APPENDIX A

トラブルシューティング

CiscoWorks Common Services は、Security Manager に、サーバ上でのインストール、アンインストール、および再インストール用のフレームワークを提供します。Security Manager サーバ ソフトウェアのインストールまたはアンインストールでエラーが発生した場合は、Common Services のオンライン ヘルプまたは Cisco.com（http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.1/install/guide/IGSG31.html）の「Troubleshooting and FAQs」を参照してください。

次のトピックは、スタンドアロン バージョンの Cisco Security Agent を含む、クライアント システムまたはサーバ上に Security Manager 関連ソフトウェア アプリケーションをインストール、アンインストール、または再インストールしたときに発生する可能性のある問題の解決に役立ちます。

- 「Cisco Security Manager サービスの起動要件」（P.A-1）
- 「必要な TCP ポートと UDP ポートの包括的リスト」（P.A-2）
- 「Security Manager サーバのトラブルシューティング」（P.A-3）
- 「Security Manager クライアントのトラブルシューティング」（P.A-9）
- 「サーバ セルフテストの実行」（P.A-16）
- 「サーバ トラブルシューティング情報の収集」（P.A-16）
- 「サーバ プロセス ステータスの表示と変更」（P.A-17）
- 「サーバ インストール ログ ファイルの確認」（P.A-18）

Cisco Security Manager サービスの起動要件

Cisco Security Manager サービスは、特定の順序で起動しなければ、Security Manager が正しく機能しません。これらのサービスの初期化は、Cisco Security Manager Daemon Manager サービスによって制御されます。Cisco Security Manager サービスの起動タイプは変更しないでください。また、Cisco Security Manager サービスは手動で停止または開始しないでください。特定のサービスを再起動しなければならない場合は、Cisco Security Manager Daemon Manager を再起動して、すべての関連サービスが正しい順序で停止および開始する必要があります。

必要な TCP ポートと UDP ポートの包括的リスト

Cisco Security Management Suite アプリケーションは、クライアントや他のアプリケーションと通信する必要があります。その他のサーバ アプリケーションは別のコンピュータ上にインストールできます。通信を成功させるためには、特定の TCP ポートと UDP ポートを開いて、トラフィック送信に使用できるようにする必要があります。通常は、「必要なサービスとポート」（P.3-1）に記載されているポートを開くだけで十分です。ただし、アプリケーションが通信不能なことを検出した場合は、次の表内のポートも開く必要もあります。リストはポート番号順に並んでいます。

表 A-1　必要なサービスとポート

サービス	対象または使用アプリケーション	ポート番号 / ポートの範囲	プロトコル	着信	発信
ping	RME	—	ICMP	—	X
FTP	Security Manager と TMS サーバ間の通信	21	TCP	—	X
SSH	Common Services	22	TCP	—	X
	Security Manager	22	TCP	—	X
	RME	22	TCP	—	X
Telnet	Security Manager	23	TCP	—	X
	RME	23	TCP	—	X
SMTP	Common Services	25	TCP	—	X
TACACS+（ACS の場合）	Common Services	49	TCP	—	X
	RME		TCP	—	X
TFTP	Common Services	69	UDP	X	X
HTTP	Common Services	80	TCP	—	X
	Security Manager		TCP	—	X
SNMP（ポーリング）	Common Services	161	UDP	—	X
	Performance Monitor	161	UDP	—	X
SNMP（トラップ）	Common Services	162	UDP	—	X
	Performance Monitor	162	UDP	X	—
HTTPS（SSL）	Common Services	443[1]	TCP	X	—
	Security Manager		TCP	X	X
	AUS		TCP	X	—
	Performance Monitor		TCP	X	—
Syslog[2]	Security Manager	514	UDP	X	—
	Common Services（Security Manager がインストールされていない場合）	514 または 49514（この行の脚注を参照）	UDP	X	—
	Performance Monitor（Security Manager がインストールされていない場合）	514	UDP	X	—
リモート コピー プロトコル	Common Services	514	TCP	X	X

表 A-1　必要なサービスとポート （続き）

サービス	対象または使用アプリケーション	ポート番号 / ポートの範囲	プロトコル	着信	発信
HTTP	Common Services	1741	TCP	X	—
	Security Manager		TCP	X	—
	AUS		TCP	X	—
	Performance Monitor		TCP	X	—
RADIUS LDAP Kerberos	Security Manager（外部 AAA サーバへ）	1645、1646、1812（新規）、389、636（SSL）、88	TCP	—	X
Access Control Server HTTP/HTTPS	Security Manager	2002	TCP	—	X
CiscoWorks ゲートキーパー用の HIPO ポート	Common Services	8088	TCP	X	X
Tomcat シャットダウン	Common Services	9007	TCP	X	—
Tomcat Ajp13 コネクタ	Common Services	9009	TCP	X	—
データベース	Security Manager	10033	TCP	X	—
License Server	Common Services	40401	TCP	X	—
Daemon Manager	Common Services	42340	TCP	X	X
Osagent	Common Services	42342	UDP	X	X
データベース	Common Services	43441	TCP	X	—
Sybase	Auto Update Server	43451	TCP	X	X
	Performance Monitor	43453	TCP	X	X
DCR と OGS	Common Services	40050 ～ 40070	TCP	X	—
Event Services	Software Service	42350/44350	UDP	X	X
	Software Listening	42351/44351	TCP	X	X
	Software HTTP	42352/44352	TCP	X	X
	Software Routing	42353/44353	TCP	X	X
転送メカニズム（CSTM）	Common Services	50000 ～ 50020	TCP	X	—

