情報とセキュリティ

●盗聴と通信傍受

通信傍受法(日本)

マスコミ報道・反対運動――「盗聴法」

■通信傍受法、8 月 15 日施行へ

政府は 14 日の閣議で、電子メールや携帯電話の盗聴捜査を初めて合法化する通信傍受法(盗聴法)を 8 月 15 日施行することを定めた政令を決定する。盗聴法は昨年 8 月 12 日に、参院本会議で盗聴法を含む組織犯罪対策 3 法案の採決が行われ、自自公 3 党などの賛成多数(賛成 142 、反対 99)で可決、成立した。

盗聴法をめぐっては、憲法で保障された「通信の秘密」などに抵触する恐れがあることから反対の声も多く、同法案成立後も市民グループなどによる反対運動は続いている。(Mainichi Interactive: 2000 年 7 月 13 日)

通信傍受法(犯罪捜査のための通信傍受に関する法律、平成 11 年 8 月 18 日法律第 137 号)

第 1 条(目的) この法律は、組織的な犯罪が平穏かつ健全な社会生活を著しく害していることにかんがみ、数人の共謀によって実行される組織的な殺人、薬物及び銃器の不正取引に係る犯罪等の重大犯罪において、犯人間の相互連絡等に用いられる電話その他の電気通信の傍受を行わなければ事案の真相を解明することが著しく困難な場合が増加する状況にあることを踏まえ、これに適切に対処するため必要な刑事訴訟法(昭和 23 年法律第 131 号)に規定する電気通信の傍受を行う強制の処分に関し、通信の秘密を不当に侵害することなく事案の真相の的確な解明に資するよう、その要件、手続その他必要な事項を定めることを目的とする。

第 2 条(定義)

(1) この法律において「通信」とは、電話その他の電気通信であって、その伝送路の全部若しくは一部が有線(有線以外の方式で電波その他の電磁波を送り、又は受けるための電気的設備に附属する有線を除く。)であるもの又はその伝送路に交換設備があるものをいう。

(2) この法律において「傍受」とは、現に行われている他人間の通信について、その内容を知るため、当該通信の当事者のいずれの同意も得ないで、これを受けることをいう。

FBI・NSAの「盗聴」関連疑惑(アメリカ)

カーニボア

米連邦捜査局(FBI)は米下院公聴会で、インターネットを流れる情報の犯罪捜査目的の「盗聴」を今年に入ってから 16 件実施したことを明らかにした。「カーニボア」と呼ぶ特別のソフトウエアを使い、標的とする人物や組織のメールの伝達経路、内容を把握したという。「カーニボア」は FBI が開発したソフトで、接続業者(プロバイダー)の通 信システムに組み込み、ネットを行き交う膨大な情報から特定の内容やあて先のものを取り出せる。 2 年前に完成、これまでに計 25 件の捜査に使った。こうしたソフトを多用すると無関係な一般のネットユーザーのプライバシーも侵害され兼ねないとの声も出ている。(2000 年 7 月 27 日報道)

エシュロン(Echelon)

欧州委員会は 10 月、『エシュロン(Echelon)』の活動についての完全な報告を命じる予定だ。エシュロンとは、米国最大の秘密情報組織『国家安全保障局(NSA)』が運営の一翼を担う、国際的な秘密情報収集網だ。

「率直に言って、エシュロンの存在を少しでも疑うのは米国人だけだ」と述べるのは、欧州議会の英国メンバーで、同議会の技術諮問委員会『科学技術選択肢評価(Scientific and Technical Options Assessment: STOA)』の責任者、グリン・フォード氏。

エシュロンは、世界中に送信された全ての電子的通信(電話、データ、携帯電話、ファクス、電子メール、テレックス)の傍受や記録、翻訳ができるとされている。欧州議会の報告書は、このシステムが拡張され、欧州の企業や議員の秘密に照準を合わせているのではないかという懸念に焦点を当てることになる。(1998 年 9 月 30 日、HotWired)

問題――我々の通信はすでに安全ではあり得ないのか。

対処策としての「暗号」…… PGP (pretty good privacy)、SSL など

セキュリティに関する別の考え方

●通信は安全か？

受信者による意図的なリークの例……エムス電報事件(The Ems Telegram: 1870)

