

KASPERSKY LABS JAPAN

---

# Kaspersky<sup>®</sup> Anti-Virus for Linux File Server 5.7

管理者マニュアル



© Kaspersky Labs Japan

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

2008 年 1 月

## 目次

第 1 章 はじめに .....	4
1.1. コンピュータウイルスとマルウェア .....	4
1.2. Kaspersky Anti-Virus の目的と主な機能 .....	5
1.3. バージョン 5.7 の新機能.....	5
1.4. システム要件 .....	6
1.5. ユーザサポート.....	6
1.6. このガイドで使用される表記規則.....	7
第 2 章 製品の機能.....	8
第 3 章 KASPERSKY ANTI-VIRUS の インストール.....	10
3.1. Linux が動作するコンピュータへのアプリケーション導入 .....	10
3.2. インストール手順 .....	10
3.3. インストール後の設定.....	10
3.4. ネットワークエージェントのインストール.....	11
3.5. ネットワークエージェントの設定 .....	12
3.6. バージョン 5.7 へのアプリケーション更新 .....	12
3.7. アプリケーションファイルの場所.....	12
第 4 章 KASPERSKY ANTI-VIRUS の使用 .....	15
4.1. 定義データベースの更新 .....	15
4.1.1. 定義データベースの自動更新 .....	16
4.1.2. 定義データベースのオンデマンド更新 .....	17
4.1.3. 定義データベース保存用ディレクトリの作成 .....	17
4.2. アンチウイルスによるファイルシステムの保護 .....	18
4.2.1. スキャン対象 .....	19
4.2.2. オブジェクトのスキャンと感染駆除のモード.....	20
4.2.3. オブジェクトに対して実行する操作 .....	20
4.2.4. 個別ディレクトリのオンデマンドスキャン .....	21
4.2.5. スケジュールスキャン .....	22
4.2.6. 追加機能: スクリプトファイルの使用.....	22
4.2.6.1. アーカイブ内にある感染オブジェクトの感染駆除 .....	22
4.2.6.2. 管理者への通知 .....	22
4.3. リアルタイムのアンチウイルス.....	23
4.4. ライセンスキーの管理.....	24
4.4.1. ライセンスキー詳細の表示 .....	25
4.4.2. ライセンスの更新 .....	25
第 5 章 追加設定 .....	27
5.1. Webmin を使用した製品管理の設定 .....	27

---

5.2. Kaspersky Anti-Virus の動作の最適化 .....	27
5.3. 隔離ディレクトリへのオブジェクト移動 .....	29
5.4. 感染オブジェクトのバックアップ .....	30
5.5. 日時形式のローカライズ .....	30
5.6. Kaspersky Anti-Virus のレポート作成設定 .....	31
第 6 章 KASPERSKY ADMINISTRATION KIT を使用したアプリケーション管理 .....	33
6.1. アプリケーションの管理 .....	34
6.1.1. アプリケーション設定の構成 .....	35
6.2. タスクの管理 .....	36
6.2.1. タスクの作成 .....	36
6.2.2. タスク設定の指定 .....	40
6.2.3. タスクの開始と停止 .....	41
6.3. ポリシーの管理 .....	41
6.3.1. ポリシーの作成 .....	41
6.3.2. ポリシー設定の表示と編集 .....	43
第 7 章 KASPERSKY ANTI-VIRUS の アンインストール .....	46
第 8 章 KASPERSKY ANTI-VIRUS の動作確認 .....	47
付録 A. 追加情報 .....	48
A.1. Kaspersky Anti-Virus 設定ファイル .....	48
A.2. kavscanner コンポーネントのコマンドラインパラメータ .....	55
A.3. kavscanner コンポーネントのリターンコード .....	58
A.4. kavmonitor コンポーネントのコマンドラインパラメータ .....	59
A.5. licensemanager コンポーネントのコマンドラインパラメータ .....	59
A.6. licensemanager コンポーネントのリターンコード .....	60
A.7. keepup2date コンポーネントのコマンドラインパラメータ .....	60
A.8. keepup2date コンポーネントのリターンコード .....	61
A.9. kavmiddleware コンポーネントのコマンドラインパラメータ .....	61
付録 B. よくある質問 .....	62
付録 C. カスペルスキーラプス .....	66
C.1. 製品ラインナップ .....	66
C.2. お問い合わせ先 .....	69
付録 D. ソフトウェア使用許諾契約書 .....	70

## 第 1 章 はじめに

コンピュータユーザの数が増え、メールやインターネットトラフィックが増加する中で、悪意あるコンピュータプログラム（マルウェア）によるウイルス感染やデータの破損/盗難の脅威が増え続けています。

マルウェアの主な拡散ルートには以下のものがあります。

### インターネット

全世界的な情報ネットワークは、あらゆるタイプのマルウェアの主な拡散ルートです。一般に、ウイルスやその他悪意あるプログラムは、有益なソフトウェアまたはフリーウェアであるかのように偽って、人気のあるインターネットサイトに置かれます。マルウェアがスクリプト内に埋め込まれ、ブラウザへ Web サイトがロードされるときに自動的に実行することもあります。

### メールメッセージ

ユーザのメールボックスに配信されてメールデータベースに保管されるメールメッセージには、ウイルスが含まれていることがあります。マルウェアは、メッセージ本文に埋め込まれているか、添付ファイルとしてメールに添付されます。一般的に、感染したメールにはウイルスまたはメールワームが含まれており、メールを開いたりハードディスクに添付ファイルを保存したりすると、コンピュータ内のデータが感染するおそれがあります。

### ソフトウェアの脆弱性

ハッカーによる攻撃は、多くの場合、「ソフトウェアのセキュリティホール」を利用して行われます。こうした脆弱性を通じてハッカーがコンピュータへリモートアクセスし、結果的にデータや LAN リソースやその他情報が不正アクセスを受けます。

Unix ベースのシステムをターゲットにしたウイルスは、特性上、Windows OS を狙ったものほど数は多くありません。かといって、Unix ユーザに対する脅威を無視することはできません。以下のセクションでは、マルウェアのタイプについて詳しく見ていきます。

## 1.1. コンピュータウイルスとマルウェア

コンピュータに対する潜在的な脅威を把握するには、悪意あるソフトウェア（マルウェア）のタイプと機能について知っておくことが大切です。一般的に、悪意あるプログラムは 3 つのカテゴリに分かれます。

- **ワーム** - ネットワークリソースを利用して自己拡散する、悪意あるプログラム。これらのプログラムは、ネットワークやメール、その他の経路を通じてコンピュータからコンピュータへと伝播する能力を持つことから「ワーム」と呼ばれています。この伝播能力によって、ワームは非常に短期間で拡散します。

ワームの拡散は、コンピュータへの侵入、近隣にあるコンピュータの IP アドレスの確認、自己コピーの作成および近隣コンピュータへの送信、という段階を経て行われます。ネットワークアドレスとは別に、メールクライアントアプリケーションのアドレス帳に含まれるデータが利用されることが多々あります。ワームはディスク上に作業ファイルを作成する場合がありますが、感染コンピュータでメモリ以外のリソースを使用しなくても機能することができます。

- **ウイルス** - 自分のコードを他のプログラムのコードに追加することで感染し、感染したファイルが実行されたときに動作を掌握するプログラム。単純化していえば、ウイルスの主な動作はコンピュータプログラムに感染することです。ウイルスは、ワームよりも感染速度が多少遅めです。

- **トロイの木馬** - 感染したコンピュータで不正な動作を見せるプログラム。状況によって、ハードディスクの情報の消去、システムのフリーズ、機密情報の盗用などを行います。厳密に言えば、トロイの木馬はプログラムやデータに感染するわけではないので、ウイルスではありません。単独でコンピュータに侵入することはできず、なんらかの「有益な」ソフトウェアを装って配信されることがほとんどです。しかし、トロイの木馬がもたらすダメージは、通常のウイルス攻撃よりもはるかに大きい場合があります。

最近では、Unix ベースのシステムに見られるマルウェアのタイプとしては、ワームとトロイの木馬が大多数を占めるようになりました。



このマニュアルではこれ以降、「ウイルス」はウイルス、トロイの木馬、ワームを指す用語として使用します。特定タイプのマルウェアについては、必要な箇所の説明を加えていきます。

## 1.2. Kaspersky Anti-Virus の目的と主な機能

**Kaspersky Anti-virus® for Linux File Server** (以降、「Kaspersky Anti-Virus」または「アプリケーション」と表記) は、Linux オペレーティングシステムが動作するファイルサーバを保護するための製品です。

Kaspersky Anti-Virus for Linux には以下の機能があります：

- ファイルシステムを悪性コードからリアルタイムに保護 - ファイルへのアクセスをフックして分析し、感染オブジェクトの感染駆除または削除を行います
- オブジェクトのオンデマンドスキャン - 感染ファイルおよび感染が疑われるファイル（指定したスキャン範囲内のファイルなど）のスキャン、ファイルの分析、感染オブジェクトの感染駆除または削除を行います
- 疑わしいオブジェクトおよび破損オブジェクトの隔離 - 感染が疑われるファイルを隔離フォルダに保存します
- 感染オブジェクトに重要な情報が含まれている場合にオブジェクトを復元できるように、オブジェクトのコピーをバックアップストレージ内に作成してからオブジェクトの感染駆除または削除を行います
- 定義データベースの更新 - データベースはカスペルスキーのアップデートサーバから更新されます。ローカルフォルダから更新するように設定することもできます
- アプリケーション設定ファイル、Webmin、Kaspersky Administration Kit を使用して Kaspersky Anti-Virus の管理と設定を行います

## 1.3. バージョン 5.7 の新機能

**Kaspersky Anti-Virus for Linux File Server 5.7** では、以下の機能が新たに追加されました。

- Kaspersky Administration Kit を使用した Kaspersky Anti-Virus の設定と管理に対応

## 1.4. システム要件

Kaspersky Anti-Virus の動作要件は以下のとおりです：

- 必要なハードウェア：
  - Intel Pentium<sup>®</sup> プロセッサ、133 MHz 以上
  - 64 MB RAM
  - ハードディスク空き容量 100 MB (アプリケーションのインストール用、一時ファイル保管用)
- 必要なソフトウェア：
  - いずれかの 32 ビットプラットフォーム：
    - RedHat Enterprise Linux Advanced Server 4 UPD4
    - Fedora Core 6
    - SUSE Linux Enterprise Server 10
    - openSUSE Linux 10.2
    - Debian GNU/Linux 3.1 (r4)
    - Mandriva 2007
  - いずれかの 64 ビットプラットフォーム：
    - RedHat Enterprise Linux Advanced Server 4 UPD4
    - Fedora Core 6
    - SUSE Linux Enterprise Server 10
- openSUSE Linux 10.2. Webmin プログラム ([www.webmin.com](http://www.webmin.com)) - Kaspersky Anti-Virus のリモート管理用
- Perl 5.0 以上 ([www.perl.org](http://www.perl.org))
- which ユーティリティ
- ソフトウェアコンパイル用のパッケージ (gcc、binutils、glibc-devel、make、ld) およびカーネルソース (kavmonitor コンポーネント用)



Kaspersky Anti-Virus は SELinux に対応していません。SELinux を使用すると、さまざまな警告がログファイルに書き込まれます。






## 1.5. ユーザサポート

Kaspersky Anti-Virus の登録済みユーザは、各種サポートを受けることができます。

販売代理店までお問い合わせください。

## 1.6. このガイドで使用される表記規則

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

書式	意味/用途
太字	メニュー名、メニュー項目、ウィンドウ、ダイアログボックス、ダイアログの要素など
 注	追加情報、注釈
 注意	重要な情報
 実行するには...: 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。
 タスク、例	問題の提起、アプリケーションの機能を示す例
 ソリューション	タスクの実施方法
<b>[修飾子]</b> - 修飾子の目的	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

## 第 2 章 製品の機能

Kaspersky Anti-Virus は複数のアプリケーションモジュールで構成されており、各モジュールはコンピュータを保護するための固有の機能を持っています。

Kaspersky Anti-Virus には以下の機能があります：

- kavscanner - オンデマンドでウイルススキャンを行うコンポーネント
- kavmonitor - リアルタイムでウイルススキャンを行うコンポーネント
- keepup2date - 定義データベース更新を行うモジュール
- licensemanager - ライセンスキー管理用ユーティリティ
- kavmiddleware - Kaspersky Administration Kit を使用したリモート管理用のユーティリティ
- Webmin アプリケーションと連動するリモート管理モジュール

ここでは、リアルタイム保護を基にして (kavmonitor コンポーネントを例にとりて) アプリケーションのアルゴリズムについて詳しく見ていきます。

このコンポーネントは以下のように動作します：

1. コンピュータ上のアプリケーションがファイルシステムオブジェクトにアクセスしてファイルのオープン、実行またはクローズを試みると、その呼び出しが kavmonitor のカーネルモジュールによってフックされ、ファイルはウイルススキャンされます
2. フックされたファイルは、kavmonitor コンポーネントに付属しているデーモンアプリケーションを使って処理されます。このデーモンは、設定ファイルの指定に基づいて、ウイルスや悪質なプロセスがないかどうかオブジェクトをスキャンします。感染駆除オプションが選択されている場合は定義データベースを使用して駆除が行われるなど、いくつかの処理方法があります
3. ファイルが処理されると、kavmonitor は、ファイルステータスを規定するアクセスコード (allowed/prohibited) をカーネルモジュールに送信します
4. kavmonitor コンポーネントは、オブジェクトのステータスに基づいてファイルへのアクセスを許可またはブロックします。アクセスがブロックされると、ファイルへのアクセスを要求しているアプリケーションは、アクセスが拒否されたことを示すエラーコードを受け取ります

スキャンおよび処理では、以下のいずれかのファイルステータスが割り当てられます：

- **Clean** - オブジェクトは感染していません
- **Infected** - オブジェクトは感染しています
- **Cured** - 感染オブジェクトは正常に感染駆除されました
- **CureFailed** - 感染オブジェクトを駆除できませんでした
- **Warning** - オブジェクトコードが既知のウイルスのコードと似ています
- **Suspicion** - オブジェクトは未知のウイルスに感染している疑いがあります
- **Protected** - オブジェクトが暗号化されているためスキャンできません
- **Corrupted** - オブジェクトが破損しています
- **Error** - オブジェクトスキャン中にシステムエラーが発生しました

---

各ステータスのオブジェクトに対する処理は、設定ファイルでの指定内容に基づいて行われます。詳細については付録 A を参照してください。

## 第 3 章 KASPERSKY ANTI-VIRUS のインストール

Kaspersky Anti-Virus のインストール前に、以下の作業をお勧めします：

- 使用するシステムが Kaspersky Anti-Virus のハードウェア要件とソフトウェア要件を満たしていることを確認する (1.4 項を参照)
- インターネット接続を設定する
- **root** としてログインする

### 3.1. Linux が動作するコンピュータへのアプリケーション導入

Linux OS 向け Kaspersky Anti-Virus は、以下の形式で提供されています：

- **.rpm** - RPM パッケージマネージャ対応システム向け
- **.deb** - Debian ベースの OS ディストリビューション向け



Kaspersky Anti-Virus のインストールを .rpm パッケージから開始する場合は、コマンドラインで以下のように入力します：

```
# rpm -i <distribution_package_filename>
```



Kaspersky Anti-Virus のインストールを .deb パッケージから開始する場合は、コマンドラインで以下のように入力します：

```
# dpkg -i <distribution_package_filename>
```

### 3.2. インストール手順

インストール手順は 2 つのステージに分かれています。最初のステージは以下のステップで構成されています：

1. kluser ユーザと klusers グループの作成
2. 配布パッケージからインストール先コンピュータへのファイル解凍
3. 必要なサービスの登録 (ホストシステムによって異なる)
4. 製品コンポーネントの設定ファイルの各種デフォルト設定の指定

### 3.3. インストール後の設定

インストール後の設定は、Kaspersky Anti-Virus セットアップの第 2 ステージです。製品の設定を開始するには、`/opt/kaspersky/kav4fs/lib/bin/setup` ディレクトリにある `postinstall.pl` スクリプトを使用します。



**Debian** が動作するコンピュータへのインストール中に、このスクリプトが自動的に起動されます。

スクリプトが起動したら、以下のステップを実行します：

1. ライセンスキーファイルへのパスを指定します
2. インターネット接続用に、プロキシサーバのパラメータを以下の形式で設定します：

```
http://<IP of the proxy server>:<port>
```

または

```
http://<user_name>:<password>@<IP of the proxy server>:  
<port>,
```

プロキシ認証の必要があるかどうかに従って、上記のいずれかを選択してください。アプリケーション更新コンポーネント (`keepup2date`) は、この値を使用してカスペルスキーのサーバに接続し、定義データベースの更新をダウンロードします

インターネット接続でプロキシを使用しない場合は、パラメータを **no** に設定します

3. カスペルスキーのサーバから定義データベースをダウンロードします。**yes** または **no** を入力して、すぐに更新を行うかどうかを指定します
4. Webmin との通信を設定します
5. `kavmonitor` モジュールのコンパイルを開始します。このステージでは、`kavmonitor` の動作に必要なライブラリをコンパイルします。カーネルソースがデフォルトディレクトリにない場合は、以下のように入力して `kavmonitor` コンポーネントをコンパイルします：

```
# /opt/kaspersky/kav4fs/src/kavmon.pl -b [PATH]
```

[PATH] は、カーネルソースへのパスを表します

## 3.4. ネットワークエージェントのインストール

Kaspersky Administration Kit を使用してアプリケーションをリモート管理する場合は、ネットワークエージェントをインストールする必要があります。



ネットワークエージェントのインストールを `.rpm` パッケージから開始する場合は、コマンドラインで以下のように入力します：

```
# rpm -i <distribution_package_filename>
```



ネットワークエージェントのインストールを `.deb` パッケージから開始する場合は、コマンドラインで以下のように入力します：

```
# dpkg -i <distribution_package_filename>
```

## 3.5. ネットワークエージェントの設定

インストールが終了したら、ネットワークエージェントが Kaspersky Administration Kit と正しく通信できるように設定する必要があります。設定を開始するには、`/opt/kaspersky/klagent/lib/bin/setup` ディレクトリにある `postinstall.pl` スクリプトを使用します。



Debian が動作するコンピュータへのインストールを実行している間、このスクリプトは自動的に起動されます。スクリプトが起動したら、以下のステップを実行します：

自分の管理サーバの DNS 名または IP アドレスを指定します

1. 管理サーバのポート番号を指定します
2. 管理サーバの SSL ポート番号を指定します
3. データ転送に SSL 接続を使用するかどうかを決定します
4. デフォルト管理グループの名前を指定します

## 3.6. バージョン 5.7 へのアプリケーション更新



アップグレード処理は、バージョン 5.5-27 で正常に機能します。

アップグレードの前に、`kavmonitor` サービスを停止します。コマンドラインで以下のように入力してください：

```
# /etc/init.d/kav4fs stop
```



Kaspersky Anti-Virus のアップグレードを `.rpm` パッケージから開始する場合は、コマンドラインで以下のように入力します：

```
# rpm -U <distribution_package_filename>
```



Kaspersky Anti-Virus のアップグレードを `.deb` パッケージから開始する場合は、コマンドラインで以下のように入力します：

```
# dpkg -i <distribution_package_filename>
```

