

資料6



実はここにも

総務省

MIC

Ministry of Internal Affairs
and Communications

法制度の在り方について

平成19年9月27日
事務局

迷惑メールの現状や現行の特定電子メール法の施行状況等を踏まえると、現行の特定電子メール法を以下の観点から見直すことが必要ではないか。

1 悪質化・巧妙化する迷惑メールへの対応の強化

ボットネットを利用した迷惑メール、フィッシングメールその他現行法の適用が回避されている悪質化・巧妙化した電子メールへの対策を総合的に講じていく上で、対策が必要な電子メールについて、法制度上、違法であることを明確化すべきではないか。

2 法の実効性の強化

より効果的な迷惑メール対策を行っていく上で、法の実効性の強化が必要であり、下記の実現に資するようにすべきではないか。

- ・ 迷惑メールの送信者にとって、迷惑メール送信のコスト、リスクがより高くなる制度
- ・ 迷惑メールの受信者にとって、迷惑メール受信の防止のコスト、リスクがより低くなる制度
- ・ 電子メールサービスを提供する事業者にとって、自主的な対策を行いやすくなる制度
- ・ 法の執行機関にとって、法執行のための措置が円滑かつ機動的にとりやすくなる制度

3 国際的整合性・連携の強化

インターネットは国際的なネットワークであり、特に最近、外国発の迷惑メール等国境を越えて送受信される迷惑メールが増加していることから、我が国が国際的な迷惑メール対策の抜け穴とならないよう国際的整合性を一層向上させ、各国との連携の強化に資する制度とすべきではないか。

悪質化・巧妙化する迷惑メールの
対応の強化について

電子メールの送信に関する法規制について

(1) メディア横断的な法規制（電子メールの送信に関わるもの）

規制されている電子メールの送信	根拠法	罰則
名誉毀損、侮辱、脅迫 人の名誉を毀損する多数の者への電子メールの送信の禁止 他人を侮辱する多数の者への電子メールの送信の禁止 他人を脅迫する電子メールの送信の禁止	刑法第230条（名誉棄損） 刑法第231条（侮辱） 刑法第222条（脅迫）	3年以下の懲役若しくは禁錮又は50万円以下の罰金 拘留又は科料 2年以下の懲役又は30万円以下の罰金
風説の流布、業務妨害（信用毀損、株価操作等） 風説の流布等により、信用を毀損し、又は業務を妨害する電子メールの送信の禁止 有価証券等の相場の変動を図る目的をもって、風説を流布する電子メールの送信を禁止	刑法第233条（信用毀損及び業務妨害） 金融商品取引法第158条、第197条	3年以下の懲役又は50万円以下の罰金 5年以下の懲役又は100万円以下の罰金
わいせつ物頒布、児童ポルノ提供等 わいせつ画像データを含む電子メールの送信の禁止 人を児童との性交等の相手方となるように誘引する電子メールの送信の禁止 人に児童買春をするように勧誘する電子メールの送信の禁止 児童ポルノの画像等を含む電子メールの送信の禁止	刑法第175条（わいせつ物頒布等（1）） 出会い系サイト規制法第6条、第16条 児童ポルノ処罰法第6条第1項 児童ポルノ処罰法第7条第1項	2年以下の懲役又は250万円以下の罰金若しくは科料 100万円以下の罰金 5年以下の懲役又は500万円以下の罰金 3年以下の懲役又は300万円以下の罰金
著作権の侵害 著作物の無断配信等著作権を侵害する電子メールの送信の禁止	著作権法第119条	5年以下の懲役又は500万円以下の罰金
ネズミ講への勧誘 業として、ネズミ講に加入することを勧誘する電子メールの送信の禁止 ネズミ講に加入することを勧誘する電子メールの送信の禁止	ねずみ講防止法第6条 ねずみ講防止法第7条	1年以下の懲役又は30万円以下の罰金 20万円以下の罰金
詐欺 架空請求等の詐欺行為の実行の着手となる電子メールの送信の禁止	刑法第246条（詐欺（2））	10年以下の懲役
個別分野における広告 （例）医薬品等の虚偽又は誇大広告、承認前の医薬品等の広告を行う電子メールの送信の禁止	薬事法第66条第1項、第68条、第85条	2年以下の懲役又は200万円以下の罰金又はこれを併科
ウイルスの頒布 ウイルスを添付した電子メールの送信の禁止	刑法第168条の2（不正指令電磁的記録供用）（3）	3年以下の懲役又は50万円以下の罰金

（1）現行の刑法第175条の適用についての判例（横浜地川崎支判平成7年7月14日）あり。また、この行為を条文上明確化するための改正法案が平成16年に国会に提出されたが現時点で未成立。（2）財物の交付がなされていない場合は詐欺未遂。（3）改正法案が平成16年に国会に提出されたが現時点で未成立。

電子メールの送信に関する法規制について

(2) 電子メールの送信についての規制

規制されている電子メールの送信	根拠法	罰則
受信者が再送信の拒否の通知を行った場合の広告・宣伝メールの送信の禁止 (特定商取引法上の指定商品・指定役務について上記の送信の禁止)	特定電子メール法第4条、第7条、第32条 特定商取引法第12条の3等	措置命令。違反した場合、1年以下の懲役又は100万円以下の罰金 指示。違反した場合、100万円以下の罰金 業務停止命令。違反した場合、2年以下の懲役又は300万円以下の罰金(併科あり)
営業のための架空電子メールアドレス宛の多数の者への電子メールの送信の禁止	特定電子メール法第5条、第7条、第32条	措置命令。違反した場合、1年以下の懲役又は100万円以下の罰金
送信者情報を偽った広告・宣伝メールの送信の禁止	特定電子メール法第6条、第32条	1年以下の懲役又は100万円以下の罰金(4)

