Cisco Unity Connection リリース 12.x セキュリティ ガイド

初版： 年 月 日

最終更新： 年 月 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/

Text Part Number:

【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。

目 次

第 1 章

Cisco Unity Connection に必要な IP コミュニケーション

Cisco Unity Connection に必要な IP コミュニケーション

サービス ポート

表 1：Cisco Unity Connection とのインバウンド接続に使用される TCP および UDP ポートは、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 Unity 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*：*Cisco Unity Connection* とのインバウンド接続に使用される *TCP* および *UDP* ポート

ポートとプロトコル[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	説明
TCP：20500、20501、20502、19003、1935	Unity Connection クラスタ内のサーバ間でだけ開かれる	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Unity 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。

ポートとプロトコル[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	説明
TCP：**21000 ～ 21512**	オープン（Open）	CuCsMgr/Unity 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、Unity 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**	オープン（Open）	CuCsMgr/Unity 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 Administration 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。
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 TCP ポート 5001、5002、5003、および 5004 が開きます。 例：**5060 ～ 5199**	オープン（Open）	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Conversation Manager によって処理される Unity 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	Unity Connection クラスタ内のサーバ間でだけ開かれる	CuLicSvr/Unity 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）。

ポートとプロトコル[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	説明
TCP：1502、1503（/etc/services の「ciscounity_tcp」）	Unity Connection クラスタ内のサーバ間でだけ開かれる	unityoninit/Unity Connection DB	root	Unity 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**	オープン（Open）	CuImapSvr/Unity 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**	オープン（Open）	CuSmtpSvr/Unity Connection SMTP サーバ	cusmtpsvr	Unity 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/Unity 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**	オープン（Open）	CuMixer/Unity 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。

ポートとプロトコル[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	説明
UDP：7774 ～ 7900	ブロックされる（内部使用のみ）	CuMixer/ 音声認識 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	Unity Connection クラスタ内のサーバ間でだけ開かれる	CuSrm/ Unity Connection サーバ ロール マネージャ	cusrm	クラスタ SRM RPC です。 Unity 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：22001 UDP：22001	Unity Connection クラスタ内のサーバ間でだけ開かれる	CuSrm/ Unity 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。 Unity 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**	オープン（Open）	CuDbProxy/ Unity 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。

ポートとプロトコル[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	説明
TCP：**22**	オープン（Open）	Sshd	root	リモート CLI アクセス用の TCP 22 接続、および Unity 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 Unity Connection サーバに接続できる必要があります。 Unity 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**	オープン（Open）	Snmpd Platform SNMP Service	root	—
UDP：**500**	オープン（Open）	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、Unity 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**	オープン（Open）	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。 Unity 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。

ポートとプロトコル[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	説明
UDP：**123**	オープン（Open）	Ntpd Network Time Service	ntp	Unity 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。 Unity 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	オープン（Open）	Tomcat/Cisco Tomcat（SOAP Service）	tomcat	Unity 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	Unity 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。 Unity 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	Unity Connection クラスタ内のサーバ間でだけ開かれる	dblrpm/Cisco DB Replication Service	root	Unity 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。

ポートとプロトコル[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	説明
TCP：8001	Unity 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	Unity 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	Unity Connection クラスタ内のサーバ間でだけ開かれる	RisDC/Cisco RIS Data Collector	ccmservice	Unity 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	Unity 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 Unity 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。

ポートとプロトコル[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	説明
TCP：**80、443、8080、8443**	オープン（Open）	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。 Unity 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。 （注） これらのポートは、IPv4 アドレスと IPv6 アドレスの両方をサポートします。ただし、IPv6 アドレスは、Connection プラットフォームがデュアル（IPv4/IPv6）モードで設定されている場合にのみ機能します。Cisco Unity Connection Survivable Remote Site Voicemail SRSV では、IP 通信用にこれらのポートをサポートします。

ポートとプロトコル[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	説明
TCP：8081、8444	HTTPS ネットワーキングのサーバ間でのみ開きます。	tomcat/Cisco Tomcat	tomcat	HTTPS ネットワーキング サーバが通信のために、これらのポート上で相互に接続できる必要があります。Unity Connection HTTPS ディレクトリのフィーダ サービスは、ディレクトリ同期のためにこれらのポートを使用します。 （注） Unity Connection HTTPS ディレクトリのフィーダ サービスは IPv4 モードのみをサポートします。
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**	オープン（Open）	—	—	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：7443	オープン（Open）	jetty/Unity Connection Jetty	jetty	Jabber および Web Inbox 通知を保護します。「utils cuc jetty ssl enable」CLI コマンドを使用してポートを有効にできます。 （注） SSL 経由で jetty を有効にするには、内部通信用にポート 7080 が開いている必要があります。

ポートとプロトコル[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	説明
TCP：7080	オープン（Open）	jetty/Unity Connection Jetty	jetty	*Exchange 2010* のみ、単一受信トレイのみ：Unity Connection ボイス メッセージの変更に関する Jabber および Web Inbox EWS 通知。
UDP：9291	オープン（Open）	CuMbxSync/Unity Connection メールボックス同期サービス	cumbxsync	単一受信トレイのみ：Unity Connection ボイス メッセージの変更に関する WebDAV 通知。
TCP：6080	オープン（Open）	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	ビデオ サーバは、通信用にこのポートの Unity Connection に接続できる必要があります。

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。

Unity Connection が行うアウトバウンド接続

表 2：ネットワーク内の他のサーバとの接続のために Unity Connection によって使用される TCP ポートおよびUDP ポート 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 *2*：ネットワーク内の他のサーバとの接続のために *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	説明
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	Unity Connection SCCP クライアントと Cisco Unified CM の接続（SCCP を使用して統合されている場合）。
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	Unity Connection アウトバウンド オーディオ ストリーム トラフィック
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、Unity 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：6972	CuCsMgr	cucsmgr	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、Unity Connection で Cisco Unified CM への HTTPS クライアント接続が行われて、ITL 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。

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	説明
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 Unity 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、Unity 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、Unity 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	（注） これらのポートは、IPv4 アドレスと IPv6 アドレスの両方をサポートします。

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	説明
TCP：80、8080、443、および 8443（HTTP および HTTPS）	CuCsMgr tomcat	cucsmgr tomcat	Unity 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 Unity 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 （注） これらのポートは、IPv4 アドレスと IPv6 アドレスの両方をサポートします。 （注） Cisco Unity Connection Survivable Remote Site Voicemail SRSV では、IP 通信用にこれらのポートをサポートします。
TCP：143、993（IMAP および IMAP over SSL）	CuCsMgr	cucsmgr	Unity Connection は、Unity 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	Unity Connection は、VPIM ネットワーキングや Unity 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 Unity Connection サーバへのクライアント接続を行います。

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	説明
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 Unity 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。
UDP：514 TCP：601	syslog/Cisco syslog サーバ	syslog	Unity Connection サーバは、これらのポート経由でリモート syslog サーバに監査ログを送信できる必要があります。

トランスポート層の保護

Unity Connection は、シグナリングとクライアント/サーバ通信に Transport Layer Security（TLS）プロトコルとセキュア ソケット レイヤ（SSL）プロトコルを使用します。Unity Connection では、Cisco Unity Connection の各種インターフェイス間のセキュア通信のために TLS 1.0、TLS 1.1、および TLS 1.2 をサポートしています。TLS 1.2 は最も安全な認証済み通信プロトコルです。

Unity Connection 12.0(1) 以降では、部門のセキュリティ ポリシーと導入能力に応じて、TLS 最小バージョンを設定できます。TLS の最小バージョンが設定されると、Unity Connection では設定された最小バージョン以降の TLS がサポートされます。たとえば、TLS の最小バージョンとして TLS 1.1 を設定すると、Unity Connection は通信に TLS 1.1 以降のバージョンを使用し、この設定値よりも低い TLS バージョンを求める要求を拒否します。デフォルトで、TLS 1.0 が設定されます。

