総務市民委員会　会議録

＝＝

日　時　令和５年９月５日（火曜日）
　　午後１時開会　午後１時５４分閉会
場　所　第３委員会室

日　程
　１　開　会
　２　委員長挨拶
　３　協議事項
　　（１）本市職員の不正アクセス禁止法違反及び土浦市個人情報保護条例違反による事件送致について
　４　その他
　５　閉　会

出席委員（８名）

委員長	奥谷　崇
副委員長	目黒　英一
委　員	古沢　喜幸
委　員	篠塚　昌毅
委　員	小坂　博
委　員	滝田　賢治
委　員	菅井　歩美
委　員	栁澤　健二

説明のため出席した者（６名）

副市長	東郷　和男
市長公室長	船沢　一郎
総務部長	塚本　哲生
行革デジタル推進課長	元川　宏
総務課長	細野　賢司
人事課長	塚本　浩幸

事務局職員出席者
　主　査　　津久井　麻美子

　傍聴者（なし）

○奥谷委員長　ただ今から、総務市民委員会を開催いたします。早速、協議に入ります。協議事項（１）本市職員の不正アクセス禁止法違反及び土浦市個人情報保護条例違反による事件送致についてを議題といたします。この案件につきましては、本日の全員協議会において、執行部から全議員に対し説明がございましたが、所管の委員会として、なお詳細な事実確認をする必要があるとの御意見がありましたことから、本日委員会を開催するものでございます。ここで、副市長からひと言お願いいたします。

○東郷副市長　大変お忙しい中、委員会を開催いただきまして、誠にありがとうございました。また、説明させていただく機会を設けていただきまして、ありがとうございました。ただ今ありましたように、市職員によります不正アクセス禁止法違反、それから、個人情報保護条例違反による事件送致という事態を招いてしまったこと、議員の皆様、そして市民の皆様にまずもってお詫びを申し上げなければならないというふうに思っています。市の情報セキュリティの責任者として改めてお詫びを申し上げたいというふうに思います。先日、検察庁のほうに送致を受けまして、引き続き、検察官の取り調べに協力するということ。それから、処分につきましては、司法の判断を待って、厳正に対処したいというふうに考えてございます。その対応につきましては、すぐに対応したもの。それから、今後更なるセキュリティの強化、そして、システムの専門家を招いて、職員の研修と対策の強化を図るとともに、改めて職員に対して個人情報の適正な取扱いについて、再度徹底的に教育したいというふうに思っています。大変申し訳ありませんでした。

○奥谷委員長　それでは、執行部から説明を願います。

○船沢市長公室長　それでは、私のほうから説明させていただきます。資料が全員協議会と同じものになりますが、総務市民委員会フォルダ、令和５年、９月５日開催の資料、そちらのほうをお開き願います。職員の不祥事につきまして、御報告のほうをさせていただきます。本市職員につきましては、庁内ネットワークの不正アクセスによりまして、警察による捜査が行われておりましたが、御案内のとおり、９月１日に検察庁に送致となるということで報告をいただきましたので、皆様のほうに取り急ぎメールのほうで、同じ内容について御連絡させていただいた次第でございます。内容が分野横断的な内容になりますことから、私から資料に沿って補足説明を入れながら、御説明させていただきます。資料の冒頭部分から始めさせていただきます。市職員が庁内のネットワークに不正にアクセスいたしまして、保管する権限のないファイル、これは業務と関係のないファイルでございます。市職員につきましては、市のほうで情報セキュリティポリシーを定めてございまして、職務に関係のない情報につきましては、保有、取得ができないことになってございます。それにも関わらず、保管する権限のないファイル、市職員の個人情報を含むファイルでございますが、自身の業務用端末に保存してございました。これによりまして、不正アクセスの禁止法、それから、市の個人情報の保護条例違反の疑いで、９月１日付けで検察庁に書類送致されたものでございます。送致につきましては、手順といたしまして、事案が発生した時にまず警察のほうに相談いたしまして、警察のほうで事情聴取や捜査が行われます。次の段階といたしまして、検察庁のほうに送

