インタラクティブ・エッセイ

プライバシーとセキュリティ

曽我正和
静岡大学情報学部

インターネット上でのセキュリティの問題には，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，あえて火中の栗を拾うつもりで私見を述べる．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．何かを改めるべきではないだろうか．

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ィアムチップに1個ずつユニークなシリアルナンバ（Processor Serial Number, PSN, http://www.intel.co.jp/jp/PentiumIII/utility.htm）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．そこでインテルはすぐに譲歩のアナウンスを出し，ユーザが容易にPSNを隠蔽してしまえるように新たな機能を追加することとした．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ィの向上に寄与する，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．法律によって罰則が明確化されるべきことは必須であり，それはある程度抑止力として働くことは期待される．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がほしい．

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．類似する問題はたと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くれているが，場合によっては犯罪の手段に使われることもある．だからといって自動車自体を悪者扱いする見方はきわ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1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．たとえば自動車にはナンバ登録制度，運転免許制度，車検制度，などが確立している．

これらに対して費用負担の面で不満を持つ人は多いが，プライバシー保護の面から異を唱える人はまずいない．むしろ「ナンバプレートは自由に取りはずしてよろしい」とい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，ということである．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．

このままでよいか

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？　もちろん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．

1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「こうすればよい」と煮詰めたものにはまだ至っていない．

(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にはログとして一定期間署名付きで保管される．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，ここでいう署名は正しく発信者を特定し得るものでなければならない．逆にいうと，特定できればよいのだから，氏名でなくそれに変わる別の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良い案とはいえない．

私の提案は公開鍵システムを利用するもので，いわゆるディジタル署名を使う，という案である．この場合のディ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，同一人の署名でもケースごとに形が変わる．

問題はディジタル署名に使う個人秘密鍵をどのように保管するかである．これは秘密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，あるいは盗作されることに等しい．私の見解では，これは所有者にすら読み取られてはならない．所有者は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れば目的に近づく．

(4) 以上の要件を満たす具体的な実現方法はいくつかあると思われるが，1つの案を示す．これはどこかですでに試行されている可能性もある．

- ユーザは秘密鍵を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．
- ディ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カードは暗証番号の打ち込みを要求し，正しい番号を確認した後，ディ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（新たな署名要求のつど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カード内の秘密鍵はICカードの製造時にハードウェア的にプリセットされ，これを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，対応する公開鍵の登録，管理，等は認証局が行う．

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いえる．その意味では情報処理学会の場での話題から一寸逸脱しているかもしれないが，当面の大きな問題と思うので意見を述べた．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もぜひお聞きしたい．技術的にバックアップした点は，個人のIDナンバ（秘密鍵コード）を外部から勝手に覗かれぬように工夫した点である．

(1999.2.24)

インターネットの匿名性は強くない，むしろプライバシー侵害の方がおそろしい

工藤育男
(株) ジャストシステム

曽我先生は，インターネット上で起こるセキュリティ問題に匿名性が隠れ蓑として悪用されているので，インターネット上の匿名性を制限するための方策を提案しておられる．重要な問題を提起された点に敬意を表したい．

インターネットの匿名性について

匿名性の持つマイナス面だけでなく，プラス面も評価しておかないとフェアではない．

(1) 投書の場合では意見を集めやすくするために主催者側が匿名性を認めている場合が多い．匿名を認めるか認めないかは主催者側の問題である．また，世論調査や意識調査など統計目的の場合は，匿名の方が望ましい場合や必ずしも実名の必要性がない場合がある．

(2) プライバシー保護の観点から匿名性を望むケースがある．たとえば，匿名での寄付，著名人の発言など．

(3) 内部告発の告発者に匿名性を認めないとすると不利益になる．匿名性を認めない方が社会的にマイナスとなる．

(4) 言論の自由が保障されているからこそ，匿名なしでも意見を述べることが可能なのであって，言論の自由が認められていない状況下にある人達の存在を忘れるべきではない．

現在の社会状況から匿名を利用したマイナス面も多いのも事実である．

(1) 匿名で他人のコンテンツを配信するサイト，もしくは，匿名でのダウンロードを可能にしたサイト．これらは著作権を侵害する可能性がある．これについては，著作権管理団体が違法サイト撲滅作戦を行っている．また，著作権保護の仕組みを考慮した配信システムの考案も行われている．

