Cisco TelePresence Management Suite 15.0

ソフトウェア リリース ノート
最終更新日：2016 年 3 月

製品に関する資料

製品のインストール、初期設定、および動作については、次のドキュメントを参照してください。

- *Cisco TelePresence Management Suite インストレーションおよびアップグレード ガイド*
- *Cisco TelePresence Management Suite 管理者ガイド*
- *Cisco TMS 拡張機能導入ガイド*

15.0 の新機能

監査ログ設定を TMS ツールに移動

次の設定を TMS ツールに移行して、アプリケーションのセキュリティを向上させました。

- **[管理ツール（Administrative Tools）] > [設定（Configuration）] > [全般設定（General Settings）] > [監査の有効化（Enable Auditing）]**
- **[管理ツール（Administrative Tools）] > [TMS サーバ メンテナンス（TMS Server Maintenance）] >[監査ログ データ消去設定（Audit Log data purge settings）]**

監査ログ設定は、Cisco TMS アプリケーションから編集できなくなりました。

監査を有効にし、監査ログ データを表示および削除するには、**[TMS ツール（TMS Tools）] > [高度なセキュリティ設定（Advanced Security Settings）] > [監査（Auditing）]** を選択します。

Cisco TMS のパフォーマンスを改善しました。

64 ビット モードで IIS アプリケーション プールを実行することで、Cisco TMS の全体的なパフォーマンスが大幅に向上しました。

レガシーシステムのサポートの削除

Cisco TMSから次のシステムのサポートが削除されました。

- VCON エンドポイント
- BioData Babylon Encryptor
- AdTran Atlas システム

VCON エンドポイント、BioData Babylon Encryptor、AdTran Atlas システムのサポートを削除した後、Cisco TMS 15.0 では、これらのレガシーシステムは以下のように処理されます。

- Cisco TMS 内の VCON エンドポイント、BioData Babylon Encryptor、AdTran Atlas システムはすべて、**[SystemType]** が「*System Not Found*」として表示されます。
- これらのエンドポイントは、「*管理対象外エンドポイント*」として Cisco TMS に追加する必要があります。

レポートの削除

次のレポートが Cisco TMS から削除されました。

- **[レポート（Reporting）] > [システム（System）] > [リモコンの電池残量低下（Low Battery On Remote Control）]**
- **[レポート（Reporting）] > [システム（System）] > [FTP 監査（FTP Audit）]**
- **[レポート（Reporting）] > [投資回収率（Return on Investment）] > [グローバル投資回収率（Return On Investment Global）]**
- **[レポート（Reporting）] > [投資回収率（Return on Investment）] > [ローカル投資回収率（Return On Investment Local）]**
- **[レポート（Reporting）] > [CO2 の削減（CO2 Savings）]**
- **[レポート（Reporting）] > [ネットワーク（Network）] > [パケット損失ログ（Packet Loss Log）]**
- **[レポート（Reporting）] > [ネットワーク（Network）] > [パケット損失会議（Packet Loss Conference）]**
- **[レポート（Reporting）] > [ネットワーク（Network）] > [帯域幅の使用量（Bandwidth Usage）]**

また、次のフィールドが **[管理ツール（Administrative Tools）] > [設定（Configuration）] > [統計設定（Statistics Settings）]** から削除されました。

- **投資回収率統計の平均システムコスト**
- **投資回収率統計の平均旅費**
- **統計ROI/CO2内のエンドポイントごとの平均参加者数**
- **統計ROI/CO2内の最小通話期間**
- **1 人当たりの旅行の CO2 削減量の統計（Kg CO2）**

[ネットワーク（Network）] の **[ネットワーク履歴（Network History）]** メニューが **[履歴（History）]** に変更され、**[レポート（Reporting）] > [システム（System）]** に移動しました。

クライアント証明書の確認の削除

[Cisco TMS ツール（TMS Tools）] > [セキュリティ設定（Security Settings）] > [高度なセキュリティ設定（Advanced Security Settings）] の **[トランスポート層セキュリティのオプション（Transport Layer Security Options）]** から、**[HTTPS API のクライアント証明書を要求（Request Client Certificates for HTTPS API）]** が削除されました。

