１　件　名　　令和３年度　第１回古賀市情報公開・個人情報保護運営審議会
２　日　時　　令和３年７月６日（火）１５時００分～１７時００分
３　場　所　　市役所第１庁舎第２委員会室
４　出席委員　荻委員、近藤委員、三輪委員、井手上委員、南正覚委員、清水委員、上野委員
５　事務局　　簑原総務課長、総務課政策法務係（西村、山田、古田、村瀬）
６　説明者　　中村市民国保課長、市民国保課国保係（渋田、福原）、
内デジタル推進課長
７　傍聴者　　なし
８　内　容　　①会長の互選
②会議の公開等について
③諮問第１号
（１）国民健康保険の第三者行為求償に係る粕屋北部消防本部と古賀市の連携による個人情報の収集について
④諮問第２号
（１）テレワークにおける共有フォルダーの取扱について
（２）LINE 及び LoGo チャットにおける個人情報の取扱について
⑤令和２年度古賀市情報公開制度運用状況報告
⑥令和２年度古賀市個人情報保護制度運用状況報告
⑦その他

８　会議概要（要約筆記）

（総務課長）　挨拶

（自己紹介）

（事務局）

本日の会議は、古賀市情報公開個人情報保護運営審議会条例第６条第２項に規定されている委員の過半数以上の出席があるので、成立している。委嘱状については事前に送付している。古賀市情報公開個人情報保護運営審議会条例第５条に基づいて、会長と職務代理者を互選にて選出する。立候補していただける方はいるか。

→立候補無し

（事務局から推薦）

会長に荻正憲委員、職務代理者に南正覚委員を推薦。委員の拍手をもって承認としたい。

→拍手（承認）

（会長）挨拶

以下、会長による進行

（会長）古賀市情報公開条例第 23 条に基づき、会議を公開としたいがよろしいか。

→了承

（会長）

諮問第１号国民健康保険の第三者行為求償に係る粕屋北部消防本部と古賀市の連携による個人情報の収集について、古賀市個人情報保護条例第７条第３項第８号に基づく諮問となり、具体的には、個人情報を収集することが相当であると認めるかについての意見を求められている。諮問第１号の説明を担当課（市民国民課）からお願いしたい。

（担当課）

今回の諮問は、古賀市個人情報保護条例第７条（収集の制限）の第３項第８号の規定に基づき行うもの。当該個人情報を本人以外から収集することが認められるかについて審議をお願いしたい。なお、本件については、情報を提供する側である粕屋北部消防本部の個人情報保護審査会において、情報の提供について相当であるとの決定をいただいている。

諮問書４番の個人情報取扱事務の目的について。第三者行為求償とは、国民健康保険の被保険者が病院で治療を受ける原因が、第三者による加害、または本人の不法行為によるものであれば、その治療に係る医療費は、第三者または不法行為を行った者（加害者）が負うべきものとして、国民健康保険が給付した医療費を請求するもので、国民健康保険法第６４条に定められている。第三者による加害とは、交通事故、暴行、落下物によるけが、飼い犬などにかまれる犬咬傷、施設の不備による受傷などのことをいい、本人の不法行為によるものとは、飲酒運転事故、スピード違反による交通事故、自傷行為などを指す。このような場合に治療に要した医療費は、加害者が本来負担すべきものであるが、これを国民健康保険で負担したままであれば、加害者は不当に利益を受けることになる上、その負担が保険税に反映されることにより、不公平な結果が生じることとなる。

そのため、国民健康保険は、第三者による加害や不法行為による医療費給付を把握し、加害者への適切な賠償を求め、医療費適正化及び保険財政の安定化を推進する必要がある。国民健康保険の保険者である福岡県も、福岡県国民健康保険運営方針の中で、第三者行為求償事務の取組強化について言及しており、第三者行為求償に係る消防本部等関係機関との連携について推奨し、さらなる取組強化を推進しているところである。以上のことから、粕屋北部消防本部が所有する救急搬送記録の提供を受け、第三者行為による受傷の発見の機会を増やすことを目的としている。

次に、５番の個人情報対象者の範囲について説明する。現在予定しているのは、古賀市在住で０歳から７４歳までの交通事故、交通事故加害一般負傷による救急搬送記録の提供である。７５歳以上は全員後期高齢者医療保険に加入しているため除外している。０歳から７４歳までの人は、国民健康保険のほか、社会保険や生活保護受給者の可能性もあるが、粕屋北部消防本部で国保の加入者のみを抽出することは困難であるため、被保険者の抽出については、情報提供を受けた後、古賀市で行う予定。また、交通事故、加害、一般負傷という区分は、粕屋北部消防本部で従来そのような事故種別によって分類していることを確認済み

次に、６番の収集する個人情報の内容については、別紙の記録簿（案）を参照していただきたい。提供を受ける個人情報の内容については、救急搬送者氏名、生年月日、年齢、住所、事故発生年月日、救急搬送出動場所、収容医療機関名、事故種別、事故概要を予定している。粕屋北部消防本部の負担にならないよう、通常記録している内容の一部を提供してもらう予定。また、氏名や搬送先が分かれば、医療機関からの報告書であるレセプトの内容に基づいて、病院または本人へ内容の照会が可能なため、提供内容について粕屋北部消防本部へ個別の問合せは行わないこととしている。

次に７番、情報提供の方法について。指紋認証つきのUSBを使用し、月に１回情報提供の依頼をする予定。USBの情報は提供される度に削除する予定としている。ただし、USBは紛失などの可能性もあるので、今後は、閉鎖環境でのデータ送信など、より安全な方法についても検討していく予定。

次に８番の情報の管理について、提供されたデータは、古賀市で住民基本台帳などの事務で使う基幹系のPC内で、データ共有出来ないフォルダーを作成して保管する予定となっ

ている。また、情報提供に使用するUSBには、紛失防止策を施し、鍵付きの棚への保管を予定している。

次に、情報の破棄について。救急搬送情報を使用する必要がなくなった場合は、速やかにデータを削除する予定。削除するのは、提供を受けた時点で国保以外の人の救急搬送記録を削除。その後、受診から2か月後に到着するレセプト情報と搬送の記録を照らし合わせ、第三者行為による受傷でないと確認できたものを削除。第三者行為に該当する搬送記録については、求償事務完了後に削除という流れになると想定している。

10番の情報提供開始時の依頼について。本審議会で情報提供が相当であると認められた場合は、まず、別紙覚書の締結を行う。情報提供開始時及び更新時には、別途依頼文書を、粕屋北部消防本部に提出する予定としている。

（会長）

判断する上で今回の情報収集の重要性を理解する必要があると考える。国民健康保険の支払いについて、第三者行為の場合は加害者に払ってもらうということだが、国民健康保険の主体は市と県であり、支払いは県が行っているのではなかったか。支払いの部分で市がどうかかわるのか。

（説明者）

国民健康保険は平成３０年度から都道府県単位で運営することとなっている。都道府県は財政運営を行い、市町村は資格の管理や保険税の決定、賦課徴収などの事務をやっている。県は市に対して納付金の額を示し、市が納付金を納める。そして、県は市が医療機関に払っている保険給付費の全額を市に対して交付する流れとなっている。

