LiveCycle® ES2 の堅牢化とセキュリティ

Adobe® LiveCycle® ES2

バージョン 9

2010 年 9 月 24 日

© 2010 Adobe Systems Incorporated and its licensors. All rights reserved.

Adobe® LiveCycle® ES2 の堅牢化とセキュリティ
2010 年 9 月 24 日

This reference guide is licensed for use under the terms of the Creative Commons Attribution Non-Commercial 3.0 License. This License allows users to copy, distribute, and transmit the guide for noncommercial purposes only so long as (1) proper attribution to Adobe is given as the owner of the guide; and (2) any reuse or distribution of the guide contains a notice that use of the guide is governed by these terms. The best way to provide notice is to include the following link.To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/.

Adobe, the Adobe logo, Adobe Reader, Acrobat, Flash, and LiveCycle are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. IBM and AIX trademarks of International Business Machines Corporation in the United States, other countries, or both. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Oracle, Java, Sun, and Solaris are trademarks or registered trademarks of Oracle and/or its affiliates. Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries. SUSE is a registered trademark of Novell, Inc. in the United States and other countries.UNIX is a registered trademark of The Open Group in the US and other countries. All other trademarks are the property of their respective owners.

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

目次

このドキュメントの内容 5
このドキュメントの対象読者 5
このガイドで使用する表記 5
関連情報 6
1 セキュリティに関する一般的な考慮事項 7
ベンダー固有のセキュリティ情報 7
オペレーティングシステムのセキュリティ情報 7
アプリケーションサーバーのセキュリティ情報 8
データベースのセキュリティ情報 8
デフォルト以外の HTTP ポートを使用するための JBoss の設定 9
LiveCycle ES2 のセキュリティに関する考慮事項 10
データベース内の電子メールの秘密鍵証明書は暗号化されない 10
データベース内の機密性の高い LiveCycle Rights Management ES2 の情報 11
adobe-ds.xml 内の平文形式のパスワード 11
2 環境の堅牢化 12
インストール前 12
ネットワーク層のセキュリティ 13
オペレーティングシステムのセキュリティ 14
インストール 14
インストール後の手順 15
LiveCycle ES2 サーバーのセキュリティ 15
LiveCycle Content Services ES2 ユーザーデータのチェックイン容量の制限 18
アプリケーションサーバーのセキュリティ 20
JBoss での JMX コンソールの使用 21
データベースのセキュリティ 21
Windows 上での統合セキュリティの設定 21
データベース内の機密性の高い情報の保護 23
LDAP のセキュリティ 23
監査とログ 24
LiveCycle ES2 UNIX システムライブラリの依存関係 24
Convert PDF サービス 24
XMLForms 25
社外にアクセスするための LiveCycle ES2 の設定 27
Web アクセスのリバースプロキシの設定 27
ネットワーク設定の保護 29
LiveCycle ES2 物理アーキテクチャ 29
LiveCycle ES2 で使用されるネットワークプロトコル 30
アプリケーションサーバーのポート 31
SSL の設定 32
SSL リダイレクトの設定 32
Windows 固有のセキュリティに関する推奨事項 33
JBoss サービスアカウント 33
ファイルシステムのセキュリティ 34
JBoss 固有のセキュリティに関する推奨事項 34
JBoss 管理コンソールおよび JMX コンソール 34
ディレクトリ参照の無効化 34

WebLogic 固有のセキュリティに関する推奨事項 35
ディレクトリ参照の無効化 35
WebLogic SSL ポートの有効化 35
WebSphere 固有のセキュリティに関する推奨事項 35
ディレクトリ参照の無効化 35
WebSphere 管理セキュリティの有効化 35
3 管理者設定のセキュリティ保護 36
サービスへの不要なリモートアクセスの無効化 36
サービスへの不要な匿名アクセスの無効化 37
サンプルのユーザーとロールアサインの削除 38
デフォルトグローバルタイムアウトの変更 39
LiveCycle 7.x 下位互換性 API アクセスの無効化 39

このドキュメントの内容

このガイドでは、Adobe® LiveCycle® ES2（Adobe LiveCycle Enterprise Suite 2）実稼働環境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。

LiveCycle ES2 に関するその他のセキュリティ情報については、LiveCycle デベロッパーセンターを参照してください。

LiveCycle ES2 のセキュリティ情報と速報については、「セキュリティ情報」サイトを参照してください。

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 LiveCycle ES2 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

このガイドで使用する表記

このガイド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
[LiveCycle ES2 root]	C:¥Adobe¥Adobe LiveCycle ES2¥	すべての LiveCycle ES2 ソリューションコンポーネントで使用するインストールディレクトリ。このディレクトリには、LiveCycle Configuration Manager、LiveCycle ES2 SDK、およびインストールされた各 LiveCycle ES2 ソリューションコンポーネントがサブディレクトリに分かれて格納されています。
[JBoss_ES2 root]	C:¥Adobe¥Adobe LiveCycle ES2¥jboss	LiveCycle ES2 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。

