



## シスコ データセンターへの Oracle E-Business Suite 11i の統合

**【注意】シスコ製品をご使用になる前に、安全上の注意  
([www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/))をご確認ください。**

**本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。  
米国サイト掲載ドキュメントとの差異が生じる場合があるため、正式な内容については米国サイトのドキュメントを参照ください。  
また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。**

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

シスコ データセンターへの Oracle E-Business Suite 11i の統合  
Copyright © 2007 Cisco Systems, Inc.  
All rights reserved.

Copyright © 2008, シスコシステムズ合同会社 .  
All rights reserved.



## CONTENTS

<b>シスコ データセンターへの Oracle E-Business Suite 11i の統合</b>	<b>1</b>
はじめに	1
範囲	1
アプリケーション アーキテクチャ	2
アーキテクチャの概要	2
デスクトップ層	3
アプリケーション層	5
データベース層	6
ネットワーク アーキテクチャ	7
データセンター ネットワーク コンポーネント	7
コア レイヤ	8
アグリゲーション レイヤ	8
アクセス レイヤ	9
設計の目標	10
設計と実装の詳細	10
ACE ワンアーム モード設計	11
ACE ワンアーム モデル設計のトラフィック パターンの概要	14
ACE ワンアーム モード設計のアーキテクチャの詳細	17
Oracle E-Business Suite 11i 環境	17
Oracle E-Business Suite 11i 環境と統合ネットワーク サービス	18
その他の統合サービス オプション	21
ACE 透過モード設計	21
ACE 透過モード設計のトラフィック パターンの概要	23
ACE 透過モード設計のアーキテクチャの詳細	26
Oracle E-Business Suite 11i 環境	26
Oracle E-Business Suite 11i 環境と統合ネットワーク サービス	26
その他のサービス統合オプション	28
アプリケーション設定の詳細	29
HTTP ロード バランシング	30
フォーム リスナ サーブレット	31
SSL アクセラレータ	33
クッキーとセッションの永続性	35
ネットワーク設定例	36

Catalyst 6500 MSFC	36
プライマリアグリゲーション スイッチ	36
セカンダリアグリゲーション スイッチ	37
ACE 管理設定	39
ACE ワンアーム モード設定	40
ACE 透過モード設定	42
FWSM 管理設定 (管理コンテキスト)	44
FWSM 透過モード設定 (データベース コンテキスト)	45
FWSM 透過モード設定 (APPL_TOP コンテキスト)	46
付録	48
リファレンス	48
用語集	49



# シスコ データセンターへの Oracle E-Business Suite 11i の統合

このドキュメントでは、Oracle E-Business Suite 11i アプリケーション環境を強化するネットワーク設計のベスト プラクティスを示します。アプリケーションの展開に関する主要な概念とオプション、およびシスコのアプリケーションとネットワーク技術を利用するデータセンターで使用可能な詳しい設計方法を紹介します。

## はじめに

増え続ける顧客の要求、変化の激しい市場動向、地球規模での競争により、今日の企業はよりよい製品やサービスを、より安い価格で顧客に提供せざるをえなくなっています。Oracle E-Business Suite は、企業がこれらの課題を解決できるよう支援するために開発された広範なビジネス アプリケーション群です。E-Business アプリケーション フレームワークは、ビジネス プロセスの保護、拡張、発展を目的に設計された柔軟な環境です。

今日のデータセンターは、エンタープライズ ビジネス アプリケーションをサポートするコンピューティング能力とストレージリソースが複雑に入り組んだシステムです。データセンターは単なる施設ではなく、これらのアプリケーションが取り組む真のビジネス目標を実現するために戦略上重要な、競争の最前線です。したがって、データセンター ネットワークの物理設計と論理設計では、そうした重要なビジネス アプリケーションを最適化し、企業がその目標を実現できるような、柔軟かつ安全で可用性の高い環境を提供する必要があります。

## 範囲

シスコ データセンター アーキテクチャは、可用性と堅牢性に優れたネットワーク インフラストラクチャと統合されたアプリケーション サービスを提供する、定評のあるマルチレイヤ アプローチです。このドキュメントでは、シスコ データセンター設計で Oracle E-Business Suite を展開し、統合されたロード バランシング サービスとセキュリティ サービスを利用する方法について説明します。

## アプリケーション アーキテクチャ

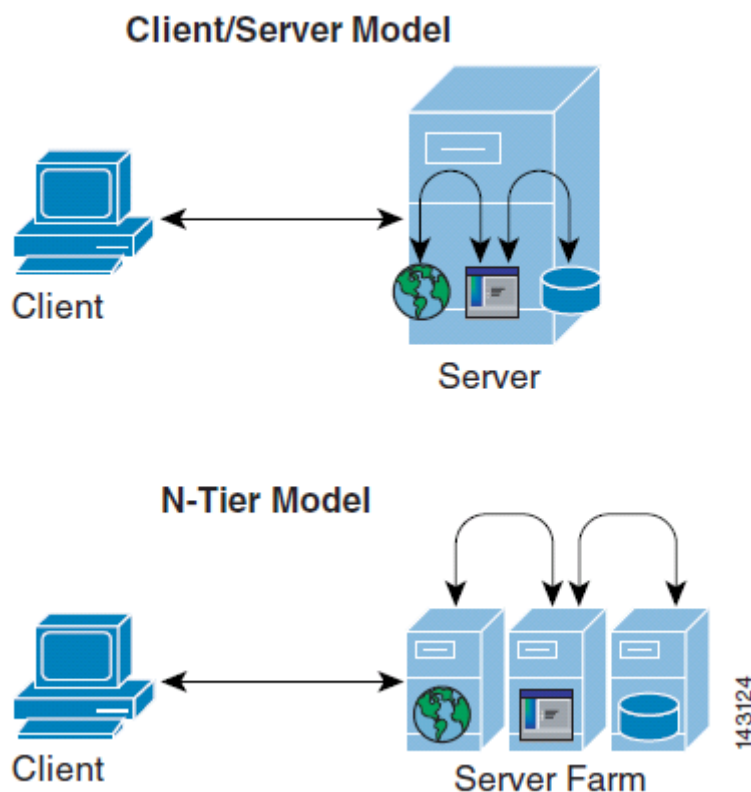
ここでは、Oracle E-Business Suite 11i のアプリケーション アーキテクチャについて説明します。

### アーキテクチャの概要

データセンターは、エンタープライズ ソフトウェア アプリケーションのリポジトリです。エンタープライズ ソフトウェア アプリケーションは、ビジネスの要件を満たし、最新の技術の進歩や方式に対応するために絶えず変化しています。その結果、それらのソフトウェア アプリケーションをホストするデータセンター サーバファームとネットワーク インフラストラクチャの論理的および物理的な構造も絶えず変化しています。

サーバファームは、かつてのクライアント / サーバ モデルから N 階層アプローチへと進化しました。N 階層の「N」は、2 階層や 4 階層など、基本的にはアーキテクチャで使用されている独立した階層の数を表します。N 階層モデルでは、機能領域を作成することにより、エンタープライズ アプリケーションを論理的または物理的に分離します。これらの領域は、通常は Web フロントエンド層、アプリケーション ビジネス ロジック層、およびデータベース層と定義されます。図 1 に、クライアント / サーバから N 階層へのエンタープライズ アプリケーションの進化を示します。

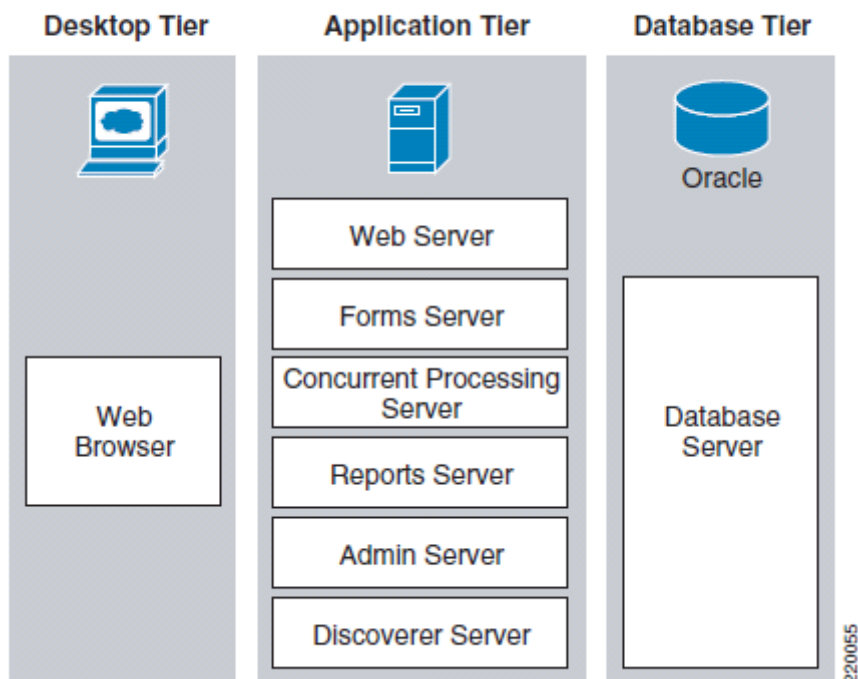
図 1 クライアント / サーバ モデルと N 階層モデル



N 階層モデルは、よりスケーラブルで管理しやすいエンタープライズ アプリケーション環境を提供します。これは、ソフトウェア アプリケーション内に独立したサービス可能領域が作成されるからです。アプリケーションは分散型となり、またシングル ポイント障害が設計から取り除かれるため、復元力が高まります。

Oracle のアプリケーション アーキテクチャでは、N 階層モデルを利用し、アプリケーション サービスをサーバファーム内のノードに分散させます。図 2 に示す Oracle アプリケーション アーキテクチャでは、デスクトップ層、アプリケーション層、およびデータベース層にアプリケーションを論理的に分離しています。重要なのは、必要なパフォーマンスまたはアプリケーション可用性を企業に提供するために、各階層を 1 つ以上の物理ホストで構成できるということです。

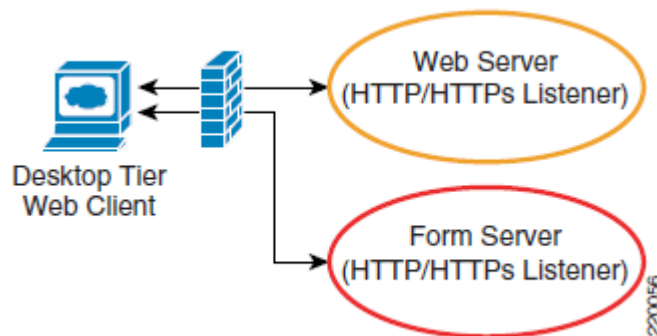
図 2 Oracle アプリケーション アーキテクチャ



## デスクトップ層

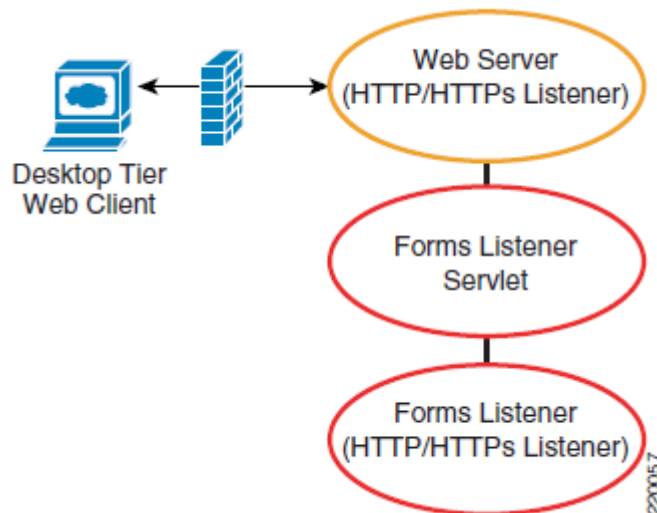
一般にプレゼンテーション層と呼ばれているデスクトップ層は、クライアント ユーザ インターフェイス、つまり Web ブラウザで構成されます。ブラウザは、HTTP または HTTPS を介してアプリケーション層の Web サーバまたはフォーム サーバに接続します。従来、フォーム サーバを使用するには、クライアント側アプレットの Oracle JInitiator を使用する必要がありました。Oracle JInitiator は、フォーム サーバへのダイレクト ソケット接続を使用して、クライアントのブラウザ上で ActiveX またはプラグインとして実行されます。このダイレクト接続環境では、クライアントがフォーム サーバに直接アクセスする必要があります。そのため、ファイアウォールに「穴」を設けて企業 LAN または WAN の境界を越えた接続を許可する必要があります。企業は潜在的なセキュリティ リスクにさらされることになります。図 3 に、ダイレクト ソケット接続がファイアウォールと企業のセキュリティに与える影響を示します。

図3 デスクトップからフォーム サーバへの従来型の接続



2002 年、Oracle E-Business Suite により、Java フォーム リスナ サーブレットが Web リスナを介してフォーム サーバ要求をインターセプトできるようにする、「インターネット フレンドリ」なフォーム サーバアプリケーションが導入されました。フォーム リスナ サーブレットにより、クライアント（デスクトップ層）とアプリケーション層の間で単一の HTTP 接続または HTTPS 接続を使用することが可能になります。図 4 に、安全性の高いフォーム リスナ サーブレット展開モデルを示します。このモデルでは、標準の SSL オフロードおよびロード バランシング アプローチを利用することもできます。

図4 フォーム リスナ サーブレット アーキテクチャ



(注) フォーム リスナ サーブレット展開モデルは、今日のエンタープライズ データセンターにおいて一般的なものです。このドキュメントではこれ以降、このフォーム戦略が使用されているものと想定します。

## アプリケーション層

Oracle E-Business Suite のアプリケーション層は、管理サービスとビジネス ロジックを提供し、デスクトップ層のエンド ユーザがデータベース層で検索された情報を利用できるようにします。図 2 は、このレイヤに存在する主要なサーバを示しています。

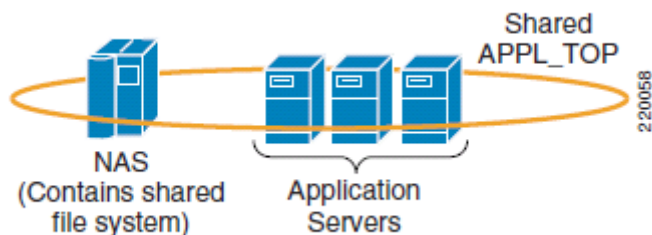
- Web サーバ
- フォーム サーバ
- 並行処理サーバ
- 管理サーバ
- レポート サーバ
- ディスカバラ サーバ

各アプリケーション サーバは、Oracle E-Business Suite に対応している企業に、ビジネス プロセス ロジックまたは管理サービスを提供します。デスクトップ層は、Web サーバ リスナを介してアプリケーションと通信します (図 4)。

アプリケーション層は、通常は APPL\_TOP と呼ばれます。APPL\_TOP は、単一の物理ノードに常駐するか、「共有」マルチノード アプリケーション層展開の複数のノードにまたがるのが可能です。共有 APPL\_TOP は、11i インストールの各ノードによってマウントされる共通ディスクに常駐します。共有 APPL\_TOP により、任意のノードで Web サーバやフォーム サーバなどの 6 つの主要サーバ機能呼び出すことが可能になります。共有アプリケーション層展開の大きな利点は、マルチノード展開内の単一のファイルシステムにパッチや変更を適用し、それらの変更をすべてのノードに同時に伝えられることです。