PDF へレポートをエクスポートする機能の削除

レポート データを PDF ファイルにエクスポートするオプションは Cisco TMS で使用できなくなりました。この機能をサポートしているすべてのレポートについては、**[レポート（Report）]** タブと次のボタンが削除されています。

- **PDF へレポートをエクスポート（Export Report to PDF）**
- **[予約（Booking）] > [会議の一覧（List Conferences）]** からの **[会議のレポート（Conference Report）]**。

レポート データの抽出は、**[Excel にエクスポート（Export to Excel）]** 機能を使用して行うことができます。

また、**[統計レポートを無効にする（Disable Statistics Report）]** フィールドも **[管理ツール（Administrative Tools）] > [設定（Configuration）] > [統計設定（Statistics Settings）]** から削除されました。

統計設定メニューの名前の変更

[統計設定（Statistics Settings）] メニューの名前が **[レポートの設定（Reporting Settings）]** に変更されました 。また, **[管理ツール（Administrative Tools）] > [設定（Configuration）] > [レポートの設定（Reporting Settings）]** にある次のフィールドも更新されています。

- **レポート履歴（日）（Reporting History（in days））**
- **レポートのデフォルト開始時刻（Reporting Default Start Time）**
- **レポートのデフォルト終了時刻（Reporting Default End Time）**

スケジュールされたポイントツーポイント コールの早期参加の有効化

[管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）] の **[会議の接続（Conference Connection）]** で **[参加者に対し 5 分前の接続を許可する（Allow Participants to Join 5 Minutes Early）]** が *[はい（Yes）]* に設定されている場合、ポイントツーポイント会議の参加者は、予定時刻の 5 分前に参加できるようになりました。これにより、会議のすべてのタイプの参加者に [参加（Join）] ボタンが表示されます。

優先通話プロトコルを選択するオプションの追加

[ルーティングの優先プロトコル（Preferred Protocol in Routing）] オプションでは、会議のルーティング時に *H.323* と *SIP* の間でコール プロトコルを選択できます。この機能は、**[管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）]**、**[詳細設定（Advanced）]** セクションの下に追加されます。

システム サポートの追加

Cisco TMS にコラボレーション エンドポイント ソフトウェア（CE）8.0 で実行されるエンドポイントのサポートが追加されました。

エンドポイントの設定の更新

コラボレーション エンドポイント ソフトウェア 8.0 のユーザは、Cisco TMS で Cisco Intelligent Proximity の設定を構成できるようになりました。

[システム（Systems）] > [ナビゲータ（Navigator）] >コラボレーション エンドポイント ソフトウェア 8.0 で実行するエンドポイントを選択 **> [設定（Settings）] > [シスコ プロキシミティ設定（Cisco Proximity Settings）]** に新しい設定が追加されました。

新しい構成テンプレートの追加

コラボレーション エンドポイント ソフトウェア 8.0 の構成テンプレートが Cisco TMS に追加されました。

CE を追加するための設定可能なユーザ ログイン情報

Cisco TMS で通信用に CE ソフトウェア エンドポイントを作成して管理するために、ユーザ名（「admin」以外のユーザ）を変更するオプションが追加されました。Cisco TMS で現在使用されているログイン情報について、CE エンドポイントのパスワードを編集できます。これによりエンドポイントのパスワードが変更され、Cisco TMS で新しいパスワードが使用されます。Cisco TMS でパスワードを編集するには、使用する CE エンドポイントを選択して **[全般（General）]** の **[設定（Settings）] > [設定の編集（Edit Settings）]** に移動し、**[パスワード（Password）]** テキストボックスに入力します。

