資料6

迷惑メールに係る対応方策の検討について
（論点整理（案）（制度面以外））

平成２３年１月２５日

事　　務　　局

目　次

3　電気通信事業者等による自主的な取組み

現状

- 電気通信事業者による自主的な取組として、契約約款に基づく利用停止等の措置を実施
- 利用停止措置を受けた契約者の情報を事業者間で交換し、いわゆる「渡り」を防止

論点

○　約款に基づく利用停止等の措置等が行われているが、電気通信事業者が新たに取り得る自主的な取組みとして、どのようなものがあるか。

○　携帯電話各社で検討中のSMSの相互接続に起因して迷惑メールが増加することはないか。

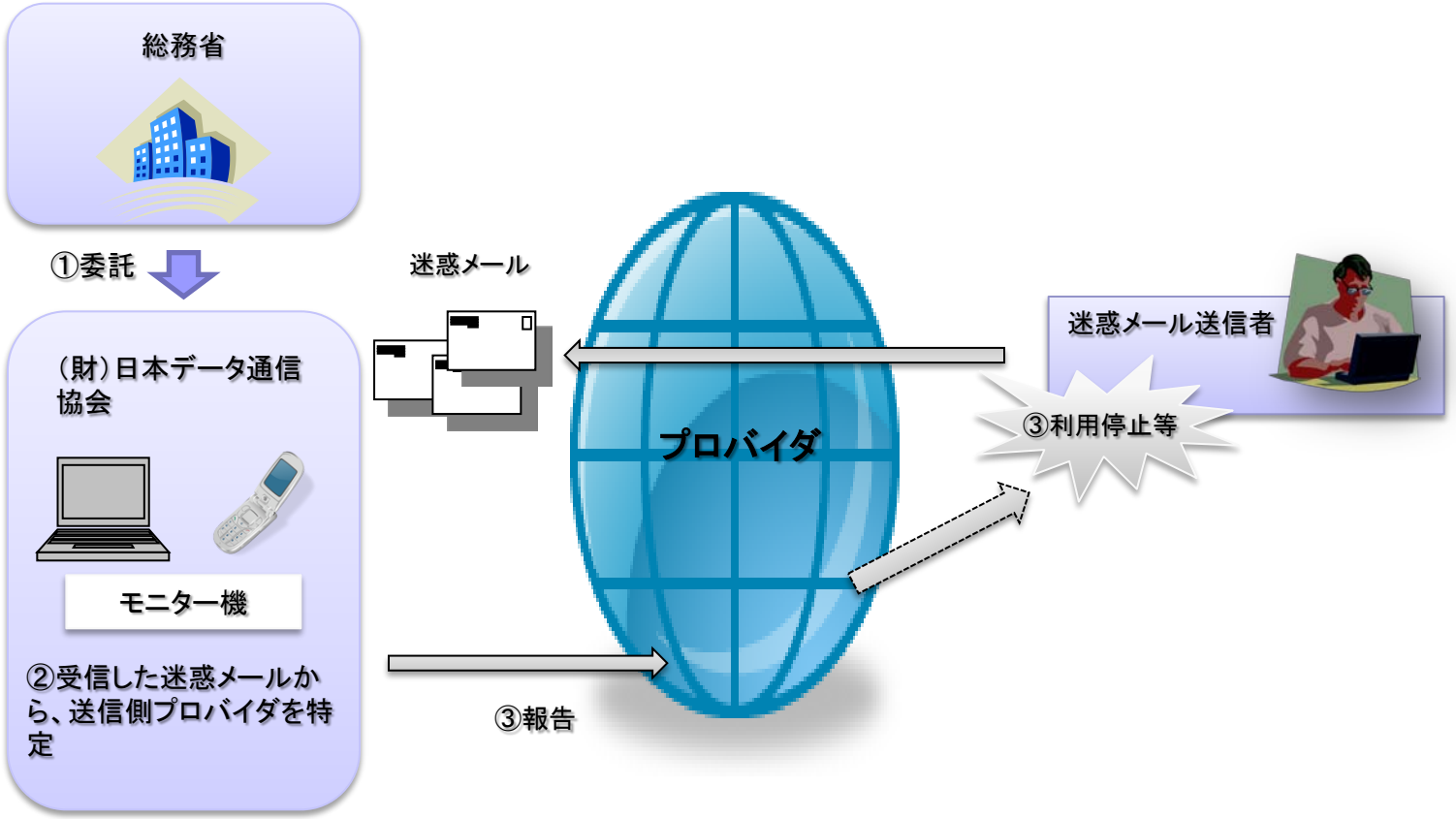
※　「迷惑メール追放支援措置プロジェクト」に伴うISPへの対応依頼：10,951件（958社、21年度実績）

※　「（利用停止措置を受けた契約者の）情報交換の議論を始める際に問題となっていたのは携帯電話宛の迷惑メールであった。また、携帯電話事業者の数も少なかったこともあり、携帯から始めたという経緯がある」【第2回WG構成員発言】

※　NTTドコモ、ソフトバンクモバイル、イー・モバイル、KDDI及び沖縄セルラー電話の5社は、現在各社で提供している3G携帯電話におけるSMSの事業者間接続の実現に向けた検討を進めていく上での基本事項に関して昨年9月に合意した。TCA「迷惑メール送信者情報交換に連絡部会」において、前記のSMS相互接続後の迷惑メール（SMS）対策について電気通信事業法その他の法令との関係を踏まえつつ検討中【第2回WG　KDDI資料】

迷惑メール追放支援プロジェクト

総務省は、2005年から、プロバイダ及び携帯電話事業者等と連携して、迷惑メール送信回線の利用停止措置等の円滑な実施を促す「迷惑メール追放支援プロジェクト」を実施。



4　広告関係事業者等による自主的な取組み (a)広告関係事業者による取組み

現状

・　広告関係事業者（媒体社、広告会社等）の取組みとして、電子メール広告に関する業界ガイドライン、自主基準等を定め、法の遵守に努めてきている。

論点

○　広告関係事業者の取組みとして、さらにどのようなことが期待されるか。

※　「インターネット広告掲載基準ガイドライン」「メール広告の運用ガイドライン」「メール広告のパーミッション取得のためのガイドライン」等の業界ガイドラインを作成し、会員各社に対し、準拠を強く推奨。また、会員各社では、業界ガイドラインに沿った自主基準を策定している。

※　引き続き、法の周知啓発に努めていくとともに、電気通信事業者と広告関係事業者が連携して、迷惑メール対策を行っていくことが重要ではないか。

広告関係事業者の迷惑メール対策

	迷惑メール対策
ガイドラインによる対応	■「インターネット広告掲載基準ガイドライン」の策定（2000年制定） ・ガイドラインにおいて、「日本国憲法及び法律に反するような類の広告は掲載しない」等を記載。 [一般社団法人インターネット広告推進協議会]
	■「メール広告の運用ガイドライン」（2001年制定） ・ガイドラインにおいて、「配信許諾を徹底する」、「責任の所在を明確にする」、「ユーザーからの配信拒否に対して即時対応を行う」、「迷惑行為を防止する」等を記載。 [一般社団法人インターネット広告推進協議会]
	■「メール広告のパーミッション取得のためのガイドライン」（2004年制定） ・ガイドラインにおいて、「事前に消費者に利用目的を明示し、個人情報がどのように取り扱われるかを理解させ、提供の有無を判断する機会を与え、パーミッション取得をしなければならない」「配信にあたっては、広告媒体者名・サービス名称など配信元の所在を明らかにするべきである」等を記載。 [一般社団法人インターネット広告推進協議会]
団体としての法遵守の宣言	■「電子メール広告の健全な発展のために　～広告に関わる者として、迷惑行為、違法行為と明確な一線を～」を公表（2003年） ・広告に関わる媒体社、広告会社等の活動がユーザーのクレームの対象とならないよう、法の内容を正しく理解し、厳しく自らを律していくことを宣言　[一般社団法人インターネット広告推進協議会]
説明会による法律の理解促進	■「特定電子メール法改正」に伴う会員社への説明会の開催（2008年度）[JIAA] ■「特定電子メール法改正」に伴う会員社への説明会の開催（2008年度） [（社）日本アドバタイザーズ協会・（社）日本広告業協会]

4 広告関係事業者等による自主的な取組み(b)メール配信事業者による取組み

現状

・ メール配信事業者の取組みとして、オプトイン・オプトアウト機能の提供、配信エラーのメンテナンス機能の提供、送信ドメイン認証技術への対応等を行ってきている。

論点

・ メール配信事業者の取組みとして、さらに、どのようなことが期待されるか。

※ メール配信事業者の取組みとして、契約時の企業情報確認と利用規約による禁止行為の規定、オプトイン・オプトアウト情報を管理する機能の提供、配信エラー情報のデータベースへの反映機能、SPFレコードの公開、DKIM署名付きメール送信機能の提供等を行っている。【第3回WG エイケア・システムズ(株)、(株)パイプドビッツ資料】

