Cisco Unity Connection セキュリティ ガイド

リリース 8.x
改訂：2011 年 8 月

【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/）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。

Cisco Unity Connection セキュリティ ガイド 8.x

CONTENTS

はじめに

対象読者および使用

『*Cisco Unity Connection セキュリティ ガイド*』には、Cisco Unity Connection システムのセキュリティに関する情報が記載されています。このガイドの各章では、セキュリティに関する潜在的な問題について説明し、とるべき対策に関する情報、意思決定に役立つ推奨事項、下した決定の効果に関する情報、およびベストプラクティスを紹介します。

表記法

表 1　　『*Cisco Unity Connection セキュリティ ガイド*』の表記法

表記法	説明
太字	次の場合は太字を使用します。 • ユーザが入力する情報。（例：[ユーザ名（User Name）] ボックスに **Administrator** と入力します）。
< > （山カッコ）	ユーザが値を指定するパラメータを囲むために使用します。（例：ブラウザで、**https://<Cisco Unity Connection サーバの IP アドレス>/cuadmin** に移動します）。
- （ハイフン）	同時に押す必要があるキーを表します。（例：Ctrl-Alt-Delete を押します）。
> （右向きの山カッコ）	Cisco Unity Connection Administration のナビゲーション バーで選択する順序を表します。（例：Cisco Unity Connection Administration で、[連絡先（Contacts）] > [システム連絡先（System Contacts）] を展開します）。

『*Cisco Unity Connection セキュリティ ガイド*』では、次の表記法も使用します。

（注）　「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

注意　「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

Cisco Unity Connection のマニュアル

Cisco.com 上の Cisco Unity Connection に関するマニュアルの説明と URL については、『*Documentation Guide for Cisco Unity Connection*』*Release 8.x* を参照してください。このドキュメントは Connection に同梱されていますが、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/roadmap/8xcucdg.html から入手することもできます。

Cisco Unified Communications Manager Business Edition に関するマニュアル リファレンス

この製品は、バージョン 8.0 以前では Cisco Unified Communications Manager Business Edition という名称ですが、バージョン 8.5 以降では Cisco Unified Communications Manager Business Edition 5000 に変更されています。

『Cisco Unity Connection 8.x』マニュアル セットの Cisco Unified Communications Manager Business Edition および Cisco Unified CMBE に関するリファレンスは、Business Edition バージョン 8.0 および Business Edition 5000 バージョン 8.5 以降の両方に適用されます。ただし Business Edition 6000 には適用されません。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は 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がデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

シスコ製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、http://www.access.gpo.gov/bis/ear/ear_data.html で参照できます。

CHAPTER 1

Cisco Unity Connection 8.x で必要な IP 通信

次の項を参照してください。

Cisco Unity Connection 8.x のサービス ポート

表 1-1 は、Cisco Unity Connection サーバへのインバウンド接続に使用される TCP ポートと UDP ポート、および Connection によって内部的に使用されるポートを示しています。

表 1-1　Cisco Unity Connection サーバへのインバウンド接続に使用される TCP ポートおよび UDP ポート

ポートおよびプロトコル[1]	オペレーティング システムのファイアウォール設定	実行可能ファイル / サービスまたはアプリケーション	サービス アカウント	コメント
TCP：20500、20501、20502、19003	Connection クラスタ内のサーバ間でだけ開かれる	CuCsMgr/Connection Conversation Manager	cucsmgr	Connection クラスタ内のサーバは、これらのポート上で互いに接続できる必要があります。
TCP：**21000 ～ 21512**	開かれる	CuCsMgr/Connection Conversation Manager	cucsmgr	IP 電話は、一部の電話クライアント アプリケーション用に、Connection サーバ上のこの範囲のポートに接続できる必要があります。
TCP：**5000**	開かれる	CuCsMgr/Connection Conversation Manager	cucsmgr	ポートステータス モニタリングの読み取り専用接続のために開かれます。このポート上でデータを確認するには、事前に Connection の管理 でモニタリングを設定する必要があります（デフォルトではモニタリングがオフになります）。 管理ワークステーションはこのポートに接続します。

表 1-1　Cisco Unity Connection サーバへのインバウンド接続に使用される TCP ポートおよび UDP ポート（続き）

ポートおよびプロトコル[1]	オペレーティング システムのファイアウォール設定	実行可能ファイル/サービスまたはアプリケーション	サービス アカウント	コメント
管理者によって SIP トラフィック用に割り当てられた TCP ポートおよび UDP ポート 例：**5060 ～ 5100**	開かれる	CuCsMgr/Connection Conversation Manager	cucsmgr	Conversation Manager によって処理される Connection SIP コントロール トラフィックです。 SIP デバイスはこれらのポートに接続できる必要があります。
TCP：20055	Connection クラスタ内のサーバ間でだけ開かれる	CuLicSvr/Connection ライセンス サーバ	culic	localhost だけに制限されます（このサービスへのリモート接続は不要です）。
TCP：1502、1503（/etc/services の「ciscounity_tcp」）	Connection クラスタ内のサーバ間でだけ開かれる	unityoninit/Connection DB	root	Connection クラスタ内のサーバは、これらのデータベース ポート上で互いに接続できる必要があります。 データベースへの外部アクセスには、CuDBProxy を使用します。
TCP：**143、993、7993、8143、8993**	開かれる	CuImapSvr/Connection IMAP サーバ	cuimapsvr	クライアント ワークステーションは、IMAP Inbox アクセスおよび IMAP over SSL Inbox アクセス用に 143 ポートおよび 993 ポートに接続できる必要があります。
TCP：**25、8025**	開かれる	CuSmtpSvr/Connection SMTP サーバ	cusmtpsvr	Connection ポート 25 に SMTP を配信するサーバです。たとえば、UC デジタル ネットワーク内の他のサーバなどです。
TCP：4904	ブロックされる（内部使用のみ）	SWIsvcMon（Nuance SpeechWorks Service Monitor）	openspeech	localhost だけに制限されます（このサービスへのリモート接続は不要です）。
TCP：4900:4904	ブロックされる（内部使用のみ）	OSServer/Connection Voice Recognizer	openspeech	localhost だけに制限されます（このサービスへのリモート接続は不要です）。
UDP：**16384 ～ 21511**	開かれる	CuMixer/Connection Mixer	cumixer	VoIP デバイス（電話およびゲートウェイ）は、これらの UDP ポートにトラフィックを送信してインバウンド オーディオ ストリームを配信できる必要があります。
UDP：7774 ～ 7900	ブロックされる（内部使用のみ）	CuMixer/ Speech recognition RTP	cumixer	localhost だけに制限されます（このサービスへのリモート接続は不要です）。
TCP：22000 UDP：22000	Connection クラスタ内のサーバ間でだけ開かれる	CuSrm/ Connection サーバ ロール マネージャ	cusrm	クラスタ SRM RPC です。 Connection クラスタ内のサーバは、これらのポート上で互いに接続できる必要があります。

表 1-1　Cisco Unity Connection サーバへのインバウンド接続に使用される TCP ポートおよび UDP ポート（続き）

ポートおよびプロトコル[1]	オペレーティング システムのファイアウォール設定	実行可能ファイル / サービスまたはアプリケーション	サービス アカウント	コメント
TCP：22001 UDP：22001	Connection クラスタ内のサーバ間でだけ開かれる	CuSrm/ Connection サーバ ロール マネージャ	cusrm	クラスタ SRM ハートビートです。 ハートビート イベント トラフィックは暗号化されませんが、MAC でセキュリティ保護されます。 Connection クラスタ内のサーバは、これらのポート上で互いに接続できる必要があります。
TCP：**20532**	開かれる	CuDbProxy/ Connection データベース プロキシ	cudbproxy	このサービスが有効化されている場合、オフボックス クライアントは、管理目的でデータベースへの読み取り / 書き込み接続を行うことができます。たとえば、一部の ciscounitytools.com ツールはこのポートを使用します。 管理ワークステーションはこのポートに接続します。
TCP：**22**	開かれる	Sshd	root	リモート CLI アクセス用の TCP 22 接続、および Connection クラスタでの SFTP 対応のため、ファイアウォールが開かれている必要があります。 管理ワークステーションは、このポート上で Connection サーバに接続できる必要があります。 Connection クラスタ内のサーバは、このポート上で互いに接続できる必要があります。
UDP：**161**	開かれる	Snmpd Platform SNMP Service	root	—
UDP：**500**	開かれる	Raccoon ipsec isakmp（キー管理）サービス	root	ipsec の使用はオプションです。デフォルトではオフになります。 このサービスが有効になっている場合、Connection クラスタ内のサーバは、このポート上で互いに接続できる必要があります。
TCP：**8500** UDP：**8500**	開かれる	clm/ クラスタ管理サービス	root	クラスタ管理サービスは、Voice Operating System の一部です。 Connection クラスタ内のサーバは、これらのポート上で互いに接続できる必要があります。

表 1-1　Cisco Unity Connection サーバへのインバウンド接続に使用される TCP ポートおよび UDP ポート（続き）

ポートおよびプロトコル[1]	オペレーティング システムのファイアウォール設定	実行可能ファイル/サービスまたはアプリケーション	サービス アカウント	コメント
UDP：**123**	開かれる	Ntpd Network Time Service	ntp	Connection クラスタ内のサーバ間で時刻の同期を維持するため、ネットワーク時刻サービスが有効化されます。 パブリッシャ サーバは、パブリッシャ サーバのオペレーティング システムの時刻を使用することも、別の NTP サーバの時刻を使用して同期することもできます。サブスクライバ サーバは、常にパブリッシャ サーバの時刻と同期します。 Connection クラスタ内のサーバは、このポート上で互いに接続できる必要があります。
TCP：5007	開かれる	Tomcat/Cisco Tomcat（SOAP Service）	tomcat	Connection クラスタ内のサーバは、これらのポート上で互いに接続できる必要があります。
TCP：1500、1501	Connection クラスタ内のサーバ間でだけ開かれる	cmoninit/Cisco DB	informix	これらのデータベース インスタンスには、LDAP 統合ユーザの情報とサービスアビリティ データが含まれています。 Connection クラスタ内のサーバは、これらのポート上で互いに接続できる必要があります。
TCP：1515	Connection クラスタ内のサーバ間でだけ開かれる	dblrpm/Cisco DB Replication Service	root	Connection クラスタ内のサーバは、これらのポート上で互いに接続できる必要があります。
TCP：8001	Connection クラスタ内のサーバ間でだけ開かれる	dbmon/Cisco DB Change Notification Port	データベース	Connection クラスタ内のサーバは、これらのポート上で互いに接続できる必要があります。
TCP：2555、2556	Connection クラスタ内のサーバ間でだけ開かれる	RisDC/Cisco RIS Data Collector	ccmservice	Connection クラスタ内のサーバは、これらのポート上で互いに接続できる必要があります。
TCP：1090、1099	Connection クラスタ内のサーバ間でだけ開かれる	Amc/Cisco AMC Service（Alert Manager Collector）	ccmservice	バックエンドのサービスアビリティ データの交換を実行します。 1090：AMC RMI オブジェクト ポート 1099：AMC RMI レジストリ ポート Connection クラスタ内のサーバは、これらのポート上で互いに接続できる必要があります。

表 1-1　Cisco Unity Connection サーバへのインバウンド接続に使用される TCP ポートおよび UDP ポート（続き）

ポートおよびプロトコル[1]	オペレーティングシステムのファイアウォール設定	実行可能ファイル/サービスまたはアプリケーション	サービス アカウント	コメント
TCP：**80**、**443**、**8080**、**8443**	開かれる	tomcat/Cisco Tomcat	tomcat	クライアント ワークステーションと管理ワークステーションの両方が、これらのポートに接続する必要があります。 Connection クラスタ内のサーバは、HTTP ベースの対話（REST など）を使用する通信のために、これらのポート上で互いに接続できる必要があります。
TCP：5001、8005	ブロックされる（内部使用のみ）	tomcat/Cisco Tomcat	tomcat	内部の tomcat サービス コントロールおよび axis ポートです。
TCP：**32768** ～ **61000** UDP：**32768** ～ **61000**	開かれる	—	—	動的に割り当てられたクライアント ポートを持つものが使用する、エフェメラルなポート範囲です。
TCP：7080	開かれる	jetty/Connection Jetty	jetty	*Exchange 2007 および Exchange 2010 のみ、単一受信トレイのみ。：*Connection ボイス メッセージの変更に関する EWS 通知です。
UDP：9291	開かれる	CuMbxSync/ Connection Mailbox Sync Service	cumbxsync	*Exchange 2003 のみ、単一受信トレイのみ。：*Connection ボイス メッセージの変更に関する WebDAV 通知です。

1. 太字で示されているポート番号は、オフボックス クライアントからの直接接続のために開かれています。

Cisco Unity Connection 8.x サーバが行うアウトバウンド接続

表 1-2 は、ネットワーク内の他のサーバとの接続のために Cisco Unity Connection によって使用される TCP ポートおよび UDP ポートを示しています。

表 1-2　ネットワーク内の他のサーバとの接続のために Cisco Unity Connection によって使用される TCP ポートおよび UDP ポート

ポートおよびプロトコル	実行可能ファイル	サービス アカウント	コメント
TCP：2000*（デフォルトの SCCP ポート） SCCP over TLS を使用する場合は TCP ポート 2443*（オプション）。 * 多くのデバイスおよびアプリケーションでは、設定可能な RTP ポート割り当てが許可されます。	cucsmgr	cucsmgr	Cisco Unified CM への Connection SCCP クライアント接続です（SCCP を使用して連動する場合）。
UDP：16384 ～ 32767*（RTP） * 多くのデバイスおよびアプリケーションでは、設定可能な RTP ポート割り当てが許可されます。	cumixer	cumixer	Connection のアウトバウンド オーディオ ストリーム トラフィックです。
UDP：69	cucsmgr	cucsmgr	暗号化された SCCP、暗号化された SIP、または暗号化されたメディア ストリームを設定するときには、Connection で Cisco Unified CM への TFTP クライアント接続が行われて、セキュリティ証明書がダウンロードされます。
TCP：53 UDP：53	任意	任意	DNS 名前解決の実行が必要なプロセスで使用されます。
TCP：53、および 389 または 636	CuMbxSync cucsmgr tomcat	cumbxsync cucsmgr tomcat	Exchange でのユニファイド メッセージングに Connection が設定されている場合、および Exchange サーバの検索のために 1 つまたは複数のユニファイド メッセージング サービスが設定されている場合に使用されます。 ドメイン コントローラとの通信に使用するプロトコルに LDAP を選択した場合、Connection はポート 389 を使用します。 ドメイン コントローラとの通信に使用するプロトコルに LDAPS を選択した場合、Connection はポート 636 を使用します。
TCP：80、443（HTTP および HTTPS）	CuMbxSync cucsmgr tomcat	cumbxsync cucsmgr tomcat	Connection は、外部サービスとの通信（Connection 8.0）またはユニファイド メッセージング（8.5 以降）のために、他のサーバへの HTTP および HTTPS クライアント接続を行います。たとえば、単一受信トレイと予定表の統合のための Microsoft Exchange への接続などがあります。

表 1-2　ネットワーク内の他のサーバとの接続のために Cisco Unity Connection によって使用される TCP ポートおよび UDP ポート（続き）

ポートおよびプロトコル	実行可能ファイル	サービス アカウント	コメント
TCP：80、8080、443、および 8443（HTTP および HTTPS）	cucsmgr tomcat	cucsmgr tomcat	Connection では、次の HTTP および HTTPS クライアント接続が行われます。 • デジタル ネットワーキング自動参加のための、他の Connection サーバへの接続。 • AXL ユーザ同期のための、Cisco Unified CM への接続。
TCP：143、993（IMAP および IMAP over SSL）	cucsmgr	cucsmgr	Connection は、Connection ユーザの Exchange メールボックスで電子メール メッセージの音声合成変換を実行するために、Microsoft Exchange サーバへの IMAP 接続を行います。
TCP：25（SMTP）	cusmtpsvr	cusmtpsvr	Connection は、VPIM ネットワーキングや Connection デジタル ネットワーキングなどの機能のために、SMTP サーバおよびスマート ホスト、または他の Connection サーバへのクライアント接続を行います。
TCP：21（FTP）	FTP	root	インストール フレームワークは、FTP サーバが指定されると、FTP 接続を行ってアップグレード メディアをダウンロードします。
TCP：22（SSH/SFTP）	CiscoDRFMaster sftp	drf root	ディザスタ リカバリ フレームワークは、ネットワーク バックアップ サーバへの SFTP 接続を行って、バックアップを実行したり、復元のためにバックアップを取得したりします。 インストール フレームワークは、SFTP サーバが指定されると、SFTP 接続を行ってアップグレード メディアをダウンロードします。
UDP：67（DHCP/BootP）	dhclient	root	DHCP アドレッシングを取得するためのクライアント接続です。 DHCP はサポートされていますが、固定 IP アドレスを Connection サーバに割り当てることを強く推奨します。
TCP：123 UDP：123（NTP）	Ntpd	root	NTP クロック同期のためのクライアント接続です。

CHAPTER 2

Cisco Unity Connection 8.x での不正通話の防止

この章では、あらゆる組織においてセキュリティ上の問題となる可能性がある、不正通話について説明します。また、予防措置を講じるのに役立つ情報や、不正通話を防止するためのベスト プラクティスも紹介します。

