資料2－3

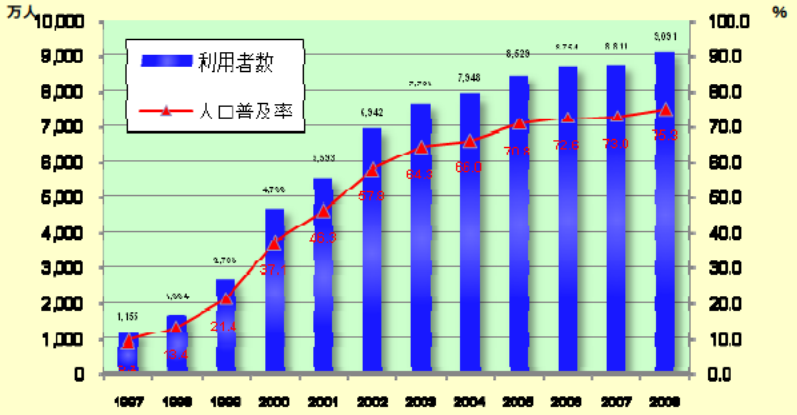
送信ドメイン認証技術の概要

2009年10月2日

電子メールの普及と迷惑メール

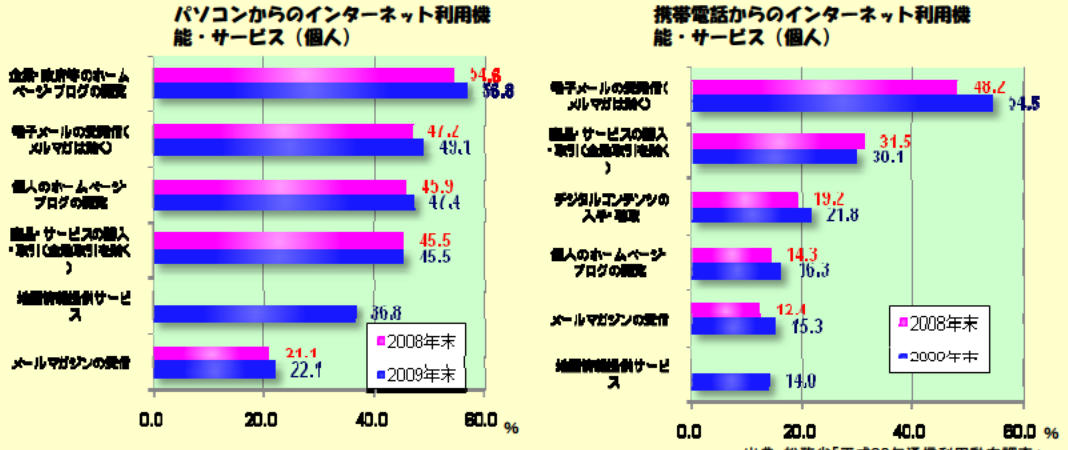
✓ 電子メールは、社会経済活動や、市民生活での必要不可欠な連絡・伝達の手段となっている

