SpamTitan Version.7

アンチスパム・ソリューション

製品のご案内

2021年11月15日 Rev 2.1

ジュピターテクノロジー

Email : info@jtc-i.co.jp　URL : http://www.jtc-i.co.jp

SPAMTITAN アンチスパムシリーズ

SPAM TITAN

SpamTitan は、アイルランドのTitanHQ社が開発を続けているSPAMメール除去フィルタリングシステムです。
日常業務で日々受信する、宣伝や広告を目的とした、本来必要のない迷惑メール（SPAMメール）を自動的に除去、一定期間保管します。

この SpamTitan システムは、WindowsやUnix系OSのソフトウエアとしてではなく、１つの完結したアプライアンスとして提供されます。
形態としては、ハードウエアアプライアンスと仮想環境で稼動する仮想アプライアンスとなります。
多数のノードでクラスタリングを構成でき、流量の多いメールストリームサイトにも柔軟に対応できます。

ネットワークにはプロキシ型の接続となるので、他のプロトコルやセッションを邪魔せず、また障害時にネットワークのサービスをブロックしてしまうこともありません。設置も撤去、移設も簡単で、他のデバイスに影響を与えません。

Webインターフェースは一般的なブラウザでアクセスでき、日本語表示にも対応しています。
管理者のほか、一般ユーザーにもインターフェースを展開することができ、それぞれのユーザーが検疫されたメールをリリースしたり、個人的なブラック/ホワイトリストを作成したり、レポートを受信したりすることができます。

ウイルス除去フィルタは著名な２系統が準備され、それぞれのライセンスはSpamTitanのライセンスに内包されるため、運用期間を通してこの２系統を使用する事ができます。

障害対応はメーカーサポートによるリモート接続で行ないます。

また、メーカーの開発スタンスとして、新技術トレンドへの対応が比較的柔軟でキャッチアップがすばやい傾向があります。

世界中で膨大なユーザーが利用しているため、世界標準と言っても過言ではありません。

製品ラインナップ

□Spam Titan Gateway（オンプレミス）

＊OS不要の仮想アプライアンス（ISOイメージ、VMwareイメージ）
＊ハードウエアアプライアンス（Blue Vault Spam Titan）
＊最小50ユーザー、最大無制限ユーザー
＊シングルノードシステム
＊複数ノードHAクラスタシステム（ノード追加可能）
＊1/2/3年契約　※

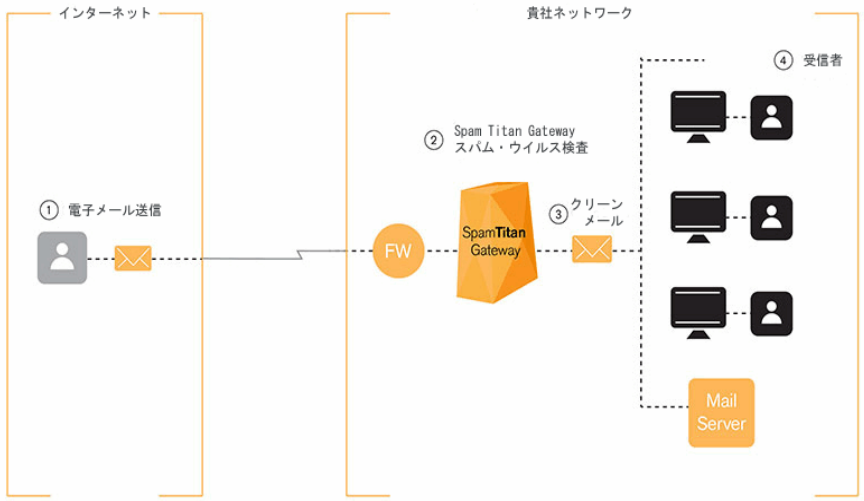
□Spam Titan Private Cloud（クラウドサービス）
（オンプレミスと機能同等）

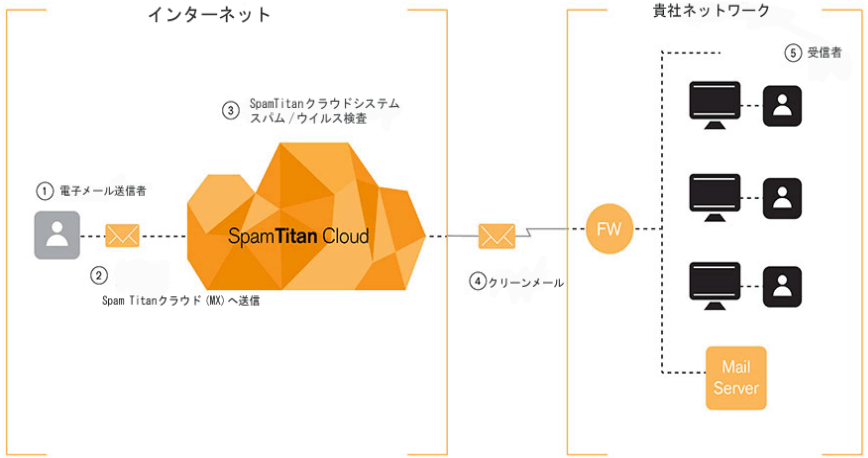
＊運用開始まで数分
＊OS、ハードウエア、ソフトウエア不要
＊専用クラウドサービス（複数ノードHAクラスタ）
＊最小1000ユーザー、最大無制限ユーザー
＊1/2/3年契約　※

□Spam Titan Cloud（共有クラウドサービス）

＊運用開始まで数分
＊OS、ハードウエア、ソフトウエア不要
＊共用クラウドサービス/設定項目限定版
＊最小50ユーザー、最大5000ユーザー
＊1/2/3年契約　※

※契約期間4年以上をご希望の場合はご相談ください。



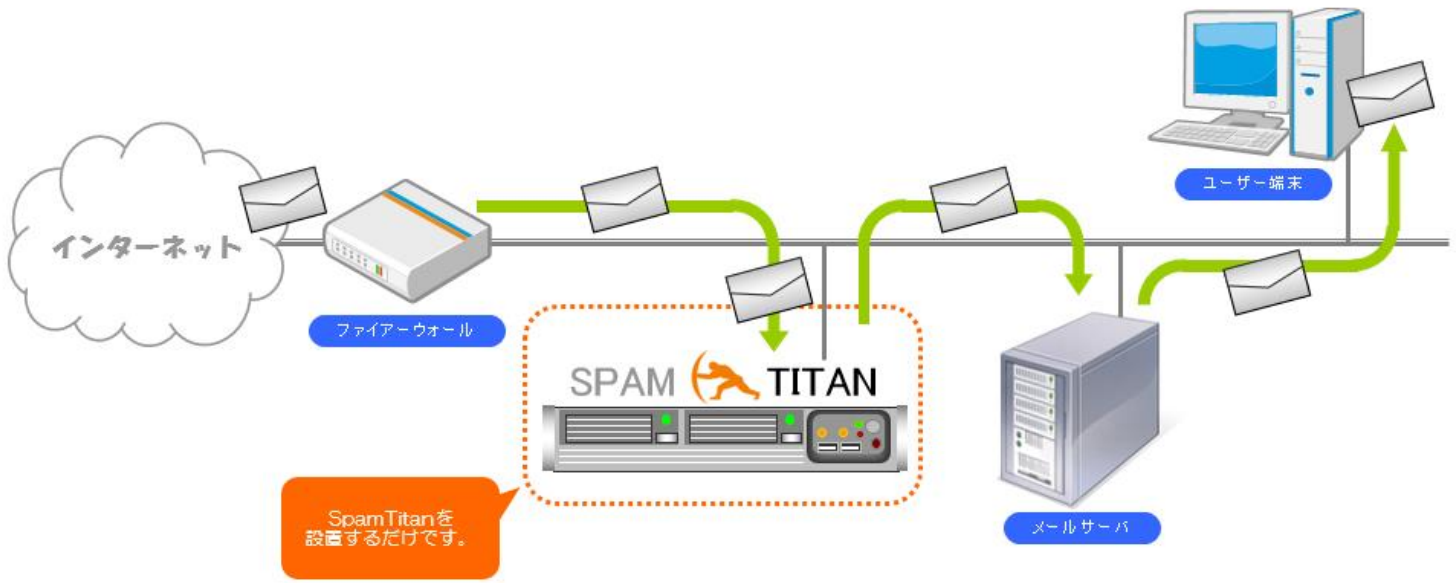


設置はプロキシ型。

SpamTitanはプロキシ型でネットワークに接続するので、既存のネットワークへの導入負荷が低く、
また、障害が発生してサービスが停止しても他のプロトコルやサービスが停止することはありません。

SpamTitanはSpamフィルタリングに特化しているため、メールボックス機能はありません。
メールボックスを持つメールサーバーの前段に位置するように設置します。
前段であれば、SpamTitanはDMZや社内ネットワークの内側、外側など、どこに設置しても構いません。

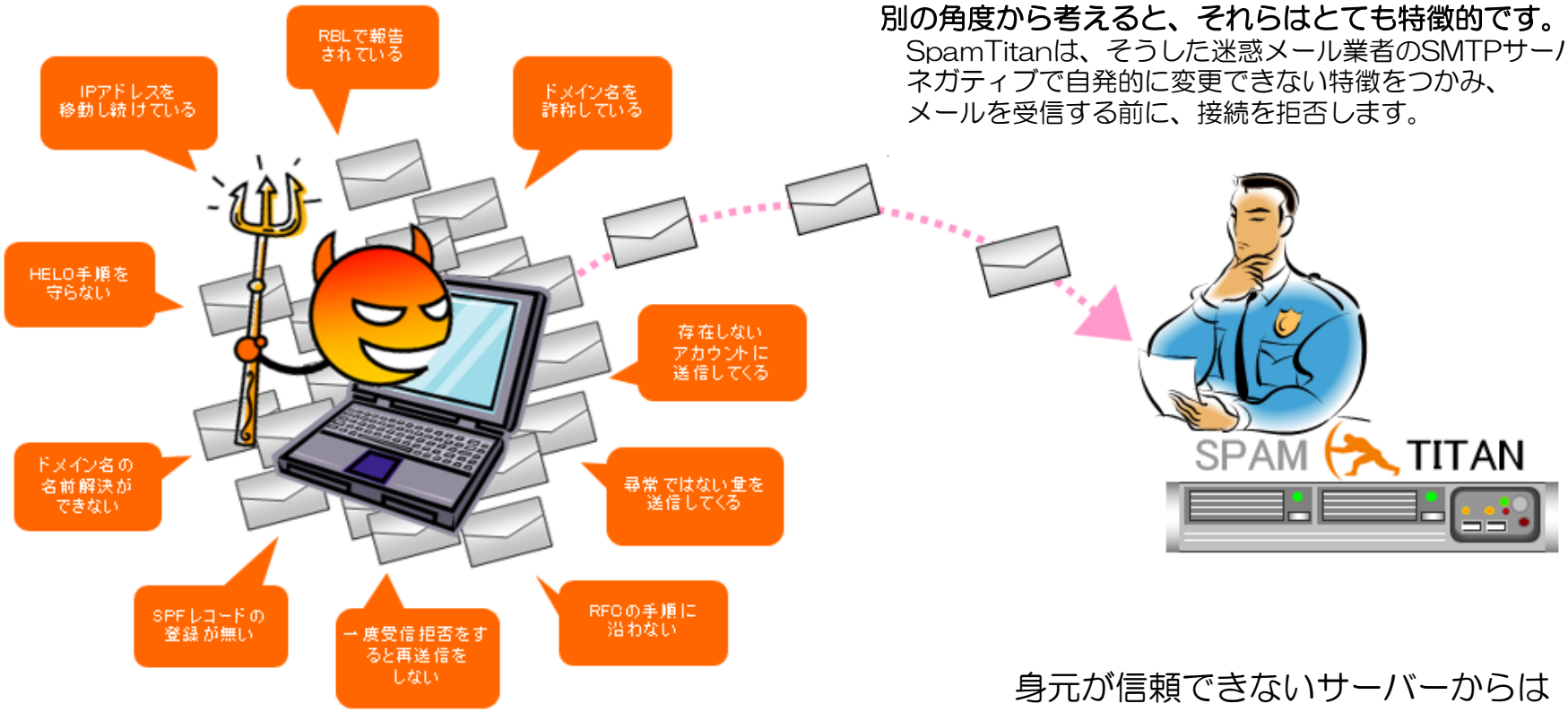
そしてもちろん、送信メールの検査も行うことができます。（共有クラウド省く）



受け取らない作戦。

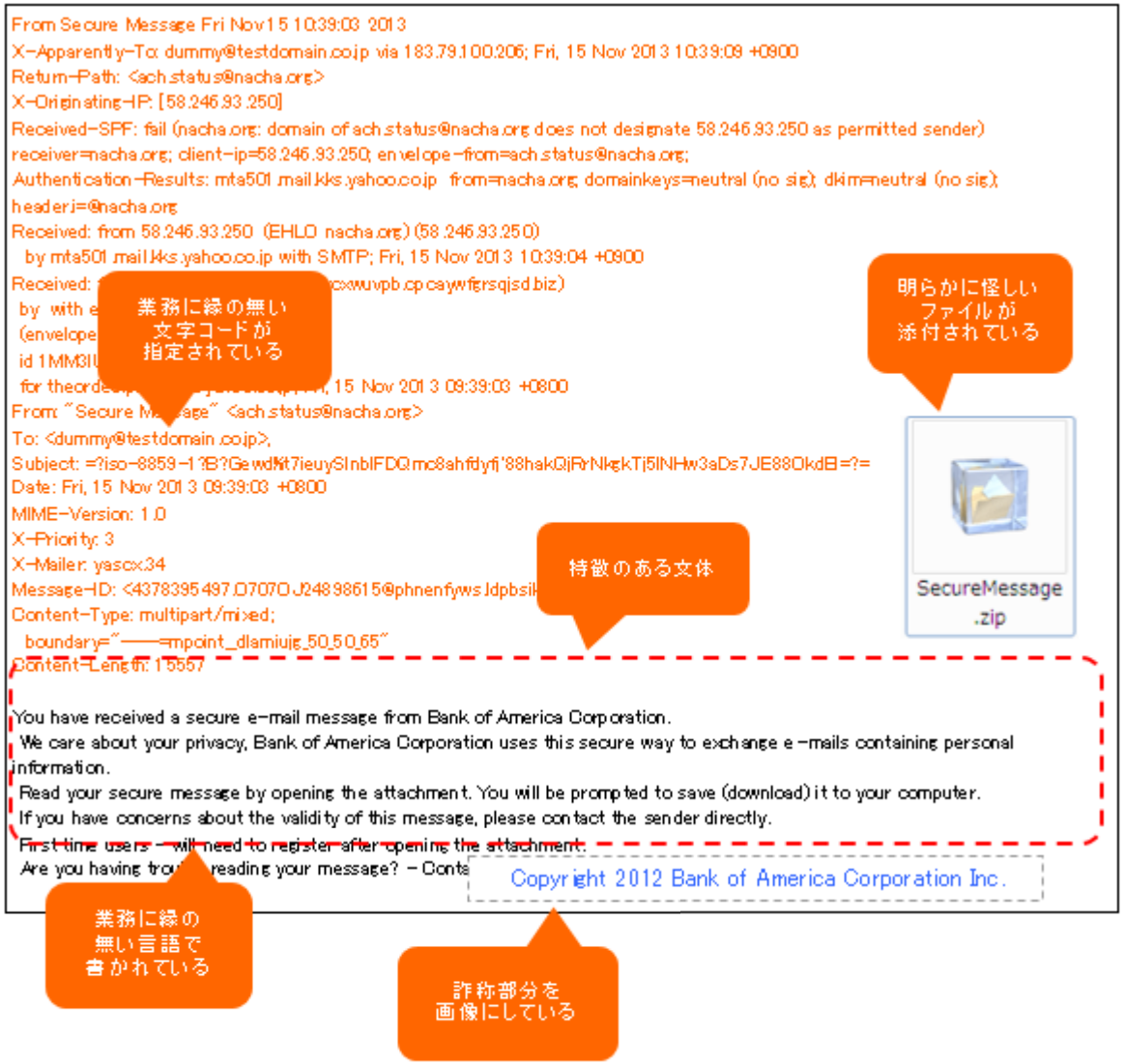
迷惑メール送信業者が使うSMTPサーバーには、特徴があります。
迷惑メール対策を取りにくくするためだったり、
身元を判らなくするような仕掛けだったり、
膨大な量をこなすための合理化だったり。

別の角度から考えると、それらはとても特徴的です。
SpamTitanは、そうした迷惑メール業者のSMTPサーバーの
ネガティブで自発的に変更できない特徴をつかみ、
メールを受信する前に、接続を拒否します。



身元が信頼できないサーバーからは
そもそもメールを受け取らない。

これが SpamTitan の作戦です。



迷惑メールからは、いろいろな情報を取得できます。
使われている文字コード、
使われている言語、
半角スペースで単語を区切っている、
件名を改行している、
特徴的な単語を繰り返している、
本文に問題のあるURLのリンクがある、など。

すでに世界のどこかで受信された迷惑メールは、
ボランティアの協力や、自動化されたシステムにより
迷惑メールそのものや、あるいは特徴を抽出されて
パターン化されたものが全世界で公開されています。
SpamTitanはこれらの情報を上手に利用します。

