・特別企画：テクノロジーから国際情勢まで8人が語る・

「監視」「規制」されるinternet

ユーザーの秩序にゆだねられていたインターネットだが、1億数千万人まで人口が増加し、規制が必要だという議論が絶えなくなっている。そんな中、日本では改正風営法のような規制のための法律が登場している。一方で、「盗聴法」のようにインターネットでの通信を監視する法案が審議されている。ジョージ・オーウェルが「1984年」で描いた「ビッグブラザー」の出現を懸念する声もある。本当にインターネットに法律は必要なのだろうか？　インターネットの「規制」と「監視」について見ていくことにする。

Fukutomi Tadakazu
福冨忠和

法制化が進むインターネット

拙速な審議が問題

盗聴法か通信傍受法か

7月初頭、衆議院で盗聴法（通信傍受法案）の審議が行われている。法案批判の筆頭である保坂展人議員とテレビ朝日社員の電話での会話が盗聴され、そのテープが警察官を名乗る人物から報道機関に送りつけられるなどのできごとが報道されている。

「盗聴法」という呼称について法務省がマスコミ各社に「通信傍受法」と呼ぶように要請し、野党が抗議する一幕もあった。議会の審議でも同様の要請に福島瑞穂議員が「言論の自由」を楯に反論している。

国際要請による緊急性はない

しかし、財産没収などの項を含む組織犯罪対策三法が、当初からその一部である盗聴法に代表されて呼称されてきたのも理由がある。一般に「欧米など主要各国では盗聴捜査が合法化されており、国際的な法制化の要請がある」と法整備の必要を説明される。

ところが盗聴については、FATFが設立された1989年のアルシュサミット経済宣言以降、要請の事実は見られない。逆に「国際組織犯罪に対するナポリ政治宣言及び世界行動計画」（1994年）では、「電子的監

立では説得力はない。当時のオウム真理教は正規の宗教法人であり、正規の弁護士が一連の犯罪に荷担していたと言われるからだ。

問題が大きいインターネット

インターネットユーザーにとって、法案の問題点は電話以上に大きい。

電話の盗聴では無関係な会話が交わされたときに会話の録音を止めるなどの法案上の歯止めがある。従来の家宅捜査でサーバー上の電子メールを押収する場合も、全押収物の目録が立会人に交付される。しかし、インターネット盗聴の場合はこういうチェックがきかない。サーバーから電子メールを拾い出さなくても（国会の議論では、これは盗聴ではなく押収とされている）、専用線を盗聴したり、ルーターとサーバーの間にネットワークプロトコルアナライザーのような機械を設置して特定の通信を抽出したりすることもできる。

メールサーバーの設定ファイルに電子メールをコピーして別のアドレスに送るように一行プログラムを書くだけで、警察官が警察署にいながら盗聴することも可能だ。こういう方法を果たして盗聴と呼ぶべきかどうかは疑問もあるが、法案に具体的な方法について書かれてはいないのだ。

さらに、電話はリアルタイムの会話だが、サーバーに届く電子メールは本人が読んだとは限らない。他人をおとしめるために電子メールを送りつけ、密告するなどの方法はいくらでも使える。また、高度な暗号を利用するなど、確信犯的な組織犯罪者は盗聴捜査を回避できるのに、無防備な一般人ユーザーが簡単に対象になりやすい。

暗号利用に規制がかかる

同じ国会に不正アクセス禁止法が上程されていることも気になる。不正アクセス禁止法は、システムを破壊しなくてもサーバーなどへの無断のアクセス自体を罪とするものだ。インターネットにおける家宅侵入罪のようなものだが、不正に対する恣意的な判断が横行することも予想される。

同法案審議過程で警察庁が「アクセスログの保存義務」規定を主張したのに対し、郵政省が「通信の秘密」の観点から保存すべきでないと反対して見送られたのは当然だろう。しかし、この法律はネットワーク犯罪防止法として、キーリカバリー制度など、暗号の利用規制条項とともに外郭団体から答申されていた。「暗号の利用制限」はもちろん、盗聴捜査が可能となることを見越してのことだった。

ビッグブラザーの出現か？

国会には「国民総背番号制」こと住民基本台帳法の改正案も上程されている。現在のコンピュータの検索技術・能力から考えれば、たかだか住民票の発行のために国民に通し番号を添付する必要はないだろう。にもかかわらず「番号」が必要なのは、ほかのシステムとの間で横断的にこの番号を活用することが前提になっているからにほかならない、という指摘がある。

このように盗聴法、不正アクセス禁止法、国民総背番号制など、ネットワークにかかわる法案が同時期に登場してきた経緯から、犯罪対策を越えた「1984年」のような国家の思惑を見て取る向きも多い。どれも拙速な審議で決めるような法案ではないのだ。

