迷惑メールの現状とこれまでの対策

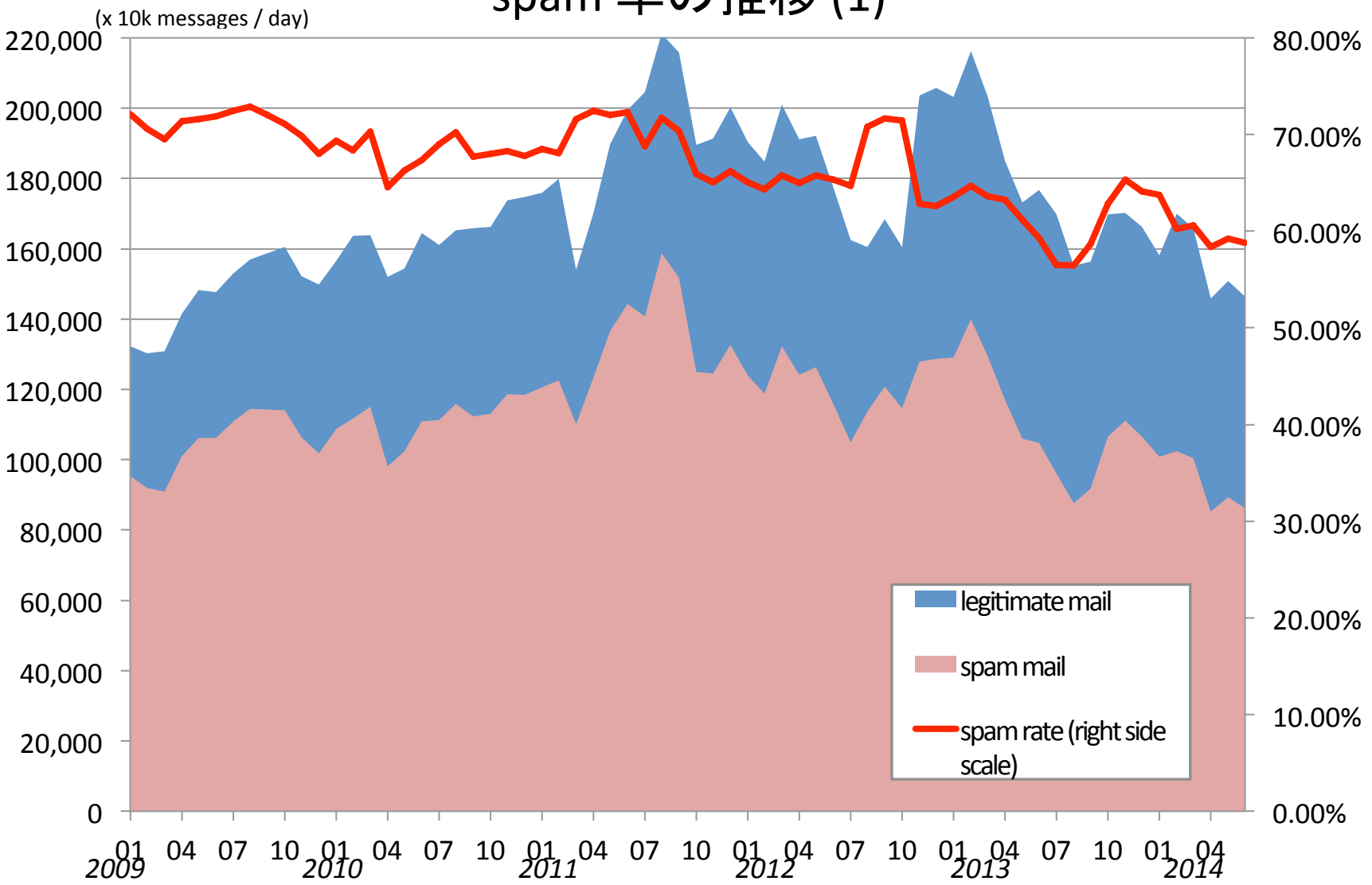
第11回 IAjapan 迷惑メール対策カンファレンス

2014.10.08

Shuji SAKURABA
Internet Initiative Japan Inc. (IIJ)

迷惑メールの現状

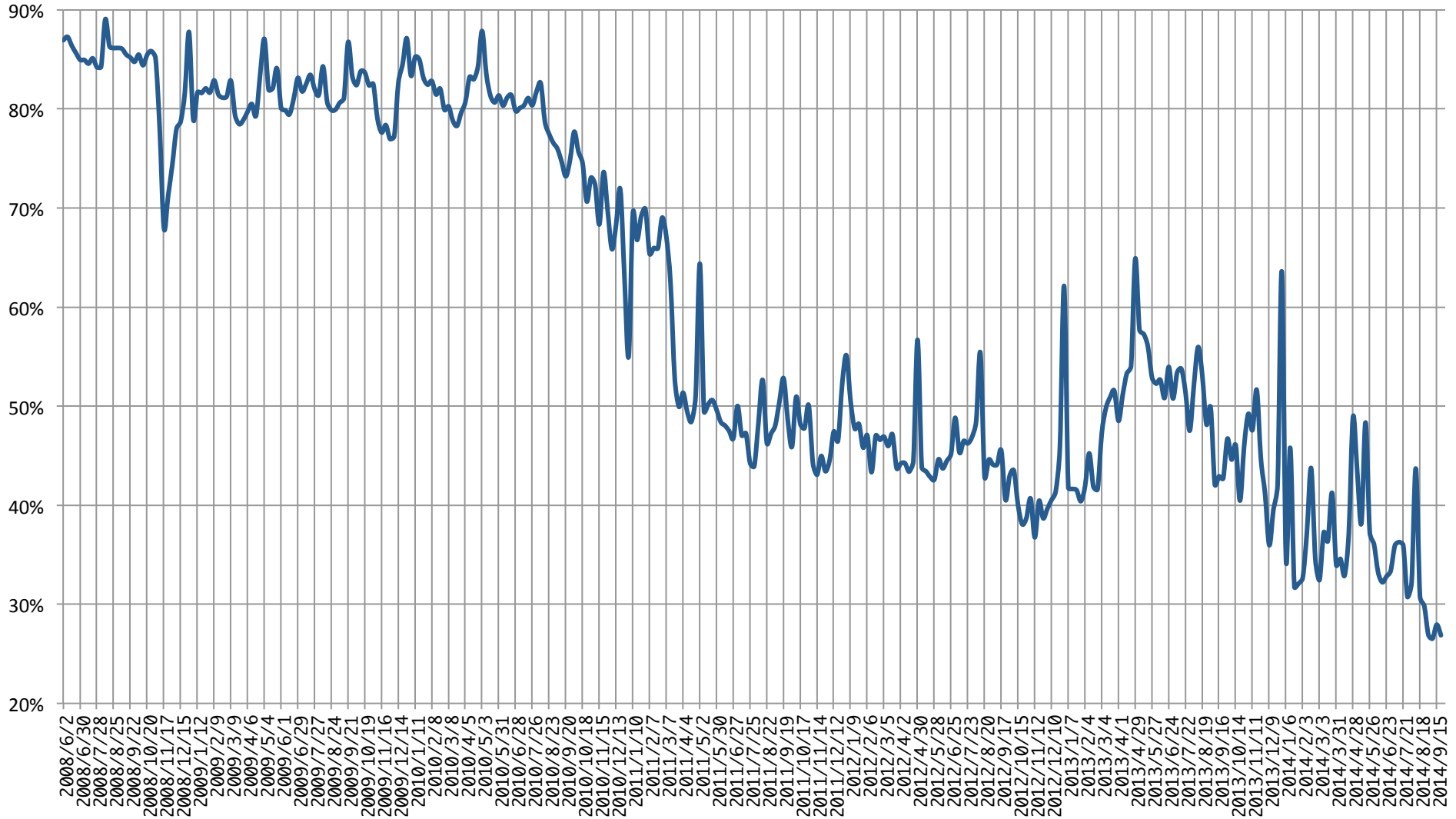
spam 率の推移 (1)



