Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の設定

この章では、Cisco VG224 アナログ電話ゲートウェイ用の Foreign Exchange Station（FXS）ポートに接続され、Cisco Unified Communications Manager Express（Cisco Unified CME）によって制御されるアナログ電話の、セキュア シグナリングおよびメディアの暗号化について説明します。

このモジュール内の機能情報の検索

ご使用の Cisco IOS ソフトウェア リリースが、この章で説明している機能の一部をサポートしていない場合があります。このモジュール内に記載されている特定の機能のリンクにアクセスする場合、および各機能がサポートされているリリースのリストを参照する場合は、「Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の機能情報」（P.221）を参照してください。

プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索するには

プラットフォームのサポートと、Cisco IOS および Catalyst OS ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

- 「Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の制約事項」（P.202）
- 「Cisco VG224 のセキュア シグナリングおよびメディアの暗号化について」（P.202）
- 「Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の設定方法」（P.203）
- 「Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の設定例」（P.214）
- 「参考資料」（P.219）
- 「Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の機能情報」（P.221）

Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の前提条件

Cisco IOS ゲートウェイ

- Cisco IOS Release 12.4(11)XW 以降のリリース。
- 次のいずれかの方法を使用して、システム クロックを設定します。詳細については、ご使用の Cisco IOS リリースの『*Cisco IOS Network Management Configuration Guide*』にある「Performing Basic System Management」の章を参照してください。
  - Network Time Protocol（NTP; ネットワーク タイム プロトコル）を設定する。
  - **clock set** コマンドを使用して、ソフトウェア クロックを手動で設定する。Cisco サービス統合型ルータで、**clock set** コマンドと **clock update-calendar** コマンドを使用します。

Cisco Unified CME のアナログ エンドポイント

- Cisco Unified CME 4.2 以降のバージョン。

Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の制約事項

- この機能は、Cisco Unified Communications Manager のアナログ SCCP エンドポイントではサポートされません。

Cisco VG224 のセキュア シグナリングおよびメディアの暗号化について

Cisco VG224 のセキュア シグナリングおよびメディアの暗号化をイネーブルにするには、次の概念について理解しておく必要があります。

- 「メディアの暗号化（SRTP）」（P.202）

メディアの暗号化（SRTP）

Cisco Unified CME 4.2 以降のバージョンのメディアの暗号化（SRTP）およびコンパニオン音声セキュリティ Cisco IOS 機能では、Cisco VG224 アナログ電話ゲートウェイ エンドポイントに接続されたセキュア アナログ エンドポイントを含めて、セキュア音声コール機能を提供します。

Cisco Unified CME のメディア暗号化（SRTP）機能では、次の機能をサポートします。

- SCCP エンドポイント用の SRTP を使用するセキュア音声コール
- 混合共有回線環境のセキュア音声コールにより、RTP と SRTP の両方でエンドポイントを使用できます。共有回線のメディア セキュリティは、エンドポイント設定に応じて異なります。
- H.450 を使用するセキュア補足サービスは次のとおりです。
  - 自動転送
  - コール転送

- コール保留と保留解除
- コール パークとコール ピックアップ
- 非セキュア ソフトウェア会議

（注） H.323 を介した SRTP 電話会議では、コールが会議に参加するときに、0 ～ 2 秒間隔のノイズが発生する可能性があります。

- H.450 以外の環境でのセキュア コール
- セキュア Cisco Unified CME のセキュア Cisco Unity との相互動作
- セキュア Cisco Unified CME の Cisco Unity Express との相互動作（相互動作がサポートされ、コールが非セキュア モードにダウングレードされる）
- DSP ファーム変換が設定されたリモート電話のセキュア変換

Cisco Unified CME のこれらの機能の詳細については、『*Cisco Unified CME System Administration Guide*』の「Configuring Security」モジュールを参照してください。

Cisco VG224 アナログ電話ゲートウェイ用の SRTP を設定するには、「Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の設定方法」（P.203）を参照してください。

Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の設定方法

Cisco Unified CME のメディア暗号化（SRTP）は、セキュア Cisco VG224 アナログ電話ゲートウェイ エンドポイントなどのセキュア音声コール機能を提供します。

（注） Cisco Unified CME のこの機能の詳細については、『*Cisco Unified CME System Administration Guide*』の「Configuring Security」モジュールを参照してください。