1. Cisco Security Monitoring, Analysis, and Response System（Cisco Security MARS）アプライアンスと情報を共有または交換するために、Security Manager はデフォルトでポート 443 上の HTTPS を使用します。この目的で別のポートを使用するかどうかを選択できます。
2. Security Manager のインストールまたはアップグレード時に、Common Services syslog サービス ポートが 514 から 49514 に変更されます。あとで Security Manager がアンインストールされた場合、ポートは 514 に戻されません。

Security Manager サーバのトラブルシューティング

この項では、次の疑問にお答えします。

- 「インストール中のサーバ障害」（P.A-4）
- 「インストール後のサーバ障害」（P.A-5）
- 「アンインストール中のサーバ障害」（P.A-8）

インストール中のサーバ障害

Q. サーバ ソフトウェアのインストール時に表示されたこのインストール エラー メッセージはどういう意味ですか。

A. サーバ ソフトウェアのインストール エラー メッセージと説明を表 A-2（P.A-4）に示します。この表は先頭の文字のアルファベット順に並べられています。

表 A-2　インストール エラー メッセージ（サーバ）

メッセージ	メッセージの理由	ユーザ操作
`License file failed.ERROR: The file with the name c:¥progra~1¥CSCOpx¥setup does not exist`	先に Common Services 依存アプリケーションをアンインストールしようとして失敗しました。	1. サーバをシャットダウンしてから、再起動します。 2. レジストリ エディタを使用して次のエントリを削除します。 `$HKEY_LOCAL_MACHINE¥SOFTWARE¥Cisco¥Resource Manager¥CurrentVersion` 3. Security Manager をインストールしたディレクトリで、*setup* という名前のサブディレクトリを作成します。 4. CMFLOCK.TXT を削除します（存在する場合）。 5. Security Manager を再インストールします。
`Corrupt License file. Please enter a valid License file.`	ライセンス ファイルが破損しているか、ライセンス ファイルの内容が無効です。	「ライセンスに関する支援」（P.2-6）を参照してください。
`Corrupt License file entered for 5 tries. Install will proceed in EVAL mode. Press OK to proceed.`	5 回連続で無効なライセンス ファイルへのパス名を入力した可能性があります。試行が 5 回失敗したら、インストールが評価モードに変わります。	[OK] をクリックして、ライセンス エラー ダイアログ ボックスを閉じて、ウィザードの次の画面に進みます。
`One instance of CiscoWorks Installation is already running.If you are sure that no other instances are running, remove the file C:¥CMFLOCK.TXT.This installation will now abort.`	先に Common Services 依存アプリケーションをインストールしようとして失敗した可能性があります。	C:¥CMFLOCK.TXT ファイルを削除してから、もう一度試してみてください。

`Severe`
 	
`Failed on call to FileInsertLine.`
	サーバがハード ドライブ スペースに関する要件を満たしていません。	「サーバの要件および推奨事項」（P.3-3）を参照してください。

`Temporary directory used by installation has reached _istmp9x. If _istmp99 is reached, no more setups can be run on this computer, they fail with error -112.`	サーバ上で、ソフトウェア インストール中に自動的に削除される予定の一時ファイルが残っています。	サーバ上の一時ディレクトリで名前に「_istmp」文字列が含まれるサブディレクトリを探します。このようなサブディレクトリをすべて削除します。

表 A-2　インストール エラー メッセージ（サーバ）（続き）

メッセージ	メッセージの理由	ユーザ操作
Windows cannot find 'C:¥Documents and Settings¥Administrator¥WINDOWS¥System32¥cmd.exe'. Make sure you typed the name correctly, and then try again. To search for a file, click the Start button, and then click Search.	サポートされていないにもかかわらず、Terminal Services をインストール中にイネーブルにした可能性があります。「インストール準備状況チェックリスト」（P.4-3）を参照してください。	1. Terminal Services をディセーブルにします。 この手順については、次の URL にある『*Installing and Getting Started With CiscoWorks LAN Management Solution 3.1*』の「Terminal Server Support for Windows 2000 and Windows 2003 Server」トピックを参照してください。 http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_lan_management_solution/3.1/install/guide/IGSG31.html 2. Security Manager をもう一度インストールしてみてください。
Setup has detected that unInstallShield is in use. Close unInstallShield and restart setup. Error 432.	インストール中に Windows アカウント権限がチェックされます。CiscoWorks Common Services をインストールしている Windows アカウントがローカル管理者特権を持っていない場合は、InstallShield にこのエラー メッセージが表示されます。	1. %WINDIR% に書き込むための適切な権限が付与されていることを確認します。インストールまたはアンインストールは、ローカル管理者グループのメンバーが実施する必要があります。 2. [OK] をクリックしてエラー メッセージを閉じ、Windows からログアウトして、ローカル管理者特権を持つアカウントを使用して Windows に再ログインします。

Q. サーバ インストーラが処理を中断（ハングアップ）した場合はどうしたらいいですか。

A. リブートしてもう一度試してみてください。

Q. Cisco Security Manager と Cisco Secure Access Control Server の両方を 1 つのシステム上にインストールできますか。

A. インストールしないことを推奨します。同じサーバ上での Security Manager と Cisco Secure ACS for Windows の共存はサポートされていません。

Q. Security Manager データベースのバックアップが失敗するのはなぜですか。

A. Tivoli などのネットワーク管理アプリケーションを使用して、Security Manager がインストールされたシステム上に Cygwin をインストールした場合は、Security Manager データベースのバックアップに失敗します。Cygwin をアンインストールしてください。