アップグレード手順が完了すると、製品の設定ファイルがバージョン 5.5 から 5.7 に置き換わります。設定ファイルには、必要な修正を手作業で加えてください。

## 3.7. アプリケーションファイルの場所



Kaspersky Anti-Virus 関連のファイルは、デフォルトで以下の場所に置かれます：

/etc/opt/kaspersky/ - Kaspersky Anti-Virus 設定ファイルが含まれるディレクトリ

kav4fs.conf - 設定ファイル

/opt/kaspersky/kav4fs/ - Kaspersky Anti-Virus のメインディレクトリ。以下の内容が含まれます：

/bin/ - Kaspersky Anti-Virus コンポーネントの実行ファイルが置かれるディレクトリ

kav4fs-kavscanner - アンチウイルスコンポーネントの実行ファイル

kav4fs-keepup2date - 定義データベース更新コンポーネントの実行ファイル

kav4fs-licensemanager - ライセンスキー管理コンポーネントの実行ファイル

/lib/ - Kaspersky Anti-Virus の補助ファイルが含まれるディレクトリ

/setup/ - アプリケーション設定に必要なスクリプトが含まれるディレクトリ

postinstall.pl - インストール後の製品設定で使用するスクリプト

uninstall.pl - アプリケーション削除スクリプト

setup.pl - アプリケーション設定スクリプト

/sbin/ - Kaspersky Anti-Virus の補助サービスが含まれるディレクトリ

kav4fs-kavmonitor - アンチウイルスコンポーネントの実行ファイル

kav4fs-kavmiddleware - リモート管理コンポーネント kavmiddleware の実行ファイル

/src/ - アプリケーションのアンチウイルスカーネルモジュールが含まれるディレクトリ

/opt/kaspersky/kav4fs/share/contrib/kav4fs.wbm - Webmin アプリケーションに対するプラグイン

/opt/kaspersky/kav4fs/share/contrib/vox.sh - アーカイブの感染駆除で使用されるスクリプト

/opt/kaspersky/kav4fs/share/doc/LICENSE - 使用許諾契約書

/opt/kaspersky/kav4fs/share/man/ - マニュアルが含まれるディレクトリ

/var/opt/kaspersky/kav4fs/bases/ - 定義データベースが含まれるディレクトリ

/var/opt/kaspersky/kav4fs/bases.backup/ - 最後の更新が行われるまで最新であった定義データベースが含まれるディレクトリ

/var/opt/kaspersky/kav4fs/licenses - ライセンス情報が含まれるディレクトリ



Kaspersky Anti-Virus のヘルプシステム (マニュアルページ) にアクセスするには、MANPATH 環境変数に [/opt/kaspersky/kav4fs/share/man](#) を割り当ててください。



Linux OS が動作するサーバの場合、Kaspersky Anti-Virus のインストール後にネットワークエージェント関連ファイルが以下の場所に置かれます：

/opt/kaspersky/klagent/ - ネットワークエージェントのメインディレクトリ。以下の内容が含まれます：

/bin/ - 次のようなネットワークエージェントユーティリティの実行ファイルが保管されるディレクトリ:

klmover - クライアント PC を管理サーバに手動で接続するユーティリティ (このユーティリティの使用については『Kaspersky Administration Kit 参照ガイド』を参照してください)

klmagchk - 管理サーバへの手動接続をチェックするユーティリティ (このユーティリティの使用については『Kaspersky Administration Kit 参照ガイド』を参照してください)

/lib/ - ネットワークエージェントの補助ファイルが含まれるディレクトリ

/bin/setup - ネットワークエージェントの設定スクリプトが含まれるディレクトリ

/share/man/ - マニュアルが含まれるディレクトリ

/sbin/ - ネットワークエージェントサービスの実行ファイルが含まれるディレクトリ

## 3.8. セットアップの完了

インストールプロセスが問題なく完了すると、確認メッセージが表示されます。アプリケーション配布キットに含まれる設定ファイルには、アプリケーションの使用を開始するのに必要な設定がすべて含まれています。

## 第 4 章 KASPERSKY ANTI-VIRUS の使用

Kaspersky Anti-Virus を使用して、コンピュータのアンチウイルスシステムを個別ファイルのレベルまたはファイルシステム全体のレベルで構築することができます。

アプリケーションの機能は、管理者が実行可能ないくつかのタスクにまとめることができます。Kaspersky Anti-Virus を使って実施できるタスクは、以下のグループに分かれます。

- ウイルスの検知と感染オブジェクトの感染駆除で使用する定義データベースの更新 (4.1 項を参照)
- スケジュールスキャンおよびオンデマンドスキャンを使用した、ファイルシステムのアンチウイルス (4.2 項を参照)
- リアルタイムのアンチウイルス (4.3 項を参照)

この章では、こうした標準的なタスクについて説明します。各企業ネットワークの状況に合わせ、各種タスクを組み合わせさせて運用することができます。

### 4.1. 定義データベースの更新

定義データベースの更新は `keepup2date` コンポーネントによって行われます。このコンポーネントは、十分なウイルス対策に欠かせません。定義データベースの更新に使用されるデフォルト更新元は、カスペルスキーのアップデートサーバです。以下のサーバがあります：

<http://downloads1.kaspersky-labs.com/>

<http://downloads2.kaspersky-labs.com/>

<ftp://downloads1.kaspersky-labs.com/> ほか

更新のダウンロード元として使用可能な URL のリストは、アプリケーションの配布キットに含まれる `updcfg.xml` ファイルにあります。アップデートサーバのリストを見るには、コマンドラインで以下のように入力します：

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date -s
```

更新処理を行うとき、`keepup2date` コンポーネントはこのリストの最初にあるアドレスをまず選択し、そこから定義データベースのダウンロードを試みます。アプリケーション設定ファイルの **[updater.options]** セクションにある **RegionSettings** パラメータを使用して、コンピュータの現在の場所 (ISO 3166-1 標準に基づいた 2 文字表記の国コード) を指定することができます。`keepup2date` コンポーネントは、指定の地域に属するアップデートサーバの選択を開始します。選択したアドレスからの更新ができない場合は、次の URL に対してダウンロードが試みられます。



定義データベースの更新は、カスペルスキーのアップデートサーバへ 1 時間ごとにアップロードされます。



カスペルスキーとは関係のないサーバを更新元として使用することができます。ただし、このサーバ上の定義データベースは、コンピュータにインストールされたデータベースよりもバージョンが古い可能性があります。このようなサーバから更新を行うと、新しいデータベースが古いデータベースに置き換えられます。

更新が問題なく完了すると、設定ファイルの **[updater.options]** セクションで指定された **PostUpdateCmd** パラメータが実行されます。デフォルトでは、このコマンドによって定義データベースが自動的にリロードされます。この設定に不正な変更が加えられると、更新された定義データベースを使用できなくなったり、アプリケーションが正しく機能しなくなったりすることがあります。



keepup2date コンポーネントの設定はすべて、設定ファイルの **[updater.\*]** セクションにまとめられています。

ローカルエリアネットワークの構造が複雑である場合は、アップデートサーバから 1 時間ごとに定義データベースをダウンロードしてネットワークディレクトリに置き、ネットワーク内のローカルコンピュータがこのディレクトリを更新元として使用するように設定してください。ネットワークディレクトリの作成については、4.1.3 項を参照してください。

更新は、**cron** ユーティリティを使用してスケジュールを設定する (4.1.1 項を参照) か、管理者がコマンドラインから手動で行う (4.1.2 項を参照) ことができます。



定義データベースの更新を 1 時間ごとに行うように設定することを強くお勧めします。

### 4.1.1. 定義データベースの自動更新

設定ファイルを変更して、定義データベースの定期的な自動更新を設定することができます。



**タスク:** 定義データベースの自動更新が 1 時間ごとに行われるように設定する。システムログにはアプリケーションエラーだけを記録する。開始されたタスクすべてについて一般ログをとるが、画面には情報を表示しない。



**ソリューション:** タスクを実行するには、以下の手順を実行します：

1. アプリケーションの設定ファイルで、以下の値を指定します。設定例は以下のとおりです：
 

```
[updater.options]
KeepSilent=yes
[updater.report]
Append=yes
ReportLevel=1
```
2. 以下のように入力して、**cron (crontab -e)** プロセス用に設定ファイルを編集します：
 

```
0 0-23/1 * * * /opt/kaspersky/bin/kav4fs-keepup2date
```



**タスク:** カスペルスキーのアップデートサーバから行う定義データベース更新で、keepup2date コンポーネントに含まれるリストにあるアップデートサーバの URL が自動的に選択されるように設定する。



**ソリューション:** タスクを実行するには、以下の手順を実行します：

アプリケーション設定ファイルの **[updater.options]** セクションで、**UseUpdateServerUrl** に **No** の値を指定します。



**タスク:** 管理者の指定した URL から定義データベースの更新をダウンロードするように、コンポーネントを設定する。この URL からダウンロードできない場合は、ダウンロード処理を中断する。



**ソリューション:** タスクを実行するには、以下の手順を実行します：

**[updater.options]** セクションの **UseUpdateServerUrl** と **UseUpdateServerUrlOnly** に、**Yes** の値を指定します。**UpdateServerUrl** には、アップデートサーバの URL を指定する必要があります。



**タスク:** 指定された URL から定義データベースの更新をダウンロードするように、コンポーネントを設定する。この URL からダウンロードできない場合は、keepup2date コンポーネントに含まれるリストで指定されている URL からデータベースを更新する。



**ソリューション:** タスクを実行するには、以下の手順を実行します：

[**updater.options**] セクションの **UseUpdateServerUrl** に **Yes** の値を指定し、**UseUpdateServerUrlOnly** に **No** の値を設定します。**UpdateServerUrl** には、アップデートサーバの URL を指定する必要があります。

## 4.1.2. 定義データベースのオンデマンド更新

定義データベースの更新は、コマンドラインからいつでも行うことができます。以下のコマンドを入力します：

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date
```



**タスク:** 定義データベースの更新を開始し、結果を /tmp/updatesreport.log に記録する。



**ソリューション:** タスクを実行するには、コマンドラインで以下のように入力します

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date -l/tmp/updatesreport.log
```

複数のコンピュータにある定義データベースを更新する場合は、アップデートサーバから更新をダウンロードしてネットワークディレクトリに置き、各コンピュータがこのディレクトリを更新元として使用する方法が便利です。



**タスク:** ネットワークディレクトリ **/home/bases** から定義データベースを更新するように設定し、このディレクトリにアクセスできない場合またはディレクトリが空白の場合にはカスペルスキーのアップデートサーバから更新するように設定する。結果は **report.txt** ファイルに出力する。



**ソリューション:** タスクを実行するには、以下の手順を実行します：

1. アプリケーションの設定ファイルで、該当する値を指定します：

```
[updater.options]
UpdateServerUrl=/home/bases
UseUpdateServerUrl=yes
UseUpdateServerUrlOnly=no
```

2. コマンドラインで以下のように入力します：

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date -l
/tmp/report.txt
```

## 4.1.3. 定義データベース保存用ディレクトリの作成

定義データベースをネットワークディレクトリから正しく更新するには、ディレクトリのファイル構造がカスペルスキーのアップデートサーバと同じである必要があります。以下のセクションでは、このタスクについて詳しく見ていきます。



**タスク:** ネットワーク内のローカルコンピュータが定義データベースの更新元として使用するネットワークディレクトリを作成する。



**ソリューション:** タスクを実行するには、以下の手順を実行します:

1. ローカルディレクトリを作成します
2. 以下のように入力して `keepup2date` コンポーネントを起動します:

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date -u
<dir>
```

<dir> には、ローカルディレクトリへのフルパスを指定します

3. このディレクトリに対する読み取り専用のネットワークアクセス権を、ローカルコンピュータに付与します



**タスク:** 定義データベースの更新がプロキシサーバ経由で行われるように設定する。



**ソリューション:** タスクを実行するには、以下の手順を実行します:

1. **[updater.options]** セクションの **UseProxy** に **Yes** の値を指定します
2. 設定ファイルの **[updater.options]** セクションで、**ProxyAddress** にプロキシサーバの URL を指定します。アドレスは「**http://username:password@ip\_address:port**」の形式で指定してください。**ip address** と **port** は必ず指定する必要がありますが、**username** と **password** はプロキシサーバに認証が必要な場合にのみ指定します

または

1. **[updater.options]** セクションの **UseProxy** に **Yes** の値を指定します
2. 環境変数 **http\_proxy** を「**http://username:password@ip\_address:port**」の形式で指定します。この環境変数は **[updater.options]** セクションの **UseProxy** がない場合または **Yes** が指定されている場合に限って考慮されます

## 4.2. アンチウイルスによるファイルシステムの保護

`kavscanner` コンポーネントは、ファイルのスキャンを行ったり、感染オブジェクトや感染が疑われるオブジェクトの処理を設定に基づいて行うことで、コンピュータのファイルシステムをウイルスから保護します。



`kavscanner` コンポーネントの設定はすべて、アプリケーション設定ファイルの **[scanner.\*]** セクションにまとめられています。



デフォルトでは、オンデマンドスキャンを開始できるのは **root** ユーザだけです。

ファイルシステム全体、個別のディレクトリ、個別のファイルのスキャンすることができます。保護設定は、以下の内容でグループ分けされます:

- スキャン対象 (4.2.1 項を参照)
- オブジェクトのスキャン方法と感染駆除方法 (4.2.2 項を参照)

- オブジェクトに対して実行する操作 (4.2.3 項を参照)
- 操作結果レポートの作成に使われる設定 (5.6 項を参照)

コンピュータのファイルシステムに対するスキャンは、以下のように開始することができます：

- 1 度だけのタスクとして、コマンドラインから開始する (4.2.4 項を参照)
- **cron** ユーティリティを使って設定したスケジュールに基づいて開始する (4.2.5 項を参照)



コンピュータ全体のウイルススキャンには、非常に多くのリソースが必要です。したがって、このタスクを開始する場合はコンピュータのパフォーマンスが低下するため注意が必要です。多くのリソースを必要とするアプリケーションが動作していないときにスキャンを行ってください。問題発生を避けるため、ディレクトリを個別に選択してスキャンすることをお勧めします。

## 4.2.1. スキャン対象

スキャン対象は、おおまかに 2 つに分けることができます：

- スキャンパス - ウイルススキャンの対象となるディレクトリおよびオブジェクトのリスト
- スキャンオブジェクト - ウイルススキャンの対象となるオブジェクトのタイプ (アーカイブなど)

デフォルトでは、利用可能なファイルシステムのオブジェクトに対するスキャンは、カレントディレクトリから開始されます。



コンピュータのファイルシステムをすべてスキャンするには、ルートディレクトリに切り替えるか、コマンドラインでスキャン対象を「/」と指定します。

スキャンパスは、以下の方法で定義し直すことができます：

- スキャン対象となるディレクトリおよびファイルを、コマンドラインですべて列挙する (スペース区切り)。パスは、絶対パスまたは相対パス (カレントディレクトリから見て) を使用する
- スキャンパスをテキストファイルに列挙し、このファイルを使用するようにコマンドラインで **-@<filename>** を指定する。ファイル内の各オブジェクトは改行して入力し、絶対パスを使用する



スキャンパスとスキャンオブジェクトのテキストファイルの両方をコマンドラインで指定すると、ファイル内に指定されたパスだけがスキャン対象となります。コマンドラインで入力されたパスは無視されます。

- スキャン対象から除外するファイルおよびディレクトリのマスクを設定ファイル **kav4fs.conf** に指定して (**[scanner.options]** セクションの **ExcludeMask** および **ExcludeDirs**)、デフォルトのパス (カレントディレクトリから始まるすべてのパス) またはコマンドラインに列挙されたパスに制限をかける
- スキャン対象の再帰的スキャンをオフにする (**[scanner.options]** セクションの **Recursion**、またはコマンドラインパラメータ **-r**)

- 別の設定ファイルを作成し、このファイルを使用するようにコンポーネント起動時にコマンドラインで **-c <filename>** を指定する

デフォルトのスキャンオブジェクトは設定ファイル **kav4fs.conf** の **[scanner.options]** セクションで指定されており、以下の方法で定義し直すこともできます：

- ファイルを直接編集する
- コンポーネント起動時にコマンドラインパラメータを使用する
- 別の設定ファイルを使用する

## 4.2.2. オブジェクトのスキャンと感染駆除のモード

このモードの設定は非常に重要です。感染ファイルが検知されたときにアプリケーションが感染駆除を行うかどうか、この設定によって決定されます。

デフォルトでは、感染駆除はオフになっています。オブジェクトをスキャンし、ウイルスや疑わしいファイルまたは破損したファイルが検知された場合にメッセージを表示してレポートに情報を記録する、というのがデフォルト動作です。

ウイルススキャンの結果として、各オブジェクトにはいずれかのステータスが割り当てられます：

- **Clean** - ウイルスは検知されませんでした（オブジェクトは感染していません）
- **Infected** - オブジェクトは感染しています
- **Warning** - オブジェクトコードが既知のウイルスのコードと似ています
- **Suspicion** - オブジェクトは未知のウイルスに感染している疑いがあります
- **Corrupted** - オブジェクトが破損しています
- **Protected** - オブジェクトが暗号化されている（パスワード保護されている）ためスキャンできません
- **Error** - オブジェクトのスキャン中にエラーが発生しました

駆除モードがオンになっている場合（**[scanner.options]** セクション、**Cure = yes**）、**Infected** ステータスのオブジェクトだけがアンチウイルス処理を受けます。駆除の結果として、各オブジェクトにはいずれかのステータスが割り当てられます：

- **Cured** - オブジェクトの感染は正常に駆除されました
- **CureFailed** - オブジェクトの感染を駆除できませんでした。このステータスのファイルは、感染オブジェクトに関して指定されているルールに従って処理されます
- **Error** - オブジェクトのスキャン中にエラーが発生しました

## 4.2.3. オブジェクトに対して実行する操作

オブジェクトに対して実行される動作は、オブジェクトのステータスによって異なります（第 2 章を参照）。デフォルトでは、感染オブジェクトまたは感染が疑われるオブジェクトの検知に関して通知が行われるだけです。しかし、**Infected**、**Suspicious**、**Warning**、**Error**、**Protected**、**Corrupted** のステータスが割り当てられたオブジェクトに対して以下のような対応を設定することができます：

- ディレクトリへの移動 - 指定されたステータスのオブジェクトをディレクトリへ移動します。単体オブジェクトもコンテナオブジェクトも移動可能です
- ファイルシステムからの削除
- コマンドの実行 - 標準の Unix スクリプトファイルまたはそれと同等のものを使用してファイルを処理します

Kaspersky Anti-Virus は単体のオブジェクト（ファイル）とコンテナオブジェクト（複数のオブジェクトで構成されたもの。例：アーカイブ）を区別します。これらのオブジェクトに対する動作も区別されており、設定ファイル内での指定位置が分かれています。単体オブジェクトの場合は **[scanner.object]** セクション、コンテナオブジェクトの場合は **[scanner.container]** セクションで動作が指定されます。



自己解凍型アーカイブに対する動作を区別することができます。アーカイブ自体が感染している場合、アーカイブは単体オブジェクトと見なされます。アーカイブ内のオブジェクトが感染している場合は、コンテナと見なされます。したがって、アーカイブに対して実行される動作は、状況に基づいて、設定ファイルの該当セクションで指定された設定によって決定します。

オブジェクトに対する動作は、以下の方法で選択することができます：

- デフォルト動作として使用する場合は、**kav4fs.conf** 設定ファイル内で指定します (**[scanner.object]** セクションと **[scanner.container]** セクション)
- 別の設定ファイルで動作を指定し、コンポーネントの起動時にこのファイルを使用します



コンポーネントの起動時にコマンドラインで設定ファイルが指定されていない場合は、**kav4fs.conf** ファイルの動作設定が使用されます。このファイルを起動時に使用するのに、特別な設定は必要ありません。

- 現在の作業セッションに対しては、コンポーネント起動時にコマンドラインパラメータを使用して設定可能です

単体オブジェクトに対する動作とコンテナオブジェクトに対する動作では、同じ構文を使用します (**[scanner.object]** セクションと **[scanner.container]** セクション)。

#### 4.2.4. 個別ディレクトリのオンデマンドスキャン

Kaspersky Anti-Virus に実装されている最も一般的なタスクには、個別ディレクトリのウイルススキャンと感染駆除があります。



**タスク:/tmp** ディレクトリのウイルススキャンを開始し、検知された感染オブジェクトを自動的に感染駆除する。感染を駆除できなかったオブジェクトは削除する。

**infected.lst, suspicion.lst, corrupted.lst, warning.lst** ファイルを作成し、スキャンで検知された感染オブジェクト、疑わしいオブジェクト、破損オブジェクトのファイル名を記録する。

コンポーネント動作の結果（起動日、感染していないファイル以外のファイルに関する情報）を、カレントディレクトリに作成されるレポートファイル **kav4fs-kavscanner-current\_date-pid.log** に出力する。



**ソリューション:** タスクを実行するには、コマンドラインで以下のように入力します：