(2) 匿名メールの転送サービス．このサービスを利用した無責任な投書，もしくは，個人への電子メール攻撃がある．サイトを作った人の意図に反して悪用されるケースが増えてきたので，このようなサイトは閉鎖する方向にある．

インターネットの匿名性が犯罪の隠れ蓑として利用されているというのは本当だろうか？　それならば警察はどうして犯人を逮捕できたのであろうか？　電子メールのアドレスからプロバイダが分かり，プロバイダとの契約から犯人に関する情報を引き出すことができる．したがって，一般に信じられているほどインターネットの匿名性は高くないのである．専門家が「インターネットは匿名性が高い」と一般人に吹聴することこそ誤りなのである．「インターネットでも悪いことをすれば必ず捕まるよ」と教育すべきなのである．携帯電話であれ，インターネットであれ，必ず接点がある．捜査の障害になるのは証拠の保全と刻々と変化する膨大な空間に対する捜査能力の問題である．個人に対する規制を行う前にやるべきことが多く残されているように思われる．

しのびよるプライバシー侵害

ネットサーフィンするだけでも，電子メールアドレス，プロバイダ，ブラウザの種類，OS，リンク元，登録名，興味などが分かる．電子メールアドレスからは所属組織，勤務地や勤務時間が，さらに，名簿業者から年齢，職業，性別，住所，電話番号，学歴や職歴，年収や財産（借金），家族構成や趣味に至る情報まで入手できる．カルテが電子化されることで病歴なども入手できるかもしれない．PHSの情報からは行動パターン（時刻と存在場所）まで特定できる危険性がある．このような方法で個人情報が名寄せされる危険性がある．

欧州では1995年に域内各国に対しプライバシー保護のためのEU指令を出し，ドイツでは身分証明書法の中で個人IDによるデータの統合（名寄せ）を禁止している．

日本国内では，国レベルでは「行政機関の保有する電子計算機処理にかかわる個人情報の保護に関する法律」が成立しているが，地方公共団体，民間部門には及ばない．民間レベルでは業界ごとにガイドラインが設定され，プライバシー保護マークを付与する試みがなされているが，法律的な強制力や罰則は有していないのが実状である[1]．企業の倒産，合併により，個人情報が流出，名寄せされていく危険性がある．このような状況の中で，PSNが発表されたので，米国のプライバシー団体が反発するのは当然であろう．PSNを使えばより効率的かつ効果的に名寄せが可能になるからである．その後，インテルではPSNの使用を選択できるようにしたので，使用後の問題はユーザに任されたことになる．PSNに対する正確なコメントはできないが，大規模なLANの管理や不正アクセスの防止には効果がありそうであるが，個人レベルのユーザにはメリットがなさそうである．

曽我案に対するコメント

ネット上での犯罪捜査を行うためには，ログの管理が必要である．一方で，ログを採るということは，本来匿名にしておきたいデータまで第三者に記録されることを意味する．ログの使用，保管に関する問題とプライバシー保護の問題は裏腹の関係になる．したがって，バランスをとることが重要であるが，前者の議論のみが活発化しているのが気がかりである．

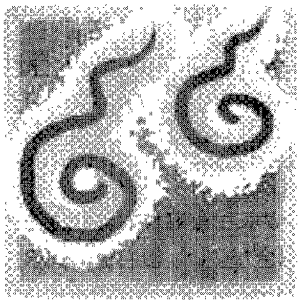
曽我先生のご提案は，既存のネットをできる限り利用しながら，公然性の強い情報発信には法制度的に網を被せ，発信者責任を明らかにする仕組みを導入しようということと思われる．認証局よりIDを発行することにより，本人同定を行うものである．

ディジタルコンテンツの流通に関して認証を行う仕組み（たとえば超流通[2]，OPIMA[3]）に似ている．後者は利用者に対する認証制度であるのに対し，前者は発言者に対する責任を保証するためのものである．