※ 特電法改正セミナー、送信ドメイン認証セミナー等の啓蒙活動を実施。【第3回WG エイケア・システムズ(株)資料】

※「問い合わせ窓口を設けているが、一般の方がそこが窓口だと認知できるようにはなっていないので、そこをどうアピールするかが課題だと思っている。」【第3回WGエイケア・システムズ(株)発言】

※「前回の改正でオプトイン規制が導入されたことにより、オプトアウトが堂々とできるようになったと思ったら、なかなかそうはなっていない現実がある。それは送信者をどう信頼するかという部分だと思うので、正しいメールを配信されているメール配信事業者も一緒に考えて欲しい。」【第3回WG構成員発言】

メール配信事業者の迷惑メール対策

	迷惑メール対策
技術的な対応	■ ダブルオプトイン、オプトアウト機能の標準装備 ［エイケアシステムズ(株)、(株)パイプドビッツ］
	■ エラーメール解析エンジンの提供 （※致命的なエラー（ドメイン不明、ユーザ不明、受信拒否）になったアドレスは自動的に配信対象から除外）［エイケアシステムズ(株)、(株)パイプドビッツ］
	■ 送信ドメイン認証技術の導入［エイケアシステムズ(株)、(株)パイプドビッツ］
	■ Fromアドレス制限（※顧客保有のドメイン以外の使用不可） ［エイケア・システムズ(株)］
	■ 文章の自動差込機能 （※あらかじめテンプレート登録する事により、メール本文の末尾に自動的に追加されることにより、特定電子メール法の表示義務に対応）［エイケア・システムズ(株)］
サービスを不適正に利用されないための対応	■ 約款上で、禁止事項を記載 （※同意のない相手への配信の禁止など特定電子メール法に則した禁止事項の記載、問題がある場合に解約される旨の明記） ［エイケアシステムズ(株)、(株)パイプドビッツ］
	■ 契約前の調査 （※メール配信の目的、お客様事業内容、Fromに使用するドメインの所有者などの確認）［エイケアシステムズ(株)、(株)パイプドビッツ］
	■ 運用中のモニタリング（※配信されたメール本文のキーワード検査） ［エイケア・システムズ(株)］

4 広告関係事業者等による自主的な取組み (c)アフィリエイト事業者による取組み

現状

・ アフィリエイト事業者による取組みとして、アフィリエイターの審査、メールマガジンでの広告配信許可制の導入、ガイドラインによる禁止行為の規定等の対応を行ってきている。

論点

・ アフィリエイト事業者の取組みとして、さらに、どのようなことが期待されるか。

※ 迷惑アフィリエイター対策への取組みとして、アフィリエイターの審査、クライアント(広告出稿者)との提携承認、提携承認後のサイト変更認識、不正パートナー情報の共同利用、メールマガジンでの広告配信許可制等を行っている。【第3回WG 日本アフィリエイト・サービス協会資料】

※ 法規違反(迷惑メールを含む)に関する広告媒体主、媒体主の審査基準を設け、審査を実施。【第3回WG モバイルアフィリエイト協議会資料】

※ 「広告メールの中にリンクコードがあり、どの提携承認をしたアフィリエイトパートナーに収入があがるのかということが明確になっている。このため、どのアフィリエイトパートナーが迷惑行為をしたのかということの推測はできるが、第三者が悪意をもって、迷惑メールの中に(リンクコードを)仕込んで、送信するという可能性があるので、確定はできないため、違法行為者の特定が困難な場合もある(悪意の者には収入は上がらない)。」【第3回WG 日本アフィリエイト・サービス協会発言】

※ 「広告主に対する審査基準は、モバイルアフィリエイト協議会では作成しておらず、モバイルアフィリエイト協議会加盟各社の審査基準に基づいて審査を実施。」【第3回WG モバイルアフィリエイト協議会発言】

※ 今後、違法迷惑メールへの対応協力、「迷惑メール追放啓発キャンペーン」等によるアフィリエイト・パートナーへの啓発活動の実施を検討。【第3回WG 日本アフィリエイト・サービス協会資料】

※ 今後、迷惑メールWGへの協力・依頼対応、モバイルアフィリエイト事業運用管理体制適合基準への迷惑メールに関する記述追加の検討、迷惑メール防止キャンペーンの企画・実施を検討【第3回WG モバイルアフィリエイト協議会資料】

アフィリエイト団体の迷惑メール対策

	迷惑メール対策
ガイドラインによる対応	■「日本アフィリエイト・サービス協会　アフィリエイト・ガイドライン」で迷惑行為の一類型として、「迷惑メールの配信による自身のサイトへの誘導」を盛り込み、その行為を禁止。［日本アフィリエイト・サービス協会］
	■「モバイルアフィリエイト事業運用管理体制適合基準」で、アフィリエイターの媒体が法規違反となる場合や法規違反を誘引・助長ほう助等する場合は、利用停止する旨の審査基準を加盟社で作成することを盛り込んでいる［モバイルアフィリエイト協議会］
サービスを不適正に利用されないための対応	■ 日本アフィリエイト・サービス協会の加盟社間で、強制退会処分としたアフィリエイターの情報を共有。［日本アフィリエイト・サービス協会］
	■ アフィリエイターの審査（加盟全社で実施）［日本アフィリエイト・サービス協会、モバイルアフィリエイト協議会］
	■ 広告主が認めたアフィリエイターのサイトにのみ出稿させるため、アフィリエイターと広告主との提携の承認制（加盟全社で実施）［日本アフィリエイト・サービス協会］
	■ アフィリエイターによるメールマガジンでの広告配信の許可制（加盟全社で実施）［日本アフィリエイト・サービス協会］

4 広告関係事業者等による自主的な取組み (d)大量送信対応

現状

・ 短期間で大量に広告宣伝メールが送信されること等により、メール受信設備に負荷がかかる。

論点

○ 広告関係事業者から一度に大量に送信される電子メールは、電気通信事業者への設備負荷が大きいことから、どのように考えるべきか。

○ メルマガ等のリスト管理が不十分なことによる問題について、どのように考えるか。

※ 大量にメールを送信する場合は、受信側メールサーバの負荷を考慮し、時間帯や送信ピッチなどについて配慮してほしい。【第2回WG JAIPA資料】

※ 短時間で大量送信するなど過度にメール受信設備に負担をかけるような送信の在り方の是正 → メール本来の仕組みに基づいた運用を【第2回WG JEAG資料】

※ 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【第2回WG JAIPA資料】

※ 自ら申し込んだメールマガジン等について、オプトアウトがしづらいことにより、オプトアウトしたい場合でも、そのまま継続して受信したり、フィルタリングで受信しないような措置をとる場合もある【第2回WG JAIPA資料】

4 広告関係事業者等による自主的な取組み (d)大量送信対応

【不要な電子メールの大量送信対応のための検討の場の設置が必要】

※「まとめている切り口なのだが、広告関係事業者と電気通信事業者というまとまり毎にまとめているのが本当に良いのかというのがわからない。主観的に迷惑だと考えられているようなものもきちんと整理するとメールの通数がかなり減るのだが、メール全体を減らしていくためには、今までの枠組みでの話し合いだけだと上手くいかない。例えば、ここで書かれているJIAAさんは代理店の集まりで配信側であり、アフィリエイトも広告宣伝で配信側である。この枠組みに入ってない人たちもいて、そういう人達はどういう枠組みで今後話をしていくのが良いのかというところをもう1度考え直す必要があるのではないか。」【第4回WG構成員発言】

※ 論点整理案では、民間事業者における自主的取組みについて、(1)電気通信事業者等による自主的な取組み、(2) 広告関係事業者等による自主的な取組み の2つの切り口から検討を行うこととされています。

しかしながら、「不要なメールが大量に流れている」という問題に対処するにあたっては、個々の事業者(団体)の自主的な取組みを促進するという観点だけでなく、広告メールに関わる事業者が広く関係しながら統一的な対応を議論し、実践してゆくことを促進するというという切り口からも、検討すべきではないかと考えます。

具体的な進め方として、新しい場を設けるか、それとも既存の枠組みを活用するか(例えば迷惑メール対策推進協議会を活用する等)は要検討ですが、「関係事業者が広く集まって広告メールに関するベストプラクティスを検討する」場を設けるべきことを、迷惑メールWGにおいて検討いただくべきと考えます。【構成員提出意見】

5 技術的対策 (a)OP25B(Outbound Port 25 Blocking)

