

利用者視点を踏まえたICTサービスに係る諸問題に関する研究会  
迷惑メールの対応の在り方に関する検討WG(第2回会合)

資料5

# ISPから見た迷惑メールの現状と取組状況

2010年10月21日  
社団法人日本インターネットプロバイダー協会  
立石 聡明

1. **ISPから見た迷惑メールの状況**
2. **迷惑メールに対するISPの取組**
3. **ISPから見た課題の変化**
4. **大量のメール送信者に対する要望**

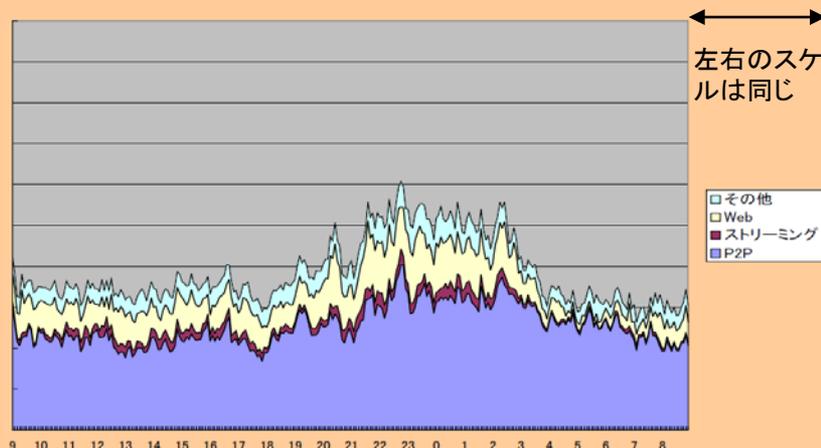
- ・ **迷惑メールの量、割合は相変わらず増加傾向だが、急増といえる状況ではない。(当WG第1回資料2 P4)**
- ・ **しかし、これに対応するメール受信設備(サーバー等)などは増強が必要で、ISPの投資負担となっている。**
- ・ **送信面については、国内での対策の徹底(法規制の強化やOP25Bなど)により、海外発がほとんどとなった。(当WG第1回資料2 P5)**
- ・ **受信サーバー等の設備の負担は大きい一方で、ISPバックボーンのトラヒックでいうと、P2Pや動画共有サービスなどに比べ、メールが占める割合はそれ程多くない。(次頁参考資料参照)**

# (参考)メールのトラフィックが占める帯域(例)

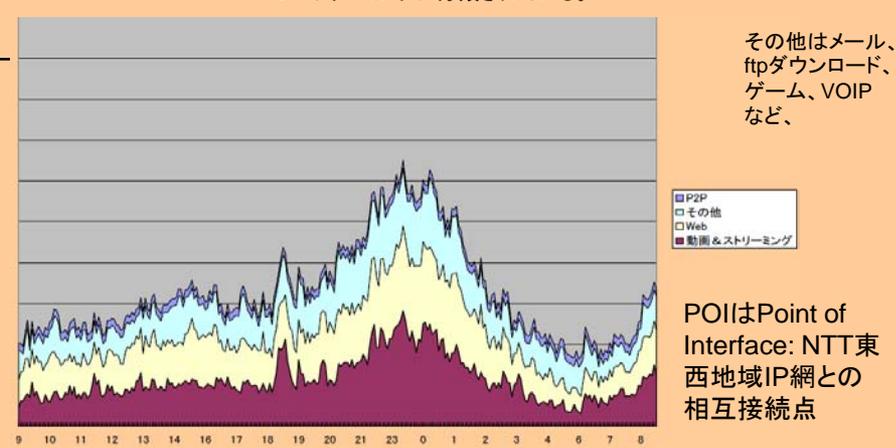
「インターネット政策懇談会」(第5回) 平成20年6月27日  
資料5-2 社団法人日本インターネットプロバイダー協会 説明資料より

## ある大手ISPによる調査 (下りトラフィック)\*

\*(注)ISPからユーザにむけてのトラフィック  
データはあるISPがNTT地域IP網に接続するある県のPOIに設置  
した帯域制御装置で取得。  
フラッシュ動画は2005年はWebに含まれているが、2008年は動画  
&ストリーミングに分類されている。



2005年(P2P帯域制御前)



2008年(P2P帯域制御後)

