資料8

迷惑メールに係る対応方策の検討について
（論点整理（案））

平成２２年１１月２９日

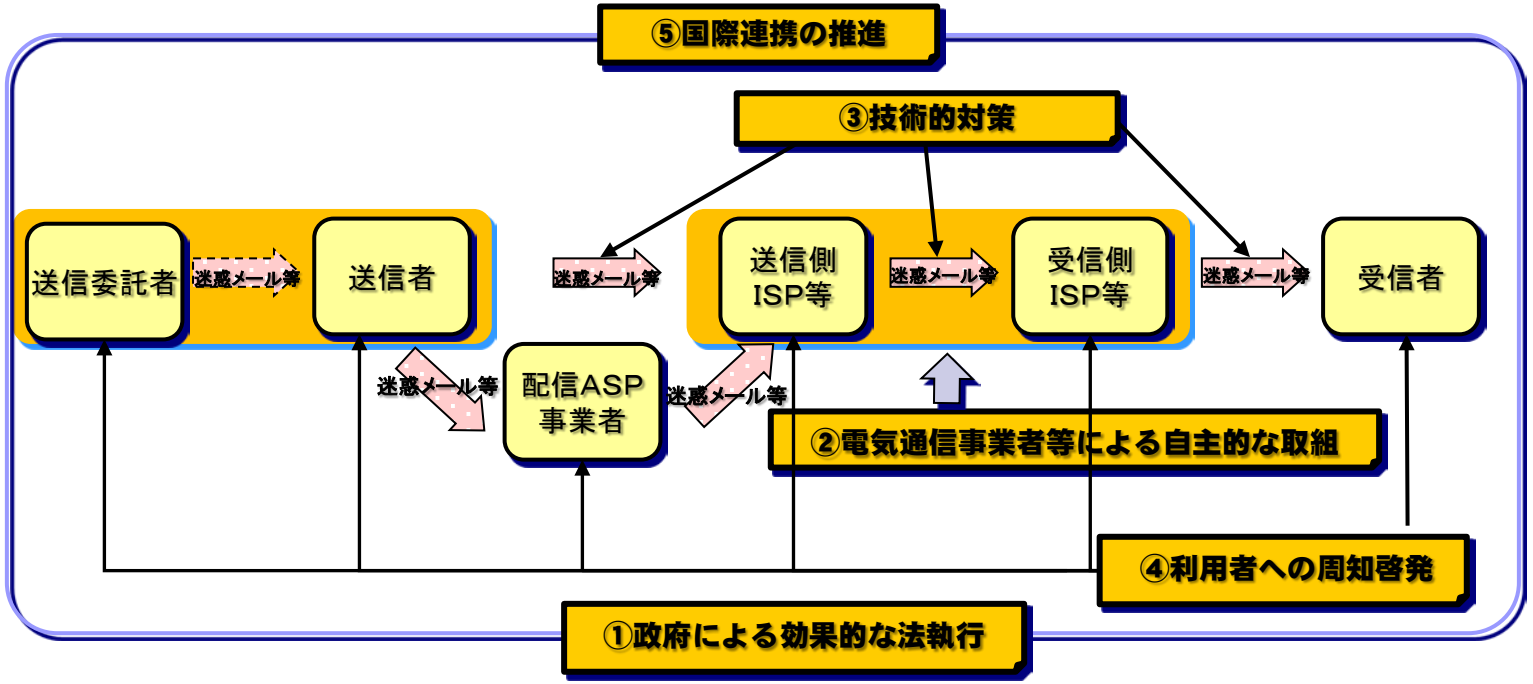
事　　務　　局

目　次

1. 迷惑メール対策の枠組み

現状

これまで、迷惑メール対策の検討は、①政府による効果的な法執行　②電気通信事業者等による自主的な取組　③技術的対策　④利用者への周知啓発　⑤国際連携の推進　の枠組みにより総合的に実施



論点

上記の枠組みについて見直すべき点はあるか。

※　広告関係事業者等による迷惑メール対策に関する自主的な取組が行われていることから、「電気通信事業者等による自主的な取組」から切り出して位置づけてはどうか。

２　政府による効果的な法執行　(a)オプトイン規制の評価（法第３条、第４条）

現状

【オプトイン規制】

・あらかじめ同意した者以外の者への電子メールの送信の原則禁止

［例外］

・送信者・送信委託者に電子メールアドレスを通知したもの

（原則書面による通知。ただし、同意の確認のための電子メールに対する返信等については任意の方法）

・電子メールを手段とする広告又は宣伝に係る営業を営む者と取引関係にあるもの

・インターネットを利用して、自己の電子メールアドレスを公表している団体又は営業を営む個人

（ただし、自己の電子メールアドレスと併せて、特定電子メールの送信をしないように求める旨を表示していた場合を除く）

【表示義務】

・送信者等の氏名又は名称（電子メールの任意の場所に表示）

・送信者等の住所（電子メールの任意の場所に表示。なお、リンク先での表示とすることも可能。）

・オプトアウトの通知ができる旨（オプトアウトの連絡先となる電子メールアドレス等の前後に表示）

・オプトアウトの連絡先となる電子メールアドレスまたはURL（電子メールの任意の場所に表示）

・苦情・問合せ等を受け付けるための電話番号、電子メールアドレス又はURL

（電子メールの任意の場所に表示。なお、リンク先での表示とすることも可能。）

２　政府による効果的な法執行　(a)オプトイン規制の評価（法第３条、第４条）

【記録保存義務】

・あらかじめ同意した者について、同意があったことを証する記録を保存する義務

（保存すべき内容（以下のいずれか））
①同意を取得している個別の電子メールアドレスに関し同意を取得した際の時期、方法等の状況を示す記録
②同意の取得に際し、書面の提示やWEBサイトから通信文の伝達をしていた場合は、電子メールアドレスリストに加え、以下の区分に応じた記録
　・同意の取得に際し、書面の提示・交付をした場合　　当該書面に記載した定型的な事項
　・同意の取得に際し、電子メールの送信をした場合　　当該電子メールの通信文のうち定型的な事項
　・同意の取得に際し、WEBサイトから通信文の伝達をした場合　　当該通信文（WEBサイトに表示された事項）のうち定型的な事項

（保存期間：記録の保存に係る特定電子メールを最後に送信した日から１ケ月間。ただし、措置命令後１年の間に特定電子メールを送信した場合は、当該特定電子メールを最後に送信した日から１年を経過する日、もしくは当該特定電子メールを最後に送信したから１月を経過する日のいずれか遅い日）

【オプトアウト】

・受信拒否者への再送信の禁止

（オプトアウトの通知の方法）
電子メールアドレスを明らかにすることが必要であるが、具体的な方法については任意の方法で可能。

（オプトアウトの例外（受信拒否の通知を受けた場合であっても送信できる場合））
・契約や取引の履行に関する事項を通知する電子メールにおいて、付随的に広告宣伝が行われる場合
・いわゆるフリーメールサービスを利用して送信する電子メールにおいて、付随的に広告宣伝が行われる場合
・広告宣伝以外の行為を主たる目的として送信される電子メール（受信者の意思に反することなく送信されるものに限る）において、付随的に広告宣伝が行われる場合

２　政府による効果的な法執行　(a)オプトイン規制の評価（法第３条、第４条）

論点

①　オプトイン規制の導入により、迷惑メール対策の実効性はあがっているか。

※　電子メールに占める迷惑メールの比率は、7割弱で推移【第1回WG事務局資料（8頁参照）】
※　諸外国から送信された迷惑メールの比率が9割強であり、国内からの送信は1割弱【第1回WG事務局資料（9頁参照）】
※　行政処分（措置命令）件数：オプトアウト規制時0.94件/年　→　オプトイン規制時5.14件/年【第1回WG事務局資料（9頁参照）】

②　オプトイン規制の下で、広告宣伝メールの送信が認められる場合は、適切なものとなっているか（過度に、正当な営業行為を規制していないか）。

※　広告宣伝メールを送信する際に、同意を取得しないと送信ができないことで過度の負担が生じたことはあるか。
（オプトイン規制の例外事項（送信者・送信委託者に電子メールアドレスを通知したもの等）以外）

※　オプトイン規制の例外事項により、同意を取得せずに広告宣伝メールができることで受信者に過度の負担が生じたことはあるか。

２　政府による効果的な法執行　(a)オプトイン規制の評価（法第３条、第４条）

③適切な同意の取得にあたり、デフォルトオンについて、どう考えるか。

※　現在の「特定電子メールの送信等に関するガイドライン」では、以下のように記述されている。

『同意の有無は、①受信者の認識があったかどうかと、②賛成の意思表示があったかどうかということにより判断すべきであるとの考え方からすれば、同意の有無は一概にデフォルトオンかデフォルトオフかのみで決まるものではなく、同意を取得する際の利用者への表示の方法が、同意により電子メールの送信があることを利用者が認識できるようになっているかどうか、利用者の賛成の意思表示が示されたものといえるかどうか、によって決まるものであると考えられる。

ただし、デフォルトオンと比較して、デフォルトオフの方が、受信者の意思が明確に表示されることになるのは確かであり、サービスの内容等にもよるが、その実施が可能な場合には、デフォルトオフによることが推奨される。

また、デフォルトオンの場合にあっては、例えば、チェックボックスのチェックを外さない場合には送信に同意したこととなる旨の記載やチェックの外し方に関する記載を行うこと、デフォルトオンなのかデフォルトオフなのかをわかりやすく表示することなどが推奨される。』

