インターネット
セキュリティ
電子メール

❶情報漏えいやスパムを遮断
❷負荷分散で処理能力の低下を防ぐ

メール・フィルタリング活用法

情報漏えいやスパムを遮断

メール・フィルタリングは，企業がやり取りする膨大な数のメールを監視するソフトウエアです。機密情報の社外への漏えいを防止したり，スパム・メールやウイルス感染などから社内ネットワークを守ります。今回は，このメール・フィルタリングの機能や仕組み，利用方法を解説します。

（本文中☞の付いた用語は欄外で解説）

宮 紀雄 | インフォサイエンス社長

スパム・メール
spam mail。受信者の意図に関係なく届く広告や勧誘などの電子メール。第三者のメール・サーバーを踏み台にして送信元を隠す手口が一般化している。この場合，送信者の特定は困難である。社会問題化するスパム・メールに対処するため，米国では，反スパム法案が米下院商業委員会を通過。2000年夏にも，下院本会議で票決される見通しとなった。

企業の情報化とネットワーク化により，電子メールは企業間の情報交換の重要な手段として定着してきました。これに伴い，社内の機密情報を外部に漏らすなどの不正行為の危険が以前よりも増加しています。話の内容が他人の耳に触れる機会の多い電話や，一般に部署に1台ずつしかないFAXとは異なり，電子メールは他人の目にまったく触れずに，情報のやり取りが可能だからです。

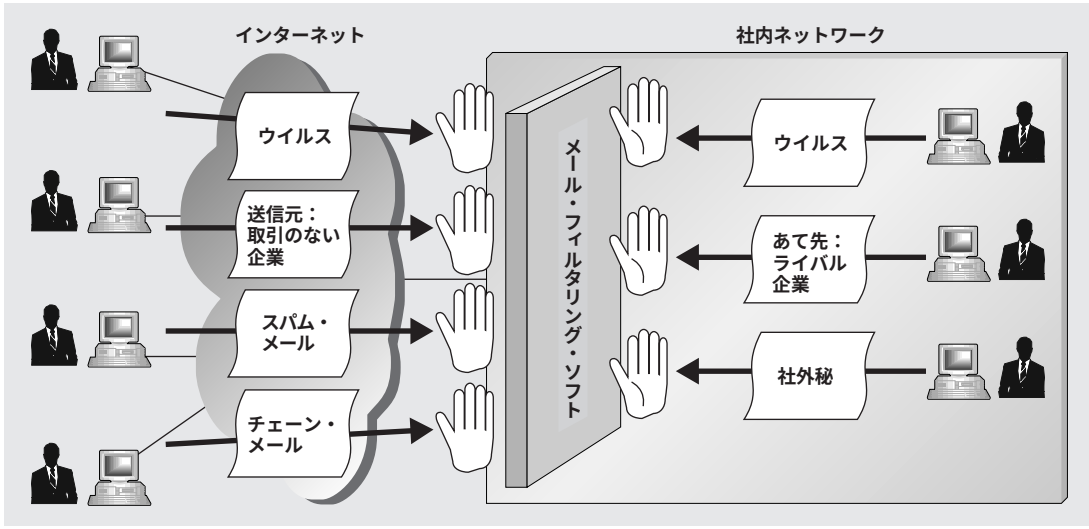
また，無作為に大量のメールを送信してくる☞スパム・メールや，コンピュータ・ウイルスに感染したメールも，企業にとっては大きな脅威です。メールが重要な連絡手段になるにつれ，スパム・メールやウイルスによるメール・システムの停止が，業務に重大な影響を及ぼす可能性が高くなってきています。

こうしたメールに関する様々な問題を解決するために登場したのが，メールの内容をリアルタイムに監視するサーバー用ソフトウエアのメール・フィルタリング・ソフト（以下メール・フィルタ）です（**表1**）。メールの本文やヘッダー，添付ファイルの中身を検査し，不正なメールの送信を中止したり，システム管理者に転送して問題に対処します。

