

KASPERSKY LABS JAPAN

Kaspersky® Administration Kit ver. 6.0

管理者用マニュアル

KASPERSKY

© Kaspersky Labs Japan

<http://www.kaspersky.co.jp>

2008 年 1 月

目次

1 KASPERSKY ADMINISTRATION KIT	4
1.1. Kaspersky Administration Kit について.....	4
1.2. システム要件	5
1.3. 本書の目的.....	6
1.4. 記号の意味.....	7
2 KASPERSKY ADMINISTRATION KIT 概要	8
2.1. 論理ネットワーク.....	8
2.1.1. 論理ネットワークと管理サーバ.....	8
2.1.2. 管理サーバの階層.....	8
2.1.3. クライアント PC とグループ.....	9
2.1.4. 管理コンピュータ.....	10
2.1.5. プラグイン.....	11
2.1.6. ポリシー、設定、タスク.....	11
2.1.7. ポリシーとローカルアプリケーション設定との関連性.....	13
2.2. クライアントを管理サーバに接続するには.....	14
2.3. 管理サーバへの安全な接続.....	15
2.3.1. 管理サーバ証明書.....	15
2.3.2. 管理サーバの認証（管理コンソールのサーバへの接続時）.....	15
2.3.3. 管理サーバの認証（クライアントとの接続確立時）.....	16
2.4. 論理ネットワーク上のコンピュータの識別.....	16
2.5. 論理ネットワークアクセス権.....	16
2.6. アンチウイルスを論理ネットワーク上のコンピュータに導入するには.....	18
2.7. 一元管理保護システムの構築.....	18
2.8. 論理ネットワークの管理.....	19
2.9. 管理者間の共同作業の調整.....	20
2.10. ユーザインターフェイス.....	20
2.10.1. アプリケーションの起動.....	20
2.10.2. メインウィンドウ.....	21
2.10.3. コンソールツリー.....	22
2.10.4. ショートカットメニュー.....	23

3 アプリケーションの使用方法.....	27
3.1. 管理サーバへの接続.....	27
3.2. 権限の付与.....	28
3.3. ネットワーク情報、ドメイン、IP サブネット、Active Directory グループの参照.....	29
3.4. クイックスタートウィザード.....	31
3.5. 論理ネットワークの表示、作成、構成.....	32
3.5.1. グループ.....	35
3.5.2. クライアント PC.....	36
3.5.3. スレーブ管理サーバ.....	38
4 ポリシーのリモート管理.....	40
4.1. アプリケーションの設定.....	40
4.1.1. ポリシーの管理.....	40
4.1.2. ローカルアプリケーション設定.....	44
4.2. アプリケーションの管理.....	45
5 定義データベースとモジュールの更新.....	50
5.1. 管理サーバによる更新の受信.....	50
5.2. クライアント PC の更新処理.....	53
5.3. スレーブサーバとクライアントの更新.....	54
5.4. 更新エージェントを使用した更新処理.....	55
6 メンテナンス.....	56
6.1. ライセンスの更新.....	56
6.2. 隔離とバックアップストレージ.....	58
6.3. イベントログとイベントフィルタ.....	60
6.4. レポート.....	63
6.5. コンピュータの検索.....	65
6.6. コンピュータフィルタ.....	66
6.7. アウトブレイクの監視.....	68
6.8. 管理サーバデータのコピーと復元.....	71
付録A. 用語解説.....	73
付録B. KASPERSKY LAB.....	79
B.1. 製品ラインナップ.....	79
B.2. お問い合わせ先.....	84

1 KASPERSKY ADMINISTRATION KIT

1.1. Kaspersky Administration Kit について

Kaspersky® Administration Kit は、企業向けカスペルスキー製品の管理作業を一元管理する目的で開発されたリモート管理ツールです。Kaspersky Administration Kit で管理できるカスペルスキー製品は、Kaspersky Business Space Security に含まれる各アプリケーションです。管理ツールを使用すれば、企業のアンチウイルスポリシーを全面的に管理・運用することができます。Kaspersky Administration Kit は TCP/IP プロトコルを使用するすべてのネットワーク構成をサポートしています。

Kaspersky Administration Kit は、企業のネットワーク管理者およびウイルス対策担当者に最適なツールです。

このアプリケーションを利用して、管理者は次のことができます：

- **カスペルスキー製品の導入**：ネットワークを介してリモートコンピュータへ導入します。管理者のPCでカスペルスキー製品のインストールパッケージを作成し、複数のコンポーネントをネットワークに接続されている任意のコンピュータに一度にインストールすることができます。
- **効率的なライセンスキー管理**：Kaspersky Administration Kit では、すべてのカスペルスキー製品のライセンスキーを一ヶ所にインストールし、ライセンスの数とネットワーク上にインストールされているカスペルスキー製品との対応を監視し、ライセンスの有効期限を管理できます
- **カスペルスキー製品のリモート管理**：コンピュータにインストールされている複数のカスペルスキー製品を一ヶ所からリモート管理できます。Kaspersky Administration Kit では、1 台の管理ワークステーションから管理する複数階層のアンチウイルス保護システムを構築できます。これは複数の拠点を持つ企業にとっては特に重要です。この機能を利用して、管理者は次のことができます：
 - コンピュータの「管理グループ」を作成する
 - 「グループポリシー」を適用してアプリケーション設定を同時に実施する
 - 「アプリケーション設定」を使用することで個別コンピュータの要件に適したインストールを行う
 - 「グループおよびグループタスク」を割り当てることで複数のアプリケーションを管理する
 - 異なる管理グループのコンピュータにインストールされているアプリケーションにタスクのスケジュールを設定する
- **定義データベースの自動更新**：各コンピュータをカスペルスキーのアップデートサーバに直接接続することなくすべてのアプリケーションのアンチウイルスデータベースを集

中のアップデートできます。アップデートを指定した時間に自動的に実行することにより、最新の保護状態を維持するとともにクライアント PC のアップデート状況を監視できます

- **レポートの収集:** Kaspersky Administration Kit の拡張レポート機能により、動作統計データを集め、最新のデータに基づいてレポートを作成できます。このプログラムでは、1つのカスペルスキー製品の累積ネットワークレポート（アプリケーションレポート）あるいは 1 台のコンピュータにインストールされているすべてのカスペルスキー製品のレポート（コンピュータレポート）を作成できます
- **特定イベントに関するメール通知:** 通知が必要なイベント類を指定できます。アプリケーション実行時に起きるイベントの例としては、ウイルスの検知、更新の失敗、ネットワーク上の新規コンピュータの出現などがあります

Kaspersky Administration Kit は、以下の 3 つの主要コンポーネントで構成されます：

- **管理サーバ** - 企業のローカルコンピュータにインストールされているカスペルスキー製品の中央ストレージであり、それを管理する効率的なツールでもあります
- **ネットワークエージェント** - 管理サーバと特定のネットワークノード（ワークステーションまたはサーバ）にインストールされているカスペルスキー製品を統合します。このコンポーネントは、Kaspersky Business Space Security に含まれるすべてのアプリケーションをサポートします
- **管理コンソール** - Microsoft Management Console (MMC) のプラグインとして動作する、サーバおよびエージェント管理サービスのユーザインターフェイスです

1.2. システム要件

管理サーバ

- 必要なソフトウェア
 - Microsoft Data Access Components (MDAC) バージョン 2.8 以上
 - MSDE 2000 SP 3 または MS SQL Server 2000 SP 3 以上、MySQL バージョン 5.0.22 (デフォルトのコードページは UTF-8)、MS SQL 2--5 以上、MS SQL 2005 Express 以上
 - Microsoft Windows 2000 SP 4 以上、Microsoft Windows XP Professional SP 1 以上、Microsoft Windows XP Professional x64 以上、Microsoft Windows Server 2003 以上、Microsoft Windows Server 2003x64 以上、Microsoft Windows Vista、Microsoft Windows Vista x64

※ Kaspersky Administration Kit の配布パッケージに含まれるパッケージから MSDE をインストールできます。

- 必要なハードウェア
 - Intel Pentium III プロセッサ、800 MHz 以上
 - 128 MB RAM
 - 400 MB 以上の空きディスク容量

管理コンソール

- 必要なソフトウェア
 - Microsoft Windows 2000 SP 1 以上、Microsoft Windows XP Professional SP 1 以上、Microsoft Windows XP Professional x64 以上、Microsoft Windows Server 2003 以上、Microsoft Windows Server 2003x64 以上、Microsoft Windows Vista、Microsoft Windows Vista x64
 - Microsoft Management Console バージョン 1.2 以上
- 必要なハードウェア
 - Intel Pentium III プロセッサまたは互換 CPU 以上
 - 64 MB RAM 以上
 - 10 MB 以上の空きディスク容量

ネットワークエージェント

- 必要なソフトウェア
 - Windows 2000 SP 4 以上、Microsoft Windows XP Professional x64 以上、Microsoft Windows XP Professional SP 1 以上、Windows Server 2003 以上、Microsoft Windows Server 2003 x64 以上、Microsoft Windows Vista、Microsoft Windows Vista x64
- 必要なハードウェア
 - Intel Pentium III プロセッサまたは互換 CPU 以上
 - 64 MB RAM
 - 10 MB 以上の空きディスク容量

1.3. 本書の目的

このガイドは、Kaspersky Administration Kit の目的、概要、機能および操作の仕組みについて説明します。操作のステップ実行の説明については、『Kaspersky Administration Kit 参照ガイド』を参照してください。

1.4. 記号の意味

このガイドでは、文章の目的と意味に応じて、各種の書式およびアイコンが使用されています。このガイドで使用される記号の意味は以下のとおりです：

表記規則	意味
太字	メニュー名、コマンド、ウィンドウ名、ダイアログエレメントなど
注	追加情報、注釈
注意	重要な情報
動作の実行手順： 1. ステップ 1 2. ...	ユーザが実行する一連の手順および可能な動作の説明
[key] – 修飾子名	コマンドライン修飾子
情報メッセージとコマンドラインテキスト	設定ファイルのテキスト、情報メッセージおよびコマンドライン

2 KASPERSKY ADMINISTRATION KIT 概要

2.1. 論理ネットワーク

2.1.1. 論理ネットワークと管理サーバ

論理ネットワークは、複数の「クライアント PC」で構成される、「管理グループ」の階層構造です。クライアント PC にインストールされたカスペルスキー製品は、Kaspersky Administration Kit を利用して集中管理を行います。

管理サーバは、管理サーバコンポーネントがインストールされるコンピュータで、次の条件に当てはまるコンピュータにサービスとしてインストールされます：

- 「Kaspersky Administration Server」という名前である
- オペレーティングシステム起動時に自動でスタートアップされる
- コンポーネントインストール時の選択内容に基づいて、ローカルシステムプロファイルまたはユーザのプロファイルを使用する

管理サーバの機能は以下のとおりです：

- 論理ネットワーク構造（ネットワーク構成）についての情報を保存する
- 論理ネットワーク上にあるコンピュータの構成情報のバックアップを保存する
- カスペルスキー製品の配布ファイルを保存する
- コンピュータ上にアプリケーションをリモートからインストールまたは削除する
- 定義データベースとプログラムモジュールを更新する
- 論理ネットワーク上にあるコンピュータの「ポリシー」と「タスク」を管理する
- 論理ネットワーク上にあるコンピュータで発生したイベントについての情報を保存する
- 論理ネットワーク全体におけるアプリケーションパフォーマンスのレポートを生成する
- 論理ネットワーク上にあるコンピュータにライセンスキーを配布し、ライセンスキーについての情報を保存する
- 論理ネットワーク上にあるコンピュータで実行しているタスクからアラートを送信する。クライアント PC で検知されたウイルスなどについて通知を受けることができます

2.1.2. 管理サーバの階層

管理サーバは、「**メインサーバ - スレーブサーバ**」型の階層を形成できます。各管理サーバは、1レベルの階層に複数のスレーブサーバを所有することもネスト化された階層レベルを所有することもできます。ネスト化の制限はありません。この場合、メインサーバの論理ネットワークには、すべてのスレーブサーバの論理ネットワークが含まれます。このようにして、コンピュータネットワー

クの独立した各セクションを、異なる管理サーバによって管理することができ、同様に、メインサーバから制御されます (35 ページの 3.5.1 項を参照)。

サーバの階層作成機能は、次の目的で使用できます：

- 管理サーバの負荷を軽減する
- ネットワーク内のトラフィックを削減し、リモートオフィスとのやりとりを簡素化する。メインサーバとネットワーク上のコンピュータすべて（その他領域内に置かれたコンピュータなど）との間で接続を確立する必要はありません。ネットワークの各セグメントにスレーブ管理サーバを設け、スレーブサーバの論理ネットワーク内にコンピュータを配置し、高速通信チャネルを使用してスレーブサーバとメインサーバの間の接続を確保すれば十分です
- セキュリティ管理者間で、責任区分を明確化する。集中制御のすべての機能と、企業ネットワークのアンチウイルス状況の監視が維持されます

論理ネットワークを構成する各コンピュータは、1 台の管理サーバにしか接続できません。管理者は、ネットワーク属性によるコンピュータ検索機能を使用してさまざまなサーバの論理ネットワークにあるコンピュータを検索することで、コンピュータから管理サーバへの接続を正しく制御する必要があります。

2.1.3. クライアント PC とグループ

管理サーバとクライアント PC 間では次の通信が行われます：

- アプリケーションのステータスを配信する
- 制御コマンドを送受信する
- 構成情報の同期をとる
- アプリケーション実行されたイベントの情報をサーバに送信する
- 更新エージェントを機能させる

これらのやりとりは、ネットワークエージェントによって実行されます。このコンポーネントは、Kaspersky Administration Kit の管理下にあるすべてのコンピュータにインストールされている必要があります。

ネットワークエージェントは、以下の条件を満たすサービスとしてコンピュータにインストールされます：

- 「Kaspersky Network Agent」という名前である
- オペレーティングシステム起動時に自動的に起動する
- ローカルシステムプロファイルを使用する

Cisco NAC 向けプラグインは、管理エージェントとともにホストコンピュータにインストールされます。このプラグインは、Cisco Trust Agent アプリケーションがインストールされると呼び出されます。Cisco NAC と連動するためのパラメータは、管理サーバのプロパティで設定されます。

ネットワークエージェントと監視対象のカスペルスキー製品がインストールされているコンピュータ、サーバ、またはワークステーションは、**サーバ管理クライアント**（または「クライアント PC」）と呼ばれます。

企業の組織的または地域的構造、実行される機能、インストールされているカスペルスキー製品等に基づいて、クライアント PC を「管理グループ」にまとめることができます。この処理は、複数のコンピュータを便宜上 1 つの構成要素として管理するために行うことができます。PC をグループにまとめる場合には、管理者の定めるルールやその他属性を任意に組み合わせて使用できません。たとえば、最上位レベルを、部署に対応するグループで構成できます。各部署内の次のレベルでは、実行する機能に基づいてコンピュータをグループ分けします。あるコンピュータのグループにはすべてのワークステーションを含め、別のグループにはすべてのファイルサーバを含めるなどです。

グループは、複数のクライアント PC を 1 つの構成要素として管理できるように、何らかの属性によってまとめた一連のクライアント PC です。グループ内のすべてのクライアント PC は、次のものを共有します：

- 「グループポリシー」を使用したアプリケーション動作の共通パラメータ
- アプリケーション動作の共通モード - 指定された一連のパラメータを使って作成された「グループタスク」(アプリケーション機能)。1 つの「インストールパッケージ」の作成とインストール、定義データベースとモジュールの更新、コンピュータのオンデマンドスキャンとリアルタイム保護など

1 台のクライアント PC は、1 つのグループだけに含まれます。

管理者は、アプリケーション管理タスクの簡素化に役立つのであれば、任意の数のネスト化レベルを使ってサーバとグループの階層を作成できます。スレーブ管理サーバ、グループおよびクライアント PC は、同じ階層レベルに置くことができます。

2.1.4. 管理コンピュータ

管理コンソールを実行している企業ネットワーク上のコンピュータを**管理コンピュータ**と呼びます。管理者はこれらのコンピュータから、論理ネットワークにインストールされたすべての Kaspersky Anti-Virus コンポーネントをリモート管理することができます。

管理コンソールがインストールされると、このアプリケーションを表すアイコンが **[スタート]** → **[プログラム]** → **[カスペルスキー Administration Kit]** メニューに表示されます。

管理コンピュータは、論理ネットワークオブジェクトではありません。ただし、クライアント PC として論理ネットワークに追加できます。管理コンピュータ数に制限はありません。異なる論理ネットワークの管理コンピュータは、同一の空間を占めることができます。ローカルネットワークで使用可能な管理コンピュータであれば、どの論理ネットワークでも管理できます。

論理ネットワーク上では、1 台のコンピュータがクライアント PC、管理サーバ、または管理コンピュータとして動作できます。

2.1.5. プラグイン

ネットワークエージェントコンソールプラグインは、管理コンソール経由で特定アプリケーションに対して管理インターフェイスを提供する特別なコンポーネントです。Kaspersky Administration Kit を通じて管理されるすべての Kaspersky Anti-Virus 製品に含まれています。各アプリケーションに対応したプラグインが管理コンピュータにインストールされます。プラグインが提供する内容は以下のとおりです：

- アプリケーションポリシーの作成と編集に関するダイアログボックス
- アプリケーション設定の作成と編集に関するダイアログボックス
- タスク設定の構成に関するダイアログボックス
- アプリケーションによって実行されたタスクに関する情報
- アプリケーションによって生成されるイベントに関する情報
- 管理コンソールに送信された各クライアント PC のイベントと統計に関する情報

2.1.6. ポリシー、設定、タスク

カスペルスキー製品が実行する動作を**タスク**と呼びます。タスクには、機能によっていくつかの種類があります。各タスクは特定のアプリケーション設定に対応します。

タスクには一連のアプリケーション操作パラメータが割り当てられ、実行時に適用されます。すべてのタスクに共通なアプリケーションの一連の操作パラメータは、アプリケーション設定を形成します。各タスクタイプに固有なアプリケーション操作パラメータは、タスク設定を形成します。アプリケーション設定とタスク設定が重複することはありません。

タスクの種類の詳細については、各カスペルスキー製品のマニュアルを参照してください。

アプリケーションに動作を実行させるためには、アプリケーション設定を構成し、対応するタスクを作成して設定し、実行する必要があります。

各クライアント PC に対してローカルインターフェイス経由で定義、または管理コンソール経由でリモート定義されたアプリケーション設定は、**ローカルアプリケーション設定**と呼ばれます。

論理ネットワーク内のクライアント PC のタスク設定を集中管理するには、ポリシーを定義します。

ポリシーは、グループ内のアプリケーションが共有する一連のパラメータです。**ポリシー**には、個別タスクに固有の設定を除く、すべてのアプリケーション機能の構成が含まれます。このような設定の例には、スケジュール設定があります。

ポリシーには次の設定が含まれます：

- すべてのタスクに共通の設定 - アプリケーション設定
- 各種個別タスクのすべてに共通の設定 - ほとんどのタスク設定

リアルタイム保護やオンデマンドスキャンのタスクを含むアンチウイルスアプリケーションに対するポリシー（図 1 を参照）には、両方のタスクを実行するために必要なアプリケーション構成の設定がすべて含まれますが、これらタスクの実行スケジュールまたはスキャン範囲を定義する設定は含まれません。

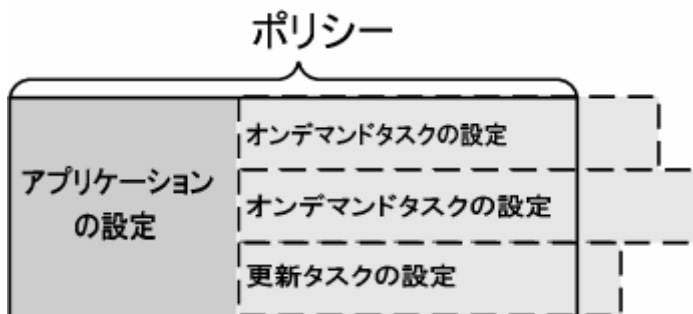


図 1. ポリシー

ポリシー内の各設定には、「ロック」属性があります。これは、この設定の変更が、階層レベル内のネスト化されたポリシー（ネスト化されたグループおよびスレブ管理サーバの場合）、タスク設定およびローカルアプリケーション設定において許可されているかどうかを示します。設定に「ロック」が割り当てられていると、下位の階層（スレブ管理サーバあるいはユーザ）では値を変更することはできません。

グループ内では、各アプリケーションに独自のポリシーが定義付けられます。異なる設定値を持ついくつかのポリシーを、1 つのアプリケーションに定義することができます。ただし、各アプリケーションに対して有効（アクティブ）にできるポリシーは 1 つだけです。

ウイルス発生時には、いっそう厳密なアンチウイルス保護設定を構築できるようにするなど、アクティブではないポリシーをイベントに基づいてアクティブにできます。

また、モバイルユーザに対応するポリシーを作成することもできます。このようなポリシーは、コンピュータが企業の論理ネットワークから切断された場合に適用されます。

グループが異なる場合は、アプリケーションの動作設定が異なる可能性があります。各グループでは、1 つのアプリケーションに対して 1 つのポリシーを個別に作成できます。

ネスト化されたグループとスレブ管理サーバは、階層の上位にあるグループからポリシーを継承します。

論理ネットワーク全体に対するタスクの作成と構成は、中央で集中的に行います。1 つの管理グループに割り当てられたタスクは「グループタスク」、個々のクライアント PC に割り当てられたタスクは「ローカルタスク」および論理ネットワーク上の異なるグループに属する複数のクライアント PC に割り当てられたタスクは「グローバルタスク」と呼ばれます。

グループタスクは、グループ内のいくつかのクライアント PC にしかカスペルスキー製品がインストールされていない場合も、グループに適用できます。この場合、グループタスクはこのアプリケーションがインストールされているコンピュータに対してのみ適用されます。

ネスト化されたグループとスレーブ管理サーバは、親グループからタスクを継承します。グループ用に定義されたタスクは、このグループに属するすべてのクライアント PC によって共有されますが、下位レベルにあるすべてのネスト化されたグループのクライアント PC によっても共有されません。

特定のクライアント PC に割り当てられたローカルタスクが実行されるのは、選択したそのコンピュータ上だけです。ローカルタスクは、このクライアントと管理サーバの同期をとるときにこのクライアント PC 用の現在のタスクの一覧に追加されます。

アプリケーション設定はすべてポリシーに支配されるため、再定義できるのはこのポリシーによって変更可能と定義されている設定と、特定のタスクに固有な設定です。ドライブのオンデマンドスキャンには、ディスク名、ファイルマスクなどを指定してください。