2007年～ 個人による動画の共有サービスの利用が急増

### (1) 技術的措置の導入

OP25B、通数制限、送信ドメイン認証

### (2) フィルタリングサービスの提供

### (3) (ISP会員による送信の場合) 送信者への警告、契約解除

### (4) 利用者に対する啓発活動

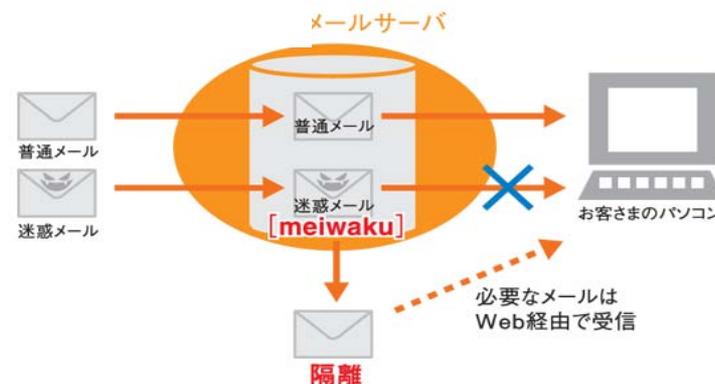
# (1) 技術的措置の導入

- ・ OP25B（詳細は当WG第1回資料2 P22参照）
  - － ほとんどのISPがOP25Bを採用することで日本発の迷惑メールを激減させる効果があった。
  - － OP25B連絡会 JAIPAは日本データ通信協会、レンタルサーバー・オルグと共同し、2007年にOP25B連絡会を結成し、企業のメール管理者に対し対策の周知を促進する活動により、ISPによるOP25Bの円滑な導入を推進した。
- ・ 通数制限
  - － OP25Bの実施により、認証された方法で大量にメールを送ることを抑止するため、多くのISPでは1アカウントから一定時間内に送信できるメールの通数に一定の制限を課している。（通常の利用には問題がない範囲）
- ・ 送信ドメイン認証（詳細は当WG第1回資料2 P23参照）
  - － 送信側：SPFについては相当程度普及している。今後DKIMの普及が課題となると考えられる。
  - － 受信側：認証結果のラベリングまでは正当業務行為として位置づけられているが、普及はまだこれから。
  - － 送信側、受信側とも相当程度普及し、ほとんどのメールにおいて一般的となった段階においては、効果や影響を検証し、認証結果に基づくフィルタリングについても正当業務行為として位置づけられることを期待したい。

## (2) フィルタリングサービスの提供

- ・ ほとんどのISPでは利用者向けに迷惑メールのフィルタリング(振分け)サービスを提供。
- ・ オプションで利用者の申込が必要。(通信の秘密に関し同意が必要なため)
- ・ 隔離フォルダの提供の有無など、機能により無償のものと有償のものがある。
- ・ 名称はISPにより異なる。
  - ・ 「迷惑メールブロックサービス」
  - ・ 「迷惑メールフォルダー」
  - ・ 「スパムメールブロック」
  - ・ 「迷惑メール振分けサービス」
  - ・ 「迷惑メールフィルター」など

フィルタリングサービスの例



### (3) 送信者への対応

- ・ **ISPは、自社のIPアドレス(個人法人の会員や固定IPアドレス契約者に割当)から迷惑メールが送られたという申告が国内や海外から寄せられた時に対応を実施している。**
  - 一般利用者(ISPのホームページの申告窓口やabuseアドレス経由)
  - 日本データ通信協会迷惑メール相談センターや日本産業協会から
  - 海外の迷惑メール対策機関、団体から
- ・ **このような場合、ISPは送信者を特定し、警告を通知。警告にも関わらず再度送信した場合は、契約を解除している。(悪質な場合は最初から警告なしに契約解除することもある)**

**ただし、ISPが受信者などから受ける苦情は最近は余り多くない状況。**

ある大手ISPの例ではspamメールの通報件数は月間数十件程度。権利侵害や違法情報など通報全体の中では数パーセントを占めるにすぎない。

# (4) 利用者に対する啓発活動(周知事例)

## ISP各社では利用者に対し、迷惑メールへの対処法などを案内 例

**迷惑メール対策@nifty**

日頃、迷惑メールでお困りのあなた。正しい知識を身につけて快適にメールを楽しもう！

**迷惑メール対策@nifty**

- 迷惑メール対策@nifty トップ
- 迷惑メールの基礎知識
- @niftyの迷惑メール対策サービス
- 迷惑メール別対処法
  - ダイレクトメール
  - なりすまし・偽装メール
  - 架空請求(詐欺)メール
  - チェーンメール・デマメール
  - ウイルスメール
  - フィッシング
- 迷惑メール対策チェック
- 迷惑メール対処テクニック
- 迷惑メールFAQ (よくあるご質問)
- @niftyの取り組み
- 関連リンク集
- 迷惑メール対策@nifty サイトマップ