source: 電気通信事業者13社のデータを総務省がとりまとめ

迷惑メールの現状

spam 率の推移 (2)



source: IIJ IIR (Internet Infrastructure Review) より

迷惑メールの現状

2014年上半期の被害状況

- インターネットバンキングに係る不正送金事犯について、平成26年上半期の被害額が昨年の総被害額を上回る (平成26年9月16日、警察庁広報資料)
  - 1,254件, 約18億5,200万円
  - 被害が多くの地方銀行や信用金庫、信用組合に拡大するとともに、法人名義口座に係る被害が拡大 (都銀その他 14, 地銀 48, 信金信組 11)
  - コンピュータウイルスの悪質、巧妙化

	被害件数	被害額
平成26年上	1,254件	18億5,200万円
平成25年下	1,098件	11億9,300万円
平成25年上	217件	2億1,300万円
平成24年	64件	4,800万円
平成23年	165件	3億800万円

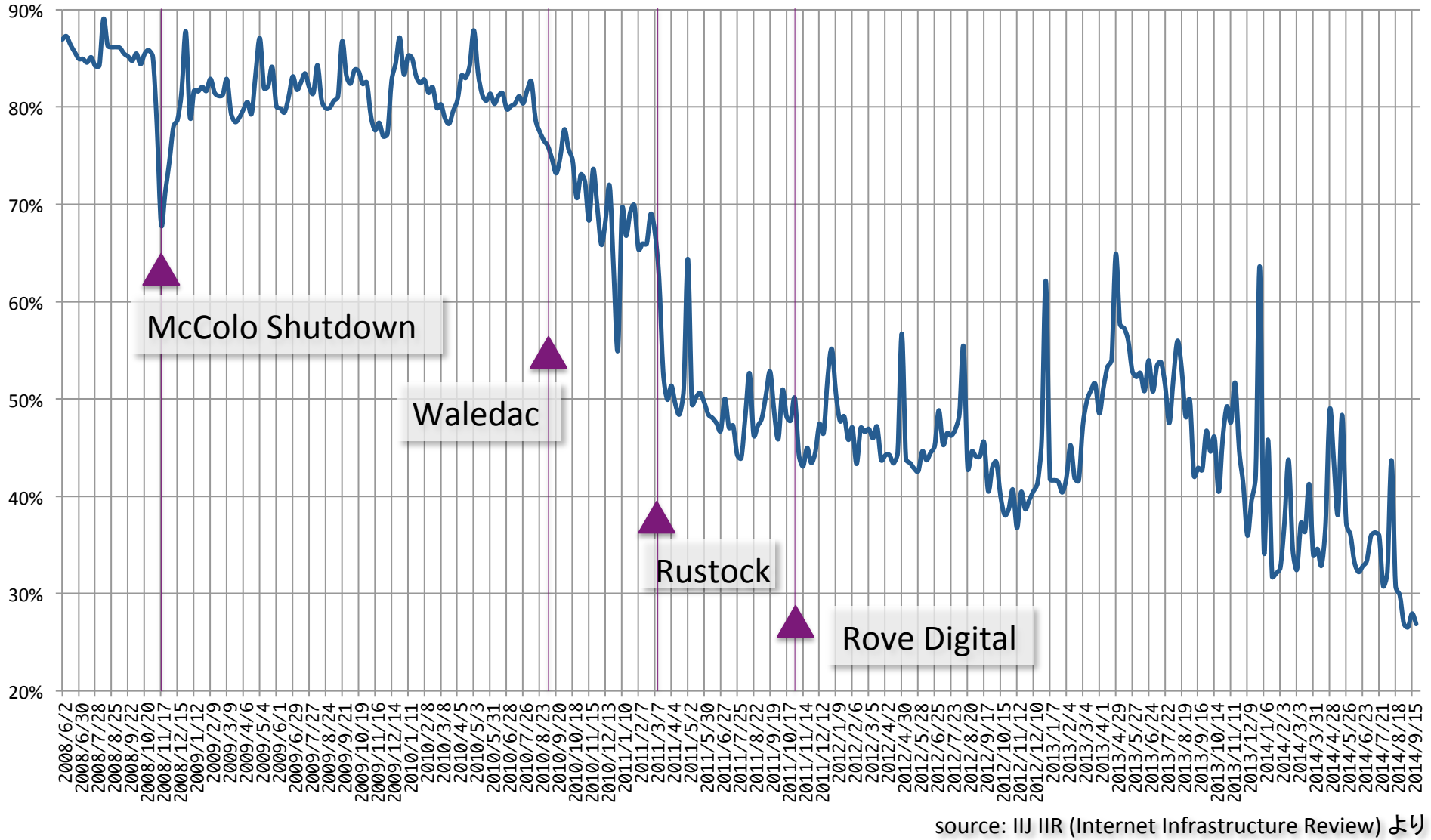
Source: https://www.npa.go.jp/cyber/pdf/H260904_banking.pdf

迷惑メール対策
送信側の対策

- ネットワーク的な対策
  - OP25B (Outbound Port 25 Blocking)
  - Source Address Validation (RFC3704, BCP84)
    - Asymmetric routing attack 対策
- メールサーバによる対策
  - SMTP-AUTH (RFC4954)
    - アクセス元地域の限定など
  - 送信数制限
  - SPF (RFC7208)
  - DKIM (RFC6376, STD76)
  - DMARC (draft-kucherawy-dmarc-base-04)
  - Contents Filter (Outbound Spam Filter)
- その他
  - Botnet の C&C サーバの takedown

