



CHAPTER 7

CTI OS セキュリティ

この章では、CTI OS セキュリティ証明書およびセキュリティ互換性の設定に関する情報を提供します。次のような構成になっています。

- 「CTI OS セキュリティ証明書の設定 (P.7-1)」
- 「CTI OS Security のレジストリ キー (P.7-6)」
- 「セキュリティ互換性 (P.7-8)」

CTI OS セキュリティ証明書の設定

CTI OS セキュリティ証明書は、次の要素で構成されます。

- CTI OS Security Setup プログラム
- 自己署名型の認証局 (CA) を使用した CTI Toolkit Desktop Client 証明書要求の署名。
- 自己署名型 CA を使用した CTI OS サーバ証明書要求の署名。
- サードパーティ CA を使用した CTI Toolkit Desktop Client 証明書要求の署名。
- サードパーティ CA を使用した CTI OS サーバ証明書要求の署名。

ここでは、これらの各エントリについて詳しく説明します。



(注) 証明書失効リスト (CRL) と証明書チェーンのいずれも、CTI OS Security ではサポートされません。

CTI OS Security Setup プログラム

CTI OS を設定するため、3つのセットアッププログラムが実装されます。これらのセットアッププログラムは Win32 CTI OS ツールキット インストールの一部であり、<drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Security\Utilities ディレクトリに配置されます。

1. 1つ目のセットアッププログラム **CreateSelfSignedCASetupPackage.exe** は、自己署名型認証局 (CA) を作成します。お客様がサードパーティの代わりに自己署名型 CA の使用を希望している場合は、このプログラムを1度実行し、**CreateSelfSignedCASetupPackage.exe** の出力を安全な場所に保存する必要があります。このプログラムにより、CA 関連のファイルが作成されます。**CtiosRoot.pem** というファイルには、プライベート CA 情報が格納されます。このファイルは、安全な場所に保管してください。**CtiosRootCert.pem** というもう1つのファイルには、パブリック CA 情報が格納されます。このセットアッププログラムを実行すると、CA のパスワード (8文字以上 30文字以内) の入力を求められます。このパスワードは、CTI OS 証明書要求に署名するときに使用します。

2. 2 つ目のセットアッププログラム **SecuritySetupPackage.exe** は、CTI Toolkit Desktop Client および CTI OS サーバに対する証明書要求の生成に使用します。証明書要求が CTI OS サーバに対するものである場合、**CtiosServerKey.pem** および **CtiosServerReq.pem** が生成されます。これらのファイルは、サーバ証明書に署名するときに使用します。証明書要求が CTI Toolkit Desktop Client に対するものである場合、**CtiosClientkey.pem** および **CtiosClientreq.pem** が生成されます。これらのファイルは、クライアント証明書に署名するときに使用します。
3. 3 つ目のセットアッププログラム **SignCertificateSetupPackage.exe** は、CTI Toolkit Desktop Client および CTI OS サーバの証明書の署名に使用します。このプログラムは、お客様が CTI Toolkit Desktop Client および CTI OS サーバの証明書に自己署名型 CA を使用して署名することに決定した場合のみ使用します。このプログラムは、**CtiosRootCert.pem** および **CtiosRoot.pem** と同じディレクトリに存在している必要があります。署名する証明書がクライアント用である場合、**CtiosClient.pem** ファイルが生成されます。署名する証明書がサーバ用である場合、**CtiosServer.pem** ファイルが生成されます。このプログラムを実行すると、次の情報の入力を求められます。
 - a. Ctios 認証局のパスワード。これは、自己署名型 CA を作成するときに使用したパスワードです。
 - b. CTI Toolkit Desktop Client 証明書要求か CTI OS サーバ証明書要求のいずれかを選択します。