（会長）

今回の第三者行為だった場合は、市から求償するという形か。

（説明者）

求償事務についても専門的な知識が必要となるため、福岡県国保連合会に委託している。求償事務によって返済された金額については市の国民健康保険の特別会計に入ってくる。

（委員）

従来はどのような形で、第三者行為求償が発生しているか確認しているのか。

（説明者）

現在、行っている取組としては、患者が受診した後に届く診療報酬明細書（医療内容点数、傷病名が記載されているもの）を提出する際に加害でケガをしたという申し出があった場合は、10.第三という記号が記載されているため、これを確認することによって把握する。この記号を記載することについては福岡県全体で医療機関に対してお願いする取り組みを実施している。しかし、この記号は交通事故や暴行など明らかに第三者から受けたものにしか記載されていない。そのため、記号が付いていないものについては、全身打撲や刺傷された傷、犬に噛まれた等の傷病名を基に市で判断し、病院や本人に照会し、怪我等の原因を教えていただくよう通知を送付したりしている。あとは、国民健康保険の通常の業務の中で、限度額適用認定証という高額な医療を受けるときの事前の限度額負担のカード等を発行する場合にも、怪我が第三者によるものでないか質問するなどして把握に努めている。

（委員）

救急搬送記録簿と覚書（案）の業務内容の救急搬送情報の内容に違いがあるが、覚書が

正しいという事でよいか。
（説明者）
覚書が正しい。
（委員）
内容的に異論はないが、諮問の仕方がこれでよいのか気になっている。今回の諮問は、個人情報保護条例第７条第３項第８号の規定に基づいての諮問となっている。この規定に基づいて見るべきは、本人から収集するのでは個人情報取扱事務の目的達成が難しいのかどうか等について判断しなければならないのではないかと思っている。これに対して、今回の諮問書には、「個人情報を収集することが相当であると認められるかについて意見を伺いたい」ということになっているので少しずれがあると感じている。
（事務局）
総務課で精査し、この第７条第３項第８号に基づいた諮問ということで良いのではないかと判断した。本人から収集することが非常に難しい状況がある。例えば交通事故であれば揉めている最中で情報が入ってこないという場合もあるので、この条文に基づいて諮問させていただいている。
（委員）
いくつかの市の条例を見たが、少し古賀市の条例は特徴的なようだ。他のところでは、例えば「公益上の必要がある場合」という書き方や、あるいは「事務の遂行上必要がある場合」というような、抽象的な書き方をしているところが多いが、古賀市の場合は「個人情報取扱い事務の目的達成」あるいは「円滑な実施」というところで、あくまでその個人情報の取扱事務に限って、本人から収集するのでは難しいという認定をし、答申を作成しなければならないのではないかと思う。内容としては異論がないので、説明の仕方だけ工夫する必要があるのではないかと思う。
（事務局）
１点補足したい。委員が言われた形で答申をいただければと思う。事務局としては、この条項に基づいて、この条項に当たるということが相当であるかについて回答いただければと考えている。
（委員）
情報の破棄に関連して、先ほど３段階で破棄すると言われたが、提供するデータはPDFなのか、それともエクセルのような一行ごと抹消できるようなものでくるのか。
（説明者）
粕屋北部消防本部と協議し、消防本部で使用しているシステムからデータを抽出し、エクセルデータを作成して、提供される予定。市としてもそのエクセルデータを加工して削除等する形で考えている。
（委員）
３段階で破棄するということに関して、きちんと書面で引継ぎされるのか。様々な情報が一旦集められるので、破棄に関してはきちんとしておかないと、第１０条の問題も出てくるので、破棄に関する対応はきちんとしてほしい。趣旨は問題ないと考える。
（会長）
破棄について、エクセルデータの行を削るようなイメージか。1行を削って、上書きして、それをもって削除とするという運用の仕方を想定しているのか。
（説明者）

１人につき１行にデータが横に入力されている状態で提供されるので、必要のない方の情報については、行を削除する。必要な方の分は一定期間残すが、長く残すものではないと考えているので、最終的に提供されたデータは全部削除するように考えている。担当が変わってもルールが守られるよう、更新時の依頼文書に明記するなどして引継ぎ漏れがないように検討する。

（会長）

資料の８番目に、「USB には紛失防止策を施し」という記載があるが、これは具体的にどのようなことを想定しているのか。

（説明者）

USB の管理については、デジタル推進課とも協議をしており、小さな USB に、大きなキーホルダー等をつけたり、大きなケースに入れたりすることで紛失防止になると考えている。まずは、小さくて失くすことがないようにする。また、ポーチに入れた場合でもさらに施錠できるようにするなどの対応を検討している。

（会長）

月に１回情報を入手し、月に１回エクセルファイルが提供されるということだと思う。不要になれば削除するということだが、例えば Windows であれば、ごみ箱に入れて全て空にするというイメージだと思うが、それでは USB 自体にはまだデータが残っている。つまり、一見削除されたように見えるが、データとしてはまだ残っている状態である。技術的な話になるが、何らかの形で USB が流出した場合、データを復元して読み取れる状態だということになるが、それを踏まえた上でデータを削除する方法については検討されていないか。

（説明者）

検討中である。

（会長）

提供されるデータのパスワードはエクセルファイルの機能を使ったパスワードを想定しているのか。

（説明者）

パスワードについてはエクセル機能のパスワードを使用する。また、USB のデータ消去の件は、消去だけでは復元できると思うが、この USB については指情報の認証機能がついたものを使うということで、デジタル推進課と打ち合わせている。これによって、第１段階の漏えいの防止にもなると考えている。

（会長）

その点はいいと思う。USB については指紋認証や、コードを入力して USB の内容そのものを暗号化するものが、２万円程度で存在するので、そういったものを使用したらいいのではないかと思う。暗号化にも色々な種類があるので、デジタル推進課と協議して安全性の高い暗号の種別を選んで製品を購入すれば紛失した際も安心ではないかと思う。今回収集する個人情報は非常に重要性の高い、また秘匿性の高いものと思うので、今後の運用についてはマニュアルをきちんと作成していただきたい。私としては今回の内容に異論はないが、運用面でもっと安心できるレベルまで詰めていただきたい。

