



BEA WebLogic Server™

プロダクション環境の
セキュリティ

著作権

Copyright © 2003, BEA Systems, Inc. All Rights Reserved.

限定的権利条項

本ソフトウェアおよびマニュアルは、BEA Systems, Inc. 又は日本ビー・イー・エー・システムズ株式会社（以下、「BEA」といいます）の使用許諾契約に基づいて提供され、その内容に同意する場合にのみ使用することができ、同契約の条項通りにのみ使用またはコピーすることができます。同契約で明示的に許可されている以外の方法で同ソフトウェアをコピーすることは法律に違反します。このマニュアルの一部または全部を、BEA からの書面による事前の同意なしに、複写、複製、翻訳、あるいはいかなる電子媒体または機械可読形式への変換も行うことはできません。

米国政府による使用、複製もしくは開示は、BEA. の使用許諾契約、および FAR 52.227-19 の「Commercial Computer Software-Restricted Rights」条項のサブパラグラフ (c)(1)、DFARS 252.227-7013 の「Rights in Technical Data and Computer Software」条項のサブパラグラフ (c)(1)(ii)、NASA FAR 補遺 16-52.227-86 の「Commercial Computer Software--Licensing」条項のサブパラグラフ (d)、もしくはそれらと同等の条項で定める制限の対象となります。

このマニュアルに記載されている内容は予告なく変更されることがあり、また BEA. による責務を意味するものではありません。本ソフトウェアおよびマニュアルは「現状のまま」提供され、商品性や特定用途への適合性を始めとする（ただし、これらには限定されない）いかなる種類の保証も与えません。さらに、BEA は、正当性、正確さ、信頼性などについて、本ソフトウェアまたはマニュアルの使用もしくは使用結果に関していかなる確約、保証、あるいは表明も行いません。

商標または登録商標

BEA、Jolt、Tuxedo、および WebLogic は BEA Systems, Inc. の登録商標です。BEA Builder、BEA Campaign Manager for WebLogic、BEA eLink、BEA Manager、BEA WebLogic Commerce Server、BEA WebLogic Enterprise、BEA WebLogic Enterprise Platform、BEA WebLogic Express、BEA WebLogic Integration、BEA WebLogic Personalization Server、BEA WebLogic Platform、BEA WebLogic Portal、BEA WebLogic Server、BEA WebLogic Workshop、および How Business Becomes E-Business は、BEA Systems, Inc の商標です。

その他の商標はすべて、関係各社がその権利を有します。

プロダクション環境のセキュリティ

パート番号	マニュアルの日付	ソフトウェアのバージョン
なし	2003年2月7日	WebLogic Server バージョン 7.0

目次

このマニュアルの内容

対象読者.....	v
e-docs Web サイト.....	vi
このマニュアルの印刷方法.....	vi
サポート情報.....	vii
表記規則.....	vii

1. セキュリティ ニーズの確認

環境の理解.....	1-1
セキュリティ コンサルタントの採用または診断ソフトウェアの使用.....	1-2
セキュリティ 関連の公開資料の参照.....	1-2

2. プロダクション環境のセキュリティの確保

WebLogic Server ホストのセキュリティ対策.....	2-1
ネットワーク接続のセキュリティ対策.....	2-7
データベースのセキュリティ対策.....	2-9
WebLogic セキュリティ サービスのセキュリティ対策.....	2-10
アプリケーションのセキュリティ対策.....	2-16



このマニュアルの内容

このマニュアルでは、**WebLogic Server** をプロダクション環境にデプロイする前に検討すべき重要なセキュリティ対策について説明します。構成は次のとおりです。

- 第1章「セキュリティ ニーズの確認」は、**WebLogic Server** のデプロイメントに必要なセキュリティのレベルを判断するための質問と補足資料のリストを示します。
- 第2章「プロダクション環境のセキュリティの確保」は、プロダクション環境を侵入者から保護するために不可欠なセキュリティアクションのリストを示します。

対象読者

このマニュアルでは、**WebLogic Server** に直接関連するセキュリティ上の問題に焦点を当てます。プロダクション環境のオペレーティング システム、ネットワーク機器、データベース、およびハードウェアが、追加的な対策を講じて保護されていることを前提としています。

このマニュアルは、アプリケーション設計者、アプリケーション管理者、およびサーバ管理者を対象としています。

アプリケーション設計者は、セキュリティの目標を設定し、組織の全体的なセキュリティ アーキテクチャを設計するだけでなく、**WebLogic Server** のセキュリティ機能を評価して最適な実装方法を判断します。アプリケーション設計者は、セキュリティ システムや最先端のセキュリティ技術とツールだけでなく、**Java** プログラミング、**Java** セキュリティ、およびネットワーク セキュリティにも精通しています。

アプリケーション管理者は、サーバ管理者と共同でセキュリティ コンフィグレーション、認証および認可方式を実装および管理したり、定義されたセキュリティ レベルでデプロイされたアプリケーション リソースへのアクセスを設定および管理したりします。アプリケーション管理者は、セキュリティの概念や

Java セキュリティ アーキテクチャの一般的な知識を持っています。アプリケーション管理者は、Java、XML、デプロイメント記述子を理解し、サーバ ログおよび監査ログでセキュリティ イベントを特定できます。

サーバ管理者は、アプリケーション設計者と連絡を密にし、サーバおよびそのサーバで動作するアプリケーションのセキュリティ方式を設計したり、セキュリティのリスクを特定したり、セキュリティ上の問題を阻止するセキュリティ コンフィグレーションを提案したりします。その他に、重要なプロダクションシステムの管理、セキュリティ レルムの設定とコンフィグレーション、サーバおよびアプリケーションリソースの認証および認可方式の実装、セキュリティ機能のアップグレード、およびセキュリティ プロバイダ データベースの管理も行う場合があります。サーバ管理者は、Web アプリケーションと EJB のセキュリティ、公開鍵のセキュリティ、および SSL を含む Java セキュリティ アーキテクチャに精通しています。

e-docs Web サイト

BEA 製品のドキュメントは、BEA の Web サイトで入手できます。BEA のホームページで [製品のドキュメント] をクリックします。

このマニュアルの印刷方法

Web ブラウザの [ファイル | 印刷] オプションを使用すると、Web ブラウザからこのマニュアルを一度に 1 章ずつ印刷できます。

このマニュアルの PDF 版は、WebLogic Server の Web サイトで入手できます。PDF を Adobe Acrobat Reader で開くと、マニュアルの全体 (または一部分) を書籍の形式で印刷できます。

