迷惑メール対策と通信の秘密
Internet Week 2006 JAIPA行政法律部会
パネルディスカッション資料

2006年12月６日

JAIPA行政法律部会　副部会長
木村　孝(ニフティ株式会社）

インターネットと通信の秘密

総務省　電気通信サービスFAQから

http://www.soumu.go.jp/joho_tsusin/d_faq/

5-4「通信の秘密の保護」に関する法律と「通信の秘密」として保護される範囲について教えてください。

（前略）このように通信の秘密が保障されなければならない理由には、通信の内容だけでなくその存在の秘密が確保されることも含まれるものですから、上記の各法律の保護の及ぶ範囲は、**通信内容だけでなく、通信当事者の住所、氏名、通信日時、発信場所等通信の構成要素や通信の存在の事実の有無を当然に含むものです。**（後略）

5-5 インターネット上の通信も「通信の秘密」として保護されるのですか。

インターネットを利用して行われる通信であっても、インターネット接続事業者のサービスを利用して行われるような場合には、電気通信事業者の取扱中に係る通信の秘密に該当し、電気通信事業法に定める保護が与えられることになります。それ以外の場合であっても、必要に応じて有線電気通信法、電波法等の保護が与えられることになります。

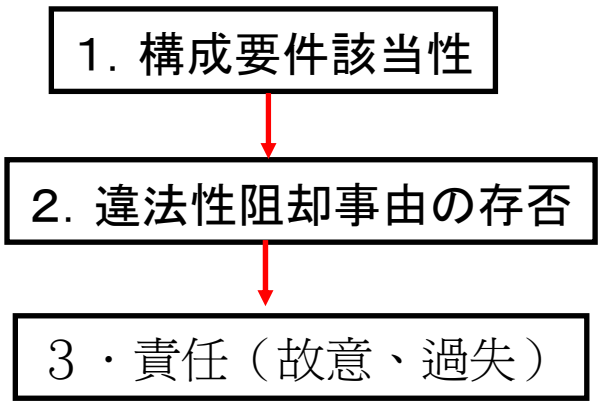
迷惑メール対策と通信の秘密

- 最初に問題になったのは2005年始め、25番ポートブロック(OP25B)の実施
- 2005年7月15日　JEAGの総会で、総務省課長補佐から口頭で25番ポートブロックが正当行為となるとの説明がされた

「OP25Bは利用者の同意なしでは「通信の秘密」の侵害、ただし正当業務行為」

- 同時に「初期設定をフィルタリングオンの状態で提供するための条件」についても口頭で説明がされた。

違法性の判定フロー



a.目的の正当性、b.手段の相当性

総務省見解　ISPによる迷惑メールフィルタリングについて

2006年1月23日　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（第18回会合）で、電気通信事業者が行う電子メールのフィルタリングと電気通信事業法第4条（通信の秘密の保護）の関係について基本的考え方が公表された。

初期設定をフィルタリングオンの状態で提供するための条件

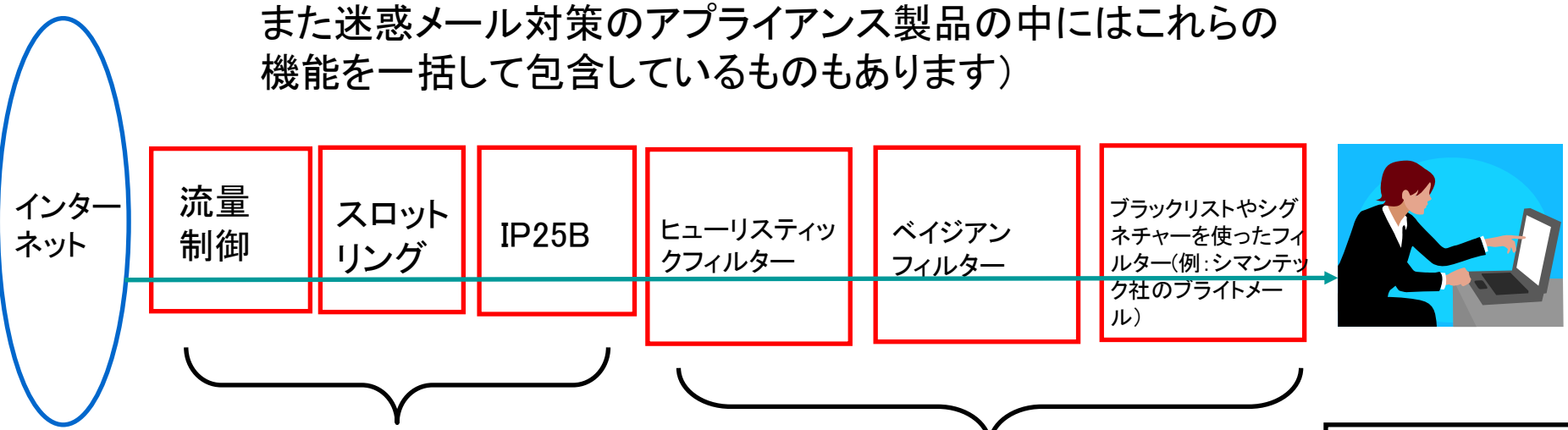
- 利用者が、いったんフィルタリングサービスの提供に同意した後も、随時、任意に同意内容を変更できる状態（設定変更できる状態）であること
- フィルタリングサービス提供に対する同意の有無にかかわらず、その他の提供条件が同一であること
- フィルタリングサービスの内容等が明確に限定されていること
- 通常の利用者であれば当該サービスの提供に同意することがアンケート調査結果等の資料によって合理的に推定されること
- 利用者に対し、フィルタリングサービスの内容等について、事前の十分な説明を実施すること（事業法第26条に規定する重要事項説明に準じた手続により説明すること）