関連情報

次の表に、LiveCycle ES2 の学習に役立つ情報を示します。

情報	参照先
LiveCycle ES2、ソリューションコンポーネントおよび開発ツール	LiveCycle ES2 の概要
LiveCycle ES2 のインストールまたはアップグレードのための環境の準備	LiveCycle ES2 のインストールの準備 LiveCycle ES2 へのアップグレードの準備
LiveCycle ES2 のインストール	LiveCycle ES2 のインストールおよびデプロイ（JBoss 版） LiveCycle ES2 のインストールおよびデプロイ（WebSphere 版） LiveCycle ES2 のインストールおよびデプロイ（WebLogic 版）
自動オプション以外の方法を使用した LiveCycle ES2 へのアップグレード	LiveCycle ES2 へのアップグレード（JBoss 版） LiveCycle ES2 へのアップグレード（WebSphere 版） LiveCycle ES2 へのアップグレード（WebLogic 版）
LiveCycle Workbench ES2 のインストール	Installing Your Development Environment
LiveCycle ES2 の一般的な管理タスクの実行	LiveCycle ES2 管理ヘルプ
LiveCycle ES2 に統合できる他のサービスや製品	Adobe LiveCycle ES2
現在のバージョンに関するパッチアップデート、テクニカルノートおよび追加情報	LiveCycle テクニカルサポート
LiveCycle ES2 の用語	LiveCycle ES2 用語集

1 セキュリティに関する一般的な考慮事項

この節には、LiveCycle ES2 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、LiveCycle ES2、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の前提条件など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。

ベンダー固有のセキュリティ情報

この節には、LiveCycle ES2 エンタープライズ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の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。

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

LiveCycle ES2 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 SP 2 （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	『Windows Server 2003 セキュリティガイド』（www.microsoft.com）を検索
Microsoft Windows Server® 2008 Enterprise Edition、Standard Edition	『Windows Server 2008 セキュリティガイド』（www.microsoft.com）を検索
Microsoft Vista™ SP1、すべてのフレーバー、32 ビットおよび 64 ビット（実稼働環境以外の場合のみ）	『Windows Vista セキュリティガイド』（www.microsoft.com）を検索
Red Hat® Linux® AP または ES	Red Hat Enterprise Linux セキュリティガイド
Sun Solaris 10	Solaris のシステム管理（セキュリティサービス）
SUSE™ Linux® Enterprise Server 10.0	Linux Security

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

LiveCycle ES2 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® 10g R3	『Understanding WebLogic Security』（http://download.oracle.com/docs/）を検索
IBM WebSphere® 6.1 または 7.0	Securing applications and their environment（バージョン 6.1） Securing applications and their environment（バージョン 7.0）
Red Hat® JBoss® 4.2.0 または 4.2.1	Security on JBoss

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）

LiveCycle ES2 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
Microsoft SQL Server 2005 SP2 または 2008	SQL Server 2005: Security SQL Server 2008: Security

データベース	セキュリティ情報
MySQL 5	MySQL 5.0 General Security Issues MySQL 5.1 General Security Issues
Oracle® 10g または 11g	Security Considerations and Requirements（バージョン 10g） 「Oracle 11g Documentation Library」のセキュリティの章を参照

次の表では、LiveCycle ES2 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 LiveCycle ES2 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 Server	7001
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。

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 では、8080 をデフォルトの HTTP ポートとして使用します。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上にある場合は、以下の手順にしたがって LiveCycle ES2 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で開きます。

   JBoss の自動インストール：[JBossES2 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-bin
dings.xml</attribute>
     <attribute name="StoreFactoryClassName">
       org.jboss.services.binding.XMLServicesStoreFactory
     </attribute>
   </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. [JBossES2 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。

LiveCycle ES2 のセキュリティに関する考慮事項

この節では、理解しておく必要のある LiveCycle ES2 固有のセキュリティ情報について記載しています。

データベース内の電子メールの秘密鍵証明書は暗号化されない

LiveCycle ES2 アプリケーションに保存されている電子メールの秘密鍵証明書は、LiveCycle ES2 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。

データベース内の機密性の高い LiveCycle Rights Management ES2 の情報

LiveCycle ES2 は、LiveCycle ES2 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。

adobe-ds.xml 内の平文形式のパスワード

LiveCycle ES2 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、データソース設定ファイルにデータベースのパスワードを平文で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、パスワードが平文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： LiveCycle ES2 JBoss 自動インストーラ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 環境の堅牢化

