

KASPERSKY LABS JAPAN

Kaspersky[®] Anti-Spam 3.0

管理者ガイド

KASPERSKY[®]

© Kaspersky Labs Japan

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

Revision date: July, 2008.

目次

第1章 KASPERSKY ANTI-SPAM 3.0.....	6
1.1. ライセンスポリシー	6
1.2. システム要件	7
1.3. 本書で使用されるアイコンの説明.....	8
第2章 KASPERSKY ANTI-SPAM の構造およびスパムフィルタリングの原理.....	9
2.1. 製品の構造	9
2.2. 認識技術.....	13
2.2.1. 形式的な兆候の分析	13
2.2.2. コンテンツフィルトレーション.....	14
2.2.3. 外部サービスを使用するチェック	15
2.2.4. 緊急検知システム.....	15
2.3. 認識結果およびメッセージに適用する動作.....	16
2.4. コンテンツフィルトレーションデータベース	18
2.5. フィルトレーションポリシー	18
2.6. Control Center	19
2.7. 監視.....	19
第3章 KASPERSKY ANTI-SPAM のインストール.....	21
3.1. インストールの準備	21
3.2. Kaspersky Anti-Spam 配布パッケージのインストール.....	22
3.3. ライセンスキーのインストール.....	23
3.4. メールサーバへの Kaspersky Anti-Spam の統合	24
3.5. Control Center へのアクセス設定.....	25
3.6. コンテンツフィルトレーションデータベースの更新および UDS の使用に 関する設定	26
第4章 スパムフィルトレーションサーバの管理	28
4.1. Kaspersky Anti-Spam コンポーネントの起動および管理.....	28
4.2. Kaspersky Anti-Spam Control Center.....	29
4.3. フィルトレーションポリシーの管理	30

4.3.1. 一般フィルトレーションポリシー.....	31
4.3.1.1. [General]セクション.....	32
4.3.1.2. [DNS & SPF Checks]セクション.....	35
4.3.1.3. [Headers Checks]セクション.....	36
4.3.1.4. [Eastern Encodings]セクション.....	38
4.3.1.5. [Obscene Content]セクション.....	38
4.3.2. ホワイトリストおよびブラックリストの管理.....	39
4.3.3. 使用する DNSBL サービスのリストの管理.....	41
4.3.4. 保護対象ドメインリストの管理.....	43
4.3.5. グループ管理.....	44
4.3.6. グループフィルトレーションポリシーの管理.....	47
4.3.7. メッセージに適用する動作.....	48
4.4. コンテンツフィルトレーションデータベースの更新.....	51
4.4.1. 更新パラメータの設定.....	51
4.4.2. 更新の開始.....	54
4.5. スпамフィルトレーションサーバの設定.....	55
4.5.1. 共通フィルトレーションサーバパラメータ.....	56
4.5.2. フィルトレーションマスタプロセスのパラメータ.....	58
4.5.3. フィルタリングプロセスのパラメータ.....	59
4.5.4. スпам認識パラメータ.....	60
4.5.5. クライアントモジュールの設定.....	62
4.5.6. 拒否されたメッセージに関する通知.....	63
4.6. Control Center の設定.....	64
4.7. ライセンスキーの管理.....	65
4.7.1. ライセンス情報の表示.....	66
4.7.2. 新しいライセンスキーのインストール.....	67
4.7.3. ライセンスキーの削除.....	68
4.8. フィルトレーションサーバアクティビティの監視.....	68
4.8.1. 全般的なステータス情報.....	68
4.8.1.1. アンチスパムエンジンに関する詳細情報.....	70
4.8.1.2. 更新用モジュールに関する詳細情報.....	71
4.8.1.3. ライセンシングモジュールに関する詳細情報.....	73
4.8.2. システムメッセージの監視とレポート.....	74

4.9. Kaspersky Anti-Spam の統計情報	75
第 5 章 カスペルスキーアンチスパムのアンインストール	77
第 6 章 よくある質問と回答 (FAQ)	79
付録 A. KASPERSKY ANTI-SPAM の追加情報.....	82
A.1. ファイルシステム内の製品ファイルの場所	82
A.2. 各種メールサーバのクライアントモジュール.....	83
A.2.1. クライアントモジュールとフィルタリングサーバ間のやり取り	83
A.2.2. クライアントモジュールの共通設定	84
A.2.3. <i>kas-milter</i> – Sendmail メールサーバ用のクライアントモジュール.....	85
A.2.4. <i>kas-pipe</i> – Postfix および Exim メールサーバ用のクライアントモジュール	87
A.2.4.1. <i>kas-pipe</i> と連動するよう Postfix を設定する	90
A.2.4.2. <i>kas-pipe</i> と連動するよう Exim を設定する.....	92
A.2.5. <i>kas-exim</i> – Exim メールサーバ用のクライアントモジュール	94
A.2.6. <i>kas-qmail</i> – Qmail メールサーバ用のクライアントモジュール.....	96
A.2.7. <i>kas-cgpro</i> – CommuniGate Pro メールサーバ用のクライアントモジュール.....	97
A.3. Kaspersky Anti-Spam 設定ファイル.....	100
A.3.1. メイン設定ファイル <i>filter.conf</i>	100
A.3.2. <i>kas-thttpd.conf</i> 設定ファイル.....	106
A.4. Kaspersky Anti-Spam のユーティリティ	106
A.4.1. <i>kas-htpasswd</i>	106
A.4.2. <i>kas-show-license</i>	107
A.4.3. <i>install-key</i>	107
A.4.4. <i>remove-key</i>	108
A.4.5. <i>kas-restart</i>	109
A.4.6. <i>mkprofiles</i>	110
A.4.7. <i>sfmonitoring</i>	111
A.4.8. <i>sfupdates</i>	112
A.5. フィルタリングモジュール用の特別なヘッダ	113
A.6. cron サービスを使用した設定	115
付録 B. スパムメールの報告方法.....	118

付録 C. KASPERSKY LAB	119
C.1. カスペルスキーラボのその他の主な製品	119
C.2. お問い合わせ先	124
付録 D. THIRD PARTY SOFTWARE	125
付録 E. 使用許諾契約書	139

第1章 KASPERSKY ANTI-SPAM 3.0

Kaspersky® Anti-Spam 3.0 迷惑メール対策用ソリューションです。

Kaspersky Anti-スパムは、管理者が定めたポリシーに則ったスパムフィルタリングを行います。スパムメールの受信や遮断、配信を行わなかった旨の通知、ヘッダの追加他、管理者が指定する動作を実行します。

スパムの判定は、送受信者、メッセージサイズおよびヘッダー(From と To を含む)をベースに行うほか、以下のフィルタリングを行います：

- ブラックリストとホワイトリストを用いた送信者アドレス
- DNS ベースリアルタイムブラックホールリスト(DNSBL)中の送付者の IP アドレス
- 送信サーバ用 DNS レコードの有用性
- 送付者の IP アドレスのチェックに SPF ベースのドメインを参照
- SURBL (Spam URL Realtime Blocklists)を利用したアドレス及びメッセージ中のリンクのチェック

さらに、メールサブジェクトを含むメッセージのコンテンツフィルタリングを行います。Anti-Spamには単語の組み合わせをベースにした言語解析のアルゴリズムが搭載されています。また、メッセージの署名からスパム判定を行うことも出来ます(2.3を参照)。

管理者は判定ポリシーをコントロールセンターで一元設定できます(2.6を参照)。

1.1. ライセンスポリシー

Kaspersky Anti-Spam 3.0 のライセンスは、以下のポリシーに従った上限を設定し発行されます。

- 一日あたりのメールトラフィック総量
- 保護対象のメールアドレス数
- メールシステムが管理するユーザ数

これらの上限は、保護対象のドメイン内において、送信者(sender)が指定する受信者へのメールについてのみ有効です。保護対象のドメインはコントロールセンターにて設定できます(43ページの4.3.4を参照)、(44ページの4.3.4項を参照)。保護対象に設定していないドメインに属する受信者宛のメールはフィルタされません。



保護対象のドメインを特定してから Kaspersky Anti-Spam を使用してください。

1.2. システム要件

Kaspersky Anti-Spam 3.0 を使用する最小システム要件は以下です。

- ハードウェア必要条件：
 - Intel Pentium III 500 MHz-class プロセッサ
 - 512Mb 以上の RAM
- ソフトウェア必要条件：

以下のうちいずれかの OS

- RedHat Linux 9.0
- Fedora Core 3
- RedHat Enterprise Linux Advanced Server 3
- SuSe Linux Enterprise Server 9.0
- SuSe Linux Professional 9.2
- Mandrake Linux version 10.1
- Debian GNU/Linux 3.1
- FreeBSD 5.4
- FreeBSD 6.2.






以下のうちいずれかのメール配送システム:

- Sendmail 8.13.5 with Milter API support
- Postfix 2.2.2
- Qmail 1.03
- Exim 4.50
- Communigate Pro 4.3.7.

“bzip2”、” which”ユーティリティ

Perl インタプリタ

1.3. 本書で使用されるアイコンの説明

アイコン	意味
太字	メニュータイトル、コマンド、ウインドウタイトル、ダイアログエレメント 他
 情報	追加情報やノート
 注意	重要な情報
 実行手順: ステップ 1. ...	処理を実行するための手順
 タスク:	パラメタ定義、機能などの例としての タスク
 キー	定式化されたタスクの解決

第2章 KASPERSKY ANTI-SPAM の構造およびスパムフィルタリングの原理

この章では、主な製品コンポーネントおよびフィルタリングの原理について説明します。また、Kaspersky Anti-Spam の管理および設定を行うためのメインツールである Control Center についても解説します。

2.1. 製品の構造

Kaspersky Anti-Spam 3.0 は、スパムを認識してフィルタリングするシステムであり、メールサーバの一部として機能します。Kaspersky Anti-Spam 3.0 は、メールの受信、中継、受信者のメールボックスへの配信を行うことができるフル機能のメールサーバではありません。図1は、Kaspersky Anti-Spamの構造を示しています。

Kaspersky Anti-Spam は、以下のコンポーネントで設定されています。

- **クライアントプラグインモジュール** – メールサーバとの統合用。
- **アンチスパムエンジン** – メールメッセージの評価を分析してメッセージを処理するフィルトレーションサーバコンポーネント。フィルトレーションサーバには、各種機能の提供とメールサーバとの統合を可能にする、以下のような補助モジュールが用意されています。
 - **フィルトレーションモジュール** – スパムをフィルタリングするモジュール。
 - **ライセンスモジュール** – 製品のライセンスおよび保護対象ドメインのリストを管理するモジュール。
 - **コンテンツフィルトレーションデータベース** – フィルトレーションサーバがメッセージを評価する際に使用するデータを集めたもの。コンテンツフィルトレーションデータベースの更新は、カスペルスキーラボスのサーバ上でおよそ 20 分おきに公開されます。
 - **コンテンツフィルトレーションデータベースの更新用モジュール** – このシステムは、新しいコンテンツフィルトレーションデータベースを更新サーバから自動的にダウンロードし、アン

チスパムエンジンが使用できるようにデータベースをインストールします。

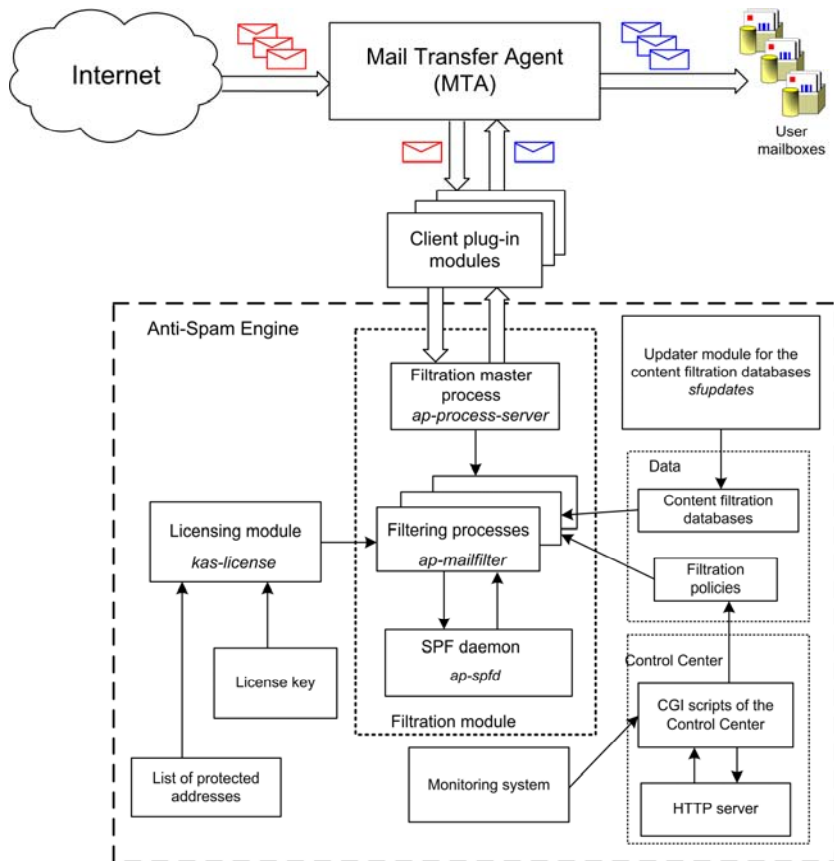


図 1. Kaspersky Anti-Spam の構造

- Control Center – Web ベースのインタフェース。管理者は、このインタフェースを使用して、製品の設定やステータスおよび機能の分析を行います。
- 監視システム – このシステムは、Kaspersky Anti-Spam および各コンポーネントのステータスを監視して、運用上のさまざまな問題についてシステム管理者に通知します。

クライアントプラグインモジュールは、Kaspersky Anti-Spam をさまざまなメールサーバと統合するために設計されたモジュールです。各クライアントプラグイ

ンは、対応するメールサーバの特性と指定された統合方法を考慮するよう設計されています。

Kaspersky Anti-Spam の配布パッケージには、Sendmail、Postfix、Exim、Qmail、および CommuniGate Pro 用のクライアントプラグインが含まれています。

原則として、メールサーバからのメッセージの受信を分析したり、変更済みのメールを返したりするためには、クライアントプラグインをフィルタとしてインストールする必要があります。

クライアントプラグインモジュールは、それぞれ対応するメールサーバから起動されます。ただし、Sendmailだけはクライアントプラグインを起動しません。メールサーバは、複数のメールを並行処理するために、複数のクライアントプラグインを起動できます。クライアントプラグインモジュールおよびその統合方法の詳細については、83ページの付録A.2を参照してください。

各クライアントモジュールの特性に関係なく、各モジュールは、ネットワークまたはローカルソケット経由で、内部データ交換プロトコルを使用してフィルトレーションサーバとやり取りします。

アンチスパムエンジンは、アクセス中のクライアントからの要求に応答し、クライアントからメッセージを受信して分析し、分析結果を返します。

標準的なインストール方法では、クライアントプラグインが統合されたメールサーバとフィルトレーションサーバが、同一コンピュータ上にインストールされることが想定されています。

ただし、Kaspersky Anti-Spam のアンチスパムエンジンを別のサーバにインストールすることもできます。その場合、別のコンピュータ(サーバ)上で稼働しているクライアントモジュールが、ローカルネットワーク経由でTCPを使用して、フィルトレーションサーバとデータをやり取りします。

専用コンピュータで稼働しているアンチスパムエンジンは、使用するコンピュータのパフォーマンスがすべてのメールトラフィックを十分に処理できる場合、一度に複数のメールサーバを扱うことができます。

アンチスパムエンジンは、以下のコンポーネントで設定されています。

- メッセージの分析を行うフィルトレーションモジュール
- ライセンシングモジュール。有効なライセンスキーファイルの可用性と、購入したライセンスで指定されている制限を遵守しているかについてチェックします。
- SPF を処理するデーモン
- コンテンツフィルトレーションデータベースの自動ダウンロードおよびコンパイルを行うスクリプト
- Control Center
- 補助的なプログラムおよびスクリプト

フィルタリングモジュールのメインコンポーネントは、フィルトレーションマスタプロセス(*ap-process-server*)です。このプロセスでは、以下のタスクが実行されます。

- クライアントモジュールからのフィルタリングプロセスへの接続要求の監視
- 使用可能なフィルタリングプロセスがなくなった場合の、新規フィルタリングプロセスの開始
- 実行中のプロセスのステータスの監視
- 信号(SIGHUP など)発生時の子プロセスの終了

トラフィック量が多い場合、実行中のフィルトレーションプロセス数が数十個にも及ぶ可能性があります。メールサーバの負荷が小さくなったときに、アイドル状態のフィルタリングプロセスが終了されます。実行中のフィルトレーションプロセスの最大数および最小数は、アンチスパムエンジンの設定によって定義されます(100ページの付録A.3.1を参照)。

フィルタリングプロセス(*ap-mailfilter*)の開始時に、既存のフィルトレーションポリシーとコンテンツフィルトレーションデータベースがロードされます。クライアントモジュールとの接続が確立されると、フィルタリングプロセスは、モジュールからメッセージのヘッダおよび本文を受信し、それらを分析し、分析結果をクライアントモジュールに返します。

SPFポリシーに従ってメッセージの送信者をチェックする必要がある場合は、フィルタリングプロセスが、**SPFデーモン**(*ap-spfd*)に要求を送信します。SPFデーモンは、必要なクエリをDNSサーバに送信し、その結果をフィルタリングプロセスに返します。

有効なライセンスキーが存在する場合、アプリケーションはメッセージを分析し、フィルトレーションポリシーに定義されているルールをメッセージに適用します。

すべてのライセンスチェックは、フィルトレーションプロセスからの要求に基づいて、ライセンシングモジュール(*kas-license*)が行います。

メッセージのプロセスが完了しても、フィルタリングプロセスは終了せず、新しい要求が送信されるのを待機します。フィルタリングプロセスは、指定されている1プロセスあたりの最大数(原則として300)のメッセージをプロセスした後、終了、またはアイドル状態で長時間待機します。

更新の自動ロード用スクリプト(*sfupdates*)は、スケジュールに従って稼働し(**cron**サービスを使用)、更新サーバから最新版のコンテンツフィルトレーションデータベースをダウンロードします。さらに、データベースを構築して、フィルトレーションサーバが使用できるようにインストールも行います。

Control Centerは、Webベースのインタフェースです。管理者は、このインタフェースを使用して、製品およびスパムフィルトレーションポリシーを設定できま

す。

監視システムは、Kaspersky Anti-Spamの各コンポーネントのステータスを監視し、フィルトレーションサーバおよびその他の製品コンポーネントの運用上で発生している問題についてシステム管理者に通知します。

Kaspersky Anti-Spam 3.0 は、以下のアルゴリズムでメールトラフィックをプロセスします。

1. クライアントプラグインモジュールが、インストールされているメールサーバに統合されます。
2. メールサーバが、フィルトレーションサーバで分析を行うメッセージをクライアントモジュールに送信します。
3. フィルトレーションサーバは、メッセージをスキャンしてスパムの兆候がないかチェックし、その結果に応じて、既存のルールに従ってメッセージを変更します。
4. クライアントプラグインモジュールが、配信するためにプロセス済みのメッセージをメールサーバに返します。

2.2. 認識技術

Kaspersky Anti-Spam は、メールトラフィック内のスパムを検出する強力なツールを提供します。このセクションでは、この製品に実装されているスパム認識技術の概要について簡単に説明します。

2.2.1. 形式的な兆候の分析

この方法では、特定のメッセージヘッダの検査と、一般的なスパムメッセージのヘッダとの比較に基づく一連のルールが使用されます。ヘッダ分析に加えて、メッセージの構造、サイズ、添付ファイルの有無、およびその他の類似する兆候も考慮されます。

また、SMTP セッション中に送信者によって送信されたデータの分析も行われます。特に、以下の情報が評価対象になります。

- メッセージを送信したサーバの IP アドレスと、そのアドレスが受信者のホワイトリストまたはブラックリストに含まれているかどうか
- 受信したヘッダから取得した中間中継サーバのIPアドレス
- SMTP セッションコマンドで送信されたメッセージの送信者および受信者のメールアドレス
- ホワイトリストまたはブラックリストに送信者および受信者のアドレスがあるかどうか

- SMTP セッション中に送信されたアドレスが、メッセージヘッダおよびその他のチェックで指定されているアドレスと一致するかどうか

2.2.2. コンテンツフィルトレーション

メッセージ分析では、次のようなコンテンツフィルタリングアルゴリズムが使用されます。アプリケーションが、人工知能的技術を使用してメッセージコンテンツ(件名ヘッダを含む)と以下の形式の添付物(添付ファイル)を分析します。

- プレーンテキスト(ASCII、非マルチバイト)
- HTML (2.0、3.0、3.2、4.0、XHTML 1.0)
- Microsoft Word (バージョン 6.0、95/97/2000/XP)
- RTF



スパムフィルタリングの目的は、ユーザのメールボックスに受信される不要なメッセージの量を減らすことです。条件をあまり厳しくすると必然的に通常のメッセージもフィルタリングされてしまうため、すべてのスパムメッセージを検出することは不可能です。

このアプリケーションは、主に以下の3つの方法を使用して、スパムの疑いがあるメッセージを検出します。

- さまざまなカテゴリの**内容サンプルとのテキスト比較**(メッセージ本文内のキー用語(単語および単語の組み合わせ)の検索と、その後の確率論的解析に基づく)。この方法では、テキスト内の典型的な語句や表現のヒューリスティック検索が行われます。
- **サンプルメッセージの集合を使用して検査を行うメッセージのあいまい比較**。メッセージの特徴を比較します。この方法は、変更されたスパムメッセージを検出するのに役立ちます。
- **添付画像の分析**

分類インデックス(カテゴリの階層リスト)や典型的な用語など、Kaspersky Anti-Spam がコンテンツフィルタリングに使用するすべてのデータは、コンテンツフィルトレーションデータベースに保存されています。



カスペルスキーラボスのスパム分析グループが、コンテンツフィルトレーションデータベースの追加および改善を休みなく行っています。したがって、このデータベースを定期的に更新することをお奨めします(51ページのセクション4.4を参照)。

また、Kaspersky Anti-Spam が認識できなかったスパムメールのサンプルや、誤ってスパムとして分類されたメッセージのサンプル

を、カスペルスキーラボス宛てにお送りいただくこともできます。お送りいただいたデータを使用してコンテンツフィルトレーションデータベースを改善し、新種のスパムに適宜対応いたします。サンプルメッセージの転送方法については「付録 B」を参照してください。

2.2.3. 外部サービスを使用するチェック

メッセージのテキストおよびヘッダの分析に加えて、Kaspersky Anti-Spam では、外部のネットワークサービスを使用して、以下のようなさまざまなチェックを行うことができます。

- DNS レコードを使用して、メッセージ送信者の IP をチェックします(DNS 逆引き)。
- 送信者の IP アドレスが、DNS ベースのリアルタイムブラックホールリスト(DNSBL)に含まれているかどうかをチェックします。
- 送信者のアドレスが SPF (Sender Policy Framework : 送信者ポリシーフレームワーク)ポリシーに準拠しているかどうかを、メッセージの送信に使用されたサーバが含まれているドメインでチェックします。
- メッセージテキストに含まれているアドレスおよびサイトへのリンクが、スパムURLリアルタイムブロックリストデータベース(www.surbl.org)に含まれているかどうかをチェックします。
- UDS (Urgent Detection System : 緊急検知システム)技術を使用してメールメッセージを認識します。

UDS 以外の上記のすべてのチェックは、DNS プロトコルを使用して行われるため、基本的にネットワークの追加設定は必要ありません。

2.2.4. 緊急検知システム

緊急検知システムは、カスペルスキーラボスが開発およびサポートを行う独自のスパム検出技術です。この技術は、以下の原理に基づいています。

1. 分析対象メッセージからプロパティの集合が選択されます。このプロパティの集合を使用して、メッセージを特定することができます。プロパティの集合には、ヘッダ情報、テキスト部分、および処理メッセージに関するその他の情報が含まれます。

2. フィルトレーションサーバは、収集されたプロパティを使用して小さい UDS 要求を生成し、それをカスペルスキーラボスのいずれかの UDS サーバに送信します。



この製品は、処理メールの受信者やテキストの表示を可能にするデータを外部のサーバに送信することはありません。したがって、この方法を使用しても、お客様の情報の安全性または機密性が危険にさらされることはありません。

3. UDS サーバが、既知のスパムが登録されているデータベースを使用して、受信した要求をチェックします。受信した要求が既知のスパムサンプルと一致した場合は、そのメールがスパムである可能性が高いことを知らせるメッセージが、フィルトレーションサーバに送信されます。この情報に基づいて、メールにステータスが割り当てられます。



UDS 技術により、コンテンツフィルトレーションデータベースを更新する前に、既知のスパムをフィルタリングできるようになりました。

フィルトレーションサーバは、通信ポート 7060 を使用して、UDP 経由でカスペルスキーラボスの UDS サーバとやり取りします。UDS を使用するには、フィルトレーションサーバがこのポートを介して送信用の接続を確立できなければなりません。

使用可能な UDS サーバに関する情報が、コンテンツフィルトレーションデータベースに追加されます。メッセージ分析に使用される UDS は、アクセス可能な UDS サーバの応答時間に基づいて自動的に選択されます。

2.3. 認識結果およびメッセージに適用する動作

分析処理の結果、以下のいずれかのステータスがメッセージに割り当てられます。

- **[Spam]** – このメッセージは、スパムである可能性が高いと認識されました。
- **[Probable Spam]** – このメッセージには、スパムであると考えられる何らかの兆候が含まれていますが、確実にスパムであると判断することはできません。
- **[Formal]** – これは公式のメッセージです。たとえば、メールの配信や配信不能またはウイルス感染メッセージについて知らせるメールサーバからの通知などです。メールクライアントから自動的に送信されたメッセー

どもこのカテゴリに含まれます。通常は、これらのメッセージはスパムであるとみなされません。

- **[Trusted]** – このメッセージは、信頼できるソース(内部メールサーバなど)から受信されたメッセージです。管理者は、信頼できるソースのリスト(送信者のホワイトリスト)を作成する必要があります。該当するグループポリシー設定に従って、メールのスキャンを行わないユーザ宛てのメッセージにも、**[Trusted]**ステータスが割り当てられます。
- **[Blacklisted]** – このメッセージは、ブラックリストに含まれているアドレスから受信されました。管理者は、ブラックリストを作成する必要があります。
- **[Not detected]** – このメッセージは、スパムであると認識されませんでした。

各メッセージには、上記のステータスが1つだけ割り当てられます。分析後にメッセージに割り当てられたステータスは、**X-Spamtest-Status-Extended**という特別なヘッダに記録されます。フィルタリング後にメールメッセージに追加されるヘッダの詳細については、113ページのセクション**A.5**を参照してください。認識後、メッセージに対して以下のいずれかの動作が適用されます。

- メッセージの受け入れ
- メッセージまたはそのコピーの別のアドレスへの中継
- メッセージの件名フィールドへのテキストマークの追加
- メッセージに特別なヘッダの追加
- メッセージの削除
- メッセージの拒否

システム管理者は、メッセージのステータスごとに実行する動作を定義できます。



システム管理者は、すべての有益なメールの保存を最優先してください。1通でも重要なメッセージを失うことは、大量のスパムメッセージを受け取ることよりも大きな問題に繋がる可能性があります。必要なメールを失わないようにするために、コンテンツ分析によってスパムまたはスパムの可能性があると思われたメールに関しても、非破壊的な動作のみを適用することをお奨めします。たとえば、件名ヘッダに**[!! SPAM]**などのラベルを追加することをお奨めします。

2.4. コンテンツフィルトレーションデータベース

アプリケーションは、定期的に更新されるコンテンツフィルトレーションデータベースのレコードを使用して、スパムメッセージを認識します。このデータベースには、フィルタリングプロセスで使用されるルールセット、用語、およびメッセージの特徴が格納されています。

コンテンツフィルトレーションデータベースは、更新用モジュールを使用して、カスペルスキーラプスの更新サーバからダウンロードできます。このダウンロードでは、変更箇所があるファイルのみロードされるようになっているため、ダウンロードデータ量を抑えることができます。

新しいスパムメッセージのサンプルが日々出現するため、製品を正常に機能させるには、コンテンツフィルトレーションデータベースを定期的に更新する必要があります。20分おきに更新することをお奨めします。



製品のセットアップが完了したら、すぐにコンテンツフィルトレーションデータベースを更新してください。

2.5. フィルトレーションポリシー

Kaspersky Anti-Spam は、フィルトレーションポリシーを使用して、スパム認識方法、メッセージに適用する動作、および送信者のブラックリストおよびホワイトリストを決定します。

この製品は、デフォルトの一般フィルトレーションポリシーとグループフィルトレーションポリシーからなる2層式のフィルトレーションポリシーを使用します。デフォルトのフィルトレーションポリシーには、スパム認識方法や送信者のブラックリストおよびホワイトリストなど、すべてのグループに共通する設定が含まれています。グループポリシーには、上記の設定に加えて、メッセージのステータスに応じて実行される動作の定義も含まれます。

管理者は、グループポリシーを設定する前に、メッセージ受信者のアドレスがリストされているグループを作成する必要があります。

フィルトレーションポリシーは、つぎのルールに従って適用されます。一般フィルトレーションポリシーは、すべてのグループのデフォルト設定を定義します。グループ設定は、デフォルト設定の値を継承するか、定義しなおします。したがって、たとえば徹底的なメッセージフィルトレーションを必要とするユーザのグループに対して、高度なスパム認識方法を使用して厳密な動作を適用することができます。

認識設定の組み合わせは、コンテンツフィルトレーションデータベースのプロパティと密接に関係します。新種のスパムおよびスパム認識ルールとして、認識設定の組み合わせをデータベースに追加したり変更したりできます。コンテンツフィルトレーションデータベースの更新と同時に、Kaspersky Anti-Spam Control

Center によって提供されるインターフェースにも設定が追加されます。

2.6. Control Center

Control Center は、Web ベースのアプリケーションです。管理者は、このアプリケーションを使用して、Kaspersky Anti-Spam の設定や、アクティビティの制御を行なうことができます。

Control Center では、以下のタスクを実行できます。

- 製品および各コンポーネントの現在のステータスの監視
- ライセンスキーのインストールおよび保護対象ドメインリストの管理
- 処理メッセージに関する統計情報の出力およびエクスポート
- スпамフィルタリングのデフォルトおよびグループポリシーの管理
- フィルトレーションサーバおよびその他の製品コンポーネントの設定

2.7. 監視

Kaspersky Anti-Spam には、フィルトレーションサーバのステータスを制御するための監視モジュールが含まれています。

システムのステータス情報は、Control Center の[Monitoring]タブに表示されます。

The screenshot shows the 'Monitoring - General Status' page in the Kaspersky Anti-Spam Control Center. The interface includes a navigation menu with 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Monitoring' tab is active, displaying a sidebar with links to 'General Status', 'Anti-Spam Engine', 'Updates', and 'License'. The main content area is divided into two sections: 'System Information' and 'Kaspersky Anti-Spam'. The 'System Information' section shows Host Name: mail.test.local, System: FreeBSD 5.4-RELEASE-p7 i386, and Load Average: 0.13. The 'Kaspersky Anti-Spam' section shows Product: Kaspersky Anti-Spam Enterprise Edition, Version: 3.0.0 [0221] KAS30/Release, built at Feb 17 2006, 16:22:45, Anti-Spam Engine: Errors..., Updates: OK, and License: Errors... The footer contains the copyright notice: Copyright © 2002-2006 Kaspersky Lab. All rights reserved.

