



ホワイト ペーパー

# Cisco Security Agent 導入ベスト プラクティス ガイド

## はじめに

Cisco<sup>®</sup> Security Agent (CSA) は、悪意のあるネットワーク活動による未知の脅威から、エンドポイント サーバとデスクトップを保護するために使用します。Cisco Security Agent は、悪意のある動作を識別して防止するので、既知および未知 (Day Zero) の攻撃からネットワークを守ることができます。Cisco Security Agent では、悪意のあるモバイル コードに対する保護、システムの完全性保証、監査ログの統合のほか、侵入検知や分散ファイアウォール機能を提供することによって、複数のエンドポイント セキュリティ機能の集約と拡張を実現します。Cisco Security Agent をネットワーク全体にわたって適切に展開し、Cisco Security Agent Management Center (CSA MC) からエージェントの設定と管理を行うことによって、こうした機能を有効に利用できます。

Cisco Security Agent を企業全体で適切に展開するには、まず Cisco Security Agent の運用や操作に精通している必要があります。この情報は、次の文書に記載されています。

- 『Management Center for Cisco Security Agents ユーザ ガイド』
- 『Management Center for Cisco Security Agents のインストール』

これらの文書のほか、より確実な展開のための手段には、次のようなものがあります。

- Cisco Security Agent 管理者トレーニング「Securing Hosts Using Cisco Security Agent」(シスコのトレーニング パートナーが提供している 2 日間のコース) を受講する。
- 展開に必要な技術リソースが社内で用意できない場合は、シスコのパートナー各社 (認定トレーニングを修了している必要があります)、あるいはシスコのセキュリティ サービス グループに相談する。

この文書では主に、企業全体への Cisco Security Agent の導入についてのベスト プラクティスを紹介します。この文書は Cisco Security Agent を展開する準備段階で非常に役立ちますが、エージェントの実装を成功させるには、次の資料を読むことが不可欠です。

- 『Management Center for Cisco Security Agents ユーザ ガイド』および『Management Center for Cisco Security Agents のインストール』 (製品メディアに含まれている製品マニュアル)

この文書はいくつかの章に分かれています。

- 展開プロセスの概要
- デフォルト ポリシーを使用した展開のベスト プラクティス (第一段階では、テスト モードで、デフォルト ポリシーを使用して展開します。テスト モード期間が完了したら、必要に応じて、デフォルト ポリシーの一部だけを保護モードにし、それ以外のデフォルト ポリシーはテスト モードのままにして使用できます。この場合、システムは一部の攻撃に対しては脆弱なままですが、ただちに完全な保護機能を起動する機能も装備されており、すべてのテストを企業の本稼働環境で実施できます。)
- ユーザ側で作成したポリシーを使用した展開のベスト プラクティス (お客様が非常に制限的な環境を必要としている場合においても、まずはデフォルト ポリシーを使用した実装を完成させてからそのような環境を構築することを推奨します。)

## 展開の概要

ネットワーク環境に新しいセキュリティツールを導入しようとする、いろいろな難問や落とし穴が必ず発生します。そうした問題を克服するには、新しいセキュリティツールを展開する最初の段階での実装計画が重要になります。ネットワークおよびセキュリティのベスト プラクティス手順では、新しいソフトウェアやツールをネットワークに展開する場合、まずテストネットワークで展開します。このテスト ネットワークには、本稼働のネットワークで使用するシステムのサンプルが稼働しているのが理想的です。こうすれば、ネットワーク技術者やセキュリティスタッフは、本稼働のシステムに影響を与えずに新しいソフトウェアの影響を評価できます。この方法は小規模なネットワークでは難しい場合もあります。しかし、ある程度でも実施することを推奨します。このような作業は、セキュリティおよびネットワーク スタッフにとって、新しいソフトウェアやツールに精通する貴重な機会にもなります。