http://www.soumu.go.jp/joho_tsusin/d_syohi/060123_1.html

ISPにおける迷惑メール対策(受信側)

通常ISPは多段階のフィルタリングにより迷惑メール対策を施している

注:この図は一般的な考え方を示したもので、実際にこの順番ですべての処理を行っていることを示すものではありません。また迷惑メール対策のアプライアンス製品の中にはこれらの機能を一括して包含しているものもあります)



自社の設備を守るため(全員一律)

利用者の希望によりオプションで提供(振り分けられた迷惑メールはサーバー上のフォルダに一定期間保管)

送信ドメイン認証の結果を使ったフィルタリングはまだ表示の追加(ラベリング)にとどまる　一部のISPのみ

特定電子メールの送信の適正化等に関する法律 11条が根拠

基本的に受信者の個別の承諾なしにはISP側でフィルタリングすることはできないため

総務省が迷惑メール対策と通信の秘密の考え方を公表

インターネット協会　第3回迷惑メール対策カンファレンスで発表
2006年5月16日

http://www.iajapan.org/anti_spam/event/2006/conf0516/index.html

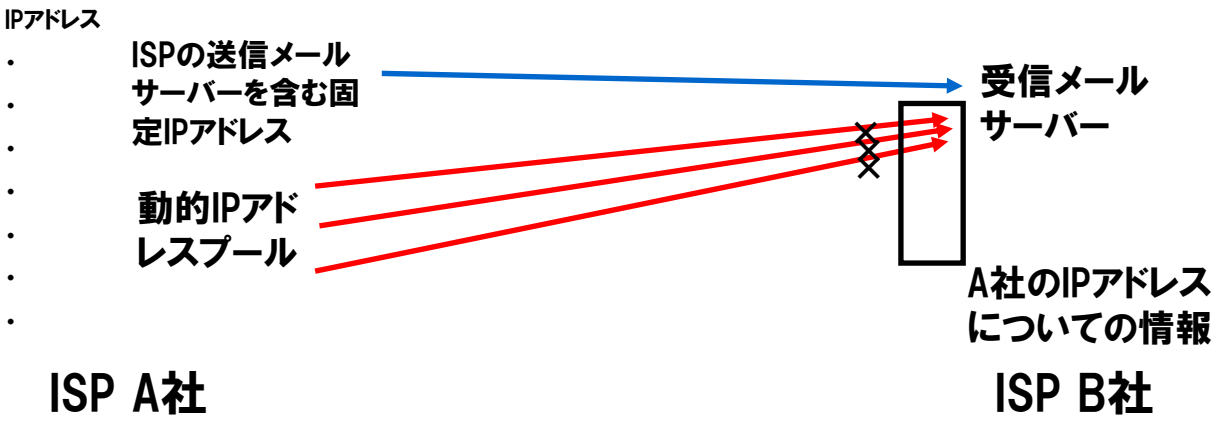
「迷惑メール対策技術導入を検討されている事業者の方へ」
2006年11月14日　公表

http://www.soumu.go.jp/joho_tsusin/d_syohi/jigyosha.html

・送信ドメイン認証及び25番ポートブロックに関する法的留意点の概要
・受信側における送信ドメイン認証技術導入に関する法的な留意点
・Outbound Port 25 Blocking導入に関する法的な留意点
・Inbound Port 25 Blocking導入に関する法的な留意点

