



## **Cisco Unified Contact Center ソリューションリリース 11.5(1) ポート活用ガイド**

初版：2016年08月10日

最終更新：2017年03月17日

### **シスコシステムズ合同会社**

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

**【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、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、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。

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.

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 および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。 To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned 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. (1110R)

© 2003-2016 Cisco Systems, Inc. All rights reserved.



## 目次

### はじめに v

変更履歴 v

このマニュアルについて vi

対象読者 vi

マニュアルの入手方法およびテクニカル サポート vi

フィールドアラートおよびフィールド通知 vi

マニュアルに関するフィードバック vi

表記法 vii

### システム サービスのポート使用状況 1

ポート使用状況表の列 1

システム サービス ポートの使用状況 2

### Contact Center Enterprise のポート使用状況 7

ポート使用状況表の列 7

Contact Center Enterprise ポートの使用状況 8

Unified CCMP のポート使用状況 25

Unified CRM Connector のポート使用状況 28

Cisco Agent Desktop (CAD) のポート使用状況 29

Genesys コールセンターへの Cisco Voice の統合 34

### Unified CVP のポート使用状況 37

ポート使用状況表の列 37

Unified CVP のポート使用状況 38

### Cisco VVB のポート使用状況 47

ポート使用状況表の列 47

Cisco VVB ポートの使用状況 48

### Finesse のポート使用状況 51

ポート使用状況表の列 51

Finesse のポート使用状況	52
<b>MediaSense のポート使用状況</b>	<b>57</b>
ポート使用状況表の列	57
MediaSense のポート使用状況	58
<b>SocialMiner のポート使用状況</b>	<b>61</b>
ポート使用状況表の列	61
SocialMiner のポート使用状況	62
<b>Unified Intelligence Center のポート使用状況</b>	<b>67</b>
ポート使用状況表の列	67
Unified Intelligence Center のポート使用状況	68



## はじめに

- [変更履歴](#), [v ページ](#)
- [このマニュアルについて](#), [vi ページ](#)
- [対象読者](#), [vi ページ](#)
- [マニュアルの入手方法およびテクニカル サポート](#), [vi ページ](#)
- [フィールドアラートおよびフィールド通知](#), [vi ページ](#)
- [マニュアルに関するフィードバック](#), [vi ページ](#)
- [表記法](#), [vii ページ](#)

## 変更履歴

次の表に、このガイドで行われた変更のリストを示します。最新の変更が上部に表示されます。

変更内容	参照先	日付
Contact Center Enterprise のソリューションをサポートする各種のシステム サービスのポートを別の章に移動。	「システム サービスのポート使用状況」	2017 年 3 月
新しいポート TCP 1051 および UDP 1051 を追加	「Unified CVP のポート使用状況」	2017 年 2 月
リリース 11.5(1) 向けのマニュアルの初期リリース		2016 年 8 月
PG3 のポートを追加	「Contact Center Enterprise ポートの使用状況」	
多くのポートでトラフィックの方向を追加	「Contact Center Enterprise ポートの使用状況」	

## このマニュアルについて

このドキュメントでは、Cisco Unified Contact Center 製品が使用する TCP および UDP ポートの一覧を示します。Quality of Service (QoS) およびファイアウォール/VPN ソリューションを設定するには、この情報を使用します。AVVID（音声、映像、および統合データのアーキテクチャ）を搭載したネットワークにおいて、適切な設定は重要です。

## 対象読者

このガイドの主な対象読者は、ネットワーク管理者です。

## マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool (BST) の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、<https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html> から入手できます。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、RSS フィードとして購読できます。また、リーダーアプリケーションを使用して、コンテンツを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。

## フィールドアラートおよびフィールド通知

シスコは、自社製品を変更したり、重要なキープロセスを決定したりすることがあります。これらの変更は、シスコのフィールドアラートおよび Cisco Field Notice を使用して通知されます。フィールドアラートおよびフィールド通知は、Cisco.com の Product Alert Tool で登録すると受信できます。このツールを使用して関心のある製品を選択し、通知を受信するプロファイルを作成することができます。

[www.cisco.com](http://www.cisco.com) にサインインして、<https://www.cisco.com/cisco/support/notifications.html> のツールにアクセスします。

## マニュアルに関するフィードバック

このマニュアルに関するご意見をお寄せいただくには、以下のアドレスに電子メールを送信してください。[contactcenterproducts\\_docfeedback@cisco.com](mailto:contactcenterproducts_docfeedback@cisco.com)

お客様からのご意見をお待ちしております。

# 表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
<b>[boldface]</b> フォント	<p>アイコン、ボタン名、ダイアログボックス名など、画面に表示される項目は、[ ] で囲んで表示しています。次に例を示します。</p> <ul style="list-style-type: none"> <li>• [編集 (Edit) ] &gt; [検索 (Find) ] を選択します。</li> <li>• [終了 (Finish) ] をクリックします。</li> </ul>
<i>italic</i> フォント	<p>イタリック体は、以下の場合に使用しています。</p> <ul style="list-style-type: none"> <li>• 新しい用語の紹介。例：スキルグループとは、類似したスキルを持つエージェントの集合です。</li> <li>• ユーザが置き換える必要がある構文値。例：IF (<i>condition, true-value, false-value</i>)</li> <li>• ドキュメントのタイトル。例：<i>Cisco Unified Contact Center Enterprise Installation and Upgrade Guide</i>を参照してください。</li> </ul>
window フォント	<p>Courier などのウィンドウ フォントは、次の場合に使用されます。</p> <ul style="list-style-type: none"> <li>• コード中のテキストや、ウィンドウに表示されるテキスト。例： &lt;html&gt;&lt;title&gt;Cisco Systems, Inc. &lt;/title&gt;&lt;/html&gt;</li> </ul>
< >	<p>山カッコは、以下の場合に使用しています。</p> <ul style="list-style-type: none"> <li>• コンテキストでイタリックが許可されない引数 (ASCII出力など)。</li> <li>• ユーザが入力する文字列で、ウィンドウには表示されないもの (パスワードなど)。</li> </ul>







# 第 1 章

## システム サービスのポート使用状況

- [ポート使用状況表の列, 1 ページ](#)
- [システム サービス ポートの使用状況, 2 ページ](#)

### ポート使用状況表の列

このドキュメントに含まれるポート使用状況表の列について、次に説明します。

#### リスナー（プロセスまたはアプリケーション プロトコル）

サーバまたはアプリケーションを表す値と、（必要に応じて）オープンまたは独自のアプリケーション プロトコル。

#### リスナー プロトコルおよびポート

サーバまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

#### リモート デバイス（プロセスまたはアプリケーション プロトコル）

プロトコルで指定されるサーバまたはサービスに接続するリモート アプリケーションまたはデバイス、またはリモート プロトコルおよびポートでリッスンするリモート アプリケーションまたはデバイス。

#### リモート プロトコルおよびポート

リモート サービスまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

#### トラフィックの方向

ポートを通過するトラフィックの流れる方向（着信、双方向、発信）。



(注) オペレーティング システムは、ローカルアプリケーションまたはサービスがリモートデバイスの宛先ポートへの接続に使用する送信元ポートを動的に割り当てます。ほとんどの場合、このポートは、TCP/UDP 1024 より大きい番号でランダムに割り当てられます。

## システム サービス ポートの使用状況

表 1: システム サービス ポートの使用状況

リスナー (プロセスまたはアプリケーションプロトコル)	リスナー プロトコルおよびポート	リモートデバイス (プロセスまたはアプリケーションプロトコル)	リモートプロトコルおよびポート	トラフィックの方向	目的
システムサービス	TCP 7	エディタ (Editor)	—	双方向	- エディタのエコー - ICM コントローラ
システムサービス	TCP 22	—	—	双方向	SFTP および SSH アクセス
Tomcat (HTTP)	TCP 80	—	—	双方向	- Web アクセス - 通話録音サーバ - Unified CCMP Web サーバおよび AXL のプロビジョニング - CRM Connector サーバ - メディア サーバからのメディアおよび「外部 VXML」ファイルを取得する音声ブラウザのデフォルトポート
システムサービス	UDP 123	—	—	双方向	NTP、ネットワーク時間の同期
SNMP エージェント	UDP 161	—	—	着信	SNMP ベースの管理アプリケーションにサービスを提供

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	目的
Tomcat	TCP 443	クライアントブラウザ	—	双方向	CCE Web 管理およびインターネットスクリプトエディタのための Web アクセス  - Unified CCMP クライアント - メディア サーバからのメディアおよび「外部 VXML」ファイルを取得する音声ブラウザのデフォルトポート
AON Management Console (AMC) サービス	TCP 1090	クラスタ内通信	—	双方向	RTMT データ収集、ロギング、およびアラート機能（AMC RMI オブジェクトポート）を提供
AON Management Console (AMC) サービス	TCP 1099	クラスタ内通信	—	双方向	RTMT データ収集、ロギング、およびアラート機能（AMC RMI レジストリポート）を提供
DBMON	TCP 1500	—	—	双方向	これは、IDS エンジンが DB クライアントをリッスンするポートです。
DBMON	TCP 1501	—	—	双方向	- これは、アップグレード中に IDS の 2 次インスタンスを始動するための代替ポートです。 - ローカルホストトラフィック専用
DBL RPC	TCP 1515	クラスタ内通信	—	双方向	DBL RPC。インストール時にこれを使用して、ノード間に IDS レプリケーションを設定します。

リスナー（プロセスまたはアプリケーション プロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーション プロトコル）	リモート プロトコルおよびポート	トラフィックの方向	目的
Real-time Information Server (RIS) のデータ収集サービス (RISDC)	TCP 2555	クラスタ内通信	—	双方向	RISDC プラットフォーム サービスで使用されます。Real-time Information Server (RIS) は、デバイス登録ステータス、パフォーマンスカウンタ統計、生成された重大アラームなど、Cisco Unified CM のリアルタイム情報を保持します。Cisco RISDC サービスは、RTMT、SOAP アプリケーション、Cisco Unified CM の管理、AMC などのアプリケーションに、クラスタ内のすべての RIS ノードに格納された情報を取得するためのインターフェイスを提供します。
RISDC	TCP 2556	クラスタ内通信	—	双方向	RIS クライアント接続で、リアルタイム情報を取得できるようにする
ディザスタリカバリ システム (DRS)	TCP 4040	—	—	双方向	リアルタイム サービス
リアルタイム サービス	TCP 5001	—	—	双方向	SOAP モニタ
Perfmon サービス	TCP 5002	—	—	双方向	SOAP モニタ
コントロールセンター サービス	TCP 5003	—	—	双方向	SOAP モニタ
ログ収集サービス	TCP 5004	—	—	双方向	SOAP モニタ