特に迷惑メールの作者の癖が
文章構成という形で特徴抽出できます。

SpamTitan は、こうしたメールのヘッダや本文の他、
送信に使用したOSの特徴などを判定に利用します。

迷惑メールの特徴を抽出して
世界のデータベースと突き合わせる。

これが SpamTitan の作戦です。

特徴を抽出する作戦。

SPAM TITAN

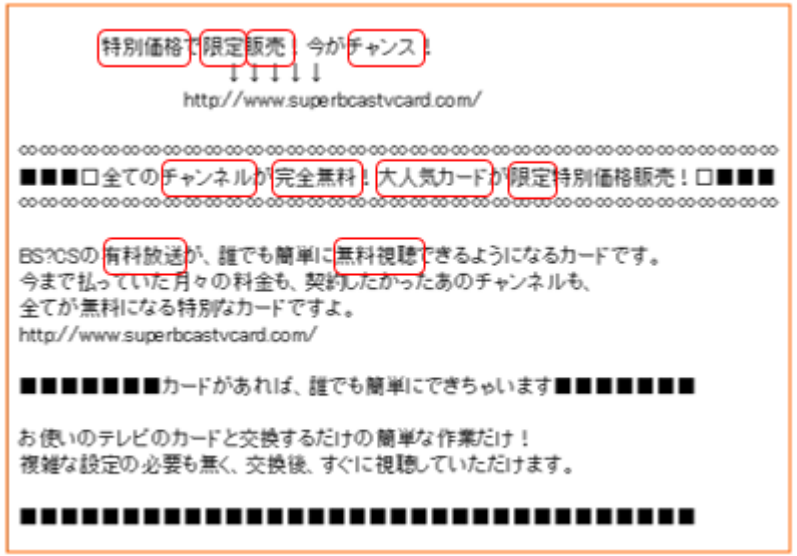
石油化学や医薬品を事業とする場合、送受信するメールに「バーゲン」や「特売セール」という言葉が現れることは稀でしょう。
一方、アパレル小売事業の場合、この言葉は頻繁に出現するでしょう。

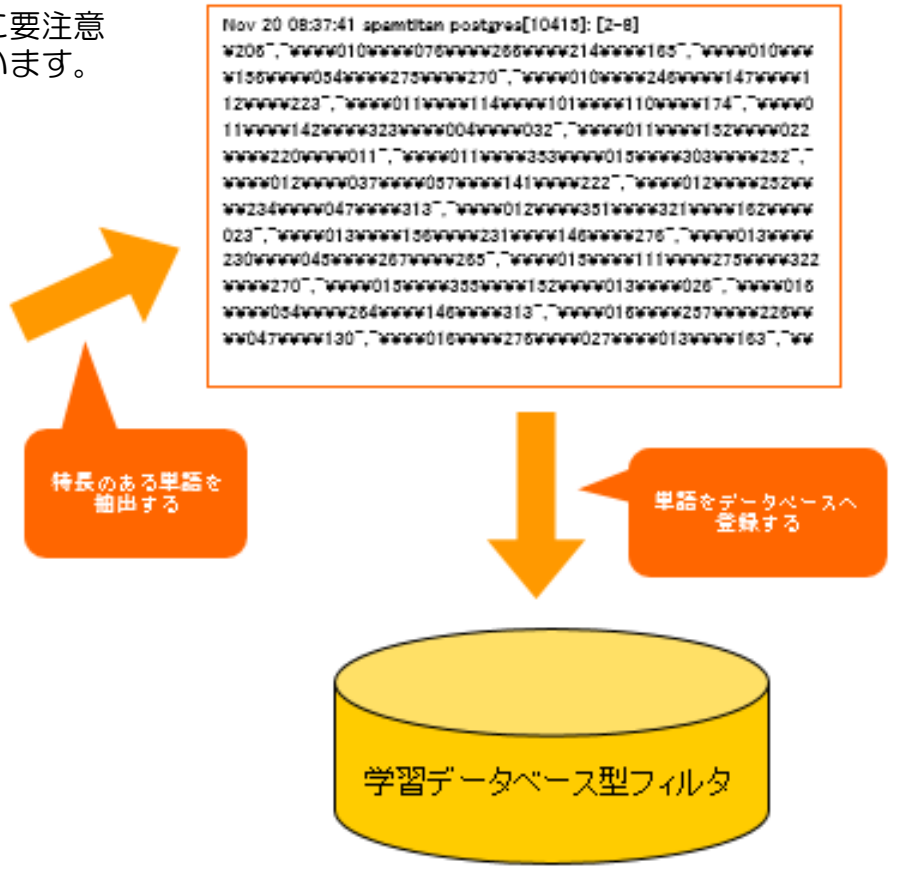
業種によって日常的に使われる言葉に特徴があります。
SpamTitanは迷惑メールと判断されたメールの特徴的な単語を抽出してデータベースに登録します。
その業種で迷惑メールと判断されたメールに出現する単語は、徐々に要注意単語として浮かび上がり、その単語を使ってフィルタリングを行ないます。

学習型フィルタを長く使って育てる。

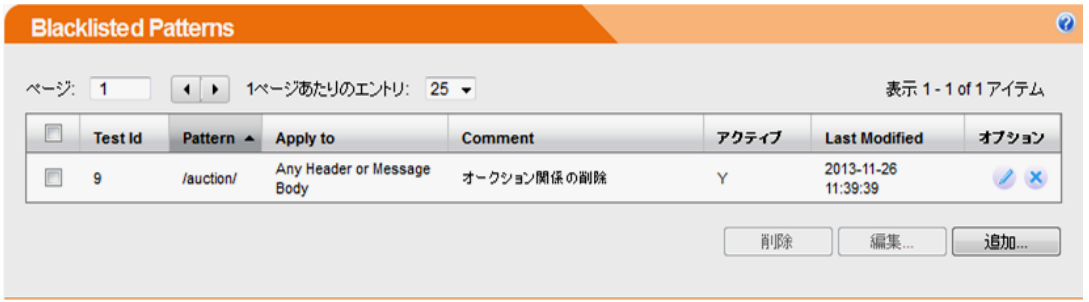
これが SpamTitan の作戦です。

育てる作戦。





日本語は西洋のアルファベットによる言語と違って単語をスペースで区切らないため、単語パターンマッチングはマシンパワーを必要とする上、単語同士の接続による誤検出が発生しがちです。
SpamTitanにもキーワードフィルタが用意されていますが、このフィルタが使用できる文字コードはUTF-8に限定されます。



全世界で流通するメールで使用されているUTF-8の普及率は５割を超えたところと言われており、日本ではiso-2022-jpの使用が主流であって、UTF-8は９割のメールクライアントがサポートしているだけという状況に過ぎません。
一方、SpamTitanは、キーワードフィルタリングを必要とせず、無くても十分な性能を発揮するように設計されています。

SpamTitanのこのキーワードフィルタリング機能、実は ダメ押しの機能 なのです。
誤検疫されたり、検出できずに抜けてくる迷惑メールのヘッダや本文のシグネチャなどをピンポイントで指定する奥の手として用意されています。

このキーワードフィルタリング機能は正規表現が可能であり、メールのソースのどの部分も指定可能であるため、たとえば、あまり使われないヘッダフィールドやリレーされた途中のIPアドレス、アルファベットのシグネチャなど、さまざまな部分を狙うことができます。

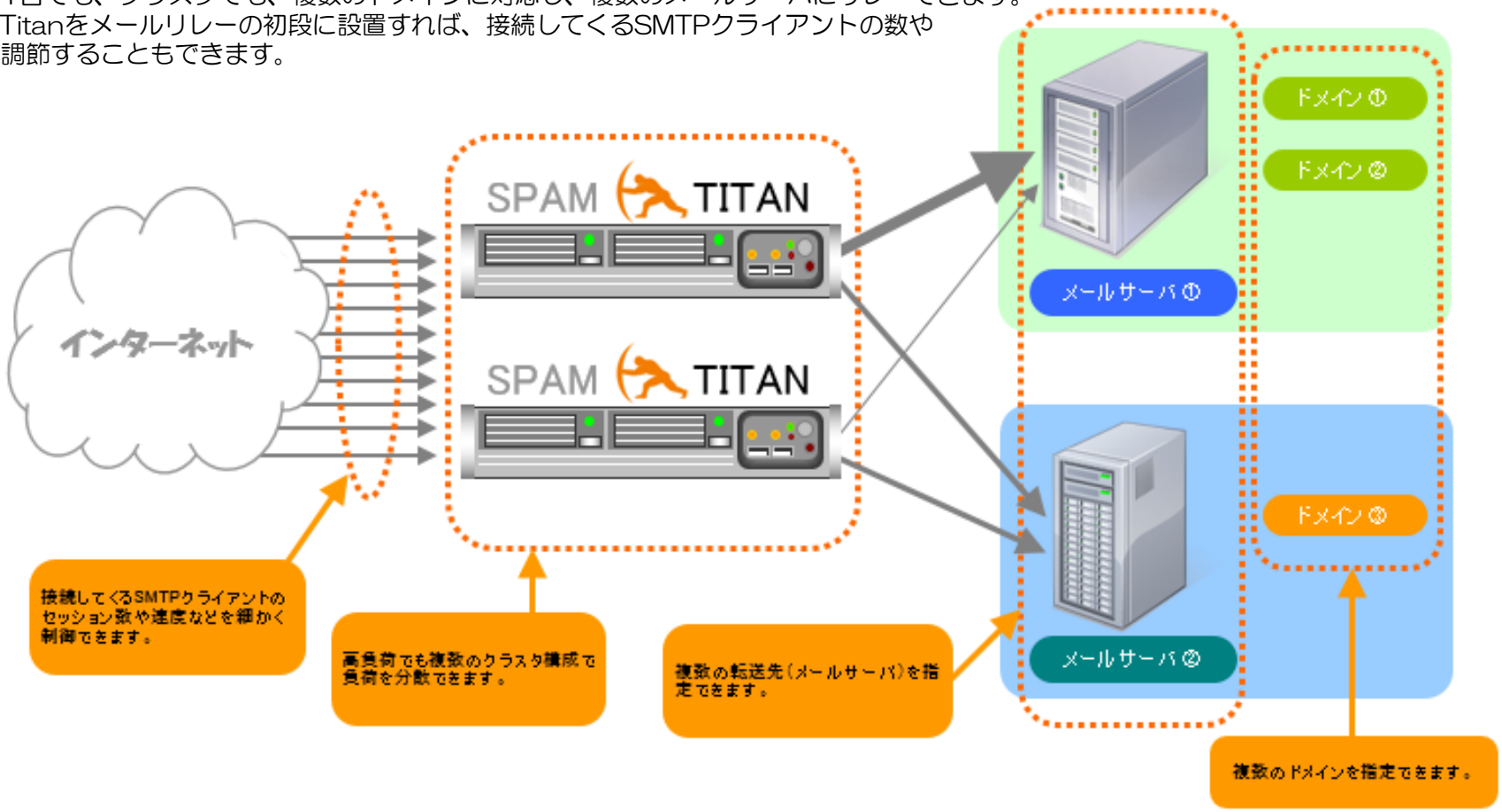
重要な取引先から、営業的なメールマガジンが発行されてくる場合、社会的にそのメールマガジンが迷惑メールだと判断されると、SpamTitanもそのトレンドに影響されますが、キーワードフィルタリング機能を使用すれば、取引先からの連絡を通過させることができるでしょう。

キーワードフィルタリングは、慣れた管理者にとっては定番かもしれません。

キーワードフィルタ、あります。

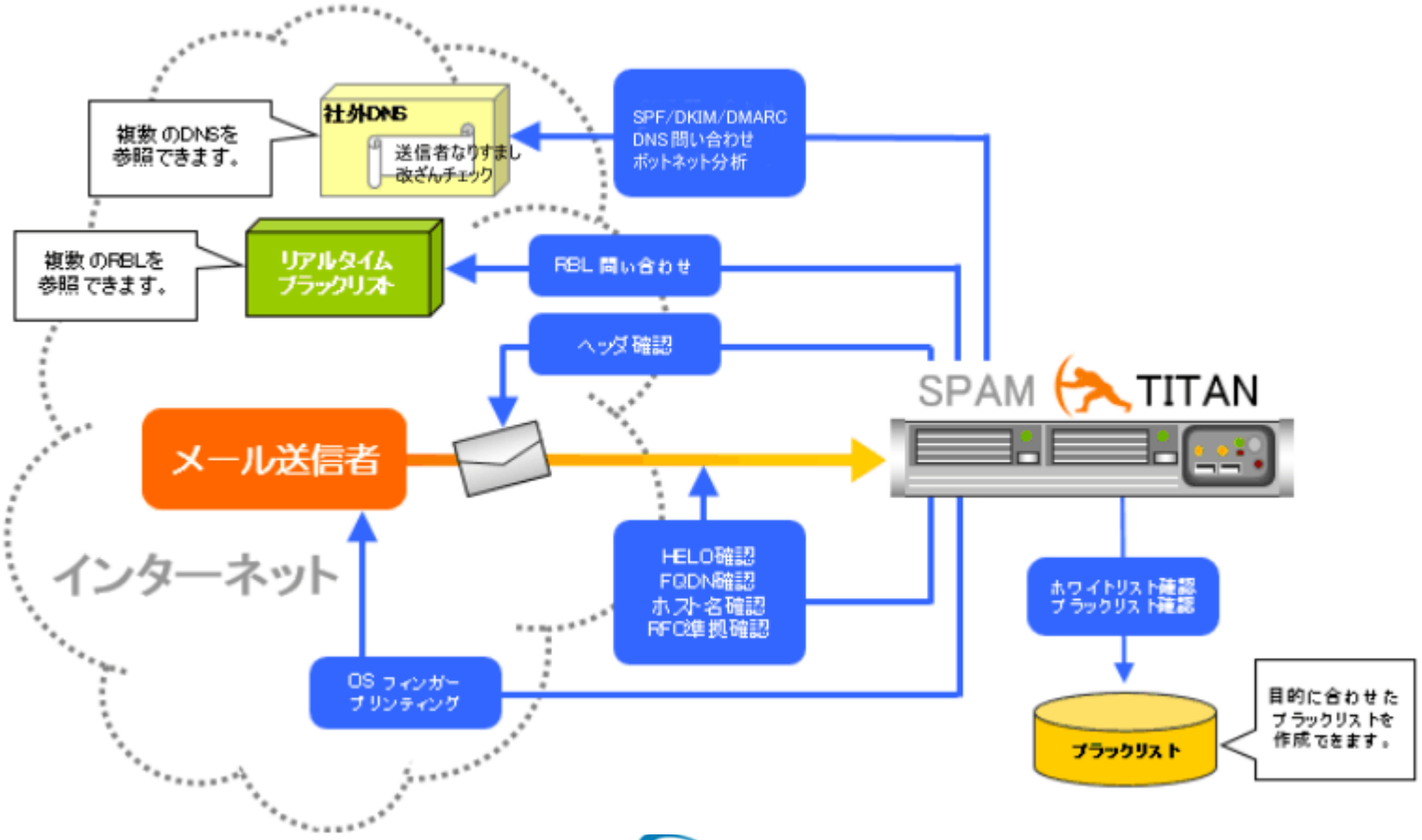
機能概略　ネットワーク機能

SpamTitanは高負荷メールストリームに先進的な対応が可能です。
SpamTitanは、複数のユニットでクラスタを組むことで、高負荷状況のメール送受信に対応できます。
また、1台でも、クラスタでも、複数のドメインに対応し、複数のメールサーバにリレーできます。
SpamTitanをメールリレーの初段に設置すれば、接続してくるSMTPクライアントの数や
速度を調節することもできます。



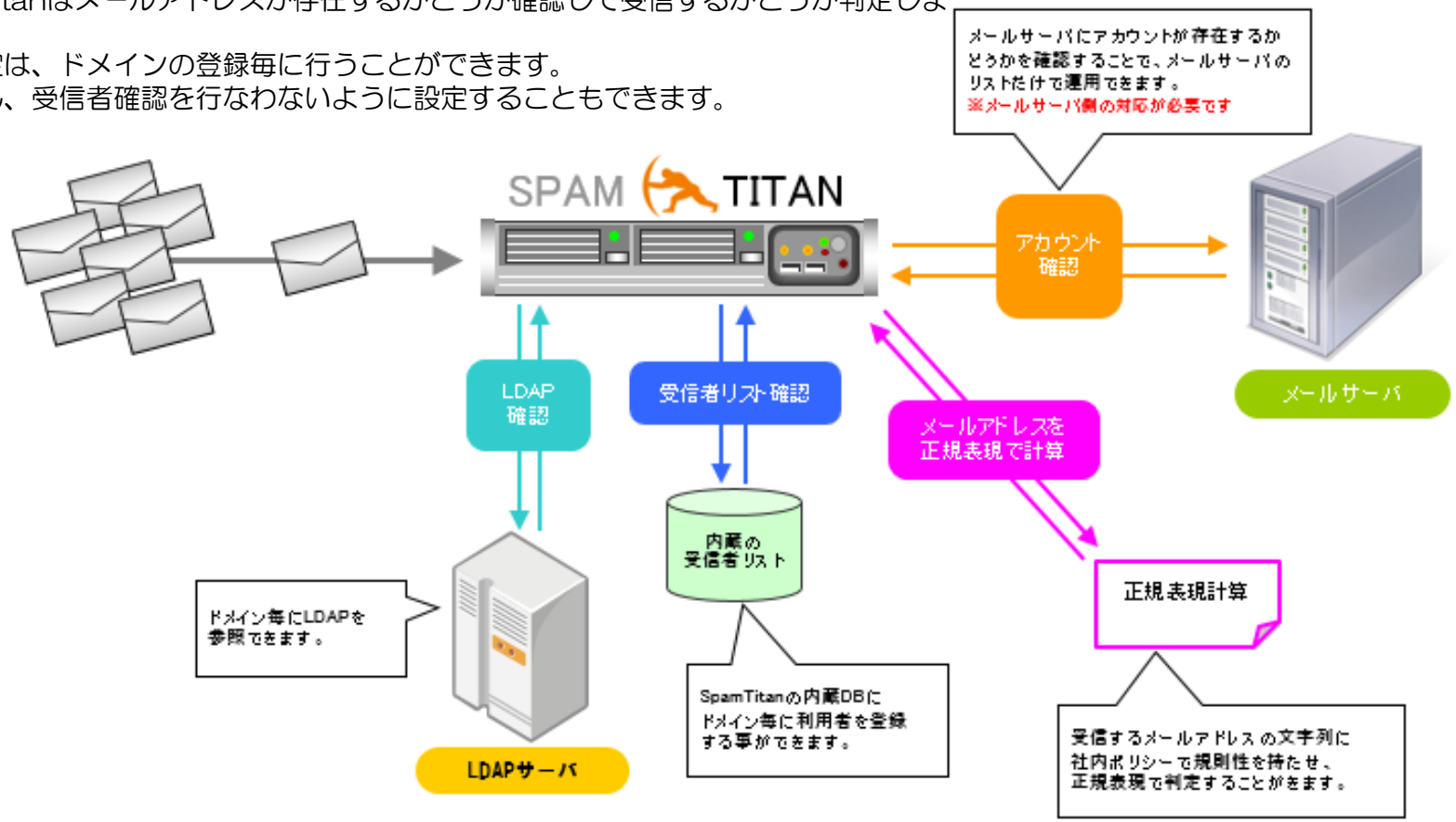
機能概略　メール送信サーバーの確認

SpamTitanは、さまざまな手段でメール送信者の身元確認を行ないます。
メールを送信するメールサーバーについて、インターネット上の評判やサーバー設置の正規性を参照してスパムを送信するメールサーバーかどうかを判断します。