System Information		12:06
Host Name:	mail.test.local	
System:	FreeBSD 5.4-RELEASE-p7 i386	
Load Average:	0.13	

Kaspersky Anti-Spam	
Product:	Kaspersky Anti-Spam Enterprise Edition
Version:	3.0.0 [0221] KAS30/Release, built at Feb 17 2006, 16:22:45
Anti-Spam Engine:	Errors...
Updates:	OK
License:	Errors...

図 2. Control Center の[Monitoring]タブ

このセクションには、監視システムが追跡するパラメータと製品モジュールからのメッセージが表示されます。これらの情報から、Kaspersky Anti-Spam コンポーネントの現在のステータスを分析することができます。

この監視システムは、実行中に通知やレポートも生成します。監視スクリプトは、定期的に起動され、問題が検出されると、そのことを知らせるメッセージをシステム管理者に送信します。問題が検出されるとすぐにメッセージが送信されるため、管理者の介入を必要とする状況が適宜確実に通知されます。

通知後、問題が解決されなかった場合は、検出されて保留状態になっているすべての問題がまとめられた日次レポートが送信されます。

監視システムによる通知の送信先電子メールアドレスを Control Center で指定する必要があります。

第3章 KASPERSKY ANTI-SPAM のインストール

このセクションでは、プログラムのインストール方法、ホストメールサーバへのクライアントプラグインモジュールの統合方法、および Control Center (製品の管理ツール)へのアクセス設定について説明します。

3.1. インストールの準備

Kaspersky Anti-Spam のインストールを開始する前に、以下の準備を行う必要があります。

- システムが Kaspersky Anti-Spam のハードウェアおよびソフトウェアの要件を満たしていることを確認してください。
- Kaspersky Anti-Spam 3.0 のライセンスキーがあることを確認してください。
- *bzip2* および *perl* がインストールされていることを確認してください。
- 使用しているシステムにインストールされているメールサーバが正常に機能することを確認してください。
- メールサーバの設定ファイルのバックアップを作成します。
- **root** としてシステムにログインします。



メールサーバの負荷が最も小さい時間帯に製品のインストールを行うことをお奨めします。

Kaspersky Anti-Spam のインストールは、以下の 5 つの手順に分かれます。

1. Kaspersky Anti-Spam 配布パッケージのインストール
2. ライセンスキーのインストール
3. メールサーバへのクライアントプラグインモジュールの統合
4. Control Center へのアクセス用 HTTP サーバの設定
5. コンテンツフィルトレーションデータベースの更新および UDS サービスの使用に関する設定

以降のセクションで、上記の手順について詳しく説明します。

3.2. Kaspersky Anti-Spam 配布パッケージのインストール

Kaspersky Anti-Spam 3.0 は、以下のようなインストールパッケージとして配布されます。

- Linuxオペレーティングシステムのほとんどのバージョン(RedHat, SuSe, Mandrake, Fedora, その他)に対応する.rpmパッケージ
- Debian Linux ディストリビューションの.deb パッケージ
- FreeBSD 4.10 オペレーティングシステム用の.tgz パッケージ
- FreeBSD 5.4 オペレーティングシステム用の.tbz パッケージ

コンピュータにインストールされているオペレーティングシステムに応じてインストールパッケージを選択します。

.rpm パッケージから Kaspersky Anti-Spam のインストールを開始するには、コマンドラインで以下のコマンドを入力します。

```
# rpm -i kas-3-<package version>.i386.rpm
```

.deb パッケージから Kaspersky Anti-Spam のインストールを開始するには、コマンドラインで以下のコマンドを入力します。

```
# dpkg -i kas-3-<package version>.i386.deb
```

.tgz パッケージから Kaspersky Anti-Spam のインストールを開始するには、コマンドラインで以下のコマンドを入力します。

```
# pkg_add kas-3-<package version>.tgz
```

.tbz パッケージから Kaspersky Anti-Spam のインストールを開始するには、コマンドラインで以下のコマンドを入力します。

```
# pkg_add kas-3-<package version>.tbz
```

インストール処理では、以下の動作が実行されます。

- Kaspersky Anti-Spam を実行する際に使用される適切な権限を持つ **mailfilt3** ユーザアカウントおよびグループが作成されます。
- Kaspersky Anti-Spam スイートに含まれているすべてのプログラムが、*/usr/local/ap-mailfilter3* ディレクトリにインストールされます。
- フィルトレーションマスタプロセス(*ap-process-server*)、SPFデーモン(*ap-spf*)、ライセンスモジュール(*kas-license*)、およびHTTPサーバ(*kas-thttpd*)をオペレーティングシステムの起動時に自動的に起動するスクリプトが作成されてインストールされます。
- 必要なプログラムおよびサービスが起動されます。

- **mailflt3** アカウントの場合、コンテンツフィルトレーションデータベースの更新をダウンロードするスクリプトとフィルトレーションサーバアクティビティを監視するスクリプトを自動的に実行する cron タスクが作成されます。

フィルトレーションサーバのセットアップが完了したら、ライセンスキーをインストールし、ホストメールサーバに Kaspersky Anti-Spam を統合します。

3.3. ライセンスキーのインストール

購入したライセンスに対応するライセンスキーが、Kaspersky Anti-Spam の配布パッケージに付属しています。



何らかの理由でライセンスキーがない場合は、カスペルスキーラボの技術サポートサービスに連絡してください(カスペルスキーラボの Web サイトの「**Services/Technical Support**」セクションを参照)。



Control Center を使用して新しいライセンスキーをインストールするには、以下の手順を実行します。

1. Web ブラウザのアドレス行に「**http://localhost:3080/**」と入力して **Control Center** に接続します。接続用のユーザ名として「**admin**」、パスワードとして「**admin**」を入力します。
2. ライセンスキーの管理を行う**[License]**→**[License Keys]**ページを開きます。
3. ページ下部の**[Install a New License Key]**セクションの下にあるフィールドを使用してライセンスキーファイルのパスを指定するか、**[Choose]**ボタンをクリックして必要なファイルを選択します。
4. **[Apply]**ボタンをクリックします。

ライセンスキーがインストールされていない場合や、インストールされたキーが無効な場合、Kaspersky Anti-Spam によるメールのフィルタリングは行われません。その場合、メールサーバのパフォーマンスに影響はありませんが、分析されていないメールトラフィックが送信されます。

この製品は、保護対象ドメインリストにアカウントが追加されている受信者のメールのみフィルタリングすることを忘れないでください。



Kaspersky Anti-Spam の使用を開始する前に、保護対象ドメインのリストを作成してください。

詳細については、43ページのセクション**4.3.4**を参照してください。

3.4. メールサーバへの Kaspersky Anti-Spam の統合

クライアントプラグインモジュールをインストールして設定ファイルに必要な変更を加えることにより、ホストメールサーバに Kaspersky Anti-Spam が統合されます。

これらの作業は、共通設定スクリプトによって自動的に実行されます。共通スクリプトで統合できない場合は(メールサーバが標準的に設定されていない場合など)、メールサーバ固有の設定スクリプトを使用して統合します。

サポート対象の各メールサーバにクライアントプラグインモジュールを統合する方法と、それらの設定ファイルの変更方法の詳細については、83ページの付録 A.2を参照してください。



サーバにインストールされているメールサーバに *Kaspersky Anti-Spam* を統合するには、共通設定スクリプトを実行します。

```
# /usr/local/ap-mailfilter3/bin/MTA-config.pl
```

このスクリプトは、メールサーバの種類を特定し、設定ファイルに必要な変更を加えます。

しかし、メールサーバが標準外の場所にインストールされている場合や、デフォルト以外の設定を使用している場合は、*MTA-config.pl* スクリプトが設定ファイルを見つけられない場合があります。そのような場合は、メールサーバ固有の設定スクリプトを使用します。

- Kaspersky Anti-Spam を Sendmail に統合するには、**root** として以下のコマンドを実行します。

```
# /usr/local/ap-mailfilter3/bin/config-sendmail.pl <path>
```

path は、Sendmail 設定ファイルのパスです。

- Kaspersky Anti-Spam を Postfix に統合するには、**root** として以下のコマンドを実行します。

```
# /usr/local/ap-mailfilter3/bin/config-postfix.pl <path>
```

path は、*master.cf* (Postfix 設定ファイル)のパスです。

- Kaspersky Anti-Spam を Exim に統合するには、**root** として以下のコマンドを実行します。

```
# /usr/local/ap-mailfilter3/bin/config-exim.pl <path>
```

path は、Exim 設定ファイルのパスです。



Exim メールサーバへの Kaspersky Anti-Spam の統合は、Debian Linux ディストリビューションの場合と異なる点がある。

いくつかあります。適切に統合するために、`/usr/local/ap-mailfilter3/bin/config-exim-debian.pl` スクリプトを使用してください。詳細については、92ページのセクションA.2.4.2を参照してください。

- Kaspersky Anti-Spam を Qmail に統合するには、**root** として以下のコマンドを実行します。

```
# /usr/local/ap-mailfilter3/bin/config-qmail.pl <path>
```

path は、Qmail 設定ファイルのパスです。



Qmail で **qmailq** アカウントおよび **qmail** グループが使用されている場合のみ(デフォルトで使用される)、`config-qmail.pl` スクリプトを実行して Qmail に Kaspersky Anti-Spam を正しく統合できます。

Exim (kas-exim クライアントプラグインモジュールを使用)および CommuniGate Pro に Kaspersky Anti-Spam を統合する場合は、管理者が統合作業を手動で行う必要があります。

これらのクライアントモジュールの特性および適用可能なインストール方法については、83ページのセクション以降を参照してください。

統合を元に戻してメールサーバの設定を復元する方法については、77ページのセクションを参照してください。

3.5. Control Center へのアクセス設定

製品のセットアップ完了時に、`kas-thttpd` サービスが実行されます。このサービスにより、<http://127.0.0.1:3080/> の Control Center へのローカルアクセスが可能になります。登録には以下の情報が使用されます。

- ユーザ名 : **admin**
- パスワード : **admin**



Kaspersky Anti-Spam のインストール完了後に、Control Center にアクセスするためのユーザ名およびパスワードを必ず変更してください。デフォルト値を使用していると、システムの安全が脅かされる可能性があります。

また、Control Center への接続に使用するポートも変更することをお奨めします。

ユーザ名およびパスワードは、CGI スクリプト用の Control Center ディレクトリである `/usr/local/ap-mailfilter3/control/www/` にある `.htpasswd` ファイルに保存されます。

新規ユーザを作成したり既存のパスワードを変更したりするには、Kaspersky

Anti-Spam に含まれている *kas-htpasswd* ユーティリティを使用します。このユーティリティの起動時に、作成するユーザやパスワードを変更する既存のユーザのパスワードおよび名前が含まれているファイルのパスを、以下のように指定します。

```
# /usr/local/ap-mailfilter3/bin/kas-htpasswd
/usr/local/ap-mailfilter3/control/www/.htpasswd <user name>
```

上記のコマンドを実行すると、指定されたユーザのパスワードを入力するよう要求されます。

指定されたユーザのパスワードを保存するファイルを新規作成するには、`-c` コマンドラインオプションを使用します。

```
# /usr/local/ap-mailfilter3/bin/kas-htpasswd -c
/usr/local/ap-mailfilter3/control/www/.htpasswd <user name>
```

パスワードの変更は、*.htpasswd* ファイルの変更後すぐに有効になります。



Control Center にアクセスするためのパスワードは、暗号化された *.htpasswd* ファイルに保存されます。

Control Center への接続に使用されるインタフェースおよびポート番号は、*/usr/local/ap-mailfilter3/etc/kas-thttpd.conf* ファイル内で、それぞれ **host** および **port** パラメータを使用して指定します。たとえば、以下のような値を指定します。

```
host=0.0.0.0
port=3080
```

この場合、Control Center は、すべてのサーバインタフェースのポート 3080 で、接続が入ってくるのを待ち受けます。デフォルトでは、Control Center は、Kaspersky Anti-Spam がインストールされているサーバからのみアクセスできます (**host** パラメータに **127.0.0.1** が設定されている)。

ポート番号を変更したら、Control Center の設定をリロードします。Linux ディストリビューションの場合、以下のコマンドを実行します。

```
# /etc/init.d/kas3-control-center restart
```

FreeBSD の場合、以下のコマンドを実行します。

```
/usr/local/etc/rc.d/kas3-control-center.sh restart
```

3.6. コンテンツフィルトレーションデータベースの更新および UDS の使用に関する設定

デフォルトでは、Kaspersky Anti-Spam のインストール後、コンテンツフィルトレーションデータベースの更新および UDS の使用は無効になっています。データベースの更新を許可し、UDS を有効化するには、以下のように

`enable-updates.sh` スクリプトを実行します。
/usr/local/ap-mailfilter3/bin/enable-updates.sh

```
Restarting as mailflt3
Enabling UDS...
uds-rtts finished successfully
Enabling automatic updates...
Install crontab for user mailflt3 - ok
```

```
=====
You can adjust automatic updates settings via control center.
```

```
=====
Automatic updates and UDS are now enabled.
```

また、Control Center インタフェースから、コンテンツフィルトレーションデータベースの更新を有効化したり(51ページのセクション4.4を参照)、UDSサービスを有効化したりできます(60ページのセクション4.5.4を参照)。

第4章 スпамフィルトレーションサーバの管理

Kaspersky Anti-Spam を使用して、不要なスパムメールからメールトラフィックを保護することができます。このアプリケーションの主機能である以下のタスクにより、保護が提供されます。Kaspersky Anti-Spam によって実行されるタスクは、主に以下の3つのグループに分けられます。

- スпамからのメールトラフィックの保護
- スпам検出に使用されるコンテンツフィルトレーションデータベースの更新
- アンチスパムエンジンアクティビティの監視

各グループには、類似するタスクが含まれています。この章では、典型的なタスクについて詳しく説明します。管理者は、組織固有の要件に合わせて、これらのタスクを組み合わせて機能を強化することができます。

本書では、コマンドラインからローカルでタスクを設定および実行する方法と、Control Center を使用した製品管理方法について説明します。

4.1. Kaspersky Anti-Spam コンポーネントの起動および管理

フィルタリングマスタプロセス(*ap-process-server*)、ライセンスングモジュール(*kas-license*)、および SPF デーモン(*ap-spf*)などのフィルトレーションサーバの主要コンポーネントは、特別なスクリプトによってオペレーティングシステムの起動時に起動されます。このスクリプトは、オペレーティングシステムが Linux か FreeBSD かによって名前と場所が異なります。Linux オペレーティングシステムは、*/etc/init.d* ディレクトリにある *kas3* スクリプトを使用し、FreeBSD オペレーティングシステムは、*/usr/local/etc/rc.d* ディレクトリにある *kas3.sh* スクリプトを使用します。

管理者は、以下のコマンドラインパラメータと共にこれらのスクリプトを使用することにより、フィルトレーションサーバの主要コンポーネントの起動、停止、再起動を行うことができます。

[start] – フィルトレーションサーバの主要コンポーネントを起動します。

[stop] – フィルトレーションサーバの主要コンポーネントの処理を停止します。

[restart] – フィルトレーションサーバの主要コンポーネントを再起動します。**stop** 動作を実行してから **start** 動作を実行した場合と同じです。Kaspersky Anti-SpamのControl Centerへのアクセスを可能にする`kas-tthttpd`サービスは、`kas3-control-center` スクリプト (Linux の場合) および `kas3-control-center.sh`スクリプト(FreeBSDの場合)によって起動されます。`kas-tthttpd`サービスを起動、停止、再起動するには、このスクリプトと共に`kas3`スクリプトのところで説明したコマンドラインパラメータを使用します。

4.2. Kaspersky Anti-Spam Control Center

Control Center は、Kaspersky Anti-Spam を管理するためのメインツールです。Control Center は、Web ベースのアプリケーションです。このアプリケーションを使用して、フィルトレーションサーバの運用で使用されるパラメータをリモートで設定することができます。このセクションでは、このアプリケーションのすべてのインタフェースコンポーネントについて詳しく説明します。

The screenshot displays the Kaspersky Anti-Spam Control Center interface. At the top, there is a navigation bar with tabs for Monitoring, Statistics, Policies, Settings, and License. The 'Monitoring' tab is active, showing a 'Monitoring' sidebar with links for General Status, Anti-Spam Engine, Updates, and License. The main content area is divided into two sections: 'System Information' and 'Kaspersky Anti-Spam'. The 'System Information' section, timestamped 12:06, lists Host Name (mail.test.local), System (FreeBSD 5.4-RELEASE-p7 i386), and Load Average (0.13). The 'Kaspersky Anti-Spam' section lists Product (Kaspersky Anti-Spam Enterprise Edition), Version (3.0.0 [0221] KAS30/Release, built at Feb 17 2006, 16:22:45), Anti-Spam Engine (Errors...), Updates (OK), and License (Errors...). A footer at the bottom indicates Copyright © 2002-2006 Kaspersky Lab, All rights reserved.

図 3. Kaspersky Anti-Spam Control Center

メインウィンドウの上部にあるタブを使用して、Control Center の以下の各機能セクションにすぐにアクセスできます。

- **[Monitoring]** – このセクションには、フィルトレーションサーバのコンポーネントのステータスに関する情報が表示されます。これらの情報から、発生している問題を特定できます。

- **[Statistics]** – このセクションには、統計レポートが表示されます。これらの情報から、システムによって処理されたメッセージ数を分析できます。
- **[Policies]** – このセクションを使用して、スパムフィルタリングポリシーをカスタマイズします。
- **[Settings]** – このセクションには、アンチスパムエンジン、Control Center、およびコンテンツフィルトレーションデータベースを更新するサブシステムの設定が表示されます。
- **[License]** – このセクションを使用して、Kaspersky Anti-Spamのライセンスを管理したり、製品の管理権限を持つユーザを登録したりできます。

メインウィンドウの左側部分には、現在のセクション内のページのリストがメニューとして表示されます。このメニューの内容は、選択されたセクションに応じて変わります。

上記のナビゲーション手段の他に、メインウィンドウの上部には、Control Center セクション階層内での現在のページのパスを示すアドレス行も表示されます。次に、フィルトレーションサーバおよび各コンポーネントの管理に関する主要タスクについて説明します。

4.3. フィルトレーションポリシーの管理

Kaspersky Anti-Spam の主な機能は、迷惑メールの検出およびフィルトレーションです。この管理システムでは、スパムの認識およびメッセージの処理に関する設定を、効果的に組み合わせて提供します。

メッセージフィルトレーションポリシーの設定は、Control Center の **[Policies]** セクションに表示されます。

[Policies]メニューには、以下のサブセクションがあります。

- **[Common]** – 一般フィルトレーションポリシーの設定。このサブセクションには、さらに以下のセクションが含まれています。
 - **[Default Rules]** – スパム認識ルールを管理するセクション。
 - **[Black List]** – ブロックする受信メールの送信元アドレスのリストを管理するセクション。
 - **[White List]** – 信頼できるアドレスのリストを管理するセクション。このリストに含まれるアドレスからのメッセージは、スパムチェックが行われません。
 - **[DNS Black Lists]** – 使用するDNSBLサービスのリストを管理するセクション。

- **[Protected Domains]**
- **[Groups]** – ユーザグループ、各グループに適用する認識ポリシー、およびメッセージに適用する動作セットの設定。
 - **[Group list]** – ユーザグループを管理するセクション。グループを作成および削除したり、グループプロパティエディタを起動したりできます。

グループポリシーエディタで、グループポリシーのパラメータを設定できます。このエディタは、**[Group list]**ウィンドウから起動します。

[Build]メニューの**[Rebuild All Policies]**リンクを使用して、フィルタリングポリシーのコンパイル(構成設定の読み込みおよび適用)を強制的に実行できます。たとえば、フィルトレーションポリシーの設定がアプリケーションによって正しく読み込まれなかった場合などに、コンパイルを強制実行して設定を更新する必要があります。

4.3.1. 一般フィルトレーションポリシー

[Default Rules] (図4を参照)セクションには、すべてのグループに共通するデフォルトフィルトレーションポリシーの設定が含まれています。このセクションを表示するには、**[Policies]**セクションに表示される**[Common]**メニューの**[Default Rules]**リンクを使用します。

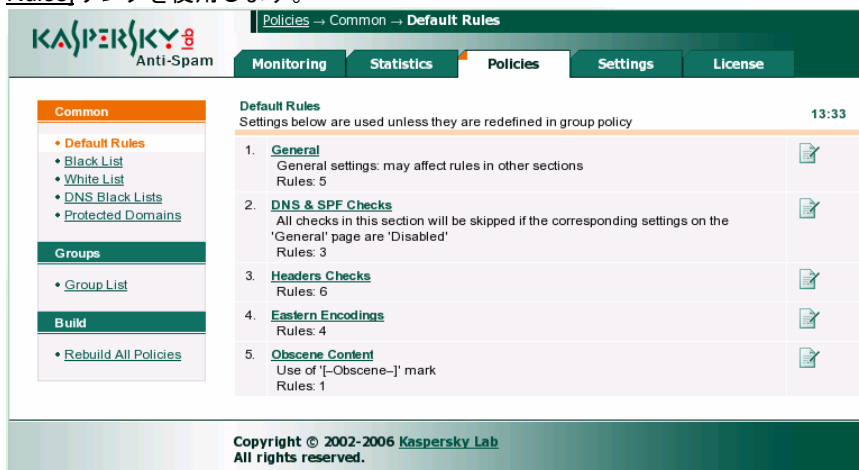


図 4. デフォルトフィルトレーションポリシーの設定

スパム認識ルールの設定は、その機能性に応じていくつかのセクションにグルー



分けられています。メインページには、これらのセクションのリストが表示されます。



設定と機能セクションの組み合わせは、コンテンツフィルトレーションデータベースによって指定されます。データベースを更新すると、利用可能なセクションおよびパラメータのセットが変わる場合があります。

リストには、セクションタイトルの他に以下の情報が表示されます。

- セクションの簡単な説明
- セクション内のルール数
- コンテンツフィルトレーションデータベースのオリジナル設定と比較して、変更が加えられているルールの数

各セクションの説明の右側に、そのセクションに含まれているルール用のエディタを開くボタン  があります。変更されたルールが含まれているセクションのボタンは、オレンジ色で強調表示されます。このボタンをクリックすると、ページが表示され、フィルトレーションポリシーを編集できます。ポリシーエディタは、機能セクションのタイトルをクリックして起動することもできます。  ボタンをクリックすると、セクション内の変更がキャンセルされます。

4.3.1.1. [General]セクション

[General]セクションのルールを設定するには、デフォルトフィルトレーションポリシーールールのリストでセクションタイトルをクリックします(図5を参照)。

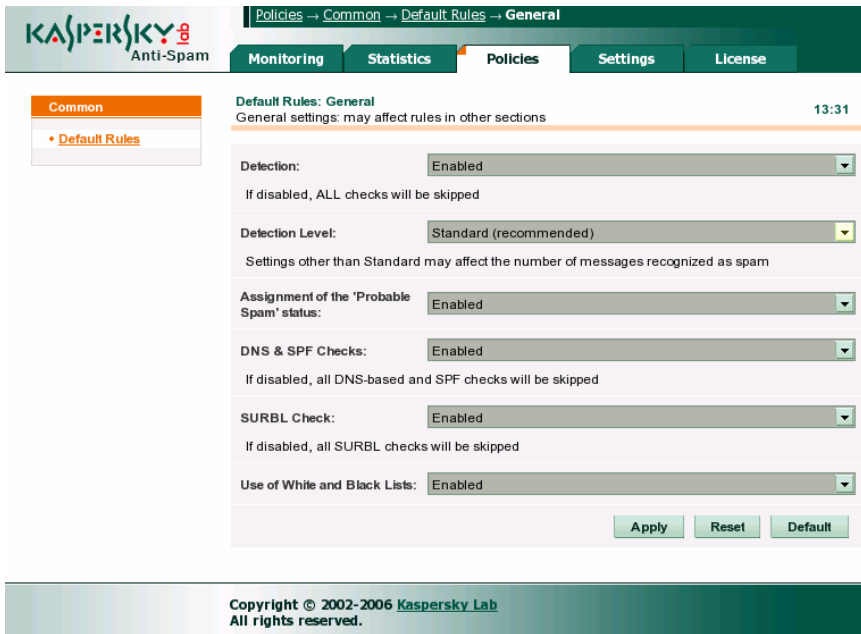


図 5. デフォルトフィルトレーションポリシーの[General]ルールセクション

[General]セクションでは、以下のパラメータを設定できます。

- **[Detection]**は、メッセージのスパムチェックを行うかどうかを定義します。スパム認識を無効にすると、すべてのメッセージに**[Trusted]**ステータスが割り当てられず(ステータスの詳細については、16ページのセクション2.3を参照)。



共通ポリシーレベルでスパム認識を無効にすることはお奨めしません。製品のテスト中に、少数のユーザグループのみスパムをフィルタリングする必要がある場合などに、この機能が役立つ場合があります。

- **[Detection Level]**は、どの程度厳格にスパム認識を行うかを定義します。アプリケーションは、フィルトレーションモジュールがメッセージ内で検出した複数の兆候に基づいて、メッセージにスパムが含まれているかどうかを決定します。この設定は、メッセージのステータスを設定する前に、フィルタがこれらの兆候をどのように解釈するかを指定します。フィルトレーションポリシーには、**[Minimum]**、**[Standard]**、**[High]**、および**[Maximum]**の 4 つの検出レベルがあります。このレベルが高いほど、少

ない数の兆候でメッセージがスパムであると認識されます。検出レベルを低くすると、同じ兆候を持つメッセージでも、スパムの疑いがあるとみなされたり([**Probable Spam**]ステータス)、スパムでないともなされたりします。



[Standard]検出レベルを使用することをお奨めします。

Kaspersky Anti-Spam がスパムメッセージを検出しない場合や、スパムメッセージをスパムの疑いがある([**Probable Spam**]ステータス)と認識する場合などに、検出レベルを高くします。ただし、検出レベルを高くすると、通常のメッセージがスパムであると認識されることがあるため、誤報の発生確立が高くなります。

検出レベルを低くすると、誤報の確立は低くなります。ただし、スパムメッセージがフィルタを通過する可能性が高くなります。



フィルトレーション結果は、検出レベルの他に、使用するスパム認識方法の影響も受けます。誤報が発生する場合は、スパム認識方法も見直す必要があります。

- **[Assignment of the 'Probable Spam' status]** – [**Probable Spam**]ステータスの割り当てを有効または無効にします。このパラメータに[**Disable**]が設定されている場合、Kaspersky Anti-Spam はメールメッセージに[**Probable Spam**]ステータスを割り当てません。
- **[DNS & SPF Checks]** – DNS 内の送信者情報のチェックおよび DNS ベースのサービス(DNSBL や SPF など)を使用するチェック。



DNS チェックおよび DNS ベースのチェックを行うと、メッセージの処理速度がかなり遅くなる可能性があります。フィルタのパフォーマンスが著しく低下する場合は、この機能を無効にしてください。

このパラメータは、フィルトレーションサーバがDNSサービスを使用するかどうかを指定します。個々のサービスの有効/無効については、[**DNS & SPF Checks**]セクションで指定できます(35ページのセクション**4.3.1.2**を参照)。

DNSBLサービスおよびその使用方法については、41ページのセクション**4.3.3**を参照してください。


- **[SURBL Check]** – SURBL サービスの使用。
- **[Use of White and Black Lists]** – 信頼できるソースおよびブロックされるソースのIPアドレスおよび電子メールアドレスが含まれているホワイトリストおよびブラックリストの使用。ホワイトリストおよびブラックリ

ストの使用方法については、39ページのセクション4.3.2を参照してください。

[Apply]ボタンは、設定を保存します。このボタンをクリックすると、フィルトレーションポリシーが保存されてコンパイルされ、フィルトレーションモジュールが再起動されます。それにより、入力された変更内容がすぐに有効になります。

[Reset]ボタンは、パラメータを最初の値に戻します(つまり、保存されていない変更をキャンセルする)。

[Default]ボタンは、設定をコンテンツフィルトレーションデータベースに指定されているデフォルト値に戻します。また、デフォルトフィルトレーションポリ

シールールのリストで、セクションタイトルの反対側にある  ボタンを使用してデフォルト値に戻すこともできます。

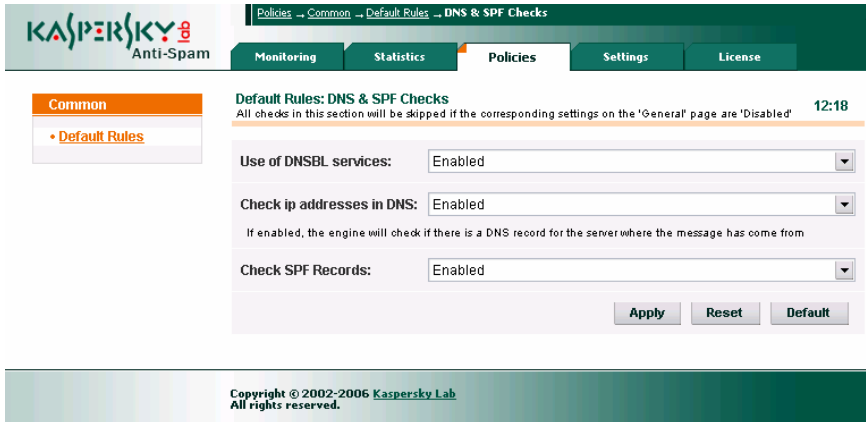
一般デフォルトポリシールールのリストに戻るには、**[Apply]**ボタンをクリックするか(現在の変更を保存する場合)、または**[Common]**メニューの**[Default Rules]**リンクを使用します(変更を保存しない場合)。