Cisco VG224 アナログ電話ゲートウェイをセキュア Cisco Unified CME システムに追加するには、次の作業を実行します。

- 「外部 CA サーバの設定」（P.203）（必須）
- 「VG224 でのトラストポイントの作成」（P.206）（必須）
- 「STCAPP、トラストポイント、およびセキュリティの設定」（P.209）（必須）
- 「Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の検証とトラブルシューティング」（P.211）（任意）

外部 CA サーバの設定

外部 Certificate Authority（CA; 認証局）サーバを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**

3. **crypto pki server** *cs-label*
4. **database level {minimal | names | complete}**
5. **grant auto**
6. **database url** *root-url*
7. **no shutdown**
8. **exit**
9. **crypto pki trustpoint** *label*
10. **revocation-check** *method1* [*method2*[*method3*]]
11. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
12. **exit**
13. **ip http server**
14. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki server** *cs-label* **例：** `Router(config)# crypto pki server cserver1`	証明書サーバのラベルを定義し、証明書サーバ コンフィギュレーション モードを開始します。 • *cs-label*：CA 証明書サーバ名。
ステップ 4	**database level** {**minimal** | **names** | **complete**} **例：** `Router(cs-server)# database level complete`	（任意）証明書登録データベースに保管されるデータのタイプを制御します。 • **minimal**：新しい証明書を、継続して問題なく発行できる程度の情報が保管されます。これがデフォルトの機能です。 • **names**：各証明書のシリアル番号と題名はデータベースに保存され、管理者が必要に応じて特定の証明書を検索したり、無効にしたりするための十分な情報を提供します。 • **complete**：minimal レベルおよび names レベルで提供される情報以外に、発行済みの各証明書がデータベースに書き込まれます。 （注） **complete** キーワードでは大量の情報が生成されるため、**database url** コマンドを使用してデータを保存する外部 TFTP サーバを指定してください。

	コマンドまたはアクション	目的
ステップ 5	**grant auto** **例：** `Router(cs-server)# grant auto`	（任意）あらゆる要求者に対して証明書が自動的に発行されるようにします。このコマンドが使用されない場合に推奨される方法およびデフォルトは、手動登録です。 **ヒント** このコマンドは、簡易ネットワークのテストおよび構築中に登録する場合のみ使用してください。セキュリティのベスト プラクティスは、証明書が継続的に供与されないように、設定後に **no grant auto** コマンドを使用してこの機能をディセーブルにすることです。
ステップ 6	**database url** *root-url* **例：** `Router(cs-server)# database url nvram:`	（任意）証明書サーバのすべてのデータベース エントリが書き出される場所を指定します。このコマンドが指定されていない場合、すべてのデータベース エントリは NVRAM に書き込まれます。 • *root-url*：データベース エントリが書き出される場所。URL は Cisco IOS ファイル システムでサポートされる任意の URL です。 • CA が大量の証明書を発行使用としている場合、証明書を保存するためのフラッシュやその他のストレージ デバイスなどの適切な保存場所を選択します。 **（注）** 洗濯された保存場所がフラッシュで、このデバイスのファイル システムの形式が Class B（LEFS）の場合、定期的にこのデバイスの空き領域をチェックし、**squeeze** コマンドを使用して、削除されたファイルによって使用されている領域を解放します。このプロセスには数分かかる場合があり、スケジュールされたメンテナンス期間または低負荷時に実行する必要があります。
ステップ 7	**no shutdown** **例：** `Router(cs-server)# no shutdown`	（任意）CA をイネーブルにします。 • このコマンドは、CA を完全に設定した後にのみ使用する必要があります。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 8	**exit** **例：** `Router(cs-server)# exit`	証明書サーバ コンフィギュレーション モードを終了します。
ステップ 9	**crypto pki trustpoint** *label* **例：** `Router(config)# crypto pki trustpoint cserver1`	（任意）トラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • この CA が Cisco Unified CME ルータのローカルにある場合は、このコマンドと **enrollment url** コマンドを使用します。これらのコマンドは、外部ルータで動作している CA には不要です。 • *label*：トラストポイント名。この手順の *label* は、ステップ 3 の *cs-label* と同じにする必要があります。