表1　主なメール・フィルタリング・ソフト

製品名	Spamghetti	MIMEsweeper for SMTP Ver4.1J	MailGuardian/Wall Version 2.0	WorldSecure Server	InterScan eManager
開発元	インフォサイエンス	英コンテント･テクノロジー	住友金属システム開発	米タンブルウィード・コミュニケーションズ	米トレンド・マイクロ
販売元	インフォサイエンス ☎03-5463-1586	フォーバルクリエーティブ ☎03-5466-3560，シー・エス・イー ☎03-3463-5633	住友金属システム開発 ☎03-5815-7270	アイフォー ☎03-5436-7858	トレンドマイクロ ☎03-5334-3650
価格	48万円～	50万円～	120万円～	49万8000円～	95万円
主な特徴	システム管理者以外に，エンドユーザー自身によるポリシーの設定が可能	ポリシー設定をツリー構造で一覧できる専用ソフトを付属	機密情報の漏えい防止に機能を絞った製品。社内ユーザーの権限を設定できる	S/MIMEによるメールの暗号化とディジタル署名に対応	ワクチン・ソフト「InterScan VirusWall」上のプラグイン

図1　メール・フィルタの機能　フィルタリング・ソフトでキーワードやアドレスなどを指定し，①メールによる社内の機密情報の流出，②業務と無関係なメールの受信，③取引のない企業とのメール交換――などを防ぐ。また，ワクチン・ソフトと連携してウイルスもチェックできる。



メールを常時監視し不正使用を防止

メールの内容を常に監視するメール・フィルタは，メール専用の☞ファイアウォールのようなものです。主な導入目的には，①社内の機密情報の社外への漏えい防止，②広告や勧誘などのスパム・メールの排除，③メールによるウイルス感染の防止――があります（図1）。

企業がメール・フィルタを導入する大きな目的の一つは，社内の機密情報が電子メールによって外部に漏れることを防ぐことです。例えば，社内から社外へ送るメールの本文が「社外秘」などといった文字列を含んでいた場合に，該当するメールを外部に送信できないようにしたり，システム管理者に転送したりします。また，社外からのメールについても，広告や勧誘など業務に不要なスパム・メールを社内のユーザーが受信する前に破棄できます。

メール・フィルタが監視できるのは，メールの本文だけではありません。メールに添付された☞Word，一太郎，Excel，PowerPointなどの特定のアプリケーション・ファイルの中身も検査できます。また，一定の容量を超えたサイズのメールや添付ファイルの受信を拒否するといった使い方も可能です。

ワクチン・ソフトとの連携機能も

また多くのメール・フィルタは，☞ワクチン・ソフトとの連携機能を持っています。メール・フィルタが添付ファイルを検査すると同時にワクチン・ソフトのウイルス検出機能が働きます。メールを媒体としたウイルスの流入を防ぐとともに，誤って外部の取引先などにウイルスを送信してしまう事故を防げます。

ウイルスに感染した添付ファイルを発見した際には，添付ファイルを削除して本文だけを送受信したり，ウイルスを除去して正常な添付ファイルに修復して送受信することもできます。

また，ワクチン・ソフトとの連携機能を利用せずに，メール・フィルタだけの機能でも，ウ

ファイアウォール
社内ネットワークとインターネットなどの外部ネットワークとの境界線に設置するセキュリティ・システム。外部からのアクセスを制限することで，内部のセキュリティを高める。

Word，一太郎，Excel，PowerPoint
Word，Excel，PowerPointは米マイクロソフトの製品で，それぞれ日本語ワープロ・ソフト，表計算ソフト，プレゼンテーション作成ソフト。一太郎はジャストシステムの日本語ワープロ・ソフト。

