

KASPERSKY LABS JAPAN

Kaspersky[®] Administration Kit ver. 6.0

導入ガイド



© Kaspersky Labs Japan

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

2008年1月

目次

1 KASPERSKY ADMINISTRATION KIT	4
1.1. 目的、構造、主な機能.....	4
1.2. システム要件.....	5
1.3. 本書の目的	7
1.4. 記号の意味	7
2 アンチウイルス保護の一般的な導入スキーム.....	8
2.1. 論理ネットワーク内のコンピュータに対する アンチウイルス保護の導入スキーム	8
2.2. 一元管理保護システムの構築.....	8
3 KASPERSKY ADMINISTRATION KIT の導入	10
3.1. Kaspersky Administration Kit 付属の MSDE のインストール	11
3.2. ローカルホストへの管理サーバおよび 管理コンソールのインストール.....	13
3.3. Kaspersky Administration Kit の削除	25
3.4. アプリケーションバージョンの更新.....	26
4 ソフトウェアのインストールと削除.....	27
4.1. ソフトウェアのリモートインストール	28
4.1.1. インストールパッケージの作成	29
4.1.2. インストールパッケージ設定の確認と構成	32
4.1.3. ネットワークエージェントインストールパッケージの 作成と構成	36
4.1.4. 管理サーバインストールパッケージの作成と構成.....	39
4.1.5. スレーブ管理サーバへのインストールパッケージ配布タスクの作成.....	40
4.1.6. ネットワークエージェントを使用したグループ内への インストールパッケー ジの配布	41
4.1.7. 導入タスクの構成.....	53
4.1.8. スレーブ管理サーバへのアプリケーション導入	55
4.1.9. ソフトウェアのリモート削除.....	56
4.2. 導入ウィザード	57
4.3. ソフトウェアのローカルインストール	61
4.3.1. ネットワークエージェントのローカルインストール	62
4.3.2. アプリケーション管理プラグインのローカルインストール	67
4.3.3. アプリケーションの非対話モードでのインストール	67

付録A. 用語解説.....	69
付録B. KASPERSKY LAB.....	75
B.1. 製品ラインナップ.....	75
B.2. お問い合わせ先.....	80

1 KASPERSKY ADMINISTRATION KIT

1.1. 目的、構造、主な機能

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、管理者は以下のことができます：

- カスペルスキー製品の導入と削除：ネットワーク内部のネットワーク接続しているコンピュータに対して、この作業を行うことができます。管理者はこの機能を使用して、選択したコンピュータに一連の必要なカスペルスキー製品をコピーし、これらの製品をネットワークコンピュータに配布できます。
- カスペルスキー製品のリモートからの一元管理：管理者はこの機能を使用して、複数レベルのアンチウイルスシステムを作成し、1 台の管理コンピュータからすべてのアプリケーションの動作を管理できます。この機能は、いくつかの建物またはオフィスをカバーする多数のコンピュータで構成されるローカルネットワークを持つ大企業にとって特に重要です。この機能を利用して、管理者は以下のことができます：
 - コンピュータの実行する機能や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基づいて、コンピュータを「管理グループ」にグループ分けする
 - グループポリシーを作成して適用することで、アプリケーション設定を中央集散的に構成する
 - アプリケーション設定を使用して、個別のコンピュータのアプリケーション設定を個別に構成する
 - 「グループタスク」と「グローバルタスク」を作成して実行することで、アプリケーションの動作を中央集散的に管理する
 - 異なる管理グループに属する一連のコンピュータに対するタスクを作成して実行することで、アプリケーション動作の個別パターンを作成する
- コンピュータ上の定義データベースとアプリケーションモジュールの自動更新：この機能を使用すると、カスペルスキーのインターネット上のアップデートサーバに個別にアクセスしなくても、インストールされているカスペルスキー製品す

べてに対して定義データベースを中央から一括して更新できます。更新は、管理者が設定したスケジュールに従って自動的に実行されます。管理者は、クライアント PC に対する更新のインストールを監視できます

- **専用システムを使用したレポートの受信**：この機能を使用して、インストールされているカスペルスキー製品の動作に関する統計情報を中央で収集し、これら製品の動作が正しいかどうかを確認し、入手した情報に基づいてレポートを作成することができます。管理者は、アプリケーション動作に関する累積型ネットワークレポート、または各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動作に関するレポートを作成できます
- **イベント通知システムの使用、メールによる通知の送信システム**：この機能を使用して、アプリケーション動作におけるイベントの一覧を作成し、それらに関する通知を受け取ることができます。このリストには、新規ウイルスの検知、定義データベースの更新で発生したエラー、ネットワーク内での新規コンピュータの検知などのイベントが含まれます
- **ライセンス管理の実施**：この機能は、インストールされているすべての企業アプリケーションに対するライセンスキーの一括インストールと、ライセンス契約の準拠状況（実行中のアプリケーション数とライセンス数に対応しているかどうか）およびライセンス契約の有効期限の追跡をサポートしています
- **Cisco Network Admission Control (NAC) との連携**：この機能は、ホストのアンチウイルス保護と Cisco NAC ステータスとの間のマッピングを行います

Kaspersky Administration Kit は、3 つの主要コンポーネントで構成されています：

- **管理サーバ**は、企業ネットワークにインストールされているカスペルスキー製品に関する情報や、そうした製品の管理に関する情報を集中的に保管する場所（ストレージ）として機能します
- **ネットワークエージェント**は、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との間のやりとりを調整します。このコンポーネントは、Kaspersky Business Security に含まれるすべての Windows アプリケーションをサポートします
- **管理コンソール**は、管理サーバとネットワークエージェントの管理サービスに対し、ユーザインターフェイスを提供します。この管理モジュールは、Microsoft Management Console (MMC) の拡張機能として実装されます

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 NT4 SP 6a 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。文書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 アンチウイルス保護の一般的な導入スキーム

2.1. 論理ネットワーク内のコンピュータに対する アンチウイルス保護の導入スキーム

Kaspersky Administration Kit を使用して社内ネットワークにセキュリティシステムを導入するには、以下の 2 通りの方法があります：

- 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者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って使用してください

Kaspersky Administration Kit を使用したリモートインストールでは、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。

2.2. 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、まずはじめに論理ネットワークを設計します。ここでは、以下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。管理サーバの階層を使用することで、通信チャンネルの負荷を大幅に削減し、システムの信頼性を向上させることができます
2. メイン管理サーバ、スレーブ管理サーバ、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。カスペ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を決定する。グループ階層をどのようにするかを決定する

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

次の段階では、管理者は論理ネットワークを構築する必要があります。以下の **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

次のステップでは、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。

次の段階では、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、対応する管理プラグインを管理者コンピュータにインストールする必要があります。

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。

最終段階では、グループポリシーを割り当てて適用し、タスクを作成することで、インストールされたアプリケーションを構成する必要があります。

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。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 for Windows Workstations** 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。

3 KASPERSKY ADMINISTRATION KIT の導入

インストールを開始する前に、管理サーバと管理コンピュータのソフトウェア要件とハードウェア要件をコンピュータが満たしていることを確認してください (5ページの 1.2 項を参照)。

管理サーバ情報の保管には、MSDE (Microsoft Data Engine)、MySQL Server または Microsoft SQL Server が使用されます。MSDE または SQL Server がインストールされていない場合は、管理サーバのインストール前にいずれかをインストールする必要があります。Kaspersky Administration Kit に付属する MSDE を使用するには、3.1項を参照してください。

Kaspersky Administration Kit のインストールには、インストールが行われるコンピュータの管理者権限が必要です。

セットアップウィザードを利用すれば、Kaspersky Administration Kit のアプリケーションコンポーネント (管理サーバと管理コンソール) を簡単に導入することができます。これは、一元管理システム作成の初期段階での推奨設定です。

インストールされたアプリケーションコンポーネントが正しく機能するように、必要なポートがホストコンピュータ上ですべて開いている必要があります。Kaspersky Administration Kit で使用されるデフォルトポートは、表 1 のとおりです。

表 1

ポート番号	プロトコル	説明
管理サーバが動作するホスト		
13000	TCP および UDP	SSL プロトコルが以下の目的で使用されます： <ul style="list-style-type: none"> クライアントからデータを受信する 更新エージェントに接続する スレーブ管理サーバに接続する ホストのシャットダウンについて通知を受信する
13292	TCP	モバイル接続のため使用されます

ポート番号	プロトコル	説明
14000	TCP	以下の目的で使用されます： <ul style="list-style-type: none"> クライアントからデータを受信する 更新エージェントに接続する スレーブ管理サーバに接続する
18000	HTTP	Cisco NAC 認証サーバからデータをダウンロードするために、管理サーバによって使用されます
アップデートサーバに指定されたホスト		
13000	TCP	接続のためにクライアントによって使用されます
13001	TCP	管理サーバの置かれたホストが更新エージェントに指定されている場合、クライアント PC によって使用されます
14000	TCP	接続のためにクライアントによって使用されます
14001	TCP	管理サーバの置かれたホストが更新エージェントに指定されている場合、クライアント PC によって使用されます
管理エージェントが動作するクライアント		
15000	UDP	管理サーバへの接続要求を受信するために使用されます

3.1. Kaspersky Administration Kit 付属の MSDE のインストール

MSDE のインストール前に、[Microsoft Data Access Components \(MDAC\) 2.8](#) 以上をインストールする必要があります。MDAC が導入されていない場合は、[Microsoft の Web サイト](#)から入手してください。

Kaspersky Administration Kit 配布パッケージからコンピュータへの MSDE のインストールは、ローカルで実行されます。

MSDE をインストールするには：

1. Kaspersky Administration Kit インストール CD の **MSDE2KSP3** ディレクトリにある実行ファイルを実行します。インストールウィザードが起動し、設定の構成とアプリケーションの実行が促されます。セットアップウィザードの指示に従って作業を進めてください

2. インストールに必要なファイルが解凍され、ハードディスクへのコピー、必須ソフトウェアの検証、ライセンス契約の承認が行われ、ユーザおよび企業に関する情報が表示されます
3. 続いて、**[インストール先を選ぶ]** ダイアログボックスで以下の内容を定義します：
 - **[プログラムファイル]** フィールド - MSDE アプリケーションファイルのインストール用フォルダ。デフォルトのフォルダは「<ドライブ名:¥Program Files¥Microsoft SQL Server」です。このフォルダがない場合は、自動的に作成されます
 - **[データファイル]** フィールド - MSDE サーバデータベースの保管に使用されるフォルダ。デフォルトのフォルダは、同様に「<ドライブ名:¥Program Files¥Microsoft SQL Server」です

フォルダを指定するには、**[参照]** ボタンを使用します

4. 続いて、**[MSDE2000 インスタンス名]** ダイアログボックス (図 1. を参照) に、このサーバに割り当てる名前を指定します。この名前はデフォルトでは作成されず、サーバがインストールされているコンピュータの名前がサーバの名前に使用されます。別の名前を割り当てる場合は、**[デフォルト]** ボックスをオフにし、**[インスタンス名]** に新しい名前を入力します

設定が終わったら、内容を確認してインストールを開始できます。インストールが正常に完了すると、MSDE がコンピュータにインストールされます。

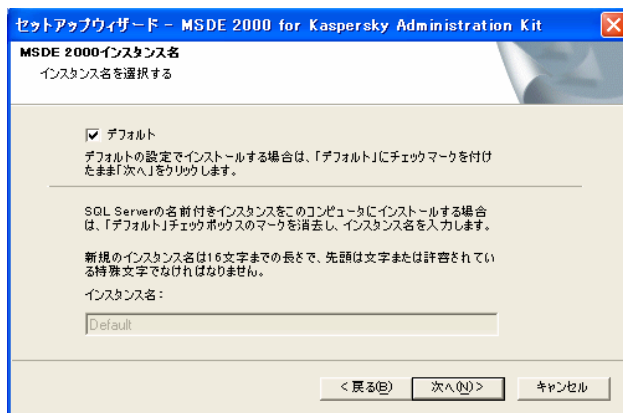


図 1. サーバ名の選択

3.2. ローカルホストへの管理サーバおよび 管理コンソールのインストール

この項では、管理サーバまたはコンソール、あるいはその両方のローカルインストールについて説明します。ネットワーク上で管理サーバが 1 台だけ実行している場合でも、リモートインストールタスクで強制的なインストールを使用して追加のサーバをインストールできます。タスクを作成する場合は、管理サーバのインストールパッケージを使用します。

管理サーバまたは管理コンソール、あるいはその両方をローカルホストにインストールするには：

1. **setup.exe** ファイルを実行します。インストールウィザードが起動し、設定の構成が要求されます。セットアップウィザードに従って作業を進めてください
2. まず、配布パッケージから必須ファイルが解凍され、ハードディスクにファイルがコピーされ、ライセンス契約の承認が要求され、ユーザおよび企業に関する情報の提供が要求されます
3. 続いて、コンポーネントのインストールに使用されるフォルダを定義します。デフォルトのフォルダは「<ドライブ>:\Program Files\Kaspersky Lab\Kaspersky Administration Kit」です。このフォルダがない場合は、自動的に作成されます。フォルダを変更するには、**[参照]** ボタンを使用します
4. 続いて、インストールする Kaspersky Administration Kit コンポーネントを選択します (図 2. を参照)：
 - **管理サーバ** - このオプションでは、Cisco NAC と統合する標準のカスペルスキーコンポーネントをインストールするかどうかを指定できます。インストールが必要な場合は、**[Kaspersky Lab Posture Validation Server for Cisco NAC]** をオンにします。Cisco NAC と連動するためのパラメータは、プロパティまたは管理サーバのポリシーで構成できます (『Kaspersky Administration Kit 参照ガイド』を参照)
 - **管理コンソール**
 - **ネットワークエージェント**

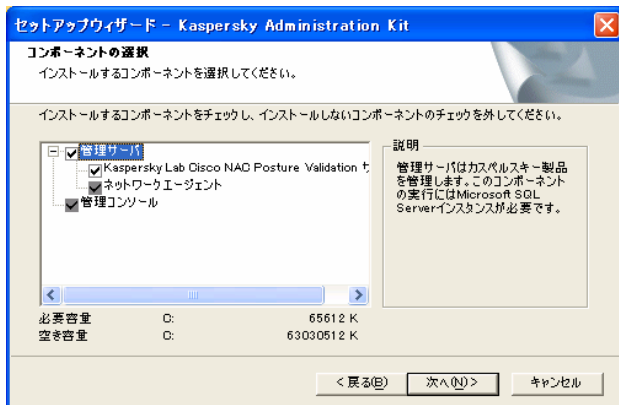


図 2. インストールするコンポーネントの選択

すべてのコンポーネントのインストール、または管理コンソールだけのインストールを選択できます。コンソールをインストールしないと、管理サーバのインストールを選択できません。デフォルトのオプションでは、すべてのコンポーネントがインストールされます。

サーバ向けネットワークエージェントは、管理サーバとともにインストールされます。クライアント向けネットワークエージェントではインストールできません。このコンポーネントがすでにインストールされている場合は、削除してから管理サーバを再インストールしてください。

作業の際には、ウィザードウィンドウに表示される以下の情報をご確認ください：

- 右側の [説明] フィールド - 選択されたコンポーネントに関する情報
- 下部セクション - 選択されたコンポーネントのインストールに必要なディスク容量、およびインストール用に選択されたドライブで使用可能なディスク容量に関する情報

管理コンソールしか選択していない場合、インストール設定はこれ以上必要ありません。このまま設定確認の段階に進み、インストールを開始します

5. 管理サーバのインストールを選択した場合は、以下の手順で、管理サーバをサービスとして起動するアカウントを選択します (図 3. を参照)

