APPENDIX **B**

同梱 Cisco Security Agent：概要

Cisco Security Agent は、ホストベースの侵入防御を提供します。Security Manager に関して、Cisco Security Agent には、外部と同梱の 2 つのバージョンがあります。

- 外部 Cisco Security Agent：Cisco Security Manager インストールの一部としてインストールされない Cisco Security Agent
- 同梱 Cisco Security Agent：Cisco Security Manager インストールの一部としてインストールされる Cisco Security Agent。同梱 Cisco Security Agent は、「カスタマイズされたスタンドアロン エージェント」と呼ばれることがあります。これは、このエージェントが Security Manager 用にカスタマイズされており、Management Center for Cisco Security Agents がインストールされない、つまり、スタンドアロンであるためです。

この付録では、Security Manager サーバ上に頻繁にインストールされる同梱バージョンの Cisco Security Agent について説明します。

- Cisco Security Agent の一般的なユーザ マニュアルは、Cisco.com の http://www.cisco.com/en/US/products/sw/secursw/ps5057/tsd_products_support_series_home.html にあります。ただし、サーバ上の同梱エージェントは、Security Manager 用にカスタマイズされています。同梱エージェントは設定できないことと、Management Center for Cisco Security Agents がインストールされていないことから、Management Center for Cisco Security Agents のマニュアルには該当しない情報が記載されています。
- スタンドアロン エージェントで発生する可能性のある問題を理解して対処するには、「同梱 Cisco Security Agent のトラブルシューティング」（P.A-16）を参照してください。

この付録は、主に、次の内容で構成されています。

基本

Security Manager のインストールを開始したときに、ターゲット サーバが外部 Cisco Security Agent で保護されていなかった場合は、特定の条件下で Security Manager が変更不可能な事前定義のポリシーを使用して、同梱 Cisco Security Agent をインストールします。「Cisco Security Agent」（P.1-3）を参照してください。

注意 外部 Cisco Security Agent（Cisco Security Manager インストールの一部としてインストールされない Cisco Security Agent）がサーバ マシン上にインストールされている場合は、Cisco Security Manager が期待どおりに動作しない可能性があります。

インストール後に、同梱 Cisco Security Agent は、特定のシステム処理を許可または拒否するポリシーを使用してシステムの動作を制御します。このエージェントは、システム リソースがアクセスされ、動作しなくなる前に、処理が許可されたのか、拒否されたのかをチェックします。また、このエージェントは、禁止されたまたは予期せぬシステム動作が検出されるまで、日常業務を妨げることはありません。しかし、そのルールは、ルートキットなどの悪質なソフトウェアからサーバを保護するように作られているため、非常に厳密です。

同梱 Cisco Security Agent は、Security Manager 固有のポリシーと Windows のベースライン ポリシーを組み合わせて使用します。Windows のベースライン ポリシーについては、Cisco.com アカウントにログインしてから、http://www.cisco.com/cgi-bin/Software/Tablebuild/doftp.pl?ftpfile=cisco/crypto/3DES/cw2000/csa/fcs-csamc-4.5.1.616-CSA-Policy-Descriptions.zip&app=Tablebuild&status=showC2A にアクセスしてください。

（注） Cisco Security Agent が有効な操作をブロックしていると思われる場合は、Cisco TAC にお問い合わせください。「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。

エージェント ログ ファイル

スタンドアロン エージェント用の次のログ ファイルが、C:¥Program Files¥Cisco Systems¥CSAgent¥log subdirectory に保存されています。

CSAgent-Install.log	インストール ログ ファイル
csalog.txt	一般的なログ ファイル
securitylog.txt	セキュリティ イベント ログ ファイル

セキュリティ レベル設定の理解と管理

セキュリティ レベル設定は、サーバ システム トレイ内のエージェント アイコンを右クリックすることによって、いつでも変更できます。セキュリティ レベル設定によって、エージェントが [high]、[medium]、または [low] のセキュリティ制限をサーバに課すかどうか、または、何の制限も課さないかが決定されます。デフォルトは [medium] です。選択したレベルに応じて、セキュリティと利便性のバランスが異なります。

エージェント セキュリティ レベルを [high] に設定した場合は、Security Manager と Common Services が使用している特定のポートを除く、すべての UDP ポートまたは TCP ポート上のインバウンド接続がサーバから拒否されます。加えて、レベルが [high] で、エージェントが信頼できないルートキットを検出した場合は、すべての接続（インバウンドとアウトバウンド）がブロックされます。

同梱 Cisco Security Agent のアンインストール

エージェントが課したすべての制限を解除するプロセスで同梱 Cisco Security Agent をアンインストールできますが、サーバは非常に脆弱になり、エージェントがインストールされていたときと比べて攻撃されやすくなります。Cisco Security Agent のアンインストールは推奨できません。

一時的な代替手段として、サーバのシステム トレイ内のエージェント アイコンを右クリックしてから、より低いセキュリティ レベル設定を選択するか、スタンドアロン エージェントを一時的にディセーブルにするオプションを選択できます。