```
# /opt/kaspersky/kav4fs/bin/kav4fs-kavscanner -rlq pi/tmp/infected.lst  
-ps/tmp/suspicion.lst -pc/tmp/corrupted.lst -pw/tmp/warning.lst
```

```
-o/tmp/kav4fs-kavscanner-`date "+%Y-%m-%d-%S"` .log -i3-ePASBMe -j3 -mCn /tmp
```

## 4.2.5. スケジュールスキャン

Kaspersky Anti-Virus のタスクの実行は、**cron** アプリケーションを使用してスケジュール可能です。



**タスク:** **/home** ディレクトリのウイルススキャンを毎日 **0:00** に行い、設定ファイル **/etc/kav/scanhome.conf** で指定されたスキャン設定を使用する。



**ソリューション:** タスクを実行するには、以下の手順を実行します：

1. 設定ファイル **/etc/kav/scanhome.conf** を作成し、必要なスキャン設定をこのファイルに指定します
2. 以下のように入力して、cron (**crontab -e**) プロセスの動作を規定する設定ファイルを編集します：

```
0 0 * * * /opt/kaspersky/kav4fs/bin/kav4fskavscanner -c
/etc/kav/scanhome.conf /home
```

## 4.2.6. 追加機能：スクリプトファイルの使用

Kaspersky Anti-Virus では、標準の Unix コマンドおよびスクリプトファイルを使用して、ウイルス分析時にオブジェクトの追加処理を行うことができます。これらのツールを使用してステータスが異なる各オブジェクトに対する動作を定義することで、Kaspersky Anti-Virus の機能を拡張することができます。

### 4.2.6.1. アーカイブ内にある感染オブジェクトの感染駆除

Kaspersky Anti-Virus はアーカイブ内の感染ファイルまたは疑わしいファイルを検知しますが、感染駆除は行いません。しかし、スクリプトファイルを使用することで、アーカイブ内のファイルの感染を駆除することができます。以下に示す例では、Kaspersky Anti-Virus の配布パッケージに含まれるスクリプトファイル **vox.sh** を使用して **tar** および **zip** の感染を駆除する方法を紹介します。

スクリプトは、起動するとアーカイブを解凍してウイルススキャンを行い、個別のオブジェクトを処理して、スキャン済みのファイルを再び圧縮します。必要な圧縮ツールがシステムにインストール済みであることが前提です。



**タスク:** **tar** および **zip** 形式のアーカイブを、スクリプト **vox.sh** を使用してスキャンする。



**ソリューション:** タスクを実行するには、以下の手順を実行します：

コマンドラインで以下のように入力します：

```
# /opt/kaspersky/kav4fs/share/contrib/vox.sh <archive-path>
```

### 4.2.6.2. 管理者への通知

通常の Unix ツールを使用して、ファイルシステムで感染オブジェクト、疑わしいオブジェクト、または破損オブジェクトが検知された場合に管理者へ通知を送るように設定することができます。



**タスク:** 設定ファイル **kav4fs.conf** の設定を使ったシステムスキャンで感染ファイルまたはアーカイブが検知された場合に管理者へ通知が行われるように指定する。チェック対象オブジェクトに対し、シンボリックリンクの解決を有効にする。



**ソリューション:** タスクを実行するには、以下の手順を実行します：

単体オブジェクトとコンテナオブジェクトの処理に関するルールを、**kav4fs.conf** で指定します：

```
[scanner.options]
FollowSymlinks=yes
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is

infected by %VIRUSNAME% |
mail -s kav4fs-kavscanner admin@localhost.ru
[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is

infected, viruses list is in the attached file %LIST%
| mail -s kav4fs-kavscanner -a %LIST%
admin@localhost.com
```



このサンプルを実行する前に、**mail** ユーティリティが標準のインストールパスにあることを確認してください。

## 4.3. リアルタイムのアンチウイルス



ファイルシステムに対するリアルタイムのアンチウイルスは、**kavmonitor** によって実施されます。

**kavmonitor** コンポーネントの設定はすべて、アプリケーション設定ファイルの **[monitor.\*]** セクションにまとめられています。**kavmonitor** コンポーネントは、別のプログラムがファイルアクセス（ファイルを開く、閉じる、実行する）を要求した場合にウイルススキャンを行うように設定されています。ファイルを閉じるという動作の場合は、ファイルが変更された場合にのみスキャンが行われます。デフォルトでは、ユーザが指定したすべてのオブジェクトタイプがスキャンされますが、以下のものはスキャンされません：

- アーカイブ
- 自己解凍型アーカイブ
- メールデータベース
- メールメッセージ



シンボリックリンクのスキャンでは、リンクの対象オブジェクトがチェックされます。対象オブジェクトが保護の範囲外であっても同様です。シンボリックリンクが **IncludeDirs** リストに追加されていると、**kavmonitor** コンポーネントによって解決されません。

スキャン結果をふまえて、アプリケーション設定ファイルで指定された設定を使ってアンチウイルス機能によるオブジェクト処理が行われます。



デフォルトでは、感染オブジェクトの感染駆除は無効になっています。変更するには、アプリケーション設定ファイルで **[monitor.options]** セクションの **Cure** 設定に **Yes** の値を設定します。

**Infected, Suspicious, Warning, Error, Protected, CureFailed** のステータスが割り当てられたオブジェクトに対し、以下のようなスキャン後の対応を設定することができます：

- ディレクトリへの移動 - 指定されたステータスのオブジェクトをディレクトリへ移動します。単体オブジェクトもコンテナオブジェクト（フルパスを復元）も移動可能です
- ファイルシステムからの削除
- コマンドの実行 - 標準の Unix スクリプトファイルまたはそれと同等のものを使用してファイルを処理します

アプリケーションの設定ファイルで、オブジェクト処理のルールを設定することができます (**[monitor.actions]** セクション)。

また、以下の追加設定も可能です：

- **ExcludeDirs** および **ExcludeMask** を使用して、スキャン対象から除外するディレクトリを定義する
- ヒューリスティックコードアナライザと iChecker 技術を使用する
- 同時にスキャン可能なオブジェクトの最大数を設定してサーバの負荷を軽減する



**Kaspersky Administration Kit** を使用してアプリケーションをリモート管理する場合は、アプリケーション設定ファイルの **[monitor.\*]** セクションに変更を加えないでください。このセクションのパラメータは、**Kaspersky Administration Kit** の設定によってオーバーライドされます。

## 4.4. ライセンスキーの管理

ライセンスキーファイルはアプリケーションを使用する権利を与えるものであり、ライセンスのタイプ、有効期限、販売代理店情報など購入したライセンスに関する必須情報が含まれています。

アプリケーションを使用する権利だけでなく、ライセンス期間中には以下のサービスを受けることができます：

- 24 時間体制のテクニカルサポート
- 1 時間ごとにリリースされる定義データベース更新
- アプリケーションの更新（パッチ）
- 新規バージョンのアプリケーション（アップグレード）
- 新規ウイルスに関する最新情報

ライセンスの期限が切れると、上記サービスを受ける権利が自動的に失われます。**Kaspersky Anti-Virus** はアンチウイルス機能を継続しますが、ライセンス期限切れ時点で最新であった定義データベースが使用されます。定義データベースの更新機能は利用できません。

したがって、ライセンスキーの詳細を含むレポートファイルを定期的に確認し、ライセンス有効期限を把握しておくことが非常に重要です。

### 4.4.1. ライセンスキー詳細の表示

インストールされているライセンスキーの情報は kavscanner、kavmonitor、keepup2date コンポーネントに関するレポートに表示されます。これは、各コンポーネントが起動時にライセンスキー情報をロードするためです。

これとは別に、Kaspersky Anti-Virus には、キーの全情報を見るだけでなく分析データも受け取れるようにする特別な licensemanager コンポーネントが備わっています。

情報はすべて画面に出力されます。



ライセンスキーに関する情報を表示するには：

コマンドラインで以下のように入力します：

```
#/opt/kaspersky/kav4fs/bin/kav4fs-licensemanager -s
```

以下に示すような情報が画面に出力されます：

```
Kaspersky license manager Version 5.7 Copyright © Kaspersky Lab 1997-2007. Portions  
Copyright (C) Lan Crypto License file 0003D3EA.key, serial 0038-000419
```

```
0003D3EA, "Kaspersky Anti-Virus for Unix", expires
```

```
04-07-2003 in 28 days License file 0003E3E8.key, serial 011E-000413-0003E3E8,  
"Kaspersky Anti-Virus for Linux File Srv(licence per e-mail address)", expires  
25-01-2004 in234 days
```



特定のライセンスキーに関する情報を表示するには：

コマンドラインで以下のように入力します：

```
# /opt/kaspersky/kav4fs/bin/kav4fs-licensemanager -k<key filename>
```

<key filename> には、ライセンスキーファイルの名前を指定します (例：0003D3EA.key)。

以下のような情報が画面に出力されます：

```
Kaspersky license manager Version 5.7 Copyright (C) Kaspersky Lab. 1997-2007.  
Portions Copyright (C) Lan Crypto Serial 0038-000419-0003D3EA, "Kaspersky  
Anti-Virus  
for Linux", expires 04-07-2003 in 28 days
```

### 4.4.2. ライセンスの更新

Kaspersky Anti-Virus のライセンスを更新することで、アプリケーションの機能を完全な状態に保つことができます。つまり、定義データベースの更新や、4.3 項に挙げられた追加サービスが可能な状態となります。

ライセンス期間は、アプリケーション購入時に選択したライセンスタイプによって異なります。



Kaspersky Anti-Virus のライセンスを更新するには：

購入元の販売代理店までお問い合わせください。



ライセンスの更新は特別価格にてご利用いただけます。詳細については販売代理店までお問い合わせください。

購入済みのライセンスキーをインストールする必要があります。

新しいライセンスキーをインストールするには：

コマンドラインで以下のように入力します：

```
# /opt/kaspersky/kav4fs/bin/kav4fs-licensemanager -a<key filename>
```

キーのインストール後に定義データベースを更新することをお勧めします (4.1 項を参照)。



ライセンスキーを削除するには：

コマンドラインで以下のように入力します。アクティブなライセンスキーを削除するには：

```
# /opt/kaspersky/kav4fs/bin/kav4fs-licensemanager -da
```

追加のライセンスキーを削除するには：

```
# /opt/kaspersky/kav4fs/bin/kav4fs-licensemanager -dr
```

## 第 5 章 追加設定

この章では、Kaspersky Anti-Virus の追加設定について説明します。これらの追加設定によって、アプリケーションの機能を拡張し、特定企業の要件に合わせてアプリケーションをカスタマイズすることができます。

### 5.1. Webmin を使用した製品管理の設定

Kaspersky Anti-Virus をリモート管理する場合は、Webmin パッケージを使用するように設定してください。

Webmin を使用することで、たとえばユーザパスワードを設定してアプリケーション機能へのリモートアクセスを制限することができます。

Webmin プログラムを使用してリモート設定された Kaspersky Anti-Virus 設定は、デフォルトのアプリケーション設定ファイルに保存されます。



Webmin を使用して別の設定ファイルを作成するには、以下の作業が必要です：

1. 既存の設定ファイルのデータを新規ファイルにコピーし、新規ファイルを別の名前で保存します。この新しい（別の）設定ファイルを、目的に合わせて変更します
2. この設定ファイルの名前を、[Config edit] タブの [Full path to KAV config] フィールドで指定します



Webmin プログラム設定の詳細については、製品のマニュアルを参照してください。また、アプリケーションリモート管理用プラグインについては、Webmin のオンラインマニュアルを参照してください。  
このガイドでは、**Webmin 経由のリモート管理については説明しません。**

### 5.2. Kaspersky Anti-Virus の動作の最適化

コンピュータの CPU にかかる負荷を軽減し、アンチウイルスの処理速度を向上させるために、いくつかの方法で Kaspersky Anti-Virus を最適化することができます。このセクションでは、これら機能に関する詳細を取り上げます。



iChecker データベースの使用、および 2 レベル構成のスキャン済みファイルキャッシュの使用

このアプリケーションではいくつかの技術を採用し、ファイルがアクセスを受けるたびに繰り返しスキャンを行う必要性をなくし、可能であれば既存の情報と単に比較するだけで済むようにしています。オブジェクト（ファイル）のウイルススキャンに使用されるアルゴリズムは以下のとおりです：

ファイルの初回のスキャンが終わった後、スキャン結果（ファイル名、チェックサム）が以下のいずれかのデータベースに登録されます。

- iChecker データベース - スキャン済みの感染していないファイルに関する情報が保管される共通のデータベース。このデータベースには、kavmonitor および kavscanner によってスキャンされたオブジェクトに関する情報が含まれます

- スキャン済みファイルのキャッシュ - kavmonitor によってスキャンされたファイルに関する情報が保管されるデータベース。キャッシュは 2 つのレベルに分かれています。第 1 のレベルには、比較的頻繁にアクセスを受ける**クリーンな（感染していない）ファイル**に関する情報が保管されます。このキャッシュはカーネルモジュール内に置かれ、アクセスにかかる時間を大幅に短縮しています。要求されたファイルに関するデータが第 1 レベルのキャッシュにある場合、そのファイルには自動的に **Clean** ステータスが割り当てられ、それ以上のウイルススキャンは行われません。要求された情報が第 1 レベルのキャッシュにない場合は、第 2 レベルで検索が行われます。第 2 レベルには、**すべてのスキャン済みファイル**に関する情報が含まれます。いずれのキャッシュデータベースもメモリ内に置かれ、アプリケーションが閉じられるとメモリから削除されます。

したがって、あるファイルに関する情報がスキャン中に iChecker データベースへ追加されなかった場合（ファイルが感染していない場合または iChecker がサポートしない形式のファイルである場合）でも、キャッシュには情報が追加されます。

ファイルへのアクセスが試みられるたびに、まず第 1 レベルのキャッシュで検索が行われ、続いて iChecker データベースと第 2 レベルのキャッシュで検索が行われます。検索は、ファイル名に基づいて行われます。いずれかのデータベースでファイル名が見つかり、ファイル情報とデータベース内の情報が比較されます。現在の情報とデータベース内の情報がまったく同じであれば、そのファイルは変更されていないものと見なされ、ウイルススキャンの対象外となります。

要求されたファイルの情報がどちらのデータベースにもない場合は、そのファイルに対して完全なウイルススキャンが実行されます。



**Kaspersky Anti-Virus** の使用中に定義データベースセットを切り替えた場合は、iChecker データベースから情報を手動で削除する必要があります。データベースへのフルパスは、アプリケーション設定ファイルの **[path]** セクションにある **ICheckerDbFile** パラメータで定義されています。

このデータベースには通常の定義データベースでは検知されないが拡張セットを使って検知可能な感染オブジェクトが含まれる可能性があるため、この情報を削除する必要があります。iChecker データベースに記載されているファイルは再スキャンされないため、コンピュータが感染してしまう可能性があります。



#### CPU への負荷の制限

コンピュータのファイルシステムをスキャンする場合、保管されているデータの量によってはスキャンに時間がかかる可能性があります。こうした場合に別のタスクが実行されると、CPU に非常に大きな負荷がかかります。したがって、負荷が指定のしきい値を超えるとウイルススキャンが一時停止するようなツールを備えておくことをお勧めします。

Kaspersky Anti-Virus には、そうしたメカニズムが備わっています。バージョン 5.7 では、設定ファイルの **[scanner.options]** セクションに **MaxLoadAvg** が追加されています。この設定がオンになっていると、プロセッサの **load average** 値が指定のレベルに下がるまでの間、kavscanner がスキャンを一時停止します。

さらに、設定ファイルの **[monitor.options]** セクションにある **CheckFileLimit** を使用して、リアルタイムモードで同時にスキャンされるオブジェクトの数を制限することができます。これによって CPU への負荷が軽減され、一部オブジェクトのスキャン速度が向上します。

システムリソースへの負荷をさらに軽減するには、kavmiddleware を無効にします。このサービスは Kaspersky Anti-Virus と Kaspersky Administration Kit の間での通信を担当します。Kaspersky Administration Kit と連動していない場合は、kavmiddleware サービスを停止してかまいません。コマンドラインで以下のように入力してください：

```
# /etc/init.d/kavmiddleware stop
```

## 5.3. 隔離ディレクトリへのオブジェクト移動

すべての感染オブジェクトが隔離用ディレクトリへ移動されるように、Kaspersky Anti-Virus を設定することができます。

この機能は、オブジェクトの感染を駆除できなかったがファイル自体に有益な情報が含まれているような場合に使用します。たとえば、ファイルに感染している 3 つのウイルスのうち 2 つしか削除できなかった場合などです。

隔離されたオブジェクトの置かれたディレクトリをファイルシステム内に残しておく場合は、設定ファイルの **[scanner.options]** セクションで **ExcludeDirs** にディレクトリのフルパスを指定して、このディレクトリをスキャン範囲から除外してください。

この後は、ファイルシステムのスキャンで検知された感染オブジェクトの隔離タスクについて説明します。



**タスク:** /tmp/download.lst にリストアップされたオブジェクトをすべてウイルススキャンし、感染オブジェクトが検知されたらオブジェクトのフルパスを使って /tmp/infected ディレクトリに移動する。感染オブジェクト、疑わしいオブジェクト、破損オブジェクトの情報をレポートファイルに出力する。



**ソリューション:** タスクを実行するには、以下の手順を実行します：

1. 感染オブジェクトの処理を指定するには、設定ファイルの **[scanner.object]** セクションと **[scanner.container]** セクションに以下の行を入力します：

```
OnInfected=MovePath /tmp/infected
```

2. 駆除モードがオンになっている場合はオフ (**Cure = no**) にします。
3. コマンドラインで以下のように入力します：

```
# /opt/kaspersky/kav4fs/bin/kav4fs-kavscanner -@/tmp/download.lst -ePASBME  
-rq -i0 -o/tmp/report.log -j3 -mCn
```

/tmp/infected ディレクトリ内にあるファイルへのアクセス権を読み取りと書き込みに限定することで、タスクをさらに複雑化することができます。指定するには、標準の Unix ツール (**chmod** コマンド) を使用します。タスクの実施内容は、以下のように変更します：

設定ファイルの **[scanner.object]** セクションと **[scanner.container]** セクションに以下の行を入力し、感染オブジェクトの処理に関するルールを指定します。

```
OnInfected=exec mv %FULLPATH%/%FILENAME%  
/tmp/infected/%FILENAME%; chmod -x  
/tmp/infected/%FILENAME%
```



**タスク:** アクセスが試みられたファイルをすべてスキャンし、感染オブジェクトの感染を駆除する。駆除できなかった場合は、感染オブジェクトをフルパスで /tmp/infected ディレクトリに移動する。



**ソリューション:** タスクを実行するには、以下の手順を実行します：

1. 感染オブジェクトに対する駆除モードをオンにします (設定ファイルの **[monitor.options]** セクション、**Cure = yes**)。
2. 感染オブジェクトの隔離に関するルールを指定します。設定ファイルの **[monitor.actions]** セクションで、以下のように設定します：