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	目的
システムサービス	TCP 5007	—	—	双方向	SOAP モニタ - SOAP インフラストラクチャ用のトラブルシューティングツール
DBMON (CN)	TCP 8001	クラスタ内通信	—	双方向	DB 変更通知ポート
Tomcat (HTTP)	TCP 8080	クライアントブラウザ	—	双方向	<p>-管理インターフェイスまたはユーザ オプションのインターフェイスへのアクセスを試行するクライアントブラウザ。</p> <p>- RTMT、設定 API、およびモバイルスーパーバイザアプリケーションを使用している Web サービスのクライアント。</p> <p>-通話録音サーバのデータレプリケーション</p> <p>- ライブ データの OAMP</p> <p>-CRM Connector for SAP（レジストリにより調整可能）</p>
HTTP	UDP 8080	ブラウザ	—	双方向	プラットフォーム管理、プラットフォーム サービスアビリティ、およびディザスタリカバリ システムへのアクセスに使用するセキュアでないポート。
Tomcat	TCP 8443	—	—	双方向	SOAP による DB アクセス。Tomcat が AXL への SOAP 要求を転送します。

リスナー（プロセスまたはアプリケーション プロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーション プロトコル）	リモートプロトコルおよびポート	トラフィックの方向	目的
Tomcat (HTTPS)	TCP 8443	クライアント ブラウザ	—	双方向	-管理インターフェイスまたはユーザ オプションのインターフェイスへのアクセスを試行するクライアント ブラウザ  - RTMT、設定 API、およびモバイルスーパーバイザアプリケーションを使用している Web サービスのクライアント
HTTPS	UDP 8443	ブラウザ	—	双方向	-プラットフォーム管理、プラットフォーム サービスアビリティ、およびディザスタリカバリ システムへのアクセスに使用するセキュアポート。
IPSec マネージャ デモン	TCP 8500	—	—	双方向	接続テスト。独自プロトコルを使用します。
IPSec マネージャ デモン	UDP 8500	—	—	双方向	プラットフォーム データ（ホスト）証明書のクラスタレプリケーションなど。独自プロトコルを使用します。
Cisco IdS	TCP 8553	—	—	—	Cisco IdS の HTTPS



## 第 2 章

# Contact Center Enterprise のポート使用状況

- [ポート使用状況表の列, 7 ページ](#)
- [Contact Center Enterprise ポートの使用状況, 8 ページ](#)
- [Unified CCMP のポート使用状況, 25 ページ](#)
- [Unified CRM Connector のポート使用状況, 28 ページ](#)
- [Cisco Agent Desktop \(CAD\) のポート使用状況, 29 ページ](#)
- [Genesys コールセンターへの Cisco Voice の統合, 34 ページ](#)

## ポート使用状況表の列

このドキュメントに含まれるポート使用状況表の列について、次に説明します。

### リスナー（プロセスまたはアプリケーション プロトコル）

サーバまたはアプリケーションを表す値と、（必要に応じて）オープンまたは独自のアプリケーションプロトコル。

### リスナー プロトコルおよびポート

サーバまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### リモート デバイス（プロセスまたはアプリケーション プロトコル）

プロトコルで指定されるサーバまたはサービスに接続するリモートアプリケーションまたはデバイス、またはリモート プロトコルおよびポートでリッスンするリモートアプリケーションまたはデバイス。

### リモート プロトコルおよびポート

リモート サービスまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### トラフィックの方向

ポートを通過するトラフィックの流れる方向（着信、双方向、発信）。



(注) オペレーティングシステムは、ローカルアプリケーションまたはサービスがリモートデバイスの宛先ポートへの接続に使用する送信元ポートを動的に割り当てます。ほとんどの場合、このポートは、TCP/UDP 1024 より大きい番号でランダムに割り当てられます。

## Contact Center Enterprise ポートの使用状況

次の表に、Unified CCE と CTI OS の情報を示します。

一部のポート定義には数式を使用しています。次に例を示します。

TCP 40007 + (インスタンス番号 \* 40)

この例では、インスタンス 0 がポート 40007、インスタンス 1 がポート 40047、インスタンス 2 がポート 40087（以下同様）を使用します。



表 2 : Unified CCE のポート使用状況 : ルータ、PG、管理およびデータ サーバ、ロガー

リスナー (プロセスまたはアプリケーション プロトコル)	リスナー プロトコルおよびポート	リモート デバイス (プロセスまたはアプリケーション プロトコル)	リモート プロトコルおよびポート	トラフィックの方向	注記
ルータ (B 側) (MDS)	<p><b>プライベート低 :</b></p> <ul style="list-style-type: none"> <li>• TCP 41004 + (インスタンス番号 * 40)</li> </ul> <p><b>プライベート中 :</b></p> <ul style="list-style-type: none"> <li>• TCP 41016 + (インスタンス番号 * 40)</li> </ul> <p><b>プライベート高 :</b></p> <ul style="list-style-type: none"> <li>• TCP 41005 + (インスタンス番号 * 40)</li> </ul> <p><b>CIC の状態転送 :</b></p> <ul style="list-style-type: none"> <li>• TCP 41022 + (インスタンス番号 * 40)</li> </ul> <p><b>HLGR の状態転送 :</b></p> <ul style="list-style-type: none"> <li>• TCP 41021 + (インスタンス番号 * 40)</li> <li>• TCP 41032 + (インスタンス番号 * 40)</li> </ul> <p><b>RTR の状態転送 :</b></p> <ul style="list-style-type: none"> <li>• TCP 41020 + (インスタンス番号 * 40)</li> </ul> <p>UDP 39500~39999</p> <p><b>DBAgent の状態転送 :</b></p> <ul style="list-style-type: none"> <li>• TCP 41033 + (インスタンス番号 * 40)</li> </ul>	ルータ (A 側) (MDS)		双方向	<p>中央コントローラ サイトのプライベート ネットワーク</p> <p>(注) ルータのプライベート インターフェイスで QoS が有効になっている場合、UDP ポートは使用されません。</p>

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
ルータ（B側） （MDS）	MDS プロセス ポート TCP 41000	MDS プロセス クライアント		双方向	
ルータ（B側） （MDS）	MDS 状態転送ポート TCP 41001	MDS プロセス クライアント（同期）		双方向	
ICM PG1（A側およびB側） （pgagent）	TCP 43006 +（インスタンス番号 * 40）	ICM PG1（反対側：A側またはB側） （pgagent）		双方向	パブリック ネットワーク （テストの相手側）
ICM PG2（A側およびB側） （pgagent）	TCP 45006 +（インスタンス番号 * 40）	ICM PG2（反対側：A側またはB側） （pgagent）		双方向	パブリック ネットワーク （テストの相手側）
ICM PG3（A側およびB側） （pgagent）	TCP 47506 +（インスタンス番号 * 40）	ICM PG3（反対側：A側またはB側） （pgagent）		双方向	パブリック ネットワーク （テストの相手側）

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
ICM PG1（A側およびB側） （MDS）	<ul style="list-style-type: none"> <li>プライベート低： TCP 43004 + (インスタンス番号 * 40)</li> <li>プライベート中： TCP 43016 + (インスタンス番号 * 40)</li> <li>プライベート高： TCP 43005 + (インスタンス番号 * 40)</li> <li>OPC の状態転送： TCP 43023 + (インスタンス番号 * 40)</li> </ul> UDP 39500～39999	ICM PG1（反対側：A側またはB側）		双方向	プライベート ネットワーク （注） ICM PG のプライベート インターフェイスで QoS が有効になっている場合、UDP ポートは使用されません。
ICM PG2（A側およびB側） （MDS）	<ul style="list-style-type: none"> <li>プライベート低： TCP 45004 + (インスタンス番号 * 40)</li> <li>プライベート中： TCP 45016 + (インスタンス番号 * 40)</li> <li>プライベート高： TCP 45005 + (インスタンス番号 * 40)</li> <li>OPC の状態転送： TCP 45023 + (インスタンス番号 * 40)</li> </ul> UDP 39500～39999	ICM PG2（反対側：A側またはB側）		双方向	プライベート ネットワーク （注） ICM PG のプライベート インターフェイスで QoS が有効になっている場合、UDP ポートは使用されません。

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
ICM PG3（A側およびB側） （MDS）	<ul style="list-style-type: none"> <li>プライベート低： TCP 47504+（インスタンス番号 * 40）</li> <li>プライベート中： TCP 47516+（インスタンス番号 * 40）</li> <li>プライベート高： TCP 47505+（インスタンス番号 * 40）</li> <li>OPC の状態転送： TCP 47523+（インスタンス番号 * 40）</li> </ul> UDP 39500～39999	ICM PG3（反対側：A側またはB側）		双方向	プライベート ネットワーク （注） ICM PG のプライベート インターフェイスで QoS が有効になっている場合、UDP ポートは使用されません。
ICM PG1（B側） （MDS）	MDS プロセス ポート TCP 43000	MDS プロセス クライアント		双方向	
ICM PG1（B側） （MDS）	MDS 状態転送ポート TCP 43001	MDS プロセス クライアント（同期）		双方向	
ICM PG2（B側） （MDS）	MDS プロセス ポート TCP 45000	MDS プロセス クライアント		双方向	
ICM PG2（B側） （MDS）	MDS 状態転送ポート TCP 45001	MDS プロセス クライアント（同期）		双方向	
ICM PG3（B側） （MDS）	MDS プロセス ポート TCP 47500	MDS プロセス クライアント		双方向	

