被害との戦いと戦術に関して

T.F

2008 年 3 月 17 日

目 次

1　はじめに

加害者は、不当な盗聴による個人情報の漏洩を目論み、個人を標的にして付き纏う、卑劣極まりない犯罪を犯しています。しかし、被害者は、戦う術を十分に持たず、個人情報を守る為の一般的な防衛すら行わずに、被害を訴えている為、インターネット上での批判に曝されている現状があります。
この厳しい現状を打破すべく、問題点を洗い出し、解決法を検討していますが、現状では、力及ばずと言った所です。ですが、被害者が、個人的に戦う事のできる原理が、多少なりとも存在している事が分かりましたので、まとめてみました。少々長い文書となりましたが、一読して頂ければ幸いです。

2　電子署名と暗号化に関して

ネット上で使用される電子文書としては、メール、添付資料、ホームページの公開など複数の方法がありますが、何れの方法にしても、筆跡が残らないため、誰が書いた文書なのか、判断ができないという問題が生じていると思います。
匿名の文書にしたいのであれば良い方法だと考えられますが、それにしても、不当な改竄が行われたとしても、一部分の改竄の場合、執筆者が気付く事がなければ、改竄された事が、誰にも判断ができないのは大きな問題だと考えられます。

しかし、このような問題もハッシュコードを計算して、ハッシュ値を暗号化して添付する事で問題は解決します。暗号化されたハッシュの事を電子署名と表現しています。
重要な文面を、電報、ハガキで送る人はいないと思いますし、重要度が増せば、封書、内容証明など、必要に応じた文書形態を要求されます。
電子文書のメールの場合は、ハガキと同等の扱いと考えられますが、しかし、筆跡がありませんので、ハガキよりも文書形態としては粗末な事は確かです。

ですが、電子署名を添付する事で、筆跡の問題は解決しますし、暗号化する事により、封書を用いた文書と同等の扱いが可能となります。電子署名と暗号化を同時に施す事で、印鑑を捺印した文書を、封書で郵送するのと同等の扱いが可能です。

電子署名と暗号化のもう一つの使用法として、迷惑メール対策に使えます。署名の施されているメールと、署名のないメールを、自動で識別する事ができますし、後述してある PGP、GPG を使用する場合、署名の有る無しが、一目で確認できますので便利です。

電子署名と暗号化は、電子文書に於ける印鑑やサイン、封書機能を齎しますが、このために必要な要素として、ハッシュ関数の計算、公開鍵（非対称鍵）の作成、その適用と言った、少々難しい問題もあります。しかし、これらの計算を一括して、システマティックに行う事の可能なソフトとして、PGP、GPG 等が開発されており、広く普及しています。一般的な要求と、必要な条件を、すべて満たしたソフトは意外に少ないのですが、現在の所、これらのソフト・ウエアーを利用するのが賢明だと判断しています。いずれのソフトも無料で使用可能ですし、オープン・ソースとなっています。性能に関しては、軍事用に匹敵します。

3　メールの危険性

メールが何故危険なのか説明しますと、インターネット上の情報を管理するサーバー、大型コンピューターによる大規模なルーターなどは、人手による管理がなくては、機能を維持する事は不可能であり、大勢のコンピューター管理者を必要としています。もしも、一人でも加害者に加担する者が従事しておれば、情報を盗み出し、不正な改竄などの犯罪を行う事は容易い事です。

実際にあった問題として、オウム信者がプログラマーとして、ルーターの開発に従事していた事が問題視された事を記憶しています。この報道を、記憶している方も居ると思いますが、当時、危機管理が指摘されていたのは確かです。しかし、この信者が、不正な活動をしていた証拠は何も無いので、付け加える必要があるかと思います。

他の事件としては、現在、存続している、某巨大カルト信者による NTT 通信記録、盗み出し事件が発生したのも記憶に新しい所です。NTT 内には、交換機に接続された、インターネット接続用のルーターが存在しますし、通信記録だけの被害に留まらない事は、ルーターの存在からも判断できる分けです。この事件の場合、有罪判決が下された事実もあり、重大な社会問題です。