インターネットの利用者数・人口普及率



出典：総務省「平成20年通信利用動向調査」

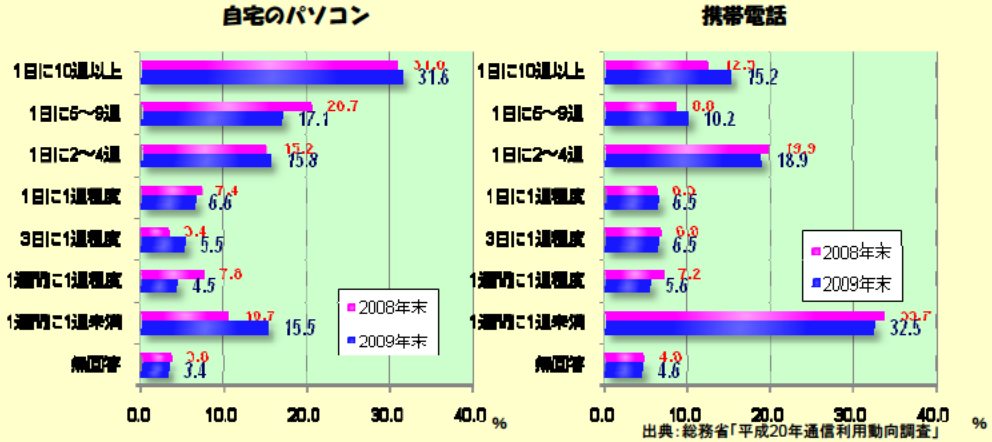
インターネットの利用目的



出典：総務省「平成20年通信利用動向調査」

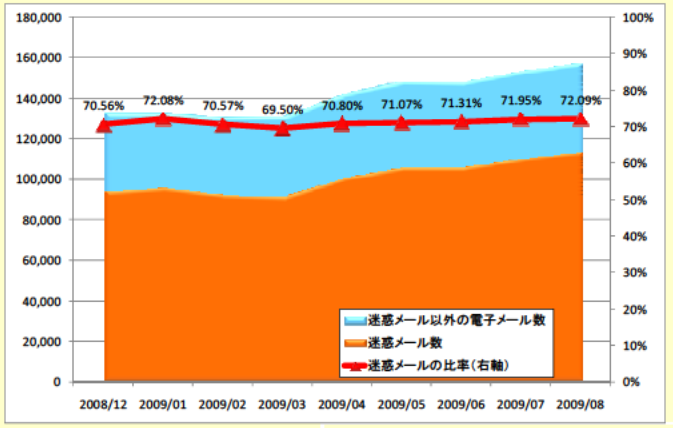
✓ その一方で、迷惑メールが深刻な問題となっており、利用者が不要なメールに悩まされたり、事業者が不要なメールの配送を強いられたりしている状況にある

