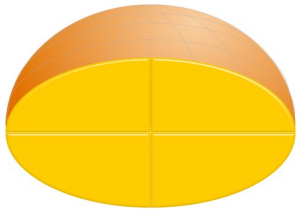
複合型脅威に対処するための トータルセキュリティ対策

（2006年7月14日）

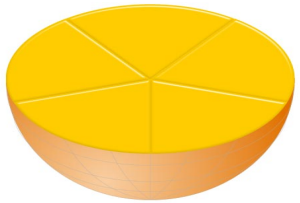
株式会社シマンテック
ソリューション営業統括本部
飯田　律子

会社紹介

情報セキュリティ　＋　情報可用性　＝　情報の完全性



Information
Security



Information
Availability

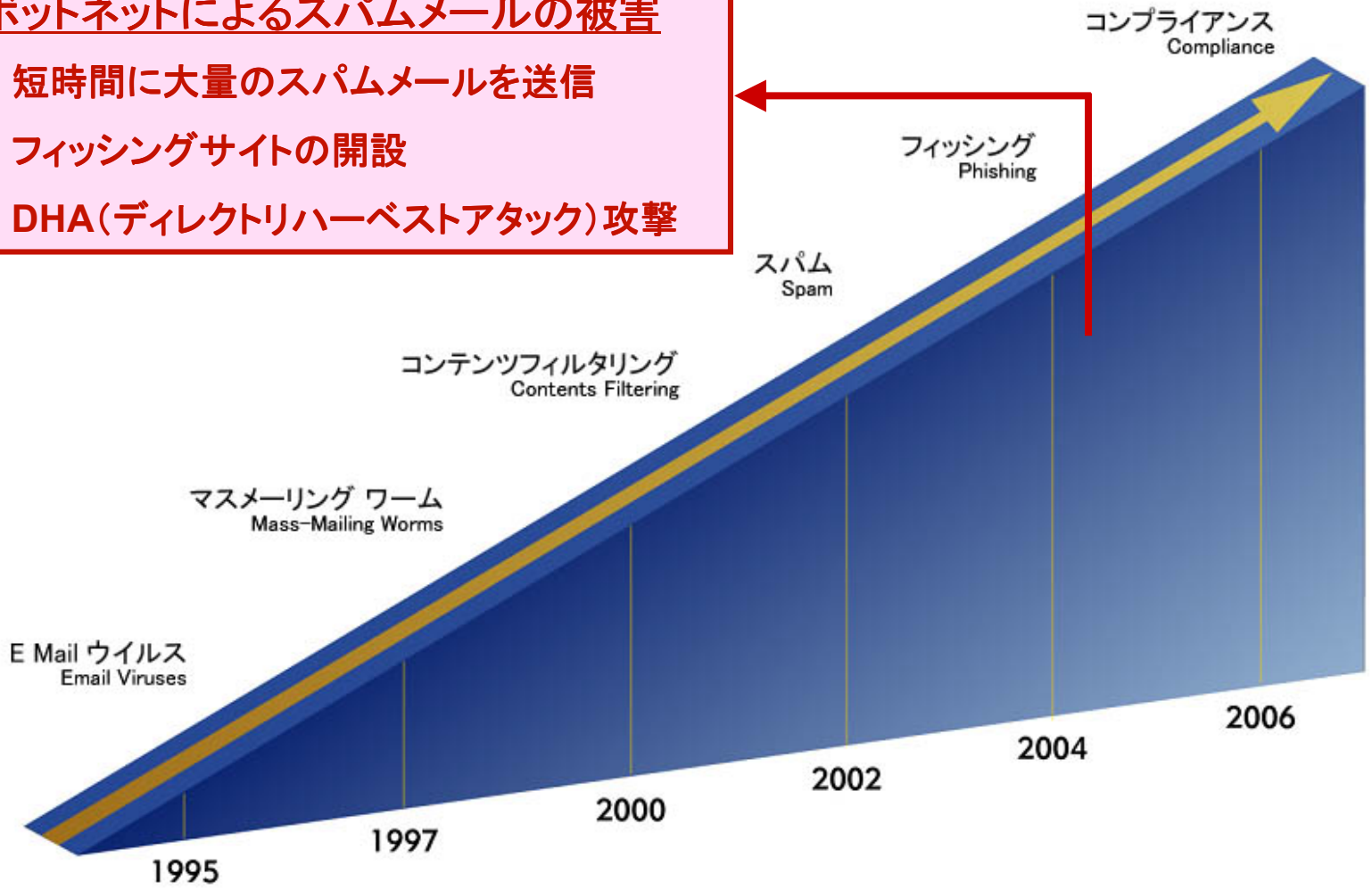
Information
Integrity

（1）メールの脅威

