平成２７年度第１回山梨県個人情報保護審議会議事録

１　日　時　　平成２７年6月9日（火）　午前１０時３０分～午後１２時１０分

２　場　所　　恩賜林記念館２階特別会議室

３　出席者（敬称略）
（委　　員）吉澤宏治、坂本玲子、堀内寿人、原敏、市川由美
（事 務 局）森田課長、関総括課長補佐、文書・情報公開担当（４人）
（市町村課）行政選挙担当（３人）

４　傍聴者数　　０人

５　会議に付した議題等
(1)山梨県個人情報保護審議会委員の任命書交付式
(2)特定個人情報保護評価
（住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務の第三者点検）
(3)その他
平成２６年度山梨県個人情報保護条例の施行状況について

６　議事の概要
(1)山梨県個人情報保護審議会委員の任命書交付式

○　個人情報保護条例第５９条第７項の規定により、委員が互選し、吉澤委員を会長に選任した。
○　続いて、同条第９項の規定により、吉澤会長が堀内委員を会長代理に指名した。

(2)特定個人情報保護評価

（議長）
まず、「全項目評価」について、事務局に説明をお願いする。

（事務局）
－　資料に基づき、特定個人情報保護評価の概要及び現在の状況について説明　－

（市町村課）
－　資料に基づき、全項目評価書の内容を説明　－

（事務局）
－　資料に基づき、内部点検について説明　－

（議長）
以上の説明について、質問等はあるか。

（委員）
　このシステムは、インターネットからは独立しているということか。

（市町村課）
　インターネットからは独立している。

（委員）
　生体認証を行うということだが、例えば、網膜で認証する場合には、「ものもらい」を患った場合にも認証できなくなることもある。その場合に、網膜での認証ができなくなるので、生体認証自体を外してしまうということがよく行われるが、その辺についてはどうか。

（市町村課）
　生体認証については、掌の静脈によるものとなっている。地方公共団体情報システム機構にも確認してみたが、認証する際の環境の変化にできる限り左右されない方法を採用したということである。

（委員）
　掌の静脈による方法でも、手術をしたりすると認証できなくなる。その場合に、その人は担当者から外すということであれば安心であるが、生体認証を外してパスワードだけでやってしまうということが現場ではよくあるがどうか。

（市町村課）
　まず、一つは両手を登録するようにしているので、片方の手で認証できなくても、もう一方の手で認証できる。それから、生体認証を経ないで操作をするということは認めていないので、仮に生体認証で認証できない場合には、複数の担当者のうちの一人が対応することになる。

（委員）
　私自身は、こういう分野では専門家ではないが、今回年金機構のいろいろな問題がある中で、一般的にはどの辺に弱点が想定されていて、どのような対策がされているのか、こういったことを一般の住民は考えたらいいのか。先ほど、パブリックコメントを１ヶ月くらい行ったところ、何もなかったということだったが、おそらくついていけてないだけであると思う。どの辺に問題があるのかということを簡単に説明してほしい。

（委員）
　簡単に説明するのは難しいかもしれないが、基本的には、システム上の保護措置と人的な管理ということがあると思うがどうか。

（市町村課）
　年金機構の問題は、社会保険システムという、ここでいえば住基ネットサーバのようなところから個人情報を抽出してインターネットに接続されている共有ファイルの方へパスワードをかけずに保管してしまっていたということだと思うが、現在、住基ネットにおいては、そのように情報を抽出してファイルを保管するということは行われていないし、そういうことはできない形となっているので、そのような心配はないのではないかと考えている。今後、マイナンバー法の施行後、システム的に住基ネットについてはインターネットとは分断されているが、例えば税務のシステムでマイナンバーを使える事務がある。そこで取得したマイナンバーの情報と住基ネット