> 彼[フランス外相グラモン]はナポレオン三世の同意のもとに、フランス大使ベネデッティに打電して、プロイセン王が「(スペイン)王位継承問題をむしかえさない、という確約を与えるよう」要求すべしと指示した。(……)7 月 13 日朝、ベネデッティはプロイセン王をエムスの温泉地におとずれ、確約を迫った。だがプロイセン王は拒否し、ベネデッティの非礼な態度に立腹し、午後の会見予定をも取消た。そしてその経過がベルリンに電報で伝えられた。(……)彼[ビスマルク]は鉛筆をもって電文を短縮して、異なる印象をあたえるものに変えた。(……)そして新聞に公表された。(望田 158-9)

変更前の電文(王に同行していた外務省官吏のもの)

> [大臣の一人の助言に基づき王は、]上記の要求に接してベネデッティ伯爵を再び引見しないこと、しかしベネデッティがすでにパリから受けた知らせについては陛下もすでに[レオポルトから]その確認を受け取っており、これ以上大使に対して言うべきことはない旨を副官に伝えさせることを決定された。陛下は[ビスマルク]閣下に対し、ベネデッティの新たな要求とそれを拒絶した旨を我々の大使たちと新聞の双方に伝達することあり得べしと示唆された。

変更後の電文

> 陛下はそれに対し再び大使を引見することを拒否し、その後、大使に対してこれ以上伝達することはない旨、副官をして伝えしめた。

確率の問題……「論理的な危険」と「現実的な危険」

「セキュリティレベルを高めるためには一定の資源が必要となる」

→ 従って内容の重要性より高い投資をすることは経済的に合理的ではない(経費の限界)。

逆向きの適用

「合理的な主体であれば、推測される通信内容の重要性を超える投資を行なってまで内容を解読しようとはしない」→現在主流の暗号方式。

> RSA 暗号の総当たりによる解読実験。1977 年、Martin Gardner の出題(RSA-129: 鍵は 129 桁)。1993 年、Arjen Lenstra(Bellcore)・Derek Atikins(MIT)が実験を組織。24 ヶ国から 600 人を超える参加者を組織し、合計 1600 台のワークステーション等々で 8 ヶ月間かかって解読に成功(1994 年 4 月 26 日公表)。

> そもそも、セキュリティや安全、そしてプライバシーの問題が、デジタル・コミュニケーションのなかでどのようにとらえられるべきかということは、次の三つのレベルで考えていく必要があると思います。
> 一つめは、技術の問題。二つめは、それを運用して使っていく仕組みの問題。そして三つめは、それを使う人間達の振舞いの問題。この三つのレベルを正しく分けて考える必要があるのです。(村井 182)
> インターネットの仕組みにおいては、見ようと思えば必ず、「乗換駅」で中身を見ることができるようになっています。(……)ですから中身を秘密にしたかったら、両端でする。そのための手段は暗号化しかなく、こうした事情でインターネットでは、暗号化技術がセキュリティの中心になっているのです。(村井 186)

※ 暗号に関する具体的な説明は別プリント参照。

●暗号に対する国家規制

私人による暗号通信については国家によって幾度も規制の試みがなされている。

調査権統制法(イギリス)

2000 年 7 月、企業・組織・個人間の電子メイルを傍受して解読する権限を当局に与える法案。暗号鍵を引き渡さない場合、暗号データを解読させない場合にも懲役刑の罰則。世論の批判、欧州人権裁判所からの人権侵害の可能性指摘などのために施行延期。

RSA 発表時の介入

特許申請に対し NSA による Invention Secrecy Order(発明秘密保持命令)→国家科学基金に提訴することで撤回。論文発表にも武器規制法違反の嫌疑。

輸出規制

アメリカでは暗号を武器と看做し、国際武器流通規定(ITAR: International Traffic in Arms Regulation)で規制されてきた。国務省武器流通管理事務所→ NSA から許可が出ない限り、輸出不可。多くのヨーロッパ諸国でも同様の規制が敷かれてきたが、1990 年代前半に相次いで撤廃。

クリッパーチップ

1993 年に発表された NSA の暗号規格。アルゴリズムとしてはスキップジャック(非公開)を使用。安価な暗号化/復号化チップで、通信機器に内蔵する。チップには固有のシリアルナンバーとマスター鍵が内蔵されており、ユーザはそれらを見ることができない。各鍵は国家標準技術研究所(NIST)と財務省自動システム部に寄託される。法執行機関は裁判所の許可を得て鍵を引き出し、解読に利用することができる。輸出も許可される前提。

鍵供託システム KES Key Escrowed System

アメリカ・クリントン政権が 1993 年 4 月に提唱。暗号化の鍵をいくつかに分割し、別々の機関に供託する。裁判所の許可があれば、捜査機関はそれらを引き出して暗号文を解読することができる。

<u>問題…… social security と個人の security の相克</u>

なぜ国家は「盗聴」などをするのか?

