Sun Java System Access Manager 7 2005Q4 リリースノート

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 819–3474
2008 年 8 月 19 日

080929@20795

目次

Sun Java System Access Manager 7 2005Q4 リリースノート

2008 年 8 月 19 日

Part No. 819-3474

Sun Java™ System Access Manager (Access Manager) 7 2005Q4 リリースノートには、Access Manager の新機能、既知の問題点、および利用可能な場合は回避方法を含む、Sun Java Enterprise System (Java ES) リリースの重要な情報が含まれています。このリリースのインストールおよび使用を始める前に、このリリースノートをお読みください。

このリリースノートに関する詳細は、6 ページの「改訂履歴」を参照してください。

Access Manager コレクションを含むJava ES 製品のマニュアルを確認するには、`http://docs.sun.com/prod/entsys.05q4` を参照してください。

ソフトウェアをインストールおよび設定する前だけでなく、それ以降も定期的にこのサイトをチェックして、最新のマニュアルを確認してください。

内容の紹介

Access Manager 7 2005Q4 リリースノートは、次の節で構成されています。

改訂履歴

次の表に、Access Manager 7 2005Q4 リリースノートの改訂履歴を示します。

表 1　改訂履歴

日付	変更点
2008 年 8 月 19 日	9 ページの「Access Manager 7 2005Q4 パッチリリース」の節に、Windows および HP-UX システム用のパッチ 7 に関する情報を追加。
2008 年 5 月 12 日	■ 9 ページの「Access Manager 7 2005Q4 パッチリリース」の節に、パッチ 7 に関する情報を追加。 ■ 74 ページの「システム仮想化のサポート」の節を追加。
2007 年 10 月 16 日	このリビジョンでの変更点を次に示します。 ■ 9 ページの「Access Manager 7 2005Q4 パッチリリース」の節に、パッチ 6 に関する情報を追加。 ■ 45 ページの「CR# 6522720: Windows および HP-UX システム上では、複数バイト文字を用いてコンソールオンラインヘルプの検索ができない」を更新。Windows システムでは、この問題はパッチ 6 で修正されます。ただし、HP-UX システムではこの問題が引き続き存在します。
2007 年 7 月 10 日	このリビジョンでの変更点を次に示します。 ■ 9 ページの「Access Manager 7 2005Q4 パッチリリース」の節に、HP-UX システム用パッチ126371-05 に関する情報を追加。 ■ 新たに次の問題を追加。92 ページの「Access Manager が Directory Proxy をポイントする場合、null 属性によるLDAP 検索でエラーが返される (6357975)」。
2007 年 3 月 16 日	このリビジョンでの変更点を次に示します。 ■ 9 ページの「Access Manager 7 2005Q4 パッチリリース」の節に、パッチ 5 に関する情報を追加。 ■ 101 ページの「マニュアルに関する情報」に明確な説明と新しい情報を追加。 ■ レビュアや変更要求 (CR) によるその他のさまざまな技術的変更や編集上の変更。

表 1 改訂履歴 (続き)

日付	変更点
2006 年 10 月 30 日	9 ページの「Access Manager 7 2005Q4 パッチリリース」の節の変更点を次に示します。 ■ パッチ 4 に関する情報を追加。 ■ *AccessManager-base* の矛盾する使用法を修正。 ■ 55 ページの「CR# 6440651: Cookie 応答には `com.sun.identity.session.resetLBCookie` プロパティーが必要」の説明を改訂。
2006 年 8 月 25 日	9 ページの「Access Manager 7 2005Q4 パッチリリース」の節の変更点を次に示します。 ■ パッチ 3 に関する情報を追加。 ■ パッチ 1 および 2 に関する情報を改訂および新たに追加。
2006 年 5 月 25 日	このリビジョンでの変更点を次に示します。 ■ 新たに 58 ページの「Access Manager 7 2005Q4 パッチ 2」の節を追加。 ■ HP-UX および Microsoft Windows プラットフォームのサポートに関する情報を表 4 に追加。 ■ 101 ページの「マニュアルに関する情報」に次の問題を追加。 ■ 107 ページの「リリースノートの既知の問題点に対する回避方法に誤った記述がある (6422907)」 ■ 107 ページの「`AMConfig.properties` 内のドキュメント `com.iplanet.am.session.protectedPropertiesList` (6351192)」
2006 年 2 月 9 日	109 ページの「マニュアルの更新」を改訂し、初期リリース以降に発行された Access Manager 7 2005Q4 の新規または改訂マニュアルを一覧表示。
2006 年 2 月 7 日	このリビジョンでの変更点を次に示します。 ■ 77 ページの「既知の問題点と制限事項」に次の問題を追加。 ■ 81 ページの「Access Manager と Directory Server を別のマシンにインストールすると、認証サービスが初期化されない (6229897)」 ■ 82 ページの「Access Manager の `ampre70upgrade` スクリプトがローカライズ版のパッケージを削除しない (6378444)」 ■ 109 ページの「マニュアルの更新」の節を更新。

表 1 改訂履歴 (続き)

日付	変更点
2006 年 1 月 18 日	このリビジョンでの変更点を次に示します。 ■ 新たに 64 ページの「Access Manager 7 2005Q4 パッチ 1」の節を追加。 ■ 69 ページの「分散認証」の説明を明確化。 ■ 72 ページの「ハードウェアおよびソフトウェアの要件」で、Solaris 10 ゾーンのサポートを明確にし、AMD64 プラットフォームでの Solaris 10 OS のサポートを追加。 ■ 77 ページの「既知の問題点と制限事項」に次の問題を追加。 ■ 87 ページの「RSA キーを使用した場合に、IBM WebSphere でURL署名が失敗する (6271087)」 ■ 97 ページの「Application Server 上で Access Manager を実行すると、JVM の問題が生じる (6223676)」 ■ 97 ページの「Web サービスサンプルを実行すると「Resource offering not found」が返される (6359900)」 ■ 79 ページの「パッチ 1 の適用後、`/tmp/amsilent` ファイルがすべてのユーザーの読み取りアクセスを許可する (6370691)」 ■ 84 ページの「データ移行後に `ContainerDefaultTemplateRole` 属性を追加する (4677779)」 ■ 107 ページの「LDAPv3 プラグインのロールおよびフィルタを適用したロールのサポートについて (6365196)」 ■ 108 ページの「`AMConfig.properties` ファイルの未使用のプロパティーについて (6344530)」 ■ 108 ページの「XML 暗号化を有効にする方法について (6275563)」 ■ 新たに 109 ページの「マニュアルの更新」の節を追加。
2005 年 11 月 8 日	サポートされる LDAP version 3 (LDAP v3) 準拠リポジトリについて 66 ページの「アイデンティティーリポジトリ」を変更。
2005 年 10 月 3 日	初期のリリース。
2005 年 6 月 30 日	ベータリリース。

Sun Java System Access Manager 7 2005Q4 について

Sun Java System Access Manager は、企業内および企業間 (B2B) のバリューチェーンで、組織が Web アプリケーションおよびその他のリソースにセキュリティー保護されたアクセスを行うことができるようにする Sun のアイデンティティー管理インフラストラクチャーの一部です。Access Manager は、以下の主要な機能を提供します。

- ロールに基づくアクセス制御およびルールに基づくアクセス制御の両方を使用した、集中認証および承認サービス
- 組織の Web ベースのアプリケーションに対するシングルサインオン (SSO) アクセス
- Liberty Alliance Project および Security Assertions Markup Language (SAML) による連携アイデンティティーのサポート
- Access Manager コンポーネントによるその後の分析、報告および監査のための、管理者およびユーザーのアクティビティーを含む重要な情報のログ作成。

Access Manager 7 2005Q4 パッチリリース

Access Manager 7 2005Q4 のパッチの最新リビジョンは、SunSolve Online `http://sunsolve.sun.com` からダウンロードできます。最新のパッチ ID は次のとおりです。

- SPARC® ベースのシステム上の Solaris™ オペレーティングシステム (Solaris OS): **120954-07**
- x86 プラットフォーム上の Solaris OS: **120955-07**
- Linux システム: **120956-07**
- Microsoft Windows システム: **124296-07**
- HP-UX システム: **126371-07**

注 – Access Manager 7 2005Q4 パッチは累積的なパッチです。あらかじめパッチ 1、2、3、4、5、または 6 をインストールしなくてもパッチ 7 をインストールできます。ただし、以前のパッチをインストールしていない場合は、以前のパッチの節で新機能と問題を見直し、使用する配備に当てはまる機能や問題があるかどうかを確認してください。

Access Manager 7 2005Q4 のパッチに関する情報を次に示します。

- 10 ページの「Access Manager 7 2005Q4 パッチ 7」
- 11 ページの「インストール前の注意点」
- 14 ページの「パッチのインストール手順」
- 20 ページの「インストール後の注意点」
- 23 ページの「Access Manager 7 2005Q6 パッチ 6」
- 28 ページの「Access Manager 7 2005Q4 パッチ 5」
- 46 ページの「Access Manager 7 2005Q4 パッチ 4」
- 47 ページの「Access Manager 7 2005Q4 パッチ 3」
- 58 ページの「Access Manager 7 2005Q4 パッチ 2」
- 64 ページの「Access Manager 7 2005Q4 パッチ 1」

Access Manager 7 2005Q4 パッチ 7

Access Manager 7 パッチ 7 (リビジョン 07) により、いくつかの問題が修正されます。その一覧はパッチに含まれている README ファイルに記載されています。

パッチ 7 での新機能

CR# 6637806: 再起動後に、Access Manager が無効なアプリケーション SSO トークンをエージェントに送信する

Access Manager サーバーが再起動すると、Access Manager クライアント SDK はエージェントに重要な例外を送信するようになりました。これにより、エージェントは新しいアプリケーションセッションを取得するために、自身を再認証できます。Access Manager 7 2005Q4 パッチ 5 以後、これまで Access Manager クライアント SDK は、Access Manager サーバーの再起動後に無効なアプリケーション SSO トークンをエージェントに送信していました。

この問題は、重複している CR 6496115 で修正されています。パッチ 7 には、制限のあるコンテキストでアプリケーション SSO トークンを送信するオプション (`comp.iplanet.dpro.session.dnRestrictionOnly` プロパティー) もあります。デフォルトで、エージェントはエージェントがインストールされているサーバーの IP アドレスを送信しますが、DN の厳密なチェックが必要な場合は `AMConfig.properties` ファイルでこのプロパティーを次のように設定します。

```
com.iplanet.dpro.session.dnRestrictionOnly=true
```

CR# 6612609: Session failover works if ネットワークケーブルが Message Queue サーバーから切り離されている場合に、セッションフェイルオーバーが動作する

セッションフェイルオーバー配備で、それぞれの Access Manager インスタンスおよび Message Queue ブローカが同じサーバーにインストールされている場合、ネットワークケーブルがいずれかのサーバーから切り離されていればセッションフェイルオーバーが動作するようになりました。デフォルトでは、Message Queue `imqAddressListBehavior` 接続ファクトリ属性が `PRIORITY` に設定されているため、

Message Queue はブローカアドレスリストの出現順にアドレスを試行します (例: `localhost:7777,server2:7777,server3:7777`)。この属性が `RANDOM` に設定されている場合は、ランダムな順序でアドレスが試行されます。

この属性を RANDOM に設定するには、`amsessiondb` スクリプトで次のパラメータを設定します。

```
-DimqAddressListBehavior=RANDOM
```

Message Queue `PRIORITY` 属性および `RANDOM` 属性については、『Sun Java System Message Queue 3.7 UR1 管理ガイド』の「ブローカのアドレスリスト」を参照してください。

CR# 6570409: ロードバランサの背後にある対話型サービスがアイデンティティープロバイダとして正しく動作する

ロードバランサで接続されている 2 台のサーバーが 1 つのアイデンティティープロバイダとして機能している配備では、`AMConfig.properties` ファイル内の次のプロパティーを設定する必要があります。

```
com.sun.identity.liberty.interaction.lbWspRedirectHandler
com.sun.identity.liberty.interaction.trustedWspRedirectHandlers
```

`com.sun.identity.liberty.interaction.interactionConfigClass` が現在サポートされている唯一のクラスです。そのためデフォルトでは、相互作用構成パラメータにアクセスするときには、Federation Liberty にバンドルされている相互作用構成クラスが使用されます。

CR# 6545176: 認証後処理 SPI プラグインで、リダイレクト URL を動的に設定できる

ログイン成功、ログイン失敗、およびログアウト用の認証後処理 SPI プラグインで、リダイレクト URL を動的に設定できるようになりました。事後処理プラグインが実行されていない場合、事後処理 SPI で設定されたリダイレクト URL は使用されず、その他の方法で設定されたリダイレクト URL が従来どおり実行されます。

詳細は、
`com.iplanet.am.samples.authentication.spi.postprocess.ISAuthPostProcessSample.java` のサンプルを参照してください。

インストール前の注意点

- 12 ページの「ファイルのバックアップ」
- 14 ページの「Access Manager のインストールと設定」

ファイルのバックアップ

重要 現在のインストールでカスタマイズしたファイルがある場合は、パッチをインストールする前にこれらのファイルをバックアップしてください。パッチをインストールしたあと、バックアップしたファイルをこのパッチによってインストールされた新しいファイルと比較して、カスタマイズの内容を特定します。カスタマイズの内容を新しいファイルにマージし、ファイルを保存します。カスタマイズしたファイルの処理方法の詳細については、以下の情報をお読みください。

パッチをインストールする前に、次のファイルもバックアップしてください。

Solaris システム	■ *AccessManager-base*/SUNWam/bin/amsfo ■ *AccessManager-base*/SUNWam/lib/amsfo.conf ■ /etc/opt/SUNWam/config/xml/template/ ディレクトリ内の次のファイル。 idRepoService.xml、amSOAPBinding.xml、amDisco.xml、amAuthCert.xml、amAuth.xml、amSession.xml ■ *AccessManager-base*/SUNWam/locale/ ディレクトリ内の次のファイル。 amConsole.properties、 amIdRepoService.properties、amAuthUI.properties、 amAuth.properties、amPolicy.properties、 amPolicyConfig.properties、amSessionDB.properties、 amSOAPBinding.properties、amAdminCLI.properties、 amSDK.properties、amAuthLDAP.properties、 amSession.properties、amAuthContext.properties、 amSAML.properties、amAuthCert.properties

Linux および **HP-UX** システム	■ *AccessManager-base*/identity/bin/amsfo ■ *AccessManager-base*/identity/lib/amsfo.conf ■ /etc/opt/sun/identity/config/xml/template/ ディレクトリ内の次のファイル。 idRepoService.xml、 amSOAPBinding.xml、amDisco.xml、amAuthCert.xml 、amAuth.xml、amSession.xml ■ *AccessManager-base*/identity/locale/ ディレクトリ内の次のファイル。 amConsole.properties、 amIdRepoService.properties、amAuthUI.properties、 amAuth.properties、amPolicy.properties、 amPolicyConfig.properties、amSessionDB.properties、 amSOAPBinding.properties、amAdminCLI.properties、 amSDK.properties、amAuthLDAP.properties、 amSession.properties、amAuthContext.properties、 amSAML.properties、amAuthCert.properties
Windows システム	■ *AccessManager-base*\identity\setup\AMConfigurator.properties ■ *AccessManager-base*\identity\bin\amsfo ■ *AccessManager-base*\identity\lib\amsfo.conf ■ *AccessManager-base*\identity\config\xml\template ディレクトリ内の次のファイル。 idRepoService.xml、 amSOAPBinding.xml、amDisco.xml、amAuthCert.xml 、amAuth.xml、amSession.xml ■ *AccessManager-base*\identity\locale ディレクトリ内の次のファイル。 amConsole.properties、 amIdRepoService.properties、amAuthUI.properties、 amAuth.properties、amPolicy.properties、 amPolicyConfig.properties、amSessionDB.properties、 amSOAPBinding.properties、amAdminCLI.properties、 amSDK.properties、amAuthLDAP.properties、 amSession.properties、amAuthContext.properties、 amSAML.properties、amAuthCert.properties

AccessManager-base は、ベースインストールディレクトリです。デフォルトのベースインストールディレクトリは、次のようにプラットフォームによって異なります。

- Solaris システム: /opt
- Linux および HP-UX システム: /opt/sun
- Windows システム: *javaes-install-directory*\AccessManager。例: C:\Program Files\Sun\AccessManager

Access Manager のインストールと設定

本書に記載されている Access Manager パッチでは、Access Manager はインストールされません。パッチをインストールする前に、Access Manager 7 2005Q4 をサーバーにインストールする必要があります。インストールの詳細については、『Sun Java Enterprise System 2005Q4 インストールガイド(UNIX 版)』を参照してください。

Windows システムにパッチをインストールする場合は、『Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows』を参照してください。

また、`amconfig` スクリプトを実行して Access Manager の配備、再配備、および設定を行う方法についても理解しておいてください。詳細については、『Sun Java System Access Manager 7 2005Q4 管理ガイド』の第 1 章「Access Manager 7 2005Q4 の設定スクリプト」を参照してください。

このパッチによって廃止される Access Manager パッチ、およびこのパッチをインストールする前にインストールする必要のあるパッチの一覧については、このパッチに含まれている README ファイルを参照してください。

注意 – ほかのパッチと同様に、Access Manager パッチはステージングシステムや配備前システムでテストしてから、本稼働環境に配備するようにしてください。また、カスタマイズした JSP ファイルは、パッチインストーラで正しく更新されない場合があります。その場合、Access Manager を正しく機能させるには、これらのファイルを手動で変更する必要があります。

パッチのインストール手順

Solaris システムでのパッチのインストール手順

Solaris 用パッチをインストールする前に、11 ページの「インストール前の注意点」に示したファイルをバックアップしておく必要があります。

Solaris システムでパッチの追加や削除を行うには、OS で提供されている `patchadd` コマンドと `patchrm` コマンドを使用します。

patchadd コマンド

`patchadd` コマンドは、スタンドアロンシステムにパッチをインストールするために使用します。次に例を示します。

```
# patchadd /var/spool/patch/120954-07
```

注 – Solaris 10 の大域ゾーンに Solaris パッチをインストールする場合は、 -G 引数を付けた patchadd コマンドを実行します。次に例を示します。

```
patchadd -G /var/spool/patch/120954-07
```

postpatch スクリプトでは、Access Manager アプリケーションの再配備に関するメッセージが表示されます。ただし、Access Manager SDK コンポーネントだけがインストールされているシステムの場合は表示されません。

postpatch スクリプトは、次のディレクトリに amsilent ファイルを作成します。

- Solaris システム: *AccessManager-base*/SUNWam
- Linux システム: *AccessManager-base*/identity

AccessManager-base は、ベースインストールディレクトリです。デフォルトのベースインストールディレクトリは、Solaris システムの場合は /opt、Linux システムの場合は /opt/sun です。

amsilent は amsamplesilent ファイルを基にしていますが、システムの Access Manager 設定ファイルに従っていくつかの必須パラメータが設定されます。ただし、パスワードパラメータにはデフォルト値が設定されます。配備での必要に応じて、各パスワードパラメータのコメントを解除して値を変更し、このファイル内のほかのパラメータの値も注意深く確認します。

COMMON_DEPLOY_URI パラメータ (共通ドメイン Web アプリケーションの URI プレフィックス) にもデフォルト値が設定されます。この URI をデフォルト以外の値にした場合は、必ずこの値を更新してください。更新しないと、amconfig とパッチが生成した amsilent ファイルによる Web アプリケーションの再配備が失敗します。

次のコマンドを実行します (Access Manager がデフォルトディレクトリにインストールされている場合の例)。

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

注意 – amsilent ファイルには、プレーンテキスト形式の管理者パスワードなどの機密データが含まれているため、配備に合わせてこのファイルを保護する必要があります。

amconfig スクリプトを実行したあと、updateschema.sh スクリプトを実行して XML ファイルと LDIF ファイルを読み込みます。updateschema.sh スクリプトは、パッチ 7 のインストール後に、次のディレクトリから使用できます。

- Solaris SPARC システム: *patch-home-directory* /120954-07

- Solaris x86 システム: *patch-home-directory*/120955-07

updateschema スクリプトを実行したあと、Access Manager のプロセスを再起動します。次に例を示します。

```
# cd /opt/SUNWam/bin
# ./amserver stop
# ./amserver start
```

Access Manager Web コンテナを再起動します。

patchrm コマンド

patchrm コマンドは、スタンドアロンシステムからパッチを削除するために使用します。次に例を示します。

```
# patchrm 120954-03
```

backout スクリプトでは、patchadd コマンドと同様のメッセージが表示されます。ただし、Access Manager SDK コンポーネントだけがインストールされているシステムの場合は表示されません。

パッチを削除したあと、*AccessManager-base* /SUNWam ディレクトリの amsilent ファイルを使用して Access Manager アプリケーションを再配備します。*AccessManager-base* はベースインストールディレクトリです。Solaris システムのデフォルトのベースインストールディレクトリは /opt です。

配備での必要に応じて、amsilent ファイル内のパラメータを設定します。

その後、次のコマンドを実行します (Access Manager が Solaris システムのデフォルトディレクトリにインストールされている場合の例)。

```
# cd /opt/SUNWam/bin
# ./amconfig -s /opt/SUNWam/amsilent
```

patchadd コマンドと patchrm コマンドの詳細および使用例については、該当する Solaris マニュアルページを参照してください。

詳細については、20 ページの「インストール後の注意点」も参照してください。

Solaris 10 ゾーン

Solaris 10 オペレーティングシステムでは、「ゾーン」という新しい概念が導入されました。したがって、パッチを大域ゾーンにのみ追加する新しい -G オプションが patchadd コマンドに追加されています。デフォルトでは、patchadd コマンドは、パッチを適用するパッケージの pkginfo 内で SUNW_PKG_ALLZONES 変数を探します。ただし、すべての Access Manager パッケージに SUNW_PKG_ALLZONES 変数が設定されてい

るとは限らないため、Access Manager 7 2005Q4 が大域ゾーンにインストールされている場合は -G オプションが必要になります。Access Manager が非大域ゾーンにインストールされている場合は、patchadd -G オプションは無効です。

Access Manager 7 2005Q4 のパッチを Solaris システムにインストールする場合は、-G オプションを使用することをお勧めします。次に例を示します。

```
# patchadd -G AM7_patch_dir
```

同様に、Access Manager が大域ゾーンにインストールされている場合は、-G オプションを使用して patchrm コマンドを実行する必要があります。次に例を示します。

```
# patchrm -G 120954-07
```

Linux システムでのパッチのインストール手順

Linux 用パッチをインストールする前に、11 ページの「インストール前の注意点」に示したファイルをバックアップしておく必要があります。

installpatch は、スタンドアロンの Linux システムにパッチをインストールします。次に例を示します。

```
# ./installpatch
```

postpatch スクリプトでは、Solaris システムのメッセージと同様のメッセージが出力されます。ただし、Linux システムでパッチを取り消す手順は、Solaris システムでの手順とは異なります。Linux のパッチを取り消す汎用のスクリプトはありません。下位バージョンのパッチが以前にインストールされていた場合は、そのバージョンを再インストールしてから、postpatch の手順に従って、amconfig スクリプトを実行して Access Manager アプリケーションを再配備できます。

amconfig スクリプトを実行したあと、updateschema.sh スクリプト (パッチ 5 以降のパッチ) を実行して XML ファイルと LDIF ファイルを読み込みます。updateschema.sh スクリプトは、パッチ 7 のインストール後に *patch-home-directory*/120956-07/scripts ディレクトリから使用できます。

amconfig スクリプトと updateschema.sh スクリプトを実行したあと、Access Manager Web コンテナを再起動します。

パッチが Access Manager 7 2005Q4 RTM リリースにインストールされている場合、そのパッチを削除してシステムを RTM 状態に復元するには、reinstallRTM スクリプトを使用して Access Manager の RTM ビットを再インストールする必要があります。このスクリプトは、Access Manager の RTM RPM が格納されているパスを受け取り、その RTM RPM をパッチの適用された RPM の上にインストールします。次に例を示します。

```
# ./scripts/reinstallRTM path_of_AM7_RTM_RPM_directory
```

`reinstallRTM` スクリプトを実行したあと、`amconfig` スクリプトを実行して Access Manager アプリケーションを再配備し、Web コンテナを再起動します。

詳細については、20 ページの「インストール後の注意点」も参照してください。

Windows システムでのパッチのインストール手順

Windows 用パッチをインストールするには、次の要件があります。

- Access Manager 7 2005Q4 が Windows システムにインストールされている必要があります。インストールの詳細については、『Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows』を参照してください。
- パッチスクリプトを実行するには、Windows システム上に ActivePerl 5.8 以降が必要です。

Windows 用パッチのインストール

Windows 用パッチをインストールする前に、11 ページの「インストール前の注意点」に示したファイルをバックアップしておく必要があります。

パッチスクリプトに入力するベースディレクトリパスには、スラッシュ (/) を使用します。例: `c:/sun`

Windows 用パッチをインストールするには、次の手順に従います。

1. Administrators グループのメンバーとして Windows システムにログオンします。
2. Windows 用パッチファイルをダウンロードして解凍するためのディレクトリを作成します。例: `AM7p7`
3. 前の手順で作成したディレクトリに `124296-07.zip` ファイルをダウンロードし、ファイルを解凍します。
4. Java ES 2005Q4 のすべてのサービスを停止します。
5. `AM7p7\scripts\prepatch.pl` スクリプトを実行します。
6. `AM7p7\124296-07.exe` を実行してパッチをインストールします。
7. `AM7p7\scripts\postpatch.pl` スクリプトを実行します。
8. Java ES 2005Q4 のサービスを再起動します。
9. Access Manager アプリケーションを再配備します。詳細については、20 ページの「インストール後の注意点」を参照してください。
10. `AM7p7\scripts\updateschema.pl` スクリプトを実行して Directory Server のサービススキーマを更新します。スクリプトが入力内容を検証し、ファイルを読み込みます。このスクリプトは次のログファイルも書き込みます。

    javaes-install-directory`\AccessManager\AM70Patch-upgrade-schema-` *timestamp*
11. Java ES 2005Q4 のサービスを再起動します。

