ADOBE® LIVECYCLE® ES4 の堅牢化とセキュリティガイド

法律上の注意

法律上の注意については、http://help.adobe.com/ja_JP/legalnotices/index.html を参照してください。

目次

第 1 章：このドキュメントの内容

1.1 このドキュメントの内容

この記事では、JEE 実稼働環境での AEM forms のセキュリティを最大限に強化する方法について説明します。

JEE 上の AEM forms の追加のセキュリティ情報およびベストプラクティスについては、デベロッパーセンターを参照してください。

AEM forms に関するセキュリティ情報およびセキュリティ速報については、アドビのセキュリティ情報サイトを参照してください。

1.1.1 このドキュメントの対象読者

このドキュメントは、アプリケーション設計または JEE での AEM forms のインフラストラクチャ開発およびデプロイメントを行うコンサルタント、セキュリティの専門家、システムアーキテクト、IT プロフェッショナルを読者として想定しています。また、この対象読者には、次のような一般的な職務の担当者も含まれます。

- 自社または顧客の組織に、Web アプリケーションとサーバーを保護した状態でデプロイする必要がある IT エンジニアおよびオペレーションエンジニア
- 組織内のクライアントマシンのアーキテクチャ計画に責任を負うアーキテクトおよびプランナー
- 組織内のプラットフォーム全体のセキュリティ保護に取り組む IT セキュリティ専門家
- 顧客とパートナーの詳細なリソースを必要とするアドビおよびパートナーのコンサルタント

1.1.2 このガイドで使用する規則

このドキュメントで使用する一般的なファイルパスの命名規則は、次のとおりです。

名前	デフォルト値	説明
[aem_forms root]	Windows の場合：C:\Adobe\Adobe_Experience_Manager_forms。AIX、Linux、Solaris の場合：/opt/adobe/adobe_experience_manager_forms	すべての AEM forms モジュールで使用するインストールディレクトリ。インストールディレクトリには、Configuration Manager 用のサブディレクトリが含まれます。このディレクトリには、サードパーティのテクノロジーに関連したディレクトリも含まれます。
[JBoss root]	C:\Adobe\Adobe_Experience_Manager_forms\jboss	（JBoss の自動インストール）AEM forms を実行するアプリケーションサーバーのホームディレクトリ。

第 2 章：セキュリティに関する一般的な考慮事項

2.1 セキュリティに関する一般的な考慮事項

この記事には、AEM forms 環境を堅牢化するための準備に役立つ、基本的な情報を記載しています。これには、JEE 上の AEM forms、オペレーティングシステム、アプリケーションサーバー、データベースセキュリティに関する前提条件の情報も含まれます。環境のロックダウンを行う前に、この情報を確認してください。

2.1.1 ベンダー固有のセキュリティ情報

この節には、JEE 上の AEM forms ソリューションに統合されるオペレーティングシステム、アプリケーションサーバーおよびデータベースに関するセキュリティ関連情報を記載しています。

このセクションにあるリンクを使用して、使用しているオペレーティングシステム、データベースおよびアプリケーションサーバーのベンダーに固有のセキュリティ情報を検索してください。

2.1.1.1 オペレーティングシステムのセキュリティ情報

オペレーティングシステムを保護する際には、オペレーティングシステムのベンダーが挙げている対策を実装することを慎重に検討してください。この対策には、以下のものがあります。

- ユーザー、ロール、権限を定義し、制御する
- ログと監査記録を監視する
- 不要なサービスとアプリケーションを削除する
- ファイルのバックアップを作成する

JEE 上の AEM forms がサポートするオペレーティングシステムのセキュリティ情報については、次の表の資料を参照してください。

オペレーティングシステム	セキュリティ情報
IBM® AIX® 5.3 および 6.1	IBM AIX Security Benefits
Microsoft® Windows® XP SP2（実稼働環境以外の場合のみ）	Windows XP Security Guide
Microsoft Windows 7、32 ビットおよび 64 ビット（実稼働環境以外の場合のみ）	Windows 7 Security Guide
Microsoft Windows Server® 2003 Enterprise Edition、Standard Edition	Microsoft.com の「Windows Server 2003 Security Guide」を検索してください
Microsoft Windows Server® 2008 Enterprise Edition、Standard Edition	Microsoft.com の「Windows Server 2008 Security Guide」を検索してください。
Microsoft Vista™ SP1、全エディション、32 ビットおよび 64 ビット（実稼働環境以外の場合のみ）	Microsoft.com の「Windows Vi ta Security Guide」を検索してください。
Red Hat® Linux® AP または ES	Red Hat Enterprise Linux Security Guide
Sun Solaris 10	System Administration Guide: Security Services

2.1.1.2 アプリケーションサーバーのセキュリティ情報

アプリケーションサーバーを保護する際には、サーバーのベンダーが挙げている対策を実装することを慎重に検討してください。この対策には、以下のものがあります。

- 管理者ユーザー名として推測しにくい名前を使用する
- 不要なサービスを無効にする
- コンソールマネージャーを保護する
- cookie の保護を有効にする
- 不要なポートを閉じる
- IP アドレスまたはドメインでクライアントを制限する
- Java™ Security Manager を使用して、プログラムによって権限を制限する

JEE 上の AEM forms がサポートするアプリケーションサーバーのセキュリティ情報については、次の表の資料を参照してください。

アプリケーションサーバー	セキュリティ情報
Oracle WebLogic®	http://download.oracle.com/docs/ の「Understanding WebLogic Security」を検索してください。
IBM WebSphere®	Securing applications and their environment
Red Hat® JBoss®	Security on JBoss

2.1.1.3 データベースのセキュリティ情報

データベースを保護する際には、データベースのベンダーが挙げている対策を実装することを慎重に検討してください。この対策には、以下のものがあります。

- アクセス制御リスト（ACL）を使用して操作を制限する
- 非標準ポートを使用する
- ファイアウォールの内側にデータベースを隠す
- 機密データをデータベースに書き込む前に暗号化する（データベース製造元のドキュメントを参照）

JEE 上の AEM forms がサポートするデータベースのセキュリティ情報については、次の表の資料を参照してください。

データベース	セキュリティ情報
IBM DB2® 9.1 または 9.5	DB2 Product Family Library
Microsoft SQL Server 2005 SP2 または 2008	「SQL Server 2005: Security」について Web を検索してください 「SQL Server 2008: Security」について Web を検索してください
MySQL 5	MySQL 5.0 General Security Issues MySQL 5.1 General Security Issues
Oracle® 10g または 11g	Oracle 11g documentation の「Security」の章を参照してください。

次の表では、JEE 上の AEM forms の設定プロセス中に開く必要のあるデフォルトポートについて説明します。https 経由で接続している場合、ポート情報と IP アドレス情報を適宜修正する必要があります。ポートの設定について詳しくは、使用しているアプリケーションサーバー版の『**JEE 上の AEM forms のインストールおよびデプロイ**』ドキュメントを参照してください。

製品またはサービス	ポート番号
JBoss	8080
WebLogic	7001
WebLogic 管理対象サーバー	設定時に管理者によって指定される
WebSphere	9060（Global Security が有効になっている場合、デフォルト SSL ポート値は 9043） 9080
BAM サーバー	7001
SOAP[SOAP]	8880
MySQL	3306
Oracle	1521
DB2	50000
SQL Server	1433
LDAP	LDAP サーバーを実行しているポート。デフォルトのポートは通常 389 です。ただし、SSL オプションを選択する場合、デフォルトのポートは通常 636 です。どのポートを指定するかは、LDAP の管理者に確認してください。

2.1.1.4 デフォルト以外の HTTP ポートを使用するための JBoss の設定

JBoss Application Server は、デフォルトの HTTP ポートとして 8080 を使用します。また、JBoss には事前設定のポート 8180、8280 および 8380 があり、これらは jboss-service.xml ファイルでコメントアウトされています。既にこのポートを使用しているアプリケーションがコンピューター上にある場合は、以下の手順に従って JEE 上の AEM forms で使用するポートを変更してください。

1 jboss-service.xml ファイルをエディターで開きます。

JBoss 自動インストール：**[JBoss root]**/server/lc_turnkey/conf/

JBoss 手動インストール：**[appserver root]**/server/all/conf/

2 次の mbean を見つけてコメントを解除します。

<mbean code="org.jboss.services.binding.ServiceBindingManager"

name="jboss.system:service=ServiceBindingManager">

<attribute name="**ServerName**">ports-01</attribute>

<attribute name="**StoreURL**">${jboss.home.url}/docs/examples/binding-manager/sample-bindings.xml</attribute>

<attribute name="StoreFactoryClassName">

org.jboss.services.binding.XMLServicesStoreFactory

</ 属性 >

</mbean>

3 ファイルを保存して閉じます。

4 JBoss を再起動します。

これで、JBoss はポート 8180 を使用するように設定されました。8280 または 8380 を使用する必要がある場合は、次のいずれかの代替ポートを使用するように ServerName 属性値を変更します。

- 8280 の場合：ports-02

- 8380 の場合：ports-03

JBoss に事前設定されたポート番号以外のポート番号を設定する必要がある場合は、次の手順を実行してください。

1 **[JBoss root]**（自動インストール）または **[appserver root]**（JBoss 手動インストール）の deploy/jboss-web.deployer ファイルを見つけて開きます。

2 上の手順 2 に従って、mbean を見つけてコメントを解除します。

3 ServerName 値を使用するポート番号に変更します。

4 ファイルを保存して閉じます。

5 JBoss を再起動します。

2.1.2 JEE 上の AEM forms セキュリティに関する考慮事項

ここでは、理解しておく必要のある JEE 上の AEM forms 固有のセキュリティの問題について説明します。

2.1.2.1 データベース内の電子メールの資格情報は暗号化されない

アプリケーションに保存されている電子メールの資格情報は、JEE 上の AEM forms データベースに保存される前に暗号化されません。サービスのエンドポイントで電子メールを使用するように設定した場合、エンドポイント設定の一部として使用したパスワード情報は、データベースに保存される前に暗号化されません。

2.1.2.2 データベース内の Rights Management に関する機密性情報

JEE 上の AEM forms は、JEE 上の AEM forms データベースに、ポリシードキュメントで使用した暗号化マテリアルと機密ドキュメントキー情報を保存します。データベースへの侵入を防御することで、このような機密性の高い情報を保護することができます。

2.1.2.3 adobe-ds.xml 内のクリアテキスト形式のパスワード

JEE 上の AEM forms を実行するアプリケーションサーバーでは、そのサーバー上に設定されたデータソースを介してデータベースにアクセスするように設定する必要があります。アプリケーションサーバーが、データベースのパスワードをクリアテキストでデータソース設定ファイルに公開しないことを確認してください。

adobe-ds.xml ファイルには、パスワードがクリアテキスト形式で格納されています。アプリケーションサーバーのパスワードを暗号化する方法については、アプリケーションサーバーのベンダーにお問い合わせください。例えば、JBoss® については、「Encrypting DataSource Passwords」を参照します。

注意：JEE 上の AEM forms JBoss 自動インストーラーがデータベースのパスワードを暗号化します。

IBM WebSphere Application Server および Oracle WebLogic Server は、デフォルトでデータソースのパスワードを暗号化している可能性があります。ただし、これらのサーバーを使用している場合でも、アプリケーションサーバーのドキュメントで、暗号化が行われているかどうかを必ず確認してください。

2.1.2.4 Trust Store に保管された秘密鍵の保護

Trust Store からインポートされた秘密鍵や秘密鍵証明書は、JEE 上の AEM forms データベースに保管されます。データベースを保護し、アクセスを指名された管理者のみに制限するため、適切な注意を払う必要があります。

