Mac-Lab/CardioLab アンチウイルス インストール手順（JA）

Mac-Lab/CardioLab ソフトウェアバージョン 6.9.6

はじめに

アンチウイルスソフトウェアは、HIPAA（医療保険の相互運用性と説明責任に関する法律）などのプライバシー規制に準拠できるように施設を支援します。

文書の用途

本書を使用して、Mac-Lab/CardioLab v6.9.6 システム用の確認されているアンチウイルスソフトウェアをインストールします。

改訂履歴

改訂番号	日付	コメント
A	2016 年 2 月 16 日	最初の一般公開。
B	2016 年 6 月 9 日	Trend Micro が CO_2 のサポートをアップデート。
C	2017 年 5 月 16 日	McAfee ePolicy Ochestrator、Trend Micro、および Symantec のアップデート。
D	2017 年 7 月 10 日	Symantec 12.1.6 MP5、Trend Micro 11.0 SP1、McAfee ePO 5.9、および McAfee VSE 8.8 パッチ 9 用のアップデート。
E	2017 年 8 月 14 日	McAfee ePolicy Orchestrator 5.9 および McAfee VirusScan Enterprise 8.8 パッチ 9 の参照を削除。6.9.6 R3 UI 言語を追加。
F	2017 年 9 月 25 日	McAfee ePO 5.9 および McAfee VSE 8.8 パッチ 9 を追加。Trend Micro 11 および 12 のリンクを更新。

使用の準備

アンチウイルスの要件

警告：　アンチウイルスソフトウェア要インストール

このシステムは出荷時にアンチウイルス保護が行われていません。ネットワークに接続する前に、確認されているアンチウイルスソフトウェアがシステムにインストールされていることを確認してください。確認されているアンチウイルス保護がない場合、システムが不安定になったり、故障する可能性があります。

以下の必要条件に注意してください。

- アンチウイルスソフトウェアは Mac-Lab/CardioLab システムには含まれておらず、取得、インストールおよび保守はお客様の責任となります。
- お客様にはアンチウイルスソフトウェアの定義ファイルを更新する義務があります。
- ウイルスが検出された場合は、施設のシステム管理者または GE テクニカルサポートまでお問い合わせください。
- 「確認されているアンチウイルスソフトウェア」セクションに記載されているアンチウイルスソフトウェアパッケージのみをインストールしてください。
- 管理者またはそのグループのメンバーとしてログインし、本書の作業を実行します。
- 可能な場合は、確認されているアンチウイルスソフトウェアの、オペレーティングシステムの言語と一致する言語バージョンを使用してください。確認されているアンチウイルスソフトウェアに、オペレーティングシステムの言語と一致するバージョンがない場合は、英語バージョンをインストールしてください。

確認されているアンチウイルスソフトウェア

警告：　システムの不安定化

確認されていないアンチウイルスソフトウェア（確認されていないバージョンも含む）をインストールまたは使用しないでください。そのようにすると、システムが不安定になったり、障害が発生したりする可能性があります。適切な言語バージョンで確認されているアンチウイルスソフトウェアのみ使用してください。

注：　特定の言語用のアンチウイルスソフトウェアが提供されていない場合は、英語バージョンのアンチウイルスソフトウェアをインストールしてください。

Mac-Lab/CardioLab バージョン 6.9.6 システムは、以下の表に記載されているソフトウェアと同時に実行できることが確認されています。

対応しているアンチウイルスソフトウェア	対応している MLCL 言語	対応しているアンチウイルスソフトウェアバージョン
McAfee VirusScan Enterprise	英語、フランス語、ドイツ語、イタリア語、スペイン語、スウェーデン語、デンマーク語、オランダ語、中国語、日本語	8.8 パッチ 3 8.8 パッチ 4 8.8 パッチ 8 8.8 パッチ 9
McAfee ePolicy Orchestrator（McAfee VirusScan Enterprise 付き）	英語、フランス語、ドイツ語、イタリア語、スペイン語、スウェーデン語、デンマーク語、オランダ語、中国語、日本語	v5.0 v5.3.2 v5.9
Symantec EndPoint Protection	英語、フランス語、ドイツ語、イタリア語、スペイン語、スウェーデン語、デンマーク語、オランダ語、中国語、日本語	12.1.2、12.1.6 MP5、14.0 MP1
Trend Micro OfficeScan Client/Server Edition	英語、フランス語、ドイツ語、イタリア語、スペイン語、スウェーデン語、デンマーク語、オランダ語、中国語、日本語	10.6 SP2、11.0 SP1、XG 12.0

対応しているアンチウイルスソフトウェアは、以下の表に記載されている言語で利用できます。

MLCL のバージョン	対応している MLCL 言語
M6.9.6 R1	英語
M6.9.6 R2	英語、フランス語、ドイツ語
M6.9.6 R3	英語、フランス語、ドイツ語、イタリア語、スペイン語、スウェーデン語、デンマーク語、オランダ語、中国語、日本語

アンチウイルス管理コンソールサーバーの設定

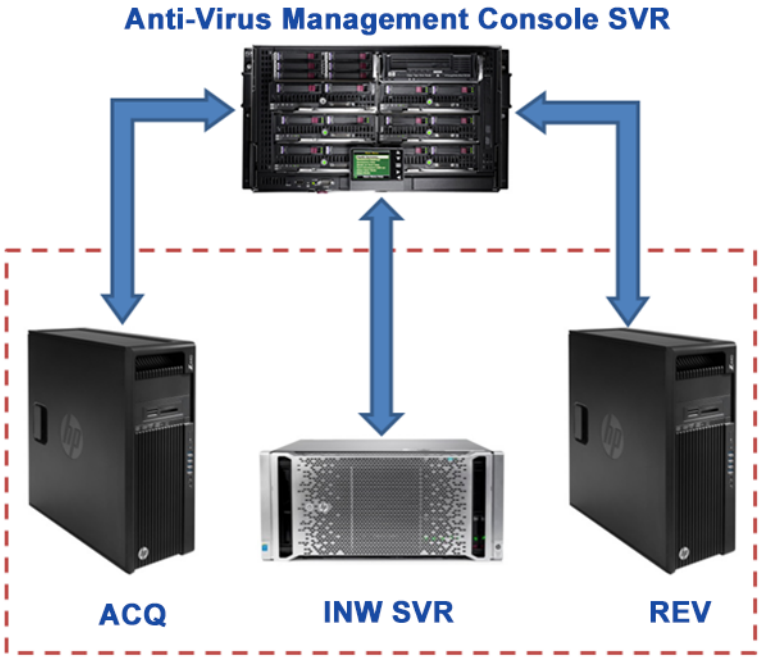
アンチウイルス管理コンソールは、Anti-virus Management Console Server にインストールする必要があります。

Anti-virus Management Console Server と Mac-Lab/CardioLab デバイスの間の通信は、環境に応じて異なる方法で実行できます。

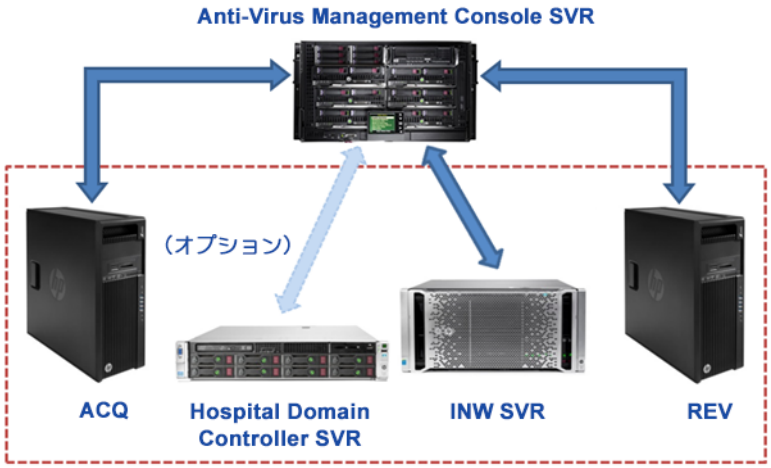
1. INW ドメインコントローラ環境 - Anti-virus Management Console SVR が INW Server ドメインに含まれない
   - 通信タイプ - 1 < 同じサブネットマスクの同じネットワーク >
   - 通信タイプ - 2 < 異なるサブネットマスクの異なるネットワーク >
2. ホスピタルドメインコントローラ環境 - Anti-virus Management Console SVR がホスピタルドメインコントローラドメインに含まれない
   - 通信タイプ - 1 < 異なるサブネットマスクの異なるネットワーク >
3. ホスピタルドメインコントローラ環境 - Anti-virus Management Console SVR がホスピタルドメインコントローラドメインに含まれる
   - 通信タイプ - 1 < 同じサブネットマスクの同じネットワーク >

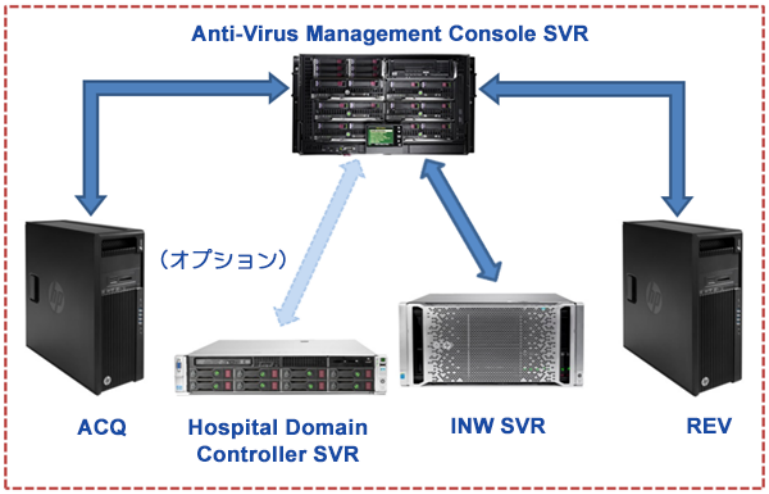
注 : Anti-virus Management Console Server には 2 つのネットワークポートが必要です。1 つのネットワークポートは Centricity Cardiology INW ネットワークに接続し、もう 1 つのネットワークポートはホスピタルネットワークに接続します。

INW ドメインコントローラ環境のブロック図



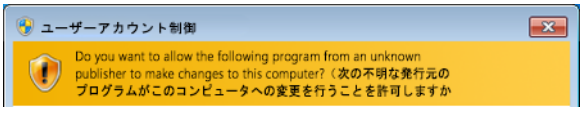
ホスピタルドメインコントローラ環境のブロック図





ユーザーアカウント制御

ユーザーアカウント制御は、コンピュータの不正な変更を防止する Windows 機能です。本書の特定の手順では、ユーザーアカウント制御メッセージが表示されます。



本書の手順に従った結果としてこのメッセージが表示された場合は、続行しても安全です。

アンチウイルスのインストール手順

インストールするアンチウイルスソフトウェアをクリックします。

アンチウイルスソフトウェアの一般的なインストール手順

このセクションの手順がアンチウイルスソフトウェアのインストール手順で参照されているときには、このセクションの手順を使用します。

ループバック接続を無効にする

Mac-Lab/CardioLab 環境に接続されているアクイジションシステムで、ループバック接続を無効にして、ドメイン上で同じサブネットマスクを使用しているすべてのクライアントシステムを検出します。

1. **管理者**またはそのグループのメンバーとしてログオンします。
2. デスクトップで ***Network*（ネットワーク）**を右クリックし、***Properties*（プロパティ）**を選択します。
3. ***Change adapter settings*（アダプターの設定の変更）**をクリックします。
4. ***Loopback Connection*（ループバック接続）**を右クリックし、***Disable*（無効）**を選択します。
5. アクイジションシステムを再起動します。

注： ドメイン内で同じサブネットマスクを使用するすべてのクライアントシステムを検出するには、アクイジションシステムでループバック接続を無効にする必要があります。

ループバック接続を有効にする

Mac-Lab/CardioLab 環境に接続されているアクイジションシステムで、以下の手順に従ってループバック接続を有効にします。

1. **管理者**またはそのグループのメンバーとしてログオンします。
2. デスクトップで ***Network*（ネットワーク）**を右クリックし、***Properties*（プロパティ）**を選択します。
3. ***Change adapter settings*（アダプターの設定の変更）**をクリックします。
4. ***Loopback Connection*（ループバック接続）**を右クリックし、***Enable*（有効）**を選択します。
5. アクイジションシステムを再起動します。

アンチウイルスのインストール前のコンピュータブラウザーサービスの設定

ネットワーク接続されたアクイジションおよびレビューシステムでコンピュータブラウザーサービスの設定が正しく設定されていることを確認します。

1. ***Start*（スタート）> *Control Panel*（コントロールパネル）> *Network and Sharing Center*（ネットワークと共有センター）**をクリックします。
2. ***Change advanced sharing settings*（共有の詳細設定の変更）**をクリックします。
3. ***Home or Work*（ホームまたは社内）**を展開します。
4. ***Turn on file and printer sharing*（ファイルとプリンターの共有を有効にする）**が選択されていることを確認します。
5. ***Save changes*（変更の保存）**をクリックします。
6. ***Start*（スタート）> *Run*（実行）**をクリックします。
7. **services.msc** と入力し、**Enter** キーを押します。
8. ***Computer Browser*（コンピュータブラウザー）**サービスをダブルクリックします。
9. ***Startup type*（スタートアップの種類）**が ***Automatic*（自動）**に設定されていることを確認します。自動に設定されていない場合は、変更して ***Start*（開始）**をクリックします。
10. ***OK*** をクリックします。
11. ***Services*（サービス）**ウィンドウを閉じます。

アンチウイルスのインストール後のコンピュータブラウザーサービスの設定

アンチウイルスソフトウェアのインストールの後で、ネットワーク接続されたアクイジションおよびレビューシステムでコンピュータブラウザーサービスの設定が正しく設定されていることを確認します。

1. ***Start*（スタート）> *Run*（実行）**をクリックします。
2. **services.msc** と入力し、**Enter** キーを押します。
3. ***Computer Browser*（コンピュータブラウザー）**サービスをダブルクリックします。
4. ***Startup type*（スタートアップの種類）**を ***Manual*（手動）**に設定します。
5. ***OK*** をクリックします。
6. ***Services*（サービス）**ウィンドウを閉じます。

Symantec EndPoint Protection（12.1.2、12.1.6 MP5、または 14.0 MP1）

インストール概要

Symantec EndPoint Protection は、ネットワーク接続された Mac-Lab/CardioLab 環境にのみインストールします。ネットワーク環境で、Symantec EndPoint Protection を Anti-virus Management Console サーバーにインストールしてから、Centricity Cardiology INW Server およびアクイジション / レビュー用ワークステーションにクライアントとして配備する必要があります。***Symantec EndPoint Protection*** をインストールして設定するには、以下の手順を使用します。

ウイルス定義の更新は施設の責任となります。最新のアンチウイルス保護がシステムに確実に施されるよう、定期的に定義をアップデートしてください。

インストール前のガイドライン

1. Symantec Anti-Virus Management Console は、Symentec の指示に従ってインストールされ、適切に機能している必要があります。
2. すべてのクライアントシステム（アクイジション、レビュー、および INW Server）上で**管理者**またはそのグループのメンバーとしてログオンし、アンチウイルスソフトウェアをインストールします。
3. **管理者として実行**モードでコマンドプロンプトを開きます。
4. C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec に移動します。

注 : INW Server を設定するには、C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec に移動します。

5. **UpdateRegSymantec.ps1** と入力し、***Enter*** キーを押します。
6. スクリプトが正常に実行されることを確認します。

   上記のフォルダパスが存在しない場合は、MLCL 6.9.6R1 INW Server（Server OS : Windows Server 2008R2）除くすべての MLCL システムに対して次の手順を実行します。

   a. ***Start*（スタート）**ボタンをクリックし、***Run*（ファイル名を指定して実行）**をクリックします。

   b. **Regedit.exe** と入力し、***OK*** をクリックします。

   c. ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing*** に移動します。

   d. ***State*** レジストリを見つけてダブルクリックします。

   e. ***Base*（表記）**を ***Decimal*（*10* 進数）**に変更します。

   f. ***Value data*（値データ）**を ***146432*** に変更します。

   g. ***OK*** をクリックし、レジストリを閉じます。

7. ループバック接続を無効にします。詳細については、ループバック接続を無効にする（6 ページ）を参照してください。

8. コンピュータブラウザーサービスを設定します。詳細については、アンチウイルスのインストール前のコンピュータブラウザーサービスの設定（7 ページ）を参照してください。

Symantec EndPoint Protection - 新規インストール実装手順（推奨プッシュインストールの方法）

1. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *Symantec EndPoint Protection Manager* > *Symantec Endpoint Protection Manager*** の順にクリックします。
2. ユーザー名とパスワードを入力して、Symantec Endpoint Protection Manager にログインします。（セキュリティプロンプトが表示されたら、***Yes*（はい）**をクリックします。）
3. ***Do not show this Welcome Page again*（次回からこのページを表示しない）**チェックボックスをオンにし、***Close*（閉じる）**をクリックしてようこそ画面を閉じます。

注： バージョン 14.0 MP1 の場合は、***Close*（閉じる）**をクリックして、***Getting Started on Symantec EndPoint Protection*（*Symantec EndPoint Protection* の使用準備）**画面を閉じます。

4. ***Symantec EndPoint Protection Manager*** ウィンドウで ***Admin*（管理）**をクリックします。
5. 下部のペインで ***Install Packages*（パッケージのインストール）**をクリックします。
6. 上部のペインで ***Client Install Feature Set*（クライアントインストール機能セット）**をクリックします。
7. ***Client Install Feature Set*（クライアントインストール機能セット）**を右クリックし、***Add*（追加）**を選択します。クライアントインストール機能セットの追加ウィンドウが表示されます。
8. 適切な名前を入力し、後で使用する場合に備えて書き留めておきます。
9. **機能セットのバージョン**が ***12.1 RU2* 以降**になっていることを確認します。
10. 以下の機能のみを選択し、その他の機能は選択しないでください。
    - ***Virus, Spyware, and Basic Download Protection*（ウイルス、スパイウェア、基本的なダウンロード保護）**。
    - ***Advanced Download Protection*（高度なダウンロード保護）**。
11. メッセージボックスで ***OK*** をクリックします。
12. バージョン 12.1.2 および 12.1.6 MP5 の場合のみ、***OK*** をクリックして、***Add Client Install Feature Set*（クライアントインストール機能セットの追加）**ウィンドウを閉じます。
13. ***Symantec EndPoint Protection Manager*** ウィンドウで ***Home*（ホーム）**をクリックします。
14. ソフトウェアのバージョンに応じて、次のいずれかを実行します。
    - **Versions 12.1.2 および 12.1.6 MP5：*Home*（ホーム）**ウィンドウの右上にある ***Common Tasks*（共通タスク）**ドロップダウンリストから ***Install protection client to computers*（コンピュータへの保護クライアントのインストール）**を選択します。Client Deployment Type（クライアントの展開タイプ）画面が表示されます。
    - **Version 14.0 MP1：*Symantec EndPoint Protection Manager*** ウィンドウで ***Clients*（クライアント）**をクリックします。***Tasks*（タスク）**の下にある ***Install a client*（ク**

ライアントのインストール）をクリックします。***Client Deployment wizard*（**クライアント展開ウィザード）**画面が表示されます。

15. ***New Package Deployment*（新規パッケージの展開）**を選択し、***Next*（次へ）**をクリックします。

16. 手順 8 で作成した機能セットの名前を選択します。他の設定は初期設定のままにし、***Next*（次へ）**をクリックします。

注 : バージョン 14.1 MP1 の場合は、***Scheduled Scans*（予約検索）**の下で、***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on*（バッテリで実行しているときには予約検索を遅らせ、検査の作成者がログオンしていないときにはユーザー定義の予約検索の実行を許可する）**の選択を解除します。

17. ***Remote push*（リモートプッシュ）**を選択し、***Next*（次へ）**をクリックします。***Computer selection*（コンピュータの選択）**画面が表示されるまで待ちます。

18. **< ドメイン >**（INW など）を展開します。ドメインに接続されているシステムが ***Computer selection*（コンピュータの選択）**ウィンドウに表示されます。

注 : すべてのシステムが認識されない場合は、***Search Network*（ネットワークの検索）**をクリックし、***Find Computers*（コンピュータの検索）**をクリックします。***search by IP address*（IP アドレスで検索）**の検索方法を使用してクライアントシステム（アクイジション、レビュー、INW Server）を識別します。

19. ドメインに接続されているすべての Mac-Lab/CardioLab クライアントマシンを選択し、**>>** をクリックします。***Login Credentials*（ログイン資格情報）**画面が表示されます。

20. ユーザー名、パスワード、ドメイン / コンピュータ名を入力し、***OK*** をクリックします。

21. 選択したすべてのマシンが ***Install Protection Client*（保護クライアントのインストール）**に表示されていることを確認し、***Next*（次へ）**をクリックします。

22. ***Send*（送信）**をクリックして、Symantec アンチウイルスソフトウェアがすべてのクライアントマシン（アクイジション、レビュー、INW Server）に実装されていることを確認します。終了すると、***Deployment Summary*（実装サマリ）**画面が表示されます。

23. ***Next*（次へ）**をクリックし、***Finish*（完了）**をクリックして Client Deployment Wizard（クライアント展開ウィザード）を完了します。

24. Symantec アイコンがシステムトレイに表示されるまで待ってから、すべてのクライアントマシン（アクイジション、レビュー、INW Server）を再起動します。再起動後にすべてのクライアントマシンで管理者またはそのグループのメンバーとしてログインします。

Symantec EndPoint Protection サーバーコンソールの設定

1. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *Symantec EndPoint Protection Manager* > *Symantec EndPoint Protection Manager*** の順に選択します。Symantec EndPoint Protection Manager のログオンウィンドウが表示されます。

2. Symantec Endpoint Protection Manager コンソールのパスワードを入力し、***Log On*（ログオン）**をクリックします。

3. ***Policies*（ポリシー）**タブを選択し、***Policies*（ポリシー）**の下にある ***Virus and Spyware Protection*（ウイルスおよびスパイウェア対策）**をクリックします。***Virus and Spyware Protection Policies*（ウイルスおよびスパイウェア対策ポリシー）**ウィンドウが開きます。

4. ***Tasks*（タスク）**の下にある ***Add a Virus and Spyware Protection*（ウイルスおよびスパイウェア対策の追加）**ポリシーをクリックします。***Virus and Spyware Protection*（ウイルスおよびスパイウェア対策）**ウィンドウが開きます。

5. ***Windows Settings*（*Windows* の設定）> *Scheduled Scans*（予約検索）**の下で ***Administrator-Defined Scans*（管理者定義のスキャン）**をクリックします。

6. ***Daily Scheduled Scan*（毎日予約検索）**を選択し、***Edit*（編集）**をクリックします。***Edit Scheduled Scan*（予約検索の編集）**ウィンドウが表示されます。

7. 検索名と説明をそれぞれ、***Weekly Scheduled Scan*（毎週の予約検索）**と ***Weekly Scan at 00:00*（週 *1* 回 *00:00* 時に検索）**に変更します。