世帯における迷惑メール受信頻度



出典：総務省「平成20年通信利用動向調査」

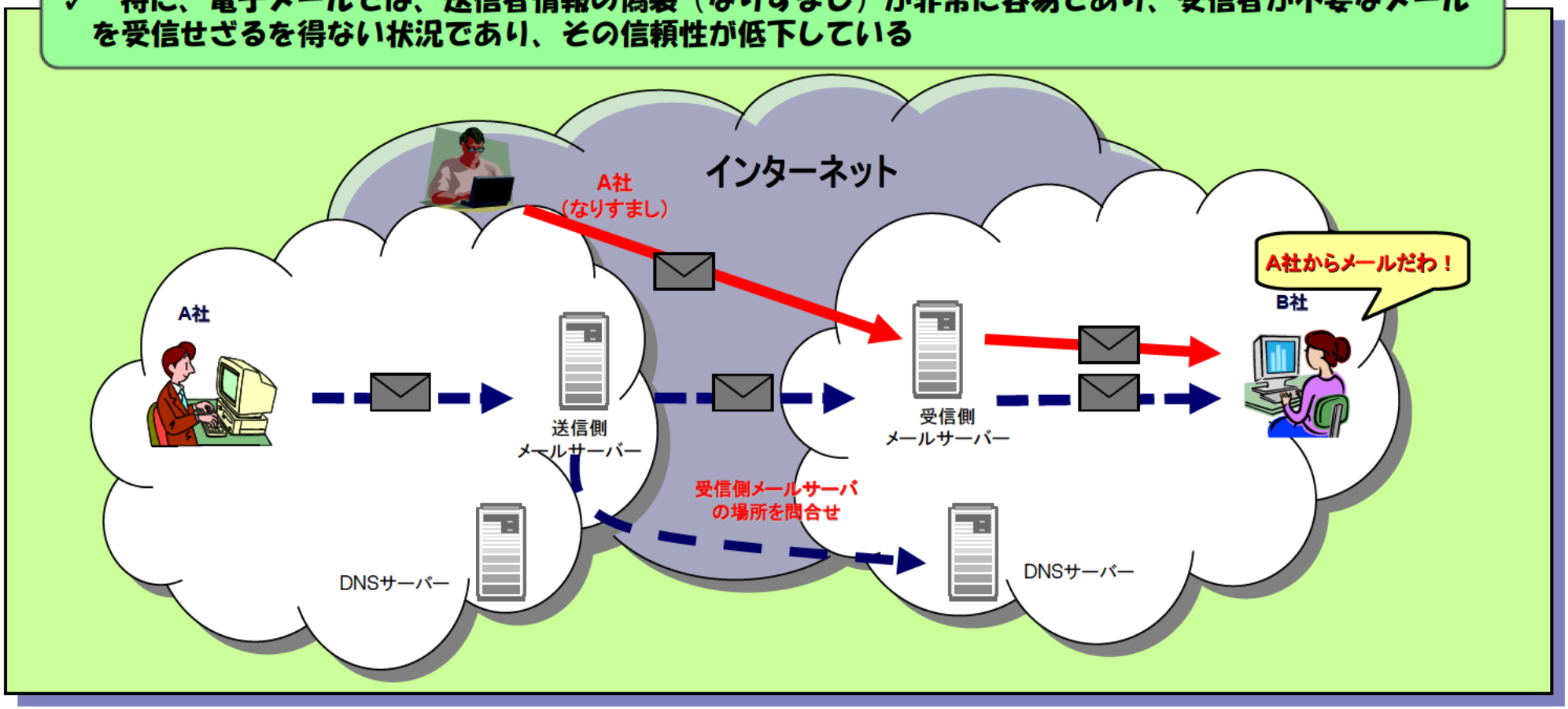
迷惑メールのトラヒック



出典：電気通信事業者15社の協力により総務省とりまとめ

電子メールの信頼性（なりすましの問題）

✓ 特に、電子メールでは、送信者情報の偽装（なりすまし）が非常に容易であり、受信者が不要なメールを受信せざるを得ない状況であり、その信頼性が低下している



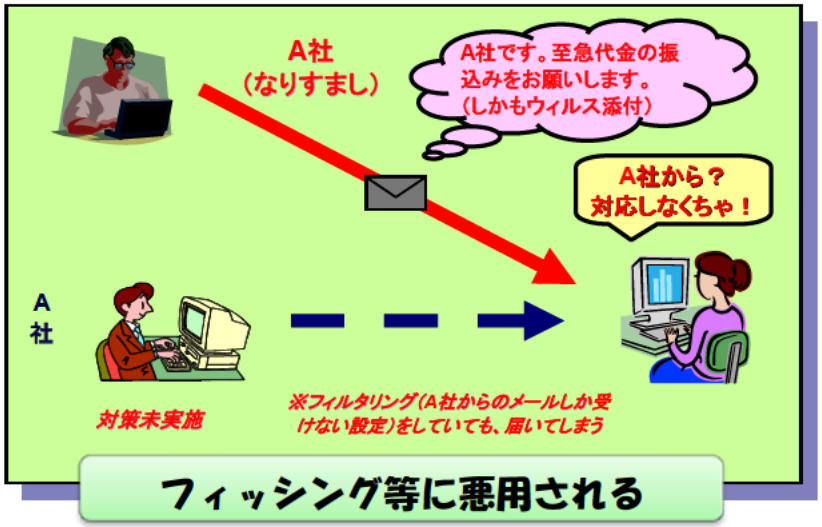
✓ **電子メールのプロトコル**（通信手順：SMTP(simple mail transfer protocol)）**では、電子メールの送受信にあたり、認証等が実施されず、送信者情報の偽装が容易**

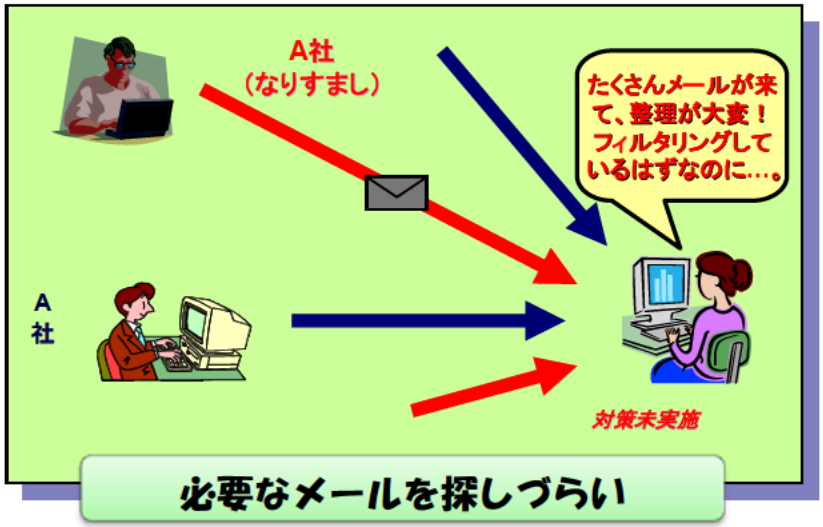
・ 送信側では、受信側メールサーバの場所の問合せを行うため、ドメイン単位での確認はしているが、受信側ではそのような確認は行われない