迷惑メール対策

Botnet Takedown



source: IIJ IIR (Internet Infrastructure Review) より

迷惑メール対策
受信側の対策

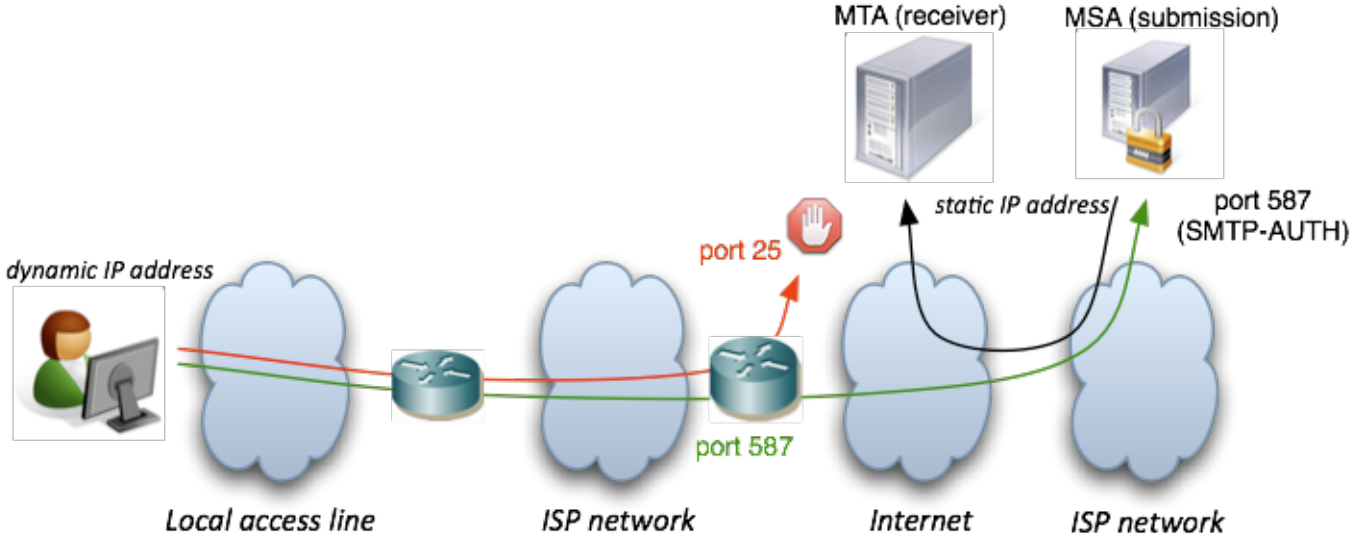
- ネットワーク的な対策
  - DNSBL (DNS Black List, IP address base)
  - GrayListing (送信元による一時的な接続拒否)
- メールサーバによる対策
  - Contents Filter (Signature, Sandbox, Heuristic Engine, etc)
    - Anti-Virus
    - Anti-Spam
  - 同一送信元からの大量受信制限 (throttling)
  - SPF (RFC7208)
  - DKIM (RFC6376, STD76)
  - DMARC (draft-kucherawy-dmarc-base-04)

ネットワーク的対策

- DNSBL (DNS Black List)
  - 仕組み: 接続元の IP アドレスを DNS の query や http を利用して Black List 管理元に問い合わせて受け取りを判断する
  - 長所: メールを受信する前に判断できるので処理負担は小さい
  - 短所1: Black List に登録されただけでメールが届かなくなる / 受け取れなくなる、解除されるまで継続する
  - 短所2: リスト解除のポリシーが曖昧なものもある
- Gray Listing
  - 仕組み: 接続元の善し悪しが判断つかない場合に temporary fail (4xx) を返答し正常な MTA であれば行われる再配送を期待する方法
  - 長所: 拒否するわけではないのでメールが失われることが (基本的には) ない
  - 短所1: 配送遅延が発生する
  - 短所2: 送信 MTA が fallback した場合など IP アドレスが変わった場合に再度 temporary fail する可能性がある (配送遅延が拡大)
- Source Address Validation
  - DNS や NTP, SNMP など UDP 通信を悪用した DDoS 攻撃の対策
  - メールに於いても、asymmetric routing attack (動的 IP を source IP として固定 IP 網から送信し、動的 IP アドレス側で受信を行う) 対策として有効

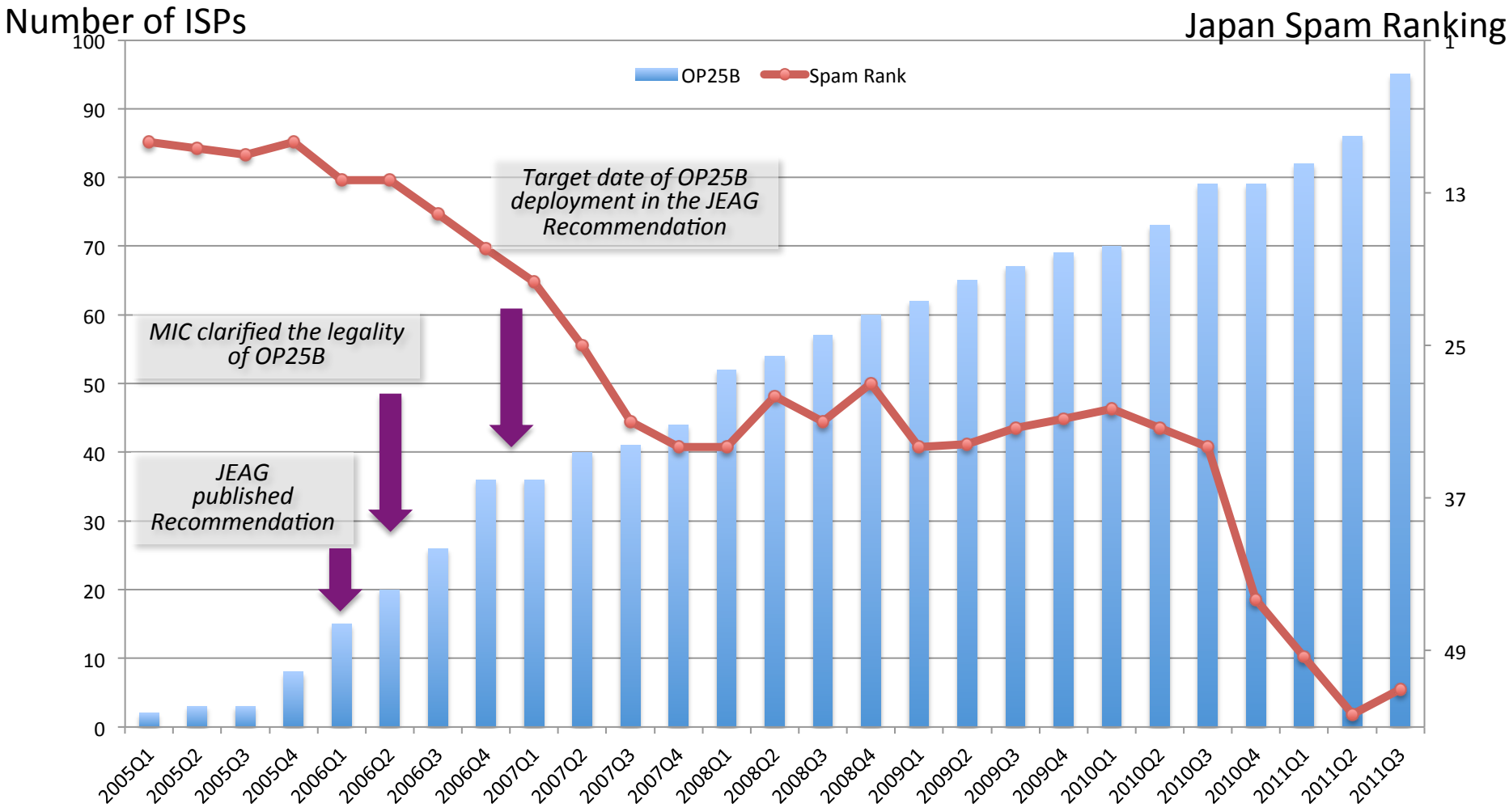
Outbound Port 25 Blocking
(OP25B)