8. ***Scan type*（検索タイプ）**として ***Full Scan*（完全検索）**を選択します。

9. ***Schedule*（スケジュール）**タブを選択します。

10. ***Scanning Schedule*（検索スケジュール）**で、***Weekly*（毎週）**を選択し、時刻を ***00:00*** に変更します。

11. ***Scan Duration*（検索時間）**の下で ***Randomize scan start time within this period (recommended in VMs)*（この期間内で検索の開始時刻をランダムにする（*VM* で推奨））**のチェックマークを外し、***Scan until finished (recommended to optimize scan performance)*（終了するまで検索（検索パフォーマンスの最適化のために推奨））**を選択します。

12. ***Missed scheduled Scans*（実行されなかった予約検索）**で、***Retry the scan within*（次の期間内に検索を再試行する）**のチェックマークを外します。

13. ***Notifications*（通知）**タブを選択します。

14. ***Display a notification message on the infected computer*（感染コンピュータに通知メッセージを表示する）**のチェックマークを外し、***OK*** をクリックします。

15. ***Administrator-Defined Scans*（管理者定義のスキャン）**ウィンドウから ***Advanced*（詳細設定）**タブを選択します。

16. ***Scheduled Scans*（予約検索）**の下で、***Delay scheduled scans when running on batteries*（バッテリで実行しているときには予約検索を遅らせる）**、***Allow user-defined scheduled scans to run when scan author is not logged on*（検索の作成者がログオンしていないときにはユーザー定義の予約検索の実行を許可する）**、および ***Display notifications about detections when the user logs on*（ユーザーのログイン時に検出についての通知を表示する）**の選択を解除します。

注 : バージョン 14.0 MP1 の場合は、***Scheduled Scans*（予約検索）**の下で、***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on*（バッテリで実行しているときには予約検索を遅らせ、検査の作成者がログオンしていないときにはユーザー定義の予約検索の実行を許可する）**の選択を解除します。

17. ***Startup and Triggered Scans*（スタートアップおよびトリガースキャン）**の下で、***Run an Active Scan when new definitions arrive*（新しい定義が到着したときにアクティブスキャンを実行する）**の選択を解除します。

18. ***Windows* の設定 > *Protection Technology*（保護テクノロジー）**の下で、***Auto-Protect*（自動保護）**をクリックします。

19. ***Scan Details*（スキャンの詳細）**タブを選択し、***Enable Auto-Protect*（自動保護を有効にする）**を選択してロックします。

20. ***Notifications*（通知）**タブを選択し、***Display a notification message on the infected computer*（感染しているコンピュータに警告メッセージを表示する）**と***Display the Auto-Protect results dialog on the infected Computer*（感染しているコンピュータに自動保護の結果を表示する）**の選択を解除してロックします。

21. ***Advanced*（詳細設定）**タブを選択し、***Auto-Protect Reloading and Enablement*（自動保護の再ロードと有効化）**の下で、***When Auto-Protect is disabled, Enable after:*（自動保護が無効になっている場合、次の後で有効にする）**オプションをロックします。

22. ***Additional Options*（追加オプション）**の下で ***File Cache*（ファイルキャッシュ）**をクリックします。***File Cache*（ファイルキャッシュ）**ウィンドウが開きます。

23. ***Rescan cache when new definitions load*（新しい定義がロードされたときにキャッシュを再スキャンする）**の選択を解除して、***OK*** をクリックします。

24. ***Windows Settings*（*Windows* の設定）> *Protection Technology*（保護テクノロジー）**の下で、***Download Protection*（ダウンロード保護）**をクリックします。

25. ***Notifications*（通知）**タブを選択し、***Display a notification message on the infected compute*** **r （感染コンピュータに通知メッセージを表示する）**の選択を解除してロックします。

26. ***Windows Settings*（*Windows* の設定 ）> *Protection Technology*（保護テクノロジー）**の下で ***SONAR*** をクリックします。

27. ***SONAR Settings*（*SONAR* の設定）**タブを選択し、***Enable SONAR*（*SONAR* を有効にする）**の選択を解除してロックします。

28. ***Windows* の設定 > *Protection Technology*（保護テクノロジー）**の下で、***Early Launch Anti-Malware Driver*（早期起動アンチマルウェアドライバ）**をクリックします。

29. ***Enable Symantec early lauch anti-malware*（*Symantec* 早期起動アンチマルウェアを有効にする）**のチェックマークを外し、ロックします。

30. ***Windows Settings*（*Windows* の設定）> *Email Scans*（*E* メールスキャン）**の下で、***Internet Email Auto-Protect*（インターネット電子メールの自動保護）**をクリックします。

31. ***Scan Details*（スキャンの詳細）**タブを選択し、***Enable Internet Email Auto-Protect*（インターネット電子メールの自動保護を有効にする）**の選択を解除してロックします。

32. ***Notifications*（通知）**タブを選択し、***Display a notification message on the infected computer*（感染しているコンピュータに警告メッセージを表示する）**、***Display a Progress indicator when email is being sent*（電子メールの送信時に進行状況インジケータを表示する）**、***Display a notification area icon*（通知領域アイコンを表示する）**の選択を解除してロックします。

33. ***Windows Settings*（*Windows* の設定）> *Email Scans*（*E* メールスキャン）**の下で、***Microsoft Outlook Auto-Protect*（*Microsoft Outlook* の自動保護）**をクリックします。

34. ***Scan Details*（スキャンの詳細）**タブを選択し、***Enable Microsoft Outlook Auto-Protect*（*Microsoft Outlook Auto-Protect* を有効にする）**の選択を解除してロックします。

35. ***Notifications*（通知）**タブを選択し、***Display a notification message on the infected compute*** **r *(* 感染コンピュータに通知メッセージを表示する *)*** の選択を解除してロックします。

36. ***Windows Settings*（*Windows* の設定）> *Email Scans*（*E* メールスキャン）**の下で、***Lotus Notes Auto-Protect*（*Lotus Notes* の自動保護）**をクリックします。

37. ***Scan Details(スキャンの詳細)*** タブを選択し、***Enable Lotus Notes Auto-Protect（Lotus Notes の自動保護を有効にする）***の選択を解除してロックします。

38. ***Notifications（通知）***タブを選択し、***Display a notification message on infected computer(感染コンピュータに通知メッセージを表示する)*** の選択を解除してロックします。

39. ***Windows Settings（Windows の設定）> Advanced Options（詳細設定オプション）***の下で、***Global Scan Options（グローバルスキャンオプション）***をクリックします。

40. ***Bloodhound(™) Detection Settings（Bloodhound(™) Detection の設定）***の下で、***Enable Bloodhound(™) heuristic virus detection（Bloodhound(™) ヒューリスティックウイルス検知を有効にする）***の選択を解除してロックします。

41. ***Windows Settings（Windows の設定）> Advanced Options（詳細設定オプション）***の下で、***Quarantine（検疫）***をクリックします。

42. ***General（全般）***タブを選択し、***When New Virus Definitions Arrive（新しいウイルス定義を配信したとき）***の下で、***Do nothing（何も実行しない）***を選択します。

43. ***Windows Settings（Windows の設定）> Advanced Options（詳細設定オプション）***の下で、***Miscellaneous（その他）***をクリックします。

44. ***Notifications（通知）***タブを選択し、***Display a notification message on the client computer when definitions are outdated（定義が古くなったときにクライアントコンピュータに通知メッセージを表示する）***、***Display a notification message on the client computer when Symantec Endpoint Protection is running without virus definitions（Symantec Endpoint Protection がウイルス定義なしで動作しているときにクライアントコンピュータに通知メッセージを表示する）***、および ***Display error messages with a URL to a solution（解決策にエラーメッセージと URL を表示する）***の選択を解除します。

45. ***OK*** をクリックして、***Virus and Spyware Protection（ウイルスおよびスパイウェア対策）***ポリシーウィンドウを閉じます。

46. ***Assign Policies（ポリシーの割り当て）***メッセージボックスで ***Yes（はい）***をクリックします。

47. ***My Company（マイカンパニー）***を選択し、***Assign（割り当て）***をクリックします。

48. メッセージボックスで ***Yes（はい）***をクリックします。

49. ***Policies（ポリシー）***の下で ***Firewall（ファイアウォール）***をクリックします。

50. ***Firewall Policies（ファイアウォールポリシー）***の下で ***Firewall policy（ファイアウォールポリシー）***をクリックし、***Tasks（タスク）***の下で ***Edit the policy（ポリシーの編集）***をクリックします。

51. ***Policy Name（ポリシー名）***タブを選択し、***Enable this policy（このポリシーを有効にする）***のチェックマークを外します。

52. ***OK*** をクリックします。

53. ***Policies（ポリシー）***の下で ***Intrusion Prevention（侵入防止）***をクリックします。

54. ***Intrusion Prevention Policies（侵入防止ポリシー）***の下で ***Intrusion Prevention（侵入防止）***ポリシーをクリックし、***Tasks（タスク）***の下で ***Edit the policy（ポリシーの編集）***をクリックします。

55. ***Policy Name（ポリシー名）***タブを選択し、***Enable this policy（このポリシーを有効にする）***のチェックマークを外します。

56. ソフトウェアのバージョンに応じて、次のいずれかを実行します。

    - **バージョン 12.1.2 :** 左ペインの ***Settings*（設定）**をクリックします。
    - **バージョン 12.1.6 MP5 および 14.0 MP1 :** 左ペインの ***Intrusion Prevention*（侵入防止）**をクリックします。

57. ***Enable Network Intrusion Prevention*（ネットワーク侵入防止を有効にする）**および ***Enable Browser Intrusion Prevention for Windows*（*Windows* のブラウザー侵入防止を有効にする）**の選択を解除してロックします。

58. ***OK*** をクリックします。

59. ***Policies*（ポリシー）**の下で、***Application and Device Control*（アプリケーションおよびデバイスコントロール）**をクリックします。

60. ***Application and Device Control Policies*（アプリケーションおよびデバイスコントロールポリシー）**の下で ***Application and Device Control Policy*（アプリケーションおよびデバイスコントロールポリシー）**をクリックし、***Tasks*（タスク）**の下で ***Edit the policy*（ポリシーの編集）**をクリックします。

61. ***Policy Name*（ポリシー名）**タブを選択し、***Enable this policy*（このポリシーを有効にする）**のチェックマークを外します。

62. ***OK*** をクリックします。

63. ***Policies*（ポリシー）**の下で ***LiveUpdate*（ライブアップデート）**をクリックします。

64. ***LiveUpdate Settings policy*（ライブアップデート設定ポリシー）**を選択し、***Tasks*（タスク）**の下で ***Edit the policy*（ポリシーの編集）**をクリックします。

65. ***Overview*（概要）> *Windows Settings*（*Windows* の設定）**の下で ***Server Settings*（サーバーの設定）**をクリックします。

66. ***Internal or External LiveUpdate Server*（内部または外部のライブアップデートサーバー）**の下で ***Use the default management server*（初期設定の管理サーバーの使用）**が選択されていることを確認し、***Use a LiveUpdate server*（ライブアップデートサーバーの使用）**の選択を解除します。

67. ***OK*** をクリックします。

68. ***Policies*（ポリシー）**の下で ***Exceptions*（例外）**をクリックします。

69. ***Exceptions policy*（例外ポリシー）**をクリックし、***Tasks*（タスク）**の下で ***Edit the policy*（ポリシーの編集）**をクリックします。

70. ソフトウェアのバージョンに応じて、次のいずれかを実行します。

    - **Versions 12.1.2 および 12.1.6 MP5 :** ***Exceptions*（例外）> *Add*（追加）> *Windows Exceptions*（*Windows* の例外）> *Folder*（フォルダ）**の順にクリックします。
    - **Version 14.0 MP1 :** ***Add*（追加）**ドロップダウンをクリックし、***Windows Exceptions*（*Windows* の例外）> *Folder*（フォルダ）**を選択します。

71. **C:\Program Files (x86)\GE Healthcare\MLCL**、**C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** フォルダパスを 1 つずつ入力し、次の手順を実行します。

    a. ***Include subfolders*（サブフォルダを含む）**が選択されていることを確認します。

注 : ***Are you sure you want to exclude all subfolders from protection?*（すべてのサブフォルダを保護から除外してもよろしいですか *?*）**メッセージボックスが表示された場合は ***Yes*（はい）**をクリックします。

b. ***Specify the type of scan that excludes this folder*（このフォルダを除外するスキャンのタイプの指定）**から ***All*（すべて）**を選択します。

c. バージョン 14.0 MP1 の場合は、***OK*** をクリックして、この例外を追加します。

72. ***OK*** をクリックします。

73. ***Tasks*（タスク）**の下で ***Assign the policy*（ポリシーの割り当て）**をクリックします。

74. ***My Company*（マイカンパニー）**を選択し、***Assign*（割り当て）**をクリックします。

75. ***Yes*（はい）**をクリックします。

76. 左ペインで ***Clients*（クライアント）**をクリックし、***Policies*（ポリシー）**タブを選択します。

77. ***My Company*（マイカンパニー）**で ***Default Group*（初期設定のグループ）**を選択し、***Inherit policies and settings from parent group "My Company"*（ポリシーと設定を親グループ *My Company* から継承する）**のチェックマークを外し、***Location-Independent Policies and Settings*（場所に依存しないポリシーと設定）**の下で ***Communications Settings*（通信の設定）**をクリックします。

注 : 警告メッセージが表示される場合は、***OK*** をクリックし、***Location-Independent Policies and Settings*（場所に依存しないポリシーと設定）**の下で ***Communications Settings*（通信の設定）**をもう一度クリックします。

78. ***Download*（ダウンロード）**の下で、***Download policies and content from the management server*（管理サーバーからポリシーとコンテンツをダウンロード）**が選択され、***Push mode*（プッシュモード）**が選択されていることを確認します。

79. ***OK*** をクリックします。

80. ***Location-independent Policies and Settings*（場所に依存しないポリシーと設定）**の下で ***General Settings*（全般設定）**をクリックします。

81. ***Tamper Protection*（改変保護）**タブを選択し、***Protect Symantec security software from being tampered with or shut down*（シマンテック製セキュリティソフトウェアを改変または終了から保護する）**の選択を解除してロックします。

82. ***OK*** をクリックします。

83. ***Admin*（管理）**をクリックし、***Servers*（サーバー）**を選択します。

84. ***Servers*（サーバー）**の下で ***Local Site (My Site)*（ローカルサイト（マイサイト））**を選択します。

85. ***Tasks*（タスク）**の下で ***Edit Site Properties*（サイトのプロパティの編集）**を選択します。***Site Properties for Locate Site (My Site)*（ローカルサイトのサイトのプロパティ（マイサイト））**ウィンドウが開きます。

86. ***LiveUpdate*** タブを選択し、***Download Schedule*（ダウンロードスケジュール）**の下でスケジュールが ***Every 4 hour(s)*（*4* 時間ごと）**に設定されていることを確認します。

87. ***OK*** をクリックします。

88. ***Log Off*（ログオフ）**をクリックし、Symantec EndPoint Protection Manager コンソールを閉じます。Symantec Endpoint Protection ポリシーがクライアントシステムでプッシュされていることを確認します。

Symantec EndPoint Protection インストール後のガイドライン

1. ループバック接続を有効にします。詳細については、ループバック接続を有効にする（6 ページ）を参照してください。
2. コンピュータブラウザーサービスを設定します。詳細については、アンチウイルスのインストール後のコンピュータブラウザーサービスの設定（7 ページ）を参照してください。
3. **管理者として実行**モードでコマンドプロンプトを開きます。
4. C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec に移動します。

注： INW Server を設定するには、C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec に移動します。

5. **RestoreRegSymantec.ps1** と入力し、***Enter*** キーを押します。

   スクリプトが正常に実行されることを確認します。
   注：続行する前に、**RestoreRegSymantec.ps1** スクリプトが正常に実行されていることを確認する必要があります。

   a. 上記のフォルダパスが存在しない場合は、MLCL 6.9.6R1 INW Server（Server OS：Windows Server 2008R2）除くすべての MLCL システムに対して次の手順を実行します。

   b. ***Start*（スタート）**ボタンをクリックし、***Run*（ファイル名を指定して実行）**をクリックします。

   c. **Regedit.exe** と入力し、***OK*** をクリックします。

   d. ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing*** に移動します。

   e. ***State*** レジストリを見つけてダブルクリックします。

   f. ***Base*（表記）**を ***Decimal*（*10* 進数）**に変更します。

   g. ***Value data*（値データ）**を ***65536*** に変更します。

   h. ***OK*** をクリックし、レジストリを閉じます。

McAfee VirusScan Enterprise

インストール概要

McAfee VirusScan Enterprise が個別の Mac-Lab/CardioLab システムにインストールされ、個別に管理されている必要があります。McAfee VirusScan Enterprise をインストールして設定するには、以下の手順を使用します。

ウイルス定義の更新は施設の責任となります。最新のアンチウイルス保護がシステムに確実に施されるよう、定期的に定義をアップデートしてください。

McAfee VirusScan Enterprise のインストール手順

1. **管理者**またはそのグループのメンバーとしてログオンします。

2. **McAfee VirusScan Enterprise 8.8 Patch 3**、**McAfee VirusScan Enterprise 8.8 Patch 4**、**McAfee VirusScan Enterprise 8.8 Patch 8 CD** または **McAfee VirusScan Enterprise 8.8 Patch 9 CD** を CD ドライブに挿入します。
3. ***SetupVSE.Exe*** をダブルクリックします。Windows Defender ダイアログが表示されます。
4. ***Yes*（はい）**をクリックします。McAfee VirusScan Enterprise セットアップ画面が表示されます。
5. ***Next*（次へ）**をクリックします。McAfee End User License Agreement（McAfee エンドユーザー使用許諾契約）画面が表示されます。
6. 使用許諾契約書をロードして、必要なフィールドに入力し、完了したら ***OK*** をクリックします。Select Setup Type（セットアップタイプの選択）画面が表示されます。
7. ***Typical*（一般的）**を選択し、***Next*（次へ）**を選択します。Select Access Protection Level（アクセス保護レベルの選択）画面が表示されます。
8. ***Standard Protection*（標準の保護）**を選択し、***Next*（次へ）**をクリックします。Ready to Install（インストール準備完了）画面が表示されます。
9. ***Install*（インストール）**をクリックし、インストールが完了するまで待機します。McAfee VirusScan Enterprise が正常にインストールされると、***McAfee Virus Scan Enterprise Setup has completed successfully*（*McAfee Virus Scan Enterprise* のセットアップが正常に完了しました）**画面が表示されます。
10. ***Run On-Demand Scan*（オンデマンドスキャンの実行）**の選択を解除して、***Finish*（完了）**をクリックします。
11. ***Update in Progress*（アップデートの進行中）**ウィンドウが表示された場合は、***Cancel*（キャンセル）**をクリックします。
12. システムを再起動することを知らせるメッセージボックスが表示された場合は、***OK*** をクリックします。
13. システムを再起動します。
14. **管理者**またはそのグループのメンバーとしてログオンします。

McAfee VirusScan Enterprise の設定

1. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *McAfee* > *VirusScan Console*（*VirusScan* コンソール *)*** を選択します。***VirusScan Console*（*VirusScan* コンソール）**画面が表示されます。
2. ***Access Protection*（アクセス保護）**を右クリックし、***Properties*（プロパティ）**を選択します。***Access Protection*（アクセス保護）**のプロパティ画面が表示されます。
3. ***Access Protection*（アクセス保護）**タブをクリックし、***Enable access protection*（アクセス保護を有効にする）**および ***Prevent McAfee services from being stopped*（*McAfee* サービスが停止しないようにする）**の選択を解除します。
4. ***OK*** をクリックします。
5. ***Buffer Overflow Protection*（バッファオーバーフロー保護）**を右クリックし、***Properties*（プロパティ）**を選択します。***Buffer Overflow Protection Properties*（バッファオーバーフロー保護のプロパティ）**画面が表示されます。

6. ***Buffer Overflow Protection*（バッファオーバーフロー保護）**タブをクリックし、***Show the messages dialog box when a buffer overflow is detected under Buffer overflow settings*（バッファオーバーフローの設定でバッファオーバーフロー検出時にメッセージダイアログを表示する）**の選択を解除します。

7. ***Buffer overflow settings*（バッファオーバーフローの設定）**で ***Enable buffer overflow protection*（バッファオーバーフロー保護を有効にする）**の選択を解除します。

8. ***OK*** をクリックします。

9. ***On-Delivery Email Scanner*（配信時の E メールスキャン）**を右クリックし、***Properties*（プロパティ）**を選択します。***On-Delivery Email Scanner Properties*（配信時の E メールスキャナのプロパティ）**画面が表示されます。

10. ***Scan items*（スキャン項目）**タブをクリックし、***Heuristics*（ヒューリスティック）**で次のオプションの選択を解除します。

    - ***Find unknown program threats and trojans*（不明なプログラムの脅威とトロイの木馬を検出する）**。
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）**。
    - ***Find attachments with multiple extensions*（複数の拡張子が付いた添付ファイルを検出する）**。

11. ***Detect unwanted programs*（不要なプログラムの検出）**で ***Detect unwanted programs*（不要なプログラムの検出）**の選択を解除します。

12. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑いのあるファイルのヒューリスティックネットワークチェック））**の下で ***Sensitivity level*（感度レベル）**の ***Disabled*（無効）**を選択します。

13. ***OK*** をクリックします。

14. ***On-Delivery Email Scanner*（配信時の E メールスキャナ）**を右クリックし、***Disable*（無効）**を選択します。

15. ***On-Access Scanner*（オンアクセススキャナ）**を右クリックし、***Properties*（プロパティ）**を選択します。***On-Access Scan Properties*（オンアクセススキャンのプロパティ）**画面が表示されます。

16. ***General*（全般）**タブをクリックし、***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑いのあるファイルのヒューリスティックネットワークチェック））**の下で ***Sensitivity level*（感度レベル）**の ***Disabled*（無効）**を選択します。

17. ***ScriptScan*（スクリプトスキャン）**タブをクリックし、***Enable scanning of scripts(スクリプトスキャンを有効にする)*** の選択を解除します。

18. ***Blocking*（ブロック）**タブをクリックし、***Block the connection when a threat is detected in a shared folder*（共有フォルダで脅威が検出されたときに接続をブロックする）**の選択を解除します。

19. ***Messages*（メッセージ）**タブをクリックし、***Show the messages dialog box when a threat is detected and display the specified text in the message*（ウイルス検出時にメッセージダイアログを表示する / メッセージに表示するテキスト *)*** の選択を解除します。

20. 左側のペインで ***All Processes*（すべてのプロセス）**をクリックします。

21. ***Scan Items*（スキャン項目）**タブをクリックし、Heuristics（ヒューリスティック）で次のオプションの選択を解除します。

- ***Find unknown unwanted programs and trojans*（不明で不要なプログラムとトロイの木馬を検出する）。**
- ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