同梱 Cisco Security Agent をリセットして、ルートキット検出ステータスをクリアするという代替手段もあります。エージェントをリセットするには、[Start] > [Programs] > [Cisco Systems] > [Cisco Security Agent] > [Reset Cisco Security Agent] を選択します。

同梱 Cisco Security Agent をアンインストールするには、[Start] > [Programs] > [Cisco Security Agent] > [Uninstall Cisco Security Agent] を選択します。この方法によるアンインストールの場合はシステムを再起動する必要があります。

アンクリーン状態にあるエージェントのクリーンアップ

Security Manager のアップグレード中に、アンインストールしたつもりの Cisco Security Agent が稼動しているのを発見する場合があります。

Cisco Security Agent をアンインストールできない場合は、Cisco Security Agent サービスを停止してみてください。

- Cisco Security Agent サービスを停止できる場合は、「標準的なクリーンアップ手順」（P.B-3）に従います。
- Cisco Security Agent サービスを停止できない場合は、「特殊なクリーンアップ手順」（P.B-3）に従います。

標準的なクリーンアップ手順

Cisco Security Agent はアンインストールできないが、Cisco Security Agent サービスは停止できる場合は、次の手順に従うと、標準的なクリーンアップを使用した Cisco Security Agent のアンインストールを実行できます。

ステップ 1　[Add/Remove Programs] から Cisco Security Agent を削除します。

[Add/Remove Programs] から CSagent を削除しようとして、CSAgent は削除できないというエラーが表示された場合は、[Add/Remove Programs] から Cisco Security Agent を削除する前に、regedit で CSAgent エントリを削除する必要があります。「特殊なクリーンアップ手順」（P.B-3）を参照してください。

ステップ 2　[Start] > [All Programs] から Cisco Security Agent を削除します。

ステップ 3　C:¥Program Files¥Cisco Systems から CSAgent フォルダを手動で削除します。

ステップ 4　レジストリを探して、「CSAgent」と「Cisco Security Agent」という文字列のすべてのエントリを削除します。レジストリにアクセスするには、[Start] > [Run] を選択します。[Open] フィールドに **regedit** と入力してから、[Open] をクリックします。

ステップ 5　サーバを再起動します。

特殊なクリーンアップ手順

Cisco Security Agent をアンインストールできないうえ、Cisco Security Agent サービスも停止できない場合は、次の手順に従うと、特殊なクリーンアップを使用した Cisco Security Agent のアンインストールを実行できます。

ステップ 1　レジストリを探して、「CSAgent」と「Cisco Security Agent」という文字列のすべてのエントリを削除します。レジストリにアクセスするには、[Start] > [Run] を選択します。[Open] フィールドに **regedit** と入力してから、[Open] をクリックします。

ステップ 2　[Start] > [All Programs] から Cisco Security Agent を削除します。

ステップ 3　[Add/Remove Programs] から Cisco Security Agent を削除します。

ステップ 4　C:¥Program Files¥Cisco Systems から CSAgent フォルダを手動で削除します。

ステップ 5　サーバを再起動します。

CSAgent バージョン 5.2.0.282 の手動削除

[Add/Remove Programs] を使用して CSAgent をアンインストールできない場合、または、エージェントのアンインストールが失敗する場合は、次の手順に従ってエージェントを手動で削除します。

ステップ 1　Windows マシンを、ネットワーキングを備えた SAFEMODE で起動します（通常は F8）。

（注）　IIS または Apache がインストールされていないシステムからエージェントを削除する場合は、ステップ 4 に進みます。

ステップ 2　..¥csagent¥bin 内の CMD シェルから次のコマンドを実行します。

- **IIS の場合**

  csa_datafilter -u iis
- **Apache 1.3 の場合**

  csa_datafilter -u apache13 <.conf file with full path name> <modules dir.path>
- **Apache 2.0 の場合**

  csa_datafilter -u apache20 <.conf file with full path name> <modules dir.path>

ステップ 3　上のスクリプトが機能しない場合は、次のようにフィルタを手動で削除します。

Apache 1_3 の場合

a.　Apache がインストールされた場所に移動します（通常は Program Files¥apache）。

b.　メモ帳を使用して apache¥conf¥httpd.conf を開きます。

c.　「csafilter」を探します。

d.　次の文字列で始まる 2 行を削除します。

「loadmodule csafilter...」

「addmodule mod_csafilter ...」

e.　apache¥modules に移動して、次のファイルを削除します。

mod_csafilter*.so

Apache 2 の場合

次を参照しないことを除いて、Apache 1_3 のステップを実行します。「addmodule mod_csafilter...」

IIS の場合

a. [My Computer] を右クリックして、[Manage] を選択します。

b. [Services and Applications] に移動します。

c. [Internet Information Services] を右クリックして、[Properties] を選択します。

d. [Master Properties] の下で、[www service] を選択します。

e. [ISAPI Filters] タブをクリックして編集します。

f. csafilter を強調表示して、[Remove] を選択します。

g. [OK] をクリックします。

ステップ 4　CSA エージェント サービスが開始されていた場合は、CSAgent を net stop します。

ステップ 5　CSA エージェント アイコン（赤色のペナント）がシステム トレイに表示されていないことを確認します。

（注）　エージェント アイコンが表示されている場合は、終了して、赤色のペナントを右クリックし、[Exit Agent Panel] をクリックします。

ステップ 6　Program Files¥Cisco (Systems)¥CSAgent フォルダを削除します。

ステップ 7　次のディレクトリを削除します。

Program Files¥InstallShield Installation Information¥{DE49974667B9-11D4-97CE-0050DA10E5AE}

