

テストレポート 2007年11月

# SpamTitan for VMware

## バージョン 4.09

### アンチスパム技術レポート

## SpamTitan for VMware バージョン 4.09

### 開発元

社名: Copperfasten Technologies  
所在地: Storm House, Galway Business Park,  
Dangan, Galway, Ireland  
電話番号: +353 91 540054  
Web サイト: [www.spamtitan.com](http://www.spamtitan.com)  
製品: SpamTitan for VMware バージョン 4.09

### テスト機関

テスト実施機関名および所在地: West Coast Labs, Unit 9 Oak Tree Court, Mulberry Drive  
Cardiff Gate Business Park, Cardiff, CF23 8RS, UK  
電話番号: +44 (0) 29 2054 8400

日付: 2007 年 11 月  
号数 : 1.0  
報告者: Rob Tanner

### 連絡先

連絡先担当者: Rob Tanner  
電話番号: +44 (0) 29 2054 8400

# SpamTitan for VMware バージョン 4.09

## 目次

はじめに	4
テストネットワーク	6
テストの方法	7
製品テストの報告	8
Checkmark 証明書	9
製品について	10
インストールと設定	11
結果	15
終わりに	16
購買者のためのセキュリティ機能ガイド	17

## SpamTitan for VMware バージョン 4.09

### はじめに

### 依然として拡大するスパムの脅威

「2年後にはスパム問題なんて解決してますよ」ビル・ゲイツがそう宣言したのは2004年の1月だった。

2004年初頭、スイスで開催された World Economic Forum においてビル・ゲイツは自信満々の表情で上記のように「予言」した。残念ながら彼の「予言」は的外れに終わり、この問題の深刻さに警鐘を鳴らすような事例の報告が後を絶たない。

2006年の下半期、かつてないほどの大量のスパムが出回った。SurfControl 社がはじき出した数字によると同年の上半期に比べて50%増のスパムが検出されたことが報告された。今やインターネット上を流れるEメールトラフィックのほぼ90%がスパムであると言ってよいような状況となっている。

スパムの性質も変わってきた。2004年の時点では、スパムの大半がポルノかバイアグラの販売目的、あるいは悪名高い「ナイジェリアの手紙」と呼ばれる手数料詐欺を狙ったものばかりだった。こういったタイプのスパムはまだたくさん出回っているが、新たなフィッシングの手口として、事前に安く購入した株の株価を人為的に吊り上げ利ざやを短期間のうちに稼ぐ“Pump-and-Dump”と呼ばれるものや、ユーザーにURLのリンクを次々とクリックさせて特殊なコードをダウンロードさせるWebサイトへと巧妙に導いてゆきPC内の情報詐取を狙うものなどが出てきた。

スパマーが攻撃を仕掛ける際に使う手口も自ずと変わってきた。大量の未承諾Eメールの大部分は、「ボットネット」と呼ばれる非常に広範囲にわたって拡大している感染したPC群を介して送信されている。これらの感染PCのユーザーはホームユーザーであることが多く、彼らは自分が問題の一端を担わされていることすら気が付いていない。

この分散システムによるアプローチが取られるようになったことで、ネットワークベースの単純な条件式によるスパムメールの振り分けは難しくなり、アンチスパム技術を提供している企業はより洗練されたフィルタリングソリューションの開発に追われている。

## SpamTitan for VMware バージョン 4.09

SurfControl 社のエンジニアとして有名な Richard Cullen 博士は最近のインタビューで次のように語っている。「ここ数年でインターネット上の脅威を取り巻く状況は様相ががらりと変わりました。マルウェアによる攻撃は今や商業目的にすら使われており、小回りのよくきくネット犯罪組織が巨大なボットネット網を背景にスパム、フィッシング、DDOS、マルウェアなどによる攻撃を次々と仕掛けてきているのです。」

同時にスパマー達はアンチスパム対策をすり抜ける新たな手段を常に考えており、そのような手段の一つとして最近増加してきているのが画像スパムだ。これは、スパマーのメッセージがランダムな文字列内に含まれた画像付きの E メールとして送信され、最新ではないスパムフィルターを通すように設計されている。Gartner 社のセキュリティリサーチディレクターである Peter Firstbrook の報告によれば、画像スパムは 2006 年第 3 四半期には全スパムのうち 6%に過ぎなかったが、第 4 四半期には 30%に跳ね上がり、現在では 40%を占めるものと思われる。