視、潜入捜査、コントロールデリバリーなどの証拠収集の方法」について、「人権及び基本的自由、特にプライバシーの権利を完全に尊重しながら、適切な司法承認又は監督下で運用される場合には、検討されるべきである」と書かれている。印象として緊急性は感じられず、その結果、盗聴法の特異性が反対派の中でクローズアップされた経緯がある。

また、「盗聴ができれば地下鉄サリン事件は防止できた」という指摘も、宗教関係者や弁護士を盗聴可能対象から外しての法案成

インターネット関連法（案）（7月15日現在） 編集部

盗聴法：参議院で審議中●組織犯罪対策法の1つ。2人以上で行われる組織的な犯罪を未然に防ぐために、犯人が行う電気通信の警察による盗聴を認める。しかし、その法案の内容は電話を想定したもので、同じ電気通信であるインターネットにそぐわない内容となっている。犯罪とは無関係な通信についても盗聴される可能性が非常に高くプライバシーの侵害にあたるとの意見も多い。「日本が認めたことのない新しい捜査方法を採用するかどうかという大きな転換点」（牧野二郎弁護士）にきている。

改正風俗営業法：4月1日より施行●無店舗で営業する風俗店（出張ヘルスなど）やインターネットの有料アダルトサイト（アダルトサイトでなくても「性的好奇心そそるため」の映像を掲載している有料サイト）などに対して公安委員会への届け出を義務付けている。また、アダルトサイトがわいせつな映像を配信できる状況にある場合は、プロバイダーがその送信を防止するために必要な措置を取らなければならないというプロバイダーの努力義務が盛り込まれている。アダルトサイトでも客が18歳未満かどうかを確認しなければならないという問題もある。

不正アクセス禁止法：参議院で審議中●他人のIDやパスワードを盗用して無断で入力したりセキュリティーのバグをついたりすることで、コンピュータやネットワークに侵入することを規制。技術に長けた確信犯的なクラッカーは不正にコンピュータに侵入する場合、痕跡を残さないことが普通であり、高校生などのいたずらレベルの犯罪が対象になるのではとの疑問もある。

改正住民基本台帳法：参議院で審議中●住民票にコード番号を付けてコンピュータで一元管理するための改正法案。いわゆる国民総背番号制の法制化。住民票に10ケタのランダムなコード番号が付けられ、ひとりひとりが違う番号を持つことになる。また、市区町村長は住所や氏名などの4つの情報と住民票番号を都道府県に通知する。これによって住民はどこの市区町村役場でも住民票の写しを取れるようになる。一見便利であるが、コンピュータネットワークが当たり前になるとどこからでも本人確認のために利用されることが懸念されている。

REGULATION

4人の論客がインターネット関連法を語る。

**慎重に審議されなければならないと思われる法案が次々と可決の方向に向かっている今国会。
この法案の多くは実をいうとインターネットを始めとするコンピュータ通信に関連するものだ。
そこで、インターネットに詳しい各方面の論客にこれらの法（案）について意見を伺った。**

[インフォシーク取締役会長]

伊藤穰一

ほかにもPSINetの取締役など肩書きは多数。郵政省や警察庁のネットワーク関連の委員なども務める。

●盗聴法

今後の暗号の規制に絡んでくると思うんだけど、**暗号や匿名システムを企業がビジネスとして成立させなければならない。**そうなれば、政府としても手が出しにくいと思う。匿名システムの間違った使い方は多いが、それ以上のメリットのほうが大きいはず。

●不正アクセス禁止法

ログの保存義務がなくなったことを考えれば、悪い法律ではないと思う。ただ、警察に捜査のリーダーシップを取ってほしくないですね。**実際の捜査はプロバイダーとかセキュリティー会社がやって**、警察の力が必要なときにこの法律の下で動いてもらうのがいい。

●改正風営法

この法律が簡単に通ってしまったのは**「新聞社」と「出版社」の怠慢**だと思う。オンラインでの出版という彼らのビジネスの範囲を叩かれているのに何も言わなかったのはおかしい。僕はどちらかと言うと警察は悪者ではなくて、何も言わなかった出版社が怠慢だったと思う。

[富山大学経済学部教授]

小倉利丸

盗聴法を始めとするインターネットの規制問題に詳しい。「インターネットの検閲に反対するメーリングリスト」などで活動中。

●盗聴法①

国会で一番問題になっているのはインターネットなんです。しかし、インターネットを含むコンピュータの通信が**法案の中で極めて曖昧な形でしか表現**されていない。想定されている条件がインターネットを前提とした場合に整合性が取れたものになっているかという法案を議論する前の段階。

