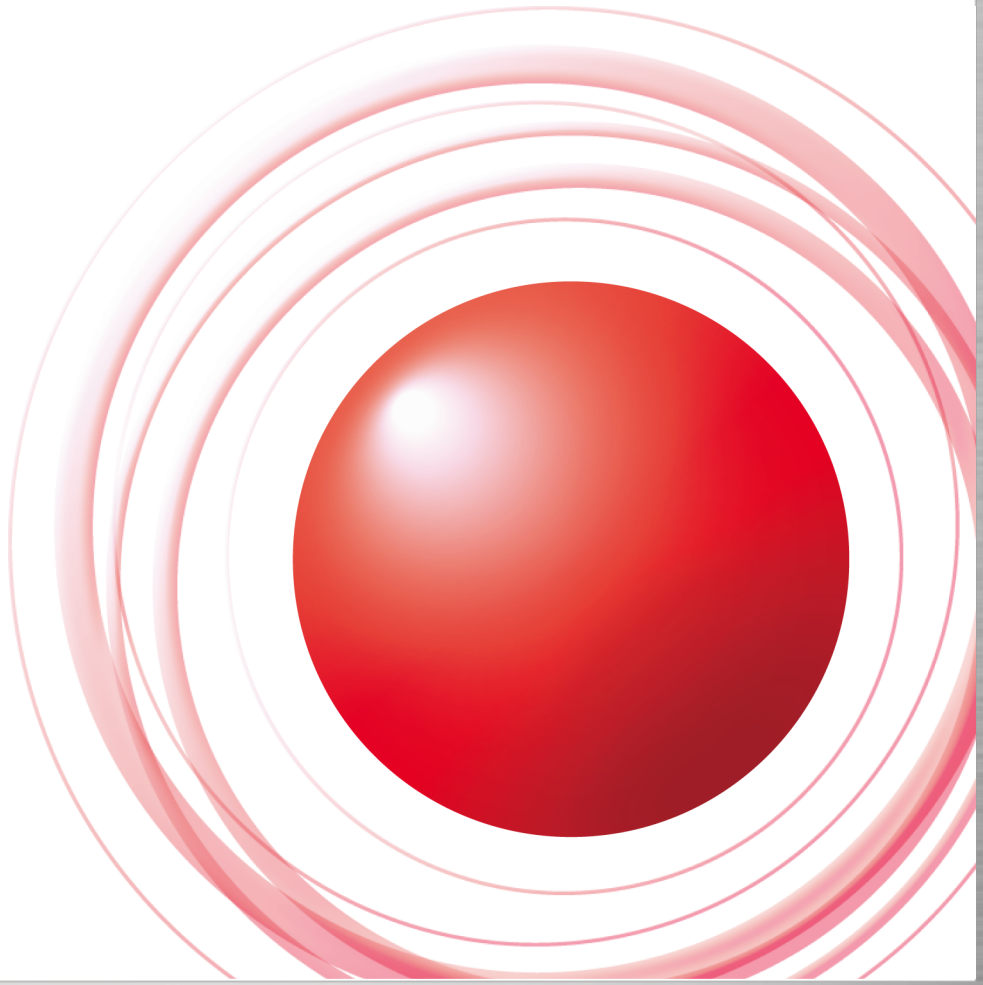
迷惑メール対策と送信ドメイン認証技術

IAjapan 第9回 迷惑メール対策カンファレンス

IIJ Internet Initiative Japan



2011.05.27

Internet Initiative Japan Inc.
SAKURABA Shuji

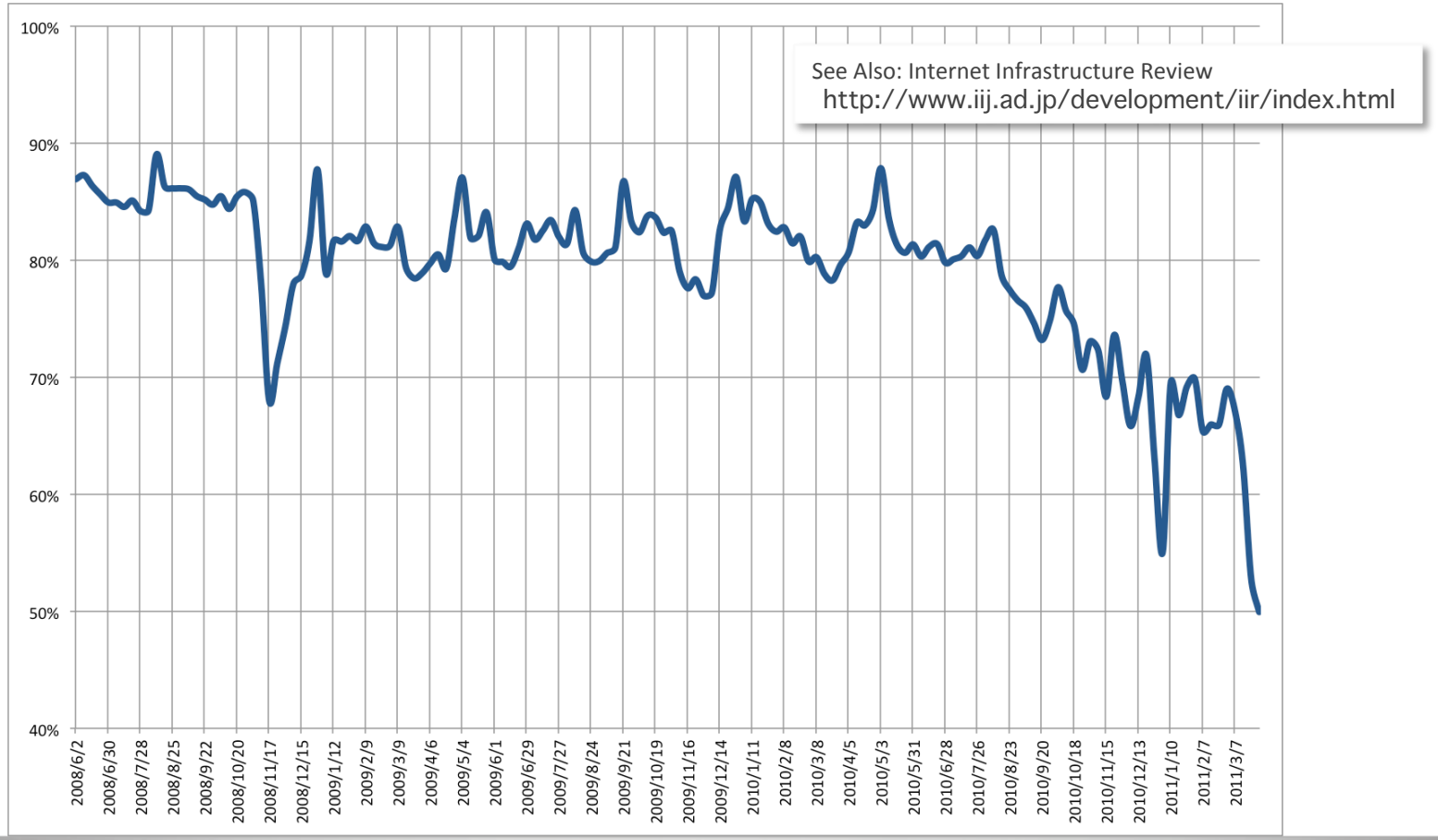
Ongoing Innovation

Agenda

- 迷惑メールの現状
- 対策の強化と懸念
- 送信ドメイン認証技術