この犯罪（ストーカー）の規模を考慮すると、加害者が一部のサーバーを運営している可能性も考慮しなくてはならないと感じています。

SSL, VPN, RSA, AES, PGP, GPG, MD5, sha1 … 、何れも、暗号化の技術を用いる際に使われる概念を表していますが、もしも、これらの技術が何らかの欠陥から、機能しない事態が発生したなら大変な事になります。インターネット上で取引されるカードの暗証番号などが、全て漏れる可能性があります。
暗号化の機能しないネットは、金銭に関わるような用途では全く使えませんし、全てのプライバシーも保証されず、高性能な糸電話と同じです。電話と違い、サーバーと言う中継コンピューターから、情報は幾らでも漏れてしまう原理がありますから、インターネット上では、金銭に関わる情報は、意識せずとも、自動的に暗号化される仕組みが備わっています。

電子文書に対する電子署名、暗号化などの対策は、言葉を変えて象徴化しますと、安全な通信路の確保という事になるかと思います。
この事は、個人的にプライバシーを守ると言う事ですが、ストーカー被害は、極論しますと、盗聴による個

人情報の流出と言う事が、その本質だと思いますので、電子文書に対しても何らかの対策が必要だと判断している分けです。
思考盗聴を受けているとの判断から、パスワードや、ディスプレー上の情報が漏れているので、暗号化は無意味だと断言する被害者もいます。
しかし、よく考えてみますと、銀行のキャッシュ・システムにしても、証券取引のオンライン・システムにしてもそうですが、すべて、安全な通信路を前提として、構築されている分けですし、PGP、GPG などの高度な暗号技術は、これらのオンライン・システムと同等の暗号強度か、それ以上の強度を誇っているのです。
この事から、暗号化した情報の漏洩は、重大な社会的規模の問題が発生した事と同値だと判断できます。このような強力な暗号を破る事は、愉快犯では不可能だと言う事ですから、我々の被害を、社会問題として捉える事が可能だと考えられる分けです。

もう一つ重要な事を書き加えますと、対称鍵方式の暗号化とは異なり、非対称鍵方式の場合、決定的な違いがあります。一般的な意味での暗号化とは異なり、秘密鍵（プライベート・キー）を盗む事ができない原理が存在します。仮に、パスワードを盗まれたとしても秘密鍵を盗まれない限り、電子署名を偽装する事はできない分けです。勿論、暗号を解く事もできない原理になりますが、しかし、テンペスト[1)]により、メールの内容が漏洩する事は防げませんので、暗号に関しては使用しても無意味かも知れません。
しかし、自身のプライベートな情報を、守る事をせずに、その漏洩を訴えている分けですので、インターネット上では、被害者は物笑いのネタにされています。このような評価を覆すには、被害者自身が、基本に立ち返って、しっかりと個人情報を守る事ではないかと思います。基本的な対策、防衛を行った上で、被害を訴えるのであれば、また違った評価が成されると感じている分けです。

その為に必要な手順は、思ったより難しくありません。PGP、GPG というソフトを、使いこなすだけの事ですし、盗聴法の成立と共に、これらのソフト・ウエアーの使用率は確実にアップしていますので、必要な情報は、望むだけ必要に応じて入手可能です。素晴らしい事に、軍事用に匹敵する高度な暗号化処理を、無料で使用可能ですし、その他の費用も一切掛かりませんので、是非、チャレンジして頂きたいと思います。

4　脳、コンピューターから漏れる電磁波の遠隔盗聴に関して

意外な事かも知れないですが、人の脳内の振動を盗聴する事の方が、コンピューターから漏れている電磁波を分析するよりも簡単だと判断しています。以下に、その根拠を書きます。