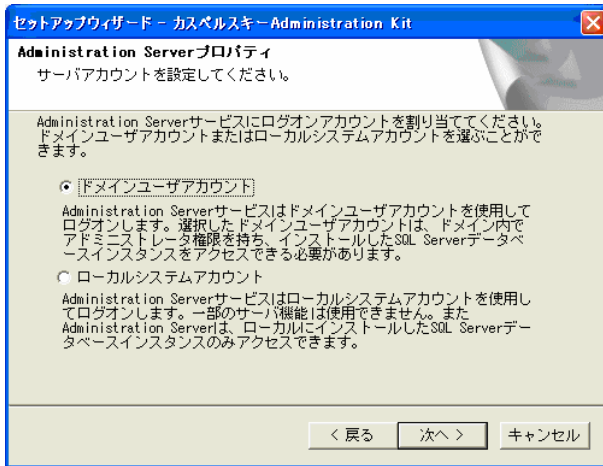


図 3. アカウントの選択

以下の 2 つのオプションから選択してください：

- **ドメインユーザアカウント** - 管理サーバは、ドメイン内に含まれるユーザアカウントの下で起動します。この場合、管理サーバはこのアカウントの権限を使用してすべての操作を実行できます。次のステップでは、アカウントが使用されるユーザを指定します。

Windows ドメイン構造が企業ネットワーク内に作成されている場合は、管理サーバの起動にドメイン管理者のアカウントを選択することをお勧めします。将来的には、導入（リモートインストール）タスクを作成するときにドメイン管理者権限を与えられたユーザのアカウントを指定するなどの追加設定を行う必要がなくなる予定です。

- **ローカルシステムアカウント** - 管理サーバは、システムアカウントの下で、このアカウントに与えられたすべての権限で起動します。この場合は、ユーザアカウントを選択しません。このまま管理サーバの情報データベースを保管するリソースの指定段階に進みます。

Kaspersky Administration Kit の正常動作には、管理サーバの起動に使用するアカウントには管理サーバの情報データベースを保管するリソースに対する管理者権限を付与する必要があります。

6. 管理サーバの起動用にドメインのユーザアカウントを選択した場合は、ユーザの指定が要求されます。

作業を行うには、ウィザードウィンドウの [ユーザ名] フィールド (図 4. を参照) で、[参照] ボタンを使ってユーザ名を選択するか、現在のドメイン内に登録されている名前の中から指定する名前を選択します。続いて、ユーザをドメインに登録するのに使用したパスワードを入力します。

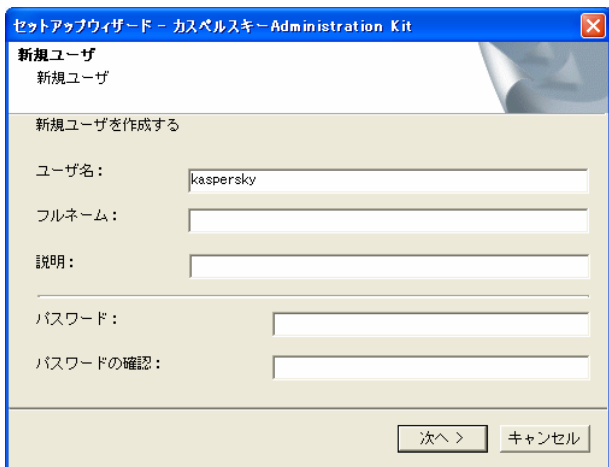


図 4. ユーザの選択

ドメイン管理者権限を持たないユーザを選択した場合、管理サーバはそのアカウントの下で起動しますが、**Kaspersky Administration Kit** の機能は若干制限されます。たとえば、起動シナリオを使用した導入タスクの実行 (53 ページの 4.1.7 項を参照) や **Windows** ネットワークの一部ドメインに対するポーリングに必要な権限が与えられません。

管理サーバを正しく動作させるには、起動に使用するアカウントに以下の権限を付与する必要があります：

- サービスとしてログオン
- オペレーティングシステムの一部として機能
- ネットワーク経由でコンピュータにアクセス
- プロセスレベルトークンの置き換え
- プロセスのメモリクォータの増加

選択したユーザがドメイン管理者で、上記権限を持たない場合は、上記権限がこのユーザに付与されます (図 5. を参照)。

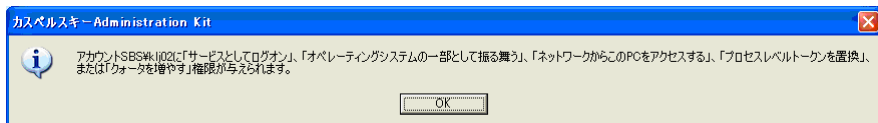


図 5. ユーザに付与される権限に関するメッセージ

7. 次のステップでは、情報データベースの保管に使用される **Microsoft SQL Server (MSDE)** または **MySQL** (図 6. を参照) を定義します。

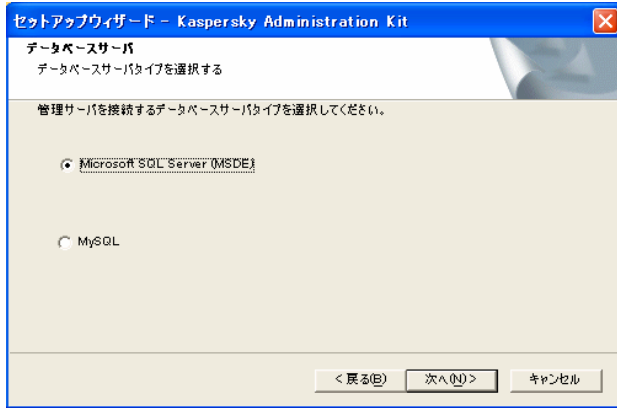


図 6. データベースの選択

- 前ステップで MSDE または Microsoft SQL Server を選択し、企業ネットワーク内にインストールされたサーバを使用して Kaspersky Administration Kit を利用する場合は、サーバ名を [サーバ名] に指定し、管理サーバデータの保管用に作成されるデータベースの名前を [データベース名] に指定します (図 7. を参照)。デフォルトのデータベース名は **KAV** です。

Kaspersky Administration Kit のインストール元のコンピュータで SQL Server が検出された場合は、[サーバ名] フィールドに「**(local)**」という値が自動的に割り当てられます。ネットワークにインストールされている Microsoft SQL Server の一覧を表示するには、[参照] ボタンを押します。

ローカル管理者アカウントまたはシステムアカウントで管理サーバを起動する場合、[参照] ボタンは使用できません。



図 7. SQL Server の選択

前ステップで MySQL Server を選択した場合は、このウィンドウ (図 8. を参照) でサーバ名を [サーバ名] フィールドに指定し (デフォルトでは Kaspersky Administration Kit がインストールされるコンピュータの IP アドレス)、接続に使用するポートを [ポート] フィールドに指定します (デフォルトポートは 3306)。[データベース名] フィールドには、データの保管用に作成されるデータベースの名前を指定します。デフォルトでは **KAV** という名前のデータベースが作成されます。

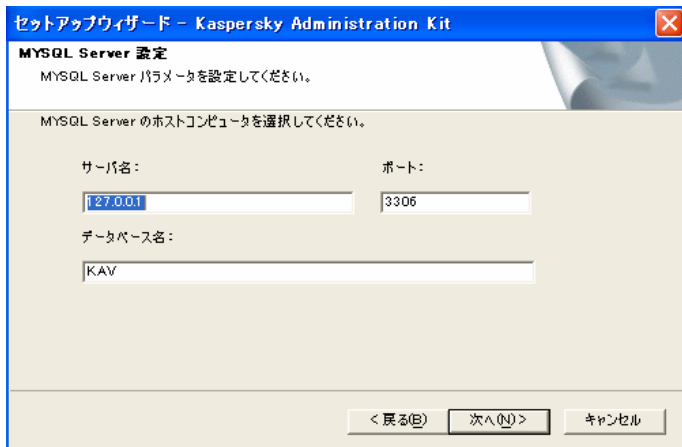


図 8. MySQL Server の選択

ネットワーク上に **SQL Server** が存在しない場合は、インストールする必要があります (11 ページの 3.1 項を参照)。

Kaspersky Administration Kit のインストール元コンピュータに **SQL Server** をインストールする場合は、インストールを中断し、**SQL Server** をインストールした後、に再開してください。

Kaspersky Administration Kit をリモートコンピュータにインストールする場合は、インストールウィザードを中断する必要はありません。**SQL Server** をインストールし、Kaspersky Administration Kit のインストールに戻ります。

9. この手順では、管理サーバが **SQL Server** に接続するために使用する認証モードを定義する必要があります

MSDE または MySQL Server について、以下の 2 つのオプションからいずれかを選択できます (図 9. を参照) :

- **Microsoft Windows 認証モード** - この場合、権限の確認には管理サーバの起動に使用されるアカウントが使用されます
- **SQL Server 認証モード** - このオプションを選択した場合、権限の確認には下で指定されたアカウントが使用されます。[**アカウント**]、[**パスワード**]、および [**パスワードの確認入力**] フィールドに情報を入力してください

管理サーバのデータベースが別のコンピュータにある場合は、管理サーバのインストールまたは更新を行うときに **SQL Server 認証モード** を選択する必要があります。



図 9. SQL Server 認証モード

MySQL Server の場合は、アカウントとパスワードを指定します (図 10. を参照)。

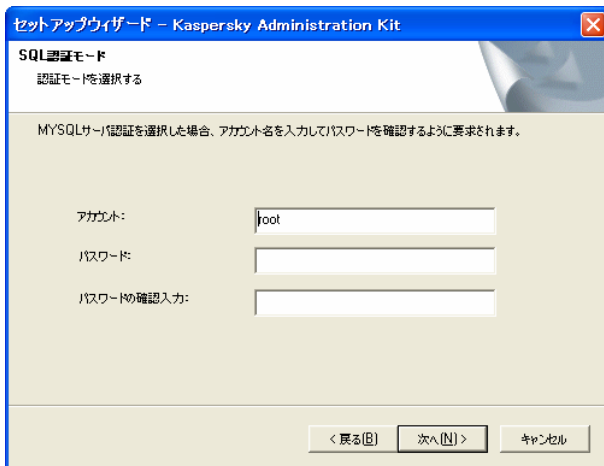


図 10. MySQL Server 認証モード

10. 続いて、使用する共有フォルダの保管場所を指定します (図 11. を参照)

- アプリケーションのリモートインストールに必要なファイルを保管する。ファイルは、インストールパッケージの作成時に管理サーバへコピーされます
- 更新元から管理サーバにコピーされた更新を保管する

このリソースは、すべてのユーザに対して読み取り専用で公開されます。



図 11. 共有フォルダの作成

以下の 2 つのオプションから選択できます：

- **新規共有フォルダを作成する** - 新規フォルダを作成するには、ウィンドウ下部のフィールドにフォルダへのパスを指定する必要があります
- **既存の共有フォルダを選択してください** - 既存フォルダの一覧から共有フォルダを選択します

共有フォルダは、インストールの実行元コンピュータにローカル保管するか、企業ネットワークに含まれる任意のコンピュータにリモート保管できます。共有フォルダは、[参照] ボタンを使用して指定するか、UNC パス（例：\\server\KLSHare）を入力して手作業で指定します。

デフォルトでは、Kaspersky Administration Kit アプリケーションコンポーネントのインストール用に指定されたフォルダの中に、**KLSHare** というローカルフォルダが作成されます。

11. ウィザードの以下のダイアログで以下の内容を指定して、管理サーバのアドレスを指定します (図 12. を参照)：
- **DNS アドレス** - このオプションは、クライアントが管理サーバアドレスを入手するために使用可能な DNS サーバがネットワークに存在する場合に使用します
 - **NetBIOS アドレス** - このオプションは、クライアントが管理サーバアドレスを NetBIOS プロトコル経由で入手する場合、またはネットワーク上に WINS サーバがある場合に使用します
 - **IP アドレス** - このオプションは、管理サーバに固定 IP アドレスが割り当てられている場合に使用します

必要に応じて [アンチハッカーで NetBIOS の名前解決を許可する] をオンにします。これによって、ホストにインストールされている Kaspersky Anti-Virus 6.0 アンチハッカーで UDP ポート 137 が開きます。このポートは、管理サーバの IP アドレスを入手するために使用されます。

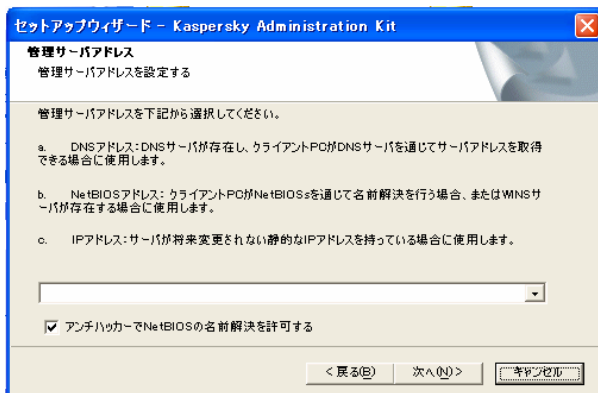


図 12. 管理サーバアドレス

12. 続いて、管理サーバへの接続に使用される設定を構成します (図 13. を参照) :

- 管理サーバへの接続に使用されるポート番号 - デフォルトでは、ポート **14000** が使用されます。すでに割り当てられている場合は、変更できます
- **SSL** プロトコルを使用した管理サーバへの接続に使用される **SSL** ポート番号 - デフォルトでは、ポート **13000** が使用されます

管理サーバが **Microsoft Windows XP SP 2** で動作している場合、組み込みファイアウォールは **TCP ポート 13000 および 14000** をブロックするため、管理サーバが動作するホストでこれらのポートを手動で開く必要があります。

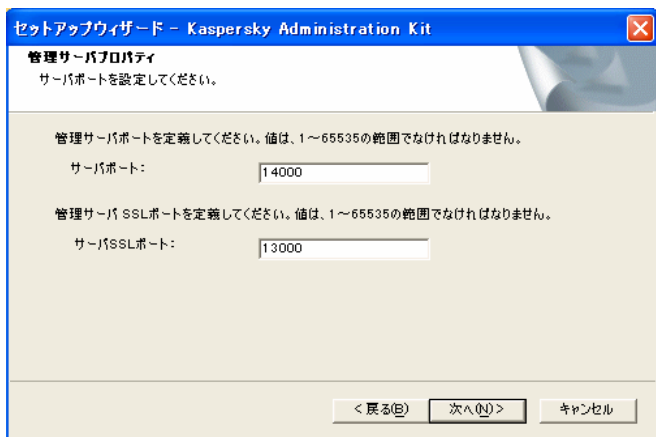


図 13. 管理サーバへの接続に使用される設定

13. このウィザードウィンドウ (図 14. を参照) で、インストール中の管理サーバの認証に使用される証明書の作成方法を指定します :

設定には以下の **2** つのオプションがあります :

- **新規証明書を作成する** - このオプションは、新規管理サーバをインストールする場合に使用します。データおよびこのサーバの論理ネットワーク構造を後で簡単に復元できるように、必要に応じて証明書のバックアップを保存してください。バックアップを作成するには **[証明書のバックアップを保存する]** ボックスをオンにします
- **証明書を復元** - このオプションは、使用できるバックアップのない管理サーバを復元する場合に使用します。以前の管理サーバのデータと論理ネットワーク構造を復元できます