現状

・ JEAGによるレコメンデーションの公表等の取組の結果、我が国の主要ISPで導入が進展。
（※中小のISPでは導入していないところもある。）

論点

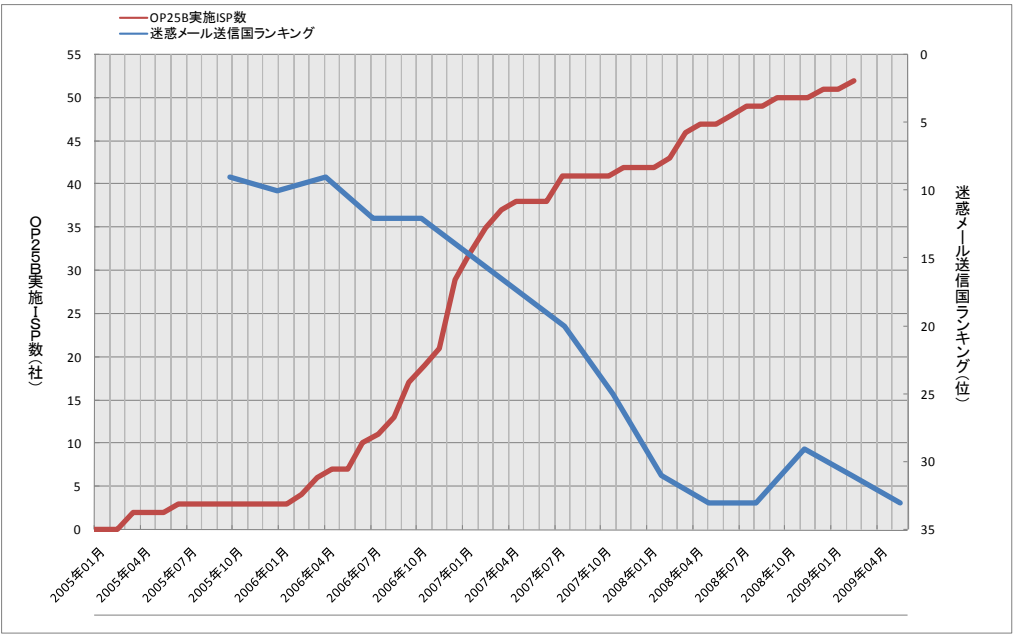
○ 国内ISPでのさらなる導入を図るために、どのような取組をすべきか。

○ OP25Bを導入していても迷惑メールが送信される場合への対応についてどう考えるか。
（例えば、送信者認証をID・パスワードを用いて行っている場合に、ID・パスワードを破られることにより、迷惑メールが送信される。）

※ 日本では、国内のOP25Bの導入が進展するにつれ、日本のスパム送信国ランキングが低下。【第1回WG事務局資料】

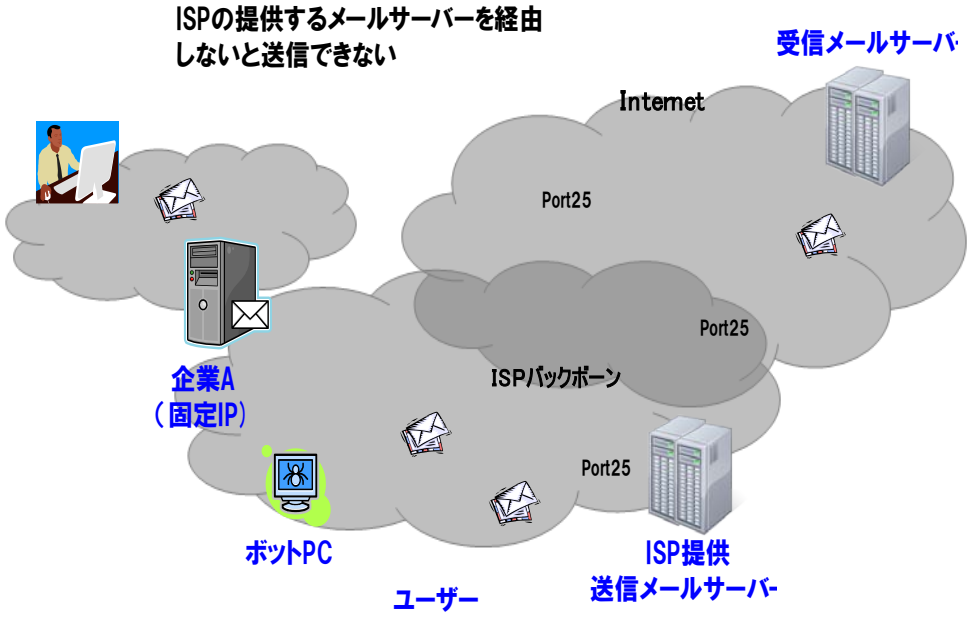
※ 国内発の迷惑メールを更に減少させるため、OP25B未導入の国内ISPへの対応が必要か。

OP25Bの導入状況と日本のスパム送信国ランキング



出典：（財）日本データ通信協会資料及びソフォス社資料より作成

OP25Bの概要



5 技術的対策 (b)送信ドメイン認証技術

現状

・ 送信ドメイン認証技術のうち、SPFの送信側導入率は4割、DKIM送信側の導入率は0.5%程度。

論点

○ SPFの送信側導入率を上げるため、ドメイン保有企業に対して、どのような取組をすべきか。

○ 国内ISPでのさらなる導入を図るために、どのような取組をすべきか。

○ なりすまさずに送られてくる迷惑メールへの対策について、どのように考えるか。

※ 政府の「情報セキュリティ2010」(情報セキュリティ会議(2010.7.22))において、送信ドメイン認証技術の推進に言及している。

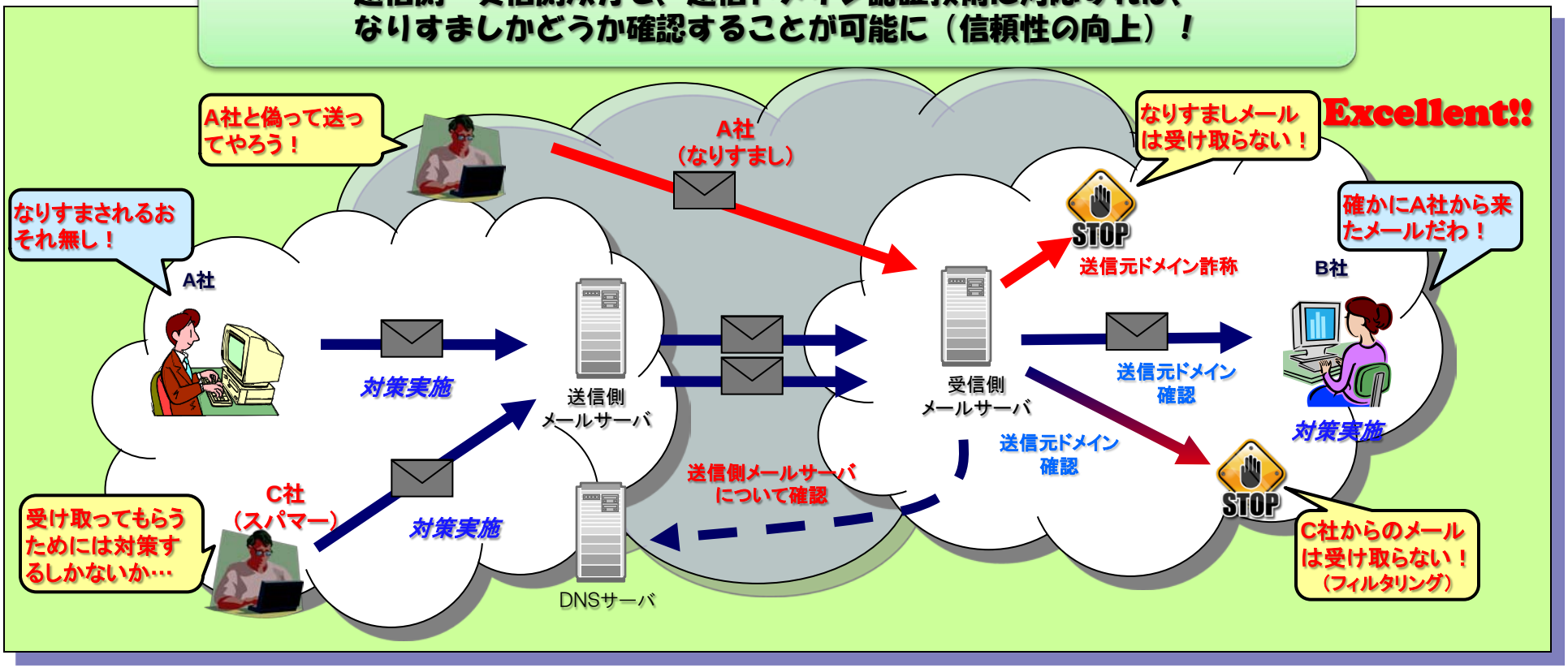
※ 迷惑メール対策推進協議会で策定した「なりすましメール撲滅プログラム」において、『2012年度までに、送信ドメイン認証技術により、受信側で、なりすましを簡単に見破ることができる環境の実現を目指す。』とされている。

※ (財)インターネット協会において、送信ドメイン認証技術の普及啓発等を図るため、迷惑メール対策カンファレンスを開催している。

※ 送信ドメイン認証技術により、Feedback Loop時に、信頼性判断に役立てることが可能【第2回WG JAIPA、JEAG資料】
(例えば、Feedback Loop時に、送信事業者は受け取ったFeedbackが本当に送ったメールであるかの判断が難しいといった問題がある)

送信ドメイン認証技術（SPF）の概要

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、なりすましかどうか確認することが可能に（信頼性の向上）！