22. ***Detect unwanted programs*（不要なプログラムの検出）**で ***Detect unwanted programs*（不要なプログラムの検出）**の選択を解除します。
23. ***Exclusions*（除外対象）**タブをクリックし、***Exclusions*（除外対象）**をクリックします。***Set Exclusions*（除外対象の設定）**画面が表示されます。
24. ***Add*（追加）**をクリックします。***Add Exclusion Item*（除外項目の追加）**画面が表示されます。
25. ***By name/location*（名前 / 場所別）**を選択し、***Browse*（参照）**をクリックします。***Browse for Files or Folders*（ファイルまたはフォルダの参照）**画面が表示されます。
26. ***C:\Program Files\GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*、*G:*** フォルダに 1 つずつ移動し、***OK*** を選択します。
27. ***Add Exclusion Item*（除外項目の追加）**ウィンドウで ***Also exclude subfolders*（サブフォルダも除外）**を選択し、***OK*** をクリックします。
28. C:\Program Files\GE Healthcare\MLCL\、D:\GEData\Studies\、E:\、G:\ フォルダが Set Exclusions（除外対象の設定）ウィンドウに表示されていることを確認します。
29. ***OK*** をクリックします。
30. ***AutoUpdate*（自動アップデート）**を右クリックし、***Properties*（プロパティ）**を選択します。McAfee AutoUpdate Properties – AutoUpdate 画面が表示されます。
31. ***Update Options*（アップデートオプション）**で以下のオプションの選択を解除します。
    - ***Get new detection engine and dats if available*（利用可能な場合に新しい検知エンジンとデータを取得する）。**
    - ***Get other available updates (service packs, upgrades, etc.)*（その他の使用可能なアップデート（サービスパック、アップグレードなど）を取得する）。**
32. ***Schedule*（スケジュール）**をクリックします。Schedule Settings（スケジュールの設定）画面が表示されます。
33. ***Schedule Settings*（スケジュールの設定）**で ***Enable (scheduled task runs at specified time)*（有効（予約タスクは指定時間に実行されます））**の選択を解除します。
34. ***OK*** をクリックします。
35. ***OK*** をクリックします。
36. ***VirusScan Console*（*VirusScan* コンソール）**ウィンドウを右クリックし、***New On-Demand Scan Task*（新しいオンデマンドスキャンタスク）**を選択します。
37. 新しいスキャンの名前を ***Weekly Scheduled Scan*（週単位の定時スキャン）**に変更します。***On-Demand Scan Properties - Weekly Scheduled Scan*（オンデマンドスキャンのプロパティ - 週単位の定時スキャン）**画面が表示されます。
38. ***Scan Items*（スキャン項目）**タブをクリックし、***Options*（オプション）**で ***Detect unwanted programs*（不要なプログラムの検出）**の選択を解除します。
39. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。
    - ***Find unknown programs threats*（不明なプログラムの脅威を検出する）。**

- ***Find unknown macro threats*（不明なマクロの脅威を検出する）。

40. ***Exclusions*（除外対象）タブをクリックし、***Exclusions*（除外対象）をクリックします。***Set Exclusions*（除外対象の設定）画面が表示されます。
41. ***Add*（追加）をクリックします。***Add Exclusion Item*（除外項目の追加）画面が表示されます。
42. ***By name/location*（名前 / 場所別）を選択し、***Browse*（参照）をクリックします。***Browse for Files or Folders*（ファイルまたはフォルダの参照）画面が表示されます。
43. ***C:\Program Files\GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*、*G:* フォルダに 1 つずつ移動し、***OK** を選択します。
44. ***Add Exclusion Item*（除外項目の追加）ウィンドウで ***Also exclude subfolders*（サブフォルダも除外）を選択し、***OK** をクリックします。
45. ***C:\Program Files\GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*、*G:* フォルダが ***Set Exclusions*（除外対象の設定）ウィンドウに表示されていることを確認します。
46. ***OK** をクリックします。
47. ***Performance*（パフォーマンス）タブをクリックし、***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑いのあるファイルのヒューリスティックネットワークチェック））で ***Sensitivity level*（感度レベル）の ***Disabled*（無効）を選択します。
48. ***Schedule*（スケジュール）をクリックします。***Schedule Settings*（スケジュールの設定）画面が表示されます。
49. ***Task*（タスク）タブをクリックし、***Schedule Settings*（スケジュールの設定）で ***Enable (scheduled task runs at specified time)*（有効（予約タスクは指定時間に実行されます））を選択します。
50. ***Schedule*（スケジュール）タブをクリックして以下を選択します。
    a. Run task（タスクの実行）：Weekly（毎週）。
    b. Start Time（開始時間）：12:00 AM
    c. Every（頻度）：1 Weeks, Sunday（1 週間、日曜日）。
51. ***OK** をクリックします。
52. ***OK** をクリックします。
53. ***VirusScan Console*（*VirusScan* コンソール）ウィンドウで ***Tools*（ツール）> ***Alerts*（アラート）をクリックします。Alert Properties（アラートのプロパティ）画面が表示されます。
54. ***On-Access Scan*（オンアクセススキャン）、***On-Demand Scan and scheduled scans*（オンデマンドスキャンとスケジュールスキャン）、***Email Scan*（*E-mail* スキャン）、***AutoUpdate*（自動アップデート）の選択を解除します。
55. ***Destination*（送信先）をクリックします。***Alert Manager Client Configuration*（*Alert Manager* クライアント設定）画面が表示されます。
56. ***Disable alerting*（アラートの通知を無効にする）を選択します。
57. ***OK** をクリックします。***Alert Properties*（アラートのプロパティ）画面が表示されます。
58. ***Additional Alerting Options*（その他のアラートオプション）タブを選択します。

59. ***Severity Filter*（アラートフィルタ）**ドロップダウンリストから ***Suppress all alerts (severities 0 to 4)*（すべてのアラートを送信しない（重要度 *0* から *4*））**オプションを選択します。

60. ***Alert Manager Alerts*（*Alert Manager* による通知）**タブを選択します。

61. ***Access Protection*（アクセス保護）**の選択を解除します。

62. ***OK*** をクリックして、***Alert Properties*（アラートのプロパティ）**ウィンドウを閉じます。

63. ***VirusScan* コンソール**ウィンドウを閉じます。

McAfee ePolicy Orchestrator

インストール概要

McAfee ePolicy Orchestrator は、ネットワーク接続された Mac-Lab/CardioLab 環境にのみインストールします。McAfee ePolicy Orchestrator を Anti-virus Management Console サーバーにインストールし、McAfee VirusScan Enterprise を Centricity Cardiology INW Server およびクライアントとしてアクイジション / レビュー用ワークステーションに実装する必要があります。McAfee ePolicy Orchestrator をインストールして設定するには、以下の手順を使用します。

以下の McAfee VirusScan Enterprise のプッシュおよび設定の手順は、パッチ 3、パッチ 4、パッチ 8 およびパッチ 9 をサポートします。

ウイルス定義の更新は施設の責任となります。最新のアンチウイルス保護がシステムに確実に施されるよう、定期的に定義をアップデートしてください。

インストール前のガイドライン

1. McAfee Anti-Virus Management Console は、McAfee の指示に従ってインストールされ、適切に機能している必要があります。

2. すべてのクライアントシステム（アクイジション、レビュー、および INW Server）上で**管理者**またはそのグループのメンバーとしてログオンし、アンチウイルスソフトウェアをインストールします。

3. ループバック接続を無効にします。詳細については、ループバック接続を無効にする（6 ページ）を参照してください。

4. McAfee VirusScan Enterprise 8.8 パッチ 9 の配備については、McAfee にお問い合わせいただき、INW Server にのみ UTN-USERFirst-Object および VeriSign ユニバーサルルート証明書をインストールしてください。証明書をインストールしたら、システムを再起動します。

注 : UTN-USERFirst-Object および VeriSign ユニバーサルルート証明書がインストールされていないと、INW Server への McAfee VirusScan Enterprise 8.8 パッチ 9 のインストールは失敗します。

5. 新規インストールの場合は、McAfee ePolicy Orchestrator Console で、次のエージェントのバージョンを McAfee ePolicy Orchestrator マスターリポジトリに追加します。***- McAfee Agent v5.0.5.658***

6. 新規インストールの場合は、以下のパッケージを McAfee ePolicy Orchestrator Console 内の McAfee ePolicy Orchestrator マスターレポジトリに追加します。

   - McAfee VirusScan Enterprise 8.8 パッチ 3：VSE880LMLRP3.ZIP（v8.8.0.1128）。

- McAfee VirusScan Enterprise 8.8 パッチ 4：VSE880LMLRP4.ZIP（v8.8.0.1247）。
- McAfee VirusScan Enterprise 8.8 パッチ 8：VSE880LMLRP8.ZIP（v8.8.0.1599）。
- McAfee VirusScan Enterprise 8.8 パッチ 9：VSE880MLRP9.ZIP（v8.8.0.1804）。

注： VSE880LMLRP3.zip にはパッチ 2 とパッチ 3 のインストールパッケージが含まれています。パッチ 2 は Windows 7 および Windows Server 2008 OS プラットフォーム用、パッチ 3 は Windows 8 および Windows Server 2012 OS プラットフォーム用です。McAfee インストーラーは Windows オペレーティングシステムのバージョンを特定することによって適切なパッチをインストールします。

7. 新規インストールの場合は、以下の拡張機能を McAfee ePolicy Orchestrator Console 内の McAfee ePolicy Orchestrator 拡張機能表に追加します。

   - McAfee VirusScan Enterprise 8.8 パッチ 3：VIRUSSCAN8800 v8.8.0.348 および VIRUSSCANREPORTS v1.2.0.228
   - McAfee VirusScan Enterprise 8.8 パッチ 4：VIRUSSCAN8800 v8.8.0.368 および VIRUSSCANREPORTS v1.2.0.236
   - McAfee VirusScan Enterprise 8.8 パッチ 8：VIRUSSCAN8800 v8.8.0.511 および VIRUSSCANREPORTS v1.2.0.311
   - McAfee VirusScan Enterprise 8.8 パッチ 9：VIRUSSCAN8800 v8.8.0.548 および VIRUSSCANREPORTS v1.2.0.346

注： VIRUSSCAN8800(348).zip と VIRUSSCANREPORTS120(228).zip は、McAfee VirusScan Enterprise 8.8 Patch 3 パッケージにあります。

VIRUSSCAN8800(368).zip と VIRUSSCANREPORTS120(236).zip は、McAfee VirusScan Enterprise 8.8 Patch 4 パッケージにあります。

VIRUSSCAN8800(511).zip と VIRUSSCANREPORTS120(311).zip は、McAfee VirusScan Enterprise 8.8 Patch 8 パッケージにあります。

VIRUSSCAN8800(548).zip と VIRUSSCANREPORTS120(346).zip は、McAfee VirusScan Enterprise 8.8 Patch 9 パッケージにあります。

McAfee ePolicy Orchestrator 5.0 または 5.3.2 - 新規インストール実装の手順（推奨プッシュインストールの方法）

1. ソフトウェアのバージョンに応じて、***Start*（スタート）> *All Programs*（すべてのプログラム）> *McAfee* > *ePolicy Orchestrator* > *Launch McAfee ePolicy Orchestrator 5.0.0 Console*（*McAfee ePolicy Orchestrator 5.0.0* コンソールの起動）**または ***Start*（スタート）> *All Programs*（すべてのプログラム）> *McAfee* > *ePolicy Orchestrator* > *Launch McAfee ePolicy Orchestrator 5.3.2 Console*（*McAfee ePolicy Orchestrator 5.3.2* コンソールの起動）**を選択し、ePolicy Orchestrator コンソールにログオンします。

注： ***Security Alert*（セキュリティアラート）**メッセージボックスが表示された場合は、***Continue with this website*（このサイトの閲覧を続行する）**をクリックします。

2. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。

3. ***Menu*（メニュー）> *Systems*（システム）> *Systems Tree*（システムツリー）**の順に選択します。Systems Tree（システムツリー）ウィンドウが開きます。

4. ***My Organization*（ユーザーの組織）**をクリックし、***My Organization*（ユーザーの組織）**をフォーカスして、画面の左隅から ***System Tree Actions*（システムツリーの操作）> *New Systems*（新規システム）**の順にクリックします。

5. ***Push agents and add systems to the current group (My Organization)*（エージェントをプッシュし、システムを現在のグループ（ユーザーの組織）に追加）**を選択し、対象のシステムで ***Browse*（参照）**をクリックします。

6. **ドメイン / ローカル管理者**のユーザー名とパスワードを入力し、***OK*** をクリックします。

7. ***Domain*（ドメイン）**ドロップダウンリストから ***INW*** ドメインを選択します。

8. ドメインに接続されているクライアントマシン（アクイジション、レビュー、INW Server）を選択して ***OK*** をクリックします。

注 : ドメイン名が ***Domain*（ドメイン）**ドロップダウンにない場合は、以下を行います。

- ***Browse for Systems*（システムの参照）**ウィンドウで ***Cancel*（キャンセル）**をクリックします。
- ***New Systems*（新規システム）**ウィンドウで、***Target systems*（ターゲットシステム）**フィールドにクライアントマシン（アクイジション、レビュー、INW Server）のシステム名を手動で入力し、次の手順を実行します。

9. ***Agent Version*（エージェントのバージョン）**に ***McAfee Agent for Windows 4.8.0*（現行）**または ***McAfee Agent for Windows 5.0.4*（現行）**を選択します。**ドメイン管理者**のユーザー名とパスワードを入力し、***OK*** をクリックします。

10. クライアントマシン（アクイジション、レビュー、INW Server）で、パッチのバージョンに応じてディレクトリが正しく作成されていることを確認してください。

- パッチ 3 とパッチ 4 については、***C:\Program Files\McAfee\Common Framework*** ディレクトリが存在し、McAfee Agent がそのディレクトリにインストールされていることを確認してください。

注 : INW Server については、***C:\Program Files (x86)\McAfee\Common Framework*** ディレクトリが存在し、McAfee Agent がそのディレクトリにインストールされていることを確認してください。

- パッチ 8 については、***C:\Program Files\McAfee\Agent*** ディレクトリが存在し、McAfee Agent がそのディレクトリにインストールされていることを確認してください。

注 : INW Server については、***C:\Program Files (x86)\McAfee\Common Framework*** ディレクトリが存在することを確認してください。

11. クライアントマシン（アクイジション、レビュー、INW Server）を再起動し、**ドメイン管理者**またはグループのメンバーとしてログオンします。

12. ソフトウェアのバージョンに応じて、***Start*（スタート）> *All Programs*（すべてのプログラム）> *McAfee* > *ePolicy Orchestrator* > *Launch McAfee ePolicy Orchestrator 5.0.0 Console*（*McAfee ePolicy Orchestrator 5.0.0* コンソールの起動）**または ***Start*（スタート）> *All Programs*（すべてのプログラム）> *McAfee* > *ePolicy Orchestrator* > *Launch McAfee ePolicy Orchestrator 5.3.2 Console*（*McAfee ePolicy Orchestrator 5.3.2* コンソールの起動）**をクリックします。

13. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。

14. ***Menu*（メニュー）> *Systems*（システム）> *Systems Tree*（システムツリー）**の順にクリックします。

15. ***My Organization*（ユーザーの組織）**をクリックし、***My Organization*（ユーザーの組織）**をフォーカスして、***Assigned Client Tasks*（割り当て済みクライアントタスク）**タブをクリックします。

16. 画面の下部で ***Actions*（操作）> *New Client Task Assignment*（新規クライアントタスクの割り当て）**ボタンをクリックします。Client Task Assignment Builder（クライアントタスク割り当てビルダー）画面が表示されます。

17. 以下を選択します。

    a. **Product（製品）:** McAfee Agent

    b. **Task Type（タスクの種類）:** 製品の実装

    c. **Task name（タスク名）:** 新規タスクの作成

18. ***Client Task Catalog: New Task- McAfee Agent: Product Deployment*（クライアントタスクカタログ：新規タスク *-McAfee Agent*：製品の実装）**画面で、次のフィールドに必要事項を入力します。

    a. **Task Name（タスク名）:** 適切なタスク名を入力します。

    b. **Target platforms（対象プラットフォーム）:** Wndows

    c. **Products and components（製品とコンポーネント）:** v6.9.6 用に認定されている VirusScan Enterprise のバージョン

    d. **Options（オプション）: *Options*（オプション）**が使用可能な場合は、各ポリシー適用時に実行してください（Windows のみ）。

19. ***Save*（保存）**をクリックします。

20. ***1 Select Task*（*1* 選択タスク）**画面で以下を選択します。

    a. **Product（製品）:** McAfee Agent

    b. **Task Type（タスクの種類）:** 製品の実装

    c. **Task Name（タスク名）:** 新規作成されたタスク名

21. ***Next*（次へ）**をクリックします。2 Schedule（2 スケジュール）画面が表示されます。

22. ***Schedule type*（スケジュールの種類）**ドロップダウンリストから ***Run immediately*（今すぐ実行）**を選択します。

23. ***Next*（次へ）**をクリックします。3 Summary（3 サマリ）画面が表示されます。

24. ***Save*（保存）**をクリックします。***System Tree*（システムツリー）**画面が表示されます。

25. ***Systems*（システム）**タブを選択し、次にドメインに接続されているすべてのクライアントマシン（アクイジション、レビュー、INW Server）を選択します。

26. ウィンドウの下部にある ***Wake up Agents*（エージェントを起動）**をクリックします。

27. デフォルト設定を維持し、***OK*** をクリックします。

28. システムトレイに McAfee アイコンが表示されるまで待ち、すべてのクライアントマシン（アクイジション、レビュー、INW Server）を再起動し、**管理者**またはグループのメンバーとしてすべてのクライアントマシンにログインします。

29. ***Log Off*（ログオフ）**リンクをクリックし、McAfee ePolicy Orchestrator Console を閉じます。

McAfee ePolicy Orchestrator 5.9.0 - 新規インストール実装の手順（推奨プッシュインストールの方法）

1. **スタート > すべてのプログラム >** ***McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** をクリックして、ePolicy Orchestrator コンソールにログオンします。

注 : ***Security Alert*（セキュリティアラート）**メッセージボックスが表示された場合は、***Continue with this website*（このサイトの閲覧を続行する）**をクリックします。

2. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。
3. ***Menu*（メニュー）> *Systems*（システム）> *Systems Tree*（システムツリー）**の順に選択します。***Systems Tree*（システムツリー）**ウィンドウが開きます。
4. ***My Organization*（ユーザーの組織）**をクリックし、***My Organization*（ユーザーの組織）**にフォーカスして、画面の一番上にある ***New Systems*（新規システム）**をクリックします。
5. ***Push agents and add systems to the current group (My Organization)*（エージェントをプッシュし、システムを現在のグループ（ユーザーの組織）に追加）**を選択し、対象のシステムで ***Browse*（参照）**をクリックします。
6. **ドメイン / ローカル管理者**のユーザー名とパスワードを入力し、***OK*** をクリックします。
7. ***Domain*（ドメイン）**ドロップダウンリストから ***INW*** ドメインを選択します。
8. ドメインに接続されているクライアントマシン（アクイジション、レビュー、INW Server）を選択して ***OK*** をクリックします。

注 : ドメイン名が ***Domain*（ドメイン）**ドロップダウンにない場合は、以下を行います。

- ***Browse for Systems*（システムの参照）**ウィンドウで ***Cancel*（キャンセル）**をクリックします。
- ***New Systems*（新規システム）**ウィンドウで、***Target systems*（ターゲットシステム）**フィールドにクライアントマシン（アクイジション、レビュー、INW Server）のシステム名をカンマで区切って手動で入力し、次の手順を実行します。

9. ***Agent Version*（エージェントのバージョン）**に ***McAfee Agent for Windows 5.0.5*（現行）**を選択します。**ドメイン管理者**のユーザー名とパスワードを入力し、***OK*** をクリックします。
10. クライアントマシン（アクイジション、レビュー、INW Server）で、***C:\Program Files\McAfee\Agent*** ディレクトリが正しく作成されたことを確認します。
11. クライアントマシン（アクイジション、レビュー、INW Server）を再起動し、**ドメイン管理者**またはグループのメンバーとしてログオンします。
12. **スタート > すべてのプログラム >** ***McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console*** をクリックして、ePolicy Orchestrator コンソールにログオンします。
13. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。
14. ***Menu*（メニュー）> *Systems*（システム）> *Systems Tree*（システムツリー）**の順にクリックします。

15. ***My Organization*（ユーザーの組織）**をクリックし、***My Organization*（ユーザーの組織）**をフォーカスして、***Assigned Client Tasks*（割り当て済みクライアントタスク）**タブをクリックします。

16. 画面の下部で ***Actions*（操作）> *New Client Task Assignment*（新規クライアントタスクの割り当て）**ボタンをクリックします。Client Task Assignment Builder（クライアントタスク割り当てビルダー）画面が表示されます。

17. 以下を選択します。

    a. **Product（製品）:** McAfee Agent

    b. **Task Type（タスクの種類）:** 製品の実装

18. ***Task Actions*（タスクの操作）> *Create New Task*（新規タスクの作成）**の順にクリックします。***Create New Task*（新規タスクの作成）**画面が表示されます。

19. ***Create New Task*（新規タスクの作成）**画面で、次のフィールドに入力します。

    a. **Task Name（タスク名）:** 適切なタスク名を入力します。

    b. **Target platforms（対象プラットフォーム）:** Windows（その他のオプションのチェックをすべてオフにする）

    c. **Products and components（製品とコンポーネント）:** VirusScan Enterprise 8.8.0.1804

20. ***Save*（保存）**をクリックします。***Client Task Assignment Builder*（クライアントタスク割り当てビルダー）**画面が表示されます。

21. ***Client Task Assignment Builder*（クライアントタスク割り当てビルダー）**画面で以下を選択します。

    a. **Product（製品）:** McAfee Agent

    b. **Task Type（タスクの種類）:** 製品の実装

    c. **Task Name（タスク名）:** 新規作成されたタスク名

    d. **Schedule Type（スケジュールの種類）:** Run immediately（今すぐ実行）

22. ***Save*（保存）**をクリックします。***Assigned Client Tasks*（割り当て済みクライアントタスク）**画面が表示されます。

23. ***Systems*（システム）**タブを選択し、次にドメインに接続されているすべてのクライアントマシン（アクイジション、レビュー、INW Server）を選択します。

24. ウィンドウの下部にある ***Wake up Agents*（エージェントを起動）**をクリックします。

25. デフォルト設定を維持し、***OK*** をクリックします。

26. システムトレイに McAfee アイコンが表示されるまで待ち、すべてのクライアントマシン（アクイジション、レビュー、INW Server）を再起動し、**管理者**またはグループのメンバーとしてすべてのクライアントマシンにログインします。