●盗聴法②

法案では暗号に関してはすべて盗聴できるとなっているんです。画像の中に暗号も埋め込めるので、画像もすべて暗号ということになる。パケットもそのままでは読めないので暗号なのかということになる。暗号だと見なされたら**インターネットの通信はすべて暗号**だということになってしまう。

●規制全般

言論の侵害はいままで何度もありました。しかし、いまは**犯罪ではない言論があたかも犯罪のように語られ始めている。**たとえば、殺人の話を電子メールでやり取りするのは、殺すことではなくて「殺人」をテーマにしたコミュニケーションなんです。それが犯罪のように見なされている。

[株式会社ベッコアメインターネット代表取締役]

尾崎憲一

1996年のベッコアメ事件から「強制捜査を受けない月はない」と、氏自ら語るほどプロバイダーに対する警察の捜査に詳しい。

●盗聴法①

強制捜査のための令状を持ってこられるのは、犯罪が確定してユーザーが特定できたからです。ところが、通信傍受法というのは捜査段階で出てくる令状です。捜査をした結果、こいつが悪者であるという特定の令状が出てきてた場合でも大変なことになるのに、傍受令状を行使されてしまうのは経済的にも大変なことになる。いまの捜査は20分から1時間ぐらいで短いですが、傍受となると1日24時間で1か月ぐらいになるわけです。まさかルートのパスワードをどうぞということはできないので、僕らが協力しなければならない。人的資源も必要になって、**中小企業だと張り付きで協力することは経済的にマイナス要素が出てくる**わけです。ログも容量も1日にCD-ROM一枚分ぐらいある、それをとっておくのも大変なんです。

●盗聴法②

（ベッコアメが最初に受けた）強制捜査で該当ユーザーのメールボックスをごっそり持っていこうとする。これは盗聴の枠に入ると思うんですよね。**盗聴が行われる捜査というのは、インターネット捜査史上では最初から行われていた**ということになります。

[弁護士]

牧野二郎

インターネット弁護士協議会代表。インターネット関連の法律にもっとも詳しい弁護士の一人。

●盗聴法

はっきり言って**一般の方でも盗聴されます。**これはデフォルメでも嘘でもなく、メーリングリストの中に1人でも犯罪者がいたら全部読まれますから。警察の態度には盗聴法をてこにして「捜査機関に白紙委任してほしい、あとのことはは国民は考えなくていい」というスタンスが見えかくれする。

●改正風営法

この法律は**米国で無効になった通信品位法にそっくり。**お金をとってアダルト情報を流す＝風俗営業になっていますが、では「一般の男性週刊誌は何だ」という話になります。通信品位法の判決の中で言われているように、インターネット上の情報流通は出版行為そのものなんです。出版は表現の自由そのもの。日本の警察はウェブが出版であるとは考えていないらしい。もう1つ問題があります。アダルトサイトを見るためには、成人であることを証明するために業者側にあらかじめ身分証明書を送付する必要があります。一方でアダルトサイトは「暴力団の関係者が経営している」から規制が必要だと警察は公然と言っています。この2つをくっつけると、「暴力団に君たちの下半身情報を渡しなさい」と言っているわけなんです。

コンテンツのレイティングは正当なのか

民間から沸き起こる「規制」

sakichan@isoternet.org
Sakiyama Nobuo
崎山伸夫

「監視」「規制」されるinternet

CDAに対する技術的解決策

最近フィルタリングソフトという言葉が一般的になってきた。これは、エンドユーザーのウェブサイトなどへのアクセスをコンテンツに依存して遮断するもので、米国での通信品位法（CDA）への反対に際して「技術的解決策」として登場した。形態としては各クライアント機器にインストールして使うものとプロキシーサーバーとして動作させるものがある。いずれの場合も、ユーザーがアクセスしたウェブページについて格付け（レイティング）情報を取得し、フィルタリングのためのプロファイルと比較してアクセスの許可／禁止を判断する。

ウェブの場合、既存メディアと異なって複数の格付けがあり、また情報発信者が知り得ない一方的な第三者による格付けが広く行われている。多くの格付けでは、単一の年齢による基準ではなく複数のカテゴリー、たとえば「性」や「暴力」といったものそれぞれについてその程度を数値で表現する（含む／含まないの2値の場合もある）。

自己格付けの場合はW3C標準のPICSに基づいて特定の格付けサービスの定義に従って行われる。このPICSの例としては、主要なブラウザーでサポートされているRSACiが最も有名だ[注]。第三者による格付けは、フィルタリングソフトでの自動的判断と格付け機関によるリストがある。前者はURLやコンテンツ中の単語のスコアリングによる。格付け機関によるリストは、PICS準拠のデータベースと製品独自の形式で提供されるものとがある。

