

第201回 横浜市個人情報保護審議会会議録

<p>議 題</p>	<p>1 会議録の承認</p> <p>2 審議事項</p> <p>(1) 税務システム等再構築・運用保守業務委託について (個人情報を取り扱う事務開始届出書、個人情報ファイル簿兼届出書及び個人情報を取り扱う事務変更届出書を含む。)</p> <p>3 報告事項</p> <p>(1) 防犯カメラ設置に係る本人外収集及び事務委託についての報告 たちばなの丘公園内防犯カメラ運用事務</p> <p>(2) 電子計算機処理に係る名簿管理についての報告 ア 液化石油ガスの保安の確保及び取引の適正化に関する法律関係事務 イ 市立特別支援学校特別支援教育就学奨励費事務</p> <p>(3) システム更新時のデータ移行業務に係る事務委託についての報告 市立特別支援学校特別支援教育就学奨励費事務</p> <p>(4) 宛名印字・宛名ラベル貼付業務に係る事務委託についての報告 「令和4年度横浜市こころの健康に関する市民意識調査」業務委託</p> <p>(5) 市のイベント・行事における参加申込み受付等業務委託についての報告 ア 横浜市庁舎におけるマイナンバーカード申請サポート運営業務委託 イ 日中韓青少年文化交流事業に係る参加者選考業務</p> <p>(6) クラウドサービスの利用に係る電子計算機の結合及び事務の委託についての報告 学生の海外派遣事業</p> <p>(7) 個人情報を取り扱う事務開始届出書 (1件)</p> <p>(8) 個人情報を取り扱う事務変更届出書 (5件)</p> <p>4 その他</p> <p>(1) 個人情報漏えい事案の報告 (令和4年6月23日から同年7月20日まで)</p> <p>(2) インターネット利用環境再整備事業における個人情報の取扱いについて</p> <p>(3) 新法66条の「安全管理措置」について</p> <p>(4) その他</p>
<p>日 時</p>	<p>令和4年7月27日(水) 午後2時から午後4時まで</p>
<p>開催場所</p>	<p>市庁舎18階共用会議室 みなと6・7</p>
<p>出席者</p>	<p>中村会長、大谷委員、加島委員、後藤委員、鈴木委員、永井委員、三品委員、吉田委員 (全員WEB会議により参加)</p>
<p>欠席者</p>	<p>板垣委員</p>
<p>開催形態</p>	<p>公開 (傍聴者なし)</p>
<p>決定事項</p>	<p>・審議事項(1)について、承認する。 ・報告事項及びその他について、了承する。</p>
<p>議 事</p>	<p>【開 会】 (事務局) それでは、ただいまから第201回横浜市個人情報保護審議会の御審議をお願いいたします。 審議に先立ちまして、本日の定足数について御報告いたします。 本日は、板垣委員から御欠席の御連絡をいただいておりますが、ほか8名の</p>

委員は御出席をいただいておりますので、横浜市個人情報保護審議会規則第4条第2項の規定による定足数を充たしており、審議会は成立しておりますことを御報告いたします。

それでは、このあとの議事につきましては、会長よろしく願いいたします。
(中村会長) ただいまから、審議会を開会いたします。

本日の審議に入る前に、本日の審議会はWEB会議による方法にて開催したいと思いますが、委員のみなさまよろしいでしょうか。

(各委員) <異議なし>

(中村会長) それでは本日はWEB会議にて開催いたします。

1 会議録の承認

(中村会長) それでは、議事に入ります。

はじめに、第200回審議会の会議録につきましては、既に送付済みですが、何か御意見等がございますでしょうか。

特に御意見がなければ、承認とさせていただきますと思いますが、よろしいでしょうか。

(各委員) <異議なし>

(中村会長) それでは承認といたします。

2 審議事項

- (1)【案件1】税務システム等再構築・運用保守業務委託について（個人情報を取り扱う事務開始届出書、個人情報ファイル簿兼届出書及び個人情報を取り扱う事務変更届出書を含む。）

(中村会長) それでは、本日の審議事項の審議に入ります。

最初に案件1「税務システム等再構築・運用保守業務委託について」の御説明をお願いします。

(事務局) <所管課及び審議事項について説明>

(所管課) <資料に基づき説明>

(中村会長) ただいま御説明がありました案件1につきまして、御質問、御意見をいただきたいと思っております。

(加島委員) 国によるシステムの標準化作業ということで、今回、一番最初に地方税について行われることをデジタル統括本部の資料で知りました。国が示した標準仕様書が、本当に横浜市のような405万件も情報を抱えている自治体に対応できるかすごく心配です。どこか先行自治体で試験的な運用を行うのでしょうか。それとも、令和7年度に一斉に標準化が行われるのですか。

(所管課) 税務システムの標準化作業に関する内部事情について少し補足で説明いたします。横浜市が古くなったシステムについて「そろそろ再構築をしなくてはいけない」という議論をしているときに、デジタル化を急加速しようという国の動きが入ってきました。そのため、国のデジタル化の政策が始まりましたので、丁度いいタイミングで税務システムの再構築に着手することができました。