✓ **拡く定着しているため、これからプロトコルを変更していくことは、非現実的**

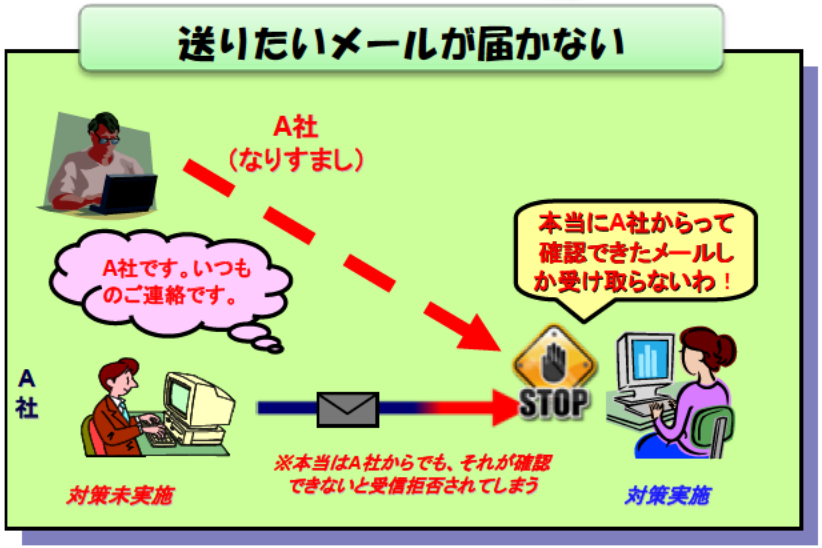
・ 電子メールの基本的なプロトコルを変更するには、全世界のメールサーバーが一斉に対応することが必要と考えられる

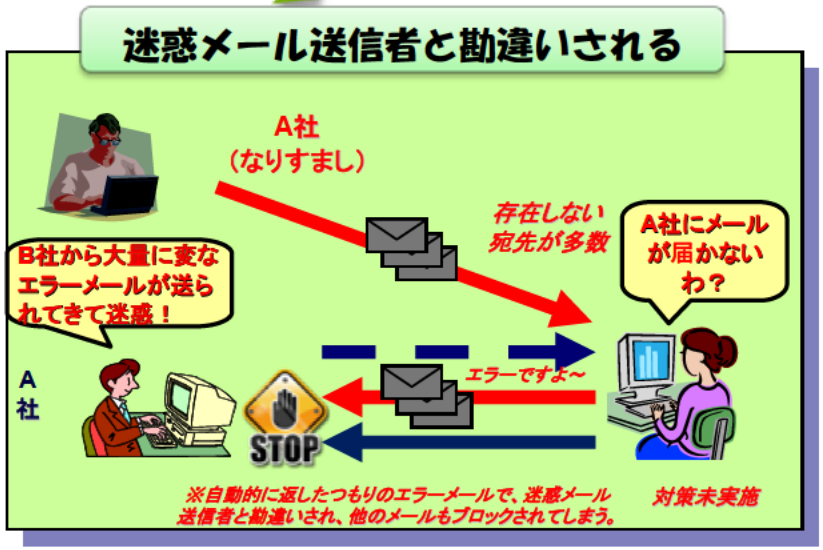
なりすまし（送信者情報の偽装）による被害





他人に送信者情報を偽装されると…





フィッシング等に悪用される

✓ **正規な送信元になりすまされ、フィッシング等に悪用される問題**

- 正規の送信者を騙って不正なサイトへ誘導等
- 不正なサイトで、IDやpasswordを入力すること等で、金銭的被害や個人情報の詐取などの被害
- 明確なものは、さらに、信頼できる送信者かの確認等

