CHAPTER 2

インストールと Cisco IME サーバの設定

この章では、Cisco Intercompany Media Engine サーバのインストールと設定について説明します。インストール手順を開始する前に、インストールについての指示すべてをよく確認してください。この章の構成は、次のとおりです。

重要な考慮事項

インストールを進める前に、次の要求事項と推奨事項について考慮してください。

- Cisco Unified Communications Manager サーバで、Cisco Unified Communications Manager ソフトウェアの互換性のあるバージョンが実行されていることを確認します。次の URL で、『*Cisco Unified Communications Manager Software Compatibility Matrix*』を参照してください。

  http://www.cisco.com/en/US/partner/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

- Cisco Unified Communications Manager サーバで NTP が有効になっていることを確認します。NTP ステータスを確認するには、Cisco Unified Communications Manager コマンド ライン インターフェイスにログインし、**utils ntp status** と入力します。

- 既存のサーバにインストールする場合、ハード ドライブはフォーマットされ、ドライブ上に存在するデータすべてが上書きされることに注意します。

- バックアップ電源によってシステムを保護できるよう、サーバが Uninterruptible Power Supply（UPS; 無停電電源装置）に接続されていることを確認します。このようにしなかった場合、物理メディアに損傷が生じて Cisco Intercompany Media Engine（Cisco IME）の新規インストールが必要となる可能性があります。

  Cisco IME ノードで UPS シグナリングを自動的に監視し、電源喪失時にグレースフル シャットダウンを自動で開始させるには、特定の UPS とサーバ モデルの使用が必要です。サポートされているモデルと設定についての詳細は、『*Release Notes for Cisco Intercompany Media Engine*』を参照してください。

- スタティック IP アドレスを使用してサーバを設定し、サーバが固定された IP アドレスを得られるようにします。
- インストール中、このサーバで DNS を有効にし、NTP を設定する必要があります。
- インストール中は、設定作業を実行しないでください。
- インストールが完了するまで、シスコで検証済みのアプリケーションはインストールしないでください。
- サーバ モデル 7825 I3（160 GB SATA ディスク ドライブ）のディスク ミラーリングには、約 3 時間かかります。
- インストールを進める前に、次の情報を注意深く読んでください。

インストールに関する FAQ

次の項では、一般的な質問と回答について取り上げます。インストールを始める前に、この項を注意深く読んでください。この項は、次の内容で構成されています。

インストールにはどれくらいの時間がかかりますか。

サーバ タイプによりますが、インストール前後の作業を除いたインストール プロセス全体で 20 ～ 30 分必要です。

どのようなユーザ名とパスワードを指定する必要がありますか。

（注）　システムはパスワードの強度をチェックします。強度の高いパスワード作成のガイドラインについては、「強度の高いパスワードとはどのようなパスワードですか。」（P.2-3）を参照してください。

インストール中、次のユーザ名とパスワードを指定する必要があります。

- 管理者アカウントのユーザ名とパスワード
- セキュリティ パスワード

管理者アカウントのユーザ名とパスワード

次の領域へのログインには、管理者アカウントのユーザ名とパスワードを使用します。

- ディザスタ リカバリ システム
- コマンド ライン インターフェイス

管理者アカウントのユーザ名とパスワードを指定するには、次のガイドラインに従います。

- 管理者アカウント ユーザ名：管理者アカウントのユーザ名には、英数字、ハイフン、アンダースコアを使用できますが、先頭は英字にします。
- 管理者アカウント パスワード：管理者アカウントのパスワードは、最低 6 文字とし、英数字、ハイフン、アンダースコアを使用できます。

コマンド ライン インターフェイスを使用して、管理者アカウント パスワードの変更や新規管理者アカウントの追加が行えます。詳しくは、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。

セキュリティ パスワード

セキュリティ パスワードは最低 6 文字とします。英数字、ハイフン、アンダースコアを使用できます。

強度の高いパスワードとはどのようなパスワードですか。

インストール ウィザードは、入力されたパスワードの強度をチェックします。強度の高いパスワードを作成するには、次の推奨事項に従います。

- 大文字と小文字を混在させる。
- 英字と数字を混在させる。
- ハイフンやアンダースコアを含める。
- 長いパスワードは短いパスワードより強度が高く、セキュアになることに留意してください。

次のタイプのパスワードの使用は避けます。

- 固有名詞や辞書にある単語など、認識可能な単語は使用しない（数字と組み合わせた場合も含む）。
- 認識可能な単語を反転させたものは使用しない。
- aaabbb、qwerty、zyxwvuts、123321 のようにパターン化された単語や数字は使用しない。
- 他の言語で認識可能な単語は使用しない。
- いかなるものにしろ、誕生日、郵便番号、子供やペットの名前のような個人情報は使用しない。

Cisco Unified Communications アンサー ファイル ジェネレータとは何ですか。

Cisco Unified Communications アンサー ファイル ジェネレータは、Cisco Intercompany Media Engine の無人インストールのアンサー ファイルを生成するウェブ アプリケーションです。個別のアンサー ファイルは USB キーまたはフロッピーディスクのルート ディレクトリにコピーされ、インストール プロセスで Cisco Intercompany Media Engine DVD に加えて使用されます。

このウェブ アプリケーションには、次のような機能があります。

- データ エントリの構文検証
- オンライン ヘルプと資料
- 新規インストールのサポート（アップグレードはサポートしません）

Cisco Unified Communications アンサー ファイル ジェネレータは、次の URL でアクセスできます。

http://www.cisco.com/web/cuc_afg/index.html

Cisco Unified Communications アンサー ファイル ジェネレータは、Internet Explorer バージョン 6.0 以降および Mozilla バージョン 1.5 以降をサポートしています。

USB キーは、Linux 2.4 互換である必要があります。Cisco では、コンフィギュレーション ファイル用として、Linux 2.4 互換で事前にフォーマットされた USB キーを使用することを推奨します。これらのキーは W95 FAT32 フォーマットを使用します。

このインストールで、Cisco はどのようなサーバをサポートしていますか。

サポートされているサーバ モデルについては、ご使用の製品リリースのリリース ノートを参照してください。

Cisco はどのような SFTP サーバをサポートしていますか。

どのような SFTP サーバ製品でも使用できますが、Cisco では Cisco Technology Developer Partner（CTDP）プログラムで Cisco が認定した SFTP 製品を推奨します。GlobalSCAPE などの CTDP パートナーは、自社製品での特定のバージョンの Cisco Unified Communications Manager の使用を保証しています。ご使用のバージョンの Cisco Unified Communications Manager の自社製品での動作を保証しているベンダーについては、次の URL を参照してください。

http://www.cisco.com/pcgi-bin/ctdp/Search.pl

サポートされている Cisco Unified Communications バージョンの GlobalSCAPE での使用については、次の URL を参照してください。

http://www.globalscape.com/gsftps/cisco.aspx

シスコでは、次のサーバを内部テストに使用しています。これらのサーバのいずれかを使用できますが、サポートについてはベンダーにお問い合わせください。

- Open SSH（http://sshwindows.sourceforge.net/ を参照）
- Cygwin（http://www.cygwin.com/ を参照）
- Titan（http://www.titanftp.com/ を参照）

（注）　CTDP プロセスによる認証を受けていないサードパーティ製品との問題のサポートについては、サードパーティ ベンダーにお問い合わせください。

サーバに他のソフトウェアをインストールできますか。

ソフトウェアのインストールとアップグレードは、すべて Command Line Interface（CLI; コマンド ライン インターフェイス）で行う必要があります。システムがアップロードして処理できるのは、Cisco Systems 承認済みソフトウェアだけです。