この節では、LiveCycle ES2 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。代わりに、この節では、企業のイントラネット内で実行する LiveCycle ES2 のセキュリティを強化するために実装する必要のある様々なセキュリティの堅牢化設定について説明します。LiveCycle ES2 アプリケーションサーバーを確実に保護するには、セキュリティの監視、検出および応答のプロシージャを実装する必要があります。

この節では、インストールおよび設定段階で、次に示すタイミングで適用する堅牢化の方法について説明します。

インストール前：この方法は、LiveCycle ES2 ソフトウェアのインストールの前に使用します。

インストール：この方法は、LiveCycle ES2 ソフトウェアのインストールプロセス中に使用します。

インストール後： この方法は、インストール終了後と、それ以降に定期的に使用します。

LiveCycle ES2 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。

インストール前

LiveCycle ES2 のインストール前に、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。この節では、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

LiveCycle ES2 のインストールまたは設定には、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ため、/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 LiveCycle ES2 をインストールする場合、または LiveCycle PDF Generator ES2 をインストールする場合は、Windows へのインストールを管理者として実行する必要があります。また、PDF Generator ES2 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 LiveCycle ES2 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。

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。この節では、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）	LiveCycle ES2 サーバーを非武装地帯（DMZ）にデプロイします。LiveCycle ES2 を実行する、ファイアウォールの内側に配置された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	LiveCycle ES2 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。 **警告：** データベースポートを変更すると、LiveCycle ES2 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、LiveCycle ES2 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。 LiveCycle ES2 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版の『LiveCycle ES2 のインストールおよびデプロイ』または『LiveCycle ES2 へのアップグレード』（「Adobe LiveCycle ES2 ドキュメンテーション」）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

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ため、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、LiveCycle ES2 サーバーの時間は正確に設定する必要があります。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、「オペレーティングシステムのセキュリティ情報」（7 ページ）を参照してください。

インストール

この節では、LiveCycle ES2 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にログインします。Windows では、「別のユーザーとして実行」コマンドを使用して、管理者ユーザーとして LiveCycle ES2 インストーラ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 LiveCycle ES2 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。Adobe DVD または信頼できるソースからのみ LiveCycle ES2 をインストールするようにしてください。

問題	説明
ディスクのパーティション	LiveCycle ES2 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、LiveCycle ES2 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計画してください （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。
下位互換性	デプロイメントで必要な場合を除き、LiveCycle 7.x の下位互換性を有効にしないでください。

インストール後の手順

LiveCycle ES2 のインストールを完了したら、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 LiveCycle ES2 サーバーを保護するための、各種の推奨タスクを詳細に説明します。

LiveCycle ES2 サーバーのセキュリティ

次の推奨設定は、管理 Web アプリケーションの外にある LiveCycle ES2 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 LiveCycle ES2 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、先にテストしてから適用し、LiveCycle ES2 アプリケーションの互換性と可用性を確保してください。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。
LiveCycle ES2 アップデートは「Enterprise products download」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）

LiveCycle ES2 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。

LiveCycle ES2 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、LiveCycle ES2 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てください。
   - 「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 ES2 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. JBoss for Adobe LiveCycle ES2 サービスをダブルクリックして、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. LiveCycle ES2 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、LiveCycle ES2 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。
8. LiveCycle ES2 アプリケーションサーバーサービスを起動します。

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

LiveCycle 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、LiveCycle ES2 データベースのブートストラップを実行します。LiveCycle 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ため、権限のあるユーザーのセキュリティは確保されていません。LiveCycle Configuration Manager がサーブレットを使用して LiveCycle ES2 の設定を完了したら、このサーブレットを無効にする必要があります。

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

LiveCycle Configuration Manager を使用して、LiveCycle Reader Extensions ES2 の秘密鍵証明書を LiveCycle ES2 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 秘密鍵証明書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、LiveCycle Configuration Manager を使用して使用権限秘密鍵証明書のアップロードを完了した後、またはそれ以降の秘密鍵証明書の管理を LiveCycle 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。

「サービスへの不要なリモートアクセスの無効化」（36 ページ）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 LiveCycle ES2 サービスには、匿名の呼び出しによって起動する操作があります。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、「サービスへの不要な匿名アクセスの無効化」（37 ページ）の手順に従って、アクセスを無効にしてください。

管理者パスワードの変更

LiveCycle ES2 をインストールしたら、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、LiveCycle Configuration Manager を使用して直ちに変更してください。

➤ **デフォルトの管理者パスワードを変更するには**

1. Web ブラウザに次の 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 Super Administrator 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。