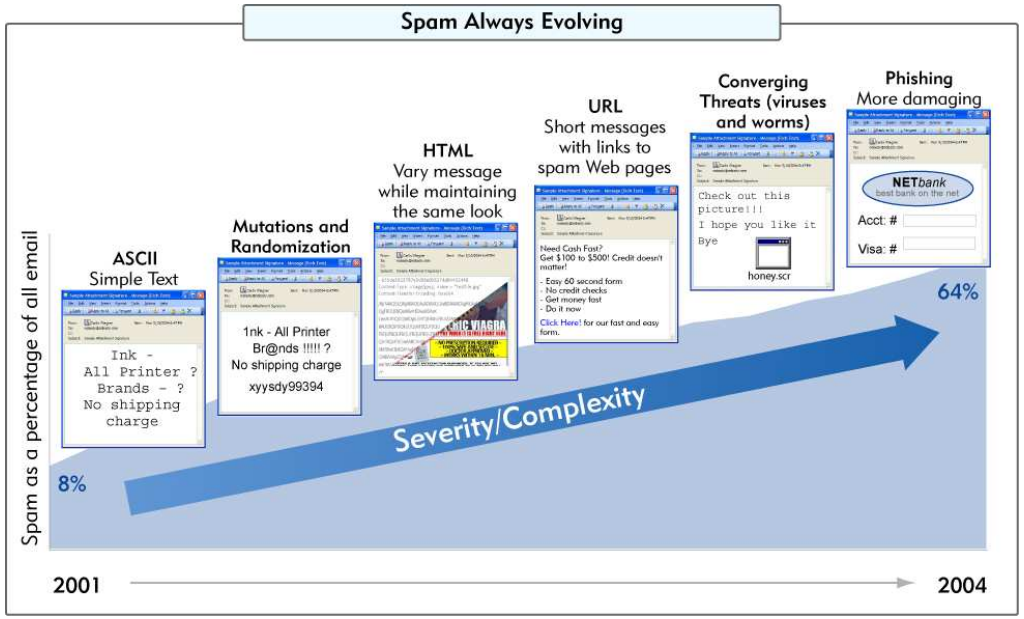
メール環境におけるキーワード

ボットネットによるスパムメールの被害

- 短時間に大量のスパムメールを送信
- フィッシングサイトの開設
- DHA（ディレクトリハーベストアタック）攻撃



スパムメールの進化



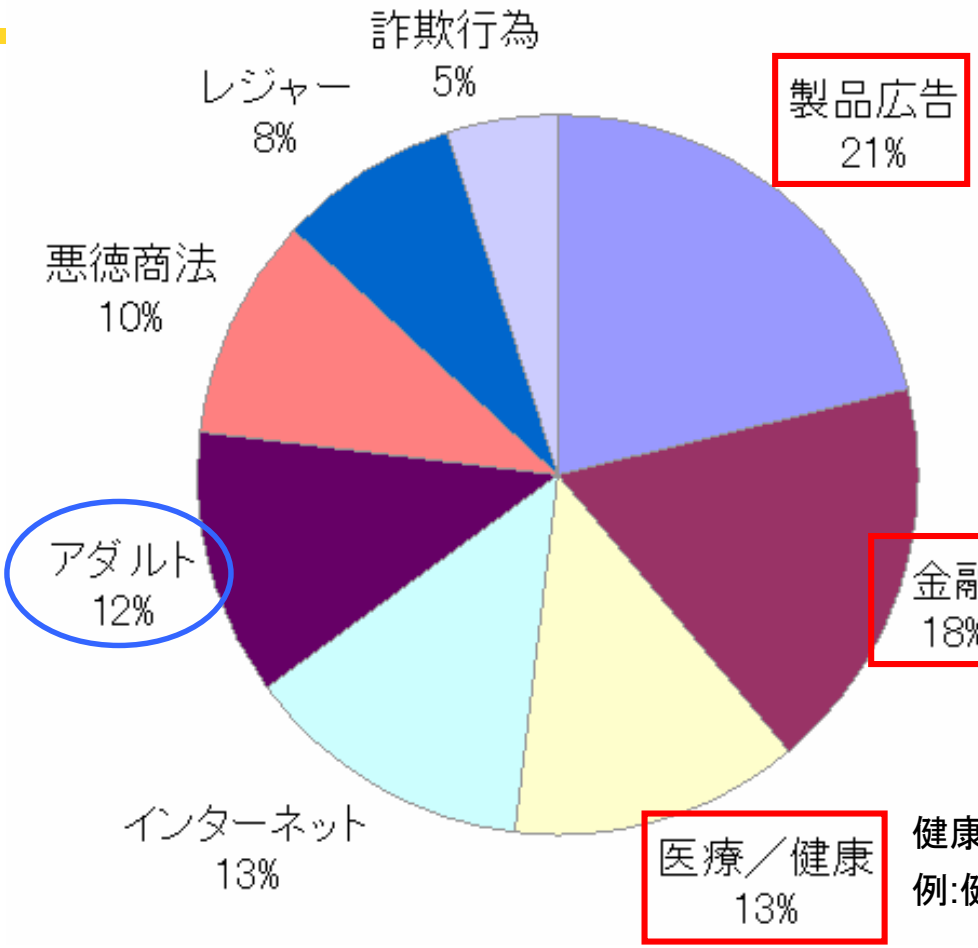
スパムメールの現状

- 米国ではスパムメールが全体の80%～85%を占める。
- ヨーロッパでは、 50%～60%
- アジア太平洋地域　40%～50% 急速に増えている。
- 国内の大手ISPでは、50%を超えている状況。

スパムメールによる被害の現状

- **500億ドル**：年間に要したスパムメール対策費用
- **メールボックスあたり170ドル**：
  米国企業の年間のスパムメール対策コスト
- **ユーザー人あたり年間718ドル**：
  手動でスパムメールを振り分けるコスト

日本国内におけるスパムの種類（2005年12月）



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・機会に関するスパム。
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、サービスに関するスパム。
例:健康食品、調合薬、医療(薬草療法)サービス