※「大量オプトインメールも利用者にとっては迷惑メールになっている。加入する際にデフォルトでチェックマークがすでに入っており、そのまま登録してしまう場合があるので、そのようなうっかり加入をなくすことが必要。」【第２回WG構成員発言】

※「（デフォルトオンについては）３年前オプトイン導入の際に議論した。同意する時に、わかりやすく表示をするとして整理されたと思う。その「わかりやすく」というところでデフォルトオンとしたことが同意をとっていないことにはならないということになったと思う。消費者にとって、わかりやすい表示や解除する場合のわかりやすい手法をどのように提供していくかということであろう。」【第２回WG構成員発言】

２　政府による効果的な法執行　(a)オプトイン規制の評価（法第３条、第４条）

④　表示義務は過度になっていないか。実効性のあるものとなっているか

※　現在の「特定電子メールの送信等に関するガイドライン」では、以下のように記述されている。
『なお、表示の方法等に関しては、受信者にとって判りやすく表示することが求められるところであり、電子メール本文の最初又は最後に記載することが推奨される。また、リンク先に記載することが認められる表示事項についても、リンク先に当該事項が表示されていることを受信者が容易に認識できるようにされていることが推奨される。ただし、リンク先のURLを記載することが認められる場合やオプトアウトの通知先をURLとする場合に関しても、何度もクリックしないと必要な表示にたどり着かないようなときには、表示として不適当なものである。』
※　オプトイン規制導入後、表示義務違反による措置命令は、5件【第１回WG事務局資料（８頁参照）】
※　特に、表示エリアが狭い携帯電話宛の電子メールで、問題は生じていないか。（携帯電話での表示義務の例（１０頁参照））

⑤　同意の記録の保存義務は、重くなっていないか。実効性のあるものとなっているか

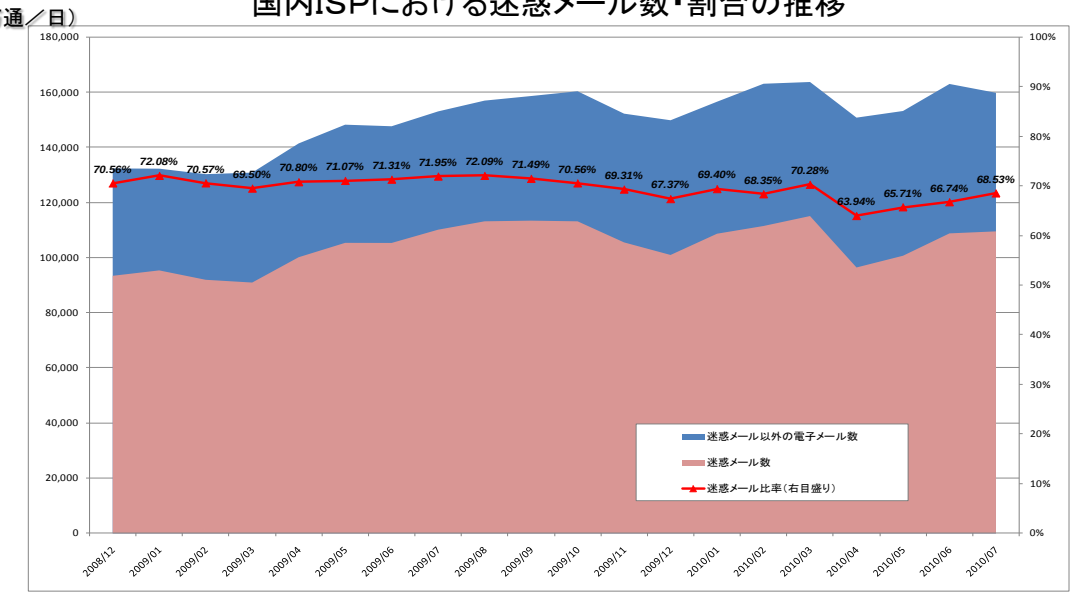
※　オプトイン規制導入後、同意の記録保存義務による措置命令は2件【第１回WG事務局資料（８頁参照）】

⑥　オプトアウト規制は、実効性のあるものとなっているか。

※　現在の「特定電子メールの送信等に関するガイドライン」では、以下のように記述されている。
『オプトアウトの通知の具体的な方法は施行規則で定められており、特定電子メールの受信に係る電子メールアドレスを明らかにすることが必要であるが、その具体的な方法は、電子メールその他の任意の方法とし、特に限定はされていない。
オプトアウトの方法が複雑であると、受信者は当該電子メールを迷惑メールとしてフィルタリングによりブロックし、場合によっては迷惑メールとして通報することがあることから、受信者との健全な関係を構築するためにも、送信者側は簡便なオプトアウトの方法を提供することが推奨される』

※「配信停止の手続もワンクリックでできるところもあるし、IDとパスワードでログインしないといけない場合もある。ID、パスワードを忘れた場合は再発行手続が必要となると、利用者は配信停止手続をせずに、そのままにしてしまうことがあり、配信手続の定型化が必要ではないかと考える。」【第２回WG構成員発言】

国内ISPにおける迷惑メール数・割合の推移



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

措置命令件数

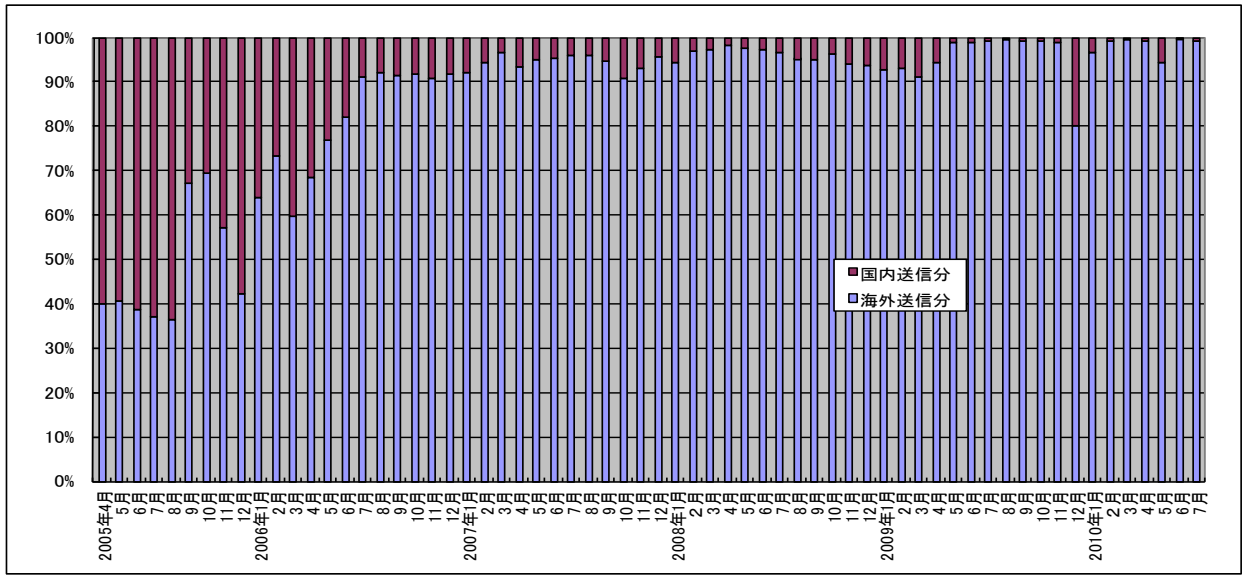
※2002年の特定電子メール法制定以降、計15件の措置命令を実施。2008年12月のオプトイン規制導入後に実施した措置命令は9件。

	年度	件数	違反内容
オプトアウト規制時	2002年度 (7月～)	1件	表示義務違反、再送信禁止義務違反
	2003年度	1件	表示義務違反
	2004年度	1件	表示義務違反
	2005年度	1件	表示義務違反
	2006年度	0件	
	2007年度	1件	表示義務違反
	2008年度 (～11月)	1件	表示義務違反
	小計	6件	（年平均0.94件）

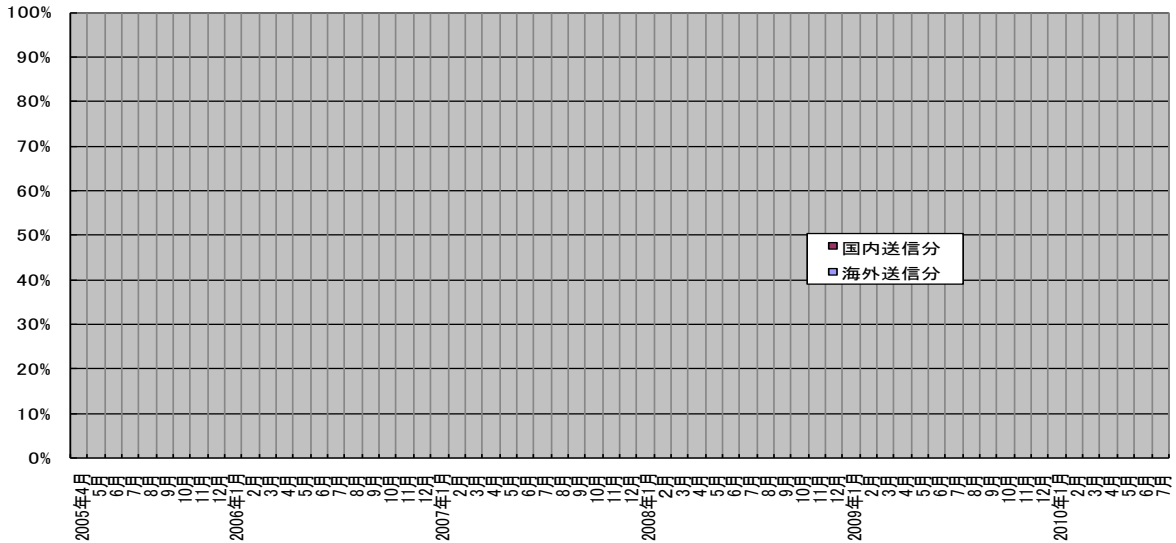
	年度	件数	違反内容
オプトイン規制時	2008年度 (12月～)	0件	
	2009年度	6件	同意なく送信・・・2件 同意なく送信、表示義務違反・・・2件 同意なく送信、記録保存義務違反、表示義務違反・・・2件
	2010年度	3件	同意なく送信・・・2件 同意なく送信、表示義務違反・・・1件
	小計	9件	（年平均5.14件）