ブロックが困難になったことは言うまでもないが、実際のところ画像スパムのメッセージはシンプルなテキストメッセージよりもサイズが大きくなるため、同時に別の問題を連鎖して引き起こしている。複数のレポートによれば、2006 年 9 月以降、平均的なスパムメッセージのサイズは 6.62Kb から 11.76Kb へと 77%増となり、さらに増大する傾向を見せている。スパムのサイズが増えたことにより無駄に使用される帯域が増えるため、Eメールの管理費が膨らみ、さらに企業サイドで受信メールの全アーカイブを作成する必要がある場合には記憶装置の使用域も増えてしまっている。

『ニューヨークタイムズ』誌のセキュリティコラム担当記者である John Markoff によれば、最近、あるボットネットの発生により、上記のような画像ベースのメッセージを水増しするランダムテキストを検索している間に Yahoo のリソースの 15%あまりが消費されるという事態に陥ったという。

この新たな脅威に対抗するため、アンチスパムソリューションの開発元は、画像スパムの特徴を分析するヒューリスティックルール技術などの既存技術の向上と光学式文字認識 (OCR) 技術などの新たなテクノロジーレイヤーの開発という両面での対策を講じる必要に迫られている。スパマーとセキュリティベンダーのいたちごっこに果して終わりはあるのだろうか？

## SpamTitan for VMware バージョン 4.09

### テストネットワーク

WCL は明らかにスパムといえるメッセージを収集するドメインを数多く所有している。これらのドメインでは様々なレベルのスパムを受信し、種々の E メール環境にも対応している。

企業環境内での E メール使用状況を反映させる目的で、各ドメイン内には数多くのユーザーアカウントを作成し、各種のニュースグループやメーリングリストへの参加を含む様々な E メール使用実例と需要を反映させている。メーリングリストで積極的に活動しているユーザーアカウントもいくつか作成した。

テスト目的で、ドメイン間で定義されたテスト要件に合致するレベルのスパムを受信するように指定したドメインを複数準備した。

テストプログラムで使用するソフトウェアソリューションは、ベンダーによって要求されている仕様の最小要件に適合するサーバー上にインストールし、アプライアンスベースのソリューションはベンダーの推奨配置図に基づいてネットワーク上に設置した。

ホスティングサービスを利用している場合をシミュレートするために、著名な E メールドメインを介してテストを実施し、MX レコードを変更してホスティングサービスから流れてくるメールストリームを転用した。

---

# SpamTitan for VMware バージョン 4.09

## テストの方法

WCL ではできるだけデフォルト設定のまま、ベンダーの推奨する設置・構成手順に沿った正しいオペレーションを確実にを行うために必要な設定のみをソリューション側で変更するという方式で最初のテストを実施した。

2 回目以降のテストは、開発元に相談しながらテスト中のソリューションの調整を行い、その指導のもとに実施された。WCL ではテスト実施日にはいつも 30 分ほどのわずかな時間をかけてソリューションを毎回微調整した。

テスト期間中は継続して、WCL によって管理されている E メールアドレスおよびドメインから様々な E メールがテストドメイン宛に送信され、実際のビジネスシーンでよく見られる E メールアクティビティ（例：会議の招集、グループへの通知、ビジネスには関係ない社交メールなど）が正確に再現された。

また、ビジネスには関係のない社交メールを送信してくる外部ユーザーや自宅で仕事を請負っているホームワーカーユーザーをシミュレートするために、Hotmail や Google の Gmail といった Web ベースのアカウントからも E メールが送信された。

このようにしてテスト期間中、スパム、メーリングリストやニュースグループからの転送メール、「正当な」個人用メールなど様々なメールをドメインで受信した。

## SpamTitan for VMware バージョン 4.09

### 製品テストの報告

製品の評価は運用/管理、機能性、性能およびその他の機能のテストの3つの分野に分けて行う。

#### 1. 運用/管理

- セットアップおよびインストール作業のしやすさ
- 使い勝手
- ログイングおよびレポート機能
- ルールの作成
- カスタマイズ
- 内容による分類項目

#### 2. 機能性

- Eメール処理の方法
- Eメールの許可/ブロック
- 検疫領域
- その他のレポート機能
- Eメール処理の手順
- Eメールアドレスによるブロック
- ブラックリスト/ホワイトリスト
- Eメールアドレスによる許可