タスクは、スケジュールによる自動実行または手動で実行することができます。タスクの実行結果は、管理サーバまたはローカルに保存されます。管理者は、タスク結果の通知を受けるか、詳細レポートを見ることができます。

ポリシー、アプリケーション設定、グローバルタスクおよびグループタスクに関する情報はサーバに保存され、同期をとるときにクライアント PC に配布されます。管理サーバは、ポリシーに制約されないローカルな変更、クライアント PC 上で実行中のアプリケーション、それらアプリケーションのステータスおよび割り当てられたタスクについてのデータを、クライアントから受信します。

2.1.7. ポリシーとローカルアプリケーション設定との関連性

ポリシーとローカルアプリケーション設定との関連性

グループに含まれるすべてのコンピュータに対するポリシーを使用して、アプリケーションの動作設定に対して同じ値を設定できます。

ポリシーによって設定される値は、ローカルアプリケーション設定を使用して、グループ内の個々のコンピュータに対して再定義できます。ただし、値を設定できるのは、ポリシーによって変更が禁止されていない設定、つまり「ロック」されていない設定だけです。

どの値をクライアント PC で使用するのか（図 2 を参照）は、設定がポリシーによって「ロック」されているかどうかによって決まります。

- 設定に対する変更が禁止されている場合、クライアント PC はポリシーで指定されている値を使用します
- 設定に対する変更が許可されている場合、各クライアント PC は、ポリシーで指定されている値ではなくローカルの設定値を使用します。この場合、設定値はローカルアプリケーション設定を通じて変更可能です

したがって、タスクがクライアント PC 上で実行されている場合、アプリケーションは次のものによって決定された値を使用します：

- ポリシーが設定への変更を禁止していない場合は、タスク設定とローカルアプリケーション設定
- ポリシーが設定への変更を禁止していない場合は、グループポリシー

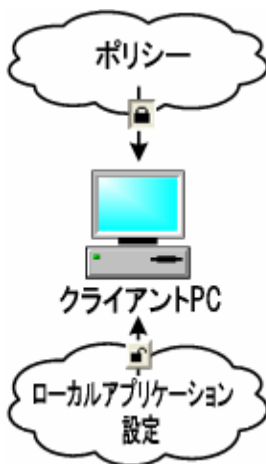


図 2. ポリシーとローカルアプリケーション設定

初期ポリシーが適用されたローカルアプリケーション設定の変更は、**[詳細]** ダイアログ（図 14を参照）のアプリケーションポリシーで定義されます。

2.2. クライアントを管理サーバに接続するには

クライアント PC と管理サーバとのやりとりを可能にするには、クライアント PC をサーバに接続する必要があります（8 ページの2項を参照）。クライアントにインストールされたネットワークエージェントが、この機能を提供します。

次の操作には、サーバとの接続が必要です：

- クライアント PC にインストールされているアプリケーションの一覧を更新する
- ポリシー、アプリケーション設定、タスクおよびタスク設定の同期をとる
- クライアント PC で実行中のアプリケーションおよびタスクの情報を更新する
- サーバで処理するイベントを配信する

ほとんどの場合、クライアント PC はサーバに接続されます。この接続を使用して、クライアントとサーバ間でデータが交換され、アプリケーションイベントの情報がサーバに送信されます。

自動同期化は、ネットワークエージェントの設定で定義されている間隔（たとえば 15 分ごと）で定期的に行われます。間隔は管理者が設定できます。

イベント情報は、イベント発生直後にサーバに送信されます。

上記の操作が終わった後は、クライアント設定で **[管理サーバから切断しない]** チェックボックスをオン/オフにして、クライアントとサーバの接続を維持/切断できます。クライアントとの接続が何らかの理由（クライアントがファイアウォール越しに置かれている、クライアント PC のポートが開けない、クライアント PC の IP アドレスが不明など）によって正常に機能しない場合は、永続的な接

続を選択することをお勧めします。または、カスペルスキー製品のパフォーマンスを継続的に監視する必要があります。

管理者は、クライアント PC でショートカットメニューの **[同期]** コマンドをクリックすることで、すぐに同期化を開始できます。この場合、接続はサーバによって開始されます。接続を有効にするため、クライアント PC の UDP ポートが開かれます。サーバはクライアントの UDP ポートに接続クエリを送信し、これを受けてクライアントに接続するサーバ権限（デジタル署名に基づいて）が検証され、署名が有効であれば接続が確立されます。

また、この UDP ポートはクライアント PC からのデータの取得、つまりクライアントで実行中のアプリケーションとタスクの一覧を更新し、アプリケーション統計をリフレッシュするときに使用されます。

2.3. 管理サーバへの安全な接続

クライアントと管理サーバ間のデータ通信およびコンソールと管理サーバ間の接続は、SSL（セキュアソケットレイヤ）プロトコルによって保護されます。SSL プロトコルは、当事者間の通信の認証、転送データの暗号化およびデータ整合性の検証を担当します。データの整合性は、送信中にデータが破損または変更されていないことを保証します。SSL 対応の接続は、ネットワーク通信セッションの両側の認証と公開キー方式を使用するデータの暗号化を伴います。

2.3.1. 管理サーバ証明書

管理サーバ証明書は、管理コンソールが管理サーバに接続要求を送信して接続が確立される場合、またはデータがクライアント PC から転送される場合の認証に使用されます。証明書はまた、マスタ管理サーバとスレーブ管理サーバの間で認証に使用されます。

管理サーバ証明書は、管理サーバのインストール時に作成されます。証明書は管理サーバのインストールディレクトリ内の **[Cert]** フォルダに保存されます。

管理サーバ証明書はサーバのインストール時に、一度だけ作成することができます。管理サーバのインストール時に、インストールウィザードを使用して証明書を保存しておくことをお勧めします。証明書を復元するには、管理サーバを再インストールし、失ったデータをバックアップから復元する必要があります。バックアップオプションについては65ページの 6.5 項を参照してください。

2.3.2. 管理サーバの認証（管理コンソールのサーバへの接続時）

管理コンソールは、管理サーバに初めて接続するときにサーバから証明書を要求し、これを管理コンピュータにローカル保存します。これ以降この名前を使用してコンソールがサーバに接続するとき、サーバはこの証明書を使用して認証されます。

サーバが認証されない場合（現在の証明書が管理コンピュータに保存されているものと異なる場合など）、コンソールはユーザにそのことを知らせ、サーバに新規の証明書を要求します。接続が承認されて別の証明書が受信された場合は、これ以降のセッションでサーバの認証に使用できるように、管理コンソールはこの新規証明書をハードディスクに保存します。

2.3.3. 管理サーバの認証（クライアントとの接続確立時）

クライアントは、管理サーバに初めて接続するときにサーバから証明書を要求し、これをローカルに保存します。

ネットワークエージェントがクライアントにローカルインストールされている場合、管理者は管理サーバ証明書を手動で選択できます。

クライアントが次回以降サーバに接続しようとする時、ネットワークエージェントは管理サーバから証明書を要求し、ローカルの証明書と比較します。証明書が異なっていると、管理サーバからクライアントへのアクセスは拒否されます。

管理サーバから UDP リクエストをクライアントに向けた場合も、同じようにネットワークエージェントが検証を行います。

2.4. 論理ネットワーク上のコンピュータの識別

論理ネットワーク上のクライアント PC は、**ホスト名**で識別されます。ホスト名はこの管理サーバ上、ユニークでなければなりません。

クライアント PC の名前は、Windows ネットワーク上で新規コンピュータが検索され時、あるいはクライアントにインストール済みのネットワークエージェントがインストール後初めてサーバに接続したときに、管理サーバに転送されます。デフォルトで、ホスト名は Windows ネットワーク上のコンピュータの名前 (NetBios 名) と一致します。この名前を持つホストがすでに存在する場合、サーバは **Name-1**、**Name-2** のように後ろに数字が付いた名前をホストに割り当てます。このホスト名は、論理ネットワーク上のコンピュータを識別するために使用されます。

2.5. 論理ネットワークアクセス権

Kaspersky Administration Kit では、アプリケーションの機能に対するアクセスに関して次のタイプの認証を提供します：

- **読み取り：**
 - 管理サーバに接続する
 - 論理ネットワーク(または管理グループ)の構造を表示する
 - アプリケーションのポリシー、タスク、設定の値を表示する
- **実行：**既存のグループタスクまたはグローバルタスクを開始および停止する、クライアント PC にインストールされているアプリケーションについてのレポートを受け取る
- **書き込み：**
 - 論理ネットワークを作成する、この論理ネットワーク(または管理グループ)にグループおよびクライアント PC を追加する
 - ネットワークエージェントコンポーネントをクライアント PC にインストールする

- カスペルスキー製品に必要なインストールパッケージを作成し、クライアント PC に(製品のライセンスキーとともに)インストールする
- クライアント PC にインストールされているアプリケーションのバージョンを更新する
- ポリシーを作成する、グループおよび個別のコンピュータに対するタスクを作成する、アプリケーション設定を構成する
- 管理サーバ、ネットワークエージェントおよび管理コンソールコンポーネントによって提供されるサービスを使用して、アプリケーションを一元管理する
- ユーザおよびユーザグループに、Kaspersky Administration Kit の機能に対するアクセス権を与える

KLAdmins および **KLOperators** に含まれるユーザには、管理サーバのインストール後、サーバへの接続と論理ネットワークでの作業に対する権限がデフォルトで与えられます。

管理サーバコンポーネントのインストール時に、管理サーバサービスの起動に選択されているアカウントとは関係なく、次の場所にグループデータが作成されます：

- 管理サーバを含むドメイン内および管理サーバコンピュータ上（このドメインに含まれるユーザのアカウントで管理サーバが起動している場合）
- 管理サーバコンピュータ上のみ（サーバがシステムアカウントで起動している場合）

グループ **KLAdmins** には、すべての権限（読み取り、実行、書き込み）が与えられます。グループ **KLOperators** には、読み取り権限が与えられます。**KLAdmins** に与えられた一連の権限は、変更できません。

グループ **KLAdmins** に含まれるユーザは、**論理ネットワーク管理者**と呼ばれます。グループ **KLOperators** に含まれるユーザは、**論理ネットワークオペレータ**と呼ばれます。

グループ **KLAdmins** および **KLOperators** の表示と変更は、標準の Windows OS 管理ツール（[管理ツール] → [ローカルユーザーとグループ]）を使って実行できます。

グループ **KLAdmins** に含まれるユーザに加え、次のユーザにも論理ネットワーク管理者の権限が与えられます：

- ドメイン管理者 - ドメイン管理者のコンピュータは、この論理ネットワーク構造に含まれます
- 管理サーバがインストールされているコンピュータ上のローカル管理者

論理ネットワーク管理者によって開始される操作はすべて、管理サーバアカウントの権限で実行されます。各管理サーバには、この特定の論理ネットワーク内に限って適用される権限を持つ独自の **KLAdmins** グループを作成することができます。

1 つのドメインに属する複数のコンピュータが複数の論理ネットワークを作成する場合、ドメイン管理者は、このように形成された各論理ネットワークに対する論理ネットワーク管理者になります。この場合、同様の論理ネットワークは、最初の管理サーバをインストールする時に作成されるのと同じグループ **KLAdmins** を共有します。オペレーティングシステムの管理ツールを使用して、こ

のグループに新規メンバを追加できます。論理ネットワーク管理者によって開始される操作は、対応する管理サーバの権限で実行されます。

Kaspersky Administration Kit でのユーザ権限は、ネットワークでの Windows ユーザ認証に基づいて決定されます。

アプリケーションのインストール後、論理ネットワーク管理者は以下の作業が可能になります（28 ページの 3.2 項を参照）:

- グループ **KLOperators** に与えられた権限を変更する
- その他のユーザグループおよび管理コンソールがインストールされているコンピュータに登録された個別のユーザに対し、Kaspersky Administration Kit の機能に対するアクセス権を与える
- 各管理グループで作業するためのさまざまなアクセス権を与える

2.6. アンチウイルスを論理ネットワーク上のコンピュータに導入するには

信頼できるアンチウイルス保護環境を Kaspersky Administration Kit を使用して導入するためには、以下の 2 つの方法があります:

- 1 台のワークステーションから論理ネットワーク全域のクライアント PC に、アプリケーションをリモートインストールできます。インストールおよびリモート管理システムへの接続は自動的に行われるため、管理者の介入は不要です。また、アンチウイルス製品を任意の数のクライアント PC にインストールすることができます
- ネットワークに接続したすべてのコンピュータに、アプリケーションをローカルインストールできます。この場合は、すべての必須コンポーネントおよび管理コンピュータを手動でインストールします。接続設定は、ネットワークエージェントのインストール時に設定されます。この導入シナリオは、リモート導入が不可能な場合に限りて使用してください

リモートインストールは、ユーザが選択したアプリケーションのインストールに使用できます。ただし、Kaspersky Administration Kit は専門のコンポーネント（アプリケーション管理プラグイン）を備えたカスペルスキー製品しかサポートしない点にご注意ください。

2.7. 一元管理保護システムの構築

Kaspersky Administration Kit を通じた企業ネットワーク全体にわたる一元管理システムを構築するには、はじめに論理ネットワークを設計します。ここでは、次のような意志決定を行う必要があります:

1. ネットワーク内で単独の領域を選択し、インストールする管理サーバの数を決定する
2. メインの管理サーバ、スレーブサーバ、管理コンピュータおよびクライアント PC として、企業ネットワーク構造内のどのコンピュータを使用するかを決定する。カスベ

ルスキー製品がインストールされるすべてのコンピュータがクライアント PC として動作するわけではないことに注意してください

3. グループ内でクライアント PC を編成するために使用する基準およびグループの階層を決定する
4. 使用する導入シナリオ（リモートインストールまたはローカルインストール）を決定する

次のステップで、管理者は論理ネットワークを構築する必要があります。次の Kaspersky Administration Kit コンポーネントを、ネットワーク接続したコンピュータにインストールします：

1. 企業ネットワーク内のコンピュータに管理サーバをインストールします
2. 管理元となるコンピュータに管理コンソールをインストールします
3. 論理ネットワーク管理者の割り当てを決定し、システムとやりとりするその他のユーザカテゴリを決定し、実行する一連の機能を各カテゴリに割り当てます
4. ユーザリストを作成し、グループに割り当てられた機能を実行するために必要なアクセス権を各グループに与えます

続いて、管理サーバの階層を作成し、各サーバに対して論理ネットワーク構造を作成する必要があります。管理グループの階層を作成し、対応するグループにコンピュータを割り振ってください。

次のステップでは、ネットワークエージェントおよび選択したカスペルスキー製品をクライアント PC にインストールし、対応するコンソールプラグインを管理コンピュータにインストールする必要があります。

一部のカスペルスキー製品は、Kaspersky Administration Kit を通じて管理アクセスが可能ですが、クライアントにリモートインストールできません。詳細については、該当するアプリケーションマニュアルを参照してください。

リモートインストールオプションを使用する場合は、任意のアプリケーションとともにネットワークエージェントをインストールします。この場合、ネットワークエージェントを別途インストールする必要はありません。

最後に、グループポリシーを割り当てて適用し（40 ページの4を参照）、タスクを作成する（44 ページの 4.1.2 項を参照）ことで、インストールされたアプリケーションを構成します。

管理者はクイックスタートウィザードを使用して、アンチウイルスシステムを簡単に導入/設定することができます（ウィザードの詳細については、28 ページの 3.2 項を参照）。アンチウイルスシステムの簡単な構成とは、Windows ネットワークのドメイン構造と同一の論理ネットワークを作成し、Kaspersky Anti-Virus 5.0 for Windows Workstation のバージョン 5.0 および 6.0 に基づいて保護システムを展開することを意味します。

2.8. 論理ネットワークの管理

論理ネットワークを構築し、アンチウイルス製品のインストールおよび設定が終了したら、次の操作を定期的に行うことをお勧めします：

- アプリケーションの実行レポートをクライアント PC に表示する
- クライアント PC および管理サーバから管理者に送付されるアラートを参照する

カスペルスキー製品が送信する通知の完全なリストは、これらのアプリケーションに添付されているドキュメントに記載されています。

- 1 台のクライアント PC で発生した事態に管理者が関与することになった場合、管理者は自分のワークステーションから作業（該当クライアント PC での感染ファイルの感染駆除など）をリモートで実行することができます
- クライアント PC 上の定義データベース（50 ページの5 項を参照）、クライアント PC にインストールされているソフトウェアモジュールを随時更新する（50 ページの5 項を参照）
- クライアントからの送信を保存するために使用可能なサーバ領域と、送信されたデータを処理するための空き領域をサーバ上に確保する。
- ローカルネットワークに登録された新規コンピュータを論理ネットワークに追加し、必要なアプリケーションを随時インストールする。
- 管理システムデータを定期的にバックアップする（65 ページの 6.5 項を参照）

2.9. 管理者間の共同作業の調整

本システムでは、複数の管理者が同時に同じリソースを扱えるようになっています。最新の変更が、それまでに保存された設定を上書きします。したがって、食い違いを防ぐために、複数の管理者の共同作業を調整する必要があります。

2.10. ユーザーインターフェイス

管理コンピュータでは、論理ネットワークの表示、作成、変更および構成できるほか、クライアントにインストールされているすべてのカスペルスキー製品を管理できます。管理インターフェイスは、Microsoft Management Console (MMC) に組み込まれている管理プラグインである管理コンソールコンポーネントによって提供されます。Kaspersky Administration Kit インターフェイスは、MMC 標準に従っています。

クライアント PC とのローカルなやりとりを保証するため、アプリケーションには、リモートデスクトップ Microsoft Windows ユーティリティへの標準コネクトを使用して管理コンソール経由でコンピュータとリモート接続を確立する機能が備わっています。

この機能を使用するには、クライアント PC 上のデスクトップとのリモート接続を許可する必要があります。

2.10.1. アプリケーションの起動

Kaspersky Administration Kit は、標準の [スタート] → [プログラム] メニューの [カスペルスキー-Administration Kit] から[カスペルスキー-Administration Kit] を選択することで起動で

きます。このプログラムグループは、管理コンソールのインストール時に、管理コンピュータ上のみに作成されます。

Kaspersky Administration Kit の機能にアクセスするには、論理ネットワーク管理サーバを起動する必要があります。

2.10.2. メインウィンドウ

プログラムのメインウィンドウ（図 3 を参照）には、メニュー、ツールバー、コントロールパネル、表示パネル、詳細パネルおよびタスクパネルがあります。メニューはファイルやダイアログボックスの管理に使用され、ヘルプピックへのアクセスを提供します。ツールバーを使うことにより、頻繁に使用されるメニューオプションに素早くアクセスできます。表示パネルには、階層型の **Kaspersky Administration Kit** のネームスペースがコンソールツリーとして表示されます。詳細パネルには、コンソールツリー内で選択されたオブジェクトの詳細が表示されます。詳細パネルにはタスクパネルが含まれます。タスクパネルには、ツリー内で選択されたコンソールに割り当てられている主な操作へのショートカット、またはオブジェクトの詳細パネルへのハイパーリンクがあります。詳細パネルは、2 つの形式で表示できます。コンソールツリー内で選択されたエレメントの名前がついたタブの形式と、**[標準]** タブの形式です。この 2 形式の違いは、**[標準]** タブにタスクパネルが含まれない点だけです。

Microsoft Windows 2000 での管理コンソールには、タスクパネルが表示されず、利用できません。

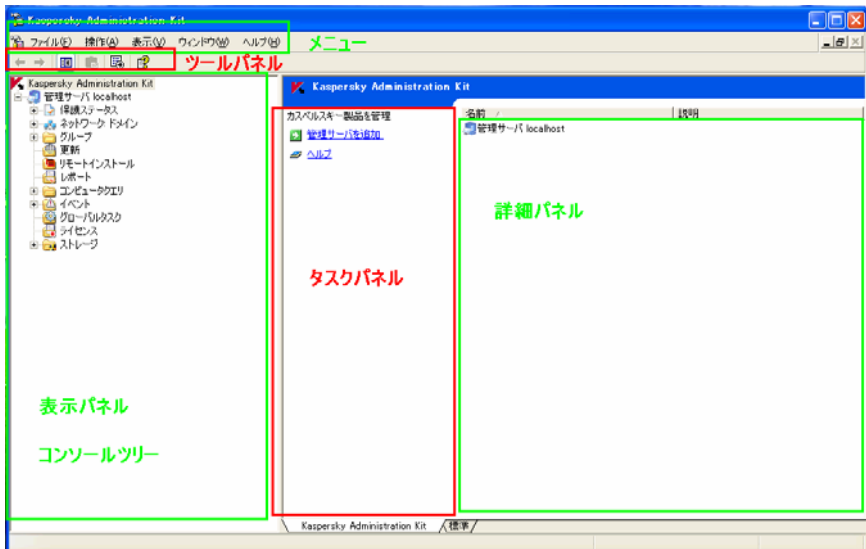


図 3. Kaspersky Administration Kit のメインウィンドウ

2.10.3. コンソールツリー

コンソールツリー（図 3 を参照）には、企業ネットワーク内に作成された論理ネットワークが表示されます。ここから、論理ネットワーク設定にアクセスできます。

Kaspersky Administration Kit ネームスペースは、（管理サーバ数までの）[管理サーバ（<サーバ名>）] など、いくつかのノードを持つことができます。

[管理サーバ（<サーバ名>）] ノードは、選択された管理サーバの構造と設定を表示するコンテンツです。[管理サーバ（<サーバ名>）] ノードには次のフォルダがあります。

- 保護ステータス
- ネットワーク
- グループ
- 更新
- リモートインストール
- レポート
- コンピュータクエリ
- イベント
- グローバルタスク
- ライセンス
- ストレージ

[保護ステータス] フォルダは、クライアント PC とコンピュータネットワーク全体の両方でのアンチウイルス保護状態に関する情報を提供するために使用されます。このフォルダには、次のような情報構造を保証するネスト化されたレポートページがあります。

- **ネットワーク** - 論理ネットワーク構造に含まれないコンピュータについての情報および管理サーバによって最後に行われたコンピュータネットワークのポーリングの結果
- **グループ** - 論理ネットワーク上のクライアント PC のアンチウイルス保護ステータス。
- **ウイルス統計** - 論理ネットワークのクライアント PC 上でのウイルスアクティビティに関する統計情報
- **更新状況** - アプリケーションが使用する定義データベースのステータス

[ネットワーク] フォルダには、管理サーバがインストールされているコンピュータネットワークの内容が表示されます。管理サーバは、Windows ネットワークと企業コンピュータネットワーク内で作成された IP サブネットワークを定期的にポーリングすることで、ネットワーク構造およびこのネットワークに含まれるコンピュータについての情報を作成して更新します。[ネットワーク] フォルダの内容は、このポーリングに基づいて更新されます。

