Business Edition サーバで Cisco Expressway™ ソリューションを導入する際の考慮事項

2013 年 12 月 17 日

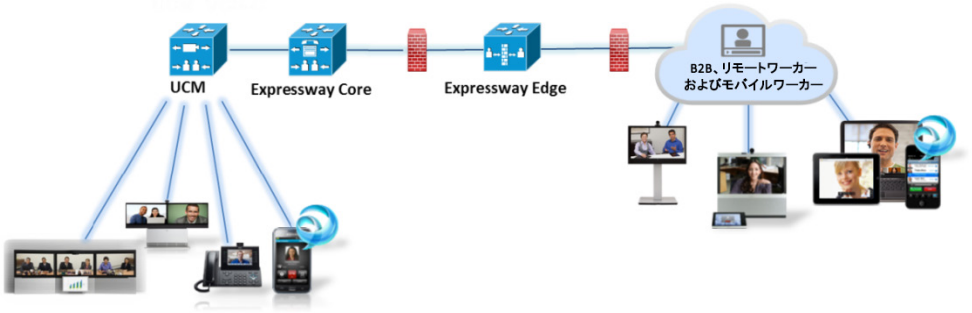
Contents

はじめに

一般的な Cisco Business Edition サーバを使用して、完全に仮想化された Cisco Expressway のリモートおよびモバイルのアクセス コラボレーション ソリューションを検討することができます。

Cisco Expressway ソリューションは、仮想プライベート ネットワークを必要とせずにリモート ビデオおよびモバイル クライアントとプライベート通信プラットフォームとの通信を可能にする Core コンポーネントと Edge コンポーネントで構成されます。これを行うため、パブリック インターネットから到達可能であり、プライベートドメインの Expressway Core サーバと安全に通信できるファイアウォール DMZ に Expressway Edge サーバが通常の場合インストールされます（図 1）。一般的な Business Edition 仮想ホストにインストールする場合は、この安全なネットワークトポロジの維持が必須です。このドキュメントでは、次の目標を達成するために考慮すべきさまざまなアプローチを示します。

図 1 Target Expressway トポロジ



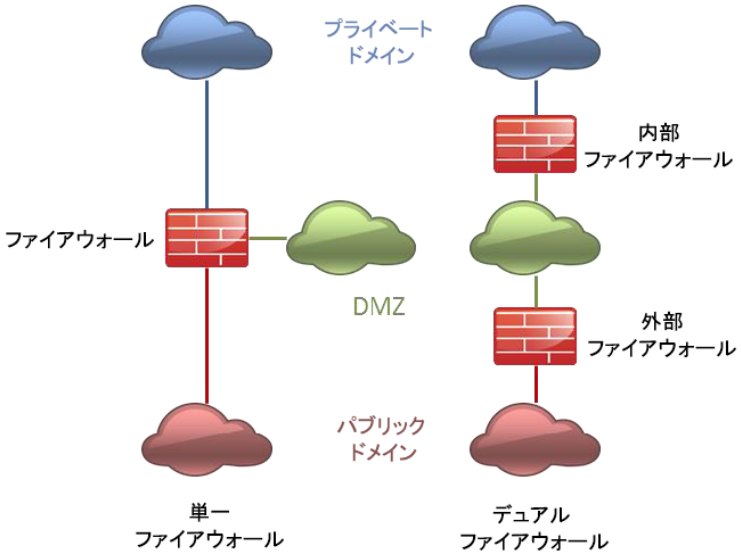
展開オプション

VCS-E の共存導入の場合、BE 6000 サーバには異なる多くのネットワーク設計要件に対応する柔軟性があります。

ファイアウォール トポロジ

ファイアウォールの非武装地帯（DMZ）を実装し、プライベートドメインを保護するためにビジネスで使用される戦略が仮想 Expressway エッジの接続要件を決定します。ファイアウォール設計に対する最も一般的なアプローチの 2 つを図 2 に示します。単一ファイアウォール設計の場合、Expressway Edge では 3 種類のセキュリティドメイン間のトラフィックフローを制御するファイアウォールへの単一のネットワーク接続を使用します。デュアルファイアウォール設計では、外部と内部のファイアウォールそれぞれを通じてパブリックドメインとプライベートドメインにアクセスするには Expressway Edge に別個のネットワーク接続が必要です。仮想化された Expressway Edge のライセンスには、いずれかのアーキテクチャでの導入を可能にする、第 2 のネットワーク インターフェイスを使用する権利が含まれています。