	コマンドまたはアクション	目的
ステップ 10	**revocation-check** *method1* [*method2*[*method3*]] **例：** `Router(ca-trustpoint)# revocation-check crl`	（任意）証明書の失効ステータスをチェックし、ステータスをチェックするための 1 つまたは複数の方法を指定します。2 番目と 3 番目の方法を指定した場合、各方法はその直前の方法でエラーが返された場合（サーバがダウンしている場合など）にだけ使用されます。 次に、*method* 引数に有効な値を示します。 • **crl**：証明書のチェックは、証明書失効リスト（CRL）によって実行されます。これがデフォルトの動作です。 • **none**：証明書のチェックは不要です。 • **ocsp**：証明書のチェックは、Online Certificate Status Protocol（OCSP）サーバによって実行されます。
ステップ 11	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **例：** `Router(ca-trustpoint)# rsakeypair exampleCAkeys 1024 1024`	（任意）証明書で使用する RSA キー ペアを指定します。 • *key-label*：キー ペアが存在していない場合、または **auto-enroll regenerate** コマンドが使用される場合に、登録中に生成されるキー ペアの名前。 • *key-size*：（任意）目的の RSA キーのサイズ。指定されなかった場合は、既存のキーが使用されます。 • *encryption-key-size*：（任意）個別の暗号化、署名キー、および証明書を要求するために使用される 2 番目のキーのサイズ。 **（注）** 複数のトラストポイントで同じキーを共有できます。
ステップ 12	**exit** **例：** `Router(ca-trustpoint)# exit`	CA-trustpoint コンフィギュレーション モードを終了します。
ステップ 13	**ip http server** **例：** `Router(config)# ip http server`	ローカル Cisco Unified CME ルータで Cisco We ブラウザのユーザ インターフェイスをイネーブルにします。
ステップ 14	**exit** **例：** `Router (config)# exit`	グローバル コンフィギュレーション モードを終了します。

VG224 でのトラストポイントの作成

Cisco VG224 でトラストポイントを作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa general-keys label** *key-label*

4. **crypto pki trustpoint** *label*
5. **enrollment url** *ca-url*
6. **serial-number none**
7. **fqdn none**
8. **ip-address none**
9. **subject-name** [*x.500-name*]
10. **revocation-check none**
11. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
12. **exit**
13. **crypto pki authenticate** *trustpoint-label*
14. **crypto pki enroll** *trustpoint-label*
15. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto key generate rsa general-keys label** *key-label* **例：** `Router(config)# crypto key generate rsa general-keys label VG224`	（任意）Rivest, Shamir, and Adelman（RSA）キー ペアを生成します。 • **general-keys**：汎用キー ペアを生成する必要があることを指定します。 • **label** *key-label*：（任意）RSA キー ペアがエクスポートされるときに使用される名前。
ステップ 4	**crypto pki trustpoint** *label* **例：** `Router(config)# crypto pki trustpoint VG224`	RA モード証明書サーバが使用するトラストポイントを宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 • *label*：トラストポイントと RA の名前。
ステップ 5	**enrollment url** *ca-url* **例：** `Router(ca-trustpoint)# enrollment url http://10.3.105.40:80`	発行元 CA 証明書サーバ（ルート証明書サーバ）の登録 URL を指定します。 • *ca-url*：ルート CA がインストールされたルータの URL。
ステップ 6	**serial-number none** **例：** `Router(ca-trustpoint)# serial-number none`	証明書要求にルータのシリアル番号を含める必要があるかどうかを指定します。 • **none**：証明書要求にシリアル番号が含まれないことを指定します。

