ユニファイド コミュニケーションのサーバ証明書要件

この章では、次の内容について説明します。

Cisco Unified Communications Manager の証明書

Mobile & Remote Access で重要な Cisco Unified Communications Manager 証明書は、次の 2 つです。

- *CallManager* 証明書
- *tomcat* 証明書

これらの証明書は Cisco Unified Communications Manager に自動的にインストールされ、デフォルトで自己署名されて同じ一般名（CN）を持ちます。

CA によって署名された証明書を使用することを推奨します。ただし、自己署名証明書を使用する場合、2 つの証明書の一般名は異なる必要があります。Expressway では同じ CN を持つ 2 つの自己署名証明書は許可されません。そのため、Expressway の信頼される CA リストで *CallManager* と *tomcat* の自己署名証明書の CN が同じ場合、Expressway はそのうちの 1 つしか信頼できません。つまり、Expressway-C と Cisco Unified Communications Manager 間のセキュア HTTP またはセキュア SIP は失敗します。

また、シスコ コラボレーション システム リリース 10.5.2 内の製品に対して tomcat 証明書の署名要求を生成する場合、CSCus47235 に注意する必要があります。ノードの FQDN がサブジェクト代替名（SAN）エントリとして証明書に含まれるようにするため、この問題を回避する必要があります。「リリース ノート」ページにある *Expressway X8.5.3* のリリース ノートに回避策の詳細が記載されています。

IM and Presence Service の証明書

XMPP を使用する場合に重要となる IM and Presence Service 証明書は、次の 2 つです。

- *cup-xmpp* 証明書
- *tomcat* 証明書

CA によって署名された証明書を使用することを推奨します。ただし、自己署名証明書を使用する場合、2 つの証明書の一般名は異なる必要があります。Expressway では同じ CN を持つ 2 つの自己署名証明書は許可されません。*cup-xmpp* 証明書と *tomcat*（自己署名）証明書が同じ CN を持つ場合、Expressway はそのうちの 1 つしか信頼せず、Cisco Expressway サーバーと IM and Presence Service サーバー間の 一部の TLS 試行が失敗します。詳細については、CSCve56019 を参照してください。

Expressway 証明書

Expressway の証明書署名要求（CSR）ツールでは、Expressway でサポートされるユニファイド コミュニケーション機能に適した関連するサブジェクト代替名（SAN）について確認が求められ、組み込まれます。

次の表は、どのユニファイドコミュニケーションの機能にどのCSR代替名の要素が適用されるかを示します。

サブジェクト代替名としてこれらの項目を追加します	**これらの目的で CSR を生成する場合**			
	モバイル & リモート アクセス	Jabber Guest	XMPP フェデレーション	ビジネス ツー ビジネス コール
Unified CM 登録ドメイン（ドメイン名にかかわらず、これらは Unified CM SIP 登録ドメインよりもサービス検出ドメインと共通点があります）	Expressway-E でのみ必要	—	—	—
XMPP フェデレーション ドメイン	—	—	Expressway-E でのみ必要	—

サブジェクト代替名としてこれらの項目を追加します	これらの目的で CSR を生成する場合			
IM and Presence チャットノードエイリアス （フェデレーション グループ チャット）	—	—	必須	—
Unified CM 電話セキュリティ プロファイル名	Expressway-C でのみ必要	—	—	—
（クラスタ化されたシステムのみ）Expressway クラスタ名	Expressway-C でのみ必要	Expressway-C でのみ必要	Expressway-C でのみ必要	—

（注）
- チャット ノード エイリアスを追加するか、名前を変更する場合、Expressway-C 用の新しいサーバ証明書の作成が必要になることがあります。つまり、IM and Presence ノードが追加されるか名前が変更される場合、または新しい TLS 電話セキュリティ プロファイルが追加される場合などです。
- 新しいチャット ノード エイリアスがシステムに追加される場合、または CM か XMPP フェデレーション ドメインが変更される場合は、新しい Cisco Expressway-E の証明書を作成する必要があります。
- 新しくアップロードされたサーバ証明書を有効にするには、Expressway を再起動する必要があります。

