Sun OpenSSO Enterprise 8.0 リリースノート

Part No: 820–7088–10
2008 年 11 月 14 日

100303@23474

目次

Sun OpenSSO Enterprise 8.0 リリースノート

最終更新日 2008 年 11 月 14 日

Sun™ OpenSSO Enterprise 8.0 は、OpenSSO プロジェクト (`http://opensso.org/`) の一部であり、Sun 商用バージョンの OpenSSO サーバーです。

このリリースノートは、Sun OpenSSO Express にも適用されます。OpenSSO Enterprise と OpenSSO Express は、本質的に同じ製品ですが、次の点で異なります。

- OpenSSO Enterprise はおよそ 12 か月ごとにリリースされ、Sun QA Engineering による広範な自動および手動テストを受け、定期的にパッチおよびホットフィックスが公開されます。
- OpenSSO Express はおよそ 3 か月ごとにリリースされ、Sun QA Engineering による広範な自動テストおよび中程度の手動テストを受けますが、パッチおよびホットフィックスは公開されません。詳細については、OpenSSO Express FAQ (`https://opensso.dev.java.net/public/about/faqcenter/SupportFAQ.html`) を参照してください。

注 – WebLogic Server を Web コンテナとして使用して OpenSSO Enterprise サーバーを配備する場合は、18 ページの「4077: WebLogic Server 上の OpenSSO Enterprise の設定に新しい `ldapjdk.jar` が必要になる」を参照してください。

内容の紹介

OpenSSO Enterprise 8.0 の使用を開始するための作業

以前に OpenSSO Enterprise をインストールしたことがない場合は、次の基本的な手順に従います。

1. 必要に応じて、12 ページの「OpenSSO Enterprise 8.0 でサポートされる Web コンテナ」のいずれかをインストール、設定、および起動します。
2. 次のいずれかのサイトから `opensso_enterprise_80.zip` ファイルをダウンロードして解凍します。
   - OpenSSO プロジェクト: `https://opensso.dev.java.net/public/use/index.html`
   - Sun: `http://www.sun.com/software/products/opensso_enterprise`
3. Web コンテナの管理コンソールまたは配備コマンドを使用して、`opensso.war` ファイルを Web コンテナに配備します。

   または、Web コンテナでサポートしている場合は、単に WAR ファイルをコンテナの自動配備ディレクトリにコピーします。
4. GUI コンフィギュレータ、コマンド行コンフィギュレータのいずれかを使用して、OpenSSO Enterprise を設定します。

   GUI コンフィギュレータを起動するには、ブラウザに次の URL を入力します: *protocol*`://` *host*`.`*domain*`:`*port*`/` *deploy_uri*

   たとえば、`http://openssohost.example.com:8080/opensso` と入力します。

   OpenSSO Enterprise から共存モードで Access Manager 7.1 スキーマ (DIT) にアクセスする場合は、31 ページの「3961: `amadmin` で共存モードの OpenSSO コンソールにログインできない」を参照してください。
5. 管理コンソールまたは新しい `ssoadm` コマンド行ユーティリティーを使用して、必要に応じて詳細な設定を行います。
6. version 3.0 のポリシーエージェントをダウンロードする場合は、`https://opensso.dev.java.net/public/use/index.html` を参照してください。

OpenSSO Enterprise 8.0 のマニュアル

OpenSSO Enterprise 8.0 のマニュアルは、次のサイトから入手できます。

`http://docs.sun.com/coll/1767.1`

このサイトを定期的にチェックして、最新のマニュアルを確認してください。

OpenSSO Enterprise 8.0 の新機能

OpenSSO Enterprise 8.0 は、以前のリリースの Sun Java System Access Manager および Sun Java System Federation Manager にある、アクセス管理、連携管理、Web サービスセキュリティーなどの機能を備えています。OpenSSO Enterprise には、この節で説明する新しい機能も含まれています。

version 3.0 のポリシーエージェントの新機能については、次のいずれかのガイドを参照してください。

- 『Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide for J2EE Agents 』

  または

- 『Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide for Web Agents 』
- 簡素化されたインストールと設定:
  - OpenSSO Enterprise は、対応する Web コンテナの管理コンソールまたはコマンド行ユーティリティーを使用して `opensso.war` ファイルを配備するだけでインストールできます。配備 URI (`/opensso`) を使用してサーバーに初めてアクセスすると、コンフィギュレータが表示され、そこで管理者パスワードや設定データストアとユーザーデータストアの指定などの初期設定作業を行えます。
  - `opensso.war` ファイルを使用して、Distributed Authentication UI Server、コンソールのみ、サーバーのみ、およびアイデンティティープロバイダ (IDP) 発見サービスを配備する特殊な WAR ファイルを作成および配備することもできます。
- 集中化されたサーバーとエージェントの設定データ:
  - OpenSSO Enterprise と version 3.0 のポリシーエージェントの設定データは、集中設定データリポジトリに格納されます。ユーザーは、OpenSSO Enterprise 管理コンソールまたは新しい `ssoadm` コマンド行ユーティリティーを使用して、設定値を指定するだけです。`AMConfig.properties` ファイルや `AMAgent.properties` ファイル内にプロパティーを設定する必要はなくなりました。
  - 設定プロパティーの多くは「ホットスワップ可能」です。つまり、プロパティーを変更したあと Web コンテナを再起動する必要はありません。
  - 組み込みデータストアオプションにより、Sun Java System Directory Server をインストールしなくても、OpenSSO Enterprise と version 3.0 のポリシーエージェントの設定データを透過的に格納することができます。
- GUI コンフィギュレータのほかに、コマンド行コンフィギュレータでも OpenSSO Enterprise サーバーの初期設定を行えます。
- OpenSSO Enterprise 管理コンソールでの共通作業:
  - SAMLv2 プロバイダの作成。SAMLv2 のホストまたはリモートのアイデンティティープロバイダ (IDP) またはサービスプロバイダ (SP) を簡単に作成できます。

  - Fedlet の作成。Fedlet は、SAMLv2 SSO プロトコルの軽量サービスプロバイダ (SP) 実装のことです。Fedlet により、アイデンティティープロバイダ (IP) で、連携を実装していない SP を有効にすることができます。SP では、Java Web アプリケーションに Fedlet を追加し、そのアプリケーションを配備するだけです。
  - 連携の接続性のテスト。新しいまたは既存の連携配備をテストまたはトラブルシューティングして、接続が正常に作成されているかどうかを判定し、問題がある場合はその原因を特定することができます。
- 新しい Web コンテナが追加されました。詳細については、12 ページの「OpenSSO Enterprise 8.0 でサポートされる Web コンテナ」を参照してください。
- 簡素化された Web サービスセキュリティーエージェントを、JSR 196 SPI に基づいたプロバイダを使用して Glassfish および Sun Java System Application Server 9.1 上に配備できます。
- WS-Federation がアイデンティティー連携仕様をサポートしました。特に OpenSSO Enterprise では、WS-Federation Passive Requestor Profile をサポートしています。
- XACML v2.0 の SAML 2.0 プロファイルに規定されているように、特に `XACMLAuthzDecisionQuery` および `XACMLAuthzDecisionStatement` での XACML version 2.0 のサポートが追加されました。
- セキュリティー保護された認証および属性の交換機能により、IDP アプリケーションと SP アプリケーション間で安全な転送を行なって、アプリケーションからユーザー認証と属性情報を提供できます。
- 複数連携プロトコルハブにより、OpenSSO Enterprise IDP が連携ハブとして動作して、SAMLv2、ID-FF、WS-Federation などの異なる連携プロトコル間でのシングルログアウトが実現します。
- SAMLv2 プロファイルサポートに、IDP プロキシング、アフィリエーション、NameID マッピング、ECP、認証クエリー、および属性クエリーが含まれるようになりました。
- 12 ページの「OpenSSO Enterprise 8.0 でサポートされる Web コンテナ」で、Security Token Service (STS) が利用可能になりました。
- SAMLv2 表明フェイルオーバーがサポートされました。
- 新しいコマンド行ユーティリティー (`ssoadm`) で、OpenSSO Enterprise サーバーと version 3.0 のポリシーエージェントの両方を設定できます。
- Sun Identity Manager、SiteMinder、および Oracle Access Manager との統合が追加されました。
- サービスタグがサポートされました。9 ページの「Sun Inventory でのサービスタグの使用」を参照してください。