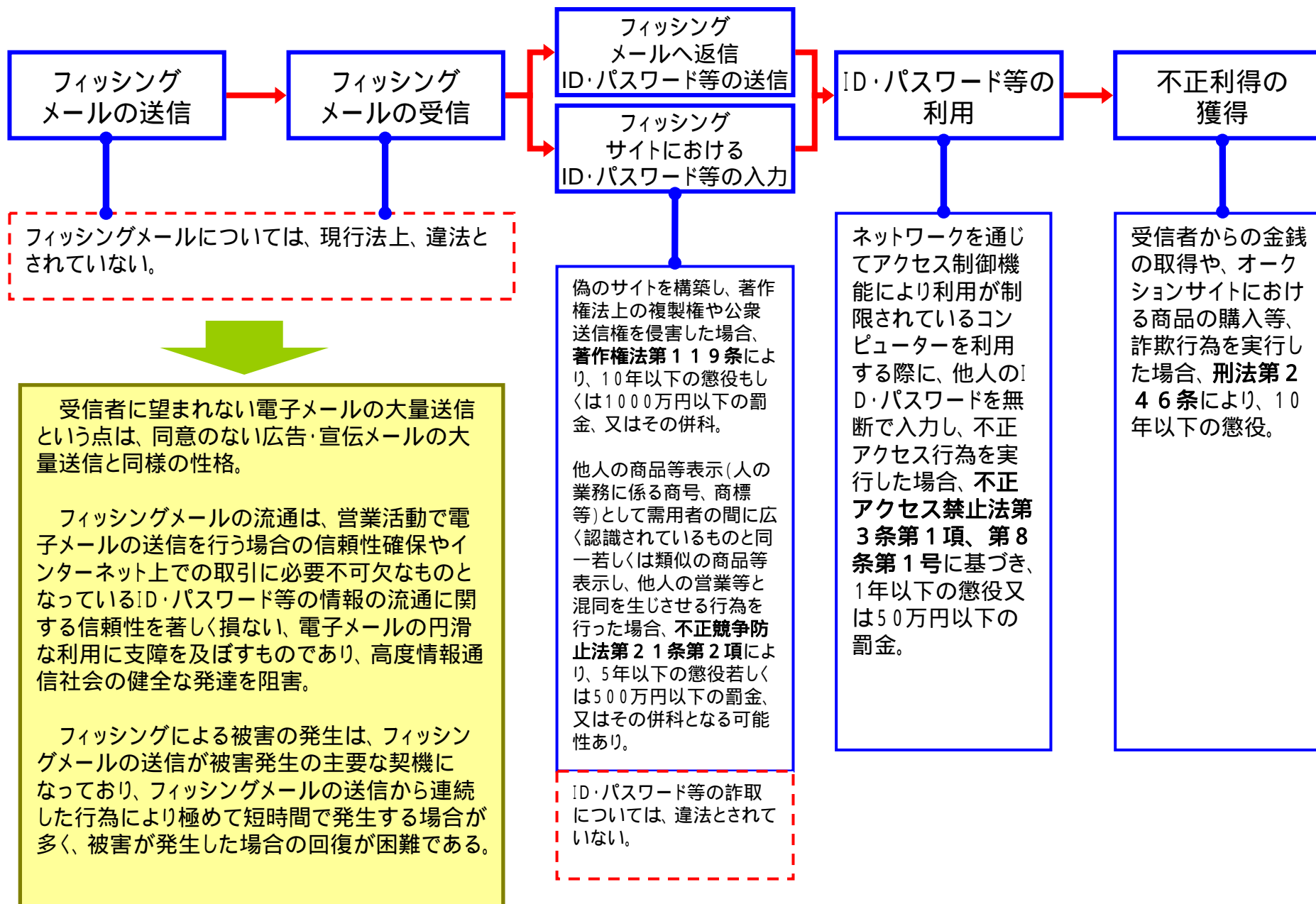
(4) 措置命令もあり。

(3) 現在問題となっているが、十分な法規制がない電子メール

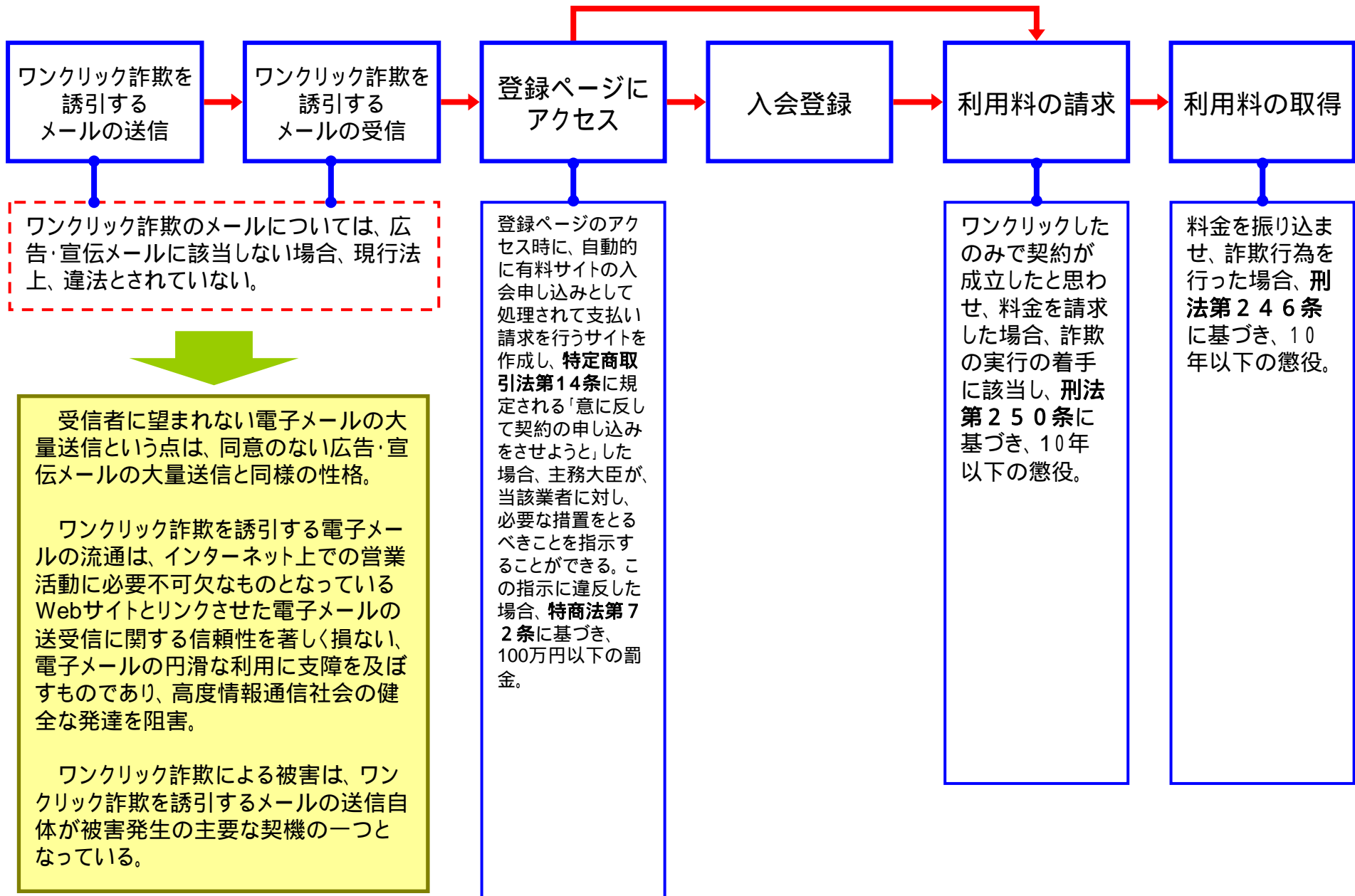
問題となっている電子メールの送信	備考
電子メールの種類が問題となるもの フィッシングメール等の送信	-
電子メールの送信の手法が問題となるもの ボットネットを利用した迷惑メールの送信 外国からの迷惑メールの送信	ボットネットを利用する者が送信者に該当する場合は、特定電子メール法第4条～第6条が適用。 送信地の外国で違法とされている場合等は、外国法の適用の可能性あり。