[グループ] ノードは、論理ネットワーク構造、グループポリシーおよびグループタスクの保存、表示、構成および変更に使われます。

[グループ] フォルダ内のルートオブジェクトは、論理ネットワーク階層の最上位レベルに対応します。[管理サーバ]、[ポリシー] および [グループタスク] フォルダはグループ項目ごとに必須で

す。これらのフォルダは、管理サーバ、ポリシーおよび上位階層レベルのタスクを扱うときに使用されます。

[更新] フォルダには、管理サーバに受信済みでクライアントに配布できる更新の一覧が含まれています。

[リモートインストール] フォルダには、論理ネットワークのクライアント PC にアプリケーションを導入するために使用できるインストールパッケージの一覧が含まれています。

[レポート] フォルダには、論理ネットワーク保護の状態に関するレポートのテンプレートが表示されます。

[コンピュータクエリ] フォルダは、指定された検索基準を使ったクライアント PC の検索、検索結果の保存、コンソールツリーの個別フォルダへの表示に使用されます。

[イベント] フォルダには、アプリケーションの実行中に登録されたイベントの一覧、イベントについての情報およびタスク実行の結果が表示されます。

[グローバルタスク] フォルダには、一連の論理ネットワークコンピュータに割り当てられたグローバルタスクの一覧が表示されます。

[ライセンス] フォルダには、クライアント PC にインストールされたライセンスが表示されます。

[ストレージ] フォルダは、アンチウイルス製品によってクライアント PC の隔離フォルダに置かれたオブジェクトの管理およびバックアップストレージに置かれたバックアップの管理に使用されます。ただし、オブジェクト自体は管理サーバにコピーされません。

管理コンソールに表示される情報は、ノードに関する限り、自動的に更新されます。

結果パネル内の情報を更新するには、**[F5]** キーを使用するか、メニューやショートカットメニューの **[更新]** コマンド、またはタスクウィンドウ枠の **[更新]** リンクを使用します。

2.10.4. ショートカットメニュー

コンソールツリーの管理サーバネームスペース内の各オブジェクトタイプには、固有のショートカットメニューがあります。標準の MMC コマンドのほか、これらのメニューにはオブジェクトの扱いに関する具体的なオプションが含まれています。特定のオブジェクトの追加コマンドは、次の表のとおりです：

表 1

オブジェクト	コマンド	処理
Kaspersky Administration Kit	新規作成/Kaspersky Administration Server	管理サーバをコンソールツリーに追加する
<サーバ名>	管理サーバに接続	管理サーバに接続する
	管理サーバから切断	管理サーバとの接続を切断する
	クイックスタートウィザード	クイックスタートウィザードを起動する

オブジェクト	コマンド	処理
	コンピュータを検索	[コンピュータエリ] ウィンドウを開く
	プロパティ	[管理サーバのプロパティ] ダイアログボックスを表示する
	すべてのタスク/ウイルス攻撃検知設定	論理ネットワークコンピュータ上でのウイルス攻撃の検知設定を構成する
ネットワーク	コンピュータを検索	[ネットワーク] フォルダ内でコンピュータ検索ウィンドウを開く
	アプリケーション導入ウィザード	導入タスクを作成して実行する
	表示/ドメイン	コンピュータネットワーク構造を Windows ドメイン/ワークグループの階層として表示する
	表示/Active Directory	アクティブディレクトリ構造に従ってコンピュータのネットワーク構造を表示する
	新規作成/IP サブネットワーク	IP サブネットワークを作成してコンピュータを表示する
	表示/管理サーバ	[ネットワーク] フォルダに含まれる管理サーバノードに切り替える
	新規作成/IP サブネットワーク	IP サブネットワークを作成してコンピュータを表示する
	すべてのタスク/コンピュータアクティビティ	ネットワーク内でコンピュータアクティビティが見られない場合に対応する管理サーバ設定を構成する
グループ	アプリケーションのインストール	グループ用に導入タスクを作成して実行する
	アプリケーションの更新	リモート更新ウィザードを起動する
	新規レポートテンプレート	選択されたグループ用に新規レポートテンプレートを作成する
	コンピュータを検索	グループ内で [PC を検索する] ウィンドウを開く
	ウイルスカウンタをリセット	このグループ内のすべてのクライアントのウイルス保護カウンタをリセットする
	強制同期	グループ内のすべてのコンピュータのデータを同期化する

オブジェクト	コマンド	処理
	新規作成/グループ	新規グループを論理ネットワーク構造に追加する
	新規作成/コンピュータ	新規クライアント PC をグループに追加する
	すべてのタスク/コンピュータアクティビティ	ネットワーク内でコンピュータアクティビティが見られない場合に対応する管理サーバ設定を構成する
	すべてのタスク/重要度	グループに対するアクセス権を構成する
	すべてのタスク/ポリシー	選択したグループの [ポリシー] フォルダに切り替える
	すべてのタスク/タスク	選択したグループの [グループタスク] フォルダに切り替える
	すべてのタスク/スレーブサーバ	選択したグループの [管理サーバ] フォルダに切り替える
ポリシー	新規作成/ポリシー	新規グループを作成する
	タイプ/継承ポリシー	継承されたポリシーを詳細パネルに表示する
グループタスク	新規作成/タスク	新規グループタスクを作成する
	すべてのタスク/インポート	ファイルからタスクをインポートする
	タイプ/継承タスク	継承されたグループタスクを詳細パネルに表示する
リモートインストール	導入タスク作成ウィザード	アプリケーション導入タスクを作成する
	アプリケーションバージョンレポート	コンピュータにインストールされているカスペルスキー製品のバージョンについてのレポートを作成して表示する
	新規作成/インストールパッケージ	新規インストールパッケージを作成する
	すべてのタスク/アプリケーション導入ウィザード	アプリケーション導入タスクを作成する
レポート	新規作成/レポートテンプレート	新規レポートテンプレートを作成する

オブジェクト	コマンド	処理
コンピュータクエリ	新規作成/新規クエリ	新規フィルタを作成してコンピュータを検索する
イベント	新規作成/新規クエリ	イベントプレビュー表にフィルタを適用する
	すべてのタスク/インポート	ファイルからタスクをインポートする
グローバルタスク	新規作成/タスク	新規グローバルタスクを追加する
ライセンス	ライセンスキーの追加	新規ライセンスキーをインストールする
	ライセンスレポート	クライアント PC にインストールされているライセンスキーについてのレポートを作成して表示する

詳細パネルでは、コンソールツリーで選択されている各項目には、それぞれの扱い方のオプションを備えた固有のショートカットメニューがあります。主なエレメントおよび対応するショートカットメニューコマンドは、次の表のとおりです。

表 2

エレメント	コマンド	処理
クライアント PC	プロテクション	クライアント PC のアンチウイルス保護ステータスについての情報を表示する
	タスク	[タスク] タブのローカルコンピュータプロパティ構成ウィンドウを開く
	アプリケーション	[アプリケーション] タブのローカルコンピュータプロパティ構成ウィンドウを開く
	イベント	クライアント PC 上でアプリケーションの実行中に登録されたイベントを表示するウィンドウを開く
	導入ウィザード	クライアント PC 用に導入タスクを作成する
	同期	クライアント PC と管理サーバのデータを同期化する
	ウイルスカウンタをリセット	特定のクライアントのウィンドウ検知カウンタをリセットする
	リモートデスクトップ接続	リモートデスクトップに接続するためのウィンドウを開く
インストールパッケージ	インストール	アプリケーション導入タスクを作成する
レポートテンプレート	レポートの作成	選択されたレポートのテンプレートを作成してプレビューする
	レポートの送信	選択されたテンプレートに基づいて、レポートの自動生成と送信のタスクを作成する

3 アプリケーションの使用方法

3.1. 管理サーバへの接続

スタートアップの後、プログラムのメインウィンドウには、最上位レベルに **Kaspersky Administration Kit** ネームスペースを持つコンソールツリーが表示されます。論理ネットワーク構造と設定を表示させるには、サーバオブジェクトをコンソールツリーに追加し、必須の管理サーバに接続する必要があります（図 4 を参照）。管理サーバから論理ネットワーク構造についての情報が受信され、コンソールツリーに表示されます。

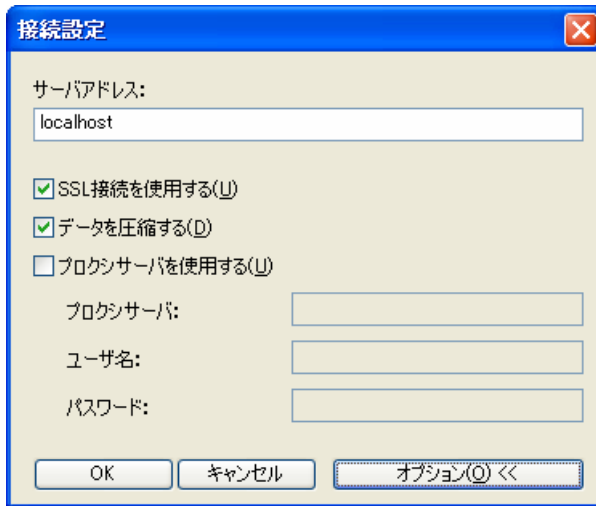


図 4. 管理サーバとの接続の確立

ユーザに接続権限がない場合、接続は拒否されます。ユーザ権限は Windows のユーザ認証手順によって検証されます。

Windows ネットワーク上に複数の管理サーバがある場合は、これらの論理ネットワークを管理コンピュータから管理できます。別の論理ネットワークを選択するには、必須の管理サーバに接続するか、いくつかのサーバをネットワークツリーに追加してこれらのサーバの 1 つに接続します。

複数の管理サーバおよび論理ネットワークを同時に管理できるのは、各論理ネットワークのオペレータまたは管理者である場合、あるいは各ネットワークに対して必要な権限を持っている場合に限られます。

3.2. 権限の付与

管理サーバのインストール後、サーバに接続する権限と論理ネットワークを扱う権限が、論理ネットワークの KLAdmins グループと KLOperators グループ内のユーザに付与されます（16 ページの 2.5 項を参照）。

KLOperators グループのアクセス権を変更し、管理コンソールがインストールされているコンピュータに登録されている別のユーザグループおよび個別ユーザに対して論理ネットワークを扱う権限を付与できます。

論理ネットワークのすべてのオブジェクトに対するアクセス権の付与は、管理サーバ設定の構成ウィンドウにある **[セキュリティ]** タブを使って行います（図 5を参照）。

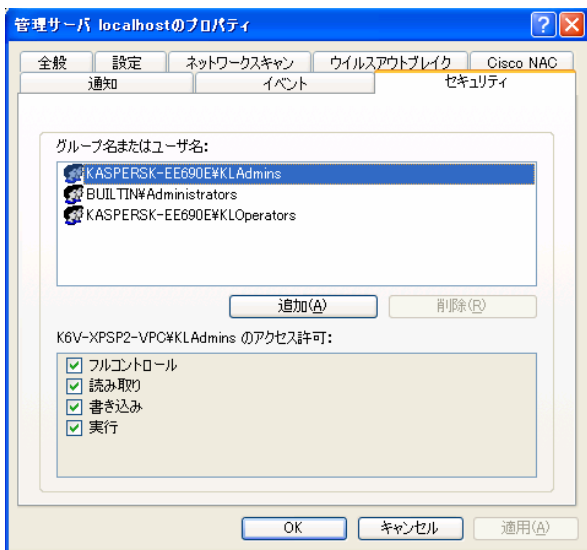


図 5. 管理サーバへのアクセス権の付与

論理ネットワーク内の各グループに個別のアクセス権を付与する機能もあります。この設定は、グループ設定ウィンドウの **[セキュリティ]** タブで行います。

管理者は、イベントログに登録された管理サーバ操作中のイベントによってユーザの動作を追跡できます。このようなイベントには「情報」というレベルが割り当てられ、冒頭に「監査」という言葉が付きます。これらは、コンソールツリーの **[イベント]** ノードにある **[監査イベント]** フォルダに表示されます。

3.3. ネットワーク情報、ドメイン、IP サブネット、Active Directory グループの参照

コンピュータネットワーク構造の情報および該当ネットワーク内のコンピュータ情報は、コンソールツリーの [ネットワーク] フォルダに表示されます。

Kaspersky Administration Kit のインストール後、[ネットワーク] フォルダには、ドメイン構造を反映したフォルダ階層および Windows ネットワークのワークグループが表示されます。エンドレベルの各フォルダには、各ドメインのコンピューターまたは論理ネットワーク構造に含まれないワークグループが含まれます。コンピュータが任意のグループに含まれると、そのコンピュータについての情報は、このフォルダからすぐに削除されます。コンピュータが論理ネットワーク構造から除外されると、そのコンピュータについての情報は、[ネットワーク] ノードの対応するフォルダに再び追加されます。



[ネットワーク] ノードフォルダの階層には、アクティブディレクトリ構造またはネットワーク内で作成された IP サブネットワークも反映されます。反映させるには、[ネットワーク] ノードのショートカットメニューで [表示] → [Active Directory] または [表示] → [IP サブネットワーク] を選択します。

[ネットワーク] ノードが IP サブネットワークを表している場合、その構造は、管理者が IP サブネットワークの作成および既存サブネットワークの設定変更から作成したことを示します。

デフォルトでは、管理サーバを伴う IP サブネットだけが IP サブネットとして表示されます

コンソールツリー内のフォルダを選択すると、そのフォルダに含まれるコンピュータは、次の情報を含むテーブルとして、結果ウィンドウに表示されます：

- **名前** - 論理ネットワーク内のコンピュータ名 (NetBios 名またはコンピュータの IP アドレス)
- **OS タイプ** - クライアント PC にインストールされている OS の種類

オペレーティングシステムのタイプに基づいて、コンピュータ名の横にアイコンが表示されます： - サーバの場合 /  - ワークステーションの場合

- **ドメイン** - 特定のコンピュータが含まれる Windows ドメインまたはワークグループ
- **Agent/Antivirus** - コンピュータにインストールされているアプリケーションのステータス。Kaspersky Administration Kit を使って管理できるネットワークエージェントまたはアンチウイルス製品¹の場合、このコンピュータにインストールされていれば「+」(プラス) 記号が表示されます。これらのアプリケーションがインストールされていない場合は、「-」(マイナス) 記号が表示されます。
- **最終表示** - ネットワーク上でサーバによってコンピュータが最後に検知された日付
- **最終更新** - コンピュータ上の定義データベースまたはアプリケーションが最後に更新された日付
- **ステータス** - 管理者が設定した基準に基づいたコンピュータの現在のステータス (OK/確認/緊急)

¹ 上記の場合、アンチウイルス製品とは、自動保護コンポーネントを含むアプリケーションを指します。

- **情報更新** - このコンピュータについての情報が最後に更新された日付
- **DNS ドメイン** - コンピュータが関連付けられている DNS ドメイン
- **ドメイン名** - コンピュータのドメイン名
- **IP アドレス** - コンピュータの IP アドレス
- **サーバへの接続** - 管理サーバを伴うコンピュータにインストールされたネットワークエージェントが最後に接続した時刻

[ネットワーク] フォルダは、同じ名前を持つサービスグループを反映します。最新状態での [ネットワーク] グループの作成とサポートは、管理サーバによって行われます。管理サーバは企業ネットワークを定期的にポーリングし、新規コンピュータまたは接続していない既存コンピュータを検知します。

管理サーバは、次のタイプのネットワークポーリングを実行できます（図 6 を参照）：

- **Windows ネットワークの簡易ポーリング** - このタイプのポーリングは、すべてのネットワークドメインおよびワークグループ内にあるノードの NetBios 名一覧を作成するために限って使用されます
- **Windows ネットワークの完全なポーリング** - オペレーティングシステムの種類、IP アドレス、DNS 名など、ノードに関する追加情報が必要な場合
- **IP サブネットのポーリング** - このモードでは、管理サーバは ICMP パケットを使用して指定範囲の IP アドレスをポーリングし、範囲内のすべてのノードに関する完全なデータを収集します
- **Active Directory グループのポーリング** - このモードでは、管理サーバは Active Directory ユニット構造に関する情報のほか、ノードの DNS 名もデータベースに記録します

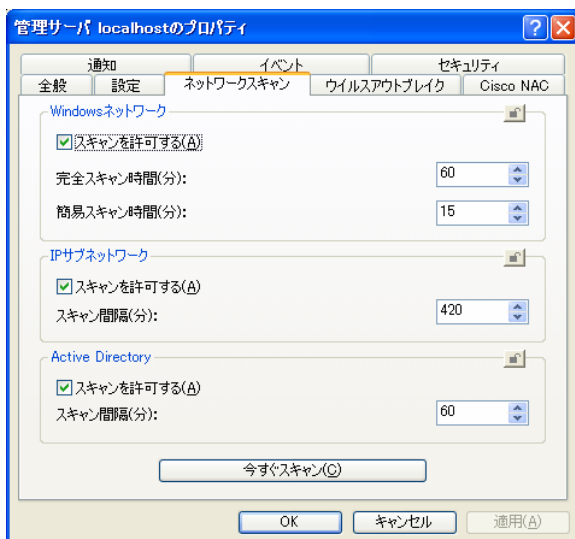


図 6. 管理サーバによるネットワークポーリング

入手した情報と論理ネットワーク構造データに基づいて、管理サーバは**ネットワークグループ**と**[ネットワーク]**フォルダの構造および内容を更新します。更新中にネットワーク内で検知されたコンピュータは、管理者によって指定された**[ネットワーク]**フォルダの構造または論理ネットワーク構造内の指定の管理グループに自動的に追加されます。**[ネットワーク]**フォルダおよび任意のネスト化されたサブグループに含まれるコンピュータのポーリングを無効化する機能もあります。

マスタ管理サーバの**[ネットワーク]**フォルダには、スレーブ管理サーバの論理ネットワークに割り当てられたホストも表示されます。その逆も同様です。

3.4. クイックスタートウィザード

Kaspersky Administration Kit のウィザードを使用することで、アンチウイルス保護の一元管理システムを構築する最小パラメータセットを構成できます。クイックスタートウィザードを使用して設定できる項目は以下のとおりです：

- 論理ネットワーク - ネットワーク構造は、管理者の裁量で次のように作成できます：
 - Windows ネットワークのドメインおよびワークグループの構造に基づいて自動的に作成する
 - 手動で作成する

論理ネットワークの作成時に**ネットワークグループ**に登録されていない（電源が入っていない、またはネットワークに接続していない）コンピュータは、論理ネットワークに追

加されません。これらのコンピュータは後から手動で追加することができます。

クイックスタートウィザードを使用して論理ネットワークを作成しても、ネットワークの整合性には影響しません。新しいグループが追加されるだけで、すでにあるグループを置き換えるわけではありません。**未割当グループ**は論理ネットワークに含まれないコンピュータだけを表示するので、すでにあるグループに割り当てられたコンピュータは、ここでは追加されません。

- 管理サーバおよびその他のカスペルスキー製品によって記録された保護関連イベントをメールまたは NET SEND 経由でアラート送信するための設定
- Kaspersky Ant-Virus for Windows Workstation 5.x および 6.x 向け、最上位階層レベルのポリシーと最小タスクセットおよび管理サーバとバックアップデータコピー用のグローバル更新タスク

Kaspersky Anti-Virus 5.0 for Windows Workstation 5.x および 6.x のポリシーは、これらアプリケーションに対するポリシーがすでに **[グループ]** フォルダに存在している場合は作成されません。

グループグループに対するグループタスクと、これらの名前を持つグローバル更新タスクおよびバックアップコピーのタスクがすでに作成されている場合、この時点ではこれらのタスクは作成されません。

インストール後に管理サーバに初めて接続するとき、クイックスタートウィザード実行に関するメッセージが表示されます。ウィザードを後で実行するには、管理サーバのショートカットメニューで **[クイックスタートウィザード]** を使用します。

3.5. 論理ネットワークの表示、作成、構成

論理ネットワークの構造、つまりスレーブ管理サーバの階層およびグループの一覧と構造は、設計段階で決定されます。グループ階層を作成してクライアント PC とスレーブ管理サーバを追加することで、論理ネットワークが Kaspersky Administration Kit のメインウィンドウの特別な **[グループ]** フォルダ内に作成されます（図 7 を参照）。

Kaspersky Administration Kit がインストールされるとすぐに、**[グループ]** フォルダにはその他オブジェクトが含まれなくなり、**[管理サーバ]**、**[ポリシー]** および **[グループタスク]** フォルダは空白になります。管理者による論理ネットワーク構造の作成時に、クライアント PC およびネスト化されたグループを **[グループ]** フォルダの構造に追加できます。

グループはフォルダとして表示されます。各フォルダは、**[グループ]** フォルダと類似した構造を持っています。

- 各グループの作成中、ネスト化されたフォルダである **[管理サーバ]**、**[ポリシー]** および **[グループタスク]** が自動的に作成され、特定グループのスレーブ管理サーバ、ポリシーおよびタスクがそこに保存されて管理されます
- クライアント PC がグループに追加されると、その情報は結果パネルに表として表示されます
- ネスト化されたグループが追加された場合、同一の構造を持つフォルダが作成されません

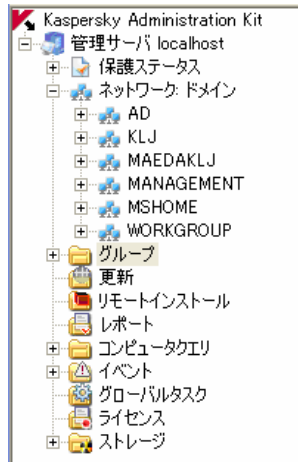


図 7. 論理ネットワークオブジェクトの表示

コンソールツリーでフォルダが選択されていると、フォルダの内容が結果ウィンドウに反映されません。

[ネットワーク] フォルダの表に表示される情報のほか、各クライアント PC に関する以下の情報を見ることができます：

- **最終完全スキャン日時** - クライアント PC で最後に実行されたウイルススキャンの日時
- **検知数** - アンチウイルスのインストール後の初回スキャンまたは値（検知されたウイルスのカウント）のリセット後にクライアント PC で検知されたウイルスの合計数。値をリセットするには、ショートカットメニューまたは **[操作]** メニューの **[ウイルスカウンタをリセットする]** を使用します
- **リアルタイム保護のステータス** - 該当クライアント PC の現在のリアルタイム保護ステータス
- **IP アドレス** - クライアント PC と管理サーバ間を接続している IP アドレス

