

KASPERSKY LABS JAPAN

Kaspersky®
Administration Kit ver. 6.0

スタートガイド

KASPERSKY 株式会社

© Kaspersky Labs Japan

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

2008 年 1 月

目次

1 はじめに	3
2 使用の開始	5
2.1. MSDE 2000 の インストール	6
2.2. Kaspersky Administration Kit のコンポーネント のインストール	6
2.3. クイックスタートウィザード	7
2.4. 管理グループの作成	8
2.5. ネットワークエージェントのリモートインストール	9
2.6. カスペルスキー製品の導入	9
2.7. 更新タスク実行のチェック	10
2.8. 通知の設定	11
2.9. 通知システムとオンデマンドスキャンタスクの テスト	12
2.10. レポートの生成	12
3 KASPERSKY ADMINISTRATION KIT 5.X および 6.0 から 6.0 MP 1 への アップグレード	14
4 まとめ	15
付録 A. KASPERSKY LAB	16
A.1. 製品ラインナップ	16
A.2. お問い合わせ先	22

1 はじめに

このマニュアルでは、カスペルスキー製品に基づいたアンチウイルス保護システムを、**Kaspersky Administration Kit** を使用して企業ネットワーク全域に迅速かつ効率よくインストールするためにネットワークセキュリティ管理者が実行する必要のある、主な手順の概要を説明します。

このマニュアルでは、Microsoft Windows オペレーティングシステムが動作する数台のコンピュータに管理サーバ階層を使用せずにアンチウイルス保護をインストールする、簡単なシナリオについて説明します。インストールを正常に行うため、PC では次のオペレーティングシステムが動作している必要があります: Microsoft Windows 2000 Service Pack 1 以上、Microsoft Windows NT4 Service Pack 6a 以上、Microsoft Windows XP Professional Service Pack 1 以上、Microsoft Windows XP Professional x64 以上、Microsoft Windows Server 2003 以上、Microsoft Windows Server 2003 x64 以上、Microsoft Windows Vista、Microsoft Windows Vista x64。

また、カスペルスキー製品のバージョン 5.x からバージョン 6.x にアップグレードする方法についても説明します。

Kaspersky Administration Kit の詳細については、『Kaspersky Administration Kit 管理者用マニュアル』および『Kaspersky Administration Kit 参照ガイド』を参照してください。

Kaspersky Administration Kit 6 は、企業ネットワーク内のアンチウイルス保護システムを管理するために設計されています。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:

- 企業ネットワークのアンチウイルス保護を保障する論理ネットワークを作成する
- ネットワーク全域に対し、企業アンチウイルスアプリケーションの導入およびアンインストールを行う
- アンチウイルス保護システムを一ヶ所からリモート管理する
- ウイルス保護関係のイベントに関する通知を受信する
- すべての製品から統計とレポートを集積する
- インストールされているアンチウイルス製品のライセンスを管理する
- アンチウイルス製品によって隔離フォルダまたはバックアップストレージに置かれたオブジェクトを、中央で一元管理する

Kaspersky Administration Kit は、次のコンポーネントで構成されています:

- **管理サーバ** - 企業ネットワークにインストールされたカスペルスキー製品に関する情報を保管し、それら製品を一元管理します。管理サーバは、企業のアンチウイルス保護システムに関するすべてのデータを、MSDE 2000 データベース (Service Pack 3 以上)、Microsoft SQL Server 2000 (Service Pack 3 以上)、MySQL 5.0.32、Microsoft SQL 2005 以上、または Microsoft SQL 2005 Express 以上に保存します。管理サーバのインストールや動作を開始する場合は、データベースが企業ネットワークで動作している必要があります。MSDE 2000 (Service Pack 3) は、Kaspersky Administration Kit 6.0 を

使用してインストールできます。インストールするには、PC に Microsoft Data Access Components (MDAC) 2.8 以上がインストールされている必要があります