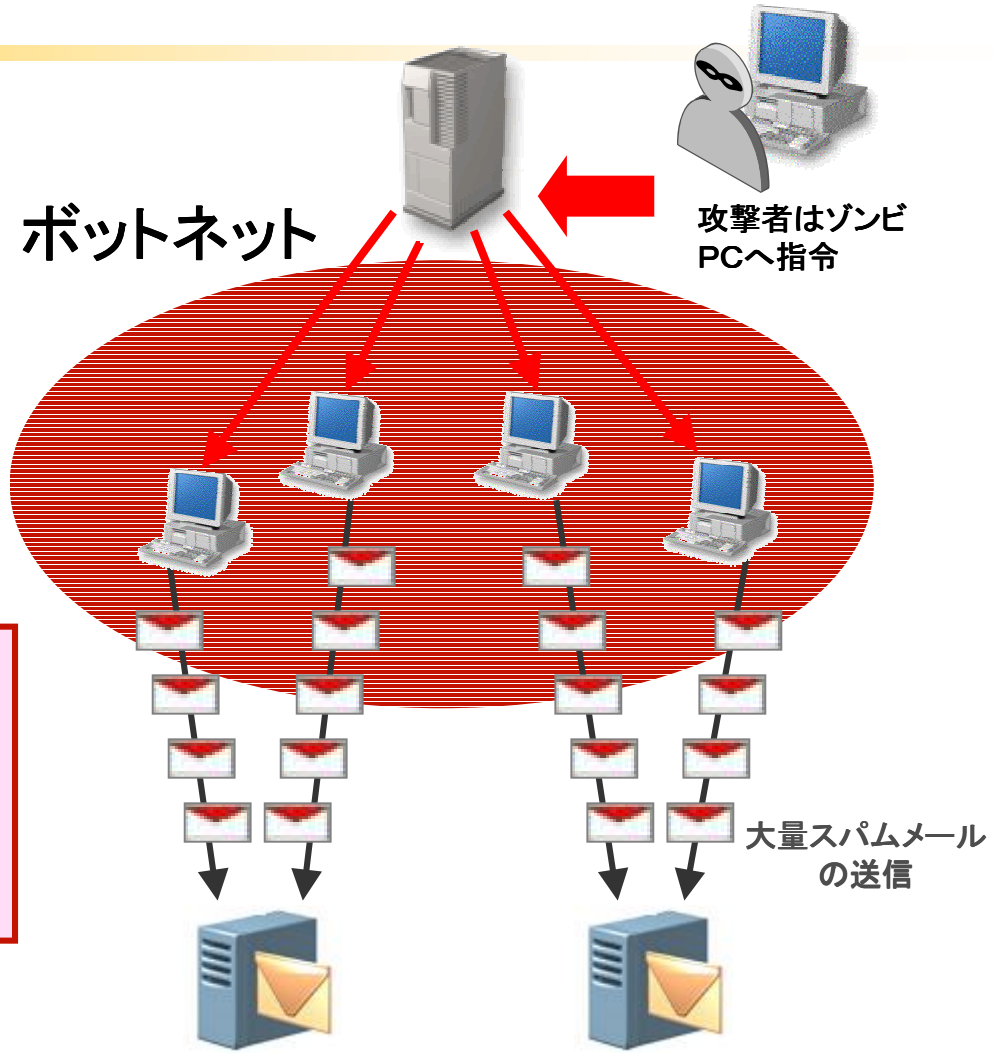
Symantec Security Update 2005 : Japan Spam by type, December 2005

新たなメールの脅威 – ボットネット

- 権限のないユーザによるコンピュータのリモート制御を可能にするために、ひそかにユーザのコンピュータにインストールされる
- ボットに感染したパソコン（ゾンビPC）は1台のパソコンから数百から数千台のゾンビPCを制御することが可能