未承認のサードパーティ ソフトウェア アプリケーションのインストールや実行はできません。

インストール前の作業

表 2-1 に、Cisco Intercompany Media Engine を確実にインストールするために必要なインストール前の作業のリストを示します。

表 2-1　インストール前の作業

	タスク	特記事項
ステップ 1	このマニュアル全体をよく読み、インストール手順についてよく理解してください。	
ステップ 2	Cisco は、Cisco IME のサイト分析と計画のセッションを完了しておくことを推奨します。これには、オフパス Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）の設定、IP アドレッシング、ピン ホール、スタティック Network Address Translation（NAT; ネットワーク アドレス変換）、Demilitarized Zone（DMZ; 非武装地帯）設定が含まれます。現在のネットワーク設定に適用される Cisco IME 要求事項について理解しておく必要があります。	*Cisco Unified Communications Manager:SRND*
ステップ 3	企業のファイアウォールで、必要なトラフィックを有効にします。 Cisco Intercompany Media Engine の設計と導入の早い段階で、企業のファイアウォールや DMZ の管理チーム（IT チームや情報セキュリティ チームなど）に参加しておく必要があります。Cisco IME コールの開始前に、企業のファイアウォールに必要な Access Control List（ACL; アクセス コントロール リスト）がすべて承認され、実装されているようにします。	「ネットワーク トラフィックの許可」（P.2-6）
ステップ 4	製造元が提供するユーティリティを実行して、すべての新規サーバ ハードウェアの整合性を検証します（ハードドライブやメモリなど）。	
ステップ 5	新規サーバを接続するスイッチ ポートの Network Interface Card（NIC; ネットワーク インターフェイス カード）の速度とデュプレックス設定を記録します。 サーバとスイッチ ポートの NIC 設定を同じにする必要があります。GigE（1000/FULL）の場合、NIC とスイッチ ポート設定は Auto/Auto にする必要があり、固定値は設定しません。	Cisco サーバに接続するスイッチポートすべてで PortFast を有効にします。PortFast を有効にすると、転送遅延をなくすことによりスイッチはポートをブロック状態から転送状態へすぐに変更します（転送遅延は、Spanning Tree Protocol（STP; スパニング ツリー プロトコル）ラーニングおよびリスニング ステートから転送ステートに変わるまでポートが待つ時間の長さを指します）。
ステップ 6	Cisco IME をインストール予定のサーバすべてが正しく DNS に登録されていることを確認します。	GoDaddy.com サーバと intercompanymedianetwork.com ブートストラップ サーバの解決と ping が実行できる必要があります。
ステップ 7	Cisco IME ライセンス ファイルを取得します。	「ライセンス ファイルの取得」（P.2-8）を参照してください。
ステップ 8	インストール予定の各サーバの設定値を記録します。	設定値の記録については、表 2-4 を参照してください。

追加情報

「関連項目」（P.2-29）

ネットワーク トラフィックの許可

この項では、IME トラフィックをサポートするために設定する必要がある、必要最低限のポートについて説明します。表 2-2 に、企業のファイアウォールに設定する必要があるポートの概要を示します。表 2-3 にオフパス ASA に設定する必要があるポートの概要を示します。これらの表中のポート設定は、デフォルト設定に基づいています。デフォルト設定を変更した場合、これらの設定を更新する必要があります。

ご使用のネットワークに他のサーバ/ポートが必要な場合、そのトラフィックの許可も必要です。

表 2-2　企業のファイアウォール設定

インターフェイス	方向	ソース	宛先	プロトコル	ポート	説明
内側	インバウンド	Cisco Unified CM IP アドレス	オフパス ASA 内部シグナリング アドレス（物理アドレスと同じ）	TCP	8060	Cisco Unified CM と ASA シグナリング アドレスとのオフパス マッピング。クラスタ内の各 Cisco Unified CM にエントリが必要。
内側	インバウンド	Cisco Unified CM IP アドレス	オフパス ASA 内部シグナリング アドレス（物理アドレスと同じ）	TCP	1024 ～ 65535	Cisco Unified CM と ASA シグナリング アドレスとのオフパス マッピング。クラスタ内の各 Cisco Unified CM にエントリが必要。
DMZ	インバウンド	オフパス ASA 内部シグナリング アドレス（物理アドレスと同じ）	Cisco Unified CM IP アドレス	TCP	5060	ASA シグナリング アドレスと Cisco Unified CM との間の SIP シグナリング。クラスタ内の各 Cisco Unified CM にエントリが必要。ポート番号設定可能。
内側	インバウンド	Cisco Unified CM IP アドレス	Cisco IME サーバ DMZ IP アドレス	TCP	5620	Cisco IME と Cisco Unified Communications Manager との間の VAP 通信
内側	インバウンド	ユニファイド コミュニケーション デバイスすべて（MeetingPlace、ボイスメール、ソフトクライアント IP 範囲、音声ゲートウェイ、ASA 経由の通信が必要なすべてのメディア デバイスを含む）	オフパス ASA 内部メディアの終端 IP	UDP	16384 ～ 32767	UDP ポートは、Cisco IME が有効な ASA メディアの終端アドレス設定および同時コール数に基づいて制限可能です。

表 2-2　企業のファイアウォール設定 （続き）

インターフェイス	方向	ソース	宛先	プロトコル	ポート	説明
DMZ	インバウンド	オフパス ASA 内部メディアの終端 IP （送信元ポート範囲は Cisco IME 設定に基づいて制限可能です）	ユニファイドコミュニケーション デバイスすべて（MeetingPlace、ボイスメール、ソフトクライアント IP 範囲、音声ゲートウェイ、ASA 経由の通信が必要なすべてのメディア デバイスを含む）	UDP	16384 ～ 32767	メディア トラフィックの UDP ポート。
内側	インバウンド	内部ネットワークまたはいずれかの管理ワークステーション	Cisco IME サーバ DMZ IP アドレス	TCP	22	ライセンス/ソフトウェアのアップロード、アップグレード、CLI アクセスのための Cisco IME サーバへの SFTP アクセス。
内側	インバウンド	内部ネットワークまたはいずれかの管理ワークステーション	Cisco IME サーバ DMZ IP アドレス	HTTPS	443	Cisco IME サーバからの RTMT ダウンロード。
DMZ	インバウンド	Cisco IME サーバ DMZ IP アドレス	GoDaddy Web サイト	HTTPS	443	GoDaddy からの証明書ダウンロード。
DMZ	インバウンド	Cisco IME サーバ DMZ IP アドレス	任意	TLS	6084	Cisco IME サーバからインターネットへのアウトバウンド IME 分散キャッシュ通信。
外側	インバウンド	任意	Cisco IME サーバ DMZ IP アドレス	TLS	6084	インターネットから Cisco IME サーバへのインバウンド IME 分散キャッシュ通信。
DMZ	インバウンド	Cisco IME サーバ DMZ IP アドレス	任意	TLS	8470	Cisco IME サーバからインターネットへのアウトバウンド IME 分散キャッシュ通信。
外側	インバウンド	任意	Cisco IME サーバ DMZ IP アドレス	TLS	8470	インターネットから Cisco IME サーバへのインバウンド IME 分散キャッシュ通信。

表 2-3　外部 Cisco IME ASA ファイアウォール（オフパス ASA）

インターフェイス	方向	ソースの説明	宛先の説明	プロトコル	ポート	説明
DMZ	インバウンド	Cisco Unified CM IP アドレス	リモート Cisco Unified CM	TCP	5560 ～ 5590	リモート Cisco Unified CM への内部 Cisco Unified CM シグナリング（リモート PAT 設定）。
DMZ	インバウンド	Cisco Unified CM IP アドレス	リモート Cisco Unified CM	TCP	5060	リモート Cisco Unified CM への内部 Cisco Unified CM シグナリング（リモート PAT 設定）。
外側	インバウンド	任意	Cisco Unified CM IP アドレス	TCP	5060	内部 Cisco Unified CM へのリモート Cisco Unified CM シグナリング。

