

迷惑メール対策に係る 今後の取組

平成16年12月15日

経済産業省
消費経済政策課

目次

1. 今後の検討課題	…	1
2. 今後の取組(案)	…	3
1) インターネット・サービス・プロバイダ、 携帯電話事業者と連携した特定商取引法の 執行強化	…	4
2) 送信者認証技術の導入	…	12
3) 国際連携の推進	…	15
4) 普及啓発の強化	…	18

1. 今後の検討課題

今後の検討課題(第1回研究会資料から抜粋)

特定商取引法の執行強化

- (1)インターネット上では法違反者を特定し、行政処分を行うことが容易ではないことを踏まえ、法違反者を放置しないようにする方策を検討すべきではないか。
- (2)最近、迷惑メールにリンクされたWebサイトが原因で不当請求等に巻き込まれるトラブルが増加していることから、これに対処するための方策を検討すべきではないか。

送信者認証技術の導入

- (1)送信者特定を容易にして迷惑メールが届かないようにするフィルタリング等の実効性を高めるために、送信者認証技術の導入を進めるべきではないか。

国際連携の推進

- (1)迷惑メールに係る悪質行為は複数国にまたがることも多く、また世界各国で迷惑メール問題に取り組んでいる現状を踏まえると、迷惑メール問題に係る国際連携を推進すべきではないか。

普及啓発の強化

- (1)迷惑メールを契機とした悪質行為の巧妙化が進んでいるため、消費者が自衛能力を高めるために普及啓発をどのように強化すべきか。
- (2)コンピュータ・ウィルス感染(ゾンビPC)やサーバの不適切な管理(オープン・リレー・サーバ)等により、迷惑メールの送信に悪用可能な状況が出現することを防止するために、どのように啓発を行っていくべきか。

2. 今後の取組(案)

1) インターネット・サービス・プロバイダ、携帯電話事業者と連携した特定商取引法の執行強化

課題

インターネット上では法違反者を特定し、行政処分を行うことが容易ではないことを踏まえ、法違反者を放置しないようにする方策を検討すべきではないか。

現状

< 行政機関(経済産業省) >

迷惑メールは、そのほとんどが特定商取引法の表示義務に違反している。

(件名欄への「未承諾広告」不記載や本文冒頭への「事業者情報」不記載等) (P5 資料1参照)

しかしながら、インターネット上では「なりすましの容易さ」及び「本人追跡の困難さ」から、迷惑メール送信者を特定し行政処分に結びつけることが容易ではない。

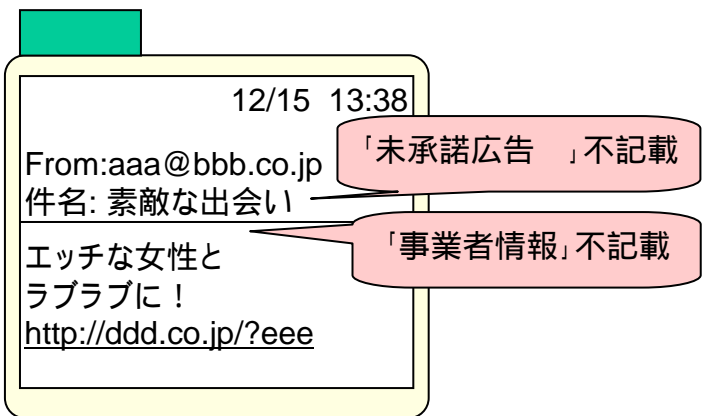
また、ISPが迷惑メール送信者に係る情報を第三者たる行政機関に開示することは、電気通信事業法における「通信の秘密」保護等を理由に禁じられている (P5 資料2参照)。

< インターネット・サービス・プロバイダ (ISP) >

多くのISPでは、契約者が迷惑メール送信等の違法行為を行った場合は、約款により利用停止等にできるとしている (P5 資料3参照)。

多くのISPでは、受信者からの迷惑メール受信の申出等があれば、に基づいて利用停止等を行っているが、受信者からの申出の不確実性や、契約者との訴訟リスク等により、利用停止等のためのより確実な証拠が欲しいとする意見が多い。