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモート デバイス（プロセスまたはアプリケーションプロトコル）	リモート プロトコルおよびポート	トラフィックの方向	注記
ICM PG3（B側） （MDS）	MDS 状態転送ポート TCP 47501	MDS プロセス クライアント（同期）		双方向	
ルータ（A側） （MDS）	MDS プロセス ポート TCP 40000	MDS プロセス クライアント		双方向	
ルータ（A側） （MDS）	MDS 状態転送ポート TCP 40001	MDS プロセス クライアント（同期）		双方向	
ICM PG1（A側） （MDS）	MDS プロセス ポート TCP 42000	MDS プロセス クライアント		双方向	
ICM PG1（A側） （MDS）	MDS 状態転送ポート TCP 42001	MDS プロセス クライアント（同期）		双方向	
ICM PG2（A側） （MDS）	MDS プロセス ポート TCP 44000	MDS プロセス クライアント		双方向	
ICM PG2（A側） （MDS）	MDS 状態転送ポート TCP 44001	MDS プロセス クライアント（同期）		双方向	
ICM PG3（A側） （MDS）	MDS プロセス ポート TCP 46000	MDS プロセス クライアント		双方向	
ICM PG3（A側） （MDS）	MDS 状態転送ポート TCP 46001	MDS プロセス クライアント（同期）		双方向	

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
ルータ（A側）DMP（ccagent）	<ul style="list-style-type: none"> <li>パブリック低： TCP 40002 + (インスタンス番号 * 40)</li> <li>パブリック中： TCP 40017 + (インスタンス番号 * 40)</li> <li>パブリック高： TCP 40003 + (インスタンス番号 * 40)</li> </ul> UDP 39500～39999	ICM PG (pgagent)		双方向	5.0 以前の PG 通信に対する中央コントローラ ルータに PG を接続するパブリックネットワーク。  (注) ICM PG のプライベート インターフェイスで QoS が有効になっている場合、UDP ポートは使用されません。
ルータ（B側）DMP（ccagent）	<ul style="list-style-type: none"> <li>パブリック低： TCP 41002 + (インスタンス番号 * 40)</li> <li>(インスタンス番号パブリック中： TCP 41017 + (インスタンス番号 * 40)</li> <li>パブリック高： TCP 41003 + (インスタンス番号 * 40)</li> </ul> UDP 39500～39999	ICM PG (pgagent)		双方向	5.0 以前の PG 通信に対する中央コントローラ ルータに PG を接続するパブリックネットワーク。  (注) ICM PG のプライベート インターフェイスで QoS が有効になっている場合、UDP ポートは使用されません。
ルータ A（rtfeed）	TCP 40007 + (インスタンス番号 * 40)	Administration & Data Server		双方向	リアルタイム フィード
ルータ B（rtfeed）	TCP 41007 + (インスタンス番号 * 40)	Administration & Data Server		双方向	リアルタイム フィード

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
ロガー（A側）	TCP 40026 + (インスタンス番号 * 40) TCP 40028 + (インスタンス番号 * 40)	管理およびデータサーバの Historical Data Server (HDS)		双方向	複製
ロガー（B側）	TCP 41026 + (インスタンス番号 * 40) TCP 41028 + (インスタンス番号 * 40)	管理およびデータサーバの Historical Data Server (HDS)		双方向	複製
プライマリ管理およびデータサーバ (rtfeed)	TCP 48008 + (インスタンス番号 * 40)	管理クライアント		双方向	リアルタイム フィード
セカンダリ管理およびデータサーバ (rtfeed)	TCP 49008 + (インスタンス番号 * 40)	管理クライアント		双方向	リアルタイム フィード
Contact Sharing	TCP 61616	ライブデータ用の ActiveMQ	TCP 61616	双方向	
CICM ルータ (A側) (INCRPNIC)	UDP 40025 + (インスタンス番号 * 40)	NAM ルータ (CIC)		双方向	CICM に NAM を接続するパブリック ネットワーク
CICM ルータ (B側) (INCRPNIC)	UDP 41025 + (インスタンス番号 * 40)	NAM ルータ (CIC)		双方向	CICM に NAM を接続するパブリック ネットワーク
CSFS	TCP 40015	CSFS デュプレックス構成ピア		双方向	CSFS イベント同期リンク

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
ロガー（A側）	40013+（インスタンス番号*40）			双方向	リカバリ
ロガー（B側）	41013+（インスタンス番号*40）			双方向	リカバリ
診断フレームワーク	TCP 7890			双方向	このサービスアビリティコンポーネントは、主要なCCE コンポーネントサーバ（ルータ、ロガー、PG、管理およびデータサーバなど）にインストールされます

表 3: Unified CCE のポート使用状況：ディストリビュータおよび Internet Script Editor

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
MSSQL		Logger ディストリビュータ	TCP 1433	双方向	



表 4 : Unified CCE のポート使用状況 : CCE Outbound Option Dialer

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
SIP		Cisco Unified Communications Manager (Unified CM)	UDP 58800	双方向	<b>SIPDialerPortBaseNumber</b> レジストリ キーで設定します。
RTP for SIP	次の式に基づく範囲の UDP ポート : <ul style="list-style-type: none"> <li>• RangeStart = RTPPortRangeStart + (instNum * 2000)</li> <li>• RangeEnd = RangeStart + 2000</li> </ul> RTPPortRangeStart は、 <b>RTPPortRangeStart</b> レジストリ キーで設定できます。instNum は、ダイヤラのインスタンス番号です。	音声ゲートウェイ		双方向	予約コール用の受信ポート。UDP ポートを選択して設定するには、 <b>RTPPortRangeStart</b> レジストリ キーを使用します
TFTP		TFTP サーバ	UDP 69	双方向	
TFTP ファイル転送			エフェメラル	双方向	
MR PG	TCP 38001 + (インスタンス数)			双方向	MR PG は、このポートを使用して SIP ダイヤラに接続します。
MR PG (SIP)	5060 および SIPDialerPortBaseNumber + インスタンス番号			双方向	このポートは、Unified Communications Manager、音声ゲートウェイ、または SIP プロキシで使用されます。

表 5 : Unified CCE のポート使用状況 : CTI および CTI Object Server

リスナー (プロセスまたはアプリケーションプロトコル)	リスナー プロトコルおよびポート	リモートデバイス (プロセスまたはアプリケーションプロトコル)	リモートプロトコルおよびポート	トラフィックの方向	注記
GED-188 (CTI サーバ)	サイド A TCP 42027 + (インスタンス番号 * 40) サイド B TCP 43027 + (インスタンス番号 * 40)	Finesse Cisco Outbound Dialer ARM インターフェイス CTI OS サーバ		双方向	CTI OS は TDM およびシステム PG でのみサポートされます。
CTI OS サーバ	TCP 42028	CTI OS クライアント CTI OS サーバピア Cisco Sync Service		双方向	CTI OS は TDM およびシステム PG でのみサポートされます。 最初の CTI OS インスタンスに適用可能。複数インスタンスの CTI OS については、カスタムポートを定義する必要があります。
CTI OS スーパーバイザデスクトップ	UDP 39200	CTI OS クライアント		双方向	デスクトップサイレントモニタリング CTI OS スーパーバイザデスクトップは、システム PG でのみサポートされます。
CTIOS サイレント モニタ サービス	TCP 42228	CTI OS クライアント		双方向	CTI OS サイレント モニタ サービスは、システム PG でのみサポートされます。
Cisco Enterprise Data Store	TCP 42228	Siebel サーバ		双方向	スクリーン コール コンテキストのサポート

表 6: Unified CCE のポート使用状況: Packaged CCE

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
データサーバおよび外部HDS	HTTPS 443	ESXi ホスト	HTTPS 443	双方向	

表 7: Unified CCE のポート使用状況: TDM/IP ペリフェラル

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
<b>IP プロセス通信</b>					
CTI/QBE		Unified CM	TCP 2748	双方向	JTAPI
PG、VRU PIM (GED-125)	TCP 5000~5001	Customer Voice Portal (または ISN) Cisco Unified IP-IVR		双方向	Unified ICM/IVR メッセージインターフェイス、VRU PIM
CCE PG	TCP 2789	Unified CM		双方向	JTAPI アプリケーションサーバ
MR PIM	TCP 2000	メディアルーティングプロセス		双方向	
<b>TDM プロセス通信</b>					
(注) ペリフェラル通信の詳細については、使用しているスイッチの『ACD Supplement』ユーザマニュアルを参照してください。					

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
Aspect PIM		Aspect ACD	TCP 8000	双方向	リアルタイムブリッジで使用
Aspect Contact Center サーバ PIM		Aspect Contact Center サーバ	TCP 6101 TCP 6102 TCP 9001	双方向	アプリケーションブリッジイベントリンク
Avaya PIM	TCP 6060～6070	Avaya ACD CMS	TCP 5678	双方向	イベントリンク
MIS プロセス	TCP 3000～3030	VRU		双方向	CTI サーバに接続し、VRU PIM をリッスンします
Avaya Aura Contact Center (AACC) PIM		Avaya ACD	TCP 3000	双方向	
UCCX ゲートウェイ PIM		UCCX	TCP 12028	双方向	ポート番号は設定可能



(注) ネットワーク インターフェイス コントローラ (NIC) のポート使用状況については、『TCP/IP-based NIC System Management Guide Supplements』および NIC または SCP 接続の設定パラメータを参照してください。

表 8 : Unified CCE のポート使用状況 : Windows 認証およびリモート管理ポート

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモート デバイス（プロセスまたはアプリケーションプロトコル）	リモート プロトコルおよびポート	トラフィックの方向	注記
RPC	TCP 135 UDP 135			双方向	
NetBIOS セッション	TCP 139			双方向	
NetBIOS 名前解決	TCP 137 UDP 137			双方向	
NetBIOS Netlogon/ブラウズ	UDP 138			双方向	
SMB	TCP 445 UDP 445 <sup>1</sup>			双方向	
LDAP	TCP 389 UDP 389			双方向	
LDAP SSL	TCP 636			双方向	
LDAP GC	TCP 3268			双方向	
LDAP GC SSL	TCP 3269			双方向	
DNS	TCP 53 UDP 53			双方向	
Kerberos	TCP 88 UDP 88			双方向	
SQL Server :	TCP 1433 UDP 1434			双方向	Q287932 を参照

<sup>1</sup> 名前付きパイプ接続でも使用。



(注) Windows 認証の詳細については、『*Service overview and network port requirements for the Windows Server system*』（Microsoft サポート技術情報の記事 Q832017）を参照してください。

