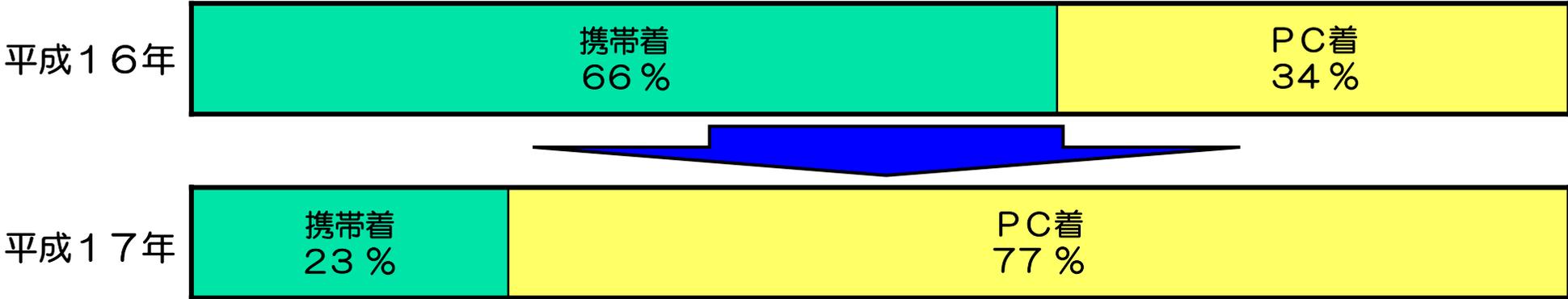


# 総務省による最近の 迷惑メール対策

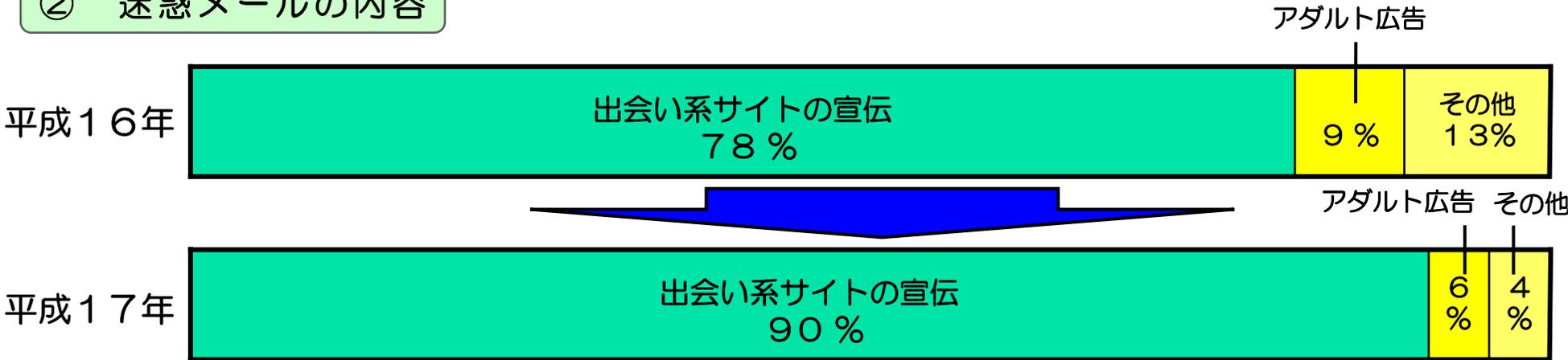
平成18年4月12日  
総務省総合通信基盤局  
消費者行政課

# 我が国における迷惑メールの現状

## ① 受信端末

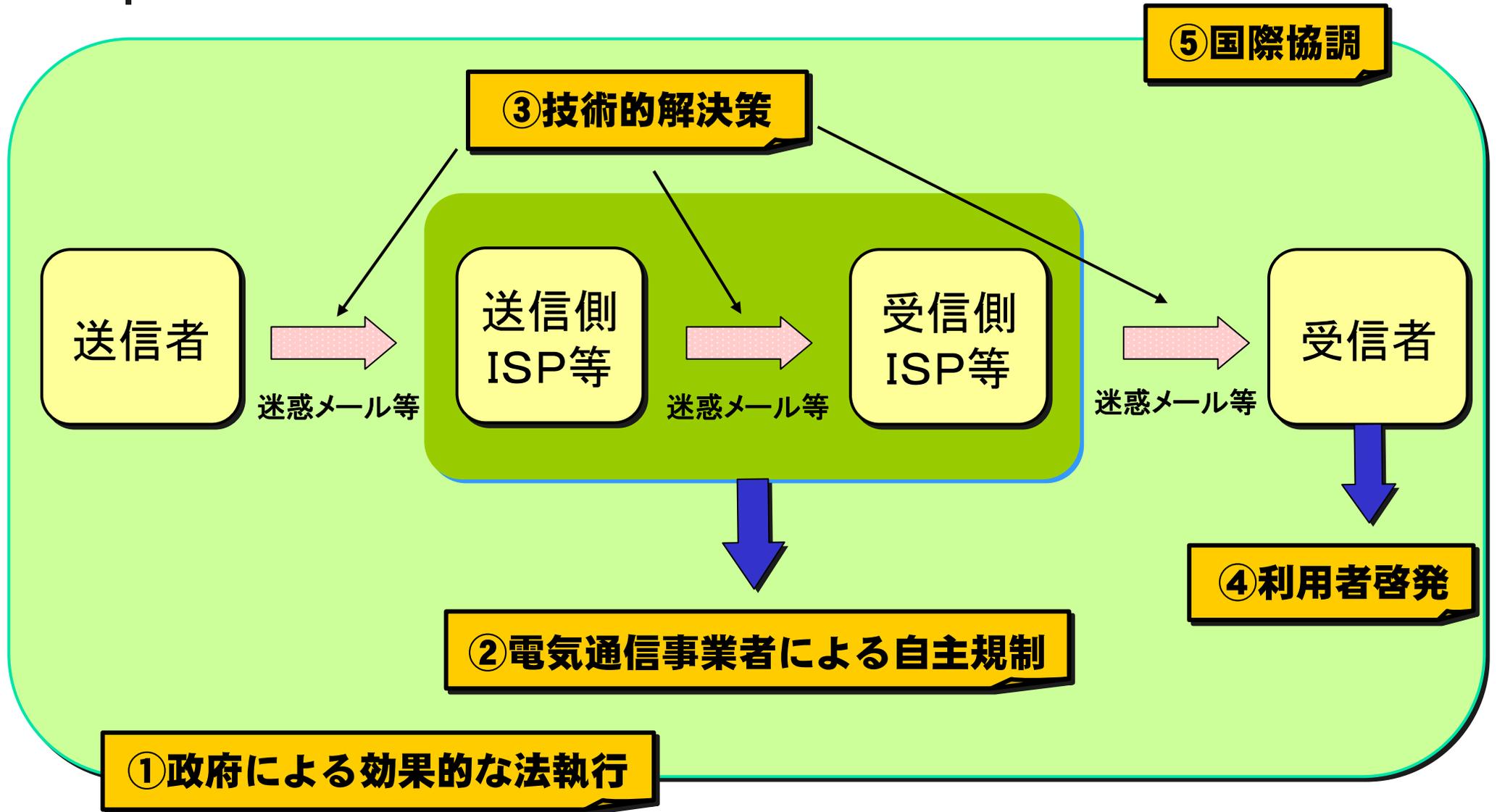


## ② 迷惑メールの内容



注) 平成16年～平成17年に迷惑メール相談センター((財)日本データ通信協会内)に寄せられた違反情報提供を分析したもの(サンプル調査)。

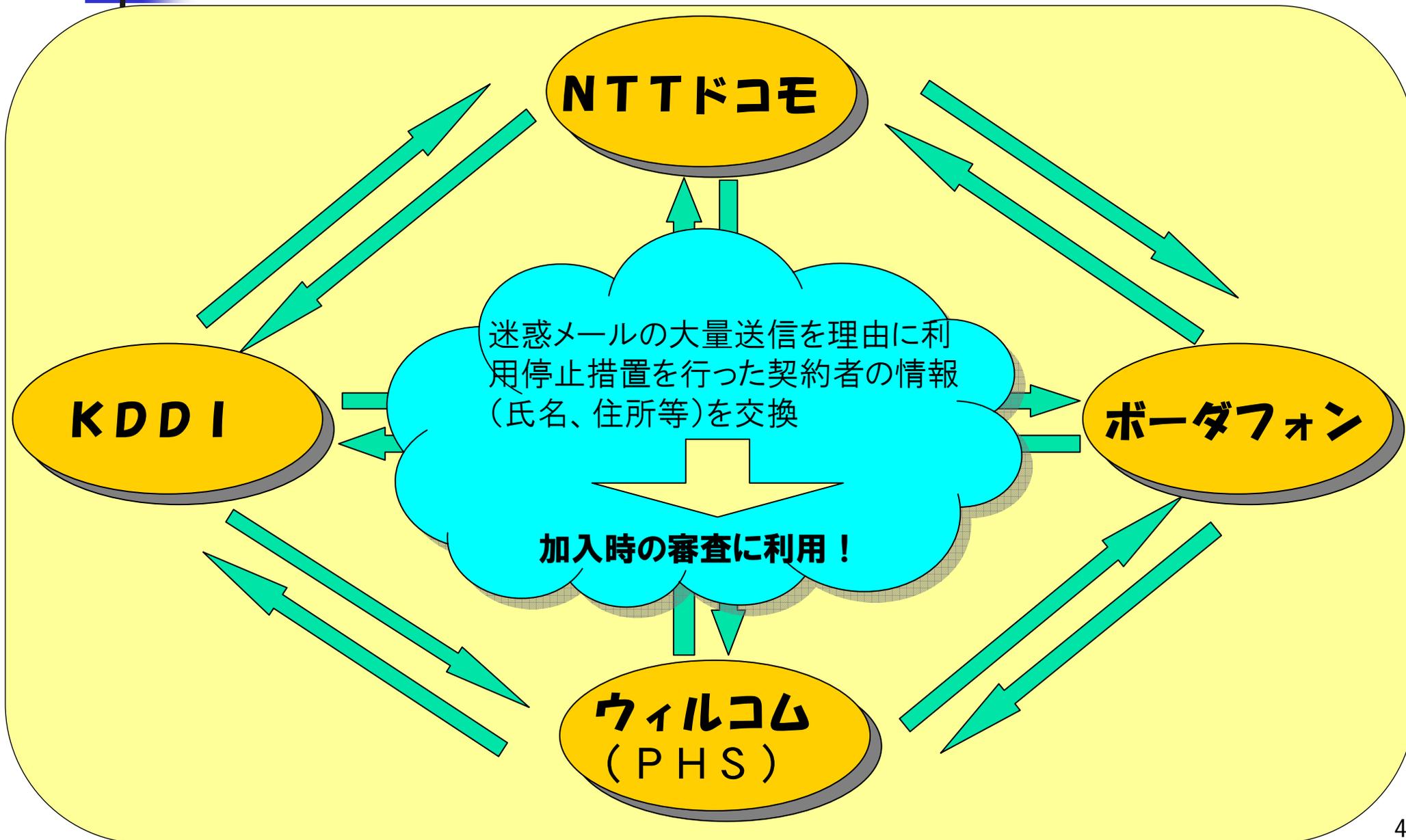
# 迷惑メール対策の全体像





〔②電気通信事業者による自主規制〕

# 携帯電話事業者による迷惑メール送信者情報（ブラックリスト）交換の実施（H18.3.1～）



## 迷惑メール送信者情報（ブラックリスト）の交換に係る規定

### 電気通信事業における個人情報保護に関するガイドライン

（迷惑メール等送信に係る加入者情報）

- 第28条 **電気通信事業者は**、一時に多数の者に対してされる電子メールの送信による電子メールの送受信上の支障を防止するため特に必要であり、かつ、適切であると認められるときは、他の電気通信事業者との間において、**加入者情報**（一時に多数の者に対し、特定電子メールの送信の適正化等に関する法律（平成十四年法律第二十六号）の規定に違反する電子メールの送信その他の電子メールの送受信上の支障を生じさせるおそれのある電子メールの送信をしたことを理由として、電気通信事業者が利用停止措置を講じ、又は契約を解除した加入者の氏名、住所その他の当該加入者に関する情報に限る。以下同じ。）**を交換することができる**。ただし、当該加入者情報を交換の対象とすることが本人の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。
- 2 電気通信事業者は、加入者情報を他の電気通信事業者との間で交換する場合は、その旨並びに交換される加入者情報の項目、交換する電気通信事業者の範囲及び交換される加入者情報の管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。
