CommuniGate Pro プラグインのご案内：Cloudmark

CLOUDMARK

この文書は、英語版の翻訳です。その目的は、日本のエンジニアの皆様の理解に資することにあります。
翻訳版作成日：2007 年 3 月 22 日

CommuniGate Systems ソフトウェアライセンス契約（EULA）

注：CommuniGate Pro を使用された場合、下記のソフトウェアライセンス契約に同意したものとみなされます。

1. ライセンス。ディスクや ROM などの媒体の種類にかかわらずに、当該媒体に保存、記憶されている CommuniGate Pro ソフトウェアおよび CommuniGate Pro に関するマニュアルや説明書（以下、「CommuniGate Pro ソフトウェア」と総称します）はいずれも、米国カリフォルニア法人 CommuniGate Systems（以下、「CGS」と呼びます）からユーザーにライセンス（使用許諾権）供与され、したがって販売されるものではありません。CommuniGate Pro ソフトウェアを使用する場合、その使用は本契約書の条項によって制限されます。ライセンスは、CommuniGate Pro ライセンスキー（以下、「ライセンスキー」と呼びます）の形で提供され、ライセンスキーは数字で構成されます。
2. 使用の許可と制限。本ライセンス契約により、ユーザーは、単一のライセンスキーセット（複数のライセンスキーのセット）を単一のサーバーコンピュータ（シングプロセッサまたはマルチプロセッサのコンピュータ）上で使用できるようになります。ライセンスキーセットはそれぞれ、単一のインターネットドメイン名（以下、「メインドメイン」と呼びます）について発行されます。したがって、そのインターネットドメイン名が存在し、また、その名前が登録済みでなければなりません。ライセンスキーの発行後は、メインドメインの名前を変更することはできません。発行済みのライセンスキーを使用し、同一の CommuniGate Pro ソフトウェアインスタンス上でメインドメインのほかに任意の数のセカンダリドメインを動作させることができます。CommuniGate Pro ソフトウェアは、適用法規によって許可されている場合を除き、逆コンパイル、リバースエンジニアリング、逆アセンブル、修正、貸出、賃貸、貸与は一切禁止されており、CommuniGate Pro ソフトウェアから派生物を作成することもできません。ただし、何らかのコンポーネントについて、マニュアルや説明書で「カスタマイズ可能」と明記されている場合には当該コンポーネントを修正することができます。発行済みのライセンスキー（のセット）は、当該ライセンスキーの発行日（以下、「起算日」と呼びます）において正式にリリース済みであり、かつ最新である CommuniGate Pro ソフトウェアバージョンのほか、当該起算日から 12 カ月の間にリリースされた新バージョンについてのみ有効です（この 12 カ月を「初期保守期間」と呼びます）。発行済みのライセンスキーは、当該ライセンスキーが有効な CommuniGate Pro ソフトウェアの各バージョン以外のバージョンには使用できません。ユーザーが本ライセンス契約のいずれかの条項を遵守しなかった場合、当該ユーザーに与えられている権利は、CGS からの事前の通知なしに失われます。
300 ユーザー以上の CommuniGate Pro ライセンスではいずれも下記の契約条件が適用されます。
CommuniGate Pro プラットフォームのソフトウェアモジュールはすべて正常に機能し、ソフトウェアモジュールにはいずれも「開発ライセンス」が付属しています。この開発ライセンスの下でソフトウェアモジュール（オプションのモジュールを含む）の正規の機能をすべて利用し、ソフトウェアの開発（アプリケーション開発を含む）とテストが可能です。ただし、こうしたソフトウェアモジュールの機能を開発とテスト以外の用途に使用する場合、各モジュールのライセンスを CGS もしくは CGS の正規リセラーから購入しなければなりません。
3. 今後のバージョン。CGS では、時宜に応じて CommuniGate Pro ソフトウェアの新バージョンを開発することがあります。ただし、本ライセンス契約によって、CGS が CommuniGate Pro ソフトウェアの機能の更新や強化を行う義務を負うことはありません。今後、新機能または新コンポーネントを開発するかどうかは CGS が選択でき、当該新機能または新コンポーネントをユーザーが使用する場合、追加のライセンスキーが必要になります。ユーザーは、当該新機能、新コンポーネントを使用しないことを選ぶことができ、使用しない場合、追加のライセンスキーを購入する義務はありません。
4. 保守（継続使用）。初期保守期間の経過後にリリースされた CommuniGate Pro バージョンを使用する場合、更新ライセンスキー（のセット）が必要です。当該更新ライセンスキーは、月の日付のうち起算日の日付と同じ日、または、当該月の日数が少ないため起算日と同じ日付がないときには当該月の末日に発行が可能です。この日を更新日と呼びます。更新ライセンスキーを購入することにより、当該更新日から 12 カ月以内にリリースされた新バージョンの CommuniGate Pro ソフトウェアを使用する権利が与えられます。当該更新日からさらに 12 カ月が経過し（つまり 2 回目の更新日が到来し）、それ以後にリリースされた新バージョンを使用する場合、さらに新規の更新ライセンスキー（のセット）を購入することが必要です。更新ライセンスキーの価格は、最後の更新日（最初のライセンスキーの場合は起算日）以降の月数にメインテナンスフィーをかけて算出されます。ライセンスキーセットを更新するときには、そのセットに含まれている各ライセンスキーをすべて一括して更新しなければなりません。
5. 年次ライセンスが必要なコンポーネント。CommuniGate Pro ソフトウェアのコンポーネント（たとえば、サードパーティのプラグインなど）によっては、毎年、ライセンス供与を受けなければならないものもあります。つまり、当該コンポーネントは 12 カ月間だけ使用でき、その後は新規のライセンスキーを購入しなければなりま