(注) この他、広告・宣伝メールの送信に関する現行のオプトアウト規制の実効性が問題となっている。

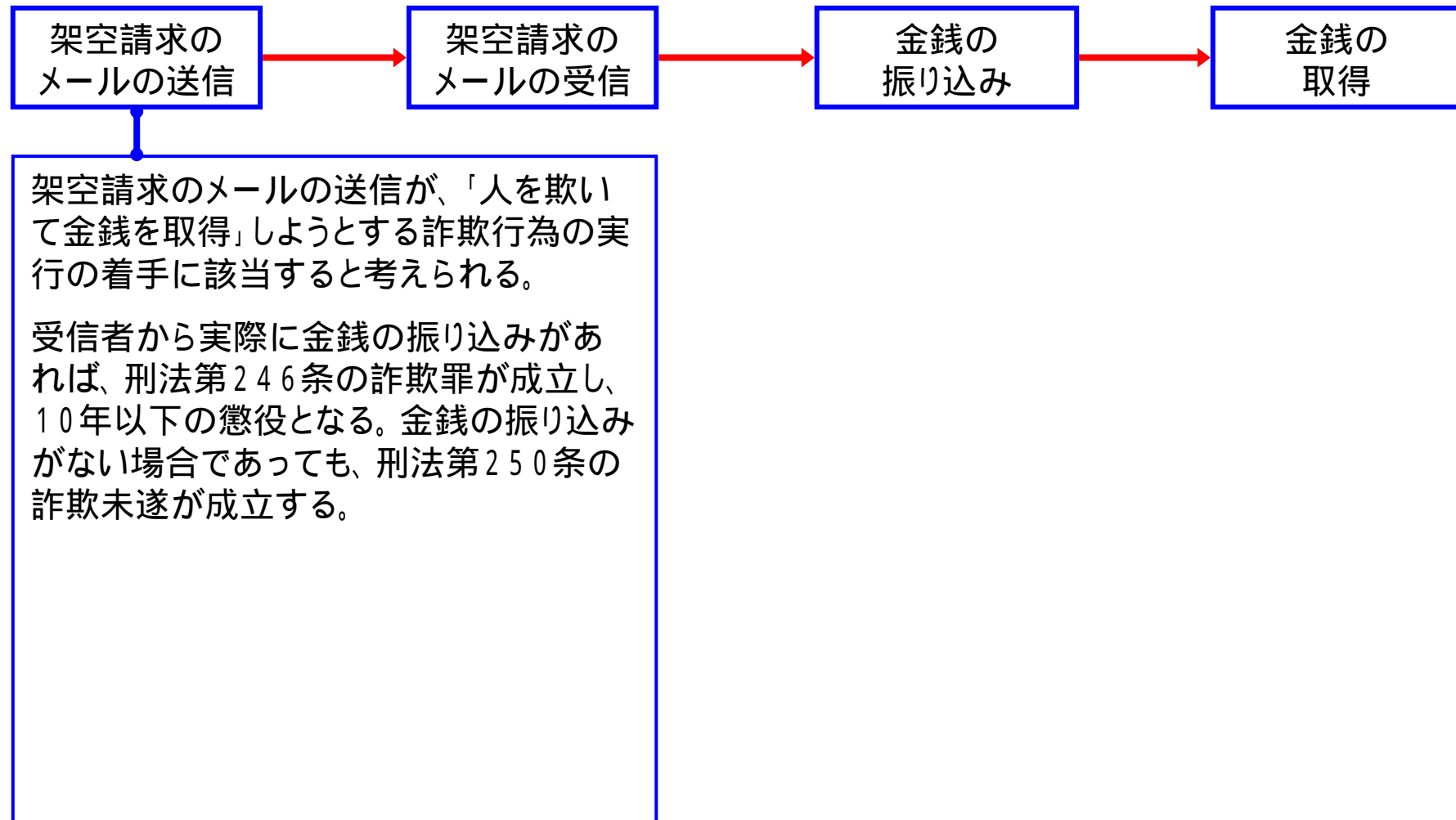
フィッシングメールに関する法規制について



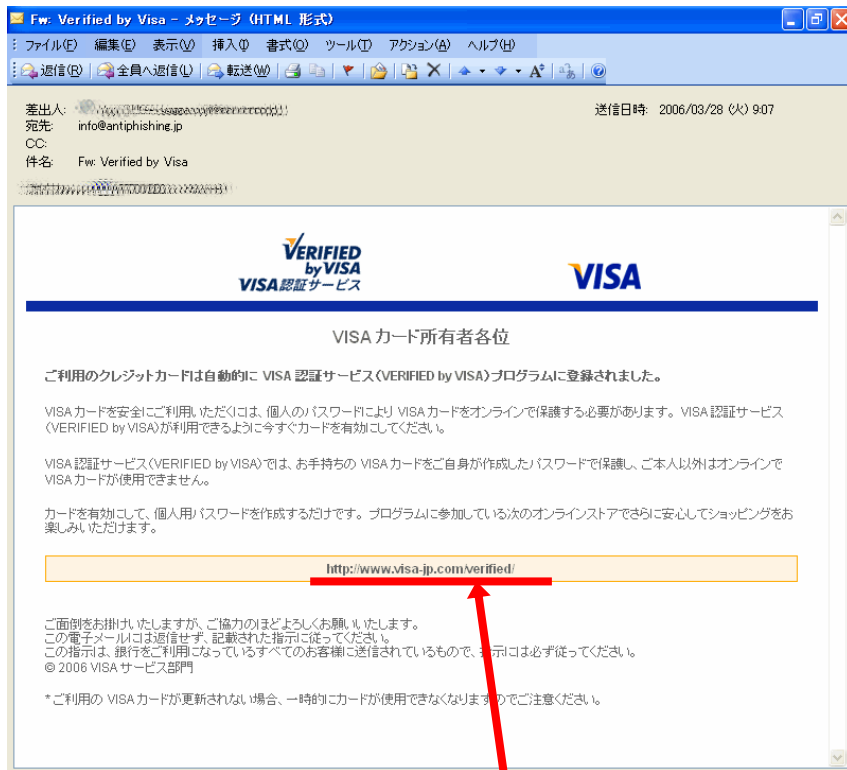
ワンクリック詐欺を誘引するメールに関する法規制について



(参考) 架空請求のメールに関する法規制について



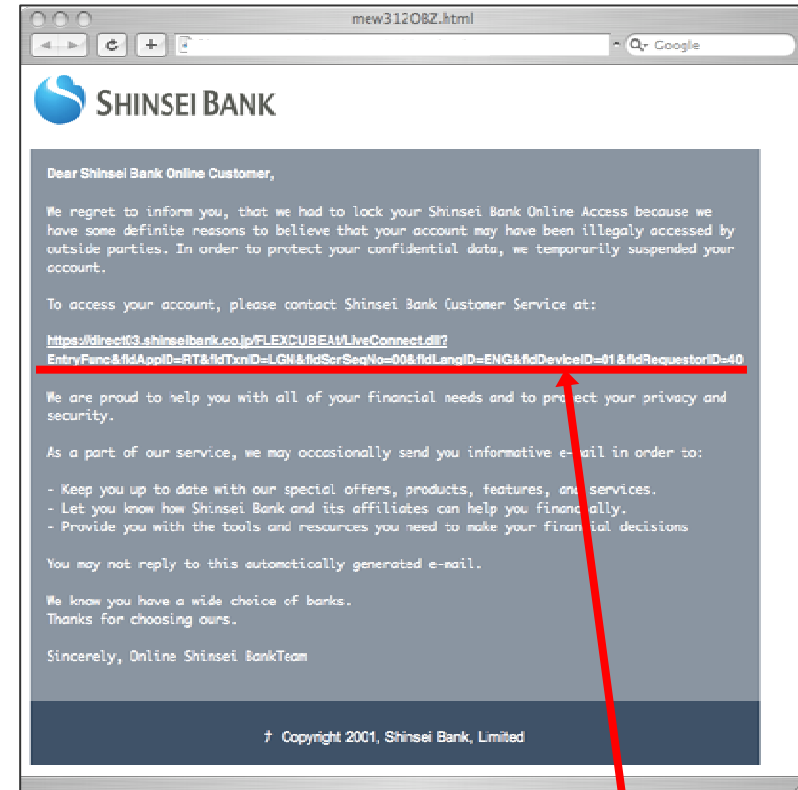
事例1



カード情報を盗みとるため、偽のサイトに誘導

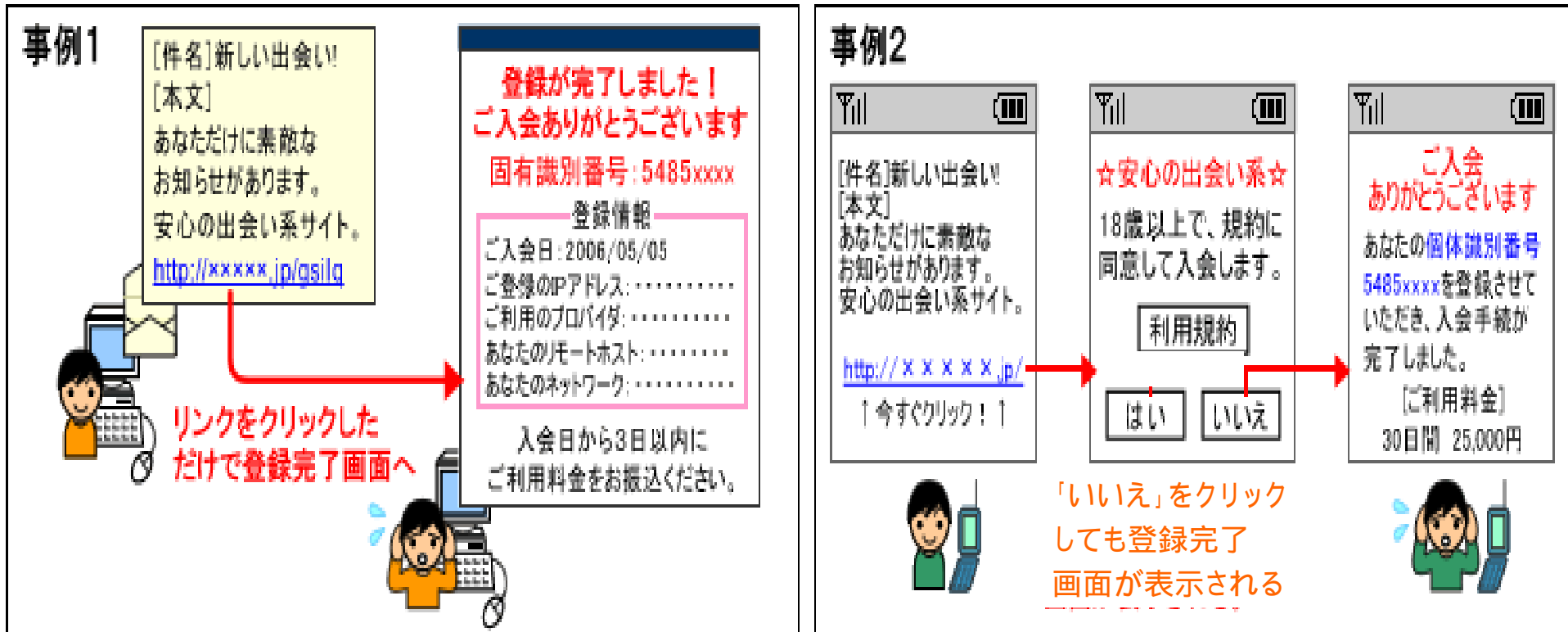
(出典: フィッシング対策協議会 <http://www.antiphishing.jp/>)

