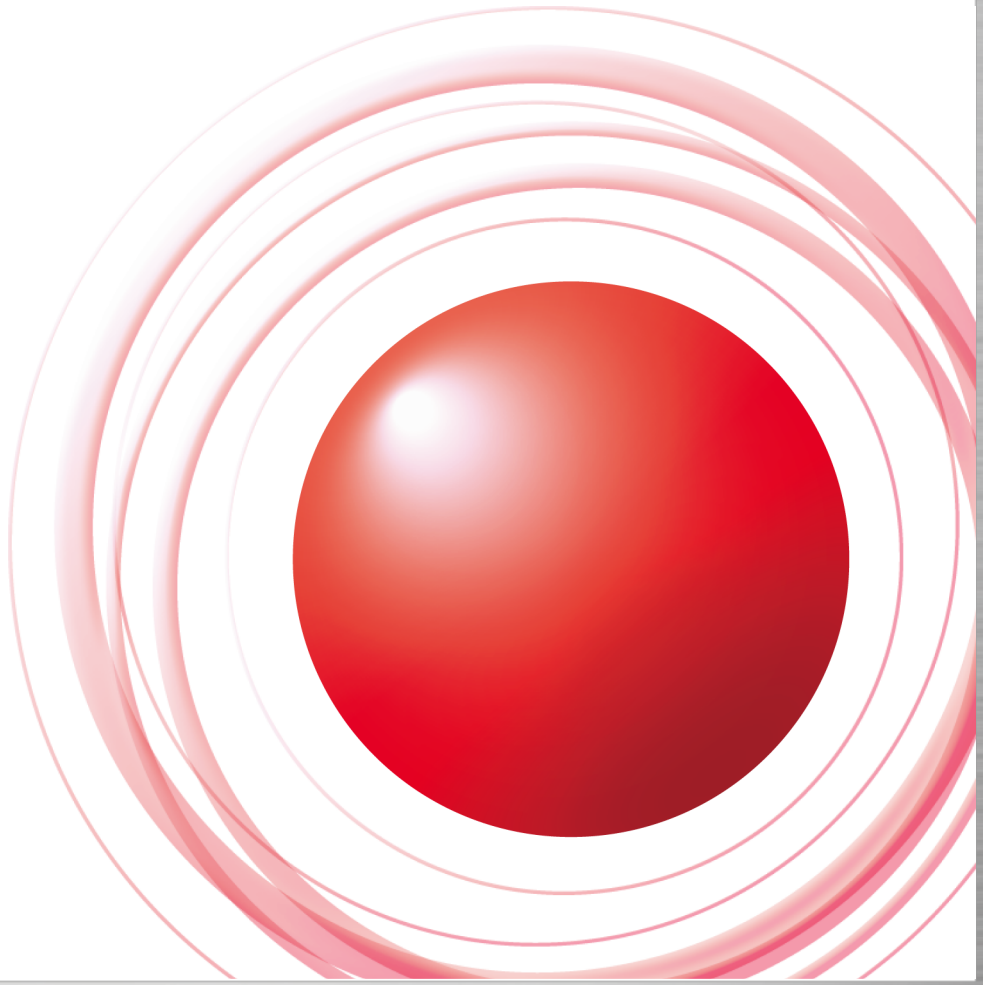
送信ドメイン認証技術の普及促進

IAjapan 迷惑メール対策セミナー [新潟]

IIJ Internet Initiative Japan



2011.11.25

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

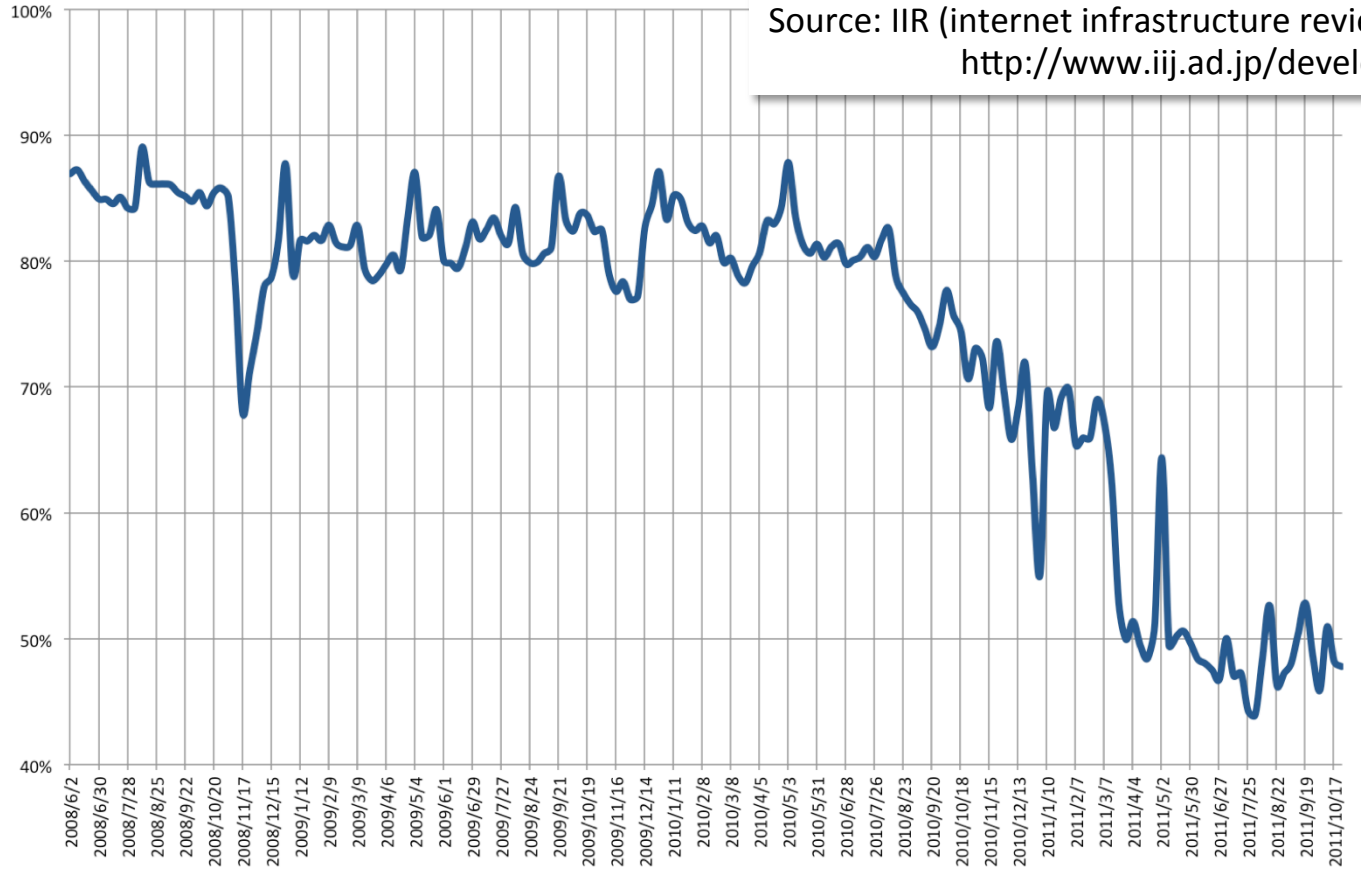
Ongoing Innovation

Agenda

- **迷惑メールの現状**
  - 迷惑メールの割合の推移
  - 送信元の割合
  - 動向について
- **送信ドメイン認証技術**
  - 概要
  - SPF/SIDF の導入
  - DKIM の導入
- **迷惑メール対策**
- **送信ドメイン認証技術の導入状況**
- **まとめ**