せん。購入により、その後、さらに 12 カ月間にわたって当該コンポーネントを使用できます。当該コンポーネントのライセンスキーは、上記のセクション 4 の規定は適用されず、したがってメインテナンスフィーは不要です。
6. 契約の終了。本ライセンス契約は、期限はなく、上記のセクション 2 に規定されている事由によってのみ終了します。
7. CommuniGate Pro ソフトウェアに関する保証の放棄。ユーザーは、CommuniGate Pro ソフトウェアを自己の危険負担においてのみ使用することを認め、同意するものとします。CommuniGate Pro ソフトウェアは、「現状のまま」でいかなる保証も付与されずに提供され、CGS は、明示または非明示を問わず、また暗黙の保証を含め、もしくはそれに限定されず、当該ソフトウェアの特定用途に関する商品価値または適合性について、保証または条件をいっさい放棄することを表明します。CGS は、CommuniGate Pro ソフトウェアに備えられている機能がユーザーの要求に合致するかどうか、または CommuniGate Pro ソフトウェアが中断せずに動作、もしくはエラーなしで動作するかどうか、または CommuniGate Pro ソフトウェアに欠陥があった場合、その欠陥を修正するかどうかに関しては一切保証しません。CGS はまた、CommuniGate Pro ソフトウェアもしくは当該ソフトウェアに関連するマニュアル・説明書の使用または使用の結果に関して、当該ソフトウェアの動作、またはマニュアル・説明書の内容、または使用の結果が正確であり、精度が高く、もしくは信頼性があることを保証しませんし、その表明も行いません。CGS または CGS の正規の代理人が保証に関して口頭または書面で何らかの情報または助言を提供した場合でも、新たな保証が追加されることはなく、保証の範囲が拡張されることも一切ありません。CommuniGate Pro ソフトウェアに欠陥が存在することが証明された場合でも、当該欠陥に関して必要となるサービス、修理、修正の費用はすべてユーザー（CGS または CGS の正規の代理人ではなく）が負担するものとします。
8. 責任の制限。本ライセンス契約を原因として、または本ライセンス契約に関連して、偶発、特殊、間接、必然の別にかかわらず、何らかの損害が発生した場合、過失を含めいかなる理由でも CGS が当該損害の責任を負うことはありません。司法管轄区域によっては、偶発または必然の損害について責任の制限が認められていないこともあり、その場合には当該責任の制限は適用されないこともあります。損害について CGS に責任が発生したときでも、全損害に対する賠償責任は、本ライセンスの購入価格を超えないものとします。
9. 輸出関連法規。CommuniGate Pro のライセンスキーは、米国の法律および当該ライセンスキーを購入した司法管轄区域の法律で認可されている方法でのみ使用でき、当該法規に反して使用、輸出、再輸出することはできません。特に、またこれに限定されず、次の国または個人に CommuniGate Pro のライセンスキーを輸出または再輸出することはできません。(i) 米国により輸出禁止国として定められている国（または当該国の国民または在住者）、(ii) 合衆国財務省指定国家リストまたは合衆国商務省拒否命令表に指定されている個人。CommuniGate Pro のライセンスキーを使用することにより、ユーザーは自分が上記の国またはリストに該当する国民または在住者ではないこと、または当該国に居住しておらず、その管理下にもないことを表明し、保証することになります。
10. 米国政府機関のエンドユーザー。CommuniGate Pro のライセンスキーが米国政府機関のエンドユーザーに提供される場合、CommuniGate Pro ソフトウェアは、FAR の条項 52.227-19 に規定されている「制限コンピュータソフトウェア」に分類されます。CommuniGate Pro ソフトウェアに対する米国政府機関の権利は、FAR の条項 52.227-19 に規定されています。
11. 管轄法と可分性。いずれかの国のユーザーが CommuniGate Pro ソフトウェアのライセンスキーを購入し、当該国に CGS の関連子会社がある場合、その関連子会社が所在する地域の法律を本ライセンス契約の管轄法とします。それ以外の場合、本ライセンス契約は、連邦法およびカリフォルニア州法によって管轄されるものとします。何らかの理由により、本契約のいずれかの条項または一部が管轄裁判所によって履行不可能と判定されたときでも、それ以外の条項はすべて、その後も完全に効力があり有効であるものとします。
12. 完全な合意。本ライセンス契約は、CommuniGate Pro ソフトウェアの使用に関して、各当事者間の完全で包括的な合意であり、以前または現時点で発生した解釈すべてに優先するものとします。本ライセンス契約の改定または修正は、当該改定または修正が書面で行われ、かつ当該書面に CGS の署名がある場合にのみ拘束力を有するものとします。この EULA を除き、英語の本ライセンス契約と日本語の本ライセンス契約の解釈において何らかの相違が発生した場合、英語の本ライセンス契約の解釈が優先されるものとします。

CommuniGate Systems, a Division of Stalker Software Inc.
655 Redwood Highway, #275
Mill Valley, CA 94941 USA

お問い合わせ先:
CommuniGate Systems Japan　Tel:046-872-4950　japan@communigate.com
日本の販売代理店:http://www.communigate.com/content/asia.html
CommuniGate Systems 本社 http://www.communigate.com　Tel:800-262-4722

Cloudmark プラグインの概要

Cloudmarkプラグイン(スパムフィルタリングプラグイン)は外部フィルタとして動作し、処理中の各メッセージについてそれぞれ、「スパムスコア(点数)」を付けるという処理を行います。一般的なスパムフィルタリングプラグインでは、あらかじめ定義された静的なパターンをもとにスパムメッセージがチェックされます。一方、Cloudmarkの場合、Cloudmarkネットワークから動的に新規のパターンが取得されるため、新しいスパムメッセージに対する精度が非常に高いのが特徴です。

スコアの範囲は、1 から 100 までです。このスコアの値が高いほど、そのメッセージがスパムである可能性が高いことを示します。スコア情報は、メッセージヘッダに追加されます。そのため、スパムメッセージは、サーバーワイド、ドメインワイド、アカウントレベルのルールで処理できます(メッセージのヘッダをチェック)。

デフォルトでは、Cloudmark によって追加されるヘッダ行は次のとおりです。

X-Cloudmark-Score: 92.120000 [XXXX] (X-Cloudmark スコア: 92.120000 [XXXX])
X-Alert: possible spam! (X-Alert: スパムの可能性あり!)
X-Color: red (X-Color: 赤)

最初の行は、数字のスコア値と「バースコア(X のリスト)」で構成されます。このバースコアは、メッセージの自動処理ルール用の簡易代替表現で、'X'の数が多いほどスコア値が高いことを示しています。スコア値とバースコアの対応は、次のとおりです。

スコア(数値)	バースコア
0	[]
1-39	[X]
40-80	[XX]
81-90	[XXX]
91-95	[XXXX]
96-99	[XXXXX]
100	[XXXXXX]

毎日、夜 12 時に Cloudmark プラグインからレポートメッセージが出力されます。このレポートメッセージには、処理されたメッセージ(メール)の数と、各メッセージのスパムスコアが記述されています。デフォルトでは、レポートメッセージは CommuniGate Pro のメインドメインのアカウント postmaster に送信されます。

注意:Cloudmark プラグインを使用できるのは、CommuniGate Pro サーバーでサポートされているプラットフォームのうちいくつかに限られます(下記のダウンロードの説明を参照)。Cloudmark プラグインのライセンスを購入する前に、現在の CommuniGate Pro サーバープラットフォーム(または使用予定のプラットフォーム)で Cloudmark プラグインがサポートされているかどうかを確認してください。

注意:Cloudmark プラグインを使用する場合、CommuniGate Pro バージョン 4.3.12 以降が必要です。ハードウェア要件:Pentium II 以上(Solaris の場合は UltraSparc)、マルチプロセッサシステムとマルチコア CPU を推奨(ただし、Intel HyperThreading は不可)、512MB の RAM、200MB のハードディスクスペース。

注意:Cloudmark を使用する場合、インターネット接続が必要です。一日に約 100MB のアップデートデータがダウンロードされます。

Cloudmark プラグインのダウンロード

Cloudmark プラグインは、下記のプラットフォーム(オペレーティングシステム)でのみ利用できます。

オペレーティングシステム	CPU	ダウンロード	
		http	ftp
Linux(RedHat、SuSE)	x86		
FreeBSD 4.x	x86		
Sun Solaris	Sparc		
Microsoft Windows NT/2000/XP/2003 Microsoft Windows 95/98/ME	x86		

Cloudmark プラグインの最新バージョンは 1.5 です。

Linux システムでのインストール

- スーパーユーザー(root)でログインします。
- CommuniGate Pro *ベースディレクトリ*に移動します(カレントディレクトリを CommuniGate Pro *ベースディレクトリ*に変更します)。
- gtar コマンド(またはgunzipコマンドとtarコマンド)を使ってCloudmarkプラグインアーカイブをアンパックします。下は例です。

  gunzip CGPCloudmark-*プラットフォーム*-*プロセッサ*.tar.gz
  tar -xf CGPCloudmark-*プラットフォーム*-*プロセッサ*.tar