< 資料1 特商法違反の表示の例 >



< 資料2 通信の秘密 >

日本国憲法

第21条 (略)

2 検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

電気通信事業法

(秘密の保護)

第4条 電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。

2 (略)

(罰則)

第179条 電気通信事業者の取扱中に係る通信(第164条第2項に規定する通信を含む。)の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。

2 電気通信事業に従事する者が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する。

3 前二項の未遂罪は、罰する。

< 資料3 ISPにおける約款の例 >

(利用停止)

第A条 当社は、契約者が第B条(禁止事項)の規定に違反したときは、ヶ月以内で当社が定める期間、サービスの一部又は全部の利用を停止することがあります。

(禁止事項)

第B条 契約者は本サービスの利用にあたり、次の行為を行わないものとします。

犯罪行為又はこれを誘発若しくは煽動する行為

受信者に無断で広告メール等を送信する行為

法令若しくは公序良俗に違反する行為 等

ISPと行政機関(経済産業省)が
連携

行政機関(経済産業省)が

(a)自ら受信用の携帯電話及びPCを設置し、

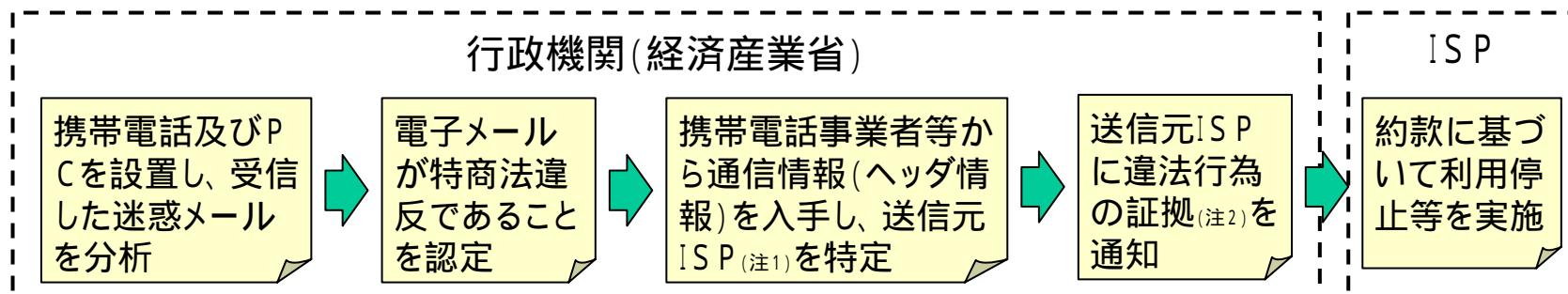
(b)当該端末で受信した迷惑メールが特定商取引法違反であることを認定し、

(c)この情報をISPに通知することによって、

ISPによる迷惑メール送信者に対する利用停止等の措置を促進すべきでないか(スキームはP7参照)。

特定商取引法と同様の迷惑メール表示規制を課している特定電子メール法の執行を担当する総務省と連携を強化し、対策の実効性を高めることについても検討すべきでないか。

< 対策として検討すべきスキーム(案) >



(注1)複数のISPを経由して迷惑メールが送信されている場合は、最後に経由したISP等に通知する。

(注2)電子メール本文に加え、ISPが迷惑メール送信者を特定するために必要な「IPアドレス」及び「通信時刻」も通知。

1) インターネット・サービス・プロバイダ、携帯電話事業者と連携した特定商取引法の執行強化

課題

最近では、迷惑メールにリンクされたWebサイトが原因で不当請求等に巻き込まれるトラブルが増加していることから、これに対処するための方策を検討すべきではないか。

現状

< 行政機関(経済産業省) >

最近では、迷惑メールで誘引される先のWebサイトの表示をクリックさせることで不当請求を行う事例が増加しているが、これらのWebサイトの表示は、特定商取引法違反と考えられる場合も多い。(虚偽誇大な表示や、意に反する申込みをさせる表示に該当) (P9 資料参照)

