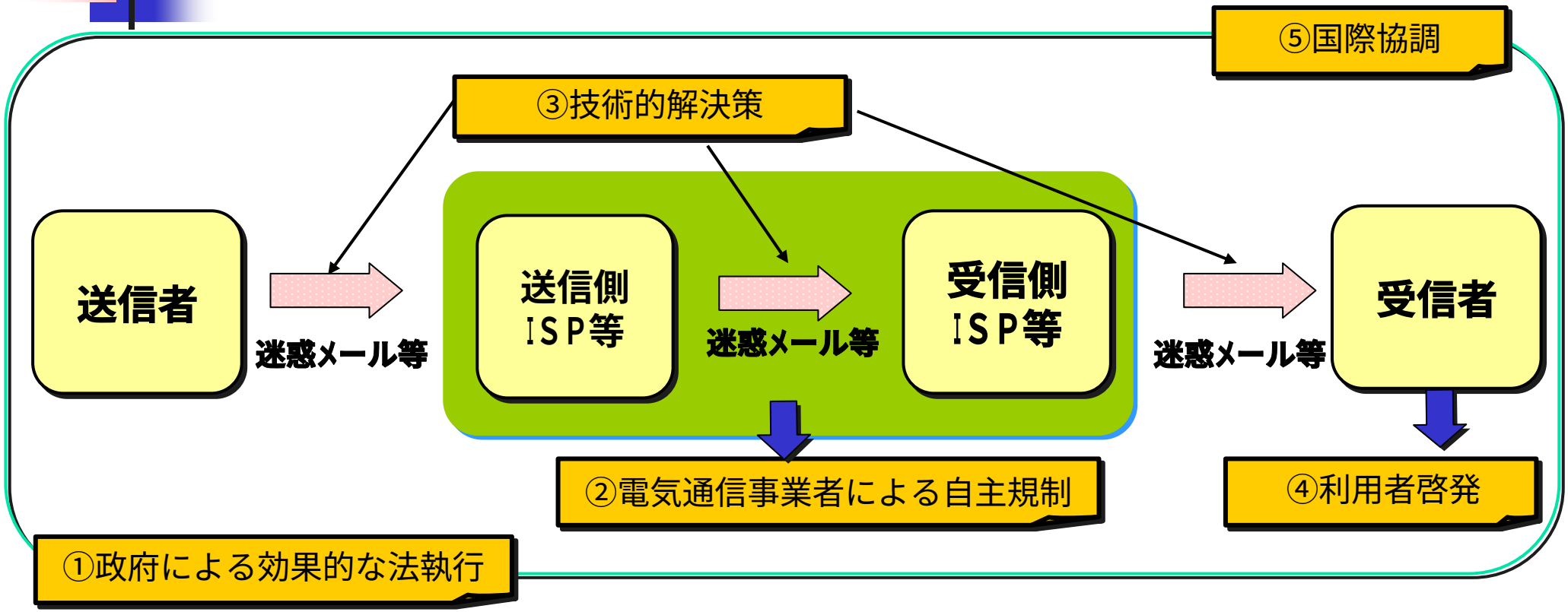
資料　4

迷惑メールに係る対応方策の検討について
(論点整理)

事　　務　　局

迷惑メールに関する対応策の検討の方向性



・迷惑メールによる諸問題に対応するためには、上記①～⑤のいずれか一つだけの取り組みだけでは困難。
→スパム対策は“ No silver bullet ”（特効薬はない）であり、多面的な対応が不可欠。
できるところから行動すべき（2004年2月開催のOECDスパムワークショップ）