次の項を参照してください。

規制テーブルを使用した、Cisco Unity Connection 8.x での不正通話の防止

不正通話とは、組織の費用負担で、組織のポリシーに違反して行われる、すべての長距離通話のことです。Cisco Unity Connection には、不正通話を防止するために使用できる規制テーブルが用意されています。規制テーブルでは、着信転送、メッセージ通知、および Connection のその他の機能に使用できる電話番号を制御します。各サービス クラスにいくつかの規制テーブルが関連付けられており、必要に応じて規制テーブルを追加することもできます。デフォルトでは、規制テーブルは、トランク アクセス コード 9 のダイヤル プランの、基本的な不正通話規制用に設定されています。使用するダイヤル プランおよび国際通話のプレフィックスに合わせて、規制テーブルを調整する必要があります。

ベスト プラクティス

ユーザ、管理者、および Cisco Unity Connection メールボックスへのアクセスを不正に取得した外部発信者による不正通話を防ぐには、次の変更を行います。

- すべての規制テーブルを、国際通話のオペレータへの呼び出しをブロックするように設定します。この設定を行うと、内線から国際通話のオペレータにダイヤルしたり、国際通話のオペレータからの着信転送を設定したりして国際通話を行うことができなくなります。たとえば、トランク アクセス コード 9 の後に 00 をダイヤルして国際通話のオペレータを呼び出すことができなくなります。
- Connection が 2 つの電話システムと連動している場合は、両方の電話システムとの連動用に、該当するトランク アクセス コードと一致する規制テーブルのパターンを追加します。たとえば、1 つの電話システム連動用のトランク アクセス コードが 99 の場合に、ダイヤル パターン 900 を規制するには、パターン 99900 も規制します。トランク アクセス コードを含むパターンが規制されると、最初にどちらかのトランクにアクセスしてから国際通話のオペレータにダイヤルして規制テーブルをバイパスする試みがブロックされます。

- 仕事で国際通話番号にアクセスする必要がない人については、国際通話番号へのすべての呼び出しをブロックするように、規制テーブルを設定します。これにより、その規制テーブルと関連付けられている Connection メールボックスへのアクセスが許可されている人が、その内線から国際通話番号への着信転送やファクス配信を設定できなくなります。
- 国内の長距離通話について、特定の市外局番への通話だけを許可するか、またはすべて禁止するように、規制テーブルを設定します。これにより、その規制テーブルと関連付けられている Connection メールボックスへのアクセスが許可されている人が、その内線から長距離通話の番号への着信転送やファクス配信を設定できなくなります。
- システム転送に使用できる番号を規制します。システム転送は、発信者がある番号をダイヤルしてから、指定した別の番号に転送できる機能です。たとえば、発信者がロビーや会議室の電話に通話を転送することはできるが、国際通話のオペレータや、長距離通話の番号への転送はできないように、規制テーブルを設定します。

規制テーブルの機能と、それらのテーブルの設定方法については、『*System Administration Guide for Cisco Unity Connection*』*(Release 8.x)*（http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html から入手可能）の「Managing Restriction Tables in Cisco Unity Connection 8.x 」の章を参照してください。

コレクト コール オプションの制限

必要に応じて、着信電話回線でのコレクト コール オプションを制限するように、電話会社と取り決めることを推奨します。

CHAPTER 3

Cisco Unity Connection 8.x、Cisco Unified Communications Manager、および IP 電話の間の接続の保護

この章では、Cisco Unity Connection、Cisco Unified Communications Manager、および IP 電話の間の接続に関連して発生する可能性がある、セキュリティ上の問題について説明します。また、とるべき対策に関する情報、意思決定に役立つ推奨事項、下した決定の効果に関する情報、およびベスト プラクティスも紹介します。

次の項を参照してください。

Cisco Unity Connection 8.x、Cisco Unified Communications Manager、および IP 電話の間の接続に関連するセキュリティ上の問題

Cisco Unity Connection システムは、Connection のボイス メッセージ ポート（SCCP 連動用）またはポート グループ（SIP 連動用）、Cisco Unified Communications Manager、および IP 電話の間の接続に関して、潜在的な脆弱性を持ちます。

次のような脅威が発生する可能性があります。

- 中間者攻撃（Cisco Unified CM と Connection の間の情報フローが監視され、改変される）
- ネットワーク トラフィック スニフィング（ソフトウェアを通じて、Cisco Unified CM、Connection、および Cisco Unified CM で管理される IP 電話の間を流れる通話内容やシグナリング情報がキャプチャされる）
- Connection と Cisco Unified CM の間のコール シグナリングの改変
- Connection とエンドポイント（IP 電話やゲートウェイなど）の間のメディア ストリームの改変

- Connection の ID 盗用（Connection 以外のデバイスが、Connection サーバとして Cisco Unified CM にアクセスする）
- Cisco Unified CM サーバの ID 盗用（Cisco Unified CM 以外のサーバが、Cisco Unified CM サーバとして Connection にアクセスする）

Cisco Unified Communications Manager の、Cisco Unity Connection 8.x ボイス メッセージ ポート用のセキュリティ機能

Cisco Unified CM では、Connection との接続を、「Cisco Unity Connection 8.x、Cisco Unified Communications Manager、および IP 電話の間の接続に関連するセキュリティ上の問題」（P.3-11）に挙げた脅威から保護できます。Connection で使用可能な Cisco Unified CM のセキュリティ機能について、表 3-1 で説明します。

表 3-1　Cisco Unity Connection で使用される Cisco Unified CM のセキュリティ機能

セキュリティ機能	説明
シグナリング認証	Transport Layer Security（TLS; トランスポート層セキュリティ）プロトコルを使用して、シグナリング パケットが転送中に改ざんされていないことを検証するプロセスです。シグナリング認証は Cisco Certificate Trust List（CTL; 証明書信頼リスト）ファイルの作成に依存します。 この機能によって、次の脅威から保護されます。 • Cisco Unified CM と Connection の間の情報フローを改変する中間者攻撃。 • コールシグナリングの改変。 • Connection サーバの ID 盗用。 • Cisco Unified CM サーバの ID 盗用。
デバイス認証	デバイスの ID を検証してエンティティが正当なものであることを確認するプロセスです。このプロセスは、Cisco Unified CM と、Connection ボイス メッセージ ポート（SCCP 連動用）または Connection ポート グループ（SIP 連動用）との間で、各デバイスがもう一方のデバイスの証明書を受け入れるときに発生します。証明書が受け入れられると、デバイス間に安全な接続が確立されます。デバイス認証は Cisco Certificate Trust List（CTL; 証明書信頼リスト）ファイルの作成に依存します。 この機能によって、次の脅威から保護されます。 • Cisco Unified CM と Connection の間の情報フローを改変する中間者攻撃。 • メディア ストリームの改変。 • Connection サーバの ID 盗用。 • Cisco Unified CM サーバの ID 盗用。

表 3-1　Cisco Unity Connection で使用される Cisco Unified CM のセキュリティ機能（続き）

セキュリティ機能	説明
シグナリング暗号化	暗号化の手法を使用して、Connection と Cisco Unified CM の間で送信されるすべての SCCP または SIP シグナリング メッセージの機密を保護するプロセス。シグナリング暗号化によって、相手に関連する情報、相手が入力した DTMF 番号、通話の状態、メディア暗号キーなどの情報が意図しないアクセスや不正なアクセスから保護されることが保証されます。 この機能によって、次の脅威から保護されます。 • Cisco Unified CM と Connection の間の情報フローを監視する中間者攻撃。 • Cisco Unified CM と Connection の間のシグナリング情報フローを監視するネットワーク トラフィック スニフィング。
メディアの暗号化	暗号化の手順を使用して、メディアの機密を保持するプロセスです。このプロセスでは、IETF RFC 3711 で定義されている Secure Real Time Protocol（SRTP）を使用して、目的の受信者だけが Connection とエンドポイント（電話機やゲートウェイなど）の間のメディア ストリームを解釈できるようにします。サポートされているのは、音声ストリームだけです。メディア暗号化には、デバイス用のメディア マスター キー ペアの作成、Connection とエンドポイントへのキーの配布、さらにはキーの転送中の安全確保が含まれます。Connection とエンドポイントは、そのキーを使用してメディア ストリームの暗号化と復号化を行います。 この機能によって、次の脅威から保護されます。 • Cisco Unified CM と Connection の間のメディア ストリームを傍受する中間者攻撃。 • Cisco Unified CM が管理する Cisco Unified CM、Connection、および IP 電話の間を流れる電話通話を盗聴するネットワーク トラフィックのスニフィング。

認証とシグナリング暗号化は、メディアを暗号化するための最小要件です。つまり、デバイスがシグナリング暗号化と認証をサポートしていない場合、メディア暗号化は行われません。

Cisco Unified CM のセキュリティ（認証および暗号化）では、Connection への通話だけを保護します。メッセージ ストアで録音されたメッセージは、Cisco Unified CM の認証および暗号化機能では保護されませんが、Connection の個人情報の安全が図られるメッセージ機能で保護できます。Connection の安全なメッセージ機能の詳細については、「プライベートまたはセキュアとマークされたメッセージが Cisco Unity Connection 8.x で処理される方法」（P.10-57）を参照してください。

Cisco Unified Communications Manager および Cisco Unity Connection 8.x のセキュリティ モード設定

Cisco Unified Communications Manager および Cisco Unity Connection には、ボイス メッセージ ポート（SCCP 連動用）またはポート グループ（SIP 連動用）について、表 3-2 に示すセキュリティ モード オプションがあります。

注意　Connection ボイス メッセージ ポート（SCCP 連動用）またはポート グループ（SIP 連動用）のクラスタ セキュリティ モード設定は、Cisco Unified CM ポートのセキュリティ モード設定と一致する必要があります。一致しないと、Cisco Unified CM での認証および暗号化が失敗します。

表 3-2　セキュリティ モード オプション

設定	効果
非セキュア	コールシグナリング メッセージがクリア（暗号化されていない）テキストとして送信され、認証された TLS ポートではなく非認証ポートを使用して Cisco Unified CM に接続されるため、コールシグナリング メッセージの完全性とプライバシーは保証されません。 また、メディア ストリームも暗号化できません。
認証	コールシグナリング メッセージは認証された TLS ポートを使用して Cisco Unified CM に接続されるため、完全性が保証されます。ただし、クリア（暗号化されていない）テキストで送信されるため、コールシグナリング メッセージのプライバシーは保証されません。 また、メディア ストリームも暗号化されません。
暗号化	コールシグナリング メッセージは認証された TLS ポートを使用して Cisco Unified CM に接続され、暗号化されるため、完全性とプライバシーが保証されます。 また、メディア ストリームも暗号化できます。 **注意**　メディア ストリームが暗号化されるようにするには、両方のエンドポイントが暗号化モードで登録されている必要があります。ただし、一方のエンドポイントが非セキュア モードまたは認証モードに設定され、もう一方のエンドポイントが暗号化モードに設定されている場合、メディア ストリームは暗号化されません。また、仲介デバイス（トランスコーダやゲートウェイなど）で暗号化が有効になっていない場合も、メディア ストリームは暗号化されません。

Cisco Unity Connection 8.x、Cisco Unified Communications Manager、および IP 電話の間の接続を保護するためのベスト プラクティス

Cisco Unity Connection と Cisco Unified Communications Manager の両方でボイス メッセージ ポートの認証および暗号化を有効にする場合は、『*Cisco Unified Communications Manager SCCP Integration Guide for Connection Release 8.x*』を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/integration/guide/cucm_sccp/cucintcucmskinny.html から入手可能です。

CHAPTER 4

Cisco Unity Connection 8.x での管理アカウントおよびサービス アカウントの保護

この章では、アカウント保護に関連して発生する可能性があるセキュリティ上の問題について説明します。また、とるべき対策に関する情報、意思決定に役立つ推奨事項、下した決定の効果に関する情報、およびベスト プラクティスも紹介します。

次の項を参照してください。

Cisco Unity Connection 8.x の管理アカウントについて

Cisco Unity Connection サーバには 2 種類の管理アカウントがあります。表 4-1 は、これら 2 つのアカウントの用途と相違点の概要を示しています。

表 4-1　Connection サーバの管理アカウント

	Operating System Administration アカウント	Application Administration アカウント
アクセス先	• Cisco Unified Operating System Administration • Disaster Recovery System • コマンド ライン インターフェイス	• Cisco Unity Connection Administration • Cisco Unified Serviceability • Cisco Unity Connection Serviceability • Real-Time Monitoring Tool
最初のアカウントの作成	インストール中に、管理者 ID およびパスワードを指定するときに作成	インストール中に、アプリケーション ユーザ名およびパスワードを指定するときに作成
アカウント名の変更方法	未サポート	Cisco Unity Connection Administration を使用。 **注意** アカウント名の変更に **utils reset_ui_administrator_name** コマンドを使用しないでください。このコマンドを使用すると、Connection が適切に機能しなくなります。

表 4-1　Connection サーバの管理アカウント（続き）

	Operating System Administration アカウント	Application Administration アカウント
アカウント パスワードの変更方法	**set password** CLI コマンドを使用	• Cisco Unity Connection Administration を使用 • **utils cuc reset password** CLI コマンドを使用 **注意** アカウント名の変更に **utils reset_ui_administrator_password** コマンドは使用しないでください。このコマンドを使用すると、Connection が適切に機能しなくなります。
追加アカウントの作成方法	**set account** CLI コマンドを使用	Cisco Unity Connection Administration を使用 **注意** 追加アカウントの作成に **set account** コマンドは使用しないでください。このコマンドを使用すると、Connection が適切に機能しなくなります。
最初のアカウント以外のアカウントの削除方法	**delete account** CLI コマンドを使用	Cisco Unity Connection Administration を使用 **注意** アカウントの削除に **delete account** コマンドは使用しないでください。このコマンドを使用すると、Connection が適切に機能しなくなります。
管理アカウントのリスト方法	**show account** CLI コマンドを使用。	Cisco Unity Connection Administration を使用
LDAP ユーザ アカウントとの連動	No	Yes

Cisco Unity Connection Administration に Connection 8.x でアクセスする際に使用するアカウントのベスト プラクティス

Cisco Unity Connection Administration は、ほとんどの管理タスクに使用する Web アプリケーションです。管理アカウントを使用して Connection の管理 にアクセスし、個々のユーザ（またはユーザ グループ）に対して Cisco Unity Connection がどのように機能するかを定義し、システム スケジュールを設定し、コール管理オプションを設定し、その他の重要なデータを変更します。これらの処理はすべて、管理アカウントが割り当てられているロールに依存します。サイトが複数の Connection サーバで構成される場合、あるサーバで Connection の管理 へのアクセスに使用されるアカウントが、ネットワーク上の他のサーバで Connection の管理 に対する認証とアクセスにも使用できることがあります。Connection の管理 へのアクセスを保護するには、次のベスト プラクティスを検討してください。

ベスト プラクティス：Application Administration アカウントの使用の制限

Cisco Unity Connection のユーザ アカウントを Connection の管理専用に作成するまでは、デフォルトの管理者アカウントと関連付けられている資格情報を使用して、Cisco Unity Connection Administration にサインインします。デフォルトの管理者アカウントは、Connection のインストール中に、インストール時に指定したアプリケーション ユーザのユーザ名およびパスワードを使用して作

成されます。デフォルトの管理者アカウントには、自動的にシステム管理者の役割が割り当てられます。この役割では、Connection の管理 への完全なシステム アクセス権限が提供されます。つまり、管理者アカウントは、Connection の管理 のすべてのページにアクセスできるだけでなく、Connection の管理 のすべてのページに対する読み取り、編集、作成、削除、および実行の各特権を持ちます。このため、高い特権を持つこのアカウントは、1 人またはごく少数の人だけが使用できるように制限する必要があります。

デフォルトの管理者アカウントの代わりとなる管理アカウントを、追加で作成できます。追加するアカウントには、それらを使用する各ユーザが実行する管理タスクに応じて、より少ない特権を持つ役割を割り当てます。

管理アカウントの作成の詳細については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』*(Release 8.x)* の「Adding Cisco Unity Connection 8.x Accounts Individually」の章にある「Adding an Administrator Account (User Without a Voice Mailbox)」の項を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html から入手可能です。

ベスト プラクティス：役割を使用した、Cisco Unity Connection Administration への各種レベルのアクセスの提供

Cisco Unity Connection Administration へのアクセスを保護するために役割の割り当てを変更する際には、次のベスト プラクティスを検討してください。