- OpenSSO Enterprise サーバーの指定、Distributed Authentication UI Server のユーザーとパスワードの入力などの初期設定作業を実行できるコンフィギュレータが、Distributed Authentication UI Server で提供されます。

  Distributed Authentication UI Server では、クロスドメインシングルサインオン (CDSSO) もサポートされます。
- 国際化およびローカリゼーションの変更点:
  - OpenSSO Enterprise は、英語のほか、フランス語、スペイン語、ドイツ語、日本語、韓国語、簡体字中国語、および繁体字中国語に対応しました。
  - ローカライズされたファイルは、デフォルトで `opensso.war` ファイルにバンドルされます (Access Manager 7 2005Q4 や Access Manager 7.1 では、それらのファイルが別個のローカライズ版パッケージに格納される)。
- UNIX、SecurID、および SafeWord 認証モジュールが、OpenSSO Enterprise と Express のリリースで利用可能になりました。SecurID は Java ベースの認証モジュールとなっています。
- アップグレードサポート:
  - Access Manager 6.3、7.0、7.1 および Federation Manager 7.0 から OpenSSO Enterprise 8.0 へのアップグレード
  - ポリシーエージェントの version 2.2 から version 3.0 へのアップグレード

Sun Inventory でのサービスタグの使用

OpenSSO 8.0 はサービスタグに対応しているので、ほかのハードウェア、ソフトウェア製品と同じように Sun Inventory を使用して OpenSSO 製品を追跡および管理することができます。サービスタグを使用するには、まず使用中の製品を登録してください。OpenSSO Enterprise、OpenSSO Express のほかナイトリービルドも登録できます。

登録するには、Sun Online Account (SOA) または Sun Developer Network (SDN) アカウントが必要です。これらのアカウントをお持ちでなくても、製品登録処理中にアカウントを取得できます。

OpenSSO 製品を登録してサービスタグを使用するには、次の手順に従います。

1. OpenSSO 管理コンソールに `amadmin` としてログインします。
2. コンソールの「共通操作」で「この製品を登録」をクリックします。
3. SOA も SDN アカウントもない場合は、新規アカウントのための情報を入力します。
4. 「登録」をクリックします。

サービスタグ登録ファイルは、*config-directory* /*deployuri*`/lib/registration` ディレクトリに保存されます (例: `opensso-config/opensso/lib/registration`)。

詳細については、次のサイトを参照してください。

- Sun Inventory: `https://inventory.sun.com/inventory/`
- サービスタグ FAQ: `http://servicetags.central/faq.html`

これらのサイトは、使用中のプラットフォームでサービスタグがサポートされているかどうか確認したり、特定の OpenSSO サーバーがすでに登録されているかどうかを調べたりする場合に役立ちます。

OpenSSO Enterprise 8.0 のハードウェアおよびソフトウェア要件

注 – Sun Microsystems 社のフルサポートが提供されるのは、この節で説明している OpenSSO Enterprise 8.0 のハードウェアおよびソフトウェア要件を満たす配備環境のみです。ここに記載された要件を満たさない環境では、サポートは提供されません。

OpenSSO Enterprise 8.0 のサポートされるハードウェアおよびソフトウェア要件に記載どおりに従っていない環境の場合、Sun Microsystems 社は一切の責任を負わないものとします。インストールおよび配備作業を始める前に、Sun プロフェッショナルサービスに相談することを強くお勧めします。ただし、追加費用が発生する場合もあります。

OpenSSO Enterprise 8.0 でサポートされるプラットフォーム

表 1　OpenSSO Enterprise 8.0 でサポートされるプラットフォーム

プラットフォーム	サポートされる Web コンテナ
SPARC、x86、および x64 システムの Solaris 10 OS SPARC および x86 システムの Solaris 9 OS	Tomcat のみを使用する Geronimo Application Server 2.1.1 を除く、12 ページの「OpenSSO Enterprise 8.0 でサポートされる Web コンテナ」すべて

表 1　OpenSSO Enterprise 8.0 でサポートされるプラットフォーム　　(続き)

プラットフォーム	サポートされる Web コンテナ
OpenSolaris	Glassfish Application Server V2 UR1 および UR2 Apache Tomcat 6.0.18
Red Hat Enterprise Linux 5 (Base および Advanced Platform、AMD サーバー上の 64 ビット版) Red Hat Enterprise Linux 4 サーバー (Base および Advanced Platform、AMD サーバー上の 64 ビット版)	Geronimo を除く、12 ページの「OpenSSO Enterprise 8.0 でサポートされる Web コンテナ」すべて
Ubuntu 8.0.4	Glassfish Application Server V2 UR1 および UR2 Apache Tomcat 6.0.18
Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition Windows Server 2003 Datacenter Edition	Geronimo を除く、12 ページの「OpenSSO Enterprise 8.0 でサポートされる Web コンテナ」すべて
64 ビットサーバー上の Windows Server 2003 R2	12 ページの「OpenSSO Enterprise 8.0 でサポートされる Web コンテナ」すべて
Windows XP Windows Vista	Oracle Server、JBoss Application Server、および Geronimo を除く、12 ページの「OpenSSO Enterprise 8.0 でサポートされる Web コンテナ」すべて
Windows 2008 Server	Glassfish Application Server V2 UR1 および UR2 Apache Tomcat 6.0.18
IBM AIX 5.3	IBM WebSphere Application Server 6.1

注:

- これらのベースリリースのパッチや更新の OpenSSO Enterprise でのサポートについては、たとえば、Red Hat Linux 4.7 または Red Hat Linux 5.2 のあとに続くパッチおよび更新はサポートされています。
- サポートされる OpenSSO Enterprise の Web コンテナがオペレーティングシステムの 32 ビットモードと 64 ビットモードをサポートする場合、OpenSSO Enterprise もそのオペレーティングシステムの 32 ビット版と 64 ビット版をサポートします。

OpenSSO Enterprise 8.0 でサポートされる Web コンテナ

表 2　OpenSSO Enterprise 8.0 でサポートされる Web コンテナ

Web コンテナ	考慮事項
Sun Java System Application Server 9.1 Update 1 および Update 2	ダウンロード: http://www.sun.com/download/index.jsp
Glassfish Application Server V2 UR1 および UR2	Glassfish サイト: https://glassfish.dev.java.net/ Glassfish のダウンロード: Glassfish V2 UR1: https://glassfish.dev.java.net/downloads/v2ur1-b09d.html Glassfish V2 UR2: https://glassfish.dev.java.net/downloads/v2ur2-b04.html
Sun Java System Web Server 7.0 Update 3 (32 ビットおよび 64 ビット)	ダウンロード: http://www.sun.com/download/index.jsp Update 3 のみ。Updates 1 と 2 はサポートされていません。
Apache Tomcat 5.5.27 および 6.0.18 以降	http://tomcat.apache.org/ を参照してください。
Oracle WebLogic Server 9.2 MP2	http://www.oracle.com/appserver/index.html を参照してください。
Oracle WebLogic Server 10	http://www.oracle.com/appserver/index.html を参照してください。 次のサイトに示されるオペレーティングシステムでサポートされます。 http://e-docs.bea.com/platform/suppconfigs/configs100/100_over/overview.html#1122259
Oracle Application Server 10g	http://www.oracle.com/technology/products/database/oracle10g を参照してください。 Version 10.1.3.1 がサポートされます。

表 2　OpenSSO Enterprise 8.0 でサポートされる Web コンテナ　(続き)

