OSSTech OpenAM 14 リリースノート

OSSTech(株)

更新日 2024 年 10 月 11 日

目次

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-openam14-14.5.0-52 です。

このパッケージは OpenAM コンソーシアム版 OpenAM 14.0.0 のソースコードをベースとしています。コンソーシアム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://github.com/openam-jp/openam/wiki/OpenAM-14.0.0-%E3%83%AA%E3%83%AA%E3%83%BC%E3%82%B9%E3%83%8E%E3%83%BC%E3%83%88

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-openam14
osstech-openam14-14.5.0-52.el8.noarch
```

2 OSSTech OpenAM 14.5 の新機能

本章では OSSTech OpenAM 14.5 の新機能について説明します。

2.1 学認連携への対応

OSSTech OpenAM 14.5 では学術認証フェデレーションとの連携に対応するために Shibboleth IdP 互換の機能が追加されました。

- 送信属性同意機能
- メタデータ自動更新機能
- eduPersonTargetedID (ComputedId) 送信機能
- SAML2 リモート SP 新規登録時の初期値を定義する機能

2.2 SAML2 のエンハンス

OSSTech OpenAM 14.5 では従来 OpenAM サーバー全体か IdP 毎に設定していた項目を SP 毎に設定できるようになりました。 SAML IdP として、より柔軟に運用することが可能です。

- SP に NameID 値マップを設定する機能
- IdP / SP 毎に署名アルゴリズムを指定する機能
- ポリシー保護機能を SP 毎に有効化する機能

2.3 OAuth 2.0 / OpenID Connect のエンハンス

OSSTech OpenAM 14.5 では利用しないグラントタイプや Dynamic Client Registration を無効化できるようになりました。 OP として、より細やかな制御が可能です。

2.4 ダッシュボードからのデバイス登録機能

OSSTech OpenAM 14.5 では FIDO2 や FrOATH のデバイスをダッシュボード画面から登録／再登録できます。機種変更の際にデバイスの設定を移行できない場合でも、簡単に新しい機器を認証デバイスとして登録しなおす事ができます。

2.5 ユーザーネームレス認証を Safari でサポート

OSSTech OpenAM 14.5 では Safari で WebAuthn のユーザーネームレス認証 (ディスカバラブル・クレデンシャル) が動作するようになりました。

Safari では WebAuthn API が動作する前にユーザーインタラクションが必要な仕様となっています。ユーザーネームレス認証を有効にした場合、従来はログイン画面の初期表示で WebAuthn API を動作させていましたが、 14.5 ではユーザーがボタンを押下した後に API が動作するようになりました。

3 OSSTech OpenAM 14.2 の新機能

本章では OSSTech OpenAM 14.2 の新機能について説明します。

3.1 Microsoft 365 向け設定ウィサード

OSSTech OpenAM 14.2 では Microsoft 365 を SAML SP として設定するウィサードが追加されました。

ウィザードでは Microsoft 365 連携に必要な設定を入力できます。また、PowerShell で実行すべきコマンドが表示されるため、従来よりも簡単に Microsoft 365 との SAML 連携を構成できます。

3.2 ユーザーのダッシュボードのエンハンス

OSSTech OpenAM 14.2 ではユーザーのダッシュボード画面のエンハンスを行いました。

新しいダッシュボード画面では表示されるマイアプリケーションのソートやグループ化が可能です。対応する LDAP 属性のプロビジョニングにより管理者がユーザーに表示させるアプリケーションのグループ／順序を定義することができます。また、設定によってユーザー自身がグループ／順序を決めることも可能です。

3.3 マイアプリケーション用スクリプト機能

OSSTech OpenAM 14.2 ではユーザーのダッシュボード画面に表示されるアプリケーションを条件によって切り換えることができるスクリプト機能が追加されました。

IP アドレスによる社内／社外の判定やユーザーの属性による権限の判定の結果によって必要なアプリケーションを抽出してダッシュボード画面に表示させることが可能です。

3.4 初期設定画面のリニューアル

OSSTech OpenAM 14.2 では初期設定画面及びアップグレード画面をリニューアルしました。

リニューアルにより UI が更新されています。ただし、設定手順は従来と同様です。また、利用している JavaScript ライブラリの関係上、Internet Explorer はサポート対象外となります。 OpenAM の管理用端末に IE のみがインストールされている環境では他のブラウザーをご用意いただくか、コマンドラインツールによるセットアップ／アップグレードをご検討ください。

4 OSSTech OpenAM 14.1 の新機能

本章では OSSTech OpenAM 14.1 の新機能について説明します。

4.1 SMS OTP 認証

OSSTech OpenAM 14.1 では SMS OTP 認証モジュールが追加されました。

従来の OpenAM ではワンタイムパスワードの送信方式としてメールのみがサポートされていました。本モジュールでは Short Message Service (SMS) を利用して、ユーザーのスマートフォンへワンタイムパスワードを送信することが可能です。

なお、SMS の送信には Amazon Simple Notification Service を利用します。

4.2 ID 認証

OSSTech OpenAM 14.1 では ID 認証モジュールが追加されました。

従来の認証方法では、ユーザーを特定するためにデータストア認証モジュールや OpenLDAP 認証モジュールのような ID とパスワードを用いる認証が必要でした。 そのため、ID とワンタイムパスワードを組み合わせた認証連鎖を実現できませんでした。本モジュールは ID のみを用いてユーザーを特定するため、ID とワンタイムパスワードのようなを実現できます。より柔軟に認証連鎖を設定できるようになりました。