機能概略　メール受信者の確認

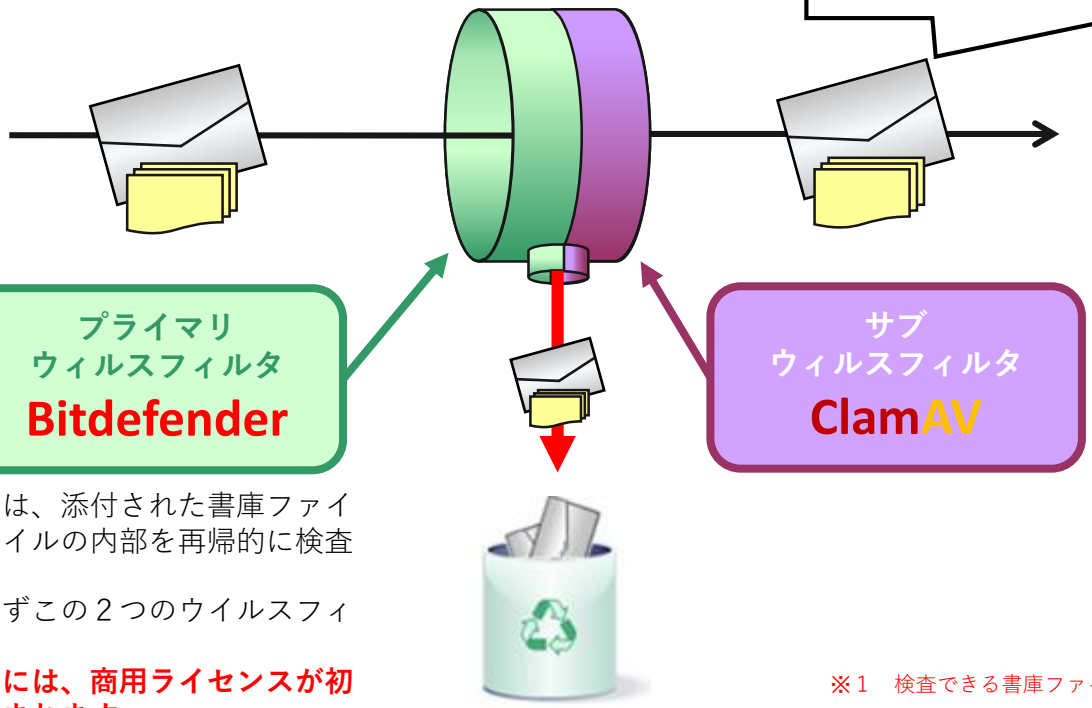
SpamTitanは、送られてきたメールの受信者確認を行ないます。
スパム送信者は、よくある名前やよくあるエイリアスへメールを送信します。
SpamTItanはメールアドレスが存在するかどうか確認して受信するかどうか判定します。
この設定は、ドメインの登録毎に行うことができます。
もちろん、受信者確認を行なわないように設定することもできます。



機能概略　ウイルス・脅威対策

SpamTitanは、２つのウイルス・脅威フィルタを装備しています。
SpamTitanは、一番最初にウイルス・脅威フィルタでメールを検査をします。
メールに含まれる脅威は電子ウイルスの添付ファイルや本文に仕掛けられたマルウエアのスクリプトなどです。
SpamTitanはBitdefenderとClamAVの２つのアンチウイルスエンジンを使って
脅威が含まれるメールからユーザーを守ります。

ウィルスが特定されたメールは、**削除・受信拒否・検疫・タグをつけて通過**などできます。
検疫されたメールを**リリース**することも可能です。



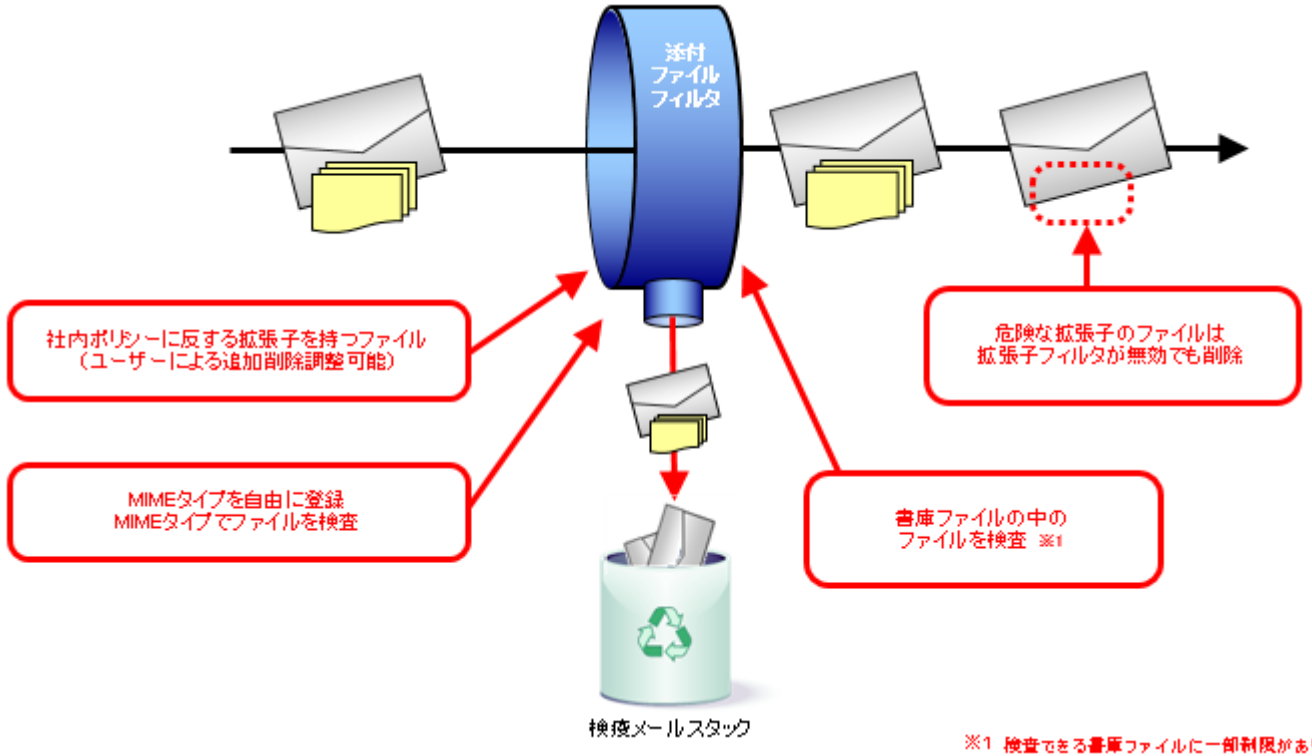
２つのウイルスフィルタは、添付された書庫ファイル※１や電子メールファイルの内部を再帰的に検査します。
すべてのメッセージは必ずこの２つのウイルスフィルタの検査を受けます。
アンチウイルスエンジンには、商用ライセンスが初めからシステム料金に含まれます。

※１　検査できる書庫ファイルに一部制限があります。

機能概略　添付ファイルフィルタリング

添付ファイルの拡張子によるフィルタリングが可能です。

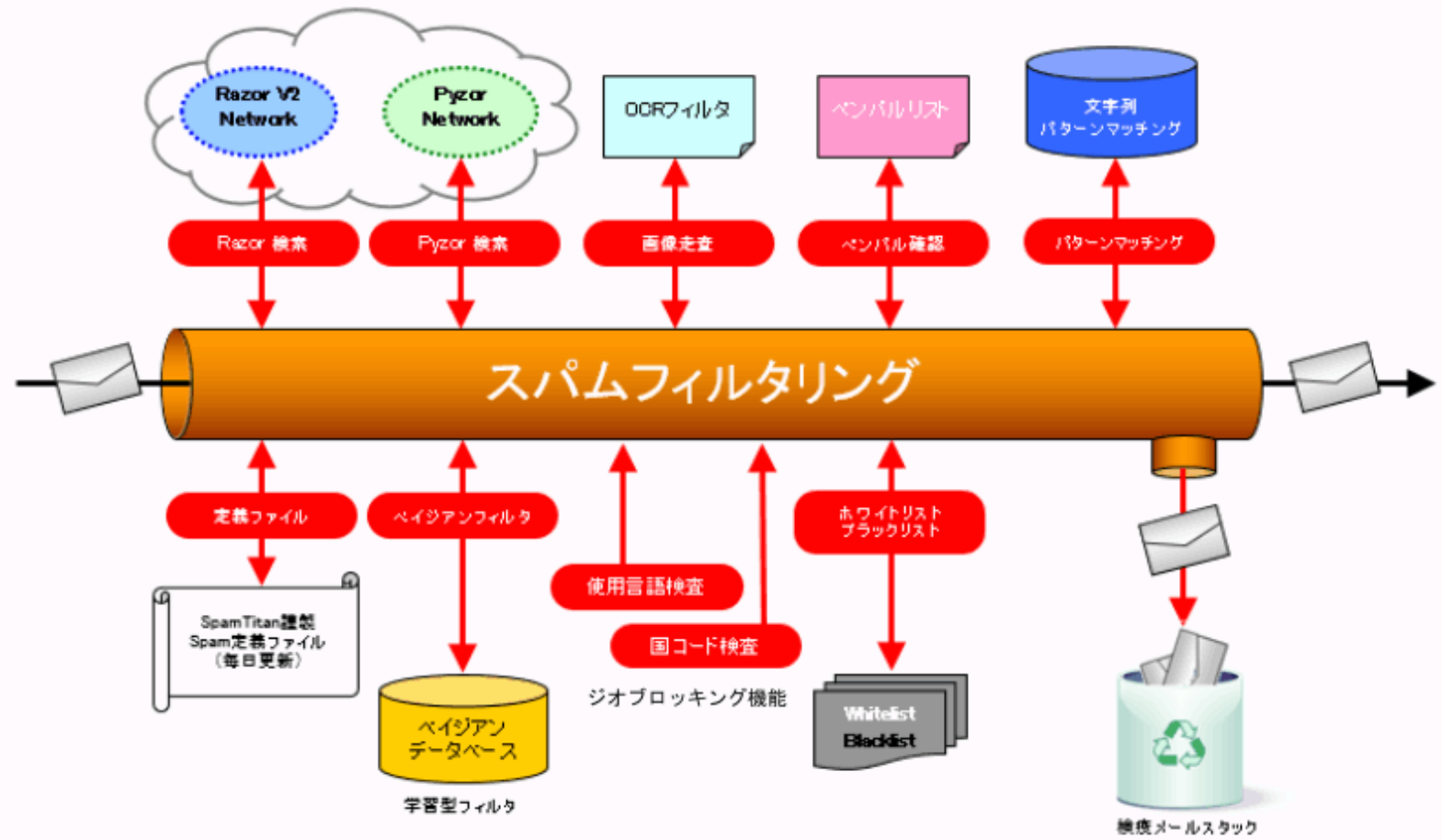
許可する拡張子、許可しない拡張子、許可するMIMEタイプ、許可しない
MIMEタイプなどを設定できます。
影響度の高いファイルの拡張子を設定することで、添付ファイルフィルタリ
ングが稼動していない場合でもファイルを強制削除する設定も可能です。



※1 検査できる書庫ファイルに一部制限があります。

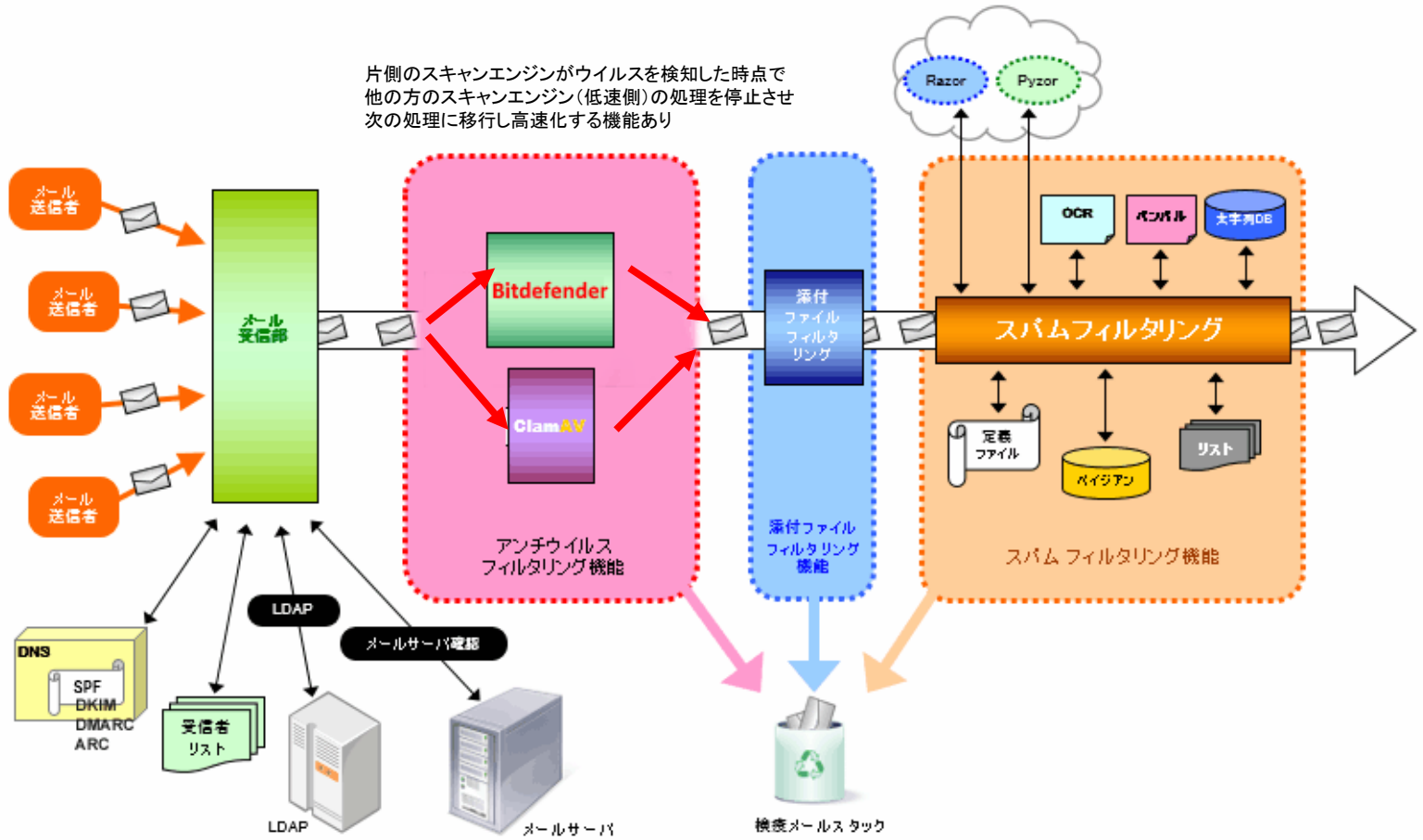
機能概略　スパムフィルタリング

SpamTitanはこの図のようなさまざまなスパムフィルタを利用してスパムメールを除外します。



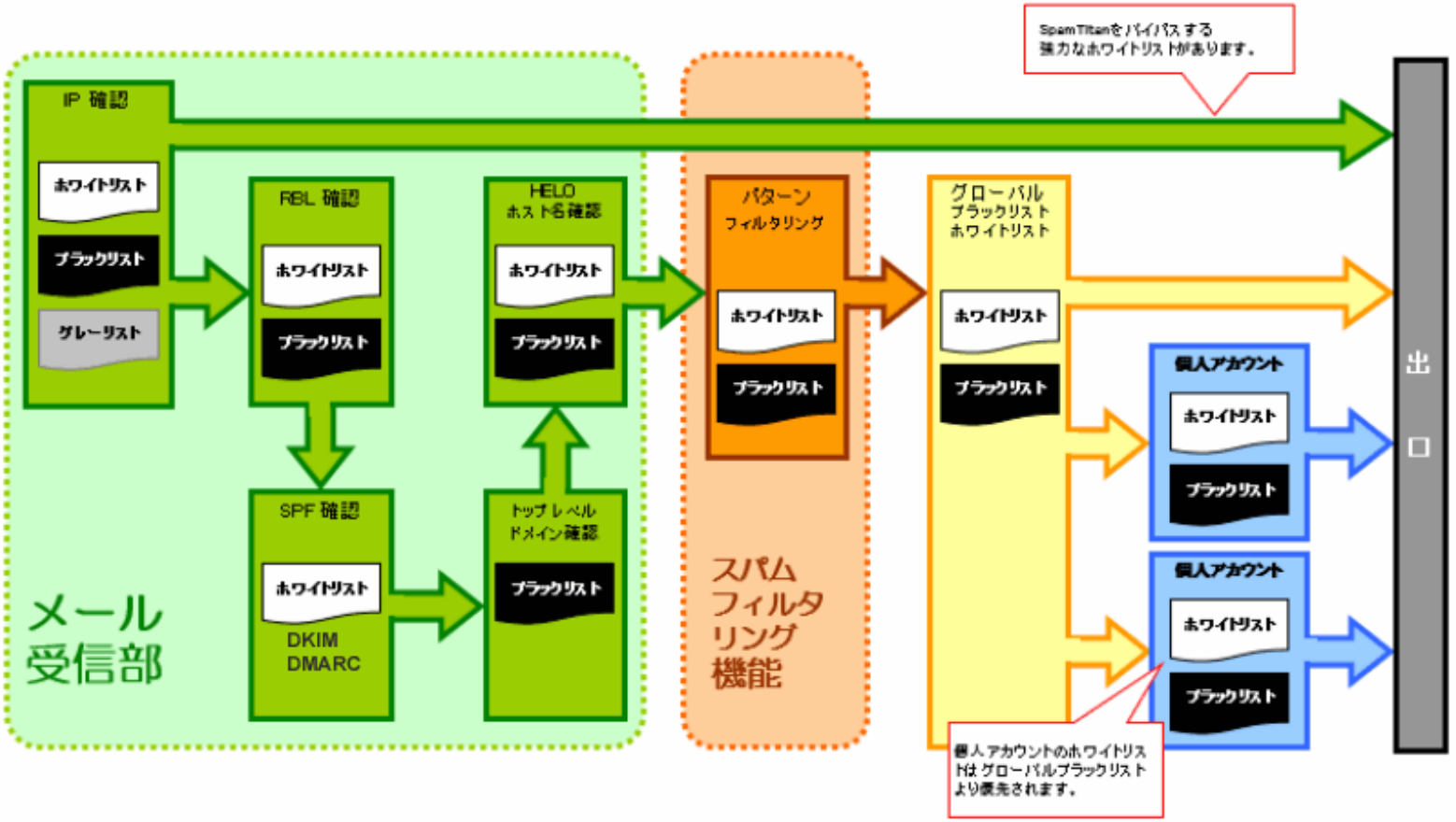
機能概略　各モジュールの接続俯瞰

以上の機能は、内部で以下のように接続されています。



機能概略　ブラックリスト・ホワイトリスト

SpamTitanには、以下の機能ブロック毎にブラックリストやホワイトリストが用意されています。
これらのリストはすべて個別に編集可能であるため、強力なフィルタリングを設定しても、誤検出を回避するバイパスを用意することができます。