Web コンテナ	考慮事項
IBM WebSphere Application Server 6.1	http://www-01.ibm.com/software/webservers/appserv/was/ を参照してください。
Apache Geronimo Application Server 2.1.1	http://geronimo.apache.org/ を参照してください。 Solaris システムで Tomcat のみを使用する場合にサポートされます。
JBoss Application Server 4.x	http://www.jboss.com/ を参照してください。

Web コンテナごとの考慮事項や配備前の作業などの詳細については、『Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide』の第 2 章「Deploying the OpenSSO Enterprise Web Container」を参照してください。

OpenSSO Enterprise 8.0 の JDK 要件

表 3　OpenSSO Enterprise 8.0 の JDK 要件

OpenSSO Enterprise 8.0	サポートされる JDK のバージョン
サーバー	JDK 1.5.x または 1.6.x サポートされる Web コンテナ上の 64 ビット JVM **Solaris** 仮想記憶要件。Solaris システムの場合、特に JVM がヒープサイズ 4G バイトを超える 64 ビットモードで設定された場合は、JVM ヒープサイズの 2 倍以上の容量の仮想記憶を設定してください。そのため、オペレーティングシステムのスワップ領域を増やす必要が生じる可能性があります。
クライアント (OpenSSO SDK)	JDK 1.4.x、1.5.x、または JDK 1.6.x

OpenSSO Enterprise 8.0 のデータストア要件

表 4　OpenSSO Enterprise 8.0 のデータストア要件

データストアの種類	サポートされるデータストア
設定データストア (サービス管理データストアとも呼ばれる)	■ Sun Java System Directory Server 5.2、6.0、6.2、および 6.3 ■ OpenSSO 設定データストア

表 4　OpenSSO Enterprise 8.0 のデータストア要件　*(続き)*

データストアの種類	サポートされるデータストア
ユーザーデータストア	■ Sun Java System Directory Server 6.3 ■ Windows Server 2003 R2 上の Microsoft Active Directory 2003 ■ IBM Tivoli Directory Server 6.1 ■ OpenSSO ユーザーデータストア 注: OpenSSO ユーザーデータストアは、製品の配備ではサポートされません。プロトタイプ、POC (proof of concept)、または少数のユーザーから成る開発者配備用としてのみ推奨されます。

データストアの詳細については、『Sun OpenSSO Enterprise 8.0 Deployment Planning Guide』の第 2 章「Building the Deployment Architecture」を参照してください。

OpenSSO Enterprise 8.0 のセッションフェイルオーバー要件

表 5　OpenSSO Enterprise 8.0 のセッションフェイルオーバー要件

コンポーネント	要件
OpenSSO Enterprise 8.0	2 つ以上の OpenSSO Enterprise インスタンスが異なるホストサーバー上で動作して、ロードバランサの背後にあるサイトとして設定されるようにします。 ロードバランサについては特に要件はありません。ただし、一般には cookie ベースのセッション維持型設定をサポートするロードバランサのほうが、パフォーマンスは高くなります。
Sun Java System Message Queue 4.1	Message Queue ブローカを異なるサーバー上のクラスタモードで実行してください。
Oracle Berkeley DB 4.6.18	Berkeley DB のクライアントとデータベースは Message Queue ブローカと同じサーバー上に配備してください。 Message Queue ブローカと Berkeley DB は OpenSSO Enterprise インスタンスを実行しているのと同じサーバー上に配備できます。ただし、異なるサーバー上にブローカをインストールしたほうが、パフォーマンスは高くなります。

詳細については、『Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide』の第 8 章「Implementing OpenSSO Enterprise Session Failover」を参照してください。

OpenSSO Enterprise 8.0 でサポートされるポリシーエージェント

表 6　OpenSSO Enterprise 8.0 でサポートされるポリシーエージェント

ポリシーエージェントのバージョン	OpenSSO Enterprise サポート
Version 3.0 のポリシーエージェント	OpenSSO Enterprise は、新しい version 3.0 の J2EE と Web ポリシーエージェントを、version 3.0 の新機能とともにサポートします。 利用できる version 3.0 エージェントなど詳細については、`http://docs.sun.com/coll/1322.1` を参照してください。
Version 2.2 のポリシーエージェント	OpenSSO Enterprise は、version 2.2 の J2EE と Web ポリシーエージェントをサポートします。 ただし、OpenSSO Enterprise とともに配備した場合、version 2.2 のポリシーエージェントでは version 2.2 の機能を使用し続けてください。たとえば、エージェントの設定データはそのエージェントの `AMAgent.properties` ファイルにローカルに保存され、OpenSSO Enterprise の集中エージェント設定はサポートされません。 利用できる version 2.2 エージェントなど詳細については、`http://docs.sun.com/coll/1809.1` を参照してください。
Version 2.1 のポリシーエージェント	OpenSSO Enterprise は version 2.1 のポリシーエージェントをサポートしません。

OpenSSO Enterprise 8.0 のハードウェア要件

表 7　OpenSSO Enterprise 8.0 のハードウェア要件

コンポーネント	要件
RAM	プロトタイプまたは開発者配備: 1G バイト 本稼働配備: 4G バイトを推奨

表 7　OpenSSO Enterprise 8.0 のハードウェア要件　*(続き)*

コンポーネント	要件
ディスク容量	コンソールつきサーバー、サーバーのみ、またはコンソールのみの OpenSSO Enterprise 配備については次のとおりです。 ■ サーバー: OpenSSO Enterprise のバイナリファイルおよび設定データ用に 512M バイト ■ ログファイル: コンテナのログファイルを含めたログファイル用に 7G バイト クライアント SDK 配備については次のとおりです。 ■ クライアント SDK: 100M バイト以上 ■ ログファイル: デバッグレベル (`com.iplanet.services.debug.level`) が `message` に設定されている場合、デバッグログ用に 5 GB を推奨 ログファイルについての考慮事項: ログファイル要件は実際の本稼働時の負荷によって変化するため、適宜調整可能です。ディスク容量要件は、デフォルトの 100M バイトのログファイルサイズ、ログファイルの種類ごとに 1 つの履歴ファイル、という条件で算出しています。次の点に注意してください。 ■ 特にデバッグレベルを `message` に設定している場合には、デバッグログファイルを定期的に削除します。 ■ `logs` ディレクトリにある `.access` ログと `.error` ログのサイズと内容を定期的にチェックします。 ■ 最も古いファイルから削除できるよう、ログローテーションの設定を検討します。

OpenSSO Enterprise 8.0 でサポートされる Web ブラウザ

表 8　OpenSSO Enterprise 8.0 でサポートされる Web ブラウザ

ブラウザ	プラットフォーム
Firefox 2.0.0.x および 3.0.x	Windows Vista、Windows XP、および Windows Server 2003 Solaris OS、バージョン 9 および 10 Red Hat Linux 4 および 5
Firefox 1.0.7 および 1.5	Windows XP Windows 2000 Solaris OS、バージョン 9 および 10 Red Hat Linux 4 および 5

表 8　OpenSSO Enterprise 8.0 でサポートされる Web ブラウザ　　(続き)

ブラウザ	プラットフォーム
Microsoft Internet Explorer 7	Windows Vista、Windows XP、および Windows Server 2003
Microsoft Internet Explorer 6.0 SP1	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows 2000
Mozilla 1.7.12	Solaris OS、バージョン 9 および 10
	Windows XP
	Windows 2000
	Red Hat Linux 4 および 5

OpenSSO Enterprise 8.0 の問題

OpenSSO Enterprise の問題の詳細については、次のサイトを参照してください。

`https://opensso.dev.java.net/servlets/ProjectIssues`

Web コンテナおよびサーバーの問題

- 21 ページの「3837: Oracle Application Server 10g で設定が失敗する」
- 21 ページの「2222: パスワードリセットサービスとアカウントロックアウトサービスが通知エラーを報告する」