Windows 用パッチのバックアウト

Windows 用パッチをバックアウトするには、次の手順に従います。

1. Administrators グループのメンバーとして Windows システムにログオンします。
2. `Uninstall_124296-07.bat` ファイルを実行します。
3. `AM7p7\scripts\postbackout.pl` スクリプトを実行します。
4. Access Manager アプリケーションを再配備します。
5. Java ES 2005Q4 のサービスを再起動します。

注: パッチをバックアウトしても、`AM7p7\scripts\updateschema.pl` スクリプトによって追加されたスキーマの変更は Directory Server から削除されません。ただし、パッチをバックアウトしたあとで、これらの変更が Access Manager の機能や使い勝手に影響を与えることはないため、これらの変更を手動で削除する必要はありません。

HP-UX システムでのパッチのインストール手順

HP-UX 用パッチをインストールまたは削除するには、`swinstall` コマンドまたは `swremove` コマンドを使用します。たとえば、スタンドアロンシステムにパッチをインストールするには、次のコマンドを使用します。

```
# swinstall /var/spool/patch/126371-07
```

また、スタンドアロンシステムからパッチを削除するには、次のコマンドを使用します。

```
# swremove 126371-07
```

`swinstall` コマンドと `swremove` コマンドの詳細は、`swinstall` と `swremove` のマニュアルページを参照してください。

パッチのインストールまたは削除を行なったあとは、20 ページの「インストール後の注意点」の説明に従って Access Manager アプリケーションを再配備する必要があります。

Access Manager アプリケーションを再配備したあと、`updateschema.sh` スクリプト (パッチ 5 以降のパッチ) を実行して XML ファイルと LDIF ファイルを読み込みます。`updateschema.sh script` スクリプトは、パッチ 7 のインストール後に *patch-home-directory*`/120956-07/scripts` ディレクトリから使用できます。`amconfig` スクリプトと `updateschema.sh` スクリプトを実行したあと、Access Manager Web コンテナを再起動します。

注: パッチを削除しても、`updateschema.sh` スクリプトによって追加されたスキーマの変更はDirectory Server から削除されません。ただし、パッチを削除したあとで、これらのスキーマの変更が Access Manager の機能や使い勝手に影響を与えることはないため、これらのスキーマの変更を手動で削除する必要はありません。

HP-UX システムへの Access Manager の配備の詳細については、『Sun Java System Access Manager 7 2005Q4 Release Notes for HP-UX』を参照してください。

インストール後の注意点

Access Manager 7 2005Q4 パッチのインストール後の注意点を次に示します。

- 20 ページの「CR# 6254355: postpatch スクリプトの Access Manager アプリケーションが Access Manager のパッチで配備されない」
- 23 ページの「CR# 6436409: 分散認証およびクライアント SDK の WAR ファイルの再配備」

CR# 6254355: postpatch スクリプトの Access Manager アプリケーションが Access Manager のパッチで配備されない

カスタマイズされた WAR ファイルの一部がパッチインストーラで保持されず、カスタマイズされていないバージョンで置き換えられる場合があります。WAR ファイルのカスタマイズ内容を特定して手動で更新するには、次の手順に従うとよいでしょう。

次に示す例では、*AccessManager-base* はベースインストールディレクトリです。デフォルトのベースインストールディレクトリは、Solaris システムの場合は `/opt`、Linux システムの場合は `/opt/sun` です。

Windows システムでは、*AccessManager-base* は *javaes-install-directory*`\AccessManager` です。例: `C:\Program Files\Sun\AccessManager`

パッチが適用される WAR ファイルは次のとおりです。

- `console.war`
- `password.war`
- `services.war`

これらのファイルは、Solaris システムでは *AccessManager-base*`/SUNWam`、Linux システムでは *AccessManager-base*`/identity` にあります。

Windows システムでは、 パッチが適用される WAR ファイルは *AccessManager-base*`\` にあります。

WAR ファイル内で変更可能な内容は次のとおりです。

- プロパティーファイル:
  - Solaris システム: *AccessManager-base*`/SUNWam/locale/*.properties`
  - Linux システム: *AccessManager-base*`/identity/locale/*.properties`
  - Windows システム: *AccessManager-base*`\locale\*.properties`
- タグライブラリ記述子:

  - Solaris システム:
    AccessManager-base/SUNWam/web-src/applications/WEB-INF/*.tld
  - Linux システム:
    AccessManager-base/identity/web-src/applications/WEB-INF/*.tld
  - Windows システム: *AccessManager-base*\web-src\applications\WEB-INF*.tld
- web.xml ファイルと、その構築に使用されるファイル (WEB-INF/web.xml と WEB-INF/*.xml)
- アプリケーションに固有のファイル。JSP (*.jsp) ファイル、画像 (*.gif) ファイル、およびバックグラウンドカラー、フォントサイズなどのスタイルシート (*.css) ファイル

すべてのカスタマイズ内容を確実に保持するには、次の手順に従います。ファイルに変更を加える前に、必ずファイルをバックアップします。

1. パッチをインストールします。
2. WAR ファイルを一時ディレクトリに展開します。たとえば、Solaris システムのデフォルトディレクトリに Access Manager がインストールされている場合は、次のようにします。

   ```
   # cd temporary-directory
   # jar -xvf /opt/SUNWam/console.war
   # jar -xvf /opt/SUNWam/services.war
   # jar -xvf /opt/SUNWam/password.war
   ```
3. 一時ディレクトリで展開されたファイルをチェックして、カスタマイズ済みファイルがパッチインストーラによって変更されたかどうかを確認し、変更されたファイルに元のカスタマイズ内容を手動で追加します。
   AccessManager-base/web-src/ ディレクトリにあっても、パッチが適用される WAR ファイルに含まれていないファイルについては、変更を追加し直す必要はありません。
4. 変更したファイルを使用して WAR ファイルを更新します。たとえば、Solaris システムのデフォルトディレクトリに Access Manager がインストールされている場合は、次のようにします。

   ```
   # cd temporary-directory
   # jar -uvf /opt/SUNWam/console.war $path/$modified file
   # jar -uvf /opt/SUNWam/services.war $path/$modified file
   # jar -uvf /opt/SUNWam/password.war $path/$modified file
   ```

   手順 2 - 4 の例を次に示します。

   ```
   # mkdir /tmp/war.tmp
   # cd /tmp/war.tmp
   # jar -xvf /opt/SUNWam/services.war
   # vi index.html
   # jar -uvf /opt/SUNWam/services.war index.html
   ```

5. パッチによって生成されたサイレント設定ファイル (amsilent) を再利用するか、amsamplesilent テンプレートファイルに基づいてサイレント設定ファイルを新規作成し、そのファイルに次を含む適切な設定変数を設定します。

   - DEPLOY_LEVEL=21
   - DIRECTORY_MODE=5
   - DS_DIRMGRPASSWD、ADMINPASSWD、および AMLDAPUSERPASSWD のパスワード
   - Access Manager Web コンテナの変数

   Windows システムでは、postpatch.pl スクリプトによって生成されたサイレント設定ファイル (amsilent) を再利用し、*AccessManager-base*\setup\AMConfigurator.properties-tmp に有効な値が設定されていることを確認します。次に、このファイルの名前を *AccessManager-base*\setup\AMConfigurator.properties に変更します。

   Web コンテナの変数の詳細については、amsamplesilent ファイルを参照してください。このファイルは、Solaris システムでは /opt/SUNWam/bin ディレクトリ、Linux システムでは /opt/sun/identity/bin ディレクトリにあります。

   Windows システムでは、この設定ファイルは *AccessManager-base*\setup\AMConfigurator.properties です。

6. amconfig スクリプトを次のように実行します。amconfig を実行するには、Directory Server および Access Manager Web コンテナが稼働している必要があります。たとえば、Access Manager がデフォルトのベースインストールディレクトリにインストールされている Solaris システム上で amconfig を実行するには、次のように入力します。

   ```
   # cd /opt/SUNWam/bin
   # ./amconfig -s /opt/SUNWam/amsilent
   ```

7. amconfig スクリプトを実行したあと、Access Manager のプロセスを再起動します。次に例を示します。

   ```
   # cd /opt/SUNWam/bin
   # ./amserver stop
   # ./amserver start
   ```

8. カスタマイズしたすべての JSP ファイルが *AccessManager-base*/SUNWam/web-src/ ディレクトリ (Solaris システムの場合) または *AccessManager-base*/identity/web-src/ (Linux システムの場合) の下の適切なサブディレクトリに配置されていること、およびカスタマイズしたすべてのファイルがバックアップされていることを確認します。

   Windows システムでは、これらのファイルは *AccessManager-base*\web-src\ にあります。

9. Access Manager Web コンテナを再起動します。

`amconfig` スクリプトの実行の詳細については、『Sun Java System Access Manager 7 2005Q4 管理ガイド』の第 1 章「Access Manager 7 2005Q4 の設定スクリプト」を参照してください。

CR# 6436409: 分散認証およびクライアント SDK の WAR ファイルの再配備

分散認証またはクライアント SDK を使用している場合は、パッチをインストールしたあとで、分散認証 WAR ファイルまたはクライアント SDK WAR ファイル、あるいはその両方を再作成して再配備します。詳細については、次のドキュメントを参照してください。

- 分散認証 WAR ファイルの構築: 『Technical Note: Using Access Manager Distributed Authentication』
- クライアント SDK WAR ファイルの構築: 『Sun Java System Access Manager 7 2005Q4 Developer's Guide』の「Installing the Client SDK」
- クライアントSDK WARファイルの配備: 『Sun Java System Access Manager 7 2005Q4 Developer's Guide』の「To Deploy amclientwebapps.war」

Access Manager 7 2005Q6 パッチ 6

Access Manager 7 パッチ 6 (リビジョン 06) により、いくつかの問題が修正されます。その一覧はパッチに含まれている README ファイルに記載されています。パッチ 6 には、次の新機能、問題、および変更されたマニュアルが含まれています。

パッチ 6 での新機能

- 24 ページの「Access Manager は JDK 1.5 `HttpURLConnection setReadTimeout` メソッドをサポートする」
- 25 ページの「プライマリが復旧すると Access Manager SDK はプライマリ Directory Server にフォールバックする」
- 25 ページの「複数の Access Manager インスタンスは個別のログファイルにログを記録する」
- 26 ページの「Access Manager 7 は複数の Cookie ドメインに対応可能」
- 26 ページの「Microsoft IIS 6.0 認証後プラグインは SharePoint Server をサポートする」
- 27 ページの「Access Manager は Internet Explorer 7 をサポートする」

パッチ 6 での既知の問題点と制限事項

- 27 ページの「CR# 6379325 セッションフェイルオーバー中にコンソールにアクセスすると null ポインタ例外がスローされる」
- 27 ページの「CR# 6508103: Windows で管理コンソールの「ヘルプ」をクリックするとアプリケーションエラーが返される」

- 28 ページの「CR# 6564877: Access Manager 7 パッチをインストールすると SAML v2 ファイルが上書きされる」

注 – パッチ 6 をインストールする前に、次のコンポーネントのアップグレードまたはパッチ適用を行うことをお勧めします。

- Sun Java System Web Server 6.1 SP5 以前を使用している場合は、次のサイトからダウンロードできる Web Server 6.1 SP7 にアップグレードします。

  `http://www.sun.com/download/products.xml?id=45c90ca9`

  『Sun Java System Web Server 6.1 SP7 リリースノート』の「アップグレード」で説明されているアップグレードプロセスに従います。
- SunSolve Online (`http://sunsolve.sun.com`) から NSS、JSS、および NSPR 用の最新のセキュリティーパッチをダウンロードしてインストールします。
  - Solaris 8 SPARC プラットフォーム: 119209
  - Solaris 8 x86 プラットフォーム: 119210
  - Solaris 9 SPARC プラットフォーム: 119211
  - Solaris 9 x86 プラットフォーム: 119212
  - Solaris 10 SPARC プラットフォーム: 119213
  - Solaris 10 x86 および AMD64 プラットフォーム: 119214
  - Windows システム: 124392
  - HP-UX システム: 124379

Access Manager は JDK 1.5 `HttpURLConnection setReadTimeout` メソッドをサポートする

`setReadTimeout` メソッドをサポートするために、`AMConfig.properties` ファイルに次の新しいプロパティーが追加され、読み取りのタイムアウト値を設定できるようになりました。

```
com.sun.identity.url.readTimeout
```

Web コンテナで JDK 1.5 が使用されている場合は、多数の `HttpURLConnections` が開いてサーバーがハングアップすることを防止するために、このプロパティーを適切な値に設定して接続をタイムアウトさせるようにしてください。デフォルトは 30000 ミリ秒 (30 秒) です。

`com.sun.identity.url.readTimeout` が `AMConfig.properties` ファイル内に存在しない場合または空の文字列に設定されている場合、`setReadTimeout` メソッドは無視されます。

プライマリが復旧すると **Access Manager SDK** はプライマリ **Directory Server** にフォールバックする

Sun Java System Directory Server がマルチマスターレプリケーション (MMR) 用に設定されている場合、プライマリサーバーがダウンしたあとで復旧すると、Access Manager SDK はプライマリ Directory Server にフォールバックするようになりました。以前は、プライマリサーバーが復旧した後も Access Manager SDK は引き続きセカンダリ Directory Server にアクセスしていました。

この新しい動作をサポートするために、`AMConfig.properties` ファイルに次の新しいプロパティーが追加されました。

```
com.sun.am.ldap.fallback.sleep.minutes
```

このプロパティーは、プライマリサーバーの復旧後にプライマリサーバーにフォールバックする前の、セカンダリ Directory Server インスタンスのスリープ時間を分単位で設定します。デフォルトは 15 分です。

`com.sun.am.ldap.fallback.sleep.minutes` プロパティーは隠されています。このプロパティーをデフォルト (15 分) 以外の値に設定するには、このプロパティーを明示的に `AMConfig.properties` ファイルに追加します。値を 7 分に設定する場合の例を次に示します。

```
com.sun.am.ldap.fallback.sleep.minutes=7
```

新しい値を有効にするために、Access Manager Web コンテナを再起動します。

複数の **Access Manager** インスタンスは個別のログファイルにログを記録する

同じホストサーバーで複数の Access Manager インスタンスが実行されている場合、`AMConfig.properties` ファイルに次の新しいプロパティーを設定することにより、インスタンスごとに異なるログ用サブディレクトリの個別のログファイルにログを記録できるようになりました。

```
com.sun.identity.log.logSubdir
```

デフォルトのログディレクトリを管理コンソールで変更した場合を除き、デフォルトのログディレクトリは次のとおりです。

- Solaris システム: `/var/opt/SUNWam/logs`
- Linux および HP-UX システム: `/var/opt/sun/identity/logs`
- Windows システム: `C:\Sun\JavaES5\identity\logs`

最初の Access Manager インスタンスは、常にデフォルトのログディレクトリにログを記録します。追加の Access Manager インスタンスに対して別のログ用サブディレクトリを指定するには、追加した各インスタンスごとに `AMConfig.properties` ファイルで `com.sun.identity.log.logSubdir` プロパティーを設定します。

たとえば、am-instance-1、am-instance-2、および am-instance-3 という3 つのインスタンスがあり、それらすべてが同じSolaris ホストサーバーで実行されている場合は、プロパティーを次のように設定します。

```
com.sun.identity.log.logSubdir=am-instance-2
com.sun.identity.log.logSubdir=am-instance-3
```

com.sun.identity.log.logSubdir プロパティーは隠されています。必要に応じてこのプロパティーを明示的に AMConfig.properties ファイルに追加してから、Access Manager Web コンテナを再起動してサブディレクトリの値を有効にする必要があります。

その後、Access Manager インスタンスは次のディレクトリにログを記録します。

```
/var/opt/SUNWam/logs/log-files-for-am-instance-1
/var/opt/SUNWam/logs/am-instance-2/log-files-for-am-instance-2
/var/opt/SUNWam/logs/am-instance-3/log-files-for-am-instance-3
```

Access Manager 7 は複数の Cookie ドメインに対応可能

複数の Cookie ドメインをサポートするために、Access Manager に次の新しいプロパティーが追加されました。

```
com.sun.identity.authentication.setCookieToAllDomains
```

デフォルトは true です。この新しいプロパティーは隠されています。値を false に設定するには、このプロパティーを明示的に AMConfig.properties ファイルに追加してから、Access Manager Web コンテナを再起動します。

Microsoft IIS 6.0 認証後プラグインは SharePoint Server をサポートする

Microsoft Internet Information Services (IIS) 6.0 認証プラグインは、Microsoft Office SharePoint Server をサポートするようになりました。ユーザーは、ユーザー ID またはログイン名で Access Manager にログインできます。ただし、SharePoint Server はログイン名を受け入れるため、ユーザーがユーザー ID を指定すると問題が発生します。

SharePoint Server へのログインを可能にするために、認証後プラグイン (ReplayPasswd.java) で次の新しいプロパティーが使用されるようになりました。

```
com.sun.am.sharepoint_login_attr_name
```

この新しいプロパティーは、SharePoint Server での認証に使用されるユーザー属性を指定します。たとえば、次のプロパティーは、認証に共通名 (cn) を使用するように指定します。

```
com.sun.am.sharepoint_login_attr_name=cn
```

認証後プラグインは、com.sun.am.sharepoint_login_attr_name プロパティーを読み取り、そのユーザーに対応する属性値を Directory Server から取得します。次に、プラグインは承認ヘッダーを設定して、ユーザーが SharePoint Server にアクセスできるようにします。

このプロパティーは隠されています。このプロパティーを設定するには、このプロパティーを明示的に AMConfig.properties ファイルに追加してから、Access Manager Web コンテナを再起動して値を有効にします。

Access Manager は Internet Explorer 7 をサポートする

Access Manager 7 2005Q4 パッチ 6 では、Microsoft Windows Internet Explorer 7 がサポートされるようになりました。

CR# 6379325 セッションフェイルオーバー中にコンソールにアクセスすると null ポインタ例外がスローされる

このシナリオでは、Cookie ベースのスティッキー要求ルーティングに対応するように設定されたロードバランサの背後に、複数の Access Manager サーバーがセッションフェイルオーバーモードで配備されています。Access Manager 管理者はロードバランサ経由で Access Manager コンソールにアクセスします。管理者がコンソールにログインすると、Access Manager サーバーの 1 つにセッションが作成されます。そのサーバーがダウンした場合、コンソールセッションは予定どおり別の Access Manager サーバーにフェイルオーバーされます。ただし、管理者はブラウザおよび Web コンテナエラーログに null ポインタ例外が断続的に記録されるという問題に遭遇することがあります。

この問題は、フェイルオーバー時にアクティブになっている Access Manager コンソールセッションのみに影響し、Access Manager サーバーの機能には影響しません。

回避方法: このような null ポインタ例外が断続的に発生することを防ぐには、次の手順を実行します。

- 一時的な解決方法としては、ブラウザの表示を更新するか、いったんコンソールからログアウトして再度ログインします。
- 根本的な解決方法としては、セッションフェイルオーバーに参加しない独立した Access Manager インスタンスに Access Manager コンソールを配備します。

CR# 6508103: Windows で管理コンソールの「ヘルプ」をクリックするとアプリケーションエラーが返される

Windows 2003 Enterprise Edition では、Access Manager が英語以外のロケールで Sun Java System Application Server に配備されている場合、レルムモードの管理コンソールで「ヘルプ」をクリックするとアプリケーションエラーが返されます。

回避方法:

1. *javaes-install-dir*\share\lib\jhall.jar ファイルを %JAVA_HOME%\jre\lib\ext ディレクトリにコピーします。

   ここで、*javaes-install-dir* は Windows のインストールディレクトリです

2. Application Server インスタンスを再起動します。

CR# 6564877: Access Manager 7 パッチをインストールすると SAML v2 ファイルが上書きされる

SAML v2 プラグインがインストールされている場合、パッチをインストールすると SAML v2 の関連ファイルが上書きされ、postpatch スクリプトで次のメッセージが表示されるようになります。

```
The postpatch script detected that the SAML v2 plug-in is installed in your
environment. When you run the amconfig script to redeploy the Access Manager
applications, the script will recreate the amserver.war file and the SAML v2
related files will be lost. Therefore, after you run amconfig, recreate and
redeploy the amserver.war file, as described in the Sun Java System SAML v2
Plug-in for Federation Services User's Guide.
```

回避方法: パッチをインストールして amconfig スクリプトを実行したあと、SAML v2 プラグインを使用する Federation Manager や Access Manager の配備に対して、amserver.war ファイルを再作成および再配備します。

具体的な手順については、『Sun Java System SAML v2 Plug-in for Federation Services User's Guide』の第 2 章「Installing the SAML v2 Plug-in for Federation Services」を参照してください。

Access Manager 7 2005Q4 パッチ 5

Access Manager 7 パッチ 5 (リビジョン 05) により、いくつかの問題が修正されます。その一覧はパッチに含まれている README ファイルに記載されています。パッチ 5 には、次の新機能、問題、および変更されたマニュアルが含まれています。

パッチ 5 での新機能

- 30 ページの「HP-UX システムのサポート」
- 30 ページの「Microsoft Windows システムのサポート」
- 31 ページの「LDIF ファイルと XML ファイルを読み込む新しい updateschema.sh スクリプト」
- 32 ページの「特定のアプリケーションのアイドルセッションタイムアウト値のサポート」
- 33 ページの「CDC サーブレットは、分散認証 UI サーバーに配備できる」
- 33 ページの「CDC サーブレットが Access Manager のログイン URL にリダイレクトされる場合はレルムを指定できる」

パッチ **5** での既知の問題点と制限事項

国際化 **(g11n)** に関する問題

- 45 ページの「CR# 6524251: Windows システム上での Access Manager の設定中に、出力メッセージ内の複数バイト文字が文字化けする」
- 45 ページの「CR# 6526940: 英語以外のロケールの Windows システムに対するパッチ 5 のインストール中に、メッセージテキストではなくプロパティーキーが表示される」

変更されたマニュアル

- 102 ページの「Access Manager がレルムモードから旧バージョンモードに戻らないことについて (6508473)」
- 102 ページの「持続検索の無効化の詳細について (6486927)」
- 103 ページの「Access Manager がサポートする権限とサポートしない権限について (2143066)」
- 104 ページの「Cookie ベースのスティッキー要求ルーティングについて (6476922)」
- 105 ページの「Windows 2003 の Windows デスクトップ SSO の設定について (6487361)」
- 106 ページの「分散認証 UI サーバーのパスワードの設定手順について (6510859)」
- 106 ページの「「新しいサイト名を作成する」のオンラインヘルプ情報を詳細化する必要がある (2144543)」
- 107 ページの「Windows システムの管理者パスワードの設定パラメータが `ADMIN_PASSWD` であることについて (6470793)」

HP-UX システムのサポート

パッチ **126371** は、HP-UX システムに対するサポートを提供します。詳細については、次のトピックを参照してください。

- 19 ページの「HP-UX システムでのパッチのインストール手順」
- 20 ページの「インストール後の注意点」

HP-UX システムへのインストールについては、『Sun Java Enterprise System 2005Q4 インストールガイド(UNIX 版)』を参照してください。

Microsoft Windows システムのサポート

パッチ **124296** は、Windows システムに対するサポートを提供します。詳細については、次のトピックを参照してください。

- 18 ページの「Windows システムでのパッチのインストール手順」
- 20 ページの「インストール後の注意点」
- 38 ページの「Windows システムで使用できるチューニングスクリプト」

Windows システムへのインストールについては、『Sun Java Enterprise System 2005Q4 Installation Guide for Microsoft Windows』を参照してください。

LDIF ファイルと XML ファイルを読み込む新しい updateschema.sh スクリプト

パッチ 5 以降のパッチには、次のファイルを読み込んで Directory Server サービススキーマを更新する updateschema.sh スクリプトが含まれています。

- AddLDAPFilterCondition.xml
- amPolicyConfig_mod_ldfc.xml
- accountLockoutData.xml
- accountLockout.ldif
- idRepoServiceAddAttrSchemaRequest_Cache.xml
- wsf1.1_upgrade.xml
- amAuth_mod.xml
- amAuthCert_mod.xml

Access Manager の以前のリリースでは、これらのファイルを手動で読み込む必要がありました。

updateschema.sh スクリプトを実行するには、次の手順に従います。

1. スーパーユーザー (root) としてログインします。
2. パッチディレクトリに移動します。
3. スクリプトを実行します。Solaris システムの場合の例を示します。

