

KASPERSKY LABS JAPAN

Kaspersky[®] Anti-Virus for Linux Mail Server 5.6

管理者ガイド

© Kaspersky Labs Japan

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

2011 年 2 月

目次

第1章.	はじめに.....	6
1.1.	新機能.....	7
1.2.	製品要件.....	8
第2章.	アプリケーションの構造および動作アルゴリズム.....	9
第3章.	アプリケーションのインストールおよびアンインストール.....	12
3.1.	Linux が動作するサーバへのアプリケーション導入.....	12
3.2.	FreeBSD が動作するサーバへのインストール.....	13
3.3.	アプリケーションファイルの場所.....	14
3.3.1.	Linux が動作するサーバのディレクトリ構造.....	14
3.3.2.	FreeBSD が動作するサーバのディレクトリ 構造.....	16
3.4.	インストール後のセットアップ.....	17
3.5.	SELinux システムおよび AppArmor システムでのアクセス権ルールの設定.....	20
3.6.	Kaspersky Anti-Virus を管理する Webmin モジュールのインストール.....	22
3.7.	アプリケーションの削除.....	24
第4章.	MTA との統合.....	25
4.1.	Exim との統合.....	26
4.1.1.	ルータの変更による post-queue 形式の統合.....	26
4.1.2.	ダイナミックロードライブラリによる pre-queue 形式の統合.....	29
4.2.	Postfix との統合.....	31
4.2.1.	post-queue による統合.....	32
4.2.2.	pre-queue による統合.....	34
4.2.3.	Milter による統合.....	36
4.3.	qmail との統合.....	38
4.4.	Sendmail との統合.....	39
4.4.1.	.cf ファイルによる Sendmail との統合.....	40
4.4.2.	.mc ファイルによる Sendmail との統合.....	41
第5章.	メールアンチウイルス.....	42
5.1.	グループの設定.....	42
5.2.	メール分析ポリシーの定義.....	44

5.3. メールスキャンモード.....	44
5.3.1. ウイルススキャン.....	45
5.3.2. コンテンツフィルタリング.....	46
5.4. オブジェクトに適用する処理.....	47
5.5. 定義済みセキュリティプロファイル.....	49
5.5.1. recommended プロファイル.....	49
5.5.2. maximum protection プロファイル.....	50
5.5.3. maximum performance プロファイル.....	51
5.6. バックアップ.....	52
5.7. 通知.....	53
5.7.1. 通知の設定.....	53
5.7.2. 通知のテンプレート.....	55
5.7.3. 通知テンプレートのカスタマイズ.....	58
第 6 章. アンチウイルスによるファイル システムの保護.....	65
6.1. スキャン対象.....	65
6.2. オブジェクトのスキャンと感染駆除の モード.....	67
6.3. オブジェクトに対して実行する操作.....	68
6.4. 個別ディレクトリのオンデマンド スキャン.....	69
6.5. スケジュールスキャン.....	69
6.6. 管理者への通知.....	70
第 7 章. 定義データベースの更新.....	71
7.1. 定義データベースの自動更新.....	72
7.2. 定義データベースのオンデマンド更新.....	73
7.3. 定義データベース保存用ディレクトリの 作成.....	73
第 8 章. ライセンスキーの管理.....	75
8.1. キー詳細の表示.....	76
8.2. キーの更新.....	78
第 9 章. レポートと統計値.....	79
9.1. アプリケーションログ.....	79
9.2. アプリケーション統計値.....	82
第 10 章. 高度な設定.....	85
10.1. SNMP による保護ステータスの監視.....	85
10.2. アプリケーションのセットアップスクリプトの使用.....	89

10.3. コマンドラインからのアプリケーション管理	91
10.4. メッセージ内の追加情報フィールド	93
10.5. 表示される日時形式のローカライズ	94
第 11 章. アプリケーションのテスト	95
付録 A. 追加情報	97
A.1. アプリケーション設定ファイル「kav4lms.conf」	97
A.1.1. [kav4lms:server.settings] セクション	97
A.1.2. [kav4lms:server.log] セクション	100
A.1.3. [kav4lms:server.statistics] セクション	101
A.1.4. [kav4lms:server.snmp] セクション	102
A.1.5. [kav4lms:server.notifications] セクション	104
A.1.6. [kav4lms:filter.settings] セクション	105
A.1.7. [kav4lms:filter.log] セクション	107
A.1.8. [kav4lms:groups] セクション	109
A.1.9. [path] セクション	109
A.1.10. [locale] セクション	110
A.1.11. [options] セクション	111
A.1.12. [updater.path] セクション	111
A.1.13. [updater.options] セクション	111
A.1.14. [updater.report] セクション	112
A.1.15. [updater.actions] セクション	113
A.1.16. [scanner.display] セクション	115
A.1.17. [scanner.options] セクション	115
A.1.18. [scanner.report] セクション	118
A.1.19. [scanner.container] セクション	119
A.1.20. [scanner.object] セクション	120
A.1.21. [scanner.path] セクション	121
A.2. グループ設定ファイル	121
A.2.1. [kav4lms:groups.<group_name>. definition] セクション	122
A.2.2. [kav4lms:groups.<group_name>. settings] セクション	123
A.2.3. [kav4lms:groups.<group_name>.actions] セクション	125
A.2.4. [kav4lms:groups.<group_name>. contentfiltering] セクション	126
A.2.5. [kav4lms:groups.<group_name>. notifications] セクション	129
A.2.6. [kav4lms:groups.<group_name>. backup] セクション	131
A.3. kav4lms-licensemanager コンポーネントのコマンドラインパラメータ	132

A.4. kav4lms-licensemanager コンポーネントのリターンコード	133
A.5. kav4lms-keepup2date コンポーネントのコマンドラインパラメータ	134
A.6. kav4lms-keepup2date コンポーネントのリターンコード	135
付録 B. KASPERSKY LAB	136
B.1. 製品ラインナップ	136
B.2. お問い合わせ先	138
付録 C. サードパーティ製ソフトウェア	139
C.1. <i>Pcre</i> library.....	139
C.2. <i>Expat</i> library	140
C.3. <i>AgentX++v1.4.16</i> library	140
C.4. <i>Agent++v3.5.28a</i> library	145
C.5. <i>Boost v 1.0</i> library	147
C.6. <i>Milter</i> library.....	149
C.7. <i>Libkavexim.so</i> library	150
付録 D. 使用許諾契約書	157

第1章. はじめに

Kaspersky Anti-Virus® for Linux Mail Server 5.6 (以降、「Kaspersky Anti-Virus」または「アプリケーション」と表記) は、Linux または FreeBSD がオペレーティングシステムとして動作し、Sendmail、Postfix、qmail、または Exim MTA を使用するサーバで、メールトラフィックおよびファイルシステムのアンチウイルス処理を行います。

以下の機能があります：

- サーバファイルシステムおよび送受信されるメールメッセージをすべてチェックして脅威の有無を確認する
- 感染オブジェクト、疑わしいオブジェクト、破損したオブジェクト、パスワード保護されたオブジェクト、およびスキャンできないオブジェクトの検知
- ファイルおよびメールメッセージで検出した脅威の無害化および感染オブジェクトの駆除
- アンチウイルス処理とフィルタリングを適用するメールメッセージのバックアップ
- 送信者/受信者グループに事前設定されているルールに従ったメールトラフィックの処理
- 添付ファイルの名前、タイプ、およびサイズによってメールトラフィックをフィルタリングし、フィルタリングされたオブジェクトに対して個別に処理ルールを適用する
- 感染オブジェクト、疑わしいオブジェクト、破損したオブジェクト、パスワード保護されたオブジェクト、およびスキャンできないオブジェクトを含むメールメッセージを検知したことを送信者、受信者、および管理者に通知する
- アプリケーションのパフォーマンスに関する統計値とレポートの生成
- カスペルスキーのアップデートサーバを使用した、スケジュールまたはオンデマンドによる定義データベースの更新

定義データベースは、感染オブジェクトの検知と駆除に使用します。スキャン中は、各ファイルのコードをさまざまな脅威によく見られるコードと比較して分析します

- Kaspersky Anti-Virus をローカルで (コマンドラインオプション、シグナル、アプリケーション設定ファイルの修正など、標準の OS ツールを使用)、またはリモートから (Web ベースの Webmin インターフェイスを使用)、設定および管理する
- 製品の設定および動作に関する統計値を SNMP 経由で収集し、特定のイベントが発生したときに SNMP Trap を生成するようにアプリケーションを設定する

1.1. 新機能

Kaspersky Anti-Virus for Linux Mail Server のバージョン 5.6 では、Kaspersky Anti-Virus 5.5 for Linux and FreeBSD Mail Server および Kaspersky Anti-Virus 5.6 for Sendmail with Milter API の機能が統合され、さらに以下の機能が追加されています：

- Exim との統合では、pre-queue による方法と post-queue による方法がサポートされています。pre-queue の場合、メールはキューに追加される前にスキャンされます。post-queue の場合は、キューに追加された後にスキャンされます。新たにアプリケーション設定スクリプトによる自動統合も可能となりました。統合手順の詳細については、第 4 章 (25 ページ) を参照してください
- メールスキャン機能の設定方法が拡張され、2 つのスキャン方法を使用できるようになりました。1 通のメッセージを、1 つのオブジェクトとしてスキャンする方法と、最初に 1 つのオブジェクトとしてスキャンした後でパーツの集合体としてもう一度スキャンする方法があります。この 2 つの方法は、保護レベルに違いがあります。詳細については、5.2 (44 ページ) を参照してください
- アプリケーションの設定が変更されました。今回追加されたのは、複数の送信者/受信者グループを個別に設定する機能です。グループ設定の詳細については、5.1 (42 ページ) を参照してください
- メッセージに対する処理リストが拡張されました。これまでに検知したマルウェアに対応した新しい処理タイプが追加されています。詳細については、5.4 (47 ページ) を参照してください
- コンテンツフィルタリング機能が拡張され、添付ファイルのサイズを基準にしたフィルタリングが追加されました。詳細については、5.3.2 (46 ページ) を参照してください
- 通知テンプレートのライブラリに、管理用テンプレートが追加されました。また、管理用テンプレートは専用ディレクトリに保管されるようになりました
- バックアップに感染オブジェクトを移動することはできなくなりました
- バックアップ機能が強化され、情報ファイルをバックアップ項目ごとに作成できるようになりました。詳細については、5.6 (52 ページ) を参照してください
- ログ設定を詳細に指定できるようになり、レポート機能が向上しました。詳細については、9.1 (79 ページ) を参照してください
- 統計機能が拡張され、メッセージごとの統計値が追加されました。詳細については、9.2 (82 ページ) を参照してください
- 設定、統計、アプリケーションステータスに対する SNMP クエリをサポートできるようになりました。SNMP Trap もサポート対象です。詳細については、10.1 (85 ページ) を参照してください

- アプリケーションパッケージにコマンドライン管理ツールが追加されました。アプリケーション機能をさまざまな側面から管理できます。詳細については、10.3 (91 ページ) を参照してください

1.2. 製品要件

Kaspersky Anti-Virus のシステム要件は以下のとおりです：

- 1 日あたり 200MB のトラフィックがあるメールサーバに必要なハードウェア：
 - Intel Pentium IV プロセッサ、3GHz 以上
 - 1GB 以上のメモリ
 - ハードドライブの空き容量 200MB 以上 (これとは別にバックアップメッセージを保管するための容量が必要)
- 必要なソフトウェア：
 - いずれかの 32 ビットオペレーティングシステム：
 - Red Hat Enterprise Linux Server 5.2
 - Fedora 9
 - SUSE Linux Enterprise Server 10 SP2
 - openSUSE Linux 11.0
 - Debian GNU/Linux 4.0 r4
 - Mandriva Corporate Server 4.0
 - Ubuntu 8.04.1 Server Edition
 - FreeBSD 6.3, 7.0
 - いずれかの 64 ビットオペレーティングシステム：
 - Red Hat Enterprise Linux Server 5.2
 - Fedora 9
 - SUSE Linux Enterprise Server 10 SP2
 - openSUSE Linux 11.0
 - いずれかのメールシステム：Sendmail 8.12.x 以上、qmail 1.03、Postfix 2.x、Exim 4.x
 - オプション - Webmin プログラム (www.webmin.com) - Kaspersky Anti-Virus のリモート管理用
 - Perl 5.0 以上 (www.perl.org)

第2章. アプリケーションの構造および動作アルゴリズム

Kaspersky Anti-Virus は、以下のコンポーネントで構成されています：

- フィルタ - メールシステムへの接続用サービスで、Kaspersky Anti-Virus が特定の MTA と通信するための独立したプログラムです。製品配布パッケージには、サポートされている各メールシステムに対応したモジュールが含まれています：
 - kav4lms-milter - Milter API 経由で Sendmail と Postfix に接続する Milter サービス。
 - kav4lms-filter - SMTP サービス。Postfix および Exim との接続に使用
 - kav4lms-qmail - qmail 用のメールキューハンドラ
- kavmd - アプリケーションのメインサービス。フィルタ要求を待機し、メールトラフィックを保護するためのアプリケーションのアンチウイルス機能を実行する
- kav4lms-kavscanner - サーバファイルシステムのアンチウイルス
- kav4lms-keepup2date - カスペルスキーのアップデートサーバまたはローカルディレクトリから新しいデータをダウンロードして、定義データベースを更新する
- kav4lms-licensemanager - 製品キーを使用する操作（インストール、削除、統計値情報の表示）用のコンポーネント
- kav4lms.wbm - Web ベースのインターフェイス（オプション）からアプリケーションをリモート管理するための Webmin プラグインモジュール。定義データベースの設定および起動、統計値情報の表示、ステータスに応じたオブジェクト処理の定義、およびアプリケーションの動作結果の監視を行う
- kav4lms-cmd - コマンドラインから実行するアンチウイルス管理ユーティリティ

メールチェックは以下のアルゴリズムを使って行われます：

1. フィルタが MTA からメッセージを受信します。フィルタとメインサービスが同じコンピュータで動作している場合、分析用に渡されるのは実際のメッセージではなく、メッセージファイルの名前です
2. フィルタは、メッセージが属する複数グループのうち優先度が最も高いグループを選択し（42 ページの 5.1 を参照）、分析を行うメインサービスにメールを転送します。どのグループにも属さないメッセージは、アプリケーションの配布パッケージに含まれる **Default** グループに設定されているルールに従って処理されます

メインサービスは、グループの設定ファイルで指定されているパラメータを使用してメッセージをスキャンします。メッセージは、1 つのオブジェクトとしてスキャンする方法、または最初に全体をスキャンしてから個々のパーツをチェックするという 2 段階の手法で

分析することができます (44 ページの 5.2 を参照)。どちらの方法を使用するかは、**ポリシー**で定義されています

複合分析の場合、メッセージを全体的にチェックした後で個々のパーツをチェックするという 2 段階で行われる (2 段階ポリシー) ので、パフォーマンスは多少低下しますが、徹底的な分析が行われ、高い保護レベルが実現します

3. メールのウイルススキャンが有効になっている場合 (44 ページの 5.3 を参照)、メインサービスはメッセージを 1 つのオブジェクトとしてチェックします。チェック後に割り当てられたステータスに従って (44 ページの 5.3.1 を参照)、メインサービスは、メッセージ送信のブロック、メッセージの許可または拒否、メッセージと警告の置き換え、メッセージヘッダーの変更を行います (47 ページの 5.4 を参照)。マルウェアのタイプごとに専用の処理が定義されている場合 (**VirusNameList** オプション)、マルウェアが検知されると指定された処理が実行されます (**VirusNameAction** オプション)。メッセージの処理順序は、グループ設定ファイルで指定されています

グループ設定でバックアップが有効になっている場合は、メッセージを処理する前にそのバックアップが作成されます

4. グループ設定でフィルタリングが有効になっている場合は、メッセージのウイルススキャンに続いてフィルタリングが行われます

フィルタリングは、添付ファイルの名前、タイプ、およびサイズに基づいて行うことができます (46 ページの 5.3.2 を参照)。チェックの結果、グループの設定ファイルのフィルタリング設定で定義されている処理が実行されます。グループ設定で 2 段階処理が有効になっている場合、フィルタリング基準に一致する処理済みオブジェクトに対して、さらにパーツごとの分析が行われます

5. メールをパーツごとに検査する場合、その MIME 構造の解析およびメッセージコンポーネントの処理が行われます

メッセージオブジェクトは、メッセージ全体に割り当てられたステータスとは関係なく、個々のオブジェクトに割り当てられたステータスに従って処理されます

メッセージを 1 つのオブジェクトとして検査すると感染済みと認識されるのに個々のパーツを検査すると何も脅威が発見されない場合、感染メールに対して定義されている処理 (**InfectedAction** オプション) がメッセージ全体に対して適用されます。感染していないメッセージに添付されているオブジェクトのネストレベルがグループ設定で指定されている制限値 (**MaxScanDepth** オプション) を超えている場合は、スキャン中にエラーとして検出された文字列に対して定義されている処理 (**ErrorAction** オプション) がメッセージ全体に対して適用されます

メインサービスは、メッセージオブジェクトを処理する際、オブジェクトの名前変更、削除、または警告との置き換え、情報ヘッダーの追加、またはメッセージの許可を行います (47 ページの 5.4 を参照)。感染メッセージは、駆除されます。グループ設定でバックアップが有効になっている場合は、メッセージを処理する前に元のメッセージ全体のバックアップが作成されます

6. メインサービスは、スキャンと処理を終えたメッセージをフィルタに戻します。処理されたメッセージは、スキャンと感染駆除の結果通知とともに MTA に転送されます。MTA

はメールメッセージをローカルユーザに送信するか、または別のメールサーバに転送
します

第3章. アプリケーションのインストール およびアンインストール

Kaspersky Anti-Virus をインストールする前に、インストール先のシステムで以下の準備をしてください:

- システムが1.2 (8 ページ) で説明されている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
- サーバにインストールされているメールシステムの設定ファイルのバックアップを作成する
- インターネット接続を設定する
- **root** 権限でシステムにログインするか、またはスーパーユーザ権限を持つアカウントでシステムにログインする

警告!

アプリケーションのインストールは、負荷の低い時間帯またはメールトラフィックが一番少ないときに実行してください。

3.1. Linux が動作するサーバへのアプリケーション導入

Linux が動作するサーバの場合は、Linux ディストリビューションのタイプに基づいて、2 種類のうちのいずれかの Kaspersky Anti-Virus パッケージが提供されます。

Red Hat Enterprise Linux、Fedora、SUSE Linux Enterprise Server、openSUSE および Mandriva Linux にインストールする場合は、rpm パッケージを使用します。

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 <package_name>
```

警告!

アプリケーションを rpm パッケージからインストールした場合は、postinstall.pl スクリプトを実行してインストール後の設定を行う必要があります。postinstall.pl スクリプトは、デフォルトでは、Linux の場合は /opt/kaspersky/kav4lms/lib/bin/setup/ ディレクトリに、FreeBSD の場合は /usr/local/libexec/kaspersky/kav4lms/setup/ に、それぞれ置かれています。

Debian GNU/Linux および Ubuntu の場合は、deb パッケージからインストールします。

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 <package_name>
```

コマンドを入力すると、アプリケーションは自動的にインストールされます。インストールが完了すると、インストール後の設定に関する情報が表示されます (16 ページの 3.4 を参照)。

警告！

Mandriva ディストリビューションでのセットアップ手順は、少し特殊です。

インストール後に Kaspersky Anti-Virus が正常に起動されるようにするには、オペレーティングシステムの一部ファイルの保管先として /root/tmp ディレクトリを使用し、そのディレクトリに対する書き込み権限を、アプリケーションの実行に使用するアカウント (デフォルトでは kluser) に付与する必要があります。

場合によっては、そのディレクトリのアクセス権を変更するか、環境変数の **TMP** と **TEMP** を再定義または削除して、アプリケーションが正常に動作するために必要なアクセス権が設定された別のディレクトリ (/tmp/ など) をシステムが使用するようする必要があります。

3.2. FreeBSD が動作するサーバへのインストール

FreeBSD が動作するサーバに Kaspersky Anti-Virus をインストールするには、pkg パッケージを使用します。

Kaspersky Anti-Virus のインストールを pkg 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：

```
# pkg_add <package_name>
```

コマンドを入力すると、アプリケーションは自動的にインストールされます。インストールが完了すると、インストール後の設定に関する情報が表示されます (16 ページの 3.4 を参照)。

3.3. アプリケーションファイルの場所

Kaspersky Anti-Virus のセットアップ中は、サーバ上のプログラムディレクトリにアプリケーションファイルがコピーされます。

注意！

`man <man_page_name>` コマンドでアプリケーションのマニュアルページが表示されるようにするには、以下の手順を実行する必要があります：

- Debian および SuSE Linux ディストリビューションの場合は、`/etc/manpath.config` ファイルに以下の行を追加します：
`MANDATORY_MANPATH /opt/kaspersky/kav4lms/share/man`
- Red Hat Linux および Mandriva Linux ディストリビューションの場合は、`/etc/man.config` ファイルに以下の行を追加します：
`MANPATH /opt/kaspersky/kav4lms/share/man`
- FreeBSD ディストリビューションの場合は、`/etc/manpath.config` ファイルに以下の行を追加します：
`MANDATORY_MANPATH /usr/local/man`

MANPATH 変数を使用する場合、以下のコマンドを実行して、アプリケーションのマニュアルページが含まれるディレクトリへのパスをその値リストに追加します：

```
# export MANPATH=$MANPATH:<path to the man pages directory>
```

3.3.1. Linux が動作するサーバのディレクトリ構造

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/kav4lms.conf` - アプリケーションのメインの設定ファイル

`/etc/opt/kaspersky/kav4lms` - Kaspersky Anti-Virus 設定ファイルが含まれるディレクトリ

`groups.d/` - グループの設定ファイルが含まれるディレクトリ

`default.conf` - デフォルトグループの設定が含まれる設定ファイル

`locale.d/strings.en` - アプリケーションが使用する文字列が含まれるファイル

`profiles/` - 事前定義された設定プロファイルが含まれるディレクトリ：

`default_recommended/` - デフォルト設定ファイルが含まれるディレクトリ

`high_overall_security/` - 高セキュリティプロファイルの設定ファイルが含まれるディレクトリ

`high_scan_speed/` - 高速スキャンプロファイルの設定ファイルが含まれるディレクトリ

`templates/` - 通知テンプレートが含まれるディレクトリ

`templates-admin/` - 管理者の通知テンプレートが含まれるディレクトリ

kav4lms.conf - アプリケーションのメイン設定ファイル

/opt/kaspersky/kav4lms/ - Kaspersky Anti-Virus のメインディレクトリ。以下の内容が含まれません:

- /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
 - kav4lms-cmd - コマンドラインツールの実行ファイル
 - kav4lms-setup.sh - アプリケーションのセットアップスクリプト
 - kav4lms-kavscanner - ファイルシステムスキャンコンポーネントの実行ファイル
 - kav4fs-licensemanager - キー管理コンポーネントの実行ファイル
 - kav4lms-keepup2date - 更新処理コンポーネントの実行ファイル
- sbin/ - アプリケーションのサービスの実行ファイルが含まれるディレクトリ
- lib/ - Kaspersky Anti-Virus のライブラリファイルが含まれるディレクトリ
 - bin/avbasestest - kav4lms-keepup2date コンポーネントが使用する、定義データベースのダウンロード済み更新を検証するユーティリティ
- share/doc/ - 使用許諾契約書および導入マニュアル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
- share/scripts/ - アプリケーションスクリプトが含まれるディレクトリ
- share/snmp-mibs/ - Kaspersky Anti-Virus の MIB が含まれるディレクトリ
- share/webmin/ - Webmin アプリケーションのプラグインが含まれるディレクトリ

/etc/init.d/ - アプリケーションのサービスの制御スクリプトが含まれるディレクトリ:

- kav4lms - アプリケーションのメインサービスの制御スクリプト
- kav4lms-filters - Kaspersky Anti-Virus フィルタの制御スクリプト

/var/opt/kaspersky/kav4lms/ - Kaspersky Anti-Virus の可変データが含まれるディレクトリ:

- backup/ - メッセージのバックアップおよび情報ファイルが含まれるディレクトリ
- bases/ - 定義データベースが含まれるディレクトリ
- bases.backup/ - 定義データベースのバックアップが含まれるディレクトリ
- licenses/ - キーファイルが含まれるディレクトリ
- nqueue/ - メールキューファイルが含まれるディレクトリ
- patches/ - アプリケーションモジュールの更新が含まれるディレクトリ
- stats/ - 統計ファイルが含まれるディレクトリ
- updater/ - 最後に行われた更新に関する情報ファイルが含まれるディレクトリ

警告!

このマニュアルでは、これ以降は Linux 関連のパスを使用します。

3.3.2. FreeBSD が動作するサーバのディレクトリ構造

FreeBSD OS が動作するサーバ上では、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:

/usr/local/etc/Kaspersky/kav4lms.conf - アプリケーションのメインの設定ファイル

/usr/local/etc/kaspersky/kav4lms/ - Kaspersky Anti-Virus の設定ファイルが含まれるディレクトリ:

groups.d/ - グループの設定ファイルが含まれるディレクトリ

default.conf - デフォルトグループの設定が含まれる設定ファイル

locale.d/strings.en - アプリケーションが使用する文字列が含まれるファイル

profiles/ - 事前定義された設定プロファイルが含まれるディレクトリ:

default_recommended/ - デフォルト設定ファイルが含まれるディレクトリ

high_overall_security/ - 高セキュリティプロファイルの設定ファイルが含まれるディレクトリ

high_scan_speed/ - 高速プロファイルの設定ファイルが含まれるディレクトリ

templates/ - 通知テンプレートが含まれるディレクトリ

templates-admin/ - 管理者の通知テンプレートが含まれるディレクトリ

kav4lms.conf - アプリケーションのメイン設定ファイル

/usr/local/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:

kav4lms-cmd - コマンドラインツールの実行ファイル

kav4lms-setup.sh - アプリケーションのセットアップスクリプト

kav4lms-kavscanner - ファイルシステムスキャンコンポーネントの実行ファイル

kav4lms-licensemanager - キー管理コンポーネントの実行ファイル

kav4lms-keepup2date - 更新処理コンポーネントの実行ファイル

/usr/local/sbin/ - アプリケーションのサービスの実行ファイルが含まれるディレクトリ

/usr/local/etc/rc.d/ - アプリケーションのサービスの制御スクリプトが含まれるディレクトリ:

kav4lms.sh - アプリケーションのメインサービスの制御スクリプト

kav4lms-filters.sh - Kaspersky Anti-Virus フィルタの制御スクリプト

/usr/local/lib/kaspersky/kav4lms/ - Kaspersky Anti-Virus のライブラリファイルが含まれるディレクトリ

/usr/local/libexec/kaspersky/kav4lms/avbasestest - kav4lms-keepup2date コンポーネントが使用する、定義データベースのダウンロード済み更新を検証するユーティリティ

/usr/local/share/doc/kav4lms/ - 使用許諾契約書および導入マニュアルが含まれるディレクトリ

/usr/local/man/ - マニュアルが含まれるディレクトリ

/usr/local/share/kav4lms/scripts/ - アプリケーションスクリプトが含まれるディレクトリ

/usr/local/share/kav4lms/snmp-mibs/ - Kaspersky Anti-Virus の MIB が含まれるディレクトリ
/usr/local/share/kav4lms/webmin/ - Webmin アプリケーションのプラグインが含まれるディレクトリ
/var/db/kaspersky/kav4lms/ - Kaspersky Anti-Virus の可変データが含まれるディレクトリ:
 backup/ - メッセージのバックアップおよび情報ファイルが含まれるディレクトリ
 bases/ - 定義データベースが含まれるディレクトリ
 bases.backup/ - 定義データベースのバックアップが含まれるディレクトリ
 licenses/ - キーファイルが含まれるディレクトリ
 nqueue/ - メールキューファイルが含まれるディレクトリ
 patches/ - アプリケーションモジュールの更新が含まれるディレクトリ
 stats/ - 統計ファイルが含まれるディレクトリ
 updater/ - 最後に行われた更新に関する情報ファイルが含まれるディレクトリ

3.4. インストール後のセットアップ

アプリケーションのファイルがサーバにコピーされるとすぐに、システム設定プロセスが実行されません。設定手順は自動的に始まります。パッケージマネージャ (rpm など) で対話式スクリプトの使用が禁じられている場合は、手動で設定手順を開始する必要があります。

製品の設定を開始するには、コマンドラインで以下のように入力します：

Linux の場合：

```
# /opt/kaspersky/kav4lms/lib/bin/setup/postinstall.pl
```

FreeBSD の場合：

```
# /usr/local/libexec/kaspersky/kav4lms/setup/postinstall.pl
```

以下の操作を実行します：

1. コンピュータ上に Kaspersky Anti-Virus 5.5 for Linux Mail Server または Kaspersky Anti-Virus 5.6 for Sendmail with Milter API の設定ファイルが存在する場合、その設定ファイルを選択して現在の製品バージョンの形式に変換し、保存することができます。既存の設定ファイルを選択した場合は、配布パッケージに含まれるデフォルトの設定ファイルの代わりに、設定ファイルを変換したファイルが使用されます

「**yes**」を入力すると、配布パッケージの設定ファイルが変換された設定ファイルに置き換えられます。「**no**」を入力すると、配布パッケージの設定ファイルが使用されます

変換された設定ファイルは、デフォルトでは以下のディレクトリに保存されます:

```
kav4mailservers -  
/etc/opt/kaspersky/kav4lms/profiles/kav4mailservers5.  
5-converted  
kavmilter -  
/etc/opt/kaspersky/kav4lms/profiles/kavmilter5.6-  
converted
```

2. キーファイルへのパスを指定します

製品キーがインストールされていないと、インストール中に定義データベースの更新および保護対象ドメインの作成が行なわれません。その場合は、キーをインストールした後で、手動でそれらの作業を実行する必要があります

3. 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指定します:

```
http://<IP-proxy_server_address>:<port>
```

または

```
http://<user_name>:<password>@<proxy_server_IP_address>:<port>
```

(プロキシサーバが認証を必要とする場合)

インターネット接続でプロキシサーバを使用しない場合は「**no**」を入力します

kav4lms-keepup2date 更新コンポーネントは、ここで指定された値を使用して更新元に接続します

4. 定義データベースを更新するには、「**yes**」を入力します。更新しない場合は「**no**」を入力します。後で更新手順を実行する場合は、kav4lms-keepup2date コンポーネントを使用します (詳細は 73 ページの 7.2 を参照)

注記:

定義データベースを更新するには、インストールされている製品キーが必要です。

5. 定義データベースの自動更新を設定するには、「**yes**」を入力します。ここでは自動更新を設定しない場合は「**no**」を入力します。後で更新を設定する場合は、kav4lms-setup コンポーネントを使用するか (72 ページの 7.1 を参照)、または手動で設定します (89 ページの 10.2 を参照)