- **管理エージェント** - ネットワークホスト (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管理サーバと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に共通です。
- **管理コンソール** - サーバとエージェントの管理サービス用にユーザインターフェイスを提供します。管理コンソールは、Microsoft Management Console (MMC) プラグインとして実装されます

2 使用の開始

企業ネットワークを取り巻く効果的な保護システムを構築するには、次の手順に従います：

Microsoft Data Access Components (MDAC) 2.8 以上をインストールします。このコンポーネントが企業ネットワークにすでにインストールされている場合は、インストールする必要はありません

MSDE 2000 SP 3 以上(6 ページの 2.1 項を参照)、Microsoft SQL 2000 SP 3 以上、MySQL 5.0.32、Microsoft SQL 2005 以上、または Microsoft SQL Express 以上をインストールします。いずれかのデータベースサーバがネットワークにすでにインストールされている場合は、この手順を省略してください

管理サーバと管理コンソールをインストールします (6 ページの 2.2 項を参照)

クイックスタートウィザードを使用して、アンチウイルス保護システムの初期設定を構成します(7 ページの 2.3 項を参照)

管理グループが作成されていない場合は、クイックスタートウィザードを使用して作成します (8 ページの 2.4 項を参照)。管理グループを使用すると、ポリシーやグループタスクを適用することで一連のクライアント PC を 1 つの構成要素として管理できます

アンチウイルスアプリケーションと管理サーバがやりとりできるように、ネットワークエージェントをクライアント PC にリモートインストールします(8 ページの 2.5 項を参照)

企業ネットワークのアンチウイルス保護を確実に実施し、カスペルスキーAdministration Kit を通じた管理をサポートするために、選択したクライアントPCにリモートインストールします(9 ページの 2.6 項を参照)。これらの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、この手順は必要ありません

管理サーバがウイルス定義データベースの更新をインターネットからダウンロードするように設定し、その操作が正常に行われるかどうかを検証します。クライアント PC 上でデータベースが正常に更新されていることを確認してください(10 ページの 2.7 項を参照)

クライアント PC 上のウイルス関連イベントのイベントを管理者に通知するオプションを設定します(11 ページの 2.8 項を参照)

クライアント PC 上でオンデマンドスキャンを実行し、通知タスクがクライアント PC 上で実施されたかどうかをチェックします(11 ページの 2.9 項を参照)。

アンチウイルス保護およびカスペルスキー製品が検知したウイルスの数についてのレポートを表示します(11 ページの 2.10 項を参照)

上記の手順が正常に完了すると、企業ネットワーク向けの信頼できるアンチウイルス保護システムが構築されます。

これ以降の項では、これらの手順について詳しく説明します。

2.1. MSDE 2000 のインストール

MSDE 2000 SP 3、Microsoft SQL Server 2000 SP 3、MySQL 5.0.32、Microsoft SQL 2005 以上、または Microsoft SQL 2005 Express 以上が企業ネットワークにすでにインストールされている場合は、この手順を省略してください。

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 (配布パッケージは Microsoft の Web サイトから入手可能)。

Kaspersky Administration Kit に含まれるパッケージから MSDE 2000 をインストールするには：管理サーバデータベースをインストールするコンピュータを選択します。通常は、管理サーバとデータベースは同じコンピュータにインストールします

Kaspersky Administration Kit 6.0 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、ローカルで実行します

セットアップウィザードの指示に従います

すべてのインストール手順を実施すると、選択したコンピュータに MSDE 2000 SP 3 がインストールされます。MSDE 2000 SP 3 は、管理の必要がありません。

管理サーバは、MSDE 2000 SP 3 または SQL Server 2000 SP 3 を使用してアンチウイルス保護データを中央のデータベースに保存します。

管理サーバデータは、Kaspersky Administration Kit に付属している **klbackup** ユーティリティを使用するか、管理サーババックアップのグローバルタスクを使用してバックアップできます。詳細については『管理者用マニュアル』を参照してください。