  - 3 電気通信事業者は、前項の交換される加入者情報の管理について責任を有する者の氏名又は名称を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くものとする。
  - 4 加入者情報の交換をした電気通信事業者は、当該加入者情報を**加入時の審査**以外の目的のために使用してはならない。
  - 5 加入者情報を提供し、又は提供を受けた電気通信事業者は、当該加入者情報の適正な管理に特に万全を期すものとする。

# JEAGによる「リコメンデーション」について

## 1. 「JEAG」について

- 迷惑メール対策を業界全体で取り組むべき問題と位置付け、技術的な見地を元にして対策を検討・実施するため、国内の主要インターネットサービスプロバイダ(ISP)や携帯通信事業者が中心となり、平成17年3月15日に設立された民間団体 (Japan Email Anti-Abuse Group)
- 平成18年2月23日現在、31社が参加。  
総務省・経済産業省・(財)日本データ通信協会がオブザーバーとして参加。

## 2. WGとリコメンデーション

- 以下の4つのWGにおいて検討。
  - ① 「Wirelessサブワーキンググループ」——携帯電話宛の迷惑メールの撲滅について議論するWG
  - ② 「Outbound Port 25 Blockingサブワーキンググループ」  
——自網外への25番ポート接続を遮断する対策について議論するWG
  - ③ 「送信ドメイン認証サブワーキンググループ」  
——メール送信者の詐称をさせないスキームとしてのドメイン認証を議論するWG
  - ④ 「迷惑メール対策啓蒙活動サブワーキンググループ」——迷惑メール撲滅のための啓蒙活動WG
- ⇒ ①～③について、平成18年2月23日、WGにおける検討を踏まえた事業者・メールサーバ管理者向けの提案書(リコメンデーション)を公表。

## 各リコメンデーションの概要

### 1. JEAG Recommendation ～携帯電話宛の迷惑メールに対する提言書～

- メールを送信側と受信側それぞれの取組について、携帯電話事業者及びISPがこれまで実施して効果があった対策を整理し、導入を推奨
  - ・ 携帯電話事業者: 受信フィルタ機能の提供、利用停止措置等
  - ・ ISP: 送信数制限、Outbound Port 25 Blocking等