自己署名型 CA を使用した CTI Toolkit Desktop Client 証明書要求の署名

CTI Toolkit Desktop Client 証明書要求に署名するには、次の手順を実行します。

-
- ステップ 1 自己署名型 CA が存在しない場合、**CreateSelfSignedCASetupPackage.exe** を実行し、**CreateSelfSignedCASetupPackage.exe** プログラムによって作成されたファイルをすべて安全な場所に保管します。
 - ステップ 2 CTI Toolkit Desktop Client マシンから、**CtiosRoot.pem** と **CtiosRootCert.pem** が存在するマシンに **CtiosClientkey.pem** ファイルおよび **CtiosClientreq.pem** ファイルをコピーします。**CtiosClientkey.pem** と **CtiosClientreq.pem** の両ファイルを **CtiosRoot.pem** および **CtiosRootCert.pem** と同じディレクトリにコピーする必要があります。
 - ステップ 3 **CtiosClientkey.pem**、**CtiosClientreq.pem**、**CtiosRoot.pem**、および **CtiosRootCert.pem** が存在するディレクトリから **SignCertificateSetupPackage.exe** を実行し、[CTIOS Client Certificate Request] を選択して、「Ctios 認証局パスワード」を入力します。この手順が成功すると **CtiosClient.pem** ファイルが生成され、失敗するとエラーメッセージが表示されます。
 - ステップ 4 CTI Toolkit Desktop Client がインストールされているマシンに **CtiosClient.pem** と **CtiosRootCert.pem** の両方をコピーし、<drive>:\Program Files\Cisco Systems\CTIOS Client\CTIOS Security ディレクトリに保存します。
 - ステップ 5 CTI Toolkit Desktop Client がインストールされているマシンから、**CtiosClientkey.pem** を削除します。
 - ステップ 6 **SignCertificateSetupPackage.exe** を実行したマシンから、**CtiosClientkey.pem**、**CtiosClientreq.pem**、および **CtiosClient.pem** を削除します。
-

自己署名型 CA を使用した CTI OS サーバ証明書要求の署名

CTI OS サーバ証明書要求に署名するには、次の手順を実行します。

-
- ステップ 1** 自己署名型 CA が存在しない場合、**CreateSelfSignedCASetupPackage.exe** を実行し、**CreateSelfSignedCASetupPackage.exe** プログラムによって作成されたファイルをすべて安全な場所に保管します。
- ステップ 2** CTI OS サーバマシンから、**CtiosRoot.pem** と **CtiosRootCert.pem** が存在するマシンに **CtiosServerKey.pem** ファイルおよび **CtiosServerReq.pem** ファイルをコピーします。**CtiosServerKey.pem** と **CtiosServerReq.pem** の両ファイルを **CtiosRoot.pem** および **CtiosRootCert.pem** と同じディレクトリ (<drive>:\icm\<Instance name>\CTIOS1\Security) にコピーする必要があります。
- ステップ 3** **CtiosServerKey.pem**、**CtiosServerReq.pem**、**CtiosRoot.pem**、および **CtiosRootCert.pem** が存在するディレクトリから **SignCertificateSetupPackage.exe** を実行し、[CTIOS Server Certificate Request] を選択して、「Ctios 認証局パスワード」を入力します。この手順が成功すると **CtiosServer.pem** ファイルが生成され、失敗するとエラー メッセージが表示されます。
- ステップ 4** CTI OS サーバが存在するマシンに **CtiosServer.pem** および **CtiosRootCert.pem** をコピーして、<drive>:\icm\<Instance name>\CTIOS1\Security ディレクトリに保存します。
- ステップ 5** CTI OS サーバがインストールされたマシンから **CtiosServerkey.pem** を削除します。
- ステップ 6** **SignCertificateSetupPackage.exe** を実行したマシンから、**CtiosServerKey.pem**、**CtiosServerReq.pem**、および **CtiosServer.pem** を削除します。
- ステップ 7** CTI OS サーバがピア サーバである場合は、次の作業を行います。
- CTI OS サーバマシンから、**CtiosRoot.pem** と **CtiosRootCert.pem** が存在するマシンに **CtiosClientkey.pem** ファイルおよび **CtiosClientreq.pem** ファイルをコピーします。**CtiosClientkey.pem** と **CtiosClientreq.pem** の両ファイルを **CtiosRoot.pem** および **CtiosRootCert.pem** と同じディレクトリにコピーする必要があります。
 - CtiosClientkey.pem**、**CtiosClientreq.pem**、**CtiosRoot.pem**、および **CtiosRootCert.pem** が存在するディレクトリから **SignCertificateSetupPackage.exe** を実行し、[CTI Desktop Client Certificate Request] を選択して、「Ctios 認証局パスワード」を入力します。この手順が成功すると **CtiosClient.pem** ファイルが生成され、失敗するとエラー メッセージが表示されます。
 - CTI OS サーバが存在するマシンに **CtiosClient.pem** をコピーして、<drive>:\icm\<Instance name>\CTIOS1\Security ディレクトリに保存します。
 - CTI OS サーバがインストールされたマシンから **CtiosClientkey.pem** を削除します。
 - SignCertificateSetupPackage.exe** を実行したマシンから、**CtiosClientkey.pem**、**CtiosClientreq.pem**、および **CtiosClient.pem** を削除します。
-