事例2



口座情報を盗むため、偽のサイトに誘導

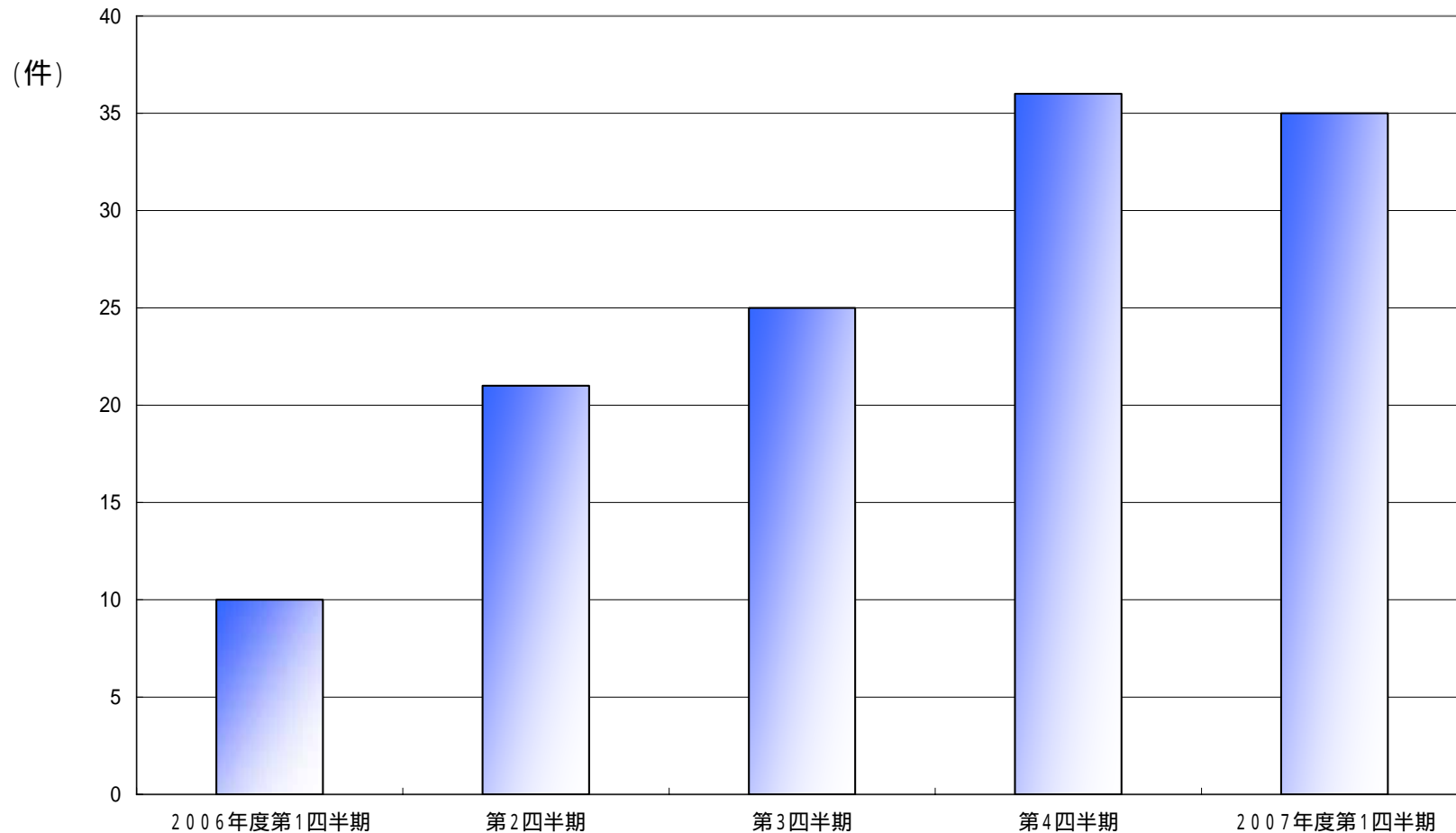
(出典: 迷惑メールへの対応の在り方に関する研究会第2回 III 櫻庭氏提出資料)



出典: 総務省 国民のための情報セキュリティサイト



フィッシング対策協議会に寄せられたフィッシングメールの件数の推移（国内）



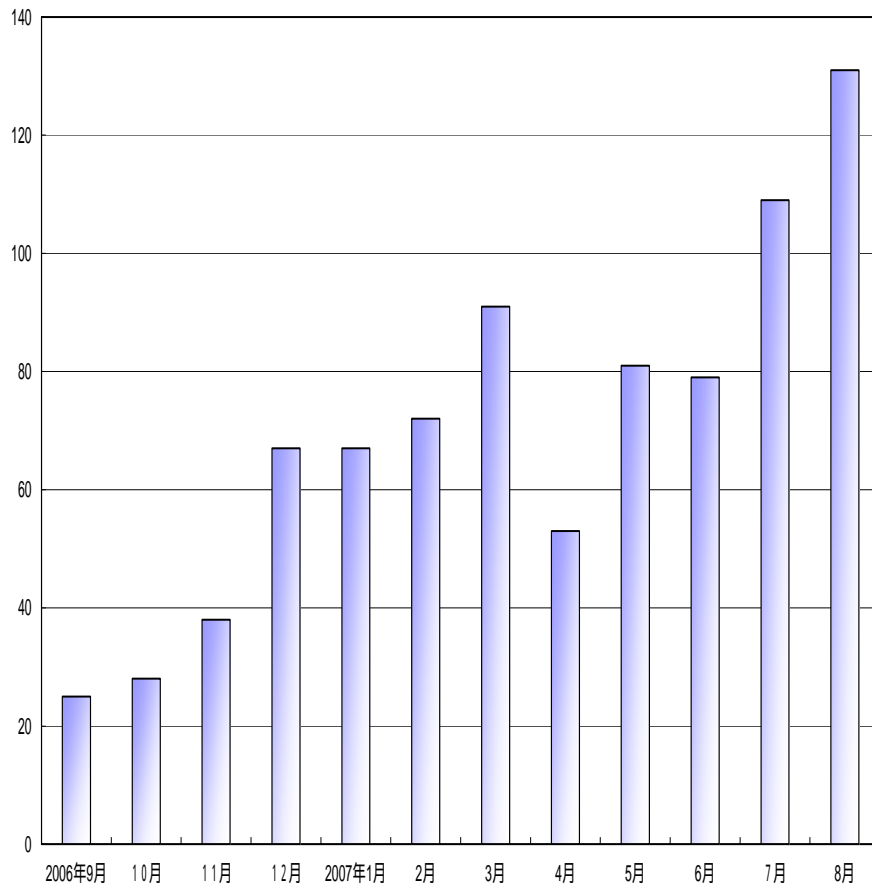
（出典：フィッシング対策協議会「月次報告書フィッシング情報届出状況」

<http://www.antiphishing.jp/report/index.html>）

ワンクリック詐欺を誘引するメールに関わる相談件数推移

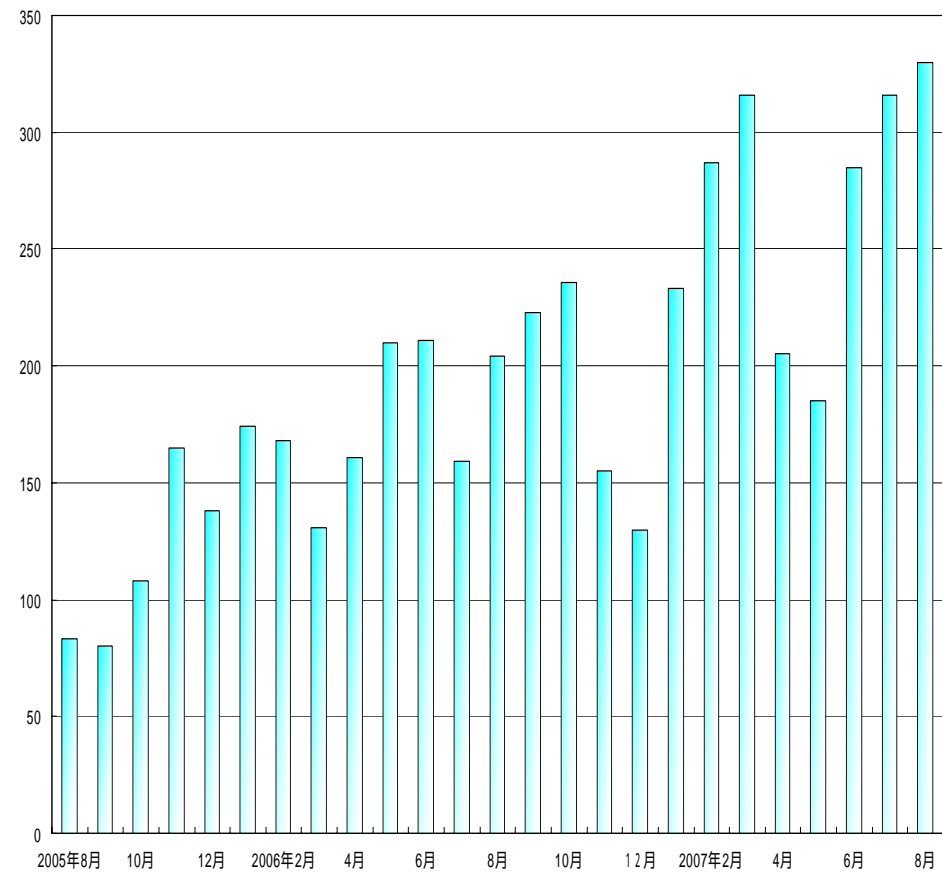
迷惑メール相談センターに寄せられた
情報料請求に関する相談件数

(件)