図 2 ファイアウォール設計



レイヤ 2 ネットワーク接続性

図 2 に示したセキュリティドメインを実装すると、企業は物理的にも、論理的にも、ネットワーク セグメントの分離を確保することができます。これは、専用のイーサネット スイッチが各ネットワーク セグメントに使用されている、または共通デバイス内の分離を維持するために仮想 LAN（VLAN）機能が使用されているという場合があります。VLAN を使用すると、サーバへの接続に専用のポートを使用して、あるドメインのトラフィック量が別のドメインのトラフィック量に影響しないようにすることができます。または、VLAN トランクを使用してポートの使用を最適化することができます。
Business Edition サーバは、バンドルされた Virtualization Hypervisor とともに、これらの接続シナリオに対応するネットワーク接続性と構成オプションを提供します。

接続復元力

前述の LAN アーキテクチャでは、セカンダリ ネットワーク接続を使用して復元力を高めることもできます。Business Edition サーバは、パフォーマンスの向上と個々のリンクの損失に対する保護の両方を可能にするインターフェイス チーミングのサポートを提供します。インターフェイス チーミングの詳細については、付録 A を参照してください。

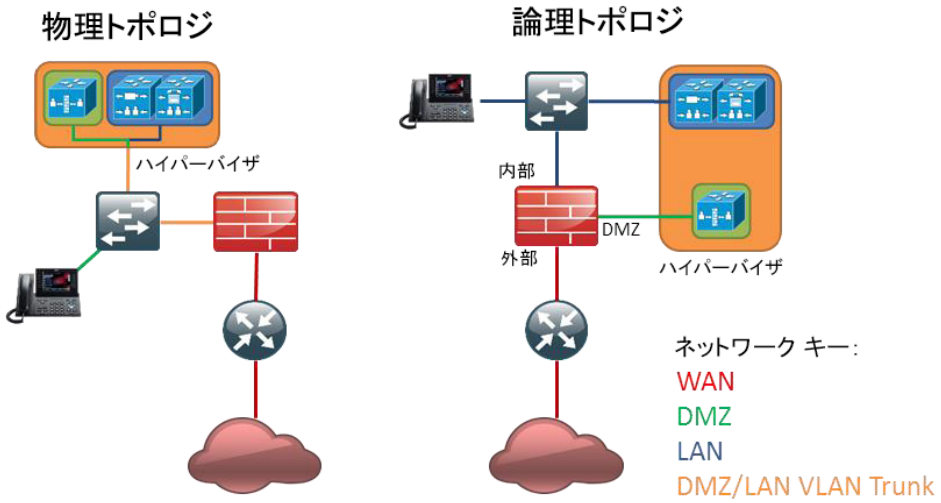
VMware ハイパーバイザ ネットワーキングの概要

Cisco Virtualization Hypervisor（VMware vSphere Hypervisor）には、前のセクションで述べたファイアウォール設計の実装に使用可能な次のネットワーキング概念が含まれています。
vSwitch：ホスト サーバ内の VLAN 対応レイヤ 2 スイッチの仮想実装。vSwitch は、外部ネットワークに接続される場合も、されない場合もあります。
仮想マシン ポート グループ：複数の vSwitch「ポート」、つまりグループに割り当てることができる、ポート設定オプションのテンプレートを定義します。本文書では、各ポート グループが基本的に VLAN とそのポートのメンバーシップを定義します。

仮想マシンのネットワーク アダプタ：仮想マシンのイーサネット インターフェイス。各ネットワーク アダプタは、1 つの仮想マシン ポート グループ（つまり、1 つの VLAN）に関連付けることができます。シスコの各アプリケーションには、1 つ以上のネットワーク アダプタが含まれています。
物理アダプタ：外部ネットワークに接続するための vSwitch に関連付けることができる物理ホストのネットワーク インターフェイス。複数の VLAN が関連付けられている vSwitch に作成されている場合、物理アダプタが 802.1q VLAN トランク（VLAN スイッチ タギング モード）として自動的に設定されます。
NIC チーミング：接続帯域幅やリンク損失に対する保護を増強するため、複数の物理アダプタを vSwitch と関連付けることができます。スループットの向上のためのチーミング インターフェイスの場合、すべての接続が同じスイッチに存在する必要があります。インターフェイス チーミングの詳細については、付録 A を参照してください。