第 3 章：JEE 上の AEM forms 環境の堅牢化

3.1 JEE 上の AEM forms 環境の堅牢化

この記事では、JEE 上の AEM forms を実行するサーバーを保護するための推奨事項とベストプラクティスについて説明します。ここでは、オペレーティングシステムとアプリケーションサーバーのホストの堅牢化について包括的な説明はしません。企業のイントラネット内で運用している JEE 上の AEM forms のセキュリティを強化するために行うことが望ましい、様々なセキュリティ堅牢化設定について説明します。なお、JEE 上の AEM forms アプリケーションサーバーのセキュリティを確実に保つには、これだけでなく、セキュリティの監視、検出および応答の方策を実装することも必要です。

この記事では、インストールと設定の作業において、次の各段階で適用する堅牢化手法について説明します。

- **インストール前：**この手法は、JEE 上の AEM forms をインストールする前に実行します。
- **インストール時：**この手法は、JEE 上の AEM forms ソフトウェアをインストールする作業の一環として実行します。
- **インストール後：**この手法は、インストール終了後と、それ以降の定期的な管理作業として実行します。

JEE 上の AEM forms は詳細なカスタマイズが可能で、様々な環境で動作します。推奨事項には、一部の組織のニーズに合わないものも含まれている可能性があります。

3.1.1 インストール前

JEE 上の AEM forms をインストールする前には、ネットワーク層とオペレーティングシステムに対してセキュリティソリューションを適用することができます。ここでは、いくつかの問題と、この領域におけるセキュリティの脆弱性を減らすための推奨事項について説明します。

UNIX および Linux へのインストールと設定

JEE 上の AEM forms のインストール作業や設定作業を実行するときは、ルートシェルを使用しないでください。デフォルトでは、ファイルは /opt ディレクトリの下にインストールされるので、インストールを実行するユーザーには /opt 以下のすべてのファイルの権限が必要です。または、各ユーザーには /user ディレクトリに対するすべてのファイル権限があらかじめ付与されているので、/user ディレクトリにインストールを実行することもできます。

Windows へのインストールと設定

自動オプションインストールを使用して JBoss に JEE 上の AEM forms をインストールする場合、または PDF Generator をインストールする場合、Windows へのインストールは管理者として実行する必要があります。また、PDF Generator をネイティブアプリケーションサポートと共に Windows にインストールする場合は、Microsoft Office をインストールしたのと同じ Windows ユーザーとしてインストールを実行する必要があります。インストールの権限について詳しくは、使用しているアプリケーションサーバー版の『**JEE** 上の **AEM forms** のインストールおよびデプロイ』ドキュメントを参照してください。

3.1.1.1 ネットワーク層のセキュリティ

ネットワークセキュリティの脆弱性は、インターネットまたはイントラネットに接続しているすべてのアプリケーションサーバーにとって、最も重大な脅威の 1 つです。ここでは、このような脆弱性に対してネットワーク上のホストを堅牢化する手順について説明します。具体的には、ネットワークのセグメント化、TCP/IP（Transmission Control Protocol/Internet Protocol）スタックの堅牢化、ホスト保護のためのファイアウォールの使用などの手順を取り上げます。

次の表では、ネットワークセキュリティの脆弱性を減らすための一般的なプロセスについて説明します。

問題	説明
非武装地帯（DMZ）	forms サーバーを非武装地帯（DMZ）にデプロイします。ファイアウォールの内側に配置された、JEE 上の AEM forms を実行するアプリケーションサーバーに対して、少なくとも 2 つのレベルでセグメント化が必要です。Web サーバーを含む DMZ から外部ネットワークを分離します。同様に、外部ネットワークは内部ネットワークからも分離している必要があります。ファイアウォールを使用して、この分離した層を実装します。必要最小限のデータのみが許可されるように、各ネットワーク層を通過するトラフィックを分類して制御します。
プライベート IP アドレス	AEM forms アプリケーションサーバーで、RFC 1918 プライベート IP アドレスと NAT（ネットワークアドレス変換）を使用します。プライベート IP アドレス（10.0.0.0/8、172.16.0.0/12 および 192.168.0.0/16）を割り当てることにより、インターネットを通じて、NAT を使用する内部ホストに対して攻撃者がトラフィックをルーティングできないようにします。
ファイアウォール	次の基準を使用して、ファイアウォールソリューションを選択します。 • 単純なパケットフィルタリングソリューションではなく、プロキシサーバーまたは「ステートフルインスペクション」をサポートするファイアウォールを実装する。 • 「明示的に許可されたサービス以外はすべて拒否する」セキュリティパラダイムをサポートするファイアウォールを使用する。 • デュアルホームまたはマルチホームのファイアウォールソリューションを実装する。このアーキテクチャによって、最も高いセキュリティレベルが実現し、権限のないユーザーがファイアウォールセキュリティを迂回できないようにすることができます。
データベースポート	データベースのデフォルトのリスニングポート（MySQL - 3306、Oracle - 1521、MS SQL - 1433）は、使用しないでください。データベースポートの変更について詳しくは、データベースのドキュメントを参照してください。 データベースポートを変更すると、JEE 上の AEM forms の設定全体に影響します。デフォルトポートを変更した場合、JEE 上の AEM forms のデータソースなど、設定の別の領域を変更内容に合わせて修正する必要があります。 JEE 上の AEM forms におけるデータソースの設定について詳しくは、使用しているアプリケーションサーバー製品に応じて、『AEM forms ドキュメントセット』にある、該当する『**JEE** 上の **AEM forms** インストールおよびデプロイ』または『**JEE** 上の **AEM forms** へのアップグレード』を参照してください。

3.1.1.2 オペレーティングシステムのセキュリティ

次の表では、オペレーティングシステムに存在するセキュリティの脆弱性を最小にするために役立つ方法について説明します。

問題	説明
セキュリティパッチ	ベンダーのセキュリティパッチとアップデートが迅速に適用されない場合、権限のないユーザーがアプリケーションサーバーにアクセスするリスクが高まります。実稼働サーバーにセキュリティパッチを適用する場合は、適用する前にテストしてください。 さらに、パッチを定期的にチェックしてインストールするためのポリシーとプロシージャを作成してください。
ウイルス対策ソフトウェア	ウイルススキャンプログラムは、署名をスキャンするか、異常な動作を監視することによって、感染ファイルを識別します。スキャンプログラムでは、ウイルスの署名をファイルに保管します。通常、このファイルはローカルハードドライブに格納されます。新しいウイルスは次から次へと出現するので、ウイルススキャンプログラムですべての最新のウイルスを識別できるように、このファイルを頻繁に更新する必要があります。
ネットワークタイムプロトコル（NTP）	フォレンジック分析のために、forms サーバーの時計は常に正確に設定されている必要があります。NTP を使用して、インターネットに直接接続しているすべてのシステムの時間を同期させてください。

オペレーティングシステムのその他のセキュリティ情報については、「2 ページの「2.1.1.1 オペレーティングシステムのセキュリティ情報」」を参照してください。

3.1.2 インストール

ここでは、AEM forms インストールプロセスで、セキュリティの脆弱性を減らすために使用できる方法について説明します。これらの方法では、状況によってはインストールプロセスのオプションを使用します。次の表では、各方法について解説します。

問題	説明
権限	ソフトウェアのインストールには、必要最小限の権限を使用してください。Administrators グループに属していないアカウントでコンピューターにログインします。Windows では、runas コマンドを使用して、管理者ユーザーとして JEE 上の AEM forms インストーラーを実行することができます。UNIX および Linux システムでは、sudo などのコマンドを使用してソフトウェアをインストールします。
ソフトウェアソース	信頼できないソースから JEE 上の AEM forms をダウンロードまたは実行しないでください。 悪意のあるプログラムには、データの盗難、改変、削除、サービス拒否などの様々な手段でセキュリティを侵害するコードが含まれています。必ず、Adobe DVD または信頼できるソースから入手した JEE 上の AEM forms をインストールしてください。
ディスクのパーティション	JEE 上の AEM forms は、専用のディスクパーティションに配置してください。ディスクのセグメント化とは、セキュリティを強化するために、サーバー上の特定のデータを個別の物理ディスクに保管するプロセスのことです。この方法でデータを整理すると、ディレクトリトラバーサル攻撃のリスクを軽減することができます。システムパーティションとは別に、JEE 上の AEM forms コンテンツディレクトリをインストールするパーティションを作成することを検討してください（Windows のシステムパーティションには system32 ディレクトリまたはブートパーティションが含まれています）。
コンポーネント	既存のサービスを評価し、不要なサービスを無効化またはアンインストールしてください。不要なコンポーネントやサービスをインストールしないでください。 アプリケーションサーバーのデフォルトインストールには、サーバーの用途によっては必要のないサービスが含まれている可能性があります。攻撃のエントリポイントを最小限に抑えるために、デプロイメントに先立って、不要なサービスをすべて無効にする必要があります。例えば、JBoss では、META-INF/jboss-service.xml 記述子ファイル内の不要なサービスをコメントアウトします。
クロスドメインポリシーファイル	サーバー上に crossdomain.xml ファイルが存在すると、そのサーバーを直ちに弱化させる可能性があります。ドメインのリストに可能な限り制限をかけることをお勧めします。ガイド（非推奨）を使用する場合、開発環境から実稼働環境への移行中に使用される crossdomain.xml ファイルを配置しないでください。Web サービスで使用されるガイドの場合、ガイドを提供するサーバーと同じサーバー上にそのサービスがあれば、crossdomain.xml ファイルはまったく必要ありません。しかし、サービスが別のサーバー上にある場合や、クラスターが関係している場合は、crossdomain.xml ファイルが存在している必要があります。crossdomain.xml ファイルについて詳しくは、http://kb2.adobe.com/cps/142/tn_14213.html を参照してください。
オペレーティングシステムのセキュリティ設定	Solaris プラットフォームで 192 ビットまたは 256 ビット XML 暗号化を使用する必要がある場合、pkcs11_softtoken.so ではなく、必ず pkcs11_softtoken_extra.so をインストールします。

3.1.3 インストール後の手順

JEE 上の AEM forms のインストールが完了したら、セキュリティ上の観点から、定期的に環境の保守を行うことが重要です。

次の節では、デプロイ済みの forms サーバーを保護するための、各種の推奨タスクについて詳細に説明します。

3.1.3.1 AEM forms セキュリティ

次の推奨設定は、管理 Web アプリケーションの外にある JEE 上の AEM forms サーバーに適用されます。サーバーのセキュリティリスクを軽減するには、この設定を JEE 上の AEM forms のインストール直後に適用してください。

セキュリティパッチ

ベンダーのセキュリティパッチとアップデートが迅速に適用されない場合、権限のないユーザーがアプリケーションサーバーにアクセスするリスクが高まります。実稼働サーバーにセキュリティパッチを適用する場合は、事前にテストを実施し、アプリケーションの互換性と可用性を確認した上で適用してください。また、パッチのチェックとインストールを定期的に行うためのポリシーと手続きを定めてください。JEE 上の AEM forms のアップデートは Enterprise 製品のダウンロードサイトにあります。

サービスアカウント（Windows への JBoss 自動インストールのみ）

JEE 上の AEM forms は、デフォルトでは、LocalSystem アカウントを使用してサービスをインストールします。組み込み LocalSystem ユーザーアカウントは、高いレベルのアクセス権限を付与されており、Administrators グループに属しています。ワーカープロセス ID を LocalSystem ユーザーアカウントで実行した場合、そのワーカープロセスはシステム全体に対してフルアクセス権限を持ちます。