  - 概要
  - SPF/SenderID
  - DKIM
  - 効果
  - 導入状況
  - 運用
- おわりに

迷惑メールの現状 - I

- **迷惑メール割合の推移**
  - IIJ の迷惑メールファイルによる検知率
  - 2008.06.08 ～ 2011.04.03 (148週間)

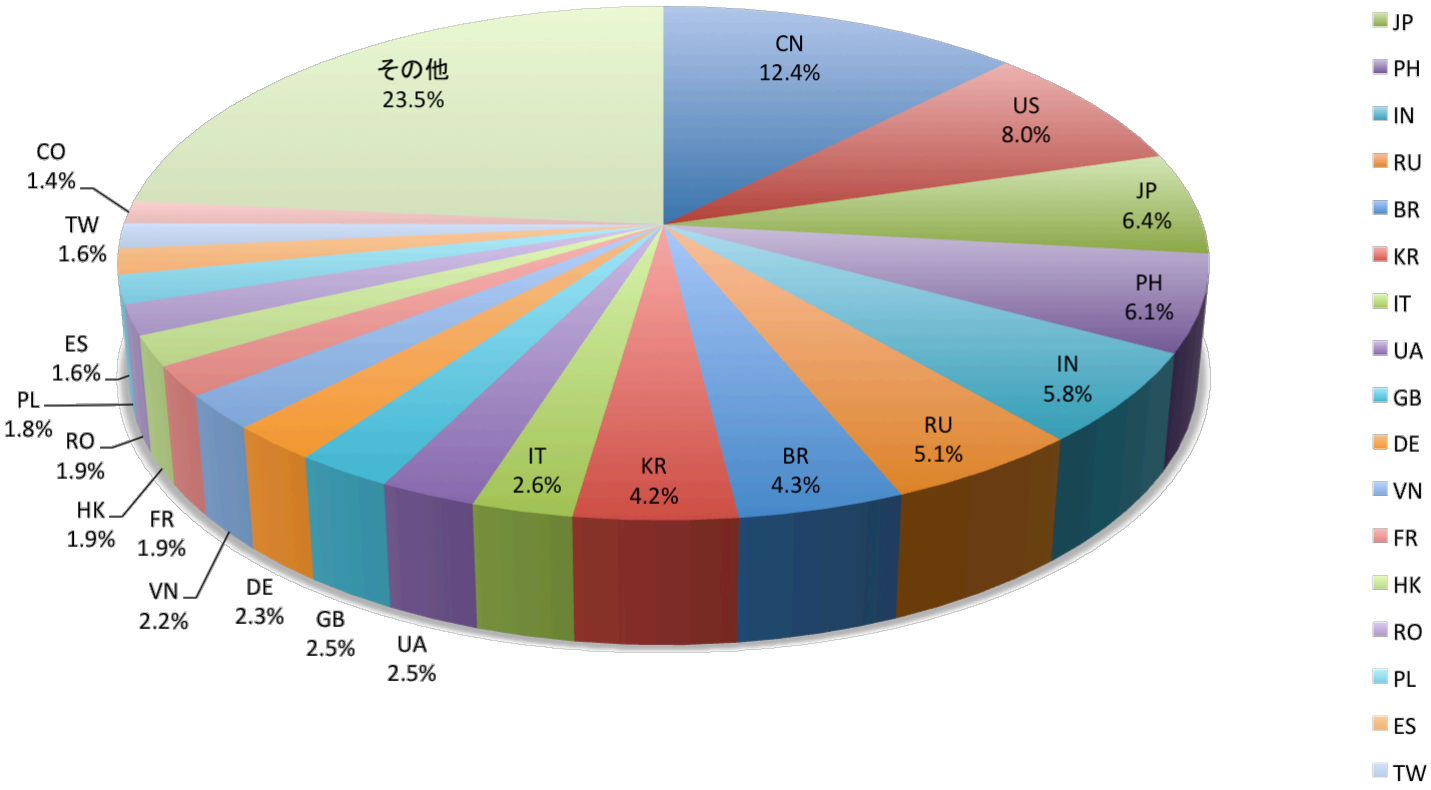


See Also: Internet Infrastructure Review
http://www.iij.ad.jp/development/iir/index.html