ステップ 8　次のドライバ ファイルを削除します。使用しているオペレーティング システムによっては、Windows（または WINNT）¥system32¥drivers¥ に配置されている場合があります。

- csacentr.sys
- csafile.sys
- csanet.sys
- csareg.sys
- csatdi.sys

ステップ 9　Start Menu¥Programs ディレクトリで csagent へのすべての参照を削除します。

ステップ 10　WINDOWS¥system32¥csauser.dll を削除します。使用しているオペレーティング システムによっては、WINNT¥system32¥ に配置されている場合があります。

（注）　キー全体を削除するのではなく、CSAUSER.DLL だけを削除します。AppInit_DLLs レジストリ キー内で参照されている他の DLL は他のプログラムに必要であり、削除するとシステムが不安定になる可能性があります。

このファイルを削除できない場合は、この DLL をロードするレジストリ キーを変更してから、リブートすれば、削除できます。これを実行するには、次の手順を実行します。

a. [Start] > [Run] > [regedit] を選択して、レジストリ エディタを開きます。

b. [HKLM] > [SOFTWARE] > [Microsoft] > [Windows NT] > [CurrentVersion] > [Windows] に移動します。

c. AppInit_DLLs レジストリ キーを変更して、参照を csauser.dll から *xyz* に変更します。

（注）　参照を *xyz* に変更し、サーバをリブートしても、csauser.dll ファイルが残っている可能性があります。その場合は、次のサブステップを省略して、次のステップに進みます。

d. 再起動します。

（注）　AppInit_DLLs レジストリ キーから csauser.dll を削除したら、リブートしなければ、Windows 上で csauser.dll ファイルを削除できません。

ステップ 11　WINNT または WINDOWS¥system32¥csafilter.dll、csa_uninstall.bat、csarule.dll（存在する場合）を削除します。

ステップ 12　[Start] > [Programs] > [Startup] で Cisco Security Agent への参照を削除します。

ステップ 13　次のレジストリ キーを削除します。

- [HKLM] > [system] > [controlset001] > [control] > [session manager] > [knowndlls] > [csauser.dll]
- [HKLM] > [system] > [controlset002] > [control] > [session manager] > [knowndlls] > [csauser.dll]
- [HKLM] > [system] > [controlset003] > [control] > [session manager] > [knowndlls] > [csauser.dll（WinNT）]
- [HKLM] > [System] > [Currentcontrolset] > [Services] > [csacenter、csafile、csanet、csareg、csaTDI、csagent、csafilter、csahook]
- [HKEY_Local_Machine] > [Software] > [Cisco] > [CSAgent]
- [HKEY_Local_Machine] > [Software] > [Cisco] > [CSAgentinstalled]
- [HKEY_Local_Machine] > [Software] > [Microsoft] > [windows] > [currentversion] > [uninstall] > [{DE499746-67B9-11D4-97CE-0050DA10E5AE}]

ステップ 14　**W2K、WINXP、W2K3**

a. Windows のデバイス マネージャで Cisco Security Agent* リソースへの参照を削除します（[Start] > [Control Panel] > [System] > [Hardware] > [Device Manager] に移動します）。[show hidden devices]（[View] > [Show hidden devices]）が選択されていることを確認し、非プラグアンドプレイ セクションを展開します。

b. 各 Cisco Security Agent* リソースを右クリックして、アンインストールします。

（注）　すべての 「Cisco Security Agent*」リソースがアンインストールされるまでリブートしないでください。

c. 再起動します。変更を有効にするには再起動する必要があります。

ステップ 15　**WINNT の場合**

a. Windows のデバイス マネージャで「Cisco Security Agent*」リソースへの参照を削除します

b. 各「Cisco Security Agent*」リソースを右クリックして、アンインストールします。

（注）　すべての「Cisco Security Agent*」リソースがアンインストールされるまでリブートしないでください。

c. 再起動します。変更を有効にするには再起動する必要があります。

ステップ 16　サーバをリブートして、Windows のデバイス マネージャですべての CSA リソースが削除されていることを確認します（ステップ 14 を参照）。

ステップ 17　リブート後に WINNT または WINDOWS¥system32¥csauser.dll を削除します。

ステップ 18　レジストリを探して、「CSAgent」と「Cisco Security Agent」という文字列のすべてのエントリを削除します。レジストリにアクセスするには、[Start] > [Run] を選択します。[Open] フィールドに **regedit** と入力してから、[Open] をクリックします。

エントリの一部は削除できません。

ステップ 19　CSAgent が [Control Panel] > [Add/Remove Programs] に表示されていないことを確認します。