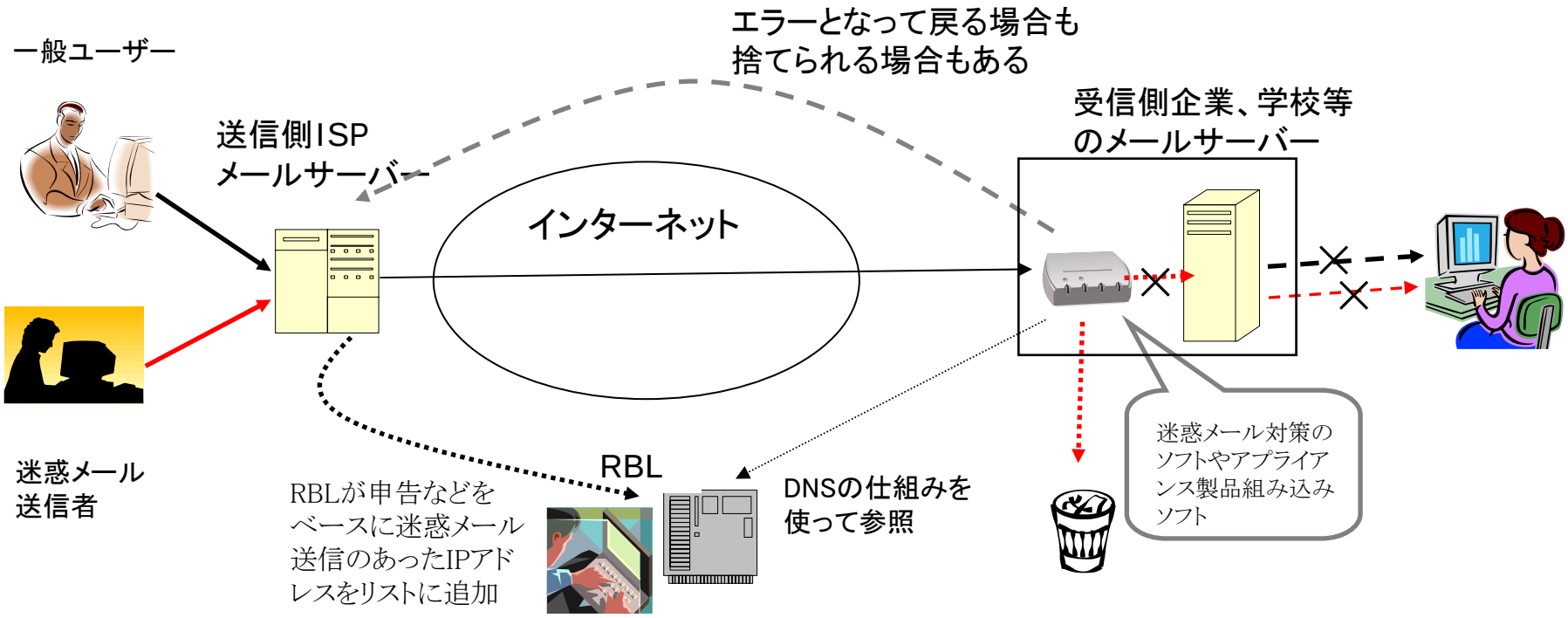
IP25Bとは

- OP25Bがメール送信側のISPにおいて、動的IPアドレスからの外向け25番ポートを閉じることで大量の迷惑メールを送ることを困難にする措置
- IP25Bはメール受信側のISPにおいて、送信元のISPの動的IPアドレスからの送信をブロックすること。
- IP25Bのためには自社以外のISPの動的IPアドレスレンジについての正確な情報が必要
- 総務省も正当業務行為として認めているが、実際の導入に当たっては相談して欲しいと言われている。
- 公にIP25Bを行なっていると公開しているISPは少ないと思われる。
- しかし実際には受信側ではIP25Bを行っていることは送信者に対して一般的に周知することは必要かも知れない。
- 動的IPアドレスのレンジを公開しているISPも少ない。しかも頻繁に変更、追加があるので正確な最新情報の把握、管理は難しい