最小 TLS バージョンを設定する前に、Unity Connection のすべてのインターフェイスが保護されており、設定される最小 TLS バージョン以降のバージョンを通信に使用していることを確認します。ただし、Unity Connection のインバウンド インターフェイスの最小 TLS バージョンを設定できます。

表 3 に、サポートされており Unity Connection で最小 TLS バージョンを設定できるインターフェイスを示します。

表 *3*：セキュア通信でサポートされているインターフェイス

ポート	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	説明
8443、443、8444	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。 Unity 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。
7443	jetty/Unity Connection Jetty	jetty	Jabber および Web Inbox 通知を保護します。
993	CuImapSvr/Unity Connection IMAP サーバ	cuimapsvr	クライアント ワークステーションは、IMAP over SSL での受信トレイ アクセスのためにポート 993 に接続できる必要があります。
25	CuSmtpSvr/Unity Connection SMTP サーバ	cusmtpsvr	Unity 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。
5061-5199	CuCsMgr/Unity Connection Conversation Manager	cucsmgr	Conversation Manager によって処理される Unity 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。

ポート	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	説明
LDAP（アウトバウンド インターフェイス）	CuMbxSync cucsmgr tomcat	cumbxsync cucsmgr tomcat	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、Unity Connection はポート 636 を使用します。

サポートされている Cisco Unity Connection のインバウンド インターフェイスの詳細については、「サービス ポート」を参照してください。

最小 TLS バージョンの設定

Cisco Unity Connection で最小 TLS バージョンを設定するには、次の CLI コマンドを実行します。

- set tls min-version <tls minVersion>

クラスタのパブリッシャとサブスクライバの両方でこのCLIコマンドを実行する必要があります。

さらに次の CLI コマンドを実行して、Unity Connection の最小 TLS バージョンとして設定している値を確認することもできます。

- show tls min-version

CLI の詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。このドキュメントは http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にあります。

注意 最小 TLS バージョンの設定が完了すると、Cisco Unity Connection サーバが自動的に再起動します。

第 2 章

不正通話の防止

はじめに

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。

不正通話の防止に役立つ規制テーブルの使用

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 Unity 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。

- Unity 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 Unity 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 Unity 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。

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。

第 3 章

Cisco Unity Connection：制限版と無制限版

Cisco Unity Connection：制限版と無制限版

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。

Cisco Unity Connection には、制限版と無制限版という 2 種類の Connection ソフトウェアがあります。これは、一部の国におけるユーザ データ暗号化に関連する輸入要件に対応することを目的としています。Cisco Unity Connection 制限版では、製品の暗号化機能を有効にすることで、以下に示すセキュリティ モジュールを使用できるようになりますが、無制限版ではセキュリティ モジュールの使用は許可されていません。

機能	Connection 制限版	Connection 無制限版
ボイス メッセージへのアクセスに使用する SSL for IMAP 接続	許可する	許可しない
コール シグナリングおよびメディアのためのセキュア SCCP、SIP、および SRTP	許可する	許可しない
ネットワーク接続している Connection サーバまたはクラスタ間の（セキュア MIME による）通信接続	許可する	許可しない
Comet 通知の SSL（Jetty SSL コマンド）	許可する	許可しない

Cisco Unity Connection：制限版と無制限版

注意 Connection ソフトウェアの制限版と無制限版が利用可能な場合は、ソフトウェアをダウンロードするか、または DVD を注文してください。制限版を無制限版にアップグレードすることもできますが、その後のアップグレードは無制限版へのアップグレードに限定されます。無制限版から制限版へのアップグレードはサポートされていません。

Unity Connection 12.0(1) 以降では、評価モードでの制限版製品ではデフォルトで暗号化が無効になっています。そのため制限版では、エクスポート制御機能を有効にするトークンを使用して製品を Cisco Smart Software Manager（CSSM）または Cisco スマート ソフトウェア マネージャ サテライトに登録するまでは、上記のセキュリティ モジュールを使用できません。評価モードの Unity Connection 制限版の動作は、Unity Connection 無制限版の動作に似ています。

12.0(1) より前の Cisco Unity Connection を 12.0(1) 以降のリリースにアップグレードすると、Cisco Unity Connection で暗号化が次のように動作します。

アップグレード パス	アップグレード前のクラスタ モード	アップグレード前のライセンス ステータス	アップグレード後のライセンス ステータス	操作
12.0(1) より前のリリースから 12.0(1) へ	セキュア	デモまたは PLM Licensed	評価モード	Cisco Unity Connection は引き続きセキュア モードで動作します。評価期間が期限切れになる前に、エクスポート制御機能対応トークンを使用してこの製品を CSSM またはサテライトに登録していない場合、評価期間の期限が切れると RTMT に関するアラームが生成されます。

注意 登録解除後に「Connection Conversation Manager」または「Connection IMAP Server」のいずれかのサービスが再起動されると、セキュリティ モジュールを使用できなくなります。たとえば、IMAP Server が再起動する場合は IMAP、Cisco Unity Connection で Connection Conversation Manager が再起動する場合は SCCP/SIP/SRTP が使用できなくなります。

（注） リリース 12.0(1) 以降で、 12.0(1) から 12.0(1) 以降へのアップグレードでは、アップグレード完了後にシステムの既存の暗号化ステータスが維持されます。

CSSM またはサテライトへの製品の登録方法の詳細については、『Upgrade and Maintenance Guide for Cisco Unity Connection 12.x』の「Managing Licenses」の章を参照してください。このガイドは

Cisco Unity Connection：制限版と無制限版

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/install_upgrade/guide/b_12xcuciumg.html にあります。

Cisco Unity Connection 制限版で暗号化を有効または無効にできるようにするため、新しい CLI コマンド「utils cuc encryption <enable/disable>」が Unity Connection 12.0(1) 以降に導入されました。

CLI の詳細については、最新のリリースの『Command Line Interface Reference Guide for Cisco Unified Solutions』を参照してください。このガイドは http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にあります。

Cisco Unity Connection：制限版と無制限版

第 4 章

Cisco Unity Connection、Cisco Unified Communications Manager、および IP フォン間の接続の保護

Cisco Unity Connection、Cisco Unified Communications Manager、および IP フォン間の接続の保護

はじめに

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、講じ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。

Unity Connection、Cisco Unified Communications Manager、および IP フォン間の接続に関するセキュリティの問題

Cisco Unity Connection システムは、 Unity Connection のボイス メッセージ ポート（SCCP 統合用）またはポート グループ（SIP 統合用）、Cisco Unified Communications Manager、および IP フォンの間の接続に関して、潜在的な脆弱性ポイントを持ちます。

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 Unity Connection 間の情報フローの監視と改変）

- ネットワーク トラフィック スニフィング（Cisco Unified CM、Unity Connection、および Cisco Unified CM で管理される IP フォン間の通話内容やシグナリング情報のソフトウェアによるキャプチャ）
- Unity Connection と Cisco Unified CM 間のコール シグナリングの改変
- Unity Connection とエンドポイント（IP フォンやゲートウェイなど）の間のメディア ストリームの改変
- Unity Connection の ID 盗用（Unity Connection 以外のデバイスが Cisco Unified CM に対し、そのデバイス自体が Unity Connection サーバであると示す場合）
- Cisco Unified CM サーバの ID 盗用（Cisco Unified CM 以外のサーバが Unity Connection に対し、そのサーバ自体が Cisco Unified CM サーバであると示す場合）

Unity Connection のボイス メッセージング ポート用の Cisco Unified Communications Manager セキュリティ機能

Cisco Unified CM は、「Unity Connection、Cisco Unified Communications Manager、および IP フォン間の接続に関するセキュリティの問題」に記載されている脅威から Unity Connection への接続を保護できます。Unity Connection が利用できる Cisco Unified CM のセキュリティ機能を表 4：Cisco Unity Connection が使用する Cisco Unified CM セキュリティ機能 に示します。