✓ **メール受信者では、正規の送信者かどうかの確認が行いづらいという問題**

送りたいメールが届かない

✓ **送信側でなりすまし対策をしていないと、送りたいメールが受信してもらえないことがある**

- 受信側でなりすまし対策を実施している場合に、送信側でなりすまし対策に対応していないと、正規のメールでも受信してもらえないこともある

必要なメールを探しづらい

✓ **迷惑メールが大量にくることにより、必要なメールが探しづらくなるという問題**

✓ **送信元が詐称されていることにより、フィルタリングが行いづらいことも一因**

- ドメインを指定しての拒否や限定受信にあたり、ドメインを詐称したメールが誤判定される

迷惑メール送信者と勘違いされる

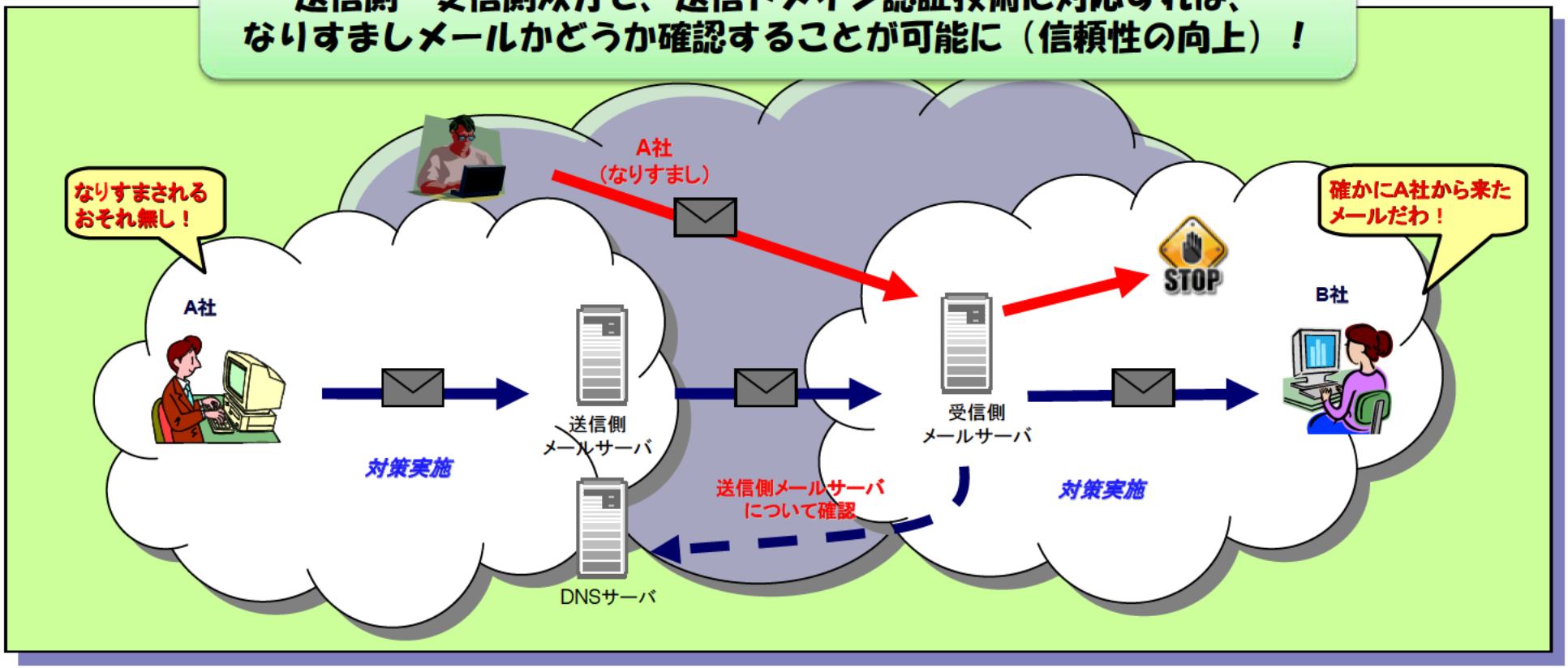
✓ **迷惑メールに対してエラーメールを返すことによる問題が生じている**

- 迷惑メールには、存在しないアドレスに宛てられたものも多い
- 詐称された送信元に対してエラーメールが大量に送信されるという問題あり
- エラーメールが大量に送信されることにより、エラーメールの送信元（迷惑メールの受信者）がスパマーと判断される事象も生じている（ブラックリストに掲載され、ブロックされることもあり）

✓ **迷惑メールの受信側が、迷惑メール送信者とされてしまう**

送信ドメイン認証技術による対応

**送信側・受信側双方で、送信ドメイン認証技術に対応すれば、
なりすましメールかどうか確認することが可能に（信頼性の向上）！**



- ✓ **送信元情報のうちドメイン名が送信元に対して正当であるかを技術的に確認可能**
- ✓ **送信元情報をドメイン単位で判断**（DNS(Domain Name System)サーバーと連携）
  - ・ 不確かなメールは、フィルタリング等の処理
  - ・ 明確なものは、さらに、信頼できる送信者かの確認等
- ✓ **既存のメール配送の仕組み（SMTP）を変更することなく、上位互換的に導入可能**
- ✓ **受信側で受ける電子メールを選別していくことが可能になる（電子メールの信頼性の向上）**
- ✓ **なお、（送信元ドメイン以外の）送信者情報の詐称の有無や、迷惑メールであるかどうかを判定する技術ではない**

送信ドメイン認証技術の普及

なりすましメールのない世界を目指して

送信側

① 自らのドメインになりすまされることによる被害を理解しよう
② SPF/SenderIDのDNSへの設定をしよう
③ 信頼性が必要とされるドメインの場合には、DKIMにも対応しよう

