ネットワーク時代の情報セキュリティ

東郷 行紀 (水交会 研究･普及委員)

はじめに

尖閣列島沖における中国漁船衝突事件のビデオを、海上保安官の手によって流出させた事案は、ネットワーク時代の情報管理に、大きな問題が多数有ることを、改めて明らかにしました。海上自衛隊においても、過去にネットワークを通じた情報漏洩事案があり、情報管理態勢を強化しつつあります。しかし、この種の管理に絶対はなく、引き続きより高度な情報管理態勢を構築する努力を続けなければなりません。

そこで本稿では、ネットワークやパソコン（以下PCと表記）にあまりなじみの無い方にも分かり易く、問題点の分析とその対策について述べてみたいと思います。しかしながら、筆者はテレビ番組の解説委員のような能力もなく、一部の方には何を言っているのかさっぱり分からないと、おしかりを受ける内容になったことを最初にお詫びいたします。

さて、本論に入る前にネットワークとは何か、情報セキュリティとは何かを改めて整理してみます。

(1) ネットワークとは何か

ネットワークの定義はいろいろありますが、概念としては「ネットワーク自身が提供する共通サービスを用いた情報の共有」であると筆者は考えています。ネットワークは物理的には、有線や無線で情報をやり取りするツールです。しかし、ネットワークを単に情報をやり取りするツールだとするのなら、昔からある電話やファックスもネットワークということになります。それでは現代のネットワークは、電話やファックスと、どこが違うのでしょうか。

われわれの身近にあるインターネットを考えてみると、PCをネットワークにつなぐだけで、メールができ、新聞、雑誌が読め、チケット等が買え、銀行の決済ができ、画像も動画も楽しめます。これらは全てインターネットというネットワークが提供する、共通サービスにより実施できます。またネットワーク上を流れる全ての情報は、デジタル化されています。このため、一つのネットワークを多くの人が共用できる点が、従来のアナログの電話やファックスとは根本的に異なります。（現在の電話やファックスの一部はデジタル化されています）

(2) 情報セキュリティとは何か

情報セキュリティとは一般的に、知ることを許可された人だけが、情報にアクセスできる「機密性」、情報が改ざんされたり変化・劣化しない「完全性」許可された人が情報を自由に加工する等して利用できる「可用性」の、3つが担保されることを意味します。尖閣列島における中国漁船の映像を流出させた海保事案の場合、報道によれば、機密性が不十分であったため、許可のあるなしにかかわらず、誰でも問題の映像にアクセスでき、それを持ち出すことも可能だったということになります。また流失した映像は、流失させ

た保安官が6分割して投稿したそうですが、6分割できたということは、完全性にも問題があったことが分かります。

1. ネットワーク時代の情報セキュリティでは何が問題なのか

(1) ファイル

ファイルとはコンピュータが取り扱うデータの固まりであり、文字、画像、音声、プログラム等全てのデータの基本単位はファイルとして扱われます。ファイルがやっかいなのはPCを操作する人（ユーザー）が意図的に作るファイルもあれば、操作の過程でPCが勝手に作るファイル（作業ファイルやバックアップファイル等）も多数あることです。PCが勝手に作った、例えばバックアップファイルには、元のファイルと全く同じ内容が書き込まれ、本体に秘を含めばバックアップにも当然秘が含まれます。バックアップファイルは、アプリケーションソフトによってはユーザーが見えない（操作できない）こともあって、管理が極めて難しいのです。しかし、このファイルを適切に管理しなければ、情報セキュリティは成り立ちません。

(2) パソコン

現在市販のPCは、一般的にはスタンドアロン型と呼ばれ、PC単体でほとんど全ての機能を有し、前述のファイルを作ったり加工したり、それを保存したり、またネットワークを通じ、情報を収集したり発信することが容易にできます。市販のPCにはもちろん情報セキュリティの要（かなめ）である、機密性、完全性、可用性を担保する機能もありますが、あくまでそれらの機能の活用はユーザーの判断です。