システムの機能が成り立っているのか検討を重ねてきましたし、国に意見を

述べたり、調整を重ねているところですので、国の標準化仕様書が横浜市に対応しないのではないかという心配はしていません。

(加島委員) 毎年、税法改正の度に、1,700の自治体がシステムを直さなければいけないという現状を鑑みると、標準化自体は非常に良いことだと思います。税法改正に合わせて政府がシステムを換えるという仕組みに変わることになるので、横浜市としては、今まで行っていた作業が相当楽になるとは思います。どこか小さい自治体で試験的に運用しているものを横浜市に導入するのであればよいのですが、最初から405万件も情報を抱えているような自治体に導入するというので、セキュリティの問題等が心配です。

デジタル統括本部の資料の中でも、標準化仕様書について「情報が不足している」と書いてありました。これからその標準化仕様書がうまく使えるのか、今までのデータをうまく移行できるのか、すごく心配はあります。個人情報保護の観点も含めて、しっかり検討を重ねてもらえればと思います。

(所管課) ありがとうございます。

(後藤委員) 7ページの「3 審議に係る事務【電子計算機の結合】」と21ページ、22ページにクラウドについての記載があります。21、22ページを見ると、税務システム(COKAS-i)は全てクラウドシステムであると記載があり、このクラウドは、NECの「Cloud IaaS」を利用するということではないでしょうか。

22ページを見ると、左上の部分だけがクラウドと書いてあります。そうすると、それ以外の北部データセンター等がいわゆるプロプライエタリなシステムになるという理解でいいのでしょうか。

また、プロプライエタリな部分の開発は、今回はしないのですか。プロプライエタリな部分もつくり直すのでしょうか。

(所管課) まずクラウド上にシステムを設けるという仕様になっているので、このとおりに設計をする予定です。使用するクラウドについては、ガバメントクラウドを標準的に使用することになってはいますが、この仕様については令和4年夏以降、これから提示されると聞いています。その仕様をしっかりと確認した上で、ガバメントクラウドに情報を載せられるのかということです。仕様と共に費用負担も示されます。また、NECもISMAPのリストに載っているクラウドを持っていますので、どちらにするかを決めていきたいと思っています。

いずれにしても、国の認証ではないですが、ISMAPのリストに載っていることは間違いのないので、どちらを利用するかは使い勝手や費用負担等で比べていこうと思います。

(後藤委員) そこはクラウドの部分についてだけですよね。住民記録システム等は既存のものを活用し、新しいシステムと連携するというのでいいのでしょうか。

(所管課) そうですね。ほかに二重業務で掲げられているような住民記録システムは、「これから標準化について検討する」という段階です。私どもとしては、現行の住民記録システムを前提に連携していこうと考えています。

(後藤委員) 6ページの「3 審議に係る事務【電子計算機処理の開始】」の「内容・対象者」に「(3) ダウン対策サーバの運用」とあります。このサーバはバックアップサーバと理解していましたが、何のバックアップになりますか。

(所管課) 大地震等大規模災害のときを想定し、北部データセンターにバックアップを置き、災害証明等証明書の発行等最低限のことができるようにしておこうという目的です。

(後藤委員) 22ページの図でどの部分にバックアップサーバができるのですか。クラウド上のシステムと緑色の住民記録システムがあります。その一部だけはバックアップサーバを別途用意しようという理解でいいですか。

(所管課) そうですね。基本的には、上のほうにある青い枠で囲まれているところに保存されている情報の内、証明に使いそうな情報を抽出しようということです。

(後藤委員) NECのガバメントクラウド内に入っているものをローカルサーバに持ってきて把握できるようにしようという理解でいいですか。

(所管課) そのとおりです。

(後藤委員) 私はBCPを専門にしているのですが、災害時には横浜市のサーバがダウンすることを考えているのでしょうか。それとも、別の機関のサーバがダウンすることを考えているのでしょうか。

(所管課) どのサーバがダウンするのかわかるのかによって対応も変わってくると思います。基幹ネットワークになるので、ここがダウンするようではよほど被害が甚大だろうと想定されます。本市と各区役所とをつなぐもので、少なくとも復旧の順番が早いであろう北部データセンターに設ければ適切かと考えています。

(後藤委員) BCPにおいては、想定する大規模災害をどう考えるかという視点と、復旧が大事なのかデータのほうが大変なのかという視点を重視することがあります。今、話題になっているウクライナ等は、海外にバックアップを持っています。そういう事態まで考えるかどうかで大分変わってくるわけです。

バックアップのところでは、情報漏えい等のリスクが高まることもありますので、是非検討してもらえればと思います。

最後に確認なのですが、ガバメントクラウドかISMAPしか使わないというのは、横浜市の方針ということでしょうか。

(所管課) そうですね。今、デジタル統括本部でガバメントクラウドをどう扱うのかを検討しているところです。少なくともシステム標準化法に書かれているので、それに倣うという考えです。

(後藤委員) ISMAPには関わっていますが、それは推奨であって義務ではありません。責任が取れば、ISMAPに載っていないクラウドを使うことは構わないと思います。非常に厳格だなと思って聞きました。

