

最新技術動向

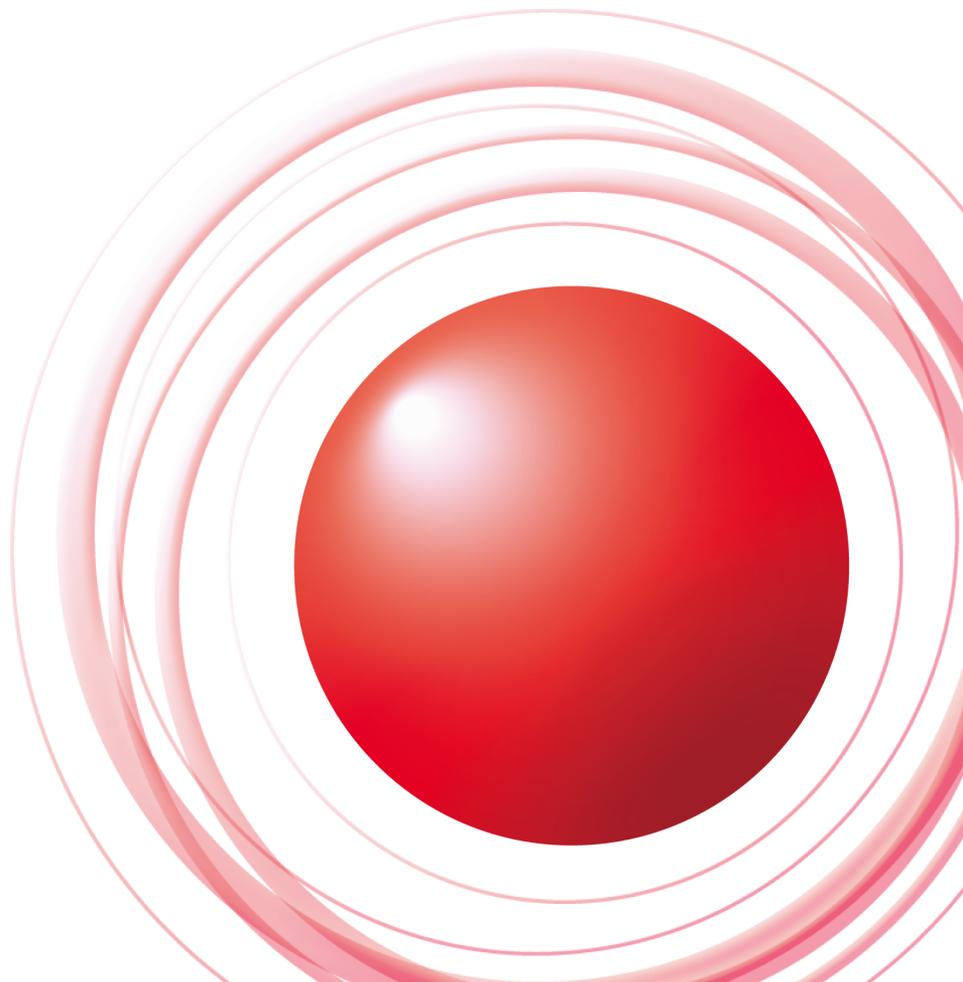
迷惑メール対策セミナー [松山]



2010.07.02

Internet Initiative Japan Inc. (IIJ)
Shuji SAKURABA (櫻庭秀次)

Ongoing Innovation

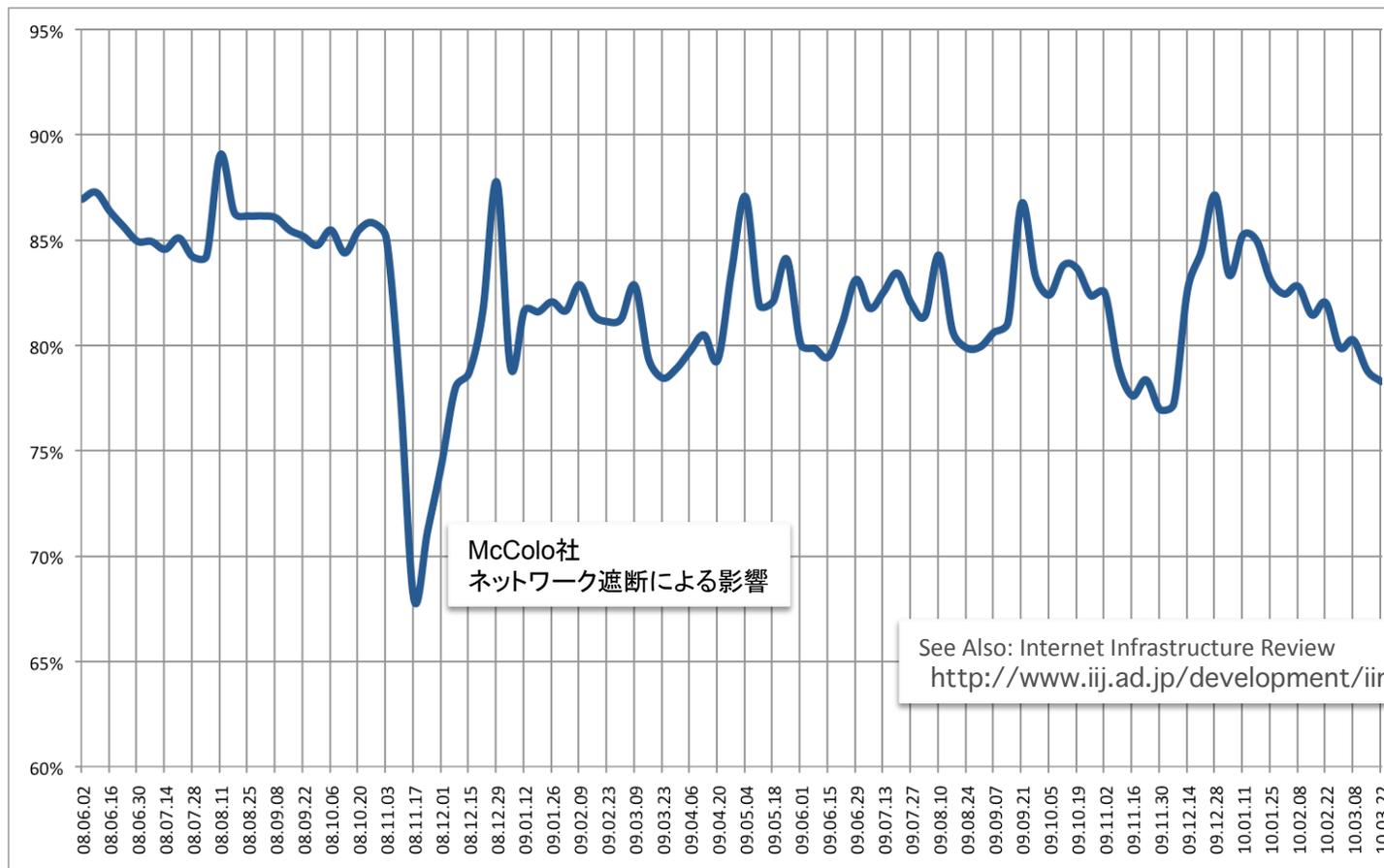


Agenda

- 迷惑メールの現状
- 対策の強化とその懸念
- 送信ドメイン認証技術
 - 概要解説
 - 導入状況
 - 受信側の認証導入
 - 送信側の導入
- 迷惑メール対策の取り組み
 - JEAG
- おわりに

迷惑メールの現状 - I

- 迷惑メール割合の推移
 - 迷惑メールフィルタによる検知率
 - 2008.06.02 ~ 2010.03.28 (95週間)