  CommuniGate Pro *ベースディレクトリ*の中にCGPCloudmarkディレクトリが作成されます。
- CGPCloudmarkディレクトリの中に移動します。
  cd CGPCloudmark
- CGPCloudmarkディレクトリの中にあるlibcmae.soファイルを/usr/libディレクトリに移します。または、LD_LIBRARY_PATH環境変数に指定されているディレクトリでもけっこうです。
  mv libcmae* /usr/lib/
- CGPCloudmarkディレクトリから抜けます。
  cd ..
- Cloudmarkプラグインの動作テストの説明にしたがって動作テストを行います。

注意: Linuxプラットフォームの場合、Cloudmarkオーソリティエンジンの動作には次の各ライブラリが必要です。

ライブラリ名	場所
libz.so.1	/usr/lib
libstdc++-libc6.2-2.so.3	/lib
libpthread.so.0	/lib
libdl.so.2	/usr/lib
libm.so.6	/lib
libc.so.6	/lib

FreeBSD システムでのインストール

- スーパーユーザー(root)でログインします。
- CommuniGate Pro *ベースディレクトリ* に移動します。
- gtar コマンド(またはgunzipコマンドとtarコマンド)を使ってCloudmarkプラグインアーカイブをアンパックします。下はコマンド例です。
  gunzip CGPCloudmark-*プラットフォーム*-*プロセッサ*.tar.gz
  tar -xf CGPCloudmark-*プラットフォーム*-*プロセッサ*.tar
  CommuniGate Pro *ベースディレクトリ*の中にCGPCloudmarkディレクトリが作成されます。
- CGPCloudmarkディレクトリの中に移動します。
  cd CGPCloudmark
- CGPCloudmarkディレクトリの中にあるlibcmae.soファイルを/usr/libディレクトリに移します。または、LD_LIBRARY_PATH環境変数に指定されているディレクトリでもけっこうです。
  mv libcmae* /usr/lib/
- CGPCloudmarkディレクトリから抜けます。
  cd ..
- Cloudmarkプラグインの動作テストの説明にしたがって動作テストを行います。

注意: FreeBSDプラットフォームの場合、Cloudmarkオーソリティエンジンの動作には次の各ライブラリが必要です。

ライブラリ名	場所
libc_r.so.4	/usr/lib
libm.so.2	/usr/lib

Solaris システムでのインストール

- スーパーユーザー(root)でログインします。
- CommuniGate Pro *ベースディレクトリ*に移動します。
- gtar コマンド(またはgunzipコマンドとtarコマンド)を使ってCloudmarkプラグインアーカイブをアンパックします。下はコマンド例です。
  gunzip CGPCloudmark-*プラットフォーム-プロセッサ*.tar.gz
  tar -xf CGPCloudmark-*プラットフォーム-プロセッサ*.tar

  CommuniGate Pro *ベースディレクトリ*の中にCGPCloudmarkディレクトリが作成されます。
- CGPCloudmarkディレクトリの中に移動します(下記はコマンド例)。
  cd CGPCloudmark
- CGPCloudmarkディレクトリの中にあるlibcmae.soファイルを/usr/libディレクトリに移します。または、LD_LIBRARY_PATH環境変数に指定されているディレクトリでもけっこうです。
  mv libcmae* /usr/lib/
- CGPCloudmarkディレクトリから抜けます。
  cd ..
- Cloudmarkプラグインの動作テストの説明にしたがって動作テストを行います。

注意: Solaris プラットフォームの場合、Cloudmarkオーソリティエンジンの動作には次の各ライブラリが必要です。

ライブラリ名	場所
libz.so	/usr/lib
libpthread.so.1	/usr/lib
libpthread.so.0	/usr/lib
libsocket.so.1	/usr/lib
libnsl.so.1	/usr/lib
libresolv.so.2	/usr/lib
libdl.so.1	/usr/lib
librt.so.1	/usr/lib
libstdc++.so.2.10.0	/usr/local/lib
libm.so.1	/usr/lib
libc.so.1	/usr/lib
libmp.so.2	/usr/lib
libaio.so.1	/usr/lib
libthread.so.1	/usr/lib

libstdc++.so.2.10.0 は、Cloudmarkプラグインの配布アーカイブのCGPCloudmark/lib/サブディレクトリに用意されています。既存のシステムにlibstdc++.so.2.10.0 がない場合、このファイルを/usr/local/lib/に入れてください。

MS Windows システムでのインストール

- CommuniGate Pro ベースディレクトリに移動します。
- CGPCloudmark-Win32-Intel.zip プラグインアーカイブファイルをダウンロードします。
- "unzip"ツールを使ってプラグインをアンパックします。
  pkunzip CGPCloudmark-*.zip
  CommuniGate Pro ベースディレクトリ の中に CGPCloudmark ディレクトリが作成されます。
- Cloudmarkプラグインの動作テストの説明にしたがって動作テストを行います。

注意: Windows プラットフォームの場合、Cloudmark オーソリティエンジンの動作には次の各ライブラリが必要です。

ライブラリ名	場所
MSVCR71.DLL	{SystemDir}¥system32
MSVCP71.DLL	{SystemDir}¥system32

Cloudmark プラグインのアップデート

Cloudmark プラグインをアップデート(プログラムを更新)する場合、次のようにします。

- 現在使用している Cloudmark プラグインのデフォルトの設定を変更している場合、次のファイルの内容を保存します(設定は、各ファイルに格納されています)。
  - CGPCloudmark.cfg (設定ファイル)
  - whitelist.cfg (ホワイトリストファイル)
  - cartridge.cfg (カートリッジファイル)
- CommuniGate Pro の WebAdmin インターフェイスを使って Cloudmark プラグインの動作を停止させます。
- CGPCloudmarkディレクトリにあるファイルをすべて削除します。
- Cloudmark プラグインのアップデート(新バージョン)をインストールします(インストール手順は上記を参照)。
- 新バージョンのCGPCloudmark.cfg、whitelist.cfg、cartridge.cfgの内容を修正し、修正後のファイルを使用します。

Cloudmark プラグインの動作テスト

UNIX システムの場合、次のようにしてテストします。

- CommuniGate Pro ベースディレクトリに移動します。
  cd /var/CommuniGate
- 移動したディレクトリの中にある CGPCloudmark アプリケーションを次のようにして起動します。
  CGPCloudmark/CGPCloudmark

  重要: CGPCloudmark アプリケーションは必ず、CommuniGate Pro ベースディレクトリから起動してください（CGPCloudmark/CGPCloudmark）。CGPCloudmark ディレクトリからは起動しないでください（ ./CGPCloudmark）。
  CGPCloudmark アプリケーションの起動後、次の各行が出力されます。
  ＊ CGPCloudmark プラグインバージョン n.m プラットフォーム-プロセッサ ビルド 日付 開始
  ＊ エンジンを初期化中、お待ちください...
  ＊ Cloudmark オーソリティエンジンバージョン x.y.z 初期化完了
  ＊ カートリッジバージョン: x.y.z.a アップデート バージョン=nnn

- 次のコマンドを実行します。
  1 FILE CGPCloudmark/test.msg
  プラグインから応答（ADDHEADER）のほか、メッセージヘッダ行（スコア付き）が返ります。