さらに、単一のファイルシステムを使用するので、複数のノードを使用しているにもかかわらず、単一のファイルシステムをバックアップするだけで済みます。図 5 に、NFS を介してアプリケーション ファイルシステムを共有する 3 つのサーバ ノードを示します。この場合の共有マウントポイントは、ネットワーク内にあるストレージ デバイスです。

図 5 共有アプリケーション ファイルシステム



(注)

Windows システムは Oracle 11i 環境の共有アプリケーション層をサポートしません。共有アプリケーション層ファイルシステムの詳細については、Oracle Metalink Document 243880.1 を参照してください。

## データベース層

データベースは、データの構造化された集まりです。この複雑な構築物は、テーブル、インデックス、およびストアド プロシージャで構成されます。これらはいずれも、データを整理したり、データにアクセスしたりするための重要な要素です。Oracle には、アプリケーション層によって収集されたデータを操作するためのデータベース管理システム (DBMS) または リレーショナル DBMS (RDBMS) が用意されています。データベース層はデスクトップ層と直接やり取りするわけではありません。代わりに、データベースはアプリケーション層を仲介者として利用します。Oracle では、パフォーマンス、スケーラビリティ、および可用性を向上させるために、複数のノードで単一のデータベース インスタンスをサポートすることを可能にする Real Application Clusters (RAC; リアルアプリケーション クラスタ) が提供されます。



(注)

---

Oracle アプリケーションの詳細については、[www.oracle.com](http://www.oracle.com) の製品番号 B19295-02 「Oracle Application Concepts Release 11i」を参照してください。

---

## ネットワーク アーキテクチャ

データセンター インフラストラクチャ アーキテクチャでは、可用性が高く、スケーラブルで安全なアプリケーション環境を提供する必要があります。ここでは、シスコ データセンター ネットワーク アーキテクチャの概要を示し、この設計の基本について説明します。トピックは次のとおりです。

- データセンター ネットワーク コンポーネント
- 設計の目標



(注) シスコシステムズのベスト プラクティスと推奨するデータセンター設計の詳細については、[http://www.cisco.com/en/US/netsol/ns656/networking\\_solutions\\_design\\_guidances\\_list.htm#anchor3](http://www.cisco.com/en/US/netsol/ns656/networking_solutions_design_guidances_list.htm#anchor3) を参照してください。

## データセンター ネットワーク コンポーネント

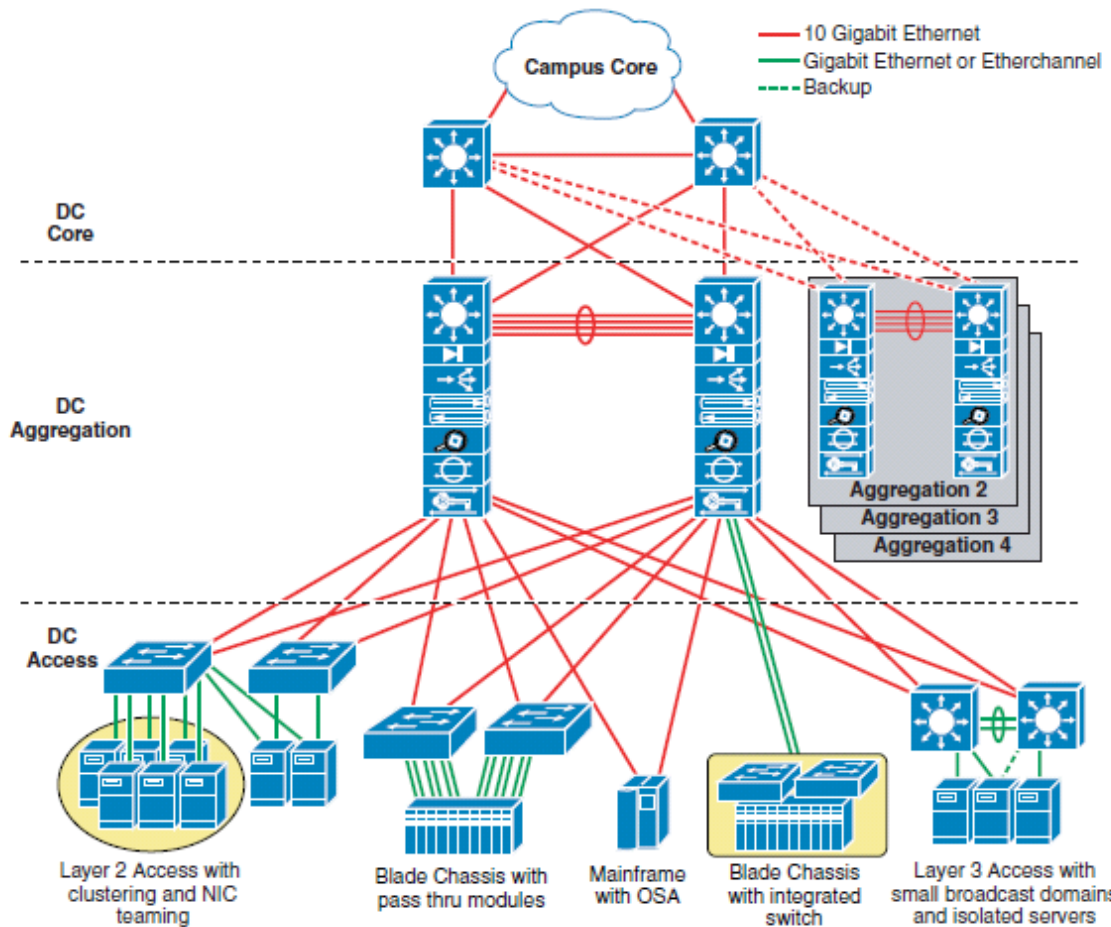
データセンター インフラストラクチャのデバイスは、その役割に応じて、フロントエンド ネットワークとバックエンド ネットワークに分けることができます。

- フロントエンド ネットワークは、IP ルーティングおよびスイッチング環境を提供します。これには、クライアント / サーバ間、サーバ / サーバ間、およびサーバ / ストレージ間のネットワーク接続が含まれます。
- バックエンド ネットワークは、Storage Area Network (SAN; ストレージ エリア ネットワーク) ファブリックと、サーバとその他のストレージ デバイス (ストレージ アレイ、テープ デバイスなど) の間の接続をサポートします。

フロントエンド ネットワークには、コア レイヤ、アグリゲーション レイヤ、アクセス レイヤの 3 つの独立した機能領域が含まれます。

図 6 に、多階層フロントエンド ネットワーク トポロジと、これらの各レイヤで使用可能なさまざまなサービスを示します。

図6 データセンターの多階層モデルトポロジ



## コア レイヤ

コア レイヤは、キャンパスの WAN、イントラネット、エクストラネットなどの外部エンティティへの高速接続を提供するゲートウェイです。データセンター コアはレイヤ 3 ドメインで、その基本的な目的は効率的かつ迅速にパケットを転送することです。そのため、データセンター コアは高帯域幅リンク（10GE）を使用して構築され、ルーティングのベスト プラクティスを利用してトラフィックフローを最適化します。

## アグリゲーション レイヤ

アグリゲーション レイヤは、ネットワークトラフィックが集まるポイントであり、アクセスレイヤのサーバファームと企業のその他の部分の間の接続を提供します。アグリゲーション レイヤはレイヤ 2 およびレイヤ 3 の機能をサポートし、集中管理されたアプリケーションサービス、セキュリティサービス、および管理サービスを導入するのに最適な場所です。これらのデータセンターサービスは、アクセスレイヤのサーバファームの間で共有され、共通のサービスを効率的でスケーラブルに、かつ予測可能で確定的に提供します。

アグリゲーション レイヤは、データセンターのための包括的な機能セットを提供します。これらの機能は次のデバイスによってサポートされます。

- マルチレイヤ アグリゲーション スイッチ
- ロード バランシング デバイス
- ファイアウォール
- 侵入検知システム
- コンテンツ エンジン
- Secure Sockets Layer (SSL) オフローダ
- ネットワーク分析デバイス

## アクセス レイヤ

アクセス レイヤの主要な役割は、サーバ ファームに必要なポート密度を提供することです。さらに、アクセス レイヤはクライアント / サーバ間およびサーバ / サーバ間のトラフィックをサポートするために、柔軟かつ効率的で予測可能な環境である必要があります。レイヤ 2 ドメインは、次のものを提供することにより、これらの要件を満たします。

- サーバとサービス デバイスの間のレイヤ 2 隣接関係
- 確定的で高速に収束する、ループフリーなトポロジ

サーバ ファームのレイヤ 2 隣接関係を使用すると、レイヤ 2 での情報交換だけを必要とするサーバまたはクラスタを展開できます。また、レイヤ 2 隣接関係は、ロード バランサやファイアウォールといったアグリゲーション レイヤのネットワーク サービスへのアクセスを容易にサポートします。これによって、共有の集中管理ネットワーク サービスをサーバ ファームで効率的に使用することが可能になります。

これに対し、サービスが各アクセス スイッチに展開されている場合、それらのサービスを利用できるのは、そのスイッチに直接接続されているサーバに限定されます。レイヤ 2 のアクセスを利用することで、新しいサーバをアクセス レイヤに簡単に挿入できます。アグリゲーション レイヤはデータセンター サービスを行い、レイヤ 2 環境はスケーラブルなポート密度をサポートすることに専念します。

アクセス レイヤでは、安定したレイヤ 2 ドメインを保証するために、確定的な環境を提供する必要があります。予測可能なアクセス レイヤにより、フェールオーバーやフェールバック時にスパンニング ツリーをすばやく収束および復元することが可能になります。



(注)

このドキュメントでは、SAN のベスト プラクティスについては取り上げません。詳細については、[www.cisco.com/go/srmd](http://www.cisco.com/go/srmd) を参照してください。

## 設計の目標

シスコ データセンター アーキテクチャは、ネットワークとネットワークがサポートするアプリケーションの連動を可能にする包括的なアプローチです。この設計の主要な目標は、データセンター内のエンタープライズ アプリケーションのパフォーマンス、可用性、スケーラビリティ、管理性を向上させるとともに、安全な環境を提供することです。さらに、仮想化技術とネットワーク設計のベスト プラクティスを使用することにより、エンタープライズ アプリケーションの複雑さと実装時間を軽減します。このドキュメントではこれ以降、シスコ データセンター インフラストラクチャのサービスを使用して Oracle E-Business Suite 11i アプリケーションを導入する場合の、これらの各目標について説明します。

## 設計と実装の詳細

ここでは、Cisco Application Control Engine (ACE) と Cisco Firewall Services Module (FWSM) を統合し、エンタープライズ データセンターで集中管理されたアプリケーション サービスを提供する方法について詳しく説明します。トピックは次のとおりです。

- データセンターでの ACE ワンアーム モード設計
- データセンターでの ACE 透過モード設計

これらの設計は、シスコシステムズのデータセンター インフラストラクチャ アーキテクチャでの Oracle の E-Business Suite アプリケーションの多階層導入に対応するものです。これらの設計は、集中管理されたサーバ ロード バランシング サービス、SSL オフロード サービス、およびファイアウォール サービスをアプリケーションに提供します。さらに、FWSM と ACE の両方の仮想化機能を使用すると、単一の物理デバイスで複数の論理デバイスを提供できます。システム管理者は、単一の仮想デバイスをビジネス ユニットまたはアプリケーションに割り当て、アプリケーション パフォーマンスの目標またはサービスレベル契約 (SLA) を達成することができます。

図 7 に、単一の Catalyst 6500 シリーズ アグリゲーション スイッチ内での「サービス チェーン」の概念を示します。この例では、ACE と FWSM の仮想化を利用することにより、複数のビジネス ユニットで、コンテキストと呼ばれる論理的に独立したネットワーク サービス デバイスを同じ Catalyst デバイス内で定義することができます。仮想化の柔軟性により、システム管理者は顧客のビジネス要件やアプリケーションの技術要件のそれぞれに応じてネットワークベースのサービスを展開できます。専用のアプライアンスを別途購入することなくサービスを分離できるため、データセンターのスペースや電力を余分に使用せずに済みます。

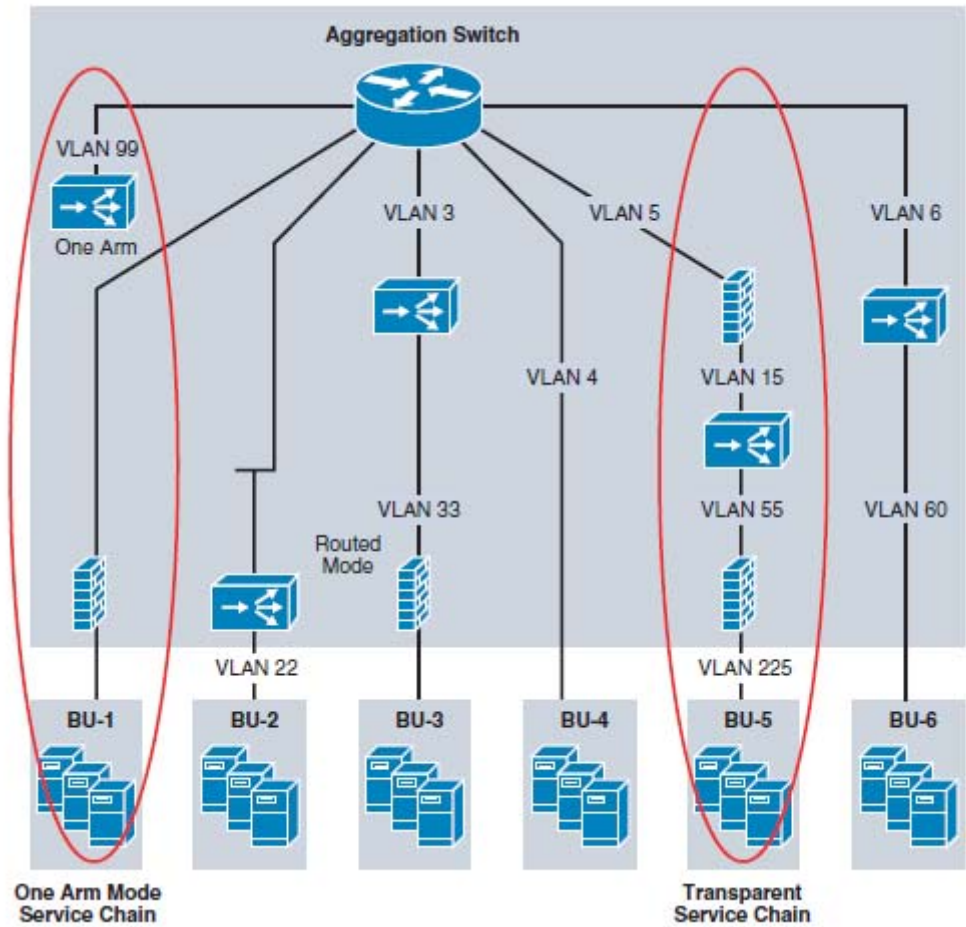


(注)

各仮想コンテキストでは、CPU、帯域幅、ACL、接続などのアプリケーション ルールとリソース使用レベルが独自に定義されます。

図 7 は、一般的に考えられる設定のいくつかを示していますが、可能なサービス チェーンの組み合わせをすべて表しているわけではありません。

図7 ビジネスユニット サービス チェーンの例



## ACE ワンアーム モード設計

ACE は、Catalyst 6500 シリーズ プラットフォーム用の統合サービス モジュールであり、ハイアベイラビリティ サービス、スケーラビリティ サービス、およびセキュリティ サービスをエンタープライズ アプリケーションに提供します。ワンアーム モードの ACE は、Oracle の E-Business Suite にこれらのサービスを効果的に統合できるようにすることで、これらの目的をサポートします。この設計では、ACE と FWSM を通じて、サーバロード バランシングとファイアウォール機能をアーキテクチャのアプリケーション層に提供します。