インストール後のサーバ障害

Q. Security Manager インターフェイスが表示されない、または、正しく表示されない、あるいは、特定のインターフェイス要素が欠けています。原因は何でしょうか。

A. いくつかの可能性が考えられます。このリスト内のシナリオを参照して、インターフェイスに影響を与える可能性のある単純な問題を特定し、対処してください。

- 必要なサービスのいくつかがサーバ上で動作していません。サーバのデーモン マネージャを再起動して、すべてのサービスの起動が完了するのを待ってから、Security Manager クライアントを再起動して接続し直してみてください。
- サーバに十分な空きディスク スペースがありません。サーバ上の Security Manager パーティションの空き容量が 500 MB 以上あることを確認してください。

- 基本ライセンス ファイルが破損しています。「ライセンスに関する支援」（P.2-6）を参照してください。
- サーバで使用されている Windows 言語が間違っています。米国英語バージョンの Windows 上の英語と、日本語バージョンの Windows 上の日本語しかサポートされていません（「サーバの要件および推奨事項」（P.3-3）を参照）。他の言語はインストールされたバージョンの Security Manager に悪影響を与える可能性があります。また、GUI 要素の欠落は可能性のある症状の 1 つです。サポートされていない言語を使用している場合は、サポートされている言語を選択してから、Security Manager をアンインストールして再インストールしてください。「サーバ アプリケーションのアンインストール」（P.5-20）を参照してください。
- ネットワーク接続上で Security Manager インストール ユーティリティを実行しましたが、この使用方法はサポートされていません（「Security Manager サーバ、Common Services、および AUS のインストール」（P.5-3）を参照）。サーバ ソフトウェアをアンインストールして再インストールする必要があります。「サーバ アプリケーションのアンインストール」（P.5-20）を参照してください。
- クライアント システムが最小限の要件を満たしていません。「クライアントの要件」（P.3-9）を参照してください。
- HTTP を使用しようとしましたが、必要なプロトコルは HTTPS です。
- ボタンだけが表示されません。Security Manager クライアントを使用している最中に、クライアント システム上で [Display Properties] コントロール パネルを開いて、[Appearance] タブでいくつかの設定を変更した可能性があります。この問題に対処するには、Security Manager クライアントを終了してから、再起動してください。
- 間違ったグラフィックス カードのドライバ ソフトウェアがクライアント システム上にインストールされています。「クライアントの要件」（P.3-9）を参照してください。

問題　Web ブラウザを使用して Security Manager への Web インターフェイスを開こうとしたときに、Security Manager サーバ上の /cwhp/LiaisonServlet にアクセスするための権限がないことを伝えるメッセージが表示されました。これはどういう意味ですか。

ソリューション　下の表に、この問題の一般的原因と提案されている対処法を示します。

表 A-3　LiaisonServlet エラーの原因と対処法

原因	対処法
サーバ上にアンチウイルス アプリケーションがインストールされている	アンチウイルス アプリケーションをアンインストールします。
サーバ上に IIS がインストールされている	IIS は Security Manager と互換性がないため、アンインストールする必要があります。

表 A-3　LiaisonServlet エラーの原因と対処法 （続き）

原因	対処法
Security Manager に必要なサービスが正しい順序で開始されていない	自動に設定する必要があるサービスは Cisco Security Manager Daemon Manager だけです。他の CiscoWorks サービスは手動に設定する必要があります。Daemon Manager が他の Ciscoworks サービスを起動するまでに数分かかる場合があることに注意してください。これらのサービスは、正しい順序で起動する必要があります。手動でサービスを起動した場合はエラーを引き起こす可能性があります。
casuser パスワード	casuser ログインは、Windows 管理者と同じで、すべての Common Services タスクと Security Manager タスクにアクセスできます。次のように casuser パスワードをリセットします。 1. サーバ上でコマンド プロンプトを開きます。 （注） Windows Server 2008 を使用している場合は、コマンド プロンプトを開くときに [Run as administrator] オプションを使用する必要があります。 2. `C:¥Program Files¥CSCOpx¥setup¥support¥resetCasuser.exe` と入力して、Enter を押します。 3. オプション 1（casuser パスワードのランダム生成）を選択します。

Q. Security Manager を使用してサーバ上のディレクトリを参照したときに、ローカル ボリュームだけが表示され、マップされたドライブは表示されません。どうしてですか。

A. Microsoft はサーバ セキュリティを強化するために Windows の設計にこの機能を組み込みました。Security Manager で選択する必要のあるすべてのファイル（ライセンス ファイルなど）をサーバ上に配置する必要があります。

Q. 日本語バージョンの Windows の [Start] メニューに Security Manager が表示されないのはなぜですか。

A. サーバ上の地域と言語のオプションを、英語を使用するように設定した可能性があります。日本語バージョンの Windows 内の言語として英語はサポートされていません（「サーバの要件および推奨事項」（P.3-3）を参照）。コントロール パネルを使用して、言語を日本語にリセットしてください。

Q. サーバの SSL 証明書が無効になっています。また、DCRServer プロセスが開始しません。原因は何でしょうか。

A. サーバの日付または時刻が SSL 証明書の有効範囲外にリセットされています。「インストール準備状況チェックリスト」（P.4-3）を参照してください。この問題に対処するには、サーバの日付 / 時刻の設定をリセットしてください。

Q. サーバとクライアント間の通信に使用されるプロトコルの入力が要求されませんでした。デフォルトで使用されるプロトコルは何ですか。他のモードを使用してこの設定を手動で変更する必要がありますか。

A. サーバのインストール中にクライアントをインストールした場合は、デフォルトで、サーバとクライアント間の通信プロトコルとして HTTPS が使用されます。通信はデフォルト プロトコルを使用して保証されているため、この設定を手動で変更する必要はありません。