#### 3. 性能

- 検出されたスパムの量または割合
- 正当な購読メール
- 誤って許可されたスパムメール
- ブロックされた正当メール
- ブロックされた誤検出メールの割合

## SpamTitan for VMware バージョン 4.09

### Checkmark 証明書

テストが全て終わると、個々の製品結果が分析され、スパムの捕捉率に基づいてアンチスパム製品に授与される以下の2種類の Checkmark 証明書のどちらかが認定される。

- 97%以上のスパム捕捉率が確認された場合  
Checkmark アンチスパム製品証明書プレミアム
- 90%以上のスパム捕捉率が確認された場合  
Checkmark アンチスパム製品証明書スタンダード



## SpamTitan for VMware バージョン 4.09

### 製品について

はじめに

SpamTitan は、インターネットと社内メールサーバー間の E メールトラフィックを様々な目的でフィルタすることができるため、エンドユーザーである企業にとって専用の E メール保護ソリューションとなりうる製品である。このソリューションを導入することによって、マルウェアやスパムを媒体とした脅威といった E メールベースの望ましくないコンテンツからネットワークを保護することができる。また、スパムエンジンの自動更新が標準装備されているために保守費用がほとんど掛からず、コスト削減効果が期待できる。

SpamTitan は ISO イメージとしても VMware 認定仮想アプライアンスとしても使用できる製品であり、どちらのオプションもインターネットからダウンロードする。今回のテスト用として WCL では VMware オプションを選択した。テストの主要目的は Checkmark アンチスパム製品証明書の認定評価を行うことである。



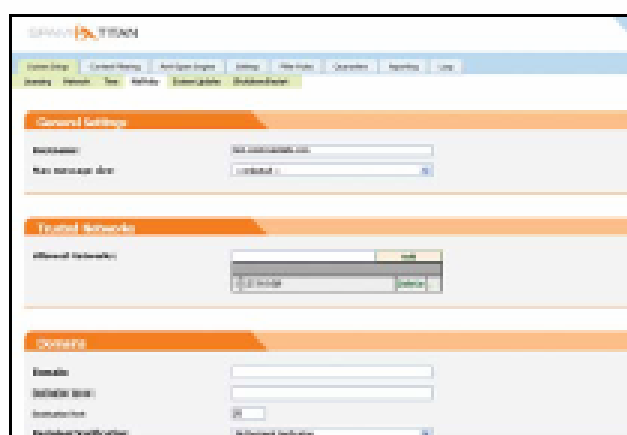
## SpamTitan for VMware バージョン 4.09

### インストールと設定

まず最初に、仮想アプライアンスをダウンロードし、VMware Workstation を実行している比較的低いスペックのコンピュータにインストールした。仮想マシンの起動シーケンスが完了すると、インストールウィザードが起動し、設定項目の入力に進む。この最初のインストール段階で入力する情報は、サーバーの IP アドレスやドメイン名などである。

物理アプライアンスや従来からある一般的なソフトウェアベースのソリューションとしてではなく、VMware 仮想アプライアンスとして展開することによって、評価/テストプロセスで扱いやすくなったのはいうまでもないことだが、ビジネスユーザーにとっても冗長性、バックアップのしやすさ、拡張性、可動性といった部分で実質的に使いやすさが向上するものと思われる。

次に、実際のインターネットドメインからスパムメッセージ、ハムメッセージ(正当なメッセージ)、グレーメッセージを含む全ての受信 E メールを社内の E メールサーバーに転送するように設定した。この設定は Web ブラウザを使用して管理コンソールにアクセスし、対応する社内 E メールサーバーの IP アドレスを入力することによって行った。