4.3 Touch ID、Face ID を利用した際の Attestation に対応

2021 年 4 月 8 日に W3C 勧告の WebAuthn Level 2 に追加された、Apple Anonymous Attestation に対応しました。 OSSTech OpenAM 14.1 の WebAuthn 認証は Touch ID、Face ID の搭載された Apple 製品を認証器としてサポートします。

4.4 多要素認証を一定期間省略する機能

OSSTech OpenAM 14.1 では持続 Cookie 認証モジュールに多要素認証を一定期間省略する機能が追加されました。

持続 Cookie 認証モジュールは、認証成功時にユーザー情報を JWT として有効期限付きの Cookie に保存し、次回以降の認証時にその Cookie を利用して認証するモジュールです。従来は認証を一定期間省略する機能がありましたが、新機能として多要素認証を一定期間省略する機能が追加されました。

また、多要素認証の省略をユーザーに選択させる機能も追加しています。

4.5 位置情報を履歴と比較するリスクベース認証

OSSTech OpenAM 14.1 ではアダプティブリスク認証モジュールに位置情報を履歴と比較する機能が追加されました。

従来のアダプティブリスク認証にも位置情報を利用したリスクベース認証がありましたが、クライアントの IP アドレスから識別した国コードを設定値と比較する機能でした。新機能では、過去の認証で識別した国コードを履歴としてユーザー属性に保存しておき、認証時に比較することができます。

4.6 リスクの高いログイン成功時に警告メールを送信する機能

OSSTech OpenAM 14.1 ではアダプティブリスク認証モジュールに、リスクの高いログイン成功時に警告メールを送信する機能が追加されました。

新機能では、アダプティブリスク認証でリスクが高いとして失敗した後、追加の認証が成功した場合に「リスクの高いログイン成功」として警告メールをユーザーに送信することができます。

4.7 音声 OTP 認証

OSSTech OpenAM 14.1 では Voice OTP 認証モジュールが追加されました。

従来の OpenAM ではワンタイムパスワードの送信方式としてメールのみがサポートされていました。本モジュールでは音声通話を利用して、ユーザーの電話機へワンタイムパスワードを送信することが可能です。

なお、音声通話によるワンタイムパスワードの送信には Amazon Pinpoint を利用します。

5 最新の修正内容

OSSTech 提供の OpenAM 14.5.0-52 では以下の修正を行いました。

5.1 コンソーシアム版 14.0.0 以降に統合される修正（バックポート）

なし

5.2 OSSTech 独自の修正

- サイトの URL が認識されない場合がある問題を修正

6 コンソーシアム版との差異

OSSTech 提供の OpenAM 14.x はコンソーシアム版 OpenAM 14.0.0 と以下の差異があります。

6.1 コンソーシアム版 14.0.0 以降に統合される修正（バックポート）

- Cookie ドメインが設定されていない場合にいくつかの認証モジュールが動作しない問題を修正
  - https://github.com/openam-jp/openam/issues/11
- 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
  - https://github.com/openam-jp/openam/issues/46
- Client Configuration Endpoint の応答が仕様に準拠していない問題の修正
  - https://github.com/openam-jp/openam/issues/53
- 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
  - https://github.com/openam-jp/openam/issues/56
- 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
  - https://github.com/openam-jp/openam/issues/59
- SAML2 認証で NullPointerException が発生する問題を修正
  - https://github.com/openam-jp/openam/issues/63
- Google Apps の表示を G Suite に更新
  - https://github.com/openam-jp/openam/issues/93
- 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
  - https://github.com/openam-jp/openam/issues/111
- メンバーシップポリシー条件の設計画面の改善
  - https://github.com/openam-jp/openam/issues/125
- OAuth2 プロバイダー設定のサポートするスコープ／クレームの項目がホットスワップではない問題の修正
  - https://github.com/openam-jp/openam/issues/138
- OpenAM が発行する Cookie に SameSite 属性を付与する機能を追加
  - https://github.com/openam-jp/openam/issues/206
- 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

- OAuth2/OIDC 認証の PKCE 対応
  - https://github.com/openam-jp/openam/issues/230
- 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
- アクセス制御の不備の脆弱性を修正
  - https://github.com/openam-jp/openam/issues/283
- ECDSA で署名された JWT の署名検証に失敗する場合がある問題を修正
  - https://github.com/openam-jp/forgerock-commons/issues/21
- OAuth 2.0 におけるテンプレートインジェクションの脆弱性を修正
  - https://github.com/openam-jp/openam/issues/298
- SAML 1.x におけるなりすましの脆弱性を修正
  - https://github.com/openam-jp/openam/issues/286

6.2 OSSTech 独自の修正

- ロゴ / favicon 等の変更
- 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