法制度見直し等の特定の部分のみに着目するのではなく、他の部分において可能な取り組みとの連携を踏まえ、総合的な対応方策を検討する。

迷惑メールに関する対応策の具体例

①政府による効果的な法執行

- ショートメッセージサービス（ＳＭＳ）による迷惑メール等を規制対象に追加
- 特に悪質な違反行為に直接刑事罰を科すことを可能とする直罰化

②電気通信事業者による自主規制

- 法令や約款に基づき悪質な迷惑メール送信者に対し利用停止等の措置を実施
- 特定のＩＳＰ等だけでなく多くの事業者が連携して迷惑メール送信を困難化

③技術的解決策

- メール送信者の情報を認証する送信者認証技術の導入

④利用者啓発

- ＩＳＰ等により提供されるフィルタリングサービス等の積極的な活用

⑤国際協調

- 迷惑メール対策に関する諸外国との協調推進（MoU締結等）

1　政府による効果的な法執行①

「特定電子メール」等の定義の見直し

- 現在、通常のインターネット経由のメール送信に用いられるＳＭＴＰを利用した電子メールのみが対象とされているが、最近におけるＳＭＳを利用した広告宣伝メールの増加に鑑み、特定電子メールの定義にＳＭＳを含むように措置することが考えられる。
- 送信の対象として、現在は個人に限定（ただし、事業のために利用している場合は対象外）しているが、法人あるいは事業で利用している個人のメールアドレスあての送信についても対象とすることが考えられる。（法第2条関係）

論点

- 各社で様々なサービス内容が存在するＳＭＳの範囲をどのように画定するか。
- ＳＭＳを対象とする場合、表題部が存在しなかったり、文字数等表現能力が限定されていたりすることにより、現在ＳＭＴＰによるメールに課している表示義務を満たすことが困難となる場合があるが、異なる内容の表示義務を設けるべきか。
- 端末間で直接情報の送受信を行い事業者のサーバを経由しない場合、受信回避のための技術的対応が困難ではないか。
- 事業用メールアドレス等に対象を拡大する場合、事業を営む者の間でのメール送受信について、たとえば一定の継続的な取引関係にある場合を除外するか否かなど、具体的にどの範囲までを対象とすべきか。

SMTP：シンプルメールトランスファープロトコル。インターネットで電子メールを送信する際に、一般的に用いられている通信方式。
SMS　：ショートメッセージサービス。携帯電話同士で、短い文字メッセージを電話番号あてに送受信できるサービス。

SMTP以外の通信方式を使った主なメールサービス（SMS）一覧

○ **各社共通の特徴**
- 受信者の電話番号あてに送信
- 件名がない（ボーダフォンのロングメール等を除く）
- 事業者側で、フィルタリング等を行うことが技術的に困難

	サービス名	文字数	送信料金※	備　考
NTTドコモ	ショートメール	50文字	5円	固定電話、公衆電話等からも送信可
	SMS（FOMA）	70文字	5円	
au	Cメール	50文字	3円	
ボーダフォン	スカイメール	64文字	2円	固定電話、公衆電話等からも送信可
	ロングメール	3,000文字	4円	件名入力可能
	SMS（VGS）	70文字	5円	
TUKA	スカイメール	64文字	5円	固定電話、公衆電話等からも送信可
DDIポケット	ライトメール	45文字	6円	固定電話、公衆電話等からも送信可
	DXメール	1,000文字	10円	固定電話、公衆電話等からも送信可 一部機種のみ件名入力可能
	Pメール	半角20字	6円	固定電話、公衆電話等からも送信可

※「送信料金」は、料金プランにより異なる場合あり

1　政府による効果的な法執行②

架空アドレスあてメール送信を禁止する範囲の見直し

- 現在、架空アドレスあてのメール送信行為について、①自動アドレス生成ソフトウェアの使用により得たアドレスであること、②自己又は他人の営業についての広告又は宣伝の目的であること、が要件とされている。
- 電気通信事業者の設備に与える本来不要な過大な負荷については、大量の宛先不明メールが送信されている限りその送信手法による差異はないことから、この範囲を拡大することが考えられる。（法第5条関係）