### 2. JEAG Recommendation ～Outbound Port 25 Blockingについて～

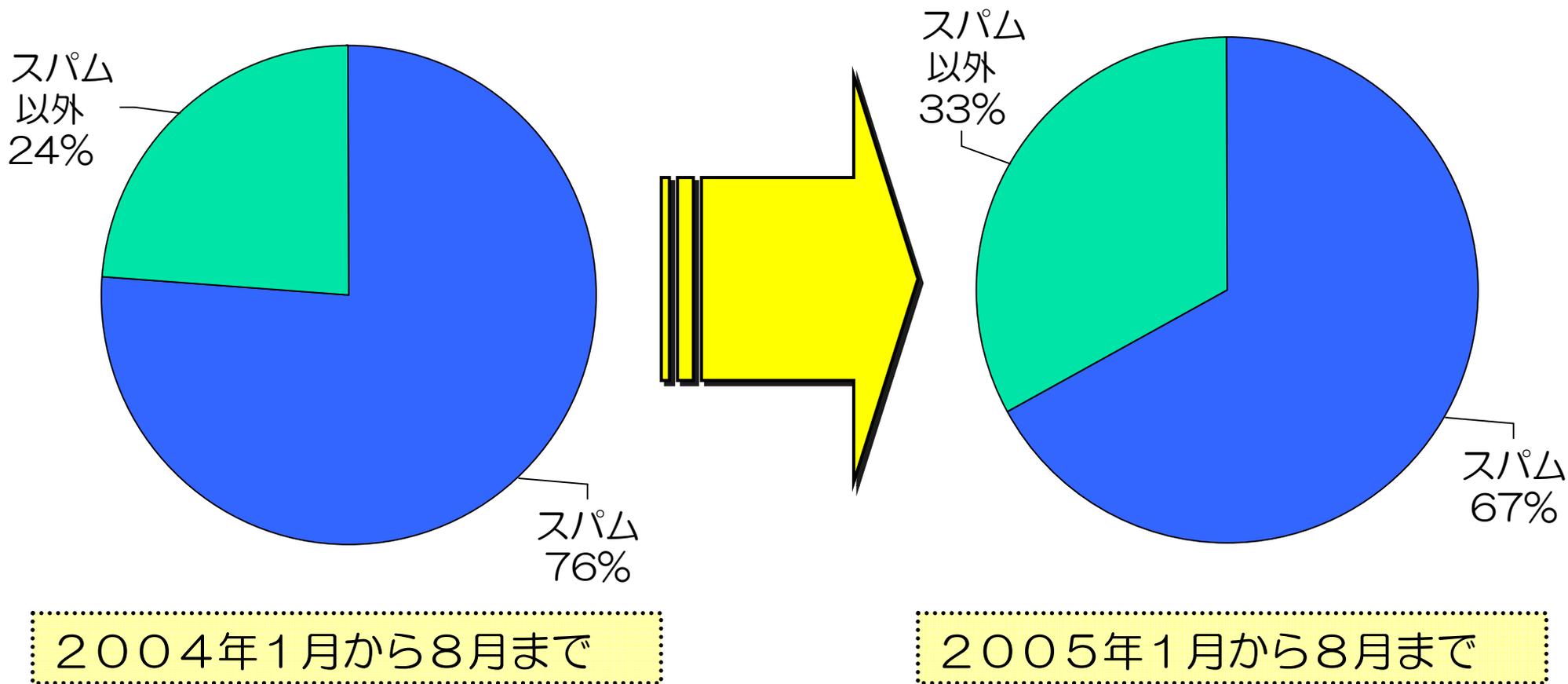
- Outbound Port 25 Blockingについて、導入プロセスの提案、導入における課題の検討、Outbound Port 25 Blockingと併せて実施すべきSubmission PortやSMTP authの導入を提案
- 2006年9月までにSubmission Portを利用者に提供すること、2007年3月までにすべてのメール送信についてOutbound Port 25 Blockingを導入すること等を提案

### 3. JEAG Recommendation ～送信ドメイン認証について～

- 送信ドメイン認証技術の2種類の方式(SPF、DKIM)のいずれかを事業者が導入することを目標。
- 導入時の設定の提案や各種サービスの運用方法について提案
- 2006年3月末までに、いずれかの送信ドメイン認証技術について、送信側での対応(SPFレコードの宣言又はDKIMの署名情報付加)を行うこと等を提案

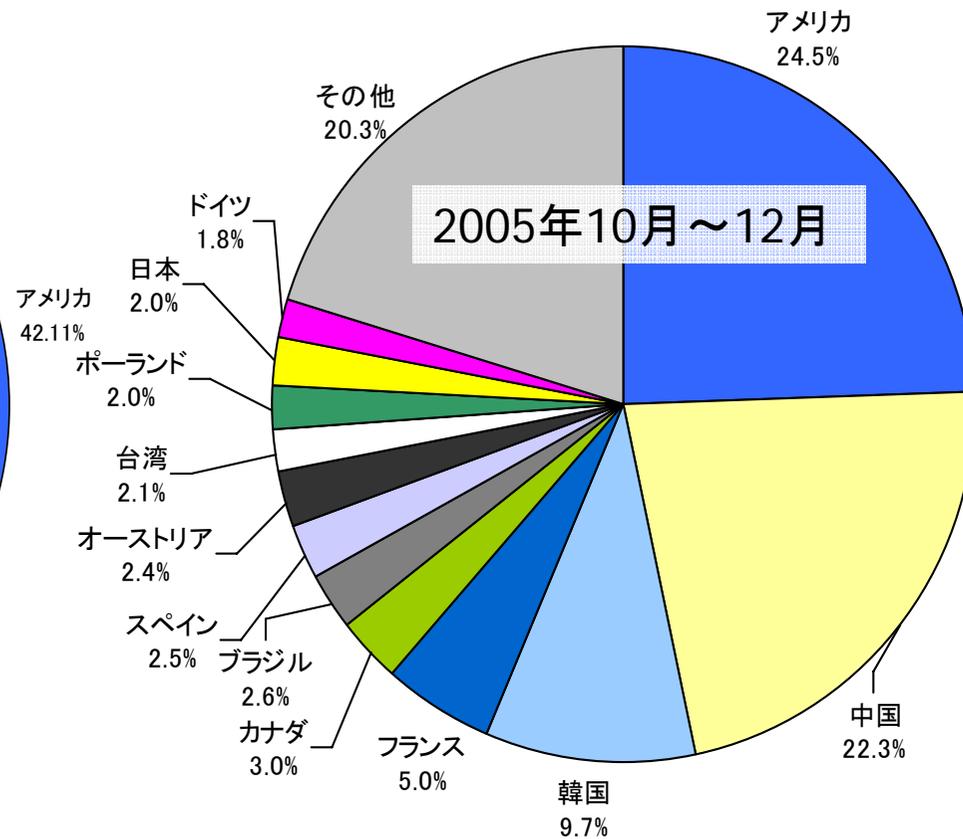
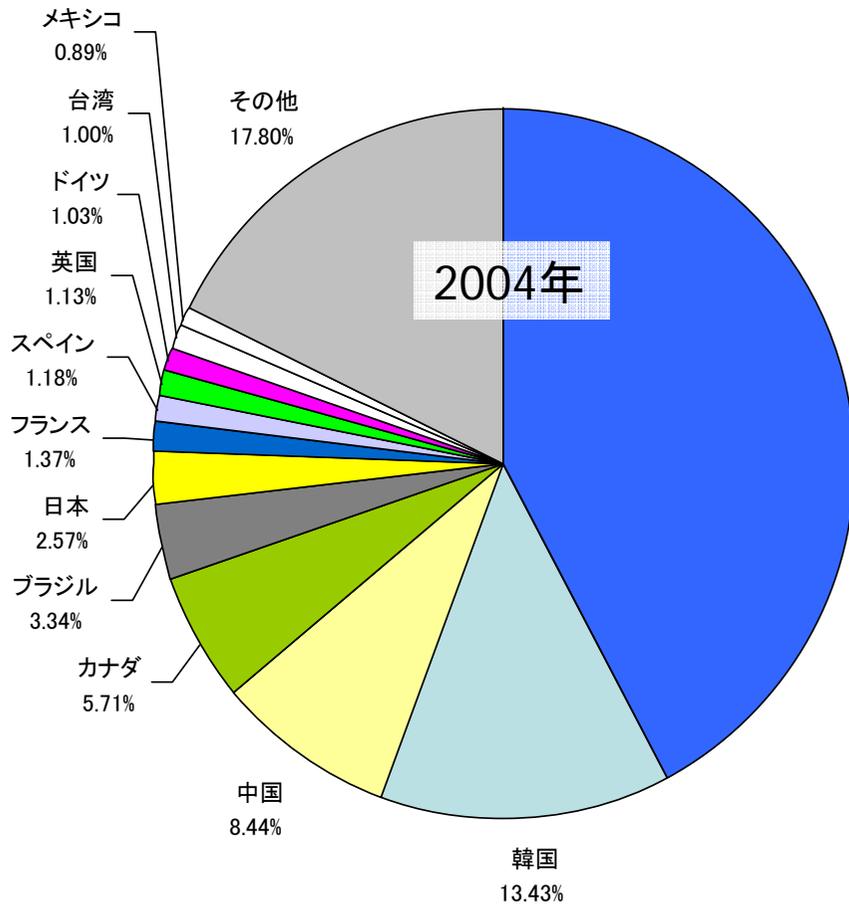
〔⑤国際協調〕