実稼働環境における 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。

➤ **WSDL の生成を無効にするには**

1. Web ブラウザに次の 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。

LiveCycle Content Services ES2 ユーザーデータのチェックイン容量の制限

デフォルトでは、Content Services ES2 はユーザーが一度にサーバーにチェックインできるデータの容量を制限しません。大量のデータは、他の操作を実行するためのシステムリソースが不足するため、システムにとって脅威となることがあります。このような状況が原因で、他の受信プロセスに対してサービス拒否が起きる可能性があります。Content Services ES2 での容量の管理を有効にするには、JVM 引数を使用します。

警告： これらの JVM 引数は、ユーザーを同期する前に渡す必要があります。ユーザーを同期すると、このユーザーの容量は変更できません。

➤ **Content Services ES2 上での容量管理の有効化：**

JBoss の場合

1. [jboss root]/bin ディレクトリに移動して、テキストエディタでスタートアップスクリプトを開きます。
   - °（**Windows**）run.bat
   - °（**Linux および UNIX**）run.sh

2. `Set JAVA_OPTS` 引数の下に次のプロパティを追加します。

   `-Dsystem.usages.enableQuotaSize=true -Dsystem.usages.quota=[サイズ（KB）]`

3. ファイルを保存して閉じます。

4. ユーザーを同期する前に JBoss サーバーを再起動します。

WebLogic の場合

1. WebLogic Server Administration Console にアクセスして、Web ブラウザの URL 行に http://[host name]:[port]/console と入力します。ここで、[port] は、安全ではないリスニングポートです。デフォルトでは、このポート番号は 7001 です。

2. ログイン画面で、WebLogic ユーザー名とパスワードを入力して「Log In」をクリックします。

3. Change Center で、「Lock & Edit」をクリックします。

4. 「Domain Structure」で、Environment ／ Servers をクリックし、右側のウィンドウで、管理対象サーバー名をクリックします。

5. Settings for Server ウィンドウで、「Configuration」タブ／「Server Start」タブをクリックします。

6. 「Arguments」ボックスに、以下の引数をスペースで区切って入力します。

   `-Dsystem.usages.enabled=true`

   `-Dsystem.usages.quota=[サイズ（KB）]`

7. 「Save」をクリックし、「Activate Changes」をクリックします。

8. ユーザーを同期する前に WebLogic サーバーを再起動します。

WebSphere の場合

1. WebSphere Administrative Console のナビゲーションツリーで、アプリケーションサーバーに対して次の操作を実行します。

   （WebSphere 6.x）Servers ／ Application servers をクリックします。

   （WebSphere 7.x）Servers ／ Server Types ／ WebSphere Application Servers をクリックします。

2. 右側のウィンドウで、サーバー名をクリックします。

3. 「Server Infrastructure」で、Java and Process Management ／ Process Definition をクリックします。

4. 「Additional Properties」で、「Java Virtual Machine」をクリックします。

5. 「Generic JVM arguments」ボックスで、`-Dsystem.usages.enableQuotaSize=true` および `-Dsystem.usages.quota=<`サイズ（KB）`>` をカンマで区切って、既存のプロパティに追加します。

6. 「OK」または「Apply」をクリックし、「Save directly to master configuration」をクリックします。

7. ユーザーを同期する前に WebSphere サーバーを再起動します。

アプリケーションサーバーのセキュリティ

次の表では、LiveCycle ES2 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 LiveCycle ES2 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。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。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。LiveCycle 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>`

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 LiveCycle ES2 をインストールしていて、自動インストールに含まれていた 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。

➤ **JBoss JMX コンソールを有効にするには**

1. JBoss.org サイトから、JBoss 4.2.0（またはそれ以降）をダウンロードします。
2. JBoss Application Server 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 [JBoss root]/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

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、LiveCycle ES2 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。その他のデータベースにおける要件については、『LiveCycle ES2 のインストールの準備』を参照してください。

Windows 上での統合セキュリティの設定

この節の説明は、Windows Server で実行している SQL サーバーデータベースおよび LiveCycle ES2 を対象としています。

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 ドライバを使用している場合は設定できません。

➤ **統合セキュリティを使用して、JBoss 上の SQL Server との信頼できる接続を確保するには**

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の Windows システムパスに sqljdbc_auth.dll を追加します。sqljdbc_auth.dll ファイルは、Microsoft SQL JDBC 1.2 ドライバ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 Adobe LiveCycle ES2）のログオンプロパティを、ローカルシステムから、LiveCycle ES2 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。

➤ 統合セキュリティを使用して、WebLogic 上の SQL Server との信頼できる接続を確保するには

1. Web ブラウザの URL 行に次の URL を入力して WebLogic Server Administration Console 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の Windows システムパスに sqljdbc_auth.dll を追加します。sqljdbc_auth.dll ファイルは、Microsoft SQL JDBC 1.2 ドライバ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。