サードパーティ CA を使用した CTI Toolkit Desktop Client 証明書要求の署名

CTI Toolkit Desktop Client 証明書要求に署名するには、次の手順を実行します。

-
- ステップ 1** CTI Toolkit Desktop Client マシンから、サードパーティ CA が存在するマシンに **CtiosClientreq.pem** ファイルをコピーします。
 - ステップ 2** サードパーティ CA を使用して CTI Toolkit Desktop Client 証明書要求 (CtiosClientreq.pem) に署名することで、CTI Toolkit Desktop Client 証明書が生成されます。証明書の名前を **CtiosClientCert.pem** に変更します。
 - ステップ 3** サードパーティ CA では、証明書のパブリック情報がファイルに保存されます。このファイルの名前を **CtiosRootCert.pem** に変更します。
 - ステップ 4** CTI Toolkit Desktop Client が存在するマシンに **CtiosClientCert.pem** と **CtiosRootCert.pem** の両方をコピーし、<drive>:\Program Files\Cisco Systems\CTIOS Client\Security ディレクトリに保存します。
 - ステップ 5** CTI Toolkit Desktop Client マシンの **CtiosClientCert.pem** ファイル内のデータと **CtiosClientkey.pem** ファイル内のデータを **CtiosClient.pem** という 1 つのファイルにコピーします。順序は非常に重要であり、**CtiosClient.pem** には最初に **CtiosClientCert.pem** データ、次に **CtiosClientkey.pem** データが格納される必要があります。
 - ステップ 6** CTI Toolkit Desktop Client マシンから **CtiosClientCert.pem** および **CtiosClientkey.pem** を削除します。
-

サードパーティ CA を使用した CTI OS サーバ証明書要求の署名

CTI OS サーバ証明書要求に署名するには、次の手順を実行します。

-
- ステップ 1** CTI OS サーバマシンから、サードパーティ CA が存在するマシンに **CtiosServerReq.pem** ファイルをコピーします。
 - ステップ 2** サードパーティ CA を使用して CTI OS サーバ証明書要求 (CtiosServerReq.pem) に署名すると、CTI OS サーバ証明書が生成されます。証明書の名前を **CtiosServerCert.pem** に変更します。
 - ステップ 3** サードパーティ CA では、証明書のパブリック情報がファイルに保存されます。このファイルの名前を **CtiosRootCert.pem** に変更します。
 - ステップ 4** CTI OS サーバが存在するマシンに **CtiosServerCert.pem** および **CtiosRootCert.pem** をコピーして、<drive>:\icm\<Instance name>\CTIOS1\Security ディレクトリに保存します。
 - ステップ 5** CTI OS サーバマシンの **CtiosServerCert.pem** ファイル内のデータと **CtiosServerkey.pem** ファイル内のデータを **CtiosServer.pem** と呼ばれる 1 つのファイルにコピーします。順序は非常に重要であり、**CtiosServer.pem** には最初に **CtiosServerCert.pem** データ、次に **CtiosServerkey.pem** データが格納される必要があります。
 - ステップ 6** CTI OS サーバマシンから **CtiosServerCert.pem** および **CtiosServerkey.pem** を削除します。
 - ステップ 7** CTI OS サーバがピアサーバである場合は、次の作業を行います。
 - a.** CTI OS サーバマシンから、サードパーティ CA が存在するマシンに **CtiosClientreq.pem** ファイルをコピーします。
 - b.** サードパーティ CA を使用して CTI Toolkit Desktop Client 証明書要求 (CtiosClientreq.pem) に署名することで、CTI Toolkit Desktop Client 証明書が生成されます。証明書の名前を **CtiosClientCert.pem** に変更します。