# 全メールトラフィックに占めるスパムの比率



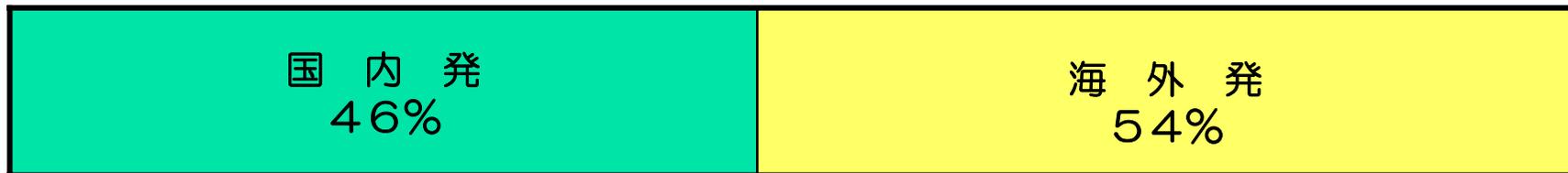
出典：MXロジック社（米国ソフトウェア会社）公表資料（2005年9月22日）<sub>8</sub>

# 世界における迷惑メールの発信国（ソフォス社）

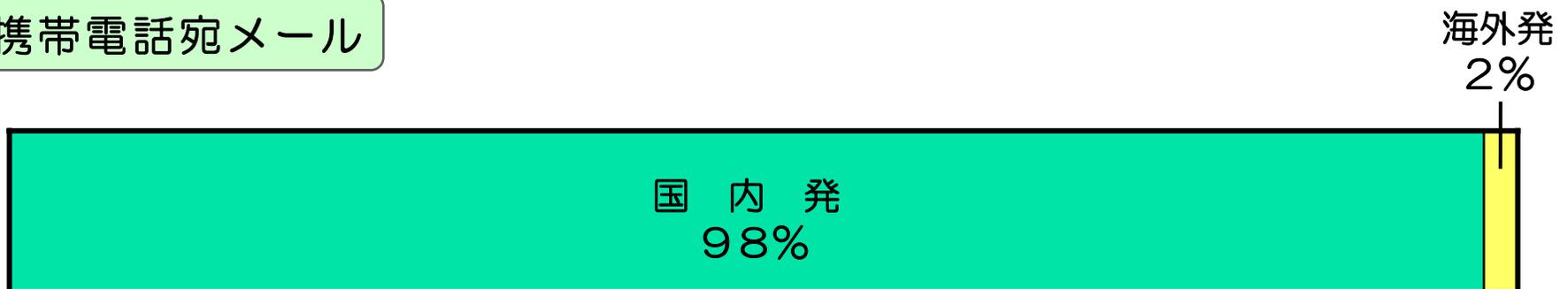


## 我が国に着信する迷惑メールの発信元（国内・海外）比率

### ① PC宛メール



### ② 携帯電話宛メール



注1) 2005年7月～12月に(財)日本データ通信協会に設置したモニター機に着信した迷惑メール(25,827通)を分析したもの。

注2) 国内発・海外発の別は、受信したメールのヘッダ情報から発信元ISPを洗い出し、分析した結果に基づき分類。

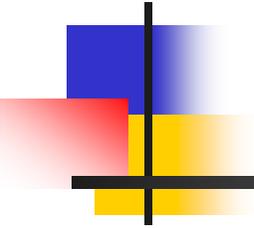
# スパム対策・国際連携の取組

## 【マルチ（多国間）】

- **OECD「スパムタスクフォース」（04年7月～）**
  - ・ 06年6月までに「アンチスパム・ツールキット（包括的スパム対策）」を取りまとめる予定。
- **LAP（ロンドンアクションプラン）（04年11月～）**
  - ・ 年1回の会合及び年最低4回の電話会議等を通じ、法執行の強化をテーマに議論。
- **スパム対策の協力に関する多国間M o U（覚書）（05年4月～）**
  - ・ アジア太平洋地域の12機関が締結した覚書に基づき、具体的な協力策等について定期的に議論。
- **ITU**
  - ・ 世界規制庁シンポジウム（05年11月）等でスパム対策について定期的に意見交換。
- **APEC**
  - ・ 電気通信サブグループ等でスパム対策について定期的に意見交換。
- **ICPEN（国際消費者保護執行ネットワーク）（92年～）**
  - ・ 国境を越える違法な対消費者取引行為を規制するために結成された会合。05年にはスパムの実態調査を行った。

## 【バイ（二国間）】

- **日伊情報通信政策協議（05年2月）**
  - ・ 両国のスパム対策等について意見交換。
- **日米情報通信政策協議（05年6月）**
  - ・ 両国のスパム対策等について意見交換。  
（06年4月、米国FTC消費者保護局長と総務省総合通信基盤局長が会談）
- **日加情報通信政策協議（05年10月）**
  - ・ 両国のスパム対策等について意見交換。
- **日EU定期協議（05年10月）**
  - ・ 両者のスパム対策等について意見交換。
- **日豪情報通信政策協議（05年10月）**
  - ・ 両国のスパム対策等について意見交換。
- **日仏定期協議（06年2月）**
  - ・ 両国のスパム対策等について意見交換。



# 參考資料

---

# 特定電子メールの送信の適正化等に関する法律（特電法）の概要

(H14.7.1施行、H17.11.1改正)

## 表示義務

特定電子メール（受信者の同意を得ずに送信される広告宣伝メール）の送信にあたり、送信者に次の事項の表示を義務づけ（第3条）

- ① 特定電子メールである旨（⇒「未承諾広告※」）
- ② 送信者の氏名又は名称
- ③ 送信者の住所、電話番号
- ④ 受信拒否の通知をすることができる旨及び当該通知を受けるための電子メールアドレス  
 <違反者には総務大臣の措置（是正）命令>

## 拒否者への再送信禁止

受信拒否の通知をした者に対する特定電子メールの再送信を禁止（第4条）  
 <違反者には総務大臣の措置（是正）命令>

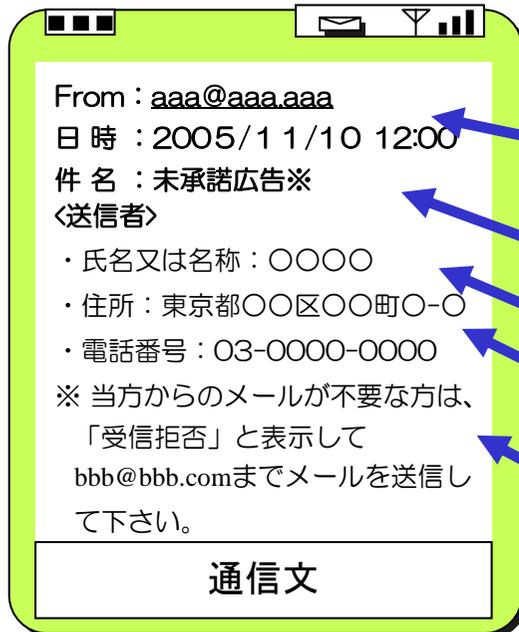
## 送信者情報を偽った送信の禁止

電子メールアドレス等の送信者情報を偽って広告宣伝メールを送信することを禁止（第6条）  
 <違反者には刑事罰（懲役1年以下又は100万円以下の罰金）>

## その他

- ・自動生成プログラムを用いて作成した架空電子メールアドレスに宛てて、電子メールを送信することを禁止（第5条）
- ・電気通信事業者は、一時に多数の電子メールが送信された場合等、必要な範囲内において、その電気通信役務の提供を拒むことができる（第11条）

