暗号管理

暗号管理

暗号の管理はオプションの機能で、すべての TLS および SSH 接続で許可されるセキュリティ暗号のセットを制御できます。暗号管理を使用すると、弱い暗号を無効にして最小レベルのセキュリティを有効にすることができます。

[**Cipher Management**] ページには、デフォルト値はありません。代わりに、暗号化管理機能は、許可されている暗号を設定している場合にのみ有効になります。**[暗号管理（Cipher Management）]** ページで設定している場合でも、特定の弱い暗号は許可されません。

次の TLS インターフェイスおよび SSH インターフェイスで暗号を設定することができます。

- [All TLS（すべての TLS）]：このフィールドに割り当てられている暗号は、Unified Communications Manager および IM and Presence Service の TLS プロトコルをサポートするすべてのサーバおよびクライアント接続に適用されます。
- [HTTPS TLS]：このフィールドに割り当てられる暗号は、Unified Communications Manager および IM and Presence Service の TLS プロトコルをサポートするポート 443 および 8443 上のすべての Cisco Tomcat 接続に適用されます。

（注） **[HTTPS TLS]** および **[すべての TLS（All TLS）]** フィールドに暗号を割り当てる場合、**[HTTPS TLS]** 上で設定されている暗号が **[すべての TLS（All TLS）]** 暗号を上書きします。

- **SIP TLS**: このフィールドに割り当てられる暗号は、ユニファイドコミュニケーションマネージャー上の TLS プロトコルをサポートする sip tls インターフェイスを介して送受信されるすべての暗号化接続に適用されます。SCCP または CTI デバイスには適用されません。

認証モードの SIP インターフェイスは、ナル-SHA 暗号のみをサポートしています。

SIP インターフェイスまたはすべてのインターフェイスで暗号化を設定した場合は、認証モードはサポートされなくなります。

SIP TLSおよび**ALL TLS**フィールドで暗号を割り当てる場合、SIP TLS で設定した暗号は、ALL TLSs 暗号を上書きします。

- [SSH 暗号（SSH Ciphers）]：このフィールドに割り当てられる暗号は、Unified Communications Manager および IM and Presence Service の SSH 接続に適用されます。
- [SSH キー交換（SSH Key Exchange）]：このフィールドで割り当てられるキー交換アルゴリズムは、Unified Communications Manager および IM and Presence Service の SSH インターフェイスに適用されます。

カーブのネゴシエーション

次に、曲線のネゴシエーションの点を示します。

- ECDSA の暗号は、ECDSA 証明書のキーサイズに基づいて、さまざまな EC カーブとネゴシエートされます。
- RSA の暗号化は、証明書のキーサイズに関係なく、すべての EC カーブとネゴシエートされます。
- ECDSA 証明書のキーサイズは、TLS ネゴシエーションを発生させるための曲線サイズと同じである必要があります。

例：

クライアントが P-384 EC のカーブを提供する場合、384 キー証明書と ECDSA の暗号がネゴシエートされます。

曲線のネゴシエーションは、RSA 暗号と ECDSA 暗号の両方のクライアント設定に基づいています。

証明書のサイズが 384 ビットであり、クライアントのオファーリングが P-521 の場合、P-384 P-256 EC のネゴシエーションが発生すると、P-521 の曲線で TLS ネゴシエーションが発生します。クライアントによって提供されるカーブは最初の P-521 であり、P-384 曲線もリストから利用できます。証明書サイズが 384 ビットであり、クライアントオファーリングが P-521、P-256 の場合、P-384 曲線がクライアントによって提供されないため、TLS ネゴシエーションは行われません。

EC カーブでサポートされている暗号を次に示します。

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
```

```
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

推奨される暗号

デフォルトでは、Unified Communications Manager および IM and Presence Service は、サードパーティ製品を含む他のほとんどの製品との安全な統合をサポートする一連の暗号（下記の TLS および SSH 暗号のセクションを参照）をすでに使用しています。したがって、通常は変更を加える必要はありません。暗号スイートの不一致によって TLS ハンドシェイクが失敗する場合は、Unified Communications Manager 暗号管理を使用して、サポートされている暗号のリストに暗号を追加できます。

暗号管理は、顧客がより制限を加えて、TLS ハンドシェイク中に特定の暗号スイートがネゴシエートされないようにしたい場合にも使用できます。暗号を設定した後で変更を有効にするには、影響を受けるサービスを再起動するか、サーバーをリブートします。