- 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
- 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
- 旧画面のログイン／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
- SAML 2.0 ／ OAtuth 2.0 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
- 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

- SAML2 認証が出力するデバッグログの一部を抑制
- 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
- 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
- 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
- CDSSO で SunQueryParamsString がエンコードされない問題を修正
- Fedlet を従来通りのアーカイブで作成するように修正
- URL 比較処理の結果を OSSTech OpenAM 11 に合わせる
- 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
- RPM アップデート後に XUI のコンテンツをブラウザーに更新させるように修正
- 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
- 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
- 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
- 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
- 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
- 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
- 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
- SAML2 認証が出力するデバッグログの一部を抑制
- 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
- 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
- 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

- 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
- ForgeRock Authenticator 認証のログ出力の改善
- REST API のセッションエンドポイントの改善
- 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
- ユーザーキャッシュタイムアウトのデフォルト値を変更
- HOTP 認証で OTP 入力を複数回試行可能にする設定を追加
- Red Hat Enterprise Linux 8 / CentOS 8 をサポート
- パッケージが依存する Java 環境を OpenJDK 11 に変更
- パッケージが依存するサーブレットコンテナを OSSTech Tomcat 9 に変更
- ログインページで表示する選択画面をラジオボタンからドロップダウンリストに変更
- ポリシー設定サービスの TLS バージョンのデフォルトを TLSv1.2 に変更
- 認証連鎖分岐モジュールを追加
- LINE OTP 認証モジュールを追加
- PKCE を OAuth Client 毎に有効化する設定を追加
- 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設定を追加
- 管理画面に表示される PKCE のリンクを修正
- LINE OTP 認証を認証連鎖分岐モジュールで利用できない問題を修正
- PKCE の code_challenge_method パラメーターがオプショナルとして扱われていない問題を修正
- 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
- LINE OTP を認証連鎖分岐モジュールで利用すると確認画面の表示が崩れる問題を修正
- アダプティブリスクのエラーメッセージをカスタマイズする機能を追加
- ダッシュボードで Internal Server Error と表示される問題を修正
- FrOATH 認証のデバイス登録時に鍵文字列を表示する画面を追加
- FrOATH 認証のデフォルトの鍵サイズを変更
- プロパティファイルに関連する例外処理の改善
- 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
- SMS OTP 認証モジュールを追加

- データストア認証及び OpenLDAP 認証に認証連鎖の中で特定された ID を引き継ぐ機能を追加
- ダッシュボードの表示で AuthenticatorWebAuthnService デバッグログが肥大化する問題を修正
- 特定のサーブレットの初期化に失敗する問題を修正
- 冗長構成時にセッション数をカウントするデフォルトの挙動を変更
- ID 認証モジュールを追加
- Linux + Chrome 環境で Yubikey 5 のレジデントキー登録に失敗する問題を修正
- SAML でメモリーリークが発生する問題を修正
- G Suite の設定時に IdP の NameID マッピングを更新しないように修正
- データストアのユーザー属性として entryUUID を設定せずに WebAuthn を利用すると NullPointerException が発生する問題を修正
- 共通タスクが意図していない言語で表示される問題を修正
- データストア認証及び OpenLDAP 認証でパスワードのみの入力を求める場合に特定されたユーザー名を表示するように修正
- 持続 Cookie の発行有無を選択する認証モジュールを追加
- メッセージ表示にエスケープ処理を追加
- 初期設定画面でドットから始まる Cookie ドメインを許容しないように修正
- OAuth2 認証の Scope のデフォルト値をカンマではなくスペース区切りに修正
- war 単体でデプロイできない問題を修正
- WebAuthn 登録／認証でブラウザーが WebAuthn をサポートしていない場合に自動でキャンセル処理を行うように修正