インターネット上では「なりすましの容易さ」及び「本人追跡の困難さ」から、違法Webサイト所有者を特定し行政処分に結びつけることが容易ではない。

また、ISPがこれらの違法Webサイト所有者に係る情報を第三者たる行政機関に開示することは、電気通信事業法における「通信の秘密」保護等を理由に禁じられている。

< インターネット・サービス・プロバイダ、ISP >

多くのISPでは、契約者が違法行為を行った場合は、約款によりWebサイトの削除等ができるとしている。

多くのISPでは、受信者からの申出等によりWebサイトの削除等を行っているが、契約者との訴訟リスク等により、Webサイトの削除等のためのより確実な証拠が欲しいとする意見が多い。

<資料 特定商取引法違反のWebサイトの例>

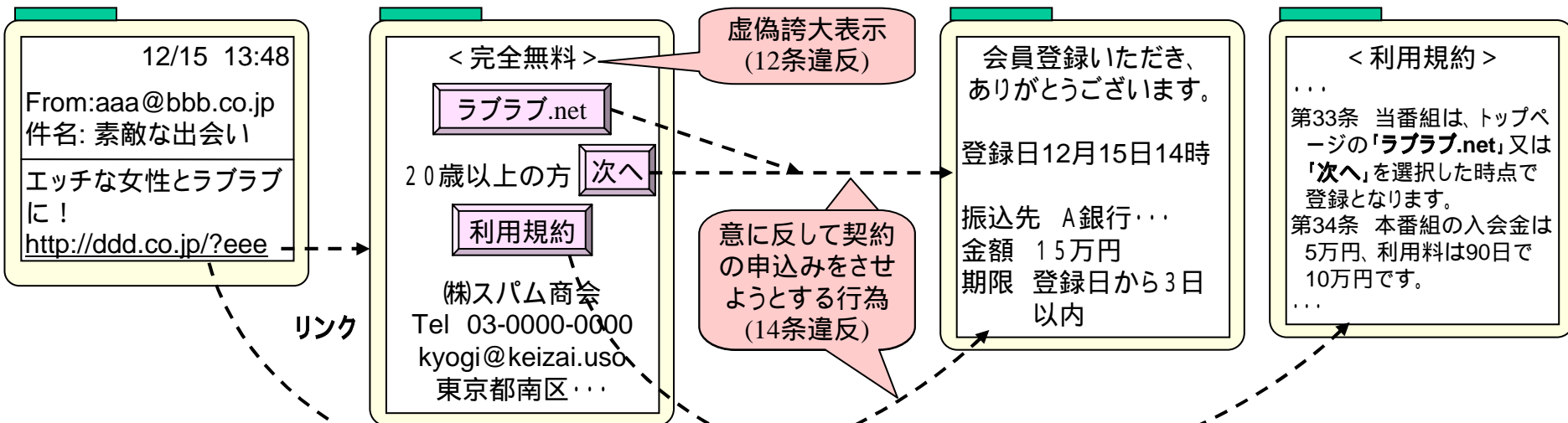
<受信メール>

<トップページ>

<特商法違反事項>

<登録ページ>

<利用規約ページ>



中には、URLをクリックするだけで会員登録されてしまうWebサイトもある。

ISPと行政機関(経済産業省)が 連 携

行政機関(経済産業省)が

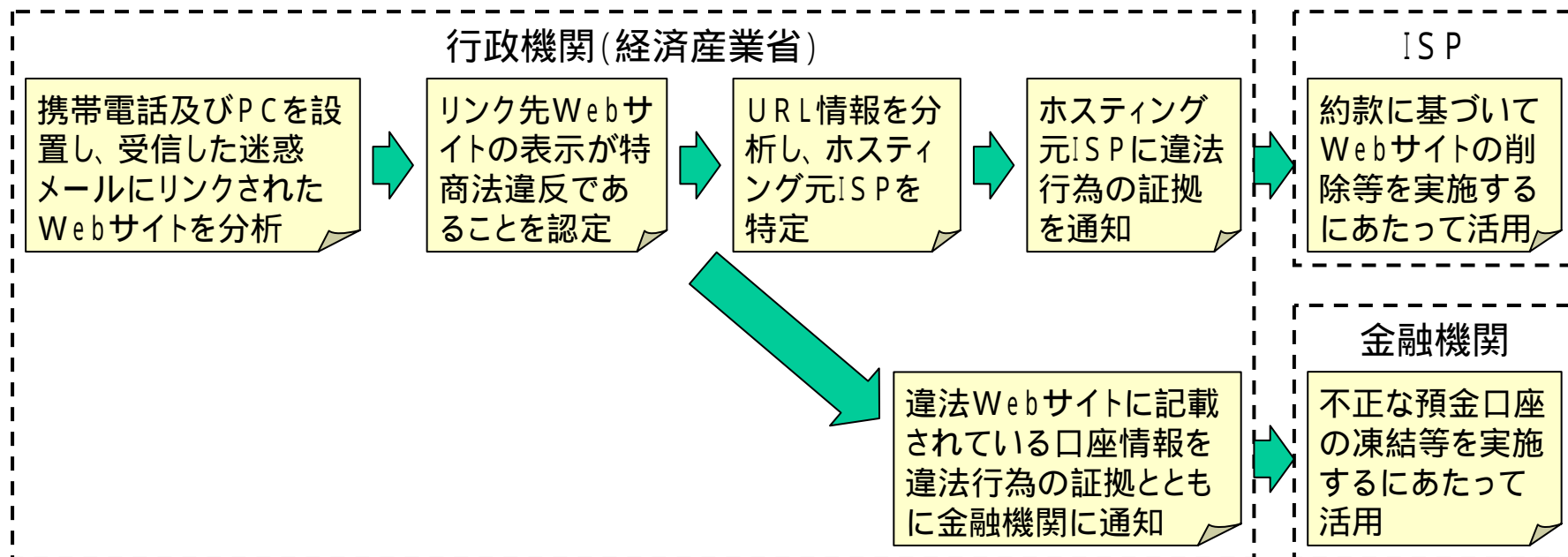
- (a)自ら受信用携帯電話及びPCを設置し、
- (b)当該端末で受信した迷惑メールにリンクされたWebサイトの表示が特定商取引法違反であることを認定し、