- デフォルトの管理者アカウントへの役割の割り当ては変更しません。その代わりに、Connection の管理 への適切なレベルのアクセスを提供する、追加の管理ユーザ アカウントを作成します。たとえば、管理ユーザ アカウントをユーザ管理者の役割に割り当てて、管理者がユーザ アカウント設定を管理したり、すべてのユーザ管理機能にアクセスしたりできるようにします。または、管理ユーザ アカウントをヘルプ デスク管理者の役割に割り当てて、管理者がユーザ パスワードおよび PIN をリセットしたり、ユーザ アカウントのロックを解除したり、ユーザ設定ページを表示したりできるようにします。
- 追加の管理ユーザ テンプレートを作成し、それぞれのテンプレートに、さまざまなレベルのアクセスを提供する役割を割り当てます。デフォルトでは、管理者ユーザ テンプレートには、システム管理者の役割が割り当てられます。管理者ユーザ テンプレートから作成されたすべての管理ユーザ アカウントにはシステム管理者の役割が割り当てられ、管理者は Connection のすべての管理機能に対するフル アクセス権を与えられます。この管理者テンプレートを慎重に使用して、管理ユーザ用のアカウントを作成します。
- デフォルトでは、ボイスメール ユーザ テンプレートにはどの役割も割り当てられず、このテンプレートに管理役割を割り当てることはできません。その代わりに、このテンプレートを使用して、メールボックスを持つエンド ユーザ用のアカウントを作成します。（メールボックスを持つエンド ユーザに割り当てる唯一の役割は、グリーティング管理者の役割です。この役割では、「管理」機能だけが Cisco Unity Greetings Administrator にアクセスでき、ユーザはコール ハンドラ用の録音済みグリーティングを電話で管理できます）。

Cisco Unity Connection によって提供される事前定義の役割および各役割に含まれる特権のレベルの詳細については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』*(Release 8.x)*（http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html から入手可能）の「Preparing to Add User Accounts in Cisco Unity Connection 8.x」の章にある「Roles in Cisco Unity Connection 8.x」の項を参照してください。

ベスト プラクティス：異なるアカウントを使用した、ボイスメールボックスおよび Cisco Unity Connection Administration へのアクセス

Cisco Unity Connection 管理者が Cisco Unity Connection Administration にアクセスするときに、Cisco Personal Communications Assistant（PCA）または電話インターフェイスへのサインインに使用するのと同じアカウントを使用しないことを推奨します。

ユニファイド メッセージング サービス アカウントの保護（Cisco Unity Connection 8.5 以降のみ）

Cisco Unity Connection 8.5 以降のユニファイド メッセージングを設定する場合は、Connection が Exchange との通信に使用する 1 つ以上の Active Directory アカウントを作成します。Exchange メールボックスにアクセスする権限を持つ Active Directory アカウントと同様に、このアカウントのアカウント名とパスワードを知っているユーザは、メールを読んだり、音声メッセージを聞いたり、メッセージを送信および削除したりできます。このアカウントは、Exchange における広範囲の権限を持っていないため、たとえば、Exchange サーバの再起動などに使用できない場合があります。

アカウント保護のために、大文字、小文字、数字、および特殊文字からなる 20 文字以上の長いパスワードをアカウントに与えることを推奨します。パスワードは AES 128 ビットの暗号化方式によって暗号化され、Connection データベースに保存されます。データベースはルート アクセスによってしかアクセスできず、ルート アクセスは Cisco TAC からのサポートによってしか使用できません。

アカウントを無効にしないでください。無効にすると、Connection がアカウントを使用して Exchange メールボックスにアクセスできなくなります。

CHAPTER 5

Cisco Unity Connection 8.6 における FIPS コンプライアンス

Cisco Unity Connection 8.6 は、FIPS モードをサポートしています。FIPS モードは、連邦情報処理標準 140-2（FIPS）要件に準拠しています。

Cisco Unified Communications Manager Business Edition（CUCMBE）では、FIPS モードはサポートされていません。管理者に対して **utils fips <option>** コマンドライン インターフェイス（CLI）コマンドが表示されますが、これは機能しません。

次の場合に、Connection の FIPS モードをイネーブルにすることを推奨します。

- Cisco Unity Connection 8.6 の新規インストールを実行し、FIPS モードを使用する場合は、Connection サーバの設定とテレフォニー統合の追加を行う前に FIPS をイネーブルにする必要があります。
- Cisco Unity Connection 8.6 へのアップグレードを実行する場合は、既存のテレフォニー統合を使用する前に、証明書を手順に従って再生成してください。証明書を再生成する方法については、FIPS の証明書の再生成の項を参照してください。

次の項を参照してください。

FIPS の CLI コマンドの実行

Cisco Unity Connection で FIPS 機能をイネーブルにするには、**utils fips enable** CLI コマンドを使用します。また、次の CLI コマンドも使用できます。

- **utils fips disable**：FIPS 機能をディセーブルにします。
- **utils fips status**：FIPS コンプライアンスのステータスをチェックします。

utils fips <option> CLI コマンドの詳細については、該当する『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このガイドは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。

注意　FIPS モードをイネーブル化またはディセーブル化した後、Cisco Unity Connection サーバが自動的に再起動します。

注意　Cisco Unity Connection サーバがクラスタ内にある場合は、現在のノード上で FIPS の操作が完了し、システムが再起動して稼動するまで、他のすべてのノード上の FIPS 設定を変更しないでください。

FIPS の証明書の再生成

既存のテレフォニー統合を備えた Cisco Unity Connection サーバの場合は、FIPS モードをイネーブル化またはディセーブル化した後に手動で再生成されたルート証明書を持っている必要があります。テレフォニー統合が Authenticated モードまたは Encrypted Security モードを使用する場合は、対応するすべての Cisco Unified Communications Manager サーバに、再生成されたルート証明書を再アップロードする必要があります。新規インストールの場合は、テレフォニー統合を追加する前に FIPS モードをイネーブルにすると、ルート証明書の再生成を回避できます。

FIPS モードをイネーブルまたはディセーブルにするたびに、次の手順を実行します。

（注）　クラスタの場合は、すべてのノード上で次の手順を実行します。

1. Cisco Unity Connection Administration にログインします。
2. [テレフォニー統合（Telephony Integrations）] > [セキュリティ（Security）] > [ルート証明書（Root Certificate）] を選択します。
3. [ルート証明書の表示（View Root Certificate）] ページで [新規作成（Generate New）] をクリックします。
4. テレフォニー統合が Authenticated モードまたは Encrypted Security モードを使用する場合は、ステップ 5 ～ 10 を実行してください。そうでない場合は、ステップ 12 へ進んでください。
5. [ルート証明書の表示（View Root Certificate）] ページで [右クリックして証明書をファイルとして保存（Right-Click to Save the Certificate as a File）] リンクを右クリックします。
6. [名前を付けて保存（Save As）] を選択して Cisco Unity Connection ルート証明書を保存する場所を参照し、.pem ファイルとして保存します。

注意　証明書は、拡張子 .pem（.htm ではなく）のファイルとして保存する必要があります。そうしないと、Cisco Unified CM で証明書が認識されません。

7. 次のサブステップを実行して、Cisco Unity Connection ルート証明書をすべての Cisco Unified CM サーバにコピーします。

a. Cisco Unified CM サーバで Cisco Unified Operating System Administration にサインインします。
b. [セキュリティ（Security）] メニューから [証明書の管理（Certificate Management）] オプションを選択します。
c. [証明書の一覧（Certificate List）] ページで [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] を選択します。
d. [証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] ページで、[証明書の名前（Certificate Name）] ドロップダウンから [CallManager-trust] を選択します。
e. [ルート証明書（Root Certificate）] フィールドに「Cisco Unity Connection Root Certificate」と入力します。
f. [ファイルのアップロード（Upload File）] フィールドで [参照（Browse）] をクリックし、ステップ 5 で保存した Cisco Unity Connection ルート証明書を見つけて選択します。
g. [ファイルのアップロード（Upload File）] をクリックします。
h. [閉じる（Close）] をクリックします。

8. Cisco Unified CM サーバで Cisco Unified Serviceability にサインインします。
9. [ツール（Tools）] メニューから [サービス管理（Service Management）] を選択します。
10. [コントロール センター - 機能サービス（Control Center - Feature Services）] ページで、Cisco CallManager サービスを再起動します。
11. Cisco Unified CM クラスタ内にある残りのすべての Cisco Unified CM サーバ上で、ステップ 5 ～ 10 を繰り返します。
12. 次の手順に従って、Connection Conversation Manager Service を再起動します。
    a. Cisco Unity Connection Serviceability にログインします。
    b. [ツール（Tools）] メニューから [サービス管理（Service Management）] を選択します。
    c. [重要なサービス（Critical Services）] セクションで [停止（Stop）] を選択して Connection Conversation Manager サービスを停止します。
    d. [ステータス（Status）] エリアに、Connection Conversation Manager サービスが正常に停止されたというメッセージが表示されたら、そのサービスの [スタート（Start）] を選択します。
13. 新規および既存のテレフォニー統合のポートが Cisco Unified CM に正常に登録されます。

FIPS は、Cisco Unified Communications Manager と Cisco Unity Connection の間の SCCP 統合および SIP 統合の両方でサポートされています。

証明書の管理の詳細については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection*』の「Security」の章の「Manage Certificates and Certificate Trust Lists」の項を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/os_administration/guide/8xcucosag060.html#wp1053189 から入手可能です。

FIPS モード使用時の追加設定

FIPS コンプライアンスを維持するためには、次の機能への追加設定が必須です。

- ネットワーキング：サイト内、サイト間、VPIM
- ユニファイド メッセージング：ユニファイド メッセージング サービス

次の項を参照してください。

FIPS モード使用時のネットワーキングの設定

Cisco Unity Connection から別のサーバへのネットワーキングは、IPsec ポリシーによって保護される必要があります。これには、サイト間リンク、サイト内リンク、および VPIM ロケーションが含まれます。リモート サーバには、独自の FIPS コンプライアンスを保証する責任があります。

（注） セキュア メッセージは、IPsec ポリシーが設定されない限り FIPS 準拠の方法では送信されません。

FIPS モード使用時のユニファイド メッセージングの設定

ユニファイド メッセージング サービスには、次の設定が必要です。

- Cisco Unity Connection と Microsoft Exchange または Cisco Unified MeetingPlace の間に IPsec ポリシーを設定します
- [Connection 管理（Connection Administration）] の [ユニファイド メッセージング サービスの編集（Edit Unified Messaging Service）] ページにある [Web ベース認証モード（Web-Based Authentication Mode）] を [基本認証（Basic）] に設定します。

注意 サーバ間の IPsec ポリシーは、基本 Web 認証のプレーン テキストの形式を保護するために必要です。

FIPS モード使用時の IPsec ポリシーの設定

IPsec ポリシーの設定については、『*Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection*』の「Security」の章の「IPSEC Management」の項を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/os_administration/guide/8xcucosagx.html から入手可能です。

Microsoft Exchange サーバの IPsec ポリシーの設定については、Microsoft の IPsec 関連のマニュアルを参照してください。

FIPS モード使用時にサポートされない機能

FIPS モードがイネーブルの場合、次の Cisco Unity Connection の機能はサポートされません。

- SpeechView 音声テキスト変換サービス
- SIP ダイジェスト認証（SIP テレフォニー統合用の設定）

サインインするタッチトーン カンバセーション ユーザのボイスメール PIN の設定

Cisco Unity Connection 8.6 の FIPS をイネーブルにすると、次の 2 つのオプションの両方に該当する場合、タッチトーン カンバセーションのユーザがサインインして音声メッセージを再生または送信したり、ユーザ設定を変更したりするのを防ぎます。

- Cisco Unity 5.x またはそれ以前のバージョンでユーザが作成され、その後 Connection に移行した場合。
- Connection ユーザが、Cisco Unity 5.x またはそれ以前のバージョンで割り当てられたボイスメール PIN を保持している場合。

タッチトーン カンバセーションのユーザは、ID（通常はユーザの内線番号）とボイスメール PIN を入力してサインインします。ID および PIN は、ユーザの作成時に割り当てられます。管理者またはユーザのいずれかが PIN を変更できます。Connection Administration では、管理者が PIN にアクセスできないように、PIN がハッシュされます。Cisco Unity 5.x 以前のバージョンでは、Cisco Unity が MD5 ハッシュ アルゴリズム（FIPS 非準拠）を使用して PIN をハッシュします。Cisco Unity 7.x 以降、および Connection では、復号化がより困難な SHA-1 アルゴリズム（FIPS 準拠）を使用して PIN をハッシュします。

バージョン 8.5 以前では、ユーザが Connection をコールして ID と PIN を入力した場合、Connection がデータベースのチェックを行い、ユーザの PIN が MD5 と SHA-1 アルゴリズムのどちらでハッシュされたのかを判別します。Connection はユーザが入力した PIN をハッシュし、その PIN を Connection データベース内でハッシュされた PIN と比較します。PIN が一致した場合は、ユーザがログインします。

次の項では、FIPS がイネーブルの場合に Connection でボイスメール PIN を設定する方法について説明します。

- 「Cisco Unity Connection 8.6(1) 以降のバージョンでの SHA-1 アルゴリズム使用によるすべてのボイスメール PIN のハッシュ」（P.5-23）
- 「Cisco Unity 5.x またはそれ以前のバージョンでの、MD5 によってハッシュされたボイスメール PIN と SHA-1 アルゴリズムとの置き換え」（P.5-24）

Cisco Unity Connection 8.6(1) 以降のバージョンでの SHA-1 アルゴリズム使用によるすべてのボイスメール PIN のハッシュ

バージョン 8.6 以降では、FIPS がイネーブルの場合、Cisco Unity Connection はデータベースのチェックを行なわず、ユーザのボイスメール PIN が MD5 と SHA-1 アルゴリズムのどちらでハッシュされたのかを判別しません。Connection はすべてのボイスメール PIN を SHA-1 でハッシュし、その PIN を Connection データベース内でハッシュされた PIN と比較します。ユーザが入力して MD5 によってハッシュされたボイスメール PIN が、データベース内で SHA-1 によってハッシュされたボイスメール PIN と一致しない場合、ユーザはサインインを許可されません。

Cisco Unity 5.x またはそれ以前のバージョンでの、MD5 によってハッシュされたボイスメール PIN と SHA-1 アルゴリズムとの置き換え

Cisco Unity 5.x またはそれ以前のバージョンで作成された Connection ユーザ アカウントでは、MD5 アルゴリズムによってハッシュされたボイスメール PIN が SHA-1 アルゴリズムに置き換えられる必要があります。MD5 によってハッシュされたパスワードを SHA-1 によってハッシュされたパスワードに置き換える際には、次の点を考慮します。

- User Data Dump ユーティリティの最新バージョンを使用して、MD5 によってハッシュされた PIN を持っているユーザの数を判別します。各ユーザの [Pin_Hash_Type] カラムに MD5 または SHA-1 のいずれかが表示されます。このユーティリティの最新バージョンをダウンロードして [ヘルプ（Help）] を表示する方法については、次の URL にある Cisco Unity Tools Web サイトの [User Data Dump] ページを参照してください。
  http://ciscounitytools.com/Applications/CxN/UserDataDump/UserDataDump.html

（注）　User Data Dump ユーティリティの古いバージョンには、[Pin_Hash_Type] カラムは含まれていません。

- FIPS をイネーブルにする前に、[Connection 管理（Connection Administration）] の [パスワードの設定（Password Settings）] ページで、[次回サインイン時に、ユーザによる変更が必要（User Must Change at Next Sign-In）] チェックボックスをオンにしてください。これにより、ユーザは Connection にサインインして自分のボイスメール PIN を変更できるようになります。
- ボイスメール PIN を変更していないユーザがいる場合は、Bulk Password Edit ユーティリティを実行します。Bulk Password Edit ユーティリティを使用すると、PIN をランダムな値に選択的に変更し、そのデータを .csv ファイルとしてエクスポートできます。エクスポートされるファイルには、PIN が変更された各ユーザの名前、エイリアス、電子メール アドレス、および新しい PIN が含まれます。この .csv ファイルを使用して、新しい PIN を持つ各ユーザに電子メールを送信することができます。このユーティリティは、次の URL にある Cisco Unity Tools Web サイトから入手できます。
  http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html

CHAPTER 6

Cisco Unity Connection 8.x での、パスワード、PIN、および認証規則の管理

Cisco Unity Connection では、認証規則によって、すべてのユーザ アカウントのユーザ パスワード、PIN、およびアカウント ロックアウトが管理されます。Connection の認証規則を次のように定義することを推奨します。

- ユーザが PIN とパスワードを頻繁に変更することを必須にする。
- ユーザの PIN およびパスワードには、一意で、簡単に推測できないものを設定することを必須にする。

認証規則を綿密に設定すると、無効な PIN またはパスワードを何回も入力したユーザをロック アウトできるため、Connection アプリケーションへの不正アクセスの阻止にも役立ちます。

この章では、上に挙げたタスクの実行や、PIN およびパスワードのセキュリティに関連するその他の問題に関する情報を提供します。Cisco Unity Connection パスワードの管理の範囲を理解するのに役立つように、この章の最初の項では、Cisco Personal Communications Assistant（PCA）、Connection カンバセーション、Cisco Unity Connection Administration、およびその他の管理 Web アプリケーションへのアクセスに必要な、さまざまなパスワードについて説明します。その後の各項では、とるべき対策に関する情報、意思決定に役立つ推奨事項、下した決定の効果に関する情報、およびベスト プラクティスを紹介します。