- c. CTI OS サーバが存在するマシンに **CtiosClientCert.pem** ファイルをコピーして、
<drive>:\icm\<Instance name>\CTIOS1\Security ディレクトリに保存します。
- d. CTI OS サーバ マシンの **CtiosClientCert.pem** ファイル内のデータと **CtiosClientkey.pem** ファイル内のデータを **CtiosClient.pem** と呼ばれる 1 つのファイルにコピーします。ファイルは必ずこの順序でコピーして、**CtiosClient.pem** に最初に **CtiosClientCert.pem** データ、次に **CtiosClientkey.pem** データが保存されるようにします。
- e. CTI OS サーバ マシンから **CtiosClientCert.pem** および **CtiosClientkey.pem** を削除します。

CTI OS Security のパスワード

CTI OS Security には、次の 5 つのタイプのパスワードが導入されています。

1. CTI OS クライアント証明書パスワード：管理者またはインストーラは、CTI OS クライアントセキュリティをインストールするときに、このパスワードを入力します。このパスワードは、CTI OS クライアント証明書要求の秘密キーに使用され、任意の文字にすることができます。管理者およびインストーラはこのパスワードを覚えておく必要はありません。
2. CTI OS サーバ証明書パスワード：管理者またはインストーラは、CTI OS サーバセキュリティをインストールするときに、このパスワードを入力します。このパスワードは、CTI OS サーバ証明書要求の秘密キーに使用され、任意の文字にすることができます。管理者およびインストーラはこのパスワードを覚えておく必要はありません。
3. CTI OS ピア証明書パスワード：管理者またはインストーラは、CTI OS サーバセキュリティをインストールするときに、このパスワードを入力します。このパスワードは、CTI OS ピアサーバ証明書要求の秘密キーに使用され、任意の文字にすることができます。管理者およびインストーラはこのパスワードを覚えておく必要はありません。
4. モニタモードパスワード：管理者またはインストーラは、CTI OS サーバセキュリティをインストールするときに、このパスワードを入力します。このパスワードは、エージェントが AllAgents や AllCalls などの CTI OS モニタモードアプリケーションを使用してセキュアな CTI OS サーバに接続するときに使用されます。このパスワードは、両方の CTI OS ピアサーバで同一である必要があります。管理者またはインストーラと、CTI OS モニタモードアプリケーションのユーザはこのパスワードを覚えておく必要があります。
5. 認証局 (CA) パスワード：管理者またはインストーラが自己署名型 CA を作成するときに、このパスワードを入力します。パスワードは任意の文字にすることができます。管理者またはインストーラは、この CA で証明書要求に署名するときに常にこのパスワードを使用するので、覚えておく必要があります。

CTI OS Security のレジストリ キー


[HKEY_LOCAL_MACHINE¥SOFTWARE¥CiscoSystems, Inc.¥CTIOS¥<CTIOS_InstanceName>¥CTIOS1¥Server¥Security] にあるレジストリ キーは、CTI OS サーバセキュリティの設定を定義します。