Expressway-C/Expressway-E の個々の機能要件についての詳細は、次のとおりです。

Expressway-C のサーバ証明書の要件

Expressway-E サーバー証明書には、そのサブジェクト代替名（SAN）のリストに次の要素が含まれる必要があります。

- **Unified CM 電話機セキュリティ プロファイル**：暗号化された Transport Line Signaling（TLS）用に構成され、リモートアクセスを必要とするデバイスに使用される Unified CM の**電話機セキュリティ プロファイル**の名前。完全修飾ドメイン名（FQDN）形式を使用し、複数のエントリをカンマで区切ります。

  Expressway-C の既存のクラスタに新しい Expressway-C ノードを追加する間は、新しいノードの証明書署名要求（CSR）を生成する必要があります。CUCM でモバイルおよびリモートア

クセス（CUCM）クライアントの安全な登録が必要な場合、CUCM に安全なプロファイル名を付ける必要があります。「Unified CM Phone のセキュリティプロファイル名」が CUCM デバイスのセキュリティプロファイルの名前またはホスト名だけである場合、新しいノードでの CSR の作成は失敗します。これにより、管理者は **[安全な電話機プロファイル（Secure Phone Profile）]** ページの下で、CUCM で 「Unified CM Phone のセキュリティプロファイル名」の値を変更する必要があります。

X12.6から、Unified CMのセキュリティプロファイル名は完全修飾ドメイン名（FQDN）である必要があります。名前、ホスト名、または値だけでは使用できません。

たとえば、`jabbersecureprofile.domain.com`、`DX80SecureProfile.domain.com`

（注） FQDNは複数レベルで構成できます。各レベルの名前に使用できるのは文字、数字、ハイフンのみで、各レベルはピリオド（ドット）で区切ります。レベル名はハイフンで開始または終了できません。また、最後のレベル名は文字で開始する必要があります。

代替名としてセキュア電話プロファイルを持つことは、Unified CM がそのプロファイルを使用するデバイスからメッセージを転送する場合に、Expressway-C とトランスポートラインシグナリング（TLS）経由で通信できることを意味します。

- **IM and Presence チャットノードエイリアス（フェデレーテッドグループチャット）**：IM and Presence サーバーで設定される**チャットノードエイリアス**（たとえばchatroom1.example.com）。これらは、フェデレーテッド連絡先とのTLSを介したグループチャットをサポートするユニファイド コミュニケーション XMPP フェデレーション導入にのみ必要です。

  Expressway-C は一連の IM&P サーバを検出すると、CSR にチャット ノード エイリアスを自動的に含めます。

CSR を生成するときは、チャット ノード エイリアスに DNS 形式を使用することを推奨します。Expressway-E サーバ証明書の代替名には、同一のチャット ノードエイリアスを含める必要があります。

図 *1: Expressway-C* の証明書署名要求ジェネレータでのセキュリティプロファイルおよびチャットノードエイリアスに対するサブジェクト代替名の入力

Expressway-E のサーバ証明書の要件

Expressway-E サーバ証明書には、そのサブジェクト代替名（SAN）のリストに次の要素が含まれる必要があります。Expressway-E が他の FQDN によって知られている場合は、すべてのエイリアスがサーバ証明書 SAN に含まれている必要があります。

- **Unified CM 登録ドメイン**：Unified CM の登録用に Expressway-C で構成されているすべてのドメイン。エンドポイント デバイスと Expressway-E 間のセキュアな通信に必要です。

  Expressway の設定と Expressway-E の証明書に使用される Unified CM 登録ドメインは、サービス検出時に *_collab-edge* DNS SRV レコードをルックアップするモバイルおよびリモート アクセス クライアントによって使用されます。これにより、Unified CM での MRA 登録が有効になり、サービス検出に役立ちます。