- Fedlet が動作しない問題を修正
- webauthn.js がトランスパイルされていない問題を修正
- 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
- アダプティブリスク認証の設定画面がセクションで区切られていない問題を修正
- SAML NameID としてセッションプロパティを利用する機能を追加
- OSSTech 独自認証モジュールがアップグレードした環境で有効にならない問題を修正
- 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
- 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
- OAuth2 認証のデフォルトの設定値を変更

- WebAuthn 認証及び ID 認証のログイン画面にユーザー名を記録する機能を追加
- SecurID のエラーがデバッグログに出力される問題を修正
- サブレルムにプロバイダーポリシーセットを作成できない問題を修正
- DNS エイリアスの設定時に重複チェックを行うように修正
- データストアの検索属性を uid から変更している場合にダッシュボードにデバイスが表示されない問題を修正
- アカウントロックの持続時間を設定した場合もロックアウト属性を確認するように修正
- SAML2 IdP のポリシー保護機能で NullPointerException が発生する問題を修正
- アダプティブリスク認証に位置情報を履歴と比較する機能を追加
- アダプティブリスク認証でリスクの高いログイン成功時に警告メールを送信する機能を追加
- 一部の REST API のエラー応答を修正
- セッションチェック認証モジュールを追加
- アダプティブリスク認証の設定（位置情報履歴の履歴サイズ）で設定可能な最大値を変更
- ssoadm でレルムを作成できない問題を修正
- SAML2 シングルログアウトで RelayState が失われる問題を修正
- ssoadm で重複した DNS エイリアスを設定できる問題を修正
- 複数の SAML SP に対して SSO 状態からのシングルログアウトで RelayState が失われる問題を修正
- アダプティブリスクの認証失敗チェックで NullPointerException が発生する問題を修正
- ID 認証モジュールののエラーメッセージをカスタマイズする機能を追加
- WebFinger の脆弱性 (CVE-2021-29156) を修正
- OpenAM 停止時に ClassCastException が発生する問題を修正
- Attestation の設定によって WebAuthn 認証が iOS で動作しない問題を修正
- FrOATH 認証のスキップ機能のデフォルト無効化
- Voice OTP 認証を追加
- OpenAM 起動時の Session デバッグログへの不要な出力を修正
- OATH 認証及び FrOATH 認証のデフォルト値を変更
- Microsoft 365 を SAML SP として設定するウィザードを追加
- デスクトップ SSO の認証連鎖でログイン失敗 URL が動作しない問題を修正
- 設定画面でオートコンプリートが動作する問題を修正

- 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
- SAML における XML インジェクションの脆弱性を修正
- ID を指定可能な認証モジュールが複数ある認証連鎖の構成で、データストアに存在する ID と存在しない ID が指定された場合の動作を修正
- ワンタイムパスワード用のテンプレート HTML を追加
- クロスサイトスクリプティングの脆弱性を修正
- FrOATH 認証の入力欄の autocomplete 属性を one-time-code に変更
- 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
- ユーザーのダッシュボード画面のエンハンス
- 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/
- マイアプリケーションのソートが Android で動作しない問題を修正
- マイアプリケーションに表示する内容を条件によって変更するスクリプト機能を追加
- セキュリティトークンサービスで SAML2 トークンを発行する場合に NameID として利用する属性を設定する機能を追加
- OpenDJ が changelogDb に書き込む際の同期制御を修正
- OAuth 2.0 デバイフローの処理を修正
- マイアプリケーションのリンクを別タブで開くように変更
- REST API のエラー応答を調整
- エージェントのセッションが破棄されている場合にユーザーがセッション数制限でログインできない問題を修正
- 初期設定画面のリニューアル
- OAuth 2.0 の処理にリソースオーナーのステータスチェックを追加
- マイアプリケーションの表示内容を変更するスクリプトにタブ・ソート情報を返却する機能を追加
- アップグレード処理の修正
- マイアプリケーションの表示内容を変更するスクリプトにセッションプロパティを参照する機能を追加
- ログイン成功時の URL を XUI のパスに変更すると表示できない問題を修正
- SAML2 プロバイダーの作成画面にベース URL の入力欄を追加
- SP に送付する属性を生成するスクリプト機能を追加
- ポリシー設定サービスにセカンダリ LDAP サーバーの設定欄を追加
- SAML SP に NameID 値マップの設定欄を追加

- ログアウト URL におけるパラメーターの処理を修正
- OpenLDAP データストアの持続検索のバグを修正
- SAML2 送信属性同意機能を追加
- OAuth 2.0 プロバイダー及びクライアントにサポートするグラントタイプを指定する機能を追加
- ダッシュボード画面から FrOATH デバイスを登録・再登録する機能を追加
- SAML2 のポリシー保護機能を SP 毎に有効化する機能を追加
- アップグレード画面が表示されない問題を修正
- SAML 属性をエスケープせずに送信する機能を追加
- グローバルサービスにある OAuth 2.0 プロバイダーのグラントタイプ設定を変更できない問題を修正
- OAuth 2.0 プロバイダーのグラントタイプ設定がアップグレードで期待通りに設定されない問題を修正
- 高多重ログイン時に認証連鎖分岐モジュールが失敗する問題を修正
- SAML IdP 及び IdP プロキシの AuthnContext 判定処理を修正
- OIDC Dynamic Client Registration を無効化するオプションを追加
- 認証連鎖分岐モジュールや SAML2 認証で余分なセッションが残る問題を修正
- reCAPTCHA v3 認証を追加
- SAML2 メタデータ自動更新機能を追加