日本着の迷惑メールの国内発・海外発の比率の推移

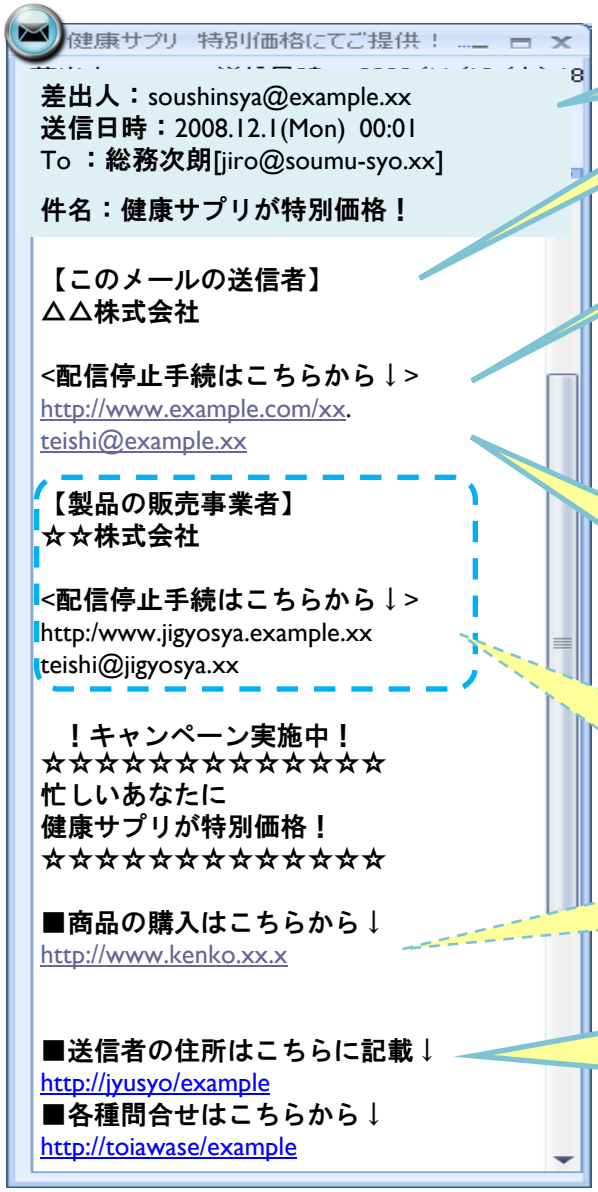
ＰＣあて



携帯あて



特定電子メール法の表示義務



送信者情報（送信に用いた電子メールアドレス、IPアドレス、ドメイン名）を偽って送信することは禁止

✓送信者など※１の氏名または名称

✓受信拒否の通知ができる旨
　受信拒否の通知先の直前または直後に表示する必要。送信に用いられた電子メールあてに送信することで通知できる場合は、その旨を電子メールの中の受信者が容易に認識できる場所に表示する必要。

✓受信拒否の通知を受けるための電子メールアドレスまたはURL※２
　ＵＲＬとする場合は、リンク先において、受信拒否に必要な情報が明確かつ平易に提供され、受信拒否の通知が容易に行うことができるよう、必要な措置が講じられている必要。

特定商取引法上の販売業者などと送信者などが異なる場合
✓販売業者などの氏名または名称
✓相手方が電子メール広告の提供を受けない旨の意思を表示するための電子メールアドレスまたはURL※２

特定商取引法に基づくその他の表示事項はリンク先での表示とすることも可能。

✓送信者などの住所
✓苦情・問合せなどを受け付けることができる電話番号、電子メールアドレス、URL※２
リンク先での表示とすることも可能です。その場合は、表示場所を示す情報を電子メールの中に表示する必要があります。

※１　電子メールの送信を委託している場合は、送信者または委託者のうち送信に責任を有するもの
※２　ハイパーリンクとすることも可能

２　政府による効果的な法執行(b)その他の前回改正事項の評価

(i) 契約者情報の提供の求め（法第29条）

現状

・電気通信事業者に対し、広告宣伝メールを送信した者の氏名、住所等の提供を求めることができる（受信者の端末画面に表示されたもの又はヘッダ情報等の電子メール送信のために用いられた送信者情報に限る）。なお、この規定は、個人情報保護法の特則として、電気通信事業者等による個人情報にあたる情報の総務大臣への提供を可能とするもの。（※前回改正で新規追加）

論点

○　契約者情報提供の求めにより提供される情報は、法執行に有効なものとなっているか。情報が取得できない場合など、問題はないか。

※　制度導入後、22年10月までに、27事業者に対して、延べ207回の契約者情報の照会を実施。

※「例えば「WHOIS」（インターネット上でのドメイン名等の所有者を検索するためのシステム）の情報が正しくない等、（契約の際に）偽情報が許されている状況は、業界も含めて改善していくべき。」【第2回WG構成員発言】

２　政府による効果的な法執行(b)その他の前回改正事項の評価

(ii) 外国執行当局への情報提供（法第30条）

現状

・総務大臣は、特定電子メール法に相当する外国の法令を執行する外国当局に対し、外国当局の法執行等に資する情報の提供を行うことができる。（※前回改正で新規追加）

論点

○　これまで、法30条に基づく、外国執行当局への情報提供がされていないが、制度上見直しの必要があるか。

※「特定電子メール法第30条について、現在、働きかけをしているが、（相手があることもあり）実現には至っていない状況。」

【第１回WG事務局発言】

※　法第三十条　総務大臣は、この法律に相当する外国の法令を執行する外国の当局に対し、その職務（この法律に規定する職務に相当するものに限る。次項において同じ。）の遂行に資すると認める情報の提供を行うことができる。

２　前項の規定による情報の提供については、当該情報が当該外国執行当局の職務の遂行以外に使用されず、かつ、次項の規定による同意がなければ外国の刑事事件の捜査（その対象たる犯罪事実が特定された後のものに限る）又は審判（同項において「捜査等」という。）に使用されないような適切な措置がとられなければならない。

３　総務大臣は、外国執行当局からの要請があったときは、次の各号のいずれかに該当する場合を除き、第一項の規定により提供した情報を当該要請に係る外国の刑事事件の捜査等に使用することについて同意をすることができる。

一　当該要請に係る刑事事件の捜査等の対象とされている犯罪が政治犯罪であるとき、又は当該要請が政治犯罪について捜査等を行う目的で行われたものと認められるとき。

二　当該要請に係る刑事事件の捜査等の対象とされている犯罪に係る行為が日本国内において行われたとした場合において、その行為が日本国の法令によれば罪に当たるものでないとき。

三　日本国が行う同種の要請に応ずる旨の要請国の保証がないとき。

４（略）

２　政府による効果的な法執行(b)その他の前回改正事項の評価

(iii)送信委託者への措置命令等(法第7条等)

現状

・送信者だけではなく、送信委託者に対して、報告徴収、措置命令等を行うことが可能。

（※前回改正で「送信委託者」を追加）

論点

○　これまで、送信委託者に対する行政処分（措置命令）は行われていないが、改善すべき点はあるか。

※　現在の「特定電子メールの送信等に関するガイドライン」では、以下のように記述されている。
『「送信者」とは、「電子メールの送信をする者」であり、電気通信としての電子メールを発信する操作の主体となる者（団体を含む。）と解される。「送信委託者」とは、「電子メールの送信を委託した者」であり、電子メールの送信に関し送信先や送信事項について一定の指示をしている者であると解される。したがって、例えば、単に広告の依頼を行っているだけの者や自らは電子メールを発信する操作をせずに他人に電子メール送信のためのシステムを提供しているだけのメール配信サービス事業者・配信ASP（Application Service Provider）事業者は、送信者や送信委託者には該当しない。』

※　「（送信委託者に対する行政処分の実績がないのは）結果として、たまたまそうなったと思う。措置命令まで行かなくても、我々が警告をしていく段階で送信を止めている送信者・送信委託者というのもかなりいるので、結果として送信委託者には命令まで行ったことがないのにすぎないものと思う。」【第1回WG事務局発言】

２　政府による効果的な法執行(b)その他の前回改正事項の評価

(iv)罰則の強化(法第34条・35条・37条)

現状

・オプトイン規制違反、表示義務違反、架空電子メールアドレスによる送信
　→　措置命令

・送信者情報の偽装、措置命令違反(同意の記録保存義務を除く)
　→　１年以下の懲役または百万円以下の罰金(法人:三千万円以下の罰金)。

・措置命令違反(同意の保存記録義務)、報告徴収・立入検査忌避等
　→　百万円以下の罰金(法人:百万円以下の罰金)