セキュリティ機能の拡張

このリリースには、Cisco TMS のセキュリティ拡張機能が含まれています。

通信セキュリティの向上

セキュア通信を強化するために、2 つのセキュリティ設定が 1 つの新しい設定 **[通信セキュリティ（Communication Security）]** に統合されました。**[管理ツール（Administrative Tools）] > [設定（Configuration）] > [ネットワーク設定（Network Settings）]** の **[セキュアなデバイスのみの通信（Secure-Only Device Communication）]** セクションにあった **[セキュアなデバイスのみの通信（Secure-Only Device Communication）]** と **[証明書の検証（Validate Certificates）]** オプションは削除されました。これで、以下のように、Cisco TMS のすべての接続に対して、通信セキュリティのレベルを *[中（Medium）]*、*[中 - 高（Medium-High）]*、および *[高（High）]* の間で設定できるようになりました。

- *中（Medium）*：Cisco TMS は通信に HTTPS を優先しますが、HTTP にフォールバックします。前回の通信でシステムに対して使用したプロトコルを記憶して、同じプロトコルを使用し続けます。Telnet や SNMPv2 のような安全でないプロトコルも使用されます。
- *中 - 高（Medium-High）*：Cisco TMS は接続に SSL のみを使用して通信します。SSL には HTTPS と SSH が含まれます。
- *高（High）*：Cisco TMS は、接続の通信に SSL のみを使用し、有効な署名付き証明書があるかどうかを通信時に確認します。

新規インストールとアップグレードの場合、デフォルト値は *[中（Medium）]* に設定されます。ただし、通信のセキュリティ向上のために設定を変更することもできます。*[中 - 高（Medium-High）]* または *[高（High）]* を選択すると 、CTS、TCS、および Polycom HDX w などのシステムでは、Cisco TMS の一部またはすべての機能が失われます。

この新しい設定は 、**[Cisco TMS ツール（TMS Tools）] > [セキュリティ設定（Security Settings）] > [高度なセキュリティ設定（Advanced Security Settings）]** の **[トランスポート層セキュリティのオプション（Transport Layer Security Options）]** の下で確認できます。

強化されたバナー機能

Cisco TMS では、Web UI とレポートの他に、電子メール テンプレートにカスタム バナーが追加されました。Cisco TMS ツール アプリケーションから、バナーの色とテキストも選択できます。バナーを適用するには、**[Cisco TMS ツール（TMS Tools）] > [セキュリティ設定（Security Settings）] > [高度なセキュリティ設定（Advanced Security Settings）]** の **[バナー（Banners）]** に移動します。

Cisco TelePresence Management Suite Extension Booking API（Cisco TMSBA）

WebEx 例外のサポート

Cisco TMSBA クライアントが API バージョン 16 以上を公開していれば、**OwnedExternally** フラグで予約した場合には、Webex の例外が Cisco TMSBA でサポートされます。この Cisco TMSBA 機能は、今後の Webex リリースでの例外サポートに備えたものです。一連の定期的な会議の例外に関する Webex サポートの最新情報については、お使いの Cisco TMS および Webex Meeting Center のバージョンの 『Cisco CMR Hybrid リリース ノート』を参照してください。

次の *WebExInstanceType* 要素は、クライアントが WebEx 会議を例外的にスケジュールするために使用できます。

- *標準（Normal）*：インスタンスの Webex データは、一連の会議の Webex データと同じです。
- *変更（Modify）*：インスタンスの Webex データは、一連の会議の Webex データとは異なります。
- *削除（Delete）*：インスタンスの Webex データはありません。

OwnedExternally

Webex オブジェクトの **OwnedExternally** 属性は、Webex 会議が最初に外部クライアントで予約されたかどうかを制御します。この属性は、主に Cisco TMSXE およびほかの Cisco 製品で使用することを目的としていますが、Cisco CMR Hybrid 会議をスケジュール設定する際にほかの Cisco TMSBA クライアントが使用することもできます。