- 導入目的
  - 動的 IP アドレスからの port 25 へのアクセスを禁止
  - 利用者の区別がしづらい個人向け接続サービスを利用した spam 送信対策 (検知され遮断されるまで spam を大量送信)
  - Malware 等に感染させられた PC (Bot) からの spam 送信対策
- 導入手順
  - MSA での port 587 での投稿できるよう準備 (SMTP-AUTH も導入)
  - 顧客提供用 IP アドレスの整理 (動的 IP と固定 IP を分離しやすいよう整理)
  - 顧客および他 ISP 等への事前周知
  - 適切なポイントでの Router への ACL (Access Control List) を設定
  - サポート窓口での適切な顧客対応の準備



Outbound Port 25 Blocking

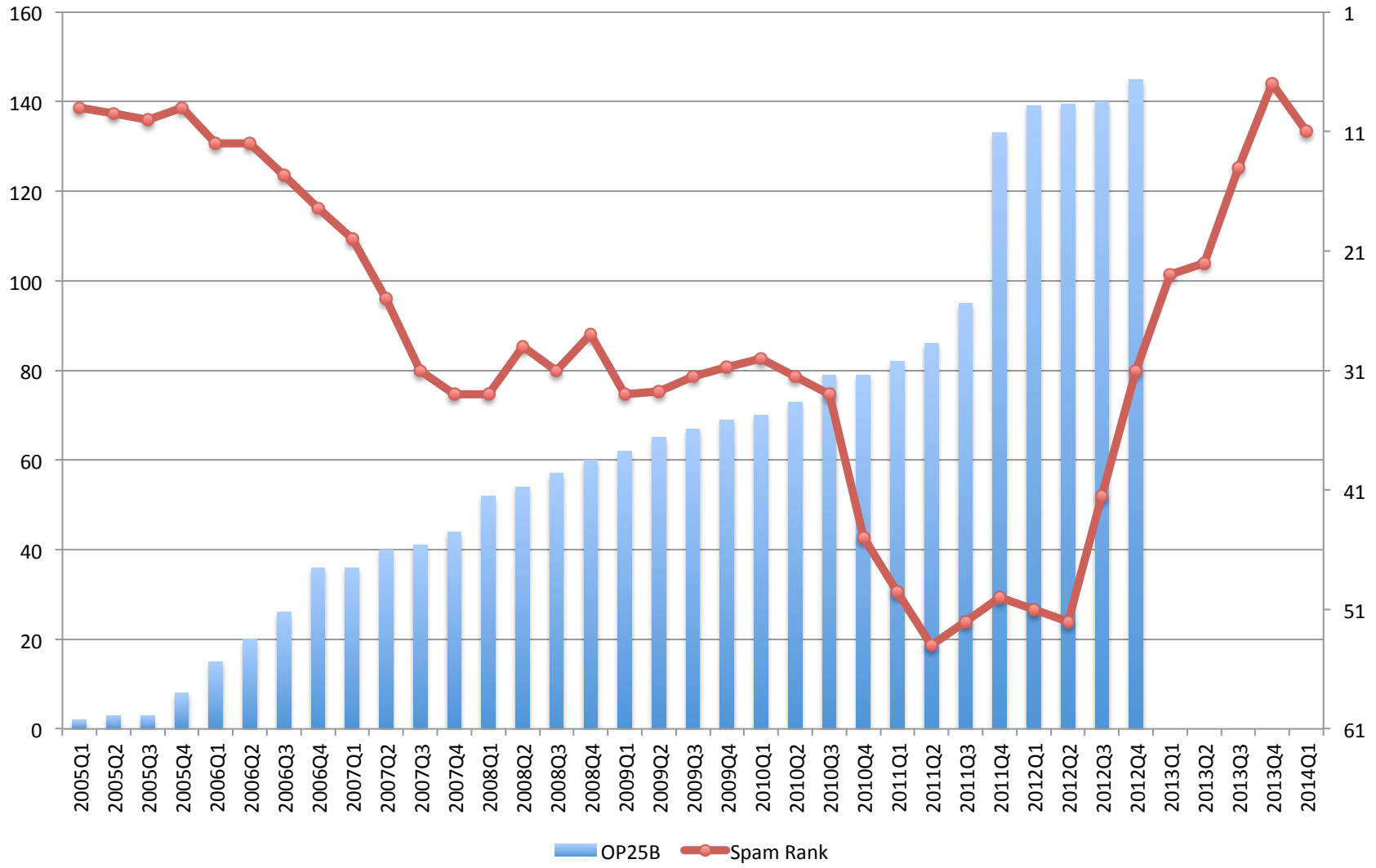
(効果)



Spam Rank: Based on Sophos's Dirty Dozen report
MIC: Ministry of Internal Affairs and Communication
JEAG: Japan Email Anti-Abuse Group

Outbound Port 25 Blocking

(現在の状況)