概要

- ✓ 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)サーバと連携
- ✓ 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

メリット

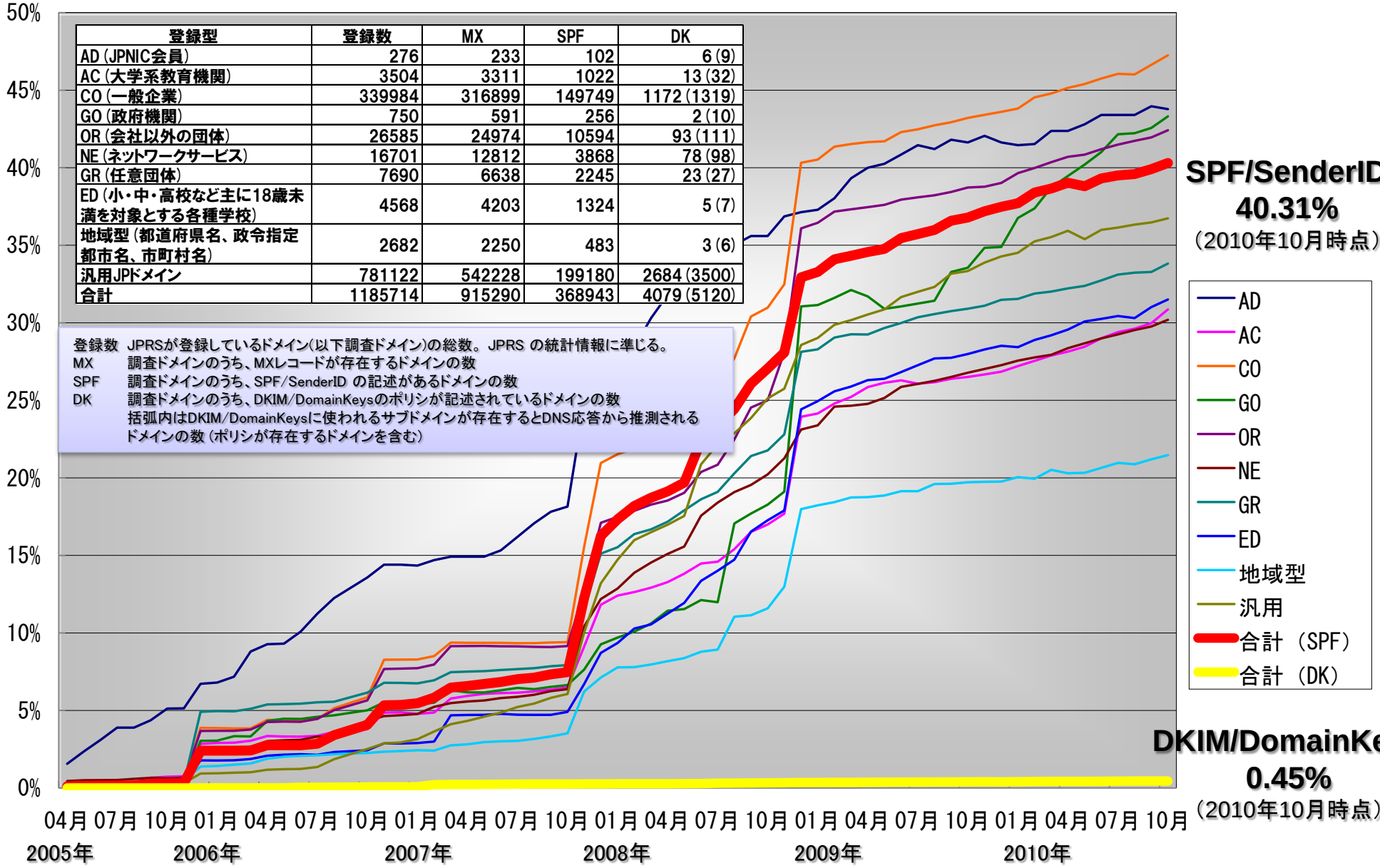
【送信側】 送信するメールが受け取られやすく
- 自ドメインの信頼性の確保
- 受信側が対応していれば、受け取られやすくなる

【受信側】 受ける電子メールを選別していくことが可能
- 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、フィルタリング等の他の技術と組み合わせることで、信頼できる送信者かの確認等（効率的な迷惑メール対策）

送信ドメイン認証技術の導入状況

登録型	登録数	MX	SPF	DK
AD（JPNIC会員）	276	233	102	6 (9)
AC（大学系教育機関）	3504	3311	1022	13 (32)
CO（一般企業）	339984	316899	149749	1172 (1319)
GO（政府機関）	750	591	256	2 (10)
OR（会社以外の団体）	26585	24974	10594	93 (111)
NE（ネットワークサービス）	16701	12812	3868	78 (98)
GR（任意団体）	7690	6638	2245	23 (27)
ED（小・中・高校など主に18歳未満を対象とする各種学校）	4568	4203	1324	5 (7)
地域型（都道府県名、政令指定都市名、市町村名）	2682	2250	483	3 (6)
汎用JPドメイン	781122	542228	199180	2684 (3500)
合計	1185714	915290	368943	4079 (5120)

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(2010年10月時点)より作成

5 技術的対策 (c)その他の技術的対策

現状

・ 迷惑メールの技術的対策として、OP25B、送信ドメイン認証技術の他、送信通数制限、フィルタリング等がある。

論点

○ OP25B、送信ドメイン認証技術の他、積極的に進めて行くべき技術的な対策として、どのようなものがあるか。

※ 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。オプションで利用申込が必要。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。【第2回WG JAIPA資料】

※ 各携帯電話事業者において、迷惑メール設定機能を提供【第2回WG NTTドコモ、KDDI、ソフトバンクモバイル資料】

※ 「電子メールはコストがかからず送信できるものであり、送らなければ損というシステム。そういう中で受信する側が絞り込むというのは難しいが、最終的にそこに切り込んでいかないと本質的な解決にならないと思うので、今後、どういった研究開発が必要なのかということにも触れてもらえると有り難い。」【第4回WG構成員発言】

迷惑メール送信・受信防止のための主な技術

【迷惑メール送信防止のための主な技術】

技術名	技術の概要
1. 送信数制限	同一アカウントからの送信量を制御する方法
2. 送信トラフィック制御	一定期間内に送信されるメールの通数をIPアドレスで制御する方法
3. 送信者認証(SMTP-AUTH)	送信側のISPで、自社メールサーバからの送信時に、IDとパスワードによる認証を行う方法
4. OP25B (Outbound Port25 Blocking)	ISPのメールサーバを経由しない動的IPアドレス（インターネットに接続される度に割り当てられるIPアドレス）からのメール送信を遮断する方法

【迷惑メール受信防止のための主な技術】

技術名		技術の概要
1. キーワード（ブラックワード）判定		メールのヘッダ及び本文中の特定のキーワードに合致するものを迷惑メールと判定する方法
2. 送信元情報参照による判定		メールの送信元情報を参照し、迷惑メールであるかを判定する方法
	ブラックリスト	迷惑メール送信元として知られるIPアドレスをまとめたリストからのメールを、迷惑メールと判定する方法
	送信ドメイン認証	自社のメールドメインから正しく発信されたメールであることを示す情報をDNSを利用して表明することにより、メール受信側で送信者情報が詐称されているかどうかを判断する方法
3. 内容参照による判定		主にメールの内容を検査し、流通する迷惑メールから分析した情報に基づいて迷惑メールかどうかを判定する方法
4. 受信トラフィック制御		特定の送信元から一時的に大量受信した場合や、存在しないあて先を多く含むメールを受信した場合等、迷惑メールの送信元である可能性が高い送信元からのメール受信に際し、トラフィック量を制御する方法

携帯電話・PHS 各社の提供するフィルタサービス

		au	docomo	Softbank	EMOBILE	WILLCOM
指定受信（設定数）	ドメイン・メールアドレス	200件 指定拒否と併用可能	120件 指定拒否と併用可能	20件 指定受信と拒否の併用不可 (どちらか一方を選択)	20件 指定受信と拒否の併用不可 (どちらか一方を選択)	20件 指定受信と拒否の併用不可 (どちらか一方を選択)
指定拒否（設定数）	ドメイン	200件 指定受信と併用可能 ※メールからアドレスを選んでそのまま指定拒否登録できるワンタッチ機能にも対応	120件 ※[指定受信][アドレス指定拒否]併用可能			
	メールアドレス		120件 ※[指定受信][ドメイン指定拒否]併用可能			
一括設定（携帯・PHS事業者、インターネットなど）		○	○	○	○	×
ドメイン認証		○	○	×	○	×
なりすまし対策		○	○	○	○	×
あて先指定受信		○	○	○	×	×
URL付きメール受信拒否		○	×	○	○	×
特定URL付きメール受信拒否		×	○	○	×	×
HTMLメール受信拒否		○※2	×	×	×	×
大量送信メールの受信制限		×	○	×	×	×
未承諾広告※メールの受信拒否		×（廃止）	○	○	○	○
迷惑メールコンテンツフィルタ		×	×	○	×	×
簡易設定（子ども向け設定含む）		○	○	○	×	×
有料サービス						
受信許可リスト拡張版		×	×	○	×	×