警告!

qmail の自動更新と統合する場合は、以下のコマンドを実行します:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \  
--install-cron-updater --user=root
```

6. Webmin の Web インターフェイスで Kaspersky Anti-Virus を管理するための Webmin モジュールをインストールします

リモート管理プラグインがインストールされるのは、Webmin がデフォルトディレクトリにインストールされている場合だけです。プラグインがインストールされた後、プラグインとアプリケーションの間の通信設定に関するガイドラインが表示されます

Webmin モジュールをインストールするには「**yes**」を、インストールしない場合は「**no**」を入力します

7. メールトラフィックをウイルスから保護するドメインのリストを指定します。デフォルト値は「**localhost, localhost.localdomain**」です。そのまま使用の場合は [Enter] キーを押します

手動でドメインのリストを指定する場合は、コマンドラインで入力します。複数の値を指定する場合は、カンマ区切り形式で入力します。マスクや正規表現を使用できます。ピリオドはスラッシュでエスケープします

例:

```
re:.*\.example\.com
```

8. Kaspersky Anti-Virus を MTA と統合します。コンピュータに既存の MTA と統合する方法として、提示されたデフォルト値をそのまま使用するか、またはここで統合せずに手動で実行することもできます。MTA との統合の詳細については、第 4 章 (25 ページ) を参照してください

デフォルトでは、Exim と Postfix のキュー追加後の統合が行われます (26 ページの 4.1.1 および 32 ページの 4.2.1 を参照)

警告!

Sendmail との自動統合スクリプトは、常に `.mc` ファイルの変更を試みます。これは、その後の更新では入力された値が保持されるからです。存在しない `.mc` ファイルを参照するインクルードが `.mc` ファイル内で設定されている場合、この `.mc` ファイルは Kaspersky Anti-Virus の統合で使用できません。その場合は、**sendmail-cf** パッケージをインストールして、`.cf` ファイルを使用した統合を行います。

統合で `.mc` ファイルを使用できない場合は、代わりに `.cf` ファイルが使用されます。

3.5. SELinux システムおよび AppArmor システムでのアクセス権ルールの設定

Kaspersky Anti-Virus の動作に必要なルールを使用して SELinux モジュールを作成するには、セットアップとメールシステムとの統合が完了した後で、以下の手順を実行します：

1. SELinux を Permissive モードに切り替えます：

```
# setenforce Permissive
```
2. テストメッセージを 1 件以上送信して、メッセージがウイルススキャンをパスして受信者に送信されることを確認します
3. ブロックレコードに基づいてルールモジュールを作成します：
Fedora の場合：

```
# audit2allow -l -M kav4lms -i /var/log/messages
```


RHEL の場合：

```
# audit2allow -l -M kav4lms -i /var/log/audit/audit.log
```
4. 生成されたルールモジュールを読み込みます：

```
# semodule -i kav4lms.pp
```
5. SELinux を enforcement モードに切り替えます：

```
# setenforce Enforcing
```

Kaspersky Anti-Virus に関する新しい監査メッセージが表示された場合は、ルールモジュールファイルを更新する必要があります：

Fedora の場合：

```
# audit2allow -l -M kav4lms -i /var/log/messages  
# semodule -u kav4lms.pp
```

RHEL の場合：

```
# audit2allow -l -M kav4lms -i /var/log/audit/audit.log  
# semodule -u kav4lms.pp
```

詳細については、以下の資料を参照してください：

- **RedHat Enterprise Linux**：『Red Hat Enterprise Linux Deployment Guide』の第 44 章「Security and SELinux」
- **Fedora**：Fedora SELinux Project Pages

- **Debian**: 『Documentation for Security Enhanced Linux』selinux-doc パッケージの『Configuring the SELinux Policy』

Kaspersky Anti-Virus の動作に必要な AppArmor プロファイルを更新するには、セットアップとメールシステムとの統合が完了した後で、以下の手順を実行します：

1. アプリケーションのルールをすべて complain モードに切り替えます：

```
# aa-complain /etc/apparmor.d/*  
# /etc/init.d/apparmor reload
```
2. メールシステムを再起動します：

```
# /etc/init.d/postfix restart
```
3. kav4lms と kav4lms-filters を再起動します：

```
# /etc/init.d/kav4lms restart  
# /etc/init.d/kav4lms-filters restart
```
4. テストメッセージを 1 件以上送信して、メッセージがウイルススキャンをパスして受信者に送信されることを確認します
5. プロファイル更新ユーティリティを起動します：

```
# aa-logprof
```
6. AppArmor ルールを再度読み込みます：

```
# /etc/init.d/apparmor reload
```
7. アプリケーションのルールをすべて enforcement モードに切り替えます：

```
# aa-enforce /etc/apparmor.d/*  
# /etc/init.d/apparmor reload
```

Kaspersky Anti-Virus に関する新しい監査メッセージが表示された場合は、ステップ 5 と 6 を繰り返す必要があります。

詳細については、以下の資料を参照してください：

- **openSUSE** および **SUSE Linux Enterprise Server**: 『Novell AppArmor Quick Start』、『Novell AppArmor Administration Guide』
- **Ubuntu**: 『Ubuntu Server Guide』の第 8 章「Security」

3.6. Kaspersky Anti-Virus を管理する Webmin モジュールのインストール

Kaspersky Anti-Virus の動作は、Webmin を使って Web ブラウザでリモートコントロールできません。


Webmin は、Linux/Unix システムの管理を簡単に行えるようにするプログラムです。このソフトウェアはモジュール構造になっており、新規モジュールやカスタムモジュールの接続をサポートします。Webmin についての追加情報、Webmin パッケージのダウンロードについては、www.webmin.com を参照してください。

Kaspersky Anti-Virus の導入パッケージには、Webmin モジュールが含まれています。このモジュールへの接続は、システムに Webmin がインストール済みであればアプリケーションインストール後の設定 (17 ページの 3.4 を参照) のとき、または Webmin インストール後にいつでも可能です。

これ以降では、Webmin モジュールに接続して Kaspersky Anti-Virus を管理できるようにするために必要な手順を詳しく説明します。

Webmin のインストールでデフォルト設定を使用してあれば、インストール手続きの終了後すぐに HTTP/HTTPS を使用してポート 10000 に接続し、Web ブラウザから Webmin にアクセスできます。

Webmin モジュールをインストールするには：

1. Web ブラウザを使用して、管理者権限で Webmin にアクセスします
2. プログラムメニューの [**Webmin Configuration**] タブを選択し、[**Webmin Modules**] セクションに進みます。
3. [**Install Module**] セクション内の [**From Local File**] を選択し、 をクリックします (図 1)

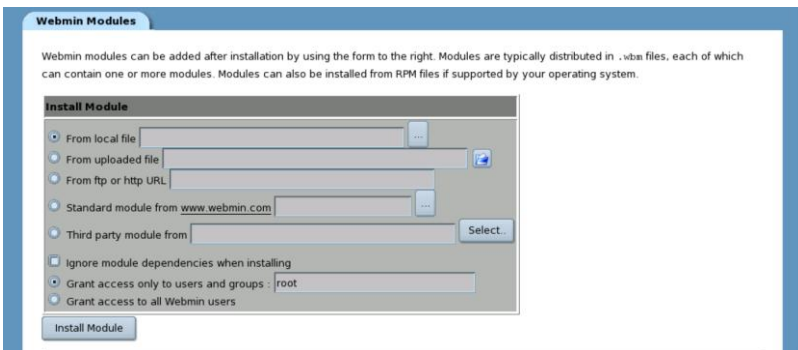


図 1. [**Install Module**] セクション

4. 製品の Webmin モジュールへのパスを選択し、[OK] をクリックします

注記:

Webmin モジュールは mailgw.wbm というファイルです。このモジュールは /opt/kaspersky/kav4lms/share/webmin/ ディレクトリ (Linux の場合) または /usr/local/share/kav4lms/webmin/ ディレクトリ (FreeBSD の場合) にデフォルトでインストールされます。

Webmin モジュールのインストールが正常に行われたことを示すメッセージが、画面に表示されます。

[**Others**] タブ内のアイコンをクリックすると、Kaspersky Anti-Virus の設定にアクセスできます (図 2)



図 2. [**Others**] タブ内の Kaspersky Anti-Virus

3.7. アプリケーションの削除

Kaspersky Anti-Virus をサーバから削除するには、スーパーユーザ (**root**) 権限が必要です。必要な権限を持っていないユーザは、まず **root** としてログオンしてから削除処理を開始する必要があります。

警告！

削除処理は自動実行され、アプリケーションが停止します。ユーザによる操作は必要ありません。

削除処理では、アプリケーションが停止され、インストール時に作成されたファイルとディレクトリが削除されます。ただし、管理者が作成または変更したファイルとディレクトリ (アプリケーションの設定ファイル、グループの設定ファイル、テンプレート通知ファイル、バックアップディレクトリ、キーファイル) は削除されずに残ります。

アプリケーションの削除処理は、パッケージマネージャごとに異なる方法で起動できます。ここでは、それぞれの方法について詳細に説明します。

rpm パッケージからインストールした Kaspersky Anti-Virus を削除する場合は、コマンドラインで以下のように入力します：

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

deb パッケージからインストールした Kaspersky Anti-Virus を削除する場合は、コマンドラインで以下のように入力します：

```
# dpkg -P <package_name>
```

アプリケーションと一緒に設定ファイルも削除されます。または、以下のように入力するとアプリケーションは削除されますが、設定ファイルは削除されません：

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

pkg パッケージからインストールした Kaspersky Anti-Virus を削除する場合は、コマンドラインで以下のように入力します：

```
# pkg_delete <package_name>
```

アプリケーションの削除が正常に行われたことを示すメッセージが、画面に表示されます。

アプリケーションのリモート管理プラグイン (Webmin モジュール) がインストールされている場合は、標準の Webmin ツールを使用して手動で削除する必要があります。

第4章. MTA との統合

インストールした Kaspersky Anti-Virus は、ホストのメールシステムと統合する必要があります。そのためには、アプリケーションと MTA のそれぞれの設定ファイルのパラメータを変更します。統合を実行するには、配布パッケージに含まれる設定スクリプトを使用するか (17 ページの 3.4 および 89 ページの 10.2 を参照)、またはそれぞれの設定ファイルを手動で変更します。

Exim での統合は、pre-queue による方法と post-queue による方法がサポートされています。pre-queue による統合の場合、メッセージは MTA キューに追加される前に分析のために転送されます。post-queue による統合の場合、メッセージは MTA キューに追加された後に分析されません。

注記:

post-queue による統合を使用する場合、MTA でメールを拒否することはできません。ただし、Kaspersky Anti-Virus の設定でオブジェクトに対する操作として **reject** が選択されている場合、送信者はメッセージ拒否通知を受信します。通知テキストは、グループ設定ファイルの **[kav4lms: groups. <group_name>.settings]** セクションの **RejectReply** オプションで定義します。

MTA、フィルタ、および Kaspersky Anti-Virus のメインサービスとの間のデータ交換で使用されるソケットは、以下のルールに従って割り当てられます:

- `inet:<port>@<ip_address>` - ネットワークソケットの場合
- `local:<socket_path>` - ローカルソケットの場合

警告!

ソケットを使用する場合、以下のルールに従う必要があります:

- ポート番号 (ネットワークソケット定義の一部) は 1024 よりも大きくなければならない
- フィルタとメインサービスはどちらも、使用するローカルソケットにアクセスするために必要な権限を持っていないなければならない

4.1. Exim との統合

Kaspersky Anti-Virus では、2 つの方法で Exim と統合できます：

- **ルータの変更による post-queue 形式の統合**：保護対象サーバを通過するメールトラフィックはすべて、MTA キューに追加された後にスキャンのために転送される (post-queue のフィルタリング)
- **ダイナミックロードライブラリによる pre-queue 形式の統合**：メッセージは、MTA キューに追加される前にスキャンのために転送される (pre-queue のフィルタリング)

4.1.1. ルータの変更による post-queue 形式の統合

ルータの変更による統合では、すべてのメール転送エージェントからのメッセージがスキャンのために転送されます。そのためには、各 Exim ルータの **pass_router** オプションの値として **kav4lms_filter** を指定する必要があります。

post-queue による統合では、Kaspersky Anti-Virus へのメール転送および MTA への返送を正常に動作させるために、以下の条件を満たす必要があります：

1. MTA からのメッセージをフックするようにフィルタを設定する必要があります。「フィルタ - MTA」接続の終端は、メインのアプリケーション設定ファイルの **[kav4lms:filter.settings]** セクションの **FilterSocket** オプションで定義されるソケットです
2. フィルタは、スキャンのためにメインサービスにメッセージを渡す必要があります。「フィルタ - メインサービス」接続の終端は、メインのアプリケーション設定ファイルの **[kav4lms:server.settings]** セクションの **ServiceSocket** オプションで定義されるソケットです

警告！

フィルタを Exim と統合する場合、**FilterSocket**、**ServiceSocket**、および **ForwardSocket** の各オプションがネットワークソケットを参照するように設定する必要があります。

3. フィルタはメッセージを MTA に返送する必要があります。「アプリケーション - MTA」接続の終端は、メインのアプリケーション設定ファイルの **[kav4lms:filter.settings]** セクションの **ForwardSocket** オプションで定義されるソケットです

アプリケーション設定スクリプトを使用して Kaspersky Anti-Virus を Exim と統合するには:

以下のコマンドを実行します:

Linux の場合:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \  
--install-filter=exim
```

FreeBSD の場合:

```
# /usr/local/bin/kav4lms-setup.sh \  
--install-filter=exim
```

手動で Kaspersky Anti-Virus を Exim と統合するには:

1. Exim 設定ファイルのバックアップを作成します
2. Exim 設定ファイルの **main configuration settings** セクションに以下の行を追加します:

```
#kav4lms-filter-begin-1  
local_interfaces=0.0.0.0.25:<forward_socket_ip>.\ \  
<forward_socket_port_number>  
#kav4lms-filter-end-1
```

<forward_socket_ip>.<forward_socket_port_number> には、スキャン後にメールを転送するソケットの IP アドレスとポートを設定します

3. Exim 設定ファイルの **routers** セクションに以下の行を追加します:

```
#kav4lms-filter-begin-2  
kav4lms_dnslookup:  
    driver = dnslookup  
    domains = ! +local_domains  
    ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8  
    verify_only  
    pass_router = kav4lms_filter  
    no_more  
  
kav4lms_system_aliases:  
    driver = redirect  
    allow_fail  
    allow_defer  
    data = ${lookup{$local_part}lsearch{/etc/aliases}}  
    verify_only  
    pass_router = kav4lms_filter
```

```

kav4lms_localuser:
    driver = accept
    check_local_user
    verify_only
    pass_router = kav4lms_filter

failed_address_router:
    driver = redirect
    verify_only
    condition = "{0}"
    allow_fail
    data = :fail: Failed to deliver to address
    no_more

kav4lms_filter:
    driver = manualroute
    condition = "${if or {{eq {$interface_port}} \
<forward_socket_port_number>}} \
    {eq {$received_protocol}{spam-scanned}} \
    }{0}{1}"
    transport = kav4lms_filter
    route_list = "* localhost byname"
    self = send
#kav4lms-filter-end-2

```

<forward_socket_port_number> は、チェック後のメールが転送されるポート番号です

4. Exim の **transports** セクションに以下の行を追加します:

```

#kav4lms-filter-begin-3
kav4lms_filter:
    driver = smtp
    port = <filter_socket_port_number>
    delay_after_cutoff = false
    allow_localhost
#kav4lms-filter-end-3

```

<filter_socket_port_number> は、フィルタサービスが待機するポート番号です

5. **ForwardSocket** パラメータにステップ 2 の
<forward_socket_ip>.<forward_socket_port_number> を設

定します。**ForwardSocket** パラメータは、kav4lms.conf 設定ファイルの **[kav4lms:filter.settings]** セクションにあります

6. kav4lms-filter サービスを停止します
7. 以下の行を /var/opt/kaspersky/applications.setup (Linux の場合) または /var/db/kaspersky/applications.setup (FreeBSD の場合) の **[1043]** セクションに追加します

```
FILTER_SERVICE=true
FILTER_SERVICE=kav4lms-filter
```

8. kav4lms-filter サービスを開始します
9. Exim を再起動します

4.1.2. ダイナミックロードライブラリによる pre-queue 形式の統合

フィルタは、スキャンのためにメインサービスにメッセージを渡す必要があります。「フィルタ - メインサービス」接続の終端は、メインのアプリケーション設定ファイルの **[kav4lms:server.settings]** セクションの **ServiceSocket** オプションで定義されるソケットです。

アプリケーション設定スクリプトを使用して Kaspersky Anti-Virus を Exim と統合するには:

以下のコマンドを実行します:

Linux の場合:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=exim-dlfunc
```

FreeBSD の場合:

```
# /var/db/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=exim-dlfunc
```

Kaspersky Anti-Virus を Exim と手動で統合するには:

1. Exim で dlfunc コンテンツフィルタリング機能がサポートされていることを確認します。
以下のコマンドを実行します:

```
exim -bV
```

サポートされている場合は、以下のようなテキストが表示されます

```
Expand_dlfunc
```

2. Exim 設定ファイルのバックアップを作成します
3. Exim 設定ファイルの **main configuration settings** セクションに以下の行を追加します:

```
#kav4lms-filter-begin  
acl_smtp_data = acl_check_data  
#kav4lms-filter-end
```

4. Exim 設定ファイルの **ACL** セクションに以下の行を追加します:

```
acl_check_data:  
#kav4lms-dlfunc-begin  
warn set acl_m0 = \  
${dlfunc{<libkavexim.so>}{kav}{<socket>}\ \  
{/var/tmp//.kav4lms-exim}}  
accept condition = ${if match{$acl_m0}{\N^kav4lms: \  
continue\N}{yes}{no}}  
logwrite = kav4lms returned continue  
deny condition = ${if match{$acl_m0}{\N^kav4lms: \  
reject.*\N}{yes}{no}}  
logwrite = kav4lms returned reject  
message = Kaspersky Anti-Virus rejected the mail  
discard condition = ${if match{$acl_m0}\ \  
{\N^kav4lms: drop.*\N}{yes}{no}}  
logwrite = kav4lms returned drop  
message = Kaspersky Anti-Virus dropped the mail  
defer condition = ${if match{$acl_m0}\ \  
{\N^kav4lms: temporary failure.*\N}{yes}{no}}  
logwrite = kav4lms returned temporary failure  
message = Kaspersky Anti-Virus returned \  
temporary failure  
accept  
#kav4lms-dlfunc-end
```

<socket> はフィルタと Kaspersky Anti-Virus のメインサービスとの通信に使用されるソケットを表し、Kaspersky Anti-Virus のメイン設定ファイルの

[kav4lms:server.settings] セクションにある **ServiceSocket** によって設定されています。<libkavexim.so> は、libkavexim.so ライブラリまでのパスを表します

32ビット Linux ディストリビューションの場合:

```
/opt/Kaspersky/kav4lms/lib/libkavexim.so
```

64ビット Linux ディストリビューションの場合:

```
/opt/Kaspersky/kav4lms/lib64/libkavexim.so
```

FreeBSD の場合:

```
/usr/local/lib/Kaspersky/kav4lms/libkavexim.so
```

5. kav4lms-filter サービスを停止します
6. 以下の行を /var/opt/kaspersky/applications.setup (Linux の場合) または /var/db/kaspersky/applications.setup (FreeBSD の場合) の **[1043]** セクションに追加します:

Linux の場合:

```
FILTER_SERVICE=false  
FILTER_PROGRAM=/opt/kaspersky/kav4lms/lib/libkavexim\  
.so
```

FreeBSD の場合:

```
FILTER_SERVICE=false  
FILTER_PROGRAM=/usr/local/lib/kaspersky/kav4lms/  
libkavexim.so
```

7. Exim を再起動します:

4.2. Postfix との統合

Anti-Virus を Postfix と 3 つの方法で統合することができます。

- **post-queue** による統合: 保護されるサーバを通過するすべてのメールトラフィックは、メールシステムのキューに追加される前に、スキャンのために転送されます
- **pre-queue** による統合: メッセージは、メールシステムのキューに追加される前に、スキャンのために転送されます

- Milter による統合: メッセージは、Milter インタフェースを利用して、スキャンのために転送されます。

4.2.1. post-queue による統合

Kaspersky Anti-Virus へのメール転送および MTA への返送を正常に動作させるために、以下の条件を満たす必要があります:

1. MTA からのメッセージをフックするようにフィルタを設定する必要があります。「フィルタ - MTA」接続の終端は、メインのアプリケーション設定ファイルの **[kav4lms:filter.settings]** セクションの **FilterSocket** オプションで定義されるソケットです
2. フィルタは、スキャンのためにメインサービスにメッセージを渡す必要があります。「フィルタ - メインサービス」接続の終端は、メインのアプリケーション設定ファイルの **[kav4lms:server.settings]** セクションの **ServiceSocket** オプションで定義されるソケットです

警告!

Postfix と統合する場合、**FilterSocket**、**ServiceSocket**、および **ForwardSocket** の各オプションがネットワークソケットまたはローカルソケットを参照するように設定できません。

3. フィルタはメッセージを MTA に返送する必要があります。「アプリケーション - MTA」接続の終端は、メインのアプリケーション設定ファイルの **[kav4lms:filter.settings]** セクションの **ForwardSocket** オプションで定義されるソケットです

アプリケーション設定スクリプトを使用して Kaspersky Anti-Virus を Postfix と統合するには:

以下のコマンドを実行します:

Linux の場合:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=postfix
```

FreeBSD の場合:

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=postfix
```

手動で Kaspersky Anti-Virus を Postfix と統合するには:

1. master.cf ファイルに以下の行を追加します:

```
#kav4lms-filter-begin
kav4lms_filter    unix      -      -      n\
-                10      smtp
-o smtp_send_xforward_command=yes
```

```
<forward_socket_ip_address>:<forward_socket_port>\
    inet      n      -      n      -      10\
    smtpd
    -o content_filter=
    -o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings
```

注記:

Postfix 2.3 以上でローカルソケットを使用する場合、no_milters オプションの上に、以下の行も追加します:

```
-o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings,no_milters

-o smtpd_helo_restrictions=
-o smtpd_client_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=\
permit_mynetworks,reject
-o mynetworks=127.0.0.0/8, [::1]/128
-o smtpd_authorized_xforward_hosts=\
127.0.0.0/8, [::1]/128
#kav4lms-filter-end
```

<forward_socket_ip_address>:<forward_socket_port> には、アプリケーションによるチェック後にメールを転送するソケットの IP アドレスとポートを設定します

2. main.cf ファイルに以下の行を追加します:

```
#kav4lms-filter-begin
content_filter = \
kav4lms_filter:<filter_socket_ip_address>:\
<filter_socket_port>
#kav4lms-filter-end
```

<filter_socket_ip_address>:<filter_socket_port> には、フィルタプログラムが待機するソケットの IP アドレスとポートを設定します

3. kav4lms-filter サービスを停止します
4. 以下の行を /var/opt/kaspersky/applications.setup (Linux の場合) または /var/db/kaspersky/applications.setup (FreeBSD の場合) の **[1043]** セクションに追加します:

```
FILTER_SERVICE=true
FILTER_PROGRAM=kav4lms-filter
```

5. kav4lms-filter サービスを開始します
6. Postfix を再起動します:

4.2.2. pre-queue による統合

Kaspersky Anti-Virus へのメール転送および MTA への返送を正常に動作させるために、以下の条件を満たす必要があります:

1. MTA からのメッセージをフックするようにフィルタを設定する必要があります。「フィルタ - MTA」接続の終端は、メインのアプリケーション設定ファイルの [kav4lms:filter.settings] セクションの FilterSocket オプションで定義されるソケットです
2. フィルタは、スキャンのためにメインサービスにメッセージを渡す必要があります。「フィルタ - メインサービス」接続の終端は、メインのアプリケーション設定ファイルの [kav4lms:server.settings] セクションの ServiceSocket オプションで定義されるソケットです

警告!

Postfix と統合する場合、**FilterSocket**、**ServiceSocket**、および **ForwardSocket** の各オプションがネットワークソケットまたはローカルソケットを参照するように設定できません。

3. フィルタはメッセージを MTA に返送する必要があります。「アプリケーション - MTA」接続の終端は、メインのアプリケーション設定ファイルの [kav4lms:filter.settings] セクションの ForwardSocket オプションで定義されるソケットです

注記:

本マニュアルから Postfix の設定へ文字列をコピーする場合は、" \ " 記号を取り除き改行しないで続けるようにしてください。

アプリケーション設定スクリプトを使用して Kaspersky Anti-Virus を Postfix と統合するには:

以下のコマンドを実行します:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \  
--install-filter=postfix-prequeue
```

in FreeBSD:

```
# /usr/local/bin/kav4lms-setup.sh \  
--install-filter=postfix-prequeue
```

手動で Kaspersky Anti-Virus を Postfix と統合するには:

1. master.cf ファイルに以下の行を追加します:

```
#kav4lms-prequeue-begin
kav4lms_filter      unix      -      -      n\
-      10      smtp
-o smtp_send_xforward_command=yes
<forward_socket_ip_address>:<forward_socket_port>\
inet      n      -      n      -      10\
smtpd
-o content_filter=
-o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings
```

注記:

Postfix 2.3 以上でローカルソケットを使用する場合、no_milters オプションの上に、以下の行も追加します:

```
-o receive_override_options=\
no_unknown_recipient_checks,no_header_body_checks,\
no_address_mappings,no_milters

-o smtpd_helo_restrictions=
-o smtpd_client_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=\
permit_mynetworks,reject
-o mynetworks=127.0.0.0/8, [::1]/128
-o smtpd_authorized_xforward_hosts=\
127.0.0.0/8, [::1]/128
#kav4lms-prequeue-end

<forward_socket_ip_address>:<forward_socket_port> には、アプリケーションによるチェック後にメールを転送するソケットの IP アドレスとポートを設定します
```

2. main.cf ファイルに以下の行を追加します:

```
smtp inet n - n - 20 smtpd
add the parameter
#kav4lms-prequeue-begin
-o smtpd_proxy_filter=:<filter_socket_port>
#kav4lms-prequeue-end
```

3. kav4lms-filter サービスを停止します
4. 以下の行を /var/opt/kaspersky/applications.setup (Linux の場合) または /var/db/kaspersky/applications.setup (FreeBSD の場合) の **[1043]** セクションに追加します:

```
FILTER_SERVICE=true
FILTER_PROGRAM=kav4lms-filter
```

5. kav4lms-filter サービスを開始します
6. Postfix を再起動します:

4.2.3. Milter による統合

Kaspersky Anti-Virus へのメール転送および MTA への返送を正常に動作させるために、以下の条件を満たす必要があります:

1. MTA からのメッセージをフックするようにフィルタを設定する必要があります。「フィルタ - MTA」接続の終端は、メインのアプリケーション設定ファイルの [kav4lms:filter.settings] セクションの FilterSocket オプションで定義されるソケットです
2. フィルタは、スキャンのためにメインサービスにメッセージを渡す必要があります。「フィルタ - メインサービス」接続の終端は、メインのアプリケーション設定ファイルの [kav4lms:server.settings] セクションの ServiceSocket オプションで定義されるソケットです

警告!