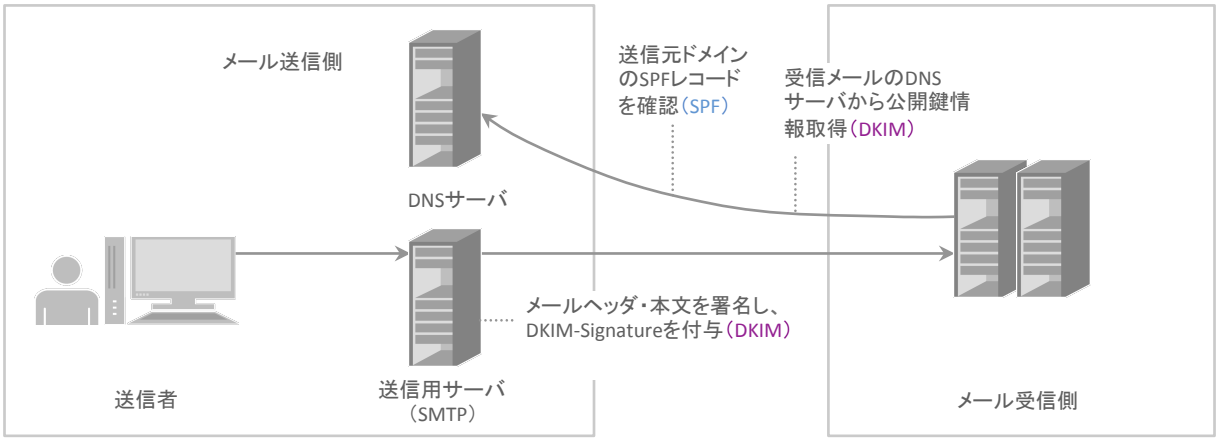


MSA での対策
送信者認証

- SMTP-AUTH (RFC4954)
  - メール送信時に ID/password による認証を行う
    - SASL (Simple Authentication and Security Layer, RFC4422) フレームワークを利用した認証メカニズム
    - PLAIN, LOGIN など暗号化されない認証では TLS (or over SSL) を併用すること
  - 認証した ID 毎に単位時間あたりの通数制限をかける
    - 例: 1,000通/日および一時的な大量送信時には送信効率を下げる制御の実施 (https://www.iij4u.or.jp/guide/mail_control/)
    - メルマガなど大量送信を行う場合は専用サービスの利用を推奨
  - 何かあった場合に送信 (認証) 元を判断するために有効
- その他注意
  - 古い認証の仕組みである POP before SMTP は送信者の特定困難さ (通数制限の適用等) や NAT 環境下での利用に適していない等のため廃止することが望ましい

送信ドメイン認証技術 (1)

- 基本的な仕組み
  - 送り手は送信元を明確に表明 (ごまかしがきかない情報を利用)
  - 受け手は送信元情報が正しく表明されているか確認 (認証)
  - DNS を利用することにより外部の認証機関が不要



SPF: Sender Policy Framework (RFC7208)
DKIM: DomainKeys Identified Mail (RFC6376, STD76)

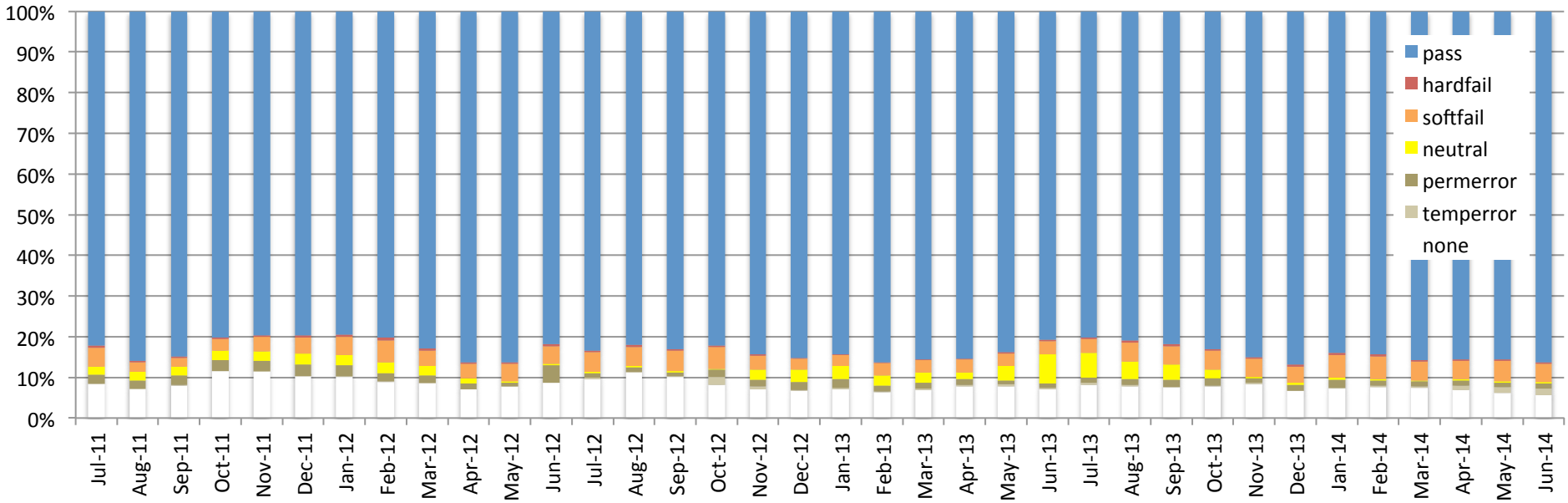
送信ドメイン認証技術 (2)

- 期待される効果
  - 受け取るべき送信者からのメールかを識別
  - 巧妙化する不正行為を事前に見破る
    - 有名サイトを騙ったフィッシング → 偽のサイトへ誘導し ID やパスワードを搾取
    - 信頼性が高そうな送信者を騙った不正プログラムの実行 (添付ファイルや不正サイトへの誘導) → botnet の拡散、malware の混入
    - 情報搾取を目的とした標的型攻撃 → 内部情報の外部への漏洩等
    - etc…
  - 迷惑メールを判定するのではなく送信者情報を認証する技術

→ メールに関連する種々の問題を解決するための基盤技術

SPF の動向 (1)