（委員）

第三者求償について、現状で加害者に請求できていない件数を把握しているか。古賀市でなくても他の自治体や県などで検証したエビデンス（検証結果）はあるのか。

（説明者）
第三者求償できている件数というのは、各自治体からの報告によってある程度数字が分かるが、漏れている件数というのは正直、把握が難しい。転んだ際の受傷といっても、転んだ場所によって第三者行為となるかどうかというようなこともあるので、把握できていない件数の調査というのは正直難しいところがある。
（委員）
粕屋北部消防本部は、古賀市と新宮町から構成されており、そのやりとりの中で、新宮は紙媒体で情報を受け取ることになっており、それは設備が整っていないためのようだが、行政機関としてはUSBで提供されることが望ましいというコンセンサスは確立されていると理解してよいか。
（説明者）
粕屋北部消防本部との協議の中で、古賀市は件数が多くなるため、紙媒体ではなくUSBで提供いただくよう希望し、了承いただいたという状況である。
（委員）
先ほど指紋認証機能のあるUSBを使用するとのことだったが、担当者の指紋情報が残っているので、ハッキングしようとした場合には指紋認証もリスクはあると思う
（委員）
救急搬送記録簿の一番右の欄、事故概要には、令和元年１２月６日付の粕屋北部消防本部との連携についての３ページ目（参考）の事故形態が記載されるのか。それともももっと詳細な内容が記載されるのか。
（説明者）
救急搬送記録簿の右から二番目の欄、事故種別には、例えば交通事故との記載しかないため、事故概要の欄に単独事故なのか車同士の事故なのか等、事故の簡単な内容が記載されると聞いている。この欄については、粕屋北部消防本部からの提案で追加している。
（委員）
簡単な内容とは、参考資料の事故形態とは異なるのか。
（説明者）
それとは別のもの。
（会長）
通常は、第三者行為ではないかと思われたものに対して、問合せをするという形になっていると思うが、その判断は古賀市がするのか。
（説明者）
現在は、病院から報告されるレセプトの中で、交通事故と疑われるものについて、システム上で決まった傷病名が抽出できる。抽出された場合、本人に交通事故ではなかったか確認する文書を送り、傷病届の提出をお願いしている。今回の情報提供が可能となった場合は、より第三者行為かどうかの判断が分かりやすくなり、勧奨通知を送ることができるようになるものと考えている。
（会長）
第三者行為によるものではないか判断し、勧奨通知を送るという事は今までもやっていたが、より精度の高い情報がほしいという趣旨という理解でよいか。
（説明者）
そのとおり。

（会長）
実際には通知を送った後、きちんと回答が得られるのか。
（説明者）
個人に通知した際は、おおむね回答を得たり、何かしらの問合せがあったりしている。ただし、交通事故に関しては損害保険会社に直接連絡することもある。
（会長）
通知を送るというのは非常に確度が高く、今回の件で提供される情報については、国保の運営においても確度の高い情報が手に入ると思ってよいか。
（説明者）
はい。
（委員）
交通事故の場合に過失割合があり、色々な割合の場合があるが、この第三者求償事務において、過失割合に応じて請求できるのか。
（説明者）
双方に損害保険会社が関与している交通事故であれば、損保会社のほうで過失割合を決定するので、その過失割合に応じた求償額を計算して相手方に請求することになる。場合によっては、損害保険会社の関与がない場合もあるので、市民国保課で事故内容を精査して、判例タイムズなどの事例をもとに、過失割合を調整して、その分だけを加害者に請求するという流れとなっている。
（委員）
今回の情報の収集自体には全く異論がないが、条例の第７条第３項第８号該当性が、今回の事例で、端的に認められるのかというのは疑問があるのではないかと思う。条例の第７条第３項第８号については、非常に狭い範囲でしか適用できないのではないかなと思うので、可能であれば条例の改正を検討されてはどうかと思う。
（委員）
条項の「個人情報取扱い事務」というところがネックになってくると思っている。ここが単に「事務」であれば第三者行為求償事務の目的達成、円滑な実施に関しては本人から収集では十分にできない、ということで認められると思うが、あくまで「個人情報取扱い事務」というようにはっきり書かれているので、考え方を工夫しないといけないかなと思う。そこで、本人収集だと全ての情報を把握できないという事になり、当然、個人情報を取り扱う以上はそれに該当する個人情報というのは網羅的に把握する必要があるが、本人収集であれば漏れが出てきてしまう。漏れがあれば、今回の第三者求償に該当する方の個人情報を取り扱う事務の実施としては、十分ではない、というところで、この条項に該当すると解釈できると考えることもできるのではないかと思う。
（事務局）
今いただいた御意見に関して、市の条例では「本人から収集することにより、個人情報取扱い事務の目的の達成に支障が生じ、又は円滑な実施を困難にするおそれがある」という内容になっている。事務の手引き上は、「事務事業の目的、性質から判断して、本人から収集したのでは目的が達成しないおそれがある場合、本人から収集したのでは多大な経費と労力を要するため、当該事務の円滑な実施が困難になる恐れがある場合等、本人以外から収集することに、社会通念上客観的に見て合理的な理由がある場合をいう。」ということで当市としての解釈をしているところである。現状では、説明したとおり、第三者求

償できるかどうかということを確認すること自体にかなりの困難と労力が存在していると思っている。さらに、直接、連絡できる場合は、お答えいただいて第三者求償できるということになるが、通常、あなた事故の加害者ですかと言われて、はいそうですという答えを期待することは難しいのではないかと考えている。そのような観点からしても、やはり今回のような形で粕屋北部消防本部から情報をいただくということが、多大な経費と労力等の事情も含めて、社会通念上客観的に見て合理的な理由があると言えるのではないかと考えている。

（会長）

今回のような事案に本条項が適切かと言われると、疑問がないわけではないと思うし、条例改正という方法も考えられなくはないが、現時点で審議会としては、現状でできる最善のことというのを考えると、この条項に従って、今回の事務を粛々と進めていきたい。一応、私としては今回この諮問の一文には特に異論はない。

（委員）

平成３０年から財政運営は県が、賦課徴収については市が行うという形になっている。今回の審議事項について公平公正な負担の担保として、レセプト点検と合わせて非常に重要な情報収集であると考える。そこで、個人情報保護条例については、市域にしか適用されないが、保険制度の視点から考えると、市民は古賀市内だけで事故にあうわけではないし、他の地域にも消防署が設置されているので、求償事務の精度を上げるために、今後の展望をどのように考えられているのか聞かせてほしい。

（説明者）

今回、粕屋北部消防本部から情報提供を受けることが糟屋地区においては最初ということで、中南部の消防署との連携については、今後検討する内容になってくると思われる。今後は、各自治体が保険者でもあることから、各地域の消防署からの情報収集がスタンダードになったり、県が統一して行ったりという状況が望ましいと考えている。現在はまだ県内でも２７自治体が消防署と連携をしているという状況。これが今後広がってきて、スタンダードになっていけば良いと考えている。現在のところ、市としては、できる連携をできる限りスタートさせていくというのが、我々にできることだと思っている。

（委員）

個人情報取扱事務の守備範囲について問題になっているが、第６条に記載されている名称や目的など登録簿の内容は全て満たされていると理解してよいか。

（説明者）

粕屋北部消防本部から、救急搬送情報提供を受ける前に、第６条にある個人情報取扱い事務登録簿を作成する。現在作成する準備を進めているところ。

（会長）

他にご意見・質問などないか。なければ、審議会としての結論を出したい。諮問内容としては個人情報を収集することが相当であると認められるかということだが、審議会の結論としては、個人情報を収集することが相当であるとしたいと思うが、皆様よろしいか。