プロトコルとして HTTP を選択するオプションは、サーバ インストーラとは別に、クライアント インストーラを実行して Security Manager クライアントをインストールした場合にのみ使用できます。ただし、サーバとクライアント間の通信プロトコルとして HTTP を使用しないことを推奨します。クライアントは、サーバが使用するように設定されたプロトコルを使用する必要があります。

Q. VMware セットアップを使用しているとシステムのパフォーマンスが受け入れられないほど低下します。たとえば、システムのバックアップに 2 時間もかかります。

A. Security Manager を実行している VM に複数の CPU が割り当てられていることを確認してください。1 つの CPU しか割り当てられていないシステムでは、一部のシステム アクティビティに対して受け入れられないほどのパフォーマンスを示すことがわかっています。

Q. 検証などのいくつかの操作が、SQL クエリー例外をログに出力して失敗します。原因は何でしょうか。

A. Sybase の一時ディレクトリのディスク領域が足りなくなり、一時ファイルの作成に失敗した可能性があります。デフォルトでは、Windows の一時ディレクトリの下に Sybase の一時ファイルが作成されます。システム変数 SA_TMP が定義されている場合は、SA_TMP に指定されたディレクトリに一時ファイルが作成されます。Sybase の一時ファイルが配置されるディスク領域をクリアしてから、Security Manager を再起動します。

アンインストール中のサーバ障害

Q. このアンインストール エラー メッセージはどういう意味ですか。

A. アンインストール エラー メッセージと説明を表 A-4（P.A-8）に示します。この表は先頭の文字のアルファベット順に並べられています。アンインストール エラー メッセージの詳細については、Cisco.com 上で Common Services 3.2 のマニュアルを参照してください。

表 A-4　アンインストール エラー メッセージ

メッセージ	メッセージの理由	ユーザ操作
C:¥*NMSROOT*¥MDC¥msfc-backend refers to a location that is unavailable. It could be on a hard drive on this computer, or on a network. Check to make sure that the disk is properly inserted, or that you are connected to the Internet or your network, and then try again. If it still cannot be located, the information might have been moved to a different location.	このメッセージは害がない可能性があります。[OK] をクリックしてメッセージを消去する以外は何もする必要がありません。そうしなかった場合は、次の条件の一方または両方が適用されるサーバ上でメッセージが表示される可能性があります。 - 簡易ファイル共有が Windows 上でイネーブルになっている。 - オフライン ファイル同期が Windows 上でイネーブルになっている。	メッセージを消去してアンインストールが失敗した場合は、次の可能性のある対処法の一方または両方を試して、もう一度アンインストールを行ってみてください。 **簡易ファイル共有** 1. [Start] > [Settings] > [Control Panel] > [Folder Options] を選択します。 2. [View] タブをクリックします。 3. [Advanced Settings] ペインの一番下までスクロールします。 4. [Use simple file sharing (Recommended)] チェックボックスをオフにしてから、[OK] をクリックします。 **オフライン ファイル同期** 1. [Start] > [Settings] > [Control Panel] > [Folder Options] を選択します。 2. [Offline Files] タブをクリックします。 3. [Enable Offline Files] チェックボックスをオフにしてから、[OK] をクリックします。

表 A-4　アンインストール エラー メッセージ （続き）

メッセージ	メッセージの理由	ユーザ操作
C:¥temp¥<*subdirectory*>¥ setup.exe - Access is denied. The process cannot access the file because it is being used by another process. 0 file(s) copied. 1 file(s) copied.	アンインストールが失敗しました。	サーバをリブートしてから、「サーバ アプリケーションのアンインストール」（P.5-20）に記載されている手順を実行してください。
Windows Management Instrumentation (WMI) is running. The setup program has detected Windows Management Instrumentation (WMI) services running. This will lock some Cisco Security Manager processes and may abort uninstallation abruptly. To avoid this, uninstallation will stop and start the WMI services. Do you want to proceed? Click Yes to proceed with this uninstallation. Click No to exit uninstallation.	組織で WMI が使用されているか、誰かが誤ってサーバ上の WMI サービスをイネーブルにした可能性があります。	[Yes] をクリックします。

Q. アンインストーラがハングアップした場合はどうしたらいいですか。

A. リブートしてからもう一度試してみてください。

Q. アンインストーラに *crmdmgtd* サービスが応答していないという内容のメッセージが表示され、「Do you want to keep waiting?」と尋ねられた場合はどうしたらいいですか。

A. アンインストール スクリプトには、スクリプトがタイムアウトする前に命令に応答しなかった crmdmgtd サービスを停止する命令が含まれています。[Yes] をクリックします。ほとんどの場合、crmdmgtd サービスは、その後、予想どおりに停止します。

Security Manager クライアントのトラブルシューティング

この項では、次の疑問にお答えします。

- 「インストール中のクライアント障害」（P.A-9）
- 「インストール後のクライアント障害」（P.A-12）

インストール中のクライアント障害

Q. クライアント ソフトウェアのインストール時に表示されたこのインストール エラー メッセージはどういう意味ですか。

A. クライアント ソフトウェアのインストール エラー メッセージと説明を表 A-5 に示します。この表は先頭の文字のアルファベット順に並べられています。

表 A-5　インストール エラー メッセージ（クライアント）

メッセージ	メッセージの理由	ユーザ操作
`Could not install engine jar`	以前のソフトウェア インストールとアンインストールが原因で InstallShield が正しく動作していません。	1. 次のとおりに移動します。**C:¥Program Files¥Common Files¥InstallShield¥Universal¥common¥Gen1**. 2. Gen1 フォルダの名前を変更してから、もう一度 Security Manager クライアントのインストールを試してみてください。 Gen1 が存在しない場合は、代わりに **common** の名前を変更します。