	コマンドまたはアクション	目的
ステップ 7	**fqdn none** **例：** `Router(ca-trustpoint)# fqdn none`	証明書要求に「unstructuredName」として含まれる完全修飾ドメイン名（FQDN）を指定します。 • **none**：証明書要求にルータの FQDN が含まれません。
ステップ 8	**ip-address none** **例：** `Router(ca-trustpoint)# ip-address none`	証明書要求に「unstructuredAddress」として含まれるドット付きの IP アドレスまたはインターフェイスを指定します。 • **none**：証明書要求に IP アドレスが含まれないことを指定します。
ステップ 9	**subject-name** [*x.500-name*] **例：** `Router(ca-trustpoint)# subject-name cn=VG224, ou=ABU, o=Cisco Systems Inc.`	証明書要求の件名を指定します。 **（注）** この例は、証明書の件名の形式を IP 電話の場合と同様に設定する方法を示しています。
ステップ 10	**revocation-check none** **例：** `Router(ca-trustpoint)# revocation-check none`	（任意）証明書の失効ステータスをチェックし、ステータスをチェックするための 1 つまたは複数の方法を指定します。2 番目と 3 番目の方法を指定した場合、各方法はその直前の方法でエラーが返された場合（サーバがダウンしている場合など）にだけ使用されます。 • **none**：証明書のチェックは不要です。
ステップ 11	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **例：** `Router(ca-trustpoint)# rsakeypair VG224`	（任意）証明書で使用する RSA キー ペアを指定します。 • *key-label*：キー ペアが存在していない場合、または **auto-enroll regenerate** コマンドが使用される場合に、登録中に生成されるキー ペアの名前。 • *key-size*：（任意）目的の RSA キーのサイズ。指定されなかった場合は、既存のキーが使用されます。 • *encryption-key-size*：（任意）個別の暗号化、署名キー、および証明書を要求するために使用される 2 番目のキーのサイズ。 **（注）** 複数のトラストポイントで同じキーを共有できます。
ステップ 12	**exit** **例：** `Router(ca-trustpoint)# exit`	CA-trustpoint コンフィギュレーション モードを終了します。
ステップ 13	**crypto pki authenticate** *trustpoint-label* **例：** `Router(config)# crypto pki authenticate VG224`	CA 証明書を取得して、認証します。証明書フィンガープリントをチェックするよう求められた場合、証明書フィンガープリントをチェックします。 • *trustpoint-label*：トラストポイントのラベル。 **（注）** CA 証明書がコンフィギュレーションにすでにロードされている場合、このコマンドはオプションです。

	コマンドまたはアクション	目的
ステップ 14	**crypto pki enroll** trustpoint-label **例：** `Router(config)# crypto pki enroll VG224`	CA に登録し、このトラストポイントの証明書を取得します。 • *trustpoint-label*：トラストポイントのラベル。
ステップ 15	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

STCAPP、トラストポイント、およびセキュリティの設定

STCAPP、トラストポイント、およびセキュリティ モードを設定するには、Cisco VG224 で次の手順を実行します。

前提条件

- Cisco 音声ゲートウェイで SCCP がイネーブルになっていること。設定される STC アプリケーション グループが作成されていること。詳しい設定手順については、「音声ゲートウェイでの SCCP のイネーブル化」（P.33）を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **stcapp ccm-group** *group-id*
4. **stcapp security trustpoint** *line*
5. **stcapp security mode** [**authenticated** | **encrypted** | **none**]
6. **stcapp**
7. **dial-peer voice** *tag* **pots**
8. **security mode** [**authenticated** | **encrypted** | **none**]
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**stcapp ccm-group** *group-id* **例：** `Router(config)# stcapp ccm-group 1`	STC アプリケーション グループを設定します。 • 設定されるグループは、**sccp ccm group** コマンドを使用してすでに作成されています。「音声ゲートウェイでの SCCP のイネーブル化」（P.33）を参照してください。
ステップ 4	**stcapp security trustpoint** *line* **例：** `Router(config)# stcapp security trustpoint VG224`	STCAPP エンドポイントの TLS 接続のセットアップに使用されるトラストポイントを指定します。 • STCAPP サービスを開始するには、このコマンドを設定する必要があります。
ステップ 5	**stcapp security mode [authenticated | encrypted | none]** **例：** `Router(config)# stcapp security mode encrypted`	STCAPP エンドポイントのセキュリティをイネーブルにします。 • STCAPP エンドポイントに対してセキュリティをイネーブルにするには、このコマンドと前の手順の **stcapp security trustpoint** コマンドを設定する必要があります。
ステップ 6	**stcapp** **例：** `Router(config)# stcapp`	グローバル レベルで STCAPP をイネーブルにします。
ステップ 7	**dial-peer voice** *tag* **pots** **例：** `Router(config)# dial-peer voice 1 pots`	（任意）ダイヤルピア音声コンフィギュレーション モードを開始します。
ステップ 8	**security mode** [**authenticated** | **encrypted** | **none**] **例：** `Router(config-dialpeer)# security mode encrypted`	（任意）ダイヤルピア レベルの STCAPP エンドポイント セキュリティをイネーブルにして、グローバル コンフィギュレーションを上書きします。 • **authenticated**：シグナリング認証を使用して、STCAPP エンドポイントをイネーブルにします。 • **encrypted**：データの暗号化を使用して、STCAPP エンドポイントをイネーブルにします。 • **none**：ダイヤルピア レベルの STCAPP エンドポイント セキュリティ コンフィギュレーションをディセーブルにして、グローバル レベルのコンフィギュレーションをデフォルトにします。
ステップ 9	**end** **例：** `Router(config-dialpeer)# end`	ダイヤルピア コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の検証とトラブルシューティング