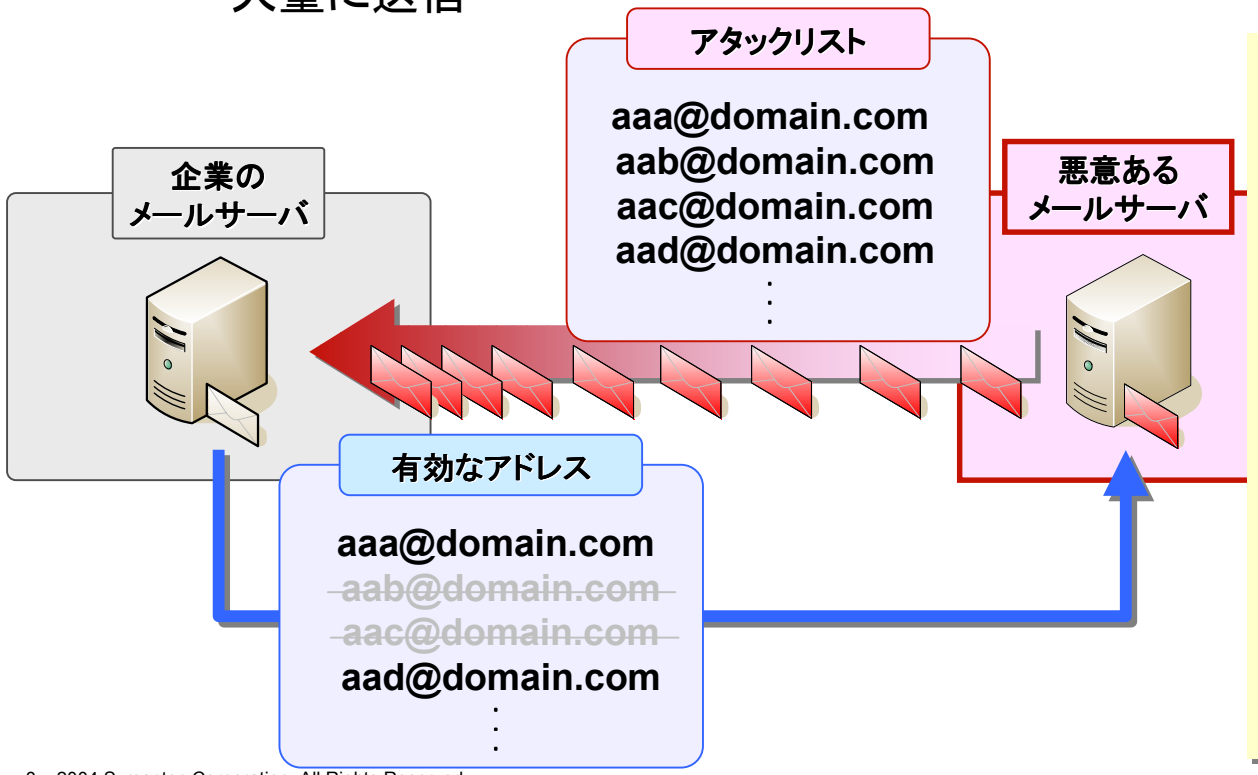
ボットネットによるスパムの被害

- 短時間に大量のスパムメールを送信
- フィッシングサイトの開設
- DHA攻撃



DHA攻撃（Directory Harvest Attack）

- **DHA攻撃（Directory Harvest Attack）**
  - 短期間に企業内で使用されている大量のメールアドレスを収集
  - 収集した結果を元に、スパムやウイルス添付メール、詐欺メールを大量に送信



【影響】
- リソースの浪費（メールサーバですべての接続要求を処理する必要がある）
- 企業データの流出

【課題】
- コンテンツベースのスキャニングでは対処できない
- MTAがメッセージを受け入れる前に攻撃に対処する必要がある

ボットに感染したコンピュータの割合上位10カ国

- 半年間で日本でのボット感染率が増加

2005年1月～6月 最新のランク	2004年7月～12月 前回のランク	国別	2005年1月～6月 ボットに感染したコンピュータの割合	2004年7月～12月 ボットに感染したコンピュータの割合
1	1	イギリス	32%	25%
2	2	アメリカ	19%	25%
3	3	中国	7%	8%
4	4	カナダ	5%	5%
5	6	フランス	4%	4%
6	9	韓国	4%	3%
7	7	ドイツ	4%	4%
8	**10**	**日本**	**3%**	**3%**
9	5	スペイン	3%	4%
10	8	台湾	2%	3%

出典：シマンテックコーポレーション

国内フィッシングの実例

“Yahoo!かんたん決済“をかたるフィッシングサイト – 2006年1月20日

****
このメールはYahoo!かんたん決済よりお送りしております。
Yahoo!かんたん決済は、お取引相手にクレジットカード情報や金融機関の口座
情報を知らせずに、オークション落札代金の支払い・受け取りが簡単に行える
便利なサービスです。
このメールにお心当たりのない方は、大変お手数ですが、次のURLよりヘルプ
ページにアクセスし、ページ下段の「いいえ」をクリックして、「お問い合わ
せフォーム」からご連絡ください。
http://help.yahoo.co.jp/help/jp/payment/
****

keyplaza2004 様

Yahoo!かんたん決済をご利用いただき、ありがとうございます。

Yahoo!かんたん決済のお支払い手続きを受け付けました。
下記の内容で出品者へのお振り込みを予定しております。

＜決済内容＞
●決済ID ：020415575172
●振込金額 ：191000 円
●決済手数料(税込) ：128 円
●出品者への入金(予定)日：2006年01月13日

＜オークション内容＞
●オークションID ：r22950588
●出品者 ：tae_onlylonely
●商品タイトル ：FMV-DESKPOWER TX90M/D 未開封
●終了日時 ：1月11日 17時14分
●落札価格 ：191000 円