PICS使用のガイドライン
Jump www.w3.org/TR/NOTE-PICS-Statement

RSAC
Jump www.rsac.org

民間レベルの検閲という意見

フィルタリングソフトへの代表的批判は「民間レベルの検閲である」というものだ。PICSを制定したW3Cに対しても同様の批判があり、その結果、1998年6月にPICS使用についての非公式ガイドラインが出ている。これはPICS対応ソフトの作成・使用・運用にあたって、多様性の尊重、透明性の確保（基準の開示、情報発信者に対しての格付けの開示、訂正権）、説明責任（エンドユーザーに対してと管理者に対して）を満たすように求め、そのための具体的な方法を述べている。

ところが、これらの理念をPICS対応のサービスやそのほかのフィルタリングソフトが満たしているとは到底言えないのが実情だ。

フィルタリングソフトの多くが開発されている米国では、フィルタリング推進派は反同性愛・反フェミニズムの宗教保守派との関係が強く、こういった内容が格付けリストに反映されているケースが少なくない。

同性愛に関するコンテンツをおしなべてポルノ扱いする場合もあれば、「同性愛」というカテゴリーを用意してブロックすることを推奨しているケースもある。

The Censorware Project
Jump www.censorware.org

強制法案が下院を通過

また、格付け基準はほとんどの場合に主観的で曖昧である。反復可能性を意図した格付け規則を公開しているのはRSACiのみである。そのRSACiでさえも米国中流層の文化的背景を持たない人にとっては正しく格付けを行うことは困難だ。

さらに製品独自の格付けサービスでは、独自の自動格付け技術の卓越性や匿名の格付け担当者の経歴や人数を誇るばかりで基準はまったく示されない場合がほとんどである。第三者格付けの場合、仮にデータ全体の開示があれば帰納的に基準を読み取ることは不可能ではないが、サービス提供者にとってはデータベース全体は企業秘密に属する知的財産であり、開示はまずありえない。個別の格付けデータの開示さえもまったく行われていない場合が多い。

フィルタリングソフトがこのような質のものである一方で、強制の動きが強まっている。現在アメリカでは学校と図書館でフィルタリングソフトの使用を強制する法案が下院を通過し、上院でも委員会を通過している。また、RSACiをベースにして国際的な標準格付けをめざすICRA（Internet Content Rating Association）という団体も作られている。

日本では通産省系の業界団体である電子ネットワーク協議会が情報処理振興事業協会の資金を得て、半官半民のPICS準拠の格付け機関を構築している。RSACiを手本としつつ、第三者格付けを中心とし、かつ、透明性や説明責任のための技術的条件を意図して実装しない姿勢をとっているが、教育用ネットワークでの採用が広がっている。

[注]：RSACiはRSAC（Recreational Software Advisory Council）が制定したインターネット用格付けサービス。RSACは名前からわかるように、もとはコンシューマー向けゲームソフトの格付けのために設立された。

Suzuki Hironobu
鈴木裕信

時代遅れな「キーエスクロー」

政府による暗号システム介入はあるか

政府が復号できる

キーエスクローの基本アイデアは、人々が暗号化したデータの内容を政府が復号してその内容に自由にアクセスできるというものだ。このアイデアは米国政府内に古くからあったらしいが1993年に初めて表に出てきた。英語のエスクロー（escrow）という言葉は法的権限を持つ執行機関に委託するというニュアンスを含むので、推進する側は途中からソフトな響きの「サードパーティーキーリカバリー」という言葉を使い始めた。「第三者による鍵回復システム」というなんとなく中立的な響きを持つ言葉に変えてはいるが、本質は何も変わってはいない。ここでは、もちろんキーエスクローという言葉を使う。

結論を言えば、もう死んでしまった過去の話でいまさら解説もないだろうという気もする。現在（キーエスクローなど使わない）安全な暗号システム使い、コンピュータシステムの安全性とプライバシー保護を高めようという法案（SAFE act, HR 850）が米国議会に上程されている。

Americans for Computer Privacy
Jump www.computerprivacy.org

非現実的なシステム

技術的見地から言って、インターネット時代においてキーエスクローはあきれるほど非現実的な方法だからだ。論点は次の3点だ。

①時代遅れなコンピュータ利用モデル
②管理コストが膨大
③集中管理は極めてリスクが高い

「監視」「規制」されるinternet

①について見てみると、キーエスクローでは暗号システムが特殊なシステムにしか使われないとしか考えていない。インターネット時代のコンピュータでは、安全性確保のため暗号システムは各所に使われている。たとえば、今日の普通のパソコンユーザーですらPGP、S/MIME、SSH、SSL程度の複数の暗号システムを使っているし、さらに安全性を必要とする人たちは暗号化ファイルシステムやIPv6のような暗号化可能な次世代IPなどを使っている。それ以外にも個々のアプリケーションにはファイルを暗号化する機能が入っている。このような別々の暗号システムを同時に使っている時代に、暗号システムごとに鍵を申告してから使うなどというのは非現実的である。