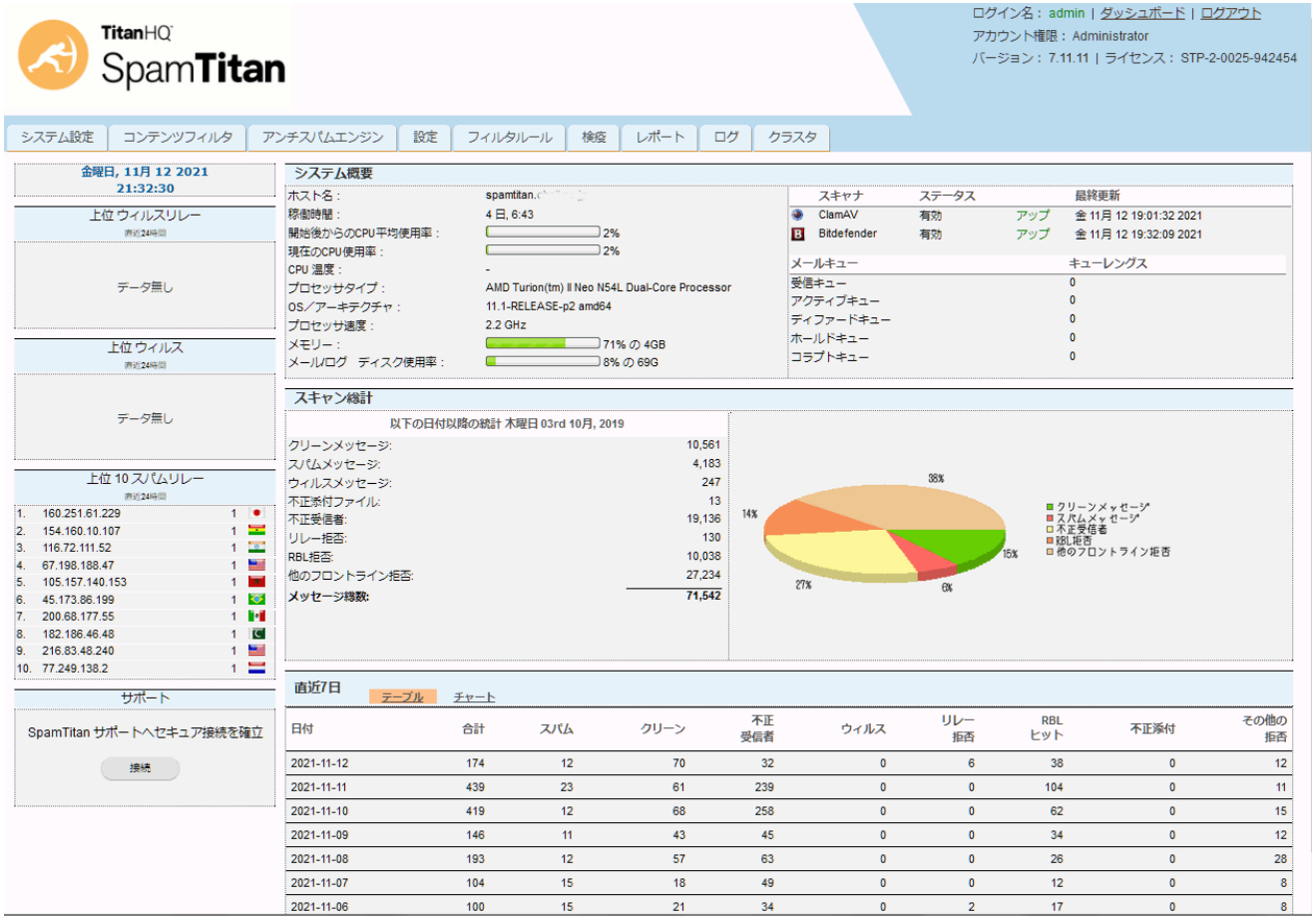
機能

インターフェース①

SpamTitanの管理インターフェースはWebインターフェースとなります。
ブラウザからアクセスできれば、どこからでも管理インターフェースを開くことができます。
対応するブラウザは以下の通りです。

- **Internet Explorer 最新/またはEdge最新**
- **FireFox 最新**
- **Chrome 最新**

Internet Explorer は環境によっては表示が正しくできない場合がある為、
FireFox/chrome の最新版を推奨いたします。



機能

インターフェース②

SpamTitan をインストールしたハードウエアが出力するインターフェースは、CLIです。
ハードウエア側はキーボードのみで操作できます。
このインターフェースは、初期の設定を行なう場合と、システムが正常に稼動しなくなった場合に使用します。

SpamTitan はFreeBSDというOSで稼動していますが、このOSにアクセスすることはできません。
ISOイメージによるインストールは、ほぼ全自動で導入されます。

機能

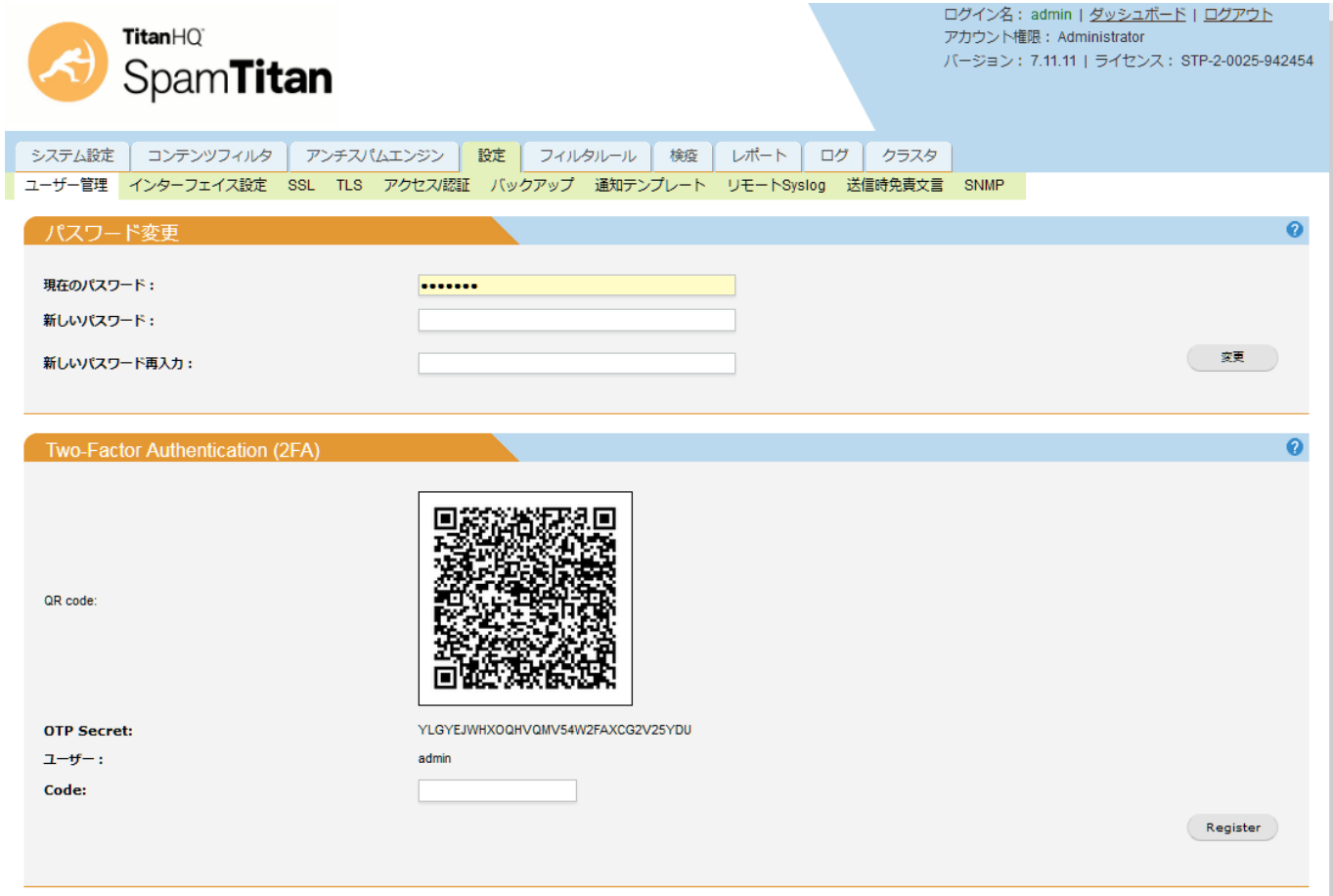
インターフェース③

SpamTitan には、管理者の他に一般ユーザーの専用ウインドウが用意されています。
このウインドウで設定できる機能は、その一般ユーザーのアカウントロールが反映されます。
指定する一般ユーザーのアカウントにそれぞれ設定したアカウントロールを指定することで機能タブが増減し、設定できる範囲が可変します。

この専用ウインドウは受信できるメールアカウントの数だけ用意され、ユーザーにインターフェースを展開するかどうかも含めて細かく設定できます。

また、ユーザーは仮パスワードの発行を自分で行い、専用インターフェースを利用するため、ユーザーが膨大な量であっても、運用に手間はかかりません

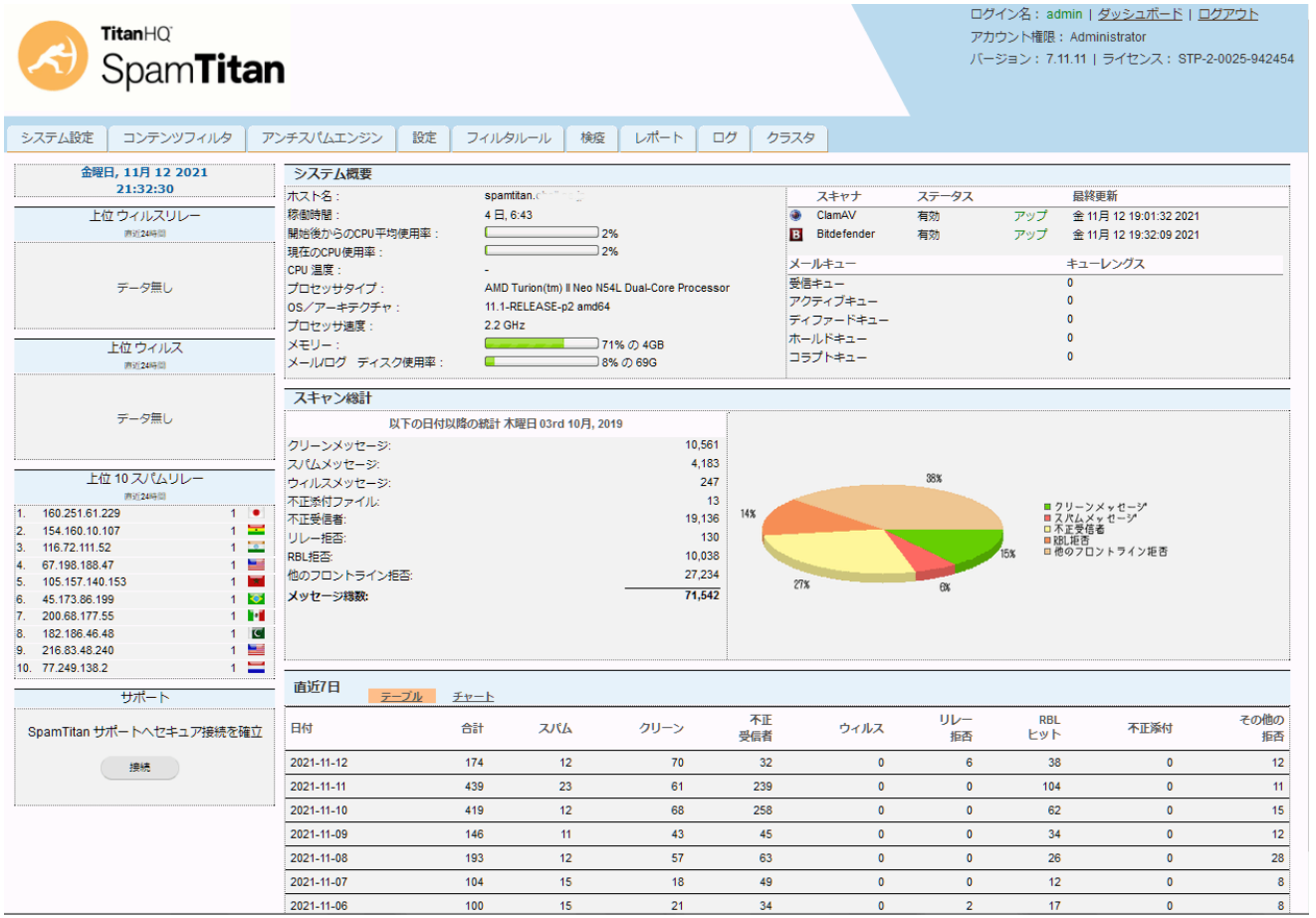
またSpmatitanの内蔵パスワード認証の他に外部認証として2要素認証機能も組み込まれていますので、より安全にログイン可能な仕組みも整っています。



機能

インターフェース④

SpamTitan のインターフェースは、色味や左上のページタイトル、ロゴなどを簡単かつ自由に変更できます。
コーポレートカラーやスクールカラーなどで自由にデコレートできます。
また、ヘルプなども別のWebサーバーで参照可能なURLにリンクすることも可能です。



機能

インターフェースのSSL対応

インターフェースはSSLに対応しており、また
CSRの自動生成機能も備えています。

有償の証明書をインポートする事も可能であり、
Let's Encyptにも対応しています。

機能

インターフェースのTLS暗号化

Web インターフェースの HTTPS によるアクセスは、暗号化やネットワーク、ポートなど非常に細かく指定することができます。

Webインターフェースのアクセス制御は、以下の方法を選択できます。

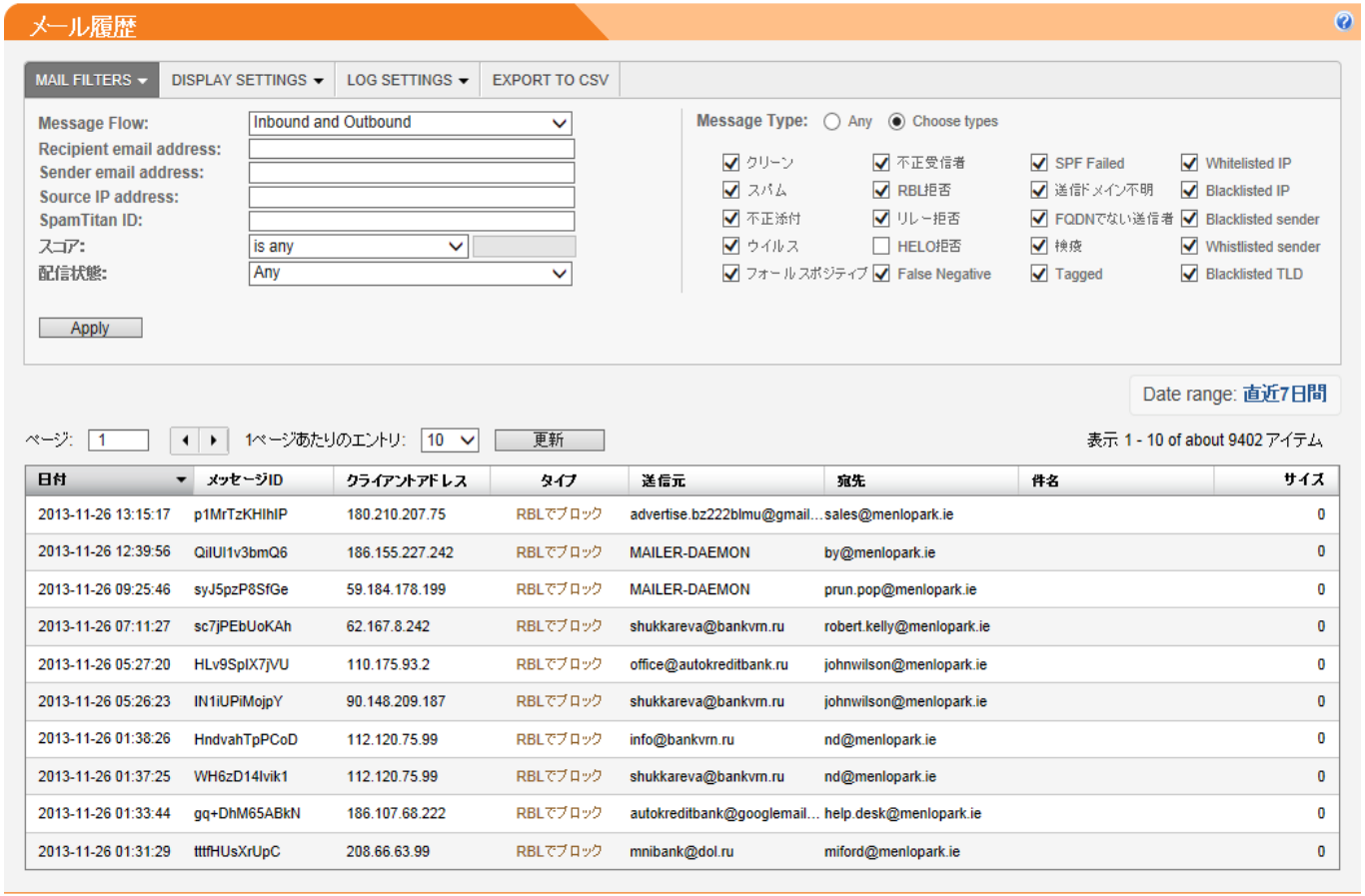
- **SpamTitan** 内部のリストによるアクセス許可
- LDAPによるアクセス許可
- SQLサーバーによるアクセス許可
- POP3によるアクセス許可
- IMAPによるアクセス許可

