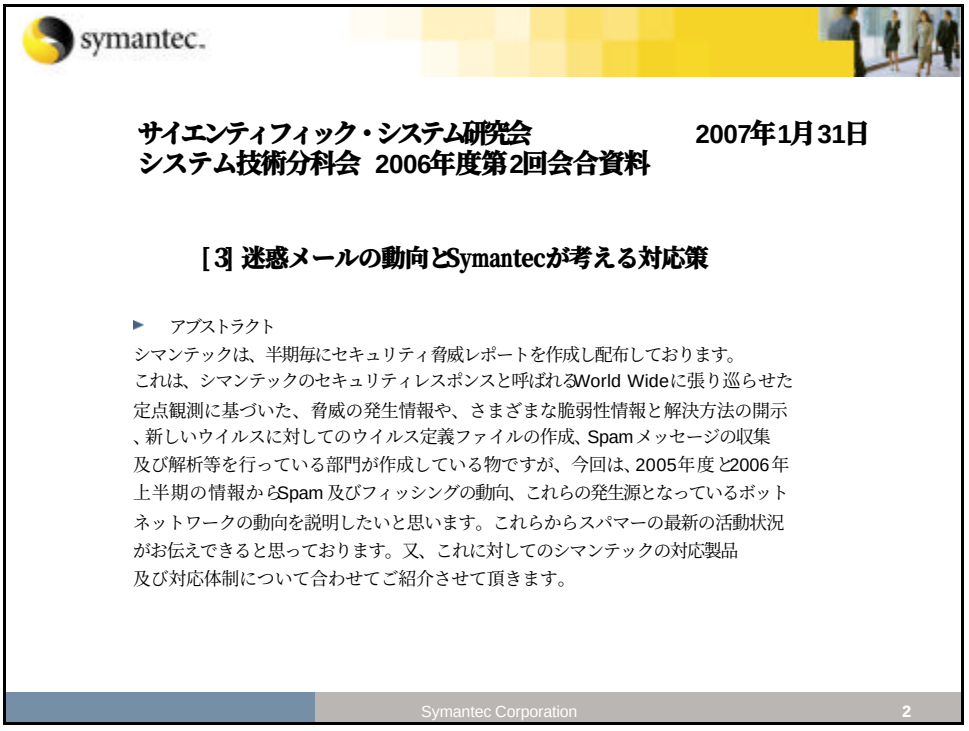
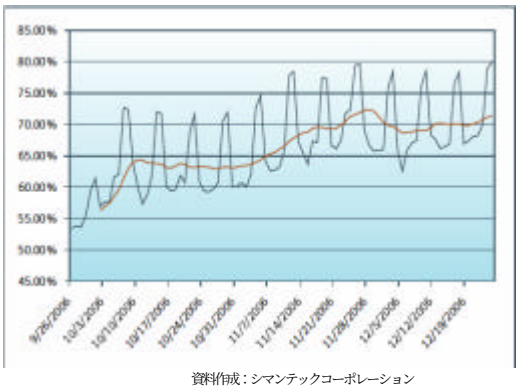

symantec.
システム技術分科会第2回会合
迷惑メールの動向とSymantecが考える対応策
株式会社シマンテック
システムエンジニアリング本部
エンタープライズSE部
エンタープライズSE第2グループ
安元　英行


symantec.
サイエンティフィック・システム研究会　　2007年1月31日
システム技術分科会　2006年度第2回会合資料
[3] 迷惑メールの動向とSymantecが考える対応策
アブストラクト
シマンテックは、半期毎にセキュリティ脅威レポートを作成し配布しております。
これは、シマンテックのセキュリティレスポンスと呼ばれるWorld Wideに張り巡らせた
定点観測に基づいた、脅威の発生情報や、さまざまな脆弱性情報と解決方法の開示
、新しいウイルスに対してのウイルス定義ファイルの作成、Spamメッセージの収集
及び解析等を行っている部門が作成している物ですが、今回は、2005年度と2006年
上半期の情報からSpam及びフィッシングの動向、これらの発生源となっているボット
ネットワークの動向を説明したいと思います。これらからスパマーの最新の活動状況
がお伝えできると思っております。又、これに対してのシマンテックの対応製品
及び対応体制について合わせてご紹介させて頂きます。
Symantec Corporation
2

Agenda

- スパムの現状
  - 近年における電子メール全体に占めるスパムの割合
  - スパムの種類
  - イメージスパムの増加及びその手法
  - スパム発信元情報
  - ボットに感染したコンピュータの割合上位10カ国
  - 何故、ボットが脅威なのか？
  - 悪意コードを含むスパムについて
  - Webブラウザの脆弱性の遷移
  - スパムに対しての考察
- フィッシングの現状
  - フィッシングの現状
  - 業界別のフィッシングの活動
  - Symantec のフィッシング対応状況の考察
  - フィッシングに対しての考察
- 製品のご紹介