追加情報

「インストール前の作業」（P.2-5）

ライセンス ファイルの取得

製品付属の Product Authorization Key（PAK; 製品認可キー）を使用して、Cisco IME サーバに必要なライセンスを取得できます。ライセンス ファイルには、Cisco IME のサポートされているバージョン、Cisco IME サーバの MAC アドレス、ライセンスされれた Cisco IME アプリケーション数（ピアカウント）、GoDaddy からの証明書取得に必要な情報（タグと署名）が含まれます。証明書によって、Cisco IME サーバが IME 分散キャッシュ リング上にある他の Cisco IME サーバへの TLS 接続を確立できるようになります。

例 2-1 に、Cisco IME ライセンス ファイルの例を示します。

例 2-1　ライセンス ファイルの例

```
INCREMENT IME_SERVICE cisco 8.0 permanent uncounted ¥
    VENDOR_STRING=<ime><peercount>5</peercount><tag>163d18ab727c0fa14fce75c6651b1362</tag>
    <signature>154fe09fdbb012407cbfac8c74c55cb6be460199c813b0af29b83bc3b10824519bef7427f7a
    be7a7b9e6692e9b905e73fa9a1199c90ef7fd269c89f0a9179677bbee34cb1eeb915f03e2372cb1e9d272d
    af907be0077c7fd128ecc0216f036bb9447f06857cdcb4b066e746dc80ebe33fc212117b5c6c95aa404751
    6120e403c320f703a9a94ac7c177a07963dd83aa79b75c1c585250481bce340ef3bf02f86633f245cbfaef
    c2a1851b29c6cf48f580655c8a983b65d5584e316f350a15ff90478cbcb8e39128049edbb6972b33203130
    00f28db28cc51a8eb7666a40184cb5389e216cdfeac7c1d42b0e4fdf2c608bea28faeff807fcc0862497dd
    59ca676</signature></ime><LicFileVersion>1.0</LicFileVersion> ¥
    HOSTID=00163569b2e0 ¥
    NOTICE="<LicFileID>20090730162506350</LicFileID><LicLineID>1</LicLineID> ¥
    <PAK></PAK>" SIGN="0288 1F4A 07D6 0C34 F35B D4D5 0339 C538 ¥
    AC1E BC65 8697 9D5F 18D3 A57D 27DD 18D2 8C3B 14BA E72F 4932 ¥
    E27D 7BE9 C410 5477 9B85 AAF7 2F42 8C44 0985 CFF1"
```

Cisco IME サーバのライセンス ファイルを取得するには、次の手順に従います。

手順

ステップ 1　Cisco Intercompany Media Engine に付属の Product Authorization Key（PAK; 製品認可キー）を、http://www.cisco.com/go/license にある License Registration Web ツールに入力します。

ステップ 2　[Submit] をクリックします。

ステップ 3　システム プロンプトの指示に従います。Cisco Intercompany Media Engine をインストール予定のサーバの Network Interface Card（NIC; ネットワーク インターフェイス カード）の MAC アドレスと、有効な電子メール アドレスを入力する必要があります。MAC アドレスを知るには、Cisco IME Command Line Interface（CLI; コマンド ライン インターフェイス）にログインし、**show status** と入力します。[License MAC] フィールドに MAC アドレスが表示されます。

システムは、入力された電子メール アドレス宛てに電子メールでライセンス ファイルを送信します。

ライセンス ファイルの形式は、IME<timestamp>.lic です。.lic 拡張子を保持していれば、ライセンス ファイルの名前を変更することもできます。ファイルの内容に何らかの編集を加えると、ライセンスは使用できなくなります。

ステップ 4　ライセンス ファイルは、ステップ 3 で入力した MAC アドレスに一致するサーバにアップロードする必要があります。「ライセンス ファイルのアップロード」（P.2-23）を参照してください。

追加情報

「インストール前の作業」（P.2-5）

インストールのための情報収集

表 2-4 を使用して、サーバについての情報を記録します。すべての情報を取得する必要はありません。ご使用のシステムとネットワーク設定に関連する情報だけを収集します。

（注）　一部のフィールドはオプションであり、ご使用の設定には適用されない場合があります。

注意　一部のフィールドは、いったんインストールすると、ソフトウェアを再インストールしない限り変更できません。入力する値はよく確認してください。

表の最後の列に、インストール後にフィールドを変更できるかが示されています。変更できる場合、そのための適切な Command Line Interface（CLI; コマンド ライン インターフェイス）コマンドも示されています。

表 2-4　サーバ設定データ

パラメータ	説明	インストール後の変更の可否
[管理者 ID(Administrator ID)] 入力内容：	このフィールドは、Cisco Intercompany Media Engine サーバ上の CLI へのセキュア シェル アクセスに使用する管理者アカウントのユーザ ID を指定します。	インストール後はエントリを変更できません。 **（注）**　インストール後に追加の管理者アカウントを作成することはできますが、元の管理者アカウントのユーザ ID は変更できません。

表 2-4　サーバ設定データ （続き）

パラメータ	説明	インストール後の変更の可否
[管理者パスワード (Administrator Password)] 入力内容：	このフィールドは、CLI へのセキュア シェル アクセスに使用する管理者アカウントのパスワードを指定します。 このパスワードは、adminsftp ユーザでも使用します。adminsftp ユーザは、ローカル バックアップ ファイルへのアクセスやサーバライセンスのアップロードなどに使用します。 パスワードは最低 6 文字とし、英数字、ハイフン、アンダースコアを使用するようにします。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set password admin**
[国 (Country)] 入力内容：	リストから、インストールに応じて適切な国を選択します。 **（注）** 入力した値は、Certificate Signing Request（CSR; 証明書署名要求）の生成に使用されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**
[DHCP] 入力内容：	Cisco は、[DHCP] オプションに [いいえ (No)] を選択するよう要求します。[いいえ (No)] を選択した後、ホスト名、IP アドレス、IP マスク、ゲートウェイを入力します。	インストール後にエントリを変更しないでください。
[DNS 有効 (DNS Enable)] 入力内容：	DNS サーバは、ホスト名を IP アドレスに、IP アドレスをホスト名に解決します。 Cisco IME では DNS サーバの使用が必須です。[はい (Yes)] を選択して、DNS を有効にします。	インストール後にエントリを変更しないでください。
[DNS プライマリ (DNS Primary)] 入力内容：	プライマリ DNS サーバとして指定する DNS サーバの IP アドレスを入力します。IP アドレスは、ドット付き 10 進表記形式（ddd.ddd.ddd.ddd）で入力します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network dns** DNS とネットワークの情報を参照するには、次の CLI コマンドを使用します。 CLI > **network eth0 detail**
[DNS セカンダリ (DNS Secondary)]（オプション） 入力内容：	セカンダリ DNS サーバ（オプション）として指定する DNS サーバの IP アドレスを入力します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network dns**
[ゲートウェイアドレス (Gateway Address)] 入力内容：	ネットワーク ゲートウェイの IP アドレスを入力します。 ゲートウェイがない場合でも、このフィールドには 255.255.255.255 を設定する必要があります。ゲートウェイがない場合、通信はご使用のサブネット上のデバイスだけに制限されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network gateway**