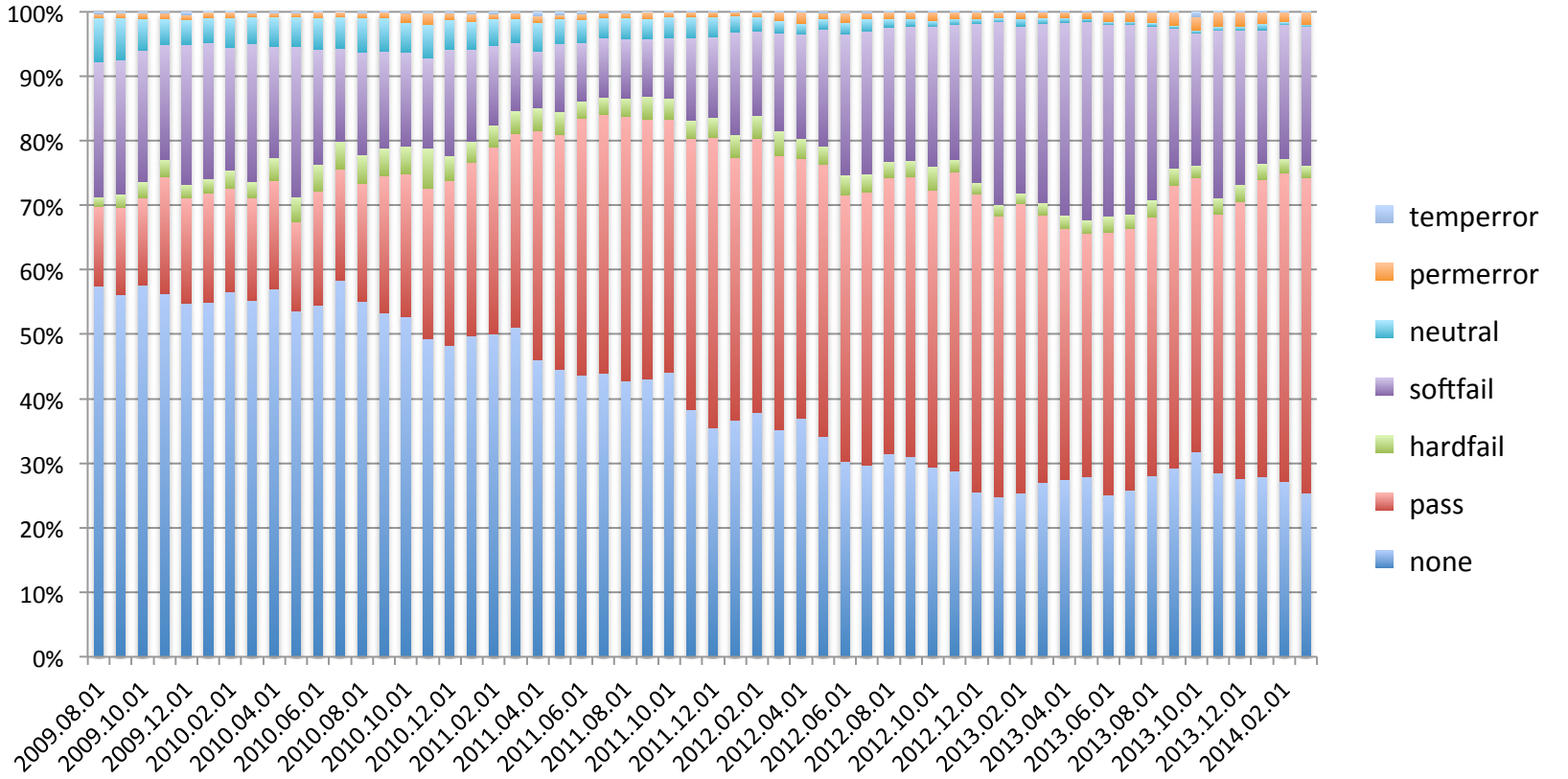
- SPF の導入状況
  - 総務省のとりまとめ (電気通信事業者7者の協力)
  - 94.31% 認証可能メールの割合 (2014.06)
  - 86.32% 認証結果が “pass” の割合 (2014.06)
    - 全体の迷惑メール割合と比べても高い (認証可能メールの 91.53% が “pass”)



Source: MIC survey (cooperate with 7 ISPs)

SPF の動向 (2)

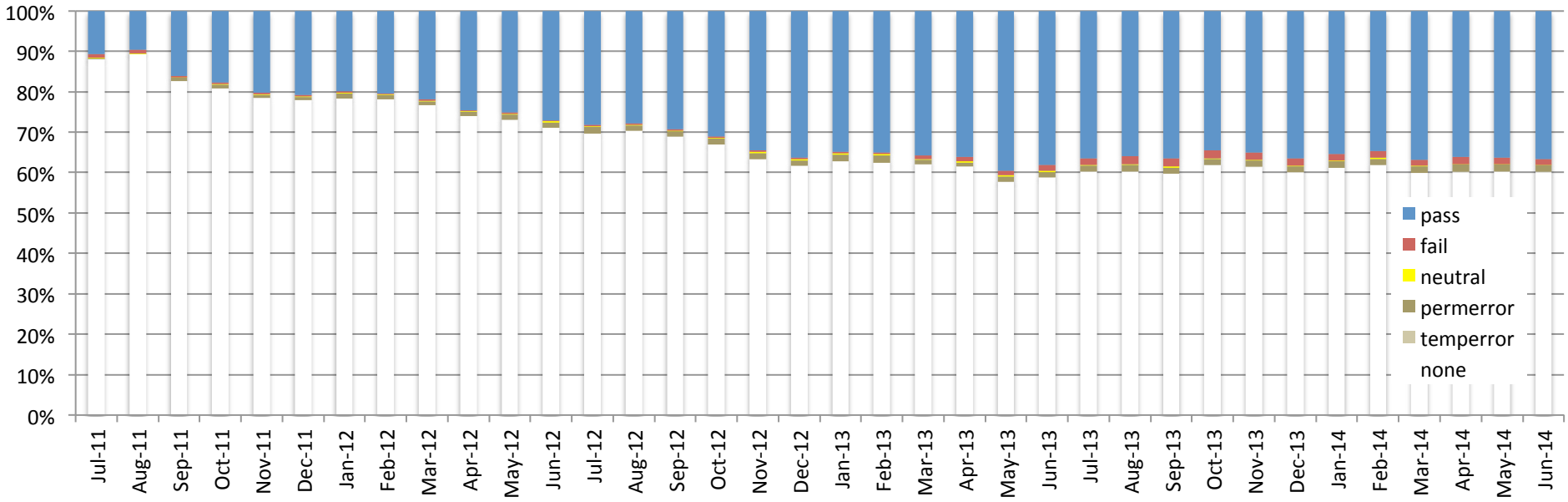
- SPF 認証結果割合の推移
  - 期間: 2009.08～2014.03
  - 74.59% 認証可能メールの割合 (2014.03)



Source: IIJ IIR (Internet Infrastructure Review)

DKIM の動向 (1)