警告 SSH MAC インターフェイスで sha2-512 を設定すると、DRS と CDR の機能が影響を受けます。

暗号 aes128-gcm@openssh.com の設定、"ssh Cipher の" フィールド内の aes256-gcm@openssh.com、または ssh kex "の sha2-nistp256 アルゴリズムのみを設定すると、DRS と CDR の機能が失われます。

シスコでは、TLS および SSH インターフェイスの構成用に次の暗号ストリングをサポートしています。

TLS

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:
ECDHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA
```

SSH 暗号

```
aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,
aes256-gcm@openssh.com
```

SSH MAC

```
hmac-sha2-512,hmac-sha2-256,hmac-sha1
```

SSH KEX

```
ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256,
diffie-hellman-group14-sha1, diffie-hellman-group16-sha512, diffie-hellman-group14-sha256
```

暗号ストリングの設定

- [すべての TLS（All TLS）]、[SIP TLS]、および [HTTPS TLS] フィールドに必ず暗号ストリングを OpenSSL 暗号ストリング形式で入力してください。
- また、**[SSH 暗号（SSH Ciphers）]**、**[SSH MAC]**のアルゴリズム、および**[SSH キー交換（SSH Key Exchange）]** フィールドには、OpenSSH 形式で暗号またはアルゴリズムも入力してください。
- 推奨される暗号 （3 ページ）を確認してください。

異なるセキュアなインターフェイスで暗号ストリングを設定するには、「暗号の制限事項」セクションを参照してください。

手順

Step 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、**[セキュリティ（Security）]** > **[暗号の管理（Cipher Management）]** を選択します。
[暗号の管理（Cipher Management）] ページが表示されます。

Step 2 **ALL TLS**、**SIP TLS**、**HTTP TLS**フィールドで暗号ストリングを設定するには、暗号ストリングを OpenSSL 暗号ストリング フォーマットで **[暗号ストリング（Cipher String）]** フィールドに入力します。

Step 3 次のフィールドに暗号ストリングを設定しない場合に発生する状況を以下に示します。

- **[すべての TLS（All TLS）] または [HTTPS TLS]** フィールド：HTTPS TLS インターフェイス ポート（8443）は、**[エンタープライズパラメータ（Enterprise parameters）]**（HTTPS 暗号）ページから設定を実行します。
- [すべての TLS（All TLS）] または [SIP TLS] フィールド：SIP インターフェイスポート（5061）は、暗号化モードの [エンタープライズパラメータ]（TLS 暗号）ページと認証モードの NULL-SHA 暗号から設定を取得します。

（注） **[HTTPS TLS]** または **[SIP TLS]** フィールドに暗号ストリングを設定しない場合、システムはデフォルトで**[ALL TLS（すべての TLS）]** フィールドから設定を取得します。

OpenSSL 暗号ストリングの形式の詳細については、https://www.openssl.org/docs/man1.0.2/apps/ciphers.htmlを参照してください。

Step 4 **SSH 暗号化**、フィールドで暗号ストリングを設定するには、暗号ストリングを OpenSSL 暗号ストリング フォーマットで **[暗号ストリング（Cipher String）]** フィールドに入力します。

SSH 暗号の OpenSSH 暗号ストリング形式の詳細については、https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.htmlを参照してください。

[SSH 暗号（SSH Ciphers）] フィールドに暗号ストリングを設定しなかった場合、デフォルトでは、次の暗号がすべての SSH 接続に適用されます。

FIPS モードで、次の様になります。

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

非 FIPS モードで、次のようになります。

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

Step 5 **[SSHキー交換（SSH Key Exchange）]** のキー交換アルゴリズムを設定するには、**[アルゴリズム文字列（Algorithm String）]** フィールドにアルゴリズム文字列を OpenSSH 文字列形式で入力します。

SSH キー交換用の OpenSSH アルゴリズム文字列形式の詳細については、https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.htmlを参照してください。

[SSH キー交換（SSH Key Exchange）]フィールドでキー交換アルゴリズムを設定しなかった場合、デフォルトでは、次のキー交換アルゴリズムがすべての SSH 接続に適用されます。

FIPS モードで、次の様になります。

```
diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

非 FIPS モードで、次のようになります。

```
diffie-hellman-group1-sha1, diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

Step 6 **[SSH MAC]** フィールドで MAC アルゴリズムを設定するには、**[アルゴリズム文字列（Algorithm String）]** フィールドにアルゴリズム文字列を OpenSSH 文字列形式で入力します。

SSH MAC の OpenSSH アルゴリズム文字列形式の詳細については、https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.htmlを参照してください。

[SSH MAC] フィールドで MAC アルゴリズムを設定しなかった場合、次の MAC アルゴリズムがデフォルトですべての SSH 接続に適用されます。

FIPS モードで、次の様になります。