が持っているマイナンバーの情報を照らし合わせて完全に一致するかどうか、税務が持っている個人番号が間違っていないかを確認するために、一定のデータを抽出して照らし合わせるということをするが、それについては、ネットワーク接続はしないということになっている。実際にはＣＤを用いて行うが、サーバ室内にそれぞれのサーバがあるので、閉鎖された室内においての媒体の移動ということで実施するので、ネットワークで漏れるとかということはない。また、人的な面になるが、それが外部に持ち出されるということがないようにしっかり対策を取る。まずは、閉鎖された中で処理を行うということで安全管理を担保したいと考えている。住基ネットについては、他のネットワークとは接続されていないということが一番の特徴だと思う。

（委員）
　業務端末と代表端末があるようであるが、両方とも閉鎖された環境の中にあるのか。

（市町村課）
　代表端末については、入退室管理のある部屋にあるが、業務端末については、例えばパスポートセンターにおいて、かつては住民票により住所を確認していたものを業務端末を用いて検索することによって住所の確認ができるということでやっている。その業務端末については、パスポートセンターの中にあるので、物理的に来庁者から見えないところに置くなどの環境は整えている。また、生体認証をして操作するが、画面を開きっぱなしにしないなどの人的な管理をするということでやっている。

（委員）
　私は、一般県民の視線ということで質問させてもらう。今回の年金機構の情報漏洩ということで非常に関心がある部分であるが、今、ネットワークと接続をしないということで、それは一安心である。ただし、市町村の職員が一番操作をする中で、市町村の住基ネット所管課の職員を対象とした研修をするということであるが、やはり人が行うという中で、今、性善説に立っているなという感じがする。この辺の厳格な管理というのは徹底してできると言えるのか。

（市町村課）
　マイナンバー法に移るに当たっての手だてとしては、こちらでも年に１回講師を招いて研修をしている。例えば、そのテキストの中には今回のような標的型の攻撃に対する危険性ということも情報として入っている中で研修をしている。そこから、市町村においては、全国統一的なチェックであるが、だいたい１２０項目くらいの問のあるチェックシートにより、研修を受けてから４週間で自己評価を行うことになっている。それを県で集計してその結果を総務省でヒアリングを受けて、ヒアリング時に示された留意点などを、市町村にフィードバックするという形を取っている。研修会は５月１８日に実施した。マイナンバー制度に移行するので、今現在、自己評価をしてもらっている。１０月にマイナンバー制度に移行したあとのチェックシートも８月頃出る予定になっている。それに基づいて、マイナンバー制度が施行された以後、今年度はもう一回チェックをすることになっている。住基ネットに関しては全国的な仕組みであるので、そのような形で安全確保を行うこととしている。

（委員）
　業務端末は、直接、都道府県サーバにつながっているということか。

（市町村課）
　業務端末は、直接、都道府県サーバにつながっている。

（委員）

市町村コミュニケーションサーバが、直接、全国サーバにつながっているのか。

（市町村課）

市町村コミュニケーションサーバとは直接にはつながっておらず、都道府県サーバを通じてということになっている。まず、そこで市町村からの通知を受けて、都道府県のファイルを更新して、そのあとその情報が機構の方に通知されるということになっている。

（委員）

集約センターのところでつながっているように書いてあるが。

（市町村課）

つながっているが、仕組み上は市町村が県へ通知をして、県が機構へ通知するということになっている。

（委員）

システム的に直接のアクセスはできるのか。

（委員）

物理的にはつながっているが、論理的にはつながっていないということだと思う。

（委員）

業務端末については、先ほど、パスポートセンターにあるということだったが、どこにどれだけあるのか。

（市町村課）

パスポートセンターに４台、県税事務所に２台、パスポート業務を行う４つの地域県民センターにあるが富士・東部だけは２台あり地域県民センターの計で５台、全部で１１台である。

（委員）

入退室管理がされているのは代表端末であり、業務端末については入退室管理をしているということはないのか。

（市町村課）

そうである。

（委員）

（資料３【別図】に）「山梨県の他の執行機関又は他部署」というものがあって、２－①は本人確認情報の照会、２－②は本人確認情報の提供・移転と書いてある。これは業務端末を使わずに行うのか。