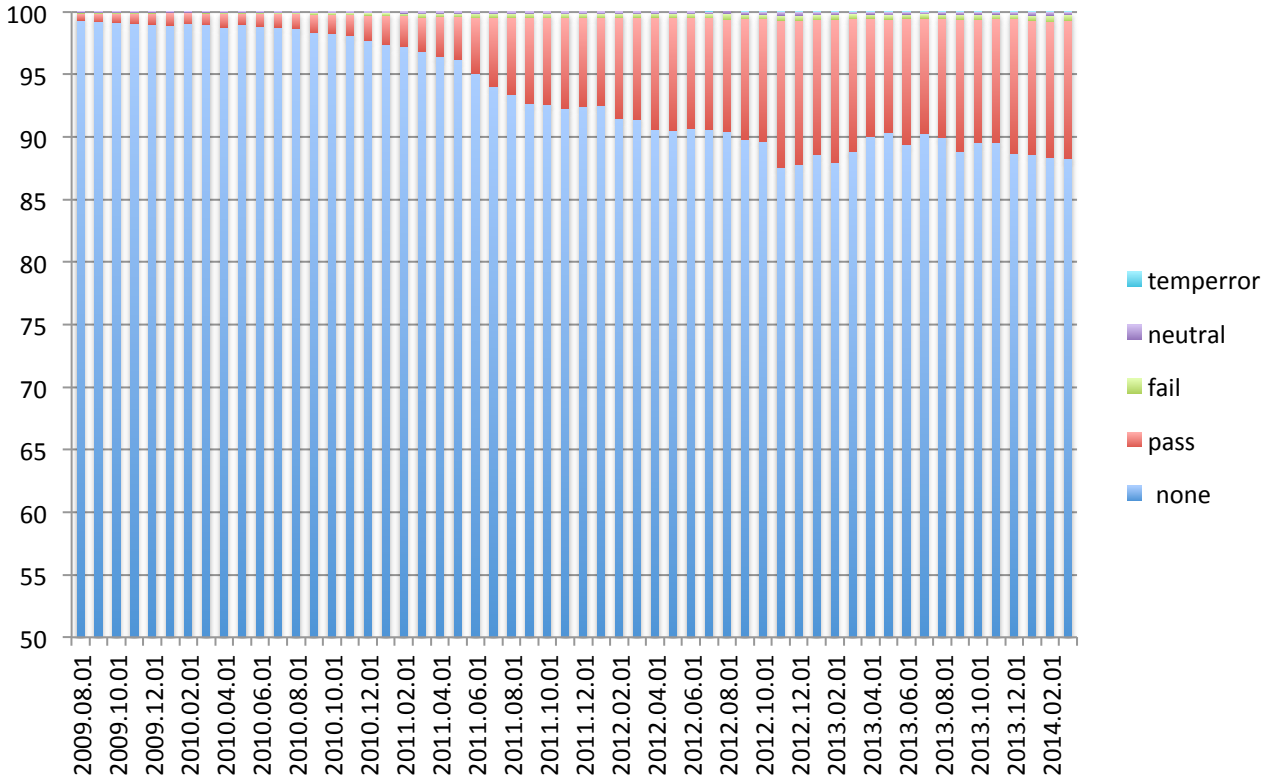
- DKIM の導入状況
  - 総務省のとりまとめ (電気通信事業社4社の協力)
  - 39.84% 認証可能メールの割合 (2014.06)
  - 36.73% 認証結果が “pass” の割合 (2014.06)
    - 92.19% (認証可能メールの “pass” の割合)



Source: MIC survey (cooperate with 4 ISPs)

DKIM の動向 (2)

- DKIM 認証結果割合の推移
  - 期間: 2009.08～2014.03
  - 11.72% 認証可能メールの割合 (2014.03)



Source: IIJ IIR (Internet Infrastructure Review)

DMARC

Domain-based Message Authentication, Reporting & Conformance

- 目的
  - ドメイン詐称を防ぐために既にある個別の仕組みをオープン化
  - 認証識別子の標準的な利用方法の確立
  - 認証の運用上の各種問題解決に役立てる
  - SPF & DKIM のより広い導入の動機付け
  - より積極的な認証方針 (policy) への奨励

- 特徴
  - 複数の認証技術 (SPF, DKIM) を利用
  - 信頼関係を築きより強い方針 (policy) を導入できるように受信側から送信側へフィードバックを行う
  - 認証の対象は、メールヘッダ上 (From: ヘッダ) のドメイン

DMARC (2)

- 動機と経緯
  - eBay, PayPal と Yahoo!, Google (Gmail) が DKIM を利用したフィッシング対策を開始
    - eBayとPayPal, フィッシング対策でGmailと協力 (2008.07.09, 日経BP ITpro News)
  - 初期のテスト結果は比較的良好
    - しかしながら認証が失敗するケースも多少あった
    - 単一の認証技術だけでなく複数の認証技術を利用すことに
    - 認証失敗の原因を究明できるよう Feedback が行えるような仕組みも必要
  - さらに他の送受信事業者を含めてより広いグループに拡張
  - グループで初期ドラフトを作成し、2011年の MAAWG で提示、2012.01.30 DMARC.org として発足 (dmarc-discuss ML)
  - 2012.11 85th IETF @ Atlanta で dmarc WG を提案、その後 IETF へ (dmarc-ietf ML)

DMARC
(3)

- 送信側としての準備
  - DKIM と SPF の導入 (and/or)
  - 利用する識別子の整理 (Identifier Alignment)
  - フィードバック受信の準備 (メールアドレスの用意)
  - DMARC policy (DMARC record) の宣言
    - 対象となるドメインの “_dmarc” サブドメインの TXT RR
    - 最初は “p=none” から

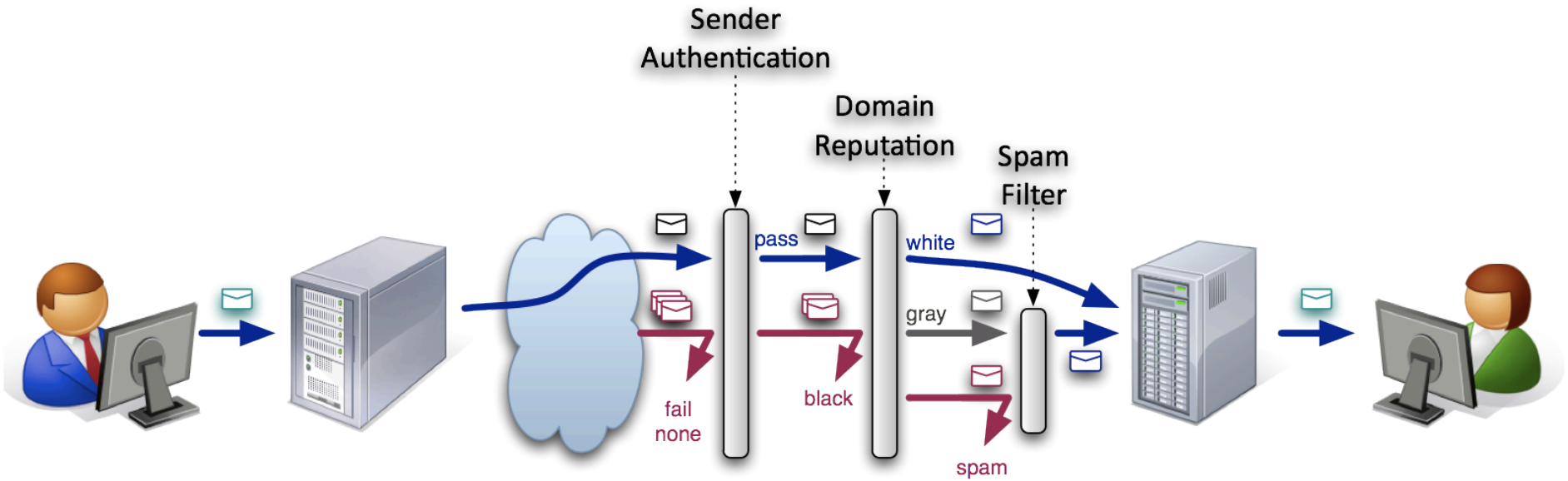
```
_dmarc.example.jp TXT "v=DMARC1; p=none; rua=mailto:dmarc-feedback@example.jp"
```