4.3.1.2. *[DNS & SPF Checks]*セクション

[DNS & SPF Checks] (図6を参照)セクションには、スパム認識に使用する外部サービスを定義する設定が含まれています。

このセクションのパラメータを使用して、以下の機能を有効/無効にすることができます。

- **[Use of DNSBL services]** – DNSBLサービスセットを使用する、送信者のIPアドレスのチェック。このチェックに使用するサービスのリストは、**[Policies]**→**[Common]**→**[DNS Black Lists]**ページでカスタマイズできます。詳細については、41ページのセクション4.3.3を参照してください。
- **[Check ip addresses in DNS]** – 送信者のIPアドレスがDNSに存在するかどうかのチェック(DNS逆引き)。
- **[Check SPF Records]** – SPFを使用する、送信者のIPアドレスのチェック。



Policies → Common → Default Rules → DNS & SPF Checks

Monitoring Statistics Policies Settings License

Common

- Default Rules

Default Rules: DNS & SPF Checks 12:18

All checks in this section will be skipped if the corresponding settings on the 'General' page are 'Disabled'

Use of DNSBL services: Enabled

Check ip addresses in DNS: Enabled

If enabled, the engine will check if there is a DNS record for the server where the message has come from

Check SPF Records: Enabled

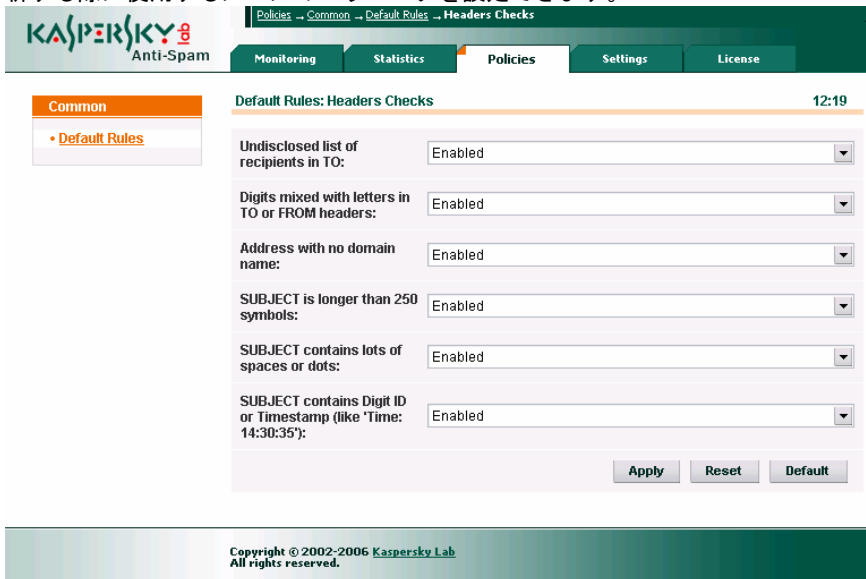
Apply Reset Default

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

図 6. [DNS & SPF Checks]セクション

4.3.1.3. [Headers Checks]セクション

[Headers Checks]セクション(図7を参照)では、メールメッセージのヘッダを分析する際に使用するルールのパラメータを設定できます。



Policies → Common → Default Rules → Headers Checks

Monitoring Statistics Policies Settings License

Common

- Default Rules

Default Rules: Headers Checks 12:19

Undisclosed list of recipients in TO: Enabled

Digits mixed with letters in TO or FROM headers: Enabled

Address with no domain name: Enabled

SUBJECT is longer than 250 symbols: Enabled

SUBJECT contains lots of spaces or dots: Enabled

SUBJECT contains Digit ID or Timestamp (like 'Time: 14:30:35'): Enabled

Apply Reset Default

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

図 7. デフォルトフィルトレーションポリシールールの[Headers Checks]セクション

このセクションでは、Kaspersky Anti-Spam がメッセージヘッダの分析に使用す

るルールをすべてリストしているわけではありません。適用すると、特定のスパムの兆候がある有益なメールを除去する可能性があるルールのみリストしています。以下の兆候がリストされています。

- **[Undisclosed list of recipients in TO]** – 宛先ヘッダに非公開の受信者リストが存在します。
- **[Digits mixed with letters in TO or FROM headers]** – 多くの場合、スパム配布プログラムは、数字の集まりを含む自動生成アドレスを送信者や受信者のアドレスとして使用します。メールサーバのユーザのアドレスに数字が含まれていない場合は、このルールを有効にすることをお奨めします。
- **[Address with no domain name]** – スパマーは、不完全なアドレス(メールアドレスドメインを省略したアドレス)を使用することがよくありますが、通常の電子メールプログラムは、ドメインを含む完全な電子メールアドレス(`user@domain.com`など)を指定します。不完全なアドレスを使用したメッセージの配信を実際に許可している受信者に対しては、このルールを無効にすることをお奨めします。
- **[SUBJECT is longer than 250 symbols]** – 多くのスパム配布プログラムは、メールフィルタを通過するために、件名フィールドに長い(250文字以上)ランダムな文字または単語の羅列を挿入します。メールシステムでそのようなメッセージの配信を許可する場合は、このルールの使用を無効にします。
- **[SUBJECT contains lots of white space or dots]** – 多くのスパム配布プログラムは、メッセージヘッダにたくさんのスペースやドットを挿入します。メールシステムでそのようなメッセージの配信を許可する場合は、このルールの使用を無効にします。
- **[SUBJECT contains DIGIT ID or Timestamp (like 'Time: 14:30:35')]** – メッセージの件名に数字ベースのIDやタイムスタンプを追加する方法も、自動スパムソフトウェアがアンチスパムフィルタを通過するために使用する1つの方法です。

各ルールの右側にあるドロップダウンリストを使用して、ルールを有効([Enabled])または無効([Disabled])にできます。



アプリケーションは、最終的には複数のさまざまな兆候からステータスの割り当てを決定します。したがって、ここで個別または複数のルールを有効/無効にすることで、メッセージが完全にスパムであると認識されたり、反対にフィルトレーションサーバで許可されたりするわけではありません。これらのルールを設定することにより、メッセージ形式の認識において、誤りが発生する確率が低くなります。

これらのルールの有効/無効は、デフォルトフィルトレーションポリシー内のすべてのユーザ、または特定のグループポリシー内のユーザグループに対して指定できます。

4.3.1.4. [Eastern Encodings]セクション

[Eastern Encodings]セクション(図8を参照)では、スパムとみなされずにメールシステム内の受信者への配信を許可するメッセージの言語およびエンコードを指定できます。

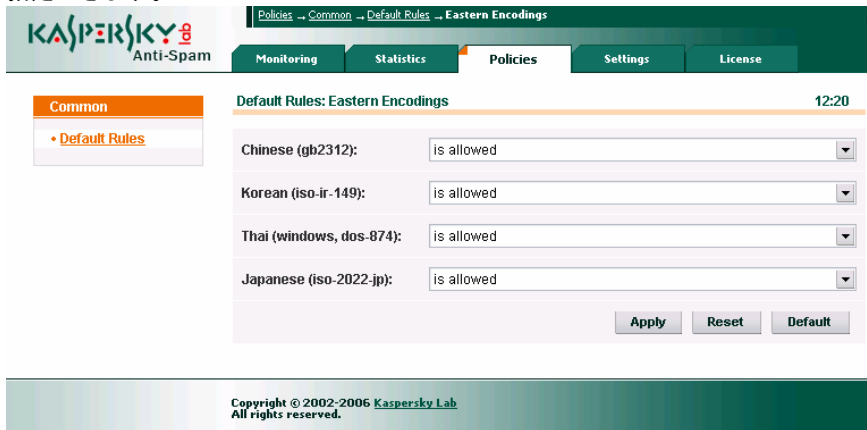


図 8. デフォルトフィルトレーションポリシールールの[Easter Encodings]セクション

本バージョンでは、アジア言語(中国語、韓国語、タイ語、日本語)を認識してスパムを制御できます。

メールシステムのユーザがこれらの言語をメールで使用する場合、該当する言語のドロップダウンリストで、[is allowed]オプションを選択します。これらの中にメールシステムのユーザが使用しない言語がある場合は、その言語に[is treated as suspicious]を設定します。

4.3.1.5. [Obscene Content]セクション

[Obscene Content]セクション(図9を参照)では、わいせつな言葉が含まれているメッセージに印を付けるかどうかを定義します。Kaspersky Anti-Spamは、ロシア語および英語のわいせつな言葉を認識できます。



図 9. デフォルトフィルトレーションポリシールールの[Obscene Content]セクション

[Message with obscene words and phrases]パラメータに[mark in Subject]を設定すると、わいせつな言葉が含まれたすべてのメッセージの件名に[--Obscene--]という印が付きます。

4.3.2. ホワイトリストおよびブラックリストの管理

信頼できる送信者のリスト([White List])には、スパムチェックの必要がない信頼できるメッセージソースとなるアドレスを明示的に指定します。このリストには、社内でメールを転送する際に使用するメールサーバのIPアドレスや、内部メーリングリストのアドレスなどを追加できます。ホワイトリストに含まれている送信者からのメールには、[Trusted]ステータスが割り当てられます。

ブロックされる送信者のリスト([Black List])には、ホワイトリストの反対の意味があります。フィルトレーションサーバの管理者は、スパマーが大量メール送信に使用するアドレスをこのリストに追加することができます。ブラックリストに含まれているアドレスから送信されたメッセージには、[Blacklisted]ステータスが割り当てられます。

これらのリストは、同じ方法で管理できます。このセクションでは、例としてホワイトリストの設定方法について説明します(図10を参照)。

信頼できる送信者のホワイトリストを編集するフォームは、[Policies]→[Common]→[White List]メニューからアクセスできます(ブロックされる送信者のリストは[Policies]→[Common]→[Black List]からアクセス)。

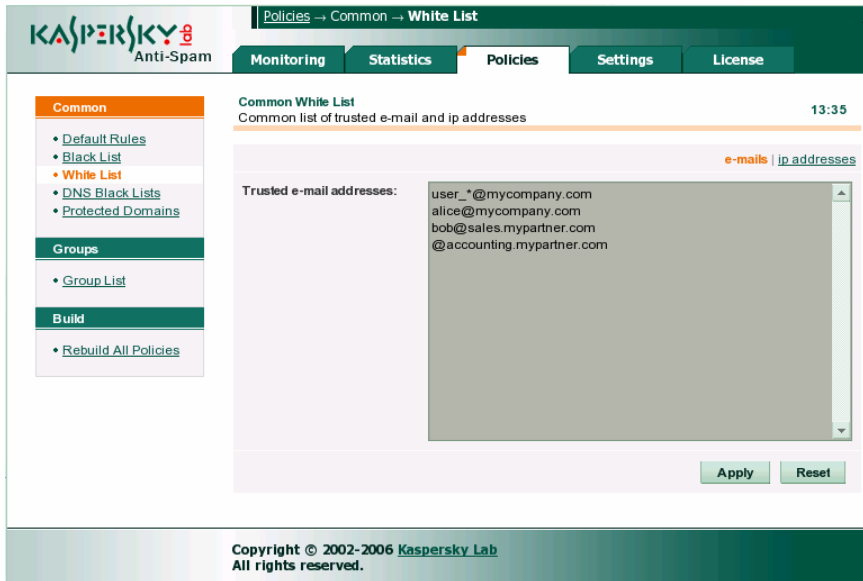


図 10. ホワイトリストの設定ページ

信頼できる送信者のリストは、電子メールアドレスのリストとIPアドレスのリストで設定されます。ページ中央のテキストフィールドにアドレスを入力できます。**[e-mails | ip addresses]**スイッチを使用して、表示するホワイトリストのレコードタイプを選択します。

[Apply]ボタンをクリックすると、入力した情報が保存されます。保存していない変更をキャンセルするには、**[Reset]**ボタンを使用します。



[e-mails | ip addresses]スイッチを使用する前に変更を保存してください。表示を切り替えると、保存されていない変更がすべて失われます。

電子メールアドレスは、以下の形式で入力します。

- *user@domain* – 特定のアドレスを指定する場合
- *@domain* – **[domain]**ドメイン内のすべての電子メールアドレスを指定する場合

電子メールアドレスには、以下のワイルドカードを使用できます。

- * (アスタリスク) – 任意の長さの文字列
- ? (クエスチョンマーク) – 任意の 1 文字

たとえば、「`user*@mycompany.com`」というレコードは、`mycompany.com`メールアドレス内の「`user`」で始まるアドレスを表します。

IP アドレスは、以下のバリエーションが使用可能な CIDR 表記で登録します。

- `aaa.bbb.ccc.ddd` – 特定のIPアドレス(「`192.168.0.17`」など)
- `aaa.bbb.ccc.ddd/mm` – 番号およびマスクを指定したサブネットアドレス(「`192.168.0.0/16`」など)

リスト内のアドレスは、スペース、改行記号、カンマ、セミコロンで区切ることができます。

4.3.3. 使用する DNSBL サービスのリストの管理

DNSBL サービスのリストを管理するページを開くには、[Policies]セクションに表示される[Common]メニューの[DNS Black Lists]リンク(図11を参照)を使用します。

使用する DNSBL のリストの設定は、デフォルトフィルトレーションポリシーに適用されます。ユーザグループごとに DNSBL ベースのチェック結果を使用するかどうかを後で指定できます。使用するサービスのリストは、すべてのユーザグループに共通です。

Policies → Common → DNS Black Lists

Monitoring Statistics Policies Settings License

Common

- Default Rules
- Black List
- White List
- **DNS Black Lists**
- Protected Domains

Groups

- Group List

Build

- Rebuild All Policies

Default DNS Black Lists
List of default DNS-based Black List services 17:02

	Hostname	Rate
1	dnsbl.njabl.org	40
2	bl.spamcop.net	40
3	intercept.datapacket.net	30
4	bl.spamcannibal.org	30
5	dnsbl-1.uceprotect.net	40

Default list:

User Defined DNS Black Lists
List of user defined DNS-based Black List services

	Hostname	Rate
+	<input type="text"/>	<input type="text"/>

Apply Reset

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

図 11. DNSBL サービスリストの設定ページ

ページ中央に、使用するサービスのリストが表示されます。DNSBL サービスごとに、そのサーバへのアクセスに使用するアドレスと評価を指定します。Kaspersky Anti-Spam は、このリスト内のすべてのサービスに要求を送信します。指定された IP アドレスは迷惑メールの送信に使用されるアドレスであるという認識結果がサービスから返されると、その結果が評価として合計されます。使用された DNSBL サービスの評価の合計が 100 を超えた場合、その送信者はブラックリストに含まれているとみなされ、他のチェック結果に関係なく、そのメッセージに**[blacklisted]**ステータスが割り当てられます。一定の検出レベルでは、ブラックリストに送信者が含まれていることを発見したサービスの評価の合計が 100 未満の場合でも、アプリケーションによる分析が行われます。その場合、ブラックリストに含まれている送信者に関する情報がスパムの兆候として補足的に使用され、他の分析方法でさらにスパムの兆候があることが明らかになった場合は、そのメッセージがスパムであると認識されます。DNSBL サービスのリストでは、以下の操作を実行できます。

- デフォルト DNSBL サービスの有効化と無効化
- ユーザ定義 DNSBL サービスへの追加と削除、および評価値の変更

これらの操作について詳しく説明します。

- **デフォルト DNSBL サービスの有効化/無効化**

Default list: から有効/無効(Enabled/Disabled)を選択して **[Apply]** をクリックして保存します。

- **ユーザ定義DNSBLサービスのリストに追加するには、以下の手順を実行します。**
 1. 追加するサービスのアドレスを、リスト下部にある+マークが付いた空の行に入力します。
 2. サービスの評価を入力します。
 3. **[Apply]**をクリックして入力を保存します。
- **ユーザ定義 DNSBL サービスの評価を変更するには、以下の手順を実行します。**
 1. 該当するサービスの**[Rate]**列に、新しい評価の値を入力します。
 2. **[Apply]**をクリックして入力を保存します。
- **ユーザ定義DNSBLサービスを削除するには、以下の手順を実行します。**

削除するサービスのアドレス行の右側にある **✕** ボタンをクリックします。



使用する DNSBL サービスを選択する際には注意が必要です。サービスごとに異なるポリシーを使用してリストが生成されています。メールフィルトレーションでこれらのサービスを使用する前に、各サービスのポリシーをよく調べてください。

4.3.4. 保護対象ドメインリストの管理

保護対象ドメインリストには、トラフィックを受信するドメインの名前がリストされます。これらのドメインのトラフィックは、受信メッセージストリーム内のスパムがチェックされて除去されます。**[Policies]→[Common]→[Protected Domains]**ページ(図12を参照)で、このリストを管理できます。

The screenshot shows the Kaspersky Anti-Spam web interface. The breadcrumb path is "Policies → Common → Protected Domains". The main content area is titled "Protected Domains" with a timestamp of "20:00". Below the title, it says "List of domains to be protected by Anti-Spam engine". There is a text input field labeled "Protected domains:" containing the text "example.com" and "localnet?.net". At the bottom right of this field are "Apply" and "Reset" buttons. On the left side, there is a sidebar with a "Common" section containing links for "Default Rules", "Black List", "White List", "DNS Black Lists", and "Protected Domains" (which is highlighted). Below this are sections for "Groups" (with a "Group List" link) and "Build" (with a "Rebuild All Policies" link).

図 12. 保護対象ドメインのリスト

ドメイン名の入力では、ワイルドカードを使用できます。「*」は任意の長さの文字列、「?」は任意の1文字を表します。たとえば、**example.com** ドメインおよびそのサブドメインをすべて保護対象ドメインリストに追加するには、以下のレコードを追加するだけで済みます。

*example.com

すべての受信メールをフィルタリングするよう設定するには、このリストを空にするか、以下のレコードをリストに追加します。

*

リストの編集が終了したら、**[Apply]**ボタンをクリックして変更を確定するか、**[Reset]**ボタンをクリックして変更をキャンセルします。



保護対象リストに追加されたドメインは、ライセンス制限を遵守するように制御されます(たとえば、ライセンスにおいてメールトラフィック量が制限されている場合は、メールトラフィック量が制御される)。

保護対象ドメインリストの変更は、コマンドラインからローカルで入力することもできます。オリジナルのドメインリストは、`/usr/local/ap-mailfilter3/conf` ディレクトリ内にある `protected_domains` テキストファイルに保存されています。ファイルの編集後、**root** として以下のコマンドを実行します。

```
# /usr/local/ap-mailfilter3/bin/kas-restart -f
```



Kaspersky Anti-Spam は、保護対象リストに含まれていないドメイン内のユーザのすべてのメッセージアドレスに、以下のヘッダを追加します。

X-SpamTest-Info: Not protected

特別なヘッダの詳細については、113ページのセクションA.5を参照してください。

4.3.5. グループ管理

フィルトレーションサーバの管理者は、ユーザごとにさまざまなスパム認識設定を定義できます。定義するには、**スパムフィルトレーションのグループポリシー**を使用します。

グループポリシーのルールを設定する前に、グループポリシーを適用するメールアドレスのリストを定義する必要があります。

管理者が作成するグループの他に、セットアップ時にデフォルトで作成される**All**グループも使用できます。このグループは、他のどのグループにも属さないメールメッセージを処理するためのルールを定義します。**All**グループはシステムグループであるため、削除できません。

グループ設定は、**[Policies]**セクションウィンドウの左側にある**[Groups]**メニューからアクセスできます。

[Group List]リンクを選択すると、既存のすべてのグループのリストが表示されるページが開きます(図13を参照)。

グループについて以下の操作を実行できます。

- グループプロパティの編集
- グループの新規作成
- 既存のグループの削除

- グループのリスト順序の変更

これらの作業について詳しく説明します。



グループプロパティのエディタを開くには、以下の手順を実行します。


変更するグループ名の右側にある  ボタンをクリックします。

図 13. Kaspersky Anti-Spam で使用されるグループのリスト

グループプロパティのエディタでは、以下の要素を設定できます。

- 全般的なグループパラメータ。グループ名、コメント、グループルールを適用するメールアドレスのリストなど。
- スпам認識ルール
- メールメッセージに適用する動作
- 送信者のブラックリストおよびホワイトリスト



All グループは、管理者が作成したどのグループにも送信者と受信者が属さないメッセージを処理するためのルールを定義するグループなので、このグループの名前とメールアドレスリストは編集できません。



新しいグループを作成するには、以下の手順を実行します。

1. グループリストについては  ボタンをクリックします。

2.表示されたウィンドウで(図14を参照)、グループ名、コメント(必要に応じて)、およびメールアドレスのリストを入力します。

[Group Id]フィールドには、作成時に割り当てられるグループ ID が表示されます。このパラメータは変更できません。

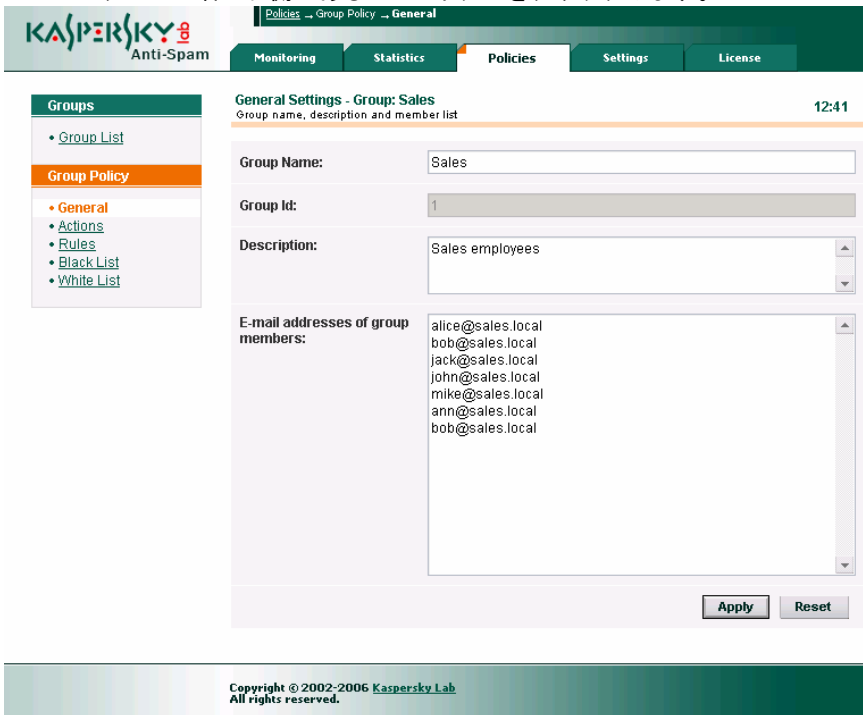
[Comments]フィールドに入力したテキストは、グループリストでグループ名の下に表示されます。

メールアドレスは、送信者のブラックリストおよびホワイトリストと同じ形式で入力します(39ページのセクション4.3.2を参照)。



既存のグループを削除するには、以下の手順を実行します。

グループ名の右側にある  ボタンをクリックします。



The screenshot shows the 'General Settings - Group: Sales' page in the Kaspersky Anti-Spam interface. The page title is 'Policies -> Group Policy -> General'. The main content area is titled 'General Settings - Group: Sales' and includes the subtitle 'Group name, description and member list'. The page is timestamped '12:41'. The interface has a sidebar on the left with 'Groups' and 'Group Policy' sections. The 'Group Policy' section is expanded to show 'General', 'Actions', 'Rules', 'Black List', and 'White List'. The main content area has tabs for 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Policies' tab is active. The 'General Settings' section includes the following fields:

- Group Name:** Sales
- Group Id:** 1
- Description:** Sales employees
- E-mail addresses of group members:**
 - alice@sales.local
 - bob@sales.local
 - jack@sales.local
 - john@sales.local
 - mike@sales.local
 - ann@sales.local
 - bob@sales.local


At the bottom right of the main content area, there are 'Apply' and 'Reset' buttons.

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

図 14. 新規グループ作成用ページ



グループのリスト順序を変更するには、以下の手順を実行します。

グループ名の左側にある  ボタンをクリックします。選択したグループ

プが上に移動します。

メッセージの処理中に、フィルトレーションモジュールが、グループリストに定義されている順序で(リストの最初から終わりまで)グループをチェックします。受信者のアドレスが含まれている最初のグループのルールを使用してメッセージが処理されます。受信者がどのグループにも含まれていない場合は、[All]グループのルールを使用してメッセージが処理されます。

4.3.6. グループフィルトレーションポリシーの管理

[All]グループを含む各グループについて、スパム認識パラメータおよび送信者のブラックリストおよびホワイトリストの設定をそれぞれ指定できます。それにより、ユーザグループごとにさまざまな認識ルールを定義できます。

デフォルトでは、各グループの認識ルールの設定は、デフォルトフィルトレーションポリシーで指定されている値を継承します。ただし、これらの値は再定義できます。

グループプロパティエディタに表示される[Group Policy]メニューの[Rules]リンクを使用して、グループフィルトレーションポリシーの認識ルールを設定することができます。ルール構造は、デフォルトフィルトレーションポリシーのルール構造と同じです(31ページのセクション4.3.1を参照)。

唯一の相違点は、グループポリシーの設定では、選択可能なパラメータ値のリストに[by default]という値が含まれているという点です。この値が指定されているパラメータは、デフォルトフィルトレーションポリシーで指定されている値を継承します。

図15は、グループフィルトレーションポリシーの[Rules]ウィンドウの例です。

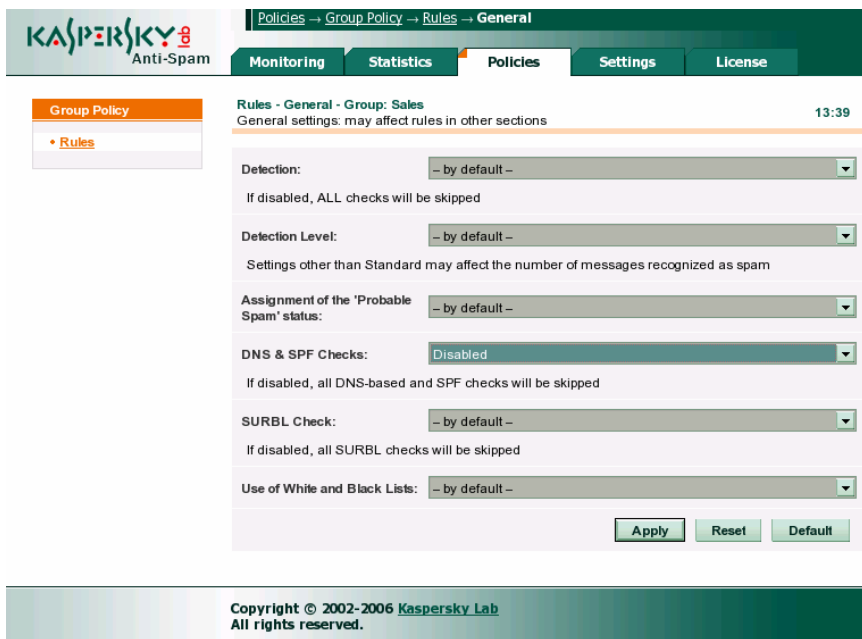


図 15. グループフィルトレーションポリシーの[Rules]ページ

図からわかるように、このグループは、[DNS & SPF Checks]パラメータを除くすべてのパラメータが、デフォルトポリシー設定を継承しています([by default]が設定されている)。[DNS & SPF Checks]の機能は無効になっています。送信者のブラックリストおよびホワイトリストを作成するには、[Group Policy]メニューの[White List]および[Black List]リンクを使用します。グループごとにこれらのリストを設定する方法は、デフォルトフィルトレーションポリシーの場合と同じです(31ページのセクション4.3.1を参照)。

4.3.7. メッセージに適用する動作

グループポリシーには、フィルトレーションモジュールによって認識されたメールメッセージの転送および変更に関する動作セットも含まれています。グループプロパティエディタに表示される[Group Policy]メニューの[Actions]リンクを使用して、これらの動作を設定することができます。フィルトレーションモジュールの処理結果としてメッセージに割り当てられるステータスごとに、メッセージに適用する具体的な動作を指定します。[Actions]ページ(図16を参照)のフォームでは、割り当てられる可能性があるメッセージステータスごとに適用する動作を指定できます。

適用する動作は、メッセージのステータスを示すヘッダの下にあるドロップダウンリストで指定します。

管理者は、以下の動作を選択できます。

- **[Accept this message]** – メールサーバは、メッセージを受信して受信者に配信します。
- **[Send a copy of this message to other recipient(s)]** – メールサーバは、メッセージを受信して受信者に配信し、メッセージのコピーを**[Send message to]**フィールドに指定されているアドレスに送信します。
- **[Redirect this message to other recipient(s)]** – メールサーバは、メッセージを受信し、そのメッセージを**[Send message to]**フィールドに指定されているアドレスに転送します。このメッセージは、本来の受信者には配信されません。スパムアーカイブの保存用メールボックスにメッセージを転送する場合に、この方法を使用できます。
- **[Reject this message]** – メールサーバは、メッセージを拒否し、配信不可能であることを知らせる通知を送信者に返信します。すべての受信者のメッセージ配信が拒否された場合、SMTPセッション中に、サーバが直ちに配信拒否の通知を返します(*拒否メッセージ*)。少なくとも1人の受信者のメッセージ配信が許可された場合、一部の受信者にメッセージを配信できなかったことを知らせる通知が送信者に送信されます(*不達通知*)。これらの通知のテキストは、**[Settings]**→**[Reject Messages]**セクションでカスタマイズできます(詳細については、60ページのセクション**4.5.4**を参照)。
- **[Delete this message]** – メールサーバは、メッセージを受信し、受信者に転送せずにメッセージを削除します。メッセージの送信者には、配信不可能であることを知らせる通知が送信されません。

The screenshot displays the 'Actions' configuration page for a group policy named 'Sales'. The interface is organized into several sections, each corresponding to a different message recognition status:

- If a message is recognized as 'Spam':** Action: 'Accept this message'. Prepend to the Subject: '[! SPAM]'. Set X-SpamTest-Header: (empty).
- If a message is recognized as 'Probable Spam':** Action: 'Accept this message'. Prepend to the Subject: '[?? Probable Spam]'. Set X-SpamTest-Header: (empty).
- If a message is recognized as 'Blacklisted':** Action: 'Accept this message'. Prepend to the Subject: '[! BLACKLISTED]'. Set X-SpamTest-Header: (empty).
- If a message is recognized as 'Formal':** Action: 'Accept this message'. Prepend to the Subject: '[-Formal Message-]'. Set X-SpamTest-Header: (empty).
- If a message is recognized as 'Trusted':** Action: (empty). Prepend to the Subject: (empty). Set X-SpamTest-Header: (empty).
- If a message is recognized as 'Not Detected':** Action: (empty). Prepend to the Subject: (empty). Set X-SpamTest-Header: (empty).

At the bottom right, there are 'Apply' and 'Reset' buttons. The left sidebar shows navigation options: 'Groups', 'Group List', 'Group Policy', 'General', 'Actions', 'Rules', 'Black List', and 'White List'.