ワンアーム モード設計を使用すると、システム管理者はネットワーク トラフィックが ACE のサービスを必要としない場合に ACE をバイパスし、不要な負荷を取り除くことによって ACE のパフォーマンスを最適化することができます。さらに、ワンアーム モードではデータセンターのルーティング パフォーマンスが最適化されます。これは、Catalyst 6500 シリーズ Multilayer Switch Feature Card (MSFC; マルチレイヤ スイッチ機能カード) がファーム内のサーバのデフォルト ゲートウェイとして、ルーティングの役割を果たすからです。

図 8 ACE ワンアーム モード展開と透過ファイアウォール サービス

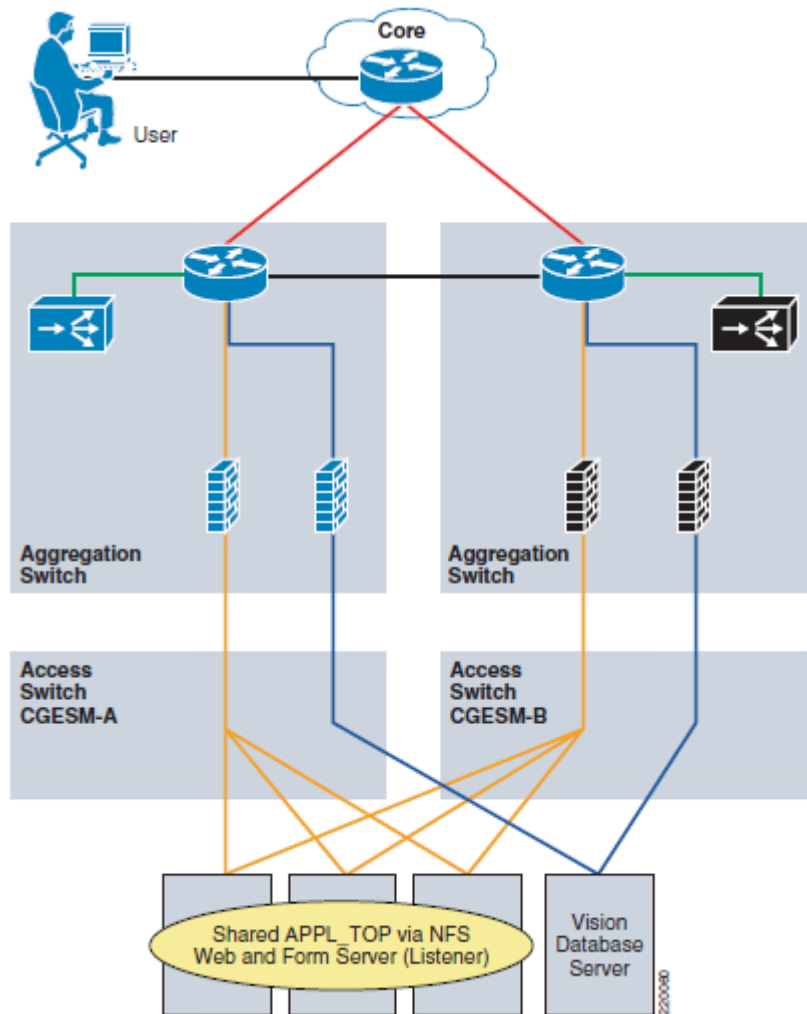


図 8 に、ワンアーム サービス チェーン 設定での仮想 ACE および FWSM コンテキストの論理ビューを示します。ACE および FWSM コンテキストはアグリゲーション レイヤに常駐します。MSFC は、共有 APPL\_TOP サーバおよび Vision データベースのデフォルト ルートです。FWSM は、サーバファームの前面に配置された 2 つの透過デバイスとしてアクセス コントロールを適用します。

ACE は、状態監視機能を通じて、可用性の高い Oracle 環境を提供します。前述のように、Oracle の E-Business Suite では、メッセージングに標準のプロトコル (HTTP または HTTPS) を使用します。したがって、次の状態プローブを 1 つ以上使用して、アプリケーション サーバの状態を判断することをお勧めします。

- TCP プローブ
- HTTP プローブ
- HTTPS プローブ
- TCL スクリプト



(注) ACE モジュールのサーバ状態監視機能の詳細については、[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_1cn/ace/ace\\_301/slbgd/probe.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_1cn/ace/ace_301/slbgd/probe.htm) を参照してください。

ACE によってサポートされるロード バランシング プレディクタ (アルゴリズム) には、次のものがあります。

- ラウンドロビン
- 最小接続数
- ハッシュ アドレス
- ハッシュ クッキー
- ハッシュ ヘッダー
- ハッシュ URL

これらのアルゴリズムにより、アプリケーション環境で作業負荷を分散するための十分な柔軟性がシステム管理者に与えられます。

さらに、ACE はセッション アフィニティを提供できます。これは、ACE が Oracle アプリケーションによって作成されたクッキーまたは URL データを読み取る方法、または独自のクッキーを挿入する方法を理解しているからです。ACE はこの情報を使用して、セッションの継続中にアプリケーションのユーザを単一のサーバに効果的に結び付けることができます。単一のデバイスへのセッション アフィニティにより、アプリケーションで共有セッション状態データベースまたはアプリケーション サーバの別のインスタンスのリソースを使用するのではなく、サーバのローカル キャッシュを使用して、セッション状態情報を取得することが可能になります。

通常、APPL\_TOP サーバは、プロセッサのリソースを使用してクライアントとアプリケーションサーバの間のアフィニティを保証することにより、Oracle ソリューションでのセッション永続性を提供します。ACE を Web およびアプリケーション層の前面に論理的に配置することにより、ネットワークで状態監視とサーバ ロード バランシングに加えて、セッション アフィニティを提供することが可能になります。ACE は Web サーバをセッション アフィニティとロード バランシングの役割から解放します。この ACE 機能により、アプリケーションの全体的なパフォーマンスが向上するとともに、複雑さが軽減されます。

ACE の統合された SSL (HTTPS) 機能により、電子商取引トランザクションの安全性はさらに向上します。ACE は、ハードウェアベースの SSL アクセラレーションを提供し、プロセッサへの負荷が大きい機能をサーバの CPU または NIC からネットワークに移動します。SSL サービスをネットワーク内で集中管理することにより、その他のネットワークベース サービス (IDS、IPS、または暗号化されていない「クリアな」トラフィックなしでは適用できないその他のネットワーク分析デバイス) によって安全なトランザクションを効率的に処理および検査することが可能になります。

図 8 は、アプリケーション層とデータベース層の間のファイアウォール サービスを示しています。VLAN を通じたネットワークの論理的なセグメント化により、この論理分割が実現します。管理者は、各ネットワーク セグメント (アプリケーションおよびデータベース) に対し、より細かいセキュリティ ポリシーとトラフィック フィルタリング ルールを適用することができます。

ロード バランサは、応答の遅いサーバをロード バランシング計算から取り除き、サーバファーム トランザクションの効率を向上させることにより、可用性を向上させます。ファイアウォールのセキュリティ サービスを組み合わせることにより、Oracle アプリケーションのトラフィックはより安全で、最適化されたものになります。



(注)

ワンアーム設計では、送信元 Network Address Translation (SNAT; ネットワーク アドレス変換) または Policy-Based Routing (PBR; ポリシーベース ルーティング) を使用して、ロード バランサがサーバ / サーバ間アプリケーション接続のすべての側面を監視することを保証する必要があります。SNAT は ACE モジュールで簡単に設定できます。このドキュメントではこれ以降、ACE へのシンメトリック トラフィック フローを保証するために SNAT が使用されているものと想定します。

## ACE ワンアーム モデル設計のトラフィック パターンの概要

ここでは、データセンターでの次のフローのトラフィック パターンについて説明します。

- クライアント / サーバ間
- サーバ / データベース間

### クライアント / サーバ間のトラフィック フロー

図 9 に、ACE をワンアーム モードで使用した場合のデータセンター内のクライアント / サーバ間トラフィック フローを示します。クライアントは、エンタープライズ データセンター内の Web ページを要求しています。また図 9 は、ネットワークにおける HTTPS (SSL) トランザクションも示しています。

ワンアーム データセンター設計での適切なトランザクションは、次の手順で行われます。

1. クライアントは ACE モジュール上の Versatile Interface Processor (VIP; パーサタイトル インターフェイス プロセッサ) に関連付けられている URL を要求します。
2. MSFC は要求を ACE モジュールにルーティングします。
3. ACE コンテキストは、システム管理者のアプリケーション ポリシーに基づいて、セキュリティとロード バランシングの両方の意思決定を行い、実際のサーバを選択します。この時点で、ACE コンテキストは VIP アドレスを実際のサーバの IP アドレスで置き換え、ローカル NAT プールから SNAT アドレスを割り当てます。ACE コンテキストは、実際のサーバの宛先 IP アドレスと自らの SNAT アドレスを使用して、MSFC 上のデフォルト ゲートウェイに要求を転送します。



**(注)** クライアントの IP アドレスを維持する必要がある場合は、ACE コンテキストで PBR を使用できます。もう 1 つの選択肢は、HTTP ヘッダー挿入と SNAT の組み合わせを使用し、以降のロギング機能用にクライアントの元の IP アドレスを HTTP ヘッダー内に配置することです。

ACE コンテキストは、アクセス コントロール機能と HTTP ディープ パケット インスペクション機能を備えています。HTTP ディープ パケット インスペクションを使用すると、システム管理者は HTTP プロトコルを監視し、ユーザ定義のトラフィック ポリシーに基づいてトラフィックを許可または拒否することができます。HTTP アプリケーション インスペクションがカバーするセキュリティ機能は次のとおりです。

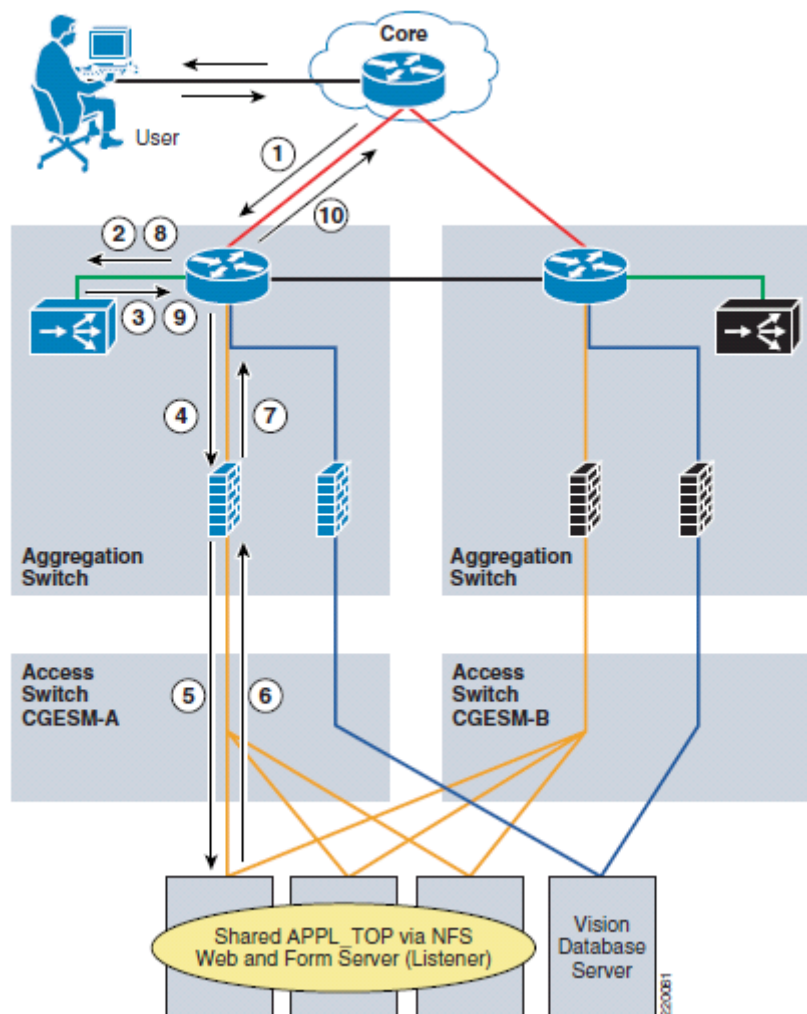
- RFC 準拠の監視と RFC メソッドフィルタリング (RFC 2616)
- コンテンツ、URL、および HTTP ヘッダー長のチェック
- 転送エンコーディング方式
- コンテンツ タイプの検証とフィルタリング
- ポート 80 の悪用

ACE の正規表現機能を HTTP データ ペイロードに対して使用することにより、通常は IDS デバイスまたは IPS デバイスが行う「シグネチャ」ベースのセキュリティ意思決定を行うことができます。

4. MSFC は、透過モードの FWSM コンテキストによって保護される実際のサーバに要求を送ります。
5. FWSM コンテキストは、「内部」ネットワークと「外部」ネットワークの間でトラフィックをブリッジし、適切なセキュリティ ポリシーをネットワーク セグメントに適用します。スイッチはパケットを Oracle 11i APPL\_TOP サーバに転送します。

6. サーバは要求に応答し、トラフィックを L2 で MSFC に送信します。このトラフィックには、自らの送信元 IP アドレスと、宛先 IP アドレスである ACE の SNAT アドレスが含まれています。
7. FWSM はトラフィックを MSFC にブリッジします。
8. MSFC は SNAT アドレスが常駐する ACE モジュールにトラフィックをルーティングします。
9. ACE コンテキストはリターン トラフィックの送信元 IP アドレスを、実際のサーバの IP アドレスから ACE コンテキストの VIP へ書き換えます。再構築されたパケットが ACE コンテキストのデフォルト ゲートウェイである MSFC に送信されます。
10. MSFC はトラフィックをエンド ユーザにルーティングします。

