平成17年11月11日判決言渡　同日原本交付　裁判所書記官
平成17年(ネ)第214号　損害賠償請求控訴事件（原審・札幌地方裁判所平成16年(ワ)第1231号）
口頭弁論終結日　平成17年9月21日

判　　決

主　　文

1　原判決中控訴人敗訴部分を取り消す。
2　被控訴人の請求を棄却する。
3　訴訟費用は，第1，第2審を通じ，被控訴人の負担とする。

事実及び理由

第1　控訴の趣旨
　主文と同旨
第2　事案の概要
1　本件は，被控訴人を被疑者とする捜査情報が，控訴人に所属する警察官の私有パソコンからインターネットを通じて外部に流出したこと（以下「本件情報流出」という。）は，当該警察官の職務行為にかかる不法行為，平成13年以降の北海道警察本部長（以下「道警本部長」という。）が捜査用のパソコン導入を怠って私有パソコンの利用を禁止してこなかったという不作為の不法行為又は当該警察官の所属する警察署長及び管理担当者が情報流出を防止すべき管理義務に違反したという不法行為を選択的に主張する被控訴人が，控訴人に対し，国家賠償法（以下「国賠法」という。）1条1項に基づき，被控訴人の被った精神的損害の賠償として200万円及びこれに対する不法行為の後であり，訴状送達の日の翌日である平成16年6月16日から支払済みまで年5分の割合による金員の支払を求めたところ，原審が，当該警察官の職務行為にかかる不法行為責任を認め，控訴人に対し，40万円及びその遅延損害金の支払を命じる限度でこれを認容したため，控訴人が控訴をした事案である。
2　事実及び争点（当事者の主張）は，以下のとおり改めるほか，原判決書「事実及び理由」欄の「第2　事案の概要」の「2　争いのない事実並びに後掲証拠及び弁論の全趣旨によって明らかに認められる事実」（以下「争いのない事実等」という。），「3　争点及び当事者の主張」記載のとおりであるから，これを引用する。
(1) 原判決書4頁24行目の冒頭に「ア　」を挿入する。
(2) 原判決書5頁8行目の「影響はない。」の次に
「また，A巡査が，本件捜査情報を本件パソコンのハードディスクへ保存し，自宅に持ち帰る，インターネットに接続するなどの行為は，一般的なノートパソコンの利用形態であり，ノートパソコンを職務に利用する以上，客観的・外形的に職務行為となり，ましてやアイコン（パソコン画面上に表示されるファイルや機器，機能などを表す小さな絵で，これをクリックすることでソフトの起動やファイルを開いたりする操作が直接的に行えるもの。）を作成していたのであり，警察署や派出所以外の場所で実際に職務を行う可能性を帯びていたのであるから，このようなパソコンを起動させること自体が『職務を行うについて』のものであると認定できる。
イ　A巡査には，本件パソコンをインターネットに接続することによって，本件情報流出の予見可能性があったといえる。
　すなわち，平成15年においても，不正なプログラムを忍ばせた悪意のウエブサイトを訪問したり，電子メールを開いたりして閲覧すると，不正なプログラムが実行されてしまうことが新聞記事（2件）で紹介され，総務省，経済産業省，警察庁などが，インターネット接続によるウイルス感染とそれによる情報流出の危険性を広く利用者に呼びかける記事が出ており，平成16年にも7件の同種記事があるから，パソコンを利用し，かつインターネットに接続する者は，だれでも，いつでも，新手のウイルスによる情報流出の危険性を負っている。また，専用ネットワークやファイアウォー

ル（外部からの攻撃に対する障壁）の利用により，情報流出の防止ができるとされた住民基本台帳ネットワークシステム（以下「住基ネット」という。）を巡り，住基ネットがインターネットに接続されているパソコンとLAN（庁内情報通信網）で接続されていれば，そこからウイルスに感染することが判明し，情報が流出する危険性があることが認識されていた。さらに，A巡査は，北海道警察において，情報管理の講義を受けており，それなりの知識を持っていたほか，ウイルス感染を防止するため，出所不明のソフトウエアは利用しないという知識はあったはずである。

こうした状況の下で，A巡査は，インターネットに接続し，ウイニーを起動し，ウイルスに感染している可能性のある見知らぬファイルが勝手にたまることを容認し，ウイルスに感染したファイルを開き，本件情報流出を招いたのであるから，本件情報流出につき予見可能性があったといえる。