表 9: **Unified CCE** のポート使用状況：ネットワーク管理およびリモート管理

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
SNMP トラップ	UDP 162			双方向	
Syslog	UDP 514			双方向	
Telnet	TCP 23			双方向	
RDP（ターミナルサービス）	TCP 3389			双方向	
pcAnywhere	TCP 5631 UDP 5632			双方向	
VNC	TCP 5900 TCP 5800（Java HTTP）			双方向	RealVNC

表 10: **Unified CCE** のポート使用状況：カスタマーインタラクションアナライザ

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
VPN/ターミナルサービス	TCP 3389	通話録音サーバ		双方向	

表 11 : Unified CCE のポート使用状況 : ライブ データ

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモート デバイス（プロセスまたはアプリケーションプロトコル）	リモート プロトコルおよびポート	トラフィックの方向	注記
ルータ（A側およびB側）（TIP イベント）	ルータ A : 40034+(インスタンス数 * 40) ルータ B : 41034+(インスタンス数 * 40)	CUIC/ライブデータ		双方向	パブリック ネットワークのライブ データ イベント。
ルータ（A側およびB側）（TIP TOS）	ルータ A : 40035+(インスタンス数 * 40) ルータ B : 41035+(インスタンス数 * 40)	CUIC/ライブデータ		双方向	パブリック ネットワークのライブ データ テストの相手側。
ICM PG1（A側およびB側）（TIP イベント） <sup>2</sup>	A 側 : 42034+(インスタンス数 * 40) B 側 : 43034+(インスタンス数 * 40)	CUIC/ライブデータ		双方向	パブリック ネットワークのライブ データ イベント。
ICM PG2（A側およびB側）（TIP イベント）	A 側 : 44034+(インスタンス数 * 40) B 側 : 45034+(インスタンス数 * 40)	CUIC/ライブデータ		双方向	パブリック ネットワークのライブ データ イベント。
ICM PG1（A側およびB側）（TIP TOS）	A 側 : 42035+(インスタンス数 * 40) B 側 : 43035+(インスタンス数 * 40)	CUIC/ライブデータ		双方向	パブリック ネットワークのライブ データ テストの相手側。
ICM PG2（A側およびB側）（TIP TOS）	A 側 : 44035+(インスタンス数 * 40) B 側 : 45035+(インスタンス数 * 40)	CUIC/ライブデータ		双方向	パブリック ネットワークのライブ データ テストの相手側。
Socket.IO のセキュアでないポート	TCP 12007	CUIC/ライブデータ	Socket.IO	双方向	

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
Socket.IO のセキュアポート	TCP 12008	CUIC/ライブデータ	Socket.IO	双方向	
CCE ライブデータ Cassandra サービス	TCP 12000			双方向	ライブデータ Cassandra のコマンドおよびデータ用 TCP ポート
CCE ライブデータ Cassandra サービス	TCP 12001			双方向	ライブデータ Cassandra の暗号化通信用 SSL ポート。 （暗号化オプションで有効にしないかぎり未使用）
CCE ライブデータ Cassandra サービス	TCP 9160			双方向	Thrift がクライアントをリッスンするのに使用するライブデータ Cassandra ポート
CCE ライブデータ Storm DRPC サービス	TCP 3772			双方向	ライブデータ DRPC ポート
CCE ライブデータ Storm DRPC サービス	TCP 3773			双方向	ライブデータ DRPC 呼び出しポート
CCE ライブデータ Zookeeper サービス	TCP 2181			双方向	ライブデータ レポート
CCE ライブデータ Web サービス	TCP 12004 ~ 12006			双方向	ライブデータ レポート



リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモート デバイス（プロセスまたはアプリケーションプロトコル）	リモート プロトコルおよびポート	トラフィックの方向	注記
CCE ライブ データ Storm Nimbus サービス	TCP 6627			双方向	ライブ データ Nimbus Thrift ポート
CCE ライブ データ ActiveMQ サービス	TCP 61616			双方向	ライブ データ ActiveMQ Openwire トランスポート コネクタ ポート
CCE ライブ データ ActiveMQ サービス	TCP 61612			双方向	ライブ データ ActiveMQ Stomp トランスポート コネクタ ポート
Unified Intelligence Center	TCP 8081			双方向	HTTP - Unified Intelligence Center

- <sup>2</sup> TIP/TOS 接続のポートの割り当ては、PG ペア（A 側および B 側）が同じサーバ上にインストールされた順番に基づいて行われます。たとえば、最初に追加された PG（PG1 A 側および B 側）に、それぞれ TIP 基本ポート 42034/43034 が割り当てられます。2 番目にインストールされる PG ペア（PG2 A 側および B 側）には、44034/45034 が割り当てられ、以後同様に割り当てられます。同じ割り当ては TOS ポートにも適用されます。

## Unified CCMP のポート使用状況

表 12 : Cisco Unified Contact Center Management Portal のポート使用状況

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモート プロトコルおよびポート	リモート デバイス（プロセスまたはアプリケーションプロトコル）	トラフィックの方向	注記
<b>CCMP Web/アプリケーション サーバ A</b>					
SQL	TCP 1433	CCMP DB サーバ A/B			標準の SQL 接続

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートプロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	トラフィックの方向	注記
LDAP	TCP 389	ドメインコントローラ	UDP 389		スーパーバイザがプロビジョニングで使用する AD アカウント情報を読み取るために使用
<b>CCMP Web/アプリケーション サーバ B</b>					
SQL	TCP 1433	CCMP DB サーバ A/B			標準の SQL 接続
LDAP	TCP 389	ドメインコントローラ	UDP 389		スーパーバイザがプロビジョニングで使用する AD アカウント情報を読み取るために使用
<b>CCMP データベース サーバ A</b>					
SQL	TCP 1433	CCMP DB サーバ B			SQL レプリケーション用
	TCP 1433	CCE/CCH 管理およびデータサーバ A 側			CCE/CCH ディメンションデータのインポート用
	TCP 1433	CCE/CCH 管理およびデータサーバ B 側			CCE/CCH ディメンションデータのインポート用
*MSDTC	TCP 135	CCMP DB サーバ B	TCP 1024～5000		CCMP 監査アーカイブジョブ用
SMB over IP	UDP 445*		TCP 445		CVP ファイルアップロードおよびファイルレプリケーション用
*名前付きパイプ接続でも使用。					
<b>CCMP データベース サーバ B</b>					

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートプロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	トラフィックの方向	注記
SQL	TCP 1433	CCMP DB サーバ A			SQL レプリケーション用
	TCP 1433	CCE/CCH 管理およびデータサーバ A 側			CCE/CCH ディメンションデータのインポート用
	TCP 1433	CCE/CCH 管理およびデータサーバ B 側			CCE/CCH ディメンションデータのインポート用
*MSDTC	TCP 135	CCMP DB サーバ A	TCP 1024～5000		CCMP 監査アーカイブジョブ用
SMB over IP	UDP 445*		TCP 445		CVP ファイルアップロードおよびファイルレプリケーション用

これらは、すべてのサーバ名が TCP/IP アドレスまたは DNS 名である（したがって NetBIOS ポートは不要である）ことを前提としています。

サポート上の理由で、すべての Unified Contact Center Management Portal サーバにアクセスする場合にもポートが必要です（pcAnywhere とターミナルサービスのどちらでも）。



(注) このリストには、DNS や Kerberos などの標準の Windows ポートは含まれていません。

\* MSDTC 応答ポートは、デフォルトでは 1024 ～ 5000 の範囲で動的に割り当てられたポートを使用します。この範囲を設定するには、HKEY\_LOCAL\_MACHINE\Software\Microsoft\Rpc\Internet location レジストリ キーを作成し、次のレジストリ値を追加します。

- Ports (REG\_MULTI\_SZ) - 1 行に 1 つのポート範囲 (3000-3005 など) を指定します
- PortsInternetAvailable (REG\_SZ) - この値は常に "Y" に設定します (引用符を含みません)
- UseInternetPorts (REG\_SZ) - この値は常に "Y" に設定します (引用符を含みません)

## Unified CRM Connector のポート使用状況

表 13 : Cisco Unified CRM Connector for SAP

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
CRM DataStore for SAP	TCP 42029	CRM Connector for SAP			

表 14 : Cisco Unified CRM Connector for Microsoft CRM、Oracle PeopleSoft、Salesforce.com

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
MSCRM サーバ	TCP 81	MSCRM クライアント			MSCRM のみ
CRM Connector サーバ	TCP 5666	CRM アダプタ			\\Program Files\Cisco\CRM Connector\MCIS\Config.ini で設定可能
.NET アダプタ	TCP 5558	Agent Desktop			リモート処理ポート
CRM Connector サーバ	TCP 42027	Cisco CTI サーバ			A 側のデフォルトポート。Config.ini ファイルの [CTIModule Setting] の Port_A で設定可能。
CRM Connector サーバ	TCP 44027	Cisco CTI サーバ			B 側のデフォルトポート。Config.ini ファイルの [CTIModule Setting] の Port_B で設定可能。

リスナー (プロセスまたはアプリケーションプロトコル)	リスナープロトコルおよびポート	リモートデバイス (プロセスまたはアプリケーションプロトコル)	リモートプロトコルおよびポート	トラフィックの方向	注記
CRM Connector サーバ	TCP 65372	サーバ管理ツール			\Program Files\Cisco\CRM Connector\MCIS\Config.ini および \Program Files\Cisco\CRM Connector\Server Administration Tool\WebComponent\server.config で設定可能

## Cisco Agent Desktop (CAD) のポート使用状況



**重要** Unified CCE 11.0(1) では、Cisco Agent Desktop は推奨されません。



(注) Agent Desktop クライアントが Citrix 環境で動作している場合、Citrix サーバは CAD/CTIOS クライアントのポートをランダムに選択します。Citrix が Windows 2008 で動作している場合、ランダムに割り当てられるポート番号は Internet Assigned Numbers Authority (IANA) の標準の範囲である 49152 ~ 65535 に含まれます。

表 15: Cisco Agent Desktop (CAD) のポート使用状況

リスナー (プロセスまたはアプリケーションプロトコル)	リスナープロトコルおよびポート	リモートデバイス (プロセスまたはアプリケーションプロトコル)	リモートプロトコルおよびポート	トラフィックの方向	注記
<b>Cisco Agent Desktop</b>					
デスクトップ モニター	TCP 59020	Cisco Supervisor Desktop			
FCCServer	TCP 3002	Supervisor Desktop	TCP 3101		