Connection パスワードを保護する手順および認証規則を定義する手順については、次の各項を参照してください。

ユーザが使用する PIN およびパスワードについて

「ユーザが Cisco Unity Connection 8.x アプリケーションへのアクセスに使用する PIN およびパスワードについて」（P.6-26）

PIN とパスワードの割り当て方法、およびそれらを最初にセキュリティで保護する方法について

「Cisco Unity Connection 8.x での、ユーザへの一意で安全な PIN およびパスワードの割り当て」（P.6-26）

ユーザの PIN およびパスワードを変更する方法

「Cisco Unity Connection 8.x Web アプリケーションのパスワードの変更」（P.6-27）

「Cisco Unity Connection 8.x の電話機 PIN の変更」（P.6-28）

認証規則を定義する方法

「Cisco Unity Connection 8.x でパスワード、PIN、およびロックアウト ポリシーを指定する認証規則の定義」（P.6-28）

ユーザが Cisco Unity Connection 8.x アプリケーションへのアクセスに使用する PIN およびパスワードについて

Cisco Unity Connection のユーザは、各種の Connection アプリケーションへのアクセスに、異なる PIN およびパスワードを使用します。Connection パスワードの管理の範囲を理解するうえで、各アプリケーションにどのパスワードが必要なのかを知ることが重要です。

電話機の PIN

ユーザは、電話機の PIN を使用して、Cisco Unity Connection カンバセーションに電話機からサインインします。PIN（数値だけで構成）は、電話機のキーパッドを使用して入力するか、音声認識が有効な場合は読み上げます。

Web アプリケーション（Cisco PCA）のパスワード

ユーザは、Web アプリケーションのパスワードを使用して、Cisco Personal Communications Assistant（Cisco PCA）にサインインします。これにより、Messaging Inbox（Connection 8.0）Messaging Assistant、および Personal Call Transfer Rules Web ツールにアクセスできます。

管理の役割を割り当てられているユーザは、Web アプリケーションのパスワードを使用して次の Connection アプリケーションにサインインすることもあります。

- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability
- Cisco Unified Serviceability
- Real-Time Monitoring Tool

（注） Cisco Unified Communications Manager Business Edition（CMBE）または LDAP の認証を使用している場合、ユーザは、ユーザの Cisco Unified CMBE または LDAP アカウント パスワードを使用して Connection Web アプリケーションにアクセスする必要があります。

Cisco Unity Connection 8.x での、ユーザへの一意で安全な PIN およびパスワードの割り当て

不正アクセスや不正通話から Cisco Unity Connection を保護するには、すべてのユーザに一意の電話機 PIN および Web アプリケーション（Cisco PCA）パスワードを割り当てる必要があります。

ユーザを Connection に追加する際には、そのユーザ アカウントの作成に使用したテンプレートによって、電話機 PIN と Web アプリケーション パスワードが決まります。デフォルトでは、ユーザ テンプレートには、ランダムに生成された文字列が電話機 PIN および Web パスワードとして割り当てられます。1 つのテンプレートから作成されたすべてのユーザに、同じ PIN およびパスワードが割り当てられます。

次のオプションを検討して、アカウントの作成時、またはその直後に、各ユーザに一意で安全な PIN およびパスワードが確実に割り当てられるようにしてください。

- 少数のユーザ アカウントを作成する場合、または Cisco Unity Connection Administration を使用してアカウントを作成した後は、[ユーザ（Users）] > [ユーザ（Users）] > [パスワードの変更（Change Password）] ページで各ユーザの電話機 PIN と Web パスワードを変更します。または、ユーザに対し、できるだけ速やかにサインインして自分の PIN とパスワードを変更するように指

示します（この場合は、アカウントの作成に使用したテンプレートの [パスワードの編集（Edit Password）] ページにある [次回サインイン時に、ユーザによる変更が必要（User Must Change at Next Sign-In）] チェックボックスをオンにしてください）。

- 複数のユーザ アカウントを作成する場合は、アカウント作成後、Bulk Password Edit ツールを使用して Connection の各エンド ユーザ アカウント（メールボックスを持つユーザ）に一意のパスワードと PIN を割り当てます。Bulk Password Edit ツールは、CSV ファイルとともに使用します。CSV ファイルには、複数のパスワードおよび PIN を一括して適用するための、パスワードおよび PIN 用の一意の文字列が含まれています。

  Bulk Password Edit ツールは、Windows ベースのツールです。http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html からツールをダウンロードし、トレーニング ビデオとヘルプを参照してください。

Cisco Unity Connection 8.x Web アプリケーションのパスワードの変更

個々のユーザの Web アプリケーション（Cisco PCA）パスワードは、Cisco Unity Connection Administration の [ユーザ（Users）] > [ユーザ（Users）] > [パスワードの変更（Change Password）] ページでいつでも変更できます。

パスワードの有効期限が切れると、ユーザおよび管理者は、Cisco PCA や Connection の管理 に次にサインインするときに新しいパスワードを入力する必要があります。

ユーザは、自分の Cisco PCA パスワードを Connection Messaging Assistant で変更することもできます。

複数のエンド ユーザ アカウント（メールボックスを持つユーザ）のパスワードを変更する場合は、Bulk Password Edit ツールを使用して、一意の新しいパスワードを各アカウントに割り当てることができます。Bulk Password Edit ツールは、CSV ファイルとともに使用します。CSV ファイルには、複数のパスワードを一括して適用するための、パスワード用の一意の文字列が含まれています。Bulk Password Edit ツールは、Windows ベースのツールです。http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html からツールをダウンロードし、トレーニング ビデオとヘルプを参照してください。また、Cisco Unity Connection Bulk Administration Tool（BAT）を使用して複数のユーザ パスワードを一度に変更することもできます。BAT の使用方法については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』*（Release 8.x）*（http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html）の付録「Using the Cisco Unity Connection 8.x Bulk Administration Tool」を参照してください。

IMAP クライアントのボイス メッセージにアクセスできるユーザの場合は、Cisco PCA パスワードを Messaging Assistant で変更するたびに、IMAP クライアント内のパスワードも更新する必要があることを認識する必要があります。パスワードは、IMAP クライアントと Cisco PCA の間で同期されません。両方のアプリケーションで Cisco PCA パスワードを更新しても、IMAP クライアントでのボイス メッセージの受信に問題が発生した場合は、『*User Workstation Setup Guide for Cisco Unity Connection*』*（Release 8.x）*（http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_setup/guide/8xcucuwsx.html から入手可能）の「Configuring an Email Account to Access Cisco Unity Connection 8.x Voice Messages」の章にある「Troubleshooting IMAP Client Sign-In Problems in Cisco Unity Connection 8.x」の項を参照してください。

ベスト プラクティス

8 文字以上の長さの、単純でないパスワードを指定します。同じ方法に従ってパスワードを変更するようにユーザに奨励するか、それを必須とする認証規則をユーザに割り当てます。Cisco PCA パスワードは、6 か月ごとに変更する必要があります。

Cisco Unity Connection 8.x の電話機 PIN の変更

個々のユーザの電話機 PIN は、Cisco Unity Connection Administration の [ユーザ（Users）] > [ユーザ（Users）] > [パスワードの変更（Change Password）] ページでいつでも変更できます。

ユーザは、Connection の電話通話または Connection Messaging Assistant を使用して、電話機 PIN を変更できます。

複数のエンド ユーザ アカウント（メールボックスを持つユーザ）の PIN を変更する場合は、Bulk Password Edit ツールを使用して、一意の新しい PIN を各アカウントに割り当てることができます。Bulk Password Edit ツールは、CSV ファイルとともに使用します。CSV ファイルには、複数の PIN を一括して適用するための、PIN 用の一意の文字列が含まれています。Bulk Password Edit ツールは、Windows ベースのツールです。
http://www.ciscounitytools.com/Applications/CxN/BulkPasswordEdit/BulkPasswordEdit.html からツールをダウンロードし、トレーニング ビデオとヘルプを参照してください。また、Cisco Unity Connection Bulk Administration Tool（BAT）を使用して複数のユーザ PIN を一度に変更することもできます。BAT の使用方法については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』*（Release 8.x）*（http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html）の付録「Using the Cisco Unity Connection 8.x Bulk Administration Tool」を参照してください。

PIN の有効期限が切れると、ユーザは、Connection のカンバセーションに次にサインインするときに新しい PIN を入力する必要があります。

ユーザは Messaging Assistant を使用して電話機 PIN を変更できるため、適切な手段を講じてアプリケーション（Cisco PCA）のパスワードの安全も維持することによって、PIN のセキュリティを確保できます。

ユーザは、電話機 PIN と Cisco PCA パスワードが同期されないことを理解する必要があります。初回の登録時に、電話機の初期 PIN を変更するように求められますが、そのときには Cisco PCA の Web サイトへのサインインに使用するパスワードを変更できません。

ベスト プラクティス

各ユーザに、6 桁以上で単純でない、一意の PIN が割り当てられる必要があります。同じ方法に従うようにユーザに奨励するか、それを必須とする認証規則をユーザに割り当てます。

Cisco Unity Connection 8.x でパスワード、PIN、およびロックアウト ポリシーを指定する認証規則の定義

（注） Cisco Unity Connection の認証規則は、Cisco Unified Communications Manager Business Edition（CMBE）でのユーザ パスワードの管理や、LDAP 認証が有効になっているときには適用されません。これらの場合、認証は Connection では処理されないためです。

認証規則を使用して、ユーザが電話で Connection にアクセスするときに Cisco Unity Connection によって適用されるサインイン、パスワード、およびロックアウト ポリシーをカスタマイズします。また、ユーザが Cisco Unity Connection Administration、Cisco PCA、およびその他のアプリケーション（IMAP クライアントなど）にアクセスする方法もカスタマイズします。

Connection の管理 の [認証規則の編集（Edit Authentication Rule）] ページで指定する設定によって、次の値が決まります。

- アカウントがロックされるまでに許容される、Connection 電話インターフェイス、Cisco PCA、または Connection の管理 へのサインイン試行回数。
- アカウントがリセットされるまでロックが維持される分数。
- ロックされたアカウントを管理者が手作業でロック解除する必要があるかどうか。
- パスワードと PIN に許可される最小長。
- パスワードまたは PIN の有効期限が切れるまでの日数。

ベスト プラクティス

セキュリティを強化するため、認証規則を定義する際には、次のベスト プラクティスに従うよう推奨します。

- ユーザが少なくとも 6 か月に 1 回 Connection のパスワードと PIN を変更することを必須とする。
- Web アプリケーションのパスワードは 8 文字以上の単純でないパスワードにすることを必須とする。
- ボイスメール PIN は 6 文字以上の単純でない PIN にすることを必須とする。

セキュリティをさらに強化するには、PIN やパスワードを簡単に推測できないものにし、また、長期間使用しないようにする認証規則を設定します。それと同時に、複雑すぎる PIN やパスワードを設定するようにしたり、PIN やパスワードをあまりに頻繁に変更するようにしたりすると、ユーザが PIN やパスワードを書き留めなくてはならなくなるので、そのような規則は避けます。

また、次の各フィールドで認証規則を指定する際には、次のガイドラインに従ってください。

- サインイン試行回数（Failed Sign-In __ Attempts）
- 失敗したサインイン試行回数をリセットする間隔（Reset Failed Sign-In Attempts Every __ Minutes）
- ロックアウト期間（Lockout Duration）
- クレデンシャルの有効期限（Credential Expires After __ Days）
- 最小クレデンシャル長（Minimum Credential Length）
- 以前のクレデンシャルの保存数（Stored Number of Previous Credentials）
- 単純すぎるパスワードの確認（Check For Trivial Passwords）

サインイン試行回数（Failed Sign-In __ Attempts）

このフィールドでは、ユーザが間違った PIN またはパスワードを繰り返し入力した場合に、Connection がどのように処理するかを指定します。サインインの試みが 3 回失敗した場合にユーザ アカウントをロックするように設定することを推奨します。

失敗したサインイン試行回数をリセットする間隔（Reset Failed Sign-In Attempts Every __ Minutes）

このフィールドでは、サインインの試みが失敗した回数を Connection がクリアするまでの分数を指定します（サインイン失敗回数の制限をすでに超えて、アカウントがロックされている場合を除く）。30 分超過してから、サインインの試みが失敗した回数をクリアするように設定することを推奨します。

ロックアウト期間（Lockout Duration）

このフィールドでは、ロックアウトされたユーザが再度サインインを試みるまで待機する時間を指定します。

セキュリティをさらに強固にするには、[管理者によるロック解除が必要（Administrator Must Unlock）] チェックボックスをオンにします。そうすることで、ユーザは、管理者が該当する [ユーザ（User）] > [パスワードの設定（Password Settings）] ページでそのユーザのロックを解除するまで、アカウントにアクセスできなくなります。[管理者によるロック解除が必要（Administrator Must Unlock）] チェックボックスは、管理者がすぐに対応できる場合、またはシステムが不正アクセス / 不正通話されやすい場合にだけ、オンにしてください。

クレデンシャルの有効期限（Credential Expires After __ Days）

[無期限（Never Expires）] オプションは有効にしないことを推奨します。その代わりに、このフィールドを 0 より大きい値に設定し、ユーザが X 日（X は、[クレデンシャルの有効期限（Credential Expires After）] フィールドで指定した値）ごとにパスワードの変更を求められるようにします。

Web パスワードは 120 日後に、電話機 PIN は 180 日後に期限切れになるように設定することを推奨します。

最小クレデンシャル長（Minimum Credential Length）

このフィールドは 6 以上の値に設定することを推奨します。

Web アプリケーションのパスワードに適用される認証規則については、ユーザが 8 文字以上のパスワードを使用することを必須にするよう、推奨します。

電話機 PIN に適用される認証規則については、ユーザが 6 桁以上の PIN を使用することを必須にするよう、推奨します。

最小クレデンシャル長を変更すると、ユーザは、ユーザの PIN およびパスワードを次回変更するときに、最小クレデンシャル長の新しい値を使用する必要があります。

以前のクレデンシャルの保存数（Stored Number of Previous Credentials）

このフィールドに値を指定することを推奨します。そうすることによって、Connection が各ユーザの以前のパスワードまたは PIN を、指定した数だけ保存して、パスワードの一意性を強制できるようになります。ユーザがパスワードと PIN を変更すると、Connection で、新しいパスワードまたは PIN が、資格履歴に保存されているパスワードまたは PIN と比較されます。Connection では、履歴に保存されているパスワードまたは PIN と一致するパスワードまたは PIN が拒否されます。

デフォルトでは、Connection の資格履歴に 5 つのパスワードまたは PIN が保存されます。

単純すぎるパスワードの確認（Check For Trivial Passwords）

ユーザが単純すぎない PIN およびパスワードを使用するように、このフィールドを有効にすることを推奨します。

単純すぎない電話機 PIN には、次の特性があります。

- PIN が、ユーザの姓または名を数値で表したものと一致しない。
- PIN に、ユーザのプライマリ内線番号や代行内線番号が含まれていない。
- PIN に、ユーザのプライマリ内線番号や代行内線番号を逆順で示す数値が含まれていない。
- PIN に、数値の組み合わせが繰り返されたもの（408408、123123 など）が含まれていない。
- PIN に含まれているのが 2 つの数値のみ（121212 など）ではない。
- 値が 3 回以上連続して使用（28883 など）されていない。
- PIN は、昇順または降順の連続する数値（012345、987654 など）ではない。

- 指定されている最小クレデンシャル長と一致する数値グループの場合、キーパッド上で 1 列に並んだ数値グループが含まれていない（たとえば、3 桁の長さが指定されている場合、123、456、または 789 を PIN として使用することはできない）。

単純すぎない Web アプリケーション パスワードには、次の特性があります。

- パスワードに、大文字、小文字、数値、および記号のうち、少なくとも 3 つの文字が含まれている。
- パスワードに、ユーザのエイリアス、または逆順にしたユーザのエイリアスが含まれていない。
- パスワードに、プライマリ内線番号や代行内線番号が含まれていない。
- 1 つの文字が 4 回以上連続して使用（!Cooool など）されていない。
- 昇順または降順の、すべて連続する文字（abcdef、fedcba など）が使用されていない。

CHAPTER 7

Cisco Unity Connection 8.6 以降でのシングル サインオン

Cisco Unity Connection 8.6 以降のバージョンは、シングル サインオン機能をサポートしています。この機能により、エンド ユーザは、一度ログインするだけで次の Cisco Unity Connection アプリケーションを追加のサインオンなしで使用できます。

- Cisco Personal Communications Assistant
- Web Inbox
- Cisco Unity Connection Administration
- Cisco Unity Connection Serviceability

シングル サインオン機能の詳細については、シスコのホワイト ペーパー『*A complete guide for the installation, configuration and integration of Open Access Manager 9.0 with CUCM 8.5, 8.6 /CUC 8.6 and Active Directory for SSO*』を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf から入手可能です。

次の項を参照してください。

- 「シングル サインオンの設定チェックリスト」（P.7-33）
- 「シングル サインオンのシステム要件」（P.7-34）
- 「シングル サインオンの設定」（P.7-35）

シングル サインオンの設定チェックリスト

この項では、ネットワーク内のシングル サインオン機能を設定するためのチェックリストを示します。

表 7-1　シングル サインオン設定チェックリスト

設定手順		関連項目およびマニュアル
ステップ 1	使用環境が「シングル サインオンのシステム要件」（P.7-34）で説明されている要件を満たしていることを確認します。	—
ステップ 2	Active Directory の OpenAM サーバをプロビジョニングし、keytab ファイルを生成します。 **（注）** 使用している Windows のバージョンに keytab ファイルを生成するための ktpass ツールが含まれていない場合は、別途入手する必要があります。	Microsoft Active Directory のマニュアル