## 携帯電話の場合の表示（例）

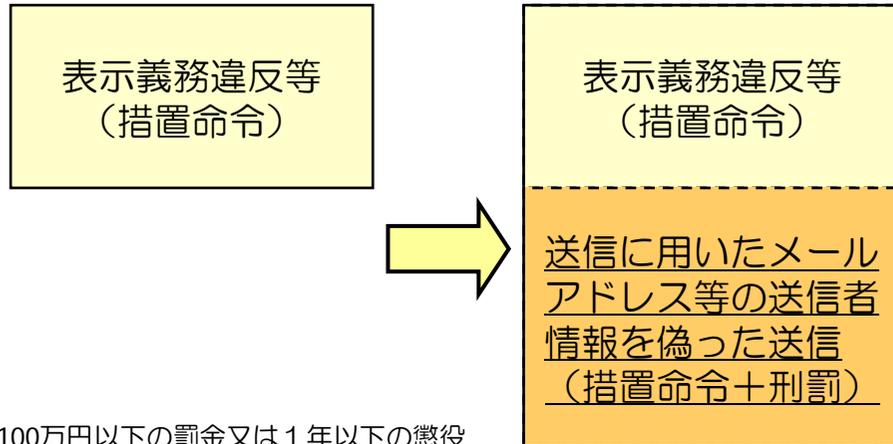


## 送信者情報（送信に用いた電子メールアドレス等）を偽った送信は禁止！

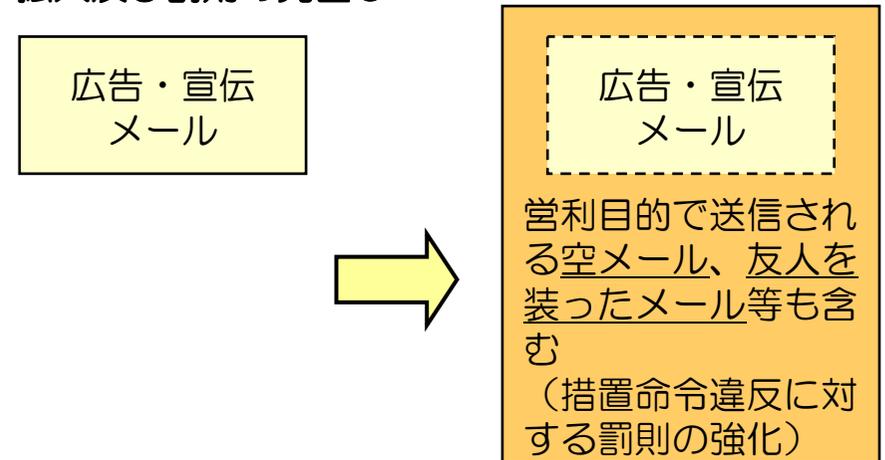
表示事項	表示場所
未承諾広告※	特定電子メールの表題部の最前部
特定電子メールの送信者の氏名又は名称	特定電子メールの通信文より前
特定電子メールの送信者の住所・電話番号	任意の場所
電子メールで受信拒否の通知ができる旨及び当該通知を受けるための電子メールアドレス	特定電子メールの通信文より前

# 「特定電子メールの送信の適正化等に関する法律」(特電法)の一部を 改正する法律の概要(平成17年5月13日成立、同年11月1日施行)

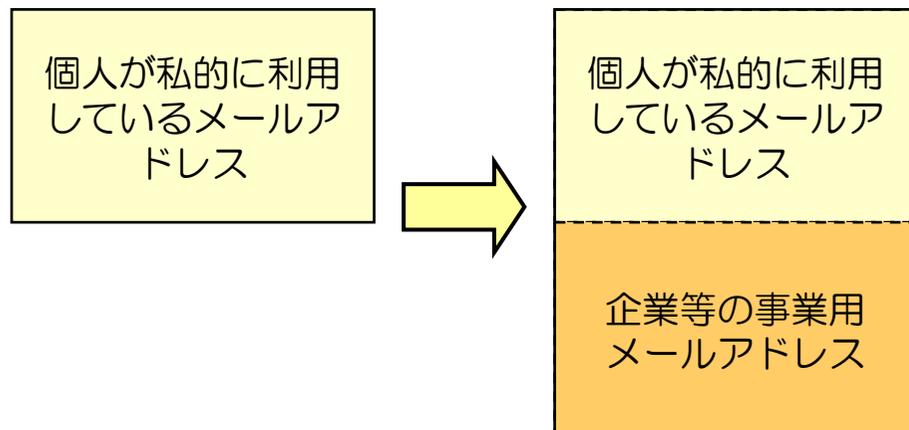
## 1. 送信者情報を偽った電子メール送信の禁止及び 刑罰(直罰)規定(※)の整備



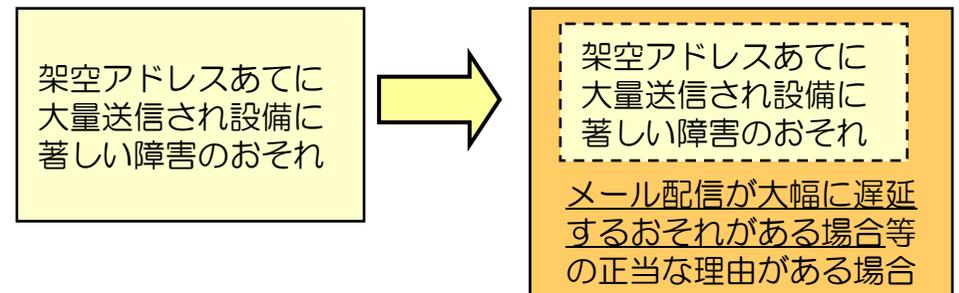
## 2. 架空アドレスあてのメール送信を禁止する範囲の 拡大及び罰則の見直し



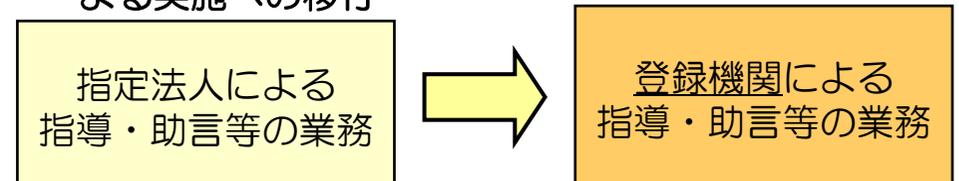
## 3. 特定電子メールの範囲の拡大



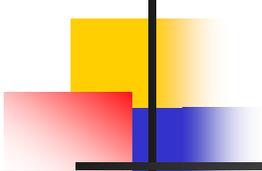
## 4. 電気通信事業者による役務提供拒否事由の拡大



## 5. 指定法人による指導・助言等の業務の登録機関に よる実施への移行



注：省令改正でSMSも対象に



# 「送信ドメイン認証技術」について

## 1. 背景

迷惑メールやフィッシングメールは、捜査機関等の追跡から逃れるため、メールアドレス等の発信元の情報を偽っているケースが多くなっている。

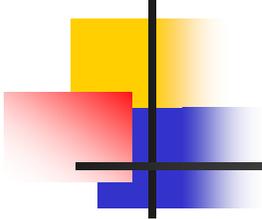
注：(財)日本データ通信協会の調査によれば、迷惑メールの94%が送信元を偽装

## 2. 概要

- メールが発信元サーバの情報(ドメイン)を、受信側サーバで認証する技術のこと。これにより、「送信元が特定可能なメール」と確認できたもののみ受信するなどといった設定が可能となる。
- 送信ドメイン認証技術は、認証方法の違いからドメイン名とIPアドレスを照合する「SPF」(又はSender ID)と電子署名の仕組み(秘密鍵・公開鍵)を用いた「Domain Keys」(又はDKIM)の2種類に大きく分けられる。SPFにおいてはメールの転送の場合に、Domain Keysにおいてはメールリングリストの場合に認証を正しく行えない場合がある等の課題があり、対応策について、現在更なる検討が進められている。