## Cisco Agent Desktop (CAD) のポート使用状況

リスナー (プロセス またはアプ リケーショ ンプロトコ ル)	リスナープ ロトコルお よびポート	リモート デバイス (プロ セスまたはアプリー ケーション プロトコル)	リモートプロ トコルおよ びポート	トラフィックの方向	注記
チャット (Chat)	TCP 59020	Cisco Desktop Base Services			
CTI OS		CTI OS サーバ	TCP 42028		
SIP	UDP/TCP 5060 *	Unified CVP および Cisco Unified Communications Manager (Cisco Unified Communications Manager IM and Presence Service を 含む)	UDP/TCP 5060 *		CA は SIP over TLS をサ ポートしません
AXL (SOAP)	HTTPS 443	Cisco Unified Communications Manager IM and Presence Service			
<b>Cisco Supervisor Desktop</b>					
チャット (Chat)	TCP 59021	Cisco Desktop Base Services			チャット (Chat)
Cisco Unified Presence	TCP 5060	Cisco Desktop Base Services			Unified CVP および Unified Communications Manager (Cisco Unified CM IM and Presence Service を含む)
RTP	UDP 59010 UDP 59012	Cisco Desktop VoIP Monitor Service			VoIP
RTP	UDP 59014 UDP 59016	Cisco Desktop Recording Server			再生
<b>Cisco Desktop Base Services</b>					
LRM	TCP 65431 TCP 65432	Cisco Agent Desktop Cisco Supervisor Desktop			
チャット (Chat)	TCP 59000 TCP 37350	Cisco Agent Desktop Cisco Supervisor Desktop			

リスナー (プロセス またはアプ リケーショ ンプロトコ ル)	リスナープ ロトコルお よびポート	リモート デバイス (プロ セスまたはアプリー ケーション プロトコル)	リモートプロ トコルおよ びポート	トラフィックの方向	注記
エンタープ ライズ	TCP 59004	Cisco Agent Desktop Cisco Supervisor Desktop			
エンタープ ライズ	TCP 3004				OmniOrbUsePort (サー バ)
Rascal	TCP 59003	Cisco Agent Desktop Cisco Supervisor Desktop			
ディレクト リ (Directory)	TCP 38983	Cisco Agent Desktop Cisco Supervisor Desktop			LDAP
TrueUpdate	TCP 8088	Cisco Agent Desktop Cisco Supervisor Desktop			Tomcat
LRM	TCP 65431 TCP 65432	Cisco Desktop Base Services			冗長用
MSL	UDP 27871	Cisco Desktop Base Services			冗長用
ディレクト リ (Directory)	TCP 38983	Cisco Desktop Base Services			冗長用
LRM	TCP 65431	Cisco Desktop VoIP Monitor Service			
LRM	TCP 65432	ライセンス サーバ			
LDAP	TCP 38983	Cisco Desktop VoIP Monitor Service			
チャット (Chat)	TCP 3002				LDAP VPN クライアント
チャット (Chat)	TCP 3100				LDAPOmniOrbUsePort (クライアント)

リスナー (プロセス またはアプ リケーショ ンプロトコ ル)	リスナープ ロトコルお よびポート	リモート デバイス (プロ セスまたはアプリー ケーション プロトコル)	リモートプロ トコルおよ びポート	トラフィックの方向	注記
チャット (Chat)	TCP 59000				LDAPOmniOrbUsePort (サーバ)
LRM	TCP 65431 TCP 65432	Cisco Desktop Recording Service			
LDAP	TCP 38983	Cisco Desktop Recording Service			
LRM	TCP 65431 TCP 65432	Cisco Desktop Administrator			
エンタープ ライズ	TCP 59004	Cisco Desktop Administrator			
ディレクト リ (Directory)	TCP 38983	Cisco Desktop Administrator			
TAI	TCP 59010	Cisco Desktop Administrator			
Sync	TCP 59011	Cisco Desktop Administrator			
Sync	TCP 27872				
TrueUpdate	TCP 8088	Cisco Desktop Administrator			Tomcat
IPPA	TCP 59012	Cisco Agent Desktop Browser Edition			
IPPA	TCP 59010				
Tomcat	TCP 8088	Cisco Agent Desktop Browser Edition			
GED-188		CTI サーバ (CTI Server)	A 側 : TCP 42027 B 側 : TCP 43027		コール イベント



リスナー (プロセス またはアプ リケーショ ンプロトコ ル)	リスナープ ロトコルお よびポート	リモートデバイス(プロ セスまたはアプリー ケーションプロトコル)	リモートプロ トコルおよ びポート	トラフィックの方向	注記
MSSQL		ディストリビュータ	TCP 1433		Rascal
AXL (SOAP)	ダイナミッ ク	Unified CM	TCP 80		
<b>Cisco Desktop VoIP Monitor Server</b>					
プライマリ サーバ (Primary Server)	TCP 59002	Cisco Agent Desktop Cisco Supervisor Desktop Cisco Desktop Base Services			OmniOrbUsePort (サー バ)
IP 検出	TCP 37606	Cisco Agent Desktop Cisco Supervisor Desktop			
VPN ポート (サーバ)	TCP 37606				
AXL (SOAP)	ダイナミッ ク	Unified CM	TCP 80		電話機の MAC アドレス ルックアップ
<b>Cisco Desktop Recording Server</b>					
プライマリ サーバ (Primary Server)	TCP 59005	Cisco Agent Desktop Cisco Supervisor Desktop Cisco Desktop Base Services			OmniOrbUsePort (サー バ)
IP 検出	TCP 59027	Cisco Supervisor Desktop Cisco Desktop Base Services			
VPN サーバ ポート	TCP 59027				

リスナー (プロセス またはアプ リケーショ ンプロトコ ル)	リスナープ ロトコルお よびポート	リモート デバイス (プロ セスまたはアプリー ケーション プロトコル)	リモートプロ トコルおよ びポート	トラフィックの方向	注記
RTP	UDP 59500 ~59700	Cisco Agent Desktop Cisco Desktop VoIP Monitor Server			
	59500				ポート範囲の開始 (クラ イアント)
	59700				ポート範囲の終了 (クラ イアント)
<b>RP サーバ</b>					
プライマリ サーバ	59005				
VPN サーバ ポート	59027				
クライアン ト ポートへ	59014				クライアント
クライアン ト ポートか ら	59016				クライアント

## Genesys コールセンターへの Cisco Voice の統合

リスナー (プ ロセスまた はアプリー ケーション プロトコ ル)	リスナーブ ロトコルお よびポート	リモートデバイス (プロセ スまたはアプリー ケーション プロトコル)	リモートブ ロトコルお よびポート	トラフィック の方向	注記
Genesys System Interoperability Manager	TCP 2555	Genesys T-Server Alcatel A4400			CSTA このポートはレジストリで 調整できます。







## 第 3 章

# Unified CVP のポート使用状況

- [ポート使用状況表の列, 37 ページ](#)
- [Unified CVP のポート使用状況, 38 ページ](#)

## ポート使用状況表の列

このドキュメントに含まれるポート使用状況表の列について、次に説明します。

### リスナー（プロセスまたはアプリケーション プロトコル）

サーバまたはアプリケーションを表す値と、（必要に応じて）オープンまたは独自のアプリケーション プロトコル。

### リスナー プロトコルおよびポート

サーバまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### リモート デバイス（プロセスまたはアプリケーション プロトコル）

プロトコルで指定されるサーバまたはサービスに接続するリモート アプリケーションまたはデバイス、またはリモート プロトコルおよびポートでリッスンするリモート アプリケーションまたはデバイス。

### リモート プロトコルおよびポート

リモート サービスまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### トラフィックの方向

ポートを通過するトラフィックの流れる方向（着信、双方向、発信）。



(注) オペレーティングシステムは、ローカルアプリケーションまたはサービスがリモートデバイスの宛先ポートへの接続に使用する送信元ポートを動的に割り当てます。ほとんどの場合、このポートは、TCP/UDP 1024 より大きい番号でランダムに割り当てられます。

## Unified CVP のポート使用状況



(注) オペレーション コンソール サーバは、他のコンポーネントとの通信に動的ポートを使用します。そのサーバと他の Unified CVP コンポーネント間に、ファイアウォールを展開することはできません。

表 16 : Cisco Unified Customer Voice Portal のポート使用状況

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
コールサーバ JMX	2098	JConsole	ランダム (Random)	双方向	JConsole によるコールサーバへの JMX アクセス
CVP メッセージングレイヤ	TCP 23000 ~ 28000 (最初に使用可能)	CVP サブシステム	CVP コンポーネント間のローカル/リモート	双方向	CVP メッセージバス通信
CVP コールサーバ	UDP 5060 TCP 5060	SIP エンドポイント	ランダム (Random)	双方向	受信した SIP 要求のリスナーポート。ポートは設定可能。
VXML Server : HTTP	TCP 7000	IOS VXML ゲートウェイ/VVB	ランダム (Random)	双方向	VXML over HTTP。HTTP サーバがポート 7000 で応答したコール/セッション (HTTP サーバはローカルシステムポート 9080 の WAS に要求をリレーする)。

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモート デバイス（プロセスまたはアプリケーションプロトコル）	リモート プロトコルおよびポート	トラフィックの方向	注記
VXML Server : HTTPS	TCP 7443	IOS VXML ゲートウェイ/VVB	ランダム (Random)	双方向	VXML over HTTPS。HTTPS サーバがポート 7443 で応答したコール/セッション。
Tomcat を含む VXML Server	TCP 7005	ローカル マシン		ローカル (Local)	ローカル アクセスだけに制限されるポート
	TCP 7009			ローカル (Local)	AJP/1.3 Connector
VXML Server JMX	TCP 9696	JConsole	ランダム (Random)	双方向	JConsole による VXML Server への JMX アクセス
VXML Server	TCP 10100	ローカル VXML Server の管理スクリプト		ローカル (Local)	ローカル アクセスだけに制限されるポート
CVP コール サーバ Tomcat : HTTP	TCP 8000	Web ブラウザ	ローカル/リモートでランダム	双方向	HTTP
CVP コール サーバ Tomcat : HTTPS	TCP 8443	Web ブラウザ	ローカル/リモートでランダム	双方向	HTTPS
CVP IVR Server	TCP 8002	VXML Server		ローカル (Local)	TCP 経由のメッセージ (注) このポートは、コールサーバと VXML サーバ間の通信に使用されません。
CVP コール サーバ : HTTP	TCP 8005			ローカル (Local)	ローカル アクセスだけに制限されるポート
CVP OPSConsole : HTTP	TCP 9000	Web ブラウザ	ランダム (Random)	双方向	CVP コンポーネントを設定するための Web ベース インターフェイス