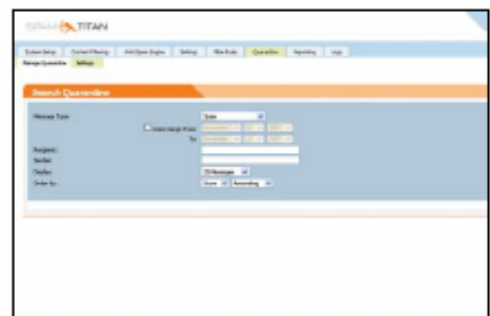


## SpamTitan for VMware バージョン 4.09

### 操作性および主要機能

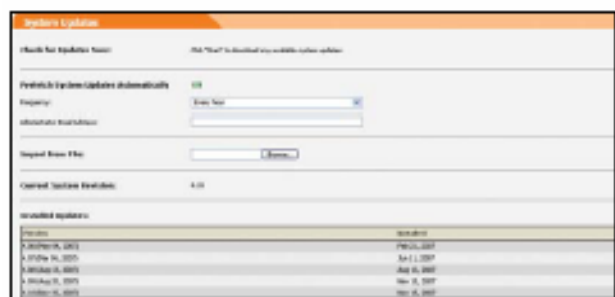
WCL では製品テストを行うにあたり、複数ドメインのサポート、エンドユーザーの検疫機能、ホワイトリスト/ブラックリスト、包括的な自動生成レポート一式など主要な機能と特長を特定し、確認した。

LDAP との統合、出入両方向での E メールスキャン機能、メッセージへの法的免責文言の追加機能、潜在的なポットネットソースの検出機能など、ビジネスユーザーにとって便利だと思われるその他の機能についても確認した。



WCL ではテストプロセス全体を通じて SpamTitan 付属のマニュアルを使用し、このマニュアルが分かりやすく正確であること、設定の指示が順を追って書かれていること、ヘルプやサポートガイドとして有用であることを確認した。

このソリューションの中核となるアンチスパム技術部分には、Kaspersky 社製および Clam 社製のマルウェア検出エンジンが組み込まれており、さらなる機能性の拡張と賞賛に値する性能が実現されている。



SpamTitan は「デフォルト状態でのセキュリティ」パラダイムを主眼に置いたソリューションであることも特記しておくべきであろう。このことは基盤となる OS として FreeBSD を採用している点やメールの中継用として信頼のおけるネットワークを構成する必要がある点によっても証明されている。

## SpamTitan for VMware バージョン 4.09

その他の特長の中で最も重要なことは、製品の配布方式によってもたらされていると行ってよいかもしれない。現在、VMware 認定仮想アプライアンスとして使用可能なものの中で、ソフトウェアパッケージとして売り出されている製品は比較的少なく、SpamTitanはそのうちの1つだ。

仮想マシン構造基盤を持つということは、ソフトウェアと物理アプライアンスの両方のメリットを併せ持っており、柔軟性が高く、すぐに使用可能状態となるソリューションであることを意味している。このことは、例えば、WCLで今回のテストを行う上でSpamTitanの配置や評価を行うためのOS基盤を別に構築したり構成したりする必要がなく、即テストを実施できたことによって示されている。

この事例において、VMware版を使用することのメリットは他にもある。まず、1台の仮想マシンを複数の場所へ配置し再利用することが簡単に行えること、本質的に複数の物理アプライアンスを配置するのと同様のバックアップ機能および冗長性オプションが用意されていること、ビジネスニーズの変動に応じて必要であればすぐに追加メモリやCPUリソースを簡単に割り当てることができる拡張性などである。

## SpamTitan for VMware バージョン 4.09

### レポート機能

WCL では内蔵の管理機能および SSL 暗号化されている Web ベースのコンソールを経由して提供されているレポート機能を活用した。

ダッシュボードと呼ばれる総合ページには、現在のリソース使用率の概要、出入両方向でのスパムメッセージの累積スキャン統計、直近のマルウェアのアクティビティ、現在のメールキューの詳細などが表示される。操作性の良い拡張レポート機能を使ってこのデータを補完することによって、システムアクティビティとEメールスループットの全履歴を追跡することができる。レポートは表形式とグラフ形式の両方をサポートしている。複数ドメイン環境においては、柔軟性を高める目的でドメインごとにレポートが生成されるようになっている。



WCL が確認したところでは、レポーティングエンジンは機能豊富で、非常に多くの管理オプションおよび設定オプションが存在し、どんなビジネス環境にも適応可能である。

---

## SpamTitan for VMware バージョン 4.09

### 結果

メールタイプ	「正当」と検出	「スパム」と検出
正当メール	100%	0%
スパムメール	1%	99%

テスト期間のパフォーマンスレベルは一貫して高かったことがわかる。SpamTitan が正しくスパムメールを捕捉した率は 99%であり、正当メールはすべて正しく受信した。

スパムメールを見分ける際には、ルールベースの分析と高度なベイジアンフィルタリングが組み合わされて用いられていることが確認された。また、画像スパムの判定には光学式文字認識(OCR)ソフトウェアが用いられていた。