- Ctrl-D を押して、CGPCloudmark アプリケーションを終了します。

Windows システムの場合、次のようにしてテストします。

- CommuniGate Pro ベースディレクトリ に移動します。
  cd "C:¥CommuniGate Files"
- CommuniGate Pro ベースディレクトリ から CGPCloudmark.exe アプリケーションを起動します。
  CGPCloudmark¥CGPCloudmark.exe

  重要: CGPCloudmark.exe アプリケーションは必ず、CommuniGate Pro ベースディレクトリから起動してください（CGPCloudmark¥CGPCloudmark.exe）。CGPCloudmark ディレクトリからは起動しないでください。
  CGPCloudmark アプリケーションの起動後、次の各行が出力されます。
  ＊ CGPCloudmark プラグインバージョン n.m Windows-Intel ビルド 日付 開始
  ＊ エンジンを初期化中、お待ちください...
  ＊ Cloudmark オーソリティエンジンバージョン x.y.z 初期化完了
  ＊ カートリッジバージョン: x.y.z.a アップデート バージョン=nnn

- 次のコマンドを実行します。
  1 FILE CGPCloudmark¥test.msg
  プラグインから応答（ADDHEADER）のほか、メッセージヘッダ行（スコア付き）が返ります。
- Ctrl-Z を押して、CGPCloudmark アプリケーションを終了します。

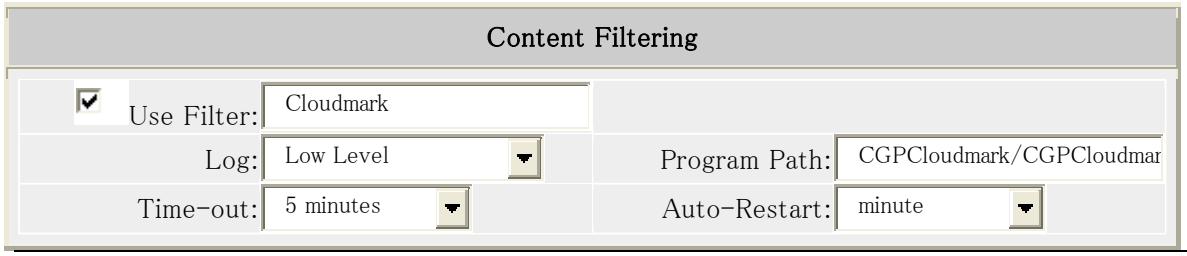
注意: CGPCloudmarkのエンジンの初期化（また更新情報のダウンロード）は、インターネットの帯域幅（通信速度）とCPUスピードによっては数分かかることがあります。

Cloudmark プラグインと CommuniGate Pro の統合(プラグインの組み込み)

ステップ 1:ヘルパーの作成

ヘルパーについては、詳しくはCommuniGate Proマニュアルの外部フィルタのセクションをご覧ください。

WebAdmin インターフェイスの[Settings]セクションの[General]ページを開きます。続いて[Helpers]リンクをクリックします。Cloudmark プラグインの設定(ヘルパーの作成)ページが開きます。



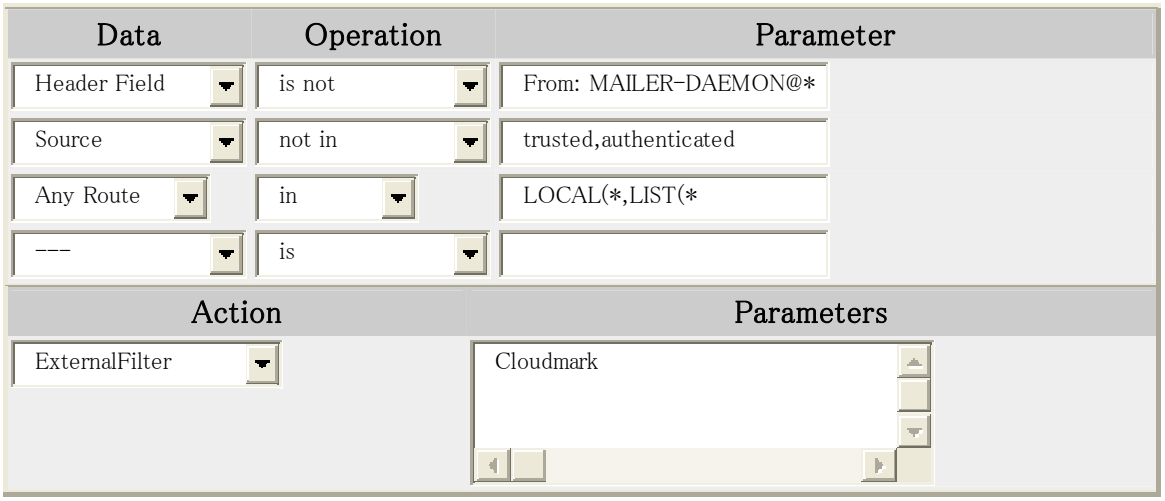
注意: MS Windowsシステムの場合、[Program Path]フィールドには"CGPCloudmark¥CGPCloudmark.exe"と入力します。パスの区切り文字はスラッシュ(/)ではなくバックスラッシュ(日本語システムでは¥)ですので注意が必要です。

ステップ 2:スキャニングルールの作成

Cloudmarkプラグイン(ヘルパーまたは外部フィルタとも呼びます)を起動する場合、サーバーワイド(サーバー全体で有効な)ルールを作成しなければなりません。ルールのアクションは"ExternalFilter"、パラメータは"Cloudmark"です(外部フィルタとしてCloudmarkを使用)。このルール(スキャニングルール)により、Cloudmarkがメッセージに対して機能し、メッセージヘッダにスパムスコア(行)が追加されます。

注意: ルールは、ドメインワイドルールまたはアカウントレベルのルールではなく、サーバーワイドルールでなければなりません(サーバー全体に対して動作させます)。

下記は、スキャニングルールの設定例です(この設定を推奨します)。



上のルールでは、MAILER-DAEMONアドレスからのメッセージ(配信不能レポート、受け取り通知など)、クライアントIPアドレスからのメッセージ、認証済み差出人からのメッセージはすべてスキップ(チェックなし)されます。結局、ローカルアカウントとメーリングリスト宛てのメッセージだけがルールによってチェックされます。