犯罪者集団(特に麻薬犯罪)・テロ集団の通信

問題点

犯罪に関する通信かどうかは内容を見ないとわからない。

見たときにはすでにプライバシーは侵害されている。

暗号化は本当に犯罪捜査の敵か?

暗号化を禁止するような法律を作ったとして、職業的犯罪者(暴力団とか、大がかりな密輸業者とか)がその規制に従うと考えられるだろうか。

おそらく正しいだろうこと……暗号化規制は、ハードコアな犯罪者(確信犯、暴力団や麻薬犯罪者)の摘発には(少なくとも直接的には)役立たない。犯罪フォロワー層(ちんぴらなど低強度の犯罪者)の捜査には役立つ可能性がある。周辺捜査から本丸へというのは確かに一つの手法だから可能性がないではないが、あまり期待はもてそうにない。

「総論賛成、各論反対」

国家のいくつかの試み……暗号規制、バックドア

個人による対抗……暗号の利用

●可能な選択肢？

ネットワークからの退却

> 『エシュロン』のハッキングから逃れるためには、どうしたらいいか。／電子通信では、暗号化が進められている。暗号を使っても、ハッキングから完全には逃れることはできないが、解読されるまでの時間を稼ぐことができる。／同時に、従来の手紙も見直されているという。デジタル技術のハッキングを防ぐには、アナログ通信しかないのだ。(河崎 195)
>
> インターネット経由で、家庭や企業内の電化製品や制御機器を制御できるようになった時、テロリストやハッカーが、インターネット経由でガス、電気、水道などのライフ・ラインを操作して、殺人さえ起こすことも可能になるだろう。(河崎 210-1)
>
> 究極のセキュリティのためにはオフラインしかない(河崎)

国家管理の強化

ニフティ事件原告主張

インターネットに免許制を

> その犯罪を防ごうとすれば、インターネットの「自由」を考え直すべきではないだろうか。自由と民主主義を守るためには、国民の一定のルールが必要なように、インターネットもルールを設ける時期にきているのではないかと思う。／インターネットの利用者には、自動車を運転する時と同様に、『インターネット免許』の制度を提案したい。(河崎 215)
>
> 特定の管理者のいないインターネット上の秩序を守るためには、現段階ではとりあえず国家単位で法律を制定して、犯罪や不正行為を取り締まるしか方法はないのであり、新規立法が、即、権力の乱用に繋がると考えるのは早計である。もちろん、権力の乱用は許してはならないが、立法技術上の配慮により、かなりの問題は回避できると考えられる。(藤原 20)
>
> 会員に対し議論のレベルでの対応ができない不当な人身攻撃にも自らの危険において対処を期待することは、広く開かれたネットワークではなく、名誉やプライバシー侵害にも立ち向かう覚悟を持った気丈な対応能力のある一部の限られた者のネットワークへと変容していかざるをえないであろう。(高木 196)

可能な処方箋

復号できない暗号は存在しない(少なくともコミュニケーションを目的とする暗号においては)。絶対に安全な通信など、それが通信である限り存在し得ない。我々にできることはただ、危険を知りつつそれを manage することのみである。

ネットワークは単なる通信経路であり、起点・終点で必ず現実世界に接続されなくてはならない。現実世界のあり方を離れた「ネットワーク」論などあり得ない。→ ネットビジネスなどを考える場合にも重要な問題。

国家による安全(Security by States)と国家からの安全(Security from States)の相剋可能性。国家による安全を求めるとき、我々は国家を信頼して警戒を放棄するよう迫られる。しかし国家は果たして(1)信頼に足る存在なのか？(2)我々の信頼に応え得る存在なのか？

BIBLIOGRAPHY

望田幸男『ドイツ統一戦争: ビスマルクとモルトケ』教育社歴史新書（教育社 1979）

村井純『インターネット』岩波新書（岩波書店 1995）

河崎貴一『インターネット犯罪』文春新書（文藝春秋 2001）

高木篤夫「名誉毀損とプライバシー侵害をどう防ぐか」藤原宏高(編)『サイバースペースと法規制: ネットワークはどこまで自由か』第 3 章（日本経済新聞社 1997）

藤原宏高「サイバースペースの法整備を急げ」藤原宏高(編)『サイバースペースと法規制: ネットワークはどこまで自由か』序章（日本経済新聞社 1997）

一松信『暗号の数理: 作り方と解読の原理』講談社ブルーバックス（講談社 1980）

サイモン・シン『暗号解読: ロゼッタストーンから量子暗号まで』青木薫(訳)（新潮社 2001）