→全員賛成

（会長）

全員賛成、反対意見なしということで、審議会の結論として、本件、諮問第１号については、個人情報を収集することは相当であるという結論にしたい。

諮問第２号（１）テレワークにおける共有フォルダーの取扱いについて
（会長）
古賀市情報公開個人情報保護運営審議会条例第２条第１項の規定に基づく諮問であり、具体的には当該事項について、個人情報保護のために必要な措置が講じられていると認められるかについて意見を求められている。担当課から説明をお願いする。
（説明者）
追加資料として経済産業省の規定を配付している。この資料右肩に記載のとおり、取扱注意の文書なので、後ほど回収させていただく。
まずセキュリティー面の話をした上で、諮問内容についての詳細説明をさせていただく。若干技術的な内容も含むため説明が難しくなる部分もあると思われる。
まず、セキュリティー面について、資料のネットワーク概念図を見ていただきたい。古賀市では、情報資産の取り扱いに関して、ネットワークを３つに分離している。①マイナンバー系で１つのネットワーク、②基幹系（住民基本台帳や税等）、③一般的な事務を行う情報系ネットワークの３つ。いずれもインターネットには直接つながっていない。そして、それぞれはお互いに通信を行う線は設けていない。
今回はテレワークの話になるが、現在、自宅からインターネットを通じてNTT東日本（IPA）にあるシンテレワークシステム（IPAのバーチャルプライベートネットワーク）というものを使い、③番の情報系ネットワークにある個人が使用しているパソコンに画面転送という形で入って操作を行う、という形でテレワークを行っている。言い換えると、③番の情報系ネットワークから市の情報資産として特に重要性が高いマイナンバー系や住基情報等には一切アクセスできない状況である。
次に、シンテレワークシステム概要資料をご覧いただきたい。シンテレワークシステムは、NTT東日本とIPAによるシステムで、不正ログイン対策として、２要素認証を行っている。いわゆるワンタイムパスワード。これに加え、MACアドレス認証というPC固有の識別コード（MACアドレス）を事前に登録し、その登録をしているパソコンからしか職場のパソコンにアクセスできないという設定も行っている。
以上のことから、現時点ではかなり最高峰のセキュリティー対策を講じているものと考えている。そのため、なりすましやハッキングの可能性は極めて低い作りとなっている。
また、情報資産については、職員による不正持ち出し等の可能性を含めて考えなければならないが、資料の４点目に記載しているとおり、画面転送方式なので、データ持ち出しは一切できない形になっている。具体的には、職場のPCのエクセルファイル等のファイルを自宅のパソコンに直接コピーはできないし、CSVを開いてその情報をコピーして自宅のパソコンにコピーもできない。また、自宅のプリンタに印刷することもできないという設定になっている。
以上のことから職員による不正持ち出しについても万全な体制を備えていると自負している。
さらに、自宅のパソコンがウイルス等に感染して何らかの形で不正操作行おうとしても、職場のPCは直接つながっていないので、無制限にデータが漏えいするような事態はあり得ないものと考えている。
追加配付の経産省の資料をご覧いただきたい。２ページに経産省の格付の記載がある。３条で格付の記載があるが、経産省は情報資産が高い順に３、２、１としているが、古賀市は逆に１、２、３で高い順となっている。まず経産省の一番機密性が高いものについて

は、特定秘密や秘密文書、特に機密性の高い情報で不開示情報、存否を明らかにしないようなもの、これらが機密性３と考えられている。そして、機密性２としては、不開示情報に該当すると判断されるもので機密性３ではないものが該当する、という建付けになっている。この辺は古賀市とつくりが違うところである。３ページは情報端末に関しての管理規程の資料となっている。この中でテレワークに該当する部分は、右列の支給品以外の情報機器端末のところだと考えている。基本的にテレワークでは、支給品以外の情報機器端末であれば、機密性２にしか使えないというのが原則とされている。しかし、※１に、機密性２かつ関係者限り以上の情報は暗号化またパスワードで保護する、※２に、例えば、端末に情報を残さないものや、印刷やクリックボードのコピー等が制限されるようなものであれば、テレワークの際に、支給品以外の情報端末でも、機密性３の情報を利用できるというようにされている。

そして、この情報を踏まえて、古賀市でどの程度の機密情報をテレワークで使うことが許されるかということを考えてきたところである。

諮問内容の詳細についてだが、コロナ禍に入り、一部の部署で試行的にテレワークを実施しており、その中で、どうしても他の職員とファイルを共有しながら作業することが、業務の効率的な運営上必要になってきた。このような中で、どのような個人情報を取り扱うことが認められるかを検討する必要が出てきた。

そして、デジタル推進課としては、かなり強固なセキュリティー対策を講じているが、どのようなセキュリティー対策を講じても、最終的にはセキュリティーリスクをゼロにすることはできないと考えている。そのため、今回諮問したい内容というのは、誤解を恐れずに言えば、万が一情報が漏洩しても、どの程度であれば許容されるかという事になるのではないかと思われる。そしてこれらは行政に限った話ではなく、民間の企業等であっても、仕事をする以上、一定程度の個人情報は扱うこととなる。

配付資料の重要性分類ごとの情報資産をご覧いただきたい。重要性分類ごとに例示をしている。具体的にどのようなものが重要性分類の１、２、３、４に当たるかというのを記載した資料である。

重要性分類については、個人情報及びセキュリティー侵害が住民の生命財産等へ重大な影響及ぼす情報というものを重要性分類 1 としている。これに当てはまるものが、マイナンバーの情報や、住民基本台帳の情報、課税や滞納の情報、生活保護の情報、虐待の情報等であると考えている。

重要性分類２として、例えば住所等が記載された委員名簿などがある。

行政が扱う以上は個人情報をゼロにするのは難しいが、このような区分の中で、どこで線を引いてテレワークで利用させるのかということについては、強固なセキュリティー対策を講じているので、基本的には重要性分類２まで認めてよいのではないかと考えている。そして、基本的にはマイナンバー情報等は別のネットワーク上にあるが、一時的に情報を別のところから持ってくる可能性もあるため、このような情報については、ファイルのパスワード等を付与することで、万一、職員以外の者が見ようと思ってもアクセスできないような措置を講じればいいのではないかと考えているところである。

（委員）

画面転送方式というものがよく理解できないので、教えていただきたい。

（説明者）

画面転送というのは、ビデオカメラで映しているようなイメージ。そのため、自宅のパソコ

ンで操作しても、その映像のみが写っている状態で、映像はリモコンのようにマウスで操作していることになる。自宅のパソコンには一切データが残らない。全て職場のパソコンで操作する形となっている。例えばシステムを使う、ファイルを開く、そういったものも、職場のパソコンで開いて、開いた画面だけを、自宅のパソコンから見に行くという形であり、そういう意味で画面転送という形になっている。

（委員）

今の説明だと例えば、業務でデータを書換えないといけないという場合は、それはできないという理解でよいのか。

（説明者）

書き換えは可能である。書換えは可能だが、あくまで遠隔で職場のパソコンを操作して書換えている形となる。

（委員）

テレワークをこのような形で進めてきた背景にはコロナのことがあったと思う。この先はテレワークを進めていく方向で考えているのか。

（説明者）

これについては、市長の方針でもあるが、やはり今後は色々な働き方を模索していくべき時期だと考えている。例えば今後は、子育てをしながら、介護をしながら仕事をするという場合であっても、テレワークであれば、離職しなくても続けていけるような場合もあると思うので、そのような面からも、今後コロナが終息したとしても、引き続き行っていければと考えているところである。

（委員）

職員が自宅で業務をする場合に、周りから画面を見られる可能性もあるので、自宅で働く環境について何らかのガイドラインはあるのか。

（委員）

ガイドラインを作成しており、例えば自宅で勤務する場合には、個室的な場所ですること、離席する場合には、ログオフしたり、スクリーンセーバーになったりする機能を使って、横から見られたりしないような対策を講じることという条件を設けているところである。