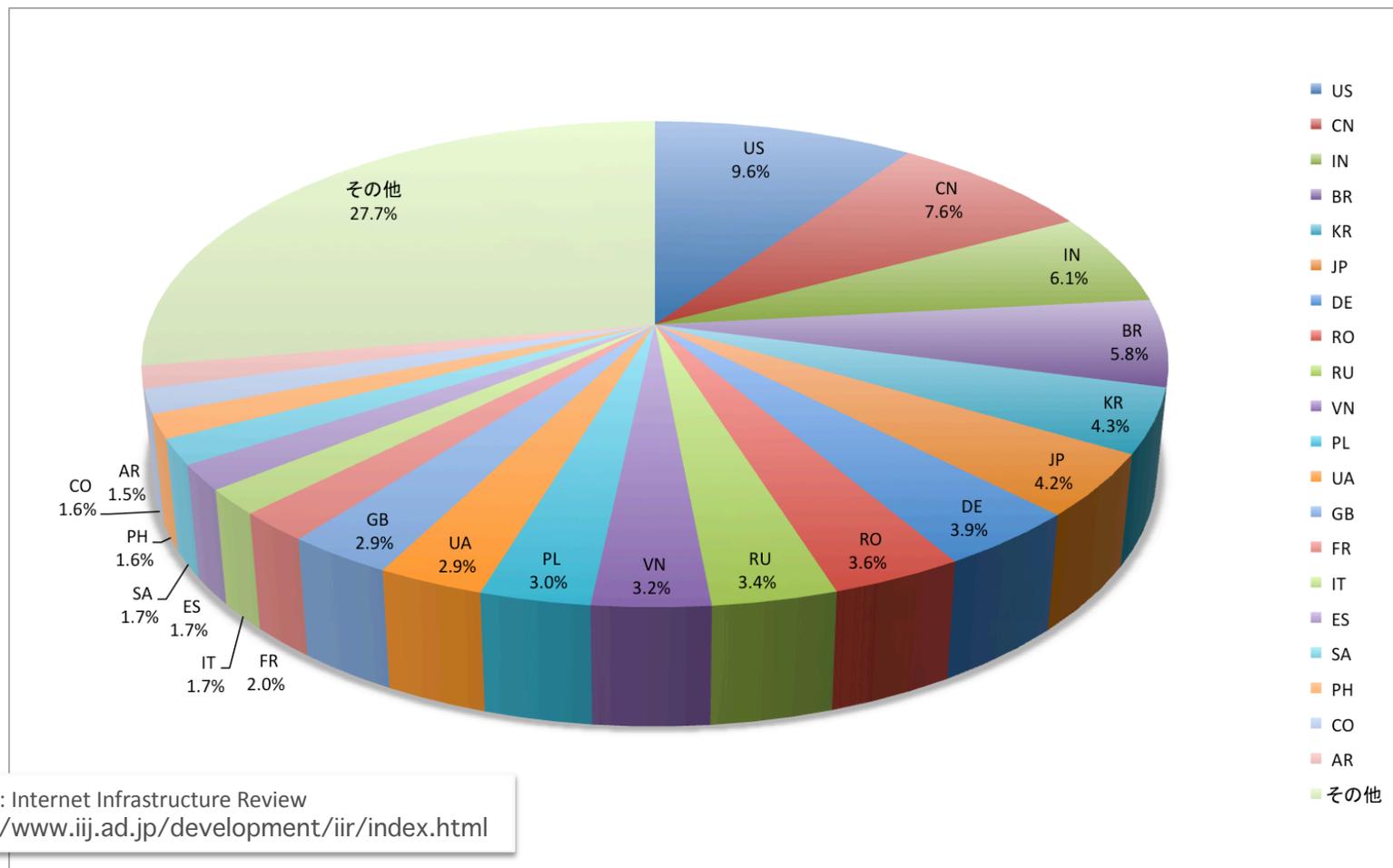
McColo社
ネットワーク遮断による影響

See Also: Internet Infrastructure Review
<http://www.ij.ad.jp/development/iir/index.html>

迷惑メールの現状 - II

- 送信元の地域別分布

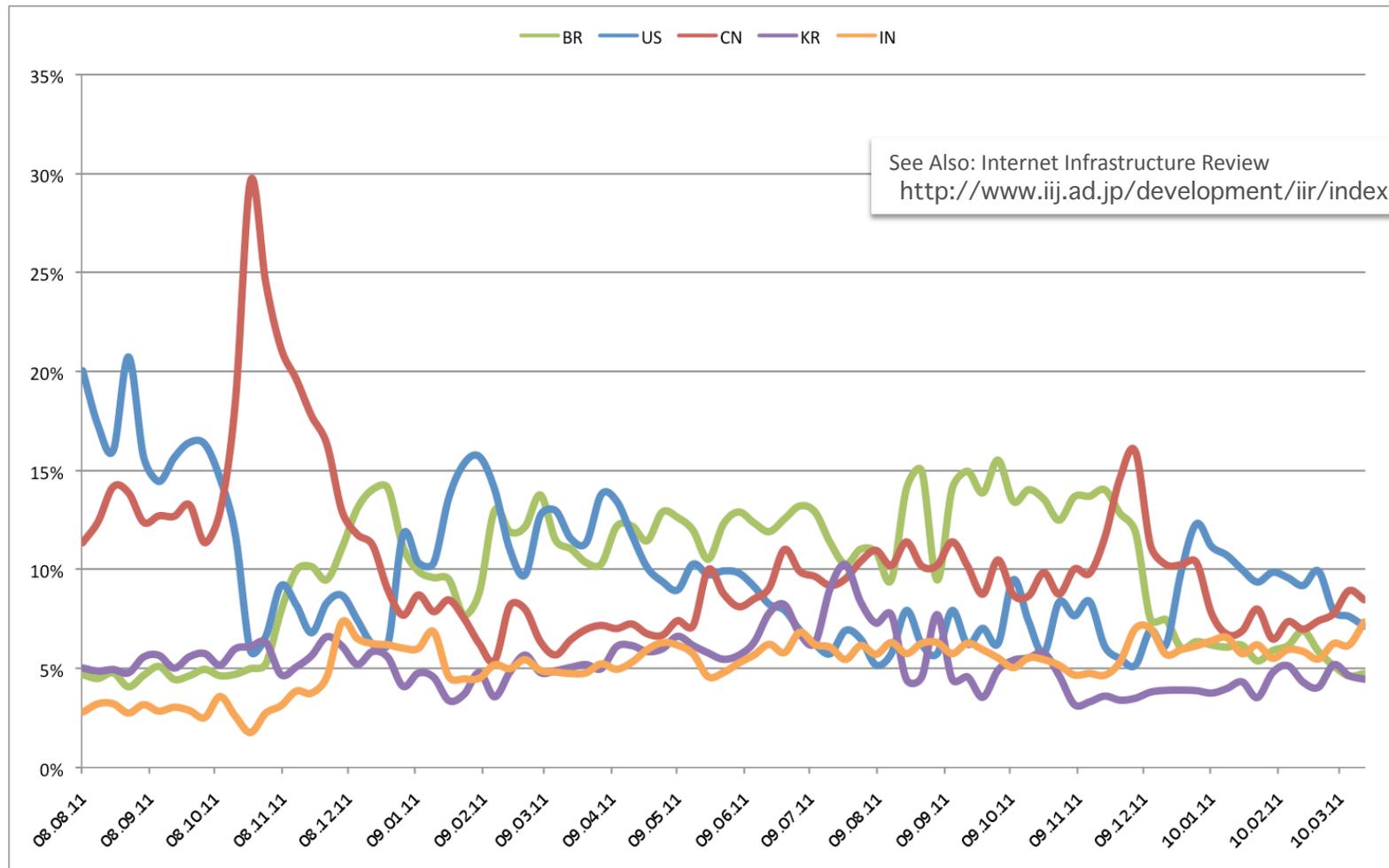
— 2010.01.04 ~ 2010.03.28 (12 週間)



迷惑メールの現状 - III

- 主要送信元の推移

— 2008.08.11 ~ 2010.03.28 (85週)

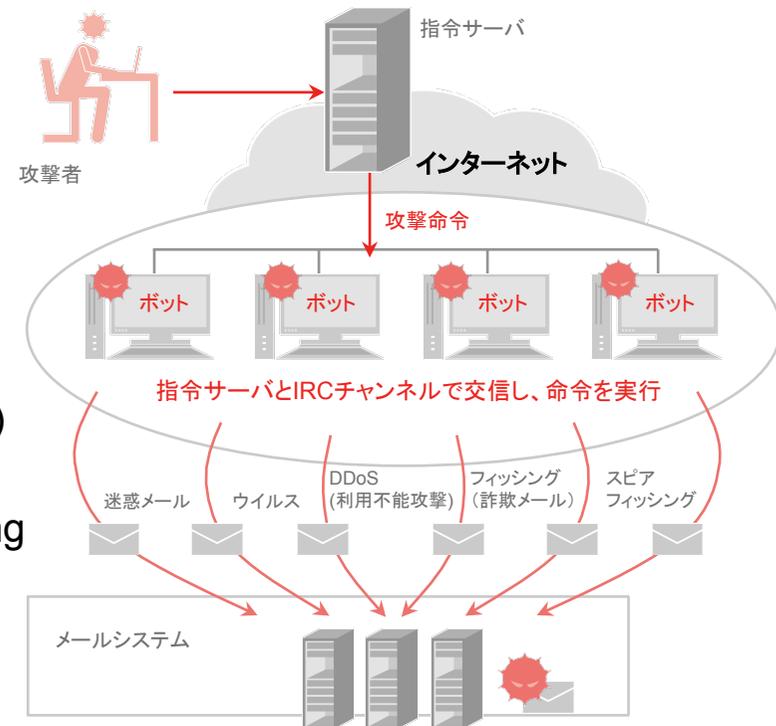


See Also: Internet Infrastructure Review
<http://www.ij.ad.jp/development/iir/index.html>