近年における電子メール全体に占めるスパムの割合



資料作成：シマンテックコーポレーション

補足：

近年における電子メールトラフィックに対してのスパムメールの割合。

2005年　上半期：61%　下半期：50%

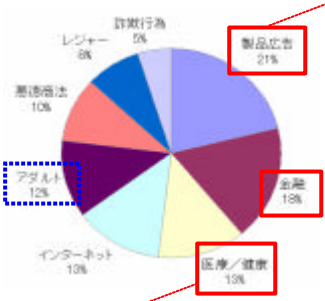
2006年　上半期：54%　下半期 12月中旬時点で７０%強。ピーク時は、80%に達していた。

２００６年上半期までは、右肩下がりの傾向であったが、２００６年下半期の状況では、グラフの通り右肩上がりの傾向になっている。

スパムの種類　2005年下半期と2006年上半期）

日本国内における2005年下半期の分類

一般的な品物の販売もしくは品物の広告する品物
およびサービスに関するスパム。
例: プリンタ消耗品、宝石・貴金属、
コンシューマ製品等

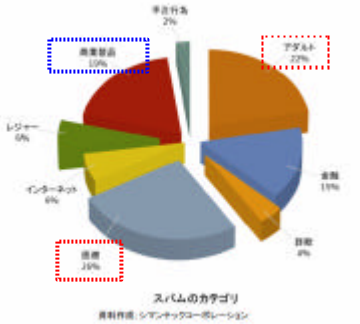


投資、株式市場あるいは他の金
融不動産の勧誘に関するスパム
例：投資、信用調査報告書、不
動産、ローン

健康食品や健康グッズ販売、サービスに関スパム。
例:健康食品、調合薬、医療(薬草療法)サービス

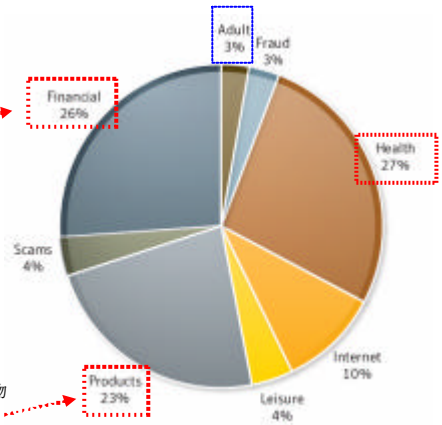
Symantec Security Update 2005 : Japan Spam by type, December 2005

World Wideにおける2006年上半期の分類



スパムの種類　2006年下半期）

World Wideにおける2006年下半期の分類



投資、株式市場あるいは他の金
融不動産の勧誘に関するスパム
例：投資、信用調査報告書、不
動産、ローン

健康食品や健康グッズ販売、
サービスに関スパム。
例:健康食品、調合薬、医療
(薬草療法)サービス

一般的な品物の販売もしくは品物
の広告する品物
およびサービスに関するスパム。

イメージスパムの増加 （2006年下半期）

World Wideにおける2006年下半期のイメージスパムの電子メール全体に占める割合

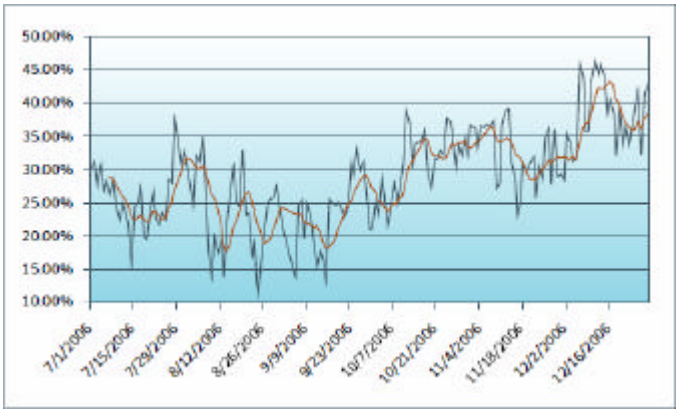


Image Spam Techniques – Jig Saw Background

Notes

- 光学式文字認識フィルタをから免れる手法となります。
- 背景を変える事で複数のパターンのSpamメッセージが用意に作成できます。

Image Spam Techniques – Large randomized border

Image Spam Techniques – “Mr. Ransom”