OwnedExternally を *True* に設定して予約を行う Cisco TMSBA クライアントは、Webex クラウドとの独自の統合を担当します。クライアントは、最初に Webex API を使用して Webex クラウドで会議をスケジュールし、その後 Cisco CMR Hybrid 会議のテレプレゼンス部分をスケジュールする際に、Webex API によって返された Webex の詳細（*SiteUrl*、*HostKey* やその他の属性など）を Cisco TMSBA に提供する必要があります。**OwnedExternally** を *True* に設定すると、Cisco TMS は提供された Webex データの検証を試みません。これはクライアントの責任範囲と見なされるためです。Cisco TMS は会議用に会議ブリッジのみを予約し、スケジュールされた開始時刻に（*SipUrl* 要素でクライアントが指定したダイヤル文字列を使用して）Webex にダイヤル アウトするようブリッジに指示します。

OwnedExternally を *True* に設定して予約すると、Cisco TMSBA で定例会議の 1 つのインスタンスに対して Webex を追加または削除することができます。また、後で Cisco CMR Hybrid に対応した定例会議のインスタンスを移動することも可能です。一連の会議で Webex が **OwnedExternally** である場合、Cisco TMSBA では、別の Webex サイトを使用するように一部のインスタンスを変更するなど、一連の会議の個々のインスタンスごとに異なる Webex データを提供することもできます。

解決済みおよび未解決の問題

このリリースの未解決の問題に関する最新情報については、以下のリンクを参照してください。

https://tools.cisco.com/bugsearch/search?kw=*&pf=prdNm&pfVal=283688292&rls=15.0&sb=anfr&srtBy=byRel&bt=custV

Cisco バグ検索ツールにログインした後、ブラウザの表示を更新する必要があります。

制限事項

機能	制限事項
サポートされるタイムゾーン	■ Cisco TMS サーバのタイムゾーンを変更することはできません。 ■ DST の日付やタイム ゾーンのリージョンの変更など、国際タイムゾーンの修正は、Microsoft Windows の更新プログラムによって Cisco TMS サーバと Cisco TMS で自動的に更新されます。Cisco TelePresence TE または TC ソフトウェアを実行しているエンドポイントについても同じです。これらのエンドポイントには、手動で定義されたタイム ゾーンのリストがあるため、DST 日付またはタイムゾーン リージョンの変更は反映されません。これにより、直接管理されているエンドポイントでタイムゾーンの不一致エラーが発生する可能性があります。スケジューリングは影響を受けませんが、Cisco TMS はタイムゾーン データの読み取り/書き込みに失敗する可能性があります。
TelePresence Conductor のスケジューリング	TelePresence Conductor は、会議と会議の間でリソースを解放するまでに最大 30 秒待機する場合があります。そのため、参加者が会議への参加と退席を繰り返すと、連続する会議の着信や発信が拒否されたり、使用率が急上昇したりする可能性があります。バグツールキットの識別子: CSCuf34880。 この制限は、予定されている TelePresence Conductor および Cisco TMS のリリースで対処されます。 「スケジュール設定 の改善 [p.1]」も参照してください。
TelePresence Conductor のスケジューリング	Cisco TMS では、複数の TelePresence Conductor クラスタ ノードはサポートされていません。
TelePresence Conductor のスケジューリング	Cisco TMSPE によって生成されたコラボレーション会議室のスケジュールはサポートされていません。
TSP の音声と会議の拡張	WebEx によって 2 つの会議が同じ TSP 音声番号に割り当てられている場合は、Cisco TMS はそのことを認識せずに会議を拡張するかどうかを決定します。それにより、 2 つの会議で音声参加者が同じになる可能性があります。
モニタリングとレポート	■ FindMe と Multiway を使用した会議では、会議制御センターとレポートで重複が発生する可能性があります。 ■ 参加者が保留になっているか、または転送された会議は、会議制御センターとレポートで重複が発生する可能性があります。 ■ 会議制御センターとグラフィカル モニタは、Google Chrome バージョン 42 以上では、Netscape プラグイン アプリケーション プログラミング インターフェイス（NPAPI）をサポートしていないため、動作しません。今後のリリースで Netscape プラグイン アプリケーション プログラミング インターフェイス（NPAPI）のサポートが完全に削除されるまでは、次の手順を実行して Google Chrome での会議制御センターとグラフィカル モニタの起動を試みることができます。 a. システムで、管理者としてコマンドプロンプトを開きます。 b. **reg add HKLM\software\policies\google\chrome\EnabledPlugins /v 1 /t REG_ SZ /d java** コマンドを実行します。 c. Google Chrome を再起動します。 ■ 会議制御センターの参加者のスナップショットとイベント ログ データの自動更新機能は、どのバージョンの Google Chrome でも機能しません。