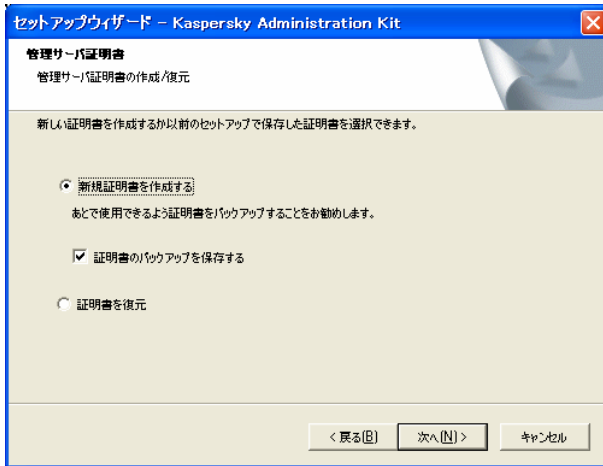


図 14. 管理サーバ証明書の受信に使用される方法の選択

14. 前段階で新規証明書の作成とバックアップの保存を選択した場合は、以下の内容を対応するウィンドウで指定します (図 15. を参照) :

- 証明書ファイルのバックアップを保存するフォルダ
- 新規証明書作成時の暗号化およびバックアップオブジェクトの復元時に使用するパスワード
- パスワードの確認

管理サーバのデータを後で復元できるようにするには、サーバの証明書を保存する必要があります。

証明書を復元する場合は、バックアップ作成に使用したのと同じパスワードを入力する必要があります。誤ったパスワードを入力すると、証明書は復元されません。



図 15. 証明書のバックアップを保存するフォルダの選択

Kaspersky Administration Kit のインストール設定が終わったら、内容を確認してインストールを開始できます。

管理コンソールのインストールが終了すると、コンピュータの [スタート] → [プログラム] → [カスペルスキー Administration Kit] メニューにアイコンが表示されます。このアイコンを使用してコンソールを起動できます。

管理サーバおよびエージェントは、表 2 に挙げられた属性を持つサービスとしてホストコンピュータにインストールされます。この表には、適切なコンポーネントが管理サーバとともにインストールされている場合に、問題となっているホストで実行する Kaspersky Lab Posture Validation Server (PVS) for Cisco NAC のプロパティも含まれています。

表 2

プロパティ	管理サーバ	Kaspersky Lab PVS for Cisco NAC	管理エージェント
サービス名	CSAdminServer	nacserver	klagent
表示されるサービス名	管理サーバ	Kaspersky Lab Cisco NAC Posture Validation Server	ネットワークエージェント
Windows タスクマネージャでのプロセス名	klserver.exe	klnacserver.exe	klagent.exe

プロパティ	管理サーバ	Kaspersky Lab PVS for Cisco NAC	管理エージェント
スタートアップの種類	オペレーティングシステムの起動時に自動スタートアップ		
ユーザ名	Local Service またはユーザ指定		

サーバ向けネットワークエージェントは、管理サーバとともにコンピュータにインストールされます。これは管理サーバコンポーネントの構造に含まれ、管理サーバとともにインストールまたは削除されます。また、ローカルにインストールされた管理サーバのみとやりとりします。管理サーバに接続するためにエージェントが使用する設定は、構成する必要はありません。これらのコンポーネントが同じコンピュータにインストールされるという前提に基づいて、接続はプログラマ的に実装されています。これによって、追加設定の必要性を回避し、別個にインストールした場合にコンポーネントの操作で生じる可能性のある競合を回避できます。

サーバ向けネットワークエージェントは、クライアント向けネットワークエージェントと同じ属性でインストールされ、同じアプリケーション管理機能を実行します。管理サーバのコンピュータがクライアント PC として含まれるグループのポリシーに基づいて動作し、ネットワークエージェントに備わるタスクは、サーバ変更タスクを除いてすべて作成されます。

ネットワークエージェントを管理サーバのコンピュータに別途インストールする必要はありません。この機能はサーバ向けネットワークエージェントによって実行されます。

標準の Windows 管理ツールの [コンピュータの管理] → [サービス] を使用して、管理サーバ、ネットワークエージェント、および **Kaspersky Lab Cisco NAC Posture Validation Server** のプロパティを確認し、これらサービスの動作を監視できます。管理サーバサービスの動作に関する情報は、管理サーバがインストールされているコンピュータの Windows システムログ (**Kaspersky Event Log** とは別のブランチ) に登録および保存されます。

さらに、管理サーバがインストールされているコンピュータにローカルユーザグループ **KLAdmins** および **KLOperators** が作成されます。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実行する場合、ドメインユーザグループのリストにはグループ **KLAdmins** および **KLOperators** が追加されます。グループリストの変更は、標準の Windows 管理ツールを使用して行います。

3.3. Kaspersky Administration Kit の削除

Kaspersky Administration Kit は、[スタート] → [プログラム] → [カスペルスキー Kaspersky Administration Kit] メニューの [カスペルスキー Administration Kit のアンインストール] オプションを使用するか、Windows の [アプリケーションの追加と削除] を使用してアンインストールできます。これによって、PC からすべてのアプリケーションコンポーネント (プラグインを含む) をアンインストールするウィザードが起動します。

共有フォルダ (KLSHare) の削除を要求しない場合は、必要なすべてのタスクが完了した後
に手動で削除します。

プログラムを削除するときに、管理サーバのバックアップの保存が提案されます。

3.4. アプリケーションバージョンの更新

Kaspersky Administration Kit バージョン 4.x および 5.0 をバージョンアップするには、以
前のバージョンをアンインストールしてから本書の手順に従って新しいバージョンをイン
ストールする必要があります。

バージョン 5.0 (Planned Update 3) および 6.0 を新しいバージョンに更新する場合は、古
いバージョンのアプリケーションによって作成されたバックアップからデータを復元でき
ます。復元するには、以下の手順に従ってください：

新バージョンへのデータ移行は、Kaspersky Administration Kit バージョン 5.0 MP3 以降
でのみサポートされています。

1. **klbackup.exe** ユーティリティを使用して、インストール済み管理サーバのデー
タのバックアップを作成します。このユーティリティは **Kaspersky Administration
Kit** 配布パッケージに含まれ、管理サーバのインストール後はルートインストール
フォルダに配置されます。管理サーバのデータを後で完全に復元できるようにす
るには、サーバの証明書を保存する必要があります。これは、**klbackup.exe** ユ
ーティリティの必須設定です
2. 以前のバージョンの管理サーバまたは管理コンソール、あるいはその両方がイン
ストールされているコンピュータで、**Kaspersky Administration Kit 6.0** の更新済み
バージョンのインストールを実行します。コンポーネントをアップグレードして
ください。アップグレード中、以前のバージョンの管理サーバまたは管理コンソ
ール、あるいはその両方のデータがすべて保存され、新規バージョンで使用可能
になります。管理サーバの新旧バージョン間での下位互換性がサポートされてい
ます。新規バージョンの管理サーバは、以前のバージョンとの下位互換性があり
ます
3. ネットワークコンピュータ上のネットワークエージェントをアップグレードする
には、コンポーネントの新規バージョンをインストールするグループタスクまた
はグローバルタスクを作成します。タスクを手動で実行するか、スケジュールに
従って実行してください。タスクが正常に完了すると、ネットワークエージェン
トが新規バージョンにアップグレードされます

インストール中になんらかの問題が発生した場合は、アップグレード前に作成し
た管理サーバデータのバックアップを使用して、**Kaspersky Administration Kit** の以
前のバージョンを復元できます

1 台の管理サーバがインストールされていても、リモートインストールタスクと管理サー
バインストールパッケージを使用して、追加のサーバを更新できます。

4 ソフトウェアのインストールと削除

インストールの開始前に、コンピュータのソフトウェアとハードウェアが該当の要件を満たしていることを確認する必要があります (5ページの 1.2 項を参照)。

Kaspersky Administration Kit では、カスペルスキー製品を以下の方法でインストールおよび削除できます：

- 管理コンソールを利用したリモートインストール
- 端末ごとのローカルインストール

管理サーバとクライアント PC との接続は、ネットワークエージェントコンポーネントによって確保されます。したがって、アンチウイルス製品のインストール前に、リモート管理システムに接続する各コンピュータに、このコンポーネントがインストールされている必要があります。リモート方式でアプリケーションをインストールする場合は、ネットワークエージェントをそれらのアプリケーションとともにインストールできます。

管理サーバがインストールされているコンピュータでは、サーバ向けネットワークエージェントしか使用できません。これは管理サーバ構造に組み込まれ、管理サーバとともにインストールおよび削除されます (13 ページの3.2 項を参照)。
このコンピュータにネットワークエージェントをインストールする必要はありません。

ネットワークエージェントは、アプリケーション同様、リモートまたはローカルでインストールできます。

ネットワークエージェントは、インストールされているカスペルスキー製品によって異なります。製品によっては、ネットワークエージェントのローカルインストールしか実行できません。詳細については、該当するアプリケーション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は、クライアント PC に一度だけインストールされます。

Kaspersky Administration Kit アプリケーションの管理インターフェイスは、対応する管理プラグインによって実装されます。したがって、アプリケーションの管理インターフェイスにアクセスするには、対応するプラグインが管理者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。リモートインストール方式の場合、対応するアプリケーションの最初のインストールパッケージが作成されるときに、プラグインが自動的にインストールされます。クライアント PC にローカルインストールする場合、管理者は管理プラグインを手動でインストールする必要があります。

現行バージョンの Kaspersky Administration Kit では、以下のカスペルスキー製品がリモート管理に対応しています：

- ワークステーションおよびファイルサーバ向け製品：
 - Kaspersky Antivirus 5.0 for Windows File Servers
 - Kaspersky Antivirus 6.0 for Windows Server
 - Kaspersky Antivirus 5.0 for Windows Workstations

- Kaspersky Antivirus 6.0 for Windows Workstation
- ゲートウェイ向け製品：
 - Kaspersky Antivirus 5.6 for Microsoft ISA Server 2000 Enterprise Edition（2007年4月現在、日本語版の取り扱い無し）
- メールサーバ向け製品：
 - Kaspersky Antivirus 5.5 for Microsoft Exchange Server 2000/2003, Planned Update 1（2007年4月現在、日本語版の取り扱い無し）
 - Kaspersky Security 5.5 for Microsoft Exchange Server 2003, Planned Update 1（2007年4月現在、日本語版の取り扱い無し）

Kaspersky Administration Kit を使用した上記アプリケーションの管理については、該当するアプリケーションのマニュアルを参照してください。

4.1. ソフトウェアのリモートインストール

ソフトウェアのリモートインストールは、管理者コンピュータから、Kaspersky Administration Kit のメインウィンドウから実行できます。

一部のカスペルスキー製品は、リモートインストールに対応していません。詳細については、該当アプリケーションのマニュアルを参照してください。ただし、Kaspersky Administration Kit を使用したこれらアプリケーションのリモート管理は可能です。

ソフトウェアのリモートインストールを実行するには：

1. インストールパッケージを作成します (53 ページの 4.1.7 項を参照)。このパッケージは、アプリケーションのインストールに必要なファイルと、インストールパッケージの設定を含むファイルで構成されます

インストールパッケージには **setup.exe** が含まれています。このファイルを使用して、非対話モードでアプリケーションのローカルインストールが実行されます。

2. リモートインストールのタスクを作成します (53 ページの 4.1.7 項を参照)

論理ネットワーク内のすべてのコンピュータ、いくつかの管理グループ、またはさまざまなグループの特定のコンピュータにアプリケーションをインストールするには、グローバル導入 (リモートインストール) タスクを作成する必要があります

管理グループのすべてのコンピュータ(すべてのネスト化されたグループとスレーブサーバを含む)にアプリケーションをインストールするには、グループ導入 (リモートインストール) タスクを作成する必要があります

導入ウィザード (57 ページの 4.2 項を参照) を使用して、グループタスクまたはグローバルタスクを作成できます

作成したタスクは、スケジュールに従って実行します。各クライアント PC のアプリケーション動作設定は、グループポリシーおよびアプリケーションのデフォルト設定に基づいて構成されます

タスクの実行を手動で中断することで、インストールプロセスを中断できます

管理サーバに対して作成されたすべてのインストールパッケージは、コンソールツリーの [リモートインストール] フォルダに置かれます。これらのインストールパッケージは、管理サーバ上の [Packages] フォルダ内にある指定の共有フォルダに保管されます。

[<パッケージ名>のプロパティ] ウィンドウを使用して、インストールパッケージのプロパティを確認し、名前と設定を変更できます (図 19. を参照)。このウィンドウは、ショートカットメニューの [プロパティ] コマンドを使用するか、[操作] メニューの同様の項目を使用して開きます。

作成されたインストールパッケージは、スレーブ管理サーバ(39 ページの 4.1.4 項を参照)と、更新エージェントを使用するグループ内のコンピュータ (41 ページの 4.1.6 項を参照) に配布されます。

導入タスクの作成に、1 つのインストールパッケージを何度でも再利用できます。

アプリケーションは、非対話モードでもインストールできます。

4.1.1. インストールパッケージの作成

インストールパッケージを作成するには：

1. 必要な管理サーバに接続します
2. コンソールツリーの [リモートインストール] ノードでショートカットメニューを開き、[新規作成] → [インストールパッケージ] を選択するか、[操作] メニューの同様の項目を使用します。これによって、ウィザードが起動します。ウィザードの指示に従います
3. インストールパッケージの名前を指定します。また、以下の手順では、インストールするアプリケーションを指定します (図 16. を参照)

Kaspersky Administration Kit 経由のリモートインストールをサポートするアプリケーションをインストールする場合は、ドロップダウンリストの [カスペルスキー製品のインストールパッケージを作成する] オプションを選択する必要があります。**[参照]** ボタンを使用して、アプリケーションの説明を含むファイル(拡張子は .kpd、Kaspersky Administration Kit 経由のリモート管理がサポートされている

すべてのカスペルスキー製品にバンドルされている)、またはカスペルスキー製品の自己解凍型アーカイブ(拡張子は .exe、カスペルスキーの Web サイトからダウンロード可能) を選択します。アプリケーション名とバージョン番号のフィールドに、情報が自動的に表示されます。

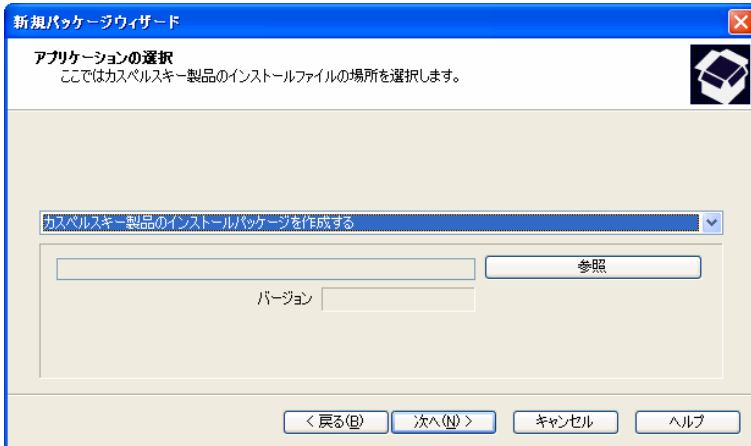


図 16. インストールパッケージの作成 - インストールするアプリケーションの選択

インストールパッケージの設定はデフォルトで作成され、インストールを選択したアプリケーションに対応しています。パッケージの作成後に、パッケージのプロパティ確認ウィンドウで設定を変更できます(32 ページの 4.1.2 項を参照)。