ワクチン・ソフト
コンピュータ内のファイルがウイルスに汚染されていないかを検査・除去するソフトウエア。アンチウイルス・ソフトとも言う。個々のクライアント・パソコンに常駐させるものと部門サーバーやメール・サーバーなどに常駐させるものがある。

ラブ・ウイルス
メールを使って自己増殖を繰り返すウイルスで，2000年5月に発見された。「I LOVE YOU」のタイトルで送信されてくる。添付ファイルを実行するとウイルスを複製し，アドレス帳に登録した全ユーザーあてに同じウイルスを送信する。このため，短期間で世界各国に被害が拡大した。

DNS
domain name system。ビット列であるIPアドレスを，人間が覚えやすいアルファベットの文字列に対応付けるための分散型オンライン・データベース・システム。

SMTP
simple mail transfer protocol。インターネット上で電子メールを送受信するためのプロトコル。メール・サーバー同士または，メール・クライアントからメール・サーバーへの送信時に使う。

イルスの感染を防げる場合があります。例えば，2000年5月に猛威を振るった「☞ラブ・ウイルス」は，メールのタイトルが「I LOVE YOU」でした。こうした特定の文字列をタイトルに含むメールの送受信を停止することで，ある程度は，ウイルスの流入や流出を防げます。

既存システムには事前の設定変更が必要

メール・フィルタには，メールの内容を監視するフィルタリング機能と，メールを社内外のメール・サーバーにリレー（中継）する機能の二つがあります。導入時には，☞DNSサーバーや社内メール・サーバーの設定変更が必要です。

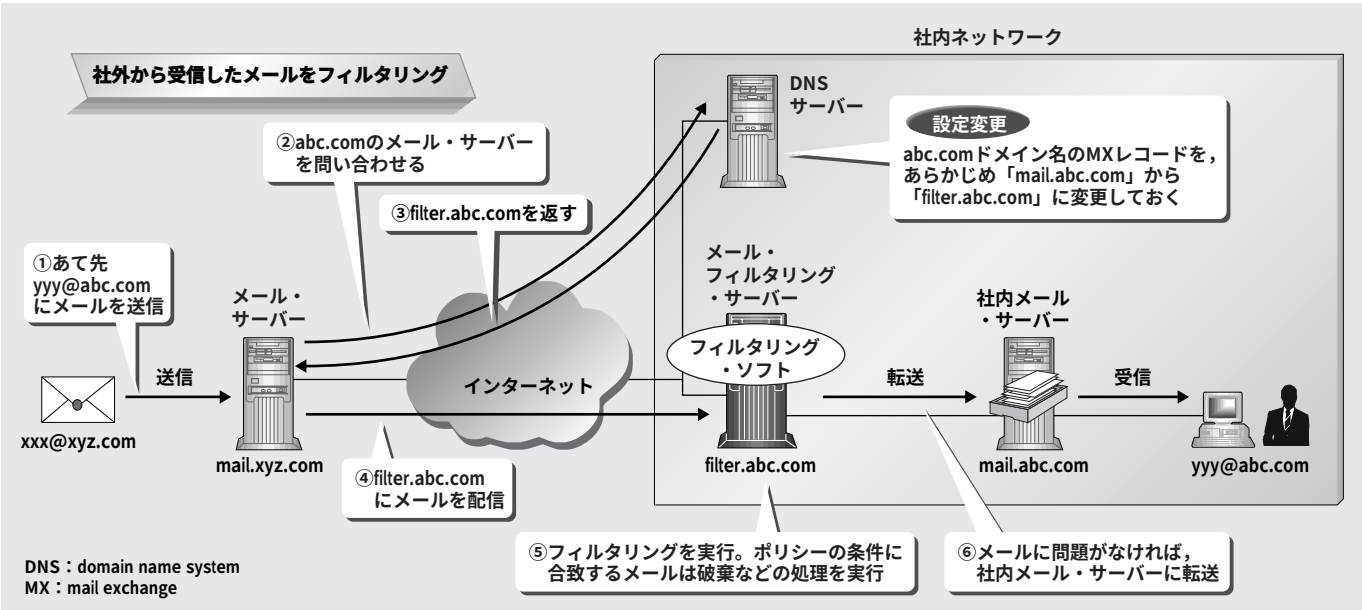
メール・フィルタが動作するメール・フィルタリング・サーバーは，社外のメール・サーバーと社内のメール・サーバーの間に設置します。二つのメール・サーバー間の☞SMTP通信を中継する際にフィルタリングを実行し，問題のないメールだけを，あて先のメール・サーバーに中継する仕組みとなっています。