- WebAuthn デバイスを検索する際の LDAP フィルターから objectClass を削除
- SAML2 リモート IdP の表明処理のページを表示できない問題を修正
- SAML2 リモート SP 新規登録時の初期値を定義する機能を追加
- WebAuthn 認証をディスカバラブル・クレデンシャルで利用する場合、ユーザーがボタンを押下した後に WebAuthn API が動作するように修正
- OpenDJ の管理者ポートが利用する証明書の署名アルゴリズムを SHA-256 に変更
- SAML2 IdP / SP 毎に署名アルゴリズムを指定する機能を追加
- LDAP ユーザー検索属性を変更すると OpenLDAP データストアのパーシステントサーチが動作しない問題を修正
- SAML2 リモートプロバイダーの設定を変更できない問題を修正
- ダッシュボード画面から FIDO2 デバイスを登録する機能を追加
- SP に送付する属性を生成するスクリプトに Shibboleth ComputedId を生成する機能を追加
- WebAuthn 認証に transports を送信するかどうかの設定を追加
- SAML2 送信属性同意画面にロゴが表示されない問題を修正

- WebAuthn 認証の Resident Key の表記を Discoverable Credential に変更
- SMS OTP 認証がユーザーキャッシュを無効化している環境で動作しない問題を修正
- クエリパラメーターでレルム名を指定した場合にダッシュボード画面が正常に表示されない問題を修正
- トラストサークルの編集画面で設定の保存に失敗する場合がある問題を修正
- SMS OTP 認証の Web OTP API 対応
- OAuth 2.0 デバイスフローのデバイス認可リクエストで response_type パラメーターが必須となっている問題を修正
- SMS OTP 認証がエラーを出力することなく OTP 送信に失敗する場合がある問題を修正
- 認証モジュールのインスタンス作成時にデフォルト設定が反映されない問題を修正
- SAML2 送信属性同意画面にスクリプトで定義した値が表示されない問題を修正
- ユーザーセルフサービスでユーザー属性を更新時、LDAP サーバーから Constraint violation が応答された場合に内部サーバーエラーと表示される問題を修正
- ユーザープロファイル画面の JavaScript に Internet Explorer で動作しない処理が含まれている問題を修正
- SAML2 の署名に使用するダイジェストアルゴリズムを IdP / SP 毎の署名アルゴリズムに基づいて決定するように変更
- Red Hat Enterprise Linux 9 / AlmaLinux 9 / Rocky Linux 9 をサポート
- ssoadm で SAML2 のメタデータをエクスポートする際に日本語が文字化けする問題を修正
- データストアの設定を REST API で行うためのエンドポイントを追加
- SAML2 送信属性同意画面に NameID の XML 文字列の代わりに ID を表示するように変更
- SAML2 送信属性同意機能が無効な場合も証明書が読み込まれる問題を修正
- 暗号化された SAML2 メッセージの復号に失敗した際に出力されるデバッグログの一部を抑制
- SAML2 メタデータ自動更新が一日に複数回実行される問題を修正
- 認証モジュール、データストア、WebAuthn Authenticator サービスの設定画面から LDAPS のプロトコルバージョンの設定を削除
- グローバルサービスのセカンダリ設定インスタンスの中のセカンダリ設定インスタンスの設定を REST API で行うためのエンドポイントを追加
- REST API でグローバルサービスのダッシュボードのセカンダリ設定インスタンスのスキーマを取得できない問題を修正

- ID 認証モジュールの認証画面でユーザー名が空の場合はログインボタンを押下できないように変更
- REST API の応答に含まれる _id の値が小文字になる場合がある問題を修正
- サービス運用妨害 (DoS) の脆弱性を修正
- 認証モジュール設定取得 API で存在しない認証モジュール名を指定した場合に設定値が返却される問題を修正
- Fedlet が動作しない問題を修正
- 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
- OpenJDK 11 非互換問題の修正
- データベースリポジトリが他のデータベースリポジトリの初期化失敗の影響で正常に動作しなくなる問題を修正
- OpenJDK 21 上で動作するように変更 (el7 パッケージの OpenAM 14.x は対象外)
- Windows デスクトップ SSO 認証モジュールに特定のエラーメッセージの出力を抑制する機能を追加
- ユーザーの管理を REST API で行うためのエンドポイントを追加
- データストアの LDAP ユーザー検索属性を変更すると管理画面でグループからメンバーを削除できなくなる問題を修正
- トラストサークルを管理するための REST API が応答するスキーマに誤りがある問題を修正
- Java のバージョンに依存して OpenAM が起動しない問題を修正
- CTS のモニタリングでメモリーリークが発生する問題を修正
- OpenJDK 21 上で SAML 1.x の Browser/Artifact Profile が動作しない問題を修正
- グループの管理を REST API で行うためのエンドポイントを追加
- SAML2 の認証要求に NameIDPolicy が含まれない場合に SP の NameID 値マップが適用されない問題を修正
- サイトの URL が認識されない場合がある問題を修正

7 パッケージ更新履歴

- 2024 年 10 月 11 日 osstech-openam14-14.5.0-52
  - サイトの URL が認識されない場合がある問題を修正
- 2024 年 8 月 29 日 osstech-openam14-14.5.0-50
  - グループの管理を REST API で行うためのエンドポイントを追加
  - SAML2 の認証要求に NameIDPolicy が含まれない場合に SP の NameID 値マップが適用されない問題を修正
- 2024 年 8 月 14 日 osstech-openam14-14.5.0-48
  - OAuth 2.0 におけるテンプレートインジェクションの脆弱性を修正
  - SAML 1.x におけるなりすましの脆弱性を修正
  - Windows デスクトップ SSO 認証モジュールに特定のエラーメッセージの出力を抑制する機能を追加
  - ユーザーの管理を REST API で行うためのエンドポイントを追加
  - データストアの LDAP ユーザー検索属性を変更すると管理画面でグループからメンバーを削除できなくなる問題を修正