Cisco VG224 のセキュア シグナリングおよびメディアの暗号化を検証およびトラブルシューティングするには、次の手順を実行します。

手順の概要

1. **show sccp**
2. **show dial-peer voice**
3. **debug sccp tls**
4. **debug sccp message**
5. **debug voip application stcapp all**
6. **show stcapp device voice-port** *port*
7. **show call active voice brief**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show sccp** **例：** `Router> show sccp`	管理ステータスや動作ステータスなどの SCCP 情報を表示します。
ステップ 2	**show dial-peer voice** **例：** `Router> show dial-peer voice`	セキュリティ モードなどのダイヤル ピア情報を表示します。
ステップ 3	**debug sccp tls** **例：** `Router# configure terminal`	SCCP のデバッグ情報や関連アプリケーション（変換や会議）を表示します。
ステップ 4	**debug sccp message** **例：** `Router# debug sccp message`	SCCP のデバッグ情報や関連アプリケーション（変換や会議）を表示します。
ステップ 5	**debug voip application stcapp all** **例：** `Router# debug voip application stcapp all`	STCAPP のコンポーネントのデバッグ情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**show stcapp device voice-port** *port* **例：** `Router# show stcapp device voice-port 1/0/0`	指定された STCAPP アナログ音声ポートの設定情報を表示します。
ステップ 7	**show call active voice brief** **例：** `Router# show call active voice brief`	通話中の音声コールの短縮されたバージョンのコール情報を表示します。

例

次に、STCAPP およびセキュリティ モード設定の検証およびトラブルシューティングに使用されるコマンドの出力例を示します。

show dial-peer voice：例

```
Show dial-peer voice 5001

VoiceEncapPeer5001
peer type = voice, system default peer = FALSE, information type = voice,
description = `',
tag = 5001, destination-pattern = `',
voice reg type = 0, corresponding tag = 0,
…….
      …….
digit_strip = enabled,
register E.164 number with H323 GK and/or SIP Registrar = TRUE
fax rate = system,   payload size =  20 bytes
supported-language = ''
preemption level = `routine'
bandwidth:
    maximum = 64 KBits/sec, minimum = 64 KBits/sec
voice class called-number:
    inbound = `', outbound = `'
dial tone generation after remote onhook = enabled
```

次の行に、イネーブルになっている暗号化が示されます。

```
 Signaling and Media Security = Encrypted

Time elapsed since last clearing of voice call statistics never
Connect Time = 0, Charged Units = 0,
Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
Accepted Calls = 0, Refused Calls = 0,
Last Disconnect Cause is "",
Last Disconnect Text is "",
Last Setup Time = 0.
Last Disconnect Time = 0.
```

show sccp：例

```
show sccp
SCCP Admin State: UP
Gateway IP Address: 10.4.177.53, Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
```

```
Call Manager: 10.4.177.51, Port Number: 2000
       Priority: N/A, Version: 4.0, Identifier: 1

Alg_Phone Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.4.177.51, Port Number: 2443
TCP Link Status: CONNECTED, Device Name: AN0C8639A24D400
```

以下の行に、セキュア メディアおよびシグナリング ステータスが示されます。

```
Security
 Signaling Security: ENCRYPTED TLS
Media Security: SRTP
Supported crypto suites :AES_CM_128_HMAC_SHA1_32
Reported Max Streams: 1, Reported Max OOS Streams: 0
Supported Codec: RFC 2833 dtmf, Maximum Packetization Period: 30
Supported Codec: g711ulaw, Maximum Packetization Period: 20
Supported Codec: g711alaw, Maximum Packetization Period: 20
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: g729ar8, Maximum Packetization Period: 220
Supported Codec: g729br8, Maximum Packetization Period: 220
Supported Codec: g729r8, Maximum Packetization Period: 220

Alg_Phone Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.4.177.51, Port Number: 2000
TCP Link Status: CONNECTED, Device Name: AN0C8639A24D401
```