※1　auについては、平成22年12月初旬に実施予定のバージョンアップ後の状態
※2　インターネット発のメールにのみ適用される。

携帯3社における簡易設定機能の比較

○：自動的にON　×：自動的にOFF　－：簡易設定機能での設定なし

	au		DoCoMo			Softbank		
名称	カンタン設定		かんたん設定			かんたん設定		
設定名	「携帯、PHS，PCメールを受信」	「携帯、PHSメールを受信」	「キッズオススメ」	「受信拒否強」	「受信拒否　弱」	「きっずオススメ」	「推奨ブロック」	「ケータイ/PHS設定」
指定受信（ホワイトリスト優先受信）	－	－	－		－	○	○	○
なりすまし対策	○	○	○		○	×	×	×
あて先指定受信	×	×	－		－	－	－	－
一括設定（PCメール拒否）	×	○	○		×	○	×	○
一括設定（海外からのメール拒否（SMSのみ））	－	－	－		－	○	×	×
ドメイン認証	SPF/SenderID（含むPRA）で判定	－	-		送信メールのFromアドレスのドメインについてDNSの応答を確認し、実在するドメインか判定し、実在する場合のみ受信。	－		
URL付きメール受信拒否	×	×	－		－	○	×	×
特定URL付きメール受信拒否	－	－	○		○	×	○	○
HTMLメール受信拒否	×	×	－		－	－	－	－
大量送信メールの受信制限	－	－	－		－	－	－	－
未承諾広告※メールの受信拒否	×（廃止）	×	－		－	○	○	○
迷惑メールコンテンツフィルタ	－	－	－		－	○	○	○

※auについては、平成22年12月初旬に実施予定のバージョンアップ後の状態

用語説明

指定受信・拒否
メールアドレス・ドメイン・電話番号など、任意の受信・拒否リストを設定できる機能。
一括設定
携帯電話、PHSやPCからのメールなど、送信元の種類によって、一括で受信・拒否が設定出来る機能。
ドメイン認証
一般ISPからの送信メールを、ドメイン詐称されてないか確認してくれる、なりすまし対策のパソコン版。迷惑メールは、身元を詐称して送ることが多いので非常に有効です。ただし、詐称される正規のISPのドメインがSPFレコードをDNSへ登録していることが条件です。
なりすまし対策
パソコンから送信しているのに、携帯・PHS会社のメールアドレスになりすましたメールを拒否する機能。ただし、一般ISPのドメインになりすましたメールは見抜けないので、その場合はドメイン認証をすることで対処できます。
あて先指定受信
パソコンから転送設定していて、従来は「なりすまし」と判定され届かなかったメールについて、転送元のメールアドレスを登録することで受信出来るようになる「なりすまし対策」「ドメイン認証」の救済機能。
URL付きメール受信拒否
URL(http://www～～/など)リンクが含まれるメールを拒否する機能。
特定URL付きメール受信拒否
出会い系・アダルト系・違法行為・グロテスクなどの有害な特定サイトのURLリストを管理し、そのリストにマッチした場合、メールを拒否する機能。迷惑メールにはこのようなURLリンクが含まれることが多いので非常に有効です。
HTMLメール受信拒否
HTML形式で送られるメールを拒否する機能。HTMLを使うと受信者にURLを見せずにサイトに誘導できるため、フィッシングメールなどで多く使われており、フィッシング的なスパムの対策として有効です。（auについては、インターネット発のメールのみ対象）
大量送信メールの受信制限
1日あたり、1台の携帯電話から大量に送信される迷惑メールを、500通目以降から受信拒否の設定が出来ます。
未承諾広告※メールの受信拒否
件名に「未承諾広告※」と記載のあるメールを拒否する機能。
受信許可リスト拡張版
ネットワークにアドレス帳を補完するサービスを利用し、登録されたメールアドレスを優先的に受信する機能。

5 技術的対策 （参考）スマートフォン対策

現状

・ 今後、スマートフォンの普及が進展することが予想される。
（2010年10月現在、携帯電話台数に占めるスマートフォンの構成比は20%超（BCN調査））

論点

○ スマートフォンでの迷惑メール対策は適切に行われているか。

※ スマートフォンでの携帯電話事業者が提供しているメールサービスを利用した場合の迷惑メール対策については、従来の携帯電話事業者が提供している迷惑メール対策とほぼ同様。【第2回WG NTTドコモ、KDDI、ソフトバンクモバイル資料】

※ 一方、スマートフォンでは、携帯電話事業者が提供しているメールサービスのほか、アプリケーションを追加することにより、その他のメールサービスも利用することが可能であるが、その場合には、当該メールサービスの迷惑メール対策を利用することとなる。

スマートフォンは、携帯電話事業者の電子メールサービスの他、様々な電子メールサービスを使用することが可能。

携帯電話

スマートフォン

PC

携帯電話事業者のメールサービス

携帯電話事業者のメールサービス

プロバイダ等の提供するメールサービス

インターネット

スマートフォンと従来の携帯電話との迷惑メール設定機能の相違

【NTTドコモ（迷惑メール設定機能）】

機能名称	概要	spモード	iモード
かんたん設定	迷惑メール設定を簡易な操作で実施	○	○
URL付きメール拒否設定	URL付きメールを拒否	○	○
宛先指定受信	なりすましメールを拒否設定にした場合に、送信元等の電子メールアドレスを指定することで指定したアドレスからのメールの受信が可能	10件	10件
ドメイン・アドレス受信設定	ドメイン及びメールアドレスを指定して受信する	120件	120件
アドレス拒否設定	指定したメールアドレスの受信を拒否する	120件	120件
ドメイン拒否設定	指定したドメインの受信を拒否する	120件	120件
なりすましメール拒否	なりすましのメールの受信を拒否する	○	○
iモード/spモードメール大量送信者からのメール受信制限	１日あたり１台から送信される500通目以降のiモード／spモードメールの受信を拒否する	○	○
未承諾広告※メール拒否	「未承諾広告※」が付いた電子メールの受信を拒否する	○	○

※NTTドコモが提供するメールサービスを利用する場合。

（参考） 同時送信機能

	spモード	iモード
同時送信	100件まで	5件まで

スマートフォンと従来の携帯電話との迷惑メール設定機能の相違

【KDDI（迷惑メール設定機能）】

機能名称	概要	スマートフォン	EZweb
カンタン設定	迷惑メール設定を簡易な操作で実施	○	○
一括指定受信	インターネット、携帯電話各社、PHSからの電子メールを受信するかどうか選択して一括設定する。	○	○
なりすまし規制	なりすましのメールの受信を拒否する	高・中・低	高・中・低
指定拒否リスト設定	指定したドメインやメールアドレスの受信を拒否する	200件	200件
指定受信リスト設定	指定したドメインやメールアドレスの受信を許可する	200件	200件
指定受信リスト設定 （なりすまし転送メール許可）	なりすまし規制を設定した場合に、送信元等の電子メールアドレスを指定することで指定したアドレスからのメールの受信が可能	20件	20件
HTMLメール規制	携帯、PHS以外から送信されるHTML形式のメールの受信を拒否する	○	○
URLリンク規制	URL付きメールを拒否	○	○
拒否通知メール返信設定	メールフィルタで受信をブロックしたメールに対し、拒否通知メールを返信する	○	○
ワンタッチ拒否登録	受信したメールアドレスに含まれるメールアドレスから簡易に指定拒否リストに登録する	○	○

※auが提供するメールサービスを利用する場合。
※上記は、H22年12月のバージョンアップを実施した後の状態

（参考） 同時送信機能

	スマートフォン	EZweb
同時送信	30件まで	30件まで

スマートフォンと従来の携帯電話との迷惑メール設定機能の相違

【ソフトバンク（迷惑メール設定機能）】

機能名称	概要	スマートフォン S！メール（MMS）	従来の携帯電話 S！メール（MMS）
かんたん設定	各種迷惑メールブロック設定を、一括設定	○	○
なりすましメール	送信元アドレスを携帯電話・PHS事業者のドメインに詐称したメールを拒否	○	○
ともだちメール安心設定	S！電話帳バックアップに登録されたメールアドレスからのEメールを受信	×	○(＊1)
未承諾広告メール拒否設定	件名に「未承諾広告※」と表示のあるメールを拒否	○	○
URLリンク付きメール拒否設定	特定URLもしくはすべてのURLを含むメールを拒否	○	○
受信許可・拒否設定	特定のアドレスやドメイン等からのメールを「受信拒否」、「受信許可」または「ケータイ/PHSからのみ受信」を設定	○	○
海外からの拒否設定	海外事業者から電話番号で送られてくるメールを拒否	○	○
迷惑メールフィルター	迷惑メールフィルター機能を利用できる	○	○

※ソフトバンクが提供するメールサービスを利用する場合。
（＊1）S！電話帳バックアップに加入していない場合は、当ブロック機能は無効となる。

（参考） 同時送信機能

	スマートフォン S！メール（MMS）	従来の携帯電話 S！メール（MMS）
同時送信	20件まで	20件まで(＊2)