Enlargement

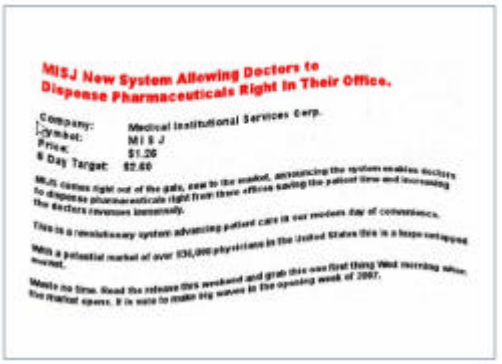
On

www.usably.net

Notes

- 各々の文字をイメージ化しサイズもばらばらにする事にてフィルタ処理を難しくさせます。

New Image Spam Techniques No1
“Captcha” Image Spam



Notes

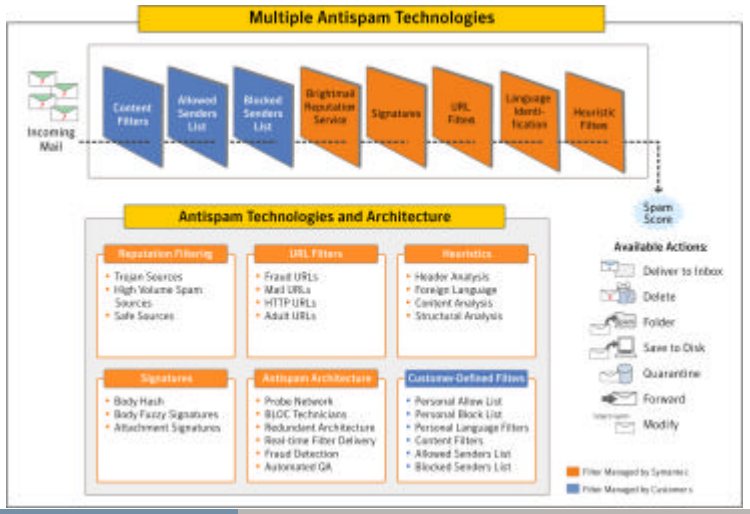
- 光学式文字認識フィルタをから免れる手法となります。

New Image Spam Techniques No2
Newsletter and Advertisment “Injection”

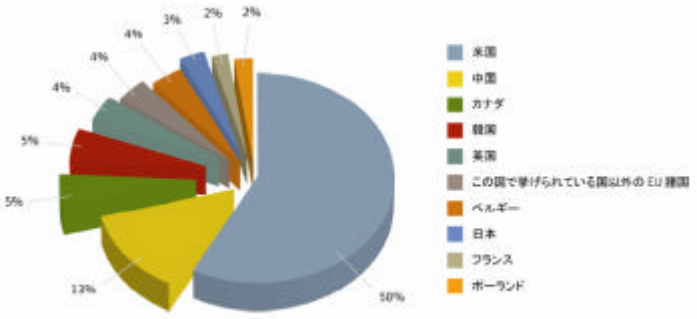
Notes

- 広告メッセージの中にNewsletter等を挿入する事にてSpamの判定をごまかす手法

Filtering Overview



スパム発信元情報



スパム発信数上位 10 か国
資料作成：シマンテックコーポレーション

- 中国からの発信が増加している。
- これは、ボットに感染したコンピュータの多い国にリンクしている。

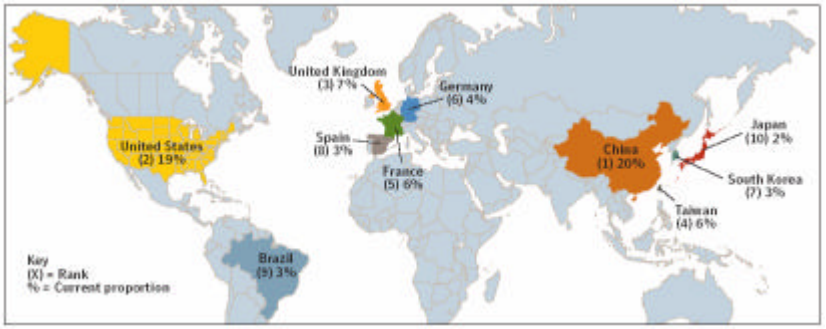
ボットに感染したコンピュータの割合上位10カ国（2005年度版）

- 日本もTOP１０に入っている。

2005年7月～12月 最新のランク	2004年1月～7月 前回のランク	国 別	2005年7月～12月 ボットに感染したコンピュータの割合	2005年1月～7月 ボットに感染したコンピュータの割合
1	2	アメリカ	26%	19%
2	1	イギリス	22%	32%
3	3	中国	9%	7%
4	6	フランンス	4%	4%
5	4	韓国	4%	4%
6	5	カナダ	4%	5%
7	7	台湾	3%	2%
8	9	スペイン	3%	3%
9	8	ドイツ	3%	4%
10	10	日本	2%	3%