新しいソフトウェア製品、ソフトウェアパッチ、またはシステムをネットワークに展開する場合と同様に、Cisco Security Agent の展開でも、事前の計画と時間が必要です。さらに、最終的に問題のない展開を実現するためには、何度でもやり直せる環境が用意されていることが必要です。ネットワーク全体への Cisco Security Agent ソフトウェアの展開を成功させるには、次のようなステップが必要です。

- CSA MC をインストールする。
- 使用する Cisco Security Agent 展開モデルを決定する。
  - 完全
  - デスクトップ システムのみ
  - サーバのみ
  - すべてのサーバと特定のデスクトップ / ノート
  - 特定のサーバと特定のデスクトップ / ノート
  - 特定のサーバのみ
- 展開の段階を定義する。
- テスト展開ネットワークを構築し、展開タイプに応じて Cisco Security Agent を展開する。
- テスト ネットワーク上で Cisco Security Agent の展開を調整（チューニング）する。
- テスト環境用に作成した展開モデルに従って、Cisco Security Agent を本稼働環境に段階的に展開する。
- 展開の各段階をモニタし、必要に応じて調整する。

以下では、上記の各段階についてより詳しく説明します。この文書は、Cisco Security Agent ソフトウェアをネットワークに展開する際の 1 つの指針として利用してください。

## CSA MC のインストール

CSA MC は、CiscoWorks VPN/Security Management Solution (VMS) ソフトウェアにバンドルされています。CSA MC は、現時点では、Windows 2000 Server または Windows 2000 Advanced Server にのみインストール可能です。簡単に説明すると、CSA MC は、エンドポイント システムに Cisco Security Agent キットを配信するための中央ロケーションであり、同時にポリシー アップデート サイトおよびアラーム コンソールでもあります。CSA MC ホストは、認証サーバや Syslog サーバといった管理ホストと一緒に、ネットワークの管理モジュールに配置してください。CSA MC とエージェント間の通信には、HTTP および HTTPS が使用されます。エージェントは、CSA MC との通信に TCP/5401 ポートを使用し、それが使用できない場合は代替ポートとして TCP/443 を使用します。Cisco Security Agent Profiler は、CSA MC との通信に TCP/5401 ポートを使用します。CSA MC は、Microsoft SQL Server データベース（大規模実装の場合）または Microsoft SQL Server Desktop Engine (MSDE)（小規模実装の場合）のいずれかを使用します。このデータベースは、企業全体の異なるエージェントに適用されるさまざまなポリシーの中央リポジトリとなるほか、アラームが集約され、情報の相関性が表示される中央ロケーションとなります。さらに CSA MC は、エンドポイント クライアントが Cisco Security Agent のインストールキットをダウンロードする際の中央ポイントでもあ

ります。CSA MC システムのハードウェアは、展開しようとしているネットワークの規模に合わせて適切に選択してください。能力不足のシステムを使用すると、Cisco Security Agent ソフトウェアの展開と動作においてボトルネックとなる可能性があります。このホストは、Cisco Security Agent ソフトウェア展開モデルの中心であり、Cisco Security Agent を実行しているすべてのホストから接続できる必要があります。CSA MC の最新バージョンでは、企業全体に展開した最大 10,000 エージェントを管理できます。エージェントがそれより多い場合は CSA MC を追加して、より多くのエージェントが処理できるようにする必要があります。

## Cisco Security Agent 展開モデルの決定

Cisco Security Agent ソフトウェアは、ユーザ デスクトップ システムとサーバの両方に展開できます。そのため、数種類の展開モデルが考えられます。ここでは、これらの展開モデルを紹介し、各モデルの長所と短所について説明します。検討中のネットワークに最適な展開モデルは、ネットワーク管理者と経営陣の判断によって決まります。

### 特定のサーバのみ

この展開モデルでは、インターネットに公開された Web サーバ、DNS (ドメイン ネーム システム) サーバ、データベース システム、その他の業務上「重要な」システムなど、特定のサーバだけに Cisco Security Agent ソフトウェアを展開します。これにより、重要なネットワーク関連サービスを提供するシステムについてのエンドポイント保護を実現できます。