致されまして、検察庁のほうで調べが入ります。その中で起訴、不起訴も含める形で司法的な判断がなされるという手続きがこれから始まるということになります。資料の冒頭でございますが、補足といたしまして、市のネットワークについて、全協のほうで一度御説明をさせていただきましたが、市のネットワークにつきまして、３系統のネットワークがございますということで御説明させていただきました。改めまして、御説明させていただきたいと思います。まず、庁内ネットワークというものがございます。これは、一般的にはグループウェアと呼ばれるものでございますが、職員間でネットワークを組んでございまして、３系統はハード的に分離されているものでございます。このグループウェアの中には、例えば、職員に対して業務連絡を行う時に、ここに掲示することによって、みんながその業務連絡を見ることができたり、職員間でのメールのやり取りといったものもグループウェアで行うことができます。また、職員が業務上必要となる書類なども作成いたしますので、その書類の中には業務として使用する市民の名前や住所などが入っている場合もございます。こういった形で使っているものが、庁内ネットワークでございます。二つ目、こちらがインターネット接続用の端末で、ハード的に分離してございます。それから、三つ目。こちらは、基幹系ネットワークと申しまして、住民基本台帳とか課税台帳といった情報を扱うネットワークでございまして、アクセスについては静脈認証というセキュリティ対策を行っているものでございます。このように三つの系統がある中で、今回のケースにつきましては、１番最初に申し上げました庁内ネットワークの中の情報の不正アクセスという案件でございます。中ほど、内容となってございます。職員につきましては、３１歳の男性職員。事由といたしましては、法と条例の二つの違反の疑いというものでございます。当該職員につきましては、平成３０年から令和４年１１月まで庁内のネットワークに不正にアクセスを行いまして、閲覧、保管する権限のないファイルを取得し、自身の業務用端末に保管しておりました。このファイルの一部には、市職員の個人情報が含まれておりました。内部職員からの報告がございまして、令和４年１１月に当該職員の端末を確認いたしましたところ、保管権限のない、職員の業務と関係のないファイルが保管されていることが確認されました。補足説明させていただきます。庁内のイントラネットにつきましては、職員が主に利用するフォルダとそれ以外に職員が見ることができない、表示されない非常用のバックアップフォルダというものがございます。今回のケースにつきましては、画面上に表示されない、見ることのできない、管理者権限なく、ロックなくファイルを開ける非常用のバックアップフォルダに不正にアクセスし、保管する権限のないファイルを取得したものでございます。表示されない非常用のバックアップフォルダにつきましては、その存在も含めまして職員には知らされていないものですが、当該職員につきましては、故意に、フォルダの所在を示す記号番号を類推し、直接入力する不正操作によりまして、保管が禁止されているデータを取得し、保管していたものでございます。また、資料の６行目に戻らせていただきます。また、当該職員からの聞き取りによりまして、私的端末にもフォイルを保存していたことが判明いたしました。以上を受けまして、警察に相談、捜査が済んだ結果、９月１日に検察庁へ送致されたものでございます。なお、ファイルの

一部には、市職員の個人情報のほか、市民の個人情報も含まれているものもございましたが、当該職員から外部への流出は確認されてございません。ここでも、補足説明のほうをさせていただきます。当該職員につきましては、本人の好奇心を満たす目的で、職員の個人情報の入手を考え、不正アクセスをして情報を入手し、閲覧を行っていたものでございます。この事態を受けまして、直ちにネットワークのセキュリティを強化する対応を行いました。職員に対しては、これまでも個人情報の取扱いに関する教育を行ってまいりましたが、なお一層の個人情報の適切な管理を徹底してまいります。当該職員の懲戒処分につきましては、今後、司法の判断が行われますので、そちらを踏まえまして、厳正に対処してまいりたいというふうに考えております。司法の判断が出ましたら、市のほうで懲罰委員会という内部組織がございますので、その中で処分について決定するという流れになってございます。その際は、皆様に御報告させていただきます。最後になりますが、コンピュータ端末の不正使用という行為が信頼を損ねたことによりまして、深くお詫び申し上げますとともに、再発防止に向けまして、職員が一丸となり取り組んでまいりますので、よろしくお願いいたします。説明につきましては、以上でございます。