受信側

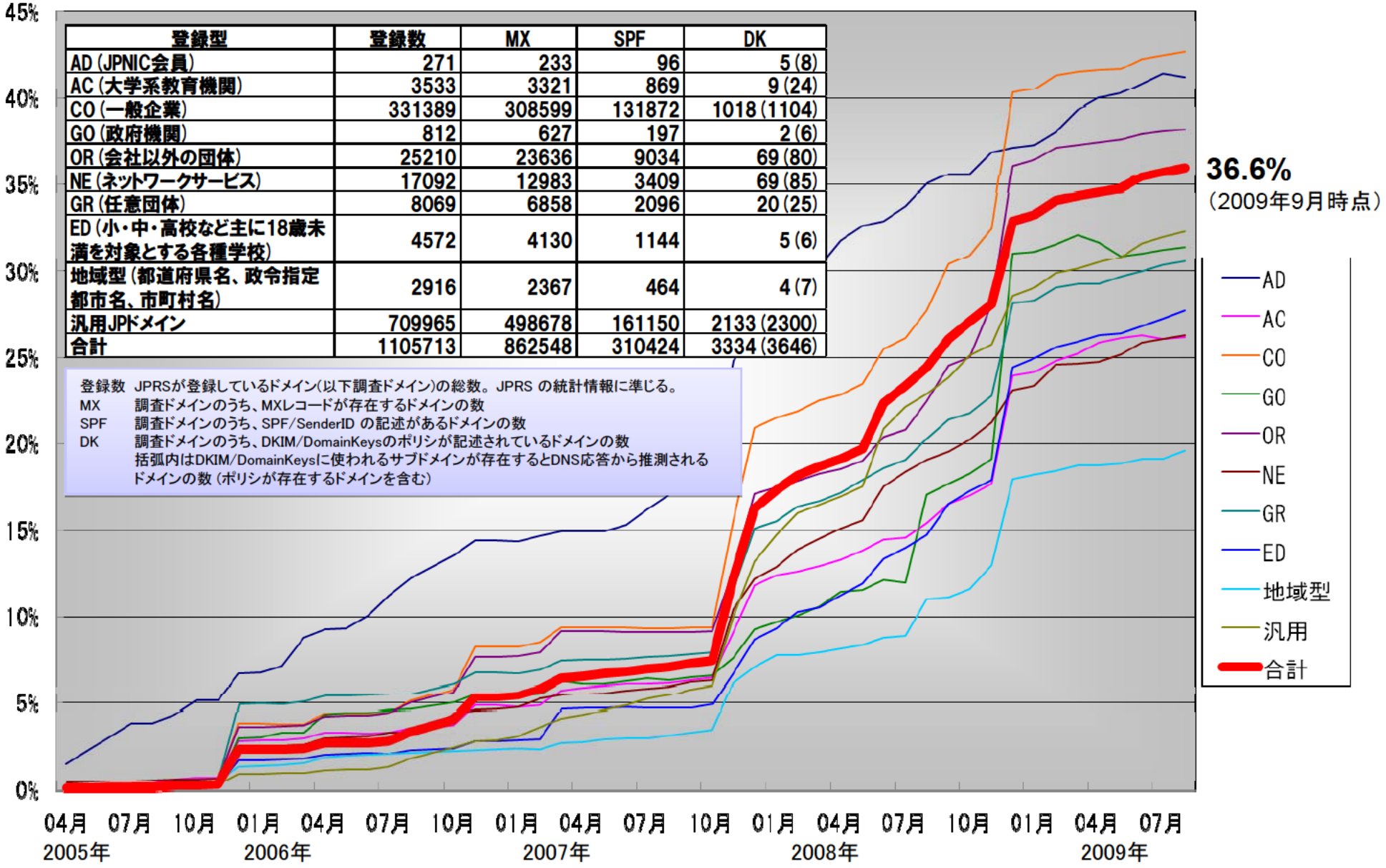
【個人】
① 利用しているプロバイダが対応しているか調べよう
② なりすましメールをフィルタリングで隔離してみよう
【企業等】
③ 必要に応じて、受信側でも、送信ドメイン認証技術を活用しよう

参考資料

送信側でのDNSへの設定状況

登録型	登録数	MX	SPF	DK
AD (JPNIC会員)	271	233	96	5 (8)
AC (大学系教育機関)	3533	3321	869	9 (24)
CO (一般企業)	331389	308599	131872	1018 (1104)
GO (政府機関)	812	627	197	2 (6)
OR (会社以外の団体)	25210	23636	9034	69 (80)
NE (ネットワークサービス)	17092	12983	3409	69 (85)
GR (任意団体)	8069	6858	2096	20 (25)
ED (小・中・高校など主に18歳未満を対象とする各種学校)	4572	4130	1144	5 (6)
地域型 (都道府県名、政令指定都市名、市町村名)	2916	2367	464	4 (7)
汎用JPドメイン	709965	498678	161150	2133 (2300)
合計	1105713	862548	310424	3334 (3646)