- (c)この情報を違法Webサイト所有者が契約しているISP(ホスティング元ISP)に通知することで、ISPによるWebサイトの削除等の措置を促進すべきでないか(スキームはP11参照)。

特に悪質な虚偽の広告表示に対しては、特定商取引法第12条に基づき、刑事罰を適用していくことが妥当ではないか。

海外のISPにホスティングしている違法Webサイトも多いことから、国際連携に力を入れることも必要ではないか。

なお、上記の違法Webサイトに代金振込先として口座が記載されている場合には、金融機関に情報提供することにより、口座の凍結等の措置を促進すべきではないか(スキームはP11参照)。

< 対策として検討すべきスキーム(案) >



2) 送信者認証技術の導入

課題

送信者特定を容易にして迷惑メールが届かないようにするフィルタリング等の実効性を高めるために、ISPにおける送信者認証技術の導入を進めるべきではないか。

現状

迷惑メール送信者は、送信の度にFrom欄などの送信者情報を変更するため、フィルタリング・ソフトに受信拒否アドレス/ドメインを登録しても、効果が上がりにくい状況にある。

また、送信者の特定が困難であるために、行政処分を行うのが容易ではない。

対策

現在、IETF(Internet Engineering Task Force)等においてドメインレベルの送信者認証技術について検討が進められている。(「Sender-ID」、「Domain Keys」等(技術の概要については、P13、P14参照))