### サーバのみ

この展開モデルでは、企業 LAN と DMZ に存在するすべてのサーバに Cisco Security Agent をインストールします。この展開モデルの場合、業務上の重要性が高いシステムだけでなく、重要性が低いシステムにも Cisco Security Agent をインストールします。この展開モデルの主な利点は、Cisco Security Agent をインストール可能なサーバ システムすべてをカバーできることです。

### 特定のサーバと特定のデスクトップ システム

この展開モデルでは、インターネットに公開された Web サーバ、DNS ホスト、データベース システム、その他の「重要な」システムといった特定のサーバに Cisco Security Agent をインストールします。さらに、デスクトップ システムにも Cisco Security Agent をインストールします。ただし、すべてのデスクトップにインストールするのではなく、企業の財務部門、人事部門、その他の機密データを処理する部門の社員が使用するホストに限定します。また、企業の内部 LAN から別のコンピューティング環境に持ち出す可能性のある、営業部門などの社員が使用するノート型システムにも、Cisco Security Agent をインストールする可能性があります。

### サーバと特定のデスクトップ システム

この展開モデルでは、業務上重要なサーバだけでなく、企業のすべてのサーバに Cisco Security Agent を展開し、さらに上記の「特定のサーバと特定のデスクトップ システム」展開モデルで説明したデスクトップ システムに Cisco Security Agent をインストールします。

### デスクトップ システムのみ

この展開モデルでは、すべてのエンドユーザ システム プラットフォームに Cisco Security Agent をインストールします。サーバはデスクトップよりもはるかに数が少なく、IT/情報セキュリティのスタッフが直接管理するため、常にモニタ、保守、およびパッチの適用が行われているという理由で、これには含めません。これに対してエンドユーザ デスクトップは数が多く、エンドユーザがどのように使っているかも多種多様です。さらに通常、ウィルスはユーザとの対話を必要とするので、これらのシステムに対策を施すことが必要になります。その他の脅威としては、攻撃者がユーザ アカウント情報の収集に使用するトロイの木馬プログラムなどがあります。この展開モデルの主な利点は、そのカバーする範囲の広さです。

## 完全

この展開モデルでは、サポート対象のプラットフォームすべて（サーバとデスクトップの両方）に Cisco Security Agent をインストールして保護します。このモデルの主な利点の 1 つは、カバーする範囲の広さです。

## 展開の段階の定義

多く場合、展開の各段階は、Cisco Security Agent ソフトウェアを使用するネットワークの規模によって異なります。ネットワークが小規模の場合は、短時間のうちに Cisco Security Agent エージェント キットをダウンロードしてインストールできるので、一度に展開することが可能です。ネットワークの規模が大きくなると、展開作業を複数の段階に分割し、部門組織ごとに実行するといったことが必要になります。したがってネットワーク スタッフは、Cisco Security Agent ソフトウェアを「限定された環境」に展開して、エージェントとポリシーを環境単位でモニタおよび調整するといった対応が必要です。いずれの場合も、Cisco Security Agent ソフトウェアの展開は、以下の一般的モデルが適用できます。

## テスト展開の構築

展開モデルを選択したら、次にテスト展開を構築します。テスト展開には、以下のようないくつかの目的があります。

- ネットワークおよびセキュリティ スタッフが、CSA MC のインストールと操作を経験できる。
- 展開モデルをテストするためのサンプル システムを用意できる。
- 本稼働環境への完全展開を行う前に、Cisco Security Agent ソフトウェアをシステム上に展開し、必要に応じて調整し、実装上の問題点を解決できるような環境を用意できる。
- ネットワークおよびセキュリティ スタッフが、Cisco Security Agent ソフトウェア システムの展開およびトラブルシューティングを経験できる。
- イベント ログの最適な管理方法を検討して決定できる。
- セキュリティ スタッフが、ネットワーク スキャナや攻撃ツールを利用して、Cisco Security Agent がインストールされたシステムに攻撃を実行し、ソフトウェアが起動する各種のアラームとその解析方法を経験できる。