メール受信にはDNSの設定を変更

社外のメール・サーバーからメールを受信する際には，受信前にメール・フィルタリング・サーバーを経由する必要があります。外部のネットワークからは，メール・フィルタリング・サーバーが社内のメール・サーバーとして認識されなければなりません。このため，社内のDNSサーバーの設定変更が必要になります。

具体的には，DNSサーバーの設定項目の一つである☞MXレコードに，メール・フィルタリング・サーバーのホスト名を登録します。MXレコードを書き換えることで，従来のメール・サーバーではなく，メール・フィルタリング・サーバーのIPアドレスをインターネット上に送

図2　メール・フィルタリングの仕組み（メール受信時）　社外から受信したメールは，メール・フィルタリング・サーバーを経由して，社内のメール・サーバーに転送される。フィルタリング・ソフトを導入するためには，DNS（domain name system）サーバーのMX（mail exchange）レコードを，メール・フィルタリング・サーバーのドメイン名に変更する必要がある。



出します。社外のメール・サーバーは，このIPアドレスに向けてメールを送信します（**図2**）。

メールを受信したメール・フィルタリング・サーバーは，あらかじめ設定した条件に基づいてメールの検査を実施します。そして，問題がないメールだけを本来の社内メール・サーバーに転送します。

送信時にはメール・サーバーの転送機能を利用

一方，社内から社外にメールを送信する場合は，送信するすべてのメールの内容をメール・フィルタで検査しなければなりません。このため，送信すべきメールをいったんメール・フィルタリング・サーバーに転送するように，メール・サーバーに設定します（**図3**）。メール・フィルタは，検査結果に問題がなければ，それぞれのメールのあて先にメールを送信します。

各エンドユーザーがメール・クライアント・ソフトに設定してあるメール・サーバー名を変更する必要はありません。

複数の条件設定で確実に不正メールを発見

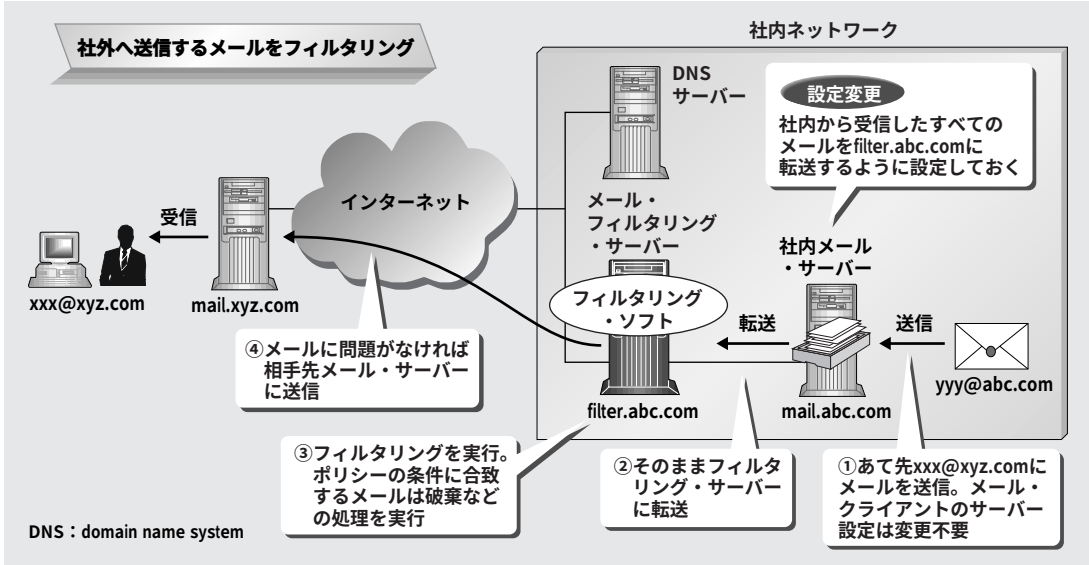
メール・フィルタは，あらかじめ設定した「条件」に合致したメールを発見した場合に，そのメールを，あらかじめ設定した「アクション」に基づいて処理します。こうして，送受信メールに問題がないかどうかを検査します。多くのメール・フィルタは，この条件とアクションの組み合わせを「ポリシー」と呼んでいます。