ISP等はこの検討に積極的に参加し、これら技術の導入を進めるべきではないか。

効果

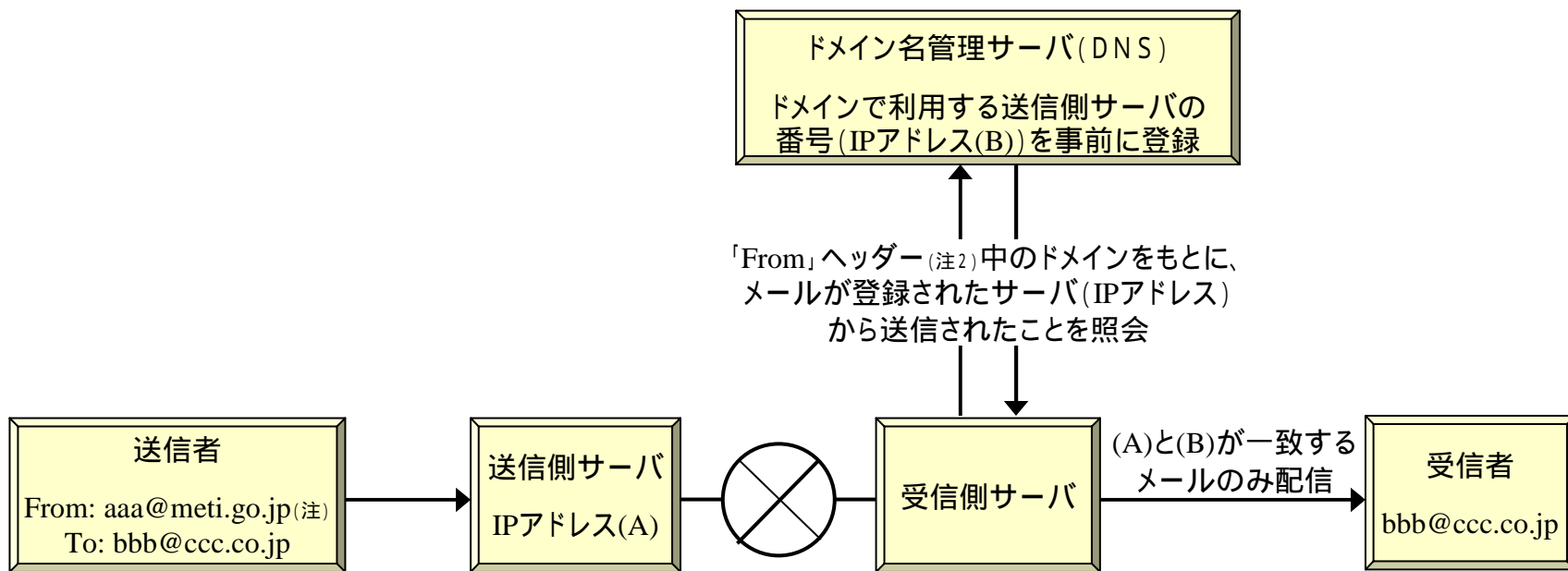
送信者認証技術の導入により、送信者情報を詐称した電子メールを効果的に排除できるようになると、フィルタリングがより有効に機能するようになることが期待される。