  これらのサービス検出ドメインは SIP 登録ドメインと一致することもしないこともあります。これは展開方法により異なるため、一致する必要はありません。たとえば、社内ネットワークの Unified CM で .local または類似するプライベート ドメインを使用し、Expressway-E FQDN とサービス検出にパブリック ドメイン名を使用する展開の場合、Expressway-E の証明書にパブリック ドメイン名を SAN として含める必要があります。Unified CM で使用するプライベート ドメイン名を含める必要はありません。エッジ ドメインのみを SAN としてリストする必要があります。

  DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。代わりに、*CollabEdgeDNS* フォーマットを選択でき、これは、入力するドメインにプリフィックス collab-edge を追加するだけである。この形式は、トップ レベル ドメインを SAN として含めたくない場合に推奨されます（次のスクリーンショットの例を参照してください）。

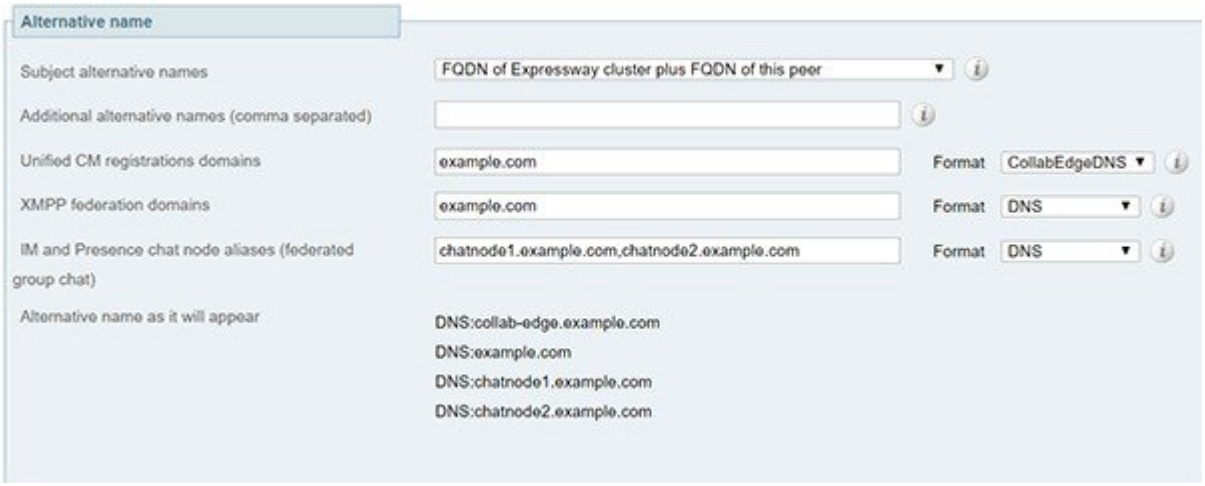
- **XMPP フェデレーションドメイン**：ポイントツーポイント XMPP フェデレーションに使用するドメイン。これらは、IM&P サーバで設定され、XMPP フェデレーション用のドメインとして Expressway-C でも設定する必要があります。

  DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。*XMPPAddress* 形式を使用しないでください。この形式は CA によってサポートされない可能性があり、Expressway ソフトウェアの将来のバージョンでは廃止される可能性があります。

- **IM and Presence チャット ノード エイリアス（フェデレーテッド グループ チャット）**：Expressway-C の証明書で入力されたものと同じ**チャットノードエイリアス**のセット。フェデレーテッド連絡先との TLS を介したグループ チャットをサポートする音声とプレゼンスの導入にのみ必要です。

  チャットノードエイリアスのリストは、Expressway-C 対応の「**CSR の作成（Generate CSR）**」ページからコピーできます。

図 *2 : Expressway-E* の 証明書署名要求ジェネレータでの *Unified CM* 登録ドメイン、*XMPP* フェデレーション ドメイン、およびチャット ノード エイリアスに対するサブジェクト代替名の入力



翻訳について
このドキュメントは、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。