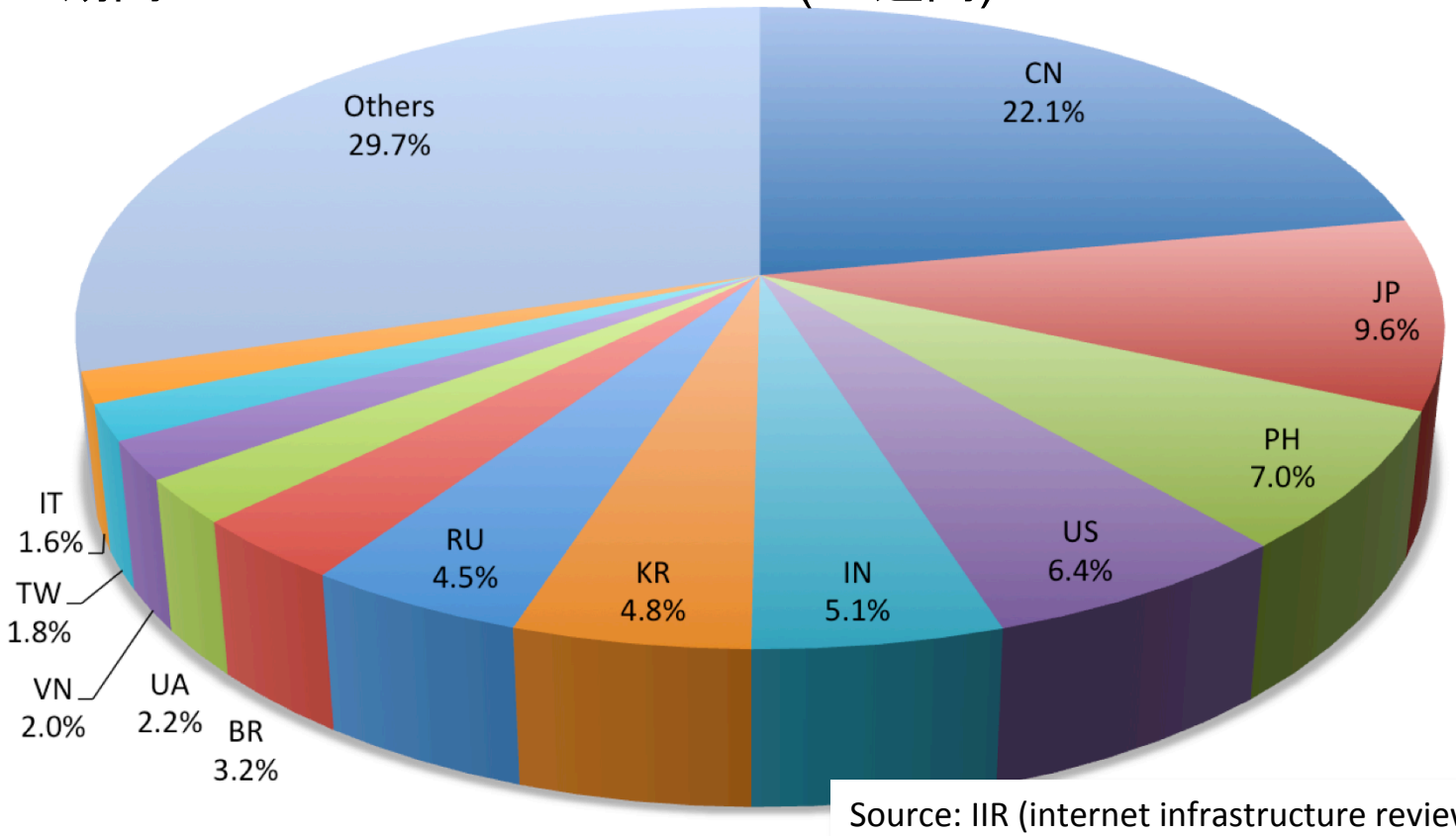
迷惑メールの現状 – 割合の推移

- **調査概要**
  - IIJ が提供する迷惑メールフィルタによる検知率の推移
  - 2008.06.02 ～ 2011.10.30 (178週)