[グループ] フォルダ内のオブジェクトは、ショートカットメニューのコマンド（23 ページの 2.10.4 項を参照）およびタスクパネルのリンクを使用して管理します。

Windows ネットワークのドメインおよびワークグループと同一構造を持つ論理ネットワークを作成する場合は、クイックスタートウィザードを使用できます（28 ページの 3.2 項を参照してください）。

設計済みの論理ネットワーク構造を手動で作成するには：

1. 必要な管理サーバに接続します
2. ネスト化されたグループを作成して、グループ階層を編成します
3. クライアント PC をそのグループに追加します
4. スレーブ管理サーバを追加します

論理ネットワークの構造は、[グループ] フォルダ内に反映されます。論理ネットワークの各オブジェクト、つまりスレーブサーバ、グループおよびクライアント PC についての情報を入手できます。提供されるデータには、オブジェクトの作成日および設定の最終変更日が含まれます。また、オブジェクト(スレーブサーバ、クライアント PC、またはグループ内の全クライアント PC) が管理サーバとのやりとりに使用する設定を確認できます。これらの内容は、必要であれば設定を変更できます。

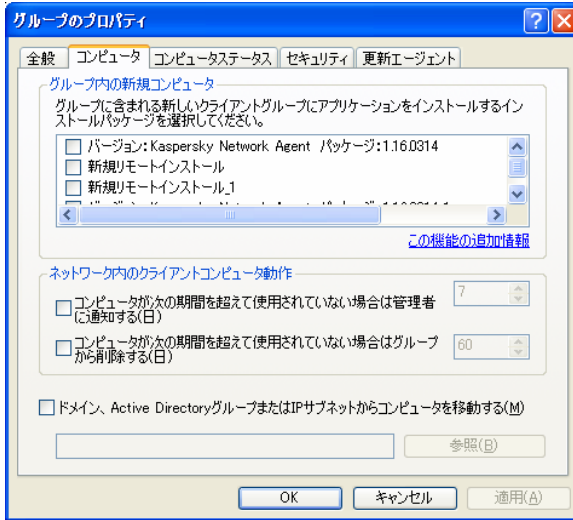


図 8. グループのプロパティの表示 - [コンピュータ] タブ

特定のクライアント PC に関する情報を入手するには、論理ネットワーク内でコンピュータ検索機能を利用します。この検索には、スレーブ管理サーバの論理ネットワークについての情報を使用できます。このような検索を実行し、コンピュータについての情報をコンソールツリーの別のフォルダに表示するには、フィルタ作成機能を使用してください。

企業ネットワーク構成に変更を加えた場合は、論理ネットワークにもしかるべき変更を加えてください。以下のことができます：

- 論理ネットワークに、ネスト化レベルグループを任意の数だけ追加する（次の階層レベルを形成するスレーブ管理サーバとネスト化されたグループをグループに追加できます）

また、該当グループのすべてのクライアント PC に自動インストールするカスペルスキー製品も定義できます。

- クライアント PC をグループに追加する

Microsoft Windows 98/ME が動作する新たにネットワーク接続したコンピュータに対してカスペルスキー製品の自動インストールを有効にするには、ネットワークエージェントをインストールする必要があります。

- 個々のクライアント PC とグループ全体を別のグループに移動することで、論理ネットワーク上のオブジェクトの階層順を変更する
- マスタサーバの負荷と内部トラフィックを削減し、リモート管理システムの信頼性を向上させるために、論理ネットワーク構造にスレーブ管理サーバを追加する
- 論理ネットワーク間でクライアント PC を移動する

3.5.1. グループ

新規グループを追加するには、ネスト化されたグループの追加先グループでショートカットメニューの **[新規作成]** → **[グループ]** を使用します。コンソールツリーの **[グループ]** ノード（図 7 を参照）には、指定した新規フォルダが指示どおりの名前で表示されます。ネスト化された **[管理サーバ]**、**[ポリシー]** および **[グループタスク]** フォルダは、このフォルダ内に自動的に作成されます。これらのフォルダには、グループポリシーの定義、グループタスクおよびスレーブサーバの作成段階で情報が追加されます。

次の階層を形成するクライアント PC およびネスト化されたグループは、このグループに含めることができます。継承ポリシーおよびネスト化されたグループタスクの表示は、カスタマイズ可能です。

また、このグループに追加されたすべてのクライアント PC に自動インストールするカスペルスキー製品も定義できます。

グループの名称変更、別のグループへの移動、または削除は、後からでも実行できます。

グループは、すべてのネスト化されたグループ、スレーブ管理サーバ、クライアント PC、グループポリシーおよびタスクと一緒に移動されます。論理ネットワークオブジェクトの階層における新しい状況と対応する設定がすべて、このグループに適用されます。

グループの移動は、標準のショートカットメニューコマンド **[切り取り]** → **[貼り付け]** または **[操作]** メニューの利用、あるいはマウスを使用しても行うことができます。

グループを移動する場合は、1 階層内のグループそれぞれに固有の名前が必要である点に注意してください。名前の競合を解決するには、移動前にグループの名前を変更してください。変更しなかった場合は、名前の最後に「_1」「_2」などが自動で追加されます。

[グループ] フォルダは管理コンソールの組み込みエレメントであるため、名前を変更できません。

グループ内にスレーブ管理サーバ、ネスト化されたグループ、クライアント PC が含まれず、グループに対してタスクやポリシーがない場合は、そのグループを論理ネットワークから削除できます。ショートカットメニューの **[削除]** コマンドまたは **[操作]** メニューの同様の項目を使用して、選択したグループを削除できます。

3.5.2. クライアント PC

グループにクライアント PC を追加するには、コンピュータの追加先グループでショートカットメニューの [新規作成] → [コンピュータ] コマンドを使用します。

ウィザードに沿って作業を正常に完了すると、コンピュータがグループに追加され、管理サーバによって決定された名称で結果パネルに反映されます (図 9 を参照)。

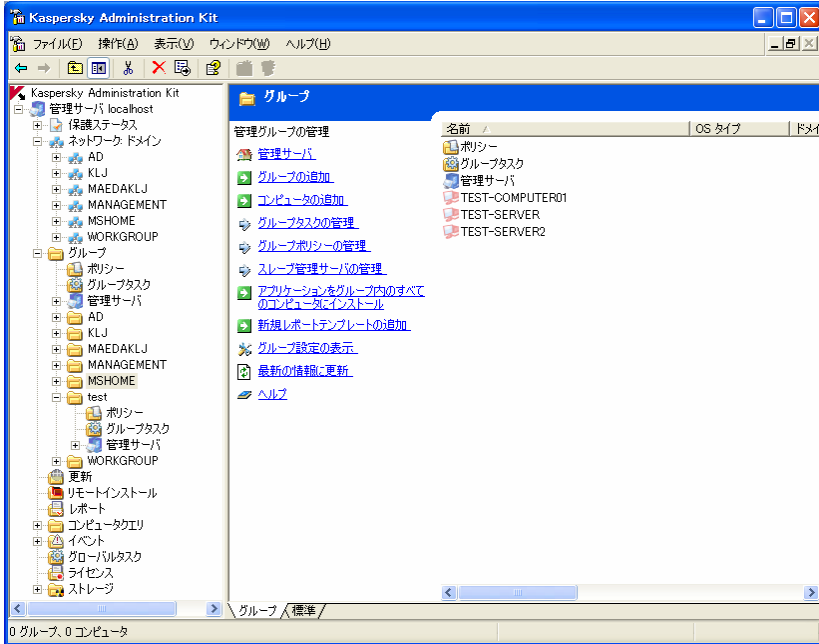


図 9. グループ内のクライアント PC

論理ネットワークにクライアント PC を追加するにあたって、検知されたすべてのコンピュータを指定の管理グループへ自動的に追加する方法を設定できます。この場合、対応する設定が [ネットワーク] グループのプロパティで構成されている必要があります (図 10 を参照)。

[ネットワーク] フォルダから論理ネットワークフォルダへコンピュータをマウスでドラッグしても、Kaspersky Administration Kit のメインウィンドウにコンピュータを追加できます。

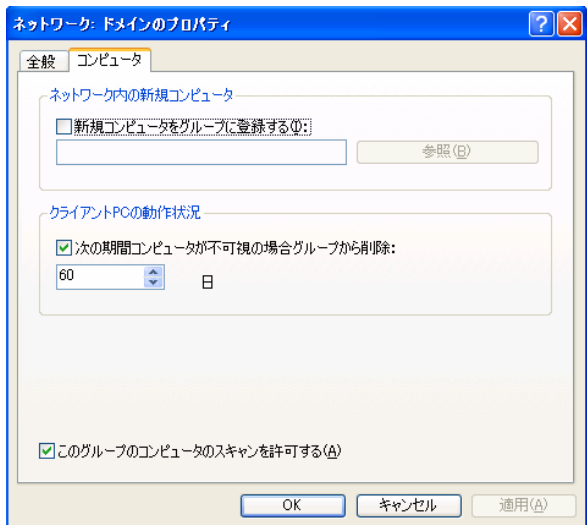


図 10. 新規コンピュータのグループへの自動追加の設定

クライアント PC を論理ネットワークから除外することで、あるグループから別のグループにクライアント PC を移動できます。この作業には、標準のショートカットメニューコマンド [切り取り] → [貼り付け] および [削除] を使用するか、[操作] メニューの同様の項目を使用します。論理ネットワークから削除されたコンピュータは、[ネットワーク] グループに移動されます。移動の操作は、マウスを使って行うこともできます。

クライアント PC は、ある論理ネットワークから別の論理ネットワークに移動できます。たとえば、スレーブ管理サーバを追加する場合、マスタサーバの論理ネットワークからスレーブサーバの論理ネットワークにクライアント PC を移動できます。この作業を行うには、クライアント PC が新規管理サーバに接続されている必要があります。

別の管理サーバへのクライアント PC の接続は、**管理サーバ変更**タスクを作成して起動することで行います。グローバルタスクを作成して個々のコンピュータを移動するか、グループタスクを使って特定の管理グループからすべてのクライアント PC を移動することができます。**サーバ変更**タスクを実行すると、このタスクに関連するクライアント PC は古い管理サーバから切断され、新しいサーバの [ネットワーク] グループに表示されます。クライアント PC を古い論理ネットワークの管理グループから削除し、管理コンソールを使って新しい論理ネットワークへ手動で追加することができます。

クライアント PC から、異なる管理サーバにローカル接続できます。
この操作は、ネットワークエージェントに含まれている *klmover.exe* ユーティリティを使用して実行されます。ネットワークエージェントのインストール後、このユーティリティはコンポーネントのルートインストールフォルダに配置されます。

3.5.3. スレーブ管理サーバ

サーバ階層を使用して、すべてのスレーブ管理サーバおよびこれに接続しているクライアント PC に対し、メインサーバから次の操作を実行できます：

- 「アプリケーションポリシー」を作成して配布する
- 「グループタスク」(配布タスクを含む) を作成して配布する
- メインサーバによって受信された「更新」と「インストールパッケージ」を配布する
- すべてのスレーブ管理サーバについての総合的な情報による「レポート」を作成する

マスタ管理サーバから受信したポリシーとタスクは、スレーブサーバでは変更できません。

スレーブサーバを追加するには、グループ内の管理サーバオブジェクトに対し、必要に応じて **[新規作成]** → **[管理サーバ]** を使用します。これによって、スレーブサーバ追加ウィザードが起動します。このウィザードでは、以下の作業を行います。

- スレーブ管理サーバを追加する
- スレーブサーバに管理コンソールを接続する
- メインサーバへの接続設定を構成する
- スレーブサーバについての情報を、メイン管理サーバのデータベースに追加する
- 接続と設定はウィザード終了後に手動で実行することができます。その場合は、スレーブサーバとして使用するサーバに管理コンソール経由で接続し、メインサーバへの接続設定を指定します (図 11 を参照)

スレーブ管理サーバが正常に追加されると、サーバのアイコンと名前が **[管理サーバ]** フォルダの該当するグループに表示されます。

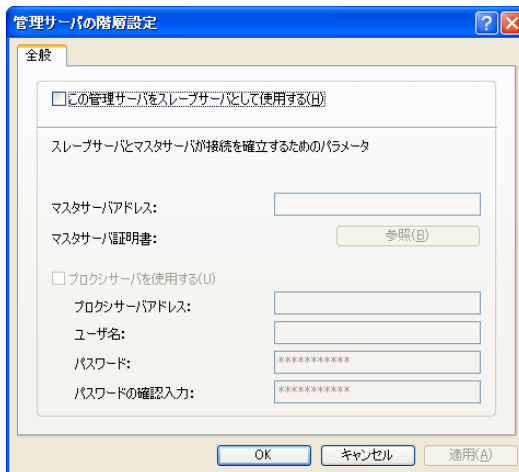








図 11. メイン管理サーバへの接続設定の構成

スレーブ管理サーバの論理ネットワークは、メインサーバの論理ネットワークにある [管理サーバ] ノード経由で管理できます。または、新規管理サーバとしてコンソールツリーにサーバを追加することで直接管理することもできます。

スレーブサーバは十分な機能を備えた管理サーバであり、スレーブサーバ論理ネットワーク内で管理サーバの機能をすべて実行します。

スレーブ管理サーバはさらに、自分の含まれているグループのすべてのタスクとポリシーをメインサーバから継承します。継承されたポリシーとタスクは、次のようにスレーブサーバに表示されません：

- アイコン() は、メインの管理サーバから受け取ったポリシーの名前の横に表示されます (通常のポリシーアイコンは )
- 継承されたポリシーの設定値は、スレーブサーバでは変更できません (値にアクセスできません)
- 継承されたポリシーでの変更が許可されていない設定は、スレーブサーバ上のすべてのアプリケーションポリシーではアクセスまたは変更できず、継承されたポリシーに指定されている値が使用されます (アイコン )
- 継承されたポリシーでの変更が許可されている設定の値は、スレーブサーバのポリシー内で変更できます (アイコン )。この設定がスレーブサーバのポリシーで「ロック」されていない場合は、アプリケーション設定またはタスク設定で変更可能です (13 ページの 2.1.7 項を参照)
- アイコン() は、メインの管理サーバから受け取ったグループタスクの名前の横に表示されます (通常のタスクアイコンは )

グローバル導入タスクは、スレーブサーバに転送できません。グループタスクの転送は、タスクのプロパティで設定します。

スレーブ管理サーバのクライアント PC の更新は、次のように設定できます。メインサーバによって更新が受信されると、スレーブサーバによる更新受信のタスクが自動的に起動され、このタスクが完了した後にスレーブ管理サーバのクライアント PC に対するアプリケーション更新タスクが起動されます (54 ページの 5.3 項を参照)。

4 ポリシーのリモート管理

Kaspersky Administration Kit は、専門のコンポーネント（配布パッケージに含まれるアプリケーション管理プラグイン）を備えたカスペルスキー製品のみをサポートします。

4.1. アプリケーションの設定

4.1.1. ポリシーの管理

アプリケーション用にポリシーを作成できるのは、このアプリケーション用のプラグインが管理コンピュータにインストールされている場合に限られます。

ポリシーを作成するには、[ポリシー] フォルダのショートカットメニューの [新規作成] → [ポリシー] コマンドを使用します。ポリシー作成のこの段階では、アプリケーション操作に必要な最低限のパラメータセットを構成します。その他の設定はすべてデフォルト設定され、アプリケーションのローカルインストール時に適用されるデフォルト値と対応しています。

カスペルスキー製品のポリシー設定の詳細は、各アプリケーションのマニュアルに記載されています。

設定値の変更、ネスト化されたグループおよびアプリケーション設定内でのポリシーでの設定の変更禁止は、後で行うことができます（図 12 を参照）。

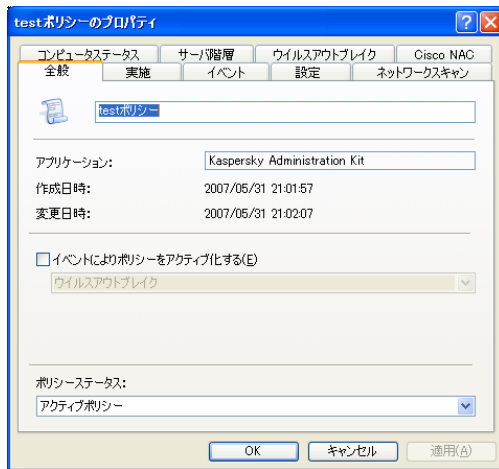


図 12. ポリシーの編集

ポリシーによって支配される設定項目および修正が禁止されている設定項目には、そのことを示すアイコンが表示されます。変更を禁止するにはアイコンをクリックして、アイコンが変化させます。これらの設定は、アプリケーションの設定、タスク設定、ネスト化されたグループおよびスレーブ管理サーバのポリシーを使ってアクセスできなくなります。

ローカル設定は、ポリシー設定よりも高い優先度を持ちます（13 ページの 2.1.7 項を参照）。特定の設定に対してポリシーで指定された値を使用する場合は、それらの設定項目をロックする必要があります。

新規ポリシーが作成されると、ポリシーは対応するグループの [ポリシー] フォルダに追加され（図 13 を参照）、継承ポリシーとしてすべてのネスト化されたグループおよびスレーブ管理サーバに適用されます。

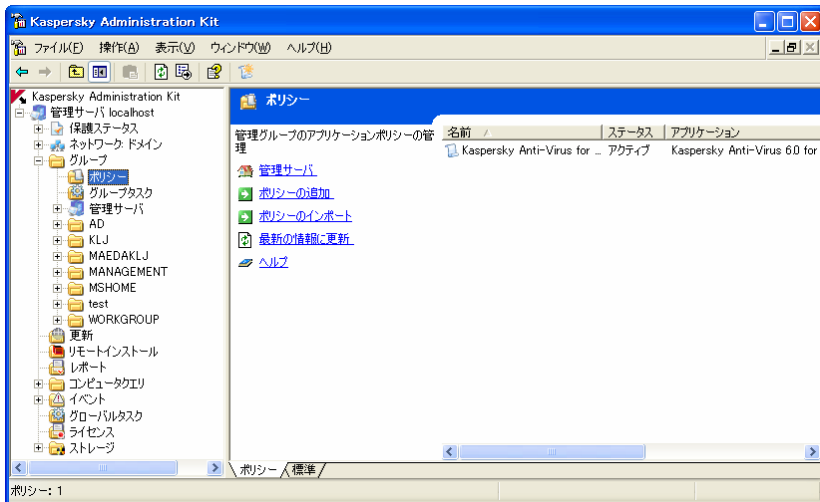


図 13. [ポリシー] フォルダ

結果ウィンドウで選択されたポリシーのショートカットメニューを使用して、作成したポリシーを削除、コピー、あるグループから別のグループへエクスポートまたはインポートできます。

各アプリケーションに対して複数のグループポリシーを作成できますが、その設定内容を有効（アクティブ）にできるポリシーは 1 つだけです。このようなポリシーの設定では、[アクティブポリシー] パラメータが選択されている必要があります。

ポリシーは、特定のイベントによって起動されて自動的にアクティブ化されます。ただし、以前のポリシーに戻る作業は手動で行う必要があります。

また、企業の論理ネットワークからコンピュータが切断されたときただちに実施されるモバイルユーザ用のポリシーを作成することもできます。

論理ネットワークから管理サーバへの接続試みが 3 回失敗すると、ノードの接続が切断されたとみなされます。接続試みの間隔は、管理エージェントの設定を通じて指定されます。[同期間隔(分)] フィールドを使用します (デフォルト設定は 15 分)。

ポリシー導入の結果は、管理サーバのポリシープロパティウィンドウの管理コンソールを通じて表示できます (図 15 を参照)。

各クライアントのローカルアプリケーションパラメータに対する変更は、[詳細設定] ウィンドウで選択されているオプションに従って実施されます。このウィンドウには、ポリシープロパティウィンドウの [実施] タブにある [詳細設定] リンクからアクセスできます。

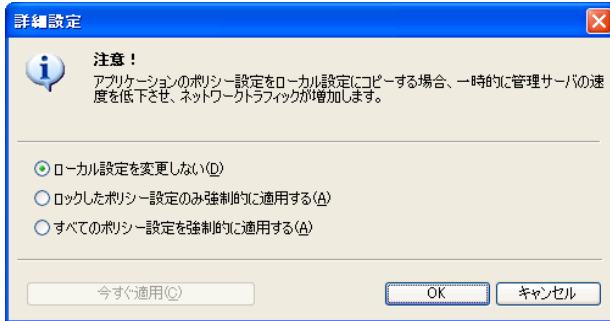


図 14. ポリシー適用の構成

ローカルパラメータは、ポリシーがクライアントへ最初に適用されるとき (次に示す場合) に選択されたオプションに基づいて自動的に更新されます:

- ポリシーを適用可能な領域にクライアントが追加された場合
- ポリシーが有効になった場合
- ポリシーが適用されるアンチウイルス製品がクライアントにインストールされた場合

次のいずれかのオプションを選択できます:

- **ローカル設定を変更しない** - ポリシー設定でアイコン (🔒) が付いているパラメータのみがアプリケーションに適用されます。残りのパラメータは、ローカル設定によって支配されます。これはデフォルトオプションです

ポリシーが削除または無効化されると、アプリケーションはポリシーが適用される前に有効だった値に戻ります。

- **ロックしたポリシー設定のみ強制的に適用する** - ポリシー設定でアイコン (🔒) が付いているパラメータのみがアプリケーションに対して実施されます。

ポリシーが削除または無効化されると、ポリシーの元で編集可能なパラメータ (🔒 が付いたもの) だけが元の値に戻ります。

- **すべてのポリシー設定を強制的に適用する** - これによって、すべてのローカルパラメータがポリシー設定の値とみなされます。

ポリシーが削除または無効化された後も、ポリシーで定義された設定が引き続き使用されます。設定は、後から手動で変更することもできます。

ポリシーは、手動でも変更できます。[今すぐ適用] をクリックしてください。これによって、上記で選択された設定に従ってポリシーが適用されます。

ローカルアプリケーション設定の値を各クライアント PC で変更する方法は、[ロックしたポリシー設定のみ強制的に適用する] ボックスのステータスによって異なります（13 ページの 2.1.7 項を参照）。