表 *4*：*Cisco Unity Connection* が使用する *Cisco Unified CM* 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	トランスポート層セキュリティ（TLS）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 証明書信頼リスト（CTL）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。 • 中間者攻撃（Cisco Unified CM と Unity Connection 間の情報フローの改変） • コールシグナリングの改変。 • Unity Connection サーバの ID 盗用 • Cisco Unified CM サーバの ID 盗用

セキュリティ機能	説明
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、Unity Connection ボイス メッセージング ポート（SCCP 統合用）または Unity Connection ポート グループ（SIP 統合用）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 証明書信頼リスト（CTL）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。 • 中間者攻撃（Cisco Unified CM と Unity Connection 間の情報フローの改変） • メディア ストリームの改変。 • Unity Connection サーバの ID 盗用 • Cisco Unified CM サーバの ID 盗用
シグナリング暗号化	暗号化の手法を使用して、Unity 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。 • 中間者攻撃（Cisco Unified CM と Unity Connection 間の情報フローの監視） • ネットワーク トラフィック スニフィング（Cisco Unified CM と Unity Connection 間のシグナリング情報フローの監視）

セキュリティ機能	説明
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 Unity 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 Media Player キー ペアの作成、Unity 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。Unity 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。 • 中間者攻撃（Cisco Unified CM と Unity Connection 間のメディア ストリームのリッスン） • ネットワーク トラフィック スニフィング（Cisco Unified CM、Unity Connection、および Cisco Unified CM で管理される IP フォン間の電話による通話内容の盗聴）

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 セキュリティ（認証と暗号化）では、Unity Connection へのコールだけが保護されます。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、Unity Connection のプライベート セキュア メッセージング機能で保護できます。Unity Connection のセキュア メッセージング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の処理」を参照してください。

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

Cisco Unified Communications Manager と Cisco Unity Connection のボイス メッセージング ポート（SCCP 統合用）またはポート グループ（SIP 統合用）のセキュリティ モード オプションを表 5：セキュリティ モード オプション に示します。

注意 Unity Connection ボイス メッセージ ポート（SCCP 統合用）またはポート グループ（SIP 統合用）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。一致していない場合、Cisco Unified CM の認証と暗号化は失敗します。

表 *5*：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、認証済み 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。 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、Cisco Unified Communications Manager、および IP フォン間の接続の保護に関するベスト 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ング ポートに対し認証と暗号化を有効にするには、『*Cisco Unified Communications Manager SCCP Integration Guide for Unity Connection Release 12.x*』を参照してください。このファイルは次の URL から入手可能です。

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/integration/guide/cucm_sccp/b_12xcucintcucmskinny.html

Cisco Unity Connection、Cisco Unified Communications Manager、および IP フォン間の接続の保護に関するベスト プラクティス

第 5 章

管理とサービス アカウントの保護

管理とサービス アカウントの保護

はじめに

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。

Cisco Unity Connection 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 6：Unity Connection サーバの管理アカウント 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 *6*：*Unity 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

	Operating System Administration アカウント	Application Administration アカウント
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、Unity Connection が適切に機能しなくなります。
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 コマンドの使用 **注意** アカウント名の変更に **utils reset_ui_administrator_password** 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、Unity 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** コマンドを使用しないでください。このコマンドを使用すると、Unity 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 コマンドの使用	Cisco Unity Connection Administration を使用 **注意** アカウントの削除に **delete account** コマンドを使用しないでください。このコマンドを使用すると、Unity 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 コマンドの使用。	Cisco Unity Connection Administration を使用
LDAP ユーザ アカウントとの連動	なし	あり

Cisco Unity Connection Administration へのアクセスに使用するアカウントに関するベスト プラクティス

Cisco Unity Connection 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 Administration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 Unity Connection サーバで構成される場合、あるサーバで Connection Administration 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 Administration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 Administration 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

Unity Connection のユーザ アカウントを Unity 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、Unity 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 Administration 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 Administration のすべてのページにアクセスできるだけでなく、Connection Administration 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。

（注） 次のアプリケーション ユーザ名はエラーを生成するため、使用しないでください。

- CCMSysUser
- WDSysUser
- CCMQRTSysUser
- IPMASysUser
- WDSecureSysUser
- CCMQRTSecureSysUser
- IPMASecureSysUser
- TabSyncSysUser
- CUCService

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 Administration 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る管理ユーザアカウントはシステム管理者の役割に割り当てられ、管理者には Unity Connection のすべての管理機能に対するフルアクセス権が与えられます。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）。

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は、Cisco Personal Communications Assistant（PCA）または電話インターフェイスにサインインするときに使用するものと同じアカウントを使用しないことが推奨されます。

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 12.x にユニファイド メッセージングを設定する場合は、Unity 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、Unity 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、Unity 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。

ファイルの整合性の確認

Unity Connection では、さまざまなインターフェイス（Cisco Unity Connection の Cisco Unity Connection Administration や Cisco Unity Connection Serviceability など）からダウンロードできるファイルの整合性を管理者が確認できるようにし、セキュリティ強化を図っています。ファイルの整合性を検証するため、Unity Connection はすべてのダウンロード ファイルに対して SHA-512 チェックサム値を提供します。たとえば、Cisco Unified Real-Time Monitoring Tool プラグインの SHA-512 チェックサム値は [プラグインの検索（Search Plugin）] ページの [説明（Description）] フィールドに表示されます。

管理者は、ファイルの整合性を確認するためにファイルをダウンロードし、オンラインで利用できる外部ツールを使用してファイルのチェックサムを生成できます。次に、表示されているチェックサムと、ダウンロードしたファイルのチェックサムを比較します。両方のファイルのチェックサムが同一である場合は、ダウンロードしたファイルにはエラーがありません。

第 6 章

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

Cisco Unity Connection 11.0(1) における FIPS コンプライアンス

FIPS の CLI コマンドの実行

Cisco Unity Connection で FIPS 機能を有効にするには、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 機能を無効にします。
- 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/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html から入手可能です。

注意 FIPS モードを有効または無効にした後、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働するまで、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。

（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 にサインインします。
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、Cisco Unity Connection ルート証明書を .pem ファイルとして保存する場所を参照します。

（注） 証明書は、拡張子が（.htm ではなく）.pem 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. Cisco Unity Connection ルート証明書をすべての Cisco Unified CM サーバにコピーするため、次のサブ手順を実行します。
   a. Cisco Unified CM サーバで、[Cisco Unified オペレーティング システムの管理（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、Unity Connection Conversation Manager Service を再起動します。
    a. Cisco Unity Connection Serviceability にサインインします。
    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 Unity Connection Conversation Manager サービスを停止します。
    d. [ステータス（Status）] エリアに、Unity 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 の間での SCCP 統合と 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」 を参照してください。このガイドは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/os_administration/b_12xcucosagx.html にあります。

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。

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 間で IPsec ポリシーを設定します。
- [Unity Connection 管理（Unity 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） 管理者には、FIPS モードで NTLM に設定する Web ベースの認証モードを設定するオプションがあります。この設定では、ユニファイド メッセージング インターフェイスが FIPS に準拠しなくなることに注意してください。

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」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/voice_ip_comm/connection/12x/os_administration/b_12xcucosagx.html にあります。

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。このマニュアルは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/os_administration/b_12xcucosagx.html にあります。

FIPS モード使用時にサポートされない機能

FIPS モードが有効な場合、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）。
- ビデオ メッセージング

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 で FIPS を有効にすると、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。
- Unity 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 Unity 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。

Unity Connection でのすべての SHA-1 アルゴリズムによるボイス メール PIN のハッシュ

FIPS が有効な場合、Cisco Unity Connection はデータベースのチェックを行わず、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。Unity 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 Unity 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 Unity 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 の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 を有効にする前に、[Unity Connection の管理（Unity Connection Administration）] の [パスワードの設定（Password Settings）] ページで、[ユーザは次回サインイン時に変更する必要あり（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 Unity 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

