次世代のセキュリティ

- 概要 （1 ページ）
- Next Generation Security Over HTTPS インターフェイス （2 ページ）
- Next Generation Security Over SIP インターフェイス （3 ページ）
- Next Generation Security Over SRTP インターフェイス （4 ページ）

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拡張性の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。

次世代のセキュリティ	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（Encryption）	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 経由で展開された 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 *1* : *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）
すべてのサポートされているECおよびRSA暗号方式	• 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暗号方式のみ	• 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（SRTP Ciphers）]** ドロップダウンリストから暗号を選択します。

（注） SIP インターフェイスでの次世代のセキュリティは、暗号化セキュリティ モードのみを使用します。

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 14*』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/14/integration/cucm_sip/b_14cucintcucmsip.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 14*』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/14/integration/cucm_sip/b_14cucintcucmsip.html にあります。