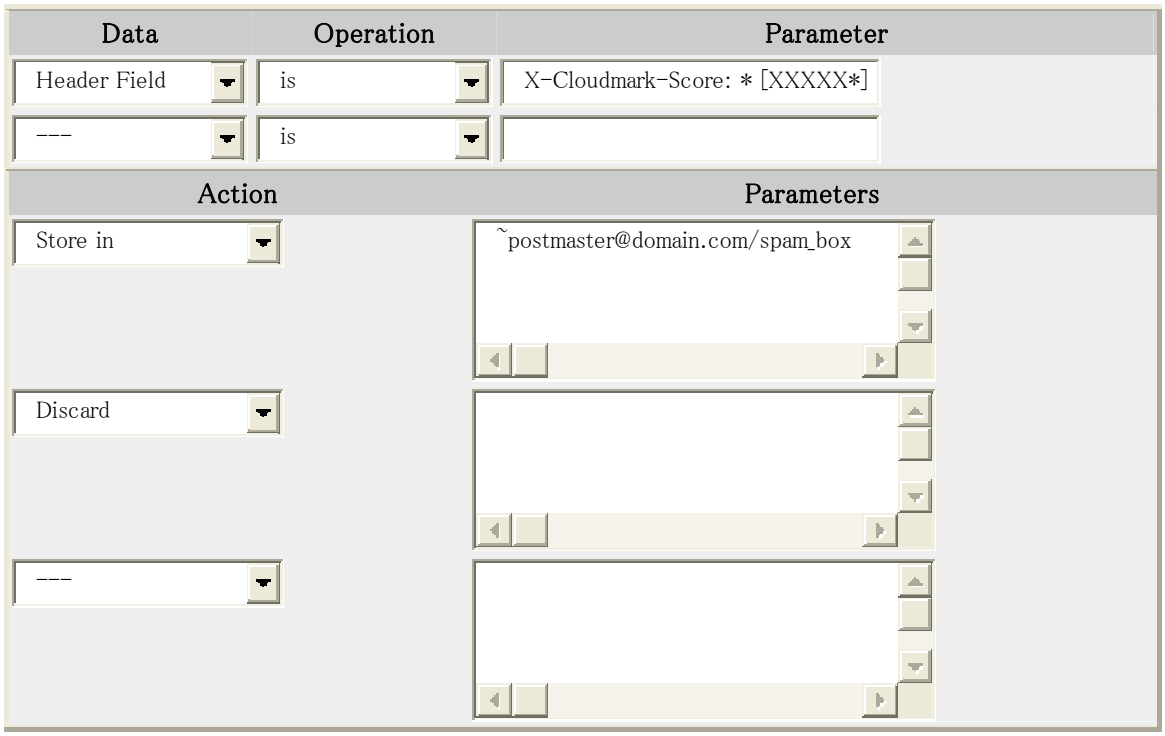
注意: Cloudmarkプラグインのライセンスを取得していない場合(未ライセンスバージョンを使用している場合)、プラグインによって処理されるメッセージは 1 時間に 5 つまでに限定されます。この上限を超えるメッセージは、プラグインを素通りします(後述のプラグイン設定ファイルの説明を参照)。

ステップ 3:スコアが付加されたメッセージの処理

Cloudmark プラグインは、それ自体にはスパムを排除する機能はありません。メッセージにスパムスコアが追加されるだけです。したがって、スパムをブロックする場合、上記のルール(スキャニングルール)とは別に、スパムスコアに応じてスパムを実際にブロックするルールを作成しなければなりません。方法は色々あります。以下、シナリオを例に説明します。

シナリオ 1: このルールは、システムの規模が小さいときに適しています。たとえば、社内の誰か一人(postmasterなど)が毎日スパムメッセージをチェックし、「偽陽性」のメッセージ(誤ってスパムと判断されたメッセージ)があれば所定のアドレスにリダイレクトする、といった場合に適当です。

この場合のルールは、サーバーワイドルールとします(サーバー全体に機能します)。内容は次のとおりです。



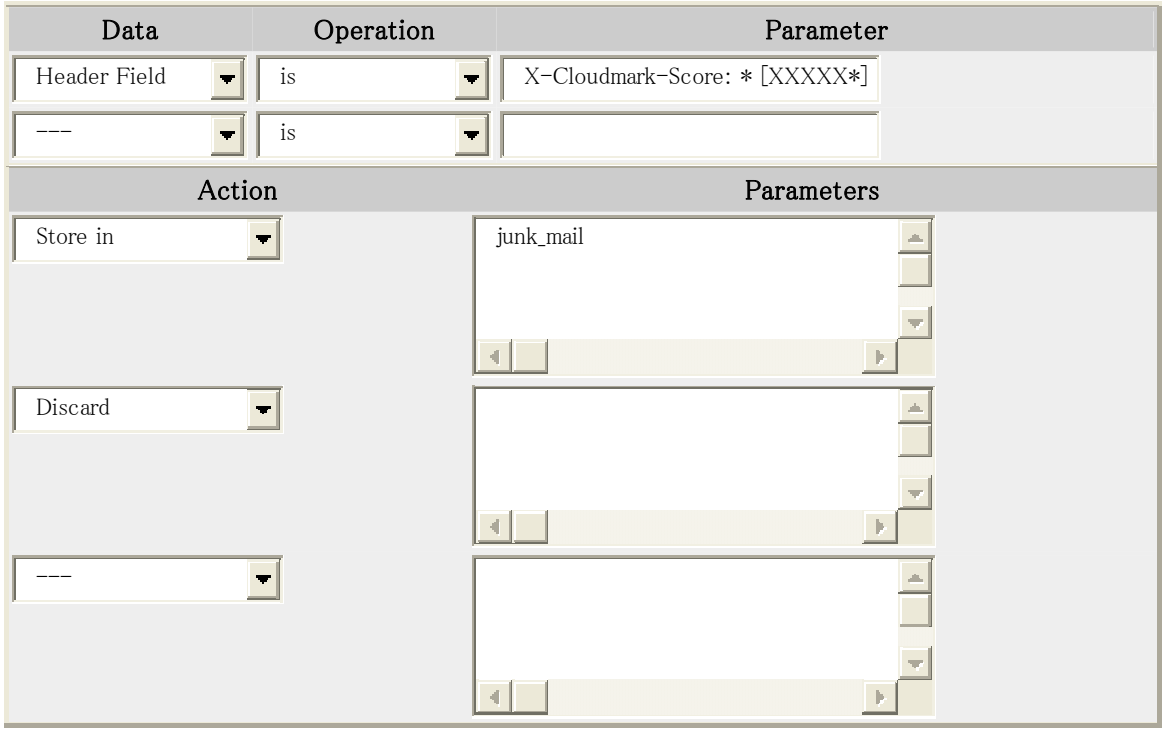
このルールでは、スパムスコアが 96(Xが 5 つ)以上の受信メッセージがアカウントpostmaster@domain.comの"spam_box"メールボックスに配信されます("Store in"アクション)。

また、"Discard" アクションにより、該当するメッセージは当初のデスティネーション(ユーザーのINBOX)には送られず、廃棄されます。なお、[XXXXX*]の中の"*"記号は、6 つめのXを表しています。つまり、Xが 5 つ、またはそれ以上(ここでは 6 つまで)のメッセージがすべてフィルタリングされることになります。この"*"がない場合、Xが 5 つのメッセージだけがフィルタリングされます。

注意: このサーバーワイドルールの優先度は、スキャニングルール(上記)の優先度より低くなければなりません。

シナリオ 2: このルールは、大規模企業またはISPに適しています。このルールの場合、ユーザーは自分でスパムの管理が可能です(アカウントレベルのルールを作成します)。