4077: WebLogic Server 上の OpenSSO Enterprise の設定に新しい ldapjdk.jar が必要になる

weblogic.jar に古い ldapjdk.jar ファイルがバンドルされているため、WebLogic Server 上で OpenSSO Enterprise の設定が失敗します。

Sun は、セキュリティーおよびパフォーマンス関連の修正を含む、新しい ldapjdk.jar ファイルを提供しています。WebLogic Server 9.2 および WebLogic Server 10 では、次の回避方法を実行します。

回避方法: 次のように、CLASSPATH 内で Sun の ldapjdk.jar を weblogic.jar の前に指定します。

1. 次のコマンドを実行して、opensso.war から ldapjdk.jar を一時ディレクトリに抽出します。

   ```
   jar xvf opensso.war WEB-INF/lib/ldapjdk.jar
   ```

2. 抽出した ldapjdk.jar を WebLogic の lib ディレクトリにコピーします。

   たとえば、Solaris または Linux システム上の WebLogic Server 10 では、*BEA_HOME*/weblogic_10.0/server/lib ディレクトリになります。

   Windows 上の WebLogic Server 9.2 では、*BEA_HOME*\weblogic92\server\lib ディレクトリになります。

3. この ldapjdk.jar のパスを既存のクラスパスの先頭に付加します。これは、WebLogic Server の起動に使用する起動スクリプトを編集して行います。次の例では、*BEA_HOME* に WebLogic Server がインストールされているものとします。

   Windows 上の WebLogic 9.2 の場合、次のファイルを編集します。

   BEA_HOME\weblogic92\samples\domains\wl_server\bin\startWebLogic.cmd

   set CLASSPATH=%CLASSPATH%;%MEDREC_WEBLOGIC_CLASSPATH% を次のように変更します。

```
set CLASSPATH=BEA_HOME\weblogic92\server\lib\ldapjdk.jar;%CLASSPATH%;%MEDREC_WEBLOGIC_CLASSPATH%
```

   Windows 上の WebLogic 10 の場合、次のファイルを編集します。

   BEA_HOME\wlserver_10.0\samples\domains\wl_server\bin\startWebLogic.cmd

   set CLASSPATH=%CLASSPATH%;%MEDREC_WEBLOGIC_CLASSPATH% を次のように変更します。

```
set CLASSPATH=
BEA_HOME\wlserver_10.0\server\lib\ldapjdk.jar;%CLASSPATH%;%MEDREC_WEBLOGIC_CLASSPATH%
```

Solaris または Linux 上の WebLogic 9.2 MP2 の場合、次のファイルを編集します。

```
/bea/weblogic92/samples/domains/wl_server/bin/startWebLogic.sh
```

または

```
/usr/local/bea/user_projects/domains/base_domain/bin/startWebLogic.sh
```

`CLASSPATH="${CLASSPATH}${CLASSPATHSEP}${MEDREC_WEBLOGIC_CLASSPATH}"` を次のように変更します。

```
CLASSPATH=
"BEA_HOME/weblogic92/server/lib/ldapjdk.jar${CLASSPATH}${CLASSPATHSEP}${MEDREC_WEBLOGIC_CLASSPATH}"
```

Solaris または Linux 上の WebLogic 10 の場合、次のファイルを編集します。

```
/bea/wlserver_10.0/samples/domains/wl_server/bin/startWebLogic.sh
```

または

```
/bea/user_projects/domains/wl10_domain/bin/startWebLogic.sh
```

`CLASSPATH="${CLASSPATH}${CLASSPATHSEP}${MEDREC_WEBLOGIC_CLASSPATH}"` を次のように変更します。

```
CLASSPATH=
"BEA_HOME/wlserver_10.0/server/lib/ldapjdk.jar${CLASSPATH}${CLASSPATHSEP}${MEDREC_WEBLOGIC_CLASSPATH}"
```

4. サーバーを再起動します。
5. OpenSSO Enterprise を設定します。

設定中に **WebLogic Server** の `StuckThreadMaxTime` 値を超過した

コンフィギュレータを使用した WebLogic Server 9.2 MP2 または 10 の設定時に、600 秒を過ぎても設定作業が完了しなかった場合、端末、WebLogic Server ドメイン、およびサーバーログに次のエラーが返されます。

```
<Error> <WebLogicServer> <BEA-000337> <[STUCK] Exe
cuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)' has been busy
for "681" seconds working on the request "Http Request: /opensso/setup/setSetup
Progress", which is more than the configured time (StuckThreadMaxTime) of "600"
seconds. Stack trace: ...
```

このエラーは、WebLogic Server で「Stuck Thread Max Time:」のデフォルト値 600 秒を超過したために発生します。

回避方法: コンフィギュレータが応答しない場合は、再起動します。WebLogic Server の「Stuck Thread Max Time」値をデフォルトの 600 秒から 1200 秒などもっと大きい値に変更することも検討してください。この値は WebLogic コンソールを使用して変更します (*base_domain* > 「Environment」 > 「Servers」 > 「Admin Server」 > 「Configuration/Tuning」)。

4099: JDK 1.4 WAR を使用する ID-WSF サンプルが例外を返す

WebLogic Server 8.1 で、ID-WSF 用に設定された `opensso-client-jdk14.war` からサービス検索中にエラーが返されます。

回避方法: *weblogic-home*`/jdk142_08/jre/lib/` に、次の JAR ファイルを追加します: `jax-qname.jar`、`namespace.jar`、`relaxngDatatype.jar`、`xalan.jar`、および `xsdlib.jar`。

`xalan.jar` ファイルは、`opensso.war` の `WEB-INF/lib` ディレクトリにあります。そのほかのファイルは、`opensso-client-jdk14.war` の `WEB-INF/lib` ディレクトリにあります。

4094: `amadmin` パスワードと設定データストア用ディレクトリマネージャーのパスワードが異なる場合にマルチサーバー設定が失敗する

この問題は、次の条件が成立したときにのみ発生します。

- 使用している設定データストアが Sun Java System Directory Server である。
- マルチサーバーインストールを実行しようとしている。
- `amadmin` パスワードが Directory Server のバインド `dn` パスワードと異なっている。

回避方法: この回避方法には 2 つの部分があります。

1. 設定 Directory Server のバインド `dn` パスワードが `amadmin` パスワードと同じであることを確かめます。
2. 2 つ目以降の追加 OpenSSO Enterprise サーバーを設定します。2 つ目のサーバーのインストールを実行し、最初の OpenSSO Enterprise サーバーの設定ディレクトリを指すようにするには、2 つ目の OpenSSO Enterprise サーバーの「コンフィギュレータ」ページにアクセスして、`amadmin` パスワード、cookie ドメイン、および手順 1 と手順 2 に必要なその他の詳細情報を入力します。

   手順 3 では、「既存の配備に追加」を選択しません。その代わりに、最初のインスタンスオプションを選択し、同じ Directory Server 名、ポート、DN、パスワード、最初のサーバーの暗号化鍵を入力します。その後、通常どおりに設定を続行します。

4055: コンソールで拡張プロパティーを追加するとエラーが発生する

コンソールで拡張プロパティーを追加すると、OpenSSO Enterprise サーバーからエラーが返されます。この問題は、どの拡張設定プロパティーを追加しても発生する可能性があります。

回避方法: コンソールでデフォルトのサーバー設定を変更した場合は、OpenSSO Enterprise サーバーの Web コンテナを再起動してください。

3837: Oracle Application Server 10g で設定が失敗する

Web コンテナとして Oracle Application Server 10g version 10.1.3.1 を使用すると、OpenSSO Express の設定が例外エラーで失敗します。

回避方法: OpenSSO を設定する前に、ターゲットの Oracle Application Server 10g サーバーインスタンスの「Server Properties」に次の JVM オプションを追加します。

```
-Doc4j.jmx.security.proxy.off=true
```

2222: パスワードリセットサービスとアカウントロックアウトサービスが通知エラーを報告する

OpenSSO Enterprise から、修飾されていない送信者名 `Identity-Server` を使用した電子メール通知が送信され、ログにエラーエントリが返されます。