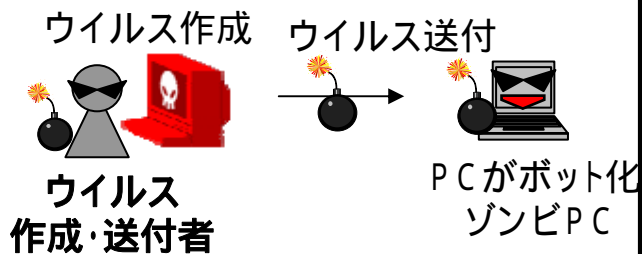
出典：財団法人日本データ通信協会迷惑メール相談センター

情報処理推進機構セキュリティセンターに寄せられた
ワンクリック不正請求に関する相談件数



出典：独立行政法人情報処理推進機構セキュリティセンター（IPA / ISEC）

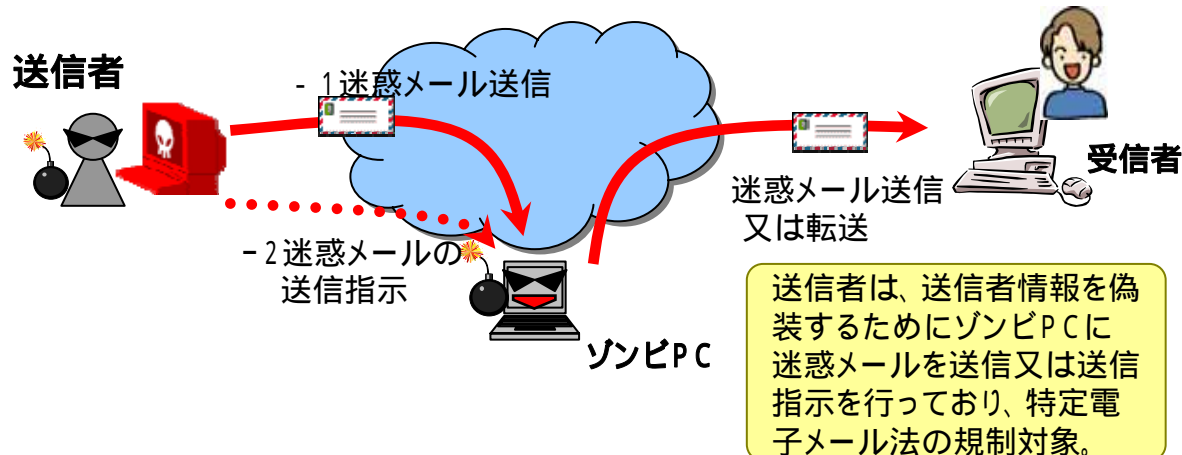
フェーズ1(ウイルス作成～ポット化)



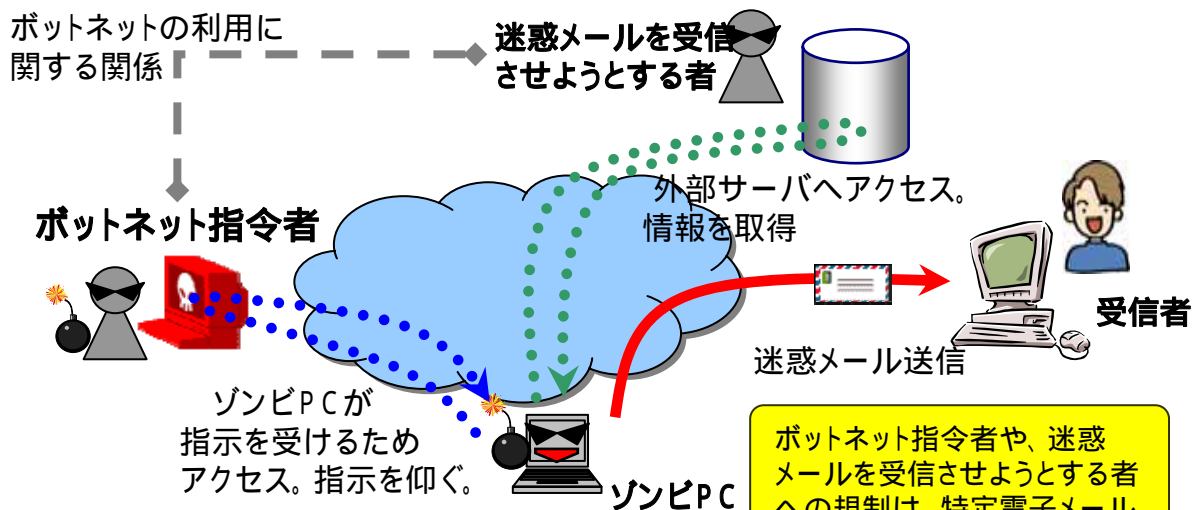
コンピュータ・ウイルスを作成した場合、不正指令電磁的記録作成罪(刑法第168条の2())
コンピュータウイルスを送付した場合、不正指令電磁的記録供用罪(刑法第168条の2())

フェーズ2(迷惑メールの送信)

パターン1: ゾンビPCを踏み台として、迷惑メールを送信するケース



パターン2: ゾンビPCがボットネット指令者のPCにアクセスし、次に外部のサーバ等にアクセスし、迷惑メールの情報を取得した上で、迷惑メールを送信するケース



オーストラリア

(2003年スパム法)

商用電子メッセージの定義に、不正な利益取得の支援・可能化を目的とする電子メールを含めている。

6 商用電子メッセージ

(1)本法の目的のため、商用電子メッセージとは、…そのメッセージの目的または目的の一つが以下のいずれかであると結論することができると思われるものをいう。

(a)～(l)(商品又はサービスの広告宣伝等を行うこと)

(m)ある人が別の人の所有する財産を不正に取得することを詐欺によって支援するか、またはそれを可能にすること。

(n)ある人が別の person から経済的利益を不正に取得することを詐欺によって支援するか、またはそれを可能にすること。

(o)ある人が別の person から不正に利益を取得することを支援するか、またはそれを可能にすること。

16 望まれない商用電子メッセージを送ってはならない

(1)人は、以下に該当する商用電子メッセージを送信してはならず、また送信させてもならない。

・送信者の場所にかかわらず、受信者又は受信メールにアクセスするための機器がオーストラリアに所在していれば規制対象。

・単なる送信(send)行為のほか、送信させる行為(cause to be sent; 結果として送信されることとなるような行為)も禁止。

ボットネットを用いた迷惑メールの送信も規制対象に含まれると解される。

7 オーストラリアン・リンク

本法の目的のため、商用電子メッセージは以下のいずれかの場合に、またこれらの場合に限り、オーストラリアン・リンクを含んでいる。

(c)そのメッセージへのアクセスに使用されるコンピュータ、サーバ、またはデバイスがオーストラリアに置かれている。

(d)該当する電子アカウント所有者(=あて先メールアドレスに責任を有する者)が以下のいずれかの条件に当てはまる場合。

(i)そのメッセージがアクセスされるときにオーストラリアに実在する個人。

(ii)そのメッセージがアクセスされるときにオーストラリアにおいてビジネスまたは活動を行っている組織。または

(e)該当する電子アドレス(=あて先メールアドレス)が存在しないためにメッセージを配信できない場合 その電子アドレスが存在するものと仮定すると、オーストラリアにあるコンピュータ、サーバまたはデバイスを用いてそのメッセージがアクセスされるだろうと合理的に推定できる。

16 望まれない商用電子メッセージを送ってはならない

(1)人は、以下に該当する商用電子メッセージを送信してはならず、また送信させてもならない。

(a)オーストラリアン・リンクを含んでいる。

米国

(CAN-SPAM法)

許可なくアクセスしたコンピュータを通じた送信及び転送等を禁止。

Sec.7704(b)(3)

Sec.7704(a)で違法とされている商業電子メールメッセージを、許可なくアクセスした保護されたコンピュータ又はコンピュータネットワークから、保護されたコンピュータへ意図的に転送又は再送信することは違法

Sec.1037(a)(1)

許可なく保護されたコンピュータにアクセスし、意図的にそのコンピュータから、又はそれを通して、複数の商業電子メールメッセージを送信することを禁止(刑事罰)

