuth2 認可サーバーのポリシー保護機能で LDAP フィルター条件を利用できない問題を修正
 - メンバーシップポリシー条件の設定画面を修正

- SAML2 IdP/OAuth2 認可サーバーのポリシー保護機能でメンバーシップ条件を利用できない問題を修正
 - Client Configuration Endpoint のエラー処理の修正
 - SAML2 フェイルオーバーを有効にした場合に SAML2 認証が動作しない問題を修正
 - 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 08 月 09 日 osstech-openam13-13.0.0-151
 - SAML2 IdP のポリシー保護機能で LDAP フィルター条件を利用できない問題を修正
 - SAML2 IdP のポリシー保護機能でリソースが正しく表示されない問題を修正
 - 2019 年 07 月 11 日 osstech-openam13-13.0.0-149
 - SAML2 IdP/OAuth2 認可サーバーをポリシーで保護する機能を追加
 - セキュリティ脆弱性の修正 (AM20190722-1)
 - HTML ファイル取得の遅延によりログイン画面が表示できなくなる問題を修正
 - 2019 年 05 月 17 日 osstech-openam13-13.0.0-143
 - 認可コード/アクセストークンを CTS から読み込めない場合にリトライを行うオプションを追加
 - 認証 REST API が HTML 応答を返却した場合にログイン画面でエラーメッセージが表示されない問題を修正
 - 2019 年 03 月 22 日 osstech-openam13-13.0.0-141
 - セッションを発行したサーバーにアクセスできない場合に SAML アサーションを発行できない問題を修正
 - SAML2 フェイルオーバー有効時にシングルログアウト用の情報を更新できない問題を修正
 - 2019 年 01 月 22 日 osstech-openam13-13.0.0-138
 - ForgeRock Authenticator 認証のログ出力の改善
 - JavaMail のデバッグログの抑制
 - SAML のアサーション暗号化に RSA_OAEP を利用するオプションを追加
 - OAuth 2.0 同意画面の日本語化
 - REST API のセッションエンドポイントの改善
 - Apache Commons FileUpload を 1.3.3 にアップデート (CVE-2016-1000031)
 - OpenID Connect OP の署名アルゴリズムとして RS384/RS512 をサポート
 - セキュリティ脆弱性の修正 (AM20190206-1)
 - 2018 年 10 月 18 日 osstech-openam13-13.0.0-126
-

- SAML IdP として動作している場合にレルムの設定に依存してログインに失敗する問題を修正
 - 2018 年 9 月 19 日 osstech-openam13-13.0.0-125
 - 監視の状態が無効の場合、CoreSystem にエラーが出力される問題の修正
 - Agent のログアウトにより Active Session 数に実際の値との差が生じる問題を修正
 - 2018 年 8 月 10 日 osstech-openam13-13.0.0-123
 - 署名の無い SAML ECP リクエストを許容するように修正
 - Office 365 向けの SAML IdP アダプターを追加
 - REST API のユーザーセルフサービスエンドポイントの改善
 - ユーザーセルフサービスに関する修正
 - ForceAuth によるセッションアップグレードに失敗する問題を修正
 - 2018 年 6 月 12 日 osstech-openam13-13.0.0-117
 - REST API の users エンドポイントの改善
 - ログイン画面にエラーメッセージが 2 回表示される問題を修正
 - OpenDJ がレプリケーション先と接続できない場合のログ出力を改善
 - 2018 年 5 月 1 日 osstech-openam13-13.0.0-113
 - IE11 で発生する JavaScript のエラーを修正
 - goto パラメーターに特定の文字が含まれていると意図したページに遷移しない問題を修正
 - セッションアップグレード中に認証セッションのタイムアウトが発生すると認証を継続できない問題を修正
 - XUI の挙動を変更するオプションの追加
 - セキュリティ脆弱性の修正 (AM20180604-1)
 - 2018 年 2 月 15 日 osstech-openam13-13.0.0-96
 - goto 及び gotoOnFail パラメーターに関する問題を修正
 - ログアウト URL アクセス時に unknown エラーが表示される問題を修正
 - 2017 年 12 月 19 日 osstech-openam13-13.0.0-94
 - 冗長構成の場合に OpenDJ に書き込みできなくなる問題を修正
 - SAML2 認証が出力するデバッグログの一部を抑制
 - SAML2 認証で NullPointerException が発生する問題を修正
 - [同梱 osstech-tomcat パッケージの systemd 対応](#)
 - 2017 年 11 月 21 日 osstech-openam13-13.0.0-91
 - デスクトップ SSO 失敗時に ClassCastException が発生する問題を修正
-