（会長）

今回の答申は条例に合致するかという話ではなく、今回の対策で十分に情報保護されているかということを我々がある程度納得できるかという部分にかかってきているのではないかと思っている。そこで質問だが、今の話のように、テレワークで後から見られたりするというケースも当然あるわけだが、テレワークを自宅でするとは限らず、サテライトオフィスのようなところで行うということも将来的には考えられるのではないかと思うが、そのような場合の運用については規則が作られているのか。

（説明者）

在宅勤務等の要領については人事秘書課が作成しているところである。基本的に現時点では、テレワークは自宅で行うという形で制限を設けている。もしサテライトオフィスのようなところでする場合については、それに応じた対策を講じる必要があると考えている。

（会長）

テレワークで使用するのは、VMware 等を使うということか。

（説明者）

VMware ではなく、NTT と IPA が作成して無償で民間企業や自治体が使えるシステムであるシ

ンテレワークシステムというものを使っている。
（会長）
シンテレワークシステムというのは、いわゆる仮想デスクトップというようなものを提供するようなシステムなのか。
（説明者）
イメージとしてはVMwareに近いようなものと思う。VMwareも画面転送なので、それに近いものと御理解いただければと思う。
（会長）
1番普及しているもので言えばリモートデスクトップだと思うが、そのような使い方をするというようなイメージで良いか。
（説明者）
そのとおり。シンテレワークシステムは、リモートデスクトップの機能を拡張して使っているようなものと思っている。リモートデスクトップだけでは、例えばパスワードを漏えいしたときの体制がとれないことから、ワンタイムパスワード等を使っていると御理解いただければと思う。
（会長）
実際に職員がテレワークを始める際に、どのようにワンタイムパスワードを入手して接続するのかという流れを教えていただきたい。
（説明者）
順を追って説明する。まず自宅においてシンテレワークシステムでプログラムを起動する。そして、パスワードを送信すると、NTTのサーバーから登録済みのメールアドレスに、その時限りのパスワード（ワンタイムパスワード）が送られてくる。そして、そのパスワードを入力することで、まず職場のパソコンにつながることができる。さらに職場のパソコンでは、再度仕事で使っているパスワードを入力して、ようやく市の庁舎の情報系ネットワークに入ることができる。
（会長）
実際にデータを操作するのは、職場のパソコンということだと思うが、そういうことであれば、職場のパソコンは、常に電源が入っており起動している状態のまま置かれているということでよろしいか。
（説明者）
はい。職場のパソコンは電源が入っている状態であるが、基本的にはログオフした状況で置かれている形。そして、シンテレワークシステムで接続した瞬間に画面が全てオフになる。
（会長）
その接続するパソコンというのは、各職員の机上にある、いわゆる個人用職場のパソコンということでよろしいか。
（説明者）
そのとおりである。
（委員）
テレワークにおいて現在どの共有フォルダーにアクセスできる状況になっているのか。
（説明者）
共有フォルダーについては、基本的には、課ごとに設定したフォルダーにアクセスすることを認めている。

（委員）
課ごとのフォルダーにはⅠ～Ⅳの情報が含まれているのか。
（説明者）
課によっては含まれている。既にテレワークを実施している部署については、個人情報が含まれるものについては、パスワードを付与するかもしくは共有フォルダーから移動するかという措置を講じているところである。
（会長）
分類分けによる制限は、課や個人に任されているのか。例えば、自宅に帰る前に、分類Ⅰに属するデータを自分のパソコンにコピーするなどして自宅に帰り、そこからまたアクセスした場合、分類Ⅰのデータが見えるということか。
（説明者）
現時点で共有フォルダーの重要性分類ごとのアクセス権付与というのができていないので、共有フォルダーにあれば、基本的に無制限で見ることができる状況となっている。
（会長）
要するにファイルごとのアクセス制限はできていないという理解でよいか。
（説明者）
デジタル推進課で個人情報が含まれているかどうか、全ファイルを検索し、実際に個人情報が含まれている場合には、各課で移動、パスワード設定、もしくは削除するよう処置をしてもらっている。そのため、現時点ではファイルごとは何らかの措置が講じられていると思う。
（会長）
情報を分類はしているが、システム的に分けているのではなく、人の手で分けているということでよろしいか。
（説明者）
そのとおり。
（委員）
先ほどの発言で「講じられていると思う。」というのが気にかかっている。今後、この制度を導入して重要性分類ごとに利用についてルールを決めたとしても、課ごとに事前の措置が講じられているという前提がないと意味がない。何らかのチェックをする必要があるのではないか。
（説明者）
ファイルに個人情報があるかどうかということは、昨年度１月～２月頃にシステム上で、各課が持っている全ファイルにアクセスした上で、ツールを使って確認し、該当するリストを各課に配布した。そして、各課で措置し、その完了報告を受けている。この報告があった部署についてはテレワークしても差し支えないという形で対応している。
（委員）
ツールを使ってチェックすれば、いつでも措置が講じられているか確認できるという理解でよいか。
（説明者）
はい。
（会長）
ツールでのチェックは今後も定期的に実施するのか。
（説明者）

このツールはかなり高価なので、どの程度の頻度で使えるか分からないが、定期的にチェックする必要があると考えているところである。

（会長）

先ほどの話のように、自宅に帰る前に重要なファイルを自分のパソコンの共有フォルダーに移動させれば、分類が用をなさないので、運用規則等をある程度細かいスパンで決定するような運用方法を検討していただきたい。それと同時に、最終的には、システム的に重要性分類を決めたファイルは共有フォルダーの移動や保存ができないように対策を講じてほしい。

（説明者）

補足だが、ファイルの移動等については、SKYSEA というソフトを使っており、どの職員がファイルにアクセスし、コピーしたか等、履歴が全て残っている。そのため、万一情報漏洩が発生した場合は、そういったログをたどって確認することが可能となっている。

（委員）

今回の諮問は、共有フォルダーに関してどこまでパスワードをかければいいかという内容であると思うが、重要性分類がⅠ～Ⅳまであって、Ⅲ以降は公開しているものなので、ⅠのみにするかⅡまでかけるかというところで検討したものと思う。セキュリティー自体はすごく強固だと思うので、そもそも漏洩することはめったにないことだと思うし異論はないが、分類Ⅱまでパスワードをかけると事務的にすごく煩雑になる等の問題があるので、分類Ⅰのみにしたいという思いがあるのか。

（説明者）

仮に分類Ⅱまでパスワードをかけるとすると、普段テレワークでないときもパスワードを入力する必要が出てくるので、かなり煩雑になると考えている。

（会長）

ファイルにパスワードをかけるというのは具体的にはどうしているのか。

（説明者）

使用しているファイルは、エクセルやワードが多いが、これらのファイルを開くときに入力するパスワードを使用している。PDF や CSV、テキストファイル等については、暗号化付 ZIP ファイルを作る形で実施している。

（会長）

暗号化されているファイルも共有フォルダーにあれば自宅からでも操作することはできるのか。

（説明者）

ファイルを操作することは可能である。パスワードを知っている職員であれば、パスワードを入力することで開くことも可能となる。

（会長）

実際に使う自分の机上の職場 PC はインターネットにはつながっていないという事だが、例えば USB メモリや CD、DVD ドライブは使えるようになっているのか。

（説明者）

テレワークをする場合、USB等がつながっていれば見ることができる。また、イントラネット内に共有フォルダーがあるので、その中のファイルも見ることができる。個人の PC のハードディスクの中も見ることができるようになっている。