購入したばかりの状態では使い勝手を重視するあまり、可用性は十分担保されますが、機密性、完全性はユーザーの高度な専門知識と、それを支える別売りのセキュリティーソフトを使わなければなりません。例えばPCの中にあるファイルはユーザーによって容易に変更（改ざんを含む）でき、またUSBメモリー等により容易に持ち出すことも可能です。そこで、セキュリティーソフトを導入し、例えば、資格のある人でなければ、特定のファイルにアクセスできない、ファイルに暗号をかける、また、USBメモリー等でファイルをPCから持ち出すことを禁止するソフトも市販されています。このような対策を講じ、ある程度の機密性と完全性は担保出来ることになります。昔、PCはソフトが無ければ、ただの箱と、言われたことがありますが、今やPCは、セキュリティーソフトが無ければ、ただの危ない箱なのです。

市販のPCは、これだけネットワークが普及しているにもかかわらず、相変わらずスタンドアロンの発想を抜け切れていません。例えば利用するほとんどのソフトを、PC自らが持たなくては機能しないようになっています。よってネットワークの定義でも述べたように、ネットワークが提供する共通サービスでの情報の共有を、必ずしも追求しているとは思われません。

一方で、PCの世界でもネットワーク・セントリック・コンピューティング（ネットワークを中心としたコンピュータの運用形態）がようやく実現しつつあります。

(3) インターネットとイントラネット

インターネットは全世界で使われている最も一般的なネットワークですが、極めてオープンな一般の人が誰でも利用できるネットワークであるが故に、サイバー攻撃等の危険に曝され易いのが問題です。報道によれば、2010年4月に米政府系のインターネットに、約18分間にわたり中国のサーバーを経由した工作が行われたようです。残念ながらインターネットでは、サイバー攻撃を完全に防ぐ手段は無いのが実状です。防衛省自衛

隊でも、インターネットを使わなければ仕事にならず、一部のPCはインターネットに接続しています。もちろん接続するにあたり、強固な壁（ファイアーウォール）を作り、容易に外部から侵入されない、また内容が流出しない態勢をとっています。

インターネットは全世界的ネットワークですが、これと全く同じ仕組みを、部内だけで利用し、部外とは接続しない利用方法もあり、これをイントラネットと呼称しています。防衛省自衛隊でもイントラネットを導入していますが、インターネットとイントラネットはセキュリティ上、完全に分けて使用しています。物理的にインターネットとイントラネットを分ければ、イントラネットに対するサイバー攻撃等は防ぐことができます。

(4) 文書とファイル

過去も現在も正式な命令や通達等は、全て紙媒体の文書でなされることが一般的です。防衛省には保全関係規則の他、文書管理規則があり、文書の管理態勢は、一応整っていると言っても良いと思われます。何故なら紙媒体には問題のファイルは一切含まれず、確実な管理ができるからです。

電報は、紙媒体の文書とファイルの持つ柔軟性を併せ持つ、今後もずっと使われるであろう情報伝達手段ですが、規則上は文書の一部です。電報はネットワークを通じ、ファイルで送られますが、そのファイルを決して相手に渡さないシステムなのです。正確には電信室まではファイルは行きますが、そこで原則として紙媒体に変換し、ファイルは電報システムの外に出ることはありません。最近では電報閲覧用の特別なシステムを使い、所要の電報を検索、表示させることができますが、閲覧者は元のファイルにアクセスできないようになっています。

文書も電報も、基本的には紙媒体であり、相手にファイルを渡さないシステムであることに加え、完備された規則の下で長い運用実績があり、機密性、完全性は担保されています。問題は紙媒体ですから、可用性に限界があります。ファイルならば、それを受け取った相手がいかようにも加工する等して利用できますが、紙ではその情報に基づき、またファイルを作らなければなりません。

2. ネットワーク時代の情報セキュリティ実現のために

今まで縷々述べてきたことをまとめますと、ネットワーク時代の情報セキュリティ上、最大の問題点はファイルの管理に尽きると言っても過言ではありません。そこで本稿では、どうやったら容易にファイルを管理できるのかに的を絞り、その対策について述べてみたいと思います。