➤ 統合セキュリティを使用して、WebSphere 上の SQL Server との信頼できる接続を確保するには

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、右側のペインで「IDP_DS」をクリックします。

3. 右側のペインの「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、右側のペインで「RM_DS」をクリックします。

6. 右側のペインの「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 ドライバのインストールディレクトリ（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 < バージョン > - < ノード >）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。

データベース内の機密性の高い情報の保護

LiveCycle ES2 データベーススキーマには、システム設定と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ため、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、LiveCycle ES2 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 ES2 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、「データベースのセキュリティ情報」（8 ページ）を参照してください。

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の情報ソースとして、またパスワード認証の手段として LiveCycle ES2 に使用されます。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 LiveCycle ES2 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。

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、LiveCycle ES2 への認証でユーザーが繰り返しエラーになったときに、LiveCycle ES2 がロックアウトを実行します。LiveCycle 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 LiveCycle ES2 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。

➤ 自動アカウントロックを設定するには

1. LiveCycle 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。

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	適切な LiveCycle ES2 ログファイルをアクセス制御リスト（ACL）に設定してください。 適切な秘密鍵証明書を設定することで、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。LiveCycle ES2 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 LiveCycle ES2 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に対してパスワード推測攻撃が行われた場合などに役立ちます。

LiveCycle ES2 UNIX システムライブラリの依存関係

以下の情報は、UNIX 環境での LiveCycle ES2 のデプロイメントを計画する際に役立ちます。

Convert PDF サービス

LiveCycle ES2 に含まれている Convert PDF サービスには、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 (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)
```

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

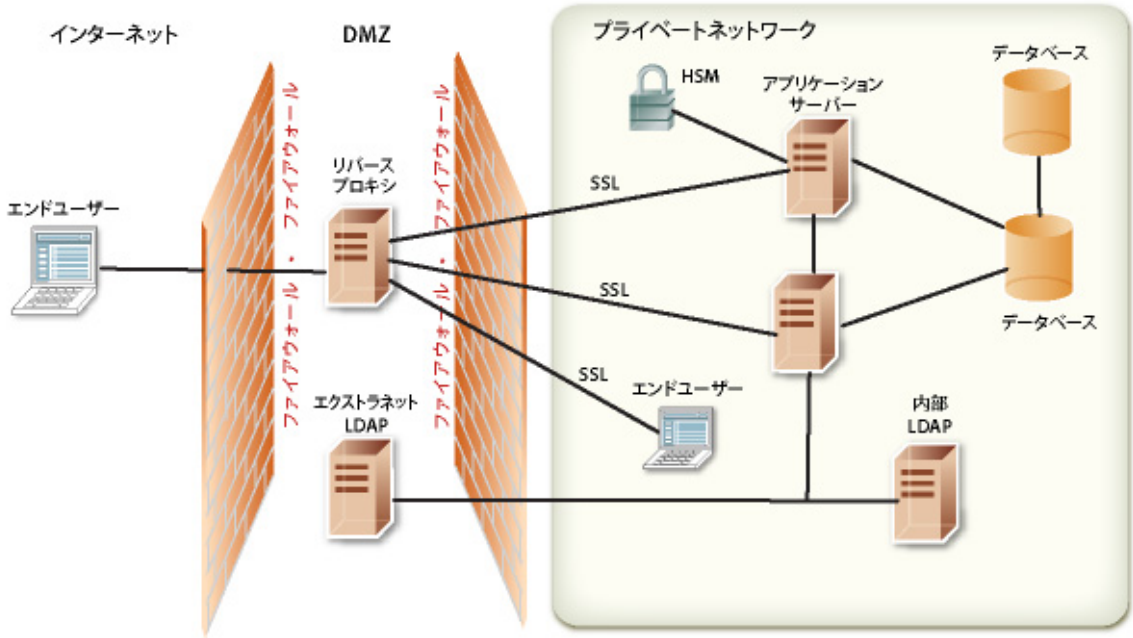
```
/usr/lib/
   libpthread.a(shr_comm.o)
   libpthread.a(shr_xpg5.o)
   libc.a(shr.o)
   librtl.a(shr.o)
   libdl.a(shr.o)
   libX11.a(shr4.o)
   libiconv.a(shr4.o)
   libpthreads.a(shr_comm.o)
/unix
   /usr/lib/libcrypt.a(shr.o)
   /usr/lib/libIM.a(shr.o)
   /usr/lib/libpthreads.a(shr_xpg5.o)
```

社外にアクセスするための LiveCycle ES2 の設定

LiveCycle ES2 のインストールを完了したら、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。この節では、LiveCycle ES2 実稼働サーバーのセキュリティを維持するにあたり、推奨するタスクについて説明します。

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、LiveCycle ES2 Web アプリケーションの URL のセットを、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、LiveCycle ES2 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、LiveCycle ES2 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ため、リバースプロキシに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 LiveCycle ES2 ルート URL

次のアプリケーションルート URL は、各 LiveCycle ES2 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。LiveCycle 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 ドキュメントの使用権限を適用する LiveCycle Reader Extensions ES2 エンドユーザー Web アプリケーション	有	可
/edc/*	LiveCycle Rights Management ES2 エンドユーザー Web アプリケーション	有	可
/edcws/*	Rights Management ES2 用の Web サービス URL	無	有
/pdfgui/*	LiveCycle PDF Generator ES2 管理 Web アプリケーション	有	可
/workspace/*	LiveCycle Workspace ES2 エンドユーザー Web アプリケーション	有	可
/workspace-server/*	Workspace ES2 クライアントアプリケーションが必要とする LiveCycle Workspace ES2 サーブレットおよびデータサービス	有	可
/contentspace/*	LiveCycle Contentspace ES2 エンドユーザー Web アプリケーション	有	可
/adobe-bootstrapper/*	LiveCycle ES2 リポジトリのブートストラップを実行するサーブレット	無	不可
/adobe-lcm-boot strapper/*	ブートストラップサーブレットへリダイレクト、または LiveCycle 7.x 形式のブートストラップ要求を /adobebootstrapper/ にリダイレクト	無	不可
/soap/*	LiveCycle ES2 Web サービスの情報ページ	無	不可