上記の結果を鑑みて、WCL は謹んで SpamTitan for VMware に Checkmark アンチスパム製品証明書プレミアムを認定する。

## SpamTitan for VMware バージョン 4.09

### 終わりに

SpamTitan は、高度なスパム検出機能と使いやすさを融合した、パワフルでコスト効果の高いフレキシブルなソリューションであり、E メールを介した脅威の検出・保護に威力を発揮するプラットフォームとして役立つ製品であるといえる。拡張性と柔軟性が融合された設計は、規模を問わず全ての組織にメリットをもたらすであろう。

このソリューションは VMware 仮想アプライアンスとして配布されているため、インストール、管理、テスト、バックアップが非常に簡単である。場合によっては、従来どおりの物理アプライアンスやソフトウェアをインストールするモデルよりもずっとメリットが大きいといえる。使用する基盤システムをフレキシブルに選択でき、障害時の復旧も迅速に行えるためである。

高度な設定オプションと包括的なレポート機能についてわかりやすく書かれた詳細なマニュアルが付属しているため、新しいユーザーにとっても VMware 製品に親しんでいるユーザーにとっても単にセットアップがしやすいというだけでなく、SpamTitan を導入するすべての企業に最適な状態に適合させることができる。

# SpamTitan for VMware バージョン 4.09

## 購買者のためのセキュリティ機能ガイド

SpamTitan for VMware はスパム、フィッシング、ウィルス、迷惑メールなどから E メールを保護する仮想 E メールゲートウェイアプライアンスである。本製品は仮想アプライアンスとして配布されており、VMware 製品スイート上で実行可能であることが証明されている。

url : <http://www.spamtitan.com>

## SpamTitan for VMware バージョン 4.09

### 購買者のためのセキュリティ機能ガイド

ビジネス上のメリット     CopperFasten 社の報告より

SpamTitan はビジネスにおける有用性とコスト削減効果を高めるために、次の 3 点に重点をおいて設計された製品である。

#### 1. 購買価格

SpamTitan は、仮想アプライアンスとして配布することを前提とした優位な価格設定が行われているため、製品の購入から展開にいたるまでの間に大きなコスト削減効果がもたらされる。仮想アプライアンス方式が採用されているため、既存のハードウェアリソースを最大限に活用することが可能であり、それによる一層のコスト削減効果が期待できる。

#### 2. 保守費

SpamTitan は可能な限り保守費用を発生させないで運用できるよう設計されている。自動更新、バックアップ、レポート、通知などの機能により、経営/管理部門が介入しなければならないような機会は最小限に抑えられているため余計な出費はほとんど発生しない。

#### 3. 問題解決によるコスト削減

SpamTitan のスパム検出精度は非常に高く、優れたエンドユーザー管理ツールが付属しているため、Eメール使用に関して生産性が損なわれるという問題の大半は解決する。

## SpamTitan for VMware バージョン 4.09

### 購買者のためのセキュリティ機能ガイド

技術的なメリット      CopperFasten 社の報告より

SpamTitan はスタンドアロンのメールゲートウェイとして設計されており、専用のアンチスパムエンジンは 98.5%以上のスパム防御率、誤検出率は 0.03%以下という卓越した性能を誇っている。搭載されている Kaspersky 社製と Clam 社製のアンチウイルスエンジンは両方とも受賞経験のある優れたエンジンである。そのほか、エンドユーザーの検疫機能、完全に自動化されている一連のレポート機能、自動更新、ドメインごとのレポートおよび管理機能、LDAP との統合、ホワイトリスト/ブラックリスト、出入両方向でのメールスキャン機能、免責文言の追加機能、シンプルな展開および管理、画像スパムからの保護機能、ボットネット検出機能など機能性の高さを示す特長が多くある。このような高い機能性と仮想アプライアンスであることによって得られるメリットが相乗して、今日の E メール保護における問題の動的側面に対応するために必要な柔軟な管理を行うことができるようになっている。

url : <http://www.spamtitan.com/anti-spam/vmware/technicalspecifications>

## SpamTitan for VMware バージョン 4.09

### 購買者のためのセキュリティ機能ガイド

12 ヶ月間の開発成果 CopperFasten 社の報告より

この 12 ヶ月間以上にわたって、弊社では SpamTitan をさらに便利にする新機能と新たなアンチスパムルールセットの開発に取り組んできた。両方とも緊急を要する新手のスパム手口に対抗する能力を高め、管理者がこのような新たな手口の出現に対応できるようにすることを目的とした。