さらに、ポリシーが実施されているかどうかに関係なく、手動で行った選択内容と設定を一致させることができます。[適用] をクリックしてください（図 15 を参照）。

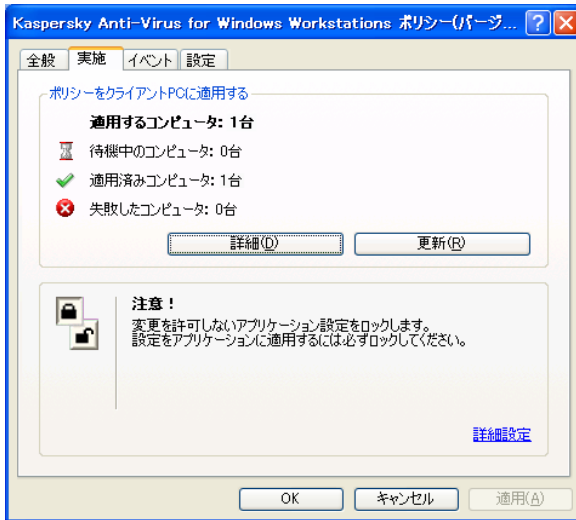


図 15. ポリシー実施設定の構成

ポリシーは次の方法で適用されます。常駐タスク（リアルタイム保護）がクライアントで実行中の場合、新しい設定値が即座に適用されます。クライアントでスケジュールタスク（オンデマンドスキャン、データベース更新）が実行中の場合は、古い値で作業が継続されます。新規ポリシーは、タスクの次回スタートアップ時に適用されます。新規ポリシーが適用された後は、特定のクライアント PC のプロパティウィンドウにある管理コンソールを通じてアプリケーション設定を表示できます。

階層構造の場合、スレープ管理サーバがマスタサーバからポリシーを取得し、これらのポリシーをクライアント PC に適用します。ポリシー設定を変更できるのは、マスタ管理サーバだけです。その後、スレープサーバは必要に応じてポリシーを修正し、クライアント PC 全体に配布します。

マスタ管理サーバとスレープ管理サーバの接続が切断された場合、ポリシーはスレープサーバ上で、以前の設定で引き続き有効です。管理サーバ上で更新されたポリシー設定は、接続が再度確立されたときにスレープサーバに反映されます。

管理サーバとクライアントの接続が切断された場合は、ローミングユーザ用ポリシーがクライアント上で有効になる（定義されている場合）か、接続が再度確立されるまでポリシーが以前の設定で引き続き有効となります。

スレープ管理サーバへのポリシー配布の結果は、マスタ管理サーバのポリシープロパティウィンドウに表示されます。

クライアント PC へのポリシー配布の結果も同様に、スレープ管理サーバに接続した後、スレープ管理サーバのポリシープロパティウィンドウに表示できます。

カスペルスキー製品のポリシー設定の詳細は、各アプリケーションのマニュアルに記載されています。ネットワークエージェントと管理サーバのポリシー構成については、『Kaspersky Administration Kit 参照ガイド』を参照してください。

4.1.2. ローカルアプリケーション設定

Kaspersky Administration Kit システムでは、管理コンソールを使用して、クライアント PC にインストールされたローカルアプリケーションの設定をリモート管理できます（図 16 を参照）。アプリケーションの設定を使用して、グループ内の各クライアント PC に対するアプリケーション動作設定の値を個別に設定できます。特定アプリケーションのグループポリシーによって変更が禁止されていない設定（「ロック」されていない設定）についてのみ、値を変更することができます。

ローカル設定の構成は、["<アプリケーション名>" アプリケーション設定] で各クライアント PC について個別に実行されます。このウィンドウは、クライアントのプロパティウィンドウにある [アプリケーション] タブから呼び出します。

各カスペルスキー製品には、独自の一連のローカル設定があります。これら設定の詳細については、該当製品のマニュアルを参照してください

ネットワークエージェント設定および管理サーバ設定の詳細については、『Kaspersky Administration Kit 参照ガイド』をご覧ください。



図 16. ローカルアプリケーション設定の構成ウィンドウ

4.2. アプリケーションの管理

クライアント PC にインストールされているアプリケーションの動作は、すべての主要機能（アプリケーションとライセンスキーのインストール、ファイルのスキャン、定義データベースとアプリケーションモジュールの更新など）を実装するタスクを作成して開始することで管理されます。

Kaspersky Administration Kit は、ローカルアプリケーション管理用に提供されるすべてのタスクをサポートしています。さらに、対応するネットワークエージェント管理タスクを使用してアプリケーションをリモートから開始および停止する機能もあります。カスペルスキー製品それぞれに関するタスクタイプの説明については、特定のアプリケーションのマニュアルをご覧ください。

リモートからのアプリケーションの開始および停止は、対応するタスクを使って管理コンソール経由で実行されます。

アプリケーションに対してタスクを作成できるのは、このアプリケーションに対する管理プラグインが管理コンピュータにインストールされている場合にに限られます。

ネットワーク保護を確実に実行できるように、管理者は Kaspersky Administration Kit を使って管理されているすべてのアプリケーションに対し、さまざまなタスク（一度限りで作成されるタスクを除く）を任意の数だけ作成できます。

たとえば、クライアント PC 上のウイルススキャンを実行するには、Kaspersky Anti-Virus for Windows Workstation に対するオンデマンドスキャンタスクを作成する必要があります。

アプリケーション管理機能と全般的なサービス操作は、Kaspersky Administration Kit、管理サーバおよびネットワークエージェントコンポーネントのタスクを実行します。このコンポーネントに対し、次のタイプのタスクが定義されます：

- 管理サーバの変更
- アプリケーションの起動/停止
- アプリケーション導入
- アプリケーションのリモートアンインストール
- 管理サーバによる更新の受信
- 管理サーバのバックアップコピーの作成
- レポートの送付
- インストールパッケージの配布

これらのタスクには、作成と起動に関する固有の機能がいくつか備わっています。これらタスクの管理の詳細については、『Kaspersky Administration Kit 参照ガイド』をご覧ください。

すべてのタイプのタスクに、グループ、グローバル、またはローカルタスクを作成できます。

導入の場合は、グループタスクとグローバルタスクの両方を作成できます。**更新の受信、バックアップの作成、レポートの送付**のタスクの場合は、グローバルタスクだけを作成できます。

更新の受信および管理サーバのバックアップコピーの作成のタスクは、1 つの構成要素内では作成できず、1 台のコンピュータ（管理サーバ）に対してしか実行できません。

タスクを使用するには、[グループタスク] フォルダまたは [グローバルタスク] フォルダでショートカットメニューの [新規作成] → [タスク] コマンドを使用します。

作成されたグループタスクは、該当するグループのネスト化されたフォルダ [グループタスク] に置かれます（図 17 を参照）。グループタスクは、コンソールツリー内の [グループタスク] と呼ばれる特別なコンテナ内に置かれます。クライアント PC のプロパティウィンドウ内で、クライアント PC のローカルタスク一覧を確認できます。

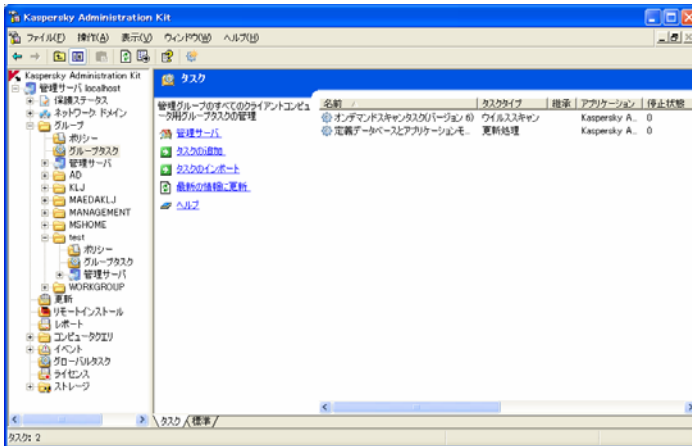


図 17. グループタスク

ネットワークエージェントがサーバに接続したとき、ローカルアプリケーションと Kaspersky Administration Kit の情報データベースとの間で、タスクについての情報が交換されます。ローカルで作成されたタスクについての情報が、管理サーバデータベースに転送されます。

ショートカットメニューのコマンドを使用して、タスク設定の変更、タスク実行の監視、あるグループから別のグループへのタスクのコピー、エクスポートまたはインポート、あるいはタスクの削除を行うことができます。

各クライアント PC でタスクを実行する間に、グループポリシー、タスク設定およびクライアント PC にインストールされている特定アプリケーションの設定に従って、アプリケーション動作設定がインストールされます (13ページの 2.1.7 項を参照)。

ほとんどの設定は、このタスクを実行するアプリケーションのポリシーによって定義されます。たとえば、感染オブジェクトを検知した場合の動作、定義データベースの更新に使用されるリソースなどです。これらの設定がロックされている場合は、タスク設定で変更できません (図 18 を参照)。

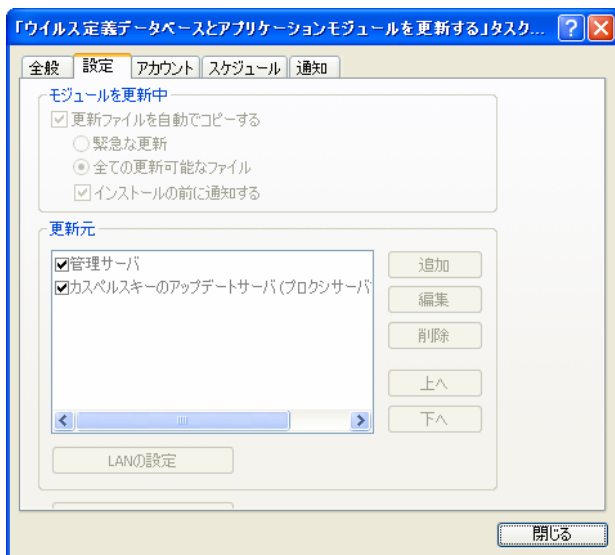


図 18. ポリシー内でロックされているタスク設定

ただし、設定の一部は特定のタスクに固有です。たとえばタスク開始のスケジュール、タスクを開始するアカウント、自動スキャンタスクのスキャン範囲などです。これら設定の値は、設定内で各タスクに関して設定され、タスクの作成後に変更することができます (図 19 を参照)。

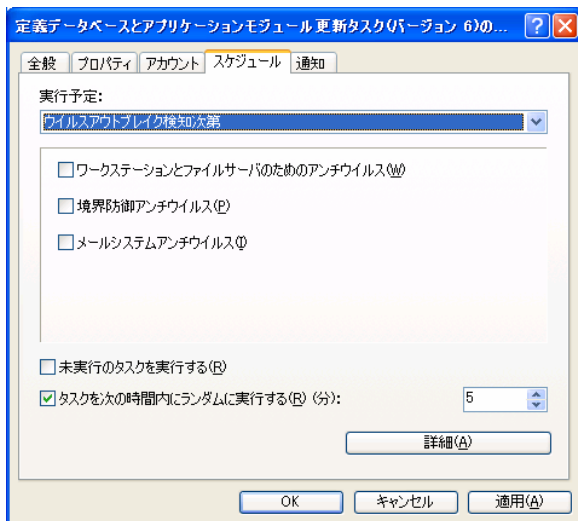


図 19. タスクの開始スケジュール

タスクはスケジュールに従って開始されます。スケジュールされた起動時刻にコンピュータがオフである場合は、「Wake On LAN 機能」を使用してオペレーティングシステムを自動的にロードできます。この機能を使用するには、[スケジュール] タブ(図 19 を参照)で[詳細] ボタンを押すと開く、対応するボックス(図 20 を参照)をオンにする必要があります。

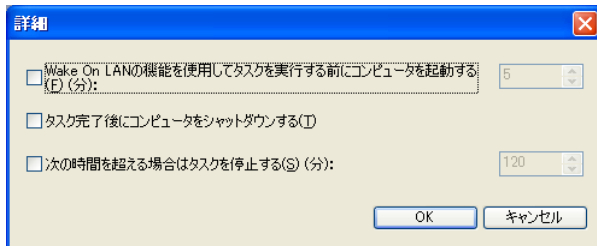


図 20. オペレーティングシステムの自動ロードの有効化

スケジュールされたタスクが完了した後にコンピュータが自動的にオフになるように設定することもできます。

タスク実行時間を制限することができます。こうすることで、指定された実行時間が経過した後、タスクが停止します。スケジュールされたタスクの開始を無効にすることができます。この場合、タスクは削除されませんが、開始もされません。

さらに、ショートカットメニューのコマンドまたはタスク設定表示ウィンドウを使用して、手動でタスクを開始、中断、一時停止、再開できます(図 21 を参照)。

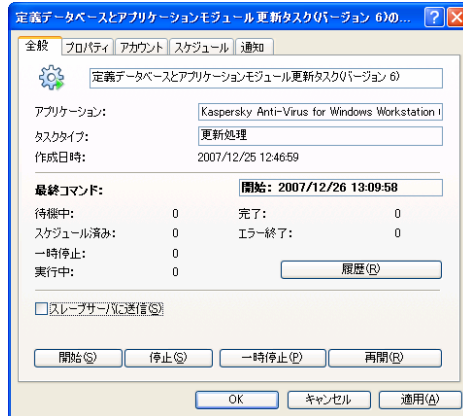


図 21. タスク実行の管理

クライアント PC 上のタスクは、対応するアプリケーションが実行していないと実行されません。アプリケーションを閉じると、実行中のタスクはすべて終了します。

タスク設定ウィンドウで、タスクの実行を監視し、実行の結果を見ることができます（図 21 を参照）。

タスクの実行結果は、設定に従って Windows イベントログと Kaspersky Administration Kit イベントログに登録および保存されます。これらのログは、管理サーバの中央集中的な場所と、各クライアント PC のローカルにあります。管理者およびその他ユーザは、タスク実行の結果について通知を受けることができます。通知の形式と方法も、タスク設定で決定されます。

Kaspersky Administration Kit に登録されたタスク実行結果は、コンソールツリーの [イベント] ノードで見ることができます。各クライアント PC のタスク実行結果は、コンピュータのプロパティウィンドウで見ることができます。

管理サーバの階層構造では、対応するパラメータがタスク設定に含まれていると（図 21 を参照）、スレープサーバはメイン管理サーバからグループタスクを受け取り、それをクライアント PC に配布します。グループタスクの設定は、メインの管理サーバで変更できます。変更の後、それに応じてスレープ管理サーバが自分のグループタスクを変更し、接続しているクライアント PC にこれを配布します。

スレープ管理サーバへのグループタスク配布の結果は、管理サーバのグループタスクプロパティウィンドウの [タスク履歴] ウィンドウに表示されます。

同様に、クライアント PC へのグループタスク配布の結果は、スレープ管理サーバに接続した後、スレープ管理サーバのグループタスクプロパティウィンドウで確認できます。

5 定義データベースとモジュールの更新

定義データベースおよびアプリケーションモジュール（パッチ）の更新を定期的に行うことは、あらゆる脅威からネットワークを保護するためにとても重要です。

カスペルスキーの Web ベースの定義データベースは、およそ 1 時間ごとに更新されます。定義データベースの更新とプログラムパッチのインストールを、クライアント側でも同じ頻度で行うことを強くお勧めします。

Kaspersky Administration Kit を通じて管理されている定義データベースとプログラムモジュールを更新するには、Kaspersky Administration Kit が更新を取得するためのグローバルタスクを作成する必要があります。Kaspersky Administration Kit は、グローバルタスク設定に従って、更新されたデータベースとモジュールをアップデートサーバやフォルダからダウンロードします。ダウンロードされた更新は、管理サーバのパブリックフォルダ [更新] に保管されます。更新が完了すると、ここからクライアント PC およびスレーブ管理サーバに更新が自動配布されます。このパブリックアクセスフォルダは、管理サーバのインストール時に作成されます。デフォルトでは、このフォルダは「KLSHare」という名前前で管理サーバコンポーネントのインストールディレクトリ（<ドライブ>:\Program Files\Kaspersky Lab\Kaspersky Administration Kit）に置かれます。

更新は、アプリケーション更新タスクを使用してクライアント PC に配布されます。スレーブサーバの更新は、管理サーバによる更新の受信タスクを使用して行われます。これらのタスクは、タスク設定のスケジュールとは関係なく、マスタサーバが更新を受信した直後に自動的に開始されるように設定できます。

5.1. 管理サーバによる更新の受信

管理サーバによる更新の受信のタスクはグローバルタスクであり、1 つのインスタンスしか作成できません。このタスクは、1 台のコンピュータ、つまり管理サーバがインストールされているコンピュータのみに対して作成および実行されます。

クイックスタートウィザードを使用した場合、管理サーバによる受信のタスクはすでに作成済みであり、コンソールツリーの [グローバルタスク] ノード内にあります。

管理サーバによる受信のタスクを作成するには、[グローバルタスク] ノードからタスク作成ウィザードを起動します。タスク作成対象アプリケーションとして [Kaspersky Administration Kit]、タスクのタイプとして [更新ダウンロードタスク] を選択します（図 22 を参照）。

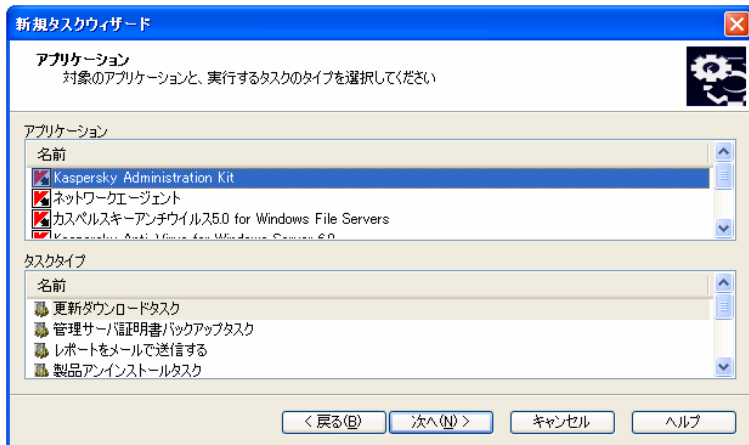


図 22. 更新タスクの作成 - アプリケーションとタスクタイプの選択

論理ネットワーク内で管理サーバ階層が作成されている場合（または作成の予定がある場合）は、更新がスレーブサーバに自動配布されるように、メインサーバのタスク設定で **[スレーブサーバを強制更新する]** ボックス（図 23 を参照）をオンにする必要があります。これによって、メインサーバが更新された直後に、スレーブサーバの更新タスクが開始されます（このようなタスクが作成してある場合）。

[スレーブサーバを更新する] ボックスがオンになっていると、スレーブ管理サーバによる更新受信のタスクは自動作成されません。これらのタスクは、各スレーブサーバについて手動で個別に作成する必要があります。

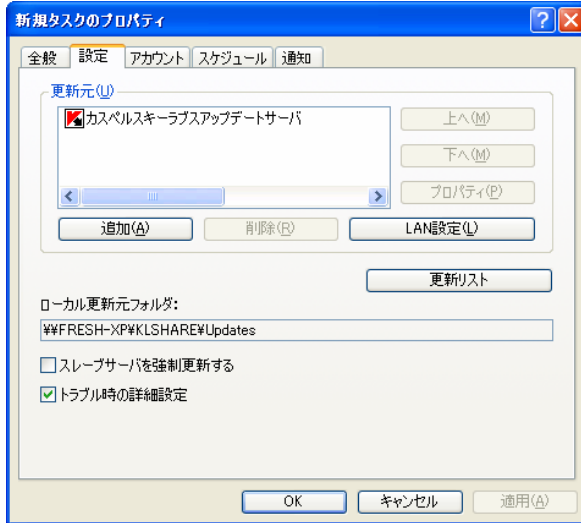


図 23. 更新受信タスクの設定

管理サーバによる更新の受信タスクが実行されると、定義データベースとアプリケーションモジュールの更新が更新元からダウンロードされ、パブリックアクセスフォルダに置かれます。

ダウンロードされた更新は、パブリックアクセスフォルダからクライアント PC (53 ページの 5.2 項を参照)とスレープ管理サーバ (54 ページの 5.3 項を参照) に配布されます。

管理サーバの更新元として、次のものを使用できます。

- カスペルスキーのアップデートサーバ
- メイン管理サーバ
- ftp/http サーバまたはネットワークの更新用フォルダ

どれを使用するのは、タスク設定によって異なります。

更新が ftp/http サーバまたはネットワークフォルダから実行される場合は、サーバを正しく更新するために、更新を含むフォルダの構造 (更新コピー時にカスペルスキーのツールで作成された構造と一致) が、これらの更新元にコピーされている必要があります。

コンソールの [更新] フォルダで、受信した更新についての情報を確認できます。更新の一覧は、結果パネルに表示されます (図 24 を参照)。

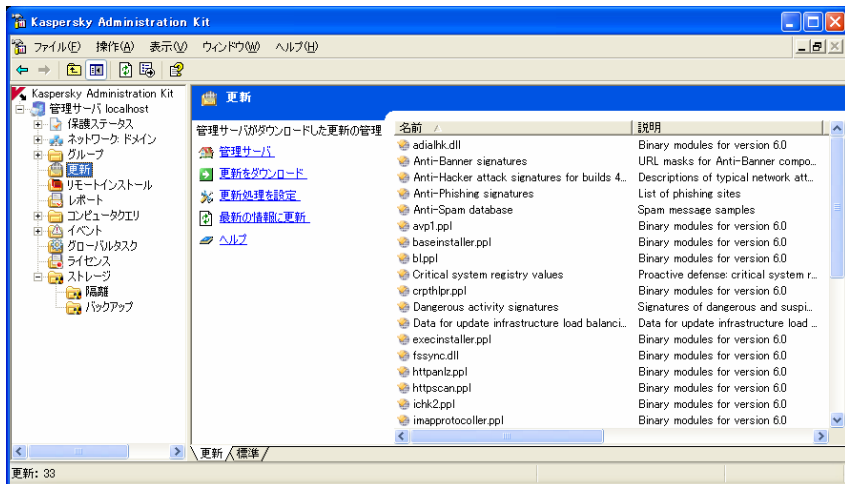


図 24. 受信した更新の表示

5.2. クライアント PC の更新処理

アンチウイルス保護の信頼性を高めるために、論理ネットワーク内のアンチウイルス保護システムに含まれるアプリケーションすべてに対して更新処理のタスクを作成する必要があります。

論理ネットワーク内の各クライアント PC に適用されている定義データベースとアプリケーションモジュールを同期するには、更新タスクの設定で更新元に管理サーバを選択してください。

アプリケーション更新タスクで更新元として管理サーバが選択されていると、サーバの階層構造を受けて、クライアント PC は接続しているサーバ(メインサーバではなくスレープサーバ)から更新を受け取ります。

アプリケーション更新タスクの作成手順については、該当するアプリケーションのマニュアルをご覧ください。

トラフィックおよび管理サーバに対するクライアント PC の呼び出しを削減し、多数のクライアント PC を伴う論理ネットワークでは、更新タスクの設定ミスや実行エラーを避けるために、自動更新処理の適用をお勧めします。