`Error - Cannot Connect to Server`
 	
`The client cannot connect to the server. This can be caused by one of the following reasons:`
`The server name is incorrect.`
`The protocol (http, https) is incorrect.`
`The server is not running.`
`Network access issues. Please confirm that the server name and protocol are correct.`
`The server is running and you are not experiencing network connectivity issues by loading the CS Manager home page in your browser.`
	サーバが誤って HTTPS トラフィック用に設定されている可能性があります。	1. ブラウザから、**https://**<*server*>**/CSCOnm/servlet/login/login.jsp** にある Cisco Security Management Suite デスクトップにログインします。
		2. [Server Administration] をクリックします。
		3. [Admin] ウィンドウで、[Server] > [Security] を選択します。
		4. TOC で、[Single Server Management] > [Browser-Server Security Mode Setup] を選択してから、[Enable] オプション ボタンが選択されていることを確認します。
		オプション ボタンが選択されていなかった場合は、それを選択してから、[Apply] をクリックします。
		5. プロンプトが表示されたら、Cisco Security Manager Daemon Manager を再起動します。
		6. 5 分待ってから、もう一度 Security Manager クライアントを使用してみてください。
		それでも接続できない場合は、エラー メッセージが示している他の可能性のある問題を検討してください。

`Error - Cisco Security Agent Running`
 	
`Installation cannot proceed while the Cisco Security Agent is running`
 	
`Do you want to disable the Cisco Security Agent and continue with the installation?`
	クライアントのインストール中は、Cisco Security Agent を停止する必要があります。	• Cisco Security Agent をディセーブルにする場合は、[Yes] をクリックします。
		• 操作をキャンセルして、Cisco Security Agent を手動で停止する場合は、[No] をクリックします。
		• Security Manager クライアントのオンライン ヘルプにアクセスする場合は、[Help] をクリックします。

表 A-5　インストール エラー メッセージ（クライアント）（続き）

メッセージ	メッセージの理由	ユーザ操作
Error - Cisco Security Agent not Stopped The installation will be aborted because the Cisco Security Agent could not be stopped. Please attempt to disable Cisco Security Agent before repeating the installation process.	Security Manager クライアントから Cisco Security Agent を停止できませんでした。	[OK] をクリックして、このエラー メッセージを閉じ、インストールを中断します。もう一度インストールを試す前に、Cisco Security Agent を手動でディセーブルにします。
Error occurred during the installation: null.	以前のソフトウェア インストールとアンインストールが原因で InstallShield が正しく動作していません。	1. C:¥Program Files¥Common Files¥InstallShield¥Universal¥common¥Gen1 に移動します。 2. Gen1 フォルダの名前を変更してから、もう一度 Security Manager クライアントのインストールを試してみてください。 Gen1 が存在しない場合は、代わりに **common** の名前を変更します。
Errors occurred during the installation. • null	ログイン アカウントに管理特権が付与されている Windows ユーザだけが、Security Manager Client をインストールできます。	Windows 管理者としてログインしてから、もう一度 Security Manager クライアントのインストールを試してみてください。
Internet Explorer cannot download CSMClientSetup.exe from <*server*>. Internet Explorer was not able to open this Internet site. The requested site is either unavailable or cannot be found. Please try again later.	クライアント システム上の OS が Windows 2008 の場合は、Internet Explorer セキュリティ強化のデフォルト設定が原因で、サーバからクライアント ソフトウェア インストール ユーティリティをダウンロードできない可能性があります。	1. [Start] > [Control Panel] > [Add or Remove Programs] を選択します。 2. [Add/Remove Windows Components] をクリックします。 3. Windows コンポーネント ウィザード ウィンドウが開いたら、[Internet Explorer Enhanced Security Configuration] チェックボックスをオフにして、[Next] をクリックし、[Finish] をクリックします。
Please read the information below. The following errors were generated: • WARNING: The <*drive*> partition has insufficient space to install the items selected.	空きスペースが不十分なドライブまたはパーティション上に Security Manager クライアントをインストールしようとした可能性があります。	[Back] をクリックしてから、Security Manager クライアントをインストールする別の場所を選択してください。
Unable to Get Data A database failure prevented successful completion of this operation.	サーバ データベースが完全に稼動する前に、クライアントを使用してサーバに接続しようとした可能性があります。	数分待ってから、もう一度ログインしてみてください。問題が解決されない場合は、必要なすべてのサービスが実行していることを確認してください。

Q. クライアント インストーラが処理を中断（ハングアップ）した場合はどうしたらいいですか。

A. 次の手順を試してみてください。いずれかの手順で問題が解決される可能性があります。

- クライアント システム上にアンチウイルス ソフトウェアがインストールされている場合は、それをディセーブルにしてから、もう一度インストーラを実行してみてください。
- クライアント システムをリブートしてから、もう一度インストーラを実行してみてください。
- クライアント システム上でブラウザを使用して、**http://**<*server_name*>**:1741** にある Security Manager サーバにログインします。「Forbidden」または「Internal Server Error」というエラー メッセージが表示された場合は、必要な Tomcat サービスが実行していません。最近サーバをリブートして、Tomcat の稼動までに十分な時間がなかったことがない場合は、サーバ ログを確認するか、その他のステップを実行して、Tomcat が動作していない理由を調査する必要があります。