(大谷委員) 開始するシステムの可用性は、個人情報保護にも大きく関係すると思います。この開発そのものが何とか成功することを期待します。

やはりデータ移行が大変な難所だと思います。過去に整理されたドキュメント等については、現在のシステムを正確に示しているかどうか、恐らく不安要素もあるという説明もありました。横浜市独自のシステムはどこが開発して、どのようなドキュメントを持っているのか、現状での分析の状況を教えてください。

また、やはり短期間でデータ移行を成功させるためには、ある程度コンティンジェンシープランも作成しなければいけないと思っています。どの段階で前に戻すというようなコンティンジェンシープランにしているのか教えて

もらいたいです。

(所管課) まず、現在の状況についてお話しします。現在、システムは富士通で構築と運用をしています。何分、歴史のあるシステムなので、横浜市の職員が自分でプログラム改修をしていた時期がありました。そのような時期も含め、若干、データのレイアウト等の仕様書と現状が違うのではないかといいところは幾つか出ています。これまでもデータの分析等を設計図の範囲の中で行ってきましたが、やはり中身を見てみないと分かりません。ただ、今のホストデータは気軽に見られるものではありません。実は、私もその全容は見たことがなく、早い段階で新しいシステムにデータがきちんと載るかどうかが、正確に分析を行う必要があると思っています。

続いて、コンティンジェンシープランについて御回答します。今回、1週間程の期間で巨大なデータを全部事故なく移行できるかどうか、という大事業が待っていますので、仮に駄目だったときにはどうするか、という点については、正に今、検討しているところです。税制改正のメンテナンスを今の古い富士通のシステムにかけること、それから、12月から1月にかけて、税の世界では色々なバッチ処理を流しますので、このバッチ処理を流すべきなのか、等といった点について、どこかの段階で判断をしなければならぬかと思っています。この場合にはどこまで切り戻しをするのか、というところはデータを見て、どこまできれいになっているか、これからデータのクリーニングがどこまで徹底してできるかを考え合わせて慎重に計画を練っていきたいと思います。気軽に「1年間延長しようか」等とはできないホストシステムなので、慎重に検討を重ねていきたいと思っています。

(大谷委員) ありがとうございます。メインフレームからのデータ移行の困難さはよく知っているつもりです。まだデータの全部を見たことがないという状況でもあり、ベンダーの交代がかなり大きな障害になるケースもあると聞いています。既存のベンダーについて最後までサポートが受けられる体制を持続してもらい、ベンダーとのコミュニケーションが起点となり、うまくデータが移行され、新システムの可用性が担保されるように祈ります。たくさんの方のことを考慮しながら計画を立てていることが分かりました。大きな開発でもあるので、もし困った状況が発生した場合には速やかにエスカレーションしてもらいたいようなことも今後考えていく必要があるかと思っています。

(所管課) デジタル統括本部をはじめとして注目をされている事業なので、情報提供や状況等は、常に逐一報告できる状態にしておきたいと思っています。

(中村会長) ありがとうございます。他に何か御質問等がなければ、案件1を承認するというところでよろしいでしょうか。

(各委員) <異議なし>

(中村会長) それでは承認といたします。

3 報告事項

(1) 防犯カメラ設置に係る本人外収集及び事務委託についての報告

たちばなの丘公園内防犯カメラ運用事務

(2) 電子計算機処理に係る名簿管理についての報告

ア 液化石油ガスの保安の確保及び取引の適正化に関する法律関係事務

- イ 市立特別支援学校特別支援教育就学奨励費事務
- (3) システム更新時のデータ移行業務に係る事務委託についての報告
市立特別支援学校特別支援教育就学奨励費事務
- (4) 宛名印字・宛名ラベル貼付業務に係る事務委託についての報告
「令和4年度横浜市こころの健康に関する市民意識調査」業務委託
- (5) 市のイベント・行事における参加申込み受付等業務委託についての報告
ア 横浜市庁舎におけるマイナンバーカード申請サポート運営業務委託
イ 日中韓青少年文化交流事業に係る参加者選考業務
- (6) クラウドサービスの利用に係る電子計算機の結合及び事務の委託についての報告
学生の海外派遣事業
- (7) 個人情報を取り扱う事務開始届出書（1件）
- (8) 個人情報を取り扱う事務変更届出書（5件）

4 その他

- (1) 個人情報漏えい事案の報告（令和4年6月23日から同年7月20日まで）
- (2) インターネット利用環境再整備事業における個人情報の取扱いについて
- (3) 新法66条の「安全管理措置」について
- (4) その他

(中村会長) それでは次に、順番が前後しますが、先に「4 その他」の「(2) インターネット利用環境再整備事業における個人情報の取扱いについて」、事務局から説明をお願いします。

(事務局) 簡単に申しますと、平成27年の年金機構における情報流出事件を受けた国の指示により、文書管理システム等の本市の業務システムは、インターネットと切断し、独自の回線上で動いていました。

これにより、セキュリティは向上しましたが、クラウドの活用がしづらい等、DX時代を迎え、不都合も生じています。

そこで、国はガイドラインを改訂し、一部の業務システムは、インターネット上で稼働させることとなりました。もちろん、セキュリティ対策は向上させた上で、ということになります。

これは、多くの業務システムに共通する話ですので、システム管理について統括をしておりますデジタル統括本部から包括的に説明し、御審議いただくことで、審議全体の効率化を図れればと考えています。

