平成１６年（ワ）第１６７０２号　損害賠償請求事件（第１事件）

原　告　○○○○ 外１１８名

被　告　西東京市

平成１７年（ワ）第１０４９２号　損害賠償請求事件（第２事件）

原　告　○○○○ 外４名

被　告　西東京市

準　備　書　面　(10)

平成１８年5月２６日

東京地方裁判所　民事第７部　合B通係　御中

原告ら訴訟代理人弁護士　清　水　勉

弁護士　増　田　利　昭

弁護士　鈴　木　雅　人

弁護士　佐　渡　島　啓

弁護士　冨　田　千　鶴

弁護士　関　口　正　人

弁護士　結　城　大　輔

1　はじめに

原告らは，平成 18 年 4 月 17 日付準備書面（9）15 頁において，被告が住基法 36 条の 2 の「適切な管理のために必要な措置」を果たしていないことの一例として，近年頻発している Winny による情報漏えい事件（甲 44 の 1～2）を摘示したが，同様な義務を定める，西東京市個人情報保護条例（1 条 1 項，3 条，9 条 1 項(2)等）の問題でもある。

2　問題の所在

ファイル共有ソフト Winny により住基ネット関連情報が流出していることが報道されているが，このことは物理的環境としての住基ネットのネットワークシステムそのものに欠陥があるということではない。なお，被告が住基ネットの“内側”“外側”という区別をどれほど重視しているかわからないが，ここでは総務省の考え方によることにする。すなわち，改正住基法によって新たに設定された住基ネットシステムの範囲内が住基ネットであり（“内側”），市町村の既存住基システムは住基ネットの“外側”に位置する。

このような区別をし，物理的環境としての住基ネットのネットワークシステムそのものに欠陥がないとしても，住基ネットの“外側”にある住基ネット管理マニュアルやパスワードなどの住基ネット関連情報が Winny によりインターネット上に流出していたという事実が存在することも確かである。

このような状況を，「住基ネットの欠陥ではない」「本人確認情報が流出したのではない」として無視することもひとつの考え方ではある。

しかし，本人確認情報はもともと既存住基システムで作成保管されているもので，それが住基 CS に送信されるという関係にあるから，既存住基システムは住基 CS と同等の重要性を有するものである。厳しい管理マニ

ュアルを作ったり（すべての自治体が実行できているかどうかは甚だ疑問。），VPN で送信したり，多額のセキュリティ費用をかけたりしているのは，本人確認情報を確実に守ることの重要性を自覚しているからではないか。そうであれば，住基ネットシステムそのものの欠陥ではないとしても，同様に重要な問題として対応を考え実行しなければならない。

3　人的要因

情報漏えいの原因の 90%以上は，不正アクセス，セキュリティホールなどのコンピュータ技術に関係する要因（テクニカルファクター，技術的要因）ではなく，紛失，盗難，漏えい流出等の人的要因（ヒューマンファクター，被技術的要因）によるものであると言われている（甲 50）。

最近の主な Winny による情報漏えい事件については，別表にあるように，いずれも職員等が業務に使用していた私用パソコンから，Winny を通じて外部に漏えい流出したものばかりである。

このような事態を引き起こさないようにするには，個々の職員が情報の保守管理を徹底すればよいはずだと，だれもが考える。技術基準やセキュリティポリシーを定め，悪質な行為については重い罰則を課すことにすれば，職員は自覚と規律を持って情報の処理・管理にあたるのであり，人的要因による情報漏えいなど一掃されるはずであるとも考える。

しかし，ひとりひとりの公務員は，様々な性格を有し，様々な事情を抱える「人間」である。だれもが常に基準どおりに行動するとは限らない。公金の不正経理や公共事業に関する談合など犯罪行為であることがわかり切っていながら，国の行政機関でも地方自治体でも全国的に蔓延してきた（いる）ことは，日本社会に生活する者にとって公知の事実である。