迷惑メールの現状 – 送信元の割合

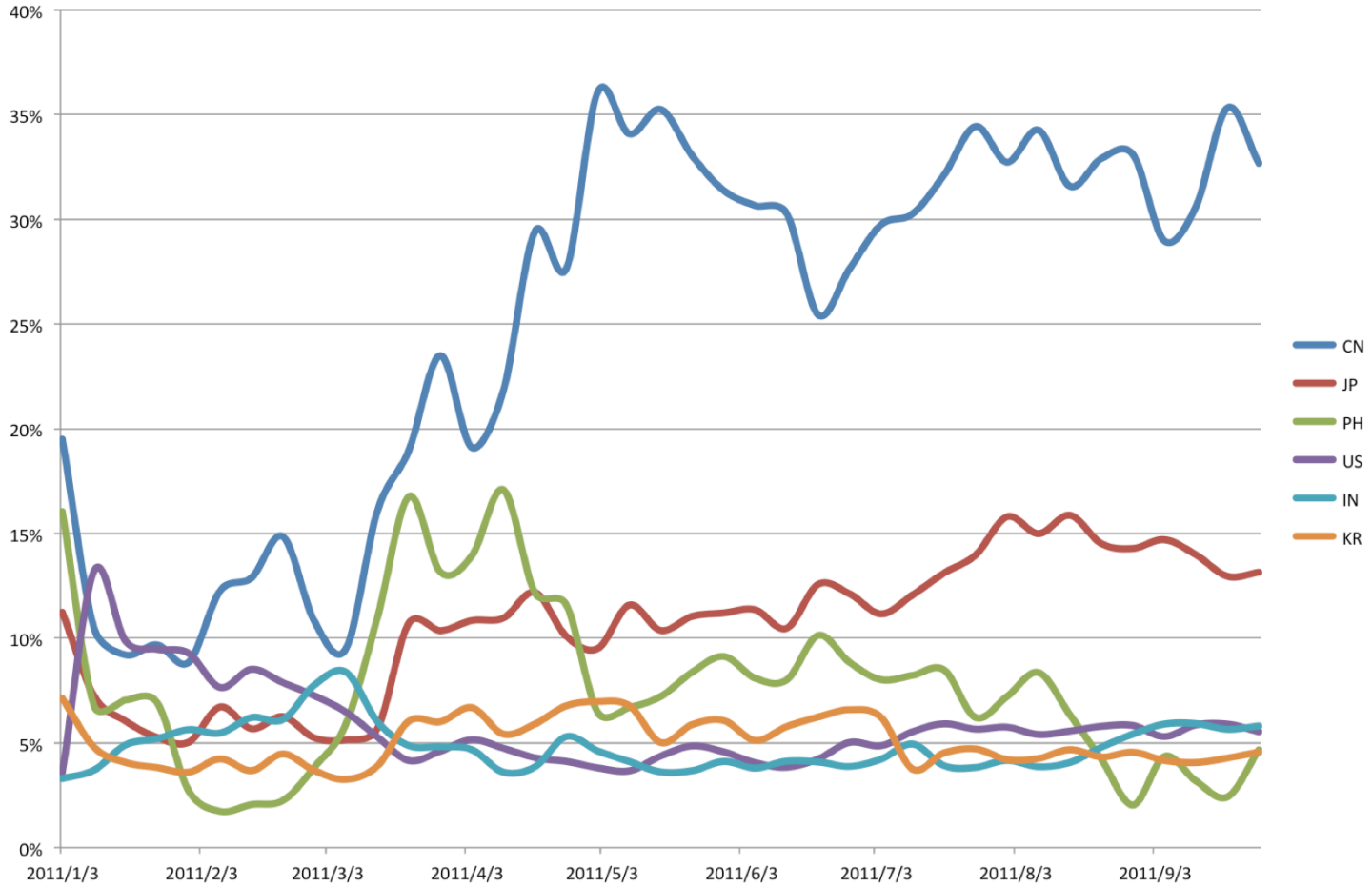
- **調査概要**
  - IIJ が提供する迷惑メールフィルタで検知した送信元の割合 (一部)
  - 期間: 2011.01.03 – 2011.09.25 (39週間)



Source: IIR (internet infrastructure review)
http://www.iij.ad.jp/development/iir/

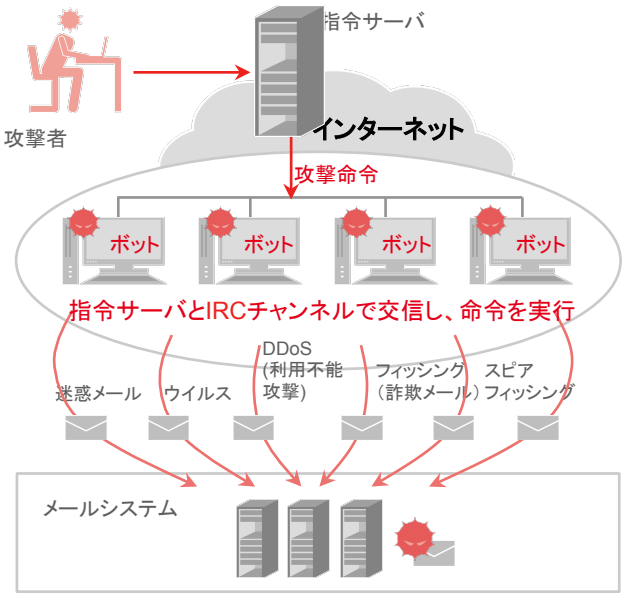
迷惑メールの現状 – 主要送信元の推移

- **調査概要**
  - 上位6地域の割合の推移 (2011.01.03 – 2011.09.25, 39週間)



迷惑メールの現状 – グローバル動向

- **Botnet の活動低下と送信元の変化**
  - 2010年後半から Rustock, Waledac など大規模な botnet を活動停止に追い込んだことにより世界的に迷惑メール (spam) 量が減少
  - 2011年Q2 (7月～9月) で平均 48.2% (2011Q1は50.2%なので微減) となりやや底を打った状況
  - 日本で受信する迷惑メールの主要送信元は欧米からアジアにシフト、botnet (米国, 欧州) から近隣 (CN, PH, KR, etc) の特定送信元へ
- **脅威の変化**
  - APT (Advanced Persistent Threat)
  - 大量送信からより巧妙な手法やソーシャル的な手法等を用いた標的型 (targeted,spear) 攻撃へ以降していると情報も



迷惑メールの現状 – 日本の動向

- **グローバルとの対策の違い**
  - 日本では、主要 ISP が OP25B (Outbound Port 25 Blocking) を導入していることにより、元々 bot 発の迷惑メールが少ない
- **不正プログラム (malware) の被害と対策**
  - 警察庁によると、全国の金融機関のインターネットバンキングで、利用者の契約者番号やパスワードが抜き取られ、預金が他人名義の口座に不正送金される被害が相次ぎ、今年4月から今月上旬までの半年ほどの間に総額で約2億8千万円の被害が出ていることが判明 (msn産経ニュース *2011.10.18*)
  - 警察庁によりますと、被害にあったパソコンからは、数年前からアメリカやヨーロッパの金融機関で大きな被害が出たものと似たタイプのスパイウェアが見つかりました (NHK *2011.10.19*)
  - 政府機関における標的型不審メール訓練について (情報セキュリティ対策推進会議 (CISO等連絡会議) 第3回会合、政府機関における標的型不審メール訓練について)

迷惑メールの現状 – 対策について

- **入り口防御**
  - Firewall　等に守られた組織内部への侵入にはメールが依然として有効な手段 (door opener)
  - ウイルス対策や組織内部のメール受信者の啓蒙にも限度
  - 送信元を確認して必要なメールだけを受け取る

