

Philip Zimmermann 氏講演 前半部サマリ

日本の暗号政策は、OECDの鍵寄託に影響を受けていると聞いた。2年前、パリのOECDでのことである。アメリカ政府が「国家は暗号鍵にアクセスできる」という自国の暗号政策案をそのままOECDへ提案事項として持ち込んだ。しかし、OECDに参加している各種の人権擁護団体は、国家が鍵にアクセスできることは問題であると主張した。世界のいくつもの人権擁護団体はPGPを使っている。人権擁護団体のドキュメントはPGPを使って暗号化している。

なぜ私がPGPを作ろうとしたか。答えはそこにある。人権擁護団体を保護するためのプロジェクトとしてPGPをスタートさせたのだ。各地の人権擁護団体はアメリカも含めて、政府からの不法な弾圧を受けている。アメリカの警察や司法組織では、たとえばFBIでは、むかしから電話や会話の盗聴を捜査手法として使っている。それに立ち向かうのがPGPである。

暗号は人権擁護のために使われる。それは政府と国民との関係において力関係を正常に保つためである。もし政府が何かに疑義をもち無制限の情報へのアクセスができるなら、それは非常に危険なことである。アメリカでは盗聴は合法であり、政府は捜査手法として用いているが、技術の向上と共にこれがそのまま進めば、すべての国民を監視することが可能になる。現在の技術開発のペースでいけば全国民の使用する電話での会話、電子メール、そのたの情報をすべてチェックすることが現実に行えるようになる。

言論の自由やプライバシーの保護といったことは民主主義を貫く上で重要な要素である。暗号技術は、その言論の自由やプライバシーを守る。ジョージオウエルの1984は、そのような言論の自由やプライバシーが国家により剥奪されたファシズムの世界を描いている。

現在、あちらこちらに監視カメラがついている。そこに画像識別のシステムが加われば、すべての人がどこで何をしているかを常に監視し、記録することができる。これは現在におけるコンピュータの性能向上のスピードを勘案すれば、そんなに先のことではない。自動車もセンサーがついていて、誰がどこに移動しているのかもわかるようになるだろう。電話も音声認識の向上により誰がどんな内容を話しているかわかるようになるだろう。町中のあちらこちらにある監視カメラと人相識別により、ビルの入退館、電車の乗り降り、あるいは町中のどこを歩いてもわかるようになるだろう。

このような人々を監視するようなシステムは、インドネシア、マレーシアといった民主主義を弾圧している国家に取っては非常に便利なシステムである。これらのシステムは非民主主義的国家の国民だけ適用されるのではなくアメリカのクリントン大統領のような政治リーダーに対しても適用されるだろう。なぜならセックススキャンダルをつかみ相手の失脚を狙うものにとっても有効なシステムであるからだ。このようにアメリカでは政争の道具としてシステムは使われることになるだろう。

かくして政府が全知全能の神になるパワーの根源としてこれらのシステムは使われる。政府はそれを理解しているが多くの国民はそれに気づいていない。ここまでの話は、あくまでも可能性であり、現在はまだそのような状態にはなっていない。しかし、みんなはカエルのお話を知っているだろうか。熱いお湯にカエルを入れれば、熱さに慌てて飛び出す。しかし、ただの水にカエルを入れて徐々に熱していくと、カエルはその熱さを感じないので逃げ出さず、最後は茹だって死んでしまう。そうなるから遅い。

技術の乱用は我々のプライバシーをあばき、我々の将来の民主主義を脅かす。PGPは、それに対抗するための技術なのである。

この文章は以下のRLで参照できます。

<http://www.pp.ijj4u.or.jp/~h2np/pgp/OsakaSummary.html>

文責
すずきひろのぶ
hironobu@h2np.suginami.tokyo.jp