27. ***Log Off*（ログオフ）**リンクをクリックし、McAfee ePolicy Orchestrator Console を閉じます。

McAfee ePolicy Orchestrator 5.0 および 5.3.2 サーバーコンソールの設定

1. ソフトウェアのバージョンに応じて、***Start*（スタート）> *All Programs*（すべてのプログラム）> *McAfee* > *ePolicy Orchestrator* > *Launch McAfee ePolicy Orchestrator 5.0.0 Console*（*McAfee ePolicy Orchestrator 5.0.0* コンソールの起動）**または ***Start*（スタート）> *All Programs*（すべてのプログラム）> *McAfee* > *ePolicy Orchestrator* > *Launch McAfee ePolicy Orchestrator 5.3.2 Console*（*McAfee ePolicy Orchestrator 5.3.2* コンソールの起動）**をクリックします。
2. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。
3. ***Menu*（メニュー）> *Systems*（システム）> *Systems Tree*（システムツリー）**の順にクリックします。
4. ***My Organization*（ユーザーの組織）**をクリックし、My Organization（ユーザーの組織）をフォーカスして、***Assigned Client Tasks*（割り当て済みクライアントタスク）**タブをクリックします。
5. 画面の下部で ***Actions*（アクション）> *New Client Task Assignment*（新規クライアントタスクの割り当て）**ボタンをクリックします。***Client Task Assignment Builder*（クライアントタスク割り当てビルダー）**画面が表示されます。
6. 以下を選択します。
   a. ***Product*（製品）：**VirusScan Enterprise 8.8.0
   b. ***Task Type*（タスクの種類）：**オンデマンドスキャン
   c. ***Task name*（タスク名）：**新規タスクの作成
7. ***Client Task Catalog: New Task - VirusScan Enterprise 8.8.0: On Demand Scan*（クライアントタスクカタログ：新規タスク *-VirusScan Enterprise 8.8.0*：オンデマンドスキャン）**画面で、次のフィールドに必要事項を入力します。
   a. ***Task Name*（タスク名）：**週 1 回の定期的なスキャン
   b. ***Description*（説明）：**週 1 回の定期的なスキャン
8. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。
9. ***Options*（オプション）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。
10. Heuristics（ヒューリスティック）で以下のオプションの選択を解除します。
    - ***Find unknown program threats*（不明なプログラムの脅威を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**
11. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。
12. ***Add*（追加）**をクリックします。***Add/Edit Exclusion*（除外対象の追加 / 編集）**項目画面が表示されます。
13. ***By pattern*（パターン別）**を選択し、**C:\Program Files\GE Healthcare\MLCL**、**C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** フォルダを

1 つずつ入力し、Also exclude subfolders（サブフォルダも除外）を選択します。***OK*** をクリックします。

14. ***Performance*（パフォーマンス）**タブをクリックします。***Performance*（パフォーマンス）**画面が表示されます。
15. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑わしいファイルのヒューリスティックネットワークチェック）**から ***Disabled*（無効）**を選択します。
16. ***Save*（保存）**をクリックします。
17. ***1 Select Task*（*1* 選択タスク）**画面で以下を選択します。
    - ***Product*（製品）:** VirusScan Enterprise 8.8.0
    - ***Task Type*（タスクの種類）:** オンデマンドスキャン
    - ***Task Name*（タスク名）:** 週 1 回の定期的なスキャン
18. ***Next*（次へ）**をクリックします。***2 Schedule*（*2* スケジュール）**画面が表示されます。
19. ***Scheduled type*（スケジュールの種類）**ドロップダウンリストから ***Weekly*（週 *1* 回）**を選択し、***Sunday*（日曜日）**を選択します。
20. ***Start time*（開始時刻）**を ***12:00 AM*** に設定し、***Run Once at that time*（その時に *1* 回実行）**を選択します。
21. ***Next*（次へ）**をクリックします。***3 Summary*（*3* サマリ）**画面が表示されます。
22. ***Save*（保存）**をクリックします。***System Tree*（システムツリー）**画面が表示されます。
23. ***Assigned Policies*（割り当て済みポリシー）**タブを選択します。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。
24. ***Product*（製品）**ドロップダウンリストから ***VirusScan Enterprise 8.8.0*** を選択します。
25. ***On-Access General Policies*（オンアクセスの全般ポリシー）**の ***My Default*（デフォルト）**をクリックします。***VirusScan Enterprise 8.8.0* > *On-Access General Policies*（オンアクセスの全般ポリシー）> *My Default*（マイデフォルト）**画面が表示されます。
26. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択し、***General*（全般）**タブをクリックします。***General*（全般）**画面が表示されます。
27. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑わしいファイルのヒューリスティックネットワークチェック）**から ***Disabled*（無効）**を選択します。
28. ***ScriptScan*（スクリプトスキャン）**タブをクリックします。***ScriptScan*（スクリプトスキャン）**画面が表示されます。
29. ***Enable scanning of scripts*（スクリプトスキャンを有効にする）**の選択を解除します。
30. ***Blocking*（ブロック）**タブをクリックします。***Blocking*（ブロック）**画面が表示されます。
31. ***Block the connection when a threatened file is detected in a shared folder*（共有ファイルで危険なファイルが検出された場合に接続を遮断する）**の選択を解除します。
32. ***Messages*（メッセージ）**タブを選択します。***Messages*（メッセージ）**画面が表示されます。

33. ***Show the messages dialog box when a threat is detected and display the specified text in the message*（脅威が検出されたときにメッセージダイアログボックスを表示し、メッセージに指定されたテキストを表示する）**の選択を解除します。

34. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択し、***General*（全般）**タブをクリックします。***General*（全般）**画面が表示されます。

35. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑わしいファイルのヒューリスティックネットワークチェック）**から ***Disabled*（無効）**を選択します。

36. ***ScriptScan*（スクリプトスキャン）**タブを選択します。***ScriptScan*（スクリプトスキャン）**画面が表示されます。

37. ***Enable scanning of scripts*（スクリプトスキャンを有効にする）**の選択が解除されていることを確認します。

38. ***Blocking*（ブロック）**タブをクリックします。***Blocking*（ブロック）**画面が表示されます。

39. ***Block the connection when a threatened file is detected in a shared folder*（共有ファイルで危険なファイルが検出された場合に接続を遮断する）**の選択を解除します。

40. ***Messages*（メッセージ）**タブを選択します。***Messages*（メッセージ）**画面が表示されます。

41. ***Show the messages dialog box when a threat is detected and display the specified text in the message*（脅威が検出されたときにメッセージダイアログボックスを表示し、メッセージに指定されたテキストを表示する）**の選択を解除します。

42. ***Save*（保存）**をクリックします。

43. ***On-Access Default Processes Policies*（オンアクセスデフォルトプロセスポリシー）**の***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0* > *On-Access Default Policies*（オンアクセスのデフォルトポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

44. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

45. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。

46. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。

    - ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

47. ***Detect unwanted programs*（不要なプログラムの検出）**で ***Detect unwanted programs*（不要なプログラムの検出）**の選択を解除します。

48. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。

49. ***Add*（追加）**をクリックします。***Add/Edit Exclusion Item*（除外対象項目の追加 / 編集）**画面が表示されます。

50. ***By pattern*（パターン別）**を選択し、**C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。

51. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択し、***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。

52. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。

    - ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

53. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。

54. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。

55. ***Add*（追加）**をクリックします。***Add/Edit Exclusion Item*（除外対象項目の追加 / 編集）**画面が表示されます。

56. ***By pattern*（パターン別）**を選択し、**C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。

57. ***Save*（保存）**をクリックします。

58. ***On-Access Low-Risk Processes Policies*（オンアクセス低リスクプロセスポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies*（オンアクセス低リスクプロセスポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

59. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

60. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。

61. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。

    - ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

62. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。

63. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。

64. ***Add*（追加）**をクリックします。***Add/Edit Exclusion*（除外対象の追加 / 編集）**項目画面が表示されます。

65. ***By pattern*（パターン別）**を選択し、**C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。

66. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択し、***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。

67. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。

- ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
- ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

68. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。
69. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。
70. ***Add*（追加）**をクリックします。***Add/Edit Exclusion*（除外対象の追加 / 編集）**項目画面が表示されます。
71. ***By pattern*（パターン別）**を選択し、**C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。
72. ***Save*（保存）**をクリックします。
73. ***On-Access High-Risk Processes Policies*（オンアクセス高リスクプロセスポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies*（オンアクセス高リスクプロセスポリシー）> *My Default*（マイデフォルト）**画面が表示されます。
74. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。
75. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。
76. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。
    - ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**
77. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。
78. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。
79. ***Add*（追加）**をクリックします。***Add/Edit Exclusion*（除外対象の追加 / 編集）**項目画面が表示されます。
80. ***By pattern*（パターン別）**を選択し、**C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。
81. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択し、***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。
82. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。
    - ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

83. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。
84. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。
85. ***Add*（追加）**をクリックします。***Add/Edit Exclusion*（除外対象の追加 / 編集）**項目画面が表示されます。
86. By pattern（パターン別）を選択し、**C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。
87. ***Save*（保存）**をクリックします。
88. ***On Delivery Email Scan Policies*（オンデリバリー *E* メールスキャンポリシー）**の ***My Default(*デフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies*（オンデリバリー *E* メールスキャンポリシー > *My Default*（マイデフォルト）**画面が表示されます。
89. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。
90. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。
91. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。
    - ***Find unknown unwanted programs and trojans*（未知のプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**
    - ***Find attachments with multiple extensions*（複数の拡張子を持つ添付ファイルを検出する）。**
92. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。
93. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑わしいファイルのヒューリスティックネットワークチェック）**から ***Disabled*（無効）**を選択します。
94. ***Scanning of email*（*E* メールのスキャン）**で ***Enable on-delivery email scanning*（オンデリバリー *E* メールスキャンの有効可）**チェックボックスをオフにします。
95. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択します。
96. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。
97. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。
    - ***Find unknown unwanted programs and trojans*（未知のプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**
    - ***Find attachments with multiple extensions*（複数の拡張子を持つ添付ファイルを検出する）。**
98. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。

99. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑わしいファイルのヒューリスティックネットワークチェック）**から ***Disabled*（無効）**を選択します。

100. ***Scanning of email*（*E* メールのスキャン）**で ***Enable on-delivery email scanning*（オンデリバリー *E* メールスキャンの有効可）**チェックボックスをオフにします。

101. ***Save*（保存）**をクリックします。

102. ***General Options Policies*（全般オプションポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0* > *General Options Policies*（全般オプションポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

103. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

104. ***Display Options*（オプションの表示）**タブをクリックします。***Display Options*（オプションの表示）**画面が表示されます。

105.***Console options*（コンソールオプション）**で以下を選択します。

- ***Display managed tasks in the client console*（クライアントコンソールに管理対象タスクを表示する）。**
- ***Disable default AutoUpdate task schedule*（デフォルトの *AutoUpdate*（自動アップデート）タスクスケジュールを無効にする）。**

106.***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択します。

107.***Display Options*（オプションの表示）**タブをクリックします。***Display Options*（オプションの表示）**画面が表示されます。

108. ***Console options*（コンソールオプション）**で以下を選択します。

- ***Display managed tasks in the client console*（クライアントコンソールに管理対象タスクを表示する）。**
- ***Disable default AutoUpdate task schedule*（デフォルトの *AutoUpdate*（自動アップデート）タスクスケジュールを無効にする）。**

109. ***Save*（保存）**をクリックします。

110. ***Alert Policies*（アラートポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0* > *Alter Policies*（変更ポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

111. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

112. ***Alert Manager Alerts*（*Alert Manager* による通知）**タブをクリックします。***Alert Manager Alerts(Alert Manager* による通知）**画面が開きます。

113. ***Components that generate alerts*（通知を生成するコンポーネント）**で、***On-Access Scan*（オンアクセススキャン）**、***On-Demand Scan and scheduled scans*（オンデマンドスキャンと予約スキャン）**、***Email Scan*（*E-mail* スキャン）**、***AutoUpdate*（自動アップデート）**の選択を解除します。

114. ***Alert Manager*（アラートマネージャ）**のオプションで ***Disable alerting*（アラートの通知を無効にする）**を選択します。

115. ***Components that generate alerts*（通知を生成するコンポーネント）**で ***Access Protection*（アクセス保護）**の選択を解除します。

116. ***Additional Alerting Options*（その他のアラートオプション）**をクリックします。***Additional Alerting Options*（その他のアラートオプション）**画面が表示されます。

117. ***Severity Filters*（重要度フィルタ）**ドロップダウンメニューから、***Suppress all alerts (severities 0 to 4)*（すべてのアラートを送信しない（重要度 *0 ～ 4*））**を選択します。

118. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択し、***Alert Manager Alerts*（*Alert Manager* による通知）**タブを選択します。***Alert Manager Alerts*（*Alert Manager* による通知）**画面が開きます。

119. ***Components that generate alerts*（通知を生成するコンポーネント）**で、***On-Access Scan*（オンアクセススキャン）**、***On-Demand Scan and scheduled scans*（オンデマンドスキャンと予約スキャン）**、***Email Scan*（*E-mail* スキャン）**、***AutoUpdate*（自動アップデート）**の選択を解除します。

120. ***Alert Manager*（アラートマネージャ）**のオプションで ***Disable alerting*（アラートの通知を無効にする）**を選択します。

121. ***Components that generate alerts*（通知を生成するコンポーネント）**で ***Access Protection*（アクセス保護）**の選択を解除します。

122. ***Additional Alerting Options*（その他のアラートオプション）**をクリックします。Additional Alerting Options（その他のアラートオプション）画面が表示されます。

123. ***Severity Filters*（重要度フィルタ）**ドロップダウンメニューから、***Suppress all alerts (severities 0 to 4)*（すべてのアラートを送信しない（重要度 *0 ～ 4*））**を選択します。

124. ***Save*（保存）**をクリックします。

125. ***On-Access General Policies*（オンアクセスの全般ポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > Access Protection Policies*（アクセス保護ポリシー）*> My Default*（マイデフォルト）**画面が表示されます。

126. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

127. ***Access Protection*（アクセス保護）**タブをクリックします。***Access Protection*（アクセス保護）**画面が表示されます。

128. ***Access protection settings*（アクセス保護設定）**で以下のオプションの選択を解除します。

    - ***Enable access protection*（アクセス保護を有効にする）。**
    - ***Prevent McAfee services from being stopped*（*McAfee* サービスの停止を阻止する）。**

129. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択します。

130. ***Access Protection*（アクセス保護）**タブをクリックします。***Access Protection*（アクセス保護）**画面が表示されます。

131. ***Access protection settings*（アクセス保護設定）**で以下のオプションの選択を解除します。

    - ***Enable access protection*（アクセス保護を有効にする）。**
    - ***Prevent McAfee services from being stopped*（*McAfee* サービスの停止を阻止する）。**

132. ***Save*（保存）**をクリックします。

133. ***Buffer Overflow Protection Policies*（バッファオーバーフロー保護ポリシー）の *My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies*（バッファオーバーフロー保護ポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

134. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

135. ***Buffer Overflow Protection*（バッファオーバーフロー保護）**タブをクリックします。***Buffer Overflow Protection*（バッファオーバーフロー保護）**画面が表示されます。

136. ***Client system warning*（クライアントシステムの警告）**で、***Show the messages dialog box when a buffer overflow is detected*（バッファオーバーフローが検出されたときにメッセージダイアログボックスを表示する）**の選択を解除します。

137. ***Buffer overflow settings*（バッファオーバーフローの設定）**で ***Enable buffer overflow protection*（バッファオーバーフロー保護を有効にする）**の選択を解除します。

138. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択します。

139. ***Buffer Overflow Protection*（バッファオーバーフロー保護）**タブをクリックします。***Buffer Overflow Protection(* バッファオーバーフロー保護）**画面が表示されます。

140. ***Client system warning*（クライアントシステムの警告）**で、***Show the messages dialog box when a buffer overflow is detected*（バッファオーバーフローが検出されたときにメッセージダイアログボックスを表示する）**の選択を解除します。

141. ***Buffer overflow settings*（バッファオーバーフローの設定）**で ***Enable buffer overflow protection*（バッファオーバーフロー保護を有効にする）**の選択を解除します。

142. ***Save*（保存）**をクリックします。

143. ***Product*（製品）**ドロップダウンメニューから、***McAfee Agent*** を選択します。McAfee Agent の ***Policies*（ポリシー）**ウィンドウが表示されます。

144. ***Repository*（リポジトリ）**の ***My Default*（マイデフォルト）**をクリックします。***McAfee Agent > Repository*（リポジトリ）> *My Default*（マイデフォルト）**画面が表示されます。

145. ***Proxy*（プロキシ）**タブをクリックします。***Proxy*（プロキシ）**画面が表示されます。

146. ***Proxy settings*（プロキシ設定）**で、***Use Internet Explorer settings (For Windows)/ System Preferences settings (For Mac OSX)*（*Internet Explorer* の設定（*Windows*）/ システム設定管理の設定（*Mac OSX*）を使用する）**を選択します。

147. ***Save*（保存）**をクリックします。

148. ***Systems*（システム）**タブをクリックします。

149. 設定済みポリシーを配備するすべてのクライアントシステム（アクイジション、レビュー用、および Centricity Cardiology INW サーバー）を選択します。

150. ***Wake Up Agents*（ウェイクアップエージェント）**を選択します。***Wake Up Agents*（ウェイクアップエージェント）**画面が表示されます。

151. ***OK*** をクリックします。

152. ePolicy Orchestrator からログオフします。

McAfee ePolicy Orchestrator 5.9.0 サーバーコンソールの設定

1. ソフトウェアのバージョンに応じて、**スタート > すべてのプログラム > *McAfee* > *ePolicy Orchestrator* > *Launch McAfee ePolicy Orchestrator 5.9.0 Console*（*McAfee ePolicy Orchestrator 5.9.0* コンソールの起動）**を選択します。
2. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。
3. ***Menu*（メニュー）> *Systems*（システム）> *Systems Tree*（システムツリー）**の順にクリックします。
4. ***My Organization*（ユーザーの組織）**をクリックし、My Organization（ユーザーの組織）をフォーカスして、***Assigned Client Tasks*（割り当て済みクライアントタスク）**タブをクリックします。
5. 画面の下部で ***Actions*（アクション）> *New Client Task Assignment*（新規クライアントタスクの割り当て）**ボタンをクリックします。***Client Task Assignment Builder*（クライアントタスク割り当てビルダー）**画面が表示されます。
6. 以下を選択します。
   a. ***Product*（製品）:** VirusScan Enterprise 8.8.0
   b. ***Task Type*（タスクの種類）:** オンデマンドスキャン
7. ***Task Actions*（タスクの操作）**で ***Create New Task*（新規タスクの作成）**をクリックします。***Create New Task*（新規タスクの作成）**画面が表示されます。
8. ***Create New Task*（新規タスクの作成）**画面で、次のフィールドに入力します。
   a. ***Task Name*（タスク名）:** 週 1 回の定期的なスキャン
   b. ***Description*（説明）:** 週 1 回の定期的なスキャン
9. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。
10. ***Options*（オプション）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。
11. Heuristics（ヒューリスティック）で以下のオプションの選択を解除します。
    - ***Find unknown program threats*（不明なプログラムの脅威を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**
12. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。
13. ***Add*（追加）**をクリックします。***Add/Edit Exclusion*（除外対象の追加 / 編集）**項目画面が表示されます。
14. ***By pattern*（パターン別）**を選択し、**C:\Program Files\GE Healthcare\MLCL**、**C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** フォルダを 1 つずつ入力し、Also exclude subfolders（サブフォルダも除外）を選択します。***OK*** をクリックします。
15. ***Performance*（パフォーマンス）**タブをクリックします。***Performance*（パフォーマンス）**画面が表示されます。

16. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑わしいファイルのヒューリスティックネットワークチェック）**から ***Disabled*（無効）**を選択します。
17. ***Save*（保存）**をクリックします。***Client Task Assignment Builder*（クライアントタスク割り当てビルダー）**画面が表示されます。
18. Client Task Assignment Builder（クライアントタスク割り当てビルダー）画面で以下を選択します。
    - ***Product*（製品）：**VirusScan Enterprise 8.8.0
    - ***Task Type*（タスクの種類）：**オンデマンドスキャン
    - ***Task Name*（タスク名）：**週 1 回の定期的なスキャン
19. ***Scheduled type*（スケジュールの種類）**ドロップダウンリストから ***Weekly*（週 *1* 回）**を選択し、***Sunday*（日曜日）**を選択します。
20. ***Start time*（開始時刻）**を ***12:00 AM*** に設定し、***Run Once at that time*（その時に *1* 回実行）**を選択します。
21. ***Save*（保存）**をクリックします。***Assigned Client Tasks*（割り当て済みクライアントタスク）**画面が表示されます。
22. ***Assigned Policies*（割り当て済みポリシー）**タブを選択します。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。
23. ***Product*（製品）**ドロップダウンリストから ***VirusScan Enterprise 8.8.0*** を選択します。
24. ***On-Access General Policies*（オンアクセスの全般ポリシー）**の ***My Default*（デフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > On-Access General Policies*（オンアクセスの全般ポリシー）*> My Default*（マイデフォルト）**画面が表示されます。
25. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択し、***General*（全般）**タブをクリックします。***General*（全般）**画面が表示されます。
26. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑わしいファイルのヒューリスティックネットワークチェック）**から ***Disabled*（無効）**を選択します。
27. ***ScriptScan*（スクリプトスキャン）**タブをクリックします。***ScriptScan*（スクリプトスキャン）**画面が表示されます。
28. ***Enable scanning of scripts*（スクリプトスキャンを有効にする）**の選択を解除します。
29. ***Blocking*（ブロック）**タブをクリックします。***Blocking*（ブロック）**画面が表示されます。
30. ***Block the connection when a threatened file is detected in a shared folder*（共有ファイルで危険なファイルが検出された場合に接続を遮断する）**の選択を解除します。
31. ***Messages*（メッセージ）**タブを選択します。***Messages*（メッセージ）**画面が表示されます。
32. ***Show the messages dialog box when a threat is detected and display the specified text in the message*（脅威が検出されたときにメッセージダイアログボックスを表示し、メッセージに指定されたテキストを表示する）**の選択を解除します。
33. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択し、***General*（全般）**タブをクリックします。***General*（全般）**画面が表示されます。

34. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑わしいファイルのヒューリスティックネットワークチェック）**から ***Disabled*（無効）**を選択します。

35. ***ScriptScan*（スクリプトスキャン）**タブを選択します。***ScriptScan*（スクリプトスキャン）**画面が表示されます。

36. ***Enable scanning of scripts*（スクリプトスキャンを有効にする）**の選択が解除されていることを確認します。

37. ***Blocking*（ブロック）**タブをクリックします。***Blocking*（ブロック）**画面が表示されます。

38. ***Block the connection when a threatened file is detected in a shared folder*（共有ファイルで危険なファイルが検出された場合に接続を遮断する）**の選択を解除します。

39. ***Messages*（メッセージ）**タブを選択します。***Messages*（メッセージ）**画面が表示されます。

40. ***Show the messages dialog box when a threat is detected and display the specified text in the message*（脅威が検出されたときにメッセージダイアログボックスを表示し、メッセージに指定されたテキストを表示する）**の選択を解除します。

41. ***Save*（保存）**をクリックします。Assigned Policies（割り当て済みポリシー）画面が表示されます。

42. ***On-Access Default Processes Policies*（オンアクセスデフォルトプロセスポリシー）**の***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0* > *On-Access Default Policies*（オンアクセスのデフォルトポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

43. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

44. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。

45. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。

    - ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

46. ***Detect unwanted programs*（不要なプログラムの検出）**で ***Detect unwanted programs*（不要なプログラムの検出）**の選択を解除します。

47. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。

48. ***Add*（追加）**をクリックします。***Add/Edit Exclusion Item*（除外対象項目の追加 / 編集）**画面が表示されます。

49. ***By pattern*（パターン別）**を選択し、**C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。

50. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択し、***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。

51. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。

- ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
- ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

52. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。
53. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。
54. ***Add*（追加）**をクリックします。***Add/Edit Exclusion Item*（除外対象項目の追加 / 編集）**画面が表示されます。
55. ***By pattern*（パターン別）**を選択し、**C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。
56. ***Save*（保存）**をクリックします。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。
57. ***On-Access Low-Risk Processes Policies*（オンアクセス低リスクプロセスポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies*（オンアクセス低リスクプロセスポリシー）> *My Default*（マイデフォルト）**画面が表示されます。
58. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。
59. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。
60. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。
    - ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**
61. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。
62. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。
63. ***Add*（追加）**をクリックします。***Add/Edit Exclusion*（除外対象の追加 / 編集）**項目画面が表示されます。
64. ***By pattern*（パターン別）**を選択し、**C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。
65. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択し、***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。
66. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。
    - ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

67. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。

68. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。

69. ***Add*（追加）**をクリックします。***Add/Edit Exclusion*（除外対象の追加 / 編集）**項目画面が表示されます。

70. ***By pattern*（パターン別）**を選択し、**C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。

71. ***Save*（保存）**をクリックします。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。

72. ***On-Access High-Risk Processes Policies*（オンアクセス高リスクプロセスポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies*（オンアクセス高リスクプロセスポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

73. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

74. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。

75. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。

    - ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

76. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。

77. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。

78. ***Add*（追加）**をクリックします。***Add/Edit Exclusion*（除外対象の追加 / 編集）**項目画面が表示されます。

79. ***By pattern*（パターン別）**を選択し、**C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。

80. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択し、***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。

81. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。

    - ***Find unknown unwanted programs and trojans*（未知の望ましくないプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**

82. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。

83. ***Exclusions*（除外対象）**タブをクリックします。***Exclusions*（除外対象）**画面が表示されます。

84. ***Add*（追加）**をクリックします。***Add/Edit Exclusion*（除外対象の追加 / 編集）**項目画面が表示されます。

85. By pattern（パターン別）を選択し、**C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** フォルダを 1 つずつ入力し、***Also exclude subfolders*（サブフォルダも除外）**を選択します。***OK*** をクリックします。

86. ***Save*（保存）**をクリックします。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。

87. ***On Delivery Email Scan Policies*（オンデリバリー *E* メールスキャンポリシー）**の ***My Default*（デフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies*（オンデリバリー *E* メールスキャンポリシー > *My Default*（マイデフォルト）**画面が表示されます。

88. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

89. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。

90. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。

    - ***Find unknown unwanted programs and trojans*（未知のプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**
    - ***Find attachments with multiple extensions*（複数の拡張子を持つ添付ファイルを検出する）。**

91. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。

92. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑わしいファイルのヒューリスティックネットワークチェック）**から ***Disabled*（無効）**を選択します。

93. ***Scanning of email*（*E* メールのスキャン）**で ***Enable on-delivery email scanning*（オンデリバリー *E* メールスキャンの有効可）**チェックボックスをオフにします。

94. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択します。

95. ***Scan Items*（スキャン項目）**タブをクリックします。***Scan Items*（スキャン項目）**画面が表示されます。

96. ***Heuristics*（ヒューリスティック）**で以下のオプションの選択を解除します。

    - ***Find unknown unwanted programs and trojans*（未知のプログラムとトロイの木馬を検出する）。**
    - ***Find unknown macro threats*（不明なマクロの脅威を検出する）。**
    - ***Find attachments with multiple extensions*（複数の拡張子を持つ添付ファイルを検出する）。**

97. ***Detect unwanted programs*（望ましくないプログラムの検出）**で ***Detect unwanted programs*（望ましくないプログラムの検出）**の選択を解除します。

98. ***Artemis (Heuristic network check for suspicious files)*（*Artemis*（疑わしいファイルのヒューリスティックネットワークチェック）**から ***Disabled*（無効）**を選択します。

99. ***Scanning of email*（*E* メールのスキャン）で ***Enable on-delivery email scanning*（オンデリバリー *E* メールスキャンの有効可）**チェックボックスをオフにします。

100. ***Save*（保存）**をクリックします。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。

101. ***General Options Policies*（全般オプションポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0* > *General Options Policies*（全般オプションポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

102. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

103. ***Display Options*（オプションの表示）**タブをクリックします。***Display Options*（オプションの表示）**画面が表示されます。

104. ***Console options*（コンソールオプション）**で以下を選択します。

- ***Display managed tasks in the client console*（クライアントコンソールに管理対象タスクを表示する）。**
- ***Disable default AutoUpdate task schedule*（デフォルトの *AutoUpdate*（自動アップデート）タスクスケジュールを無効にする）。**

105. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択します。

106. ***Display Options*（オプションの表示）**タブをクリックします。***Display Options*（オプションの表示）**画面が表示されます。

107. ***Console options*（コンソールオプション）**で以下を選択します。

- ***Display managed tasks in the client console*（クライアントコンソールに管理対象タスクを表示する）。**
- ***Disable default AutoUpdate task schedule*（デフォルトの *AutoUpdate*（自動アップデート）タスクスケジュールを無効にする）。**

108. ***Save*（保存）**をクリックします。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。

109. ***Alert Policies*（アラートポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0* > *Alter Policies*（変更ポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

110. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

111. ***Alert Manager Alerts*（*Alert Manager* による通知）**タブをクリックします。***Alert Manager Alerts*（*Alert Manager* による通知）**画面が開きます。

112. ***Components that generate alerts*（通知を生成するコンポーネント）**で、***On-Access Scan*（オンアクセススキャン）**、***On-Demand Scan and scheduled scans*（オンデマンドスキャンと予約スキャン）**、***Email Scan*（*E-mail* スキャン）**、***AutoUpdate*（自動アップデート）**の選択を解除します。

113. ***Alert Manager*（アラートマネージャ）**のオプションで ***Disable alerting*（アラートの通知を無効にする）**を選択します。

114. ***Components that generate alerts*（通知を生成するコンポーネント）**で ***Access Protection*（アクセス保護）**の選択を解除します。

115. ***Additional Alerting Options*（その他のアラートオプション）**をクリックします。***Additional Alerting Options*（その他のアラートオプション）**画面が表示されます。

116. ***Severity Filters*（重要度フィルタ）**ドロップダウンメニューから、***Suppress all alerts (severities 0 to 4)*（すべてのアラートを送信しない（重要度 *0 ～ 4*））**を選択します。

117. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択し、***Alert Manager Alerts*（*Alert Manager* による通知）**タブを選択します。***Alert Manager Alerts(Alert Manager* による通知）**画面が開きます。

118. ***Components that generate alerts*（通知を生成するコンポーネント）**で、***On-Access Scan*（オンアクセススキャン）**、***On-Demand Scan and scheduled scans*（オンデマンドスキャンと予約スキャン）**、***Email Scan*（*E-mail* スキャン）**、***AutoUpdate*（自動アップデート）**の選択を解除します。

119. ***Alert Manager*（アラートマネージャ）**のオプションで ***Disable alerting*（アラートの通知を無効にする）**を選択します。

120. ***Components that generate alerts*（通知を生成するコンポーネント）**で ***Access Protection*（アクセス保護）**の選択を解除します。

121. ***Additional Alerting Options*（その他のアラートオプション）**をクリックします。Additional Alerting Options（その他のアラートオプション）画面が表示されます。

122. ***Severity Filters*（重要度フィルタ）**ドロップダウンメニューから、***Suppress all alerts (severities 0 to 4)*（すべてのアラートを送信しない（重要度 *0 ～ 4*））**を選択します。

123. ***Save*（保存）**をクリックします。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。

124. ***On-Access General Policies*（オンアクセスの全般ポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > Access Protection Policies*（アクセス保護ポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

125. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

126. ***Access Protection*（アクセス保護）**タブをクリックします。***Access Protection*（アクセス保護）**画面が表示されます。

127. ***Access protection settings*（アクセス保護設定）**で以下のオプションの選択を解除します。

    - ***Enable access protection*（アクセス保護を有効にする）。**
    - ***Prevent McAfee services from being stopped*（*McAfee* サービスの停止を阻止する）。**
    - **拡張自己保護の有効化**

128. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択します。

129. ***Access Protection*（アクセス保護）**タブをクリックします。***Access Protection*（アクセス保護）**画面が表示されます。

130. ***Access protection settings*（アクセス保護設定）**で以下のオプションの選択を解除します。

    - ***Enable access protection*（アクセス保護を有効にする）。**
    - ***Prevent McAfee services from being stopped*（*McAfee* サービスの停止を阻止する）。**

■ **拡張自己保護の有効化**

131. ***Save*（保存）**をクリックします。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。

132. ***Buffer Overflow Protection Policies*（バッファオーバーフロー保護ポリシー）**の ***My Default*（マイデフォルト）**をクリックします。***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies*（バッファオーバーフロー保護ポリシー）> *My Default*（マイデフォルト）**画面が表示されます。

133. ***Settings for*（設定対象）**ドロップダウンリストから ***Workstation*（ワークステーション）**を選択します。

134. ***Buffer Overflow Protection*（バッファオーバーフロー保護）**タブをクリックします。***Buffer Overflow Protection(* バッファオーバーフロー保護）**画面が表示されます。

135. ***Client system warning*（クライアントシステムの警告）**で、***Show the messages dialog box when a buffer overflow is detected*（バッファオーバーフローが検出されたときにメッセージダイアログボックスを表示する）**の選択を解除します。

136. ***Buffer overflow settings*（バッファオーバーフローの設定）**で ***Enable buffer overflow protection*（バッファオーバーフロー保護を有効にする）**の選択を解除します。

137. ***Settings for*（設定対象）**ドロップダウンリストから ***Server*（サーバー）**を選択します。

138. ***Buffer Overflow Protection*（バッファオーバーフロー保護）**タブをクリックします。***Buffer Overflow Protection(* バッファオーバーフロー保護）**画面が表示されます。

139. ***Client system warning*（クライアントシステムの警告）**で、***Show the messages dialog box when a buffer overflow is detected*（バッファオーバーフローが検出されたときにメッセージダイアログボックスを表示する）**の選択を解除します。

140. ***Buffer overflow settings*（バッファオーバーフローの設定）**で ***Enable buffer overflow protection*（バッファオーバーフロー保護を有効にする）**の選択を解除します。

141. ***Save*（保存）**をクリックします。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。

142. ***Product*（製品）**ドロップダウンメニューから、***McAfee Agent*** を選択します。McAfee Agent の ***Policies*（ポリシー）**ウィンドウが表示されます。

143. ***Repository*（リポジトリ）**の ***My Default*（マイデフォルト）**をクリックします。***McAfee Agent > Repository*（リポジトリ）> *My Default*（マイデフォルト）**画面が表示されます。

144. ***Proxy*（プロキシ）**タブをクリックします。***Proxy*（プロキシ）**画面が表示されます。

145. ***Proxy settings*（プロキシ設定）**で、***Use Internet Explorer settings (For Windows)/ System Preferences settings (For Mac OSX)*（*Internet Explorer* の設定（*Windows*）/ システム設定管理の設定（*Mac OSX*）を使用する）**が選択されていることを確認します。

146. ***Save*（保存）**をクリックします。***Assigned Policies*（割り当て済みポリシー）**画面が表示されます。

147. ***Systems*（システム）**タブをクリックします。

148. 設定済みポリシーを配備するすべてのクライアントシステム（アクイジション、レビュー用、および Centricity Cardiology INW サーバー）を選択します。

149. ***Wake Up Agents*（ウェイクアップエージェント）**を選択します。***Wake Up Agents*（ウェイクアップエージェント）**画面が表示されます。

150. ***OK*** をクリックします。

151. ePolicy Orchestrator からログオフします。

McAfee ePolicy Orchestrator インストール後のガイドライン

ループバック接続を有効にします。詳細については、ループバック接続を有効にする（6 ページ）を参照してください。

Trend Micro OfficeScan Client/Server Edition 10.6 SP2

インストール概要

Trend Micro OfficeScan Client/Server Edition は必ずネットワーク上の Mac-Lab/CardioLab 環境でインストールします。Trend Micro OfficeScan は、Anti-Virus Management Console サーバーにインストールしてから、Centricity Cardiology INW Server およびアクイジション / レビュー用ワークステーションにクライアントとして配備する必要があります。以下の手順に従い、***Trend Micro OfficeScan Client/Server Edition*** をインストールします。

ウイルス定義の更新は施設の責任となります。最新のアンチウイルス保護がシステムに確実に施されるよう、定期的に定義をアップデートしてください。

インストール前のガイドライン

1. Trend Micro Anti-Virus Management Console は、Trend Micro の指示に従ってインストールすることにより適切に動作します。
2. Trend Micro OfficeScan のインストール中に、Anti-Virus Management Console サーバーで以下を実行します。
    a. ***Anti-virus Feature*（アンチウイルス機能）**ウィンドウで、***Enable firewall*（ファイアウォールを有効にする）**のチェックマークを外します。
    b. ***Anti-spyware Feature*（アンチスパイウェア機能）**ウィンドウで、***No, Please do not enable assessment mode*（いいえ、評価モードを有効にしないでください）**を選択します。
    c. ***Web Reputation Feature*（*Web* レピュテーション機能）**ウィンドウで、***Enable web reputation policy*（*Web* レピュテーションポリシーを有効にする）**のチェックマークを外します。
3. Mac-Lab/CardioLab システムで、PDM に ***CO_2*** 機能を使用している場合、Trend Micro OfficeScan はお勧めできません。
4. Trend Micro OfficeScan が必要な場合：
    a. Mac-Lab/CardioLab システム用に別の Trend Micro Anti-Virus Management Console サーバーを設定することをお勧めします。Mac-Lab/CardioLab システムで PDM とともに ***CO_2*** 機能を使用するには、アンチウイルス設定をグローバル変更する必要があります。
    b. 別の Trend Micro Anti-Virus Management Console サーバーを設定できない場合は、インストール後に既存の Trend Micro Anti-Virus Management Console サーバーへのグローバル設定を変更する必要があります。この変更により、既存の Trend Micro Anti-

Virus Management Console サーバーに接続されているすべてのクライアントシステムが影響を受けるため、実行前に IT 担当者と検討する必要があります。

5. すべてのクライアントシステム（アクイジション、レビュー、および INW Server）上で**管理者**またはそのグループのメンバーとしてログオンし、アンチウイルスソフトウェアをインストールします。
6. ループバック接続を無効にします。詳細については、ループバック接続を無効にする（6 ページ）を参照してください。
7. コンピュータブラウザーサービスを設定します。詳細については、アンチウイルスのインストール前のコンピュータブラウザーサービスの設定（7 ページ）を参照してください。

Trend Micro OfficeScan - 新規インストールの配備手順（推奨プッシュインストール方法）

1. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *TrendMicro OfficeScan server*（*TrendMicro OfficeScan* サーバー）- < サーバー名 > > *Office Scan Web Console*（ウイルスバスター *Corp. Web* コンソール）**をクリックします。

注 : ***Continue to this website (not recommended)*（このサイトの閲覧を続行する（推奨されません））**を選択して続行します。Security Alert（セキュリティの警告）ウィンドウで、***In the future, do not show this warning*（今後、この警告を表示しない）**にチェックマークを入れ、***OK*** をクリックします。

2. サイトが信用できないことを示す証明書エラーを受け取ったら、証明書に Trend Micro OfficeScan を含めるように管理します。
3. プロンプトが表示されたら、***AtxEnc*** アドオンをインストールします。Security Warning（セキュリティ警告）画面が表示されます。
4. ***Install*（インストール）**をクリックします。
5. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。
6. プロンプトが表示されたら、***Update Now*（今すぐ更新）**をクリックして新しいウェジットをインストールします。新しいウェジットが更新されるまで待ちます。更新完了画面が表示されます。
7. ***OK*** をクリックします。
8. 左側のメニューバーで、***Networked Computers*（ネットワーク上のコンピュータ）> *Client Installation*（クライアントインストール > *Remote*（リモート）**の順にクリックします。
9. プロンプトが表示されたら、***AtxConsole*** アドオンをインストールします。Security Warning（セキュリティ警告）画面が表示されます。
10. ***Install*（インストール）**をクリックします。
11. ***Remote Installation*（リモートインストール）**ウィンドウで ***My Company*（マイカンパニー）**をダブルクリックします。すべてのドメインが ***My Company*（マイカンパニー）**の下に一覧表示されます。
12. リストからドメイン（例：INW Server）をダブルクリックします。そのドメインに接続されているすべてのシステムが表示されます。

13. ドメインまたはシステムが ***Domain and Computers*（ドメインとコンピュータ）**ウィンドウに一覧表示されない場合は、以下の各クライアントシステム（アクイジション、レビュー、INW Server）で以下のことを実行します。

    a. 管理者またはすべてのクライアントマシンのグループメンバーとしてログインします。

    b. ***Start*（スタート）> *Run*（実行）**をクリックします。

    c. ***<Anti-Virus Management Console_server_IP_address>*** を入力して、***Enter*** を押します。プロンプトが表示されたら、管理者ユーザー名とパスワードを入力します。

    d. ***<Anti-Virus Management Console_server_IP _address>**ofsscan** に移動して、***AutoPcc.exe*** をダブルクリックします。プロンプトが表示されたら、管理者ユーザー名とパスワードを入力します。

    e. インストールが完了したらクライアントシステムを再起動します。

    f. すべてのクライアントマシンで**管理者**またはグループメンバーとしてログインし、システムトレイの Trend Micro OfficeScan アイコンが青に緑のチェックマークの付いた記号に変わるまで待ちます。

    g. この手順の残りの部分を省略し、「Trend Micro OfficeScan サーバーコンソールの設定」の手順に進みます。

14. クライアントマシン（アクイジション、レビュー、INW Server）を選択し、***Add*（追加）**をクリックします。

15. < ドメイン名 >\ ユーザー名とパスワードを入力し、***Log on*（ログオン）**をクリックします。

16. ***Selected Computers*（選択したコンピュータ）**領域でクライアントマシン（アクイジション、レビュー、INW Server）を 1 つずつ選択し、***Install*（インストール）**をクリックします。

17. 確認ボックスで ***Yes*（はい）**をクリックします。

18. ***Number of clients to which notifications were sent*（通知を送信したクライアント数）**メッセージボックスで、***OK*** をクリックします。

19. すべてのクライアントマシン（アクイジション、レビュー、INW Server）を再起動し、すべてのクライアントマシンで管理者またはそのグループのメンバーとしてログインして、システムトレイの Trend Micro OfficeScan アイコンが青に緑のチェックマークの付いた記号に変わるまで待ちます。

20. ***Log off*（ログオフ）**リンクをクリックし、***OfficeScan Web Console*（ウイルスバスター *Corp. Web* コンソール）**を閉じます。

Trend Micro OfficeScan サーバーコンソールの設定

1. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *TrendMicro Office Scan server* < サーバー名 > > *Office Scan Web Console***（ウイルスバスター Corp. Web コンソール）を選択します。***Trend Micro OfficeScan Login*（*Trend Micro OfficeScan* ログイン）**画面が表示されます。

2. ユーザー名とパスワードを入力し、***Login*（ログイン）**をクリックします。***Summary*（サマリ）**画面が表示されます。

3. 左側の領域で、***Networked Computers*（ネットワーク上のコンピュータ）> *Client Management*（クライアント管理）**リンクを選択します。
4. 右側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
5. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Manual Scan Settings*（手動検索設定）**を選択します。***Manual Scan Settings*（手動検索設定）**画面が表示されます。
6. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。
   - ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
   - ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
   - ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**
   - ***Virus/Malware Scan Settings only*（ウイルス / 不正プログラム検索設定のみ）> *Scan boot area*（ブートエリア検索）。**
   - ***CPU Usage*（*CPU* 使用率）> *Low*（低）。**
   - ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
   - ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
   - ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed and select Add path to agent Computers Exclusion list*（*Trend Micro* 製品がインストールされているディレクトリを除外し、クライアントのコンピュータ除外リストへのパスの追加を選択する）。**
   - **C:\Program Files (x86)\GE Healthcare\MLCL\、C:\Program Files\GE Healthcare\MLCL\、D:\GEData\Studies、E:\、G:** フォルダを 1 つずつ入力し、***Add*（追加）**をクリックします。
7. ***Apply To All Clients*（すべてのクライアントに適用）**をクリックします。
8. ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier.*（以前にクライアントツリーで選択したクライアントまたはドメインの除外リストは、この画面の除外リストに差し替えられます。続行しますか *?*）**というメッセージで、***OK*** をクリックします。
9. ***Close*（閉じる）**をクリックし、***Manual Scan Settings*（手動検索設定）**画面を閉じます。
10. 左側の領域で、***Networked Computers*（ネットワーク上のコンピュータ）> *Client Management*（クライアント管理）**リンクを選択します。
11. 右側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
12. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Real-time Scan Settings*（リアルタイム検索設定）**を選択します。***Real-time Scan Settings*（リアルタイム検索設定）**画面が表示されます。
13. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。
   - ***Real-time Scan Settings*（リアルタイム検索設定）> *Enable virus/malware scan*（ウイルス / 不正プログラムの検索を有効にする）。**
   - ***Real-time Scan Settings*（リアルタイム検索設定）> *Enable spyware/grayware scan*（スパイウェア / グレーウェア検索を有効にする）。**

- ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
- ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
- ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**
- ***Virus/Malware Scan Settings Only*（ウイルス / 不正プログラム検索設定のみ）> *Enable IntelliTrap*（*IntelliTrap* を有効にする）。**
- ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
- ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
- ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed*（トレンドマイクロ製品がインストールされているディレクトリの除外）。**
- ***C:\Program Files (x86)\GE Healthcare\MLCL*、*C:\Program Files \GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*、*G:*** のフォルダパスが ***Exclusion List*（除外リスト）**にあることを確認します。

14. ***Action*（処理）**タブをクリックします。
15. デフォルト設定は変更せず、以下のオプションのチェックマークを外します。
    - ***Virus/Malware*（ウイルス / 不正プログラム）> *Display a notification message on the client computer when virus/malware is detected.*（ウイルス / 不正プログラムが検出された場合にクライアントコンピュータに通知メッセージを表示する）。**
    - ***Spyware/Grayware*（スパイウェア / グレーウェア）> *Display a notification message on the client computer when spyware/grayware is detected.*（スパイウェア / グレーウェアが検出された場合にクライアントコンピュータに通知メッセージを表示する）。**
16. ***Apply To All Clients*（すべてのクライアントに適用）**をクリックします。
17. ***Close*（閉じる）**をクリックし、***Real-time Scan Settings*（リアルタイム検索設定）**画面を閉じます。
18. 左側の領域で、***Networked Computers*（ネットワーク上のコンピュータ）> *Client Management*（クライアント管理）**リンクを選択します。
19. 右側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
20. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Scheduled Scan Settings*（予約検索設定）**を選択します。***Scheduled Scan Settings*（予約検索設定）**画面が表示されます。
21. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。
    - ***Scheduled Scan Settings*（予約検索設定）> *Enable virus/malware scan*（ウイルス / 不正プログラムの検索を有効にする）。**
    - ***Scheduled Scan Settings*（予約検索設定）> *Enable spyware/grayware scan*（スパイウェア / グレーウェアの検索を有効にする）。**
    - ***Schedule*（スケジュール）> *Weekly, every Sunday, Start time:00:00 hh:mm*（毎週、毎日曜日、開始時間：*00:00 hh:mm*）。**
    - ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
    - ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
    - ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**