```
hmac-sha1
```

非 FIPS モードで、次のようになります。

```
hmac-sha1
```

Step 7 **[保存（Save）]** をクリックします。

（注） **[暗号拡張文字列（Cipher Expansion String）]** および **[アルゴリズム拡張文字列（Algorithm Expansion String）]** フィールドを編集することはできません。

システムは、**All TLS**、**STP TLS**、**HTTPS TLS**、および**SSH 暗号化** における暗号化を検証し、**[実際の暗号方式（Actual Ciphers）]** フィールドに自動的に暗号方式を入力します。

[暗号ストリング（Cipher String）] フィールドに無効な暗号が入力されると、[暗号化拡張文字列（Cipher Expansion String）] フィールドに自動的な入力は行われず、以下のエラーメッセージが表示されます。

無効な暗号ストリングが入力されました

システムは、**[SSHキー交換（SSH Key Exchange）]** および **[SSH MAC]** フィールドのアルゴリズムを検証し、**[アルゴリズム拡張文字列（Algorithm Expansion String）]** フィールドに自動的にアルゴリズム文字列を入力します。

[アルゴリズム文字列（Algorithm String）] フィールドに無効なアルゴリズムが入力されると、**[アルゴリズム拡張文字列（Algorithm Expansion String）]** フィールドに自動的な入力は行われず、以下のエラーメッセージが表示されます。

無効なアルゴリズム文字列が入力されました

（注） [実際の暗号方式（Actual Ciphers）] または [実際のアルゴリズム（Actual Algorithms）] フィールドに自動的に入力される暗号またはアルゴリズムは、有効な暗号またはアルゴリズムです。システムは、**[暗号拡張文字列（Cipher Expansion String）]** または **[アルゴリズム拡張文字列（Algorithm Expansion String）]** フィールドから暗号またはアルゴリズムを選択します。

対応するフィールドに暗号を設定した場合は、それぞれのサービスをリブートまたは再起動する必要があります。

表 *1:* 設定された暗号と対応するアクション

設定された暗号フィールド	操作
All TLS	暗号ストリングを有効にするために、クラスタ内のすべてのノードをリブートします。
HTTPS TLS	暗号ストリングを有効にするため、すべてのノードで Cisco Tomcat サービスを再起動します。
SIP TLS	暗号ストリングを有効にするために、すべてのノードで Unified Communications Manager を再起動します。
SSH 暗号	暗号ストリングを有効にするために、クラスタ内のすべてのノードをリブートします。
SSH キー交換 または SSH MAC	アルゴリズム文字列を有効にするために、クラスタ内のすべてのノードをリブートします。

（注） 暗号は、**[暗号の管理（Cipher Management）]** ページの **[暗号ストリング（Cipher String）]** フィールドに入力して有効にできます。これらの暗号を入力しない場合は、アプリケーションでサポートされているデフォルトの暗号すべてが有効になります。ただし、**[暗号の管理（Cipher Management）]** ページの **[暗号ストリング（Cipher String）]** フィールドに暗号ストリングを入力しない場合は、特定の弱い暗号を無効にすることもできます。

暗号の制限

[Cipher **Management** configuration] ページでは任意の数の暗号を設定できますが、各アプリケーションには、そのインターフェイスでサポートされている暗号のリストがあります。たとえば、**すべてのTLS**インターフェイスで ECDHE、DHE またはECDSA ベースの暗号が表示される場合がありますが、Unified Communications Manager などのアプリケーションでは、EC カーブまたは DHE アルゴリズムはこのアプリケーションのインターフェイスに対して有効ではないため、このような暗号をサポートしていない場合があります。個々のアプリケーションインターフェイスでサポートされている暗号のリストの詳細については、「アプリケーションの暗号のサポート （8 ページ）」セクションを参照してください。

（注） [暗号管理（Cipher Management）] ページで暗号が構成されているクラスタをアップグレードする場合は、[すべて（ALL）] フィールドと [HTTPS] フィールドの間に少なくとも 1 つの共通暗号を構成するようにしてください。

GUI での検証

[暗号管理（Cipher Management）] ページの暗号は、OpenSSL のガイドラインに従って検証されます。たとえば、次のように設定されている暗号があるとします。失敗しました。!MD5、暗号文字列は"不良"は暗号化されていないことを認識していても、有効であると見なされます。OpenSSL は、これを有効な文字列と見なします。AES128-SHA ではなく、AES128_SHA が設定されている場合（ハイフンの代わりに下線を使用）、OpenSSL はこれを無効な暗号スイートとして識別します。

認証モード (NULL 暗号)

アプリケーションインターフェイスがNULLの暗号を使用している場合は、**暗号管理**ページの**ALL TLS**または**SIP TLS** フィールドに暗号リストを設定することによって、NULL 暗号のサポートを無効にすることができます。

NULL 暗号を使用するアプリケーションインターフェイスの例は次のとおりです。

- **すべての TLS インターフェイス：**[TLS コンテキストの設定（TLS Context Configuration）] ページ経由のIM and Presence の Unified Communications Manager SIP プロキシ。

- **SIP TLS インターフェイス**：>SIP または SCCP で、いずれかの [デバイス セキュリティ プロファイル（Device Security Profile）] が [認証済み（Authenticated）] モードに設定されている場合に、SIP または SCCP が経由します。

NULL 暗号を使用する必要がある場合は、これら 2 つのインターフェイスのいずれについても暗号を設定しないでください。

オーバーライド機能

[暗号管理（Cipher Management）] ページの設定により、各アプリケーションと、暗号が設定されているその他の場所のデフォルト設定が上書きされます。つまり、[**Cipher Management**] ページで暗号が設定されていない場合は、すべてのインターフェイスの元の機能が保持されます。

[エンタープライズパラメータ（Enterprise Parameter）]「**[TLS の暗号（TLS Ciphers）]**」 が、「*[*サポートされているすべての暗号（*ALL Supported Ciphers*）*]*」 を使用して設定されていて、**[暗号管理（Cipher Management）]** ページが、**[すべての TLS（All TLS）]** インターフェイスの「*AES256-GCM-SHA384:AES256-SHA256*」暗号によって設定されている場合、すべてのアプリケーション SIP インターフェイスは 「*AAES256-GCM-SHA384:AES256-SHA256*」 暗号のみをサポートし、**[エンタプライズパラメータ（Enterprise Parameter）]** の値は無視されます。

アプリケーションの暗号のサポート

次の表は、アプリケーションインターフェイスと、TLS および SSH インターフェイスでサポートされているすべての対応する暗号、およびアルゴリズムを示しています。

表 *2: TLS* 暗号のためのユニファイドコミュニケーションマネージャーの暗号サポート