迷惑メールの現状 - II

- 最近の迷惑メールの送信元地域分布
  - 2011.01.03 ～ 2011.04.03

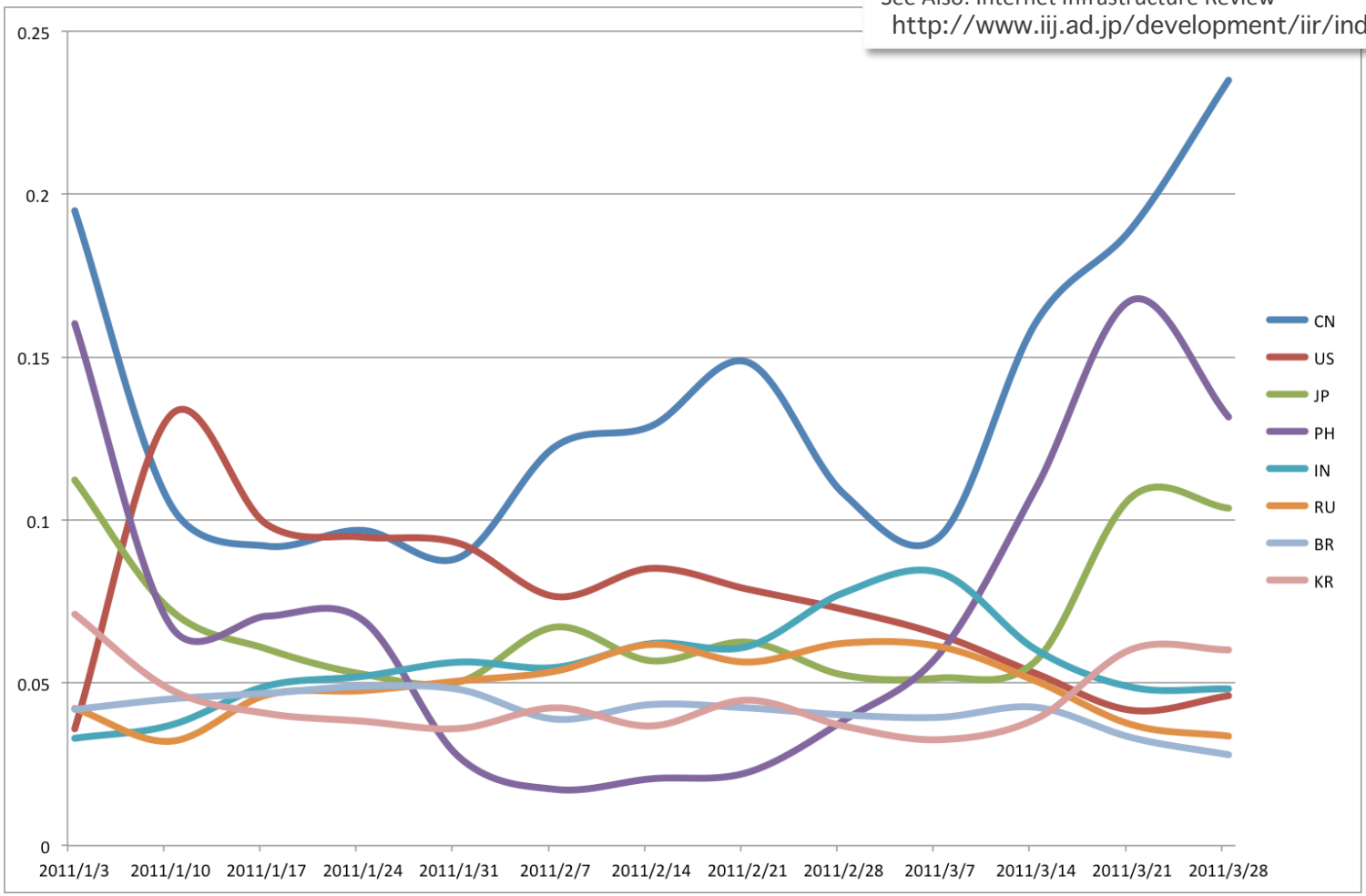
See Also: Internet Infrastructure Review
http://www.iij.ad.jp/development/iir/index.html



迷惑メールの現状 - III

- 主要送信元の推移
  - 2011.01.03 ～ 2011.04.03

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



迷惑メールの現状 - IV

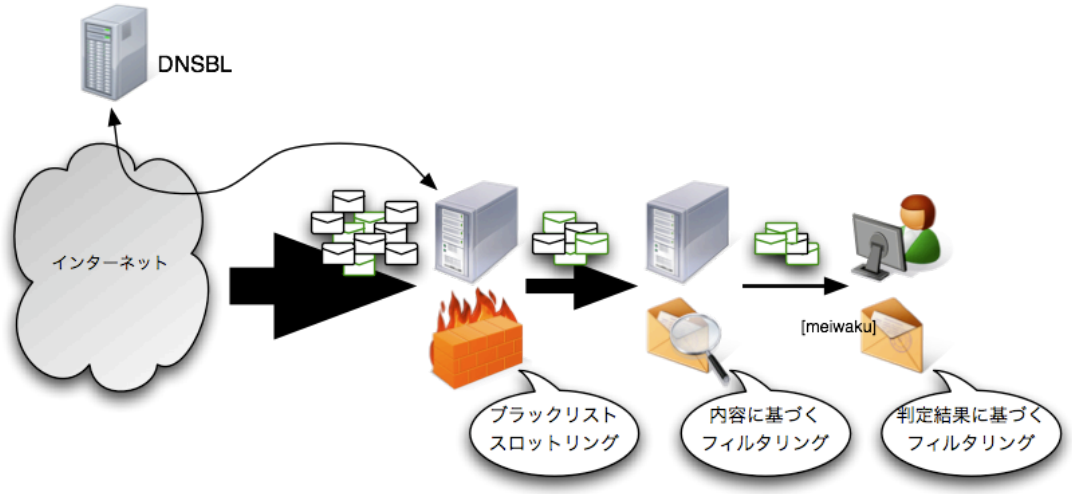
- グローバルでの動向
  - 2010年後半から続く様々な対策 (特にボットネット対策) により全体として迷惑メール量は減少してきている
    - Canadian Pharmacy などのアフィリエイトなどを行っていた spamit.com が活動を停止 → Storm, Waledec などボットネットにも影響 *(2010.09)*
    - MS と米司法当局が Rustock ボットネットの制御元 (C&C) サーバを押収 (2011.03)

- 日本の動向
  - 日本向けの迷惑メール量にそれほど変化が無いため相対的に割合が増加している
    - 固定回線を利用したメール配送事業者のシステムを利用した大量送信
    - 海外に拠点を置きそこから日本に向けて大量送信

対策の強化と懸念 - I

- **迷惑メール対策手法**
  - 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の問題
    - データの信憑性 (データの収集方法や偏り)
    - 運用方針 (誤判定時の解除手続きが不明瞭)
    - 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)
    - 汚れた IP アドレス再割当の問題
  - IPv6 の利用が進むと既存の仕組みでは困難
    - 広大なアドレス空間
      - IPv4: 約 2^{32} (= 約42億) 個
      - IPv6: 約 2^{128} (=約340澗) 個　　(cf. 億、兆、京、垓、秭(秭)、穣、溝、澗)
    - DNS の仕組み (キャッシュ含む) では事実上提供困難
    - 新たなデータ参照のための方法が必要
    - ホワイトリスト (正規メールサーバ) を提供する方式への転換?