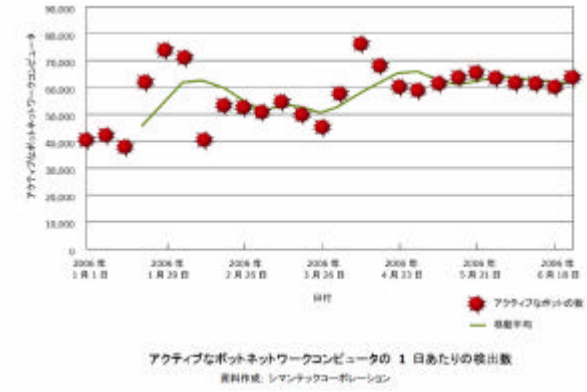
ボットに感染したコンピュータの割合上位10カ国（2006年度上半期）

- 中国が格好の標的になっている。
- 日本は横ばい



Source: Symantec Internet Security Threat Report 2006 Jan-Jun

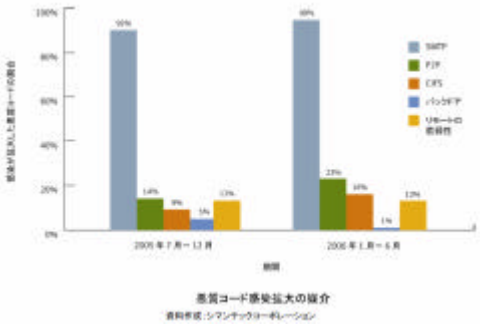
何故 ボットネットが脅威なのか？ その1)



- 2006年上半期に検出されたボット感染コンピュータは、一日平均 57,717台に達している。
- 2005年下半期の同様な値は、9,163台
- ボットをコントロールしているサーバは、6,337台。

何故 ボットネットが脅威なのか？ その2)

- **悪質コードの感染拡大の媒体としては、CIFS及びSMTPを使用していたが、Mytobは、感染拡大の媒介として SMTPとリモートで悪用可能な脆弱性を中心的に使用するボットである。**
- **MytobやZotobの作成者は、クレジットカード詐欺のツールとしてこれらのボットを作成している。**

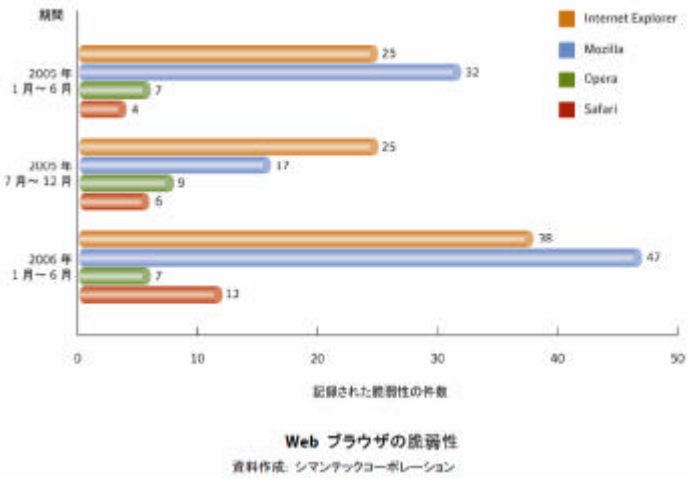


悪意コードを含むスパムについて

- **悪意コードを含むスパムの割合の変化**
  - 2006年上半期　：0．81%

    これは、スパム122件に1件の割合となる。
  - 2006年　年明け：1．27%
  - 2006年　6月：0．56%
- **減少理由**
  - 悪質コードが含まれているとさまざまな対策に対してブロックされてしまう。
  - URLを本文に含むケースが増加している。
  - ユーザのWebブラウザーの脆弱性を悪用するケースが増えている。

Webブラウザの脆弱性の遷移（参考資料）



スパムに対しての考察

- 手法の回帰現象
  - イメージスパムの復活
  - 本文へのURLの挿入
- ターゲットカテゴリーの変化
- 新しい手法？
  - ミスリーディングアプリケーション
    - ユーザのシステムに発見されたセキュリティ上の脅威について、虚偽または誇張した情報を提供し、その「脅威」を取り除くという主旨で、セキュリティソフトウェアの購入やバージョンアップをユーザに促し、その代金を獲得しようとする類である。この購入行為時に銀行口座、クレジットカードなどの個人情報を開示するとID情報の盗難、クレジットカード詐欺等の犯罪に悪用されるおそれがある。
  - DHAとDos攻撃の複合型
  - Subjectを複数行使用するメッセージ
    - システムがSpamと判定後にSubjectに文字を挿入する事を見越した配信方法。