- ***Virus/Malware Scan Settings only*（ウイルス / 不正プログラム検索設定のみ）> *Scan boot area*（ブートエリア検索）。**
- ***CPU Usage*（*CPU* 使用率）> *Low*（低）。**
- ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
- ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
- ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed*（トレンドマイクロ製品がインストールされているディレクトリの除外）。**
- ***C:\Program Files (x86)\GE Healthcare\MLCL*、*C:\Program Files \GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*\、*G:*\ のフォルダパスが Exclusion List（除外リスト）にあることを確認します。

22. ***Action*（処理）**タブをクリックします。
23. デフォルト設定は変更せず、以下のオプションのチェックマークを外します。
    - ***Virus/Malware*（ウイルス / 不正プログラム）> *Display a notification message on the client computer when virus/malware is detected.*（ウイルス / 不正プログラムが検出された場合にクライアントコンピュータに通知メッセージを表示する）。**
    - ***Spyware/Grayware*（スパイウェア / グレーウェア）> *Display a notification message on the client computer when spyware/grayware is detected.*（スパイウェア / グレーウェアが検出された場合にクライアントコンピュータに通知メッセージを表示する）。**
24. ***Apply To All Clients*（すべてのクライアントに適用）**をクリックします。
25. ***Close*（閉じる）**をクリックし、***Scheduled Scan Settings*（予約検索設定）**画面を閉じます。
26. 左側の領域で、***Networked Computers*（ネットワーク上のコンピュータ）> *Client Management*（クライアント管理）**リンクを選択します。
27. 右側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
28. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Scan Now Settings*（今すぐ検索の設定）**を選択します。***Scan Now Settings*（今すぐ検索の設定）**画面が表示されます。
29. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。
    - ***Scan Now Settings*（今すぐ検索の設定）> *Enable virus/malware scan*（ウイルス / 不正プログラムの検索を有効にする）。**
    - ***Scan Now Settings*（今すぐ検索の設定）> *Enable spyware/grayware scan*（スパイウェア / グレーウェアの検索を有効にする）。**
    - ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
    - ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
    - ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**
    - ***Virus/Malware Scan Settings only*（ウイルス / 不正プログラム検索設定のみ）> *Scan boot area*（ブートエリア検索）。**
    - ***CPU Usage*（*CPU* 使用率）> *Low*（低）。**
    - ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**

- ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
- ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed*（トレンドマイクロ製品がインストールされているディレクトリの除外）。**
- ***C:\Program Files (x86)\GE Healthcare\MLCL*、*C:\Program Files \GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*** および ***G:*** を確認します。

30. ***Apply To All Clients*（すべてのクライアントに適用）**をクリックします。
31. ***Close*（閉じる）**をクリックし、***Scan Now Settings*（今すぐ検索の設定）**画面を閉じます。
32. 左側の領域で、***Networked Computers*（ネットワーク上のコンピュータ）> *Client Management*（クライアント管理）**リンクを選択します。
33. 右側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
34. ***Settings*（設定）**オプションから、***Web Reputation Settings*（*Web* レピュテーション設定）**を選択します。***Web Reputation Settings*（*Web* レピュテーション設定）**画面が表示されます。
35. ***External Clients*（外部クライアント）**タブをクリックし、***Enable Web reputation policy on the following operating systems*（次のオペレーティングシステムで *Web* レピュテーションポリシーを有効にする）**のチェックマークを外します（インストール時に既に選択されている場合）。
36. ***Internal Clients*（内部クライアント）**タブをクリックし、***Enable Web reputation policy on the following operating systems*（次のオペレーティングシステムで *Web* レピュテーションポリシーを有効にする）**のチェックマークを外します（インストール時に既に選択されている場合）。
37. ***Apply To All Clients*（すべてのクライアントに適用）**をクリックします。
38. ***Close*（閉じる）**をクリックして、***Web Reputation*（*Web* レピュテーション）**画面を閉じます。
39. 左側の領域で、***Networked Computers*（ネットワーク上のコンピュータ）> *Client Management*（クライアント管理）**リンクを選択します。
40. 右側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
41. ***Settings*（設定）**オプションから、***Behavior Monitoring Settings*（挙動監視設定）**を選択します。***Behavior Monitoring Settings*（挙動監視設定）**画面が表示されます。
42. ***Enable Malware Behavior Blocking*（不正プログラムの挙動ブロックを有効にする）**オプションおよび ***Enable Event Monitoring*（イベント監視を有効にする）**オプションのチェックマークを外します。
43. ***Apply To All Clients*（すべてのクライアントに適用）**をクリックします。
44. ***Close*（閉じる）**をクリックして、***Behavior Monitoring*（挙動監視）**画面を閉じます。
45. 左側の領域で、***Networked Computers*（ネットワーク上のコンピュータ）> *Client Management*（クライアント管理）**リンクを選択します。
46. 右側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

47. ***Settings*（設定）**オプションから、***Device Control Settings*（デバイスコントロール設定）**を選択します。***Device Control Settings*（デバイスコントロール設定）**画面が表示されます。

48. ***External Clients*（外部クライアント）**タブをクリックして、以下のオプションのチェックマークを外します。

    - ***Notification*（通知）> *Display a notification message on the client computer when OfficeScan detects unauthorized device access*（*OfficeScan* がデバイスへの不正アクセスを検知した場合、クライアントコンピュータに通知メッセージを表示する）。**
    - ***Block the AutoRun function on USB storage devices*（*USB* ストレージデバイスの自動実行機能をブロックする）。**
    - ***Enable Device Control*（デバイスコントロールを有効にする）。**

49. ***Internal Clients*（内部クライアント）**タブをクリックして、以下のオプションのチェックマークを外します。

    - ***Notification*（通知）> *Display a notification message on the client computer when OfficeScan detects unauthorized device access*（*OfficeScan* がデバイスへの不正アクセスを検知した場合、クライアントコンピュータに通知メッセージを表示する）。**
    - ***Block the AutoRun function on USB storage devices*（*USB* ストレージデバイスの自動実行機能をブロックする）。**
    - ***Enable Device Control*（デバイスコントロールを有効にする）。**

50. ***Apply To All Clients*（すべてのクライアントに適用）**をクリックします。

51. ***Close*（閉じる）**をクリックして、***Device Control Settings*（デバイスコントロール設定）**画面を閉じます。

52. 左側の領域で、***Networked Computers*（ネットワーク上のコンピュータ）> *Client Management*（クライアント管理）**リンクを選択します。

53. 右側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

54. ***Settings*（設定）**オプションから、***Privileges and Other Settings*（権限とその他の設定）**を選択します。

55. ***Privileges*（権限）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

    - ***Scan Privileges*（検索権限）> *Configure Manual Scan Settings*（手動検索設定の構成）。**
    - ***Scan Privileges*（検索権限）> *Configure Real-time Scan Settings*（リアルタイム検索設定の構成）。**
    - ***Scan Privileges*（検索権限）> *Configure Scheduled Scan Settings*（予約検索設定の構成）。**
    - ***Proxy Setting Privilege*（プロキシ設定権限）> *Allow the client user to configure proxy settings*（クライアントユーザーによるプロキシ設定を許可する）。**
    - ***Uninstallation*（アンインストール）> *Require a password for the user to uninstall the OfficeScan Client*（ウイルスバスター *Corp.* クライアントのアンインストール時にユーザーにパスワードを要求する）。**適切なパスワードを入力して、パスワードを確認します。
    - ***Unloading*（アンロード）> *Require a password for the user to unload the OfficeScan Client*（ウイルスバスター *Corp.* クライアントのアンロード時にユーザーにパスワードを要求する）。**適切なパスワードを入力して、パスワードを確認します。

56. ***Other Settings*（その他の設定）**タブをクリックします。

57. ***Client Security Settings*（クライアントセキュリティ設定）> *Normal*（標準）**を選択し、その他のオプションのチェックマークを外します。

注 : 必ず以下のオプションのチェックマークを外してください。

- ***Client Self-protection*（クライアントの自己保護）> *Protect OfficeScan client services*（ウイルスバスター *Corp.* クライアントサーバーを保護する）。**
- ***Client Self-protection*（クライアントの自己保護）> *Protect files in the OfficeScan client installation folder*（ウイルスバスター *Corp.* クライアントインストールフォルダ内のファイルを保護する）。**
- ***Client Self-protection*（クライアントの自己保護）> *Protect OfficeScan client registry keys*（ウイルスバスター *Corp.* クライアントレジストリキーを保護する）。**
- ***Client Self-protection*（クライアントの自己保護）> *Protect OfficeScan client processes*（ウイルスバスター *Corp.* クライアントプロセスを保護する）。**

58. ***Apply To All Clients*（すべてのクライアントに適用）**をクリックします。

59. ***Close*（閉じる）**をクリックし、***Privileges and Other Settings*（権限とその他の設定）**画面を閉じます。

60. 左側の領域で、***Networked Computers*（ネットワーク上のコンピュータ）> *Client Management*（クライアント管理）リンク**を選択します。

61. 右側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

62. ***Settings*（設定）**オプションから、***Additional Service Settings*（その他のサービスの設定）**を選択します。

63. ***Enable service on the following operating systems*（次のオペレーティングシステムでサービスを有効にする）**オプションのチェックマークを外します。

64. ***Apply To All Clients*（すべてのクライアントに適用）**をクリックします。

65. ***Close*（閉じる）**をクリックし、***Additional Service Settings*（その他のサービスの設定 *)*** 画面を閉じます。

66. 左側の領域で、***Networked Computers*（ネットワーク上のコンピュータ）> *Global Client Settings*（グローバルクライアント設定）**リンクをクリックします。

67. 以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

- ***Scan Settings*（検索設定）> *Configure Scan settings for large compressed files*（大きな圧縮ファイル用の検索設定）。**
- ***Scan Settings*（検索設定）> *Do not scan files in the compressed file if the size exceeds 2 MB*（サイズが *2 MB* を超える場合は圧縮ファイルのファイルを検索しない）。**
- ***Scan Settings*（検索設定）> *In a compressed file scan only the first 100 files*（圧縮ファイル内の最初の *100* ファイルだけを検索する）。**
- ***Scan Settings*（検索設定）> *Exclude the OfficeScan server database folder from Real-time Scan*（ウイルスバスター *Corp.* サーバーのデータベースフォルダをリアルタイム検索の対象から除外）。**
- ***Scan Settings*（検索設定）> *Exclude Microsoft Exchange server folders and files from scans*（*Microsoft Exchange* サーバーのフォルダおよびファイルを検索から除外）。**
- ***Reserved Disk Space*（予約ディスク空き容量）> *Reserve 60 MB of disk space for updates*（ディスク空き容量の *60 MB* をアップデート用に予約する）。**

- ***Proxy Configuration*（プロキシ設定）> *Automatically detect settings*（設定を自動で検出する）。**

注 : ***Alert Settings*（警告設定）> *Display a notification message if the client computer needs to restart to load a kernel driver*（カーネルドライバをロードするためにクライアントコンピュータを再起動する必要がある場合、通知メッセージを表示する）**のチェックマークを外すことが重要です。

68. ***Save*（保存）**をクリックします。
69. 左側の領域で、***Updates*（更新）> *Networked Computers*（ネットワーク上のコンピュータ）> *Manual Updates*（手動更新）**リンクを選択します。
70. ***Manually select client*（クライアントを手動で選択する）**を選択して、***Select*（選択）**をクリックします。
71. ***OffceScan Server*（*OffceScan* サーバー）**の下にある適切なドメイン名をクリックします。
72. 一度に 1 つのクライアントシステムを選択して、***Initiate Component Update*（コンポーネントの更新を開始する）**をクリックします。
73. メッセージボックスで ***OK*** をクリックします。
74. ***Log off*（ログオフ）**をクリックし、ウイルスバスター Corp. Web コンソールを閉じます。

Trend Micro OfficeScan インストール後のガイドライン

1. アクイジションシステムで以下の手順を実行し、Trend Micro を設定します。
   a. ***Start*（スタート）> *Control Panel*（コントロールパネル）> *Network and Sharing Center*（ネットワークと共有センター）**をクリックします。
   b. ***Change adapter settings*（アダプターの設定の変更）**をクリックします。
   c. ***Local Area Connection*（ローカル エリア接続）**を右クリックして、***Properties*（プロパティ）**を選択します。
   d. ***Internet Protocol Version 4 (TCP/IPv4)*（インターネット プロトコル バージョン *4* （*TCP/IPv4*））**を選択して ***Properties*（プロパティ）**をクリックします。
   e. IP アドレス _____ を記録します。
   f. 開いているウィンドウをすべて閉じます。
   g. ***Start*（スタート）> *Run*（実行）**をクリックし、**regedit** と入力します。
   h. ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion*** に移動します。
   i. 右領域で空白スペースを右クリックし、***New*（新規）> *String value*（文字列値）**を選択します。
   j. 名前に **IP Template** と入力し、**Enter** を押します。
   k. ***IP Template*（*IP* テンプレート）**レジストリをダブルクリックします。
   l. ***Value*（値）**データフィールドに、ステップで記録したローカルエリア接続 IP アドレスを入力します e。
   m. ***OK*** をクリックします。

n. レジストリエディタを閉じます。

2. ループバック接続を有効にします。詳細については、ループバック接続を有効にする（6 ページ）を参照してください。

3. コンピュータブラウザーサービスを設定します。詳細については、アンチウイルスのインストール後のコンピュータブラウザーサービスの設定（7 ページ）を参照してください。

Trend Micro のグローバル設定の設定

注 : Mac-Lab/CardioLab システムで PDM による CO_2 機能を使用する場合のみ、以下の手順を実行してください。以下の手順を進める前に、IT 担当者と検討済みであることを確認します。

1. Anti-Virus Management Console サーバーで、***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV*** フォルダに移動します。
2. ***ofcscan.ini*** ファイルをテキストエディタで開きます。
3. ***Global Setting*（グローバル設定）**セクションの下で、以下のキーの値を「**1**」に設定します。
   [グローバル設定] ***RmvTmTDI=1***
4. ofcscan.ini ファイルを保存して閉じます。
5. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *TrendMicro OfficeScan server*（*TrendMicro OfficeScan* サーバー）- < サーバー名 > > *Office Scan Web Console*（ウイルスバスター *Corp. Web* コンソール）**をクリックします。
6. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。***Summary*（サマリ）**画面が表示されます。
7. ***Networked Computers*（ネットワーク上のコンピュータ) > *Global Client Settings*（グローバルクライアントの設定）**をクリックします。***Save*（保存）**をクリックします。
8. 左側の領域で、***Updates*（更新）> *Networked Computers*（ネットワーク上のコンピュータ）> *Manual Update*（手動更新）**リンクを選択します。
9. ***Manually select clients*（クライアントを手動で選択する）**を選択して、***Select*（選択）**をクリックします。
10. ***OffceScan Server*（*OffceScan* サーバー）**の下にある適切なドメイン名をクリックします。
11. 一度に 1 つのクライアントシステムを選択して、***Initiate Component Update*（コンポーネントの更新を開始する）**をクリックします。
12. メッセージボックスで ***OK*** をクリックします。
13. 各アクイジションシステムで、以下を実行します。
    a. レジストリエディタを開きます。
    b. ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc*** に移動します。
    c. ***RmvTmTDI*** レジストリの値が「**1**」に設定されていることを確認します。
    d. ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services*** に移動します。

e. ***tmtdi*** レジストリキーがある場合は削除します。

f. レジストリエディタを閉じます。

g. クライアントシステムを再起動します。

h. 管理者またはそのグループのメンバーとしてクライアントシステムにログインします。

i. 各クライアントシステムで、管理者権限でコマンドプロンプトを開き、「***sc query tmtdi***」とコマンドを入力します。

j. ***The specified service does not exist as an installed service*（指定されたサービスはインストールされたサービスとして存在しません）**というメッセージが表示されるのを確認します。

14. Anti-Virus Management Console サーバーで、***Log off*（ログオフ）**をクリックしてウイルスバスター Corp. Web コンソールを閉じます。

Trend Micro OfficeScan Client/Server Edition 11.0 SP1

Trend Micro OfficeScan Client/Server Edition は必ずネットワーク上の Mac-Lab/CardioLab 環境でインストールします。Trend Micro OfficeScan は、Anti-Virus Management Console サーバーにインストールしてから、Centricity Cardiology INW Server およびアクイジション / レビュー用ワークステーションにクライアントとして配備する必要があります。以下の指示に従って、***Trend Micro OfficeScan Client/Server Edition 11.0 SP1*** をインストールします。

ウイルス定義の更新は施設の責任となります。最新のアンチウイルス保護がシステムに確実に施されるよう、定期的に定義をアップデートしてください。

インストール前のガイドライン

1. Trend Micro Anti-Virus Management Console は、Trend Micro の指示に従ってインストールすることにより適切に動作します。

2. Trend Micro OfficeScan のインストール中に、Anti-Virus Management Console サーバーで以下を実行します。

   a. ***Anti-virus Feature*（アンチウイルス機能）**ウィンドウで、***Enable firewall*（ファイアウォールを有効にする）**のチェックマークを外します。

   b. ***Anti-spyware Feature*（アンチスパイウェア機能）**ウィンドウで、***No, Please do not enable assessment mode*（いいえ、評価モードを有効にしないでください）**を選択します。

   c. ***Web Reputation Feature*（*Web* レピュテーション機能）**ウィンドウで、***Enable web reputation policy*（*Web* レピュテーションポリシーを有効にする）**のチェックマークを外します。

3. Mac-Lab/CardioLab システムで PDM による CO_2 機能を使用する場合は、Trend Micro OfficeScan は推奨されません。

4. Trend Micro OfficeScan が必要な場合：

   a. Mac-Lab/CardioLab システム用に別の Trend Micro Anti-Virus Management Console サーバーを設定することをお勧めします。Mac-Lab/CardioLab システムで PDM による CO_2 機能を使用するには、アンチウイルス設定へのグローバルな変更が必要です。

b. 別の Trend Micro Anti-Virus Management Console サーバーを設定できない場合は、インストール後に既存の Trend Micro Anti-Virus Management Console サーバーへのグローバル設定を変更する必要があります。この変更により、既存の Trend Micro Anti-Virus Management Console サーバーに接続されているすべてのクライアントシステムが影響を受けるため、実行前に IT 担当者と検討する必要があります。

5. すべてのクライアントシステム（アクイジション、レビュー、および INW Server）上で**管理者**またはそのグループのメンバーとしてログオンし、アンチウイルスソフトウェアをインストールします。

6. ループバック接続を無効にします。詳細については、ループバック接続を無効にする（6 ページ）を参照してください。

7. コンピュータブラウザーサービスを設定します。詳細については、アンチウイルスのインストール前のコンピュータブラウザーサービスの設定（7 ページ）を参照してください。

8. アクイジション、レビュー、INW クライアントの各マシンでのインストールには、以下のルート証明書および中間証明書が必要です。

   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt

9. 以下のサブステップを繰り返して、ステップ 8 にリストされている 5 つの必要なルートおよび中間レベルの証明書をインストールします。

   a. C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro*** に移動します。
   注 INW で、C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro に移動します。

   b. 上記のフォルダパスが存在しない場合は、インストールに必要なルートおよび中間レベルの証明書を手動で取得します。

   c. ***AddTrustExternalCARoot.crt*** をダブルクリックして、MLCL システム（アクイジション、レビュー、INW）にインストールします。

   d. 証明書を開いて、***Install Certificate*（証明書のインストール）**をクリックします。

   e. ***Certificate Import Wizard*（証明書のインストールウィザード）**が表示されたら、***Next*（次へ）**をクリックします。

   f. ***Certificate Store*（証明書ストア）**ウィンドウで、***Place all certificates in the following store*（すべての証明書を次のストアに置く）**を選択して ***Browse*（参照）**をクリックします。

   g. ***Show physical stores*（物理ストアを表示する）> *Trusted Root Certification Authorities*（信頼されたルート証明機関）> *Local Computer*（ローカルコンピュータ）**にチェックマークを入れて ***OK*** をクリックします。

   h. ***Certificate Import Wizard*（証明書のインポートウィザード）**で、***Next*（次へ）**をクリックします。

   i. ***Finish*（完了）**をクリックします。***The import was successful*（インポートが正常に完了しました）**メッセージが表示されるはずです。

j. ステップ 8 にリストされている他の証明書について、ステップ 9 を繰り返します。

注 : 各証明書には有効期限があります。証明書の有効期限が切れたら、OfficeScan エージェントが期待通りに機能するように MLCL システムで証明書を更新する必要があります。

Trend Micro OfficeScan - 新規インストールの配備手順（11.0 SP1 用推奨プッシュインストール方法）

1. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *TrendMicro OfficeScan server*（*TrendMicro OfficeScan* サーバー）- < サーバー名 > > *Office Scan Web Console*（ウイルスバスター *Corp. Web* コンソール）**をクリックします。

注 : ***Continue to this website (not recommended)*（このサイトの閲覧を続行する（推奨されません））**を選択して続行します。Security Alert（セキュリティの警告）ウィンドウで、***In the future, do not show this warning*（今後、この警告を表示しない）**にチェックマークを入れ、***OK*** をクリックします。

2. サイトが信用できないことを示す証明書エラーを受け取ったら、証明書に Trend Micro OfficeScan を含めるように管理します。

3. プロンプトが表示されたら、***AtxEnc*** アドオンをインストールします。Security Warning（セキュリティ警告）画面が表示されます。

   a. ***Install*（インストール）**をクリックします。

4. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。

5. プロンプトが表示されたら、***Update Now*（今すぐ更新）**をクリックして新しいウェジットをインストールします。新しいウェジットが更新されるまで待ちます。更新完了画面が表示されます。

   a. ***OK*** をクリックします。

6. トップメニューバーで、***Agents*（エージェント）> *Agent Installation*（エージェントのインストール）> *Remote*（リモート）**をクリックします。

7. プロンプトが表示されたら、***AtxConsole*** アドオンをインストールします。Security Warning（セキュリティ警告）画面が表示されます。

   a. ***Install*（インストール）**をクリックします。

8. ***Remote Installation*（リモートインストール）**ウィンドウで、***OfficeScan Server*（*OfficeScan* サーバー）**をダブルクリックします。***OfficeScan Server*（*OfficeScan* サーバー）**の下に、すべてのドメインが一覧表示されます。

9. リストから、ドメイン（例：INW Server）をダブルクリックします。そのドメインに接続されているすべてのシステムが表示されます。

注 : ドメインまたはシステムが ***Domains and Endpoints*（ドメインとエンドポイント）**ウィンドウに一覧表示されない場合は、ドメインおよびエンドポイントウィンドウに一覧されていないドメインまたはシステムのトラブルシューティング（77 ページ）に移動して手動で追加するか、クライアントマシンから直接インストールを実行します。

10. クライアントマシン（アクイジション、レビュー、INW Server）を選択し、***Add*（追加）**をクリックします。

11. < ドメイン名 >\ ユーザー名とパスワードを入力し、***Log on*（ログオン）**をクリックします。

12. ***Selected Endpoints*（選択したエンドポイント）**領域でクライアントマシン（アクイジション、レビュー、INW Server）を 1 つずつ選択し、***Install*（インストール）**をクリックします。