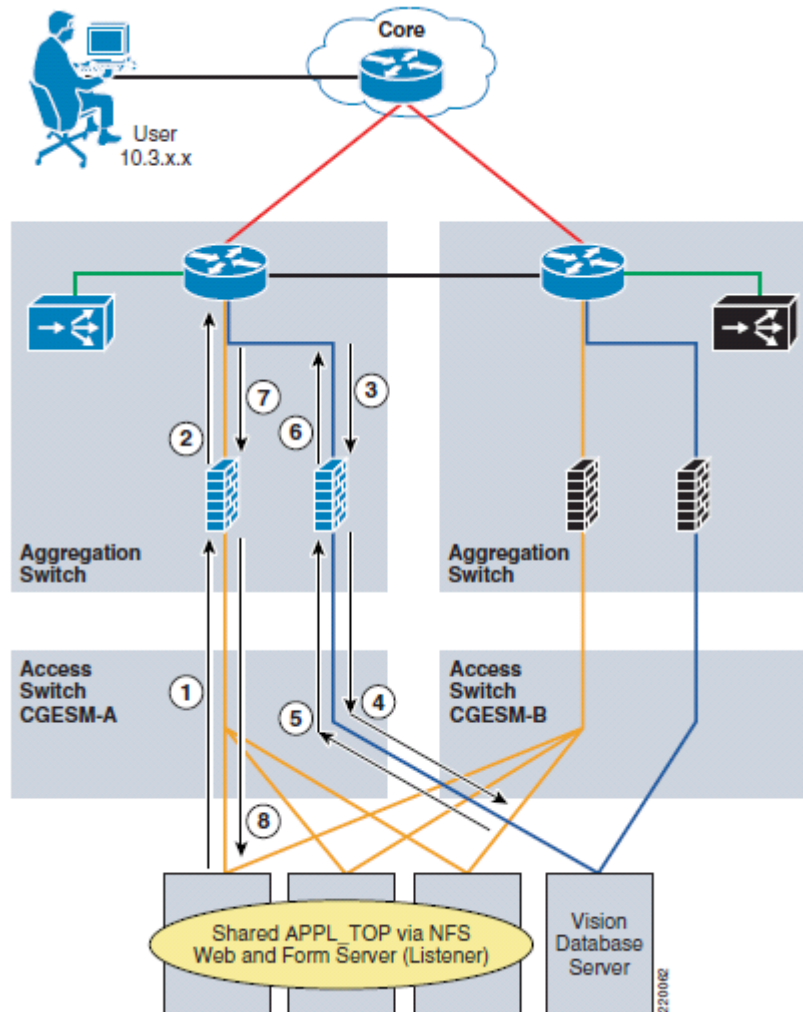
図9 クライアント/サーバ間のトラフィック パターン



## サーバ/データベース間のトラフィック フロー

図 10 に、ACE をワンアーム モードで使用し、FWSM を透過モードで使用した場合の、データセンターにおける APPL\_TOP サーバ / データベース サーバ間のトラフィック フローを示します。APPL\_TOP サーバは、エンタープライズ データセンター内のデータベース サーバの情報を要求しています。APPL\_TOP/ データベース サーバ間のトラフィックは、ACE サービスを使用せず、FWSM のステートフル インスペクション サービスのみを使用します。

図 10 サーバ/データベース間のトラフィック パターン



このワンアーム データセンター設計における APPL\_TOP サーバとデータベース サーバの間の正常なトランザクションは、次の手順で行われます。

1. APPL\_TOP サーバは TCP 接続を通じてデータベース要求を開始します。要求は MSFC 上のデフォルト ゲートウェイに送信されます。宛先 IP アドレスはデータベース サーバの IP アドレスであり、宛先ポートは既知の TNS ポートである 1521 です。
2. アプリケーション層のファイアウォール コンテキストは内部インターフェイスで要求を受信します。FWSM コンテキストはトラフィックを MSFC にブリッジし、ローカル接続テーブル内に有効な接続エントリを作成します。

3. MSFC は TNS 要求をデータベース サーバに転送します。
4. データベース層のファイアウォール コンテキストは外部インターフェイスで要求を受信します。FWSM コンテキストは、TNS トラフィックが許可されることを判断し、要求をデータベース サーバに転送して、ローカル接続テーブル内に新しい接続を作成します。
5. データベース サーバは TNS 要求に回答し、デフォルト ゲートウェイである MSFC に回答を転送します。ファイアウォール コンテキストはトラフィックを MSFC にブリッジします。
6. MSFC はデータベース サーバの回答をアプリケーション層のファイアウォールを介して APP\_TOP サーバにルーティングします。
7. 回答は、FWSM コンテキストにより、最初の TCP SYN パケットによって作成された有効な接続エントリに基づいて、発信元のサーバに透過的にブリッジされます。
8. TNS 回答が APPL\_TOP サーバに到達します。

## ACE ワンアーム モード設計のアーキテクチャの詳細

ここでは、テストベッドのアプリケーションおよびネットワーク トポロジについて説明します。トピックは次のとおりです。

- Oracle E-Business Suite 11i 環境
- Oracle E-Business Suite 11i 環境と統合ネットワーク サービス
- その他の統合サービス オプション

## Oracle E-Business Suite 11i 環境

ここでは、テスト アプリケーション トポロジの概要を紹介し、テストで使用するハードウェアとソフトウェアを示します。

### ハードウェア

単一の HP p-Class BladeSystem がアプリケーション層およびデータベース層を構成するノードを収容します。サーバ プラットフォームには、BL25p と BL30p の組み合わせを使用します。BL25p データベース サーバは、Vision データベース ファイル システムが格納された Diamond Atto アレイにファイバチャネルで接続されます。単一の APPL\_TOP ノード (BL25p) は、「共有」APPL\_TOP が常駐する別の Diamond Atto アレイにファイバチャネルで接続されています。残りの APPL\_TOP サーバ ノードは、NFS を使用して、ファイバチャネルで接続された BL25p から使用可能な共有ファイルシステムをマウントします。

### ソフトウェア

Red Hat の Enterprise Linux AS リリース 4 (Nahant Update 2) を、テストベッドのすべてのノードのオペレーティング システムとして使用します。Oracle テスト環境は次のソフトウェア パッケージで構成されます。

- E-Business Suite 11i バージョン 11.5.10.2
- Oracle Database バージョン 9.2.06.0

Oracle の E-Business Suite には、Vision という名前のサンプル データベースが含まれています。Vision データベースを使用することにより、11i スイートの運用対応アプリケーションを利用してテストベッドで有効なアプリケーション トラフィックを生成することができます。

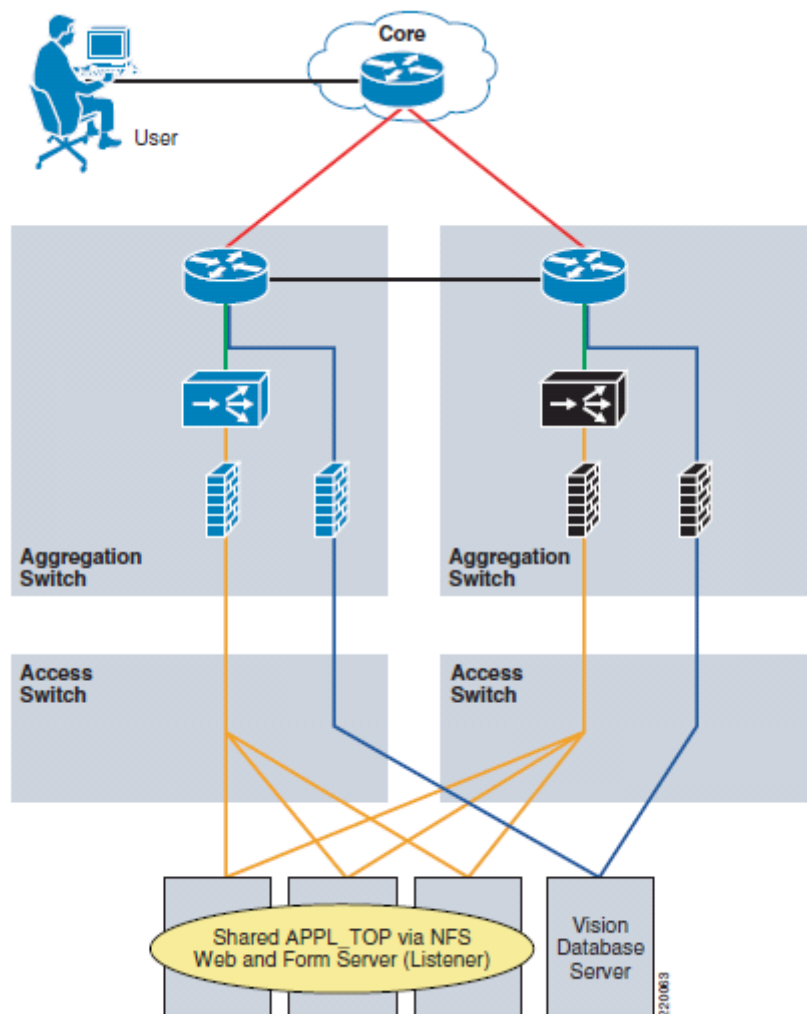
## Oracle E-Business Suite 11i 環境と統合ネットワーク サービス

ここでは、Oracle E-Business Suite ソリューション トポロジへのネットワーク サービスの導入について説明します。主なトピックは次のとおりです。

- ソフトウェア
- ハードウェア
- テスト トポロジ

図 11 に、このドキュメントのすべての設計で使用する物理トポロジを示します。

図 11 CE ワンアーム モデル設計



## ソフトウェア

このテストで使用するソフトウェア イメージは次のとおりです。

- Catalyst 6500 Supervisor 720s 用の Cisco ネイティブ Internetwork Operating System (IOS) ソフトウェア バージョン 12.2(18)SXF5
- Cisco FWSM ソフトウェア バージョン 3.1(1)

- Cisco ACE ソフトウェア バージョン 3.0(0)A1(2)
- CGESM ソフトウェア バージョン 12.2(25)SED
- Cisco MDS ソフトウェア バージョン 2.1(2b)

## ハードウェア

このテストで使用するネットワーク機器は次のとおりです。

- Catalyst 6500 および Supervisor 720
- Cisco Firewall Services Module (FWSM)
- Cisco Application Control Engine (ACE)
- HP p-Class BladeSystem 用の Cisco Gigabit Ethernet Switch (CGESM)
- Cisco MDS 9216i

図 11 は、このドキュメントで説明するすべての設計に使用する物理トポロジを示しています。HP ブレード サーバは、統合された CGESM スイッチにデュアルホームされ、Catalyst 6515 アグリゲーション スイッチへの IP 接続を提供します。各 Catalyst 6500 シリーズ スイッチは、統合されたネットワーク サービス モジュールを含み、アプリケーション サービスとセキュリティ サービスを提供します。アグリゲーション レイヤでは、10 ギガビット イーサネット ラインカードを使用してコアクラウドへのアップストリーム接続と Inter-Switch Link (ISL; スイッチ間リンク) を提供します。ISL は 2 つの 10 ギガビット イーサネット リンクで構成されます。

テストベッドでは、一対のストレージ アレイへの冗長接続を提供する 2 つの MDS 9216i デバイスを介して共有ストレージを使用します。2 つのブレード サーバはこのファブリックを利用します。データベース サーバは 1 つの Logical Unit Number (LUN; 論理ユニット番号) にデータベース ファイルを格納します。1 つのアプリケーション サーバが、SAN 内の別の LUN に収容される APPL\_TOP ファイルシステムにアクセスします。



(注)

SAN 内の APPL\_TOP ファイルシステムにアクセスするアプリケーション サーバは、NFS サービスを提供すると同時に、APPL\_TOP ディレクトリをエクスポートします。NFS により、他のアプリケーション サーバで SAN 内の APPL\_TOP ファイルシステムを「マウント」して共有することが可能になります。

## トポロジ

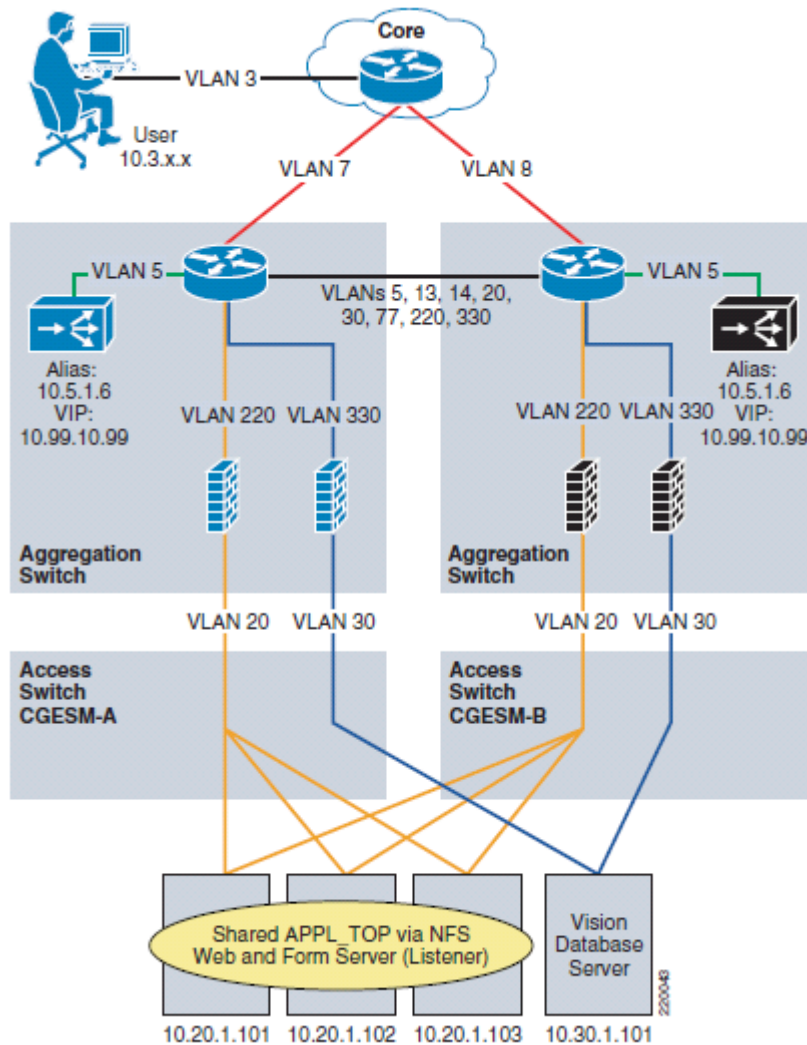
図 12 に、Cisco ACE をワンアーム モード設計で使用する Oracle E-Business Suite 11i テストベッドの論理トポロジを示します。ACE は、Oracle アプリケーション環境へのクライアント接続のためのロード バランシングとセッション永続性を提供します。FWSM は、サーバ ファーム内のすべてのトランザクションにステートフル インспекションを提供します。各仮想ファイアウォール コンテキストは、この多階層環境の内部インターフェイスと外部インターフェイスの間でトラフィックをブリッジします。この方法で、FWSM は各仮想ファイアウォール コンテキストによって個別に適用される詳細なトラフィック フィルタリングを提供します。



(注)

図 12 では、2 つのアグリゲーション スイッチ間の ISL により、運用トラフィック VLAN の 5、20、30、220、330 と、フォールトトレラントおよびレプリケーション VLAN の 13、14、77 が伝達されます。

図 12 ACE ワンアーム モデル テストベッド トポロジ



(注)

セッション永続性は、送信元 / 宛先間 IP を使用して、または ACE クッキーを挿入することにより実現されます。これらの各方式は Oracle によってサポートされており、ネットワーク設定例のセクションに示されています。サポートされるロード バランシング方式の詳細については、「Oracle Metalink ドキュメント 217368.1」を参照してください。

アプリケーション サーバとデータベース サーバは MSFC をデフォルト ゲートウェイとして使用し、統合された CGESM アクセス スイッチにデュアルホームされます。統合されたブレード スイッチは、リンク アグリゲーション制御プロトコル (802.3ad) を使用して 4 つのギガビットイーサネット ポートを単一の論理チャンネルにバンドルすることにより、アグリゲーション レイヤの Catalyst 6500 シリーズ スイッチに接続します。このチャンネルでは、統合されたブレード スイッチのトランク フェールオーバー機能 (リンク ステート追跡とも呼ばれます) を使用します。トランク フェールオーバーは、シスコのブレード スイッチで使用できるハイアベイラビリティ メカニズムであり、外部アップリンクのリンク ステートにブレード スイッチの内部サーバ ポートを結び付けます。この機能により、サーバの NIC チューニング機能が最適化され、アプリケーションの可用性が向上します。

テストベッドの仮想の ACE コンテキストと FWSM コンテキストはアクティブ / スタンバイ シナリオで展開され、障害状態が冗長性を通じて許容されます。データセンターの収束時間は、障害の種類と場所によって決まります。ACE のフェールオーバー時間は 1 秒未満で、エンド ユーザからはわかりません。これは、クッキーの永続性データに加えて、アクティブな接続ステートが 2 つの仮想デバイス間で維持されるからです。