その前にもう一度情報セキュリティーの定義を復習してみましょう。それは情報の「機密性」「完全性」「可用性」を担保することです。実はこの3つ、互いに相矛盾するのです。すなわち、機密性の担保を厳格にすればするほど、本来の目的である情報の共有も、可用性の担保も難しくなります。また完全性を追求すれば、当然可用性は損なわれます。よってファイルの管理を考える際には、情報セキュリティの3要素をバランス良く考慮しなければなりません。

(1) ユーザーにファイルを持たせない。

一般的なPCの上で、ユーザーは自由にファイルを作ったり、既存のファイルを加工することができ、でき上がったファイルはPC上で保管することができます。しかしファイルの厳格な管理のためには、ファイルに暗号をかけたり、作業終了後はファイルをPCから取り出し、それを保全ロッカーに格納保管する等、ユーザー自らが、煩雑な管理をする必要があります。しかし、このやり方では、必ずしも万全とは言えません。何故ならユーザーが意図しない、PCが勝手に

作る作業ファイルや、バックアップファイルの管理が不十分なのと、悪意をもったユーザーの情報流出等の犯罪行為を防ぐことができないからです。現在ウィキリークというサイトが話題になっています。これは内部告発と称していますが、実態は部内関係者自らが、職務上接することのできる秘密を含む多量のファイルを不正に持ち出し、ウィキリークサイトに投稿するという犯罪行為です。現在のファイル管理体制では、部内関係者のファイル持ち出し等の不正行為を防止するのは極めて難しいのが実状です。ですから例えウィキリークスを廃止に追い込んだとしても、似たようなことは再び起こり得るのです。

そこで、ユーザーが作ったファイルは、ユーザーに持たせない、正確にはユーザーが作ったファイルは、作成したPCとは別の場所に自動的に保管させるようにし、それを管理者が厳格に管理すれば、問題は解決できます。逆に言えば、PC端末にはファイルを残さないことです。これはスタンドアロンのPC単体では困難ですが、ネットワークを利用すれば簡単にでき、まさにネットワーク時代の情報セキュリティなのです。

(2) PC端末にファイルを残さない方法

さて、ネットワークを使用してファイルをユーザーに持たせない方法は、一般的にはクライアント・サーバー方式と言われる方法を応用することで可能です。クライアント・サーバーとは、ユーザーの端末をクライアントと呼び、クライアント端末はサーバーと呼ばれる親機にネットワークで接続する形態です。実はクライアント・サーバーは既に20年以上も運用されていて、実に多くの形態があり、日々進歩しています。例えばインターネットでは、情報を見るウェブ・ブラウザがクライアントであり、ウェブ・サーバーにある情報を探してユーザーに見せます。インターネットのメールも全く同じ仕組みです。PC内にあるメーリングソフトがクライアントであり、メーリングソフトはメールサーバーにある自分宛のメールを探して表示できます。

PCはそれ自体がサーバーにもクライアントにもなるのですが、PCをクライアントとして使う場合、どんなことをすれば、ユーザーにファイルを持たせないようにできるのでしょうか。

その方法はシン・クライアント等いくつか方法がありますが、その中でも最も簡便に安価にできる方法は、インターネットの仕組み、すなわちウェブ・ブラウザとウェブ・サーバーを使うことです。

現在は技術が進み、ウェブ・サーバーが提供するワープロ等を用い、ウェブブラウザー上で文書を作成することや、エクセルに代表される表計算、パワーポイントに代表されるプレゼンテーション等は、ほぼ問題なく実施できるようになりました。（最近では、これらをクラウドコンピューティングと呼称しています。クラウドコンピューティングは前述のネットワーク・セントリック・コンピューティングの一形態と言うことができます。）

例えばウェブ・ブラウザー上のワープロソフトで文書を作ると、作った全てのファイルはウェブ・サーバー上に保管され、ユーザーPCのウェブ・ブラウザー上には何も残りません。これこそがユーザーにファイルを持たせない方法なのです。