(※前回改正で、法人に対する罰金額を100万円以下から3000万円以下に引き上げ)

論点

○　罰則の更なる強化(罰金額の引き上げ、法第３条１項違反の直罰化等)を図る必要があるか。

※　刑事罰を課せられた事案　：　４件(送信者情報の偽装(法第５条違反))【第1回WG事務局資料】

※　措置命令違反、報告徴収・立入検査忌避等による罰金刑　：　措置命令を受けても改善せず、報告徴収等の忌避をして罰則を適用された事例はない。

警察による摘発
（送信者情報を偽って広告宣伝メールを送信したことによる摘発）

摘発年月	概要	判決内容
2006年5月	千葉県警が東京都内の男性を逮捕	懲役8ケ月、執行猶予3年。法人については罰金80万円。
2006年8月	大阪府警が大阪市内の元会社社長等を書類送検	元社長に罰金100万円、従業員1名に罰金50万円。
2007年1月	千葉県警が東京都内の会社社長等を逮捕	2名に懲役8ケ月、執行猶予4年。 1名に懲役6ケ月、執行猶予5年。 1名に懲役6ケ月、執行猶予3年。
2008年2月	警視庁が東京都内の男性を逮捕	懲役6ケ月、執行猶予3年。

２　政府による効果的な法執行(c) その他の検討事項

(i)特定電子メールの範囲(法第2条)

現状

・特定電子メールの範囲は、営利を目的とする団体及び営業を営む個人が自己又は他人の営業につき、広告宣伝を行うための電子メール

論点

○　特定電子メールの範囲を、「広告宣伝メール」以外にも拡大する必要があるか。

※　諸外国でも、その多くが、「広告宣伝メール」のみを規制の対象としている。(17ページ参照)

諸外国における迷惑メールの範囲

米国	カナダ	英国	ドイツ
商業電子メール（商業的製品、サービスの商業広告または販売促進を主たる目的とした電子メール）	以下の内容を含む商業電子メール ・商品、サービス、土地等の販売、賃貸、物々交換の申し出。 ・事業、投資、賭博の機会の提供。 ・上記に関連することを行う人物を宣伝すること	DM目的の電子メール	商業電子メール（直接的、間接的に企業等の商品、サービスの販売促進等のために送信される電子メール）
フランス	**オーストラリア**	**韓国**	**中国**
DM目的の電子メール	以下の内容を含む商業電子メール ・品物、サービスの供給申出、宣伝・販促、品物・サービスのサプライヤー等の宣伝 ・土地、土地の権利の供給申出、宣伝・販促、土地、土地の権利のサプライヤー等の宣伝 ・ビジネス機会、投資機会の提供申出、宣伝、サプライヤーの宣伝 ・財産の不正取得を詐欺により支援すること ・経済的利益の不正取得を詐欺により支援すること ・不正利益の取得を支援すること	営利目的の広告電子メール	商業広告の電子メール

2　政府による効果的な法執行 (c) その他の検討事項

(ii) 禁止事項

現状

現在、特定電子メール法では、オプトイン規制の他、以下の禁止事項が規定されている。

・電子メールの送信者情報の偽装の禁止（法第5条）

・架空電子メールアドレスによる送信の禁止（法第6条）

論点

○　現在禁止されている行為類型以外に、さらに禁止が必要な類型はあるか。

※　諸外国の一部では、例えば、ソフトウェアによる電子メールアドレスの自動収集・販売、同意のない他者のPCへのプログラムのインストールの禁止、オプトアウト通知受信後の送信停止期限、携帯電話に広告性の電子メールを午後9時から翌日の午前8時までに送信する場合は、オプトインとは別の事前同意を得る等の規制を設けている例がある。

諸外国における迷惑メールの規制類型（日本にない迷惑メール規制）

1. 電子メールアドレスの自動収集・販売等

	規制類型	日本国内法での対応
米　国	他人のウェブサイトから自動取得したアドレス及び自動生成したアドレスを使用した送信の禁止 ［PC向けメール］	個人情報保護法第16条（事前の同意）、電子メールが送信された場合（メルアド公開者が特定電子メールを送信しないよう求めていた場合）、特定電子メール法第3条
フランス	メールアドレスの不正収集・使用禁止	
オーストラリア	① メールアドレスの自動収集ソフトの供給、取得、使用の禁止	
	② メールアドレスの自動収集ソフトを使用して作成されたメールアドレスリストの供給、取得、使用の禁止	
韓　国	事前同意なしのプログラムによる自動電子メールアドレスの販売・収集の禁止	
中　国	自動収集又は自動作成したメールアドレスの販売等及びこれによる送信の禁止	

2. 同意のない他者のPCへのプログラムのインストール禁止等

	規制類型	日本国内法での対応
米　国	他人のコンピュータに無許可でアクセスし、商業電子メールの送信禁止。 ［PC向けメール］	不正アクセス禁止法第3条
カナダ	同意なく他人のコンピュータに以下の機能を持つプログラムのインストール禁止。 ・コンピュータに保存された個人情報の収集 ・所有者のコンピュータセキュリティを妨げる ・コンピュータの設定を所有者が知らないうちに変更または妨げる ・コンピュータに保存されているデータについて、所有者の正当な使用を妨害する ・コンピュータの所有者の許可無しに、他のコンピュータと通信する。 ・コンピュータの所有者の許可無しに、第三者がコンピュータを起動できる	
中　国	電子メール送信のため、同意なく他者のコンピュータの使用禁止	

3. オプトアウト通知受信後の送信停止期限等

	規制類型	日本国内法での対応
米　国	①オプトアウト受信後、10営業日経過後も、商業電子メールの送信を行うことの禁止［PC向けメール］ ②オプトアウト受信後、10日経過後も、商業電子メールの送信を行うことの禁止［携帯電話向けメール］	ー
	③商業電子メール送信後、30日以上、オプトアウトができる状態にする。 ［PC向け、携帯電話向けメール］	
カナダ	①　オプトアウト受信後、10営業日経過後も、商業電子メールの送信を行うことの禁止	
	②　オプトアウトのための電子メールアドレス、WEBページが商業電子メールが送信後60日間有効であることを保証。	
	③　送信者に対する連絡先が商業電子メール送信後60日間有効であることを保証	
中　国	受信同意時から30日間は、オプトアウトを受け付けるためのコンタクトポイントを維持することを義務づけ	

4. その他

	規制類型	日本国内法での対応
米　国	①　実際の登録者を実質的に偽る情報を使用し、5件以上の電子メールアカウント、もしくは2件以上のドメイン名について登録を行い、複数の商業電子メールの送信禁止。［PC向けメール］	ー
	②　5件以上のIPアドレスの登録者またはその合法的な継承者であると偽り、当該アドレスから複数の商業電子メールの送信の禁止。［PC向けメール］	ー
	③　性的内容を含む商業電子メールには、警告ラベルを貼らなければならない。［PC向けメール］	ー

諸外国における迷惑メールの規制類型（日本にない迷惑メール規制）

	規制類型	日本国内法での対応
韓　国	①　携帯電話宛に広告性の電子メールを午後9時から翌日の午前8時までに送信する場合は、オプトインとは別の事前同意を得なければならない	―
	②　オプトアウトする際に発生する金銭的費用を受信者が負担しないような措置を取らなければならない	―

２　政府による効果的な法執行(d) 執行体制

現状

・　迷惑メールに関する情報提供件数は約586万件（21年度）。
・　迷惑メール対策に資するため、昨年度、迷惑メール分析システムを開発、今年度、通報システム（プラグインソフト）を開発中。