対策の強化と懸念 - 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

▼

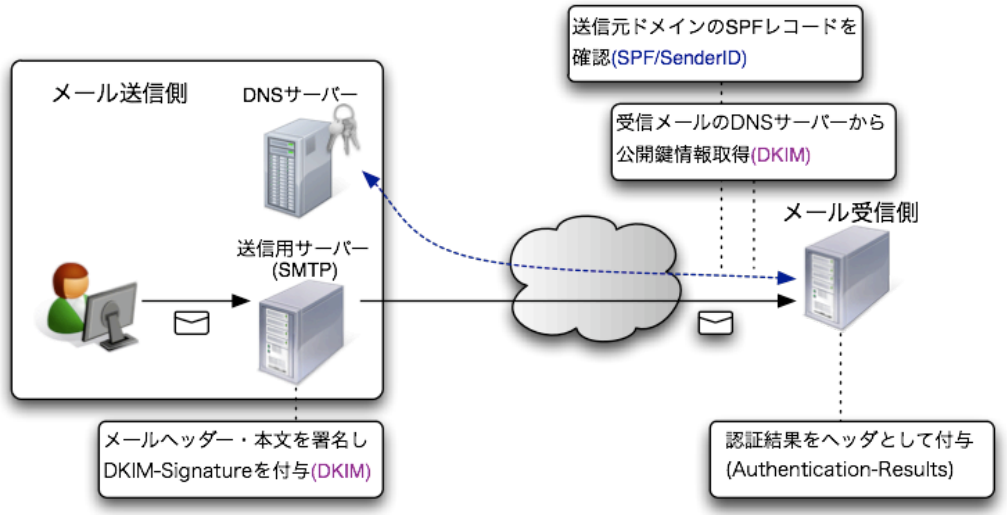
正しいメールを判断するための共通基盤としての

送信ドメイン認証技術

送信ドメイン認証技術 – 概要 I

- **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 (認証)

- **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 – 概要 II

	SPF／Sender ID	DKIM
名称	Sender Policy Framework (RFC4408) Sender ID Framework (RFC4406,4407)	DomainKeys Identified Mail (RFC4871,5672)
特徴	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）	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）
導入コスト	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**	送信側は**相対的に高め**（1通ずつ署名作成・付加が必要） 受信側では**一定の処理が必要**
長所	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）	**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**
短所	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）	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）

✓ **まずは、すべてのドメインにおいて、DNSにSPFレコードの記載をすることが望ましい**
- 送信側のコストは、ほとんどゼロ
- 自ドメインのなりすましを防ぐ（受信側で正当なものか確認する）ことが可能になる

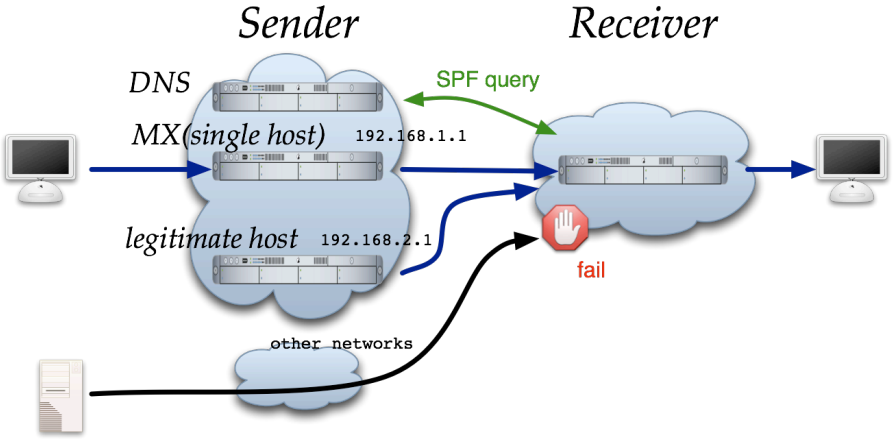
✓ **さらに、ビジネスとしてのメール送信などでは、両者を組み合わせて対応することが望ましい**

送信ドメイン認証技術 – SPF/SenderID

- **送信元を認証する仕組み**
  - メール受信時に送信元 (IPアドレス) が正しい出口であるかを判断
  - 送信者情報から送信元ドメインを抽出 → SPF レコードを参照
- **送信側の設定**
  - 対象となるドメイン名を使うメールの出口を把握する
  - ドメイン名の SPF (TXT) レコードに出口を記述

```
example.jp    TXT   "v=spf1 +mx +ip4:192.168.2.1 –all"
```

- **受信側の設定**
  - 外部から最初にメールを受け取る受信サーバに認証機能を導入
  - 認証結果を Authentication-Result ヘッダに記述
  - 認証結果を各種フィルタに利用したりポリシーに従った処理に利用する