テスト展開段階を完全に省略することは可能ですが、本稼働環境への展開に先立って Cisco Security Agent をテスト環境に展開することは非常に重要です。これによって、ネットワーク管理者やセキュリティ スタッフは、Cisco Security Agent ソフトウェアのインストールや操作を経験し、問題が発生する可能性のある領域についての知識を得られます。さらに、既存のセキュリティ対策と Cisco Security Agent とが矛盾する可能性を発見しやすくなります。最初にテスト モデルを利用すれば、本稼働環境への Cisco Security Agent の展開が成功する可能性は格段に高まります。

テスト環境を利用できない場合でも、VMware を使用すれば、Cisco Security Agent ソフトウェアの影響をテストできます。VMware では、抽象レイヤを提供することによって、単一のホスト上に「仮想システム」を作成できます。これにより、実際には仮想環境を利用している、専用ハードウェア上と同様に OS（オペレーティング システム）を実行できます。VMware を利用すれば、物理ハードウェアに多額のコストをかけることなく、さまざまなシステムに対する Cisco Security Agent の影響をテストできます。

ネットワーク上の典型的なアプリケーション ホストとなるシステムを選択してパイロット システムを構築すれば、ネットワーク内の特定のホストに対する Cisco Security Agent の影響をテストすることも可能です。こうしたホストのサブグループを利用することによって、本稼働環境全体には影響を与えずに、テスト用本稼働環境で Cisco Security Agent ソフトウェアを展開して評価できます。

## テスト展開における Cisco Security Agent の調整

### Cisco Security Agent のデフォルト ポリシーの実装

テスト展開で Cisco Security Agent を展開する場合は、OS 保護用のデフォルトの Cisco Security Agent ポリシーを基にして、サーバの OS の基本的な保護機能を提供するカスタムポリシーを作成するのが最適です。デフォルトの Cisco Security Agent ポリシーには、Nimda や Blaster のような新しい未知の攻撃をすべて阻止した実績があります。

テスト展開システムは、次のガイドラインに基づいて選択します。

- 各アプリケーション環境に、少なくとも 1 つのテスト システムを用意する。
- テスト システムは、本稼働システムの代表となるように設定する。
- 可能な場合は、必ず Quality Assurance (QA; 品質保証) サーバと本稼働環境サーバを含める (QA サーバは、Cisco Security Agent ソフトウェアのインストールによって悪影響が生じないことを確認するために使用します)。

保護する必要のあるアプリケーション環境のタイプごとに 1 つのグループをテスト モードで作成します。アプリケーション環境は、OS とサポート対象のアプリケーションという標準的な構成で構築します。以下のような例が考えられます。

- セールス部門の社員用のデスクトップ構成
- e- ビジネス アプリケーション サーバ
- バックエンド データベース サーバ

テスト モードでは、関連付けられたポリシーによって拒否されるようなイベントが起こっても、Cisco Security Agent はアクションを拒否せず、すべてのアクションをロギングします。テスト モードを使用すれば、技術者および管理者は、ホストに対するポリシー展開の影響を実施前に確認できます。これは、保護するアプリケーション環境に悪影響を与えないことを保証するために不可欠のステップです。

テスト展開を進める前に、セキュリティ スタッフがデフォルトの Cisco Security Agent ポリシーを検討して、自社のソリューションのセキュリティ要件に最も適合するポリシーを特定しておくことを推奨します。デフォルトの OS ポリシーは、ポリシー作成の開始点として最適です。さらに Cisco Security Agent には、Microsoft IIS や SQL Server といった、特定のアプリケーションに合わせて調整されたデフォルト ポリシーが付属しています。特定アプリケーション向けのこれらのポリシーは、各アプリケーション専用サーバのセキュリティを保護するために使用するテンプレートです。