   ```
   # cd /120954-07
   # ./updateschema.sh
   ```

   Windows システムでは、このスクリプトの名前は updateschema.pl です。
4. スクリプトからユーザーの入力を要求されたら、次の項目を入力します。
   - Directory Server のホスト名とポート番号
   - Directory Server の管理ユーザー DN とパスワード
   - amadmin DN とパスワード
5. スクリプトが入力内容を検証し、ファイルを読み込みます。このスクリプトは次のログファイルも書き込みます。
   - Solaris システム: /var/opt/SUMWam/logs/AM70Patch.upgrade.schema. *timestamp*
   - Linux システム: /var/opt/sun/identity/logs/AM70Patch.upgrade.schema. *timestamp*
6. スクリプトの実行が終了したら、Access Manager Web コンテナを再起動します。

注: パッチ 5 をバックアウトした場合、updateschema.sh スクリプトによって追加されたスキーマの変更は Directory Server から削除されません。ただし、パッチをバックアウトしたあとで、これらの変更が Access Manager の機能や使い勝手に影響を与えることはないため、これらの変更を手動で削除する必要はありません。

特定のアプリケーションのアイドルセッションタイムアウト値のサポート

パッチ 5 では、アプリケーションごとに異なるセッションアイドルタイムアウト値を設定できます。企業では、セッションサービスに指定されたセッションアイドルタイムアウトより小さいセッションアイドルタイムアウト値が一部のアプリケーションで必要になる場合があります。たとえば、セッションサービスのセッションアイドルタイムアウト値を 30 分に指定したが、HR アプリケーションはユーザーが 10 分以上アイドル状態だったらタイムアウトするべきである場合などです。

この機能を使用するための要件は、次のとおりです。

- アプリケーションを保護するエージェントは、Access Manager から URL ポリシー決定を適用するように設定する必要があります。
- エージェントは、自己ポリシー決定キャッシュモードで動作するように設定する必要があります。次のプロパティーを参照してください。
  - Web エージェントの場合: `com.sun.am.policy.am.fetch_from_root_resource`
  - J2EE エージェントの場合: `com.sun.identity.policy.client.cacheMode`
- Access Manager の `AMConfig.properties` ファイルで、条件が最後に評価されるようにポリシーコンポーネントの評価順序を指定する必要があります。次のプロパティーを参照してください。

  `com.sun.identity.policy.Policy.policy_evaluation_weights`
- エージェントがローカルにキャッシュされた決定に基づいて許可したアプリケーションアクセスは、Access Manager の条件では認識されません。このため、実際のアプリケーションアイドルタイムアウトの範囲は、アプリケーションのアイドルタイムアウト値から、アプリケーションのアイドルタイムアウトからエージェントのキャッシュ期間を引いた値までになります。

この機能を使用するには、次の手順に従います。

- アプリケーション固有のセッションアイドルタイムアウトを必要とするアプリケーションを保護するポリシーに認証方式条件を追加します。
- 認証方式条件にアプリケーション名とタイムアウト値を指定します。
- アプリケーションのリソースに適用されるすべてのポリシーで、同じアプリケーション名とタイムアウト値を使用します。
- タイムアウト値は分単位で指定します。値が 0 であるか、セッションサービスに指定されたセッションアイドルタイムアウト値より大きい場合、その値は無視され、セッションサービスのタイムアウトが適用されます。

たとえば次の認証方式条件を持つポリシー `http://host.sample.com/hr/*` があるとします。

- 認証方式: LDAP
- アプリケーション名: HR

- タイムアウト値: 10

HR アプリケーションのリソースを保護するために定義されたポリシーが複数ある場合は、すべてのポリシーに条件を追加してください。

個別のセッション内のユーザーが Access Manager エージェントによって保護された HR アプリケーションにアクセスしようとすると、そのユーザーは LDAP 方式への認証を要求されます (ユーザーがまだ認証されていない場合)。

ユーザーがすでに LDAP 方式に認証されている場合は、最後に認証が行われた時間またはそのユーザーが HR アプリケーションに最後にアクセスした時間から 10 分以上経過していなければ、そのユーザーにアクセスが許可されます。それ以外の場合は、ユーザーがアプリケーションにアクセスしようとすると、再度 LDAP 方式への認証が要求されます。

CDC サーブレットは、分散認証 UI サーバーに配備できる

DMZ 内で CDC サーブレットと分散認証 UI サーバーを共存させることにより、クロスドメインシングルサインオン (CDSSO) を使用可能にできます。Access Manager サーバーは、ファイアウォールの背後に配備できるため、CDSSO を実現するために行われる Access Manager へのすべてのアクセスは、分散認証 UI サーバー内の CDC サーブレットによって処理されます。CDSSO を使用可能にするには、各ポリシーエージェントのマニュアルを参照し、次の追加手順を実行してください。

- エージェントの `AMAgent.properties` ファイルを変更して、分散認証側 (クライアント) の CDC サーブレットをポイントします。たとえば、Web エージェントの場合は、次のプロパティーを変更します。

  ```
  com.sun.am.policy.agents.config.cdcservlet.url=
      http://DAhost.DAdomain:DAport/DISTAUTH_DEPLOY_URI/cdcservlet
  ```

- Access Manager で、エージェントで保護する必要があるリソースのポリシーを必要に応じて定義します。たとえば、エージェントが `host.example.com:80` にある場合は、リソースのポリシーを `http://host.example.com:80/*` として定義します。

CDC サーブレットが Access Manager のログイン URL にリダイレクトされる場合はレルムを指定できる

CDC サーブレットに対してレルム名を指定すると、Access Manager のログイン URL へのリダイレクトが発生したときにレルム名が取り込まれ、ユーザーは特定のレルムにログインできます。次に例を示します。

```
com.sun.am.policy.agents.config.cdcservlet.url=
    http://lb.example.com/amserver/cdcservlet?org=realm1
```

証明書認証でユーザープロファイルのマッピングに UPN 値を使用できる

従来の証明書認証では、ユーザープロファイルをマップするために subjectDN の dn コンポーネントだけが使用されていました。現在の Access Manager では、プロファイルのマッピングに SubjectAltNameExt のユーザー主体名 (UPN) の値を使用できます。

複数サーバー環境でログアウトの認証ポストプロセスが発生する

複数サーバー環境で、ユーザーが最初にログインしたサーバーとは別のサーバーをログアウトすると、セッションフェイルオーバーが設定されているかどうかに関係なく、認証ポストプロセスが発生します。

SAML による新しい名前 ID SPI のサポート

SAML は、サイトが SAML 表明に含まれる名前 ID をカスタマイズできるように、新しい名前 ID サービスプロバイダインタフェース (SPI) をサポートします。サイトは、新しい NameIdentifierMapper インタフェースを実装することにより、ユーザーアカウントを SAML 表明の対象に含まれる名前 ID にマップできます。

サイト監視の新しい設定プロパティー

Access Manager のサイト監視機能に、サイト状態チェックの動作を指定できる次の新しいプロパティーが追加されています。

プロパティー	説明
com.sun.identity.urlchecker.invalidate.interval	停止したサイトや無応答のサイトを認識するための時間間隔 (ミリ秒単位)。 デフォルト: 70000 ミリ秒 (70 秒)。
com.sun.identity.urlchecker.sleep.interval	サイト状態チェックをスリープさせる間隔 (ミリ秒単位)。 デフォルト: 30000 ミリ秒 (30 秒)。
com.sun.identity.urlchecker.targeturl	Access Manager のプロセスステータスを確認するための別のターゲット URL。 デフォルト: "/amserver/namingservice".

パッチでは、これらのプロパティーは AMConfig.properties ファイルに追加されません。これらの新しいプロパティーをデフォルト値以外の値で使用するには、次の手順に従います。

1. AMConfig.properties ファイルにプロパティーとその値を追加します。ポリシーエージェントの場合は、これらのプロパティーを AMAgents.properties ファイルに追加します。
2. Access Manager Web コンテナを再起動して、値を有効にします。

ユーザーは認証チェーンで 2 回認証する必要がない

たとえば、次のような場合です。サイトに、3 つの LDAP モジュールを使用して認証チェーンが設定されています。すべてのモジュールが SUFFICIENT に設定され、iplanet-am-auth-shared-state-enabled オプションと iplanet-am-auth-store-shared-state-enabled オプションがどちらも true に設定されています。次に例を示します。

```
<AttributeValuePair>
   <Value>A-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>B-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
   <Value>C-LDAP SUFFICIENT iplanet-am-auth-shared-state-enabled=true
iplanet-am-auth-store-shared-state-enabled=true</Value>
</AttributeValuePair>
```

パッチ 5 では、新しいモジュールオプションとして iplanet-am-auth-shared-state-behavior-pattern オプションが追加されます。このオプションに指定できる値は、 tryFirstPass (デフォルト) と useFirstPass の 2 つです。

ユーザーが (前のシナリオに示したように) 認証を受けるためにユーザー ID とパスワードを 2 回入力しなければならない状況を避けるには、チェーン内のすべてのモジュールで、この新しいオプションを useFirstPass に設定します。従来は、3 番目の LDAP インスタンスにしか存在しないユーザーは、認証を受けるために、ユーザー ID とパスワードを 2 回入力する必要がありました。

パフォーマンスチューニングスクリプトの変更

パッチ 5 には、パフォーマンスチューニングスクリプトに対する次の変更が含まれています。

- 36 ページの「チューニングスクリプトによるパスワードファイルのサポート」
- 36 ページの「チューニングスクリプトで Directory Server から不要な ACI を削除する」
- 37 ページの「チューニングスクリプトで分散認証 UI サーバー Web コンテナを調整できる」
- 38 ページの「amtune-os スクリプトだけで Solaris OS と Linux OS の両方を調整する」
- 38 ページの「Solaris 10 のローカルゾーンでもチューニングスクリプトが最後まで実行される」

- 38 ページの「Windows システムで使用できるチューニングスクリプト」
- 38 ページの「Sun Fire T1000 および T2000 サーバーのチューニングに関する注意点」

40 ページの「CR# 6527663: com.sun.identity.log.resolveHostName プロパティーのデフォルト値を true ではなく false にする」も参照してください。

チューニングスクリプトによるパスワードファイルのサポート

パッチ 5 では、チューニングスクリプトのパスワードをテキストファイルで指定できます。従来は、コマンド行引数としてパスワードを入力するしかなく、セキュリティー上の問題がありました。パスワードファイルを使用するには、必要に応じて次の変数をパスワードファイルに設定します。

```
DS_ADMIN_PASSWORD=DirectoryServer-admin-password
AS_ADMIN_PASSWORD=ApplicationServer8-admin-password
```

たとえば、Application Server 8 を調整する場合は、次のようにします。

```
# ./amtune-as8 password-file
```

password-file には、Application Server 8 の管理者パスワードに設定された `AS_ADMIN_PASSWORD` が含まれます。

チューニングスクリプトは、Directory Server の `ldapmodify`、`ldapsearch`、`db2index`、および `dsconf` ユーティリティーを呼び出すときに、`-j` *password-file* オプションを使用します。

チューニングスクリプトで Directory Server から不要な ACI を削除する

Access Manager 7 2005Q4 がレルムモードでインストールされている場合は、委譲権限を使用してアクセス権が決定されるため、一部の Directory Server ACI が不要です。Access Manager 7 2005Q4 パッチ 5 では、`amtune-prepareDSTuner` スクリプトを実行することにより、不要な ACI を削除できます。このスクリプトは、`remacis.ldif` ファイルから ACI のリストを読み取り、`ldapmodify` ユーティリティーを呼び出してそれらの ACI を削除します。

`amtune-prepareDSTuner` スクリプトを実行して、Solaris、Linux、HP-UX、および Windows システム上の不要な ACI を削除できます。スクリプトの実行方法を含む詳細は、『Technical Note: Sun Java System Access Manager ACI Guide』を参照してください。

チューニングスクリプトで分散認証 UI サーバー Web コンテナを調整できる

分散認証 UI サーバーを Web コンテナに配備したあと、Access Manager のチューニングスクリプトを実行することにより、Web コンテナを調整できます。次の表に示すチューニングスクリプトは、該当する Web コンテナの JVM やその他のチューニングオプションを設定します。

表 2　Access Manager Web コンテナのチューニングスクリプト

Web コンテナ	チューニングスクリプト
`amtune-ws61`	Web Server 6.1
`amtune-as7`	Application Server 7
`amtune-as8`	Application Server Enterprise Edition 8.1

分散認証 UI サーバーの Web コンテナを調整するには、次の手順に従います。

1. 分散認証 UI サーバーが配備されているシステムには Access Manager サーバーがインストールされていないため、(上の表に示した) 該当する Web コンテナのチューニングスクリプト、`amtune-env` 設定ファイル、および `amtune-utils` スクリプトを Access Manager サーバーインストールからコピーします。Solaris または Linux オペレーティングシステムを調整する場合は、`amtune-os` スクリプトもコピーします。
2. `amtune-env` 設定ファイルのパラメータを編集して、Web コンテナとチューニングのオプションを指定します。スクリプトを REVIEW モードで実行するため、`amtune-env` ファイルに `AMTUNE_MODE=REVIEW` を設定します。
3. Web コンテナのチューニングスクリプトを REVIEW モードで実行します。REVIEW モードでは、スクリプトは `amtune-env` ファイルの値に従ってチューニングによる変更箇所を示しますが、配備に対する実際の変更は行いません。
4. デバッグログファイルで、推奨されるチューニングを確認します。必要な場合は、この実行結果に基づいて `amtune-env` ファイルに変更を加えます。
5. チューニングによる変更を行うため、`amtune-env` ファイルに `AMTUNE_MODE=CHANGE` を設定します。
6. チューニングスクリプトを CHANGE モードで実行し、配備に対してチューニングによる変更を行います。

チューニングスクリプトを実行して Access Manager Web コンテナを調整する方法の詳細は、『Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide』の第 2 章「Access Manager Tuning Scripts」を参照してください。

amtune-os スクリプトだけで Solaris OS と Linux OS の両方を調整する

パッチ 5 には、Solaris OS と Linux OS の両方を調整する amtune-os スクリプトが含まれています。このスクリプトは、uname -s コマンドの結果から OS の種類を判定します。従来の Access Manager には、各 OS を調整するために別々の amtune-os スクリプトが用意されていました。

Solaris 10 のローカルゾーンでもチューニングスクリプトが最後まで実行される

Solaris 10 のローカルゾーンに Access Manager がインストールされている場合は、amtune-os 以外のすべてのチューニングスクリプトをローカルゾーンで実行できます。amtune-os スクリプトは、ローカルゾーンでは警告メッセージを表示し、OS のチューニングを行いません。その後、要求されたほかのチューニングスクリプトの実行を継続します。従来は、ローカルゾーンでは、amtune-os スクリプトは中断し、要求された後続のチューニングスクリプトは実行されませんでした。

Solaris 10 の大域ゾーンでは、amtune スクリプトが実行を要求されたほかのスクリプトとともに amtune-os を呼び出して OS を調整します。

Windows システムで使用できるチューニングスクリプト

パッチ 5 には、Windows システム用のチューニングスクリプトが含まれています。Windows システムでのチューニングスクリプトの実行は、Solaris システムや Linux システムでの実行とほぼ同じですが、次のような違いがあります。

- Windows のスクリプトは Perl で作成されているため、Active Perl 5.8 を実行する必要があります。
- Directory Server を調整する場合は、amtune-prepareDSTuner.pl スクリプトを実行したあと、amtune-utils.pl、amtune-directory.pl、remacis.ldif、および amtune-samplepassordfile ファイルを Directory Server システムにコピーしてください。これは、このスクリプトがこれらのファイルを圧縮できないためです。
- Windows オペレーティングシステムを調整するスクリプトは用意されていません。
- ゾーンのサポートは提供されていません。
- スクリプトを実行する前に、amtune-env.pl ファイルの $BASEDIR パラメータを Access Manager のインストールディレクトリに設定してください。

Sun Fire T1000 および T2000 サーバーのチューニングに関する注意点

Access Manager が Sun Fire T1000 または T2000 サーバーにインストールされている場合、パッチ 5 の Web Server 6.1 および Application Server 8 用のチューニングスクリプトは、JVM GC ParallelGCThreads パラメータを 8 に設定します。

```
-XX:ParallelGCThreads=8
```

このパラメータは、32 スレッドを実行可能なシステムでは不必要に多い可能性があるガベージコレクションスレッドの数を減らします。ただし、Sun Fire T1000 または T2000 サーバーなどの 32 仮想 CPU マシンで、フルガベージコレクションのアクティビティーが最小限に抑えられている場合は、この値を 16 - 20 まで増やすことができます。

また、CoolThreads テクノロジによる CMT プロセッサを搭載した Solaris SPARC システムでは、`/etc/opt/SUNWam/config/AMConfig.properties` ファイルの末尾に次のプロパティーを追加することをお勧めします。

```
com.sun.am.concurrencyRate=value
```

value のデフォルトは 16 ですが、Sun Fire T1000 または T2000 サーバーのコア数に応じて、このプロパティーをさらに小さい値に設定できます。

IIS 6.0 ポリシーエージェントの基本認証

Microsoft Internet Information Services (IIS) 6.0 の基本認証を有効にするには、ポリシーエージェントがユーザーの名前とパスワードを取得する必要があります。パッチ 5 には、ユーザーのパスワードの DES 暗号化を使用してこの機能を有効にする次の新しいクラスが含まれています。

- `DESGenKey.java` は、ユーザーのパスワードの暗号化と復号化に使用される一意の鍵を生成します。
- `ReplayPasswd.java` は、`AMConfig.properties` ファイルの `com.sun.am.replaypasswd.key` プロパティーから暗号化鍵の値を読み取り、パスワードを暗号化し、それを `sunIdentityUserPassword` セッションプロパティーに割り当てます。

IIS 6.0 の基本認証を使用するには、Access Manager サーバー側と IIS 6.0 ポリシーエージェント側の両方の手順を実行する必要があります。

Access Manager サーバー側では、次の手順に従います。

1. `DESGenKey.java` を実行して、パスワードの暗号化と復号化に使用する一意の暗号化鍵を生成します。`DESGenKey.java` ファイルは、Solaris システムでは `/opt/SUNWam/lib` ディレクトリの `am_sdk.jar` に含まれている `com/sun/identity/common` ディレクトリの下にあります。たとえば、次のコマンドで暗号化鍵を生成します。

   ```
   # cd /opt/SUNWam/lib
   # java -cp am_sdk.jar com.sun.identity.common.DESGenKey
   ```

2. 手順 1 で得られた暗号化鍵を `AMConfig.properties` ファイルの `com.sun.am.replaypasswd.key` プロパティーに割り当てます。
3. `ReplayPasswd.java` を認証後プラグインとして配備します。プラグインを設定するときは、次のように完全なクラス名を使用します。
   `com.sun.identity.authentication.spi.ReplayPasswd`

IIS 6.0 ポリシーエージェント側では、次の手順に従います。

1. サーバー側で得られた暗号化鍵の値を `AMAgent.properties` ファイルの `com.sun.am.replaypasswd.key` プロパティーに割り当てます。Access Manager サーバーと IIS 6.0 ポリシーエージェントの両方で同じ暗号鍵を使用してください。
2. IIS 6.0 マネージャーで、基本認証を有効にします。

IIS 6.0 ポリシーエージェントがセッションの応答から暗号化されたパスワードを読み取り、`com.sun.am.replaypasswd.key` プロパティーからパスワードを復号化し、認証ヘッダーを設定することにより、基本認証の実行が可能になります。

IIS 6.0 ポリシーエージェントについては、『Sun Java System Access Manager Policy Agent 2.2 Guide for Microsoft Internet Information Services 6.0』を参照してください。

CR# 6567746: HP-UX システムでパスワード再試行回数を超過した場合、Access Manager パッチ 5 は間違ったエラーコード値を報告する

ユーザーのアカウントがロックされている場合、パスワード再試行回数を超過すると、HP-UX システムの Access Manager 7 2005Q4 パッチ 5 は `errorCode = 107` ではなく `errorCode = null` を報告します。

回避方法: なし。

CR# 6527663: `com.sun.identity.log.resolveHostName` プロパティーのデフォルト値を `true` ではなく `false` にする

`amtune-identity` チューニングスクリプトを実行する前に、`false` に設定した次のプロパティーを `AMConfig.properties` ファイルに追加することをお勧めします。

```
com.sun.identity.log.resolveHostName=false
```

値を `false` にすることで、ホスト名解決の負担が最小限に抑えられ、パフォーマンスが向上します。ただし、クライアントマシンのホスト名を `amAuthentication.access` ログに出力する場合は、この値を `true` に設定してください。

CR# 6527528: パッチを削除すると、クリアテキスト形式の `amldapuser` パスワードを含む XML ファイルが残る

Access Manager のフルサーバーインストールからパッチ 5 を削除すると、`amAuthLDAP.xml` ファイルと `amPolicyConfig.xml` ファイルに、クリアテキスト形式の `amldapuser` パスワードが含まれています。これらのファイルは、使用中のプラットフォームに応じて、次のディレクトリにあります。

- Solaris システム: `/etc/opt/SUNWam/config/xml`
- Linux および HP-UX システム: `/etc/opt/sun/identity/config/xml`

回避方法: amAuthLDAP.xml ファイルと amPolicyConfig.xml ファイルを編集して、クリアテキスト方式のパスワードを削除します。

CR# 6527516: WebLogic 上のフルサーバーでは JAX-RPC 1.0 JAR ファイルがクライアント SDK と通信する必要がある

Access Manager 7 2005Q4 パッチでは、BEA WebLogic Server 用の Access Manager 設定スクリプト (amwl81config) が WebLogic インスタンスの classpath に JAX-RPC 1.1 JAR ファイルを追加します。この変更は Sun Java System Portal Server などの製品には有用ですが、WebLogic Server に配備されたフルサーバーインストール (DEPLOY_LEVEL=1) はクライアント SDK インストールと通信できないため、それ以降は例外が発生します。

Access Manager 7 2005Q4 サーバーが BEA WebLogic Server にインストールされている場合は、startWebLogic.sh スクリプトの CLASSPATH を、Access Manager のクライアント SDK と通信する JAX-RPC 1.0 JAR ファイルの場所に設定する必要があります。

回避方法: Access Manager パッチを適用する前に、WebLogic Server インスタンスが JAX-RPC 1.1 JAR ファイルではなく JAX-RPC 1.0 JAR ファイルを使用するように、startWebLogic.sh スクリプトの CLASSPATH を設定します。

1. Access Manager サーバーで、スーパーユーザー (root) としてログインするか、スーパーユーザーになります。
2. startWebLogic.sh スクリプトを編集し、JAX-RPC 1.0 JAR ファイルを使用するように CLASSPATH を置き換えます。次に例を示します。

現在の値:

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-spi.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-impl.jar:
```

新しい値:

```
CLASSPATH=/etc/opt/SUNWam/config:
AccessManager-base/AccessManager-package-dir/lib/jax-qname.jar:
AccessManager-base/AccessManager-package-dir/lib/namespace.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc_1.0/jaxrpc-api.jar:
AccessManager-base/AccessManager-package-dir/lib/jaxrpc-ri.jar:
```

AccessManager-base は、ベースインストールディレクトリです。デフォルト値は、Solaris システムでは /opt、Linux システムおよび HP-UX システムでは /opt/sun です。*AccessManager-package-dir* は、Access Manager のパッケージディレクトリです。

5. WebLogic Server インスタンスを再起動します。

CR# 6523499: パッチ 5 の amsilent ファイルが Linux システム上のすべてのユーザーに対して読み込み可能になっている

Linux システムでは、postpatch スクリプトは、すべてのユーザーに読み取りアクセスを許可する 644 のアクセス権で /opt/sun/identity/amsilent ファイルを作成します。

回避方法: installpatch スクリプトを実行したあとで、所有者だけに読み取りと書き込みのアクセスを許可するように amsilent ファイルのアクセス権を変更します。次に例を示します。

```
# chmod 600 /opt/sun/identity/amsilent
```

CR# 6520326: 同じサーバー上の 2 つめの Access Manager インスタンスにパッチ 5 を適用すると、1 つめのインスタンスの serverconfig.xml が上書きされる

この配備シナリオでは、2 つの Access Manager インスタンスが同じホストサーバーに配備され、各インスタンスは異なる Web コンテナインスタンス上にあります。次の手順を実行します。

1. パッチ 5 を適用します。
2. amsilent ファイルを変更し、1 つめの Access Manager インスタンスを再配備します。
3. 2 つめの Access Manager インスタンスのために再度 amsilent を変更し、そのインスタンスを再配備します。

amsilent ファイルに NEW_INSTANCE=false が設定されていると、1 つめの Access Manager インスタンス用の serverconfig.xml ファイルが 2 つめの Access Manager インスタンスの情報で上書きされます。それ以降、1 つめの Access Manager インスタンスの再起動は失敗します。serverconfig.xml ファイルは、使用中のプラットフォームに応じて、次のディレクトリにあります。

- Solaris システム: /etc/opt/SUNWam/config
- Linux システム: /etc/opt/sun/identity/config

回避方法: 2 つめの Access Manager を配備するときに、amsilent ファイルに NEW_INSTANCE=true を設定します。2 つめの Access Manager インスタンス用の serverconfig.xml ファイルが正しい情報で更新され、1 つめの Access Manager インスタンス用の serverconfig.xml ファイルが上書きされません。

CR# 6520016: パッチ 5 の SDK のみのインストールで、samples ディレクトリ内の Makefile が上書きされる

パッチ 5 を SDK のみのマシンに適用すると、samples ディレクトリ内の Makefile が上書きされます。

回避方法: パッチ 5 を SDK のみのマシンに適用するときは再設定の必要はありませんが、samples ディレクトリ内の Makefile を使用する場合は、次の手順に従って samples ディレクトリ内の Makefile の LDIF ファイルとプロパティーファイルを更新します。つまり、タグスワッピングを実行します。

1. DEPLOY_LEVEL=14 で amconfig スクリプトを実行することにより、SDK をアンインストールして Web コンテナを設定解除します。
2. DEPLOY_LEVEL=4 で amconfig スクリプトを実行することにより、SDK を再インストールして Web コンテナを再設定します。

CR#6515502: LDAPv3 リポジトリプラグインがエイリアス検索属性を正しく処理しないことがある

ほとんどの検索では、この問題は修正されています。ただし、エイリアス検索属性を設定するときは注意してください。エイリアス検索属性の値を組織内で一意にする必要があります。複数のエイリアス検索属性が設定された場合は、データストア内のあるエントリが一方の属性に一致し、別のエントリがもう一方の属性に一致する可能性があります。このような場合、Access Manager サーバーは次のエラーをスローします。