2.2. Kaspersky Administration Kit のコンポーネントのインストール

インストール手順では、**管理サーバ**、**Kaspersky Posture Validation Server for Cisco NAC**、**管理エージェント**および**管理コンソール**のうちから、必要なコンポーネントを選択できます。管理エージェントとコンソールは、オプションではありません。常にインストールされます。Kaspersky Lab Posture Validation Server for Cisco NAC は、Cisco Network Admission Control と統合する場合の標準のカスペルスキーコンポーネントであり、このマニュアルでは扱いません。デフォルトでは、すべてのコンポーネントがインストールされます。

必要であれば、管理コンソールを別のコンピュータにインストールし、ネットワーク経由で管理サーバを管理できます。

管理サーバまたは管理コンソール、あるいはその両方をインストールするには：

コンポーネントをインストールするコンピュータを選択します。ネットワークに Windows ドメイン構造がある場合は、そのドメインのメンバーに管理サーバをインストールすることをお勧めします

Kaspersky Administration Kit 6.0 (Maintenance Pack 1) またはコンソール、あるいはその両方は、管理サーバまたはコンソールあるいはその両方のバージョン 5.x または 6.0 が動作するのと同じホストにインストール可能です

製品をインストールする場合には、ドメイン管理者権限を持っている必要があります。これによって、**KLAdmins** グループと **KLOperators** グループが自動的に作成され、管理サーバが動作する予定のアカウントに対する必要な資格情報が準備できます

Kaspersky Administration Kit インストール CD の setup.exe ファイルを実行します

ウィザードの指示に従います

このコンピュータ上での管理サーバが動作するサービスアカウントとして、ドメイン管理者アカウントを選択します。

2.3. クイックスタートウィザード

アンチウイルス保護設定を初期設定するには：

[スタート] → [プログラム] → [カスペルスキー Administration Kit] → [カスペルスキー Administration Kit] の順に選択して、管理コンソールを起動します

コンソールツリーの [管理サーバ] ノードをクリックして管理サーバに接続します。サーバ証明書を承認します

ショートカットメニューを開き、[クイックスタートウィザード] を選択します。

管理サーバがネットワークを検索し、ネットワーク上のすべてのコンピュータを検知し終わるまで待ちます

次のいずれかの方法で、管理グループを作成します：

- 数台のテストコンピュータだけを扱う場合は、[**手動で論理ネットワークを作成**] を選択してテスト用クライアント PC を手動でグループに追加します
- 企業ネットワーク内のすべてのホストに製品を導入する場合は、管理グループを自動的に作成できます。[**Windows ネットワークに基づく論理ネットワークを作成**] を選択します。これによって、Microsoft Windows ドメインおよびワークグループに基づいて論理ネットワークが作成されます。管理グループは、Microsoft Windows ドメインおよびワークグループに一致します

カスペルスキー製品によるメール通知および NET SEND 通知の送信に関するオプションを指定します。これらの設定は、管理サーバのプロパティの一部として編集できます。詳細については、『管理者用マニュアル』を参照してください

アンチウイルス製品のポリシーを作成するプロセスと、企業ネットワークにおけるアンチウイルス保護システムの正しく動作を規定する複数のタスクを実行します。Kaspersky Administration Kit 6 では、グループポリシーを使用して、グループ内のすべてのコンピュータに設定を一律に適用します。タスクとは、グループ内のすべてのコンピュータにインストールされているアンチウイルス製品によって実行される動作です

次のオブジェクトが作成されます：

- デフォルト設定の Kaspersky Anti-Virus for Windows Workstation 5.0 および 6.0 用の上位レベルポリシー。ポリシー設定は、後で表示して修正でき

ます。ポリシーに加えた変更をクライアント PC に適用し、ユーザがこの設定を変更できないようにするには、 を使用します

- 管理サーバをインターネットから更新するグローバルタスク

定義データベースとプログラムモジュールに対する更新がカスペルスキーのアップデートサーバからダウンロードされ、管理サーバのインストール時に指定した共有フォルダに保存されます。クライアント PC は、この共有フォルダから更新を取得します。より柔軟にクライアント PC が更新を受け取れるように、スレーブ管理サーバおよび更新エージェントに更新を配布する方法を後で使用できます。詳細については、『管理者用マニュアル』を参照してください。カスペルスキーのアップデートサーバから更新を受け取る場合の設定を更新するには、**[プロパティ]** ボタンをクリックします