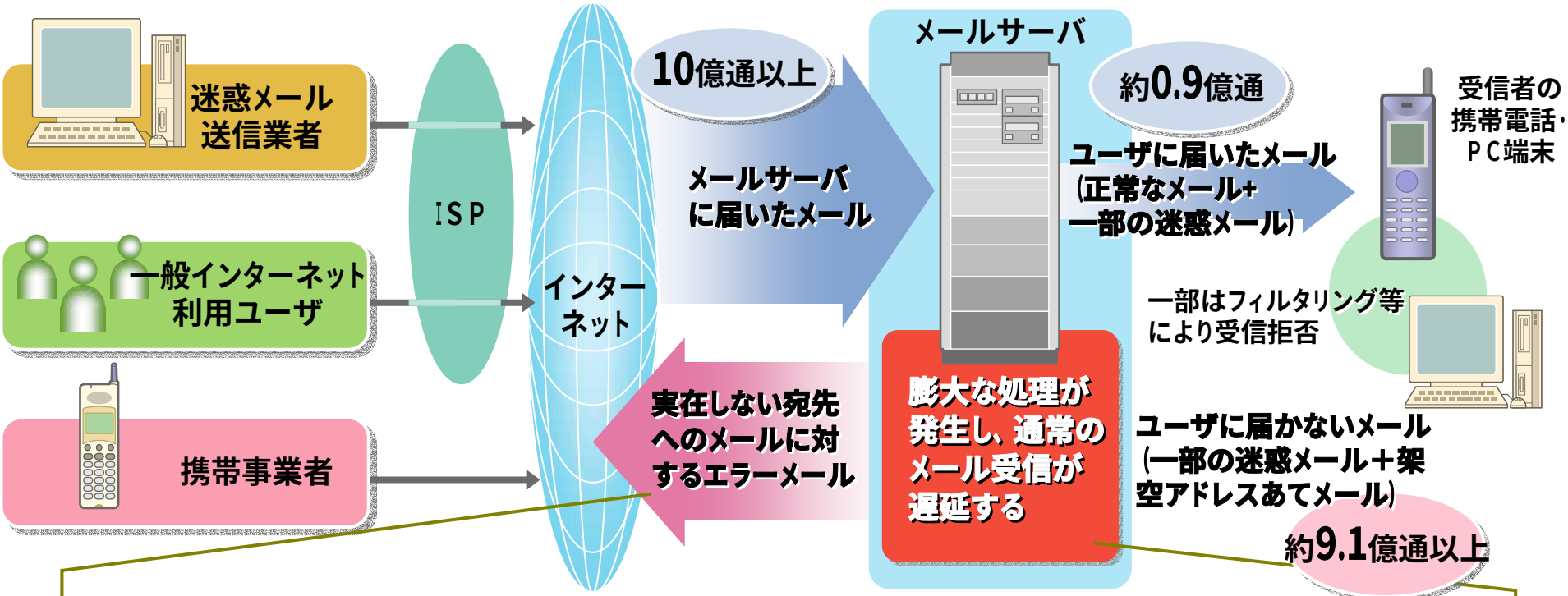
論点

- 上記①について、自動アドレス生成ソフトウェアを使用する場合以外のアドレス生成手法としては、どのようなものが考えられるか。
- 上記②について、広告宣伝目的のメール送信以外に、大量に架空アドレスあてにメールを送信する行為としては具体的にどのようなものが考えられるか。
- 架空アドレスあての送信とは異なるが、web上を巡回して自動的にメールアドレスを収集して大量に送信する行為について取り締まりの対象とする必要はないか。

（架空電子メールアドレスによる送信の禁止）
第五条　送信者は、自己又は他人の営業につき広告又は宣伝を行うための手段として電子メールの送信をするときは、電子メールアドレスとして利用することが可能な符号を作成する機能を有するプログラム（電子計算機に対する指令であって一の結果を得ることができるように組み合わされたものをいい、総務省令で定める方法により当該符号を作成するものに限る。）を用いて作成した架空電子メールアドレス（符号であってこれを電子メールアドレスとして利用する者がないものをいう。第十条及び第十六条第一項において同じ。）をその受信をする者の電子メールアドレスとしてはならない。