また、APIによるインターフェースへのアクセスも可能です。

機能

受信履歴

SpamTitan へアクセスのあったセッションはすべて記録することができます。
受信拒否をした場合やアクセス拒否をした場合は、アクセス内容のみが記録に残り、メッセージの詳細は記録に残りませんが、システムがメッセージをリレーした場合は、クリーンメールとして配送した場合であっても、すべて記録として残すことが可能です。

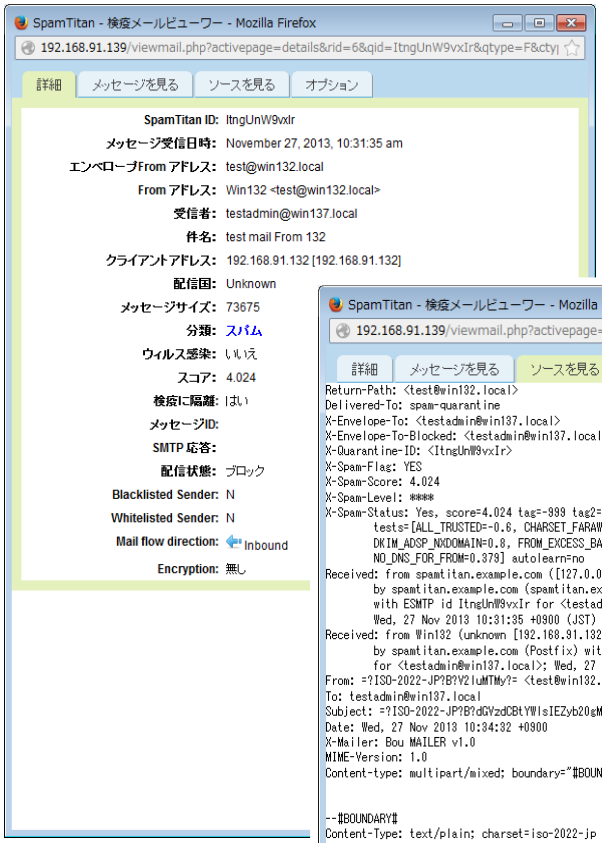


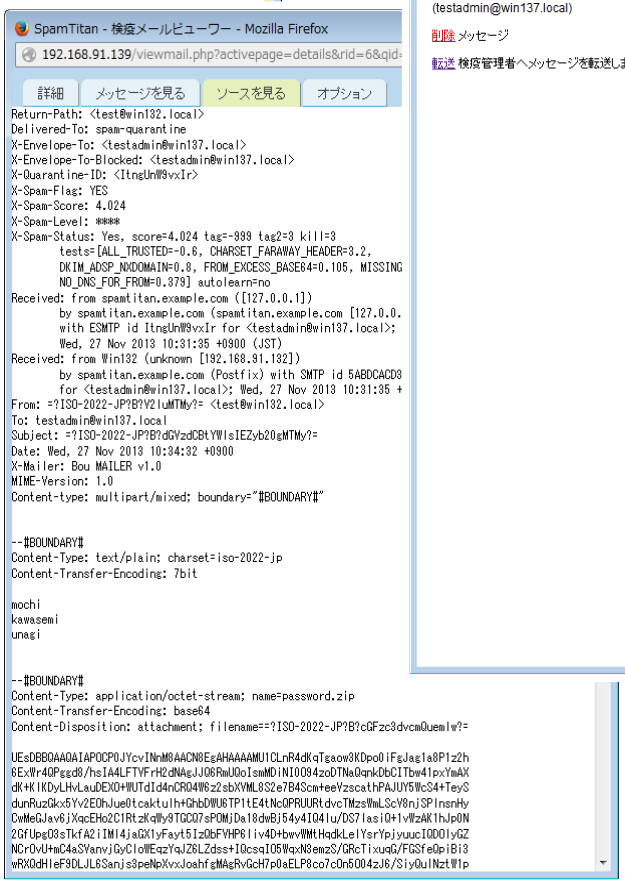
機能

受信履歴 詳細

SpamTitan がリレーしたメッセージで検疫されたメッセージ（あるいは、クリーンだが記録をアーカイブされたメッセージ）は、受信履歴の機能から、メッセージの詳細を確認し、リリース・転送、削除などをすることができます。
このポップアップウインドウを表示するには、メール履歴を１クリックするだけです。

一般ユーザーの専用インターフェースの場合は、自分のメールアカウントへの配信が指定されていたメールのみを閲覧、操作することができます。





機能

ポリシー

SpamTitan には3**種類のポリシー**が用意されています。

送信ポリシー

SpamTitan を通してメールを送信する場合の、メールの検査と処理の設定です。

ドメインポリシー

メールを受信した場合の、各ドメイン毎のメールの検査と処理の設定です。
これはドメイン毎に設定しますので、ドメインの数だけ存在します。

ユーザーポリシー

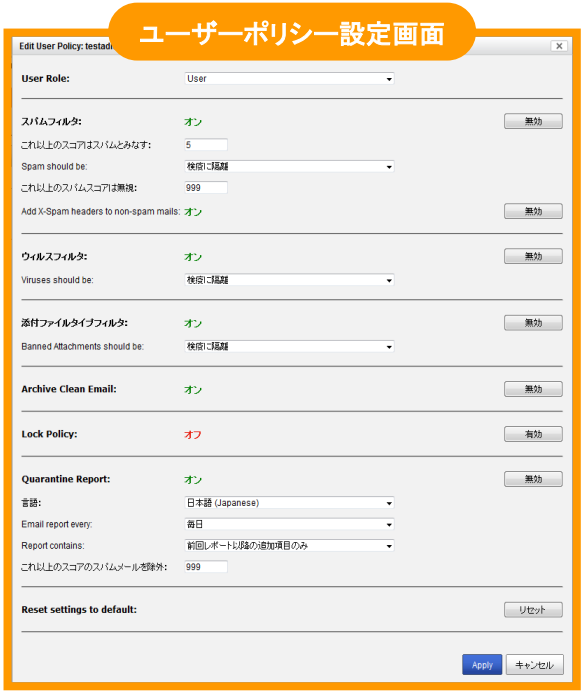
メールを受信した場合の、各メールアカウント毎のメールの検査と処理の設定です。
これはドメイン側のポリシー設定をベースに、メールアカウント毎に設定しますので、最大でメールアカウントの数だけ存在します。

ユーザーポリシーは使用してもいいし、しなくても構いません。ユーザーポリシーは初期設定のみドメインポリシーと同値ですが、個々で設定後はロックをかけてドメインポリシーの設定変更に引きずられないようにすることができます。

送信ポリシー設定画面

ドメインポリシー設定画面

ユーザーポリシー設定画面



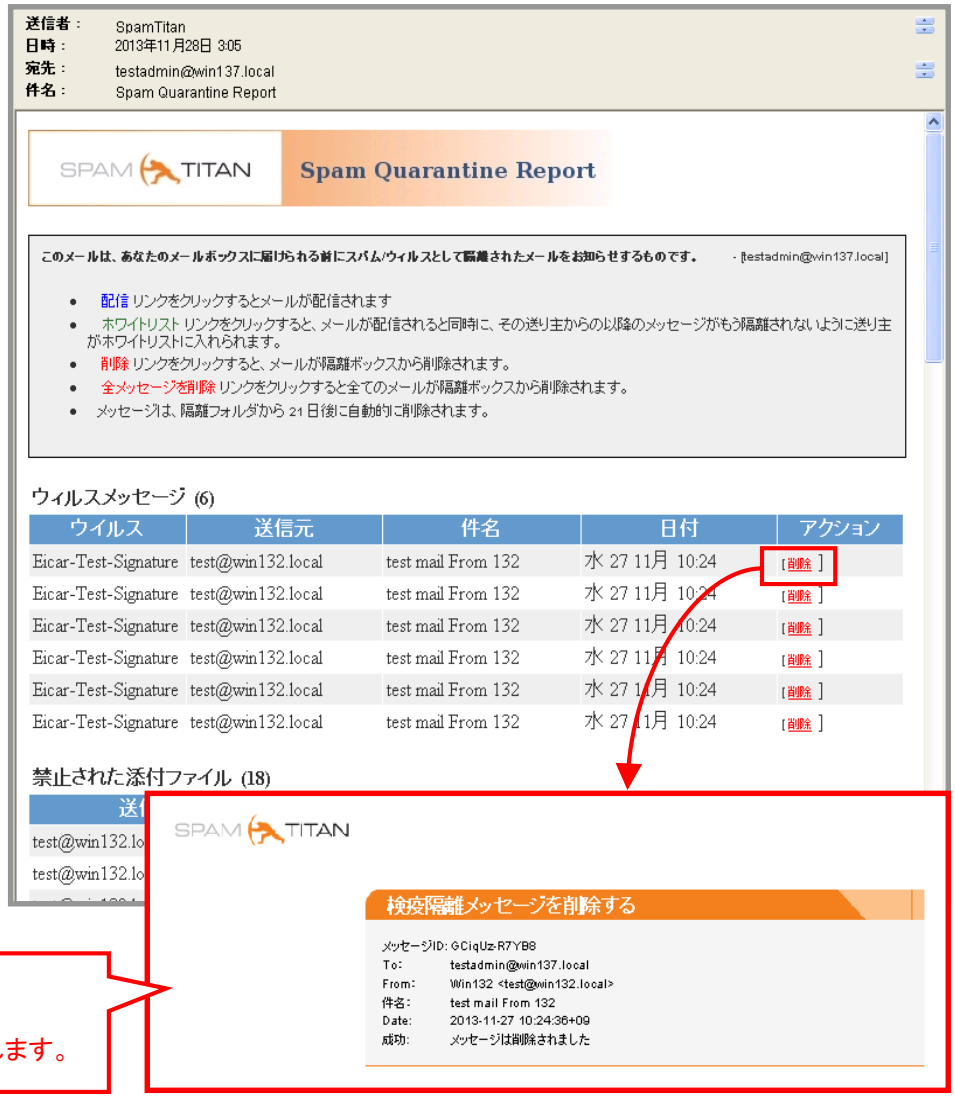
機能

検疫レポート①

SpamTitan が検疫隔離したメールは、検疫レポートという形でユーザーアカウントにレポートが発行されます。
このレポートは毎日や全平日といった発行タイミングや、前回からの追加分のみ、全項目といった内容部分を指定できます。

このメールに設けられた
- **配信**
- **ホワイトリストに登録**
- **削除**
- **全メッセージを削除**

といったリンクをクリックするだけで、検疫隔離されたメッセージを受け取ったり削除するなどの操作が可能です。

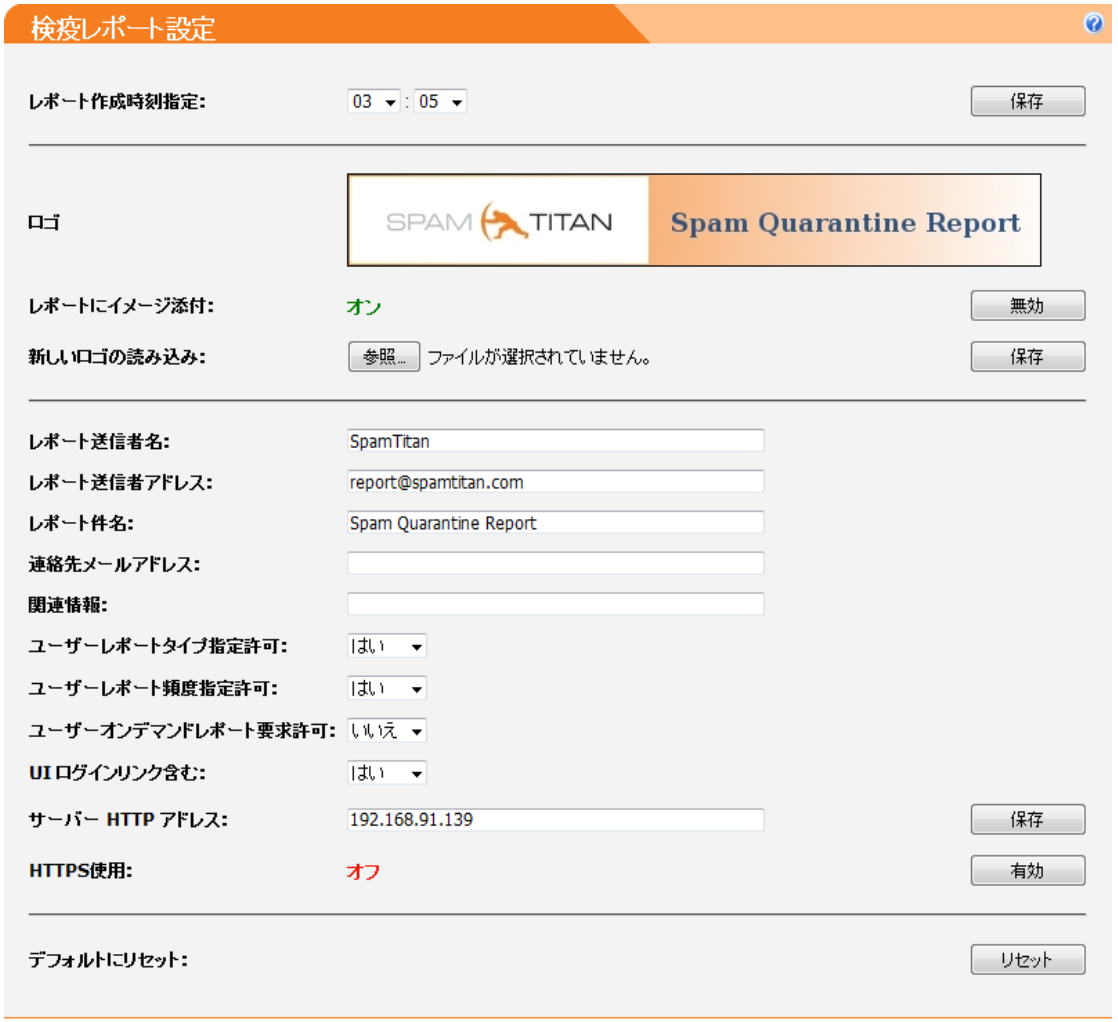


ブラウザが起動し、
この様な画面が表示されます。

機能

検疫レポート②

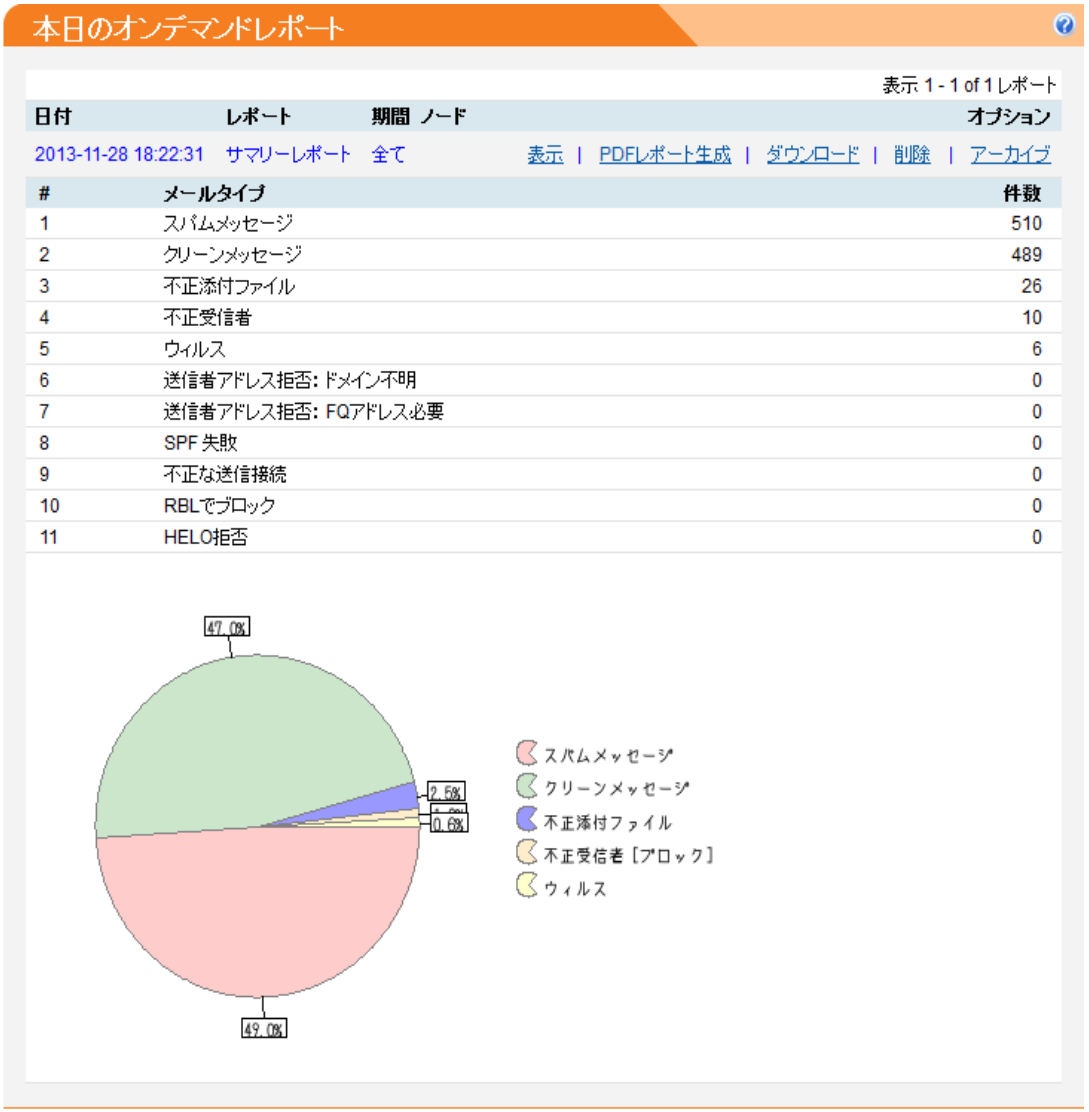
この検疫レポートは、HTML形式で構成されており、ある程度のカスタマイズが可能です。
たとえば、SpamTitanを導入しても、Spamフィルタとして固有の名前を与え、ロゴを作成してオリジナルのシステム名からの検疫レポートとすることもできます。