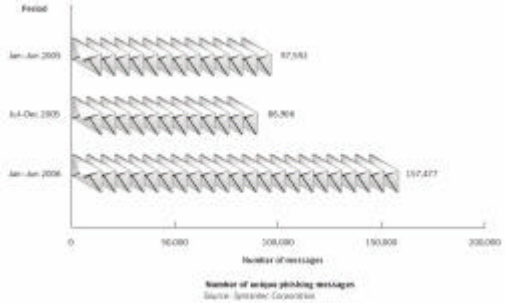
フィッシングの現状

2005年度のシマンテックの情報：

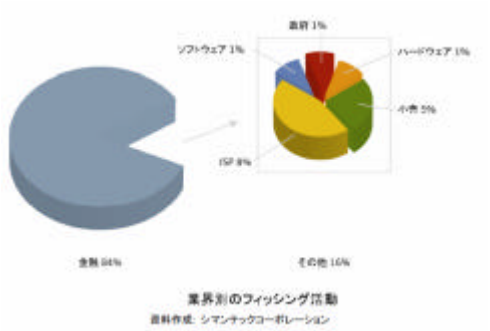
- **下半期に処理したメッセージ全体の0．８４%がフィッシングであった。**
  - **これは、メッセージの119通に1通の割合でフィッシング目的のメッセージが存在する事を意味する。決して少ない数値ではない。=>対策が必要。**
  - **ちなみに上半期は、125通に１通の割合であった。増加傾向にあるのは明らか。**

2006年度のシマンテックの情報：

- **2005年下半期に対し81%増加の固有な157,477ものフィッシングメッセージを検知した。**
- **84%が金融マーケットをターゲットにしている。**
- **増加の要因として、たくさんのドメインを用意して頻繁にURLを変更している等が考えられる。**



業界別のフィッシングの活動



業界別のフィッシング活動

資料作成：シマンテックコーポレーション

ランク	フィッシング攻撃の標的となったブランド
1	chase.com
2	paypal.com
3	ebay.com
4	bankofamerica.com
5	wellsfargo.com
6	barclays.co.uk
7	hsbc.com
8	premierbank.com
9	volksbank.de
10	wamu.com

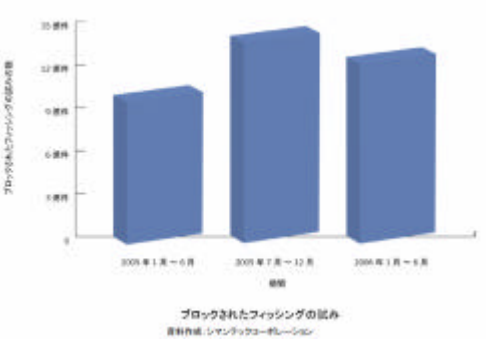
フィッシング攻撃件数上位 10 種のブランド

資料作成：シマンテックコーポレーション

特徴

- 当然とは言えるが、金融業界が依然ターゲットである。
- WorldWideではあるが、標的にされたサイトの多くが金融業界である。第 3位のebayも第2位のpaypalと同時に使用しているケースが多い為と見てる。
- フィッシングは、リテラシー教育も必須である。

Symantecのフィッシング対応状況の考察



ブロックされたフィッシングの試み

資料作成：シマンテックコーポレーション

考察

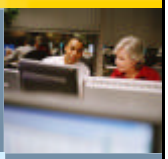
- 前頁での説明の通り、フィッシングは増加傾向である。
- Symantecとしてブロック件数が減少しているのは、フィッシャーが送信対象を絞り込んで送信している事が起因していると考えている。
- スピアフィッシングの増加？

フィッシングに対しての考察

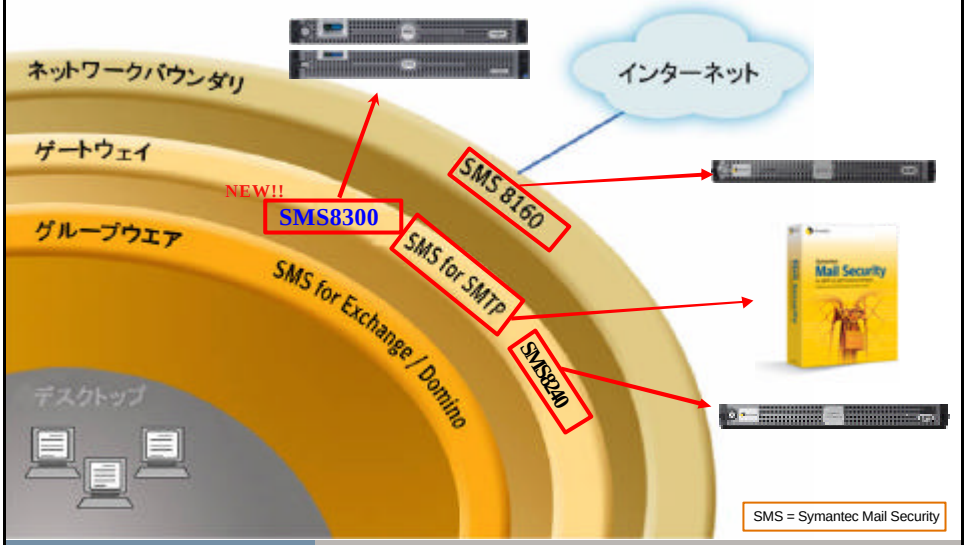
- 物理予防策
  - MTAレベルでのフィルタリング
  - IPベースでのフィルタリング
  - HTTPフィルタリング
  - DNSブロックリスト
  - ドメイン認証
- リテラシー教育
  - フィッシングにかからない為の教育