果たして，発言者が同定されてしまうということが，誹謗中傷発言への抑止力となるのであろうか？　また，最初に述べた匿名の長所を奪うことになりはしないか？　現在のシステムでも，匿名メールサーバのような提供がなければ，かなりの問題が防げたのではないだろうか？　また，サイトを運営する側が時間と費用をかけ管理運営していれば，問題が減っていた可能性はないのだろうか？　情報の発信者責任を明確に指摘している点は先生のご意見に賛成であるが，まず，教育面で対処すべきではないか．自分のなした行為がどういう影響を持つのかを推し量れる力を養うことが大事である．インターネットも電話も同じ道具であり，なしたことに対する責任がついてまわることを教えるべきではなかろうか？　最後に，現実の被害を受けている人への救済策としては，ネット上で救済支援団体（NGO）の活躍に期待したい．

参考文献
1) 橋本, 金田: ネットワーク上での情報統合に対するプライバシー保護システムのあり方, 情報処理学会電子化知的財産社会基盤研究会 3-3 (Jan. 30 1999).
2) Mori, R. and Kawahara, M.: Superdistribution: An Electronic Infrastructure for the Economy of the Future, 情報処理学会論文誌, Vol.38, No.7 (July1997).
3) http://drogo.cselt.stet.it/ufv/leonardo/opima/

(1999.3.12)



プライバシーもセキュリティも守ろう

苗村 憲司
慶應義塾大学環境情報学部

プライバシーとセキュリティの関係

プライバシーは「伝統的には，私生活の自由，私事決定の自由または1人に放任される自由を」指していたが，「これに個人情報へのアクセス権をも含めて定義し直す必要が生じ…，自己に関する情報の流れをコントロールする権利」を含むようになった（杉村敏正，天野和夫編「新法学辞典」日本評論社 1991）．一方，情報セキュリティの主目的は秘匿性（confidentiality），一貫性（integrity），可用性（availability）の3つとされる．秘匿性のねらいの1つがプライバシー保護だ．プライバシー保護手段として匿名通信を実現するにもセキュリティ技術が必要となる．だから，プライバシーは，セキュリティに依存する．両者は対立するものではない．

問題は，プライバシーを語って匿名性を悪用し，システムのセキュリティを破壊したり他者の利益を不当に害したりする行為である．インターネットが高度情報通信時代の社会基盤として役立つためには，そのような行為を排除する必要がある．それは，決してプライバシーを否定するものではない．プライバシーを重視するならば，それを支えるセキュリティを損なう「偽のプライバシー」に対しては頑として戦うべきである．

PSNと曽我案の比較

いずれの案も，匿名性の悪用を排除しつつセキュリティを実現するための認証に必要なIDをハードウェアに組み込む点は類似している．上述の条件を満たすかどうか，真剣に検討する価値があろう．両者が異なるのは主に次の2点だろう．

(1) PSNではIDをCPUに埋め込むのに対し，曽我案ではICカードに埋め込む．

(2) 曽我案ではIDを暗号化することにより直接読み取れなくする．

プライバシー保護の立場からすれば，IDが個人に1対1対応するのは避けたい．この意味で，個人が持ち運ぶことを前提とするICカードに埋め込む方式には懸念がある．

一方，ICカードを挿入したときだけIDを有効とする方式は有効性があると思われる．

PSNでも実用化にあたってはユーザがIDをオン・オフする機能をつけることによって同様の目的を実現することになるかもしれない．

また，PSNではメーカの責任においてIDの割当てが行われるのに対し，曽我案では，IDの割当てと管理がメーカから独立になる代わりにそのための組織が必要となる．プライバシー保護のためにいずれが有利か検討の必要があろう．

IDを直接読めなくする機能は，PSNでもセキュリティ上の理由で必要になるかもしれない．

これらの点を含めて両案を検討し，現実的な解決策を探求する必要がある．

プライバシー保護の明確化を

日本の現行制度では公的機関が保有する個人情報の保護については一応の規制があるが，民間機関が保有するものについては野放しの状態にある．EUでは比較的強いプライバシー保護を定めた指令が法として施行されている．インターネットのウェブ上での個人情報の送受については，W3CのP3P（Platform for Privacy Preferences; http://www.w3.org/P3P/）が標準となることが期待される．いずれも，"informed consent" の理念を原則としている．