架空アドレスあてに大量にメールを送信することによる電気通信事業者の設備に対する過剰な負荷について

ＰＣから行われる携帯電話やＰＣ端末への架空アドレスあての大量送信が集中した場合、たとえば１日にユーザに届くメールが約１億通程度であるのに対し、ユーザに届かないメールがその１０倍もの規模に達する場合もある。



②宛先が実在しないメール等に対してエラーメールを返す場合には、さらに膨大な処理が行われる。
　また、送信者の情報を偽ることによりこのエラーメールを利用して無関係な第三者にエラーメールとして迷惑メールを送りつける手法もみられる。

①宛先が実在しない大多数のメールについても処理を行う必要があるため、設備に過大な負荷が生じることになる。
　このため、一般ユーザが送信したメールの処理についても遅延してしまう。

本来処理する必要のない大量の架空アドレスあてのメールを処理するために、電気通信事業者においていわば過剰な設備を保有・運用する必要が生じており、業務上も経費上も大きな負担となっている。

1　政府による効果的な法執行③

悪質な違反行為の直罰化

- 現在、特定電子メール法に違反する行為を行った場合には総務大臣の措置命令がまず行われることとなっており、その命令に反してさらに違反行為を行った者に対してはじめて刑事罰を科すものとしているが、迷惑メール送信行為の巧妙化・悪質化や、それに伴う送信者の特定の困難さから、措置命令の発出そのものが困難である。
- 現行制度に違反するような行為など、迷惑メールの送信に関して特に違法性の高い行為であると考えられるものについて、総務大臣の措置命令を経ずに直接刑事罰を科すことができるよう措置することが考えられる。

（第3条～第6条、罰則規定関係）

論点

- 直接刑事罰の対象となる禁止行為として、禁止範囲の限定性・明確性が要求されるため、現行規定における禁止対象行為の書きぶりに比較して特に悪質な行為に限定する必要があるが、具体的にはどのような行為が想定されるか。
- 刑事罰をもって取り締まるべき高度の違法性や被害の深刻性がどの程度あるか。
- 偽計業務妨害罪（刑法第２３３条）や電子計算機損壊等業務妨害罪（刑法第２３４条の２）等、既存の刑事罰の対象行為との合理的な整理が可能か。

1　政府による効果的な法執行④

オプトイン方式の採用

- 欧州指令においてオプトイン方式を採用した結果、英国をはじめとする欧州諸国においてはオプトイン方式が採用されている。また、オーストラリアにおいてもオプトイン方式が採用されている。
- 米国では基本的にオプトアウト方式を採用しているが、本年8月に公表されたＦＣＣルールにおいては、携帯電話あてに送信される商業広告メールに関してオプトイン方式が採用されている。
- 我が国においても、制度の枠組みを変更してオプトイン方式を採用することが考えられる。

論点

- オプトイン方式を採用する場合、オプトアウト方式を採用している現行制度の全面的な変更を意味することとなるが、オプトイン方式が取り締まりの枠組みとして明確に優れているという論拠があるか。
- オプトイン方式においては、受信者の同意の有無がもっぱら合法・違法のメルクマールとなるが、現在でも見られるように送信者が受信者の同意を得ていると主張している場合には結局違法性の認定が困難なのではないか。

オプトアウト方式：メールの送信者に受信拒否の意思を伝えた場合、以後の送信を認めない方式
オプトイン方式　：あらかじめメールの受信を承諾している者に対してのみ送信を認める方式

2　電気通信事業者による自主規制①

役務の提供を拒否できる範囲の見直し

- 現在、電気通信事業者が迷惑メールの送信について役務提供拒否することの正当性を規定しているのは、①電気通信設備に著しい障害を生じ、電気通信役務の提供に著しい支障を生ずるおそれがある場合について、②架空アドレスあてに送信した電子メールについての役務提供を拒否する場合、に限定されている。
- 迷惑メールが送信されることで電気通信事業者の設備に過大な負担がかかること等により役務提供拒否が正当化される事由は、必ずしも上記に限定されないと考えられることから、対象範囲を見直すことが考えられる。（法第１０条関係）