  受け取るべきメールを判断するための仕組み → 送信ドメイン認証技術

- **出口防御**
  - 内部から踏み台にされていないか監視が必要
  - メール送信側として受け取ってもらうための努力も必要

  受け取ってもらうための仕組み → 送信ドメイン認証技術

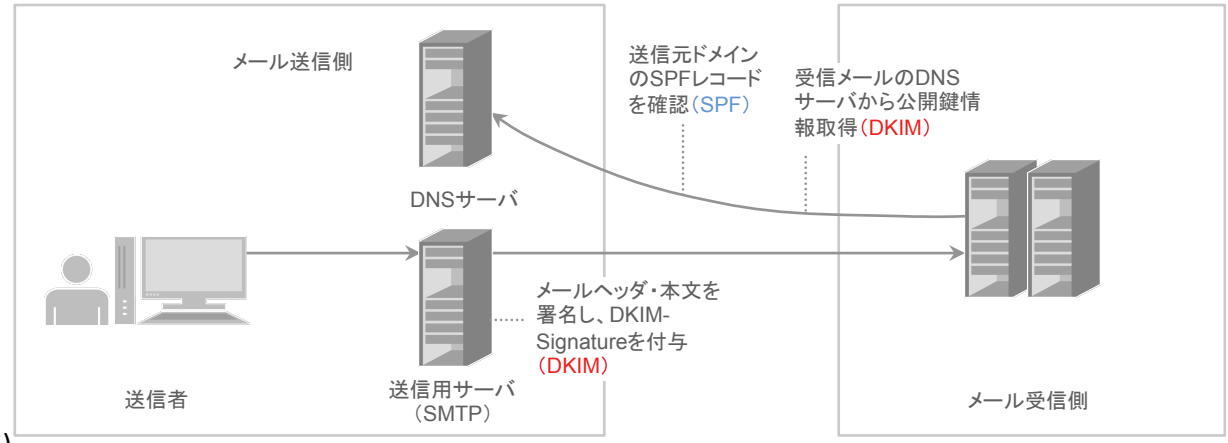
送信ドメイン認証技術 – 概要 I

- **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
- **期待される効果**
  - 信頼できる送信者からのメールを識別 → 優先受信等
  - 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、spyware 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

送信ドメイン認証技術 – 概要 II

- **ネットワーク方式 (SPF/SIDF)**
  - メールの送信元 (IP アドレス) と送信者情報のドメインを利用
  - SPF の送信者情報: reverse-path (メール配送上の送信者)
  - SIDF の送信者情報: PRA (Purported Responsible Address, メールヘッダ上の送信者)
- **電子署名方式 (DKIM)**
  - メール送信側はメールのヘッダと本文から電子署名を作成
  - 電子署名はヘッダとして記述、署名者の情報 (ドメイン) も含む

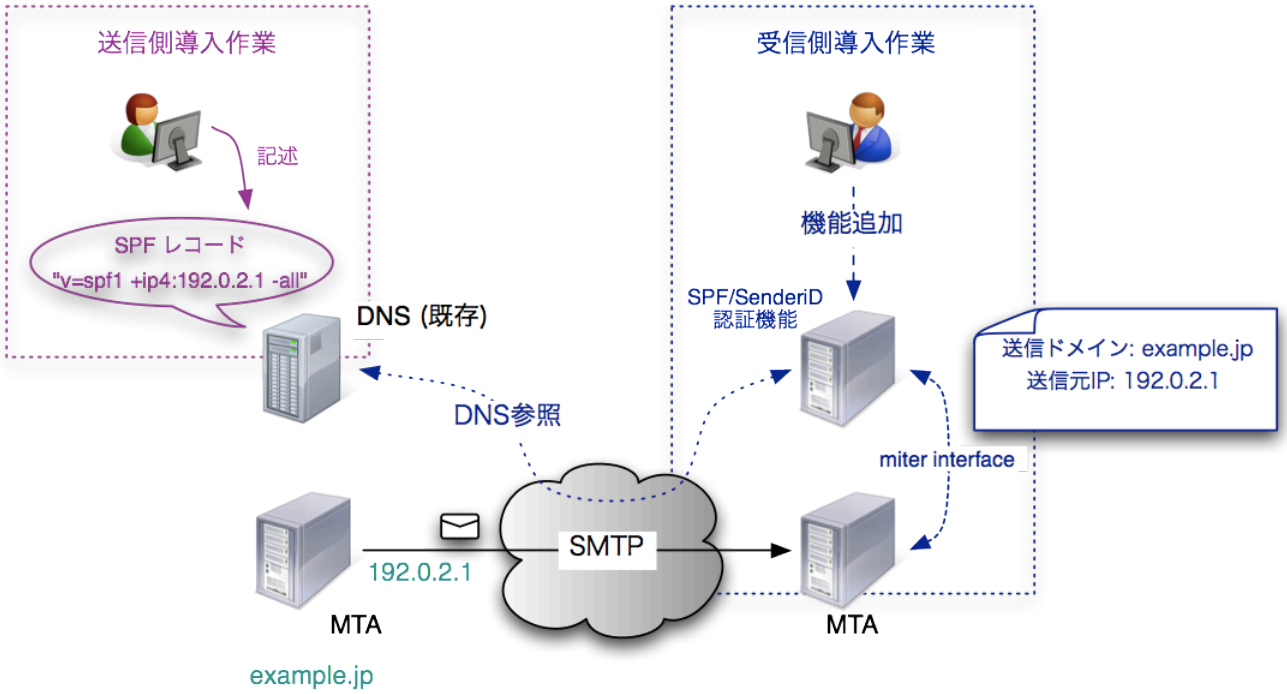


SPF: Sender Policy Framework (RFC4408)
SIDF: SenderID Framework (RFC4406,4407)
DKIM: DomainKeys Identified Mail (RFC6376)

SPF / SIDF の導入 – 導入方法

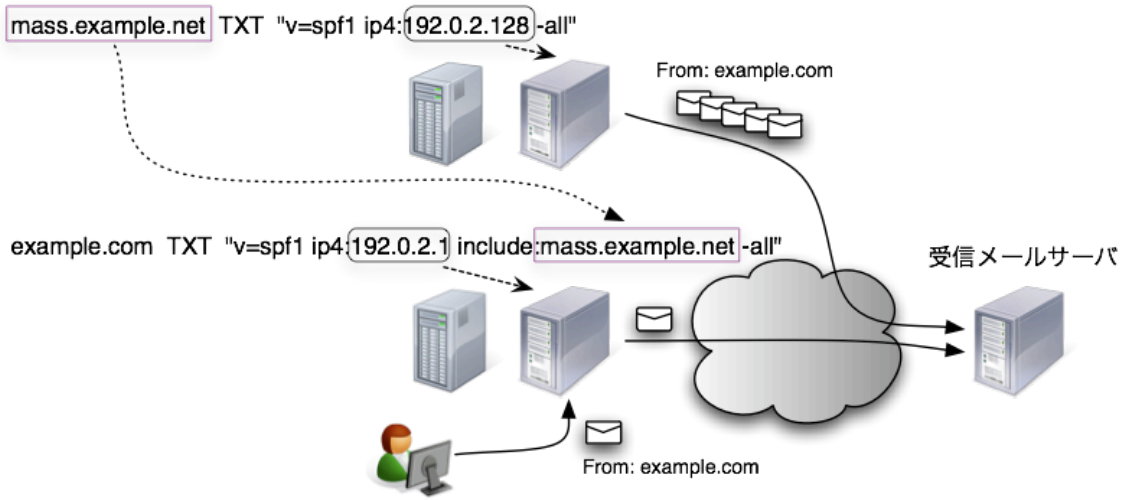
- **送信側**
  - 対象ドメインにメールの出口を示す SPF レコード (TXT) を設定
- **受信側**
  - 受信 MTA に認証機能を追加

milter interface:
open souce の MTA である Sendmail/Postfix で機能拡張時に外部プログラムと連携するためのインタフェース