- 脳内のパルスの場合、電磁パルスを照射する事で、任意の変調を行う事ができる[2)]原理があるのに対して、コンピューターでは、そのような事は不可能です。
  人間の場合、思考に変調が発生しても、そのまま作動し続けますが、コンピューターの場合は、誤動作を起こしてフリーズしてしまいます。
- 信号の流れる速度も、コンピューターの方が桁違いに高速です。脳の場合、全体として見れば、数メガヘルツ程度の速度がありますが、実質的に言って細胞レベルでは、数キロから、数十キロヘルツ程度

[1)] テンペストに関しては、5 ページの段落を参照してください。
[2)] 脳波の引き込み現象とは、音、超音波、光、電磁波の振動に対して、脳波が共鳴を起こす現象の事です。

が上限です。しかし、コンピューターの場合は実質的に言って、数百メガから、数ギガヘルツ以上あります。

- 脳の場合は、統計的な手法を駆使して特徴を捉える事が可能ですが、コンピューターの場合は、一ビットでも誤りが発生すれば、フリーズ（凍結）してしまう特徴のある事から、統計的な手法など意味がありません。
- 更に、コンピューターの場合、多重並列化処理（パイプライン）により高速化されていますので、CPUの蓋を開けて、直接電極を取り付けて信号を読み出したとしても、その情報を解読[3)]する事は至難の業となります。しかし、スペクトルを分析する事により、ある程度の情報は得られるとは思いますが、この分析から、ファイルの内容を読み出せる事はないと考えられます。この方法では、恐らく、高度な暗号を解読するような確率的な検索を必要とすると予測できます。
- デジタル回路の場合、信号線は、並列に並んだ状態で、しかも、それぞれの配線や回路に流れる信号は、完全に同期している分けではありません。この事は、ストローブと呼ばれるデジタル制御技術をみても分かります。この事から、同じ繰り返しの信号が流れていたとしても、スペクトルは、毎回異なる事が理解できます。所謂、ジッターがある分けです。この状態で、現在の CPU、マザーボードから漏れる微弱な電磁波を、遠隔地から検出して、信号を分離する技術は、今の所、知られていません。

  強いて言えば、超高精度な干渉計の利用と、信号を分離するための、ブラインド・デコンボリューション技術でしょうか。しかし、平行して存在する信号のスペクトルは非常に類似性が高いですから、位相レベルで正確に信号を検出できたとしても、複数の信号の合成の結果が分かるだけですし、ジッターを正確に知る事は、神でもない限り不可能です。従って、やはり、確率的な分析を行わなければ信号を分離する事は不可能と判断できます。

  この観点から見る限り、デジタル回路と脳は、スペクトル的に、よく似た電磁波が漏れてると思えます。

結論しますと、脳とコンピュータの決定的な違いは、脳の場合、外部からの電磁パルス等の刺激により、任意の変調が可能だと言う事に尽きると思います。その次に、スピードの違いです。それから、脳は、電磁ノイズに非常に強い[4)]のに対し、コンピューターの場合は、非常に弱い事が挙げられます。
現在普及している、コンピューター内部から漏れる電磁波を検出して、分析から、ファイルの内容を復元する事と、人の脳内の、ニューロン細胞から漏れる電磁波を検出分離する事は、信号の分析技術と言う観点からは、同じ技術が使われると考えられます。しかし、任意の変調ができない場合、いずれの場合にも、信号を分離する事は原理的に言って不可能だと思います。

コンピューターの場合、シールドを強化する事が可能ですし、更に、簡単な装置で、電磁ノイズを発生する事で、コンピューター部品から漏れる微弱な電磁波を、隠蔽して防衛する事[5)]も簡単にできます。

もしも、コンピューター内から漏れる信号を、正確に盗聴する技術があるとすれば、大規模なテロを簡単に起こせると判断しています。

[3)] この情報は機械語の羅列ですから、逆変換により、ニーモニックに変換できますが、必要な情報だけを抽出する事は、想像以上に困難です。機械語を理解している人であれば、予測が付くと思います。