- ForgeRock Authenticator 認証でリカバリーコードを発行しないオプションを追加
 - アダプティブリクス認証のにユーザー属性の存在チェック機能を追加
 - XUI のキャッシュ防止用クエリーパラメーターを修正
 - セッションアップグレード時の認証に失敗すると既存のセッションが破棄される問題を修正
 - デスクトップ SSO が認証連鎖に含まれるときに後続の認証が失敗する問題を修正
 - osstech-openam13-tools パッケージに管理者コマンドを追加
 - 2017 年 10 月 13 日 osstech-openam13-13.0.0-85
 - ssoadm の認証にアダプティブリクスの IP アドレスレンジを利用できない問題を修正
 - OAuth 2.0 Introspection Endpoint のレスポンスに含まれる exp がトークンの有効期限切れとなる時刻を示す値となるよう修正
 - 認証ポストプロセスクラスで設定した認証成功時のリダイレクト先がクエリーパラメータで指定したものよりも優先されるように修正
 - 2017 年 9 月 19 日 osstech-openam13-13.0.0-82
 - IE11 で管理画面からポリシーを編集できない問題の修正
 - 2017 年 9 月 11 日 osstech-openam13-13.0.0-81
 - ForgeRock Authenticator 認証をセッションアップグレードで利用できない問題を修正
 - ForgeRock Authenticator 認証の日本語化
 - ForgeRock Authenticator 認証で生成する QR コードのフォーマットの変更
 - Groovy 及び Groovy Sandbox ライブラリのアップデート
 - 2017 年 5 月 30 日 osstech-openam13-13.0.0-79
 - 認証ポストプロセスで設定した認証成功時の URL に遷移しない問題を修正
 - 秒単位の LDAP タイムアウト設定がミリ秒単位で扱われている問題を修正
 - Client Configuration Endpoint の応答が仕様に準拠していない問題の修正
 - SAML の認証コンテキストクラスの問題を修正
 - OAuth クライアントに関するログ出力の問題を修正
 - ログローテーション用 logrotate 設定の組み込み
 - セッションプロパティのポリシー条件でドットを含むプロパティ名を管理画面から設定できない問題の修正
 - LDAP フィルター条件で Time Limit/Size Limit を適切に利用するように修正
 - 2017 年 3 月 17 日 osstech-openam13-13.0.0-72
-

- UMA Provider のサービス設定をキャッシュするように修正
 - ScriptingService の設定をキャッシュするように修正
 - OIDC/OAuth2.0 認証モジュールで jwk_url 使用時 OP からの応答に x5c が含まれていると認証に失敗する問題の修正
 - CTS の削除スレッドで予期せぬ例外が発生した場合にコネクションをクローズしない問題を修正
 - デフォルトで登録されている認証モジュールのインスタンスを削除すると後から作成した同じ認証モジュールのインスタンスも削除される問題を修正
 - OAuth2.0/OIDC 認証モジュールで jwk_url に応答される json に楕円暗号方式があると認証に失敗する問題を修正
 - ログイン成功 URL へ遷移しない問題を修正
 - 管理画面で作成した認証モジュールと同じ名称のインスタンスを ssoadm から削除できない問題を修正
 - XUI アクセス時のクエリーパラメーターをバージョン情報からハッシュに変更
 - ssoadm/ampassword の java オプションを追加
 - CTS に不正なエントリが存在した場合に削除処理として当該エントリを無視するように修正
 - 2017 年 2 月 14 日 osstech-openam13-13.0.0-62
 - OAuth2/OIDC 認証モジュールで署名にクライアントアントシークレットを使う場合二箇所を設定する必要がある問題を修正
 - 2017 年 2 月 14 日 osstech-openam13-13.0.0-61
 - OpenDJ が changelogDb を読み込めなくなる問題を修正
 - SAML2 認証の内部で呼び出す認証にフォーカスが当たらない問題を修正
 - アダプティブリクス認証の設定画面でタブを切り替えた際に更新前の設定が表示される問題を修正
 - favicon を変更
 - ログイン失敗画面のリンクのクエリーがエンコードされていない問題を修正
 - 認証成功時に sharedState のユーザー名を上書きする機能を OpenLDAP 認証に追加
 - 最初のコールバックが RedirectCallback の場合はセッションタイムアウトで認証失敗画面に遷移するように修正
 - 2017 年 1 月 27 日 osstech-openam13-13.0.0-54
 - RPM アップデート後に XUI のコンテンツをブラウザに更新させるように修正
 - IE で画面が日本語化されない問題を修正
-