ドメインワイドルールを作成します。または、ユーザーがそれぞれアカウントレベルのルールを作成することもできます(各ユーザーまたは管理者が必要に応じて設定します)。

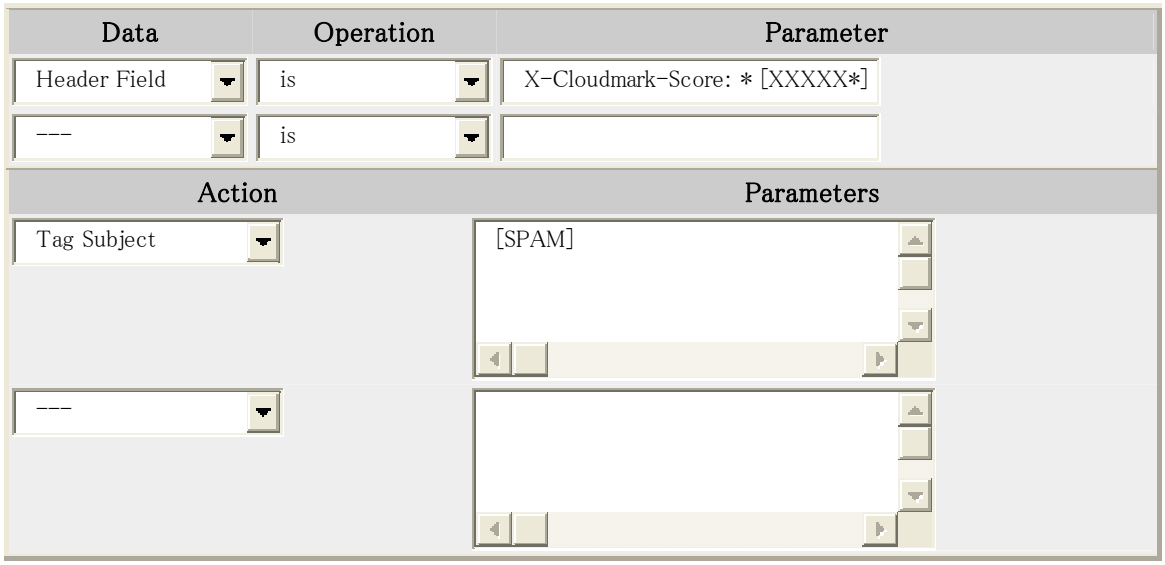


このルールでは、スコアが 96 以上のメッセージがすべて、受取人アカウント(ユーザー)の"junk_mail"(迷惑ルール)メールボックスに配信されます。したがって、ユーザーは"junk_mail"メールボックスをチェックし、不要なメッセージを削除できます。また、"Discard" アクションにより、該当するメッセージは当初のデスティネーション(ユーザーのINBOX)には送られず、廃棄されます。なお、[XXXXX*]の中の"*"記号は、6 つめのXを表しています。つまり、Xが 5 つ、またはそれ以上のメッセージがすべてフィルタリングされることになります。この"*"がない場合、Xが 5 つのメッセージだけがフィルタリングされます。

"junk_mail"メールボックス(名前は任意)は必ず、存在しなければなりません。存在しないときには、このルールは機能せず、メッセージはユーザーの INBOX に配信されます。

シナリオ 3: このルールは、大規模企業のユーザーまたはISPの顧客ユーザーがINBOX以外にはアクセスしない場合(たとえば、全員がPOP3 ユーザーの場合)に適しています。

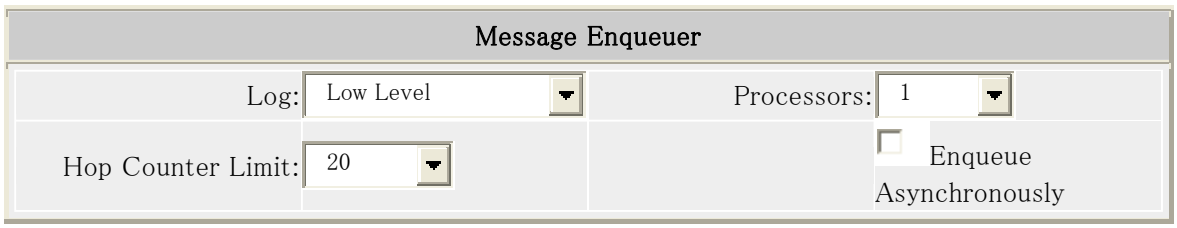
ドメインワイドルールを作成します。または、ユーザーがそれぞれアカウントレベルのルールを作成することもできます(各ユーザーまたは管理者が必要に応じて設定します)。



このルールでは、スパムメッセージ(スコアが 96 以上のメッセージ)の[件名(Subject)]に接頭辞として[SPAM] 付加されます(件名の先頭に[SPAM]という文字列が追加されます)。

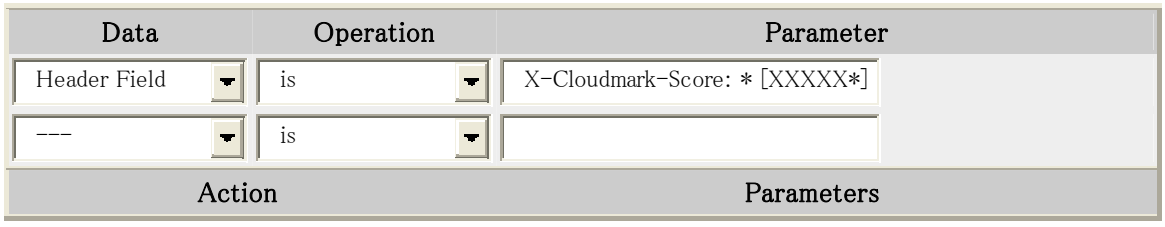
シナリオ 4: このルールは、入力トラフィックが比較的少ない企業に向いています。このルールは、CommuniGate Proバージョン 5.1 以降で使用できます。

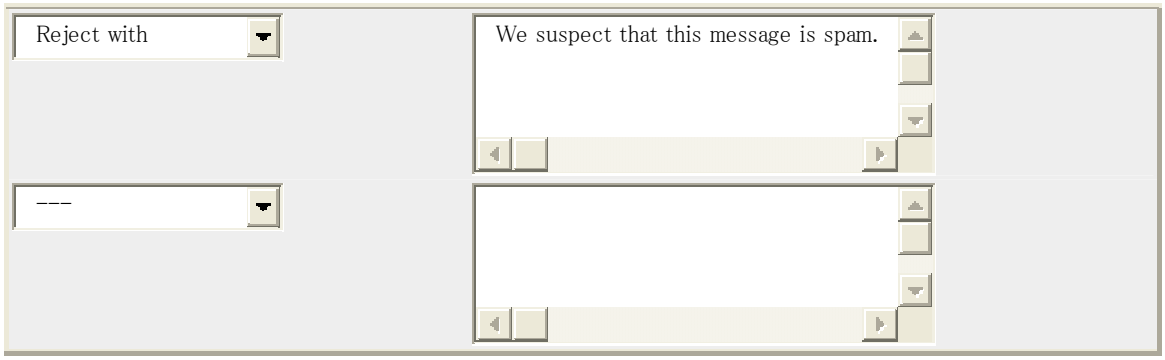
CommuniGate Pro バージョン 5.1 以降では、メッセージの同期エンキュー(SMTP トランザクションレベルでの待ち行列処理)が可能です。同期エンキューを有効にしたい場合、WebAdmin インターフェイスで Enqueuer(エンキューア)コンポーネントを設定します。手順は、[Settings]セクションの[Queue]ページを開きます。その後、[Enqueue Asynchronously](非同期エンキュー)チェックボックスの選択を解除します。



Enqueuer コンポーネントについては、詳しくは[CommuniGate Proのマニュアル]を参照してください。

このシナリオの場合、サーバーワイドルールを作成します。内容は次のとおりです。





同期エンキューが有効になっている場合、サーバーワイドルールによってメッセージが拒否されると、そのメッセージは SMTP レベル（トランザクション）で拒否されます（5xx エラーコードを出力）。つまり、どこかで受け取られることもありませんし、バウンスされることもありません。