JEE 上の AEM forms のデプロイ先のアプリケーションサーバーを実行するには、次の手順に従って、管理者以外の固有のアカウントを使用してください。

1. Microsoft 管理コンソール（MMC）で、forms サーバーサービスへのログインに使用するローカルユーザーを作成します。
   - 「**ユーザーはパスワードを変更できない**」オプションを選択します。
   - 「**所属するグループ**」タブに、「**ユーザー**」グループが表示されていることを確認してください。

   注意：PDF Generator 用のこの設定は変更できません。
2. **スタート／設定／管理ツール／サービス**を選択します。
3. JEE 上の AEM forms 向けの JBoss をダブルクリックして、サービスを停止します。
4. 「**ログオン**」タブで、「**アカウント**」を選択し、作成したユーザーアカウントを参照して、アカウントのパスワードを入力します。
5. MMC で、「**ローカルセキュリティ設定**」を開き、**ローカルポリシー／ユーザー権利の割り当て**を選択します。
6. forms サーバーを実行しているユーザーアカウントに、次の権限を割り当てます。
   - ターミナルサービスを使ったログオンを拒否する
   - ローカルでログオンを拒否する
   - サービスとしてログオン（通常は既に設定済み）
7. 新しく作成したユーザーアカウントに、JEE 上の AEM forms Web コンテンツディレクトリの項目に対する「読み取りと実行」、「フォルダーの内容の一覧表示」、「読み取り」の各権限を付与します。
8. アプリケーションサーバーを起動します。

Configuration Manager ブートストラップサーブレットの無効化

Configuration Manager は、アプリケーションサーバーにデプロイ済みのサーブレットを利用して、JEE 上の AEM forms データベースのブートストラップを実行します。Configuration Manager は、設定が完了する前にこのサーブレットにアクセスするので、承認済みユーザーのみにアクセスを限定するセキュリティは施されていません。Configuration Manager を使用して JEE 上の AEM forms の設定を完了した後は、このサーブレットを無効にしてください。

1. adobe-livecycle-[appserver].ear ファイルを解凍します。
2. META-INF/application.xml ファイルを開きます。

3 adobe-bootstrapper.war セクションを検索します。

```
<!-- bootstrapper start -->
<module id="WebApp_adobe_bootstrapper">
    <web>
        <web-uri>adobe-bootstrapper.war</web-uri>
        <context-root>/adobe-bootstrapper</context-root>
    </web>
</module>
<module id="WebApp_adobe_lcm_bootstrapper_redirector">
    <web>
        <web-uri>adobe-lcm-bootstrapper-redirector.war</web-uri>
        <context-root>/adobe-lcm-bootstrapper</context-root>
    </web>
</module>
<!-- bootstrapper end-->
```

4 adobe-bootstrapper.war および adobe-lcm-bootstrapper-redirectory. war モジュールを次のようにコメントアウトします。

```
<!-- bootstrapper start -->
<!--
<module id="WebApp_adobe_bootstrapper">
    <web>
        <web-uri>adobe-bootstrapper.war</web-uri>
        <context-root>/adobe-bootstrapper</context-root>
    </web>
</module>
<module id="WebApp_adobe_lcm_bootstrapper_redirector">
    <web>
        <web-uri>adobe-lcm-bootstrapper-redirector.war</web-uri>
        <context-root>/adobe-lcm-bootstrapper</context-root>
    </web>
</module>
-->
<!-- bootstrapper end-->
```

5 META-INF/application.xml ファイルを保存して閉じます。

6 EAR ファイルの zip ファイルを作成し、アプリケーションサーバーに再デプロイします。

7 URL をブラウザーに入力して変更をテストし、URL が機能しないことを確認します。

Trust Store へのリモートアクセスのロックダウン

Configuration Manager を使用して、Acrobat Reader DC Extensions 10 の資格情報を JEE 上の AEM forms Trust Store にアップロードできます。つまり、リモートプロトコル（SOAP および EJB）経由の Trust Store 資格情報サービスへのアクセスは、デフォルトで有効になっています。このアクセスは、Configuration Manager を使用して使用権限資格情報のアップロードを完了した後、またはそれ以降の資格情報の管理を管理コンソールを使用して行う場合は、必要なくなります。

30 ページの「4.1.1 サービスへの不要なリモートアクセスの無効化」の手順に従って、Trust Store の全サービスへのリモートアクセスを無効にすることができます。

すべての不要な匿名アクセスの無効化

一部の forms サーバーサービスには、匿名の呼び出しによって実行される操作があります。このようなサービスへの匿名アクセスが必要ない場合は、31 ページの「4.1.2 サービスへの不要な匿名アクセスの無効化」の手順に従って、アクセスを無効にしてください。

3.1.3.1.1 デフォルトの管理者パスワードの変更

JEE 上の AEM forms をインストールすると、上級管理者ユーザーまたはログイン ID 管理者ユーザーのために、デフォルトパスワードが「**password**」であるデフォルトユーザーアカウントが 1 つ設定されます。このパスワードは、Configuration Manager を使用して直ちに変更してください。

1 Web ブラウザーに次の URL を入力します。

`http://[host name]:[port]/adminui`

デフォルトのポート番号は次のいずれかです。

JBoss：8080

WebLogic Server：7001

WebSphere：9080

2 「**ユーザー名**」フィールドに administrator と入力し、「**パスワード**」フィールドに password と入力します。

3 **設定**／**User Management** ／**ユーザーとグループ**をクリックします。

4 「**検索**」フィールドに administrator と入力し、「**検索**」をクリックします。

5 ユーザーの一覧で「**上級管理者**」をクリックします。

6 ユーザーを編集ページで「**パスワードの変更**」をクリックします。

7 新しいパスワードを指定し、「**保存**」をクリックします。

次の手順を実行することで CRX 管理者のデフォルトパスワードの変更もお勧めします。

1 デフォルトのユーザー名／パスワードを使用して、http://[ホスト名]:[ポート]/lc/libs/granite/security/content/admin.html にログインします。

2 検索フィールドに「管理者」と入力し、「**移動**」をクリックします。

3 検索結果から「**管理者**」を選択し、ユーザーインターフェイスの右下で「**編集**」アイコンをクリックします。

4 「**新しいパスワード**」フィールドに新しいパスワードを、「**パスワード**」フィールドに古いパスワードを指定します。

5 ユーザーインターフェイスの右下で「保存」アイコンをクリックします。

3.1.3.1.2 WSDL の生成の無効化

Web Service Definition Language（WSDL）の生成は、開発者が WSDL の生成を使用してクライアントアプリケーションを構築する開発環境でのみ有効にしてください。実稼働環境では WSDL の生成を無効化して、サービスの内部詳細が公開されないようにすることができます。

1 Web ブラウザーに次の URL を入力します。

`http://[host name]:[port]/adminui`

2 **設定**／**コアシステム設定**／**設定**をクリックします。

3 「**WSDL を有効にする**」のチェックを外して「**OK**」をクリックします。

3.1.3.2 アプリケーションサーバーのセキュリティ

次の表では、JEE 上の AEM forms アプリケーションのインストール後に、アプリケーションサーバーを保護するために使用するいくつかの方法について説明します。

問題	説明
アプリケーションサーバーの管理コンソール	アプリケーションサーバーで JEE 上の AEM forms のインストール、設定およびデプロイを完了したら、アプリケーションサーバーの管理コンソールへのアクセスを無効にする必要があります。詳しくは、アプリケーションサーバーのドキュメントを参照してください。
アプリケーションサーバーの cookie の設定	アプリケーションの cookie は、アプリケーションサーバーが管理しています。アプリケーションをデプロイするときに、アプリケーションサーバーの管理者は cookie の環境設定をサーバー全体に対してまたは個別のアプリケーションに対して指定することができます。デフォルトでは、サーバーの設定が優先します。 アプリケーションサーバーで生成されるすべてのセッション cookie に HttpOnly 属性が含まれている必要があります。例えば、JBoss アプリケーションサーバーを使用する場合、deploy/jbossweb.sar/context.xml ファイルで、SessionCookie 要素を httpOnly="true" に修正することができます。 cookie の送信には HTTPS のみを使用するように制限することもできます。このように設定すると、cookie が HTTP を経由して暗号化されずに送信されることはありません。アプリケーションサーバーの管理者は、サーバーの cookie 保護をグローバルに有効化する必要があります。例えば、JBoss アプリケーションサーバーを使用する場合、server.xml ファイルで、secure=true へのコネクタ要素を修正することができます。 cookie の設定について詳しくは、アプリケーションサーバーのドキュメントを参照してください。
ディレクトリの参照	存在しないページに対する要求、またはディレクトリ名に対する要求（最後がスラッシュ（/）で終わる要求文字列）が行われた場合、アプリケーションサーバーによってディレクトリの内容が返されないようにする必要があります。これが行われないようにするには、アプリケーションサーバーのディレクトリ参照を無効にします。管理コンソールアプリケーションおよびサーバーで実行している他のアプリケーションについても、ディレクトリ参照を無効にしてください。 JBoss の場合、web.xml ファイルの DefaultServlet プロパティの初期化パラメーターの listings 値を false に設定します。次に例を示します。 <servlet> <servlet-name>default</servlet-name> <servlet-class> org.apache.catalina.servlets.DefaultServlet </servlet-class> <init-param> <param-name>listings</param-name> <param-value>false</param-value> </init-param> <load-on-startup>1</load-on-startup> </servlet> WebSphere の場合、ibm-web-ext.xmi ファイルの directoryBrowsingEnabled プロパティを false に設定します。 WebLogic の場合、weblogic.xml ファイルの index-directories プロパティを false に設定します。次に例を示します。 <container-descriptor> <index-directory-enabled>false </index-directory-enabled> </container-descriptor>

3.1.3.3 JBoss での JMX コンソールの使用

Java Management Extensions（JMX）コンソールが JBoss と共にインストールされている場合、システムの機密性の高い情報を漏洩するおそれのある XSS（クロスサイトスクリプティング）として URL が構築される可能性があります。

自動オプションを使用して JEE 上の AEM forms をインストールし、自動インストールに含まれる JBoss を使用する場合、セキュリティリスクを最小限に抑えるために、JBoss JMX コンソールはデフォルトで削除されます。しかし、JBoss JMX コンソールを使用する必要がある場合は、次の手順に従って再インストールしてください。

1. JBoss.org から、JBoss 4.2.0（またはそれ以降）をダウンロードします。
2. JBoss アプリケーションサーバーを停止します。
3. ダウンロードしたアーカイブ zip ファイルから **[JBossroot]**/deploy/jmx-console.war/ 以下のファイルを抽出します。
4. jmx-console.war/... ファイルを JBoss のインストールディレクトリのデプロイディレクトリに置きます。
5. JBoss を再起動します。
6. 次の URL に移動し、JBoss JMX コンソールが利用可能であることを確認します。

   http://localhost:8080/jmx-console

3.1.3.4 データベースのセキュリティ

データベースの保護を行う場合、データベースのベンダーが挙げている対策を実装することを慎重に検討してください。データベースのユーザーには、JEE 上の AEM forms でデータベースを使用するために必要な最小限の権限を付与するようにします。例えば、データベースの管理権限を持つアカウントは使用しないでください。

Oracle では、データベースアカウントで使用する必要がある権限は、CONNECT、RESOURCE および CREATE VIEW だけです。他のデータベースについての同様の要件については、『JEE 上の AEM forms のインストールの準備（シングルサーバー）』を参照してください。