```
An internal authentication error has occurred. Contact your system administrator.
```

回避方法: なし

CR# 6515383: 分散認証と J2EE エージェントが同じ Web コンテナで動作しない

分散認証 UI サーバーと J2EE ポリシーエージェントは、同じ Web コンテナにインストールすると動作しません。

回避方法: 2 つめの Web コンテナインスタンスを作成し、分散認証 UI サーバーと J2EE ポリシーエージェントを Web コンテナの異なるインスタンスに配備します。

CR# 6508103: Windows システム上の Application Server で、オンラインヘルプにアプリケーションエラーが返される

Windows システム上の Sun Java System Application Server に Access Manager を配備した場合、レルムモードコンソールで「ヘルプ」をクリックすると、ヘルプ画面の左側のパネルにアプリケーションエラーが返されます。

回避方法: *javaes-install-dir*\share\lib\jhall.jar ファイルを JAVA_HOME\jre\lib\ext ディレクトリにコピーし、Application Server を再起動します。

CR# 6507383 および CR# 6507377: 分散認証には明示的な goto URL パラメータが必要である

明示的な goto URL パラメータを指定しなかった場合、分散認証 UI サーバーは Access Manager に指定された成功 URL の goto にリダイレクトしようとします。このリダイレクトは、次の理由で失敗することがあります。

- URL が相対的で、対応するページが分散認証 UI サーバーに用意されていない
- URL が絶対的で、ブラウザが URL に到達できない

回避方法: 分散認証 UI サーバーに対して、常に明示的な goto URL パラメータを指定します。

CR# 6402167: LDAP JDK 4.18 によって LDAP クライアント/Directory Server に問題が発生する

Access Manager 7 2005Q4 は、Java ES 2005Q4 リリースの一部である LDAP JDK 4.18 とともにリリースされましたが、その結果、Access Manager と Directory Server の通信にさまざまな問題が発生しました。

回避方法: 次のいずれかの Sun Java System LDAP Java Development Kit パッチを適用します。

- Solaris OS、SPARC、および x86 プラットフォーム: 119725-04
- Linux OS: 120834-02

これらのパッチは、SunSolve Online (http://sunsolve.sun.com) から入手できます。

CR# 6352135: 分散認証 UI サーバーのファイルが誤った場所にインストールされる

Solaris システムでは、Java ES インストーラが分散認証 UI サーバーの Makefile.distAuthUI ファイル、README.distAuthUI ファイル、および amauthdistui.war ファイルを誤った場所 (/opt/SUNComm/SUNWam) にインストールします。

回避方法: 上記のファイルを正しい場所 (/opt/SUNWam) にコピーします。

注: パッチで修正された分散認証 UI サーバーの問題は、/opt/SUNComm/SUNWam/amauthdistui.war ファイルに格納されるため、Access Manager サーバーにパッチを適用し、この WAR ファイルを再構築して配備する場合は、上記のファイルも /opt/SUNWam ディレクトリにコピーしてください。

CR# 6522720: Windows および HP-UX システム上では、複数バイト文字を用いてコンソールオンラインヘルプの検索ができない

Access Manager が日本語などの複数バイト文字を使用するロケールで Windows システムまたは HP-UX システムにインストールされている場合、複数バイト文字を使用して入力されたキーワードによるコンソールオンラインヘルプの検索はできません。

回避方法: なし

パッチ 6 での更新情報: Windows システムでは、この問題は Access Manager 7 2005Q4 パッチ 6 で修正されます。ただし、HP-UX システムではこの問題が引き続き存在します。

CR# 6524251: Windows システム上での Access Manager の設定中に、出力メッセージ内の複数バイト文字が文字化けする

Access Manager が日本語や中国語などの Windows システムにインストールされている場合、Access Manager の設定中に端末ウィンドウに出力されるメッセージ内の複数バイト文字が文字化けします。

回避方法: なし。ただし、この問題は設定自体には影響しません。

CR# 6526940: 英語以外のロケールの Windows システムに対するパッチ 5 のインストール中に、メッセージテキストではなくプロパティーキーが表示される

英語以外のロケールの Windows システムにパッチ 5 (124296-05) をインストールすると、インストールパネルの一部の文字列が実際のメッセージテキストではなくプロパティーキーとして表示されます。表示されるプロパティーキーは、たとえば、`PRODUCT_NAME`、`JES_Patch_FinishPanel_Text1`、`JES_Patch_FinishPanel_Text2` などです。

回避方法: なし

CR# 6513653: `com.iplanet.am.session.purgedelay` プロパティーの設定で問題が発生する

Access Manager の `amtune` スクリプトは、できるだけ多くの Access Manager セッションを許可するため、`com.iplanet.am.session.purgedelay` プロパティーを 1 に設定します。このプロパティーは、パージセッション操作を遅延する時間を分単位で指定します。ただし、Sun Java System Portal Server などのクライアントでは、値が 1 では不十分な場合があります。

回避方法: `amtune` スクリプトを実行したあとで、次のようにして `com.iplanet.am.session.purgedelay` プロパティーをリセットします。

1. AMConfig.properties ファイルで、このプロパティーを新しい値に設定します。次に例を示します。

   ```
   com.iplanet.am.session.purgedelay=5
   ```

2. Access Manager Web コンテナを再起動して、新しい値を有効にします。

Access Manager 7 2005Q4 パッチ 4

Access Manager 7 2005Q4 パッチ 4 (リビジョン 04) では、次の問題を修正します。

- CR# 6463796: genericHTML の iPlanetAMClientDetection サービスを無効にすると、Access Manager の HTML ページにアクセスできない
- CR# 6463779: 分散認証の amProfile_Client と Access Manager サーバーの amProfile_Server が無害な例外でいっぱいになる
- CR# 6463730: goto パラメータと gx-charset パラメータにクロスサイトスクリプト (XSS) の脆弱性が存在する
- CR# 6435889: RestrictedTokenContext が設定されていないため、Session.getSession メソッドが失敗する

パッチ 4 での既知の問題点と制限事項

- 46 ページの「CR# 6470055: 分散認証 UI サーバーのパフォーマンスの改善」
- 47 ページの「CR# 6455079: パスワードが変更されたときに、パスワードリセットサービスから通知エラーが報告される」

CR# 6470055: 分散認証 UI サーバーのパフォーマンスの改善

分散認証 UI サーバーユーザーのユーザー属性の読み取り、検索、および比較のパフォーマンスを改善するには、次の手順を実行します。

1. Makefile.distAuthUI ファイルで、アプリケーションユーザー名を anonymous から別のユーザーに変更します。次に例を示します。

   ```
   APPLICATION_USERNAME=user1
   ```

2. Directory Server で、新しいユーザー (たとえば、user1) と ACI を追加し、ユーザー属性の読み取り、検索、および比較を許可します。次の例では、新しい ACI を追加しています。

   ```
   dn:ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com
   changetype:modify add:aci
   aci: (target="ldap:///ou=1.0,ou=SunAMClientData,ou=ClientData,dc=example,dc=com")
   (targetattr = *")(version 3.0;
   acl "SunAM client data access to a Distributed Auth App User";
   allow (read, search, compare)
   userdn =  "ldap:///uid=user1,ou=people,dc=example,dc=com";)
   ```

CR# 6455079: パスワードが変更されたときに、パスワードリセットサービスから通知エラーが報告される

パスワードが変更されると、Access Manager は資格を取得していない送信者名 Identity-Server を使用して電子メール通知を送信します。その結果、amPasswordReset ログにエラーが書き込まれます。次に例を示します。

```
07/19/2006 10:26:04:010 AM PDT: Thread[service-j2ee,5,main]
ERROR: Could not send email to user [Ljava.lang.String;@999262
com.sun.mail.smtp.SMTPSendFailedException: 553 5.5.4 <Identity-Server>...
Domain name required for sender address Identity-Server
```

回避方法: amPasswordResetModuleMsgs.properties ファイルで、次のようにしてホストサーバーの完全修飾ドメイン名が含まれるように from アドレスを変更します。

1. from アドレスのラベルを変更します。次に例を示します。

   ```
   fromAddress.label=<Identity-Server@amhost.example.com>
   ```

2. lockOutEmailFrom プロパティーを変更して、正しい from アドレスがロックアウト通知に確実に使用されるようにします。次に例を示します。

   ```
   lockOutEmailFrom=<Identity-Server@amhost.example.com>
   ```

   amPasswordResetModuleMsgs.properties ファイルは、Solaris システムの場合は *AccessManager-base*/SUNWam/locale ディレクトリ、Linux システムの場合は *AccessManager-base*/identity/locale ディレクトリにあります。

   AccessManager-base は、ベースインストールディレクトリです。デフォルトのベースインストールディレクトリは、Solaris システムの場合は /opt、Linux システムの場合は /opt/sun です。

Access Manager 7 2005Q4 パッチ 3

Access Manager 7 パッチ 3 (リビジョン 03) により、いくつかの問題が修正されます。その一覧はパッチに含まれている README ファイルに記載されています。パッチ 3 には、次に示す新機能と既知の問題があります。

パッチ 3 での新機能

- 48 ページの「サイト監視の新しい設定プロパティー」
- 49 ページの「Liberty Identity Web Services Framework (ID-WSF) 1.1 のサポート」

パッチ 3 での既知の問題点と制限事項

- 50 ページの「CR# 6463779 分散認証の amProfile_Client ログと Access Manager サーバーの amProfile_Server ログが無害な例外でいっぱいになる」
- 51 ページの「CR# 6460974 デフォルトの分散認証アプリケーションユーザーは amadmin にしないようにする」

サイト監視の新しい設定プロパティー

Access Manager のサイト監視機能に、次に示す新しいプロパティーが追加されています。

プロパティー	説明

com.sun.identity.sitemonitor.interval	サイト監視の間隔です (ミリ秒単位)。サイト監視機能は、指定された間隔で各サイトの可用性をチェックします。デフォルト: 60000 ミリ秒 (1 分)。
com.sun.identity.sitemonitor.timeout	サイトの可用性チェックのタイムアウトです (ミリ秒単位)。サイト監視機能は、指定された時間だけサイトからの応答を待ちます。デフォルト: 5000 ミリ秒 (5 秒)。

パッチでは、これらのプロパティーは AMConfig.properties ファイルに追加されません。これらの新しいプロパティーをデフォルト値以外の値で使用するには、次の手順に従います。

1. 各プロパティーとその値を AMConfig.properties ファイルに追加します。このファイルはプラットフォームによって次のディレクトリにあります。
   - Solaris システム: /etc/opt/SUNWam/config
   - Linux システム: /etc/opt/sun/identity/config

   ポリシーエージェントの場合は、これらのプロパティーを AMAgents.properties ファイルに追加します。
2. Access Manager Web コンテナを再起動して、値を有効にします。

カスタム実装。また、com.sun.identity.sitemonitor.SiteStatusCheck クラスでは、次のインタフェースを使用して、サイトの可用性チェックに使用する独自の実装をカスタマイズすることもできます。

```
package com.iplanet.services.naming.WebtopNaming$SiteStatusCheck
```

各実装クラスは doCheckSiteStatus メソッドを使用する必要があります。

```
public interface SiteStatusCheck {
public boolean doCheckSiteStatus(URL siteurl);
}
```

Liberty Identity Web Services Framework (ID-WSF) 1.1 のサポート

Access Manager 7 パッチ 3 では、ID-WSF のデフォルトのバージョンは WSF1.1 です。ID-WSF をトリガーするために個別の設定を行う必要はありませんが、サンプルでは新しいセキュリティー機構を使用する必要があります。ID-WSF1.1 の新しいセキュリティー機構は次のとおりです。

```
urn:liberty:security:2005-02:null:X509
urn:liberty:security:2005-02:TLS:X509
urn:liberty:security:2005-02:ClientTLS:X509
urn:liberty:security:2005-02:null:SAML
```

```
urn:liberty:security:2005-02:TLS:SAML
urn:liberty:security:2005-02:ClientTLS:SAML
urn:liberty:security:2005-02:null:Bearer
urn:liberty:security:2005-02:TLS:Bearer
urn:liberty:security:2005-02:ClientTLS:Bearer
```

Liberty ID-WSF サポートの新しいプロパティー

`com.sun.identity.liberty.wsf.version` プロパティーは、Access Manager が WSC として動作しているときに、受信メッセージやリソースオファリングから Liberty ID-WSF のフレームワークを判定できない場合に、そのフレームワークを決定します。指定できる値は 1.0 または 1.1 で、デフォルトは 1.1 です。

注 パッチのインストールでは、`com.sun.identity.liberty.wsf.version` プロパティーは `AMConfig.properties` ファイルに追加されません (CR# 6458184)。この新しいプロパティーを使用するには、パッチのインストール後、このプロパティーを `AMConfig.properties` ファイルに追加して適切な値を設定し、Access Manager Web コンテナを再起動します。

Access Manager 7 パッチ 3 のインストール後、次のコマンドを実行してスキーマの変更を読み込みます (Access Manager が Solaris システムのデフォルトディレクトリにインストールされている場合の例)。

```
# /opt/SUNWam/bin/amadmin -u amadmin -w amadmin_password
-t /etc/opt/SUNWam/wsf1.1_upgrade.xml
```

ID-WSF 検索登録では、登録時にこれらの新しいセキュリティー機構を使用できます。また、WSC は WSP との通信中に、使用するバージョンを自動的に検出できます。ID-WSF1.1 を設定するには、製品に含まれている Liberty ID-FF sample1 および ID-WSF のサンプルの Readme ファイルに従ってください。

CR# 6463779 分散認証の amProfile_Client ログと Access Manager サーバーの amProfile_Server ログが無害な例外でいっぱいになる

分散認証 UI を介して Access Manager サーバーに要求があると、`distAuth/amProfile_Client` ログと Access Manager サーバーの `debug/amProfile_Server` ログに例外が記録されます。多くのセッションのあとでは、`amProfile_Client` ログは数ギガバイト、Access Manager サーバーの `amProfile_Server` ログは数メガバイトになる場合があります。このような例外がログに記録されることによって機能が失われることはありませんが、ユーザーに誤ったアラームが発生したり、ハードディスク容量がログでいっぱいになったりする原因になります。

回避方法: ログファイルの内容を null にする `cron` ジョブを実行します。次に例を示します。

- 分散認証 UI クライアントマシンで、トラフィック量に応じて数時間ごとに "`cat /dev/null > distAuth/amProfile_Client`" を実行します。

- Access Manager サーバーで、数時間ごとではなく数日ごとに "`cat /dev/null > /var/opt/SUNWam/debug/amProfile_Server`" を実行します。

CR# 6460974 デフォルトの分散認証アプリケーションユーザーは amadmin にしないようにする

分散認証 UI サーバーを配備する場合は、分散認証の管理者を `amadmin` にするべきではありません。デフォルトの分散認証アプリケーションユーザーは、`Makefile.distAuthUI` ファイルでは `amadmin` であり、クライアント側で `distAuth.war` ファイルが配備されたあと `AMConfig.properties` ファイルでも同様になります。`amadmin` ユーザーは `AppSSOToken` を持っていますが、これは `amadmin` セッションがタイムアウトすると期限切れになり、それによって `amSecurity` ログファイル (デフォルトでは `/tmp/distAuth` ディレクトリにある) に FATAL ERROR が記録されることがあります。

回避方法: 分散認証アプリケーションユーザーとして `UrlAccessAgent` を指定します。次に例を示します。

クライアントの Web コンテナに `distAuth.war` ファイルを配備する前に、`Makefile.distAuthUI` ファイルで次のパラメータを変更します。

```
APPLICATION_USERNAME=UrlAccessAgent
APPLICATION_PASSWORD=shared-secret-password or amldapuser-password
```

または

クライアントの Web コンテナに `distAuth.war` ファイルを配備したあとで、各 Access Manager サーバーの `AMConfig.properties` ファイルで次のプロパティーを変更します。

```
com.sun.identity.agents.app.username=UrlAccessAgent
com.iplanet.am.service.password=shared-secret-password or amldapuser-password
```

55 ページの「CR# 6440697: 分散認証は amadmin ユーザー以外のユーザーで実行するようにする」も参照してください。

CR# 6460576 コンソールのオンラインヘルプの「フィルタを適用したロール」にユーザーサービスへのリンクがない

Access Manager コンソールのオンラインヘルプには、「フィルタを適用したロール」の下にユーザーサービスへのリンクがありません。オンラインヘルプで、「目次」、「フィルタを適用したロール」、「フィルタを作成する」の順に移動します。ページの下へ移動すると、選択したアイデンティティーの種類に応じてサービスの一覧が表示されますが、ユーザーサービスへのリンクは用意されていません。

回避方法: なし

CR# 6460085 reinstallRTM を実行して Web アプリケーションを再配備すると、WebSphere 上のサーバーにアクセスできなくなる

Red Hat Linux AS 3.0 Update 4 で IBM WebSphere Application Server 5.1.1.6 上の DEPLOY_LEVEL=1 配備に Access Manager 7 パッチ 3 を適用したあと、reinstallRTM スクリプトを実行して RTM RPM を復元します。次に、reinstallRTM スクリプトによって生成された amsilent ファイルを編集してから、Web アプリケーションを再配備します。stopServer.sh スクリプトと startServer.sh スクリプトを使用して WebSphere を再起動します。しかし、ログインページにアクセスすると、amlcontroller フィルタに関連する 500 エラーが WebSphere で表示されます。

この問題は、reinstallRTM スクリプトによって生成される新しい server.xml ファイルが破損しているために発生します。

回避方法: amconfig スクリプトでバックアップした server.xml ファイルは有効です。この以前のコピーを次の手順で使用します。

1. サーバーを停止します。
2. 破損している server.xml を、amconfig スクリプトでバックアップしておいたコピーで置き換えます。

   amconfig スクリプトでバックアップされた server.xml ファイルの名前は server.xml-orig-*pid* になります。ここで、*pid* は amwas51config スクリプトのプロセス ID です。このファイルは、次のディレクトリにあります。

   WebSphere-home-directory/config/cells/*WebSphere-cell*/nodes/*WebSphere-node*/servers/*server-name*
3. サーバーを再起動します。

CR# 6455757: アップグレードの前に sunISManagerOrganization マーカークラスを組織に追加する必要がある

Access Manager 7 リリースより前に作成された Access Manager DIT 内の組織は、sunISManagerOrganization オブジェクトクラスを持たない場合があります。また、Access Manager 以外の製品で作成された組織も、その定義に sunISManagerOrganization オブジェクトクラスを持ちません。

回避方法: Access Manager 7 2005Q4 にアップグレードする前に、DIT 内のすべての組織の定義に sunISManagerOrganization オブジェクトクラスが含まれていることを確認します。アップグレードの前に、必要に応じてこのオブジェクトクラスを手動で追加します。

CR# 6454489: Access Manager 7 2005Q4 パッチ 2 のアップグレードによってコンソールの「現在のセッション」タブにエラーが表示される

アップグレードによって、Access Manager コンソールの「現在のセッション」タブに次のエラーが表示されます。

```
Failed to get valid Sessions from the Specified server
```

この問題は、`o=orgname` という形式のルートサフィックスを持つ Access Manager 6 バージョンからアップグレードする配備で発生します。

回避方法: Access Manager 7 2005Q4 のインストール後、Access Manager 7 パッチ 3 を適用してから `amupgrade` スクリプトを実行して、次のようにデータを移行します。

1. Access Manager 6 DIT をバックアップします。
2. `ampre70upgrade` スクリプトを実行します。
3. 「あとで設定」オプションを指定して Access Manager 7 2005Q4 をインストールします。
4. Access Manager Web アプリケーションの配備を取り消します。
5. Access Manager Web アプリケーションを配備します。
6. Access Manager 7 パッチ 3 を適用します。ただし、XML/LDIF の変更は適用しないでください。XML/LDIF の変更は、次の手順で `amupgrade` スクリプトを実行したあとで適用する必要があります。
7. `amupgrade` スクリプトを実行します。
8. Access Manager 7 パッチ 3 の変更のため、Access Manager Web アプリケーションを再配備します。
9. Access Manager コンソールにアクセスします。

CR# 6452320: クライアント SDK でポーリングを使用すると例外がスローされる

Access Manager クライアント SDK (`amclientsdk.jar`) を配備してポーリングを有効にすると、次のようなエラーが発生することがあります。

```
ERROR: Send Polling Error:
com.iplanet.am.util.ThreadPoolException:
amSessionPoller thread pool's task queue is full.
```

このようなエラーは、クライアントマシンに分散認証 UI サーバーまたは J2EE エージェントを配備したあと、あるいは、Access Manager クライアント SDK を配備する任意の状況で発生することがあります。

回避方法: 並行セッションの数が数百程度であれば、次のプロパティーと値を AMConfig.properties ファイルまたは AMAgents.properties ファイルに追加します。

```
com.sun.identity.session.polling.threadpool.size=10
com.sun.identity.session.polling.threadpool.threshold=10000
```

数千または数万のセッションがある場合は、amtune-identity スクリプト実行後の Access Manager AMConfig.properties ファイル内の通知用の値と同じ値を設定するようにしてください。たとえば、マシンに 4G バイトの RAM がある場合、Access Manager の amtune-identity スクリプトでは次の値が設定されます。

```
com.sun.identity.session.notification.threadpool.size=28
com.sun.identity.session.notification.threadpool.threshold=76288
```

4G バイトの RAM を備えたクライアントマシンに分散認証 UI サーバーまたは Access Manager クライアント SDK を配備するときは、AMAgent.properties ファイルまたは AMConfig.properties ファイルで、類似の値をクライアント側に設定します。

CR# 6442905 認証されたユーザーの SSOToken が不正なサイトに公開される可能性がある

認証された Access Manager ユーザーが不正なサイトの URL をクリックすると、その不正なサイトに SSOToken が公開されてしまう可能性があります。

回避方法: 参加しているすべてのポリシーエージェントについて、常に一意のエージェントユーザープロファイルを Access Manger に作成し、サイトが不正でないことを確認します。また、これらの一意のエージェントユーザーで使用されるパスワードが、共有シークレットパスワードまたは amldapuser パスワードと同じでないことを確認します。デフォルトでは、ポリシーエージェントは Access Manager アプリケーション認証モジュールに対して UrlAccessAgent ユーザーとして認証されます。

Access Manager 管理コンソールを使用してエージェントを作成する方法については、『Sun Java System Access Manager 7 2005Q4 管理ガイド』の「エージェント」を参照してください。

CR# 6441918: サイト監視の間隔およびタイムアウトのプロパティー

Access Manager のサイトフェイルオーバーに、次に示す新しいプロパティーが追加されています。

```
com.sun.identity.sitemonitor.interval
com.sun.identity.sitemonitor.timeout
```

詳細については、48 ページの「サイト監視の新しい設定プロパティー」を参照してください。

CR# 6440697: 分散認証は amadmin ユーザー以外のユーザーで実行するようにする

デフォルトの管理ユーザー (amadmin) 以外の、分散認証アプリケーションの認証に使用する分散認証管理者を作成するには、次の手順に従います。

1. 分散認証管理者の LDAP ユーザーを作成します。次に例を示します。

   ```
   uid=DistAuthAdmin,ou=people,o=am
   ```

2. 分散認証管理者を特殊ユーザーのリストに追加します。次に例を示します。

   ```
   com.sun.identity.authentication.special.users=cn=dsameuser,
   ou=DSAME Users,o=am|cn=amService-UrlAccessAgent,ou=DSAME Users,
   o=am|uid=DistAuthAdmin,ou=People,o=am
   ```

   このプロパティーをすべての Access Manager サーバーの AMConfig.properties ファイルに追加して、セッションのタイムアウトによって分散認証管理者の AppSSOToken が期限切れにならないようにします。

CR# 6440695: 分散認証 UI サーバーとロードバランサ

複数の分散認証 UI サーバーの前でロードバランサを使用する配備の場合は、WAR ファイルを配備したあと、次のプロパティーを AMConfig.properties ファイルに設定します。

```
com.iplanet.am.lbcookie.name=DistAuthLBCookieName
com.iplanet.am.lbcookie.value=DistAuthLBCookieValue
```

CR# 6440651: Cookie 応答には com.sun.identity.session.resetLBCookie プロパティーが必要

Access Manager のセッションフェイルオーバーで Cookie 応答を正しく動作させるには、値を true に設定した com.sun.identity.session.resetLBCookie プロパティーをポリシーエージェントと Access Manager サーバーの両方に追加します。次に例を示します。