機能	制限事項
WebEx	■ CMR Hybrid に対する高度な定期的なパターンはサポートされません。[新しい会議（New Conference）] ページから予約する場合は、Webex を含めてから、サポートされている定期的なパターンのみが表示されるように定期的なパターンを指定してください。 ■ 1 つのインスタンスが進行中に定例会議シリーズを削除すると、Cisco TMS では会議が削除されますが、WebEx では削除されません。これは、WebEx が進行中の会議に変更を許可しないためです。これには削除が含まれます。 ■ Cisco TMS ツールで **[通信セキュリティ（Communication Security）]** のオプション *[中 - 高（Medium-High）]* または *[高（High）]* を選択すると、Cisco TMS の一部またはすべての機能が失われます。
コラボレーション エッジ	Cisco TMS は現在コラボレーション エッジの背後にあるデバイスをサポートしていません。
Expressway	Cisco Expressway-C と Cisco Expressway-E は、システム タイプ TANDBERG VCS を使用して Cisco TMS に表示されます。
[システムタイプ（System Type）] フィールド	以前に TANDBERG がシステム タイプに含まれていた一部のシステムが、Cisco TMS に引き続き TANDBERG として表示されることがあります。これはシステムの API からシステム タイプを直接読み取る Cisco TMS に主に基づいています。API を介して使用できなかったシステム タイプが追加されることがあります。そのため、その名前とシステム タイプ TANDBERG が表示され続けることがあります。
下部バナー	Cisco TMS ツールで下部バナーが有効になっている場合、Internet Explorer 10 で Cisco TMS Web アプリケーションを使用して、強化されたセキュリティ設定を有効にすると、ウィンドウの下部にあるリンクとボタンが無効になります。
Cisco TMSPE が Cisco TMS と通信できない	Cisco TMS 15.0 で新しいセキュリティ モードが *[高（High）]* に設定されている場合、Cisco TMSPE は Cisco TMS との通信に失敗します。 この制限は、Cisco TMSPE の将来のリリースで対処されます。
Cisco TMS での会議のスケジューリング	24 時間以上スケジュールされた会議と重複している定例会議は予約できないことがあります。 Bug Toolkit の ID：CSCux64873。
延長時のリソース可用性チェック（Resource Availability Check on Extension）	**[延長会議モード（Extend Conference Mode）]** を **[自動ベスト エフォート（Automatic Best Effort）]** に設定した状態で **[延長時のリソース可用性チェック（Resource Availability Check on Extension）]** を **[無視（Ignore）]** に設定し、**[参加者に対し早期接続を許可する（Allow participants to Join Early）]** を **[はい（Yes）]** に設定した場合、会議の参加者のうち 1 人がポイント ツー ポイント ミーティングに参加していると、予期せぬ結果が発生する可能性があります。

相互運用性

この製品の相互運用性テスト結果は、http://www.cisco.com/go/tp-interop に掲載されています。ここでは、他の Cisco TelePresence 製品の相互運用性テストの結果も確認できます。

15.0 へのアップグレード

アップグレードする前に

冗長展開

冗長 Cisco TMS の導入をご利用のお客様は、Cisco TMS15.0 にアップグレードする前に『Cisco TelePresence Management Suite インストレーションおよびアップグレード ガイド 15.0』のアップグレード手順を必ずお読みください。

14.4 または 14.4.1 からのアップグレード

Cisco TMSXE または Cisco TMSXN を使用する 14.4 または 14.4.1 からアップグレードする場合は、CISCO TMS15.0 にアップグレードする際に、『Cisco TelePresence Management Suite インストレーションおよびアップグレード ガイド 15.0』[英語] で説明されているアップグレード手順に従う必要があります。