○奥谷委員長　ただ今の説明について、委員の皆様から御意見、御質問はございますか。

○篠塚委員　庁内ネットワークは、コロナ禍の中で在宅勤務をするのにも使用されていたものだと思うのですが、平成３０年から令和４年までの長い期間なんで、時系列で分かれば。いつ頃から始まって、内部告発がいつあって、その辺分かれば教えていただけますか。

○元川行革デジタル推進課長　平成３０年頃からというのは、本人からの聞き取り等で話があった時期でございまして、最初の報告、相談があったのが、令和４年の９月３０日でございます。人事課のほうに相談がありまして、行革デジタル推進課のほうに調査の依頼がまいりました。その当時、調査を行ったんですが、本人が間違いなくアクセスしているかどうかという部分が、個人の特定ができないという状況でしたので、この時点では詳細は判明しなかったという経緯がございます。その後、１１月に入ってから再度報告がありまして、その際に人事課のほうでしか知り得ない情報も絡んでいるということで、ほぼ間違いないんじゃないかという話がございましたので、アクセスログでは確認がとれなかったという経緯もございましたことから、本人が退庁したあと、本人の機器をリモートで確認したところ、デスクトップ上に他部署のショートカットとか、そういったものが見られましたことから、その時点で１１月１８日になりますけれども、１８日時点で証拠保全の観点から業務用のパソコンを引き上げたような経緯がございます。その後、内容につきまして、警察に相談すべき案件か、どういった法に抵触するのかと言う部分で、ファイルを調査した経緯もございます。その中で、今回の不正アクセス禁止法及び個人情報保護条例違反が間違いないということで、警察に相談する案件だということが固まってきてから証拠保全の関係で、それ以上は調査のほうは控えていたような経緯がございまして、警察に相談したのが今年の１月に入ってからということで、何度かやり取りをする中で、警察のほうが捜査が始まりまして、今般書類送検というよ

うな形に至った経緯がございます。
○篠塚委員　そうしますと、平成３０年から発覚する令和４年までは全く分からなかったということなんですね。こういうものにアクセスできるような部署にいたのか。それから、そんな情報をどこから持ってくるような部署にいたのか。バックアップフォルダを出すのに、いろいろなセキュリティがあると思うんですけど、その辺はどのようになっていたのですか。
○元川行革デジタル推進課長　おっしゃるとおり、平成３０年から昨年報告を受けて機器の確認までは、本人が不正にアクセスしているという状況は、把握できておりませんでした。と言いますのも、先ほどの市長公室長のお話にもありました、非常用のバックアップサーバーということで、こちらの存在自体、職員に周知していないようなものでございます。表示もされないサーバーになってございまして、本人の話によりますと、通常のサーバーというのはまた別にございまして、そちらのサーバーのインターネットで言うとアドレスのようなもの、アクセスパスというものなんですが、記号とアルファベット、数字の羅列のようなもの、そこからもしかしたら別のサーバーもあるんじゃないかということで、類推して試しにやっているうちにそこに侵入できてしまったということでありまして、バックアップサーバーについては、職員がアクセスするという想定はしておりません。所管のデジタル推進係のほうでは、何かトラブルがあった際にアクセスするという想定はできるんですが、通常一般の職員がアクセスするという想定はしておりませんでしたので、記号番号が分かるとアクセスできるような状態ということでございました。今回、本人が類推して侵入できてしまったという部分を受けて、判明した３日後にはもうそちらのほうはロックをかけて、入れないような対応を即座に取ったような状況がございます。以上でございます。
○篠塚委員　発覚して３日後。でも、その５年間は何もしていなかった、分からない状況で、どれだけの情報がいったかも分からない。今、司法の手に渡ったので、そちらのほうで調べると思うんですけれども、庁舎内の情報だけという理解でよろしいんですか。
○元川行革デジタル推進課長　職員が作成したファイルのサーバーということですので、様々なファイルがございます。例えば、その所管で必要な市民の住所とか名前のメモのようなファイルが中にもあったことは確認しておりますし、内部の業務に係るファイルが全てなんですが、その一部には、人事課であれば職員の評価に関するファイルもあれば、別の部署に行けばそこでやり取りしている市民の方の情報も含まれているということで、外部という部分で、例えば、住民基本台帳とか課税の情報とかそういったシステムからは切り離してはいるんですけれども、所管で作っているファイルが含まれているというような状況で、機器が警察のほうということですので、そちらのほうがまだ全部調査できていないような状況でございます。
○目黒副委員長　職員の自宅の捜査は、やはり警察のほうで今後行われる予定なんでしょうか。
○元川行革デジタル推進課長　捜査の内容については、こちらも教えていただけない部分がございます。ただ、何度か警察とやり取りをする中で、本人の家宅捜索もやってい