Q. インストーラに、以前のバージョンのクライアントがインストールされているためアンインストールされるという内容のメッセージが表示されます。しかし、以前のバージョンのクライアントはインストールされていません。これは障害ですか。

A. クライアントのインストールまたは再インストール中に、インストーラがインストールされていないクライアントを検出して、そのクライアントがアンインストールされるという内容の誤ったメッセージを表示することがあります。このメッセージは、システム内に特定の古いレジストリ エントリが残っていることが原因で表示されます。このメッセージが表示されてもクライアントのインストールは正常に進行しますが、レジストリ エディタを使用して次のキーを削除して、今後のインストールでこのメッセージが表示されないようにします。HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Uninstall¥Cisco Security Manager Client（レジストリ エディタを開くには、[Start] > [Run] を選択して **regedit** と入力します）。また、C:¥Program Files¥Zero G Registry¥.com.zerog.registry.xml ファイルの名前を変更します（どんな名前でも可）。

インストール後のクライアント障害

Q. インターフェイスが正しく表示されないのはなぜですか。

A. 古いビデオ（グラフィックス）カードは、ドライバ ソフトウェアをアップグレードしなければ、Security Manager GUI を正しく表示しない可能性があります。この問題がクライアント システムに影響するかどうかをテストするには、[My Computer] を右クリックして、[Properties] を選択し、[Hardware] を選択して、[Device Manager] をクリックしてから、[Display adapters] エントリを展開します。アダプタのエントリをダブルクリックして、使用されているドライバのバージョンを確認します。その後で、次のいずれかを実行できます。

- クライアント システムで ATI MOBILITY FireGL ビデオ カードが使用されている場合は、カードに付属していたビデオ ドライバ以外のドライバを入手しなければならない場合があります。使用するドライバは、手動で Direct 3D が設定できる必要があります。このような機能のないドライバは、Security Manager GUI 内の要素をクライアント システムに表示できない可能性があります。
- ビデオ カードの場合は、PC メーカとカード メーカの Web サイトにアクセスして、最新の Java2 グラフィックス ライブラリの表示との非互換性をチェックしてください。既知の非互換性が残っているほとんどのケースで、半分以上のメーカが互換性のあるドライバを入手してインストールするための手段を提供しています。

Q. 日本語バージョンの Windows の [Start] メニューに Security Manager クライアントが表示されないのはなぜですか。

A. クライアント システム上で英語を使用するように、地域と言語のオプションを設定している可能性があります。日本語バージョンの Windows 内の言語として英語はサポートされていません。コントロール パネルを使用して、言語を日本語にリセットしてください。

Q. Security Manager クライアントがインストールされたワークステーション上で一部または全部のユーザの [Start] メニューに Security Manager クライアントが表示されないのはなぜですか。

A. クライアントをインストールするときに、製品をインストールしているユーザ専用のショートカットを作成するのか、すべてのユーザ用のショートカットを作成するのか、どのユーザ用のショートカットも作成しないのかを選択します。インストール後にこの選択を変更する場合は、Cisco Security Manager Client フォルダを Documents and Settings¥<user>¥Start Menu¥Programs¥Cisco Security Manager から Documents and Settings¥All Users¥Start Menu¥Programs¥Cisco Security Manager にコピーすることによって、手動で変更できます。ショートカットを作成しないことにした場合は、指定された All Users フォルダ内にショートカットを手動で作成する必要があります。

Q. クライアント システムとサーバ間の接続が異常に遅いと感じる場合、または、ログイン時に DNS エラーが表示される場合はどうしたらいいですか。

A. クライアント システム上の **hosts** ファイル内に Security Manager サーバ用のエントリを作成しなければならない場合があります。このようなエントリは、ネットワーク用の DNS サーバに登録されていない場合にサーバへの接続の確立に役立つ可能性があります。クライアント システム上でこの有効なエントリを作成するには、メモ帳またはその他のプレーン テキスト エディタを使用して、C:¥WINDOWS¥system32¥drivers¥etc¥hosts を開きます（ホスト ファイル自体にエントリの追加方法に関する詳細な手順が保存されています）。

Q. Security Manager クライアントを使用してログインしようとしたときにエラー メッセージが表示されることなくログイン資格情報が受け入れられましたが、Security Manager デスクトップが空の状態で使用できません。認証セットアップの何が間違っているのでしょうか（また、Security Manager サーバ上の Common Services でログイン資格情報が受け入れられましたが、Web ブラウザ上で Cisco Security Management Suite デスクトップのロードに失敗します。これも同じ原因でしょうか）。

A. Security Manager と Common Services に対してログイン認証サービスを提供するための Cisco Secure ACS に必要なステップが完了していない可能性があります。ACS でログイン資格情報を入力しましたが、Security Manager サーバを AAA クライアントとして定義していません。この定義を行わなければ、ログインできません。詳しい手順については、ACS のマニュアルを参照してください。

Q. Security Manager クライアントを使用してサーバにログインできず、次のようなメッセージが表示されます。どうしたらいいですか。

... repeatedly that the server is checking its license.	サーバが最小限のハードウェア要件とソフトウェア要件を満たしていることを確認してください。「サーバの要件および推奨事項」（P.3-3）を参照してください。

`Synchronizing with DCR.`	2 通りの可能性が考えられます。 • サーバの再起動直後に Security Manager クライアントを起動した可能性があります。その場合は、サーバが完全に使用可能になるまで数分待ってから、Security Manager クライアントを使用してみてください。 • CiscoWorks 管理パスワードにアンパサンド（&）などの特殊文字が含まれている可能性があります。その結果、Security Manager のインストール時にサーバ上の *NMSROOT*¥lib¥classpath サブディレクトリで comUser.dat ファイルを作成できませんでした。ここで、*NMSROOT* は Common Services をインストールしたディレクトリです（デフォルトは C:¥Program Files¥CSCOpx です）。 **a.** Cisco TAC に連絡して、**comUser.dat** の交換または Security Manager の再インストールに関する支援を要請してください。 **b.** または、特殊文字を含まない Common Services パスワードを作成します。