論点

○　迷惑メールの執行を支援するために、その他、どのような手段が必要か。

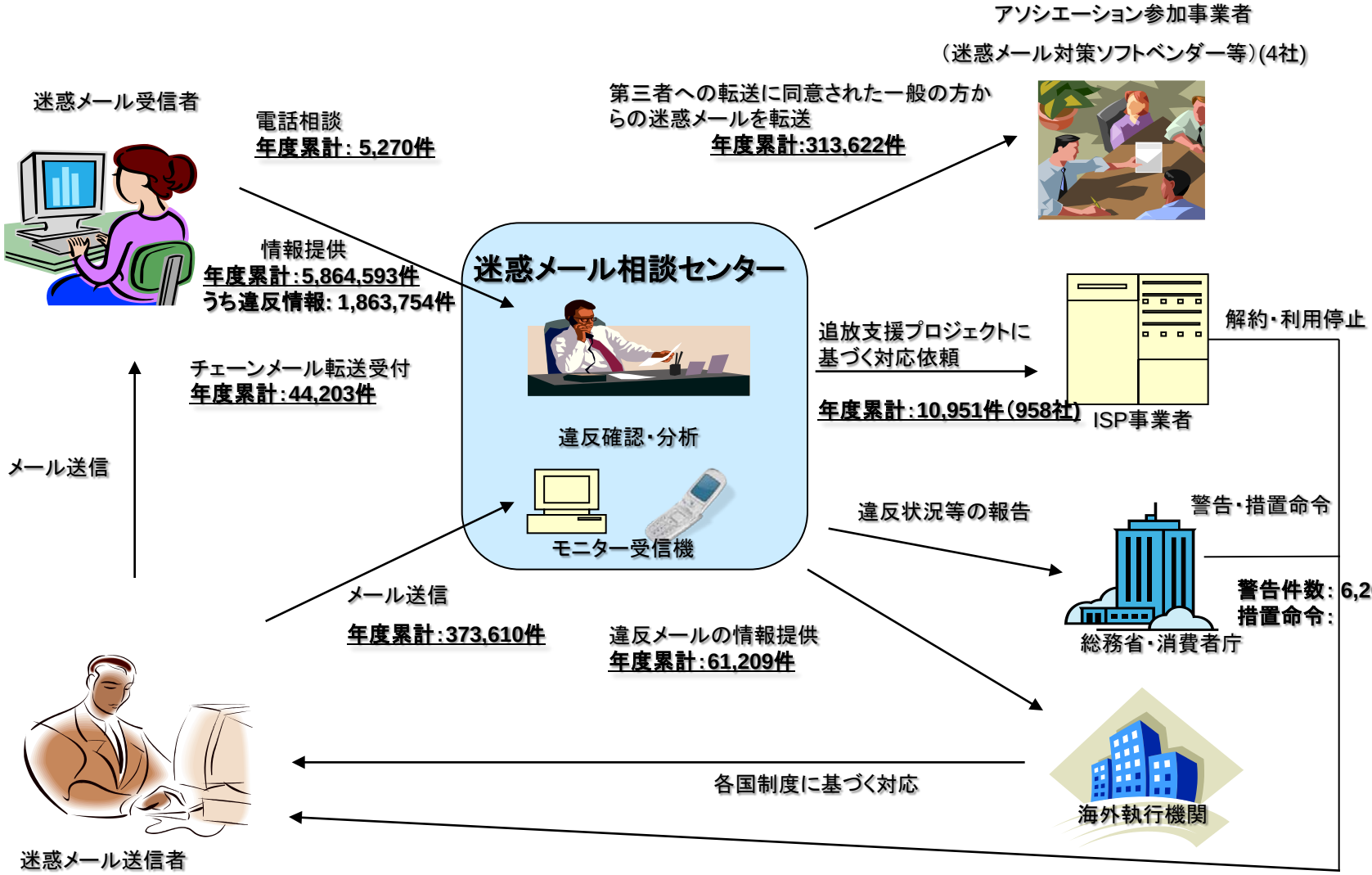
※「（財）日本データ通信協会で受けている）迷惑メール受信者からの情報提供のうち、法違反に関する以外のものが66％ある。具体的には、66％のうち、1／3が外国メール、1／3が文字化け、1／3が情報不足メールとなっている。【第2回WG構成員発言】

※「消費者生活センターで迷惑メール相談の際には連絡先を周知しているが、消費者は携帯事業者1箇所に連絡して終了してしまうケースが多い。そうすると、（財）日本データ通信協会の迷惑メール相談センターには情報が行かない」【第2回WG構成員発言】

※「（携帯事業者間で行っている情報交換は）迷惑メール送信者の情報交換なので、さほど数は多くない。一方、消費生活相談センターに寄せられる情報は受信された迷惑メールの情報。迷惑メールの情報はどの事業者も受けており、特に迷惑メールは大量送信されるので、受信者は多数となるため、事業者各社で同じような情報を受けている。従って、ISP事業者としては、特に情報交換をしなくても、同じ情報が共有されている状況だと考えている。実際、（財）日本データ通信協会及び（財）日本産業協会からも情報提供はくるが、契約者より情報がすでにきているため、新しい情報というのは見あたらない。【第2回WG構成員発言】

※　諸外国の一部では、迷惑メール対策に資するため、通報・分析システムを運用中【第3回WG事務局資料】

（財）日本データ通信協会　迷惑メール相談センター業務（H21年度実績）



諸外国における迷惑メールの通報・分析システム

	フランス	オーストラリア	
システム名	Signal Spam	Spam Matters	Spam Intelligence Database(SID)
概　　要	・受信者が受信した迷惑メールを、オンラインによりワンクリックで担当機関に報告することが可能。 ・担当機関では、通報された情報を分析し、ISPに提供する。	・受信者が受信した迷惑メールを、オンラインによりワンクリックで担当機関に報告することが可能。	・Spam Matters等によって得られたスパム情報を分析するためのシステムであり、アンチスパムチームの活動に役立てるとともに、ISPに情報を提供する。
使用方法	プラグインソフトをメールソフトに組み込んで使用して、情報提供する。 （対応メールソフト） Microsoft Outlook 2003、2007 Thunderbird2.x、3.x	プラグインソフトをメールソフトに組み込んで使用して、情報提供する。 （対応メールソフト） Microsoft Outlook 2003、2007 Microsoft Outlook Express 5,6	ー
導入時期	2007年	2006年	2009年
利用状況	サービス開始後、約5万人のユーザーから、約1,400万件の通報を受ける（2008年末時点）。	サービス開始後、約29万人のユーザーから約4,000万件の通報を受ける。（2009年7月時点）	不明

	韓国
システム名	スパム対応システム
概　　要	・迷惑メールの情報提供を受けて、担当機関で情報を分析し、ISP等に発信者情報の提供を要請。情報入手後、発信者に直接連絡を取り、迷惑メール送信の事実を確認し、放送通信委員会に処分を依頼。
使用方法	携帯電話スパム簡易届出サービス（簡単な操作でスパムを担当機関に転送できる）、WEB申告等を使用して、情報提供する。
導入時期	2003年
利用状況	約3,562万件の通報を受ける（2009年）

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。

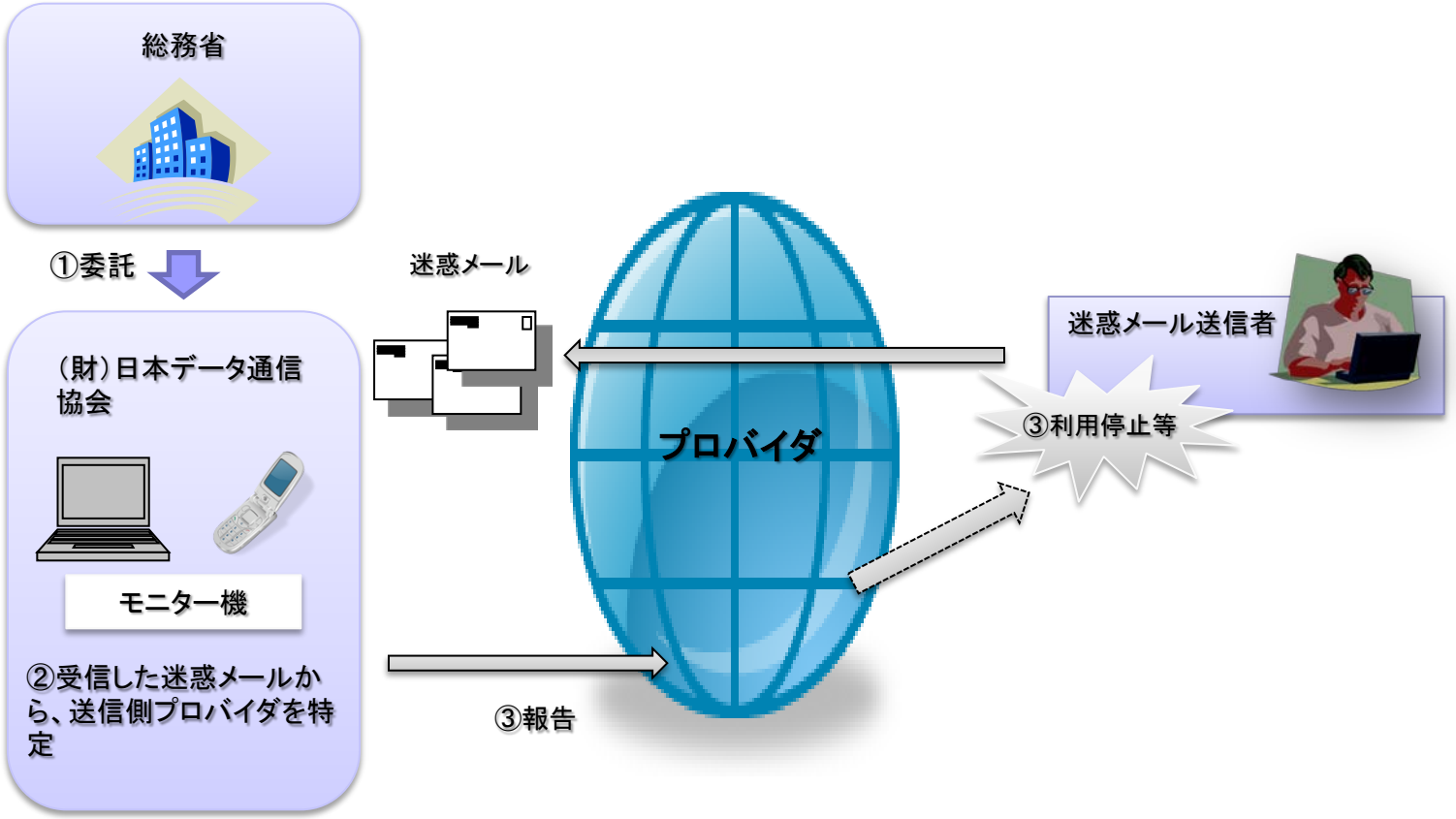
※「迷惑メール追放支援措置プロジェクト」に伴うISPへの対応依頼：10,951件（958社、21年度実績）

※「（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

・　広告関係事業者の取組みとして、電子メール広告に関するガイドライン等を定め、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。

