視　点

「メタデータ・ネットワーク時代のセキュリティと保護」(3)

東京大学　国際・産学共同研究センター　教授　　安田　　浩

キーワード
IT封鎖、メタデータ、コンテンツ流通、次世代ネットワーク通信、ネットワークセキュリティ、知的財産権保護、プライバシー保護、ユビキタス通信環境

1．　はじめに

ディジタル化され、ネットワーク化されると格段に便利になるが、それと裏腹に対面コミュニケーションの時代には考えられなかった危険が生じてくる。第一編で、ネットワークやその上に流れる情報にどのような変化が生じているのかについて分析し、電子化ディジタルコンテンツ（以下コンテンツと略称）流通上の最も特徴的な変化がメタデータの整備・流通にあることを示した。第二編では、このような時代の特徴を捉え、コンテンツ流通が21世紀産業の基盤となるところから、コンテンツ流通に関わる安全性、特に知的財産権の保護について現状と将来展望を示し、コンテンツを特徴づける識別子（以下IDと略称）付けを重点として、この動きについて述べた。アプリケーションあってのネットワークであることを示すために、このような順序で話を進めたが、セキュリティの高いネットワークができなければアプリケーションでのセキュリティが確保できないことも明らかである。第三編では、ネットワークセキュリティの課題について述べる。

2．ワシントンDCでのテロ体験から

「America under ATTACK」あの忌まわしいテロ事件に米国マスコミがつけた名前である。2001年９月11日午前テロ発生の瞬間、私は仲間21人とともにワシントンDCにいた。それもペンタゴンを09：10頃かすめて南へ15Km移動し、その地点でペンタゴン突入時の「ドーン」という大きな音を耳にし、立ち上る煙を目にしたのである。その後の言語を絶する航空界大混乱の中で何とか便をさがし、ワシントンダレス空港から日本への再開１番機の席に収まって、離陸した瞬間は感無量であった。テロ行為の忌まわしさをまさに実体験として感じたわけであるが、テロ発生後旅程をすべてキャンセルされ、帰国の飛行機に乗り込むまで約50時間、ホテルに缶詰になりただひたすらテロと飛行便の情報をチェックする中で、セキュリティに関する少なからぬ考察を行うことができたことは、今後の研究生活に大きな影響を持ったと確信している。

何が気になったか。第一は国際通信に関わることである。テロ発生が起こったとほぼ同時に幸いにも我々は詳細な情報を入手することができた

（たまたま打ち合わせ中の相手がCATV会社でTV情報を簡単に入手できた）ので、直ちに全員の安全を日本に連絡するように図ったが、すでに国際回線は超輻輳の状況でなかなか接続できず、約２時間かかってようやく連絡がついた次第である。たまたま日本が深夜にかかる時間帯であったので、日本側での混乱が大きくなることは無かったのが不幸中の幸いであった。その後もこの状態は継続し、混乱を避けるためか、国際電話はクレジットカード通話のみに制限され、慣れない人たちは連絡がなかなか取れずイライラがつのっていた。一方インターネット接続は、ワシントンDC近傍と言う地の利から、どのネットワークともアクセスポイントが市内に存在し簡単に接続ができた。あの混乱の中でも接続ポイントが輻輳することはなく、またインターネット自身の動作にもそれほど輻輳の影響があるようには感じられなかった。電子メールによる連絡でどれだけ助かったことか。逆にインターネットにも問題が出たらもっともっと大騒ぎになったことと確信する。ウィルスNimdaの攻撃がテロに遅れたことは不幸中の幸いであり、これがもし同時を意図されたものであったらと思うとぞっとするのは私だけではないと思う。

すなわちネットワークなしではすでにビジネスだけでなく、生活すらできないことは明らかになっており、ネットワークを失わないことに全力を挙げなければならない状況を確信・確認した次第である。日本のネットワークは大丈夫かを後で述べたい。