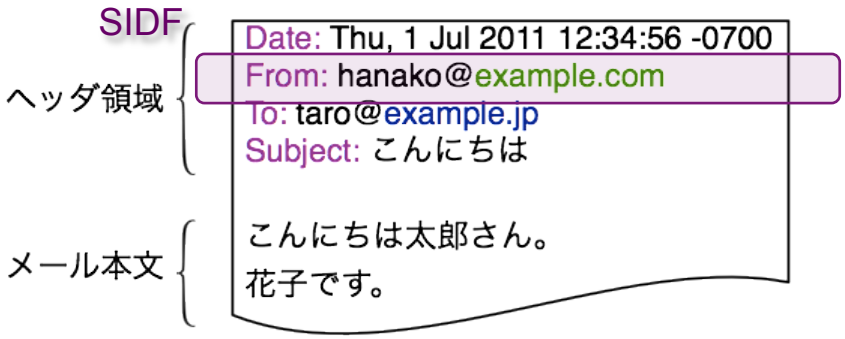
SPF / SIDF の導入 – 送信側

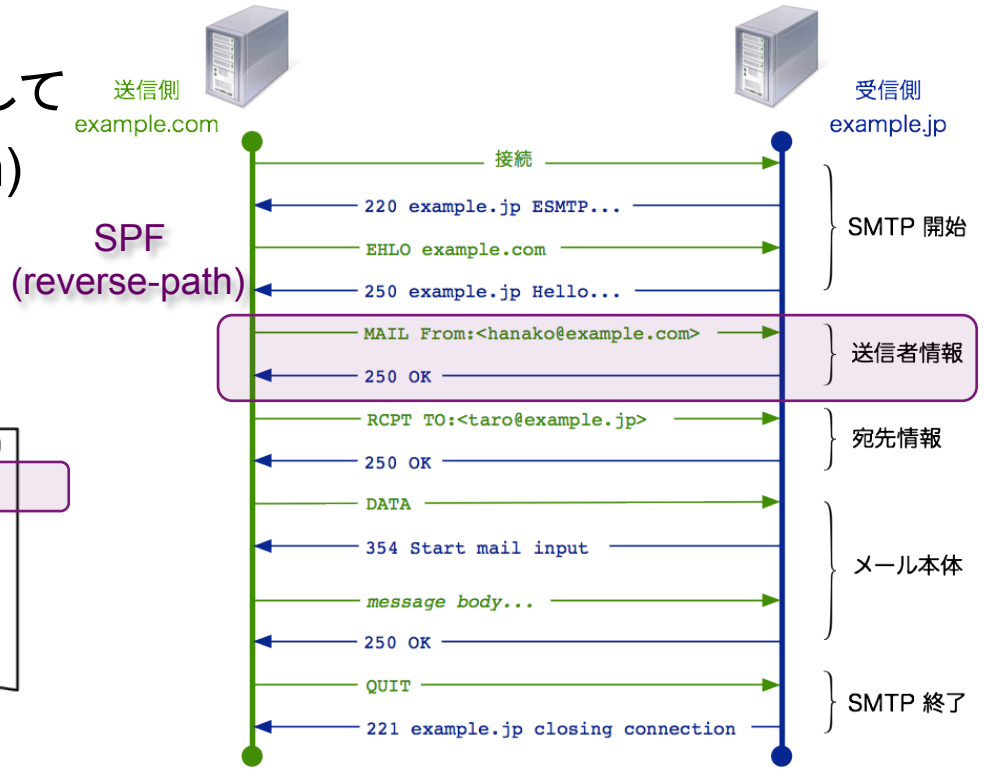
- **SPF レコードの設定**
  - 受信側にとって DNS の参照は負荷の増大につながるため最小限の lookup にとどめるべき (`"ip4"` or `"ip6"` を推奨)
  - SPF の仕様では DNS 参照の上限は10回 (`include` なども含む)
  - `"mx"` や `"ptr"` レコードの利用は DNS 参照を増加させるので注意
  - 参照先が設定変更する可能性があるので，管理外のホスト名を勝手に記述したり SPF レコードを `"include"` しない
  - メール配信業者やホスティング業者は，include 用の SPF レコードを用意 → ドメイン管理側が取り込みやすい様に



SPF / SIDF の導入 – 受信側

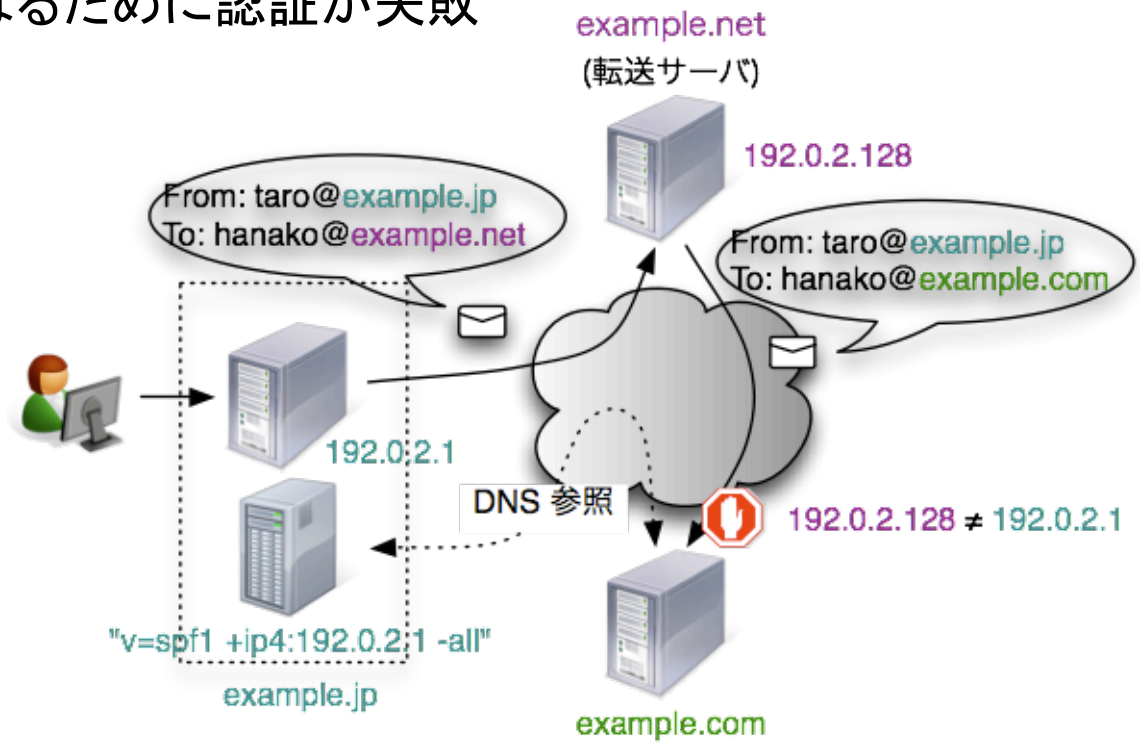
- **SPF が認証する送信者情報**
  - 配送 (SMTP) 上の reverse-path
  - 通常メール受信者 (受取手) が見ることが出来ない情報
- **SIDF が認証する送信者情報**
  - ヘッダ上の送信者 (PRA)
  - 必ずしも一般的に送信者として提示されるヘッダ (ex. From) が優先して参照されない (ex. Resent-*, Sender)