※　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。

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

論点

P

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

論点

P

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】

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

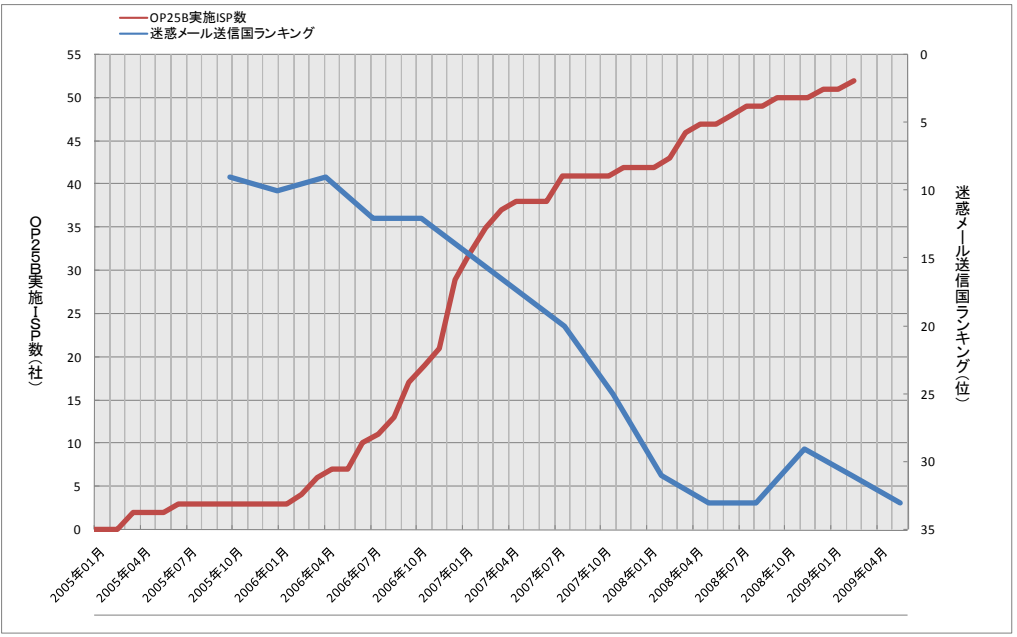
○ 国内ISPでのさらなる導入を図るために、どのような取組をすべきか。

○ OP25Bを導入していても迷惑メールが送信される事態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】

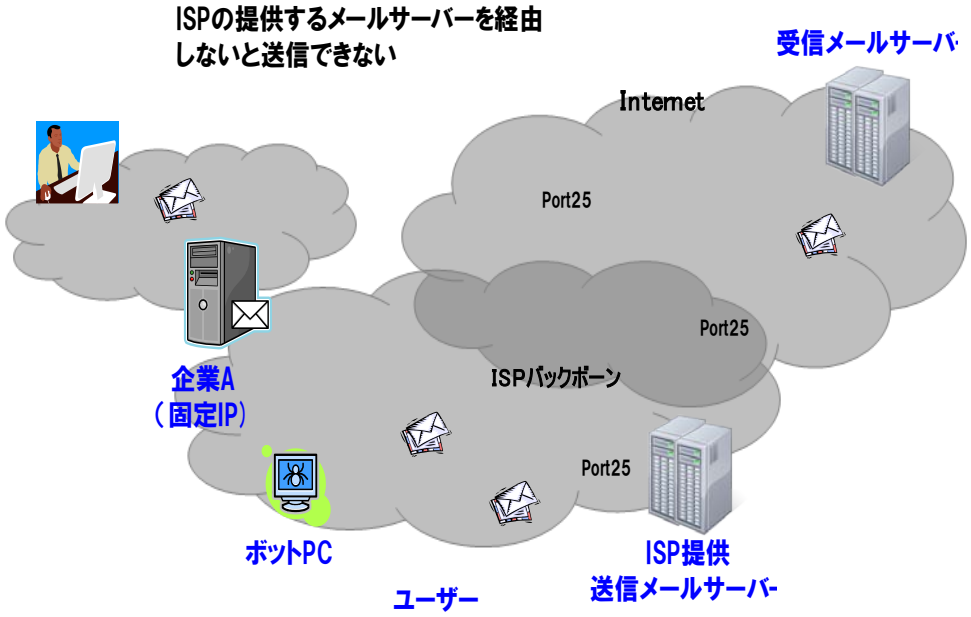
※ 国内発の迷惑メールを更に減少させるため、OP25B未導入の国内ISPへの対応が必要か。

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1%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。

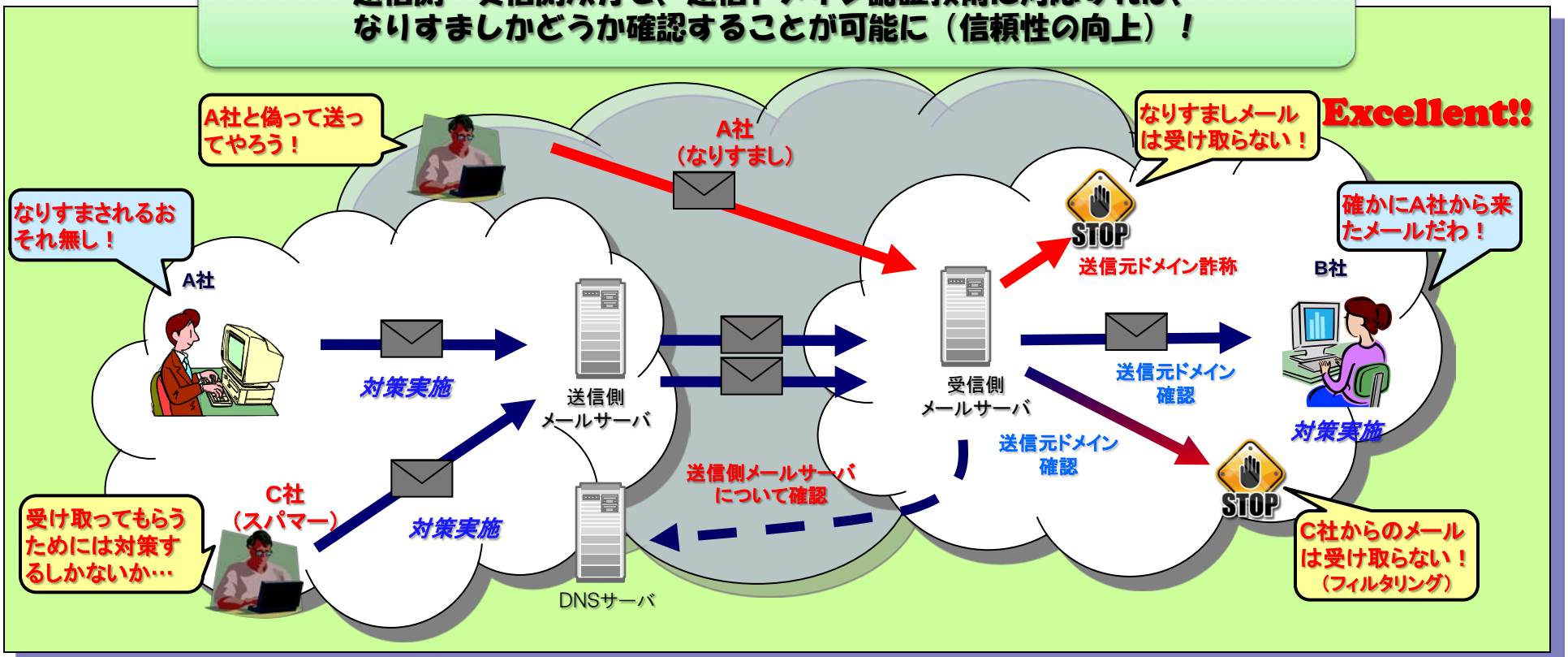
※ 民間事業者において、DKIMの普及促進を図るため、「Japan DKIM Working Group」が設立(2010.11.15)