機能

レポート

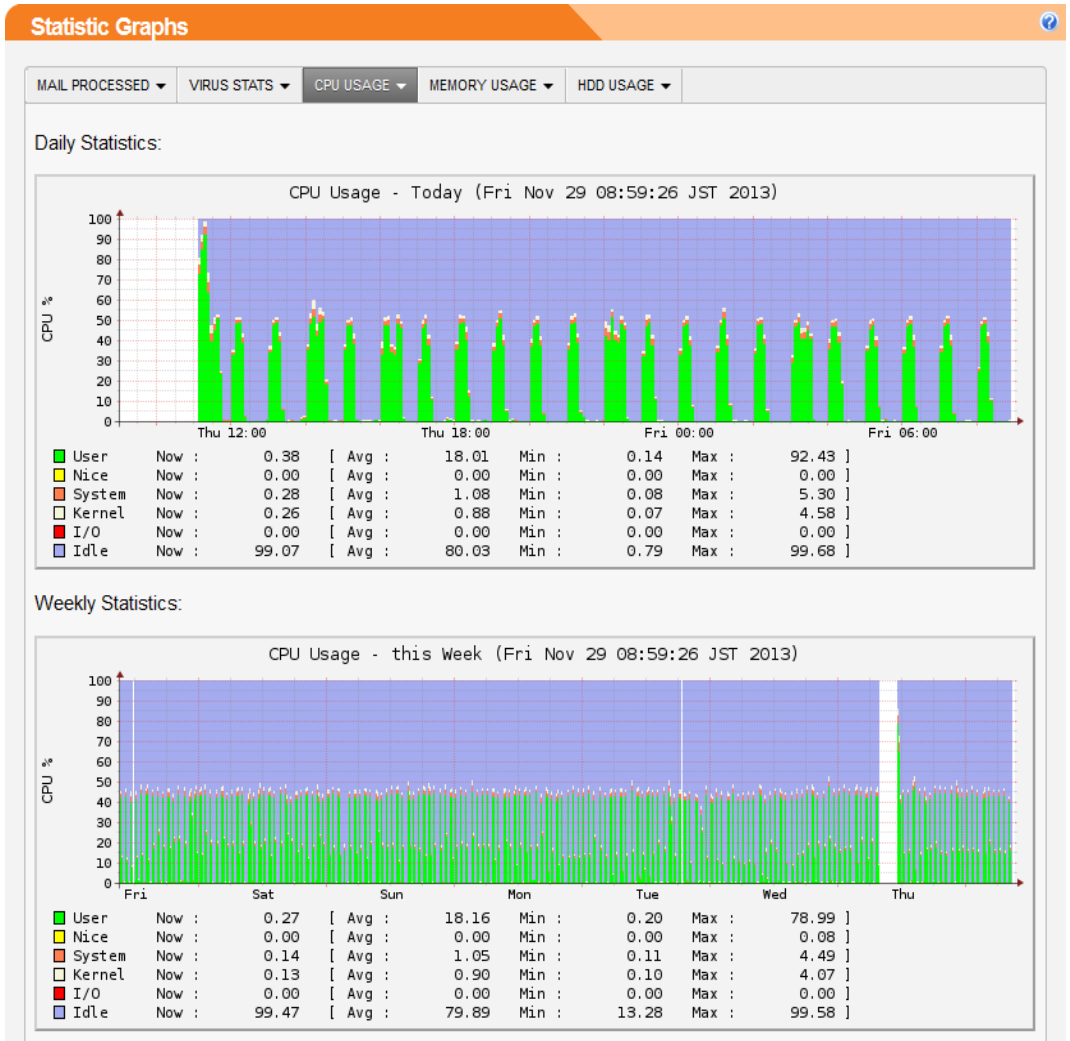
メールの処理状況や注意すべき情報を随時、あるいはスケジューリングを行い、アーカイブすることができます。
レポートは内容の他にタイムスケールを指定することができ、CSVやPDF形式でダウンロードできます。
レポートはタイムスケールに関係なく、日次、週次、月次などで生成され、アーカイブ指定することでシステムに保持することができます。



機能

グラフ機能

システムの稼働状況をグラフ表示します。
このグラフは、メールの処理状況、ウイルス受信状況、CPU、主記憶、ストレージの使用状況を、１日、１週間、１ヶ月、１年間というタイムスケールで記録します。
リソースの消費量を目安にシステムを運用することができます。

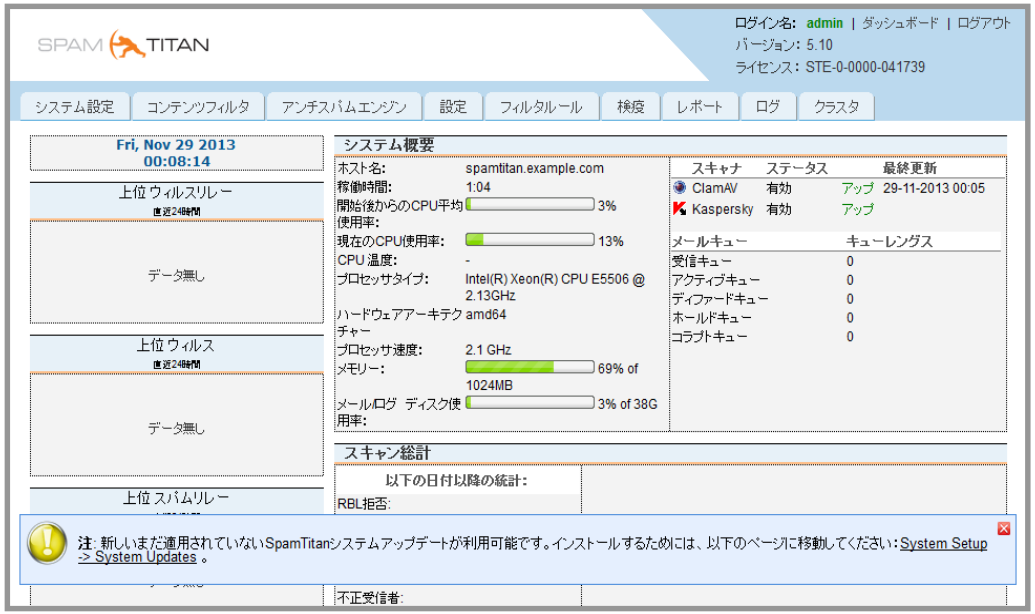


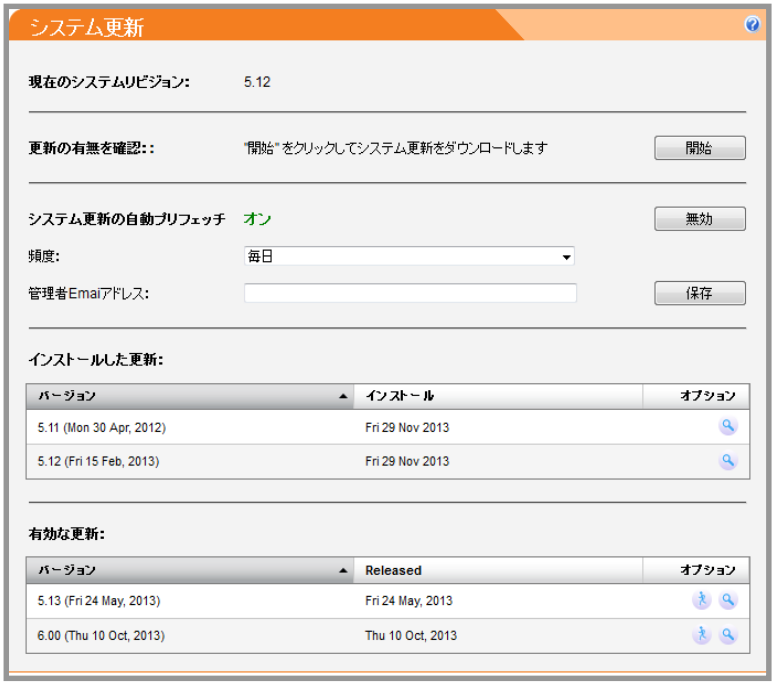
機能

アップデート機能

アップデートは不定期に年に3～5回程度、細かい不具合修正や改良を目的としてオンラインで配布されます。
アップデートの通知はシステムのWebインターフェースにオーバーラップされる形で表示され、バージョンアップはWebインターフェースから適用することができます。（アップデートファイルという形では配布されません。）ライセンス期間中に配布されたアップデートは、すべて利用することができます。

ベースOSのアップデートやVMToolsのアップデートなどもすべてシステムのアップデートに含まれ、個別に管理する必要はありません。
大型のアップデートの場合は、新しいISOイメージが配布されます。
オンラインによるアップデートの代わりに、ISOイメージでシステムを新たに作ることも可能です。



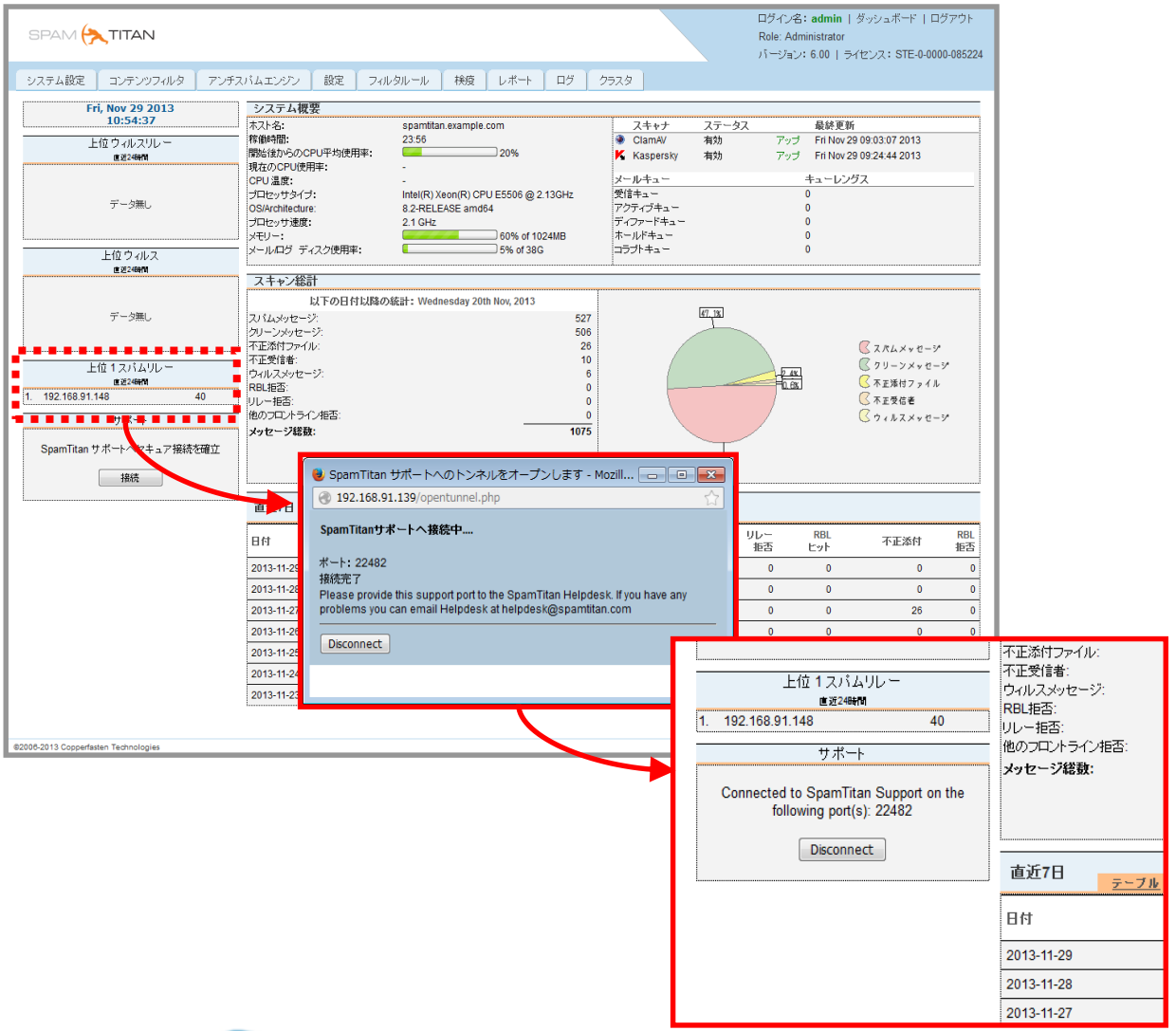


機能

リモートサポート機能

システムに障害が発生して、修復が必要な場合、SpamTitanではメーカーサポートがSSH接続をしてリモート操作で修正を行います。
このメーカーサポートによるリモートサポートは夜間に行なわれ、立会いの必要はありません。

サポートの申し込みは弊社に予定日の午後３時までにご連絡いただき、結果の報告を翌日行ないます。



機能

設定のバックアップ機能

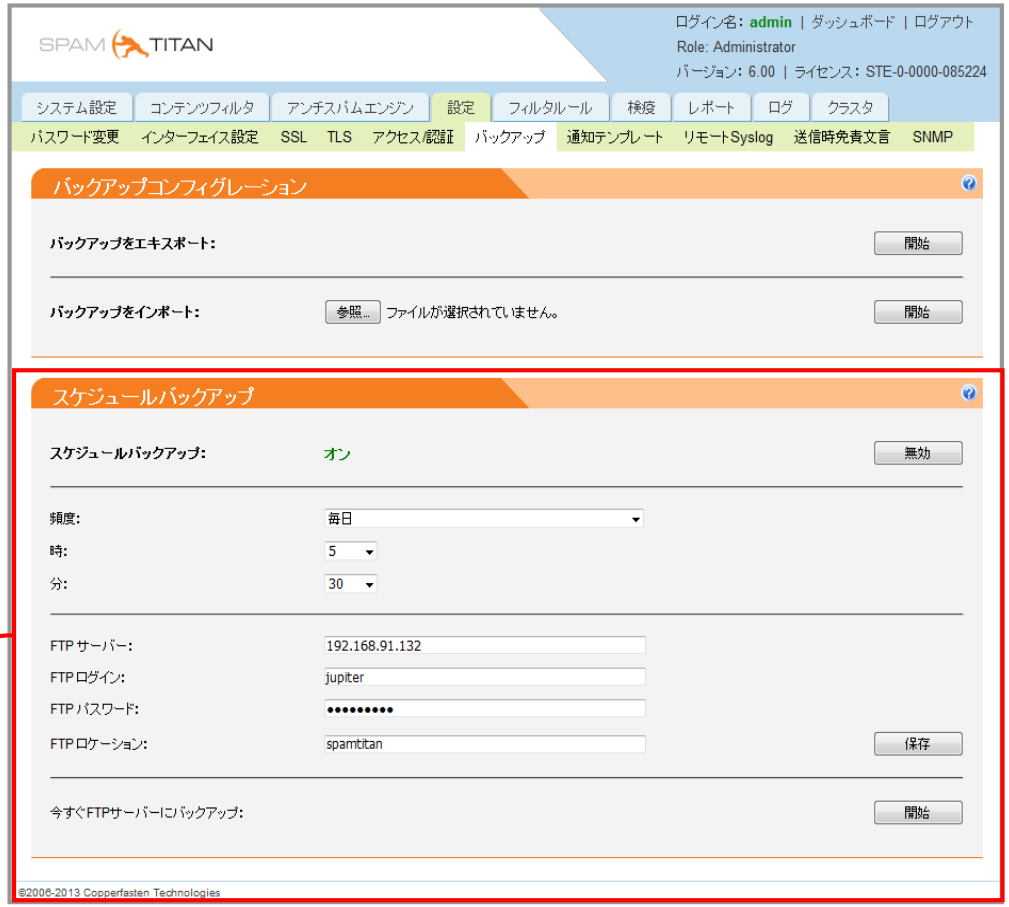
システム設定のバックアップは、以下の方法があります。
- Webインターフェースから直接取得する方法
- スケジュール機能を使ってFTPサーバーに保存する方法

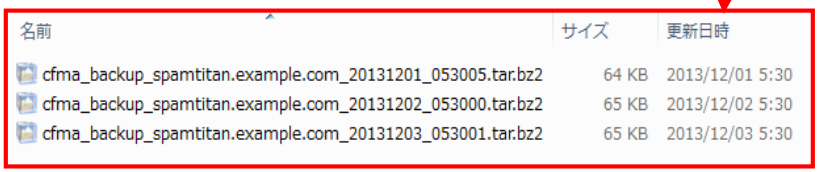
バックアップファイルはtarボール化され、bzip2形式で圧縮されます。
バックアップファイルはこの形式のまま取り扱い、リストアする場合もアーカイブを展開せずにWebインターフェースから読み込ませます。

バックアップファイルは、常に同じバージョンでのみリストアすることができます。
つまり、SpamTitanをバージョンアップすると、それまでに保存したバックアップファイルが使えなくなることを意味します。