  - トラストサークルを管理するための REST API が応答するスキーマに誤りがある問題を修正
  - Java のバージョンに依存して OpenAM が起動しない問題を修正
  - CTS のモニタリングでメモリーリークが発生する問題を修正
  - OpenJDK 21 上で SAML 1.x の Browser/Artifact Profile が動作しない問題を修正
- 2024 年 6 月 7 日 osstech-openam14-14.5.0-39
  - OpenJDK 21 上で動作するように変更 (el7 パッケージの OpenAM 14.x は対象外)
- 2024 年 4 月 30 日 osstech-openam14-14.5.0-38
  - データベースリポジトリが他のデータベースリポジトリの初期化失敗の影響で正常に動作しなくなる問題を修正
- 2024 年 2 月 22 日 osstech-openam14-14.5.0-37
  - OpenJDK 11 非互換問題の修正
- 2024 年 1 月 19 日 osstech-openam14-14.5.0-33
  - サービス運用妨害 (DoS) の脆弱性を修正
  - 認証モジュール設定取得 API で存在しない認証モジュール名を指定した場合に設定値が返却される問題を修正
  - Fedlet が動作しない問題を修正

  - 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 11 月 29 日 osstech-openam14-14.5.0-28
  - ECDSA で署名された JWT の署名検証に失敗する場合がある問題を修正
  - SAML2 メタデータ自動更新が一日に複数回実行される問題を修正
  - 認証モジュール、データストア、WebAuthn Authenticator サービスの設定画面から LDAPS のプロトコルバージョンの設定を削除
  - グローバルサービスのセカンダリ設定インスタンスの中のセカンダリ設定インスタンスの設定を REST API で行うためのエンドポイントを追加
  - REST API でグローバルサービスのダッシュボードのセカンダリ設定インスタンスのスキーマを取得できない問題を修正
  - ID 認証モジュールの認証画面でユーザー名が空の場合はログインボタンを押下できないように変更
  - REST API の応答に含まれる _id の値が小文字になる場合がある問題を修正
- 2023 年 8 月 31 日 osstech-openam14-14.5.0-21
  - SAML2 送信属性同意画面に NameID の XML 文字列の代わりに ID を表示するように変更
  - SAML2 送信属性同意機能が無効な場合も証明書が読み込まれる問題を修正
  - 暗号化された SAML2 メッセージの復号に失敗した際に出力されるデバッグログの一部を抑制
- 2023 年 6 月 16 日 osstech-openam14-14.5.0-18
  - SAML2 の署名に使用するダイジェストアルゴリズムを IdP / SP 毎の署名アルゴリズムに基づいて決定するように変更
  - Red Hat Enterprise Linux 9 / AlmaLinux 9 / Rocky Linux 9 をサポート
  - ssoadm で SAML2 のメタデータをエクスポートする際に日本語が文字化けする問題を修正
  - データストアの設定を REST API で行うためのエンドポイントを追加
- 2023 年 4 月 24 日 osstech-openam14-14.5.0-14
  - ユーザーセルフサービスでユーザー属性を更新時、LDAP サーバーから Constraint violation が応答された場合に内部サーバーエラーと表示される問題を修正
  - ユーザープロファイル画面の JavaScript に Internet Explorer で動作しない処理が含まれている問題を修正

- 2023 年 3 月 29 日 osstech-openam14-14.5.0-12
  - 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
  - アクセス制御の不備の脆弱性を修正
  - クエリパラメーターでレルム名を指定した場合にダッシュボード画面が正常に表示されない問題を修正
  - トラストサークルの編集画面で設定の保存に失敗する場合がある問題を修正
  - SMS OTP 認証の Web OTP API 対応
  - OAuth 2.0 デバイスフローのデバイス認可リクエストで response_type パラメーターが必須となっている問題を修正
  - SMS OTP 認証がエラーを出力することなく OTP 送信に失敗する場合がある問題を修正
  - 認証モジュールのインスタンス作成時にデフォルト設定が反映されない問題を修正
  - SAML2 送信属性同意画面にスクリプトで定義した値が表示されない問題を修正
- 2023 年 1 月 12 日 osstech-openam14-14.5.0-1
  - SMS OTP 認証がユーザーキャッシュを無効化している環境で動作しない問題を修正
- 2022 年 12 月 21 日 osstech-openam14-14.5.0-0
  - SAML2 送信属性同意機能を追加
  - OAuth 2.0 プロバイダー及びクライアントにサポートするグラントタイプを指定する機能を追加
  - ダッシュボード画面から FrOATH デバイスを登録・再登録する機能を追加
  - SAML2 のポリシー保護機能を SP 毎に有効化する機能を追加
  - アップグレード画面が表示されない問題を修正
  - SAML 属性をエスケープせずに送信する機能を追加
  - グローバルサービスにある OAuth 2.0 プロバイダーのグラントタイプ設定を変更できない問題を修正
  - OAuth 2.0 プロバイダーのグラントタイプ設定がアップグレードで期待通りに設定されない問題を修正
  - 高多重ログイン時に認証連鎖分岐モジュールが失敗する問題を修正
  - SAML IdP 及び IdP プロキシの AuthnContext 判定処理を修正
  - OIDC Dynamic Client Registration を無効化するオプションを追加
  - 認証連鎖分岐モジュールや SAML2 認証で余分なセッションが残る問題を修正

  - reCAPTCHA v3 認証を追加
  - SAML2 メタデータ自動更新機能を追加
  - WebAuthn デバイスを検索する際の LDAP フィルターから objectClass を削除
  - SAML2 リモート IdP の表明処理のページを表示できない問題を修正
  - SAML2 リモート SP 新規登録時の初期値を定義する機能を追加