Adobe Acrobat Reader は Adobe の Web サイト (<http://www.adobe.co.jp>) で無料で入手できます。

サポート情報

BEA のドキュメントに関するユーザからのフィードバックは弊社にとって非常に重要です。質問や意見などがあれば、電子メールで docsupport-jp@beasys.com までお送りください。寄せられた意見については、ドキュメントを作成および改訂する BEA の専門の担当者が直に目を通します。

電子メールのメッセージには、ご使用のソフトウェアの名前とバージョン、およびドキュメントのタイトルと日付をお書き添えください。本バージョンの BEA WebLogic Server について不明な点がある場合、または BEA WebLogic Server のインストールおよび動作に問題がある場合は、BEA WebSupport (www.bea.com) を通じて BEA カスタマ サポートまでお問い合わせください。カスタマ サポートへの連絡方法については、製品パッケージに同梱されているカスタマ サポートカードにも記載されています。

カスタマ サポートでは以下の情報をお尋ねしますので、お問い合わせの際はあらかじめご用意ください。

- お名前、電子メールアドレス、電話番号、ファクス番号
- 会社の名前と住所
- お使いの機種とコード番号
- 製品の名前とバージョン
- 問題の状況と表示されるエラー メッセージの内容

表記規則

このマニュアルでは、全体を通して以下の表記規則が使用されています。

表記法	適用
太字	用語集で定義されている用語を示す。

表記法	適用
[Ctrl] + [Tab]	複数のキーを同時に押すことを示す。
<i>斜体</i>	強調または書籍のタイトルを示す。
等幅テキスト	コードサンプル、コマンドとそのオプション、データ構造体とそのメンバー、データ型、ディレクトリ、およびファイル名とその拡張子を示す。等幅テキストはキーボードから入力するテキストも示す。 例： <pre>#include <iostream.h> void main () the pointer psz chmod u+w * \tux\data\ap .doc tux.doc BITMAP float</pre>
太字の等幅 テキスト	コード内の変数を示す。 例： <pre>void commit ()</pre>
<i>斜体の等幅</i> <i>テキスト</i>	コード内の変数を示す。 例： <pre>String <i>expr</i></pre>
すべて大文 字のテキス ト	デバイス名、環境変数、および論理演算子を示す。 例： <pre>LPT1 SIGNON OR</pre>
{ }	構文の中で複数の選択肢を示す。実際には、この括弧は入力しない。

表記法	適用
[]	<p>構文の中で任意指定の項目を示す。実際には、この括弧は入力しない。</p> <p>例：</p> <pre>buildobjclient [-v] [-o name] [-f file-list]... [-l file-list]...</pre>
	<p>構文の中で相互に排他的な選択肢を区切る。実際には、この記号は入力しない。</p>
...	<p>コマンドラインで以下のいずれかを示す。</p> <ul style="list-style-type: none"> ■ 引数を複数回繰り返すことができる。 ■ 任意指定の引数が省略されている。 ■ パラメータや値などの情報を追加入力できる。 <p>実際には、この省略符号は入力しない。</p> <p>例：</p> <pre>buildobjclient [-v] [-o name] [-f file-list]... [-l file-list]...</pre>
.	<p>コードサンプルまたは構文で項目が省略されていることを示す。実際には、この省略符号は入力しない。</p>



1 セキュリティ ニーズの確認

WebLogic Server および J2EE アプリケーションをプロダクション環境にデプロイする前に、以下の節で説明するように、セキュリティ ニーズを確認し、適切なセキュリティ対策が確実に行われるようにする必要があります。

- 1-1 ページの「環境の理解」
- 1-2 ページの「セキュリティ コンサルタントの採用または診断ソフトウェアの使用」
- 1-2 ページの「セキュリティ関連の公開資料の参照」

環境の理解

セキュリティ ニーズを明確に把握するために、次の質問の回答を検討してください。

- 保護対象とするリソースはどれか

プロダクション環境には、WebLogic Server がアクセスするデータベース内の情報、Web サイトの可用性、パフォーマンス、および整合性を始めとして、保護可能な数多くのリソースがあります。セキュリティのレベルを決める際に、保護するリソースを十分検討します。

- WebLogic サイトリソースを何から保護するのか

ほとんどの Web サイトリソースの場合は、インターネット上のすべてのユーザから保護しなければなりません。しかし、社内のイントラネット上で従業員から Web サイトを保護する必要がありますか。従業員が WebLogic Server 環境内のすべてのリソースにアクセスする必要がありますか。システム管理者がすべての WebLogic リソースにアクセスする必要がありますか。システム管理者はすべてのデータにアクセスできる必要がありますか。機密性の高いデータや重要なリソースへのアクセスは、十分に信頼できるごく一部のシステム管理者に限定した方がよい場合もあります。また、データやリ

ソースには、システム管理者がアクセスできないようにする方がよい場合もあります。

- 重要なリソースの保護に失敗した場合に何が起こるか

場合によっては、セキュリティ スキーマの欠点が簡単に見つけられても迷惑なだけということもあります。また、欠点が原因で、Web サイトを利用する会社や個人の顧客に大きな損害を与えることもあります。各リソースのセキュリティが失敗した場合の結果を理解しておく、適切な保護のレベルを判断する参考になります。

