令和２年（ネ）第１０９号マイナンバー離脱等請求控訴事件

控訴人　　坊真彦　外

被控訴人　国

控訴審第４準備書面

２０２１年8月２５日

名古屋高等裁判所金沢支部　御中

控訴人ら訴訟代理人

弁護士　　岩　淵　正　明

第１　はじめに

控訴人らは，本書面において，新たに発生した特定個人情報の漏えい等の事故事例及びサイバー攻撃，サイバー犯罪の事例について主張する。

第２　新たに発生した事故事例

１　２０２１年１月１８日，丸紅パワー&インフラシステムズ株式会社は，ファイルサーバーに対する外部からの不正アクセスにより，同サーバー内のデータの一部が流出した可能性があることを明らかにした。

２０２０年７月３日，同サーバーにて異常が検知され，その後，調査を実施した結果，同年６月３０日頃より，外部から不正アクセスされた痕跡が発見され，同サーバーに保管されていたデータの一部が流出した可能性があることが判明した（甲５４）。

同サーバーには，１３２名の特定個人情報をはじめとする個人情報が保管されており，これらが流出した可能性があるということになる（甲５４）。

そして，１０１人分以上の特定個人情報が流出していること，同社が同年７月３１日，１０月１日に個人情報保護委員会へ報告を行っていることからすれば，この事故は「重大な事態」（番号法２９条の４）に該当する。

２　２０２１年２月４日，東京都世田谷区は，個人番号カードの更新時において，申請者から従前のカードについて返還希望があったため，ＩＣチップに穿孔処理を行い，

本人限定受取郵便で更新カードとともに申請者へ送付したところ，別人に誤送付した（甲５５）。

原因は，通常の個人番号カードの封入と作業工程が異なったため，職員が誤って封入したことにあるとされている。

３　２０２１年2月１６日，公益財団法人前橋市まちづくり公社は，７３２名分の個人番号を含む個人情報をＵＳＢメモリに保存していたところ，同ＵＳＢメモリを紛失する事故を発生させた（甲５６）。

そして，１０１人分以上の特定個人情報が流出していること，同公社が同年７月３１日，１０月１日に個人情報保護委員会へ報告を行っていることからすれば，この事故は「重大な事態」（番号法２９条の４）に該当する。

４　２０２１年3月２日，佐賀市は，同市ホームページにおいて，問い合わせ等の際に添付された個人情報を含む画像データがインターネット上で閲覧可能な状態になっていたことを明らかにした（甲５７）。その画像データのうち，１２３件については個人番号カード・同通知カードの画像データが含まれるものであった。

原因は，メール送信フォームへの機能追加の際，受託者に対して画像データの保存フォルダへの第三者からのアクセスを制限するよう指示をしていたが，適切に処理されていなかったこと，指示した処理が適切に実施されているかどうかの確認ができていなかったことにあるとされている。

５　２０２１年3月１９日，宝ホールディングス株式会社は，同社の新給与システム導入に伴うマイナンバーデータの移行作業を行っていたところ，同社担当者がダミーデータのエクセルファイルを作成する際に，マイナンバーの本データのファイルを使用し加工したことで，残っていた本データのシートを削除し忘れたまま外部の給与システム開発業者に誤送信して，４１６７人分の特定個人情報が漏えいする事故が発生した（甲５８）。

６　２０２１年4月２０日，佐賀市は，市民生活課の会計年度任用職員が，家族の個人番号カードを受け取りに来た女性に対し誤って別人のカードを渡してしまったこと

を明らかにした（甲５９）。同カードには１０歳未満の男児１人の個人番号，住所，名前，生年月日，性別，顔写真が掲載されていた。

保管庫には複数のカードが置いてあり，個人番号カードを受け取りに来た女性が持参した交付通知書との照合が不十分であったことが原因とされている。

7　小括

(1)　上記の１の事故事例は，外部からの不正アクセスにより特定個人情報が大量漏えいした事故であり，番号法上の「重大な事態」にも該当する重大事故である。

この事故は，民間企業が管理している特定個人情報について，番号法１２条の安全管理措置及び特定個人情報の適正な取扱いに関するガイドラインに基づく管理措置を課しても不正アクセスによる特定個人情報の不正取得を防ぐことができなかったものであるから，まさに制度上の欠陥による重大事故にほかならない。