図 16. グループフィルトレーションポリシーの[Actions]ページ

[Not detected]ステータスのメッセージ(スパムであると認識されなかったメッセージ)または**[Trusted]**ステータスのメッセージ(信頼できるソースから受信したメッセージや、グループポリシーの設定によりメールをスキャンしないことになっている受信者宛てのメッセージ)は、常に指定された受信者にルーティングされます。



この製品は、スパム認識の改善とフィルタによる誤報の減少をめざして開発が続けられていますが、通常のメッセージをスパムである

と認識する可能性を完全に無くすことは不可能です。したがって、**メッセージを削除する動作は十分に注意して適用してください。**

メッセージを転送する動作の他に、メッセージを変更する動作も定義できます。この動作は、認識結果を表示する場合や、後続処理でユーザの電子メールクライアントソフトウェアのフィルタと組み合わせて使用する場合などに役立ちます。Kaspersky Anti-Spam では、以下のようにメッセージを変更できます。

- メッセージの件名フィールド(件名のテキストの先頭)にラベルを追加します。**[Prepend to the Subject]**フィールドで、ラベルのテキストを定義します。
- 管理者が指定するテキストを含む特別なX-Spamtestヘッダを追加します。このヘッダは、エンドユーザが使用している電子メールソフトウェアで、メッセージの自動処理を行う際に使用できます。**[Set X-Spamtest-Header]**フィールドで、ヘッダテキストを定義します。フィルトレーションプロセスの結果としてメールメッセージに追加されるヘッダの詳細については、113ページのセクションA.5を参照してください。

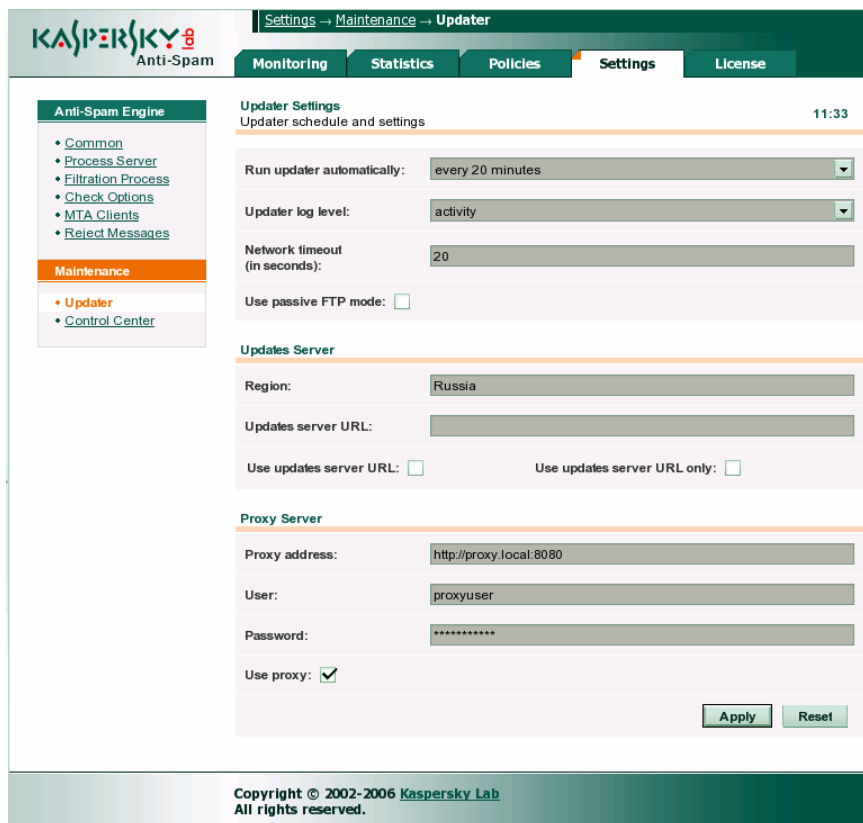
4.4. コンテンツフィルトレーションデータベースの更新

メールメッセージの内容を分析する際に使用されるコンテンツフィルトレーションデータベースは、*sfupdates* という特別な更新用モジュールで更新されます。このモジュールは、インターネット(カスペルスキーラボスの更新サーバ)またはネットワークディレクトリを、コンテンツフィルトレーションデータベースの更新のソースとして使用します。

更新処理は、コマンドラインから更新スクリプトを実行して手動で開始するか、cron を使用して自動的に実行されるようスケジュールすることもできます。

4.4.1. 更新パラメータの設定

更新パラメータをカスタマイズするには、Control Center の **[Settings]** → **[Maintenance]** → **[Updater]** ページを使用します(図17を参照)。



Settings → Maintenance → Updater

Monitoring Statistics Policies Settings License

Anti-Spam Engine

- Common
- Process Server
- Filtration Process
- Check Options
- MTA Clients
- Reject Messages

Maintenance

- Updater
- Control Center

Updater Settings 11:33
Updater schedule and settings

Run updater automatically: every 20 minutes

Updater log level: activity

Network timeout (in seconds): 20

Use passive FTP mode:

Updates Server

Region: Russia

Updates server URL:

Use updates server URL: Use updates server URL only:

Proxy Server

Proxy address: http://proxy.local:8080

User: proxyuser

Password: *****

Use proxy:

Apply Reset

Copyright © 2002-2006 Kaspersky Lab
All rights reserved.

図 17. Kaspersky Anti-Spam の更新用モジュールの設定

[Updater Settings]セクションには、以下の全般的な更新パラメータが含まれています。

- **[Run updater automatically]** – 更新サーバからコンテンツフィルトレーションデータベースの更新をダウンロードする間隔。この間隔は、およそ3分～3時間の範囲で指定できます。



更新間隔をできる限り短く設定することをお奨めします。コンテンツフィルトレーションデータベースを頻繁に更新すれば、サーバがより迅速に新しいスパムに対応できます。

パラメータの値は、製品を更新するcronタスクが開始される間隔です。必要に応じて、cronタスクを手動で設定することもできます。手動による設定の詳細については、54ページのセクション4.4.2を参照してください。

- **[Updater log level]** – 更新中のレポートファイルへの記録の詳細レベルを定義するパラメータ。以下の詳細レベルを定義できます。
 - **[fatal]** – 致命的なエラーに関するメッセージのみ記録します。
 - **[error]** – すべてのエラー(致命的なエラーおよびそれ以外のエラー)に関するメッセージを記録します。
 - **[warning]** – 警告およびエラーメッセージを記録します。
 - **[info]** – 警告およびエラーメッセージに加えて、情報的なレコード(更新モジュールの開始に関する情報や、更新結果など)を記録します。
 - **[activity]** – **[info]**レベルのすべてのデータと、更新処理(更新サーバへの接続、サーバからのファイルのダウンロードなど)に関する追加情報を記録します。
 - **[debug]** – **[activity]**レベルのすべてのデータと、デバッグメッセージを記録します。
- **[Network timeout]** – コンテンツフィルトレーションデータベースを更新する際のネットワーク処理用のタイムアウト時間(秒単位)。推奨値は **30** 秒です。
- **[Use passive FTP mode]** – FTP経由で更新サーバに接続する場合に、パッシブ接続モードの使用を推奨します。

[Updates Server]セクションには、更新のソースとして使用するサーバに関するパラメータが含まれています。

- **[Region]** – ユーザの地域。このパラメータの値を使用して、地理的に最適な位置にある更新サーバが選択されます。
- **[Updates server URL]** – 更新のソースとなるサーバのアドレス。このパラメータは、**[Use updates server URL]**および**[Use updates server URL only]**パラメータと組み合わせて使用します。デフォルトでは、コンテンツフィルトレーションデータベースの更新に使用するサーバのリストは、製品パッケージに含まれている *updcfg.xml* ファイル内に定義されています。更新中に、Kaspersky Anti-Spamがこのリストからサーバを自動的に選択します。**[Use updates server URL]**オプションを使用すると、**[Updates server URL]**パラメータで定義されているアドレスが更新のソースとして優先的に使用されます。**[Use updates server URL only]**オプションを使用すると、Kaspersky Anti-Spamは、指定されたサーバからのみコンテンツフィルトレーションデータベースの更新を行います。他のアドレスは使用されません。

このパラメータには、以下の URL を更新のソースとして設定できます。

- HTTP サーバ。レコード形式 : `http://<サーバアドレス>`
- FTP サーバ。レコード形式 : `ftp://<サーバアドレス>`
- ローカルディレクトリ。レコード形式 : `<ディレクトリパス>`

ローカルディレクトリを更新のソースとして使用すると、大規模なネットワークにおいて、単一のソースから複数のサーバの更新を実行できます。

[Proxy Server]セクションには、プロキシサーバへのアクセスに必要な以下のパラメータが含まれています。

- **[Proxy address]** – インターネット接続に使用されるプロキシサーバのアドレス。このパラメータは、`http://url:port`という形式で指定します。「url」および「port」は、プロキシへの接続に使用するアドレスおよびポートです。このアドレスが指定されていない場合、更新用モジュールは`http_proxy`環境変数の値を使用します。
- **[User]** – プロキシサーバへのアクセスに使用するユーザ名
- **[Password]** – プロキシサーバへのアクセスに使用するユーザパスワード
- **[Use proxy]** – 更新サーバへの接続にHTTPプロキシサーバを使用するかどうかを指定します。

4.4.2. 更新の開始

コンテンツフィルトレーションデータベースの更新を開始するには、以下の2つの方法があります。

- 自動スケジュール起動
- コマンドラインからの手動による起動

自動スケジュール更新を設定することをお奨めします。それにより、コンテンツフィルトレーションデータベースを最新の状態に保つことができるため、最も効果的にスパムをフィルタリングできます。



更新を手動で開始するには、コマンドラインに以下のコマンドを入力します。

```
# /usr/local/ap-mailfilter3/bin/sfupdates [key]
```

[key]は、更新スクリプトを開始するためのコマンドラインオプションです。*sfupdates*スクリプトの全パラメータの完全なリストについては、112ページの付録A.4.8を参照してください。

コマンドラインキーを使用せずにこのスクリプトを開始した場合、更新サーバから新しい更新がダウンロードされ、更新の完全性のチェックが行われ、新しいデータベースがインストールされて、フィルトレーションモジュールが再起動されます。それにより、フィルトレーションモジュールが、新しいデータベースを使用するようになります。

mailflt3 ユーザの場合、Kaspersky Anti-Spam のセットアップ中に、*cron* が 20 分おきに更新スクリプトを実行するようデフォルトで設定されます。何らかの理由で、更新スクリプトを手動で実行するタスクを設定する必要がある場合は、以下の手順を実行します。

1. **mailflt3** ユーザの **cron** タスクを編集するために、以下のコマンドを使用します。

```
# crontab -u mailflt3 -e
```

2. このタスクファイルに、たとえば以下のような行を追加します。

```
* /20 * * * * /usr/local/ap-mailfilter3/bin/sfupdates -q
```



更新の自動起動を設定する前に、**mailflt3** ユーザが */usr/local/ap-mailfilter3/cfdata* および */usr/local/ap-mailfilter3/conf* ディレクトリに対する書き込み権限を持っていることを確認してください。

4.5. スパムフィルトレーションサーバの設定

[Settings]セクションのページには、スパムフィルタリングサーバのコンポーネントの設定が含まれています。ページの表示を切り替えるには、[Anti-Spam Engine]メニューの以下のリンクを使用します。

- [Common] – フィルトレーションサーバの全般的なパラメータ
- [Process Server] – 運用中にフィルトレーションマスタプロセス *ap-process-server* で使用されるパラメータ
- [Filtration Process] – 運用中にフィルタリングプロセス *ap-mailfilter* で使用されるパラメータ
- [Check Options] – スパム認識パラメータ

- **[MTA Clients]** – クライアントプラグインモジュールのパラメータ
- **[Reject Messages]** – メッセージが拒否された場合に、メッセージの送信者に返される通知のテキスト

フィルトレーションサーバコンポーネントのパラメータは、*filter.conf*設定ファイルを手動で編集して指定することもできます。*filter.conf*設定ファイルの詳細については、100ページの付録A.3.1を参照してください。

4.5.1. 共通フィルトレーションサーバパラメータ

フィルトレーションサーバの共通パラメータは、**[Settings]**→**[Anti-Spam Engine]**→**[Common]**ページに表示されます(図18を参照)。以下のパラメータがあります。

- **[Syslog facility]** – Kaspersky Anti-Spamのコンポーネントからのメッセージを記録するシステムログ機能。デフォルトでは、mail機能を使用してメッセージが記録されます。ただし、必要に応じてフィルトレーションサーバの管理者が、mail、user、local0 – local7の中からログ機能を選択できます。



[Syslog facility]パラメータの変更後は、指定された機能のメッセージを記録するようsyslogデーモンを設定してください。この設定を行うには、手動で/etc/syslog.confファイルを編集する必要があります。詳細については、syslogdおよびsyslog.confのマニュアルを参照してください。

監視システムは、システムログを使用して、フィルタリングサーバおよびそのコンポーネントに関するメッセージを表示します。監視システムは、必要なファイルが保存されているディレクトリを特定するために、/etc/syslog.conf設定ファイルのパラメータ値を使用します。

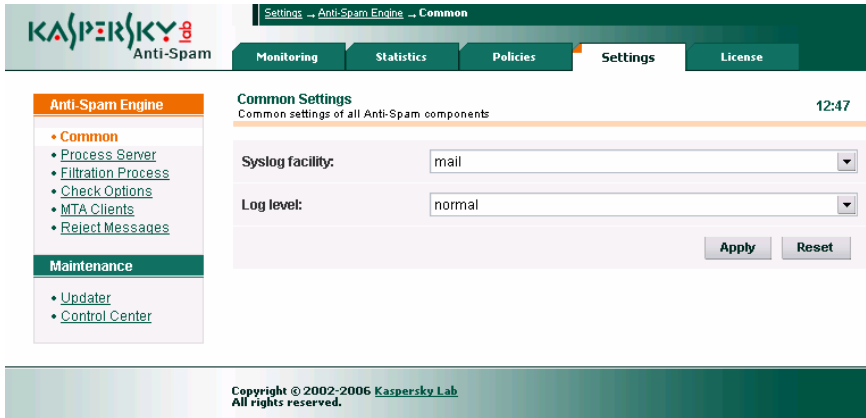


図 18. フィルトレーションサーバの共通設定

- [Verbose level]** – Kaspersky Anti-Spamのモジュールによって生成されるアクティビティログの詳細レベル。このパラメータには、**[minimum]**、**[low]**、**[normal]**、**[high]**、**[debug]**、および**[more debug]**のいずれかの値を設定できます。パラメータ値を設定する際は、機能(Syslog機能)によっては、`/etc/syslog.conf`設定ファイル内の設定により情報の詳細レベルにさらに制限が加えられる可能性があることに注意してください。特に、**mail**機能の場合に、FreeBSDのデフォルト値である**mail.info**レベルが指定されている場合、**[Verbose level]**パラメータに**[more debug]**値を設定しても、詳細レベルが下がります。



[more debug]詳細レベルを設定すると、サーバの負荷が上昇してパフォーマンスが低下する可能性があります。このレベルを使用するのは、アプリケーションの処理をデバッグするときだけにしてください。

フィルトレーションサーバの共通パラメータを変更したら、**[Apply]**ボタンをクリックし、以下のコマンドを使用してフィルトレーションサーバを再起動します。

(Linux ディストリビューションの場合)

```
# /etc/init.d/kas3 restart
```

(FreeBSD の場合)

```
# /usr/local/etc/rc.d/kas3.sh restart
```

4.5.2. フィルトレーションマスタプロセスのパラメータ

[Settings]→[Anti-Spam Engine]→[Process Server]ページには、フィルトレーションマスタプロセス用の以下の設定が含まれています(図19を参照)。

- **[Max. number of filtration processes]** – 同時に実行できるフィルタリングプロセスの最大数。デフォルト値は **10** です。
- **[Number of filtration processes at server start-up]** – フィルタリングプロセスの開始時に開始されるフィルトレーションプロセスの数。デフォルト値は **0** です。その場合、メッセージが到着したときに、フィルトレーションモジュールの処理が開始されます。
- **[Number of spare filtration processes]** – 分析要求を待機しているフィルトレーションプロセスの最大数。プロセス数が指定された制限値を超えた場合、使用されていないプロセスが終了されます。デフォルト値は **0** です。

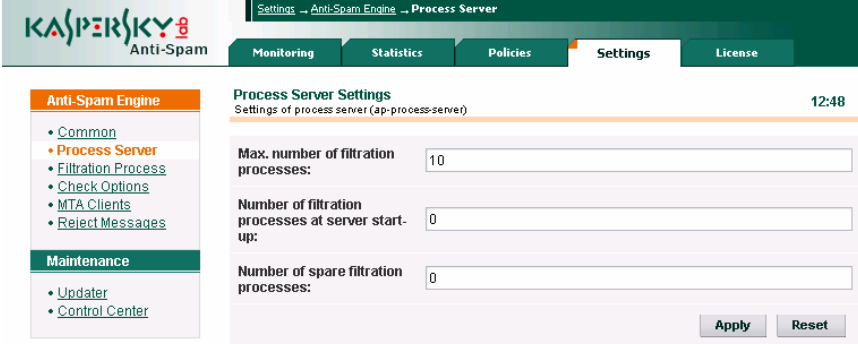
マスタプロセスの共通パラメータを変更したら、**[Apply]**ボタンをクリックし、以下のコマンドを使用してフィルトレーションサーバを再起動します。

(Linux ディストリビューションの場合)

```
# /etc/init.d/kas3 restart
```

(FreeBSD の場合)

```
# /usr/local/etc/rc.d/kas3.sh restart
```



Settings - Anti-Spam Engine - Process Server

Monitoring Statistics Policies **Settings** License

Anti-Spam Engine

- [Common](#)
- **Process Server**
- [Filtration Process](#)
- [Check Options](#)
- [MTA Clients](#)
- [Reject Messages](#)

Maintenance

- [Updater](#)
- [Control Center](#)

Process Server Settings 12:48

Settings of process server (ap-process-server)

Max. number of filtration processes:

Number of filtration processes at server start-up:

Number of spare filtration processes:

Copyright © 2002-2006 Kaspersky Lab. All rights reserved.

図 19. フィルトレーションマスタプロセスのパラメータ

4.5.3. フィルタリングプロセスのパラメータ

[Settings]→[Anti-Spam Engine]→[Filtration Process]ページ(図20を参照)には、フィルタリングプロセス*ap-mailfilter*の以下のパラメータが含まれています。

- **[Max. number of mail messages to be processed]** – 単一のフィルタリングプロセスで処理可能なメールメッセージの最大数。指定された数のメッセージの処理が終了すると、そのフィルタリングプロセスは終了し、代わりに新しいプロセスが開始されます。このパラメータの値は、フィルトレーションサーバの負荷に応じて調整できます。推奨値は **300** です。
- **[Max. number of mail messages randomization]** – 単一のフィルタリングプロセスで処理可能なメッセージの最大数を定義するために Kaspersky Anti-Spam が使用する値。この値は、**[Max. number of mail messages to be processed]**パラメータの値を最小値、**[Max. number of mail messages to be processed]** および **[Max. number of mail messages randomization]**パラメータの合計を最大値とする範囲内で、ランダムに選択されます。したがって、これらのパラメータの値がそれぞれ **300** と **30** の場合、単一のフィルタリングプロセスで処理可能なメッセージ数は、300~330 になります。このパラメータを設定することにより、サーバの負荷がピークに達しているときに、フィルタリングプロセスが同時に終了して新たな多数のフィルタリングプロセスが同時に開始されるのを防ぐことができます。
- **[Max. idle time (in seconds)]** – フィルタリングプロセスがアイドル状態である最大時間(秒単位)。フィルタリングプロセスが分析するメッセージを受け取らないまま指定されている秒数が経過すると、アクティビティが中止されます。デフォルト値は **300** です。
- **[Exit delay (in seconds)]** – フィルタリングプロセスが停止コマンドを受け取ってから停止するまでの最大遅延時間(秒単位)。デフォルト値は **0** です。その場合、コマンドが到着すると、すべてのフィルタリングプロセスが、現在のメッセージの処理の終了後、直ちに終了します。

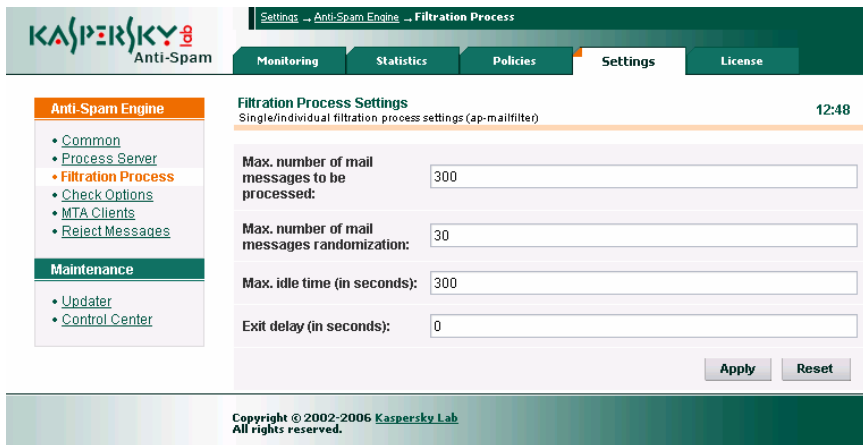


図 20. フィルタリングプロセスのパラメータ

4.5.4. スпам認識パラメータ

[Settings]→[Anti-Spam Engine]→[Check Options]ページ(図21を参照)には、フィルタリングプロセス *ap-mailfilter* の以下の認識パラメータが含まれています。

- [Number of 'Received' headers to be parsed while retrieving ip address (for use in DNSBL checks)]** – DNSBL を使用して中間サーバをチェックする必要があることを示すパラメータ。基本的に、フィルタが送信者の IP アドレスをチェックする際には、メッセージをフィルタリングサーバに渡したサーバの IP を使用してチェックを行います。しかし、メッセージが送信中に 1 つ以上の中間サーバを通過してきた場合は、本来の送信者の IP が見えなくなってしまいます。最後のサーバだけでなく中間サーバの IP アドレスもチェックする場合は、このパラメータで、チェックする中継サーバの数を指定します。分析では、*[Received]*ヘッダが使用されます。0 を指定すると、*[Received]*ヘッダが分析されません。



設定値が大きいほど、フィルトレーションサーバは、より多くの中間サーバをチェックするため、複数の中間メールサーバを経由してきたスパムメッセージを認識できる確率が高くなります。ただし、それと同時に、フィルトレーションサーバに余計に負荷がかかったり、フィルタによる偽陽性判定を引き起こす原因になったりする可能性があります。

- **[Overall timeout of all DNS requests (in seconds)]** – DNSベースのチェックの実行中に、アプリケーションがDNSサーバからの応答を待機する時間(秒単位)。デフォルト値は **10** です。
- **[Check MS Word and RTF files]** – Word ドキュメント(doc)および RTF 形式の添付ファイルの分析を有効/無効にするパラメータ。
- **[UDS enabled]** – UDS ベースのメッセージスキャンモードを有効/無効にするパラメータ。このチェックを使用することにより、コンテンツフィルトレーションデータベースの更新をダウンロードする前に、スパムメールを適宜ブロックできます。このチェックによりフィルタリングサーバのパフォーマンスが大幅に低下する場合や、フィルトレーションサーバとカスペルスキーラブスの UDS サーバ間のやり取りが不可能な場合以外は、UDS ベースのチェックを有効にすることをお奨めします。

UDSの詳細については、15ページのセクション**2.2.4**を参照してください。

- **[Timeout for receiving response from UDS server (in seconds)]** – フィルタリングサーバと UDS サーバ間で確立される接続のタイムアウト時間。フィルトレーションサーバが UDS からの応答を受信しないまま指定された秒数が経過すると、フィルトレーションサーバは、カスペルスキーラブスの別の UDS サーバに接続します。

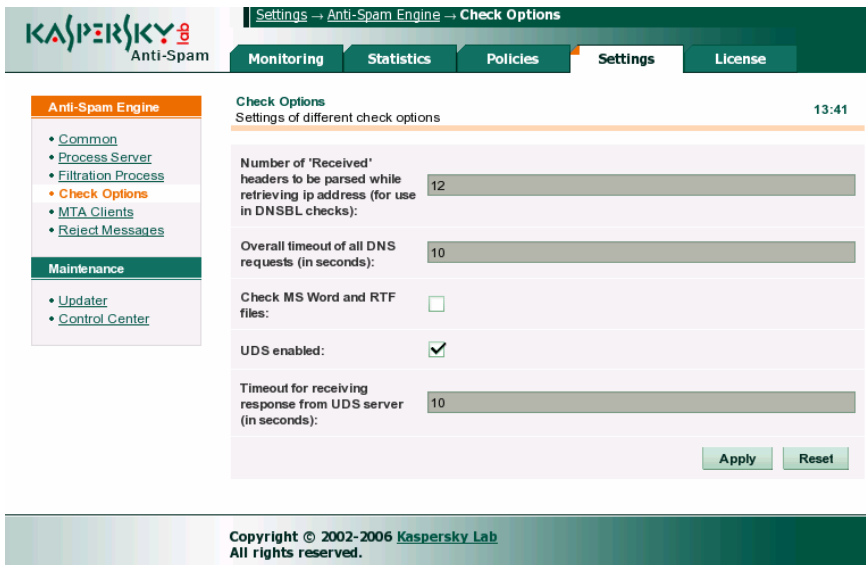


図 21. スパム認識パラメータ

4.5.5. クライアントモジュールの設定

[Settings]→[Anti-Spam Engine]→[MTA Clients]ページ(図22を参照)には、電子メールサーバとアンチスパムエンジンの間のやり取りを可能にするクライアントプラグインモジュールの設定が含まれています。

- **[Filtering size limit (KB)]** – フィルトレーションサーバによって処理されるメッセージの最大サイズ(KB)。指定されたサイズを超えているメッセージは、フィルトレーションサーバによって処理されません。デフォルト値は **500** です。
- **[On filtering error]** – クライアントモジュールは、フィルトレーションサーバとのやり取りで発生したエラーに対応します。このパラメータには、以下の値を設定できます。
 - **[accept message]** – エラーが発生した場合は、メッセージがフィルトレーションサーバによって処理されずに受信者に送信されます。
 - **[reject message]** – 処理中にエラーの原因となったメッセージが配信されません。
 - **[generate temporary error]** – メッセージが配信されません。アプリケーションにより、一時的なメールサーバエラーに関する通知が送信者に返されます。この場合、送信者のメールサーバが、しばらくしてからメッセージを再び送信することになります。
- **[Default domain]** – メールドメインが省略されているアドレスで代用されるメールドメイン名。たとえば、デフォルトドメインとして「*mycompany.com*」を指定した場合、「*someuser*」というアドレスは「*someuser@mycompany.com*」として解釈されます。
- **[Connection timeout (in seconds)]** – クライアントモジュールとフィルトレーションサーバ間で確立される接続のタイムアウト時間(秒単位)。デフォルト値は **40** です。
- **[Data exchange timeout (in seconds)]** – フィルトレーションサーバとクライアントモジュール間のデータ交換中に、ネットワークを介して行われる読み取りおよび書き込みのタイムアウト時間(秒単位)。デフォルト値は **30** です。



アンチスパムエンジンの運用中に定期的エラーが発生する場合は、ご購入された販売代理店にお問い合わせください。

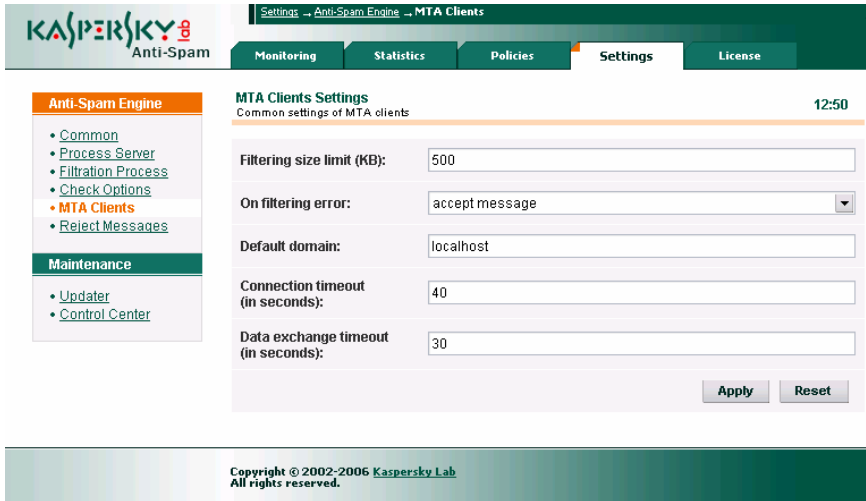


図 22. クライアントモジュールの設定

4.5.6. 拒否されたメッセージに関する通知

特定のステータスのメッセージに[Reject this message]動作を適用するよう指定されている場合、フィルトレーションサーバは、このメッセージを本来の受信者にルーティングしません。代わりに、このメールが配信不能であることを知らせる通知をメッセージの送信者に返します。

フィルトレーションサーバは、2 種類の通知を使用します。使用するメッセージのタイプは、設定と認識結果によって決まります。

通知の 1 つは、**拒否メッセージ**です。このメッセージは、SMTP セッション中に、メッセージが配信されなかったことを知らせるエラーコードと共に直ちに送信者に送信されます。以下の SMTP セッションの例には、**拒否メッセージ**のテキストが含まれています。

Server: 220 mail.mycompany.com ESMTP

Client: HELO spamhost.whatever.com

Server: 250 mail.mycompany.com

Client: MAIL FROM: <spamer@whatever.com>

Server: 250 Ok

Client: RCPT TO: <someuser@mycompany.com>

Server: 250 Ok

Client: DATA

Server: 354 End data with <CR><LF>.<CR><LF>

Client: >>>

Client: >>> Message text ...

Client: >>>

Client: .

Server: 550 The message is rejected by spam filtering engine.

Client: QUIT

Server: 221 Bye...