欺瞞的な表題を付した商業電子メールメッセージの送信も違法とされている。

Sec. 7704 商業電子メールの利用者のためのその他の保護

(a)メッセージ送信において要請されること

(2)欺瞞的表題の禁止

商業電子メールメッセージについて、その表題が、メッセージの内容又は主題に関する重大な事実について、客観的状況下において合理的に行動している受信者に対して誤解を与える可能性が高いということを、その送信者が実際に知り、又はその状況下で十分に知っていると考えられる場合には、当該メールの保護されたコンピュータへの送信は違法。

Sec. 7702 定義

(2)商業電子メールメッセージ

(A)一般規定

「商業電子メール・メッセージ」という用語は、商業製品またはサービス(商業目的で運営されるインターネット・ウェブサイト上のコンテンツを含む。)の、商業広告または宣伝を主たる目的とするすべての電子メール・メッセージを意味する。

現行のオプアウト方式の見直しについて

法の実効性及び国際的整合性・連携の強化の観点から、正当な営業活動における電子メールの利用への影響も十分勘案した上で、現行のオプトアウト方式をオプトイン的な方向に見直すべきではないか。

1 現行のオプトアウト方式の趣旨と実効性の強化

現行のオプトアウト方式は、電子メールというメディアの特性を利用して大量に送信される広告・宣伝メールに対し、広告・宣伝メールの送信の基準を受信者側の拒否の有無とした上で、送信者側への影響の大きさ(1)や技術的手段への期待(2)から、一度広告・宣伝メールを受信をした者から拒否の通知を受けた場合の再送信を禁止することとしたものと考えられる。

- 1 送信前に拒否の有無を確認することは広告・宣伝を行おうとする送信者側の負担が過度に重いのではないかと
という点
- 2 「未承諾広告」の表示義務を課すことにより、当該表示のあるメールを技術的にブロックできるのではないかと
期待

しかしながら制度導入後、正当な営業活動の一環として広告宣伝メールが送信される場合に関しては、受信者側の意識や広告宣伝効果等から、オプトイン的な運用が大勢となっている一方、技術的手段に関しては、技術的にブロックされると、そもそも広告・宣伝としての意味をなさないとの点から、前提となる表示義務がほとんど守られず、効果を発揮できていないという結果が生じている。

さらにオプトアウト方式は、受信者からの拒否の通知が前提になるが、実態として、拒否の通知がかえって受信者が望まない広告・宣伝メールの送信を招く場合もあり、制度が円滑に機能していない。

こうした状況の下において、少なくとも受信者側の拒否が推定できるような場合には、本来の立法趣旨と法の実効性の強化の観点から、オプトイン的な方式を導入することが適当なのではないか。

なお、オプトイン的な方式での違反は、現行のオプトアウト方式での表示義務違反とは異なり、送信違反となるため、関係機関における送信防止のための措置が取りやすくなるのではないか。

2 国際的な整合性・連携の強化

特定電子メール法の制定時(2002年)においては、特定電子メール法は、迷惑メール対策として世界的にも先駆的な立法であったが、その後、各国で迷惑メール対策の立法が進み、我が国より、対策が強化されている国が多くなっている。

特に、広告・宣伝メールの送信の規制に関しては、主要国では、オプトイン方式を採用する国が多数となってきた()。

米国では、携帯電話あてを除いてはオプトアウト方式の制度となっているが、受信拒否要請後の電子メールアドレス売却・移転、他人のウェブサイトから自動取得したアドレスを使用した送信などを禁止している。

インターネットは国際的なネットワークであり、特に最近、外国発のメール等国境を越えて送受信される迷惑メールが増加していることから、国際的な連携の強化が急務であり、その前提として、我が国が国際的な迷惑メール対策の抜け穴とならないよう、制度的な国際的整合性を向上させることが必要と考えられる。こうした観点からも、オプトイン的な方式を導入することが適当ではないか。

3 オプトイン的な方式への移行に当たっての留意点

オプトイン的な方式への移行に当たっては、規制を必要最小限のものとする等、正当な営業活動における電子メールの利用に関し、過度な負担とならないような規制とすべきではないか。

・オプトアウトの問題点として挙げられている送信者に受信拒否の通知をすることがかえって迷惑メールを招くという点について。

2007年8月に(財)日本データ通信協会が実施したWebアンケートにおいて、「今後の受信を希望しない旨の通知を行った後、かえって広告や宣伝を内容とするメールが増えたと感じるか。」と質問したところ、「増えた」と感じている人は45%。

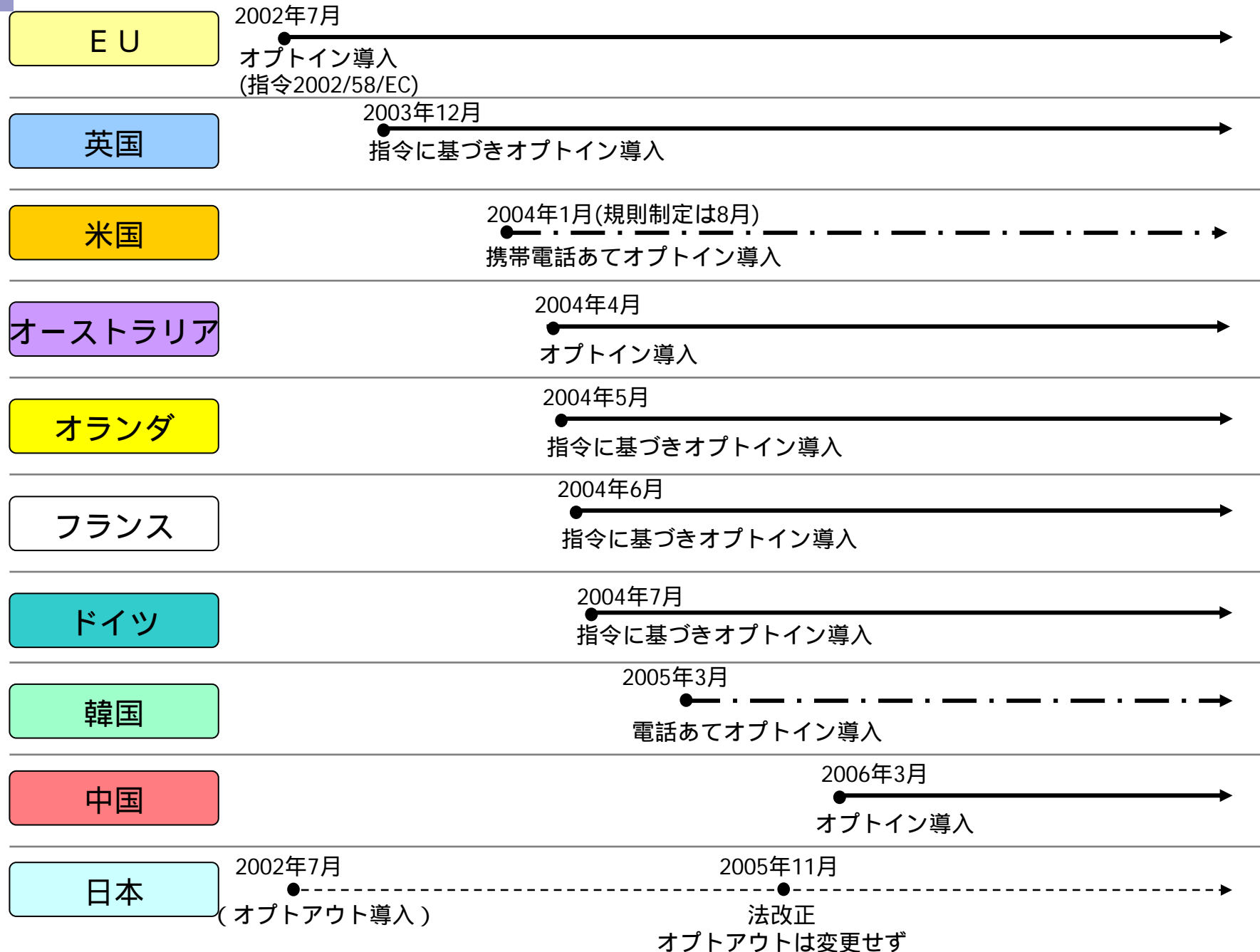
オプトアウトを行った結果、5ヶ月間のうちに、8150通の迷惑メールを受信したとの研究結果。

(出典:社団法人情報処理学会研究報告 2005年5月13日 中京大学長谷川明生氏他)

広告メールを受け取らないことを希望しない旨を通知したにもかかわらず広告メールの送信が止まらない、あるいは、当該通知をした結果かえって広告メールが増えてしまったとして、一般の消費者から寄せられた情報提供件数は、2006年度で1866件。

(出典:産業構造審議会特定商取引小委員会第7回会合配布資料)