表 7-1　シングル サインオン設定チェックリスト（続き）

設定手順		関連項目およびマニュアル
ステップ 3	Cisco Unity Connection の OpenAM サーバを設定します。	「OpenAM サーバの設定」（P.7-35）
ステップ 4	OpenAM のサーバ証明書を Cisco Unified Communications Manager tomcat 信頼ストアにインポートします。	http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf
ステップ 5	Active Directory および OpenAM を使用して Windows シングル サインオンを設定します。	http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf
ステップ 6	シングル サインオンのクライアント ブラウザを設定します。	http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf
ステップ 7	Cisco Unified Communications Manager のシングル サインオンをイネーブルにします。	「シングル サインオンの CLI コマンドの実行」（P.7-36）

シングル サインオンのシステム要件

Cisco Unity Connection のシングル サインオンのシステム要件を次に示します。

- クラスタ内の各サーバに Cisco Unity Connection リリース 8.6(1) 以上。

この機能は、シングル サインオン機能を設定するために次のサードパーティ製アプリケーションが必要です。

- Active Directory を導入するための Microsoft Windows Server 2003 SP1/SP2 または Microsoft Windows Server 2008 SP2。
- Microsoft Active Directory サーバ（任意のバージョン）。
- ForgeRock Open Access Manager（OpenAM）バージョン 9.0。
- Apache Tomcat 7.0.0

シングル サインオン機能は、Active Directory および OpenAM を同時に使用し、クライアント アプリケーションにシングル サインオン アクセスを提供します。

シングル サインオン機能に必要なサードパーティ製アプリケーションは、次の設定要件を満たしている必要があります。

- Active Directory は、LDAP サーバとしてではなく、Windows ドメインベースのネットワーク設定で導入される必要があります。
- OpenAM サーバは、ネットワーク上において Connection サーバ、すべてのクライアント システム、および Active Directory サーバから名前でアクセスできなければなりません。
- OpenAM サーバは、Microsoft Windows 2003 サーバまたは RedHat Enterprise Linux（RHEL）サーバにイストールできます。
- Active Directory（ドメイン コントローラ）サーバ、Windows クライアント、Cisco Unity Connection、および OpenAM は、同じドメイン内に存在する必要があります。
- DNS をドメイン内で有効にする必要があります。
- シングル サインオンに参加するすべてのエンティティのクロックを同期させる必要があります。

サードパーティ製品の詳細については、各製品のマニュアルを参照してください。

シングル サインオンの設定

シングル サインオンのための Connection および OpenAM サーバの設定手順の詳細については、シスコのホワイト ペーパー『*A complete guide for the installation, configuration and integration of Open Access Manager 9.0 with CUCM 8.5, 8.6 /CUC 8.6 and Active Directory for SSO*』を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf から入手可能です。この項では、Connection 固有の設定に従う必要がある重要なステップや手順について説明します。しかし、シングル サインオンの設定を初めて行う場合は、シスコのホワイト ペーパーに記載されている詳細な手順に従うことを強く推奨します。

- 「OpenAM サーバの設定」（P.7-35）
- 「シングル サインオンの CLI コマンドの実行」（P.7-36）

OpenAM サーバの設定

OpenAM サーバを設定するには、次の手順を実行する必要があります。

ステップ 1：OpenAM サーバ上のポリシーの設定

OpenAM サーバ上のポリシーを設定するには、OpenAM にログインして [アクセス コントロール（Access Control）] タブを選択する必要があります。[トップ レベル レルム（Top Level Realm）] オプションをクリックし、[ポリシー（Policies）] タブを選択して新しいポリシーを作成します。新しいポリシーの作成は、シスコのホワイト ペーパー（http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf）に記載されているステップに従ってください。また、ホワイト ペーパーの手順に従うと同時に、次のような Connection 固有の情報を持つポリシーを作成してください。

- ポリシーにルールを追加するときは、次の点を確認してください。
  - 各ルールは、URL ポリシー エージェント サービスのタイプである必要があります
  - 各ルールの GET および POST チェックボックスをオンにします
  - 次の各リソースに対してルールを作成します。「fqdn」は Connection サーバの完全修飾ドメイン名を示します。

    https://<fqdn>:8443/*

    https://<fqdn>:8443/*?*

    https://<fqdn>/*

    https://<fqdn>/*?*

    http://<fqdn>/*

    http://<fqdn>/*?*
- ポリシーにサブジェクトを追加するときは、次の点を確認してください。
  - [サブジェクトのタイプ（Subject Type）] フィールドが Authenticated Users であることを確認してください。
  - サブジェクト名を指定します
  - [排他的（Exclusive）] チェックボックスはオンにしないでください。
- ポリシーに条件を追加するときは、次の点を確認してください。
  - [条件（Condition）] のタイプを Active Session Time とします

- 条件名を指定します
- アクティブ セッション タイムアウトを 120 分に設定し、[セッション終了（Terminate Session）] オプションで [いいえ（No）] を選択します。

ステップ 2：Windows Desktop SSO ログイン モジュール インスタンスの設定

Windows Desktop の設定は、シスコのホワイト ペーパー（http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf）に記載されている手順に従ってください。

ステップ 3：Policy Agent 3.0 の J2EE Agent Profile の設定

新しい J2EE エージェントの作成は、シスコのホワイト ペーパー（http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf）に記載されている手順と、次の Connection 固有の設定に従ってください。

- エージェントのプロファイル名として示される名前は、Connection サーバ上で SSO がイネーブルである場合や、「Enter the name of the profile configured for this policy agent」というメッセージが表示された場合に入力する必要があります。
- ここで入力されるエージェント パスワードは、Connection サーバ上で「Enter the password of the profile name」というメッセージが表示された場合にも入力する必要があります。
- [アプリケーション（Application）] タブ上の [ログイン フォーム URI（Login Form URI）] セクションに次の URI を追加します。
  - cuadmin/WEB-INF/pages/logon.jsp
  - cuservice/WEB-INF/pages/logon.jsp
  - ciscopca/WEB-INF/pages/logon.jsp
  - inbox/WEB-INF/pages/logon.jsp
  - ccmservice/WEB-INF/pages/logon.jsp
- [アプリケーション（Application）] タブの下の [URI 処理を強制しない（Not Enforced URI Processing）] セクションに、次の URI を追加します。
  - inbox/gadgets/msg/msg-gadget.xml

上記の Connection 固有の設定の他に、次の点を確認してください。

- LDAP から Connection にユーザをインポートします。ユーザが Cisco Unity Connection Administration、または Cisco Unity Connection Serviceability にログインするには、適切な役割を設定されている必要があります。
- シスコのホワイト ペーパー（http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf）の「Configuring SSO on Cisco Unified Communications Manager 8.6」の項の説明に従って、OpenAM 証明書を Connection にアップロードします。

シングル サインオンの CLI コマンドの実行

次の各項では、シングル サインオンを設定する CLI コマンドについて説明します。

- utils sso enable
- utils sso disable
- utils sso status

詳細については、シスコのホワイト ペーパー（http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/miscellany/oam90-cucm8586-cuc86-sso.pdf）を参照してください。

- **utils sso enable**

utils sso コマンドは、SSO-based 認証のイネーブル化と設定に使用します。クラスタ内のすべてのノード上でこのコマンドを実行してください。

注意　Cisco Unity Connection へのシングル サインオンをイネーブルまたはディセーブルにすると、Web サーバ（Tomcat）が再起動します。

コマンド構文

utils sso enable

パラメータ

enable：SSO-based 認証をイネーブルにします。このコマンドにより、シングル サインオン設定ウィザードが開始されます。

- **utils sso disable**

このコマンドは、SSO-based 認証をディセーブルにします。また、SSO がイネーブルになっている Web アプリケーションをリスト表示します。指定されたアプリケーションのシングル サインオンをディセーブルにするよう求められた場合は、「Yes」と入力します。クラスタ内のすべてのノード上でこのコマンドを実行する必要があります。

コマンド構文

utils sso disable

- **utils sso status**

このコマンドにより、シングル サインオンのステータスおよび設定パラメータが表示されます。

コマンド構文

utils sso status

CHAPTER 8

Cisco Unity Connection 8.x セキュリティ パスワード

Cisco Unity Connection 8.x セキュリティ パスワードについて

Connection のインストール中に、他のユーザに関連付けられていないセキュリティ パスワードを指定します。このパスワードには 2 つの目的があります。

- Connection クラスタが設定されると、クラスタ内の 2 つのサーバが、データを複製する前にセキュリティ パスワードを使用して相互に認証します。クラスタ内の一方のサーバ上でセキュリティ パスワードを変更した場合、もう一方のサーバ上でもパスワードを変更する必要があります。また、この 2 つのサーバは、データやメッセージを複製することはできません。
- クラスタが設定されているかどうかにかかわらず、セキュリティ パスワードは、Disaster Recovery System の暗号キーとして使用されます。Connection サーバをバックアップし、セキュリティ パスワードを変更した後、バックアップからデータを復元しようとする場合は、サーバのバックアップを行ったときに有効だったセキュリティ パスワードを入力する必要があります。（現在のセキュリティ パスワードが、バックアップが行われたときのセキュリティ パスワードと一致する場合は、データを復元するためのパスワードを指定する必要はありません）。

セキュリティ パスワードを変更するには、**set password user** CLI コマンドを使用します。クラスタ内のサーバ上でパスワードを変更する手順など、詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 8.x*』の該当するバージョンを参照してください。このガイドは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。

CHAPTER 9

SSL を使用した、Cisco Unity Connection 8.x でのクライアント / サーバ接続の保護

この章では、証明書署名要求の作成、SSL 証明書の発行（または外部の認証局による発行）、証明書の Cisco Unity Connection サーバへのインストールによる Cisco Personal Communications Assistant（Cisco PCA）および IMAP 電子メール クライアントから Cisco Unity Connection へのアクセスの保護について説明します。

Cisco PCA の Web サイトでは、ユーザが Connection でのメッセージと個人設定の管理に使用できる、各種 Web ツールにアクセスできます。IMAP クライアントから Connection のボイス メッセージへのアクセスは、ライセンスが必要な機能です。

次の項を参照してください。

SSL 証明書をインストールして Cisco PCA および IMAP 電子メール クライアントから Cisco Unity Connection 8.x へのアクセスを保護するかどうかの決定

Cisco Unity Connection をインストールすると、ローカル証明書が自動的に作成され、インストールされて、Cisco PCA と Connection の間、および IMAP 電子メール クライアントと Connection の間の通信が保護されます。これは、Cisco PCA と Connection 間のすべてのネットワーク トラフィック（ユー

ザ名、パスワード、その他のテキスト データ、およびボイス メッセージを含む）が自動的に暗号化されることを意味します。また、IMAP クライアントで暗号化を有効にしている場合には、IMAP 電子メール クライアントと Connection 間のネットワーク トラフィックが自動的に暗号化されます。ただし、中間者攻撃のリスクを軽減する必要がある場合は、この章で説明する手順を実行してください。

SSL 証明書のインストールを決定した場合は、認証局の信頼証明書をユーザのワークステーションの信頼されたルート ストアに追加することも検討してください。この追加を行わないと、Cisco PCA にアクセスするユーザ、および一部の IMAP 電子メール クライアントで Connection のボイス メッセージにアクセスするユーザに対して、Web ブラウザでセキュリティ警告が表示されます。

（セキュリティ アラートの管理については、『*User Workstation Setup Guide for Cisco Unity Connection*』*(Release 8.x)*の「Setting Up Access to the Cisco Personal Communications Assistant」の章にある「Managing Security Alerts When Using Self-Signed Certificates with SSL Connections」の項を参照してください。サポートされる IMAP 電子メール クライアントの設定については、同じガイドの「Configuring an Email Account to Access Cisco Unity Connection Voice Messages」の章を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_setup/guide/8xcucuwsx.htm から入手可能です）。

Connection の管理、Cisco PCA、および IMAP 電子メール クライアントからの Cisco Unity Connection 8.x へのアクセスの保護

Cisco Unity Connection Administration、Cisco Personal Communications Assistant、および IMAP 電子メール クライアントから Cisco Unity Connection へのアクセスを保護するには、次のタスクを実行して、SSL サーバ証明書を作成し、インストールします。

1. Microsoft 証明書サービスを使用して証明書を発行する場合は、Microsoft 証明書サービスをインストールします。Windows Server 2003 を実行しているサーバに Microsoft 証明書サービスをインストールする方法については、「Microsoft 証明書サービスのインストール（Windows Server 2003 の場合のみ）」（P.9-53）を参照してください。それ以降のバージョンの Windows Server を実行しているサーバに Microsoft 証明書サービスをインストールする方法については、Microsoft 社のドキュメントを参照してください。

   別のアプリケーションを使用して証明書を発行する場合は、そのアプリケーションをインストールします。インストールの方法については、製造元が提供しているドキュメントを参照してください。その後で、タスク 2. に進みます。

   外部の認証局を使用して証明書を発行する場合は、タスク 2. に進みます。

（注）　Microsoft 証明書サービス、または証明書署名要求を作成できる別のアプリケーションをすでにインストールしてある場合は、タスク 2. に進みます。

2. Connection クラスタが設定されている場合は、`set web-security` CLI コマンドをクラスタ内の両方の Connection サーバで実行し、両方のサーバに同じユーザの別名を割り当てます。ユーザの別名は、証明書署名要求と証明書に、自動的に含められます。`set web-security` CLI コマンドについては、該当する『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このガイドは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。

3. Connection クラスタが設定されている場合は、タスク 2. で割り当てたユーザの別名を含んでいる DNS A レコードを設定します。まず、パブリッシャ サーバをリストしてください。それによって、すべての IMAP 電子メール アプリケーションおよび Cisco Personal Communications Assistant が、Connection のボイス メッセージに同じ Connection サーバ名を使用してアクセスできるようになります。

4. 証明書署名要求を作成します。その後で、Microsoft 証明書サービスまたは証明書を発行するその他のアプリケーションをインストールしたサーバに証明書署名要求をダウンロードするか、証明書署名要求を外部の CA に送る際に使用するサーバに要求をダウンロードします。「証明書署名要求を作成およびダウンロードするには」（P.9-43）の手順を行います。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

5. Microsoft 証明書サービスを使用してルート証明書のエクスポートおよびサーバ証明書の発行を行う場合は、「ルート証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスの場合のみ）」（P.9-54）の手順を実行します。

   証明書の発行に別のアプリケーションを使用する場合は、証明書の発行についてアプリケーションの資料を参照してください。

   証明書の発行に外部の CA を使用する場合は、外部の CA に証明書署名要求を送信します。外部 CA から証明書が返されたら、タスク 6. に進みます。

   Connection にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

6. ルート証明書とサーバ証明書を Connection サーバにアップロードします。「ルート証明書とサーバ証明書を Cisco Unity Connection サーバにアップロードするには」（P.9-44）の手順を行います。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

7. Connection IMAP サーバ サービスを再起動して、Connection および IMAP 電子メール クライアントが新しい SSL 証明書を使用するようにします。「Connection IMAP サーバ サービスを再起動するには」（P.9-45）の手順を行います。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

8. ユーザが Connection の管理、Cisco PCA、または IMAP 電子メール クライアントを使用して Connection にアクセスするたびにセキュリティ警告が表示されないようにするには、ユーザが Connection へのアクセスを行うすべてのコンピュータ上で、次のタスクを実行します。

   - タスク 6. で Connection サーバにアップロードしたサーバ証明書を証明書ストアにインポートします。手順は、使用するブラウザまたは IMAP 電子メール クライアントによって異なります。詳細については、ブラウザまたは IMAP 電子メール クライアントのドキュメントを参照してください。
   - タスク 6. で Connection サーバにアップロードしたサーバ証明書を Java ストアにインポートします。手順は、クライアント コンピュータ上で実行されているオペレーティング システムによって異なります。詳細については、オペレーティング システムのドキュメントおよび Java ランタイム環境のドキュメントを参照してください。

証明書署名要求を作成およびダウンロードするには

ステップ 1　Cisco Unity Connection サーバで Cisco Unified Operating System Administration にサインインします。

ステップ 2　[セキュリティ（Security）] メニューで [証明書の管理（Certificate Management）] を選択します。

ステップ 3　[証明書の一覧（Certificate List）] ページで、[CSR の作成（Generate CSR）] を選択します。

ステップ 4　[証明書署名要求の作成（Generate Certificate Signing Request）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat] を選択します。

ステップ 5　[CSR の作成（Generate CSR）] を選択します。

ステップ 6　CSR が正常に生成されたことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 7　[証明書の一覧（Certificate List）] ページで、[CSR のダウンロード（Download CSR）] を選択します。

ステップ 8　[証明書署名要求のダウンロード（Download Certificate Signing Request）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat] を選択します。

ステップ 9　[CSR のダウンロード（Download CSR）] を選択します。

ステップ 10　[ファイルのダウンロード（File Download）] ダイアログボックスで、[保存（Save）] を選択します。

ステップ 11　[名前を付けて保存（Save As）] ダイアログボックスの [保存の種類（Save As Type）] リストで、[すべてのファイル（All Files）] を選択します。

ステップ 12　**tomcat.csr** ファイルを、Microsoft 証明書サービスをインストールしたサーバ、または外部の認証局に CSR を送信するのに使用できるサーバ上の場所に保存します。