論点

- もともと電気通信事業法における役務提供義務の例外となる正当な拒否事由の一例として規定しているという性格のものであることから、明らかに役務提供を拒否することに正当性があると考えられる場合のみが対象となり、むやみに範囲を拡大することは不適当ではないか。
- 上記のほか、役務の提供を拒否した場合に拒否された送信者との間における紛争を防止するために、プロバイダ責任制限法のように電気通信事業者の損害賠償責任を限定するような措置は考えられないか。

（電気通信役務の提供の拒否）
第十条　電気通信事業者（電気通信事業法第二条第五号に規定する電気通信事業者をいう。）は、一時に多数の架空電子メールアドレスをその受信をする者の電子メールアドレスとして電子メールの送信がされた場合において、自己の電気通信設備（同法第二条第二号に規定する電気通信設備をいう。）の機能に著しい障害を生ずることにより電子メールの利用者に対する電気通信役務（同条第三号に規定する電気通信役務をいう。以下この条において同じ。）の提供に著しい支障を生ずるおそれがあると認められるときは、当該架空電子メールアドレスに係る電子メールの送信をした者に対し、その送信をした電子メールにつき、電気通信役務の提供を拒むことができる。

2　電気通信事業者による自主規制②

迷惑メール送信者情報の共有

- 迷惑メールの送信者は、特定のＩＳＰ等において利用停止等の処分を受けると、他のＩＳＰ等と契約して送信を継続しようとするものと考えられるが、ＩＳＰ等において迷惑メール送信者による利用を回避しようとする場合には、契約締結時に申込者が迷惑メールの送信者であるか否かを識別する必要がある。
- そのためには、各ＩＳＰ等の内部における利用停止等の履歴情報を保持するだけでなく、他のＩＳＰ等との間で当該情報を共有したり共同で利用できるようにしたりすることが考えられる。

論点

- 迷惑メールの送信者であっても、その契約者情報や送信したメールの内容等の情報は、個人情報として、また通信の秘密として、それぞれ保護される対象となるものが含まれていると考えられるため、どのような範囲の情報について、どのような要件を満たせばＩＳＰ等の間で共有等を行うことができるのか等の整理を行う必要がある。
- 利用停止等の処分を受けた送信者について、電気通信事業者と契約することが実質的にできなくなる場合には、過度の制約を設けるものとならないか。

※電気通信事業における個人情報の保護の在り方については、「電気通信事業分野におけるプライバシー情報に関する懇談会」（プライバシー懇談会）においても議論が行われており、本年8月に中間報告書がとりまとめられ、これを受けて「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」の改訂を行ったところ。
※来年4月1日から、個人情報保護法の全面施行が予定されている。

2　電気通信事業者による自主規制③

事業者による連携した対策の実施

- 特に多くの事業者が存在する固定系のＩＳＰにおいては、各社の迷惑メール対策の取り組みが必ずしも統一されていないため、特定のＩＳＰでは被害が防止できても、他の（対策をあまりとっていない）ＩＳＰでは送信することが可能である。
- このような場合、単に送信に利用しやすいＩＳＰに迷惑メール送信者が集中するだけの結果となり、被害防止の実効があがらないこととなるため、電気通信事業者において、できるだけ連携して一定程度以上の対策が広く行われるように体制を整備することが考えられる。

論点

- 特定のサービス実施を事業者に一律に要求することにより過度の負担を与えないように配慮する必要がある。
- どのようなサービスを提供するかは各事業者が競争して充実度をあらそう面も考えられることから、そのような創意工夫を害しないように配慮する必要がある。
- ＩＳＰをインターネットへの接続のためにのみ利用し、メールサーバを自前で用意して送信する（ＩＳＰのメールサーバを利用しない）場合には、ＩＳＰ側ではどのような送信行為が行われているかを認識できないため、ＩＳＰのメールサーバについて送信に一定の制限を加えたとしても、極めて限定的な効果しか期待できないのではないか。

3　技術的解決策

送信者認証技術の確立・普及

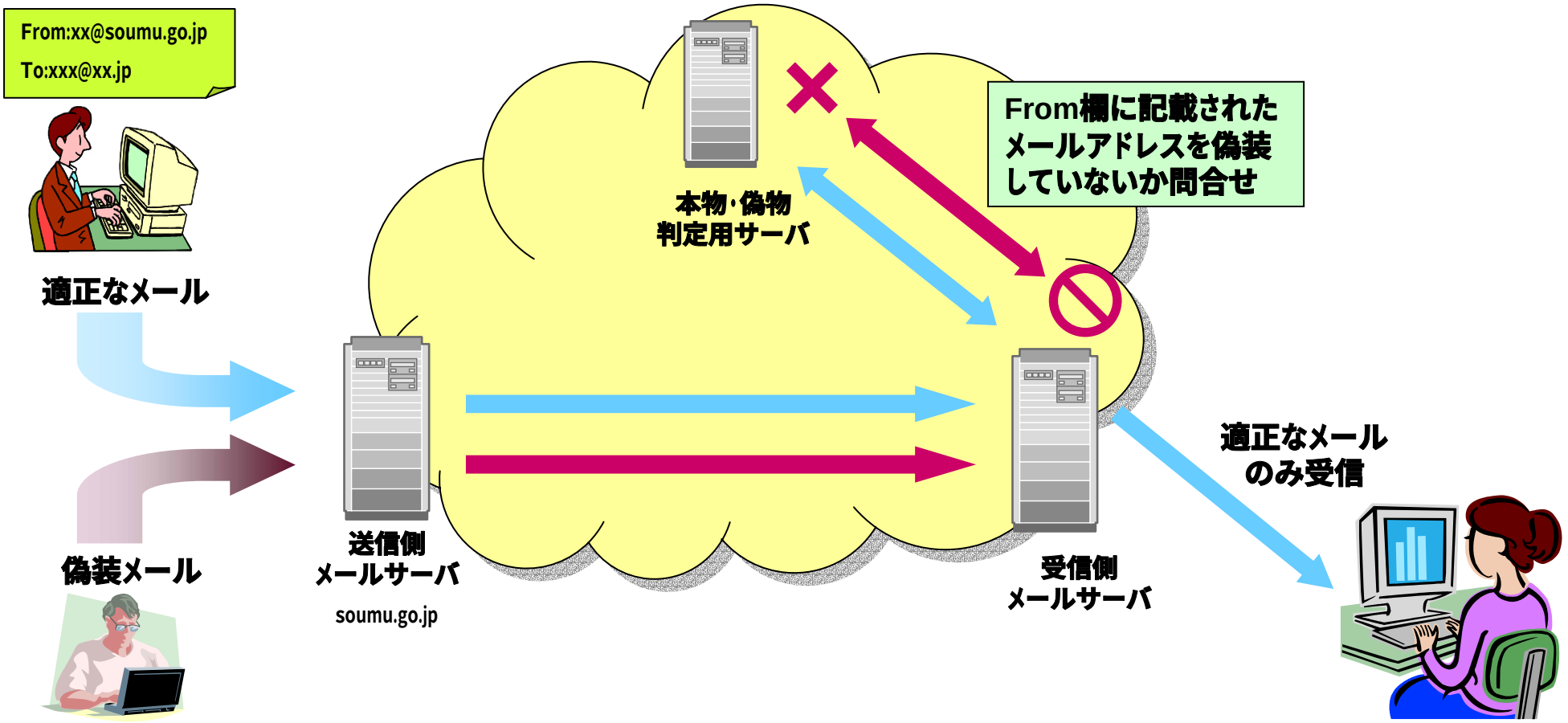
・多くの迷惑メールは、送信者の情報が改竄されており送信者の確認が困難となっている。
・現在ＩＥＴＦにおいて標準化作業が進められている「Sender-ID」や、「Domain Keys」のような電子メールの送信者を認証して他者へのなりすましを防止するような技術の普及を図ることにより、技術的に迷惑メールの受信を回避する仕組みを整えることが考えられる。

論点

・送信者認証技術は電子メールの送信者が偽装しているか否かのみを判断するものであるため、送信者を偽っていないメールを防止することはできないのではないか。
・標準化中の「Sender-ID」などの技術は、より多くの事業者が採用するのでなければ効果が発揮できないが、技術の採用に伴う実装コストなどの面で普及の障害となる要素があるのではないか。
・送信者認証技術の採用のほか、技術的にメール送信に一定の制約を加えることも検討されている（２５番ポートの封鎖等）が、我が国において導入することに問題はないか。

Sender-ID　：米マイクロソフトを中心に提案され、現在標準化作業が進められている電子メールの送信者認証技術。あらかじめ登録された送信者のドメイン情報と照合することで、受信側で送信者情報が偽装されているか否かをチェックすることができる。
Domain Keys　：米Yahooが提案している電子メールの送信者認証技術。電子署名の技術を活用することで、送信者情報やメール内容の偽装をチェックすることができる。

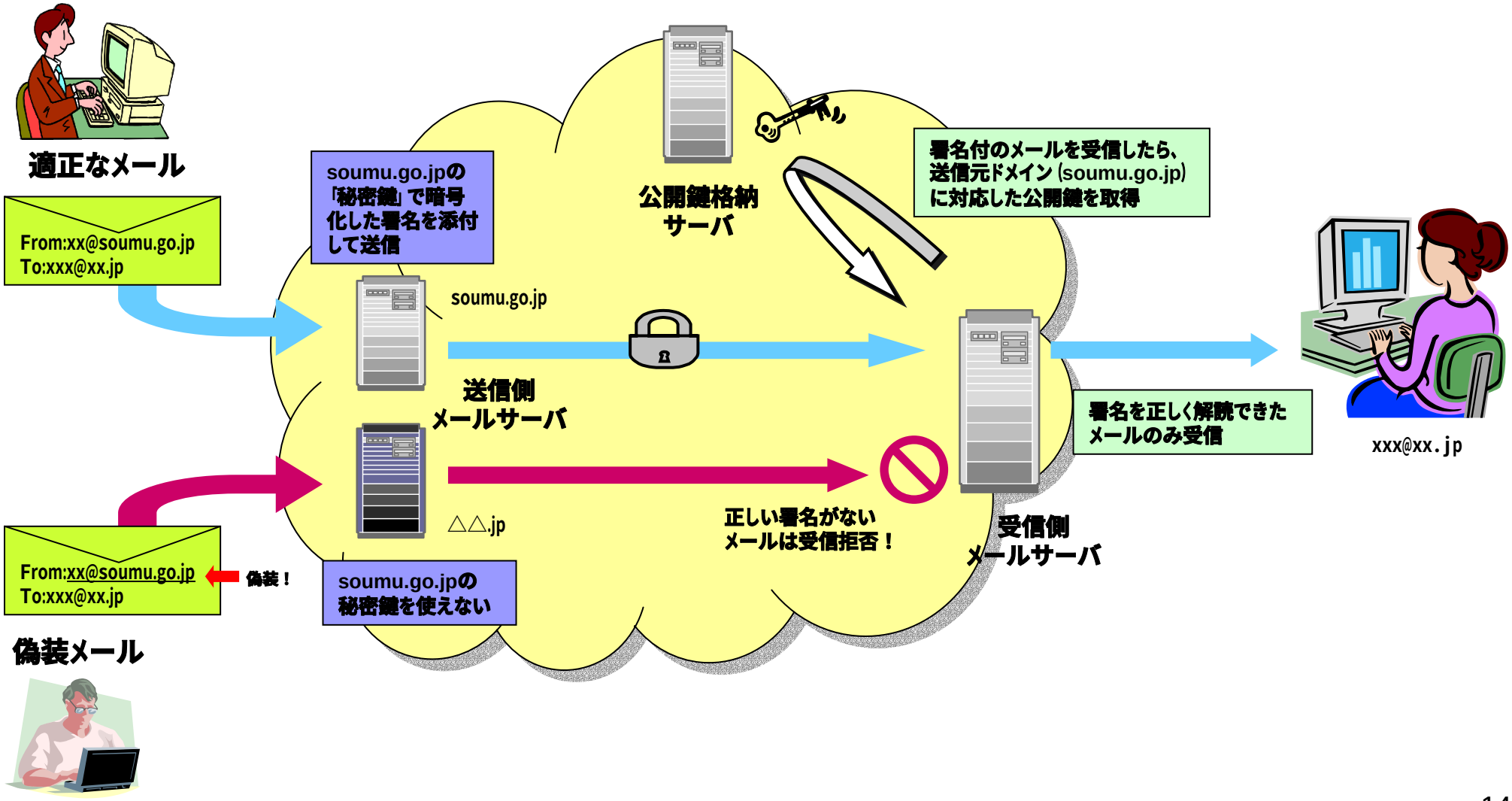
（参考）
Sender ID（メール送信ID：メールアドレス偽装判定技術）の概要