職場で業務資料の持ち出しを禁止されていても，どうしても明日の朝までに仕上げなければならない仕事など業務遂行のために必要であれば，自

宅に業務データを持ち帰って使用してしまう（別表の８）。業務のために必要であれば，捜査書類や自衛隊の有事演習計画などの極秘扱いの情報でも，私用パソコンで使用したり，自宅のパソコンで処理したりしてしまう（別表の 1～3，5，9～10，15）。警察庁は，警視庁・道府県警察本部を通じて，全国の警察官に私用パソコンを捜査業務に使用することを禁止する旨告知し，各警察官に念書を書かせているようであるが，このような手法で現場の状況が一変するものか，甚だ疑問である。実際には，一度禁止されたからといって，私用パソコンでの業務資料の使用等を必ず止めるというものではないのである（別表の 6 と 11，13）。

4　Winny 問題

以上の基本的な視点を踏まえて，Winny の仕組みや情報漏えいの仕組みと危険性，情報漏えい対策等について論ずる。

(1)　ファイル共有システムについて

インターネットなどのコンピューターネットワークにおいて，個々のパソコン端末間でファイルを共有する方式としては，①クライアント／サーバー型と，②ピアツーピア（P2P）型の 2 種類がある。クライアント／サーバー型は，専用サーバーがファイルを一元的に管理し，個々の端末はサーバーを介してファイルを共有するものであり，いわば「１対 n 型」の中央集中型システムである。インターネット上の Web サイト（ホームページ）などがその例である。他方，ピアツーピア型は，専用サーバーは不要で，同一のネットワークに接続した個々のパソコン端末同士が，対等な立場でファイルをやりとりするものであり，いわば「1 対 1 型」の分散型システムである（甲 48・75 頁）

(2)　Winny のしくみと特徴

ア　Winny の構成

Winny は，次のように 3 つの構成要素から成る（甲 49・24 頁）。

① Winny 本体プログラム（Winny.exe）

Windows 用アプリケーションであり，キーの検索，ファイル転送等の各種機能を実行する。

② 設定ファイル

基本設定や起動時に接続しに行く相手のリストなどを記述したファイル。

③ ファイル共有用フォルダ

以下の 3 種類のフォルダよりなる。

Ⅰ キャッシュ・フォルダ（¥Cache）

外部とのやりとりに使うキャッシュ・ファイルを格納するフォルダ。なお，Winny が実際に通信相手とやりとりするのは，キャッシュ・フォルダから出し入れするキャッシュ・ファイルである。

Ⅱ ダウンロード・フォルダ（¥Down）

ダウンロードし終えたファイルをキャッシュ・ファイルから，実体ファイルに変換し，格納するフォルダ

Ⅲ アップロード・フォルダ（¥Up）

ファイルを公開するために使うフォルダ（ただし，初期状態では存在しない）

イ Winny のファイル共有方法

まず，Winny は，共有しようとする「元ファイル」から，ファイルの名前や存在場所などが書かれている「キー」と，元ファイルを暗号化して細かいブロックに分けた「キャッシュ・ファイル」の 2 つを作成する（甲 49・24 頁）。

次に，Winny は，ファイルを公開している「ノード」（Winny が稼働し

ている個々のパソコン)が,キーを定期的にネットワーク上に拡散させる。具体的には，ファイルを公開しているノードに対して，同じネットワークに接続している上流のノードから，検索リンクを通じて拡散要求（コマンド）が届くと，ファイルを公開しているノードはこの要求に対して自分の持っているキーを送る（なお，Winny においては，光ファイバーのような高速な回線により接続しているノードほど「上流」となり，その「下流」に他の低速なノードがぶら下がる格好となる)。このため，ある特定のファイルを持っているノードが 1 台であっても，そこにファイルがあるという情報は，より上流方向にある多数のノードが持つことになる。他方，ファイルを探しているノード（検索元）からの検索要求も，同様に，上流方向に流れることになる。そのため，特定のキーと，それに対応する検索要求が上流で合致し，ファイルの存在場所等が当該ネットワーク上で明らかとなる（甲 49・25～26 頁）