表 7-1 に、これらのキーのレジストリ値を示します。

表 7-1 CTI OS サーバのレジストリ値

レジストリ値の名前	値の種類	説明	デフォルト
AuthenticationEnabled	DWORD 値	このマニュアルの 認証メカニズム の項を参照してください。	1
CAType	DWORD 値	インストール時に作成されます。値 1 は、選択された CA タイプが自己署名型であり、値 2 は選択した CA タイプがサードパーティであることを意味します。	1
NumBytesRenegotiation	DWORD 値	セッションの再ネゴシエーション、つまり、すでに確立された接続時におけるハンドシェイクの実行要求に使用されます。これにより、CTI OS クライアントの資格情報が再評価され、新しいセッションが作成されます。長時間の SSL 接続に対しては定期的にセッション キーを置換することが重要です。そうすることで、CTI OS サーバと CTI OS クライアントの接続の安全性が高まります。再ネゴシエーションは、CTI OS サーバが CTI OS クライアントに 10000000 バイトを送信した後で行われます。デフォルトは最小値の 10000000 です。	10000000
SecurityEnabled	DWORD 値	インストール時に作成されます。値 1 は CTI OS Security が有効であり、値 0 は CTI OS Security が無効であることを意味します。	0

表 7-1 CTI OS サーバのレジストリ値 (続き)

レジストリ値の名前	値の種類	説明	デフォルト
MonitorModeDisableThreshold	DWORD 値	<p>モニタ モードが無効になるまでの、モニタ モード機能へのアクセスの連続失敗回数を制御します。</p> <p> (注) 詳細については、「モニタ モードのセキュリティ」の項を参照してください。</p>	3 (デフォルト)
MonitorModeDisableDuration	DWORD 値	<p>モニタ モード機能へのアクセスに対して設定された連続失敗回数に達した後で、モニタ モード機能が無効になる時間の長さを制御します。</p> <p> (注) 詳細については、「モニタ モードのセキュリティ」の項を参照してください。</p>	15 分 (デフォルト)

[HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\CTI OS Client\CtiOs] にあるレジストリ キーは CTI OS クライアントセキュリティの設定を定義します。表 7-2 に、これらのキーのレジストリ値を示します。

表 7-2 CTI OS クライアントのレジストリ値

レジストリ値の名前	値の種類	説明	デフォルト
CAType	DWORD 値	インストール時に作成されます。値 1 は、選択された CA タイプが自己署名型であり、値 2 は選択した CA タイプがサードパーティであることを意味します。	1
HandShakeTime	DWORD 値	インストール時に作成されます。このキーは、SSL/TLS ハンドシェイク段階で CTI OS クライアントが待機する時間を定義します。	5

モニタ モードのセキュリティ

CTI OS サーバのセキュリティが有効である場合、サーバは、モニタ モード機能へのアクセスを取得しようとする不正な試みからサーバ自体を保護します。これには、モニタ モード機能へのアクセスの失敗回数を追跡します。モニタ モード機能へのアクセスに対して設定された連続失敗回数に達すると（デフォルトでは3回）、CTI OS サーバはモニタ モード機能を無効にします。その場合、モニタ モード機能へのアクセスはすべて失敗します。この状況は、最後にモニタ モード機能へのアクセスに失敗してから、設定された時間が経過するまで続きます。この時間は、デフォルトで15分に設定されます。

デフォルトを変更できるように、`[MonitorModeDisableThreshold]` レジストリ設定と `[MonitorModeDisableDuration]` レジストリ設定が `HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Ctios\CTIOS<instance>\<ServerName>\Server\Security` に追加されました。

- `[MonitorModeDisableThreshold]` : このレジストリ フィールドは `DWORD` です。モニタ モードが無効になるまでの、モニタ モード機能へのアクセスの連続失敗回数を制御します。
- `[MonitorModeDisableDuration]` : このレジストリ フィールドは `DWORD` です。モニタ モード機能へのアクセスに対して設定された連続失敗回数に達した後で、モニタ モード機能が無効にある時間の長さを制御します。

セキュリティ互換性

ネットワーク上で安全にデータを受け渡すことは、シスコにとってもお客様にとっても重要です。CTI OS 6.0 以前のリリースは、どのタイプのセキュリティもサポートしません。CTI OS 7.0 には、セキュリティを扱うため、次の2つの機能が実装されました。

- **ワイヤ レベル暗号化** : トランスポート層セキュリティ (TLS) を使用する CTI OS サーバと CTI OS クライアント間のすべてのトラフィックを保護するのに役立ちます。このプロトコルは、トランスポート層 (TCP) で暗号化と証明書を提供します。
- **認証メカニズム** : IPCC および System IPCC に対してのみ、エージェントが適切なパスワードを入力した場合に限り、正常にログインできるようにします。