  - WebAuthn 認証をディスカバラブル・クレデンシャルで利用する場合、ユーザーがボタンを押下した後に WebAuthn API が動作するように修正
  - OpenDJ の管理者ポートが利用する証明書の署名アルゴリズムを SHA-256 に変更
  - SAML2 IdP / SP 毎に署名アルゴリズムを指定する機能を追加
  - LDAP ユーザー検索属性を変更すると OpenLDAP データストアのパーシステントサーチが動作しない問題を修正
  - SAML2 リモートプロバイダーの設定を変更できない問題を修正
  - ダッシュボード画面から FIDO2 デバイスを登録する機能を追加
  - SP に送付する属性を生成するスクリプトに Shibboleth ComputedId を生成する機能を追加
  - WebAuthn 認証に transports を送信するかどうかの設定を追加
  - SAML2 送信属性同意画面にロゴが表示されない問題を修正
  - WebAuthn 認証の Resident Key の表記を Discoverable Credential に変更
- 2022 年 8 月 23 日 osstech-openam14-14.2.0-16
  - ログイン成功時の URL を XUI のパスに変更すると表示できない問題を修正
  - SAML2 プロバイダーの作成画面にベース URL の入力欄を追加
  - SP に送付する属性を生成するスクリプト機能を追加
  - ポリシー設定サービスにセカンダリ LDAP サーバーの設定欄を追加
  - SAML SP に NameID 値マップの設定欄を追加
  - ログアウト URL におけるパラメーターの処理を修正
  - OpenLDAP データストアの持続検索のバグを修正
- 2022 年 5 月 13 日 osstech-openam14-14.2.0-2
  - マイアプリケーションの表示内容を変更するスクリプトにセッションプロパティを参照する機能を追加
- 2022 年 5 月 2 日 osstech-openam14-14.2.0-0
  - セキュリティトークンサービスで SAML2 トークンを発行する場合に NameID として利用する属性を設定する機能を追加
  - OpenDJ が changelogDb に書き込む際の同期制御を修正

  - OAuth 2.0 デバイフローの処理を修正
  - マイアプリケーションのリンクを別タブで開くように変更
  - REST API のエラー応答を調整
  - エージェントのセッションが破棄されている場合にユーザーがセッション数制限でログインできない問題を修正
  - 初期設定画面のリニューアル
  - OAuth 2.0 の処理にリソースオーナーのステータスチェックを追加
  - マイアプリケーションの表示内容を変更するスクリプトにタブ・ソート情報を返却する機能を追加
  - アップグレード処理の修正
- 2022 年 1 月 26 日 osstech-openam14-14.1.0-19
  - マイアプリケーションのソートが Android で動作しない問題を修正
  - マイアプリケーションに表示する内容を条件によって変更するスクリプト機能を追加
- 2021 年 12 月 20 日 osstech-openam14-14.1.0-17
  - OAuth2/OIDC 認証の PKCE 対応
  - FrOATH 認証の入力欄の autocomplete 属性を one-time-code に変更
  - 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
  - ユーザーのダッシュボード画面のエンハンス
  - アクセス制御の不備の脆弱性を修正
- 2021 年 9 月 28 日 osstech-openam14-14.1.0-11
  - クロスサイトスクリプティングの脆弱性を修正
- 2021 年 9 月 13 日 osstech-openam14-14.1.0-10
  - ワンタイムパスワード用のテンプレート HTML を追加
- 2021 年 8 月 31 日 osstech-openam14-14.1.0-9
  - ID を指定可能な認証モジュールが複数ある認証連鎖の構成で、データストアに存在する ID と存在しない ID が指定された場合の動作を修正
- 2021 年 8 月 18 日 osstech-openam14-14.1.0-8
  - 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 6 日 osstech-openam14-14.1.0-7
  - 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
- 2021 年 7 月 28 日 osstech-openam14-14.1.0-4
  - デスクトップ SSO の認証連鎖でログイン失敗 URL が動作しない問題の修正を

更新

- 2021 年 7 月 5 日 osstech-openam14-14.1.0-3
  - Microsoft 365 を SAML SP として設定するウィザードを追加
  - デスクトップ SSO の認証連鎖でログイン失敗 URL が動作しない問題を修正
  - 設定画面でオートコンプリートが動作する問題を修正
- 2021 年 5 月 27 日 osstech-openam14-14.1.0-0
  - Attestation の設定によって WebAuthn 認証が iOS で動作しない問題を修正
  - FrOATH 認証のスキップ機能のデフォルト無効化
  - Voice OTP 認証を追加
  - OpenAM 起動時の Session デバッグログへの不要な出力を修正
  - OATH 認証及び FrOATH 認証のデフォルト値を変更
  - ロゴの更新
- 2021 年 5 月 6 日 osstech-openam14-14.0.0-74
  - ID 認証モジュールののエラーメッセージをカスタマイズする機能を追加
  - WebFinger の脆弱性 (CVE-2021-29156) を修正
  - OpenAM 停止時に ClassCastException が発生する問題を修正
- 2021 年 3 月 19 日 osstech-openam14-14.0.0-71
  - ssoadm で重複した DNS エイリアスを設定できる問題を修正
  - 複数の SAML SP に対して SSO 状態からのシングルログアウトで RelayState が失われる問題を修正
  - アダプティブリスクの認証失敗チェックで NullPointerException が発生する問題を修正
- 2021 年 2 月 16 日 osstech-openam14-14.0.0-68
  - ssoadm でレルムを作成できない問題を修正
  - SAML2 シングルログアウトで RelayState が失われる問題を修正
- 2021 年 2 月 3 日 osstech-openam14-14.0.0-66