以下の行に、セキュア メディアおよびシグナリング ステータスが示されます。

```
Security
 Signaling Security: AUTHENTICATED TLS
Reported Max Streams: 1, Reported Max OOS Streams: 0
Supported Codec: RFC 2833 dtmf, Maximum Packetization Period: 30
Supported Codec: g711ulaw, Maximum Packetization Period: 20
Supported Codec: g711alaw, Maximum Packetization Period: 20
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: g729ar8, Maximum Packetization Period: 220
Supported Codec: g729br8, Maximum Packetization Period: 220
Supported Codec: g729r8, Maximum Packetization Period: 220

Alg_Phone Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.4.177.51, Port Number: 2000
TCP Link Status: CONNECTED, Device Name: AN0C8639A24D402
Reported Max Streams: 1, Reported Max OOS Streams: 0
Supported Codec: RFC 2833 dtmf, Maximum Packetization Period: 30
Supported Codec: g711ulaw, Maximum Packetization Period: 20
Supported Codec: g711alaw, Maximum Packetization Period: 20
Supported Codec: g729r8, Maximum Packetization Period: 220
Supported Codec: g729ar8, Maximum Packetization Period: 220
Supported Codec: g729br8, Maximum Packetization Period: 220
Supported Codec: g729r8, Maximum Packetization Period: 220
```

show stcapp device voice-port：例

```
Show stcapp device voice-port 2/0
Port Identifier:  2/0
Device Type:      ALG
Device Id:        2
Device Name:      AN0C8639A24D400
```

次の行に、デバイスのセキュリティ ステータスが示されます。

```
Device Security Mode : Encrypted
Modem Capability: None
Device State:     IS
```

```
Diagnostic:       None
Directory Number: 5001
Dial Peer(s):     5001
Dialtone after remote onhook feature: activated
Last Event:       STCAPP_CC_EV_CALL_DISCONNECT_DONE
Line State:       IDLE
Hook State:       ONHOOK
mwi:              DISABLE
vmwi:             OFF
PLAR:             DISABLE
Number of CCBs:   0
Global call info:
    Total CCB count      = 0
    Total call leg count = 0
```

Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の設定例

次に、システム レベルでイネーブルになっている STCAPP セキュリティおよびダイヤル ピアで設定されたセキュリティ モードの例を示します。

```
Router# show running-config
Building configuration...
Current configuration : 8906 bytes
!
! Last configuration change at 15:41:09 PDT Mon Oct 23 2006
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname akash
!
boot-start-marker
boot-end-marker
!
logging buffered 400000 debugging
no logging console
enable password lab
!
no aaa new-model
!
resource policy
!
clock timezone PST -8
clock summer-time PDT recurring
no ip domain lookup
!
!
!
```