またバックアップファイルには、ベイジアンデータベースのデータ、検疫されたメール、ライセンスは含まれません。
ユーザーが能動的に入力したデータのみ保存されます。

ファイルサイズは大きくても1MB程度です。





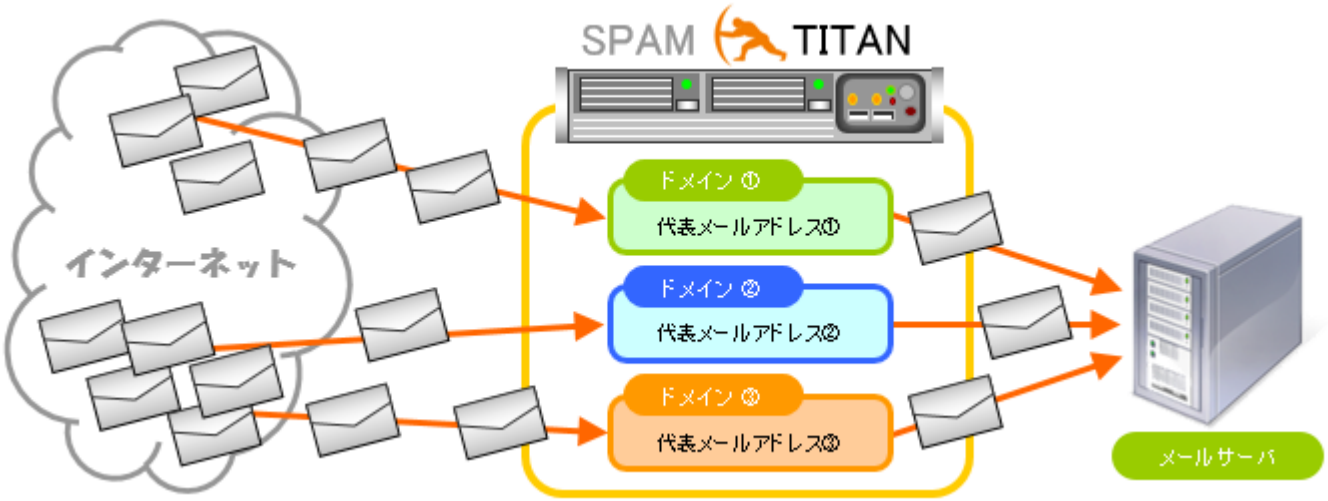
ケーススタディ①

１つのメールアドレスしか持たないドメインを大量に管理するケース

飲食店やサービス業の店舗の代表お問い合わせメールアドレスを多数管理しているお客様のケースです。
代表メールアドレスが１つしか存在しないドメインを、店舗の数だけ設定し、１つのメールサーバーへ集めます。
飲食店のWebには代表メールアドレスが露出していますが、このメールアドレスがSpam業者のメールアドレス自動収集ロボットに検知され、Spam送信のターゲットとなりがちです。
つまり、不特定多数のお客様から不特定の内容の連絡を受信するメールアドレスなのに、常に不特定の内容のSpamが大量に送られてきてしまいます。

SpamTitanは不審なIPアドレスやドメインからのメールを受け取らず、またインターネットのどこかで収集されたSpamの見本があればそれを除去するため、大変効率よく、また高い精度でSpamを除去する事ができます。

これは店舗の例ですが、学部、学科、研究室ごとにドメインを持つ教育機関にも応用できるフィルタリング例でしょう。
学会などで名刺を配る機会が多い立場の方は、Spamのターゲットにされてしまうことも多いようです。

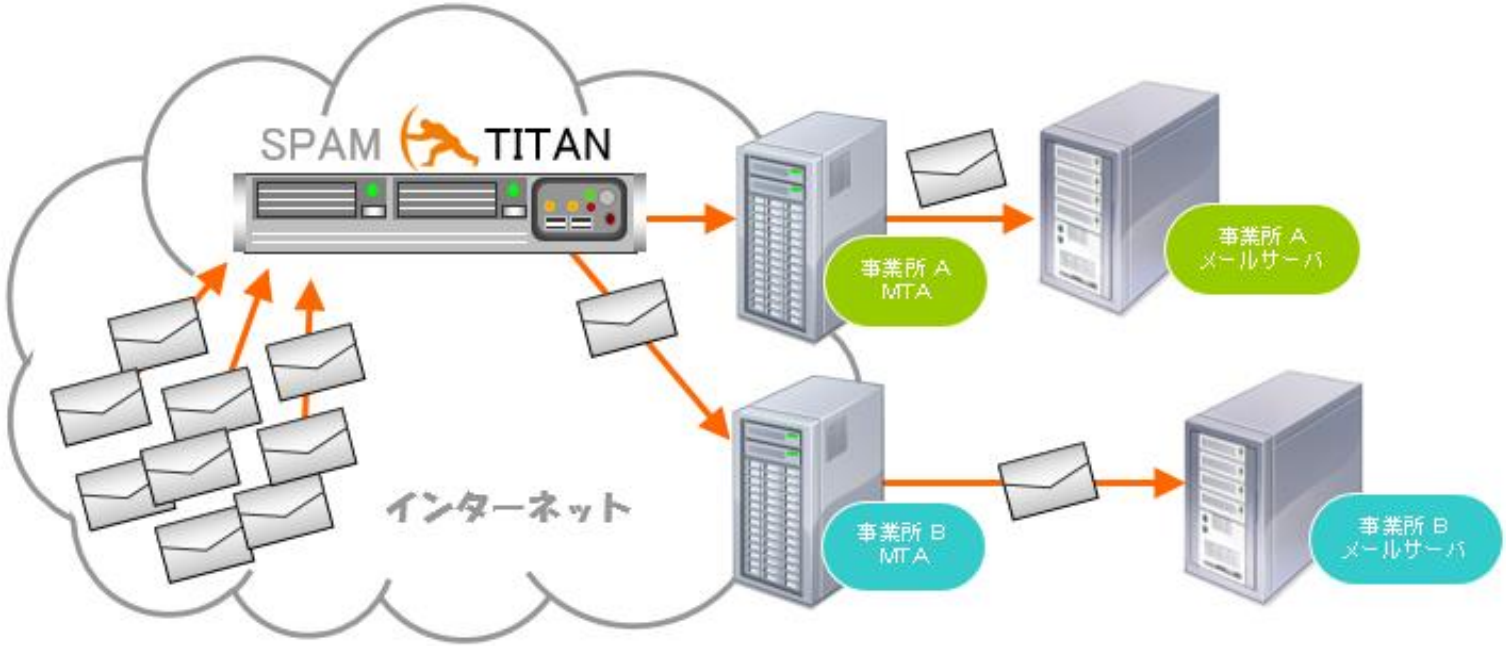


ケーススタディ②

遠隔地の拠点へメールをリレーするケース

事業所間に距離があり、拠点間をVPNで結ぶ場合メールリレーを社内LANで行なわないケースです。
この場合、SpamTitanを自社とは関係ないデータセンターのハウジングサービスに設置し、MXレコードをこのSpamTitanへ向けます。
SpamTitanだけが社外に単体で存在する形です。
このSpamTitanが受信したメールを、各事業所へリレーします。各事業所のMTAはこのSpamTitanからメールを受け取るように設定します。Spamフィルタが必要のないドメインは、各MTAが直接メールを受信します。

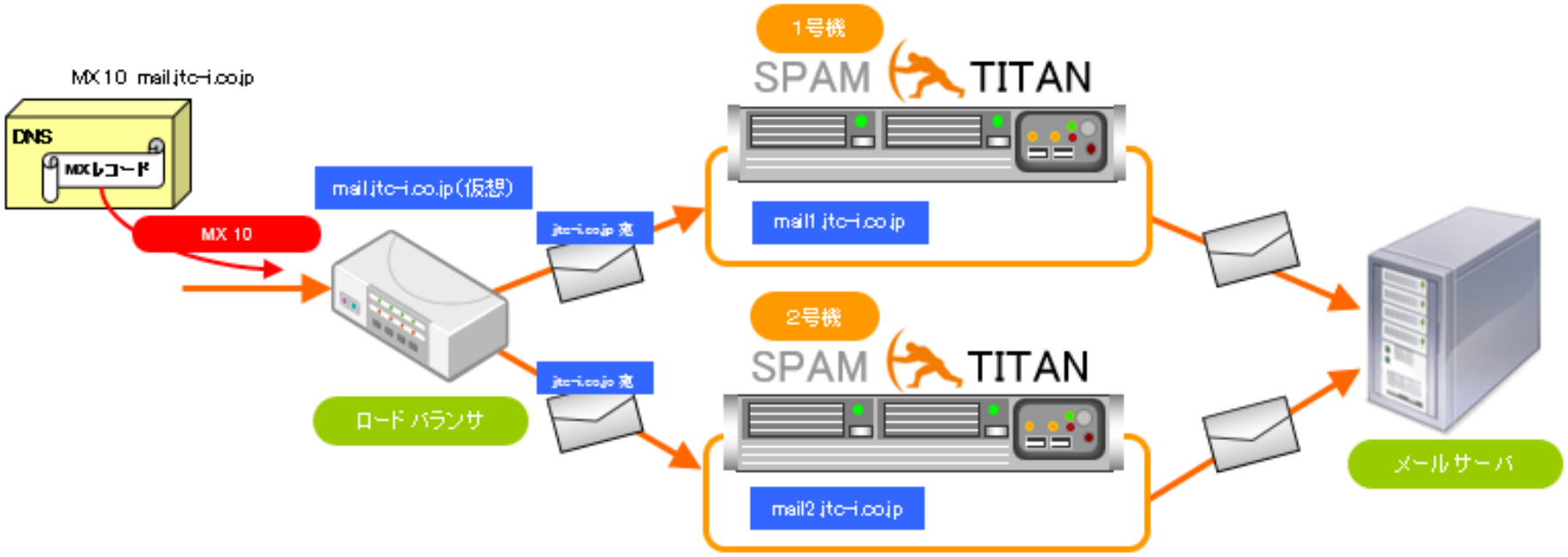
このケースのお客様は、SpamTitanの維持運用までをハウジングサービスに委託していました。



ケーススタディ③

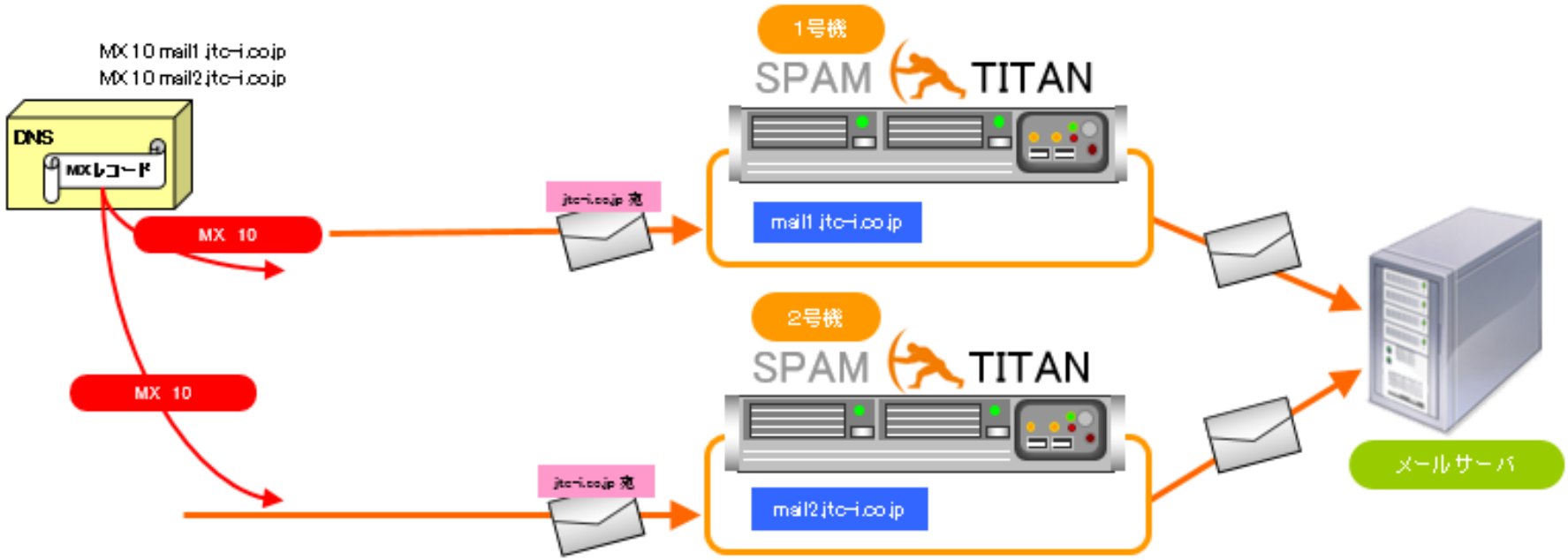
負荷分散装置を用いた構成

SpamTitanでクラスタ構成のシステムを構成し、１つのドメインを複数のSpamTitanで担当する場合は、前段にロードバランサを設置し、ハードウエア（負荷分散装置）でメール受信処理を行います。
将来的にSpamtitanサーバーを追加（３号機～）した場合にもDNS MXレコードの変更の必要もなく、また外部から実Spamtitanサーバーのホスト名が見えることはありません。



DNS MX Preference値で分散する場合

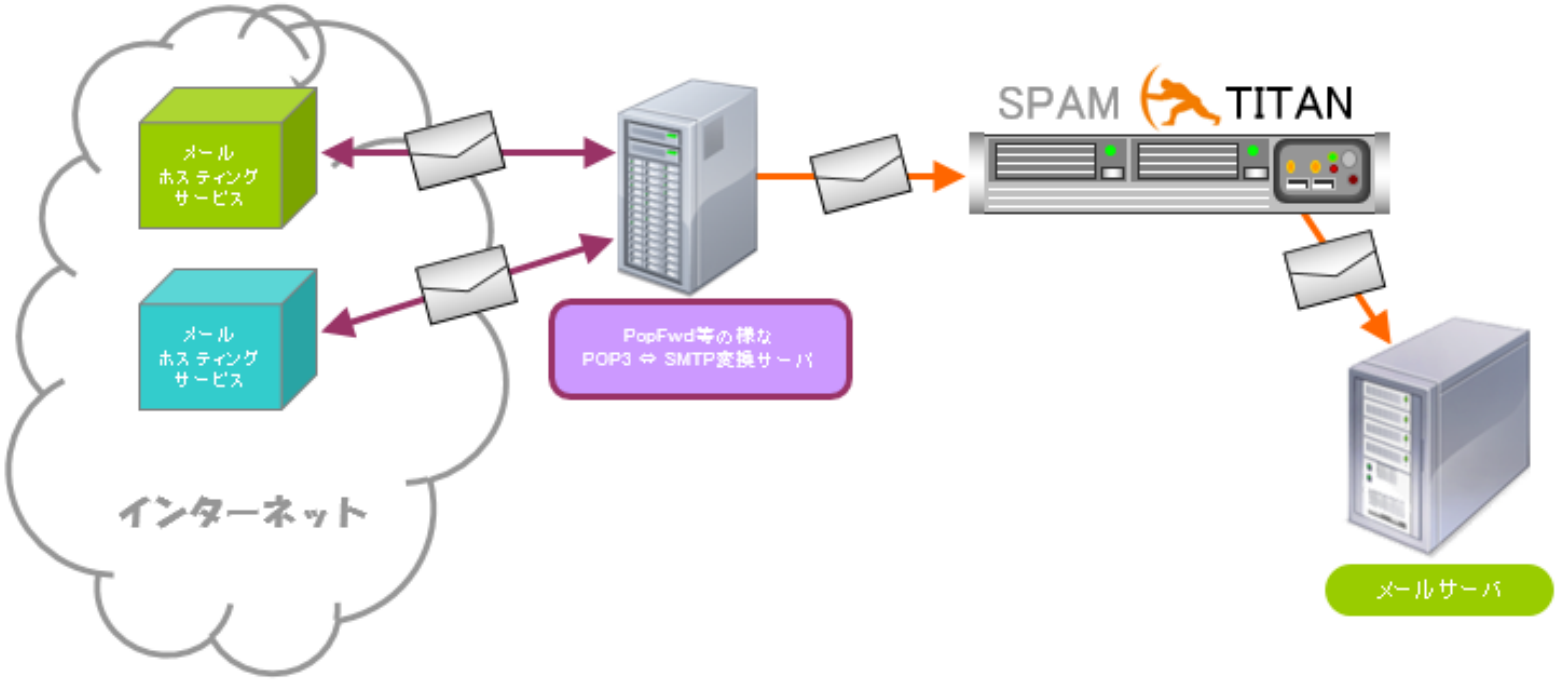
Preference値で分散させる場合は高額なロードバランサが必要なくなりますが、DNS　MXレコードの追加や、
SpamTitanのドメイン名が露出されることになります。
DNSのMXレコードの追加が必要なだけで、簡単にクラスタシステムが構成できるメリットがあります。



ケーススタディ④

SpamTitanを副次的なSpamフィルタとして使用するケース

自社でメールホスティングサービスを利用して、POP3でメールボックスからメールを取得し、SMTPで任意のメールサーバへメールを転送するというような構成の場合に、SpamTitanを副次的なSpamフィルタとして使用できます。
この場合、ホスティングサービスがメールを既に取得しているので、SpamTitanの受信時のフィルタリングをすべて使用できませんが、それ以外の機能は利用できます。
これはたとえば、代表メールアドレスなどでホスティングサービスを利用しているが、ホスティングサービス提供者のフィルタリングに自由度が少なかったり、より細かい制限を設けたい場合に有用です。
利用しているホスティングのアカウントが少ない場合、SpamTitanの最小ライセンスでも十分でしょう。



システム要件

SpamTitan をインストールするハードウエアのシステム要件は、次の通りです。
ベースシステム（物理サーバ）：FreeBSD がインストール可能なシステム（ISOイメージによる構築時）
ベースシステム（仮想サーバ）：ESXi 5.1 以降（OVFファイルによる構築時。ISOイメージの場合は弊社までお問い合わせください）