表 2-4　サーバ設定データ （続き）

パラメータ	説明	インストール後の変更の可否
[ホスト名 (Hostname)] 入力内容：	サーバの一意なホスト名を入力します。 ホスト名は最大 64 文字で、英数字とハイフンを使用できます。ハイフンは先頭に使用できません。	インストール後にエントリを変更できます。 CLI > **set network hostname**
[IP アドレス (IP Address)] 入力内容：	ご使用のサーバの IP アドレスを入力します。	インストール後にエントリを変更できます。 CLI > **set network ip eth0** **（注）** ネットワーク耐障害性が有効になっている場合、IP アドレスの変更前に set network failover dis と入力して無効にする必要があります。IP アドレス変更後、set network failover ena と入力してネットワーク耐障害性を再度有効にします。
[IP マスク (IP Mask)] 入力内容：	このマシンの IP サブネット マスクを入力します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network ip eth0**
[ロケーション (Location)] 入力内容：	サーバの場所を入力します。 システムは、サードパーティの証明書取得に使用する Certificate Signing Requests（CSR; 証明書署名要求）の生成にこの情報を使用します。 組織にとって意味のある任意の場所を入力できます。例ではサーバの所在する都道府県や都市を含めています。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**
[MTU サイズ (MTU Size)] 入力内容：	Maximum Transmission Unit（MTU; 最大伝送ユニット）は、ホストがネットワーク上で送信する最大のパケットをバイト単位で表します。 ご使用のネットワークの MTU サイズをバイト単位で入力します。ネットワークの MTU 設定がよくわからない場合、デフォルト値を使用します。 デフォルトでは 1500 バイトが指定されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network mtu**
[NIC デュプレックス (NIC Duplex)] 入力内容：	Network Interface Card（NIC; ネットワーク インターフェイス カード）のデュプレックス モードを Full と Half から選択します。 **（注）** このパラメータは、自動ネゴシエーションを使用しないよう選択した場合にだけ表示されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network nic**

表 2-4　サーバ設定データ （続き）

パラメータ	説明	インストール後の変更の可否
[NIC スピード (NIC Speed)] 入力内容：	NIC のスピードを、10 メガビット毎秒と 100 メガビット毎秒から選択します。 **（注）** このパラメータは、自動ネゴシエーションを使用しないよう選択した場合にだけ表示されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set network nic**
[NTP サーバ (NTP Server)] 入力内容：	同期に使用する 1 つ以上の Network Time Protocol（NTP; ネットワーク タイム プロトコル）サーバのホスト名または IP アドレスを入力します。 NTP サーバは 5 つまで入力できます。 **（注）** 互換性、精度、およびネットワークジッタに関する潜在的な問題を回避するには、プライマリ ノードに指定した外部 NTP サーバが NTP v4（バージョン 4）である必要があります。IPv6 アドレッシングを使用している場合、外部 NTP サーバは NTP v4 である必要があります。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **utils ntp server**
[組織 (Organization)] 入力内容：	組織の名前を入力します。 **ヒント** このフィールドを使用して、複数の組織ユニットを入力できます。複数の組織ユニット名を入力するには、エントリをカンマで区切ります。カンマを含むエントリの場合、エントリの一部に含まれるカンマの前にバックスラッシュを入力します。 **（注）** 入力した値は、Certificate Signing Request（CSR; 証明書署名要求）の生成に使用されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**
[セキュリティパスワード (Security Password)] 入力内容：	パスワードは、最低 6 文字の英数字である必要があります。パスワードにはハイフンとアンダースコアを使用できますが、先頭に使用できるのは英数字だけです。 **（注）** このパスワードを保存します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set password security**
[都道府県 (State)] 入力内容：	サーバの所在する都道府県を入力します。 **（注）** 入力した値は、Certificate Signing Request（CSR; 証明書署名要求）の生成に使用されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set web-security**

表 2-4　サーバ設定データ （続き）

パラメータ	説明	インストール後の変更の可否
[タイムゾーン (Time Zone)] 入力内容：	このフィールドは、現地タイム ゾーンと Greenwich Mean Time（GMT; グリニッジ標準時）からの差を指定します。 マシンの所在地に適したタイム ゾーンを選択します。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set timezone** 現在のタイム ゾーン設定を参照するには、次の CLI コマンドを入力します。 CLI > **show timezone config**
[ユニット (Unit)] 入力内容：	ユニットを入力します。 **（注）** 入力した値は、Certificate Signing Request（CSR; 証明書署名要求）の生成に使用されます。	次の CLI コマンドを使用してインストール後にエントリを変更できます。 CLI > **set password admin**

追加情報

「インストール前の作業」（P.2-5）

インストールの開始

このセクションでは、オペレーティング システムと Cisco Intercompany Media Engine アプリケーションのインストール方法について説明します。オペレーティング システムとアプリケーションのインストールは、1 つのインストール プログラムを実行して行います。

インストール ウィザード内での移動方法については、表 2-5 を参照してください。

表 2-5　インストール ウィザードのナビゲーション

機能	キー
次のフィールドへ移動	**Tab**
前のフィールドへ移動	**Alt-Tab**
オプションの選択	Space または Enter
リスト内のスクロール	↑または↓
前のウィンドウに戻る	Space または Enter で [戻る (Back)] を選択（使用可能時）
ウィンドウについてのヘルプ表示	Space または Enter で [ヘルプ (Help)] を選択（使用可能時）

インストールを開始するには、次の手順に従います。

手順

ステップ 1　アンサー ファイル ジェネレータが生成した設定情報が入った USB キーがある場合、ここで USB キーを挿入します。

（注）　ソフトウェアがプレインストールされた新規サーバの場合、より新しい製品リリースでサーバの再イメージ化を行うのでない限り、DVD からインストールする必要はありません。直接 ステップ 9 に進めます。

ステップ 2　インストール DVD をトレイに入れてサーバを再起動し、DVD からサーバを起動します。サーバの起動シーケンス完了後、[DVD が見つかりました (DVD Found)] ウィンドウが表示されます。

ステップ 3　メディア チェックを実行する場合、[はい (Yes)] を選択します。メディア チェックをスキップする場合、[いいえ (No)] を選択します。

メディア チェックは DVD の整合性をチェックします。すでにメディア チェックに合格している DVD の場合、メディア チェックのスキップを選択できます。

ステップ 4　[はい (Yes)] を選択してメディア チェックを実行した場合、[メディアチェックの結果 (Media Check Result)] ウィンドウが表示されます。次の作業のいずれかを実行します。

a. [メディアチェックの結果 (Media Check Result)] に [合格 (Pass)] と表示された場合、[OK] を選択してインストールを継続します。

b. メディアがメディア チェックに不合格だった場合、Cisco.com から改めてダウンロードするか、別の DVD を Cisco から直接入手します。

ステップ 5　システム インストーラは次のハードウェア チェックを実行して、システムが正しく設定されていることを確認します。インストーラがハードウェア設定に何らかの変更を加える場合、システムの再起動を求めるプロンプトが表示されます。再起動中、DVD はドライブに入れたままにしておきます。

- 最初に、インストール プロセスは正しいドライバかどうかをチェックします。次の警告が表示される場合があります。

  ```
  No hard drives have been found.You probably need to manually choose device drivers for
  install to succeed.Would you like to select drivers now?
  ```

  インストールを継続するには、[はい (Yes)] を選択します。

- インストールでは次に、サポートされているハードウェア プラットフォームかどうかをチェックします。サーバがハードウェア要件を厳密に満たしていない場合、インストール プロセスに重大なエラーが発生して失敗します。この失敗が正常なものでないと思われる場合、エラーをキャプチャして Cisco サポートに報告します。
- インストール プロセスは次に、RAID 設定と BIOS 設定を確認します。

（注）　このステップが反復される場合、もう一度 [はい (Yes)] を選択します。

- インストール プログラムで BIOS 更新が必要な場合、システムの再起動が必要なことが通知されます。何かキーを押してインストールを継続します。

ハードウェアのチェックが完了すると、[製品配置の選択 (Product Deployment Selection)] ウィンドウが表示されます。

ステップ 6　[製品配置の選択 (Product Deployment Selection)] ウィンドウで、[OK] を選択します。

ステップ 7　ソフトウェアが現在サーバにインストールされている場合、[ハードドライブの上書き (Overwrite Hard Drive)] ウィンドウが表示され、ハード ドライブ上の現在のソフトウェアのバージョンと DVD 上のバージョンとが表示されます。インストールを継続する場合 [はい (Yes)] を、キャンセルする場合 [いいえ (No)] を選択します。

注意　[ハードドライブの上書き (Overwrite Hard Drive)] ウィンドウで [はい (Yes)] を選択した場合、ハード ドライブ上の既存のデータはすべて上書きされて消去されます。