（会長）

職場 PC に USB メモリを挿せばその内容を見られるし、CD や DVD を入れればその内容が見られ

るという事でよいか。
（説明者）
そういうことである。
（会長）
インターネット上から落としてきた何らかのアプリケーションを USB ドライブや CD に焼くなどして、それを職場に持ってきて職場 PC の中にインストールすることは可能ということか。
（説明者）
可能ではあるが、アプリケーションを入れる前には、デジタル推進課への申請が必要となっている。
（会長）
アプリケーションをインストールしたことを、デジタル推進課がリモートで認識することできないのか。
（説明者）
SKYSEA というソフトで、ログを確認することができる。
（会長）
SKYSEA を使うというのは事後処理の話であって、リアルタイムで分かるものではないということか。
（説明者）
はい。以前は、プログラムのインストールを一切できないようにしている状況で、必要に応じて、管理者権限を外して、一時的にインストールを許可するという運用をしていた時期もあった。しかし、その運用だとどうしても頻繁に管理者権限で入る必要があったので、現在は届出さえあれば任意にインストールできるような状況になっている。
（会長）
デジタル推進課への申請以外には、実際にインストールしたかどうかの確認はしていないということか。
（説明者）
はい。
（会長）
エクセルファイルや ZIP ファイル等に関して、世の中には解析ソフトが存在するので、そのような解析ソフトをインストールしたり、あるいはインストール不要のものを職場 PC の中に入れておいたりすれば、家から解析してファイルが開けるのではないかという事を危惧している。そのようなことは想定されていないか。
（説明者）
パスワード解析については、例えばプログラムに長けた職員であれば、自分でプログラムを組んでエクセルのマクロで実行することも可能となっている。しかし、それら全てをデジタル推進課で監視するのは正直難しいと考えているので、その辺りについては、職員の性善説に任せているという状況である。
委員の皆さんが心配されているのは、住基情報などの重要な情報が漏洩しては困るということではないかと思うが、最初に説明したように基本的にネットワークは３つに分離しており、マイナンバー等の情報は情報系のネットワークには入ってこないという建付けになっている。もしも情報があるとすれば、一部を取り出したような情報となっており、取り出す場合には事前にデジタル推進課に申し出が必要となっている。そして、デジタル推進課の執務室で USB に

ダウンロードするという流れとなっているので、このような部分は問題がないのではないかと考えているところである。
（会長）
SKYSEA というツールでログを取られているというのは、職員は分かっているのか。
（説明者）
明確にログを取っていることは伝えていない。
（委員）
アプリケーションのインストールについては、テレワークが始まったから取扱い方法が変わったわけではなく、以前から自由にインストールできないようにして、市役所内のパソコンを保護する方策をとっているということでよいか。
（説明者）
そのとおり。
（委員）
古賀市の職場におけるパソコンの管理や倫理の話と、今回、リモートで勤務するときの話が出ていて、かなり広い範囲で議論されているので、テレワークに関してというところに絞った方がいいのではないかと思う。また、データは物理的には漏れないということだが、やはり気になるのは各職員の倫理観の部分で、極端な話でいえば、自宅で機密性の高い情報を画面に出して写メで撮ってしまえば問題なので、自宅で一人になったときにきちんと守るということを徹底していただきたい。システムは強固だということは理解できるので、個々の職員の自宅での対応に関してはきちんと見ていただきたいと思う。
（説明者）
例えば、テレワークの運用基準の中で明記するなどの対応をしていければと思っている。
（委員）
テレワークが始まって以降、今まで１年以上の間に何か問題があったということはなかったということでよいか。
（説明者）
はい。古賀市として問題は発生していない。
（委員）
もしこれで決まった場合、例えば情報公開で開示する場合には、重要性分類に関する資料はどれが示されることになるか。
（説明者）
重要性分類というのは、個人情報保護条例ではなく、古賀市情報セキュリティー対策基準というものに基づくので、開示請求等と必ずしもリンクしているものではないと理解していただければと思う。
（会長）
今回の諮問内容について、重要分類Ⅰのみにパスワードを付与するということにしたいということだが、個人情報の保護について、職員の倫理観に寄っているという話が出ている。セキュリティーを考えるときに倫理観をよりどころにするのは不安があると思う。デジタル推進課の方で、システムやその運用について検討していただければと思う。SKYSEA というログを取得するソフトについては、職員に知らせずにログを取得していても役に立たないので、きちんとログを取得しているという事を職員に伝えることによって抑止力になると思う。このようなことについて、デジタル推進課で研修やテレワークをする上で、運用規則や研修内容の中で職員

に伝え、情報漏洩はできないという事を教育した上で運用していただければと思う。
分類Ⅰのみにパスワードを付与するという形は私としてはそれでよいのではないかと思うが、実際の運用について不安に思うところもあるので、今後の改善や、より良いセキュリティーのレベルを望みたいと思う。
他にご質問等ないか。
→なし
（会長）
今回の諮問第２号（１）については、当該事項について個人情報保護のために必要な措置が講じられていると認めるかという点については、個人情報保護のために必要な措置が講じられているということで、審議会としては結論として判断したいと思う。よろしいか。
→全員賛成

（会長）
諮問第２号（２）LINE 及びLoGo チャットにおける個人情報の取扱いについて、古賀市個人情報保護運営審議会条例第２条第１項の規定に基づく諮問であり、具体的には当該事項について個人情報保護のため必要な措置が講じられていると認められるかについて意見を求められている。まず、担当課より説明をお願いする。
（説明者）
まず、LINE についてはニュースでも騒がれたように、LINE のデータサーバーが国内になく、運営会社が自由にメッセージの内容を閲覧できる状態であるということから、機密情報を扱うには心配があるという状況であり、国がガイドラインを示しているところである。古賀市においても国の通達に沿った取扱いを考えているところである。
次に、自治体 DX が叫ばれており、例えば電話や電子メールに換わってビジネスチャットが普及してきている現状があり、古賀市においても LoGo チャットという LGWAN 環境下で使えるビジネスチャットを使用している。これは LINE とは異なりデータサーバーが国内にあり、運営会社であっても閲覧することができない、かなり秘匿性の高いサービスである。
このように、秘匿性の高低に応じて情報資産を取り扱える範囲を分けて運用することで、適切な措置といえるかという事を諮問させていただいている。
具体的には、秘匿性の低い LINE 等のサービスについては、基本的に重要性分類Ⅲ、Ⅳのみとし、秘匿性の高いサービスについてはⅡ、Ⅲ、Ⅳを利用可能とする。秘匿性の高いサービスの場合、例えば重要性分類Ⅰの情報を使用する場合にはフルネームではなく、A さん、B さんのような形で書くことで使用を妨げないのではないかなと考えている。以上のような形で今後、取扱いをしていければと考えているところである。ご審議のほどよろしくお願したい。
（委員）
確認だが、表では秘匿性の高いサービスの重要性分類Ⅰは×になっているが、そうではなくて、一部を秘匿化するなどの措置を講じていれば利用可能としたいという趣旨ということでよいか。
（説明者）
基本的には表のとおりである。ただし、秘匿化する、つまり、個人情報であることが分からなければ、ビジネスチャットで使ってもいいと私は考えている。あくまで、そのままの情報を使う場合はこのルールで取り扱いたいという諮問と受け取っていただければと思う。
（委員）

