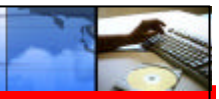
FUJITSU THE POSSIBILITIES ARE INFINITE



Sendmailを中心とした最新メール動向

2004年8月5日

株式会社富士通ソーシアルサイエンスラボラトリ

電子メールの生い立ち

「Original ARPAnet」 コンピューター共有というコンセプト

- コンピュータが高価であった
- ARPAnetの利用は学者および研究者に制限されていた
- オリジナル・プロトコル Telnet(リモートログイン)およびFTP(ファイル転送)
- メールがすぐに登場(FTPの一部として)すぐに キラー・アプリケーション」となった

1984年1月1日 :ARPAnet → インターネットになった

- 依然としてアクセスは制限されたものであった
- SMTPはメール配送のために創られた
- 認証はなし―コンピュータ共有することに意味があったため
- sendmailは最初のSMTPの実装プログラム

1995年4月30日 :インターネットの民営化

- お金があれば誰でもどんな目的でも利用可能になった
- あると便利なもの → ビジネスインフラとして必要不可欠
- お金を稼ぐもの →マネーを産む(予期しない結果: スパム)

メールをとりまく環境 (1)

全世界	2001	2002	2003	2004	2005
メールボックス総数 (百万)	547	708	939	1,258	1,715
emailユーザ総数 (百万)	365	404	470	559	686

メールボックス総数の平均成長率 = 33% *Radicati Group, 2001*
ユーザ総数の平均成長率 = 17%
ユーザ1人当たりのメールボックスは1.5から2.5へ増加

アジア太平洋	2001	2002	2003	2004	2005
emailユーザ総数 (百万)	58	69	85	112	144

アジア太平洋地域のemailユーザ総数の平均成長率 = 26% *Radicati Group, 2001*

メールをとりまく環境 (2)

業務コミュニケーションの中心 1日 1人平均 65.8通と年々増加 (2003年：ガードナー)

スパム問題 2003年に送信されたメールの４０％はスパムメール。２００４年は６０％へ (2003年：ガードナー)

ハイテク犯罪 フィッシング詐欺が米で急増 被害者数は1000万人

情報漏えい 個人情報漏えいによる事件が多発

メールセキュリティにおける課題

- 2004年米でフィッシング詐欺（個人情報盗難）が急増
- フィッシング詐欺のツールとしてなりすましメール
- 対策によりインターネット全体に影響の可能性がある
- 運用管理者の問題ではなく全メールユーザに影響

もっとも影響範囲の大きな課題

スパムとフィッシング詐欺

スパム

- スパムを多数受け取ることで、受信者のメール利用効率が低下する
- メール配送リソースをスパムのために消費される（SP等で深刻）
- DDos攻撃

フィッシング詐欺

- 現在アメリカでスパム以上に深刻な問題となっている
- 巧妙な文章の記されたHTMLメールにURLを掲載、偽Webサイトに誘導して、個人情報を入力させて盗み出すもの
- Citibankといった金融サービスや、eBay、PayPalなどの流通小売などのWebサイトになりすまし、口座を確認するという名目で入力させる

(phishing ： phは“sophisticated”から)

現状のスパム対策と課題

ブラックリスト　＋　コンテンツフィルタ　＋　フローコントロール

コンテンツフィルタ

－メールの内容を見てスパムかスパムでないか判断
－False positives（誤認：必要なメールをスパムと判定）
－False negatives（誤認：スパムを必要なメールと判定）
－ベイジアン理論等は最良の結果を得るためには、学習する必要がある

スパム送信者との競争

－Snowflaking　（スパムDB：フィンガープリンティング回避のため一通ごとに内容を変更）
－Noise words　（ベイジアン理論の精度を下げるため、業務で使用する言葉を埋め込む）
－通常の送信者はメールの記述パターンを頻繁には変更しない

何故「Authentication」なのか？

・SMTPには認証機能がないため、誰でも他人になりすますことが可能

・フィッシング詐欺に対抗するための仕組み

from: が、abc@citibank.com　でも、Citibankから来たものと証明されているわけではない

認証技術による次世代アンチスパム技術

・「認証技術」は広く採用してもらうため無償提供が必要

Authentication」のスキーム

IPアドレスベース

送信者の身元は本当に証明されているか確認する仕組み

－例 :SPF、Microsoft Call-Id for Email （この２つは現在統合された)

暗号化 証明書)ベース

送信者は、メッセージに公開かぎを使用したデジタル署名を添付して、公開かぎを公開する。受信者は署名をチェックし比較する

－例 :Yahoo! DomainKeys

勝利者による一人勝ち」ではなく、多数のスキームは共存可能

現在の送信者認証プロポーザル

暗号化 証明書ベース）

－DomainKeys
sendmailを含むいくつかのオープンソースのテストでインプリメンテーション中

IPアドレスベース

－SPF
実装テストを展開 AOL、IIJ)
多くの送信ドメインがSPFレコードを公開 (4万 ドメイン)

－Caller-ID
sendmailはオープンソースでテスト・インプリメンテーションを実装中
いくつかのドメインでCaller-IDレコードを発行中

－Sender Id
IETFを通じてCaller-IDとSPFの統合 (2004年９月)

SPF(Sender Policy Framework)

送信 IPアドレスが、送信者アドレスのドメインから送信されたかどうか調べる仕組みを提供。DNSの拡張により、SPFレコード（送信メールサーバIPアドレス）とエンベロープのIPアドレスを照合する