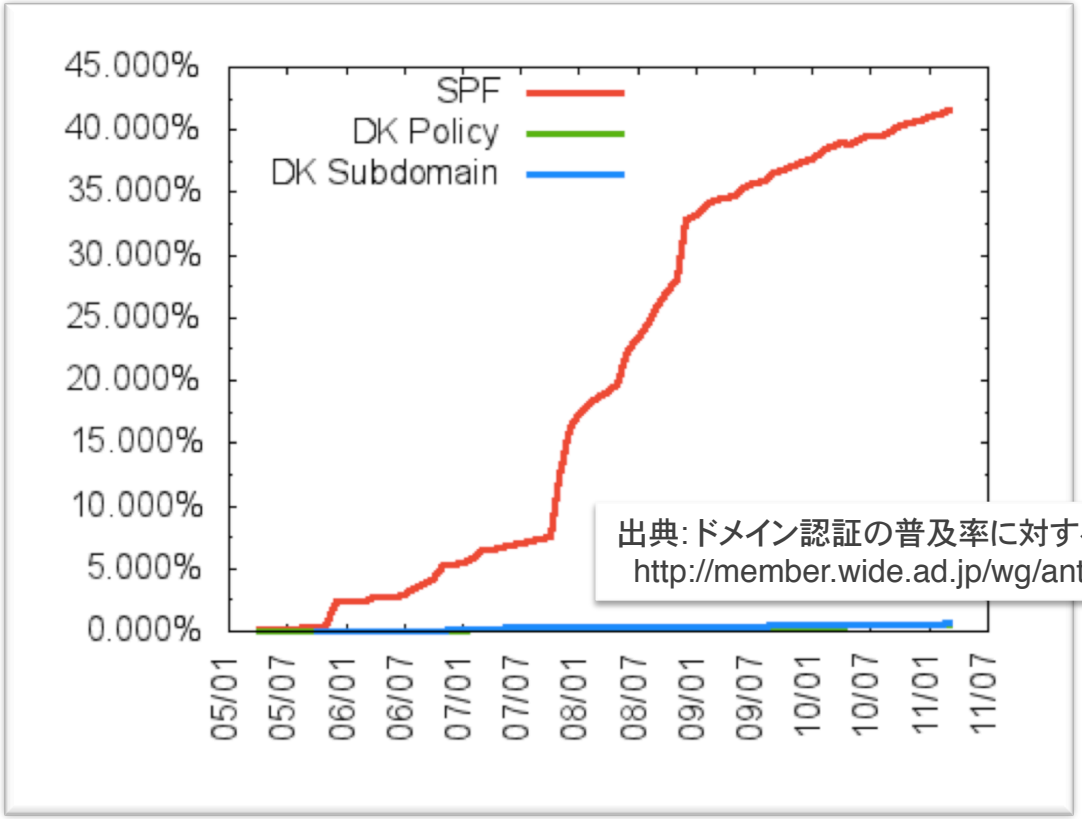
送信ドメイン認証技術 - DKIM

- **送信元を認証する仕組み**
  - 正しい送信元でなければ作れない電子署名情報をメールに添付
  - メール受信時に電子署名が合っているかを判断
- **送信側の設定**
  - 対象となるドメイン名や署名ポリシー、メールの出口やを把握する
  - 送信メールサーバに電子署名を挿入する機能を追加
  - 電子署名に必要となる鍵 (秘密鍵、公開鍵) を作成 ← 定期的に更新
  - 公開鍵を DNS 上に公開する (brisbane._domainkey.example.com)
- **受信側の設定**
  - 外部から最初にメールを受け取る受信サーバに認証機能を導入
  - 認証結果を Authentication-Result ヘッダに記述
  - 認証結果を各種フィルタに利用したりポリシーに従った処理に利用する

```
DKIM-Signature: v=1; a=rsa-sha256; s=brisbane; d=example.com;
    c=simple/simple; q=dns/txt; i=joe@football.example.com;
    h=Received : From : To : Subject : Date : Message-ID;
    bh=2jUSOH9NhtVGCQWNr9BrIAPreKQjO6Sn7XIkfJVOzv8=;
    b=AuUoFEfDxTDkHlLXSZEpZj79LICEps6eda7W3deTVFOk4yAUoqOB
      4nujc7YopdG5dWLSdNg6xNAZpOPr+kHxt1IrE+NahM6L/LbvaHut
      KVdkLLkpVaVVQPzeRDI009SO2Il5Lu7rDNH6mZckBdrIx0orEtZV
      4bmp/YzhwvcubU4=;
```

送信ドメイン認証技術 – 導入状況 I

- 日本 (jp ドメイン)
  - WIDE プロジェクトと JPRS による共同研究による調査
  - 2011年3月時点で “jp” ドメインの SPF 宣言率は 41.62%
  - “co.jp” ドメインについては 48.90%

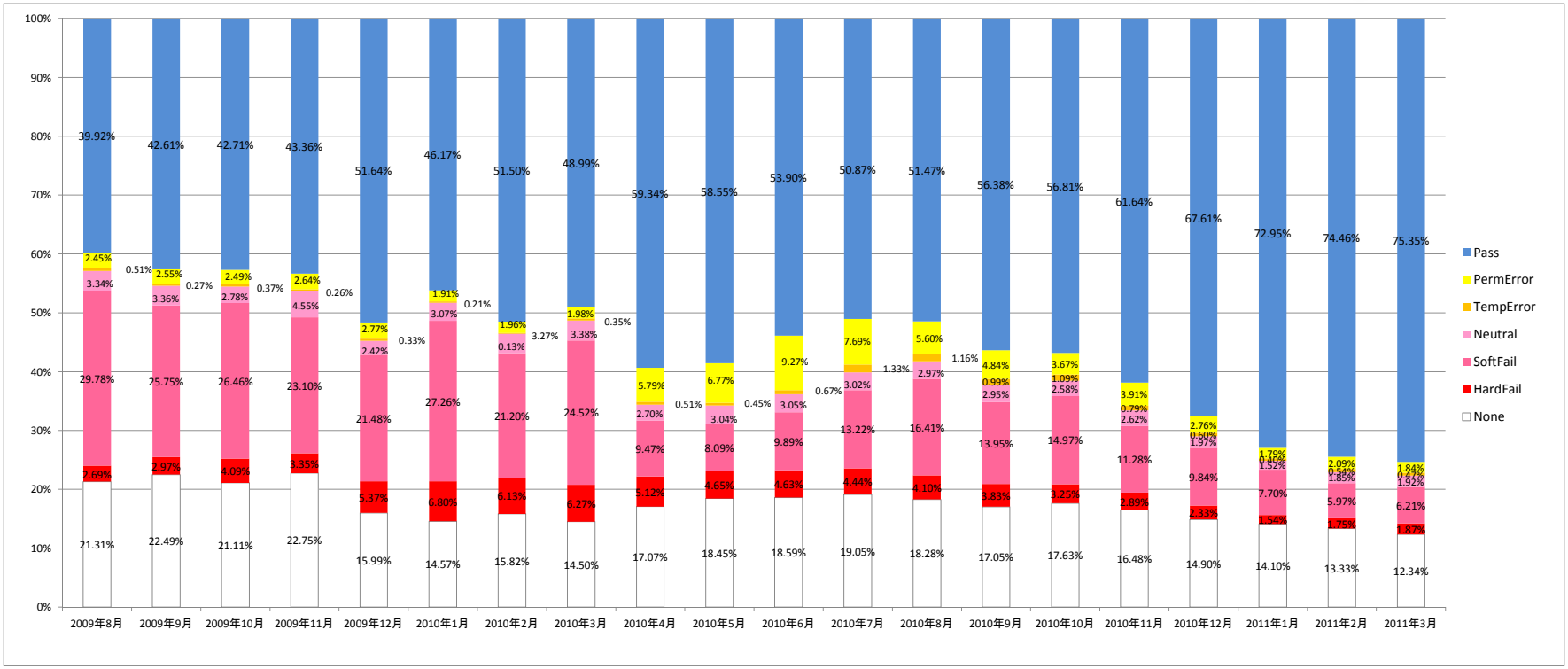


出典: ドメイン認証の普及率に対する測定結果
http://member.wide.ad.jp/wg/antispam/stats/index.html.ja

送信ドメイン認証技術 – 導入状況 II

- **電気通信事業者の調査**
  - 7社の調査結果を総務省がとりまとめて公表
  - 2011年03月時点で「none」は12.34% (導入割合は 87.66%)