別のアプリケーションをインストールするためのインストールパッケージを作成するには、以下の作業を行います(図 17. を参照)：

- ドロップダウンリストから、**[指定した実行ファイルのインストールパッケージを作成する]** を選択する
- アプリケーション配布パッケージへのパスを、**[参照]** ボタンを使用して指定する
- 配布ファイルが置かれているフォルダのコンテンツ全体をパッケージに含める必要がある場合は、**[全てのフォルダをパッケージへコピー]** ボックスをオンにする
- 必要であれば、実行ファイルの実行で使用する設定を入力用フィールドに指定する(例：非対話モードで実行する場合はスイッチ「/s」を使用する)

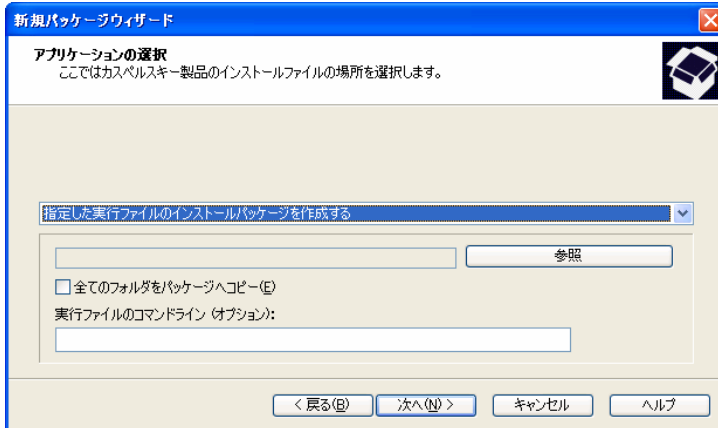


図 17. ユーザによって指定されたアプリケーションのインストールパッケージの作成

4. 以下のウィザードウィンドウ (図 18. を参照) で、インストールパッケージに含めるライセンスキーを指定できます。指定するには、[参照] ボタンを押し、ライセンスキーのファイル (拡張子が **.key** のファイル) を選択します。

インストールパッケージにライセンスキーを含めない場合は、[次へ] ボタンを押します。

管理サーバおよび管理エージェントのインストールパッケージを作成する場合、ライセンスキーは必要ありません。

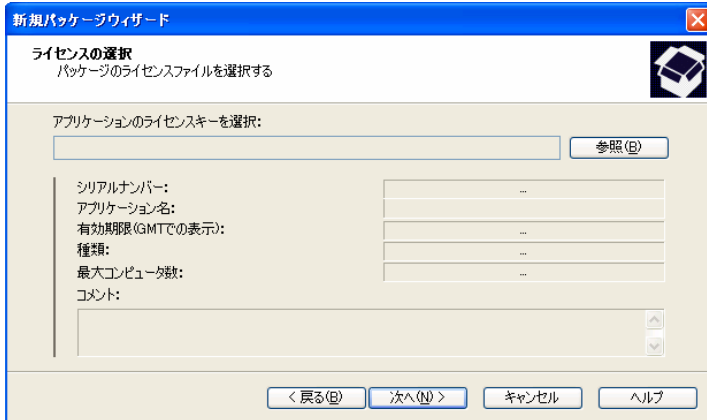


図 18. インストールパッケージの作成 - ライセンスキーの選択

5. 続いて、指定アプリケーションのクライアント PC へのインストールに必要な一連のファイルが管理サーバの共有フォルダにダウンロードされ、選択されたアプリケーションの管理プラグインが管理者のワークステーションにインストールされているかどうかのチェックが行われます。このようなプラグインがインストールされていない場合、またはプラグインのバージョンが配布パッケージに含まれるバージョンよりも古い場合は、新しいプラグインがインストールされて古いプラグインと置き換えられます

ウィザードが完了すると、作成されたインストールパッケージが [リモートインストール] ノードに追加され、結果パネルに表示されます。

4.1.2. インストールパッケージ設定の確認と構成

インストールパッケージのプロパティを確認し、名前や設定を変更するには：

コンソールツリーで [リモートインストール] ノードを展開し、結果パネルで必要なインストールパッケージを選択し、ショートカットメニューの [プロパティ] コマンドまたは [操作] メニューの同様の項目を使用します。

これによって、[<インストールパッケージ名>のプロパティ] ウィンドウ (図 20. を参照) が開きます。このウィンドウは [全般]、[プロパティ]、[ライセンス情報]、[OS 再起動] タブで構成されています。

[全般] タブ (図 19. を参照) には、パッケージに関する一般的な情報が含まれます。

- パッケージ名
- インストールパッケージでインストールされるアプリケーションの名前とバージョン

- パッケージのサイズ
- 作成日

[プロパティ] タブ (図 20. を参照) には、インストールパッケージでインストールされるアプリケーションのインストールパッケージ設定が含まれます。これらの設定はパッケージ作成段階にデフォルトで作成され、必要に応じて変更できます。

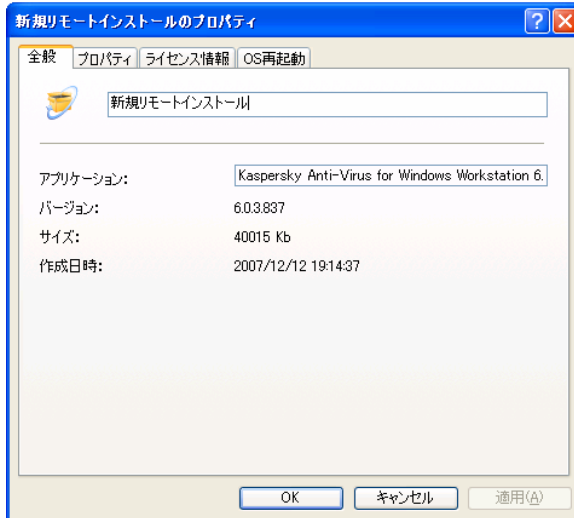


図 19. インストールパッケージのプロパティ確認ウィンドウ
[全般] タブ

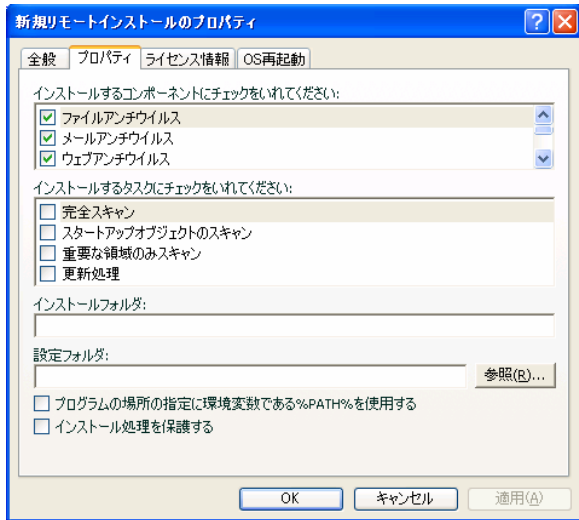


図 20. インストールパッケージのプロパティ確認ウィンドウ
[設定] タブ

[ライセンス情報] タブ (図 21. を参照) には、インストールパッケージでインストールされるアプリケーションのライセンスに関する全般的な情報が含まれます。

ネットワークエージェントのプロパティまたは管理サーバのインストールパッケージのプロパティでは、[ライセンス情報] タブを使用できません。

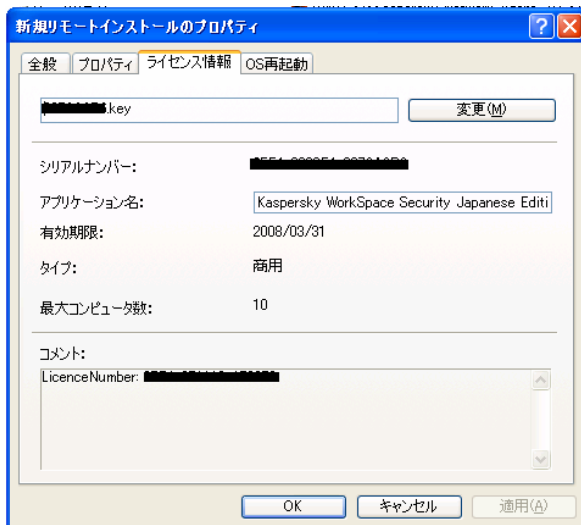


図 21. インストールパッケージのプロパティ確認ウィンドウ
[ライセンス情報] タブ

[OS 再起動] タブ (図 22. を参照) では、アプリケーションのインストール後にコンピュータを再起動する必要がある場合に実行される動作を決定できます。以下のオプションからいずれかを選択できます：

- **オペレーティングシステムを再起動しない** - オペレーティングシステムを再起動しません
- **必要に応じて自動的にオペレーティングシステムを再起動する** - 必要な場合にだけ、オペレーティングシステムを再起動します
- **ユーザに処理を要求する** - このオプションを選択した場合は、以下のことができます：
 - オペレーティングシステムを再起動する必要があることをユーザに通知する情報メッセージを作成する
 - オペレーティングシステムの再起動について通知する頻度を指定する。[プロンプト繰り返し間隔 (分)] ボックスをオンにし、メッセージ表示の間隔を指定します
 - アプリケーションがインストールされた瞬間から起算して指定期間内にコンピュータのオペレーティングシステムの再起動が行われなかった場合、PC が自動的に再起動するように指定する。指定するには、[強制的に再起動するまでの時間 (分)] ボックスをオンにし、期間を指定します

ロックされたコンピュータを再起動する必要がある場合は、[実行アプリケーションを自動的に閉じる] をオンにします。デフォルトでは、この設定はオフになっています。

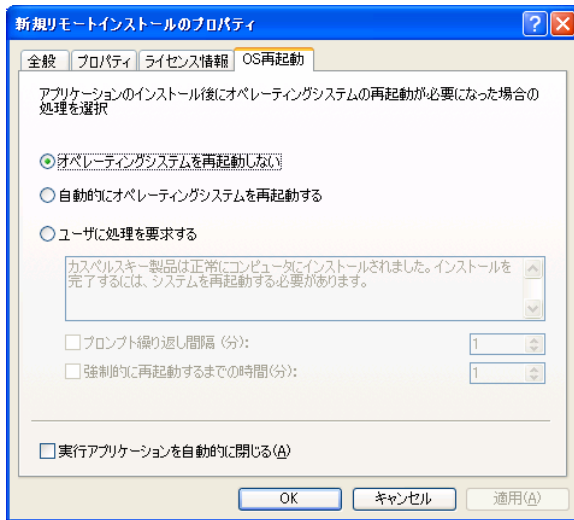


図 22. インストールパッケージのプロパティ確認ウィンドウ
[OS 再起動] タブ

4.1.3. ネットワークエージェントインストールパッケージの作成と構成

ネットワークエージェントのリモートインストール用パッケージは、手動での作成は必要ありません。Kaspersky Administration Kit のインストール中に自動的に作成され、[リモートインストール] ノードに置かれます。

ネットワークエージェントのリモートインストール用パッケージを削除し、もう一度作成する場合は、説明を含むファイルとして Kaspersky Administration Kit のインストールパッケージの [NetAgent] フォルダにあるファイル `knagent.kpd` を選択します。

ネットワークエージェントのインストール設定には、インストール後にコンポーネントが直ちに動作するために必要な最低限の設定セットが含まれます。設定の値は、デフォルトのアプリケーション設定の値と一致します。必要であれば、インストールパッケージのプロパティウィンドウにある [設定] タブと [管理グループ] タブを使用して値を変更できます。

[設定] タブ (図 20. を参照) には、クライアント PC へのインストール後にネットワークエージェントが管理サーバへの接続で使用する設定が含まれます。デフォルトでは、現在のサーバの値が作成時に使用されます：

- 管理サーバがインストールされているコンピュータのアドレス
- 管理サーバへの保護されていない接続に使用されるポートの番号。デフォルトでは、ポート **14000** が使用されます。このポートが使用中である場合は、変更できません
- 管理サーバへの SSL プロトコルで保護された接続に使用されるポートの番号。デフォルトでは、ポート **13000** が使用されます

※10 進表記しか使用できません

- 管理サーバへのアクセスの認証で使用される証明書ファイル。この設定の値は、**[サーバ証明書を使用する]** ボックスで定義します

このボックスがオフになっていると (デフォルト)、エージェントが最初に管理サーバに接続するときに証明書ファイルが自動的に入手されます

[サーバ証明書を使用する] ボックスがオンになっていると、**[参照]** ボタンを使って指定された証明書ファイルに基づいて認証が行われます。このファイルは **.cer** という拡張子が付いており、**Kaspersky Administration Kit** インストールフォルダの **[Cert]** フォルダにあります。**[参照]** ボタンを使用して必要なファイルを選択することで、証明書ファイルを変更できます。

- サーバ接続にネットワークエージェントが使用するポート (シンプルまたはセキュア)。この設定の値は、**[SSL 接続を使用する]** ボックスで定義します。ボックスがオンになっていると、接続は SSL プロトコルを使って保護されたポートを経由して行われます。ボックスがオフになっていると、接続は保護されていないポートを経由して行われます
- プロキシサーバの接続設定。ネットワークエージェントがプロキシサーバを使用してサーバに接続する場合は、**[プロキシサーバ接続設定]** をクリックします。表示されたウィンドウで **[プロキシサーバを使用する]** ボックスをオンにして、プロキシサーバのアドレス、ユーザ名、パスワードを入力します
- **Kaspersky Anti-Virus 6.0** アンチハッカーで管理サーバの IP アドレスを入手するために使用される UDP ポート 137 のオープン。**[アンチハッカーで NetBIOS の名前解決を許可する]** をオンにします。
- 管理エージェントが利用する UDP ポートを Microsoft Windows ファイアウォールの除外リストへ追加。**[Microsoft Windows ファイアウォールにネットワークエージェントのポートを開ける]** をオンにします。

ネットワークエージェントのインストール後に、ポリシーとアプリケーションの設定を使用して、管理サーバへの接続に使用する値を変更できます。

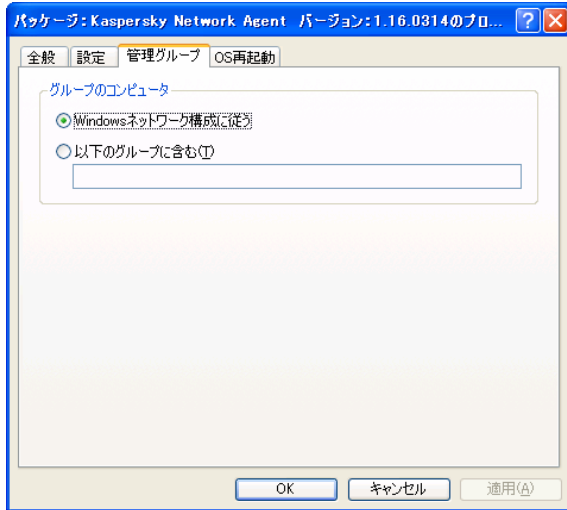
クライアント PC にネットワークエージェントをリモートから再インストールする場合、サーバへの接続に使用される設定の値と管理サーバの証明書は、新しいものと置き換えられます。

[管理グループ] タブ (図 23. を参照) は、ネットワークエージェントのインストール後にコンピュータが追加される [ネットワーク] グループのサブグループを定義するために使用されます。以下のオプションからいずれかを選択できます：