/soap/services/*	すべての LiveCycle ES2 サービス用の Web サービス URL	無	不可
/edc/admin/*	LiveCycle Rights Management ES2 管理 Web アプリケーション	有	不可
/adminui/*	LiveCycle 管理コンソールのホームページ	有	不可
/TruststoreComponent/ secured/*	Trust Store Management 管理ページ	有	不可
/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 ES2 IVS アプリケーション	有	不可
/OutputIVS/adminui/ secured/admin/*	HTML のイメージを取得するための Output ES2 IVS 管理ページ	有	不可
/OutputAdmin/*	LiveCycle Output ES2 管理ページ	有	不可
/FormServer/*	LiveCycle Forms ES2 Web アプリケーションファイル	有	不可
/FormServer/GetImage Servlet	HTML 変換時に、JavaScript の取得に使用	無	不可

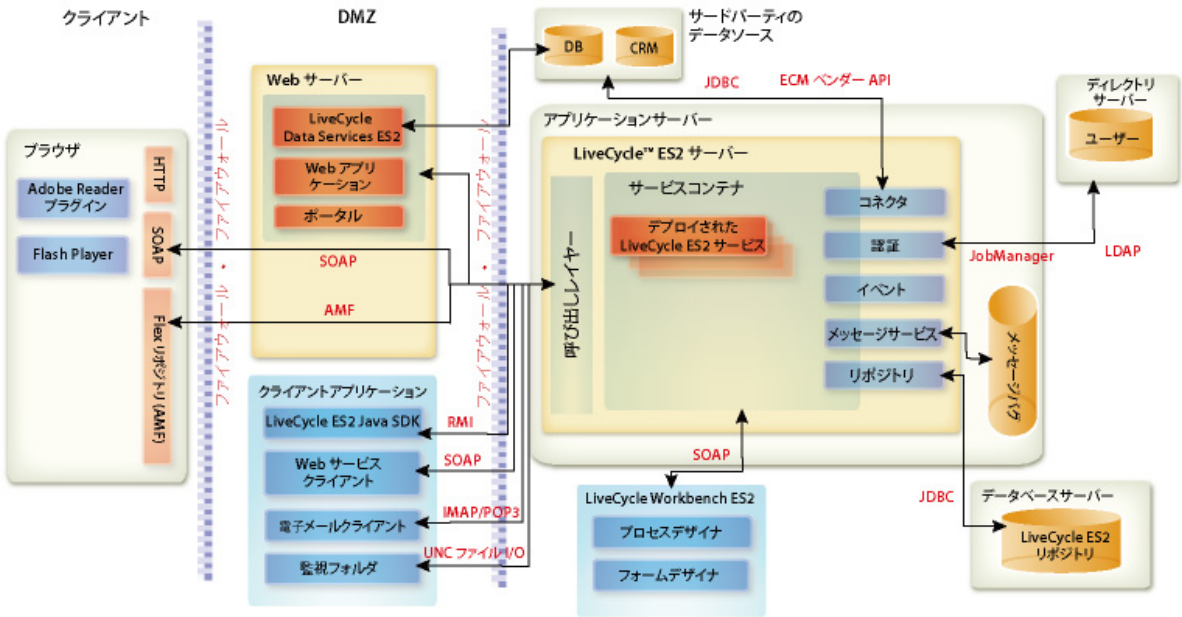
ルート URL	用途および関連する Web アプリケーション	Web ベースの インターフェイス	エンド ユーザー アクセス
/FormServerAdmin/*	LiveCycle Forms ES2 管理ページ	有	不可
/repository/*	WebDAV（デバッグ）アクセス用の URL	有	不可
/appstore/Forms/*	互換性：LiveCycle Form Manager 7.x WebDAV のクライアントのリポジトリ WebDAV 実装へのリダイレクト	無	不可
/AACComponent/*	アプリケーションおよびサービスユーザーインターフェイス	有	不可
/WorkspaceAdmin/*	LiveCycle Workspace ES2 管理ページ	有	不可
/rest/*	残りのサポートページ	有	不可
/CoreSystemConfig/*	LiveCycle ES2 Core 設定ページ	有	不可
/um/*	User Management 管理インターフェイス	有	不可

ネットワーク設定の保護

この節では、LiveCycle ES2 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内に LiveCycle ES2 をデプロイするための推奨事項を示します。

LiveCycle ES2 物理アーキテクチャ

次の図に、代表的な LiveCycle ES2 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。



LiveCycle ES2 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 LiveCycle ES2 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	用途
HTTP	● LiveCycle 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に表示する ● すべての SOAP 接続
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 LiveCycle ES2 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 LiveCycle ES2 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 LiveCycle ES2 SDK によって呼び出される ● LiveCycle Workbench ES2 設計環境
RMI	Enterprise JavaBeans（EJB）モードで使用された場合に LiveCycle ES2 SDK によって呼び出される
IIOP	LiveCycle 7.x アプリケーション（PDF Manipulation Module API）が CORBA 下位互換性層を介して LiveCycle ES2 サービスを呼び出す
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を LiveCycle ES2 の監視フォルダで監視する（監視フォルダエンドポイント）
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 ● 内部アクセス LiveCycle ES2 リポジトリ
WebDAV	任意の WebDAV クライアントによる LiveCycle ES2 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	LiveCycle ES2 サービスが Remoting 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	JMX を使用した監視用の MBeans を LiveCycle ES2 が公開する

アプリケーションサーバーのポート

この節では、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。これらのポートは、LiveCycle ES2 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、ファイアウォールの内側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

目的	ポート
Web アプリケーションへのアクセス	[JBoss root]/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
LiveCycle ES2 サービスへのアクセス	[JBoss root]/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	[JBoss root]/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	[JBoss root]/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 [JBoss root]/server/all/deploy/snmp-adaptor.sar/managers.xml ポート 1162

WebLogic ポート

目的	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
LiveCycle ES2 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 ● ノードマネージャリスンポート：デフォルトは 5556

WebSphere 6.1 ポート

LiveCycle ES2 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

LiveCycle ES2 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。

SSL の設定

「LiveCycle ES2 物理アーキテクチャ」（29 ページ）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ついて SSL を設定する必要があります。特に、ネットワーク上にユーザーの秘密鍵証明書が公開されないように、すべての SOAP 接続を SSL 経由で行う必要があります。

JBoss、WebLogic および WebSphere 上で SSL を設定する手順については、LiveCycle ES2 管理ヘルプの「SSL の設定」を参照してください。

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、LiveCycle ES2 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。

➤ JBoss で SSL リダイレクトを設定するには

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>:
```