控訴人は，ウイルスの種類について，アンティニーには種類があり，本件情報流出にかかる「Antinny．G」（以下「アンティニーG」という。）の発見が，本件情報流出の直前であるとするが，アンティニー関係のウイルスの存在は，インターネットのウイルス情報で容易に知りうるのであるから，雑誌等に載っていないことで，一般人が知り得なかったとすることはできない。

ウ　A巡査は，個人情報を扱う本件パソコンをインターネットに接続しないという極めて簡単な方法により，結果を回避することができた。

控訴人は，A巡査がウイルス駆除システムを利用していたとするが，次々と新種のウイルスが登場している以上，完璧なウイルス駆除システムはあり得ず，そのことで予見可能性も結果回避可能性もないとはいえない。

また，A巡査は，出所不明のファイルを開きさえしなければ，結果を回避できたのである。

以上から，A巡査には，結果回避可能性があったといえる。

エ　控訴人は，A巡査の行為と本件情報流出には，相当因果関係がないとし，確かに，事象を見れば偶然が重なったといえるとしても，A巡査が本件捜査情報を私有パソコンである本件パソコンに保存した上，本件パソコンをインターネットに接続し，いつでも，また，不正アクセスやウイルスなど，どのような形態においても，本件情報流出の可能性のある状態を作り上げた以上，本件情報流出は必然的結果であって，相当因果関係があることは明らかである。」

を加入する。

(3) 原判決書5頁18行目の次に，行を改めて

「　すなわち，A巡査が本件パソコンを利用して公文書を作成することは職務行為といえようが，これはパソコンをいわば筆記用具として利用したにすぎない。一方，公務に供しているパソコンを自宅に持ち帰り，文書等を作成することはもちろん，ゲームに興じたり，私的興味を満たすためこれをインターネットに接続することは，社会通念的に見ても，原則としてそれ自体が独立した私的行為であると推定するのが相当であって，公務の延長であるとの特段の事情がない限り，客観的外形的に見ても，職務行為であると解すべき合理的根拠はない。現時点における私的用途におけるパソコンの利用は，既に，一般的，普遍的といえる程度にまで一般家庭においても普及しており，自宅における私的パソコンの操作が，公権力の行使である職務執行であるとか，会社員としての業務遂行行為であると解することは，異例かつ，不自然であり，そのように解する社会的基盤は全くない。

また，通達によって捜査情報の持ち出しを規制していることは，私的行為性を払拭させるものではない。」

を加入する。

(4) 原判決書5頁21行目の次に，行を改めて

「　本件パソコンは，A巡査の私有パソコンであり，公務に供したのち，自宅に

持ち帰ってインターネットに接続し，メール交信をしたり，専ら私的用途に利用する公務員は多数存在し，こうしたA巡査の私的な行為と本件情報流出との間の事実上の因果関係の全てを相当因果関係に該当するとすることは，国賠法1条1項の解釈を誤るものである。」

を加入する。

⑸ 原判決書5頁24行目の次に，行を改めて

「 すなわち，①インターネットを通じた情報の取得・交換や同回線を利用した電子メール通信によるコミュニケーションが全世界的に一般化・日常化している現状において，インターネットへの接続自体に情報流出の危険性があるため，接続により情報が流出した場合，責任を負担させられるとすることは社会常識に反しており，適切な注意を払い情報流出への対処をしておけば，情報が流出しても許されると考えるべきであること，②本件情報流出が発生した当時，A巡査は，パソコンについての一定の知識を持ち，ウイルス対策ソフトを導入しかつ常時稼働させ，ウイルス定義を適宜更新するとともに，インターネットのプロバイダーがサービスとして実施しているウイルス駆除システムを併用して対策を講じていたこと，③アンティニーGは，それまで理解されていたウイニーを媒介として自己の感染を拡大する単純な自己増殖型のウイルスとは異なり，パソコン内のファイルを外部に流出させる機能を持つウイルスであるが，その発見は遅くとも平成16年3月24日ころであり，同ウイルスの記事が日本語で掲載され始めたのが，同月29日ころからであって，A巡査を始め，一般ユーザーは，同日の京都府警からの情報流出の記事が全国に配信されることにより初めて同ウイルスの存在を知り得たものであるうえ，ユーザーにより実際の対策が取られるまでにはさらに時間的経過が必要であり，それまではウイルス対策ソフトに頼らざるを得ず，予見可能性の判断の基準時は本件捜査情報が保存された時点と考え，その時点までの通常人をして収集し得た資料を総合し，個人差も考慮した上，経験則，論理則に照らして予見可能性の有無を判断すべきところ，本件捜査情報が本件パソコンに保存された時点では，アンティニーGの存在やその対処法が，一般通常人の認識できる新聞や雑誌等ではなく，専門業者のホームページ上に掲載されたのみであったこと等からすると，A巡査には，本件情報流出につき予見可能性がないというべきである。」