第 7 章

Cisco Unity Connection の EnhancedSecurityMode

Cisco Unity Connection の EnhancedSecurityMode

概要

Unity Connection が EnhancedSecurityMode で動作できる場合、システム導入を保護する一連の厳密なセキュリティおよびリスク管理コントロールが実装されます。

EnhancedSecurityMode には次の機能があります。

- **厳密なパスワード要件**：新規ユーザパスワードと既存のパスワードの変更時に適用される厳密なクレデンシャル ポリシーが導入されました。クレデンシャル ポリシー, （42 ページ）を参照してください。
- **リモート監査ログ**：すべての監査ログとイベント syslog はローカルに保存され、またリモート syslog サーバにも保存されます。

  リモート監査ログ, （42 ページ）を参照してください。
- **システム ロギング**：CLI ログインや間違ったパスワードの使用などのすべてのシステム イベントが記録、保存されます。
- **ログオンの制限**：インターフェイスの同時セッションの最大数を設定できます。設定されている制限を超えると、新しいセッションはすべて切断されます。EnhancedSecurityMode では、[テレフォニー インターフェイスの最大セッション数（ユーザあたり）（Maximum Concurrent Sessions for Telephony Interface (Per User)）] のデフォルト値は 2、[IMAP インターフェイスの最大セッション数（ユーザあたり）（Maximum Concurrent Sessions for IMAP Interface (Per User)）] のデフォルト値は 5 です。詳細については、「パスワード、PIN、および認証規則の管理」の章を参照してください。

- **非アクティブユーザの無効化**：ユーザの非アクティブタイムアウトの日数を設定できます。ユーザがボイスメールアカウントにログインしていない期間が、設定されている日数に達すると、アカウントは無効になり、今後のアクセスは拒否されます。

  EnhancedSecurityMode では、[ユーザの非アクティブ タイムアウト（日数）（User Inactivity Timeout (in Days)）] のデフォルト値は 90 です。詳細については、「パスワード、PIN、および認証規則の管理」を参照してください。パスワード、PIN、および認証規則の管理, （49 ページ）

ロール ベースのアクセス

EnhancedSecurityMode では、「スーパー カスタム管理者（Super Custom Administrator）」という新しい権限が [カスタム役割（Custom Roles）] ページの権限リストに追加されます。システム管理者は「スーパー カスタム管理者（Super Custom Administrator）」権限を使用して、システム内で 2 レベルの管理者階層を作成できます。

クレデンシャル ポリシー

EnhancedSecurityMode が有効になると、プラットフォーム管理者に対し新規パスワードとパスワード変更に関する厳密なクレデンシャル ポリシーを適用できます。このポリシーにより適用されるデフォルトのパスワード要件を次に示します。

- クレデンシャルの長さは 14 ～ 127 文字です。
- パスワードには少なくとも 1 つの小文字、1 つの大文字、1 つの数字、および 1 つの特殊文字が含まれている必要があります。
- 以前のクレデンシャルの保存数は 24 であり、この 24 個のクレデンシャルはいずれも再利用できません。
- クレデンシャルの最小有効期間は 1 日、最大有効期間は 60 日です。
- 連続するクレデンシャル間での最小変更文字数は 4 文字です。

EnhancedSecurityMode を有効にした後で、管理者は認証規則を使用してパスワード要件を変更し、すべてのパスワード変更に関する厳密なパスワードポリシーを適用できます。クレデンシャルポリシーについては、「パスワード、PIN、および認証規則の管理」の章を参照してください。

リモート監査ログ

セキュリティ要件に準拠するため、Unity Connection でリモート監査ログを設定する必要があります。

EnhancedSecurityMode では、システムはデフォルト プロトコルとして TCP を使用して、リモート syslog サーバに監査イベントとアラームを送信します。通常の動作モードでシステムで使用され

る UDP とは異なり、TCP にはすべてのパケットの配信を保証するメカニズムがあります。ただし、必要に応じてこのモードで UDP を使用するようにシステムを再設定することもできます。

転送エラーが発生すると、TCPRemoteSyslogDeliveryFailed アラームとアラートがトリガーされ、管理者に対し TCP 転送エラーについて通知されます。スロットリング メカニズムにより、1 時間あたりに送信されるアラームとアラートはそれぞれ 1 つずつに限定されます。このため、管理者に対して同じアラームとアラートが大量に送信されることがありません。管理者は通信の再確立時にローカル監査ログをバックアップとして使用できます。

Unity Connection 12.0(1) 以降では、Transport Layer Security（TLS）1.2 を syslog の通信プロトコルとして使用できます。TLS 1.2 プロトコルにより、Cisco Unity Connection と syslog サーバ間でセキュアな接続を確立できます。

（注） セキュアな接続は syslog サーバが TLS 1.2 プロトコルをサポートしている場合にのみ確立されるため、syslog サーバが TLS 1.2 プロトコルをサポートしていることを確認してください。

EnhancedSecurityMode の前提条件

- FIPS 140-2 モードの設定：EnhancedSecurityMode を有効にする前に、FIPS モードを有効にする必要があります。FIPS モードがまだ有効ではない場合は、EnhancedSecurityMode を有効にする時点で、FIPS モードを有効にするように促されます。
- リモート syslog サーバをセットアップし、Unity Connection とリモート サーバ（この間のゲートウェイを含む）の間で IPSec を設定します。
- スマート ホストをセットアップし、Unity Connection と Exchange（Exchange がスマート ホストとして稼働、この間のゲートウェイを含む）の間で IPSec を設定します。IPSec 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」を参照してください。このガイドは https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/os_administration/b_12xcucosagx.html にあります。

EnhancedSecurityMode での設定タスクのフロー

ステップ 1 Unity Connection で EnhancedSecurityMode を有効にします。EnhancedSecurityMode の設定, （44 ページ）を参照してください。

ステップ 2 システム クレデンシャル ポリシーがセキュリティ ガイドラインを満たしていることを確認します。クレデンシャル ポリシーの設定, （44 ページ）を参照してください。

ステップ 3 モードの監査フレームワークを設定します。

Unity Connection の監査ロギング フレームワークをセットアップします。これには、すべての監査ログとアラームに対するリモート syslog サーバのセットアップも含まれます。監査フレームワークの設定，（45 ページ）を参照してください。

EnhancedSecurityMode の設定

EnhancedSecurityMode を有効または無効にするには、次の手順を使用します。ただし、**EnhancedSecurityMode** を有効にする前に FIPS モードを有効にしておく必要があります。

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils EnhancedSecurityModestatus** コマンドを実行して、モード ステータスが有効と無効のいずれに設定されているかを確認します。

ステップ 3 モードが無効な場合は、次のコマンドを実行して **EnhancedSecurityMode** を有効にします。

```
utils EnhancedSecurityMode enable
```

同様にモードを無効にするには **utils EnhancedSecurityMode disable** コマンドを実行します。

ステップ 4 Cisco Unity Connection のすべてのノードでこの手順を繰り返します。

クレデンシャル ポリシーの設定

システム クレデンシャル ポリシーを更新するには、次の手順を実行します。

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

ステップ 2 [認証規則（Authentication Rules）] > [認証規則の編集（Edit Authentication Rule）] を選択します。

ステップ 3 要件に基づいて認証規則を更新します。

ステップ 4 [保存（Save）] をクリックします。

クレデンシャル ポリシーについては、「パスワード、PIN、および認証規則の管理」の章を参照してください。

監査フレームワークの設定

Unity Connection で **EnhancedSecurityMode** の監査要件を設定するには、次のタスクを実行します。

ステップ 1 リモート監査ログを設定します。
リモート監査ログの監査ログ設定を行います。

ステップ 2 リモート監査ログの転送プロトコルを設定します。
（オプション）デフォルトで **EnhancedSecurityMode** が有効な場合、システムはリモート監査ログの転送プロトコルとしてTCPを使用します。この手順では、UDPを使用するようにシステムを再設定できます。