- **Windows ネットワーク構成に従う** - Windows ネットワークにおけるこのコンピュータの位置に対応するフォルダ、ドメインまたはワークグループにコンピュータを追加する。デフォルトではこのオプションがオンになっています
- **以下のグループに含む** - 入力フィールドで指定したグループに、すべてのコンピュータを追加する。このオプションをオンにした場合は、フォルダの名前を下のフィールドに入力します。[ネットワーク] グループ内にそのようなフォルダがない場合は、フォルダが作成されます。[ネットワーク] グループ内の既存フォルダの名前を指定することもできます

ネットワークエージェントのインストール前にコンピュータが管理サーバによって検知され、既に該当するネットワークに対応するフォルダに置かれている場合でも、ネットワークで新しく検知されたコンピュータの保存にはこのフォルダが使用されます。ネットワークエージェントのインストール前にネットワークで検知されたコンピュータは、[ネットワーク] グループ内の以前の場所にそのまま残ります。

この設定はポリシー設定およびアプリケーション設定に含まれないため、ネットワークエージェントのインストール後は [ネットワーク] グループ内のコンピュータを保管するフォルダを変更できません。



23. 管理エージェントインストールパッケージのプロパティウィンドウ - [管理グループ] タブ

ネットワークエージェントは、以下のような一連の属性を持つサービスとしてコンピュータにインストールされます：

- サービス名が「**KLNAgent**」である
- 「カスペルスキーネットワークエージェント」という名前で表示される
- オペレーティングシステム起動時に自動的に起動する
- ローカルシステムアカウントを使用する

カスペルスキーネットワークエージェントサービスのプロパティ確認、起動、停止、および動作の監視は、Windows 管理ツールの [コンピュータの管理] → [サービス] を使用して行います。

4.1.4. 管理サーバインストールパッケージの作成と構成

インストールパッケージを説明付きのファイルとして作成する場合は、Kaspersky Administration Kit の配布パッケージのルートディレクトリにあるファイル **ak6.kpd** を選択します。

管理サーバインストールパッケージのプロパティは、[全般] タブ (図 19. を参照) と [OS 再起動] タブ (図 22. を参照) に表示されます。その他のプロパティは、管理サーバのデフォルト設定と同じです。

4.1.5. スレーブ管理サーバへのインストールパッケージ配布タスクの作成

スレーブ管理サーバへのインストールパッケージ配布のタスクを作成するには：

1. 必要な管理サーバに接続します
2. コンソールツリーの [グローバルタスク] ノードでショートカットメニューを開き、[新規作成] → [タスク] を選択するか、[操作] メニューの同様の項目を使用します。これによって、ウィザードが起動します。ウィザードの指示に従います
3. Kaspersky Administration Kit アプリケーションの場合は、[製品再インストールタスク] というタスクタイプを選択します
4. 次のウィザードウィンドウ (図 24. を参照) で、配布するインストールパッケージを選択します。以下のいずれかのオプションを選択します：
 - **すべてのインストールパッケージ** - すべてのインストールパッケージ
 - **選択されたインストールパッケージ** - 下の表で、必要なインストールパッケージの名前の横にあるボックスをオンにします

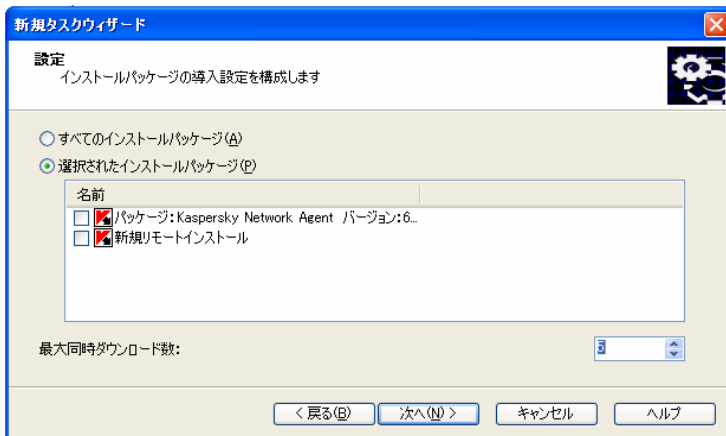


図 24. 一連のインストールパッケージの作成

[最大同時ダウンロード数] に、必要な値を指定します

5. 次のウィザードウィンドウ (図 25. を参照) で、インストールパッケージの配布先となるスレーブ管理サーバの横にあるボックスをオンにします

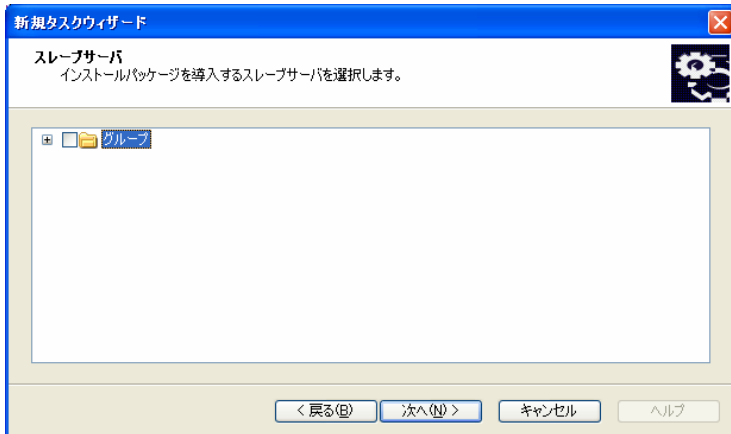


図 25. スレーブ管理サーバの選択

6. 次のウィザードウィンドウで、タスクの開始スケジュールを指定します (詳細については 53 ページの 4.1.7 項を参照)
7. ウィザードが完了したら、[終了] ボタンを押してウィザードを閉じます

4.1.6. ネットワークエージェントを使用したグループ内へのインストールパッケージの配布

インストールパッケージをグループ内に配布するには、更新エージェントを使用します。更新エージェントはインストールパッケージと更新を管理サーバから受信し、カスペルスキー製品のインストールフォルダに保存します。

更新とインストールパッケージを含むフォルダの場所は変更できません。また、フォルダのサイズも制限できません。

インストールパッケージは、後でマルチアドレス配信を使ってクライアント PC に配布されます。グループ内への新規インストールパッケージの配布は、一度しか実行できません。配布時にクライアント PC が企業の論理ネットワークに接続していない場合は、インストールタスクが実行されたときに、必要なインストールパッケージをネットワークエージェントが更新エージェントから自動的にダウンロードします。

更新エージェントのリストを作成し、グループ内のコンピュータにインストールパッケージを配布するようにエージェントを構成するには：

1. 必要な管理サーバに接続します

2. コンソールツリーの必要なグループでショートカットメニューを開き、[プロパティ] を選択するか、[操作] メニューの同様の項目を使用します
3. グループのプロパティウィンドウが開きます。[更新エージェント] タブ (図 26. を参照) で [追加] および [削除] ボタンを使用して、グループ内で更新エージェントとして機能するコンピュータのリストを作成します

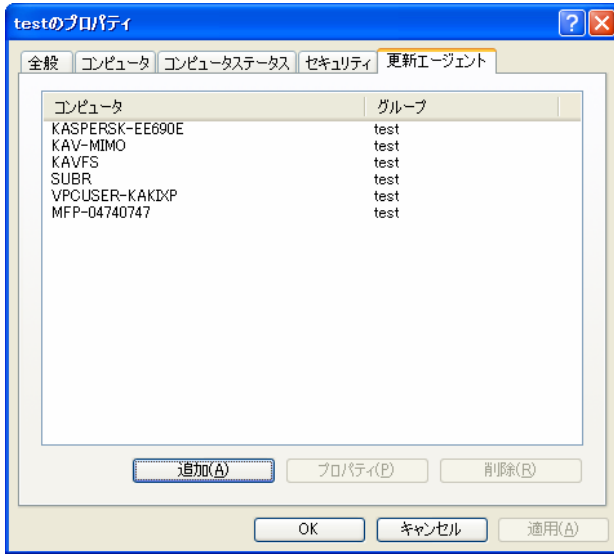


図 26. グループのプロパティウィンドウ -
[更新エージェント] タブ

4. 更新エージェントの設定を編集します。編集するには、リスト内でエージェントを選択し、[プロパティ] ボタンを押します。表示された [プロパティ <更新エージェント名>] ウィンドウ (図 27. を参照) で、以下の作業を行います：
 - 更新エージェントへの接続にクライアント PC が使用するポートの番号を指定する。デフォルトのポート番号は **14001** です。このポートが使用中である場合は、番号を変更できます
 - 更新エージェントへの SSL プロトコルを使った安全な接続にクライアント PC が使用するポートの番号を指定する。デフォルトのポート番号は **13001** です
 - [マルチキャストを使用する] ボックスをオンにし、[マルチキャスト IP] および [IP マルチキャストポート番号] フィールドに情報を入力する
5. [適用] または [OK] ボタンを押します

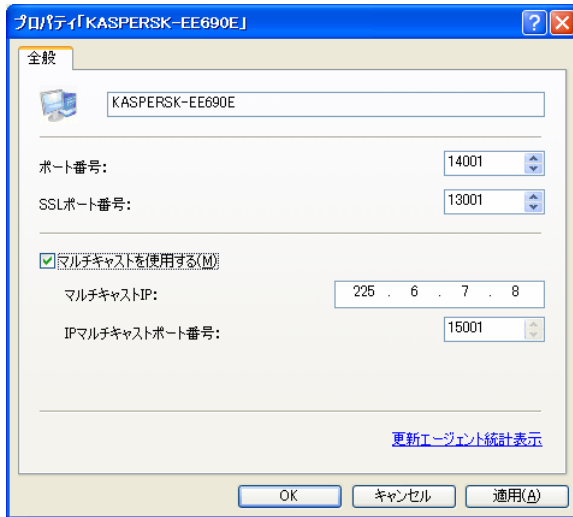


図 27. 更新エージェントのプロパティウィンドウ - リモートインストールタスクの作成

このタスクが実行されると、**[プッシュインストール]** または **[ログインスクリプトベースのインストール]** のいずれかを使用して、クライアント PC にソフトウェアがリモートインストールされます。

[プッシュインストール] を指定すると、論理ネットワーク内の特定のクライアント PC にソフトウェアをリモートインストールできます。タスクが実行されると、管理サーバはインストールに必要な一連のファイルを共有フォルダから各クライアント PC の一時フォルダにコピーし、各コンピュータ上でインストーラを起動します。強制インストールのタスクを正常に実行するには、管理サーバが論理ネットワーク内のクライアント PC に対するローカル管理者の権限を持っている必要があります。この方法は、この機能をサポートする Microsoft Windows NT/2000/2003/XP のコンピュータで使用できます。

管理サーバとクライアント PC の接続がインターネット経由で確立されている場合、またはファイアウォールによって保護されている場合は、共有フォルダを使ってデータを転送できません。この場合、クライアント PC へのアプリケーションのインストールに必要なファイルは、ネットワークエージェントによって配布されます。そのようなコンピュータにはネットワークエージェントをローカルにインストールする必要があります。

もうひとつの方法 (**ログインスクリプトベースのインストール**) では、特定のユーザ (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。タスクを実行すると、インストーラの起動に関する記録が、選択されたユーザのスタートアップシナリオに書き込まれます。インストーラアプリケーションは、管理サーバの共有フォルダに置かれています。タスクを正常に行うには、タスクが実行されるアカウントまたは管理サーバが、ドメインコントローラデータベースでスタートアップシナリオを変更する権限を持っている必要があります。ドメインにユーザを登録すると、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。

スタートアップシナリオを使用したリモートインストールのタスクを正常に行うには、シナリオを変更するユーザが該当のコンピュータに対するローカル管理者権限を持っている必要があります。

クライアント PC へのソフトウェアのリモートインストールに関するグローバルタスクは、強制的インストールでしか実行できません。グローバルタスクを作成する場合は、強制インストールとスタートアップシナリオを使用したインストールのいずれかを選択できます。

プッシュインストールを使用したリモートインストールのグローバルタスクを作成するには：

1. 必要な管理サーバに接続します
2. コンソールツリーの [グローバルタスク] ノードでショートカットメニューを開き、[新規作成] → [タスク] を選択するか、[操作] メニューの同様の項目を使用します。これによって、タスク作成ウィザードが起動します。ウィザードの指示に従います
3. タスク名を指定します
4. アプリケーションおよびタスクのタイプを選択するには、それぞれ「Kaspersky Administration Kit」および「製品導入タスク」を指定します (図 28. を参照)

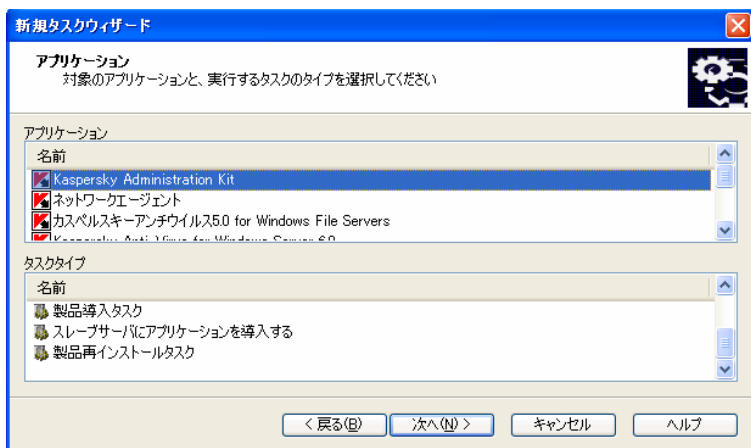


図 28. タスクタイプの指定

5. 続いて、このタスクを実行したときにインストールされるインストールパッケージを指定します (図 29. を参照)。特定の管理サーバに対して作成されたパッケー

ジから必要なものを選択するか、**[新規]** ボタンを使用して新規パッケージを作成します

Kaspersky Administration Kit を経由した管理をサポートする一部のアプリケーションは、コンピュータにローカルインストールしかできません。詳細については、該当するアプリケーションのマニュアルを参照してください。

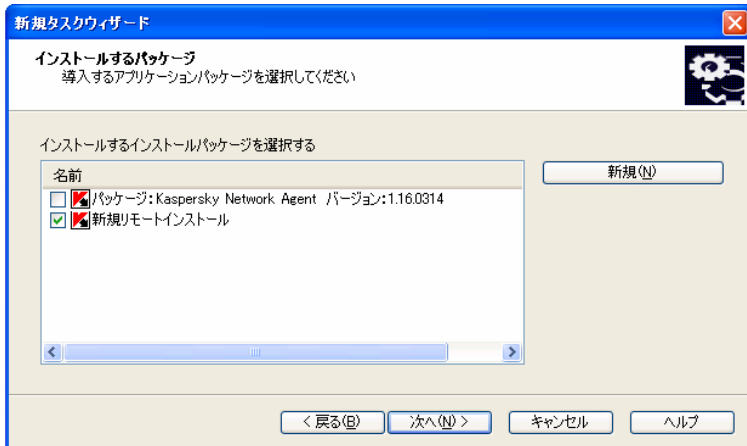


図 29. インストールするインストールパッケージの選択

6. ここでは、**[プッシュインストール]** オプションを選択します (図 30. を参照)