スキャン結果により、指定されたすべての受信者へのメッセージ配信が禁止された場合のみ、アンチスパムエンジンは**拒否メッセージ**を使用します。

1つのメッセージが複数の受信者宛てに送信されており、フィルトレーションポリシーにより少なくとも1人の受信者への配信が許可される場合、メッセージが受け入れられたSMTPセッションの間、サーバが応答します。その後、サーバは、メッセージが配信されなかった受信者に関する情報と共に**不達通知**を送信者に返します。

Control Centerの[Settings]→[Anti-Spam Engine]→[Reject Messages]ページで、これらのメッセージのテキストを編集できます(図 23を参照)。

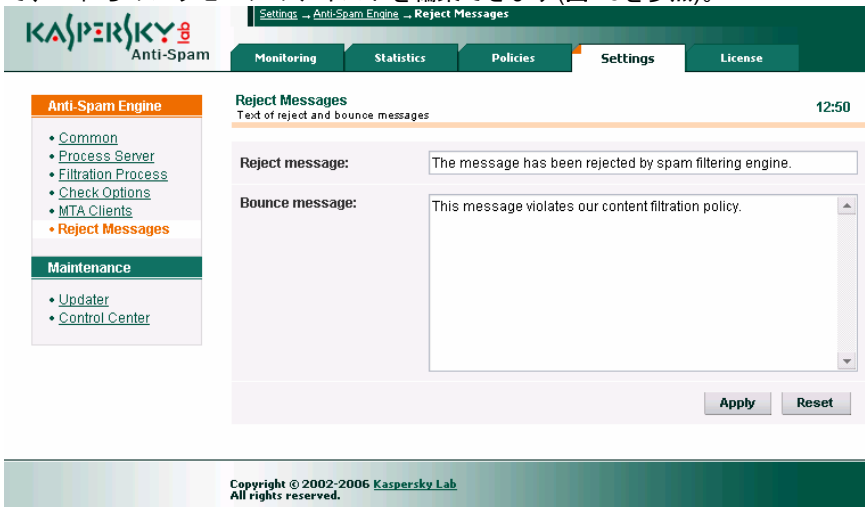


図 23. 拒否/不達通知の編集ページ

4.6. Control Center の設定

[Settings]→[Maintenance]→[Control Center]ページ(図24を参照)に含まれているパラメータを使用して、以下の設定を行うことが可能です。

- 監視システムのメッセージおよび cron サービスによるスクリプトの実行中に発生したエラーに関するメッセージを、監視システムが送信する際の

宛先アドレスを指定します([Send alerts to]パラメータ)。

- kas-thttpd HTTP サーバアクティビティの監視を有効/無効にします([Monitoring of kas-thttpd daemon]パラメータ)。
- Sendmail とのやり取りに使用する kas-milter クライアントモジュールの監視を有効/無効にします([Monitoring of kas-milter daemon]パラメータ)。

kas-thttpd および kas-milter の処理の監視中に生成されるメッセージは、[Monitoring]→[Anti-Spam Engine]ページに表示されます(79 ページのセクション 4.8.1.1 を参照)。

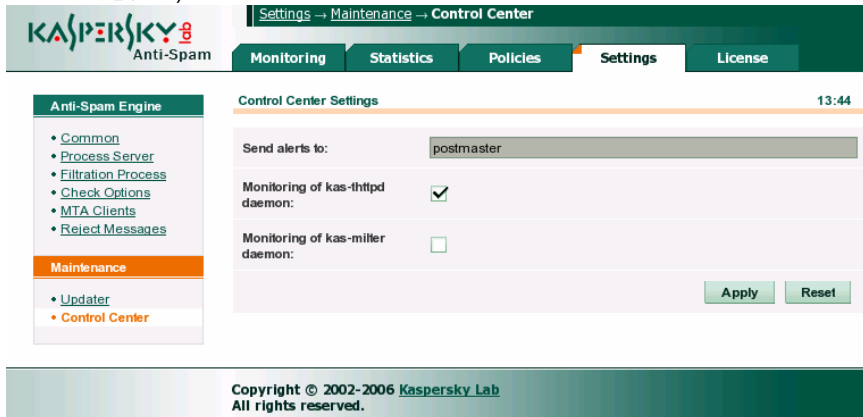


図 24. Control Center の設定

4.7. ライセンスキーの管理

Kaspersky Anti-Spam を使用できるかどうかは、ライセンスキーが有効かどうかによって決まります。ライセンスキーは、製品パッケージに含まれています。このキーは、キーを購入してインストールした日からアプリケーションを使用する権利をお客様に与えるものです。



ライセンスキーがないと、Kaspersky Anti-Spam は機能しません。その場合、すべてのメールメッセージが、フィルタリングされずに送信されます。

ライセンスキーには、ライセンスタイプ、有効期限、販売元に関する情報など、お客様が購入したライセンスに関する必要な情報がすべて含まれています。ライセンス期間にアプリケーションを使用する権利の他に、以下の特典を受けられます。

- 24 時間利用可能な技術サポート
- およそ 20 分おきに提供されるコンテンツフィルトレーションデータベースの更新

ライセンスの期限が切れても、アプリケーションの機能はそのまま維持されますが、コンテンツフィルトレーションデータベースを更新できなくなります。期限切れ後もスパムをフィルタリングできますが、期限後に発行されたデータベースは利用できません。そのため、新種のスパムを効率的にフィルタリングできない可能性があります。

したがって、Kaspersky Anti-Spam の使用ライセンスを適宜更新する必要があります。また、バックアップキーをインストールしておけば、現在のキーが期限切れになったときにすぐにそのキーを使用してアプリケーションが起動されます。インストールされているライセンスキーの管理に関する操作は、すべて Control Center で行えます。

4.7.1. ライセンス情報の表示

ライセンス情報の表示およびライセンスキーの管理は、[License]→[License Keys]ページで行います(図25を参照)。

The screenshot shows the 'License Keys' page in the Kaspersky Anti-Spam Control Center. The top navigation bar includes 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'License' section is active, showing 'Active License Information' with a timestamp of 11:46. The information includes: Product: Kaspersky Anti-Spam, License: Users 10, and Valid till: Jul 24 2006 (expires in 90 days). Below this is a table of 'License Key Files' with columns for File, Serial, Type, Volume, and Valid till. One file is listed: 000FF1AE.key, Serial: 02B1-0004A0-000FF1AE, Type: Users (Beta), Volume: 10, Valid till: Jul 24 2006. At the bottom, there is a section for 'Install a New License Key' with a text input field for the license key file, a 'Choose' button, and an 'Apply' button. The footer contains copyright information: Copyright © 2002-2006 Kaspersky Lab All rights reserved.

図 25. Kaspersky Anti-Spam のライセンスに関する情報

ページ上部の[Active License Information]セクションには、以下の情報が表示されます。

- インストールされている製品の名前
- 現在アクティブなライセンスの種類
- ライセンスの有効期限

システム管理者は、下の 2 行の情報に基づいて、購入ライセンス条件を遵守するよう制御します(有効期限、指定された制限)。

現在の状態に応じて、各行の左に表示されるアイコンが、以下のように変化します。



– ライセンス条件が遵守されています。



– ライセンスで指定されている制限に極めて近い状態で製品が機能しているか、2 週間以内にライセンスの有効期限が切れます。



– ライセンスの有効期限が切れているか、ライセンスで指定されている制限(処理メールトラフィック量など)を超えています。

後者の 2 つのアイコンが表示されている場合は、行の中に説明も表示されます。これらの情報の下に、インストールされている Kaspersky Anti-Spam のライセンスキーと共に各キーの簡単な情報が表示されます。

4.7.2. 新しいライセンスキーのインストール

新しいライセンスキーをインストールするには、Control Center を使用するか、コマンドラインからローカルでキーをインストールします。



Control Center を使用して新しいライセンスキーをインストールするには、以下の手順を実行します。

1. ライセンスキーの管理を行う **[License]** → **[License Keys]** ページを開きます。
2. ページ下部の **[Install a New License Key]** セクションの下にあるフィールドでライセンスキーファイルのパスを指定するか、入力フィールドの右側のボタンをクリックしてファイルシステムから必要なファイルを選択します。
3. **[Apply]** をクリックします。



コマンドラインを使用してローカルで新しいライセンスキーをインストールするには、以下のコマンドを実行します。

```
# /usr/local/ap-mailfilter3/bin/install-key <key>
```

key は、ライセンスキーが含まれているファイルのパスです。

現在のキーの期限が切れる前に新しいライセンスキーをインストールしたい場合は、新しいキーを予備のキーとして追加することができます。予備のキーは、現在のキーが期限切れになったときに機能し始めます。バックアップキーのライセンス期間は、キーが有効になったときに開始します。予備のキーは 1 つしかインストールできません。

4.7.3. ライセンスキーの削除

現在のライセンスキーと予備のライセンスキーを削除するには、コマンドラインに以下のコマンドを入力します。

```
# /usr/local/ap-mailfilter3/bin/remove-key -a
```

予備のライセンスキーを削除するには、コマンドラインに以下のコマンドを入力します。

```
# /usr/local/ap-mailfilter3/bin/remove-key -r
```



Control Center のインターフェースからはライセンスキーを削除できません。

4.8. フィルトレーションサーバアクティビティの監視

Kaspersky Anti-Spam には、各コンポーネントのステータスを監視するシステムが含まれています。このシステムにより、製品の運用を効果的に制御できます。また、管理者は、Control Center のインターフェースから、システムの機能上のトラブルを把握できます。

4.8.1. 全般的なステータス情報

システム管理者は、**[Monitoring]** → **[General Status]** ページで、Kaspersky Anti-Spam およびその主要コンポーネントに関する簡単な情報を確認できます (図26を参照)。

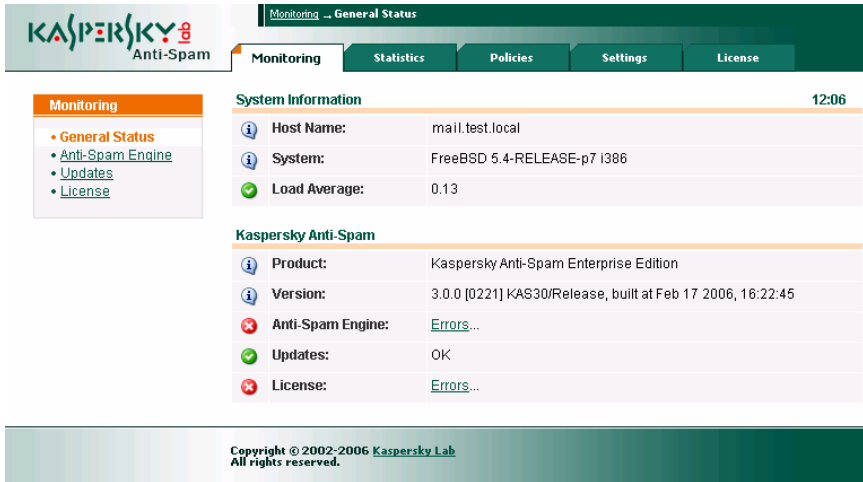


図 26. Kaspersky Anti-Spam コンポーネントのステータスに関する全般的な情報
監視対象コンポーネントごとに、ステータスデータに加えて、コンポーネントに
関する特定イベントの発生情報が表示されます。

各パラメータの隣に表示されるアイコンは、付加的な情報を示しています。この
アイコンは、監視対象コンポーネントのステータスに応じて変化します。



－ エラー：コンポーネントの不具合。または、監視対象パラメータ
の値が指定されている値を超えています。



－ 警告：コンポーネントの運用上で問題が発生していますが、製品
の機能上、致命的な問題ではありません。または、パラメータの
値が、指定されている制限値に近付いています。



－ 正常：コンポーネントは正しく機能しています。または、監視対
象パラメータの値が許容値です。

[System Information]セクションには、Kaspersky Anti-Spam がインストールさ
れているサーバに関する以下の情報が含まれています。

- [Host Name] – サーバ名
- [System] – 使用されているオペレーティングシステムの名前、バージョ
ン、および構造タイプ
- [Load Average] – サーバの負荷を表す数値パラメータ。このパラメータ
の詳細については、*top* および *uptime* ユーティリティのマニュアルを参照
してください。

[Kaspersky Anti-Spam]セクションには、製品および主要コンポーネントのス
テータスに関する概要が含まれています。このセクションには、以下のフィール
ドがあります。

- **[Product]** – インストールされている製品の名前
- **[Version]** – 使用されているフィルトレーションモジュールのバージョンおよびビルド番号
- **[Anti-Spam Engine]** – フィルトレーションサーバの現在のステータス
- **[Updates]** – コンテンツフィルトレーションデータベースおよび更新システムのステータス
- **[License]** – ライセンシングモジュールのステータス

4.8.1.1. アンチスパムエンジンに関する詳細情報

[Monitoring]メニューの**[Anti-Spam Engine]**リンクをクリックすると、フィルトレーションサーバのコンポーネントに関する詳細情報のページが表示されます(図27を参照)。

The screenshot shows the 'Monitoring - Anti-Spam Engine' interface. The top navigation bar includes 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Monitoring' section is active, showing a sidebar with links for 'General Status', 'Anti-Spam Engine', 'Updates', and 'License'. The main content area displays the engine's status as 'OK' for several components:

Component	Status	Details
Version:	3.0.0 [0232]	KAS30/Release, built at May 17 2006, 17:57:59
ap-process-server:	OK	pid=70527
ap-mailfilter:	OK	processes: 0
ap-spfid:	OK	processes: 17
kas-thtpd:	OK	pid=71493
Monitoring & Statistics:	OK	

Below the status table, there is a section for 'Last Anti-Spam Engine Events' with a 'View' dropdown set to 'Notifications, Warnings and Errors'. The events list shows:

- 05:22 13:50:48 kas-restart: kas-milter is restarted
- 05:22 12:50:42 kas-restart: No ap-mailfilter processes running

At the bottom of the page, the copyright notice reads: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

図 27. フィルトレーションサーバの主要部分を監視するページ

[Anti-Spam Engine]セクションには、以下のフィールドがあります。

- **[Version]** – 使用されているフィルトレーションモジュールのバージョンおよびビルド番号
- **[ap-process-server]** – フィルトレーションマスタプロセスのステータス。正常にプロセスが行われている間は、プロセス ID 情報(pid)が、行の中に表示されます。
- **[ap-mailfilter]** – フィルタリングプロセスのステータス。正常にプロセスが行われている間は、現在実行中のプロセスに関する情報が、行の中に表示されます。
- **[ap-spfd]** – SPF デーモンのステータス。デーモンのプロセスが正常に行われている間は、現在実行中のプロセス数がフィールドに表示されます。
- **[kas-thttpd]** – Control Center によって使用される HTTP サーバのステータス
- **[Monitoring & Statistics]** – 統計情報の監視およびプロセスに関するスクリプトの運用情報。mailflt3 ユーザの場合、さらにこれらのスクリプトを実行するcronタスクの制御も行われます。詳細については、115ページの付録A.6を参照してください。

[Last Anti-Spam Engine Events]セクションには、システムログ(syslog)に追加された、フィルトレーションサーバコンポーネントからのメッセージのログが表示されます。日付が新しい順にメッセージが並んでおり、対応するアイコンは、メッセージの重要度を表しています。**[View]**ドロップダウンリストを使用して、ログに表示するメッセージのカテゴリを指定できます。このドロップダウンリストには、以下の値が含まれています。

- **[All messages]** – 表示可能なすべてのメッセージが表示されます。
- **[Notifications, Warnings and Errors]** – 情報的なメッセージ以外のすべてのメッセージがページに表示されます。
- **[Warnings and Errors]** – 致命的なエラーおよび警告に関するメッセージのみページに表示されます。
- **[Errors only]** – 致命的なエラーに関するメッセージのみ表示されます。

4.8.1.2. 更新用モジュールに関する詳細情報

更新用モジュールに関する情報とコンテンツフィルトレーションデータベースのステータスが表示されるページを開くには、**[Monitoring]**メニューの[\[Updates\]](#)リンクを使用します(図28を参照)。

The screenshot displays the 'Monitoring - Updates' interface. At the top, there are navigation tabs for 'Monitoring', 'Statistics', 'Policies', 'Settings', and 'License'. The 'Monitoring' tab is active, showing a 'Monitoring: Updates' section with a timestamp of 13:34. This section includes three items: 'Automatic Updates' (Enabled), 'Anti-Spam Database Id' (Daily update 17.02.2006 (day060217) + Recent 21.02.06 12:44:00 (MSK)), and 'Last Update' (2006-02-21 13:13). Below this is the 'Last Updater Events' section, which has a 'View' dropdown menu set to 'Notifications, Warnings and Errors'. A list of three events is shown, each with a green checkmark icon and a timestamp: '02-21 13:33:02 sfupdates: Data are up to date (upd time = 21.02.06 12:44:00 (MSK))', '02-21 13:13:11 sfupdates: New data installed (upd time = 21.02.06 12:44:00 (MSK))', and '02-21 11:09:05 sfupdates: New data installed (upd time = 21.02.06 10:44:00 (MSK))'. The footer contains the copyright notice: 'Copyright © 2002-2006 Kaspersky Lab. All rights reserved.'

図 28. 更新用モジュールの監視ページ

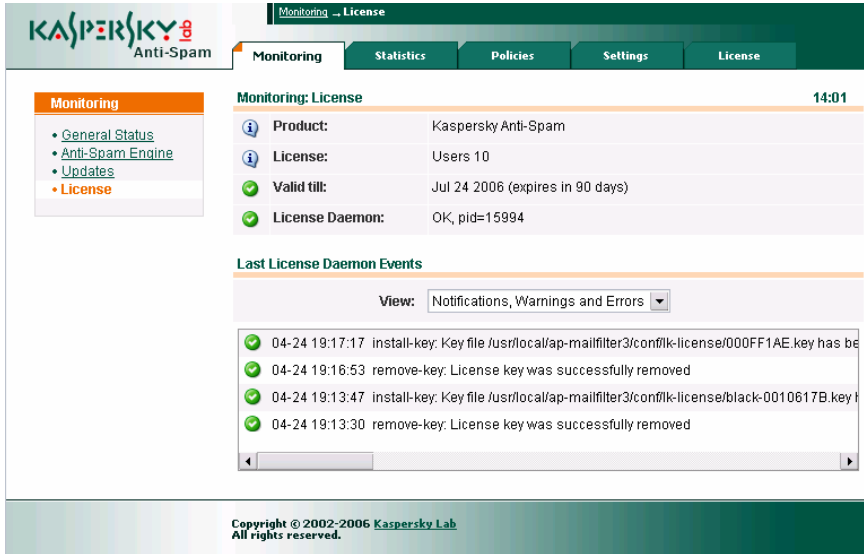
ページ上部の[Anti-Spam Updates]セクションには、以下のフィールドがあります。

- **[Automatic Updates]** – コンテンツフィルトレーションデータベースの自動更新が有効になっているかどうかを示すフィールド。コンテンツフィルトレーションデータベースを更新するスクリプトの設定については、51ページのセクション4.4.1および115ページの付録A.6を参照してください。
- **[Anti-Spam Database Id]** – インストールされているコンテンツフィルトレーションデータベースに関する情報。データベースのリリース日時と最終更新時刻。
- **[Last Update]** – コンテンツフィルトレーションデータベースの最終更新日時。長期間データベースが更新されていないと、監視システムが警告を表示します。

[Last Updater Events]セクションには、システムログ(syslog)に追加された、製品の更新システムから返されたメッセージのログが表示されます。日付が新しい順にメッセージが並んでおり、対応するアイコンは、メッセージの重要度を表しています。[View]ドロップダウンリストを使用して、ログに表示するメッセージのカテゴリを指定できます。ドロップダウンリストに表示される値とその意味は、フィルトレーションサーバの監視ページのセクションで説明されているものと同じです(79ページのセクション4.8.1.1を参照)。

4.8.1.3. ライセンシングモジュールに関する詳細情報

[Monitoring]→[License]ページには、現在のライセンスに関する情報とライセンシングモジュールから返されたメッセージのログが表示されます(図29を参照)。



The screenshot displays the Kaspersky Anti-Spam interface. At the top, there is a navigation bar with tabs for Monitoring, Statistics, Policies, Settings, and License. The 'License' tab is selected. The main content area is titled 'Monitoring: License' and shows the following details:

Product:	Kaspersky Anti-Spam
License:	Users 10
Valid till:	Jul 24 2006 (expires in 90 days)
License Daemon:	OK, pid=15994

Below the license details is a section for 'Last License Daemon Events'. A dropdown menu is set to 'Notifications, Warnings and Errors'. The event log shows the following entries:

- 04-24 19:17:17 install-key: Key file /usr/local/ap-mailfilter3/conf/ik-license/000FF1AE.key has be
- 04-24 19:16:53 remove-key: License key was successfully removed
- 04-24 19:13:47 install-key: Key file /usr/local/ap-mailfilter3/conf/ik-license/black-0010617B.key f
- 04-24 19:13:30 remove-key: License key was successfully removed

図 29. ライセンシングモジュールの監視ページ

ページ上部の[Monitoring:License]セクションには、以下のフィールドがあります。

- **[Product]** – インストールされている製品の名称
- **[License]** – 現在のライセンスと、その制限に関する情報
- **[Valid till]** – ライセンスの有効期限。監視システムは、ライセンスの有効期限が切れる 1 ヶ月前から警告を表示し始めます。
- **[License Daemon]** – ライセンシングサービスのステータス。正常にサービスが処理されている間は、プロセス ID (pid)もフィールド内に表示されます。

[Last License Daemon Events]セクションには、システムログ(syslog)に追加された、製品のライセンシングモジュールから返されたメッセージのログが表示されます。日付が新しい順にメッセージが並んでおり、対応するアイコンは、メッ

ページの重要度を表しています。[View]ドロップダウンリストを使用して、ログに表示するメッセージのカテゴリを指定できます。ドロップダウンリストに表示される値とその意味は、フィルトレーションサーバの監視ページのセクションで説明されているものと同じです(79 ページのセクション4.8.1.1を参照)。

4.8.2. システムメッセージの監視とレポート

Control Center で利用できる監視ツールの他に、Kaspersky Anti-Spam には、アンチスパムエンジンのステータスを休みなく監視できる *sfmonitoring* スクリプトが含まれています。このスクリプトは、*cron* サービスを使用して自動的に実行されます。*sfmonitoring* は、起動後、フィルトレーションサーバのステータスをチェックし、問題を検出すると、管理者に適切な通知を送信します。この監視スクリプトは、以下の 2 種類のメッセージを管理者に送信します。

- **新たに検出されたエラーに関するメッセージ** – フィルトレーションサーバの運用中に問題を検出したことを知らせるメッセージ。問題が発生した状況の説明も含まれます。このエラーメッセージは、1 回しか送信されません。問題が解決されなかった場合、1 日 1 回送信される既知の問題に関するレポートで問題が報告されます。
- **既知の問題に関する日次レポート** – レポート送信時に判明しているエラーおよび警告のリスト。このレポートには、新しいエラーと、レポートが生成されるまでに解決されなかった既知の問題の両方が含まれます。このレポートは、1 日 1 回午前 0 時に送信されます(サーバの時計に基づく)。レポートを強制的に配信するには、**root** として以下のコマンドを実行します。

```
# su -m mailft3 -c '/usr/local/ap-mailfilter3/control/  
bin/sfmonitoring -m'
```

サーバのコンソールにレポートを出力するには、以下のコマンドを実行します。

```
# su -m mailft3 -c '/usr/local/ap-mailfilter3/control/  
bin/sfmonitoring -p'
```



RedHat が稼働しているサーバに Kaspersky Anti-Spam がインストールされている場合は、以下のコマンドを使用して *sfmonitoring* ユーティリティを起動します。

```
su --m mailft3 -c  
'/usr/local/ap-mailfilter3/control/bin/sfmonitoring  
-<parameters>'
```

監視システムによって生成されたメッセージは、[Settings]→[Maintenance]→[Control Center]ページで指定されているアドレスに送信されます(64ページのセクション4.6を参照)。

4.9. Kaspersky Anti-Spam の統計情報

製品の運用結果を数量的に分析するために、Control Center には、処理メッセージに関する統計データを収集して Control Center のインタフェース内に表示するモジュールが含まれています。

cronサービスによって起動される特別なスクリプトが、統計データを収集して処理します(このスクリプトの詳細については、115ページの付録A.6を参照)。処理結果は、[Statistics]セクションのページにグラフで表示されます(図30を参照)。

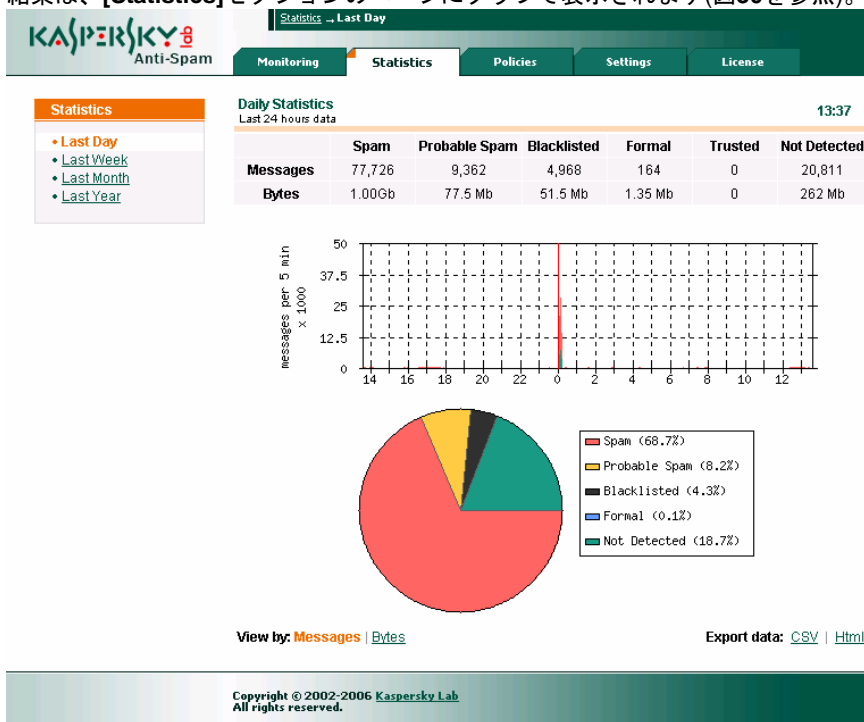


図 30. [Statistics]セクションのページ

[Statistics]セクションの各ページには、特定の期間の統計情報が表示されます。表示可能な以下のページへのリンクが、[Statistics]ウィンドウの右側にある[Period]メニュー内に配置されています。

- [\[Last Day\]](#) – 直前の 24 時間に処理されたメッセージの統計情報
- [\[Last Week\]](#) – 直前の 7 日間に処理されたメッセージの統計情報
- [\[Last Month\]](#) – 直前の 30 日間に処理されたメッセージの統計情報
- [\[Last Year\]](#) – 直前の 365 日間に処理されたメッセージの統計情報

ページ上部には、処理されたさまざまなタイプのメッセージの数およびサイズが、表にまとめられています。

表の下には、検出されたさまざまなタイプのメッセージ量の分布を示すグラフ(選択された期間の)と、割合(パーセント)を示す円グラフが表示されます。



円グラフでは、スパム認識結果から同じステータスを割り当てられたメールメッセージの量が色分けされて示されます。見やすくするために、比較的サイズが小さい区分は、**[Other]**という 1 つの区分にまとめられて表示されます。

左下にある[\[Messages\]](#)および[\[Bytes\]](#)リンクを使用して、処理されたメールトラフィックの統計情報を表示する際の測定単位(それぞれメッセージ数とバイト数)を選択できます。

右下にある[\[Export data CSV | Html\]](#)リンクを使用して、統計データを CSV (カンマ区切り)形式または HTML テーブルとしてエクスポートできます。

第5章 カスペルスキーアンチスパムの アンインストール

カスペルスキーアンチスパムをアンインストールするには、特権ユーザ（root）で作業してください。



アンインストールを行うと、自動的にカスペルスキーアンチスパムの機能が停止します。

アンインストールを行うと、カスペルスキーアンチスパム機能は停止し、インストール時に作成されたファイルやディレクトリが削除されます。ただし、設定ファイル・フィルタデータベース・ライセンスキーファイルは削除されません。また、メールサーバ設定は、インストール前のものを復元しようとしています。



カスペルスキーアンチスパムをインストール後、更にメールサーバ設定を変更している場合でも、メールサーバ設定はカスペルスキーアンチスパムインストール直前のものにに戻ります。従って、差分がある場合は手入力でマージする必要があります。

mailflt3 ユーザアカウントおよびグループは削除されません。

パッケージマネージャにより、アンインストール作業はいくつかの方法に分かれます。

- rpm パッケージを使用してインストールした場合は、次にコマンドでアンインストールします：

```
# rpm -e kas-3-<package version>
```
- deb パッケージを使用してインストールした場合は、次にコマンドでアンインストールします：

```
# dpkg -P kas-3
```
- tgz もしくは tbz パッケージを使用してインストールした場合は、次にコマンドでアンインストールします：

```
# pkg_delete kas-3-<package version>
```



Communicate Pro mail server に統合して使用している場合は、手動作業になります。アンインストールを行う前に Communicate Pro の設定からカスペルスキーアンチスパムの項目を削除します（付録 A.2.7 112 ページ参照）。

メールサーバ設定を、カスペルスキーアンチスパムをアンインストールせずに、インストールする直前の設定に戻す場合は、

/usr/local/ap-mailfilter3/bin/MTA-unconfig.pl を使用しません。

ただし、次の場合はメールサーバ設定復元ができないことがあります：

- カスペルスキーアンチスパムをインストール後に、更にメールサーバ設定を変更している場合。
- kas-exim クライアントプラグインを exim とともに使用している場合。
- Communicate Pro ユーザ。

上記の場合、メールサーバ設定を手作業で変更してください。詳しくは A.2 項 (96 ページ) をご参照ください。

第6章 よくある質問と回答（FAQ）

インストールや設定、操作に関するFAQです。分からないことがあったら、まずこちらを参照してください。



質問： ライセンスキー無しで製品は動きますか？

ライセンスキー無しではプログラムは動作しません。

プログラムの試用をお望みの場合は 2 週間(または 1 ヶ月)有効のトライアル用キーを発行いたします。試用期間が過ぎるとライセンスキーは無効になります。



質問： ライセンスキーの期限が切れるとどうなりますか？

ライセンスキーの有効期限が切れてもプログラムは機能を続けます。アップデート機能だけが無効となるので、既にダウンロード済みの定義ファイルを利用してメールトラフィックのフィルタリングやスパムメールの判定を実行できますが、最新のスパムメールには対応できません。

ライセンス期限が切れた場合には管理者に知らせるか、販売元あるいはカスペルスキーラボスで新しいキーを購入してください。



質問： なぜ定期的なアップデートが必要なのですか？

スパムメールは全ネットワークユーザにとって深刻な問題です。最新のデータによると、インターネット上の総メール量のうち 75~80%がスパムメールであり、更に、スパムメールは絶えず新しいタイプのものが出現します。このような状況に対応するためには、最新のデータベースが必要です。カスペルスキーでは約 20 分毎にデータベースの更新を実施しています。



質問： プログラムが動作しません。どうしたらいいですか？

取扱説明書あるいは弊社サイトに対応策が書かれていないか確認してください。

解決しない場合は、販売元または弊社サポートサービス (support@kaspersky.co.jp)あるいはライセンスキー情報に記載されている宛先に問い合わせてください。