管理サーバの負荷を削減するために、更新エージェントの使用をお勧めします。これによって、管理グループ内で更新が確実に適用されます。

5.3. スレーブサーバとクライアントの更新

管理サーバの階層構造が論理ネットワークにまとめられている場合にスレーブサーバが更新ファイルを受信後、自分に接続しているクライアント PC に配布するには、以下の作業を行う必要があります：

- 各スレーブ管理サーバが更新を受信するためのタスクを作成する
- スレーブサーバの更新受信タスクの設定で、更新元として **[マスタ管理サーバ]** を選択する（図 25 を参照）
- スレーブサーバへの自動更新配布モードを、メイン管理サーバによる更新受信タスクの設定で **[スレーブサーバを更新する]** ボックスをオンにして有効にする
- 必要であれば、管理グループ内で更新エージェントを指定する（55 ページの 5.4 項を参照）
- Kaspersky Anti-Virus for Windows Workstation バージョン 6.0 および 5.0、Kaspersky Anti-Virus 5.0 for Windows File Servers ならびに Kaspersky Anti-Virus 6.0 for Windows Servers がインストールされているクライアント PC への自動更新配布モードを有効にする。その他アプリケーションの場合は、管理サーバからの更新受信のタスクを作成または構成します

更新は、クライアント PC が接続している管理サーバ、つまりメインサーバではなくスレーブサーバからダウンロードされます。

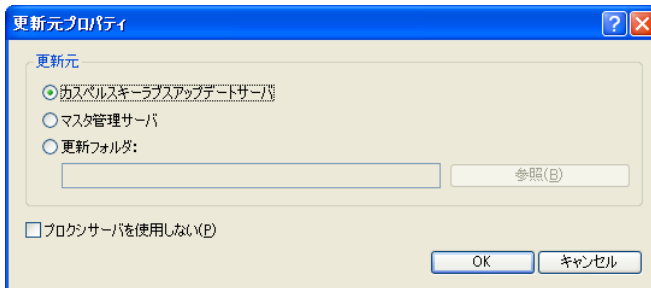


図 25. メイン管理サーバからの更新

5.4. 更新エージェントを使用した更新処理

グループ内のクライアント PC に更新を配布するために、「更新エージェント」を使用できます。これは、管理グループ内で更新およびインストールパッケージを配布するための中継センターとして機能するコンピュータです。更新エージェントは管理サーバから更新を受け取り、アプリケーションインストールフォルダに置きます。グループ内で必要とされる更新だけがダウンロードされます。グループ内のクライアント PC は、後でこのエージェントを使用して、SSL 接続を使って更新をダウンロードできます。

更新とインストールパッケージを含むフォルダの場所を変更すること、またはそうしたフォルダのサイズに制限を設けることは、許可されていません。

更新エージェント一覧の作成およびエージェントの構成は、グループプロパティウィンドウの [更新エージェント] タブで実行します (図 26 を参照)。

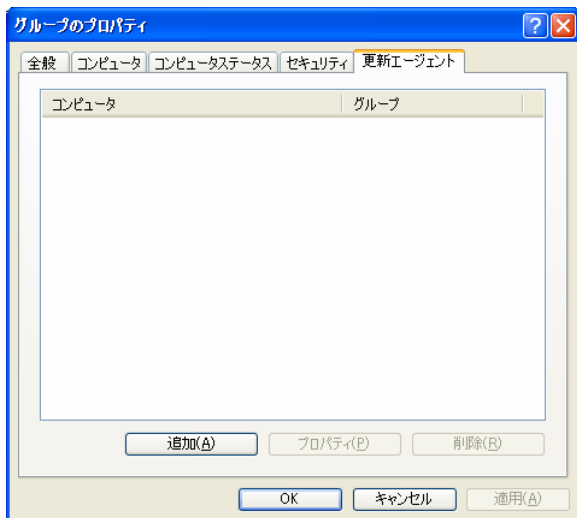


図 26. 更新エージェント一覧の作成

6 メンテナンス

6.1. ライセンスの更新

カスペルスキー製品を使用する権利は、ソフトウェア製品を購入したときに交わすライセンス契約に基づいて付与されます。

ライセンスの有効期間中は、以下のサービスを受けていただくことができます：

- 製品のアンチウイルス機能の使用
- 定義データベースおよびモジュールの更新
- バージョンの無償アップグレード
- 製品のインストール、設定および操作に関するテクニカルサポート
- 疑わしいオブジェクトや感染オブジェクトのカスペルスキーへの送付および解析

Kaspersky Administration Kit のアクティベーションにはライセンスキーは必要ありません。

テクニカルサポートにお問い合わせの場合は、**Kaspersky Administration Kit** を通じて管理される購入済みのカスペルスキー製品のライセンス情報をご確認ください。

Kaspersky Administration Kit はライセンスをチェックし、すべてのカスペルスキー製品に不可欠なパーツであるライセンスキーを使用してライセンス有効期間を確認します。1 つのアプリケーションが所有できる有効なライセンスキーは 1 つだけです。ライセンスキーにはソフトウェアの使用期限が含まれており、特別なプログラム手段で読み取って検証できます。

ライセンスの有効期間が過ぎると、上記のオプションを使用できなくなります。ライセンスを更新するには、新しいライセンスキーを購入してインストールする必要があります。

Kaspersky Administration Kit を使用することで、企業論理ネットワーク全域にわたるクライアントについて、ライセンスキー有効期限の監視と新規ライセンスキーのインストールを一元管理・実行できます。

Kaspersky Administration Kit を使用してライセンスキーをインストールすると、そのライセンスキーについての情報が管理サーバに保存されます。この情報は、ライセンス有効期限が間もなく終了する場合または許可された最大ユーザ数を超えた場合に、ライセンス適用状況に関するレポートの作成および管理者への通知に使用されます。ライセンスキーに関する通知のパラメータは、管理サーバ設定で編集できます。

論理ネットワーク内のクライアント PC にインストールされたライセンスキーのステータスについてのレポートを作成するには、組み込みテンプレート「**ライセンスキーレポート**」を使用するか、新しいタイプのテンプレートを同じ名前で作成します。

ライセンスキーレポートテンプレートを使って作成されたレポートには、現在のライセンスキーとバックアップ用ライセンスキー、ライセンスが使用されているコンピュータの表示、ライセンスの制約など、論理ネットワーク内のクライアント PC にインストールされたすべてのライセンスキーに関する完全な情報が含まれます。

クライアントにインストールされているライセンスキーの一覧は、[ライセンス] ノードに表示されます。各キーについて入手できるデータは、以下のとおりです：

- **シリアル番号** - ライセンスキーのシリアル番号
- **タイプ** - ライセンスキーの種類（例：商用、またはトライアル）
- **制約** - ライセンスキーに課されたライセンスの制約
- **ライセンス期間** - ライセンスキーの有効期限

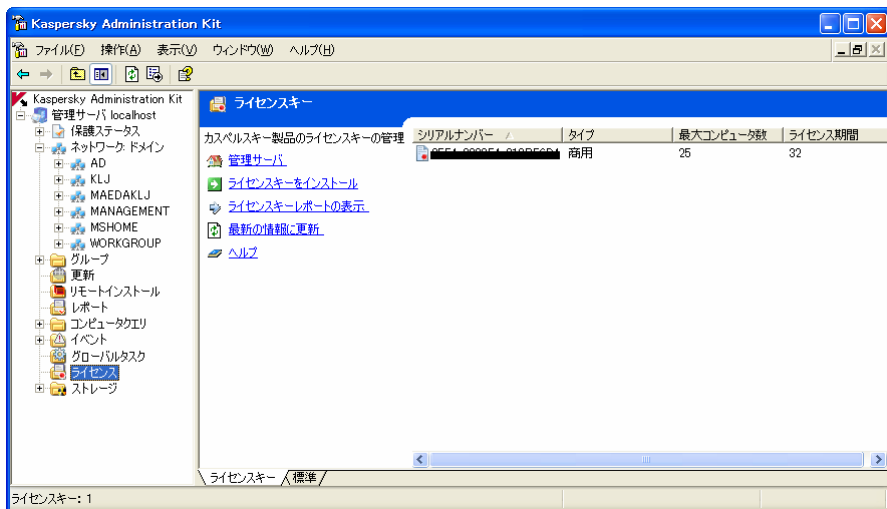


図 27. ライセンスキー

特定クライアントのアプリケーションに対して適用されているライセンスキーの情報を表示するには、アプリケーションのプロパティダイアログボックスを開きます。

ライセンスキーを適用するには、**ライセンスキーの適用**タスクを作成します。

ライセンスキーの適用タスクは、グループタスク、グローバルタスク、またはローカルタスクとして作成できます。ライセンスキーを適用するグローバルタスクは、ウィザードを使用して作成できます。

インストール済みのライセンスキーを置き換える場合、またはライセンスキーを現在のキーとしてインストールする場合は、以前に作成したタスクを使用前に設定変更して使用できます。

6.2. 隔離とバックアップストレージ

隔離とバックアップストレージを取り扱うことができるのは、Kaspersky Anti-Virus for Windows Workstation と Kaspersky Anti-Virus for Windows Servers バージョン 5.0 および 6.0 のみです。

アンチウイルス製品を使用して、疑わしいオブジェクトを特別なストレージに保存できます。各コンピュータには、隔離用フォルダとバックアップ保管用フォルダがローカルに備わっています。隔離用ストレージは、疑わしいオブジェクトの保管に使用されます。バックアップ用ストレージには、処理または削除される前の感染オブジェクトのバックアップコピーが保管されます。

Kaspersky Administration Kit には、カスペルスキー製品によってストレージに置かれたオブジェクトの集中管理型リストを維持する機能があります。この情報は、ネットワークエージェントによってクライアント PC から転送され、管理サーバの情報データベースに保管されます。管理コンソールを経由して、ストレージに置かれたオブジェクトのプロパティの表示、ストレージに対するアンチウイルススキャンの開始、ストレージ内のオブジェクトの削除、といった機能を実行することができます。

ローカルストレージ内のオブジェクトに対するリモート管理機能を有効にするには、ネットワークエージェントのポリシーで、[隔離オブジェクトの情報を管理サーバに転送する] ボックスと [バックアップストレージ内オブジェクトの情報を管理サーバに転送する] ボックスをオンにする必要があります (図 28 を参照)。

ストレージ設定は、各アプリケーションのポリシーまたはアプリケーション設定内で個別に定義されます。

[**ストレージ**] フォルダを使用して、論理ネットワーク内クライアント PC のストレージに置かれているオブジェクトの表示と管理を行うことができます (図 29 を参照)。

Kaspersky Administration Kit は、オブジェクトを管理サーバにコピーしません。すべてのオブジェクトは、クライアント PC のローカルストレージに置かれます。オブジェクトは、「管理コンソール」がインストールされているコンピュータの管理者によって指定されているフォルダに復元されます。

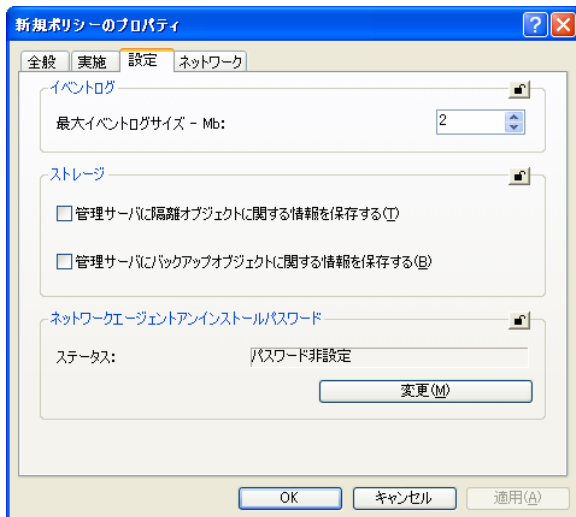


図 28. リモートストレージの構成

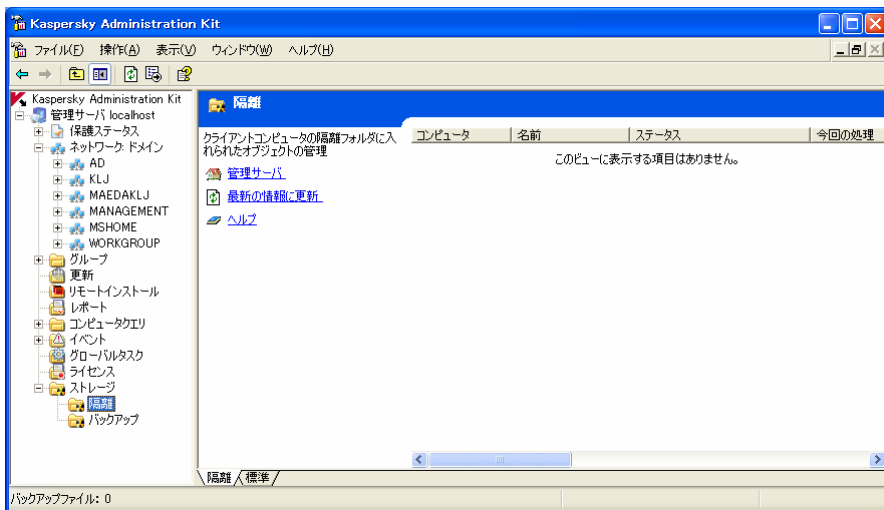


図 29. ストレージの内容の表示

6.3. イベントログとイベントフィルタ

Kaspersky Administration Kit は、アンチウイルス保護システムの動作を監視するさまざまなオプションを備えています。

管理サーバの動作および Kaspersky Administration Kit を使って管理されるすべてのアプリケーションの動作についてのイベントログを保持する機能があります。データは、Microsoft Windows のシステムログまたは Kaspersky Administration Kit のイベントログに保存されます。

ログには、アプリケーションの実行中に登録されたイベントおよびタスクの実行結果が記録されません。

各アプリケーションの実行中に記録されたイベントの一覧と、各管理グループの管理者およびその他ユーザに対するイベント通知手順を設定できます。これらのパラメータは、アプリケーショングループポリシーで決定されます。パラメータは、グループポリシー設定ウィンドウの [イベント] タブで指定します (図 30 を参照)。

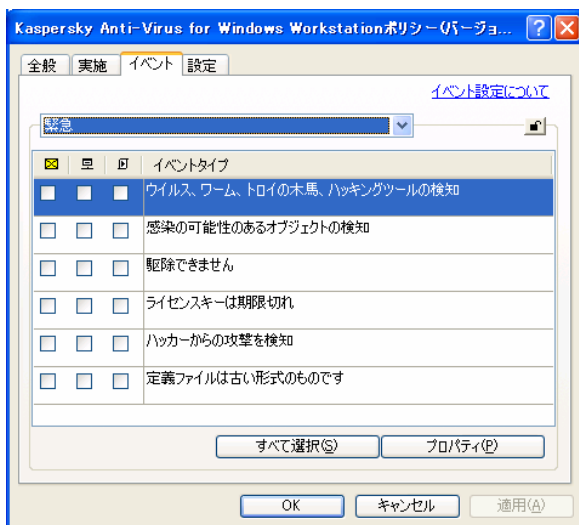


図 30. ポリシーの編集 - [イベント] タブ

タスクの実行結果の保存手順と、結果の通知形式および方法は、タスク設定で決定されます。

通知は、メールまたはネットワーク経由でのメッセージ送信、またはアプリケーションやスクリプトの起動によって行われます。

登録されたイベントおよびタスク実行結果についての情報は、管理サーバで一元的に保存されるか、各クライアント PC にローカル保存されます。

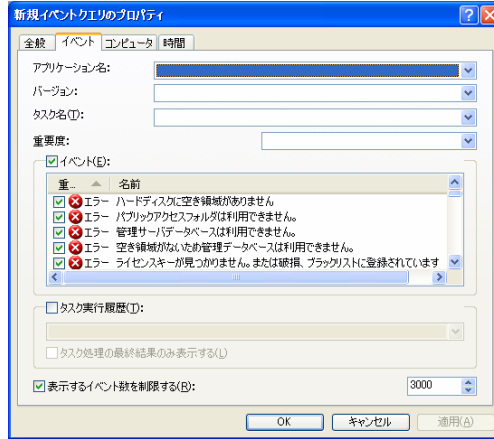


図 32. イベントフィルタの構成

登録されたイベントは、ポリシーによって指定された保存期間を過ぎると自動的に削除されます。ショートカットメニューの **[削除]** コマンドを使用して手動で削除することもできます。結果パネルで選択された個別のイベント、すべてのイベント、または特定の条件を満たすイベントを削除できます。

各クライアント PC に関してアプリケーション実行中に登録されたイベントの一覧を、プロパティウィンドウで確認できます（図 33 を参照）。ここでは、管理サーバに保管された Kaspersky Administration Kit イベントログの情報が表示されます。情報を検索するには、イベントフィルタを使用します。

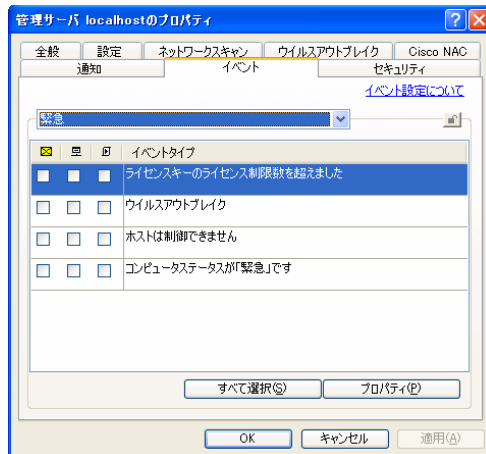


図 33. 管理サーバに保管されたイベントの表示

6.4. レポート

管理サーバに保存されている情報に基づいた現在のアンチウイルス保護システムのステータスについて、レポートを受信できます。

アンチウイルス保護のステータスは、管理エージェントによってシステムレジストリに書き込まれたデータを使用して、クライアント上でも追跡されます。

レポートの範囲は以下のとおりです：

- アンチウイルス保護システム全般
- 特定の管理グループに含まれているコンピュータ
- さまざまな管理グループ内にある一連のクライアント PC
- スレーブ管理サーバの論理ネットワークのアンチウイルス保護システム

作成できるレポートは以下のとおりです：

- **定義データベースバージョンレポート** - カスペルスキー製品が使用する定義データベースのバージョン情報が含まれます
- **エラーレポート** - クライアント PC にインストールされているアプリケーションの動作中に登録されたエラー（機能上の不具合）についての情報が含まれます
- **ライセンスレポート** - アプリケーションによって使用されているライセンスキーのステータスについての情報と、それらライセンスによって課される制約についての情報が含まれます
- **最も感染したクライアントレポート** - 疑わしいオブジェクトと感染しているオブジェクトの検知数が最も多いクライアント PC についての情報が含まれます
- **ウイルス保護レポート** - アンチウイルスの保護レベルが十分でないクライアント PC についての情報が含まれます
- **ソフトウェアバージョンレポート** - クライアント PC にインストールされているカスペルスキー製品のバージョンについての情報が含まれます
- **ウイルスアクティビティレポート** - 論理ネットワーク内クライアント PC のアンチウイルススキャン結果についての情報が含まれます
- **外部アプリケーションレポート** - クライアント PC にインストールされている、Kaspersky Administration Kit を通じた管理をサポートしていない外部アプリケーションまたはカスペルスキー製品についての情報が含まれます
- **ネットワーク攻撃レポート** - クライアント PC に登録されたネットワーク攻撃についての情報が含まれます
- **アプリケーションタイプのサマリレポート** - 論理ネットワークにインストールされているアンチウイルスアプリケーションのタイプ、それらアプリケーションによって検知された感染オブジェクトについての情報、実行された処理についての情報が含まれます
- **ワークステーションおよびファイルサーバ保護製品のサマリレポート** - ワークステーションおよびファイルサーバにインストールされているアンチウイルスアプリケーション

についての詳細情報、このアプリケーションによって検知された感染オブジェクトについての情報、関連の処理についての情報が含まれます

- **境界防御製品のサマリレポート** - インストールされているアンチウイルス境界防御アプリケーションについての詳細情報、このアプリケーションによって検知された感染オブジェクトについての情報、関連の処理についての情報が含まれます
- **メールシステム保護製品のサマリレポート** - インストールされているメールシステム保護アプリケーションについての詳細情報、このアプリケーションによって検知された感染オブジェクトについての情報、関連の処理についての情報が含まれます

前もって作成されているテンプレートに基づいて、レポートを作成できます。ほとんどのデフォルトテンプレートは、コンソールツリーの **[レポート]** の下にあります (図 34 を参照)。追加のレポートは、レポート ウィザードを使用して作成します。

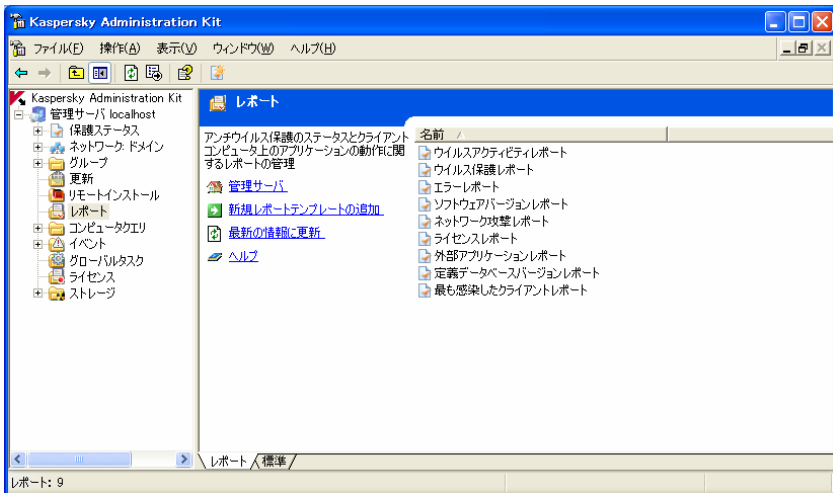


図 34. 管理サーバに保存されたタスク実行結果の表示

アンチウイルス保護ステータスのレポートには、それぞれに対応した 13 個の標準テンプレートがあります。

このほかに、新規テンプレートを作成、既存テンプレートを削除、テンプレートパラメータを表示および編集することができます。

レポートは、デフォルトのブラウザを使用して表示されます。

管理サーバの階層構造の場合は、スレーブ管理サーバの情報を含む全般的なレポートを作成できます。

一部の管理サーバが利用できない場合は、それについての情報がレポートに含まれます。

6.5. コンピュータの検索

特定のコンピュータまたはコンピュータのグループについての情報を受け取るには、指定の基準に基づいたコンピュータ検索機能を使用します。スレーブ管理サーバの情報は、検索で使用できません。検索結果は、テキストファイルに保存できます。