13. 確認ボックスで ***OK*** をクリックします。

14. ***Number of clients to which notifications were sent*（通知を送信したクライアント数）**メッセージボックスで、***OK*** をクリックします。

15. すべてのクライアントマシン（アクイジション、レビュー、INW Server）を再起動し、すべてのクライアントマシンで管理者またはそのグループのメンバーとしてログインして、システムトレイの Trend Micro OfficeScan アイコンが青に緑のチェックマークの付いた記号に変わるまで待ちます。

16. ***Log off*（ログオフ）**リンクをクリックし、***OfficeScan Web Console*（ウイルスバスター *Corp. Web* コンソール）**を閉じます。

11.0 SP1 用 Trend Micro OfficeScan サーバーコンソールの設定

1. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *TrendMicro Office Scan server* < サーバー名 > > *Office Scan Web Console***（ウイルスバスター Corp. Web コンソール）を選択します。***Trend Micro OfficeScan Login*（*Trend Micro OfficeScan* ログイン）**画面が表示されます。

2. ユーザー名とパスワードを入力し、***Login*（ログイン）**をクリックします。***Summary*（サマリ）**画面が表示されます。

3. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

4. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

5. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Manual Scan Settings*（手動検索設定）**を選択します。***Manual Scan Settings*（手動検索設定）**画面が表示されます。

6. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

   - ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
   - ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
   - ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**
   - ***Virus/Malware Scan Settings only*（ウイルス / 不正プログラム検索設定のみ）> *Scan boot area*（ブートエリア検索）。**
   - ***CPU Usage*（*CPU* 使用率）> *Low*（低）。**

7. Scan Exclusion（検索除外）タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

   - ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
   - ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**

- ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed*（トレンドマイクロ製品がインストールされているディレクトリの除外）。**
- ***Saving the officescan agent's exclusion list does the following:*（以下を行なう *officescan* エージェントの除外リストの保存：）**の下にあるドロップダウンリストから ***Adds path to*（パスの追加先）**を選択します。
- **C:\Program Files (x86)\GE Healthcare\MLCL\、C:\Program Files\GE Healthcare\MLCL\、D:\GEData\Studies、E:\、G:** フォルダを 1 つずつ入力し、**+** をクリックします。

8. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。
9. ***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier.*（以前にクライアントツリーで選択したクライアントまたはドメインの除外リストは、この画面の除外リストに差し替えられます。続行しますか *?*）**というメッセージで、***OK*** をクリックします。
10. ***Close*（閉じる）**をクリックし、***Manual Scan Settings*（手動検索設定）**画面を閉じます。
11. 上部領域で、***Agent*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。
12. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
13. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Real-time Scan Settings*（リアルタイム検索設定）**を選択します。***Real-time Scan Settings*（リアルタイム検索設定）**画面が表示されます。
14. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。
    - ***Real-time Scan Settings*（リアルタイム検索設定）> *Enable virus/malware scan*（ウイルス / 不正プログラムの検索を有効にする）。**
    - ***Real-time Scan Settings*（リアルタイム検索設定）> *Enable spyware/grayware scan*（スパイウェア / グレーウェア検索を有効にする）。**
    - ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
    - ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
    - ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**
    - ***Virus/Malware Scan Settings Only*（ウイルス / 不正プログラム検索設定のみ）> *Enable IntelliTrap*（*IntelliTrap* を有効にする）。**
15. Scan Exclusion（検索除外）タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。
    - ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
    - ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
    - ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed*（トレンドマイクロ製品がインストールされているディレクトリの除外）。**
    - ***C:\Program Files (x86)\GE Healthcare\MLCL*、*C:\Program Files \GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*、*G:*** のフォルダパスが ***Exclusion List*（除外リスト）**にあることを確認します。
16. ***Action*（処理）**タブをクリックします。

17. デフォルト設定は変更せず、以下のオプションのチェックマークを外します。

    - ***Virus/Malware*（ウイルス / 不正プログラム）> *Display a notification message on endpoints when virus/malware is detected*（ウイルス / 不正プログラムを検知した場合、エンドポイントに通知メッセージを表示する）。**
    - ***Spyware/Grayware*（スパイウェア / グレーウェア）> *Display a notification message on endpoints when spyware/grayware is detected*（スパイウェア / グレーウェアを検知した場合、エンドポイントに通知メッセージを表示する）。**

18. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。

19. ***Close*（閉じる）**をクリックし、***Real-time Scan Settings*（リアルタイム検索設定）**画面を閉じます。

20. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

21. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

22. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Scheduled Scan Settings*（予約検索設定）**を選択します。***Scheduled Scan Settings*（予約検索設定）**画面が表示されます。

23. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

    - ***Scheduled Scan Settings*（予約検索設定）> *Enable virus/malware scan*（ウイルス / 不正プログラムの検索を有効にする）。**
    - ***Scheduled Scan Settings*（予約検索設定）> *Enable spyware/grayware scan*（スパイウェア / グレーウェアの検索を有効にする）。**
    - ***Schedule*（スケジュール）> *Weekly, every Sunday, Start time:00:00 hh:mm*（毎週、毎日曜日、開始時間：*00:00 hh:mm*）。**
    - ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
    - ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
    - ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**
    - ***Virus/Malware Scan Settings only*（ウイルス / 不正プログラム検索設定のみ）> *Scan boot area*（ブートエリア検索）。**
    - ***CPU Usage*（*CPU* 使用率）> *Low*（低）。**

24. ***Scan Exclusion*（検索除外）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

    - ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
    - ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
    - ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed*（トレンドマイクロ製品がインストールされているディレクトリの除外）。**
    - ***C:\Program Files (x86)\GE Healthcare\MLCL*、*C:\Program Files \GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*、*G:*** のフォルダパスが Exclusion List（除外リスト）にあることを確認します。

25. ***Action*（処理）**タブをクリックします。

26. デフォルト設定は変更せず、以下のオプションのチェックマークを外します。

- ***Virus/Malware*（ウイルス / 不正プログラム）> *Display a notification message on the endpoints when virus/malware is detected*（ウイルス / 不正プログラムを検知した場合、エンドポイントに通知メッセージを表示する）。**
- ***Spyware/Grayware*（スパイウェア / グレーウェア）> *Display a notification message on the endpoints when spyware/grayware is detected*（スパイウェア / グレーウェアを検知した場合、エンドポイントに通知メッセージを表示する）。**

27. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。
28. ***Close*（閉じる）**をクリックし、***Scheduled Scan Settings*（予約検索設定）**画面を閉じます。
29. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。
30. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
31. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Scan Now Settings*（今すぐ検索の設定）**を選択します。***Scan Now Settings*（今すぐ検索の設定）**画面が表示されます。
32. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。
    - ***Scan Now Settings*（今すぐ検索の設定）> *Enable virus/malware scan*（ウイルス / 不正プログラムの検索を有効にする）。**
    - ***Scan Now Settings*（今すぐ検索の設定）> *Enable spyware/grayware scan*（スパイウェア / グレーウェアの検索を有効にする）。**
    - ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
    - ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
    - ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**
    - ***Virus/Malware Scan Settings only*（ウイルス / 不正プログラム検索設定のみ）> *Scan boot area*（ブートエリア検索）。**
    - ***CPU Usage*（*CPU* 使用率）> *Low*（低）。**
33. ***Scan Exclusion*（検索除外）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。
    - ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
    - ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
    - ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed*（トレンドマイクロ製品がインストールされているディレクトリの除外）。**
    - ***C:\Program Files (x86)\GE Healthcare\MLCL*、*C:\Program Files \GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*、*G:*** のフォルダパスが Exclusion List（除外リスト）にあることを確認します。
34. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。
35. ***Close*（閉じる）**をクリックし、***Scan Now Settings*（今すぐ検索の設定）**画面を閉じます。
36. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

37. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

38. ***Settings*（設定）**オプションから、***Web Reputation Settings*（*Web* レピュテーション設定）**を選択します。***Web Reputation Settings*（*Web* レピュテーション設定）**画面が表示されます。

39. ***External Agents*（外部エージェント）**タブをクリックし、***Enable Web reputation policy on the following operating systems*（次のオペレーティングシステムで *Web* レピュテーションポリシーを有効にする）**のチェックマークを外します（インストール時に既に選択されている場合）。

40. ***Internal Agents*（内部エージェント）**タブをクリックし、***Enable Web reputation policy on the following operating systems*（次のオペレーティングシステムで *Web* レピュテーションポリシーを有効にする）**のチェックマークを外します（インストール時に既に選択されている場合）。

41. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。

42. ***Close*（閉じる）**をクリックして、***Web Reputation*（*Web* レピュテーション）**画面を閉じます。

43. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

44. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

45. ***Settings*（設定）**オプションから、***Behavior Monitoring Settings*（挙動監視設定）**を選択します。***Behavior Monitoring Settings(* 挙動監視設定 *)*** 画面が表示されます。

46. ***Enable Malware Behavior Blocking for known and potential threats*（既知の脅威および潜在的な脅威に対する不正プログラムの挙動ブロックを有効にする）**オプションおよび ***Enable Event Monitoring*（イベント監視を有効にする）**オプションのチェックマークを外します。

47. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。

48. ***Close*（閉じる）**をクリックして、***Behavior Monitoring*（挙動監視）**画面を閉じます。

49. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

50. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

51. ***Settings*（設定）**オプションから、***Device Control Settings*（デバイスコントロール設定）**を選択します。***Device Control Settings*（デバイスコントロール設定）**画面が表示されます。

52. ***External Agents*（外部エージェント）**タブをクリックして、以下のオプションのチェックマークを外します。

    - ***Notification*（通知）> *Display a notification message on endpoints when OfficeScan detects unauthorized device access*（*OfficeScan* がデバイスへの不正アクセスを検知した場合、エンドポイントに通知メッセージを表示する）。**
    - ***Block the AutoRun function on USB storage devices*（*USB* ストレージデバイスの自動実行機能をブロックする）。**

53. ***Internal Agents*（内部エージェント）**タブをクリックして、以下のオプションのチェックマークを外します。

- ***Notification*（通知）> *Display a notification message on endpoints when OfficeScan detects unauthorized device access*（*OfficeScan* がデバイスへの不正アクセスを検知した場合、エンドポイントに通知メッセージを表示する）。**
- ***Block the AutoRun function on USB storage devices*（*USB* ストレージデバイスの自動実行機能をブロックする）。**

54. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。
55. ***Close*（閉じる）**をクリックして、***Device Control Settings*（デバイスコントロール設定）**画面を閉じます。
56. ***Settings*（設定）**オプションから、もう一度 ***Device Control Settings*（デバイスコントロール設定）**を選択します。***Device Control Settings*（デバイスコントロール設定）**画面が表示されます。
57. ***External Agents*（外部エージェント）**タブをクリックして、***Enable Device Control*（デバイスコントロールを有効にする）**のチェックマークを外します。
58. ***Internal Agents*（内部エージェント）**タブをクリックして、***Enable Device Control*（デバイスコントロールを有効にする）**のチェックマークを外します。
59. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。
60. ***Close*（閉じる）**をクリックして、***Device Control Settings*（デバイスコントロール設定）**画面を閉じます。
61. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。
62. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
63. ***Settings*（設定）**オプションから、***Privileges and Other Settings*（権限とその他の設定）**を選択します。
64. ***Privileges*（権限）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。
    - ***Scans*（検索）> *Configure Manual Scan Settings*（手動検索設定の構成）。**
    - ***Scans*（検索）> *Configure Real-time Scan Settings*（リアルタイム検索設定の構成）。**
    - ***Scans*（検索）> *Configure Scheduled Scan Settings*（予約検索設定の構成）。**
    - ***Proxy Settings*（プロキシ設定）> *Allow users to configure proxy settings*（ユーザーにプロキシ設定を許可する）。**
    - ***Uninstallation*（アンインストール）> *Requires a password*（パスワードが必要）。**適切なパスワードを入力して、パスワードを確認します。
    - ***Unloading and Unlock*（アンロードとアンロック）> *Requires a password*（パスワードが必要）。**適切なパスワードを入力して、パスワードを確認します。
65. ***Other Settings*（その他の設定）**タブをクリックします。
66. ***OfficeScan Agent Security Settings*（*OfficeScan* エージェントセキュリティの設定）> *Normal: Allow users to access OfficeScan agent files and registries*（標準：ユーザーに *OfficeScan* のエージェントファイルおよびレジストリへのアクセスを許可する）**を選択し、その他のオプションのチェックマークを外します。

注 : 必ず以下のオプションのチェックマークを外してください。

- ***OfficeScan AgentSelf-protection*（*OfficeScan* エージェントの自己保護）> *Protect OfficeScan agent services*（*OfficeScan* エージェントサーバーを保護する）。**

- ***AgentSelf-protection*（*OfficeScan* エージェントの自己保護）> *Protect files in the OfficeScan agent installation folder*（*OfficeScan* エージェントインストールフォルダ内のファイルを保護する）。**
- ***AgentSelf-protection*（*OfficeScan* エージェントの自己保護）> *Protect OfficeScan agent registry keys*（*OfficeScan* エージェントレジストリキーを保護する）。**
- ***OfficeScan AgentSelf-protection*（*OfficeScan* エージェントの自己保護）> *Protect OfficeScan agent processes*（*OfficeScan* エージェントプロセスを保護する）。**

67. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。
68. ***Close*（閉じる）**をクリックし、***Privileges and Other Settings*（権限とその他の設定）**画面を閉じます。
69. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。
70. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
71. ***Settings*（設定）**オプションから、***Additional Service Settings*（その他のサービスの設定）**を選択します。
72. ***Enable service on the following operating systems*（次のオペレーティングシステムでサービスを有効にする）**オプションのチェックマークを外します。
73. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。
74. ***Close*（閉じる）**をクリックし、***Additional Service Settings*（その他のサービスの設定 *)*** 画面を閉じます。
75. 上部領域で、***Agents*（エージェント）> *Global Agent Settings*（グローバルエージェント設定）**リンクを選択します。
76. 以下のオプションのみ選択します。その他のオプションのチェックマークは外します。
    - ***Scan Settings for Large Compressed Files*（大きな圧縮ファイルの検索設定）> *Configure Scan settings for large compressed files*（大きな圧縮ファイル用の検索設定）。**
    - ***Scan Settings for Large Compressed Files*（大きな圧縮ファイルの検索設定）> *Do not scan files in the compressed file if the size exceeds 2 MB*（サイズが *2 MB* を超える場合は圧縮ファイルのファイルを検索しない）**。これは、***Real-Time Scan*（リアルタイム検索）**および ***Manual Scan/Schedule Scan/Scan Now*（手動検索 */* 予約検索 */ ScanNow*）**にも適用されます。
    - ***Scan Settings for Large Compressed Files*（大きな圧縮ファイルの検索設定）> *In a compressed file scan only the first 100 files*（圧縮ファイル内の最初の *100* ファイルだけを検索する）。**これは、***Real-Time Scan*（リアルタイム検索）**および ***Manual Scan/Schedule Scan/Scan Now*（手動検索 */* 予約検索 */ScanNow*）**にも適用されます。
    - ***Scan Settings*（検索設定）> *Exclude the OfficeScan server database folder from Real-time Scan*（ウイルスバスター *Corp.* サーバーのデータベースフォルダをリアルタイム検索の対象から除外）。**
    - ***Scan Settings*（検索設定）> *Exclude Microsoft Exchange server folders and files from scans*（*Microsoft Exchange* サーバーのフォルダおよびファイルを検索から除外）。**
    - ***Reserved Disk Space*（予約ディスク空き容量）> *Reserve 60 MB of disk space for updates*（ディスク空き容量の *60 MB* をアップデート用に予約する）。**

- ***Proxy Configuration*（プロキシ設定）> *Automatically detect settings*（設定を自動で検出する）。**

注： カーネルモードドライバをロードするためにエンドポイントを再起動する必要がある場合、***Alert Settings*（警告設定）> *Display a notification message*（通知メッセージを表示する）**のチェックマークを外すことが重要です。

77. ***Save*（保存）**をクリックします。
78. 上部領域で、***Updates*（更新）> *Agents*（エージェント）> *Manual Updates*（手動更新）**リンクを選択します。
79. ***Manually select agents*（エージェントを手動で選択する）**を選択して、***Select*（選択）**をクリックします。
80. ***OffceScan Server*（*OffceScan* サーバー）**の下にある適切なドメイン名をダブルクリックします。
81. クライアントシステムを 1 つずつ選択して、***Initiate Update*（更新を開始する）**をクリックします。
82. メッセージボックスで ***OK*** をクリックします。
83. ***Log off*（ログオフ）**をクリックし、ウイルスバスター Corp. Web コンソールを閉じます。

Trend Micro のグローバル設定の設定

注：Mac-Lab/CardioLab システムで PDM による CO_2 機能を使用する場合のみ、以下の手順を実行してください。以下の手順を進める前に、IT 担当者と検討済みであることを確認します。

1. ***Anti-Virus Management Console* サーバーで、*C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV* フォルダに移動します。**
2. ***ofcscan.ini*** ファイルをテキストエディタで開きます。
3. Global Setting（グローバル設定）セクションの下で、以下のキーの値を「**1**」に設定します。[グローバル設定] ***RmvTmTDI=1***
4. ofcscan.ini ファイルを保存して閉じます。
5. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *TrendMicro OfficeScan server*（*TrendMicro OfficeScan* サーバー）- < サーバー名 > > *Office Scan Web Console*（ウイルスバスター *Corp. Web* コンソール）**をクリックします。
6. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。***Dashboard*（ダッシュボード）**画面が表示されます。
7. ***Agents*（エージェント）> *Global Agent Settings*（グローバルエージェントの設定）**をクリックします。
8. ***Save*（保存）**をクリックします。
9. 左側の領域で、***Updates*（更新）> *Agents*（エージェント）> *Manual Update*（手動更新）**リンクを選択します。
10. ***Manually select clients*（クライアントを手動で選択する）**を選択して、***Select*（選択）**をクリックします。
11. ***OffceScan Server*（*OffceScan* サーバー）**の下にある適切なドメイン名をクリックします。

12. クライアントシステムを 1 つずつ選択して、***Initiate Update*（更新を開始する）**をクリックします。
13. メッセージボックスで ***OK*** をクリックします。
14. 各アクイジションシステムで、以下を実行します。
    a. レジストリエディタを開きます。
    b. ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc*** に移動します。
    c. ***RmvTmTDI*** レジストリの値が「***1***」に設定されていることを確認します。
    d. ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services*** に移動します。
    e. ***tmtdi*** レジストリキーがある場合は削除します。
    f. レジストリエディタを閉じます。
    g. クライアントシステムを再起動します。
    h. 管理者またはそのグループのメンバーとしてクライアントシステムにログインします。
    i. 各クライアントシステムで、管理者権限でコマンドプロンプトを開き、「***sc query tmtdi***」とコマンドを入力します。
    j. ***The specified service does not exist as an installed service*（指定されたサービスはインストールされたサービスとして存在しません）**というメッセージが表示されるのを確認します。
15. Anti-Virus Management Console サーバーで、***Log off*（ログオフ）**をクリックしてウイルスバスター Corp. Web コンソールを閉じます。

Trend Micro OfficeScan インストール後のガイドライン

1. ループバック接続を有効にします。詳細については、ループバック接続を有効にする（6 ページ）を参照してください。
2. コンピュータブラウザーサービスを設定します。詳細については、アンチウイルスのインストール後のコンピュータブラウザーサービスの設定（7 ページ）を参照してください。

Trend Micro OfficeScan Client/Server Edition XG 12.0

インストール概要

Trend Micro OfficeScan Client/Server Edition は必ずネットワーク上の Mac-Lab/CardioLab 環境でインストールします。Trend Micro OfficeScan は、Anti-Virus Management Console サーバーにインストールしてから、Centricity Cardiology INW Server およびアクイジション / レビュー用ワークステーションにクライアントとして配備する必要があります。以下の指示に従って、***Trend Micro OfficeScan Client/Server Edition XG12.0*** をインストールします。

ウイルス定義の更新は施設の責任となります。最新のアンチウイルス保護がシステムに確実に施されるよう、定期的に定義をアップデートしてください。

インストール前のガイドライン

注 : OfficeScan マネージャを実行するのに必要な IE ブラウザーは Internet Explorer 10 以上です。

1. Trend Micro Anti-Virus Management Console は、Trend Micro の指示に従ってインストールすることにより適切に動作します。
2. Trend Micro OfficeScan のインストール中に、Anti-Virus Management Console サーバーで以下を実行します。
   a. ***Anti-virus Feature*（アンチウイルス機能）**ウィンドウで、***Enable firewall*（ファイアウォールを有効にする）**のチェックマークを外します。
   b. ***Anti-spyware Feature*（アンチスパイウェア機能）**ウィンドウで、***No, Please do not enable assessment mode*（いいえ、評価モードを有効にしないでください）**を選択します。
   c. ***Web Reputation Feature*（*Web* レピュテーション機能）**ウィンドウで、***Enable web reputation policy*（*Web* レピュテーションポリシーを有効にする）**のチェックマークを外します。
3. すべてのクライアントシステム（アクイジション、レビュー、および INW Server）上で**管理者**またはそのグループのメンバーとしてログオンし、アンチウイルスソフトウェアをインストールします。
4. ループバック接続を無効にします。詳細については、ループバック接続を無効にする（6 ページ）を参照してください。
5. コンピュータブラウザーサービスを設定します。詳細については、アンチウイルスのインストール前のコンピュータブラウザーサービスの設定（7 ページ）を参照してください。
6. アクイジション、レビュー、INW クライアントの各マシンでのインストールには、以下のルート証明書および中間証明書が必要です。
   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt
7. 以下のサブステップを繰り返して、ステップ 6 にリストされている 5 つの必要なルートおよび中間レベルの証明書をインストールします。
   a. C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro*** に移動します。
   注 INW で、C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro に移動します。
   b. 上記のフォルダパスが存在しない場合は、インストールに必要なルートおよび中間レベルの証明書を手動で取得します。
   c. ***AddTrustExternalCARoot.crt*** をダブルクリックして、MLCL システム（アクイジション、レビュー、INW）にインストールします。
   d. 証明書を開いて、***Install Certificate*（証明書のインストール）**をクリックします。

e. ***Certificate Import Wizard*（証明書のインストールウィザード）**が表示されたら、***Next*（次へ）**をクリックします。

f. ***Certificate Store*（証明書ストア）**ウィンドウで、***Place all certificates in the following store*（すべての証明書を次のストアに置く）**を選択して ***Browse*（参照）**をクリックします。

g. ***Show physical stores*（物理ストアを表示する）> *Trusted Root Certification Authorities*（信頼されたルート証明機関）> *Local Computer*（ローカルコンピュータ）**にチェックマークを入れて ***OK*** をクリックします。

h. ***Certificate Import Wizard*（証明書のインポートウィザード）**で、***Next*（次へ）**をクリックします。

i. ***Finish*（完了）**をクリックします。***The import was successful*（インポートが正常に完了しました）**メッセージが表示されるはずです。

j. ステップ 6 にリストされている他の証明書について、ステップ 7 を繰り返します。

注 : 各証明書には有効期限があります。証明書の有効期限が切れたら、OfficeScan エージェントが期待通りに機能するように MLCL システムで証明書を更新する必要があります。