回避方法: 次のファイルで、送信者名を `Identity-Server` から `Identity-Server@hostname.domainname` に変更します。

- `amPasswordResetModuleMsgs.properties` で `fromAddress.label` を変更します。
- `amAuth.properties` で `lockOutEmailFrom` を変更します。

データストアの問題

- 21 ページの「4102: サービス管理設定の TTL が機能しない」
- 21 ページの「4085: OpenSSO Enterprise で CRL を LDAP ディレクトリに格納できない」
- 22 ページの「3827: 2 つ目の Glassfish インスタンスで設定の複製がハングアップする」
- 22 ページの「3350、2867: Active Directory データストアで「LDAP がリフェラルに従う」を無効にする必要がある」
- 22 ページの「Access Manager SDK (AMSDK) プラグインでフェイルオーバーが機能しない」

4102: サービス管理設定の TTL が機能しない

サービス管理設定の有効期間 (TTL) が、TTL プロパティーが初期化されていないために、正常に機能していません。

4085: OpenSSO Enterprise で CRL を LDAP ディレクトリに格納できない

破棄証明書リスト (CRL) を CRL 配布ポイント拡張から取得したあと、その CRL が OpenSSO Enterprise から LDAP ディレクトリに格納されません。

3827: 2 つ目の Glassfish インスタンスで設定の複製がハングアップする

この問題は、OpenSSO Enterprise が Windows Vista サーバー上の 2 つの Glassfish (または Application Server 9.1) インスタンスに配備されるシナリオで発生します。2 つ目の OpenSSO Enterprise インスタンスの設定中に、「既存の配備に追加」オプションを使用した設定の複製がハングアップします。

回避方法: この問題は、Windows Vista システムでは現在回避できません。Vista 以外の Windows システムでは、次の Glassfish (または Application Server 9.1) JVM オプションを追加してください。

```
-Dcom.sun.enterprise.server.ss.ASQuickStartup=false
```

3350、2867: Active Directory データストアで「LDAP がリフェラルに従う」を無効にする必要がある

Active Directory データストアが原因でシステムがハングアップすることがあります。この問題は、新規 Active Directory データストアの作成時に発生する可能性もあります。

回避方法: OpenSSO Enterprise 管理コンソールで、当該 Active Directory データストアの「LDAP がリフェラルに従う」を無効にします。

1. 「アクセス制御」、*top-level-realm*、「データストア」、*ActiveDirectory-data-store-name* の順にクリックします。
2. 「LDAP がリフェラルに従う」の「有効」のチェックを外します。
3. 変更を保存します。

Access Manager SDK (AMSDK) プラグインでフェイルオーバーが機能しない

OpenSSO Enterprise が AMSDK プラグインで設定され、ディレクトリサーバーが MMR に設定されている場合、ディレクトリサーバーインスタンスがダウンしてもフェイルオーバーが機能しません。

認証に関する問題

- 23 ページの「4103: Windows デスクトップ SSO 認証モジュールが「設定が見つかりません」エラーを返す」
- 23 ページの「4100: CRL チェックを使用した証明書認証が失敗する」
- 23 ページの「4054: URL org パラメータを使用した amadmin 認証が失敗する」
- 23 ページの「1781: Data Store 以外の認証で amadmin ログインが失敗する」

4103: Windows デスクトップ SSO 認証モジュールが「設定が見つかりません」エラーを返す

Windows Server 2003 上の Internet Explorer 6.0 から Kerberos 認証を実行するように Windows デスクトップ SSO 認証モジュールを設定すると、「設定が見つかりません」エラーが返されます。

4100: CRL チェックを使用した証明書認証が失敗する

証明書認証を設定して「証明書を CRL と照合」を有効にすると、認証が失敗します。関連する問題である21 ページの「4085: OpenSSO Enterprise で CRL を LDAP ディレクトリに格納できない」も参照してください。

4054: URL `org` パラメータを使用した `amadmin` 認証が失敗する

OpenSSO Enterprise の管理者 (`amadmin`) が新規レルム (たとえば `myorg`) を作成し、その後次のように入力してその新しいレルムにログインを試みたとします。

```
http://host:port/opensso/UI/Login?org=myorg
```

OpenSSO Enteprise から「認証できませんでした」エラーが返されます。

回避方法: `amadmin` としてログインできるのは、ルートレルム (かつデータストアモジュールかアプリケーションモジュール) だけです。

1781: Data Store 以外の認証で `amadmin` ログインが失敗する

ルートレルムの認証モジュールを `DataStore` 以外に変更すると、`amadmin` でコンソールにログインできなくなります。

回避方法: `http://host.domain/deployurl/UI/Login?module=DataStore` を使用してログインします。

ポリシーに関する問題

- 23 ページの「3952: サーバーのサンプルにポリシーサンプルへのリンクがない」
- 24 ページの「3949: OCSP チェックで `server.policy` ファイルへのアクセス権の追加が必要になる」
- 24 ページの「3796: コンソールのみの配備でコンソールでの Fedlet の作成が失敗する」
- 24 ページの「2381: Access Manager ロールポリシーサブジェクトが Access Manager リポジトリデータストアでしかサポートされない」

3952: サーバーのサンプルにポリシーサンプルへのリンクがない

host: *port*/*uri*/`samples` の `index.html` で次のものが表示されます。

```
1. Authentication Samples
2. ID-FF Sample
3. SAMLv2 Sample
4. Multi-Federation Protocols Sample
```

ただし、ポリシーサンプルへの次のリンクが `index.html` にありません: *host*:*port*/*uri*/`samples/policy/policy-plugins.html`

回避方法: *host*:*port*/*uri*/`samples/policy/policy-plugins.html` ファイルをブラウザで開きます。

3949: OCSP チェックで `server.policy` ファイルへのアクセス権の追加が必要になる

Java Security Manager を有効にした OpenSSO Web コンテナで OCSP チェックを有効にするには、`server.policy` (またはそれに相当する) ファイルに次のアクセス権を追加します。

```
permission java.security.SecurityPermission "getProperty.ocsp.*";
```

3796: コンソールのみの配備でコンソールでの Fedlet の作成が失敗する

コンソールのみの配備を生成し、「コンソールでの共通作業」ページから Fedlet を作成すると、「`sp-extended.xml` 用のファイルまたはディレクトリがありませんでした」という意味のエラーメッセージが表示されて失敗します。コンソールのみのコンフィギュレータでは、`com.iplanet.services.configpath` プロパティーが設定されません。

回避方法: `AMConfig.properties` ファイルを編集して、`com.iplanet.services.configpath` プロパティーを設定ディレクトリに設定します。次のような形式になります。

```
com.iplanet.services.configpath=/consoleonly
```

2381: Access Manager ロールポリシーサブジェクトが Access Manager リポジトリデータストアでしかサポートされない

Access Manager ロールポリシーサブジェクトは、Access Manager リポジトリ (AMSDK) データストアでのみサポートされます。デフォルトでは、このサブジェクトはポリシー設定で無効になります。そのため、データストアの種類が AMSDK プラグインを使用する設定になっている場合にのみ、Access Manager ロールポリシーサブジェクトを有効にしてください。

詳細については、『Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide』の第 15 章「Enabling the Access Manager SDK (AMSDK) Identity Repository Plug-in」を参照してください。

セッションの問題

3910: ssoSessionTools.zip の setup.bat でツールをインストールできない

ssoSessionTools.zip を解凍したあと setup.bat スクリプトを実行すると、セッションスクリプトのインストールが失敗し、次のエラーが返されます。

1.4 以降の仕様に適合する JRE が見つかりません

回避方法: setup.bat スクリプトにある java.exe コマンドから -version:"1.4+" を削除し、スクリプトを再実行します。

2827: サイトを設定してもそのサイトに 2 つ目のサーバーが追加されない

セッションフェイルオーバー設定で、割り当てたサーバーリストに 2 つ目の OpenSSO Enterprise インスタンスが追加されません。

回避方法: OpenSSO Enterprise コンソールまたは ssoadm ユーティリティーを使用して、サーバーリストに 2 つ目のサーバーインスタンスを手動で追加します。