なお、旧システムから新システムにデータを移行することにつきましては、システムごとに類型案件にて報告します。

では、詳細につきましては、デジタル統括本部から御説明いたします。

(所管課) <資料に基づき説明>

(中村会長) ただいまの報告につきまして、何かございますか。

(大谷委員) セキュリティ対策については、私もなじみのあるEDRやMDRの有名な事業者もおりますので、かなり高度な対策が講じられると思います。

業務用端末を利用する職員がたくさんいて、5万件を予定しているということです。個々の業務用端末についての認証や、業務用システムに接続している

端末の管理が非常に重要になると思います。その辺りのセキュリティについてもある程度教えていただけると、全体のセキュリティ対策がすき間なく施されているかどうかの確認ができると思います。その辺りも補足で説明いただける有り難いです。

(所管課) 今、職員が使っている業務用端末をL GWANエリアからインターネット側のエリアに変えると説明しました。基本的には職員が何かをするということではなく、ネットワークの入り口の構成を変えるだけで、環境全体をそのままインターネット側に持っていくんです。そのため、内部のIPアドレス体系等はいじらないのでトラブルは想定していません。

また、現状、横浜市のネットワークにつながる端末1台1台をハード認証しています。そのハード認証によって、許可された端末しかIPアドレスを振らない仕掛けをつくっており、端末での認証方法そのものに変更はありません。

(大谷委員) ハード認証というのは、MACアドレスで接続できるIPアドレスをあらかじめ決めておき、全く関係ない端末が接続されれば検疫システムが発動して、データの抜取りや不正なソフトの導入もされないようにコントロールしているということでしょうか。

(所管課) そのとおりです。

(大谷委員) 実際にEDRを入れていても、インターネット系で接続している端末は様々な脅威にさらされています。例えば、メール等を介しても様々なマルウェアが入ってくる可能性もありますが、個々の端末には個人データは置かないという整理で、個人情報の問題はクリアされているという理解でいいですか。

(所管課) メールは個人情報で、今、各端末の内部に入っており、この状況は変わりません。

現在の横浜市のメールシステムは無害化システムを採用しており、マルウェアは入ってこないメールシステムになっています。インターネット環境に移っても無害化システムはそのまま残しますので、無害化したものでないとメールは受信しないことになっています。

(大谷委員) メールを介したマルウェアへの感染ということでは、あらかじめ無害化がなされているので大丈夫ということですね。

端末から積極的に、指定されたURLに入っていく、不正なプログラムを配信しているところにアクセスしたとしても、どこかの入り口でコントロールされているため、大丈夫ということですね。

(所管課) それを検知するためのEDRです。今回のEDRの仕掛けで、端末のふるまい検知をし、もしサーバに不正なアクセスがある場合には、検知します。今はインターネットに直接繋がらないので、そのようなふるまい自体があり得ませんが、今後はあり得ると思うので、それを検知するための仕掛けがEDRとMDRです。

(大谷委員) 私も類似の製品を利用しています。1種類だけの利用だとなかなかセキュリティ対策として厳しいと思いますが、かなり優秀で、新しい情報もすぐに更新されるものなので、恐らくふるまい検知機能によって、未知のウイルスにも対応していると思います。アラートに対して適切に対応できるセクションがあればうまく機能するのかなと思います。セキュリティ面で怖い点

は残るかなとも思います。

標準的なインターネットに接続する端末を持っているネットワークで講じられているセキュリティのレベルには達していると思いましたが。ありとあらゆる可能性に対し、今までのシャットアウトされていた状態と比べると本当にリスクが増していきます。常にレベルアップを考え続けなければいけない状況になると理解しています。説明ありがとうございました。

(後藤委員) 今回、横浜市のネットワーク環境が大きくシフトすると理解しました。資料の4ページにも内部のセキュリティ対策や訓練等をしっかり行うと書いています。現在の研修がどのようなレベルかによるかもしれませんが、研修や教育を強化する必要がある気がしました。この点については、どうお考えでしょうか。

もう1点の質問は、EDR、MDRの製品はもう決まっているのかという点です。EDRもMDRもピンキリで、どのレベルの商品を使うかによって相当セキュリティレベルが変わると思います。技術的には非常に発展途上の分野で、今後更に強固な商品が出てくると思います。決め打ちというよりも、今後の発展も見据えて新しい技術に対応していく必要があるだろうと思っています。

さらに、EDRは逆に職員の監視システムとして利用される場合もあります。職員のプライバシー問題も発生し得ると思っています。横浜市の中で何か特別配慮したことはありますか。

(所管課) まず、研修についてですが、本市のセキュリティに関する研修としては、毎月、全職員を対象にした情報セキュリティと個人情報保護に関する研修を行っています。また、インターネット利用環境の再整備に関しては、このセキュリティの月次研修で、どのように変わるかという点やリスクの増大等についても周知や意識の醸成をしたいと思っています。

さらに、今回、新たにインターネットに接続されるということで、メールでの攻撃に対するリスクも増大していくので、今年度から標的型メール訓練を新たに導入し、職員のリスクに対する意識の醸成を図っていきます。