まず，日本におけるプライバシー保護のあり方に関する議論を行う必要がありそうだ．コンピュータ関連のさまざまな技術用語を和訳せずにカタカナで表記することは許容できるが，個人の人格の保護にかかわる "informed consent" の適切な和訳がないことは，日本人として恥ずかしいことではないだろうか？　そのうえで，インターネットにおいてプライバシーとセキュリティの両立をいかにして実現するかの議論をじっくりと行う必要がある．その両者を保護することは，インターネットが仮想空間でなく実社会で信頼を得るための必須条件である．このことを確認したうえで，現実的な解決策を議論する必要がある．

(1999.3.16)

信頼できるネット社会への道

曽我正和
静岡大学情報学部

お2人の識者から貴重なコメントをいただいた．これらについて私が再度コメントするとともに今後の問題点を挙げてみる．

匿名性のプラス面

工藤氏からご指摘あった匿名性のプラス面については，確かにその通りであり，私が触れていなかった部分である．またインターネットを使う上でのモラル教育の重要性にも異論はない．

これらに関連して重要な疑問を提起されている．すなわち，「果たして，発言者が同定されてしまうということが，誹謗中傷発言への抑止力となるであろうか？　また最初に述べた匿名の長所を奪うことになりはしないか？」これについて私の意見を述べる．

まず抑止力についてであるが，自らを明らかにしてでも誹謗中傷したい発信者には抑止力にはならない．この場合は発信者の言論の自由を尊重すべきなのか名指しされた人のプライバシーを尊重すべきなのか，法律専門家の見解を伺いたいところである．

いずれにしろそういう発信者は非常に少ないと予想する．私は現実的にはそれで抑止効果があると考える．

次に匿名性の長所を奪う問題である．私の先の提案では「公然性を有する発信には匿名は許さない.」との案になっているが，単純にこれだけの条件付けでは工藤氏のご指摘の匿名の長所を認めるべきケースも含まれてしまう（例；世論調査）．この点で，重要なご指摘に感謝したい．そこで問題は，しからば常に匿名を認める路線へ戻るか，ということになる．

私は匿名の長所も認めつつもやはり野放しにすることの害を防ぐべきと考える．逆に匿名の長所を認めるべきケースは指定可能と考える．そこでたとえば，一定のテーマ（テーマ内容に制約を加える必要はない）での公的発言の電子的な場では匿名を許すことが考えられる．

この場合そのサーバ管理者はテーマ外の発言を削除せねばならない．逆に言うと常設のテーマ無制約の発言の場では匿名は許さないこととなる．

次に苗村先生からいただいたコメントを取り上げる．

プライバシーとセキュリティ

「問題は，プライバシーを語って匿名性を悪用し，システムのセキュリティを破壊したり他者の利益を不当に害したりする行為である．インターネットが高度情報通信時代の社会基盤として役立つためには，そのような行為を排除する必要がある.」私の考えもまったくこの通りであり，目指すところは何ら相違ない．

PSNと曽我案との比較の部分でいくつかの視点からコメントをいただいて，両案をさらに検討すべきとされている．ここで私がIDをICカードに埋め込むことを提案した理由を補足する．まず第1は，パソコンから独立したプロセッサとなるので，IDの秘匿性を高め得るからである．第2は使い勝手の面でポータブルにいつも身につけている身分証感覚で使えるからである．第3にIDの発行元をパソコンメーカから独立させ得るからである．IDを発行し管理する組織がいかにあるべきか，については苗村先生ご指摘のように今後の検討課題である．現状では公的機関の介在を避けるべしとの論が多いが，さりとて民間でやろうとすると，何を根拠にIDを発行するか，難しい面もある．

プライバシー保護のあり方

「日本におけるプライバシー保護のあり方に関する議論を行う必要がありそうだ.」まったく同感である．そこで1つ私の希望を述べたい．それは，過去の日本においてプライバシーを論議する視点は常に権力による人権侵害を防ぐ視点からであった．従来の社会ではその心配だけでもよかった．しかしネット社会では，誰もが誰からもプライバシー侵害される危険があり，一度侵害されると修復しようがない大きなダメージを受ける．バランス上この視点も重視していきたい．いずれにしろ目指すところは，「実社会で信頼を得る」ネット社会へ近づくことである．

むすび

有意義なコメントに感謝します．このような議論を今後も続けることが，現実の諸問題と折り合える具体的なコンセンサスの形成の一助になれば幸甚です．

(1999.3.22)

～　議論の続きは，次のURLをご覧ください．http://www.ipsj.or.jp/magazine/interessay.html　～