・メリット
低コストで実現可能

・デメリット
フィッシング詐欺に対し効果が薄い
fowardingに対応が困難

・例：
V=spf1 +a +mx –all

・既にSPFレコードを登録済みドメインがある
・受信者がチェックしているかは不明

Caller ID For Email (microsoft)

送信 IPアドレスが、送信者アドレスのドメインから送信されたかどうか調べる仕組みを提供。DNSの拡張により、SPFレコード（送信メールサーバIPアドレス）とメールヘッダのResent-Sender、Resent-From、Sender、FromのIPアドレスを照合する

・メリット
低コストで実現可能
フォワーディングに対応が可能とされている
・デメリット
認証前にメッセージ本文を読み込む必要がある
XMLで記述され長すぎる

・例：

```
<ep xmlns='http://ms.net/1'>
  <out>
   <m><a></a></m><m><mx/></m>
  </out>
</ep>
```

Sende ID (SPF + Caller Id)

IETFで標準化中（2004年９月）
SPF とCaller Id を統合。シンタックスはSPFベースを採用。SMTPの拡張が必要

・メリット
低コストで実現可能
フォワーディングに対応可能とされている
メッセージ本体を読み込む必要はない
シンプルなシンタックス

・デメリット
送信者、受信者のソフトウエアを変更する必要がある

・例：
MAIL FROM:<…> SUBMITTER=sende@example.com

Domain Keys (Yahoo!)

RSA公開かぎによる暗号化技術がベース。DNSで送信元メールサーバの公開かぎを取得する。ヘッダを含めたメッセージ全体にデジタル署名を行う。

・メリット
フォワーディングの問題がない
メッセージ本体を読み込む必要はない

・デメリット
コード変換をして中継するMTAが存在する

※暗号化ベースの方式として他に、EmailPostmarks（microsoft＋ベリサイン）、Identified Internet Mail(cisco) がある

実現に向けた課題（1）

技術的課題

－IPに基づいたスキームはフォワーディングの問題を持っている
－暗号化ベースのスキームは配送中に変更された場合、復号できなくなる
－暗号化ベースのスキームは、暗号化にコンピュータパワーを多く必要とする
－どちらのスキームも、DNSのロードを増加させる

法的課題

－実装が知的財産クレームを受ける可能性
－ブラックリストに記載された送信者が訴訟をおこす可能性

政治的課題

－各ベンダーは実際に協力しあうことができるか
－消費者は身元証明ベースのスキームを受けいれるか

実現に向けた課題（2）

経済的課題

－送信者にかかるコストが低く、受信者にかかるコストが大きいことが根本的な原因で、
逆にシフトする必要がないか

－たとえば１通１ｾﾝﾄ。通常の送信者は支払い可能だが、スパム送信者は相当なコスト負担

－送信者の支払い方法
ePostage/マイクロペイメント

－電子メールマーケティングで受信者にポイントまたは電子マネーが貯まる
→マイクロペイメントシステムの実現を引き起こすキラー・アプリケーションになるか

－新ビジネスモデル：第３者によるAccreditation（認定）/Reputation（実績評価）サービス

今後について

Eric Allmanの予測

・フィッシング詐欺を実行することは難しくなるはず
・スパムはなくならないが、２～３年後には管理可能になる
・匿名のメール送信は困難になるが不可能ではない
・送信者認証はスパムを食い止めるものではないが、他のテクノロジーのベースとなる
・“許可リスト”ベースのシステムの信頼性が確保される

長期的な展望：
・送信者認証されていないメールを受け取ることをやめる人もでてくる

まとめ

■スパムだけでなくフィッシング詐欺が深刻な問題
■全ユーザ、全メールシステムへ影響がある可能性がある
■現在のスパム対策（ブラックリスト、コンテンツフィルタ、フローコントロール）
■なりすまし防止のための電子メールアドレスの認証（Authentication）
■ IPアドレスベース(Sender Id)と暗号化ベース(DomainKeys)
■実現に向けた課題（技術的、法的、政治的、経済的）
■送信者負担の考え方
■メール送信がマイクロペイメント普及のキーになる可能性

富士通SSLのビジネスメールソリューション

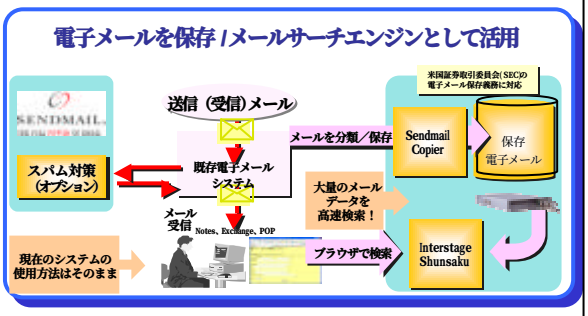
サービスメニュー

■商用版Sendmailを中心とした大規模メールインテグレーション
■スパム対策、メール監査システム等のメールセキュリティ対策
■ Ⅱ書面一括法に準拠したメールASPサービス 「セキュアパッケージ配信」

電子メール保存/検索

メールサーチエンジン導入で
セキュリティ対策・ビジネス生産性向上

- **電子メールのセキュリティ監査が可能**
- **過去の電子メールを保存してナレッジベース**
- **１００万通を１０秒で高速検索**
- **ブラウザでシンプル操作**



FUJITSU

THE POSSIBILITIES ARE INFINITE