Enterprise Messaging Security

メールセキュリティ製品とスパム解析機関について

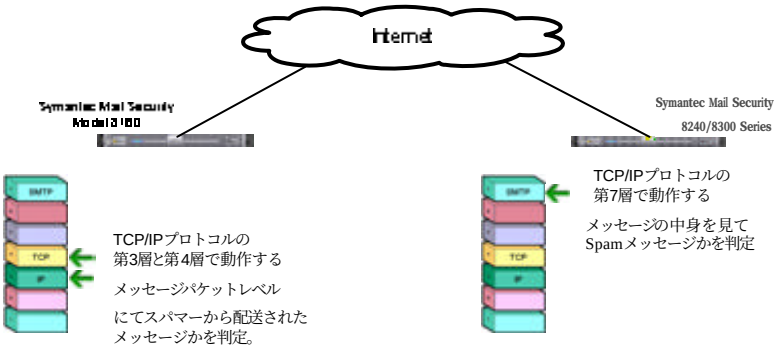


マルチレイヤにおけるEメールセキュリティソリューション



SMS8160とSMS8240/8300シリーズの相違点

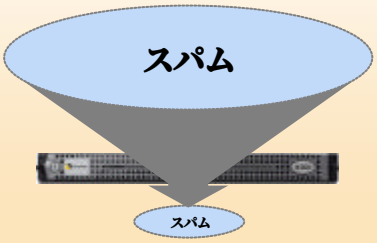
- パケット対メッセージ（AntiSpam機能）



SMS8160とSMS8200/SMS8300シリーズの特長

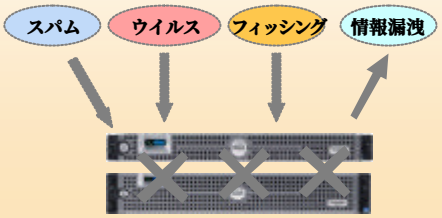
SMS8160

スパムメールを独自のトラフィックシェーピング機能を使用し大幅にスパムを削減します。
(2000名以上の組織・大規模ネットワークに有効)

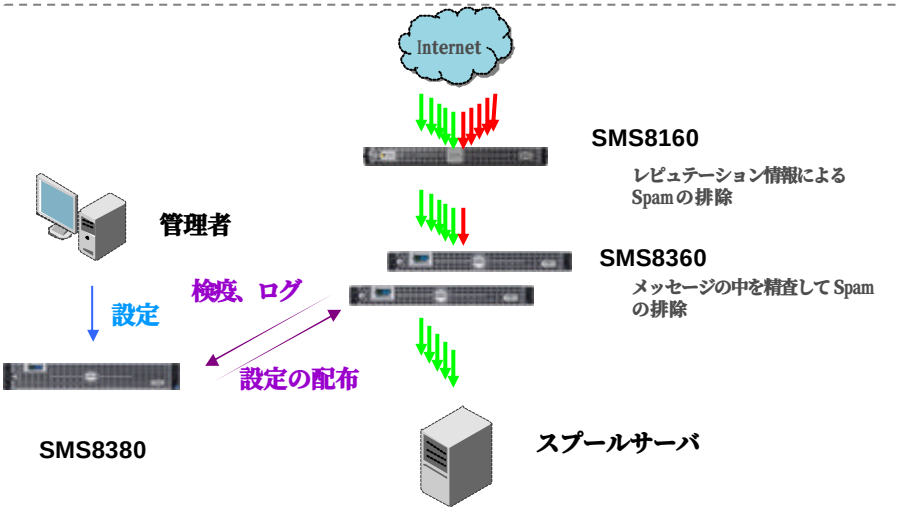


SMS8200/SMS8300シリーズ

アンチスパムだけでなく、アンチウイルス、Eメールファイアウォール、コンテンツコンプライアンスフィルタ等を使用し、Emailに関連するあらゆる脅威から守ります。

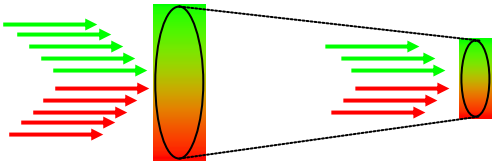


SMS8160とSMS8200/SMS8300シリーズの特長 その2)