```
OnInfected=MovePath /tmp/infected
```

## 5.4. 感染オブジェクトのバックアップ

スキャンしたファイルが感染しており、感染オブジェクトに対してファイルシステムからの削除が指定されている場合は、重要なデータが失われる危険性があります。データ損失を避けるために、ファイルをバックアップストレージへコピーすることができます。

オブジェクトの感染駆除または削除の前に、オブジェクトのコピーが自動的にバックアップディレクトリに作成されます (**[monitor.path]** セクション、**BackupPath**)。これによってバックアップが作成され、駆除の途中にオブジェクトが破損した場合でも元のファイルを復元できるようになります。バックアップストレージには、オブジェクトがフルパスでコピーされます。バックアップストレージに同じオブジェクトが 2 回保存される場合、古い方のコピーが新しいコピーによって自動的に上書きされます。

注) デフォルトでは、バックアップディレクトリにファイルがコピーされません。また、バックアップディレクトリの場所も設定ファイルに規定されていません。

バックアップモードをオンにするには、オブジェクトのバックアップを保管するディレクトリのパスを手動で指定します。



オブジェクトをファイルシステムから削除しても、バックアップは、管理者が削除しない限りバックアップディレクトリに残ります。



設定ファイルで指定されている感染オブジェクトに対する動作は、バックアップディレクトリ内のファイルに対しては実行されません。

## 5.5. 日時形式のローカライズ

Kaspersky Anti-Virus の動作中には各コンポーネントに関するレポートが作成され、ユーザや管理者に通知が送信されます。この情報には、常に作成日時が示されています。

Kaspersky Anti-Virus で使用されるデフォルトの日時形式は、UNIX の **strftime** 関数と同じです。

**%H:%M:%S** - 時刻の形式

**%d/%m/%y** - 日付の形式

管理者は、日時形式を変更することができます。日時形式のローカライズは、設定ファイルの **[locale]** セクションで行います。たとえば、以下の形式を指定することができます:

**%I:%M:%S %P** - 時刻を 12 時間表記 (AM/PM 表示) で表示する場合

**%y/%m/%d** および **%m/%d/%y** - 日付 (DateFormat) をそれぞれ **年/月/日** および **月/日/年** の形式で表示する場合

## 5.6. Kaspersky Anti-Virus のレポート作成設定

Kaspersky Anti-Virus のコンポーネントの動作結果は、レポートファイルに記録されます。



コンピュータのファイルシステムをアンチウイルス処理した結果は、画面にも表示されます。デフォルトでは、レポートに出力される情報と画面に出力される情報は同じです。レポートファイルに記録されたのとは異なる情報を画面に表示するには、追加設定が必要です。

アプリケーション動作をシステムログに記録するには **[monitor.report]**、**[scanner.report]**、**[updater.report]** セクションの **ReportFileName** パラメータを **syslog** に設定します。

記録/表示する情報の詳細レベルは、レポート詳細レベルを変更することで調整できます。

**詳細レベル**は、コンポーネントの動作に関する情報をレポートに記録する際の情報詳細レベルを表す数値です。各レベルに含まれる情報は、ひとつ前のレベルに情報が追加された内容です。

以下の表では、レポート詳細レベルについて説明します。

レベル	レベルの意味	説明
0	緊急エラー	緊急エラーに関する情報のみ。コンポーネントが感染している、検証中やデータベースまたはライセンスキーのロード中にエラーが発生した、など。緊急エラーの情報には、ログファイル内で「F」が付けられます。
1	エラー	コンポーネントの停止を引き起こすようなその他エラーに関する情報。オブジェクトスキャンのエラーに関する情報など。これらエラーの情報には、ログファイル内で「E」が付けられます。
2	警告	アプリケーションの停止を引き起こすようなエラーに関する情報。ディスク空き容量の不足、ライセンスキーの期限切れに関する情報など。これらの情報には、ログファイル内で「W」が付けられます。
3	情報、通知	重要な情報の通知。コンポーネントが実行中かどうかの情報、設定ファイルのパス、スキャン対象、定義データベース情報、ライセンスキー情報、スキャン結果の統計情報など。これらの情報には、ログファイル内で「I」が付けられます。
4	動作	現在のアプリケーション動作に関する情報。スキャン中のオブジェクトの名前など。これらの情報には、ログファイル内で「A」が付けられます。
9	デバッグ	デバッグ情報。これらの情報には、ログファイル内で「D」が付けられます。

緊急エラーに関する情報は、どのレベルを選択した場合でも常に含まれます。最適なレベルは 4 であり、このレベルにデフォルト設定されています。



Kaspersky Administration Kit から開始されたオンデマンドスキャンタスクまたは更新処理タスクに関しては、ファイルへの記録がデフォルトで無効になっています。記録を有効にするには、設定ファイルの **[middleware.options]** セクションで **ReportLevel** および **ReportsDir** を使用して、レポート詳細レベルとレポート保管用ディレクトリを指定してください。

## 第 6 章 KASPERSKY ADMINISTRATION KIT を使用したアプリケーション管理

**Kaspersky Administration Kit** を使用すると、企業ネットワークのセキュリティシステムを運営する上での主要な管理タスクを一元管理することができます。

Kaspersky Anti-Virus 5.7 はカスペルスキー製品ラインのひとつであり、ローカルでコマンドラインを使用して管理（前述）することも、リモート一元管理システム **Kaspersky Administration Kit** を使用してリモートから管理することもできます。

アプリケーションの導入手順は 2 段階に分かれています：

- ネットワークに管理サーバを導入し、管理者のコンピュータに管理コンソールをインストールする。詳細については、『Kaspersky Administration Kit 管理者用マニュアル』を参照してください
- リモート管理対象となるネットワーク接続済みコンピュータに Kaspersky Anti-Virus 5.7 とネットワークエージェントを導入する

図 1 は管理コンソールを示しています。ここから、Kaspersky Administration Kit を通じてアプリケーションをリモート管理することができます。インターフェイスは **MMC (Microsoft Management Console)** と統合されており、管理者は以下の操作が可能です：

- ネットワーク接続したコンピュータにインストールされている Kaspersky Anti-Virus をリモート設定する
- 定義データベースを更新する
- クライアント PC 上でのアプリケーション動作に関する情報を見る

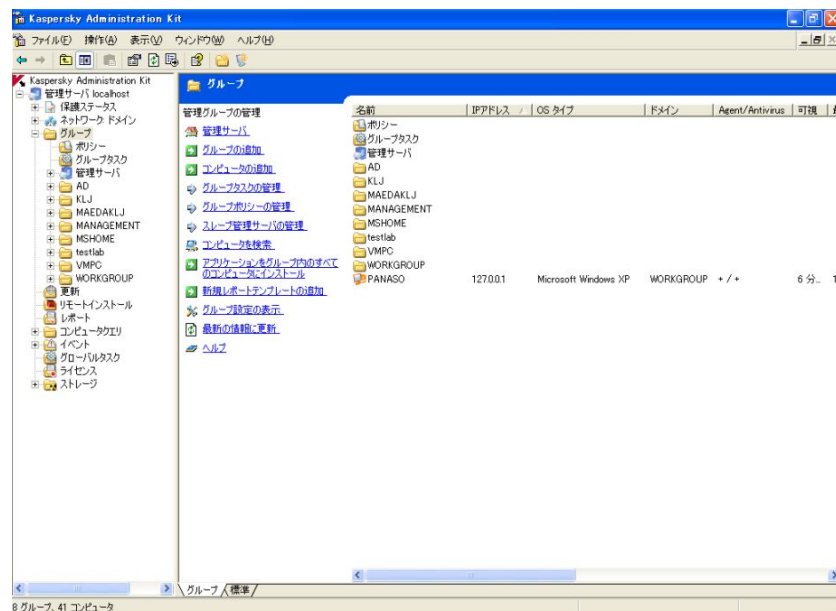


図 1. Kaspersky Administration Kit 管理コンソール

Kaspersky Administration Kit を通じてアプリケーションを一元管理する場合、管理者はポリシーおよびタスクの設定、アプリケーションの設定を行います。保護機能はこれらの設定に基づいて構築されます。

**アプリケーション設定**はアプリケーション動作に関する全般的な設定であり、全般的な保護設定や保護対象の設定が含まれます。

**タスク**は、アプリケーションが実行する具体的な動作です。Kaspersky Anti-Virus のタスクには、以下のタイプがあります：

- オンデマンドスキャンタスク
- 定義データベース更新タスク

各タスクには、タスク設定と呼ばれる一連の設定が指定されており、タスク実行時にはこれが使用されます。

一元管理の主な機能には、リモートコンピュータのグループ化があります。グループポリシーを作成して設定することでグループを管理します。

**ポリシー**とは、コンピュータの論理ネットワークグループ内における Kaspersky Anti-Virus の動作を規定する設定の集合を指します。

ポリシーにはアプリケーション設定および全種タスクの設定（タスクスケジュールのような、特定コンピュータに対して個別に指定されたものを除く）が含まれているため、ポリシーによってアプリケーションの機能を完全に管理することができます。

ポリシーはまた、アプリケーション設定またはタスク設定への変更を制限することもできます。

## 6.1. アプリケーションの管理

Kaspersky Administration Kit を使用すると、個々のクライアント PC にインストールされている Kaspersky Anti-Virus をリモート管理することができます。たとえば、スキャンの開始と停止、保護の有効化や無効化などの全般的な設定、レポート作成に関する設定などを管理できます。

アプリケーション設定を管理するには：

1. 対象となるクライアント PC を含むグループを、**[グループ]** フォルダ内で選択します（図 1）
2. 結果パネルで、アプリケーション設定を変更する必要があるクライアント PC を選択します。コンテキストメニューまたは **[操作]** メニューで、**[プロパティ]** を選択します
3. クライアント PC のプロパティウィンドウの **[アプリケーション]** タブ（図 2）で、クライアント PC にインストールされているカスペルスキー製品のリストを参照します
4. **[Kaspersky Anti-Virus for Linux Workstation and File Server 5.7]** を選択します。リストの下で、以下のボタンが利用可能となっています：
  - **イベント** - サーバまたはクライアント PC でのアプリケーション動作中に発生し、管理サーバに記録されたイベントのリストを表示します
  - **統計** - アプリケーション動作に関する統計情報を表示します
  - **プロパティ** - 表示された **[Kaspersky Anti-Virus for Linux Workstation and File Server 5.7 の設定]** ウィンドウでアプリケーションを設定します

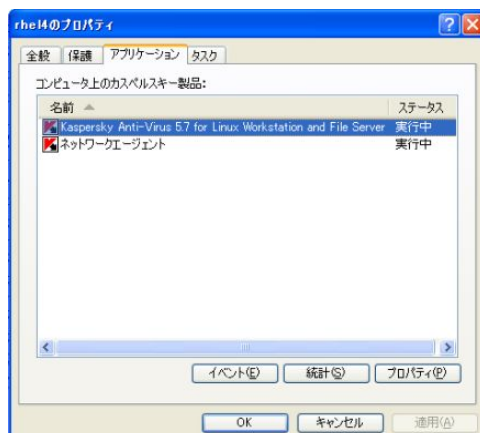


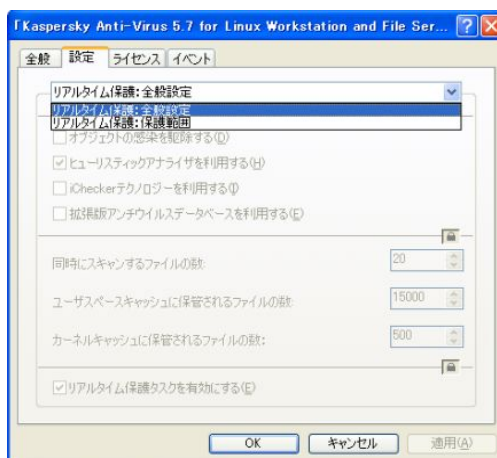
図 2. カスペルスキー製品のリスト

### 6.1.1. アプリケーション設定の構成

アプリケーション設定を表示または設定するには：

1. クライアント PC のプロパティウィンドウで [アプリケーション] タブを開きます (図 2)。
2. [Kaspersky Anti-Virus for Linux Workstation and File Server 5.7] を選択します。[プロパティ] をクリックしてアプリケーション設定ウィンドウを開きます。

[プロパティ] タブ以外のタブはすべて、Kaspersky Administration Kit 標準のタブです。標準のタブの詳細については、『Kaspersky Admin Kit 管理者用マニュアル』の「クライアント PC に関する情報の表示」を参照してください。

図 3. Kaspersky Anti-Virus 設定の構成  
[プロパティ] タブ

ポリシーによって一部設定の変更が禁止されている場合 (6.3.1 項を参照) は、対応する設定が無効化されます。

[プロパティ] タブでは、全般的な保護設定と保護範囲設定を指定することができます。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。

### 6.1.1.1. [プロパティ] タブ - [リアルタイム保護:全般設定] セクション

[リアルタイム保護:全般設定] セクションでは、以下の設定が可能です：

- ホストコンピュータのリアルタイム保護を有効/無効にする
- 感染オブジェクトの感染駆除を有効/無効にする
- ヒューリスティックコードアナライザと iChecker 技術を有効/無効にする
- アプリケーションの動作設定（同時にスキャンするファイルの数、カーネルキャッシュおよびユーザスペースキャッシュに保管されるファイルの数）を指定する

### 6.1.1.2. [プロパティ] タブ - [リアルタイム保護:保護対象] セクション

[リアルタイム保護:保護対象] セクションでは、以下の設定が可能です：

- 信頼する領域を設定する（スキャンから除外するディレクトリを選択する）
- スキャンから除外するファイル名マスクを指定する（標準的なシェルのマスクとして定義）
- 保護領域（スキャン対象ディレクトリのリスト）を設定する
- スキャン対象オブジェクトのタイプを選択する

## 6.2. タスクの管理

このセクションでは、Kaspersky Anti-Virus のタスクの作成と設定について説明します。

Kaspersky Administration Kit を使用した一元管理では、以下のタスクを作成して使用することができます：

- オンデマンドスキャンタスク
- 定義データベース更新タスク

### 6.2.1. タスクの作成

独自のスキャンタスクおよび定義データベース更新タスクを作成することができます。

クライアント PC に対して作成されたタスクの一覧を表示するには：

1. 対象となるクライアント PC を含むグループを、[グループ] フォルダ内で選択します（図 1）
2. 結果パネルで、ローカルタスクを参照するコンピュータを選択します。コンテキストメニューまたは [操作] メニューの [タスク] コマンドを選択します。クライアント PC のプロパティウィンドウが開きます
3. プロパティウィンドウの [タスク] タブ（図 4）に、このクライアント PC に対して作成されたタスクが表示されます

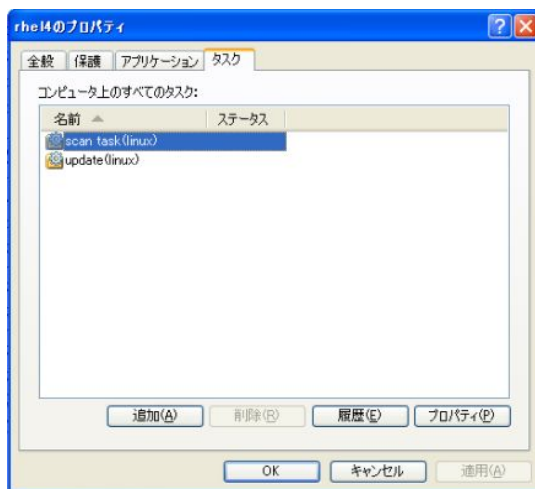


図 4. アプリケーションタスクのリスト

Kaspersky Administration Kit を通じてアプリケーションを管理する場合は、以下のタスクを作成することができます：

- ローカルタスク - 個別のコンピュータに対して設定
- グループタスク - 1 つのネットワークグループに属するすべてのコンピュータに対して設定
- グローバルタスク - すべてのネットワークグループから選択したクライアント PC のサブセットに対して設定

コンテキストメニューまたは [操作] メニューの [コピー]/[貼り付け] および [削除] コマンドを使用して、タスク設定の変更、パフォーマンスの監視、グループ間でのタスクのコピーおよび移動、タスクの削除を行うことができます。

各コンピュータでのタスク設定は、当該コンピュータのグループポリシー、タスク設定およびアプリケーション設定によって決定されます。

### 6.2.1.1. ローカルタスクの作成

ローカルタスクを作成するには：

1. [グループ] フォルダ (図 1) 内で、ローカルタスクの作成対象となるクライアント PC を含むグループを選択します
2. グループ内のコンピューター一覧から対象のコンピュータを選択し、コンテキストメニューの [プロパティ] または [操作] メニューの [タスク] を選択します。[<コンピュータ名> のプロパティ] ウィンドウが開き、クライアント PC のプロパティが表示されます
3. [タスク] タブ (図 4) に、このクライアント PC に対して作成されたタスクが表示されます。新規のローカルタスクを追加するには、[追加] をクリックします。タスク設定を変更するには、[プロパティ] をクリックします。選択したタスクをリストから削除するには、[削除] を使用します