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco CallManager	TCP/TLS	2443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA128-SHA CAMELLIA256-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
DRS	TCP/TLS	4040	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: DHE-RSA-CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA
Cisco Tomcat	TCP/TLS	8443 / 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco CallManager	TCP/TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 ECDHE-ECDSA-AES256-SHA: CAMELLIA256-SHA: CAMELLIA128-SHA: ECDHE-ECDSA-DES-CBC3-SHA
Cisco CTL Provider （注） Cisco CTL Provider は、リリース 14SU3 以降では使用できません。	TCP/TLS	2444	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:
Cisco Certificate Authority Proxy Function	TCP/TLS	3804	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
CTIManager	TCP/TLS	2749	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA
シスコ信頼検証サービス	TCP/TLS	2445	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA
Cisco Intercluster Lookup Service	TCP/TLS	7501	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
安全な設定ダウンロード (HAPROXY)	TCP/TLS	6971、6972	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-DES-CBC3-SHA: CAMELLIA128-SHA:
認証済み UDS 連絡先の検索	TCP/TLS	9443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-DES-CBC3-SHA:

表 *3 : Unified Communications Manager IM & Presence* 暗号サポートが *TLS* の暗号でサポートされています

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA:
Cisco SIP Proxy	TCP/TLS	5062	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	8083	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco Tomcat	TCP/TLS	8443、443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: EDH-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA128-SHA: CAMELLIA256-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: DHE-RSA-CAMELLIA128-SHA: DHE-RSA-CAMELLIA256-SHA: ECDHE-ECDSA-AES256-SHA:

アプリケーション/プロセス	プロトコル	ポート	サポート対象の暗号方式
Cisco XCP XMPP Federation Connection Manager	TCP/TLS	5269	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-RSA-AES256-SHA:
Cisco XCP Client Connection Manager	TCP/TLS	5222	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: （注） リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA128-SHA: CAMELLIA256-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-RSA-AES256-SHA:

表 *4 : SSH* 暗号の暗号サポート

サービス	暗号/アルゴリズム
SSH サーバ	• 暗号 aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC アルゴリズム： hmac-sha2-256 hmac-sha2-512 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 • 非 FIPS モードのホストキーアルゴリズム： rsa-sha2-256 rsa-sha2-512 ssh-rsa • FIPS モードのホストキーアルゴリズム： rsa-sha2-256 rsa-sha2-512

サービス	暗号/アルゴリズム
SSH クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC アルゴリズム： hmac-sha2-256 hmac-sha2-512 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 • 非 FIPS モードのホストキーアルゴリズム： rsa-sha2-256 rsa-sha2-512 ssh-rsa • FIPS モードのホストキーアルゴリズム： rsa-sha2-256 rsa-sha2-512

サービス	暗号/アルゴリズム
DRS クライアント	• 暗号： aes256-ctr aes256-cbc aes128-ctr aes128-cbc aes192-ctr aes192-cbc • MAC アルゴリズム： hmac-md5 hmac-sha2-256 hmac-sha1 hmac-sha1-96 hmac-md5-96 • KEX アルゴリズム： ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group1-sha1 （注） Unified CM サーバーで暗号管理機能を設定している場合、Kex アルゴリズム diffie-hellman-group-exchange-sha256、diffie-hellman-group-exchange-sha1、および diffie-hellman-group1-sha1 は、リリース 12.5(1)SU4 からサポートされません。暗号が設定されていない場合、DRS クライアントはこれらのアルゴリズムを使用します。
SFTP クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1

サービス	暗号/アルゴリズム
エンドユーザ	hmac-sha512 SHA-512 - Hashing (salted)
DRS バックアップ/ RTMT SFTP	AES-128 - Encryption
アプリケーションユーザ	AES-256 - Encryption

暗号の制限

[暗号管理（Cipher Management）] ページでは、OpenSSL または OpenSSH がサポートする暗号を設定できます。ただし、暗号の一部は、偶発的なデータが偶発的に公開されることを回避するために、Cisco のセキュリティ標準に基づいて内部的に無効になっています。

[**Cipher Management**] ページで暗号を設定すると、次の暗号が基本的に無効になります。

TLS を無効にした暗号