メールにてお問合わせの際には、対応を早めるため、次の情報をご記入ください(メールはテキスト形式で作成してください)：

- 件名にお使いのOS、カスペルスキー製品の名称、トラブル概要をご記入ください。例：
Linux, カスペルスキーアンチスパム 3.0, アップデートが機能しない
- 本文の始めにOSと製品のバージョン、ライセンスキーナンバーを記入してください。ライセンスキー情報は、コントロールセンターの **License** ページで確認ができます。(4.7.1 項 74 ページ参照)。
- カスペルスキー社が連絡可能なアドレスからメールを送信してください。



質問：プログラムが実際にスパムメールをフィルタしているかどうか確認する方法はありますか？

GTUBE (Generic Test for Unsolicited Bulk Email) の雛形を使用可能です。GTUBE を使用した動作検証は、テストウイルス EICAR を使用した動作確認と同様です。

以下の文字列を含むメールを作成してください：

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-T  
EST-EMAIL*C.34X
```

そのうえで、カスペルスキーアンチスパムの保護対象になっているメールアドレス宛にメールを送信してください。スパムメールと判定されれば、設定されたルールに従い、カスペルスキーアンチスパムは動作するでしょう。



質問：サーバの負荷が上がり、スパムフィルタが機能しません。
X-SpamTest-Info: Not processed
というヘッダが付与されます。

トラフィックの上昇により、ライセンスモジュール (*kas-license*) がアプリケーションと通信できなくなっている可能性があります。

FilterLicenseConnectTimeout と **FilterLicenseDataTimeout** 設定パラメータを増やし、*kas-license* のタイムアウトを延長してください。



質問: スпамメールをフィルタしません。次のヘッダが付与されます：
X-SpamTest-Info: No License
ライセンス有効期限が切れている、もしくはライセンスがインストールされていない状態です。ライセンスを正しくインストールしてください (4.7 項 74 ページ参照)



質問: ヘッダから得られる IPv6 アドレスをチェックできません。

IPv6 には対応していません。



質問: Exim と連携させようとすると *MTA-config.pl* が失敗し、次のメッセージが出ます：

Your Exim configuration file /usr/local/etc/exim/configure already contains kas-exim local_scan configuration parameters. If your Exim hasn't been integrated with kas-exim, remove all local_scan parameters and try again.

ご利用中の Exim は、既に kas-exim プラグインモジュールと連動しているようです。*MTA-config.pl* スクリプトは、kas-pipe プラグインモジュールをインストールするものですので、まず、kas-exim モジュールの削除を行ってください (A.2.5 項 108 ページをご参照ください)

付録A. KASPERSKY ANTI-SPAM の追加情報

A.1. ファイルシステム内の製品ファイルの場所

Kaspersky Anti-Spam をインストールすると、配布ファイルが以下の場所に保存されます。

`/usr/local/ap-mailfilter3/` – 製品がインストールされるメインディレクトリ。このディレクトリには、以下のディレクトリが含まれています。

`bin/` – 実行ファイルおよびスクリプトが保存されるディレクトリ

`cfdata/` – コンテンツフィルタリングデータベースおよび Kaspersky Anti-Spam モジュールの更新が保存されるディレクトリ

`conf/` – 設定ファイルが保存されるディレクトリ。このディレクトリには、以下のサブディレクトリが含まれています。

`def/` – メッセージフィルタリングポリシーのコンパイルに必要なファイルが含まれているディレクトリ。コンテンツフィルタリングデータベースのソースファイルやフィルタリングポリシーに関する情報が含まれているファイルなど。

`data/` – 設定バイナリファイルが保存されるディレクトリ。

`src/` – ルールのコンパイルに使用されるフィルタリングルールの一時的な形態が含まれているディレクトリ

`tmp/` – 設定データの処理に使用される一時ファイルを保存するディレクトリ

`control/` – Control Center のファイルが含まれているディレクトリ。このディレクトリには、以下のサブディレクトリが含まれています。

`bin/` – Control Center の実行ファイルおよびスクリプトが含まれているディレクトリ

`lib/` – Control Center によって使用されるライブラリファイルが含まれているディレクトリ

`stat/` – ログ処理および統計情報収集システムのデータファイルが含まれているディレクトリ

`tmp/` – Control Center の一時ファイルを保存するディレクトリ

`www/` – Control Center の Web インタフェースによって使用される cgi スクリプトおよびグラフィックファイルが含まれているディレクトリ

`etc/` – Kaspersky Anti-Spam 設定ファイルが含まれているディレクトリ

`lib/` – ランタイムライブラリ

`log/` – フィルタリングサーバのログを保存するディレクトリ。このログは、

統計情報の処理に使用されます。

run/– 製品の作業ディレクトリ。このディレクトリには、フィルタリングサーバの実行中の処理の、*pid* ファイルも保存されます。

src/– *kas-exim* モジュールのソースファイルが含まれているディレクトリ

A.2. 各種メールサーバのクライアントモジュール

Kaspersky Anti-Spam には、さまざまなメールサーバに製品を統合できるように、以下のクライアントモジュールが含まれています。

- *kas-milter* – Sendmail メールサーバ用のクライアントモジュール
- *kas-pipe* – 共通クライアントモジュール。Postfix および Exim メールサーバの場合、デフォルトで使用されます。
- *kas-exim* – Exim メールサーバ用のクライアントモジュール(代替バージョン)
- *kas-qmail* – Qmail メールサーバ用のクライアントモジュール
- *kas-cgpro* – Communigate Pro メールサーバ用のクライアントモジュール

Kaspersky Anti-Spam のインストール中に、特別な設定スクリプトを実行することにより、製品がメールサーバに統合されます。

この付録では、クライアントモジュールの操作、設定ファイル、およびメールサーバ固有の設定について詳しく説明します。

A.2.1. クライアントモジュールとフィルタリングサーバ間のやり取り

クライアントモジュールとフィルタリングサーバ間のやり取りは、以下のアルゴリズムで行われます。

1. クライアントモジュールが、メールサーバからメールメッセージを受信し、フィルタリングサーバに接続要求を送信します。
2. マスタプロセスが、既に行われているフィルタリングプロセスを選択するか、新規でフィルタリングプロセスを作成し、クライアントモジュールと指定されたフィルタリングプロセス間の接続を確立します。
3. メッセージのチェックを受けるために、クライアントモジュールが、確立された接続を介してメッセージを送信し、フィルタリングプロセスから処理結果を受け取ります。

4. 受け取った処理結果に従って、クライアントモジュールがメッセージを変更し(必要な場合)、メールサーバに返します。

クライアントモジュール、フィルタリングマスタプロセス、およびフィルタリングプロセスの間のやり取りは、ネットワークまたはローカルソケットを介して、インターネットプロトコルを使用して行われます。

ネットワークソケットを使用する場合は、フィルタリングサーバとメールサーバを配置して、クライアントモジュールをさまざまなサーバに統合することができます。メールトラフィックの処理量があまり多くない場合は、専用フィルタリングサーバで多数のメールサーバに対応することができます。その場合は、Kaspersky Anti-Spam とメールサーバコンポーネント間のやり取りを制御する設定を手動で調整する必要があります。

A.2.2. クライアントモジュールの共通設定

Kaspersky Anti-Spam バージョン 3.0 では、クライアントモジュールの設定は、フィルタリングサーバの共通設定ファイル(filter.conf)に保存されます。このファイルは、`/usr/local/ap-mailfilter3/etc/`ディレクトリ内に作成されます。

以下の設定は、すべてのクライアントモジュールに共通な設定です。

- **ClientConnectTo** – フィルタリングサーバとのやり取りで使用するソケットアドレス。「`tcp:<host>:<port>`」形式のエントリ(`<host>`はフィルタリングサーバの IP アドレス、`<port>`は接続ポート)はネットワークソケットを指し、「`unix:<path_to_file>`」形式のエントリ(`<path_to_file>`はファイルのパス)はローカルソケットを指しています。
- **ClientConnectTimeout** – フィルタリングサーバに接続する際の最大待機時間(秒単位)
- **ClientDataTimeout** – フィルタリングサーバとデータ交換を行う際の最大待機時間(秒単位)
- **ClientOnError** – エラー処理モード(フィルタリングサーバへの接続を確立できない場合やデータ交換中にタイムアウトになった場合など)。以下の値を指定できます。
 - **reject** – メッセージを受け入れずに、SMTP セッション中にエラーコード 5xx を返します。
 - **tempfail** – 一時的にメッセージを拒否し、SMTP セッション中にエラーコード 4xx を返します(デフォルト)。
 - **accept** – メッセージを受け入れます。



Sendmail メールサーバを使用している場合に **accept** を指定すると、メッセージを受け入れますが、サーバで使用され

ている Kaspersky Anti-Spam よりも後となる Milter-filters による処理が行われません。

- **ClientDefaultDomain** – メールドメインが指定されていないアドレスに設定されるメールドメイン名。たとえば、たとえば、デフォルトドメインとして「mycompany.com」を指定した場合、「someuser」というアドレスは「someuser@mycompany.com」として解釈されます。このパラメータを定義しなかった場合、ドメイン名の代入が行われません(デフォルトでは、このパラメータは定義されていない)。
- **ClientFilteringSizeLimit** – フィルタリングサーバに渡すことが可能な最大メッセージサイズ(キロバイト単位)。このサイズを超えるメールメッセージは、フィルタリングサーバで処理されずに通過します。デフォルト値は **500** です。
- **ClientMessageStoreMem** – ディスクでの一時データの保存が許可される最小メッセージサイズ(キロバイト単位)。このモードを使用して、RAMの使用量を制御できます。すべてのデータをRAMに保存するには、このパラメータに **0** (デフォルト値)を設定します。
- **ClientTempDir** – 一時ファイル保存ディレクトリのパス

A.2.3. kas-milter – Sendmail メールサーバ用のクライアントモジュール

Sendmail メールサーバとの統合では、Kaspersky Anti-Spam は *kas-milter* モジュールを使用します。クライアントモジュールとメールサーバ間のやり取りは、*libmilter* ライブラリを使用して行われます。

図 31には、Kaspersky Anti-SpamがSendmailと共に使用されている場合の、モジュール間のやり取りが示されています。

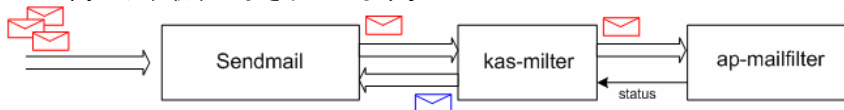


図 31. Kaspersky Anti-Spam と Sendmail メールサーバ間のやり取り

クライアントモジュールとメールサーバ間のやり取りは、特別なスクリプト(24ページのセクション3.4を参照)を使用するか、手動で設定することができます。クライアントモジュールを手動で設定するには、`/usr/local/ap-mailfilter3/etc/`ディレクトリにある *filter.conf* 設定ファイルを編集します。クライアントモジュールの設定は、このファイル内の以下の部分に含まれています。

```
ClientConnectTo tcp:127.0.0.1:2277
```

```
ClientConnectTimeout 10
ClientDataTimeout 30
SendMailAddress unix:/var/run/kas-milter.socket
ClientOnError accept
ClientFilteringSizeLimit 500
ClientDefaultDomain localhost
```

付録A.2.2で説明されている設定に加えて、kas-milterモジュールの場合、*filter.conf* ファイル内で**SendMailAddress**パラメータを設定することができます。このパラメータは、Sendmailとのやり取りで使用されるソケットを定義します。Sendmailがkas-milterとやり取りするよう設定するには、以下の行を*sendmail.cf* 設定ファイルに追加します。

```
Xkasfilter,S=local:/var/run/kas-milter.socket, T=C:10s,S:20s, R:30s
O InputMailFilters=kasfilter
```

sendmail.cf フィルタの設定に関する詳細情報については、Sendmailのマニュアルを参照してください。



一般に、オペレーティングシステムのロード中に、Kaspersky Anti-Spam よりも前に Sendmail が起動します。そのため、Sendmail が、適切なソケットを見つめることができず、システムログに以下の警告メッセージを書き込みます。

WARNING: Xkas: local socket name <socket_file> missing

見つからないソケットファイルは、Kaspersky Anti-Spam の実行後に kas-milter モジュールによって作成されるため、この警告は不具合を示すものではありません。

kas-milter モジュールを Sendmail メールサーバと共に使用する場合、以下のような特徴があります。

- kas-milter は、処理中にメッセージのコピーを作成しません。つまり、異なる処理ルールが設定されているさまざまなグループに属する多数の受信者にメッセージが送信される場合、すべてのグループの設定に従ってメッセージが処理されます。たとえば、以下のようになります。

あるメッセージが、alice@mycompany.comとbob@mycompany.comという電子メールアドレス宛てに送信されます。これらの電子メールアドレスは、それぞれ[sales]グループおよび[managers]グループに属しています。フィルタリング結果に従って、このメッセージは、[sales]グループの場合は[Spam]ステータス、[managers]グループの場合は[Not detected]ステータスが割り当てられました。[sales]グループに定義されているルールに従って、スパムであると認識された([Spam]ステータスが割り当てられた)メッセージの件名に、[!! SPAM]というタグが付けられます。[managers]グループに定義されているルールでは、[Not Detected]ステータス

タスのメッセージはすべて受け入れられます。その結果、**[!! SPAM]**タグの付いたメールメッセージが、両方の受信者に配信されます。このメッセージには、以下のヘッダが含まれることになります。

X-Spamtest-Status-Extended: SPAM

X-Spamtest-Status-Extended: Not detected

X-Spamtest-Group-ID: 00000002

X-Spamtest-Group-ID: 00000001

これらのヘッダは、1 と 2 (**[sales]**グループと**[managers]**グループのID)のIDを持つグループに定義されているルールに従ってメッセージが処理され、メッセージに**[SPAM]**ステータスと**[Not Detected]**ステータスが割り当てられたことを示しています。ヘッダの詳細については、113ページのセクションA.5を参照してください。

- メッセージが複数の受信者宛てに送信されていて、一部の受信者への配信が禁止され(受信拒否動作が選択されている)、残りの受信者への配信は許可されている(受信許可動作が選択されている)場合は、各受信者に対して不達通知は送信されません。
- Sendmail でポート 25 への同時接続数を制限できないため、*ap-mailfilter* フィルタリングプロセスの実行数は、入力接続数に依存します。そのため、サーバに余計な負荷がかかる可能性があります。

A.2.4. *kas-pipe* – Postfix および Exim メールサーバ用のクライアントモジュール

kas-pipe モジュールは、Kaspersky Anti-Spam の共通クライアントモジュールです。このモジュールは、サポート対象のすべてのメールサーバとの統合に使用できます。

デフォルトインストールでは、Postfix および Exim との統合に *kas-pipe* が使用されます。

kas-pipe モジュールは、メールを受け取り、フィルタリングプロセス後、SMTP または LMTP プロトコルを使用してそのメッセージをメールサーバに返します。*kas-pipe* モジュールは、外部アプリケーション(メールサーバなど)から起動されます。メールの送信には、ネットワークまたはローカルソケットが使用されます。また、*fork* および *exec* コマンドを使用して、受け取りアプリケーションを実行することもできます。

図 32には、Kaspersky Anti-Spamが*kas-pipe*と共に使用されている場合の、モジュール間のやり取りが示されています。

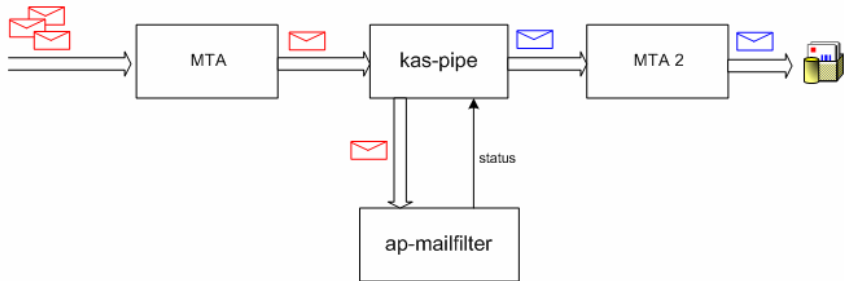


図 32. kas-pipe モジュールの使用

設定が異なる 2 つ目のインスタンスの実行をサポートするメールサーバ、LMTP プロトコル経由で配信を行うメールサーバ、またはすべてのメールを SMTP 経由で指定されたメールサーバに配信するメールサーバの場合に、この実装方法を使用できます。

クライアントモジュールとメールサーバ間のやり取りは、特別なスクリプト(24 ページのセクション3.4を参照)を使用するか、手動で設定することができます。クライアントモジュールを手動で設定するには、`/usr/local/ap-mailfilter3/etc/ディレクトリ`にある `filter.conf` 設定ファイルを変更します。クライアントモジュールの設定は、このファイル内の以下の部分に含まれています。

```

ClientConnectTo tcp:127.0.0.1:2277
ClientConnectTimeout 10
ClientDataTimeout 30
PipeInProtocol lmtpt
PipeOutProtocol lmtpt
PipeOutgoingAddr exec:/usr/sbin/sendmail -bs
PipeMultipleMessagesAllowed yes
ClientDefaultDomain localhost
ClientOnError accept
ClientFilteringSizeLimit 500

```

付録A.2.2で説明されている設定に加えて、kas-pipeモジュールの場合、`filter.conf` ファイル内で以下のパラメータを設定することができます。

- **PipeInProtocol** – メールメッセージの受信に使用するプロトコル。 **smtp** または **lmtpt** を指定できます。
- **PipeOutProtocol** – 処理済みメールメッセージの送信に使用するプロトコル。 **smtp** または **lmtpt** を指定できます。

- **PipeHELOGreeting** – *kas-pipe* モジュールが SMTP セッション中にグリーティング用を使用するドメイン名。デフォルト値は、**kas30pipe.+ <サーバドメイン名>**です。
- **PipeOutgoingAddr** – 処理済みメッセージの送信に使用するソケットアドレス。「**tcp:<host>:<port>**」形式のエントリ(<host>はフィルタリングサーバの IP アドレス、<port>は接続ポート)はネットワークソケットを指し、「**unix:<path_to_file>**」形式のエントリ(<path_to_file>はソケットファイルのパス)はローカルソケットを指し、「**exec:/<path to the program executable> – <parameters>**」形式のエントリはメッセージの送信用に実行されるプログラムを指しています。
- **PipeOutConnectTimeout=5...600** – ソケットまたは処理済みメッセージの送信に使用されるプログラム(**PipeOutgoingAddr** パラメータで定義される)への接続を確立する際のタイムアウト時間
- **PipeOutDataTimeout=5...600** – **PipeOutgoingAddr** パラメータで定義されるソケットまたはプログラムを介したデータ送信のタイムアウト時間
- **PipeMultipleMessagesAllowed** – フィルタリング結果がユーザごとに異なる場合にメッセージのコピーを作成するかどうか。**yes** または **no** を指定できます。
- **PipeUseXForward** – メッセージの送信元サーバの IP アドレスを検索する XForward コマンドのサポート(Postfix を使用する場合のみ)。**yes** または **no** を指定できます。
- **Pipe8BitHack** – 8BITMIME 拡張の使用。**yes** または **no** を指定できます。使用しているメールサーバが、8BITMIME 拡張をサポートするよう設定されている場合は、**yes** を指定します。
- **PipeBufferedIO** – メールメッセージ処理中のバッファリングの使用。バッファリングを使用することにより、RAM の使用量が追加されるため、メッセージ処理を高速化できます。**yes** または **no** を指定できます。

kas-pipe クライアントモジュールを使用する場合、以下のような特徴があります。

- メールメッセージが SMTP または LMTP を介して *kas-pipe* に送信されるため、メッセージの送信元サーバの IP アドレスを定義することができません(Postfix 以外のメールサーバの場合)。[Received]ヘッダ内のアドレスに対してのみ、すべての DNS チェックを実行できます。Postfix メールサーバを使用する場合、**PipeUseXForward** に **yes** を設定すると、*kas-pipe* がメッセージの送信元サーバの IP アドレスを検索できるようになります。
- *kas-pipe* は、メッセージキューに入った後にメールサーバに統合されるため、SMTP セッション中に **reject** 動作を実行できません。メッセージに対

して **reject this message** 動作が選択されている場合は、不達通知が送信者に送信されます。

A.2.4.1. kas-pipe と連動するよう Postfix を設定する

このセクションでは、以下の運用体系を実装する Postfix メールサーバ用の *kas-pipe* の設定例について説明します。

- *kas-pipe* は、コンテンツフィルタ (*content_filter*) として機能します。
- *kas-pipe* は、Postfix 設定ファイルにおいて手動で定義された *localhost:9026* ネットワークソケットおよび *kas3scan* サービスを介してメールを受信します。
- *kas-pipe* は、SMTP プロトコルを使用して、処理済みメールを *localhost:9025* ソケットを介して Kaspersky Anti-Spam に送信します。



kas3scan サービスは、同時接続の数を制限し、*smtp_send_xforward_command* オプションを使用して、送信者のサーバの IP アドレスを *kas-pipe* モジュールに送信します。



この運用体系を実装するには、以下の手順を実行します。

1. *filter.conf* 設定ファイルで、以下の値を指定します。

```
ClientConnectTo tcp:127.0.0.1:2277
PipeMultipleMessagesAllowed Yes
PipeInProtocol smtp
PipeOutProtocol smtp
PipeOutgoingAddr          tcp:127.0.0.1:9025
PipeUseXForward yes
```

2. Postfix 設定ファイル (*master.cf*) を以下のように変更します。

```
smtp      inet  n       -       n       -       -       smtpd
### KASPERSKY ANTI-SPAM BEGIN ###
  -o content_filter=kas3scan:127.0.0.1:9026
### KASPERSKY ANTI-SPAM END ###

pickup   fifo  n       -       n       60     1       pickup
### KASPERSKY ANTI-SPAM BEGIN ###
  -o content_filter=kas3scan:127.0.0.1:9026
```

```

### KASPERSKY ANTI-SPAM  END ###

### KASPERSKY ANTI-SPAM  BEGIN ###
127.0.0.1:9026 inet n  n  n  -  20  spawn
user=mailft3 argv=/usr/local/ap-mailfilter3/bin/
kas-pipe
127.0.0.1:9025 inet  n  -  n  -  25  smtpd
-o smtpd_authorized_xforward_hosts=127.0.0.0/8
  -o local_recipient_maps=
  -o relay_recipient_maps=
  -o smtpd_restriction_classes=
  -o smtpd_client_restrictions=
  -o smtpd_helo_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,
reject
  -o mynetworks=127.0.0.0/8
  -o strict_rfc821_envelopes=no
  -o smtpd_error_sleep_time=0
  -o smtpd_soft_error_limit=1001
  -o smtpd_hard_error_limit=1000
  -o receive_override_options=no_address_mappings

kas3scan  unix  -  -  n  -  10  smtp
  -o smtp_send_xforward_command=yes
### KASPERSKY ANTI-SPAM  END ###

```



Postfix バージョン 2.1 以上の場合、プロキシフィルタ (*smtpd_proxy_filter*) として機能するよう *kas-pipe* を設定できます。その場合、SMTP セッション中に **reject** 動作が使用されるため、メッセージの処理が速くなります。ただし、メールサーバの負荷が重い場合は、この設定を使用しないでください。プロキシフィルタとして機能するよう *kas-pipe* を設定するには、上記の例の最初の 2 行を以下の行に置き換えてください。

```

smtp      inet      n      -      n      -      -      smtpd
  -o smtpd_proxy_filter=127.0.0.1:9026

```

A.2.4.2. kas-pipe と連動するよう Exim を設定する

kas-pipe を Exim メールサーバに統合するには、Exim 設定ファイル内のルータリストの先頭に新規ルータを追加し、kas-pipe の起動に使用するこのルータ用のトランスポートを追加します。このルータは、ローカルで ESMTP プロトコルを使用して送信されたメールの処理には使用されないため、条件付きのルータです。Exim に統合されている kas-pipe クライアントモジュールは、以下の体系に従ってメールメッセージを処理します。

1. Exim は、入ってくるメッセージをポート 25 で受信し、それらをキューに入れます。
2. Exim は、キューからメッセージを選択し、リスト内のルータを試して、メッセージに適するルータを決定します。kas-pipe を指すルータがリストの先頭にあるため、すべてのメッセージが、対応するトランスポートを使用して kas-pipe クライアントモジュールに送信されます。
3. メッセージの処理が完了したら、kas-pipe は、`exim -bs` コマンドを使用してメッセージを返します。メッセージは、再び Exim のキューに入ります。ただし、メールがローカルで送信されたため、kas-pipe モジュール用のルータがスキップされます。
4. Exim が、メッセージを受信者に配信します。



この運用体系を実装するには、以下の手順を実行します。

1. `filter.conf` 設定ファイルで、以下の値を指定します。

```
PipeInProtocol lmtpt
PipeOutProtocol smtp
PipeOutgoingAddr exec:/usr/local/sbin/exim -bs
```
2. Exim 設定ファイルを以下のように変更します。
 - **ROUTERS** セクションに以下の行を追加します。

```
begin routers

# ROUTER ADDED BY KAS 3.0 INSTALLER
kas30router:
  driver = accept
  local_parts = passwd;$local_part : lsearch
```

```
condition = "${if !eq {$received_protocol}
{local-esmtp}{yes}}"
transport = kas30transport
```

- **TRANSPORTS** セクションに以下の行を追加します。

```
begin transports
# TRANSPORT ADDED BY KAS 3.0 INSTALLER
kas30transport:
driver = lmtp
batch_max = 100
command = /usr/local/ap-mailfilter3/bin/kas-pipe
return_path_add = false
```

Debian ディストリビューションパッケージの場合、メールサーバの設定が `/etc/exim4/exim4.conf.template` テンプレートの特別なスクリプト (`update-exim4.conf`)、または `/etc/exim4/conf.d/` ディレクトリ内の複数のテンプレートから生成されるため、Exim と統合することでさまざまな固有の機能を使用できるようになります。テンプレートの数(1 つまたは複数)は、Exim の `exim4-update.conf.conf` 設定ファイルの **use_split_files** オプションで定義されます。生成された設定は、`/var/lib/exim4/config.autogenerated` ファイルに保存されます。

Debianディストリビューションパッケージの場合、手動または自動で特別なスクリプトを使用してKaspersky Anti-SpamをEximメールサーバに統合できます(24ページのセクション3.4を参照)。



kas-pipe モジュールと連動するよう Exim メールサーバを設定するには、以下の手順を実行します。

- `exim4.conf.template` テンプレートをEximの設定に使用する場合は、上記の文字列を、対応する**ROUTERS**および**TRANSPORTS**セクションに追加します。
- `/etc/exim4/conf.d/` ディレクトリ内のテンプレートをEximの設定に使用する場合は、以下の手順を実行します。
 1. `/etc/exim4/conf.d/router/` ディレクトリ内に、`099_exim4-config_kas30router` というファイルを新規作成し、このファイルに以下の文字列を追加します。

```
kas30router:
driver = accept
local_parts = passwd;$local_part : lsearch
```

```
condition = "${if !eq {$received_protocol}
{local-esmtp}{yes}}"
transport = kas30transport
```

2. `/etc/exim4/conf.d/transport/` ディレクトリ内に、`30_exim4-config_kas30transport` というファイルの新規作成し、このファイルに以下の文字列を追加します。

```
kas30transport:
driver = lmtp
batch_max = 100
command = /usr/local/ap-mailfilter3/bin/kas-pipe
return_path_add = false
```

変更が完了したら、`update-exim4.conf` スクリプトを実行して新しい値を適用します。

A.2.5. *kas-exim* – Exim メールサーバ用のクライアントモジュール

kas-exim モジュールにより、*localscan API* を使用する Exim メールサーババージョン 4.xx への Kaspersky Anti-Spam の統合が可能になります。

kas-exim モジュールは、代替ソリューションとして使用されます。標準的なインストールの場合、*kas-pipe* クライアントモジュールを使用して Exim との統合が行われます。*kas-pipe* とは異なり、*kas-exim* モジュールは、メールメッセージの送信用にメールサーバの 2 つ目のコピーを起動する必要がありません。

localscan API を使用するには、Exim をコンパイルし直す必要があります。そのため、*kas-exim* モジュールは、C 言語で記述されたソースコードとして出荷されており、手動でインストールする必要があります。



Exim メールサーバと統合された *kas-exim* モジュールをコンパイルし直すには、以下の手順を実行します。

1. `/usr/local/ap-mailfilter3/src/` に作成されている `kas_exim.c` ファイルを、Exim ソースファイルのツリー内の *Local* ディレクトリに保存します。
2. *Local* ディレクトリ内の *Makefile* ファイルを以下のように変更します。

```
CFLAGS= -I/usr/local/ap-mailfilter3/include
EXTRALIBS_EXIM=-L/usr/local/ap-mailfilter3/lib
-lspamtest
LOCAL_SCAN_SOURCE=Local/kas_exim.c
```

```
LOCAL_SCAN_HAS_OPTIONS=yes
```

3. Exim をコンパイルします。



kas-exim の操作に必要な値は、すべて Exim 設定ファイル内で指定されます (filter.conf ではありません)。

以下の例は、Exim 設定ファイル内の、kas-exim モジュール用のオプションが含まれている部分です。