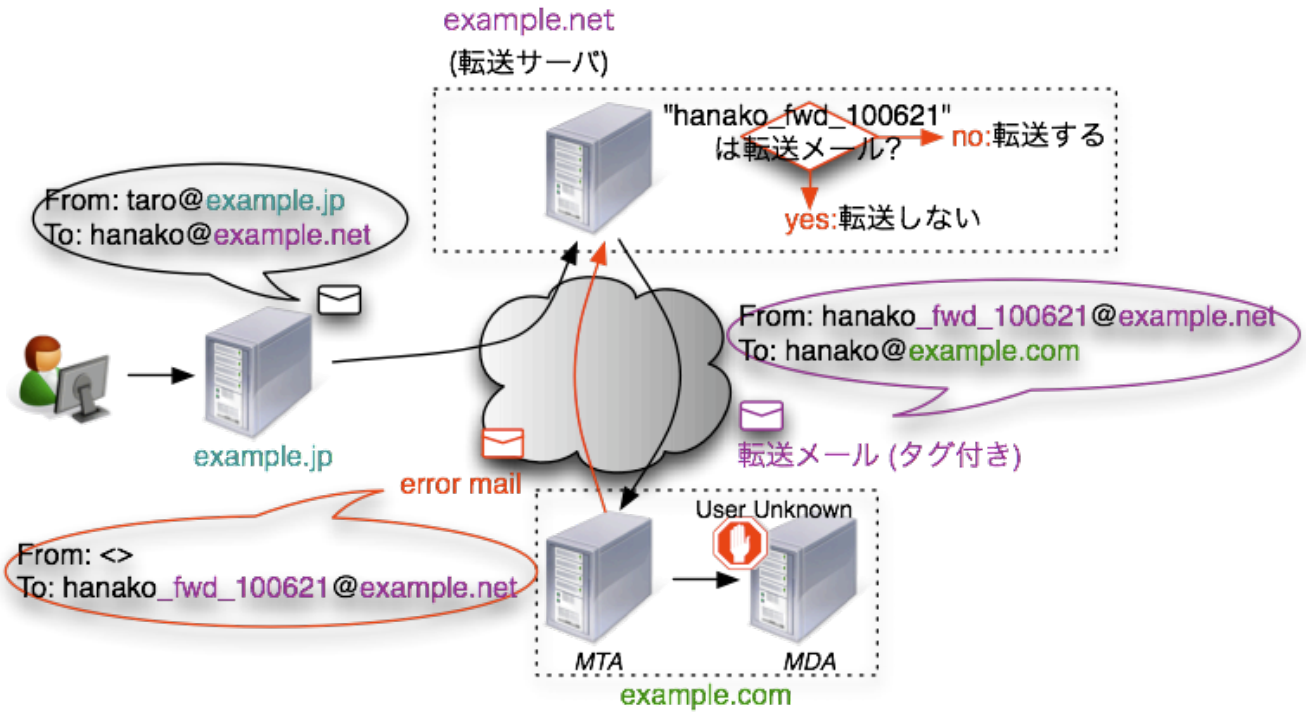
SPF / SIDF の導入 – 転送問題 I

- **ネットワーク方式の課題**
  - メールの配送経路が変わる場合（ex. メール転送）に送信者情報がそのままでは認証が失敗する
  - 転送先（最終受信側，example.com）では最初の送信者の SPF レコード（example.net）を参照するため直近の送信元（example.net）と異なるために認証が失敗



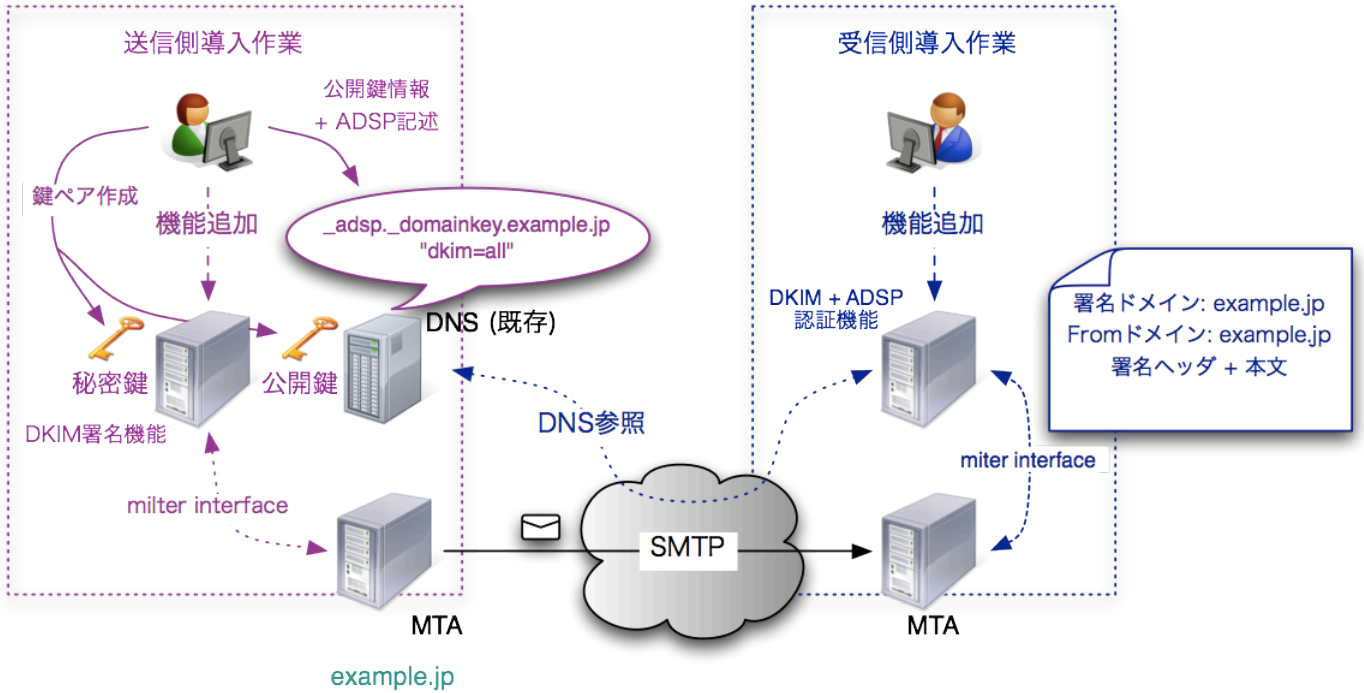
SPF / SIDF の導入 – 転送問題 II

- **転送問題の回避策**
  - メール転送時に転送元 (example.net) を送信者情報に書き換える
  - 単純に書き換えた場合にエラーメールがループする可能性があるので転送時に印 (ex. タグ等) を付与してループを回避
  - SIDF は優先度の高い PRA を転送時に付与 (Resent-From 等)