※ (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

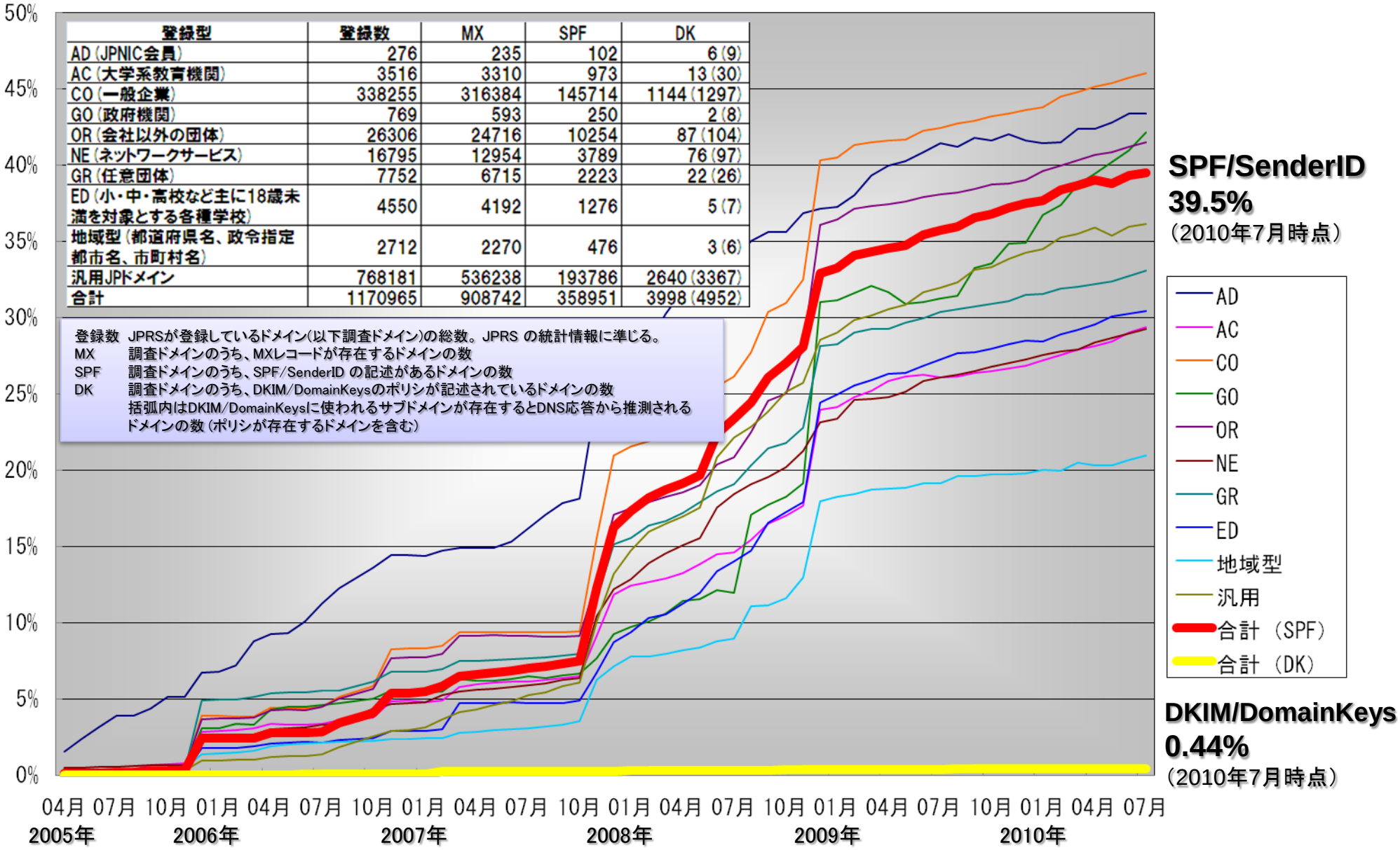
【送信側】送信するメールが受け取られやすく
- 自ドメインの信頼性の確保
- 受信側が対応していれば、受け取られやすくなる

【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	235	102	6（9）
AC（大学系教育機関）	3516	3310	973	13（30）
CO（一般企業）	338255	316384	145714	1144（1297）
GO（政府機関）	769	593	250	2（8）
OR（会社以外の団体）	26306	24716	10254	87（104）
NE（ネットワークサービス）	16795	12954	3789	76（97）
GR（任意団体）	7752	6715	2223	22（26）
ED（小・中・高校など主に18歳未満を対象とする各種学校）	4550	4192	1276	5（7）
地域型（都道府県名、政令指定都市名、市町村名）	2712	2270	476	3（6）
汎用JPドメイン	768181	536238	193786	2640（3367）
合計	1170965	908742	358951	3998（4952）

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）



SPF/SenderID
39.5%
（2010年7月時点）

DKIM/DomainKeys
0.44%
（2010年7月時点）

http://member.wide.ad.jp/wg/antispam/stats/index.html.ja(2010年7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】

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

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））

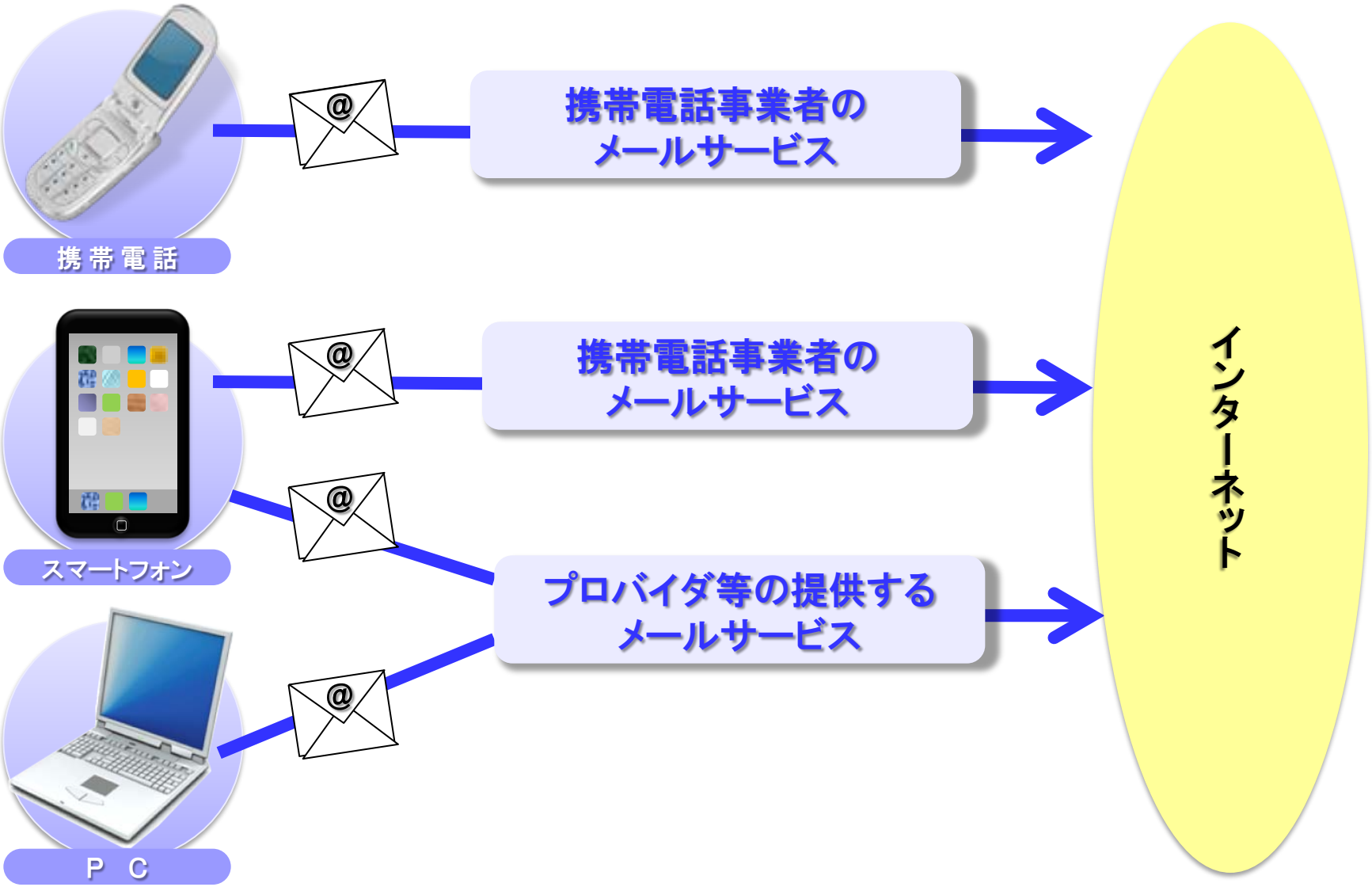
論点

○ 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。



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】

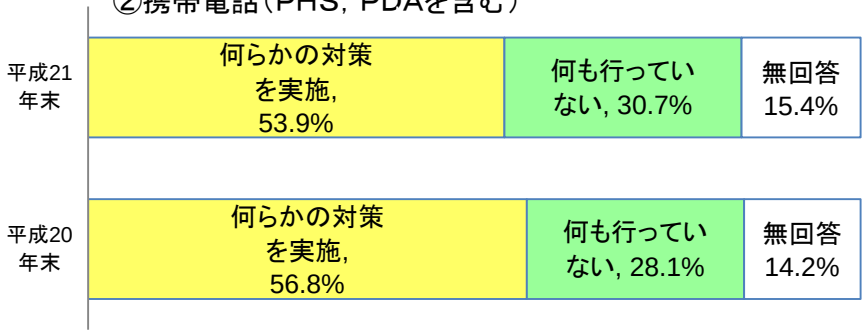
※　単なる広告宣伝ではなく、リンク先をクリックすることでマルウェア（ウィルス）感染を狙うなど、セキュリティ上の脅威となるメールも増大している（第2回WG　JAIPA資料）ことから、より一層の周知啓発が必要ではないか。

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。

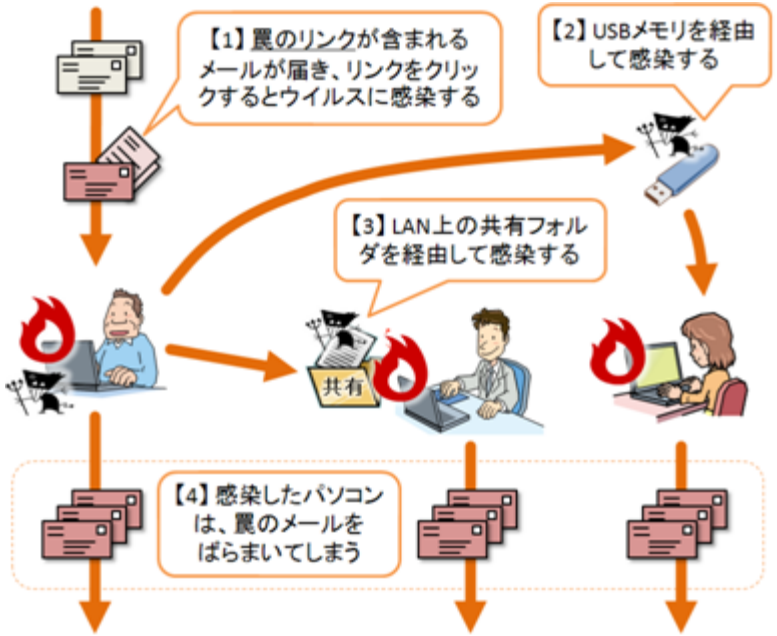
①パソコン

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
(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