キーにはファイルの持ち主のアドレスが書かれているので，キーを受け取った検索元のノードは，持ち主に直接接続してファイルの転送を要求する（甲 49・25 頁)。

ウ　Winny の特徴（その１）－ファイル拡散のしくみ

Winny ネットワークでは，キャッシュ・ファイルの形でファイルをやりとりすることから，あるノードがダウンロードした後にキャッシュ・フォルダに残っているキャッシュ・ファイルも，元の実体ファイルと全く同じファイルとして取り扱われる。そのため，大元のファイル公開ノードが，当該ファイルを抹消なり公開停止したとしても，一旦，ネットワーク上の他のノードにダウンロードされたファイルは，Winny ネットワーク上に存在し続けることとなる（甲 48・77～78 頁，甲 49・26 頁)。

また，Winny のノードは，自分が持っているキーを他のノードに渡すときに，キーに含まれるファイルのアドレス情報を自分のものに書き換える

ことがある。書き換えの確率は，自分が持っているキャッシュ・ファイルの量に応じて高くなり，完全なコピーを持っている場合は 100%，全く持っていない場合でも 4%の確率でキーが書き換えられる。完全なコピーを持っていないノードがキーを書き換えた場合は，完全なファイルを持っている他のノードから足りない分（キャッシュ・ファイルの残りの断片）を取り寄せつつ，要求があったノードにファイルを中継する。このように，キーを書き換えたノードは，あたかもプロキシ（代理）・サーバーのように働くことになる（甲 49・26～27 頁）。

このため，時間が経つにつれ，ファイルのコピーが（キャッシュ・ファイルの形で）増殖するとともに，配布先を教えるキーの種類も増えることになる。キーが書き換えられると，大元のファイル公開ノードのアドレス情報も書き換えられるので，時間が経つほど判別し難くなる。そのため，一旦，Winny ネットワークに流れたファイルは，ネットワーク上に拡散するとともに，どこから流れたのか分からなくなるということになる。

エ　Winny の特徴（その２）－ポートを開かなくても外部のノード経由でファイルを公開できる

Winny は，LAN 内にあるノードから送られたキーに含まれる IP アドレスを外部のノードが書き換えるしくみを備えている。そのため，外部からのアクセスを受け付けないようにルーターのポートを開けていない場合でも（外部のポートを開けていない状態のノードを「Port0 ノード」という），当該 LAN と接続し，かつインターネットに直接つながっている他のノード（「RAW ノード」という）からの要求によってキーを Winny ネットワークに拡散し，他のノードからのファイル送信要求は RAW ノードを経由して受取り，Port0 ノードは要求ノードに対してリンクを張ってファイルを転送する（甲 49・27 頁）。

このようにして，一般的なサーバー・ソフトと異なり，Winny はポート

が開いていない状態でもファイルを公開することができる。

(3)　情報漏えいの元凶－暴露ウィルス

Winnyによる情報漏えい事件のほとんどは，Winnyが「暴露ウィルス」と言われるWinnyをターゲットとするウィルス・ソフトに感染することによって引き起こされている（甲48・76頁，甲49・33～35頁）。

したがって，ウィルス対策をきちんとしていれば，Winnyを使っていても，暴露ウィルスに感染して情報漏えいすることは十分に予防できる。

しかし，それでも暴露ウィルスに感染してしまうのは次のような理由による（甲48・78～79頁，甲49・30～32頁）。

① Winnyユーザーの目的はファイルをダウンロードして使うことにあるため，ウィルス感染への誘引が強い。

② Winnyで流れているファイルには，暴露ウィルスが含まれている可能性が高い。甲49・30頁によれば，約2700個のファイルに対して，800個以上がウィルスに感染していたということであるから，感染率は約3割となる。