仮想ネットワークを使用した設定手順

次の手順で、図 3 に示した VLAN トランキングによる単一ファイアウォール ソリューションのニーズを満たすための Virtualization Hypervisor およびスイッチド ネットワークの設定方法について詳しく説明します。サーバに複数の物理接続を追加する手順については、付録 A を参照してください。
図 3：ソリューション例



1. DMZ のコンテキストまたはサブネットワークを含めるようにファイアウォールを設定します。内部ネットワークと外部ネットワークの両方との Expressway Edge 通信を許可するトラフィック ポリシー ルールが作成されていることを確認します。内部/DMZ 境界および外部/DMZ 境界をまたぐ Expressway エッジ IP ポートの使用方法の詳細については、次のガイドを参照してください。
   http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X8-1.pdf
2. DMZ トラフィック用の VLAN を含めるようにレイヤ 2 スイッチ ネットワークを設定し、ファイアウォール DMZ ポートに適切にマッピングされていることを確認します。

3. Business Edition サーバに割り当てられたスイッチ ポートを VLAN トランクとして設定し、内部および DMZ ネットワークのみを許可し、Business Edition サーバのネットワーク インタフェース” to “インターフェース 1 に接続するようにします。Cisco Catalyst スイッチを使用してこれをどのように設定するかを次の例で示します。

```
vlan 1
 name default
!vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE Server Network Interface 1 (Internal/DMZ trunk)
 switchport trunk allowed vlan 1,30
 switchport mode trunk
 spanning-tree portfast trunk
!
```

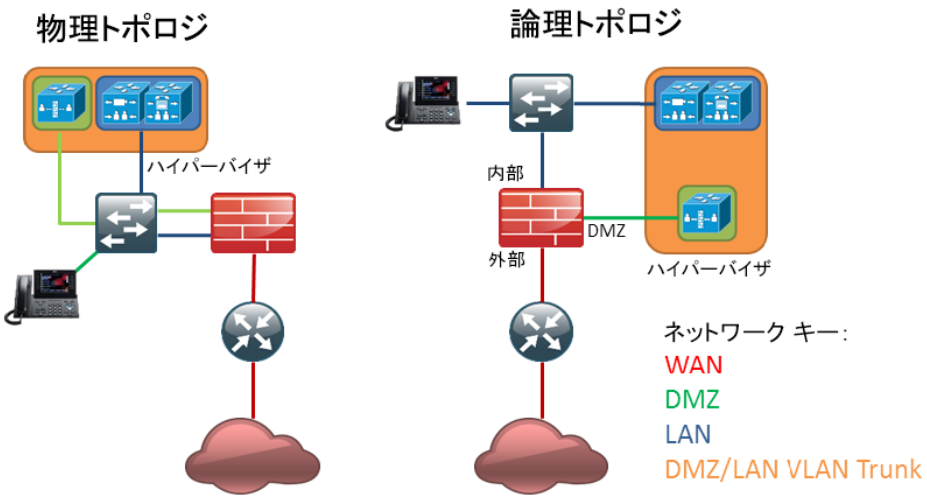
注:この例では、内部ネットワークにネイティブ(タグ付けされていない)VLAN を使用して、デフォルトのハイパーバイザ設定に対応することを想定しています。DMZ で VLAN 30 を使用していますが、これはあくまで例を示すためです。このため、任意の VLAN ID が使用される場合があります。

4. ハイパーバイザ ネットワーク機能を設定するには、vSphere クライアントを次のように使用します。
    a. 左側にある [Inventory] パネルのホスト アイコンをクリックしてネットワーク設定画面にアクセスし、[**Configuration**] タブから [**Networking**] オプションを選択します。デフォルトの仮想マシン ポート グループを使用するためにコア アプリケーションが設定されていることに注意してください。vSwitch0 の [**Properties**] をクリックし、スイッチの設定画面にアクセスします。
    b. [**Add…**] をクリックしてネットワーク追加ウィザードを開始します。
    c. デフォルトの設定をそのまま使用して仮想マシンのネットワークを追加し、[**Next**] をクリックします。
    d. **ネットワーク ラベル**と **VLAN ID** を追加してネットワーク設計に対応し、[**Next**] をクリックします。**注**:ドロップダウン ボックスを使用せずに、VLAN ID を直接入力する必要があります。
    e. 新しい仮想マシン ポート グループの設定を確認し、[**Finish**] をクリックします。
    f. Expressway エッジ アプリケーションに OVA を導入し、新しい DMZ ポート グループがプライマリ仮想マシンのネットワーク アダプタに選択されていることを確認します。
    g. Expressway エッジ アプリケーションを導入した後、新しいポート グループで DMZ VLAN が使用されます。