- 光学式文字認識(OCR)プラグイン 増大している画像のみのスパムに対抗する。このプラグインにより、画像ファイルに埋め込まれた特定のキーワードがチェックされる。
- オンデマンドの検疫レポート ユーザーからのリクエストによりオンデマンドで検疫レポートを生成できる。
- ペンパルホワイトリストの自動生成 ローカルユーザーによって指定したアドレスに送信されたことのあるメッセージに対する返信メッセージに対するスパムスコアが下がる。これにより、ユーザーが頻繁に連絡を取っている E メールアドレスからの誤検出を防ぐことができる。
- 検疫メールビューワーの[View Source(ソースの表示)]タブ フォーマットされていない生のメッセージソースを確認できる。
- スпам検疫の削除レベルの設定 管理者はスパムの検疫ポリシーを設定すると同時に指定レベルを超えるスコアのメッセージを削除することができる。このポリシーはドメインごとでもユーザーごとでも設定可能である。
- 設定時にドメインリストをインポートする機能 これはとりわけ数百あるいは数千のドメインを扱うサイトにインストールする場合に有用である。

## SpamTitan for VMware バージョン 4.09

- メールキューの管理機能 メールキューが発信される際にメッセージの表示、保留、リリース、削除が実行できる。
- スпамメッセージの件名にスパムスコアを付加 ポリシーが「Tag and Pass(タグを付けて通過)」の場合に、転送されるスパムメッセージに適用される。
- 検疫済みメッセージを個人用の E メールアドレスに転送 詳細を調べるために管理者のみに許可される行為。検疫メールビューワーから直接メッセージをリリース、削除、ホワイトリストへ登録することも可能。
- ボットネット検出プラグイン スпамボットネット経由でメッセージを受信した場合、アンチスパムスコアリングシステム全体に影響を与えるボットネットを指定する。

## SpamTitan for VMware バージョン 4.09

### 購買者のためのセキュリティ機能ガイド

その他の特記事項      CopperFasten 社の報告より

SpamTitan for VMware について特筆すべきことは、その配布方式とそれを採用したことによって得られるメリットだ。厳密に言えば本製品はソフトウェアなのだが、仮想アプライアンスとして配布されている。SpamTitan は世界的に見ても数少ない VMware 認定仮想アプライアンスのひとつだ。仮想アプライアンスはソフトウェア配布の利点と物理アプライアンスの利点の両方の恩恵を得ることができる。物理アプライアンスの「プラグアンドプレイ」によるメリットに加えて、従来どおりのソフトウェア配布による柔軟性の両方が実現されたといえる。OS の構築やインストールが不要であるということは、そのことを示す好例である。VMware スイート製品を使用すると、SpamTitan を既存のサーバー上の仮想マシン内で実行されている仮想アプライアンスとして公開し、稼働させることができる。ネットワーク上では他の物理アプライアンスと同様に認識される。ユーザーは物理アプライアンスにアクセスするときと同じ方法で、Web ベースの GUI を経由して SpamTitan にアクセスする。ユーザーは VMware を使ってこの仮想アプライアンスに割り当てるリソース メモリ、CPU、ディスク領域などを指定できる。

この配布方式は、ユーザーに従来のソフトウェアや物理アプライアンスでは考えられない大きな恩恵 とりわけ柔軟性に関わる恩恵をもたらす。製品がダウンロード方式で配布されているため、すぐに試用してみることができ、試用結果のコピーをファイルとして保存することも可能だ。OS やサーバーを構築する手間も必要ない。ネットワークを通じて世界中のオフィスに配布することもできる。通常であればバックアップ用の物理アプライアンスを必要とするような作業であるが、VMware 製品を使えばバックアップを取ったり復元したりといった時間のかかる作業も数分で可能だ。また、SpamTitan 仮想アプライアンスは必要に応じてスケールの調整ができる。メールの量が増えてきたため使用中の仮想アプライアンスにもっとメモリや CPU を多く割り当てる必要が出てきたとき、キーボードを数回叩くだけで簡単にメモリや CPU の割り当てを増やすことができるのだ。

westcoast labs

翻訳

ジュピターテクノロジー株式会社

〒183-0055

東京都府中市 1 - 1 - 5 府中高木ビル 5F

TEL : 042 - 358 - 1250

FAX : 042 - 360 - 6221

URL : <http://www.jtc-i.co.jp>