そうであるなら逆に秘匿性の低いサービスの方も、例えば匿名化すれば使ってもいいという考えであるということか。

（説明者）

現時点ではまだ明確には決めていない。

（会長）

秘匿性の低いサービスというのが LINE のことで、秘匿性の高いサービスは LoGo チャットのことだという認識でよいということか。

（説明者）

はい、そのとおり。また、国の方も LINE 等の業務利用は控えるように通達しているところである。

（委員）

秘匿性の低いサービスの典型例として LINE が挙がっているが、LINE 以外にも秘匿性の低いサービスに当たるものを将来的に使う可能性もあると考えているということか。

（委員）

そのとおりであり、また、LINE は現時点では秘匿性が低いサービスに位置づけられているが、データサーバーを国内に置く、メッセージを見られない、そういう対応がされれば、秘匿性の高いサービスに変わると考えているところである。

（会長）

今の話であれば、取得性の高いサービスか低いサービスかというのは、サーバーが国内にあるかどうかという話のように思えたが、違うか。

（説明者）

国が、LINE は秘匿性が低いと判断したのは、サーバーが韓国や中国などの国外にあるという事が 1 つ。中国などでは、国から情報を出せと言われれば出さなければならない状況であり、国内情報が筒抜けになるといった心配がある。このことから、秘匿性の高いサービスであればサーバーは国内にあるべきという考えを国が持っている。それに加えて、運営会社が自由にメッセージを見ることができるようなサービスは、よろしくないという考えを持っている。その２要件に該当するものは秘匿性が低いと考えているところである。

（委員）

LINE と LoGo チャットのどちらを使用するかという話だが、基本的に業務で使う場合は秘匿性を高いサービスを使って、どうしても秘匿性の低いサービスを使わないといけない場合だけ利用するというような、基本的な発想はないのか。

（説明者）

原則論としてデジタル推進課としては秘匿性が高いビジネスチャットの方を使用するように伝えている。また、基本的には庁舎内のデータのやり取りであればグループウエア上でメッセージを送受信できる形となっている。しかし、自宅等で PC に接続する環境がない場合に連絡する手段としては電話以外になく、このような時に使用できるのがビジネスチャットであると考えている。今までは LINE 等で連絡していたケースもあったが、そのような運用は止めた方がいいという状況があり、基本は LoGo チャット等のビジネスチャットに変える方向で考えているところである。しかし、予算の関係もあり、全職員に配布が難しい現状もある。

（会長）

LoGo チャットは有償だと思うが、個人のスマートフォンにインストールすることは可能か。そして、インターネット回線を使って LoGo チャットを使用することができるのか。

（説明者）
個人のスマートフォンでの利用も可能となっている。ただし、その場合には LGWAN という国、政府専用の回線を通じてのみ使用できる。
（会長）
LINE というのは非常にセキュリティー的に弱いものだと思っているが、それ以外のものを使う考えはないか。例えば、非常にセキュリティー的に高いと言われ、LINE よりも機能豊富な「シグナル」というソフトウエアの使用は考えていないか。
（説明者）
シグナルというソフトウエアを承知していないが、LoGo チャットを使用している経緯として、自治体はインターネットに直接接続できないという状況があり、その中でも通常のイントラネットの中でメッセージのやり取りができるのが、現在 LoGo チャットしかない。シグナルというのがインターネット非接続で使用できないのであれば、使用する候補には挙がらないのではないかと思う。
（会長）
LoGo チャットは問題ないと考えている。LoGo チャットはサーバーの内容を見ることができないということなので、おそらく端末間で暗号化され復号されないで通信されるものではないかと思う。また、サーバーの中には暗号化されたものが入っているということではないかと思うが、そういうことか。
（説明者）
恐らくそれは違うのではないかと思われる。LINE は運営会社がメッセージを見るパーミッション（アクセス権）を持っている形で、LoGo チャットのようなサービスは運営会社にメッセージを見る権限を持たせていないというデータベースの割り振りをしている形となっている。それによって見られるか見られないかという違いが出ている。
（会長）
そのような形であればサーバー側で内容確認をしようと思えばできるという事でよいか。
（説明者）
はい。契約に当たってそのようなことが無いような形で契約している。
（会長）
契約上の話ということで、理解した。先ほどのシグナルというのはオープンソースのメッセンジャーソフトであり、メッセージが相手の端末に到達するまで全て暗号化された状態で行くので、運営側が見ることができない仕組みになっており、非常に秘匿性が高い。このような、より秘匿性の高いサービスを、LINE に替えて利用する事は検討されていないか。
（説明者）
現在、システム的にはクラウドサービスという使い方がメインになってきているし、自治体の場合はビジネスチャットの使い方としては、現場の職員のスマートフォンと市役所にいる職員のパソコンとがメッセージをやり取りする使い方も想定しているため、シグナルのような Peer to Peer のサービスには合わないのではないかと考えている。
その他のサービスについては、システムを開発する会社が似たような新しいサービスを開始するという話も聞いている。そのようなシステムに乗り換える可能性はある。また、国の方針でインターネットには一切接続しないというのが原則であるが、この制限が緩やかになる可能性もあるので、その場合は別のサービスの使用を検討する余地もあるのではないかと考えている。

（委員）
確認だが、今議論しているのは、令和３年５月１１日付の「古賀市における LINE サービス等の利用の際の考え方」の表の、③の個人カウント等業務連絡等に利用する場合の、情報の分類のところを諮問書の裏の表で扱ってるという理解で間違いないか。
（説明者）
そのとおり。
（委員）
職員さんの実際の感覚からして、これが仮に導入されるとなると頻繁に使えるものなのか。
（説明者）
既にもう利用しているが、その中で明確に機密性情報をどこまで使っていいかを示しておらず、一般的には機密性情報は使っていないとは思うが、どこかのタイミングで明確に示す必要があることから、今回諮問させていただいたところである。
（委員）
この手のサービスで機密性の高い、匿名性の高い情報をやりとりすること自体が想定できず、日常の業務連絡等における使用しかイメージしてなかったため、重要性分類Ⅱの情報も可能にする必要性があるのか疑問に思っていたところである。ただ、どうしても使用しないといけない場合に、ガイドラインがないと、ラインが引けないので、表にあるような形で今回設定するという趣旨は理解した。
（説明者）
補足だが、一般的には重要性分類Ⅲ以下の使い方がメインではないかと思うが、委員が言われた通り、例えば利用が進んでいくと、滞納や差押えをする場合の連絡などもチャットを通じて行う可能性もゼロではないのではないかと思う。滞納等の話については機密性情報Ⅰであることが多いと思うが、それ以外の例えば委員の名簿を送る必要があることも考えられる。委員名簿で住所が入っていることもあり、そういったものを送れなくなってしまうこともあるので、明確に基準を設けておいたほうがいいのではないかと考えているところである。
（会長）
本来は LoGo チャットをメインで使ったほうがいいけれども予算的に厳しいということで良いか。
（説明者）
予算面の都合もあるし、職員にとって LINE の方が普及しているということもあり、同僚間でのやりとりは LINE がやはり多いという現状がある。ただその中で、無制限に使わせるのは問題があると考えているところもまた事実である。
（会長）
今回話を聞いて思うのは、職員のセキュリティーに関する教育というのを、倫理観だけに頼るのではなく、何らかの教育をしていただきたいということ。職員がどのような倫理観を持つかというのも大事であると思うし、本人が意図せずにインシデントを起こしている可能性もあるので、職員の倫理観の醸成ということも含めて行ってほしい。そうでなければ、なかなか安心して対策を講じていると認めるとは言いづらい部分があると思う。ただ、重要性や必要性はあると思うので、問題なく運用できるための裏付けとなるきちんとした教育や運用方針を制定し、例えば毎年１回必ずセキュリティー教育を行う等ということをやっていただいて、その記録をエビデンスとして残して、将来何かあった時のためにもそのようなシステムで行ってほしい。当然、中途で採用した方や、外部から来ている職員に対しても実施していただくよう申し