- クライアント PC 上のウイルス定義データベースを更新するための上位レベルのグループタスクが、デフォルト設定で作成されます (Kaspersky Anti-Virus for Windows Workstation 5.0 および 6.0)。クライアント PC は、共有フォルダから更新を取得するように設定されます
- クライアント PC のオンデマンドスキャンタスクが、デフォルト設定で作成されます (Kaspersky Anti-Virus for Windows Workstation 5.0 および 6.0)

管理サーバによる更新受け取りのタスクをすぐに開始するか、スケジュールに従って実行するかを指定します

最後のウィンドウでは、クイックスタートウィザードの終了後すぐに導入ウィザードを開始するかどうかを指定します

2.4. 管理グループの作成

新規グループを論理ネットワーク構造に追加するには：

コンソールツリーまたは詳細ウィンドウ枠の **[グループ]** フォルダで、新規グループを追加するグループを選択します。ショートカットメニューを開き、**[新規作成]** → **[グループ]** の順に選択します。新規グループの名前を入力し、**[OK]** をクリックします

カット&ペーストまたはドラッグ&ドロップを使用して、選択したクライアント PC を **[ネットワーク]** グループから新規グループに移動します。または、ポップアップメニューで **[新規作成]** → **[コンピュータ]** の順に選択し、表示されたウィザードに従います

管理グループに移動する一連のコンピュータをいくつかの基準に基づいて検索するには、**[コンピュータを検索]** コマンドまたは **[操作]** メニューの同様のコマンドを使用します。詳細については、『管理者用マニュアル』を参照してください。

Kaspersky Administration Kit 5.x および 6.0 をバージョン 6.0 (Maintenance Pack 1) に更新する方法については、14 ページの 3 章を参照してください

2.5. ネットワークエージェントのリモートインストール

管理エージェントは、単独で導入されるか、必要なアプリケーションとともに導入されます。ここでは、管理エージェントのインストールのみについて説明します。必要なバージョンのアンチウイルス製品がすでにクライアントにインストールされている場合に便利です。

ネットワークエージェントをリモートから導入（インストール）するには：

管理コンソールのショートカットメニューから、アプリケーション導入ウィザードを実行します

クイックスタートウィザードによって作成されたネットワークエージェントインストールパッケージを選択します。このパッケージは管理サーバのインストール時に作成され、ネットワークエージェントが管理サーバへの接続に使用する設定が含まれています

ネットワークエージェントのインストール先となるコンピュータを含む管理グループのコンピュータを選択します

リモートインストール設定を構成します

必要であれば、クライアント PC にアクセスするためのアカウントを入力します。管理サーバのサービスアカウントが選択したクライアント PC に対する管理者権限を持っていない場合は、デフォルトアカウントを使用します

ウィザードの次の手順では、選択したクライアント PC へのネットワークエージェント導入に関するグループタスクが作成されて実行されます。ウィザードウィンドウでは、タスク実行の結果がリアルタイムに表示されます

タスクが完了すると、タスクの結果が表示されます。アプリケーション導入ウィザードを終了します

管理サーバがいつでもネットワークエージェントと接続を確立可能であるためには、クライアント PC で UDP ポート 15000 が開いている必要があります。この UDP ポートが開けない場合は、クライアント PC の設定に使用する **<コンピュータ名>のプロパティ** ダイアログボックスの **[全般]** タブにある **[管理サーバから切断しない]** ボックスをオンにします

インストールが正常に行われたことを確認するには、ネットワークエージェントをインストールしたコンピュータのいずれかでショートカットメニューの **[プロパティ]** オプションをクリックします。**[アプリケーション]** タブで、カスペルスキーネットワークエージェントのステータスが **[実行中]** であることを確認します。