ステップ 13　[証明書署名要求のダウンロード（Download Certificate Signing Request）] ページで、[閉じる（Close）] を選択します。

ルート証明書とサーバ証明書を Cisco Unity Connection サーバにアップロードするには

ステップ 1　証明書署名要求を作成した Cisco Unity Connection サーバで、Cisco Unified Operating System Administration にサインインします。

ステップ 2　[セキュリティ（Security）] メニューで [証明書の管理（Certificate Management）] を選択します。

（注）　[検索（Find）] を選択し、現在そのサーバにインストールされている証明書のリストを表示すると、既存の、自動的に生成された、Tomcat の自己署名証明書が表示されます。この証明書は、この手順でアップロードする Tomcat 証明書とは関係のないものです。

ステップ 3　ルート証明書をアップロードします。

a.　[証明書の一覧（Certificate List）] ページで、[証明書のアップロード（Upload Certificate）] を選択します。

b.　[証明書のアップロード（Upload Certificate）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat-trust] を選択します。

c.　[ルート証明書（Root Certificate）] フィールドは空白のままにします。

d.　[参照（Browse）] を選択して、ルート CA 証明書の場所を参照します。

証明書の発行に Microsoft 証明書サービスを使用した場合は、「ルート証明書をエクスポートし、サーバ証明書を発行するには」（P.9-54）の手順でエクスポートしたルート証明書がこの場所に保存されます。

証明書の発行に外部の認証局を使用した場合は、外部の認証局から受け取ったルート CA 証明書がこの場所に保存されます。

e. ファイルの名前を選択します。

f. [開く（Open）] を選択します。

g. [証明書のアップロード（Upload Certificate）] ページで、[ファイルのアップロード（Upload File）] を選択します。

h. アップロードに成功したことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 4　サーバ証明書をアップロードします。

a. [証明書の一覧（Certificate List）] ページで、[証明書のアップロード（Upload Certificate）] を選択します。

b. [証明書のアップロード（Upload Certificate）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat] を選択します。

c. [ルート証明書（Root Certificate）] フィールドに、ステップ 3 でアップロードしたルート証明書のファイル名を入力します。

d. [参照（Browse）] を選択して、サーバ証明書の場所を参照します。

証明書の発行に Microsoft 証明書サービスを使用した場合は、「ルート証明書をエクスポートし、サーバ証明書を発行するには」（P.9-54）の手順で発行したサーバ証明書がこの場所に保存されます。

証明書の発行に外部の認証局を使用した場合は、外部の認証局から受け取ったサーバ証明書がこの場所に保存されます。

e. ファイルの名前を選択します。

f. [開く（Open）] を選択します。

g. [証明書のアップロード（Upload Certificate）] ページで、[ファイルのアップロード（Upload File）] を選択します。

h. アップロードに成功したことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 5　Tomcat サービスを再起動します（このサービスは Cisco Unified Serviceability からは再起動できません）。

a. SSH アプリケーションを使用して Connection サーバにサインインします。

b. 次の CLI コマンドを使用して Tomcat サービスを再起動します。

```
utils service restart Cisco Tomcat
```

Connection IMAP サーバ サービスを再起動するには

ステップ 1　Cisco Unity Connection Serviceability にログインします。

ステップ 2　[ツール（Tools）] メニューで [サービス管理（Service Management）] を選択します。

ステップ 3　[オプション サービス（Optional Services）] セクションで、Connection IMAP サーバ サービスに [停止（Stop）] を選択します。

ステップ 4　Connection IMAP サーバ サービスが正常に停止したことを示すメッセージがステータス エリアに表示されたら、このサービスに [開始（Start）] を選択します。

Exchange の予定表、連絡先、および電子メールへのアクセスの保護

Exchange の予定表、連絡先、および電子メールへのアクセスの保護については、次の該当するマニュアルを参照してください。

- *（Cisco Unity Connection 8.5 以降）『Unified Messaging Guide for Cisco Unity Connection Release 8.5 and Later』*の「Configuring Cisco Unity Connection 8.5 and Later and Microsoft Exchange for Unified Messaging」の章。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/unified_messaging/guide/85xcucumgx.html から入手可能です。
- *（Cisco Unity Connection 8.0）『System Administration Guide for Cisco Unity Connection Release 8.x』*の「Configuring Text-to-Speech Access to Exchange Emails in Cisco Unity Connection 8.0」の章または「Creating Calendar and Contact Integrations in Cisco Unity Connection 8.0」の章。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html から入手可能です。

Cisco Unified MeetingPlace へのアクセスの保護

MeetingPlace へのアクセスを保護するには、次のタスクを実行します。

1. MeetingPlace 用に SSL を設定します。詳細については、*『Administration Documentation for Cisco Unified MeetingPlace Release 8.0』*の「Configuring SSL for the Cisco Unified MeetingPlace Application Server」の章を参照してください。このガイドは、http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_maintenance_guides_list.html から入手可能です。
2. Connection と MeetingPlace を連動させます。Connection を MeetingPlace の予定表と連動するように設定するときには、セキュリティ トランスポート用に SSL を指定します。

   詳細については、該当するマニュアルを参照してください。

   - *（Connection 8.5 以降）『Unified Messaging Guide for Cisco Unity Connection Release 8.5 and Later』*の「Configuring Cisco Unity Connection 8.5 and Later and Cisco Unified MeetingPlace for Unified Messaging」の章。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/unified_messaging/guide/85xcucumgx.html から入手可能です。
   - *（Connection 8.0）『System Administration Guide for Cisco Unity Connection Release 8.x』*の「Creating Calendar and Contact Integrations in Cisco Unity Connection 8.0」の章の「Creating a Calendar and Contact Integration with Cisco Unified MeetingPlace」の項。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html から入手可能です。
3. Connection サーバで、タスク 1. で MeetingPlace サーバにインストールしたサーバ証明書の入手元認証局のルート証明書をアップロードします。次の点に注意してください。
   - このルート証明書は、MeetingPlace サーバにインストールした証明書と同じものではありません。認証局のルート証明書には、MeetingPlace サーバにアップロードした証明書の信頼性を確認するのに使用できる、公開キーが含まれています。

- Connection にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。
- ルート証明書のファイル名には、スペースを含めることはできません。

ルート証明書を Connection サーバにアップロードするには

ステップ 1　管理者のアカウントとパスワードを使用して、Cisco Unified Operating System Administration にサインインします。

Connection のインストール時に作成した管理者アカウントは、Connection の管理 へのサインインに使用するアカウントおよびパスワードとは異なります。

ステップ 2　[セキュリティ（Security）] メニューで [証明書の管理（Certificate Management）] を選択します。

ステップ 3　[証明書のアップロード（Upload Certificate）] を選択します。

ステップ 4　[証明書の名前（Certificate Name）] リストで、[Connection-trust] を選択します。

ステップ 5　[参照（Browse）] を選択し、MeetingPlace 用の証明書を発行した認証局のルート証明書が含まれているファイルを見つけます。

ステップ 6　[ファイルのアップロード（Upload File）] を選択します。

Cisco Unified MeetingPlace Express（Cisco Unity Connection 8.0 のみ）へのアクセスの保護

（注） Cisco Unity Connection 8.5 以降では、Cisco Unified MeetingPlace Express との統合はサポートされていません。

MeetingPlace Express へのアクセスを保護するには、次のタスクを実行します。

1. MeetingPlace Express 用に SSL を設定します。詳細については、次のマニュアルを参照してください。
   a. http://docwiki.cisco.com/wiki/Cisco_Unified_MeetingPlace_Express%2C_Release_2.x にある DocWiki、『Cisco Unified MeetingPlace Express, Release 2.x』を表示します。
   b. 「Configuration and Maintenance Tasks」の「Configuring SSL and Managing Certificates for Cisco Unified MeetingPlace Express」を選択します。
2. Cisco Unity Connection と MeetingPlace Express を連動させます。Connection を MeetingPlace Express の予定表と連動するように設定するときには、セキュリティ トランスポート用に SSL を指定します。『*System Administration Guide for Cisco Unity Connection Release 8.x*』の「Creating Calendar and Contact Integrations in Cisco Unity Connection 8.0」の章の「Creating a Calendar and Contact Integration with Cisco Unified MeetingPlace Express」の項を参照してください。このガイドは、http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html から入手可能です。
3. Connection サーバで、タスク 1. で MeetingPlace Express サーバにインストールしたサーバ証明書の入手元認証局のルート証明書をアップロードします。次の点に注意してください。

- このルート証明書は、MeetingPlace Express サーバにインストールした証明書と同じものではありません。認証局のルート証明書には、MeetingPlace Express サーバにアップロードした証明書の信頼性を確認するのに使用できる、公開キーが含まれています。
- Connection にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。
- ルート証明書のファイル名には、スペースを含めることはできません。

ルート証明書を Connection サーバにアップロードするには

ステップ 1　管理者のアカウントとパスワードを使用して、Cisco Unified Operating System Administration にサインインします。

Connection のインストール時に作成した管理者アカウントは、Connection の管理 へのサインインに使用するアカウントおよびパスワードとは異なります。

ステップ 2　[セキュリティ（Security）] メニューで [証明書の管理（Certificate Management）] を選択します。

ステップ 3　[証明書のアップロード（Upload Certificate）] を選択します。

ステップ 4　[証明書の名前（Certificate Name）] リストで、[Connection-trust] を選択します。

ステップ 5　[参照（Browse）] を選択し、MeetingPlace 用の証明書を発行した認証局のルート証明書が含まれているファイルを見つけます。

ステップ 6　[ファイルのアップロード（Upload File）] を選択します。

LDAP ディレクトリへのアクセスの保護

LDAP サーバおよび Cisco Unity Connection 間で転送されるデータの保護については、*System Administration Guide for Cisco Unity Connection*（Release 8.x）（http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html）の「Integrating Cisco Unity Connection 8.x with an LDAP Directory」の章にある「Uploading SSL Certificates on the Cisco Unity Connection Server」の項を参照してください。

Connection ネットワーキングが設定されている場合の、Connection と Cisco Unity ゲートウェイ サーバの間の通信の保護

Connection の管理、Cisco Personal Communications Assistant、および IMAP 電子メール クライアントから Cisco Unity Connection へのアクセスを保護するには、次のタスクを実行して、SSL サーバ証明書を作成し、インストールします。

1. Microsoft 証明書サービスを使用して証明書を発行する場合は、Microsoft 証明書サービスをインストールします。Windows Server 2003 を実行しているサーバに Microsoft 証明書サービスをインストールする方法については、「Microsoft 証明書サービスのインストール（Windows Server 2003

の場合のみ）」（P.9-53）を参照してください。それ以降のバージョンの Windows Server を実行しているサーバに Microsoft 証明書サービスをインストールする方法については、Microsoft 社のドキュメントを参照してください。

別のアプリケーションを使用して証明書を発行する場合は、そのアプリケーションをインストールします。インストールの方法については、製造元が提供しているドキュメントを参照してください。その後で、タスク 2. に進みます。

外部の認証局を使用して証明書を発行する場合は、タスク 2. に進みます。

（注）　Microsoft 証明書サービス、または証明書署名要求を作成できる別のアプリケーションをすでにインストールしてある場合は、タスク 2. に進みます。

2. Connection クラスタが Connection ゲートウェイ サーバ用に構成されている場合は、`set web-security` CLI コマンドをクラスタ内の両方の Connection サーバで実行し、両方のサーバに同じユーザの別名を割り当てます。ユーザの別名は、証明書署名要求と証明書に、自動的に含められます。`set web-security` CLI コマンドについては、該当する『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このガイドは、http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html から入手可能です。

3. Connection クラスタが Connection ゲートウェイ サーバ用に設定されている場合は、タスク 2. で割り当てたユーザの別名を含んでいる DNS A レコードを設定します。まず、パブリッシャ サーバをリストしてください。それによって、Cisco Unity は、Connection ボイス メッセージに同じ Connection サーバ名を使用してアクセスできるようになります。

4. Connection ゲートウェイ サーバで、証明書署名要求を作成します。その後で、Microsoft 証明書サービスまたは証明書を発行するその他のアプリケーションをインストールしたサーバに証明書署名要求をダウンロードするか、証明書署名要求を外部の CA に送る際に使用するサーバに要求をダウンロードします。「Connection ゲートウェイ サーバで証明書署名要求を作成し、ダウンロードするには」（P.9-50）の手順を行います。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

5. Cisco Unity ゲートウェイ サーバで、証明書署名要求を作成します。その後で、Microsoft 証明書サービスまたは証明書を発行するその他のアプリケーションをインストールしたサーバに証明書署名要求をダウンロードするか、証明書署名要求を外部の CA に送る際に使用するサーバに要求をダウンロードします。「Cisco Unity ゲートウェイ サーバで証明書署名要求を作成し、ダウンロードするには」（P.9-51）の手順を行います。

   Cisco Unity フェールオーバーが設定されている場合は、このタスクをプライマリ サーバとセカンダリ サーバに対して実行します。

6. Microsoft 証明書サービスを使用してルート証明書のエクスポートおよびサーバ証明書の発行を行う場合は、「ルート証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスの場合のみ）」（P.9-54）の手順を実行します。

   証明書の発行に別のアプリケーションを使用する場合は、証明書の発行についてアプリケーションの資料を参照してください。

   外部の CA を使用して証明書を発行する場合は、証明書署名要求をその外部 CA に送信します。外部 CA から証明書が返されたら、タスク 7. に進みます。

   Connection にアップロードできるのは、PEM 形式（Base-64 エンコードされた DER）の証明書だけです。証明書のファイル名拡張子は .pem であることが必要です。証明書がこの形式でない場合、通常は、OpenSSL など、無償で使用できるユーティリティを使用して PEM 形式に変換できます。

このタスクを、Connection サーバ（Connection クラスタが設定されている場合は両方のサーバ）と Cisco Unity サーバ（フェールオーバーが設定されている場合は両方のサーバ）に対して実行します。

7. ルート証明書とサーバ証明書を Connection サーバにアップロードします。「ルート証明書とサーバ証明書を Cisco Unity Connection サーバにアップロードするには」（P.9-44）の手順を行います。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

8. Connection IMAP サーバ サービスを再起動して、Connection および IMAP 電子メール クライアントが新しい SSL 証明書を使用するようにします。「Connection IMAP サーバ サービスを再起動するには」（P.9-45）の手順を行います。

   Connection クラスタが設定されている場合は、Connection クラスタ内の両方のサーバに対してこのタスクを実行します。

9. ルート証明書とサーバ証明書を Cisco Unity サーバにアップロードします。「ルート証明書とサーバ証明書を Cisco Unity サーバにアップロードするには」（P.9-53）の手順を行います。

   フェールオーバーが設定されている場合は、このタスクをプライマリ サーバとセカンダリ サーバに対して実行します。

Connection ゲートウェイ サーバで証明書署名要求を作成し、ダウンロードするには

ステップ 1　Cisco Unity Connection サーバで Cisco Unified Operating System Administration にサインインします。

ステップ 2　[セキュリティ（Security）] メニューで [証明書の管理（Certificate Management）] を選択します。

ステップ 3　[証明書の一覧（Certificate List）] ページで、[CSRCritical Services の作成（Generate CSR）] を選択します。

ステップ 4　[証明書署名要求の作成（Generate Certificate Signing Request）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat] を選択します。

ステップ 5　[CSR の作成（Generate CSR）] を選択します。

ステップ 6　CSR が正常に生成されたことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 7　[証明書の一覧（Certificate List）] ページで、[CSR のダウンロード（Download CSR）] を選択します。

ステップ 8　[証明書署名要求のダウンロード（Download Certificate Signing Request）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat] を選択します。

ステップ 9　[CSR のダウンロード（Download CSR）] を選択します。

ステップ 10　[ファイルのダウンロード（File Download）] ダイアログボックスで、[保存（Save）] を選択します。

ステップ 11　[名前を付けて保存（Save As）] ダイアログボックスの [保存の種類（Save As Type）] リストで、[すべてのファイル（All Files）] を選択します。

ステップ 12　**tomcat.csr** ファイルを、Microsoft 証明書サービスをインストールしたサーバ、または外部の認証局に CSR を送信するのに使用できるサーバ上の場所に保存します。

ステップ 13　[証明書署名要求のダウンロード（Download Certificate Signing Request）] ページで、[閉じる（Close）] を選択します。

Cisco Unity ゲートウェイ サーバで証明書署名要求を作成し、ダウンロードするには

ステップ 1　Windows の [スタート（Start）] メニューで、[プログラム（Programs）] > [管理ツール（Administrative Tools）] > [インターネット インフォメーション サービス（IIS）マネージャ（Internet Information Services (IIS) Manager）] を選択します。

ステップ 2　Cisco Unity サーバ名を展開します。

ステップ 3　[Web サイト（Web Sites）] を展開します。

ステップ 4　[既定の Web サイト（Default Web Site）] を右クリックし、[プロパティ（Properties）] を選択します。

ステップ 5　[既定の Web サイト プロパティ（Default Web Site Properties）] ダイアログボックスで、[ディレクトリのセキュリティ（Directory Security）] タブを選択します。