製品によって異なりますが，ユーザーはかなり複雑なポリシーを設定できます。複数のポリシーがある場合には，それぞれの優先度を設定し，各ポリシーを処理する順番をあらかじめ決めておきます（p.152の**図4**，**写真1**）。複数のポリシーをうまく組み合わせれば，不正なメールをより確実に発見できます。

ポリシーの条件設定には，メールの本文やヘッダー情報に対するキーワードや，送信元/あて先のメール・アドレスを指定できます。指定できるキーワードやアドレスの数は製品によって様々ですが，複数のキーワードやアドレスを

MXレコード
MXはmail exchangeの略。DNSサーバーに設定する項目の一つ。DNSサーバーで管理するドメイン名あての電子メールを処理するメール・サーバー名を指定する。

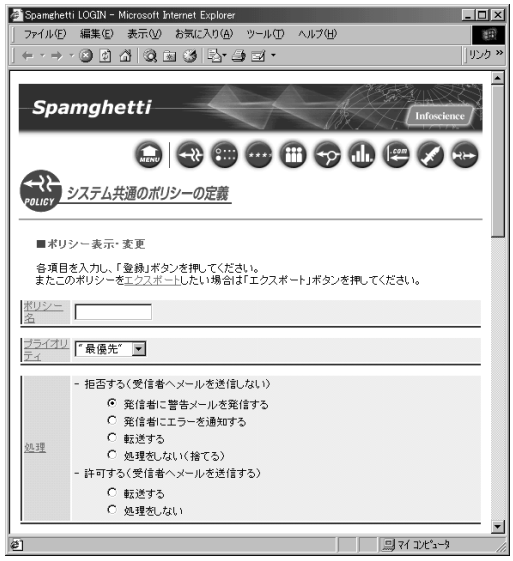
図3　メール・フィルタリングの仕組み（メール送信時）　社内から送信するメールは，社内のメール・サーバーを経由して，メール・フィルタリング・サーバーに転送される。社内メール・サーバーの転送先を固定的にメール・フィルタリング・サーバーに設定する。クライアントのメール・ソフトの設定変更は必要ない。



論理演算子
　一つまたはそれ以上の項目の関係を表す記号や単語。AND（～かつ～），OR（～または～）など。

正規表現
　「^」，「$」，「+」などの文字を使って特別な文字列を表現する方法。UNIXなどのコマンドでファイル中の文字列を検索するキーワード指定に利用される。例えば，「^」は「行頭」を意味する。「^至急」と指定すれば，行頭に「至急」がある文字列を検索できる。