ステップ 3 RTMT で、電子メール アラート用の電子メール サーバをセットアップします。

ステップ 4 TCPRemoteSyslogDeliveryFailed アラートの電子メール通知を設定します。

リモート監査ログの設定

EnhancedSecurityMode で稼働している Unity Connection システムのリモート監査ログを設定する前に、次の点を確認してください。

- リモート syslog サーバをすでにセットアップしている必要があります。
- また、各クラスタ ノードとリモート syslog サーバ（中間のゲートウェイを含む）間で、IPSec を設定している必要があります。

  IPSec 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」を参照してください。このガイドは、

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/os_administration/b_12xcucosagx.html にあります。

ステップ 1 Cisco Unified Serviceability で、[ツール（Tools）] > [監査ログ設定（Audit Log Configuration）] を選択します。

ステップ 2 [サーバ（Server）] ドロップダウン メニューから、パブリッシャ ノード以外のクラスタ内のサーバを選択し、[実行（Go）] をクリックします。

ステップ 3 [すべてのノードに適用（Apply to All Nodes）] チェックボックスをオンにします。

ステップ 4 [サーバ名（Server Name）] フィールドに、リモート syslog サーバの IP アドレスまたは完全修飾ドメイン名を入力します。

ステップ 5 [監査ログ設定（Audit Log Configuration）] ウィンドウの残りのフィールドに値を入力します。フィールドとその説明を含むヘルプについては、オンライン ヘルプを参照してください。

ステップ 6 [保存（Save）] をクリックします。

リモート監査ログの転送プロトコルの設定

リモート監査ログの転送プロトコルを設定するには、次の手順を使用します。**EnhancedSecurityMode** でのデフォルト設定は TCP です。

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils remotesyslog show protocol** コマンドを実行して、設定されているプロトコルを確認します。

ステップ 3 プロトコルを変更する必要がある場合は、次の手順を実行します。
TCP を設定するには、**utils remotesyslog set protocol tcp** コマンドを実行します。UDP を設定するには、**utils remotesyslog set protocol udp** コマンドを実行します。TLS を設定するには、**utils remotesyslog set protocol tls** コマンドを実行します。

ステップ 4 ノードを再起動します。

ステップ 5 すべての Unity Connection クラスタ ノードに対してこの手順を繰り返します。

アラート通知用の電子メール サーバの設定

アラート通知用の電子メール サーバをセットアップするには、次の手順を使用します。

ステップ 1 Real-Time Monitoring Tool のシステム ウィンドウで、[アラート セントラル（Alert Central）] をクリックします。

ステップ 2 [システム（System）] > [ツール（Tools）] > [アラート（Alert）] > [電子メール サーバの設定（Config Email Server）] の順に選択します。

ステップ 3 [メール サーバ設定（Mail Server Configuration）] ポップアップで、メール サーバの詳細を入力します。

ステップ 4 [OK] をクリックします。

電子メール アラートの有効化

TCPRemoteSyslogDeliveryFailed アラームの電子メール警告をセットアップするには、次の手順を使用します。

ステップ 1 Real-Time Monitoring Tool の [システム（System）] 領域で、[アラート セントラル（Alert Central）] をクリックします。

ステップ 2 [アラート セントラル（Alert Central）] ウィンドウで、**TCPRemoteSyslogDeliveryFailed** を選択します。

ステップ 3 [システム（System）] > [ツール（Tools）] > [アラート（Alert）] > [アラート アクションの設定（Config Alert Action）] の順に選択します。

ステップ 4 [アラート アクション（Alert Action）] ポップアップで、[デフォルト（Default）] を選択して、[編集（Edit）] をクリックします。

ステップ 5 [アラート アクション（Alert Action）] ポップアップで、受信者を追加します。

ステップ 6 ポップアップ ウィンドウで、電子メール アラートを送信するアドレスを入力して、[OK] をクリックします。

ステップ 7 [アラート アクション（Alert Action）] ポップアップで、アドレスが [受信者（Recipients）] に表示されていることと、[有効（Enable）] チェックボックスがオンになっていることを確認します。

ステップ 8 [OK] をクリックします。

第 8 章

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。Unity 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。

綿密に考えられた認証規則により、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することで、Cisco Personal Communications Assistant（Cisco PCA）や Cisco Unity Connection Survivable Remote Site Voicemail などの Unity Connection アプリケーションへの不正アクセスを阻止できます。

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）、Unity 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。

Unity 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。

- パスワード、PIN、および認証規則の管理，49 ページ

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。Unity 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。

綿密に考えられた認証規則により、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することで、Cisco Personal Communications Assistant（Cisco PCA）や Cisco Unity Connection Survivable Remote Site Voicemail などの Unity Connection アプリケーションへの不正アクセスを阻止できます。

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）、Unity 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。

Unity 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 Unity Connection 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 ユーザは、さまざまな Unity Connection アプリケーションへのアクセスに異なる PIN やパスワードを使用します。Unity 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

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 Unity 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
- Cisco Unity Connection SRSV Administration

（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 Unity Connection Web アプリケーションにアクセスする必要があります。ユーザに対して、Cisco Unity Connection で、一意で安全な PIN およびパスワードを最初に割り当てるようにします。

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 Unity 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、[Users（ユーザ）]>[Users（ユーザ）]>[Change Password（パスワードの変更）] 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 [ユーザは次回サインイン時に変更する必要あり（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 Unity 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、ヘルプを参照してください。

Unity Connection SRSV のパスワードと共有秘密

中央 Unity Connection サーバから Unity Connection SRSV サーバに対するすべての要求は通信に Unity Connection SRSV 管理者クレデンシャルを使用しますが、Unity Connection SRSV から Unity Connection への要求は、認証に秘密トークンを使用します。

中央 Unity Connection サーバは、Unity Connection SRSV の管理者ユーザ名とパスワードを使用してサーバへのアクセスを認証します。Unity Connection SRSV のユーザ名とパスワードは、中央 Unity Connection サーバに新しいブランチを作成するときに、Connection データベースに格納されます。

Unity Connection SRSV を使用するプロビジョニング サイクルごとに、中央 Unity Connection サーバは秘密トークンを生成し、Unity Connection SRSV と共有します。Unity Connection SRSV サイトからプロビジョニングが完了した後、中央 Unity Connection サーバに同じトークンを使用して通知します。その後、プロビジョニング サイクルの完了後すぐ、このトークンは中央 Unity Connection と Unity Connection SRSV サーバの両方から削除されます。ランタイム トークン キーの概念は、共有秘密として知られています。

Unity Connection SRSV の詳細については、『Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV) Release 12.x』を参照してください。このガイドは https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/srsv/guide/b_12xcucsrsvx.html にあります。

Web アプリケーション パスワードの変更

Web アプリケーション（Cisco PCA）のパスワードは、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 Administration 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。

また、ユーザは Unity Connection Messaging Assistant で各自の Cisco PCA パスワードを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、ヘルプを参照してください。また、Cisco Unity Connection 一括管理ツール（BAT）を使用して、複数のユーザ パスワードを一括で変更できます。

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。

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。

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、Unity Connection の電話カンバセーションや Unity 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、ヘルプを参照してください。また、Cisco Unity Connection 一括管理ツール（BAT）を使用して、複数のユーザ PIN を一括で変更できます。

PIN が期限切れになると、ユーザは、Unity Connection 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 Web 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。

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 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 認証が有効な場合には適用されません。これは、このような状況では認証が Unity Connection で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 Unity 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の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 Administration 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、Unity Connection 電話インターフェイス、Cisco PCA、または Connection Administration 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 Unity 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）：

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、Unity 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。

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 Unity 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。