```
com.sun.identity.session.resetLBCookie='true'
```

- ポリシーエージェントの場合は、このプロパティーを AMAgents.properties ファイルに追加します。
- Access Manager サーバーの場合は、このプロパティーを AMConfig.properties ファイルに追加します。

注: このプロパティーは、Access Manager のセッションフェイルオーバーを実装した場合にのみ必要です。

CR# 6440648: com.iplanet.am.lbcookie.name プロパティーのデフォルト値は amlbcookie と仮定される

デフォルトでは、ポリシーエージェントと Access Manager サーバーではロードバランサの cookie 名は amlbcookie と仮定されます。バックエンドサーバーで cookie 名を変更する場合は、ポリシーエージェントの AMAgent.properties ファイル内でも同じ名前を使用する必要があります。また、Access Manager クライアント SDK を使用している場合は、バックエンドサーバーで使用されているものと同じ cookie 名を使用する必要があります。

CR# 6440641: com.iplanet.am.lbcookie.value プロパティーは推奨されなくなった

Access Manager では、ロードバランサ cookie をカスタマイズするためのサーバーの com.iplanet.am.lbcookie.value プロパティーはサポートされなくなりました。代わりに、エージェントによって再生される cookie の値と名前に、セッション設定の一部として設定されるサーバー ID を使用するようになりました。

CR# 6429610: ID-FF SSO ユースケースで SSO トークンを作成できない

Liberty Identity Federation Framework (ID-FF) サンプル 1 を設定したあと、連携は成功するが、SSO が失敗します。

回避方法: dsameuser の uuid を AMConfig.properties ファイル内の com.sun.identity.authentication.special.users プロパティーに追加します。アプリケーション認証には、Access Manager サーバーの dsameuser ユーザーの SSO トークンが無期限である必要があります。

CR# 6389564: Access Manager のログイン時に、LDAP v3 データストア内のユーザーのロールメンバーシップに関するクエリーが繰り返し発生する

ユーザーが Access Manager にログインするとき、ユーザーの nsRoleDN 属性に関する LDAP 検索が繰り返し発生します。

回避方法: Access Manager 7 パッチ 3 のインストール後、次のコマンドを実行します (Access Manager が Solaris システムのデフォルトディレクトリにインストールされている場合の例)。

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/idRepoServiceAddAttrSchemaRequest_Cache.xml
```

CR# 6385185: 認証モジュールで "goto" URL を上書きして別の URL を指定できる必要がある

認証モジュールでは、"goto" URL を上書きして、ユーザーステータスを検証するために外部 Web サイトの別の URL にリダイレクトするよう要求できます。

認証の完了後に "goto" URL を上書きするには、次の例に示すプロパティーを `SSOToken` に設定します。このプロパティーを設定するには、`AMPostAuthProcessInterface` を実装して `PostProcess` クラスの `onLoginSuccess` メソッドを使用します。たとえば、"goto" URL を上書きする URL が *OverridingURL* の場合は、次のように指定します。

```
public class <..> implements AMPostAuthProcessInterface {
...
    public void onLoginSuccess(...) {
        try {
            ssoToken.setProperty("PostProcessSuccessURL", OverridingURL);
         } catch (Exception ...) {
         ...         }
...
}
```

CR# 6385184: SSO トークンがまだ無効な状態での、カスタム認証モジュール内からのリダイレクト

カスタム認証モジュールの新しい `RedirectCallback` を使用すると、ユーザーを検証するために、認証 UI を介して外部 Web サイトにリダイレクトできます。正常に認証された場合、ユーザーは元の Access Manager サーバーの URL に再びリダイレクトされます。サンプルファイルは次のとおりです。

- `LoginModuleSample.java`
- `LoginModuleSample.xml`
- `testExtWebSite.jsp`

この機能を実装するには、次の手順に従います。

1. サンプル `LoginModuleSample.java` を使用して、カスタム認証モジュールを作成します。
2. このモジュールを Access Manager サーバーに読み込みます。
3. サンプル `LoginModuleSample.xml` を使用して、XML ファイルに `RedirectCallback` を構築します。
4. モジュールをテストするために、外部 Web サイトとしてサンプル `testExtWebSite.jsp` ファイルを使用します。
5. 次の URL を使用してログインします。

   ```
   http://example.com/amserver/UI/Login?module=LoginModuleSample
   ```

検証のためにユーザー名とパスワードが外部 Web サイトにリダイレクトされます。ユーザー名とパスワードが有効な場合、ユーザーは正常に認証され、元の Access Manager サーバーの URL に再びリダイレクトされます。

たとえば、配備でカスタム認証モジュールを使用してプロビジョニング/クレジットカードサイトにアクセスする、次のようなシナリオが考えられます。

1. ユーザーがカスタム認証モジュールの認証プロセス/ログインページを呼び出します。
2. ユーザーは資格情報 (ユーザー名とパスワード) を入力し、カスタム認証モジュールに要求を送信します。
3. カスタム認証モジュールは、外部のプロビジョニング/クレジットカードサイトにユーザーをリダイレクトして、必要なユーザー情報とともに要求を送信します。
4. 外部のプロビジョニング/クレジットカードサイトは、ユーザーのステータスを確認し、要求を返します。返送される要求には、成功または失敗の情報が設定されます。
5. カスタム認証モジュールは、手順 4 で返されたステータスに基づいてユーザーを検証し、対応するステータスを認証サービスに返します。
6. ユーザーの認証は成功または失敗で完了します。

CR# 6324056: アーティファクトプロファイルを使用したときに連携が失敗する

回避方法: この問題を修正するには、「Core Mobile Access」パッチの最新バージョンを適用します。このバージョンは、プラットフォームに応じて次のようになります。

- SPARC ベースシステム上の Solaris OS: 119527
- x86 プラットフォーム上の Solaris OS: 119528
- Linux システム: 119529

パッチを適用したあと、Web コンテナを再起動します。

Access Manager 7 2005Q4 パッチ 2

Access Manager 7 2005Q4 パッチ 2 (リビジョン 02) により、いくつかの問題が修正されます。その一覧はパッチに含まれている README ファイルに記載されています。パッチ 2 には、次に示す新機能と既知の問題があります。

パッチ **2** での新機能

- 59 ページの「ユーザー管理、アイデンティティーリポジトリ、およびサービス管理キャッシュの新しいプロパティー」
- 61 ページの「連携サービスプロバイダの新しいプロパティー」

- 61 ページの「LDAP フィルタ条件のサポート」

パッチ 2 での既知の問題点と制限事項

- 62 ページの「CR# 6283582: Access Manager インスタンスの間でログイン失敗回数が共有されない」
- 62 ページの「CR# 6293673: セッションタイムアウトの通知を送信するときに元のセッション情報を保持する必要がある」
- 62 ページの「CR# 6244578: ブラウザの cookie のサポートが無効または使用不可の場合は、Access Manager でユーザーに警告するようにする」
- 63 ページの「CR# 6236892: ログイン後に CDCServlet で AuthNResponse を処理するときの画像/テキストのプレースホルダ」
- 63 ページの「CR# 6363157: どうしても必要な場合に、新しいプロパティーで持続検索を無効にする」
- 64 ページの「CR# 6385696: 既存および新規の IDP と SP が表示されない」

ユーザー管理、アイデンティティーリポジトリ、およびサービス管理キャッシュの新しいプロパティー

パッチ 2 には、ユーザー管理 (Access Manager SDK)、アイデンティティーリポジトリ (IdRepo)、およびサービス管理キャッシュ用に次のような新しいプロパティーも含まれています。これらのプロパティーを使用すると、配備要件に基づいてさまざまなキャッシュを個別に有効または無効にしたり、キャッシュエントリの有効時間 (TTL) を設定したりできます。

表 3 ユーザー管理、アイデンティティーリポジトリ、およびサービス管理キャッシュの新しいプロパティー

プロパティー	説明
キャッシュを有効および無効にするための新しいプロパティー	
`com.iplanet.am.sdk.caching.enabled`	アイデンティティーリポジトリ (IdRepo)、ユーザー管理、およびサービス管理キャッシュを有効 (true) または無効 (false) にするグローバルプロパティー。true であるか、このプロパティーが `AMConfig.properties` ファイル内に存在しない場合は、3 つのキャッシュすべてが有効になります。
注: 特定のキャッシュを有効または無効にする次の 3 つのプロパティーは、上記のグローバルプロパティーが false に設定されている場合のみ適用されます。	
`com.sun.identity.amsdk.cache.enabled`	ユーザー管理 (Access Manager SDK) キャッシュのみを有効 (true) または無効 (false) にします。

表 3 ユーザー管理、アイデンティティーリポジトリ、およびサービス管理キャッシュの新しいプロパティー *(続き)*

com.sun.identity.idm.cache.enabled	アイデンティティーリポジトリ (IdRepo) キャッシュのみを有効 (true) または無効 (false) にします。
com.sun.identity.sm.cache.enabled	サービス管理キャッシュのみを有効 (true) または無効 (false) にします。
TTL に関する新しいユーザー管理キャッシュのプロパティー	
com.iplanet.am. sdk.cache.entry.expire.enabled	ユーザー管理キャッシュの有効時間 (次の 2 つのプロパティーで定義) を有効 (true) または無効 (false) にします。
com.iplanet.am. sdk.cache.entry.user.expire.time	最終変更後にユーザー管理キャッシュのユーザーエントリを有効なままにしておく時間 (分) を指定します。つまり、(最終変更後またはディレクトリからの読み取り後) 指定した時間を過ぎたら、キャッシュされたエントリのデータは期限切れになります。その後は、これらのエントリのデータに対する新しい要求をディレクトリから読み取る必要があります。
com.iplanet.am. sdk.cache.entry.default.expire.time	最終変更後にユーザー管理キャッシュのユーザー以外のエントリを有効なままにしておく時間 (分) を指定します。つまり、(最終変更後またはディレクトリからの読み取り後) 指定した時間を過ぎたら、キャッシュされたエントリのデータは期限切れになります。その後は、これらのエントリのデータに対する新しい要求をディレクトリから読み取る必要があります。TTL に関する新しいアイデンティティーリポジトリキャッシュのプロパティー
com.sun.identity. idm.cache.entry.expire.enabled	IdRepo キャッシュの有効時間 (次のプロパティーで定義) を有効 (true) または無効 (false) にします。
com.sun.identity. idm.cache.entry.default.expire.time	最終変更後に IdRepo キャッシュのユーザー以外のエントリを有効なままにしておく時間 (分) を指定します。つまり、(最終変更後またはリポジトリからの読み取り後) 指定した時間を過ぎたら、キャッシュされたエントリのデータは期限切れになります。その後は、これらのエントリのデータに対する新しい要求をリポジトリから読み取る必要があります。

新しいキャッシュプロパティーの使用

Access Manager 7 2005Q4 のパッチでは、新しいキャッシュプロパティーは AMConfig.properties ファイルに自動的に追加されません。

新しいキャッシュプロパティーを使用するには、次の手順に従います。

1. テキストエディタを使用して、各プロパティーとその値を AMConfig.properties ファイルに追加します。このファイルはプラットフォームによって次のディレクトリにあります。
   - Solaris システム: /etc/opt/SUNWam/config
   - Linux システム: /etc/opt/sun/identity/config
2. Access Manager Web コンテナを再起動して、値を有効にします。

連携サービスプロバイダの新しいプロパティー

新しい com.sun.identity.federation.spadapter プロパティーは、com.sun.identity.federation.plugins.FederationSPAdapter の実装クラスを定義します。これは、サービスプロバイダ側で連携処理中にアプリケーション固有の処理を追加するために使用されます。

64 ページの「CR# 6385696: 既存および新規の IDP と SP が表示されない」も参照してください。

LDAP フィルタ条件のサポート

パッチ 2 には LDAP フィルタ条件のサポートが追加されています。ポリシー管理者は、ポリシーを定義するときに、LDAP フィルタを条件に指定できるようになりました。ユーザーの LDAP エントリが、条件で指定されている LDAP フィルタを満たす場合のみ、ユーザーにポリシーが適用されます。ユーザーの LDAP エントリは、ポリシー設定サービスで指定されているディレクトリから検索されます。

LDAP フィルタ条件を登録して使用するには、Access Manager 7 パッチ 2 のインストール後に次のコマンドを実行します (Access Manager が Solaris システムのデフォルトディレクトリにインストールされている場合の例)。

```
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-s /etc/opt/SUNWam/AddLDAPFilterCondition.xml
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/amPolicyConfig_mod_ldfc.xml
```

パッチ **5** に関する注**:** Access Manager 7 2005Q4 パッチ 5 を追加して updateschema.sh スクリプトを実行した場合は、amadmin を使用してこれらのファイルを読み込む必要はありません。詳細は、31 ページの「LDIF ファイルと XML ファイルを読み込む新しい updateschema.sh スクリプト」を参照してください。

CR# 6283582: Access Manager インスタンスの間でログイン失敗回数が共有されない

Access Manager 7 パッチ 2 のインストール後、次のコマンドを実行します (Access Manager が Solaris システムのデフォルトディレクトリにインストールされている場合の例)。

```
# cd DirectoryServer-base/shared/bin
# ./ldapmodify -h DirectoryServerHost -p DirectoryServerPort
-D "cn=Directory Manager" -w DirectoryMangerPassword
-a -f /etc/opt/SUNWam/accountLockout.ldif
# /opt/SUNWam/bin/amadmin -u amadmin
-w amadmin_password
-t /etc/opt/SUNWam/accountLockoutData.xml
```

DirectoryServer-base のデフォルト値は、Solaris システムでは `/var/opt/mps/serverroot`、Linux システムでは `/var/opt/sun/directory-server` です。

パッチ 5 に関する注: Access Manager 7 2005Q4 パッチ 5 を追加して `updateschema.sh` スクリプトを実行した場合は、`amadmin` を使用してこれらのファイルを読み込む必要はありません。詳細は、31 ページの「LDIF ファイルと XML ファイルを読み込む新しい `updateschema.sh` スクリプト」を参照してください。

CR# 6293673: セッションタイムアウトの通知を送信するときに元のセッション情報を保持する必要がある

`AMConfig.properties` ファイル内の新しい `com.sun.identity.session.property.doNotTrimList` プロパティーは、セッションプロパティー名のリストをコンマ区切り形式で保持できます。セッションがタイムアウトしても、このリストに定義されているプロパティーは削除されず、セッションが破棄されるまではこれらのプロパティーにアクセスできます。次に例を示します。

```
com.sun.identity.session.property.doNotTrimList=UserId,HostName
```

CR# 6244578: ブラウザの cookie のサポートが無効または使用不可の場合は、Access Manager でユーザーに警告するようにする

`AMConfig.properties` ファイル内の新しい `com.sun.identity.am.cookie.check` プロパティーは、ブラウザで cookie がサポートされ有効になっていることをサーバーでチェックするかどうかを指定します。値が `true` の場合、サーバーはブラウザで cookie がサポートされ有効になっているかどうかをチェックし、ブラウザで cookie がサポートされていないか有効になっていないときはエラーページをスローします。サーバーが認証機能で cookie なしモードをサポートするように想定されている場合は、この値を (デフォルトの) false に設定するようにしてください。

CR# 6236892: ログイン後に CDCServlet で AuthNResponse を処理するときの画像/テキストのプレースホルダ

次に示す新しいプロパティーが AMConfig.properties ファイルに追加されています。これらは CDCServlet で読み取られます。

- com.iplanet.services.cdc.WaitImage.display が true に設定されている場合は、CDSSO シナリオでユーザーが保護されたページを待機しているとき、ブラウザに画像が表示されます。デフォルトは false です。
- com.iplanet.services.cdc.WaitImage.name は、画像の名前を指定します。デフォルトは waitImage.gif です。この画像は login_images ディレクトリからコピーされます。
- com.iplanet.services.cdc.WaitImage.width は、画像の幅を指定します。デフォルトは 420 です。
- com.iplanet.services.cdc.WaitImage.height は、画像の高さを指定します。デフォルトは 120 です。

CR# 6363157: どうしても必要な場合に、新しいプロパティーで持続検索を無効にする

AMConfig.properties ファイル内の新しい com.sun.am.event.connection.disable.list プロパティーは、無効にできるイベント接続を指定します。指定できる値は次のとおりです。大文字と小文字は区別されません。

aci - LDAP フィルタ (aci=*) を使用した検索における aci 属性の変更。

sm - Access Manager 情報ツリー (またはサービス管理ノード) の変更。これには、sunService または sunServiceComponent マーカーオブジェクトクラスを持つオブジェクトが含まれます。たとえば、保護されたリソースのアクセス権限を定義するためのポリシーを作成する場合や、既存のポリシーのルール、対象、条件、または応答プロバイダを変更する場合があります。

um - ユーザーディレクトリ (またはユーザー管理ノード) の変更。たとえば、ユーザーの名前やアドレスを変更する場合があります。

たとえば、Access Manager 情報ツリー (またはサービス管理ノード) の変更に対する持続検索を無効にする場合は、次のようになります。

```
com.sun.am.event.connection.disable.list=sm
```

複数の値を指定する場合は、各値をコンマで区切って記述します。

注意 – 持続検索により、Directory Server にパフォーマンスオーバーヘッドが発生します。本稼働環境でこのパフォーマンスオーバーヘッドの一部を削減することが決定的に重要だと判断される場合は、`com.sun.am.event.connection.disable.list` プロパティーを使用して、1 つ以上の持続検索を無効にできます。

ただし、持続検索を無効にする前に、先に述べた制限事項を理解するようにしてください。どうしても必要な場合以外は、このプロパティーを変更しないことを強くお勧めします。複数の 2.1 J2EE エージェントを使用すると、それぞれのエージェントがこれらの持続検索を確立するため、このプロパティーはそのような場合に Directory Server に対するオーバーヘッドを回避することを主な目的として導入されました。2.2 J2EE エージェントは、これらの持続検索を確立しないため、このプロパティーを使用する必要はない可能性があります。

詳細は、102 ページの「持続検索の無効化の詳細について (6486927)」を参照してください。

CR# 6385696: 既存および新規の IDP と SP が表示されない

`AMConfig.properties` ファイル内の新しい `com.sun.identity.federation.spadapter` プロパティーは、アプリケーションが表明や応答情報を取得できる連携サービスプロバイダアダプタのデフォルトの実装を指定します。次に例を示します。

```
com.sun.identity.federation.spadapter=com.sun.identity.federation.plugins.FSDefaultSPAdapter
```

Access Manager 7 2005Q4 パッチ 1

Access Manager 7 2005Q4 パッチ 1 (リビジョン 01) により、いくつかの問題が修正されます。その一覧はパッチに含まれている README ファイルに記載されています。パッチ 1 には、次に示す新機能と既知の問題があります。

デバッグファイルの作成

Access Manager のデバッグファイルは、`AMConfig.properties` ファイル内の `com.iplanet.services.debug.level` プロパティーが error に設定されている場合でも、デバッグディレクトリ内にデフォルトで作成されます。Access Manager 7 パッチ 1 がリリースされる前は、最初のデバッグメッセージがデバッグファイルに記録されるときにはじめてファイルが作成されていました。

LDAPv3 プラグインでのロールとフィルタを適用したロールのサポート

Access Manager 7 パッチ 1 では、データを Sun Java System Directory Server に保存する場合の、LDAPv3 プラグインでのロールとフィルタを適用したロールのサポートを追加しています。詳細については、107 ページの「LDAPv3 プラグインのロールおよびフィルタを適用したロールのサポートについて (6365196)」を参照してください。

CR# 6320475: サーバー側の com.iplanet.am.session.client.polling.enable を true にしてはいけない

`AMConfig.properties` ファイル内の `com.iplanet.am.session.client.polling.enable` プロパティーは、サーバー側でデフォルトで false に設定されており、true にリセットしてはいけません。

CR# 6358751: 暗号化鍵にスペースが含まれていると Access Manager 7 パッチ 1 の適用が失敗する

パスワードの暗号化鍵にスペースが含まれていると、パッチの適用が失敗します。

回避方法: スペースを含んでいない新しい暗号化鍵を使用します。暗号化鍵を変更するための詳細な手順については、『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』の付録 B「パスワード暗号化キーの変更」を参照してください。

このリリースでの新機能

Access Manager の各パッチリリースの新機能については、9 ページの「Access Manager 7 2005Q4 パッチリリース」を参照してください。Access Manager 7 2005Q4 の初期リリースには、次の新機能が含まれています。

- 71 ページの「ログの機能拡張」

Access Manager モード

Access Manager 7 2005Q4 には、レルムモードおよび旧バージョンモードが含まれます。両方のモードで次の機能がサポートされます。

- 新しい Access Manager 7 2005Q4 の機能
- 次の制限事項を除く Access Manager 6 2005Q1 の機能
  - レルムが作成された場合、Sun Java System Directory Server には対応する組織は作成されません。
  - 新しい Access Manager 7 2005Q4 コンソールでは、サービスクラス (CoS) テンプレートの優先度を設定できません。88 ページの「新しい Access Manager コンソールは CoS テンプレート優先度を設定できない (6309262)」を参照してください。
- Sun Java System Directory Server およびその他のデータストアでのアイデンティティーリポジトリ

次の場合は旧バージョンモードが必要です。

- Sun Java System Portal Server
- Messaging Server、Calendar Server、Instant Messaging、Delegated Administrator などの、Sun Java System Communications Services サーバー
- Access Manager 6 2005Q1 および Access Manager 7 2005Q4 が同じ Directory Server にアクセスする場合の共存配備

新しい Access Manager コンソール

Access Manager コンソールは、このリリースのために再設計されました。ただし、Access Manager が Portal Server、Messaging Server、Calendar Server、Instant Messaging、または Delegated Administrator とともに配備される場合、Access Manager を旧バージョンモードでインストールし、Access Manager 6 2005Q1 コンソールを使用する必要があります。

詳細は、74 ページの「互換性の問題」を参照してください。

アイデンティティーリポジトリ

Access Manager のアイデンティティーリポジトリには、ユーザー、グループ、およびロールなどのアイデンティティーに関する情報が含まれます。アイデンティティーリポジトリは、Access Manager または Sun Java System Identity Manager などのプロビジョニング製品のどちらかを使用して作成または維持できます。

現在のリリースでは、アイデンティティーリポジトリは Sun Java System Directory Server または Microsoft Active Directory のどちらかに常駐できます。Access Manager は、アイデンティティーリポジトリに対する読み取り/書き込みアクセス権または読み取り専用アクセス権を持つことができます。

Access Manager 情報ツリー

Access Manager 情報ツリーには、システムアクセスに関連する情報が含まれます。それぞれの Access Manager インスタンスは、Sun Java System Directory Server 内で別々の情報ツリーを作成し、維持します。Access Manager 情報ツリーには、任意の名前 (サフィックス) を付けることができます。Access Manager 情報ツリーには、次の節で説明するレルム (必要に応じてサブレルム) が含まれます。

Access Manager レルム

レルムおよび任意のサブレルムは Access Manager 情報ツリーの一部であり、ユーザーまたはグループあるいはその両方を定義する設定情報、ユーザーの認証方法、ユーザーがアクセスできるリソース、ユーザーがリソースへのアクセス権を与えられた後にアプリケーションで利用可能な情報が含まれます。レルムまたはサブレルムには、国際化設定、パスワードリセット設定、セッション設定、コンソール設定、およびユーザー設定などの、その他の設定情報も含まれます。レルムまたはサブレルムは、空であってもかまいません。

レルムを作成するには、Access Manager コンソールまたは `amadmin` CLI ユーティリティーのどちらかを使用します。詳細は、コンソールのオンラインヘルプまたは『Sun Java System Access Manager 7 2005Q4 管理ガイド』の第 14 章「amadmin コマンド行ツール」を参照してください。

セッションフェイルオーバーの変更

Access Manager は、 Sun Java System Message Queue (Message Queue) を通信ブローカとして、また Sleepycat Software, Inc. による Berkeley DB をセッションストアデータベースとして使用し、Web コンテナに依存しないセッションフェイルオーバーの実装を提供します。Access Manager 7 2005Q4 の拡張機能には、セッションフェイルオーバー環境を設定するための `amsfoconfig` スクリプト、Message Queue ブローカや Berkeley DB クライアントを起動および停止するための `amsfo` スクリプトが含まれます。

詳細は、『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』の「Access Manager セッションフェイルオーバーの実装」を参照してください。

セッションプロパティーの変更通知

セッションプロパティーの変更通知機能により、特定のセッションプロパティーに変更が生じた場合に、Access Manager が特定のリスナーに通知を送信することができるようになります。この機能は、Access Manager 管理コンソールで「プロパティーの変更通知を有効」属性が有効になっている場合に有効になります。たとえば、シングルサインオン (SSO) 環境では、1 つの Access Manager セッションを複数のアプリケーションで共有できます。「通知プロパティー」リストで定義された特定のセッションプロパティーに変更が発生した場合、Access Manager は登録されたすべてのリスナーに通知を送信します。

詳細は、『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』の「セッションプロパティー変更通知の有効化」を参照してください。

セッション割り当て制限

セッション割り当て制限機能により、Access Manager 管理者 (`amadmin`) が「アクティブなユーザーセッション」属性を設定して、ユーザーに許可されている並行セッションの最大数を制限できます。管理者は、すべてのユーザーに対してグローバルレベルで、または、1 人以上の特定のユーザーにのみ適用される組織、レルム、ロール、ユーザーなどのエンティティーに対して、セッション割り当て制限を設定することができます。

デフォルトでは、セッション割り当て制限は無効 (OFF) ですが、管理者が Access Manager 管理コンソールで「割り当て制限を有効」属性を有効にした場合は、これを有効にすることができます。