かんたん決済利用明細受取明細はこちら
http://vb.url.cx/?107101121112108097122097050048048052

【ご注意】
出品者が受取口座情報を変更した場合、上記でお知らせしている出品者への入
金(予定)日が変更される場合がありますので、入金(予定)日については、
Yahoo!かんたん決済利用明細画面をご確認ください。

Yahoo!が提供する、オークション落札代金の支払い・受け取りが簡単に行えるサービス「かんたん決済」をかたったフィッシングメールとフィッシングサイトです。偽装サイトに誘導されると、「パスワードの再確認」という画面上にIDが表示され、「パスワードの再入力」を要求されます。

ANTIPHISHINGJAPAN（フィッシング対策協議会）: フィッシング事例より

フィッシングメ

新たなフィッシングの脅威：スピアフィッシング（SpearPhishing ）

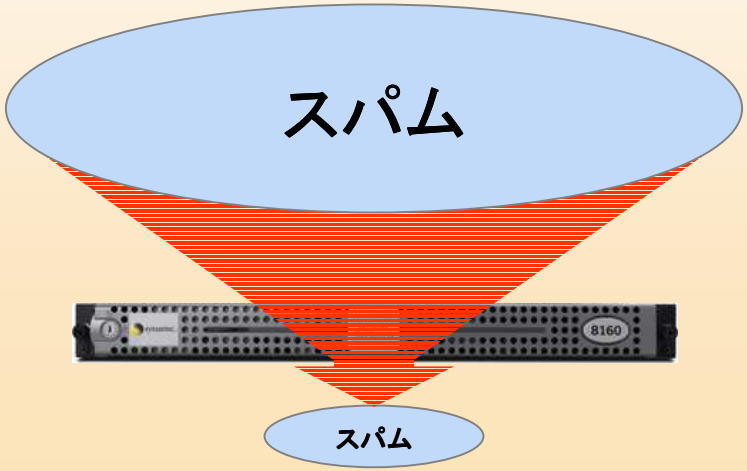
特定の人物や組織を狙い、偽のメールを送ったりウイルス（トロイの木馬）を仕込んだりしてパスワードや個人情報などを搾取する詐欺。

不特定多数のユーザを狙う通常のフィッシングとは異なり、対象の素性を調査した上で、その個人に合わせた手法が個別に考案されるのが特徴。
また、対象があらかじめ定められているために、スピアフィッシングによって盗まれる情報も通常より重大なものである場合が多い。