ステップ 6　[セキュアな通信（Secure Communications）] の [サーバー証明書（Server Certificate）] を選択します。

ステップ 7　Web サーバ証明書ウィザード（Web Server Certificate Wizard）で、次の手順を実行します。

a. [次へ（Next）] を選択します。

b. [新しい証明書の作成（Create a New Certificate）] を選択し、[次へ（Next）] を選択します。

c. [要求を今用意し、後で送信する（Prepare the Request Now, But Send It Later）] を選択し、[次へ（Next）] を選択します。

d. 証明書の名前と長さ（ビット）を入力します。

512 ビットの長さを選択することを強く推奨します。ビット長を大きくすると、パフォーマンスが低下する可能性があります。

e. [次へ（Next）] を選択します。

f. 組織の情報を入力し、[次へ（Next）] を選択します。

g. サイトの通常名として、Cisco Unity サーバのシステム名または完全修飾ドメイン名を入力します。

注意　この名前は、Connection サイト ゲートウェイ サーバが Cisco Unity サーバにアクセスするために URL を構築するのに使用する名前と正確に一致する必要があります。この名前は、Connection Administration の [ネットワーク（Networking）] > [リンク（Links）] > [サイト間リンク（Intersite Links）] ページの [ホスト名（Hostname）] フィールドの値です。

h. [次へ（Next）] を選択します。

i. 地理情報を入力し、[次へ（Next）] を選択します。

j. 証明書要求のファイル名と場所を指定します。このファイル名と場所の情報は次の手順で必要となるので、書き留めてください。

k. ファイルは、ディスク、または認証局（CA）のサーバがアクセスできるディレクトリに保存します。

l. [次へ（Next）] を選択します。

m. 要求ファイルの情報を確認し、[次へ（Next）] を選択します。

n. [終了（Finish）] を選択して、Web サーバ証明書ウィザード（Web Server Certificate Wizard）を終了します。

ステップ 8　[OK] をクリックして、[既定の Web サイト プロパティ（Default Web Site Properties）] ダイアログボックスを閉じます。

ステップ 9　[インターネット インフォメーション サービス マネージャ（Internet Information Services Manager）] ウィンドウを閉じます。

ルート証明書とサーバ証明書を Cisco Unity Connection サーバにアップロードするには

ステップ 1　証明書署名要求を作成した Cisco Unity Connection サーバで、Cisco Unified Operating System Administration にサインインします。

ステップ 2　[セキュリティ（Security）] メニューで [証明書の管理（Certificate Management）] を選択します。

（注）　[検索（Find）] を選択し、現在そのサーバにインストールされている証明書のリストを表示すると、既存の、自動的に生成された、Tomcat の自己署名証明書が表示されます。この証明書は、この手順でアップロードする Tomcat 証明書とは関係のないものです。

ステップ 3　ルート証明書をアップロードします。

a. [証明書の一覧（Certificate List）] ページで、[証明書のアップロード（Upload Certificate）] を選択します。

b. [証明書のアップロード（Upload Certificate）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat-trust] を選択します。

c. [ルート証明書（Root Certificate）] フィールドは空白のままにします。

d. [参照（Browse）] を選択して、ルート CA 証明書の場所を参照します。

証明書の発行に Microsoft 証明書サービスを使用した場合は、「ルート証明書をエクスポートし、サーバ証明書を発行するには」（P.9-54）の手順でエクスポートしたルート証明書がこの場所に保存されます。

証明書の発行に外部の認証局を使用した場合は、外部の認証局から受け取ったルート CA 証明書がこの場所に保存されます。

e. ファイルの名前を選択します。

f. [開く（Open）] を選択します。

g. [証明書のアップロード（Upload Certificate）] ページで、[ファイルのアップロード（Upload File）] を選択します。

h. アップロードに成功したことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 4　サーバ証明書をアップロードします。

a. [証明書の一覧（Certificate List）] ページで、[証明書のアップロード（Upload Certificate）] を選択します。

b. [証明書のアップロード（Upload Certificate）] ページの [証明書の名前（Certificate Name）] リストで、[tomcat] を選択します。

c. [ルート証明書（Root Certificate）] フィールドに、ステップ 3 でアップロードしたルート証明書のファイル名を入力します。

d. [参照（Browse）] を選択して、サーバ証明書の場所を参照します。

証明書の発行に Microsoft 証明書サービスを使用した場合は、「ルート証明書をエクスポートし、サーバ証明書を発行するには」（P.9-54）の手順で発行したサーバ証明書がこの場所に保存されます。

証明書の発行に外部の認証局を使用した場合は、外部の認証局から受け取ったサーバ証明書がこの場所に保存されます。

e. ファイルの名前を選択します。

f. [開く（Open）] を選択します。

g. [証明書のアップロード（Upload Certificate）] ページで、[ファイルのアップロード（Upload File）] を選択します。

h. アップロードに成功したことを示すメッセージがステータス エリアに表示されたら、[閉じる（Close）] を選択します。

ステップ 5　Tomcat サービスを再起動します（このサービスは Cisco Unified Serviceability からは再起動できません）。

a. SSH アプリケーションを使用して Connection サーバにサインインします。

b. 次の CLI コマンドを使用して Tomcat サービスを再起動します。

```
utils service restart Cisco Tomcat
```

Connection IMAP サーバ サービスを再起動するには

ステップ 1　Cisco Unity Connection Serviceability にログインします。

ステップ 2　[ツール（Tools）] メニューで [サービス管理（Service Management）] を選択します。

ステップ 3　[オプション サービス（Optional Services）] セクションで、Connection IMAP サーバ サービスに [停止（Stop）] を選択します。

ステップ 4　Connection IMAP サーバ サービスが正常に停止したことを示すメッセージがステータス エリアに表示されたら、このサービスに [開始（Start）] を選択します。

ルート証明書とサーバ証明書を Cisco Unity サーバにアップロードするには

ステップ 1　Cisco Unity サーバで、コンピュータ アカウントの証明書 MMC をインストールします。

ステップ 2　証明書をアップロードします。詳細については、Microsoft 社のドキュメントを参照してください。

Microsoft 証明書サービスのインストール（Windows Server 2003 の場合のみ）

サードパーティの認証局を使用して SSL 証明書を発行する場合や、Microsoft 証明書サービスがすでにインストールされている場合は、この項の手順を省略してください。

Microsoft 証明書サービスを使用して独自の証明書を発行する場合で、Windows Server 2003 を実行しているサーバにこのアプリケーションをインストールする場合に、この項の手順を実行します。

ルート認証局（Microsoft 証明書サービスの一般的な名称）を Windows Server 2008 サーバにインストールする場合は、Windows Server 2008 のオンライン ヘルプを参照してください。

Microsoft 証明書サービス コンポーネントをインストールするには

ステップ 1　Cisco PCA を使用するすべてのクライアント コンピュータ、または IMAP クライアントを使用して Cisco Unity Connection のボイス メッセージにアクセスするすべてのクライアント コンピュータで解決できる DNS 名（FQDN）または IP アドレスを持つサーバ上で、ローカル Administrators グループのメンバであるアカウントを使用して Windows にサインインします。

ステップ 2　Windows の [スタート（Start）] メニューで、[設定（Settings）] > [コントロール パネル（Control Panel）] > [プログラムの追加と削除（Add or Remove Programs）] を選択します。

ステップ 3　[プログラムの追加と削除（Add or Remove Programs）] の左側のパネルで、[Windows コンポーネントの追加と削除（Add/Remove Windows Components）] を選択します。

ステップ 4　[Windows コンポーネント（Windows Components）] ダイアログボックスで、[証明書サービス（Certificate Services）] チェックボックスをオンにします。他の項目は変更しないでください。

ステップ 5　コンピュータ名の変更やドメイン メンバーシップの変更ができないことを通知する警告が表示されたら、[はい（Yes）] を選択します。

ステップ 6　[次へ（Next）] を選択します。

ステップ 7　[CA の種類（CA Type）] ページで、[スタンドアロンのルート CA（Stand-alone Root CA）] を選択し、[次へ（Next）] を選択します。（スタンドアロンの認証局（CA）とは、Active Directory を必要としない CA です）。

ステップ 8　[CA の ID 情報（CA Identifying Information）] ページの [この CA の通常名（Common Name for This CA）] フィールドに、認証局の名前を入力します。

ステップ 9　[識別名サフィックス（Distinguished Name Suffix）] フィールドで、デフォルトの値を受け入れます。

ステップ 10　有効期間として、デフォルト値の [5 年（5 Years）] を受け入れます。

ステップ 11　[次へ（Next）] を選択します。

ステップ 12　[証明書データベース設定（Certificate Database Settings）] ページで、[次へ（Next）] を選択してデフォルト値を受け入れます。

インターネット インフォメーション サービスがコンピュータ上で実行されており、先に進むにはこのサービスを停止する必要があることを通知するメッセージが表示されたら、[はい（Yes）] を選択してこのサービスを停止します。

ステップ 13　Windows Server 2003 のディスクをドライブに挿入するように求められたら、そのように実行します。

ステップ 14　[Windows コンポーネントの完了ウィザード（Completing the Windows Components Wizard）] ダイアログボックスで、[終了（Finish）] を選択します。

ステップ 15　[プログラムの追加と削除（Add or Remove Programs）] ダイアログボックスを閉じます。

ルート証明書のエクスポートとサーバ証明書の発行（Microsoft 証明書サービスの場合のみ）

Microsoft 証明書サービスを使用して証明書を発行する場合だけ、次の手順を実行します。

ルート証明書をエクスポートし、サーバ証明書を発行するには

ステップ 1　Microsoft 証明書サービスをインストールしたサーバで、Domain Admins グループのメンバであるアカウントを使用して Windows にサインインします。

ステップ 2　Windows の [スタート（Start）] メニューで、[プログラム（Programs）] > [管理ツール（Administrative Tools）] > [証明機関（Certification Authority）] を選択します。

ステップ 3　左側のパネルで、[認証局（ローカル）（Certification Authority (Local)）] > **<認証局の名前>** を展開します。<認証局の名前> は、「Microsoft 証明書サービス コンポーネントをインストールするには」（P.9-54）の手順で Microsoft 証明書サービスをインストールしたときに認証局に付けた名前になります。

ステップ 4　ルート証明書をエクスポートします。

a. 認証局の名前を右クリックし、[プロパティ（Properties）] を選択します。

b. [全般（General）] タブで、[証明書の表示（View Certificate）] を選択します。

c. [詳細（Details）] タブを選択します。

d. [ファイルのコピー（Copy to File）] を選択します。

e. [証明書のエクスポート ウィザードの開始（Welcome to the Certificate Export Wizard）] ページで、[次へ（Next）] を選択します。

f. [エクスポート ファイルの形式（Export File Format）] ページで [次へ（Next）] をクリックして、デフォルト値 [DER Encoded Binary X.509 (.CER)] を受け入れます。

g. [エクスポートするファイル（File to Export）] ページで、.cer ファイルのパスとファイル名を入力します。Connection サーバからアクセス可能なネットワーク上の場所を選択します。

パスとファイル名を書き留めます。この情報は後の手順で必要になります。

h. ウィザードでエクスポートが完了するまで、画面に表示される指示に従って操作します。

i. [OK] を選択して [証明書（Certificate）] ダイアログボックスを閉じ、もう一度 [OK] を選択して [プロパティ（Properties）] ダイアログボックスを閉じます。

ステップ 5　サーバ証明書を発行します。

a. 認証局の名前を右クリックし、[すべてのタスク（All Tasks）] > [新しい要求の送信（Submit New Request）] を選択します。

b. 「証明書署名要求を作成およびダウンロードするには」（P.9-43）の手順 で作成した証明書署名要求ファイルの場所に移動し、このファイルをダブルクリックします。

c. [認証局（Certification Authority）] の左側のパネルで [保留中の要求（Pending Requests）] を選択します。

d. b. で送信した保留中の要求を右クリックし、[すべてのタスク（All Tasks）] > [発行（Issue）] を選択します。

e. [認証局（Certification Authority）] の左側のパネルで [発行済み証明書（Issued Certificates）] を選択します。

f. 新しい証明書を右クリックし、[すべてのタスク（All Tasks）] > [バイナリ データのエクスポート（Export Binary Data）] を選択します。

g. [バイナリ データのエクスポート（Export Binary Data）] ダイアログボックスの [バイナリ データが含まれている列（Columns that Contain Binary Data）] リストで、[バイナリ証明書（Binary Certificate）] を選択します。

h. [バイナリ データをファイルに保存（Save Binary Data to a File）] を選択します。

i. [OK] を選択します。

j. [バイナリ データの保存（Save Binary Data）] ダイアログボックスで、パスとファイル名を入力します。Cisco Unity Connection サーバからアクセス可能なネットワーク上の場所を選択します。

パスとファイル名を書き留めます。この情報は後の手順で必要になります。

k. [OK] を選択します。

ステップ 6　[認証局（Certification Authority）] を閉じます。

CHAPTER 10

Cisco Unity Connection 8.x でのユーザ メッセージの保護

ユーザは、メッセージの機密性を設定することで、ボイス メッセージにアクセスできる人や、そのボイス メッセージを他の人に再配信できるかどうかを制御できます。Cisco Unity Connection には、ユーザがボイス メッセージを WAV ファイルとしてハード ドライブ、または Connection サーバ外の他の場所に保存することを防止する機能もあります。この機能を使用すると、メッセージをアーカイブまたは消去するまでそれらのメッセージを保持する期間を制御できます。Connection はまた、メッセージのセキュアな削除を管理するためのメソッドを提供します。

次の項を参照してください。

- 「プライベートまたはセキュアとマークされたメッセージが Cisco Unity Connection 8.x で処理される方法」（P.10-57）
- 「すべてのメッセージをセキュアとしてマークするための Cisco Unity Connection の設定」（P.10-60）
- 「すべてのボイス メッセージに対する、Cisco Unity Connection 8.0 Messaging Inbox の [名前を付けて保存（Save Recording As）] オプションのディセーブル化」（P.10-62）
- 「セキュアな削除のためのメッセージ ファイルの破棄（Cisco Unity Connection 8.5 以降のみ）」（P.10-62）
- 「Cisco Unity Connection 8.x での IMAP クライアント アクセスのメッセージ セキュリティ オプション」（P.10-64）

プライベートまたはセキュアとマークされたメッセージが Cisco Unity Connection 8.x で処理される方法

ユーザが電話を使用して Cisco Unity Connection でメッセージを送信するときには、そのメッセージをプライベート、セキュア、またはその両方としてマークできます。また、外部の発信者が残したメッセージを Connection でプライベート、セキュア、またはその両方としてマークするかどうかも指定できます。

プライベート メッセージ

- すべての受信者が、Connection ユーザ以外も含め、プライベート メッセージを受信できます。受信者は、電話、Connection Messaging Inbox（Connection 8.0 の場合）または Connection Web Inbox（8.5 以降の場合）、ViewMail for Outlook、ViewMail for Notes、Cisco Unified Personal Communicator、Cisco Unified Messaging with IBM Lotus Sametime、または IMAP クライアントを使用して、プライベート メッセージを聞くことができます。

- プライベート メッセージは、電話での転送、Messaging Inbox（Connection 8.0 の場合）または Web Inbox（8.5 以降の場合）からの転送、ViewMail for Outlook または ViewMail for Notes からの転送はできません。
- プライベート メッセージに IMAP クライアントからアクセスする場合、別途指定しない限り、プライベート メッセージを WAV ファイルとして転送したりローカルの場所に保存したりできます。(ユーザがプライベート メッセージを再生および転送できないようにする方法や、プライベート メッセージを WAV ファイルとして保存できないようにする方法については、「Cisco Unity Connection 8.x での IMAP クライアント アクセスのメッセージ セキュリティ オプション」（P.10-64）を参照してください)。
- ユーザがプライベート メッセージに応答するときには、プライベートとしてマークされます。
- ユーザがメッセージを送信するときに、そのメッセージをプライベートとしてマークするかどうかを選択できます。
- システムにプライベート メッセージ用のメッセージ配信と機密性オプションが設定されている場合は、外部の発信者がメッセージを残すときに、そのメッセージをプライベートとしてマークできません。(Connection 8.6 以降のみで利用できます)。
- ユーザが他のユーザにメッセージを残す前に、そのユーザのメールボックスに明示的にサインインしない場合は、メッセージをプライベートとしてマークできます（システムにこのオプションが設定されている場合)。
- デフォルトでは、Connection は、SMTP リレー アドレスにメッセージをリレーする 1 つ以上のメッセージ操作が設定されているユーザに対して、プライベート メッセージ（プライベート フラグの付いた通常のメッセージ）をリレーします。プライベート メッセージのリレーを無効にするには、Cisco Unity Connection Administration の [システム設定（System Settings）] > [詳細設定（Advanced）] > [メッセージング（Messaging）] ページの [プライベート メッセージのリレーを許可する（Allow Relaying of Private Messages）] チェックボックスをオフにします。