ると。また、本人に出頭してもらって、聞き取りをやっているというようなことは伺っております。
○目黒副委員長　１１月に判明してから、検察のほうに送致されるまでの間、職員はどのような対応をされていたのでしょうか。
○塚本人事課長　職員の対応でございますが。この段階ではまだ本人に、どういったことでやっていたのかとか、いつ頃からやっていたのかとかいろいろと聞き取りをやっているところでございました。
○奥谷委員長　今の目黒副委員長の質問に関連して。その間、職員は出勤はさせていなくて、自宅待機というような形だったんでしょうか。
○塚本人事課長　その間は、通常どおり勤務はしておりました。ただ、所属長と係長には経緯を説明して、しっかり職務中も注意をして勤務に当たらせるということをしておりました。
○菅井議員　ピンと来ない所があって、気になっていたんですけれども、職員本人が好奇心を満たすためにというお話だったんですけれども、個人情報や一部市民の個人情報も含まれているというところで、普通だったらこういった情報を得たら、悪用してしまおうとか、どこかに売ってしまおうとか、何かしら自分のメリットと言ったらあれなんですけど、そういうものがあってやる方ばかりかなという印象だったので、一体この方には何のメリットがあって、本当に自己満足のためになのかというふうに疑ってしまう部分があるんですけど、今確認はされていないけれども、今後、もしかしたら、実は情報が漏れていたとか、そういった可能性というのは、ないのでしょうか。
○塚本人事課長　私どもの聞き取り調査の段階におきましては、先ほど元川課長からも説明がありましたとおり、記号番号を類推してアクセスしたと。その中からいろいろと情報を見ることができるということが分かったようで、その中で、勤務の評定であったりとか、あるいは、自分が行きたい部署に異動するためにはどうしたらいいのかとか、こういった自己の好奇心からいろいろと探っていたということを本人からは確認しておりまして、それ以外の目的については、本人に確認したところ、本人は特にそういうことはないと。あくまでも、人事情報、自分の評価を上げるためにはどうすればいいかとか、行きたい部署に行くにはどうしたらいいかと。そのことで見ていたということで、お話は聞いております。
○菅井委員　ここ最近になって気づいたということで、気づかなかった期間が長い中で、気づかなかった年月が長すぎて、この職員の方、個人情報を見られる状況下にあって、自分の評価が実際に上がったというメリットはあったのか、意味はあったのかという点が疑問だらけなんですけれども。今回、令和４年の１１月頃になって、内部の職員からの連絡でということですが、なぜ急に分かったんでしょうか。今までずっと気づいてこなかったのに、急に分かったのはなぜなんでしょうか、
○塚本人事課長　まず、昨年の９月の３０日に内部の職員から、こういったことは人事課しか知らないじゃないかと言われるような情報を、この職員が知っていたという情報が寄せられました。その段階で、先ほども元川課長から説明がありましたけれども、ア