Postfix と統合する場合、**FilterSocket**、**ServiceSocket** の各オプションがネットワークソケットまたはローカルソケットを参照するように設定できます。

注記:

本マニュアルから Postfix の設定へ文字列をコピーする場合は、" \ " 記号を取り除き改行しないで続けるようにしてください。

アプリケーション設定スクリプトを使用して Kaspersky Anti-Virus を Postfix と統合するには:

以下のコマンドを実行します:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=postfix-milter
```

in FreeBSD:

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=postfix-milter
```

手動で Kaspersky Anti-Virus を Postfix と統合するには:

1. main.cf ファイルに以下の行を追加します:

```
smtpd_milters = inet:127.0.0.1:10025,
#kav4lms-milter-begin
milter_connect_macros = j _ {daemon_name} {if_name} \
{if_addr}
```

```
milter_helo_macros = {tls_version} {cipher} \  
{cipher_bits} {cert_subject} {cert_issuer}  
milter_mail_macros = i {auth_type} {auth_authen} \  
{auth_ssf} {auth_author} {mail_mailer} {mail_host} \  
{mail_addr}  
milter_rcpt_macros = {rcpt_mailer} {rcpt_host} \  
{rcpt_addr}  
milter_default_action = tempfail  
milter_protocol = 3  
milter_connect_timeout=180  
milter_command_timeout=180  
milter_content_timeout=600  
#kav4lms-milter-end
```

2. kav4lms-milter サービスを停止します
3. 以下の行を /var/opt/kaspersky/applications.setup (Linux の場合) または /var/db/kaspersky/applications.setup (FreeBSD の場合) の **[1043]** セクションに追加します:

```
FILTER_SERVICE=true  
FILTER_PROGRAM=kav4lms-milter
```

4. kav4lms-milter サービスを開始します
5. Postfix を再起動します:

4.3. qmail との統合

qmail MTA では、フィルタリングの拡張がサポートされていません。フィルタリングは、アプリケーションに付属の `/opt/kaspersky/kav4lms/lib/bin/kav4lms-qmail` (FreeBSD の場合は `/usr/local/libexec/kaspersky/kav4lms/kav4lms-qmail`) バイナリによって実装され、qmail の `qmail-queue` バイナリの代わりにこのバイナリが使用されます。このバイナリはフィルタリングを実行し、メールトラフィックを qmail の `qmail-queue` に送信します。メッセージは、MTA キューに追加される前に、分析のために転送されます (`pre-queue` によるフィルタリング)。

警告！

qmail と統合する場合、**ServiceSocket** オプションがネットワークソケットまたはローカルソケットを参照するように設定できます。

アプリケーション設定スクリプトを使用して Kaspersky Anti-Virus を qmail と統合するには:

以下のコマンドを実行します:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=qmail
```

FreeBSD の場合:

```
# /usr/local/bin/kav4lms-setup.sh \
--install-filter=qmail
```

手動で Kaspersky Anti-Virus を qmail と統合するには:

1. `/var/qmail/bin` ディレクトリにある `qmail-queue` ファイルの名前を `qmail-queue-real` に変更します
2. `/opt/kaspersky/kav4lms/lib/bin/kav4lms-qmail` (FreeBSD の場合は `/usr/local/libexec/kaspersky/kav4lms/kav4lms-qmail`) ファイルを `/var/qmail/bin` ディレクトリにコピーして、名前を `qmail-queue` に変更します
3. `qmail-queue` ファイルと `qmail-queue-real` ファイルのアクセス権を以下のように設定します:

```
-rws-x--x 1 qmailq qmail
```

4. `kav4lms-filter` サービスを停止します
5. 以下のディレクトリとその内容の所有者とグループを `qmailq:qmail` に変更します:
 - Linux の場合:

```
# /opt/Kaspersky/kav4lms/bin/kav4lms-setup.sh \
--switch-credentials=qmailq,qmail
```

- FreeBSD の場合:

```
# /usr/local/bin/kav4lms-setup.sh \  
--switch-credentials=qmailq,qmail
```

6. 以下の行を /var/opt/kaspersky/applications.setup (Linux の場合) または /var/db/kaspersky/applications.setup (FreeBSD の場合) の **[1043]** セクションに追加します:

Linux の場合:

```
FILTER_SERVICE=false  
FILTER_SERVICE=/opt/kaspersky/kav4lms/lib/bin\  
/kav4lms-qmail
```

FreeBSD の場合:

```
FILTER_SERVICE=false  
FILTER_SERVICE=/usr/local/libexec/kav4lms\  
/kav4lms-qmail
```

7. qmail を再起動します:

4.4. Sendmail との統合

Sendmail には、カスタムフィルタとの統合を実装するための Milter API が用意されています。メールトラフィックは Sendmail から Kaspersky Anti-Virus に渡され、Milter インターフェイス呼び出しを使用して返送されます。メッセージは、MTA キューに追加される前に、分析のために転送されます (pre-queue による統合)。

一般に、Sendmail と統合する場合、手動で変更するのは mc 形式の MTA 設定ファイルだけであり、cf ファイルは自動的に変更されます。cf ファイルの自動変更がサポートされていない場合は、mc ファイルを変更した後で、対応する cf ファイルも変更する必要があります。

注記:

cf ファイルだけを変更した場合、その内容は次に mc ファイルから cf ファイルが生成されたときに失われます。

警告!

Sendmail と統合する場合、**FilterSocket** および **ServiceSocket** の各オプションがネットワークソケットまたはローカルソケットを参照するように設定できます。

4.4.1. .cf ファイルによる Sendmail との統合

アプリケーション設定スクリプトを使用して Kaspersky Anti-Virus を Sendmail と統合するには:

以下のコマンドを実行します:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \
--install-filter=sendmail-milter
```

FreeBSD の場合:

```
# /usr/local/bin/bin/kav4lms-setup.sh \
--install-filter=sendmail-milter
```

手動で Kaspersky Anti-Virus を Sendmail と統合するには:

1. sendmail.cf ファイルのバックアップを作成します
2. sendmail.cf ファイルに以下の文字列を追加します:

```
#kav4lms-milter-begin-filter
O InputMailFilters=kav4lms_filter
O Milter.macros.connect=j, _, {daemon_name}, \
{if_name}, {if_addr}
O Milter.macros.helo={tls_version}, {cipher}, \
{cipher_bits}, {cert_subject}, {cert_issuer}
O Milter.macros.envfrom=i, {auth_type}, \
{auth_authen}, {auth_ssf}, {auth_author}, \
{mail_mailer}, {mail_host}, {mail_addr}
O Milter.macros.envrcpt={rcpt_mailer}, {rcpt_host}, \
{rcpt_addr}
#kav4lms-milter-end-filter
```

3. sendmail.cf ファイルに以下の行を追加します:

- a) ネットワークソケットを使用した統合の場合:

```
#kav4lms-milter-begin-socket
Xkav4lms_filter,
S=inet:<filter_port>@<filter_address>,F=T, \
T=S:3m;R:5m;E:10m
#kav4lms-milter-end-socket
```

<filter_port> はフィルタサービスが待機するネットワークソケットのポート番号です。<filter_address> はフィルタサービスが動作するサーバの名前または IP アドレスです

- b) ローカルソケットで接続する場合は、以下のようにソケット定義セクションを変更します:

```
#kav4lms-milter-begin-socket
```

```
Xkav4lms_filter,
S=unix:<filter_socket_file_path>,F=T,T=S:3m;\
R:5m;E:10m
#kav4lms-milter-end-socket
```

<socket_file_path> はローカルソケットへのパスです

4. kav4lms-milter サービスを停止します
5. 以下の行を /var/opt/kaspersky/applications.setup (Linux の場合) または /var/db/kaspersky/applications.setup (FreeBSD の場合) の **[1043]** セクションに追加します:

```
FILTER_SERVICE
FILTER_PROGRAM=kav4lms-milter
```

6. kav4lms-milter サービスを開始します
7. Sendmail を再起動します:

4.4.2. .mc ファイルによる Sendmail との統合

.mc ファイルを使用してアプリケーションを Sendmail と統合するには:

1. .mc ファイルのバックアップを作成します
2. .mc ファイルに以下の文字列を追加します:

```
dnl kav4lms-milter-begin dnl
define(`_FFR_MILTER', `true')dnl
INPUT_MAIL_FILTER(`kav4lms_filter',\
`S=inet:10025@127.0.0.1,F=T,T=S:3m;R:5m;E:10m')dnl
dnl kav4lms-milter-end dnl
```

3. オペレーティングシステムのルールに従って、.cf 設定ファイルをコンパイルします
4. kav4lms-filter サービスを停止します
5. 以下の行を /var/opt/kaspersky/applications.setup (Linux の場合) または /var/db/kaspersky/applications.setup (FreeBSD の場合) の **[1043]** セクションに追加します:

```
FILTER_SERVICE=true
FILTER_SERVICE=kav4lms-milter
```

6. kav4lms-filter サービスを開始します
7. Sendmail を再起動します:

第5章. メールアンチウイルス

5.1. グループの設定

グループは、Kaspersky Anti-Virus の同一設定でメッセージを処理する複数の送信者と受信者のアドレスで構成されます。

カスタムメールスキャン設定は、グループごとに定義できます。カスタム設定の例は以下のとおりです：

- メールスキャン方法 (44 ページの 5.2 を参照)
- メールスキャンモード (44 ページの 5.3 を参照)
- メッセージおよびそのオブジェクトに対する処理 (47 ページの 5.4 を参照)
- 処理対象メールの事前バックアップ (52 ページの 5.6 を参照)
- 検知したオブジェクトに関する通知 (53 ページの 5.7 を参照)

各グループの設定は、別々の設定ファイルに保管されます (121 ページの A.2 を参照)。グループ設定ファイルはすべて、メインのアプリケーション設定ファイル `kav4lms.conf` の **[kav4lms:groups]** セクションで、`_include` 設定項目を使用して指定する必要があります。グループ設定を指定する場合、設定ファイル名を使用するか、または全グループ設定ファイルが含まれるディレクトリの名前を使用します。

デフォルトでは、グループ設定ファイルは `/etc/opt/kaspersky/kav4lms/groups.d/` ディレクトリに配置する必要があります。

配布パッケージには、**Default** グループ設定ファイル `default.conf` が含まれています。この設定ファイルは、製品をインストールした後に `/etc/opt/kaspersky/kav4lms/groups.d/` に配置されます。各グループ設定ファイルで指定されていない値は、**Default** グループ設定ファイルで定義されている値がデフォルトとして使用されます。**Default** グループ設定ファイルのパラメータは、グループが存在しない場合に使用されます。

アンチウイルスがメッセージをスキャンする場合、メッセージの送信者と受信者が見つかったグループの設定を使用します (MAIL FROM コマンドおよび RCPT TO コマンドを使用)。送信者とすべての受信者が属するグループが複数存在する場合は、優先度の高いグループが選択されます。属するグループが見つからないメッセージは、**Default** グループ設定ファイル (優先度は最も低い **0**) の設定を使用して処理されます。したがって、優先度の高いグループほど高い保護レベルを指定することをお勧めします。

優先度は、一意なグループ ID です。その値は、グループ設定ファイルの **[kav4lms:groups.<group_name>.definition]** セクションにある **Priority** オプションで定義します。

送信者と受信者は、グループ設定ファイルの `[kav4lms:groups.<group_name>.definition]` セクションにある **Senders** オプションと **Recipients** オプションで定義します。

新規グループを作成するには:

1. メイン設定ファイルの `[kav4lms:groups]` セクションで指定されているディレクトリにグループ設定ファイルを作成します。デフォルトディレクトリは、`/etc/opt/kaspersky/kav4lms/groups.d/` です

注記:

グループ設定ファイルを作成するときは、`default.conf` ファイルをテンプレートとして使用してください。以下のコマンドを実行すると、グループ名を一括置換できます:

```
# cd /etc/opt/kaspersky/kav4lms/groups.d
# sed 's|groups.default|groups.<group_name>|' default.conf
> <group_name>.conf
```

2. グループ設定ファイルの `[kav4lms:groups.<group_name>.definition]` セクションにある **Priority** オプションで、グループの優先度を定義します。値には任意の自然数を指定できます。複数のグループに同じ優先度を設定することはできません。また、優先度として **0** は設定できません
3. グループ設定ファイルの `[kav4lms:groups.<group_name>.definition]` セクションにある **Senders** オプションと **Recipients** オプションで、送信者と受信者のアドレスを定義します

マスクでワイルドカード (「*」と「?」) を使用できます。また、接頭辞「re:」で始まる正規表現も使用できます。複数のアドレス (アドレスマスク) を指定する場合、1 行に 1 つずつ記述する必要があります:

```
Senders=reporter@*.mydomain.com
Recipients=re:office\d+@central\.mydomain\.com
```

Recipients オプションと **Senders** オプションは、少なくともどちらか 1 つを指定する必要があります。グループ定義で **Recipients** オプションまたは **Senders** オプションが指定されていない場合、`default.conf` でそのパラメータに指定されているデフォルト値「*@*」(すべてのアドレス) が使用されます

警告!

正規表現では、大文字と小文字が区別されます。

4. 必要であれば、メールスキャンのオプションをグループ設定ファイルの対応するセクションで指定します (121 ページの A.2 を参照)。グループ設定ファイルで定義されていないオプションについては、**Default** グループ設定ファイル `default.conf` でそのパラメータに指定されている値が使用されます

5.2. メール分析ポリシーの定義

アンチウイルスによるメール分析には、以下の 2 つの方法があります：

- メッセージ全体を 1 つのオブジェクトとみなしてスキャンする方法 - メッセージのヘッダーと本文がまとめて分析されます
- 2 段階の手法 - メッセージを最初に 1 つのオブジェクトとしてスキャンし、その後メッセージを複数のオブジェクトに分解して (メッセージ本文、添付ファイルなど) 個々にチェックします。この手法により、保護レベルと信頼性が高まります

注記：

メッセージパーツに適用可能な処理がメッセージ全体に対する処理として選択されている場合は (47 ページの 5.4 を参照)、どちらの方法が選択されたかに関係なく、パーツごとのスキャンが行われます。

メールスキャン方法はポリシーによって決定され、グループ設定ファイルの **[kav4lms:groups.<group_name>.settings]** セクションにある **ScanPolicy** オプションで定義されます。

メッセージを 1 つのオブジェクトとしてスキャンするには

ScanPolicy オプションに **message** を設定

2 段階処理でメッセージをスキャンするには

ScanPolicy オプションに **combined** を設定

5.3. メールスキャンモード

グループ設定の次のステップは、メールスキャンモードの選択です。Kaspersky Anti-Virus には、以下のスキャンモードがあります：

- マルウェアがあるかどうかのスキャン
- コンテンツフィルタリング

グループのスキャンモードは、グループ設定ファイルの

[kav4lms:groups.<group_name>.settings] セクションの **Check** オプションで指定します。以下の値を指定できます：

- **anti-virus** - ウイルスメールスキャンを実行
- **content-filter** - 添付ファイルの名前、タイプ、およびサイズによるフィルタリング
- **all** - ウイルスチェックおよびコンテンツフィルタリングの両方を実行

- **none** - メールスキャンを行わない

ウイルススキャンおよびフィルタリングを両方とも有効にした場合、以下の順序で分析が行われ
ます:

1. メッセージを 1 つのオブジェクトとみなしたウイルススキャン
3. 添付ファイルのフィルタリング
2. メッセージパーツごとのスキャン (**ScanPolicy=combined** の設定で 2 段階スキャンが選択されている場合)

5.3.1. ウイルススキャン

ウイルススキャンを有効にするには、グループ設定ファイルの **[kav4lms:groups.<group_name>.settings]** セクションの **Check** オプションに **anti-virus** または **all** を設定します。

メッセージのウイルススキャンが終わると、メッセージまたはそのオブジェクトに以下のいずれかのステータスが割り当てられます:

- **clean** - メッセージにマルウェアが含まれていない
- **infected** - メッセージ (またはそのパーツ) に有害なオブジェクトが含まれている
- **suspicious** - メッセージ (またはそのパーツ) に疑わしいオブジェクトが含まれている (ヒューリスティックアナライザが有効な場合にのみ割り当てられる)
- **protected** - メッセージ (またはそのパーツ) がパスワード保護または暗号化されている
- **error** - メッセージが破損しているか、またはスキャン処理でエラーが発生した

スキャンで割り当てられたステータスは、その後のメッセージとそのオブジェクトの処理で使用されます (47 ページの 5.4 を参照)。

感染メッセージ (**infected**) には、検知された脅威の名前に応じて固有の処理を定義できます (グループ設定ファイルの **[kav4lms:groups.<group_name>.actions]** セクションにある **VirusNameAction** オプション)。Kaspersky Anti-Virus は検知した脅威の名前をカスペルスキーの表記法 (<http://www.viruslistip.com/> を参照) で返します。処理するウイルス名のリストは、**[kav4lms:groups.<group_name>.contentfiltering]** セクションの **VirusNameList** パラメータで指定します。このパラメータにはウイルス名をそのまま指定するか、正規表現 (POSIX 標準) を指定します。

スキャン機能をカスタマイズして、スキャンの詳細度または速度を上げることができます。スキャンエンジンのパフォーマンスに関する設定は、グループ設定ファイルの **[kav4lms:groups.<group_name>.settings]** セクションで指定します。以下のオプションがあります:

- アーカイブをスキャンするかどうか (**ScanArchives** パラメータ)

- 圧縮された実行ファイルをスキャンするかどうか (**ScanPacked** パラメータ)
- ヒューリスティック分析を実行するかどうか (**UseCodeAnalyzer** パラメータ)

注記:

このパラメータに **yes** を設定するとステータス **suspicious** が有効になり、それ以外の値を設定すると無効になります。

- メッセージまたはメッセージのオブジェクトのスキャンの最大実行時間 (**MaxScanTime** パラメータ)。実際のスキャン時間が指定された最大時間を超えると、スキャンは **error** ステータスで終了します
- RFC 標準に準拠していない MIME オブジェクトをヒューリスティックアルゴリズムでデコードするかどうか (**MIMEEncodingHeuristics** オプション)
- 検知するマルウェアのタイプ (kav4lms.conf ファイルの **[kav4lms:server.settings]** セクションにある **UseAVBasesSet** パラメータ)

5.3.2. コンテンツフィルタリング

コンテンツフィルタリングサービスを有効にするには、グループ設定ファイルの **[kav4lms:groups.<group_name>.settings]** セクションにある **Check** パラメータに **content-filter** または **all** を設定します。

コンテンツフィルタリングでは、以下の基準を使用できます：

- 添付ファイルの MIME タイプ (Content-Type ヘッダーに適用)

警告!

宣言されている MIME タイプと実際のコンテンツが一致しない場合があります。この場合、コンテンツの識別は行われません。

- 添付ファイル名 (添付ファイルの名前と拡張子に適用)
- 添付ファイルサイズ (メッセージパーツのサイズに適用。パーツのサイズは添付ファイルの解凍後に計算)

注記:

ウイルススキャンとコンテンツフィルタリングの両方が有効な場合、コンテンツフィルタリング、ウイルススキャンの順に実行されます。

フィルタリング基準は、グループ設定ファイルの **[kav4lms:groups.<group_name>.contentfiltering]** セクションで定義します。

フィルタリング基準には、以下のルールを設定できます：

- 包含ルール。このルールは、以下のパラメータでフィルタリング対象オブジェクトを指定します：
 - **IncludeMime** - MIME タイプのリストを指定
 - **IncludeName** - 添付ファイル名のリストを指定
 - **IncludeSize** - オブジェクトのサイズのリストを指定
- 除外ルール。このルールは、以下のパラメータでフィルタリング対象外オブジェクトを指定します：
 - **ExcludeMime** - MIME タイプのリストを指定
 - **ExcludeName** - 添付ファイル名のリストを指定
 - **ExcludeSize** - オブジェクトのサイズのリストを指定

警告！

包含ルールに何も指定されず、除外ルールが指定されている場合は、除外ルールと一致しないすべてのオブジェクトがフィルタリング対象になります。

どちらのルールも指定されていない場合は、**Check** パラメータの値と関係なく、コンテンツフィルタリングは実行されません。

フィルタリング基準のうち MIME タイプと添付ファイル名に対するルールは、以下の項目のリストとして指定する必要があります：

- 文字列
- ワイルドカード (UNIX 標準)
- 正規 (POSIX 標準) 表現

警告！

正規表現は接頭辞「re:」で始まる文字列で、大文字と小文字が区別されます。

オブジェクトサイズのルールは、以下の項目で指定する必要があります：

- バイト数
- 数字と単位 (「KB」または「MB」)
- 比較演算子

5.4. オブジェクトに適用する処理

Kaspersky Anti-Virus は、スキャンとコンテンツフィルタリングの実行後に、メッセージとそのパーツに対して特定の処理を実行します。その中には、メッセージ全体に対して適用される処理と、

メッセージパーツだけに適用される処理があります。実行する処理を指定するパラメータには、以下の値を指定できます：

- **warn** - メッセージ全体が、危険なオブジェクトの存在を警告するテキストで置き換えられます
- **drop** - メッセージは受け付けられませんが、受信者に送信されずに破棄され、通知もされません
- **reject** - メッセージの送信は拒否されます（この処理は Postfix との post-queue による統合または Exim との統合を使用している場合は実行されない。その場合はバウンス処理が実行される）。この処理が選択されている場合、送信者は **RejectReply** オプションで定義されている通知を受信します
- **skip** - メッセージまたはそのパーツはそのままパスされ、スキャン結果がアプリケーションログに記録されます
- **cure** (メッセージパーツのウイルススキャンの実行後のみ指定可能) - 感染オブジェクトの駆除が行われます。駆除できなかった場合は、**delete** 処理が実行されます
- **rename** (メッセージパーツのコンテンツフィルタリングの実行後にかぎり指定可能) - **RenameTo** パラメータの値で添付ファイルの名前を変更します。この値が拡張子 (.vir など) として定義されている場合は、添付ファイルの名前に付加されます。拡張子ではない場合はファイル名全体が指定されたものとみなし、添付ファイルの名前全体が置き換えられます
- **delete** - メッセージパーツが削除され、**UsePlaceholderNotice** パラメータが **yes** に設定されていれば通知テキストで置き換えられます。通知テキストは、part_<action> という名前のテンプレートファイルから読み込まれます

ウイルススキャン実行後の処理は、**InfectedAction**、**SuspiciousAction**、**ProtectedAction**、**ErrorAction**、および **VirusNameAction** の各パラメータで指定されます。フィルタリング実行後の処理は、**FilteredMimeAction**、**FilteredNameAction**、および **FilteredSizeAction** の各パラメータで指定されます。

処理関連のパラメータは、グループ設定ファイルの

[kav4lms:groups.<group_name>.actions] セクションにあります。

警告！

スキャンの前にコンテンツフィルタリングが行われるので、メッセージ全体をスキャンしてステータスが **infected** と判定されたのに、メッセージパーツのスキャンでは感染部分が見つからないという場合があります。こうした状況は、コンテンツフィルタリングの実行後処理として **delete** が選択され、フィルタリング後にそのメッセージパーツが削除された場合に発生する可能性があります。

5.5. 定義済みセキュリティプロファイル

Kaspersky Anti-Virus の配布パッケージには、以下のメール保護レベルを実現するための定義済みプロファイルが含まれています：

- **recommended** - default_recommended ディレクトリに保管（詳細は 49 ページの 5.5.1 を参照）
- **maximum protection** - high_overall_security ディレクトリに保管（詳細は 50 ページの 5.5.2 を参照）
- **maximum performance** - high_scan_speed ディレクトリに保管（詳細は 51 ページの 5.5.3 を参照）

プロファイルは 2 つの設定ファイル、つまり kav4lms.conf と default.conf (groups.d サブディレクトリにある) で構成されます。/etc/opt/kaspersky/kav4lms/profiles ディレクトリ内にプロファイル名と一致するサブディレクトリがあり、そこに保管されます。

定義済みプロファイルはそのまま使用できますが、アプリケーションの設定ファイルにメール保護設定を手動で設定することもできます。

定義済みプロファイルを使用するには：

1. アプリケーションの設定ファイル (kav4lms.conf および groups.d/default.conf) のバックアップを作成します
2. 使用するプロファイルのディレクトリの内容を /etc/opt/kaspersky/kav4lms ディレクトリにコピーします
3. 以下のコマンドを実行して、新しい設定を適用します：

```
/etc/init.d/kav4lms reload
```

5.5.1. recommended プロファイル

ウイルスの保護レベルとスキャン速度のバランスが最適化されているプロファイルです。以下の特徴があります：

- メールメッセージは、**message** スキャンポリシーに従ってスキャンされます。メッセージは 1 つのオブジェクトとしてスキャンされます
- 拡張定義データベースに基づいてスキャンが行われます
- MIME オブジェクトでのメッセージのネストレベルの最大値は 10 です
- アンチウイルス処理が適用されるすべてのメッセージについてバックアップと情報ファイルが作成されます
- 感染メッセージは駆除されます

- MIME タイプによる添付ファイルのフィルタリングが有効になっています。外部オブジェクト (message/external-body タイプ) および拡張子が .pif、.com、.bat、.exe である添付ファイルへのリンクがメッセージから削除されます
- 疑わしいメッセージ、パスワード保護されたメッセージ、エラーを含むメッセージ、MIME タイプと添付ファイル名でフィルタリングされたメッセージについて警告が生成されます。具体的な脅威が検知されたメッセージは破棄されます
- メッセージのヘッダーと本文に、処理結果に関する情報が追加されます
- メッセージスキャンに関する通知がメッセージの受信者に送信されます。送信者または管理者には送信されません
- デバッグ情報を除くすべてのアプリケーションメッセージがレポートに記録されます
- アプリケーション動作について、あらゆる面の統計値が収集されます

5.5.2. maximum protection プロファイル

メールトラフィックが最大限に包括的に保護されるプロファイルです。以下の特徴があります：

- メールメッセージは、**combined** スキャンポリシーに従ってスキャンされます。最初はメッセージが 1 つのオブジェクトとしてウイルススキャンされ、次に、感染オブジェクトが見つかったかどうかに関係なく、メッセージパーツが個別にスキャンされます
- RFC 標準に準拠していないメッセージはヒューリスティックアルゴリズムによって解析され、デコードが正常終了した後にスキャンが行われます
- 拡張定義データベースに基づいてスキャンが行われます
- MIME タイプによるメールメッセージのフィルタリングが有効になっています。外部オブジェクト (message/external-body) を参照するメールがフィルタリングされ、削除されます。また、.pif、.com、.bat、および .exe の拡張子を持つ添付ファイルが削除されます
- メッセージのネストレベルに制限はありません
- アンチウイルス処理とフィルタリングが適用されるすべてのメッセージについて情報ファイルが作成されます
- 感染オブジェクトは駆除されます
- メッセージの疑わしいオブジェクト、保護されたオブジェクト、およびフィルタリングされたオブジェクトはすべて削除されます。指定されたリストに記載されている脅威が含まれるメッセージは破棄されます
- メッセージに含まれるオブジェクトでスキャンの際にエラーが発生した場合、メッセージの内容は通知で置き換えられます
- メッセージスキャンに関する通知がメッセージの受信者に送信されます。送信者または管理者には送信されません

- デバッグ情報を除くすべてのアプリケーションメッセージがレポートに記録されず
- 統計値は保存されません

5.5.3. maximum performance プロファイル

アンチウイルスの信頼性を多少犠牲にしても、アプリケーションのパフォーマンスを最大化するプロファイルです。以下の特徴があります：

- メールメッセージは、**message** スキャンポリシーに従ってスキャンされます。メッセージは 1 つのオブジェクトとしてスキャンされます
- メッセージオブジェクトのフィルタリングが無効になっています
- 破棄の処理および警告の処理が適用されるすべてのメッセージについて、バックアップが作成されます。情報ファイルは作成されません
- メールメッセージの感染オブジェクト、保護されたオブジェクト、エラーを含むオブジェクトについて警告が生成されます。指定されたリストに記載された脅威が検知されたメッセージは破棄されます
- メッセージのヘッダーに、処理結果に関する情報が追加されます
- メッセージスキャンに関する通知がメッセージの受信者に送信されます。送信者または管理者には送信されません
- アプリケーションの動作に関するあらゆる情報、たとえば詳細レベル、致命的エラーやその他のエラー、および重要な情報に関するメッセージが、アクティビティレポートに記録されます
- 検知したウイルスに関する統計値が収集されます
- メインサービスに対するクライアントからの要求の最大数は、recommended プロファイルや maximum protection プロファイルの 2 倍です。同時に行うことのできるスキャン要求の数に制限はありません

5.6. バックアップ

メッセージを処理する前にそのバックアップを作成する機能がサポートされています。バックアップ設定は、グループ設定ファイルの `[kav4lms:groups.<group_name>.backup]` セクションで指定します。

メールバックアップモードは Policy オプションによって決定されます。このオプションには以下の値を指定できます：

- **message** - メッセージのコピーだけが作成されます
- **info** - メッセージのコピーのほかに情報ファイルが作成されます。情報ファイルには、以下の情報が含まれています：
 - MTA クライアントの IP アドレス (使用可能ならホスト)
 - MTA コネクタの IP アドレス (使用可能ならホスト)
 - MTA コネクタから渡されるメッセージの送信者
 - 処理サーバのアドレス
 - 分析の際にメッセージが分類されたグループの名前
 - MTA コネクタから渡されるメッセージの受信者リスト
 - バックアップ処理の原因 (cured、deleted、rejected、filtered など)
 - 元のファイルへのパス (バックアップ先からの相対パス)
 - アプリケーションインスタンスの情報 (プロセス ID およびスレッド ID)
- **none** - メッセージはバックアップされません

Options パラメータは、バックアップの理由になった処理を指定します：

- **cured** - 元のメッセージオブジェクトが駆除された
- **deleted** - 元のメッセージオブジェクトが削除された
- **rejected** - 元のメッセージが拒否されたが (MTA クライアントがエラーコードを受信)、管理者が感染メッセージをバックアップするように指定した
- **dropped** - 元のメッセージオブジェクトが破棄された
- **warning** - 元のメッセージは警告で置き換えられた
- **renamed** - メッセージの少なくとも 1 つのオブジェクト (MIME 要素) がフィルタリングルールに一致して名前が変更された
- **all** - 上記のすべてが該当した

Options パラメータには、上記のいずれか 1 つ、またはカンマ区切りリストを指定できます。

メッセージのバックアップおよび情報ファイルは、**Destination** パラメータで指定されているディレクトリに保管されます。

5.7. 通知

通知は、処理されたメッセージの説明が含まれるメールメッセージで、処理されたメッセージの受信者、送信者、またはサーバ管理者に送信されます。

メッセージの説明のほかに、何らかの理由でメッセージから削除されたオブジェクトの説明も含まれます。

通知に元のメールを追加することもできます。ただし、それが可能なのは、受信者に送信する通知だけです。管理者と送信者には、通知テキストだけが含まれるメールメッセージが送信されます。

5.7.1. 通知の設定

通知関連のパラメータは以下のセクションにあります：

- アプリケーションの設定ファイル `kav4lms.conf` の **[kav4lms:server.notifications]** セクション
- グループ設定ファイルの **[kav4lms:groups.<group_name>.notifications]** セクション

通知を設定するには、以下のステップを実行します。

ステップ 1 通知の送信先

通知は以下の相手に送信できます：

- メッセージの送信者 (グループ設定ファイルの **NotifySender** パラメータ)
- メッセージの受信者 (グループ設定ファイルの **NotifyRecipients** パラメータ)
- セキュリティ管理者 (グループ設定ファイルの **NotifyAdmin** パラメータ)。セキュリティ管理者のメールアドレスリストは、グループ設定ファイルの **AdminAddresses** パラメータで指定されています
- 製品管理者 (`kav4lms.conf` ファイルの **ProductNotify** パラメータで指定)。製品管理者のアドレスリストは、ファイルの **ProductAdmins** パラメータで指定されています

メッセージ送信者への通知は、上記のパラメータを **none** 以外の値に設定すれば有効になります。**none** を設定すると、通知は無効になります。

ステップ 2 通知の内容

メッセージの送信者、受信者、およびセキュリティ管理者は、以下の内容の通知を受信します：

- **InfectedAction** (詳細は 47 ページの 5.4 を参照) が実行された (少なくとも 1 つのオブジェクトが感染していた)。この通知タイプは、該当するパラメータに **infected** を設定すると有効になります
- **ProtectedAction** (詳細は 47 ページの 5.4 を参照) が実行された (少なくとも 1 つのオブジェクトが保護されていた)。この通知タイプは、該当するパラメータに **protected** を設定すると有効になります
- **ErrorAction** (詳細は 47 ページの 5.4 を参照) が実行された (少なくとも 1 つのオブジェクトにエラーが含まれていた)。この通知タイプは、該当するパラメータに **error** を設定すると有効になります
- フィルタリングルールに一致した (詳細は 46 ページの 5.3.2 を参照)。この通知タイプは、該当するパラメータに **filtered** を設定すると有効になります
- 上記のすべて。この通知タイプは、該当するパラメータに **all** を設定すると有効になります

製品管理者は、以下の内容の通知を受信します：

- 定義データベースの新しい更新がダウンロードされた。この通知タイプは、**ProductNotify** パラメータに **update** を設定すると有効になります
- アプリケーションに重大なエラー (復旧可能または復旧不可) が発生したこの通知タイプは、**ProductNotify** パラメータに **fault** を設定すると有効になります
- ライセンスに関する通知。この通知タイプは、**ProductNotify** パラメータに **license** を設定すると有効になります
- 上記のすべて。この通知タイプは、**ProductNotify** パラメータに **all** を設定すると有効になります

ライセンスに関する通知は特殊なケースであり、リストから除外することはできません。このタイプの通知は必ず送信され、通知が無効の場合はログ項目だけが生成されます。

ライセンスに関する通知は、以下のタイミングで送信されます：

- キーの有効期限 - 有効期限の 14 日前に最初の通知が送信され、その後は有効期限まで毎日、通知が送信されます。有効期限の翌日には、キーの期限切れ通知が送信されます
- ライセンス制限違反 - キーで許可されているユーザ数またはトラフィック量を超えた場合に送信されます