迷惑メールの現状 - IV

• 送信手法の高度化・多様化

- 高速回線を利用した短時間での大量送信 (主に国内からの送信)
- 海外拠点からの大量送信 (OP25B による国内送信の抑制: 後述)
- Botnet の利用
 - 不正プログラム (malware: malicious software) に PC を感染させる
 - インターネット経由で外部から制御
 - ロボットのように操られることから Bot
 - 複数の Bot をネットワーク化 (Botnet)
 - Botnet を様々な用途に悪用
- 正規メールサーバを踏み台に利用
 - フリーメールのアカウントを大量取得
 - CAPTCHA を解読するための様々な試み
 - ISP のメールサーバを利用 (malware 利用)
 - メール受信側はブロックしづらいことを悪用
 - 評判を乗っ取る意味で Reputation Hijacking
- 代理サーバ (socks, http, proxy, etc) の利用およびその国際化



CAPTCHA: Completely Automated Public Turing test to tell Computers and Humans Apart

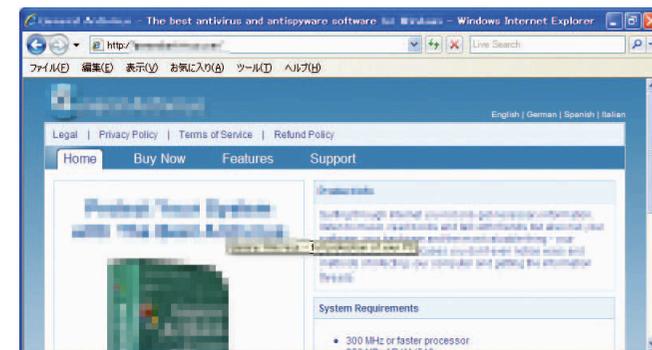
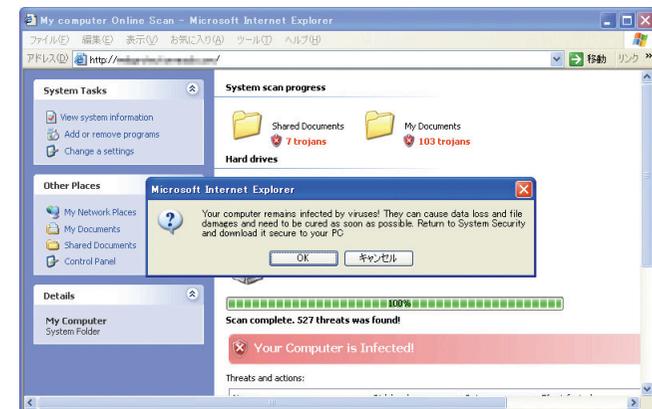
迷惑メールの現状 - V

● 被害の多様化

- 偽のWebサイトへの誘導による個人情報の搾取 (phishing)
- 偽のセキュリティソフトを装った脅迫による金銭搾取 (scareware)
 - ウイルスチェックの実行を装い感染を警告 (例えばここまでは無料)
 - 除去のためにはセキュリティソフトの購入が必要と警告 (有料)
 - アップデート称して別の不正プログラムを誘導
 - 日本語版も出回っている
- ブラックマーケット
 - 搾取した個人情報 (カード情報等) の売買
 - 正規アカウント情報の売買
 - ボットネットの時間貸し出し (クラウドサービス?)

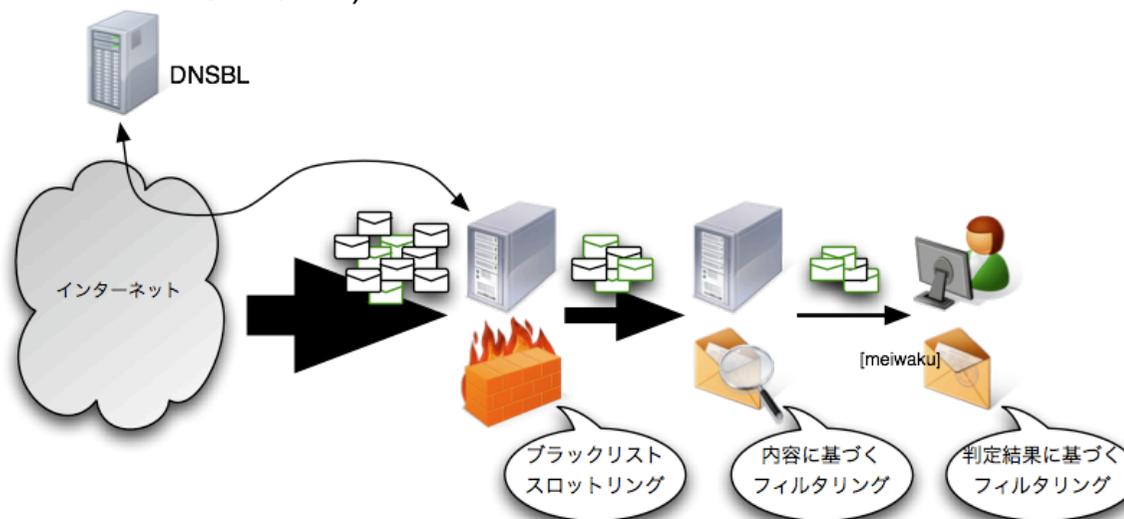
● 動機

- Less Risk
 - Less Violence
 - Less Jail Time
 - More Profit



対策の強化とその懸念 - I

- 迷惑メール対策
 - 送信元情報などによるネットワークレベルでの抑制
 - メールの内容による判断
 - 最終的には受信者の判断によるフィルタリング (が望ましい)
- 懸念点
 - 判定処理の負荷 (設備, 運用, コスト)
 - 判定精度
 - 正しいメールを迷惑メールと誤判定 (false positive)
 - 迷惑メールを正しいメールと誤判定 (false negative)
 - 判定を回避するための様々な手法と急激な増加への対応遅れ (ウイルス対策と同根の問題)



対策の強化とその懸念 - II

- **送信元による判断 – 外部データの利用**
 - DNS の仕組みを利用した IP アドレスによる Black List (DNSBL)
 - 接続時点での判断が可能で設備負荷も比較的小さい
 - 判定精度と運用方針
 - データの信憑性 (データの収集方法とその範囲)
 - 運用方針 (誤判定時の解除手続き等)
 - 正規のメールサーバが登録された場合の影響 (送信側のみならず受信側も)
- **送信元による判断 – 自身の判断**
 - 正規のメールサーバかどうかを接続元情報から独自に判断
 - IP アドレスの逆引きが設定されているかどうか
 - 単位時間あたりの接続数や宛先不明率
 - 未知の送信元を一時保留 (greylisting) することによる判定
 - 送信元の大規模分散化に対応可能か (一時保留した接続元の保持が必要)
 - 配送経路が変更されることの考慮がなされているか
 - 一時保留することによるメール配送の遅延は許容できるのか
- **対策手法の法的留意点**
 - 電気通信事業法の範囲では制約がある (原則利用者の同意が必要)
 - 幾つかの技術 (OP25B, 送信ドメイン認証技術) に関しては法的整理が行われている

ご参考:

http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/jigyosha.html

対策の強化とその懸念 - III

- 迷惑メール対策の今後

- 迷惑メール送信で利益を得られる間は減少はあまり期待できない
- 迷惑メールが減少しない限りは今後も対策の強化は避けられない
- 対策には誤判定のリスクが常に存在
- メールはコミュニケーションのための重要なツール