RBL (Real-time Black List)

- 通常RBL自身ではフィルタリングを行なうものではない。受信側メールサーバーに組み込まれた迷惑メール対策製品が各種のRBLを参照することにより、迷惑メール送信元とリストされているIPアドレスからのメールを受信できないようにする。
- その場合の結果は無視される場合や送信元に返される場合などあるが、それは受信側の実装により異なる。
- 日本では通信の秘密との関係でISPが利用者の同意なしにRBLを参照することは違法とされている。



アメリカには「通信の秘密」の概念がない

アメリカ合衆国憲法にはそもそも「通信の秘密」という言葉がない

連邦通信法ではそもそもIPベースのサービスは電気通信サービスではなく、情報サービスとして分類されている。

規制としては情報サービスとしても、本当にインターネット上の「通信」内容に秘密は保障されていないの？

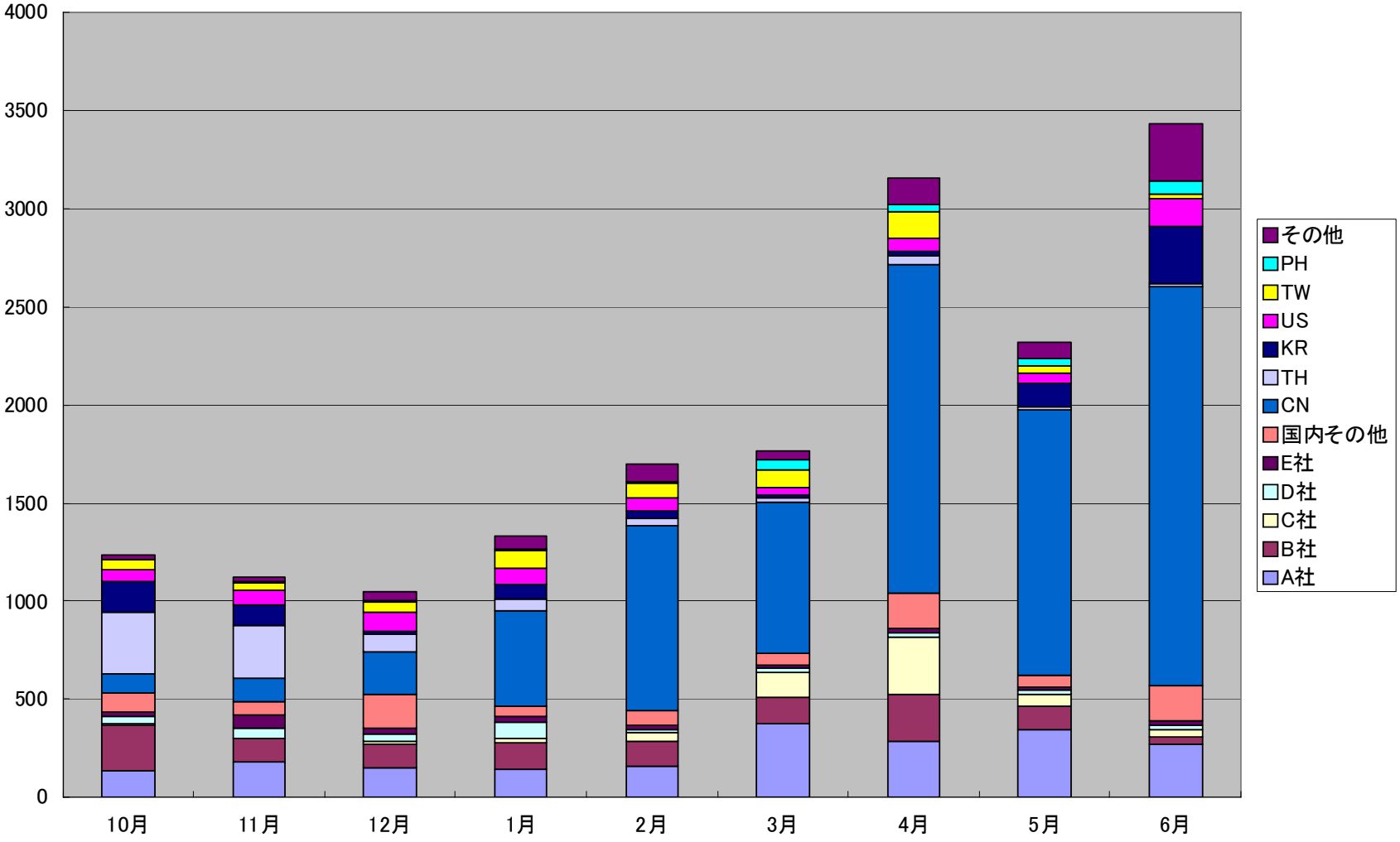
平成15 年度社会安全研究財団委託調査研究報告書
「アメリカにおけるハイテク犯罪に対する捜査手段の法的側面」報告書
「犯罪捜査におけるコンピュータ捜索・差押および電子的証拠の獲得」
(司法省マニュアル)の翻訳とその解説 平成16 年3 月