写真1　インフォサイエンスの「Spamghetti」のポリシー設定画面



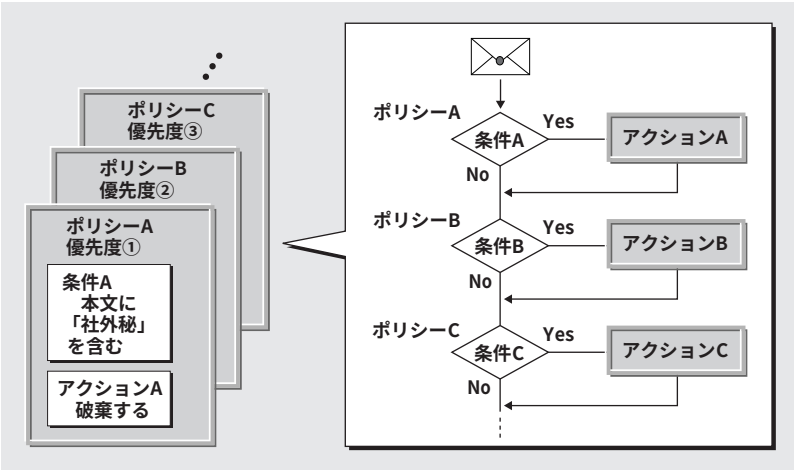
指定できる場合は「AND」や「OR」の☞論理演算子を使用します。また，☞正規表現を利用したキーワード指定が可能な製品もあります。

　ポリシーのアクションには，その条件に合致したメールを発見した場合のメール・フィルタの処理方法を記述します。一般には，メールの破棄，受信拒否，システム管理者への転送――などを指定します。

　ポリシーの条件に「重み付け」と「しきい値」を指定できる場合もあります。例えば，「本文中にある『金もうけ』を6点，『副業』を3点，『利殖』を1点の重み付けで，しきい値を10点」などのように設定します。アクションを「受信拒否」にすれば，三つの語句すべてがメールの本文にある場合に累積点数が10点となり，メールの受信を拒否します。しかし二つ以下であれば受け取ります。

　これはスパム・メールの排除などに有効です。スパムに使われそうな語句の重み付けを重くし，スパムと業務の両方で使われそうな語句を軽くすれば，業務で送られてきたメールをスパムと間違える可能性を低くできます。

図4　ポリシーの構成　フィルタの基となるポリシーは，条件とアクションで構成する。設定した条件に合致する場合に，アクションが実行される。ポリシーが複数個ある場合は，各ポリシーの優先度を設定して，条件検査の優先順位付けをする。ただし，アクションに破棄やシステム管理者への転送などを指定した場合は，次の条件検査には進まない。