連続するクレデンシャル間での最小変更文字数（Minimum Number of Character Changes between Successive Credentials）：

このフィールドを使用して、ユーザが Web アプリケーション パスワードの更新時に変更する必要がある文字の数を指定します（PIN には適用されません）。

このフィールドの値は、[最小クレデンシャル長（Minimum Credential Length）] フィールドの値以下に設定してください。

デフォルトでは、このフィールドの値は 1 に設定されており、ユーザは古いパスワードと新しいパスワードの間で少なくとも 1 文字を変更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、Unity 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、Unity Connection で、新しいパスワードまたは PIN が、クレデンシャル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。Unity 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、Unity Connection のクレデンシャル履歴に 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。
- 数字は 3 回以上続けて使用できない（たとえば 28883）。

- PIN は、昇順または降順の連続する数値（012345、987654 など）ではない。
- PIN に、許可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 桁の長さが許可されている場合、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。

Unity Connection SRSV ユーザ PIN の変更

Unity Connection SRSV ユーザ PIN を変更する場合、Cisco Unity Connection Administration インターフェイスを介して実行できます。選択したユーザの PIN を変更した後、Unity Connection SRSV データベースのユーザ情報を更新するよう、関連するブランチをプロビジョニングする必要があります。

（注） Cisco Unity Connection SRSV Administration インターフェイスを介して SRSV ユーザの PIN を変更することはできません。

同時セッションの最大数の制限

Unity Connection では、ユーザが次に示すインターフェイスで実行できる同時セッションの最大数を管理者が制限できるようにすることで、セキュリティ強化を図っています。

- **テレフォニー インターフェイス**：テレフォニー インターフェイスでは、設定されている最大制限数を超えてユーザが新しいセッションを試行すると、コールが切断されます。
- **ビジュアル ボイスメール インターフェイス**（*PIN* ベースの認証）：ビジュアル ボイスメールインターフェイスでは、設定されている最大制限数を超えてユーザが新しいセッションを試行すると、ユーザはインターフェイスにログインできなくなります。
  テレフォニー セッションまたはビジュアル ボイスメール セッションには、プライマリ内線番号と代行内線番号の両方からのコールが含まれます。両方のインターフェイスでこの機能を有効にするには、Cisco Unity Connection Administration にログインし、[システム設定（System Settings）] > [詳細設定（Advanced）] > [カンバセーション（Conversation）] に移動し、[テレフォニー インターフェイスの最大セッション数（ユーザあたり）（Maximum Concurrent

Sessions for Telephony Interface (Per User)）] フィールドにセッションの最大数の値を入力します。

- **IMAP インターフェイス**：IMAP インターフェイスでは、設定されている最大制限数を超えてユーザが IMAP アカウントにログインしようとすると、ログインが失敗します。IMAP インターフェイスでこの機能を有効にするには、Cisco Unity Connection Administration にログインし、[システム設定（System Settings）] > [詳細設定（Advanced）] > [メッセージング（Messaging）] に移動し、[IMAP インターフェイスの最大セッション数（ユーザあたり）（Maximum Concurrent Sessions for IMAP Interface (Per User)）] フィールドにセッションの最大数の値を入力します。

デフォルトでは、[テレフォニーインターフェイスの最大セッション数（ユーザあたり）（Maximum Concurrent Sessions for Telephony Interface (Per User)）] と [IMAP インターフェイスの最大セッション数（ユーザあたり）（Maximum Concurrent Sessions for IMAP Interface (Per User)）] フィールドの値がゼロに設定されています。この場合、この機能は無効です。

（注） このフィールドの推奨最小値は、Outlook 2010 では 4、Outlook 2013 では 2 です。

非アクティブ タイムアウトの設定

Unity Connection のセキュリティ強化のための新機能では、管理者がユーザの非アクティブ タイムアウトの日数を設定できます。ユーザが Unity Connection インターフェイス（TUI や Web Inbox など）からボイスメール アカウントにログインしていない期間が、設定された日数に達すると、アカウントが無効になり、今後のアクセスが拒否されます。

この機能を有効にするには、Cisco Unity Connection Administration にログインし、[システム設定（System Settings）] > [詳細設定（Advanced）] > [Connection 管理（Connection Administration）] に移動し、[ユーザの非アクティブ タイムアウト（日数）（User Inactivity Timeout (in Days)）] フィールドに非アクティブ タイムアウトの値を入力します。

（注） デフォルトでは [ユーザの非アクティブ タイムアウト（日数）（User Inactivity Timeout (in Days)）] フィールドの値はゼロに設定されており、この機能は無効になっています。

この機能が有効な場合は、以下の設定が Unity Connection に適用されます。

- 非アクティブなユーザを検索するため、Cisco Unity Connection Administration の [ユーザ（Users）]>[ユーザの検索（Search Users）]ページで検索条件を [非アクティブ ユーザ（Inactive Users）] に絞り込むことができます。
- Cisco Unity Connection Administration の [ユーザ（Users）] > [ユーザの基本設定の編集（Edit User Basics）] で、ユーザの [ボイスメール アプリケーションへのアクセス（VoiceMail Application Access）] を [アクティブ（Active）] または [非アクティブ（Inactive）] に更新できます。

- 設定された間隔で [非アクティブ ユーザの確認（Check Inactive Users）] sysagent タスクを実行し、ユーザがログインしていない期間が設定されている日数を超えている場合にそのユーザを非アクティブにするように設定できます。

第 9 章

Cisco Unity Connection のセキュリティ パスワード

Cisco Unity Connection のセキュリティ パスワード

セキュリティ パスワードについて

Unity 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。

- Unity 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、ディザスタ リカバリ システムの暗号キーとして使用されます。Unity 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 12.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/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html から入手可能です。

第 10 章

SSL を使用したクライアント/サーバ接続の保護

SSL を使用したクライアント/サーバ接続の保護

はじめに

この章では、Cisco Personal Communications Assistant（Cisco PCA）、および IMAP 電子メール クライアントが Cisco Unity Connection へ安全にアクセスするための、証明書の署名要求の作成、SSL 証明書の発行（または外部の認証局による証明書の発行）、および Cisco Unity Connection サーバにおける証明書のインストールについて説明します。

Cisco PCA の Web サイトでは、ユーザが Unity 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 Unity 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。

関連資料

この章には、マルチサーバの証明書またはシングルサーバの証明書を使用して、ユーザが証明書署名要求（CSR）を作成、生成、ダウンロードおよびアップロードする必要がある場合の複数のインスタンスが含まれています。詳細については、『Cisco Unified Communications Operating System Administration Guide for Cisco Unity Connection Release 12.x』の「Security」の章を参照してください。このガイドは https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/os_administration/b_12xcucosagx.html にあります。

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

Unity Connection をインストールする場合、ローカル自己署名証明書が自動的に作成されてインストールされ、Cicso PCA と Unity Connection との間の通信、IMAP 電子メール クライアントと Unity Connection との間の通信、および Unity Connection SRSV と中央 Unity Connection サーバとの間の通信が保護されます。これは、Cisco PCA と Unity Connection との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、IMAP クライアントで暗号化を有効にした場合は IMAP 電子メール クライアントと Unity Connection との間のネットワーク トラフィックが自動的に暗号化され、Unity Connection SRSV と中央 Unity Connection サーバとの間のネットワーク トラフィックが自動的に暗号化されることを意味しています。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 Unity 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 12.x』の「Setting Up Access to the Cisco Personal Communications Assistant」の章の「Managing Security Alerts When Using Self-Signed Certificates with SSL Connections」の項を参照してください。このガイドは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/user_setup/guide/b_12xcucuwsx.html にあります。

自己署名証明書の詳細については、『Complete Reference Guide for Cisco Unity Connection Survivable Remote Site Voicemail (SRSV), Release 12.x』の「Security in Cisco Unity Connection Survivable Remote Site Voicemail」の章を参照してください。このガイドは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/srsv/guide/b_12xcucsrsvx.html にあります。