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、MAAWG(国際的な民間の迷惑メール対策団体)、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。

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

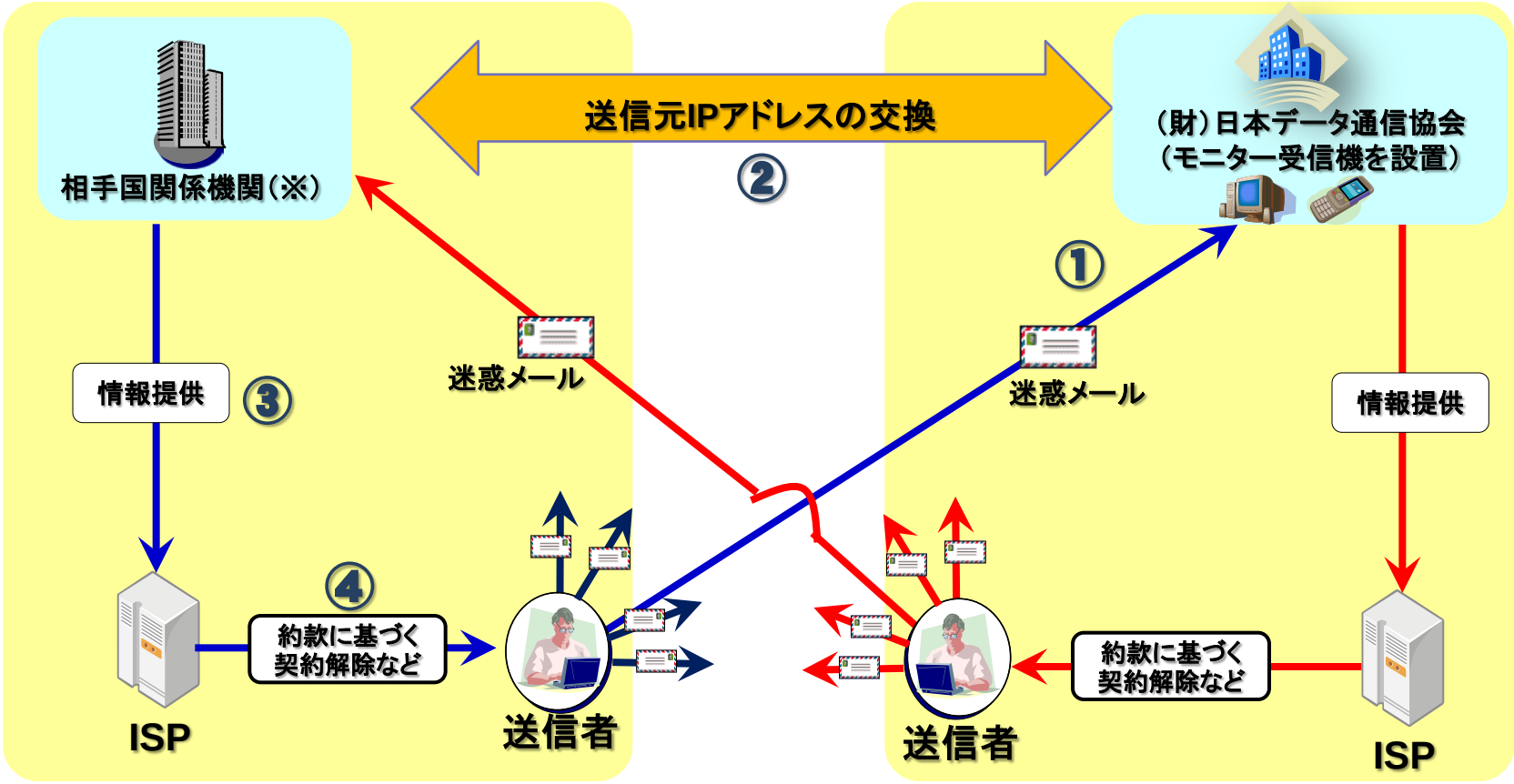
○ オーストラリア
・日豪情報通信政策協議等で迷惑メール対策について意見交換。

○ 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。

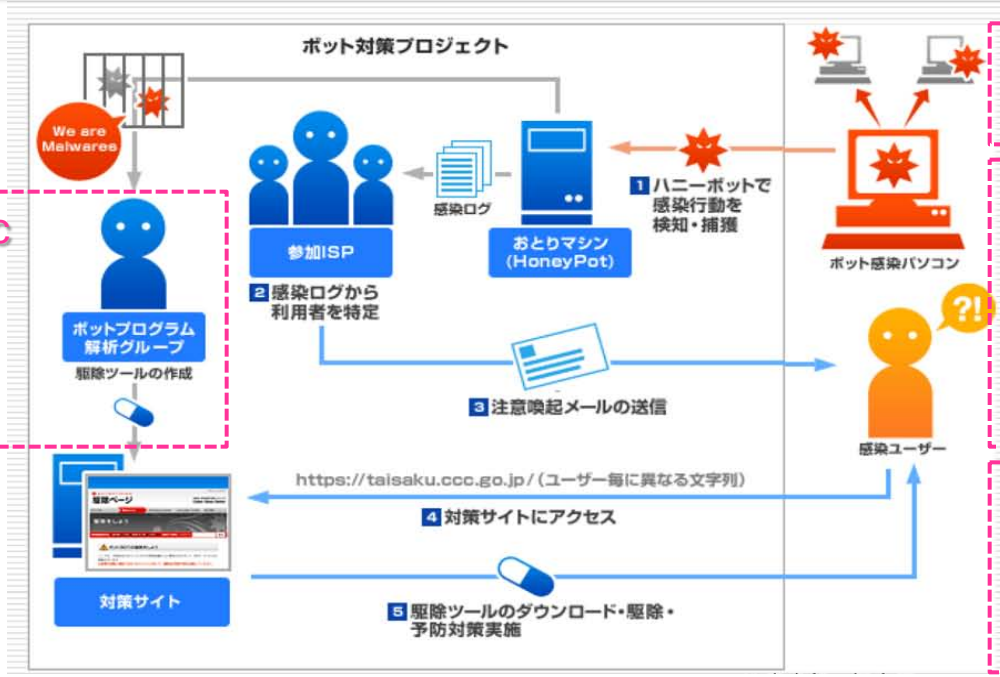


①（財）日本データ通信協会のモニター受信機で迷惑メールを受信
②提供された迷惑メールの送信元ＩＰアドレスを分析し、中国発の場合は、送信元ＩＰアドレスを中国インターネット協会（ＩＳＣ）に提供
③送信元のＩＳＰにＩＰアドレスを提供
④送信元ＩＳＰにおいて、送信者との契約解除などの措置

※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。

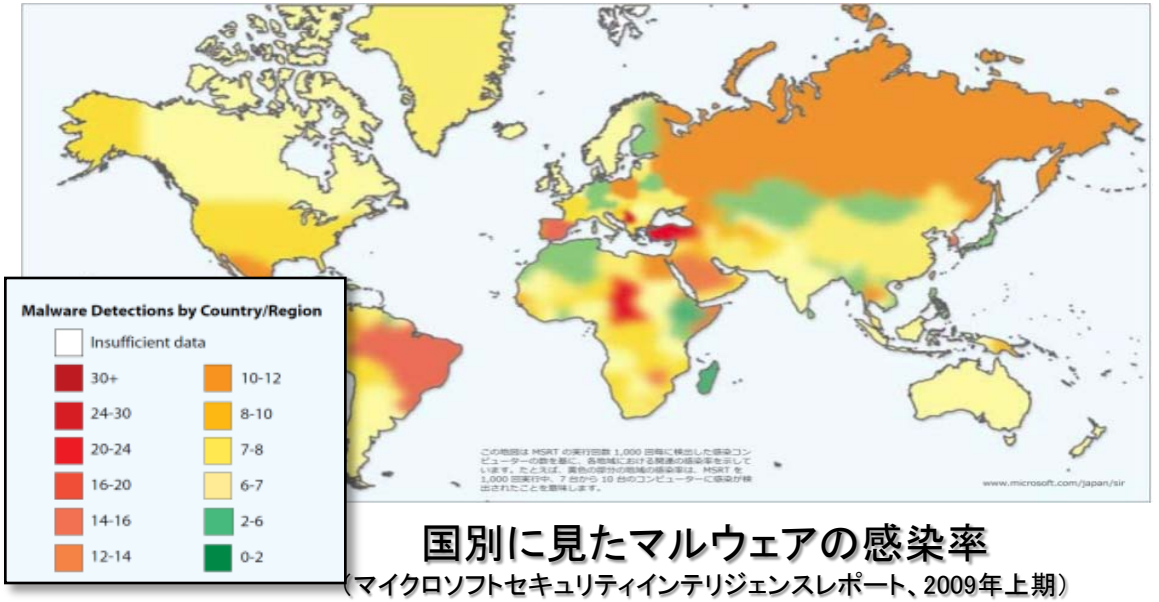
ウイルス感染者を減らし、世界トップクラスの低ボット感染率を実現

○ 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