**迷惑メール対策サービス**

@niftyの迷惑メール対策サービスなら、効率的に迷惑メールをシャットアウトできます。  
→ クリックするだけで設定完了  
→ 受信しにくいメールを自分で設定

**迷惑メールの基礎知識**

迷惑メール対策の第一歩  
なぜ、迷惑メールは届くの？

**迷惑メール最新情報**

2009/04/03  
フィッシングメールにご注意ください

**@niftyの取り組み**

安心、安全なインターネットライフのために  
@niftyではさまざまな迷惑メール対策を実施しています。  
「25番ポートブロック(Outbound Port25 Blocking)」の実施

**迷惑メールFAQ**

よくあるご質問はこちらから

**迷惑メール対策チェック**

簡単な10の質問に答えるだけで、迷惑メール対策度が診断できます。あなたの迷惑メール対策は万全かな？

**迷惑メール対策チェック 診断へGo**

**迷惑メール対処テクニック**

あなたの疑問を解決する対処テクニックをご紹介します。

- 大量に届く迷惑メール、見ないようにはできないの？
- プロバイダーでは迷惑メールに対応してくれないの？
- 自分のアドレスから迷惑メールが届いた、どうして？
- HTMLメールは危険っていうけど、何が危険なの？

**OCN 迷惑メール対策**

→セキュリティ対策ページへ

**迷惑メール対策サービス**

大量の迷惑メールは不快になるだけでなく、詐欺の被害に陥る危険性もあります。OCNの迷惑メール対策サービスを活用して、安心のメール生活をおくりましょう。

**迷惑メールブロックサービス**

迷惑メール、詐欺メールを届けません！  
メールサーバ上で受信したメールの迷惑メール判定を行い、迷惑メールの隔離(保存や件名へ[meiwaku])の付与を行います。

**迷惑メール自動判定 (Mail ON)**

サーバが迷惑メールを自動で判定!!  
メールサーバ上でメールの自動判定を行い、迷惑と判定されたメールの件名に[meiwaku]の表示を追加します。  
メールを受信するパソコンのメールソフトで、フィルタリングを行えば、迷惑メールを隔離することもできます。

**メール自動削除設定 (Mail ON)**

サーバでお客様指定の条件でメール削除!!  
特定の送信元メールアドレスや件名を登録することにより、お客様のメールボックスに到着前に自動でそのメールを削除します。

**もっと知りたい! 迷惑メールの手法と対処方法**

迷惑メールにはさまざまなタイプがあります。それぞれの特徴を学び、正しく対処しましょう。

- CASE 1 宣伝メール** 出会い系のメールにご注意
- CASE 2 架空請求メール** 料金請求にもあわない
- CASE 3 ウイルスメール** 不審な添付ファイルは開かない
- CASE 4 フィッシングメール** ID・パスワードの入力は慎重に
- CASE 5 オークション詐欺メール** おいしい話には気をつけましょう