Windows 固有のセキュリティに関する推奨事項

この節では、LiveCycle ES2 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。

JBoss サービスアカウント

LiveCycle ES2 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。

➤ **管理者以外の固有のアカウントを使用して LiveCycle ES2 アプリケーションサーバーを実行するには**

1. Microsoft 管理コンソール（MMC）で、LiveCycle ES2 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てください。
   - 「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. LiveCycle ES2 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、LiveCycle ES2 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、LiveCycle ES2 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. LiveCycle ES2 アプリケーションサーバーサービスを起動します。

ファイルシステムのセキュリティ

LiveCycle ES2 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に格納する

LiveCycle ES2 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。

JBoss 固有のセキュリティに関する推奨事項

この節では、LiveCycle ES2 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に関する推奨事項について説明します。

JBoss 管理コンソールおよび JMX コンソール

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 LiveCycle ES2 をインストールした時に設定されます。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。

ディレクトリ参照の無効化

LiveCycle 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_ES2 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>]
```

WebLogic 固有のセキュリティに関する推奨事項

この節では、LiveCycle ES2 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。

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>
```

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 Administration Console でこのポートを有効にしてください。

WebSphere 固有のセキュリティに関する推奨事項

この節では、LiveCycle ES2 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。

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。

WebSphere 管理セキュリティの有効化

➤ **WebSphere 管理セキュリティを有効にするには**

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。

3 管理者設定のセキュリティ保護

通常、開発者はアプリケーションのビルドとテストに LiveCycle ES2 実稼働環境を使用しません。そのため、プライベートな開発環境では必要であっても実稼働環境で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。