3.1.3.4.1 Windows 上での統合セキュリティの設定（JBoss 版）

1. **[JBOSS_HOME]**¥server¥all¥deploy¥adobe-ds.xml を修正し、接続先 URL に integratedSecurity=true を追加します。次に例を示します。

   ```
   jdbc:sqlserver://<serverhost>:<port>;databaseName=<dbname>;integratedSecurity=true
   ```

2. アプリケーションサーバーを実行しているコンピューターの Windows システムパスに sqljdbc_auth.dll ファイルを追加します。sqljdbc_auth.dll ファイルは、Microsoft SQL JDBC 1.2 ドライバーのインストール先ディレクトリ（デフォルトでは **[InstallDir]**¥sqljdbc_1.2¥enu¥auth¥x86）にあります。
3. JBoss Windows サービス（JBoss for JEE 上の AEM forms）のログオンプロパティを、ローカルシステムから、JEE 上の AEM forms データベースと最低限の権限を持つログインアカウントに変更します。Windows サービスとしてではなく、コマンドラインから JBoss を実行している場合、この手順を行う必要はありません。
4. SQL Server のセキュリティを「**混合**」モードから「**Windows 認証のみ**」に変更します。

3.1.3.4.2 Windows 上での統合セキュリティの設定（WebLogic 版）

1. Web ブラウザーの URL 行に次の URL を入力して、WebLogic Server 管理コンソールを起動します。

   ```
   http://[host name]:7001/console
   ```

2. Change Center で、「**Lock & Edit**」をクリックします。
3. 「Domain Structure」で、[base_domain] ／ **Services** ／ **JDBC** ／ **Data Sources** をクリックし、右側のウィンドウの「**IDP_DS**」をクリックします。
4. 次の画面の「**Configuration**」タブで「**Connection Pool**」タブをクリックし、「**Properties**」ボックスに integratedSecurity=true と入力します。

5 「Domain Structure」で、**[base_domain]** ／ **Services** ／ **JDBC** ／ **Data Sources** をクリックし、右側のウィンドウの「**RM_DS**」をクリックします。

6 次の画面の「**Configuration**」タブで「**Connection Pool**」タブをクリックし、「**Properties**」ボックスに integratedSecurity=true と入力します。

7 アプリケーションサーバーを実行しているコンピューターの Windows システムパスに sqljdbc_auth.dll ファイルを追加します。sqljdbc_auth.dll ファイルは、Microsoft SQL JDBC 1.2 ドライバーのインストール先ディレクトリ（デフォルトでは **[InstallDir]**¥sqljdbc_1.2¥enu¥auth¥x86）にあります。

8 SQL Server のセキュリティを「**混合**」モードから「**Windows 認証のみ**」に変更します。

3.1.3.4.3 Windows 上での統合セキュリティの設定（WebSphere 版）

WebSphere では、統合セキュリティを設定できるのは外部の SQL Server JDBC ドライバーを使用している場合のみです。WebSphere の埋め込みの SQL Server JDBC ドライバーを使用している場合は設定できません。

1 WebSphere Administrative Console にログインします。

2 ナビゲーションツリーで、**Resources** ／ **JDBC** ／ **Data Sources** をクリックし、右側のウィンドウで「**IDP_DS**」をクリックします。

3 右側のウィンドウの「Additional Properties」で「**Custom Properties**」をクリックし、「**New**」をクリックします。

4 「**Name**」ボックスに integratedSecurity と入力し、「**Value**」ボックスに true と入力します。

5 ナビゲーションツリーで、**Resources** ／ **JDBC** ／ **Data Sources** をクリックし、右側のウィンドウで「**RM_DS**」をクリックします。

6 右側のウィンドウの「Additional Properties」で「**Custom Properties**」をクリックし、「**New**」をクリックします。

7 「**Name**」ボックスに integratedSecurity と入力し、「**Value**」ボックスに true と入力します。

8 WebSphere がインストールされているコンピューター上で、Windows システムパス（C:¥Windows）に sqljdbc_auth.dll ファイルを追加します。sqljdbc_auth.dll ファイルは、Microsoft SQL JDBC 1.2 ドライバーのインストール先ディレクトリ（デフォルトは **[InstallDir]**¥sqljdbc_1.2¥enu¥auth¥x86）と同じ場所にあります。

9 **スタート／コントロールパネル／サービス**を選択し、WebSphere の Windows サービス（IBM WebSphere Application Server <version> - <node>）を右クリックして、「**プロパティ**」を選択します。

10 プロパティダイアログボックスで、「**ログオン**」タブをクリックします。

11 「**アカウント**」を選択し、必要な情報を入力して、使用するログインアカウントを設定します。

12 SQL Server のセキュリティを「**混合**」モードから「**Windows 認証のみ**」に変更します。

3.1.3.5 データベース内の機密性の高い情報の保護

AEM forms データベーススキーマには、システム設定やビジネスプロセスに関する機密性の高い情報が含まれているので、ファイアウォールの内側に隠しておく必要があります。データベースは、forms サーバーと同じ信頼境界内にあると見なされる必要があります。情報の意図しない開示やビジネスデータの盗難を防ぐために、データベース管理者（DBA）は、権限のある管理者のみにアクセスを制限するようにデータベースを設定する必要があります。

追加の予防策として、データベースベンダー固有のツールを使用して、次のデータを含むテーブルの列を暗号化することを考慮してください。

- Rights Management ドキュメントキー
- Trust Store HSM PIN 暗号化キー
- ローカルユーザーパスワードハッシュ

ベンダー固有のツールについて詳しくは、「3 ページの「2.1.1.3 データベースのセキュリティ情報」」を参照してください。

3.1.3.6 LDAP のセキュリティ

LDAP（Lightweight Directory Access Protocol）ディレクトリは、通常、エンタープライズユーザーおよびグループ情報のソースとして、またパスワード認証実行の手段として JEE 上の AEM forms で使用されます。LDAP ディレクトリが SSL（Secure Socket Layer）を使用するように設定されていること、および JEE 上の AEM forms が SSL ポートを使用して LDAP ディレクトリにアクセスするように設定されていることを確認してください。

3.1.3.6.1 LDAP のサービス拒否

LDAP を使用した最もよく行われる攻撃は、攻撃者が大量の認証エラーを故意に引き起こすというものです。この攻撃を受けると、LDAP ディレクトリサーバーは、すべての LDAP 依存のサービスからユーザーをロックアウトしなければならなくなります。

試行できる認証エラーの回数と、それに伴うロックアウト時間の値を設定すると、AEM forms への認証でユーザーが繰り返しエラーになったときに、AEM forms がロックアウトを実行します。管理コンソールでは、小さい値を選択します。認証エラーの許容回数を選択するときは、許容回数に達した後に、LDAP ディレクトリサーバーより前に AEM forms がユーザーをロックアウトすることを理解することが重要です。

3.1.3.6.2 自動アカウントロックの設定

1. 管理コンソールにログインします。
2. **設定**／**ユーザー管理**／**ドメイン管理**をクリックします。
3. 「自動アカウントロックの設定」で、「**連続する認証エラーの最大回数**」を 3 などの小さい値に設定します。
4. 「**保存**」をクリックします。

3.1.3.7 監査とログ

アプリケーションの監査およびログ機能を適切に保護した状態で使用することで、セキュリティを確保し、他の異常なイベントを追跡して、それらのイベントを可能な限り迅速に検出することができます。アプリケーション内における監査とログの効果的な使用には、成功したログインと失敗したログインの追跡、キーレコードの作成と削除などのキーアプリケーションイベントの追跡などが挙げられます。

監査を使用して、各種の攻撃を検出することができます。具体的には、以下のものがあります。

- ブルートフォースパスワードアタック
- サービス拒否攻撃
- 敵意のある入力値と関連するクラスのスクリプト挿入攻撃

次の表では、サーバーの脆弱性を減らすために使用できる監査およびログの方法について説明します。

問題	説明
ログファイル ACL	JEE 上の AEM forms ログファイルには、適切なアクセス制御リスト（ACL）を設定します。 適切な資格情報を設定することで、攻撃者によってファイルが削除されないように防御します。 ログファイルディレクトリのセキュリティ権限として、Administrators グループおよび SYSTEM グループのフルコントロール権限が必要です。AEM forms ユーザーアカウントには、読み取りおよび書き込み権限のみが必要です。
ログファイルの冗長性	リソースに余裕があれば、攻撃者がアクセスできないように、Syslog、Tivoli、Microsoft Operations Manager（MOM）やその他のメカニズムを使用して、ログを別のサーバーにリアルタイムで送信してください。 この方法でログを保護することで、改ざんを防ぐことができます。さらに、中央リポジトリにログを保管することで、対比と監視に役立ちます（例えば、複数の forms サーバーを使用している場合に、パスワードの照会先となる複数のコンピューターに対してパスワード推測攻撃が行われた場合など）。

3.1.3.8 JEE 上の AEM forms Unix システムライブラリの依存関係

UNIX 環境での JEE 上の AEM forms デプロイメントを計画する際には、次の情報を参考にしてください。

3.1.3.8.1 Convert PDF サービス

AEM forms に含まれる Convert PDF サービスには、次の最小システムライブラリが必要です。

Linux

```
/lib/
    libdl.so.2 (0x00964000)
    ld-linux.so.2 (0x007f6000)
/lib/tls/
    libc.so.6 (0x00813000)
    libm.so.6 (0x0093f000)
    libpthread.so.0 (0x00a5d000)
/usr/lib/libz.so.1 (0x0096a000)
/gcc410/lib/
    libgcc_s.so.1 (0x00fc0000)
    libstdc++.so.6 (0x00111000)
```

Solaris

```
/usr/platform/SUNW,Sun-Fire-V210/lib/libc_psr.so.1
/usr/lib/
    libc.so.1
    libdl.so.1
    libintl.so.1
    libm.so.1
    libmp.so.2
    libnsl.so.1
    libpthread.so.1
    libsocket.so.1
    libstdc++.so.6
    libthread.so.1
```

AIX

```
/usr/lib/
    libpthread.a(shr_comm.o)
    libpthread.a(shr_xpg5.o)
    libc.a(shr.o)
    librtl.a(shr.o)
    libpthreads.a(shr_comm.o)
    libcrypt.a(shr.o)
/aix5.2/lib/gcc/powerpc-ibm-aix5.2.0.0/4.1.0/libstdc++.a(libstdc++.so.6)
/aix5.2/lib/gcc/powerpc-ibm-aix5.2.0.0/4.1.0/libgcc_s.a(shr.o)
```

3.1.3.8.2 XMLForms

XMLForms には、以下のシステムライブラリが最低限必要です。

Linux

```
/lib/
    libdl.so.2
    libpthread.so.0
    libm.so.6
    libgcc_s.so.1
    libc.so.6
    librt.so.1
    ld-linux.so.2
/usr/X11R6/lib/
    libX11.so.6
```

Solaris

```
/usr/lib/
    libdl.so.1
    libpthread.so.1
    libintl.so.1
    libsocket.so.1
    libnsl.so.1
    libm.so.1
    libc.so.1
    librt.so.1
    libX11.so.4
    libmp.so.2
    libmd5.so.1
    libscf.so.1
    libaio.so.1
    libXext.so.0
    libdoor.so.1
    libuutil.so.1
    libm.so.2
usr/platform/SUNW,Sun-Fire-V210/lib/libc_psr.so.1
usr/platform/SUNW,Sun-Fire-V210/lib/libmd5_psr.so.1
```