SMS 8160の通信制御方法の有効性 -1-

SPAMにおける、通常の帯域制御ツールの限界

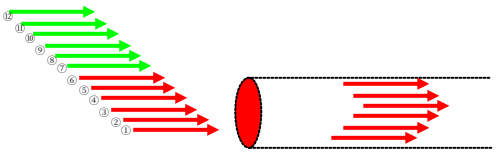


仮に10分の1に帯域を制御することで
サーバへの負荷は低減できるが、
本来正常に届くべきメールが遅延する結果となります。

通常メール
SPAMメール

SMS 8160の通信制御方法の有効性 -2-

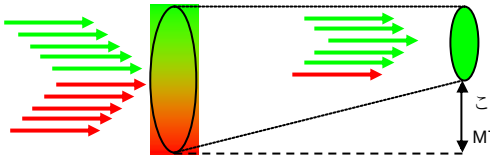
SPAMにおける、通常の帯域制御ツールの限界



帯域制御は通常通信が早く届いたものから
優先に帯域を割り当てられる為、
SPAM送信者が常に大量のSPAMを送信し続けた場合
SMTP帯域全てがSPAMに汚染される可能性があり
通常メールが大幅に遅延する可能性があります。

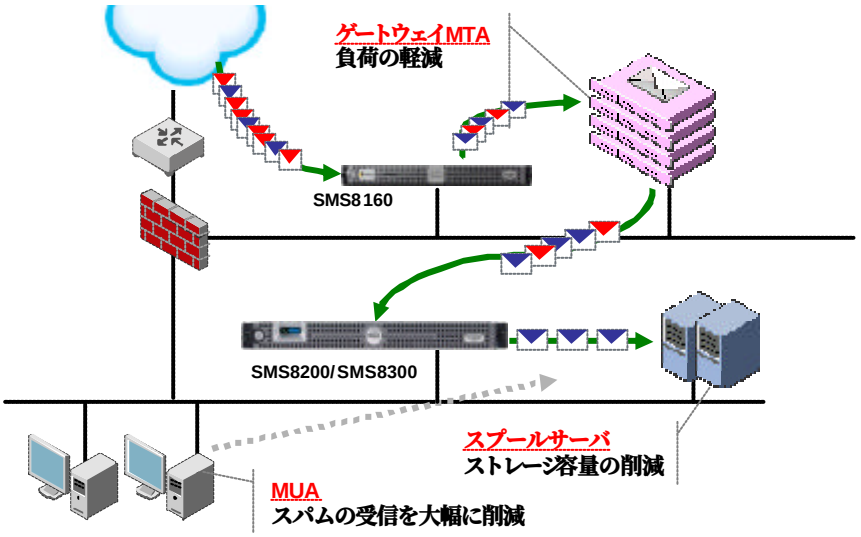
SMS 8160の通信制御方法の有効性 -3-

理想的な帯域制御

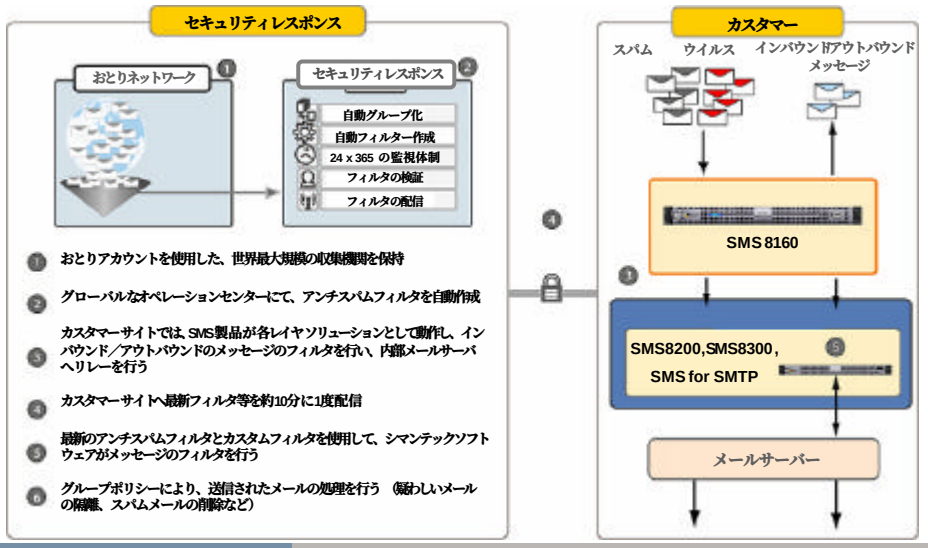


SPAM送信元を判別しSPAM送信元からの
通信だけ帯域制御を行い、残りの帯域全てを
正常メール配信に割り当てることが可能であれば
有効な帯域活用が行う事が可能となります。