(注)

このマニュアルに記載されている情報は、Cisco Unified System Contact Center Enterprise (Unified SCCE) の導入環境に関連する内容ではありません。Cisco IPCC Enterprise Web Administration Tool は Unified SCCE の管理に使用します。(Unified SCCE Release 7.5 は、8.0(1) ソリューションでサポートされます)。

ワイヤ レベル暗号化

ワイヤ レベル暗号化は、CTI OS サーバ 7.0 と CTI OS クライアント 7.0 間にのみ暗号化メカニズムを提供します。デフォルトでは、ワイヤ レベル暗号化はオフになります。`[SecurityEnabled]` レジストリ キーの値が 0 の場合、セキュリティ機能は無効です。`[SecurityEnabled]` レジストリ キーの値が 1 の場合、セキュリティ機能は有効です。このキーは、次の場所に存在します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<InstanceName>\CTIOS1\Server\Security
```


CTI OS サーバ 7.0 でセキュリティ機能が有効になっている場合、以前のバージョンの CTI OS クライアントとこのバージョンの CTI OS サーバ間の下位互換性は維持されません。また、CTI OS サーバでセキュリティ機能が有効になっている場合、.NET CIL、Java CIL、または Siebel Driver を使用する CTI OS 7.0 クライアントは CTI OS サーバに接続できません。ある CTI OS サーバでセキュリティ機能が有効であり、このサーバにピアが存在する場合は、ピアサーバでもセキュリティ機能を有効にする必要があります。表 7-3 に、CTI OS ツールキットのリストを示します。

表 7-3 ワイヤ レベル暗号化 : CTI OS ツールキットのリスト

	C++ CIL ツールキット	COM CIL ツールキット	Java CIL ツールキット	.NET CIL ツールキット
ワイヤ レベル暗号化のサポート	Yes	Yes	No	No

表 7-4 に、CTI OS サーバ 8.0 と CTI OS クライアント 8.0 の間の互換性情報を示します。

表 7-4 ワイヤ レベル暗号化 : CTI OS ツールキットのリスト

	C++ CIL ツールキット を使用する CTI OS クラ イアント 8.0	COM CIL ツールキット を使用する CTI OS クラ イアント 8.0	Java CIL ツールキット を使用する CTI OS クラ イアント 8.0	.NET CIL ツールキット を使用する CTI OS クラ イアント 8.0
CTI OS サーバ 8.0 (セキュリティ 機能が有効)	Yes	Yes	No	No
CTI OS サーバ 8.0 (セキュリティ 機能が無効)	Yes	Yes	Yes	Yes

表 7-5 に、CTI OS サーバ 7.0 と CTI OS クライアント 6.0 以前のバージョンの間の互換性情報を示します。

表 7-5 ワイヤ レベル暗号化 : CTI OS サーバ 7.0 と CTI OS クライアント 6.0 以前のバージョン

	C++ CIL ツール キットを使用する CTI OS クライ アント 6.0 以前の バージョン	COM CIL ツール キットを使用する CTI OS クライ アント 6.0 以前の バージョン	Java CIL ツール キットを使用する CTI OS クライ アント 6.0
CTI OS サーバ 7.0 (セキュリティ機能が 有効)	No	No	No
CTI OS サーバ 7.0 (セキュリティ機能が 無効)	Yes	Yes	Yes

認証メカニズム

認証メカニズムは、IPCC 専用です。デフォルトではオンになります。[AuthenticationEnabled] レジストリ キーの値が 0 の場合、認証機能は無効です。[AuthenticationEnabled] レジストリ キーの値が 1 の場合、認証機能は有効です。このキーは、次の場所に存在します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<InstanceName>\CTIOS1\Server\Security
```

IPCC、System IPCC、または HIPCC 以外のすべてのペリフェラルについては、このレジストリ キーは使用されません。



(注)