専用ネットワーク接続を使用した設定手順

次の手順では、仮想化ハイパーバイザと、図 4 に示すように、各セキュリティドメインに対して専用ネットワーク接続を使用した単一ファイアウォール ソリューションのニーズを満たすためのスイッチド ネットワークの設定方法を詳しく説明します。

図 4 : ソリューション例



1. DMZ のコンテキストまたはサブネットワークを含めるようにファイアウォールを設定します。内部ネットワークと外部ネットワークの両方との Expressway Edge 通信を許可するトラフィック ポリシー ルールが作成されていることを確認します。内部/DMZ 境界および外部/DMZ 境界間での Expressway エッジ IP ポートの使用方法の詳細については、次のガイドを参照してください。
   http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X8-1.pdf
2. DMZ トラフィック用の VLAN を含めるようにレイヤ 2 スイッチ ネットワークを設定し、ファイアウォール DMZ ポートに適切にマッピングされていることを確認します。または、異なる物理スイッチがこの分離を行うために使用される場合があります。
3. 内部ネットワークと DMZ ネットワークへのアクセスに Business Edition サーバに割り当てられたスイッチを設定して、別の Business Edition サーバ ネットワーク インターフェイスに接続します。次の例に、VLAN を使用してトラフィックを分離する場合に Cisco Catalyst スイッチを使用してどのように設定できるかを示します（各セキュリティドメインに異なるスイッチを使用する場合は、デフォルトのポート設定で通常は十分です）。

```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE Server Network Interface 1 (Internal Network)
 spanning-tree portfast
!
interface GigabitEthernet1/2
 description BE Server Network Interface 2 (DMZ Network)
 switchport access vlan 30
 spanning-tree portfast
!
```

注:この例では、内部ネットワークにネイティブ(タグ付けされていない)VLAN を使用して、デフォルトのハイパーバイザ設定に対応することを想定しています。DMZ で VLAN 30 を使用していますが、これはあくまで例を示すためです。このため、任意の VLAN ID が使用される場合があります。

4. ハイパーバイザ ネットワーク機能を設定するには、vSphere クライアントを次のように使用します。
    a. 左側のパネルのホスト アイコンをクリックしてネットワーク設定画面にアクセスし、[**Configuration**] タブから [**Networking**] オプションを選択します。デフォルトの仮想マシン ポート グループを使用するためにコア コラボレーション アプリケーションが設定されていることに注意してください。[**Add Networking…**] をクリックしてネットワークの追加ウィザードを開始します。
    b. デフォルトの設定をそのまま使用して仮想マシンのネットワークを追加し、[**Next**] をクリックします。
    c. 新しい vSphere 標準スイッチを未使用の物理ネットワーク インターフェイス(この場合は vmnic1)で作成するオプションを選択し、[**Next**] をクリックします。
    d. 新しいスイッチのラベルを追加しますが、**VLAN ID** はゼロのままにします。[**Next**] をクリックして変更を確認し、次に [**Finish**] をクリックします。
    e. Expressway エッジ アプリケーションに OVA を導入し、新しい DMZ スイッチがプライマリ仮想マシンのネットワーク アダプタに選択されていることを確認します。
    f. Expressway エッジ アプリケーションを導入した後は、新しい vSwitch に接続されます。

デュアル ファイアウォール ソリューションの設定

デュアル ファイアウォール ソリューションを導入する場合、設定は、主として前のセクションで詳しく説明した手順(この場合は最初の DMZ 接続が外部ファイアウォールにあると想定)に従います。新しい仮想マシン ポート グループ(VLAN)または内部ファイアウォールへの接続用 vSwitch を作成する手順を繰り返してから、この新しいネットワークに 2 つめのネットワーク アダプタを割り当てるように Expressway エッジ仮想マシンを編集します。最後に、内部ファイアウォール サブネットワークの外部ネットワークに新しい VLAN または物理スイッチを追加します。