どんな場合でも、スパムメッセージをまったく保存せずに「盲目的」に廃棄するのは推奨できません。中には「偽陽性」のメッセージもあるためです。また、スパムを自動的に拒否（Reject）するのも推奨できません（ただし、シナリオ 4 の同期エンキューモードの場合は例外です）。理由は、スパムメッセージは一般にリターンアドレスが改変されており、したがって拒否通知が善意の第三者やスパムトラップに送られるためです。その結果、こちらのサーバー（CommuniGate Pro）がブラックリストに登録されることがあります。一方、同期エンキューモードでの拒否の場合、送信元のホストで SMTP トランザクションの際にエラーが受信されるため、この問題は起こりません。また、CommuniGate Pro サーバー上でバウンスが生成されることもありません。

スパムスコアの推奨しきい値（メッセージをスパムと判定し始めるときのスコアの値）は 96 です。この値でスパムを十分捕捉できない（すり抜けるスパムが多い）ときには、しきい値を 90 に下げます。これで、スパムスコアが 90（以上）と判定されたメッセージもフィルタリングされます。一方、偽陽性メッセージ（スパムでないのにスパムと判定されるメッセージ）が多い場合、しきい値を 100 に上げます。

Cloudmark プラグイン設定ファイル

Cloudmarkプラグインの起動時、カレントディレクトリにあるCGPCloudmark.cfgファイル（プラグイン設定ファイル）の内容がCloudmarkプラグインによって読み取られます。このファイルのデータ要素のフォーマットについては、http://www.stalker.com/CommuniGatePro/Data.htmlに説明がありますので、そちらをご覧ください。また、データ要素の説明は、CGPCloudmark.cfgファイルの中にも記述されています。デフォルトのCGPCloudmark.cfgは、ここにあります。

以下、デフォルトのCGPCloudmark.cfgファイルの内容について説明します。

Header="X-Cloudmark-Score: ^1 [^2]";

ヘッダ。このヘッダ（スコア）がメッセージに追加されます。^1（マクロ）は、数値スコアに置換されます。^2 は、バースコア（Xで構成）に置換されます。

複数行のヘッダを生成したい場合、行区切り文字として¥e を使用します。各行ともRFC準拠のヘッダでなければなりません。行の先頭はそれぞれ、接頭辞 "X-" で始めるようにします。たとえば、Header="X-Score: ^1¥eX-Bar-Score: ^2" などとなります。

AlertLevel=96;

この行には、スコア（数値）を指定します（96 が推奨値）。メッセージのスコア（Cloudmarkプラグインによって追加されたスパムスコア）が、この値以上だった場合、AlertHeader（アラートヘッダ、下記を参照）がメッセージに挿入されます。また、そのメッセージのソース（送信元）アドレスとデスティネーション（受信元）アドレスがそれぞれ、日次レポートにスパムソース（Spam Source）とスパムターゲット（Spam Source Target）として記録されます。

AlertHeader="X-Alert: possible spam!¥eX-Color: red";

処理対象のメッセージのスコアが上記のAlertLevelの値以上だった場合、ここに指定されているヘッダがメッセージに挿入されます。右側の"X-Color: red"は色を表します。このメッセージは、CommuniGate ProのWebメールインターフェイスでは、ここで指定された色で表示されます。

注意: ルールでスパムを処理する（たとえばjunk_boxに配信する）場合、メッセージのスコア（[Parameter]フィールドの値、たとえば"X-Cloudmark-Score: * [XXXXX*]"）の代わりにAlertHeaderの内容（たとえば"X-Alert: possible spam!"）をチェックすることもできます。ただし、この方法はあまり柔軟ではありません。この方法の場合、各ユーザーがそれぞれ別々のスコアを指定してメッセージを処理することができなくなります（AlertLevelで指定されているスコアが全ユーザーに対して一律に使用されます）。

SubmittedDirectory = "Submitted";

この行には、CommuniGateProのSubmittedディレクトリを指定します。この定義にしたがってPIPEモジュールを介してレポートが出力されます。パスは、相対または絶対のどちらでも可能です（たとえば、"/var/CommuniGate/Submitted"）。

OnLicenseLimitReached=Pass;

この行では、処理対象のメッセージ数が、Cloudmark プラグインのライセンスで許可されているメッセージ数の上限を超えたときの Cloudmark プラグインの動作を指定できます。"Delay"（遅延）が指定されている場合、CommuniGate Pro のキュー処理モジュールによる処理が次のウィンドウまで中断されます。"Pass"（通過）が指定されているときには、上限を超えたメッセージはそのまま評価されずに（スコア付けなしで）通過します。スコアのないメッセージとは、X-Cloudmark-Score ヘッダがないメッセージをいいます。なお、メッセージ数が、ライセンスで許可されているメッセージ数の上限を超えたときには、その旨が CommuniGate Pro のログに記録されます。

Cloudmark エンジン設定ファイル

Cloudmarkの初期化時、Cloudmarkエンジンによって、cartridge.cfgファイル（カートリッジ）に格納されている設定オプションの内容、またwhitelist.cfgファイル（ホワイトリスト）のwhitelistingオプションの内容が読み取られます。

マイクロアップデート

マイクロアップデート（Micro-update）とはメカニズムの名称で、このメカニズムのもとでCloudmark カートリッジによって最新の「指紋データ」が定期的にダウンロードされます。その後、ダウンロードされた「指紋データ」を使って、不適正メッセージ（スパム）が識別されます。指紋データは、極めて信頼性が高い情報筋からの報告のほか、Cloudmark コラボラティブセキュリティネットワークの信頼性評価システムによる分析をもとにほぼリアルタイムで生成、提供されます。言い換えると、マイクロアップデートは、カートリッジの精度を維持する上で非常に重要なメカニズムであり、このマイクロアップデートを介して新たなスパムメッセージやフィッシングメッセージ、ウィルスメッセージが報告されます。

デフォルトのcartridge.cfgファイルの内容は、ここにあります。

ネットワークとポート

Cloudmark のマイクロアップデートの内容（更新情報）は、標準の HTTP 要求を使ってダウンロードされます。HTTP プロキシが無効の場合（デフォルトの設定）、所定の時間間隔で、ポート 80 を介してフィルタリングサーバー（Cloudmark）からマイクロアップデートサービスへの接続とダウンロードが試行されます。ここで、ポート 80 でのマイクロアップデートサービスへの接続に失敗したときには、ポート 25 を使ってダウンロードが試行されます。ポート 25 によるダウンロードにも失敗した場合、マイクロアップデート辞書のデータファイルのうち最新のデータファイル（オフラインバージョン）を使って処理が行われます。その後、次回のマイクロアップデートのダウンロード時刻になると再度、ダウンロードが試行されます。

データファイルの整合性とセキュリティ

マイクロアップデートのデータファイルのデータはいずれも圧縮され、暗号化されています。また、暗号化されているデータでも、その暗号化キーが不適正なデータは無視されます。その結果、DNS スプーフィングや IP スプーフィングといった問題は発生しません。データファイルの内容は Cloudmark の起動時にメモリに読み込まれるため、いつも新しいデータが使用されます。また、新規のファイルがダウンロードされるたびに、そのファイルが使用されます。

カートリッジ統計データ

デフォルトでは、Cloudmark カートリッジ（プラグインのカートリッジ）からカートリッジ設定情報とメッセージスキャニング統計データ（スキャニングの結果データ）が Cloudmark 社に返送されるように設定されています。Cloudmark 社では、この情報を分析することによりスパム検出の精度の向上に努めています。したがって、通常、顧客ユーザーが精度について Cloudmark 社に連絡する必要はありません。ただし、企業側でとくにプライバシーに関して懸念がある場合（統計