AIX 6.1

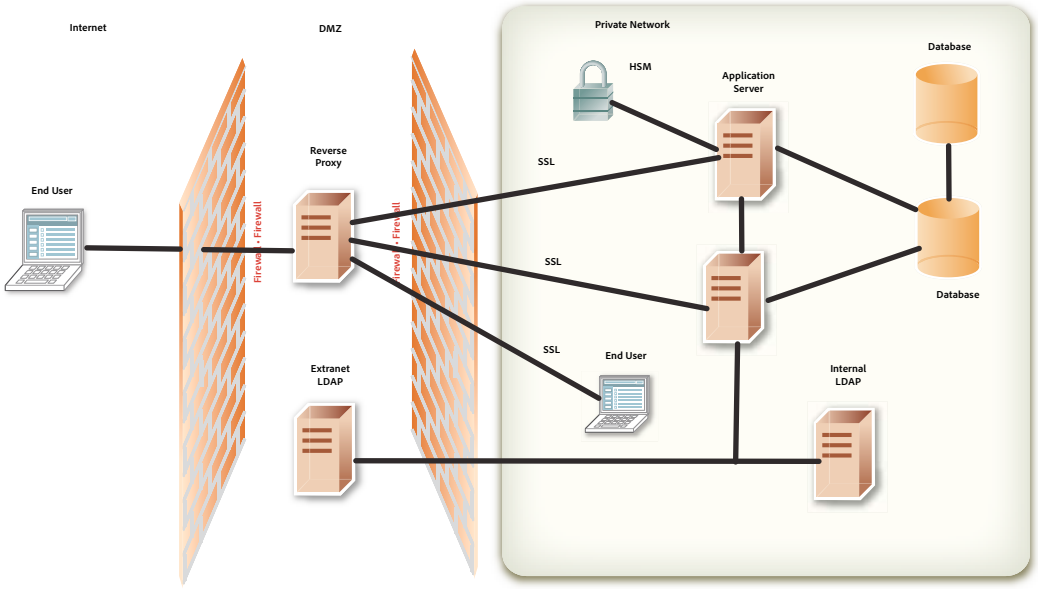
```
/usr/lib/
    libpthread.a(shr_comm.o)
    libpthread.a(shr_xpg5.o)
    libc.a(shr.o)
    librtl.a(shr.o)
    libdl.a(shr.o)
    libX11.a(shr4.o)
    libiconv.a(shr4.o)
    libpthreads.a(shr_comm.o)
/unix
    /usr/lib/libcrypt.a(shr.o)
    /usr/lib/libIM.a(shr.o)
    /usr/lib/libpthreads.a(shr_xpg5.o)
```

3.1.4 社外からのアクセスを可能にするための JEE 上の AEM forms の設定

JEE 上の AEM forms のインストールが完了したら、定期的に環境のセキュリティの保守を行うことが重要です。ここでは、JEE 上の AEM forms 実稼働サーバーのセキュリティを維持するための推奨タスクについて説明します。

3.1.4.1 Web アクセスのリバースプロキシの設定

「リバースプロキシ」は、1 セットの JEE 上の AEM forms Web アプリケーションの URL を、外部ユーザーと内部ユーザーの両方から利用できるように設定するものです。この設定は、JEE 上の AEM forms を実行するアプリケーションサーバーへのユーザーの直接接続を許可する方法よりも、高いセキュリティで保護されます。リバースプロキシは、JEE 上の AEM forms を実行しているアプリケーションサーバーに対するすべての HTTP 要求を実行します。ユーザーは、リバースプロキシに対するネットワークアクセスしか持たないので、リバースプロキシでサポートされている URL 接続のみを試みることができます。



リバースプロキシサーバーで使用する JEE 上の AEM forms ルート URL

次のアプリケーションルート URL は、各 JEE 上の AEM forms Web アプリケーションのものです。リバースプロキシは、エンドユーザーに提供する Web アプリケーション機能の URL だけを公開するように設定する必要があります。

一部の URL は、エンドユーザーが使用する Web アプリケーションを示しています。Configuration Manager のその他の URL は、リバースプロキシ経由の外部ユーザーのアクセスを許可しないので、公開しないでください。

ルート URL	用途および関連する Web アプリケーション	Web ベースのインターフェイス	エンドユーザーアクセス
/ReaderExtensions/*	PDF ドキュメントに使用権限を適用する Acrobat Reader DC Extensions エンドユーザー Web アプリケーション	Yes	Yes
/edc/*	Rights Management エンドユーザー Web アプリケーション	Yes	Yes
/edcws/*	Rights Management の Web サービス URL	No	Yes
/pdfgui/*	PDF Generator 管理 Web アプリケーション	Yes	Yes
/ ワークスペース /*	Workspace エンドユーザー Web アプリケーション	Yes	Yes
/workspace-server/*	Workspace クライアントアプリケーションが必要とする Workspace サーブレットおよび Data Services	Yes	Yes
/adobe-bootstrapper/*	JEE 上の AEM forms をブートストラップするサーブレット	No	No

ルート URL	用途および関連する Web アプリケーション	Web ベースのインターフェイス	エンドユーザーアクセス
/soap/*	forms サーバー Web サービスの情報ページ	No	No
/soap/services/*	すべての forms サーバーサービス用の Web サービス URL	No	No
/edc/admin/*	Rights Management 管理 Web アプリケーション	Yes	No
/adminui/*	管理コンソールのホームページ	Yes	No
/TruststoreComponent/secured/*	Trust Store Management 管理ページ	Yes	No
/FormsIVS/*	フォームのレンダリングのテストとデバッグを行う Forms IVS アプリケーション	Yes	No
/OutputIVS/*	Output サービスのテストとデバッグを行う Output IVS アプリケーション	Yes	No
/rmws/*	Rights Management のための REST URL	No	Yes
/OutputAdmin/*	Output 管理ページ	Yes	No
/FormServer/*	Forms Web アプリケーションファイル	Yes	No
/FormServer/GetImage サーブレット	HTML 変換時に、JavaScript の取得に使用	No	No
/FormServerAdmin/*	Forms 管理ページ	Yes	No
/repository/*	WebDAV（デバッグ）アクセス用の URL	Yes	No
/AACComponent/*	アプリケーションおよびサービスユーザーインターフェイス	Yes	No
/WorkspaceAdmin/*	Workspace 管理ページ	Yes	No
/rest/*	残りのサポートページ	Yes	No
/CoreSystemConfig/*	JEE 上の AEM forms Core 設定ページ	Yes	No
/um/	User Management 認証	No	Yes
/um/*	User Management 管理インターフェイス	Yes	No
/DoumentManager/*	HTTP ドキュメント対応の SOAP トランスポートまたは EJB トランスポート経由でリモートエンドポイント、SOAP WSDL エンドポイントおよび Java SDK にアクセスするときに、処理するドキュメントをアップロードおよびダウンロードする。	Yes	Yes

3.1.5 クロスサイト要求偽造攻撃からの保護

クロスサイト要求偽造（CSRF）攻撃とは、ユーザーに対する Web サイトの信頼を悪用して、ユーザーが許可していないコマンドを知らないうちに送信することです。この攻撃は、Web ページ上に配置したリンクまたはスクリプトや、電子メールメッセージに含めた URL を介して、既にユーザーの認証が済んでいる別のサイトへのアクセスを達成するという形で行われます。

例えば、管理者は、他の Web サイトを閲覧しながら管理コンソールにログインすることがあります。CSRF 攻撃者は、このような状況を狙って、閲覧されるサイトの Web ページに含まれている HTML img タグの src 属性などに、攻撃対象 Web サイト内のサーバー側スクリプトを参照する URL を記述しておきます。Web ブラウザーに備わっている Cookie ベースの

セッション認証メカニズムにより、攻撃者の Web サイトは正当なユーザーを装って、攻撃対象のサーバー側スクリプトに悪意ある要求を送信することができます。その他の例については、https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)#Examples を参照してください。

CSRF に共通の特性を次に示します。

- ユーザーの ID を信頼したサイトに関与する。
- その ID に対するサイトの信頼を利用する。
- ユーザーのブラウザーをだましてターゲットサイトに HTTP 要求を送信させる。
- 副次的な悪影響のある HTTP 要求に関与する。

JEE 上の AEM forms では、リファラーフィルター機能を使用して CSRF 攻撃を防ぎます。ここでは、次の用語を使用してリファラーフィルターメカニズムについて説明します。

- **許可されているリファラー：**リファラーは、要求をサーバーに送信するソースページのアドレスです。JSP ページまたはフォームの場合、リファラーは一般的にブラウザー履歴の前のページになります。画像のリファラーは、通常、画像が表示されるページです。許可されているリファラーリストにリファラーを追加すると、サーバーリソースにアクセスできるリファラーを識別できます。
- **許可されているリファラーの例外：**許可されているリファラーリストの特定のリファラーに対して、アクセス範囲を制限することができます。この制限を適用するには、そのリファラーのパスを、許可されているリファラーの例外リストに個別に追加します。許可されているリファラーの例外リストに含まれるパスから要求が発行された場合、AEM forms サーバー上のリソースは呼び出されません。許可されているリファラーの例外リストは、特定のアプリケーションに対して定義できます。また、すべてのアプリケーションに適用される例外のグローバルリストを使用することもできます。
- **許可されている URI：**リファラーヘッダーを確認せずに提供されるリソースのリストです。例えば、サーバーの状態に変更を加えることのない、リソースのヘルプページをこのリストに追加できます。許可されている URI リストのリソースは、リファラーが何であっても、リファラーフィルターでブロックされることはありません。
- **ヌルリファラー：**関連付けられていない、または送信元が親 Web ページではないサーバー要求は、ヌルリファラーからの要求と見なされます。例えば、新しいブラウザーウィンドウを開き、アドレスを入力して、Enter キーを押すと、サーバーには null のリファラーが送信されます。Web サーバーに HTTP 要求を送信するデスクトップアプリケーション（.NET または SWING）も、ヌルリファラーをサーバーに送信します。