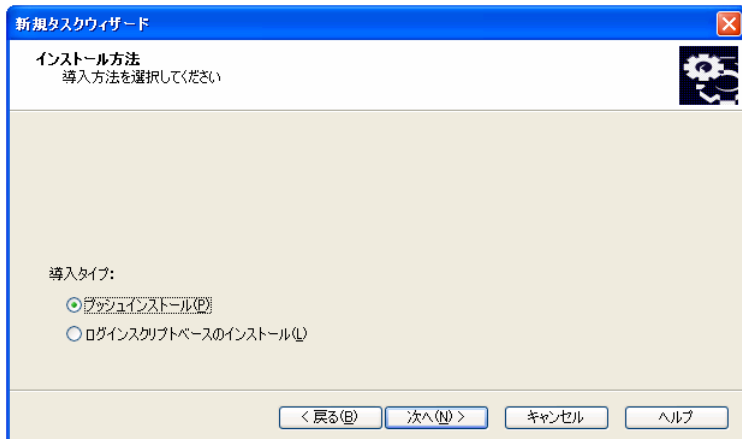


図 30. インストール方法の選択

7. このウィンドウ (図 31. を参照) では、追加のインストール設定を決定します：

- アプリケーションがすでにコンピュータにインストールされている場合、アプリケーションを再インストールするかどうか

インストールが繰り返されないようにするには、**[アプリケーションがすでにインストールされている場合インストールしない]** ボックスをオンにします。デフォルトではオンになっています。アプリケーションがローカルインストールされているコンピュータの場合、または予定されたリモートインストールタスクが以前に実行されている場合は、タスクが開始されません

このボックスがオフになっている場合、リモートインストールタスクは、最大試行回数に達するまでスケジュールに従って開始されます

- クライアント PC へのアプリケーションのインストールに必要なファイルの配布方法を指定する

指定するには、**[インストールパッケージの読み込み]** の各フィールドで以下のように指定します

- クライアント PC へのアプリケーションのインストールに必要なファイル転送を **Windows ツールと共有フォルダ** を使って行う場合は、**[Microsoft Windows の共有フォルダを使用する]** ボックスをオンにします。デフォルトではオンになっています
- 各コンピュータにインストールされているネットワークエージェントによってクライアント PC にファイルを配布するには、**[ネットワークエージェントを使用する]** ボックスをオンにします。デフォルトではオンになっています
- **[最大同時ダウンロード数]** に、Administration Sever から情報をダウンロード可能なクライアント PC の最大数を指定します
- スケジュールされたタスクが開始した場合のインストール試行回数を、**[再試行回数]** フィールドに指定します。インストールの最中にエラーが発生した場合は、インストールが繰り返し試みられます

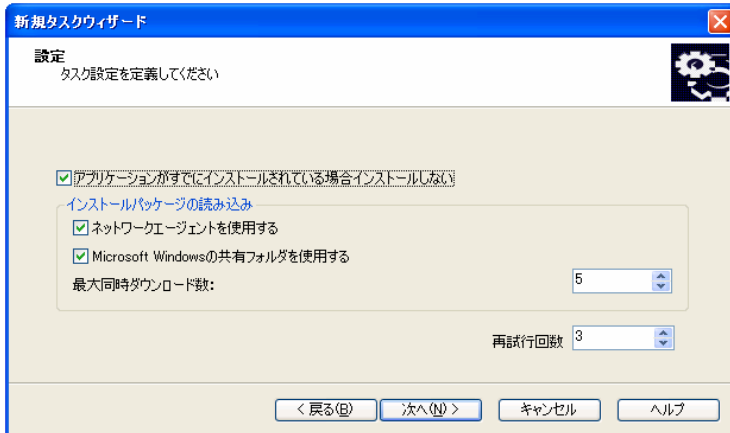


図 31. 追加のインストール設定

8. この手順 (図 32. を参照) では、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

管理サーバの負荷を削減するために、まとめてインストールすることをお勧めします。[ネットワークエージェントとともにインストールする] ボックスをオンにし、必要なインストールパッケージの名前の横にあるチェックボックスをオンにします。必要であれば、[作成] ボタンを使用して新規インストールパッケージを作成します

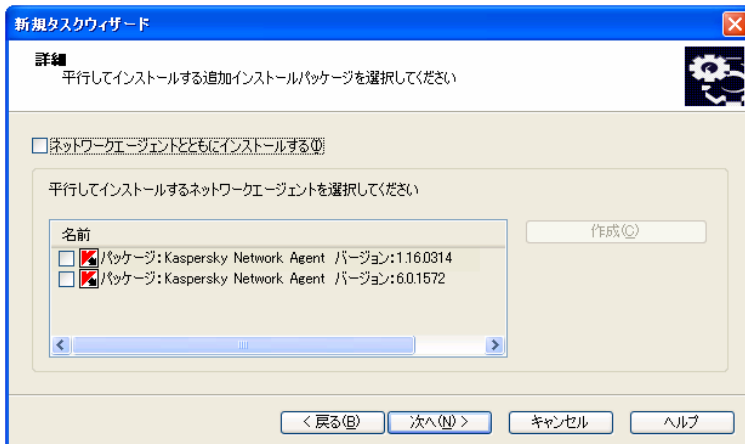


図 32. ネットワークエージェントとの同時インストールの選択

9. タスクが作成されるコンピュータの選択方法を決定します (図 33.を参照) :

- **Windows ネットワークを使用してコンピュータを選択します** - この場合、インストール対象のコンピュータは、管理サーバが受信した企業の Windows ネットワークのポーリングデータを基に選択されます
- **手動でコンピュータアドレス (IP、DNS または NetBIOS) を定義します** - この場合、インストール対象のコンピュータは手動で選択します

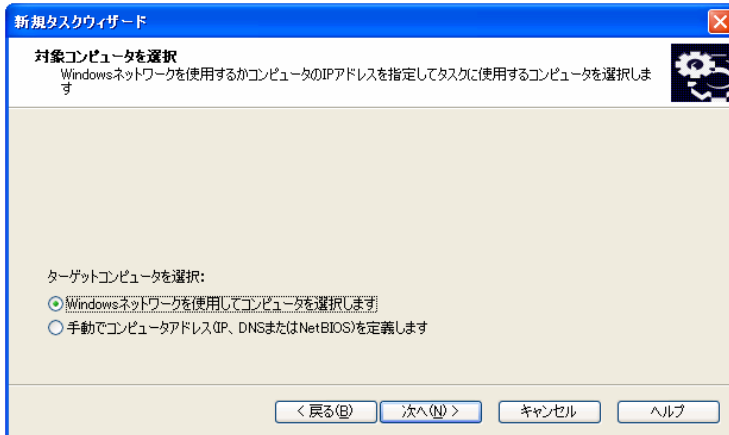


図 33. クライアント PC 選択に使用される方法の選択

Windows ネットワークのポーリングによって取得されたデータに基づいてコンピュータが選択されると、ウィザードウィンドウにリストが作成され (図 34. を参照)、コンピュータを論理ネットワークに追加する場合と同じ方法で実行されます。詳細については、『Kaspersky Administration Kit 参照ガイド』を参照してください。論理ネットワークのコンピュータ ([グループ] フォルダ)、または論理ネットワークに含まれていないコンピュータ ([ネットワーク] フォルダ) を選択できます。

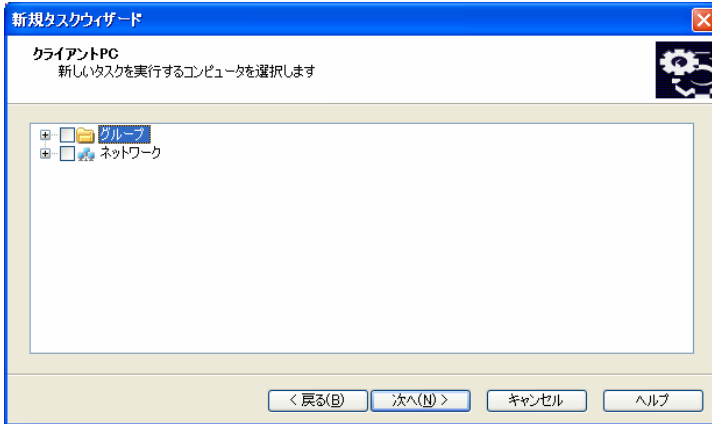


図 34. Windows ネットワークデータに基づいたインストール対象コンピュータリストの作成

コンピュータを手動で選択する場合は、コンピュータの NETBIOS 名または DNS 名、あるいは IP アドレス (または IP アドレスの範囲) を入力するか、各アドレスが行ずつ入力されたテキストファイルからリストをインポートすることで、リストを作成します (図 35. を参照)。

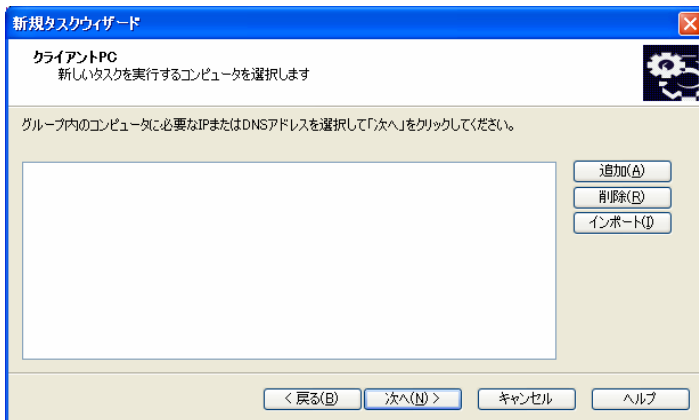


図 35. IP アドレスに基づいたインストール対象コンピュータリストの作成

10. 次のウィザードウィンドウでは、コンピュータ上で導入タスクが実行されるアカウントを指定します (図 36. を参照)

アカウントは、ソフトウェアのリモートインストールを予定しているすべてのコンピュータに対して管理者権限を持っている必要があります。

異なる管理サーバドメインに含まれるコンピュータにソフトウェアをインストールする場合は、そうしたドメインと管理サーバが動作しているドメインの間で信頼関係が確立されている必要があります。

以下のいずれかのオプションを選択します：

- **デフォルトアカウント** - 管理サーバがドメインユーザのアカウントで実行され (13 ページの3.2 項を参照)、このアカウントがソフトウェアのインストールに必要な権限を持っている場合
- **指定アカウント** - 管理サーバがシステムアカウントで実行されている場合、または管理サーバのアカウントが導入タスクの開始に必要な権限を持っていない場合

ドメインに含まれないコンピュータにソフトウェアをリモートインストールする場合は、それらのコンピュータに対して管理者権限を持つユーザのアカウントでリモートインストールタスクを開始してください。

下の各フィールドに、要件を満たすアカウントを所有するユーザの属性を指定します。

図 36. アカウントの選択

11. 続いて、タスク開始のスケジュールを作成します (図 37. を参照)

- **[実行予定]** ドロップダウンリストから、タスク開始モードを選択する
 - 手動

- **N 時間ごと**
 - **毎日**
 - **毎週**
 - **毎月**
 - **一回** - 導入タスクは、実行結果に関係なくコンピュータ上で一度だけ実行されます
 - **即時** - タスクが作成されてウィザードが完了した後、すぐに実行されます
- 選択したモードに従って、一連のフィールドでスケジュール設定を構成します。詳細については、『**Kaspersky Administration Kit 参照ガイド**』を参照してください

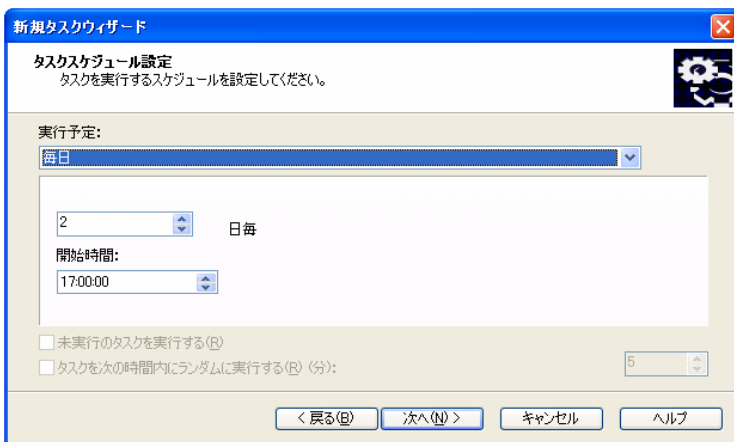


図 37. 毎日開始されるタスク

ログインスクリプトベースのグローバル導入タスクを作成するには：

1. 必要な管理サーバに接続します
2. コンソールツリーの [**グローバルタスク**] ノードでショートカットメニューを開き、**[新規作成]** → **[タスク]** を選択するか、**[操作]** メニューの同様の項目を使用します。これによって、タスク作成ウィザードが起動します。ウィザードの指示に従います
3. タスク名を指定します

4. アプリケーションおよびタスクのタイプを選択する場合は、それぞれ「**Kaspersky Administration Kit**」および「**製品導入タスク**」を選択します (図 28. を参照)
5. 次のウィンドウ (図 29. を参照) で、インストールに使用するインストールパッケージを指定します。指定方法は、強制的なインストールの場合と同じです (前述の説明を参照)
6. 続いて、[**ログインスクリプトベースのインストール**] オプションを選択します (図 30. を参照)
7. 次のウィザードウィンドウ (図 35. を参照) で、スタートアップシナリオを変更する必要があるユーザのアカウントを選択します

インストールタスクが開始されると、**Kaspersky Administration Kit** は、選択されたユーザ以外のユーザにスタートアップスクリプトが指定されていないかどうかをチェックします。指定されている場合、インストールは続行されません。エラー情報は、ログファイルに書き込まれます。

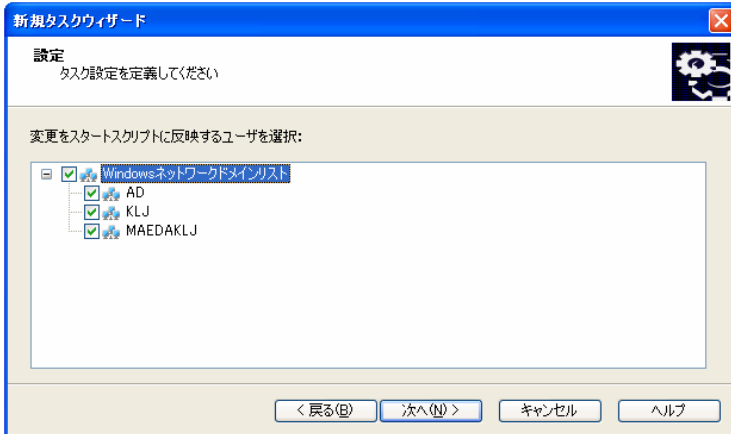


図 38. アカウントの選択

8. ウィザードの次の手順 (図 36. を参照) は、強制的なインストールの場合と同じです (前述の説明を参照)
9. **タスク**の開始スケジュール指定のウィンドウ (図 37. を参照) では、強制的なインストールの場合と同じ方法でスケジュールを作成します (前述の説明を参照)

ウィザードが完了すると、作成した導入タスクが [**グローバルタスク**] ノードに追加され、結果ウィンドウに表示されます。必要であれば、設定を変更できます (詳細については 53 ページの 4.1.7 項を参照)

作業を行うには：

コンソールツリーで **[リモートインストール]** ノードを選択し、結果パネルで必要なインストールパッケージを選択し、ショートカットメニューを開いて **[インストール]** コマンドを選択するかまたは **[操作]** メニューの同様の項目を使用します。これによって前述の導入タスク作成ウィザードが起動しますが、このウィザードにはタスクタイプとインストールパッケージの選択の手順が含まれません。ウィザードの指示に従います

また、グループ導入タスク作成ウィザードを起動することもできます。

作業を行うには：

コンソールツリーの **[グループタスク]** ノードで、ショートカットメニューを開いて **[アプリケーションのインストール]** コマンドを選択するか、**[操作]** メニューの同様の項目を使用します。これによって前述のグループ導入タスク作成ウィザードが起動しますが、このウィザードにはタスクタイプとコンピュータグループの選択の手順が含まれません。ウィザードの指示に従います