管理者は、「セッション制限がいっぱいになった場合に生じる動作」属性を設定して、セッション割り当て制限がいっぱいになった場合の動作を設定することもできます。

- DENY_ACCESS: Access Manager は、新しいセッションへのログイン要求を拒否します。
- DESTROY_OLD_SESSION: Access Manager は、同じユーザーの次に有効期限切れとなる既存のセッションを破棄し、新しいログイン要求が成功するようにします。

「トップレベルの管理者に制限の確認を免除」属性は、「Top-level Admin Role」を持つ管理者にセッション割り当て制限を適用するかどうかを指定します。

詳細は、『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』の「セッション割り当て制限の設定」を参照してください。

分散認証

Access Manager 7 2005Q4 には分散認証 UI が含まれています。これは、配備内の 2 つのファイアウォール間のセキュリティー保護された分散認証を提供するリモート認証 UI コンポーネントです。分散認証 UI コンポーネントを使用しないと、Access Manager サービス URL がエンドユーザーに公開されてしまう可能性があります。これは、プロキシサーバーを使用して防ぐこともできますが、プロキシサーバーが必ずしもすべての配備に適しているとは限りません。

分散認証 UI コンポーネントは、Access Manager 配備のセキュリティー保護されていない (DMZ) レイヤー内の 1 つまたは複数のサーバーにインストールします。分散認証 UI サーバーでは、Access Manager を実行しません。Web ブラウザを通じて、エンドユーザーとの認証インタフェースを提供するためにのみ存在します。

エンドユーザーが分散認証 UI に HTTP 要求を送信すると、ログインページが表示されます。次に、分散認証コンポーネントは、2 つ目のファイアウォールを通じて、Access Manager サーバーにユーザーの要求を送信します。これによって、エンドユーザーと Access Manager サーバー間のファイアウォールに穴を開ける必要がなくなります。

詳細については、『Technical Note: Using Access Manager Distributed Authentication』を参照してください。

複数の認証モジュールインスタンスのサポート

すべての認証モジュール (アウトオブボックス) は拡張され、コンソール UI サポートとともにサブスキーマをサポートします。それぞれのモジュールタイプ (読み込まれたモジュールクラス) ごとに、複数の認証モジュールインスタンスを作成できます。たとえば、LDAP モジュールタイプ用に `ldap1` および `ldap2` の名前のついたインスタンスでは、それぞれのインスタンスが異なる LDAP ディレクトリサーバーを示すことができます。タイプとして同じ名前のモジュールインスタンスが、下位互換性のためにサポートされています。次のように呼び出します。

server_deploy_uri`/UI/Login?module=`*module-instance-name*

認証の「指定設定」または「連鎖」ネームスペース

組織/レルムに、認証モジュールインスタンスの連鎖である個別の名前空間が作成されます。同じ連鎖を再利用して、組織/レルム、ロール、ユーザーに割り当てることができます。認証サービスインスタンスは、認証連鎖と同じです。次のように呼び出します。

server_deploy_uri/UI/Login?service=*authentication-chain-name*

ポリシーモジュールの拡張機能

個別設定属性

ルール、対象、条件に加え、ポリシーに個別設定属性 (IDResponseProvider) を付加できるようになりました。ポリシー評価からクライアントに送信されるポリシー決定には、適用可能なポリシーにポリシーベースの応答個別設定属性が含まれるようになりました。2 種類の個別設定属性がサポートされています。

- 静的属性: ポリシー内の属性名と値を定義します。
- 動的属性: ポリシー内の属性名を列挙します。値はポリシー評価時にアイデンティティーリポジトリデータストアから取得されます。

ポリシー適用ポイント (エージェント) では通常、これらの属性値を HTTP ヘッダー、Cookie、または要求属性として、保護されたアプリケーションに転送します。

Access Manager 7 2005Q4 は、ユーザーによる応答プロバイダインタフェースのカスタム実装をサポートしていません。

セッションプロパティー条件

セッションポリシー条件の実装 (SessionPropertyCondition) では、ユーザーの Access Manager セッションで設定されたプロパティーの値に基づいて、ポリシーが要求に適用可能かどうかを判断します。ポリシーの評価時に、ユーザーの Access Manager セッションですべてのプロパティーが条件に定義されている値を持つ場合にのみ、条件は「true」を返します。条件に複数の値が定義されているプロパティーの場合、ユーザーセッションで条件内に少なくとも 1 つの値がプロパティーに示されていれば十分です。

ポリシー対象

ポリシー対象の実装 (Access Manager アイデンティティー対象) により、設定されたアイデンティティーリポジトリからのエントリをポリシー対象値として使用でるようになります。

ポリシーのエクスポート

amadmin コマンドを使用して、ポリシーを XML 形式でエクスポートできます。amAdmin.dtd ファイル内の新しい GetPolicies および RealmGetPolicies 要素が、この機能をサポートしています。

ポリシーの状態

ポリシーには状態属性が追加され、アクティブまたは非アクティブに設定できます。アクティブでないポリシーは、ポリシーの評価時に無視されます。

サイト設定

Access Manager 7 2005Q4 では「サイトの概念」が導入され、Access Manager の配備を集中設定管理できるようになりました。Access Manager がサイトとして設定されると、クライアント要求は常にロードバランサを経由するため、配備が単純化されると同時にクライアントとバックエンド Access Manager サーバー間のファイアウォールなどの問題が解決されます。

詳細は、『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』の「サイトとしての Access Manager 配備の設定」を参照してください。

一括連携

Access Manger 7 2005Q4 では、ユーザーアカウントとビジネスパートナーに委託したアプリケーションとの一括連携が行えます。以前は、アカウントの連携ではサービスプロバイダ (SP) とアイデンティティープロバイダ (IDP) との間でそれぞれのユーザーが SP および IDP のサイトにアクセスする必要があり、アカウントが存在しない場合には作成し、Web リンクを経由して 2 つのアカウントを連携する必要がありました。この処理には、多くの時間を必要としました。これは、既存のアカウントが存在する配備、それ自体がアイデンティティープロバイダとして動作するサイト、または片方のパートナーを認証プロバイダとして使用する場合には、必ずしも適切ではありませんでした。

詳細は、『Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide』を参照してください。

ログの機能拡張

Access Manager 7 2005Q4 には、新しいいくつかのログ機能の拡張が含まれています。

- 新しいフィールド (または列): `MessageID` フィールドには、ログイベントのメッセージ ID が含まれます。`ContextID` フィールドにはコンテキスト ID が含まれます。この ID はセッション ID に類似しており、特定のユーザーのログインセッションのすべてのイベントに適用されます。ユーザーの固有のログインセッションでは、ログイベントに対して `ContextID` はすべてのログファイルで同じになります。
- ログ API。API には、データベース (DB) へのログが設定されている場合、DB からのものを含むログレコードの読み取りのための追加が含まれます。`/opt/SUNWam/samples/logging` ディレクトリにある `LogReaderSample.java` を参照してください。フラットファイルまたは DB テーブルリポジトリから取得されたログレコードが表示されます。

注意 – データベーステーブルは、フラットファイルのログよりもサイズが大きくなる傾向があります。そのため、大量のデータにより Access Manager サーバーリソースがすべて消費される可能性があるので、特定の要求ではデータベーステーブル内のすべてのレコードを取得しないでください。

ハードウェアおよびソフトウェアの要件

次の表に、このリリースに必要なハードウェアとソフトウェアを示します。

表 4 ハードウェアおよびソフトウェアの要件

コンポーネント	要件
オペレーティングシステム (OS)	SPARC™ ベースシステム上の Solaris OS、バージョン 8、9、および 10。Solaris 10 の全体ルートローカルゾーンのサポートを含む
	x86 プラットフォーム上の Solaris OS、バージョン 9 および 10。Solaris 10 の全体ルートローカルゾーンのサポートを含む
	AMD64 プラットフォーム上の Solaris OS、バージョン 10。全体ルートローカルゾーンのサポートを含む
	Red Hat™ Linux、 WS/AS/ES 2.1 Update 6 以降
	Red Hat Linux、 WS/AS/ES 3.0
	Red Hat Linux、 WS/AS/ES 3.0 Updates 1、 2、 3、および 4
	HP-UX OS。Sun Java Enterprise System 2005Q4 HP-UX 版のドキュメントコレクションを参照: http://docs.sun.com/coll/1258.2
	Windows OS。Sun Java Enterprise System 2005Q4 Microsoft Windows 版のドキュメントコレクションを参照: http://docs.sun.com/coll/1259.2
Java 2 Standard Edition (J2SE)	J2SE platform 1.5.0_04、 1.5_01、 1.5、および 1.4.2
Directory Server	Access Manager 情報ツリー: Sun Java System Directory Server 5 2005Q4
	Access Manager アイデンティティーリポジトリ: Sun Java System Directory Server 5 2005Q4 または Microsoft Active Directory

表 4 ハードウェアおよびソフトウェアの要件 (続き)

コンポーネント	要件
Web コンテナ	Sun Java System Web Server 6.1 2005Q4 SP5
	Sun Java System Application Server Enterprise Edition 8.1 2005Q2
	BEA WebLogic Server 8.1 SP4
	IBM WebSphere Application Server 5.1 および 5.1.1 (および関連する累積バグ修正)
RAM	基本テスト: 512M バイト
	実際の配備: スレッド、Access Manager SDK、HTTP サーバー、およびその他の内部用に 1G バイト
ディスク容量	Access Manager および関連するアプリケーション用に 512M バイト

コンポーネントのその他のバージョンのサポートについての質問は、Sun Microsystems の技術担当者にご連絡ください。

サポートされているブラウザ

次の表に、Sun Java Enterprise System 2005Q4 リリースでサポートされているブラウザを示します。

表 5 サポートされているブラウザ

ブラウザ	プラットフォーム
Microsoft Internet Explorer™ 5.5 SP2	Windows™ 2000
Microsoft Internet Explorer 6.0	Windows 2000
	Windows XP
Mozilla 1.7.1	Solaris OS、バージョン 9 および 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0

表 5 サポートされているブラウザ (続き)

ブラウザ	プラットフォーム
Netscape™ 7.0	Solaris OS、バージョン 9 および 10
	Java Desktop System
	Windows 2000
	Red Hat Linux 8.0

システム仮想化のサポート

システム仮想化とは、複数のオペレーティングシステム (OS) インスタンスが共有ハードウェア上で独立して動作することを可能にするテクノロジのことです。機能的には、仮想化環境内でホストされている OS に配備されたソフトウェアは通常、配下のプラットフォームが仮想化されていることを認識しません。Sun では、適切なサイズと設定の仮想化環境上で、仮想化されていないシステム上の場合と同様に Sun Java System 製品が機能することを確認できるよう、選択したシステム仮想化と OS の組み合わせについて Sun Java System 製品のテストを実行しています。仮想化環境での Sun Java System 製品の Sun のサポートについては、http://docs.sun.com/doc/820–4651 を参照してください。

互換性の問題

Access Manager 旧バージョンモード

Access Manager を次の製品とともにインストールする場合は、Access Manager 旧バージョン (6.x) モードを選択する必要があります。

- Sun Java System Portal Server
- Messaging Server、Calendar Server、Instant Messaging、Delegated Administrator などの、Sun Java System Communications Services サーバー

Java ES インストーラの実行方法によっては、Access Manager 旧バージョン (6.x) モードを選択します。

- 75 ページの「「後で設定」インストールオプション」

Access Manager 7 2005Q4 のインストールに関する決定については、76 ページの「Access Manager モードの確認」を参照してください。

状態ファイルを使用した Java ES サイレントインストール

Java ES インストーラのサイレントインストールは、非対話モードで、同じような設定の複数のホストサーバーに Java ES コンポーネントをインストールできます。最初にインストーラを実行して状態ファイルを生成し (実際にはコンポーネントをインストールせずに)、Access Manager およびほかのコンポーネントをインストールする予定の各ホストサーバー用に、状態ファイルのコピーを編集します。

Access Manager の旧バージョン (6.x) モードを選択するには、インストーラをサイレントモードで実行する前に、状態ファイルで (ほかのパラメータと一緒に) 次のパラメータを設定します。

```
...
AM_REALM = disabled
...
```

状態ファイルを使用した Java ES インストーラのサイレントモードでの実行方法の詳細については、『Sun Java Enterprise System 2005Q4 インストールガイド(UNIX 版)』の第 5 章「サイレントモードでのインストール」を参照してください。

グラフィカルモードでの「今すぐ設定」インストールオプション

Java ES インストーラをグラフィカルモードで実行し、「今すぐ設定」オプションを選択した場合、「Access Manager: 管理 (1 / 6)」パネルでデフォルトの値である「旧バージョンモード (バージョン 6.x スタイル)」を選択します。

テキストベースモードでの「今すぐ設定」インストールオプション

Java ES インストーラをテキストベースモードで実行しており、「今すぐ設定」オプションを選択した場合、`Install type (Realm/Legacy) [Legacy]` でデフォルトの値である `Legacy` を選択します。

「後で設定」インストールオプション

Java ES インストーラを「後で設定」オプションで実行した場合、インストール後に `amconfig` スクリプトを実行して Access Manager を設定する必要があります。旧バージョン (6.x) モードを選択するには、設定スクリプト入力ファイル (`amsamplesilent`) で次のパラメータを設定します。

```
...
AM_REALM=disabled
...
```

Windows システムでは、この設定ファイルは *AccessManager-base*\setup\AMConfigurator.properties です。

amconfig スクリプトを実行した Access Manager の設定については、『Sun Java System Access Manager 7 2005Q4 管理ガイド』を参照してください。

Access Manager モードの確認

Access Manager 7 2005Q4 のインストールが、レルムモードまたは旧バージョンモードのどちらの設定で実行されたかを確認するには、次のように指定します。

```
http(s)://host:port/amserver/SMSServlet?method=isRealmEnabled
```

結果は次のとおりです。

- true: レルムモード
- false: 旧バージョンモード

Access Manager ポリシーエージェント

次の表に、ポリシーエージェントと Access Manager 7 2005Q4 モードとの互換性を示します。

表 6 ポリシーエージェントと Access Manager 7 2005Q4 モードとの互換性

エージェントとバージョン	互換モード
Web および J2EE エージェント、バージョン 2.2	旧バージョンモードおよびレルムモード
Web エージェント、バージョン 2.1	旧バージョンモードおよびレルムモード
J2EE エージェント、バージョン 2.1	旧バージョンモードのみ

インストールに関する注意事項

Access Manager のインストールに関する注意事項には、次の情報が含まれます。

- 74 ページの「Access Manager 旧バージョンモード」
- 79 ページの「インストールに関する問題」

既知の問題点と制限事項

この節では、リリース時での、次の既知の問題点、および利用可能な場合は回避方法について説明します。

互換性の問題

Java ES 2004Q2 サーバーと Java ES 2005Q4 上の IM との間に互換性がない (6309082)

次の配備シナリオでは問題が発生します。

- サーバー-1: Java ES 2004Q2: Directory Server
- サーバー-2: Java ES 2004Q2: Application Server、 Access Manager、 および Portal Server
- サーバー-3: Java ES 2004Q2: Calendar Server と Messaging Server
- サーバー-4: Java ES 2005Q4: Application Server、 Instant Messaging、 および Access Manager SDK

imconfig ユーティリティーを実行してサーバー-4 上の Instant Messaging を設定しても、設定は成功しません。サーバー -4 上の Instant Messaging (IM) で使用される Access Manager 7 2005Q4 SDK は、Java ES 2004Q2 リリースと互換性がありません。

回避方法: Access Manager サーバーおよび Access Manager SDK は、同じリリースであることが理想的です。詳細は、『Sun Java Enterprise System 2005Q4 アップグレードガイド』を参照してください。

旧バージョンモードでコア認証モジュールに非互換性が存在する (6305840)

Access Manager 7 2005Q4 旧バージョンモードでは、Access Manager 6 2005Q1 からのコア認証モジュールに次の非互換性があります。

- 組織認証モジュールが旧バージョンモードで削除されています。
- 「管理者認証設定」および「組織認証設定」の表示方法が変更されました。Access Manager 7 2005Q4 コンソールでは、ドロップダウンリストの ldapService がデフォルトで選択されています。Access Manager 6 2005Q1 コンソールでは、「編集」ボタンが表示され、LDAP モジュールはデフォルトで選択されませんでした。

回避方法: なし。

「組織にプロファイルがない」ために、エージェントがログインできない (6295074)

Access Manager コンソールで、エージェントをレルムモードで作成します。ログアウトしてからエージェント名を使用してもう一度ログインすると、エージェントはレルムにアクセスする権限がないため、Access Manager はエラーを返します。

回避方法: エージェントに対して読み取り/書き込みアクセスができるように、アクセス権を変更します。

Delegated Administrator commadmin ユーティリティーがユーザーを作成しない (6294603)

Delegated Administrator commadmin ユーティリティーを -S mail,cal オプションで使用すると、デフォルトドメインにユーザーが作成されません。

回避方法: この問題は、Access Manager をバージョン 7 2005Q4 にアップブレードして Delegated Administrator をアップグレードしなかった場合に発生します。Delegated Administrator のアップグレードについては、『Sun Java Enterprise System 2005Q4 アップグレードガイド』を参照してください。

Delegated Administrator をアップグレードする予定がない場合は、次の手順を実行します。

1. UserCalendarService.xml ファイルで、mail、icssubcribed、および icsfirstday 属性を必須ではなく省略可能としてマークします。このファイルはデフォルトで、Solaris システム上の /opt/SUNWcomm/lib/services/ ディレクトリにあります。
2. Access Manager で次のように amadmin コマンドを実行して、既存の XML ファイルを削除します。

```
# ./amadmin -u amadmin -w password -r UserCalendarService
```

3. Access Manager で、更新した XML ファイルを次のように追加します。

```
# ./amadmin -u amadmin -w password
-s /opt/SUNWcomm/lib/services/UserCalendarService.xml
```

4. Access Manager Web コンテナを再起動します。

Delegated Administrator commadmin ユーティリティーが組織を作成しない (6292104)

Delegated Administrator commadmin ユーティリティーを -S mail,cal オプションで使用すると、組織が作成されません。

回避方法: 前の問題の回避方法を参照してください。

インストールに関する問題

パッチ 1 の適用後、/tmp/amsilent ファイルがすべてのユーザーの読み取りアクセスを許可する (6370691)

パッチ 1 の適用後、/tmp/amsilent ファイルはすべてのユーザーに読み取りアクセスを許可します。

回避方法: パッチの適用後、Access Manager 管理者のみ読み取りアクセスを許可するように、ファイルのアクセス権をリセットします。

SDK インストールでコンテナ設定を行う際に、通知 URL が正しくない (6327845)

SDK のインストールをコンテナ設定 (DEPLOY_LEVEL=4) とともに実行すると、通知 URL が正しくありません。

回避方法:

1. `AMConfig.properties` ファイルで、次のプロパティーを設定します。

   ```
   com.iplanet.am.notification.url=
   protocol://fqdn:port/amserver/servlet/com.iplanet.services.comm.client.
   PLLNotificationServlet
   ```

2. Access Manager を再起動すると、新しい値が有効になります。

Access Manager `classpath` が、有効期限の切れた JCE 1.2.1 パッケージを参照する (6297949)

Access Manager `classpath` が、2005 年 7 月 27 日に期限が切れた Java Cryptography Extension (JCE) 1.2.1 パッケージ (署名証明書) を参照しています。

回避方法: なし。パッケージ参照が `classpath` にあっても、Access Manager はそのパッケージを使用しません。

Access Manager を既存の DIT にインストールすると、Directory Server のインデックスの再作成が必要になる (6268096)

検索のパフォーマンスを改善するため、Directory Server ではいくつかの新しいインデックスを用意しています。

回避方法: Access Manager を既存の Directory Information Tree (DIT) とともにインストールした後、Directory Server のインデックスを `db2index.pl` スクリプトを実行して再作成します。次に例を示します。

```
# ./db2index.pl -D "cn=Directory Manager" -w password -n userRoot
```

`db2index.pl` スクリプトは *DS-install-directory/slapd-hostname/* ディレクトリから利用可能です。

root ではないユーザーのログディレクトリおよびデバッグディレクトリのアクセス権が正しくない (6257161)

サイレントインストール設定ファイルで root ではないユーザーが指定された場合、デバッグ、ログ、および起動ディレクトリのアクセス権が適切に設定されません。

回避方法: root ではないユーザーのアクセスが許可されるように、これらのディレクトリのアクセス権を変更します。

Access Manager と Directory Server を別のマシンにインストールすると、認証サービスが初期化されない (6229897)

インストール時に `classpath` およびその他の Access Manager Web コンテナ環境変数は更新されますが、インストールプロセスでは Web コンテナが再起動されません。インストール後、Web コンテナが再起動する前に、Access Manager にログインしようとすると、次のエラーが返されます。

```
Authentication Service is not initialized.
Contact your system administrator.
```

回避方法: Access Manager にログインする前に、Web コンテナを再起動します。ログインする前に、Directory Server も実行している必要があります。

インストーラが既存のディレクトリインストールにプラットフォームエントリを追加しない (6202902)

Java ES インストーラは、既存のディレクトリサーバーのインストール (DIRECTORY_MODE=2) にプラットフォームエントリを追加しません。

回避方法: レルム/DNS エイリアスおよびプラットフォームサーバーリストエントリを手動で追加します。手順については、『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』の「プラットフォームサーバーリストおよびレルムまたは DNS エイリアスへのインスタンスの追加」を参照してください。

アップグレードに関する問題

- 84 ページの「データ移行後に ContainerDefaultTemplateRole 属性を追加する (4677779)」

Access Manager の ampre70upgrade スクリプトがローカライズ版のパッケージを削除しない (6378444)

Access Manager を Access Manager 7 2005Q4 にアップグレードする場合、ampre70upgrade スクリプトによって、システムにインストールされているローカライズ版のパッケージが削除されません。

回避方法: Access Manager 7 2005Q4 にアップグレードする前に、pkgrm コマンドを使用して、システムにインストールされている Access Manager のローカライズ版パッケージをすべて手動で削除します。

AMConfig.properties ファイルに Web コンテナ用の古いバージョンが含まれている (6316833)

Access Manager および Application Server を Java ES 2005Q4 バージョンにアップグレードした後、Access Manager の AMConfig.properties ファイルには Application Server の古いバージョンが含まれます。

回避方法: Delegated Administrator 設定プログラム (config-commda) を実行する前に、AMConfig.properties ファイルの次のプロパティーを変更します。

```
com.sun.identity.webcontainer=IAS8.1
```

ノードエージェント server.policy ファイルが、Access Manager アップグレードの一部として更新されない (6313416)

Access Manager をアップグレードしたあと、ノードエージェントの server.policy ファイルが更新されません。

回避方法: ノードエージェント用の server.policy ファイルを次のファイルと置き換えます。

```
/var/opt/SUNWappserver/domains/domain1/config/server.policy
```

アップグレードの後、条件リストの中に「セッションプロパティー条件」がない (6309785)

Access Manager をバージョン 2005Q1 からバージョン 2005Q4 へアップグレードした後、条件をポリシーに追加しようとしても、「セッションプロパティー条件」がポリシー条件リストの中に選択肢として表示されません。

回避方法: 対応するレルムで、ポリシー設定サービスのテンプレート内の「セッションプロパティー条件」タイプを選択します。

アップグレードの後、ポリシー対象リストに「アイデンティティー対象」タイプがない (6304617)

Access Manager をバージョン 2005Q1 からバージョン 2005Q4 へアップグレードした後、新しく追加されたポリシー対象タイプである「アイデンティティー対象」が、ポリシー対象リスト内に選択肢として表示されません。

回避方法: ポリシー設定サービスのテンプレートで、「アイデンティティー対象」タイプをデフォルトの対象タイプとして選択します。

classpath が移行されないため、Access Manager のアップグレードが失敗する (6284595)

Access Manager を Java ES 2004Q2 から Java ES 2005Q4 へのアップグレード中、Java ES 2004Q2 から Java ES 2005Q1 へのアップグレードは失敗します。Access Manager が配備されていた Application Server も Java ES 2004Q2 から Java ES 2005Q4 へアップグレードされるため、アップグレード後の `domain.xml` ファイル内の `classpath` に、Access Manager JAR ファイルのパスがないことが原因です。

回避方法: 次の手順を実行します。

1. `comm_dssetup.pl` スクリプトには問題があるため、`amupgrade` スクリプトを実行する前に、Directory Server のインデックスを再作成します。
2. Access Manager のエントリをノードエージェントの `server.policy` ファイルに追加します。デフォルトのサーバーポリシー (`/var/opt/SUNWappserver/domains/domain1/config/server.policy`) からの `server.policy` のコピーで十分です。
3. ノードエージェントの `domain.xml` ファイル内の `classpath` を、次の手順で更新します。`server.xml` ファイルにある `java-config` 要素の `server-classpath` 属性から、`classpath-suffix` および該当する `classpath` を、`domain.xml` の `java-config` 要素のそれぞれの属性にコピーします。`java-config` 要素は、`domain.xml` 内の `config` 要素の下にあります。

アップグレードの後、amadmin コマンドで間違ったバージョンの表示が返される (6283758)

Access Manager をバージョン 6 2005Q1 からバージョン 7 2005Q4 へアップグレードした後、`amadmin --version` コマンドが間違ったバージョン Sun Java System Access Manager version 2005Q1 を返します。