セキュリティ コンサルタントの採用または診断ソフトウェアの使用

インターネットまたはイントラネット上で WebLogic Server をデプロイする場合には、独立したセキュリティ専門家に依頼して、セキュリティ プランと手順を検討してもらい、インストール済みシステムの監査を受け、改善点のアドバイスを受けるとういでしょう。WebLogic Server のプロダクション環境の保護に役立つ、BEA パートナ提供のサービスおよび製品もあります。BEA パートナのページ (<http://beasys.instantsoft.com/partners/catalog.shtml>) を参照してください。

BEA パートナのページに加えて、BEA dev2dev の Web サイトには環境のセキュリティを評価するソフトウェアが用意されています。たとえば、PentaSafe VigilEnt Security Agent は、WebLogic Server アプリケーションの詳細なセキュリティ監査を提供し、コンフィグレーション、アクセス、および CGI-BIN の脆弱性をプロアクティブに識別します。アプリケーションを迅速に評価するには、30 日間無料の試用版を <http://dev2dev.bea.com/resourcelibrary/utilitiestools/security.jsp> からダウンロードしてください。

セキュリティ関連の公開資料の参照

セキュリティ問題に関する資料を参照してください。

- Web サーバのセキュリティ対策の最新情報については、カーネギーメロン大学が運営する CERT™ Coordination Center が公開している「**Security Improvement Modules, Security Practices, and Technical Implementations**」をお勧めします。
- BEA のセキュリティ勧告については、dev2dev Web サイト (<http://dev2dev.bea.com/advisories>) にある BEA の **Advisories & Notifications** ページを参照してください。このページでは、セキュリティ関連のパッチをダウンロードしたり、新しいセキュリティ勧告の通知を受けるよう登録したりできます。

BEA 製品に関するセキュリティ問題は、secalert@bea.com にご報告ください。

1 セキュリティ ニーズの確認

2 プロダクション環境のセキュリティの確保

プロダクション環境のセキュリティを確保するために、以下のアクションを実行することをお勧めします。

- 2-1 ページの「WebLogic Server ホストのセキュリティ対策」
- 2-7 ページの「ネットワーク接続のセキュリティ対策」
- 2-9 ページの「データベースのセキュリティ対策」
- 2-10 ページの「WebLogic セキュリティ サービスのセキュリティ対策」
- 2-16 ページの「アプリケーションのセキュリティ対策」

WebLogic Server ホストのセキュリティ対策

WebLogic Server のプロダクション環境は、それが動作しているマシンと同じレベルでしかセキュリティは確保されません。したがって、物理的なマシン、オペレーティング システム、およびホスト マシン上にインストールされたその他のすべてのソフトウェアをロックダウンすることが重要です。以下に、プロダクション環境の WebLogic Server ホストをロックダウンするためのアドバイスを示します。また、マシンおよびオペレーティング システムのベンダに推奨のセキュリティ対策を確認してください。

2 プロダクション環境のセキュリティの確保

表 2-1 WebLogic Server ホストのセキュリティ対策

セキュリティ アクション	説明
ハードウェアを物理的に保護する	ハードウェアは、無認可のユーザがデプロイメント用マシンやネットワーク接続に不用意に触れることがないように安全な場所に設置する。
オペレーティング システムの提供するネットワーク サービスを保護する	電子メール プログラムやディレクトリ サービスなどのネットワーク サービスを専門家に評価してもらい、悪意ある攻撃者がオペレーティング システムまたはシステムレベルのコマンドにアクセスできないことを確認する。 企業ネットワークの他のマシンとファイル システムを共有しない。
不正アクセスを防止できるファイル システムを使用する	各 WebLogic Server ホストのファイル システムで、保護対象リソースへの不正アクセスを防止できることを確認する。たとえば、Windows コンピュータ上では、NTFS のみを使用する。
ホスト マシンでユーザ アカウントの数を制限する	WebLogic Server ホストで複数のユーザ アカウントを作成することは避け、各アカウントに付与されるファイル アクセス特権を制限する。ホスト マシンでは、システム管理者特権を持つユーザ アカウント 1 つと、WebLogic Server を実行する十分な特権を持つユーザ 1 つが理想的。 アクティブなユーザ アカウントを定期的に再検討する。また、退職者があった場合にも見直す。 背景情報： WebLogic Server コンフィグレーション データの一部と Java Server Pages (JSP) および HTML ページを含む URL (Web) リソースの一部は、ファイル システム上にクリア テキストで保存される。ユーザまたは侵入者がファイルとディレクトリの読み込みアクセス権を持っていれば、WebLogic Server の認証および許可スキーマに施したセキュリティ メカニズムを破ることができる。
パスワードを保護する	プロダクション マシンでのユーザ アカウントのパスワードは推測しにくいものにし、注意深く保護される必要がある。 パスワードの有効期間が一定期間で切れるようにポリシーを設定する。 パスワードをクライアント アプリケーションにコーディングしないようにする。