付録 A – NIC チーミング

はじめに

このドキュメントの本文で示すソリューションは、仮想化された Business Edition サーバ内の DMZ および内部ネットワークの適切な分離を維持することに重点を置いています。この分離に加えて、ハイパーバイザ NIC チーミング機能により複数の物理アダプタを vSwitch に関連付けて外部ネットワークにロード シェアリングおよびフェールオーバー接続を提供することができます。

フェールオーバーとロード バランシング

追加の物理アダプタを vSwitch に割り当てるときに、アクティブまたはスタンバイとして割り当てることができます。サーバの物理ネットワークへの接続方法に応じて、仮想マシンからのトラフィックはアクティブ接続全体で負荷分散することができ、リンク障害が発生したときにスタンバイ アダプタがアクティブになって引き継ぎます。

スイッチド ネットワーク トポロジ

障害に対する復元力を最大化するため、通常、チーム化されたインターフェイスが別のスイッチング機器に接続されます。これには、シャーシへの別のラインカードの接続、スタックへのスイッチの接続、または、完全に独立したデバイスへの接続が含まれることがあります。独立した物理スイッチを使用する場合、チーム化されたインターフェイスをアクティブに設定して、ループを発生させる接続を Ethernet スパニング ツリー プロトコルでブロックします。リンクやスイッチに障害が発生した場合は、スパニング ツリー プロトコルがサーバへの保守可能な接続を使用するように再収束します。VLAN トランキングを使用する場合は、通常、スパニング ツリー プロトコルを VLAN ごとに設定して、通常動作下の DMZ や内部ネットワークトラフィックに異なる接続を使用します。
IEEE 802.3ad リンク集約をサポートする共通論理スイッチ（つまりシャーシまたはクラスタ）に対して接続した場合は、通常動作下のリンク グループのすべてのアクティブ メンバ間のトラフィックを負荷分散できます。リンク集約は、スパニング ツリーよりも迅速にリンク障害に対応でき、VLAN には透過的であるため、専用ネットワークまたは VLAN トランク接続に使用される場合があります。
次の表に、Business Edition サーバがネットワーク分離と NIC チーミングにどのように対応できるかを示します。中密度サーバには、VLAN トランキングを使用するようにリンクを設定した NIC チーミングを使用するのに十分なインターフェイスのみがあることに特に注意してください。

サーバ リンクのタイプ	BE6000 MD NIC x 2	BE6000 HD NIC x 6	BE7000 NIC x 12
VLAN Trunk	✓	✓	✓
専用リンク	✗	✓	✓

設定

次の手順で、NIC チーミングを含めるには、このドキュメントからどのように構成を拡張するかについて説明します。

スイッチの設定

サーバ インターフェイスを集約する場合は、802.3ad リンク集約を使用するように接続するスイッチ ポートを設定する必要があります。次の例に、Cisco Catalyst スイッチへの VLAN トランキングを使用してこれをどのように設定するかを示します。

```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE Server Network Interface 1 (Internal/DMZ trunk group)
 switchport trunk allowed vlan 1,30
 switchport mode trunk
 spanning-tree portfast trunk
 channel-group 1 mode passive
!
interface GigabitEthernet1/5
 description BE Server Network Interface 2 (Internal/DMZ trunk group)
 switchport trunk allowed vlan 1,30
 switchport mode trunk
 spanning-tree portfast trunk
 channel-group 1 mode passive
!
```

サーバ インターフェイスを別のスイッチに接続する場合のスイッチ ポートの設定は、このドキュメントの前出の単一リンクの例と同じです。ただし、スパニング ツリー Portfast は使用しないでください。

```
vlan 1
 name default
!
vlan 30
 name DMZ
!
interface GigabitEthernet1/1
 description BE Server Network Interface 1 (Internal/DMZ trunk)
 switchport trunk allowed vlan 1,30
 switchport mode trunk
!
```