データセンター インフラストラクチャのフェールオーバー時間と復元時間は、[http://www.cisco.com/univercd/cc/td/doc/solution/dci\\_srnd.pdf](http://www.cisco.com/univercd/cc/td/doc/solution/dci_srnd.pdf) で参照できます。詳しい設定については、36 ページの「ネットワーク設定例」と 29 ページの「アプリケーション設定の詳細」を参照してください。

## その他の統合サービス オプション

このドキュメントでは、Oracle のエンタープライズクラス アプリケーションである E-Business Suite へのネットワーク サービスの統合について説明しています。サーバ ロード バランシングとセキュリティは、データセンター アプリケーションによって使用される基本的なサービスです。しかし、企業が使用できる統合ネットワーク サービスはこれだけではありません。次のネットワーク サービスもサービス モジュールまたはアプライアンスとして簡単に使用できます。

- SSL オフローディング (ACE プラットフォームに統合されたハードウェアベース オプション)
- 侵入防御システム
- 侵入検知システム
- ネットワーク分析デバイス
- WAN 最適化システム (WAAS、AVS)
- キャッシング デバイス

## ACE 透過モード設計

透過展開モデルの ACE コンテキストでは、データセンター内のインテリジェント ネットワーク サービスのシームレスな統合が可能です。透過 ACE コンテキストは、レイヤ 2 トラフィックをブリッジし、アプリケーション セキュリティ サービスとロード バランシング サービスをシステム管理者のポリシーに従って適用します。透過展開では、サーバ ファーム内のサーバのデフォルト ゲートウェイは ACE ではなく、ルータ、ファイアウォール、ロード バランサなどの別のレイヤ 3 デバイスです。

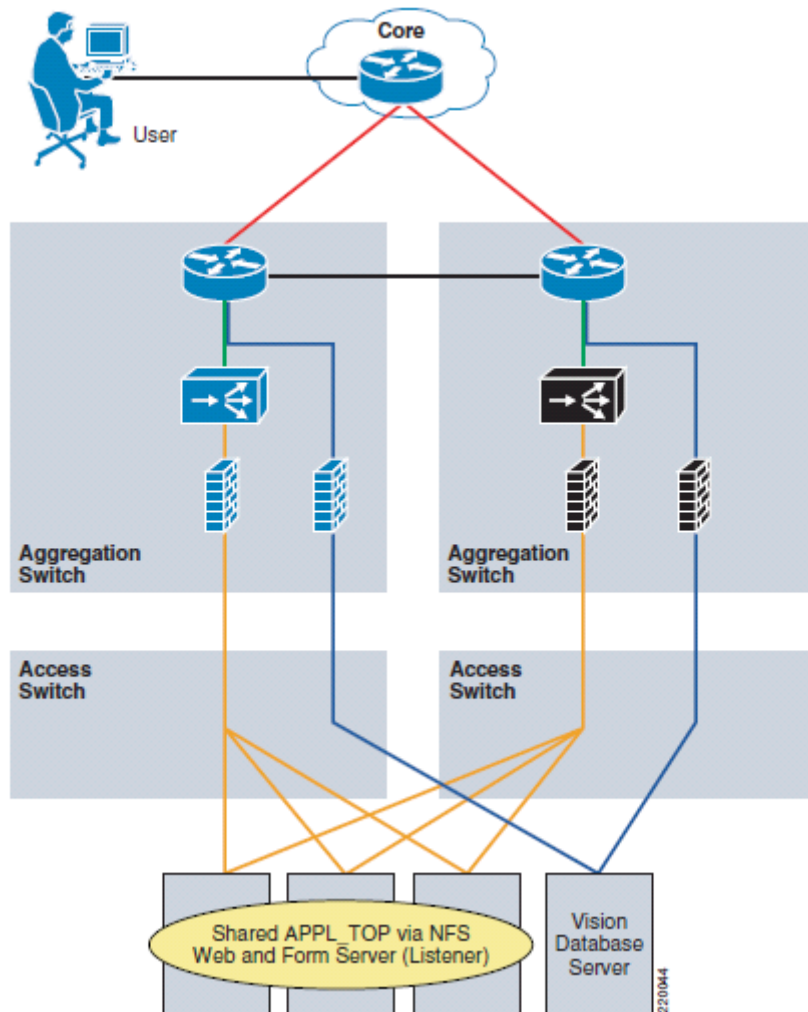
アグリゲーション レイヤは、ネットワーク アプリケーション サービスを展開するのに最適な場所です。これは、トラフィックの大半がデータセンターのこの領域に集まるからです。図 13 に、透過ブリッジング モデルで設定された仮想 ACE コンテキストおよび FWSM コンテキストの論理ビューを示します。ACE サービス モジュールと FWSM サービス モジュールは、データセンターのアグリゲーション スイッチに物理的に配置され、仮想デバイス コンテキストを通じてサービスを提供します。このモデルでは、MSFC はサーバ ファームのデフォルト ゲートウェイです。すべての入力サーバトラフィックと出力サーバトラフィックは、ACE とファイアウォール仮想コンテキストを経由します。つまり、ステートフル パケット インスペクション、ロード バランシング、およびアプリケーション サービスが一律に適用されるということです。これらの機能により、可用性、スケーラビリティ、および安全性が高いアプリケーション環境が実現します。

透過サービス チェーンでは、ACE はワンアーム設計と同じようにロード バランシング、セッション永続性、および SSL オフロード機能を提供することが可能です。大きな違いは、すべてのトラフィックが ACE および FWSM を経由する必要があるということです。そのため、FWSM と ACE の両方が提供できる、高性能なハードウェアベースのサービスが必要になります。

ACE のパフォーマンス機能の詳細については、  
[http://www.cisco.com/en/US/products/hw/modules/ps2706/products\\_data\\_sheet0900aecd8045861b.html](http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet0900aecd8045861b.html) を  
 参照してください。

FWSM のパフォーマンス機能の詳細については、  
[http://www.cisco.com/en/US/products/hw/modules/ps2706/products\\_data\\_sheet0900aecd803e69c3.html](http://www.cisco.com/en/US/products/hw/modules/ps2706/products_data_sheet0900aecd803e69c3.html) を  
 参照してください。

図 13 ACE 透過モード設計



## ACE 透過モード設計のトラフィック パターンの概要

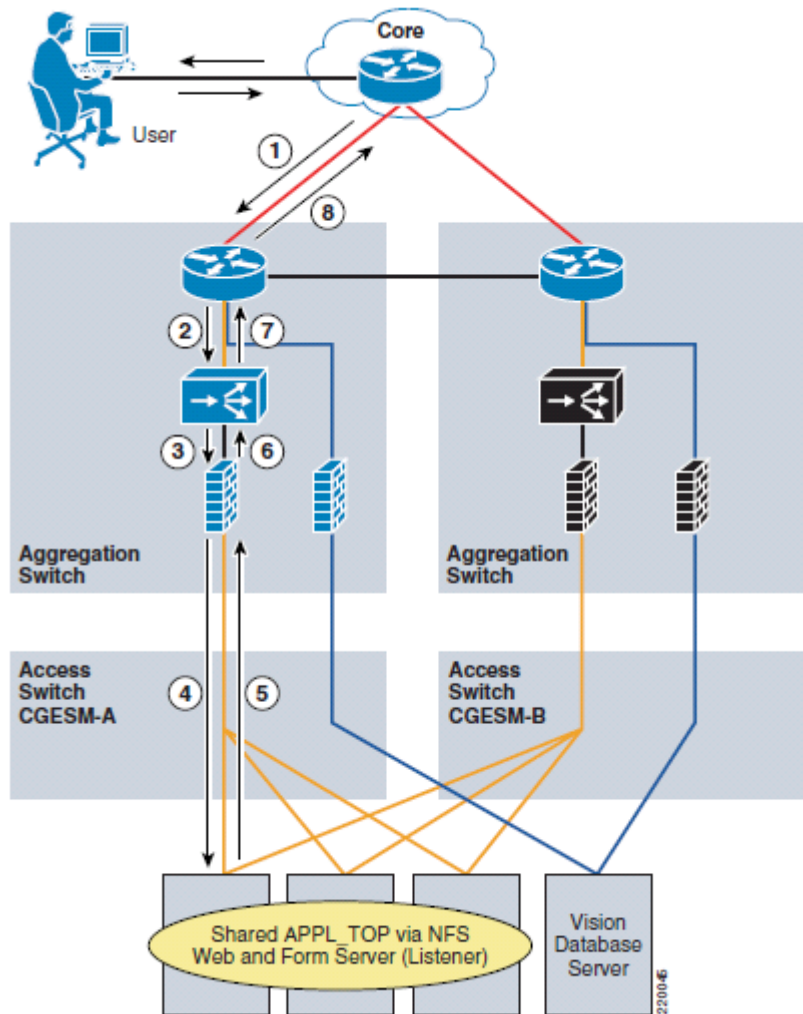
ここでは、トラフィック パターンについて説明します。

### クライアント/サーバ間のトラフィック フロー

図 14 に、ACE と FWSM を透過モードで使用している場合のデータセンターにおけるクライアント/サーバ間のトラフィック フローを示します。クライアントは、エンタープライズ データセンター内の Web ページを要求しています。透過モードのデータセンター設計での正常なトランザクションは、次の手順で行われます。

1. クライアントは ACE モジュールの VIP に関連付けられている URL を要求します。
2. MSFC は要求を ACE モジュールにルーティングします。
3. ACE モジュールは、VIP アドレスに関連付けられている透過コンテキストで要求を受信します。ACE はセキュリティ サービスとロード バランシング サービスを提供します。11i 環境では、送信元/宛先間 IP アドレスまたはクッキー ベースの永続性方式が使用できます。ACE は VIP アドレスを APPL\_TOP サーバ ファーム内の実際のサーバの IP アドレスで置き換えます。ACE はトラフィックを FWSM コンテキストに転送し、APPL\_TOP サーバを保護します。
4. FWSM 透過コンテキストは要求トラフィックを受信し、システム管理者のアクセス ルールに基づいてトラフィックを許可します。要求が実際のサーバに渡されます。
5. 実際のサーバは要求を受信し、クライアントの宛先 IP アドレスを使用して応答します。
6. 透過 FWSM はトラフィックをブリッジします。
7. 透過 ACE は実際のサーバの送信元 IP アドレスを VIP の IP アドレスで置き換え、応答を MSFC にブリッジします。
8. MSFC は応答をクライアントにルーティングします。

図 14 クライアント/サーバ間のトラフィック パターン (透過モード)



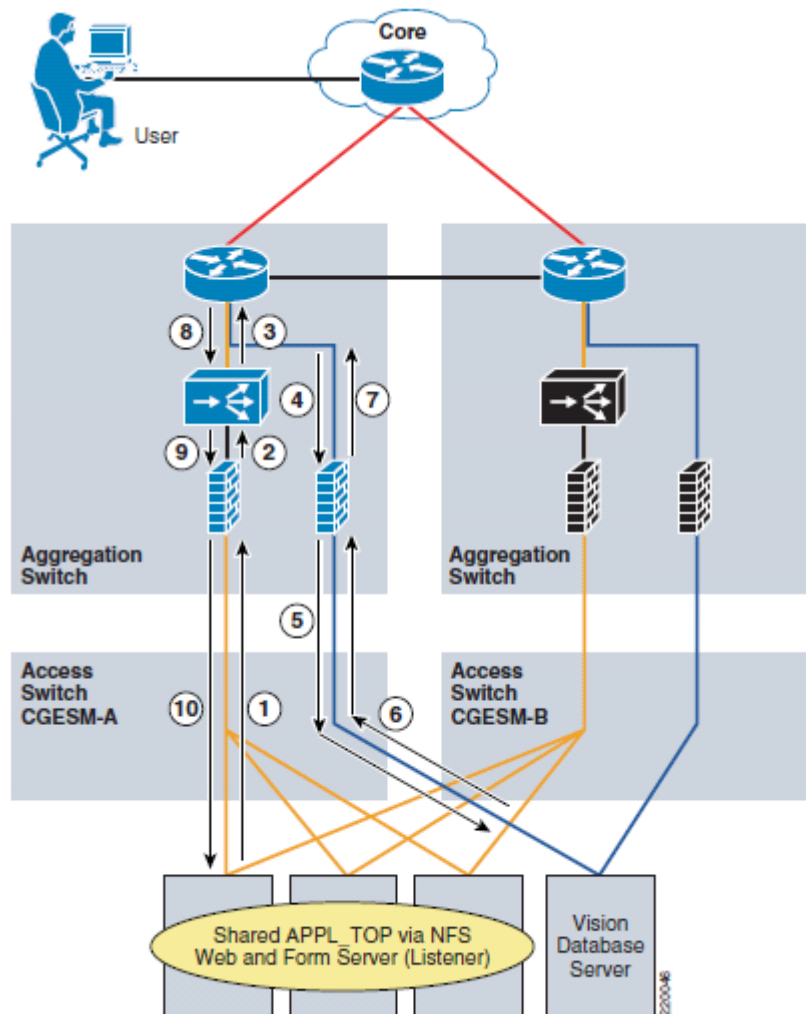
### サーバ/データベース間のトラフィック フロー

図 15 に、ACE コンテキストと FWSM コンテキストを透過モードで使用した場合のデータセンターにおける APP\_TOP サーバ/データベースサーバ間のトラフィックフローを示します。APPL\_TOP サーバは、TNS ポート上で TCP を通じてデータベースサーバに要求を行っています。このトポロジの APPL\_TOP 層とデータベース層の間の正常なトランザクションは、次の手順で行われます。

1. APPL\_TOP サーバはポート 1521 への TCP 接続を通じてデータベース要求を開始します。要求はサーバのデフォルトゲートウェイ（この場合は MSFC）に送信されます。
2. 透過モードの FWSM コンテキストは、内部インターフェイスから外部インターフェイスへトラフィックをブリッジします。トラフィックの転送は、システム管理者によって確立されたセキュリティルールに依存します。この場合は、ポート 1521 上でのデータベースサーバへの APPL\_TOP トラフィックが許可されます。
3. 透過モードの ACE コンテキストは、内部インターフェイスから外部インターフェイスにトラフィックをブリッジし、APPL\_TOP サーバのデフォルトゲートウェイである MSFC にトラフィックを渡します。ACE はロードバランシングサービスを提供するように設定されていません。APPL\_TOP/データベース間のトラフィックは単にブリッジされますが、ACL が適用される場合があります。

4. MSFC はトラフィックをデータベース サーバにルーティングします。
5. データベース層のファイアウォール コンテキストは外部インターフェイスで要求を受信します。FWSM コンテキストは、TNS トラフィックが許可されることを判断し、要求をデータベース サーバに転送して、ローカル接続テーブル内で新しい接続を作成します。
6. データベース サーバは TNS 要求に応答し、デフォルト ゲートウェイの MSFC に応答を転送します。
7. ファイアウォール コンテキストはトラフィックを MSFC にブリッジします。
8. MSFC は、アプリケーション レイヤの ACE コンテキストを通じて、データベース サーバの応答を APPL\_TOP サーバにルーティングします。ACE は外部インターフェイスから内部インターフェイスへトラフィックをブリッジします。
9. 最初の TCP SYN パケットによって作成された有効な接続エントリに基づき、応答が FWSM コンテキストによって発信元のサーバに透過的にブリッジされます。
10. TNS 応答が APPL\_TOP サーバに到達します。

図 15 サーバ/データベース間のトラフィック (透過モード)