[追加] をクリックすると、タスク作成ウィザードが起動します。ウィザードは一連のウィンドウで構成され、[戻る] と [次へ] を使用してウィンドウ間を移動することができます。[完了] をクリックしてウィザードを完了します。[キャンセル] をクリックすると、その時点でウィザードが停止します。

これ以降のセクションでは、ウィザードを使用したタスク作成方法について説明します。

### ステップ 1. タスクに関する全般的データの入力

最初のウィンドウでは、[名前] フィールドにタスク名を指定します。

### ステップ 2. アプリケーションとタスクタイプの選択

[アプリケーション] リストで **[Kaspersky Anti-Virus for Linux Workstation and File Server 5.7]** を選択します。[タスクタイプ] リストでタスクタイプを選択します。Kaspersky Anti-Virus では、以下のタスクタイプを選択可能です：

- オンデマンドスキャン
- 定義データベースの更新

### ステップ 3. 選択したタスクタイプの設定

選択したタスクタイプによって、次に表示されるウィンドウの内容が異なります。

#### オンデマンドスキャンタスクの設定

オンデマンドスキャンタスクの場合は、以下の内容を指定します：

- スキャン対象オブジェクトのタイプ
- スキャン対象（スキャン対象オブジェクトのパスをコロン区切りで指定）
- 感染オブジェクトが検知された場合にオブジェクトに適用される操作
  
- その他のパラメータ（ヒューリスティックアナライザの使用、iChecker™ の使用、拡張版定義データベースの使用、新規タスクを完全スキャンタスクとして起動するかどうかなど）

#### 定義データベース更新タスクの設定

定義データベース更新タスクの場合は、以下の内容を指定します：

- 更新のダウンロード元。カスペルスキーのアップデートサーバを使用するか、ユーザ定義の更新元を指定することができます
- パッシブ FTP モードが必要かどうか
- 接続タイムアウト（秒単位）

プロキシサーバの使用を有効/無効にし、**[プロキシサーバを設定する]** をクリックして表示されたウィンドウでプロキシ設定を指定することができます。

## ステップ 4. スケジュールの設定

[タスクスケジュール設定] ウィンドウで、タスクの実行に使用するスケジュールを設定します。

[実行予定] ドロップダウンリストで、タスクのスケジュールタイプを選択します。ウィンドウの中央部に表示されるデータ入力フィールドは、選択内容によって異なります。

タスクのスケジュール設定の詳細については、『Kaspersky Administration Kit 管理者用マニュアル』を参照してください。

## ステップ 5. タスク作成の完了

ウィザードの最後のウィンドウには、タスクが正常に作成されたことを知らせるメッセージが表示されます。

### 6.2.1.2. グループタスクの作成

グループタスクを作成するには：

1. タスクの作成対象となるグループを、コンソールツリー (図 1) で選択します
2. グループの [タスク] フォルダを選択し、コンテキストメニューで [新規作成] → [タスク] の順に選択するか、[操作] メニューで同様のコマンドを選択します。タスク作成ウィザードが起動します。ローカルタスクの作成ウィザードと内容は同じです (詳細については 6.2.1.1 項を参照)。ウィザードの指示に従います

ウィザードが完了すると、当該グループ内の [タスク] フォルダとすべてのサブグループにタスクが追加され、結果パネルに表示されます。

### 6.2.1.3. グローバルタスクの作成

グローバルタスクを作成するには：

1. コンソールツリー (図 1) で [タスク] フォルダを選択し、コンテキストメニューで [新規作成] → [タスク] の順に選択するか、[操作] メニューで同様のコマンドを選択します
2. タスク作成ウィザードが起動します。ローカルタスクの作成ウィザードと内容は同じです (詳細については 6.2.1.1 項を参照)。唯一異なるのは、タスクの適用先としてネットワーク接続しているクライアント PC を選択する点です
3. タスクを実行するコンピュータを、ネットワークから選択します。異なるフォルダからコンピュータを選択することも、フォルダ全体を選択することも可能です (詳細については『Kaspersky Administration Kit 管理者用マニュアル』を参照)



グローバルタスクは、選択されたコンピュータでしか実行されません。たとえばリモート導入タスクが作成されているグループに新しいクライアント PC が追加されても、このタスクは新規クライアントに対しては実行されません。新しくタスクを作成するか、既存タスクを変更する必要があります。

ウィザードが完了すると、コンソールツリー内の [タスク] フォルダにグローバルタスクが追加され、結果パネルに表示されます。

## 6.2.2. タスク設定の指定

クライアント PC に対するタスクを表示して変更するには：

1. クライアント PC のプロパティウィンドウで **[タスク]** タブを開きます (図 4)
2. タスクを選択して **[プロパティ]** をクリックします。タスク設定のウィンドウが開きます (図 5)

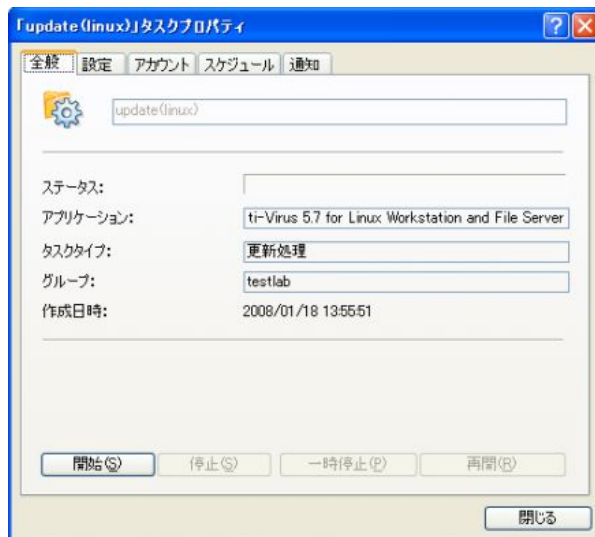


図 5. タスク設定の指定

以下のタブは、すべてのタスクに共通です：

- **全般** - タスク、タスクの開始、タスクの一時停止に関する一般的な情報が表示されます
- **スケジュール** - タスク実行スケジュールを作成します
- **通知** - タスク実行結果の通知を設定します (詳細については『Kaspersky Administration Kit 管理者用マニュアル』を参照)

### 6.2.2.1. オンデマンドスキャンタスク

タスク作成時に指定した内容に加え、以下のタスク設定をカスタマイズすることができます：

- スキャン対象オブジェクトのタイプ
- 信頼ゾーン - スキャンから除外するオブジェクトおよびオブジェクト名マスクのリスト
- ローカルファイルシステムだけをスキャンするかどうか
- ディレクトリを再帰的にスキャンするかどうか

- スキャン中にシンボリックリンクを解決するかどうか
- 現在のタスクを完全スキャンとして開始するかどうか

### 6.2.2.2. 定義データベース更新タスク

更新処理タスクには以下の設定があります：

- 更新のダウンロード元。カスペルスキーのアップデートサーバを使用するか、ユーザ定義の更新元を指定することができます
- 地域の設定。コンピュータの現在地を指定すると、指定地域のアップデートサーバから更新が行われます
- パッシブ FTP モードが必要かどうか
- 接続タイムアウト（秒単位）

プロキシサーバの使用を有効/無効にし、**[プロキシサーバを設定する]** をクリックして表示されたウィンドウでプロキシ設定を指定することができます。

### 6.2.3. タスクの開始と停止

タスクの起動、一時停止および再開は、スケジュールに基づいて自動的に行うか、コンテキストメニューまたはタスクのプロパティウィンドウから行います。

タスクを手動で開始または停止するには：

結果パネルから該当するタスクを選択し、コンテキストメニューで **[開始]**/**[停止]** を選択するか、**[操作]** メニューで同様のコマンドを選択します。

同様の操作は、タスクのプロパティウィンドウの **[全般]** タブ (図 5) にある **[開始]** と **[停止]** を使用して実行できます。



クライアント PC 上のタスクは、対応するアプリケーションが実行していないと実行されません。アプリケーションが停止されると、開始されたタスクはすべて終了します。

## 6.3. ポリシーの管理

ポリシーを設定することで、アプリケーション設定およびタスク設定を一連のクライアント PC へ一度に適用することができます。

このセクションでは、Kaspersky Anti-Virus のポリシーの作成と設定について説明します。

### 6.3.1. ポリシーの作成

Kaspersky Anti-Virus のポリシーを作成するには：


1. **[グループ]** フォルダ (図 1) で、ポリシー作成対象となるコンピュータのグループを選択します

2. 選択したグループの [ポリシー] フォルダを選択し、コンテキストメニューで [新規作成] → [ポリシー] の順に選択してポリシー作成ウィザードを起動します。

ポリシーはポリシーウィザードによって作成されます。ウィザードは一連のウィンドウで構成され、[戻る] と [次へ] を使用してウィンドウ間を移動することができます。[完了] をクリックしてウィザードを完了します。[キャンセル] をクリックすると、その時点でウィザードが停止します。

これ以降のセクションでは、ウィザードを使用したタスク作成方法について説明します。



ポリシー作成の各ステップ (ステップ 3 ~ 5) では、 ボタンを使って設定をロックすることができます。設定がロックされていると、クライアント PC では編集できません。

### ステップ 1. ポリシーに関する全般的データの入力

最初のウィンドウでは、[名前] フィールドにポリシー名を指定します。続いて、[アプリケーション] リストで [Kaspersky Anti-Virus for Linux Workstation and File Server 5.7] を選択します。

### ステップ 2. ポリシーステータスの選択

このウィンドウでは、ポリシーステータスを指定します。[アクティブポリシー]、[非アクティブポリシー]、[モバイルユーザポリシー] (コンピュータがネットワークから切断されたときに実施されるポリシー) のいずれかを選択してください。



1 つのグループ内で 1 つのアプリケーションに対して複数のポリシーを作成できますが、その設定内容を有効 (アクティブ) にできるポリシーは 1 つだけです。

### ステップ 3. ポリシーの設定

アプリケーション設定は 2 つのカテゴリに細分化されます：

- 全般的な設定
- 保護範囲と保護対象オブジェクトの設定

全般的な設定には、以下の内容が含まれます：

- リアルタイム保護の設定
- 検知された感染オブジェクトに対する動作 (感染オブジェクトに対する駆除の有効化/無効化)
- ヒューリスティックアナライザと iChecker™ 技術の使用

保護設定には、以下の内容が含まれます：

- 信頼ゾーン (スキャンから除外するディレクトリのリスト)
- スキャンから除外するファイルのマスクを指定する (標準的なシェルのマスクとして定義)
- 保護対象オブジェクトタイプのリスト

ディレクトリおよびオブジェクトマスクのリストは、コロン区切り形式です。

## ステップ 4. ポリシー作成の完了

ウィザードの最後のウィンドウには、タスクが正常に作成されたことを知らせるメッセージが表示されます。

ウィザードが完了すると、Kaspersky Anti-Virus ポリシーが該当するグループの [ポリシー] フォルダに追加され、結果パネルに表示されます。

新規ポリシーの設定を編集し、アイコンを使用して設定の変更に制限をかけることができます。ロックされた設定は、アプリケーションやタスクのプロパティでは変更できなくなります。ポリシーは、クライアント PC が初めてサーバと同期するときにクライアント PC へ適用されます。

コンテキストメニューまたは [操作] メニューの [コピー]/[貼り付け] および [削除] コマンドを使用して、グループ間でのポリシーのコピーおよび移動、ポリシーの削除を行うことができます。

## 6.3.2. ポリシー設定の表示と編集

ポリシーは編集可能です。また、ネスト化されたグループポリシーやアプリケーション設定、タスク設定に対する変更を禁止することもできます。

1. 設定編集の対象となるコンピュータグループを、コンソールツリーの [グループ] フォルダ (図 1) から選択します
2. グループ内の [ポリシー] フォルダを選択します。結果パネルに、そのグループに対して作成されたポリシーがすべて表示されます
3. **Kaspersky Anti-Virus for Linux Workstation and File Server 5.7** ([アプリケーション] フィールドで指定されたアプリケーション名) 向けポリシーのリストから、編集対象のポリシーを選択します
4. ポリシーを選択し、コンテキストメニューの [プロパティ] を選択します。いくつかのタブで構成されたポリシーのプロパティウィンドウが表示されます

[全般]、[実施]、および [イベント] タブは、Kaspersky Administration Kit の標準的なタブです。詳細については『Kaspersky Administration Kit 管理者用マニュアル』を参照してください。

[設定] タブ (図 6) には、Kaspersky Anti-Virus 固有の設定があります。詳細は以下のとおりです。

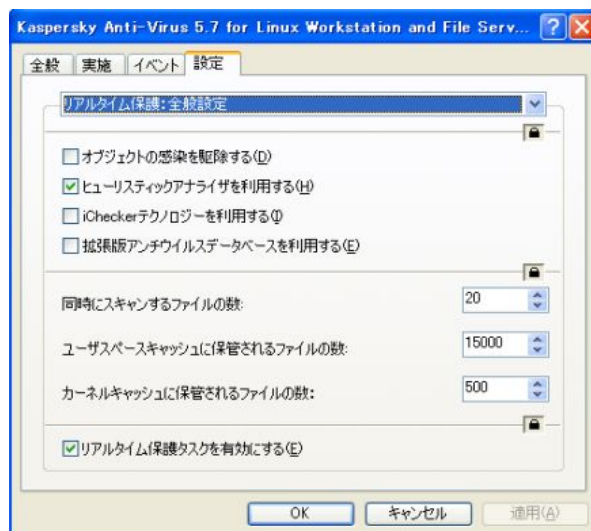


図 6. ポリシーの設定



ポリシー設定を編集する場合には、 ボタンを使用して、このポリシーに関して指定されたデータをロックすることができます。ロックされた設定は、アプリケーションやタスクのプロパティでは変更できなくなります。

### 6.3.2.1. 保護対象の設定

[設定] タブの [リアルタイム保護: 保護対象] セクションでは、以下の設定が可能です：

- 信頼する領域を設定する（スキャンから除外するディレクトリを選択する）
- 保護から除外するファイルのマスクを指定する（標準的なシェルのマスクとして定義）
- スキャン対象を指定する（スキャン対象ディレクトリのリスト）

ディレクトリおよびオブジェクトマスクのリストは、コロン区切り形式です。

### 6.3.2.2. 保護対象オブジェクトタイプの指定

保護対象となるオブジェクトのタイプを [設定] タブの [リアルタイム保護: 保護対象] セクションで指定することができます。

以下のスキャン対象を選択できます：

- 圧縮された実行ファイル
- アーカイブ
- 自己解凍型アーカイブ
- メールデータベース
- プレーンテキスト形式のメール

### 6.3.2.3. オブジェクトに適用される動作の設定

[設定] タブの [リアルタイム保護:全般設定] セクションでは、以下の設定が可能です:

- 感染オブジェクトの感染駆除を有効/無効にする
- リアルタイム保護を有効/無効にする
- ヒューリスティックアナライザを有効/無効にする
- iChecker™ 技術を有効/無効にする
- 拡張版定義データベースの使用を有効/無効にする

### 6.3.2.4. 追加設定の指定

[設定] タブの [リアルタイム保護:全般設定] セクションでは、以下の追加設定を指定することができます:

- 同時にスキャンするファイルの数
- ユーザスペースキャッシュに保管されるファイルの数
- カーネルキャッシュに保管されるファイルの数

## 第 7 章 KASPERSKY ANTI-VIRUS の アンインストール

Kaspersky Anti-Virus をアンインストールするには、以下のものがが必要です：

- 特権ユーザ権限 (**root**)。アプリケーションをアンインストールするには、**root** ユーザとしてシステムにログインする必要があります
- インストールプロセスのレポートファイル
- インストール済み Kaspersky Anti-Virus ファイルのファイル名とサイズは、インストールプロセスのレポートファイルに記載されているものと完全に対応している必要があります

アプリケーションのアンインストールを開始する前に、**kavmonitor** コンポーネントを停止する必要があります。コマンドラインで以下のように入力してください：