クセスログといいまして、どういった所にアクセスしてきたかという記録が残っていなくて分からなったという状況で、本人からも確認をする必要があるということで、その後の経過も行革デジタル推進課のほうで、注視をしていただいたと。その後に、１１月の段階で本人が意向調査というものを人事課のほうで行うんですが、その意向調査というのは、本人がどういった部署に行きたいかと、希望するような部署はどういった所かと。あるいは、異動したいのかしたくないのかと。そういったものを１１月頃に例年やっているんですが、そこに書いてあった文言が一般の職員が使わないような、この言い方というのは人事課の職員ではないと使わないような、いわゆる専門用語の記載があったということで、これは人事の情報を本人が見ているのではないかなということを確認ができたものですから、本人のパソコンを押収して確認したところ、いろいろとデータが保管されていたというところでございます。

○菅井委員　ありがとうございます。判明したのが昨年で、その前の令和元年、２年、３年という所も意向調査はあるかなと思うんですけれども、そういった所では、一切怪しい様子は見られなかったから、気づくことがなかったということでよろしかったですか。

○塚本人事課長　人事課のほうでそのような情報を掴んだのが昨年の１１月ということで、それまでには特に不審な点はなかったというところかと思います。

○菅井委員　ありがとうございます。こういったケースを聞くのが初めてだったので、どうしてそういう情報が漏れてしまって、気づくまでに時間がかかったのがすごく気になったので。お話が聞けて少し分かってきたので。また、新たな情報がありましたら、引き続き教えていただきたいなと思いました。ありがとうございます。

○栁澤委員　いくつか質問させてください。まず、非常用のバックアップフォルダというお話がありました。これは、サーバーで間違いないということですね。非常用のバックアップサーバーですね。おそらく、こういう大きな組織の中でバックアップをとっていないということはまずないと思うので、少しコンピュータが得意な人からすると、当事者の方からすれば、ちょっと得意な人だったと思うんですけれども、まずその存在というのは疑うとは思うんですね。試しに打ってみたらつながってしまって。それで、開いてみたらパスもかかってないやという状況で、本人も多分びっくりしたと思うんですよ。その後は好き放題拾ったのか分からないですけれども、好きに触れる状態ではあったわけですよね。そこで、アクセスログが残らないというようなお話だったんですが、ちょっと聞きそびれてしまったかもしれないんですが、アクセスログが残らないのは庁内のネットワークの仕様ではなくて、その当事者の方が足跡が残らないように何か処理をしたということでしたか。

○元川行革デジタル推進課長　アクセスログについての御質問について、容量の関係でアクセスログを保存できないような状態ということで、後は追えたとしても、部署くらいまでしか追えないような状況がございました。こちらの部分については、今後のことも考えまして、新たなシステムを、まだ未導入なんですが、１０月にログの管理とか監視とかそういったものができるシステムの導入を予定しているところでございます。以