デフォルト ポリシーだけで要件を満たせる場合は、OS 保護用のデフォルト ポリシーと、個別のデフォルト ポリシー (専用 IIS サーバ用など) の両方を、適切なグループに適用してください。ただし、Cisco Security Agent に付属のデフォルト ポリシーおよびグループは変更しないでください。デフォルト ポリシーおよびグループは、常に適当な名前を付けたコピーを作成して使用します (たとえば、テスト モードでセールス デスクトップを含むグループを作成する場合には、TEST-SALES-DESKTOPS といった名前を付けます)。

Cisco Security Agent のデフォルト ポリシーの微調整のためにデータ収集処理が必要であれば、Cisco Security Agent インストレーションキットを構築します。このエージェント キットは、ポート スキャン検出、SYN フラッディング保護、欠陥パケット検出などの機能を必要とするシステムにネットワーク シムをインストールします。保護するシステムに VPN またはファイアウォール保護が装備されていれば、ネットワーク シム機能は不要な場合もあります。テスト環境に展開するエージェント キットを準備したら、CSA MC にネットワーク経由でアクセスさせてキットをダウンロードするか、システム管理ソフトウェアによって対象のシステムにキットを送り込むことによって配布できます。

エージェント キットをすべて展開したら、テスト展開フェーズの次のステップは、(利用可能なら) テスト環境でアプリケーションまたはホスト機能のすべてのテストを実施することです。これによって、各アプリケーション環境用のデフォルト ポリシーの調整に必要な、アプリケーション固有のデータがすべて生成されます。

テスト展開作業と並行して、本稼働環境にあるすべてのパイロット システムでデータを収集することを推奨します。これは、QA 環境とともに本稼働環境に対して悪影響を与える可能性のあるルールを特定するのに役立ちます。展開規模によって異なり

ますが、**最低でも 2 ～ 4 週間**、本稼働システムでデータ収集を行います。システム管理者は、このデータ収集期間中に、運用に必要なスクリプトおよびソフトウェアをすべて実行します。実行すべき事柄には、以下のようなものが考えられます。

- システム バックアップ
- ネットワーク管理ソフトウェア
- システム スケジューラ

QA サーバでのデータ収集処理が完了したら、そのデータを分析して、(保護モードで適用した場合) アプリケーション環境に悪影響を与える可能性のあるポリシー ルールを特定します。

システムに悪影響を与える可能性のあるルールを特定したら、チューニング ウィザードを使用し、該当するアクションの「Allow ルール」を作成することによって、適用するポリシーを修正します。チューニング ウィザードを使用すれば、悪影響を発生させたルールのアクションを変更できます。このウィザードによって、イベント発生時にアプリケーション クラスとリソース情報を収集する「例外」の Allow ルールが自動生成され、Deny アクションの原因となったルールを打ち消すために Allow ルールが作成されます。

例外ルールを正しく構成することは重要です。例外ルールは、以下のように構成します。

- 保護するすべてのシステムに必要な Allow ルールを含めた企業の例外ポリシーを作成する。企業全体の例外ルールをすべてこのポリシーに追加する。
- グループごとに 1 つの例外ポリシーを作成する。このグループ例外ポリシーには、特定のグループに適用されるすべての Allow ルールを含める。

必要な例外ポリシーがすべて完成したら、それらのポリシーをそれぞれのグループに適用し、もう一度データ収集および調整を実施します。

このポリシーの調整の手順を 2 回繰り返せば、ルールが悪影響を与えない (正しく動作する) と言うことができます。パイロットシステムでは、保護モードを一度に 1 グループずつ有効にして、テスト計画のその他のコンポーネント (セキュリティ テスト、パフォーマンス、運用) を各グループについて実行し、ソリューションが計画どおり機能することを確認してください。

エージェント キットをアプリケーション環境に展開する場合に各 Cisco Security Agent グループで実行する手順をまとめると次のようになります。

- Cisco Security Agent をテスト モードで対象のすべてのシステムに展開する。
- データ収集と (必要に応じて) ポリシーの調整を行う。
- 保護モードを有効にする。
- セキュリティ、運用、およびエンジニアリングで機能させ、展開時に問題が生じないことを確認する。