SMS8160とSMS8200シリーズの特長

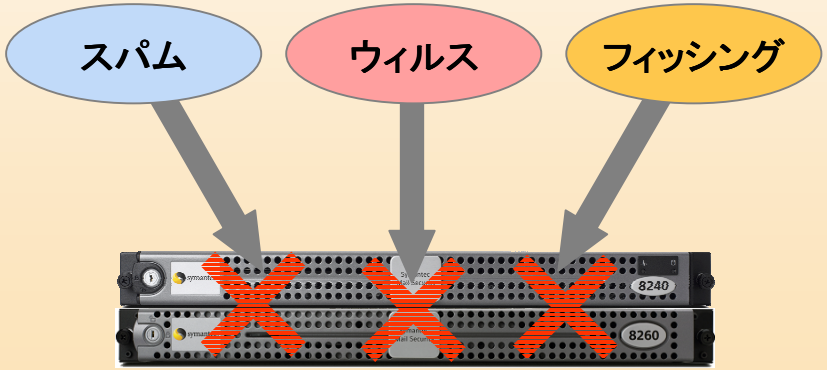
SMS8160

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シリーズ

アンチスパムだけでなく、アンチウイルス、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。



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

解析能力

デコイアカウントからのSpamメッセージ：2,000万通/日

一日に作成するフィルタの量：約15,000/日

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

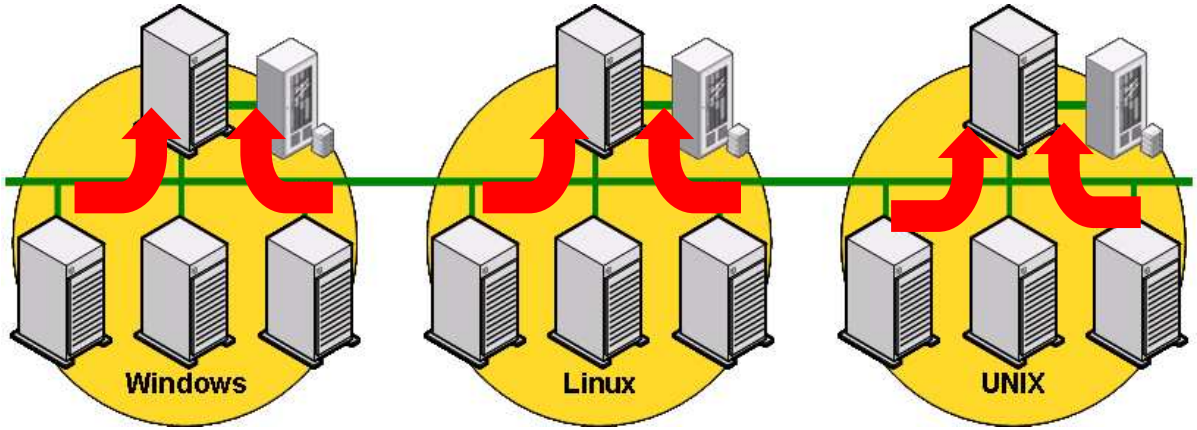
- 4つのアンチスパムに特化したレスポンスセンター
- 300万以上のデコイアカウントを保有
- 1日につき、数千万通のメールを収集
- 1時間おきにレピュテーションフィルタをアップデート

（2） 統合バックアップ

情報の可用性

混在環境のおける問題点
OS毎にバックアップソフトが違う場合 問題点

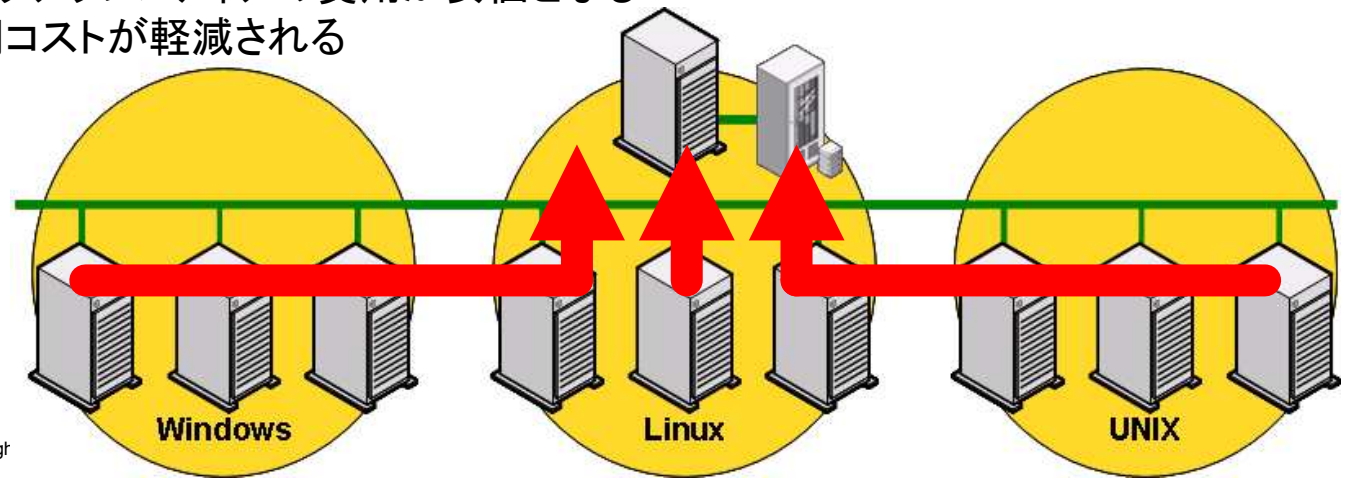
- 定義
  - 運用に関して
    - プラットフォーム毎に運用ポリシーの構築をする必要がある
    - 運用が煩雑となる
    - オペレーションの共通化ができない
  - 無駄となるコスト
    - バックアップデバイス、ソフトウェアの保守費用
    - バックアップメディアの費用
    - 運用コスト