http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei

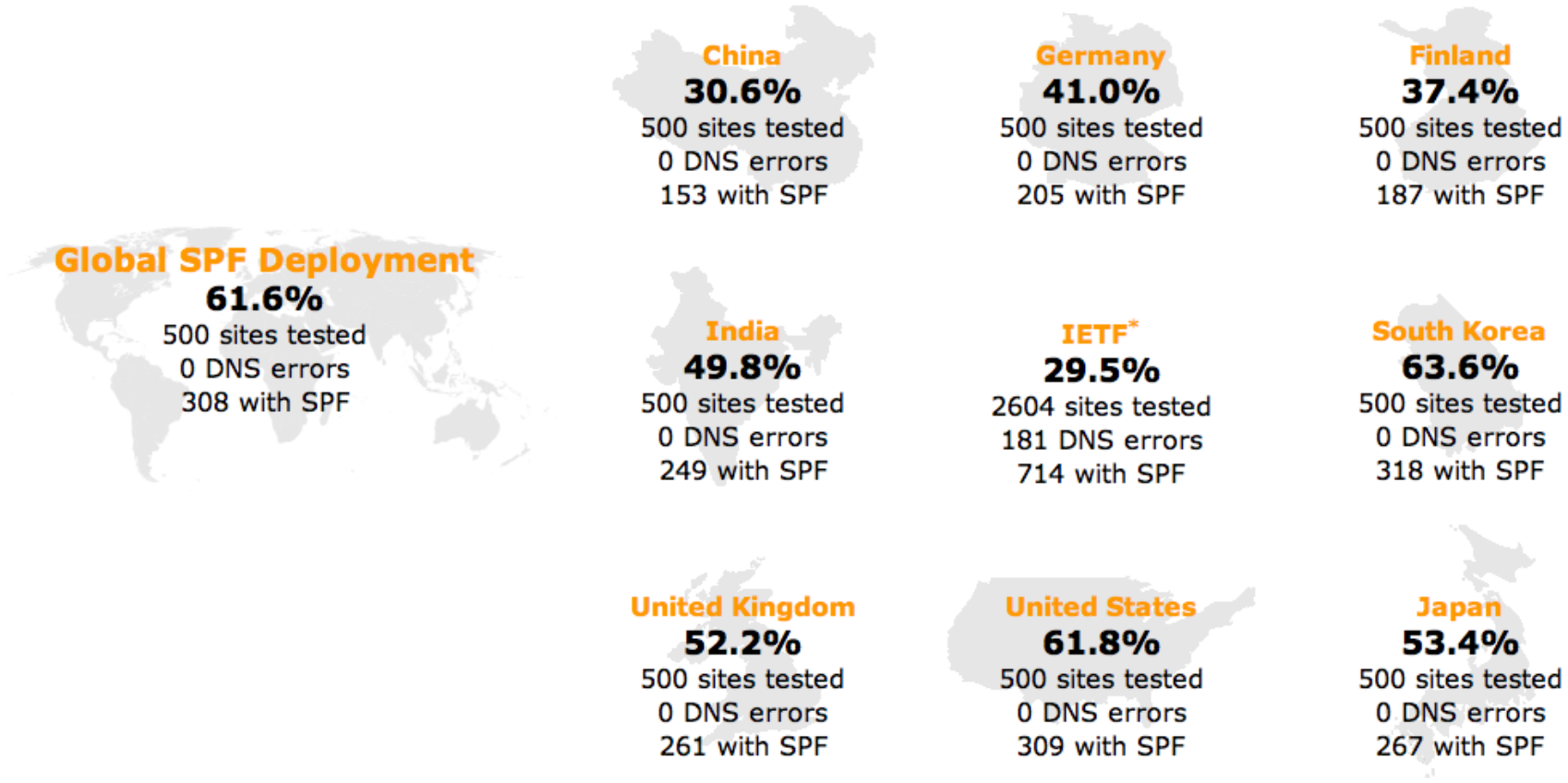


出典：電気通信事業者7社※の協力により、総務省がとりまとめ とりまとめ

※ 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 ?一株式会社

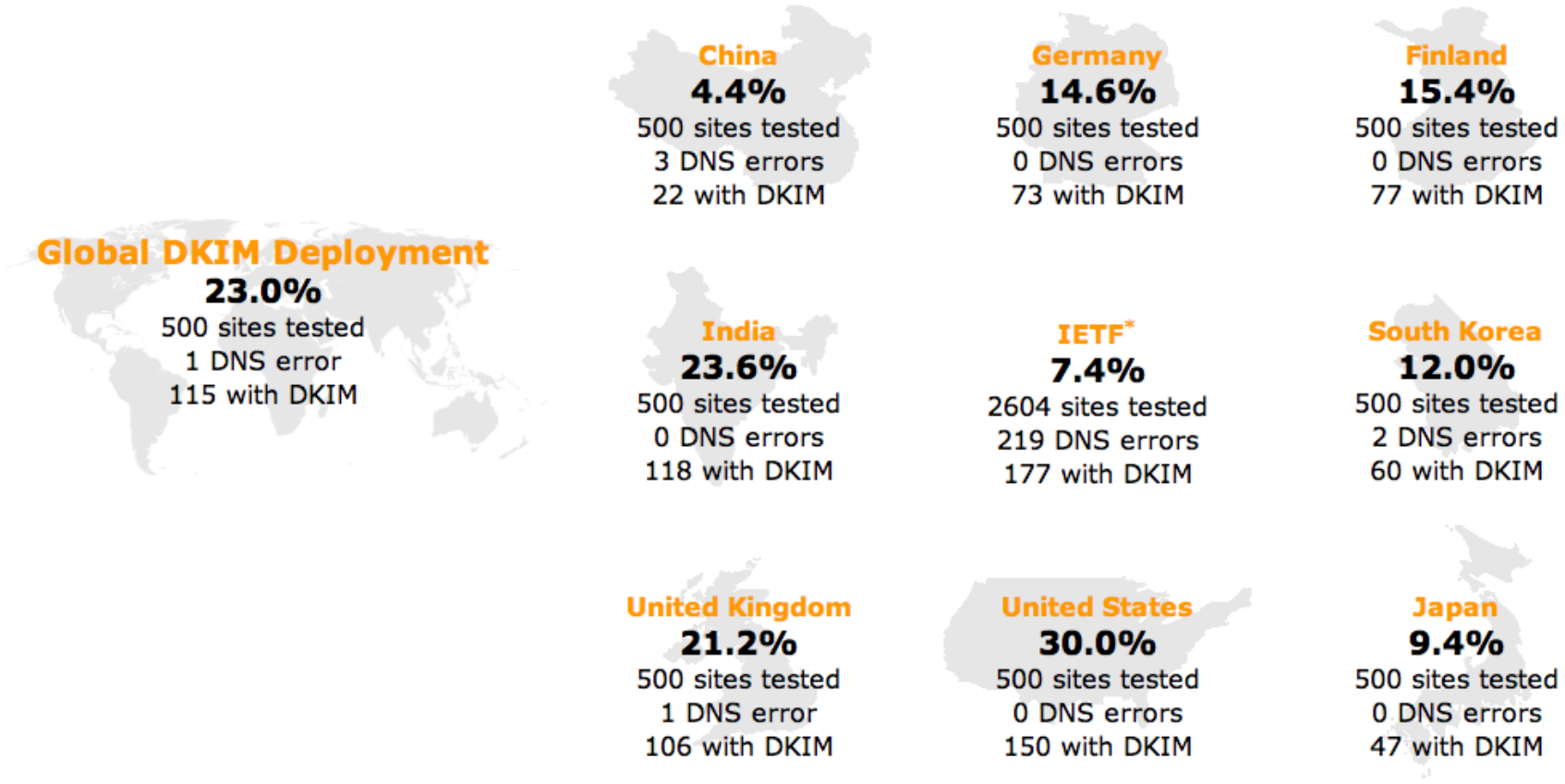
送信ドメイン認証技術 – 導入状況 III

- 各国の導入状況