回避方法: Access Manager をアップグレードした後、`amconfig` スクリプトを実行して Access Manager を設定します。`amconfig` を実行する場合、設定ファイル (`amsamplesilent`) のフルパスを指定します。たとえば、Solaris システムの場合は次のように指定します。

```
# ./amconfig -s ./config-file
```

または

```
# ./amconfig -s /opt/SUNWam/bin/config-file
```

データ移行後に ContainerDefaultTemplateRole 属性を追加する (4677779)

Access Manager で作成されていないユーザーのロールは組織の下に表示されません。デバッグモードで、次のメッセージが表示されます。

```
ERROR: DesktopServlet.handleException()
com.iplanet.portalserver.desktop.DesktopException:
DesktopServlet.doGetPost(): no privilige to execute desktop
```

このエラーは Java ES インストーラ移行スクリプトを実行すると、明らかになります。組織を既存のディレクトリ情報ツリー (DIT) またはほかのソースから移行した場合に、ContainerDefaultTemplateRole 属性は自動的に組織に追加されません。

回避方法: Directory Server コンソールを使用して、別の Access Manager の組織から ContainerDefaultTemplateRole 属性をコピーし、影響を受ける組織に追加します。

設定に関する問題

Application Server 8.1 server.policy ファイルは、デフォルトでない URI を使用する場合は編集する必要がある (6309759)

Access Manager 7 2005Q4 を Application Server 8.1 に配備し、サービス、コンソール、およびパスワード Web アプリケーションのそれぞれのデフォルトである amserver、amconsole、および ampassword ではない URI を使用している場合、Web ブラウザ経由で Access Manager にアクセスする前にアプリケーションサーバードメインの server.policy ファイルを編集する必要があります。

回避方法: `server.policy` ファイルを次のように編集します。

1. Access Manager が配備されている Application Server インスタンスを停止します。
2. `/config` ディレクトリに移動します。次に例を示します。

```
cd /var/opt/SUNWappserver/domains/domain1/config
```

3. `server.policy` ファイルのバックアップコピーを作成します。次に例を示します。

```
cp server.policy server.policy.orig
```

4. `server.policy` ファイルで、次のポリシーを探します。

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amserver/-" { ...
};
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amconsole/-" { ...
};
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/ampassword/-" { ...
};
```

5. 次の行で、`amserver` をサービス Web アプリケーションで使用するデフォルトでない URI に置き換えます。

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amserver/-" {
```

6. 旧バージョンモードのインストールの場合、次の行で `amconsole` をコンソール Web アプリケーションで使用するデフォルトでない URI に置き換えます。

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/amconsole/-" {
```

7. 次の行で、`ampassword` をパスワード Web アプリケーションで使用するデフォルトでない URI に置き換えます。

```
grant codeBase "file:\${com.sun.aas.instanceRoot}/
applications/j2ee-modules/ampassword/-" {
```

8. Access Manager が配備されている Application Server インスタンスを起動します。

プラットフォームサーバーリストおよび FQDN エイリアス属性が更新されない (6309259、6308649)

複数のサーバー配備では、Access Manager を 2 番目 (およびそれ以降) のサーバーにインストールした場合、プラットフォームサーバーリストおよび FQDN エイリアス属性が更新されません。

回避方法: レルム/DNS エイリアスおよびプラットフォームサーバーリストエントリを手動で追加します。手順については、『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』の「プラットフォームサーバーリストおよびレルムまたは DNS エイリアスへのインスタンスの追加」を参照してください。

サービス内の必須属性のデータ妥当性検査 (6308653)

Access Manager 7 2005Q4 では、サービス XML ファイルの必須属性には、デフォルト値が割り当てられていなければなりません。

回避方法: 値のない必須属性のあるサービスが存在する場合、属性に値を追加してからサービスを再読み込みします。

セキュリティー保護された WebLogic 8.1 インスタンス上に配備する際の問題に対する回避方法 (6295863)

Access Manager 7 2005Q4 をセキュリティー保護された (SSL が有効な) BEA WebLogic 8.1 SP4 インスタンスに配備する場合、それぞれの Access Manager Web アプリケーションの配備中に例外が発生します。

回避方法: 次の手順を実行します。

1. BEA から入手可能な WebLogic 8.1 SP4 パッチ JAR `CR210310_81sp4.jar` を適用します。
2. `/opt/SUNWam/bin/amwl81config` スクリプト (Solaris システム) または `/opt/sun/identity/bin/amwl81config` スクリプト (Linux システム) で、`doDeploy` 関数および `undeploy_it` 関数を更新してパッチ JAR のパスを `wl8_classpath` の先頭に追加します。これは Access Manager Web アプリケーションの配備および配備取消しに使用される `classpath` を含む変数です。

   `wl8_classpath` を含む次の行を検索します。

   ```
   wl8_classpath= ...
   ```
3. 手順 2 で検索した行のすぐ後に、次の行を追加します。

   ```
   wl8_classpath=path-to-CR210310_81sp4.jar:$wl8_classpath
   ```

amconfig スクリプトが、レルム/DNS エイリアスおよびプラットフォームサーバーリストのエントリを更新しない (6284161)

複数サーバーの配備では、`amconfig` は追加の Access Manager インスタンスに対してレルム/DNS エイリアスおよびプラットフォームサーバーリストのエントリを更新しません。

回避方法: レルム/DNS エイリアスおよびプラットフォームサーバーリストエントリを手動で追加します。手順については、『Sun Java System Access Manager 7 2005Q4 配

備計画ガイド』の「プラットフォームサーバーリストおよびレルムまたはDNSエイリアスへのインスタンスの追加」を参照してください。

デフォルトの Access Manager モードが設定状態ファイルテンプレートでレルムに設定されている (6280844)

デフォルトでは、Access Manager モード (AM_REALM 変数) は設定状態ファイルテンプレートで enable に設定されています。

回避方法: Access Manager を旧バージョンモードでインストールまたは設定するには、状態ファイルの変数を次のようにセットし直します。

```
AM_REALM = disabled
```

RSA キーを使用した場合に、IBM WebSphere でURL署名が失敗する (6271087)

IBM WebSphere で RSA キーを使用すると、URL 文字列の署名が次の例外を発行して失敗します。

```
ERROR: FSSignatureUtil.signAndReturnQueryString: FSSignatureException
occured while signing query string: no such provider: SunRsaSign
```

回避方法: SunRsaSign プロバイダは WebSphere バンドル版の JDK に含まれていません。この問題を修正するには、*websphere_jdk_root*/jre/lib/security/java.security ファイルを編集し、次の行を追加して、プロバイダの 1 つとして SunRsaSign を有効にします。

```
security.provider.6=com.sun.rsajca.Provider
```

Access Manager コンソールに関する問題

- 88 ページの「SAML で、信頼パートナーをコンソールで複製すると、エラーが発生する (6326634)」
- 88 ページの「amConsole.access および amPasswordReset.access でリモートログが機能していない (6311786)」
- 88 ページの「コンソールで amadmin プロパティーをさらに追加すると、amadmin ユーザーパスワードが変更される (6309830)」
- 88 ページの「新しい Access Manager コンソールは CoS テンプレート優先度を設定できない (6309262)」
- 89 ページの「ポリシー管理ユーザーとしてグループをユーザーに追加すると例外エラーが発生する (6299543)」
- 89 ページの「旧バージョンモードで、ロールからすべてのユーザーを削除できない (6293758)」

- 89 ページの「ディスカバリサービスリソースオファリングを追加、削除、変更できない (6273148)」
- 89 ページの「対象検索で、間違った LDAP バインドパスワードを使用すればエラーが発生するはずである (6241241)」
- 89 ページの「旧バージョンモードで、Access Manager はコンテナに組織を作成できない (6290720)」
- 90 ページの「Portal Server 関連のサービスを追加すると、古いコンソールが表示される (6293299)」
- 90 ページの「リソース制限に達すると、コンソールは Directory Server から設定した結果を返さない (6239724)」

SAML で、信頼パートナーをコンソールで複製すると、エラーが発生する (6326634)

Access Manager コンソールで、SAML 信頼パートナーを「連携」>「SAML」タブから作成します。次に、同じ信頼パートナーを複製しようとすると、エラーが発生します。

回避方法: なし。この問題はパッチ 1 で修正されています。特定のプラットフォームにパッチを適用する方法については、64 ページの「Access Manager 7 2005Q4 パッチ 1」を参照してください。

amConsole.access および amPasswordReset.access でリモートログが機能していない (6311786)

リモートログを設定すると、`amConsole.access` およびパスワードリセット情報の `amPasswordReset.access` 以外のすべてのログは、リモートの Access Manager インスタンスに書き込まれます。しかし、ログレコードはどこにも書き込まれません。

回避方法: なし。

コンソールで amadmin プロパティーをさらに追加すると、amadmin ユーザーパスワードが変更される (6309830)

管理コンソールの `amadmin` ユーザーの一部のプロパティーを追加または編集すると、`amadmin` ユーザーパスワードが変更されます。

回避方法: なし。この問題はパッチ 1 で修正されています。特定のプラットフォームにパッチを適用する方法については、64 ページの「Access Manager 7 2005Q4 パッチ 1」を参照してください。

新しい Access Manager コンソールは CoS テンプレート優先度を設定できない (6309262)

新しい Access Manager 7 2005Q4 コンソールでは、サービスクラス (CoS) のテンプレート優先度を設定または変更できません。

回避方法: Access Manager 6 2005Q1 コンソールにログインし、CoS テンプレート優先度を設定または変更します。

ポリシー管理ユーザーとしてグループをユーザーに追加すると例外エラーが発生する (6299543)

Access Manager コンソールは、ポリシー管理ユーザーとしてグループをユーザーに追加すると、例外エラーを返します。

回避方法: なし。

旧バージョンモードで、ロールからすべてのユーザーを削除できない (6293758)

旧バージョンモードでは、ロールからすべてのユーザーを削除しようとすると、1 人のユーザーが残ります。

回避方法: もう一度ロールからユーザーを削除します。

ディスカバリサービスリソースオファリングを追加、削除、変更できない (6273148)

Access Manager 管理コンソールでは、ユーザーがユーザー、ロール、またはレルムのリソースオファリングを追加、削除、変更することを許可していません。

回避方法: なし。この問題はパッチ 1 で修正されています。特定のプラットフォームにパッチを適用する方法については、64 ページの「Access Manager 7 2005Q4 パッチ 1」を参照してください。

対象検索で、間違った LDAP バインドパスワードを使用すればエラーが発生するはずである (6241241)

Access Manager 管理コンソールは、間違った LDAP バインドパスワードが使用された場合にエラーを返しません。

回避方法: なし。

旧バージョンモードで、Access Manager はコンテナに組織を作成できない (6290720)

コンテナを作成して、コンテナに組織を作成しようとすると、Access Manager は「一意性の違反エラー」を返します。

回避方法: なし。

Portal Server 関連のサービスを追加すると、古いコンソールが表示される (6293299)

Portal Server および Access Manager は同じサーバーにインストールされます。旧バージョンモードでインストールされた Access Manager で、`/amserver` を使用して新しい Access Manager コンソールにログインします。既存のユーザーを選択して NetFile または Netlet などのサービスを追加しようとすると、古い Access Manager コンソール (`/amconsle`) が突然表示されます。

回避方法: なし。Portal Server の現在のバージョンには、Access Manager 6 2005Q1 コンソールが必要です。

リソース制限に達すると、コンソールは Directory Server から設定した結果を返さない (6239724)

Directory Server をインストールしてから Access Manager を既存の DIT オプションでインストールします。Access Manager コンソールにログインし、グループを作成します。グループ内のユーザーを編集します。たとえば、フィルタ `uid=*999*` でユーザーを追加します。その結果表示されるリストボックスは空で、コンソールはエラー、情報または警告のメッセージをまったく表示しません。

回避方法: グループのメンバーシップは、Directory Server 検索サイズの上限よりも多くすることはできません。グループのメンバーシップが多い場合、それに応じて検索サイズの上限を変更します。

SDK およびクライアントに関する問題

- 90 ページの「サブレルムでセッションサービス設定を削除できない (6318296)」
- 91 ページの「ポリシー条件を指定したとき、CDC サーブレットが無効なログインページにリダイレクトする (6311985)」
- 91 ページの「サーバーを再起動した後、クライアントが通知を受け取れない (6309161)」
- 91 ページの「サービススキーマの変更の後、SDK クライアントを再起動する必要がある (6292616)」

サブレルムでセッションサービス設定を削除できない (6318296)

最上位のレルムのサブレルムを作成した後で、サブレルムにセッションサービスを追加すると、続いてセッションサービス設定を削除しようとした場合にエラーメッセージが表示されます。

回避方法: デフォルトの最上位 ID リポジトリである AMSDK1 を削除し、このリポジトリを再び設定に追加します。

この問題はパッチ 1 で修正されています。特定のプラットフォームにパッチを適用する方法については、64 ページの「Access Manager 7 2005Q4 パッチ 1」を参照してください。

ポリシー条件を指定したとき、CDC サーブレットが無効なログインページにリダイレクトする (6311985)

CDSSO モードの Apache エージェント 2.2 では、エージェントの保護されたリソースにアクセスするとき、CDC サーブレットはデフォルトのログインページではなく匿名認証ページにリダイレクトします。

回避方法: なし。この問題はパッチ 1 で修正されています。特定のプラットフォームにパッチを適用する方法については、64 ページの「Access Manager 7 2005Q4 パッチ 1」を参照してください。

サーバーを再起動した後、クライアントが通知を受け取れない (6309161)

クライアント SDK (`amclientsdk.jar`) を使用して書かれたアプリケーションは、サーバーを再起動しても通知を受け取れません。

回避方法: なし。

サービススキーマの変更の後、SDK クライアントを再起動する必要がある (6292616)

任意のサービススキーマを変更した場合、`ServiceSchema.getGlobalSchema` は新しいスキーマではなく古いスキーマを返します。

回避方法: サービススキーマを変更した後、クライアントを再起動します。

この問題はパッチ 1 で修正されています。特定のプラットフォームにパッチを適用する方法については、64 ページの「Access Manager 7 2005Q4 パッチ 1」を参照してください。

コマンド行ユーティリティーに関する問題

Access Manager が Directory Proxy をポイントする場合、null 属性による LDAP 検索でエラーが返される (6357975)

Sun Java System Directory Proxy Server を使用している場合は、null 属性による LDAP 検索を行うとエラーが返されます。次に例を示します。

```
# ldapsearch -b base-dn uid=user ""
```

Access Manager が LDAP ディレクトリサーバーを直接ポイントする場合、この検索は成功します。

回避方法: Directory Proxy Server を使用している場合は、検索で null 属性検索を使用可能にするか、検索のための属性名を指定します。

amserveradmin スクリプトに新しいスキーマファイルがない (6255110)

インストール後に、amserveradmin スクリプトを実行して Directory Server にサービスを読み込む必要がある場合、defaultDelegationPolicies.xml スキーマファイルおよび idRepoDefaults.xml スキーマファイルがスクリプトにありません。

回避方法: amadmin CLI ツールで -t オプションを指定して使用し、defaultDelegationPolicies.xml ファイルおよび idRepoDefaults.xml ファイルを手動で読み込みます。

Internet Explorer 6.0 でエスケープ文字のある XML ドキュメントを保存できない (4995100)

特殊文字 (「&」の隣に文字列 「amp;」など) を XML ファイルに追加した場合、ファイルは正常に保存されますが、あとで Internet Explorer 6.0 を使用して XML プロファイルを取得するとファイルが正しく表示されません。もう一度プロファイルを保存しようとすると、エラーが返されます。

回避方法: なし。

認証に関する問題

- 93 ページの「UrlAccessAgent SSO トークンの有効期限が切れる (6327691)」
- 93 ページの「パスワードを訂正した後、LDAPV3 プラグイン/動的プロファイルでサブレルムにログインできない (6309097)」
- 93 ページの「旧バージョン (互換) モードでの統計サービスに関する Access Manager デフォルト設定の非互換性 (6286628)」
- 93 ページの「最上位の組織で、ネーミング属性の一意性が壊れる (6204537)」

UrlAccessAgent SSO トークンの有効期限が切れる (6327691)

アプリケーションモジュールが特殊ユーザー DN を返さないため、UrlAccessAgent SSO トークンの有効期限が切れます。その結果、特殊ユーザー DN 一致と有効期限の切れないトークンの設定に失敗します。

回避方法: なし。この問題はパッチ 1 で修正されています。特定のプラットフォームにパッチを適用する方法については、64 ページの「Access Manager 7 2005Q4 パッチ 1」を参照してください。

パスワードを訂正した後、LDAPV3 プラグイン/動的プロファイルでサブレルムにログインできない (6309097)

レルムモードでは、ldapv3 データストアを「間違った」パスワードでレルムに作成して、あとで amadmin としてパスワードを変更した場合、変更後のパスワードでログインしようとしても、プロファイルが存在しないというメッセージが表示され、ログインが失敗します。

回避方法: なし。

旧バージョン (互換) モードでの統計サービスに関する Access Manager デフォルト設定の非互換性 (6286628)

Access Manager を旧バージョンモードでインストールしたあと、統計サービスのデフォルト設定が変更されています。

- サービスがデフォルトでオンになっています (com.iplanet.services.stats.state=file)。以前はオフでした。
- デフォルトの間隔 (com.iplanet.am.stats.interval) が 3600 から 60 に変更されています。
- デフォルトの統計ディレクトリ (com.iplanet.services.stats.directory) が /var/opt/SUNWam/debug から /var/opt/SUNWam/stats に変更されています。

回避方法: なし。

最上位の組織で、ネーミング属性の一意性が壊れる (6204537)

Access Manager をインストールした後、amadmin としてログインし、o、sunPreferredDomain、associatedDomain、sunOrganizationAlias、uid、および mail 属性を「一意の属性リスト」に追加します。2 つの組織を同じ名前で作成した場合、操作は失敗しますが、予期した「属性の一意性に違反しています」のメッセージではなく「その組織はすでに存在します」のメッセージが表示されます。

回避方法: なし。正しくないメッセージを無視してください。Access Manager は正常に動作しています。

セッションおよび SSO に関する問題

タイムゾーンを越えた Access Manager インスタンスがほかのユーザーセッションをタイムアウトにする (6323639)

異なるタイムゾーンを越えて同じトラストサークル内に Access Manager インスタンスがインストールされている場合、ユーザーセッションのタイムアウトが発生します。

セッションフェイルオーバー (amsfoconfig) スクリプトには Linux 2.1 システムに対して不正なアクセス権が設定されている (6298433)

セッションフェイルオーバーの設定スクリプト (/opt/sun/identity/bin/amsfoconfig) には不正なアクセス権が設定されいるため、Linux 2.1 システム上で実行できません。

回避方法: アクセス権を変更して amsfoconfig スクリプトを実行できるようにします (たとえば、755)。

この問題はパッチ 1 で修正されています。特定のプラットフォームにパッチを適用する方法については、64 ページの「Access Manager 7 2005Q4 パッチ 1」を参照してください。

セッションフェイルオーバー (amsfoconfig) スクリプトが Linux 2.1 システムで失敗する (6298462)

タブ文字 (\t) が正しく解釈されないため、Linux 2.1 サーバー上でセッションフェイルオーバーの設定スクリプト (amsfoconfig) が失敗します。

回避方法: セッションフェイルオーバーを手動で設定します。詳細は、『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』の「セッションフェイルオーバーの手動での設定」を参照してください。

この問題はパッチ 1 で修正されています。特定のプラットフォームにパッチを適用する方法については、64 ページの「Access Manager 7 2005Q4 パッチ 1」を参照してください。

ロードバランサに SSL 終了を設定した場合に、システムが無効なサービスホスト名を作成する (6245660)

ロードバランサに SSL 終了を設定した Web コンテナとしての Web Server に Access Manager が配備されている場合、クライアントは正しい Web Server ページにダイレクトされません。Access Manager コンソールで「セッション」タブをクリックしても、ホストが無効なためエラーが返されます。

回避方法: 次の例では、Web Server はポート 3030 で待機します。ロードバランサはポート 80 で待機し、要求を Web Server にリダイレクトします。

web-server-instance-name/config/server.xml ファイルで、使用している Web Server のリリースに従って servername 属性をロードバランサを示すように変更します。

Web Server 6.1 Service Pack (SP) リリースでは、servername 属性を次のように編集します。

```
<LS id="ls1" port="3030" servername="loadbalancer.example.com:80"
defaultvs="https-sample" security="false" ip="any" blocking="false"
acceptorthreads="1"/>
```

Web Server 6.1 SP2 (または以降) では、プロトコルを http から https または https から http へと切り替えることができます。つまり、servername を次のように編集します。

```
<LS id="ls1" port="3030"
servername="https://loadbalancer.example.com:443" defaultvs="https-sample"
security="false" ip="any" blocking="false" acceptorthreads="1"/>
```

サードパーティー Web コンテナで HttpSession を使用する (CR 番号なし)

認証用にセッションを維持するデフォルトの方法は、HttpSession ではなく、「内部セッション」です。無効なセッションの最大時間値は、デフォルトの 3 分で十分です。amtune スクリプトは、Web Server または Application Server の場合に、この値を 1 分に設定します。ただし、サードパーティー Web コンテナ (IBM WebSphere または BEA WebLogic Server) とオプションの HttpSession を使用する場合は、Web コンテナの最大 HttpSession 時間を制限して、パフォーマンスの問題を避ける必要がある可能性があります。

ポリシーに関する問題

ポリシー設定サービスで動的属性を削除すると、ポリシーの編集で問題が発生する (6299074)

ポリシー設定サービスで動的属性を削除すると、次のシナリオのポリシーの編集で問題が発生します。

1. ポリシー設定サービスで 2 つの動的属性を作成します。
2. ポリシーを作成し、(手順 1 からの) 動的属性を応答プロバイダで選択します。
3. ポリシー設定サービスで動的属性を削除し、属性をさらに 2 つ作成します。
4. 手順 2 で作成したポリシーを編集します。

上記の手順を実行するとエラーとなり、「エラー 無効な動的プロパティーが設定されています」というメッセージが返されます。デフォルトでは、表示されるポリシーはありません。検索が終了した後、ポリシーが表示されますが、既存のポリシーを編集または削除したり、新しいポリシーを作成したりすることはできません。

回避方法: ポリシー設定サービスから動的属性を削除する前に、ポリシーからこれらの属性への参照を削除します。

サーバーの起動に関する問題

- 96 ページの「Access Manager の起動時に、デバッグエラーが発生する (6309274, 6308646)」
- 96 ページの「Web コンテナとしての BEA WebLogic Server の使用」

Access Manager の起動時に、デバッグエラーが発生する (6309274, 6308646)

Access Manager 7 2005Q4 の起動では、`amDelegation` および `amProfile` デバッグファイルにデバッグエラーを返します。

- `amDelegation`: 委譲のためのプラグインのインスタンスを取得できません
- `amProfile`: 委譲の例外を取得します

回避方法: なし。このメッセージは無視できます。

Web コンテナとしての BEA WebLogic Server の使用

BEA WebLogic Server を Web コンテナとして使用して Access Manager を配備した場合、Access Manager にアクセスできないことがあります。

回避方法: WebLogic Server を 2 回再起動すると Access Manager にアクセスできるようになります。

Linux OS に関する問題

Application Server 上で Access Manager を実行すると、JVM の問題が生じる (6223676)

Red Hat Linux で Application Server 8.1 を実行している場合、Application Server 用に Red Hat OS が作成するスレッドのスタックサイズは 10M バイトですが、Access Manager ユーザーセッション数が 200 に達すると、JVM リソースの問題が発生する可能性があります。

回避方法: Application Server を起動する前に、`ulimit` コマンドを実行して、Red Hat OS が操作するスタックサイズを 2048K バイトまたは 256K バイトなどの小さな値に設定します。`ulimit` コマンドは、Application Server の起動に使用する同じコンソールで実行します。次に例を示します。