上でございます。
○柳澤委員　ありがとうございます。そうしましたら、アクセスログの追跡よりはアナログなんですけれども、例えばサーバーの中、ネットワーク上の人間はそれぞれユーザー名を充てられていると思うんですけれども、例えばエクセルファイルを開いたら、プロパティを見れば最後に誰が触ったかというユーザー名というのが出るものだと思うんですけれども、そういったものも残らない状態であったということなんでしょうか。
○元川行革デジタル推進課長　柳澤委員がおっしゃるとおり、ユーザーごとに個別に割り当てていれば、当該個人にたどり着いたんですけれども、現時点での管理の方法が部署、各課ごとに割り当てているような状況ですので、その課の誰がという部分で確証がとれないような状況でございました。
○柳澤委員　ありがとうございます。各課の誰がアクセスしたかまでは特定できないと。逆に言えば、課の課長クラスにはアクセス権があるんですかね。
○元川行革デジタル推進課長　課長のほうも部署の一人ということで、通常のサーバーですと、所管部署以外は権限が与えられていないので、見られないような状況でございます。ログにしても課長であっても課員であっても、同じように個人を特定できない部分、あとは、今回の当該人物の業務用のパソコンであっても、間違いなくその人が操作しているかどうかという部分まで確認ができないということで、先ほど経緯の中で申し上げた当初相談があった時はそこまでしか追えず、特定ができない状況でございました。以上でございます。
○柳澤委員　そうしますと、誰かがというのは特定できなかったかもしれないですが、アクセスの頻度などは分かりましたか。
○元川行革デジタル推進課長　相談があって以降、その部署のアクセスログのほうを係員が監視しておりました。ですので、アクセスの頻度までは分かったんですけれども、誰がという部分で決め手といいますか、本人特定できないというような状況でございました。
○柳澤委員　ありがとうございます。そうしますと、各部署でアクセス権限のある方が何人いるかというのもあるんですけれども、逆算していくとこの人が頻度的にこんなに見るかなという、一日に何回以上アクセスがあったらこれはちょっと変だなというような閾値みたいなものは設けられそうですかね。
○元川行革デジタル推進課長　なかなかその閾値という部分が、今回の件ですと、保管や見る権限のないファイルにアクセスという部分がありますので、そういう所で判断とか、あるいは今後は先ほど申し上げた所属ではなく、個人ごとのＩＤ、パスにして、アクセスログを監視するような方策も講じていければということで、今のところ考えております。
○柳澤委員　ありがとうございます。また、サーバーのほうに戻りまして、サーバーはミラーリングで最新版が保存されているような状態であって、最新版をその方も見ていたような状態だったのでしょうか。
○元川行革デジタル推進課長　サーバーのほうは一日に２回ファイル等の更新を行って

いるようなものですので、１日２回の頻度での最新の状態でございました。
○栁澤委員　ありがとうございます。それと、当事者の私的端末にデータを移したというふうに説明がありましたが、これは有線で行ったのか、それともメールやドライブ、クラウドなどに入れてそこから落としたのか、その辺りは追えていますか。
○元川行革デジタル推進課長　私物の機器につきましては、外付けのハードディスク、ＵＳＢフラッシュメモリという状況でございます。ですので、外付けのハードディスクはそのままつないで、私物のパソコンは本人の話ですとＵＳＢを使って移していたような話もございました。ＵＳＢについては、少し前に尼崎のほうで紛失という件があったかと思います。それを受けて、そもそもＵＳＢの使用は禁じていたんですけれども、改めてその辺り厳格な対応ということで、市職員にも周知を図っている状況で、先ほど新たなシステムということで、アクセスログを管理が可能なものというシステムにつきましては、物理的にＵＳＢも使えないような対応も取れるようなシステムとなっておりますので、その辺も万全を期した体制で対応をとってまいりたいと考えております。以上でございます。
○篠塚委員　この事件が起こったことにより、市民の方が不安になると思うので、その辺の説明をしっかりしていただきたい。今後のことに関しては、セキュリティを高めたりやっていると思うんですが、５年間近くやり放題やっていたと。いくら個人の情報を見るだけだとは言っても、いろいろな情報が入っているものを閲覧できたわけですから、例えば入札情報であったり、個人情報もかなりあったでしょうし、その辺の不安があると思いますので、しっかりと調べていただいて、もし、問合せがあったら、それは真摯に応えるしかないと思うので、その辺はしっかりしていただきたい。それから、今後のことに関しては、セキュリティを高めることをお願いしたい。もう一つは、３１歳の職員が入庁して何年も経たないうちですよね、これが始まったのは。教育もそうでしょうけど、どのような評価をして採用したのか、その辺はどうなんでしょうか。
○塚本人事課長　採用の部分につきましても、どこまで追えるかということはございますが、入庁後に職員研修での公務員倫理、そういうものも含めて、先ほども話がございました情報セキュリティポリシーをしっかり遵守できるような職員を育てていきたいというふうに考えてございます。
○船沢市長公室長　職員の新人研修の中で、もちろん公務員としてのコンプライアンスもしっかりやらせていただいているんですけど、合わせて情報セキュリティについても研修をやってございますので、周知はしているんですけれども、改めて徹底してやってまいりたいと考えてございます。
○細野総務課長　個人情報の保護に関して、これまで個人情報保護制度に関する定期的な研修を毎年度実施してまいりました。この内容としましては、個人情報の保護に関する取扱いのほかに、情報漏洩防止の研修、情報漏洩防止などの適正な管理、そして職務上知り得た情報を不正目的に使用しないといった内容で研修を実施しておりまして、昨年度については、２月に全ての係長を対象として実施してまいりました。このほかに、個人情報の取扱いに関する留意点をまとめました個人情報取り扱いの事務の手引き、こ