また，この事故は，不正アクセスにより特定個人情報を含む個人情報が狙われたものであるから，特定個人情報に高い価値が見出されていたことを示すものであるとともに，不審なメール，連絡が入ることを想定していることからも，二次被害，三次被害をもたらすおそれは十分にある。

そして，被控訴人によれば，外部からの不正アクセスによる特定個人情報の取得は，刑罰の対象となり，罰則を設けることで個人番号や特定個人情報の適正な利用等を担保しているということであった。

しかし，この事故事例により，罰則を設けることで特定個人情報の適正な利用等が担保されておらず，厳重な罰則が不正アクセス等の抑止になっていないということが改めて明らかとなったのである。

また，この事故事例に対し，報告を受けた個人情報保護委員会（以下「委員会」という。）は，どのように対応して，どのような権限行使をしたのか，どのようにして特定個人情報の適法，適正な取扱いを担保したのかも明らかとなっておらず，その証拠もない。本来であれば，委員会は，このような重大事故については，公表して国民に対して注意喚起等をすべきであるところ，委員会がそのような対応

をしたという証拠はない。

したがって，やはり委員会は機能不全に陥っているのである。

このように，もはや被控訴人の反論が破綻していることは明らかである。

(2) 上記２，３，４，５，６の各事故事例は，個人番号カードを誤送付，誤交付した，特定個人情報を誤送信した，紛失した，管理端末の不具合により個人番号カードの発行事務等が滞留した，というものであり，従前から同様の事故が多発していて，全く改善の見込みがない。しかも，現行の番号法上，後を絶たない同様の事故事例を防ぐことができる仕組み，システムもないから，もはや法制度上の不備，制度上の欠陥により，特定個人情報の漏えい事故が止められない状態になっているといわざるを得ない。

また，これらの各事故事例に対し，委員会は，どのように対応して，どのような権限行使をして，特定個人情報の適法，適正な取扱いを担保しているのかも明らかとなっておらず，やはり委員会は機能不全に陥っているのである。

(3) 上記４の事故事例は，個人番号カード，同通知カードの画像を含む画像データが佐賀市ホームページにおいて，閲覧可能な状態となっていた事故であり，個人番号カード，同通知カードが誤送付，誤交付されて特定個人情報が漏えいしたに等しいものである。

画像へのアクセスは，全て情報提供者のアクセスであるとされているが（甲５７），少なくとも上記画像データに映っている個人情報が流出して悪用される可能性があることは否定できない。だからこそ，佐賀市は，「市役所職員を騙る不審電話にお気をつけください」と注意喚起しているのである。

この事故事例に対しても，委員会は，どのように対応して，どのような権限行使をして，特定個人情報の適法，適正な取扱いを担保しているのかも明らかとなっておらず，やはり委員会は機能不全に陥っているのである。

第３　令和２年中に発生したサイバー攻撃，サイバー犯罪の事例

１　控訴人は控訴理由書において，原判決が人為的ミスと故意の不正行為を同列に論

じていることには明らかな誤りがあると主張し，「故意の不正行為の場合は，その目的いかんによっては，例えば個人情報取得の目的による防御システムの突破などによる番号制度自体の悪用もありうる。」と主張した。

しかして，令和２年度において故意によるサイバー攻撃・サイバー犯罪が以下の通り多発していることが明らかとなった。（甲６０・１４～７頁，甲６１）

(1) 防御関連企業に対するサイバー攻撃

三菱電機は，１月にはサイバー攻撃を受け情報が外部に流出した可能性があることを，２月には流出した可能性のある情報には防御関連情報が含まれていたことをそれぞれ公表した。さらに11月，同企業は再びサイバー攻撃を受け，国内取引先の金融機関口座に関する情報が流出したと発表した。このサイバー攻撃は，１月及び２月に公表したサイバー攻撃とは異なる手口が用いられた可能性が高いとしている。