以下の行に、システム レベルでイネーブルになっている STCAPP セキュリティが示されます。

```
stcapp ccm-group 1
stcapp security trustpoint analog
stcapp security mode encrypted
stcapp
!
voice-card 0
dsp services dspfarm
!
crypto pki trustpoint analog
enrollment url http://10.4.177.51:80
serial-number
revocation-check none
certificate ca 01
30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 0D303630 35303132
33303130 335A170D 30393034 33303233 30313033 5A301431 12301006 03550403
1309756E 69746974 65737430 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 C2D07857 B8DF7F55 3C2365B3 2E1524CF EE898D1F D7A04075
D36F0229 392803DF B45246B4 A447506F A3FCDD00 9FC93CD7 5B5573E0 7BFD25E1
AB2F24E2 740D5765 7F628B6E 0FD39BEE 940D80FF 3B9F9F17 7ACA8F82 1A9E3179
458781E8 87C95E1B 17E6A61C 7D138AC1 D8E30F3C 88BFAFEE A94D5F8C E433DF71
F076E96C 9BB5327F 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 168014B5
418287D0 61FE277C 9A1862B3 673BF7F7 0E47DD30 1D060355 1D0E0416 0414B541
8287D061 FE277C9A 1862B367 3BF7F70E 47DD300D 06092A86 4886F70D 01010405
00038181 002BB76E 22A59D73 6DBB62BA BAC3D5B4 2F739A26 D5FFF911 EDEB9BDC
7B29FECC E0B68E0F 22A3C0D0 8BA64592 30C6B628 5EFA3905 1B13BFE7 7CEB1456
55214435 07F752A6 73D5646A 4BB7B3C2 61E2C185 3A638FCA AE5AC6A1 3DB3590B
C3C6C924 D1E1E365 FE041B07 F3E2AF24 3701B664 A7879229 AFDF163A 00AA12AA
85866101 53
quit
crypto pki certificate chain analog
certificate 0A
308201BF 30820128 A0030201 0202010A 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 0D303630 35333032
31313630 345A170D 30373035 33303231 31363034 5A302A31 28301206 03550405
130B4648 4B303930 37463050 47301206 092A8648 86F70D01 09021605 616B6173
68305C30 0D06092A 864886F7 0D010101 0500034B 00304802 4100A6AD 0A376A6C
9EB668CC D0DF2A17 180E6CA2 FA5F243B 861EAA29 BE5FC488 A22AD4E8 5DFC22AC
13B43337 2F9FBA64 14E838EA 888E79DE 93AB63E4 4B4E2ECD 256D0203 010001A3
4F304D30 0B060355 1D0F0404 030205A0 301F0603 551D2304 18301680 14B54182
87D061FE 277C9A18 62B3673B F7F70E47 DD301D06 03551D0E 04160414 34D2D41C
274AB6E3 71A3A32C EC19D533 D3C0A020 300D0609 2A864886 F70D0101 04050003
818100A2 3947B1D0 FC5E9B79 0C1A28E7 BCB34C6C BB68C5F6 356F3F61 7525053E
0AED7325 9F286888 887810A6 B62FBAF3 BDC81542 C9828BBF 6A9FE936 AD3ED33B
D4F5AD22 E703C8E0 C3DDEAC8 2097A209 542551F7 6340A2A4 55A25A99 6A87367F
A0CBD9B6 E38D5E40 6479EB71 EFA644B3 93222D6F 235039AE BB9AA7B7 B1D07B3C FC6339
quit
certificate ca 01
30820201 3082016A A0030201 02020101 300D0609 2A864886 F70D0101 04050030
14311230 10060355 04031309 756E6974 69746573 74301E17 0D303630 35303132
33303130 335A170D 30393034 33303233 30313033 5A301431 12301006 03550403
1309756E 69746974 65737430 819F300D 06092A86 4886F70D 01010105 0003818D
00308189 02818100 C2D07857 B8DF7F55 3C2365B3 2E1524CF EE898D1F D7A04075
D36F0229 392803DF B45246B4 A447506F A3FCDD00 9FC93CD7 5B5573E0 7BFD25E1
AB2F24E2 740D5765 7F628B6E 0FD39BEE 940D80FF 3B9F9F17 7ACA8F82 1A9E3179
458781E8 87C95E1B 17E6A61C 7D138AC1 D8E30F3C 88BFAFEE A94D5F8C E433DF71
F076E96C 9BB5327F 02030100 01A36330 61300F06 03551D13 0101FF04 05300301
01FF300E 0603551D 0F0101FF 04040302 0186301F 0603551D 23041830 168014B5
418287D0 61FE277C 9A1862B3 673BF7F7 0E47DD30 1D060355 1D0E0416 0414B541
8287D061 FE277C9A 1862B367 3BF7F70E 47DD300D 06092A86 4886F70D 01010405
00038181 002BB76E 22A59D73 6DBB62BA BAC3D5B4 2F739A26 D5FFF911 EDEB9BDC
```

```
7B29FECC E0B68E0F 22A3C0D0 8BA64592 30C6B628 5EFA3905 1B13BFE7 7CEB1456
55214435 07F752A6 73D5646A 4BB7B3C2 61E2C185 3A638FCA AE5AC6A1 3DB3590B
C3C6C924 D1E1E365 FE041B07 F3E2AF24 3701B664 A7879229 AFDF163A 00AA12AA
85866101 53
quit
!
!
voice service voip
!
!
interface FastEthernet0/0
ip address 10.4.177.53 255.255.0.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
ip route 0.0.0.0 0.0.0.0 1.4.0.1
!
ip http server
no ip http secure-server
!
no cdp advertise-v2
!
!
control-plane
!
!
voice-port 2/0
!
voice-port 2/1
!
voice-port 2/2
!
voice-port 2/3
!
voice-port 2/4
!
.
.
.
!
voice-port 2/23
!
!
!
sccp local FastEthernet0/0
sccp ccm 10.4.177.51 identifier 1 version 4.0
sccp
!
sccp ccm group 1
associate ccm 1 priority 1
!
dial-peer voice 5001 pots
service stcapp
port 2/0
!
dial-peer voice 5002 pots
service stcapp
```