ちらを全所属に配布してまいりました。また、個人情報の漏洩事案等がありましたら、庁内のグループウェアに掲載しまして、注意喚起を図ってまいりました。今後は、研修を実施してまいります。今年度につきましては、１２月を予定しているんですが、全課長を対象にしまして、実施する予定でございます。また、本年４月に策定しました個人情報の適切な管理を定めました安全管理措置要項というものがあるんですけれども、こちらに基づきまして、全職員を対象にしまして、個人情報の管理に関する自己点検を実施してまいります。今現在、グループウェアのほうでこちらを流しまして、自己点検を実施している状況でございます。また、所属長に関してもこの自己点検というのを実施しておりまして、所属長の自己点検表に基づきまして、監査事務局による内部監査というのを実施してまいります。これらによりまして、全庁的に個人情報の適正な管理を図るとともに、職員の意識付けを図ってまいりたいと考えております。以上でございます。

○目黒副委員長　市民の個人情報等なんですけれども、マイナンバーカードの情報は含まれていたんでしょうか。

○元川行革デジタル推進課長　全てのファイルがまだ確認できていない状況でございます。本人が使っていた業務用のパソコンと私物のパソコンが実は昨日警察のほうからこちらに戻ってきたところでございます。こちらについては、重要な証拠品ということでございますので、この後検察庁のほうから提出依頼が来るかどうかという部分も想定されますので、その辺は警察、検察のほうと調整して、調査が可能となった時点でそういった情報があるかどうかも含めて、どんなファイルがあるのか速やかに調査させていただきたちと思います。

○目黒副委員長　市民の方、一番そこが気にされていると思うので、一番にぜひよろしくお願いいたします。

○菅井委員　自分のことになるんですけれども、すごく若い時に自分の個人情報が売られていたということがあったんです。知らない所からいきなり連絡が来て、電話が軽い感じの話し方である日突然来て、どうして私の番号を知っているんですかというふうに聞いてみたんです。そうしたら、個人情報は簡単に売られているのを知らないのかと言われて腹が立ったということがあったんですが。電話をかけてきた人もすごく若い人だったので、若い人たちほど、若い人が全員とは言いませんけれども、個人情報とか、何が守秘義務で、何を話してはいけないのか。そして、それが今回の件があって、私も自分の保育園のほうで、職員だったり園児さんの情報が漏れる可能性があるよということは、どんなに親しい仲でも、それが家族であろうとも、それは話してはいけないという話を朝礼で話したので、些細なことだから大丈夫であろうというような意識が若い人たちだとまだそれがどういう所につながってしまうのかというのが分からない、多分教えてもらわないと分からないということがたくさんあると思うので、こういう大きな事態につながってしまうんだよということも含めて、新しく仕事で入ってきた人たちには、今回の事例についても、こういうこともあるんだよということも含めて、きちんと伝えていって欲しいと思いました。そういったことで、人間不信になったりだとか、その人の人生を狂わせてしまうことがあるかなと思ったので、引き続き、対応のほうしていた