### 本稼働環境への Cisco Security Agent の展開

テスト展開 (または本稼働環境内のパイロット展開) で Cisco Security Agent ソフトウェアの影響を確認できたら、次のステップは、本稼働環境全体にわたる Cisco Security Agent ソフトウェアの展開です。そのための方法には、次の 2 種類があります。

- 本稼働環境への段階的な展開
- 一度に展開

展開を成功させるためには、本稼働環境への段階的な展開を推奨します。この方式では、展開を管理可能な複数の部分に分割することになります。この分割は、以下のいくつかの特性に基づいて決定します (推奨される順番)。

- ネットワークにおけるシステムの役割 (データベース サーバ、アプリケーション サーバ、Web サーバなど)
- ネットワーク IP アドレスのブロック
- システムの物理的位置

システムの役割に基づいたグループに分割し、そのグループごとに Cisco Security Agent を展開するのが望ましい方法です。この方法では、エージェントキットを類似した複数システムに展開するので、予期しない問題が発生しても、同じような方法で対応できます。各段階における Cisco Security Agent ソフトウェアの展開は、テスト環境またはパイロット環境で実行したとおりに、まず最初に該当のポリシーセットをテスト モードで使用して実行します。こうしたやり方は二度手間のようなようですが、本稼働環境に Cisco Security Agent ソフトウェアを導入したために発生する問題をすべてモニタできます。システムの各グループに Cisco Security Agent をインストールしてあれば、ポリシー内の該当する場所で Deny アクションをアクティブ化するのは短時間でできます。

### 企業への大規模展開に関する考慮事項

企業への大規模展開では、企業の IT サポート スタッフの能力や経験に応じて、この文書で説明している方法を拡張する必要があるかもしれません。場合によっては、本稼働ネットワークへのエージェントの展開を、上記の方法よりもさらに細かく分割することが必要です。たとえば、人事部門や財務部門といったグループに Cisco Security Agent を展開するのではなく、それぞれのサブグループへの小規模な展開に分割することが必要になる可能性があります。これは特に、複数の地理的領域にまたがり、リモート ユーザにも影響を与えるような展開に当てはまります。展開する範囲をさらに分割することにより、Cisco Security Agent の展開が IT サポート スタッフのレベルで処理できるようになります。このような方法では余計に時間がかかる場合もありますが、展開における最大限の成功を保証するのに役立ちます。

### エンドポイントの調査 — Cisco Security Agent Profiler の使用

Cisco Security Agent Profiler は、アプリケーション環境の**厳重な**セキュリティポリシーを作成するためのツールです。プロファイラの主な目的は、Cisco Security Agent ソフトウェアでエンドポイントを分析できるようにして、使用中のアプリケーションのプロファイルおよび動作を定義することです。Cisco Security Agent Profiler を使用すれば、エンドポイントの分析結果に基づいて、ポリシーを自動生成することもできます。プロファイラ方式には2つの意味があります。

- アプリケーションをシステムから保護する。
- システムをアプリケーションから保護する。

Cisco Security Agent Profiler は、現在のアプリケーションと動作に基づいて、エンドポイント環境を把握するための強力なツールです。この情報を利用すれば、アプリケーション環境の非常に厳しいセキュリティ要件を満たすポリシーを作成できます。カスタムポリシーの実装手順には、デフォルトポリシーの実装で実行するすべての作業と、この後で説明する追加作業があります。

以下の**すべての条件**が該当する場合には、Cisco Security Agent Profiler を使用してカスタムポリシーを作成してください。

- アプリケーション環境のセキュリティ要件が極めて厳しい。
- ホストが特定のアプリケーション環境専用である（他のアプリケーションと共有されていない）。
- 本稼働のアプリケーションサーバに厳格な変更管理手順が存在する。すべての変更は、情報セキュリティおよび IT 管理部門との緊密な調整の下で承認、テスト、および展開が行われる。
- Cisco Security Agent の実装をサポートするために、アプリケーションの専門家とテスト リソースを大量に投入する用意がある。これらのアプリケーションの専門家とテスト リソースが、分析およびポリシー調整プロセスに不可欠となっている。
- ポリシーのカスタマイズのために相当な予算を投入する用意がある（カスタムポリシーの作成には、相当なコンサルティング リソースが必要であり、通常、最短でも3カ月かかります）。