上げたい。
（説明者）
教育に関しては、現在でも行っている。まず、新規採用職員については新規採用職員研修の中で行っており、また、全職員向けのセキュリティー研修を数年に１回のペースで、国の J-LIS という機関のプログラムを使って実施している。しかしながら、倫理観だけに頼らないような更なる啓発には取り組んでいきたいと考えている。
（会長）
教育を行っているということは理解した。数年に 1 回という数年というのは何年に 1 回のことか。
（説明者）
３、４年に 1 回だったかと思うが、昨年に実施しており、それとは別に今年も実施する予定となっている。今年は全職員対象ではなく、職員を絞ってのオンライン研修を検討しているところである。
（委員）
職員が LINE を導入していて使用頻度が高いのは分かるが、委員としてではなく、一般の市民の感覚からして、たとえ公開されている情報や、重要性分類Ⅲや Ⅳの情報でも、このような情報が LINE 上でやり取りされていることに関して違和感を感じないのかどうか一度検討いただきたい。業務で必要なのは分かるが、LINE というものに対する今の信用性を含めて考えると、業務でやり取りするものに関しては、きちんとしたものでやってほしいというのが一般的な市民の気持ちではないかと思うので、便利なのは分かるが、市民の視点も加味した上で、あくまでも原則は LoGo チャット等秘匿性の高いツールを使うのが大前提ではないかと思う。
（会長）
私も同様の意見。使いやすさや慣れているという理由で LINE を使うのは危険ではないかと思う。LINE の規約を読んだことがあるが、サーバー上の情報を国外に出す可能性があるという文言が書いてある。韓国とベトナムに流すことがあるということが堂々と書いてあるものに対して、使うのはどうかという思いが正直ある。規約の内容から LINE 内の情報はすべて他国へ流出していることを前提に使用する必要があると思う。そういったことを踏まえると、慣れているから使うというのは引っかかるところである。職員研修等によって新しい安全なツールに慣れていただき、別のツールに変えていくということも検討した方がいいのではないかと考える。確かに市民として、仮に重要性分類Ⅲなどであったにせよ、自分の名前などが流れているというのは嫌だなと思う感情もある。皆さんもそのようなイメージは持たれているのではないかと思う。一度検討いただきたい。
（説明者）
国が示すガイドラインの中で、機密性を有する情報については LINE での利用を控えるようにとなっている。これに準じて、私どもとしては重要性分類Ⅲ、Ⅳに関しては機密性を有しないと考えることから、LINE で利用しても良いのではないかという判断をしている。しかしながら、業務上のやり取りなので、基本的にはイントラネット内のグループウエア上のメッセージもしくは LoGo チャット等の秘匿性の高いサービスを利用することとしており、副次的に LINE を利用することはやむを得ないという感覚で考えている。
（委員）
私としてはこれだけ LINE が普及している中で使用を禁止することによって、職務上の連絡を黙って LINE 上でやるような状況になるよりは、LINE の使用を否定するのではなく、LINE を使

用しても不都合が生じないような形で明確な基準を設けることで、利用する事を許可する方が現実的ではないかと思う。この基準を周知することで、職員が、個人情報が入ったものは絶対に使ってはいけないということを知る契機にもなると考える。
（説明者）
以前は緊急連絡を電話で行っていたが、現在はメールやLINEで一斉送信というのが主流になってきている。それは、LINEであれば、日頃使っているため見落としが少ないということがある。緊急連絡は機密情報には当たらないので問題ないと考えている。このように、普段使いしているツールをある程度認める方が、業務の運用上は良いかと思う。また、災害の対応などを考えると、複数の手段を確保するというのが災害対応の基本であるので、LoGoチャットが使えなくなった場合のことを考えると、複数の手段を確保するためにLINEについても一定程度、規程を設けた上で利用を認める方が現実的ではないかと考える。
（会長）
他に意見や質問等はないか。色々と説明を受けた上で、セキュリティー上ある程度のレベルはきちんと確保されているというふうに審議会としては考えたい。今回の諮問②（２）LINE及びLoGoチャットにおける個人情報の取扱については、適切な措置が講じられているという結論としたい。よろしいか。
→反対意見なし
（会長）
レジュメの６、７については、通常毎年報告を受けていることなので、内容を各自見て、疑問点等あれば事務局の方に個別にメールやFAX、電話で問合せいただければと思う。
（委員）
１点確認したい。職務上請求の申請書の開示依頼がいくつかきているが、これは同じ人からか。
（事務局）
それらはそれぞれ違う人からの請求となっている。
（委員）
本人以外から住民票の請求があったことが分かった時に誰が請求したのか気になる方が多いのではないかと思われる。
（委員）
個人情報開示請求処理状況詳細一覧の１６番の不開示理由の「１７条第２項」というのは何か。
（事務局）
請求内容としては、申請書及び添付書類であったが、存在したのは申請書のみで、添付書類については不存在であったため、「第１７条第２項」ということを記載した。
（委員）
不存在の理由になるか疑問に思うところ。
（委員）
ちょっと違和感はある。恐らく、資料が存在するが開示しないという時に、その理由を通知しないといけないという規定になるので、存在しない場合は根拠条文が無いのではないかという気がする。
（事務局）
第１７条に不存在の時どうするかというようなところが直接明示されているとは言い難いか

もしれないが、１７条第２項の後半部分で「前条の規定により、開示請求を拒否するとき及び開示請求に係る個人情報を保有していないときも同様とする」というふうになっているので、所有していない時にも通知をするということで、この規定に基づいて不存在だということを認定して通知したという形になると考えている。

（委員）

第１７条の規定は通知するというところがメインなので、不存在の場合の根拠条文としては適切ではないように思われるが、他にどこが該当するかというと難しい。趣旨は理解した。

（会長）

今までも不存在の場合、同様に記載されていたと思うが、疑問点として挙がらなかった。言われてみれば不適切な気もする。

（委員）

市政情報の開示請求の方も同じで、一覧の３１番や４２番に関して、決定内容の欄は部分開示、不開示情報の欄は不存在となっていることに違和感がある。部分開示というのは基本的に一つの文書の中に見せられない部分がある場合に黒塗りして出すというものであるが、不存在というのは正確ではないと思う。おそらく複数の請求があった場合に、そのうちの一部は出せるが一部は不存在という事だと思うが、それは全部開示と不存在というのが適切であって「不開示」という表記が正しいのか疑問がある。対処方法としては全く問題ないと思うが、表記の仕方を改めた方がいいと思う。

（会長）

事務局の方で今後検討していただきたい。

（事務局）

記載方法を見直していきたい。