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
CVP OPSConsole : HTTPS	TCP 9443	Web ブラウザ	ランダム (Random)	双方向	SSL を使用して CVP コンポーネントを設定するための Web ベース インターフェイス
CVP OPSConsole	TCP 9005	ローカル マシン		ローカル (Local)	ローカル アクセスだけに制限されるポート
CVP OPSConsole	TCP 9009	ローカル マシン		ローカル (Local)	AJP/1.3 Connector
CVP OPSConsole	TCP 1529	ローカル マシン		ローカル (Local)	ローカル アクセスだけに制限されるポート
CVP Resource Manager の FTP サーバ	TCP 21	コンテンツサービス スイッチ	ランダム (Random)	双方向	CVP OPSConsole と同じマシンに配置された Resource Manager のみで開く
CVP Resource Manager	TCP 2099	CVP OPSConsole	ランダム (Random)	双方向	OPSConsole からリモートデバイス上の CVP Resource Manager への JMX 通信
CVP Resource Manager の Java サービス ラッパー	TCP 32000 ~ 32999 (最初に使用可能)	ラッパーが起動する JVM インスタンス	ランダム (Random)	ローカル (Local)	CVP Resource Manager サービス ラッパーは、最初の JVM インスタンスを接続した後は接続を受け入れません。
RTP/RTCP	UDP : 16384 ~ 32767		UDP 16384 ~ 32767	双方向	音声メディア 通常、RTP は偶数番号のポートに割り当てられ、RTCP はその次に大きいポート番号になります。



リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモート デバイス（プロセスまたはアプリケーションプロトコル）	リモート プロトコルおよびポート	トラフィックの方向	注記
CVP SNMP サブエージェント	UDP 5517、5519、5521、5523、5525、5527、5529、5531、5533、5535、5537、5539、5541、5543、5545、5547、5549、5551、5553、5555	CVP SNMP サブシステム	UDP 5516、5518、5520、5522、5524、5526、5528、5530、5532、5534、5536、5538、5540、5542、5544、5546、5548、5550、5552、5554	ローカル (Local)	CVP SNMP サブエージェントは CVP SNMP サブシステムからのローカル要求を処理します

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
CVP SNMP サブシステム	UDP 5516、5518、5520、5522、5524、5526、5528、5530、5532、5534、5536、5538、5540、5542、5544、5546、5548、5550、5552、5554	CVP SNMP サブエージェント	UDP 5517、5519、5521、5523、5525、5527、5529、5531、5533、5535、5537、5539、5541、5543、5545、5547、5549、5551、5553、5555	ローカル (Local)	CVP SNMP サブシステムは CVP SNMP サブエージェントからのローカル要求を処理します
CVP ICM サブシステム	TCP 5000	IPCC Enterprise VRU CTI (ICM/IVR メッセージインターフェイス)	ランダム (Random)	双方向	CVP ICM サブシステム (コールサーバ) と Unified CCE/ICM VRU PG の間。ポートは設定可能。
Web サーバ : HTTP	TCP 80	音声ブラウザ	ランダム (Random)	双方向	音声ブラウザは、メディアサーバからメディアと「外部 VXML」ファイルを取得します。 このポートは、設定可能です。
Web サーバ : HTTPS	TCP 443	音声ブラウザ	ランダム (Random)	双方向	音声ブラウザは、メディアサーバからメディアと「外部 VXML」ファイルを取得します。 このポートは、設定可能です。

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
IBM Informix	TCP 1526	CVP Reporting Subsystem および CUIC	CUIC からランダム	双方向	データベース接続
IBM Informix Storage Manager	TCP 7939 ~ 7942 TCP 111	CVP Reporting Server		ローカル (Local)	IBM Informix Storage Manager サービス
IBM WAS コンソール	TCP 9043、9060	CVP Reporting Server	リモートデスクトップではランダム	双方向	
CVP Web Services Manager : HTTP	TCP 8101、8110、8111 TCP 10001、10002	Unified System CLI、診断ポータル、カスタムエージェントデスクトップ	ランダム (Random)	双方向	REST Web サービス TCP 10001 および 10002 OAMP ポートは、VXML サーバおよびコールサーバの設定および管理に関連するデータ転送に使用されません。

表 17: ネットワーク管理およびリモート管理

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
SNMP Master Agent	UDP 161	SNMP 管理アプリケーション	ランダム (Random)	双方向	SNMP マスターエージェントは、リモートの SNMP 管理アプリケーションからの要求をリッスンし、UDP ポート 161 で応答を送信します。

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
SNMP Master Agent	TCP 7161	ローカル SNMP サブエージェント		ローカル (Local)	SNMP マスター エージェントは、ローカル SNMP サブエージェントからの TCP 接続をリッスンします。
SNMP トラップ	UDP 162	SNMP Master Agent	ランダム (Random)	双方向	SNMP マスター エージェントは、SNMP 管理アプリケーションに SNMP トラップを送信します。
Syslog	UDP 514	Syslog 管理アプリケーションまたはサーバ	ランダム (Random)	双方向	syslog プロトコルは、マシンがイベント通知メッセージを IP ネットワーク経由でイベントメッセージコレクタに送信するためのトランスポートを提供します。ポートは設定可能。
SSH	TCP 22				ポート 22 は AIX に対して telnet ではなく SSH を使用するユーザ用。
Telnet	TCP 23				
RDP (Terminal Services)	TCP 3389	リモート デスクトップ	ランダム (Random)	双方向	

表 18: Windows 認証およびリモート管理ポート

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
RPC	TCP 135				
NetBIOS セッション	TCP 139				

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
NetBIOS 名前解決	TCP 137 UDP 137				
NetBIOS Netlogon/ブラウズ	UDP 138				
SMB	TCP 445 UDP 445				Microsoft CIFS
DNS	TCP 53 UDP 53				
optima-vnet	TCP 1051				TCP Optima VNET
optima-vnet	UDP 1051				UDP Optima VNET
NTP	UDP 123				

エフェメラルポートは、プログラムが任意の利用可能なユーザポートを要求するときにオペレーティングシステムによって作成される短時間有効なエンドポイントです。オペレーティングシステムは事前定義された範囲（通常は1024から65535）からポート番号を選択し、関連するTCP接続の終了後、ポートを解放します。

Windows 2012 で実行される UCCE コンポーネントの場合、エフェメラルポートの範囲は49152から65535であり、これは以下のコマンドを実行することによって確認できます。

- netsh int ipv4 show dynamicport tcp
- netsh int ipv6 show dynamicport tcp



(注)

- 範囲は、各トランスポートおよび IP の各バージョンに対して個別に設定されています。このポート範囲は、開始点と終了点のある実際の範囲です。Windows Server 2008 を実行しているサーバを展開するマイクロソフトのお客様が、内部ネットワークでファイアウォールを使用している場合、サーバ間の RPC 通信に問題が生じる可能性があります。このような場合、49152 から 65535 までの動的ポート範囲内のサーバ間のトラフィックを許可するように、ファイアウォールを再構成することをお勧めします。この範囲は、サービスおよびアプリケーションによって使用されるウェルノウンポートに追加されるものです。また、サーバによって使用されるポート範囲は、各サーバで変更することができます。この範囲を調整するには、netsh コマンドを使用します。
- Windows 認証およびリモート管理ポートの詳細については、『*Service overview and network port requirements for the Windows Server system*』（Microsoft サポート技術情報の記事 Q832017）を参照してください。
- Windows オペレーティング システムのポート要件の詳細については、<https://support.microsoft.com/en-us/help/832017/service-overview-and-network-port-requirements-for-windows> と <https://support.microsoft.com/en-us/help/929851/the-default-dynamic-port-range-for-tcp-ip-has-changed-in-windows-vista-and-in-windows-server-2008> を参照してください。



## 第 4 章

# Cisco VVB のポート使用状況

- [ポート使用状況表の列, 47 ページ](#)
- [Cisco VVB ポートの使用状況, 48 ページ](#)

## ポート使用状況表の列

このドキュメントに含まれるポート使用状況表の列について、次に説明します。

### リスナー（プロセスまたはアプリケーション プロトコル）

サーバまたはアプリケーションを表す値と、（必要に応じて）オープンまたは独自のアプリケーションプロトコル。

### リスナー プロトコルおよびポート

サーバまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### リモート デバイス（プロセスまたはアプリケーション プロトコル）

プロトコルで指定されるサーバまたはサービスに接続するリモート アプリケーションまたはデバイス、またはリモート プロトコルおよびポートでリッスンするリモート アプリケーションまたはデバイス。

### リモート プロトコルおよびポート

リモート サービスまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### トラフィックの方向

ポートを通過するトラフィックの流れる方向（着信、双方向、発信）。



(注) オペレーティングシステムは、ローカルアプリケーションまたはサービスがリモートデバイスの宛先ポートへの接続に使用する送信元ポートを動的に割り当てます。ほとんどの場合、このポートは、TCP/UDP 1024 より大きい番号でランダムに割り当てられます。

## Cisco VVB ポートの使用状況

表 19: Cisco VVB ポートの使用状況

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
VBONINIT	TCP 1504	HRC のような外部プロセス、WallBoard クライアント、外部 DB クライアント（カスタム レポート用の Squirrel など）が接続できます。	—	双方向	Cisco VVB データベースポート
VVB_Engine	TCP、UDP 5060	SIP ゲートウェイ	—	双方向	SIP ゲートウェイと通信
VVB_CVD	TCP 5900	クラスタ内の他のノードの CVD	—	双方向	クラスタの CVD 間のハートビート
VVB_CVD	TCP 6161	内線	6161	双方向	クラスタ内の JMS ネットワーク コネクタ経由で JMS イベントを公開
CVD	TCP 6295	クラスタ内の他のノードの CVD	—	双方向	ブートストラップ HTTPD サービスポート
VVB_CVD	TCP 6999	エンジン、Tomcat、CVD、エディタ	—	双方向	RMIポート（RMI Port）



リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
VVB_Engine	TCP 9080	—	—	双方向	- HTTP トリガー、ドキュメント、プロンプト、または文法へのアクセスを試行するクライアント - Cisco VVB エンジンが使用する Tomcat インスタンス
Cisco IP Voice Media Streaming Application	UDP 24576～32767	—	—	双方向	- 音声メディアのストリーミング。 - カーネルストリーミングデバイスドライバ
汎用ポート	TCP、UDP 32768～61000	—	—	双方向	汎用エフェメラル TCP および UDP ポート





## 第 5 章

# Finesse のポート使用状況

- [ポート使用状況表の列, 51 ページ](#)
- [Finesse のポート使用状況, 52 ページ](#)

## ポート使用状況表の列

このドキュメントに含まれるポート使用状況表の列について、次に説明します。

### リスナー（プロセスまたはアプリケーション プロトコル）

サーバまたはアプリケーションを表す値と、（必要に応じて）オープンまたは独自のアプリケーション プロトコル。

### リスナー プロトコルおよびポート

サーバまたはアプリケーションがリスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### リモート デバイス（プロセスまたはアプリケーション プロトコル）

プロトコルで指定されるサーバまたはサービスに接続するリモート アプリケーションまたはデバイス、またはリモート プロトコルおよびポートでリスンするリモート アプリケーションまたはデバイス。

### リモート プロトコルおよびポート

リモート サービスまたはアプリケーションがリスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### トラフィックの方向

ポートを通過するトラフィックの流れる方向（着信、双方向、発信）。



(注) オペレーティング システムは、ローカルアプリケーションまたはサービスがリモートデバイスの宛先ポートへの接続に使用する送信元ポートを動的に割り当てます。ほとんどの場合、このポートは、TCP/UDP 1024 より大きい番号でランダムに割り当てられます。

## Finesse のポート使用状況

表 20 : Cisco Finesse Tomcat

リスナー (プロセスまたはアプリケーション プロトコル)	リスナー プロトコルおよびポート	リモート デバイス (プロセスまたはアプリケーション プロトコル)	リモート プロトコルおよびポート	トラフィックの方向	注記
HTTP	TCP 80、8082	ブラウザ		双方向	Finesse 管理コンソール、Finesse エージェントおよびスーパーバイザ デスクトップ、Finesse Web サービス、および Finesse デスクトップの Finesse デスクトップ モジュール (ガジェット) に使用するセキュアでないポート。
HTTPS	TCP 443、8445	ブラウザ		双方向	Finesse 管理コンソール、Finesse エージェントおよびスーパーバイザ デスクトップ、Finesse Web サービス、および Finesse デスクトップの Finesse デスクトップ モジュール (ガジェット) に使用するセキュアなポート。

表 21 : Cisco Finesse Notification Service

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
XMPP	TCP 5222	ブラウザ、エージェントデスクトップ		双方向	HTTP 通信で使用する Finesse サーバと、エージェントまたはスーパーバイザデスクトップ上のカスタムアプリケーションとの間のセキュアでない XMPP 接続。
XMPP	TCP 5223	ブラウザ、エージェントデスクトップ		双方向	HTTPS 通信で使用する Finesse サーバと、エージェントまたはスーパーバイザデスクトップ上のカスタムアプリケーションとの間のセキュアな XMPP 接続。
BOSH (HTTP)	TCP 7071	ブラウザ、エージェントデスクトップ		双方向	HTTP 通信で使用する、Finesse サーバとエージェントおよびスーパーバイザデスクトップ間のセキュアでない BOSH 接続。
BOSH (HTTPS)	TCP 7443	ブラウザ、エージェントデスクトップ		双方向	HTTPS を介した通信で使用する、Finesse サーバとエージェントおよびスーパーバイザデスクトップ間のセキュアな BOSH 接続。

表 22: プライマリおよびセカンダリノード通信

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
XMPP	TCP 5222			双方向	プライマリおよびセカンダリの Finesse サーバでは、この XMPP 接続を使用して互いに通信し、接続をモニタします。

表 23: サードパーティ（外部）Web サーバ

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
HTTP			TCP 80、8082	双方向	サードパーティ（外部）Web サーバでホストされたガジェットは、前述の Web サーバによって公開されるポートの Finesse サーバから取得されます。
HTTPS			TCP 443、8445	双方向	サードパーティ（外部）Web サーバでホストされたガジェットは、前述の Web サーバによって公開されるポートの Finesse サーバから取得されます。

表 24 : Unified Contact Center Enterprise

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
管理およびデータ サーバの設定					
JDBC (SQL)			TCP 1433 <sup>1</sup>	双方向	エージェントとスーパーバイザの認証と認可のための AWDB への接続
CTI サーバの設定（A 側および B 側）					
GED-188			A 側 : TCP 42027 <sup>1</sup> B 側 : TCP 43027 <sup>1</sup>	双方向	CTI サーバイベント（エージェント、チーム、キュー、コールイベントなど）のための Agent PG への接続

<sup>1</sup> 一覧のポートはこれらの接続のデフォルトポートです。この表で指定されているポートとは異なるポートも使用できます。







## 第 6 章

# MediaSense のポート使用状況

- [ポート使用状況表の列, 57 ページ](#)
- [MediaSense のポート使用状況, 58 ページ](#)

## ポート使用状況表の列

このドキュメントに含まれるポート使用状況表の列について、次に説明します。

### リスナー（プロセスまたはアプリケーション プロトコル）

サーバまたはアプリケーションを表す値と、（必要に応じて）オープンまたは独自のアプリケーションプロトコル。

### リスナー プロトコルおよびポート

サーバまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### リモート デバイス（プロセスまたはアプリケーション プロトコル）

プロトコルで指定されるサーバまたはサービスに接続するリモート アプリケーションまたはデバイス、またはリモート プロトコルおよびポートでリッスンするリモート アプリケーションまたはデバイス。

### リモート プロトコルおよびポート

リモート サービスまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### トラフィックの方向

ポートを通過するトラフィックの流れる方向（着信、双方向、発信）。



(注) オペレーティング システムは、ローカルアプリケーションまたはサービスがリモートデバイスの宛先ポートへの接続に使用する送信元ポートを動的に割り当てます。ほとんどの場合、このポートは、TCP/UDP 1024 より大きい番号でランダムに割り当てられます。

## MediaSense のポート使用状況

表 25: MediaSense のポート使用状況

リスナー (プロセスまたはアプリケーション プロトコル)	リスナー プロトコルおよびポート	リモート デバイス (プロセスまたはアプリケーション プロトコル)	リモート プロトコルおよびポート	トラフィックの方向	コメント
HTTPS	TCP 443、8443	Web ブラウザ	任意 (Any)		管理、サービスアビリティで使用
HTTPS	TCP 8440	クライアント アプリケーション	任意 (Any)		API アクセスで使用
HTTPS	TCP 9443	クライアント アプリケーション	任意 (Any)		認証された要求をリダイレクトするためにメディア デバイスによって使用される。
HTTPS	TCP 8446	Web ブラウザ、API クライアント	任意 (Any)		コール制御サービスで使用。
HTTPS	TCP 9081	クライアント アプリケーション	任意 (Any)		認証された要求をリダイレクトするためにメディア デバイスによって使用される。
HTTP	TCP 80、8080	Web ブラウザ	任意 (Any)		管理、サービスアビリティで使用
HTTP	TCP 8081	Web ブラウザ、API クライアント	任意 (Any)		コール制御サービスで使用
HTTP	TCP 8085	別の CMS のノード	任意 (Any)		コール制御サービスで使用
HTTP	TCP 8087	CMS クラスター ノードのみ	任意 (Any)		システム サービスで使用

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	コメント
HTTP	TCP 8088	CMS クラスタ ノードのみ	任意 (Any)		コンフィギュレーションサービスで使用
RTSP	TCP 554、8554	RTSP メディア プレーヤー	任意 (Any)		SM エージェントで使用
RTSP	TCP 9554	クライアントアプリケーションまたはメディアプレーヤー	任意 (Any)		認証された要求をリダイレクトするためにメディアデバイスによって使用される。
SIP	TCP 5060 UDP 5060	Unified Communications Manager または Unified Border Element	TCP 5060 UDP 5060		コール制御サービス。
TCP/IP	TCP 1543	CMS クラスタ ノードのみ	任意 (Any)		プライマリ サーバとセカンダリ サーバ間の接続を確立するために Informix ER によって使用される。  JDBC を Informix と接続するために API サービスまたはコンフィギュレーションサービスによって使用される。
キープアライブハートビート	UDP 8091	CMS クラスタ ノードのみ	UDP 8091		他のコール制御サービスのアベイラビリティを検出するためにコール制御サービスによって使用される。
JMS	TCP 61610	CMS クラスタ ノードのみ	任意 (Any)		API サービスで使用
JMS	TCP 61612	CMS クラスタ ノードのみ	任意 (Any)		コール制御サービスで使用
JMS	TCP 61616	CMS クラスタ ノードのみ	任意 (Any)		SM エージェントで使用
エフェメラルポート範囲	UDP 32768 および 61000	RTP メディア ストリームを送信する電話機またはゲートウェイ。	任意 (Any)		RTP メディア ストリームを受信するためにメディアサービスによって使用されるポート範囲。





## 第 7 章

# SocialMiner のポート使用状況

- [ポート使用状況表の列, 61 ページ](#)
- [SocialMiner のポート使用状況, 62 ページ](#)

## ポート使用状況表の列

このドキュメントに含まれるポート使用状況表の列について、次に説明します。

### リスナー（プロセスまたはアプリケーション プロトコル）

サーバまたはアプリケーションを表す値と、（必要に応じて）オープンまたは独自のアプリケーションプロトコル。

### リスナー プロトコルおよびポート

サーバまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### リモート デバイス（プロセスまたはアプリケーション プロトコル）

プロトコルで指定されるサーバまたはサービスに接続するリモート アプリケーションまたはデバイス、またはリモート プロトコルおよびポートでリッスンするリモート アプリケーションまたはデバイス。

### リモート プロトコルおよびポート

リモート サービスまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### トラフィックの方向

ポートを通過するトラフィックの流れる方向（着信、双方向、発信）。



(注) オペレーティング システムは、ローカルアプリケーションまたはサービスがリモートデバイスの宛先ポートへの接続に使用する送信元ポートを動的に割り当てます。ほとんどの場合、このポートは、TCP/UDP 1024 より大きい番号でランダムに割り当てられます。