米国においては、「通信の秘密」という概念は、特に定められておらず、むしろ、「プライバシーの合理的な期待」という表現のもとに「通信の秘密」に対応する法的利益の擁護が図られている。

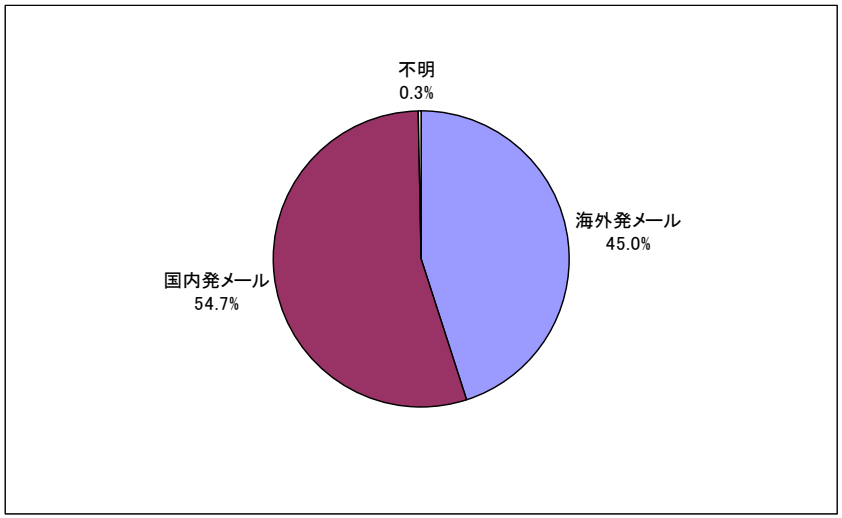
アメリカ合衆国憲法　修正4条（1791年）

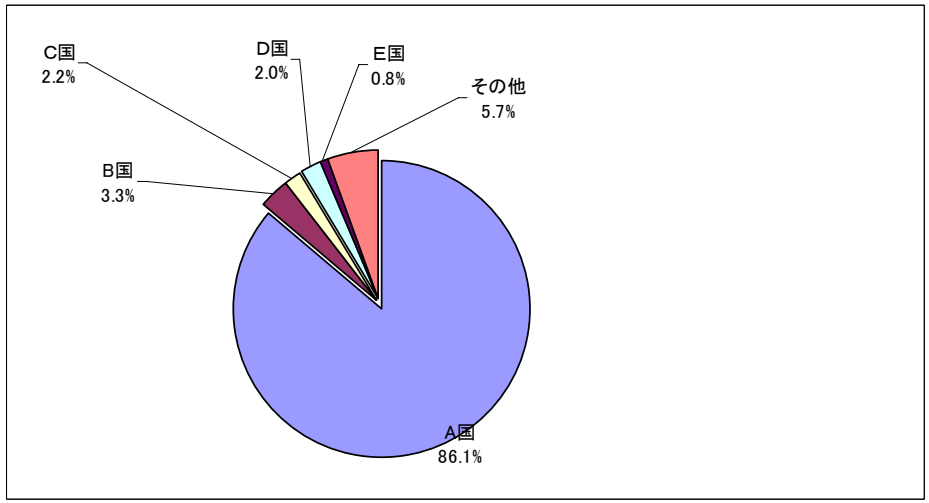
不合理な捜索及び逮捕・押収に対してその身体、住居、書類及び所有物が保障されるという人民の権利は侵されてはならない。また令状は宣誓または確約によって裏付けられた、相当な理由に基づいていて、かつ、捜索される場所及び押収される人または物を特定的に記述していない限り、発せられてはならない。