  - 一部の REST API のエラー応答を修正
  - セッションチェック認証モジュールを追加
  - アダプティブリスク認証の設定（位置情報履歴の履歴サイズ）で設定可能な最大値を変更
- 2021 年 1 月 18 日 osstech-openam14-14.0.0-63
  - SAML2 IdP のポリシー保護機能で NullPointerException が発生する問題を修正
  - アダプティブリスク認証に位置情報を履歴と比較する機能を追加
  - アダプティブリスク認証でリスクの高いログイン成功時に警告メールを送信する

機能を追加

- 2021 年 1 月 7 日 osstech-openam14-14.0.0-61
  - OAuth2 認証のデフォルトの設定値を変更
  - WebAuthn 認証及び ID 認証のログイン画面にユーザー名を記録する機能を追加
  - SecurID のエラーがデバッグログに出力される問題を修正
  - サブレルムにプロバイダーポリシーセットを作成できない問題を修正
  - DNS エイリアスの設定時に重複チェックを行うように修正
  - データストアの検索属性を uid から変更している場合にダッシュボードにデバイスが表示されない問題を修正
  - アカウントロックの持続時間を設定した場合もロックアウト属性を確認するように修正
- 2020 年 9 月 18 日 osstech-openam14-14.0.0-54
  - G Suite の設定時に IdP の NameID マッピングを更新しないように修正
  - データストアのユーザー属性として entryUUID を設定せずに WebAuthn を利用すると NullPointerException が発生する問題を修正
  - 共通タスクが意図していない言語で表示される問題を修正
  - データストア認証及び OpenLDAP 認証でパスワードのみの入力を求める場合に特定されたユーザー名を表示するように修正
  - 持続 Cookie の発行有無を選択する認証モジュールを追加
  - メッセージ表示にエスケープ処理を追加
  - 初期設定画面でドットから始まる Cookie ドメインを許容しないように修正
  - OAuth2 認証の Scope のデフォルト値をカンマではなくスペース区切りに修正
  - war 単体でデプロイできない問題を修正
  - WebAuthn 登録／認証でブラウザーが WebAuthn をサポートしていない場合に自動でキャンセル処理を行うように修正
  - Fedlet が動作しない問題を修正
  - webauthn.js がトランスパイルされていない問題を修正
  - 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
  - アダプティブリスク認証の設定画面がセクションで区切られていない問題を修正
  - SAML NameID としてセッションプロパティを利用する機能を追加
  - OSSTech 独自認証モジュールがアップグレードした環境で有効にならない問題を修正
  - 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

  - 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 7 月 27 日 osstech-openam14-14.0.0-35
  - SMS OTP 認証モジュールを追加
  - データストア認証及び OpenLDAP 認証に認証連鎖の中で特定された ID を引き継ぐ機能を追加
  - ダッシュボードの表示で AuthenticatorWebAuthnService デバッグログが肥大化する問題を修正
  - 特定のサーブレットの初期化に失敗する問題を修正
  - 冗長構成時にセッション数をカウントするデフォルトの挙動を変更
  - ID 認証モジュールを追加
  - Linux + Chrome 環境で Yubikey 5 のレジデントキー登録に失敗する問題を修正
  - SAML でメモリーリークが発生する問題を修正
- 2020 年 5 月 11 日 osstech-openam14-14.0.0-27
  - 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
  - プロパティファイルに関連する例外処理の改善
  - 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 4 月 16 日 osstech-openam14-14.0.0-23
  - PKCE を OAuth Client 毎に有効化する設定を追加
  - 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設定を追加
  - 管理画面に表示される PKCE のリンクを修正
  - LINE OTP 認証を認証連鎖分岐モジュールで利用できない問題を修正
  - PKCE の code_challenge_method パラメーターがオプショナルとして扱われていない問題を修正
  - 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
  - LINE OTP を認証連鎖分岐モジュールで利用すると確認画面の表示が崩れる問題を修正
  - アダプティブリスクのエラーメッセージをカスタマイズする機能を追加
  - ダッシュボードで Internal Server Error と表示される問題を修正
  - FrOATH 認証のデバイス登録時に鍵文字列を表示する画面を追加
  - FrOATH 認証のデフォルトの鍵サイズを変更
- 2020 年 3 月 10 日 osstech-openam14-14.0.0-11

  - ポリシー設定サービスの TLS バージョンのデフォルトを TLSv1.2 に変更
  - 認証連鎖分岐モジュールを追加
  - LINE OTP 認証モジュールを追加
- 2020 年 2 月 10 日 osstech-openam14-14.0.0-7
  - OpenAM が発行する Cookie に SameSite 属性を付与する機能を追加
  - ユーザーキャッシュタイムアウトのデフォルト値を変更
  - HOTP 認証で OTP 入力を複数回試行可能にする設定を追加
  - Red Hat Enterprise Linux 8 / CentOS 8 をサポート
  - パッケージが依存する Java 環境を OpenJDK 11 に変更
  - パッケージが依存するサーブレットコンテナを OSSTech Tomcat 9 に変更
  - ログインページで表示する選択画面をラジオボタンからドロップダウンリストに変更
- 2019 年 12 月 24 日 osstech-openam14-14.0.0-0
  - OSSTech OpenAM 14.0.0 新規作成