一般的なウイルス対策ガイドライン

ウイルス対策ガイドライン

ウイルス対策のアプリケーションには、データのスキャンとサーバ上でのデータのスキャン方法を詳細に制御できる、多数の構成オプションがあります。

どのウイルス対策製品を使用する場合でも、スキャンとサーバパフォーマンスのバランスを取る設定が必要です。スキャンの実行を選択すればするほど、潜在的なパフォーマンスオーバーヘッドが大きくなります。システム管理者の役割は、特定の環境内でウイルス対策アプリケーションをインストールするための、最適な設定要件を判断することです。詳細な設定情報については、特定のウイルス対策製品のマニュアルを参照してください。

この章のガイドラインに準拠しているサードパーティ製のウイルス対策ソフトウェア製品を使用することができます。シスコがテスト済みのウイルス対策ソフトウェア製品の一覧については、https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-device-support-tables-list.html にある *Contact Center Enterprise* 互換性マトリクス を参照してください。

サードパーティ製ソフトウェア製品に関するシスコガイドラインの詳細については、https://www.cisco.com/c/en/us/products/collateral/customer-collaboration/unified-ip-interactive-voice-response-ivr/prod_bulletin09186a0080207fb9.html にある「サードパーティ製のソフトウェアおよびセキュリティアップデートを使用する場合の *Cisco Customer Contact* 情報」を参照してください。

警告 多くの場合、デフォルトの AV 設定により、CPU の負荷とメモリとディスク使用量が増加し、ソフトウェアパフォーマンスに悪影響を及ぼします。シスコは特定の構成をテストして製品のパフォーマンスを最大化します。Unified ICM/Unified CCE で AV ソフトウェアを使用するには、次のガイドラインを使用する必要があります。

ウイルスは予測不可能で、シスコはミッションクリティカルなアプリケーションに対するウイルス攻撃の影響に対して責任を負うことはできません。Microsoft Internet Information Server（IIS）を使用するシステムには、特に注意してください。

次のリストでは、一般的なガイドラインについて説明します。

- 企業のウイルス対策戦略に、企業のファイアウォールの外部に配置されているサーバ、またはパブリックインターネットに頻繁に接続する対象となるサーバに関する特定の規定が含まれていることを確認します。
- Unified ICM/Unified CCE のリリースに対して適格で承認されているアプリケーションおよびバージョンについては、*Contact Center Enterprise* 互換性マトリクス を参照してください。
- 組織のポリシーに従って、AV ソフトウェアと定義ファイルを定期的に更新します。
- リモートドライブ（ネットワークマッピングまたは UNC 接続など）からアクセスされているファイルのスキャンを回避します。可能な場合は、これらの各リモートマシンに、独自のウイルス対策ソフトウェアがインストールされていることを確認し、すべてのスキャンをローカルに保持します。多層構成のウイルス対策戦略では、ネットワーク全体のスキャンやネットワーク負荷の追加は必要ありません。
- AV ソフトウェアによるシステムの完全スキャンのスケジュールは、スケジュールされたメンテナンスウィンドウで**のみ**行い、AV スキャンによって他の Unified ICM メンテナンスアクティビティが中断できない場合にスケジュールを設定します。
- AV ソフトウェアが、自動またはバックグラウンドモードですべての着信データまたは変更ファイルをリアルタイムでスキャンしないように設定します。
- ヒューリスティックスキャンは、従来のウイルス対策スキャンよりもオーバーヘッドが大きくなります。この高度なスキャンオプションは、信頼できないネットワーク（電子メールやインターネットゲートウェイなど）からのデータエントリの重要なポイントでのみ使用します。
- リアルタイムまたはアクセス時のスキャンを有効にすることは可能ですが、その対象を着信ファイルだけにします（ディスクへの書き込み時）。このアプローチは、ほとんどのウイルス対策アプリケーションにとってのデフォルト設定です。ファイルの読み出しへのアクセス時のスキャンの実装は、高パフォーマンスアプリケーション環境において、システムリソースに対して必要以上に大きな影響を与えます。
- すべてのファイルを必要時にリアルタイムでスキャンすることで最適に保護できます。ただし、この設定では、悪意のあるコード（ASCII テキストファイルなど）をサポートできないファイルのスキャンのオーバーヘッドがあります。システムにリスクを与えないと分かっているすべてのスキャンモードのファイルまたはファイルのディレクトリを除外します。
- 使用時間が低い、またはアプリケーションアクティビティが最も低い時は、定期的なディスクスキャンをスケジュールします。
- サーバが電子メールを使用しない場合は、電子メールツールを無効にします。