## ACE 透過モード設計のアーキテクチャの詳細

ここでは、テストベッドのアプリケーションおよびネットワーク トポロジについて説明します。トピックは次のとおりです。

- Oracle E-Business Suite 11i 環境
- Oracle E-Business Suite 11i 環境と統合ネットワーク サービス
- その他の統合サービス オプション

## Oracle E-Business Suite 11i 環境

17 ページの「ACE ワンアーム モード設計のアーキテクチャの詳細」で説明した Oracle 11i アプリケーション トポロジは変わりません。このことは、ネットワーク サービスの追加、削除、または変更がサポート対象のアプリケーション環境に対して透過的であることを意味しており、きわめて重要です。透過モード設計で使用するソフトウェアおよびハードウェアの詳細については、前述のアーキテクチャの詳細を参照してください。

## Oracle E-Business Suite 11i 環境と統合ネットワーク サービス

ここで紹介するネットワーク サービスでは、18 ページの「Oracle E-Business Suite 11i 環境と統合ネットワーク サービス」で説明したソフトウェアおよびハードウェアと同じものを使用します。アプリケーションおよびネットワークの物理インフラストラクチャは、ワンアーム設計と透過設計のどちらでも同じです。詳細については、前のセクションを参照してください。

## トポロジ

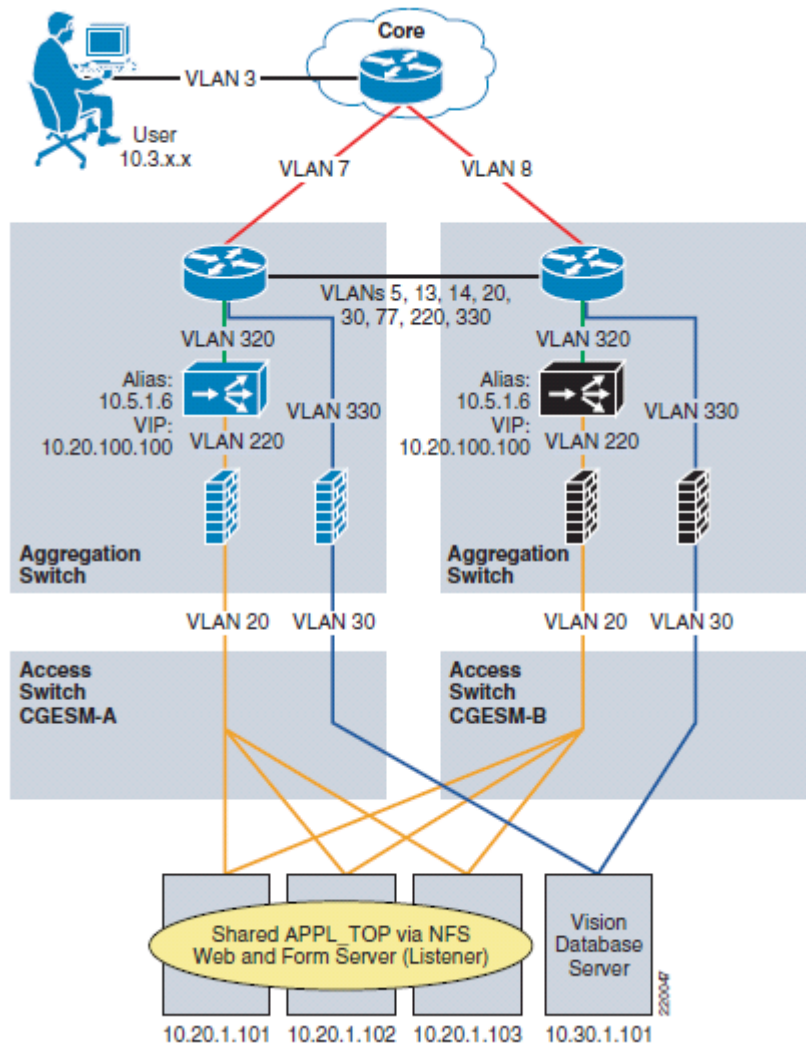
図 16 に、単一の ACE 仮想コンテキストと 2 つの FWSM 仮想コンテキストで構成される透過サービス チェーンの論理設計を示します。ACE コンテキストは、FWSM コンテキストの背後に常駐する実際の APPL\_TOP サーバを利用する仮想 IP アドレスを通じて、ロード バランシングとセッション永続性を提供します。



(注)

図 16 では、2 つのアグリゲーション スイッチ間の ISL により、運用トラフィック VLAN の 20、30、220、330 と、フォールトトレラントおよびレプリケーション VLAN の 13、14、77 が伝達されます。

図 16 透過テストベッドトポロジ



(注)

セッション永続性は、送信元 / 宛先 IP を使用して、または ACE クッキーを挿入することにより実現されます。これらの各方式は Oracle によってサポートされており、次の設定リストで示されています。サポートされるロード バランシング方式の詳細については、「Oracle Metalink ドキュメント 217368.1」を参照してください。

APPL\_TOP サーバは、Catalyst 6500 シリーズ サービス モジュールによって提供される透過サービスを認識しません。APPL\_TOP サーバはデータベース サーバと同じように、MSFC をデフォルト ゲートウェイとして使用します。データベース サーバは、独自の仮想ファイアウォール コンテキストの背後に常駐しています。透過仮想デバイスにまたがる接続エントリによってクライアントとサーバの IP アドレッシングが維持され、アプリケーション レベルおよびネットワーク レベルでのロギングが簡素化されます。

透過サービス チェーンにまたがるサーバ / サーバ間接続の例を次に示します。

```
ace# show connection
conn-id np dir proto vlan source destination state
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
7 1 in TCP 220 10.20.1.102:32869 10.30.1.101:1521 ESTAB
6 1 out TCP 320 10.30.1.101:1521 10.20.1.102:32869 ESTAB
fws# show connection
TCP out 10.30.1.101:1521 in 10.20.1.102:32869 idle 0:00:05 Bytes 155360 FLAGS - UOI
```

図 16 は、アクティブ / スタンバイ シナリオで設定された ACE および FWSM も示しています。これらはそれぞれ接続とスティッキ エントリをピアデバイスにレプリケートしてクライアント / サーバ間トラフィックとサーバ / サーバ間トラフィックの両方に可用性の高い永続的な接続を提供する機能を備えます。この設定では、ACE のフェールオーバー時間は 1 秒以下です。

データセンター インフラストラクチャのフェールオーバー時間と復元時間は、[http://www.cisco.com/univercd/cc/td/doc/solution/dci\\_srnd.pdf](http://www.cisco.com/univercd/cc/td/doc/solution/dci_srnd.pdf) で参照できます。詳しい設定については、36 ページの「ネットワーク設定例」と 29 ページの「アプリケーション設定の詳細」を参照してください。

## その他のサービス統合オプション

このドキュメントでは、Oracle のエンタープライズ クラス アプリケーションである E-Business Suite へのネットワーク サービスの統合について説明しています。サーバ ロード バランシングとセキュリティは、データセンター アプリケーションによって使用される基本的なサービスです。しかし、企業が使用できる統合ネットワーク サービスはこれだけではありません。次のネットワーク サービスもサービス モジュールまたはアプライアンスとして簡単に使用できます。

- SSL オフローディング (ACE プラットフォームに統合されたハードウェアベース オプション)
- 侵入防御システム
- 侵入検知システム
- ネットワーク分析デバイス
- WAN 最適化システム (WAAS、AVS)
- キャッシング デバイス

## アプリケーション設定の詳細

ここでは、アプリケーション環境について説明します。これには、次のようなソフトウェア環境への特別な変更が含まれます。

- HTTP ロード バランシング
- フォーム リスナ サーブレット
- SSL アクセラレータ
- クッキーとセッション永続性

ここでは、AutoConfig と呼ばれる Oracle 管理ツールを主に使用します。AutoConfig は、アプリケーション コンテキスト ファイルと一連のスクリプトを使用して、Oracle アプリケーション システムの変更を管理します。コンテキスト ファイルは XML 形式を使用し、単一のノード上のアプリケーション環境を表します。Oracle AutoConfig ツールにより、アプリケーション環境が簡素化および標準化されます。



(注)

コンテキスト ファイルの命名規則は、SID\_hostname.xml です。たとえば、ここで示す Version データベース環境では、node1 のコンテキスト ファイルは VIS\_node1.xml という名前になります。

図 17 に示す Oracle Applications Manager ( OAM ) GUI を使用すると、コンテキスト ファイルを直接設定したり、一連の設定ウィザードを使用して既存のアプリケーション ノードを変更したりすることができます。このドキュメントでは、AutoConfig および OAM の機能については説明しませんが、重要なのは、OAM を使用して個々のコンテキスト ファイルの内容を管理することに加えて、各サーバ ノードでローカルの adautocfg スクリプトを使用することです。このスクリプトを使用しないと、変更がアプリケーション環境に反映されません。

図 17 Oracle Applications Manager

Select Details	Name	Host	Last Synchronized Date	Last Update Date	Tier	Synchronized	Home	Show Cells
<input type="checkbox"/>	db1	db1	29-09-2006 10:36:25	29-09-2006 10:36:25	Database	<input checked="" type="checkbox"/>		db1
<input type="checkbox"/>	node1	node1	29-09-2006 16:19:07	29-09-2006 16:19:07	Applications	<input checked="" type="checkbox"/>		node1
<input type="checkbox"/>	node2	node2	29-09-2006 16:22:49	29-09-2006 16:22:49	Applications	<input checked="" type="checkbox"/>		node2
<input type="checkbox"/>	node3	node3	29-09-2006 16:27:20	29-09-2006 16:27:20	Applications	<input checked="" type="checkbox"/>		node3

## HTTP ロード バランシング

Oracle E-Business Suite 11i でハードウェアベースのロード バランサを使用するには、次の手順を実行します。

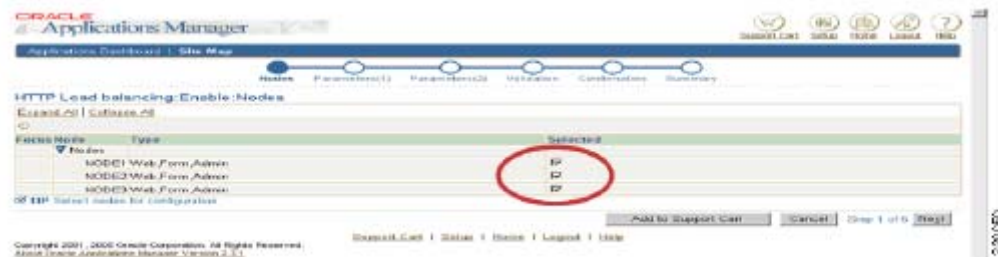
**ステップ 1** OAM にログインし、[Site Map - System Administration] タブを選択して、[AutoConfig] を選択します (図 17)。

**ステップ 2** [Launch Wizards] をクリックします。

**ステップ 3** HTTP ロード バランシングを有効にします。



**ステップ 4** ACE サーバ ファーム設定に実際のサーバとして含めるノードを選択します。



**ステップ 5** Oracle アプリケーションで整形形式の URL を作成するために必要な情報を指定します。

- s\_webentryhost : クライアントによって利用される ACE VIP の DNS 名。
- t\_session\_persistent : ACE コンテキストでクッキーまたは送信元 / 宛先間 IP ベースのスティッキを使用する場合は、チェック ボックスをオンにします。
- s\_webentrydomain : VIP に関連付けられるドメイン名。
- s\_webentryprotocol : http または https。
- Active Web Port s\_active\_webport : デフォルトでは、この値は 8000 です。この値を独自の値に変更するか、既知の HTTP ポート値である「80」を使用します。

Title	Parameter Name	Value	Description
Web Host entry point	s_webentryhost	web	The host name of the HTTP load balancer from which all incoming http requests are distributed.
	l_session_persistent	<input checked="" type="checkbox"/>	Check if HTTP load balancer supports session-persistent client connections.
	l_dns	<input type="checkbox"/>	Check if DNS Layer load balancing is in use.
Web domain entry point	s_webentrydomain	ocelab.com	The HTTP load-balancer's domain name.
Web entry protocol	s_webentryprotocol	http	This Web entry protocol. Acceptable values for this parameter are http or https.
Active Web Port	s_active_webport	80	The Active Web port should be set to the HTTP load-balancer's external port.

**TIP** For additional information on configuring the E-Business Suite Release 11i with HTTP Load-balancer information, please see the Oracle MetaLink Note 217386.1, Advanced Configurations and Topologies for Enterprise Deployments of E-Business Suite 11i.

**ステップ 6** この時点で、一連の検証パネルと確認パネルが表示されます。これらの手順を正しく完了すると、選択した各サーバノードのコンテキストファイルに基本的なロードバランシング設定が保存されます。

**ステップ 7** 対象の各ノードで `adstpall` スクリプトを使用し、現在実行されている Oracle アプリケーションをすべて停止します。

**ステップ 8** 各ノードで `adautocfg` スクリプトを実行します。

**ステップ 9** `adstrtall` スクリプトを使用し、すべてのサーバノードを起動します。



#### 注意

このプロセスの実行中に各ノードがデータベースサーバにアクセスする必要があるため、データベースは停止しないでください。

## フォームリスナサブレット

フォームリスナサブレットを使用すると、Webサーバを通じて Oracle アプリケーション環境内のフォームサーバにアクセスできます。詳細については、3 ページの「デスクトップ層」を参照してください。フォームリスナサブレットを有効にするには、次の手順を実行します。

**ステップ 1** OAM にログインし、[Site Map - System Administration] タブを選択して、[AutoConfig] を選択します (図 17)。

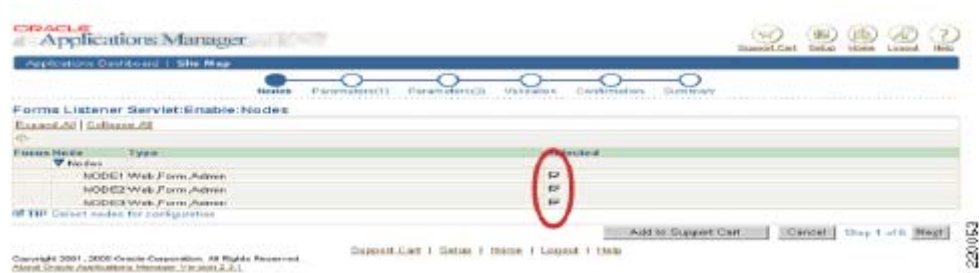
**ステップ 2** [Launch Wizards] を選択します。

**ステップ 3** [Enable Forms Listener Servlet] ボタンをクリックします。

■ アプリケーション設定の詳細



ステップ4 フォーム リスナ サブレットを使用するアプリケーション サーバ ノードを選択します。



ステップ5 フォーム リスナ サブレットのパラメータが公開されます。デフォルトのフォーム サブレット URL が表示されるので、必要な場合に限り変更します。s\_forms\_servlet\_comment が空白であることを確認してサービスを有効にするか、フィールドに # を入力してフォーム リスナ サブレットを無効にします。



- ステップ 6** この時点で、一連の検証パネルと確認パネルが表示されます。これらの手順を正しく完了すると、選択した各サーバノードのコンテキスト ファイルに基本的なロード バランシング設定が保存されます。
- ステップ 7** 対象の各ノードで `adstpall` スクリプトを使用し、現在実行されている Oracle アプリケーションをすべて停止します。
- ステップ 8** 各ノードで `adautocfg` スクリプトを実行します。
- ステップ 9** `adstrtall` スクリプトを使用し、すべてのサーバノードを起動します。

**注意**

このプロセスの実行中に各ノードがデータベース サーバにアクセスする必要があるため、データベースは停止しないでください。

## SSL アクセラレータ

SSL アクセラレータ ウィザードでは、暗号化サービスとサーバ オフロードに外部デバイスを使用するように Oracle 11i 環境を設定します。次の手順に、E-Business Suite で SSL アクセラレーションを有効にする方法をまとめます。

- ステップ 1** OAM にログインし、[Site Map - System Administration] タブを選択して、[AutoConfig] を選択します (図 17)。
- ステップ 2** [Launch Wizards] を選択します。
- ステップ 3** [Enable SSL Accelerator] ボタンをクリックします。

The screenshot shows the Oracle Applications Manager interface. The main content area is titled 'Configuration Wizards' and contains a table with the following data:

Configuration Name	Description	Action
HTTP Load balancing	Use this option to configure HTTP Load Balancing for an E-Business Suite Release 11i system if you have a third party HTTP load balancer. Use this option to also disable HTTP Load Balancing.	Enable Disable
SSL	Use this option to configure SSL for an E-Business Suite Release 11i system.	Enable Disable
SSL Accelerator	Use this option to configure an E-Business Suite Release 11i system with a SSL accelerator.	Enable Disable
Forms Listener Sentinel	Use this option to enable or disable the Forms Listener Sentinel for an E-Business Suite Release 11i system.	Enable Disable
Apache JSEv load balancing	Use this option to enable or disable Apache Jserv Load Balancing across multiple Web nodes for an E-Business Suite Release 11i system.	Enable Disable

The 'Enable' button for the 'SSL Accelerator' row is circled in red. To the right of the table is a 'Resources' section with an 'Information' box that says: 'Please setup your MetaLink Credentials to view external resources.'