SMS8160とSMS8240/8300との組み合わせ配置例



ハイレベル・アーキテクチャ



1. おとりアカウントを使用した、世界最大規模の収集機関を保持
2. グローバルなオペレーションセンターにて、アンチスパムフィルタを自動作成
3. カスタマーサイトでは、SMS製品が各レイヤソリューションとして動作し、インバウンド／アウトバウンドのメッセージのフィルタを行い、内部メールサーバへリレーを行う
4. カスタマーサイトへ最新フィルタ等を約10分に1度配信
5. 最新のアンチスパムフィルタとカスタムフィルタを使用して、シマンテックソフトウェアがメッセージのフィルタを行う
6. グループポリシーにより、送信されたメールの処理を行う（疑わしいメールの隔離、スパムメールの削除など）

ウイルス / スパム解析機関 - シマンテックセキュリティレスポンス

① おとりネットワークでは、1日あたり約3,000万通のスパムを収集
② 1日あたり、平均15,000のフィルタを作成し配信
③ 日本語スパム・フィッシングにも完全対応

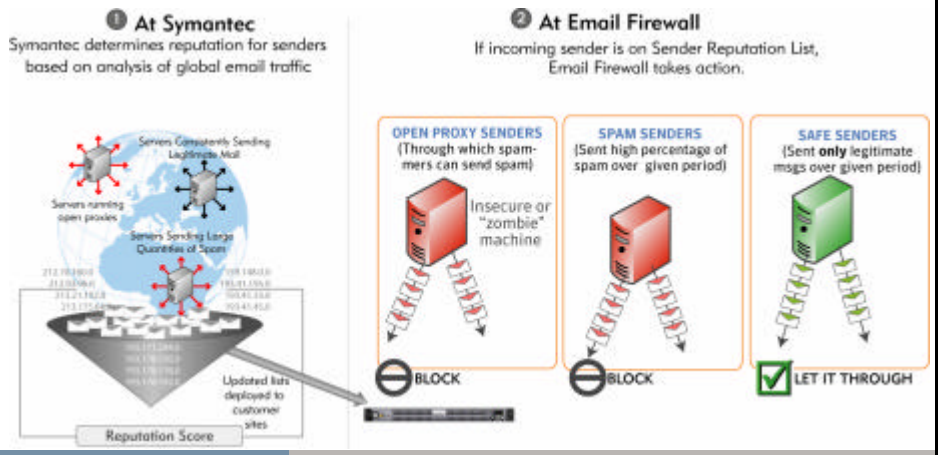
ウイルス解析機関

- 6つのセキュリティレスポンスセンター
- デジタル免疫システムインフラ
  世界中に１２０万以上のシステム
- 45ヶ国以上
- 24時間 x 365日での有人対応

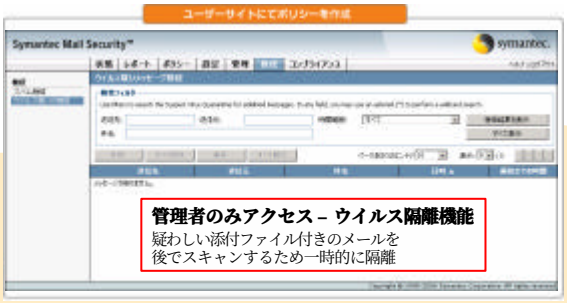
スパム解析機関

- 4つのアンチスパムに特化したレスポンスセンター
- 300万以上のデコイアカウントを保有
- 1日につき、数千万通のメールを収集
- 1時間おきにレピュテーションフィルタをアップデート

グローバルデータの活用: 送信者レピュテーションリスト



ゼロデイ "ウイルス プロテクション



- おとりネットワークでトラフィックを分析
- 早期段階でウイルスを検知
- "サスペクトウイルス シグネチャ"を作成・配信
- 疑わしき添付ファイルのあるメールを隔離
- 定義ファイルを受け取り次第、再スキャンしリリース
- その他のポリシー：削除、添付を外す、アラートを送信

用語説明　　(文責:SS研事務局)

【P.18】

CIFS(Common Internet File System) :
　Windowsのファイル共有サービスで利用されているプロトコルのSMB(Server Message Block)を拡張し、Windows以外のOSやアプリケーションソフトでも利用できるよう仕様を公開したもの。

SMTP(Simple Mail Transfer Protocol) :
　サーバ間でのメールのやりとり、クライアントがサーバにメールを送信する際に用いられるプロトコル。

【p.21】

DHA(Directory Harvest Attack ディレクトリ獲得攻撃) :
　スパマーがspam送信先のアドレスが実在するかどうかを確認するために、生成したアドレスをドメインに送信すること。

DDoS攻撃 (Distributed Denial of Service attack) :
　攻撃の踏み台になった複数のコンピュータが、標的とされたサーバ等に対して攻撃を行うこと。

【p.25】

MTA(Mail Transfer Agent) :
　MTAは SMTP(Simple Mail Transfer Protocol)を使用してホスト間でメールを転送する。

【p.34】

MUA(Mail User Agent) : メーラー(電子メールソフト)のこと。

【p.36】

デコイ : おとり