登録数　JPRSが登録しているドメイン(以下調査ドメイン)の総数。JPRS の統計情報に準じる。
MX　調査ドメインのうち、MXレコードが存在するドメインの数
SPF　調査ドメインのうち、SPF/SenderID の記述があるドメインの数
DK　調査ドメインのうち、DKIM/DomainKeysのポリシが記述されているドメインの数
括弧内はDKIM/DomainKeysに使われるサブドメインが存在するとDNS応答から推測されるドメインの数 (ポリシが存在するドメインを含む)



http://member.wide.ad.jp/wg/antispam/stats/index.html.ja(2009年9月時点)より作成

ISP等の対応状況

「送信ドメイン認証技術導入状況調査」((財)日本データ通信協会)によると　送信側導入は進んでいるものの受信側の導入はまだ少ない。

2009年7月31日現在

ISPの送信ドメイン認証実装状況		送信時実装 ※1、2		受信時判定 ※3	
No.	事業社名	SPF/ SenderID	DKIM/ DomainKeys	SPF/ SenderID	DKIM/ DomainKeys
1	株式会社テクノロジーネットワーク	☆	—	—	—
2	ニフティ株式会社	☆	☆	—	—
3	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 三河湾ネットワーク株式会社 シーシーエヌ株式会社	☆	—	—	—
4	KDDI株式会社	☆	—	○	—
5	九州通信ネットワーク株式会社	☆	—	—	—
6	NECビッグローブ株式会社	☆	—	○	○
7	中部ケーブルネットワーク株式会社	☆	—	○	○
8	トナミ運輸株式会社	☆	—	—	—
9	株式会社ドリーム・トレイン・インターネット	☆	—	—	—
10	株式会社佐渡テレビジョン	☆	—	○	—
11	株式会社ケイ・オプティコム	☆	—	—	—
12	株式会社ハイホー	☆	—	—	—
13	株式会社インターネットイニシアティブ	☆	—	◎	○
14	イッツ・コミュニケーションズ株式会社	☆	—	—	—
15	株式会社キャッチネットワーク	☆	—	—	—
16	KMN株式会社	☆	—	—	—
17	知多メディアスネットワーク株式会社	☆	—	—	—
18	株式会社エヌ・ティ・ティ・ドコモ	☆	—	—	—
19	NTTコミュニケーションズ株式会社	☆	—	○	—
20	ソフトバンクテレコム株式会社	☆	—	—	—
21	株式会社NTTデータ三洋システム	☆	—	—	—
22	ソフトバンクテレコム株式会社	☆	—	—	—
23	株式会社エヌ・ティ・ティ エムイー	☆	—	—	—
24	ソフトバンクBB株式会社 ヤフー株式会社	☆	☆	◎	◎
25	関西マルチメディアサービス株式会社	☆	—	—	—
26	飯能ケーブルテレビ株式会社	☆	—	—	—
27	株式会社ハイネット	☆	—	—	—
28	株式会社NTTぷらら	☆	—	—	—

携帯・PHS事業者		送信時実装		受信時判定	
No.	事業社名	SPF/ SenderID	DKIM/ DomainKeys	SPF/ SenderID	DKIM/ DomainKeys
29	KDDI株式会社	☆	—	◎	—
30	株式会社エヌ・ティ・ティ・ドコモ	☆	—	◎	—
31	ソフトバンクモバイル株式会社	☆	—	—	—
32	株式会社ウィルコム	☆	—	—	—

フリーメール		送信時実装		受信時判定	
No.	事業社名	SPF/ SenderID	DKIM/ DomainKeys	SPF/ SenderID	DKIM/ DomainKeys
33	ニフティ株式会社	☆	☆	—	—
34	Google株式会社	—	☆	○	○
35	NTTレゾナント株式会社	☆	—	—	○
36	株式会社ライブドア	☆	—	○	—
37	Microsoft Corp	☆	—	○	—
38	ヤフー株式会社	☆	☆	◎	◎