しかし問題が残ります。普通のPCではウェブ・ブラウザー上の文書をユーザーが印刷したり、PCのハードディスクに、ユーザーの作ったファイルをダウンロードすることができるからです。そこでもう一工夫が必要です。

(3) 機能限定OSの活用

PCは、一般的にはOSと呼ばれる基本ソフトの上で動きます。近年このOSがどんどん便利になり、ファイルの管理等ほとんど全ての操作をOSだけで、できるようになりました。OSは肥大化し、便利になり過ぎた結果、情報セキュリティーの観点からは、

問題が多いのです。

そこでウェブ・ブラウザーを見る以外、何もできない機能限定OSを作り（Linuxというオープンソースをベースにした機能限定OSが、既に市販されています）、これを既存のPCにインストールします。この機能限定OSは、非常にコンパクトなのでUSBメモリーに格納することができます。従って既存のPCに機能限定版OSの入ったUSBメモリーを挿し、USBメモリーからPCを起動すれば、極めて安価にセキュリティー万全のクライアントが誕生します。またハードディスクは一切使用せず、ハードディスクの無いPC上でも問題なく作動します。さらに古い（CPUが遅く、メモリーも少ない）PCでも問題なく動きます。

また、ウェブ・サーバーも一工夫し、機能限定OSからでないとアクセスできないようにします。機能限定OSと、そのOSにしか対応しないウェブ・サーバーの組み合わせにより、PC端末にはファイルを残さないことが可能になります。

機能限定OSの入ったUSBメモリーには、指紋認証等の個人認証の他に、アクセスレベルが書き込まれ、ウェブ・サーバーの秘区分、need to knowの原則に従ってアクセスできる範囲が限定されます。これらより機密性、可用性は極めて高いレベルで担保できます。

なお、完全性については、PDF（Portable Document Format）化する等して、担保することができます。（PDFの説明は省略します）

(4) 機能限定OSによるクラウドコンピューティングのメリット、デメリット

機能限定OSを使い、ウェブ・ブラウザーでほとんどの業務をする上での、メリット・デメリットをまとめてみます。

ア．メリット

・既存のPCがそのまま使え、極めて少ない投資で情報セキュリティを担保できる。
・ユーザーは煩雑なファイルの管理業務から開放される。
・機能制限OSの入ったUSBはどのPCに挿しても良い。（出張先でも使える）
・クライアントにセキュリティーソフトは全く必要としない。
・ウェブ・メールやチャット機能が使える。
・古いPCでも全く問題ない。（PCを更新する必要がない）
・将来的には、各種システムの端末になり得る。
・PC端末にアプリケーションソフトを購入する必要がなく、大幅なコスト低減ができる。

イ．デメリット

・PCがネットワークに接続されていなければ使えない。
・ウェブ上で動く市販のアプリケーションは現在のところ限られる。（将来性大）
・必要なウェブ・サーバー数、回線品質の影響等未だ未知数の部分がある。
・ウェブ・サーバーの管理が必要になる。
・ファイルの取り出し、印刷等は管理サーバーでしか実施できない。（不便）
・機能限定OSの入ったUSBメモリーをユーザー毎にカスタマイズする必要がある。
・機能限定OSの入ったUSBメモリーを厳格に管理する必要がある。

おわりに

ネットワーク時代における情報セキュリティとは、単にセキュリティソフトを導入するとともに、管理態勢を強化し、従事者のモラルを高めれば担保できるといった、単純なものではありません。防衛省自衛隊のように特に高度な情報セキュリティが求められる組織は、今後かなり思い切った投資と、考え方の抜本的な見直しが求められています。

機能限定OSを用いたクラウドコンピューティングは、今すぐに実現可能な解決策の一つであるだけでなく、ネットワーク時代にふさわしい情報共有のあり方、さらにはそこから生じるであろう、知識、知恵の充実にも貢献するものと信じています。

（とうごうゆきのり　幹候25）