キーエスクローは無意味なだけではなく、余計なことをする分、セキュリティーホールを作り出す危険性が高い。キーエスクローによって、これらの安全性の高いシステムを危険な状態にしてしまっているようでは本末転倒である。

次は②に関してである。いまやコンピュータはどこにでもある。その莫大な数のコンピュータに使われている複数の暗号システムの復号鍵すべてをあずかり、それを非常に高いセキュリティーレベルで管理するには、コストが膨大になるのは誰でもわかる。

最後に、そのような集中管理する鍵管理センターから復号鍵の情報が流出すれば国家規模でコンピュータシステムの安全性が一夜にして崩壊してしまうだろう。

そもそもはFBIの横車

このような無謀なアイデアは、司法省、特にFBIが後押ししていると言われている。FBIは表では犯罪捜査のための盗聴をしているが、裏ではFBI初代フーバー長官の時代から政治家や有力者のスキャンダルを盗聴で握っている、けっこう危ない組織なのである。国内ではNSA（National Security Agency、国家安全保障局）や国内での諜報活動を禁じられているCIAなどと常に勢力争いをしている。

映画「エネミー・オブ・アメリカ」ですっかり有名になったNSAは地球規模の盗聴だけではなく、米国の軍と政府関係のコンピュータセキュリティーを担当している。一般のパソコンにもキーエスクローが組み込まれるということは、当然、政府関係で使っているパソコンやいろいろなシステムに入ってくることを意味する。キーエスクローが高いリスクを持つことは先に説明したとおりである。このような危険なメカニズムはNSAの立場からは厄介なものなのだ。このことは1993年前後にすでにNSAが政府に上申しているという話が裏では知られている。表側ではNRC（National Research Council、国家研究会議）がキーエスクローは危険性があることを1996年にすでに警告している。

NSAのもう1つの顔 INFOSEC
Jump www.nsa.gov:8080/isso/

1996年にNRCが警告している
Jump www.epic.org/crypto/key_escrow/key_recovery.html

ポリシーロンダリング

90年代の初めからキーエクスローの政治勢力は優勢には見えない。なにせ有力なIT企業の多くはそっぽ向いていたからだ。RSA、

サン・マイクロシステムズ、マイクロソフトなど有力なインターネット関連企業は、常にキーエスクローに反対の立場である。

これに対抗するように、政府の旗振りで政府と深いかかわりのある企業や米国を大きな市場にしたい日系企業を集めてキーリカバリーアライアンスという企業連合を作っていた。しかし、のちにPGPを吸収したネットワークアソシエイツは脱退している。

なかなかうまくいかないので、米国政府内の推進派勢力は海外に打って出た。まず海外でキーエスクローを成立させ、それを米国内に逆輸入させるという、マネーロンダリングならぬポリシーロンダリングをやろうとしたのだ。

この幕開けが1995年のパリでのOECDで米国がブチあげたキーエスクロー構想である。筆者は、いろいろな筋から1995年パリのOECDの状況の話を聞いたのだが、まずカナダは即座に拒否し、ヨーロッパ諸国はその場では拒否しなかったが、賛成もせず、今後の検討課題と茶を濁しているという具合で、かなり米国との間に温度差があったと言う。もちろん、その後、ECははっきりとキーエスクローを拒否することになる。また1997年のOECDで決まった暗号利用ガイドラインでは、キーエスクローを強制できないような釘を刺した内容になっている。

残念ながら、日本にはこの状況が正しく伝わっていないようで、米国政府推進派のプロパガンダを持ち帰ってきた「キーエスクローが世界の趨勢」という言葉だけが日本国内に伝わったようだ。

超有力IT企業が名を並べる
反キーエスクローのリスト
Jump www.computerprivacy.org/who/

ネットワークアソシエイツが脱退
Jump www.zdnet.com/pcweek/news/1208/08ekey.html

ECが1997年にキーエスクローを拒否している
Jump www.ispo.cec.be/eif/policy/97503toc.html

1997年のOECDで決まった暗号利用ガイドラインではキーエスクローを強制できない
Jump www.oecd.org/news_and_events/release/nw97-24a.htm

1995年にOECDから米国のプロパガンダを持ち帰ったことがわかる
Jump www.vacia.is.tohoku.ac.jp/~s-yamane/articles/crypto/policy.html