Cisco Security Agent Profiler を使用する場合、最初のステップとして、アプリケーション環境のすべての主要なコンポーネント（たとえば、Web サーバ、Web アプリケーションサーバ、アプリケーションソースコード、データベース、スケジューリングシステム、OS）について、アプリケーション問題の専門家と QA リソースを割り当てる作業が必要です。ポリシーの分析、作成、および調整作業の間、アプリケーションの専門家を常に確保しておくことは極めて重要です。これらの専門家は、Cisco Security Agent の実装作業に不可欠です。カスタムポリシーの分析には、アプリケーション環境に関する深い知識が必要なので、Cisco Security Agent の実装チームが専門家に相談できるようにしておく必要があります。

## Cisco Security Agent Profiler を使用してカスタム ポリシーを実装するための追加作業

分析するアプリケーションは、CSA MC によって指定します。また CSA MC では、分析を実行するエージェント ホストを選択します。カスタム ポリシーの実装を Cisco Security Agent Profiler で作成する手順は、以下のとおりです。

- 分析を実行するエージェント ホスト、および分析を完了するまでの時間枠を選定する。
- 該当するすべてのアプリケーションの分析をサポートするアプリケーション クラスを作成する。
- 評価する各アプリケーションの分析ジョブを作成する。
- モニタ対象の OS とアプリケーション クラスを選択する。
- ロギング エージェントとして使用するホストを選択する（そのアプリケーションが実行されている場所）。

アプリケーションの分析は一度に 1 つずつ実行します。本稼働システムで実行するよりも、類似した構成を持つ QA システムを選択することを推奨します。時間枠は、アプリケーションの機能をすべて実行するのに十分な長さ（たとえば、アプリケーションのテスト サイクル全体を実行できる時間）を割り当てます。

分析が完了したら、そのジョブからカスタマイズされたポリシーを自動生成することもできます。生成されたポリシーは、CSA MC にインポートできます。インポートすると、元の分析ジョブ名に [Job] という文字を付加した名前で、プロファイラ ポリシーがポリシー リストに追加されます。次にアプリケーション問題の専門家は、生成されたポリシーを分析して、そのルールを微調整します。作成されたルールが、（アプリケーションの以前の実行だけでなく）その後のさまざまな状況でのすべての実行に対応できるほど「十分に汎用的」であることを保証するには、アプリケーション環境に関する幅広い知識が要求されます。プロファイラによるアプリケーションの分析が完了したら、次にルールを作成して、選択したホストに配布します。パラメータの設定によっては、それらのホストが CSA MC をポーリングして新しいルールを受信した後で分析ジョブが開始されます。

前に説明したデフォルト ポリシーの実装方式で、適用可能なデフォルト ポリシーが調整可能だったように、Cisco Security Agent Profiler によって生成されたポリシーもさらに調整して該当する Cisco Security Agent グループに適用できます。

### まとめ

Cisco Security Agent ソフトウェアスイートは、さまざまなホストを攻撃から保護できる強力なツールです。しかし、ネットワークベースのアプリケーションに対する Cisco Security Agent ソフトウェアの影響を最小限に抑えるため、ソフトウェアの展開設計とネットワークにおけるテストおよび配布は、慎重に検討して実行する必要があります。ネットワークでの Cisco Security Agent の実装における最初のステップは、展開で使用するモデルを定義することです。テスト環境で、または典型的な本稼働システムを使用するパイロット システムを利用して Cisco Security Agent ソフトウェアを十分にテストすれば、展開による潜在的影響を最小限に抑えることができ、ネットワーク スタッフの専門性も促進されます。

©2004 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。  
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。  
この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

問合せ URL: <http://www.cisco.com/jp/go/contactcenter/>

〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL: 03-6670-2992

電話でのお問合せは、以下の時間帯で受付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問合せ先