送信者認証技術に対応していないメールが事実上送れなくなれば、迷惑メールによるネットワークの負荷減少につながることを期待される。

(参考) Sender IDの概要

電子メールの送信に利用するサーバ固有の番号(IPアドレス)を利用して、送信元メールアドレス(ドメイン^(注1))を偽装したメールを排除する技術。

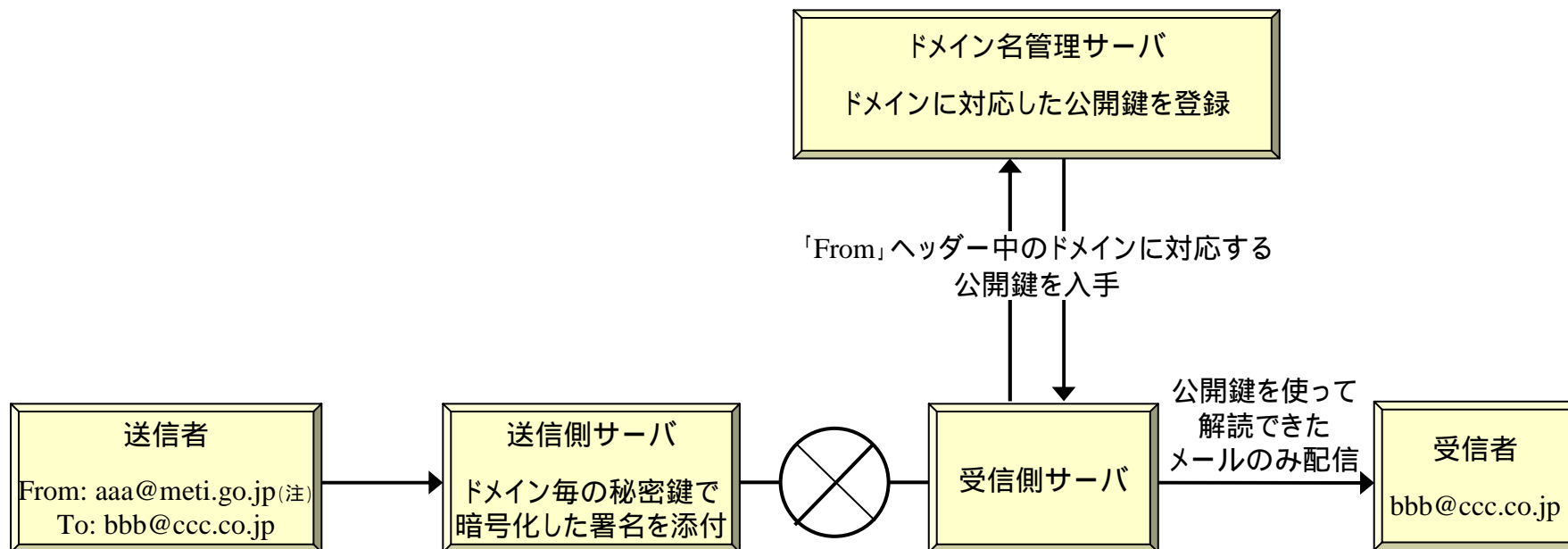
(注1)ドメインとは aaa@meti.go.jp の@より後ろの「meti.go.jp」のこと。



(注2) SMTPの「MAIL FROM」を使用することも可能

(参考) Domain Keysの概要

暗号技術を利用して、送信元メールアドレス(ドメイン)を偽装したメールを排除する技術。



3) 国際連携の推進

課題

迷惑メールに係る悪質行為は複数国にまたがることも多く、また世界各国で迷惑メール問題に取り組んでいる現状を踏まえると、迷惑メール問題に係る国際連携を推進すべきではないか。

現状

迷惑メールに係る悪質行為については、「海外からメールを送信」、「海外のサーバに置いたWebサイトで広告」といったケースが相当数存在するが、行政処分の実効性が担保できないため、対処が困難である(P16参照)。

各国で迷惑メール問題の深刻化を受けて取組を進めているため、政策情報を共有し効果的な対策を探る必要性が高まったことから、OECD等の場で情報交換が行われるなど、国際連携に向けた様々な動きが始まっている(P17参照)。