5.7.2. 通知のテンプレート

通知の作成には、以下のテンプレートを使用できます。テンプレートはアプリケーション設定ファイルの **Templates** パラメータで定義されているディレクトリに保管されています：

- **削除されたオブジェクトに関する通知のテンプレート** - アンチウイルス処理またはフィルタリングによってメッセージのいずれかのパーツが削除された場合に元のメッセージに追加されるテキスト。削除理由を示すマクロを使用できます。以下のテンプレートを使用できます：
 - `part_infected` - 感染駆除が失敗した後に削除されたオブジェクトと置き換えられるテキスト
 - `part_filtered` - MIME オブジェクトのフィルタリングの結果に基づいて削除された MIME オブジェクトと置き換えられるテキスト
 - `part_suspicious` - 疑わしいと判断されて削除されたオブジェクトと置き換えられるテキスト
 - `part_filtered` - フィルタリングの結果に従って名前が変更された元のメールオブジェクトと置き換えられるテキスト
 - `part_protected` - 保護されていてウイルススキャンを実行できなかったために削除されたオブジェクトと置き換えられるテキスト
 - `part_error` - スキャンエラーが発生したために削除されたオブジェクトと置き換えられるテキスト
- **標準通知テンプレート** - フィルタを使用するか、または SMTP コンポーネントによって送信されて新たに生成されたメッセージを使用して、送信者、受信者、管理者に送信される通知のテキスト。削除理由を示すマクロを使用できます。以下のテンプレートを使用できます：
 - `notify_common` - メッセージに適用された処理について受信者、送信者、管理者にデフォルトで送信されるテキスト
 - `notify_infected` - 感染メッセージと置き換えられるテキスト
 - `notify_suspicious` - 疑わしいオブジェクトが含まれるメッセージと置き換えられるテキスト
 - `notify_filtered` - フィルタリングされたメールメッセージと置き換えられるテキスト
 - `notify_error` - スキャンエラーが発生したメッセージと置き換えられるテキスト
 - `notify_protected` - 保護されていてスキャンできなかったメッセージと置き換えられるテキスト
 - `disclaimer` - 処理されたメッセージおよび生成されたメッセージに必ず追加されるテキスト。デフォルトでは、このテンプレートには「This message has been scanned by Kaspersky Anti-Virus. For more information about data security

please visit <http://www.kaspersky.com> and
<http://www.viruslist.com> というテキストが含まれています

- **詳細通知テンプレート** - メールメッセージのアンチウイルス処理の詳細を知りたいユーザに通知するテキスト。受信者、送信者、および管理者に送信される通知には、それぞれ固有のテンプレートがあります。このようなテンプレートを使用するには、**UseCustomTemplates** パラメータに **yes** を設定します。以下のテンプレートを使用できます:
 - 送信者への通知:
 - `notify_sender_common` - 元のメッセージに適用された処理について送信者に送信される通知のテキスト
 - `notify_sender_infected` - 感染メッセージと置き換えられるテキスト
 - `notify_sender_suspicious` - 疑わしいオブジェクトが含まれるメッセージと置き換えられるテキスト
 - `notify_sender_filtered` - フィルタリングされたメールメッセージと置き換えられるテキスト
 - `notify_sender_error` - スキャンエラーが発生したメッセージと置き換えられるテキスト
 - `notify_sender_protected` - 保護されていてスキャンできなかったメッセージと置き換えられるテキスト
 - 受信者への通知:
 - `notify_recipients_common` - 元のメッセージに適用された処理について受信者に送信される通知のテキスト
 - `notify_recipients_infected` - 感染メッセージと置き換えられるテキスト
 - `notify_recipients_suspicious` - 疑わしいオブジェクトが含まれるメッセージと置き換えられるテキスト
 - `notify_recipients_filtered` - フィルタリングされたメールメッセージと置き換えられるテキスト
 - `notify_recipients_error` - スキャンエラーが発生したメッセージと置き換えられるテキスト
 - `notify_recipients_protected` - 保護されていてスキャンできなかったメッセージと置き換えられるテキスト

- 管理者への通知:
 - notify_admin_common - 元のメッセージに適用された処理について管理者に送信される通知のテキスト
 - notify_admin_infected - 感染メッセージと置き換えられるテキスト
 - notify_admin_suspicious - 疑わしいオブジェクトが含まれるメッセージと置き換えられるテキスト
 - notify_admin_filtered - フィルタリングされたメールメッセージと置き換えられるテキスト
 - notify_admin_error - スキャンエラーが発生したメッセージと置き換えられるテキスト
 - notify_admin_protected - 保護されていてスキャンできなかったメッセージと置き換えられるテキスト
- **特別な管理者通知テンプレート** - 管理者によるチェックを必要とする重大なイベントが発生したときに送信される特別な通知に追加されるテキスト。管理用テンプレートは、アプリケーション設定ファイルの **[kav4lms:server.notifications]** セクションの **Templates** パラメータで指定されているディレクトリに保管されています。以下のテンプレートを使用できます:
 - product_update - アプリケーションの定義データベースに対する更新を受信したことを管理者に通知するテキスト
 - product_fault - Kaspersky Anti-Virus の動作中に重大なエラーが発生したことを管理者に通知するテキスト
 - product_license - 使用許諾契約違反があったこと、またはライセンス期間が終了したことを管理者に通知するテキスト

警告！

アプリケーションの起動時には、上記のテンプレートがすべて存在するかどうかの確認が行われます。1 つでも見つからないテンプレートがあると、アプリケーションはエラーで終了します。

また、各テンプレートのサイズが 8KB を超えていないかどうかの確認も行われます。

5.7.3. 通知テンプレートのカスタマイズ

管理者、送信者、受信者に送信されるデフォルトの通知テンプレートをカスタマイズすることができます。テンプレートをカスタマイズするには、特別な記述言語を使用します。

テンプレート言語は、制御ステートメントとマクロの集合です。

ここでは、この言語のルールや構文について、例をあげながら説明します。

警告！

「:」はヘッダーと解釈されてしまうので、テンプレートの最初の行に記述しないでください。通知ヘッダーと誤解されないようにするには、最初の行で改行します ([**Enter**] キーを押す)。

5.7.3.1. マクロ

マクロは、メール通知テンプレートで使用される置換要素です。テンプレートを使用して作成された通知テキストで、マクロは特定の値と置き換えられます。

マクロの構文は、`%macro_name%` です。

マクロ名に含まれる「%」はエスケープする必要があります (詳細は 62 ページの 5.7.3.5 を参照)。

マクロには複数の値を代入できます。その場合、単純に「`%macro_name%`」と記述すると、最後に代入された値が出力されます。

1 つのマクロに複数の値を代入するには、代入構文を使用します。

5.7.3.2. 代入構文

代入構文 (IC) は、テンプレート記述言語の基本要素です。

代入構文の構文を以下に示します。

```
<FOR INAME IOP IVALUE>BODY</FOR>
```

内容は次のとおりです：

<FOR - IC 定義の開始。IC 定義の開始以外の > 文字はエスケープする必要があります (62 ページの 5.7.3.5 を参照)

INAME - 「**1*(nchar)*(nchar)**」という形式の IC 名。最大長は 64 バイトです

IOP - 「**== !=**」形式の比較演算子。最大長は 2 バイトです

IVALUE - 「**1*(vchar)*(vchar)**」という形式の IC 値。最大長は 4096 バイトです。IC 値は二重引用符で囲む必要があります。疑問符を含む値と比較する場合は、エスケープ記号を使用します (62 ページの 5.7.3.5 を参照)

例:<FOR _macro_name_parent_ == "\ value 1\">

> - IC 定義の終了および代入定義の開始を表します。IC 定義の終了以外の > 文字はエスケープする必要があります (62 ページの 5.7.3.5 を参照)

BODY - 代入する本文。「*(char)」という形式で指定します

</FOR> - 代入定義の終了を表します。代入定義の終了文字以外の < 文字はエスケープする必要があります (62 ページの 5.7.3.5 を参照)

... - 「*()*(**□**)」という形式の区切り文字

nchar - a-z、A-Z、0-9、-、_ の範囲に属する文字

vchar -nchar、*、? の範囲に属する文字

char - 32 ~ 255 の範囲に属する文字

代入構文 の例:

```
<FOR _macro_name_ == "*">%_macro_name_%</FOR>
```

この代入構文を実行すると、パーサーによって以下の条件構文に変換されます:

```
<FOR _macro_name_ == " value 1">%_macro_name_%</FOR>
```

```
<FOR _macro_name_ == " value 2">%_macro_name_%</FOR>
```

```
<FOR _macro_name_ == " value 3">%_macro_name_%</FOR>
```

```
<FOR _macro_name_ == " value N">%_macro_name_%</FOR>
```

これらの構文は順番に解析されます。

そのため、代入構文を使用して、マクロの 1 つおよび複数の値を取り出すことができます。

たとえば、マクロ %FILTERNAME% の取りうる値が KAVFilter1、KAVFilter2、KAVFilter3、および SimpleFilter である場合は、以下のようになります。

構文:

```
<FOR FILTERNAME == "KAVFilter1">%FILTERNAME%</FOR>
```

変換後のテキスト:

```
KAVFilter1
```

構文:

```
<FOR FILTERNAME `== "KAVFilter?">%FILTERNAME%, </FOR>
```

変換後のテキスト:

```
KAVFilter1, KAVFilter2, KAVFilter3
```

構文:

```
<FOR FILTERNAME != "KAVFilter2">%FILTERNAME%, </FOR>
```

変換後のテキスト:

```
KAVFilter1, KAVFilter3, SimpleFilter
```

構文:

```
<FOR FILTERNAME != "KAV*">%FILTERNAME%, </FOR>
```

変換後のテキスト:

```
SimpleFilter
```

5.7.3.3. 代入構文の有効範囲

代入構文にはサブマクロを指定でき、その値は親構文の有効範囲内でのみ定義されます。代入構文は、特定のマクロの特定の値を出力するためだけでなく、サブマクロの有効範囲の定義にも使用できます。

サブマクロの有効範囲は、条件構文の開始タグと終了タグによって定義されます:

```
<FOR _macro_name_parent_ ==  
" value 1">%_macro_name_child_%</FOR>
```

この例では、マクロ値が無効な場合、すべての下位レベル (**FOR** タグの間) がマクロ `_%_macro_name_parent_%` の有効範囲に含まれます。

5.7.3.4. 変数

テンプレート記述言語を使用してテンプレートをカスタマイズする際、変数を使用すると自由度が高まります。

変数は指定された有効範囲内で定義できます:

```
<DEF _var_name_ = "const value" />
```

この変数は、何の制限も受けずに、通常のマクロとしても使用できます。

変数定義の構文は次のとおりです:

```
<DEF VNAME VOP VVALUE />
```

内容は次のとおりです:

<DEF - 変数定義構文の開始。変数定義構文の開始以外の < 文字はエスケープする必要があります (62 ページの 5.7.3.5 を参照)

VNAME - 「**1*(nchar)*(nchar)**」という形式の変数名。最大長は 64 バイトです

VOP - 「=」形式の代入演算子。最大長は 1 バイトです

VVALUE - 「1*(vchar)*(vchar)」という形式の変数値。最大長は 4096 バイトです。この値は二重引用符で囲む必要があります。引用符を含む値と比較する場合は、エスケープ文字を使用します (62 ページの 5.7.3.5 を参照)。例:

```
<DEF _value_name_ = "\" value 1\""/>
```

> - 変数定義構文の終了。変数定義の終了以外の > 文字はエスケープする必要があります (5.7.3.5 (62 ページ) を参照)。FOR 構文と違って、DEF 構文には本体がありません。そのため、タグの終わりの /> 文字で、終了タグがないことをパーサーに伝える必要があります

... - 「*()*(**□**)」という形式の区切り文字

nchar - a-z, A-Z, 0-9, -, _ の範囲に属する文字

vchar - nchar, *, ? の範囲に属する文字

変数が有効範囲内で再定義されている場合、再定義が行われるたびに新しい値で置き換えられます。以下に例を示します:

```
<DEF __NAME__ = "NAME 1"/>Now you will see the first
value: % __NAME__ %.
```

```
<DEF __NAME__ = "NAME 2"/>Now you will see the se-
cond value: % __NAME__ %.
```

出力されるテキスト:

```
Now you will see the first value: NAME_1.
```

```
Now you will see the second value: NAME_2.
```

変数の値としてマクロを使用できます。

```
<DEF _var_name_ = "% macro_name %"/>
```

この例では、まずマクロが値で置き換えられ、次に現在の有効範囲内で変数とその値で置き換えられます。

5.7.3.5. 言語構文

特殊文字

- %** マクロを表します。マクロは「%」と「%」で囲む必要があります
例: %VIRUSNAME%
- <** タグの始まり
例: <FOR FILTERNAME == "KAVFilter1">
- >** タグの終わり
例: <FOR FILTERNAME == "KAVFilter1">
- </** 終了タグの始まり
例: </FOR>
- />** 本文のない構文の終了タグの終わり
例: <DEF __NAME __ = "NAME_1"/>
- ** エスケープ文字。この文字の後にある特殊文字を通常文字として処理するようにパーサーに指示します
例: \%VIRUSNAME\%
- ==** 等号。マスクまたは値における一致を示します
例: <FOR FILTERNAME == "KAVFilter1">
例: <FOR FILTERNAME == "KAVFilter*">
- !=** 不等号。マスクまたは値における不一致を示します
例: <FOR FILTERNAME != "KAVFilter1">
例: <FOR FILTERNAME != "KAVFilter*">
- *** 任意の値と一致する値。長さに制限はありません。テンプレートと異なり、タグ内部でしか使用できません
例: <FOR FILTERNAME == "KAV*">
- ?** すべての 1 文字の値。テンプレートと異なり、タグ内部でしか使用できません
例: <FOR FILTERNAME == "KAVFilter?">
- #** コメント。パーサーは「#」で始まる行全体を無視します

予約キーワード

FOR 代入構文定義
例:<FOR FILTERNAME = "KAVFilter1">

DEF 変数定義 (終了タグのない構文)
例:<DEF __NAME__ = "NAME_1"/>

定義済みマクロ

%CRLF% 改行マクロ (CR+LF)

%TAB% タブ送りマクロ

処理はグローバルセクション内 (構文不要) または条件構文内で実行されます:

```
<FOR KAV_LANGUAGE == "5.0"> ... </FOR>
```

エスケープシーケンス

テンプレート記述言語では、以下のシーケンスを使用して特殊文字を表すことができます:

- テンプレートテキストで「\」文字を出力するには、「\\」と入力します
- 行が「\」で終わる場合、次の行に続く文字列として解釈されます。また、行末のエスケープ文字は、その次にある EOL を無効にします。エスケープ文字がない場合、EOL は出力されるメッセージに含まれます。「\」で終わる行は、パーサーによって他の処理が行われる前に、次の行と連結されます。この処理は、タグの内側または外側でエスケープシーケンスが検出されるたびに個別に行われます。行末に「□」を置く必要がある場合は、上記の項目 1 を参照してください
- テンプレートテキストで「%」文字を出力するには、「\%」と入力します
- テンプレートテキストで「/」文字を出力するには、「\/」と入力します
- テンプレートテキストで「<」文字を出力するには、「\<」と入力します
- テンプレートテキストで「>」文字を出力するには、「\>」と入力します
- テンプレートテキストで「#」文字を出力するには、「\#」と入力します

注記:

テンプレート記述言語では、大文字と小文字は区別されます。構文と構文の間の空白文字やタブ文字の数 (その有無) は規定されていません。予約キーワードは、空白文字または特殊文字によって区切る必要があります。

5.7.3.6. アプリケーションの通知マクロ

マクロは、通知テンプレートでメッセージ全体またはその一部として使用できます。マクロを使用すると、通知をカスタマイズして、元のメッセージのプロパティに関する情報や適用された処理に関する情報を追加できます。

管理者は、メッセージ全体に関する通知で、以下のマクロを使用できます：

- %VERSION% - メッセージのスキャンに使用された、インストールされている Kaspersky Anti-Virus のインスタンスのバージョン番号
- %PRODUCT% - Kaspersky Anti-Virus の正式な製品名
- %CLIENT% - メールクライアントのリモート IP アドレス
- %SERVER% - アプリケーションのメインサービスが動作しているサーバの名前
- %SENDER% - 送信者のアドレス
- %RECIPIENTS% - 受信者のアドレス
- %HEADERS% - メッセージヘッダー
- %MSGID% - メッセージ ID
- %SUBJECT% - 元のメッセージの件名 ([**Subject**] フィールド)
- %DATE% - メッセージが処理された日付
- %TIME% - メッセージが処理された時刻
- %BK_ACTION% - バックアップを作成する原因となったメッセージに適用された処理 (アプリケーションがメッセージをバックアップするように設定されている場合)
- %BK_LOCATION% - バックアップが保管されているストレージの絶対パス (ストレージが存在する場合)
- %ACTION_LIST% - メッセージとそのオブジェクトおよびそれらに適用された処理のリストに関する情報が含まれるリスト。この情報は、以下の形式で出力されます：
<status> <action> <information>
この情報は、メッセージの処理されたパーツごとに出力されます

メッセージから削除されたオブジェクトに関する通知では、以下のマクロを使用できます：

- %INFO% - 実行された以下の処理に関する情報：
 - 検知されたウイルス (悪意のあるソフトウェア) のリスト - 感染オブジェクトの場合
 - エラーコードの説明 - スキャンエラーが発生したオブジェクトの場合
 - MIME タイプまたは添付ファイルの名前 - フィルタリングされたオブジェクトの場合

マクロは通知テンプレートのテキストで指定する必要があります。

第6章. アンチウイルスによるファイルシステムの保護

kav4lms-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。

注記:

kav4lms-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。

警告!

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** ユーザと **kluser** 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 (65 ページの 6.1 を参照)
- オブジェクトのスキャン方法と感染駆除方法 (67 ページの 6.2 を参照)
- オブジェクトに対して実行する操作 (68 ページの 6.3 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 (69 ページの 6.4 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 (69 ページの 6.5 を参照)

警告!

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。

6.1. 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。

注記:

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

警告!

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。

- スキャン対象の再帰的スキャンをオフにする (**[scanner.options]** セクションの **Reursion**、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

スキャンの対象となるオブジェクトへのパスは、4096 バイト以下でなければなりません。それより長いパスに配置されているオブジェクトはスキャンされません。

デフォルトのスキャンオブジェクトは設定ファイル `kav4lms.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

6.2. 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
- **Suspicious** - 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 (**UseCodeAnalyzer=no** の場合は割り当てられません)
- **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駆除を受けます。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

6.3. 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。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処理も区別されており、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。

警告！

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処理は、以下の方法で選択することができます：

- デフォルト処理として使用する場合は、kav4lms.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処理を指定し、コンポーネントの起動時にこのファイルを使用します

注記：

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、kav4lms.conf ファイルの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、kav4lms-kavscanner 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)。

6.4. 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。

以下の条件でアンチウイルススキャンを実行します：

1. /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します。感染を駆除できなかったオブジェクトは削除します
2. 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します
3. 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 kavscanner-current_date-pid.log に出力します

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/kav4lms/bin/kav4lms-kavscanner -\  
rlq -pi/tmp/infected.lst -ps/tmp/suspicion.lst -\  
pc/tmp/corrupted.lst -pw/tmp/warning.lst -o /tmp/ \  
kav4lms-kavscanner-`date +%Y-%m-%d-%$` .log -i3 \  
\
```

6.5. 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

/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。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/kav4lms/bin/kav4lms-\  
kavscanner -c /etc/kav/scanhome.conf /home
```

6.6. 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。

設定ファイル `kav4lms.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。

警告！

例は、Linux を対象としています。

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、`kav4lms.conf` で指定します：

```
[scanner.object]
OnInfected=exec echo %FULLPATH%/%FILENAME% is \
infected by %VIRUSNAME% |
mail -s kav4lms-kavscanner admin@localhost

[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME% \
is infected, viruses list is in the attached file \
%LIST% | mail -s kav4lms-kavscanner -a %LIST% \
admin@localhost
```

警告！

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。

第7章. 定義データベースの更新

定義データベースの更新は kav4lms-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/kav4lms/bin/kav4lms-keepup2date -s
```

更新処理を行うとき、kav4lms-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。kav4lms-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。

注記：

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。

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再読み込みされます。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。

注記：

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、7.3 (73 ページ) 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 (72 ページの 7.1 を参照) か、管理者がコマンドラインから手動で行う (73 ページの 7.2 を参照) ことができます。

7.1. 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。

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。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/kav4lms/bin/kav4lms-\
keepup2date -e
```

アプリケーションに付属のリストからアップデートサーバの URL を自動的に選択するように kav4lms-keepup2date コンポーネントを設定する。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。

管理者の指定した URL から更新をダウンロードするように、keepup2date 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。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。

指定した URL から更新をダウンロードするように keepup2date 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、コンポーネントに含まれているリストで指定された URL から定義データベースを更新する。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。

7.2. 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/kav4lms/bin/kav4lms-keepup2date
```

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。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/kav4lms/bin/kav4lms-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。

ネットワークディレクトリ ftp://10.10.10.1/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します。結果は report.txt ファイルに出力します。

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=ftp://10.10.10.1/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/kav4lms/bin/kav4lms-keepup2date -l \  
/tmp/report.txt
```

7.3. 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。

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。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 kav4lms-keepup2date コンポーネントを起動します:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-keepup2date -u  
<dir>
```

<dir> には、ローカルディレクトリへの絶対パスを指定します

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

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。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

第8章. ライセンスキーの管理

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、ライセンス方式、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：

- 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

キーの期限が切れると、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、キー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。定義データベースを手動で更新した場合、そのリリース日付はキーの有効期限よりも新しい可能性があります。その場合、アプリケーションはアンチウイルス機能を失い、それに対応する注記がログに記録されます。

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

アプリケーションでは、以下のライセンス方式をサポートしています：

- **トラフィックによるライセンス方式**

このライセンス方式は、キーで指定された日次トラフィックの量に対する保護を提供します。クリーンまたは未チェックと認識された処理済みトラフィックだけが考慮されます。日次トラフィックがライセンス限度を超えた場合は、ライセンス限度を超えている最初のメッセージおよび後続のメッセージについて管理者の通知が発行されます。

- **アドレスによるライセンス方式**

このライセンス方式は、特定の数のメールアドレスに対する保護を提供します。これは、kav4lms.conf ファイルの **[kav4lms:server.settings]** セクションの **LicensedUsersDomains** パラメータで指定されたドメインのリストと、アプリケーションが動作しているサーバ上のアドレスに適用されます。

ライセンスされたドメイン名は、以下の方法で指定できます：

- そのままの文字列
- ワイルドカード表現 (UNIX 構文)
- 正規表現 (POSIX 構文)

警告！

正規表現では、大文字と小文字は区別されません。

ドメイン内のメールアドレスの数がライセンス限度を超えた場合、管理者は、追加のトラフィック量に対するキーの購入を促されます。

8.1. キー詳細の表示

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 kav4lms-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。

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/kav4lms/bin/kav4lms-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 for Linux. Version 5.6/RELEASE  
#68
```

```
Copyright (C) Kaspersky Lab, 1997-2007.
```

```
Portions Copyright (C) Lan Crypto
```

```
License info:
```

```
Product name: Kaspersky Anti-Virus BO for SendMail / Qmail  
/ Postfix Milter API International Edition. 10-14 MailAd-  
dress 1 month Beta Licence
```

```
Expiration date: 01-09-2007, expires in 28 days
```

```
Active key info:
```

```
Key file: 00BEA0DB.key
```

```
Install date: 02-08-2007
```

```
Product name: Kaspersky Anti-Virus BO for SendMail /  
Qmail / Postfix Milter API International Edition. 10-14  
MailAddress 1 month Beta Licence
```

```
Creation date: 02-02-2007
```

```
Expiration date: 03-03-2008
```

```
Serial: 0038-000413-00BEA0DB
```

```
Type: Beta
```

```
Count: 10
```

```
Lifespan: 30
```

```
Objs: 7:10
```

Objs パラメータは、ライセンスオブジェクトを表します。その値の構成は、`<type_of_objects>:<number_of_objects>` となります。

`<type_of_objects>` には、以下の値を使用できます：

- 3 - 日次トラフィック
- 7 - メールアドレス

`<number_of_objects>` の値は、Count パラメータと同じです。

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/kav4lms/bin/kav4lms-licensemanager\  
-k <key filename>
```

`<key filename>` には、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 for Linux. Version 5.6/RELEASE  
#68
```

```
Copyright (C) Kaspersky Lab, 1997-2007.
```

```
Portions Copyright (C) Lan Crypto
```

```
Product name: Kaspersky Anti-Virus BO for SendMail /  
Qmail / Postfix Milter API International Edition. 10-14  
MailAddress 1 month Beta Licence
```

```
Creation date: 02-02-2007
```

```
Expiration date: 03-03-2008
```

```
Serial: 0038-000413-00BEA0DB
```

```
Type: Beta
```

```
Count: 10
```

```
Lifespan: 30
```

```
Objs: 7:10
```

8.2. キーの更新

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、75 ページの 2 に挙げられた追加サービスが可能な状態となります。

キーの有効期間は、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。

キーを更新するには:

購入元の販売代理店までお問い合わせください。

注意:

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。

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/kav4lms/bin/kav4lms-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 (71 ページの第 7 章を参照)。

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:

アクティブなキーを削除するには:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager\  
-da
```

追加のキーを削除するには:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-licensemanager\  
-dr
```

第9章. レポートと統計値

9.1. アプリケーションログ

注記:

アプリケーションは、サーバとフィルタの両方のコンポーネントについてログを作成します。ログオプションは、サーバかフィルタかに応じて `kav4lms.conf` ファイルの `[kav4lms:server.log]` および `[kav4lms:filter.log]` セクションに保管されます。

アプリケーションコンポーネントの作業結果は、システムログまたはログファイルに保管されます。保管先は、**Destination** パラメータで指定します。保管先の構文は以下のとおりです:

- `syslog:<name>@<facility>` - アプリケーション `<name>` としてカテゴリ `<facility>` に記録します
- `file:<log_file_path>` - 指定したファイルにメッセージが記録されます

警告!

サーバとフィルタに同じファイルを記録先として使用しないでください。ログファイルを使用できるのは、1 度に 1 つのプロセスだけです。

記録される情報のタイプと完全性は、**Options** パラメータで指定します。**Options** パラメータ値は、ログオプションのリストです。ログオプションは、ドットで区切られた 2 つの部分で構成されません:

1. ログモジュール。この部分は、作業が記録されるアプリケーションの機能モジュールを表します。使用可能な値は以下のとおりです:
 - **all** - すべてのグループを含みます
 - **config** - 設定に関連したメッセージ
 - **app** - 製品のビジネスロジックからのイベント
 - **scan** - スキャンのステータス、処理
 - **cfilter** - コンテンツフィルタリングのステータス、処理
 - **backup** - バックアップ関連のメッセージ
 - **notif** - 通知システムからのメッセージ
 - **admin** - 管理機能に関連したイベント (たとえば、SNMP、コマンドなど)
 - **smtp** - MTA とアプリケーションの間の SMTP ダイアログ情報

2. レポートレベル。この部分は、記録された情報の重要度を表します。これは、名前、文字、または数字で指定できます。使用可能なオプションとその説明については、以下の表を参照してください

レベル記号	レベル名	説明
0, F	fatal	重大な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キーの読み込み中にエラーが発生した、など。重大なエラーの情報には、ログファイル内で「F」が付けられます
1, E	error	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, W	warning	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、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, I	info	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、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, A	activity	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, D	debug	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

ログオプションは、以下の方法で指定できます：

- グループとレベルの組み合わせ (たとえば、**scan.info**)
- グループとレベルの組み合わせの前に「-」を付けると、指定したオプションが除外されます

例：

```
[kav4lms:server.log]
```

```
Options = backup.all, config.error, scan.all, -scan.debug
```

```
Options = backup.all, config.E, scan.all, -scan.9
```

この例では、デバッグを除き、すべてのバックアップメッセージ、config からのすべてのエラーメッセージ、すべてのスキャンメッセージが有効になります。2 番目の例は最初の例と同じですが、レベル選択オプションを使用しています。

警告！

レポートレベルには、前の（下位の）レベルは含まれません。複数のレベルを選択するには、それらのレベルをすべて指定するか、不要なレベルを除外する必要があります。

ログファイルは急速に増大する可能性があります。そのサイズはログのローテーションを有効にすることで制限できます。この機能を有効にするには、**RotateSize** および **RotateRounds** パラメータをゼロ以外の値に設定します。

ログのローテーションを有効にした場合、ログファイルはサイズが **RotateSize** に達するまで増大します。その後、ログファイルの名前は変更され、接尾辞「.1」が付きます。この接尾辞を使用したファイルがすでに存在する場合は、数値（接尾辞）が **RotateRounds** に達するまで「.2」、「.3」などの接尾辞を使用したファイルが作成されます。**RotateRounds** 値に達すると、接尾辞が「.1」のファイルが再使用されます。

9.2. アプリケーション統計値

注記:

アプリケーション統計値収集のオプションは、メイン設定ファイルの `[kav4lms:server.statistics]` セクションにあります。

アプリケーションの実行中には、以下の 2 種類の統計値が収集されます:

- 時々収集されて全体的なアプリケーション動作を反映する**一般**統計値
- 処理されたメッセージごとに収集される**詳細**統計値

保管される統計値の種類は、**Options** パラメータで指定します。使用可能な値は以下のとおりです。

統計値のカテゴリ	オプション値	保管される情報
メッセージ	messages	受信メッセージの数、スキャン済みメッセージの数、保護されたメッセージの数、感染したメッセージの数、誤った (破損した) メッセージの数、すべてのメッセージサイズの平均 (バイト単位)、1 つのメッセージのチェックに費やされた平均時間 (ミリ秒単位)
システムリソース	resources	統計値が最後に要求された時点からの経過時間 (秒単位)、合計トラフィックサイズ (キロバイト単位)、ユーザごとの合計 CPU 使用量、システムごとの合計 CPU 使用量
検知された脅威	viruses	最後に検知された 10 個のウイルス、最も多くのウイルスを送信した上位 10 個の IP アドレス
コンテンツフィルタリング	filters	MIME フィルタリングされたメッセージの数、添付ファイルによってフィルタリングされたメッセージの数、サイズによってフィルタリングされたメッセージの数、ウイルス名によってフィルタリングされたメッセージの数
すべて	all	上記のすべて
メッセージごとの統計値	raw	メッセージごとの包括的な統計値
統計値なし	none	統計値は収集されません

Options パラメータの値は、カンマで区切られた上記値のリストです。

例:

```
Options = all
```

総計の統計値 (メッセージ、リソース、ウイルス、フィルタ) だけを収集します。

```
Options = all, raw
```

メッセージごとの統計値も収集します。

```
Options = none, raw
```

メッセージごとのデータだけを収集します (総計なし)。

統計値の収集を有効にするには、**Options** パラメータを **none** 以外の値に設定します。

警告!