**迷惑メール対策トップ**

**迷惑メール対策サービス**

- 迷惑メールブロックサービス
- 迷惑メール自動判定
- メール自動削除設定

**迷惑メール対処方法**

- 宣伝メール
- 架空請求メール
- ウイルスメール
- フィッシングメール
- オークション詐欺メール

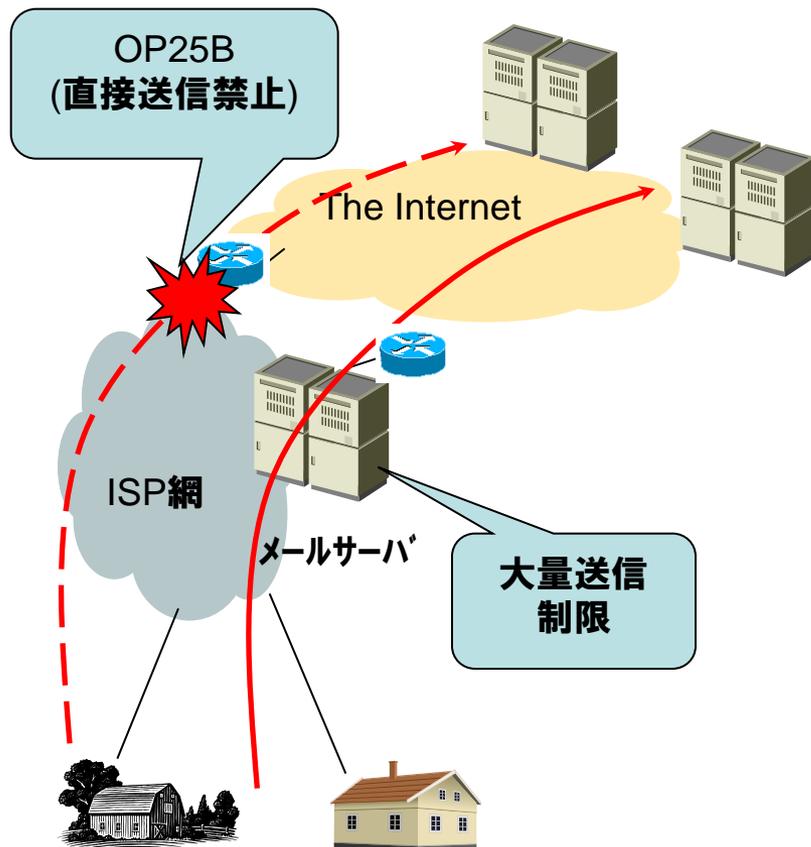
**OCNの取り組み**

- OP25B (迷惑メール送信規制)
- IP25B (迷惑メール着信規制)
- サブミッションポート587提供
- 迷惑メールに対するOCNの対応について
- 送信ドメイン認証(SPF)の対応

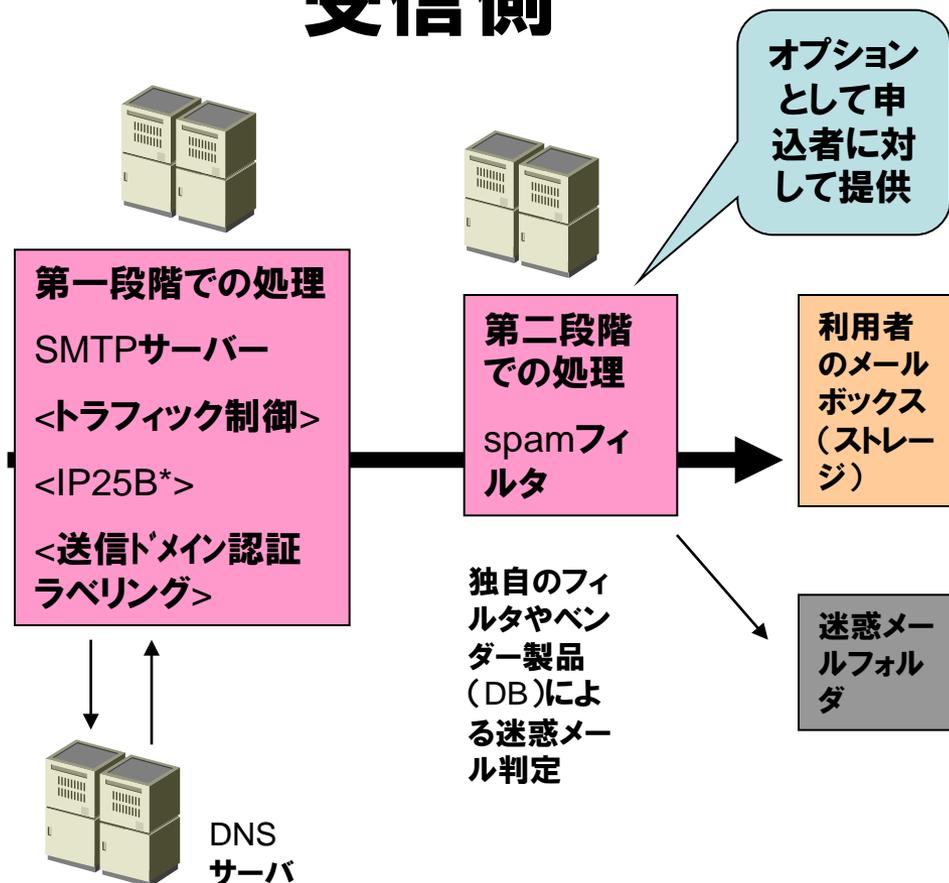
**関連情報**

- あんしんWeb セキュリティを学ぶ
- インターネット上の脅威
- セキュリティ対策の基礎
- ホントにあった怖い話
- 篠田佳奈のHow To セキュリティ
- セキュリティトレンド定点観測
- セキュリティ診断 あなたのセキュリティ度

## 送信側



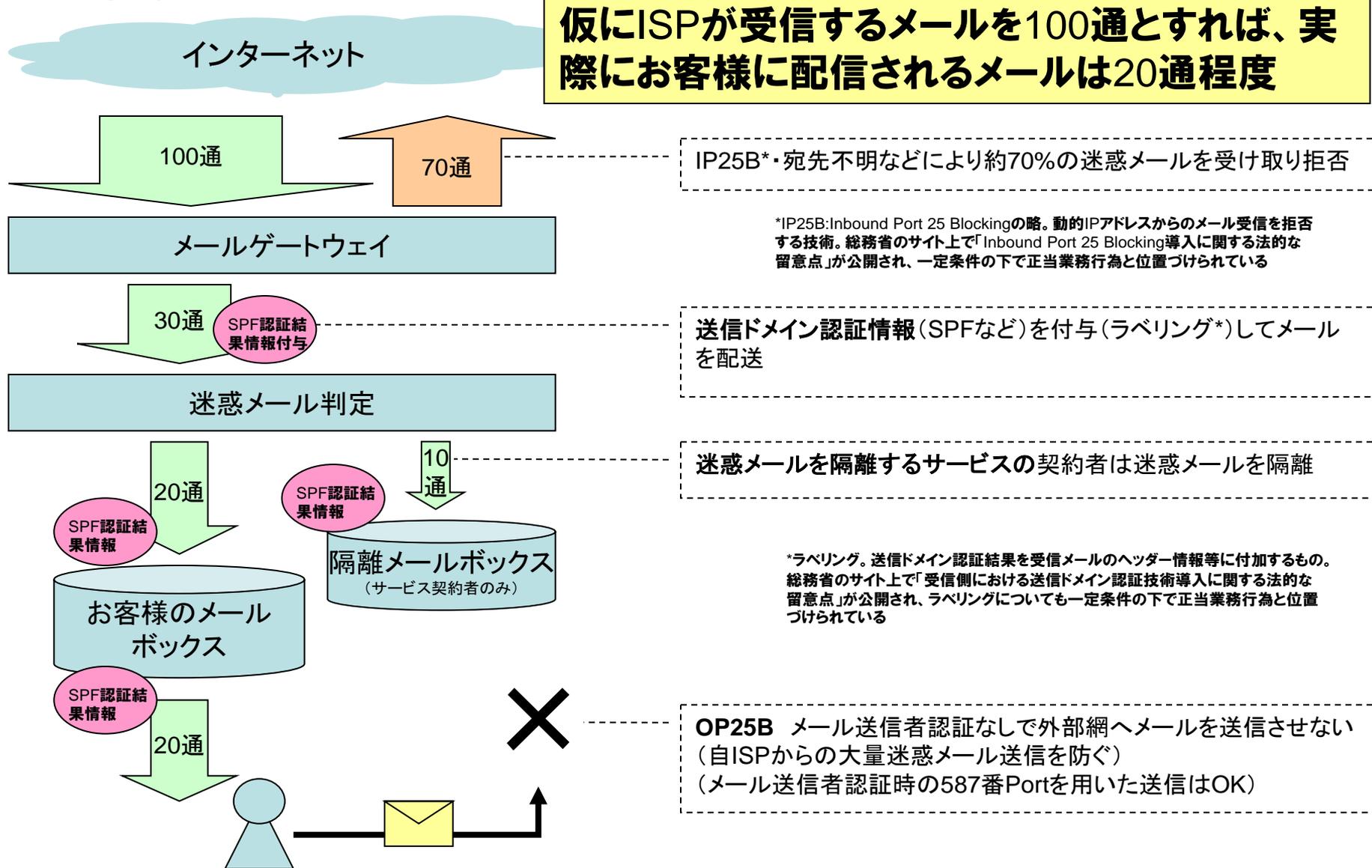
## 受信側



\*IP25B: Inbound Port 25 Blockingの略。動的IPアドレスからのメール受信を拒否する技術。総務省のサイト上で「Inbound Port 25 Blocking導入に関する法的な留意点」が公開され、一定条件の下で正当業務行為と位置づけられている

# ISPにおける迷惑メール対策の実態

## ■ISPの対応例(モデル)



### 3. ISPから見た課題の変化

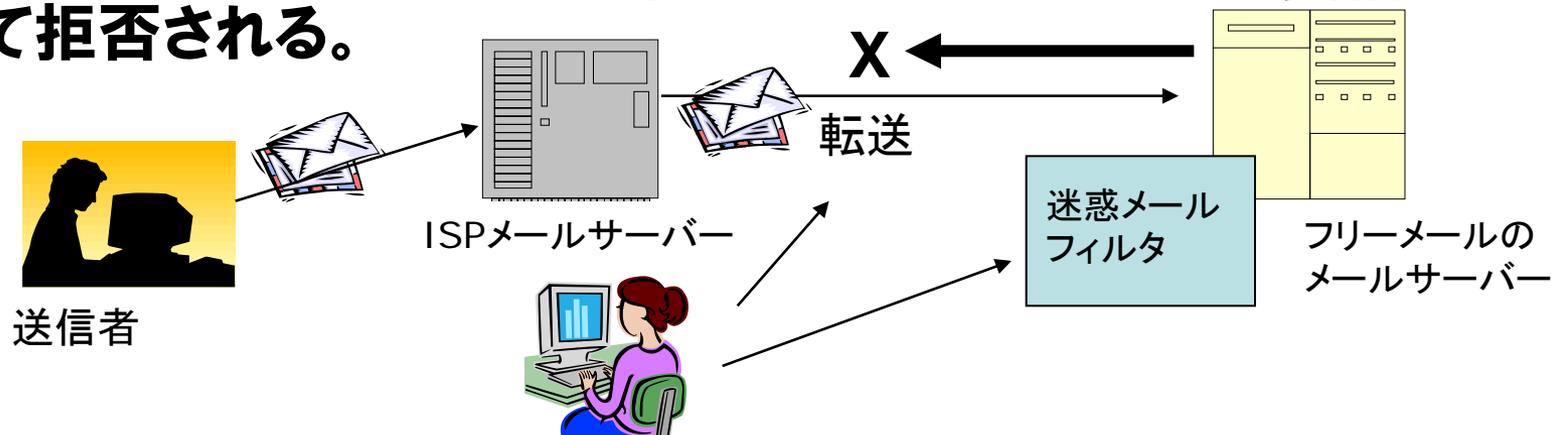
- ・ **オプトインされたメールは迷惑メールとは呼べないが、大量送信されるオプトインメールもISPにとっては設備面で課題となっている。※**
- ・ **利用者側から見ても、意識せずにオプトインした(デフォルトのオプトインのチェックを外し忘れた)メールが大量に届くのは迷惑な状況と思われる。**
- ・ **メールを取り巻くセキュリティ環境に変化の傾向 (例)単なる広告宣伝ではなく、リンク先をクリックすることでマルウェア(ウイルス)感染を狙うなど、セキュリティ上の脅威となるメールも増大している。※2**

※通信の秘密の関係でISPがメールの中身を見る事はできないので、大量送信されるメールの内容は不明。しかしあるISPの例では、メールマガジン上位5社からのメールがISPのメール全体の約12%を占めたという報告がされている。

※2 2010年10月5日 独立行政法人情報処理推進機構(IPA) セキュリティセンター(IPA/ISEC) コンピュータウイルス・不正アクセスの届出状況[9月分および第3四半期]について

### 3. ISPから見た課題の変化(続)

- 迷惑メールの振分けに利用するため、フリーメールのアドレスにメールを転送する使い方があり、しかしこれを大勢の人が行なうと、フリーメールは転送元メールサーバーを迷惑メール送信元としてブラックリストに登録し、そこからのメールの受信がすべて拒否される。



- 迷惑メール発信元ブラックリストの利用で、発信元IPアドレスに近いIPアドレスも巻き添えでブロックされる事例も発生。
- 特定送信者によりISPから携帯事業者あてのメールで宛先不明が多いと携帯事業者から受信拒否され、ISPから携帯事業者宛のメール全体の遅延が発生することもある。

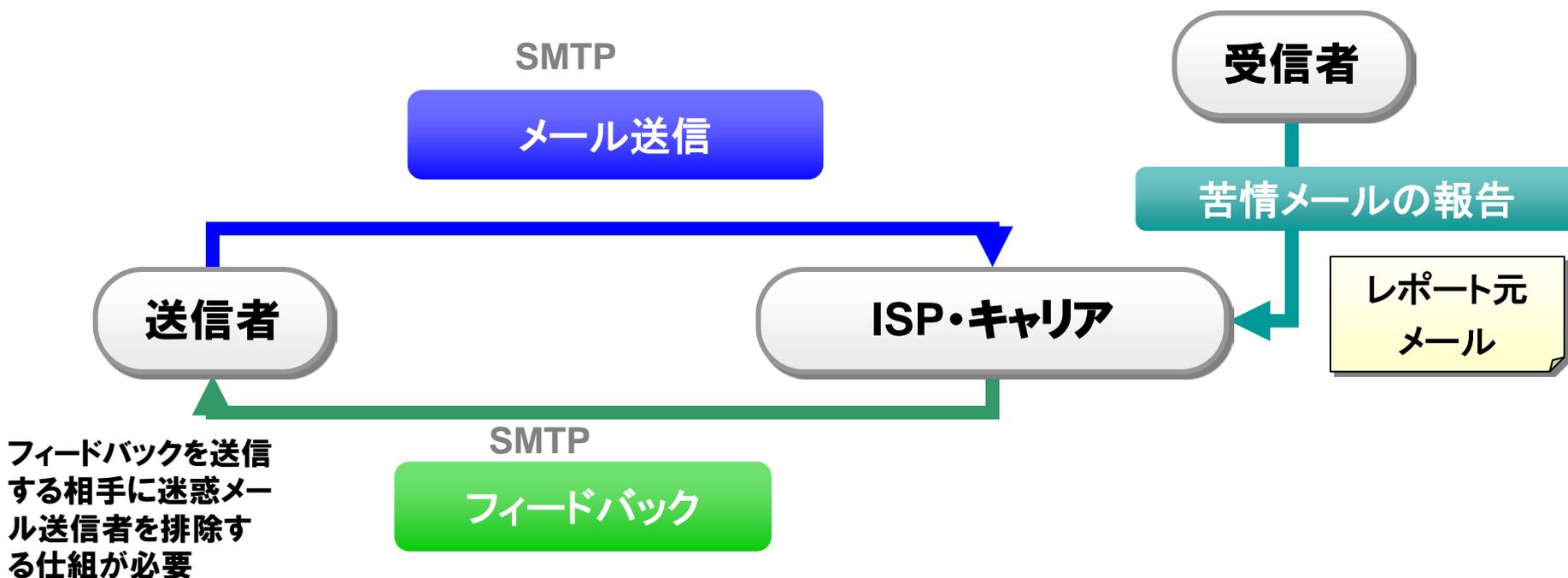
## 4. 大量メール送信者への要望

- ・ 大量にメールを送信する場合は、受信側メールサーバーの負荷を考慮し、時間帯や送信ピッチなどについて配慮してほしい。
- ・ 利用者が実際には迷惑メールとして振り分けているオプトインメールも多いと思われる。
- ・ ISPが受信者の委託を受け、送信者に対するオプトアウトを代行するフィードバックループ(FBL:次頁参照)という仕組みが米国では既に試行提供されている。\*
- ・ FBLの導入により、送信者、受信者、ISPともにメリットがあると考えられるが、導入には法制度上の問題の確認や関係者全体の合意形成が必要。

\*googleでは一部ドメインについて List-unsubscribe機能を導入、不要メルマガ解除システム(Gmail Auto-unsubscribe Search)機能を提供  
マイクロソフトでは Junk E-mail Reporting Programとして登録解除リンク提供  
Yahoo.comもComplaint feedback loopをテスト中、AOLなども同じ規格を利用

# FBL(FeedBack Loop)とは

- ISP・キャリアが、利用者からの委託を受け、メール送信者への苦情を代行しフィードバックする仕組み。Complaint feedback loop (CFL) とも呼ばれる。



インターネットの国際機関であるIETFにおいて、国際規格として提案されている。