セキュア メッセージ

- セキュア メッセージは Connection サーバにだけ保存されるため、アーカイブまたは完全に削除されるまで保持される期間を制御できます。セキュア メッセージについては、Connection Messaging Inbox（Connection 8.0)、Cisco Unity Connection ViewMail for Microsoft Outlook（バージョン 8.0)、および Cisco Unity Connection ViewMail for IBM Lotus Notes の Media Master の [オプション（Options）] メニューで、[名前を付けて保存（Save Recording As）] オプションが自動的に無効になります。
- セキュア メッセージは、メッセージ保持ポリシーを強制的に適用するのに便利です。ユーザがそのセキュア メッセージを再生したか、その他の方法で処理したかどうかに関係なく、指定した日数を超えたセキュア メッセージを自動的に削除するように、Connection を設定できます。詳細については、『*System Administration Guide for Cisco Unity Connection*』*(Release 8.x)*（http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html から入手可能）の「Controlling the Size of Mailboxes in Cisco Unity Connection 8.x」の章にある「Managing Message Aging Policies in Cisco Unity Connection 8.x」の項を参照してください。
- セキュア メッセージは、次のインターフェイスを使用して再生できます。
  - Connection 電話インターフェイス
  - Cisco Unity Connection Messaging Inbox（Connection 8.0 の場合）
  - Cisco Unity Connection Web Inbox（Connection 8.5 以降）
  - Cisco Unity Connection ViewMail for Microsoft Outlook（バージョン 8.0）
  - Cisco ViewMail for Microsoft Outlook（バージョン 8.5 以降）
  - Cisco Unity Connection ViewMail for IBM Lotus Notes

  - Cisco Unified Personal Communicator バージョン 7.0 以降
  - Cisco Unified Mobile Communicator および Cisco Mobile
  - Cisco Unified Messaging with IBM Lotus Sametime バージョン 7.1.1 以降。（Cisco Unified Messaging with Lotus Sametime を使用してセキュア メッセージを再生する際の要件については、該当する『*Release Notes for Cisco Unified Messaging with IBM Lotus Sametime*』を参照してください。このドキュメントは、http://www.cisco.com/en/US/products/ps9830/prod_release_notes_list.html から入手可能です）。
- セキュア メッセージは、次のインターフェイスを使用して転送できます。
  - Connection 電話インターフェイス
  - Cisco Unity Connection Connection Web Inbox（Connection 8.5 以降）
  - Cisco Unity Connection Messaging Inbox（Connection 8.0 の場合）
  - Cisco Unity Connection ViewMail for Microsoft Outlook 8.5
- 次のインターフェイスを使用してセキュア メッセージにアクセスすることはできません。
  - IMAP クライアント（ViewMail for Outlook または ViewMail for Notes がインストールされている場合を除く）
  - RSS リーダー
- デフォルトでは、ローカル ネットワーキング サイトをホームとしている Connection ユーザだけが、セキュア メッセージを受信できます。リモート ネットワーキング サイトをホームとしている VPIM 連絡先またはユーザもメッセージを受信できますが、受信するためには、セキュア メッセージの配信を許可するように VPIM ロケーションまたはサイト間リンクが設定されている必要があります。メッセージが Connection サイトを離れるか、VPIM ロケーションに送信されると、メッセージのセキュリティを保証できません。
- セキュア メッセージへの応答も、セキュアとしてマークされます。
- セキュア メッセージは、他の Connection ユーザ、および同報リストにある Connection ユーザに転送できます。転送されたメッセージもまた、セキュアとしてマークされます。ユーザは、転送されたメッセージおよび応答の機密性を変更できません。
- ユーザが Connection にサインインしてメッセージを送信するとき、サービス クラス設定によって、メッセージをセキュアとしてマークするかどうかが決まります。デフォルトでは、ユーザがメッセージをプライベートとしてマークすると、Connection でそのメッセージが自動的にセキュアとしてマークされます。
- *（Cisco Unity Connection 8.0(2) 以降）* Connection がユーザにメッセージがセキュアとしてマークされたことをアナウンスするよう設定するには、[システム設定（System Settings）] > [詳細設定（Advanced Settings）] > [カンバセーションの設定（Conversation Configuration）] ページで、[メッセージ ヘッダーでセキュア ステータスをアナウンスする（Announce Secure Status in Message Header）] チェックボックスをオンにします。このチェックボックスをオンにすると、Connection はセキュア メッセージを再生する前に、このメッセージが「...secure message....」であることをユーザに通知するプロンプトを再生します。
- 発信者がユーザまたはコール ハンドラのグリーティングに転送され、メッセージを残した場合、ユーザまたはコール ハンドラ アカウントの [編集（Edit）] > [メッセージ設定（Message Settings）] ページの [セキュアにする（Mark Secure）] チェックボックスの状態によって、Connection でメッセージがセキュアとしてマークされるかどうかが決まります。
- デフォルトでは、SMTP リレー アドレスにメッセージをリレーする 1 つ以上のメッセージ操作が設定されたユーザに対して、Connection でセキュア メッセージがリレーされません。リレーが設定されたユーザに対するセキュア メッセージを受信すると、Connection は、メッセージの送信者に不達確認を送信します。セキュア メッセージを Connection でリレーするように設定するには、

Cisco Unity Connection Administration の [システム設定（System Settings）] > [詳細設定（Advanced）] > [メッセージング（Messaging）] ページの [セキュアメッセージのリレーを許可する（Allow Relaying of Secure Messages）] チェックボックスをオンにします。このチェックボックスをオンにすると、セキュア メッセージはセキュア フラグ付きでリレーされますが、ほとんどの電子メール クライアントでは通常のメッセージとして扱われます。

- ファクス サーバから送られるファクス メッセージは、セキュアとしてマークされることはありません。

セキュア メッセージに関する ViewMail の制限事項

- セキュア メッセージは、Cisco Unity Connection ViewMail for Microsoft Outlook 8.0 または ViewMail for IBM Lotus Notes を使用して転送できません。
- ViewMail for Outlook 8.0 および ViewMail for Notes は、セキュア メッセージの再生だけをサポートします。
- ViewMail for Outlook 8.0 または ViewMail for Notes を使用して作成または応答されたメッセージは、[セキュア メッセージングを必須にする（Require Secure Messaging）] フィールドが [常時（Always）] または [選択する（Ask）] に設定されているサービス クラスにユーザが割り当てられている場合でも、セキュアとして送信されることはありません。

すべてのメッセージをセキュアとしてマークするための Cisco Unity Connection の設定

すべてのメッセージをセキュアとしてマークするには、次のタスク リストを使用して Cisco Unity Connection を設定します。

1. メッセージが常にセキュアとしてマークされるように、すべてのサービス クラスを設定します。「COS メンバーのメッセージ セキュリティをイネーブルにするには」（P.10-60）の手順を参照してください。（ユーザが Connection にサインインしてメッセージを送信するとき、サービス クラス設定によって、メッセージをセキュアとしてマークするかどうかが決まります）。
2. すべての外部発信者のメッセージがセキュアとしてマークされるように、ユーザ メールボックスを設定します。「外部の発信者が残したメッセージをセキュアとしてマークするようにユーザおよびユーザ テンプレートを設定するには」（P.10-61）の手順を参照してください。
3. すべての外部発信者のメッセージがセキュアとしてマークされるように、コール ハンドラを設定します。「外部の発信者が残したメッセージをセキュアとしてマークするようにコール ハンドラおよびコール ハンドラ テンプレートを設定するには」（P.10-61）の手順を参照してください。
4. *（Cisco Unity Connection 8.0(2) 以降）* Connection がユーザにメッセージがセキュアとしてマークされたことをアナウンスしないよう設定するには、[システム設定（System Settings）] > [詳細設定（Advanced Settings）] > [カンバセーションの設定（Conversation Configuration）] ページで、[メッセージ ヘッダーでセキュア ステータスをアナウンスする（Announce Secure Status in Message Header）] チェックボックスをオフにします。

COS メンバーのメッセージ セキュリティをイネーブルにするには

ステップ 1　Cisco Unity Connection Administration で、変更または新規作成する COS を探します。

ステップ 2　[サービス クラスの編集（Edit Class of Service）] ページで、[メッセージ オプション（Message Options）] の下の [セキュア メッセージングを必須にする（Require Secure Messaging）] リストから [常時（Always）] を選択します。

ステップ 3　[保存（Save）] を選択します。

ステップ 4　各サービス クラスに対してステップ 1 からステップ 3 までを繰り返します。または、[一括編集（Bulk Edit）] オプションを使用して、複数のサービス クラスを一度に編集することもできます。

外部の発信者が残したメッセージをセキュアとしてマークするようにユーザおよびユーザ テンプレートを設定するには

ステップ 1　Cisco Unity Connection Administration で、編集するユーザ アカウントまたはテンプレートを探します。

複数のユーザを同時に編集するには、[ユーザの検索（Search Users）] ページで該当するユーザのチェックボックスをオンにしてから、[一括編集（Bulk Edit）] を選択します。

ステップ 2　[編集（Edit）] メニューで、[メッセージ設定（Message Settings）] を選択します。

ステップ 3　[メッセージ設定の編集（Edit Message Settings）] ページで、[メッセージ セキュリティ（Message Security）] の下の [セキュアにする（Mark Secure）] オプションを選択します。

一括編集モードで編集する場合は、最初に [セキュアにする（Mark Secure）] フィールドの左側にあるチェックボックスをオンにして、選択されたユーザまたはテンプレートのフィールドが変更されることを示す必要があります。

ステップ 4　[保存（Save）] を選択します。

外部の発信者が残したメッセージをセキュアとしてマークするようにコール ハンドラおよびコール ハンドラ テンプレートを設定するには

ステップ 1　Cisco Unity Connection Administration で、編集するコール ハンドラまたはコール ハンドラ テンプレートを探します。

複数のコール ハンドラを同時に編集するには、[コール ハンドラの検索（Search Call Handlers）] ページで該当するコール ハンドラのチェックボックスをオンにしてから、[一括編集（Bulk Edit）] を選択します。

ステップ 2　[編集（Edit）] メニューで、[メッセージ設定（Message Settings）] を選択します。

ステップ 3　[メッセージ設定の編集（Edit Message Settings）] ページで、[メッセージ セキュリティ（Message Security）] の下の [セキュアにする（Mark Secure）] チェックボックスをオンにします。

一括編集モードで編集する場合は、最初に [セキュアにする（Mark Secure）] フィールドの左側にあるチェックボックスをオンにして、選択されたユーザのフィールドが変更されることを示す必要があります。

ステップ 4　[保存（Save）] を選択します。

すべてのボイス メッセージに対する、Cisco Unity Connection 8.0 Messaging Inbox の [名前を付けて保存（Save Recording As）] オプションのディセーブル化

デフォルトでは、プライベート、セキュア、またはその両方としてマークされているメッセージを除き、ユーザは、[名前を付けて保存（Save Recording As）] オプションを使用してメッセージを WAV ファイルとしてハード ディスクに保存できます。このオプションは、Cisco Unity Connection 8.0 Messaging Inbox の Media Master の [オプション（Options）] メニューにあります。Messaging Inbox で Media Master の [オプション（Options）] メニューの [名前を付けて保存（Save Recording As）] オプションを無効にすることによって、メッセージの機密性に関係なく、ユーザがボイス メッセージを保存できないようにすることができます。

このセキュリティ オプションを検討する際には、次の点に注意してください。

- ユーザがメッセージをハード ディスクに保存できないようにすると、ユーザがメッセージをアーカイブするために、Inbox フォルダや削除済みアイテム フォルダに長期間保持する可能性があります。
- [名前を付けて保存（Save Recording As）] オプションの無効化は、Connection サーバと関連付けられているすべてのユーザに適用されます。個々のユーザに対してだけこのオプションを無効化することはできません。
- ユーザは引き続き Media Master を使用して、グリーティングや録音名を WAV ファイルとして保存できます。

Cisco Unity Connection 8.0 Messaging Inbox の Media Master で [名前を付けて保存（Save Recording As）] オプションをディセーブルにするには

ステップ 1　Cisco Unity Connection Administration で [システム設定（System Settings）] > [詳細設定（Advanced）] を展開し、[PCA] を選択します。

ステップ 2　[PCA の設定（PCA Configuration）] ページで、[Unity Inbox：メディア マスターのオプションとしての録音の保存を無効にする（Unity Inbox: Disable Save Recording As Option in Media Master）] チェックボックスをオンにします。

ステップ 3　[保存（Save）] を選択します。

セキュアな削除のためのメッセージ ファイルの破棄（Cisco Unity Connection 8.5 以降のみ）

ユーザによる単純なメッセージの削除に加えて、組織によっては、メッセージの削除にセキュリティの追加が必要な場合があります。この場合、Cisco Unity Connection Administration の [詳細設定（Advanced Settings）] > [メッセージングの設定（Messaging Configuration）] ページで、[メッセージ ファイルの破棄レベル（Message File Shredding Level）] の設定を行います。これはシステム全体の設定であり、メッセージの削除時に指定された回数の破棄が行われ、ユーザによって削除されたメッセージのコピーがセキュアに削除されます。この機能を有効にするには、0（ゼロ）以外の値を入力します。フィールドに入力する設定値（1 ～ 10 までの数字）は、削除されたメッセージ ファイルが破棄される回数を示します。破棄は、Linux 標準の破棄ツールを介して行われます。メッセージを構成する実際のビットが、ランダムなデータのビットによって指定された回数上書きされます。

デフォルトでは、[削除済みメッセージの消去（Clean Deleted Messages）] sysagent タスクが実行されるときに、破棄プロセスが 30 分ごとに発生します。[削除済みメッセージの消去（Clean Deleted Messages）] は、読み取り専用タスクです。このタスクの設定値は変更できません。（タスクに関する情報は [ツール（Tools）] > [タスク管理（Task Management）] の下の [Cisco Unity Connection の管理（Cisco Unity Connection Administration）] で参照できます）。

メッセージのコピーまたはメッセージに関連するファイルが破棄されない場合もあります。

- 通常のメッセージ送信プロセスでは、一時オーディオ ファイルが作成されます。これらの一時オーディオ ファイルは、メッセージ送信時に削除されますが、破棄はされません。メッセージへの参照は削除されますが、オペレーティング システムにスペースを再利用する理由が生じてデータが上書きされるまで、実際のデータは、ハード ドライブ上に維持されます。これらの一時オーディオ ファイルに加えて、削除され破棄されたメッセージを配信する場合に使用される他の一時ファイルもあります（破棄をイネーブルにしている場合）。一時ファイルは、関連付けられているメッセージが削除されるとただちに破棄されることに注意してください。メッセージ自体とは異なり、一時ファイルは [削除済みメッセージの消去（Clean Deleted Messages）] sysagent タスクの実行を待機しません。
- ユーザが Messaging Inbox または Web Inbox で再生不能なファイル形式のメッセージを再生しようとした場合、メッセージは一時オーディオ ファイルに変換されます。この一時オーディオ ファイルは、ユーザがメッセージを削除すると同時に削除されますが、破棄はされません。
- 破棄は、Connection サーバ上に存在するメッセージにだけ発生する場合があります。メッセージが他のサーバから回収されないようにするには、メッセージ リレー、IMAP、ViewMail for Outlook、ViewMail for Notes、Messaging Inbox または Web Inbox、単一受信トレイ、SameTime Lotus プラグイン、Cisco Unified Personal Communicator、Cisco Mobile、またはネットワーク サーバ間の SMTP スマート ホストの機能を使用しないでください。これらの機能を使用する場合は、セキュアなメッセージング機能を使用する必要があります。セキュアなメッセージングを使用する場合、セキュアなメッセージのローカル コピーは作成されず、ユーザもローカル コピーの保存を許可されないため、メッセージのすべてのコピーが Connection サーバ上に残り、削除時に破棄されます。

  （注）　セキュアなメッセージングに関する追加情報については、「セキュア メッセージ」（P.10-58）を参照してください。

- Connection ネットワーク内のロケーション間で送信されるメッセージは、送信前に一時的なロケーションに書き込まれます。このメッセージの一時コピーは削除されますが、破棄されません。

Cisco Unity Connection クラスタで破棄をイネーブルにした場合、メッセージはプライマリ サーバとセカンダリ サーバの両方で削除時に破棄されます。

パフォーマンスの問題により、破棄レベルを 3 よりも高く設定しないことを強く推奨します。

メッセージは完全削除された場合にだけ破棄されることに注意してください。ユーザがメッセージの削除に使用できる方法と、一時的削除および完全削除の定義については、『*System Administration Guide for Cisco Unity Connection*』*（Release 8.x）*（http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html）の「Messaging in Cisco Unity Connection 8.x」の章にある「Deleting Messages in Cisco Unity Connection 8.x」の項を参照してください。

Cisco Unity Connection 8.x での IMAP クライアント アクセスのメッセージ セキュリティ オプション

機密性が通常またはプライベートとしてマークされているボイス メッセージにユーザが IMAP クライアントからアクセスするときに、IMAP クライアントで、ユーザがメッセージを WAV ファイルとしてハード ディスクに保存したり、メッセージを転送したりするのが許可されることがあります。ユーザが IMAP クライアントを使用してボイス メッセージを保存または転送するのを防止する場合は、次のサービス クラス オプションのいずれかを指定することを検討してください。

- ユーザは、メッセージの機密性に関係なく、IMAP クライアントでメッセージ ヘッダーにだけアクセスできる。
- ユーザは、プライベートとしてマークされているメッセージを除くすべてのメッセージのメッセージ本文にアクセスできる。（クライアントが Microsoft Outlook で ViewMail for Outlook がインストールされている場合、またはクライアントが Lotus Notes で ViewMail for Notes がインストールされている場合を除き、IMAP クライアントではセキュア メッセージにアクセスできません）。

INDEX

か

く

こ

さ

せ

ち

と

に

ね

は

ふ

ほ

め