次にホテルに缶詰になり、TV情報三昧の生活の中で映像情報について感じたことが２点ある。今回のような突発事故としては珍しく、２回目のWTC突入事件については発生の一部始終をプロがビデオカメラで撮影し、それが情報として提供されていた。与えられた映像情報は臨場感あふれる内容であり、映画を見ているようなと言う解説には不満であった。ところが、半日経った頃から映像に違和感を覚えだし、何がおかしいのかなと思いつつ映像を見続けたところその原因を発見した。つまり映像がどんどん作られて行く過程を目の当たりにしたので、最後の方は違和感が大きくなったのである。WTC北棟への第二の襲撃のスローモーションが半日後くらいから流れだしたが、これぞまさしく画像処理の典型といえよう。スローモーションを作るには高速度撮影機能を持った特殊なカメラが必要（通常は１秒間に30駒の映像を撮りこれを再生するが、高速度撮影では１秒間に120駒くらい撮影し、これを通常の１秒間30駒で再生して時間を４倍に引き延ばすことで、スローモーションにしている）であり、通常のビデオカメラで撮られた映像では、どんなに頑張ってもストップモーション画像でしかスローで見せることはできず、あの瞬間いかに準備の良いマスコミ関係者でも高速度撮影カメラまで用意ができていたとは思えない（準備できていれば、最初からスローモーションの映像が流せるはずであり、半日後に流されるのはおかしい。相撲中継の本番とスロー再生の関係をお考え頂ければ理解は容易であろう）。すなわち最初の数時間は実写状態の映像であったのが、その後は画像処理がふんだんに加えられた、文字通り映画を見せられていたことになる。

我々はワシントンDCのペンタゴン近くで、立ち上る黒煙を見たことから、TV映像を実感することができたが、そうでない人達もあの映像を容易に本物と信じてしまうのだろうかと考え込んでしまった。情報の信頼性・正しさとは何なのだろうかとも思う。1970年マーシャルマクルーハンは「メディア論」の中で「音声メディアはホット、映像メディアはクール」と喝破し、シンボル化された音声情報（すなわち送り手の意図で取捨選択

された情報のみが伝えられる）の危険さを訴えたが、世紀が代わってクールなはずの映像（作為の入らないはずの情報）にも危険が発生してきたことが明らかとなったのである。ネットワークを流れる情報の確かさを検証する手段を提供しないと、何を信じて良いのか解らない時代になってしまうことを切実に感じ取った次第である。

次に繰り返し流される突入シーンを、ビデオに収めておきたいと切実に思った。残念ながら出先であり、かつ簡単に自宅に連絡が取れない状況でもあったので、ついに機会を逸してしまった。この事件と映像は21世紀を象徴するものであり、繰り替えし使われ続けることになろう。多分多くの人がビデオ化しており、それが私的な使用の範囲を超えて使用されることは間違いないと思われる。厳密に言えば著作権上の違法コピーが多くの場所で登場し、使われ続けることになるわけである。このような事態を想定して、コンテンツへのID付与を検討しているのであるが、現実のこのような例が発生するに及んで、さらにID付与の重要性に思いを新たにした。

3．危ないネットワーク

このようなことを想像してはいけないのだろうが、インターネットを混乱させるには重たいSPAMメール攻撃を意図すれば簡単ではないだろうか。例えば、30万人規模のグローバル企業の全社員のアドレスを手に入れ、５MBの添付ファイルをつけて30万同報で流すことを計画する。仲間1000人が世界中に分かれて、このような同報を10種類ずつ流すとしたら何が起こるだろうか（30万同報が物理的に作り難いことは確かだが、リストさえあればコンピュータはやってくれる）。この結果、ネットワークのトラヒック量が跳ね上がって輻輳状況となり、正常な通信が妨げられることは明らかである。機械通信の脆弱さそのものと思う。同報数を制限するということが対策であろうが、ハッキングにより同時多発同報メール発信エージェントを、全世界に組み込んでしまえば同じことができることになる。インターネットが、如何に組織攻撃に弱いかはこの例から明らかである。

次に不正コピー問題を考えてみよう。コピー手段は発達を遂げて完璧の域に達してきた。これに対し、様々な技術やシステムで不正コピー防止策が試みられており、それなりの効果をあげてはいるが、まだ不安は残っている。そのため、ライブ以外はビジネスになりにくいとの話が最近は有力であるが、ネットワークの発達はそのライブをも危うくしている。第三世代携帯、第四世代携帯では、２Mbpsないし10Mbpsの伝送速度が実現し、かつAnytime Anywhereとなる。さらにマイク・ビデオカメラの性能向上は目を見はるばかりで、劇場内への持ち込みをチェックすることは困難を極めることになる。数人がマイク・ビデオカメラを持ち込み、適当に分かれた場所から携帯を使って上演をインターネット中継すれば、極めて容易にライブの違法同時立体生中継が実現可能であり、会場外で簡単にライブが楽しめることから、興業者はビジネス機会を大幅に失ってしまうことになると思われる。会場内を携帯電波が通じない世界にすれば良いというのが唯一の解決策であるが、振動モードでのかつメール形態の緊急連絡まで禁じてしまうのは、Anytime Anywhereに慣れた現代では許されないであろう（それが劇場へ入るときの契約とすれば許されるかもしれないが、そんなところに入りたいと思わないのでは？）。