検索機能を利用して、以下のコンピュータを検索できます：

- 管理サーバおよびそのスレーブサーバの論理ネットワーク内にあるクライアント PC
- 論理ネットワークには含まれないが、管理サーバおよびそのスレーブサーバがインストールされているコンピュータネットワークの構造には含まれるコンピュータ
- 特定のコンピュータが論理ネットワーク構造に含まれるかどうかに関係なく、管理サーバおよびそのスレーブサーバがインストールされているネットワーク内部にあるすべてのコンピュータ

コンピュータの検索には、コンソールツリーで選択した管理サーバノード、[ネットワーク] フォルダ、または管理グループでショートカットメニューの [コンピュータを検索] コマンドを使用します（図 35 を参照）。

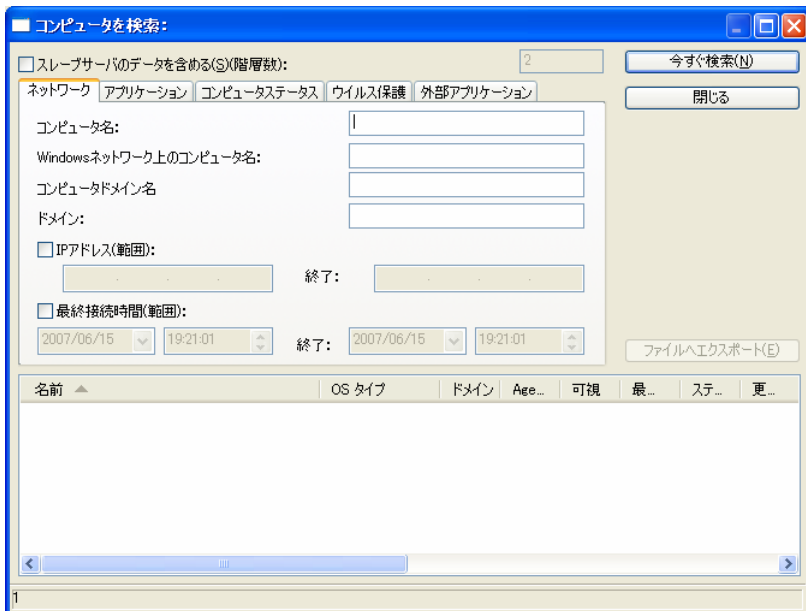


図 35. コンピュータの検索

検索を実行するノードによって、検索結果は以下ようになります：

- [グループ] グループ - 選択したグループが含まれる管理サーバ論理ネットワークに接続しているクライアント PC の検索

検索は、論理ネットワーク構造およびスレープ管理サーバのネットワーク（検索パラメータで **[スレープサーバのデータを含める]** ボックスがオンになっている場合）についての情報に基づいて実行されます

- **[ネットワーク]** グループ - 論理ネットワーク構造に含まれない管理サーバがインストールされているネットワーク内のコンピュータ

検索は、管理サーバおよびスレープサーバ（検索パラメータで **[スレープサーバのデータを含める]** ボックスがオンになっている場合）によるコンピュータネットワークのポーリングで得られたデータに基づいて実行されます

検索結果には、検索用に選択された **[ネットワーク]** グループおよびすべてのスレープサーバの **[ネットワーク]** グループ内（検索パラメータで **[スレープサーバのデータを含める]** ボックスがオンになっている場合）に含まれるクライアント PC が含まれます

- 管理サーバ <サーバ名> - コンピュータのフル検索。

検索は、論理ネットワーク構造についての情報と、選択した管理サーバおよびスレープサーバ（検索パラメータで **[スレープサーバのデータを含める]** ボックスがオンになっている場合）によるコンピュータネットワークのポーリングで得られたデータに基づいて実行されます

検索結果には、次の内容が含まれます：

- ◆ 選択した管理サーバおよびそのスレープサーバすべて（検索パラメータで **[スレープサーバのデータを含める]** ボックスがオンになっている場合）の論理ネットワークに含まれるクライアント PC
- ◆ 選択した管理サーバの **[ネットワーク]** グループおよびそのスレープサーバすべて（検索パラメータで **[スレープサーバのデータを含める]** ボックスがオンになっている場合）の **[ネットワーク]** グループに含まれるコンピュータ

コンソールツリーの別々のフォルダにあるコンピュータについて検索を実行し、情報を保存して表示するには、フィルタ作成機能を使用してください。

6.6. コンピュータフィルタ

論理ネットワーク内のクライアント PC のステータスをより柔軟に監視するために、**緊急**および**警告**ステータスのコンピュータについての情報およびネットワークで過去 24 時間に検知されたコンピュータについての情報が、コンソールツリー内の **[コンピュータタクエリ]** ノードに表示されます（図 36 を参照）。

クライアント PC のステータスは、コンピュータのアンチウイルス保護ステータスに関する情報と、ネットワーク内でのアクティビティに関する情報に基づいて診断されます。診断の設定パラメータは、各管理グループに対して **[コンピュータステータス]** タブで構成されます（図 37 を参照）。

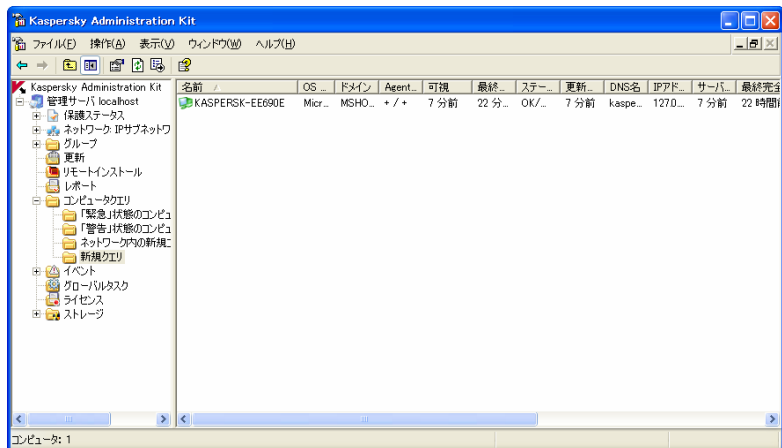


図 36. コンピュータの選択

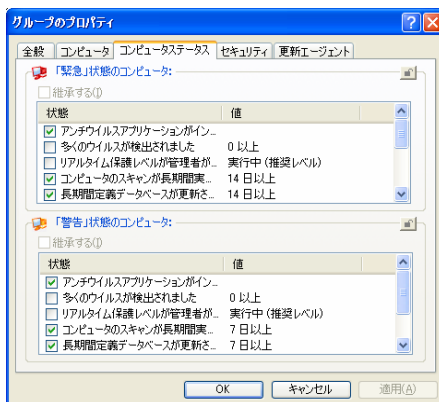


図 37. クライアント PC 診断の設定

新規コンピュータに関する情報は、管理サーバによるコンピュータネットワークのポーリング結果に基づいて提供されます。

追加フィルタを作成する機能があります。フィルタを作成するには、[コンピュータクエリ] ノードでショートカットメニューの [新規作成] → [新規クエリ] を使用します。フィルタ用に指定した名前が付いた新規フォルダが、コンソールツリーの [コンピュータクエリ] 内に表示されます。コンピュータを追加するには、フィルタパラメータを構成します (図 38 を参照)。選択内容は検索に使用可能であり、選択したコンピュータを管理グループ内へさらに移動できます。移動は、マウスを使って行います。

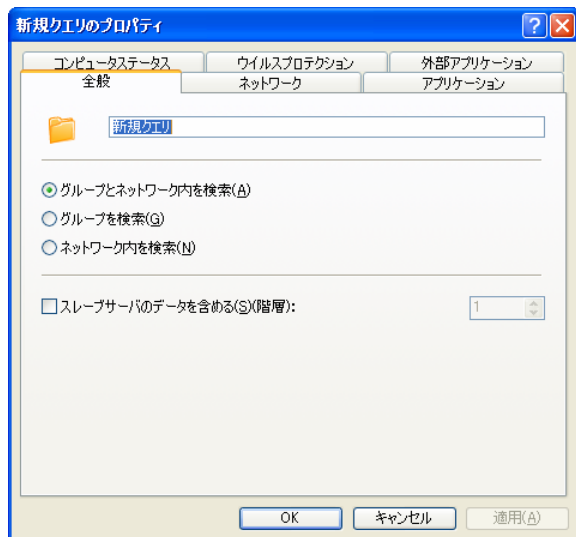


図 38. コンピュータフィルタの構成

6.7. アウトブレイクの監視

Kaspersky Administration Kit では、管理サーバコンポーネントの動作に登録されている**ウイルスアウトブレイク**イベントを使用して、論理ネットワーク内のクライアント PC でのウイルスアクティビティを監視できます。

この機能を有効に活用することで、アウトブレイク発生時の対応を円滑に行なうことができます。

ウイルスアウトブレイクイベントの登録に使用される基準は、管理サーバ設定の [**ウイルスアウトブレイク**] タブで構成されます (図 39 を参照)。

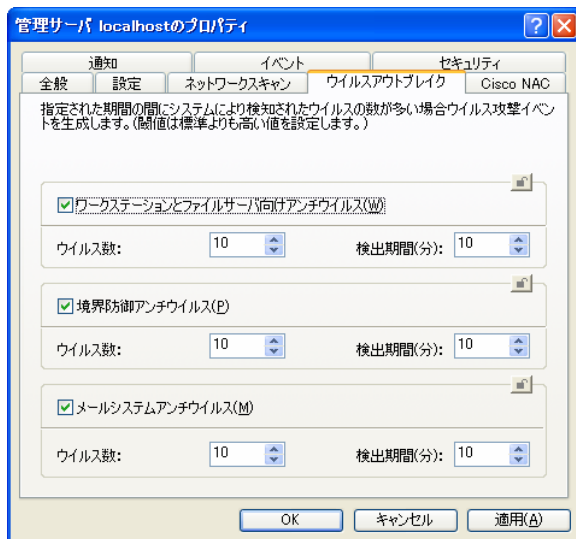


図 39. ウイルス攻撃検知設定の構成

いくつかのアプリケーションタイプについて 1 つのイベントを記録できます。ウイルス攻撃検知メカニズムを有効にするには、必要なアプリケーションタイプの横にあるチェックボックスをオンにします。

- ワークステーションとファイルサーバ向けアンチウイルス
- 境界防御アンチウイルス
- メールシステムアンチウイルス

各アプリケーションタイプについて、ウイルスアクティビティのしきい値を入力してください。しきい値を超えると、**ウイルスアウトブレイク**イベントが起動されます。

- **[ウイルス]** フィールド: このタイプのアプリケーションによって論理ネットワーク上で検知されるウイルスの数
- **検出期間 (分):** 上記数のウイルスが検知される期間

ウイルスアウトブレイクイベントは、**ウイルス検知**イベントと、アンチウイルスアプリケーションの操作における**ウイルス**、**ワーム**、**トロイ**、**ハッカーソフトウェア**の**検知**イベントに基づいて作成されるため、ウイルス発生を正しく検知するには、上記イベントについての情報がすべて管理サーバに保存されている必要があります。情報を保存するには、すべてのアンチウイルスアプリケーションのポリシーで対応するパラメータが適切に構成されている必要があります。つまり、**ウイルス検知**イベントと**ウイルス**、**ワーム**、**トロイ**、**ハッカーソフトウェア**の**検知**イベントのプロパティウィンドウの**[登録]**タブで**[管理サーバ上に保存 (日)]**がオンになっている必要があります (図 40 を参照)。

ウイルス攻撃イベントは、24 時間に 1 度しか作成できません。イベントをリセットするには管理サーバサービスを再起動する必要があります。

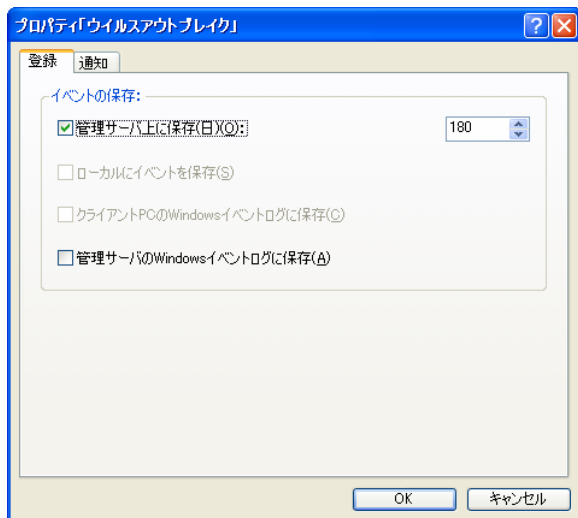


図 40. イベントログの構成

ウイルスアウトブレイクイベントの通知手順は、管理サーバプロパティの [イベント] タブで定義されます (図 41 を参照)。

アウトブレイク対応として、ポリシーのセットを状況に基づいて自動変更する事ができます。設定には、ポリシー設定と**ウイルスアウトブレイクイベント**で [イベントによりポリシーをアクティブ化する] ボックスを有効にします (図 12 を参照)。

ウイルス検知イベントとウイルス、ワーム、トロイ、ハッカーソフトウェアの検知イベントの数をカウントするために、メイン管理サーバのクライアント PC の情報だけを取得するようにしてください。

各スレーブサーバのウイルス検知イベントは、個別に設定します。

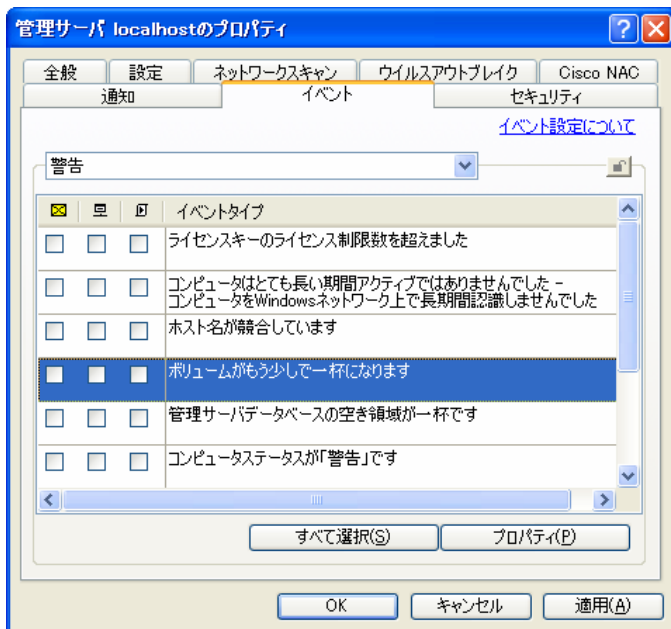


図 41. イベント通知設定の構成

6.8. 管理サーバデータのコピーと復元

バックアップをとることによって、情報を失うことなく管理サーバをコンピュータ間で移動することができ、管理サーバの情報データベースを別のコンピュータに移動する場合または新規バージョンの Kaspersky Administration Kit を更新する場合にデータを復元できます。

管理サーバがコンピュータから削除されるたびに、Kaspersky Administration Kit はバックアップの作成を提案します。

バックアップの作成時に以下のデータが保存または復元されます：

- 管理サーバ情報データベース（管理サーバに保存されているポリシー、タスク、アプリケーション設定、イベント）
- 論理ネットワークとクライアント PC の構造についての構成情報
- アプリケーション導入パッケージのストレージ（[Packages]、[Uninstall]、[Updates] フォルダのコンテンツ）
- 管理サーバ証明書

新規アプリケーションバージョンへのアップグレード時のデータの復元は、Kaspersky Administration Kit バージョン 5.0 MP3 からサポートされています。

データの復元中にパブリックフォルダへのパスが変更された場合は、共有フォルダに関わるタスク（更新タスク、導入タスク）が正しく実行しているかどうかを確認し、必要なら設定を変更してください。現在使用されている言語以外の復元はできません。

バックアップストレージ用の管理サーバデータのコピーおよび以降の復元は、バックアップコピーのタスクを使用して自動的に行うか、Kaspersky Administration Kit の配布パッケージに含まれている **klbackup** ユーティリティを使用して手動で行うことができます。データの復元は、**klbackup** ユーティリティを使用して行われます。

管理サーバのインストール後、**klbackup** ユーティリティはコンポーネントインストールフォルダに保存され、コマンドラインから実行された時にデータを（修飾子に応じて）コピーまたは復元します。

バックアップタスクは手動で作成され、[グローバルタスク] ノードに「管理サーバ データバックアップ」という名前で保存されます。バックアップの作成を有効にするには、このタスクの設定を構成する必要があります。手動でデータバックアップのタスクを作成することもできます。タスク作成対象アプリケーションとして [Kaspersky Administration Kit]、タスクのタイプとして [管理サーバによる更新の受信] を選択します。

付録A. 用語解説

この文書で使用されるアンチウイルス関連の用語集です。便宜上、用語は 50 音順に並んでいます。

英数字、記号

IChecker™ テクノロジー - 前回のスキャン以来変更のないオブジェクトを今後のスキャンから除外するテクノロジー。オブジェクトチェックサムデータベースの使用によって実装されました。

IStreams™ テクノロジー - 前回のスキャン以来変更のない、NTFS 形式ディスクに保管されたファイルをスキャンから除外するテクノロジー。ファイルチェックサムを NTFS 代替データストリーム上に保管することで実装されました。

Kaspersky Administration Kit - 重要な管理作業を一元管理するためのアプリケーション。カスペルスキー製品に基づいて企業のアンチウイルスポリシーを全面的に管理できます。

あ

アプリケーションの一元管理 - Kaspersky Administration Kit を使用してアプリケーションを管理すること。

アンチウイルス保護ステータス - コンピュータのセキュリティレベルを特徴付ける、アンチウイルスの現在のステータス。

インストールパッケージ - 論理ネットワーク上のリモートホストにカスペルスキー製品をインストールする場合に使用するファイルパッケージ。インストールパッケージは、アプリケーション配布キットに含まれる .kpd ファイルに基づいて作成されます。このファイルには、アプリケーションの基本機能をインストール後すぐ利用するために必要な最低限のパラメータセットが含まれています。パラメータ値は、アプリケーションのデフォルト設定です。

ウイルスアクティビティのしきい値 - 指定期間中に検知されるウイルスの数。この数を超えると、**ウイルスアウトブレイク**（ウイルス攻撃）とみなされます。このパラメータは、ウイルスの流行を検知し、新しい脅威にタイムリーに対応して予防措置をとるために重要です。

疑わしいオブジェクト - 既知のウイルスコードの変種または定義データベースに登録されていないウイルスらしきコードを含むオブジェクト。

オブジェクトの削除 - オブジェクト処理方法のひとつ。コンピュータからオブジェクトを物理的に削除することです。感染オブジェクトを処理する場合の推奨方法です。オブジェクトに適用される最初の操作が削除である場合は、削除前にバックアップを作成しておく必要があります。このバックアップを使用して、元のオブジェクトを復元できます。

オブジェクトのブロック - オブジェクトに対する外部アプリケーションのアクセスを遮断すること。ブロックされたオブジェクトの読み取り、実行、変更、削除はできません。

オンデマンドフルスキャン - ウイルスがないかどうかコンピュータ上のすべてのファイルのスキャンし、検知された感染オブジェクトの駆除または削除を行う、管理者定義のモード。

か

外部アプリケーション - サードパーティベンダのアンチウイルス製品、または Kaspersky Administration Kit 経由の管理に対応していないカスペルスキー製品。

拡張 OLE - OLE 技術を使用して別のファイルに埋め込まれたオブジェクト。

隔離 - 疑わしいオブジェクトを処理する方法のひとつ。オブジェクトへのアクセスはブロックされ、隔離フォルダに移動されます。

隔離フォルダ - 感染オブジェクトおよび疑わしいオブジェクトを隔離しておくための特別なストレージ。

カスペルスキーのアップデートサーバ - 更新のダウンロード元となる、カスペルスキーの http サイトおよび ftp サイト。

仮想ドライブ (RAM ドライブ) - コンピュータの物理ドライブをエミュレートする RAM 領域。

感染オブジェクト - ウイルスを含むオブジェクト。コンピュータが感染するおそれがあるため、こうしたオブジェクトは使用しないでください。

管理グループ - 機能別またはインストールされているカスペルスキー製品別にグループ分けされたコンピュータ。グループ化によって管理プロセスが大幅に簡素化され、すべてのコンピュータを 1 つのユニットとして管理できるようになります。グループ内には別のグループを含めることができます。グループのメンバにインストールされているアプリケーションに対し、グループポリシーやグループタスクを作成できます。

管理コンソール - 管理サーバおよびネットワークエージェントの管理サービス用にユーザーインターフェイスを提供する、Kaspersky Administration Kit のコンポーネント。

管理サーバ - Kaspersky Administration Kit のコンポーネント。クライアントにインストールされているカスペルスキー製品の情報の保管とこれら製品の管理を一元的に行います。

管理サーバ証明書 - 管理コンソールが管理サーバに接続する場合や、サーバとクライアントの間でデータを転送する場合の管理サーバ認証に使用される証明書。管理サーバ証明書は、管理サーバのインストール時に作成されます。インストールフォルダの [Cert] フォルダ内に置かれています。

駆除 - 感染オブジェクトの処理方法のひとつ。駆除とは、データの一部またはすべてを復元することを指します。駆除不可能であるとの結論に至ることもあります。オブジェクトの感染駆除は、定義データベースを使用して行われます。疑わしいオブジェクトに適用される最初の操作が駆除である場合は、そのオブジェクトのバックアップが作成されます。駆除処理中に一部のデータが失われても、バックアップを使用してオブジェクトを復元できます。

クライアント、管理サーバ (またはクライアント PC) - ネットワークエージェントがインストールされ、管理対象カスペルスキー製品が導入されているコンピュータ、サーバまたはワークステーション。

グループタスク - グループ内にあるすべてのクライアントに対して実行されるタスク。

グループポリシー - Kaspersky Administration Kit を通じて適用する、グループ向けの設定セット。グループポリシーはグループごとに異なっていてもかまいません。グループポリシーは、アプリケーションごとに固有です。ポリシーは、アプリケーションのすべてのパラメータ設定とかかわっています。

グローバルタスク - 異なるグループに属する複数のクライアントに対して実行されるタスク。

現在のライセンスキー - カスペルスキー製品にインストールされており、カスペルスキー製品の動作に現在使用されているライセンスキー。ライセンス有効期間と製品のライセンスポリシーを規定します。