`Error - Unable to Check License on Server.`
 	
`An attempt to check the license file on the Security Manager server has failed.`
 	
`Please confirm that the server is running. If the server is running, please contact the Cisco Technical Assistance Center.`
	次のサービスのいずれかが正しく起動していない可能性があります。サーバ上で、[Start] > [Programs] > [Administrative Tools] > [Services] を選択して、次のような名前のサービスを右クリックし、ショートカット メニューから [Restart] を選択します。
	• Cisco Security Manager Daemon Manager
	• Cisco Security Manager database engine
	• Cisco Security Manager Tomcat Servlet Engine
	• Cisco Security Manager VisiBroker Smart Agent
	• Cisco Security Manager Web Engine
	5 分待ってから、もう一度 Security Manager クライアントを起動してみてください。

Q. デフォルト ブラウザとして Internet Explorer を使用しているときにアクティビティ レポートが表示されないのはなぜですか。

A. この問題は、無効なレジストリ キー値、または Internet Explorer に関連付けられた DLL ファイルの場所に関する間違いが原因で発生します。この問題の対処法については、http://support.microsoft.com/kb/281679/EN-US から入手可能な Microsoft サポート技術情報の記事 281679 を参照してください。

Q. どうすれば、ログイン ウィンドウの [Server Name] フィールドからサーバ リストを消去できますか。

A. csmserver.txt を編集して必要のないエントリを削除します。このファイルは、Security Manager クライアントをインストールしたディレクトリ内にあります。デフォルトの場所は、C:¥Program Files¥Cisco Systems¥Cisco Security Manager Client です。

Q. バージョン ミスマッチが原因で Security Manager クライアントがロードされなかった可能性があります。これはどういう意味ですか。

A. Security Manager サーバのバージョンとクライアントのバージョンが一致していません。これを修正するには、最新のクライアント インストーラをサーバからダウンロードしてインストールします。

Q. クライアント ログ ファイルはどの場所にありますか。

A. クライアント ログ ファイルは、C:¥Program Files¥Cisco Systems¥Cisco Security Manager Client¥logs に配置されています。GUI セッションごとに専用のログ ファイルが作成されます。

Q. Security Manager が HTTPS モードで動作中かどうかはどうすれば確認できますか。

A. 次のいずれかを実行します。

- ブラウザを使用してサーバにログインしたら、アドレス フィールド内の URL を調査します。URL が https で始まっていれば、Security Manager が HTTPS モードで動作しています。
- [Common Services] > [Server] > [Security] > [Single Server Management] > [Browser-Server Security Mode Setup] に移動します。[Current Setting] が [Enabled] になっていれば、Security Manager が HTTPS モードで動作しています。この設定が [Disabled] の場合は、HTTP を使用します。
- クライアントを使用してログインするときに、まず、HTTPS モードを試してみてください（[HTTPS] チェックボックスをオンにします）。「Login URL access is forbidden; Please make sure your protocol (HTTP, HTTPS) is correct」というメッセージが表示されたら、サーバは HTTP モードで動作している可能性があります。[HTTPS] チェックボックスをオフにして、もう一度試してみてください。

Q. どうすれば、クライアント デバッグ ログ レベルをイネーブルにできますか。

A. デフォルトで C:¥Program Files¥Cisco Systems¥Cisco Security Manager Client¥jars に配置されている client.info ファイル内で、DEBUG_LEVEL パラメータに DEBUG_LEVEL=ALL を追加してから、Security Manager クライアントを再起動します。

Q. 2 画面構成で作業している場合は、Security Manager クライアントが第 2 画面上で動作していても、必ず、特定のウィンドウとポップアップ メッセージが第 1 画面に表示されます。たとえば、クライアントが第 2 画面上で動作しているときに、必ず、Policy Object Manager などのウィンドウが第 1 画面に表示されます。これを修正できますか。

A. これは、特定のオペレーティング システムにおける 2 画面サポートの実装方法に伴う既知の問題です。Security Manager クライアントを第 1 画面上で動作させることを推奨します。クライアントは、2 画面構成の設定後に起動する必要があります。

他の画面でウィンドウが開いた場合は、Alt + スペースバーを押した後に M を押すことによってそのウィンドウを移動できます。その後で、矢印キーを使用してウィンドウを移動します。

Q. クライアント システム上でソフトウェアをインストールまたはアンインストールできません。どうしてですか。

A. クライアント システム上でインストールとアンインストールを*同時に*実行した場合は、それらが別々のアプリケーションに対するものであっても、クライアント システムの InstallShield データベース エンジンに悪影響を与え、ソフトウェアのインストールまたはアンインストールができなくなります。詳細については、Cisco.com アカウントにログインしてから、Bug Toolkit を使用して CSCsd21722 と CSCsc91430 を確認してください。

サーバ セルフテストの実行

Security Manager サーバが正しく動作していることを確認するセルフテストを実行するには、次の手順を実行します。

ステップ 1　Security Manager クライアントが Security Manager サーバに接続されているシステムから、[Tools] > [Security Manager Administration] を選択します。

ステップ 2　[Administration] ウィンドウで、[Server Security] をクリックしてから、任意のボタンをクリックします。新しいブラウザが開いて、クリックしたボタンに対応する Common Services GUI のセキュリティ設定ページが表示されます。