2-2 プロダクション環境のセキュリティ

表 2-1 WebLogic Server ホストのセキュリティ対策

セキュリティ アクション	説明
各ホスト コンピュータで、1つのユーザ アカウントにのみ WebLogic リソースへのアクセス権を付与する	<p>各 WebLogic Server ホスト コンピュータでは、オペレーティング システムを使用して、WebLogic Server を実行できる特別なユーザ アカウント (<code>wls_owner</code> など) を確立する。</p> <p>このオペレーティング システム (OS) ユーザ アカウントに以下の特権を付与する。</p> <ul style="list-style-type: none"> • BEA ホーム ディレクトリ、WebLogic Server 製品ディレクトリ ツリー、およびドメイン ディレクトリのみへのアクセス特権。 <p>BEA ホーム ディレクトリとは共通ファイル用のリポジトリのことで、同じマシンにインストールされる複数の BEA 製品が使用する。WebLogic Server 製品 インストール ディレクトリには、プログラム ファイルを含む、システムにインストールする WebLogic Server ソフトウェア コンポーネントがすべて含まれる。ドメイン ディレクトリには、コンフィグレーション ファイル、セキュリティ ファイル、ログ ファイル、J2EE アプリケーション、および単一の WebLogic ドメイン用のその他の J2EE リソースが格納される。WebLogic Server のホスト コンピュータに複数のドメインをインストールする場合は、各ドメインディレクトリを保護する必要がある。</p> <p>デフォルトでは、BEA インストール プログラムはすべての BEA ファイルとドメインディレクトリを単一のディレクトリ ツリーに入れる。このツリーの最上位ディレクトリには、<code>bea</code> という名前が付けられる。WebLogic Server ファイルはすべて、このディレクトリ ツリーのサブディレクトリ (<code>bea\weblogic810</code>) となり、ドメイン ファイルは、別のサブディレクトリ (<code>bea\user_projects\domain1</code>、<code>bea\user_projects\domain2</code>、...) に入れられる。</p> <p>ただし、WebLogic Server 製品インストール ディレクトリおよびドメインディレクトリを BEA ホーム ディレクトリの外に置くこともできる。詳細については、『インストール ガイド』の「WebLogic Server インストールのディレクトリ選択」を参照。</p> <ul style="list-style-type: none"> ■ BEA ホーム ディレクトリ、WebLogic Server 製品ディレクトリ ツリー、およびドメイン ディレクトリ内での読み込み、書き込み、および実行特権を付与する。 <p>他の OS ユーザには BEA ファイルおよびドメイン ファイルに対する読み込み、書き込み、および実行のアクセス権を与えないこと。</p> <p>このセキュリティ対策を行うと、WebLogic Server と同じマシンで実行されている他のアプリケーションの BEA ファイルおよびドメイン ファイルへのアクセス機能を制限できる。このセキュリティ対策がない場合、他の一部のアプリケーションは書き込みアクセス権を得て、動的コンテンツを提供する JSP などのファイルに悪質な実行可能コードを挿入することができる。そのコードは、次にファイルがクライアントにサービスされるときに実行される。</p>

2 プロダクション環境のセキュリティの確保

表 2-1 WebLogic Server ホストのセキュリティ対策

セキュリティ アクション	説明
WebLogic Server の Windows サービスを特別な OS ユーザ アカウント下で実行する	<p>Windows プラットフォームでは、WebLogic Server インスタンスを Windows サービスとして実行できる。これにより、サーバインスタンスは Windows コンピュータを起動するたびに自動的に開始する。</p> <p>WebLogic Server インスタンスを Windows サービスとして実行するように設定するには、Windows レジストリを修正する特権を持つユーザアカウントで Windows コンピュータにログインする必要がある。詳細については、『管理者ガイド』の「WebLogic Server インスタンスの Windows サービスとしての設定」を参照。</p> <p>WebLogic Server インスタンスの Windows サービスとしての実行には、これらの管理者レベルの特権は不要である。その代わりに、Windows サービスは WebLogic Server を実行するために作成した特別な OS ユーザ アカウント下で実行しなければならない。</p> <p>WebLogic Server インスタンスが必ず特別な OS ユーザアカウント下で実行されるようにするには、Windows サービスの [プロパティ] ページでユーザ名およびパスワードを指定する。詳細については、『管理者ガイド』の「サービスを実行するユーザアカウントの確認」を参照。</p>

表 2-1 WebLogic Server ホストのセキュリティ対策

セキュリティ アクション	説明
UNIX 上で保護されているポートにバインドするには、ユーザ ID またはネットワークアドレス変換 (NAT) ソフトウェアの切り替えを行うよう、WebLogic Server をコンフィグレーションする	<p>UNIX システムでは、特権を付与されたユーザ アカウント (大概の場合は root) 下で実行されるプロセスのみが、1024 未満のポートにバインドできる。</p> <p>ただし、WebLogic Server のような長期にわたって実行されるプロセスは、これらの特権を付与されたアカウント下で実行してはならない。その代わりに、以下の処理のいずれかを行うことができる。</p> <ul style="list-style-type: none"> ■ 特権を付与されたポートにアクセスする必要のある各 WebLogic Server インスタンスについて、特権を付与されたユーザ アカウント下で起動し、特権を付与されたポートにバインドしてから、ユーザ ID を特権のないアカウントに変更するようサーバをコンフィグレーションする。 <p>サーバインスタンスの起動にノード マネージャを使用する場合は、セキュア ポート上でのみ、また単一の既知のホストのみから、要求を受け入れるようにノード マネージャをコンフィグレーションする。</p> <p>Administration Console オンライン ヘルプの「UNIX 上の保護されているポートへのバインディング」を参照。</p> <ul style="list-style-type: none"> ■ WebLogic Server インスタンスを特権を持たないアカウントから起動し、ネットワークアドレス変換 (NAT) ソフトウェアを使用して、保護されているポートを保護されないポートにマップするよう、ファイアウォールをコンフィグレーションする。BEA では NAT ソフトウェアの提供は行っていない。
プロダクション用マシン上では開発しない	<p>開発用マシン上でまず開発して、コードが完了し、テストしてから、プロダクション用マシンにコードを移植する。この手順を取ることで、開発環境のバグがプロダクション環境のセキュリティに影響するのを防止できる。</p>

2 プロダクション環境のセキュリティの確保

表 2-1 WebLogic Server ホストのセキュリティ対策

セキュリティ アクション	説明
開発およびサンプル ソフトウェアはプロダクション用マシンにインストールしない	<p>開発ツールはプロダクション用マシンにインストールしない。開発ツールをプロダクション用マシンに持ち込まないことで、侵入者が WebLogic Server のプロダクション用マシンに部分的にアクセスできた場合でも、悪用されるおそれが少なくなる。</p> <p>プロダクション用マシンに WebLogic Server サンプル アプリケーションをインストールしない。BEA インストール プログラム上で、標準インストールにするかカスタム インストールにするかを尋ねられた場合は、以下の操作を実行する。</p> <ol style="list-style-type: none">1. [カスタム インストール] を選択する。その後、[Next] をクリックする。2. [コンポーネントを選択] ページで、[Server Examples] チェックボックスからチェック マークをはずす。その後、[Next] をクリックする。3. BEA インストール プログラムの残りのページの操作を完了する。
セキュリティ監査を有効にする	<p>WebLogic Server が実行されるオペレーティング システムで、ファイルおよびディレクトリへのアクセスのセキュリティ監査がサポートされている場合は、監査ログを使用して、拒否されたディレクトリまたはファイルへのアクセス違反を追跡することをお勧めする。</p>
オペレーティング システムを保護する追加ソフトウェアの使用を検討する	<p>ほとんどのオペレーティング システムでは、プロダクション環境を保護する追加ソフトウェアを実行できる。たとえば、Intrusion Detection System (IDS) ではプロダクション環境を変更する攻撃を検出できる。</p> <p>利用可能なソフトウェアについては、オペレーティング システムのベンダに問い合わせる。</p>
オペレーティング システムのサービス パックとセキュリティ パッチを適用する	<p>推奨のサービス パックおよびセキュリティ関連パッチについては、オペレーティング システムのベンダに問い合わせる。</p>