更新 - カスペルスキーのアップデートサーバから取得した新規ファイル（定義データベースまたはプログラムモジュール）を追加/更新する機能。

更新エージェント - 管理グループ内で更新およびインストールパッケージを配布するための中継センターとして機能するコンピュータ。

高レベル - 保護レベルのひとつ。総合的な保護を行います。パフォーマンスが若干低下します。

コンソール（管理）プラグイン - 管理コンソールを通じてアプリケーションをリモート管理するためのインターフェイスを備えた特別なコンポーネント。プラグインはアプリケーションごとに固有であり、Kaspersky Administration Kit を通じて管理できるカスペルスキー製品に含まれています。

さ

重要度 - Kaspersky Anti-Virus によって記録されたイベントを分類するパラメータ。4 つのレベルに分かれています：

緊急

エラー

警告

情報

同じ種類のイベントでも、状況によって重要度が異なる場合があります。

除外 - 特定のオブジェクトをスキャンから除外する、ユーザ定義の設定。リアルタイム保護とオンデマンドスキャンの除外ルールはカスタマイズ可能であるため、完全スキャンの際にアーカイブをスキャンしないようにしたり、マスクを使ってファイルをスキャンから除外したりできます。

推奨レベル - コンピュータの最適な保護を保証する、カスペルスキーの専門家が推奨するデフォルト設定のアンチウイルス保護レベル。このレベルはデフォルトで設定されます。

スタートアップオブジェクト - オペレーティングシステムやその他ソフトウェアの起動とスムーズな操作に欠かせない一連のプログラム。スタートアップのたびに、これらのオブジェクトが起動される。一部のウイルスはスタートアップオブジェクトに感染を試み、スタートアップの不具合を生じさせる。

設定、アプリケーション - このアプリケーションが実行する各種タスクに固有のアプリケーション設定。

設定、タスク - 各種タスクに固有のアプリケーション設定。

速度重視 - 保護レベルのひとつ。処理速度は最も速くなりますが、セキュリティレベルは若干低下します。

た

タスク - カスペルスキー製品が実行する動作。

定義データベース - カスペルスキーの専門家によって作成されたデータベース。既存ウイルスの詳細な情報やそれらの検知および駆除に関するデータが含まれています。アンチ

ウイルス製品は、このデータベースを使用してウイルスの検知や駆除を行います。定義データベースはカスペルスキーの Web サイトからダウンロード可能であり、新種ウイルスの発生を受けて定期的に更新されています。カスペルスキー製品の登録済みユーザであれば、更新にアクセス可能です。コンピュータをウイルスから常に保護するため、更新を定期的にダウンロードすることを強くお勧めします。

適用可能な更新 - 蓄積された緊急の更新とアプリケーション構造に対する最新の変更を含むサービスパック。

な

ネットワークエージェント - Kaspersky Administration Kit のコンポーネント。特定のネットワークノード（ワークステーションまたはサーバ）にインストールされた管理サーバとカスペルスキー製品との間で通信を提供します。Kaspersky Lab Business Optimal および Kaspersky Corporate Suite に含まれるすべての Windows アプリケーションに共通です。

は

バックアップ - 管理サーバのデータを、保管しておいて後で復元できるようにコピーすること。バックアップ用ユーティリティを使用して、以下の内容を保存できます：

ポリシー、タスク、アプリケーション設定、イベントが保管されている管理サーバ情報データベース

論理ネットワークに関する情報、アプリケーション

リモートインストール用のクライアント設定ファイル ([Packages]、[Uninstall]、[Updates] フォルダのコンテンツ) に関する情報

管理サーバ証明書

バックアップキー - カスペルスキー製品にインストールされたライセンスキーのうち、現行のキーとして登録されていないもの。現行ライセンスの有効期限が切れると自動的に現行のキーとして登録されます。

バックアップストレージ - バックアップユーティリティによって作成された管理サーバデータのバックアップが保管されるフォルダ。

バックアップフォルダ - 削除または駆除されたオブジェクトのバックアップが保管されるディレクトリ。

復元 - バックアップユーティリティを使用した管理サーバデータの復元。データはバックアップストレージから復元されます。バックアップ用ユーティリティを使用して、以下の内容を復元できます：

ポリシー、タスク、アプリケーション設定、イベントが保管されている管理サーバ情報データベース

論理ネットワークに関する情報、アプリケーション

リモートインストール用のクライアント設定ファイル ([Packages]、[Uninstall]、[Updates] フォルダのコンテンツ) に関する情報

管理サーバ証明書

プッシュインストール - カスペルスキー製品のリモートインストール方法のひとつ。論理ネットワークの特定のクライアント PC でリモートインストールを実行できます。プッシュインストールタスクを正常に行うには、タスクの実行に使用されるアカウントが、論理ネット

ワークのクライアント PC 上でアプリケーションをリモート起動する権限を持っている必要があります。この機能をサポートする Microsoft Windows 2000/2003/XP コンピュータ、またはネットワークエージェントがインストールされている Microsoft Windows 98/Me コンピュータでの推奨方法です。

プログラムとドキュメント (拡張子で判断する) - このスキャンモードでは、スキャン対象となるファイルが拡張子によって判断されます。

プログラムとドキュメント (ファイル種別で判断する) - このスキャンモードではファイルの内容、つまりファイルヘッダの形式識別子によってスキャン対象ファイルが判断されます。

ポリシー - 「グループポリシー」を参照。

ま

未知のウイルス - 定義データベースに登録されていない新種のウイルス。通常 Kaspersky Anti-Virus では、未知のウイルスはヒューリスティックコードアナライザを使用して検知され、そうしたウイルスを含むオブジェクトは疑わしいオブジェクトとして識別されます。

メールアドレスデータベース - コンピュータに保管されているメールのデータベース。オンデマンドスキャンの対象。

ら

ライセンスキー - 個人用キーとして機能する、拡張子 .key を持つファイル。カスペルスキー製品を正しく動作させるには、このファイルが必要です。製品をカスペルスキーの代理店から購入した場合、ライセンスキーは配布キットに含まれます。製品をオンラインで購入した場合、ライセンスキーはメールで送信されます。ライセンスキーを登録しないと、カスペルスキー製品は機能しません。

ライセンス期間 - カスペルスキー製品のフル機能を利用できる期間。一般に、ライセンスキーによって規定されるライセンス期間は購入日から 1 年間です。ライセンスの期限が切れると、アプリケーションの利用はできますが定義データベースの更新はできません。

リアルタイム保護 - アンチウイルス製品がメモリに常駐するスキャンモード。このモードでは、読み取り、書き込みまたは実行の際にオブジェクトのスキャンが行われます。オブジェクトへのアクセスを有効にする前にウイルススキャンが行われ、ウイルスが検知された場合には、ユーザ定義の設定に基づいてアクセスのブロック、オブジェクトの感染駆除または削除が行われます。

リモートインストール - Kaspersky Administration Kit を使用したカスペルスキー製品のインストール。

ローカル管理 - ローカルインターフェイスを通じたアプリケーション管理。

ローカルタスク - 1 つのクライアントを対象として作成および実行されるタスク。

ログインスクリプトベースのインストール - カスペルスキー製品のリモートインストール方法のひとつ。特定のユーザアカウントまたは複数のユーザアカウントにリモートインストールタスクを割り当てることができます。ドメインにユーザが登録されると、ユーザが登録されているコンピュータからクライアント PC に対してアプリケーションのインストールが試みられます。MS Windows 95/98/Me が動作するコンピュータでの推奨方法です。

論理ネットワークオペレータ - Kaspersky Administration Kit によって管理されるアンチウイルスシステムを監視するユーザ。

論理ネットワーク管理者 - Kaspersky Administration Kit のインストール、設定およびメンテナンスを行い、論理ネットワークコンピュータにインストールされているカスペルスキー製品をリモート管理するユーザ。

付録B. KASPERSKY LAB

1997年の創始以来、Kaspersky Lab は、情報セキュリティ技術界のリーダーとして知られ、リスクウェアやスパム、ハッカー攻撃等の脅威からコンピュータとネットワークを保護する、高性能かつ包括的な情報セキュリティソリューションを開発・提供しています。

Kaspersky Lab は本社ロシアをはじめ日、中、韓、米、英、仏、独、ポーランド、ルーマニア、ベネ룩クス3国に支社を構える国際企業で、世界各国500以上の企業とのパートナーネットワークがあります。仏にはヨーロッパアンチウイルスリサーチセンタの新部門も設立されました。

現在 Kaspersky Lab は500名以上の高度専門家を抱え、うち10名がMBAを、16名が博士号を取得し、コンピュータアンチウイルスリサーチチャーズ機構(CARO)のメンバーも在籍しています。

14年余にわたるウイルス対策でスタッフが培った知識と経験が Kaspersky Lab の最大の財産となり、ウイルスの動向をも予知し、現在はもちろん、一歩先行くセキュリティ製品と12サービスを提供し続けています。

世界最高水準を自負する弊社の主力製品は、クライアントPCを始め、ファイルサーバやメールサーバ、ファイアウォール、ポケットPCを様々なネットワーク上の脅威から保護します。また柔軟な一元管理ツールを備えることにより、企業のネットワークにも万全なセキュリティを提供します。標準製品以外でもF-Secure(フィンランド)やBorderWare(加)、Blue Coat(米)、Check Point(米)、LANDesk(米)、CLEARSWIFT(英)、CommuniGate(米)、Juniper(米)、Sybari(米)、G Data(独)、Microworld(印)といった、世界のトップセキュリティベンダの製品にKaspersky Labのアンチウイルスエンジンが採用されているという事実も技術力の水準を雄弁に物語っています。国内でもエンジンの性能が評価され、@niftyのSaaSサービスやTurboLinux OS、imatrix社が提供するスパム対策アプライアンス、HDE社のLinux向けアンチウイルスソリューション、Ahkun社のWindows®向けマルウェア対策製品他に採用されています。

Kaspersky Lab 製品のユーザ様は、安定動作はもちろん、設計から開発、サポートまで、さまざまな要件に応える高度サービスを受受いただけます。ウイルス対策の要となるウイルス定義データベースは約1時間に1回という高頻度で更新され、24時間体制で多言語でのサポートを提供しています。

B.1. 製品ラインナップ

Kaspersky® OnLine Scanner

Kaspersky® OnLine-Scanner は、Kaspersky 製品をオンラインで体験いただける無償のウイルス・スパイウェア検知ツールです。すでに他社製品を導入済みでも、Microsoft® Internet Explorer を利用して、手軽に悪意あるソフトウェアの有無をチェックすることができます。スキャン時には、次のオプションを設定することもできます：

○ スキャン領域の選択

- 重要な領域 -%windir% と %tmp% システム変数で特定されるハードディスクの重要な領域をスキャンします
- メモリー 実行プロセスのディスクモジュールをスキャン

- マイコンピュータ - すべてのローカルハードディスクとマッピングされたディスクのスキャン
 - メールファイル - *.PST, *.MSG, *.OST, *.MDB, *.DBX, *.EML, *.MBS 形式のメールデータベースのスキャン
 - フォルダ - 任意のフォルダのスキャン
 - ファイル - 任意のファイルのスキャン
- スキャン設定オプション
- 圧縮ファイルおよび E メールデータベースをスキャン対象から除外または含める
 - スキャンの定義データベースを「標準」/「拡張」から選択
 - スキャン結果のレポートを.txt または.html 形式で保存

Kaspersky® Anti-Virus 7.0

Kaspersky® Anti-Virus 7.0 は、最新のプロアクティブ技術を採用しつつ、従来のアンチウイルス機能を保持した、最適なアンチウイルス製品です。

このプログラムは、以下の複合的なウイルススキャン機能を備えています：

- メールの送受信で使用される通信方式(POP3、SMTP、IMAP、MAPI、NNTP)を利用してメールの送受信を監視
- HTTP プロトコル経由のインターネット通信をリアルタイムスキャン
- 個人のファイルやフォルダ、ドライバのスキャンに加え、Microsoft Windows のスタートアップオブジェクトや OS の重要な領域を重点的にスキャンするタスクをプリセット

プロアクティブディフェンスには、次のような特徴があります：

- **ファイルシステムの改ざんを監視** - ユーザは各コンポーネントで管理するアプリケーションのリストを作成することができます
- **RAMプロセスの監視** - Kaspersky® Anti-Virus Mobile は、危険なプロセスや疑わしい動作、隠しプロセス、権限のない変更を検知すると、瞬時にユーザに通知します
- **OS レジストリ変更の監視** - 内部のシステムレジストリを管理します
- **隠しプロセスの監視** - ルートキット技術を用いた OS 内部に隠された悪意あるコードから保護します
- **ヒューリスティック分析** - プログラムによるファイルの開封、書込みなどのすべての疑わしい動作を仮想環境下でエミュレートし、悪意のあるプログラムであるかを判定します
- **システムリカバリ** - 悪意あるプログラムによる攻撃後、コンピュータのファイルシステムのレジストリへの変更をユーザの意思でロールバックさせることができます

Kaspersky® Internet Security 7.0

Kaspersky® Internet Security 7.0 はKaspersky® Anti-Virus 7.0 のアンチウイルスモジュールに、IPSとIDSに対応するパーソナルファイアウォールと迷惑メール対策を統合した総合セキュリティ製品です。ウイルスやスパイウェアを含むマルウェア、不正侵入、情報流出、迷惑メールなど

のネットワーク上の脅威から、コンピュータに保存されたデータを保護します。包括的インターフェイスで、プログラムのすべてのコンポーネントを設定・管理することができます。

Kaspersky Anti-Virus の機能に加え、Internet Security には、以下の機能が搭載されています：

- **プライバシーコントロール** - フィッシングサイトからの攻撃を監視し、機密データ(すべてのパスワード、銀行の口座番号やクレジットカード番号など)の漏洩を防ぎます。また、web 上のページで危険なスクリプトが実行されるのをブロックして、不要なポップアップウィンドウやバナー広告を遮断します。
- **アンチダイアラー** - モデムを利用して無断で海外の番号などへ繋いで有料のサービスを利用することを防止します。プライバシーコントロールモジュールは、権限のないアクセスやデータ送信などによる個人情報や機密データの漏洩を防ぎます。
- **ペアレンタルコントロール** - 不適切な内容を含む web サイトの閲覧制限をかけることができます。また、インターネットの接続時間を制限することで、ネット利用時間も管理することが可能です。
- **ファイアウォール** - IPS/IDS 機能をもつ、パーソナルファイアウォール。PC への不正侵入を遮断したり、情報流出を防ぎます。ネットワーク接続を行うソフトウェア向けのルールがあらかじめ設定されているほか、学習機能も搭載されています。

また、迷惑メール対策モジュールである、アンチスパムが統合されています。受信メールのメッセージをフィルタリングする包括的なアンチスパムは次の手法を用いてスパム判定を行います：

- 受信者が手動で作成したブラックリスト/ホワイトリストと照合(フィッシングサイトの URL を含みます)
- メール本文に貼り付けられた画像中の文字情報を分析
- 学習アルゴリズムを用いたメッセージ本文の分析

Kaspersky® Anti-Virus Mobile

Kaspersky® Anti-Virus Mobile は、Symbian OS および Microsoft Windows Mobile が動作するモバイルデバイスに対してアンチウイルス保護を提供します。このプログラムは、次のような包括的なウイルス対策機能を備えています：

- **オンデマンドスキャン** - モバイルデバイスに搭載されたメモリ、メモリカード、個別のフォルダ、または特定ファイルをスキャンします。感染ファイルが検知された場合、ファイルは隔離フォルダに移動されるか削除されます
- **リアルタイムスキャン** - 送受信されるファイルはすべて自動的にスキャンされます。同様に、ファイルアクセスが試みられた場合もスキャンが行われます
- **テキストメッセージスパムからの保護**

Kaspersky Anti-Virus for File Servers

このソフトウェアパッケージは、Microsoft Windows や Linux、Samba が動作するサーバ上のファイルシステムを、すべてのタイプのマルウェアから保護します。Kaspersky® Anti-Virus for File Server は、以下の製品群で構成されています：

- **Kaspersky® Administration Kit**

- **Kaspersky® Anti-Virus for Windows Server**
- **Kaspersky® Anti-Virus for Linux File Server**
- **Kaspersky® Anti-Virus for Samba Server**

Kaspersky® Open Space Security

企業ネットワーク内の各レイヤを“Space”という概念でグループ化し、ネットワークの構成や企業規模に応じたセキュリティを提供するソリューションです。モバイルデバイスからサーバまでのすべての企業ネットワークエンドポイントをトータルに保護します。メールやウェブトラフィック、ネットワーク通信と言ったデータトラフィックをマルウェアの脅威から保護します。モバイル PC にもネットワーク上の PC 同様の保護が提供され、パワフルな管理ツールによって徹底した管理が行えます。

Kaspersky® Open Space Security は、以下の製品群で構成されます：

- **Kaspersky® Work Space Security** – ノートPCを含むオフィスのワークステーションを一元管理下に置いて運営する、必要最小限のセキュリティスペースです。オフィスのワークステーションをウイルスやスパイウェア、ハッカー攻撃※、迷惑メール※の脅威から守ります。

※ Windows プラットフォームのみ

- **Kaspersky® Business Space Security** – ワークステーションおよびファイルサーバをウイルスやスパイウェア、トロイの木馬、ワーム等のマルウェアの脅威から守り、万が一の感染時にも拡大を防ぎます。ネットワーク上の重要データの保護に最適です
- **Kaspersky® Enterprise Space Security** – ワークステーション、ファイルサーバおよびメールサーバをインターネット上の脅威から守り、円滑なデータのやり取りはもちろん、安全なインターネットを提供します
- **Kaspersky® Total Space Security** – ワークステーションからファイルおよびメールサーバ、ゲートウェイ、迷惑メール対策までの企業ネットワークのすべてのレイヤをトータルに保護します

Kaspersky Mail & Gateway Security

Kaspersky® Mail & Gateway Security は、インターネットに接続するすべての従業員に安全な通信環境を提供します。HTTP/FTPプロトコルで転送されてくるデータのマルウェアとリスクウェアを自動的に削除します。

Kaspersky® Mail & Gateway Security は、以下の製品群で構成されます：

- **Kaspersky® Administration Kit**
- **Kaspersky® Mail Gateway (※Anti-Virus のみ)**
- **Kaspersky® Anti-Virus for Proxy Server**
- **Kaspersky® Anti-Virus for Linux Mail Server**

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam は、大量の未承諾メール（スパム）に対抗することを目的とした、企業向けのソリューションです。言語解析テクノロジーと最先端のメールフィルタリング機能（DNS ブラックリスト機能やホワイトリスト機能）を組み合わせることで、不要なトラフィックの最大 95% を識別して一掃します。

ネットワークの入り口に導入することで、受信メールを監視してスパムと認識されるオブジェクトを遮断・処理することができます。任意のメールシステムとの互換性を考慮し、既存のメールサーバにも専用メールサーバにもインストールすることができます。

高度なスパムメールの認識精度は、カスペルスキーの言語研究所によって毎日約 20 分間隔で更新されるフィルタリングデータベースによって実現されています。

Kaspersky® Second Opinion Solution (SOS)

Kaspersky® Second Opinion Solution は、すでに他社アンチウイルス製品が導入されている環境に、セカンドオピニオンとして利用するためのアプリケーションです。他社のアンチウイルス製品を使用している場合でも、競合を起こすことなく共存できるので、セキュリティ対策の多重化をはかることができ、高いウイルス検知率と最速の定義ファイル更新の Kaspersky が、パソコンのセキュリティをより強固にします。

Kaspersky® Anti-Virus for Windows Server Enterprise Edition

Kaspersky® Anti-Virus for Windows Server Enterprise Edition は、x64 バージョンを含む Windows ファイルサーバ上のデータをすべてのマルウェアの脅威から守ります。この製品は、負荷の高くなりがちな企業のオフィス用サーバで特に高いパフォーマンスを発揮するように設計されています。

このプログラムには、以下の特徴があります：

高性能を誇るパフォーマンス

- **スケーラビリティ** - マルチプロセッサ環境では、管理者はサーバアンチウイルスタスクに適用するプロセッサを指定することができます
- **負荷の分散** - アンチウイルスタスク中に、よりプライオリティが高いタスクが実行された場合に、サーバリソースの再分配を行うことができます。また、スキャンをバックグラウンドモードに切り替えることもできます
- **最適化スキャン** - iSwift と iChecker の二つのテクノロジーを搭載し、スキャンに要する時間を大幅に削減します。初回スキャン時のみすべてのファイルがスキャンされ、2 回目以降は新規に作成および編集されたファイルのみを対象とします
- **信頼するプロセスの選択** - データのバックアップやデフラグメンテーションのようなリソースを消費するプロセスを「信頼するプロセス」に登録することでスキャン対象から除外することができます

柔軟な管理ツール

- **一元管理ツール** - Kaspersky Administration Kit からプログラムのインストール、設定の変更やアプリケーションの管理などの操作を複数台のサーバに対して一度に行うことができます
- **柔軟な管理オプション** - リモート管理を含む Microsoft 管理コンソール、Kaspersky Administration Kit、またはコマンドラインからの管理が可能です。
- **自動更新** - 定義データベースおよびモジュールは、設定したスケジュールに則って自動処理されます。手動での更新にも対応し、更新ファイルの取得元もインターネット経由やローカルフォルダを指定できます。また、更新ファイルのダウンロードには最も負荷の低いサーバが自動的に選択されます
- **柔軟なスキャン時間設定** - 管理者はオンデマンドスキャンのスケジュールを設定することで、サーバリソースを必要とする平日の日中等に、ユーザにストレスを与えずにセキュアな環境を維持することができます。
- **レポート機能** - システム管理者は、Microsoft Windows や Kaspersky Administration Kit のイベントログを参照したレポートを利用してアプリケーションを管理することができます。このレポートシステムでは、膨大なログの中から必要な情報を簡単に見つけ出すことが可能です
- **ステータス情報** - 管理者は、SNMP プロトコルや MOM のサポートする E メールや NetSend によって、製品のイベントに関する豊富な情報を入手することができます。

* Kaspersky はロシア Kaspersky Lab の登録商標または商標です

* その他、記載されている会社名、製品名は、各社の登録商標または商標です。

B.2. お問い合わせ先

ご意見やご質問がありましたら、カスペルスキーラプス または弊社ディストリビュータまでご連絡ください。お電話またはメールにてお問い合わせいただけます。お客様からのご意見やご提案をお待ちしております。

住所:	東京都千代田区東神田2-3-3 東神田藤和ビル6F
TEL:	03-5687-7839
メールサポート	support@kaspersky.co.jp
WWW:	http://www.kaspersky.co.jp http://www.viruslistjp.com