[プラットフォームインストールウィザード (Platform Installation Wizard)] ウィンドウが表示されます。

ステップ 8　次のいずれかのオプションを選択します。

- 設定情報を手動入力し、インストール プログラムが設定されたソフトウェアをサーバへインストールするようにする場合、[続行 (Proceed)] を選択し、ステップ 12 に進みます。
- 次の作業のいずれかを行う場合、[スキップ (Skip)] を選択し、ステップ 9 に進みます。
  - サーバにプリインストールされたソフトウェアを手動で設定する：この場合、ソフトウェアのインストールは必要ありませんが、プリインストールされたソフトウェアの設定が必要です。
  - 無人インストールの実行：この場合、USB キーかフロッピーディスク上の既存の設定情報を準備します。
  - ソフトウェアをインストールしてから手動で設定する：この場合、インストール プログラムがソフトウェアをインストールし、手動設定を求めるプロンプトが表示されます。サーバにまずアプリケーションをプリインストールしておき、設定情報は後で入力する場合、[スキップ (Skip)] を選択します。この方法は、他の方法より時間がかかる場合があります。

ステップ 9　システムの再起動後、[既存のインストール設定 (Preexisting Installation Configuration)] ウィンドウが表示されます。

ステップ 10　アンサー ファイル ジェネレータで作成された既存の設定情報がある場合、情報はフロッピーディスクまたは USB キーに格納されます。ディスクまたは USB キーを挿入して、[続行 (Continue)] を選択します。インストール ウィザードは、インストール プロセスで設定情報を読み取ります。

（注）　システムが新しいハードウェアを検出したことを示すポップアップ ウィンドウが表示された場合、何かキーを押し、次のウィンドウで [インストール (Install)] を選択します。

[プラットフォームインストールウィザード (Platform Installation Wizard)] ウィンドウが表示されます。

ステップ 11　[プラットフォームインストールウィザード (Platform Installation Wizard)] を継続する場合、[続行 (Proceed)] を選択します。

ステップ 12　[基本インストール (Basic Install)] ウィンドウで、[続行 (Continue)] を選択し、DVD 上のソフトウェア バージョンをインストールするか、プリインストールされたソフトウェアを設定します。

ステップ 13　[タイムゾーン設定 (Timezone Configuration)] が表示されたら、サーバに適したタイム ゾーンを選択し、[OK] を選択します。

[自動ネゴシエーション設定 (Auto Negotiation Configuration)] ウィンドウが表示されます。

ステップ 14　インストール プロセスでは、イーサネット Network Interface Card（NIC; ネットワーク インターフェイス カード）の速度とデュプレックスの設定を自動ネゴシエーションによって自動設定するよう設定できます。この設定はインストール後に変更できます。

- 自動ネゴシエーションを有効にするには、[はい (Yes)] を選択し、ステップ 17 に進みます。

  [MTU 設定 (MTU Configuration)] ウィンドウが表示されます。

（注）　このオプションを使用する場合、ハブまたはイーサネット スイッチが自動ネゴシエーションに対応している必要があります。

- 自動ネゴシエーションを無効にする場合、[いいえ (No)] を選択し、ステップ 15 に進みます。

  [NIC スピードとデュプレックス設定 (NIC Speed and Duplex Configuration)] ウィンドウが表示されます。

ステップ 15　自動ネゴシエーション無効を選択した場合、ここで NIC の適切な速度とデュプレックス設定を選択し、[OK] を選択して継続します。

[MTU 設定 (MTU Configuration)] ウィンドウが表示されます。

ステップ 16　[MTU 設定 (MTU Configuration)] ウィンドウでは、MTU サイズをオペレーティング システムのデフォルトから変更できます。

Maximum Transmission Unit（MTU; 最大伝送ユニット）は、ホストがネットワーク上で送信する最大のパケットをバイト単位で表します。ネットワークの MTU 設定がよくわからない場合、デフォルト値として指定されている 1500 バイトを使用します。

注意　MTU サイズの設定が不適切な場合、ネットワークのパフォーマンスが低下する場合があります。

- デフォルト値（1500 バイト）を受け入れる場合、[いいえ (No)] を選択します。
- MTU サイズをオペレーティング システムのデフォルトから変更する場合、[はい (Yes)] を選択します。新しい MTU サイズを入力し、[OK] を選択します。

[DHCP 設定 (DHCP Configuration)] ウィンドウが表示されます。

ステップ 17　ネットワーク設定として、Cisco では Dynamic Host Configuration Protocol（DHCP; ダイナミック ホスト設定プロトコル）ではなく、サーバにスタティックなネットワーク IP アドレスを設定することを要求しています。DHCP を選択するかどうか尋ねられたときは、[いいえ (No)] を選択します。[スタティック ネットワーク設定 (Static Network Configuration)] ウィンドウが表示されます。

ステップ 18　スタティックなネットワーク設定値を設定し、[OK] を選択します。フィールドの説明については、表 2-4 を参照してください。

[DNS クライアント設定 (DNS Client Configuration)] ウィンドウが表示されます。

ステップ 19　Cisco は、DNS を有効にすることを要求します。[はい (Yes)] を選択します。DNS クライアント情報を入力し、[OK] を選択します。フィールドの説明については、表 2-4 を参照してください。

新しい設定情報を使用してネットワークが再起動します。[管理者ログイン設定 (Administrator Login Configuration)] ウィンドウが表示されます。

ステップ 20　表 2-4 の管理者ログインとパスワードを入力します。

（注）　管理者ログインは先頭がアルファベットの 6 文字以上の文字列とし、英数字、ハイフン、アンダースコアを使用できます。コマンド ライン インターフェイスへのログインでは、管理者ログインが必要です。

[証明書情報 (Certificate Information)] ウィンドウが表示されます。

ステップ 21　証明書署名要求情報を入力し、[OK] を選択します。

[NTP クライアント設定 (Network Time Protocol Client Configuration)] ウィンドウが開きます。

ステップ 22　Cisco Systems では、正確なシステム時刻のため、外部 NTP サーバの使用を推奨します。外部 NTP サーバがストラタム 9 以上まで識別できる（つまり、ストラタム 1 ～ 9 を含む）ことを確認します。

外部 NTP サーバを設定するか、システム時刻を手動設定するかを選択します。

- 外部 NTP サーバをセットアップする場合、[はい (Yes)] を選択します。最低 1 つの NTP サーバの IP アドレス、NTP サーバ名または NTP サーバ プール名を入力します。NTP サーバは 5 つまで設定できます。Cisco Systems では、最低 3 つの NTP サーバを設定することを推奨します。[続行 (Proceed)] を選択してインストールを継続します。

システムは NTP サーバと接続し、自動でハードウェア クロックに時刻を設定します。

（注）　[テスト (Test)] ボタンが表示された場合、[テスト (Test)] を選択して NTP サーバにアクセスできるかどうかを確認できます。

- システム時刻を手動設定する場合、[いいえ (No)] を選択します。ハードウェア クロックに設定する適切な日付と時刻を入力します。[OK] を選択してインストールを継続します。

[セキュリティ設定 (Security Configuration)] ウィンドウが開きます。

ステップ 23　表 2-4 のセキュリティ パスワードを入力します。

（注）　セキュリティ パスワードは先頭が英数字の 6 文字以上の文字列とし、英数字、ハイフン、アンダースコアを使用できます。

[プラットフォーム設定の確認 (Platform Configuration Confirmation)] ウィンドウが開きます。

ステップ 24　インストールを継続する場合、[OK] を選択します。プラットフォーム設定を変更する場合、[戻る (Back)] を選択します。

システムがソフトウェアのインストールと設定を行います。DVD ドライブがイジェクトされ、サーバが再起動します。DVD を再挿入しないでください。

ステップ 25　インストール プロセスが完了すると、管理者アカウントとパスワードでログインするようプロンプトが表示されます。

ステップ 26　「インストール後の作業」（P.2-18）に記載されている、インストール後の作業を実行します。

追加情報

「関連項目」（P.2-29）

インストール後の作業

サーバにソフトウェアをインストールした後、表 2-6 にリストしたインストール後の作業を完了する必要があります。

表 2-6　インストール後の作業

設定手順		関連する手順と項目
ステップ 1	Real-Time Monitoring Tool をクライアント マシンにインストールします。	Real-Time Monitoring Tool を使用して、システムの稼動状態の監視や、ログの参照と収集が行えます。 Real-Time Monitoring Tool のインストール手順と詳しい情報については、「RTMT のインストール」（P.7-1）を参照してください。
ステップ 2	サーバに Cisco Intercompany Media Engine ライセンス ファイルをアップロードします。	「ライセンス ファイルのアップロード」（P.2-23）を参照してください。
ステップ 3	GoDaddy.com から Cisco Intercompany Media Engine 証明書を取得します。	「証明書の購入と登録」（P.2-23）および「Cisco Intercompany Media Engine 証明書の手動更新」（P.2-25）を参照してください。