3.1.5.1 リファラーのフィルタリング

ここでは、リファラーのフィルタリングプロセスについて説明します。

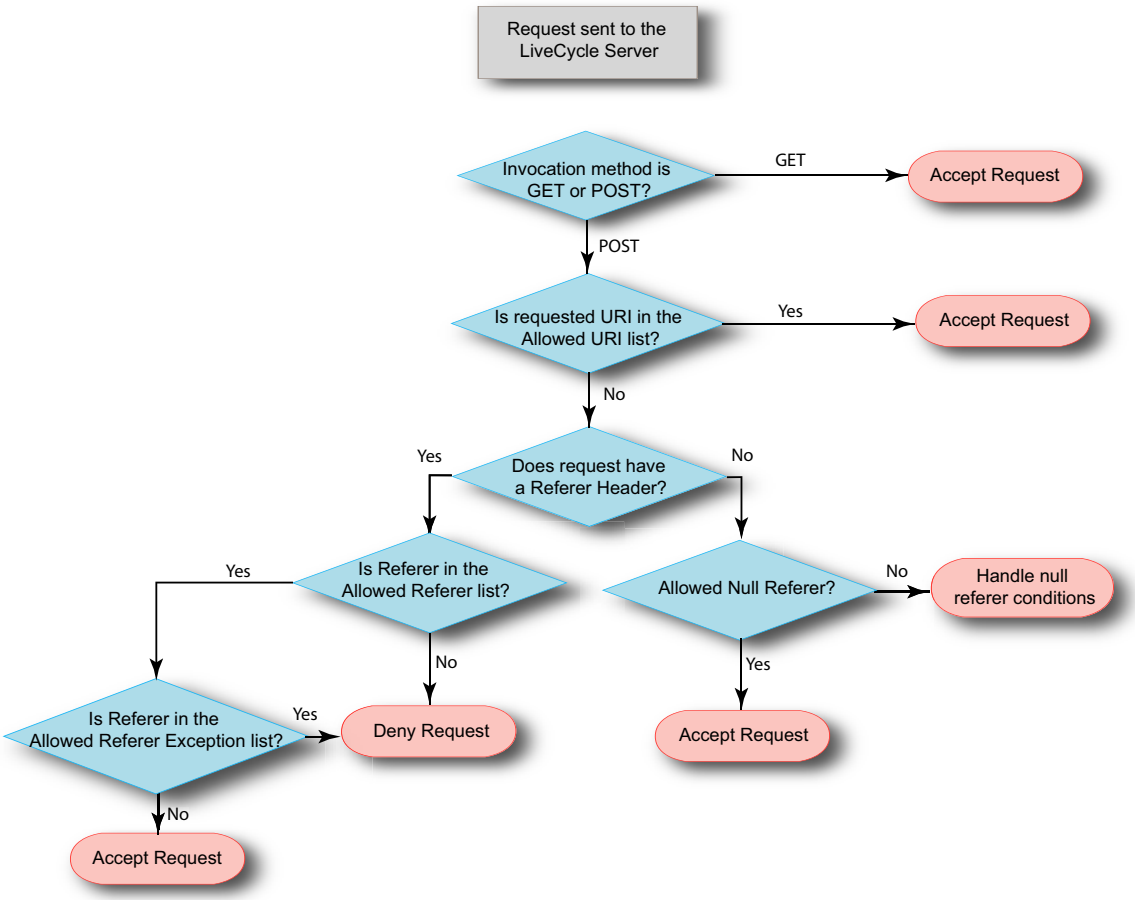
1. forms サーバーが、呼び出しに使用される HTTP メソッドを確認します。
   a. POST の場合、forms サーバーはリファラーのヘッダーのチェックを実行します。
   b. GET の場合、forms サーバーはリファラーをチェックしません。ただし、**CSRF_CHECK_GETS** が true に設定されている場合は除きます。この場合、forms サーバーはリファラーヘッダーを確認します。CSRF_CHECK_GETS は、アプリケーションの web.xml ファイル内に設定されます。
2. forms サーバーが、要求された URI がホワイトリストに登録されているかどうかを確認します。
   a. URI がホワイトリストに登録されている場合、サーバーは要求を受け入れます。
   b. 要求された URI がホワイトリストに登録されていない場合、サーバーは要求のリファラーを取得します。
3. 要求内にリファラーがある場合、サーバーはそれが許可されているリファラーかどうかを確認します。許可されている場合は、リファラーの例外を確認します。
   a. 例外の場合、要求はブロックされます。
   b. 例外でない場合、要求はパスします。

4 要求内にリファラーがない場合、サーバーはヌルリファラーが許可されているかどうかを確認します。

a null リファラーが許可されている場合、要求はパスします。

b null リファラーが許可されていない場合、サーバーは要求された URI がヌルリファラーの例外かどうかを確認し、適宜要求を処理します。

次の図は、要求がサーバーに送信されたときに JEE 上の AEM forms が実行する CSRF 確認を表しています。



3.1.5.2 リファラーフィルタリングの管理

JEE 上の AEM forms には、サーバーリソースにアクセスできるリファラーを指定するリファラーフィルターが用意されています。デフォルトでは、リファラーフィルターでは安全な HTTP メソッド（GET など）を使用する要求はフィルタリングされません。ただし、CSRF_CHECK_GETS が true に設定されている場合は除きます。許可されているリファラーのエントリのポート番号が 0 に設定されている場合、ポート番号に関係なくホストからのすべての要求がリファラーと共に許可されます。ポート番号が指定されていない場合は、デフォルトのポート 80（HTTP）またはポート 443（HTTPS）からの要求のみが許可されます。許可されているリファラーリストのすべてのエントリが削除されると、リファラーフィルタリングは無効になります。

Document Services を最初にインストールすると、許可されているリファラーリストは、Document Services がインストールされたサーバーのアドレスで更新されます。サーバーのエントリには、サーバー名、IPv4 アドレス、IPv6 アドレス（IPv6 が有効の場合）、ループバックアドレス、localhost エントリなどがあります。「許可されるリファラ」のリストに追加された名前は、ホストオペレーティングシステムにより返されます。例えば、IP アドレスが 10.40.54.187 のサーバーは次の入力を含みます。http://server-name:0, https://10.40.54.187:0, http://127.0.0.1:0, http://localhost:0 ホストのオペレーティング

システムによって返された正規でない名前（IPv4 アドレス、IPv6 アドレス、正規のドメイン名を持たない名前）の場合、ホワイトリストは更新されません。許可されているリファラーリストを、ビジネス環境に合わせて変更します。実稼働環境に forms サーバーをデプロイするとき、許可されているリファラーリストの内容がデフォルトのままになっていないことを確認してください。許可されているリファラー、リファラーの例外または URI を変更したら、必ずサーバーを再起動して、その変更を有効にします。

許可されているリファラーリストの管理

許可されているリファラーリストは、管理コンソールの User Management インターフェイスから管理できます。User Management インターフェイスを使用すると、リストを作成、編集または削除できます。許可されているリファラーリストの操作について詳しくは、管理ヘルプの「**CSRF** 攻撃の防止」を参照してください。

許可されているリファラーの例外リストおよび許可されている URI リストの管理

JEE 上の AEM forms には、許可されているリファラーの例外リストおよび許可されている URI リストを管理するための API が用意されています。この API を使用すると、リストを取得、作成、編集または削除できます。使用可能な API のリストを次に示します。

- createAllowedURIsList
- getAllowedURIsList
- updateAllowedURIsList
- deleteAllowedURIsList
- addAllowedRefererExceptions
- getAllowedRefererExceptions
- updateAllowedRefererExceptions
- deleteAllowedRefererExceptions

API について詳しくは、『JEE 上の AEM forms API リファレンス』を参照してください。

許可されているリファラーの例外の **LC_GLOBAL_ALLOWED_REFERER_EXCEPTION** リストは、グローバルレベルで使用します。つまり、すべてのアプリケーションに適用できる例外を定義します。このリストには、絶対パス（例：/index.html）または相対パス（例：/sample/）のいずれかの URI のみが含まれています。また、相対 URI の末尾に正規表現を追加することもできます（例：/sample/(.)*）。

LC_GLOBAL_ALLOWED_REFERER_EXCEPTION リスト ID は、com.adobe.idp.um.api 名前空間の UMConstants クラスで定数として定義されており、adobe-usermanager-client.jar にあります。この AEM forms API を使用すると、リストを取得、作成、編集または削除できます。例えば、グローバルで許可されているリファラーの例外リストを作成するには、次の API を使用します。

```
addAllowedRefererExceptions(UMConstants.LC_GLOBAL_ALLOWED_REFERER_EXCEPTION, Arrays.asList("/index.html",
"/sample/(.)*"))
```

アプリケーション固有の例外については、**CSRF_ALLOWED_REFERER_EXCEPTIONS** リストを使用します。

リファラーフィルターの無効化

リファラーフィルターによって forms サーバーへのアクセスが完全にブロックされ、許可されているリファラーリストを編集できない場合は、サーバー起動スクリプトを更新して、リファラーフィルタリングを無効にできます。

それには、-Dlc.um.csrffilter.disabled=true JAVA 引数を起動スクリプトに追加して、サーバーを再起動します。許可されているリファラーリストを適切に再設定したら、JAVA 引数は必ず削除するようにしてください。

カスタム WAR ファイルのリファラーフィルタリング

管理者は、ビジネス要件に合わせて JEE 上の AEM forms を操作するためのカスタム WAR ファイルを用意している場合があります。カスタム WAR ファイルに対してリファラーフィルタリングを有効にするには、**adobe-usermanager-client.jar** を WAR のクラスパスに追加し、フィルターエントリを **web.xml** ファイルに追加して、次のパラメーターを指定します。

CSRF_CHECK_GETS は、GET 要求でリファラーチェックを制御します。このパラメーターが定義されていない場合、デフォルト値は false に設定されます。このパラメーターは、GET 要求をフィルタリングする場合にのみ指定します。

CSRF_ALLOWED_REFERER_EXCEPTIONS は、許可されているリファラーの例外リストの ID です。このリファラーフィルターを使用すると、リスト ID で特定されたリスト内のリファラーからの要求では、forms サーバーのリソースを呼び出すことはできません。

CSRF_ALLOWED_URIS_LIST_NAME は、許可されている URI リストの ID です。リファラーフィルターは、要求のリファラーヘッダーの値に関係なく、リスト ID で特定されたリストのリソースに対する要求をブロックしません。

CSRF_ALLOW_NULL_REFERER は、リファラーが null の場合または存在しない場合のリファラーフィルターの動作を制御します。このパラメーターが定義されていない場合、デフォルト値は false に設定されます。このパラメーターは、ヌルリファラーを許可する場合にのみ指定します。ヌルリファラーを許可すると、ある種のクロスサイト要求偽造攻撃を許可してしまう可能性があります。

CSRF_NULL_REFERER_EXCEPTIONS は、リファラーが null の場合にリファラーチェックが行われない URI のリストです。このパラメーターは、**CSRF_ALLOW_NULL_REFERER** が false に設定されている場合にのみ有効です。リスト内で複数の URI を指定するときはコンマで区切ります。

サンプル WAR ファイルに対する **web.xml** ファイルのフィルターエントリの例を次に示します。

```
<filter>
       <filter-name> filter-name </filter-name>
       <filter-class> com.adobe.idp.um.auth.filter.RemoteCSRFFilter </filter-class>
     <!-- default is false -->
     <init-param>
      <param-name> CSRF_ALLOW_NULL_REFERER </param-name>
      <param-value> false </param-value>
     </init-param>
     <!-- default is false -->
     <init-param>
      <param-name> CSRF_CHECK_GETS </param-name>
      <param-value> true </param-value>
     </init-param>
     <!-- Optional -->
     <init-param>
       <param-name> CSRF_NULL_REFERER_EXCEPTIONS </param-name>
       <param-value> /SAMPLE/login, /SAMPLE/logout  </param-value>
     </init-param>
     <!-- Optional -->
     <init-param>
      <param-name> CSRF_ALLOWED_REFERER_EXCEPTIONS </param-name>
      <param-value> SAMPLE_ALLOWED_REF_EXP_ID </param-value>
     </init-param>
     <!-- Optional -->
     <init-param>
      <param-name> CSRF_ALLOWED_URIS_LIST_NAME </param-name>
      <param-value> SAMPLE_ALLOWED_URI_LIST_ID </param-value>
     </init-param>
</filter>
    ........
    <filter-mapping>
      <filter-name> filter-name </filter-name>
      <url-pattern>/*</url-pattern>
    </filter-mapping>
```