以上は、私が容易に解決策が思い浮かばない大きな危険である。これ以外にもいろいろ危険が一杯である。「ｅガバメント、ｅビジネス、ｅライフ」が合い言葉でインターネット基盤が推進されているが、「危険が一杯」状況も身近に迫って来

ているのである。この様子を図１に示す。

図１　コンテンツ流通：各プレイヤー間の関係

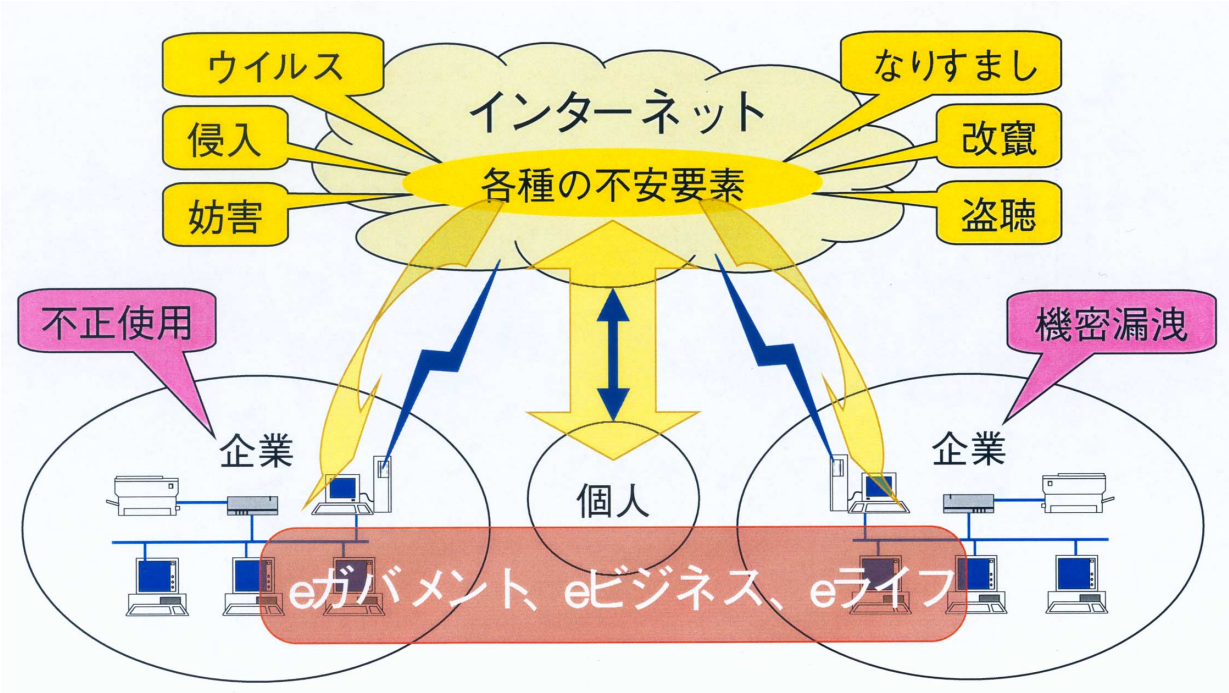

図１では、インターネットを通じて、ビジネス・生活などを営んでいる個人や組織に対し、「盗聴や改竄あるいはウィルス」といった直接的な危険がせまり、さらには「侵入・妨害」などによりPCやサーバなどがダメージを受け、なりすました悪人により徹底的に痛めつけられるという構図が見えてくる。

実際に、昨年初来あるゆるところのホームページ改竄は後をたたず、ウィルス被害も広がる一方であり、ある統計によればインターネット接続を行っている会社は平均して月に８回くらいは重大障害に及びかねない攻撃を受けていることが明らかとなっている。どのように対処すれば良いのであろうか。

４．ネットワークを守り抜かないと国、組織、個人が村八分！－ＩＴ封鎖－

上記の危険から逃れ、情報の信頼性を確保し、さらには著作権に関わる話を正常化するには、次の内容を確認し守れば良いことは明らかである。

・情報は誰からきたものか
・間違いなくその人が出したものか
・途中で改ざんされていないか
・誰かに盗聴されていないか
・必要な人のみがアクセスしているか

暗号化や電子署名によりこれらのことを確保しようというのがPKI（Public Key Infrastructure）であり、21世紀ネットワーク社会はPKIの完全さに全面的に依存することは明らかである。