ここでは、LiveCycle ES2 の管理オプションを使用して、攻撃を回避する方法について説明します。

サービスへの不要なリモートアクセスの無効化

LiveCycle ES2 のインストールと設定を完了したら、SOAP、Enterprise JavaBeans™（EJB）および LiveCycle Remoting 経由で、多くの LiveCycle ES2 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指します。

LiveCycle ES2 サービスは、認証された呼び出し元に対して有効な秘密鍵証明書を要求しますが、リモートアクセスを許可するのは、リモートでのアクセスを可能にする必要のあるサービスのみに制限してください。アクセスを制限するには、まず、リモートアクセス可能なサービスを、システムを機能させるのに必要な最小限のサービスだけにします。その後、それ以外に必要なサービスをリモート起動できるようにします。

LiveCycle ES2 サービスは常に、最低でも SOAP アクセスを必要とします。これらのサービスは、通常は LiveCycle Workbench ES2 で使用するために必要とされますが、LiveCycle Workspace ES2 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。

LiveCycle 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。

➤ サービスに対するリモートアクセスを無効にするには

1. Web ブラウザに次の URL を入力して LiveCycle 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」リストから「EJB」を選択して、「フィルタ」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」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」リストから「SOAP」を選択して、「フィルタ」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

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」列に SOAP が表示されていることを確認してください。

サービスへの不要な匿名アクセスの無効化

一部の LiveCycle ES2 サービスは、一部の操作について、認証されていない（匿名）ユーザーによる起動を許可しています。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。

➤ サービスに対する匿名アクセスを無効にするには

1. Web ブラウザに次の URL を入力して LiveCycle 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
   - Email
   - 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、有効な秘密鍵証明書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ため、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。

サンプルのユーザーとロールアサインの削除

LiveCycle ES2 のインストール時に、サンプルのユーザーやロールを設定することがあります（Kel Varsen、Finance Corp ユーザードメインなど）。User Management 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。

➤ サンプルユーザーを削除するには

1. Web ブラウザに次の URL を入力して LiveCycle 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。

➤ サンプルドメインを削除するには

1. Web ブラウザに次の URL を入力して LiveCycle 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／ドメインの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。

デフォルトグローバルタイムアウトの変更

エンドユーザーは、LiveCycle Workbench ES2、LiveCycle ES2 Web アプリケーションまたは LiveCycle ES2 サービスを呼び出すカスタムアプリケーションを使用して LiveCycle ES2 に認証を試みることができます。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）LiveCycle ES2 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。

➤ 再認証時間制限に最小値を設定するには

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

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

2. LiveCycle 管理コンソールで、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 LiveCycle ES2 の設定を使用して config.xml ファイルを生成します。
4. エディタで 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. LiveCycle 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」をクリックして、変更された config.xml ファイルをアップロードし、「OK」をクリックします。

LiveCycle 7.x 下位互換性 API アクセスの無効化

LiveCycle 7.x SDK を使用して開発されたアプリケーションは、認証済みの EJB または SOAP 要求を使用して LiveCycle ES2 サービスを呼び出すことはありません。代わりに、アプリケーションにデプロイされた CORBA サービスに対する、保護されていない CORBA 呼び出しを作成します。

LiveCycle Configuration Manager のインストールおよび設定プロセスでアップグレードオプションを選択した場合、CORBA サービスがデプロイされます。CORBA サービスがアプリケーションサーバーにデプロイされると、LiveCycle 7.x SDK を使用して実行する、既存の LiveCycle 7.x アプリケーションが許可されます。アップグレードを選択しなかった場合、CORBA サービスはインストールされません。

➤ LiveCycle 7.x 下位互換性 CORBA サービスを無効にするには

1. [LiveCycle ES2 root]/jboss/deploy ディレクトリで、adobe-livecycle-[appserver].ear ファイルを探して、この EAR ファイルのバックアップコピーを作成します。
2. adobe-core-[appserver].ear ファイル内で、adobe-core-compat-7to8-[appserver].ear ファイルを探します。この EAR ファイルが存在するのは、アップグレードオプションを使用して LiveCycle ES2 設定とデプロイメントを実行した場合のみです。

3. adobe-core-compat-7to8-[appserver].ear ファイル内で、application.xml ファイルを探します。
4. application.xml ファイルを修正し、次のモジュールをコメントアウトします。

```
<!-- adobe-PDFManipulation start -->
<module id ="WebApp_PDFManipulation">
   <web>
   < web-uri>adobe-PDFManipulation.war</ web-uri>
   < context-root>/adobe-PDFManipulation</ context-root>
   </web >
</module >
```