正しいメールがきちんと到達できる環境作りが必要

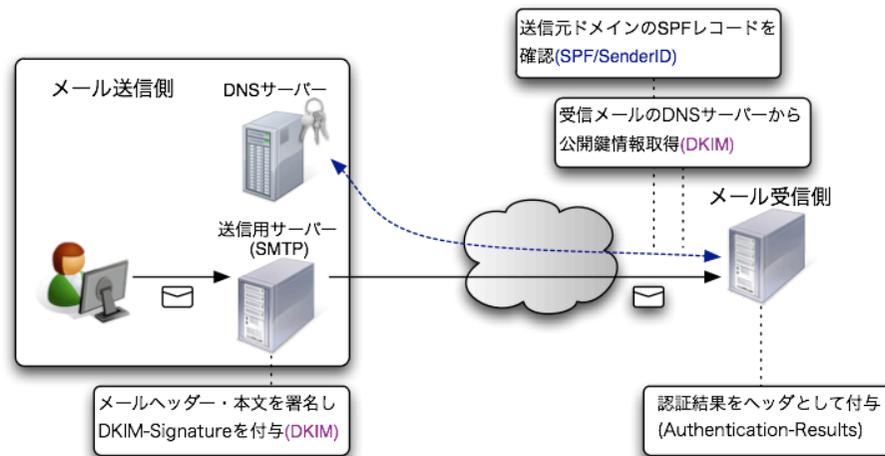


正しいメールを判断するための共通基盤としての

送信ドメイン認証技術

送信ドメイン認証技術 – 概要

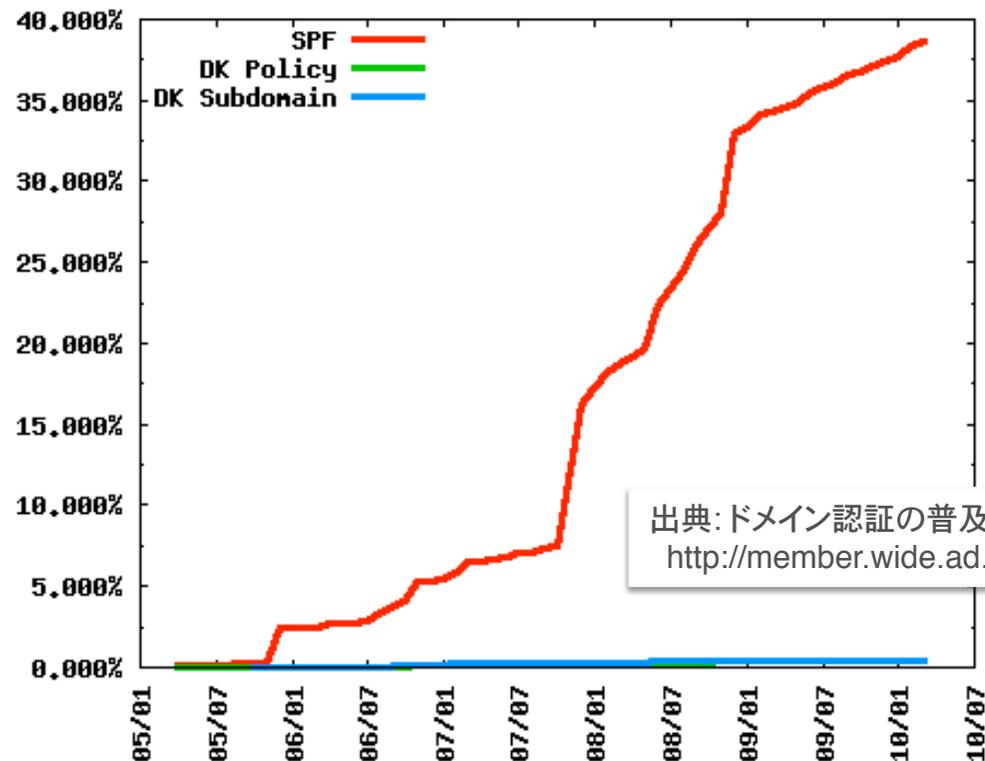
- 基本的な仕組み
 - 送り手は送信元 (メールの出口) を明確に表明
 - 受け手は送信者情報が正しく表明されているか確認
- 送信ドメイン認証技術の特徴
 - 既存のメール配信の仕組みを変更することなく下位互換を維持
 - DNS の仕組みを利用することにより新たな認証機関を必要としない
 - 送信者情報や認証の仕組みの違いによる複数の認証方法
 - SPF (Sender Policy Framework) / SIDF (Sender ID Framework)...ネットワーク方式
 - DKIM (DomainKeys Identified Mail)...電子署名方式



送信ドメイン認証技術 – 導入状況

- 日本 (jp) の導入状況

- WIDE プロジェクトと JPRS による共同研究による調査
- 2010年4月時点で “jp” ドメインの SPF 宣言率は 39.03%
- “co.jp” ドメインについては 45.15%

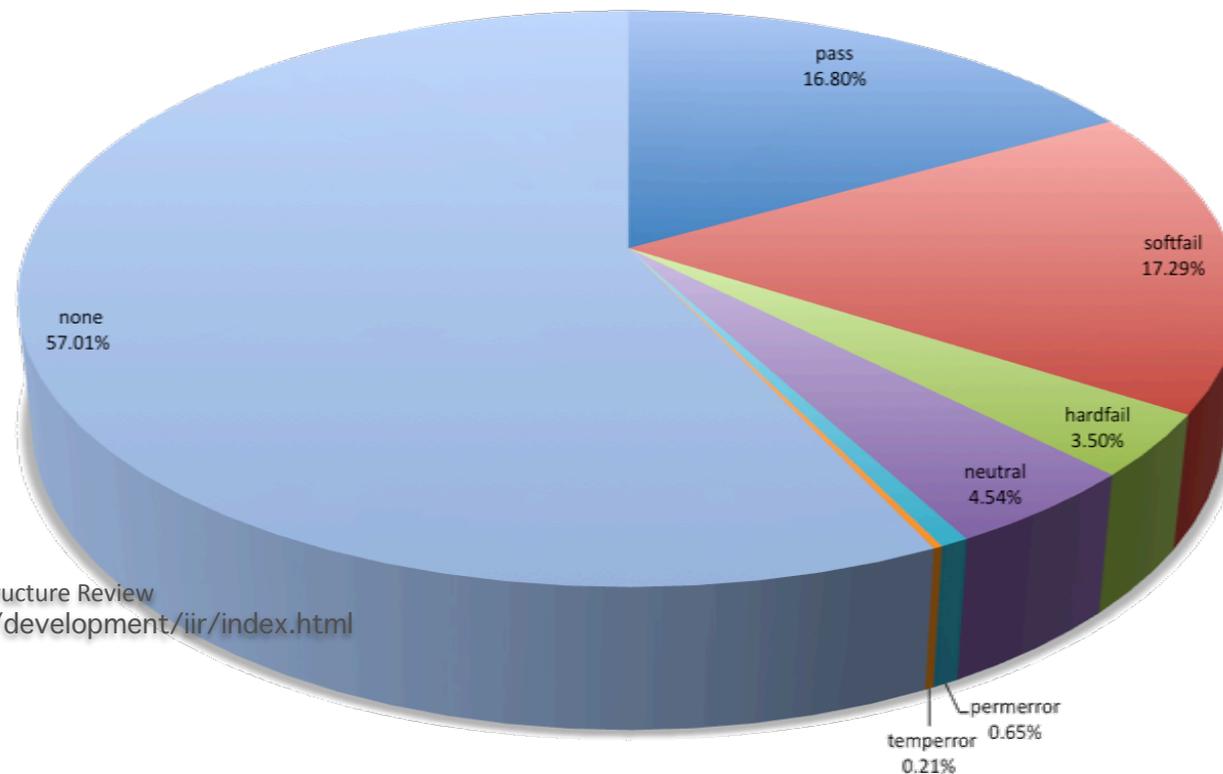


出典: ドメイン認証の普及率に対する測定結果
<http://member.wide.ad.jp/wg/antispam/stats/index.html.ja>

送信ドメイン認証技術 – 導入状況 (cont.)