[4)] 強いて言えば、脳は、変調した電磁ノイズに弱いと言う事になるでしょうか。例えば、サブリミナル効果などにも弱いと考えられますし。

[5)] この防衛方法は、脳波の遠隔盗聴[6)]に対しても、機能する事が判明しつつあります。

多くの人に危害を加えて、思考盗聴の噂が広がる事は、加害者からしてみれば不本意な事に思えます。この噂は、小規模な時とは異なり、もはや社会的な問題になるのは時間の問題だと感じているからですが、脳波の遠隔盗聴[6)]が、技術的に可能だと認知された瞬間から、立場は逆転する事になるでしょうし、連中にして見れば、これ以上の噂の広まりは好ましくないはずですが、しかし、恐らく、脳波の盗聴[6)]はできても、コンピューター内の情報を、遠隔地から盗聴する方法はないのでしょう。

私の考えでは、人の思考よりも、その生産物であるコンピューター内のファイルの方が価値があります。そのファイルは、思考の凝縮（濃縮）した結果だからです。遠隔地からの盗聴により、コンピューター内のファイルを盗めるのであれば、一瞬で済む事ですし、好き好んで、一日中、人様に付き纏う必要はないと判断しています。

被害の状況から判断しますと、被害者の生産を妨害する目的を感じ取れますし、生産物を盗む気は、最初からないとも感じ取れます。それとも、連中が恐れているものは、被害者と、連中自身の潜在意識の中に存在するのかも知れません。コンピューター内のファイルなどには、関心は無いはずですし、必然的に、その盗聴技術には関心がないか、不可能な事を知っているのだと思います。

もしも、高度な暗号化、電子署名などの改竄が多発するようであれば、自宅室内に不法に進入されていないか確かめた上で、秘密鍵を遠隔地から盗聴可能か、もう一度、検証し直す必要が生じます。秘密鍵が、CPU から漏れる電磁波により、盗聴されている事が明確に証明されるならば、重大な社会問題を提起する事になるでしょうし、思考盗聴、CPU からのファイルの盗聴、どちらが証明されるにしても、正確に検証が可能な証明であれば、世界中がパニックになる事は確かです。

5　秘密鍵の力

PGP、GPG などの公開暗号方式を用いる事で、副次的に得られる貴重な財産もあります。遠隔地からの盗聴という方法では、秘密鍵を盗む事はできない原理があると考えられるのです。

遠隔地から、盗聴によって得られる情報としては、

> 暗証番号は、通常キーボードから直接、打ち込んで使用しますが、指の動き、キーを叩く音を分析する事[7)]により、暗証番号を盗聴する事ができると言われています。過去に FBI が、この方法により暗証番号を入手して、犯罪が解決した経緯があり、IT 系の情報として流通している事実があります。
>
> また、ディスプレーから漏れる微弱な電磁波を盗聴して、FFT 解析する事で、遠隔地から画面の内容を盗聴可能なテンペスト技術が普及しています。この情報に関しては、検証した映像等がネット上に存在しています。この機材は、それほど高価なものではないようです。

しかし、現時点では、CPU から漏れる、複雑高速、微弱な電磁波から、ファイルの内容を盗む技術は存在していないと判断しています。ディスプレーから漏れる電磁波の解析とは異なり、桁違いに難しい要因がある事は確かで、一つには、電磁スペクトルのパターンが異なる事と、CPU の場合、スペクトルが、絶え

[6)] 正確には、脳内、言語野に生じているパルス列の、遠隔地からの盗聴。

[7)] 叩くキーの位置により、微妙に時間タイミングが異なり、また、キーを叩く強さの癖、等を総合的に判断する事で、パスワードを分析する事が可能だと言われています。