コマンド行ユーティリティーに関する問題

4079: Directory Server を設定データストアとして使用すると ssoadm import-svc-cfg コマンドが失敗する

OpenSSO Enterprise でサービスマネージャーデータストア内のノードを削除できないために、import-svc-cfg サブコマンドが失敗することがあります。この問題が発生する可能性があるのは、次のようなシナリオです。

1. リモート Sun Java System Directory Server を設定データストアとして使用して、OpenSSO Enterprise を設定します。
2. ssoadm export-svc-cfg コマンドを実行して、サービス XML ファイルをエクスポートします。

3. 手順 2 で取得したサービス XML データを ssoadm import-svc-cfg コマンドを実行して再インポートします。
4. 既存のデータの削除を確認されたら、「はい」を選択します。

   次のエラーメッセージが返されます: 予期しない LDAP 例外が発生しました。

回避方法**:** ssoadm import-svc-cfg コマンドを、正常終了するまで繰り返し実行します。

3955: ssoadm コマンドを実行できない

次の例外が発生するため、get-realm を使用して ssoadm コマンドを実行できません。

```
Logging configuration class "com.sun.identity.log.s1is.LogConfigReader" failed
com.sun.identity.security.AMSecurityPropertiesException: AdminTokenAction:
FATAL ERROR: Cannot obtain Application SSO token.
Check AMConfig.properties for the following properties
       com.sun.identity.agents.app.username
       com.iplanet.am.service.password
Logging configuration class "com.sun.identity.log.s1is.LogConfigReader" failed
com.sun.identity.security.AMSecurityPropertiesException: AdminTokenAction:
FATAL ERROR: Cannot obtain Application SSO token.
Check AMConfig.properties for the following properties
       com.sun.identity.agents.app.username
       com.iplanet.am.service.password
AdminTokenAction:  FATAL ERROR: Cannot obtain Application SSO token.
Check AMConfig.properties for the following properties
       com.sun.identity.agents.app.username
       com.iplanet.am.service.password
```

amadmin パスワードが、サービス管理データストア用のディレクトリマネージャーのパスワードと異なっているかどうかチェックしてください。異なっている場合は、次の回避方法を適用します。

回避方法**:** サーバー設定 XML を次のように変更します。

1. OpenSSO コンソールに amadmin としてログインします。
2. ssoadm.jsp get-svrcfg-xml を使用して、サーバー設定 XML を取得します。
3. encode.jsp を使用して、amadmin パスワードをエンコードします。
4. エンコードしたパスワードを XML 内の *amadmin-password* によって表されている 2 つの場所に設定します。次のような形式になります。

```
<User name="User1" type="proxy">
            <DirDN>
                cn=puser,ou=DSAME Users,dc=opensso,dc=java,dc=net
            </DirDN>
            <DirPassword>
```

```
                amadmin-password
            </DirPassword>
        </User>
        <User name="User2" type="admin">
            <DirDN>
                cn=dsameuser,ou=DSAME Users,dc=opensso,dc=java,dc=net
            </DirDN>
            <DirPassword>
                amadmin-password
            </DirPassword>
        </User>
        <BaseDN>
            dc=opensso,dc=java,dc=net
        </BaseDN>
    </ServerGroup>
```

5. ssoadm.jsp set-svrcfg-xml を使用して、変更したサーバー設定 XML を設定します。

2905: jss4.jar エントリが ssoadm classpath にない

ssoadm ユーティリティーの setup スクリプトを実行したあと、ssoadm を実行しようとすると、NoClassDefFoundError エラーが返されます。この問題は、アップグレードした OpenSSO Enterprise インスタンスで発生します。

回避方法: JSS を使用するには、jss4.jar を classpath に追加し、LD_LIBRARY_PATH 環境変数を設定します。(デフォルトの JCE を使用する場合は、jss4.jar を classpath に入れる必要はありません。)

クライアント SDK の問題

- 27 ページの「4081: クライアント SDK の SMS キャッシュがデフォルトで無効になる」
- 28 ページの「4080: クライアント SDK のコンフィギュレータが AMConfig.properties ファイルに間違った共有シークレットを設定する」

4081: クライアント SDK の SMS キャッシュがデフォルトで無効になる

クライアント SDK のインストールで、サービス管理サービス (SMS) のキャッシュがデフォルトで無効になります。

回避方法: Web サービスセキュリティー (WSS) アプリケーションの場合は、AMConfig.properties ファイルで com.sun.identity.sm.cache.enabled=false と設定します。そうしないと、問題 3171 の修正が機能しません。

ほかのすべてのクライアント SDK アプリケーションの場合は、`AMConfig.properties` ファイルで `com.sun.identity.sm.cache.enabled=true` と設定して SMS キャッシュを有効にします。これによって、パフォーマンスの問題を防止できます。

4080: クライアント SDK のコンフィギュレータが AMConfig.properties ファイルに間違った共有シークレットを設定する

クライアント SDK の WAR ファイルコンフィギュレータが、`AMConfig.properties` ファイルに間違った共有シークレットを設定します。

回避方法: 共有シークレット値とパスワードの暗号化鍵を OpenSSO Enterprise サーバーから、*$HOME*`/OpenSSOClient` ディレクトリにあるクライアント SDK の `AMConfig.properties` ファイルにコピーします。

連携および SAML に関する問題

- 28 ページの「3923: Oracle Application Server 上で「コンソールでの共通作業」ページからのエンティティー (IDP または SP) の作成が失敗する」
- 28 ページの「3065: ID-FF ログレコードのすべてのユーザーで同じコンテキスト ID が使用される」
- 29 ページの「2661: WebSphere Application Server 6.1 上で `logout.jsp` がコンパイルできない」
- 29 ページの「1977: WebSphere Application Server 6.1 上で SAMLv2 サンプルの `configure.jsp` ファイルが動作しない」

3923: Oracle Application Server 上で「コンソールでの共通作業」ページからのエンティティー (IDP または SP) の作成が失敗する

OpenSSO Enterprise を Oracle Application Server 上に配備している場合、「コンソールでの共通作業」ページでエンティティー (IDP または SP) を作成すると、例外が発生します。

回避方法: `opensso.war` が Oracle Application Server 上に配備されている場合は、配備計画表示で `oracle.xml` ファイルのインポートオプションを無効にします (「配備: 配備設定」 > 「クラスロードの設定」 > `oracle.xml`)。

3065: ID-FF ログレコードのすべてのユーザーで同じコンテキスト ID が使用される

すべての ID-FF ログレコードのコンテキスト (またはログイン) ID が、ユーザーが異なる場合でも同じになります。

2661: WebSphere Application Server 6.1 上で logout.jsp がコンパイルできない

logout.jsp ファイルには JDK 1.5 が必要ですが、IBM WebSphere Application Server 6.1 では JSP ファイルの JDK ソースレベルが JDK 1.3 に設定されます。

回避方法: 29 ページの「1977: WebSphere Application Server 6.1 上で SAMLv2 サンプルの configure.jsp ファイルが動作しない」の回避方法を参照してください。

1977: WebSphere Application Server 6.1 上で SAMLv2 サンプルの configure.jsp ファイルが動作しない

WebSphere Application Server 6.1 インスタンスで、/sample/saml2/sp/configure.jsp ファイルと /sample/saml2/idp/configure.jsp ファイルがコンパイルできません。configure.jsp ファイルには JDK 1.5 が必要ですが、WebSphere Application Server 6.1 では JSP ファイルの JDK ソースレベルが JDK 1.3 に設定されます。