- AV ソフトウェアでスパイウェアの検出と削除が行なわれる場合は、この機能を有効にします。感染したファイルをクリーンにするか、削除します（これらのファイルを削除できない場合）。
- AV アプリケーションでのロギングを有効にします。ログのサイズを 2 MB に制限します。
- 圧縮ファイルをスキャンするために AV ソフトウェアを設定します。
- AV ソフトウェアが CPU の使用率をいつでも 20% を超えないように設定します。
- AV ソフトウェアが使用可能な場合は、バッファオーバーフロー保護を有効します。
- AV ソフトウェアを設定して、システムの起動時に起動します。

Unified ICM/Unified CCE メンテナンスパラメータ

いくつかのパラメータは、特定の時間にアプリケーション アクティビティを制御します。Unified ICM/Unified CCE サーバで AV ソフトウェア アクティビティのスケジュールを設定する前に、重要な時期にウイルス対策ソフトウェアの設定で 「[毎日のスキャン（Daily Scans）]」「[自動 DAT 更新（Automatic DAT Updates）]」 および 「[自動製品アップグレード（Automatic Product Upgrades）]」 をスケジュールされないことを確認してください。

ロガーに関する検討事項

AV ソフトウェアアクティビティを、次のロガーのレジストリキーで指定されている時間と一致するスケジュールに設定しないでください。

- HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<inst>\Logger<A/B>\Recovery\CurrentVersion\Purge\Schedule\Schedule Value Name: Schedule
- HKLM\SOFTWARE\Cisco Systems, Inc.\ICM\<inst>\Logger<A/B>\Recovery\CurrentVersion\UpdateStatistics\Schedule Value Name: Schedule

ディストリビュータに関する検討事項

AV ソフトウェアアクティビティを、次のディストリビュータのレジストリキーで指定されている時間と一致するスケジュールに設定しないでください。

- HKLM\SOFTWARE\Cisco Systems, Inc. \ICM\<inst>\Distributor\RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\Purge\Schedule Value Name: Schedule
- HKLM\SOFTWARE\Cisco Systems, Inc. \ICM\<inst>\Distributor\RealTimeDistributor\CurrentVersion\Recovery\CurrentVersion\UpdateStatistics\Schedule Value Name: Schedule

コールルータと PG に関する検討事項

CallRouter および周辺機器ゲートウェイ（PG）で、次のタイミングで AV プログラム タスクのスケジュールを設定しないでください。

- コール負荷がピークまたは重い時間帯。
- 30 分と 1 時間の時刻になるとき。Unified ICM プロセスはこれらの時間帯に増加します。

その他のスケジュールされたタスクに関する検討事項

Windows 上で他のスケジュール された Unified ICM プロセスアクティビティは、[スケジュール済みタスク（Scheduled Tasks）] フォルダを調べることで確認できます。スケジュールされた AV プログラムアクティビティが、Unified ICM のスケジュール済みアクティビティと競合しないよう確認します。

ファイルタイプの除外に関する検討事項

Unified ICM プロセスの操作中に書き込まれるいくつかのバイナリファイルには、ウイルス感染のリスクはほとんどありません。

AV プログラムのドライブおよびオンアクセススキャン設定から、次のファイル拡張子を含むファイルを省略します。

- *.hst は PG に適用されます。
- *.ems は ALL に適用されます。
- *.repl
- *.localrepl

（注） アウトバウンド高可用性の複製を使用している場合 、**repl** ディレクトリ（`/icm/<cust>/la` または `lb/repl` は、ウイルス対策のスキャンから除外する必要があります。

（注） すべてのウイルス対策スキャンから *c:\icm* フォルダを除外します。