ず変動している事が挙げられます。CRT の場合は、映し出されている映像は静止画ですので、スペクトルは非常に安定しています。
この事から、公開鍵に用いられる秘密鍵を、遠隔地から盗聴して得る方法は、極めて限られていると考えられますし、コンピューター内に仕掛けられた、ハッキングの為のソフトなどが動いていない事が明確であるなら、秘密鍵を盗む事はできない原理になります。

この秘密鍵は、コンピューターが計算により自動的に作成しますので、作成者自身が、内容を確認する必要さえないのですから、テンペストの対象にはなりませんし、思考盗聴の対象でもありませんので、秘密鍵の場合、原理的に特別な保護（防衛機能）があると考えられます。
遠隔地から、思考（脳波）盗聴によりパスワードが漏れたとしても、秘密鍵は守られている原理です。

パスワードと秘密鍵を、遠隔地から盗むには、脳と、コンピューターの二つから、情報を盗む技術を必要としている事になります。
しかし、コンピューターの場合、１ビットでも情報が異なれば、その情報は役には立ちませんし、今日のコンピューター内部の、複雑な超並列、分散演算を行うシステムでは、直接電極を接続して情報を検出したとしても、必要な情報だけを分離、検出する事は実質的に言って不可能に近いですし、まして、遠隔地からCPU の動作状態を正確に盗聴する事は、特殊な条件があったとしても無理だと判断できます。
恐らく、直接室内に侵入して秘密鍵を盗まない限り、秘密鍵を盗む方法は存在していません。秘密鍵を、フロッピーディスク、USB メモリーなどに記録して持ち歩く事で、実質的に言って、物理的な鍵を持ち歩く事と同じ扱いが可能です。ハード・ディスクに秘密鍵を残さない事が要点になるかと思います。

> この点に関して補足しますと、OS の操作として（通常の方法）ファイルを消しても、ハードディスク上には、ファイルの内容は記録されたまま残ってしまう点に注意が必要だと思います。つまり、ファイルが見えない状態になるだけです。専用のソフトで消去するか、或いは、PGP の完全消去機能[8)]を利用して、秘密鍵をハード・ディスクから完全に消去する事をお薦めします。

この原理が、ネットを使う上での、最後の砦であり、切り札となると考えています。
強力な暗号を破る方法が無い分けではありませんが、例えば、量子コンピューターのような、特別な原理を使用したコンピューターを使わない限り、RSA 等の公開鍵を破る事は確率的に言って不可能ですし、何れにせよ、RSA、AES 等の暗号を破るには、莫大な経費を負担しなければなりません。

6　情報漏洩の他の問題

ウイルス対策ソフトの利用率は、ネット上の調べでは、現在、80 パーセントに近づいているようで、殆どの人が、何らかのウイルス対策を行っている事が分かります。これは、ウイルスに対する問題意識の高さの表れだと思います。しかし、それでも、情報の漏洩問題が増加しているのは不思議な事です。問題の背景には、P2P ソフトの取り扱いに於ける問題意識の甘さがあると指摘されています。

P2P ソフトと言われるファイルの共有技術は、java などの開発に伴って発展して来たものと言われていますが、P2P 技術そのものが一人歩きを始め、その扱いが社会問題化している経緯がある分けです。

---

8) ファイル情報に対して、特殊な乱数列を繰り返し上書きする事で、ファイルを読み出す事ができない状態にする技術の適用。

大学、役所、警察、防衛関係？、巨大企業 … などから膨大な量の個人情報の流出が報道されていますし、確認されたものだけでも大変な量ですが、実質的には、これまでに明らかにされた情報の、数十倍を上回る情報が漏洩していると思います。それ程、P2P ソフトの普及率は高いです。
P2P ソフトは、現在、インターネット上でも締め出しが行われており、新しく開発されたソフトを除けば、古い P2P ソフトは実質的に作動しない状態ですが、しかし、新作 P2P ソフトが後を絶たない事は周知の事実です。困った事です。