Trend Micro OfficeScan - 新規インストールの配備手順（12.0 用推奨プッシュインストール方法）

1. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *TrendMicro OfficeScan server*（*TrendMicro OfficeScan* サーバー）- < サーバー名 > > *Office Scan Web Console*（ウイルスバスター *Corp. Web* コンソール）**をクリックします。

注 : ***Continue to this website (not recommended)*（このサイトの閲覧を続行する（推奨されません））**を選択して続行します。Security Alert（セキュリティの警告）ウィンドウで、***In the future, do not show this warning*（今後、この警告を表示しない）**にチェックマークを入れ、***OK*** をクリックします。

2. サイトが信用できないことを示す証明書エラーを受け取ったら、証明書に Trend Micro OfficeScan を含めるように管理します。

3. プロンプトが表示されたら、***AtxEnc*** アドオンをインストールします。Security Warning（セキュリティ警告）画面が表示されます。

   a. ***Install*（インストール）**をクリックします。

4. ユーザー名とパスワードを入力し、***Log On*（ログオン）**をクリックします。

5. プロンプトが表示されたら、***Update Now*（今すぐ更新）**をクリックして新しいウェジットをインストールします。新しいウェジットが更新されるまで待ちます。更新完了画面が表示されます。

   a. ***OK*** をクリックします。

6. トップメニューバーで、***Agents*（エージェント）> *Agent Installation*（エージェントのインストール）> *Remote*（リモート）**をクリックします。

7. プロンプトが表示されたら、***AtxConsole*** アドオンをインストールします。Security Warning（セキュリティ警告）画面が表示されます。

   a. ***Install*（インストール）**をクリックします。

8. ***Remote Installation*（リモートインストール）**ウィンドウで ***My Company*（マイカンパニー）**をダブルクリックします。***OfficeScan Server*（*OfficeScan* サーバー）**の下に、すべてのドメインが一覧表示されます。

9. リストから、ドメイン（例：INW Server）をダブルクリックします。そのドメインに接続されているすべてのシステムが表示されます。

注： ドメインまたはシステムが ***Domains and Endpoints*（ドメインとエンドポイント）**ウィンドウに一覧表示されない場合は、ドメインおよびエンドポイントウィンドウに一覧されていないドメインまたはシステムのトラブルシューティング（77 ページ）に移動して手動で追加するか、クライアントマシンから直接インストールを実行します。

10. クライアントマシン（アクイジション、レビュー、INW Server）を選択し、***Add*（追加）**をクリックします。

11. < ドメイン名 >\ ユーザー名とパスワードを入力し、***Log on*（ログオン）**をクリックします。

12. ***Selected Endpoints*（選択したエンドポイント）**領域でクライアントマシン（アクイジション、レビュー、INW Server）を 1 つずつ選択し、***Install*（インストール）**をクリックします。

13. 確認ボックスで ***Yes*（はい）**をクリックします。

14. ***Number of agents to which notifications were sent*（通知を送信したエージェント数）**メッセージボックスで、***OK*** をクリックします。

15. すべてのクライアントマシン（アクイジション、レビュー、INW Server）を再起動し、すべてのクライアントマシンで管理者またはそのグループのメンバーとしてログインして、システムトレイの Trend Micro OfficeScan アイコンが青に緑のチェックマークの付いた記号に変わるまで待ちます。

16. ***Log off*（ログオフ）**リンクをクリックし、***OfficeScan Web Console*（ウイルスバスター *Corp. Web* コンソール）**を閉じます。

12.0 用 Trend Micro OfficeScan サーバーコンソールの設定

1. ***Start*（スタート）> *All Programs*（すべてのプログラム）> *TrendMicro Office Scan server* < サーバー名 > > *Office Scan Web Console***（ウイルスバスター Corp. Web コンソール）を選択します。***Trend Micro OfficeScan Login*（*Trend Micro OfficeScan* ログイン）**画面が表示されます。

2. ユーザー名とパスワードを入力し、***Login*（ログイン）**をクリックします。***Summary*（サマリ）**画面が表示されます。

3. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

4. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

5. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Manual Scan Settings*（手動検索設定）**を選択します。***Manual Scan Settings*（手動検索設定）**画面が表示されます。

6. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

- ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
- ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
- ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**
- ***Virus/Malware Scan Settings only*（ウイルス / 不正プログラム検索設定のみ）> *Scan boot area*（ブートエリア検索）。**
- ***CPU Usage*（*CPU* 使用率）> *Low*（低）。**

7. Scan Exclusion（検索除外）タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

   - ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
   - ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
   - ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed and select Add path to agent Computers Exclusion list*（*Trend Micro* 製品がインストールされているディレクトリを除外し、エージェントのコンピュータ除外リストへのパスの追加を選択する）。**
   - ***Saving the officescan agent's exclusion list does the following:*（以下を行なう *officescan* エージェントの除外リストの保存：）**の下にあるドロップダウンリストから ***Adds path to*（パスの追加先）**を選択します。
   - **C:\Program Files (x86)\GE Healthcare\MLCL**、**C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** フォルダを 1 つずつ入力し、***Add*（追加）**をクリックします。

8. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。

9. ***The exclusion list on this screen will replace the exclusion list on the agents or domains you selected in the client tree earlier. Do you want to proceed?*（この画面の除外リストは、以前クライアントツリーで選択したエージェント上またはドメイン上の除外リストに置き換わります。続行しますか *?*）**というメッセージで、***OK*** をクリックします。

10. ***Close*（閉じる）**をクリックし、***Manual Scan Settings*（手動検索設定）**画面を閉じます。

11. 上部領域で、***Agent*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

12. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

13. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Real-time Scan Settings*（リアルタイム検索設定）**を選択します。***Real-time Scan Settings*（リアルタイム検索設定）**画面が表示されます。

14. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

   - ***Real-time Scan Settings*（リアルタイム検索設定）> *Enable virus/malware scan*（ウイルス / 不正プログラムの検索を有効にする）。**
   - ***Real-time Scan Settings*（リアルタイム検索設定）> *Enable spyware/grayware scan*（スパイウェア / グレーウェア検索を有効にする）。**
   - ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
   - ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
   - ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**

- ***Virus/Malware Scan Settings Only*（ウイルス / 不正プログラム検索設定のみ）> *Enable IntelliTrap*（*IntelliTrap* を有効にする）。**

15. Scan Exclusion（検索除外）タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

    - ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
    - ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
    - ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed*（トレンドマイクロ製品がインストールされているディレクトリの除外）。**
    - ***C:\Program Files (x86)\GE Healthcare\MLCL*、*C:\Program Files \GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*\、*G:*\ のフォルダパスが ***Exclusion List*（除外リスト）**にあることを確認します。

16. ***Action*（処理）**タブをクリックします。

17. デフォルト設定は変更せず、以下のオプションのチェックマークを外します。

    - ***Virus/Malware*（ウイルス / 不正プログラム）> *Display a notification message on endpoints when virus/malware is detected*（ウイルス / 不正プログラムを検知した場合、エンドポイントに通知メッセージを表示する）。**
    - ***Spyware/Grayware*（スパイウェア / グレーウェア）> *Display a notification message on endpoints when spyware/grayware is detected*（スパイウェア / グレーウェアを検知した場合、エンドポイントに通知メッセージを表示する）。**

18. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。

19. ***Close*（閉じる）**をクリックし、***Real-time Scan Settings*（リアルタイム検索設定）**画面を閉じます。

20. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

21. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

22. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Scheduled Scan Settings*（予約検索設定）**を選択します。***Scheduled Scan Settings*（予約検索設定）**画面が表示されます。

23. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

    - ***Scheduled Scan Settings*（予約検索設定）> *Enable virus/malware scan*（ウイルス / 不正プログラムの検索を有効にする）。**
    - ***Scheduled Scan Settings*（予約検索設定）> *Enable spyware/grayware scan*（スパイウェア / グレーウェアの検索を有効にする）。**
    - ***Schedule*（スケジュール）> *Weekly, every Sunday, Start time:00:00 hh:mm*（毎週、毎日曜日、開始時間：*00:00 hh:mm*）。**
    - ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
    - ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
    - ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**
    - ***Virus/Malware Scan Settings only*（ウイルス / 不正プログラム検索設定のみ）> *Scan boot area*（ブートエリア検索）。**

- ***CPU Usage*（*CPU* 使用率）> *Low*（低）。**

24. Scan Exclusion（検索除外）タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

    - ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
    - ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
    - ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed*（トレンドマイクロ製品がインストールされているディレクトリの除外）。**
    - ***C:\Program Files (x86)\GE Healthcare\MLCL*、*C:\Program Files \GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*、*G:*** のフォルダパスが Exclusion List（除外リスト）にあることを確認します。

25. ***Action*（処理）**タブをクリックします。

26. デフォルト設定は変更せず、以下のオプションのチェックマークを外します。

    - ***Virus/Malware*（ウイルス / 不正プログラム）> *Display a notification message on the endpoints when virus/malware is detected*（ウイルス / 不正プログラムを検知した場合、エンドポイントに通知メッセージを表示する）。**
    - ***Spyware/Grayware*（スパイウェア / グレーウェア）> *Display a notification message on the endpoints when spyware/grayware is detected*（スパイウェア / グレーウェアを検知した場合、エンドポイントに通知メッセージを表示する）。**

27. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。

28. ***Close*（閉じる）**をクリックし、***Scheduled Scan Settings*（予約検索設定）**画面を閉じます。

29. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

30. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

31. ***Settings*（設定）**オプションから、***Scan Settings*（検索設定）> *Scan Now Settings*（今すぐ検索の設定）**を選択します。***Scan Now Settings*（今すぐ検索の設定）**画面が表示されます。

32. ***Target*（対象）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

    - ***Scan Now Settings*（今すぐ検索の設定）> *Enable virus/malware scan*（ウイルス / 不正プログラムの検索を有効にする）。**
    - ***Scan Now Settings*（今すぐ検索の設定）> *Enable spyware/grayware scan*（スパイウェア / グレーウェアの検索を有効にする）。**
    - ***Files to Scan*（検索対象ファイル）> *File types scanned by IntelliScan*（*IntelliScan* によって検索されるファイルの種類）。**
    - ***Scan Settings*（検索設定）> *Scan compressed files*（圧縮ファイルの検索）。**
    - ***Scan Settings*（検索設定）> *Scan OLE objects*（*OLE* オブジェクトをスキャン）。**
    - ***Virus/Malware Scan Settings only*（ウイルス / 不正プログラム検索設定のみ）> *Scan boot area*（ブートエリア検索）。**
    - ***CPU Usage*（*CPU* 使用率）> *Low*（低）。**

33. ***Scan Exclusion*（検索除外）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

- ***Scan Exclusion*（検索除外）> *Enable scan exclusion*（検索除外を有効にする）。**
- ***Scan Exclusion*（検索除外）> *Apply scan exclusion settings to all scan types*（すべての検索タイプに検索除外設定を適用する）。**
- ***Scan Exclusion List (Directories)*（検索除外リスト（ディレクトリ））> *Exclude directories where Trend Micro products are installed*（トレンドマイクロ製品がインストールされているディレクトリの除外）。**
- ***C:\Program Files (x86)\GE Healthcare\MLCL*、*C:\Program Files \GE Healthcare\MLCL*、*D:\GEData\Studies*、*E:*** および ***G:*** を確認します。

34. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。
35. ***Close*（閉じる）**をクリックし、***Scan Now Settings*（今すぐ検索の設定）**画面を閉じます。
36. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。
37. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
38. ***Settings*（設定）**オプションから、***Web Reputation Settings*（*Web* レピュテーション設定）**を選択します。***Web Reputation Settings*（*Web* レピュテーション設定）**画面が表示されます。
39. ***External Clients*（外部クライアント）**タブをクリックし、***Enable Web reputation policy on the following operating systems*（次のオペレーティングシステムで *Web* レピュテーションポリシーを有効にする）**のチェックマークを外します（インストール時に既に選択されている場合）。
40. ***Internal Agents*（内部エージェント）**タブをクリックし、***Enable Web reputation policy on the following operating systems*（次のオペレーティングシステムで *Web* レピュテーションポリシーを有効にする）**のチェックマークを外します（インストール時に既に選択されている場合）。
41. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。
42. ***Close*（閉じる）**をクリックして、***Web Reputation*（*Web* レピュテーション）**画面を閉じます。
43. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。
44. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。
45. ***Settings*（設定）**オプションから、***Behavior Monitoring Settings*（挙動監視設定）**を選択します。***Behavior Monitoring Settings(* 挙動監視設定 *)*** 画面が表示されます。
46. ***Enable Malware Behavior Blocking*（不正プログラムの挙動ブロックを有効にする）**オプションおよび ***Enable Event Monitoring*（イベント監視を有効にする）**オプションのチェックマークを外します。
47. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。
48. ***Close*（閉じる）**をクリックして、***Behavior Monitoring*（挙動監視）**画面を閉じます。
49. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。
50. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

51. ***Settings*（設定）**オプションから、***Device Control Settings*（デバイスコントロール設定）**を選択します。***Device Control Settings*（デバイスコントロール設定）**画面が表示されます。

52. ***External Agents*（外部エージェント）**タブをクリックして、以下のオプションのチェックマークを外します。

    - ***Notification*（通知）> *Display a notification message on endpoints when OfficeScan detects unauthorized device access*（*OfficeScan* がデバイスへの不正アクセスを検知した場合、エンドポイントに通知メッセージを表示する）。**
    - ***Block the AutoRun function on USB storage devices*（*USB* ストレージデバイスの自動実行機能をブロックする）。**
    - ***Enable Device Control*（デバイスコントロールを有効にする）。**

53. ***Internal Agents*（内部エージェント）**タブをクリックして、以下のオプションのチェックマークを外します。

    - ***Notification*（通知）> *Display a notification message on endpoints when OfficeScan detects unauthorized device access*（*OfficeScan* がデバイスへの不正アクセスを検知した場合、エンドポイントに通知メッセージを表示する）。**
    - ***Block the AutoRun function on USB storage devices*（*USB* ストレージデバイスの自動実行機能をブロックする）。**
    - ***Enable Device Control*（デバイスコントロールを有効にする）。**

54. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。

55. ***Close*（閉じる）**をクリックして、***Device Control Settings*（デバイスコントロール設定）**画面を閉じます。

56. ***Settings*（設定）**オプションから、もう一度 ***Device Control Settings*（デバイスコントロール設定）**を選択します。***Device Control Settings*（デバイスコントロール設定）**画面が表示されます。

57. ***External Agents*（外部エージェント）**タブをクリックして、***Enable Device Control*（デバイスコントロールを有効にする）**のチェックマークを外します。

58. ***Internal Agents*（内部エージェント）**タブをクリックして、***Enable Device Control*（デバイスコントロールを有効にする）**のチェックマークを外します。

59. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。

60. ***Close*（閉じる）**をクリックして、***Device Control Settings*（デバイスコントロール設定）**画面を閉じます。

61. 左側の領域から、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

62. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

63. ***Settings*（設定）**オプションから、***Privileges and Other Settings*（権限とその他の設定）**を選択します。

64. ***Privileges*（権限）**タブをクリックして、以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

    - ***Scan Privileges*（検索権限）> *Configure Manual Scan Settings*（手動検索設定の構成）。**
    - ***Scan Privileges*（検索権限）> *Configure Real-time Scan Settings*（リアルタイム検索設定の構成）。**

- ***Scan Privileges*（検索権限）> *Configure Scheduled Scan Settings*（予約検索設定の構成）。**
- ***Proxy Setting Privilege*（プロキシ設定権限）> *Allow the agent user to configure proxy settings*（エージェントユーザーによるプロキシ設定を許可する）。**
- ***Uninstallation*（アンインストール）> *Requires a password*（パスワードが必要）。**適切なパスワードを入力して、パスワードを確認します。
- ***Unload and Unlock*（アンロードとアンロック）> *Requires a password*（パスワードが必要）。**適切なパスワードを入力して、パスワードを確認します。

65. ***Other Settings*（その他の設定）**タブをクリックします。

66. すべてのオプションのチェックマークを外します。

注 : 必ず以下のオプションのチェックマークを外してください。

- ***OfficeScan AgentSelf-protection*（*OfficeScan* エージェントの自己保護）> *Protect OfficeScan agent services*（*OfficeScan* エージェントサーバーを保護する）。**
- ***AgentSelf-protection*（*OfficeScan* エージェントの自己保護）> *Protect files in the OfficeScan agent installation folder*（*OfficeScan* エージェントインストールフォルダ内のファイルを保護する）。**
- ***AgentSelf-protection*（*OfficeScan* エージェントの自己保護）> *Protect OfficeScan agent registry keys*（*OfficeScan* エージェントレジストリキーを保護する）。**
- ***OfficeScan AgentSelf-protection*（*OfficeScan* エージェントの自己保護）> *Protect OfficeScan agent processes*（*OfficeScan* エージェントプロセスを保護する）。**

67. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。

68. ***Close*（閉じる）**をクリックし、***Privileges and Other Settings*（権限とその他の設定）**画面を閉じます。

69. 上部領域で、***Agents*（エージェント）> *Agent Management*（エージェント管理）**リンクを選択します。

70. 左側にある ***OfficeScan Server*（ウイルスバスター *Corp.* サーバー）**を選択します。

71. ***Settings*（設定）**オプションから、***Additional Service Settings*（その他のサービスの設定）**を選択します。

72. ***Enable service on the following operating systems*（次のオペレーティングシステムでサービスを有効にする）**オプションのチェックマークを外します。

73. ***Apply to All Agents*（すべてのエージェントに適用）**をクリックします。

74. ***Close*（閉じる）**をクリックし、***Additional Service Settings*（その他のサービスの設定 *)***画面を閉じます。

75. 上部領域で、***Agents*（エージェント）> *Global Agent Settings*（グローバルエージェント設定）**リンクを選択します。

76. 以下のオプションのみ選択します。その他のオプションのチェックマークは外します。

- ***Scan Settings for Large Compressed Files*（大きな圧縮ファイルの検索設定）> *Do not scan files in the compressed file if the size exceeds 2 MB*（サイズが *2 MB* を超える場合は圧縮ファイルのファイルを検索しない）**。これは、***Real-Time Scan*（リアルタイム検索）**および ***Manual Scan/Schedule Scan/Scan Now*（手動検索 */* 予約検索 */ ScanNow*）**にも適用されます。
- ***Scan Settings for Large Compressed Files*（大きな圧縮ファイルの検索設定）> *In a compressed file scan only the first 100 files*（圧縮ファイル内の最初の *100* ファイル**

だけを検索する）。これは、***Real-Time Scan*（リアルタイム検索）**および***Manual Scan/Schedule Scan/Scan Now*（手動検索 / 予約検索 /*ScanNow*）**にも適用されます。

- ***Scan Settings*（検索設定）> *Exclude the OfficeScan server database folder from Real-time Scan*（ウイルスバスター *Corp.* サーバーのデータベースフォルダをリアルタイム検索の対象から除外）。**
- ***Scan Settings*（検索設定）> *Exclude Microsoft Exchange server folders and files from scans*（*Microsoft Exchange* サーバーのフォルダおよびファイルを検索から除外）。**

77. ***Save*（保存）**をクリックします。
78. 上部領域で、***Updates*（更新）> *Agents*（エージェント）> *Manual Updates*（手動更新）**リンクを選択します。
79. ***Manually select agents*（エージェントを手動で選択する）**を選択して、***Select*（選択）**をクリックします。
80. ***OffceScan Server*（*OffceScan* サーバー）**の下にある適切なドメイン名をダブルクリックします。
81. クライアントシステムを 1 つずつ選択して、***Initiate Update*（更新を開始する）**をクリックします。
82. メッセージボックスで ***OK*** をクリックします。
83. ***Log off*（ログオフ）**をクリックし、ウイルスバスター Corp. Web コンソールを閉じます。

Trend Micro OfficeScan インストール後のガイドライン

1. ループバック接続を有効にします。詳細については、ループバック接続を有効にする（6 ページ）を参照してください。
2. コンピュータブラウザーサービスを設定します。詳細については、アンチウイルスのインストール後のコンピュータブラウザーサービスの設定（7 ページ）を参照してください。

ドメインおよびエンドポイントウィンドウに一覧されていないドメインまたはシステムのトラブルシューティング

Trend Micro OfficeScan Client/Server Edition 11.0 SP1 および Trend Micro OfficeScan Client/Server Edition XG 12.0 いずれかの推奨プッシュインストール方法を実施するときは、システムにインストール内容をプッシュするため、ドメインおよびシステムが一覧されている必要があります。この手順では、ウイルス対策ソフトウェアをクライアント（アクイジション、レビュー、INW）にインストールする 2 つのオプションがあります。

11.0 SP1 については、Trend Micro OfficeScan - 新規インストールの配備手順（11.0 SP1 用推奨プッシュインストール方法）（58 ページ）を参照してください。
12.0 については、Trend Micro OfficeScan - 新規インストールの配備手順（12.0 用推奨プッシュインストール方法）（69 ページ）を参照してください。

1. 管理コンソールのクライアントマシン（アクイジション、レビュー、INW）の IP アドレスを使用して、以下を実行します。
   a. 各クライアントシステムの IP を 1 つずつ ***Search for endpoints*（エンドポイントの検索）**ボックスに入力してから ***Enter*** を押します。

b. ***<domain name>\username*（< ドメイン名 >\ ユーザー名）**とパスワードを入力し、***Log on*（ログオン）**をクリックします。

c. お手持ちの Trend Micro バージョンにもとづいて、次のいずれかの手順を選択してください。

i. 11.0 SP1 の場合、手順 58 ページの 10 に戻ります。

ii. 12.0 の場合、手順 70 ページの 10 に戻ります。

2. システムの IP アドレスがわからない、または以前のオプションの設定に失敗した場合は、各クライアントマシン（アクイジション、レビュー、INW Server）に戻って以下を実行します。

a. すべてのクライアントマシンで**管理者**またはグループメンバーとしてログインします。

b. ***Start*（スタート）> *Run*（実行）**をクリックします。

c. ***<Anti-Virus Management Console_server_IP_address>*** を入力して、***Enter*** を押します。プロンプトが表示されたら、管理者ユーザー名とパスワードを入力します。

d. ***<Anti-Virus Management Console_server_IP _address>**ofsscan*** に移動して、***AutoPcc.exe*** をダブルクリックします。プロンプトが表示されたら、管理者ユーザー名とパスワードを入力します。

e. インストールが完了したらクライアントシステムを再起動します。

f. すべてのクライアントマシンで**管理者**またはグループメンバーとしてログインし、システムトレイの Trend Micro OfficeScan アイコンが青に緑のチェックマークの付いた記号に変わるまで待ちます。

g. お手持ちの Trend Micro バージョンにもとづいて、次のいずれかの手順を選択してください。

i. 11.0 SP1 については、11.0 SP1 用 Trend Micro OfficeScan サーバーコンソールの設定（59 ページ）を参照してください。

ii. 12.0 については、12.0 用 Trend Micro OfficeScan サーバーコンソールの設定（70 ページ）を参照してください。