Options パラメータを **all** に設定しても生統計値は有効になりません。この統計値タイプは、明示的に指定する必要があります。

生統計値ファイルのサンプルレコード:

```
1210247100      1208      _from@example.com  
rcpt@example.com  infected      EICAR-Test-File 127.0.0.1  
1Ju4YW-000Du9-0U Default
```

内容の説明:

- 1210247100 - メッセージが処理された時刻 (UNIX 形式)
- 1208 - メッセージサイズ
- _from@example.com - メッセージ送信者のアドレス
- rcpt@example.com - メッセージ受信者のアドレス
- infected - スキャン後にメッセージに割り当てられたステータス
- EICAR-Test-File - メッセージ内で検出された脅威の名前
- 127.0.0.1 - メッセージを送信するために使用した IP アドレス
- 1Ju4YW-000Du9-0U - メールキューでのメッセージ ID
- Default - メッセージの処理に使用した設定に関連付けられているグループの名前

統計値をファイルに書き込むには、以下のコマンドを実行します:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-cmd -m statistics -x \  
write
```

このコマンドは、既存の統計値ファイルにも新しい情報を上書きします。

内部統計値カウンタをリセットするには、以下のコマンドを実行します：

```
# /opt/kaspersky/kav4lms/bin/kav4lms-cmd -m statistics -x \  
reset
```

注記：

カウンタをリセットした後に変更内容を反映するには、統計値ファイルを上書きする必要があります。

統計機能のパラメータは、kav4lms.conf ファイルの **[kav4lms:server.statistics]** セクションでグループ化されます。

統計値には、以下の 2 つのタイプがあります：

- **総計** - 時間の経過に伴って累積され、全体的な製品の動作を反映します
- **メッセージごと** - 処理されたメッセージごとに書き込まれ、その処理に関する詳細情報を示します。これらは、**生統計値**とも呼ばれます

総計の統計値は、**Destination** パラメータで指定したファイルに保管されます。生の統計値は、**RawDestination** パラメータで指定したファイルに保管されます。

警告！

スキャン判定の異なる複数のタイプのオブジェクトがメッセージに含まれている場合は、対応する各カウンタによって同じメッセージがカウントされます。したがって、カウンタは累積的ではありません。つまり、カウンタの合計はスキャンされたメッセージの総数を示していない可能性があります。

たとえば、感染した添付ファイル、パスワード保護された添付ファイル、application/msword タイプの添付ファイルを伴う単一メッセージは、設定に応じて以下のカウンタでカウントされる可能性があります：

- **total_messages** - 転送されたメッセージの 1 つであるため
- **scanned_messages** - メッセージが分析されているため
- **protected_messages** - 保護された部分がメッセージにあるため
- **infected_messages** - 感染した部分がメッセージにあるため
- **filtered_mime** - 一致する MIME タイプがメッセージにあるため

統計値は、以下の 2 つの形式で収集できます：

- **txt** ファイル
- **xml** ファイル

統計値のファイル形式は、**Format** パラメータで指定します。

第10章. 高度な設定

10.1. SNMP による保護ステータスの監視

バージョン 5.6 以降のアプリケーションでは、SNMP プロトコルを使用して以下の情報への読み取り専用アクセスを実行できます：

- 製品設定 - アプリケーションの設定ファイル (グループ設定ファイルを含む) の全セクションのパラメータ
- 動作の統計値 - アプリケーションの動作に関する包括的統計値

注記：

アプリケーションは、SNMP プロトコル v1、v2、v3 をサポートしているエージェントを扱います。この製品では v2 トラップを送信するため、それに応じてトラップシンクを設定する必要があることに注意してください。

SNMP 上でアクセスできる情報は、kav4lms.conf 設定ファイルの **[kav4lms:server.snmp]** セクションにある **SNMPServices** パラメータで決定されます。このパラメータには、以下の値を使用できます：

- **config** - アプリケーション設定情報
- **statistics** - 動作の統計値 (発行される統計値の詳細については、82 ページの 9.2 を参照)
- **admin** - 以下を含む管理情報：
 - **Status.StartedOn** - アプリケーションを起動した日付 (ISO 8601 形式)
 - **Status.UpTime** - アプリケーションを起動してから経過した時間 (秒単位)
- **update** - 以下を含むアプリケーション更新情報：
 - **Last.Checked** - 最後に更新をチェックした日付 (ISO 8601 形式)
 - **Last.Result** - 最後に行われた更新のステータス：
 - **updated** - 更新に成功し、新しい定義データベースがインストールされた
 - **not-needed** - 更新は正しく完了したが、新しいファイルは必要なかった
 - **error** - 更新プロセスが失敗した
 - **rolled-back** - 更新は成功したが、定義データベースが破損していたため、ロールバックが実行された
 - **unknown** - 最後に行われた更新のステータスを確認できなかった

- **Current.Loaded** - 最後に成功した更新の日付 (ISO 8601 形式)
- **Current.Records** - 現在使用中の定義データベースにおけるシグネチャの数
- **Current.Released** - 最後の更新がリリースされた日付 (ISO 8601 形式)
- **all** - 上記のすべての情報
- **none** - SNMP 上では、どの情報も公開しない

Kaspersky Anti-Virus は、AgentX プロトコル経由で SNMP マスタエージェントと対話する SNMP サブエージェントを使用します。AgentX プロトコルパラメータは以下のとおりです：

- **Socket** - 対話ソケット。以下の例に示すように、ローカルファイルまたはネットワークソケットを使用できます：

```
Socket=local:/var/agentx/master
```

または

```
Socket=inet:705@127.0.0.1
```

警告！

ローカル Unix ソケットを使用する場合は、サブエージェントとマスタエージェントがそのソケットにアクセスできることを確認してください。場合によっては、**RunAsUser** および **RunAsGroup** 設定と、サービス（ソケットとデータファイルが同じコンピュータ上にある場合は、メインサービス）が使用するソケットおよびデータファイルのアクセス権を変更する必要があります。

- **Timeout** - AgentX 要求のタイムアウト (秒単位)。デフォルト値は **5** です
- **Retries** - AgentX 要求の再試行回数。デフォルト値は **10** です。このパラメータが設定されていない場合は、値 **5** が使用されます。

警告！

実際の再試行回数は、指定した **Retries** 値と異なる場合があります。これは「watchdog」の動作が原因で発生するものであり、問題はありません。

- **PingInterval** - 切断状態になったサブエージェントがマスタエージェントへの接続を試みる時間間隔 (秒単位)

AgentX プロトコルをサポートする任意の SNMP エージェントをマスタエージェントとして使用できます。以下のセクションでは、「NET-SNMP」エージェントの設定例を示します。この設定例では、アプリケーションサブエージェントがローカルソケットを使用して NET-SNMP に接続します。

警告！

AgentX プロトコルを正しく実装するバージョン 5.1.2 以上の NET-SNMP を使用することをお勧めします。

マスタエージェントを設定するには、以下の手順を実行します：

1. 以下の行を `snmpd.conf` 設定ファイルに追加します:

```
master agentx
AgentXSocket /var/agentx/master
AgentXPerms 770 770 root klusers
rocommunity public localhost
trapsink localhost
```

ネットワークソケットを使用する場合は、2 行目を以下のように変更します:

```
AgentXSocket tcp:127.0.0.1:705
```

2. 以下の行を `snmp.conf` 設定ファイルに追加します:

Linux の場合:

```
mibdirs +/opt/kaspersky/kav4lms/share/snmp-mibs
mibs all
```

FreeBSD の場合:

```
mibdirs +/usr/local/share/kav4lms/snmp-mibs/
mibs all
```

パス「`/opt/kaspersky/kav4lms/share/snmp-mibs`」では、Kaspersky Anti-Virus の MIB ファイルが保管されるデフォルトディレクトリが指定されます。アプリケーションが別のディレクトリにインストールされている場合は、それに応じてこのパスを変更してください

3. NET-SNMP を再起動します

注記:

NET-SNMP に関する詳しい情報は、<http://www.net-snmp.org/> にあります。`snmpd.conf` および `snmp.conf` 設定ファイルの詳細については、該当するマニュアルページを参照してください。

製品 OID は、以下のブランチのもとでアクセスできます:

.1.3.6.1.4.1.23668.1043

または、以下のシンボリック形式でアクセスできます:

iso.org.dod.internet.private.enterprises.kaspersky.kav4lms

このノードには、以下のグループが含まれます:

- **config** - 設定ファイルの場合と同様に複数のセクションに分けられたアプリケーション設定パラメータ (グループの設定など)
- **statistics** - 処理されたメッセージ、使用中のリソース、および検出されたウイルスに関する統計情報
- **update** - アプリケーション更新情報

- **admin** - 管理情報 (アプリケーション起動時間やエラーなど)

警告!

config.Groups セクションにあるオブジェクトのパラメータ値を取得する場合は、**Get** ではなく **Walk** メソッドを使用してください。

管理者は、特定のイベントが発生した場合に SNMP Trap を送信するようにアプリケーションを設定することもできます。kav4lms.conf 設定ファイルの **[kav4lms:server.snmp]** セクションにある **SNMPTraps** パラメータでは、アプリケーションによる SNMP Trap の送信を誘発するイベントが決定されます。使用可能な値は以下のとおりです:

- **config** - 設定またはデータベースを再読み込みすると、SNMP Trap が送信されます (ConfigReloaded トラップまたは BasesReloaded トラップ)
- **admin** - SNMP Trap は、アプリケーションが起動または停止した場合 (ProductStart トラップまたは ProductStop トラップ) やアプリケーションに致命的エラーが発生した場合 (ProductError トラップ) に送信されます。また、AlertThreshold パラメータ値がゼロに設定されていない場合は、過去 1 時間内に見つかった感染メッセージの割合が特定の値を超えると、SNMP Trap が送信されます (AlertThreshold)。しきい値を超えて以降は、感染メッセージの割合が定義済みの限度を下回るまで毎時間 AlertThreshold トラップが送信されます

注記:

アプリケーションの再読み込みに対応する **ConfigReloaded** トラップが存在します。ただし、この場合は **ProductStart**、**ProductStop**、および **BasesReloaded** トラップも送信されます。これは、watchdog がアプリケーションをウォームリスタートするために起こります。

- **update** - SNMP Trap は、アプリケーションの更新を実行した場合 (UpdateStatus トラップ) や定義データベースが 5 日間より古い場合 (ObsoleteBases トラップ) に送信されます
- **all** - 上記のいずれかのイベントが発生すると、SNMP Trap が送信されます

- **none** - SNMP Trap は送信されません

警告！

NET-SNMP マスタエージェントを使用する場合は、トラップを受信するために `snmptrapd` デモンを起動する必要があります。

10.2. アプリケーションのセットアップスクリプトの使用

Kaspersky Anti-Virus では、特殊なスクリプトを使用して、インストール済みのアプリケーションを管理できます。

セットアップスクリプトは、以下のように使用します：

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh <option>
```

使用可能なオプションは以下のとおりです：

- `--install-services` - メインサービスおよびフィルタサービスを既存のシステムに登録します
- `--remove-services` - すべてのサービスを登録解除します（このシステムでは開始/停止されなくなります）
- `--check-services` - アプリケーションのサービスが登録されているかどうかを確認します
- `--install-filter=<MTA>` - 指定の MTA にフィルタを登録します。これにより、フィルタもサービスとして登録されます（該当する場合）
- `--remove-filter=<MTA>` - 指定の MTA からフィルタサービスを登録解除します
- `--remove-filters` - MTA のアクティブなフィルタをすべて削除します
- `--check-filter=<MTA>` - MTA の設定変更が行われたかどうかを確認します
- `--filter-options=<options>` - フィルタ専用オプションを設定します。このオプションは、フィルタ専用パラメータを指定するために `--install-filter` オプションとの組み合わせでのみ使用されます。Sendmail の場合は、オプションとして **tempfail**、**reject**、**pass** を使用できます
- `--install-cron=<component_name>` - 指定されたコンポーネント用の cron ジョブをインストールします
- `--remove-cron=<component_name>` - 指定されたコンポーネント用の cron ジョブを削除します

- `--check-cron=<component_name>` - コンポーネント用の cron ジョブが登録されているかどうかをチェックします
- `--user=<user_name>` - メインサービスおよびアプリケーションフィルタの実行に使用される資格情報を持ったユーザ名を指定します。このオプションを `--install-cron` および `--remove-cron` パラメータと一緒に使用すると、スケジュールの作成対象となるユーザアカウントが定義されます

例:

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \  
--install-cron=updater --user=root
```

または

```
# /opt/kaspersky/kav4lms/bin/kav4lms-setup.sh \  
--install-cron=updater --user=qmailq
```

- `--add-components-info` - コンポーネント固有のオプションを `applications.setup` ファイルに追加します
- `--del-components-info` - コンポーネント固有のオプションをアプリケーションレジストリから削除します
- `--check-components-info` - コンポーネントのオプションが存在するかどうかを確認します
- `--install-webmin-module` - Web ベースの管理モジュールを Webmin に追加します
- `--remove-webmin-module` - Webmin からモジュールを削除します
- `--check-webmin-module` - Webmin モジュールがインストールされているかどうかを確認します
- `--register-key=key-id` - 絶対パス、または `licenses` ディレクトリに関連した id によってキーを登録します
- `--group=<group_name>` - Kaspersky Anti-Virus の実行に使用するグループを指定します。このオプションを使用すると、アプリケーション設定ファイルの **[options]** セクションにある **Group** 値が変更されます
- `--switch-credentials=<user_name>[,<group_name>]` - アプリケーションのメインサービスとフィルタの開始に使用する資格情報を持つユーザとグループ (指定した場合) を指定します。このオプションを使用すると、アプリケーション設定ファイルの **[kav4lms:server.settings]** および **[kav4lms:filter.settings]** セクションにある **RunAsUser** 値および入力済みの **RunAsGroup** 値が変更されます。また、アプリケーションのメインサービスとフィルタが再起動されます

<MTA> パラメータでは、統合対象の MTA を指定します。使用可能な値は以下のとおりです：

- **exim** - Exim との post-queue による統合
- **exim-dfunc** - 動的に読み込まれるライブラリを使用した Exim との pre-queue による統合
- **postfix** - Postfix との post-queue による統合
- **qmail** - qmail との統合
- **sendmail-milter** - Sendmail との統合

<component_name> パラメータでは、アプリケーションのコンポーネント名を指定します。使用可能なオプションは **updater** です。

注記：

「--check」オプションはサイレントに実行され、チェック対象のアイテムが存在する場合は 0、存在しない場合は 0 以外 を返します。

10.3. コマンドラインからのアプリケーション管理

Kaspersky Anti-Virus には、コマンドライン管理ツールの `kav4lms-cmd` が用意されています。このツールは、`/opt/kaspersky/kav4lms/bin` ディレクトリにあります。

警告！

`ka4lms-cmd` ツールを使用するには、アプリケーションのメインサービスを実行する必要があります。

このツールのコマンドラインオプションは、以下の 2 つのカテゴリに分かれています：

1. 一般アプリケーションオプション。これには、以下のものが含まれます：
 - `-v` または `--version` - プログラムのバージョンを表示します
 - `-h` または `--help` - インラインヘルプメッセージを表示します
 - `-m` または `--module <argument>` - さらなるコマンドのために特定のモジュールを選択します。モジュールに使用できるオプションは、`config`、`filter`、`kavmd`、`statistics`、`update` です
 - `-c` または `--config <argument>` - デフォルト以外の設定ファイルを指定します
 - `-l` または `--list` - 使用可能なモジュールをリストアップします
2. モジュール別のオプション

- a) **Config** モジュール。このモジュールは、設定パラメータの照会と設定によってアプリケーションの設定ファイルを変更します:
- `-q <key>` - 設定パラメータの値を照会します。たとえば、`-q Path.TempPath`
- b) **Filter** モジュール。このモジュールは、フィルタコンポーネントを管理します。使用可能なオプションは以下のとおりです:
- `-x <command>` - フィルタコンポーネントコマンドを呼び出します。使用可能なオプションは、`start`、`stop`、`restart`、`status`、`test-service` です
- c) **Central service (kavmd)** モジュール。このモジュールは、メインアプリケーションサービスを管理します。使用可能なオプションは以下のとおりです:
- `-x <service-command>` - メインサービスコマンドを呼び出します。使用可能なオプションは、`start`、`stop`、`restart`、`reload`、`status`、`test-service` です
- d) **Statistics** モジュール。このモジュールは、アプリケーションの統計値を管理します。使用可能なオプションは以下のとおりです:
- `-x <stats-command>` - 統計コマンドを呼び出します。使用可能なオプションは、`write`、`reset` です
- e) **Update** モジュール。このモジュールは、`kav4lms-keepup2date` コンポーネントを管理します
- `-e <event-name>` - 特定のイベントの配信を指定します。オプションは、`OnUpdated`、`OnNotNeeded`、`OnError`、`OnRolledback`、`OnUnknown` です

10.4. メッセージ内の追加情報フィールド

アプリケーションでは、2 種類の方法のいずれかを使用して補足情報をヘッダーフィールドとしてメールメッセージに追加できます：

- メールメッセージへの拡張ヘッダーフィールドの追加

この情報は、アプリケーションバージョン、定義データベースの最終更新日、メッセージスキャンの日時と結果を示します。グループ設定ファイルの **[kav4lms:groups.<group_name>.settings]** セクションにある **AddXHeaders** パラメータによって決定されます。

ヘッダー形式：

```
X-Anti-Virus: <product name and version>, bases:
<date of the last update to anti-virus databases in
YYYYMMDDTHHMMSS format> #<the number of records in AV
databases>, check: <scan date in YYYYMMDD format>
<scanning status or notchecked>
```

説明：

YYYY は 4 桁形式の年を表します

MM - 月

DD - 日

HH - 時間

MM - 分

SS - 秒

例：

```
X-Anti-Virus: Kaspersky Anti-Virus for Linux Mail
Server 5.6.17/RELEASE build 4,
bases: 20080415 #705877, check: 20080415 clean
```

- メールメッセージ本文への免責テキストの追加

この情報はプレーンテキストとして追加されます。組織のセキュリティポリシー（またはその他のルール）に従って作成された記述が含まれており、**[kav4lms:groups.<group_name>.settings]** セクションの **AddDisclaimer** パラメータによって指定されます。デフォルトのメッセージテキストは、メッセージが Kaspersky Anti-Virus によってスキャン済みであることを通知する内容です。アプリケーションでは、管理者の要求に応じて情報の形式を変更できます（免責メッセージを HTML テキストで作成するなど）。

- 削除したメッセージ部分の置換

メッセージの処理中には、選択した動作に従ってメッセージの一部を削除できます。削除した部分は、理由に関する通知に置き換えることができます。そのためには、**UsePlaceholderNotice** パラメータ (グループ設定ファイルの **[kav4lms:groups.<group_name>.settings]** セクション) を **yes** に設定します。**UsePlaceholderNotice** の値が **no** の場合は、それぞれの部分がメッセージから完全に削除され、もともと存在しなかったかのような状態になります。

通知テキストは、通知マクロもサポートしている `part_<action_taken>` という名前のテンプレートファイルから取得されます (詳細については、53 ページの 5.7 を参照)。

10.5. 表示される日時形式のローカライズ

Kaspersky Anti-Virus の動作中には、各コンポーネントのレポートとユーザおよび管理者に対する各種通知が編集されます。そのような情報には、出力の日時が常に補足されます。

デフォルトでは、Kaspersky Anti-Virus は `strftime` 標準に対応する以下の日時形式を使用します:

%H:%M:%S - 時刻出力の形式 (**hh.mm.ss**)

%d-%m-%y - 日付出力の形式 (**dd.mm.yy**)


管理者は、日時形式を変更することができます。形式のローカライズは、`kav4lms.conf` 設定ファイルの **[locale]** セクションで行います。定義できる形式は以下のとおりです:

%I:%M:%S %P - 24 時間形式の時刻出力 (**TimeFormat** パラメータ)

%y/%m/%d, %m/%d/%y - 日付出力 (**DateFormat** パラメータ) (それぞれ、**yy.mm.dd, mm.dd.yy**)

第11章. アプリケーションのテスト

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。

このテスト用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。

警告！

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) からダウンロードできます。

注記:

anti_virus_test_file.htm ファイルは、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ソリューションによって HTTP 経由で転送された感染オブジェクトとして識別されて処理されます。そのため、ダウンロードの前にアンチウイルス保護を無効にする必要があります。

テストウイルスをダウンロードしたらアンチウイルス保護をすぐに有効にする必要があるので注意してください。

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)。テキストは任意のテキストエディタで編集できます。

注記:

定義データベースの最終更新日が 2003 年 10 月 24 日以降 (2003 年 10 月の累積更新が含まれている) の場合のみ、EICAR テストウイルスの変更によってアプリケーションが正しく機能していることを確認できます。

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)	感染 (Infected) - 駆除できないオブジェクト
CORR-	破損 (Corrupted)
SUSP-	感染の疑いあり (Suspicious) - 未知のウイルスコード
WARN-	感染の疑いあり (Suspicious) - 既知のウイルスコードの変種
ERRO-	未分析 (Not analyzed) - エラーが原因
CURE-	駆除 (Disinfected) - 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

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。

テストウイルスに接頭辞を追加したら、それを別の名前 (たとえば、eicar_corr.com) でファイルに保存します。

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

A.1. アプリケーション設定ファイル 「kav4lms.conf」

Kaspersky Anti-Virus のパッケージには、アプリケーションの設定が保管された設定ファイル「kav4lms.conf」が含まれています。このセクションでは、設定ファイルの設定について、製品の標準インストール後のデフォルト値も含めて詳しく説明します。

設定ファイルは、アプリケーション機能の各側面を表すセクションで構成されます。各セクションの構文としては、最初の行に **[section_name]** 形式のセクションヘッダーがあり、その後にセクションパラメータの記述が続きます。

注記:

true|false に設定できるブーリアン値の場合、設定ファイルでは同等の値である **yes|no、y|n**、または **1|0** もサポートしています。

数値パラメータには、**UINT_MAX=4294967295** という上限があります。

警告!

説明の中で「必須」と記されているパラメータは、通常のアプリケーション動作にとって不可欠です。これらのパラメータは、必ず指定してください。そうしないと、Anti-Virus は機能しません。

A.1.1. [kav4lms:server.settings] セクション

[kav4lms:server.settings] セクションには、メインアプリケーションサービスに対するパラメータが含まれます:

RunAsUser - メインサービスの実行に使用される権限を持ったアカウントの名前

必須パラメータ

デフォルト値は **kluser** です

注記:

フィルタとメインサービスが同じコンピュータにインストールされている場合は、その両方のコンポーネントに対して **RunAsUser** パラメータが同じ値に設定されていることを確認してください。これにより、共有ファイルに正しくアクセスできるようになります。

RunAsGroup - メインサービスの実行に使用される権限を持ったグループの名前

必須パラメータ

デフォルト値は **klusers** です

ServiceSocket=inet:<port>@<ip-address> | local:<path_to_socket> - Kaspersky Anti-Virus フィルタサービスがアプリケーションのメインサービスと対話するために使用するローカルまたはネットワークソケット (メインサービス - フィルタ接続のエンドポイント)

警告！

このパラメータを変更する前に、メインアプリケーションサービスを停止する必要があります。変更後は、サービスを開始して新しい値を適用してください。

構文:

`ServiceSocket=inet:<port>@<ip-address>` - ネットワークソケットの場合

`ServiceSocket=local:<path_to_socket>` - ローカルソケットの場合

説明:

- **<port>** - 対話ポート
- **<ip-address>** - IP アドレス
- **<path_to_socket>** - ローカルソケットへのパス

必須パラメータ

デフォルト値は **local:/var/run/kav4lms/kavmd.sock** です

注記:

ローカルソケットを使用する場合は、フィルタサービスとメインアプリケーションサービスの両方に対して、ソケットファイルが配置されているディレクトリとそのファイル自体が読み取りおよび書き込みアクセス可能であることを確認してください。

ServiceSocketPerms - ローカルソケットを使用する場合の **ServiceSocket** の権限。ソケットの所有者は、パラメータの **RunAsUser:RunAsGroup** ペアによって定義されます

デフォルト値は **0600** です (パラメータ値が指定されていない場合に使用される)

AdminSocket - メインサービスを (たとえば、SNMP 経由で) 管理するために使用するローカルソケット。メインサービスは、管理コマンドで制御できます。また、メインサービスは、SNMP コンポーネントからの情報要求も処理できます。対話は、この特定のソケット上で行われます

警告！

このパラメータを変更する前に、メインアプリケーションサービスを停止する必要があります。変更後は、サービスを開始して新しい値を適用してください。

必須パラメータ

デフォルトのパラメータ値は `local:/var/run/kav4lms/kavmdctl.sock` です

警告！

この設定を選択する場合は、アプリケーションが実行されるユーザアカウントに対してのみソケットファイルとソケットフォルダが書き込みアクセス可能であることを確認してください。

AdminSocketPerms - **AdminSocket** の権限。ソケットの所有者は **RunAsUser:RunAsGroup** です

デフォルト値は **0600** です

MaxWatchdogRetries=0...UINT_MAX - 「watchdog」を使用して Kaspersky Anti-Virus を再起動する際の最大再試行回数。値 **-1** は、無制限の再試行回数に相当します。値を **0** にすると、watchdog は無効になります

デフォルト値は **10** です

MaxClientRequests=0...UINT_MAX - メインサービスが受け入れて処理するクライアント要求の最大数。パラメータが **0** の場合、要求数は無制限です

デフォルト値は **20** です

MaxScanRequests=0...UINT_MAX - メッセージのスキャン要求の最大数。パラメータが **0** の場合、要求数は無制限です

デフォルト値は **0** です

LicensedUsersDomains - Kaspersky Anti-Virus for Linux Mail Server のライセンス方式に従って保護する必要があるアカウントが含まれているドメインのリスト。このオプションは、特定の数のメールアドレスについてキーが発行されている場合にのみ使用できます。カンマで区切った複数の値を指定できます

デフォルト値は `localhost`、`localhost.localdomain` です

A.1.2. [kav4lms:server.log] セクション

[kav4lms:server.log] セクションには、メインサービスのログに対するパラメータが含まれません:

Options=<functionality_category>.<details_level> - ログに登録されたイベントのカテゴリ:

- **<functionality_category>** には、次の値を使用できます: **all**、**config**、**app**、**scan**、**cfilter**、**backup**、**notif**、**admin**、**smtpt** (79 ページのセクション 9.1 を参照)
- **<details_level>** には、次の値を使用できます: **debug**、**activity**、**info**、**warning**、**error**、**fatal** (79 ページのセクション 9.1 を参照)

カンマで区切った複数のレベルを指定できます

例:

```
Options = backup.all, config.error, \
scan.all, -scan.debug
Options = backup.all, config.E, \
scan.all, -scan.9
```

必須パラメータ

デフォルト値は **all**、**-all.debug** です

Destination=syslog:<name>@<category> | file:<path_to_file> - メインアプリケーションサービスの動作に関する情報が記録されるファイルへのパス:

- **syslog:<name>@<facility>**: レポートをシステムログに書き込みます。**<name>** ではアプリケーション名、**<facility>** では記録されるカテゴリが定義されます
- **file:<path_to_file>**: 指定したパスに配置されているファイルにレポートを書き込みます

必須パラメータ

デフォルト値は **syslog:kavmd@mail** です

Append=yes | no - 情報をログファイルに追加する方法を指定します:

- **yes** - 新しい情報を既存のファイルに追加します
- **no** - アプリケーションが起動するたびに新しいログファイルを作成します

デフォルト値は **yes** です

RotateRounds=0...UINT_MAX - ローテーション中に作成されるレポートファイルの数。
この数に達すると、アプリケーションは最も古いレポートファイルの上書きを開始します。
この数がゼロ以外の場合は、ローテーションが有効になります

デフォルト値は **10** です

RotateSize=1M - レポートファイルのサイズ (バイト単位)。このサイズに達すると、新しいレポートファイルが作成されます

デフォルト値は **1M** です

警告!

Append、**RotateRounds**、および **RotateSize** パラメータは、記録先がファイルの場合にのみ有効です。

A.1.3. [kav4lms:server.statistics] セクション

[kav4lms:server.statistics] セクションには、メインサービス統計値のパラメータが含まれません:

Options=none | all | messages | resources | viruses | filters | raw - ログ用のデータカテゴリ (82 ページのセクション 9.2 を参照)。複数のカテゴリをカンマ区切りで指定できます

例:

```
Options=none, raw
```

必須パラメータ

デフォルト値は **none** です

Format=xml | txt - 統計値のファイル形式を指定します

デフォルト値は **xml** です

Destination=file:<path_to_file> - メインサービスログの作成先。現行バージョンの Kaspersky Anti-Virus では、ファイル作成先のみサポートしています

デフォルト値は以下のとおりです:

file:/var/opt/kaspersky/kav4lms/stats/statistics.xml (Linux の場合)

file:/var/db/kaspersky/kav4lms/stats/statistics.xml (FreeBSD の場合)

RawDestination= file:<path_to_file> - 生の (またはメッセージごとの) 統計値の作成先。現行バージョンの Kaspersky Anti-Virus では、ファイル作成先のみサポートしています

必須パラメータ

デフォルト値は以下のとおりです:

file:/var/opt/kaspersky/kav4lms/stats/statistics.raw (Linux の場合)

file:/var/db/kaspersky/kav4lms/stats/statistics.raw (FreeBSD の場合)

A.1.4. [kav4lms:server.snmp] セクション

[kav4lms:server.snmp] セクションには、SNMP プロトコル経由でのアプリケーションとの対話を定義するパラメータが含まれます:

SNMPServices=config | statistics | admin | update | all | none - SNMP 上で読み取ることができるアプリケーション情報:

- **config**: アプリケーション設定ファイルの全セクションの設定に関する情報
- **statistics**: アプリケーション動作に関する要約統計情報
- **admin**: アプリケーションの実行時間に関連する情報 (起動時間、稼働時間など)
- **update**: 定義データベースの更新に関する情報 (最終更新日、データベース内のレコード数など)
- **all**: すべての統計情報とアプリケーションの設定に関するデータ
- **none**: SNMP 上での情報へのアクセスは無効になります

複数の値を 1 つのリストとして定義できます。各パラメータは別々の行に入力する必要があります

例:

```
SNMPServices=config
```

```
SNMPServices=admin
```

必須パラメータ

デフォルト値は **none** です

SNMPTraps=config | admin | update | all | none - SNMP Trap によって管理者への通知を誘発するイベントのリスト

- **config**: アプリケーション設定の変更時、または定義データベースの正常な更新時
- **admin**: アプリケーションが開始または停止するか、その動作で重大なエラーが発生した場合や、感染したオブジェクトが検出され、**AlertThreshold** パラメータで定義された状態が誘発された場合
- **update**: 結果にかかわらず、定義データベースの更新時
- **all**: 上記のいずれかのイベントが発生した場合
- **none**: SNMP Trap は無効になります

複数の値を 1 つのリストとして定義できます。各パラメータは別々の行に入力する必要があります

例:

```
SNMPTraps=config
```

```
SNMPTraps=admin
```

必須パラメータ

デフォルト値は **none** です

AlertThreshold=0...100 - 過去 1 時間内にスキャンされた全メッセージにおける感染メッセージの割合のしきい値。このしきい値を超えると、アプリケーションによって SNMP Trap が送信されます (**SNMPTraps** パラメータが **admin** に設定されている場合)

デフォルト値は **10** です

Socket - マスタエージェントとの対話に使用されるソケット。ローカルまたはネットワークソケットを使用できます

構文:

```
inet:<port>@<ip-address> - ネットワークソケットの場合
```

```
local:<path_to_socket> - ローカルソケットの場合
```

説明:

- **<port>** - 対話ポート
- **<ip-address>** - IP アドレス
- **<path_to_socket>** - ローカルソケットへのパス

注記:

ローカルソケットの場合は、「master」という名前のファイルを指定する必要があります。これは SNMP での名前付け制約です。したがって、絶対パスは、「master」ファイルの名前を含む **<path_to_socket>** として指定する必要があります。

デフォルト値は **inet:705@127.0.0.1** です

Timeout=0...UINT_MAX - マスタエージェントへ送信される要求のタイムアウト (秒単位)

デフォルト値は 5 です

Retries=0...UINT_MAX - マスタエージェントへ送信される要求の試行回数

デフォルト値は **10** です

警告!

実際の再試行回数は、指定した **Retries** 値と異なる場合があります。これは、「watchdog」の動作が原因で発生するものであり、問題はありません。

PingInterval=0...UINT_MAX - 接続に失敗した場合にサブエージェントがマスタエージェントへの接続を試みる時間間隔 (秒単位)

デフォルト値は **30** です

A.1.5. [kav4lms:server.notifications] セクション

[kav4lms:server.notifications] セクションには、通知オプションが含まれます：

ProductAdmins - Kaspersky Anti-Virus 管理者のメールアドレス。複数のアドレスをカンマ区切りで指定できます

デフォルト値は **postmaster** です

ProductNotify=fault | update | license | all | none - 指定されたイベントの発生時に Kaspersky Anti-Virus の管理者に通知します：

- **fault** - 重大なエラー
- **update** - 定義データベース更新の結果
- **license** - 製品キーの有効期限、および製品キーにおけるライセンス制約を超過している状況
- **all** - すべてのイベント
- **none** - 通知は無効になります

複数の値をカンマ区切りで指定できます

必須パラメータ

デフォルト値は **all** です

Subject - Subject フィールドに追加される標準通知のヘッダー

デフォルト値は **Anti-virus notification message** です

Charset - 送信される通知で使用される文字セット

デフォルト値は **us-ascii** です

TransferEncoding - 通知エンコーディングアルゴリズムの値。デフォルト値は **7bit** です

NotifierRelay - 通知の MTA アドレスを指定します

構文：

```
NotifierRelay=<protocol>:<host>:<port>
```

デフォルト値は **smtp:127.0.0.1:25** です

NotifierQueue - 通知の MTA がキューと管理ファイルを保管するディレクトリ

デフォルト値は以下のとおりです：

/var/opt/kaspersky/kav4lms/nqueue/ (Linux の場合)

/var/db/kaspersky/kav4lms/nqueue/ (FreeBSD の場合)

NotifierTimeout=0...UINT_MAX - 通知送信のタイムアウト (秒単位)。デフォルト値は **5** です

NotifierPersistence=yes | no - 通知の MTA への接続を持続するかどうかを指定します

Templates - 製品管理者の通知用テンプレートが含まれているディレクトリ

デフォルト値は以下のとおりです:

/etc/opt/kaspersky/kav4lms/templates-admin/en (Linux の場合)、

/usr/local/etc/kaspersky/kav4lms/templates-admin/en (FreeBSD の場合)

A.1.6. [kav4lms:filter.settings] セクション

[kav4lms:filter.settings] セクションには、Kaspersky Anti-Virus のフィルタサービスに対するパラメータが含まれます:

RunAsUser - フィルタサービスの実行に使用される権限を持ったアカウントの名前

必須パラメータ

デフォルト値は **kluser** です

注記:

フィルタとメインサービスが同じコンピュータにインストールされている場合は、その両方のコンポーネントに対して **RunAsUser** パラメータが同じ値に設定されていることを確認してください。これにより、共有ファイルに正しくアクセスできるようになります。

RunAsGroup - フィルタサービスの実行に使用される権限を持ったグループの名前

必須パラメータ

デフォルト値は **klusers** です

FilterSocket=inet:<port>@<ip-address> | local:<path_to_socket> - Kaspersky Anti-Virus フィルタサービスがアプリケーションのメインサービスと対話するために使用するローカルまたはネットワークソケット (メインサービス - フィルタ接続のエンドポイント)

警告!

このパラメータを変更する前に、フィルタサービスを停止する必要があります。変更後、サービスを開始して新しい値を適用してください。

構文:

FilterSocket=inet:<port>@<ip-address> - ネットワークソケットの場合

FilterSocket=local:<path_to_socket> - ローカルソケットの場合

説明:

- **<port>** - 対話ポート
- **<ip-address>** - IP アドレス

- **<path_to_socket>** - ローカルソケットへのパス

必須パラメータ

デフォルト値は **inet:10025@127.0.0.1** です

注記:

ローカルソケットを使用する場合は、フィルタサービスとメインアプリケーションサービスの両方に対して、ソケットファイルが配置されているディレクトリとそのファイル自体が読み取りおよび書き込みアクセス可能であることを確認してください。

FilterSocketPerms - ローカル Unix ソケットを使用する場合の **FilterSocket** の権限。ソケットの所有者は **RunAsUser:RunAsGroup** です

デフォルト値は **0600** です

ServiceSocket=inet:<port>@<ip-address> | local:<path_to_socket> - Kaspersky Anti-Virus フィルタサービスがアプリケーションのメインサービスと対話するために使用するローカルまたはネットワークソケット (メインサービス - フィルタ接続のエンドポイント)。レコード形式は **FilterSocket** と同じです

警告!

このパラメータを変更する前に、フィルタサービスを停止する必要があります。変更後、サービスを開始して新しい値を適用してください。

必須パラメータ

デフォルト値は **local:/var/run/kav4lms/kavmd.sock** です

AdminSocket=local:<path_to_socket>- フィルタサービスを (たとえば、SNMP 経由で) 管理するために使用するローカルソケット。フィルタサービスは、管理コマンドで制御できます。対話は、この特定のソケット上で行われます

警告!

このパラメータを変更する前に、フィルタサービスを停止する必要があります。変更後、サービスを開始して新しい値を適用してください。

必須パラメータ

デフォルト値は **local:/var/run/kav4lms/kavmdctl.sock** です

警告!

パラメータの設定時には、アプリケーションの実行に使用されるアカウントだけにソケットファイルおよびソケットディレクトリの書き込み権限があることを確認してください。

AdminSocketPerms=0600 - **AdminSocket** の権限。ソケットの所有者は **RunAsUser:RunAsGroup** です

ForwardSocket=inet:<port>@<ip-address> | local:<path_to_socket> - Kaspersky Anti-Virus フィルタが MTA と対話するために使用するローカルまたはネットワークソケット (アプリケーション - MTA 接続のエンドポイント)

警告！

このパラメータを変更する前に、フィルタサービスを停止する必要があります。変更後、サービスを開始して新しい値を適用してください。

レコード形式は **FilterSocket** と同じです

必須パラメータ

デフォルト値は **inet:10026@127.0.0.1** です

注記:

ForwardSocket パラメータは、Postfix および Exim との統合に使用されません。

FilterTimeout=0...UINT_MAX - フィルタサービスと MTA の間の通信タイムアウト (秒単位)。ここで指定した時間中にデータ/コマンドが送信されないと、Kaspersky Anti-Virus は MTA への接続を閉じます

デフォルト値は **600** です

FilterThreads=0...UINT_MAX - MTA 要求を待機するためにフィルタサービスが生成するスレッドの数

デフォルト値は **10** です

MaxMilterThreads=0...UINT_MAX - Milter ライブラリによって同時に実行されるスレッドの最大数。値を 0 に設定すると、スレッドの数は無制限になります

デフォルト値は **0** です

警告！

Sendmail の場合にのみ適用してください。

A.1.7. [kav4lms:filter.log] セクション

[kav4lms:filter.log] セクションには、サービスのログに対するパラメータが含まれます:

Options=<functionality_category>.<details_level> - ログに登録されたフィルタイベントのカテゴリ:

- **<functionality_category>** には以下の値を使用できます: **all**、**config**、**app**、**scan**、**cfilter**、**backup**、**notif**、**admin**、**smtp** (79 ページのセクション 9.1 を参照)
- **<details_level>** には、以下の値を使用できます: **debug**、**activity**、**info**、**warning**、**error**、**fatal** (79 ページのセクション 9.1 を参照)

カンマで区切った複数のレベルを指定できます

必須パラメータ

デフォルト値は **all,-all.debug** です

Destination=syslog:<name>@<category> | file:<path_to_file> - フィルタサービスの動作に関する情報が記録されるファイルへのパス:

- **syslog:<name>@<facility>** - レポートをシステムログに書き込みます。**<name>** ではアプリケーション名、**<facility>** では記録されるカテゴリが定義されます
- **file:<path_to_file>** - 指定したパスに配置されているファイルにレポートを書き込みます

必須パラメータ

デフォルト値は **syslog:kav4lms-filters@mail** です

Append=yes | no - フィルタ動作に関する情報をログファイルに追加する方法を指定します:

- **yes** - 新しい情報を既存のファイルに追加します
- **no** - アプリケーションが起動するたびに新しいログファイルを作成します

デフォルト値は **yes** です

RotateRounds=0...UINT_MAX- ローテーション中に作成されるレポートファイルの数。この数に達すると、アプリケーションは最も古いレポートファイルの上書きを開始します。この数がゼロ以外の場合は、ローテーションが有効になります

デフォルト値は **10** です

RotateSize=1M - レポートファイルのサイズ (バイト単位)。このサイズに達すると、新しいレポートファイルが作成されます

デフォルト値は **1M** です

警告!

Append、**RotateRounds**、および **RotateSize** パラメータは、記録先がファイルの場合にのみ有効です。

A.1.8. [kav4lms:groups] セクション

[kav4lms:groups] セクションには、グループの設定ファイルへの参照が含まれます:

_includes=<path_to_directory> - グループの設定ファイルが保管されているディレクトリへのパス。ディレクトリパスは、アプリケーションのメイン設定ファイルの場所を基準とした相対パスでなければなりません

必須パラメータ

デフォルト値は **groups.d/** です

A.1.9. [path] セクション

[path] セクションには、重要なディレクトリへのパスを定義するパラメータが含まれます。

BasesPath - 定義データベースを含むディレクトリへの絶対パス

必須パラメータ

デフォルト値は、**/var/opt/kaspersky/kav4lms/bases** (Linux の場合) または **/var/db/kaspersky/kav4lms/bases** (FreeBSD の場合) です

LicensePath - キーが保管されているディレクトリへの絶対パス

デフォルト値は、**/var/opt/kaspersky/kav4lms/bases** (Linux の場合) または **/var/db/kaspersky/kav4lms/bases** (FreeBSD の場合) です

PidPath - メインアプリケーションサービス PID ファイルへのパス

必須パラメータ

デフォルト値は **/var/run/kav4lms/** です

TempPath - 一時ファイルを含むディレクトリへのパス。アプリケーションは、指定されたパスに **.kav4lms-<id>** サブディレクトリを作成します

必須パラメータ

デフォルト値は `/var/tmp/` です

iCheckerDBFile - iChecker™ データベースへのパス

必須パラメータ

デフォルト値は、`/var/opt/kaspersky/kav4lms/iChecker.db` (Linux の場合)
または `/var/db/kaspersky/kav4lms/iChecker.db` (FreeBSD の場合) です

A.1.10. [locale] セクション

[locale] セクションには、レポートと統計に日時を表示するためのオプションが含まれます。

DateFormat - レポートに表示される日付形式

必須パラメータ

デフォルト値は `%d-%m-%Y` です

TimeFormat - レポートに表示される時刻形式

必須パラメータ

デフォルト値は `%H:%M:%S` です

注記:

時刻の形式は 12 時間形式 (am, pm) に変更できます: `%I:%M:%S %P`

Strings - アプリケーションが使用する文字列定数を含んだファイルへのパス。ディレクトリパスは、アプリケーションのメイン設定ファイルの場所を基準とした相対パスでなければなりません

必須パラメータ

デフォルト値は `locale.d/strings.en` です

A.1.11. [options] セクション

[options] セクションには、他のグループに入らない各種アプリケーションパラメータが含まれません:

- **User** - アプリケーションコンポーネントの実行に使用されるシステムアカウント
必須パラメータ
デフォルト値は **kluser** です
- **Group** - アプリケーションコンポーネントの実行に使用されるシステムグループ
必須パラメータ
デフォルト値は **klusers** です

A.1.12. [updater.path] セクション

[updater.path] セクションでは、更新のために使用するディレクトリへのパスが定義されます。

BackUpPath=/var/opt/kaspersky/kav4lms/bases.backup/ - 定義データベースのバックアップストレージ用ディレクトリへの絶対パス

A.1.13. [updater.options] セクション

[updater.options] セクションには、更新オプションを定義するパラメータが含まれます。

UpdateComponentsList - 更新されるコンポーネントのリスト

デフォルト値は **AVS、AVS_OLD、CORE、Updater、BLST** です

RetranslateComponentsList - ネットワークディレクトリに更新が保存されるコンポーネントのリスト

このパラメータ値が空白 (デフォルト) の場合は、**UpdateComponentsList** パラメータ値が使用されます。

KeepSilent=yes | no - 更新に関するレポートをコンソールに表示するかどうかを定義します。**yes** に設定すると、レポートはコンソールに送られません

デフォルト値は **no** です

UseUpdateServerUrl=yes | no - **UpdateServerUrl** パラメータによって更新元として定義されたカスペルスキーのアップデートサーバの URL を使用するかどうかを定義します

デフォルト値は **no** です

UpdateServerUrl=http://url|ftp://url|/local_path/ - 更新元として使用するサーバのアドレス

デフォルトのパラメータ値は空白です

UseUpdateServerUrlOnly=yes|no - **UpdateServerUrl** で指定された URL だけを使用してデータベースを更新するかどうかを定義します。このオプションを **no** に設定すると、**UpdateServerUrl** アドレスからの更新に失敗するたびに、アプリケーションはアップデートサーバのリストから別のアドレスを使用します

デフォルト値は **no** です

RegionSettings - 最も近いカスペルスキーのアップデートサーバから定義データベースを更新するために使用される顧客の地域を定義します

デフォルト値は **ru** です

ConnectTimeout - アプリケーションが更新元への接続を試みる時間間隔 (秒単位)

デフォルト値は **30** です

ProxyAddress - プロキシサーバの IP アドレス (インターネット接続にプロキシサーバが必要な場合)

デフォルトでは、値は設定されません

UseProxy=yes|no - プロキシサーバを使用して、いずれかのアップデートサーバに接続します。このパラメータが **no** の場合は、プロキシサーバは使用されません。このパラメータが **yes** の場合は、**ProxyAddress** パラメータで定義されたプロキシサーバアドレスが使用されます

デフォルト値は **no** です

PassiveFtp=yes|no - FTP で更新をダウンロードするときにパッシブ FTP モードを使用するかどうか

デフォルト値は **yes** です

Index=u0607g.xml - カスペルスキーのアップデートサーバ上で更新のセットを選択するために使用する、更新処理システムのメインインデックスを含むファイル。この値は変更しないことをお勧めします

IndexRelativeServerPath=index/6 - 更新処理システムのメインインデックスを含むファイルへのパス。これは、アプリケーションのメイン設定ファイルの場所を基準とした相対パスでなければなりません。この値は変更しないことをお勧めします

A.1.14. [updater.report] セクション

[updater.report] セクションには、更新レポートパラメータが含まれます。

Append=yes|no - kav4lms-keepup2date コンポーネントの動作を記録する方法を決定します:

- **yes** - 新しい情報を既存のファイルに追加します
- **no** - コンポーネントが起動するたびに新しいログファイルを作成します。ログファイルには、最後の更新の結果に関する情報だけが含まれます

デフォルト値は **no** です

ReportFileName - kav4lms-keepup2date レポートファイルの名前

デフォルト値は **/var/log/kaspersky/kav4lms/keepup2date.log** です

ReportLevel=0|1|2|3|4|9 - 更新レポート内の詳細レベル (**0**: 致命的エラー、**1**: エラー、**2**: 警告、**3**: 通知、**4**: アクティビティ、**9**: デバッグ)。デフォルト値は **3** です

A.1.15. [updater.actions] セクション

[updater.actions] セクションには、特定の keepup2date イベント時に実行される操作を定義するパラメータが含まれます。

OnAny - イベントが発生するたびに実行するコマンドを指定します。デフォルトでは、他のアプリケーションコンポーネントはそのイベントについて通知されません

デフォルト値は **/opt/kaspersky/kav4lms/bin/kav4lms-cmd -m □update -e %EVENT_NAME%** (Linux の場合)、
/usr/local/bin/kav4lms-cmd -m update -e %EVENT_NAME% (FreeBSD の場合) です

OnStarted - kav4lms-keepup2date コンポーネントの起動時に実行するコマンドを指定します

デフォルトでは、この値は空白です

OnUpdated - 更新の正常終了時に実行するコマンドを指定します

デフォルト値を使用すると、アプリケーションが再起動します -

/opt/kaspersky/kav4lms/bin/kav4lms-cmd -x bases (Linux の場合)、
/var/db/kaspersky/kav4lms/bin/kav4lms-cmd -x bases (FreeBSD の場合)

OnRetranslated - 定義データベースが置かれるディレクトリにネットワークディレクトリからデータベース更新が正常にダウンロードされた場合に実行するコマンド

デフォルトでは、この値は空白です

OnNotUpdated - 更新が実行されなかった場合に実行するコマンドを指定します

デフォルトでは、この値は空白です

OnFailed - 更新が失敗した場合に実行するコマンドを指定します

デフォルトでは、この値は空白です

OnRolledBack - ロールバックの発生時に実行するコマンドを指定します

デフォルトでは、この値は空白です

OnBasesCheck - 更新後に実行して定義データベースを検証するためのコマンドを指定します。デフォルトでは、avbasestest ユーティリティを使用して定義データベースの完全性をチェックします。このユーティリティは、更新元からダウンロードされて一時ディレクトリに保管された更新をチェックします。更新が破損していない場合は、一時的な場所から定義データベースを保管しているディレクトリにコピーされます

注記:

avbasestest ユーティリティは自動的に起動するため、ユーザが関与する必要はありません。

デフォルト値は、

**/opt/kaspersky/kav4lms/lib/bin/avbasestest %TEMP_BASES_PATH%
%BASES_PATH%** (Linux の場合)、

**/usr/local/libexec/kaspersky/kav4lms/avbasestest %TEMP_BASES_PATH%
%BASES_PATH%** (FreeBSD の場合) です

注記:

avbasestest の操作では、以下のマクロをサポートしています:

- **%EVENT_NAME%** - このコマンドを誘発したイベントの名前;
- **%BASES_PATH%** - 既存のデータベースへのパス (該当する場合)
- **%TEMP_BASES_PATH%** - データベースが更新されている一時ディレクトリへのパス (該当する場合)
- **%AVS_UPDATE_DATE%** - イベントの日付 (**mm:dd:yyyy hh:mm:ss** 形式)

A.1.16. [scanner.display] セクション

[**scanner.display**] セクションには、kav4lms-kavscanner レポートを画面に出力するための設定が含まれます:

ShowContainerResultOnly=true|false - アーカイブスキャンの結果を画面に表示する場合のモード。簡単な形式の結果を表示するには、この設定に **true** を割り当てます。デフォルトでは、拡張形式のメッセージを使用します

必須パラメータ

デフォルト値は **false** です

ShowObjectResultOnly=true|false - 単体オブジェクトのスキャン結果を画面に表示する場合のモード。簡単な形式の結果を表示するには、この設定に **true** を割り当てます。デフォルトでは、拡張形式のメッセージを使用します

必須パラメータ

デフォルト値は **false** です

ShowOK=true|false - 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 **false** を割り当てます

必須パラメータ

デフォルト値は **true** です

ShowProgress=true|false - 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 **false** を割り当てます

必須パラメータ

デフォルト値は **true** です

A.1.17. [scanner.options] セクション

[**scanner.options**] セクションには、kav4lms-kavscanner コンポーネントの設定が含まれます:

ExcludeDirs=mask1:mask2:...:maskN - スキャン対象から除外されるディレクトリのマスク。これらは、標準シェルマスクとして定義されます

デフォルト値は **/dev:/udev:/proc:/sys** です

ExcludeMask=mask1:mask2:...:maskN - スキャン対象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。マスクは、標準シェルマスクとして定義されます

デフォルト値は定義されていません

Packed=true|false - 圧縮オブジェクトのスキャンモード。スキャンを無効にするには、このパラメータを **false** に設定します

必須パラメータ

デフォルト値は **true** です

Archives=true|false - 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 **false** を割り当てます

必須パラメータ。

デフォルト値は **true** です

Cure=true|false - 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 **true** を割り当てます

必須パラメータ

デフォルト値は **false** です

Heuristic=true|false - 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 **false** を割り当てます

必須パラメータ

デフォルト値は **true** です

LocalFS=true|false - 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 **true** を割り当てます

必須パラメータ

デフォルト値は **false** です

MailBases=true|false - 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 **false** を割り当てます

必須パラメータ

デフォルト値は **true** です

MailPlain=true|false - 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 **false** を割り当てます

必須パラメータ

デフォルト値は **true** です

Packed=true | false - 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 **false** を割り当てます

必須パラメータ

デフォルト値は **true** です

Recursion=true | false - アンチ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 **false** を割り当てます

必須パラメータ

デフォルト値は **true** です

SelfExtArchives=true | false - 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場合は (**Archives=yes**)、**SelfExtArchives** に **false** 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

必須パラメータ

デフォルト値は **true** です

iChecker=true | false - アンチ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 **false** を割り当てます

デフォルト値は **true** です

MaxLoadAvg - CPU の最大負荷。この値を超えると、kav4lms-kavscanner コンポーネントは動作を停止します

デフォルトでは、この値は空白です

UseAVbasesSet=standard | extended - スキャン中にアプリケーションが使用する定義データベースのセット。 **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プログラムなど) の記述が含まれます

デフォルト値は **standard** です

FollowSymlinks=true | false - 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 **true** 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り、対応するアドレスに配置されているオブジェクトをチェックします。このモードを無効にするには、パラメータを **false** に設定します

デフォルト値は **true** です

A.1.18. [scanner.report] セクション

[scanner.report] セクションには、kav4lms-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=true|false - ファイルシステムのアンチウイルススキャン結果に関するレポートを含むファイルに新しいメッセージを追加するかどうか:

- **true** - 新しいメッセージを既存のファイルに追加します
- **false** - アプリケーションが起動するたびに新しいログファイルを作成します

必須パラメータ

デフォルト値は **true** です

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

デフォルト値は **/var/log/kaspersky/kav4lms/kavscanner.log** です

ReportLevel=0|1|2|3|4|9 - レポートの詳細レベル (**0**: 致命的エラー、**1**: エラー、**2**: 警告、**3**: 通知、**4**: アクティビティ、**9**: デバッグ)

必須パラメータ

デフォルト値は **4** です

ShowOK=true|false - 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 **false** を割り当てます

必須パラメータ

デフォルト値は **true** です

ShowContainerResultOnly=true|false - アーカイブスキャンの結果を表示する場合のモード。簡単なレポートを表示するには、この設定に **true** を割り当てます。デフォルトでは、拡張形式のメッセージを使用します

必須パラメータ

デフォルト値は **false** です

ShowObjectResultOnly=true|false - 単体オブジェクトのスキャン結果を表示する場合のモード。簡単な形式で表示するには、この設定に **yes** を割り当てます。デフォルトでは、拡張形式のメッセージを使用します

必須パラメータ

デフォルト値は **false** です

A.1.19. [scanner.container] セクション

[scanner.container] セクションには、サーバのファイルシステムのアンチウイルス対策中にアーカイブに対して実行される操作を決定する設定が含まれます。

OnInfected=action - 感染オブジェクトを検知した場合に実行される処理。感染ファイルの感染駆除モードが有効になっている場合は、感染駆除できなかったオブジェクトに対して、指定の処理が実行されます

デフォルトでは、この値は空白です

OnSuspicion=action - 脅威と類似しているが Kaspersky Lab では未確認の疑わしいオブジェクトをアプリケーションが検知した場合に実行される処理

デフォルトでは、この値は空白です

OnWarning=action - 既知の脅威と類似するファイルをアプリケーションが検知した場合に実行される処理

デフォルトでは、この値は空白です

OnCured=action - アプリケーションが感染ファイルを検知して正常に感染駆除した場合に実行される処理

デフォルトでは、この値は空白です

OnProtected=action - パスワード保護されたオブジェクトをアプリケーションが検知した場合に実行される処理。このようなオブジェクトはスキャンできません

デフォルトでは、この値は空白です

OnCorrupted=action - アプリケーションが破損ファイルを検知した場合に実行される処理

デフォルトでは、この値は空白です

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

デフォルトでは、この値は空白です

action パラメータの構文は 2 つの部分で構成され、処理と追加パラメータがスペースで区切られます。追加パラメータの値は、二重引用符で囲んで指定する必要があります。

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> - <parameter>` 変数で定義された外部コマンドを実行する

アーカイブに対する **exec** 処理の追加パラメータとして、以下のマクロを使用できます：

- `%VIRUSNAME%` - 検知された脅威またはエラーの名前
- `%LIST%` - ファイル名またはアーカイブ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。レコードの形式は **<virus name> [<file name>** です
- `%FULLPATH%` - アーカイブへの絶対パス
- `%FILENAME%` - パスを伴わないファイル名
- `%CONTAINERTYPE%` - アーカイブのタイプ (文字列で指定)

A.1.20. [scanner.object] セクション

[scanner.object] セクションには、コンピュータファイルシステムのアンチウイルス対策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する設定が含まれます。

OnInfected=action - 感染オブジェクトを検知した場合に実行される処理。感染ファイルの感染駆除モードが有効になっている場合は、感染駆除できなかったオブジェクトに対して指定の処理が実行されます

デフォルトでは、この値は空白です

OnSuspicion=action - 脅威と類似しているが Kaspersky Lab では未確認の疑わしいオブジェクトをアプリケーションが検知した場合に実行される処理

デフォルトでは、この値は空白です

OnWarning=action - 既知の脅威と類似するファイルをアプリケーションが検知した場合に実行される処理

デフォルトでは、この値は空白です

OnCured=action - アプリケーションが感染ファイルを検知して正常に感染駆除した場合に実行される処理

デフォルトでは、この値は空白です

OnProtected=action - パスワード保護されたオブジェクトをアプリケーションが検知した場合に実行される処理。このようなオブジェクトはスキャンできません

デフォルトでは、この値は空白です

OnCorrupted=action - アプリケーションが破損ファイルを検知した場合に実行される処理

デフォルトでは、この値は空白です

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

デフォルトでは、この値は空白です

action パラメータの構文は、**[scanner.container]** セクションの **action** パラメータと同じです (119 ページのセクション A.1.19 を参照)。

ファイルに対する **exec** 処理の追加パラメータとして、以下のマクロを使用できます：

- %VIRUSNAME% - 検知された脅威またはエラーの名前
- %LIST% - 感染ファイル、疑わしいファイル、または破損ファイルの名前。レコードの形式は **<virus name> [] <file name>** です
- %FULLPATH% - ファイルへの絶対パス
- %FILENAME% - パスを伴わないファイル名

A.1.21. [scanner.path] セクション

[scanner.path] セクションには、kav4lms-kavscanner コンポーネントが機能するために必要なファイルへのパスを設定するパラメータが含まれます。

BackupPath= path - コンポーネントによってスキャンされ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絶対パス

デフォルトでは、この値は空白です

A.2. グループ設定ファイル

この付録では、default.conf 設定ファイルの各セクションについて詳しく説明します。default.conf 設定ファイルでは、メッセージの処理に使用される設定の **Default** グループが定義されます。

Default グループに対して指定されたパラメータは、以下の場合に使用されます：

- グループが作成されていない
- 既存のどのグループでもメッセージの送信者と受信者が見つからない
- グループ内のパラメータ値が定義されていない

警告！

Default グループの default.conf 設定ファイルに基づいてグループ設定ファイルを作成する場合は、設定ファイルのセクションタイトルに入力されているグループ名を必ず変更してください。

A.2.1. [kav4lms:groups.<group_name>.definition] セクション

[kav4lms:groups.<group_name>.definition] セクションには、グループ識別パラメータが含まれます:

Priority - グループ優先度。送信者 (受信者) に従ってメッセージが複数のグループに属する場合、そのメッセージは優先度が最も高いグループルールを使用して処理されます。任意の自然数をパラメータ値として指定できます。同じ優先度のグループ、および優先度が **0** のグループは使用できません

必須パラメータ

Default グループのパラメータ値は **0** です

Senders - メール送信者アドレスのリスト。各アドレスは別々の行で指定する必要があります。マスクと正規表現がサポートされています。このオプションを定義しないと、値は ***@*** (すべてのアドレス) であると見なされます

例:

```
Senders=user1@mycompany.com
Senders=reporter*@mycompany.com
Senders=re:office@.*\example\com
```

Default グループのパラメータ値は定義されていません

Recipients - メール受信者アドレスのリスト。各アドレスは別々の行で指定する必要があります。マスクと正規表現がサポートされています。このオプションを定義しないと、値は ***@*** (すべてのアドレス) であると見なされます

例:

```
Recipients=user2@mycompany.com
Recipients=reporter*@mycompany.com
Recipients=re:office\d+@central\mydomain\com
```

Default グループのパラメータ値は定義されていません

警告!

少なくとも 1 つの **Senders** または **Recipients** パラメータを指定する必要があります。

A.2.2. [kav4lms:groups.<group_name>.settings] セクション

[kav4lms:groups.<group_name>.settings] セクションには、メッセージスキャンポリシーと処理済みメッセージへの特殊情報フィールドの追加を定義するパラメータが含まれます。

Check=anti-virus | content-filter | all | none - グループに対するセキュリティサービス

必須パラメータ

Default グループのパラメータは **all** です

ScanPolicy=message | combined - メッセージの解析方法を定義するメールスキャンポリシー

必須パラメータ

Default グループのパラメータ値は **message** です

ScanArchives=yes | no - アーカイブのスキャン。このモードを無効にするには、パラメータを **no** に設定します

Default グループのパラメータ値は **yes** です

ScanPacked=yes | no - 圧縮された実行ファイルのスキャン。このモードを無効にするには、パラメータを **no** に設定します

Default グループのパラメータ値は **yes** です

UseAVBasesSet=standard | extended - スキャン中にアプリケーションが使用する定義データベースのセット。**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、リモート管理プログラム、ネットワークスキャナ、ウイルスシミュレータなど）の記述が含まれます

Default グループのパラメータ値は **standard** です

UseCodeAnalyzer=yes | no - ヒューリスティックコードアナライザを使用して悪意のあるプログラム、ウイルス改変、および未知のウイルスを検出するスキャン。このモードを無効にするには、パラメータを **no** に設定します。

Default グループのパラメータ値は **yes** です

MaxScanTime - アプリケーションが単体オブジェクト（メッセージまたはメッセージオブジェクト）のスキャンに費やせる最大時間（秒単位）。この値を超えると、アプリケーションはエラーを返します

Default グループのパラメータ値は **30** です

注記:

場合によっては、特定のメッセージの合計スキャン時間が **MaxScanTime** パラメータの値を超えてもエラーが発行されないことがあります。これは、**combined** タイプのスキャンポリシーを選択している場合に発生します。その場合、メッセージスキャンの合計継続時間は、オブジェクトとしてのメッセージのスキャンとパーツごとのスキャンの総計です。

MaxScanDepth=0...UINT_MAX - 単一メッセージ内で許可される MIME オブジェクトの最大ネストレベル。この値を超えると、アプリケーションはエラーを返します。値 **0** は、ネストが無制限に許可されることを意味します。

Default グループのパラメータ値は **10** です

MIMEEncodingHeuristics=yes|no - RFC 標準に準拠していない MIME オブジェクトを解析するためのモード。

デフォルトでは、アプリケーションフィルタは RFC 準拠のメッセージだけをスキャン用に転送します。**MIMEEncodingHeuristics** が **yes** に設定されていると、非準拠メッセージはヒューリスティックアルゴリズムを使用して解析され、デコードに成功した場合はスキャン用に転送されます。メッセージのデコードに失敗した場合や **MIMEEncodingHeuristics** が **no** に設定されている場合は、そのようなメッセージはスキャン用に転送されません

Default グループのパラメータ値は **no** です

注記:

このパラメータを有効にすると、スキャンが遅くなる可能性があります。

AddXHeaders=none|message|parts|all - メッセージスキャン結果を含む情報ヘッダーを追加するための指示 (詳細については、93 ページのセクション 10.4 を参照)。

必須パラメータ

Default グループのパラメータ値は **message** です

AddDisclaimer=yes|no - 処理済みまたは生成済みの各メッセージに免責テキストを追加します。このテキストは、disclaimer テンプレートの編集によってカスタマイズすることができます。免責テキストはテキスト部分としてメッセージの最後に追加されます。免責テキストによって元のメッセージの内容が影響を受けたり変更されたりすることはありません。

Default グループのパラメータ値は **no** です

UsePlaceholderNotice=yes|no - 削除されたオブジェクトに関する通知を付加します

Default グループのパラメータ値は **yes** です

RejectReply - 拒否されたメッセージに関する通知のヘッダー。qmail との製品統合の場合は、このオプションは使用されません

Default グループのパラメータ値:
Message rejected because it contains malware

A.2.3. [kav4lms:groups.<group_name>.actions] セクション

[kav4lms:groups.<group_name>.actions] には、アンチウイルススキャン後のメールオブジェクトの処理方法を決定するオプションが含まれます:

InfectedAction=warn | drop | reject | cure | delete | skip - 感染オブジェクトに適用されるデフォルトの操作

必須パラメータ

Default グループのパラメータ値は **skip** です

SuspiciousAction=warn | drop | reject | delete | skip - 未知のマルウェアに感染している疑いがあるオブジェクトに適用されるデフォルトの操作

必須パラメータ

Default グループのパラメータ値は **skip** です

ProtectedAction=warn | drop | reject | skip | delete - 脅威があるかどうかをスキャンできなかったパスワード保護オブジェクトに適用される操作

必須パラメータ

Default グループのパラメータ値は **skip** です

ErrorAction=warn | skip | delete - エラーのためにスキャンできなかった破損オブジェクトに適用される操作

必須パラメータ

Default グループのパラメータ値は **skip** です

VirusNameAction= warn | drop | reject - **VirusNameList** パラメータにリストアップされたウイルスに感染しているメッセージまたはオブジェクトに適用される操作

必須パラメータ

Default グループのパラメータ値は **skip** です

FilteredMimeAction=skip | delete | drop | reject | warn - **IncludeMime** パラメータで定義された MIME タイプの添付ファイルに適用される操作

Default グループのパラメータ値は **skip** です

FilteredNameAction=skip | delete | drop | reject | rename | warn -
IncludeName パラメータマスクによって定義された名前の付いた添付ファイルに適用される操作

Default グループのパラメータ値は **skip** です

FilteredSizeAction=skip | delete | drop | reject | warn - 添付ファイルのサイズが
IncludeSize パラメータで設定された値に一致する場合にその添付ファイルに適用される操作

Default グループのパラメータ値は **skip** です

A.2.4. [kav4lms:groups.<group_name>.contentfiltering] セクション

[kav4lms:groups.<group_name>.contentfiltering] セクションでは、メッセージフィルタリングのルールが定義されます:

IncludeMime - MIME タイプによるフィルタリングのマスクを定義します。MIME タイプが指定のマスクと一致し、スキャンからの除外 (**ExcludeMime** パラメータ) の定義に使用されるマスクと一致しない場合、オブジェクトはフィルタリングされます

複数の値を 1 つのリストとして定義できます。各パラメータは別々の行に入力する必要があります。ワイルドカード («*」、「?」) と正規表現がサポートされています

例:

```
IncludeMime=application/octet-stream
IncludeMime=application/vnd.*
IncludeMime=re:image/.*
IncludeMime=re:multipart/(encrypted|signed)
```

パラメータ値が指定されていない場合や空白の場合は、MIME タイプによるフィルタリングは実行されません

Default グループの場合、パラメータ値は空白です

ExcludeMime - フィルタリングから除外されるオブジェクトの MIME タイプマスクを定義します。これらのマスクに一致しないタイプのオブジェクトはスキップされます

ExcludeMime リストが指定され、**IncludeMime** が指定されていない場合は、**ExcludeMime** リストに属さないマスクがフィルタリングされます

複数の値を 1 つのリストとして定義できます。各パラメータは別々の行に入力する必要があります。ワイルドカード («*」、「?」) と正規表現がサポートされています

例:

```
ExcludeMime=application/octet-stream
```

```
ExcludeMime=application/vnd.*
ExcludeMime=re:image/.*
ExcludeMime=re:multipart/(encrypted|signed)
```

Default グループの場合、パラメータ値は空白です

IncludeName - 名前によるフィルタリングのマスクを定義します。オブジェクトの名前が指定のマスクと一致し、スキャンからの除外 (**ExcludeName** パラメータ) の定義に使用されるマスクと一致しない場合、アプリケーションはオブジェクトをフィルタリングします

パラメータ値が指定されていない場合や空白の場合は、添付ファイル名によるフィルタリングは実行されません

複数の値を 1 つのリストとして定義できます。各パラメータは別々の行に入力する必要があります。ワイルドカード («*」、「?」) と正規表現がサポートされています

例:

```
IncludeName=*accounting*
IncludeName=re:.*\.(doc|xls|ppt)
IncludeName=re:.*\.(pif|com|exe)
```

Default グループの場合、パラメータ値は空白です

ExcludeName - フィルタリングから除外されるオブジェクトのマスクを定義します。アプリケーションは、これらのマスクに一致するオブジェクトをスキップします

ExcludeName が指定され、**IncludeName** が指定されていない場合、**ExcludeName** リストに属さないマスクは、フィルタリング対象となります

複数の値を 1 つのリストとして定義できます。各パラメータは別々の行に入力する必要があります。ワイルドカード («*」、「?」) と正規表現がサポートされています

例:

```
ExcludeName=re:.*\.(txt|rtf)
ExcludeName=re:.*\.(doc|xls|ppt)
ExcludeName=re:.*\.(pif|com|exe)
```

Default グループの場合、パラメータ値は空白です

IncludeSize - フィルタリングするメール添付ファイルのサイズ。バイト単位の値を指定するか (たとえば、**3456261**)、または大きさを示す短いレコード形式 (たとえば、**10KB**、**100MB**) を使用できます。空白の値をフィルタリングするには、パラメータを **0** に設定します

レコード形式:

```
IncludeSize=attachment_size - 指定した値に一致するサイズの添付ファイルがフィルタリングされます
```

`IncludeSize=<attachment_size` - 指定した値よりも小さいサイズの添付ファイルがフィルタリングされます

`IncludeSize=<=attachment_size` - 指定した値以下のサイズの添付ファイルがフィルタリングされます

`IncludeSize=>attachment_size` - 指定した値よりも大きいサイズの添付ファイルがフィルタリングされます

`IncludeSize=>=attachment_size` - 指定した値以上のサイズの添付ファイルがフィルタリングされます

`IncludeSize=0` - 空の添付ファイルがすべてフィルタリングされます

パラメータ値を指定しないと、添付ファイルのタイプによるフィルタリングは実行されません

Default グループの場合、パラメータ値は空白です

ExcludeSize - フィルタリングから除外されるメール添付ファイルのサイズ。レコード形式は、**IncludeSize** パラメータと同じです。空の添付ファイルをスキップするには、パラメータを **0** に設定します

Default グループの場合、パラメータ値は空白です

VirusNameList - 感染対象のオブジェクトまたはメッセージに適用される **VirusNameAction** によって定義された特別な操作を必要とする脅威のリスト。脅威の名前は、ウイルス百科事典 (<http://www.viruslistip.com/>) での表示と同じ名前前で指定する必要があります。マスクと正規表現を使用できます。複数の値を指定するには、各値をカンマで区切ります

例:

```
VirusNameList=re:trojan.*, backdoor*
```

パラメータ値が定義されていない場合、オブジェクトはスキャン中に割り当てられたステータスに従って処理されます

Default グループの場合、パラメータ値は空白です

RenameTo=<file_name>|.<extension> - **rename** 操作を適用する際のオブジェクト名の変更モード::

- **RenameTo=<file_name>** - ファイル名は、指定した値に完全に置き換えられます

RenameTo=.<extension> - 指定した拡張子がファイル名に追加されます

例:

```
RenameTo=.vir
```

ファイル file.doc は、file.doc.vir に名前変更されます

```
RenameTo=VIRUS-DO-NOT-OPEN
```

ファイル file.doc は、VIRUS-DO-NOT-OPEN に名前変更されます

パラメータ値が定義されていない場合、アプリケーションはオブジェクトの名前を変更しません

Default グループのパラメータ値は **.vir** です

A.2.5. [kav4lms:groups.<group_name>.notifications] セクション

[kav4lms:groups.<group_name>.notifications] セクションには、通知オプションが含まれます:

NotifySender=all | filtered | infected | protected | suspicious | error | none - 指定のステータスを伴うメールメッセージ (またはメッセージオブジェクト) を検知した際に元のメール送信者に通知します

複数の値を 1 つのリストとして定義できます。各パラメータは別々の行に入力する必要があります。空白の値を指定すると、通知はメッセージ送信者に配信されません

必須のパラメータ

Default グループのパラメータ値は **none** です

注記:

さまざまなステータスを伴うオブジェクトを複数検知した際に通知が送信されるようにするには、**NotifySender** パラメータに複数の値を設定します。

例:

```
NotifySender=filtered
NotifySender=infected
```

NotifyRecipients および **NotifyAdmin** パラメータも同じ方法で割り当てることができます。

NotifyRecipients=all | filtered | infected | protected | suspicious | error | none - 指定のステータスを伴うメールメッセージ (またはメッセージオブジェクト) を検知した際に元のメール受信者に通知します

複数の値を 1 つのリストとして定義できます。各パラメータは別々の行に入力する必要があります。空白の値を指定すると、通知は元のメッセージ受信者に配信されません

必須パラメータ

Default グループのパラメータ値は **all** です

NotifyAdmin=all | filtered | infected | protected | suspicious | error | none - このステータスを伴うメールメッセージまたはメッセージオブジェクトを検知した際に管理者に通知します

複数の値を 1 つのリストとして定義できます。各パラメータは別々の行に入力する必要があります。空白の値を指定すると、通知は管理者に配信されません

必須パラメータ

Default グループのパラメータ値は **none** です

AdminAddresses - メールサーバ管理者のメールアドレス。複数のアドレスをカンマ区切りで指定できます

Default グループのパラメータ値は **postmaster** です

注記:

AdminAddresses パラメータは、Kaspersky Anti-Virus の管理者 (kav4lms.conf ファイルの **[kav4lms:server.notifications]** セクションにある **ProductAdmins** パラメータによって参照される) ではなく、セキュリティ管理者を参照します。

PostmasterAddresses - 発行された通知の送信者アドレス (FROM フィールド) として差し替えられるメールアドレス

Default グループのパラメータ値は **POSTMASTER@localhost** です

Templates - 通知テンプレートを保管するディレクトリ

Default グループのパラメータ値は以下のとおりです
/etc/opt/kaspersky/kav4lms/templates/en (Linux の場合)
/usr/local/etc/kaspersky/kav4lms/templates/en (FreeBSD の場合)

Subject - Subject フィールドに追加される標準通知のヘッダー

Default グループのパラメータ値は **Anti-virus notification message** です

Charset - 通知に使用される文字セット

Default グループのパラメータ値は **us-ascii** です

TransferEncoding - 通知エンコードアルゴリズムの値。

Default グループのパラメータ値は **7bit** です

UseCustomTemplates=yes | no - 通知を生成するためのカスタムテンプレートの使用を有効にします。このモードを有効にするには、パラメータを **yes** に設定します

Default グループのパラメータ値は **no** です

SenderSubject - 送信者通知のメール件名ヘッダー

Default グループのパラメータ値は **Anti-virus notification message** です

AdminSubject - セキュリティ管理者通知のメール件名ヘッダー

Default グループのパラメータ値は **Anti-virus notification message** です

A.2.6. [kav4lms:groups.<group_name>.backup] セクション

[kav4lms:groups.<group_name>.backup] セクションには、メールメッセージに操作を適用する前にバックアップコピーを作成するためのオプションが含まれます:

Policy=message|info|none - バックアップポリシーを定義します

Default グループのパラメータ値は **info** です

Options=cured|deleted|dropped|rejected|warning|renamed|all - バックアップを作成する必要があるメッセージのタイプ

複数のアドレスをカンマ区切りで指定できます

必須パラメータ

Default グループのパラメータ値は **all** です

Destination=/var/opt/kaspersky/kav4lms/backup/ - メッセージのバックアップを保管するディレクトリ

Default グループのパラメータ値は以下のとおりです

/var/opt/kaspersky/kav4lms/backup/ (Linux の場合)

/var/db/kaspersky/kav4lms/backup/ (FreeBSD の場合)

A.3. kav4lms-licensemanager 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:	
-h	kav4lms-licensemanager コンポーネントに関するヘルプ情報を画面に表示します
-v	アプリケーションバージョンを表示します
キー管理オプション:	
-s	インストール済みキーに関する情報を画面に表示します
-c (-C) <path_to_file>	別の設定ファイル <path_to_file> を使用します
-k <path_to_file>	キー <path_to_key_file> に関する情報を画面に表示します
-a <path_to_file>	キー <path_to_key_file> をインストールします
-d(a r)	アクティブなキーの削除 (-da) または追加のキーの削除 (-dr) を行います
-i	ライセンスされたオブジェクトに関する詳細情報をコンソールに出力します

A.4. kav4lms-licensemanager コンポーネントのリターンコード

kav4lms-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キーに関する情報が正常に読み込まれ、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	キー情報がありません。または、設定ファイルで指定されたパスにキーがありません
65	設定ファイルを読み込めません
66	設定ファイルのオプションが無効です
70	kav4lms-licensemanager コンポーネントが破損しています

A.5. kav4lms-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
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
-s	アップデートサーバのリストを画面に表示します
-k	定義データベースの更新が完了した後、 PostUpdateCmd 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、重大な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
-g <URL>	定義データベース更新用のアドレス。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
-d <path_to_file>	ローカルディレクトリ <path_to_file> 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:	
-l <path_to_file>	コンポーネントの動作結果をファイル <path_to_file> に記録します

A.6. kav4lms-keepup2date コンポーネント のリターンコード

kav4lms-keepup2date コンポーネントは、動作中に以下のコードを返します：

0	定義データベースに更新は必要ありません
1	定義データベースは正常に更新されました
10	重大なエラーが発生しました。更新処理を終了します
11	エラーが発生しました。別のアプリケーションインスタンスが動作しています
12	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
30	定義データベース更新後にコマンド PostUpdateCmd を実行できませんでした
60	キー情報がありません。または、設定ファイルで指定されたパスにキーがありません
75	設定ファイルを読み込めません。または設定エラーです

付録B. KASPERSKY LAB

Kaspersky Lab は 1997 年に創設されました。今日では、アンチウイルス、アンチスパム、アンチハッキングのシステムをはじめとする高度な情報セキュリティソフトウェア製品を幅広く取り揃えた、先進的ソフトウェア開発企業となっています。

Kaspersky Lab は国際企業です。ロシアに本社を置き、英国、フランス、ドイツ、日本、ベネルクス各国、中国、ポーランド、ルーマニア、USA（カリフォルニア）に事業所を展開しています。新しい事業所として、European Anti-Virus Research Centre がフランスに設置されました。Kaspersky Lab のパートナーネットワークには、世界中の 500 社を超える企業が参加しています。

現在、Kaspersky Lab には、10 名の MBA 取得者と 16 名の PhD 取得者を含む 1,000 名を超える優秀な専門家が働いています。すべての Kaspersky Lab の上級アンチウイルス専門家は全員、CARO (Computer Anti-Virus Researchers Organization) のメンバーです。

Kaspersky Lab の最大の資産は、コンピューターウイルスとの 14 年にわたる絶え間ない戦いで培われたユニークな知識と豊富な経験です。コンピューターウイルス動作の徹底的な分析により、Kaspersky Lab のスペシャリストは悪意のあるソフトウェアの発展の傾向を予測し、新しいタイプの攻撃に対してタイムリーな保護をお客様に提供できます。この優位性が Kaspersky Lab の製品とサービスの基本となっています。Kaspersky Lab の製品は他社の一歩前を行き、お客様に総合的なアンチウイルス対策をお届けします。

長年の努力の結果、アンチウイルスソフトウェア開発のトップ企業の 1 つになりました。Kaspersky Lab は、アンチウイルスソフトウェアの最新標準の多くを初めて開発しました。当社の代表的製品である Kaspersky Anti-Virus® は、ワークステーション、ファイルサーバー、メールシステム、ファイアウォール、インターネットゲートウェイ、携帯情報端末を含むあらゆるタイプのコンピューターシステムを、ウイルス攻撃から確実に保護します。使いやすい管理ツールにより、コンピューターと企業ネットワークのアンチウイルス保護は最大限自動化されます。世界中の数多くのソフトウェア開発企業が、Kaspersky Anti-Virus カーネルを各社製品に使用しています。

お客様には、製品の安定した動作の保証と、特定のビジネス要件への完全な適合が確かな広汎な追加サービスに満足していただいております。Kaspersky Lab は、企業のアンチウイルスシステムを設計、実装、サポートします。

B.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 “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、次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® 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® Anti-Virus for File Server

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、次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® 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® Administration Kit**

- **Kaspersky® Mail Gateway**
- **Kaspersky® Anti-Virus for Proxy Server**
- **Kaspersky® Anti-Virus for Linux Mail Server**

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ても、競争を起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 はロシア Kaspersky Lab の登録商標または商標です

* その他、記載されている会社名、製品名は、各社の登録商標または商標です。

B.2. お問い合わせ先

製品についてのお問い合わせは、ご購入元の販売代理店で承っております。

一般的なご意見・ご質問等はカスペルスキーラボ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:	http://www.kaspersky.co.jp http://www.viruslistjp.com
E-mail	support@kaspersky.co.jp

付録C. サードパーティ製ソフトウェア

Kaspersky Anti-Virus for Linux Mail Server 5.6 の開発にあたっては、次のサードパーティ製ソフトウェアが、次に示す要件に基づいて使用されています。

C.1. *Pcre* library

The following terms regulate Pcre library use:

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Release 5 of PCRE is distributed under the terms of the "BSD" licence, as specified below. The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,

Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2004 University of Cambridge

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University of Cambridge nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

C.2. *Expat* library

The following terms regulate Expat library use:

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

C.3. *AgentX++v1.4.16* library

The following terms regulate AgentX++v1.4.16 library use:

AGENTX++ LICENSE AGREEMENT

=====

THIS LICENSE AGREEMENT (this "Agreement") is made effective as of the date the product is installed by and between (i) Frank Fock, the author of AgentX++ ("LICENSOR") and the party executing this Agreement as Licensee ("LICENSEE").

1. DEFINITIONS.

1.1 The term "Software Product" means Frank Fock's AgentX++ computer software (including Source Code, derived Object Code, and derived Executable Code as defined in Section 1.3, 1.4, and 1.5) and documentation thereof, as specified in Exhibit A, that is provided by LICENSOR to LICENSEE hereunder, including bug fixes and updates thereto provided by LICENSOR to LICENSEE in connection with this Agreement. The term "derived" in the above context refers to the process of creating machine executable code from the original Source Code only. It does not refer to amendment or alteration of the original Source Code by LICENSOR or any third party.

1.2 The term "Intellectual Property Rights" means patent rights, copyright rights, trade secret rights, and any other intellectual property rights.

1.3 The term "Executable Code" is a fully compiled and linked program that contains any code derived from the Software Product. It can no longer be altered or combined with any other code. Executable code is ready to be executed by a computer and is essentially a complete software image for use in a specific product.

1.4 The term "Object Code" is any compiled version of the Software Product that can be linked and therefore combined with other code to create Executable Code. Examples of Object Code are libraries and software development kits, in particular SNMP agent development kits.

1.5 The term "Source Code" is the human readable form of the Software Product, as specified in Exhibit A.

1.6 Documentation means the documentation regarding the Licensed Software provided by LICENSOR to LICENSEE hereunder.

1.7 The term "Site" is a specific address belonging to a single business unit operating at that address.

2. GRANT OF LICENSE.

2.1 Source Code Site License. Subject to the terms and conditions of this Agreement, and upon payment by LICENSEE to LICENSOR of the one-time license fee set forth in Addendum A, LICENSOR grants LICENSEE a perpetual (subject to termination rights in Section 6), non-exclusive, non-transferable license to reproduce, use, modify, or have modified by a third party contractor (modifications in accordance to Section 2.6) subject to a confidentiality agreement no less restrictive than this Agreement, the Source Code for internal use only, for the sole purpose of developing AgentX-enabled SNMP agents at the Site (hereafter "Licensed Site") specified by LICENSEE during license purchase. Additionally, Customer's contractors and employees reporting directly and only to a manager at the Licensed Site, such as telecommuters, may use the Software Product at remote locations. Off-site employees re-porting in any way to a manager at their location are not covered under this Site License.

2.2 Except as specified in 2.1, neither the Software Product Source Code nor Object Code derived from the Software Product may be redistributed or resold. Executable Code programs derived from the Software Product may be redistributed and resold without limitation and without royalty, provided that LICENSEE added significant functionality to those derived Executable Code programs. Functionality in this context refers to the program's behavior, not appearance.

2.3 No Sublicense Right. LICENSEE has no right to transfer, or sublicense the Licensed Software to any third party, except as specified in 2.2 and except if the third party takes over the business of LICENSEE.

2.4 Other Restrictions in License Grants. LICENSEE may not: (i) copy the Licensed Software, except as necessary to use the Licensed Software in accordance with the license granted under Section 2.1 and 2.2, and except for a reasonable number of backup copies.

2.5 No Trademark License. LICENSEE has no right or license to use any trademark of LICENSOR during or after the term of this Agreement.

2.6 Proprietary Notices. The Licensed Software is copyrighted. All proprietary notices incorporated in, marked on, or affixed to the Licensed Software by LICENSOR shall be duplicated by LICENSEE on all copies, in whole or in part, in any form of the Licensed Software and not be altered, removed, or obliterated on such copies.

2.7 Reservation. LICENSOR reserve all rights and licenses to the Licensed Software not expressly granted to LICENSEE under this Agreement.

2.8 Delivery. Upon execution of this Agreement, and payment of the amounts due and owing under this Agreement, LICENSOR will provide LICENSEE with one (1) copy of the Software Product by downloading from LICENSOR's Web site.

3. PRODUCT WARRANTY.

3.1. LICENSOR warrants to LICENSEE that, at the date of delivery of the Software Product to LICENSEE and for a period ending 90 days following the date of

delivery of the Software Product to LICENSEE the Software Product shall perform substantially in accordance with the published specifications and Documentation. If notified in writing by LICENSEE, LICENSOR may, at its option, correct significant program errors in the Software Product within a reasonable time period. THE FOREGOING PRODUCT WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHETHER IMPOSED BY CONTRACT, STATUTE, COURSE OF DEALING, CUSTOM OR USAGE OR OTHERWISE.

3.2. In no event shall LICENSOR be liable to LICENSEE, in excess of the price paid to LICENSOR by LICENSEE for the Software Product hereunder, for any breach of warranty or any claim, loss or damage arising from or relating to the installation, use or performance of the Software Product (including, without limitation, any indirect, special, incidental or consequential damages).

3.3. LICENSOR reserves the right at any time to make changes to the Software Product.

3.4. IN NO EVENT SHALL LICENSOR BE LIABLE (WHETHER IN TORT, NEGLIGENCE, CONTRACT, WARRANTY, PRODUCT LIABILITY OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OR LOSS OF PROFITS OR SAVINGS ARISING OUT OF ITS PERFORMANCE OR NONPERFORMANCE OF TERMS OF THIS AGREEMENT OR THE USE, INABILITY TO USE OR RESULTS OF USE OF THE SOFTWARE PRODUCT EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

3.5 In no event will LICENSOR be liable for any third-party products used with, or installed in, the Software Product. LICENSOR does not warrant the compatibility of the Software Product with any third-party products, whether hardware or software.

3.6 The above sections do not apply for liability for damages caused by gross negligence or wilful default.

3.7 General Provision. This warranty shall not apply in any case of amendment or alterations of the Software Product made by LICENSEE.

4. INTELLECTUAL AND PROPERTY INDEMNIFICATION.

4.1. LICENSOR agrees to indemnify and hold LICENSEE harmless from any final award of costs and damages against LICENSEE for any action based on infringement of any German intellectual property rights as a result of the use of the Licensed Software: (i) under the terms and conditions specified herein; (ii) under normal use; and (iii) not in combination with other items; provided that LICENSOR is promptly notified in writing of any such suit or claim against LICENSEE and further provided that LICENSEE permits LICENSOR to defend, compromise or settle the same and gives LICENSOR all available information, reasonable assistance and authority to enable LICENSOR to do so. LICENSOR'S LIABILITY TO LICENSEE PURSUANT TO THIS ARTICLE IS LIMITED TO THE TOTAL FEES PAID BY LICENSEE TO LICENSOR IN THE CALENDAR YEAR IN WHICH ANY FINAL AWARD OF COSTS AND DAMAGES IS DUE AND OWING.

5. TRADE SECRETS AND PROPRIETARY INFORMATION.

5.1. LICENSEE acknowledges that LICENSOR is the owner of the Software Product, that the Software Product is confidential in nature and not in the public domain, that LICENSOR claims all intellectual and industrial property rights granted by law therein and that, except as set forth herein, LICENSOR does not hereby grant any rights or ownership of the Software Product to LICENSEE or any third party. Except as set forth herein, LICENSEE agrees not to copy or otherwise reproduce the Software Product, in whole or in part, without LICENSOR's prior written consent. LICENSEE further agrees to take all reasonable steps to ensure that no unauthorized persons shall have access to the Software Product and that all authorized persons having access to the Software Product shall refrain from any such disclosure, duplication or reproduction except to the extent reasonably required in the performance of LICENSEE'S rights under this Agreement.

5.2. LICENSEE agrees to accord the Software Product and the Documentation and all other confidential information relating to this Agreement the same degree and methods of protection as LICENSEE undertakes with respect to its confidential information, trade secrets and other proprietary data.

5.3. LICENSEE agrees not to challenge, directly or indirectly, the right, title and interest of LICENSOR in and to the Software Product, nor the validity or enforceability of LICENSOR's rights under applicable law. LICENSEE agrees not to directly or indirectly, register, apply for registration or attempt to acquire any legal protection for the Software Product or any proprietary rights therein or to take any other action which may adversely affect LICENSOR's right, title or interest in or to the Software Product in any jurisdiction.

5.4. LICENSEE acknowledges that, in the event of a material breach by LICENSEE of its obligations under this Article 5, LICENSOR may immediately terminate this Agreement, without liability to LICENSEE and may bring an appropriate legal action to enjoin any such breach hereof, and shall be entitled to recover from LICENSEE reasonable legal fees and costs in addition to other appropriate relief.

5.5. LICENSEE agrees to notify LICENSOR immediately and in writing of all circumstances surrounding the unauthorized possession or use of the Software Product and Documentation by any person or entity. LICENSEE agrees to cooperate fully with LICENSOR in any litigation relating to or arising from such unauthorized possession or use.

6. TERMINATION.

6.1. LICENSOR may terminate this Agreement at any time after the occurrence of any of the following events if LICENSOR provides 30 days notice of its intention to terminate as a result of the occurrence and LICENSEE fails to cure such

occurrence within such 30 days:

(a) LICENSEE is declared or acknowledges that it is insolvent or otherwise unable to pay its debts as they become due or upon the filing of any proceeding (whether voluntary or involuntary) for bankruptcy, insolvency or relief from creditors of LICENSEE;

(b) LICENSEE assigns or transfers this Agreement or any of its rights to obligations hereunder, without LICENSOR's prior written consent; or (c) LICENSEE violates any material provision of this Agreement, including without limitation, the payment obligations set forth in Addendum A.

6.2. LICENSEE may terminate this Agreement at any time after the occurrence of any of the following events if LICENSEE provides 30 days notice of its intention to terminate as a result of the occurrence and LICENSOR fails to cure such occurrence within such 30 days:

(a) LICENSOR is declared or acknowledges that it is insolvent or otherwise unable to pay its debts as they become due or upon the filing of any proceeding (whether voluntary or involuntary) for bankruptcy, insolvency or relief from creditors or LICENSOR; or

(b) LICENSOR violates any material provision of this Agreement.

6.3. Upon the termination of this Agreement for any reason, LICENSEE will discontinue all use of the Software Product and, within ten (10) days after termination, will destroy or delete all copies of the Software Product then in its possession, including but not limited to, any back-up or archival copies of the Software Product and Documentation. At LICENSOR's request, LICENSEE will verify in writing to LICENSOR that such actions have been taken.

6.4. No termination of this Agreement for any reason whatsoever shall in any way affect the continuing obligations of the parties under Articles 5 hereof.

7. APPLICABLE LAW

This LICENSE shall be deemed to have been made in, and shall be construed pursuant to, the laws of Germany, without reference to conflicts of laws principles. All controversies and disputes arising out of or relating to this Agreement shall be submitted to the exclusive jurisdiction of Esslingen am Neckar, Germany, as long as LICENSEE is deemed to be a merchant (as defined by Handelsgesetzbuch, §1-7). The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

8. GENERAL PROVISIONS.

8.1. This Agreement does not create any relationship of association, partnership, joint venture or agency between the parties.

8.2. This Agreement (including the Exhibit and Addendum attached to the Agreement) sets forth the entire agreement and understandings between the parties hereto with respect to the subject matter hereof. This Agreement merges all previous discussions and negotiations between the parties and supersedes and replaces any and every other agreement, which may have existed between LICENSOR and LICENSEE with respect to the contents hereof.

8.3. Except to the extent and in the manner specified in this Agreement, any modification or amendment of any provision of this Agreement must be in writing and bear the signature of the duly authorized representative of each party.

8.4. The failure of either party to exercise any right granted herein, or to require the performance by the other party hereto of any provision of this Agreement, or the waiver by either party of any breach of this Agreement, shall not prevent a subsequent exercise or enforcement of such provisions or be deemed a waiver of any subsequent breach of the same or any other provision of this Agreement.

8.5. Except in the case of merger, acquisition or the sale of substantial assets or equity of Licensee or assignment to any direct or indirect subsidiary or affiliate of LICENSEE, LICENSEE shall not sell, assign or transfer any of its rights, duties or obligations hereunder without the prior written consent of LICENSOR. LICENSOR reserves the right to assign or transfer this Agreement or any of its rights, duties and obligations hereunder, to any direct or indirect subsidiary or affiliate of LICENSOR.

8.6. All notices required by this Agreement must be sent by certified mail in order to be deemed effective when sent to the following:

FOR LICENSOR:

Frank Fock

Schlossstrasse 8

73765 Neuhausen, Germany

EXHIBIT A

Licensed Software

AgentX++

a. Source Code - (ANSI C++ for Linux, Solaris, Win32) Includes AgentX++ and Agent++Win32 Source Code.

b. Executable Code - AgentX++Win32 Master Agent (Win XP/2000/NT4)

ADDENDUM A

For evaluation purposes and non commercial use only, a free license is granted, provided that the LICENSEE accepts this license agreement.

In order to obtain a license to use AgentX++ in a commercial environment,

LICENSEE has to purchase a commercial license from LICENSOR. The actual pricing list and other related information can be found at <http://www.agentpp.com>

C.4. *Agent++v3.5.28a* library

The following terms regulate Agent++v3.5.28a library use:

AGENT++ API Version 3.x

Copyright (C) 2001 Frank Fock, Jochen Katz

LICENSE AGREEMENT

WHEREAS, Frank Fock and Jochen Katz are the owners of valuable intellectual property rights relating to the AGENT++ API and wish to license AGENT++ subject to the terms and conditions set forth below; and WHEREAS, you ("Licensee") acknowledge that Frank Fock and Jochen Katz have the right to grant licenses to the intellectual property rights relating to AGENT++, and that you desire to obtain a license to use AGENT++ subject to the terms and conditions set forth below; Frank Fock and Jochen Katz grants Licensee a non-exclusive, non-transferable, royalty-free license to use AGENT++ and related materials without charge provided the Licensee adheres to all of the terms and conditions of this Agreement.

By downloading, using, or copying AGENT++ or any portion thereof, Licensee agrees to abide by the intellectual property laws and all other applicable laws of Germany, and to all of the terms and conditions of this Agreement, and agrees to take all necessary steps to ensure that the terms and conditions of this Agreement are not violated by any person or entity under the Licensee's control or in the Licensee's service.

Licensee shall maintain the copyright and trademark notices on the materials within or otherwise related to AGENT++, and not alter, erase, deface or overprint any such notice.

Except as specifically provided in this Agreement, Licensee is expressly prohibited from copying, merging, selling, leasing, assigning, or transferring in any manner, AGENT++ or any portion thereof.

Licensee may copy materials within or otherwise related to AGENT++ that bear the author's copyright only as required for backup purposes or for use solely by the Licensee.

Licensee may not distribute in any form of electronic or printed communication the materials within or otherwise related to AGENT++ that bear the author's copyright, including but not limited to the source code, documentation, help files, examples, and benchmarks, without prior written consent from the authors. Send any requests for limited distribution rights to sales@agentpp.com.

Licensee hereby grants a royalty-free license to any and all derivatives based upon this software code base, that may be used as a SNMP agent development environment or a SNMP agent development tool.

Licensee may modify the sources of AGENT++ for the Licensee's own purposes. Thus, Licensee may not distribute modified sources of AGENT++ without prior written consent from the authors.

The Licensee may distribute binaries derived from or contained within AGENT++ provided that:

- 1) The Binaries are not integrated, bundled, combined, or otherwise associated with a SNMP agent development environment or SNMP agent development tool; and
- 2) The Binaries are not a documented part of any distribution material.

THIS SOFTWARE IS PROVIDED ``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

C.5. *Boost v 1.0* library

The following terms regulate Boost v 1.0 library use:

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE,

ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

C.6. *Milter* library

The following terms regulate *Milter* library use:

The following license terms and conditions apply, unless a different license is obtained from Sendmail, Inc., 6425 Christie Ave, Fourth Floor, Emeryville, CA 94608, USA, or by electronic mail at license@sendmail.com.

License Terms:

Use, Modification and Redistribution (including distribution of any modified or derived work) in source and binary forms is permitted only if each of the following conditions is met:

1. Redistributions qualify as "freeware" or "Open Source Software" under one of the following terms:

a) Redistributions are made at no charge beyond the reasonable cost of materials and delivery.

b) Redistributions are accompanied by a copy of the Source Code or by an irrevocable offer to provide a copy of the Source Code for up to three years at the cost of materials and delivery. Such redistributions must allow further use, modification, and redistribution of the Source Code under substantially the same terms as this license. For the purposes of redistribution "Source Code" means the complete compilable and linkable source code of sendmail including all modifications.

2. Redistributions of source code must retain the copyright notices as they appear in each source code file, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below.

3. Redistributions in binary form must reproduce the Copyright Notice, these license terms, and the disclaimer/limitation of liability set forth as paragraph 6 below, in the documentation and/or other materials provided with the distribution. For the purposes of binary distribution the "Copyright Notice" refers to the following language:

"Copyright (c) 1998-2004 Sendmail, Inc. All rights reserved."

4. Neither the name of Sendmail, Inc. nor the University of California nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission. The name "sendmail" is a trademark of Sendmail, Inc.

5. All redistributions must comply with the conditions imposed by the University of California on certain embedded code, whose copyright notice and conditions for redistribution are as follows:

a) Copyright (c) 1988, 1993 The Regents of the University of California. All rights reserved.

b) Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

i. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

ii. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

iii. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

6. Disclaimer/Limitation of Liability: THIS SOFTWARE IS PROVIDED BY SENDMAIL, INC. AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL SENDMAIL, INC., THE REGENTS OF THE UNIVERSITY OF CALIFORNIA OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

C.7. *Libkavexim.so* library

The libkavexim.so library is distributed in accordance with GPLv2, and its use is regulated by the following terms:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification"). Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive

copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
```

```
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
```

```
This is free software, and you are welcome to redistribute it under certain conditions; type  
`show c' for details.
```