```
# /etc/init.d/kav4fs stop
```

続いて、アプリケーションとネットワークエージェントのアンインストールを行います。



Kaspersky Anti-Virus とネットワークエージェントを **.rpm** パッケージからインストールした場合は、コマンドラインで以下のように入力します：

```
# rpm -e <package_name>
```



Kaspersky Anti-Virus とネットワークエージェントを **.deb** パッケージからインストールした場合は、コマンドラインで以下のように入力します：

```
# dpkg -r <package_name>
```

アンインストール処理は自動的に行われます。アンインストールプロセスが完了すると、確認メッセージが表示されます。

## 第 8 章 KASPERSKY ANTI-VIRUS の動作確認

Kaspersky Anti-Virus をインストールして設定したら、テスト用「ウイルス」とその亜種を使用して、アプリケーションの動作確認を行うことをお勧めします。

このテスト用ウイルスは (The European Institute for Computer Antivirus Research) が作成したアンチウイルス製品の動作確認用ウイルスです。

このテストウイルスは多くのアンチウイルス製品でウイルスとして検知されますが、**ウイルスではありません**。コンピュータに害を及ぼすコードは含まれていません。



**動作確認には実際のウイルスを使用しないでください!**

このテスト用ウイルスは、**EICAR** の公式サイト ([http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)) からダウンロードできます。

**EICAR** のサイトから入手 (またはテキストエディタで作成) したファイルには、テストウイルスのコードが含まれています。Kaspersky Anti-Virus はこれを**感染 (Infected)** オブジェクトとして検知し、設定された処理を行います。

その他タイプのウイルスに対する処理を確認するには、テスト用ウイルスにいずれかの接頭辞を追加して亜種を作成します (以下の表を参照)。

表: テストウイルスの変更例

接頭辞	オブジェクトタイプ
接頭辞なし (標準のテストウイルス)	<b>感染 (Infected)</b> - 駆除できないオブジェクト
CORR-	<b>破損 (Corrupted)</b>
SUSP-	<b>感染の疑いあり (Suspicious)</b> - 未知のウイルスコード
WARN-	<b>感染の疑いあり (Suspicious)</b> - 既知のウイルスコードの変種
ERRO-	<b>未分析 (Not analyzed)</b> - エラーが原因
CURE-	<b>駆除 (Disinfected)</b> - オブジェクトの感染が駆除され、ウイルスの「本体」は「CURE」という文字で置き換えられます
DELE-	オブジェクトは自動的に削除されます

表の 1 列目は、標準のテストウイルス文字列の最初に追加する接頭辞です。変更例は以下のとおりです:

CORR-X50!P%@AP[4YPZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H\*.

2 列目は、接頭辞を追加した後に Kaspersky Anti-Virus によって識別されるオブジェクトタイプです。それぞれのオブジェクトタイプに対する処理は、管理者が指定したアプリケーション設定によって定義されます。

## 付録 A. 追加情報

この付録では、Kaspersky Anti-Virus のインストール後に表示されるディレクトリツリー、設定ファイル、コマンドラインパラメータおよびリターンコードについて説明します。アーカイブの感染駆除用スクリプトファイルの例も、ここで扱います。

### A.1. Kaspersky Anti-Virus 設定ファイル

Kaspersky Anti-Virus のパッケージには、アプリケーションの動作設定が保管された設定ファイル **kav4fs.conf** が含まれています。ここでは、ファイル設定の各セクションについて説明します。ファイル設定がデフォルト設定されている場合は、デフォルト値を示してあります。

**[path]** セクションの設定は、アプリケーションが機能するために欠かせない重要なファイルへのパスを定義します：

**BasesPath** - 定義データベースへのフルパス

**LicensePath** - ライセンスキーが含まれるディレクトリへのフルパス

**IcheckerDbFile** - iChecker 技術を使ってチェックされるデータベースが保管されているディレクトリへのフルパス

**[locale]** セクションの設定は、日時形式を決定します：

**TimeFormat=%H:%M:%S** - strftime 標準に基づいた時間表示形式



時間表示形式を 12 時間表記 (AM/PM 表示) に変更することができます：**%I:%M:%S %P**

**DateFormat=%d/%m/%y** - strftime 標準に基づいた日付表示形式



日付表示形式を、たとえば **%y/%m/%d** または **%m/%d/%y** に変更することができます。

**[network]** セクションには、kavmiddleware の接続設定が含まれます：



通常のアプリケーション使用では、このパラメータ値を変更しないでください。

**MiddlewareAddress=/var/run/kav4fs/kavmiddleware.socket** - kavmiddleware によるネットワークエージェントおよび kavmonitor への設定の指定

**[monitor.options]** セクションには、リアルタイムウイルススキャン設定が含まれます：

- ExcludeDirs=mask1:mask2:...:maskN** - スキャンから除外されるディレクトリのマスク。デフォルトではすべてのディレクトリがスキャンされます
- ExcludeMask=mask1:mask2:...:maskN** - スキャンから除外されるファイルのマスク。デフォルトではすべてのファイルがスキャンされます
- IncludeDirs=mask1:mask2:...:maskN** - スキャンされるディレクトリのマスク
- Packed=yes** - 圧縮ファイルスキャンモード。圧縮ファイルのスキャンを無効にするには、この設定に **no** を割り当てます
- Archives=no** - アーカイブスキャンモード。アーカイブファイルのスキャンを無効にするには、この設定に **no** を割り当てます
- SelfExtArchives=no** - 自己解凍型アーカイブスキャンモード。このモードを無効にするには、この設定に **no** を割り当てます。アーカイブスキャンモードが有効になっている (**Archives=yes**) 場合は、**SelfExtArchives** に **no** が割り当てられていても自己解凍型アーカイブはスキャンされます
- MailBases=no** - メールデータベーススキャンモード。このモードを無効にするには、この設定に **no** を割り当てます
- MailPlain=no** - プレーンテキスト形式のメールメッセージのスキャン。このモードを無効にするには、この設定に **no** を割り当てます
- Heuristic=yes** - スキャンの際にヒューリスティックコードアナライザを使用するかどうか。アナライザの使用を無効にするには、この設定に **no** を割り当てます
- Cure=no** - 感染オブジェクトの感染駆除モード。このモードを有効にするには、この設定に **yes** を割り当てます
- Ichecker=no** - ウイルススキャンの際に iChecker 技術を使用するかどうか。このモードを無効にするには、この設定に **no** を割り当てます
- FileCacheSize** - ファイルキャッシュのサイズ (MB 単位)
- KernelCacheSize** - アンチウイルスカーネルに保管されるキャッシュのサイズ (MB 単位)
- CheckFileLimit=20** - 同時にスキャンされるオブジェクトの最大数
- HashType=md5** - 使用されるハッシュのタイプ
- UseAVbasesSet=standard | extended** - アプリケーションが使用する定義データベースセット。  
**extended** セットには、**standard** セットに含まれるレコードのほかにリスクウェア (アドウェアやリモート管理ツールなど) のシグネチャが含まれます

**[monitor.path]** セクションの設定は、kavmonitor モジュールが機能するために欠かせない重要なファイルへのパスを定義します:

**BackupPath= path** - スキャン済みオブジェクトのバックアップが含まれるディレクトリへのフルパス

**PidFile=path** - コンポーネントの pid ファイルへのフルパス

**[monitor.actions]** セクションの設定は、リアルタイム保護中に特定タイプのオブジェクトに対して実行される操作を定義します:

**OnInfected=action** - 感染ファイルが検知されたときに実行される処理。感染駆除モードがオンになっている場合、駆除できなかったオブジェクトに対して指定の処理が行われます

**OnSuspicion=action** - 疑わしいファイルが検知されたときに実行される処理。疑わしいファイルとは、ウイルスと類似しているが Kaspersky Lab では未確認のコードが含まれるファイルです

**OnWarning=action** - 既知のウイルスコードと類似するコードを含むファイルが検知されたときに実行される処理

**OnCured=action** - 感染オブジェクトが検知されて駆除が行われた場合の処理

**OnProtected=action** - パスワード保護されたオブジェクトが検知されたときに実行される処理。このようなオブジェクトはスキャンされません

**OnCorrupted=action** - 破損ファイルが検知されたときに実行される処理

**OnError=action** - オブジェクトスキャン中にシステムエラーが発生した場合に実行される処理

**action** 設定の構文は 2 つの部分で構成され、処理そのものとオプションのパラメータがスペースで区切られます。オプションパラメータの値は二重引用符で囲みます。例: `OnInfected=move "/tmp/infected"`

処理として、以下のいずれかの値を指定することができます:

- `move <directory>` - ファイルを `<directory>` に移動する
- `movePath <directory>` - ファイルを `<directory>` へ再帰的に移動する (絶対パスを使用)
- `remove` - ファイルを削除する
- `exec <parameter>` - オブジェクトに対し、`<parameter>` の値で規定された処理を実行する

`exec` の処理パラメータとして、以下の値を指定することができます:

- `%VIRUSNAME%` - 検知された脅威またはエラーの名称
- `%LIST%` - ファイル名またはコンテナオブジェクト内で検知された感染ファイル、疑わしいファイル、破損ファイルのリスト。ファイル形式は `<virus name>%t<filename>` です
- `%FULLPATH%` - コンテナオブジェクトへのフルパス
- `%FILENAME%` - パスを伴わないファイル名
- `%CONTAINERTYPE%` - コンテナタイプ (文字列で指定)

**[monitor.report]** セクションには、`kavmonitor` コンポーネントの動作結果に関するレポートを作成する場合の設定が含まれます:

**ReportLevel=4** - レポートの詳細レベル (5.6 項を参照)

**ReportFileName** - コンポーネントの動作結果が記録されるファイルの名前

**Append=yes** - レポートファイルに新規メッセージを追加するかどうか。このモードを無効にするには、この設定に `no` を割り当てます

**ShowOK=yes** - 感染していないファイルに関するメッセージをレポートに記録するかどうか。このモードを無効にするには、この設定に `no` を割り当てます

**[scanner.options]** セクションには、サーバのファイルシステムをスキャンする場合の設定が含まれます:

**Archives=yes** - アーカイブスキャンモード。このモードを無効にするには、この設定に **no** を割り当てます

**Cure=no** - 感染オブジェクトの感染駆除モード。このモードを有効にするには、この設定に **yes** を割り当てます

**ExcludeDirs=mask1:mask2:...:maskN** - スキャンから除外されるディレクトリのマスク。デフォルトではすべてのディレクトリがスキャンされます

**ExcludeMask=mask1:mask2:...:maskN** - スキャンから除外されるファイルのマスク。デフォルトではすべてのファイルがスキャンされます

**Heuristic=yes** - スキャンの際にヒューリスティックコードアナライザを使用するかどうか。このモードを無効にするには、この設定に **no** を割り当てます

**LocalFS=no** - ローカルファイルシステムだけをスキャンするかどうか。このモードを有効にするには、この設定に **yes** を割り当てます

**MailBases=yes** - メールデータベーススキャンモード。このモードを無効にするには、この設定に **no** を割り当てます

**MailPlain=yes** - プレーンテキスト形式のメールメッセージのスキャン。このモードを無効にするには、この設定に **no** を割り当てます

**Packed=yes** - 圧縮ファイルスキャンモード。このモードを無効にするには、この設定に **no** を割り当てます

**Recursion=yes** - ウイルススキャンの際にディレクトリを再帰的にスキャンするかどうか。このモードを無効にするには、この設定に **no** を割り当てます

**SelfExtArchives=yes** - 自己解凍型アーカイブスキャンモード。このモードを無効にするには、この設定に **no** を割り当てます。アーカイブスキャンモードが有効になっている (**Archives=yes**) 場合は、**SelfExtArchives** に **no** が割り当てられていても自己解凍型アーカイブはスキャンされます

**Ichecker=yes** - ウイルススキャンの際に iChecker 技術を使用するかどうか。このモードを無効にするには、この設定に **no** を割り当てます

**UseAVbasesSet=standard | extended** - アプリケーションが使用する定義データベースセット。  
**extended** セットには、**standard** セットに含まれるレコードのほかにリスクウェア (アドウェアやリモート管理ツールなど) のシグネチャが含まれます

**FollowSymlinks** - シンボリックリンクの処理をコントロールするオプション。パラメータが **yes** に設定されていると、アプリケーションはスキャンの際に、ディレクトリを指すリンクをたどっていきます

**MaxLoadAvg** - CPU の最大負荷

**[scanner.report]** セクションには、kavscanner コンポーネントの動作結果に関するレポートを作成する場合の設定が含まれます:

**Append=yes** - レポートファイルに新規メッセージを追加するかどうか。このモードを無効にするには、この設定に **no** を割り当てます

**ReportFileName** - コンポーネントの動作結果が記録されるファイルの名前

**ReportLevel=4** - レポートの詳細レベル (5.6 項を参照)

**ShowOK=yes** - 感染していないファイルに関するメッセージをレポートに記録するかどうか。このモードを無効にするには、この設定に **no** を割り当てます

**ShowContainerResultOnly=no** - アーカイブスキャンの結果を簡単な形式で表示するかどうか。簡単なレポートを表示するには、この設定に **yes** を割り当てます

**ShowObjectResultOnly=no** - 単体オブジェクトのスキャン結果を簡単な形式で表示するかどうか。簡単なレポートを表示するには、この設定に **yes** を割り当てます

**[scanner.container]** セクションの設定は、サーバのファイルシステムを保護する場合にアーカイブに対して実行される操作を定義します:

**OnCorrupted=action** - 破損コンテナを検知したときに実行される処理

**OnInfected=action** - コンテナオブジェクト内で感染オブジェクトが検知されたときに実行される処理。感染駆除モードがオンになっている場合、すべての処理を行っても駆除できなかったオブジェクトを含むコンテナに対して、指定の処理が行われます

**OnSuspicion=action** - コンテナオブジェクト内で疑わしいオブジェクトが検知されたときに実行される処理

**OnWarning=action** - コンテナオブジェクト内で疑わしいオブジェクトが検知されたときに実行される処理。疑わしいオブジェクトとは、既知のウイルスコードと類似するコードを含むオブジェクトです

**OnCured=action** - 感染ファイルを含むオブジェクトが感染駆除された場合に実行される処理

**OnProtected=action** - パスワード保護されたオブジェクトを検知したときに実行される処理。このようなオブジェクトはスキャンされません

**OnError=action** - コンテナスキャン中にエラーが発生した場合に実行される処理

上記オブジェクトに関して実行される処理の構文は、**[monitor.actions]** のセクションで説明されているものと同じです。

**[scanner.object]** セクションの設定は、ファイルサーバのリアルタイム保護中に特定タイプの単体オブジェクトに対して実行される操作を定義します:

**OnCorrupted=action** - 破損ファイルを検知したときに実行される処理

**OnInfected=action** - 感染ファイルを検知したときに実行される処理。感染駆除モードがオンになっている場合、駆除できなかったオブジェクトに対して指定の処理が行われます

**OnSuspicion=action** - 疑わしいファイルが検知されたときに実行される処理。疑わしいファイルとは、ウイルスと類似しているが Kaspersky Lab では未確認のコードが含まれるファイルです

**OnWarning=action** - 既知のウイルスコードと類似するコードを含むファイルが検知されたときに実行される処理

**OnCured=action** - 感染オブジェクトが検知されて駆除が行われた場合の処理

**OnProtected=action** - パスワード保護されたオブジェクトを検知したときに実行される処理。このようなオブジェクトはスキャンされません

**OnError=action** - オブジェクトスキャン中にエラーが発生した場合に実行される処理

上記オブジェクトに関して実行される処理の構文は、**[monitor.actions]** のセクションで説明されているものと同じです。

**[scanner.display]** セクションには、レポートの画面表示設定が含まれます：

**ShowContainerResultOnly=no** - アーカイブスキャンの結果を簡単な形式で画面に表示するかどうか。簡単な形式で表示するには、この設定に **no** を割り当てます

**ShowObjectResultOnly=no** - 単体オブジェクトのスキャン結果を簡単な形式で画面に表示するかどうか。簡単な形式で表示するには、この設定に **no** を割り当てます

**ShowOK=yes** - 感染していないファイルに関するメッセージを画面に表示するかどうか。このモードを無効にするには、この設定に **no** を割り当てます

**ShowProgress=yes** - 定義データベースのダウンロード処理、現在のファイルスキャンに関する情報など、現在のコンポーネント動作に関する情報を画面に表示するかどうか。このモードを無効にするには、この設定に **no** を割り当てます

**[scanner.path]** セクションの設定は、モジュールの機能に必要なファイルへのパスを定義します：

**BackupPath= path** - コンポーネントによってスキャンを受けるオブジェクトのバックアップを保管するバックアップ用ディレクトリへのフルパス

**[updater.path]** セクションの設定は、定義データベース更新コンポーネントの動作に必要なファイルへのパスを定義します：

**AVBasesTestPath** - 定義データベース保管用ディレクトリへのフルパス

**BackUpPath** - 定義データベースのバックアップ保管用ディレクトリへのフルパス

**[updater.report]** セクションには、keepup2date コンポーネントの動作結果に関するレポートを作成する場合の設定が含まれます：

**Append=yes** - レポートファイルに新規メッセージを追加するかどうか。このモードを無効にするには、この設定に **no** を割り当てます

**ReportFileName** - コンポーネントの動作結果が記録されるファイルの名前

**ReportLevel=4** - レポートの詳細レベル (5.6 項を参照)

**[updater.options]** セクションには、keepup2date コンポーネントの動作設定が含まれます：

**KeepSilent=no** - keepup2date コンポーネントの動作に関する情報を画面に表示するかどうか。表示しない場合は、この設定に **yes** を割り当てます

**ProxyAddress** - 接続で使用するプロキシサーバのアドレス。この設定は「**http://username:password@url:port**」という形式で指定します。**username** および **password** の指定は必須ではありません。アドレスが指定されていない場合は、環境変数 **http\_proxy** から値がインポートされます

**UseProxy** - カスペルスキーのアップデートサーバへの接続でプロキシサーバを使用するかどうか。**no** が割り当てられていると、プロキシサーバは使用されません。**yes** が割り当てられていると、**ProxyAddress** 設定で定義されているプロキシサーバアドレスが使用されます。**ProxyAddress** 設定に値が定義されていない場合は、環境変数 **http\_proxy** の値が使用されます。環境変数の値が定義されていない場合、プロキシサーバは使用されません

**UseUpdateServerUrl=no** - **UpdateServerUrl** で設定されたアドレスを更新で使用するかどうか

**UseUpdateServerUrlOnly=no** - **UpdateServerUrl** で設定されたアドレスのみを定義データベース更新で使用するかどうか。**no** が指定されていると、定義データベースを **UpdateServerUrl** のアドレスから更新できなかった場合に、アップデートサーバリストに記載された別のアドレスが使用されます

**UpdateServerUrl=no http://url/ | ftp://url/ | /local\_path/** - 定義データベース更新用のアドレス

**PostUpdateCmd** - 定義データベースの更新が完了した後すぐに実行されるコマンド。アプリケーションのインストールパッケージに含まれる設定ファイルで指定された値に基づいて、更新された定義データベースが自動的に再ロードされます。この設定の変更はお勧めしません

**RegionSettings=ru** - ユーザの所在地域を示すコード。定義データベース更新のダウンロードに最適なカスペルスキーのアップデートサーバを選択する際に使用されます

**ConnectTimeout=30** - 定義データベース更新のネットワークタイムアウト (秒単位)。指定期間中にサーバからデータを取得できなかった場合、カスペルスキーアップデートサーバのリストに記載された別のサーバが使用されます

**PassiveFtp=no** - 接続でのパッシブ FTP モードの使用

**[middleware.options]** セクションには、kavmiddleware サービスの設定が含まれます：



通常のアプリケーション使用では、これらの設定を変更しないでください。