次の行に、ダイヤル ピアで設定されたセキュリティ モードが示されます。

```
security mode authenticated
port 2/1
!
dial-peer voice 5003 pots
service stcapp
security mode none
port 2/2
!
dial-peer voice 2000 voip
destination-pattern 7...
session target ipv4:10.4.177.100
incoming called-number 7000
codec g711ulaw
!
dial-peer voice 1 pots
!
dial-peer voice 5004 pots
service stcapp
shutdown
port 2/3
!
dial-peer voice 5005 pots
shutdown
destination-pattern 3001
port 2/4
!
.
.
.
!
dial-peer voice 5018 pots
service stcapp
shutdown
port 2/17
!
dial-peer voice 2001 pots
destination-pattern 2001
port 2/18
!
dial-peer voice 1000 voip
destination-pattern 1...
session target ipv4:10.3.105.5
!
dial-peer voice 5900 voip
destination-pattern 59..
session target ipv4:10.3.105.5
!
dial-peer voice 500 voip
destination-pattern 5...
session target ipv4:10.4.177.51
!
dial-peer voice 5019 pots
service stcapp
shutdown
port 2/18
!
dial-peer voice 5020 pots
service stcapp
shutdown
port 2/19
!
.
```

```
.
.
!
dial-peer voice 5024 pots
service stcapp
shutdown
port 2/23
!
!
!
!
line con 0
transport output all
line aux 0
transport output all
line vty 0 4
password lab
login
transport input all
transport output all
!
ntp clock-period 17179541
ntp server 10.4.177.51
end
```

参考資料

ここでは、Cisco 音声ゲートウェイの FXS ポート用の SCCP アナログ電話機サポートに関連する資料を示します。

関連資料

関連項目	参照先
Cisco Unified Communications Manager	*Cisco Unified Communications Manager のマニュアル*
Cisco Unified Communications Manager Express	*Cisco Unified Communications Manager Express のマニュアル*
Cisco IOS のデバッグ	『*Cisco IOS Debug Command Reference*』
Cisco IOS の音声コマンド	『*Cisco IOS Voice Command Reference*』
Cisco IOS の音声設定	『*Cisco IOS Voice Configuration Library*』
Cisco 音声ゲートウェイ	• *Cisco VG200 シリーズのマニュアル* • *Cisco 1800 シリーズ サービス統合型ルータのマニュアル* • *Cisco 2800 サービス統合型ルータのマニュアル* • *Cisco 3800 シリーズ サービス統合型ルータのマニュアル* • *Cisco Unified 500 シリーズのマニュアル*
会議およびコード変換リソース	• 『*Cisco Unified CallManager and Cisco IOS Interoperability Guide*』の「Configuring Enhanced Conferencing and Transcoding for Voice Gateway Routers」の章 • 『*Cisco CallManager and IOS Gateway DSP Farm Configuration Example*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の機能情報

表 27 に、このモジュールで説明した機能をリストし、特定の設定情報へのリンクを示します。この表には、Cisco IOS Release 12.4(20)YA 以降のリリースで導入または変更された機能だけを示します。

このテクノロジーの機能でここに記載されていない情報については、「補足サービスの機能ロードマップ」（P.13）を参照してください。

ご使用の Cisco IOS ソフトウェア リリースでは、一部のコマンドが使用できない場合があります。特定のコマンドのリリース情報については、コマンド リファレンス マニュアルを参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS と Catalyst OS のソフトウェア イメージを判別できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

（注） 表 27 に、特定の Cisco IOS ソフトウェア リリース群で特定の機能をサポートする Cisco IOS ソフトウェア リリースだけを示します。特に明記されていない限り、Cisco IOS ソフトウェア リリース群の後続のリリースでもこの機能をサポートします。

表 27　機能情報

機能名	リリース	機能情報
Cisco VG224 のセキュア シグナリングおよびメディアの暗号化	12.4(11)XW	Cisco Unified CME によって制御される Cisco VG224 アナログ電話ゲートウェイ用の FXS ポートに接続されたアナログ電話のセキュア音声コール機能を提供します。 次の項で、この機能に関する情報を参照できます。 • 「メディアの暗号化（SRTP）」（P.202） • 「Cisco VG224 のセキュア シグナリングおよびメディアの暗号化の設定方法」（P.203）