を加入する。

第3 当裁判所の判断

1 本件情報流出に至る経緯については，原判決書「事実及び理由」欄の「第3 当裁判所の判断」の1⑴記載のとおりであるからこれを引用する。

2 争点⑴（A巡査の行為が国賠法1条1項の対象となるか）について

まず，A巡査の行為の「職務行為性」について検討する。

被控訴人は，A巡査の本件パソコンを利用する行為が，捜査関係書類を作成するのと同様の利用形態であるから，本件パソコンが公務に利用されている以上，そのパソコンの利用は職務行為そのものであると主張する。

確かに，本件パソコンは警察官であるA巡査が，私有物をその職務である捜査関係書類の作成に利用しているものであることは争いがないが，その利用形態は，一般人が通常パソコンを利用する形態と何ら異ならないことは被控訴人も認めるところである。

ところで，国賠法1条1項における「職務を行う」とは，職務行為自体又はこれと関連して一体不可分の関係にある行為，及び職務行為と牽連関係があり，客観的外形的に見て社会通念上職務の範囲に属するとみられる行為をいうと解されるところ，当該公務員の行為が職務行為の場合はもちろん，そうでない場合であっても，職務の内容と密接に関連し，又は職務行為に付随してなされる行為も国賠法1条1項における職務行為に含まれ，一般的外形的に見た場合に，社会通念上職務の範囲に属すると見られる場合には同項の適用がある。これを本件について見ると，A巡査の行為が警察署や派出所内で行わ

れている限りにおいては，そのパソコンの利用は，捜査関係書類の作成という点で職務行為に該当するというべきであるが，一方，自宅において，インターネットに接続するなどしてパソコンを利用することは，公務員であると私人であるとにかかわらず，車の運転などと同様にだれもが行っている行為であり，そのこと自体は，通常は職務とは無関係の行為であるというべきであるから，A巡査が，自宅でパソコンを利用することは，一般的には，外形的に見ても，社会通念上，警察官の職務の範囲に属するということはできない。

そして，A巡査が，本件情報流出に当たり，職務上本件パソコンを利用していたとする主張・立証はないから，A巡査は，職務行為としても，外形的に職務の範囲に属する行為としても，本件パソコンを利用したということはできない。

さらに，本件パソコンに本件捜査情報が保存されていたことによっても，A巡査の本件パソコンの利用の私的行為性に影響を与えるとはいえない。

よって，その余の点を検討するまでもなく，A巡査の原因行為が，国賠法1条1項に該当するとはいえないから，被控訴人の主張は理由がない。

3　争点(2)（道警本部長等による行為が国賠法1条1項の対象となるか）について

(1)　被控訴人は，歴代の道警本部長が各警察官に捜査用パソコンの配備をせず私有パソコンの使用を禁じてこなかったことをもって不作為の不法行為であると主張する。

しかし，捜査用のパソコンを各警察官に配備することは，予算上の制約などからして困難であり（弁論の全趣旨），私有パソコンの使用を禁じるべき法的根拠もないから，この点に関する被控訴人の主張は採用できない。

(2)　また，被控訴人は，江別警察署長及び管理担当者（以下「管理担当者等」という。）が，本件パソコンを管理するについて，情報の流出を防止すべき管理義務違反があったと主張する。