**ScannerExe=/opt/kaspersky/kav4fs/bin/kav4fs-kavscanner** - kavscanner コンポーネントの実行ファイルへのパス

**Keepup2dateExe=/opt/kaspersky/kav4fs/bin/kav4fs-keepup2date** - keepup2date コンポーネントの実行ファイルへのパス

**LicensemanagerExe=/opt/kaspersky/kav4fs/bin/kav4fs-licensemanager** - licensemanager コンポーネントの実行ファイルへのパス

**MonitorInitdScript=/etc/init.d/kav4fs** - kavmonitor サービス管理用スクリプトへのパス

**DirToStoreFiles=/var/opt/kaspersky/kav4fs/middleware** - kavmiddleware サービスファイルへのパス

**ReportLevel=0** - レポートの詳細レベル (5.6 項を参照)

**ReportsDir=/var/log/kaspersky/kav4fs** - アプリケーションコンポーネントのレポートファイルへのパス

## A.2. kavscanner コンポーネントのコマンドラインパラメータ

設定ファイルの各種設定は、アプリケーションの起動時にコマンドラインパラメータを使用してオーバーライドすることができます。ここでは、これらパラメータを詳しく説明していきます。

ヘルプオプション:	
<b>-h</b>	コンポーネントに関するヘルプを画面に表示します
<b>-v</b>	アプリケーションバージョンを表示します

設定オプション:	
<b>-c (-C)</b> <b>&lt;path_to_file&gt;</b>	別の設定ファイル <b>&lt;path_to_file&gt;</b> を使用します
<b>-g&lt;path_to_file&gt;</b>	定義データベースにレコードが含まれる既知のウイルスのリストをファイル <b>&lt;path_to_file&gt;</b> に置きます
<b>-f</b>	kavscanner コンポーネントの破損シグネチャを無視し、コンポーネントの感染駆除を試みます

スキャンオプション:	
<b>-e &lt;option&gt;</b>	デフォルトのスキャンオプションを変更します。 <b>&lt;option&gt;</b> には以下のモードを使用することができます:
<b>P/p</b>	圧縮ファイルのスキャンを有効/無効にします
<b>A/a</b>	アーカイブのスキャンを有効/無効にします
<b>S/s</b>	自己解凍型アーカイブのスキャンを有効/無効にします
<b>B/b</b>	メールデータベースのスキャンを有効/無効にします
<b>M/m</b>	プレーンテキストのメールメッセージのスキャンを有効/無効にします
<b>E/e</b>	ヒューリスティックコードアナライザを有効/無効にします
<b>-R/r</b>	再帰的スキャンを有効/無効にします
<b>-S/s</b>	シンボリックリンクのオープンモードを有効/無効にします
<b>-l</b>	ローカルファイルシステムのみをスキャンします

レポート生成オプション:	
<b>-q</b>	画面にメッセージを表示しません
<b>-o &lt;name&gt;</b>	コンポーネント動作に関するレポートが記録されるファイルのファイル名を指定します。ファイル名が指定されていないと、レポートは作成されません。コンポーネント動作に関する情報は、コンソールにも出力されます。システムログに記録する場合は、 <b>&lt;name&gt;</b> パラメータに「syslog」を指定します
<b>-j&lt;level&gt;</b>	このレポートに含まれる情報の量に基づいて、レポート詳細レベルを指定します。 <b>&lt;level&gt;</b> には以下の詳細レベルを使用することができます:
<b>1</b>	その他エラーに関するメッセージの表示を有効にします
<b>2</b>	情報メッセージの表示を有効にします
<b>3</b>	スキャンに関するメッセージの表示を有効にします
<b>-x &lt;option&gt;</b>	画面に表示されるスキャンレポートの詳細レベルを指定します。 <b>&lt;option&gt;</b> には以下の詳細レベルを使用することができます:

<b>O/o</b>	単体オブジェクトのスキャンに関する簡単/詳細な形式のメッセージ
<b>C/c</b>	アーカイブのスキャンに関する簡単/詳細な形式のメッセージ
<b>N/n</b>	感染していないファイルに関するメッセージの画面表示を有効/無効にします
<b>P/p</b>	コンポーネントの現在の動作に関するメッセージの画面表示を有効/無効にします
<b>-m &lt;option&gt;</b>	レポートファイルに出力されるスキャンレポートの詳細レベルを指定します。 <b>&lt;option&gt;</b> には以下のモードを使用することができます:
<b>O/o</b>	単体オブジェクトのスキャンに関する簡単/詳細な形式のメッセージ
<b>C/c</b>	アーカイブのスキャンに関する簡単/詳細な形式のメッセージ
<b>N/n</b>	感染していないファイルに関するメッセージの画面表示を有効/無効にします

ファイルオプション:	
<b>-p&lt;option&gt; &lt;file_name&gt;</b>	オブジェクトのリストを指定のファイルに保存します。各オブジェクトはフルパスで一行ずつ保存されます。 <b>&lt;option&gt;</b> には以下のモードを使用することができます:
<b>i</b>	感染オブジェクトのリストをファイル <b>&lt;file_name&gt;</b> に保存します
<b>s</b>	疑わしいオブジェクトのリストをファイル <b>&lt;file_name&gt;</b> に保存します
<b>c</b>	破損オブジェクトのリストをファイル <b>&lt;file_name&gt;</b> に保存します
<b>w</b>	既存のウイルスコードに類似したコードを持つオブジェクトのリストをファイル <b>&lt;file_name&gt;</b> に保存します
<b>-@ &lt;filelist.lst&gt;</b>	ファイル <b>&lt;filelist.lst&gt;</b> で指定されているオブジェクトをスキャンします

ファイル処理オプション (コマンドラインでこれらのパラメータを使用すると、設定ファイルで指定された動作が取り消されます):	
<b>-i0</b>	ウイルススキャンだけを行います
<b>-i1</b>	感染オブジェクトの感染駆除を行い、駆除できない場合はスキップします
<b>-i2</b>	感染オブジェクトの感染駆除を行います。駆除できない場合、単体オブジェクトであればオブジェクトを削除し、コンテナオブジェクトであれば削除を行いません

<b>-i3</b>	感染オブジェクトの感染駆除を行います。駆除できない場合、単体オブジェクトであればオブジェクトを削除し、コンテナオブジェクトであればコンテナ全体を削除します
<b>-i4</b>	感染オブジェクトおよびコンテナオブジェクトを削除します

### A.3. kavscanner コンポーネントのリターンコード

kavscanner コンポーネントは、動作中に以下のコードを返します：

<b>0</b>	ウイルスは見つかりませんでした
<b>5</b>	感染オブジェクトはすべて感染を駆除されました
<b>10</b>	パスワード保護されたアーカイブが検知されました
<b>15</b>	破損ファイルが検知されました
<b>20</b>	疑わしいファイルが検知されました
<b>21</b>	既知のウイルスコードに類似したコードを含むファイルが検知されました
<b>25</b>	感染ファイルが検知されました
<b>30</b>	ファイルスキャン中にエラーが発生しました
<b>50</b>	定義データベースをロードできません（設定ファイル内で指定されたパスが見つかりませんでした）
<b>55</b>	定義データベースが破損しています
<b>60</b>	定義データベースの日付スタンプがライセンスキーの期間を超えています
<b>64</b>	ライセンス情報がありません。または、設定ファイルで指定されたパスにライセンスキーがありません
<b>66</b>	設定ファイルのオプションが無効です
<b>65</b>	設定ファイルをロードできません
<b>70</b>	コンポーネントが破損しています
<b>75</b>	kavscanner コンポーネントが破損しており、修復できません

## A.4. kavmonitor コンポーネントのコマンドラインパラメータ

ヘルプオプション:	
<b>-h</b>	コンポーネントに関するヘルプを画面に表示します
<b>-v</b>	アプリケーションバージョンを表示します

設定オプション:	
<b>-c&lt;path_to_file&gt;</b>	別の設定ファイル <b>&lt;path_to_file&gt;</b> を使用します

## A.5. licensmanager コンポーネントのコマンドラインパラメータ

ヘルプオプション:	
<b>-h</b>	licensmanager コンポーネントに関するヘルプを画面に表示します
<b>-v</b>	アプリケーションバージョンを表示します

ライセンスキー管理オプション:	
<b>-s</b>	インストール済みライセンスキーに関する情報を画面に表示します
<b>-c (-C) &lt;path_to_file&gt;</b>	別のキーファイル <b>&lt;path_to_key_file&gt;</b> を使用します
<b>-k&lt;path_to_file&gt;</b>	キー <b>&lt;path_to_key_file&gt;</b> に関する情報を画面に表示します
<b>-a&lt;path_to_file&gt;</b>	ライセンスキー <b>&lt;path_to_key_file&gt;</b> をインストールします
<b>-d(a r)</b>	アクティブなライセンスキーの削除 ( <b>-da</b> ) または追加のキーの削除 ( <b>-dr</b> ) を行います

## A.6. licensemanager コンポーネントのリターンコード

licensemanager コンポーネントは、動作中に以下のコードを返します：

0	コンポーネントによってライセンスキーに関する情報が正常にロードされ、動作が問題なく完了しました
30	コンポーネントの動作中にエラーが発生しました
64	ライセンス情報がありません。または、設定ファイルで指定されたパスにライセンスキーがありません
65	設定ファイルをロードできません
66	設定ファイルのオプションが無効で
70	licensemanager コンポーネントが破損しています

## A.7. keepup2date コンポーネントのコマンドラインパラメータ

ヘルプオプション：	
-v	アプリケーション情報を画面に表示してコンポーネントを閉じます
-h	コンポーネントによってサポートされているコマンドラインパラメータに関するヘルプ情報を画面に表示し、コンポーネントを閉じます
-s	アップデートサーバのリストを画面に表示します
動作オプション：	
-r	最後に適用された更新をロールバックして前回バージョンに戻ります
-k	定義データベースの更新が完了した後、 <b>PostUpdateCmd</b> コマンドを実行しません
-q	コンポーネント動作中、システムメッセージは画面に表示されません
-e	コンポーネント動作中、緊急エラーに関するシステムメッセージだけが画面に表示されます
-x<path_to_file>	定義データベースの更新をすべてローカルディレクトリ <path_to_file> にコピーします

動作オプション:	
<b>-g &lt;URL&gt;</b>	定義データベースの更新用のアドレス。この修飾子が指定されている場合、更新はこのアドレスから実行されます
<b>-d&lt;path_to_file&gt;</b>	ローカルディレクトリ <b>&lt;path_to_file&gt;</b> にあるコンポーネントの pid ファイルを使用します
レポート生成オプション:	
<b>-l&lt;path_to_file&gt;</b>	コンポーネントの動作結果をファイル <b>&lt;path_to_file&gt;</b> に記録します

## A.8. keepup2date コンポーネントのリターンコード

keepup2date コンポーネントは、動作中に以下のコードを返します:

<b>0</b>	定義データベースに更新は必要ありません
<b>1</b>	定義データベースは正常に更新されました
<b>10</b>	緊急エラーが発生しました。更新処理を終了します
<b>12</b>	定義データベースのロールバック中にエラーが発生しました
<b>30</b>	定義データベース更新後にコマンド <b>PostUpdateCmd</b> を実行できませんでした
<b>60</b>	ライセンス情報がありません。または、設定ファイルで指定されたパスにライセンスキーがありません
<b>75</b>	設定ファイルをロードできません。または設定エラーです

## A.9. kavmiddleware コンポーネントのコマンドラインパラメータ

ヘルプオプション:	
<b>-v</b>	アプリケーション情報を画面に表示してコンポーネントを閉じます
<b>-h</b>	コンポーネントによってサポートされているコマンドラインパラメータに関するヘルプ情報を画面に表示し、コンポーネントを閉じます

## 付録 B. よくある質問

この付録では、Kaspersky Anti-Virus のインストール、セットアップ、操作に関してユーザから寄せられることの多い質問を取り上げ、詳しく説明していきます。

**質問:** Kaspersky Anti-Virus と他社のアンチウイルスソフトウェアを併用することは可能ですか。

アプリケーション間の競争を避けるため、Kaspersky Anti-Virus のインストール前に他社のアンチウイルスソフトウェアを削除することをお勧めします。



**質問:** Kaspersky Anti-Virus では、以前にスキャンしたファイルが再度スキャンされません。なぜでしょうか。

Kaspersky Anti-Virus は、最後にスキャンを行った後に変更されていないファイルを再スキャンしません。

これは、新しく採用された iChecker™ の技術によって可能となっています。この技術は、オブジェクトのチェックサムデータベースを活用して実装されています。



**質問:** Kaspersky Anti-Virus によってコンピュータのパフォーマンスに一定の低下が見られ、CPU に大きな負荷がかかるのはなぜでしょうか。

ウイルス検知プロセスは計算タスク（数学的タスク）であり、構造の分析やチェックサムの計算、数学的なデータ変換などが行われます。したがって、アンチウイルスソフトウェアによって使用される主なリソースはプロセッサ時間です。さらに、定義データベースに新規ウイルスが追加されるたびに全体的なスキャン時間も上乗せされます。

その他のアンチウイルスソフトウェアベンダは、全体的なスキャン時間を短縮するために、スキャン対象となるファイルの数やタイプを切り捨てる、検知しにくいウイルスや特定の地理的環境で出現頻度の低いウイルスをデータベースから除外する、複雑な分析を必要とするファイル形式（PDF など）を除外するなどしています。Kaspersky Lab では、アンチウイルスソフトウェアの目的は真のアンチウイルスセキュリティをユーザに提供することだと考えています。

Kaspersky Anti-Virus の場合、経験豊富なユーザであれば、さまざまなファイルタイプのスキャンを無効にすることでウイルススキャンの速度を向上させることができます。ただし、そのためにセキュリティレベルが低下することに注意してください。

Kaspersky Anti-Virus は 700 形式を超えるアーカイブファイルおよび圧縮ファイルを検知可能です。こうした形式のファイルには実行可能な悪質コードが含まれている場合があるため、これはアンチウイルスセキュリティにとって非常に重要な要素です。一方で、Kaspersky Anti-Virus が検知可能なウイルスの総数が日に日に増加し（1 日あたり約 30 の新種ウイルス）、処理可能な形式の数も継続的に増えているにもかかわらず、製品の最新バージョンは常に前回バージョンよりも処理速度が速くなっています。これは、Kaspersky Lab の開発した iChecker™ など、独自の新技术を採用することで実現しました。



**質問:** ライセンスキーが必要なのはなぜですか。キーがなくても Kaspersky Anti-Virus は機能しますか。

Kaspersky Anti-Virus は、ライセンスキーがないと機能しません。

Kaspersky Anti-Virus の購入を検討していてアプリケーションの使用をお望みの場合は、2 週間または 1 ヶ月間有効のトライアルキーファイルを発行いたします。試用期間が過ぎるとキーは無効になります。



**質問:** ライセンスキーの期限が切れるとどうなりますか。

ライセンスの有効期限後も Kaspersky Anti-Virus は動作しますが、定義データベース更新はできなくなります。ウイルスに感染したオブジェクトの感染駆除は引き続き行われますが、その際に使用されるのは古い定義データベースです。

ライセンスキーの期限が切れた場合はシステム管理者に知らせるか、販売代理店までご連絡ください。



**質問:** Kaspersky Anti-Virus をインストールできません。どうしたらよいでしょうか。

まず、このマニュアル（特にこの付録）または当社の Web サイトにて、問題点と解決策を探してください。

解決策が見つからない場合は、購入元の販売代理店までお問い合わせください。



**質問:** 日常的に更新を行う必要があるのはなぜですか。

数年前、ウイルス拡散はフロッピーディスクを介して行われていたため、アンチウイルスプログラムをインストールして定義データベースを時折更新することで、コンピュータを十分に保護することができました。しかし現在では、ウイルスは数時間のうちに世界全体に拡がるため、古い定義データベースを使っているアンチウイルスソフトウェアでは新規脅威に対応できない場合があります。したがって、新種のウイルスに対する防御を確実にするには、定義データベースを毎日更新する必要があります。

Kaspersky Lab では、定義データベースの更新間隔を毎年短縮してきました。現在では、データベースの更新は 1 時間ごとにサーバへアップロードされています。

これに加え、検知された脆弱性の修復や新機能の提供を行うアプリケーションモジュールの更新も利用可能です。



**質問:** バージョン 5.0 以降、更新サービスでは何が変わったのですか。

バージョン 5.0 以降の製品ラインには、新しい更新サービスが備わっています。このサービスは、ユーザからのフィードバックおよび市場からの要望に基づいて開発されたものです。さらに、Kaspersky Lab での更新作成から始まりユーザ側でのファイル更新に至る全体的な更新処理手順の効率化に取り組みました。

新しい更新サービスの利点は以下のとおりです：

- 接続が切断された場合のダウンロード再開。ネットワーク接続が切断された場合、すでに受信した更新をダウンロードし直す必要がなくなりました
- 累積的更新のサイズ削減。累積的な更新には定義データベース全体が含まれており、通常の更新よりもはるかにサイズが大きくなります。新しい更新サービスでは、インストール済みの定義データベースを累積的更新でも使用可能とする技術が採用されています
- インターネットからのダウンロード速度の向上。ユーザの所在地にあるカスペルスキーアップデートサーバが選択されるようになりました。さらに、サーバに対する負荷が処理速度に基づいて分散されます。つまり、負荷がかかっているサーバではなく使用中でないサーバに接続されます
- キーの「ブラックリスト」の使用。これによって、Kaspersky Anti-Virus のライセンスを持たないユーザは更新を実行できなくなりました。したがって、正規のライセンス済みユーザがサーバの過負荷に悩まされることがなくなります

- 企業向け製品では、ローカルアップデートサーバの作成が可能になりました。これは、カスペルスキー製品がインストールされた複数のコンピュータで構成される LAN を使用している企業にとって必要な機能です。任意のコンピュータをアップデートサーバに指定し、インターネットからダウンロードした更新をそのコンピュータのローカルディレクトリに置いて、ネットワーク内のその他コンピュータがこのディレクトリへアクセスできるようにすることができます



**質問:** 侵入者によって定義データベースが置き換えられることはありませんか。

すべての定義データベースには独自のシグネチャが割り振られており、Kaspersky Anti-Virus がデータベースを使用するときにシグネチャが検証されます。このシグネチャが Kaspersky Lab によって割り当てられたものと一致しない場合、またはライセンス有効期限日より後の日付になっている場合には、そのデータベースは使用されません。



**質問:** 自分が使っている Linux OS バージョンで Kaspersky Anti-virus は機能するでしょうか。

Kaspersky Anti-Virus 5.7 は RedHat、Debian、SUSE、および Mandriva Linux OS での動作をテスト済みです。これらの Linux ディストリビューションそれぞれに対応する Kaspersky Anti-Virus 配布パッケージが用意されています。

サポート対象のオペレーティングシステムについては、1.4 項を参照してください。

サポート対象ではないプラットフォームでは、アプリケーションが正しく動作しない場合があります。理由のひとつには、オペレーティングシステムの仕様があります。例としては、お使いのオペレーティングシステムで異なるバージョンのライブラリが使用されている場合、システム初期化スクリプトが通常とは異なる場所にある場合が挙げられます。このような場合は、当社テクニカルサービスでは対応いたしかねます。



**質問:** kavmonitor コンポーネントが複数のプロセスを同時に起動するのはなぜでしょうか。

kavmonitor によって起動されるプロセスの最大数は設定ファイルの **CheckFileLimit** 設定で制限されており、同時に処理されるファイルの数もここで決定されます。したがって、監視プロセスの数は常に 1 以上です（デフォルトでは 20 プロセスが起動）。スキャンするファイルがない場合、システムリソースによってプロセスが消費されることはありません。



**質問:** Network Control Centre for Windows を使用して Kaspersky Anti-Virus を管理することはできますか。

Network Control Centre for Windows を使用して Kaspersky Anti-Virus for Linux File Server を管理することはできません。今回のバージョンでは、Webmin パッケージの特別なモジュールを使用してアプリケーションをリモート設定することができます。



**質問:** アプリケーションが画面に出力する情報は、どのようにしてファイルに保存できますか。

Kaspersky Anti-Virus の動作中に画面出力される情報を保存するには、設定ファイル内で該当の設定を指定するか、コマンドラインで以下のように入力する必要があります。