- ポリシー条件によりアクセスが拒否される場合にポリシーサービスの結果が欠落する問題を修正
- authId クッキーがタイムアウトしている場合に認証を継続できない問題を修正
- SAML2 認証の内部で呼び出す認証連鎖が失敗すると認証を継続できない問題を修正
- 2017 年 1 月 13 日 osstech-openam13-13.0.0-49
 - OpenID Connect の RP である時に client_secret_post のみに対応するよう修正
 - カスタム認証モジュールで RedirectCallback を複数回利用できない問題を修正
 - OpenID Connect の OP である時にリクエストの acr_values にマップされる認証連鎖が存在しない場合、エラーを応答するように修正
- 2017 年 1 月 5 日 osstech-openam13-13.0.0-46
 - 管理画面の日本語化
 - Cookie ドメインが設定されていない場合でも動作するように修正
 - URL 比較処理の結果を OSSTech OpenAM 11 に合わせる
- 2016 年 12 月 12 日 osstech-openam13-13.0.0-43
 - Fedlet を作成できない問題を修正
 - OpenDJ SDK の Trace レベルのログを抑制する
 - JDK の XML パーサーを利用するように修正
 - OAuth 2.0 の同意画面を表示しないオプションを追加
 - OAuth 2.0 で同意を保存しない設定の場合に同意ページにチェックボックスを表示しない
 - OAuth 2.0 でディスプレイモードを指定した場合に同意ができない問題の修正
 - 統計情報ログが出力されない問題を修正
 - 認証 REST API 用の署名鍵が冗長構成の各サーバーで異なる問題を修正
 - 認証連鎖の途中で認証セッションがタイムアウトした場合にセッションタイムアウトの表示にならない問題を修正
 - NullPointerException が発生する問題を修正
 - 一般ユーザーのセッション毎に余分な権限キャッシュを取得していた問題を修正
 - OpenID Connect id_token bearer 認証の設定ができない問題を修正
 - 管理画面で設定項目の順序が崩れる問題を修正
 - Fedlet を従来通りのアーカイブで作成するように修正
 - AuditLog に出力される時刻を JST にするオプションの追加
 - ログイン時の XUI のレルム判定処理で DNS エイリアスを考慮するように修正
 - OpenID Connect の OP である時にセッションアップグレードをすると acr_values

の認証連鎖が有効にならない

- ログイン画面の日本語化
 - 2016年10月19日 osstech-openam13-13.0.0-28
 - サイト構成時にステートレスセッションが発行されない問題を修正
 - 2016年10月18日 osstech-openam13-13.0.0-27
 - データストアキャッシュの有効期限を設定するとデッドロックが発生する問題を修正
 - OpenDJ のエラーログが出力されない問題を修正
 - OpenJDK のバージョンを 8 に変更
 - セキュリティ脆弱性の修正 (OpenAM Security Advisory #201608)
 - アップグレード時に OAuth Provider の設定が作成される問題を修正
 - 2016年9月26日 osstech-openam13-13.0.0-23
 - XUI のログイン画面で発生する XSS の問題を修正
 - 2016年9月7日 osstech-openam13-13.0.0-22
 - セキュリティ脆弱性の修正 (OpenAM Security Advisory #201605)
 - (ただし、Issue #201605-06 を除く)
 - 2016年7月26日 osstech-openam13-13.0.0-14
 - Self Service のトークンを別の号機や再起動後に処理できない問題を修正
 - ForgeRock Commons ライブラリのアップデート
 - 2016年7月15日 osstech-openam13-13.0.0-13
 - セキュリティ脆弱性の修正 (OpenAM Security Advisory #201604)
 - 2016年4月1日 osstech-openam13-13.0.0-7
 - OpenLDAP 認証利用時、XUI のログイン画面にパスワードリセットのリンクが表示されない問題を修正
 - アカウントロックの挙動の問題を修正
 - 2016年3月11日 osstech-openam13-13.0.0-5
 - セッションフォワード時の文字エンコードの問題を修正
 - ログを syslog に出力しているとハングする場合がある問題を修正
 - SAML のエンドポイントにアクセスする際に realm パラメーターを付与すると ClassCastException が発生する問題を修正
 - パーシステントサーチのコネクションが切断された場合に復帰しない問題を修正
 - 未認証状態で encode.jsp にアクセスすると goto が showServerConfig.jsp になる問題を修正
 - 2016年3月11日 osstech-openam13-13.0.0-0
-



– OSSTech OpenAM 13.0.0 新規作成