At the bottom of the page, there is a footer with the text: 'Copyright 2001, 2005 Oracle Corporation. All Rights Reserved. About Oracle Applications Manager Version 2.3.1' and navigation links: 'Support Cart | Setup | Home | Logout | Help'.

## ■ アプリケーション設定の詳細

**ステップ 4** SSL アクセラレータ サービスを使用するノードを選択します。

Oracle Applications Manager  
Applications Dashboard | Site Map

Nodes Parameters(1) Parameters(2) Validation Confirmation Summary

SSL Accelerator:Enable:Nodes

Expand All | Collapse All

Focus Node	Type	Selected
▼ Nodes		
NCOE1	Web Form,CP Admin	<input checked="" type="checkbox"/>
NCOE2	Web Form,CP Admin	<input checked="" type="checkbox"/>
NCOE3	Web Form,CP Admin	<input checked="" type="checkbox"/>

TIP Select nodes for configuration

Add to Support Cart Cancel Step 1 of 6 Next

Support Cart | Setup | Home | Logout | Help

Copyright 2001, 2005 Oracle Corporation. All Rights Reserved.  
About Oracle Applications Manager Version 11.1.1

220121

**ステップ 5** Oracle アプリケーションで整形形式の URL を作成するために必要な情報を指定します。

- s\_webentryhost : クライアントによって使用される ACE VIP の DNS 名。
- s\_webentrydomain : VIP に関連付けられるドメイン名。
- Active Web Port s\_active\_webport : デフォルトでは、この値は 8000 です。この値を独自の値に変更するか、既知の HTTPS ポート値である 443 を使用します。

Oracle Applications Manager  
Applications Dashboard | Site Map

Nodes Parameters(1) Parameters(2) Validation Confirmation Summary

SSL Accelerator:Enable:Parameters(1)

Title	Parameter Name	Value	Description
Web Host entry point	s_webentryhost	web	The SSL accelerator's host name.
Web domain entry point	s_webentrydomain	eselab.com	The SSL Accelerator's domain name
Active Web Port	s_active_webport	8000	The Active Web port should be set to the SSL accelerator's external interfacing port.
	t_ssl_accelerator	off	SSL accelerator is in use
URL Protocol	s_url_protocol	http	URL Protocol
Local URL Protocol	s_local_url_protocol	http	Local URL Protocol
Web entry protocol	s_webentryurlprotocol	https	Web entry Protocol

TIP Note that the URL protocol, Local URL protocol, and Web entry protocol are set automatically to the values shown above. For additional information on configuring the E-Business Suite Release 11i with SSL Accelerator, please see the Oracle MetaLink Note 217399.1 - Advanced Configurations and Topologies for Enterprise Deployments of E-Business Suite 11i, and the Oracle MetaLink Note 123718.1 - A Guide to Understanding and Implementing SSL with Oracle Applications 11i.

Add to Support Cart Cancel Back Step 2 of 6 Next

Support Cart | Setup | Home | Logout | Help

Copyright 2001, 2005 Oracle Corporation. All Rights Reserved.  
About Oracle Applications Manager Version 11.1.1

220122

**ステップ 6** この時点で、一連の検証パネルと確認パネルが表示されます。これらの手順を正しく完了すると、選択した各サーバノードのコンテキストファイルに基本的なロード バランシング設定が保存されます。

- ステップ 7** 対象の各ノードで `adstpall` スクリプトを使用し、現在実行されている Oracle アプリケーションをすべて停止します。
- ステップ 8** 各ノードで `adautocfg` スクリプトを実行します。
- ステップ 9** `adstrtall` スクリプトを使用し、すべてのサーバノードを起動します。

**注意**

このプロセスの実行中に各ノードがデータベースサーバにアクセスする必要があるため、データベースは停止しないでください。

## クッキーとセッションの永続性

クッキーは、ユーザおよびそのユーザ固有のセッションに関する情報を維持するために、Webサーバによって設定されるデータの集まりです。クッキーを受け入れるように設定された Web ブラウザは、クッキーに対応した Web サイトに関連するすべてのクッキーを以降の各要求で再送信します。この動作により、ACE でクッキーデータを使用してセッション永続性を提供することが可能になります。ACE モジュールは、サーバまたは ACE によって生成されたクッキーを使用し、接続スティックを提供することができます。以下にテストベッドの Oracle E-Business Web サイトの初期ログインページに対する HTTP ヘッダーを示します。次の例に示す `Set-Cookie` コマンドは、ACE 仮想コンテキストによって挿入されています。クッキーに対応した Web ブラウザからの以降の HTTP 要求には、このデータと、Web サイトに関連するその他のクッキーが含まれます。ACE モジュールはスティックテーブルを維持し、このクッキーに基づいてクライアントを同じ `APPL_TOP` サーバに戻します。

```
GET /OA_HTML/AppsLocalLogin.jsp HTTP/1.1
Accept: */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: web.eselab.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Set-Cookie: acecookie=R193696788; path=/; expires=Wed, 18-Oct-2006 03:47:09 GMT
Date: Tue, 17 Oct 2006 03:36:40 GMT
Cache-Control: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Pragma: no-cache
Keep-Alive: timeout=15
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

GET /OA_HTML/cabo/styles/cache/oracle-desktop-2_2_18-en-ie-6-windows.css HTTP/1.1
Accept: */*
Referer: http://web.eselab.com/OA_HTML/AppsLocalLogin.jsp
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 1.1.4322)
Host: web.eselab.com
Connection: Keep-Alive
Cookie: acecookie=R193696788
```

## ネットワーク設定例

ここでは、テストの実行中に Oracle 11i アプリケーションとデータベースをサポートした Catalyst 6500 MSFC、ACE、および FWSM のネットワーク設定を示します。ここでは、制約のないセキュリティ Access Control List (ACL; アクセス コントロール リスト) について説明します。これらのリストは、運用環境に実装する前に変更し、クライアントと階層の間で許容されるトラフィック フロー用の特定のアクセス コントロール エントリ ステートメントを作成する必要があります。ACE と FWSM は、それぞれこの機能を備えています。

### Catalyst 6500 MSFC

ここでは、Catalyst 6500 MSFC のネットワーク設定を示します。

#### プライマリアグリゲーション スイッチ

関連する VLAN への ACE および FWSM のアクセスを許可します。

```
firewall multiple-vlan-interfaces
firewall module 8 vlan-group 3,20,77,146,220
svclc multiple-vlan-interfaces
svclc module 13 vlan-group 1,146,220,320
svclc vlan-group 1 5,13
svclc vlan-group 3 30,330
svclc vlan-group 20 20
svclc vlan-group 77 77
svclc vlan-group 146 146
svclc vlan-group 220 220
svclc vlan-group 320 320
```

アグリゲーション スイッチ間の ISL を設定します。このリンクでフォールトトレラント VLAN と運用 VLAN を伝達するか、またはトラフィックを複数の ISL に分割することができます。ISL の主な目的は、データセンターにパスの冗長性を提供することです。

```
interface Port-channel6
description <<*& ISL between dc01agg Ten12/3 - 4 *&>>
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 5,13,14,20,30,77,220,320,330
switchport mode trunk
no ip address
logging event link-status
logging event spanning-tree status
logging event bundle-status
logging event trunk-status
load-interval 30
```

サーバのデフォルト ゲートウェイの可用性を高めるために、HSRP を使用します。ワンアーム モードの ACE SVI 設定を次に示します。

```
interface Vlan5
description <<*& ACE OneArm VLAN *&>>
ip address 10.5.1.2 255.255.0.0
no ip redirects
no ip proxy-arp
logging event link-status
load-interval 30
standby 1 ip 10.5.1.1
standby 1 timers 1 3
standby 1 priority 51
standby 1 preempt delay minimum 120
standby 1 name ace
!
```

次の例は、アプリケーション サーバのデフォルト ゲートウェイとしての ACE 透過モード SVI を示しています。

```
interface Vlan320
  description <<** App Server DGW **>>
  ip address 10.20.1.2 255.255.0.0
  no ip redirects
  no ip proxy-arp
  ip route-cache flow
  logging event link-status
  load-interval 30
  standby 1 ip 10.20.1.1
  standby 1 timers 1 3
  standby 1 priority 51
  standby 1 preempt delay minimum 120
  standby 1 name app
!
interface Vlan330
  description <<** DB Server DGW **>>
  ip address 10.30.1.2 255.255.0.0
  no ip redirects
  no ip proxy-arp
  ip route-cache flow
  logging event link-status
  load-interval 30
  standby 1 ip 10.30.1.1
  standby 1 timers 1 3
  standby 1 priority 51
  standby 1 preempt delay minimum 120
  standby 1 name db
```

## セカンダリアグリゲーション スイッチ

セカンダリアグリゲーション スイッチの設定は、プライマリアグリゲーション スイッチとほぼ同じであり、可用性が高く予測可能なレイヤ 2 および 3 環境を提供しつつ、サービスの統合を可能にします。

```
firewall multiple-vlan-interfaces
firewall module 8 vlan-group 3,20,77,146,220
svclc multiple-vlan-interfaces
svclc module 13 vlan-group 1,146,220,320
svclc vlan-group 1 5,13
svclc vlan-group 3 30,330
svclc vlan-group 20 20
svclc vlan-group 77 77
svclc vlan-group 146 146
svclc vlan-group 220 220
svclc vlan-group 320 320
interface Port-channel6
  description <<** ISL between dc03agg Ten12/3 - 4 **>>
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 5,13,14,20,30,77,220,320,330
  switchport mode trunk
  no ip address
  logging event link-status
  logging event spanning-tree status
  logging event bundle-status
  logging event trunk-status
  load-interval 30
!
```

```
interface Vlan5
  description <<** ACE OneArm VLAN **>>
  ip address 10.5.1.3 255.255.0.0
  no ip redirects
  no ip proxy-arp
  logging event link-status
  load-interval 30
  standby 1 ip 10.5.1.1
  standby 1 timers 1 3
  standby 1 priority 50
  standby 1 preempt
  standby 1 name ace
!
interface Vlan320
  description <<** App Server DGW **>>
  ip address 10.20.1.3 255.255.0.0
  no ip redirects
  no ip proxy-arp
  logging event link-status
  load-interval 30
  standby 1 ip 10.20.1.1
  standby 1 timers 1 3
  standby 1 priority 50
  standby 1 preempt
  standby 1 name app
!
interface Vlan330
  description <<** DB Server DGW **>>
  ip address 10.30.1.3 255.255.0.0
  no ip redirects
  no ip proxy-arp
  logging event link-status
  load-interval 30
  standby 1 ip 10.30.1.1
  standby 1 timers 1 3
  standby 1 priority 50
  standby 1 preempt
  standby 1 name db
!
```

## ACE 管理設定

次の例は、ACE 管理サーバの設定を示しています。

```
dc03-ace/Admin# show run
Generating configuration....

login timeout 0
hostname dc03-ace
boot system image:c6ace-t1k9-mz.3.0.0_A1_2.bin

resource-class onearm
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource conc-connections minimum 20.00 maximum equal-to-min
  limit-resource rate connection minimum 20.00 maximum equal-to-min
  limit-resource sticky minimum 20.00 maximum equal-to-min
resource-class transparent
  limit-resource all minimum 0.00 maximum unlimited
  limit-resource conc-connections minimum 20.00 maximum equal-to-min
  limit-resource rate connection minimum 20.00 maximum equal-to-min
  limit-resource sticky minimum 20.00 maximum equal-to-min

access-list EVERYONE line 10 extended permit icmp any any
access-list EVERYONE line 20 extended permit ip any any

class-map type management match-any REMOTE_ACCESS
  10 match protocol telnet any
  20 match protocol ssh any
  30 match protocol icmp any

policy-map type management first-match REMOTE_MGMT_ALLOW_POLICY
  class REMOTE_ACCESS
    permit

interface vlan 146
  description Management Address
  ip address 172.xx.xx.xx 255.255.254.0
  peer ip address 172.xx.xx.xx 255.255.254.0
  access-group input EVERYONE
  access-group output EVERYONE
  service-policy input REMOTE_MGMT_ALLOW_POLICY
  no shutdown

ft interface vlan 13
  ip address 13.13.13.1 255.255.255.0
  peer ip address 13.13.13.2 255.255.255.0
  no shutdown

ft peer 1
  heartbeat interval 200
  heartbeat count 10
  ft-interface vlan 13
ft group 1
  peer 1
  priority 150
  peer priority 110
  associate-context Admin
  inservice

ip route 0.0.0.0 0.0.0.0 172.26.146.1

context onearm
  description Context for 1-Arm Testing
  allocate-interface vlan 5
  member onearm
context transparent
  description Context for Transparent Testing
  allocate-interface vlan 220
  allocate-interface vlan 320
```

```

member transparent

ft group 2
peer 1
priority 150
peer priority 110
associate-context onearm
inservice
ft group 3
peer 1
priority 150
peer priority 110
associate-context transparent
inservice
username admin password 5 $1$faXJEFBj$TJR1Nx7sLPTi5BZ97v08c/ role Admin domain
default-domain
username www password 5 $1$UZIiwUk7$QMvYN1JASaycabrHkhGcS/ role Admin domain
default-domain

```

## ACE ワンアーム モード設定

次の例は、ワンアーム モードの設定を示しています。

```

ace/onearm# show run
Generating configuration...

logging enable
logging standby
logging buffered 6

crypto csr-params testparams
country US
state California
locality SJ
organization-name ESE-AS
organization-unit Ch-US
common-name web.eselab.com
serial-number cisco123

access-list EVERYONE line 10 extended permit icmp any any alternate-address
access-list EVERYONE line 20 extended permit ip any any

probe http web
port 8000
interval 5
faildetect 15
passdetect interval 15
receive 2
expect status 200 200
open 2

parameter-map type ssl sslparams
cipher RSA_WITH_RC4_128_MD5
version SSL3

rserver host node1
ip address 10.20.1.101
inservice
rserver host node2
ip address 10.20.1.102
inservice
rserver host node3
ip address 10.20.1.103
inservice