FBIは自分の首は締めない

1998年からFBIはNIPC（Nation Infrastructures Protection Center、国家インフラ防衛センター）を担当することになった。それまでFBIは情報の防御をするようなことは一切していなかった。だから無責任にキーエスクローを叫んでいられたのだ。もし本当にキーエスクローなどが実施されれば、暗号を使ったセキュリティーシステムを導入しようとすると、手続きは繁雑だし、費用はかかるし、セキュリティーリスクは増えるしロクなことはない。FBIは、これ以上キーエスクローを叫ぶと、結果として自分で自分の首を締める羽目になる。もちろんFBIの対抗政治勢力がNIPCをFBIに押し付けたのは想像に難くない。いずれにしろ、これ以上、FBIはキーエスクローをプッシュできないだろう。

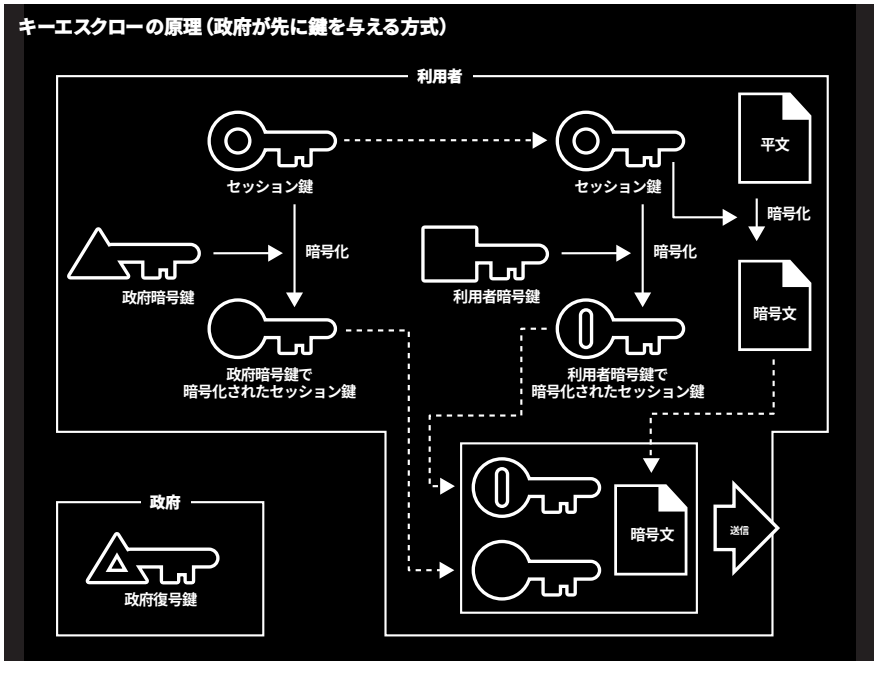
NIPCにある"Threat Information"のページは目を覆うほどおそまつ
Jump www.fbi.gov/nipc/

日本での提言は米国のコピー

日本の動きを説明しよう。一番最初のキーリカバリーの提言は、財団法人社会安全研究財団という警察の外郭団体が設置した情報セキュリティー調査委員会の報告書（1997）にある。郵政省の審議会でも「ネットワーク認証業務の在り方に関する報告書」（1997）で言及している。キーエスクローに関しては、米国の一部政治勢力の発信するプロパガンダをそのまま再発信している。なんとも背筋がぞっとする内容になっている。

どうして、警察も郵政省も同じようなことをするのかと疑問に思う人もいるだろう。理由は簡単である。両方とも同じようなメンバーで取り仕切っているからなのだ。同じ人たちが同じことを言っていれば世話はない。精力的な活動には頭の下がる思いだが、技術も政治も知らない学者が勘違いすると怖いものがある。

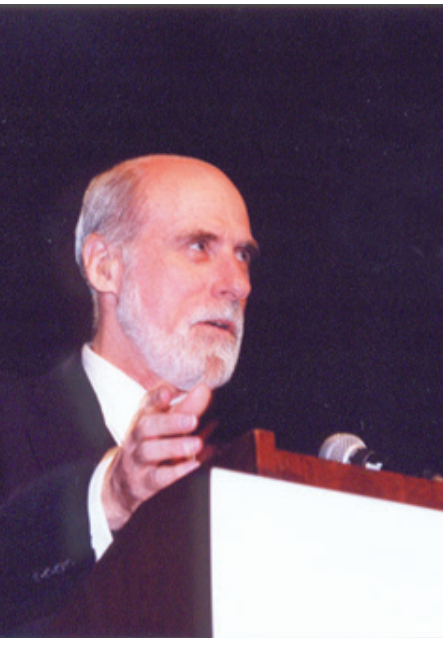
日本国内で「キーエスクローは世界の趨勢」などと散々なことを発言していた人たちは、いま、どうなっているかは筆者は知らないし、知る気もない。ただ1つ私が読者に言えることは、もし、今後キーエスクローの亡霊が出てきたら、「はっきりNOと言おう」である。世界の笑い者にならないように。