```
begin local_scan
kas_connect_to = tcp:127.0.0.1:2277
kas_connect_timeout = 40
kas_data_timeout = 30
kas_default_domain = localhost
kas_filtering_size_limit = 500
kas_on_error=accept
kas_log_level=3
```

この部分には、以下のオプションが含まれています。

- **kas_connect_to** – フィルタリングサーバとやり取りするためのソケットのアドレス。このアドレスの形式は、「**tcp:<host>:<port>**」(**<host>**はフィルタリングサーバのIPアドレス、**<port>**はネットワークソケットを指定するポート)または「**unix:<path_to_file>**」(**<path_to_file>**はソケットファイルのパス(ローカルソケットを指定する))の形式のレコードを使用します。
- **kas_connect_timeout** – フィルタリングサーバとの接続を確立する最大時間(秒単位)。
- **kas_data_timeout** – フィルタリングサーバとのデータ交換セッションの最大時間(秒単位)。
- **kas_default_domain** – オリジナルドメインが指定されていない場合に、アドレスに使用するメールアドレスの名前。
- **kas_filtering_size_limit** – フィルタリングサーバに送信することが可能なメッセージの最大サイズ(キロバイト単位)。このサイズを超えるメッセージは、処理されずに通過します。
- **kas_on_error** – エラー処理モード(フィルタリングプロセスとの接続を確立できない場合や、データ交換のタイムアウト時間を過ぎた場合など)。以下の値を指定できます。
 - **reject** – 入ってくるメッセージを拒否し、SMTP セッション中に 5xx コードを返します。

- **tempfail** – 入ってくるメッセージを一時的に拒否し、SMTP セッション中に 4xx コードを返します(デフォルト値)。
- **accept** – メッセージを受け入れます。
- **kas_log_level** – ログファイルの詳細レベル。Exim デバッグモードでデータが記録されます。

kas-exim モジュールを Exim メールサーバと共に使用する場合、以下のような特徴があります。

- kas-milter と同様に、kas-exim は、処理中にメッセージのコピーを作成しません。つまり、さまざまな処理ルールが設定されているさまざまなグループに属する複数の受信者宛てにメッセージが送信される場合、これらの各グループのルールに従ってメッセージが処理されます。
- 複数の受信者宛てに送信されたメッセージが、一部の受信者への配信が禁止されて(受信拒否)、残りの受信者への配信が受け入れられた(受信許可)場合、一部の受信者にメッセージを配信できなかったことは送信者には知らされません(不達通知は送信されない)。

A.2.6. kas-qmail – Qmail メールサーバ用のクライアントモジュール

kas-qmail モジュールにより、Kaspersky Anti-Spam と Qmail メールサーバ間のやり取りが可能になります。このモジュールを使用する場合、以下のアルゴリズムでメールトラフィックが処理されます。

1. Qmailのqmail-queueモジュールが、kas-qmailクライアントモジュールと置き換えられます。kas-qmailクライアントモジュールは、受信メールをフィルタリングサーバの処理に渡します。
2. 処理済みのメールトラフィックが kas-qmail モジュールに返され、qmail-queue に渡されます。

図 33 は、Kaspersky Anti-Spamがkas-qmailモジュールを使用する場合のモジュール間のやり取りを示しています。

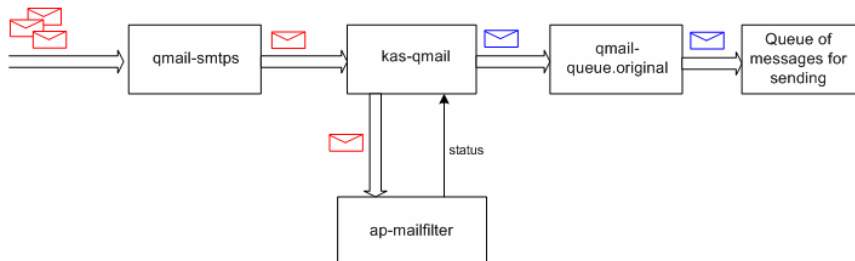


図 33. Kaspersky Anti-Spam と Qmail メールサーバ間のやり取り

手動または自動で特別なスクリプトを使用してこのクライアントモジュールを Qmail メールサーバに統合できます(24ページのセクション3.4を参照)。

クライアントモジュールオプションを手動で設定するには、`/usr/local/ap-mailfilter3/etc/1`に作成されている `filter.conf` 設定ファイルを変更します。

以下の例は、`filter.conf` 設定ファイル内の、kas-qmail 用の設定オプションが含まれている部分です。

```
ClientConnectTo tcp:127.0.0.1:2277
ClientConnectTimeout 10
ClientDataTimeout 30
QMailOriginalQueue /var/qmail/bin/qmail-queue.kas
ClientOnError accept
ClientFilteringSizeLimit 500
ClientDefaultDomain localhost
```

付録A.2.2で説明されているオプションの他に、このファイルには、本来の `qmail-queue` モジュールの完全パスを指定する `QmailOriginalQueue` オプションも含まれています。



kas-qmail クライアントモジュールと連動するよう Qmail を設定するには、以下の手順を実行します。

1. 以下のコマンドを使用して、`qmail-queue` モジュールのオリジナルファイルの名前を変更します。

```
# mv /var/qmail/bin/qmail-queue /var/qmail/bin/qmail-queue.kas
```

2. 以下のコマンドを使用して、`qmail-queue` の代わりに `kas-qmail` をインストールします。

```
# cp /usr/local/ap-mailfilter3/bin/kas-qmail
/var/qmail/bin/qmail-queue
# chown qmailq /var/qmail/bin/qmail-queue
# chgrp qmail /var/qmail/bin/qmail-queue
# chmod 04755 /var/qmail/bin/qmail-queue
```

A.2.7. *kas-cgpro* – Communigate Pro メールサーバ用のクライアントモジュール

kas-cgpro モジュールにより、Kaspersky Anti-Spam と Communigate Pro メールサーバ間のやり取りが可能になります。以下のアルゴリズムでメールトラフィッ

クが処理されます。

1. Communigate Pro が、すべての受信メールを kas-cgpro クライアントモジュールに渡します。
2. kas-cgpro モジュールがメッセージを処理し、各メッセージに特別なヘッダを挿入するなどしてメッセージを変更し、処理済みメールを *Submitted* ディレクトリに配置します。DISCARD 応答が Communigate Pro に返されます。
3. *PIPE* ドライバが、*Submitted* ディレクトリに配置されたメッセージを Communigate Pro メールサーバに渡します。Communigate Pro メールサーバは、このメッセージを *kas-cgpro* モジュールに返します。
4. kas-cgpro モジュールは処理済みメッセージ(特別なヘッダが付いたメッセージ)を処理しないため、Communigate Pro が[OK]を受け取り、メッセージが受信者に配信されます。

Communigate Pro との統合は、手動でのみ行えます。クライアントモジュールとやり取りするためのオプションは、*filter.conf* ファイル内で指定します。Communigate Pro メールサーバ用のオプションは、メールサーバの Web インタフェースを使用して変更します。

クライアントモジュールの設定は、*filter.conf* ファイル内の以下の部分に含まれています。

```
ClientConnectTo tcp:127.0.0.1:2277
```

```
ClientConnectTimeout 10
```

```
ClientDataTimeout 30
```

```
CGProSubmittedFolder Submitted
```

```
CGProMaxThreadCount 50
```

```
CGProLoopHeader X-Proceed_240578_by_spamtest
```

```
CGProAllTransports No
```

```
ClientFilteringSizeLimit 500
```

```
ClientDefaultDomain localhost
```

付録A.2.2で説明されているオプションに加えて、kas-cgproの設定用に以下のオプションを使用できます。

付録A.2.2で説明されているオプションに加えて、kas-cgproの設定用に以下のオプションを使用できます。

- **CGProMaxThreadCount** – 同時に処理されるメッセージの最大数。
- **CGProLoopHeader** – 処理済みメッセージに追加されるヘッダ。

- **CGProAllTransports** – さまざまなトランスポートを使用して受信したメールの処理を許可または禁止。以下の値を指定できます。**yes** – すべてのメールを処理します。**no** – SMTP メールトラフィックのみ処理します (デフォルト値)。



kas-cgpro モジュールと連動するよう *Communicate Pro* を設定するには、メールサーバの Web インタフェースを使用して、以下の手順を実行します。

1. **[Settings]**→**[General]**→**[Helpers]**メニューで、以下のパラメータを使用して新しい *content-filter* を追加します。

Use Filter: *kas-cgpro*

Log: Problems

Path: /usr/local/ap-mailfilter3/bin/*kas-cgpro*

Time-Out: 5 minutes

Auto-Restart: 15 seconds

2. **[Settings]**→**[Rules]**メニューで、新規ルールを作成します。このルールに従って、500KB 以下のすべてのメッセージが、スパムでないかどうかチェックされます。

Data: Message Size

Operation: less than

Parameter: 500000

Action: external filter

Parameters: *kas-cgpro*

Communicate Pro と共に *kas-cgpro* を使用する場合、以下のような特徴があります。

- SMTP セッション中に、*kas-cgpro* クライアントモジュールは、**reject this message** 動作が指定されている受信メッセージを拒否できません。代わりに、*Communicate Pro* が、メッセージを受信者に配信できなかったことを知らせる不達通知を送信者に送信します。
- 不達通知のテキストは、Management CenterのWebインタフェースで指定される**不達通知**パラメータの値ではなく、メールサーバによって定義されます(60ページのセクション4.5.4を参照)。
- フィルタリングサーバは、監視システムからのメッセージとエラーメッセージを、**mailflt3** ユーザアカウントを使用して送信します。デフォルトでは、*Communicate Pro* はシステムユーザのアカウントをデータベース

に追加しないため、**mailflt3** ユーザアカウントを Communicate Pro のユーザデータベースに手動で作成する必要があります。

- Communicate Pro で **Drop Root** オプションが使用される場合、メールサーバが **nobody** ユーザの権限を使用するよう切り替えられます。この切り替えにより、メールサーバとクライアントモジュール間の接続が切断されますが、kas-cgpro モジュールへの影響はありません。接続しなおすには、以下の手順を実行します。
 - Communicate Pro の **[Settings]** → **[General]** → **[Helpers]** メニューを選択し、**[Use Filter]** チェックボックスをオフにして、kas-cgpro フィルタの使用を無効にします。**[Update]** ボタンをクリックして設定を更新します。
 - kas-cgpro フィルタを再び追加します。フィルタのパラメータについては、前述の kas-cgpro クライアントモジュールと連動するよう Communicate Pro を設定する方法の説明を参照してください。

A.3. Kaspersky Anti-Spam 設定ファイル

このセクションでは、フィルタリングサーバの主要コンポーネントのパラメータが含まれている Kaspersky Anti-Spam 設定ファイルについて説明します。

A.3.1. メイン設定ファイル filter.conf

`/usr/local/ap-mailfilter3/etc/filter.conf` 設定ファイルには、すべての Kaspersky Anti-Spam コンポーネント(更新用モジュールを除く)の運用を調整するパラメータが含まれています。

全般的な設定 :

RootPath – Kaspersky Anti-Spam インストールディレクトリのパス。デフォルト値は、`/usr/local/ap-mailfilter3` です。

LogFacility=mail|user|local0|local1|local2|local3|local4|local5|local6|local7 – Syslog 機能でレコードが記録される際に従うカテゴリ。デフォルト値は **mail** です。

LogLevel=0|1|2|3|4|5 – Syslog 機能のレコードの詳細レベル。デフォルト値は **2** です。

User – このユーザの権限を使用して、フィルタリングサーバプロセスが開始されます。ユーザ名またはユーザの `uid` を指定できます。

Group – このグループの権限を使用して、フィルタリングサーバプロセスが

開始されます。グループ名または *gid* を指定できます。

フィルタリングサーバ設定

ServerListen – フィルタリングサーバとメールサーバに統合されているモジュールとのやり取りに使用されるソケット。この値は、「**tcp:<host>:<port>**」(<host>はメールサーバのIPアドレス(または名前)、<port>はネットワークソケットを指定するポート番号)または「**unix:<path_to_file>**」(<path_to_file>はソケットファイルのパス(ローカルソケットを指定する))の形式のレコードを使用して指定します。



互換性を持たせるために、メールサーバとフィルトレーションサーバ間のやり取り用に作成されたローカルソケットは、ログオンしているすべてのユーザによる書き込みを許可します。

FilterPath – *ap-mailfilter* フィルタリングプロセスの実行ファイルのパス

ServerStartFilters – フィルタリングモジュールの起動時に開始される *ap-mailfilter* フィルタリングプロセスの数。デフォルト値は **0** です。

ServerStartFilters の値は、**ServerMaxFilters** パラメータの値を超えてはいけません。

ServerMaxFilters=1...200 – 同時に実行できるフィルタリングプロセス *ap-mailfilter* の最大数。デフォルト値は **10** です。

ServerSpareFilters – アイドル状態(メッセージを処理していない状態)のフィルタリングプロセスの最小数。プロセス数が指定された制限値を超えた場合、アイドル状態のプロセスが強制的に終了されます。デフォルト値は **0** です。**ServerSpareFilters**の値は、**ServerMaxFilters**/パラメータの値を超えてはいけません。

フィルタリングプロセスの設定

FilterMaxMessages=10...1000 – 1つのフィルタリングプロセスで処理可能な最大メッセージ数。指定された数のメッセージの処理が完了すると、フィルタリングプロセスが終了します。デフォルト値は **300** です。



特定のフィルタリングプロセスで処理可能な最大メッセージ数は、アプリケーションが[FilterMaxMessages; FilterMaxMessages + (FilterRandMessages-1)]の範囲で選択するランダムな数になります。このオプションにより、サーバの負荷がピークに達しているときに、多数の新しいフィルタリングプロセスが同時に終了し、同時に開始されるのを防ぐことができます。

FilterRandMessages=0...50 – 特定のフィルタリングプロセスで処理可能な最大メッセージ数を定義するために使用される値

FilterMaxIdle=30...3600 – フィルタリングプロセスがアイドル状態でいられる最大時間(秒単位)。フィルタリングプロセスが、処理するメッセージを受け取らないまま指定された時間が経過すると、プロセスが終了されます。デフォルト値は **300** です。

FilterDelayedExit=0...30 – プロセスの停止コマンドを受け取ってからフィルタリングプロセスが停止するまでの最大時間(秒単位)。0以外の値を指定すると、信号の受信後、[0; (FilterDelayedExit-1)]の範囲からランダムに選択された秒数の間にフィルタリングプロセスが停止されます。デフォルト値は **0** です。

FilterDataTimeout=10...100 – フィルタリングプロセスがクライアントモジュールからのデータを待機するタイムアウト時間(秒単位)。フィルタリングプロセスが、データを受け取らないまま指定された時間が経過すると、メッセージのプロセスが停止されます。デフォルト値は **30** です。

FilterLicenseConnectTimeout=1..10 – プロセス要求がライセンス契約に準拠しているかどうかチェックするために、フィルタリングプロセスがライセンシングモジュール(*kas-license*)に接続する際のタイムアウト時間(秒単位)。デフォルト値は **2** です。

FilterLicenseDataTimeout=1..10 – フィルタリングプロセスとライセンシングモジュールが使用する適切なソケットの読み取り/書き込み操作のタイムアウト時間(秒単位)。デフォルト値は **1** です。

FilterSPFDataTimeout=1..10 – フィルタリングプロセスと SPF デーモンが使用する適切なソケットの読み取り/書き込み操作のタイムアウト時間

(秒単位)。デフォルト値は 1 です。

FilterDNSTimeout=1...60 – DNS を使用する実行可能なすべてのチェックを行う際のタイムアウト時間(秒単位)。デフォルト値は 10 です。

FilterLicenseConnectTo – ライセンシングモジュールへの接続に使用するソケットのファイルへのパス。デフォルト値は、**/usr/local/ap-mailfilter3/run/kas-license.socket** です。

FilterSPFConnectTo – SPF デーモンとのやり取りに使用するソケットファイルのパス。デフォルト値は、**/usr/local/ap-mailfilter3/run/ap-spf.socket** です。

FilterReceivedHeadersLimit=0...100 – DNSBL サービスの IP アドレスリストを使用して分析できる [Received] ヘッダの数。デフォルト値は 2 です。

FilterParseMSOffice=yes|no – Word ドキュメント(doc)および RTF 形式の添付ファイルのテキストを分析するかどうかを定義するパラメータ。デフォルト値は no です。

FilterStatLogFile – アプリケーションが処理メッセージに関する統計情報を保存するファイルのパス

FilterUserLogFile – 統計データを保存するためにユーザが定義するファイルのパス

FilterUDSCfgFile – UDS 設定が含まれているファイルのパス

FilterUDSEnabled=yes|no – UDS を使用するメールチェックを有効/無効にするパラメータ

FilterUDSTimeout=1...60 – フィルトレーションサーバと UDS サーバ間で確立される接続のタイムアウト時間。フィルトレーションサーバが UDS からの応答を受信しないまま指定された秒数が経過すると、フィルトレーションサーバは、カスペルスキーラプスの別の UDS サーバに接続します。

ライセンシングモジュールの設定

LicenseListen – ライセンシングモジュールがフィルタリングプロセスとのやり取りに使用するソケットファイルのパス。デフォルト値は、**/usr/local/ap-mailfilter3/run/kas-license.socket** です。

LicenseKeysPath – ライセンスキーが保存されるディレクトリのパス。デフォルト値は、**/usr/local/ap-mailfilter3/conf/lk-license/**です。

LicenseMaxConnections=10...300 – ライセンシングモジュールとの同時接続の最大数。デフォルト値は 200 です。

LicenseIdleTimeout=1...100 – ライセンシングモジュールが、データを送信していないアイドル状態のフィルタリングプロセスとの接続を維持できる最大時間(秒単位)。フィルタリングプロセスから要求が送信されてこないままこの秒数が経過すると、接続が切断されます。デフォルト値は **30** です。

LicenseDataTimeout=1...100 – フィルタリングプロセスとのやり取りに使用するソケットの読み取り/書き込み操作のタイムアウト時間(秒単位)。デフォルト値は **1** です。

SPF デーモンの設定

SPFDListen – SPF デーモンがフィルタリングプロセスとのやり取りに使用するソケットファイルのパス。デフォルト値は、**/usr/local/ap-mailfilter3/run/ ap-spf.socket** です。

SPFDPoolSize=1...50 – SPF デーモンが同時に実行できる子プロセスの数。デフォルト値は **5** です。

SPFDMaxRequestsPerChild=50...10000 – SPF デーモンの1つの子プロセスが処理できる要求の最大数。子プロセスが指定された数の要求を処理すると、プロセスが終了し、SPF デーモンによって新しいプロセスが開始されます。デフォルト値は **1000** です。

SPFDMaxQueueSize=10...1000 – プロセス用のキューに同時に配置できる要求の最大数。デフォルト値は **200** です。

SPFDCleanupInterval=30...3600 – SPF デーモンのキャッシュクリーンアップの間隔(秒単位)。デフォルト値は **600** です。

クライアントモジュールの全般的な設定

ClientConnectTo – クライアントモジュールがフィルタリングモジュールとやり取りする際に使用するソケットのアドレス。このアドレスの形式は、「**tcp:<host>:<port>**」(<host>はフィルタリングサーバのIPアドレス、<port>はネットワークソケットを指定する接続ポート)および「**unix:<path_to_file>**」(<path_to_file>はソケットファイルのパス(ローカルソケットを指定する))の形式のレコードを使用します。

ClientConnectTimeout=10...100 – クライアントモジュールとフィルタリングプロセス間で確立される接続のタイムアウト時間(秒単位)。デフォルト値は **40** です。

ClientDataTimeout=10...100 – クライアントモジュールとフィルタリングプロセス間で行われるデータ交換のタイムアウト時間(秒単位)

ClientOnError – エラー処理方法(フィルタリングモジュールに接続できな

い場合や、データ交換のタイムアウト時間を過ぎた場合など)。以下の値を指定できます。

- **reject** – メッセージを拒否し、SMTP セッション中に 5xx コードを返します。
- **tempfail** – 一時的にメッセージを拒否し、SMTP セッション中に 4xx コードを返します(デフォルト)。
- **accept** – メッセージを受け入れます。

ClientDefaultDomain – ドメインが指定されていないアドレスに代入するメールアドレスの名前。たとえば、デフォルトドメインが「mycompany.com」の場合、「someuser」というアドレスは、「someuser@mycompany.com」として解釈されます。この値が設定されていない場合、このようなアドレスへのドメイン名の代入が行われません。デフォルトでは、このオプションの値は設定されていません。

ClientFilteringSizeLimit=0...10000 – フィルタリングモジュールに渡すことが可能なメッセージの最大サイズ(キロバイト単位)。このサイズを超えるメッセージは、フィルタリングされずに通過します。デフォルト値は **500** です。

ClientMessageStoreMem – 一時データがディスクに保存される最小メッセージサイズ(キロバイト単位)。このモードを使用して、オペレーティングメモリの使用量を制御できます。**0** (デフォルト値)を設定すると、常にすべてのデータがオペレーティングメモリに保存されます。

ClientTempDir – 一時ファイル用のフォルダ

Control Center の設定

ControlCenterSendAlertsTo – 監視システムからのメッセージおよび cron サービスによって実行されたスクリプトのパフォーマンスに関するエラーメッセージを送信するアドレス

ControlCenterLang=en – Control Center インタフェースの言語

MonitoringHttpd=yes|no – kas-thttpd HTTP サーバのアクティビティを監視するかどうかを指定するパラメータ

MonitoringKasMilter=yes|no – Sendmail とのやり取りに使用する kas-milter クライアントモジュールのアクティビティを監視するかどうかを指定するパラメータ



各クライアントモジュールに固有のパラメータについては、83ページの付録A.2を参照してください。

A.3.2. kas-thttpd.conf 設定ファイル

`/usr/local/ap-mailfilter3/etc/1`に配置されている `kas-thttpd.conf` 設定ファイルには、Kaspersky Anti-Spam のメイン設定ツールである Management Center の Web インタフェースを提供する HTTP サーバの設定が含まれています。

このファイルには、以下のオプションが含まれています。

user – このユーザの権限を使用して、Management Center のスクリプトが実行されます。このオプションを変更するとシステムが正しく動作しなくなる可能性があるため、デフォルト値の `mailflt3` をそのまま使用することをお奨めします。

host – Web サーバが、Management Center インタフェースへの接続要求をリスンしながら待機するインタフェースの IP アドレス。「`0.0.0.0`」を指定すると、サーバがすべてのネットワークインタフェースをリスンします。

port – Management Center インタフェースへの接続に使用するポート

pidfile – HTTP サーバの pid ファイル名。デフォルト値は、`/usr/local/ap-mailfilter3/run/kas-thttpd.pid` です。

logfile – HTTP サーバのログファイル名。デフォルト値は、`/usr/local/ap-mailfilter3/log/kas-thttpd.log` です。

dir – Management Center の cgi スクリプトを保存するディレクトリのパス。デフォルト値は、`/usr/local/ap-mailfilter3/control/www` です。

cgipat – cgi スクリプト名のテンプレート。このオプションには、`/*.*.cgi` を設定します。

A.4. Kaspersky Anti-Spam のユーティリティ

このセクションでは、Kaspersky Anti-Spam の主なユーティリティについて、機能的特徴と各コンポーネントの設定に使用するコマンドラインオプションについて説明します。ユーティリティを起動するには、**root** ユーザ権限が必要です。

A.4.1. kas-htpasswd

`kas-thttpd` ユーティリティは、Management Center インタフェースへのアクセスに使用するパスワードが保存されているファイルの管理に使用します。

起動コマンド：

```
# /usr/local/ap-mailfilter3/bin/kas-htpasswd [-c] <password_file> <username> [-h]
```

コマンドラインオプション：

- **password_file** – アクセスパスワードが保存されているファイルのパス。デフォルトのファイルは *htpasswd* です。ユーティリティは、このパスワードを使用して、ファイルに新規ユーザを追加、または既存のユーザのパスワードを変更します。
- **username** – パスワードの所有者であるユーザの名前
- **-c** – パスワードを使用して、新規ファイルを作成する必要があるかどうかを指定するオプション。このオプションの値を設定しない場合は、**password_file** オプションに既存のファイルを設定する必要があります。
- **-h** – ユーティリティに関する情報をコンソールに出力します。

A.4.2. kas-show-license

コマンドラインから *kas-show-license* ユーティリティを起動すると、インストールされているライセンスキーファイルに関する情報が画面に表示されます。

起動コマンド：

```
# /usr/local/ap-mailfilter3/bin/kas-show-license  
[-k <key_file>] [-c <configuration_file>]
```

コマンドラインオプション：

- **-k <key-file>** – **key_file** ライセンスキーに関する情報が表示されます。
- **-c <configuration_file>** – *filter.conf* 設定ファイルのパスを再定義します。*filter.conf* がデフォルト以外のディレクトリに配置されている場合、**configuration_file** パラメータに *filter.conf* ファイルの完全パスを指定します。



コマンドラインオプションを使用せずにこのユーティリティを起動すると、インストールされているすべてのライセンスキーに関する情報がサーバコンソールに出力されます。

A.4.3. install-key

install-key ユーティリティは、Kaspersky Anti-Spam のライセンスキーをインストールする際に使用します。

起動コマンド：

```
# /usr/local/ap-mailfilter3/bin/install-key -i [-q] [-d]  
[-v] [-l] [-V <details_level>]  
[-L <details_level>] [-c <configuration_file>]  
[-k <kas-conf_script>] [-h]
```

コマンドラインオプション：

- **-i** – キーのインストール後にライセンス情報をコンソールに出力する処理を省略します。

- q – エラーメッセージのみ表示します。
- d – ライセンスキーのインストール処理に関する詳細なレポートを表示します。
- v – デフォルトの詳細レベルよりもさらに詳細な情報をコンソールに出力します。
- V <details_level> – 指定された詳細レベルでコンソールにメッセージを出力します。1...10 の値を指定できます。
- l – デフォルトのレベルよりも高い詳細レベルで、メッセージをシステムログに追加します。
- L <details_level> – 指定された詳細レベルでシステムログにメッセージを追加します。1...10 の値を指定できます。
- c <configuration_file> – *filter.conf* 設定ファイルのパスを再定義します。*filter.conf* がデフォルト以外のディレクトリに配置されている場合、**configuration_file** パラメータに *filter.conf* ファイルの完全パスを指定します。
- k <kas-conf_script> – Kaspersky Anti-Spam の設定を読み込む *kas-conf* スクリプトのパスを再定義します。*kas-conf* がデフォルト以外のディレクトリに配置されている場合、**kas-conf_script** パラメータに *kas-conf* ファイルの完全パスを指定します。
- h – ユーティリティに関する情報をコンソールに出力します。

A.4.4. remove-key

remove-key ユーティリティは、Kaspersky Anti-Spam のライセンスキーを削除する際に使用します。

起動コマンド：

```
# /usr/local/ap-mailfilter3/bin/remove-key [-a|-r] [-q]
[-d] [-v] [-l] [-V <details_level>]
[-L <details_level>] [-c <configuration_file>]
[-k <kas-conf_script>] [-h]
```

コマンドラインオプション：

- a – インストールされているすべてのライセンスキーを削除します。
- r – 予備のライセンスキーを削除します。
- q – エラーメッセージのみ表示します。
- d – ライセンスキーの削除処理に関する詳細なレポートを表示します。

- v – デフォルトの詳細レベルよりもさらに詳細な情報をコンソールに出力します。
- V <details_level> – 指定された詳細レベルでコンソールにメッセージを出力します。1...10の値を指定できます。
- l – デフォルトの詳細レベルよりも高い詳細レベルで、メッセージをシステムログに追加します。
- L <details_level> – 指定された詳細レベルでシステムログにメッセージを追加します。1...10の値を指定できます。
- c <configuration_file> – *filter.conf* 設定ファイルのパスを再定義します。*filter.conf* がデフォルト以外のディレクトリに配置されている場合、**configuration_file** パラメータに *filter.conf* ファイルの完全パスを指定します。
- k <kas-conf_script> – Kaspersky Anti-Spam の設定を読み込む *kas-conf* スクリプトのパスを再定義します。*kas-conf* がデフォルト以外のディレクトリに配置されている場合、**kas-conf_script** パラメータに *kas-conf* ファイルの完全パスを指定します。
- h – ユーティリティに関する情報をコンソールに出力します。

A.4.5. kas-restart

kas-restart ユーティリティは、Kaspersky Anti-Spam および各コンポーネントを再起動する際に使用します。

起動コマンド：

```
# /usr/local/ap-mailfilter3/bin/kas-restart [-f] [-p] [-s] [-m] [-w] [-W] [-q] [-d] [-v] [-l]
[-V <details_level>] [-L <details_level>]
[-c <configuration_file>] [-k <kas-conf_script>] [-h]
```

コマンドラインオプション：

- -f – フィルタリングプロセス *ap-mailfilter* を再起動します。このプロセスは、指定されているプロセス終了遅延時間およびメッセージ数に従って、メッセージを処理してから作業を終了します(詳細については、59ページのセクション4.5.3を参照)。
- -p – マスタフィルタリングプロセス *ap-process-server* を再起動します。このオプションは、フィルタリングプロセス *ap-mailfilter* も再起動します。このオプションを使用すると、フィルタリングプロセスは現在のメッセージのチェックを停止して、その直後に再起動されます。このオプションは、フィルタリングプロセスの起動に関する設定を変更する際にも使用されます。

- **-s** – ライセンシングモジュール *kas-license* を再起動します。
- **-m** – *kas-milter* モジュールを再起動します。
- **-w** – Web サーバ *kas-thttpd* を再起動します。
- **-W** – Web サーバ *kas-thttpd* のログファイルを交換します(新しいログファイルを作成)。
- **-q** – 「サイレント」モードを有効にします。エラーメッセージおよび警告のみ表示されます。
- d** – ユーティリティの処理に関する詳細なレポートを表示します。
- v** – デフォルトの詳細レベルよりもさらに詳細な情報をコンソールに出力します。
- V** **<details_level>** – 指定された詳細レベルでコンソールにメッセージを出力します。1...10 の値を指定できます。
- I** – デフォルトの詳細レベルよりも高い詳細レベルで、メッセージをシステムログに追加します。
- L** **<details_level>** – 指定された詳細レベルでシステムログにメッセージを追加します。1...10 の値を指定できます。
- c** **<configuration_file>** – *filter.conf* 設定ファイルのパスを再定義します。*filter.conf* がデフォルト以外のディレクトリに配置されている場合、**configuration_file** パラメータに *filter.conf* ファイルの完全パスを指定します。
- k** **<kas-conf_script>** – Kaspersky Anti-Spam の設定を読み込む *kas-conf* スクリプトのパスを再定義します。*kas-conf* がデフォルト以外のディレクトリに配置されている場合、**kas-conf_script** パラメータに *kas-conf* ファイルの完全パスを指定します。
- h** – ユーティリティに関する情報をコンソールに出力します。



コマンドラインオプションを使用せずにこのユーティリティを起動すると、**-f** オプションを使用してユーティリティを起動した場合と同じ処理が行われます。

A.4.6. *mkprofiles*

mkprofiles ユーティリティは、Kaspersky Anti-Spam のフィルタリングポリシーの構築およびコンパイルに使用します。

起動コマンド：

```
# /usr/local/ap-mailfilter3/bin/mkprofiles  
[-c <configuration_file>] [-l <log_file>] [-q] [-v] [-h]
```

各コマンドおよびパラメータの意味は以下の通りです。

- **-c <configuration_file>** - *filter.conf* 設定ファイルのパスを再定義します。*filter.conf* がデフォルト以外のディレクトリに配置されている場合、**configuration_file** パラメータに *filter.conf* ファイルの完全パスを指定します。
- **-l <log_file>** - ユーティリティによって実行された動作に関するレポートを、**log_file** パラメータで指定されているファイルに保存します。
- **-q** - 「サイレント」モードを有効にします。エラーメッセージおよび警告のみ表示されます。
- **-v** - コンパイルに関するすべてのメッセージをコンソールに出力します。
- **-h** - ユーティリティに関する情報をコンソールに出力します。

コマンドラインオプションを使用せずにこのユーティリティを起動すると、エラーメッセージ、警告、および正常に完了した処理に関するメッセージが表示されます。

A.4.7. *sfmonitoring*

sfmonitoring ユーティリティは、Kaspersky Anti-Spam のコンポーネントのステータスを監視します。エラーを検出すると、コンソールに情報を出力します。

起動コマンド：