14.2 より前のバージョンからのアップグレード

バージョン 14.2 以前のバージョンの Cisco TMS からアップグレードする場合は、Cisco TMS15.0 にアップグレードする前に、『CiscoTelePresence Management Suite のインストールおよびアップグレードガイド 15.0』[英語] のアップグレード手順を参照する必要があります。

前提条件とソフトウェアの依存関係

互換性のあるオペレーティング システムとデータベース サーバの完全なリストについては、『*Cisco TelePresence Management Suite インストレーションおよびアップグレード ガイド*』を参照してください。

アップグレード手順

Cisco TMS は、Cisco TMS の新規インストールと以前の Cisco TMS バージョンのアップグレードの両方に同じインストール プログラムを使用します。

アップグレードまたはインストールの完全な手順については、『*Cisco TelePresence Management Suite インストレーションおよびアップグレード ガイド*』を参照してください。

Bug Search Tool の使用

バグ検索ツールには、問題の説明と利用可能な解決策など、このリリースおよび以前のリリースの未解決の問題と解決済みの問題に関する情報があります。これらのリリース ノートに示されている ID によって、それぞれの問題の説明に直接移動できます。

このマニュアルに記載された問題に関する情報を検索するには、次の手順を実行します。

1. Web ブラウザを使用して、バグ検索ツールに移動します。
2. cisco.com のユーザ名とパスワードでログインします。
3. **[検索（Search）]** フィールドにバグ ID を入力し、**[検索（Search）]** をクリックします。

ID がわからない場合に情報を検索するには、次の手順を実行します。

1. **[検索（Search）]** フィールドに製品名を入力し、**[検索（Search）]** をクリックします。
2. 表示されるバグのリストから、**[フィルタ（Filter）]** ドロップダウンリストを使用して、*[キーワード（Keyword）]*、*[変更日（Modified Date）]*、*[重大度（Severity）]*、*[ステータス（Status）]*、または *[テクノロジー（Technology）]* のいずれかのキーワードでフィルタリングします。

バグ検索ツールのホーム ページの **[詳細検索（Advanced Search）]** を使用して、特定のソフトウェア バージョンで検索します。

Bug Search Tool のヘルプ ページには、Bug Search Tool の使用に関する詳細情報があります。

マニュアルの入手方法およびテクニカル サポート

資料の入手方法、Cisco Bug Search Tool（BST）の使用方法、サービス リクエストの送信および追加情報の収集方法については、『What's New in Cisco Product Documentation（Cisco 製品資料の更新情報）』（http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html [英語]）を参照してください。

Cisco 製品資料の更新情報には、シスコの新規および改訂版の技術マニュアルがすべて表示されます。この RSS フィードを登録するか、リーダー アプリケーションを使用してコンテンツを直接デスクトップに配信することもできます。RSS フィードは無料のサービスです。

ドキュメント変更履歴

表 1 Cisco TMS のリリース ノートの変更点

日付（Date）	リビジョン	説明
2016 年 8 月	03	Cisco TMS の制限でミーティングのスケジュール設定が追加されました。
2016 年 3 月	02	「PDF へレポートをエクスポートする機能の削除」の項の更新
2015 年 7 月	01	Cisco TMS 15.0 のリリース。

シスコの法的情報

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となります。

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。

Cisco 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 バージョンとして、UCB が開発したプログラムを採用したものです。全著作権所有。著作権©1981、カリフォルニア大学理事会。

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。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙の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。マニュアルの中の例、コマンド出力、ネットワーク トポロジー図、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。

印刷版と複製ソフトは公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices/ [英語]）をご覧ください。

シスコの商標

Cisco および Cisco のロゴは、米国およびその他の国における Cisco およびその関連会社の商標を示します。Cisco の商標の一覧については、www.cisco.com/go/trademarks.をご覧ください。本書に記載されているサードパーティの商標は、それぞれの所有者の財産です。 「パートナー」という用語の使用は Cisco 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）。