だければと思います。よろしくお願いします。
○柳澤委員　シンプルなデータの漏れる原因といいますか、メールにデータを添付して送付するということについてのチェックなどされていますか。
○元川行革デジタル推進課長　機器を引き上げさせていただいて、当課の職員のほうでその部分につきましてはできる範囲で確認しております。そういった形での漏洩は今のところ確認されていない状況でございます。
○柳澤委員　当事者の方が行った記録はないということなんですが、職員の皆さんがメールを使われることはあるんでしょうか。その時にデータを送れるようなシステムになっているのでしょうか、添付ファイルとして。
○元川行革デジタル推進課長　グループウェアということで、庁内でメールのやり取りはできるようなシステムになっております。そちらにファイルの添付も可能というような状況でございます。
○柳澤委員　ありがとうございます。そうしましたら、外部に漏れることはないというような認識でいいですかね。あくまでもオフラインということでしたので。外部にもメールを送れるんでしょうか。そのやり取りの中で。
○元川行革デジタル推進課長　内部だけではなく、茨城県のシステムを使った外部メールのやり取りできるものがございます。そちらのほうもファイルの添付が可能となっております。そちらについても、当課の職員で確認できるものは確認いたしましたが、外部に漏れているような形跡は今のところ認められていないというような状況でございます。
○柳澤委員　ありがとうございます。今までの話ですと、本来アクセス権がない人がアクセスした上で、情報漏洩ということが中心となっていた気がするんですが、逆に今はアクセス権のある方が悪用してしまうというような懸念といいますか、可能性もゼロではないと思うんですが、そこをストップさせる手段というかシステムというのはお考えでしょうか。
○船沢市長公室長　他市の事例をネットで見た記憶があるんですが、業務上個人情報を取れる方というのはおります。それは、データ以外でペーパーベースで取れる方がいらっしゃると思います。それは、業務上として取得した個人情報を外に出すことというのは、完全な違反行為になりますので、先ほど申し上げました情報セキュリティの面からも、セキュリティポリシーというのを設けておりまして、全職員に周知しているものなんですが、先ほど総務課長からお話のありました個人情報の取扱いにつきましても、職員に対して周知しているものですので、業務として取れるものをブロックというのはできませんので、当然職員としてそれをやることによって、ペナルティが課せられるというものだということについて、しっかり研修を行い、そういったことがないように取り組んでまいりたいというふうに思ってございます。
○柳澤委員　難しいんですけど、システムとして抑制する手段は最後はなくて、あくまでリテラシーポリシーで留めてもらうというような認識でよろしいでしょうか。
○船沢市長公室長　両方ですね。システム上でできることは最大限のことはやりたいと

思ってございます。こういった対策についても、もしかしたら内部職員なので、こういうケースというのはレアなんですけれども、外部なども見た場合に、不正アクセス、特にインターネットなどというのはつながりますので、そういう部分は常にステップアップできるような形で。あわせて、モラルのほうですね。我々職員については、地方公務員法でコンプライアンスが求められておりますので、違法行為ができないとはっきりと様々な観点から職員に植え付けてまいりたいと思っております。

○細野総務課長　個人情報の管理に関する自己点検ということでお話をさせていただきましたけれども、この自己点検表なのですが、個人情報の管理の状況として情報漏洩の防止措置、セキュリティ対策、書類送付の注意事項、そしてパスワードの定期更新など、適切な管理のために留意すべき３３のチェックリストからなっております。そしてこの項目の中に、添付ファイルのチェック、そして、送付先のチェックを行っているかという項目も含まれております。また、紙の個人情報に対しては、それを持ち出す際の帰庁後の紛失の確認というようなことも入っておりますので、これをきちんとチェックしていただいて、職員の意識の高揚を図ってまいりたいと考えております。

○奥谷委員長　御意見も出尽くしたようですので、以上としたいと思います。今、いろいろと意見がありましたけれども、職員のリテラシー教育とセキュリティの関係、市民からの問合せに対する関係含めて、丁寧にこれからまたお願いしたいと思います。以上で総務市民委員会を閉会いたします。お疲れ様でした。