次に、EDRとMDRの製品についてですが、製品は既に決まっていて、EDRに関しては「Cyber Reason EDR」を導入し、MDRに関しては、「Cyber Reason EDR」に対応するMDRサービスを導入します。

製品の品質に関しては、昨年度発注したのですが、基本的には国のガイドラインに準拠する形の製品です。

なお、こちらのEDRを用いて職員の監視をすることは全く想定していません。監視ではないかという意見が出てくるようであれば、丁寧に対応していきます。

(後藤委員) その辺りは、意識の違い等あるかもしれないので、準備だけはしたほうが良いような気がしました。

(所管課) 御意見ありがとうございます。

(加島委員) 今後、LGWANはもう一切使わなくなるのですか。それとも残すのでしょうか。

(所管課) LGWANは残します。

(加島委員) 切り分けはどうしているのでしょうか。

(所管課) 現在の運用はLGWAN側において、インターネットを見るたびにVDIやセキュアブラウザを使って仮想デスクトップで見ているという状態です。今後、インターネット側に事務が移るので、LGWANサービスを使うときは反対にインターネット側からVDIを使ってLGWAN側を見に行きます。

(加島委員) VDIを使用するときはLGWANで業務を行うということですか。

(所管課) LGWANを使うときには、基本的にはVDIを使って接続し、利用するイメージになります。

(加島委員) VDIを使わない業務を新しいインターネット環境で行うという切り分けですか。

(所管課) 基本的には、LGWAN-ASPとかLGWAN特有のサービスを使わない限りはこのインターネット側だけで業務ができませんが、必要なときだけLGWANを使用するというイメージです。

(加島委員) セキュリティレベルで業務を分けているわけではないということですね。

(所管課) そうですね。LGWAN側のサービスを使うときにはVDIを利用して接続するという判断です。

(事務局) 資料の4ページを見ると、メールしか書いていませんが、LGWANはメールしか使用しないということですか。

(所管課) それ以外にも利用します。メールについては例示の意味で記載しています。LGWANのセキュリティレベルと、今後、通常の業務で使うネットワークのセキュリティレベルが異なるという話が含まれていると思っています。通常の業務からLGWANに入る場合には、VDIを使って、通常のネットワークを通すだけではなくて、VDIでセキュリティを担保して利用する形になりますので、インターネット側のネットワークのセキュリティリスクをLGWANに持ち込むことはないような運用にしていきます。

(加島委員) 多分、民間の会社や警察等は、専用回線だけでインターネットはまだ使っていないと思います。ものすごくセキュリティレベルの高いものについては、やはり第一義的には専用回線、第二義的にはLGWAN、次にインターネットの新しい環境というふうに、セキュリティレベルを分けたほうがいいです。まだLGWANのほうが信用できるように私は思います。

(所管課) マイナンバーが含まれるものはLGWANともインターネット系接続とも全く別の、特別なネットワークで引き続き運用していきます。重要な情報についてはそこで扱っていく予定です。

(中村会長) 今の加島委員の質問の意図は「LGWANとインターネットでセキュリティレベルが異なる事務を扱うべきではないか」ということですよ。

(加島委員) そうです。

(中村会長) そのような発想はなく、基本的には多くのものはインターネットに繋がるので、そちらでもう業務を行っていくという発想なのではないでしょうか。

(所管課) 庁内システムに関しては、このインターネット環境で作業していくという考え方です。

(加島委員) もっとセキュリティレベルが高い事務を行うときは専用回線を使っているのだから、わざわざ中間のLGWANを使うことはない、ということですか。

よね。

(所管課) そうですね。

(加島委員) LGWANは利用料が高く、色々制約も多く、使いにくいところもあるので、インターネット環境のほうが手軽という意味もあるのかなとは思いますが。

(中村会長) ほかに御質問等がないようでしたら、本件の報告について了承するという事によろしいでしょうか。

(各委員) <異議なし>

(中村会長) それでは了承いたします。

続いて、「4 その他」の「(3) 新法66条の「安全管理措置」について、事務局から説明をお願いします。

(事務局) <資料に基づき説明>

(中村会長) ただ今の説明につきまして、御質問、御意見をいただきたいと思えます。まず、委託する事務の内容に応じ、区分をした上で安全管理措置を考えていく点について何か質問、意見はありますか。

事務局案の発想は、2ページの表の上の3つの委託事務に関しては、それ以外の委託と比較し、より厳しい基準が必要であると考えているものですか。

(事務局) 厳しい基準というか、いざというときの影響が大きいと評価しているものです。

(中村会長) 厳しい安全管理措置を設けるべきだということですか。

(事務局) そうです。

(中村会長) それ以外の委託については一般的なものでいいという発想ですか。

(事務局) そういうことです。ほかにも「こういうのも本当は危ないのではないか」という意見があれば是非聞きたいです。

(中村会長) 私はこの分類には消極的です。資料を確認した際に、これまで審議に諮った案件を振り返ってみました。例えば、第182回審議会の案件5「建築物の耐震改修促進に関する事務について」という案件がありました。業務内容としては、建築物の耐震性や耐震化の有無、耐震化に当たっての課題等について、所有者等にアンケートを行い、分析する、という業務です。