導入が正常に行われたけれどもネットワークエージェントが管理サーバに接続できない場合は、kinagchik.exe ユーティリティを使用します。このユーティリティはネットワークエージェント配布キットに含まれており、エージェントのインストール後には、ネットワークエージェントのインストールルートフォルダに置かれています。コマンドラインから実行すると、このユーティリティは、管理サーバの接続設定を詳しく診断します。このユーティリティの詳細については、『参照ガイド』を参照してください。

2.6. カスペルスキー製品の導入

ここでは、Kaspersky Anti-Virus for Windows Workstation のリモートからのインストールに焦点を当てます。その他カスペルスキー製品の導入も、ここで説明される内容と同じです。

Kaspersky Administration Kit 経由の管理に対応する一部のカスペルスキー製品は、クライアント PC 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、特定アプリケーションのガイドを参照してください。

ネットワークに接続しているコンピュータに *Kaspersky Anti-Virus for Windows Workstation* をリモートから導入するには:

ウィザードを使用して、*Kaspersky Anti-Virus for Workstations 6* のパッケージを作成します。ウィザードは、**[リモートインストール]** ノードのショートカットメニューを使用して起動します

インストールパッケージの作成に必要な **.kpd** ファイルは、*Kaspersky Anti-Virus for Workstations* 配布ファイルのルートに置かれています。*Kaspersky Anti-Virus for Workstations* のライセンスキーファイルも、このルートディレクトリに置かれています。*Kaspersky Anti-Virus for Workstations* の動作に使用されるライセンスキーファイルを指定します

必要であれば、インストールパッケージの設定を構成します。クライアント PC の自動的に再起動を有効にすることをお勧めします

管理サーバのショートカットメニューから、アプリケーション導入ウィザードを実行します

ネットワークエージェントの場合と同様に、インストールパッケージから *Kaspersky Anti-Virus for Workstations* をインストールします (9 ページの 2.5 項を参照)。*Kaspersky Anti-Virus for Workstations* とともに、ネットワークエージェントもインストールできます

リモートインストールは、*Kaspersky Anti-Virus 5.x for Workstations* が動作しているホストで実行できます。これによって、*Kaspersky Anti-Virus 5.x* は自動的に削除され、*Kaspersky Anti-Virus 6.0* に置き換えられます

インストールが正常に行われたことを確認するには、アプリケーションをインストールしたクライアント PC を選択し、プロパティウィンドウを開きます。**[アプリケーション]** タブを開き、*Kaspersky Anti-Virus for Workstations 6* のステータスが **[実行中]** であることを確認します。**[タスク]** タブには、*Kaspersky Anti-Virus for Workstations 6* によって実行されたリアルタイム保護タスクが表示されています。

2.7. 更新タスク実行のチェック

クライアント PC が正常に更新を受け取ったことを確認するには:

コンソールツリーの上位レベルにある **[タスク]** ノードから、管理サーバ上で更新タスクを実行します。このタスクは、クイックスタートウィザードによって自動的に作成されます。カスペルスキーのアップデートサーバから更新がダウンロードされ、管理サーバのインストール時に指定した共有フォルダに保存されます。タスクが完了するまでお待ちください

[履歴] ボタンをクリックしてタスクの結果を表示します

ダウンロードされた更新のリストを見るには、コンソールツリーの **[更新]** ノードをクリックします

更新手順の詳細については、カスペルスキーの Web ページ (<http://www.kaspersky.co.jp/>) を参照してください。

グループ更新タスクを、クライアント PC 上で実行します。このタスクはクイックスタートウィザードによって作成され、[グループ] ノードの [グループタスク] フォルダに保管されます。タスクが完了するまでお待ちください

[履歴] ボタンをクリックしてタスクの結果を表示します

クイックスタートウィザードによって作成されたタスクは、ネットワークエージェントと管理サーバの接続を使用してクライアント PC を更新します。次のクライアント PC 更新方法もサポートされています：




- 管理サーバの共有フォルダから更新する
- メイン管理サーバの共有フォルダから更新する (サーバ階層が使用されている場合)
- カスペルスキーのアップデートサーバから更新する
- FTP または HTTP サーバを使用して更新する

