プライバシーとセキュリテイ

曽我 正和
岩手県立大学 ソフトウエア情報学部

概要

インターネット上でのセキュリテイの問題には、クラッカー起因のものやウイルス起因のものがあるが、ここでは匿名性に起因すると思われるものについて、私見を述べる。
匿名性はプライバシーの観点からやむを得ないこととなっているが、そのことが他者のプライバシーを著しく傷つける行為や犯罪行為の隠れ蓑として悪用されている事例も多い。
匿名性に何らかの制約を課すべきではないか、との立場から考えてみた。

Privacy & Security

Masakazu Soga
Iwate Prefectural University

Anonymity on Internet is generally considered as a guard-wall for the user's privacy. But, actualy, the anonymity often aid to cause infrngement to another user's privacy. Some restriction on the anonymity may give better balance of total security on Internet.

1、インターネット上での匿名問題

最近インテルは新しいペンテイアムチップに1個づつユニークなシリアルナンバー(Processor Serial Nnmber, PSN)を付加することをアナウンスした。ところが直ちに米国内のプライバシー擁護グループから反撃を受け、インテルチップ不買運動が巻き起こる様相となった。そこでインテルは直ぐに譲歩のアナウンスを出し、出荷時点でのデフォルトではPSNを隠蔽することとした。（ユーザの指定によって隠蔽を除去可能）
インテルによると、PSNは電子商取引やその他のセキュリテイの向上に寄与する、とのことである。
他方プライバシーグループの主張によると、かかるPSNは当のユーザが気づかぬうちにショッピングソフトによって読み取られ、各ユーザの行動がトレースされ、ユーザプロファイルとしてデータベース化されるであろう、とのことである。
このようなプライバシー保護運動がある一方で、インターネットの匿名性を悪用した犯罪行為や他者のプライバシーを侵害する行為は、日本でも頻々として発生していることもまた事実である。それらに対する有効な技術的対策は見つかってはいない。法制サイドからの見直しは今検討中である。4月21日の日経新聞によると「米国政府がEUの個人情報保護基準に同意した」とのことで、我が国でもこれに追随することが予想される。法律によって基準が明確化されるべきことは必須であり、それは一定の抑止力と

して働くことは当然期待される。しかし技術的な面からも抑止効果を高める何らかの対策を検討すべきと考える。

2、どこが問題なのか

かかる現状に対して、インターネットを悪者扱いする見方がある。

他方でインターネットは単に便利な手段を提供しているだけのものであり、それを悪用するのは悪用する人間の問題である、と割り切る見方もある。類似する問題は例えば自動車にも存在する。自動車は非常に便利な移動手段を人間に提供して呉れているが、場合によっては犯罪の手段に使われることもある。だからと言って自動車自体を悪者扱いする見方は極めて少数派であろう。

しかしインターネットと自動車との比較はあまりに乱暴かもしれない。自動車は一世紀に近い歴史をもち、社会にかなり定着している。それに対してインターネットはようやく社会にデビューしたばかりで、技術面、制度面、使用モラル面、等々で発展途上である。

例えば自動車にはナンバー登録制度、運転免許制度、車検制度、等が確立している。

これら諸制度に対して費用負担の面で不満をもつ人は多いが、プライバシー保護の面から異を唱える人はまず居ない。もし「ナンバープレートは自由に取りはずしてよろしい」と言う改正案が出てくれば危険性の増加を心配し圧倒的多数で否決されるであろう。

ところが、インターネットの世界では事情は逆である。「インターネット端末にIDナンバーを取り付けよう」とのインテルの試みは袋叩きにあっている。

これは袋叩きにまわる側にも主張があり、そこにインターネットが持っている特殊性がある。それは何か？それはインターネット環境が持っている底知れないデータ処理能力である。もし端末にIDナンバーがついておれば、その端末の挙動は容易に精緻に細大漏らさず世界中に知られてしまう、と言うことである。

その結果がどのように使われるか、もまた予測不可能な気味悪さがある。

3、このままで良いか

しからば、このまま匿名性を堅持していくのがベストの解なのであろうか？

たしかに不特定多数の人々のプライバシーを保護することは必要であるが、それが特定少数の被害者には修復不可能とも思える厳しいプライバシー侵害や、ときには一命にかかわる犯罪を引き起こしていることをどう考えればよいのか？勿論被害者がもっと注意しておれば防げたものも多いが、防御しようのないプライバシー侵害も多い。

4、ひとつの提案

私の提案は、インテルの案とは多少異なるが基本的には匿名性を制限する方向の提案である。以下に提案の概要を示す。これは「かくありたい」という内容であって、それを実現する上で技術的に精密に「こうすれば良い」と煮詰めたものにはまだ至っていない。また