ある国、組織、個人がPKIを遵守することは、

何を意味するのであろうか。思い起こして頂きたいのは増水した川の堤防の状況である。すべてが同じ高さにあれば、最後の最後に一挙に瓦解することにはなっても、かなりの時間は持ちこたえることが可能であり、もしかしたら崩壊の寸前に水が引き始め難を免れることが可能となる。ところが１カ所でも低いところがあれば、早い段階でその場所から崩壊が始まり、全面的に堤防が決壊して被害は大きなものとなろう。全体の被害をさけるために被害にあっても良い地域を作り、そこが先に崩れる構造にするという考えも無きにしもあらずであるが、ネットワークには残念ながら被害にあっても良いという部分がない。

ここで言う堤防の高さが、PKIあるいはネットワークセキュリティの完全さのレベルとなっているわけであり、レベルがそろっていれば非常に強いネットワークとなるが、一カ所でも弱い所が有れば早い段階でそこから崩壊が始まることは明らかであろう。接続されたネトワーク間で崩壊の波及がくい止められないことは、ウィルス被害の例を見るまでもなく明らかであることから、ネットワーク側の対処方法も明確である。すなわち自分よりもセキュリティレベルの高い国、組織、個人のネットワークは接続するが、レベルの低いところとは絶対につながないという方針である。逆に言えば自己の傘下に弱いところを作ってはならないと言うことである。

ここで日本の特質を考えてみよう。現状は、インターネット普及率はまだ低く、セキュリティがらみの大問題が発生してはいないが、いくつか事例は発生している。例えば大学のセキュリティレベルが低く、なりすましやSPAMメールの温床になっていると指摘をうけたことは記憶に新しい。知的レベルが平均的に高く、ビジネス意欲も強いが、セキュリティ意識が低いのが日本の特徴であり、もっとも狙われやすい体質にあると言えよう。今までのインターネット普及は、それなりに技術と意識のある方々の範囲であったが、今後爆発的と見込まれる普及は、使う意欲は旺盛だが自分を守る意識の少ない平均的日本人となろう。加えてブロードバンド・常時接続となれば悪の跳梁はますます容易となり、崩壊の波及もかってないほど短期的になりうる。このような日本の状況を見る世界は何を考えるであろうか。

結論は明確であろう。電話網は、中央集権的であり組織化されたネットワークであるので、中枢のみのレベルアップでも対応は可能であり、世界に冠たる品質、安全レベルを持つ電話網に育ち、一般人・組織は意識や努力することなくグローバルな接続の効用を享受することができてきたわけである。インターネットはこの対極にあり、分散型で個人化されているのが特徴である。国のネットワーク、組織のネットワーク、家庭のネットワーク、そして個人のサイトがからみあって接続されているのがインターネットであるが、統一した管理ということはあり得ず、個々の責任において運用がまかされている。一つでもセキュリテキレベルが低いところがあれば、それは全体のレベル低下を、ひいては国全体のネットワークセキュリティレベルの低さを意味することになり、グローバルネットワークからの接続を拒否される、昔風に言えば世界ネットワークから日本のネットワークが村八分－IT封鎖－になってしまうことになる。もしそうなれば、日本のビジネス組織は窒息してしまうであろう。

５．まとめ　ーネットワーク的孤立（ＩＴ封鎖）を避ける国家施策をー

村八分を避け生き残るためには、日本地域在住者全員のセキュリティ意識を高めること、また高いレベルのセキュリティ環境を、自己の力で準備することが必要である。セキュリティ環境を他人

に依存することは、その基となった他人よりセキュリティレベルが低いことは確実であり、他よりもレベルが低いことの証明以外の何物でもない。インターネットの爆発的普及を前にして、セキュリティ対策、なかんずく自前の発想に基づくセキュリティソフトウェア開発を、国家的大方針のもとに進めることが望まれる。今この努力をなさなければ、遠からず日本地域に在住する人・組織は、グローバルネットワークからの村八分に怯えるか、周囲を無視して自分だけグローバルネットワークの信頼をかちえる努力を行わざるを得なくなるであろう。

第一編から本第三編までで、将来の日本の産業を支えるコンテンツ流通の重要性と、それを支えるネットワークセキュリティにおける村八分の恐ろしさを述べてきた。ネットワークセキュリティの分野で、縦割り行政を乗り越える大きな方針の設定を国に期待するとともに、その方向へのコンセンサス作りに努力していきたい。

３回にわたる「視点」連載を支えて頂いた、コンテンツIDフォーラムの皆様、ネットワークセキュリティ論議にご意見を頂いたセコム田尾様、INS岩見様に深謝します。