サイジングは以下の表を参考にしてください。
（備考：クリーンメールアーカイブ機能を使う場合には、HDD容量を更に大きく確保してください）

	５００ユーザー以下		１０００ユーザー以下		５０００ユーザー以下		５０００ユーザー以上	
	物理サーバ	仮想サーバ	物理サーバ	仮想サーバ	物理サーバ	仮想サーバ	物理サーバ	仮想サーバ
CPU	Inten Pentium（Wolfdale以降）2GHz 1コア以上（Corei3以上を推奨）	vCPU-1個以上	Inten Xeon（Conroe3070以降）2.5GHz 1コア以上	vCPU-2個以上	Inten Xeon 3GHz 4コア以上	vCPU-4個以上	クラスタ構成を推奨	クラスタ構成を推奨
Memory	２ GB 以上	２ GB 以上	４ GB以上	４ GB以上	８ GB以上	８ GB以上	クラスタ構成を推奨	クラスタ構成を推奨
HDD	８０ GB以上	８０ GB以上	１２０ GB以上	１２０ GB以上	２５０ GB以上	２５０ GB以上	クラスタ構成を推奨	クラスタ構成を推奨
NIC	１個～2個（100BASE)or（1000BASE)	１個～2個（100BASE)or（1000BASE)	１個～2個（100BASE)or（1000BASE)	１個～2個（100BASE)or（1000BASE)	１個～2個（100BASE)or（1000BASE)	１個～2個（100BASE)or（1000BASE)	クラスタ構成を推奨	クラスタ構成を推奨

よくある質問①

Q 01	リダンダンシ性能を確保する為にNICをチーミングすることはできますか？
A 01	SpamTitan は複数のNICを取り扱うことができますが、それぞれにIPアドレスやエイリアスを設定する必要があります。 それぞれのNICからメールストリームを受信できるので、SpamTitanの前段にロードバランサなどを設置することで、 同じ性能を備えることは可能です。あるいは、仮想マシンでシステムを構築し、仮想環境側のNICをチーミングすることは可能です。 SpamTitan のみで一般的なNICのチーミングは構成することはできません。
Q 02	IPv6の対応状況を教えてください。
A 02	IPv6については、各セッションやフィルタ機能で対応が進められております。機能のほとんどで対応済みです。
Q 03	日本語ドメインの対応状況を教えてください。
A 03	SpamTitan Ver.7ではIDN表現やPunycode変換は未だ対応しておりません。 しかし、メーカーでは開発を進めており、将来のバージョンで統合される予定です。
Q 04	添付ファイルへの検査について教えてください。
A 04	添付ファイルに関しては、入れ子状になった書庫ファイルの内部について、再帰的に検査を繰り返します。 著名な書庫ファイル形式は内部の走査ができますが、Microsoft社の製品で使われている *.cab 形式は権利関係もあり、 書庫内部の走査ができません。
Q 05	暗号化された添付ファイルはウイルス検査できますか？
A 05	SpamTitanではできません。
Q 06	インターネット上のさまざまなサービスが参照できない場所に設置できますか？
A 06	スパムフィルタリング性能が著しく低くなります。 RBLやSPFレコードへの問い合わせ、DNSを使ったボットネット検出といった機能は、外部のさまざまなデータベースを使用して 実現できる機能です。外部のデータベースを利用できない場合は、メーカーのスパム定義ファイルやAMaViSのスパムスコア 加点だけが期待されます。フィルタリング性能としては半分程度とお考えください。

よくある質問 ②

Ｑ０７	SMTPコマンドのVRFYコマンドは応答しますか？
Ａ０７	SpamTitanではVRFYコマンドは使用不可になっています
Ｑ０８	評価方法を教えてください。
Ａ０８	SpamTitanでは30日間評価できる評価ライセンスを発行できます。仮想アプライアンス版であれば簡単に評価できますので、評価ライセンスをご希望の場合は、弊社までお問い合わせください。
Ｑ０９	32bit バージョンと64bit バージョンの違いについて教えてください。
Ａ０９	提供される機能は同一ですが、32bitバージョンは主記憶が4GBまでに制限される代わりに、インストールできるハードウエアが若干多いです。64bitバージョンは、4GB以上の主記憶をサポートし、処理が重いウイルス検査や添付ファイルの検査、パターンフィルタリングの処理能力が落ちにくくなります。これは構文解析や比較検査に使用できるCPUリソースが32bitバージョンより多く定義されているためです。弊社としては64bitバージョンをお奨めしています。
Ｑ１０	評価期間を延長することはできますか？
Ａ１０	SpamTitan は評価ライセンスを２度適用することはできません。また、評価ライセンスは取得した日を起点として評価期間を計算し３０日以上の評価期間が必要な場合は、３０日後に改めて評価システムを作り直します。 その際、弊社から評価ライセンスを発行いたしますので、弊社までご連絡ください。
Ｑ１１	ウイルス検査の強度を変更することはできますか？
Ａ１１	できません。
Ｑ１２	ウイルススキャナのどちらか一方だけを止めることはできますか？
Ａ１２	メンテナンスとしてはできますが運用ではできません。サービスを動かしたまま、検査をしないという設定のみできます。
Ｑ１３	AMaViS の詳細な調整を行うことはできますか？
Ａ１３	できません。
Ｑ１４	Postfix によるディファードキューに溜まったメールの再送信間隔をすべて調整できますか？
Ａ１４	できません。ディファードキューに保存できる最大生存時間のみ設定できます。queue_run_delay は300秒に設定されています。

よくある質問 ③

Ｑ１５ フォールバック（Fallback）機能は複数構成できますか？

Ａ１５ 可能です。IPアドレスかホスト名を半角カンマで区切って表現します。
ただし、送信用SMTPサーバーの処理力が低かったりMTAが止まったりすると、送信メールサーバーを次々と変更するループが発生し易くなりますので、メールリレー経路の検討を十分に行なってください。
また、送信先SMTPサーバーがグレーリストを持つ場合、そのリストに30分ほど記録されてしまう可能性があります。

Ｑ１６ アップデート情報の入手について教えてください。

Ａ１６ アップデートがリリースされると、Webインターフェースにオーバーラップする形で通知が表示され、
システム更新セクションに詳細が表示されます。また、弊社メールマガジンやWebページにアナウンスが掲示されます。

Ｑ１７ ライセンスの有効化（アクティベーション）について教えてください。

Ａ１７ SpamTitanでは一般的なアクティベーションというライセンスの有効化はなく、実質的な日付で使用期間が決められます。
ご購入時に使用期間をご連絡いただき、それに合わせてライセンスファイルをメールでお送りいたしますので、
Webインターフェースで読み込ませていただけば、ライセンスの適用となります。
従って、使用、不使用に関わらず、ライセンス期日を迎えればライセンスファイルは使用できなくなります。
ライセンス期日を向かえたシステムは、設定の操作や機能の利用ができなくなりますので、継続使用の予定がない場合は、速やかに撤去してください。
なお、初期導入時の構築期間には評価ライセンスをご利用いただき、継続のご契約時には、１つ前のライセンスとライセンス期間が重複するように設定されたライセンスが早めに発行されます

Ｑ１８ ISOインストーラについて教えてください。

Ａ１８ SpamTitan の何らかのライセンスをお持ちの場合は、弊社Webページのソフトウエアダウンロード ページからISOイメージをダウンロードして、ご利用いただけます。
このとき、正規ライセンスを使用する場合にライセンスを二重使用しないようにご注意いただければ、システムの移設やハードウエアのアップデートなどでご利用形態が変更されても問題ありません。

よくある質問④

Q 19	VMware仮想アプライアンス ライセンスでISOイメージを基にしたシステムは利用できますか？
A 19	可能です。ライセンスの使用方法としても問題ありません。 初期にISOライセンスで導入された後で、弊社Webページのソフトウエアダウンロード ページからVMware 仮想アプライアンスをダウンロードして仮想アプライアンスをご利用頂いても問題ありません。 その逆に、VMware仮想アプライアンス ライセンスで導入された後で、ISOイメージで構築したシステムに移行することも問題ありません。 これは、仮想アプライアンスの仮想ハードウエアの設定がやや小規模であるため、仮想ハードウエアをリッチに設定するためにISOイメージを使用して仮想マシンを構築する場合があったり、あるいはISOイメージで構築したシステムを仮想環境へまとめてハードウエアの台数削減を進める場合など、ご利用形態が途中で変更されるケースが多いためです。 そのため、ISOライセンスとVMware仮想アプライアンス ライセンスは同一価格となっております。
Q 20	大規模収容アカウントの例を教えてください。
A 20	国内では６ノードクラスタ、複数のドメイン構成で数万アカウント収容の実績がございます。 収容アカウントが１０００以下でも、リダンダンシ性能確保の為に２～３ノードクラスタ構成をご選択されるケースが多いです。

ご注意 ①

SpamTitan をご利用になる上で、事前に把握しておく必要のある特徴がいくつがございます。

ハードウエア選定について

SpamTitanがインストール可能なハードウエアは、FreeBSD Ver.10/11がインストールできるハードウエアとなっております。
こちらについて、各サーバーメーカーがBTO販売を拡大させている関係もあり、どのハードウエアで稼動するか、といったリストを作りにくい状況となりました。
FreeBSDが公開しているデバイスドライバに対応しているハードウエアでも、SpamTitanをインストールできない場合があります。
端的に確認する方法としては、サーバーメーカーから評価用の機材をレンタルしたり、ハードウエアのリース会社から機材をレンタルして実際にインストールを試みる方法があります。
あるいは、VMware社の仮想環境であるESXi Ver 5.1以上をインストールして、仮想環境でSpamTitanを構築する方法があります。
VMware社のESXi上で構築する場合、ESXi側でネットワークポートのチーミングが構成でき、ディスクイメージのバックアップなども簡単に行うことができるようになるので、弊社としてはこちらをお勧めいたします。

メールの送信について

メールの送信経路にSpamTitanが含まれる場合の注意点として、メールマガジンの配信があります。

注意点 1

メールマガジンの配信に時間がかかる場合があります。
メールマガジンは一般的にファイルサイズが大きいため、スキャンにある程度の時間がかかります。（6～10秒/通）
その上、同一内容でありながら送信先が異なるために、仮に一度に2000通を送信する場合、その2000通全部を検査してしまいます。
SpamTitanに限らず他社の製品であっても事情は同じで、一般的にこうしたSpamフィルタと呼ばれるメールフィルタシステムでは、同一の内容を一度に大量の宛先へ送信する場合、その数に応じて時間がかかります。

注意点 2

一度に大量のメールを異なるSMTPサーバへ送信しているIPアドレスは、Spam送信元とみなされて、たとえば送信用IPアドレスをRBLに登録されてしまうケースが稀にあります。
そういった場合、SpamTitanがその様なRBLを参照していると障害の原因になりがちです。

上記 2 点を回避する為には、同一内容のメールを一度にたくさんのメールアドレスに送信するような業務は、一般業務から切り離し、SpamTitanを経路に挿まないように構成します。特に教育機関などでは、一斉送信メールが非常に多いのでご注意ください。

ご注意 ②

SpamTitan をご利用になる上で、事前に把握しておく必要のある特徴がいくつがございます。

クラスタノード ライセンスについて

SpamTitanをクラスタ構成でご注文されると、ライセンスはクラスタライセンスとなります。
クラスタライセンスはマスターノードライセンスとスレイブノートライセンスの２種類で構成され、スレイブノードライセンスは実際の機能としてはすべての機能を持つにも関わらず、通常のライセンスよりも低価格でご提供しております。
このスレイブノードライセンスですが、クラスタシステムに参加させずに独立したシステムとして60分以上稼動させるとメーカーのライセンス管理システムにライセンス違反ノードとして検知され、ライセンスが機能停止します。

つまり、クラスタライセンスを分解して使用することはできず、使用していないスレイブノードライセンスを独立して利用することもできません。ライセンスが機能停止した場合は、メーカーサポートによるリモートサポートが必要となります。
また、障害時やソフトウエアのアップデートのためにクラスタ構成を解消する場合、適宜インターネットから隔離するか60分以内にクラスタを再構成する必要があります。

ライセンスの違反について

SpamTitan は各種定義ファイルを取得する時に、ライセンス管理サーバーにアクセスします。
ライセンス管理は、ライセンスの認められない使用方法のほか、アカウント上限を超えてしまっても違反となります。
アカウントの上限による違反のみ、Webインターフェースから３回までリセットすることができます。（違反するとこのインターフェースが出現します）
何らかの受信者認証をしていない場合、Spam送信者が捏造した存在しないメールアカウントへのメールを受信してしまうと、すぐにアカウントの上限を超えてしまうので、何らかの受信者認証が必要です。

ライセンスの購入について

SpamTitanのライセンス形態は、サブスクリプションライセンスとなります。
価格はライセンス費用＋サポートサービスであり、サービス提供、サービス運用、メンテナンス費用ではありません。
この製品では、オンサイトサービスが付属しておりません。
サポートサービスの内容については、以下のURLを参照してください。

http://www.jtc-i.co.jp/support/specification/index.html

**※本SpamTitan Version7 のご紹介の文中における”ホワイトリスト/ブラックリスト”表記に関し、人種差別を表しているものではありません。
ご了承ください。**

ハードウエア・アプライアンスについて

SpamTitanジュピターコンパクトアプライアンスのご紹介

ユーザー数が１００人～７５０人程度のご利用環境で使用できるSpamTitanが予め導入された、1Uタイプのハードウエアアプライアンスです。
ライセンスが適用された状態でお手元に届きますので、設置後すぐにご使用できます。

ポイント！

ココがオススメ１

最新のバージョンが適用され、ライセンスが適用された状態でお届けします！
ライセンスは正規ライセンスと評価ライセンスをお選びいただけます！
※評価ライセンスの場合は、出荷＋輸送日数を引いた残日数となります。
　通常は20日前後となります。

ココがオススメ２

ライセンス未適用のコールドスタンバイをご用意できます！
障害時にはライセンスとバックアップをリストアして簡単復旧できます！

ココがオススメ３

障害時には、センドバック対応ができます！

弊社ではグラフィカルなネットワーク監視システムを取り扱っております。

無料で使用、評価できる製品を紹介しています。

詳しくは以下のURLからどうぞ！
http://www.jtc-i.co.jp/freeware/index.html

仮想アプライアンスについて

SpamTitan VMware 仮想アプライアンスのご紹介

ユーザー数が５０人～５０００人のご利用環境で使用できるSpamTitanが予め導入された、VMware社 ESXi仮想環境でご利用できる仮想マシンアプライアンスです。
メーカー謹製の仮想マシンで、OVFファイルで導入いたします。

ポイント！

ココがオススメ１
お手持ちのESXi 仮想環境をご利用できます！

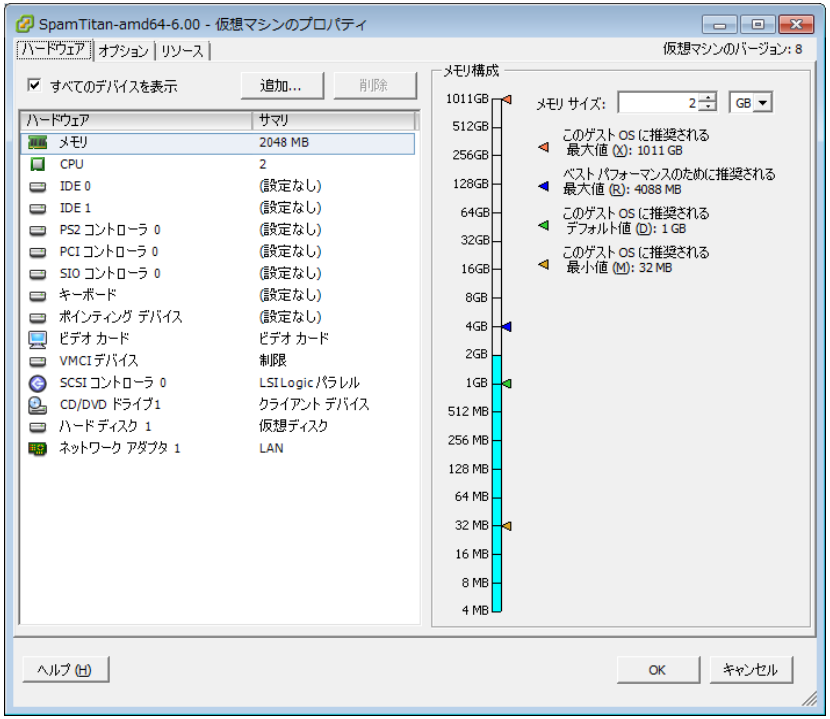
ココがオススメ２
SpamTitan のシステムイメージを簡単にバックアップできます！

ココがオススメ３
SpamTitan のシステムイメージを複数用意でき、しかも簡単に移設で来ます！

ココがオススメ４
性能が足りなくなっても、ハードウエアの交換を簡単に行うことができます！

ココがオススメ５
仮想環境ESXi側のパフォーマンスグラフで稼働状況を把握できます！

ココがオススメ６
SNMPポーリングにより一般的なネットワーク監視システムでハードウエアを監視できます！



弊社ではグラフィカルなネットワーク監視システムを取り扱っております。

無料で使用、評価できる製品を紹介しています。

詳しくは以下のURLからどうぞ！
http://www.jtc-i.co.jp/freeware/index.html

評価について

SpamTitan の評価リソースは、以下がご利用できます。

VMware社 ESXiですぐに試用できる仮想アプライアンスや、直接インストールできるISOイメージのダウンロード

弊社Webページ　ダウンロードサイト　https://www.jtc-i.co.jp/support/download/downloadlist.php

評価ライセンスのリクエスト

弊社Webページ　お問合せフォーム　https://www.jtc-i.co.jp/contact/scontact.php

お問い合わせ区分は「**トライアルキー請求**」をご選択ください。
評価ライセンスは、お申し込み当日から３０日です。発行は１～３時間かかる場合がございます。
評価ライセンスはメールで添付ファイルの形でお送りいたします。

下記の画面の「お申し込み」をクリックして頂いても、リクエストフォームの表示が可能です。

ご用命・お問い合わせは以下までお願いいたします。

JTC-i Jupiter Technology corp. ジュピターテクノロジー

Email info@jtc-i.co.jp
URL http://www.jtc-i.co.jp