## 3. 我が国における導入状況

- ・送信側サーバ：Nifty(2005年5月導入開始)、IIJ(2005年3月(職員等のメールについてDKIM、SPF)、12月(利用者のメールについてSPF)導入開始)(DKIM、SPF)  
Yahoo!(2005年8月導入開始)(Domain Keys)  
KDDI(2005年12月導入開始)、NTTドコモ(2005年12月導入開始)、WILLCOM(2006年3月導入開始)(SPF)等
- ・受信側サーバ：Yahoo!(2005年9月導入開始)(Domain Keys)  
KDDI(携帯電話のみ)(2006年度中に導入予定)(SPF)

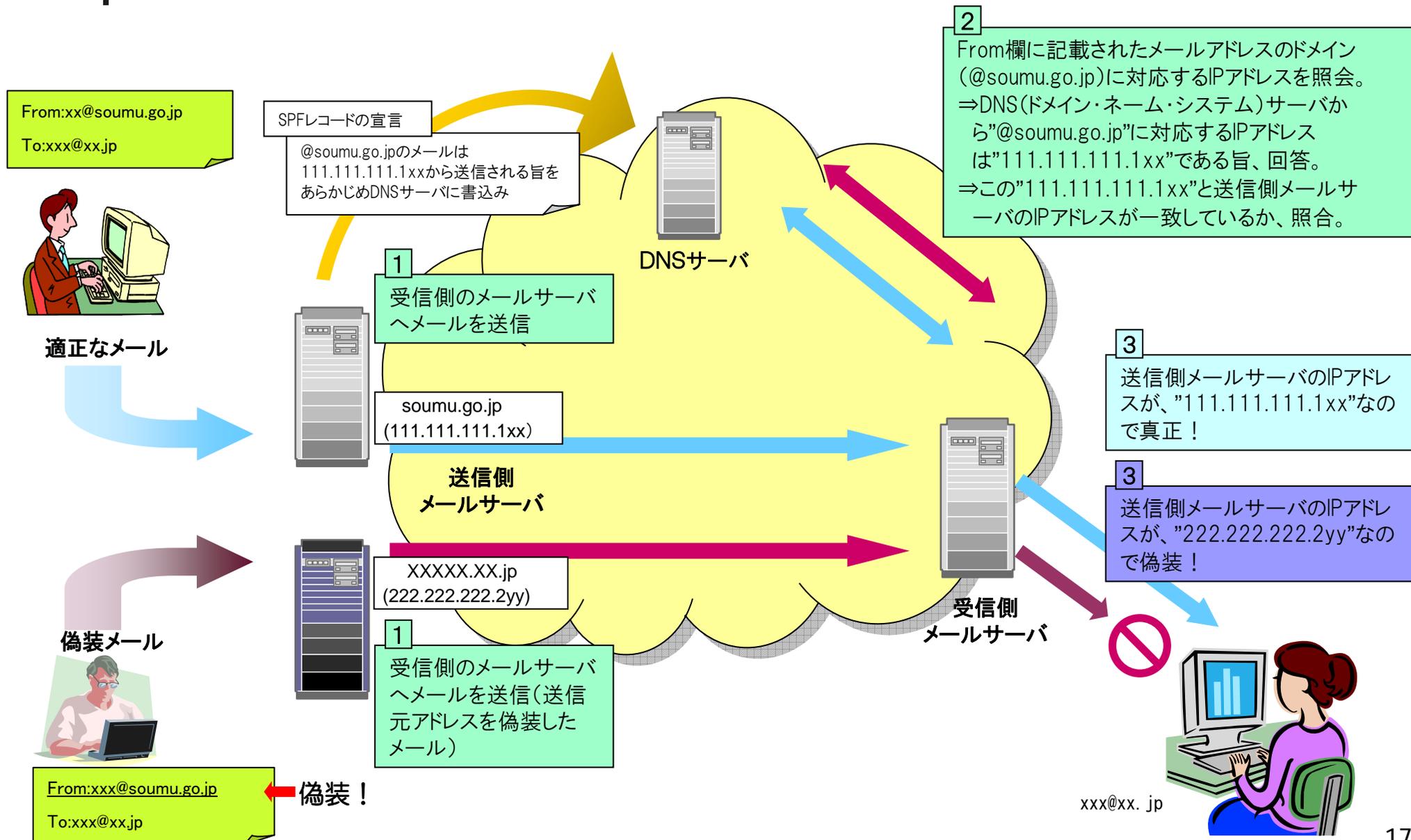


# 「ドメイン」とは

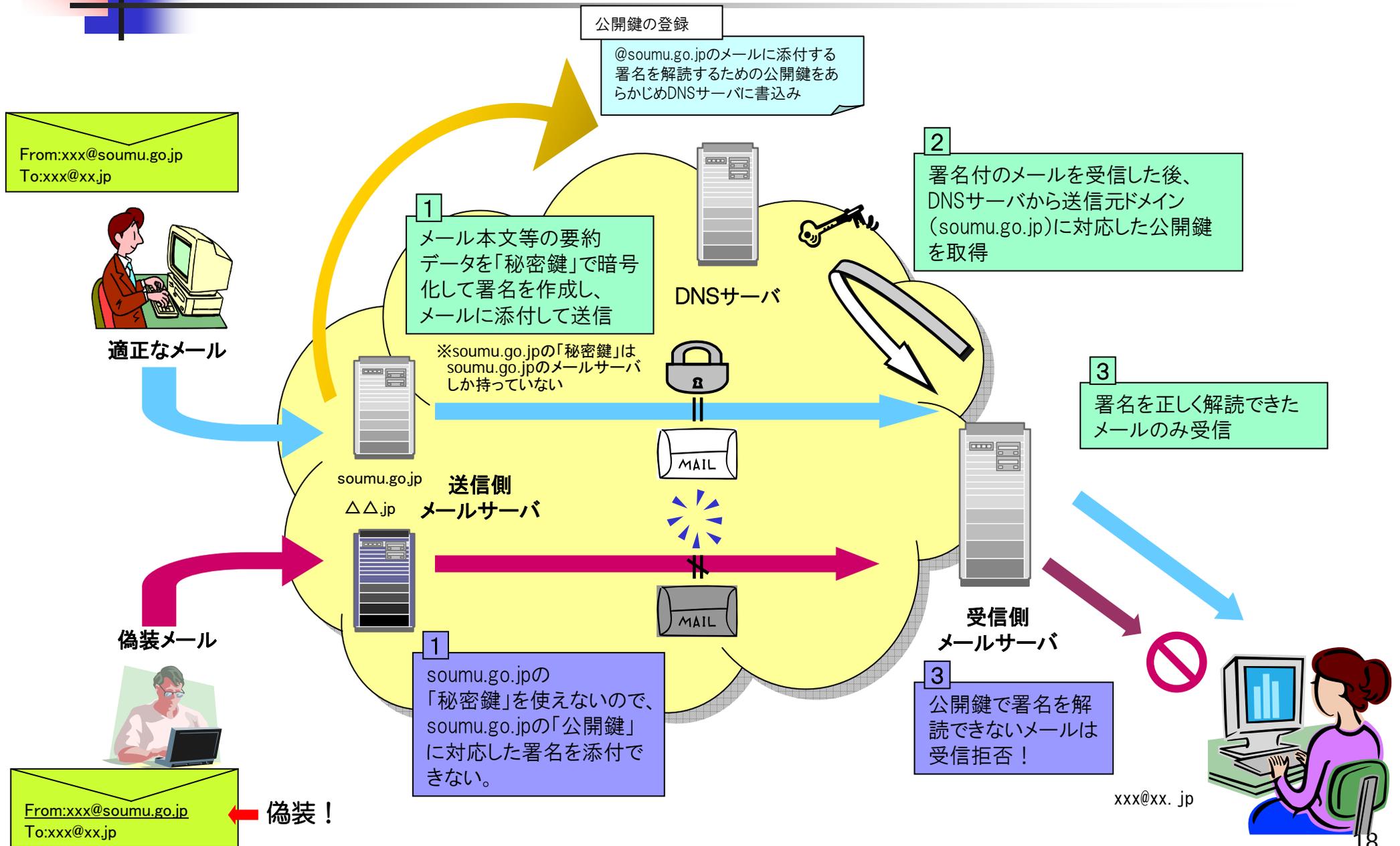
「ドメイン」とは、プロバイダ、会社など「ひとまとまりのネットワーク」を指す言葉で、インターネット上の住所のようなもの。