海外における政治とのかかわり

インターネット・ポリティクス・プライバシー

Takama Gohsuke
高間剛典



政治的に無視できなくなる

インターネットの父と呼ばれる1人、ビント・サーフは、最近のあるスピーチの中で2006年にはインターネットユーザーの数が9億人に達するという予想を提出している。また、2003年にはエレクトロニックコマースが経済活動全体の10パーセントにあたる3,200億ドルに膨らむとも予想している。実際、インターネットユーザーの数は1999年5月に1億6500万人に達した。

インターネットがここまで拡大すると、政治の側からも無視できない存在になる。各国で発生しているインターネットの規制にかかわる法律提案の動きはそれを証明しているだろう。しかしまた、政府にとってもインターネットの利用は数々のメリットをもたらすことを、現在は政府自身が理解し始めた時期と言えるのではないだろうか。

「監視」「規制」されるinternet

ビント・サーフのこのスピーチが行われたのは、6月末にワシントンDCで開催された「e-gov」というコンファレンス会場でのことだった。そこでは政府のネットワーク化を推し進める流れが起きていることが明らかに見て取れた。ただ、その大部分はいままでの手続きの電子化といった方向であり、それ自身から新しいテクノロジーが生み出されるかどうかはまだわからない。インターネットを民主主義のツールとして使う試みはまだ将来の課題になっている。

e-gov
Jump www.e-gov.com

テクノロジーの理解が遅い政府

インターネットに接続するということは、個人、政府、大企業が全部同じネットワークでつながることを意味するようになってきている。そこで起こることはいままでに前例のなかったものだ。

しかし、一般的に政府の動きはのろく、新しいテクノロジーに対する理解も遅い。米国の「通信品位法」（CDA）についての経緯を見てもわかるように、政府のインターネットに対する最初のリアクションは「新たな（マス）メディアが登場した」といったものだった。そしてマスメディアに対して有効だったように、単純に規制する法律が提案された。だがインターネットはいくつかの出版社や放送局がコントロールするメディアではない。そしてすべての法律を記憶しているのは国民の何割だろうか？

CDAの違憲性が最高裁判所ではっきりし、差し止められたあとでも、「児童オンライン保護法」（COPA）が登場するなど慣性が付いてしまっている。そして規制はポルノだけでなく、「不適切」というタグの下にいくらでも拡大されうる。

法律だけがベストではない

数か月前に英国の諜報機関MI6のスパイの名前と住所の情報が、あるウェブサイトに置かれた。この事件はマスメディアにとって格好の話題になり一気に広まったが、このように一個人によって掲載された情報が一国の諜報機関のオペレーションを翻弄することは、いままでは起こりにくかったであろう。以前は、政府機関はマスメディアのみへの対応を考えておけばよかった。しかし、インターネットの拡大はそれをバイパスしてしまう。単純なインターネット情報の規制論が登場するのは、そういった危機感の表れではないだろうか。

しかし問題はそれほど簡単ではない。テクノロジーに関する問題では法律を作ることがベストソリューションとは限らない。また、その逆もありうる。

政府によるコンテンツ検閲に対して出てきた、フィルタリングソフトウェアの使用という方法には、ソフトウェアがブロックするサイトのリストが企業秘密として開示されていないという問題があった。だがフィルタリングソフトウェアの品質保証についての法律はできただろうか？

サーベイランスが進んでいる

インターネットはサーベイランス（個人や集団の行動監視）の実行にも格好のツールになる。このとき個人はどのようにして

個人情報の一方的な収集に対抗できるのだろうか？　そしてサーベイランスの主体は政府だけでなく、大企業ということもある。

政府が国民の動きをモニターする傾向はいまに始まったことではない。しかし、世界規模のサーベイランスネットワークの構築は見逃せない動きだ。昨年、米国の国家安全保証局（NSA）と英国の組織が構築していた「Echelon」と呼ばれるサーベイランスネットワークの存在が暴露され、EU諸国は米国に対して明らかな不快感を示した。しかしヨーロッパでも1991年から始まった「Enfopol」（インフォメーションポリスの意）と呼ばれるサーベイランスネットワーク構築の流れがある。Echelonはオーストラリアとニュージーランドにもサイトがあり、衛星通信をターゲットにしていたようだが、EnfopolはインターネットとGSM携帯電話などやイタリアにコントロールセンターのあるイリジウム（衛星携帯電話）も含む、デジタル通信の音声とデータ全部をカバーしようとしていると言われている。