4.1.7. 導入タスクの構成

導入タスクは、その他のタスクと同じ方法で構成されます。詳細については『**Kaspersky Administration Kit 参照ガイド**』を参照してください。これ以降では、**[設定]** タブで指定したタスクタイプに固有の設定について詳しく説明します。

強制的なインストールを実行するタスクを編集する場合は、以下のことができます (図 39. を参照)。

- アプリケーションがすでにクライアント PC にインストールされている場合にアプリケーションを再インストールするかどうかを決定する
- クライアント PC へのアプリケーションのインストールに必要なファイルを配布するための方法を指定し、同時接続の最大数を指定する
- タスクがスケジュールに基づいて実行される場合は、インストール実行の試行回数を指定する

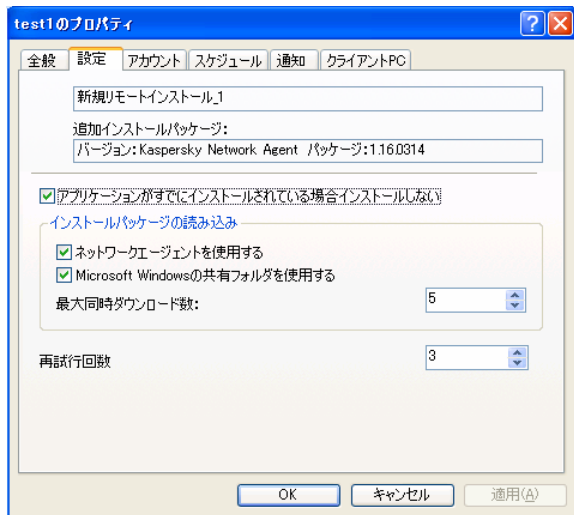


図 39. 導入タスクの構成 -
プッシュインストール

スタートアップシナリオを使用した導入タスクを構成する場合は、**[設定]** タブを使用して、スタートアップシナリオを変更するユーザーのアカウント一覧を変更できます (図 40. を参照)。リストを編集するには、**[追加]** ボタンと **[削除]** ボタンを使用します。

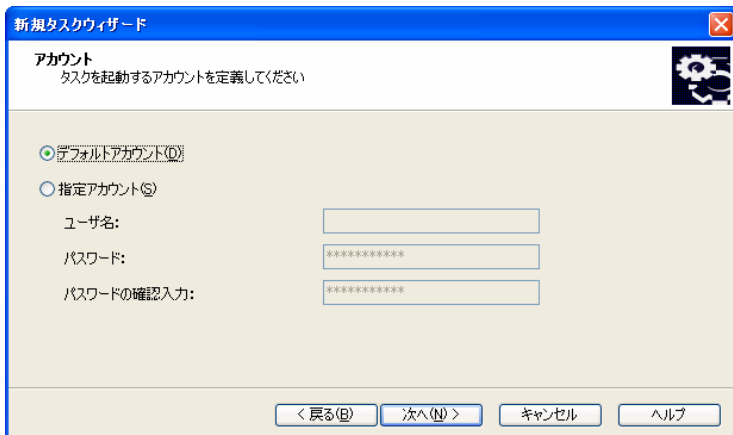


図 40. ログインスクリプトベース導入タスクの構成

4.1.8. スレーブ管理サーバへのアプリケーション導入

このタスクを使用して、スレーブサーバへのソフトウェアのインストールおよび更新を行うことができます。

タスクを作成する前に、すべてのサーバにインストールパッケージがあることを確認してください。パッケージをサーバに送信するには、**[製品再インストールタスク]**を使用します (4.1.5 項を参照)。

スレーブサーバへのアプリケーション導入タスクを作成するには：

1. 必要な管理サーバに接続します
2. コンソールツリーの **[グローバルタスク]** ノードでショートカットメニューを開き、**[新規作成]** → **[タスク]** を選択するか、**[操作]** メニューの同様の項目を使用します。これによって、タスク作成ウィザードが起動します。ウィザードの指示に従います
3. タスク名を指定します
4. アプリケーションおよびタスクタイプを選択するには、それぞれ「**Kaspersky Administration Kit**」および「**スレーブサーバにアプリケーションを導入する**」を指定します (図 28. を参照)
5. このタスクの実行によってインストールされるインストールパッケージを指定します
6. インストールが繰り返されないようにするには、**[アプリケーションがすでにインストールされている場合インストールしない]** ボックスをオンにします。デフォルトではオンになっています
7. この手順は、グローバルタスクでは利用できません。**[スレーブ管理サーバ]** を選択し (図 41. を参照)、スレーブサーバのリストを作成します

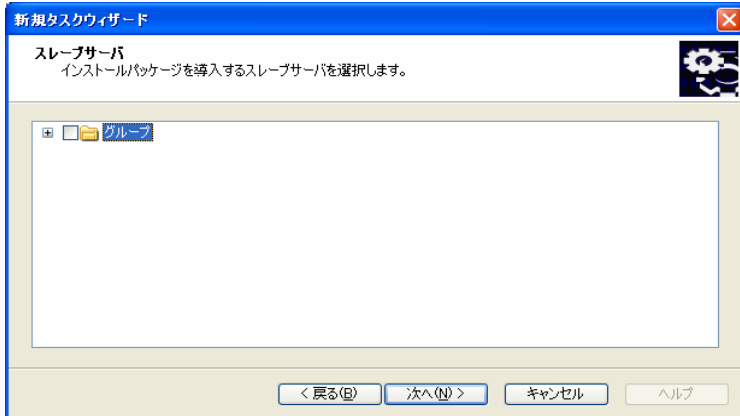
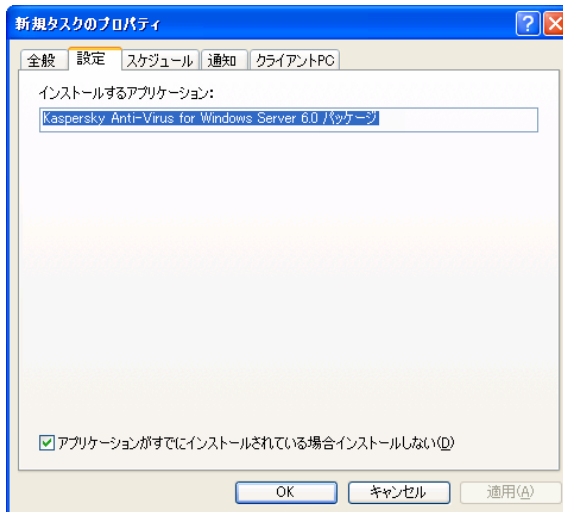


図 41. スレープ管理サーバのリストの作成

8. 続いて、タスク開始のスケジュールを作成します

図 42. スレープ管理サーバへのアプリケーション導入タスク
[設定] タブ

4.1.9. ソフトウェアのリモート削除

ソフトウェアをリモート削除するには：

導入タスクと同様の方法で、タスクを作成します (53 ページの 4.1.7 項を参照)。タスクタイプとして [製品アンインストールタスク] を選択し、[設定] ウィンドウの [アンインストールするアプリケーション] ドロップダウンリストからカスペルスキー製品を選択します (図 43. を参照)。サードパーティアプリケーションを削除する場合は、[外部アプリケーションをアンインストールする] をオンにして、削除するアプリケーションを選択します。

ドロップダウンリストには、ネットワークエージェントがコンピュータにインストールされた後に論理ネットワーク上で検知されたアプリケーションのリストが含まれます。

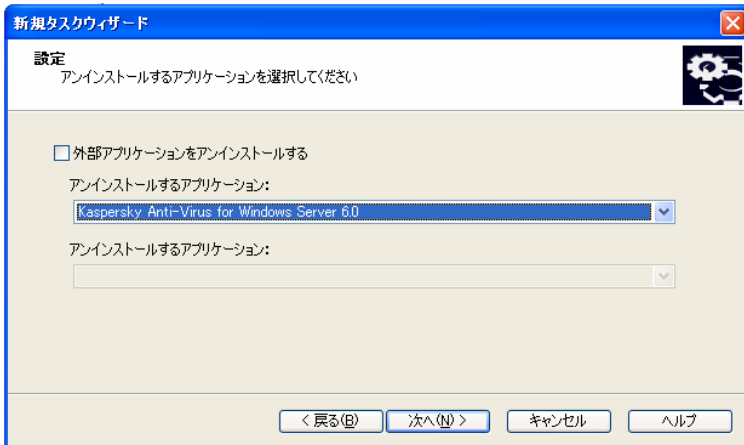


図 43. 削除するアプリケーションの選択

作成したタスクは、スケジュールに従って実行します。

4.2. 導入ウィザード

導入ウィザードを使用して、カスペルスキー製品をインストールできます。このウィザードでは、強制的なインストールによるアプリケーションの導入、作成したインストールパッケージを使用した導入、または配布パッケージから直接行われる導入を実行できます。

このウィザードでは、以下の作業を行います：

- アプリケーションインストール用のインストールパッケージの作成 (過去にそうしたパッケージがインストールされたことがない場合)。パッケージは、アプリケーションの名前とバージョンに一致する名前でも [リモートインストール] ノードに保管され、後でアプリケーションのインストールに使用できます

- グローバル導入タスクおよびグループ導入タスクの作成と開始。作成されたタスクは、タスクが作成されたグループの [グローバルタスク] または [グループタスク] に置かれ、後で手動で実行できます。タスクの名前は、アプリケーションのインストールパッケージの名前と一致します (<選択したインストールパッケージの名前> のインストール)

導入ウィザードを使用してアプリケーションをインストールするには：

1. 必要な管理サーバに接続します
2. Kaspersky Administration Kit アプリケーションのメインウィンドウのコンソールツリーで、必要な管理サーバに対応するノードを選択し、ショートカットメニューを開いて [導入ウィザード] を選択するかまたは [操作] メニューの同様のコマンドを選択します。これによって、ウィザードが起動します。ウィザードの指示に従います
3. 表示されたウィンドウ (図 44. を参照) で、インストールするインストールパッケージを指定します。配布パッケージからアプリケーションをインストールする場合またはインストールパッケージがまだ作成されていない場合、あるいはその両方の場合は、新規インストールパッケージを作成します。作業を行うには、[新規] ボタンを押します。インストールパッケージ作成ウィザードが開きます (29ページの 4.1.1 項を参照)

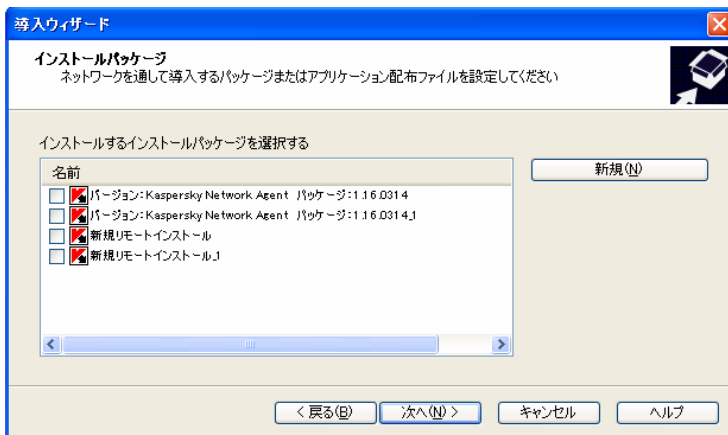


図 44. インストールパッケージの選択

4. 次のウィザードウィンドウで、必要であれば、一緒にインストールするネットワークエージェントのインストールパッケージを選択します (53 ページの 4.1.7 項を参照)

5. ウィザードウィンドウ (図 45. を参照) で、アプリケーションのインストール先となるコンピュータを決定します。作業を行うには、以下のいずれかを選択します：
- **アプリケーションを選択したコンピュータにインストールする** - このオプションをオンにすると、ウィザードが完了した後にグローバルアプリケーション導入タスクが作成されます
 - **アプリケーションを管理グループ上のコンピュータにインストールする** - ウィザードによって、グループタスクが作成されます

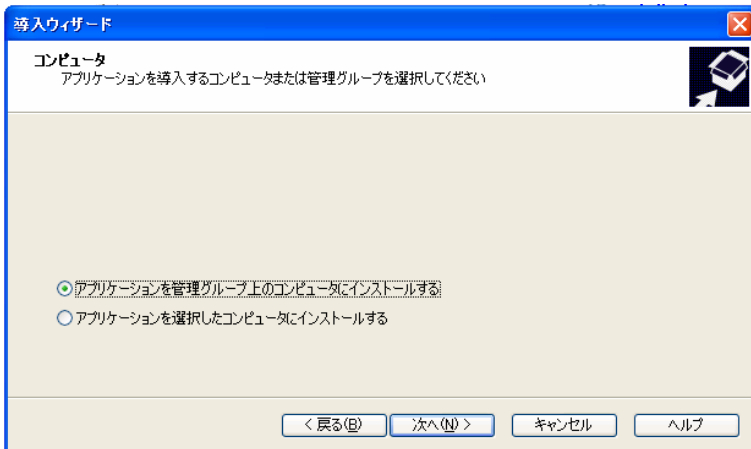


図 45. タスクタイプの選択

6. グループタスクを作成する場合は、アプリケーションのリモートインストール先のコンピュータグループを指定する (図 46. を参照) か、インストール先のコンピュータを選択します。論理ネットワーク内のすべてのクライアント PC にアプリケーションをインストールする必要がある場合は、[グループ] グループを選択します

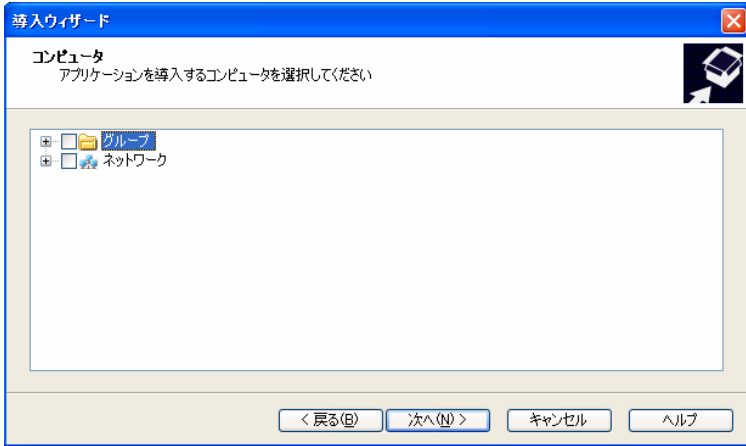


図 46. グループの選択

7. コンピュータ上で導入タスクが実行されるアカウントを決定します (詳細については 53 ページの 4.1.7 項を参照)

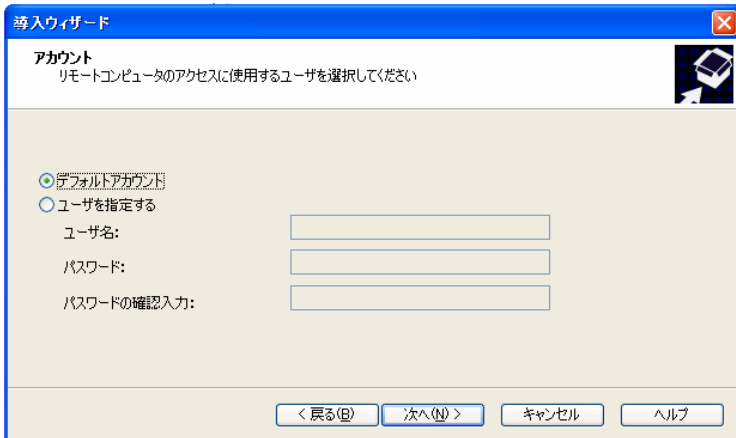


図 47. ユーザアカウントの選択

8. 続いて開くウィンドウには、選択したグループ内のコンピュータに対する導入タスクの配布と実行のプロセスが表示されます (図 48. を参照)。プロセスの完了を待たずに、ウィザードの最後のウィンドウに切り替えることができます。切り替えるには、[次へ] ボタンを押します。各コンピュータでのタスク実行結果に関する詳細情報は、[履歴] ボタンを使用して表示できます