当然これだけで問題のすべてが解決すると楽観できるわけでもない。

(1) １対１の通信、あるいは複数の相手でもそのメンバーが確定している通信、においては従来どおりのやり方を存続させる。知り合っているメンバー間の通信ではそもそも匿名の意義はないが、ショッピングや相談窓口へのブラウジングにおいてはプライバシー保護の観点から従来どおりの匿名性があってよい。ただしショッピングにおいて注文書発行になれば、ソフトのような電送品を除いて、購入品目、住所（配達先）、氏名、決済口座番号と有効期限、までは所詮示さざるを得ない。ただしこれらの注文書情報はショップの公開鍵で自動的に暗号化されて送信され第三者への漏洩を防ぐのが妥当である。

(2) １対不特定多数の通信においては、これは公然性を有する発信なので、発信者には完全な匿名は許さない。ある種の署名を要求する。署名には２つのレベルを選択できる。
１つは明示する署名である。他のものは明示しない署名である。
明示しない署名の場合は、不特定多数への開示メッセージ文には署名が明示されないが、これを受け付けるサーバーにはログとして一定期間署名つきで保管される。
なお、ここで述べている内容は法制度によって強制されないと実現しないであろう。

(3) 署名が偽名であっては意味がないので、ここで言う署名は正しく発信者を特定しうるものでなければならない。逆に言うと、特定できれば良いのだから、氏名でなくそれに代わる別の ID でも差し支えない。ここでインテルの PSN を思い浮かべるが PSN はプライバシーの漏洩の点では弱いので問題がある。
私の提案は署名必要時点で IC カードを利用するもので、IC カードからデジタル署名を発生する、という案である。この場合のデジタル署名は周知のように現実の署名や印鑑と異なり、メッセージ本体ともリンクしているから、同一人の署名でも個別メッセージごとに形が変わる。問題はデジタル署名に使う個人鍵をどのように安全に保管するか、である。これは鍵本来の目的からしてもブラウザやウイルスに読み取られることがあってはならない。それは印鑑を盗まれる、あるいはコピーされることに等しい。
これらの署名に必要な情報を、パソコン本体とは独立した IC カード上のチップ内に保管する訳である。パソコン本体のファイルには入れないこと、および IC カード上のプロセッサーに秘匿機能を持たせることで漏洩防止を完全にする。
また、個人用の鍵のうち秘密鍵については、その所有者自身にすら読み取られない方がよい。（ユーザ本人による偽造すなわち他人へのなりすましを防ぐため）所有者は本来の目的からすれば秘密鍵を裸のデータとして読み出す必要は何もない。署名に使えれば、あるいは復号計算に使えればよいのである。そこで、秘密鍵は誰からも絶対に裸のデータとしては読み出せないように保管する。

(4) 以上の要件を満たす具体的な実現方法は幾つかあると思われるが、１つの案をしめす。
これは技術としての新規性はなく、同様のものが過去に示されている。(1)(2)(3)
・ユーザは本人の鍵（公開鍵と秘密鍵）を IC カード内にプリセットした状態でオフライン的

に保管している。

・公開鍵は事前に別途登録され公開されている。

・デジタル署名が要求されたときにユーザはICカードを端末に接続する。

・ICカードは端末に暗証番号の打ち込みを要求し、正しい番号を確認して後、デジタル署名対象メッセージをICカード内のプロセッサへ取り入れ、署名計算（復号計算）をして結果を端末へ返送する。（新たな署名要求の都度暗証番号を要求する）

・署名結果が出たあとユーザはカードを抜く。

・ICカード内の鍵はICカードの製造時にハードウエア的にプリセットされ、うち秘密鍵は外部へ裸データとして読み出す手段は用意されていない。

・ICカードの配布、公開鍵の登録、管理、等は認証局がおこなう。

5、まとめ

この提案内容の多くは法制度に依存するものである。すなわち、公然性を有する発信には匿名を許さない、との法制度を提案しているとも言える。

この案の運用の主体は、このような公然性を有する発信の場を提供しているサーバーの管理組織体になるだろうし、またその実施状況を監視する制度も必要になろう。その立場からのご意見を是非お聞きしたい。技術的な面は、個人のIDナンバー（個人用鍵コード）を外部から勝手に覗かれない方法の1例を提案した点である。

参考資料

(1) 特開平10-134157「計算機カードを利用した暗号認証処理方法および装置」
NTT,1996,10,28,

(2) 特開平10-143440「デジタル情報保護方法およびその装置」
NTT,1996,11,13

(3) 特開平9-223210「携帯可能情報記憶媒体及びそれを用いた認証方法、認証システム」
大日本印刷、1996,2,19