（＊2）但し、一部の機種は除く。

スマートフォンと従来の携帯電話との迷惑メール設定機能の相違

【イー・モバイル（迷惑メール設定機能）】

機能名称	概要	スマートフォン EMnet	従来の携帯電話 EMnet
全受信	全ての受信を許可	○	○
指定拒否設定	指定した文字列が送信者のアドレスに部分的に含まれる場合、メールの受信を拒否	20件	20件
メールアドレス指定受信	指定した文字列が送信者のアドレスに部分的に含まれる場合、メールの受信を許可	20件	20件
ドメイン指定受信	既存キャリアのドメインのうち、指定するドメインから送られてくるメールのみを受信	○	○
URLフィルタ拒否	本文中にURLが含まれるメールの受信を拒否	○	○
未承諾広告拒否	件名に「未承諾広告※」を含むメールを拒否	○	○
なりすまし規制	PCから携帯電話・PHSのメールアドレスを用いて、携帯電話・PHSから送信されたかのように装ったメールの受信を拒否	○	○
送信ドメイン認証	送信元のIPアドレスについて、送信元のSPFレコードと合致しないメールを拒否	○	○
拒否通知の送信	メールフィルタ設定で拒否されたメールに対し、拒否したことを相手に通知	○	○

※　イーモバイルが提供するメールサービスを利用する場合。

（参考）　同時送信機能

	スマートフォン EMnet	従来の携帯電話 EMnet
同時送信	10件まで	10件まで

スマートフォンと従来のPHSとの迷惑メール設定機能の相違

【ウィルコム（迷惑メール設定機能）】

機能名称	概要	スマートフォン	従来のPHS
未承諾広告メール拒否	件名に「！広告！」「未承諾広告※」と表示のあるメールを拒否	○	○
メールアドレス指定受信拒否	指定したメールアドレスの受信を拒否	20件まで	20件まで
メールアドレス指定受信	指定したメールアドレスを受信	20件まで	20件まで
メールアドレス変更	電話機からメールアドレスを変更	○	○

（参考） 同時送信機能

	スマートフォン	従来の携帯電話
同時送信	100件まで	100件まで

※PHS端末の場合、端末側で機種により更に低い制限を設定（直近の機種で最大20件）

6 利用者への周知啓発

現状

・ 行政機関、(財)日本データ通信協会、ISP、携帯電話事業者、各種団体等が迷惑メール対策に関し、Web、パンフレットでの周知活動を実施。

論点

○ 利用者側での迷惑メール対策が、より適切に行われるよう、利用者への周知を強化するため、どのようなことが考えられるか。

※ 利用者における迷惑メール対策未実施の割合は、PCで48%、携帯電話で28%【第1回WG事務局資料】

※ 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（ウィルス）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（第2回WG JAIPA資料）ことから、より一層の周知啓発が必要ではないか。

※ ISPや携帯電話会社におかれては、「迷惑メールを受けて不安な気持ちになっている」消費者に向けた情報提供等をお願いするとともに、消費者被害の未然防止・拡大防止の観点から、効果的な迷惑メール対策を引き続いて検討頂きたい。
【第3回WG（独）国民生活センター資料】

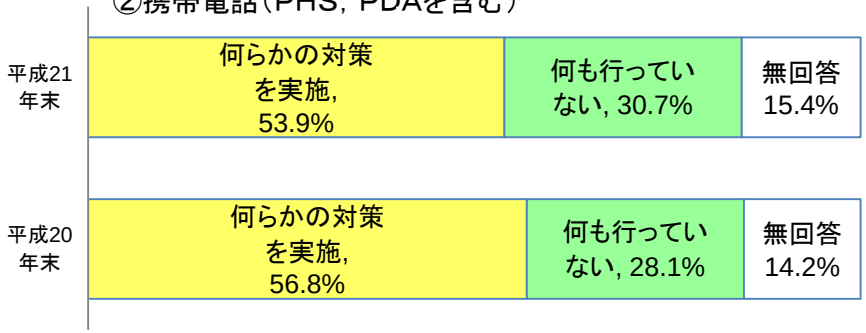
※「架空請求が送られてくると、個人情報が知られているのではないかということで5000円程度なら払ってしまう。そして、払ってしまうと入会金が必要であったということでまたお金を請求されて初めて相談になる。是非、払ってしまう前に架空請求メールというものがあるということを周知して欲しい。」【第3回WG構成員発言】

利用者における迷惑メール対策の実施状況

パソコンでの迷惑メール対策を行っていない利用者が約5割、携帯電話での迷惑メール対策を行っていない利用者が約3割となっており、迷惑メール対策があまり実施されていない。

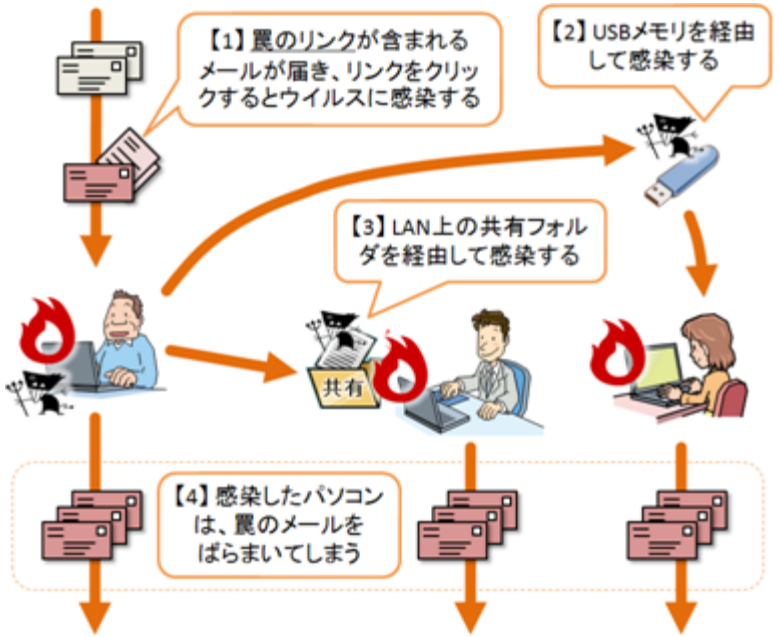
①パソコン

②携帯電話（PHS，PDAを含む）



出典：平成21年通信利用動向調査（総務省）

迷惑メールをはじめとした様々な経路で感染させようとするウィルスの仕組み



迷惑メール対策関係者による主な普及啓発活動

	主な普及啓発活動
総務省・消費者庁	・HPによる特定電子メール法、技術的対策、電気通信事業者における自主的取組の推進等の周知 ・パンフレットによる特定電子メール法の解説
(財)日本データ通信協会 迷惑メール相談センター	・HPによる迷惑メール対策の周知 ・パンフレットによる特定電子メール法の解説、利用者向け迷惑メール対策方法の解説 ・迷惑メールに関する調査研究活動と成果公表 ・電話相談　等
(財)インターネット協会 迷惑メール対策委員会	・HPによる迷惑メール対策の周知 ・迷惑メール対策カンファレンスの開催 ・地方セミナーの開催
各ISP事業者	・HP、パンフレットによる自社の迷惑メール対策サービスの周知 ・子供向け安全教室の開催 ・迷惑メール申告窓口の設置
各携帯電話事業者	・HP、パンフレットによる自社の迷惑メール対策サービスの周知 ・子供向け安全教室の開催 ・迷惑メール申告窓口の設置
消費者団体	・HPによる迷惑メールに関する相談事例等を紹介 ・通報窓口の紹介、消費者相談

7 国際連携の推進

現状

- 多国間連携（ロンドンアクションプラン、ソウル・メルボルンMOU）、二国間連携（カナダ、英国、フランス、ドイツと共同声明等）を実施。
- 中国、香港、台湾、ブラジルと送信元IPアドレスを交換。
- JEAG、(財)インターネット協会において、APCAUSE（アジア太平洋地域の民間の迷惑メール対策団体）と連携し、情報交換等を実施。
- また、JEAGにおいて、MAAWG(国際的な民間の迷惑メール対策団体）と連携し、情報交換等を実施。

論点

○ 海外発の迷惑メールが増加してきており、諸外国との連携・協調を一層行っていくべきではないか。

○ 諸外国からボットによる電子メール送信が見られることから、ボット対策に有効なOP25B等の海外普及を図るべきではないか。

※ 日本での成功事例（OP25B、送信ドメイン認証技術、etc）の海外への普及によるグローバルでの迷惑メール抑制

【第2回WG JEAG資料】

※ 二国間連携として、特に日本への迷惑メール送信が多い外国執行当局と連携し、法執行に資する情報交換を積極的に進めていくことが重要ではないか。また、送信元IPアドレスの交換対象国を更に増やしていくことが必要ではないか。

※ OP25Bの海外での普及を促進するため、分かりやすい英文の解説資料を準備して公開することが必要ではないか。また、海外のボット感染PCを減少させるため、CCC（サイバークリーンセンター）の取組みを積極的に海外に紹介していくとともに、効果的な対処のために諸外国との連携体勢を構築することが重要ではないか。

【多国間連携】

迷惑メール対策に特化した枠組み

○ ロンドンアクションプラン（LAP: London Action Plan）

・主要国の迷惑メール対策執行当局が参加し、執行当局間の意思疎通や連携、官民対話の促進などを目的として2004年11月に合意された行動計画であり、以後、同計画に基づき、継続的に活動。総務省から、定期的な電話会議や、物理的会合に参加。

・2010年10月に開催された会合に出席し、日本の迷惑メールの取組について説明・意見交換を実施

○ ソウル-メルボルン　スパム対策の協力に関する多国間Mou

・アジア太平洋地域の迷惑メール対策執行当局が参加し、迷惑メールの削減のための協力を推進するために2005年4月に合意されたMou（覚書）であり、以後、同覚書に基づき、各国の法制や、執行当局の取組について、情報交換を行うとともに、加盟機関間における執行協力に関する議論を行っている。総務省から、定期的な電話会議や、物理的会合に参加。2008年3月には東京で会合を開催。

国際機関などを通じた取組

○ 国際電気通信連合（ITU：International Telecommunication Union）

・電気通信分野に関する国際連合の専門機関。電気通信技術の標準化を扱うITU－Tにおいて、迷惑メール対策について議論。

・2009年4月に開催された世界電気通信政策フォーラムの成果文書において、迷惑メール送信者や技術的対策に関する情報交換の推進を合意。

○ 経済協力開発機構（OECD）

・2004年2月「スパムに関するワークショップ」を開催し、迷惑メールに対する多面的な方策の枠組みについて検討。

・2006年4月に迷惑メール対策の枠組みをまとめた「アンチスパム・ツールキット」を取りまとめ公表。

○ アジア太平洋経済協力（APEC）

・電気通信サブグループ等で迷惑メール対策について定期的に意見交換を実施。

○ アジア・太平洋電気通信共同体（APT）

・アジア・太平洋地域の電気通信の開発促進、地域電気通信網の整備・拡充を目的とする国際機関。

・2009年5月に開催された政策・規制フォーラムにおいて迷惑メール対策について議論。

○ 日ASEAN情報セキュリティ政策会議

・アジア地域におけるセキュアなビジネス環境の整備、安心・安全なICT利用環境の構築に向けた地域的対応を目的として、2008年6月に設置が合意された高級事務レベル会合。

・2009年2月に開催された第1回会合の成果文書において、迷惑メール等サイバー脅威への対応における連携の強化について合意。

・2010年3月にバンコクにて開催された第2回会合で、日・ASEANの協力事項を定めた「連携枠組み」に一致。

【二国間連携】

北米

○ 米国
・個別協議のほか、日米情報通信政策協議や日米規制改革イニシアティブにおいて、迷惑メール対策について意見交換。

○ カナダ
・2006年10月に迷惑メール対策に関し合意（共同声明）。日加情報通信政策協議等で迷惑メール対策について意見交換。

欧州

○ EU
・日EU定期協議（直近は2008年3月に開催）等で迷惑メール対策について意見交換。

○ 英国
・2006年9月に迷惑メール対策に関し合意（共同宣言）。日英定期協議等（直近は2008年1月開催）で迷惑メール対策について意見交換。

○ フランス
・2006年5月に迷惑メール対策に関し合意（共同声明）。日仏定期協議（直近は2010年11月開催）等で迷惑メール対策について意見交換。

○ ドイツ
・2007年7月に迷惑メール対策に関し合意（共同声明）。日独情報通信政策協議（直近は2006年9月開催）等で迷惑メール対策について意見交換。

南米

○ ブラジル
・2010年5月に第1回ブラジルージャパン　アンチスパムワークショップを開催し、迷惑メール対策について意見交換。

アジア・オセアニア

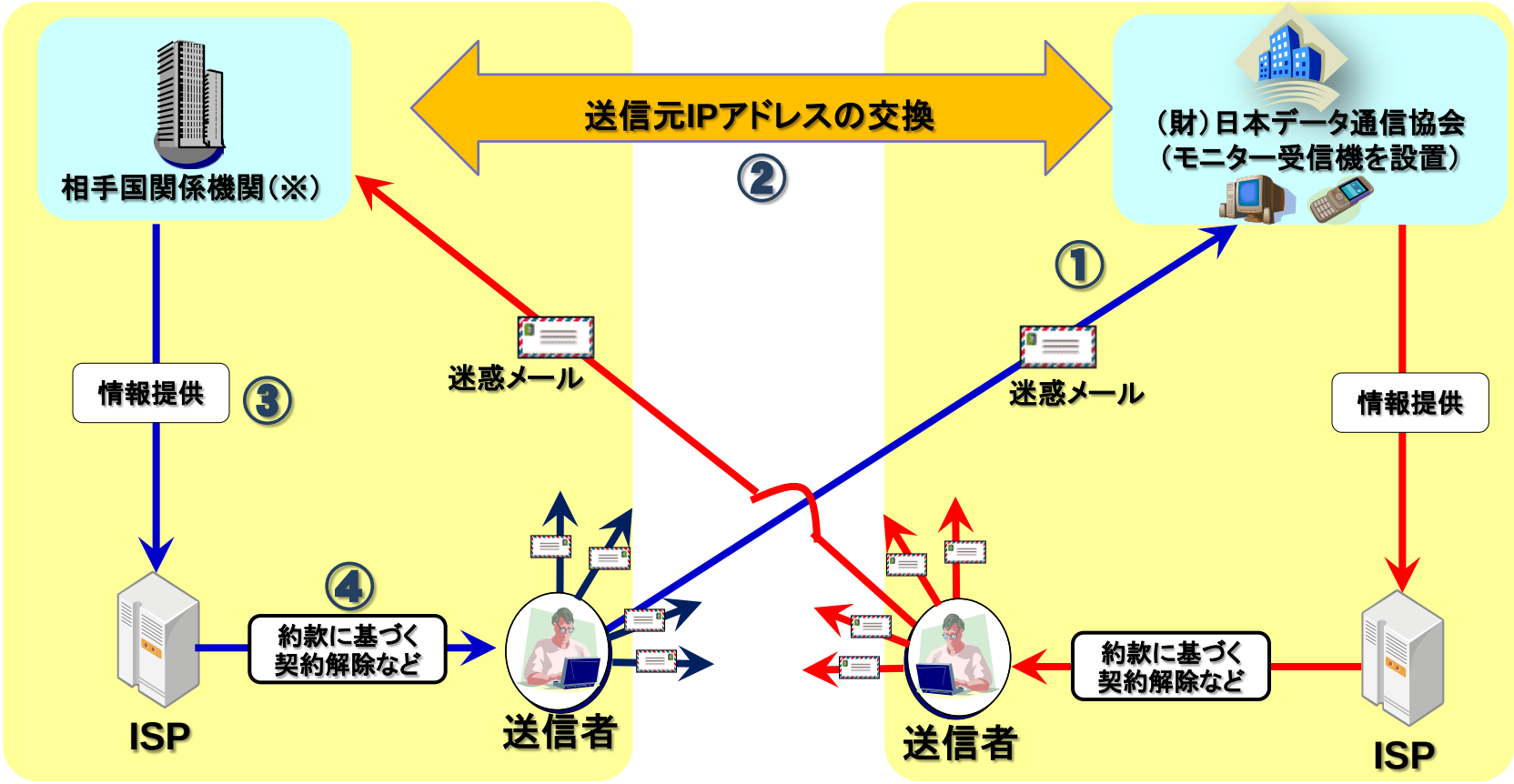
○ オーストラリア
・日豪情報通信政策協議等で迷惑メール対策について意見交換。

○ 中国
・2009年3月に迷惑メール対策に関する意見交換
・2009年5月にICT協力に関する文書を締結。
・2009年8月に日中ICT競争政策・規制制度セミナーでの迷惑メール対策に関する意見交換。

○ 韓国
・2009年5月に放送及び電気通信分野における協力に関する日本国総務省と大韓民国放送通信委員会との覚書き締結。
・2010年4月に迷惑メール対策に関する意見交換。

迷惑メールに関する国際連携の状況③

(財)日本データ通信協会において、中国、台湾、香港、ブラジルとの送信元IPアドレスの交換を実施。

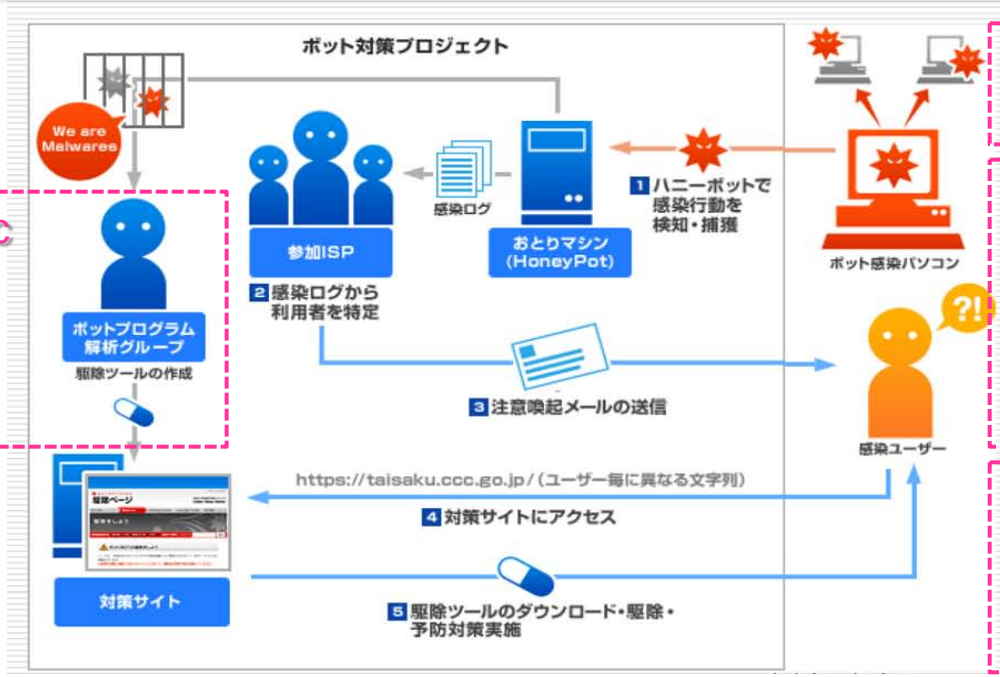


①（財）日本データ通信協会のモニター受信機で迷惑メールを受信
②提供された迷惑メールの送信元ＩＰアドレスを分析し、中国発の場合は、送信元ＩＰアドレスを中国インターネット協会（ＩＳＣ）に提供
③送信元のＩＳＰにＩＰアドレスを提供
④送信元ＩＳＰにおいて、送信者との契約解除などの措置

※２０１０年８月現在、中国：中国インターネット協会（ISC）、台湾：国家通信放送委員会（NCC）、香港：電気通信管理局（OFTA）、ブラジル：CERT.brとの間で交換を実施。

- 総務省・経産省の連携の下、セキュリティ関係機関のオールジャパン体制として「サイバークリーンセンター（CCC）」を構築し、ボットウイルスを撲滅する取組み
- 2006～2010年度の5カ年計画
- ISPのセキュリティ共同組織である「Telecom-ISAC Japan」（会長：伊藤泰彦 KDDI顧問）が中心的な役割を遂行
- 約3年半の試行により、世界トップクラスの低ボット感染率を実現。国際的にも高い評価

インターネット上のボットウイルス活動を観測し、ボット感染PCを探索。感染ユーザーにボット駆除を勧奨



1 ボットウイルスの捕獲 — Telecom-ISAC

感染PCから行われる感染攻撃を補足しウイルスの捕獲と感染元情報の取得を行う。

2 感染ユーザの特定 — ISP（76社）

感染元情報から感染ユーザを特定する。

3 注意喚起メール（封書）の送信

ユーザに感染を伝えCCCの対策サイトでの駆除・対策を依頼する。
この際に接続アドレスには、個人を識別可能な文字列を挿入し、進捗状況を把握できるようになっている。

4 対策サイトにアクセス — 一般ユーザ

5 ボット駆除ツール（CCCクリーナ）のダウンロード

CCCクリーナを使用し駆除を行うと共に再感染防止の対策を行う。

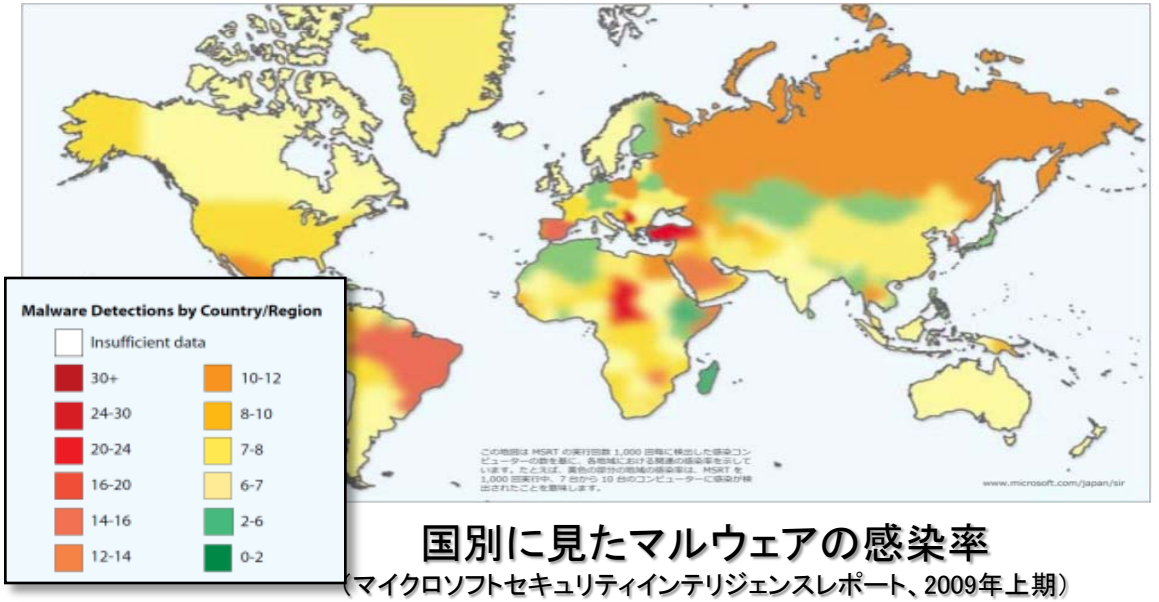
ウイルス感染者を減らし、世界トップクラスの低ボット感染率を実現

○ これまでの取組みにより、ボット感染率は、2005年の約2～2.5%（40～50万ユーザ）から、2008年には約1%（30万ユーザ）に低下

○ 在日米国商工会議所（ACCJ）も、CCCの取組みにより日本が先進国で最も低いボット感染率を達成しているとの評価（インターネット・エコノミー白書、2009年10月）

	2007年6月	2010年6月
CCCが収集したボットの数	51 万個	15万個
注意喚起メール	7,697人	3,808人

【当初3年間の運用実績】
○新種ボットウイルスの発見：　1日平均25種類
　⇒ 駆除ツールを作成、市販のウイルス対策ソフトにも反映
○注意喚起メール（発見された感染PC）：　1日平均438通
　⇒ ISP（76社）が、感染者に通知しウイルス駆除を勧奨
○感染者はCCCのサイトにアクセスし、ウイルス駆除等を実施
　CCCサイトへのアクセス：　1日平均　12,722件
　駆除ツールのダウンロード：1日平均　1,110回



国別に見たマルウェアの感染率
（マイクロソフトセキュリティインテリジェンスレポート、2009年上期）

※ 収集したウイルスのうち約16%が未知の新種ウイルス（市販のウイルス対策ソフトで検知できないもの）

独でも日本のサイバークリーンセンター（CCC）を参考に同様の取り組みを2010年9月15日から開始。

- 独のスパム送信は世界ワースト4位（2009年BSI調べ。日本はワーストでほぼ最下位）。
- 連邦内務省(BMI)傘下の連邦情報セキュリティ庁（BSI）が、ワースト10位から脱出するため当該プロジェクトを2010年9月開始。

8 総合的対策

現状

・ 2008年に、迷惑メール対策の関係者間の緊密な連絡を確保し、最新の情報共有、対応方策の検討、対外的な情報提供などを行うため、迷惑メール対策推進協議会が設立された。

論点

○ 迷惑メール対策推進協議会の取組みとして、さらに、どのようなものが期待されるか。

※ 迷惑メール対策推進協議会のこれまでの主な活動
- ■ 「迷惑メール追放宣言」の採択（2008年）
- ■ 「迷惑メール対策ハンドブック」の作成・公表（2009年、2010年）
- ■ 「送信ドメイン認証技術導入マニュアル」「なりすましメール撲滅プログラム」の作成・公表（2010年）

- ◆ 迷惑メール撲滅を目指す産官学関係者の集まり
- ◆ 2008年11月27日設立
- ◆ 緊密な連絡を確保し、最新情報共有、対応方策検討、対外的情報提供を実施

■ 体制

迷惑メール対策推進協議会

座長：新美育文　明治大学教授
座長代理：松本恒雄　一橋大学大学院教授

構成員：
電気通信事業者、送信事業者、広告事業者、配信ASP事業者、セキュリティベンダー、各関係団体、消費者、学識経験者、関係省庁など47者

- **幹事会**
- **送信ドメイン認証技術WG**
  主査：櫻庭秀次（株）インターネットイニシアティブ　シニアエンジニア
  副主査：本間輝彰　KDDI au oneプラットフォーム開発部　課長
- **事務局**
  (財)日本データ通信協会迷惑メール相談センター

■ 活動経緯