トラブルシューティング

適切なサーバー要求が CSRF フィルターによってブロックされる場合は、次のいずれかを試してみてください。

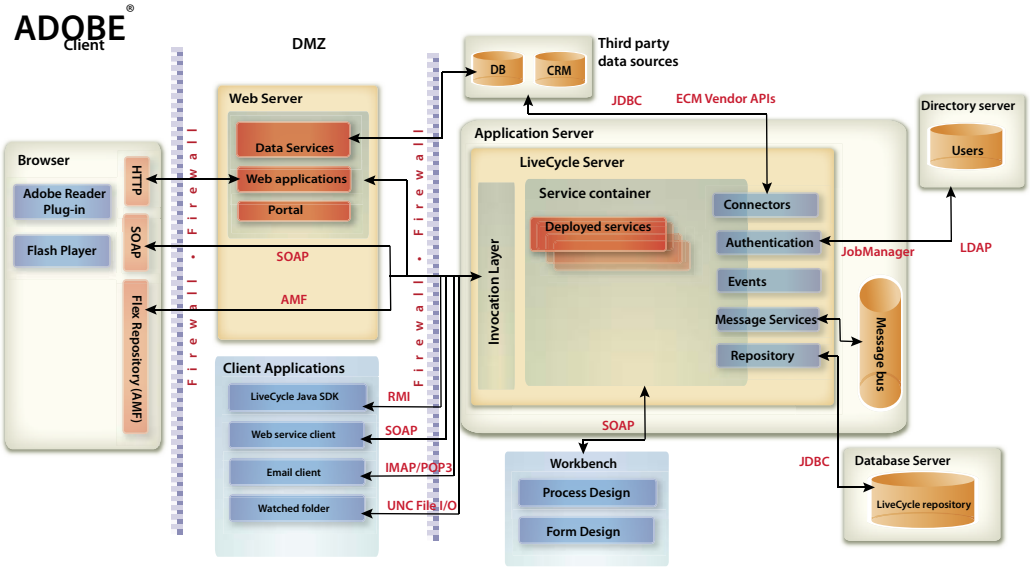
- 拒否された要求にリファラーヘッダーがある場合は、許可されているリファラーリストにそのリファラーを追加することを慎重に検討します。信頼できるリファラーのみを追加します。
- 拒否された要求にリファラーヘッダーがない場合は、リファラーヘッダーを含めるようにクライアントアプリケーションを変更します。
- クライアントがブラウザーで動作できる場合は、そのデプロイメントモデルを試してみます。
- 最後の手段として、許可されている URI リストにリソースを追加できます。ただし、これは推奨設定ではありません。

3.1.6 ネットワーク設定の保護

ここでは、JEE 上の AEM forms が必要とするプロトコルとポートについて説明し、保護されたネットワーク設定で JEE 上の AEM forms をデプロイするための推奨事項を示します。

3.1.6.1 JEE 上の AEM forms 物理アーキテクチャ

次の図に、代表的な JEE 上の AEM forms デプロイメントで使用されるコンポーネントとプロトコル、および推奨のファイアウォールトポロジを示します。



3.1.6.2 JEE 上の AEM forms で使用されるネットワークプロトコル

前の節で説明したように、保護されたネットワークアーキテクチャを設定する場合、エンタープライズネットワーク内の JEE 上の AEM forms と他のシステムのやり取りのために次のネットワークプロトコルが必要です。

プロトコル	**カメラメーカーから提供されているソフトウェアと同じカラーレンダリングが好都合である場合は、「**
HTTP	• Configuration Manager およびエンドユーザー Web アプリケーションをブラウザーに表示する • すべての SOAP 接続
SOAP[SOAP]	• .NET アプリケーションなどの Web サービスクライアントアプリケーション • Adobe Reader® は JEE 上の AEM forms サーバー Web サービスとのやり取りに SOAP を使用する • Adobe Flash® アプリケーションは forms サーバー Web サービスとのやり取りに SOAP を使用する • SOAP モードで使用された場合に JEE 上の AEM forms SDK によって呼び出される • Workbench 設計環境
RMI	Enterprise JavaBeans（EJB）モードで使用された場合に JEE 上の AEM forms SDK によって呼び出される
IMAP/POP3	• サービスに対する電子メールベースの入力（電子メールエンドポイント） • 電子メールを使用したユーザータスク通知
UNC ファイル IO	サービスに対する入力用の監視フォルダーを JEE 上の AEM forms で監視する（監視フォルダーエンドポイント）
LDAP	• ディレクトリ内の組織ユーザーとグループ情報を同期する • 対話的にやり取りするユーザーに LDAP 認証を行う
JDBC	• JDBC サービスを使用したプロセスの実行時に、外部データベースに対するクエリーとプロシージャの呼び出しを行う • JEE 上の AEM forms リポジトリへの内部からのアクセス
WebDAV	任意の WebDAV クライアントによる JEE 上の AEM forms デザイン時リポジトリ（フォーム、フラグメントなど）のリモート参照を有効にする
AMF	JEE 上の forms サーバーサービスがリモートエンドポイントとして設定されている Adobe Flash アプリケーション
JMX	JEE 上の AEM forms は監視対象の MBeans を JMX を使用して公開する

3.1.6.3 アプリケーションサーバーのポート

ここでは、サポートしている各種のアプリケーションサーバーのデフォルトポート（および代替設定の範囲）について説明します。これらのポートについては、JEE 上の AEM forms を実行しているアプリケーションサーバーに接続するクライアントに対して許可するネットワーク機能に応じて、内側のファイアウォール上で有効と無効を切り替える必要があります。

注意：デフォルトでは、サーバーは、adobe.com 名前空間内に複数の JMX MBeans を公開します。サーバーの正常性監視に有用な情報だけが公開されます。ただし、情報開示を防ぐには、信頼できないネットワーク内の呼び出し元によって JMX MBeans の参照と正常性評価基準へのアクセスが行われないようにする必要があります。

JBoss ポート

用途	ポート
Web アプリケーションへのアクセス	[JBossroot]/server/all/deploy/jbossweb-tomcat50.sar/server.xml HTTP/1.1 コネクタポート 8080 AJP 1.3 コネクタポート 8009 SSL/TLS コネクタポート 8443
forms サーバーサービスへのアクセス	[JBossroot]/server/all/conf/jboss-service.xml WebService ポート 8083 NamingService ポート 1099 RMIport 1098 ～ RMIObjectPort 4444 ～ PooledInvoker ServerBindPort 4445
J2EE クラスタサポート	[JBossroot]/server/all/deploy/cluster-service.xml ha.jndi.HANamingService ポート 1100 ～ RmiPort 1101 RMIObjectPort 4447 （クラスタのみ）ServerBindPort 4446
CORBA サポート	[JBossroot]/server/all/conf/jacorb.properties OAPort 3528 OASSLPort 3529
SNMP サポート	[JBoss root]/server/all/deploy/snmp-adaptor.sar/META-INF/jbossservice.xml ポート 1161、1162 [JBossroot]/server/all/deploy/snmp-adaptor.sar/managers.xml ポート 1162

WebLogic ポート

用途	ポート
Web アプリケーションへのアクセス	• 管理サーバーリスンポート：デフォルトは 7001 • 管理サーバー SSL リスンポート：デフォルトは 7002 • 管理対象サーバー用に設定されたポート：8001 など
JEE 上の AEM forms へのアクセスに必要とされない WebLogic 管理ポート	• 管理対象サーバーリスンポート：1 ～ 65534 の範囲で設定可能 • 管理対象サーバー SSL リスンポート：1 ～ 65534 の範囲で設定可能 • ノードマネージャーリスンポート：デフォルトは 5556

WebSphere 6.1 ポート

JEE 上の AEM forms で必要な WebSphere 6.1 ポートについて詳しくは、「Port number settings in WebSphere Application Server versions」を参照してください。

WebSphere 7.0 ポート
JEE 上の AEM forms で必要な WebSphere 7.0 ポートについて詳しくは、http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.websphere.migration.express.doc/info/exp/ae/rmig_portnumber.html を参照してください。

3.1.6.4 SSL の設定

24 ページの「3.1.6.1 JEE 上の AEM forms 物理アーキテクチャ」で取り上げている物理アーキテクチャについては、使用するすべての接続に SSL を設定する必要があります。特に SOAP 接続は、ネットワーク上にユーザー資格情報が公開されないように、すべて SSL 経由で行う必要があります。

SSL on JBoss、WebLogic、WebSphere の設定方法について詳しくは、『管理ヘルプ』の「SSL の設定」を参照してください。

3.1.6.5 SSL リダイレクトの設定

SSL をサポートするようにアプリケーションサーバーを設定した後、アプリケーションおよびサービスに対するすべての HTTP トラフィックは、SSL ポートを使用するように強制されます。

WebSphere または WebLogic で SSL リダイレクトを設定するには、使用しているアプリケーションサーバーのドキュメントを参照してください。

1. adobe-livecycle-jboss.ear に移動し、このファイルを解凍します。
2. adminui.war ファイルを抽出し、web.xml ファイルを開いて編集します。
3. 次のコードを web.xml ファイルに追加します。

```
<security-constraint>
    <web-resource-collection>
        <web-resource-name>app or resource name</web-resource-name>
        <url-pattern>/*</url-pattern>
        <!-- define all url patterns that need to be protected-->
        <http-method>GET</http-method>
        <http-method>POST</http-method>
    </web-resource-collection>
    <user-data-constraint>
        <transport-guarantee>CONFIDENTIAL</transport-guarantee>
    </user-data-constraint>
</security-constraint>
```

3.1.7 Windows 固有のセキュリティに関する推奨事項

ここでは、JEE 上の AEM forms の実行に使用する場合の Windows 固有のセキュリティ推奨事項について説明します。

3.1.7.1 JBoss サービスアカウント

JEE 上の AEM forms 自動インストールは、デフォルトで、ローカルシステムアカウントを使用してサービスアカウントを設定します。組み込みのローカルシステムユーザーアカウントは、高いレベルのアクセス権限を付与されており、Administrators グループに属しています。ワーカープロセス ID をローカルシステムユーザーアカウントで実行した場合、ワーカープロセスはシステム全体に対してフルアクセス権限を持ちます。

3.1.7.1.1 管理者以外のアカウントでのアプリケーションサーバーの実行

1. Microsoft 管理コンソール（MMC）で、forms サーバーサービスへのログインに使用するローカルユーザーを作成します。
   - 「**ユーザーはパスワードを変更できない**」オプションを選択します。

- 「**所属するグループ**」タブに、「ユーザー」グループが表示されていることを確認してください。

2 **設定**／**管理ツール**／**サービス**を選択します。

3 アプリケーションサーバーサービスをダブルクリックし、サービスを停止します。

4 「**ログオン**」タブで、「**アカウント**」を選択し、作成したユーザーアカウントを参照して、アカウントのパスワードを入力します。

5 ローカルセキュリティ設定ウィンドウの「ユーザー権利の割り当て」で、forms サーバーを実行しているユーザーアカウントに次の権限を付与します。

- ターミナルサービスを使ったログオンを拒否する
- ローカルでログオンを拒否する
- サービスとしてログオン（通常は既に設定済み）

6 新しく作成したユーザーアカウントに、JEE 上の AEM forms Web コンテンツディレクトリの項目に対する「読み取りと実行」、「フォルダの内容の一覧表示」、「読み取り」の各権限を付与します。

7 アプリケーションサーバーサービスを起動します。

3.1.7.2 ファイルシステムのセキュリティ

JEE 上の AEM forms は、次の方法でファイルシステムを利用します。

- ドキュメントの入力と出力を処理する際に使用する一時ファイルを格納する
- インストールしたソリューションコンポーネントのサポートに使用されるファイルをグローバルアーカイブストアに格納する
- ファイルシステムフォルダーからサービスへの入力として使用されるドロップファイルを監視フォルダーに格納する

forms サーバーサービスのドキュメントを送受信する方法として監視フォルダーを使用する場合、ファイルシステムのセキュリティを確保するために一層の予防策を講じる必要があります。ユーザーが監視フォルダーにコンテンツをドロップした場合、コンテンツは監視フォルダーを通じて公開されます。この場合、サービスは実際のエンドユーザーを認証していません。代わりに、フォルダーレベルに設定されている ACL と共有レベルセキュリティに応じて、サービスを呼び出して実行することのできるユーザーを決定しています。