```
# ulimit -s 256;
```

連携および SAML に関する問題

Web サービスサンプルを実行すると「Resource offering not found」が返される (6359900)

Access Manager を *AccessManager-base*`/SUNWam/samples/phase2/wsc` ディレクトリ (Solaris システムの場合) または *AccessManager-base* `/identity/samples/phase2/wsc` ディレクトリ (Linux システムの場合) にある Web サービスサンプルにアクセスするように設定している場合、ディスカバリサービスを照会したり、リソースオファリングを変更したりすると、次のエラーメッセージが返されます。

AccessManager-base は、ベースインストールディレクトリです。デフォルトのベースインストールディレクトリは、Solaris システムの場合は `/opt`、Linux システムの場合は `/opt/sun` です。

回避方法:

1. Solaris システムの場合は *AccessManager-base* `/SUNWam/samples/phase2/wsc` ディレクトリ、Linux システムの場合は *AccessManager-base*`/identity/samples/phase2/wsc` ディレクトリに移動します。
2. `index.jsp` ファイルで、次の文字列を検索します。

   ```
   com.sun.org.apache.xml.security.utils.XMLUtils.outputDOM
   ```
3. 前の手順で見つけた文字列を含む行の直前に、次の新しい行を挿入します。

   ```
   com.sun.org.apache.xml.security.Init.init();
   ```
4. サンプルを再実行します。Access Manager を再起動する必要はありません。

アーティファクトプロファイルを使用したときに連携が失敗する (6324056)

アイデンティティープロバイダ (IDP) およびサービスプロバイダ (SP) を設定し、ブラウザのアーティファクトプロファイルを使用するように通信プロトコルを変更してから、IDP および SP の間でユーザーを連携しようとすると、連携が失敗します。

回避方法: なし。

SAML ステートメント中の特殊文字 (&) は、エンコードされるはずである (6321128)

Access Manager をソースサイトおよびデスティネーションサイトとして SSO を設定すると、SAML ステートメント中の特殊文字 (&) がエンコードされず、表明のパースが失敗するため、デスティネーションサイトでエラーが発生します。

回避方法: なし。この問題はパッチ 1 で修正されています。特定のプラットフォームにパッチを適用する方法については、64 ページの「Access Manager 7 2005Q4 パッチ 1」を参照してください。

ディスカバリサービスをロールに追加しようとすると、例外が発生する (6313437)

Access Manager コンソールで、リソースオファリングをディスカバリサービスに追加しようとすると、不明な例外が発生します。

回避方法: なし。

認証コンテキスト属性が、その他の属性を設定して保存するまで設定できない (6301338)

認証コンテキスト属性は、その他の属性を設定して保存するまで設定できません。

回避方法: 認証コンテキスト属性を設定する前に、プロバイダプロファイルを設定し保存します。

ルートサフィックスに & 文字が含まれている場合、EP サンプルが動作しない (6300163)

Directory Server のルートサフィックスに「&」文字が含まれている場合、「Employee Profile Service」リソースオファリングを追加しようとすると例外がスローされます。

回避方法: なし。

連携でログアウトエラーが発生する (6291744)

レルムモードで、アイデンティティープロバイダ (IDP) およびサービスプロバイダ (SP) でユーザーアカウントを連携し、連携を終了してログアウトするとエラーが発生して「エラー: サブ組織が見つかりません。」というメッセージが返されます。

回避方法: なし。

国際化 (g11n) に関する問題

ユーザーのロケール設定が、管理コンソール全体に適用されない (6326734)

Access Manager 管理コンソールの一部は、ユーザーロケールの設定に従わず、ブラウザのロケール設定を使用します。この問題は、「バージョン」およびオンラインヘルプの内容とともに、「バージョン」、「ログアウト」、およびオンラインヘルプボタンに影響します。

回避方法: ブラウザの設定をユーザー設定と同じロケールに変更します。

Access Manager が IBM WebSphere に配備されている場合、ヨーロッパ言語のオンラインヘルプが完全には利用できない (6325024)

すべてのヨーロッパ言語ロケール (スペイン語、ドイツ語、およびフランス語) では、Access Manager が IBM WebSphere の Application Server インスタンスに配備されている場合、オンラインヘルプが完全には利用できません。オンラインヘルプでは、次のフレームで「アプリケーションエラー」が表示されます。

- 上部のフレームで、実際は「ヘルプ」および「閉じる」ボタンがある場所。
- 左側のフレームで、実際は「目次」、「インデックス」および「検索」ボタンがある場所。

回避方法: ブラウザの言語設定を英語に設定してページを更新し、左側のフレームにアクセスします。ただし、上部のフレームは「アプリケーションエラー」が引き続き表示されます。

Access Manager が IBM WebSphere に配備されている場合、バージョン情報が空白になる (6319796)

Access Manager が IBM WebSphere Application Server インスタンスに配備されているとき、どのロケールの場合でも「バージョン」ボタンをクリックしても製品バージョンは利用できません。代わりに空白のページが表示されます。

回避方法: なし。

クライアントディテクションで UTF-8 の削除が動作しない (5028779)

「クライアントディテクション」機能は正常に動作しません。Access Manager 7 2005Q4 コンソールに加えられた変更は、自動的にブラウザに送られません。

回避方法: 2 つの回避方法があります。

- 「クライアントディテクション」セクションに変更を加えた後で、Access Manager Web コンテナを再起動します。

  または

- Access Manager コンソールで、次の手順を実行します。
  1. 「設定」タブの下にある「クライアントディテクション」をクリックします。
  2. 「genericHTML」の「編集」リンクをクリックします。
  3. 「HTML」タブの下の、「genericHTML」リンクをクリックします。

4. 文字セットのリストで、エントリとして UTF-8;q=0.5 を入力します (UTF-8 q 係数がロケールのその他の文字セットよりも小さくなるようにする)。
5. 保存してログアウトし、もう一度ログインします。

複数バイト文字がログファイルで疑問符として表示される (5014120)

/var/opt/SUNWam/logs ディレクトリ内のログファイルにある複数バイトのメッセージが疑問符 (?) として表示されます。ログファイルはネイティブなエンコーディングで、常に UTF-8 ではありません。Web コンテナインスタンスを特定のロケールで起動すると、ログファイルはそのロケールのネイティブなエンコーディングになります。別のロケールに切り替えて Web コンテナインスタンスを再起動すると、それ以降のメッセージは現在のロケールのネイティブなエンコーディングになりますが、それ以前のエンコーディングのメッセージは疑問符として表示されます。

回避方法: 常に同じネイティブなエンコーディングを使用して Web コンテナインスタンスを起動するようにします。

マニュアルに関する情報

- 102 ページの「Access Manager がレルムモードから旧バージョンモードに戻らないことについて (6508473)」
- 102 ページの「持続検索の無効化の詳細について (6486927)」
- 103 ページの「Access Manager がサポートする権限とサポートしない権限について (2143066)」
- 104 ページの「Cookie ベースのスティッキー要求ルーティングについて (6476922)」
- 105 ページの「Windows 2003 の Windows デスクトップ SSO の設定について (6487361)」
- 106 ページの「分散認証 UI サーバーのパスワードの設定手順について (6510859)」
- 106 ページの「「新しいサイト名を作成する」のオンラインヘルプ情報を詳細化する必要がある (2144543)」
- 107 ページの「Windows システムの管理者パスワードの設定パラメータが ADMIN_PASSWD であることについて (6470793)」
- 107 ページの「リリースノートの既知の問題点に対する回避方法に誤った記述がある (6422907)」
- 107 ページの「AMConfig.properties 内のドキュメント com.iplanet.am.session.protectedPropertiesList (6351192)」
- 107 ページの「LDAPv3 プラグインのロールおよびフィルタを適用したロールのサポートについて (6365196)」
- 108 ページの「AMConfig.properties ファイルの未使用のプロパティーについて (6344530)」
- 108 ページの「サーバー側の com.iplanet.am.session.client.polling.enable を true にしてはいけない (6320475)」

- 108 ページの「コンソールのオンラインヘルプで、デフォルトの成功 URL が正しくない (6296751)」
- 108 ページの「XML 暗号化を有効にする方法について (6275563)」

Access Manager がレルムモードから旧バージョンモードに戻らないことについて (6508473)

Access Manager 7 2005Q4 をレルムモードでインストールした場合は、旧バージョンモードに戻すことができません。

しかし、Access Manager 7 2005Q4 を旧バージョンモードでインストールした場合は、`-M` オプションを指定して `amadmin` コマンドを実行することにより、レルムモードに変更できます。次に例を示します。

```
amadmin -u cn=amAdmin,ou=People,dc=example,dc=com -w amadmin-password
-M dc=example,dc=com
```

持続検索の無効化の詳細について (6486927)

Access Manager は、変更された Sun Java System Directory Server エントリに関する情報を受け取るために持続検索を使用します。デフォルトでは、Access Manager はサーバーの起動時に次の持続検索接続を作成します。

`aci` - LDAP フィルタ (`aci=*`) を使用した検索における `aci` 属性の変更。

`sm` - Access Manager 情報ツリー (またはサービス管理ノード) の変更。これには、`sunService` または `sunServiceComponent` マーカーオブジェクトクラスを持つオブジェクトが含まれます。たとえば、保護されたリソースのアクセス権限を定義するためのポリシーを作成する場合や、既存のポリシーのルール、対象、条件、または応答プロバイダを変更する場合があります。

`um` - ユーザーディレクトリ (またはユーザー管理ノード) の変更。たとえば、ユーザーの名前やアドレスを変更する場合があります。

注意 – これらのコンポーネントの持続検索を無効にすることはお勧めできません。これは、無効にした持続検索が Directory Server からの通知を受信しなくなるためです。その結果、Directory Server で行われたそのコンポーネントに関する変更がコンポーネントキャッシュに通知されず、コンポーネントキャッシュが無効になります。

たとえば、ユーザーディレクトリの変更に対する持続検索 (um) を無効にすると、Access Manager サーバーは Directory Server から通知を受け取りません。このため、エージェントも Access Manager から通知を受け取らず、そのローカルユーザーキャッシュを新しい値のユーザー属性で更新しません。この場合、アプリケーションがエージェントにユーザー属性を照会すると、アプリケーションはその属性の古い値を受け取る可能性があります。

このプロパティーは、特殊な状況でどうしても必要な場合に限って使用してください。たとえば、(セッションサービスや認証サービスなどのサービスに対する値の変更に関して) サービス設定の変更が本稼働環境で発生しないことがわかっている場合は、サービス管理 (sm) コンポーネントに対する持続検索を無効にできます。ただし、いずれかのサービスに関して変更が発生した場合は、サービスを再起動する必要があります。aci や um で指定されるほかの持続検索にも、同じ条件が適用されます。

詳細は、63 ページの「CR# 6363157: どうしても必要な場合に、新しいプロパティーで持続検索を無効にする」を参照してください。

Access Manager がサポートする権限とサポートしない権限について (2143066)

権限とは、レルム内に存在するロールやグループのメンバーである管理者のアクセス権を定義したものです。Access Manager では、次の管理者タイプに対するアクセス権を設定できます。

- レルム管理者は、アイデンティティーリポジトリ (データストア) の定義、認証の設定、ポリシーの定義など、レルムに関するすべてのタスクを実行できます。
- ポリシー管理者は、既存のレルムのポリシーを設定できます。

次の権限がサポートされています。

- すべてのレルムプロパティーおよびポリシープロパティーに対する読み取りおよび書き込みアクセス。レルム管理者に対して読み取りおよび書き込みアクセス権を定義します。
- ポリシープロパティーのみに対する読み取りおよび書き込みアクセス。ポリシー管理者に対して読み取りおよび書き込みアクセス権を定義します。

- サポートされている権限の組み合わせ: ポリシープロパティーのみに対する読み取りおよび書き込みのアクセス、およびデータストアに対する読み取り専用アクセス。ほかの権限の組み合わせはサポートされていません。

Cookie ベースのスティッキー要求ルーティングについて (6476922)

Access Manager サーバーがロードバランサの背後に配備されている場合は、Cookie ベースのスティッキー要求ルーティングにより、クライアント要求が誤った Access Manager サーバー (つまり、該当するセッションをホストしていないサーバー) に経路指定されなくなります。この機能は、Access Manager 7 2005Q4 パッチ 3 で実装されました。

従来の動作では、Cookie ベースのスティッキー要求ルーティングが行われないため、非ブラウザベースのクライアント (リモートの Access Manager クライアント SDK を使用するポリシーエージェントやクライアント) からの要求が、該当するセッションをホストしていない Access Manager サーバーに誤って経路指定されていました。そのため、要求を正しいサーバーに送信するには、Access Manager サーバーがバックチャネル通信を使用してセッションの妥当性検査を行う必要があり、通常はそれがパフォーマンス低下の原因になっていました。Cookie ベースのスティッキー要求ルーティングでは、このバックチャネル通信を行う必要がないため、Access Manager のパフォーマンスが向上します。

Cookie ベースのスティッキー要求ルーティングを実装するには、Access Manager の配備をサイトとして設定してください。詳細は、『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』の「サイトとしての Access Manager 配備の設定」を参照してください。

Cookie ベースのスティッキー要求ルーティングを設定するには、次の手順に従います。

1. Cookie 名を指定するため、`AMConfig.properties` ファイルに `com.iplanet.am.lbcookie.name` プロパティーを設定します。Access Manager が 2 バイトのサーバー ID (01、02、03 など) を使用してロードバランサの Cookie 値を生成します。Cookie 名を指定しなかった場合は、Access Manager がデフォルト名である `amlbcookie` と 2 バイトのサーバー ID を使用してロードバランサの Cookie 値を生成します。

   Access Manager サーバーで Cookie 名を設定する場合は、ポリシーエージェントの `AMAgent.properties` ファイル内でも同じ名前を使用する必要があります。また、Access Manager クライアント SDK を使用している場合は、Access Manager サーバーで使用されているものと同じ Cookie 名を使用する必要があります。

   注: Access Manager が 2 バイトのサーバー ID を使用して Cookie 値を設定するため、`com.iplanet.am.lbcookie.value` プロパティーは設定しないでください。

2. 手順 1 で設定された Cookie 名を使用してロードバランサを設定します。Access Manager の配備にハードウェアロードバランサまたはソフトウェアロードバランサを使用することができます。
3. セッションフェイルオーバーが実装されている場合は、ポリシーエージェントと Access Manager サーバーの両方で `com.sun.identity.session.resetLBCookie` プロパティーを有効にします。
   - ポリシーエージェントの場合は、このプロパティーを `AMAgents.properties` ファイルに追加して有効にします。
   - Access Manager サーバーの場合は、このプロパティーを `AMConfig.properties` ファイルに追加して有効にします。

   次に例を示します。

   ```
   com.sun.identity.session.resetLBCookie='true'
   ```

   フェイルオーバーの状況が発生した場合は、セカンダリ Access Manager サーバーにセッションが経路指定され、セカンダリ Access Manager サーバーのサーバー ID を使用してロードバランサの Cookie 値が設定されます。該当するセッションの後続の要求は、セカンダリ Access Manager サーバーに経路指定されます。

Windows 2003 の Windows デスクトップ SSO の設定について (6487361)

Windows 2003 で Windows デスクトップ SSO を設定するには、『Sun Java System Access Manager 7 2005Q4 管理ガイド』の「Windows デスクトップ SSO の設定」で説明されているように、次の `ktpass` コマンドを使用します。

```
ktpass /out filename /mapuser username
/princ HTTP/hostname.domainname /crypto encryptiontype /rndpass
/ptype principaltype /target domainname
```

次に例を示します。

```
ktpass /out demo.HTTP.keytab
/mapuser http /princ HTTP/demo.identity.sun.com@IDENTITY.SUN.COM
/crypto RC4-HMAC-NT /rndpass /ptype KRB5_NT_PRINCIPAL /target IDENTITY.SUN.COM
```

構文の定義については、次のサイトを参照してください。

http://technet2.microsoft.com/WindowsServer/en/library/64042138-9a5a-4981-84e9-d576a8db0d051033.mspx?mfr=true

分散認証 UI サーバーのパスワードの設定手順について (6510859)

次の手順は、Access Manager サーバーと通信する分散認証 UI サーバーに対して暗号化されたパスワードを設定する方法を説明したものです。

分散認証 UI サーバーにパスワードを設定するには、次の手順に従います。

1. Access Manager サーバーで、次の手順を実行します。
   a. `ampassword -e` ユーティリティーを使用して `amadmin` パスワードを暗号化します。Solaris システムの場合の例を示します。

      ```
      # cd /opt/SUNWam/bin
      # ./ampassword -e amadmin-password
      AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      ```

      暗号化された値を保存します。
   b. Access Manager サーバーの `AMConfig.properties` ファイルから `am.encryption.pwd` プロパティーの値をコピーして保存します。次に例を示します。

      ```
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```
2. 分散認証 UI サーバーで、`AMConfig.properties` ファイルに対して次の変更を行います。
   a. `com.iplanet.am.service.password` プロパティーをコメントにします。
   b. `com.iplanet.am.service.secret` プロパティーを手順 1a で暗号化された `amadmin` パスワードに設定します。
   c. 手順 1b でコピーした `am.encryption.pwd` と暗号化された値を追加します。次に例を示します。

      ```
      com.sun.identity.agents.app.username=username
      #com.iplanet.am.service.password=password
      com.iplanet.am.service.secret=AQIC0K3omEozd544XEJIg25GT2wi1D7UAQLX
      am.encryption.pwd=ydV8JXhJF2J35vpxjZRiGt7SH/7mUr+Y
      ```
3. 分散認証 UI サーバーを再起動します。

「新しいサイト名を作成する」のオンラインヘルプ情報を詳細化する必要がある (2144543)

Access Manager コンソールのオンラインヘルプの「設定」>「システムプロパティー」>「プラットフォーム」にある「新しいサイト名を作成する」には、保存手順が記載されていません。新しいサイト名を追加したあとで、「保存」をクリックせずにインスタンス名を追加しようとすると、処理が失敗します。このため、サイト名を追加したあとは、必ず「保存」をクリックしてからインスタンス名を追加してください。

Windows システムの管理者パスワードの設定パラメータが ADMIN_PASSWD であることについて (6470793)

Solaris システムと Linux システムの amsamplesilent ファイルでは、Access Manager の管理者 (amadmin) パスワードの設定パラメータは ADMINPASSWD です。しかし、Windows システムの AMConfigurator.properties ファイルでは、このパラメータは ADMIN_PASSWD です。

Windows システムで amconfig.bat を実行する場合は、ADMINPASSWD ではなく ADMIN_PASSWORD パラメータを使用して AMConfigurator.properties ファイルの amadmin パスワードを設定してください。

リリースノートの既知の問題点に対する回避方法に誤った記述がある (6422907)

97 ページの「Web サービスサンプルを実行すると「Resource offering not found」が返される (6359900)」 の回避方法の手順 3 が修正されました。

AMConfig.properties 内のドキュメント com.iplanet.am.session.protectedPropertiesList (6351192)

com.iplanet.am.session.protectedPropertiesList パラメータを使用すると、特定のコアまたは内部セッションプロパティーを、セッションサービスの SetProperty メソッドによるリモート更新から保護できます。この「非表示」キーセキュリティーパラメータを設定することで、認証や Access Manager のその他の機能が利用できるようにセッション属性をカスタマイズできます。このパラメータを使用するには、次の手順に従います。

1. テキストエディタで、このパラメータを AMConfig.properties ファイルに追加します。
2. 保護する必要のあるセッションプロパティーに、このパラメータを設定します。次に例を示します。

   ```
   com.iplanet.am.session.protectedPropertiesList =
   PropertyName1,PropertyName2,PropertyName3
   ```

3. Access Manager Web コンテナを再起動して、値を有効にします。

LDAPv3 プラグインのロールおよびフィルタを適用したロールのサポートについて (6365196)

各パッチを適用後、データを Sun Java System Directory Server に保存する場合に、LDAPv3 プラグインにロールおよびフィルタを適用したロールを設定できます (CR 6349959 を修正)。Access Manager 7 2005Q4 管理コンソールで、「LDAPv3 プラグインでサポートされるタイプおよび操作」フィールドの LDAPv3 の設定に、次のような値を入力します。

```
role: read,edit,create,delete
filteredrole: read,edit,create,delete
```

LDAPv3 の設定で使用するロールやフィルタを適用したロールに応じて、上のエントリのいずれかまたは両方を入力できます。

AMConfig.properties ファイルの未使用のプロパティーについて (6344530)

AMConfig.properties ファイルの次のプロパティーは使用されていません。

```
com.iplanet.am.directory.host
com.iplanet.am.directory.port
```

サーバー側の com.iplanet.am.session.client.polling.enable を true にしてはいけない (6320475)

AMConfig.properties ファイル内の com.iplanet.am.session.client.polling.enable プロパティーは、サーバー側で true に設定してはいけません。

回避方法: このプロパティーはデフォルトで false に設定されており、true にリセットしてはいけません。

コンソールのオンラインヘルプで、デフォルトの成功 URL が正しくない (6296751)

service.scserviceprofile.iplanetamauthservice.html オンラインヘルプファイル内にある「デフォルト成功 URL」が正しくありません。「デフォルト成功 URL」フィールドは、正常に認証された後に、リダイレクトされる URL を指定した複数の値が含まれるリストを受け入れます。この属性のフォーマットは clientType|URL で、URL の値だけを指定できますが、デフォルトタイプは HTML を前提としています。

デフォルト値「/amconsole」は正しくありません。

回避方法 正しいデフォルト値は「/amserver/console」です。

XML 暗号化を有効にする方法について (6275563)

Bouncy Castle JAR ファイルを使用して、Access Manager または Federation Manager で XML 暗号化を有効にしてトランスポートキーを生成するには、次の手順に従います。

1. JDK 1.5 より前の JDK バージョンを使用している場合は、Bouncy Castle サイト (http://www.bouncycastle.org/) から Bouncy Castle JCE プロバイダをダウンロードします。たとえば、JDK 1.4 の場合、bcprov-jdk14-131.jar ファイルをダウンロードします。

2. 前の手順で JAR ファイルをダウンロードした場合は、ファイルを *jdk_root*/jre/lib/ext ディレクトリにコピーします。
3. JDK の国内版の場合、Sun サイト (http://java.sun.com) から、お使いの JDK のバージョンに対応する JCE Unlimited Strength Jurisdiction Policy Files をダウンロードします。IBM WebSphere の場合は、対応する IBM サイトに移動し、必要なファイルをダウンロードします。
4. ダウンロードした US_export_policy.jar および local_policy.jar ファイルを *jdk_root*/jre/lib/security ディレクトリにコピーします。
5. JDK 1.5 より前の JDK のバージョンを使用している場合は、*jdk_root*/jre/lib/security/java.security ファイルを編集し、プロバイダの 1 つとして Bouncy Castle を追加します。次に例を示します。

   ```
   security.provider.6=org.bouncycastle.jce.provider.BouncyCastleProvider
   ```

6. AMConfig.properties ファイルで、次のプロパティーを true に設定します。

   ```
   com.sun.identity.jss.donotInstallAtHighestPriority=true
   ```

7. Access Manager Web コンテナを再起動します。

詳細については、問題 ID 5110285 (XML 暗号化には Bouncy Castle JAR ファイルが必要) を参照してください。

マニュアルの更新

Sun Java System Access Manager 7 2005Q4 コレクション

次の表に、初期リリース以降に発行された Access Manager 7 2005Q4 の新規または改訂マニュアルを示します。これらのマニュアルにアクセスするには、Access Manager 7 2005Q4 コレクションを参照してください。

http://docs.sun.com/coll/1292.1

表 7　Access Manager 7 2005Q4 マニュアル更新履歴

タイトル	発行日
『Sun Java System Access Manager 7 2005Q4 リリースノート』	表 1 を参照してください。
『Sun Java System Access Manager 7 2005Q4 管理ガイド』	2006 年 2 月
『Sun Java System Access Manager 7 2005Q4 Developers Guide』	2006 年 2 月
『Sun Java System Access Manager Policy Agent 2.2 User's Guide』	2006 年 2 月
『Sun Java System Access Manager 7 2005Q4 C API Reference』	2006 年 2 月
『Sun Java System Access Manager 7 2005Q4 Federation and SAML Administration Guide』	2006 年 2 月
『Technical Note: Using Access Manager Distributed Authentication』	2006 年 2 月
『Technical Note: Installing Access Manager to Run as a Non-Root User 』	2006 年 2 月
『Sun Java System SAML v2 Plug-in for Federation Services User's Guide 』	2006 年 2 月
『Sun Java System SAML v2 Plug-in for Federation Services Release Notes 』	2006 年 2 月
『Sun Java System SAMLv2 Plug-in for Federation Services Java API Reference 』	2006 年 2 月
『Sun Java System Access Manager 7 2005Q4 配備計画ガイド』	2006 年 1 月
『Sun Java System Access Manager 7 2005Q4 Performance Tuning Guide 』	2005 年 12 月
『Sun Java System Access Manager 7 2005Q4 Technical Overview』	2005 年 12 月

Sun Java System Federation Manager 7.0 2005Q4 コレクション

Federation Manager 7.0 2005Q4 コレクションのマニュアルにアクセスするには、以下を参照してください。

http://docs.sun.com/coll/1321.1

Sun Java System Access Manager Policy Agent 2.2 コレクション

Access Manager Policy Agent 2.2 コレクションは、新しいエージェントに関する記載を盛り込むため、継続して改訂されます。このコレクションのマニュアルにアクセスするには、以下を参照してください。

http://docs.sun.com/coll/1322.1

再配布可能ファイル

Sun Java System Access Manager 7 2005Q4 には、製品のライセンスを取得していないユーザーに再配布できるファイルは含まれていません。

問題の報告とフィードバックの方法

Access Manager または Sun Java Enterprise System で問題が生じた場合、次のいずれかの方法で Sun の担当者にご連絡ください。

- http://sunsolve.sun.com/ にある Sun サポートリソース (SunSolve)。

  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、ProductTracker 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。
- 保守契約を結んでいるお客様は、専用ダイヤルをご利用ください。

最善の問題解決のため、テクニカルサポートに連絡する際はあらかじめ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
- マシン機種、OS バージョン、および、問題の原因と思われるパッチやそのほかのソフトウェアなどの製品バージョン
- 問題を再現するための具体的な手順の説明
- 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、「コメントの送信」をクリックします。

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、Access Manager リリースノートの Part No. は 819-3474 です。

Sun が提供しているその他の情報

次の場所から Access Manager に関する情報とリソースを入手できます。

- Sun Java Enterprise System のマニュアル: http://docs.sun.com/prod/entsys.05q4
- Sun サービス: http://www.sun.com/service/consulting/
- ソフトウェア製品およびサービス: http://wwws.sun.com/software/
- サポートリソース: http://sunsolve.sun.com/
- 開発者用情報: http://developers.sun.com/
- Sun 開発者サポートサービス: http://www.sun.com/developers/support/

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。アプリケーションの最新バージョンは http://sun.com/software/javaenterprisesystem/get.html から入手できます。

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。