(2) 電気通信事業者に対するサイバー攻撃

５月，ＮＴＴコミュニケーションズは，海外拠点への侵入をきっかけとした国内のサーバーに対する不正アクセスにより，一部の情報が社外に流出した可能性があることを発表した。さらに７月，同社はリモートアクセスを 利用したＢＹＯＤ末を経由した不正アクセスにより，社内ファイルが閲覧された可能性があることを発表した。

(3) 企業等を対象としたランサムウェア感染事案

11月，カプコンがランサムウェアに感染し，同企業が保有する個人情報等が窃取されて暗号化された上，当該情報を公開しないことと引き換えに取引に応じるように脅迫を受ける二重恐喝とみられるランサムウェア感染事案が発生した。

(4) スマートフォン決済サービスに係る不正振替事犯

９月，事業者が提供するスマートフォン決済サービスに関して，同社と業務提携する金融機関に開設された口座情報を不正に入手・連携し，不正な振替（チャージ）を行う事案が確認された。

(5) データＳＩＭカードを利用したＳＭＳ認証代行事案

２月，本人確認が行われていないＳＭＳ機能付きのデータＳＩＭカードを利用し，他人にＩＰ電話アプリのアカウント作成時に必要な電話番号及び認証コードを有償で提供し，利用者と異なる電話番号を登録させるＳＭＳ認証代行の事案が確認された。本件では，携帯電話番号や認証コードを提供するため，約 100 枚ものデータＳＩＭカードを悪用しており，これにより取得された電話番号の一部が，ＩＰ電話アプリを用いて特殊詐欺に悪用されていたことが確認されている。

(6) 金融機関の公式アプリを利用した不正出金事案

金融機関の公式アプリが不正に有効化された後，キャッシュカードを用いることなく，ＡＴＭでの出金が可能なアプリの機能を用いて，被害口座から現金が不正に出金されるという新たな手口が６月に 16 件，７月に 27 件発生しており，合計約 1,400 万円の被害が確認されている。

(7) 産業制御システムを標的としたプログラム

６月，工場の生産ライン等を制御するシステム（産業制御システム）を標的とするランサムウェアとみられるものについて，警察庁において，大規模産業型制御システム模擬装置を用いて解析を実施した結果，同不正プログラムは，攻撃対象と考えられる特定の企業の社内ネットワークのみで動作するように設計されているとみられることが確認された。

２　小括

(1) このように現に発生したサイバー攻撃やサイバー犯罪は，言うまでもなく特定の目的を持った意図的な違法な行為である。このようなサイバー攻撃などが，番号法のシステムに対しても実行される危険性は十分ありうると想定しなければならない。

原判決は，番号法の禁止規定や刑事罰などにより違法行為を防げるとするようであるが，前記の意図的な違法行為であるサイバー攻撃に対して何らの防御にならないことは明らかである。

(2) しかも，サイバー攻撃やサイバー犯罪の被害をこうむったこれらの企業では，当然防御システムがとられていたものである。とりわけ防衛関連情報を有する三菱電機(前記１(1))では他企業と比較しても一層強固な防御体制がとられていたことが想定される。にもかかわらず，防衛関連情報までサイバー攻撃により流出したとされているのであるから，番号法の防御システムの突破もあり得ると考えるべきである。この意味では原判決の個人情報漏えいは技術的に防御できるとの判断は誤りと言わざるを得ない。

第４　まとめ

以上のような新たに発生した特定個人情報の漏えいの事故事例，令和２年に発生したサイバー攻撃・サイバー犯罪の事例を検討すると，原判決の法制度上，システム技術上の不備があるとは認められないとの判断は明らかに誤りであって，この点からも原判決の破棄は免れない。

以上