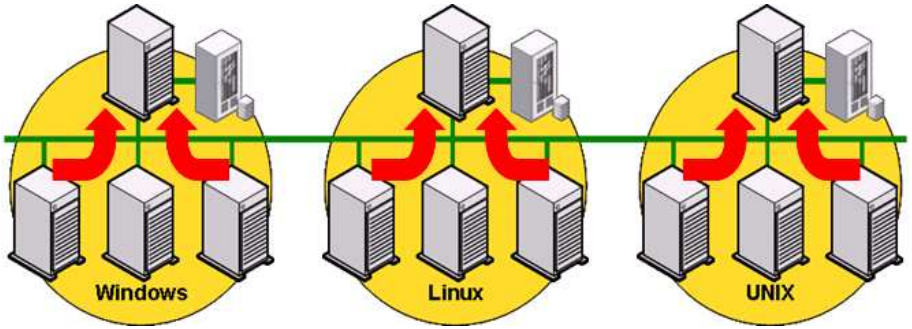
情報の可用性

混在環境のおける問題点
OS毎にバックアップソフトが違う場合 解決策

- VERITAS NetBackupの導入によるバックアップジョブの一元管理
  - 運用に関して
    - ❖ 運用ポリシーの一元管理が実施できる
    - ❖ 運用作業が簡易かされる
    - ❖ オペレーションの共通化が実施できる
  - 無駄となるコスト
    - ❖ バックアップデバイスの保守費用が安価となる
    - ❖ バックアップメディアの費用が安価となる
    - ❖ 運用コストが軽減される



コストを大幅に削減！ 某サービス業S社の導入実績から



データ容量：800GB
RDBMS：ORACLE
MS SQL
Mail：Exchange
バックアップポリシー
月～土：差分
日：フル

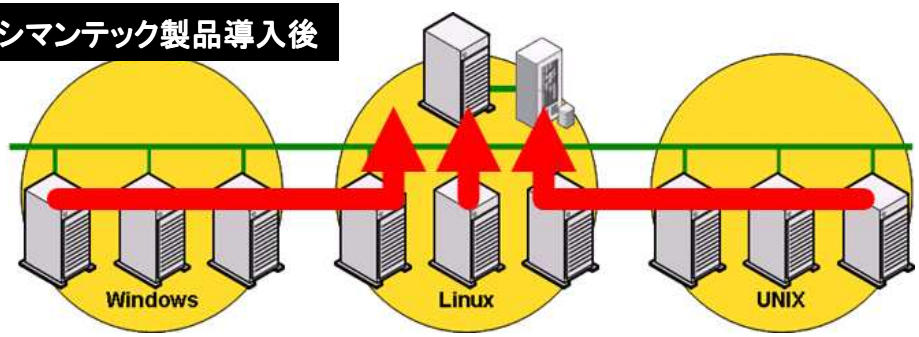
データ容量：400GB
RDBMS：ORACLE
バックアップポリシー
月～土：差分
日：フル

データ容量：1T
RDBMS：ORACLE
バックアップポリシー
月～土：増分差分混在
日：フル

ライブラリー
LTO Juke BOX × 2（ドライブ × 4）
S-DLT Juke BOX × 1
テープ使用量：80本（各2世代管理）
運用管理者：3人（各プラットフォーム毎）
年間ハードウェア保守費用：約400万円
年間ソフトウェア保守費用：約180万円

ハードウェア保守費用：年間約380万円コストセーブ
人件費：1/3（運用にかかる時間から概算で約1,300万円のコストセーブ）
テープ費用：約80万円のコストセーブ

シマンテック製品導入後



ライブラリーはLTOを流用しドライブは他のライブラリーからを追加
バックアップポリシーは一元管理

ライブラリー
LTO Juke BOX × 1
テープ使用量：40本（各2世代管理）
運用管理者：1人
年間ハードウェア保守費用：約100万円
年間ソフトウェア保守費用：約100万円