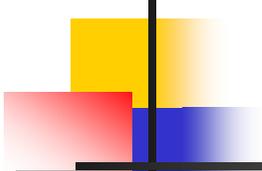
メールアドレスは、「ユーザ名@ドメイン名」という形になっており、例えば「abc-xyz99@xx.ne.jp」といったアドレスの場合、「xx.ne.jp」の部分がドメインとなる。

# SPF/Sender IDの概要



# Domain Keys (DKIM) の概要





# 「25番ポートブロック」について

## 1. 背景

迷惑メールの送信者は、契約しているISPが提供するメールサーバを利用して大量にメールを送信すると回線停止等の措置を講じられるため、自分のパソコンをメールサーバ代わりにするなどして、ISPが提供するメールサーバを回避することが多くなっている。

## 2. 概要

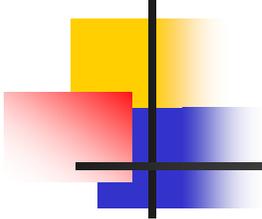
ISPが、自社の提供するメールサーバを経由しないメールをブロックする措置

## 3. 我が国における導入状況

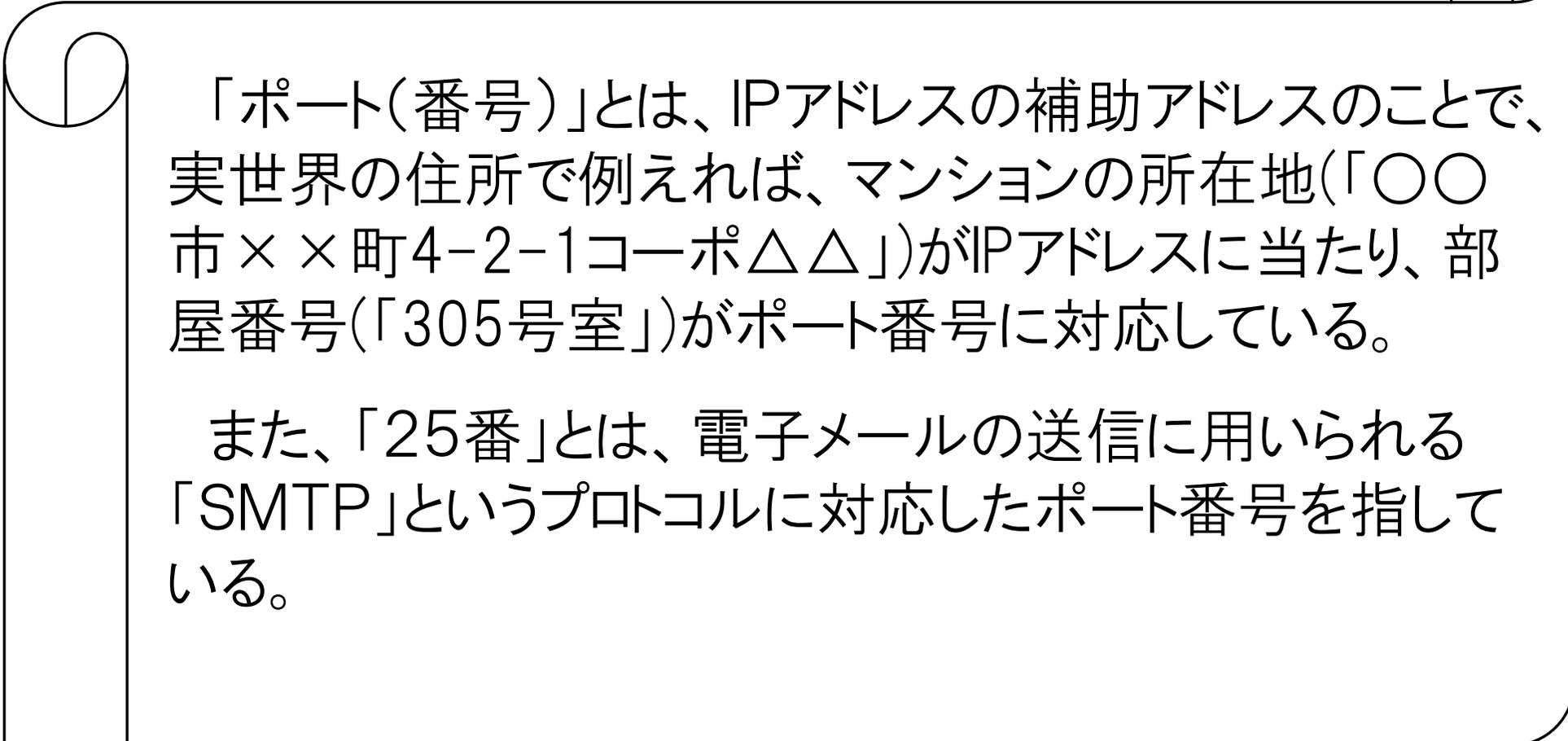
この措置は、ウイルスなどに感染した結果、迷惑メール送信などに悪用されてしまう「ゾンビPC」(注)による大量のメール送信への対策としても有効とされており、国内においても複数のISPによって導入が始まっている。

注：AOL社によると、迷惑メールの75%以上がゾンビPCから発信

- ・WAKWAK(2005年3月導入開始)、SANNET(2005年3月発表)、Nifty(2006年2月導入開始)、So-net(2006年5月開始予定)、NTT-PC(2006年6月開始予定)等  
⇒全てのメールについて実施
- ・ぷらら(2005年2月導入開始)、hi-ho(2005年9月導入開始)、IIJ(2005年9月発表)、NTT-PC(2005年10月導入開始)、KDDI(DION)(2005年11月導入開始)、SPACE TOWN(SHARP)(2005年11月導入開始)、OCN(2005年11月発表)、ZAQ(2005年12月導入開始)、DTI(2006年2月導入開始)等  
⇒携帯電話アドレスあてのメールについて実施(正規ユーザに配慮)