各国のオプトイン導入状況



法の実効性の強化について

法の実効性の強化としては、現行のオプトアウト規制の見直しのほか、我が国の法制度全体との整合性を踏まえつつ、以下の事項を検討する必要があるのではないか。

- 1 迷惑メールの送信者にとって、迷惑メール送信のコスト、リスクが高くなる制度
現行法の規定が適用されず抜け穴となっている部分について可能な限り措置を行った上で、
 - ・迷惑メールに対する措置命令や罰則の適用を増加させられるような制度としていくべきではないか。
 - ・外国でも一定の効果が出ている例があり、迷惑メールの送信に対する制裁を強化すべきではないか。
- 2 迷惑メールの受信者にとって、迷惑メール受信の防止のコストやリスクがより低くなる制度
 - ・迷惑メール防止のための技術的措置が一層容易に利用できるように制度を見直すべき点はないか。
- 3 電子メールサービスを提供する事業者にとって、自主的な対策を行いやすくなる制度
 - ・電子メールサービスを提供する事業者が、迷惑メールの送信を防止するための技術の導入や約款等に基づく措置をとろうとする場合、そうした措置をとりやすくなるような制度としていくべきではないか。
- 4 法の執行機関にとって、法執行のための措置が円滑かつ機動的にとりやすくなる制度
 - ・措置命令等を行うために必要な違法行為者を特定するための情報の入手に関し、電気通信事業者等からの協力を得やすくするような制度としていくべきではないか。また、措置命令等に関し、より機動的に措置命令等を行えるような制度的な仕組みはないか。
 - ・迷惑メールの送信に関しては、受信者からの同意の取得や具体的な送信の指示について、送信を依頼する者が実質的に行っている場合もあり、迷惑メールの送信に関わる者全体に対し関係機関による有効な執行が可能となるような制度としていくべきではないか。



諸外国の罰則に関する規定

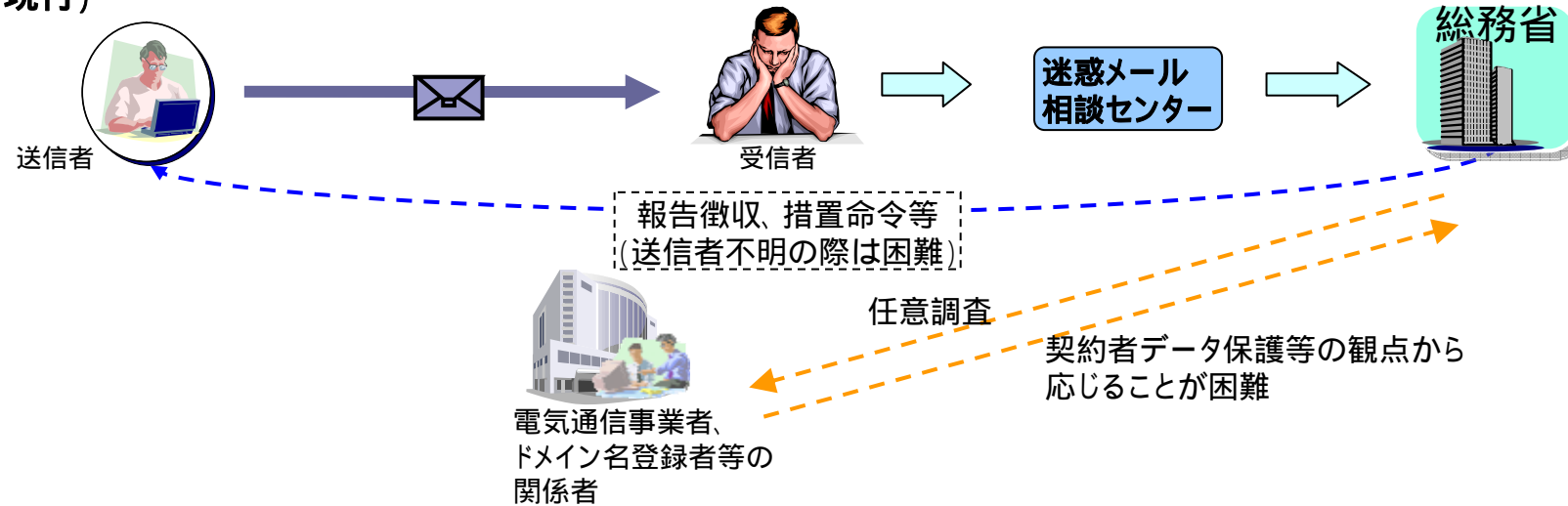
(罰金は最大額)

	罰則対象	個人に対する罰則	企業に対する罰則
米国 (CAN - SPAM法)	性的素材表示義務違反、重罪を行うため 又は再犯の場合の刑事罰規定違反 許可なくコンピュータにアクセスして送信、20 以上の電子メールアドレス又は10以上のドメイ ンを偽って登録、違反メールの大量送信、違反 メールにより多額の損害又は多額の利益、組 織の指導者等の場合(いずれも刑事罰規定) その他の刑事罰規定違反 (その他、課徴金等の制裁措置が若干あり)	5年以下の拘禁又は 25万ドル(約2900万円)の罰金(注) 3年以下の拘禁又は 25万ドル(約2900万円)の罰金(注) 1年以下の拘禁又は 10万ドル(約1200万円)の罰金(注)	50万ドル(約5800万円)の罰金 (注) 50万ドル(約5800万円)の罰金 (注) 20万ドル(約2300万円)の罰金 (注)
英国(プライバシー電子通信規制)	違反行為	5000ポンド(約120万円)の罰金	
ドイツ(テレメディア法)	「冒頭行及び件名欄に送信者及び通信の商業的 性格を隠したり、秘密にしてはならない。」に対す る違反	5000ユーロ(約800万円)の罰金	
フランス(郵便・電子通信法典)	オプトイン不遵守 個人情報たるメールアドレスの不正収集・不正 利用等	1通ごとに750ユーロ(約12万円)の罰金 5年以下の懲役又は30万ユーロ(約4800万円)の罰金	
オランダ(電気通信法)	違反行為	45万ユーロ(約7200万円)の罰金	
オーストラリア (2003年スパム法)	オプトイン、架空アドレスあて送信禁止違反 その他の違反 1日に2回以上 の違反 1日に2回以上 の違反	2200豪ドル(約22万円)の罰金 1100豪ドル(約11万円)の罰金 4万4千豪ドル(約440万円)の罰金 2万2千豪ドル(約220万円)の罰金	1万1千豪ドル(約110万円)の罰金 5500豪ドル(約55万円)の罰金 22万豪ドル(約2200万円)の罰金 11万豪ドル(約1100万円)の罰金
韓国 (情報通信網利用促進及び 情報保護等に関する法律)	オプトイン/アウト違反、表示義務違反 技術的操作禁止違反及び アドレス収集・売却・頒布・利用禁止違反	3000万ウォン(約390万円)の過料 1年以下の懲役又は1000万ウォン(約130万円)の罰金	

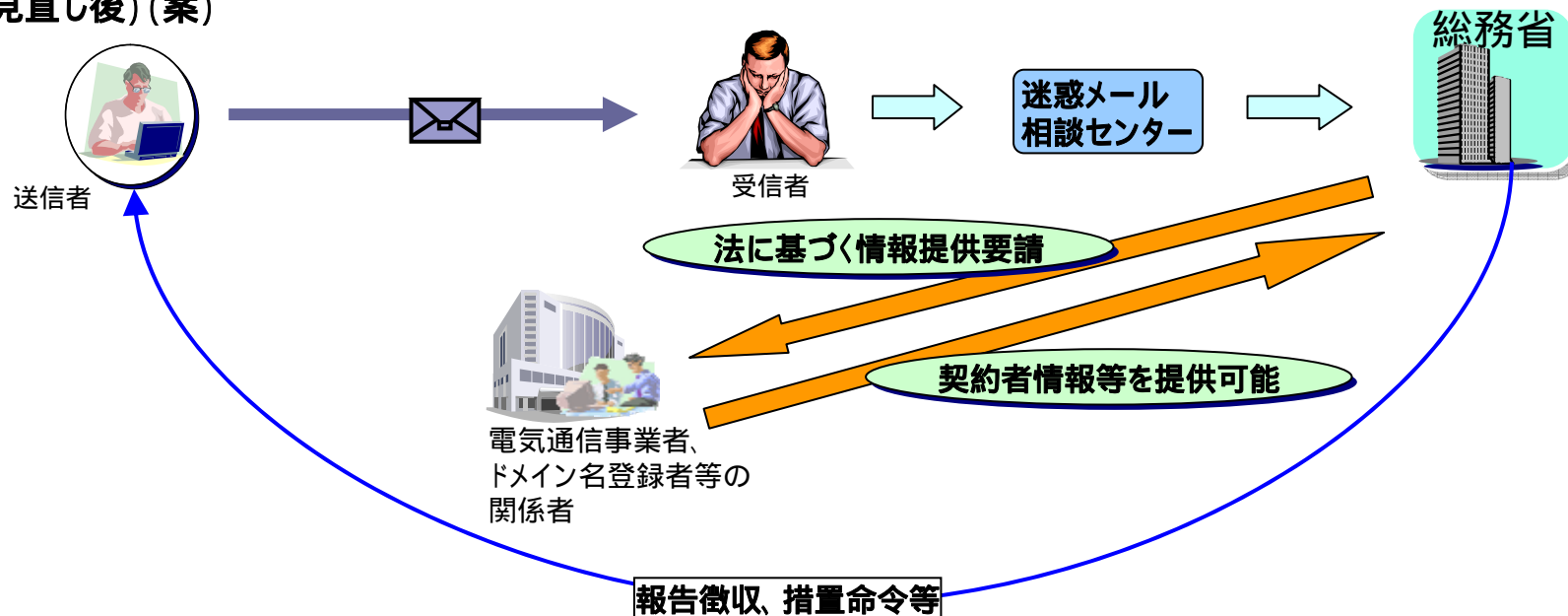
米国(注): [違反行為により被告が得た利益又は他者が被った損害の2倍の額]の方が高額な場合はその金額が上限となる。
為替レート: 1米ドル = 115円、1ポンド = 220円、1ユーロ = 160円、1豪ドル = 100円、1ウォン = 0.13円 により換算。