表 2-6　インストール後の作業 （続き）

設定手順		関連する手順と項目
ステップ 4	Cisco Unified Communications Manager と Cisco Intercompany Media Engine との間のセキュアな通信のために、自己署名またはサードパーティ製証明書にアクセスし、インストールします。	次のトピックを参照してください。 • 「Cisco Intercompany Media Engine サーバ上での自己署名証明書の生成とアップロード」（P.3-18） • 「Cisco Intercompany Media Engine 用のサードパーティ証明書の生成およびアップロード」（P.3-19）
ステップ 5	バックアップ設定を行います。 Cisco Intercompany Media Engine データは毎日バックアップするようにします。	「Cisco IME サーバのバックアップと復元」（P.5-1）を参照してください。
ステップ 6	Cisco IME サーバに、Cisco Unified Communications Manager と Cisco IME サーバとを接続して VAP シグナリングを交換可能な設定を作成する必要があります。 最初に、vapserver の名前とポートをセットアップします。	Cisco IME CLI にログインし、次のコマンドを入力します。 add ime vapserver vapserver の名前、ポート、認証モードの指定を求められます。ここで入力する名前が、このインスタンスの固有識別子となります。Cisco Unified Communications Manager の名前と一致させる必要はありません。選択する認証モードは、Cisco Unified Communications Manager と一致させる必要があります（暗号化済または認証済）。 **（注）** 同じ Cisco IME サーバを使用する複数の Cisco Unified Communications Manager がある場合、各クラスタに vapserver エントリを追加する必要があります。 各 vapserver 名につき、一意のポート番号を指定してください。 1 つのインスタンスを認証済モード用、もう 1 つを暗号化済および認証済モード用にした、複数の vapserver インスタンスを持つことができます。これらのインスタンスは、異なるポートを使用する必要があります。 コマンド オプションの詳細については、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。
ステップ 7	管理する vapserver をすべて表示します。	Cisco IME CLI にログインし、次のコマンドを入力します。 show ime vapserver all

表 2-6　インストール後の作業 （続き）

設定手順		関連する手順と項目
ステップ 8	（オプション）設定した各 vapserver インスタンスについて、必要に応じてオプションを設定します。	Cisco IME CLI にログインし、次のコマンドを入力します。 • set ime vapserver authenticationmode • set ime vapserver enabled • set ime vapserver keepaliveinterval • set ime vapserver maxconnectionsallowed • set ime vapserver port **（注）** Cisco では、認証モードを*暗号化済*に設定することを強く推奨します。 コマンド オプションの詳細については、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。
ステップ 9	VAP ユーザ クレデンシャルを Cisco IME サーバに設定します。	Cisco IME CLI にログインし、次のコマンドを入力します。 add ime vapusercredentials コマンド プロンプトがユーザ名とパスワードを尋ねます。 **（注）** 入力するアプリケーションのユーザ名とパスワードは、表 3-1 の ステップ 3 の Cisco Unified Communications Manager の管理 のアプリケーション ユーザに入力したものと一致している必要があります。 **（注）** チケットのパスワードと Epoch は、Cisco IME ASA で設定されたものと一致している必要があります。Cisco では、最低 20 文字のパスワードを作成することを推奨します。 コマンド オプションの詳細については、『*Cisco Intercompany Media Engine Command Line Interface Reference Guide*』を参照してください。

表 2-6　インストール後の作業 （続き）

設定手順		関連する手順と項目

ステップ 10	Cisco IME サーバがファイアウォール内にあり、公衆インターネットからサーバに到達するために Network Address Translation（NAT; ネットワークアドレス変換）が必要な場合、サーバが IME 分散キャッシュに参加可能になる前に Cisco IME サーバに外部アドレスを設定しておく必要があります。	1. Cisco IME CLI にログインし、次のコマンドを入力します。
		set ime addressing publicipaddrv4 *external ip addr*
		たとえば、Cisco IME のパブリック IP アドレスが 65.65.65.65 となる場合、次のように入力します。
		set ime addressing publicipaddrv4 65.65.65.65
		2. その後、次のコマンドを入力して設定を検証します。
		show ime addressing
		次の例では、Cisco IME サーバのパブリック IP アドレスとプライベート アドレスが表示されています。
		`admin: show ime addressing`
		`==========`
		`Public IP Address = 65.65.65.65`
		`Private IP Address = 10.10.10.10`
		`DHT Port = 6084`
		`Validator Port = 8470`
		`==========`

ステップ 11	Cisco IME サーバのピア ID のリストとブートストラップ サーバの IP アドレスが表示できることを確認します。	Cisco IME CLI にログインし、次のコマンドを入力します。 • show ime peerid ピア ID が表示されない場合、Cisco IME 証明書に問題がある可能性があります。設定を継続する前に、この問題を修正する必要があります。 • show ime bootstrap ip 最低 1 つの IP アドレスが表示されることを確認します。IP アドレスがまったく表示されない場合、Cisco IME が DNS 経由でブートストラップ サーバに接続できないことを意味します。

表 2-6　インストール後の作業 （続き）

設定手順		関連する手順と項目

ステップ 12	IME 分散キャッシュ上の Cisco IME サーバの状態を確認します。
	（注）　サーバがリングに参加し、ステータスがグリーンに変わるまでに 20 分かかる場合があります。
		Cisco IME CLI にログインし、次のコマンドを入力します。
		show ime dht summary
		[DHT Health] フィールドに、[Peer ID] フィールドのサーバのステータスが表示されます。グリーンは正常動作状態を示します。
		`Peer ID = 514dd001c7553593ebefee2b076ad9d4`
		`DHT Health.....= GREEN`
		`BootStrap: 5619e12c7a647e1d3364c8a46c9e58f7`
		`Last Contact (sec)..... = 48`
		`Current Sequence.....= 1250036323`
		`Num.Tokens Received.....= 3`
		`Delay from BootStrap.....= 1`
		`Peer Count Distance.....= 5`
		ピア ID のステータスがグリーンで表示されない場合、Cisco IME 証明書が正しくインストールされていることを確認し、Cisco IME ポートと Cisco IME が有効な ASA をチェックします。
		show ime addressing コマンドを使用して、パブリック IP アドレスが正しく設定されたことを確認する必要がある場合もあります。

ステップ 13	Cisco では、お客様連絡先情報を設定しておくことを強く推奨します。この情報はご使用の Cisco IME サーバ上に保存され、Cisco テクニカル サポートが Cisco IME サーバの設定ミスを検出した場合に使用されます。	Cisco IME CLI にログインし、次のコマンドを入力します。 set ime customerinfo 次の情報を尋ねるプロンプトがシステムに表示されます。 • [会社名 (Company Name)] : Cisco IME サーバを使用する企業の名前 • [ユニット名 (Unit Name)] : 企業内のユニット（都市名や部門） • [都道府県 (State)] : サーバの位置する都道府県 • [国 (Country)] : サーバの位置する国 • [サポート担当者名 (Support Contact Name)] : ご使用の Cisco IME サーバで Cisco が設定ミスを検出した場合に連絡する担当者 • [サポート電子メール (Support Contact Email)] : 会社のサポート連絡先電子メール • [サポート電話番号 (Support Contact Phone)] : サポート連絡先電話番号 お客様情報の設定後、show ime customerinfo コマンドで情報を表示できます。