スパニング ツリー VLAN の cost コマンドは、必要に応じて、リンク間でのトラフィックの分散に使用できます。詳細については、参考資料を参照してください。

ハイパーバイザの設定

ハイパーバイザ ネットワーク機能を設定するには、vSphere クライアントを次のように使用します。

1. 左側にある [Inventory] パネルのホスト アイコンをクリックしてネットワーク設定画面にアクセスし、[**Configuration**] タブから [**Networking**] オプションを選択します。vSwitch0 の [**Properties**] をクリックし、スイッチの設定画面にアクセスします。
2. スイッチに追加する必要がある**物理アダプタ**を選択します。マザーボードと PCI カードのネットワーク アダプタの混在を組み合せることをお勧めします。[Next] をクリックします。
3. 追加されたポートのフェールオーバー ポリシーを調整します。vShpere がリンクのフェールオーバーを管理する必要がある場合は、新しく追加されたアダプタをスタンバイに**降格**します。それ以外の場合はアダプタをアクティブのままにし、[**Next**] をクリックします。追加を確認し、[**Finish**] をクリックします。
4. IEEE 802.3ad リンク集約が必要ない場合、vSwitch のプロパティのページを閉じて、プロセスを修了します。リンク集約のために vSwitch を設定する場合は、[**vSwitch0 Properties**] の [**Ports**] タブを選択し、vSwitch のオブジェクトを**編集**します。

5. [**vSwitch Properties**] ダイアログから、[**NIC Teaming**] タブを選択した後に、ロード バランシング ポリシーに [**Route based on IP hash**] を選択します。[**OK**] をクリックしてダイアログを閉じ、vSwitch0 のプロパティ画面を閉じて設定を完了します。

参照

VMware ESXi5.0 ネットワーキング マニュアル:
http://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.networking.doc/GUID-35B40B0B-0C13-43B2-BC85-18C9C91BE2D4.html

VLAN Load Balancing Between Trunks Using the Spanning-Tree Protocol Port Priority(スパニング ツリー プロトコル ポート優先度を使用したトランク間での VLAN ロード バランシング):
http://www.cisco.com/en/US/tech/tk389/tk621/technologies_tech_note09186a00800ae96a.shtml

VCS Virtual Machine Deployment Guide(VCS 仮想マシン導入ガイド):
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-Virtual-Machine-Install-Guide-X8-1.pdf

VCS ポートの使用
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-IP-Port-Usage-for-Firewall-Traversal-Deployment-Guide-X8-1.pdf

Connecting Cisco UCM and VCS Deployment Guide(Cisco UCM の接続および VCS 導入ガイド):
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-SIP-Trunk-to-Unified-CM-Deployment-Guide-CUCM-8-9-and-X8-1.pdf

VCS Control with Expressway Deployment Guide(Expressway 導入による VCS 制御ガイド):
http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-1.pdf

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。
対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.
本書のその他のいかなる保証にかかわらず、これらのサプライヤのすべてのマニュアルおよびソフトウェアはすべての FAULTS.CISCO を「現状のまま」提供するものであり、上記の各サプライヤは商品性、特定目的への適合性、ならびに、権利侵害がないことまたは取引、使用または取引慣行により発生がないことを含め、それらのみに限定されることなく、明示または黙示を問わず、すべての保証を放棄します。
いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。
このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。
Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標の一覧を確認するには、http://www.cisco.com/go/trademarks を参照してください。Third-party trademarks mentioned are the property of their respective owners. パートナーという言葉は、シスコ社と他社との間のパートナーシップ関係を示唆するために使用されるものではありません。(1110R)
このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。
対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。
FCC クラス A 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。
住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。
FCC クラス B 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。これらの制限は、住宅地で使用したときに、干渉を防止する適切な保護を規定しています。本機器は、無線周波数エネルギーを生成、使用、または放射する可能性があり、指示に従って設置および使用しなかった場合、無線通信障害を引き起こす場合があります。ただし、特定のインストールにおいて干渉が発生しないことを
保証するものではありません。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。干渉しているかどうかは、装置の電源のオン/オフによって判断できます。
- 受信アンテナの向きを変えるか、場所を移動します。
- 機器と受信機との距離を離します。
- 受信機と別の回路にあるコンセントに機器を接続します。
- 販売業者またはラジオやテレビの専門技術者に連絡します。

シスコでは、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります
シスコが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリックドメインとして UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.
ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。
いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。
このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワークトポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、
偶然の一致によるものです。
Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標の一覧を確認するには、http://www.cisco.com/go/trademarks を参照してください。Third-party trademarks mentioned are the property of their respective owners. この文書で使用されている「パートナー」という用語は、シスコ社と他社との間のパートナーシップ関係を意味するものではありません。(1110R)