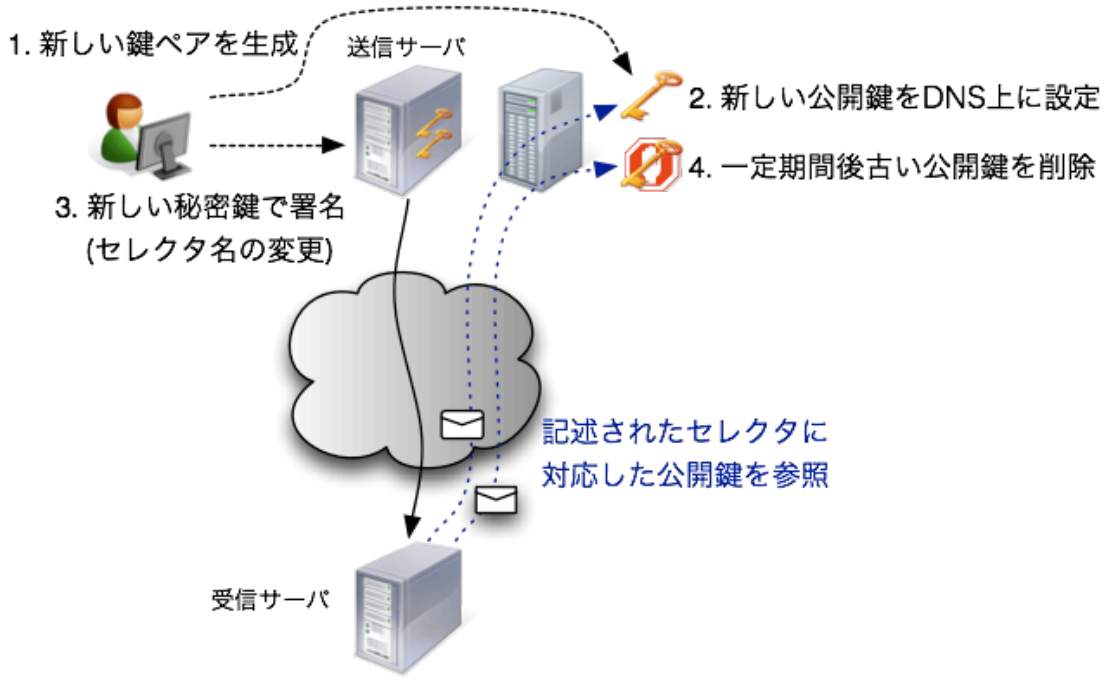
DKIM の導入 – 導入方法

- **送信側**
  - 鍵ペアを作成し公開鍵情報 (+ ADSP) を DNS 上に公開
  - 送信メールサーバに電子署名作成機能を追加
- **受信側**
  - 受信 MTA に認証機能を追加



DKIM の導入 – 運用

- **鍵の交換**
  - セキュリティ上の観点から電子署名に利用する鍵は定期的に変更することが望ましい
  - メールの配送遅延及び DNS の伝播遅延があるためにセレクタを利用して時間的余裕を持って切り替える



DKIM の導入 – 運用上の問題点

- **電子署名の有無**
  - 電子署名 (DKIM-Signature ヘッダ) がある場合は認証可能だが無い場合に判断ができない → 送信側の署名方針の表明が必要
  - ADSP (Author Domain Signing Practices, RFC5617) で表明

mail.example.com	A	192.0.2.1
_adsp._domainkey.mail.example.com	TXT	“dkim=all”

  - ADSP の記述は From ヘッダにあるドメインの下位ドメイン
    → 実際のメール送信者が異なる場合はドメインの委譲等が必要
    → 第三者署名の現実的な解がまだ無い
- **再配送時やメール内容の変更**
  - メーリングリスト等で行われる Subject ヘッダへの文字列の追加 ([members] などの挿入) やフッタ (本文末尾の定型文) の追加
  - 再署名が基本だが ADSP の問題が残る
  - メーリングリスト送信者と受信者との間で別途ホワイトリスト的な扱い等が必要となる (RFC6377)

送信ドメイン認証技術 – まとめ

- **送信ドメイン認証技術導入マニュアル**
  - http://www.dekyo.or.jp/soudan/anti_spam/report.html#dam

SPF／Sender ID		DKIM
Sender Policy Framework (RFC4408) Sender ID Framework (RFC4406,4407)	名称	DomainKeys Identified Mail (RFC6376)
送信元を**ネットワーク的**に判断 （送信元のIPドレスにより確認）	特徴	送信時に**電子署名**をメールに付加 （電子署名の検証により確認）
送信側はほぼ**皆無**（DNSの記述のみで、1通ずつの処理は不要） 受信側では**一定の処理が必要**	導入コスト	送信側は**相対的に高め**（1通ずつ署名付加・検証が必要） 受信側では**一定の処理が必要**
送信側**導入の容易さ**（特にコスト面） **普及が進展**（jpドメインでは既に40%超）	長所	**メール本文の改ざんも検知** **メールの配送経路に影響されない**
メール転送時に認証失敗となる場合がある （転送処理の見直しや転送先でのホワイトリストによる対応が必要）	短所	配送経路上でメール内容が変更されると認証失敗となる （メーリングリストなどでは設定によっては再署名が必要）