追加情報

「関連項目」（P.2-29）

ライセンス ファイルのアップロード

ライセンス ファイル要求時に入力した MAC アドレスと一致する Cisco IME サーバに対して、ライセンス ファイルをアップロードする手順は、次のとおりです。ライセンス ファイルの取得については、「ライセンス ファイルの取得」（P.2-8）を参照してください。

始める前に

サーバに Cisco IME サーバ ソフトウェアがインストールされていることを確認します。

手順

ステップ 1　Cisco IME ライセンス ファイル（.lic）を、ローカル ハード ドライブ上の一時ディレクトリに保存します。

ステップ 2　SFTP クライアントを開き、インストール中にセットアップした adminsftp ユーザと管理者パスワードを使用して Cisco IME サーバに接続します。

ステップ 3　**cd license** と入力してライセンス ディレクトリに移動し、このディレクトリにライセンス ファイルをコピーします。

ステップ 4　**put** <*license filename*> と入力します。ここで、<*license filename*> には電子メールで受け取ったライセンス ファイルの名前を指定します。

ステップ 5　Cisco IME Command Line Interface（CLI; コマンド ライン インターフェイス）にログインして **utils ime license file install <license filename>** と入力し、Cisco IME ライセンスをアップロードします。

（注）　受信するライセンス ファイルの形式は、IME<タイムスタンプ>.lic です。.lic 拡張子を保持していれば、ライセンス ファイルの名前を変更することもできます。ファイルの内容に何らかの編集を加えると、ライセンスは使用できなくなります。

インストール後、サーバはライセンス ファイルを /usr/local/ime/conf/licfiles に保存します。サーバはライセンス ログを /active/cm/trace/ime/licensing/log4j に保存します。

追加情報

「インストール後の作業」（P.2-18）

証明書の購入と登録

Cisco IME はサーバ間の通信を暗号化します。同一グループによって信頼された各サーバに証明書が必要となります。証明書への自己署名はできません。証明書により、Cisco IME サーバは IME 分散キャッシュ リング上の他の Cisco IME サーバと TLS 接続を確立できるようになります。

IME 分散キャッシュ リングの証明書は、GoDaddy が提供します。GoDaddy は、タグ、peerIDCount、署名など Cisco IME ライセンス内の情報を使用して各サーバを一意に識別し、証明書を生成します。

Cisco IME サーバ用の証明書は、GoDaddy の Web サイトで購入します。証明書購入後、GoDaddy に証明書を登録します。登録プロセスでは、証明書を取得可能な、有効なサーバがあることを示す情報を提供します。証明書は購入日から 1 年間有効です。

Cisco IME サーバは、有効期限日付の前に証明書の更新を試みます。自動登録に失敗した場合、サーバは EnrollFailure アラームを生成します。この場合、証明書の手動更新が必要です。証明書の更新の詳細については、「Cisco Intercompany Media Engine 証明書の手動更新」（P.2-25）を参照してください。

新規証明書の購入と登録は、次の手順に従います。

始める前に

ライセンスを Cisco IME サーバにインストールします。手順は 「ライセンス ファイルのアップロード」（P.2-23）に説明されています。

手順

ステップ 1　http://www.godaddy.com に移動します。

ステップ 2　アカウント マネージャにログインします。

ステップ 3　[使用している製品 (My Products)] セクションで、[SSL 証明書 (SSL Certificates)] を選択します。

ステップ 4　Cisco IME サーバ用のライセンスを購入します。

（注）　証明書購入について詳しくは、GoDaddy の Web サイト上にある Cisco Intercompany Media Engine 証明書の要求とインストールについてのサポート トピック（http://help.godaddy.com/article/5414）を参照してください。

購入プロセスでは、ご使用のサーバのサーバ ID の入力が必要です。この ID を入手するには、Cisco IME サーバの CLI にログインし、**show ime certenrollment server ID** と入力します。

ステップ 5　プロンプトが表示されたら、Cisco IME サーバ CLI に **utils ime certenrollment enroll** と入力して Cisco IME サーバに証明書をインストールします。

ステップ 6　登録に成功した場合、Cisco IME サーバは SuccessfulEnrollment アラートを生成します。失敗した場合、EnrollFailure アラートを生成します。

ステップ 7　Cisco IME サーバ上の証明書を表示するには、CLI に移動して **show cert own intercompanymedianetwork** と入力します。

（注）　システムは、手動登録と自動登録のログ ファイルを、ディレクトリ /active/platform/log/cli*.log と /active/platform/log/certm.log にそれぞれ保存します。

追加情報

「インストール後の作業」（P.2-18）

Cisco Intercompany Media Engine 証明書の手動更新

Cisco IME サーバを最初にインストールする場合、GoDaddy で証明書の購入と登録が必要です。「証明書の購入と登録」（P.2-23）に説明されています。証明書は購入日から 1 年間有効です。Cisco IME サーバは、有効期限日付の前に証明書の更新を試みます。自動登録に失敗した場合、サーバは EnrollFailure アラートを生成します。次の手順で証明書を手動更新する必要があります。

手順

ステップ 1　http://www.godaddy.com に移動します。

ステップ 2　アカウント マネージャにログインします。

ステップ 3　[使用している製品 (My Products)] セクションで、[SSL 証明書 (SSL Certificates)] を選択し、更新する証明書を探します。

（注）　証明書更新について詳しくは、GoDaddy の Web サイト上にある Cisco Intercompany Media Engine 証明書の更新についてのサポート トピック（http://help.godaddy.com/article/5415）を参照してください。

ステップ 4　GoDaddy が支払を受領すると、次のいずれかのイベントが発生します。

- GoDaddy が以前の証明書の期限前に支払を受領した場合、証明書が更新され、それ以上の作業は必要ありません。
- GoDaddy が以前の証明書の期限後に支払を受領した場合、Cisco IME サーバ CLI で **utils ime certenrollment enroll** と入力します。

ステップ 5　登録に成功した場合、Cisco IME サーバは SuccessfulEnrollment アラートを生成します。失敗した場合、EnrollFailure アラートを生成します。

ステップ 6　Cisco IME サーバ上の証明書を表示するには、CLI に移動して **show cert own intercompanymedianetwork** と入力します。

（注）　システムは、手動登録と自動登録のログ ファイルを、ディレクトリ /active/platform/log/cli*.log と /active/platform/log/certm.log にそれぞれ保存します。

追加情報

「インストール後の作業」（P.2-18）

管理者パスワードとセキュリティ パスワードのリセット

管理者パスワードやセキュリティ パスワードを紛失した場合、次の手順でこれらのパスワードをリセットします。

パスワードのリセット プロセス実行では、システム コンソールを介してシステムに接続している必要があります。つまり、サーバにキーボードとモニタを接続する必要があります。セキュア シェル セッションを介してシステムに接続している場合、パスワードはリセットできません。

（注） この手順の間、システムに物理的にアクセスできることを証明するため、有効な CD または DVD をディスクドライブから取り出し、挿入することが必要になります。