共有フォルダから最新の更新をコピーするには、このフォルダに対する読み取り権限をクライアント PC が持っている必要があります。なんらかの理由でコピーできない場合は、FTP または HTTP サーバを使用して更新をクライアント PC に導入できます。管理サーバがダウンロードした更新を保存する共有フォルダの中にある **[更新]** サブフォルダにリンクする FTP または HTTP ディレクトリを作成します (例: `ftp://admserver/updates`)。クライアント PC 上で実行する更新タスクの更新ソースとして、このフォルダ (`ftp://admserver/updates`) を指定します。


2.8. 通知の設定

ウイルス保護関連のイベントに関する通知を設定するには：

アンチウイルス製品 (Kaspersky Anti-Virus for Workstations など) の上位レベルポリシーのプロパティから、**[イベント]** タブを開きます

このタブで、通知対象とするイベントを指定し、通知の送信方法を選択します。適切な列をオンにし ( - メール、  - NET SEND 機能、  - 実行ファイルの実行)、イベントプロパティウィンドウの **[通知]** タブの設定を構成します

通知システムをテストするには (12 ページの 2.9 項を参照)、**[感染の可能性のあるオブジェクトの検知]** および **[ウイルス、ワーム、トロイの木馬、ハッキングツールの検知]** イベントに関する通知を設定するのが適切です

設定を変更できないようにするために、クライアント PC すべてに  を使用します。変更内容を適用するには、**[実施]** タブに移動して **[詳細]** リンクをクリックし、表示されたウィンドウで **[今すぐ更新]** をクリックします

手動でメッセージを送信することで、設定した内容を確認できます。確認するには、イベントプロパティウィンドウの **[通知]** タブで **[テスト]** ボタンを押します。テスト通知のウィンドウが開きます。エラーが発生した場合は、詳細情報のウィンドウが表示されます

2.9. 通知システムとオンデマンドスキャンタスクのテスト

通知システムとオンデマンドスキャンタスクをテストするには:

保護されたコンピュータに、**Eicar** テストウイルスをコピーします。リアルタイム保護タスクが実行中であると、ウイルスをコピーできません。ウイルスが検知されたという通知が受信され、コンソールツリーの **[イベント]** ノードにこのイベントが記録されます

Eicar「テストウイルス」は、PC に損害を与えるようなコードを含まないため、実際にはウイルスではありません。ただし、ほとんどのアンチウイルス製品は、このファイルをウイルスとみなします。この「テストウイルス」は、**EICAR** の公式サイト (http://www.eicar.org/anti_virus_test_file.htm) からダウンロードできます。

クライアント PC 上で、リアルタイムのウイルス保護タスクを停止します。**Eicar** テストウイルスをクライアント PC にコピーしてから、リアルタイム保護タスクをもう一度有効にします

クライアント PC グループに対し、オンデマンドスキャンのグループタスクを実行します。eicar.com ファイルが検知され、対応する通知が送信されます。このイベントの記録が、コンソールツリーの **[イベント]** ノードに記録されます

2.10. レポートの生成

管理サーバに保存されている Kaspersky Administration Kit のイベントログデータから、アンチウイルス保護システムの現況に関するレポートを生成できます。事前に設定されたレポートテンプレートには、コンソールツリーの **[レポート]** ノードからアクセスできます。

次のレポートタイプに対応する 13 種類の標準テンプレートがあります。

- 定義データベースバージョンレポート
- エラーレポート
- ライセンスレポート
- 最も感染したクライアントレポート
- ウイルス保護レポート
- ソフトウェアバージョンレポート
- ウイルスアクティビティレポート
- 外部アプリケーションレポート
- ネットワーク攻撃レポート
- アプリケーションタイプのサマリレポート
- ワークステーションおよびファイルサーバ保護製品のサマリレポート
- 境界防御製品のサマリレポート