送信時実施＝「☆」、受信時ラベリング＝「○」、受信時フィルタリング＝「◎」、未実施＝「—」

※1　送信時実装はいずれかの方式により実施されている場合に”☆”と表示しています。

※2　送信時SPF実装については、限定子が“-all”、“~all”のものを実装としています。

第3章　2009年度に取り組む重点政策

第1節　対策実施4領域における取組の推進と政策目的の着実な実現

（1）対策実施4領域

①政府機関・地方公共団体

（カ）　その他個別の情報セキュリティ対策の推進

2）「政府機関への成りすましの防止」

【具体的施策】

ア）**政府機関から発信する電子メールに係る成りすましの防止**（内閣官房、総務省及び全府省庁）

悪意の第三者が政府機関又は政府機関の職員に成りすまし、一般国民や民間企業等に害を及ぼすことが無いよう、**SPF(Sender Policy Framework)等の送信ドメイン認証技術の採用等を推進**していく。

③企業

（イ）「企業の情報セキュリティ向上に資する製品やサービスの提供促進と活性化」

【具体的施策】

シ）**スパムメール対策の強化**（総務省及び経済産業省）

巧妙化・悪質化が進展し全体として増加が続くスパムメールに対応するため、2008年の法改正によりオプトイン方式が導入された特定電子メール法及び特定商取引法の着実な執行等所用の措置を講じる。

また、国内の主要インターネット接続サービス事業者や携帯電話事業者が中心となり設立された民間団体である「JEAG」等の業界団体と連携して、スパムメール送信の防止に効果のある技術である25 番ポートブロックや**送信ドメイン認証技術等の導入を促進**する。

さらに、日本に着信するスパムメールの大部分を占める海外から発信されるスパムメールに対応するため、スパムメール対策を行う外国執行当局との連携を強化するとともに、民間における国際的なスパムメール対策の連携を推進する。

その他、違法なスパムメールに関する情報を当該スパムメールの送信塔に利用されたインターネット接続サービス事業者に通知し利用停止等の措置を促進する「迷惑メール追放支援プロジェクト」（2005年2月～）を引き続き実施する。

④個人

（ウ）対策が困難な個人も含めた情報セキュリティ水準向上に向けた取り組み

【具体的施策】

エ）**スパムメール対策の強化**（総務省及び経済産業省）

（第3章第1節（1）③（イ）シ）に同じ）

第5章　2010年に喫緊に取り組むべき課題

〔官民による技術の研究開発及び導入の推進〕

【具体的施策】

イ）**スパムメール対策の強化**（総務省及び経済産業省）

（第3章第1節（1）③（イ）シ）に同じ）

送信ドメイン認証に関する関係者の取り組み

我が国での取り組み

JEAG(Japan Email Aunti-abuse Group)

✓ 2006年に、送信ドメイン認証についてのリコメンデーションを公表

WIDEプロジェクト・JPRS

✓ 2005年以降、毎月、我が国のドメインにおける送信ドメイン認証の設定比率を調査・公表

(財)インターネット協会

✓ 毎年開催しているカンファレンスで、送信ドメイン認証技術について紹介(2005年～2007年、2009年)

(財)日本データ通信協会

✓ 2009年5月より、インターネットサービスプロバイダーにおける送信側・受信側の実装状況を調査し、公表

海外での取り組み

関連RFC

RFC4406	Sender ID: Authenticating E-Mail	Sender IDの標準規格
RFC4407	Purported Responsible Address in E-Mail Messages	Sender ID で利用するPRAの標準規格
RFC4408	Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, version 1	SPFの標準規格
RFC4871	DomainKeys Identified Mail (DKIM) Signatures	DKIMの標準規格
RFC5617	DomainKeys Identified Mail(DKIM) Authoer Domain Signing Practices(ADSP)	DKIMの署名方針に関する補助規格
RFC5672	RFC 4871 DomainKeys Identified Mail (DKIM) Signatures – Update	DKIMの標準規格の更新
RFC5451	Message Header Field for Indicating Message Authentication Status	認証結果のヘッダーへの記録形式の標準規格

BITS(Banking Industry Technology Secretariat)

米国の金融機関からなる非営利団体

✓ 2007年4月に作成したセキュリティ関係のツールキットの中で、送信ドメイン認証を紹介
✓ 2009年6月に、送信ドメイン認証導入のベストプラクティス集を公表

MAAWG(Messaging Anti-Abuse Working Group)

ウィルスなどEmailの濫用に対処するために通信関連企業が集まったグループ

✓ 2004年12月に、送信ドメイン認証技術の導入に関するホワイトペーパーを公表
✓ 2008年4月に、正しいメールを守るための基盤である送信ドメイン認証技術を解説するホワイトペーパーを公表