手順

ステップ 1　次のユーザ名とパスワードでシステムにログインします。

- ユーザ名：pwrecovery
- パスワード：pwreset

[プラットフォームパスワードのリセットへようこそ (Welcome to platform password reset)] ウィンドウが表示されます。

ステップ 2　何かキーを押して継続します。

ステップ 3　ディスク ドライブに CD や DVD が入っている場合、ここで取り出します。

ステップ 4　何かキーを押して継続します。

システムは、CD や DVD をディスク ドライブから取り出したことをテストで確認します。

ステップ 5　ディスク ドライブに有効な CD または DVD を挿入します。

（注） このテストでは、音楽 CD ではなくデータ CD を使用します。

システムはディスクが挿入されたことをテストで確認します。

ステップ 6　システムは、ディスクが挿入されたことを確認した後、次のオプションのいずれかを選択して継続するようプロンプトを表示します。

- 管理者パスワードを変更するには、a を入力します。
- セキュリティ パスワードを変更するには、s を入力します。
- 終了するには、q を入力します。

ステップ 7　選択したタイプの新しいパスワードを入力します。

ステップ 8　新しいパスワードを再入力します。

パスワードは、最低 6 文字ある必要があります。システムは新規パスワードの強度をチェックします。パスワードが強度チェックに合格しなかった場合、新しいパスワードを入力するよう求められます。

ステップ 9　システムが新しいパスワードの強度を確認すると、パスワードがリセットされます。何かキーを押してパスワード リセット ユーティリティを終了するようプロンプトが表示されます。

追加情報

「関連項目」（P.2-29）

Cisco Intercompany Media Engine ソフトウェアのアップグレード

アップグレード プロセスを開始する前に、Cisco.com から適切なアップグレード ファイルを入手しておく必要があります。

次の手順で、Cisco Intercompany Media Engine（Cisco IME）サーバ ソフトウェアをアップグレードします。

（注） Cisco IME をアップグレードする場合、Cisco Unified Communications Manager 上で Cisco IME サービスと通信するサービスは停止します。この停止により、Cisco Unified Communications Manager はアップグレードが完了し Cisco IME サーバが新しいリリースにスイッチされるまで一時的にルートの学習を停止します。この期間中、Cisco IME サービスがダウンしていることを示すアラートが Cisco Unified Communications Manager サーバに表示されます。Cisco Unified Communications Manager への影響を最小限にするため、Cisco では Cisco IME サーバのアップグレードをアクティブでない時間帯に行うことを強く推奨します。アップグレード手順には、約 20 ～ 30 分かかります。

手順

ステップ 1　Cisco Intercompany Media Engine サーバをアップグレードするためのアップグレード メディアを取得します。

Cisco.com からソフトウェア実行ファイルをダウンロードした場合、次のいずれかを実行します。

- 次のステップを実行して、ローカル ディレクトリからのアップグレードを準備します。
  - Cisco IME アップグレード ファイルをローカル ハード ドライブの一時ディレクトリにコピーします。
  - ダウンロードしたアップグレード ファイルを ISO イメージとして DVD に焼き付け、アップグレード ディスクを作成します。

    （注） .iso ファイルを DVD にコピーしても ISO イメージが作成されない場合、ご使用のサーバをその DVD でアップグレードすることはできません。ほとんどの商用ディスク作成アプリケーションは、ISO イメージ ディスクを作成できます。

  - SFTP クライアントを開き、インストール中にセットアップした adminsftp ユーザと管理者パスワードを使用して Cisco IME サーバに接続します。
  - **cd upgrade** と入力してアップグレード ディレクトリに移動し、ライセンス ファイルをそのディレクトリにコピーします。
  - **put** <*upgrade filename*> と入力します。ここで、<*upgrade filename*> には Cisco.com からダウンロードした、または DVD で入手したアップグレード ファイルの名前を指定します。
- アップグレード ファイルをアップグレード中のサーバからアクセス可能な FTP または SFTP サーバ上に置きます。

  シスコが準備したアップグレード ディスクがある場合、ディスクの内容をリモート サーバにコピーします。

  アップグレード ファイルをダウンロードした場合、ダウンロードしたファイルをリモート サーバにコピーします。

ステップ 2　DVD をサーバに挿入した後、もしくはアップグレード ファイルをリモート サーバやローカル ディレクトリにアップロードした後、Cisco IME CLI にログインし、**utils system upgrade initiate** と入力します。

ステップ 3　アップグレードするときのソースを次の中から選択します。

- 1：リモート ファイルシステム、SFTP 経由
- 2：リモート ファイルシステム、FTP 経由
- 3：ローカル DVD/CD
- 4：ローカル アップロード ディレクトリ

ステップ 4　選択したアップグレード オプションのシステム プロンプトに従います。

ステップ 5　システムは、アップグレード プロセス完了時にプロンプトを表示します。バージョンの自動切り替えオプションを選択しなかった場合、**utils system switch-version** と入力し、さらに **yes** と入力してサーバの再起動と新しいソフトウェア バージョンへの切り替えを承認します。

ステップ 6　インストールが完了したら、Cisco IME CLI にログインし、次の内容を確認します。

- Cisco IME CLI にログインし、**show ime dht summary** と入力して DHT がグリーンのヘルス ステータスを表示していることを確認します。サーバがリングに参加し、ステータスがグリーンに変わるまでに 20 分かかる場合があります。
- **show ime vapstatus summary** と入力して、[登録ステータス (Registration Status)] が [登録済み (Registered)] になり、[クライアント IP ADDR(Client IP ADDR)] が Cisco Unified Communications Manager サーバの IP アドレスと同じになっていることを確認します。

追加情報

「関連項目」（P.2-29）

インストールのトラブルシューティング

次のセクションを使用して、Cisco Intercompany Media Engine ソフトウェアのインストール中に発生する問題のトラブルシューティングを行います。

インストール中のネットワーク エラーの処理

インストール プロセスの間、インストール プログラムは入力されたネットワーク設定を使用してサーバがネットワーク接続に成功するかどうかを検証します。サーバに接続できない場合、メッセージが表示され、次のオプションのいずれかを選択するよう促されます。

- [RETRY]：インストール プログラムは再度ネットワーキングを検証します。検証に失敗すると、エラー ダイアログボックスが再度表示されます。
- [REVIEW (Check Install)]：このオプションでは、ネットワーキング設定の確認と変更が行えます。検出された場合、インストール プログラムはネットワーク設定のウィンドウに戻ります。

  ネットワーキングは各ネットワーキング ウィンドウの完了後に検証されるため、メッセージが複数回表示される場合があります。

- [停止 (HALT)]：インストールを停止します。ネットワーク設定のトラブルシューティングに役立てるため、インストール ログ ファイルを USB ディスクにコピーできます。
- [無視 (IGNORE)]：インストールを継続します。ネットワーキングのエラーのログが記録されます。場合によっては、インストール プログラムがネットワーキングを複数回検証することがあり、このエラー ダイアログボックスも複数回表示されます。ネットワーク エラーを無視して継続すると、インストールが失敗する場合があります。

追加情報

「関連項目」（P.2-29）

ログ ファイルの調査

インストールの問題が発生した場合、コマンド ライン インターフェイスで次のコマンドを入力してインストール ログ ファイルを調査できます。

コマンド ラインからインストール ログ ファイルのリストを取得するには、次のように入力します。

```
CLI>file list install *
```

コマンド ラインからログ ファイルを表示するには、次のように入力します。

```
CLI>file view install log_file
```

log_file にはログ ファイル名を指定します。

Real-Time Monitoring Tool を使用してログを表示することもできます。Real-Time Monitoring Tool の使用とインストールについて詳しくは、『*Cisco Unified Real Time Monitoring Tool Administration Guide*』を参照してください。

システム履歴ログを表示またはダウンロードすることで、インストール イベントの詳細情報を知ることができます。詳細については、次の資料を参照してください。

- 「システム履歴ログ」（P.10-1）
- 『*Cisco Unified Real Time Monitoring Tool Administration Guide*』の「Working with Trace and Log Central」の章

追加情報

「関連項目」（P.2-29）

関連項目

- 「重要な考慮事項」（P.2-1）
- 「インストールに関する FAQ」（P.2-2）
- 「インストール前の作業」（P.2-5）
- 「インストールの開始」（P.2-13）
- 「インストール後の作業」（P.2-18）
- 「管理者パスワードとセキュリティ パスワードのリセット」（P.2-26）
- 「インストールのトラブルシューティング」（P.2-28）

関連項目