表 2-1 WebLogic Server ホストのセキュリティ対策

セキュリティ アクション	説明
最新の BEA サービス パックを適用し、最新のセキュリティ 勧告を実行する	<p>サイトのセキュリティ事項を担当している場合は、BEA の Advisories & Notifications ページ (http://dev2dev.bea.com/advisories) で新しいセキュリティ 勧告の通知を受けるよう登録する。</p> <p>セキュリティ 勧告で推奨されている対策は、Advisories & Notifications ページに投稿されている。</p> <p>また、リリースされている各サービス パックの適用もお勧めする。サービス パックには、製品の各バージョンおよび以前にリリースされた各サービス パックのすべてのバグの修正が含まれている。サービス パックは、http://commerce.beasys.com/downloads からダウンロードできる。</p> <p>BEA 製品に関するセキュリティ問題は、secalert@bea.com に報告する。</p>

ネットワーク接続のセキュリティ対策

ネットワーク接続を設計するときには、管理しやすいセキュリティ ソリューションの必要性と重要な WebLogic リソースを保護する必要性のバランスを考える必要があります。次の表に、ネットワーク接続を保護するためのオプションを説明します。

表 2-2 ネットワーク接続のセキュリティ対策

セキュリティ アクション	説明
ハードウェアおよびソフトウェアを使用してファイアウォールを作成する	<p>ファイアウォールとは、2つのネットワーク間のトラフィックを制限する機能のこと。ファイアウォールは、ソフトウェアとハードウェア（ルータや専用のゲートウェイマシンなど）を組み合わせて作成できる。ファイアウォールは、プロトコル、要求されたサービス、ルーティング情報、パケットの内容、および送信元と送信先のホストまたはネットワークに基づいてトラフィックの通過を許可または拒否するフィルタを利用する。また、アクセス権を認証されたユーザのみに制限することもできる。</p> <p>WebLogic セキュリティ サービスは、境界に基づく認証 (Web サーバ、ファイアウォール、VPN) を実行し、複数のセキュリティ トークン タイプ/プロトコル (SOAP、IIOP-CSIV2) を処理するサードパーティ ID アサーション プロバイダの使用をサポートする。詳細については、『WebLogic Security の紹介』の「境界認証」を参照。</p> <p>WebLogic Server でファイアウォールを使用する方法の詳細については、『WebLogic Server Clusters ユーザーズ ガイド』の「クラスタ アーキテクチャのセキュリティ オプション」を参照。</p>
WebLogic Server 接続フィルタを使用する	<p>ハードウェアとサードパーティ ソフトウェアを使用してファイアウォールを作成する代わりに（またはそれに加えて）、WebLogic Server 接続フィルタを使用してプロトコル、IP アドレス、および DNS ノード名に基づいてネットワーク トラフィックを制限することを検討する。</p> <p>接続フィルタは、WebLogic Server ドメインのマシンがファイアウォールを介せずに互いにアクセスできる場合に最適。たとえば、ファイアウォールを使用してネットワーク外からのトラフィックを制限し、WebLogic Server 接続フィルタを使用してファイアウォールの背後でトラフィックを制限できる。</p> <p>『WebLogic Security の管理』の「接続フィルタのコンフィグレーション」を参照。</p>

表 2-2 ネットワーク接続のセキュリティ対策

セキュリティ アクション	説明
管理トラフィックにドメイン全体の管理ポートを使用する	<p>管理ポートは、WebLogic Server ドメインのサーバインスタンス間のすべての管理トラフィックを単一ポートに制限する。接続フィルタと一緒に使用すると、WebLogic Server インスタンスが単一ポートのみで、既知のマシンセットまたはサブネットからの管理要求のみを受け付けるように指定できる。</p> <p>ドメイン全体の管理ポートを有効にするには、Administration Console で [DomainName コンフィグレーション 一般] タブを使用する。</p> <p>Administration Console オンライン ヘルプの「ドメイン管理ポートの有効化」を参照。</p>
管理チャンネルを有効にする	<p>サーバ間の管理通信のセキュリティを確保するには、管理チャンネルを有効にする必要がある。管理チャンネルなしでは、一部の重要な管理メッセージがクリアテキストで渡され、メッセージの捕捉、修正、削除、および再現が可能になる。</p> <p>『WebLogic Server のコンフィグレーションと管理』の「管理ポートと管理チャンネル」を参照。</p>

データベースのセキュリティ対策

ほとんどの Web アプリケーションはデータベースを使用してデータを保存します。WebLogic Server で使われるデータベースとしては、Oracle、MicroSoft SQL Server、および Informix が一般的です。データベースには、顧客リスト、顧客の連絡先、クレジット カード情報、その他の独自の情報など、Web アプリケーションの重要なデータを保存することがよくあります。Web アプリケーションを作成する際には、データベースに保存するデータの種類とデータのセキュリティ レベルを考慮する必要があります。また、データベース製造元によるセキュリティ メカニズムを理解し、セキュリティ ニーズに十分に対応できるかどうかを判断することも必要です。メカニズムが十分でない場合は、重要なデータをデータベースに書き込む前に暗号化するなど、他のセキュリティ手法を用い