認証機能が有効になっている場合に、エージェントをログインせずにエージェント モードを設定していると、CTI OS クライアント (CIL) はイベントをブロックします。これを回避するには、認証機能をオフにするか、エージェントを実際にログインします。この問題は、モニタ モードではなく、エージェント モードでのみ発生します。

表 7-6 に、CTI OS サーバ 8.0 と CTI OS クライアント 8.0 の間の互換性情報を示します。

表 7-6 認証メカニズム : CTI OS サーバ 8.0 と CTI OS クライアント 8.0

	C++ CIL ツールキットを使用する CTI OS クライアント 8.0	COM CIL ツールキットを使用する CTI OS クライアント 8.0	Java CIL ツールキットを使用する CTI OS クライアント 8.0	.NET CIL ツールキットを使用する CTI OS クライアント 8.0
CTI OS サーバ 8.0 (認証機能が有効)	Yes	Yes	Yes	Yes
CTI OS サーバ 8.0 (認証機能が無効)	No	No	No	No

表 7-7 に、CTI OS サーバ 7.0 と CTI OS クライアント 6.0 以前のバージョンの間の互換性情報を示します。

表 7-7 認証メカニズム : CTI OS サーバ 7.0 と CTI OS クライアント 6.0 以前のバージョン

	C++ CIL ツールキットを使用する CTI OS クライアント 6.0 以前のバージョン	COM CIL ツールキットを使用する CTI OS クライアント 6.0 以前のバージョン	Java CIL ツールキットを使用する CTI OS クライアント 6.0
CTI OS サーバ 7.0 (認証機能が有効)	Yes (*、**)	Yes (*、**)	Yes (*、**)
CTI OS サーバ 7.0 (認証機能が無効)	Yes	Yes	Yes

* 当該のエージェントがまだログインしていなくても、CTI OS Agent Desktop、IPCC Supervisor Desktop、および BA Phone には常に「Agent with ID <ID> is already logged in to instrument <INSTRUMENT>」という CTI 警告が表示されます。この問題は、[WarnIfAlreadyLoggedIn] レジストリ キーを 0 に設定することで解決します。このキーは、次の場所に存在します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<InstanceName>\CTIOS1\EnterpriseDesktopSettings\All Desktops\Login\
ConnectionProfiles\Name<ConnectionProfileName>
```

** 次のシナリオが想定されています。

- エージェント A が CTI OS Agent Desktop、IPCC Supervisor Desktop、BA Phone のいずれかを使用してすでに CTIOS サーバにログインしている。
- エージェント B が CTI OS Agent Desktop、IPCC Supervisor Desktop、BA Phone のいずれかを使用して CTI OS サーバに接続している。
- エージェント B がエージェント A の ID と無効なパスワードを使用してログインしようとしている。
- エージェント B が制御障害を受信したが、デスクトップでは [Login]、[Logout]、[Ready] の 3 つのボタンすべてが有効になっている (エージェント B はこれらのボタンを使用して、エージェント A のデスクトップを操作できます)。
- エージェント B が [Ready] ボタンを押すと、ボタンの有効化が正常になる。また、エージェント B のデスクトップには、このエージェントがまだログインしていなくても、「Agent with ID <ID> is already logged in to instrument <INSTRUMENT>」という CTI 警告が表示されます。

この問題は、[WarnIfAlreadyLoggedIn] レジストリ キーを 0 に設定することで解決します。このキーは、次の場所に存在します。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems,
Inc.\Ctios\CTIOS_<InstanceName>\CTIOS1\EnterpriseDesktopSettings\All Desktops\Login\
ConnectionProfiles\Name<ConnectionProfileName>
```

また、デスクトップには、「The request specified an invalid agent password」という CTI 警告も表示されます。



(注)

1 つの CTI OS サーバがダウン状態のときに、6.0 以前のクライアントが最初にダウンした CTI OS サーバに接続しようとする、ログインに失敗する可能性があります。この場合、エージェントは再びログインを試みます。デスクトップがアップ状態の CTI OS サーバに接続すると、適切な資格情報が入力されている限り、エージェントはログインされます。