「アンケート調査・分析」の業務を委託する場合でも、このようなアンケート調査であればあまりセンシティブな個人情報が出てこないと思います。同じくシステムの開発についても、やはり必ずしもセンシティブな情報が扱われるわけではありません。

「上記以外の委託」でも、逆にセンシティブな情報が扱われたり、件数が多かったり、非常に注意しなければいけないものはありそうな気がします。事務局案で分けてしまうことの有用性はあまりないのではないのでしょうか。

(事務局) 委託業務の内容ではなく、取り扱う情報に着目して分類するほうが良いという意見ですか。

(中村会長) 資料4ページに個人情報保護委員会のガイドラインの抜粋があります。そこに考慮事項が挙がっています。下から10行目の「求められる安全管理措置」以下に、「漏えいが生じた場合に本人が被る権利利益の侵害の大きさを考慮し、事務又は業務の規模及び性質、保有個人情報の取扱状況（取扱う個人情報の性質や量を含む）、保有個人情報を記録した媒体の性質等に起因する

リスク」とあります。こういう考慮事項に基づいて何か分類ができれば、そのほうが有用性が高い気がします。

事務局は恐らく、一つひとつの案件ごとに安全管理措置といっても非常に難しいので、類型化した上で判断していきたいという考えがあると思います。類型化自体には反対しませんが、有用な類型化がもっとありそうな気がします。(事務局) そうですね。

(中村会長) その事務でセンシティブな個人情報が取得される可能性があるものとか、件数で数千件が問題になるのか数万件が問題になるのかでも違ってくるかもしれません。皆さんはどうですか。

(大谷委員) 今の会長の考えに私も共感します。分類や類型化を試みるのはいいと思いますが、業務の性質から自動的に区分できるような安全管理措置はなかなか作りにくいと思います。区分するのであれば、委託業務の内容を縦軸に置き、横軸に取り扱う個人情報の種類を置き、その中で特にセンシティブな個人情報や要配慮個人情報又は大量の個人情報を取得しなければいけないもの等、気を遣うものに二重丸を付け、該当するものについては特別の安全管理措置の基準を置いて、その基準にどれだけ合致しているかという点を評価する等というやり方であれば意義があると思います。

ですが、業務の内容で振り分けをしてしまうと、本当に重要性が高いものや、特別に配慮が必要なものがこぼれてしまう可能性も出てくると思います。これまで審議会に附議された事案を仔細に見ても、一律に区分するのは難しいのではないかと感じています。

(中村会長) 今日特に何かを決めるわけではないですよ。

(事務局) 今日、初めて御意見を伺う事項ですので、何かを決めるわけではございません。

(鈴木委員) 今の会長と大谷委員の意見に私も賛成です。基本的にリスクの度合に応じてどう対応するかが基本なので、業務の内容というよりは、扱う個人情報自体の性質に着目するほうが重要なのかなという気がしています。今まで実際どういうところでどういう事故が起きているのか、改めて振り返って見たほうがいいのかなという気がしています。

(事務局) 個人情報保護委員会で作っているガイドラインの「権利利益の侵害の大きさを考慮し」という基準はもちろん見ていました。このような分類をするときに、横浜市においては、侵害が特に大きいものを第1種安全基準、大きいものを第2種安全基準、普通程度のものを第3種安全基準のような非常に抽象的な基準をつくり、著しく大きいのか、大きいのか、普通なのかという判断を各所管課に任せるようなパターンが多くあります。

これでは恣意的な分類もできてしまうかと思い、こういった基準を一つの案として考えてみました。

確かに今、指摘のとおり、同じアンケートでも扱うものによってリスクは様々だというところがあります。御意見を踏まえてもう一度考えてみます。

(中村会長) 次に、個人情報取扱特記事項についての「再々委託の解禁」について、どうですか。

(鈴木委員) 個人情報保護に関しては、委託して再委託して再々委託してという様に、先に行くほど意識の度合はどんどん薄まると思います。横浜市の職員と委

託先を比べたとき、個人情報保護することの重要性を同じレベル感で認識しているかという点、違ふと思います。それが更に再委託先、再々委託先となれば、リスクもどんどん高まりますし、モニタリングする目もどんどん行き届きにくくなります。

再々委託自体をバツとするほどのことなのかという意見はあるにしても、解禁する以上は、今まで以上に慎重な管理措置を講じていく必要があると思います。「研修をしてください」で済むレベルなのかという点や、研修したところで浸透していなかったら意味はないので、措置を講じるにも難しさはあると思いますが、是非検討してもらいたいと思いました。

(加島委員) 私は「絶対禁止」については是非外してもらいたいと思います。

具体的に例を示しますと、例えば国民健康保険の事務を国民健康保険団体連合会に委託した場合、連合会が事務の委託先となります。さらに、連合会がベンダーに委託して再委託という形になります。

今後、さらにベンダーがクラウドを扱う事務が発生するような場合は、再々委託になってしまい、クラウド利用ができなくなってしまう可能性があります。入力や搬送委託等もできなくなってしまう可能性があります。今はそのような制約がかなりあります。

その結果、先日の尼崎市のような事故が発生することになると、個人情報管理上最悪の事態となってしまうので、絶対禁止ではなく、管理に責任を持つ形で、委託については柔軟に対応してもらいたいです。

(事務局) 確かに、クラウドや色々なものが絡むと、形式的には4次下請や5次下請のようになってしまいます。それについては時代の流れとして避けきれない気がしていますので、その方向で検討します。

(大谷委員) 再々委託が闇に潜ることを避けるためには、個人情報取扱特記事項の中に、再々委託先に求める安全管理措置の水準や、再々委託先について情報提供を受けられる旨の規定が必要です。

直接報告を求めることができるか、立入検査の規定はあるかと思います。例えば、民間企業だと、プライバシーマークを認証する「J I S Q 15001」の要求事項と同等の安全対策を講じている事業者を選定しなければならないというような義務を課したりすることで再委託先等に一定の基準を設けています。単に解禁するだけでなく、安全管理措置にももう少し工夫を加えることはできると思いますので、この条項をもう少し変更していくことも選択肢だと思っています。

また、再々委託先について外国で個人情報が取り扱われることを絶対的禁止事項として一旦挙げた上で、やむを得ない事情で海外で取り扱わなければいけない場合の例外的な申請の取扱いも決める必要があると思います。委託でも海外の事業者への第三者提供は避けなければいけないと思います。一般的な再々委託の関係と、海外で情報を取り扱う場合の禁止事項、それから再々委託先として選定する場合の基準といったような条件を、特記事項や例外的に認める場合のルール整備等を併せて行うことで、委託の末端までのコントロールを有効化できるのではないかと思います。

(事務局) 正直、まだ思いが至っていない部分も多々あります。再々委託を認めることによって、求められる基準がゆるくなるようであれば、下請・孫請を助

長することになってしまいます。それでは本末転倒なので、基本的にはもともとの安全管理措置と同水準のものを求めていくようにしなければいけないと思いました。

また、海外での個人情報の取扱いについては事務局としては想定していなかったのですが、御指摘も踏まえて、海外へ委託する場合どういう定めをしていくべきなのか考えたいと思います。

先ほど「405万件の税務情報」という話もありました。規模が大きいケースもあり、海外への委託ということも十分あり得るかと思えます。そこも引き続き検討していきたいと思えます。

(中村会長) 現実的な問題として、再々委託を禁止することは今や不可能であろうと思えます。

一方で、再々委託、再々々委託とどんどん重層化することにより、そこに安全管理措置を義務付けたとしても、基本的に市と契約関係があるのは委託先です。どうしてもゆるくなっていく可能性があります。

再々委託を認めていくかどうかを担当課が判断していくと、業者から「再々委託が必要だ」と言われたら担当課が「仕方がない」と認めていく可能性も出てきます。

(事務局) 実務的にはそうなってしまうのではないかという気がします。

(中村会長) そうすると、担当課に再々委託や再々々委託を必要とする理由をきちんと報告してもらおうという、ハードルを少し設ける必要があるかと思えます。

それに当たっては再々委託についての要件について、原則は禁止した上で、「こういう場合に認めていく」というものを規則化しておいたほうがいいのかと思います。

クラウドや入力事務や搬送業務が問題であるなら、「こういう場合はいい」とか、明示したらどうでしょうか。どんどんルーズに再々委託が続いていくことにはすごく怖さを感じるころではあります。

(事務局) 同じ再々委託でも、よくあるクラウド的なものと、そうでないものとは審査基準を分けるような感じでしょうか。

(中村会長) そうですね。クラウドの利用に関しては、もう避けて通れない点なので、それを一つの層として認める必要があると思えます。厳しい基準を設けるというのはなかなか難しいと思えます。

(事務局) クラウド利用については届出事項として済ませるけれど、一般の再々委託は許可制にするような感じですか。

(中村会長) 多分そのような感じでしょうね。

それでは、もう一つ、誓約書の廃止に関してはどうですか。

(三品委員) 基本的には事務についての責任を負うのは受託先で、通常は法人です。従業員等々を含めた個人の責任が問題となる場合や、本市として責任追及することが想定されるのでしょうか。受託先でよからぬ考えを抱いた従業員が情報を故意に売ったりした場合、当然、受託先の責任は追及するにしても、個人を放っておいていいのかという話があるのかなと思えます。

従前の誓約書は、「研修を受けたこと」の誓約書です。最後のほうで「法令や条例をきちんと守ります」と誓約させています。これがある、ないで責任追及の可否が変わるのかという問題はありますし、例えば闇サイト等で情報を売り

さばいたら、さすがに誓約書等がなくても責任追及できるのだろうとは思いません。従業員個人が悪意で色々なことをした場合、一つの取っ掛かりになるのかと思って見ていました。

今回の改正点として、受託先が「研修実施報告書」を1枚で出す形態に変更する、ということで、従業員個人については受託先に完全に任せています。その点の是非は考えるべき点としてあるのかなと思います。例えば、他の書類で誓約させているのだったら「研修を受けた」という書類はあまり関係ないのかもしれませんが、その取扱いが私には分かりませんでした。

(事務局) 特にこの誓約書以外に、個々の従業員に出させている書類はないです。

例えば、悪いことをした社員が刑事責任を負わされるケースは当然出てくると思います。しかし、きっかけをつくったのが当該社員だからといって、横浜市が当該社員に賠償請求等をする事等は基本的には考えていません。やはり一義的には元請が我々の契約相手でもあります。今後の契約の仕様書なり特記事項に「下請、孫請会社に対しても責任を持って監督する」という点と「下請、孫請会社で何か不祥事が発生した場合でも、一義的な責任は全て元請が負う」という点を明示して、責任を追及していきたいと思います。

逆にいえば、それだけの責任を元請は負うのだから、孫請も責任を持って選ぶようにというプレッシャーをかけていきたいと考えています。

(三品委員) そうだとすると、この書類を変えてもプラスマイナスは全く関係ないということですか。

(事務局) そう想定しています。

(三品委員) わかりました。

(大谷委員) セキュリティや情報管理についての誓約書等に一般的に見られる形態と違い、横浜市に対して提出するようになっていっているところに違和感を覚えます。通常は、自分と雇用関係のある先に提出し、例えば、その写しを横浜市に提出することについて「異議がない」ことを述べる形で、間接的にその業務の従事者を特定しつつ、研修が行われた記録として書類を残すというのが一般的な手法です。その点から考えると、この誓約書については、雇用や契約関係を無視しているわけではないと思いますが、その辺の配慮が少し大ざっぱな印象です。

そのため、私は誓約書について改めるというのはよい考えだと思います。民間企業でも似たような書類を必ず交わしているのですが、リモート環境の普及により、記名押印はしないように変わりつつあります。ネット環境において、確実に本人に研修が行われたことや、十分な知識の教授がされたことの記録について、研修を実施する側に、証跡を残す責任を課したりしています。そのため、今後は自署記名押印はなくしてもいいと思います。

担当業務に従事しているのがどういう人なのか確認する必要があるれば、「誓約書」については様式として残し、従業員個人が直接雇用関係のある企業に提出した書類の写しを受け取る形で、研修記録を保存していくことについては、委託先における従業者監督義務を履行した記録として残してもらうという点で意味があると思います。

総じて、改めた方がよいというのが私の意見です。

(事務局) 確かに発注者と受注者の社員が、雇用関係等を飛び越えて直接書類の

やり取りをすることについては違和感があります。適切な形に改めたいと思います。

(中村会長) 基本的には今後「研修実施報告書」1枚を提出してもらおうという考えですか。

(事務局) 若干、表現は変更したいと思います、そのような運用を予定しています。

(中村会長) 例えば、これに別紙として、いつ研修をしたのか、あるいは、研修に参加した人の一覧を添付させる、という様な工夫があってもいい気はしています。研修を実施しなかったとしても、業務上特に問題がなければ、受託者が責任を問われることはないわけですよね。そうすると、受託者の中には、「研修はやったことにしておけばいい」という考えを持つ法人等があるかもしれません。もう少しプレッシャーをかけるために、研修の受講者一覧の様なものも付けさせたほうがいいのかと思います。

(事務局) 「いつ誰に対して研修を行った」という具体的なことを書いたものを、会社の責任で提出させるということですね。

(中村会長) そうです。参加した人の個人情報を取得することになりますが、それは従前の誓約書でも取得しているので、問題はないかと思います。

ほかに質問等がなければ、この件についてはこれまで出された意見を踏まえて事務局で検討するというところでよろしいでしょうか。

(各委員) <異議なし>

(中村会長) それでは事務局での更なる検討をよろしくお願いします。

(事務局) ありがとうございます。今後、毎月のように相談することになると思うので、よろしくお願いします。

(中村会長) 続いて、「報告事項」及び「その他」の「(1) 個人情報漏えい事案の報告」に移りたいと思います。事務局から説明をお願いします。

(事務局) 本日の追加配布資料を御覧ください。内容につきましては、担当係長から御説明いたします。

(事務局) <資料に基づき説明>

配布資料により内容を御確認いただき、何かお気づきの点がありましたら、事務局まで御連絡をいただければと思います。

(中村会長) ただいまの報告につきまして、何かございますか。

御質問等がないようでしたら、報告事項及び漏えい事案の報告について了承するというところでよろしいでしょうか。

(中村会長) 本日予定された議事は以上で終了です。事務局から何かありましたら、お願いします。

(事務局) 本日予定された議事は、以上でございますので、次回の日程を確認させていただきたいと思います。

次回の審議会は臨時会となります。

次回の日程でございますが、8月26日金曜日午後2時から、本日と同じくWEB会議での開催となります。申し訳ございませんが、WEB会議システムの接続確認のため、開始の15分前にはWEB会議システムに参加していただきますようお願い申し上げます。

事務局からは以上でございます。

	<p>本日はどうもありがとうございました。 (中村会長) それでは閉会とさせていただきます。 【閉 会】</p>
資 料 特記事項	<p>1 資料 (1) 第201回横浜市個人情報保護審議会次第 (2) 第201回横浜市個人情報保護審議会追加資料</p> <p>2 特記事項 次回は令和4年8月26日(金)午後2時から開催予定 (WEB会議の方法により開催予定)</p>

本会議録は令和4年8月26日第202回横浜市個人情報保護審議会において承認を得、確定しました。