```
su -m mailft3 -c '/usr/local/ap-mailfilter3/control/bin/  
sfmonitoring [-p] [-m] [-q] [-h]'
```

RedHat が稼働しているサーバに Kaspersky Anti-Spam がインストールされている場合は、以下のコマンドをコマンドラインに入力して *sfmonitoring* ユーティリティを起動します。

```
su --m mailft3 -c '/usr/local/ap-mailfilter3/control/bin/  
sfmonitoring [-p] [-m] [-q] [-h]'
```

コマンドラインオプション：

- **-p** - システムのステータスをチェックし、Kaspersky Anti-Spam のエラーに関するメッセージをコンソールに出力します。
- **-m** - システムのステータスをチェックし、Kaspersky Anti-Spam のエラーに関する日次レポートを電子メールで送信します。
- **-q** - 「サイレント」モードを有効にします。エラーメッセージおよび警告のみ表示されます。

- **-h** – ユーティリティに関する情報をコンソールに出力します。

上記のオプションを使用せずにこのユーティリティを起動すると、ユーティリティは、システムの現在のステータスをチェックし、新たなエラーを検出した場合は、そのエラーに関する警告を電子メールで送信します。

A.4.8. *sfupdates*

sfupdates ユーティリティは、コンテンツフィルタリングデータベースの更新をダウンロードし、フィルタリングサーバで使用できるようにその更新をインストールします。

起動コマンド：

```
# /usr/local/ap-mailfilter3/bin/sfupdates  
[-c <configuration_file>] [-f] [-k <kas-conf_script>] [-s] [-q] [-v] [-d] [-V  
<details_level>] [-l]  
[-L <details_level >] [-h]
```

コマンドラインオプション：

- **-c <configuration_file>** – *filter.conf* 設定ファイルのパスを再定義します。*filter.conf* がデフォルト以外のディレクトリに配置されている場合、**configuration_file** パラメータに *filter.conf* ファイルの完全パスを指定します。
- **-f** – 設定を強制的にコンパイルします。このオプションを指定しなかった場合、コンテンツフィルタリングデータベースの更新がダウンロードされた場合のみ、設定がコンパイルされます。
- **-k <kas-conf_script>** – Kaspersky Anti-Spam の設定を読み込む *kas-conf* スクリプトのパスを再定義します。*kas-conf* がデフォルト以外のディレクトリに配置されている場合、**kas-conf_script** パラメータに *kas-conf* ファイルの完全パスを指定します。
- **-s** – 更新のダウンロードを省略します。
- **-q** – エラーメッセージのみコンソールに出力するモードを有効にします。*cron* サービスを使用する場合は、このモードを開始することをお奨めします。
- **-v** – デフォルトよりも高い詳細レベルで、コンソールにメッセージを出力します。
- **-d** – 最も高い詳細レベルで、コンソールにメッセージを出力します。
- **-V <details_level>** – 指定された詳細レベルでコンソールにメッセージを出力します。1..10 の値を指定できます。

- `-l` – デフォルトよりも高い詳細レベルで、Syslog にデータを記録します。
- `-L <details_level>` – 指定された詳細レベルでシステムログにメッセージを追加します。1...10 の値を指定できます。

上記のいずれのオプションも指定しなかった場合、エラーメッセージ、警告、および正常に完了した処理に関するメッセージがコンソールに表示されます。

A.5. フィルタリングモジュール用の特別なヘッダ

メールメッセージの処理中に、Kaspersky Anti-Spam により、処理済みのメッセージに以下のヘッダが追加されます。

- **X-Spamtest-Version** – Kaspersky Anti-Spam 配布パッケージのバージョンに関する情報が含まれているヘッダ
- **X-Spamtest-Status** および **X-Spamtest-Status-Extended** – フィルタリング後に割り当てられたメッセージのステータスが含まれているヘッダ。**X-Spamtest-Status** ヘッダは、旧バージョンの製品で使用されていたヘッダです。このヘッダには、Kaspersky Anti-Spam 2.0 に対応するステータスセットが含まれています。今回のバージョンにおいては、このヘッダは、互換性を維持する目的で使用されます。このヘッダの値を以下の表に示します。

ヘッダ	値	説明
X-Spamtest-Status	Trusted	このメッセージの送信者が送信者のホワイトリストに含まれているか、グループポリシーにおいてこの受信者宛てのメールのスパムスキャンが無効になっています。
	SPAM	このメッセージは、スパムとして分類されています。
	Probable Spam	このメッセージは、スパムの可能性があるメッセージとして分類されています。
	Not detected	このメッセージは、スパムおよびスパムの可能性があるメッセージとして分類されません。

ヘッダ	値	説明
X-Spamtest-Status-Extended	trusted	このメッセージの送信者が送信者のホワイトリストに含まれているか、グループポリシーにおいてこの受信者宛てのメールのスパムスキャンが無効になっています。
	blacklisted	このメッセージの送信者は、送信者のブラックリストに含まれています。
	spam	このメッセージは、スパムとして分類されています。
	probable_spam	このメッセージは、スパムの可能性があるメッセージとして分類されています。
	formal	このメッセージは、メールサーバからの公式の応答として分類されています。
	not_detected	このメッセージは、スパムおよびスパムの可能性があるメッセージとして分類されていません。

- **X-Spamtest-Header** – 管理者がManagement Centerを使用して指定したテキストが含まれているヘッダ(48ページのセクション4.3.7を参照)
- **X-Spamtest-Obscene** – わいせつな語句が含まれているメッセージに追加されるヘッダ
- **X-SpamTest-Formal** – **Formal** として分類されたメッセージに追加されるヘッダ
- **X-Spamtest-Rate** – 処理中にメッセージに対して割り当てられた評価が含まれているヘッダ。Kaspersky Anti-Spam は、この値を使用して、このメールメッセージにステータスを割り当てます。
- **X-Spamtest-Group-ID** – このメッセージの処理に使用されたルールが定義されているグループの ID が含まれているヘッダ
- **X-SpamTest-Categories** – フィルタリング結果に基づいてメッセージに割り当てられたカテゴリの名前が含まれているヘッダ
- **X-SpamTest-Info** – 情報的なデータが含まれているヘッダ

- **X-SpamTest-Method** – メッセージのステータスの割り当てに使用されたフィルタリング方法の名前が含まれているヘッダ。このヘッダの値を以下の表に示します。

値	方法
white ip list	IP アドレスのホワイトリストに基づくフィルタリング
white email list	電子メールアドレスのホワイトリストに基づくフィルタリング
black ip list	IP アドレスのブラックリストに基づくフィルタリング
black email list	電子メールアドレスのブラックリストに基づくフィルタリング
GSG	画像の分析
headers および headers plus	ヘッダの分析
DNSBL	DNSBL サービスを使用するフィルタリング
UDS	UDS を使用するフィルタリング
SURBL	SURBL サービスを使用するフィルタリング
Content	メッセージコンテンツのフィルタリング
probable	「Probable spam」メソッド
detection disabled	グループポリシーにおいてこの受信者宛てのメールのスパムスキャンが無効になっています。
multiple	ステータスの割り当てに複数の方法が使用されました。
None	いずれの方法でもメッセージを分類できません。このようなメッセージには、 [Not detected] ステータスが割り当てられます。

A.6. cron サービスを使用した設定

Kaspersky Anti-Spam を正しく運用するには、**mailflt3** ユーザの場合、*cron* サー

ビスを使用して一連のスクリプトを実行する必要があります。
スクリプトのパラメータを編集するには、以下のコマンドを使用します。

```
# crontab -u mailflt3 -e
```

以下のスクリプトをタスクリストに追加します。

- **コンテンツフィルタリングデータベースの更新用スクリプト**

起動コマンド : /usr/local/ap-mailfilter3/bin/sfupdates -q

推奨起動間隔 : 20 分おき



更新するサーバに負荷がかかり過ぎないようにするために、
予定しているスクリプト実行開始時間から何分か過ぎた時刻
を指定してください。たとえば、以下のように指定します。

```
7,27,47 * * * * /usr/local/ap-mailfilter3/bin/sfupdates -q
```

- **監視スクリプト**

起動コマンド :

```
/usr/local/ap-mailfilter3/control/bin/sfmonitoring -q
```

推奨起動間隔 : 5 分おき

- **フィルタリングのログの処理および統計情報の更新を行うスクリプト**

このスクリプトは、処理メッセージ数に関する統計データを Kaspersky Anti-Spam のログから収集したり、Control Center のインタフェースにメッセージを表示するためにフィルタリングサーバのログを処理したりします。

起動コマンド :

```
/usr/local/ap-mailfilter3/control/bin/dologs.sh -q
```

推奨起動間隔 : 1 分おき

- **統計グラフの更新用スクリプト**

このスクリプトは、処理メッセージに関する統計グラフを作成します。作成されたグラフは、Management Center の[**Statistics**]セクションに表示されます。

起動コマンド :

```
/usr/local/ap-mailfilter3/control/bin/dograph.sh -q
```

推奨起動間隔 : 5 分おき

- **フィルタリングサーバのログファイルの交換用スクリプト**

ディスクスペースを十分に確保し、全体的なパフォーマンスを向上させるために、フィルタリングサーバのログファイルを定期的に変換することをお奨めします。このスクリプトは、Management Center および統計システムが使用する内部ログファイルを交換します。

起動コマンド：

```
/usr/local/ap-mailfilter3/control/bin/logrotate.sh -q
```

推奨起動間隔：1日2回。システムの負荷が高くなる場合は、もっと頻繁にログファイルを交換するよう設定してください。

- **UDS サーバへのアクセスの所要時間を計算するスクリプト**

アプリケーションは、`uds-rtts.sh` スクリプトを使用して、カスペルスキーラブスの各 UDS サーバへのアクセスの所要時間を判断します。受け取ったデータから、UDS 要求を送信する最適なサーバを特定します。

起動コマンド：

```
/usr/local/ap-mailfilter3/bin/uds-rtts.sh -q
```

推奨起動間隔：10～15分おき

上記のスクリプトを設定する他に、以下の作業を行うことを強くお奨めします。

- 上記のスクリプトが実行されるディレクトリのパスを、`HOME` 変数の値として指定します。推奨されるパスは、`/usr/local/ap-mailfilter3/run` です。
- `sendmail`¹ ユーティリティを含むシステムの主なユーティリティのパスのリストを、`PATH` 変数の値として追加します。デフォルト値は、`/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin` です。
- スクリプトの実行に関するメッセージの送信先アドレスを指定します。このアドレスは、`MAILTO` 変数を使用して指定します。デフォルト値は `postmaster` です。

以下の例は、`crontab` ファイル内で、上記の設定が指定されている部分です。

```
MAILTO=admin@mycompany.com
```

```
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin
```

```
HOME=/usr/local/ap-mailfilter3/run
```

```
7,27,47 * * * * /usr/local/ap-mailfilter3/bin/sfupdates -q
```

```
* /5 * * * * /usr/local/ap-mailfilter3/control/bin/sfmonitoring -q
```

```
* * * * * /usr/local/ap-mailfilter3/control/bin/dologs.sh -q
```

```
* /5 * * * * /usr/local/ap-mailfilter3/control/bin/dograph.sh -q
```

```
0 * /12 * * * * /usr/local/ap-mailfilter3/control/bin/logrotate.sh -q
```

```
4-59/11 * * * * /usr/local/ap-mailfilter3/bin/uds-rtts.sh -
```

¹ 監視スクリプトによって使用されます。

付録B. スпамメールの報告方法

カスペルスキーラボスは新しいスパムメールもしくは誤ってスパムと判定されたという報告をお待ちしています。報告に対しては専門家が徹底的な分析を行います。従って、こういった報告は、スパム検知率の上昇・誤検知率の低減にとっても有益なのです。

連絡先は以下です。

スパムメールの申告：spam@kaspersky.com

誤検知の申告：notspam@kaspersky.com



サンプルは添付ファイルで送信してください。

メールソフトによっては、自動的にヘッダを削除することがあります。以下に、主なメールソフトの動作を示します：

1. Microsoft Office Outlook の場合：
 - 「新規作成」ボタンもしくは「**New Mail Message**」コマンドで作成したメールに、報告したいスパムメールをドラッグ&ドロップします。
 - 複数のスパムメールを報告する場合は、それらのメールを選択し、「**転送**」をクリックします。
2. Bat!の場合：
 - 報告したいスパムメールを選択し、「**Alternative Forward**」をクリックします。この機能はツールバーの「**Specials**」にあります。
 - 自動的にスパムメールを報告するには、以下のようにソートルールを設定します：
 - 「添付ファイルを送信しない」チェックボックスを外す。
 - 「標準で **MIME** を使用する」チェックボックスにチェックを入れる。
3. Microsoft Outlook Express を使用する場合は、報告するメールを選択し、「メッセージ」→「添付ファイルとして転送」を実行します。

付録C. KASPERSKY LAB

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

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

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

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

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

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

C.1. カスペルスキーラボのその他の主な製品

Kaspersky® OnLine Scanner

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

○ スキャン領域の選択

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

- マイコンピュータ - すべてのローカルハードディスクとマッピングされたディスクのスキャン
- メールファイル - *.PST, *.MSG, *.OST, *.MDB, *.DBX, *.EML, *.MBS 形式のメールデータベースのスキャン
- フォルダ - 任意のフォルダのスキャン
- ファイル - 任意のファイルのスキャン

○ スキャン設定オプション

- 圧縮ファイルおよび E メールデータベースをスキャン対象から除外または含める
- スキャンの定義データベースを「標準」/「拡張」から選択
- スキャン結果のレポートを.txt または.html 形式で保存

Kaspersky® Anti-Virus 7.0

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

このプログラムは、以下の複合的なウイルススキャン機能を備えています：

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

プロアクティブディフェンスには、次のような特徴があります：

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

Kaspersky® Internet Security 7.0

Kaspersky® Internet Security 7.0 はKaspersky® Anti-Virus 7.0 のアンチウイルスモジュールに、IPSとIDSに対応するパーソナルファイアウォールと迷惑メール対策を統合した総合セキュリティ製品です。ウイルスやスパイウェアを含むマルウェア、不正侵入、情報流出、迷惑メールなどのネットワーク上の脅威から、コンピュータに保存されたデータを保護します。包括的インターフェイスで、プログラムのすべてのコンポーネントを設定・管理することができます。

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

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

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

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

Kaspersky® Anti-Virus Mobile

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

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

Kaspersky Anti-Virus for File Servers

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

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

Kaspersky® Open Space Security

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

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

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

※ Windows プラットフォームのみ

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

Kaspersky Mail & Gateway Security

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

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

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

Kaspersky® Anti-Spam

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

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

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

Kaspersky® Second Opinion Solution (SOS)

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

Kaspersky® Anti-Virus for Windows Server Enterprise Edition

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

このプログラムには、以下の特徴があります：

高性能を誇るパフォーマンス

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

柔軟な管理ツール

- **一元管理ツール** - Kaspersky Administration Kit からプログラムのインストール、設定の変更やアプリケーションの管理などの操作を複数台のサーバに対して一度に行うことができます
- **柔軟な管理オプション** - リモート管理を含む Microsoft 管理コンソール、Kaspersky Administration Kit、またはコマンドラインからの管理が可能です。

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

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

* その他、記載されている会社名、製品名は、各社の登録商標または商標です。

C.2. お問い合わせ先

ご意見・ご質問等はカスペルスキーラボ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D.

THIRD PARTY SOFTWARE

カスペルスキーアンチスパム 3.0 では、次のサードパーティ製ソフトウェアを使用しています：

Berkeley DB 1.85 library can be used on the following terms and conditions:
Copyright (c) 1990, 1993, 1994 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Margo Seltzer. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- 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.
- All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
- 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.

THIS SOFTWARE IS PROVIDED BY THE REGENTS 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 REGENTS 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.

libjpeg 6b library can be used on the following terms and conditions:

LEGAL ISSUES

=====

In plain English:

1. We don't promise that this software works. (But if you find any bugs, please let us know!)
2. You can use this software for whatever you want. You don't have to pay us.
3. You may not pretend that you wrote this software. If you use it in a program, you must acknowledge somewhere in your documentation that you've used the IJG code.

In legalese:

The authors make NO WARRANTY or representation, either express or implied, with respect to this software, its quality, accuracy, merchantability, or fitness for a particular purpose. This software is provided "AS IS", and you, its user, assume the entire risk as to its quality and accuracy.

This software is copyright (C) 1991-1998, Thomas G. Lane.

All Rights Reserved except as specified below.

Permission is hereby granted to use, copy, modify, and distribute this software (or portions thereof) for any purpose, without fee, subject to these conditions:

(1) If any part of the source code for this software is distributed, then this README file must be included, with this copyright and no-warranty notice unaltered; and any additions, deletions, or changes to the original files must be clearly indicated in accompanying documentation.

(2) If only executable code is distributed, then the accompanying documentation must state that "this software is based in part on the work of the Independent JPEG Group".

(3) Permission for use of this software is granted only if the user accepts full responsibility for any undesirable consequences; the authors accept NO LIABILITY for damages of any kind.

These conditions apply to any software derived from or based on the IJG code, not just to the unmodified library. If you use our work, you ought to acknowledge us.

Permission is NOT granted for the use of any IJG author's name or company name in advertising or publicity relating to this software or products derived from it. This software may be referred to only as "the Independent JPEG Group's software".

We specifically permit and encourage the use of this software as the basis of commercial products, provided that all warranty or liability claims are assumed by the product vendor.

ansi2knr.c is included in this distribution by permission of L. Peter Deutsch, sole proprietor of its copyright holder, Aladdin Enterprises of Menlo Park, CA. ansi2knr.c is NOT covered by the above copyright and conditions, but instead by the usual distribution terms of the Free Software Foundation; principally, that you must include source code if you redistribute it. (See the file ansi2knr.c for full details.) However, since ansi2knr.c is not needed as part of any program generated from the IJG code, this does not limit you more than the foregoing paragraphs do.

The Unix configuration script "configure" was produced with GNU Autoconf. It is copyright by the Free Software Foundation but is freely distributable. The same holds for its supporting scripts (config.guess, config.sub, ltconfig, ltmain.sh). Another support script, install-sh, is copyright by M.I.T. but is also freely distributable.

It appears that the arithmetic coding option of the JPEG spec is covered by patents owned by IBM, AT&T, and Mitsubishi. Hence arithmetic coding cannot legally be used without obtaining one or more licenses. For this reason, support for arithmetic coding has been removed from the free JPEG software.

(Since arithmetic coding provides only a marginal gain over the unpatented Huffman mode, it is unlikely that very many implementations will support it.) So far as we are aware, there are no patent restrictions on the remaining code.

The IJG distribution formerly included code to read and write GIF files. To avoid entanglement with the Unisys LZW patent, GIF reading support has been removed altogether, and the GIF writer has been simplified to produce "uncompressed GIFs". This technique does not use the LZW algorithm; the resulting GIF files are larger than usual, but are readable by all standard GIF decoders.

We are required to state that

"The Graphics Interchange Format(c) is the Copyright property of CompuServe Incorporated. GIF(sm) is a Service Mark property of CompuServe Incorporated."

libungif library can be used on the following terms and conditions:

The GIFLIB distribution is Copyright (c) 1997 Eric S. Raymond

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.

libevent library can be used on the following terms and conditions:

Copyright (c) 2000-2004 Niels Provos <provos@citi.umich.edu>

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. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "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 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.

thttpd web-server can be used on the following terms and conditions:

Copyright 1995,1998,1999,2000,2001 by Jef Poskanzer <jef@acme.com>.

All rights reserved.

1. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
2. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
3. 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.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR 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 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.

libspf2 library can be used on the following terms and conditions:

The code in the libspf-alt distribution is Copyright 2004 by Wayne Schlitt, all rights reserved. Copyright retained for the purpose of protecting free software redistribution.

This program is free software; you can redistribute it and/or modify it under the terms of either:

- a) the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1, or (at your option) any later version,
OR
- b) The two-clause BSD license.

Some code in the 'replace' subdirectory was obtained from other sources and have different, but compatible, licenses. These routines are used only when the native libraries for the OS do not contain these functions. You should review the licenses and copyright statements in these functions if you are using an OS that needs these functions.

The two-clause BSD license:

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.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "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 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.

libpatricia library can be used on the following terms and conditions:

Copyright (c) 1997, 1998, 1999

The Regents of the University of Michigan ("The Regents") and Merit Network, Inc. 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. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of Michigan, Merit Network, Inc., and their contributors.

4. Neither the name of the University, Merit Network, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS 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 REGENTS 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.

pcre library can be used on the following terms and conditions:

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.

xdr library can be used on the following terms and conditions:

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

Sun Microsystems, Inc.

2550 Garcia Avenue
Mountain View, California 94043

zlib library can be used on the following terms and conditions:

zlib.h -- interface of the 'zlib' general purpose compression library version 1.1.3,
July 9th, 1998

Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly

Mark Adler

jloup@gzip.org

madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files <ftp://ds.internic.net/rfc/rfc1950.txt> (zlib format), [rfc1951.txt](ftp://ds.internic.net/rfc/rfc1951.txt) (deflate format) and [rfc1952.txt](ftp://ds.internic.net/rfc/rfc1952.txt) (gzip format).

expat library can be used on the following terms and conditions:

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.

STLport library can be used on the following terms and conditions:

Copyright (c) 1994

Hewlett-Packard Company

Copyright (c) 1996-1999

Silicon Graphics Computer Systems, Inc.

Copyright (c) 1997

Moscow Center for SPARC Technology

Copyright (c) 1999, 2000, 2001, 2002

Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

libmilter library can be used on the following terms and conditions:

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.

OpenSSL library can be used on the following terms and conditions:

LICENSE ISSUES

=====

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

=====

Copyright (c) 1998-2004 The OpenSSL Project. 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. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND

ANY EXPRESSED 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 OpenSSL PROJECT OR ITS 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.

=====

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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 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. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "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.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

FreeBSD libc library can be used on the following terms and conditions:

Copyright (C) 1992-2005 The FreeBSD Project. 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.

THIS SOFTWARE IS PROVIDED BY AUTHOR 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 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.

mcpp front-end program can be used on the following terms and conditions:

Copyright (c) 1998, 2002-2004 Kiyoshi Matsui <kmatsui@t3.rim.or.jp>

All rights reserved.

Some parts of this code are derived from the public domain software DECUS cpp (1984,1985) written by Martin Minow.

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.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "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 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

付録E. 使用許諾契約書

ソフトウェア使用許諾契約書

「本製品」をご使用になる前に、「本製品」使用許諾契約書（以下、「本契約」という）の内容をご確認ください。

この度は、弊社製品をご利用いただき、まことにありがとうございます。弊社では製品につきまして、下記のソフトウェア使用許諾契約書を設けさせていただいており、お客様が下記契約書にご同意いただいた場合のみ製品をご使用いただいております。

第1条（定義）

1-1 「本製品」とは、本契約に基づき提供される Kaspersky(R) Anti-Virus/ Anti-Spam/ Security 及び関連資料を指します。

1-2 「クライアント機器」とは「本製品」をインストールするコンピュータあるいはワークステーション、個人デジタル機器およびその他電子機器を指します。

第2条（許諾事項）

2-1 「本製品」にはライセンスキー(識別キーファイル)またはライセンス適用向け識別コード(アクティベーションコード)が付属しています。本契約の条項に同意されたお客様に対し、カスペルスキーラプスは、本契約の有効期間中、「本製品」の非独占的かつ譲渡不可の使用権を許諾します。お客様は1ライセンスあたり、1台の「クライアント機器」にのみ製品をインストールすることができます。ファイルサーバ向け製品に関しては、物理サーバあるいは同時稼働 OS 毎にライセンスの購入が必要となります。トラフィックライセンスは一日あたりの流量 (Megabyte per day) 分のライセンスが必要となります。

2-2 「本製品」は、単独のソフトウェア・プログラムとしてライセンスされ、同時に2台以上の「クライアント機器」や2人以上のユーザーが利用することは出来ません。

2-3 「本製品」は、「クライアント機器」またはサーバのメインメモリにロードする、もしくはストレージ(ハードディスク、CD-ROM、その他の記憶装置)にインストールした場合、その「クライアント機器」上で「使用中」と

なります。

2-4 お客様はバックアップの目的で「本製品」のコピーを一部のみ制作することが出来ますが、当該コピーについては、不法コピーや不正利用防止のために適切な措置を講ずるものとします。

2-5 お客様が、「本製品」のインストールされた「クライアント機器」あるいはサーバを売却あるいは処分される場合は、「本製品」があらかじめ削除されていることを確認してください。

第3条（禁止事項）

3-1 「本製品」の全部または一部を複製、改変、リバースエンジニアリング、翻案、再配布、譲渡、貸与、再使用許諾、中古取引、レンタル、リースすることはできません。

3-2 お客様は「本製品」の逆コンパイル、リバースエンジニアリング、逆アSEMBル、その他の方法で「本製品」の全部または一部を可読可能な形式に変換したり、第三者にそれらの行為を許可したりする事は出来ません。

3-3 「本製品」に付されている Kaspersky(R)の商標、ロゴおよび画面イメージをカスペルスキーラボスの事前の書面による許諾なく使用し「本製品」の一部または全部を配布することはできません。

3-4 お客様は、製品の貸与およびリース、またライセンス権利の譲渡、サブライセンスの発行を行うことはできません。

3-5 お客様は、この製品をウイルスコード、ウイルス検知ルーチン、悪意のあるコードやデータ検知のための他のデータやコードの生成を意図した自動、半自動、手動ツールとして、使用できません。

第4条（ライセンス）

4-1 本契約は以下の条件によって契約が終了する場合を除き、1年間が有効期間となります。ここに記載された条件、制限、要件に反する行為がお客様により行われた場合、契約は自動的に解除されます。本契約の解除および有効期間切れの場合、お客様が保有している「本製品」及びそのコンポーネントを全て破棄してください。お客様が、製品および資料のコピーを破棄した時点で、本契約は終了します。

製品が、製品購入契約書やパッケージにおいて使用可能な製品が指定され、ライセンスボリューム条項が適用されている場合、お客様はボリュームライセンスで指定された数の「クライアント機器」およびサーバに、

コピーやインストール、利用が行えます。

4-2 お客様は、ライセンス数以上の製品が「クライアント機器」あるいはサーバにインストールされないことを保証するための、適切な予防措置を講じるものとします。また、資料に関しては、合法利用の範囲内で、著作権情報を含むことを条件に、ライセンス数内でダウンロード及びコピーが許諾されます。

第5条（サポート）

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

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

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

5-4 サポートサービスとは

5-4-1 定義データベースの更新

5-4-2 バージョンアップを含む、ライセンス有効期間内の無料製品更新

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

第6条（著作権）

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

製物に、「本製品」に表示されるものと同じ財産権が表示されることに同意します。

第7条（機密保持）

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

第8条（限定保証）

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

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

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

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

8-5 お客様の唯一の救済および（8-4）の保証の違反に対するカスペルスキーラプスおよび代理店の全責任は、代理店が決定し、お客様が

保障期間にカスペルスキーラプスあるいは正規販売代理店に報告された場合、代理店の判断により、「本製品」の修理あるいは交換あるいは返金が行なわれます。

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

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

8-6-2 想定外の方法あるいは目的で「本製品」を使用した場合。

8-6-3 本契約書で許可された範囲を超えて使用した場合、

8-7 本契約書にて述べられた保証および条件は、(8-5)で定義する条件を前提として、「本製品」および付属書類の供給、供給内容、供給の不備、供給の遅れに関し、同様に適用されるものとします。但し、本契約書が「本製品」及び資料を取得する国の法律及び慣習と異なる場合は別途協議するものとする（この保証は、契約者が満足するまでの間無制限に行うものではなく、契約者が「本製品」を使用するにあたって一般的に必要と考えられる知識、及び技術を持ち合わせていることが前提であり、また一般常識内で保証するものとする）。

第9条（免責事項）

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

9-1-1 虚偽の不法行為

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

9-1-3 法による除外が不可能な義務

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

9-2-1 収入の損失

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

9-2-3 将来見込まれる貯蓄の損失

- 9-2-4 取引上の損失
 - 9-2-5 機会損失
 - 9-2-6 信用上の損失
 - 9-2-7 信用毀損
 - 9-2-8 データの消失、損傷あるいは改悪および損失
 - 9-2-9 間接又は派生的損失 (9-2) 項の損失および損害を含む)
- 9-3 (9-1)の条件のもと、ソフトウェアの提供に関連して発生するカスペルスキーラブス及び代理店の責任(契約責任によるものであると不法行為によるものであるとを問わず)は、その原因がいかなるものであれ、その損害を引き起こしたソフトウェアの入手時にお客様が支払った金額または本製品の標準価格の何れか低い方を上限とします。

第 10 条 (プライバシーポリシー)

カスペルスキー製品および弊社が運営する Web サイトに適用されるプライバシーに関する方針は以下の通りです。

プライバシーポリシーは予告なしに随時更新されますので、定期的に変更を確認してください。情報の詳細については、弊社 Web サイトを参照してください。弊社のプライバシーポリシーの取り扱い等に関するお問い合わせは、末尾の情報を参照してください。

10-1 (収集される情報の種類および保存)

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

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

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

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

さい。

10-2（情報の取り扱い）

カスペルスキーは、取得した個人情報を次の目的でのみ使用します

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

10-2-2 コンテンツ制作の補助

10-2-3 キャンペーン等の案内

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

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

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

10-3（登録の解除）

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

10-4（セキュリティ）

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

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

10-5（クッキー（Cookies））

カスペルスキーはカスペルスキーが運営する Web サイト上でクッキーを

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

10-6 (統計情報)

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

他の企業および団体に関するプライバシーポリシー

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

10-7 (非機密情報)

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

10-8 (プライバシーポリシーに関する問い合わせ先)

株式会社 Kaspersky Labs Japan

TEL : 03-5687-7839

support@kaspersky.co.jp

第 11 条 (試用版に関する特約)

11-1 カスペルスキーラボスまたは代理店は、本製品を試用版として頒

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

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

第 12 条（契約の優先）

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

第 13 条（輸出の制限）

お客様は、米国および日本の政府機関が要求する条件、輸出管理法令等を遵守するものとします。関連する輸出入法規を遵守せず、「本製品」を日本国外へ輸出することおよび国外で使用することはできません。お客様は、キューバ、北朝鮮、イラン、シリア、スーダン、およびその他の貿易制裁適用国へ、「本製品」ならび規制対象技術を含むすべてのカスペルスキー製品の輸出または再輸出をしないことに同意するものとします。

お客様が「本製品」を日本国外へ輸出または国外で使用した場合、当該行為から生ずる一切の責任はお客様が負うものとします。

株式会社 Kaspersky Labs Japan