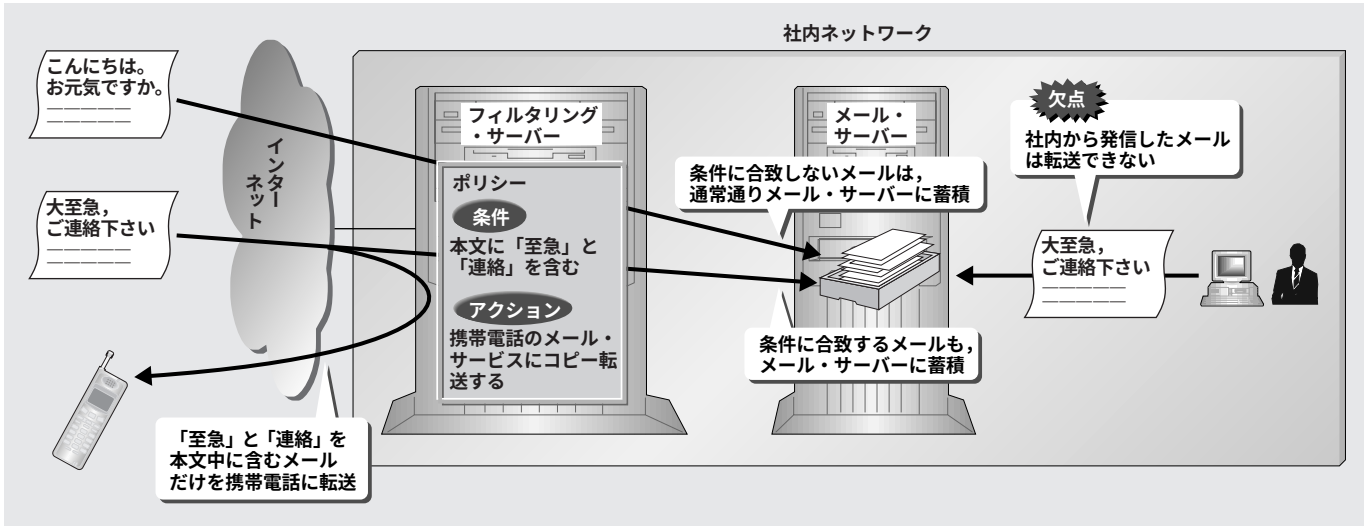


メールの転送制御などに応用する

メール・フィルタの基本機能は，問題のあるメールを発見して処理することですが，その機能を様々なメール処理に応用できます。①メールの内容による自動転送や自動振り分け，②外部アプリケーションとのアクション連携――などが挙げられます。

　メール・フィルタのポリシーは，原則としてシステム管理者が設定します。すべてのメールを監視し，不正なメールを発見するためです。ただし全体のポリシーとは別に，エンドユーザーが個々のユーザーごとのポリシーを設定できる製品もあります。この場合は，システム管理者が設定するような不正メールの発見だけではなく，送られてくるメールの流れを自由自在に制御する用途に利用できます。

図5　キーワードを指定したメールの転送制御に応用　ほとんどのメール・サーバーが標準で転送機能を備えるが，一般には受信したメールをすべて転送する方式である。メール・フィルタを利用すれば，指定したキーワードを含むメールだけを，指定したアドレス先に転送できる。ただし，社内からのメールに関しては転送制御できない。



「至急」メールだけを携帯電話に転送

例えば，社内のメール・サーバーに送信されてきたメールを携帯電話のメール・アドレスに転送するといった使い方があります（**図5**）。☞sendmailなどのメール・サーバーにも，メールの転送機能がありますが，原則として無条件にすべてのメールを転送します。このため，1日に何十通ものメールを受け取るユーザーが携帯電話にメールを転送すると，その処理が非常に煩雑になってしまいます。

メール・フィルタを使えば，必要なメールだけをフィルタリングして転送できます。例えば，「至急」，「連絡」といった緊急性を帯びた語句や，特定のプロジェクト名などをキーワードに指定すれば，緊急のメールだけを外出先でも読めるようにできます。さらに，携帯電話にメール転送する際は，添付ファイルを送らないようにも設定できます。

メール本文の内容に応じた振り分けにも利用できます。例えば，「info@ドメイン名」といった問い合わせメール・アドレスには，製品に対する質問だけでなく，故障時の対応や会社の業績に関する質問，苦情など様々な内容のメールが送られてきます。そこで，メール・フィルタを使って「資料請求」などの語句や製品名をキーワードにして転送先を振り分ければ，適切な担当者がより迅速にメールを処理できます。

外部アプリと連携してメールを自動翻訳

また製品によっては，フィルタリングの際に，「破棄」や「転送」といった決められたアクションだけではなく，外部のアプリケーションとの連携を指定できるものがあります。この連携機能によって，ある条件に合うメールだけを自由に加工できるようになります。

例としては，翻訳ソフトとの連携があります。送られてきたメールの内容が英文だった場合，メール・フィルタが翻訳ソフトと連携することで，日本語に翻訳したメールを作成できます。オリジナルの英文メールとは別に，この翻訳メールを配信すれば，社員が英文メールを処理する際の助けとなります。

sendmail
最も一般的に利用されているフリーのSMTPサーバー・ソフト。機能拡張を施した製品版「Sendmail Pro」もある。