回避方法: 次の手順に従い、JSP エンジン設定パラメータを編集して、JDK ソースレベルを 1.5 に設定します。

1. WEB-INF/ibm-web-ext.xmi ファイルを開きます。

   JSP エンジン設定パラメータは、Web モジュールの設定ディレクトリまたは Web モジュールのバイナリディレクトリのいずれかにある、WEB-INF/ibm-web-ext.xmi ファイルに格納されています。

   設定ディレクトリの例を示します。

   {WAS_ROOT}/profiles/*profilename*/config/cells/*cellname*/*applications*/*enterpriseappname*/deployments/*deployedname*/*webmodulename*/

   アプリケーションが、「Use Binary Configuration」フラグを true に設定して WebSphere Application Server に配備された場合は、バイナリディレクトリとなります。次のような形式になります。

   {WAS_ROOT}/profiles/*profilename*/*installedApps*/*nodename*/*enterpriseappname*/*webmodulename*/

2. compileWithAssert パラメータを、ファイルから文を削除するかコメントタグ (<!– と –>) で文を囲むかして、削除します。
3. jdkSourceLevel パラメータを追加し、値として 15 を設定します。次のような形式になります。

   ```
   <jspAttributes xmi:id="JSPAttribute_1" name="jdkSourceLevel" value="15"/>
   ```

   注: JSPAttribute_1 の整数部分 (_1) は、ファイル内で一意にしてください。
4. ibm-web-ext.xmi ファイルを保存します。
5. アプリケーションを再起動します。

jdkSourceLevel パラメータやそのほかの JSP エンジン設定パラメータの詳細については、次のページを参照してください。

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.nd.doc/info/ae/ae/rweb_jspengine.html

Web サービスセキュリティー (WSS) の問題

- 30 ページの「4057: エンドポイントによる動的 Web サービスプロバイダ設定が有効にならない」

4057: エンドポイントによる動的 Web サービスプロバイダ設定が有効にならない

Web サービスセキュリティー (WSS) のローンサンプルに基づいてプロキシユースケースを設定し、wsp 以外のプロファイル名を使って 2 つの Web サービスプロバイダ (WSP) を作成すると、エラーが発生します。

回避方法: JAX-WS/Web アプリケーションベースの Web サービスの場合は、複数の Web サービスをサポートする WSP 名として、静的エンドポイントを使用します。EJB ベースの Web サービスの場合は、デフォルトの WSP 設定を使用します。

アップグレード、互換性、および共存の問題

- 30 ページの「4108: 既存スキーマ (DIT) に合わせて OpenSSO Enterprise を設定すると間違った暗号化鍵が使用される」
- 31 ページの「3962: 管理者以外のユーザーを認証すると間違ったコンソール URL が返される」
- 31 ページの「3961: amadmin で共存モードの OpenSSO コンソールにログインできない」
- 31 ページの「2348: Distributed Authentication UI Server のサポート範囲」
- 32 ページの「830: ID-FF スキーマメタデータに下位互換性がない」

4108: 既存スキーマ (DIT) に合わせて OpenSSO Enterprise を設定すると間違った暗号化鍵が使用される

既存スキーマ (DIT) に合わせて OpenSSO Enterprise を設定すると、設定中に入力した暗号化鍵 (古い Access Manager または Federation Manager インスタンスからのもの) が使用されないために、設定後にコンソールにログインできません。その代わりに間違った新しい暗号化鍵が生成されるので、正しくない serverconfig.xml ファイルが作成されます。

回避方法:

1. OpenSSO Enterprise 設定ディレクトリに移動します。
2. `AMConfig.properties` ファイルにある暗号化鍵を正しい値に変更します。
3. 以前の Access Manager または Federation Manager インスタンスから `serverconfig.xml` のバックアップコピーを取得します。
4. OpenSSO Enterprise サーバーを再起動します。

3962: 管理者以外のユーザーを認証すると間違ったコンソール URL が返される

OpenSSO が Access Manager 7.1 Directory Server スキーマ (DIT) を使用して共存モードに設定されている場合、管理者以外のユーザーが OpenSSO コンソールにログインすると、正しくない URL に転送されます。次のような形式になります。

```
http://ssohost.example.com:8080/amserver/..amserver/base/AMAdminFrame
```

回避方法: URL を次のように編集します。

protocol`://`*host*`.` *domain*`:`*port*`/`*deploy_uri*`/idm/EndUser`

次のような形式になります。

```
http://ssohost.example.com:8080/amserver/idm/EndUser
```

3961: `amadmin` で共存モードの OpenSSO コンソールにログインできない

OpenSSO が Access Manager 7.1 Directory Server スキーマ (DIT) を使用して共存モードに設定されている場合、LDAP 認証を使って `amadmin` としてコンソールにログインしようとすると、失敗します。

回避方法: `amadmin` として共存モードの OpenSSO コンソールにログインするには、`module=DataStore` クエリーパラメータを追加します。次のような形式になります。

protocol`://`*host*`.` *domain*`:`*port*`/`*deploy_uri*`/UI/Login/?module=DataStore`

次のような形式になります。

```
http://ssohost.example.com:8080/amserver/UI/Login/?module=DataStore
```

2348: Distributed Authentication UI Server のサポート範囲

OpenSSO Enterprise の Distributed Authentication UI Server コンポーネントは、OpenSSO Enterprise でのみ動作します。次のようなシナリオはサポートされていません。

- Distributed Authentication UI Server 7.0 または 7.1 と OpenSSO Enterprise サーバーの組み合わせ

- OpenSSO Enterprise Distributed Authentication UI Server と Access Manager 7.0 または 7.1 サーバーの組み合わせ

830: ID-FF スキーマメタデータに下位互換性がない

以前のリリースの Access Manager または Federation Manager から OpenSSO Enterprise 8.0 にアップグレードする場合、Access Manager または Federation Manager スキーマもアップグレードしないかぎり、ID-FF プロファイルが機能しません。

回避方法: ID-FF プロファイルを試す前に、Access Manager または Federation Manager スキーマをアップグレードします。スキーマのアップグレードの詳細については、『Sun OpenSSO Enterprise 8.0 Upgrade Guide 』を参照してください。

国際化の問題

4090: 英語以外の権利書が文字化けする

回避方法: `.txt` 形式で提供されるローカライズされた権利書を表示するには、ブラウザでロケールごとに次のエンコーディングを指定してください。

- フランス語 (fr): ISO–8859-1
- スペイン語 (es): ISO–8859-1
- ドイツ語 (de): ISO–8859-1
- 簡体字中国語 (zh_CN): UTF-8
- 繁体字中国語 (zh_TW): UTF-8
- 韓国語 (ko): UTF-8
- 日本語 (ja): EUC-JP

4051: 複数バイトの信頼できるパートナー名がコンソールで文字化けする

OpenSSO コンソールで「連携」 > 「SAML1.x 設定」と選択し、「共通設定」セクションで複数バイト名を持つ信頼できるパートナーを新規作成すると、信頼できるパートナー名が文字化けします。

3993: CCK および JA ロケールで「エンドユーザー」ページに疑問符が表示される

CCK および JA ロケールの Geronimo Web コンテナ上で `amadmin` 以外のユーザーとしてログインすると、「アクセス制御」 > *realm* > 「全般」 > 「エンドユーザー」ページ (`http://`*host*`:`*port*`/`*deployuri*`/idm/EndUser`) に疑問符 (?) が表示されます。

3976: 英語以外のロケールでオンラインヘルプの「検索のヒント」に 404 エラーが表示される

OpenSSO コンソールにフランス語など英語以外のロケールでログインし、「ヘルプ」をクリックしてから「検索のヒント」をクリックすると、右側のヘルプパネルに 404 エラーが表示されます。

回避方法: ブラウザの言語を英語に設定し、オンラインヘルプウィンドウを更新すると、英語の「検索のヒント」を表示できます。

3763: C ロケールの Web コンテナで一部の非 ASCII 文字が文字化けする

C ロケールで Web コンテナを起動しブラウザをフランス語などの言語に設定すると、管理コンソールにログイン後、一部の文字が文字化けします。

3713: CCJK ロケールでパスワードリセットページがローカライズされない

CCJK ロケールで、パスワードリセットページ (`http://`*host* `:`*port*`/`*deployuri*`/password`) がローカライズされません。