て、データベースのセキュリティを向上することができます。たとえば、クレジットカード情報だけを暗号化して、その他の顧客データはプレーンテキストのままデータベースに保存するという方法があります。

WebLogic セキュリティ サービスのセキュリティ対策

WebLogic セキュリティ サービスでは、サービインスタンスで動作するサブシステムやアプリケーションを保護するための効果的で柔軟性のあるソフトウェアツールが提供されます。次の表に、プロダクション環境を保護する際に使用することが望ましい重要な機能のチェックリストを示します。

表 2-3 WebLogic セキュリティ サービスのセキュリティ対策

セキュリティ アクション	説明
最新の BEA サービス パックを適用し、最新のセキュリティ勧告を実行する	サイトのセキュリティ事項を担当している場合は、BEA の Advisories & Notifications ページ (http://dev2dev.bea.com/advisories) で新しいセキュリティ勧告の通知を受けるよう登録する。 セキュリティ勧告で推奨されている対策は、 Advisories & Notifications ページに投稿されている。 また、リリースされている各サービス パックの適用もお勧めする。サービス パックには、製品の各バージョンおよび以前にリリースされた各サービス パックのすべてのバグの修正が含まれている。サービス パックは、 http://commerce.beasys.com/downloads からダウンロードする。 BEA 製品に関するセキュリティ問題は、 secalert@bea.com に報告する。

表 2-3 WebLogic セキュリティ サービスのセキュリティ対策

セキュリティ アクション	説明
<p>プロダクション対応のセキュリティ プロバイダをセキュリティ レルムにデプロイする</p>	<p>WebLogic セキュリティ サービスは、複数のセキュリティ プロバイダ (それぞれがセキュリティ の特定の側面を処理) をデプロイできるプラグイン可能アーキテクチャを使用する。</p> <p>WebLogic Server には、包括的なセキュリティ ソリューションを提供する独自のセキュリティ プロバイダがデフォルトで含まれている。独自のセキュリティ プロバイダを購入または作成した場合は、次の処理を実行する。</p> <ul style="list-style-type: none"> ■ セキュリティ プロバイダが正しくデプロイおよびコンフィグレーションされていることを確認する。どのセキュリティ プロバイダが現時点でデプロイされているのかは、Administration Console の [セキュリティ レルム RealmName プロバイダ] フォルダで確認できる。 ■ セキュリティプロバイダをデプロイしたレルムがデフォルト (アクティブ) レルムであることを確認する。レルムをアクティブにするには、Administration Console の左ペインでセキュリティレルム フォルダの名前をクリックし、右ペインで [ドメインのセキュリティ設定] を指定する。 <p>『WebLogic Security の管理』の「デフォルトセキュリティ コンフィグレーションのカスタマイズ」を参照。</p>
<p>SSL を使用するが、デモ用の ID および信頼はプロダクション環境では使用しない</p>	<p>重要なデータを危険から守るには、HTTP プロトコルではなく SSL と HTTPS プロトコル (セキュアソケットレイヤ (SSL) 上の HTTP) を使用してデータ転送を保護する。</p> <p>WebLogic Server には、開発のみで使用するデモ用のプライベート キー、デジタル証明書、および信頼性のある認証局が用意されている。WebLogic Server をダウンロードすると、これらのデジタル証明書用のプライベート キーが必ず付属している。デモ用の ID と信頼は使用しないこと。</p> <p>『WebLogic Security の管理』の「SSL のコンフィグレーション」を参照。</p>

2 プロダクション環境のセキュリティの確保

表 2-3 WebLogic セキュリティ サービスのセキュリティ対策

セキュリティ アクション	説明
最強の暗号化を有効にする	<p>ダウンロードするバージョンの WebLogic Server では、512 ビット キーと 40 ビット バルク暗号化をサポートしている。</p> <p>最強の暗号化 (1024 ビット キーと 128 ビット バルク暗号化) をサポートするバージョンを使用する場合は、BEA の販売代理店に問い合わせる。輸出規制があるため、このバージョンの WebLogic Server は、特定国でのみ利用可能である。</p>
WebLogic Server がデジタル証明書でセキュリティ制約を施行するようにする	<p>SSL 経由で通信する場合、WebLogic Server はデフォルトで、認証局で定義された Basic Constraint エクステンションを持たない証明書チェーンのデジタル証明書を拒絶する。このレベルのセキュリティ制約の施行では、デジタル証明書のなりすましから Web サイトが保護される。</p> <p>サーバ起動コマンドで、このセキュリティ制約の施行を無効にする次のオプションが指定されていないようにする。</p> <pre>-Dweblogic.security.SSL.enforceConstraints=false</pre> <p>このオプションは起動スクリプト、またはノードマネージャで管理対象サーバを起動する場合は Administration Console の [サーバ ServerName コンフィグレーション リモートスタート] タブで見つかる。</p> <p>実際の開発環境では、WebLogic Server 7.0 サービス パック 2 以前のリリースで提供されたデモ用デジタル証明書との非互換性を回避するためにセキュリティ制約の施行が無効になっている場合がある。プロダクション環境ではこの機能を有効にすること。</p>