Connection Administration、Cisco PCA、Unity Connection SRSV、および IMAP 電子メール クライアントから Unity Connection へのアクセスの保護

Cisco Unity Connection Administration、Cisco Personal Communications Assistant、Unity Connection SRSV、および IMAP 電子メール クライアントから 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および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。

2 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 3 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 3 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 3 に進みます。

3 Unity Connection クラスタが設定されている場合は、`set web-security` CLI コマンドを実行するか、あるいはクラスタの両方の Unity Connection サーバ用のマルチサーバ SAN 証明書（SIP 統合の場合のみ）を生成し、両方のサーバに同じ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/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html から入手可能です。

4 Unity Connection クラスタを設定している場合は、タスク 3 で割り当てた別名が含まれている DNS A レコードを設定します。最初にパブリッシャ サーバを一覧表示します。これにより、すべての IMAP 電子メール アプリケーション、Cisco Personal Communications Assistant、および Unity Connection SRSV が、同一の Unity Connection サーバ名を使用して Unity Connection ボイス メッセージにアクセスできます。

5 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。

Unity Connection クラスタをシングルサーバ証明書署名要求により設定する場合は、Unity Connection クラスタ内の両方のサーバでこのタスクを実行します。

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、次を参照します。

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 7 に進みます。

Unity 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。

Unity Connection クラスタをシングルサーバ証明書署名要求により設定する場合は、Unity Connection クラスタ内の両方のサーバでこのタスクを実行します。

7 ルート証明書とサーバ証明書を Unity Connection サーバにアップロードします。

Unity Connection クラスタをシングルサーバ証明書署名要求により設定する場合は、Unity Connection クラスタ内の両方のサーバでこのタスクを実行します。

8 Unity Connection IMAP サーバ サービスを再起動して、Unity 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 サービスの再起動」を行います。

Unity Connection クラスタが設定されている場合は、Unity 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 ユーザが Connection Administration、Cisco PCA、または IMAP 電子メール クライアントを使用して Unity 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 Unity 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 7 で Unity 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 7 で Unity 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。

IMAP サーバ サービスの再起動

ステップ 1 Cisco Unity Connection Serviceability にサインインします。

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 サービスに対し [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（Status）] エリアに表示されたら、このサービスの [開始（Start）] を選択します。

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 に対し 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/c/en/us/support/conferencing/unified-meetingplace/products-maintenance-guides-list.html から入手可能です。

2 Unity Connection と MeetingPlace を統合します。Unity 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。

3 Unity 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。次の点に注意してください。

4 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。

- 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。
- Unity 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。

Unity Connection と Cisco Unity ゲートウェイ サーバ間の通信の保護

ネットワークが Unity Connection で設定されている場合に、Connection Administration、Cisco Personal Communications Assistant、および IMAP 電子メール クライアントから 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。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 Unity Connection クラスタが Unity 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 Unity 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/c/en/us/support/unified-communications/unity-connection/products-maintenance-guides-list.html から入手可能です。

3 Unity Connection ゲートウェイ サーバに対応して Unity Connection クラスタを設定している場合は、タスク 2 で割り当てた別名が含まれている DNS A レコードを設定します。最初にパブリッシャ サーバを一覧表示します。これにより、Cisco Unity が同じ Unity Connection サーバ名を使用して Unity Connection のボイス メッセージにアクセスできます。

（注） Unity 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。Unity Connection クラスタが設定されている場合は、Unity 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。

（注） 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 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。

4 ルート証明書のエクスポートとサーバ証明書の発行に Microsoft 証明書サービスを使用している場合は、「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）」で説明する手順を実行します。

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。

Unity 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 である必要があります。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、Unity Connection サーバ（Unity 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。

5 ルート証明書とサーバ証明書を Unity Connection サーバにアップロードします。

（注） Unity Connection クラスタが設定されている場合は、Unity 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 Unity Connection IMAP サーバ サービスを再起動して、Unity 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。「IMAP サーバ サービスの再起動」を行います。

Unity Connection クラスタが設定されている場合は、Unity 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 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。

（注） 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。

Cisco Unity ゲートウェイ サーバでの証明書署名要求の作成とダウンロード

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) サイトの共通名として、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、Unity 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。

Connection IMAP サーバ サービスの再起動

ステップ 1 Cisco Unity Connection Serviceability にサインインします。

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 サービスに対し [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（Status）] エリアに表示されたら、このサービスの [開始（Start）] を選択します。

Cisco Unity サーバへのルート証明書とサーバ証明書のアップロード

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 2008）

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。

ステップ 1 [サーバマネージャ（Server Manager）] を開き、[役割の追加（Add Roles）] をクリックし、[次へ（Next）] をクリックして、[Active Directory 証明書サービス（Active Directory Certificate Services）] をクリックします。[次へ（Next）] を 2 回クリックします。

ステップ 2 [役割サービスの選択（Select Role Services）] ページで、[証明機関（Certification Authority）] をクリックします。[次へ（Next）] をクリックします。

ステップ 3 [セットアップの種類の指定（Specify Setup Type）] ページで、[スタンドアロン（Standalone）] または [エンタープライズ（Enterprise）] をクリックします。[次へ] をクリックします。

（注） エンタープライズ CA をインストールするには、ドメイン コントローラへのネットワーク接続がなければなりなりません。

ステップ 4 [CA の種類の指定（Specify CA Type）] ページで、[ルート CA（Root CA）] をクリックします。[次へ（Next）] をクリックします。

ステップ 5 [秘密キーの設定（Set Up Private Key）] ページで、[新しい秘密キーを作成する（Create a new private key）] をクリックします。[次へ（Next）] をクリックします。

ステップ 6 [暗号化の構成（Configure Cryptography）] ページで、暗号化サービス プロバイダー、キーの長さおよびハッシュ アルゴリズムを選択します。[次へ（Next）] をクリックします。

ステップ 7 [CA 名を構成（Configure CA Name）] ページで、CA を識別する一意の名前を作成します。[次へ（Next）] をクリックします。

ステップ 8 [有効期間の設定（Set Validity Period）] ページで、ルート CA 証明書を有効にする年数または月数を指定します。[次へ（Next）] をクリックします。

ステップ 9 証明書データベースおよび証明書データベース ログのカスタムの場所を指定しない場合は、[証明書データベースを構成（Configure Certificate Database）] ページで、デフォルトの場所をそのまま使用します。[次へ（Next）] をクリックします。

ステップ 10 [インストール オプションの確認（Confirm Installation Options）] ページで、選択した設定すべてを確認します。これらのオプションのすべてを受け入れる場合は、[インストール（Install）] をクリックして、セットアップ プロセスが終了するまで待ちます。

ステップ 11 [Active Directory 認証局（Active Directory Certificate Authority）] を右クリックします。[役割サービスの追加（Add Role Services）] を選択し、[証明機関 Web 登録（Certificate Authority Web Enrollment）]、[オンライン レスポンダー（Online Responder）]、[ネットワーク デバイス登録サービス（Network Device Enrollment Service）] のチェックボックスを選択し、これらのサービスをインストールします。

ステップ 12 [サーバー マネージャー（Server Manager）] > [ロールの追加（Add Role）] > [次へ（Next）] と移動し、[Web Server (IIS)] ボックスを選択し、これをインストールします。

ステップ 13 [Web サーバ（IIS）（Web Server (IIS)）] を右クリックします。[役割サービスの追加（Add Role Services）] を選択し、役割サービスすべてを確認し、インストールします。

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）

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 証明書サービスのインストール（Windows Server 2008）」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。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。
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) 作成した証明書署名要求ファイルの場所を参照し、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 データを含む列（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する（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。

第 11 章

ユーザ メッセージの保護

ユーザ メッセージの保護

はじめに

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 Unity 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。Unity 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。