3590: `dounix_msgs.po` ファイルの場所の変更

UNIX 認証モジュールは将来の OpenSSO Enterprise リリースには含まれなくなるため、UNIX 認証モジュール用の `dounix_msgs.po` ファイルは翻訳されていません。35 ページの「非推奨事項の通知」を参照してください。

1793: クエリーパラメータの org または module に複数バイト文字を使用すると認証が失敗する

UTF-8 以外の文字を使った `org` または `module` パラメータを使用して OpenSSO コンソールにログインしようとすると、失敗します。例:
`http://host:port/deployuri/UI/Login?module=Japanese-string&gx_charset=UTF-8`

回避方法: ネイティブな文字の代わりに `%E3%81%A6` などの UTF-8 URL エンコーディング文字を使用します。

ローカリゼーションの問題

4017: スペイン語ロケールのコンソールで「2.2 Agents」が「Agentes」としか翻訳されていない

スペイン語ロケールの OpenSSO コンソールで、「2.2 Agents」の訳から 2.2 が抜けています。

3994: スペイン語ロケールで「設定」 > 「認証」から証明書にアクセスできない

スペイン語ロケールの OpenSSO コンソールで「設定」 > 「認証」 > 「証明書」とクリックすると、エラーが返されます。

3971: 中国語 (zh_CN) ロケールでオンラインヘルプがが英語になる

中国語 (`zh_CN`) ロケールで、コンソールのオンラインヘルプテキストが中国語ではなく英語で表示されます。ブラウザの優先言語を `zh_CN` に設定すると、左側のツリーのオンラインヘルプテキストのみ英語になります。ブラウザの優先言語を `zh` に設定すると、すべてのオンラインヘルプテキストが英語になります。

回避方法: `zh_CN` のオンラインヘルプの内容を Web コンテナの `webapps` ディレクトリ内の新規 `zh` ディレクトリにコピーし、Web コンテナを再起動します。

たとえば、Apache Tomcat の場合は、`/Tomcat6.0.18/webapps/opensso/html/zh_CN/*` を `/Tomcat6.0.18/webapps/opensso/html/zh/` という名前の新規ディレクトリにコピーします。その後、Tomcat コンテナを再起動します。

3802: 著作権表示のフランス語部分の問題

英語の著作権表示内のフランス語の部分で、「Etats-unis」にアクセントがなく、「armes nucléaires,des missiles」のコンマの後ろに空白がなく、「Etats - Unis」の空白は不要です。

OpenSSO Enterprise 8.0 へのアップグレード

OpenSSO Enterprise 8.0 へのアップグレードをサポートしているリリースは、次のとおりです。

Sun Java System Directory Server 内の設定データも含めた以前のリリース	アップグレードをサポートするプラットフォーム
Sun Java System Access Manager 7.1 サーバー Java Enterprise System インストーラと WAR ファイル配備の両方	Solaris SPARC、Solaris x86、Linux、および Windows システム
Sun Java System Access Manager 7 2005Q4 サーバー	Solaris SPARC、Solaris x86、および Linux システム
Sun Java System Access Manager 6 2005Q1 (6.3) サーバー	Solaris SPARC、Solaris x86、および Linux システム
Sun Java System Federation Manager 7.0 サーバー	Solaris SPARC、Solaris x86、Linux、および Windows システム

アップグレード処理には、既存の Access Manager または Federation Manager サーバーインスタンスのアップグレードと、Sun Java System Directory Server に格納されている対応する設定データのアップグレードが含まれます。

詳細なアップグレード手順については、『Sun OpenSSO Enterprise 8.0 Upgrade Guide』を参照してください。

非推奨事項の通知

- サービス管理サービス (SMS) の API (`com.sun.identity.sm` パッケージ) および SMS モデルは、将来のリリースの OpenSSO Enterprise には含まれなくなります。
- UNIX 認証モジュールおよび UNIX 認証ヘルパー (`amunixd`) は、将来のリリースの OpenSSO Enterprise には含まれなくなります。
- 『Sun Java System Access Manager 7.1 リリースノート』では、一般に Access Manager SDK (AMSDK) と呼ばれる Access Manager `com.iplanet.am.sdk` パッケージ、および関連するすべての API と XML テンプレートが、将来のリリースの OpenSSO Enterprise に含まれなくなると述べています。移行オプションは現時点で利用でき

ません。また、将来利用可能になる予定もありません。Sun Identity Manager に、AMSDK の代わりに利用できるユーザープロビジョニングソリューションが用意されています。Identity Manager の詳細については、http://www.sun.com/software/products/identity_mgr/index.jsp を参照してください。

問題の報告とフィードバックの方法

OpenSSO Enterprise に関するご質問や問題の報告は、http://sunsolve.sun.com/ にある Sun のサポートリソース (SunSolve) までご連絡ください。

このサイトには、ナレッジベース、オンラインサポートセンター、Product Tracker へのリンクと保守プログラムおよびサポートの連絡先電話番号へのリンクがあります。

サポートを依頼する場合は、次の情報をご用意ください。

- 問題が発生した状況および操作への影響などの、問題の具体的説明
- マシンのタイプ、オペレーティングシステムのバージョン、Web コンテナとそのバージョン、JDK のバージョン、OpenSSO Enterprise のバージョンに加え、問題に関係する可能性があるすべてのパッチ、その他のソフトウェア
- 問題を再現するための手順
- エラーログやコアダンプ

このマニュアルに関するコメント

弊社では、マニュアルの改善に努めており、お客様からのコメントおよびご忠告をお受けしております。http://docs.sun.com/ に移動し、「Feedback」をクリックしてください。

該当の欄にマニュアルの正式タイトルと Part No. をご記入ください。Part No. は、マニュアルのタイトルページ、またはマニュアルの一番上に記載されている 7 桁または 9 桁の数字です。たとえば、タイトルは『Sun OpenSSO Enterprise リリースノート』、Part No. は 820-7088 です。

Sun が提供しているその他の情報

次の場所から、役立つ情報とリソースをさらに入手できます。

- Sun サービス: http://www.sun.com/service/consulting/
- Sun ソフトウェア製品: http://wwws.sun.com/software/
- Sun サポートリソース: http://sunsolve.sun.com/

- Sun Developer Network (SDN): http://developers.sun.com/
- Sun 開発者サポートサービス: http://www.sun.com/developers/

障害を持つ方々向けのアクセシビリティー機能

このメディアの出版以降にリリースされたアクセシビリティー機能を入手するには、Sun に米国リハビリテーション法 508 条に関する製品評価資料を請求し、その内容を確認して、どのバージョンが、アクセシビリティーに対応したソリューションを配備するためにもっとも適しているかを特定してください。

アクセシビリティーに関する Sun の方針については、http://sun.com/access を参照してください。

関連するサードパーティーの Web サイト

このマニュアル内で参照している第三者の URL は、追加の関連情報を提供します。

注 – Sun は、このリリースノートに記載されたサードパーティーの Web サイトの有効性および有用性に関して責任を負いません。Sun は、これらのサイトまたはリソースで利用可能な内容、広告、製品、ほかの資料に関し、それらを保証することも、責任や義務を負うこともありません。また、このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、商品、サービスの使用や、それらへの依存に関連して発生した実際の損害や損失、またはその申し立てについても、Sun は一切の責任を負いません。

改訂履歴

表 9　改訂履歴

日付 (改訂)	変更点
2008 年 11 月 14 日 (11)	10 ページの「OpenSSO Enterprise 8.0 のハードウェアおよびソフトウェア要件」の新しい情報や変更など、最近の変更点を追加。
2008 年 11 月 11 日 (10)	初期のリリース。
2008 年 8 月 26 日 (05)	アーリーアクセス (EA) リリースドラフト。