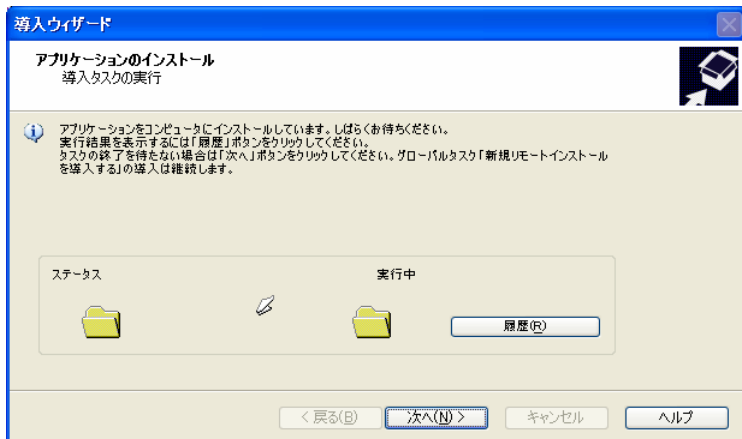


図 48. 導入タスクの実行

4.3. ソフトウェアのローカルインストール

ソフトウェアのローカルインストールは、各コンピュータ上で個別に実行されます。ローカルインストールを実行するには、ローカルコンソールに対する管理者権限が必要です。

Kaspersky Administration Kit を使用した管理をサポートする一部のアプリケーションは、リモートインストールに対応していません。詳細については、該当するアプリケーションのマニュアルを参照してください。

アンチウイルス保護システムをローカル導入する場合のソフトウェアインストールの一般的な手順は、以下のとおりです：

- ネットワークエージェントをインストールし、クライアント PC と管理サーバの間で接続を構成する (62ページの 4.3.1 項を参照)
- 該当するマニュアルの説明に従って、アンチウイルス保護システムに含まれる必須アプリケーションをコンピュータにインストールする
- インストールされているカスペルスキー製品のそれぞれに対する管理プラグインを、管理コンピュータにインストールする (67ページの 4.3.2 項を参照)

Kaspersky Administration Kit は、インストールパッケージ作成中に作成されたファイルに基づく非対話モードのローカルアプリケーションインストールをサポートしています (67ページの 4.3.3 項を参照)

4.3.1. ネットワークエージェントのローカルインストール

ネットワークエージェントをコンピュータにローカルインストールするには：

1. Kaspersky Administration Kit アプリケーション CD の **[NetAgent]** フォルダにある **setup.exe** (または **setup.msi**) を実行します。インストールプロセスは、ウィザードによってガイドされます。ウィザードでは、インストール設定を構成できます。ウィザードの指示に従います
2. インストールに必要なファイルが解凍され、ハードディスクへのファイルのコピー、ライセンス契約の承認が行われ、ユーザおよび企業に関する情報が表示されます
3. 続いて、ネットワークエージェントのインストールフォルダを定義する必要があります。デフォルトのインストールフォルダは、**Program Files\Kaspersky Lab\NetworkAgent** です。このフォルダがない場合は、フォルダが自動的に作成されます。フォルダを変更するには、**[参照]** ボタンを使用します
4. 次のウィザードウィンドウ (図 49. を参照) では、管理サーバに接続するためにネットワークエージェントが使用する設定を構成する必要があります。作業を行うには、以下の内容を定義します：
 - 管理サーバがインストールされている、またはインストールが予定されているコンピュータのアドレス。Windows ネットワーク内のコンピュータの IP アドレスまたは名前を、PC アドレスとして使用できます。また、**[参照]** ボタンを使用してコンピュータを選択することもできます
 - Kaspersky Anti-Virus 6.0 アンチハッカーで管理サーバの IP アドレスを入手するために使用される UDP ポート 137 を開く必要があるかどうか。必要であれば、**[AntiHacker で NetBIOS の名前解決を許可する]** をオンにします
 - 管理サーバへの接続でネットワークエージェントが使用するポート番号。デフォルトでは、ポート **14000** が使用されます。すでに割り当てられている場合は、変更できません。10 進表記しか使用できません
 - SSL プロトコルを使用した安全な管理サーバへの接続に使用されるポート番号。デフォルトでは、ポート **13000** が使用されます。すでに割り当てられている場合は、変更できません。10 進表記しか使用できません。接続で安全なポートを使用する (SSL プロトコルを使用する) には、**[SSL を使用してサーバに接続する]** ボックスをオンにします

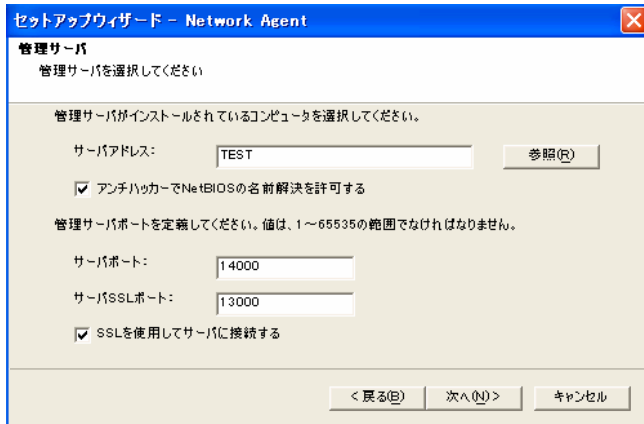


図 49. 管理サーバへの接続に使用される設定

5. ネットワークエージェントがプロキシサーバ経由でサーバに接続する (図 50. を参照) 場合は、対応する以下の接続設定を適用します：
- **[プロキシサーバを使用してカスペルスキー Administration Server に接続する]** ボックスをオンにし、プロキシサーバへの接続用の名前とポートを入力する。10 進表記しか使用できません (例：プロキシアドレス： proxy.test.com、ポート： 8080)
 - プロキシサーバへのアクセスにパスワードを使用する場合は、**[プロキシログイン]** フィールドと **[プロキシパスワード]** フィールドに情報を入力します

プロキシサーバを使用しない場合は、**[次へ]** ボタンを押してこの手順を省略します。

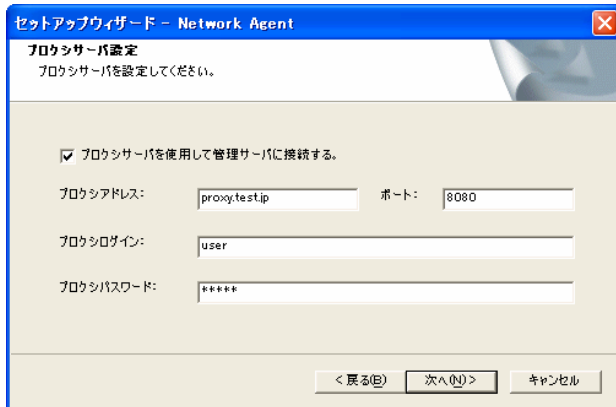


図 50. プロキシサーバ経由接続の設定の構成

6. 続いて、Windows ネットワークポーリングで管理サーバによって検知されたコンピュータが追加される **[ネットワーク]** グループのフォルダを決定します。以下のいずれかのオプションを選択します (図 51. を参照) :
- **デフォルトグループ名** - コンピュータは、このコンピュータの Windows ネットワークでの位置、つまりドメインまたはワークグループに対応するフォルダに追加されます (デフォルトのオプションです)
 - **グループ名を定義する** - PC は、**[グループ名]** フィールドで指定されたフォルダに追加されます。このオプションを選択した場合は、フォルダ名を入力します。**[ネットワーク]** グループ内にそのようなフォルダがない場合は、フォルダが作成されます。**[ネットワーク]** グループ内の既存フォルダの名前を指定することもできます

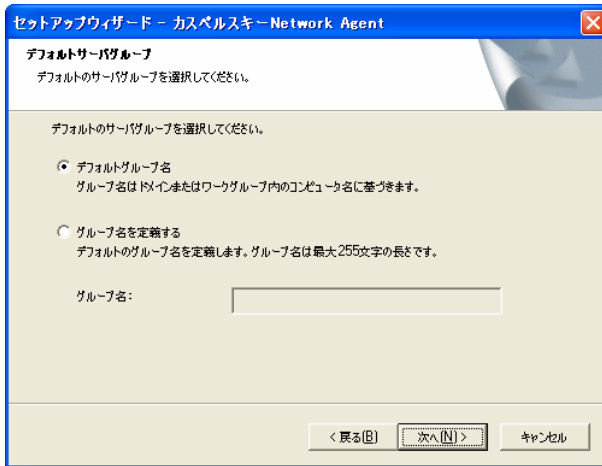


図 51. コンピュータを保管する [ネットワーク] フォルダ内グループの選択

7. 次のステップ (図 52. を参照) では、ネットワークエージェントが接続する管理サーバの証明書を受信する方法を指定する必要があります。以下のいずれかのオプションを選択します：

- **デフォルト証明書ファイル** - 管理サーバの証明書は、ネットワークエージェントが初めてサーバに接続したときに受信されます。これはデフォルトのオプションです
- **証明書ファイルを選択してください** - 管理サーバでの認証は、管理者が指定した証明書に基づいて行われます。このオプションを選択した場合は、使用する管理サーバの証明書を指定します

証明書ファイルは **.cer** という拡張子が付いており、管理サーバ上の **Kaspersky Administration Kit** インストールフォルダの **[Cert]** フォルダにあります。

証明書ファイルを共有フォルダまたはディスクにコピーし、これを使用してネットワークエージェントをインストールできます。

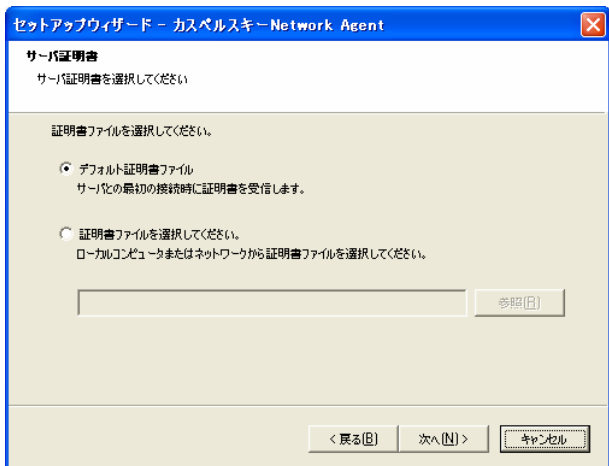


図 52. 管理サーバ証明書の受信に使用される方法の選択

8. 最後のウィザードウィンドウ (図 53. を参照) では、ウィザードの完了後すぐにネットワークエージェントを実行するかどうかを指定します。後で実行する場合は、デフォルトでオンになっている **[カスペルスキー Network Agent を起動]** ボックスをオフにします

ネットワークエージェントがインストールされているコンピュータのハードディスクを使用してディスクイメージを作成し、これを別のコンピュータに導入する予定である場合は、必ず **[カスペルスキー Network Agent を起動]** ボックスをオフにしてください。



図 53. ネットワークエージェントの起動の設定

ウィザードが完了すると、ネットワークエージェントがコンピュータにインストールされます。

カスペルスキーネットワークエージェントサービスのプロパティ確認、起動、停止、および監視は、Windows 管理ツールの [コンピュータの管理] → [サービス] を使用して行います。

Cisco Network Admission Control (NAC) と連動するためのプラグインは、常に管理エージェントとともにホストへ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。

4.3.2. アプリケーション管理プラグインのローカルインストール

アプリケーション管理プラグインをインストールするには：

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上で、アプリケーション配布 CD にある実行ファイル **klcfginst.exe** を実行します。このファイルは、Kaspersky Administration Kit 経由で管理されるすべてのアプリケーションに含まれています。インストールはウィザードによってガイドされ、設定は特に必要ありません。インストール設定を構成してインストールを開始します。

ネットワークエージェント用管理プラグインのファイル **klcfginst.exe** は、Kaspersky Administration Kit の配布パッケージの [NetAgent] フォルダにあります。

4.3.3. アプリケーションの非対話モードでのインストール

アプリケーションを非対話モードでインストールするには：

1. インストール対象アプリケーション用のインストールパッケージが作成されていない場合は、必要なインストールパッケージを作成します (4.1.1 項を参照)

インストールパッケージは、管理サーバのインストール時に管理サーバの [Packages] システムディレクトリにある共有フォルダに保存されます。サブフォルダは、各インストールパッケージに対応します。

2. インストールパッケージの設定を、必要に応じて構成します
3. 以下のいずれかの方法でアプリケーションをインストールします：

インストールパッケージに対応するフォルダ全体を、管理サーバからクライアントにコピーします。コピーされたフォルダをクライアント上で開き、/s スイッチを使用して実行ファイル (拡張子は .exe) を起動します

管理サーバ上のインストールパッケージ用共有フォルダに、クライアントからアクセスします。続いて、**/s** スイッチを使用して実行ファイルを起動します

4. 非対話モードでアプリケーションをインストールするコンピュータで、**/s** を使用してインストール対象アプリケーションの配布パッケージに含まれる **setup.exe** を実行します

インストールパッケージは、管理サーバのインストール時に指定された管理サーバ上の共有フォルダ (**[Packages]** フォルダ内) に保管されません。

Kaspersky Administration Kit を非対話的にインストールする場合は、アンサーファイルを使用できます。このファイルには、すべてのアプリケーションインストールパラメータが含まれており、同じパラメータを使用して何度でもアプリケーションをインストールできます。

Kaspersky Administration Kit のアンサーファイルを作成するには：

1. コマンドラインを使用して *Kaspersky Administration Kit* の配布パッケージを含むフォルダに移動し、**/r** スイッチと **/f1"<ファイルパス>%setup.iss"¹** スイッチを使用して実行ファイルを実行します（例：**setup.exe /r /f1"C:%setup.iss"**）
 - これによって、アプリケーションインストールウィザードがホストコンピュータ上で起動します。
2. ウィザードの指示に従って、アプリケーションのインストール設定を構成します。たとえば、管理サーバまたは管理コンソールのインストールだけを選択します

インストールが完了すると、選択したバージョンの *Kaspersky Administration Kit* がホストコンピュータにインストールされ、アンサーファイルが作成されて指定のディレクトリに置かれます。作成されたアンサーファイルは、管理サーバ上の該当するインストールパッケージのフォルダにコピーしてください。これによって、*Kaspersky Administration Kit* は、アンサーファイルに指定された設定に従って上記のいずれかの方法でインストールされます。

アンサーファイルは、*Kaspersky Administration Kit* を非対話的に更新するために使用できます。ただし、アンサーファイルの作成に使用されたアプリケーションバージョンの更新にしか使用できません。

¹ アンサーファイルへの完全なパスを指定する必要があります。

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をスキャンし、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がわっています。

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。

な

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 NT/2000/2003/XP 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。

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えただけです。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 - 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 形式のメールアドレス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리카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）を組み合わせて使用することで、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