  - Lars Eggert さん @ Nokia による調査 (https://fit.nokia.com/lars/)
  - alexa.com による上位 web site のドメインを調査 (2011.05.22)



送信ドメイン認証技術 – 導入状況 IV

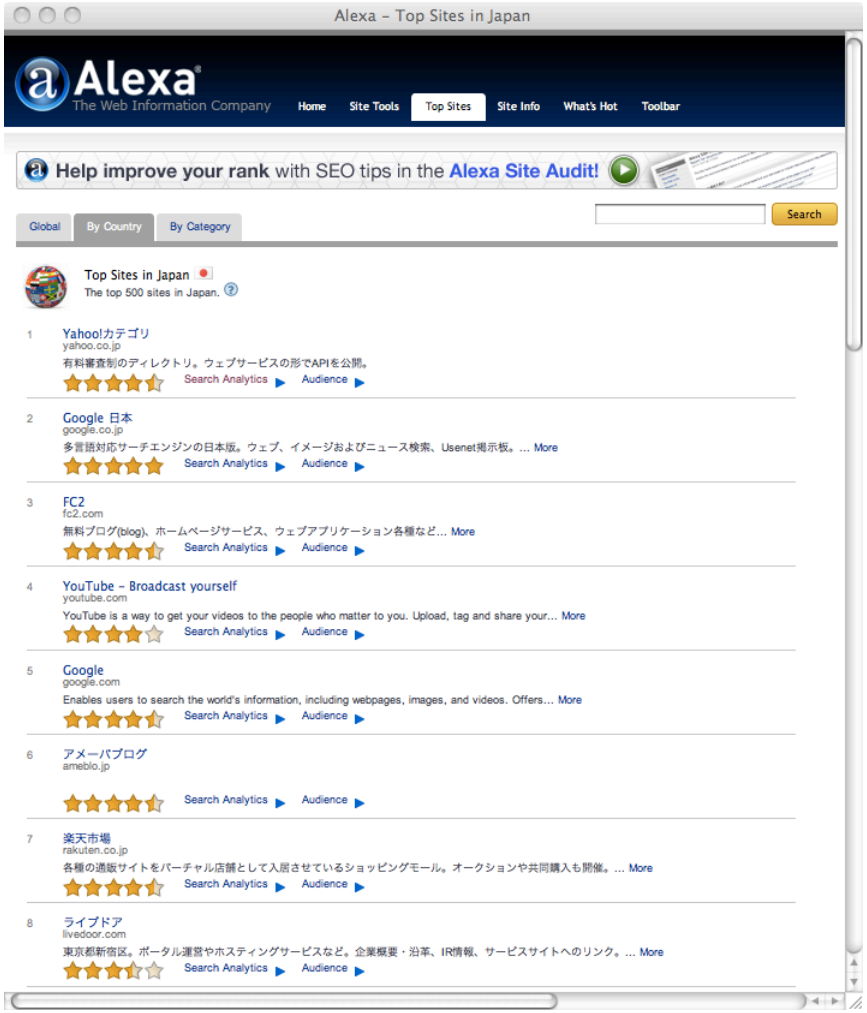
- 各国の導入状況
  - Lars Eggert さん @ Nokia による調査 (https://fit.nokia.com/lars/)
  - alexa.com による上位 web site のドメインを調査 (2011.05.22)