- 受信メールによる調査

- 期間: 2010.04.01 ~ 2010.04.30
- 受信メールの 43% のドメインが SPF レコードを宣言

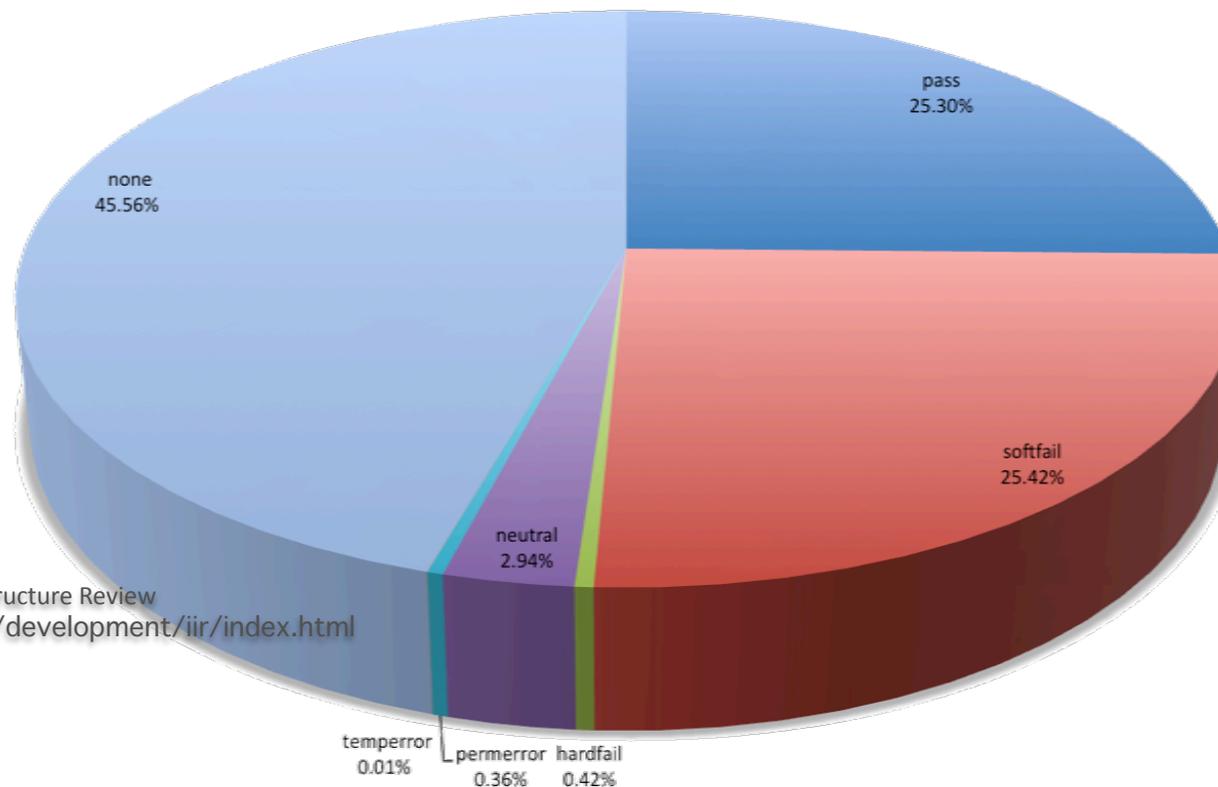


See Also: Internet Infrastructure Review
<http://www.ij.ad.jp/development/iir/index.html>

送信ドメイン認証技術 – 導入状況 (cont.)

- 受信メールによる調査 (jp ドメイン)

- 期間: 2010.04.01 ~ 2010.04.30
- 受信メールの **54.44%** のドメインが SPF レコードを宣言



See Also: Internet Infrastructure Review
<http://www.ij.ad.jp/development/iir/index.html>

送信ドメイン認証技術 – 受信側の導入

- 認証機能の導入
 - 認証方式に関わらず送信ドメイン認証を行うにはメールサーバへの機能追加が必要
 - メールサーバの負荷や DNS の負荷を予め考慮した設備設計が必要
- 迷惑メールフィルタでの利用
 - 他の判定機能と合わせた総合的な判断でフィルタリング
 - 認証結果だけを利用するのではなく送信ドメインと合わせて利用
 - 予め受信すべき送信元が明らかな場合はそのドメイン名と認証結果 (pass) とを合わせたホワイトリスト機能で受信

送信ドメイン認証フィルタ設定

https://www.ij4u.or.jp/service/setup/mail/sender_auth/confirm.do

送信ドメイン認証フィルタルール一覧

20件 ずつ表示

(4件中の4件を表示中) page: 1

優先度	対象ドメイン	SPF	動作	ルール削除
1	yahoo.co.jp	pass	<input checked="" type="radio"/> 受け取る <input type="radio"/> 通過 <input type="radio"/> ごみ箱に入れる	削除
2	yahoo.co.jp	hardfail(fail)	<input type="radio"/> 受け取る <input type="radio"/> 通過 <input checked="" type="radio"/> ごみ箱に入れる	削除
3	yahoo.co.jp	softfail	<input type="radio"/> 受け取る <input type="radio"/> 通過 <input checked="" type="radio"/> ごみ箱に入れる	削除
4	yahoo.co.jp	neutral	<input type="radio"/> 受け取る <input type="radio"/> 通過 <input checked="" type="radio"/> ごみ箱に入れる	削除

(4件中の4件を表示中) page: 1

20件 ずつ表示

次へ

→ サービストップへ

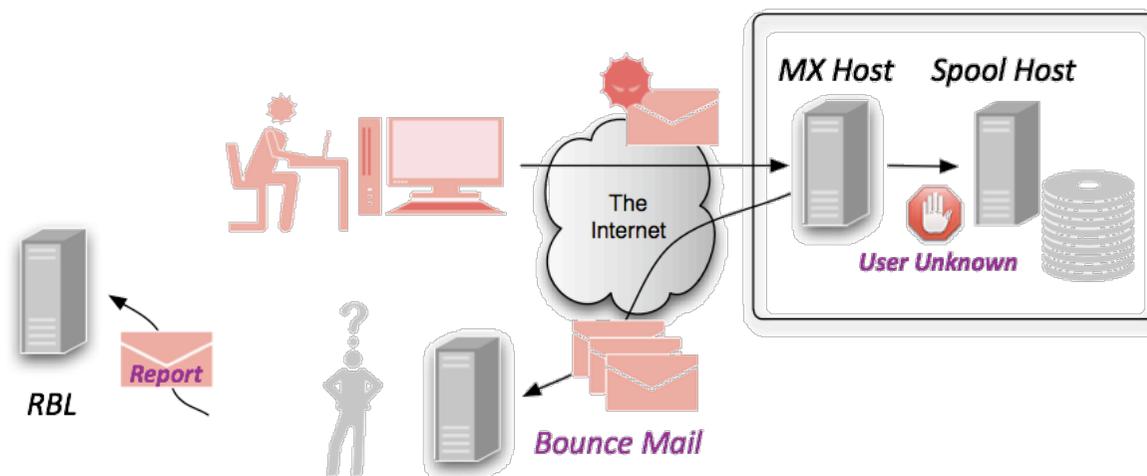
UP ▲

© 2004 - 2010 Internet Initiative Japan Inc.

[このサイトのご利用について](#) | [個人情報保護ポリシー](#) | [情報セキュリティ基本方針](#)

送信ドメイン認証技術 – 受信側の導入 (cont.)

- **Backscatter 問題**
 - 迷惑メールの多くは送信元情報が詐称されている
 - 宛先不明メールに対するエラーメールの送信先は送信者情報を利用
 - 詐称された側へ送信される大量のエラーメール
 - 無関係なエラーメールが迷惑メールと判断
 - エラーメールの送信元が Black List へ登録されるなど二次的な問題も発生
- **回避策**
 - 送信ドメイン認証技術により送信者情報が詐称されていると思われる (“fail” or “softfail”) 送信者へエラーメール送信は行わない
 - または宛先不明のメールを受け取らない → 別途 DHA (Dictionary Harvesting Attack) 対策も必要



送信ドメイン認証技術 – 受信側の導入 (cont.)