ステップ 3　[Common Services] ページの [Server] タブで、[Admin] を選択します。

ステップ 4　[Admin] ページの TOC で、[Selftest] をクリックします。

ステップ 5　[Create] をクリックします。

ステップ 6　[SelfTest Information at <*MM-DD-YYYY HH:MM:SS*>] リンクをクリックします。ここで、

- *MM-DD-YYYY* は、現在の月、日、年です。
- *HH:MM:SS* は、[Selftest] をクリックした時、分、秒を表すタイムスタンプです。

ステップ 7　[Server Info] ページでエントリを読み取ります。

サーバ トラブルシューティング情報の収集

Security Manager で問題が発生しており、エラー メッセージ内の推奨事項のすべてを試し、このマニュアル内の可能性のある解決策を確認したにもかかわらず、問題が解決されない場合は、Security Manager Diagnostics ユーティリティを使用してサーバ情報を収集します。

Security Manager Diagnostics ユーティリティは、ZIP ファイルの CSMDiagnostics.zip からサーバ診断情報を収集します。このファイル名を変更しなかった場合は、Security Manager Diagnostics を実行するたびに新しい情報でファイルが上書きされます。CSMDiagnostics.zip ファイル内の情報は、サーバ上の Security Manager または関連アプリケーションで発生した問題のシスコ テクニカルサポート エンジニアによる解決を支援します。

ヒント　Security Manager には、アプリケーションによって実施された設定変更に関する情報を収集する高度なデバッギング オプションも用意されています。このオプションをアクティブにするには、[Tools] > [Security Manager Administration] > [Debug Options] を選択してから、[Capture Discovery/Deployment Debugging Snapshots to File] チェックボックスをオンにします。診断ファイルに保存されたその他の情報はトラブルシューティングの試みに役立つ可能性がありますが、ファイルにはパスワードなどの機密情報が書き込まれている場合があることに注意してください。デバッグ レベルは、Cisco Technical Assistance Center（TAC）から変更を指示された場合にだけ変更してください。

Security Manager Diagnostics は次のいずれかの方法で実行できます。

Security Manager クライアント システムから	Security Manager サーバから
1. サーバへの Security Manager クライアント セッションを確立したら、[Tools] > [Security Manager Diagnostics] をクリックして [OK] をクリックします。 CSMDiagnostics.zip ファイルは、サーバ上の *NMSROOT*¥MDC¥etc¥ ディレクトリに保存されます。ここで、*NMSROOT* は、Common Services をインストールしたディレクトリです（C:¥Program Files¥CSCOpx など）。 2. [Close] をクリックします。 （注）　このユーティリティを実行するたびに上書きされないようにこのファイルの名前を変更することを推奨します。	1. Windows のコマンド ウィンドウを開きます。それには、たとえば [Start] > [Run] を選択し、**command** と入力します。 2. 次のように入力します。**C:¥Program Files¥CSCOpx¥MDC¥bin¥CSMDiagnostics**。または、この ZIP ファイルを *NMSROOT*¥MDC¥etc¥ とは別の場所に保存するには、**CSMDiagnostics** *drive:¥path* と入力します。たとえば、CSMDiagnostics D:¥temp と入力します。

サーバ プロセス ステータスの表示と変更

Security Manager のサーバ プロセスが正しく動作していることを確認するには、次の手順を実行します。

ステップ 1　CiscoWorks のホームページで、[Common Services] > [Server] > [Admin] を選択します。

ステップ 2　[Admin] ページの TOC で、[Processes] をクリックします。

[Process Management] テーブルにすべてのサーバ プロセスが表示されます。[ProcessState] カラム内のエントリが、プロセスが正常に動作しているかどうかを示します。

ステップ 3　必要なプロセスが動作していない場合は、それを再起動します。「サーバ上の全プロセスの再起動」（P.A-17）を参照してください。

（注）　ローカル管理者特権を持つユーザのみがサーバ プロセスを起動または停止できます。

サーバ上の全プロセスの再起動

（注）　すべてのプロセスを停止してから、それらを再起動しなければ、この方法は機能しません。

ステップ 1　コマンド プロンプトで、**net stop crmdmgtd** と入力してすべてのプロセスを停止します。

ステップ 2　**net start crmdmgtd** と入力してすべてのプロセスを再起動します。

ヒント　または、[Start] > [Settings] > [Control Panel] > [Administrative Tools] > [Services] を選択してから、Cisco Security Manager Daemon Manager を再起動できます。

サーバ インストール ログ ファイルの確認

サーバからの応答が期待していたものと違っていた場合は、サーバ インストール ログ ファイルでエラー メッセージと警告メッセージを確認できます。

テキスト エディタを使用して **C:¥Ciscoworks_install_*NNN*.log** を開きます。ここで、*NNN* は YYYYMMDD_HHMMSS 形式のタイムスタンプです。

ほとんどの場合、確認すべきログ ファイルは、ファイル名に最大の番号が付けられたファイルか、作成日が最新のファイルです。

たとえば、ログ ファイルでは、次のようなエラー エントリと警告エントリが確認できます。

```
ERROR: Cannot Open C:¥PROGRA~1¥CSCOpx/lib/classpath/ssl.properties at
C:¥PROGRA~1¥CSCOpx¥MDC¥Apache¥ConfigSSL.pl line 259.
INFO: Enabling SSL....
WARNING: Unable to enable SSL. Please try later....
```

（注） 重大な問題が発生した場合は、ログ ファイルを Cisco TAC に送信できます。「マニュアルの入手方法およびテクニカル サポート」（P.xii）を参照してください。