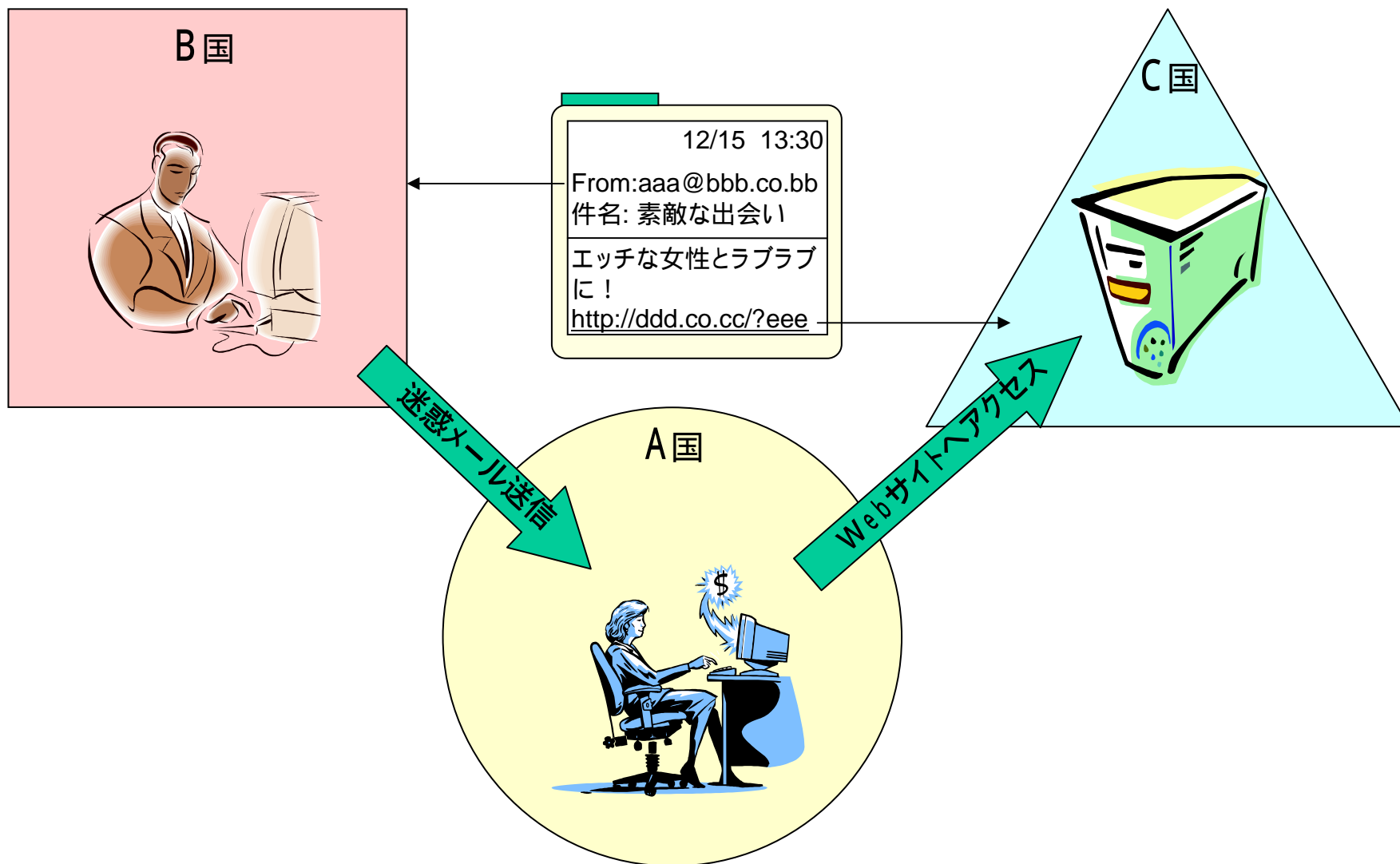
対策

前述の「特定商取引法の執行強化」において海外のサーバから送信されているなどの場合には、関係国の法執行当局に情報提供し、対策の実施を求めていくべきではないか。

OECD等の情報交換の場に積極的に参加し、諸外国の成功事例を取り入れるとともに、我が国の経験についても情報提供すべきではないか。
また、OECD諸国と連携し、OECD非加盟国への働きかけを強化していく必要があるのではないか。