表 2-3 WebLogic セキュリティ サービスのセキュリティ対策

セキュリティ アクション	説明
<p>介在者の攻撃を防止するためにホスト名の検証が有効になっていることを確認する</p>	<p>WebLogic SSL の実装はデフォルトで、接続先のホストが予定していた通信先、または許可された通信先であることを確認する。ただし、サイトへの WebLogic Server の実装時に、ホスト名の検証が無効にされている場合もある。</p> <p>ホスト名の検証が WebLogic Server デプロイメントで確実に使用されるようにするには、[ホスト名検証を無視] 設定を無効にする。この設定は、Administration Console の [サーバ ServerName 接続 SSL] タブにある。</p> <p>背景情報：</p> <p>介在者の攻撃は、ネットワークに配置されたマシンによって、無防備な通信先に対するメッセージが取り込まれたり、変更されたり、再転送されたりして発生する。介在者の攻撃を回避する 1 つの方法は、接続先のホストが予定していた通信先、または許可された通信先であることを確認すること。SSL クライアントでは、SSL サーバのホスト名と SSL サーバのデジタル証明書と比較して接続を検証できる。WebLogic Server のホスト名検証では、SSL 接続が介在者の攻撃から保護される。</p>
<p>リクエストのサイズと時間を制限してサービス拒否攻撃を防止する</p>	<p>サービス拒否攻撃を防止するために、WebLogic Server では、メッセージのサイズだけでなく、メッセージの到着にかかる最長時間も制限することができる。デフォルト設定では、最大メッセージサイズとして 2GB、完了メッセージタイムアウトとして 480 秒が許可される。</p> <p>HTTP、T3、および IIOP プロトコルのこれらの設定は、Administration Console の [サーバ ServerName 接続 プロトコル] タブでコンフィグレーションできる。</p> <p>背景情報：</p> <p>サービス拒否攻撃を受けると、Web サイトは動作していても使用不能になる。ハッカーは、Web サイトの 1 つまたは複数の重要なリソースを消耗させたり削除したりする。</p> <p>侵入者は WebLogic Server インスタンスに対してサービス拒否攻撃を仕掛けるために、サイズが非常に大きく送信が終了するまでに時間がかかるリクエストや、リクエストが終了する前にクライアントがデータの送信を止めてしまうので完了することのないリクエストを大量に送信する。</p>

2 プロダクション環境のセキュリティの確保

表 2-3 WebLogic セキュリティ サービスのセキュリティ対策

セキュリティ アクション	説明
ユーザ ロックアウトとログインの時間制限をコンフィグレーションしてユーザ アカウントに対する攻撃を防止する	<p>WebLogic セキュリティ サービスはデフォルトで、ユーザ アカウントの辞書攻撃に対して最大レベルのセキュリティを提供する。開発時に、アカウントがロックされるまでの無効なログイン試行の回数、アカウントがロックされるまでに無効なログイン試行が行われる期間、またはユーザ アカウントがロックされる時間の設定を変更した場合は、その設定を見直して実際のプロダクション環境に適しているかどうかを検証する。</p> <p>それらの設定は、Administration Console の [セキュリティ レルム RealmName ユーザ ロックアウト] タブで確認または変更できる。</p> <p>背景情報： 辞書攻撃では、ハッカーはスクリプトを作成し、「辞書」に登録されているパスワードを使用してログインを試みる。WebLogic Server のユーザ ロックアウトとログイン設定は、辞書攻撃からユーザ アカウントを保護できる。</p>
複数の認証プロバイダを使用する場合は、JAAS 制御フラグを設定する	<p>セキュリティ レルムで複数の認証プロバイダがコンフィグレーションされている場合は、JAAS 制御フラグを設定して各プロバイダの順序と優先順位をコンフィグレーションする。</p> <p>JAAS 制御フラグは、Administration Console の [セキュリティ レルム RealmName プロバイダ 認証プロバイダ AuthenticatorName 一般] タブで設定する。</p> <p>『WebLogic Security の管理』の「JAAS 制御フラグ属性の設定」を参照。</p>

表 2-3 WebLogic セキュリティ サービスのセキュリティ対策

セキュリティ アクション	説明
セキュリティ監査を有効にする	<p>監査とは、WebLogic Server 環境での重要なセキュリティイベントを記録する処理のこと。WebLogic セキュリティ サービスが提供する監査プロバイダを有効にすると、イベントが <code>DomainName\DefaultAuditRecorder.log</code> に記録される。</p> <p>監査プロバイダは、Administration Console の [セキュリティ レalmName プロバイダ 監査] ページで有効にできる。</p> <p>詳細については、Administration Console オンライン ヘルプの「監査プロバイダのコンフィグレーション」を参照。</p> <p>注意： 監査プロバイダを使用すると、数個のイベントがログに記録される場合でも WebLogic Server のパフォーマンスに悪影響が及ぶ場合がある。</p> <p>監査レコードを定期的に参照し、セキュリティ侵害やその試みを検出する。何度もログオンしようとして失敗している、または変わったパターンでセキュリティイベントが起こっていることに注目すると、重大な問題を防止できる。</p>
デフォルトの WebLogic Server セキュリティ ロールにユーザおよびグループが正しく割り当てられていることを確認する	<p>すべての WebLogic リソースはデフォルトで、デフォルトのセキュリティ ロールに基づくセキュリティ ポリシーで保護される。</p> <p>目的のユーザおよびグループがそれらのデフォルトセキュリティ ロールに割り当てられていることを確認する。</p> <p>『管理者ガイド』の「システム管理操作の保護」を参照。</p>
WebLogic Server から HTTP 応答でその名前とバージョン番号が送信されることの防止を検討する	<p>WebLogic Server のインスタンスが HTTP リクエストに応答するときには、デフォルトで、その HTTP 応答ヘッダにサーバの名前と WebLogic Server バージョン番号が含まれる。これが原因で、攻撃者が特定バージョンの WebLogic Server の脆弱性を知っている場合にセキュリティ上のリスクが生じることになる。</p> <p>WebLogic Server インスタンスからその名前とバージョン番号が送信されるのを防止するには、Administration Console で [Send Server Header を有効化] 属性を無効にする。この属性は、[サーバ ServerName 接続 HTTP] タブにある。</p>

アプリケーションのセキュリティ対策

WebLogic Server ドメインの WebLogic リソースを保護する責任のほとんどはサーバにあります。一部の責任は個々のアプリケーションにあります。一部のセキュリティ オプションでは、WebLogic セキュリティ サービスを利用してサーバと個々のアプリケーションのどちらに責任があるかを判断できます。プロダクション環境にデプロイしたアプリケーションごとに、次の表の項目を検討してリソースが保護されているかを検証する必要があります。