2004年6月22日　ASTA（マイクロソフト、AOL、Yahoo、EarthLink等で構成される業界団体）が発表したガイドラインにおいて、本技術の採用を推奨

2004年6月25日　Sender IDの仕様を標準化団体（IETF）に提出

（参考）DomainKeys（米Yahooが提案している送信者認証技術）の概要



4　利用者啓発

利用者への周知活動の促進

- 電子メールアドレスの設定・管理の方法や、フィルタリングサービス等の迷惑メール受信回避サービスについて、行政及び事業者による利用者への周知活動を促進するための措置を講じる必要があるのではないか。
- ＰＣ端末で利用可能なフィルタリング等の迷惑メール対策ソフトウェアについて、その種類・機能や導入及び利用の方法を広く周知する必要があるのではないか。

論点

- 現在、各事業者で迷惑メール対策リーフレットを作成して契約時に提供するなど、相当程度の取り組みは行われているが、周知対象を限定したり、新たな周知方法により情報を提供したりするなどの必要があるのではないか。
- フィルタリングについて、迷惑メールを遮断するとともに必要なメールを誤って迷惑メールと判定してしまうことのないよう、受信者のメール利用状況に適した導入や設定の方法を周知する必要があるのではないか。

5　国際協調

諸外国との国際協調の推進

・これまでにも韓＝豪、米＝英＝豪で覚書（MoU）が締結され、当事国間での相互情報提供等を進めていく取り組みが行われているところであるが、我が国においても、近年法制度の整備が進んできた欧米諸国や中国・韓国等のアジア諸国との間で、MoU締結等の国際協調のための取り組みを進めることが考えられる。

論点

・諸外国との迷惑メール法制や執行体制の差異を踏まえ、実際にどのような情報提供（あるいは提供を受けること）の仕組みを設けることが可能か。

・英・米・豪等の英語圏の諸国を中心に迷惑メール対策に関する国際協調が進んでいる中で、我が国のスタンスはどうあるべきか。

諸外国間で締結されているMoU
- 米･英･豪　：2004年7月2日、米連邦取引委員会（FTC）、英貿易産業省（DTI）･公正取引庁（OFT）･インフォメーションコミッショナー、豪競争･消費者委員会（ACCC）･通信庁（ACA）により締結。
- 韓･豪　：2003年10月20日、豪通信庁･国家情報経済局（NOIE）、韓国情報保護振興院（Information Security Agency）により締結。