米国の「通信傍受法」事情

米国では、1994年に「法執行機関のための通信援助法」（CALEA）が成立している。別名「デジタルテレフォニー法」と呼ばれるCALEAはアメリカの通信傍受法であり、電話会社など通信事業者と通信機器製造会社に、警察やFBIなどの法執行機関が盗聴を実施するのを支援するための装置を組み込むことを義務付けるものだ。しかし、具体的にどのような規模の盗聴能力を持ったどのような装置を用意し、予算の出所をどうするかについて、FBIと電話会社、通信機器製造会社との間で話が噛み合わないまま、法律で設定された当初の予定の1998年10月までに決まらずに2年間延長された。なぜなら、たとえばすべての携帯電話に位置情報を警察に提供できる機能を組み込むなど、FBIは法律で認可される盗聴の限度を越えたサーベイランスシステムに近いものを求めているからだ。

通話ごとの盗聴により通信内容を調べるのは、犯罪者の追跡としては実際は非効率的だと言える。そのために法執行機関はサーベイランスネットワーク構築に向かっていると考えられる。しかしそれらが秘密裏に行われるなら、政府は人々の信頼を完全に失うだろう。

プライバシー保護が必要

マーケティングは企業によるある種のサーベイランスと言えるだろう。企業ウェブサイトにとっては、ブラウザーのクッキーによるサイト訪問者のトラッキングなどは通常機能の1つになっている。しかし多数のサイトの違った情報が統合されることにより、インターネット上の個人の行動は、企業に対してかなり剥き出しなものになってしまうのだ。

たとえば、個人の銀行利用や税金、医療、運転免許などの情報は保険会社にとってたいへん有用だ。昨年米国では運転免許証の顔写真を各州の車両登録局から買い集めてデータベース化しようとしていたImageDataという会社があったが、いくつもの州から却下されて頓挫した。

このような企業の行動に対しての個人のプライバシー保護は、政治が処理しなければならないフィールドのはずだ。プライバシー保護の法律に関してはEU諸国で先に確立されてきているため、ヨーロッパから見ると米国は無法地帯に見える。

ImageData
Jump www.imagedata.com

強度の暗号が必要になる

これらの個人データが犯罪者に流れたときのことを予想すると、その被害の拡大は計り知れない。経済活動の10パーセント以上がインターネットで行われるようになるなら、犯罪者もインターネットにテリトリーを移行していくのは自然な流れだと考えられる。

データの保護がないまま、たとえば個人ID、税金、資金運用、医療情報などがインターネット上を流れるなら、犯罪者は世界中どこからでもデータを狙える。そしてB to Bコマースといわれるように、金額の大きい企業間の取引がインターネットに移行していることは、犯罪者にインターネットをますます魅力的に見せるだろう。

そして、たとえばロシアのマフィアが給料の安い研究所から科学者を大量に引き込み、NSA並みの暗号解読能力とサーベイランス能力とを構築していないと言い切れるだろうか？　もし大企業間の取引で被害が出れば、そのインパクトは社会的なものにもなりうる。そのとき安全なエレクトロニックコマースの確立のためには、簡単に解読できない強度の暗号を使う必要性は、法執行機関のために暗号を解読できるように弱くしておく必要性を上回るだろう。128ビット強度は最低必要だと考えられる。

多数のヨーロッパ諸国では暗号製品の開発・販売・輸出に規制はなく、その中でももっとも勢力的に暗号規制政策をとっていたフランスでも、今年3月にそれまでの政策を変更し、128ビットまでの暗号製品を販売できるようにしている。

法律は罰則を規定して「鞭」が存在することを見せるのであり、それだけでは必ずしも犯罪を未然に防ぐことはできない。法律を作ることだけがベストソリューションとは限らない。インターネットでの犯罪解決にはテクノロジーの裏付けが必要だ。

進歩を遅らせる規制は必要ない

現在、ISOCでは「Internet Societal Task Force」（ISTF）を組織してさまざまな政治的、社会的な問題に対応しようとしている。政治は黙っていてもやってくる問題だ。そしてインターネットと政治の関係は、テクノロジーに携わる人々の発言こそが重要になる問題ではないだろうか。

ビント・サーフは「政府は法律を作る必要はあるが、進歩を遅らせる規制を作り出すべきではない」と語ってこの日のスピーチを締めくくった。

ISTF
Jump www.istf.isoc.org

ビント・サーフの**e-gov**でのプレゼンテーション
Jump www.wcom.com/about_the_company/cerfs_up/29jun99/egov.ppt

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp