

会議の名称	平成30年度第1回個人情報保護運営審議会		
開催日時	平成30年4月19日(木)午後6時25分～9時10分		
開催場所	東村山市役所 本庁舎3階 庁議室		
出席者 及び欠席者	<p>●出席者： (委員) 臼井雅子会長・日下直喜委員・嶋田節男委員・田村初恵委員・當間丈仁委員・水越久吉委員 (市事務局) 東村総務部長・高柳総務部次長・武藤総務課長・湯浅情報公関係長・鳴海情報公関係主任</p> <p>●欠席者： 無し</p>		
傍聴の可否	傍聴不可	傍聴不可の場合はその理由	会議の中で、東村山市情報公開条例第6条各号に規定する非公開情報(個人情報や、市の情報セキュリティ対策の詳細情報など)が含まれる事項を審議するため
会議次第	(1) 会長挨拶 (2) 諮問書授受 (3) 諮問審議 ・平成30年度諮問第1号 「乳幼児医療証及び義務教育就学児医療証の印刷及び封入封緘等業務委託」(子育て支援課) ・平成30年度諮問第2号 「住民情報系基幹システム保守業務委託における仕様変更(リモート保守)」(情報政策課・保険年金課) (4) 報告 ・小学校通学路への防犯カメラ設置追加(学務課) ・「在宅医療連携推進事業委託」における受託者の追加(健康増進課) ・ペイジー口座振替受付サービス機の導入(収納課) ・東村山市個人情報保護に関する条例・同施行規則の改正(総務課)		
問い合わせ先	総務部 総務課 情報公関係 担当者名 湯浅・鳴海 電話番号 042-393-5111(内線2317) ファックス番号 042-390-6227		
会 議 経 過			
(1) 会長挨拶 平成30年度第1回個人情報保護運営審議会の開催となります。 世間では文書管理に関する問題が毎日のように取り上げられており、国のみでなく都道府県や市町村でも、文書管理について改めて振り返られることも多いかと思えます。国の問題ではありますが、地方自治体への影響もお察し申し上げます。 個人情報保護に関連しては2点のニュースが流れております。 まずは、Facebookから870万人分の情報が流出し、そのうち日本人が80万人とのことです。次に日本年金機構による業務委託について、業務委託をす			

ること自体に問題はありませんが、契約違反の再委託をし、再委託先が海外の会社であったとのこと。国外の法治下にある会社に何故再委託をしたのか、それも日本国民の個人情報が多く含まれるものであります。社会保険庁の時代に消えた年金問題を起こし、日本年金機構へと組織の変化があつたにも関わらず懲りていないのかと、本当に怖いところでもあります。

この委員会においても、安全性の確認・確保をどのようにやっていくか、年度の初めでありますので改めて気を引き締めて審議していきたいと思ひます。また、各委員にもそのようにお願いしたいと思ひます。

(2) 諮問書授受

東村総務部長から臼井会長へ諮問書を手渡す。

(3) 諮問審議

○「乳幼児医療証及び義務教育就学児医療証の印刷及び封入封緘等業務委託」について、諮問どおり行うことを「可」とする。

※委員意見及び子育て支援課の回答

- 別紙1「作業手順」を見ると、市が引き抜きリストを作成して紙媒体で受託者に渡し、受託者はこの引き抜きリストで指示された者の封筒を引き抜き、段ボールケースに梱包し納品するとある。引き抜きの対象となる者と引き抜く理由は何か。
 - 医療証の印刷から発送までの期間に転出した者など、医療証送付が不要となった者を引き抜く。引き抜いた封筒は市へ納品してもらう。
- 引き抜いた封筒を市へ返却してもらうことについて、仕様書等に記載はあるか。
 - 仕様書の6. 履行内容 (8)②において、「印刷、出力等について、ミスした帳票等は市に納品する。」と記載している。
- 念のため、ミスした帳票のみではなく「送付不要になったものも含め一切」を市へ納品する旨明記していただければ、安全性が高まると考える。
- 諮問書 P. 2の(2)に個人情報取扱責任者を1名配置するとあるが、当該責任者の役割としてどのようなものを考えているか。
 - 本業務を遂行するにあたり、データの出力から納品までに関わる一切の工程を管理監督をする役割と考えている。
- 役割が明確になっているのであれば、当該責任者の役割や責任を明記し、有事の際に当該責任者が処理するとすべきである。
- 個人情報取扱責任者は、作業担当のリーダーとしてやるといった形をイメージしてこのように記載されているということか。
 - そのかたちである。
- そうであれば、今●●委員も言われたとおり、役割が明確になるよう、仕様書に追加明記してほしい。
- 受託者への牽制の意味も含め、事業所内へ市が立ち入り検査が出来る旨を仕様書等に明記してはどうか。また、受託者がどのように業務を遂行しているか、市職員が実際に確認に行けると良い。

(情報公開係長)

「個人情報の取扱いに関する特約条項」第9条に、「甲は、取得個人情報の保護のために必要があるときは、必要があると認められる範囲内で、乙の事務所及び

作業所等を調査することができる。」と定めており、市が受託者の作業所を検査することができることは契約書上盛り込まれている。市では、個人情報を取り扱う委託の場合、この特約条項を添付するルールになっている。

- 委託する側の市が、受託者の業務遂行状況や個人情報保護体制のチェックをどのように行うかということも大事である。単年度でなく継続する委託業務であれば、担当者の異動に備え、受託者に対するチェック項目を文書化して引き継いでいくと良いと思う。
- 個人情報保護に関する特約条項をどの所管も共通に添付するといったルールにより契約書の体裁は整ってきているが、実態に市職員が受託者の体制をどのようにチェックをするかは各所管により事情も異なると思う。前任者の経験を文書化して積み上げていくと良い。
- 総務部にお聞きしたいが、市役所のなかには、委託で業務を行う場合のノウハウやヒヤリハット経験、過去の受託者の業務遂行能力などの情報を蓄積し、各部署が委託する場合はそこに相談して支援を受けられるといった部署はあるのか。民間企業だと購買部など外注をやる部署が一か所必ずあり、各部署はその支援を受けながら外注をかけるという構造がある。世間では元々処理能力がないところと委託契約を結んでしまうといった業者選択時点での誤りが見受けられることもある。現在アウトソーシング抜きで市の業務を運営していくことは考えられないが、そういった部署はあるのか。

(総務部長) 契約業務における業者選定の話としてお答えする。事業者の処理能力を見誤った発注受注がありうるのかというご懸念について、業者を選定する場合には、事前に副市長を委員長とする業者選定委員会にかけることになっており、選定委員会では指名予定業者の資本金や従業員数、受注実績などの情報を基に業務遂行が可能か検討する。このように見極めたうえで業者を選定しており、処理能力の無い業者に委託することにはないようにしている。

- おそらく選定の際に、他自治体との契約関係等も調べていると思われる。では、市職員自身が業者のヒヤリハットに気が付いたときに伝えられる文化はあるとみて良いか。

(総務部長) ある。所管のみではなく、市全体で情報が共有される仕組みとなっている。

- 一般論として、契約の相手方が適正な受託者になり得るか否かの情報はきちんと庁内で共有されているということは分かった。では次に、市が委託する側として、個人情報保護に特化して受託者のチェック体制をどうするか、こういう風に業務仕様書を作ると良いといったノウハウを各所管から集約して蓄積できると良いと思う。情報公開係でとりあえずは最大公約数的なものでも良いが、徐々に集められれば良いと考えているが、いかがなものか。

(総務部長) プロポーザルなどを実施する際の共通のチェックリスト、たとえば要件定義書など、フォーマット化されているものも一定ある。委託契約の仕様書等へ組み込むこととはしていないが、市として必要な書類は揃えているところである。

- 各所管に個人情報に係る業務を委託する際の運用基準となるものがあり、さらにきちんとチェックをすべき項目が文書化され、積み重ねられていく方向に向かうようよろしく願いたい。
- 契約書や仕様書等形式的なものは整ってきているが、受託者に対する検査の規定は実効性がなければならない。履行確保のためのチェックを随所でしていくことが必要。この点を踏まえ、情報セキュリティに関する合意書(案)第1条第1項の「～内部における責任体制を構築し、その体制を維持しなければならない

い。」とあるが、責任体制をどのように構築し維持するかを事前に報告させるべきである。第2項「～必要かつ適切な管理を行うための対策基準書を作成していただかなければならない。」とある点についても、事前に市へ当該対策基準書を提出させるべきである。その上で立ち入り検査を実施して相手方に緊張感を与える、仕様書等で取り決めた作業体制が守られているかを市が実際に確認するといったことが求められている。

- 契約書や仕様書等が整えられているが、すべてが当該書類の通りといくとは思えず、それを実際にやっていただくにはどうしたら良いかを審議会も含めこれから検討していくべきかと思う。
- 今回本業務委託の対象となる人数は何人くらいになるのか。
 - 乳幼児が約7,600人、小・中学生が約9,500人である。
- これまで本委託内容の作業を何名でどの位の期間でやられていたのか。
 - 正職員6名、臨時職員が6～7名の計12、3名の体制で2週間ほどでやっていた。
- 委託先の選定について、無断で再委託が行われぬよう、業務を実行出来るだけの人数を確保している業者をきちんと選んでいただきたい。作業人数等の条件を付した入札は可能なのか。
 - 過去に他自治体で同様の業務を受託し遂行している複数事業者の声掛けして入札に参加してもらおう。業務遂行能力について情報が皆無の業者に委託をすることはない。
- 諮問書P.2に「入退室管理の行える会議室等で作業を行う」とあるが、契約仕様書にもその旨記載し、さらに「作業する場合は施錠が可能であり、作業中は施錠する」という項目を入れるべきではないか。また、受託者にUSBを渡すが、USBをパソコンに接続せずにプリンターに直接つなぐ方法でも出力作業が出来るか考えるがいかがか。パソコンに接続せずに業務が可能であるならば、USBのデータをパソコンに移さずに作業をした方がよいので検討してほしい。

○「住民情報系基幹システム保守業務委託における仕様変更（リモート保守）」について、諮問どおり行うことを「可」とする。

※委員意見及び情報政策課・保険年金課の回答

- 本業務委託の実際の作業は、諮問書P.39仕様書の履行場所に記載のある、日立システムズ株式会社湘南オフィスで行われると思うが、当該オフィスと同ページに記載のある同社日本橋オフィス、委託契約書にある統括責任者の3つの関係について伺う。
 - 日本橋オフィス及び湘南オフィスの両拠点で、分担してSEの作業が行われる。統括責任者は通常は日本橋オフィスにいる。
- 統括責任者は受託者である統括本部長と異なるということによいか。
- 両拠点で作業するという事は、それぞれの箇所とつなぐためIP-VPN回線を少なくとも2本引くということか。
 - いずれもお見込みの通りである。
- 諮問書P.39仕様書の履行場所に、先の2つのオフィスと「他」となっているが、両拠点以外の場所でも作業が想定されるのか。
 - 2つのオフィス以外の場所からもリモート保守を行うという趣旨ではない。リモート保守開始後も、市庁舎内において作業を行うケースがある。履行場所として市役所情報政策課は明記しているが、各所管の事務室でも作業する可能性

があることから、「他」と記載したものである。

- それであれば、情報政策課“及び各所管”と明記すべきである。
- ハードウェアのリモート保守は行わない予定か。ソフトウェアの保守のみか。
- 諮問書 P. 39 仕様書“4. 履行概要”に記載の通り、ソフトウェア・ハードウェアともに障害対応を行う。例えば、リモートによりハードウェアの故障状況を事前に確認する等があげられる。
- IP-VPN 回線は常時接続されているのか、市の許可を得たときのみ接続されるのか、職員不在時に接続されることはあるのか、市の判断により市側による切断は可能かをお聞きしたい。
- リモート保守で作業を行った日時や内容等の記録を市が得る方法はあるのか。リモート保守は、原則委託者（市）側の意思で接続・遮断が出来、接続中は、その旨がわかりやすいかたちで表示されること、作業記録が確認できること、これらが重要と考える。
- 諮問書 P. 20 仕様書の“2. サービス時間帯”が接続する時間を示すのか。
- 本委託業務は稼働維持等のサポート業務と運用業務であり、夜間の稼働監視やバッチ処理の実行といったものもある。5件の契約ごとにサービス時間帯は異なり、夜間がサービス時間帯に含まれている契約については夜間も回線を接続して作業が行われる。
- これまでも夜間の作業はあって、作業時は市職員が立ち会っていたのか。
- 夜間作業はこれまでもあり、定例で行う夜間のバッチ処理や大量印刷には立ち会わないが、システムに大きな変更を加えるような業務を行う際は市職員が立ち会っていた。
- 作業に従事する人間の中に悪意のある者がいた場合の対応が心配である。
- 諮問書 P. 5 の通り、作業を行う受託者施設には生体認証等による入退室管理を義務付け、リモート保守の端末ログイン時には、指静脈とパスワードを併用する当市内部で実施する際と同等の二要素認証を必須とする。また、諮問書 P. 20 仕様書“3-3乙の拠点における入退室管理等”の記載のとおり、「あらかじめ登録した者以外が操作できないように対策するものとする。」として、安全対策をするところである。
- 事前に名簿等を提出させ、市において操作者の身元の特定が出来る状態であるという認識でよいか。
- お見込みの通り。また、二要素認証のサーバーは市庁舎内にあるので、市庁舎においてリモート保守を行う従事者として指静脈等の登録をした者以外はリモート保守を行う端末に入れない環境になる。
- 登録する従事者は何名か。
- 10名程度を想定している。
- それだけの認証等のシステムを受託者も構築する必要があるため稼働まで若干の時間がかかるということか。
- 準備期間については、セキュリティの構築も含めたものとなっている。
- これまでは市役所内での作業ということで、市職員の目がある、警備員もいるため悪意のある行為は出来ないという心理的なプレッシャーがあったと思う。リモート保守に切り替わるとそういったプレッシャーが無くなる。以前に他自治体で、受託者のアルバイトが住民情報を抜き取り売り払った事件があった。認証システムを厳しくしてそういったことを簡単に出来るわけではないということであっても、従事者がもうじき自分は交代する、退職するといった時に最後にといい気持ちで、すぐにはわからない形でデータの抜き取り、或いは時限式のウィルスを仕込んでいくという危険性は今までより高まる。こういったリスク

に対応出来るかが懸念事項である。

- 悪意をもった人の介入がどう排除される仕組みとなっているか、もう1つは従事者をどういった形で雇用し、教育しているのかについて受託者へ確認していただきたい。
- 情報抜き取りを防ぐ対策として、市で使用している端末と同様の環境で受託者の作業端末を設置してもらおう考えである。市では昨年度からパソコン端末等へUSBメモリ等の記録媒体を取り付けることがシステム的に出来なくなる仕掛けを導入しており、これに倣ってもらおう。
- 諮問書P.5では、「IP-VPN回線とする」と言い切っているが、P.20仕様書では「IP-VPN回線もしくは同等以上の回線」となっている。この違いはなにか。
- セキュリティ上、IP-VPN回線で十分と考えている。仕様書については、それ以上のものが仮にあればということ想定して「同等以上」と記載した。「IP-VPN回線若しくは専用回線」と修正する。
- 諮問書P.30東村山市情報セキュリティに関する合意書“7ネットワークへの接続及び管理”に「①受託者が委託者の情報ネットワークに接続することは禁止する」とあるが、住基情報系システムをリモート保守するということは、受託者が市のネットワークに繋がる事が出来るようになるという意味になると思われるが、ここの解釈はいかがか。
- 「受託者が委託者の情報ネットワークに接続」とは、受託者が所有するPC等の情報機器を、委託者である市の情報ネットワークに接続する行為、若しくは、受託者が業務上使用しているネットワークと市のネットワークを結ぶといった行為を意味し、これらを禁止するものである。今回のリモート保守契約では、受託者の施設内にリモート保守を行うための市所有PCを置き、市のネットワークからそのPCにつながる回線を受託者社内に設置する。市のネットワークを延長して受託者社内にある市所有PCまでつなげるというイメージ。そのPCを操作してリモート保守を受託者が行う。
- 受託者が社内でリモート保守を行うために使うPCは市のものということか。
- 先程の説明において、受託者が取扱うPCについては、「市で使用している端末と同様の環境」とするとあったがどういうことか。
- リモート保守用に市の所有するPCを受託者に渡し、セキュリティレベル等の環境も市と同等の設定にするという意味である。
- 情報セキュリティに関する合意書にはひな形があり、受託者が市のネットワークに接続することは一般的に禁止されるが、本業務委託はそういったものに当たらないと思われる。よって、7①については削除の上、さきほどの説明内容を改めて記載した方が良く思う。
- 今回は市が受託者に市所有PCを渡し、市のネットワーク回線の一つとして使用するため、7①にある「受託者が委託者のネットワークに接続する」とは異なるという理解で良いか。
- 通信回線で結ぶ受託者施設内のPCは市が用意するもので、併せて生体認証を行う装置と組み合わせて設置する。これらは市が管理するネットワークに属するものと考えており、7①には該当しないと認識である。
- 7については①に限らずすべて削除した上で、今回のリモート保守に合った文言に、「受託者に貸与する市所有のPCから、指定のIP-VPN回線を使って行うものとする。それ以外の方法で市のネットワークに接続することは禁止する。」などの明確な記載にするのが良い。
- ひな形をそのまま使用するのではなく、所管において業務内容に合っているかよく確認してほしい。市のネットワーク管理をお願いする今回の契約では、通常

の委託とは異なる例外的な業務のやり方が出てくるので、ひな形通りでは内容に矛盾が生じる。契約上の指示に矛盾が生じていると、後日受託者との間で問題が生じた場合に色々と面倒になると思う。契約書、仕様書全体として矛盾がないか、特に、今回5件まとめて委託するというのであれば、5件相互の矛盾がないかも確認するようお願いする。

- リモート保守化の利点が3つ挙げられている。経費の削減、サービス時間帯の延長、障害時対応の迅速化である。これまで各委員が指摘された危険をはらんでいたとしてもそれを上回るメリットがあるため、市として取組もうとしていると思う。現在常駐でいるSEの減員が出来るので経費の削減効果があるということかと思うが、現在本業務に関わるSEが何名おり、リモート保守とすることで何名減となるのか。
 - システムプログラムそのものを行う業務SEについては、各業務ごとに登録されており、何かシステム上の障害が起きたときに対応を行う者である。これまで市役所へ来庁することでしか作業できなかったが、日本橋オフィスの中でも作業が行えるという選択肢が増えるということであり、人数そのものについては変更はない。運用SEについては、システムの監視を行うという業務をこれまでローテーションを組み4名が市役所に常駐する形で行っていたものが2名のローテーションとなり、それ以外の夜間については湘南センターに運用SEが1名常駐するので、1名分の軽減のみである。
 - トラブル等が発生した際は、今でも常駐SEの対応というよりは出張でくるものが対応となっているのか。
 - こちらからの依頼により、必要に応じて業務SEに出張で来て作業をしてもらう形である。リモート保守になると、担当の業務SEが市へ到着するまでの時間に受託者のオフィスですぐに取り掛かれることにより、時間が軽減される。
 - サービス時間帯の延長とは具体的にどういったことか。
 - 夜間処理を行う場合、これまでサービス時間帯は7時30分から21時15分までとなっているが、これを、夜間、湘南センターと接続することによって、24時間体制の監視が行えるようになるということ、サービス時間の延長と捉えたものである。
 - これを導入した場合、入退室やPCの操作者を限定することで安全性の確保が出来るということだが、安全性の確保という視点から見ると、市職員の目の前でやられている今の方がはるかに高いかわけだが、そこはどのような認識か。
 - 自身の経験からの話も含まれるが、安全性と業務スピードの2つの面があり、例えば今は22時くらいに障害の発生が確認された場合、SEがおらず作業は翌日となるが、リモートですぐに作業が実施出来れば被害範囲が少なくなる場合がある。リモート保守には、すぐに作業実施が可能であり被害拡大の時間が少なくなるという点で今より安全性の確保が出来るといった考え方もある。
 - ディザスタリカバリの観点でも現行と同じかどうかというのを検討していただきたいと思う。大震災後の復旧作業などである。
- (総務部長) ご指摘のディザスタリカバリについては、別途、今年度からの自治体クラウドの導入・参加についての検討の中で議論していく。
- 仕様書P.39～40にはサービス提供時間の記載がない。これはどうか。24時間であれば、書かかずとも良いとはならず、どういった時間帯にサービス提供をしてくれるのかというのは、契約内容として重要な部分であるので、記載すること。
 - こちらについては夜間通しではなく、時間帯の記載が欠けていた。コンビニ交付で住民票を取得できるのは6時半から23時までだが、実際に取得できる時間

と、ソフトサポートの提供時間は同一ではない。これまでお話いただいたとおり、5件の契約間に齟齬がないように、実際の導入に向けて再度確認の上、作業を進めていく。

- P. 3 3仕様書に「常駐運用者」という言葉があるが、こちらは必ずしも常駐ではない場合もあり得るということで良いか。
- おっしゃるとおり、常駐運用者とは限らない形となる。この記述についても確認しておく。
- 基本的にはリモート保守、必要に応じて常駐運用者となる可能性があるということか。
- そうである。
- 基本的には常駐運用者がいるのかいないのか、いない場合の体制はどうなっているのか、ということを中心に把握しておく必要がある。
- P. 3 4 住民情報系システム運用管理の仕様書“1-1-2 (2) 夜間の運用監視”に、「常駐運用者は、夜間の監視を行うこととする」とあるが、今後は無くなる可能性もあるわけか。“常駐”運用者と記載されているので。
- 諮問書、仕様書等を読んだ限り、どれくらい実態を我々に理解させてくれるのかという点についてちょっと甘いところが多いことは指摘させていただく。他の委員がおっしゃったとおり、どういう仕事内容になるのか正確な内容を仕様書に落とし込み、きちんと作成していただくことをお願いしたい。また、回線接続のオン・オフが市側で出来るかという点は、回線接続の状況自体も日立システムズに監視してもらおうという理解で良いか。それとも、こちらがイニシアチブをとり、怪しい接続と判断した場合には切断できる仕組みを作る余地があるのか。
- 物理的に回線を抜いて切断する方法はあるが、それ以外の方法については未定である。

(情報公開係長) 現時点ではっきりとしていない部分については、次回以降の審議会で報告させていただくことでよいか。

- それは構わないが、回線の切断等について、日立システムズと交渉する余地があるのかを含めての確認である。
- 市がまずいと判断した場合は物理的に回線を抜くなどの対応をすべきといった、市の運用ルールを書面で作られた方が良い。
- 現在の市の情報セキュリティポリシーの中で、外部との接続中、不正アクセスと認められるような状況になった場合は、市の方から切断すると定めている。
- 市がイニシアチブをとれるところはとるつもりで、受託者に確認をお願いしたい。不正アクセスや情報抜き取りを防ぐ又は起きてしまった時に被害の拡大を防ぐために、受託者はどのような人的・物理的体制や仕組みをとるのか、また、こういうことが起きた時はこう対処するといった問題発生時の動きも含めて、確認して文書化しておくことを最低限やっていかれるようお願いしたい。情報抜き取りだけではなく、時限爆弾のように何かを仕掛けられる危険があることは否定はできない。そういった悪意の人をどう事前に排除するか、或いはグレーの人がいるのではないかと受託者又は市が感知した場合、受託者ではどう対応してくれる用意があるのか。防災と減災ではないが、微妙に異なる意味となるので、その点についても確認し、きちんとした答えがあればそれを所管の運用ルールの一部として適用することをおすすめしたい。
- 諮問書 P. 2～4に、各システムと特定個人情報の有無等を整理した一覧があるが、本表に「システムの運用」に関する項目をつけ加えて、例えば常駐の人の有無や、運用は何時から何時までどこでやるのか、といった内容を追記していただければ、大体どんな風にシステムが運用されているかがわかったと思う。所管と

しても、そういった点が一覧でわかる資料を作って、課内のどこかに保管して共有されると良いと思う。

- 課内で共有しているものとして、処理スケジュール表という紙がある。何の処理をいつやるかという月間と年間スケジュールについて、システムを利用する各所管課と連絡をとって作っている。しかし、委員がおっしゃるような、保守管理作業がどこでどの時間に行われているのか等についても確認できる一覧は無い。あれば便利かと思う。
- 情報政策課の方で不正な接続をどのように監視・防止していくかを検討し、文書の形で代々残せるようにすること、仕様書等の文言の矛盾を訂正すること、その他受託者に確認する事項をいくつかお願いしたが、それをやっていただくという条件付きで委託を可とする。確認を依頼した件については後日報告をお願いする。

(4) 報告

○ 小学校通学路への防犯カメラ設置追加 (学務課)

(情報公開係長)

28年度第1回、29年度第1回の審議会で、秋津・八坂・久米川・化成、回田・秋津東・富士見の計7校の小学校通学路にある電柱や街路灯に防犯カメラを設置したことと、撮影データを警察に提供する際のルールなどを報告した。順次小学校全校の通学路に付ける予定で、29年度末は、恩多・青葉・北山・久米川東の4校に設置した。

カメラは高さ5メートルほどの位置に設置しており、撮影データはカメラ内にあるSDカードに自動的に記録され、1週間ほどで順次上書きされる。カメラの箱には第三者がカードを取り出せないように鍵がかかっている。カメラの管理やデータ提供時のルールは、28年度の審議会における報告と同じ運用である。設置業者によるカメラの定期点検は、年1回と契約上義務付けている。

お手元にある図面は、新たに設置した4校のカメラの設置場所と映す方向がのったものである。カメラの設置場所は、警察と協議して決めている。

- 防犯カメラを設置した効果について伺いたい。
- 設置前後で犯罪発生率が減少したというような効果は、総務課では把握していない。また、警察へ捜査のために映像データを提供した際に、それが市立小学校に係る犯罪だった場合は警察から内々に犯人逮捕に至ったかどうかは教えてくれるが、提供した映像データが逮捕に貢献したかななどの具体的な回答はない。

○ 「在宅医療連携推進事業委託」における受託者の追加 (健康増進課)

(情報公開係長)

29年度第3回審議会で諮問した健康増進課の「在宅医療連携推進事業業務委託」について、30年度から歯科医師会が受託者に追加されたことを報告する。

昨年秋に医師会と薬剤師会に委託して事業を開始した。市内5カ所の地域包括支援センター内に在宅療養支援窓口を設置し、それぞれの支援窓口「助言担当の医師又は薬剤師」をつけ、かかりつけ医のいない市民から医療的な助言が必要な相談が来た場合に、支援窓口が助言担当医につないで、医師等の助言や訪問を受けられるようにするという事業である。今年度から助言担当として歯科医師が

加わる。

医療的助言が必要な方については、支援窓口から助言担当の歯科医師へ相談依頼書を送付することや、依頼書は5年保存とすることなど、個人情報の取扱いについては歯科医師会も医師会等と同じ取決めとなっている。

○ ペイジー口座振替受付サービス機の導入（収納課）

（情報公開係長）

市税や介護保険料を市民の方の口座から振替するには、市と各金融機関の間で、口座情報や税の金額などの個人情報データのやり取りが必要になる。市は、オンラインを使った金融機関との口座振替データのやり取りやとりまとめを、以前からAGS(株)に委託している。

4月から口座振替業務の一環として、新たにAGS(株)に「ペイジー口座振替受付サービス運用業務」の委託を追加した。AGSがこの業務で取り扱う個人情報の種類や、オンラインでの個人情報の流れはこれまでと同様のため、諮問ではなく報告とさせていただく。

まず「Pay-easy（ペイジー）」とは、民間企業や公共機関と金融機関をオンラインでつなぎ、インターネットバンキングやATMなどから税金や各種代金を支払ったり、口座振替の申込等を電子的にリアルタイムでできるようにするためのネットワークサービスの愛称である。「ペイジー口座振替受付サービス」とは、収納課・保険年金課・介護保険課の窓口を設置してある専用端末（クレピコ端末）を市民がご自分で操作することで、税や保険料の口座振替の開始・口座の変更等の手続が電子的に行えるサービスである。市民が本人名義の金融機関のキャッシュカードを専用端末に通し暗証番号を入力すると、端末が読み取った口座情報や振替受付の情報が暗号化されて各金融機関へオンラインで通知され、口座振替の手続が完了する。

専用端末は、直前の1件の登録情報しか残らないように設計されており、カード情報を読み取るスキミング装置の装着ができない構造になっている。また、万一端末のなかを開けられたときには、重要データ、プログラム等が消去又は無効化される仕組みである。専用端末から情報処理センターへの通信ネットワークは、NTTドコモのFOMA通信で、あらかじめ登録した端末のみが接続できるクローズド接続になっている。情報処理センターから金融機関への通信は、キャフィスというNTT DATAが提供する日本最大のカード決済総合ネットワークを使う。いずれも高い安全性を確保している。

これまで、税金や保険料の口座振替の開始、口座の変更、振替口座の解約を希望する市民は、「口座振替依頼書」という銀行届出印を押した書類を提出する必要があった。機械操作が苦手であれば、より簡単に手続ができる選択肢が増えた。

○ 東村山市個人情報保護に関する条例・同施行規則の改正（総務課）

平成29年3月、6月、12月議会において、「東村山市個人情報保護に関する条例」の改正をしている。

29年中の条例改正は、行政機関個人情報保護法等が改正され、平成29年5月30日に施行されたことに伴い、改正内容を条例に反映させることが主な目的である。

行政機関個人情報保護法の改正には、大きく二つの点がある。

一点目が、個人情報の効果的な活用が新たな産業の創出に資するものであるこ

とを踏まえて、行政機関の保有する個人情報加工して「非識別加工情報」を作成し、事業者に提供するための仕組みを設けたこと。二点目は、マイナンバーや運転免許証番号、各種被保険者証の記号・番号等を「個人識別符号」と名付け、それ単独で個人情報に該当すると位置付けることにより個人情報の範囲を明確化したこと、また、人種・信条・病歴等の社会的差別の原因となる個人情報の取扱いを厳格化する観点から、「要配慮個人情報」の規定を設けたことである。

なお、条例に反映させたのは、二点目のみである。

一点目の「非識別加工情報の民間への提供」については、国が29年度に開始したばかりであり、個人を識別できないようにデータを加工する技術基準やコストなどまだ見えてこない部分が多いため、東京都を含め地方自治体で条例改正しているところはほぼなく、当市も非識別加工情報の制度については今後の検討課題としているところである。

改正箇所が多いため、配付資料に改正箇所ごとに説明を入れてある。後ほど改めてお目通しいただければと思う。

- ビッグデータの活用は、東日本大震災の際にスマートフォンのGPS情報を活用したということはお聞きするが、産業用に活用している事例というのはあまり見聞きしない。防災や減災への活用が先になるかと思われ、経済レベルでの活用は地方自治体は困難かもしれない。
- 国の動向を見たらうえて、非識別加工情報提供制度の有用性を判断することになるかと思う。

以上

※この会議の資料（諮問書など）は、次の理由によりホームページ等での公表はしません。

【理由】

情報公開条例第6条各号に規定する非公開情報（個人情報や市の情報セキュリティ対策の詳細情報、これから予定している委託契約の情報など）が含まれており、公開することにより情報を早く得た者が契約に有利になったり、コンピュータシステムに不正侵入されるといったおそれがあるため。