```
# some_app > ./text_file 2>&1
```

some\_app - メッセージ保存対象となるアプリケーション

text\_file - 情報の保存先となるファイルへのフルパス

指定例は以下のとおりです：

```
# /opt/kaspersky/kav4fs/bin/kav4fs-keepup2date
> ./updater.log 2>&1
```

この場合、keepup2date コンポーネントの通常の実出力メッセージおよびエラーメッセージはファイル `updater.log` に記録されます。



**質問：** Administration Kit を通じてアプリケーションを起動した後のアプリケーション動作結果は、どのようにして見ることができますか。

Administration Kit を通じて起動されたアプリケーションの動作記録は、デフォルトでは無効になっています。

設定ファイルに以下の変更を加えることで、アプリケーション動作結果のファイルへの保存を有効にします：

- **[middleware.options]** セクションの **ReportLevel** パラメータを使用して、レポート詳細レベル (5.6 項を参照) を指定する
- レポートを保管するディレクトリを指定する

指定されたディレクトリに、いずれかのファイルが作成されます：

- `kavscanner_middleware.log` - オンデマンドスキャンタスクが完了した場合
- `keepup2date_middleware.log` - 更新処理タスクが完了した場合



**質問：** Kaspersky Anti-Virus によって保護されているファイルサーバと同じコンピュータでメールサーバが動作している場合、メールが送信できないのはなぜでしょうか。

ファイルサーバと同じコンピュータでメールサーバまたは Samba サーバが動作している場合、感染ファイルがメール/Samba サーバによって処理される可能性があります。kavmonitor コンポーネントは、ファイル処理の前に脅威を検知してファイルへのアクセスを防止します。

メールサーバまたはその他サーバによって処理されたデータがアンチウイルスアプリケーションによって保護されていれば、このような事態を回避できます。アプリケーション設定ファイルの **[monitor.options]** セクションにある **ExcludeDirs** リストに、一時ファイルおよびディレクトリを追加することをお勧めします。

## 付録 C. カスペルスキーラボス

1997 年の創始以来、カスペルスキーラボスは、情報セキュリティ技術界のリーダーとして知られ、コンピュータとネットワークをリスクウェアやスパム、ハッカーの攻撃等から保護する高性能かつ包括的な情報セキュリティソフトウェアを提供しています。

カスペルスキーラボスは本社ロシアをはじめ日、中、韓、英、仏、独、ポーランド、ベネルックス 3 国、米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ーの新部門も設立されました。

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

14 年余にわたるウイルス対策でスタッフが培った知識と経験がカスペルスキーラボス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ウイルス対策製品はワークステーション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 をウイルスの驚異から守ります。また柔軟な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。また Nokia ICG (米) や F-Secure (フィンランド)、Aladdin (イスラエル)、Sybari (米)、G Data (独)、Deerfield (米)、Alt-N (米)、Microworld (印)、BorderWare (加) などで 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製品の水準を雄弁に物語っています。

クライアントは製品の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提供いただけます。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。

### C.1. 製品ラインナップ

#### Kaspersky® Open Space Security

企業ネットワーク内の各レイヤをスペース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適し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** および **Kaspersky Anti-Spam – Total Space Security** に含まれる、メールシステムおよび Webトラフィックを保護する、各アプリケーションが含まれます。送受信メール保護の強化や迷惑メール対策の導入といった、個別セキュリティのニーズに合わせた製品です。

**Kaspersky Mobile Space Security** - Symbian OS および Microsoft Windows Mobile を搭載した携帯端末を保護するアプリケーションが含まれます。

## アプリケーション

### Kaspersky® Anti-Virus for Windows Workstation 6.0

Kaspersky® Anti-Virus for Windows Workstation 6.0 は、ウイルスやハッカー、スパム、スパイウェアなどのインターネット上の脅威に対して、ノートPCを含む企業のワークステーションを保護する総合セキュリティ製品です。各コンポーネントは共通のユーザインターフェイスに統合されているので、容易に設定および管理が行えるほか、リモート管理ツールであるKaspersky® Administration Kit を利用して、一元管理を行えます。

次のようなアンチウイルス機能が備わっています：

- **メールトラフィックのアンチウイルススキャン** - 使用されているメールクライアントに関係なく、データ転送プロトコルレベル（着信メールの場合は POP3、IMAP、NNTP、送信メールの場合は SMTP）でのメールトラフィックのアンチウイルススキャンを行います。プログラムは一般的なメールクライアント（Microsoft Office Outlook、Microsoft Outlook Express および The Bat!）に対するプラグインを備えており、これらメールデータベースの感染駆除をサポートしています
- **インターネットトラフィックのリアルタイムアンチウイルススキャン** - HTTP 経由で転送されるインターネットトラフィック
- **ファイルシステムの保護** - 個別のファイル、ディレクトリ、またはドライブのアンチウイルススキャンを行います。さらに、事前設定されたスキャンタスクを使用して、オペレーティングシステムの重要な領域と Microsoft Windows のスタートアップオブジェクト専用のアンチウイルス分析を開始できます
- **プロアクティブディフェンス** - アプリケーション動作およびランダムアクセスメモリ内で実行するプロセスを継続的に監視して、ファイルシステムやレジストリに危険な変更が加えられるのを防ぎ、悪意ある影響を受けた場合のロールバック機能を搭載しています

**ネット詐欺からの保護**は、フィッシング攻撃認識機能によって保障されています。機密データ（パスワード、銀行口座情報、クレジットカード番号など）の流出を防止し、Web ページやポップアップウィンドウ、広告バナーでの危険なスクリプトの実行を阻止します。**有料通話遮断**機能は、有料通話サービスへの不正な隠し接続を行うモデム使用の試みを検知し、そのような動作を阻止します。

Kaspersky® Anti-Virus for Windows Workstation 6.0 は、ネットワーク攻撃の前に行われる**ポートスキャンの試みを登録**して、一般的なハッカーの攻撃を防ぎます。また、**定義済みルールに基づいて**すべてのネットワークトランザクションを管理し、**送受信されるデータパケットを追跡**します。**ステルスモード**（SmartStealth™ テクノロジー使用）は、**外部からのコンピュータ検知を阻止**します。このモードに切り替えると、ユーザ定義ルールで許可されたトランザクションを除くすべてのネットワーク動作が遮断されます。

本アプリケーションでは、受信メールメッセージをフィルタリングするために複雑な方法を採用しています：

- 受信者のブラックリストおよびホワイトリスト（フィッシングサイトのアドレス情報を含む）との照合
- メッセージ本文のフレーズの調査
- 学習型アルゴリズムを使用したメッセージテキスト分析
- イメージファイルで送信されるスパムの認識

## 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、中小企業向けの最先端のソフトウェア製品です。言語解析テクノロジーと最新鋭のメールフィルタリング方法（DNS ブラックリスト機能や正式メール機能）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できます。任意のメールシステムとの互換性を持つため、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® SMTP Gateway

Kaspersky Mail Gateway は、メールシステムのユーザを完全に保護する包括的なソリューションです。このアプリケーションは、企業ネットワークとインターネットの間にインストールされます。ウイルスやその他マルウェア（スパイウェア、アドウェアなど）がないかどうかメールメッセージのコンポーネントをすべてスキャンし、メールストリームに対するアンチスパムフィルタリングを中央集中的に行います。アプリケーションには、名前および MIME 添付ファイルによってメールトラフィックをフィルタリングする多数の高度なツールが備わっています。また、メールシステムの負荷を削減するツール、ハッカーの攻撃を防ぐツールなど、一連のツールが含まれています。

## Kaspersky Anti-Virus® for Proxy Servers

Kaspersky Anti-Virus® for Proxy Server は、HTTP プロトコルを使用し、プロキシサーバ経由で転送される Web トラフィックを保護するためのアンチウイルスソリューションです。このアプリケーションはインターネットトラフィックをリアルタイムでスキャンし、ネットサーフィン中にマルウェアがシステムに侵入するのを防ぎ、インターネットからダウンロードされたファイルをスキャンします。

## Kaspersky® Security for PDA

Kaspersky® Security for PDA は、さまざまなハンドヘルドコンピュータおよびスマートフォンのデータをウイルスから保護します。プログラムには次のアンチウイルスツールが含まれています：

- **アンチウイルススキャナー** - 必要に応じてPDAと拡張カードのデータをスキャンします
- **アンチウイルスモニター** - 他の携帯端末や HotSync™ から転送されるファイルを監視し、ウイルスを遮断します

Kaspersky® Security for PDA は、デバイスやメモ리카ードのデータへのアクセスを暗号化することで、不正侵入からPDAを保護します。

## 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スキャン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

## C.2. お問い合わせ先

ご意見・ご質問等はカスペルスキーラボスまたは弊社ディストリビュータにてお伺いしております。

WWW :	<a href="http://www.kaspersky.co.jp">http://www.kaspersky.co.jp</a> <a href="http://www.viruslistjp.com">http://www.viruslistjp.com</a>
E-mail	support@kaspersky.co.jp

## 付録 D. ソフトウェア使用許諾契約書

「本製品」をご使用になる前に、「本製品」使用許諾契約書（以下、「本契約」という）の内容をご確認ください。この度は、弊社製品をご利用いただき、まことにありがとうございます。弊社では製品につきまして、下記のソフトウェア使用許諾契約書を設けさせていただいており、お客様が下記契約書にご同意いただいた場合のみ製品をご使用させていただいております。

### 第1条（定義）

- 1-1 「本製品」とは、本契約に基づき提供されるKaspersky(R) Anti-Virus/ Anti-Spam/ Security 及び関連資料を指します。
- 1-2 「クライアント機器」とは「本製品」をインストールするコンピュータあるいはワークステーション、個人デジタル機器およびその他電子機器を指します。

### 第2条（許諾事項）

- 2-1 「本製品」にはライセンスキー(識別キーファイル)またはライセンス適用向け識別コード(アクティベーションコード)が付属しています。本契約の条項に同意されたお客様に対し、カスペルスキーラプスは、本契約の有効期間中、「本製品」の非独占的かつ譲渡不可の使用権を許諾します。お客様は1ライセンスあたり、1台の「クライアント機器」にのみ製品をインストールすることができます。ファイルサーバ向け製品に関しては、物理サーバあるいは同時稼働OS毎にライセンスの購入が必要となります。トラフィックライセンスは一日あたりの流量(Megabyte per day)分のライセンスが必要となります。
- 2-2 「本製品」は、単独のソフトウェア・プログラムとしてライセンスされ、同時に2台以上の「クライアント機器」や2人以上のユーザーが利用することは出来ません。
- 2-3 「本製品」は、「クライアント機器」またはサーバのメインメモリにロードする、もしくはストレージ(ハードディスク、CD-ROM、その他の記憶装置)にインストールした場合、その「クライアント機器」上で「使用中」となります。
- 2-4 お客様はバックアップの目的で「本製品」のコピーを一部のみ制作することが出来ますが、当該コピーについては、不法コピーや不正利用防止のために適切な措置を講ずるものとします。
- 2-5 お客様が、「本製品」のインストールされた「クライアント機器」あるいはサーバを売却あるいは処分される場合は、「本製品」があらかじめ削除されていることを確認してください。

### 第3条（禁止事項）

- 3-1 「本製品」の全部または一部を複製、改変、リバースエンジニアリング、翻案、再配布、譲渡、貸与、再使用許諾、中古取引、レンタル、リースすることはできません。
- 3-2 お客様は「本製品」の逆コンパイル、リバースエンジニアリング、逆アセンブル、その他の方法で「本製品」の全部または一部を可読可能な形式に変換したり、第三者にそれらの行為を許可したりする事は出来ません。
- 3-3 「本製品」に付されているKaspersky(R)の商標、ロゴおよび画面イメージをカスペルスキーラプスの事前の書面による許諾なく使用し「本製品」の一部または全部を配布することはできません。
- 3-4 お客様は、製品の貸与およびリース、またライセンス権利の譲渡、サブライセンスの発行を行うことはできません。
- 3-5 お客様は、この製品をウイルスコード、ウイルス検知ルーチン、悪意のあるコードやデータ検知のための他のデータやコードの生成を意図した自動、半自動、手動ツールとして、使用できません。

### 第4条（ライセンス）

- 4-1 本契約は以下の条件によって契約が終了する場合を除き、1年間が有効期間となります。ここに記載された条件、制限、要件に反する行為がお客様により行われた場合、契約は自動的に解除されます。本契約の解除および有効期間切れの場合、お客様が保有している「本製品」及びそのコンポーネントを全て破棄してください。お客様が、製品および資料のコピーを破棄した時点で、本契約は終了します。  
製品が、製品購入契約書やパッケージにおいて使用可能な製品が指定され、ライセンスボリューム条項が適用されている場合、お客様はボリュームライセンスで指定された数の「クライアント機器」およびサーバに、コピーやインストール、利用が行えます。
- 4-2 お客様は、ライセンス数以上の製品が「クライアント機器」あるいはサーバにインストールされないことを保証するための、適切な予防措置を講ずるものとします。また、資料に関しては、合法利用の範囲内で、著作権情報を含むこと

を条件に、ライセンス数内でダウンロード及びコピーが許諾されます。

#### 第5条（サポート）

5-1 カスペルスキーラブスは、当該サポートサービスを含む製品の支払をいただいたお客様に、下記のサポートサービスをライセンスの有効期間に渡り提供します。

5-2 契約の満了時にライセンス更新料をお支払いいただき、ライセンス契約を更新されない限り、契約は更新されません。

5-3 ライセンス料をお支払いいただき、「本契約」に付属しているカスペルスキーラブスのプライバシーポリシーの条項に同意するとともに、プライバシーポリシーに詳述されているとおり、他国へのデータの転送を明示的に同意したものとみなされます。

5-4 サポートサービスとは

5-4-1 定義データベースの更新

5-4-2 バージョンアップを含む、ライセンス有効期間内の無料製品更新

5-4-3 販売元による電子メール及び電話にての技術サポート（サポートの形式、受付時間等の詳細は「本製品」の販売元にご確認ください）

#### 第6条（著作権）

「本製品」は日本の著作権法並びに国際条約の規定、その他使用される国において適用される法律により保護されています。カスペルスキーラブスならびに開発元は、は「本製品」の一切の権利、権限および持分につき、「本製品」に含まれるすべての著作権、特許、商標、営業秘密その他の知的財産権を所有し、維持しています。お客様は、「本製品」の所有、インストール、または使用など知的財産権に関する権利がお客様に譲渡されるものではないことを了承します。お客様はさらに、本契約に明示的に規定されていない限り、「本製品」のいかなる権利もお客様が取得するものではないことを了承します。お客様は、「本製品」及びマニュアルの全ての複製物に、「本製品」に表示されるものと同じ財産権が表示されることに同意します。

#### 第7条（機密保持）

お客様は、「本契約」に同意した段階で、特定のデザインと個々のプログラム構造およびライセンスキーを含む製品と資料が、カスペルスキーラブスが所有権をもつ機密情報に含まれていることに同意したとみなされます。お客様は、事前にカスペルスキーラブスの文書による承認なしに、公開、提供、あるいはそれらの機密情報を第三者が使用可能な形式にはいけません。お客様は、このような機密情報を守るために適切なセキュリティ手段を講ずる必要がある他、ライセンスキー情報の機密を保持する義務を持ちます。

#### 第8条（限定保証）

8-1 「本製品」はお客様に現状有姿にて提供され、カスペルスキーラブスは、「本製品」に対するバグや不具合を是正する責任を有さないものとします。

8-2 お客様の要求を満たすためにソフトウェアを選択されることについて、お客様がすべての責任を負うものといたします。カスペルスキーラブスは、「本製品」がお客様の特定の目的に適合すること、中断または誤りなく動作すること、第三者の権利を侵害していないことおよび「本製品」にバグや不具合がないことを保証しません。

8-3 カスペルスキーラブスは、「本製品」によるあらゆる既知のウイルスあるいはスパムその他のインターネット上の脅威の判別あるいは未感染ウイルスに誤りが無いということについて、何等の保証も行いません。

8-4 カスペルスキーラブス及び代理店は、ソフトウェア及びCD-ROM ならびに付属文書に関して、最初のダウンロード購入または物理的な媒体として購入されたソフトウェアのインストールの日から90日間、通常の使用下において、付属文書に記載された方法での使用に瑕疵がないことを条件に、その公表された性能を保証します。

8-5 お客様の唯一の救済および(8-4)の保証の違反に対するカスペルスキーラブスおよび代理店の全責任は、代理店が決定し、お客様が保障期間にカスペルスキーラブスあるいは正規販売代理店に報告された場合、代理店の判断により、「本製品」の修理あるいは交換あるいは返金がなされます。

8-6 以下のいずれかの条件に該当する場合、(8-4)の保証は適用されません。

8-6-1 使用者がカスペルスキーラブスの許可なく「本製品」を改ざんした場合。

8-6-2 想定外の方法あるいは目的で「本製品」を使用した場合。

8-6-3 本契約書で許可された範囲を超えて使用した場合。

8-7 本契約書にて述べられた保証および条件は、(8-5)で定義する条件を前提として、「本製品」および付属書類の供給、供給内容、供給の不備、供給の遅れに関し、同様に適用されるものとします。但し、本契約書が「本製品」及び資

料を取得する国の法律及び慣習と異なる場合は別途協議するものとする（この保証は、契約者が満足するまでの間無制限に行うものではなく、契約者が「本製品」を使用するにあたって一般的に必要なと考えられる知識、及び技術を持ち合わせていることが前提であり、また一般常識内で保証するものとする）。

#### 第9条（免責事項）

9-1 本契約は、次の場合のカスペルスキーラプス及び代理店の責任を除外または制限するものではありません。

9-1-1 虚偽の不法行為

9-1-2 注意義務違反による不履行、契約条項の不履行によって発生した死亡または身体障害

9-1-3 法による除外が不可能な義務

9-2 (9-1) の条件の下、次の損害または被害に対し、開発者は(契約、不法行為、賠償にかかわらず)いかなる責任も(そのような損失や被害を予見した、予見できた、知りえたかにかかわらず)負担することはありません。

9-2-1 収入の損失

9-2-2 実際のおよび将来の逸失利益（契約における利益の損失を含む）の損失

9-2-3 将来見込まれる貯蓄の損失

9-2-4 取引上の損失

9-2-5 機会損失

9-2-6 信用上の損失

9-2-7 信用毀損

9-2-8 データの消失、損傷あるいは改悪および損失

9-2-9 間接又は派生的損失 (9-2) 項の損失および損害を含む)

9-3 (9-1)の条件のもと、ソフトウェアの提供に関連して発生するカスペルスキーラプス及び代理店の責任(契約責任によるものであると不法行為によるものであるとを問わず)は、その原因がいかなるものであれ、その損害を引き起こしたソフトウェアの入手時にお客様が支払った金額または本製品の標準価格の何れか低い方を上限とします。

#### 第10条（プライバシーポリシー）

カスペルスキー製品および弊社が運営するWebサイトに適用されるプライバシーに関する方針は以下の通りです。プライバシーポリシーは予告なしに随時更新されますので、定期的に変更を確認してください。情報の詳細については、弊社Webサイトを参照してください。弊社のプライバシーポリシーの取り扱い等に関するお問い合わせは、末尾の情報を参照してください。

10-1（収集される情報の種類および保存）

カスペルスキーは、お客様の個人情報保護の意思を尊重します。ここでは、弊社がどのような情報を、どのような状況でお客様に要求することがあるかをお伝えします。カスペルスキーラプスは、お客様から製品のご注文、製品へのご登録、サービスのご依頼、調査へのご回答、コンテストへの参加、または当社とのメール交信やカスペルスキーWebサイト上での特定の活動に携わった場合に、以下の個人情報を求めることがあります。

10-1-1 オンライン販売（お客様の氏名、住所、クレジットカード番号などの取引に必要な情報）

10-1-2 テクニカルサポートへの問い合わせ（ライセンス番号、ご利用のハードウェアおよびソフトウェア情報その他サポートに必要な情報）

お客様は、個人情報を求められるこれらの行為に対し、手続きを進めるかどうかを決定することができます。ただし、お客様が求められた情報の提供を望まれない場合、処理が行われない場合があることをご了承ください。

10-2（情報の取り扱い）

カスペルスキーは、取得した個人情報を次の目的でのみ使用します

10-2-1 ウイルス警告、製品のアップグレード、新製品、サービス、ニュースレター、今後の製品のアイディアや改良についての調査

10-2-2 コンテンツ制作の補助

10-2-3 キャンペーン等の案内

10-2-4 お客様が製品の購入やダウンロード、サービスにアクセスし、その他お客様が選択された事項に関与される場合の許諾

10-2-5 情報を提供されたお客様にとって有用あるいは重要な製品およびサービスの検索

カスペルスキーラプスは、サービス提供のために外部のコントラクターのサービスを受けています。これらのコントラクターは、製品の出荷、テクニカルサポート、受注処理などを委託されている場合があります。コントラクターは、顧客の個人情報を保管し、秘密を保持する義務があり、カスペルスキーの代行としてのみ個人情報の取り扱いを行います。尚、カスペルスキーは、政府機関または法執行機関によって、お客様の個人情報の開示を法的に求められる場合が

あることをあらかじめご承知ください。

#### 10-3 (登録の解除)

もし、お客様が当社からのEメールによるニュースレターの受信や掲示板の閲覧を中止したい場合は、Eメールの件名に「登録解除」と入力してご返信ください。

#### 10-4 (セキュリティ)

カスペルスキーは、お客様の個人情報を保護するために、国際的な情報施策を採用しています。この施策は、お客様のデータの誤った使用、不正アクセスや開示、損失、改変や破棄から守る技術的かつ段階的な手順で行われています。クレジットカード情報の送信には、Secure Socket Layer(SSL)を使用しています。

カスペルスキーラボスは国際企業であり、社内の情報は当社の世界中のオフィスで共有されます。お客様が提供された個人情報は、カスペルスキーの他の国の事業所でも使用されることがあります。また、外部コントラクターが情報の収集、転送、保存、加工を請け負っている国もあります。

#### 10-5 (クッキー (Cookies))

カスペルスキーはカスペルスキーが運営するWebサイト上でクッキーを使用することがあります。クッキーとは、Webサイトからブラウザに送信することができるユニークなテキストファイルです。クッキーは利用者のブラウジングプリファレンスに基づいて、表示されるWebサイトの情報を作成することができます。カスペルスキーは、クッキーを利用して、お客様が閲覧されるページをユニークにしたり、利用者が登録した情報を記憶し、次回アクセス時のサイトの操作を容易にすることもできます。利用者がクッキーの受け入れを望まない場合は、クッキーを拒否あるいは、クッキーを受け入れる際に、ブラウザがアラートを表示するように設定することができます。ただし、クッキーを拒否することによって、Webサイト上の製品やサービスのご利用に、影響することがあります。カスペルスキーは、弊社Webサイトのアクセス状況を記録するためにもクッキーを使用します。この時、弊社のWebサーバに利用者のIPアドレスが記録されますが、この情報を元に個人を特定することはありません。

#### 10-6 (統計情報)

Webサーバに記録されるログには、利用者のドメイン名、IP アドレスおよびブラウザの種類が保存されます。これらの情報は、弊社Webサイトのアクセス状況を調べる目的にのみ利用されます。

他の企業および団体に関するプライバシーポリシー

カスペルスキーのWebサイトには、弊社の関係企業等へのリンクが含まれますが、カスペルスキーはそれらの企業・団体のプライバシー取り扱い方針に責任を負いません。それぞれのWebサイトで取られているプライバシーポリシーを確認してください。

#### 10-7 (非機密情報)

弊社が運営するフォーラムその他において、利用者がディスカッションあるいは送信する情報は、公開情報と見なされ、秘密および機密情報ではない点に留意してください。同様の情報は、サイトを閲覧している他人によって収集・利用される危険性があります。情報の取り扱いには注意を払い、責任を持って行動してください。

#### 10-8 (プライバシーポリシーに関する問い合わせ先)

株式会社Kaspersky Labs Japan

TEL: 03-5687-7839

support@kaspersky.co.jp

#### 第11条 (試用版に関する特約)

11-1 カスペルスキーラボスまたは代理店は、本製品を試用版として頒布する場合があります。お客様が本製品を試用版として入手された場合、お客様は、ソフトウェアを予め試用版で技術的に制限された期間内でのみ使用することができ、当該期間において (5-4-1) のサービスを無償で受けることができます。但し、アップデートサービスを除くその他のサービスをご利用いただくことはできません。

11-2 上記の使用期間を超えて引き続きソフトウェアを使用するためには、代理店から正規にライセンスをご購入いただく必要があります。

#### 第12条 (契約の優先)

本契約はソフトウェアの使用許諾について当事者間の完全な理解に基づいており、カスペルスキーラボスまたは代理店とお客様が本契約締結以前に口頭又は書面で交わした如何なる理解、約束、了解書面又は交渉による約束事に優先し、ソフトウェアの使用許諾に関する契約内容は全て本契約発効をもって効力を失います。