  - 送信ドメイン認証の結果確認と調整 (feedback を利用)
  - DMARC policy の調整 (“pct=” と “p=“ による段階的な強化)
    - 次の段階として “p=quarantine” と “pct=小さい値”
    - さらに次の段階として “pct=100” に
    - さらに “p=reject” と “pct=小さい値”
    - 段階的に p と pct を引き上げて行く

DMARC (4)

- 受信側の導入
  - ヘッダ From (RFC5322.From) からドメインを取り出す
    - 取り出すドメインは一つだけ
  - DMARC policy レコードを取り出す
    - DMARC TXT レコードが存在しない場合 Organizational Domain に問い合わせを行う
  - DKIM 署名の検証と SPF 認証を行う
    - 認証が成功 (pass) したドメインを利用する
  - 認証された識別子 (ドメイン) と Identifier Alignment をチェック
  - DMARC 方針 (policy) を適用して処理する
  - DMARC Feedback
    - “rua=”: 集約レポート (aggregate reports), XML 形式
    - “ruf=”: 失敗レポート (failure reports, forensic reports), ARF を利用

送信ドメイン認証技術の利用



- Sender Authentication & DMARC
  - 認証結果 none のメールを柔軟に対応 (**移行期**)
  - 正当なメールの送信元がほとんど対応していることを前提に pass 以外は詐称と判断して reject (**最終形**)
- Domain Reputation
  - 認証された送信者情報 (詐称されていない) を評価して受け取るべきメールだけを受け取る (Domain White List の利用)
- Spam Filter
  - ドメインレピュテーションで判定ができなかった送信元のメールを内容などを基に spam 判定 → 結果はレピュテーションへ feedback

課題

- メール配送形態による認証の失敗 (indirect mail flows)
  - メール転送による SPF の認証失敗
    - 転送元での RFC5321.From の書き換え → 転送先で SPF は pass → DMARC では RFC5322.From と不一致 (fail)
    - DKIM の導入 or 転送先でのホワイトリスト (転送者≒転送受信者なので) で対応
  - メーリングリスト機能
    - Mailman などでは RFC5321.From はメーリングリスト管理アドレス → SPF は pass → DMARC では RFC5322.From と不一致 (fail)
    - Subject: ヘッダの書き換え (ex. “[dmarc-ietf]” の付与等) → DKIM の認証失敗 → コンテンツの改変を止める
    - Mailman の次バージョンでは From: ヘッダを書き換える機能が追加されるとの情報もあり
- 日本におけるDKIMの普及

普及に向けて

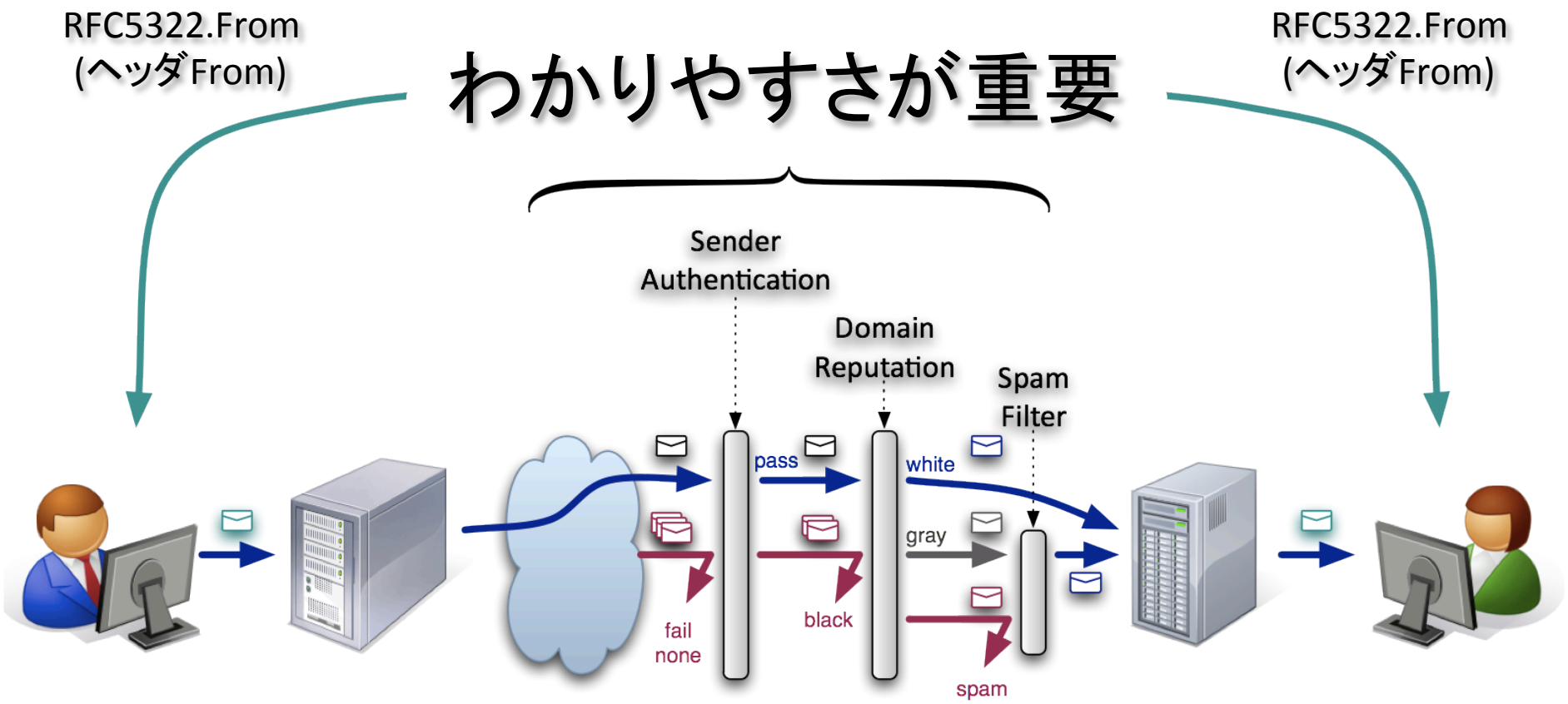
- 向かうべき方向性
  - SPF, DKIM 双方の良いところをうまく活用
  - メールの責任の所在を明確に
    → RFC5322.From (ヘッダ From) を基軸に
  - 認証がうまくいかないケースが見つけ出せる仕組み (reporting) & 対策の検討 → feedback の仕組みへと
  - 認証したドメインを評価するための仕組みとそれを利用した受信対策 → Domain Reputation

↓

DMARC

(Domain-based Message Authentication, Reporting & Conformance)

普及に向けて


RFC5322.From
(ヘッダFrom)
わかりやすさが重要
RFC5322.From
(ヘッダFrom)
Sender
Authentication
Domain
Reputation
Spam
Filter
pass
white
gray
fail
none
black
spam