- メールシステム保護製品のサマリレポート

たとえば、対応するテンプレートを使用してウイルスアクティビティレポートを作成する場合は、Kaspersky Administration Kit によって記録されたすべてのウイルス発生に関する情報が含まれます。

ネットワークエージェントがインストールされていないコンピュータを管理グループに追加すると、PC の保護のレポートには、グループ内の 1 台のコンピュータが保護されていないことを示す情報が含まれます。

3 KASPERSKY ADMINISTRATION KIT 5.X および 6.0 から 6.0 MP 1 への アップグレード

ここでは、Kaspersky Administration Kit 5.x または 6.0 をバージョン 6.0 (Maintenance Pack 1) にアップグレードする手順について説明します。これによって、Kaspersky Anti-Virus for Windows Workstation 5.x および 6.x と Kaspersky Anti-Virus for Windows Server 5.x および 6.x の論理ネットワークが作成されます。一部の手順は、前の章ですでに説明してあります。ここでは、継ぎ目のない移行方法を順を追って説明します。

一般的な移行シナリオは、次のとおりです：

インストールされている Administration データを、**klbackup.exe** ユーティリティを使用してバックアップします。このユーティリティは Kaspersky Administration Kit に付属しており、管理サーバーコンポーネントのインストール後にはインストールルートディレクトリにコピーされます。管理サーバーを完全に復元するにはサーバー証明書が必要である点に注意してください。この設定は、**klbackup.exe** ユーティリティで必須です。

管理サーバ 6.0 (Maintenance Pack 1) は、企業ネットワークにインストールされます。管理サーバ 5.x または 6.0 がすでに動作中であるホストにインストールできます。バージョン 5.x および 6.0 がバージョン 6.0 (Maintenance Pack 1) に更新されると、すべての管理サーバまたはコンソールあるいはその両方のデータと設定が保存され、新規バージョンで使用できるようになります。

5.x および 6.x アプリケーションの管理グループの論理ネットワーク構造を作成します。

論理ネットワーク上の 5.x および 6.x アプリケーションのポリシーとグループタスクを作成します。必要なアンチウイルス保護設定を構成し、ウイルス保護関連イベントの処理に関するルールを設定します。

バージョン 5.x からバージョン 6.x に移行するコンピュータを指定します。

5.x および 6.x アプリケーションのインストールパッケージを作成し、選択したコンピュータに 5.x および 6.x アプリケーションをインストールします。これによって、以前のバージョンのアンチウイルス製品が削除され、アップグレードされた製品がインストールされます。

バージョン 5.x および 6.x のアンチウイルス製品をインストールしたコンピュータに、管理サーバ 6.0 (Maintenance Pack 1) の論理ネットワークを追加します。

これまでバージョン 5.x および 6.x のアンチウイルス製品に基づいて構築されていたアンチウイルス保護が、段階的に Kaspersky Administration Kit 6.0 (Maintenance Pack 1) プラットフォームへと移行されます。

4 まとめ

Kaspersky Administration Kit 6 は、このマニュアルで取り上げた内容以外にも、さまざまな管理機能を備えています。このマニュアルでは Kaspersky Administration Kit 6 を取り上げ、アプリケーションの使用を開始する方法と、アンチウイルス保護システムをネットワーク接続したコンピュータへ導入する方法を紹介しています。このシナリオでは、管理者が次の作業を実行できるように、信頼できる保護システムの構築に関連した基本的な問題を取り扱っています。

- アンチウイルス保護管理システムを導入して構成する
- アンチウイルス製品をクライアント PC に一ヶ所から導入する
- アンチウイルス保護ポリシーを定義する
- クライアント PC 上で更新タスクを作成し、動作をテストする
- リアルタイム保護タスクの動作をテストする
- クライアント PC に対してオンデマンドスキャンタスクを作成し、テストする
- 緊急イベント後の通知送信に関するルールを設定する
- アンチウイルス保護システムによってレポートを作成し、表示する

付録 A. 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、ベネルックス 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。

A.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のスキャンします。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り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。

A.2. お問い合わせ先

ご意見やご質問がありましたら、カスペルスキーラ布斯.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