```

```
ssl-proxy service testssl
  key test.key
  cert testcert.pem
  ssl advanced-options sslparams

serverfarm host WEB
  probe web
  rserver node1 8000
    inservice
  rserver node2 8000
    inservice
  rserver node3 8000
    inservice

sticky ip-netmask 255.255.255.255 address source sticky-src-ip
  timeout 10
  replicate sticky
  serverfarm WEB
sticky http-cookie acecookie sticky-cookie-insert
  cookie insert
  replicate sticky
  serverfarm WEB

class-map match-all ACL
  2 match access-list EVERYONE
class-map match-all VIP-APP-100
  2 match virtual-address 10.99.10.100 tcp eq 9000
class-map match-all VIP-SSL-99
  2 match virtual-address 10.99.10.99 tcp eq https
class-map match-all VIP-WEB-99
  2 match virtual-address 10.99.10.99 tcp eq www
class-map type management match-any remote-mgmt
  10 match protocol ssh any
  20 match protocol telnet any
  30 match protocol icmp any
  40 match protocol http any
  50 match protocol https any
class-map match-any server-initiated
  2 match source-address 10.20.0.0 255.255.0.0
class-map match-any test
  2 match virtual-address 0.0.0.0 0.0.0.0 any

policy-map type management first-match remote-access
  class remote-mgmt
    permit
policy-map type loadbalance first-match vip-pol-99
  class class-default
    sticky-serverfarm sticky-cookie-insert
policy-map type loadbalance first-match vip-pol-SSL-99
  class class-default
    sticky-serverfarm sticky-src-ip
policy-map multi-match lb-vip
  class VIP-WEB-99
    loadbalance vip inservice
    loadbalance policy vip-pol-99
    loadbalance vip icmp-reply
    nat dynamic 1 vlan 5
  class VIP-SSL-99
    loadbalance vip inservice
    loadbalance policy vip-pol-SSL-99
    loadbalance vip icmp-reply
    ssl-proxy server testssl
policy-map multi-match server-side
  class server-initiated
    nat dynamic 1 vlan 5

interface vlan 5
  ip address 10.5.1.4 255.255.255.0
  alias 10.5.1.6 255.255.255.0
```

```

peer ip address 10.5.1.5 255.255.255.0
access-group input EVERYONE
nat-pool 1 10.5.1.10 10.5.1.20 netmask 255.255.255.0 pat
service-policy input remote-access
service-policy input lb-vip
service-policy input server-side
no shutdown

ip route 0.0.0.0 0.0.0.0 10.5.1.1

```

## ACE 透過モード設定

次の例は、ACE 透過モードの設定を示しています。

```

dc03-ace/transparent# show run
Generating configuration...

logging enable
logging standby
logging buffered 6

crypto csr-params testparams
  country US
  state California
  locality SJ
  organization-name ESE-AS
  organization-unit Ch-US
  common-name web.eselab.com
  serial-number cisco123
access-list BPDU ethertype permit bpdud

access-list EVERYONE line 10 extended permit icmp any any alternate-address
access-list EVERYONE line 20 extended permit ip any any

probe http web
  port 8000
  interval 5
  faildetect 15
  passdetect interval 15
  receive 2
  expect status 200 200
  open 2

parameter-map type ssl sslparams
  cipher RSA_WITH_RC4_128_MD5
  version SSL3

rserver host node1
  ip address 10.20.1.101
  inservice
rserver host node2
  ip address 10.20.1.102
  inservice
rserver host node3
  ip address 10.20.1.103
  inservice

ssl-proxy service testssl
  ssl advanced-options sslparams

serverfarm host WEB
  probe web
  rserver node1 8000
    inservice
  rserver node2 8000
    inservice
  rserver node3 8000

```

```
inservice

sticky ip-netmask 255.255.255.255 address source sticky-src-ip
  timeout 10
  replicate sticky
  serverfarm WEB
sticky http-cookie acecookie sticky-cookie-insert
  cookie insert
  replicate sticky
  serverfarm WEB

class-map match-all ACL
  2 match access-list EVERYONE
class-map match-all AppVIP
  description class-map for appltop loadbalancing
  10 match virtual-address 10.20.100.100 tcp eq www
class-map type management match-any remote-mgmt
  10 match protocol ssh any
  20 match protocol telnet any
  30 match protocol icmp any
  40 match protocol http any
  50 match protocol https any
class-map match-all server-initiated
  description NAT Server Initiated Connections to the VIP
  2 match source-address 10.20.0.0 255.255.0.0
  3 match destination-address 10.20.100.100 255.255.255.255

policy-map type management first-match remote-access
  class remote-mgmt
    permit
policy-map type loadbalance first-match VIP-POL-100
  class class-default
    sticky-serverfarm sticky-cookie-insert
policy-map multi-match SLB_WEB
  class server-initiated
    nat dynamic 1 vlan 220
  class AppVIP
    loadbalance vip inservice
    loadbalance policy VIP-POL-100
    loadbalance vip icmp-reply

interface vlan 220
  description South Side Server VLAN
  bridge-group 1
  access-group input BPDU
  access-group input EVERYONE
  nat-pool 1 10.20.254.250 10.20.254.254 netmask 255.255.255.0 pat
  service-policy input remote-access
  service-policy input SLB_WEB
  no shutdown
interface vlan 320
  description North Side ACE VLAN
  bridge-group 1
  access-group input BPDU
  access-group input EVERYONE
  service-policy input remote-access
  service-policy input SLB_WEB
  no shutdown

interface bvi 1
  ip address 10.20.1.5 255.255.0.0
  alias 10.20.1.7 255.255.0.0
  peer ip address 10.20.1.6 255.255.0.0
  no shutdown

ip route 0.0.0.0 0.0.0.0 10.20.1.1
```

## FWSM 管理設定 (管理コンテキスト)

次の例は、FWSM の設定を示しています。

```
FWSM(config)# show run
: Saved
:
FWSM Version 3.1(1) <system>
!
resource acl-partition 12
hostname FWSM
domain-name cisco.com
enable password 2KFQnbNIdI.2KYOU encrypted
!
interface Vlan20
  description APPL_TOP VLAN
!
interface Vlan30
  description DATABASE VLAN
!
interface Vlan77
  description LAN/STATE Failover Interface
!
interface Vlan146
  description MGMT VLAN
!
interface Vlan220
  description APPL_TOP Bridge VLAN
!
interface Vlan330
  description DATABASE Bridge VLAN
!
passwd 2KFQnbNIdI.2KYOU encrypted
class default
  limit-resource ASDM 5
  limit-resource IPsec 5
  limit-resource Mac-addresses 65535
  limit-resource SSH 5
  limit-resource Telnet 5
  limit-resource All 0
!

ftp mode passive
pager lines 30
failover
failover lan unit secondary
failover lan interface fover Vlan77
failover polltime unit msec 500 holdtime 3
failover polltime interface 3
failover interface-policy 1%
failover replication http
failover link fover Vlan77
failover interface ip fover 10.77.1.1 255.255.0.0 standby 10.77.1.2
asdm history enable
arp timeout 14400
username admin password e1z89R3cZe9Kt6Ib encrypted
console timeout 0
admin-context admin
context admin
  allocate-interface Vlan146 int1
  config-url disk:/admin.cfg
!

context appltop
  description <<*** Bridge VLAN 220 - 20 (11i APPL_TOP) ***>>
  allocate-interface Vlan20
  allocate-interface Vlan220
  config-url disk:/tp220-20.cfg
!
```

```

context db
  description <<** Bridge VLAN 330 - 30 (11i DB) **>>
  allocate-interface Vlan30
  allocate-interface Vlan330
  config-url disk:/tp330-30.cfg
!

prompt hostname context
Cryptochecksum:2f7216a14c3b94aeb334b38cf19e7b9b
: end

```

## FWSM 透過モード設定 (データベース コンテキスト)

次の例は、透過モードの FWSM の設定を示しています。

```

FWSM/db(config)# show run
: Saved
:
FWSM Version 3.1(1) <context>
!
firewall transparent
hostname db
domain-name eselab.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Vlan30
  nameif inside
  bridge-group 1
  security-level 100
!
interface Vlan330
  nameif outside
  bridge-group 1
  security-level 0
!
interface BV11
  ip address 10.30.1.4 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list outside extended permit ip any any log
access-list inside extended permit ip any any log
access-list BPDU ethertype permit bpdu
pager lines 35
logging enable
logging timestamp
logging buffered informational
logging trap informational
logging asdm informational
logging queue 0
logging device-id hostname
mtu outside 1500
mtu inside 1500
icmp permit any outside
icmp permit any inside
no asdm history enable
arp timeout 14400
access-group BPDU in interface outside
access-group outside in interface outside
access-group BPDU in interface inside
access-group inside in interface inside
route outside 0.0.0.0 0.0.0.0 10.30.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00

```

```

timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 360
ssh timeout 5
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect smtp
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
    inspect sqlnet
!
service-policy global_policy global
Cryptochecksum:c74e5affba450ceb83052cf618bf7996
: end

```

## FWSM 透過モード設定 (APPL\_TOP コンテキスト)

次の例は、FWSM APPL\_TOP コンテキストの設定を示しています。

```

FWSM/appltop(config)# show run
: Saved
:
FWSM Version 3.1(1) <context>
!
firewall transparent
hostname appltop
domain-name eselab.com
enable password 2KFQnbNIdI.2KYOU encrypted
names
!
interface Vlan220
  nameif outside
  bridge-group 1
  security-level 0
!
interface Vlan20
  nameif inside
  bridge-group 1
  security-level 100
!
interface BVI1
  ip address 10.20.1.4 255.255.0.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list outside extended permit ip any any log
access-list inside extended permit ip any any log
access-list BPDU ethertype permit bpdu
pager lines 24
logging enable
logging timestamp
logging buffered informational

```

```
logging trap informational
logging asdm informational
logging queue 0
logging device-id hostname
mtu outside 1500
mtu inside 1500
icmp permit any outside
icmp permit any inside
no asdm history enable
arp timeout 14400
access-group BPDU in interface outside
access-group outside in interface outside
access-group BPDU in interface inside
access-group inside in interface inside
route outside 0.0.0.0 0.0.0.0 10.20.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
!
class-map inspection_default
  match default-inspection-traffic
!
!
policy-map global_policy
  class inspection_default
    inspect dns maximum-length 512
    inspect ftp
    inspect h323 h225
    inspect h323 ras
    inspect rsh
    inspect smtp
    inspect sqlnet
    inspect skinny
    inspect sunrpc
    inspect xdmcp
    inspect sip
    inspect netbios
    inspect tftp
!
service-policy global_policy global
Cryptochecksum:822088e52ddf41626a20bf206a13b80c
: end
```

## 付録

表 1 に、テストに使用する Oracle E-Business Suite 11i 10.5.2 のデフォルトのポート値を示します。これらのポート値を参考にして、ACE および FWSM 上のセキュリティ ポリシーを作成することができます。

表 1 Oracle 11i 環境のデフォルトのポート値

説明	ポート値
データベース ポート	1521
RPC ポート	1626
レポート ポート	7000
Web リスナ ポート	8000
OProcMgr ポート	8100
Web PLSQL ポート	8200
サブレット ポート	8800
フォーム リスナ ポート	9000
Metrics サーバ データ ポート	9100
JTF フルフィルメント サーバ ポート	9200
Map Viewer Servlet ポート	9800
OEM Web ユーティリティ ポート	10000
VisBroker OrbServer Agent ポート	10100
MSCA サーバ ポート	10200
MSCA ディスパッチャ ポート	10300
Java オブジェクトキャッシュ ポート	12345
OACORE サブレット ポート	16000-16009
ディスカバラ サブレット ポート	17000-17009
フォーム サブレット ポート	18000-18009
XMLSVCS サブレット ポート	19000-19009



(注) 表 1 に示す用語の詳細については、[www.oracle.com](http://www.oracle.com) および [www.cisco.com](http://www.cisco.com) を参照してください。

## リファレンス

ここでは、その他のリファレンスを示します。

ACE のドキュメントについては、

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_1cn/ace/ace\\_301/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_1cn/ace/ace_301/index.htm) を参照してください。

FWSM のドキュメントについては、

[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod\\_1cn/fwsm/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_1cn/fwsm/index.htm) を参照してください。

Oracle Metalink ドキュメント ID 233428.1 : 「Oracle Applications 11i でのアプリケーション層ファイル システムの共有」

Oracle Metalink ドキュメント ID 217368.1 : 「E-Business Suite 11i のエンタープライズ導入の高度な設定とトポロジ」

Oracle Metalink ドキュメント ID 233428.1 : 「Oracle Applications 11i でのフォーム リスナ サープレットの使用」

Oracle Applications 11i ( 11.5.10.2 ) ドキュメント ライブラリ :  
[http://download-east.oracle.com/docs/cd/B25516\\_08/current/html/docset.html](http://download-east.oracle.com/docs/cd/B25516_08/current/html/docset.html)

## 用語集

表 2 に、このドキュメントで使用した主な用語の一部を示します。

表 2 用語集

用語	定義
Cisco Application Control Engine ( ACE )	Cisco Application Control Engine は、Catalyst 6500 シリーズ スイッチ内のモジュールです。特定の物理プラットフォーム内の論理グループを通じてアプリケーション リソースを分散および管理することを可能にします。また、高レベルなレイヤ 4-7 パフォーマンス ( 16 Gbps と毎秒 345,000 件の接続 ) を提供してアプリケーション パフォーマンスを最適化し、スケーラビリティを実現します。ACE サービス モジュールの詳細については、 <a href="http://www.cisco.com/en/US/products/ps6906/index.html">http://www.cisco.com/en/US/products/ps6906/index.html</a> を参照してください。
Cisco Firewall Services Module ( FWSM )	Cisco Firewall Services Module( FWSM )は、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータ用の高速な統合ファイアウォール モジュールです。業界最速のファイアウォール データ速度 ( 5 Gbps のスループット、100,000 CPS、および 1 M の同時接続 ) を提供します。単一のシャーシに最大 4 台までの FWSM をインストールし、シャーシごとに 20 Gbps までのスケーラビリティを実現できます。FWSM サービス モジュールの詳細については、 <a href="http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html">http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/index.html</a> を参照してください。
フォーム リスナ サープレット	Oracle Forms アプリケーションを HTTP 接続および HTTPS 接続上で実行できるようにする Java サープレットです。
MSFC Forms Server	Catalyst 6500 プラットフォーム用のマルチレイヤ スイッチ機能カードです。このフォーム サーバは、Oracle Applications フォームと、プロフェッショナルなインターフェイスをサポートする関連ランタイム エンジンを実行します。
サービス	単一のマシン上で実行されるプロセスのグループです。HTTP サービスなどの特定の機能を提供します。
階層	サービスのグループです。物理マシン間にまたがることもあります。階層は論理的なグループ分けを表し、それぞれに ( 複数の物理マシン上で実行される ) 特定のアプリケーションが展開された複数のネットワーク セグメント ( サブネット ) によって表すことができます。また、複数のアプリケーションを単一のネットワーク セグメントにマージすることも可能です。
透過モード	2 つの異なるレイヤ 2 セグメント間でトラフィックをブリッジしているネットワーク デバイスを表す用語です。

表 2 用語集 (続き)

用語	定義
Transparent Network Substrate (TNS)	TNS は、Oracle アプリケーション レイヤと Oracle データベース レイヤの間の接続を提供します。通常は SQL*Net プロトコルと呼ばれます。デフォルトのポート値は 1521 です。
Web サーバ	Apache によって駆動される Oracle HTTP サーバです。