③ 暴露ウィルスは，一見ウィルスには見えないように偽装しているため，間違えて感染してしまうことも多い。

とりわけ，上記①にあるように，Winnyユーザーはダウンロードしたファイルの使用に非常に関心が強いため，ウィルス対策ソフトの常駐を解除してしまうことが多い。ウィルス対策ソフトを常駐させたままだと，ウィルスが届く度に警告が出たり，ダウンロードしたファイルを削除してしまったりして，Winnyを円滑に使用することができなくなってしまうからである。そのような状況では，暴露ウィルスに感染してしまうことは，ある意味必然的ともいえるものである。

(4)　「Antinny」

なお，暴露ウィルスの代表は「Antinny」というウィルスであるが，こ

の Antinny タイプは 70 種類以上存在している。

また，最近では，Winny がなくても，感染すると勝手にパソコンの中身をインターネットに公開してしまうというウィルス（Winny 経由で拡大している「山田オルタナティブ」）なども現れており，ウィルスの進化・拡大も続いている。

5　問題解決の困難性

(1)　利便性に対する欲求と安心の落とし穴

別表に掲げた情報漏えい事件はいずれも暴露ウィルスによるものであり，当該公務員らが悪意を持って情報流出を意図して行なったものではない。好奇心や利便性に対する欲求が安全性確保のための障害の設定の必要という自制を凌駕してしまうことは，決して稀ではない。むしろ，好奇心や利便性こそが短期間のうちにコンピュータネットワークの驚異的発展の基盤であるとさえ言える。

また，自宅という最も信頼できる人たちだけが集まっている安心できる場におけるパソコンの管理がルーズになっているという，だれもが陥りそうな“落とし穴”がある。自宅で使用しているパソコンの場合，家族間で共用していなかったとしても，パスワードを設定していなかったり，設定していても家族同士で知っていたりすれば，共用の場合と同じリスク環境にあり，相互に信頼関係があるだけに，相互利用が絶対にできない環境を確保することは難しい。家族によって自分のパソコンがウィルス感染していることに気づかずに，昨日までずっと大丈夫だったという安心感から，職務上のデータを自宅のパソコンで扱ってしまうという行動をとる危険がないとは言えない。

(2)　個人データの流出と流出報道

実際に個人データ流出したということと，流出報道の有無は同じではな

い。報道機関はあらゆるデータ流出を把握しているわけではなく，取材できたものだけを報道しているに過ぎない。特定の自治体の本人確認情報がまとまったものとしてインターネット上に流出しているという報道はないが，それはそのような事実がないからかもしれないし，そのような事実があるのに報道機関に知られていないからかもしれない。

既存住基システム内における本人確認情報の流出はすでに報道されたことがあり（甲 17），個人の側からすれば，住基ネットの“内側”にあった本人確認情報か“外側”にあった本人確認情報かは関係がない。

6　住基ネットのセキュリティ対策に関する裁判例について

(1)　名古屋地裁平成 17 年 5 月 31 日判決（甲 11）

同判決は，プライバシー権侵害に対する措置として，住基法上の罰則（30 条の 35，30 条の 43，42 条，44 条）や禁止規定（30 条の 17，30 条の 29～30 条の 31，30 条の 33～35，30 条の 42，36 条の 2）や技術的水準の定めを引用し，これらの規程があることによってプライバシー侵害に対する対策は十分である旨説示する。

また，内部者等による漏えいの危険性については，そのような危険性はあらゆる制度に内在するものであり，住基ネットには具体的な情報漏えいの危険や損害の発生は認められないとし，市町村における実際の住基ネット運用状況は第三者への漏えい等が行われやすいという点については，市町村における実際の運用状況いかんによって被告ら（国，愛知県，LASDEC）の行為が違法となるものではないという形式論で排斥している。