表 2-4 アプリケーションのセキュリティ対策

セキュリティ アクション	説明
どの方法で Web アプリケーションと EJB が保護されるのかを確認する	<p>各 Web アプリケーションと EJB はデフォルトでデプロイメント記述子 (XML ファイル) を使用して、その保護対象リソースと保護対象リソースにアクセスできるセキュリティ ロールを宣言する。</p> <p>Web アプリケーションおよび EJB のデプロイメント記述子でセキュリティを宣言する代わりに、Administration Console を使用して Web アプリケーションおよび EJB へのアクセスを保護するセキュリティ ポリシーを設定できる。この方法では、すべての Web アプリケーションと EJB のセキュリティを一元的に管理できる。</p> <p>以上 2 つの方法を結合し、URL (Web) または EJB リソースの初期デプロイメント時に既存のデプロイメント記述子からセキュリティ コンフィグレーションをコピーするよう WebLogic Server をコンフィグレーションできる。セキュリティ コンフィグレーションをコピーすると、以降の更新では Administration Console を使用できる。</p> <p>『WebLogic リソースのセキュリティ』の「URL (Web) リソースと EJB (エンタープライズ JavaBean) リソース」を参照。</p>
HTML コメント タグの代わりに JSP コメント タグを使用する	<p>エンド ユーザ向けではない JSP ファイルのコメントは、HTML 構文 <code><!-- ... --></code> ではなく JSP 構文の <code><%/ * ... */%></code> を使用する必要がある。JSP コメントは JSP がコンパイルされたときに削除されるので、見ることはできない。</p>

表 2-4 アプリケーションのセキュリティ対策

セキュリティ アクション	説明
未コンパイル JSP およびその他のソース コードはプロダクション用マシンにインストールしない	<p>必ず、ソース コードはプロダクション用マシンから遠ざけておくようにする。ソース コードにアクセスできれば、侵入者はセキュリティ ホールを見つけ出すことができる。</p> <p>JSP をプリコンパイルし、コンパイル済みの JSP のみをプロダクション用マシンにインストールすることを検討する。JSP のプリコンパイルについては、『WebLogic JSP プログラマーズ ガイド』の「JSP のプリコンパイル」を参照。</p>
SSL を使用するようアプリケーションをコンフィグレーションする	<p>web.xml ファイルの user-data-constraint 要素で transport-guarantee を CONFIDENTIAL に設定する。</p> <p>『Web アプリケーションのアセンブルとコンフィグレーション』の「security-constraint」を参照。</p>
Servlet サブレットを使用しない	<p>プロダクション環境では Servlet サブレットを使用しないことをお勧めする。</p> <p>代わりに、サブレットを明示的に URI にマッピングする。プロダクション環境で Web アプリケーションを使用する前には、すべての Web アプリケーションから、WebLogic サブレットと Servlet サブレットの間の既存のマッピングをすべて削除する。</p> <p>サブレットのマッピングについては、『Web アプリケーションのアセンブルとコンフィグレーション』の「サブレットのコンフィグレーション」を参照。</p>
プロダクション環境で FileServlet をデフォルト サブレットのままにしない	<p>プロダクション環境では FileServlet サブレットをデフォルト サブレットとして使用しないことをお勧めする。</p> <p>デフォルト サブレットの設定については、『Web アプリケーションのアセンブルとコンフィグレーション』の「デフォルト サブレットの設定」を参照。</p>

2 プロダクション環境のセキュリティの確保

表 2-4 アプリケーションのセキュリティ対策

セキュリティ アクション	説明
すべての WebLogic セキュリティ ポリシーを検証する	<p>WebLogic Server 7.0 では、WebLogic リソースに「誰がアクセスできるか」という問いに対し、ACL ではなくセキュリティ ポリシーが答える。</p> <p>WebLogic リソースからセキュリティ ポリシーが削除されていないこと、そしてセキュリティ ロールの割り当てで意図したタイプのアクセス権がユーザに提供されることを確認する。</p> <p>『WebLogic リソースのセキュリティ』の「セキュリティ ポリシー」を参照。</p>
アプリケーションに信頼性のないコードが含まれている場合は、Java セキュリティ マネージャを有効にする	<p>Java セキュリティ マネージャは、JVM で動作するクラスのパーミッションを定義し強制する。多くの場合、脅威モデルでは悪意あるコードが JVM で実行されることを想定していないため、Java セキュリティ マネージャは不要。しかし、サードパーティが WebLogic Server を使用し、未知のクラスが実行される場合、Java セキュリティ マネージャが役立つ。</p> <p>サーバインスタンスの Java セキュリティ マネージャを有効にするには、サーバの起動時に次の Java オプションを使用する。</p> <pre>-Djava.security.manager -Djava.security.policy[<i>=filename</i>]</pre> <p>『WebLogic Security プログラマーズ ガイド』の「Java セキュリティを使用しての WebLogic リソースの保護」を参照。</p>

表 2-4 アプリケーションのセキュリティ対策

セキュリティ アクション	説明
サーバーレットまたは JSP がユーザの供給によるデータを返した場合に、HTML 特殊文字を置換する	<p>ユーザの供給によるデータを返す機能により、クロスサイトスクリプトと呼ばれるセキュリティの脆弱性がもたらされる。これは、ユーザのセキュリティ認可を盗用するために利用される可能性がある。クロスサイトスクリプトの詳細については、http://www.cert.org/tech_tips/malicious_code_mitigation.html の「Understanding Malicious Content Mitigation for Web Developers」(CERT のセキュリティ勧告)を参照。</p> <p>セキュリティの脆弱性をなくすには、ユーザが供給したデータを返す前に、そのデータをスキャンして HTML 特殊文字を探す。該当する文字が見つければ、それらを HTML のエンティティまたは文字参照と置き換える。文字を置換することによって、ブラウザがユーザの供給によるデータを HTML として実行することが回避される。</p> <p>『WebLogic JSP プログラマーズガイド』の「JSP におけるユーザ入力データのセキュリティ」および『WebLogic HTTP サーブレット プログラマーズガイド』の「サーバーレットでのクライアント入力のセキュリティ」を参照。</p>

2 プロダクション環境のセキュリティの確保