- メール受信者への認証結果の通知

- 受信メールサーバ側でフィルタリングが難しい場合でも受信者の MUA で個別に判断
- 認証結果を記録する統一的なフォーマット (RFC5451, Message Header Field for Indicating Message Authentication Status) を利用

```
Authentication-Results: example.com;  
sender-id=hardfail header.from=example.com;  
dkim=pass (good signature) header.i=sender@example.com
```

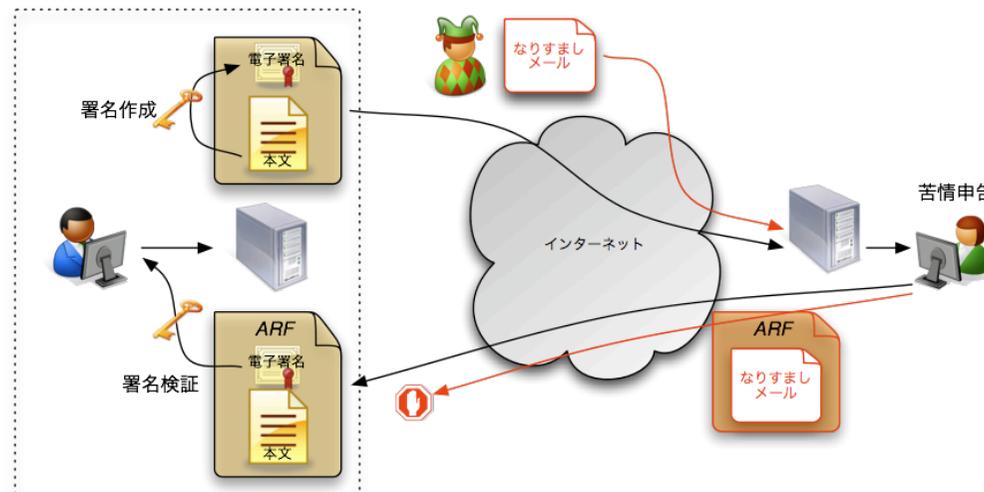
- MUA (Mail User Agent) の機能を用い受信者がフィルタリング



Apple Mail のフィルタリング例

送信ドメイン認証技術 – 受信側の導入 (cont.)

- **FBL (Feedback Loop)**
 - FBL とはメール受信者から送信側への苦情等の申し立て
 - 米国では中間事業者が仲立ちを行う事例もあり
 - 予め送信事業者は送信側の情報と連絡窓口を登録
 - 受信側で Webmail 等でのボタンによる申告 → 中間事業者への通知
 - 登録されている事業者であれば報告
 - 送信事業者の利点
 - 送信先リストからの削除 (opt-out)
 - 苦情のあったメールの識別 → 依頼元との今後の調整
 - 送信間隔の調整, etc
 - 受け取る苦情が**本当に送信側が送ったものであるかの検証が必要**
 - 申告メールに DKIM ヘッダ (DKIM-Signature) があれば再検証可能
 - **ARF (Abuse Reporting Format)** 形式であればヘッダ情報も含まれる
 - An Extensible Format for Email Feedback Reports (draft-ietf-marf-base-06)



送信ドメイン認証技術 – 送信側の導入

- 導入状況調査
 - 日本データ通信協会による調査
 - 調査時期: '09.07.31
 - SPF: 7/28 (25%)
 - DKIM: 4/28 (14%)

送信ドメイン認証 | 迷惑メール相談センター

http://www.dekyo.or.jp/soudan/auth/

迷惑メール相談センター

送信ドメイン認証

送信ドメイン認証技術について | ISP | 携帯・PHS | フリーメール

ISPの送信ドメイン認証実装状況 #1

ISP(インターネットサービスプロバイダ) 各社の送信ドメイン認証について、現在の実装状況をとりまとめています。
送信ドメイン認証技術は、迷惑メール対策としても非常に有用な技術であり、一層の普及が期待されることから、当協会では今後とも引き続き導入状況の調査を行いその結果をホームページで公表していく予定です。
2009年07月31日時点 31社31サービス

サービス名	事業者	送信#2		受信#3		詳細
		SPF/ SenderID	DKIM/ domainKeys	SPF/ SenderID	DKIM/ domainKeys	
@NetHome	株式会社テクノロジーネットワークス	☆	—	—	—	HP ※会員専用
@nifty	ニフティ株式会社	☆	☆	—	—	HP
aitainet	ひまわりネットワーク株式会社 おりべネットワーク株式会社 三河湖ネットワーク株式会社 シーシーエヌ株式会社	☆	—	—	—	—
au one net	KDDI株式会社	☆	—	○	—	—
BBIQ/九州電話インターネット	九州通信ネットワーク株式会社	☆	—	—	—	—
BIGLOBE	NECビッグロブ株式会社	☆	—	○	○	HP
Ccnet	中部ケーブルネットワーク株式会社	☆	—	○	○	—
CORALNET	トナミ運輸株式会社	☆	—	—	—	—
DTI	株式会社ドリーム・トレイン・インターネット	☆	—	—	—	HP
e-sadonet	株式会社佐藤テレビジョン	☆	—	○	—	—
eo (イオ)	株式会社ケイ・オプティコム	☆	—	—	—	HP
hi-ho	株式会社ハイホー	☆	—	—	—	HP
IJ 4U/IJmio	株式会社インターネットイニシアティブ	☆	—	○	○	HP
ITSCOM	イツツ・コミュニケーションズ株式会社	☆	—	—	—	HP
KATCHケーブルインターネットサービス	株式会社キャッチネットワーク	☆	—	—	—	—
MediaCat/ROSENET	KMN株式会社	☆	—	—	—	—
MEDIAS-NET	知多メディアネットワーク株式会社	☆	—	—	—	—
mopera U	株式会社エヌ・ティ・ティ・ドコモ	☆	—	—	—	HP
OCN	NTTコミュニケーションズ株式会社	☆	—	○	—	HP
ODN	ソフトバンクテレコム株式会社	☆	—	—	—	—
SANNET	株式会社NTTデータ三洋システム	☆	—	—	—	—
SpinNet	ソフトバンクテレコム株式会社	☆	—	—	—	—
WAKWAK	株式会社エヌ・ティ・ティ・エムイー	☆	—	—	—	HP
Yahoo!BB	ソフトバンクBB株式会社、ヤフー株式会社	☆	☆	○	○	HP
ZAQ	関西マルチメディアサービス株式会社	☆	—	—	—	HP
テレビ版権	動画ケーブルテレビ株式会社	☆	—	—	—	—
ハイネット(HI-NET)	株式会社ハイネット	☆	—	—	—	HP
ぷらら	株式会社NTTぷらら	☆	—	—	—	—

※1: 実装状況は、各事業者へのヒアリング及び公表資料等を基にした調査結果を表示しています。また、実装の有無は「☆」と表示されています。例えば、送信時実装でSPFのみ実装している場合でも、SPF/SenderIDの項目は「☆」と表示されています。

調査結果:

<http://www.dekyo.or.jp/soudan/auth/>

送信ドメイン認証技術 – 送信側の導入 (cont.)

- **送信側の運用**
 - SPF レコードの宣言はもはや必須
 - より重要なメール (顧客連絡等) には DKIM の導入を
 - ドメイン名の評判 (reputation) が下がらないような運用 (迷惑メールを送信しない) が必要
 - メール送信経路の確認 → メールシステム, 利用方法 (利用ルール)
 - 送信時の送信者認証 (SMTP-AUTH) による管理 → 事後対処等
 - 送信者情報 (SPF/Sender ID) が正しく設定されているか確認
 - DNS の負荷, RR (Resource Record) の伝播時間の考慮 (TTL値)
 - DKIM ADSP (Author Domain Signing Practices) による署名方針の表明
- **メールサービスでの運用**
 - 複数ドメインを扱う場合にはお隣さん問題に注意
 - それぞれの送信メールが正しい送信者情報を利用しているか確認
 - 転送時の PRA (Resent-* ヘッダ) 付加, リバースパスの書き換え (タグ付きによるループの回避)
 - DNS とメールサービスが分離されている場合のサポート
 - SPF/Sender ID: “include” 用の SPF レコードを提供
 - DKIM: “_domainkey” サブドメインの委譲や設定用公開鍵の提供