## SocialMiner のポート使用状況

表 26 : SocialMiner のポート使用状況

リスナー（プロセスまたはアプリケーションプロトコル）	リスナー プロトコルおよびポート	リモート デバイス（プロセスまたはアプリケーションプロトコル）	リモート プロトコルおよびポート	トラフィックの方向	注記
電子メール通知	—	—	ポート 25	外方向 (SocialMiner から設定済みの電子メールサーバへ)。	SocialMiner は、電子メール通知を送信するために（企業イントラネット内またはインターネット上の）設定済みの電子メールサーバと通信します。

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
HTTP	ポート 80	—	—	双方向	<p>次のセキュアでない（HTTP）トラフィックで使用。</p> <ul style="list-style-type: none"> <li>• UCCX サーバから SocialMiner サーバへ。</li> <li>• SocialMiner ユーザーインターフェイス（ブラウザ）または API から SocialMiner サーバへ。</li> <li>• SocialMiner サーバからインターネットへ。SocialMiner は、HTTP 経由でソーシャルコンタクト情報（Facebook 投稿やツイートなど）を取得するために外部のインターネットに向けて通信します。</li> <li>• インターネットまたは企業 Web サイトから SocialMiner サーバへ。SocialMiner は、HTTP 経由でインターネットまたは企業 Web サイトから着信するチャットおよびコールバックの要求を受信します。</li> </ul>

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
HTTPS	ポート 443	—	—	双方向	<p>次のセキュア（HTTPS）トラフィックで使用。</p> <ul style="list-style-type: none"> <li>• SocialMiner ユーザインターフェイス（ブラウザ）または API から SocialMiner サーバへ。</li> <li>• SocialMiner サーバからインターネットへ。SocialMiner は、HTTPS 経由でソーシャルコンタクト情報（Facebook 投稿やツイートなど）を取得するために外部のインターネットに向けて通信します。</li> <li>• インターネットまたは企業 Web サイトから SocialMiner サーバへ。SocialMiner は、HTTPS 経由でインターネットまたは企業 Web サイトから着信するチャットおよびコールバックの要求を受信します。</li> </ul>
電子メール通知の SSL/TLS	—	—	ポート 465（設定可能）	外方向（SocialMiner から設定済みの電子メールサーバへ）。	SocialMiner は、電子メール通知を送信するために（企業イントラネット内またはインターネット上の）設定済みの電子メールサーバと通信します。



リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
電子メール（SMTP）	—	—	ポート 587（Unified CCX Administration で設定可能）	外方向（SocialMiner から Exchange Server へ）。	電子メール返信 API で電子メールを送信するために使用。 電子メール返信 API は、SMTP を使用して顧客の電子メールメッセージへの応答を送信します。
電子メール（セキュア IMAP/IMAPS）	—	—	ポート 993（Unified CCX Administration で設定可能）	外方向（SocialMiner から Exchange Server へ）。	電子メールフィードで電子メールを取得するために使用。 IMAPS を使用すると、電子メールフィードで Exchange Server から電子メールを取得したり、電子メール返信 API で電子メールを取得したり、電子メールメッセージの下書きを保存したりできます。
レポート	ポート 1526	—	—	内方向（CUIC から SocialMiner サーバへ）。	CUIC は、レポート情報を収集するために SocialMiner と通信します。
Active Directory	ポート 3268（設定可能）	—	—	外方向（SocialMiner から設定済みの Active Directory ホストへ）	SocialMiner は、セキュアでない Active Directory 接続のために、外部の設定済みの Active Directory ホストに向けて通信します。
Active Directory SSL	ポート 3269（設定可能）	—	—	外方向（SocialMiner から設定済みの Active Directory ホストへ）	SocialMiner は、セキュアな Active Directory 接続のために、外部の設定済みの Active Directory ホストに向けて通信します。

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
外部の XMPP サーバを使用する XMPP (IM) 通知		—	ポート 5222 (設定可能)	外方向 (SocialMiner から設定済みの XMPP 通知サーバへ)。	SocialMiner は、XMPP (IM) 通知を送信するために (企業イントラネット内またはインターネット上の) 設定済みの XMPP 通知サーバと通信します。
通知サービス (TCP ソケット経由の XMPP イベント処理)	ポート 5222	—	—	内方向 (CCX から SocialMiner サーバへ)。	SocialMiner は、XMPP イベントを登録して送信するために着信 TCP ソケット接続をリッスンします。Unified CCX は、このポートを使用してソーシャルコンタクトイベントを受信します。
イベント処理およびチャット (BOSH)	ポート 7071	—	—	双方向	セキュアでない BOSH 接続は、SocialMiner ユーザーインターフェイスと SocialMiner サーバ間のイベント処理とチャット通信をサポートします。
イベント処理およびチャット (セキュア BOSH)	ポート 7443 は、XMPP イベント処理サーバへのセキュア BOSH 接続に使用されます。	—	—	双方向	セキュアな BOSH 接続は、SocialMiner ユーザーインターフェイスと SocialMiner サーバ間のイベント処理とチャット通信をサポートします。
メディアルーティング (CCE 展開で)	ポート 38001 (設定可能)			内方向 (CCE MR PG から SocialMiner サーバへ)。	CCE Media Routing Peripheral Gateway (MR PG) は、メディアルーティング接続をサポートするために、ソケット接続を介して SocialMiner と通信します。



## 第 8 章

# Unified Intelligence Center のポート使用状況

- [ポート使用状況表の列, 67 ページ](#)
- [Unified Intelligence Center のポート使用状況, 68 ページ](#)

## ポート使用状況表の列

このドキュメントに含まれるポート使用状況表の列について、次に説明します。

### リスナー（プロセスまたはアプリケーション プロトコル）

サーバまたはアプリケーションを表す値と、（必要に応じて）オープンまたは独自のアプリケーションプロトコル。

### リスナー プロトコルおよびポート

サーバまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### リモート デバイス（プロセスまたはアプリケーション プロトコル）

プロトコルで指定されるサーバまたはサービスに接続するリモート アプリケーションまたはデバイス、またはリモート プロトコルおよびポートでリッスンするリモート アプリケーションまたはデバイス。

### リモート プロトコルおよびポート

リモート サービスまたはアプリケーションがリッスンしている TCP または UDP ポートの ID と、サーバとして動作している場合の着信接続要求の IP アドレス。

### トラフィックの方向

ポートを通過するトラフィックの流れる方向（着信、双方向、発信）。



(注) オペレーティングシステムは、ローカルアプリケーションまたはサービスがリモートデバイスの宛先ポートへの接続に使用する送信元ポートを動的に割り当てます。ほとんどの場合、このポートは、TCP/UDP 1024 より大きい番号でランダムに割り当てられます。

## Unified Intelligence Center のポート使用状況

表 27 : Cisco Unified Intelligence Center と Operation Administration Maintenance and Provisioning (OAMP) への Web 要求

リスナー (プロセスまたはアプリケーションプロトコル)	リスナー プロトコルおよびポート	リモートデバイス (プロセスまたはアプリケーションプロトコル)	リモートプロトコルおよびポート	トラフィックの方向	注記
Unified Intelligence Center	TCP 8081	ブラウザ			HTTP - Unified Intelligence Center
	TCP 8444	ブラウザ			HTTPS - Unified Intelligence Center
OAMP	TCP 8080	ブラウザ			HTTP - OAMP
	TCP 8443	ブラウザ			HTTPS - OAMP

表 28 : Cisco Unified Intelligence Center とライブデータ

リスナー (プロセスまたはアプリケーションプロトコル)	リスナー プロトコルおよびポート	リモートデバイス (プロセスまたはアプリケーションプロトコル)	リモートプロトコルおよびポート	トラフィックの方向	注記
Storm DRPC サービス	TCP 3772				ライブデータ DRPC ポート
	TCP 3773				ライブデータ DRPC 呼び出しポート

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
CCE ライブデータ Cassandra サービス	TCP 12000				ライブデータ Cassandra のコマンドおよびデータ用 TCP ポート
	TCP 12001				ライブデータ Cassandra の暗号化通信用 SSL ポート。 (暗号化オプションで有効にしないかぎり未使用)
	TCP 9160				Thrift がクライアントをリスンするのに使用するライブデータ Cassandra ポート
CCE ライブデータ Zookeeper サービス	TCP 2181				ライブデータ レポート
CCE ライブデータ ActiveMQ サービス	TCP 12002				ActiveMQ JMX コネクタ ポート
	TCP 12003				ActiveMQ JMX rmi ポート
CCE ライブデータ Web サービス	TCP 12004、 12006				ライブデータ レポート
CCE ライブデータ ActiveMQ サービス	TCP 61616				ライブデータ ActiveMQ Openwire トランスポート コネクタ ポート
	TCP 61612				ライブデータ ActiveMQ Stomp トランスポート コネクタ ポート
CCE ライブデータ Storm Nimbus サービス	TCP 6627				ライブデータ Nimbus Thrift ポート

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
CCE ライブデータ Socket.IO サービス	TCP 12007、 12008				ライブデータ Socket.IO リスニング ポート

表 29 : Cisco Unified Intelligence Center 間のクラスタ内ポート

リスナー（プロセスまたはアプリケーションプロトコル）	リスナープロトコルおよびポート	リモートデバイス（プロセスまたはアプリケーションプロトコル）	リモートプロトコルおよびポート	トラフィックの方向	注記
プラットフォーム (DB)	TCP 1500、 1501	プラットフォーム (DB)			IDSのアクセスとレプリケーション（ただし、外部アクセスには非公開）
プラットフォーム (Tomcat)	TCP/5001				リアルタイム モニタリングサービスの SOAP モニタ
プラットフォーム (Tomcat)	TCP/5002				パフォーマンス モニタ サービスの SOAP モニタ
プラットフォーム (Tomcat)	TCP/5003				コントロールセンターサービスの SOAP モニタ
CUIC のレポート プロセス	UDP 54327 (マルチキャスト)	Unified Intelligence Center ノード			Hazelcast Discovery
CUIC のレポート プロセス	TCP 57011	Unified Intelligence Center ノード			Hazelcast

その他のポート利用状況の詳細については、次を参照してください。 <http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>