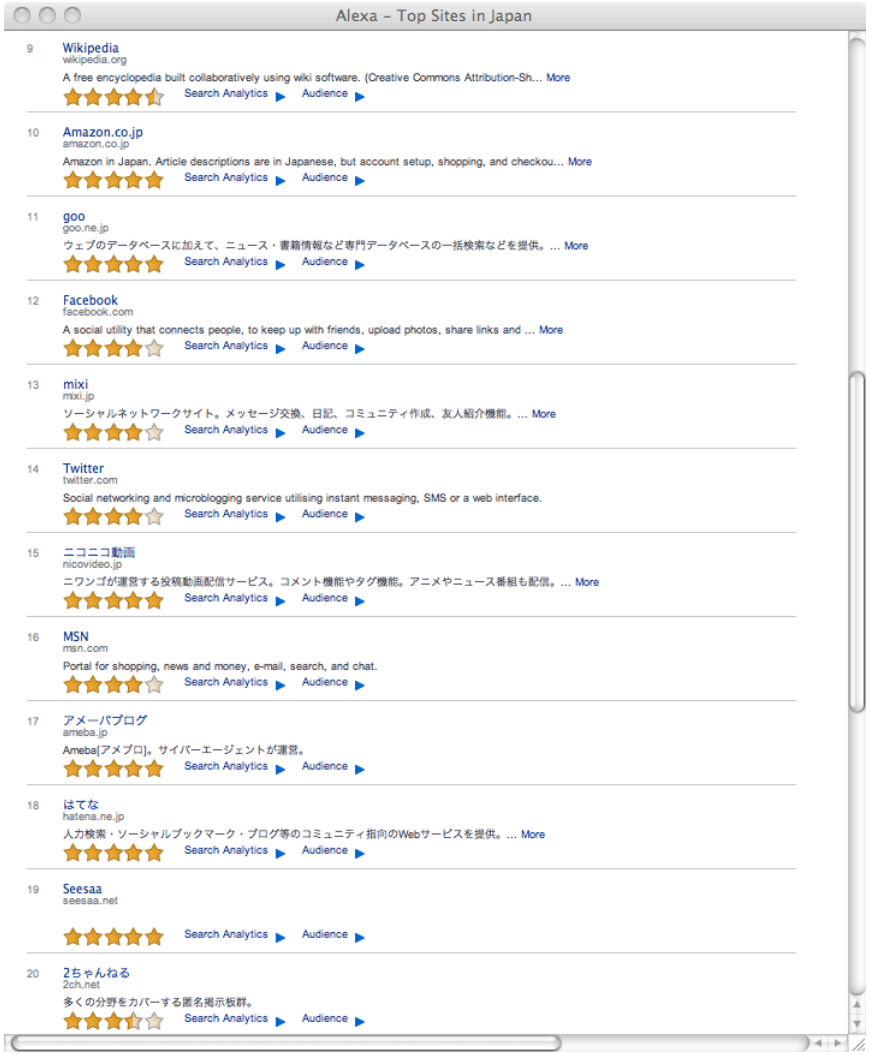


送信ドメイン認証技術 – 導入状況 V

- 上位ドメイン

http://www.alexa.com/topsites/countries/JP





送信ドメイン認証技術 – 効果 I

- **送信者情報を詐称したメールの峻別**
  - フィッシング対策
  - 詐称メールのフィルタリング (pass フィルタ)
- **迷惑メール対策**
  - 認証が通った送信者ドメインの精査 (ドメインレピュテーションの利用)
  - 紛らわしいドメインの峻別
- **受け取るべきメールの識別**
  - ホワイトリストとしての利用
  - 信頼できる送信元は迷惑メールフィルタを通さず優先受信 (設備負荷の軽減)
- **受信者側での認証結果を利用した個別フィルタリングの利用**
  - 認証結果の提示形式の統一 (RFC5451)
  - MUA (Mail User Agent) での機能拡張等で利用可能
  - ISP や携帯電話でのフィルタ設定機能等 (なりすまし対策フィルタ)
- **オプトアウトや苦情等の連絡先の信頼性判断**
  - ARF (RFC5965) などを利用した FBL (Feedback Loop) での利用

送信ドメイン認証技術 – 効果 II

- メール受信者への認証結果の通知
  - 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

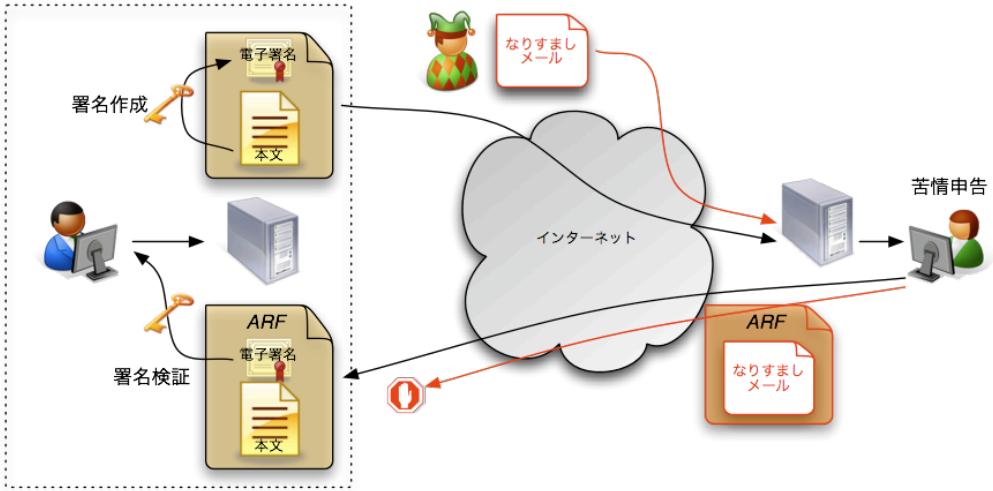
```
Authentication-Results: example.com;
    spf=hardfail smtp.mailfrom=example.com;
    dkim=pass (good signature) header.i=sender@example.com
```

  - 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 で表示することにより参照可能
  - MUA (Mail User Agent) のフィルタリング機能により受信者側が処理

Apple Mail のフィルタリング例

送信ドメイン認証技術 – 効果 III

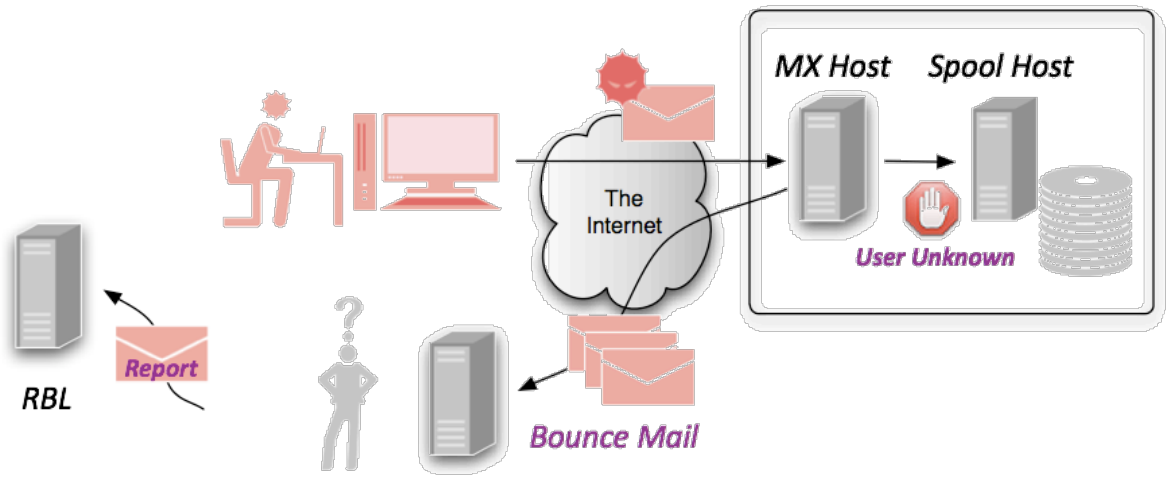
- **FBL (Feedback Loop)**
  - FBL とはメール受信者から送信側への苦情等の申し立て
  - 米国では中間事業者が仲立ちを行う事例もあり
    - 予め送信事業者は送信側の情報と連絡窓口を登録
    - 受信側で Webmail 等でのボタンによる申告 → 中間事業者への通知
    - 登録されている事業者であれば報告
  - 送信事業者の利点
    - 送信先リストからの削除 (opt-out)
    - 苦情のあったメールの識別 → 依頼元との今後の調整
    - 送信間隔の調整, etc
  - 受け取る苦情が本当に送信側が送ったものであるかの検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

- **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 – 運用

- **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

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

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

- **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，”送信ドメイン認証技術導入マニュアル”の発行、普及のための各種団体等への講演等実施
  - 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

JEAG Japan E-mail Anti-Abuse Group　MAAWG　IETF®