実効性強化のための改善策の例

(現行)



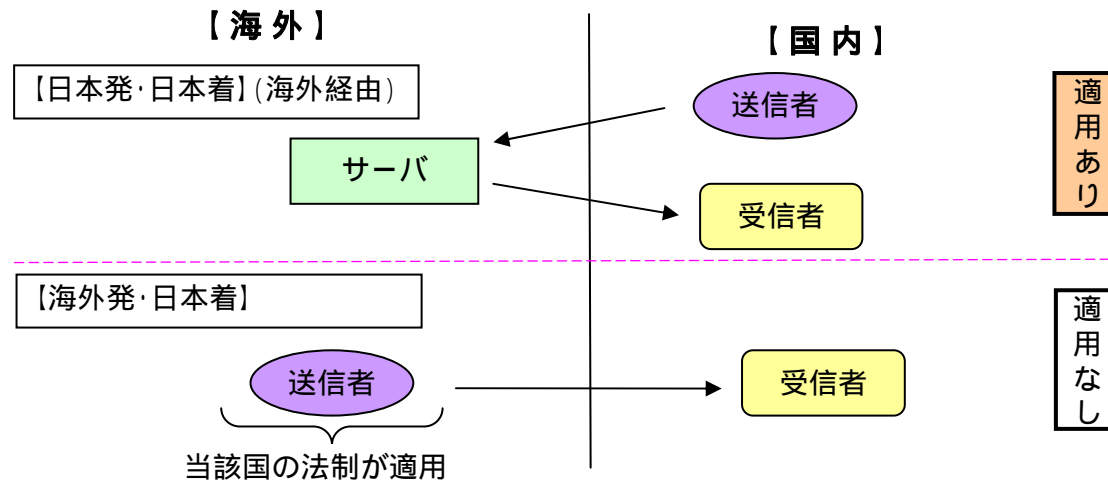
(見直し後) (案)



国際的整合性・連携の強化について

特定電子メール法

(現行法の適用関係)



諸外国の例

諸外国では、送受信者のいずれか一方が国外に存在する場合についても、法規制の対象に含める例が存在。例えば、オーストラリア(2003年スパム法)では、送信者、受信者、電子メールへのアクセスに使用される機器のいずれかが国内に存在する場合(オーストラリアン・リンクを含んでいる場合)に、規制対象となるとされている。

7 オーストラリアン・リンク

本法の目的のため、商用電子メッセージは以下のいずれかの場合に、またこれらの場合に限り、オーストラリアン・リンクを含んでいる。

- (a) そのメッセージがオーストラリアにおいて発信される。
- (b) メッセージを送信する個人もしくは組織、またはメッセージの送信を承認した個人もしくは組織が以下の条件に該当する場合。
 - (i) そのメッセージが送信されるときにオーストラリアに実在する個人、または
 - (ii) そのメッセージが送信されるときに、中枢管理機能または監督機能がオーストラリアに存在する組織。
- (c) そのメッセージへのアクセスに使用されるコンピュータ、サーバ、またはデバイスがオーストラリアに置かれている。
- (d) 該当する電子アカウント所有者が以下のいずれかの条件に当てはまる場合。
 - (i) そのメッセージがアクセスされるときにオーストラリアに実在する個人。
 - (ii) そのメッセージがアクセスされるときにオーストラリアにおいてビジネスまたは活動を行っている組織。または
- (e) 該当する電子アドレスが存在しないためにメッセージを配信できない場合 その電子アドレスが存在するものと仮定すると、オーストラリアにあるコンピュータ、サーバまたはデバイスを用いてそのメッセージがアクセスされるだろうと合理的に推定できる。

14 海外における適用

逆の意図が示されない限り、本法の適用はオーストラリアの外における行為、不作為、問題、および物に拡張される。

【マルチ（多国間）】

OECD「スパムタスクフォース」(04年7月～)

- ・ 06年4月までに「アンチスパム・ツールキット(包括的スパム対策)」を取りまとめて公表した。

LAP(ロンドンアクションプラン)(04年11月～)

- ・ 年1回の会合及び年最低4回の電話会議等を通じ、法執行の強化をテーマに議論。

スパム対策の協力に関する多国間MoU(覚書)

(05年4月～)

- ・ アジア太平洋地域の12機関が締結した覚書に基づき、具体的な協力策等について定期的に議論。

ITU

- ・ 世界規制庁シンポジウム(05年11月)等でスパム対策について定期的に意見交換。

APEC

- ・ 電気通信サブグループ等でスパム対策について定期的に意見交換。

ICPEN(国際消費者保護執行ネットワーク)

(92年～)

- ・ 国境を越える違法な対消費者取引行為を規制するために結成された会合。05年にはスパムの実態調査を行った。

【バイ（二国間）】

日EU定期協議(04年6月～)

- ・ 両者のスパム対策等について意見交換。

日仏定期協議(04年12月～)

- ・ 両国のスパム対策等について意見交換。
(06年5月、パリにて、スパム対策に関する共同声明が署名された。)

日米情報通信政策協議(05年7月～)

- ・ 両国のスパム対策等について意見交換。
(07年4月、米国FTC消費者保護次局長と総務省電気通信事業部長が会談)

日加情報通信政策協議(05年10月～)

- ・ 両国のスパム対策等について意見交換。
(06年10月、オタワにて、スパム対策に関する共同宣言が署名された。)

日豪情報通信政策協議(05年10月～)

- ・ 両国のスパム対策等について意見交換。

日英定期協議(06年7月)

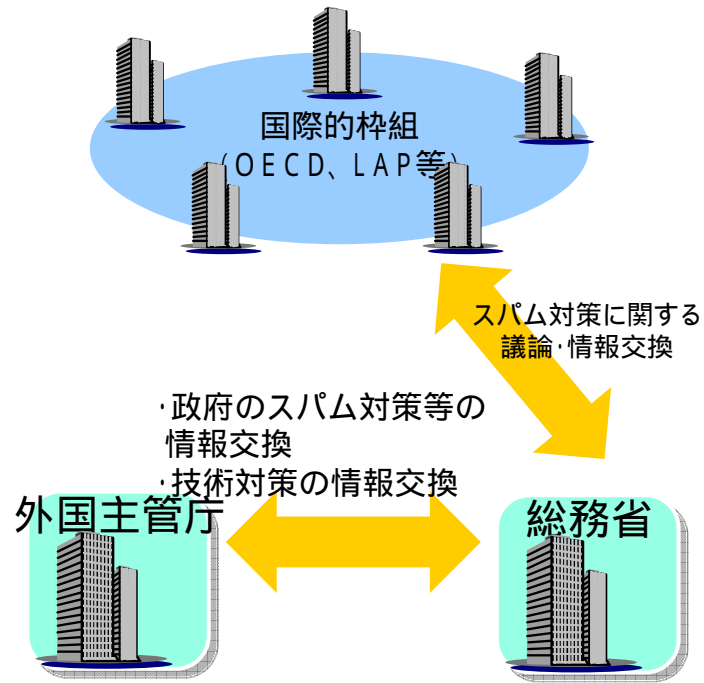
- ・ 両国のスパム対策等について意見交換。
(06年9月、東京にて、スパム対策に関する共同宣言が署名された。)

日独情報通信政策協議(06年9月)

- ・ 両国のスパム対策等について意見交換。
(07年7月、スパム対策に関する共同声明が署名された。)

今後の国際連携の方向性

これまでの取組



今後の取組の方向性