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の処理

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 Unity 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

- 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、「IMAP クライアント アクセス用メッセージ セキュリティ オプション」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。
- 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）。
- デフォルトの Unity Connection では、SMTP リレー アドレスにメッセージをリレーするように 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 Unity 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 メッセージの場合、Cisco Unity Connection ViewMail for Microsoft Outlook と Cisco Unity Connection ViewMail for IBM Lotus Notes の Media Player 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、Unity Connection を設定できます。
- 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再生できます。
  - Unity Connection 電話インターフェイス
  - Web Inbox
  - Cisco ViewMail for Microsoft Outlook（バージョン 8.5 以降）
  - Cisco Unity Connection ViewMail for IBM Lotus Notes
  - 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 を使用したセキュア メッセージの再生に関する要件については、該当する『Release Notes for Cisco Unified Messaging with IBM Lotus Sametime』（http://www.cisco.com/c/en/us/support/unified-communications/

unified-communications-manager-callmanager/products-release-notes-list.html）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転送できます。
  - Unity Connection 電話インターフェイス
  - Web Inbox
  - 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 Unity 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 Unity 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 Unity Connection ユーザ、および同報リストにある Unity 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 Unity 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、Unity 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。
- Unity 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、Unity 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、Unity 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、Unity 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、Unity 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 Unity 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 を使用して転送することはできません。
- ViewMail for Outlook 8.0 と ViewMail for Notes ではセキュア メッセージの再生だけがサポートされています。
- 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（Require Secure Messaging）] フィールドが [常時（Always）] または [選択可能（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 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 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。「サービス クラス（COS）メンバーのメッセージ セキュリティの有効化」を参照してください。（ユーザが Unity 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」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ユーザおよびユーザ テンプレートを設定する」を参照してください。
4. Unity 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。

サービス クラス（COS）メンバーのメッセージ セキュリティの有効化

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～ステップ 3 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

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

ステップ 1 Cisco Unity Connection 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。

セキュアな削除のためのメッセージ ファイルの破棄

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 Cisco Unity Connection Administration の [ツール（Tools）] > [タスク管理（Task Management）] 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 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、Unity 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復できないことを保障するには、次の機能を使用しないでください：メッセージ リレー、IMAP、ViewMail for Outlook、ViewMail for Notes、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接続されたサーバ間の SMTP スマート ホスト。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 メッセージングを使用する場合、セキュア 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 Unity Connection サーバ上に残り、削除時に破棄されます。

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

- Unity 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。

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。

IMAP クライアント アクセス用メッセージ 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）。

第 12 章

Next Generation Security

概要

Cisco Unity Connection では、Suite B 暗号化アルゴリズムを使用して機密性、整合性、および認証を提供する Next Generation Security がサポートされています。Suite B アルゴリズムには、組織のセキュリティ要件とスケーラビリティ要件に対応できるように、さまざまなコンポーネント（AES 暗号化、ECDSA 暗号など）を組み込むことができます。

Next Generation Security	サポートされるバージョン
認証署名アルゴリズム。	RSA（1024/2048/3092/4096） ECDSA（256/384/512）
メッセージ整合性	SHA-256 SHA-384 SHA-512
暗号化	AES-GCM（128/256）モード
鍵共有	ECDH（256/384）

（注）
- Unity Connection では、Next Generation Security 向けに TLS 1.2 をサポートしています。
- Next Generation Security では、FIPS が有効な場合は RSA 1024 キーはサポートされません。

Unity Connection では、次のインターフェイスで Next Generation Security がサポートされています。

- HTTPS
- SIP
- SRTP

（注）上記のインターフェイスの他に、Unity Connection では SMTP インターフェイスとデフォルト暗号設定で Next Generation Security をサポートしています。

Next Generation Security Over HTTPS インターフェイス

Next Generation Security Over HTTPS インターフェイスにより、tomcat または jetty 経由で導入された Web アプリケーションは、Unity Connection とのインバウンド接続に Suite B 暗号を使用するように制限されます。ユーザは、Jetty または Web インターフェイスで Next Generation Security をアクティブにするには、SSL を有効にする必要があります。Connection Jetty での SSL の有効化の詳細については、該当する『*Command Line Interface Guide*』を参照してください。このガイドは、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html にあります。

Next Generation Security Over HTTPS インターフェイスの設定

Next Generation Security over HTTPS インターフェイスを設定するには、次の手順を実行します。

ステップ 1 [Cisco Unity Connection の管理（Cisco Unity Connection Administration）] ページにサインインし、[システム設定（System Settings）] > [全般設定（General Configuration）] を展開し、[HTTPS 暗号（HTTPS Ciphers）] を選択します。

ステップ 2 次のオプションのいずれかを選択します。

- [サポートされているすべての EC および RSA 暗号（All Supported EC and RSA Ciphers）]：このオプションが選択されている場合、Unity Connection サーバは EC ベースの暗号および RSA ベースの暗号の両方とネゴシエートします。
- [RSA 暗号のみ（RSA Ciphers Only）]：このオプションが選択されている場合、Unity Connection サーバは RSA ベースの暗号とのみネゴシエートします。

次の表に、RSA または ECDSA 暗号の優先順に HTTPS 暗号オプションを示します。

表 *7*：*HTTPS* 暗号オプションと優先順位

HTTPS 暗号オプション	HTTPS 暗号（優先順）
サポートされているすべての EC および RSA 暗号（All Supported EC and RSA Ciphers）	• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA • SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
RSA 暗号のみ（RSA Ciphers Only）	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • SSL_RSA_WITH_3DES_EDE_CBC_SHA • SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA

ステップ 3 [保存（Save）] を選択して変更内容を適用します。

（注） HTTPS 暗号の変更後に、変更を反映するため Tomcat Service を必ず再起動してください。また、jetty SSL が有効な場合は、utils cuc jetty ssl {disable/enable} コマンドを使用して jetty over SSL を無効または有効にする必要があります。

Next Generation Security Over SIP インターフェイス

Next Generation Security over SIP インターフェイスにより、SIP インターフェイスは TLS 1.2、SHA-2、および AES256 プロトコルに基づいて Suite B 暗号を使用するように制限されます。RSA 暗号または ECDSA 暗号の優先順位に基づいて、暗号をさまざまな組み合わせで使用できます。

Next Generation Security over SIP インターフェイスを有効にするために使用する暗号を指定するには、[システム設定（System Settings）] > [全般設定（General Configuration）] に移動し、[TLS サイファ（TLS Ciphers）] ドロップダウン リストから暗号を選択します。

SIP インターフェイスでの暗号とサードパーティ証明書の設定の詳細については、『Cisco Unified Communication Manager SIP Integration Guide for Cisco Unity Connection Release 12.x』の「Setting Up a Cisco Unified Communications Manager SIP Trunk Integration」の章の「Enabling Next Generation Security over SIP Integration」を参照してください。このガイドは、https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/integration/guide/cucm_sip/b_12xcucintcucmsip.html にあります。

Next Generation Security Over SRTP インターフェイス

Next Generation Security Over SRTP インターフェイスにより、SRTP インターフェイスは SHA-2 および AES256 プロトコルに基づいて Suite B 暗号を使用するように制限されます。

Next Generation Security over SRTP インターフェイスを有効にするために使用する暗号を指定するには、[システム設定（System Settings）] > [全般設定（General Configuration）] に移動し、[SRTP サイファ（SRTP Ciphers）] ドロップダウン リストから暗号を選択します。

SRTP インターフェイスでの暗号とサードパーティ証明書の設定の詳細については、『Cisco Unified Communication Manager SIP Integration Guide for Cisco Unity Connection Release 12.x』の「Setting Up a Cisco Unified Communications Manager SIP Trunk Integration」の章の「Enabling Next Generation Security over SIP Integration」を参照してください。このガイドは、http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/integration/guide/cucm_sip/b_12xcucintcucmsip.html にあります。