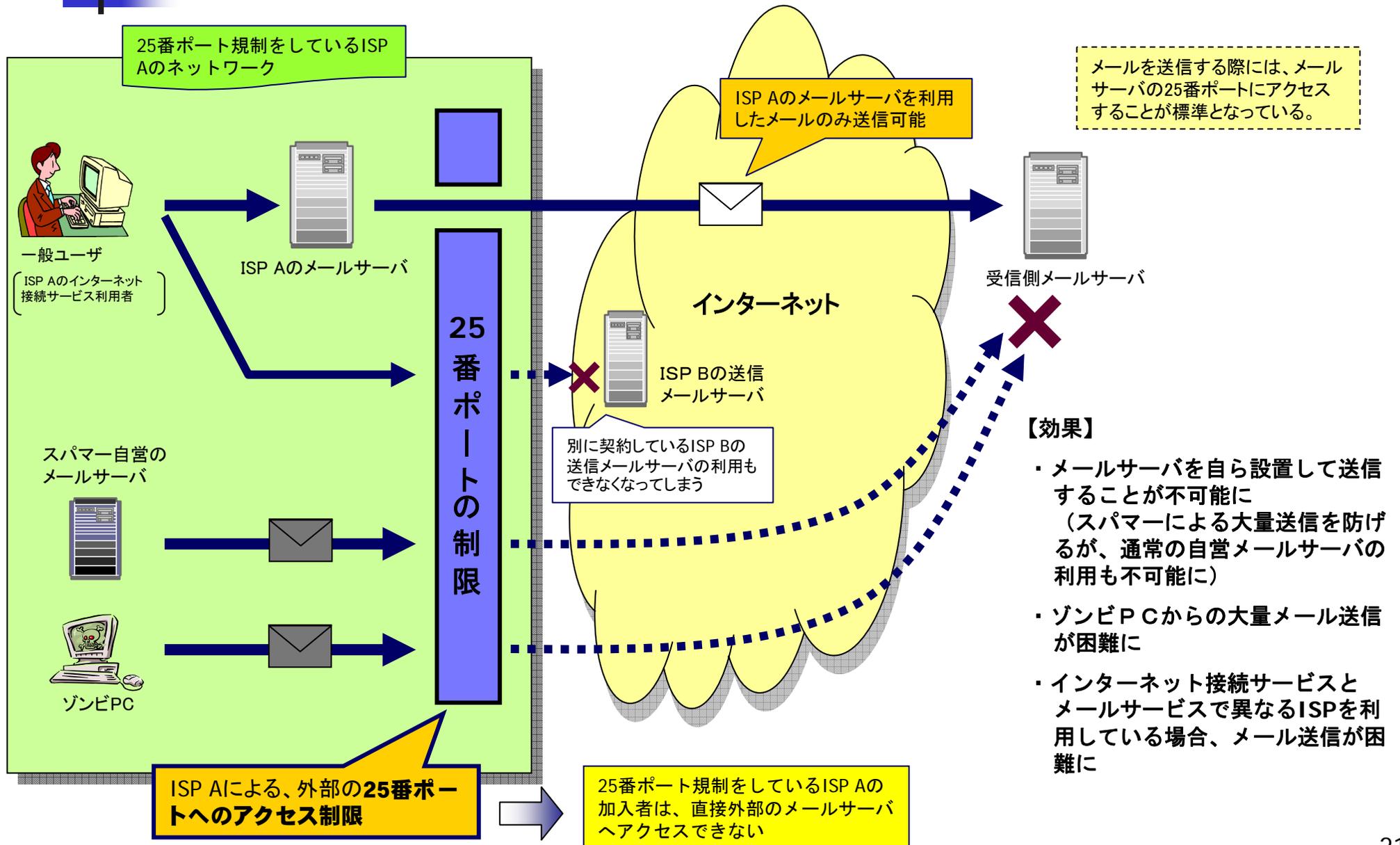
# 「ポート」とは



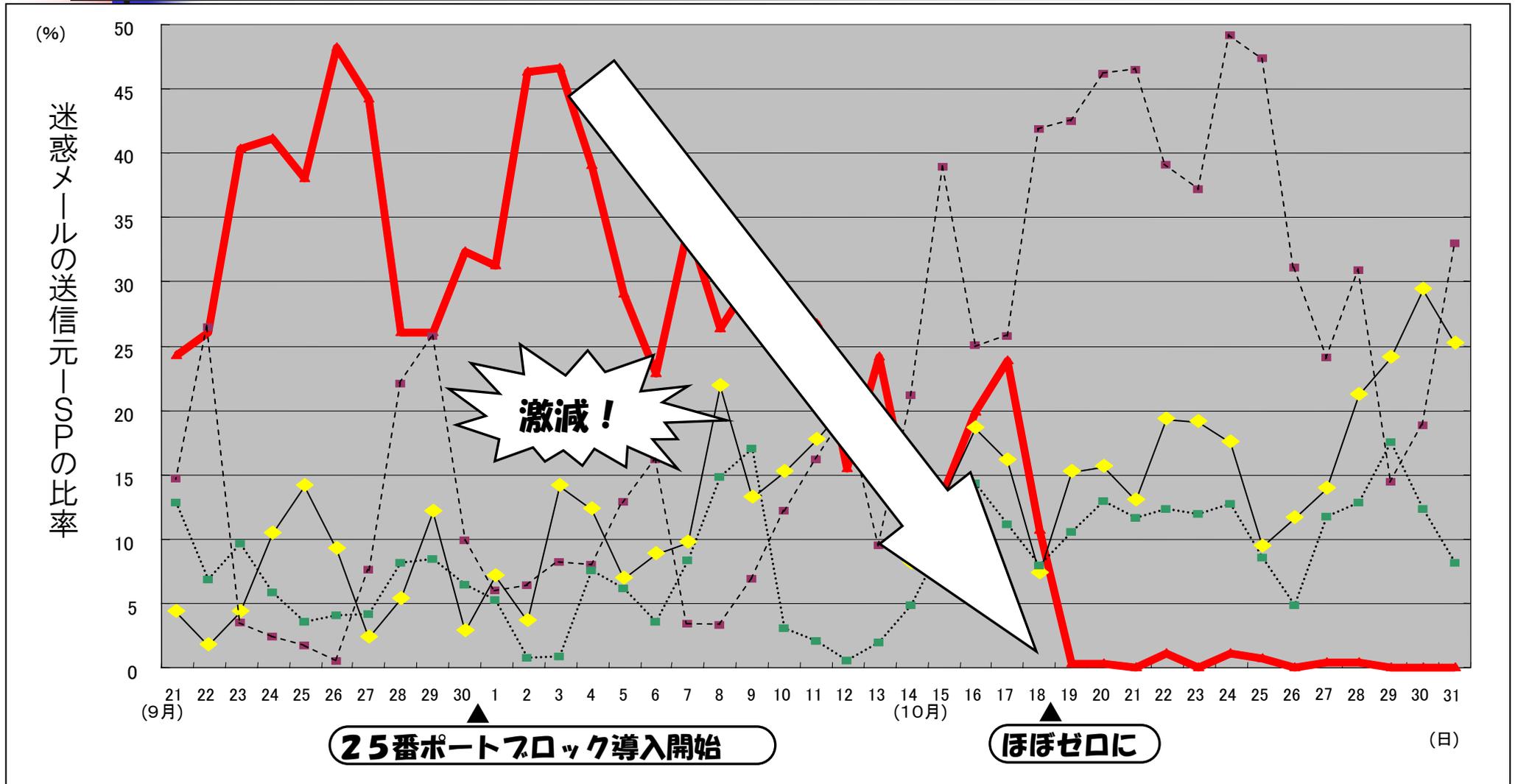
「ポート(番号)」とは、IPアドレスの補助アドレスのことで、実世界の住所で例えれば、マンションの所在地(「〇〇市××町4-2-1コーポ△△」)がIPアドレスに当たり、部屋番号(「305号室」)がポート番号に対応している。

また、「25番」とは、電子メールの送信に用いられる「SMTP」というプロトコルに対応したポート番号を指している。

# 25番ポートブロックの概要



# 「25番ポートブロック」の効果（A社のケース）



(注) (財)日本データ通信協会において、同協会あてに情報提供のあった携帯電話あての迷惑メール(9月21日から10月31日までに受信された約1.3万通)の送信元ISPをヘッダ情報から分析。