The hypothetical commands ``show w'` and ``show c'` should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ``show w'` and ``show c'`; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright interest in the program
```

```
`Gnomovision' (which makes passes at compilers) written by James Hacker.
```

```
<signature of Ty Coon>, 1 April 1989
```

```
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General.

Public License instead of this License.

付録D. 使用許諾契約書

KASPERSKY LAB 製品に関する使用許諾契約書

お客様は、本ソフトウェア（マニュアル等の付属文書を含む）の使用に際して、以下のソフトウェア使用許諾契約書（以下「本契約」といいます）に同意いただくものとします。

お客様がライセンス契約ウィンドウの [承諾する] ボタンをクリック、または対応する記号を入力、もしくは本ソフトウェアのダウンロードした時点で、この契約条件に拘束されることに同意したことになります。当該行為はお客様の署名を示すものであり、お客様は本契約に拘束され、その当事者となることに同意し、また、本契約書が署名入り契約文書と同様の執行力を持つことに同意するものとします。本契約の諸条件に同意されない場合は、本ソフトウェアのインストールをキャンセルしてください。

ソフトウェアにライセンス契約書または同様の文書が付属する場合は、当該文書に定義されているソフトウェア使用条件が、本契約よりも優先します。

ライセンス契約ウィンドウの [承諾する] ボタンをクリックするか、または対応する記号を入力すると、本契約の契約条件にしたがって本ソフトウェアを使用する権利を得られます。

1. 定義

- 1.1. **本ソフトウェア**とは、ソフトウェア、その他資料およびこれらのアップデートを意味します。
- 1.2. **権利者**（独占的であるか否かを問わず、本ソフトウェアのすべての権利の所有者）は、ロシア連邦法に基づいて設立された企業、Kaspersky Lab, ZAO を意味します。
- 1.3. **コンピューター**とは、本ソフトウェアをインストールおよび／または使用するハードウェアを意味し、パソコン、ノート PC、ワークステーション、個人用デジタル機器、スマートフォン、ハンドヘルド装置、その他、本ソフトウェアが対応する電子装置）を意味します。
- 1.4. **エンドユーザー（お客様）**とは、自身のために本ソフトウェアをインストールする個人または、本ソフトウェアのコピーを合法的に使用する個人を意味し、また、個人が雇用者など組織を代表して本ソフトウェアをダウンロードまたはインストールした場合、「お客様」とは、本ソフトウェアをその利益のためにダウンロードまたはインストールした法人も意味するものとし、ここに、かかる法人は、個人に対しその法人を代表して本契約を承諾するよう承認したものとみなします。本契約の目的において「法人」とは、合名会社、有限会社、企業、協会、合資会社、合弁会社、労働組合、法人化されていない組織、政府当局を含むがこれらに限りません。
- 1.5. **代理店**とは、権利者との契約およびライセンスに基づき本ソフトウェアを販売する法人または個人を意味します。
- 1.6. **アップデート**とは、ソフトウェアのアップグレード、機能改修、パッチ適用、機能拡張、バグ修正、メンテナンスパックの適用などを意味します。
- 1.7. **ユーザーマニュアル**とは、ユーザーマニュアル、管理者ガイド、リファレンス・ブックおよび関連する説明資料またはその他の資料を意味します。

2. ライセンスの付与

- 2.1. お客様は、ライセンス料金を支払い、更に本契約の各条項に同意する限りにおいて、

各ライセンスキーの初回適用日あるいはアクティベーション初回実施日から、ライセンス有効期限までの間、お客様の所属する法人内でのご利用に限り、本ソフトウェアがインストールされたお客様のコンピューターを、ユーザーマニュアルに記載される脅威から、ユーザーマニュアルに記載されるすべての技術要件に従って、かつ本契約の諸条件に従って保護するために、指定された数のコンピューター上へ本ソフトウェアを保存、読み込み、インストール、実行、表示（「使用」するために）する非独占の使用許諾（「ライセンス」）を供与され、お客様はそのライセンスを受諾するものとします。但し、ソフトウェアの新規バージョンあるいは後継製品の発売日を起算日とする 1 年後が到来したとき、ユーザーマニュアルに記載の方法で、確認できるライセンス有効期限にかかわらず現行バージョンの使用権は失効するものとします。この場合お客様は、バージョンアップサービスでソフトウェアをバージョンアップすることにより、新規バージョンあるいは後継製品を継続してご使用いただけます。詳細は本ソフトウェアの各言語版に対応する国の Kaspersky ウェブサイト (www.kaspersky.co.jp) をご確認ください。

トライアル版

本ソフトウェアのトライアル版を受領、ダウンロード、またはインストールし、ソフトウェアのトライアル・ライセンスのみを認められている場合は、別段の指定がない限り最初にインストールした日より 1 トライアル期間（ユーザーマニュアルに記載の方法で別段の期間が確認できない限り通常 30 日）に限り、本ソフトウェアを使用できることとします。トライアル期間中の評価以外の目的での本ソフトウェアの使用および、トライアル期間終了後の使用は厳しく禁止します。

複数の環境で使用ソフトウェア、多言語ソフトウェア、デュアルメディアで使用するソフトウェア、複数コピー、バンドル版

お客様が複数の本ソフトウェアを取得された場合でも、本ソフトウェアのすべてのバージョンをインストールすることが許可されるコンピューターの合計台数は、取得したライセンス上のコンピューター数を超えないものとします。ライセンス条件で別段の規定がない限り、取得されたライセンス数に応じて、第 2.2 条および第 2.3 条で規定する台数のコンピューターにインストールし、使用する権利が与えられます。

- 2.2. 本ソフトウェアを物理メディアで取得した場合、お客様は本ソフトウェアのパッケージに記載されている台数のコンピューターを保護するために本ソフトウェアを使用する権利を持ちます。
- 2.3. 本ソフトウェアをインターネット経由で取得した場合、お客様は本ソフトウェアのライセンス取得時に指定された台数のコンピューターを保護するために本ソフトウェアを使用する権利を持ちます。
- 2.4. 上記第 2.2 条ならびに第 2.3 条の定めにかかわらず、1 台のコンピューターに複数の OS（仮想 OS も含みます）がインストールされている環境で、それぞれの OS にソフトウェアをインストールし、同時起動する場合は、これらの OS 数に相当するライセンスが必要です。
- 2.5. 権利者は、お客様が本ソフトウェアを合法的に使用される場合に限り、バックアップ目的でのみ、必要に応じて本ソフトウェアのバックアップコピーを作る事を認めます。このバックアップコピーは、他の用途に用いてはならず、本ソフトウェアを使用する権利を失った場合や、お客様が本ソフトウェアを使用している国または地域で施行されている法令による以外の理由で、お客様のライセンスが期限切れまたは打ち切りとなった場合は、破棄しなくてはなりません。お客様は、ソフトウェアの他人への貸与やリースをしてはなりません。また、お客様が許諾されたライセンス権利を第三者に譲渡またはサ

ライセンスすることはできません。お客様が、ソフトウェアがインストールされたコンピューターを譲渡または売却する場合は、本契約に基づきお客様がインストールしたソフトウェアの全てがあらかじめインストール先のコンピューターから削除されていることを確認してください。

- 2.6. お客様は、本ソフトウェアのアクティベーション初回実施日を初日とする、またはライセンスキーファイルの初回適用後、ユーザーマニュアルに記載の方法で確認できるライセンスの有効期間に渡り、以下のサービスを受ける権利を与えられます(本ソフトウェアのトライアル版を除く)。
- 権利者によりウェブサイトまたは他のオンラインサービスを介したアップデートが公開された時、インターネット経由で本ソフトウェアのアップデートを受け取れます。受け取ったアップデートは本ソフトウェアの一部となり、本契約の契約条件が適用されます。
 - メールあるいは電話による技術サポート。

3. アクティベーションおよびライセンス有効期間

- 3.1. お客様がご自身のコンピューターの改造やコンピューターにインストールされたほかのベンダーのソフトウェアの変更を行った場合、本ソフトウェアの再アクティベーションまたはライセンスキーファイルのインストールが必要となる場合があります。権利者は、ライセンスの有効性および/またはお客様のコンピューター上にインストールおよび/または使用される本ソフトウェアのコピーの合法性について確認する手段ならびに検証手順を実行する権利を保有します。
- 3.2. 本ソフトウェアの利用可能期間は、ライセンス契約期間ならびにライセンスキーの初回適用日あるいは初回アクティベーション実施日、およびライセンス有効期限日に依存します。お客様は、ライセンスキー初回適用日(初回アクティベーション実施日)を起算とする、ライセンス契約期間が、ユーザーマニュアルに記載の方法で確認できるライセンスの有効期限までの期間よりも短い場合に限り、お求めになったライセンス期間一杯、本ソフトウェアを利用する事ができます。尚、本ソフトウェアでは、ライセンスの初回適用日時(アクティベーションの初回実施日時、およびライセンス有効期限の日時はグリニッジ標準時に基づいて管理されています。なお、ユーザーマニュアルに記載の方法で確認できるライセンス有効期限は、OS で選択している時間帯(タイムゾーン)の設定に従いグリニッジ標準時から換算した時刻です。1 年間(12 ヶ月間)は、ライセンス初回適用日(アクティベーションの初回実施日)を初日とする 365 日間(閏年の場合も同様)とし、ライセンスは当該期間末日のグリニッジ標準時の 24 時まで有効です。
- 3.3. お客様は、第 2.1 条の規定に従って、本契約に従って行われる本ソフトウェアの初回アクティベーション時点より、1 回限りのトライアル期間中(ユーザーマニュアルに記載の方法で別段の期間が確認できない限り 30 日間)、本ソフトウェアのトライアル版を無料で使用する権利を有します。ただし、トライアル版期間は、メールならびに電話によるサポートを受けることはできません。
- 3.4. 本ソフトウェアを使用するお客様のライセンスは、第 3.2 条に記載の期間に限定されます。ライセンスの残存期間はユーザーマニュアルに記載の方法で確認することができます。
- 3.5. 複数台のコンピューターに適用が可能なライセンスの利用期限は、1 台目のコンピューターでライセンスを適用あるいは、アクティベーションを実施した日を起算とする有効期間に限定されます。
- 3.6. お客様が本契約の契約条件のいずれかに違反した場合、権利者は、お客様に通知す

ることなく、また、ライセンス費用またはその一部を返金することなく、ライセンスを打ち切る権利を有するものとします。

- 3.7. お客様は、本ソフトウェアの使用、また本ソフトウェアの使用により得られたレポートその他の情報の使用にあたって、プライバシー法、著作権法、輸出管理法、わいせつ物取締法を含むがこれらに限らない適用されるすべての国際法、国内法、州法、地域および地方の法律および規制を順守することに同意するものとします。
- 3.8. 本契約に別段の具体的規定がない限り、お客様は本契約に基づき与えられた権利または権利を移転または譲渡することができません。

4. 技術サポート

- 4.1. 本契約の第 2.6 条に記載の技術サポートは、本ソフトウェアの最新アップデートを適用している場合に提供されます。
ソフトウェアのインストール、設定および使用に関するお問い合わせは、取得元の販売代理店までご連絡ください。
テクニカルサポートサイト(製品関連ページ):
<http://support.kaspersky.co.jp>

5. 制限事項

- 5.1. お客様は、本ソフトウェアの逆コンパイル、逆アセンブルまたはリバースエンジニアリングを行ったり、ソフトウェアの一部を可読可能な形式に変換したり、あるいは第三者にそれらの行為を許可したりする事はできません。また、本契約で明確に許可された場合を除き、第三者に対するコピーの許可、エラーの修正、ソフトウェアの変更、改変、翻案、ソフトウェアの派生物の作成等の行為を行ってはなりません。本書に明示されていないすべての権利は権利者またはそのサプライヤーのどちらかが保有するものとし、不正な本ソフトウェアの使用は、本契約により許諾されるライセンスの即時解除ならびに刑事上民事上の訴追がなされる場合があります。
- 5.2. お客様は、本ソフトウェアの他人への貸与やリースをしてはなりません。また、お客様が許諾されたライセンス権利を第三者に譲渡またはサブライセンスすることはできません。
- 5.3. アクティベーションコードおよびライセンスキーファイルは権利者の機密情報とみなされ、第三者に提供または、アクセス可能にしないものとします。
- 5.4. お客様は、本ソフトウェアを第三者に貸与、レンタル、リースしてはなりません。
- 5.5. お客様は、ユーザーマニュアルに記載される脅威の検出、ブロック、処理に使用されるデータまたはソフトウェアの作成に本ソフトウェアを使用しないものとします。
- 5.6. お客様が本契約の契約条件に違反した場合、キーファイルがブロックされることがあります。
- 5.7. お客様がソフトウェアのトライアル版を使用する場合、本契約の第 4 条による技術サポートを受ける権利や、本ソフトウェアを使用するライセンスや権利を第三者に譲渡する権利を持ちません。

6. 限定保証と免責条項

- 6.1. 権利者は、本ソフトウェアが、ユーザーマニュアルに規定の仕様および説明に従って実質的に機能することを保証します。ただし、(w) 権利者が明示的に保証責任を否認しているお客様のコンピューターの欠陥ならびに関連する権利侵害、(x) 誤用から生じ

る不調、欠陥、エラー。乱用、事故(アクシデント)、不履行。不適切なインストールならびに操作またはメンテナンス。盗難、破壊行為、不可抗力、テロ、停電または電力サージ、不慮の事故。改造ならびに許可されていない変更。権利者以外による修理または権利者の合理的な管理の範囲外である原因による誤動作、不具合、故障、(y)最初に生じてから合理的な期間内にお客様が権利者に通知しなかった欠陥、(z)お客様のコンピューターにインストールされているハードウェアまたはソフトウェアコンポーネントとの互換性の欠如、の場合にはかかる限定的保証は適用されないものとします。

- 6.2. お客様は、エラーのないソフトウェアは存在しないことを認知、承諾、同意し、お客様にとって適切な頻度と信頼性に基づき、不測の事態に備え、コンピューターのバックアップをとるようアドバイスを受けたことを認めるものとします。
- 6.3. ユーザーマニュアルまたは本契約の条件に違反している場合、権利者は、本ソフトウェアの正常動作を保証しません。
- 6.4. 本契約の第 2.6 条に指定のアップデートを定期的にダウンロードしていない場合は、権利者は、本ソフトウェアの正常動作を保証しません。
- 6.5. 本契約の第 3.2 条に指定されている期間の経過後、または、何らかの理由で本ソフトウェアを使用するライセンスが終了している場合は、権利者は、ユーザーマニュアルに記載される、脅威からの保護機能を保証しないものとします。
- 6.6. 本ソフトウェアは「現状有姿」で提供され、権利者は、その使用または性能に関し言質を与えず、保証を行いません。適用法により、除外または限定が行えない範囲の保証、条件、言質、契約条件を除き、権利者およびその代理店は、第三者の権利を侵害しないこと、商品性、品質、完全性、特定目的への合致性を含むが、それに限らない事柄に関し、一切の保証、条件設定、言質、契約条件設定(明示的または黙示的を問わず、また、法令、普通法、習慣、利用その他にかかわらず)を行いません。お客様は意図した結果を得るために本ソフトウェアを選択したこと、また、そのインストール方法、使用方法、および得られた結果について、その性能に関し、すべての責任とリスクを負うこととします。前項の規定を制限することなく、権利者は、本ソフトウェアにはエラーがないことや、障害その他の故障がないこと、または、権利者に開示されているか否かにかかわらず、お客様の要件の一部またはすべてを満たしているかどうかについて、一切の保証を行わず、言質を与えないものとします。

7. **免責事項**

- 7.1. 本契約は、次の場合の権利者およ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。
 - 7.1.1. 虚偽の不法行為。
 - 7.1.2. 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。
 - 7.1.3. 法による除外が不可能な義務。
- 7.2. 第 7.1 条の条件の下、次の損害または被害に対し、権利者および代理店は(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)負いません。
 - 7.2.1. 収入の損失
 - 7.2.2. 実際および将来の逸失利益(契約上の逸失利益を含む)
 - 7.2.3. 将来見込まれる貯蓄の損失

- 7.2.4. 取引上の損失
 - 7.2.5. 機会損失
 - 7.2.6. 信用上の損失
 - 7.2.7. 信用毀損
 - 7.2.8. データの消失、損傷あるいは改悪
 - 7.2.9. 間接的又は派生的損失 (錯誤回避のために第 7.2.1 項～第 7.2.8 項の損失・損害を含む)
- 7.3. 第 7.1 条の条件の下、ソフトウェアの提供に関連して発生する権利者および代理店の責任 (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。

8. GNU およびその他のサードパーティ・ライセンス

本ソフトウェアは、GNU 一般公有使用許諾 (GPL) または同様のフリーソフト・ライセンスに基づきお客様にライセンスされている (またはサブライセンスされている) ソフトウェア・プログラムを含む場合があります。これらのプログラムはほかの権利のほかにも、お客様に対し、一定のプログラムまたはその一部をコピー、変更、再配布することを許可し、またソースコードへのアクセスを許可しています (オープンソース・ソフトウェア)。バイナリ形式の実行ファイルで配布されるかかるソフトウェアの当該ライセンスで必要な場合、ソースコードをそれらのお客様が利用できるようにしなくてはならず、この場合、ソースコードは source@kaspersky.com までリクエストを送付し入手するか、またはソースコードは本ソフトウェアに付属しています。オープンソース・ソフトウェア・ライセンスが権利者に対し、オープンソース・ソフトウェア・プログラムを使用、コピー、変更する権利を提供するよう要求し、かかる権利が、本契約で認められている権利よりも大きい場合、かかる権利は、本書における権利および制限に対し優先するものとします。

9. 知的財産権

- 9.1. 本ソフトウェアおよび本ソフトウェアに含まれる著作、システム、アイデア、操作方法、マニュアル、およびその他の情報は、権利者またはその代理店の独占所有物である知的財産および企業秘密であって、また、権利者および該当する場合その代理店は、刑法および民法によって、また、ロシア連邦、EU、合衆国およびその他の国の著作権、企業秘密、商標、特許法ならびに国際条約によって保護されることにお客様は同意するものとします。本契約は、お客様に対し、権利者やその代理店の商標や商号 (「本商標」) を含む、知的財産権への権利を与えるものではありません。お客様は、商標に関する認められた慣習に従って、本ソフトウェアが生成した印刷物を商標所有者の名前等により特定する場合に限り、本商標を使用することができます。このような形で本商標を使用することにより、本商標の所有権がお客様に与えられるものではありません。権利者およびその代理店は、本ソフトウェアに関連するすべての権利、権限、および利益を所有し継続してこれを保有します。これには、権利者が行ったかまたは第三者が行ったかにかかわらず、本ソフトウェアへのエラー修正、拡張機能、アップデート、またはその他の修正が含まれ、また、すべての著作権、特許、企業秘密権、商標権、その他の知的財産権が含まれます。お客様による本ソフトウェアの所有、インストール、使用は、お客様に対して本ソフトウェアの知的財産権の所有権を移譲するものではなく、お客様は、本契約に明示的に規定されたものを除き、本ソフトウェアに対するなんら

の権利を取得しないものとします。本契約に基づいて作成された本ソフトウェアのすべてのコピーには、本ソフトウェアに表示されるものと同じ著作権表示を行わなくてはなりません。本契約は、本ソフトウェアに対する本書に記載される以外の知的所有権をお客様に供与するものではなく、本書で詳しく定義する本契約に基づき供与されるライセンスは、本契約の条件に従った限定的使用权のみを提供するものであることをお客様は認めるものとします。権利者は、本契約において明示的に供与された権利以外のすべての権利を保有するものとします。

- 9.2. お客様は、いかなる形でも本ソフトウェアを修正または改ざんしないことに同意し、本ソフトウェアのコピー上の、著作権表示その他独占所有権表示を削除または変更することもできません。

10. 準拠法、仲裁

本契約はロシア連邦の法律に管轄され、同法にしたがって解釈され、法の抵触に関する原則の適用は受けません。本契約は、「物品の国際売買契約に関する国連条約」によって管轄されないものとし、同法の適用を明示的に排除します。本契約の条件の解釈または適用、あるいは違反に起因する論争については、直接交渉により解決しない限り、ロシア連邦内の、ロシア連邦モスクワ商工会議所の国際商事仲裁裁判所によって仲裁されるものとします。仲裁人による裁定は最終的なもので、両当事者を拘束するものとし、かかる仲裁裁定は、管轄権のある裁判所により執行できるものとします。第 10 条の規定は、仲裁手続きの前、途中、後のいずれの時期においても、当事者が裁判管轄権のある法廷に衡平法上の救済を求める、または得ることを阻まないものとしてします。

11. 訴訟期間

本契約のどちらかの当事者に対し起こされる、本契約に基づく取引に由来する訴訟は、その形式を問わず、訴訟の原因が発生または、発生したことが発見されてから一（1）年以上経過した後に起訴されないものとします。ただし、知的所有権の侵害訴訟は、該当する法定期間の最大限まで起訴できるものとします。

12. 完全合意条項、分離条項、権利不放棄

本契約は、お客様と権利者との間の完全なる合意であり、口頭または書面による、本ソフトウェアまたは本契約の主題に関する、それ以前の取り決め、提案、通信内容、広告に優先するものとします。お客様は本契約を読み、理解し、その条件に拘束されることに同意するものとします。裁判管轄権のある法廷によって、何らかの理由により本契約のある条項は、一部または全部が効力がなく、無効である、または執行不可能であるとされた場合も、かかる条項を狭く解釈して、合法かつ執行可能にされるものとし、また、これにより契約全体が無効とはならず、本契約の残りの部分は、できる限りその元の意味を維持しながら、法および衡平法上許される最大限まで、完全なる効力を持続するものとします。本書の条項または条件の権利放棄は、書面により、お客様と権利者の権限を与えられた代表者の両方の署名によらない限り、有効ではないものとし、本契約の条項違反に対する異議申し立ての権利放棄は、以前、現在（同時進行）、および将来の権利放棄を構成しないものとします。本契約の条項または権利の厳守について、その不履行を権利者が指摘しなかったことは、かかる条項または権利の権利放棄として解釈されないものとします。

13. 権利者の連絡先

本契約に関する質問がある場合や、何らかの理由で権利者に連絡する場合は、以下に記載する当社の顧客サービス部門まで連絡してください。

Kaspersky Lab ZAO
10/1 1st Volokolamsky Proezd, Moscow, 123060
ロシア連邦
電話: +7-495-797-8700
Fax: +7-495-645-7939
メールアドレス: info@kaspersky.com
ウェブサイト: www.kaspersky.com

日本の連絡先
〒101-0032
東京都千代田区岩本町 3-11-9 KDX 岩本町ビル
Kaspersky Labs Japan
www.kaspersky.co.jp
support@kaspersky.co.jp

© 1997-2011 Kaspersky Lab ZAO. 無断複写・転載を禁じます。本ソフトウェアならびに付属文書は、著作権が設定され、著作権法ならびに国際著作権条約、ならびにその他の知的財産権関連の法律ならびに条約により保護されています。