迷惑メール対策の取り組み - JEAG

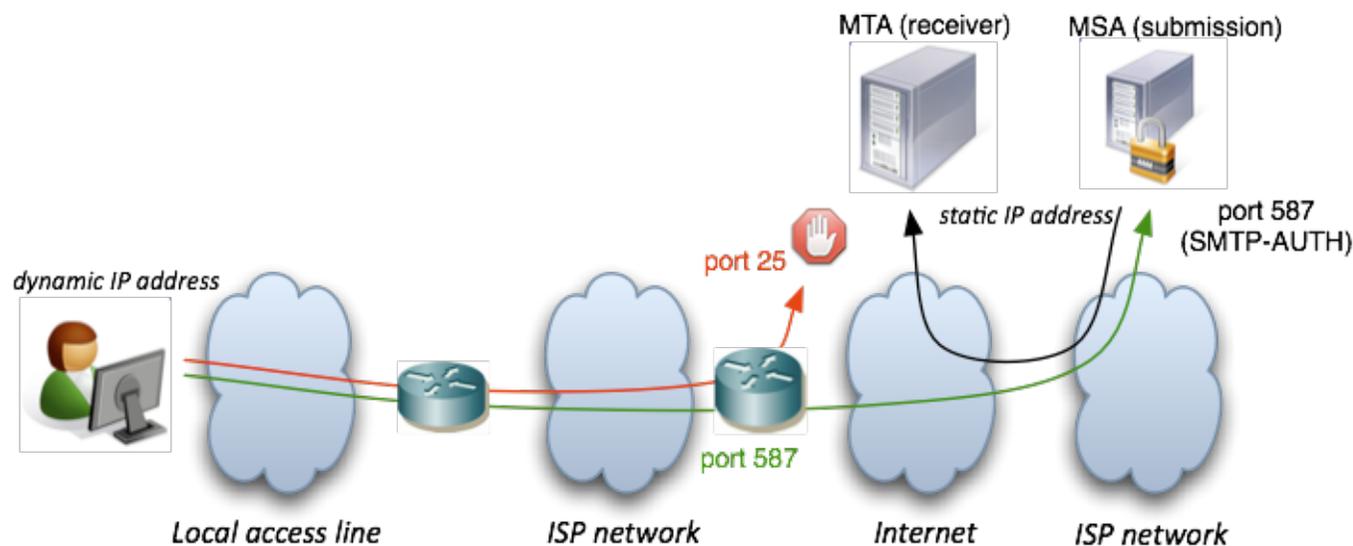
- **JEAG (Japan Email Anti-Abuse Group)**
 - MAAWG の設立 (2004.1.19) を背景として 2004 年から有識者間で活動
 - 発起人 6社により正式に発足 (2005.3.15)
 - 主要 ISPs, 携帯電話事業者, ベンダなどメンバ企業 30社で構成
 - オブザーバ: 総務省, 経産省, (財)日本データ通信協会
 - 外部団体, 組織との連携
 - MAAWG (Messaging Anti-Abuse Working Group)
 - APCAUCE (Asia Pacific Coalition Against Unsolicited Commercial Email)
 - Email Security Expo & Conference (主催 (株) ナノオプト・メディア)
 - 迷惑メール対策カンファレンス (主催 (財)インターネット協会 迷惑メール対策委員会)
 - 目的: 技術的な見地およびサービス事業者間の連携による迷惑メール対策の推進



- **JEAG Recommendation (2006.02.23 発行)**
 - 送信ドメイン認証技術
 - OP25B (Outbound Port 25 Blocking)
 - 携帯電話宛て迷惑メール対策

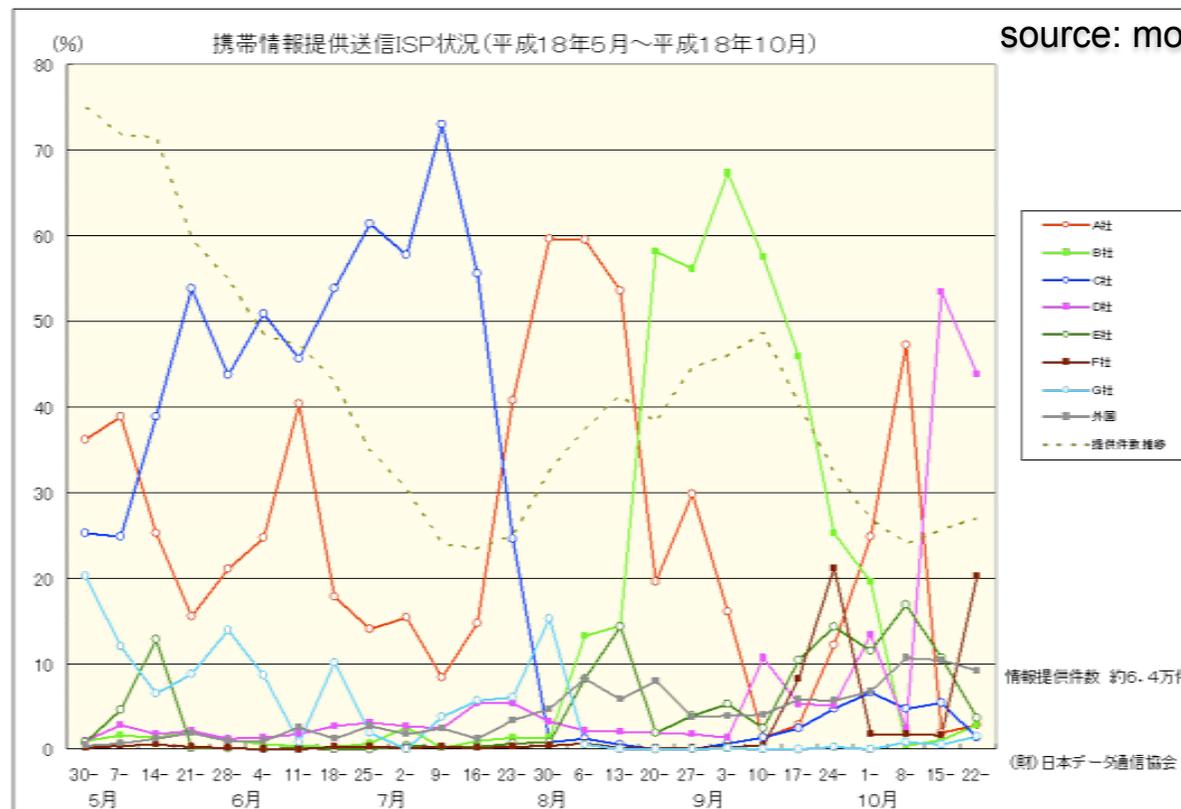
迷惑メール対策の取り組み – JEAG (cont.)

- **OP25B (Outbound Port 25 Blocking)**
 - 迷惑メール送信に使われる動的 IP アドレスからのメール送信 (受信メールサーバの port 25 への直接接続) を一律に規制
 - メール送信には ISP が提供するメールサーバ (投稿サーバ) を利用
 - 送信時は投稿ポート (port 587) を利用し送信者認証 (SMTP-AUTH) を行う
 - 管理元が明確な固定 IP アドレスは規制の対象外
- **導入方法**
 - 適切なアクセスポイントでルータに ACL (Access Control List) などのフィルタルールを導入
 - 十分な利用者周知と段階的な導入を推奨



迷惑メール対策の取り組み – JEAG (cont.)

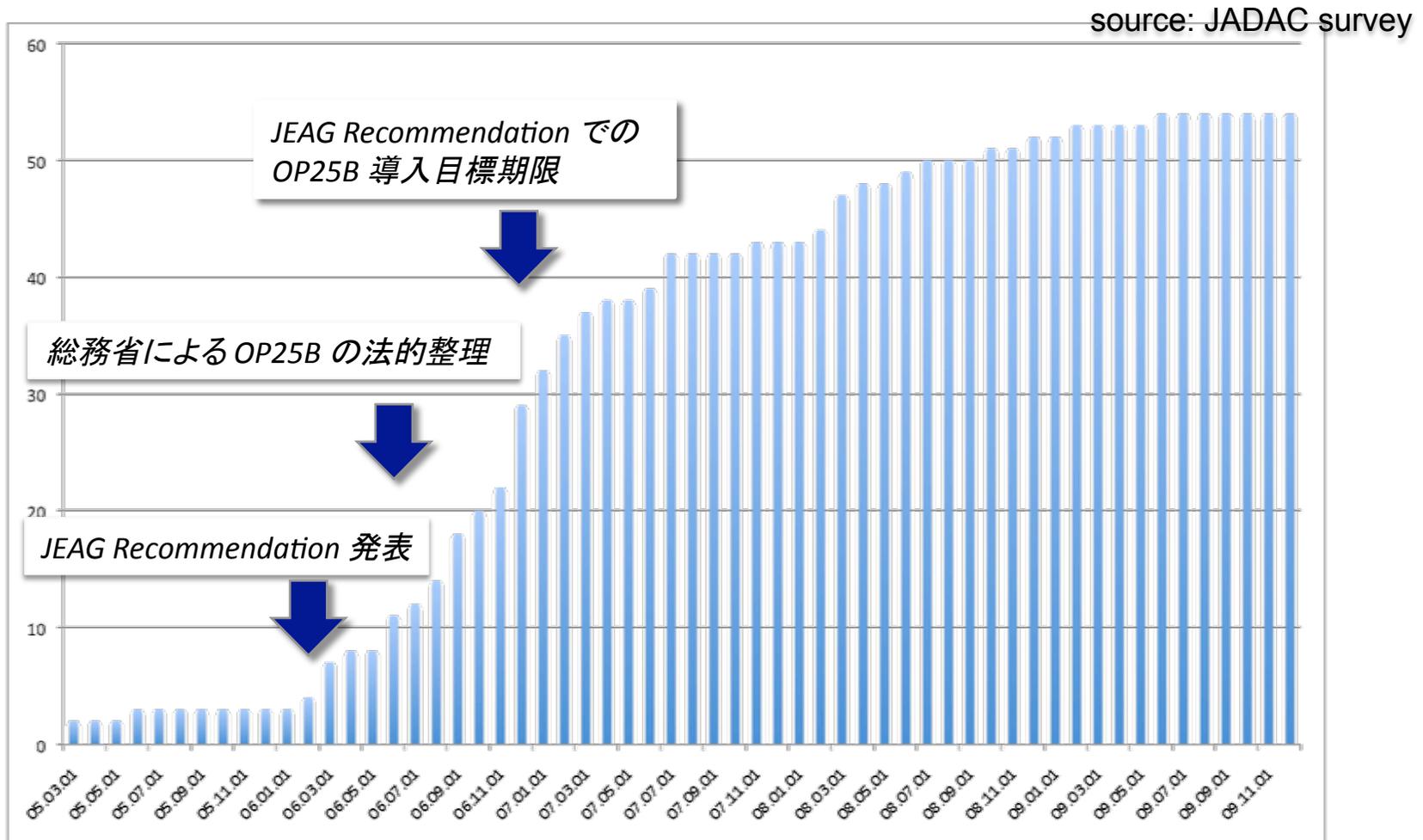
- 迷惑メール送信者の渡り
 - OP25B を導入すると迷惑メール送信が行えない
 - 導入していない別の ISP を契約して迷惑メール送信
ex. C社 → A社 → B社 → D社...
 - ISP は苦情が増えることにより OP25B 導入を早める