迷惑メール対策

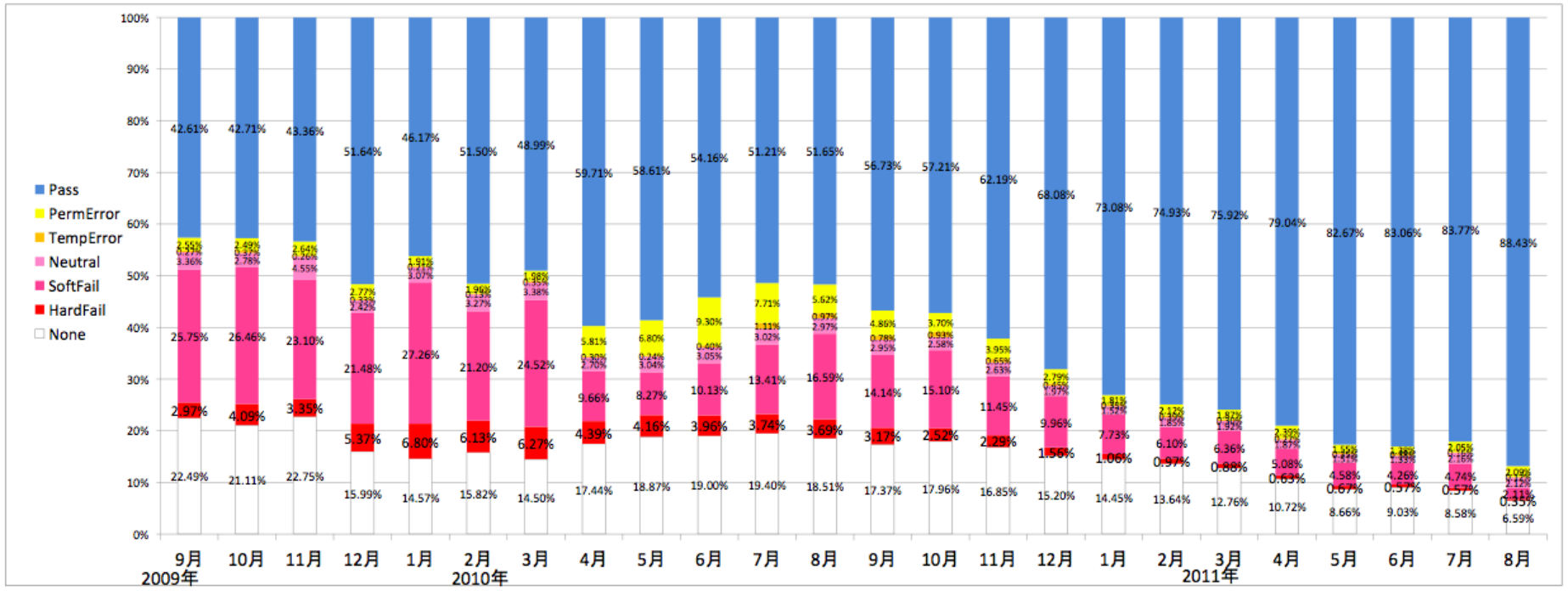
- **認証結果の利用**
  - 認証結果はヘッダ情報 (RFC5451) としてメール受信者に提示

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

  - 認証結果 (“pass” or “fail”) だけで判断しない
  - もはや “認証 pass = 受け取るべきメール” では無い
  - “受け取るべきドメイン + 認証 pass = 受け取るメール”
  - ドメインを評価するための仕組みも検討中 (IETF repute WG)
- **送信者情報を確認**
  - SPF: reverse-path
  - SIDF: PRA (Resent-Sender, Resent-From, Sender, From)
  - DKIM: 署名ドメイン (必ずしもメールの責任元とは限らないので注意)

導入状況 - I

- **調査概要**
  - 電気通信事業者7社のデータの総務省によるとりまとめ
  - 8月時点の送信側のSPF導入率は 93.41% (6月から 2.44% 増加)

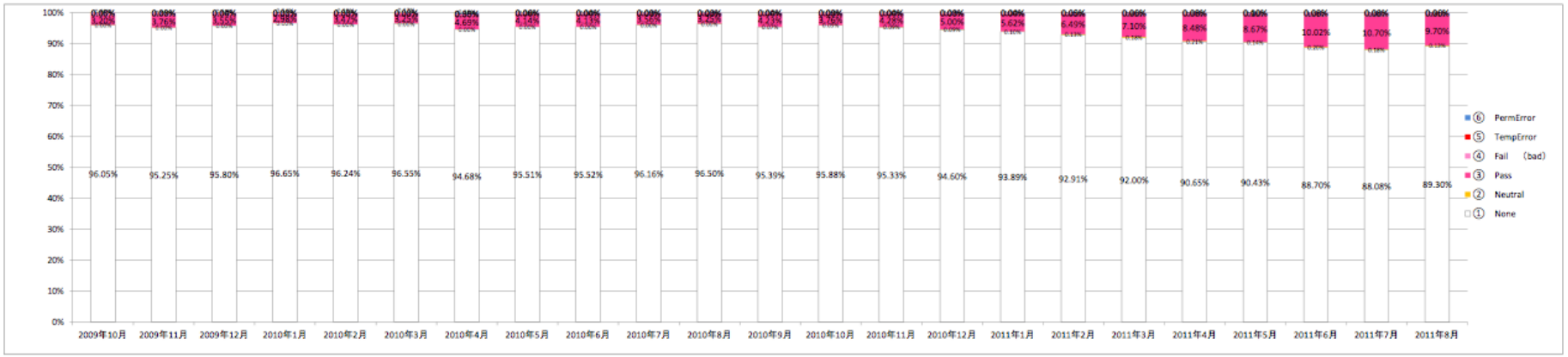


出典：電気通信事業者7社※の協力により、総務省がとりまとめ
※ KDDI株式会社、NECビッグローブ株式会社、株式会社インターネットイニシアティブ、エヌ・ティ・ティ・コミュニケーションズ株式会社、株式会社テクノロジーネットワークス、ニフティ株式会社、ヤフー株式会社

Source: http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/110302_2.pdf

導入状況 - II

- **調査概要**
  - 電気通信事業者4社のデータの総務省によるとりまとめ
  - 8月時点の送信側のDKIM導入率は 10.7%



出典：電気通信事業者4社※の協力により、総務省がとりまとめ

※ 株式会社インターネットイニシアティブ、NECビッグローブ株式会社、ニフティ株式会社、ヤフー株式会社

Source: http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/110302_3.pdf

導入状況 - III

- **政府による推進**
  - 政府の「情報セキュリティ2011」において送信ドメイン認証技術の導入を推進していくことを決定
  - 政府機関から、発受信する電子メールについて、送信ドメイン認証技術の採用を推進する
  - 総務省は「迷惑メール対策推進協議会」や「JEAG」等と連携して、送信ドメイン認証技術等の導入を促進する
  - 地方公共団体においても、発信する電子メールについて送信ドメイン認証技術の採用等を推進する
- **政府のメールアドレスを詐称されないための対策について**
  - 2011.10.14 情報セキュリティ対策推進会議 (CISO等連絡会議)
  - 本府省庁ドメインについて外局等を含む送信側SPFの設定

    H.23年7月 37.4% → H.23年10月13日現在 63.2%
  - 受信側においても、送信元を検証する機能を設定することを推進

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**
  - 受信側の対策だけでなく送信側にも注意
  - 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
  - 認証結果だけで判断しない → ドメインレピュテーション (評価判断)
  - メールの疎通は今後も悪化する可能性あり → 正しい受信対策を
- **JEAG の取り組み**
  - 行政機関との協調による効果的な施策の実践
  - 迷惑メール対策推進協議会など広範囲な場での技術分野での提言
  - MAAWG (Messaging Anti-Abuse Working Group) など国際的な民間組織との連携

JEAG
Japan E-mail Anti-Abuse Group

MAAWG