しかし，上に述べたように，Winny による機密情報の漏えい事件は後を絶たない。しかも，その原因は，法律の条文や規則・基準などを定めておけば足りるというものではなく，あくまでも実際の個人情報の使用・管理等に携わる個々の職員の問題，すなわち人的要因である。

とすると，そもそも，法律の条文や規則・基準さえ定めておけば，情報漏えい等に対する措置としては必要かつ十分であるかのような上記判決の議論は，現実的ではない。情報漏えいが，紙に書かれた次元ではなく，現実の行政実務において生じ，社会問題化していることとは，極めて対照的なアプローチといえよう。そのため，内部者等による漏えいの危険性や市町村における実際の住基ネット運用状況については具体的な考察すらなされていないが，住基ネットのセキュリティ対策に対する判断としては，誤りである。

(2)　東京地裁平成 18 年 4 月 7 日判決（乙 21）について

同判決では，人的セキュリティ対策について検討しているが，操作の際に識別カードと暗証番号を要すること，一度に多くの本人確認情報の提供がされないように提供方法が限定されているといった処理手順と，公務員の守秘義務，住基法条の罰則規定の定め等をもって，本人確認情報の漏えい，改ざんなどを防止するための相応の措置と評価できるとしている。

しかし，上に述べたように，現実には，公務員の守秘義務等の罰則規定があっても，当該職員は Winny でファイルをダウンロードして使用するという個人的な嗜好の方を優先し，安易に，私用とはいえ，機密情報を保存しているパソコンのウィルス対策ソフトの常駐すら解除してしまうことが日常的に繰り返されているのが現状である。

かかる現実を前提にすれば，処理手順の定めや罰則規定が，本人確認情報の漏えい等を防止するための，現実的な，相応の措置になっていないことは明らかである。

(3)　名古屋地裁平成 18 年 4 月 28 日判決（乙 13）

同判決は，担当職員に対する教育・研修，住基法条の刑罰規定，照会条件の限定・広域交付の制限，アクセスログの解析と調査等によれば，情報漏えいの可能性が高いとはいえないとする。

しかし，以上に述べたように，現実の情報漏えい事案からすれば，現実的に有効な情報漏えい対策とはなっていないことは明らかである。

7　結　論

人的要因による情報漏えいは，単に法律の条文で罰則を定めたり，処理手順等を定めたりするだけでは，ほとんど抑止力たり得ないのが現状である。

情報漏えい事案では，たとえ法律等で禁止されていようが，自分がどれだけ機密を要する情報を保持していようが，Winny ネットワークに流通しているファイルをダウンロードして使用するという個人的な趣味・嗜好が優先され，その結果，一般的なウィルス対策ソフトの常駐すら解除してしまう。もちろん，裁判のような公式な場で，冷静に判断すれば，そのような情報漏えいをした公務員の行動は，あまりにも軽率かつ非合理的と判断することはたやすい。しかし，これまでの情報漏えい事案を見れば明らかなように，そのような情報漏えいに至る職員個人がとりわけ特殊な人間というわけではない。また，その職場を見ても，自衛隊，警察，消防署，裁判所，自治体等，機密情報やセンシティブ情報を数多く取扱い，また，従来からも情報の取扱にはとりわけ慎重かつ厳格な組織ばかりである。

とすれば，住基法 36 条の 2 等で要請されている「適切な管理のために必要な措置」についても，法律の条文や処理手順・規則等で定めたから情報漏えいの危険性は高くないということではなく，そのような定めがあってもなお情報漏えいの危険性はなくならないということを前提にした措置を講じる必要がある。

このような観点から現行の住基ネットを見ると，情報漏えいが生じないようにするための規定は数多く存するとしても，住基ネットに関する限りでさえ，全国の自治体において実効性が十分に確保されているといえるか

どうか，甚だ疑問である。ましてや既存住基システムと連動していることをからすれば，尚更のこと，本人確認情報の保護として十分な実態になっているとは到底言えない。

以上