P2P ソフトを使用する限り、コンピューター上の個人情報は垂れ流し状態だと考えられますし、それが証拠に、大規模な集団に属す個人から、大量の個人情報が流出している分けです。企業によっては、P2P ソフトを使用した為に、運営情報の漏洩が発生した場合、解雇の対象になると言う話も聞かれます。重大な社会問題だと言えます。

P2P の技術が使われているにも関わらず、それとは知らずに、ソフトを利用している事もあるかも知れません。因みに、スカイプと言う有名なソフトも P2P ソフトです。このソフトの場合、ソース・コードの一部が公開されておらず、具体的に、どのような内容の情報が扱われているのか、疑問視する声も少なからず聞かれます。個人情報が、このようなソフトにより、インターネット上に漏れない可能性の方が低いと判断しています。

使用するソフトも、気をつけて選択する必要を感じています。使用しているソフトの大半が、P2P ソフトという状態では、集団ストーカー被害を訴えても無駄かなと感じる分けです。
安全なソフトとは、どういった物なのかを定義する事は難しいですが、一つには、ソースコードが公開されているか、或いは、信頼のある企業から発売されている物などの、ある程度の基準が満たさている事だと思います。ネット上の評価を検索する事で情報が得られる事もあります。私の場合、少しでも疑いのあるソフトは避けています。

何故、P2P ソフトがそれ程、問題なのか考えてみますと、これは一言でいって、サーバーの問題です。HTTP、FTP などの、事情の分かっているサーバーの場合、対策が立てられますが、しかし、コンピューター内部に、分けの分からないサーバーが存在すると、事情はまったく異なります。
このサーバーを介して、ハッキングなどの不正な行為を行う事は、簡単な事だと判断ができます。このようなソフトを介して、コンピューター内部のファイルを、不正に持ち出されたとしても、不正を知る術は限られていますから、一般には、不正を知る事は無理だと言う事になりますし、個人情報の漏洩が頻繁に発生してる場合は、P2P ソフトの使用を中止せざるを得ないかも知れません。
或いは、P2P ソフト専用のコンピューターを用意して、重要な情報は共有しない等の対策を施す事でも、危険を回避できると考えています。何の対策もしないまま P2P ソフトを使いこなす事は不可能ですし、対策を施していても、失敗する事があると訴える技術者もいます。ましてや、技術に精通していない者が P2P ソフトを使用する事は、無謀だと考えられます。

いずれにしても、個人情報の流出には十分注意したいです。この問題が何時、自分の身に起こらないとも限らないのですから怖い事です。もしも、会社の顧客情報、重要書類が、自分のコンピュータから … と考えると背筋が寒くなります。情報の漏洩と言う問題に関しては、P2P ソフトを使用する限り、被害に遭う確率が高くなる事は否定できません。

7　あとがき

高度な技術を身に付けた人でも、問題のあるソフトを使用すると、情報が漏洩する事があるようですし、有名な、ウイルス対策ソフトを開発している、会社のホームページが、改竄されたと言う情報も流れている時代ですが、しかし、情報の漏洩、安全な通信路の確保といった基本的な問題をクリアーした上で、個人情報の漏洩を訴えない限り、笊で水を掬うような事態になりかねないと判断しています。

集団ストーカー被害に関しては、究極の、情報の漏洩（思考、脳波、の盗聴）を訴えるのですから、一般的な対策を、すべて施した上でないと、その訴えも色あせてしまう事でしょうし、被害との戦いに勝利するには、練り上げられた作戦と、被害者間の協調を必要としていると思います。

柔道にある諺のように、重力を制する事で、小さな力と体で、より大きな力と体を制する事ができる、という表現があります。鍛錬の重要性と共に、物理的な原理の事を言っているのだと思います。

たとえ、被害者の数が、加害者の数に対して、桁違いに少なくとも、心臓を射抜くような、ポイントを押さえた対策と、継続的な努力、少しの協調があれば、巨大な犯罪組織に、風穴をあける事も不可能ではないと考えています。