```
EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:ADH-DES-CBC-SHA:
DES-CBC-SHA:KRB5-DES-CBC-SHA:KRB5-DES-CBC-MD5:EXP-EDH-RSA-DES-CBC-SHA:
EXP-EDH-DSS-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:
EXP-KRB5-RC2-CBC-SHA:EXP-KRB5-DES-CBC-SHA:EXP-KRB5-RC2-CBC-MD5:EXP-KRB5-DES-CBC-MD5:
EXP-ADH-RC4-MD5:EXP-RC4-MD5:EXP-KRB5-RC4-SHA:EXP-KRB5-RC4-MD5:ADH-AES256-GCM-SHA384:
ADH-AES256-SHA256:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:ADH-AES128-GCM-SHA256:ADH-AES128-SHA256:
ADH-AES128-SHA:ADH-SEED-SHA:ADH-CAMELLIA128-SHA:ADH-DES-CBC3-SHA:ADH-RC4-MD5:
AECDH-AES256-SHA:AECDH-AES128-SHA:AECDH-DES-CBC3-SHA:AECDH-RC4-SHA:AECDH-NULL-SHA:
DES-CBC3-MD5:IDEA-CBC-MD5:RC2-CBC-MD5:RC4-MD5:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:
ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:KRB5-RC4-SHA:
KRB5-RC4-MD5:IDEA-CBC-SHA:KRB5-IDEA-CBC-SHA:KRB5-IDEA-CBC-MD5:DHE-RSA-SEED-SHA:
DHE-DSS-SEED-SHA:SEED-SHA:KRB5-DES-CBC3-MD5:NULL-MD5:PSK-AES256-CBC-SHA:
PSK-AES128-CBC-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-NULL-SHA:ECDHE-ECDSA-NULL-SHA:
ECDH-RSA-NULL-SHA:ECDH-ECDSA-NULL-SHA:NULL-SHA256:NULL-SHA
```

SSH 無効暗号

```
3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

SSH が無効になっている KEX アルゴリズム

```
curve25519-sha256@libssh.org,gss-gex-sha1-,gss-group1-sha1-,gss-group14-sha1-
```

SSH が無効になっている MAC アルゴリズム

```
hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```

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。