データにはアドレスなどの個人データが格納されています)、この統計データ返送機能を無効にすることもできます。

統計データは、カートリッジのインストール場所ごとに収集されます。収集された統計データは、ディスクに書き込まれることはなく、また、カートリッジのインストール場所からアクセスすることもできません。デフォルトでは、統計データは、http://<*設定済みマイクロアップデート用ホスト*>/cmstatsを介してCloudmark社に送信されます。*設定済みマイクロアップデート用ホスト* は、デフォルトでは microupdates.cloudmark.com です。HTTPプロキシを使ってマイクロアップデートがダウンロードされるように設定している場合(cartridge.cfgファイルで設定)、そのHTTPプロキシを使って統計データがCloudmark社に送信・報告されます。また、デフォルトでは、統計データは 1 時間ごとにCloudmark社に送信されます。統計データの送信時間間隔は、Cloudmark社で決定、管理しています。顧客ユーザー側でスパム検出の精度に関する問題が発生したり、その問題が報告されたりした場合、Cloudmark社では、統計データの送信時間間隔を調整することがあります。

cartridge.cfg ファイルには"customer id = communigate-customername@feedback.cloudmark.com"という行がありますが、この中の"customername"(顧客名)を自社の名前に変更してください(Cloudmark 社への質問・連絡用の電子メールアドレスです)。

ホワイトリスティング(ホワイトリストへの登録)

ホワイトリストは Cloudmark カートリッジの機能の一つで、具体的には信頼できる送信者のリストです。このリストに登録されている送信者からの電子メール、またメッセージが信頼できることを示す電子メール属性(ヘッダなど)は必ず、受け取られます。この機能により、信頼できるメッセージのフィルタリングが省略されるためフィルタリング処理が最小化されます。また、管理者は、このリストを使うことで「安全な送信者」を容易に管理できます。

デフォルトのwhitelist.cfgファイルの内容は、ここにあります。

コマンドシェルからの Cloudmark プラグインの起動

Cloudmark プラグインは、いわゆるテキストオンリアプリケーションです。つまり、コマンドシェルから起動でき、コマンドラインオプションも指定できます。なお、CommuniGate Pro で Cloudmark プラグインをヘルパーアプリケーションとして使用する場合、コマンドラインオプションを指定する必要はありません。

メッセージファイルの「格付け」

Cloudmark プラグインを使って、ディレクトリに保存されている既存のメッセージファイルを分析し、スパムスコアを算出することができます。

この処理を行う場合のプログラム(コマンド)のシンタックスは、CGPCloudmark RATE [options] <directory> です(下記のコマンド例を参照)。

上で、<directory> には、処理対象のメッセージファイルが格納されているディレクトリを指定します。メッセージファイルのフォーマットは、RFC822 フォーマットまたはCommuniGateフォーマット(エンベロープ情報付きのRFC822)でなければなりません。また、一つのファイルに格納されているメッセージは一つ

でなければなりません。CommuniGate Proのメールボックスのうち.mdirフォーマットのメールボックスに格納されているメッセージも処理できます。.EML、.MSG、.mboxなどのフォーマットのメッセージは、RFC822 フォーマットに変換しなければなりません。なお、フォーマットを変換する際には、メッセージの内容を変更しないように注意する必要があります。たとえば、"Received" ヘッダが削除されてしまうことがよくあります。また、メールクライアントでは、メッセージの保存時に内容が変更されることが非常に多く、その場合、スパムスコアは必ずしも正確でないことがあります。

コマンドの例: ./CGPCloudmark RATE /var/CommuniGate/Queue

誤分類メッセージを Cloudmark ネットワークフィードバックシステムに報告

Cloudmark ネットワークフィードバックシステム（Cloudmark Network Feedback System＝CNFS）は、自動フィードバックメカニズムです。Cloudmark の顧客（ISP や企業の方々、つまり CNFS ユーザー）は、このフィードバックシステムを使用して誤分類メッセージ（スパムの判定が誤ったメッセージ）を直接、Cloudmark サービスに送信できます。また、CNFS ユーザーは、Cloudmark ネットワークフィードバックシステム上で Cloudmark コラボラティブセキュリティネットワークのメンバーになることもできます。このセキュリティネットワークのメンバーは現在、数百万に達しており、メンバーはそれぞれ最新の電子メール脅威に関するフィードバックをリアルタイムで Cloudmark サービスに提出しています。何らかのフィードバックがあった場合、Cloudmark 社では直ちに、その報告者に関する情報を収集し（報告者が必ずしも善意のメンバーとは限りません）、そのフィードバックを検討・分析します。報告者が信頼できる場合、そのフィードバックをもとに、ほぼリアルタイムでゲートウエイ（スパムフィルタリングの実行場所）の精度を向上させるように努めています。

誤分類メッセージを Cloudmark に提出していただくときの注意

- フィードバックは、エンドユーザー（CNFS ユーザー）からの誤分類メッセージに関するフィードバックでなければなりません。この要件が満たされることで、Cloudmark 社では、そのユーザー（報告者）に関する情報を調査できます（安全のため、この処理が必要です）。
- フィードバックは、誤分類メッセージが電子メールに添付された形で提出されなければなりません（誤分類メッセージは、message/rfc822 MIME アタッチメントでなければなりません）。この状態で、Cloudmark 社でメッセージをオリジナルの形式（ゲートウエイでメッセージがスキャンされたときの形式）で取得し、分析することができます。

フィードバックは、次のいずれかのアドレスに送信してください。メッセージは、偽陽性（スパムでないのにスパムと判定されるメッセージ）、偽陰性（スパムなのにスパムと判定されなかったメッセージ）、フィッシング偽陰性によってフィードバックの提出先が異なります。

communigate-legit@feedback.cloudmark.com – 偽陽性
communigate-spam@feedback.cloudmark.com – 偽陰性
communigate-phishing@feedback.cloudmark.com – フィッシング偽陰性

フィードバック（電子メール）に添付されている誤分類メッセージが RFC822 アタッチメントでなかった場合、その電子メールは Cloudmark サービスには転送されません。ただし、統計分析のため調査を行います。

Microsoft Outlook を使ってフィードバックを送信する方法：

1. Outlook を起動します。
2. ツールバーの［新規作成］ボタンをクリックします。または、［ファイル］－［新規作成］－［メッセージ］を選択します。
3. 誤分類メッセージをメッセージウィンドウにドラッグして、または、［挿入］メニューの［アイテム］オプションを使って添付します。
4. メッセージ（誤分類メッセージが添付されたメッセージ）をフィードバックの提出先アドレス（上記を参照）に送信します。

CommuniGate Pro の Web メールインターフェイスを使ってフィードバックを提出する方法

1. リストに表示されているメッセージのうち、誤分類メッセージを選択して開きます。メッセージは別のウィンドウに表示されます。
2. [Forward]リンク(またはスキンにアイコンがあれば、そのアイコン)をクリックした後、フィードバックの電子メールを作成します(誤分類メッセージを添付します)。
3. "To:"フィールドにフィードバックの提出先アドレス(上記を参照)に送信します。
4. [Send]ボタン(またはアイコン)をクリックしてメッセージを送信します。