迷惑メール対策の取り組み – JEAG (cont.)

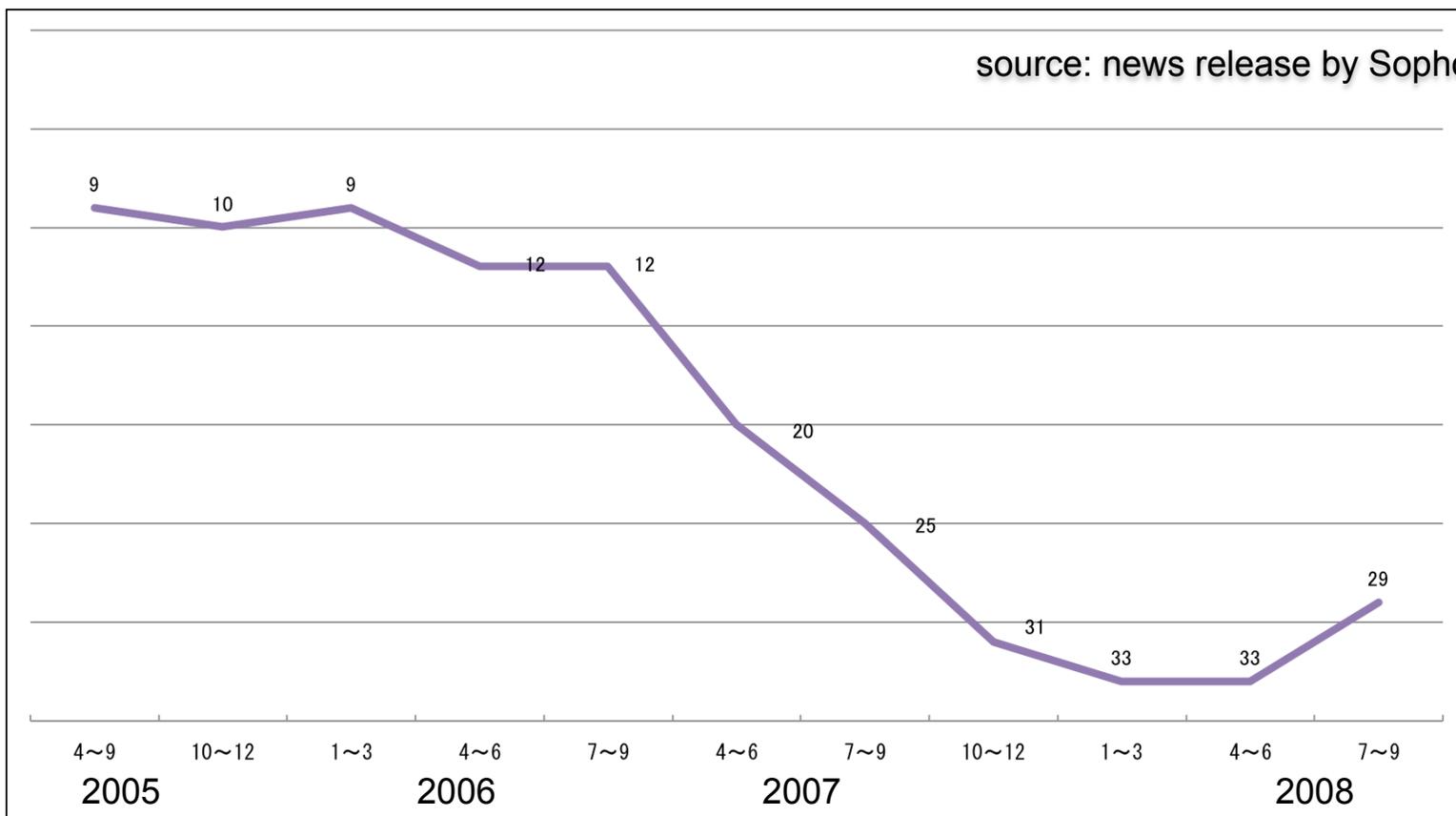
- 導入状況

- 日本の ISP での導入数の推移 (2005～2009)



迷惑メール対策の取り組み – JEAG (cont.)

- 導入効果
 - spam 送信地域ランキングでの日本順位の推移



迷惑メール対策の取り組み – 国際連携

- **MAAWG**

- 欧米を中心とした約190社の IT 企業による Working Group
- 年3回開催される General Meeting や mailing list での議論
 - 2010.06.08-10: 19th MAAWG General Meeting @ Barcelona, Spain
 - 2010.10.04-06: 20th MAAWG General Meeting @ Washington DC, USA
- 分野別のグループ
 - Technical Committee
 - Public Policy Committee
 - Anti-Phishing SIG
 - Botnet/Zombie Subcommittee
 - ISPCC (Closed Coloquium), etc



- **行政主体の多国間グループ**

- LAP (London Action Plan)
 - 2009.10.07-09: 5th Joint-LAP/CNSA Workshop @ Lisbon, Portugal
- Seoul-Melbourne MoU Meeting
- 日ASEAN情報セキュリティ会合
- ITU, OECD, etc



- **二国間協議**

- 中国 (中国工業・情報化部, ISC: Internet Society of China)
- 韓国 (KISA)
- ブラジル (CGI.br / cert.br)
 - 2010.05.07: Brazil-Japan Anti-Spam Workshop

まとめ

- **迷惑メールの今後**
 - 利益効率が良い間は今後も迷惑メールは増加
 - 新たな送信手法, 受け取ってもらうための技術は今後も進化

- **メール利用環境の整備を**
 - 今後は受信側への導入を促進し認証結果を有効活用
 - 詐称されないための対策 (送信ドメイン認証など) はもはや必須
 - メール の 疎通 は 今 後 も 悪 化 す る 可 能 性 あ り
 - 過度な対策は利便性を低下させる
 - 正しいメールを受け取る仕組み (送信ドメイン認証技術) を活用

- **様々な取り組み**
 - 迷惑メール対策推進協議会による“迷惑メール対策ハンドブック”の発行
 - 迷惑メール対策推進協議会に送信ドメイン認証技術 WG を設置し, 普及のための具体的な情報の整理など活動中
 - JEAG (Japan Email Anti-Abuse Group) Recommendation の改訂を検討中
 - MAAWG (Messaging Anti-Abuse Working Group) との実運用上の連携
 - IETF による標準技術の採用と普及





ご清聴ありがとうございました

お問い合わせ先 IIJインフォメーションセンター
TEL: 03-5205-4466 (9:30~17:30 土/日/祝日除く)
info@ij.ad.jp
<http://www.ij.ad.jp/>

Ongoing Innovation

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ、Internet Initiative Japanは、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示しておりません。©2010 Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。