ア　この点，控訴人は，管理については十分な対策を講じ，本件通達に基づき点検確認を行っているから，管理義務違反はないと反論するが，A巡査は，本件通達により，本来，私有パソコンを自宅に持ち帰る際には，公務に関する情報が残されていないことの確認を管理担当者等から受ける必要があることを認識していながら，管理担当者等のチェックを受けないまま本件パソコンを自宅に持ち帰ったことが認められるのであり（乙5，証人A），本件通達の徹底がなされておらず，捜査情報の持ち出し防止について確実な実施が行われていなかったことが認められるから，管理担当者等には，管理につき，不備があったというべきである。

イ　そこで，本件情報流出の予見可能性について検討する。

これまで認定した事実に加え，後掲の証拠及び弁論の全趣旨によれば，以下の事実を認めることができる。

（ア）　A巡査は，本件パソコンを平成15年5月初旬に購入し，職務に使用することの許可を得て，ウイルス駆除ソフトを導入し，インターネットプロバイダーのウイルス駆除サービスも利用したことがあった。（乙1，乙5，証人A）

（イ）　本件捜査情報は，遅くとも平成16年3月27日までに，A巡査により本件パソコンに保存された。（争いのない事実等(2)）

（ウ）　A巡査は，平成16年3月28日，本件パソコンを自宅に持ち帰った。（証人A）

（エ）　A巡査は，自宅でウイニーを利用していたところ，本件パソコンは，アンティニーGというウイルスソフトに感染した。ところで，アンティニーGの存在は，平成16年3月23日ころ発表されたのであり，同日から同月29日ころまでに，ウイルス対策を講じる会社のサイト等において，アンティニーGについての対策方法が紹介されるとともに，同日中に京都府警において個人情報が含まれた捜査書類がインターネットで漏洩したとの記事が，新聞に掲載された。（乙13の1・2，乙19の1から3まで・5，乙20の1・2，証人A）

（オ）A巡査は，本件パソコンが，それまでの自己増殖型とは異なり，情報流出型のアンティニーGに感染していることを知らないまま，本件パソコンをインターネットに接続したことにより，アンティニーGの作用によって，デスクトップにあった本件捜査情報のアイコンのファイルが本件パソコンの公開用フォルダに自働的に作成されたことから，そのファイルにより，本件捜査情報を第三者が閲覧できる状態となり，遅くとも同月29日には，本件情報流出が発生した。（争いのない事実等(3)，乙5，乙15，証人A）

（カ）アンティニーGは，ウイニーのウイルスソフトであるが，その特質は，それまでのウイルス定義にはなかった，ウイニーの機能を利用する形で，パソコンのデスクトップ上の情報が，他者に開示・流出する機能を有するもので，これまで，認識されていなかった性質を有するものであった。（乙14の1，乙18，乙19の1から3・5）

ウ　被控訴人は，本件パソコンをインターネットに接続することによって本件情報流出の予見可能性があったと主張する。しかし，以上の事実によれば，本件情報流出は，A巡査が，本件パソコンを自宅に持ち帰り，インターネットに接続したことが原因ではあるものの，過失の前提となる予見可能性は，結果発生に対する抽象的な危険を予見するだけでは足りず，加害者の行為から一定の経緯をたどって結果が発生するという具体的危険を予見することが必要であるところ，①A巡査が本件パソコンを自宅に持ち帰った平成16年3月28日において，アンティニーGの出現が確認されてから5日程度しか経過していないこと，②アンティニーGが，それまでのウイルスとは異なり，パソコン内の情報が外部に開示・流出するという新たな特質を有すること，③アンティニーGについての情報は，ウイルス対策ソフトを扱う会社等一部のサイトに掲載されているにとどまっており，同月29日の京都府警における捜査情報の流出の新聞記事が出るまで，一般にはアンティニーGの内容が広まってはいなかったこと等を総合すると，管理担当者等において，本件捜査情報がインターネットを通じて外部に流出するという結果について，予見可能性があったということはできない。

よって，被控訴人の主張は採用できない。

エ　以上によれば，管理担当者等に，過失があったということはできない。

(3) よって，その余の点について判断するまでもなく，管理担当者等に対する国賠法1条1項の責任を追及する主張には理由がない。

4　以上によれば，被控訴人の本件請求は理由がないから，これを棄却するのが相当であり，これと異なる原判決を取り消した上で，主文のとおり判決する。

札幌高等裁判所第2民事部

裁判長裁判官　末永　進

裁判官　千葉和則

裁判官　杉浦徳宏