3.1.8 JBoss 固有のセキュリティに関する推奨事項

ここでは、JEE 上の AEM forms を実行する際に使用される JBoss 4.2 に特有のアプリケーションサーバー設定の推奨事項について説明します。

3.1.8.1 JBoss 管理コンソールおよび JMX コンソールの無効化

JBoss 管理コンソールと JMX コンソールへのアクセスは、自動インストールオプションを使用して JBoss に JEE 上の AEM forms をインストールしたときに設定されます。独自の JBoss Application Server を使用している場合は、JBoss 管理コンソールおよび JMX 監視コンソールへのアクセスが保護されていることを確認してください。JMX 監視コンソールへのアクセスは、jmx-invoker-service.xml という JBoss 設定ファイルで設定されています。

3.1.8.2 ディレクトリ参照の無効化

管理コンソールにログインした後に、URL を変更することにより、コンソールのディレクトリ一覧を参照することができます。例えば、URL を次のいずれかの URL に変更すると、ディレクトリ一覧が表示される場合があります。

```
http://<servername>:8080/adminui/secured/
http://<servername>:8080/um/
```

ディレクトリ一覧を無効にするには、次の例に示すように、**[JBoss root]** \server\default\deploy\jbossweb-tomcatxxx.sar\conf\web.xml ファイルで、DefaultServlet プロパティの初期化パラメーターの listings の値を false に設定します（太字で示した部分）。

```
<servlet>
    <servlet-name>default</servlet-name>
    <servlet-class>
        org.apache.catalina.servlets.DefaultServlet
    </servlet-class>
    <init-param>
        <param-name>listings</param-name><param-value>false</param-value>
    </init-param>
    <load-on-startup>1</load-on-startup>
</servlet>]
```

3.1.9 WebLogic 固有のセキュリティに関する推奨事項

ここでは、JEE 上の AEM forms の実行時に WebLogic 9.1 を保護するためのアプリケーションサーバー設定の推奨事項について説明します。

3.1.9.1 ディレクトリ参照の無効化

weblogic.xml ファイルの index-directories プロパティを false に設定します。次に例を示します。

```
<container-descriptor>
    <index-directory-enabled>false
    </index-directory-enabled>
</container-descriptor>
```

3.1.9.2 WebLogic SSL ポートの有効化

デフォルトでは、WebLogic はデフォルト SSL リスンポート 7002 を有効にしません。SSL を設定する前に、WebLogic Server 管理コンソールでこのポートを有効にしてください。

3.1.10 WebSphere 固有のセキュリティに関する推奨事項

ここでは、JEE 上の AEM forms の実行時に WebSphere を保護するためのアプリケーションサーバー設定の推奨事項について説明します。

3.1.10.1 ディレクトリ参照の無効化

ibm-web-ext.xml ファイルの directoryBrowsingEnabled プロパティを false に設定します。

3.1.10.2 WebSphere 管理セキュリティの有効化

1. WebSphere Administrative Console にログインします。
2. ナビゲーションツリーで次のリンクのいずれかを選択します。

   （WebSphere 6.1）**Security** ／ **Secure administration, applications, and infrastructure**

   （WebSphere 7.0）**Security** ／ **Global Security**
3. 「**Enable administrative security**」を選択します。
4. 「**Enable application security**」および「**Use Java 2 security**」の選択を解除します。
5. 「**OK**」または「**Apply**」をクリックします。
6. 「**Messages**」ボックスで、「**Save directly to the master configuration**」をクリックします。

第 4 章：JEE 上の AEM forms 管理者設定のセキュリティ保護の設定

4.1 JEE 上の AEM forms 管理者設定のセキュリティ保護の設定

通常、開発者は、アプリケーションのビルドとテストに 実稼働環境は使用しません。したがって、プライベートな開発環境には必要でも実稼働環境には必要のないユーザーアカウントとサービスを管理する必要があります。

この記事では、JEE 上の AEM forms の管理オプションを使用して、攻撃の対象となる脆弱性を全体的に減らす方法について説明します。

4.1.1 サービスへの不要なリモートアクセスの無効化

JEE 上の AEM forms のインストールと設定が完了したら、SOAP および Enterprise JavaBeans™（EJB）経由で、多くのサービスをリモートで起動できるようになります。「リモート」という用語は、この場合、アプリケーションサーバーの SOAP、EJB または Action Message Format（AMF）のポートにネットワークアクセス可能なすべての呼び出し元を意味します。

JEE 上の AEM forms サービスを呼び出すには、承認された呼び出し元であることを示す有効な資格情報が要求されます。それでも、リモートアクセスを認める必要がないサービスをリモートアクセス可能な状態にしておくことは望ましくありません。アクセスを制限するには、まず、システムとして機能するために必要な最小限のサービス群だけをリモートアクセス可能にします。その後、必要に応じて他のサービスのリモート起動を許可していくようにします。

JEE 上の AEM forms サービスには、少なくとも SOAP アクセスが常に必要です。これらのサービスは、通常は Workbench で使用するために必要とされますが、Workspace Web アプリケーションによって呼び出されるサービスである場合もあります。

管理コンソールのアプリケーションおよびサービス Web ページを使用して、次の手順を実行します。

1 Web ブラウザーに次の URL を入力して管理コンソールにログインします。

```
http://[host name]:[port]/adminui
```

2 **サービス／アプリケーションおよびサービス／環境設定**をクリックします。

3 環境設定で、同じページにサービスとエンドポイントを 200 個まで表示するように設定します。

4 **サービス／アプリケーションおよびサービス／エンドポイントの管理**をクリックします。

5 **プロバイダー**リストから「**EJB**」を選択して、「**フィルター**」をクリックします。

6 すべての EJB エンドポイントを無効にするには、リスト内でそれぞれの横にあるチェックボックスを選択して、「**無効にする**」をクリックします。

7 「**次へ**」をクリックして、すべての EJB エンドポイントに関して、前述の手順を繰り返します。エンドポイントを無効にする前に、「プロバイダー」列に EJB が表示されていることを確認してください。

8 **プロバイダー**リストから「**SOAP**」を選択して、「**フィルター**」をクリックします。

9 SOAP エンドポイントを削除するには、リスト内でそれぞれの横にあるチェックボックスを選択して、「**削除**」をクリックします。以下のエンドポイントは削除しないでください。

   • AuthenticationManagerService

- DirectoryManagerService
- JobManager
- event_management_service
- event_configuration_service
- ProcessManager
- TemplateManager
- RepositoryService
- TaskManagerService
- TaskQueueManager
- TaskManagerQueryService
- WorkspaceSingleSignOn
- EventGenerationandReceipt
- ApplicationManager

10「**次へ**」をクリックして、上記のリストにない SOAP エンドポイントに関して、前述の手順を繰り返します。エンドポイントを削除する前に、「プロバイダー」列に SOAP が表示されていることを確認してください。

4.1.2 サービスへの不要な匿名アクセスの無効化

一部の forms サーバーサービスについては、未承認（匿名）ユーザーが呼び出して一部の操作を実行することが許可されます。つまり、サービスによって公開されている一部の操作は、認証された任意のユーザーだけでなく、認証されていない任意のユーザーによって呼び出される可能性があります。

1 Web ブラウザーに次の URL を入力して管理コンソールにログインします。

```
http://[host name]:[port]/adminui
```

2 **サービス／アプリケーションおよびサービス／サービスの管理**をクリックします。

3 無効にするサービスの名前（AuthenticationManagerService など）をクリックします。

4「**セキュリティ**」タブをクリックし、「**匿名アクセスが許可されました**」の選択を解除して、「**保存**」をクリックします。

5 以下のサービスに関して手順 3 と 4 を繰り返します。

- AuthenticationManagerService
- EJB
- 電子メール
- JobManager
- WatchedFolder
- UsermanagerUtilService
- Remoting
- RemoteEvents
- RepositoryProviderService
- EMCDocumentumRepositoryProvider
- IBMFilenetRepositoryProvider
- FormAugmenter

- TaskManagerService
- TaskManagerConnector
- TaskManagerQueryService
- TaskQueueManager
- TaskEndpointManager
- LCMTMInvoker
- UserService
- WorkspaceSearchTemplateService
- WorkspaceSignleSignOn
- WorkspacePropertyService
- OutputService
- FormsService

これらのサービスをリモート起動できるようする場合は、匿名アクセスを無効にすることを考慮してください。そうしないと、これらのサービスにネットワークアクセス可能な任意の呼び出し元が、有効な資格情報を渡さずにサービスを起動するおそれがあります。

匿名アクセスは、必要でないサービスでは無効にすることをお勧めします。内部サービスは、原則的にシステム内のすべてのユーザーが認証なしで呼び出せる必要があるので、多くの場合、内部サービスでは匿名認証を有効にする必要があります。

4.1.3 サンプルのユーザーとロールアサインの削除

AEM forms をインストールしたときの指定内容によっては、サンプルのユーザーやロールが作成されている可能性があります（Kel Varsen、Finance Corp ユーザードメインなど）。User Management の管理ページを使用して、これらのユーザードメインとロールのサンプルを削除してください。

4.1.3.1 サンプルユーザーの削除

1 Web ブラウザーに次の URL を入力して管理コンソールにログインします。

```
http://[host name]:[port]/adminui
```

2 **設定**／**User Management**／**ユーザーとグループ**をクリックします。

3 **およびドメイン**リストからサンプル組織を選択して「**検索**」をクリックします。

4 すべてのサンプルユーザーを無効にするには、リスト内でそれぞれの横にあるチェックボックスを選択して、「**削除**」をクリックします。

4.1.3.2 サンプルドメインの削除

1 Web ブラウザーに次の URL を入力して管理コンソールにログインします。

```
http://[host name]:[port]/adminui
```

2 **設定**／**User Management**／**ドメイン管理**をクリックします。

3 すべてのサンプルドメインを削除するには、リスト内でそれぞれの横にあるチェックボックスを選択して、「**削除**」をクリックします。

4 「**保存**」をクリックします。

4.1.4 デフォルトグローバルタイムアウトの変更

エンドユーザーが AEM forms に対して認証を行う手段としては、Workbench、AEM forms Web アプリケーション、および、AEM forms サーバーサービスを呼び出すカスタムアプリケーションがあります。グローバルタイムアウト設定を使用すると、再認証を要求されるまでにユーザーが（SAML ベースアサーションを使用して）AEM forms とやり取りできる時間を指定することができます。デフォルト設定は 2 時間です。実稼働環境では、この時間を、設定可能な分単位の最小値に変更する必要があります。

4.1.4.1 再認証時間制限の最小化

1 Web ブラウザーに次の URL を入力して管理コンソールにログインします。

```
http://[host name]:[port]/adminui
```

2 **設定／ User Management ／設定／既存の設定ファイルの読み込みと書き出し**をクリックします。

3 「**書き出し**」をクリックして、既存の AEM forms の設定を含んだ config.xml ファイルを生成します。

4 エディターで XML ファイルを開き、次のエントリを見つけます。

```
<entry key="assertionValidityInMinutes" value="120"/>
```

5 値を 5（分単位）より大きい任意の数に変更し、ファイルを保存します。

6 管理コンソールで、既存の設定ファイルの読み込みと書き出しページに戻ります。

7 変更された config.xml ファイルへのパスを入力するか、「参照」をクリックしてこのファイルに移動します。

8 「**読み込み**」をクリックし、変更された config.xml ファイルをアップロードして、「**OK**」をクリックします。