ある外部のモニター機での状況では



ある別のモニター機の状況



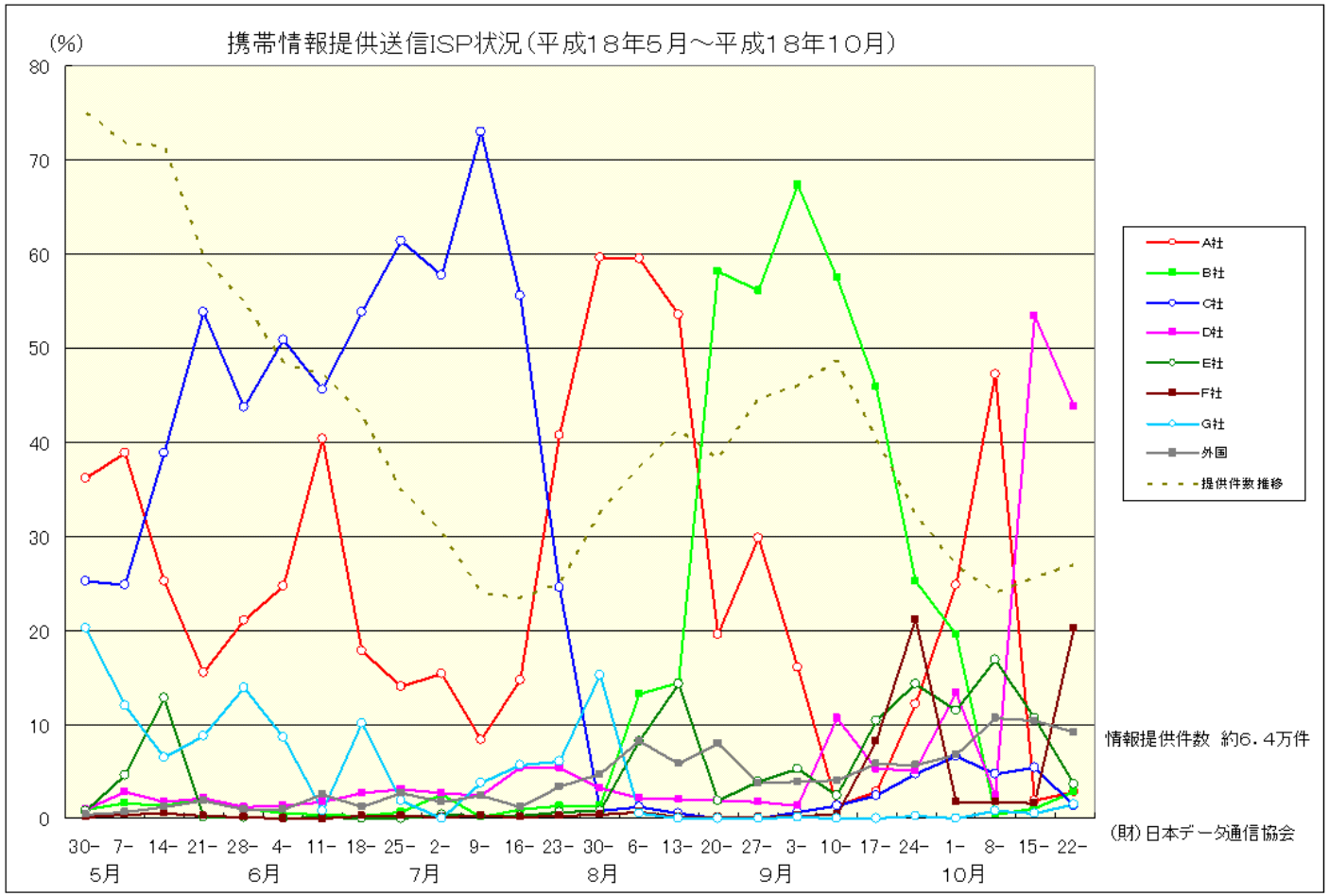


n=12116

時期　2006年9月　n=26932 携帯及びPC

OP25B対応ISPからの迷惑メール送信の減少（携帯電話向け）

（財）日本データ通信協会あてに情報提供された携帯宛違法メールの統計から



http://www.dekyo.or.jp/soudan/taisaku/i2-1.html#result3

自分宛に届いた迷惑メールを発信国別に分析すると