(参考) 国境を越える迷惑メール送信行為のイメージ

A国内の者に対し、B国から迷惑メールを送信し、そのメールにC国のサーバに置いたWebサイトをリンクさせたケース。



(参考) 国境連携に向けた様々な動き

	ロンドン アクション・プラン	米英豪MoU	韓豪MoU
締結日	2004年10月11日	2004年7月2日	2003年10月20日
参加国・機関	日韓英米豪等19カ国・29機関等（うち4機関等は民間団体） 日本からは経済産業省、総務省、公正取引委員会が参加	米国（連邦取引委員会） 英国（貿易産業省、公正取引庁、インフォメーション・コミッショナー） 豪州（競争・消費者委員会、通信庁）	韓国（情報保護院） 豪州（国家情報経済局、通信庁）
目的	迷惑メールに対する法執行の推進に向けた国際連携・官民連携の強化	捜査協力まで視野に入れた迷惑メールに対する法執行の推進のための協力強化	両国における迷惑メール被害の抑制に向けた、迷惑メール対策に係る政策情報の交換の推進
主な協力内容	迷惑メールに対する法執行を行う各国内の他の行政機関との連携 四半期毎に電話会議で以下の情報を共有 ・法執行事例 ・新規の法規制 ・法執行のための調査手法 ・消費者への普及啓発等 官民連携の推進	各機関が所有する迷惑メール送信に係る証拠の提供・交換・議論 迷惑メールの発見・調査における最大限の協力 捜査代行 迷惑メールに係る苦情に関する情報共有 迷惑メール対策の推進のための政策情報の共有	迷惑メール対策に係る政策の情報交換 法執行ノウハウの共有 官民連携の推進

MoU (Memorandum of Understanding) : 了解事項のこと

4) 普及啓発の強化

課題

迷惑メールを契機とした悪質行為の巧妙化が進んでいるため、消費者が自衛能力を高めるために普及啓発をどのように強化すべきか。

被害実態

経済産業省調査によると、30代以下の男性(特に高校生)が携帯電話に届いた迷惑メールにリンクされたWebサイトに接続したこと等により不当請求を受けるケースが多い。また、最近ではPCに届いた迷惑メールでも同様のトラブルが増加している。

対策

特にトラブルが多い高校生への普及啓発に力を入れる必要があるのではないかと。

不当請求等に関するトラブルが増加傾向にあるため、携帯電話会社やISPにおいても普及啓発を強化していく必要があるのではないかと。

	経済産業省	携帯電話会社	ISP
高校生	Webサイト パンフレット ビデオ	請求書同封物 Webサイト 販売店対応	Webサイト メールマガジン
大学生	Webサイト	Webサイト	Webサイト
社会人	Webサイト	Webサイト	Webサイト

4) 普及啓発の強化

課題

コンピュータ・ウィルス感染(ゾンビPC)やサーバの不適切な管理(オープン・リレー・サーバ)等により、迷惑メールの送信に悪用可能な状況が出現することを防止するために、どのように啓発を行っていくべきか。

現状

常時接続の増加等を背景に、コンピュータ・ウィルスに感染し、外部から指示を受けるなどして迷惑メールを送信するいわゆるゾンビPCが増加している。

サーバの管理が不適切であり、全てのメールに転送を許してしまうオープン・リレー・サーバが依然として存在している。

対策

経済産業省では、情報セキュリティの普及啓発に取り組んでいるが、これら迷惑メールの送信に悪用されないための予防知識の普及啓発にこれまで以上に力を入れるべきではないか。

- ・企業向け「情報セキュリティセミナー(全国16ヶ所開催、3,000名参加予定)」
- ・個人向け「インターネット安全教室(全国20ヶ所以上開催、7,000名参加予定)」

「特定商取引法の執行強化」のスキームで違法性が認定されたメールには、ゾンビPCやオープン・リレー・サーバを悪用して送信されたものも相当数存在するため、これをアンテナとして、ISP等と連携しながら、ウィルス除去や設定変更などにより対応を進めていくべきではないか。

(参考) 本人確認法改正の概要

改正の背景

インターネット等を通じて売買された他人名義の預金口座等を不正に利用した詐欺等の犯罪行為が多発している現状にかんがみ、預貯金通帳等を譲り受ける行為等についての処罰規定を設ける必要があるため、本人確認法を改正。(平成16年12月3日成立)

改正の概要

< 違反行為 >

- (1) 他人になりすまし、預貯金契約の役務の提供を受ける目的で通帳を譲り受ける場合
- (2) 事情を知りながら、通帳を譲り渡す場合
- (3) 正当な理由なく、有償で預貯金通帳の譲り受け、譲り渡しをする場合



< 罰則 >

罰金50万円以下の罰金

「業」としてこれらを行った場合は、2年以下の懲役か300万円以下の罰金

インターネットなどでこれらの行為をするよう勧誘した場合も、50万円以下の罰金