（市町村課）

業務端末を使って行う。

（委員）
　そうすると、５－①との違いがよく分からない。画面で見られるようにした瞬間に、もう情報の提供・移転だと思うが、２の場面と５の場面が違うのはどこか。

（市町村課）
　これについては、マイナンバー法との関係であるが、位置づけとして、代表端末を管理している市町村課のような部署において利用する場合と、同じ知事部局の中でも税務課のような違う部署の場合は、マイナンバー法上、それぞれ、税に関しては地方税法に基づく賦課徴収ということでマイナンバーを利用することができるが、利用できる事務があるからといって相互に融通して共通して使っていいというわけではなくて、その場合は移転ということで位置づけられている。５にある端末による閲覧とは異なるということで整理をしている。

（委員）
　２の場面と５の場面というのは、都道府県サーバから情報を取ってくる「人」が違う「部署」が違うということか。

（市町村課）
　部署が違うということもあるし、県税の申告で新たにマイナンバーを取得するということがある。その時に、窓口で本人確認をして番号を取得するわけであるが、本当にそれが真正な番号なのかということを確認するために、一番確かなのは、他人と全く違う４情報と番号にくっついている住基ネットの情報というものなので、住基ネットの情報を、例えば１００件申請があった場合にはデータ上、整合を確認して、例えば不一致という結果が出ればはじくような形で処理をするということになっている。そのような時に、本人確認情報自体をいったんシステムから抽出するという仕組みになっているので、照会して、検索して、閲覧するということとは違った形であり、情報の照会と提供・移転というものは別のものとして区別されている。

（委員）
　そうすると、検索できる場面というのは限定されているのか。

（市町村課）
　検索できる場面というのは、従来から住民基本台帳法の別表にある、県が利用できる事務ということになっている。

（議長）
　それでは、事前に質問をいただいているものがあるので回答をお願いしたい。

（市町村課）
・１つめの質問について
　（事前質問内容）Ｐ１２　Ⅱ６①
　　生体認証について、生体認証の種類によっては用意に突破される。どのような種類のものを用いているのか。また、複数の生体認証を組み合わせているのか。
　（回答）
　　これについては、先ほども説明したが、掌の静脈を読み取る装置によるということで、全都道府県・市町村で採用されている。ＩＤ、パスワードの入力とともに、生体認証ということになっている。複数の生体認証を組み合わせているかということであるが、本県だけでは、

例えば二重の生体認証ということを採用するということは困難な状況である。

・２つめの質問について　Ｐ１４　Ⅲ2リスク４

（事前質問内容）

専用のアプリケーションを用いるとあるが、そこへの入力直前までに申請書類など一時的にでも紙などに情報が記される可能性が高い。その媒体の取扱い方法や取扱い許可者の管理はどうなっているのか。

（回答）

特定個人情報の入手については、市町村コミュニケーションサーバから専用回線によって都道府県サーバに送信されることになっている。市町村においては、転出・転入の届けについて、住基ネットの窓口であるコミュニケーションサーバに直接入力されるのではなく、初めに既存の住基システムということで、コミュニケーションサーバの前段階で各市町村が独自に持っている住民基本台帳のシステムがあり、そこに転出入の情報が入力され、既存の住基システムのデータのうち（既存の住基システムのデータには、選挙人名簿への登載の有無、国保の情報などが入っている）、本人確認情報ということで、４情報などのみがコミュニケーションサーバに送信され、さらに都道府県サーバに送信されるという仕組みになっている。そのような仕組みなので、既存の住基のシステムに入力がされる際には紙などに情報が記される可能性はある。当該紙媒体の取扱いとか、取扱許可者の管理については、市民課長とか住民課長といった許可者のもとに紙媒体を適切に管理する必要があると、住基ネットの所管課としては考えているが、これらについては市町村の事務であるので、直接は市町村における住基事務の保護評価の中でリスク対策等が記載されることとなる。

・３つめの質問について　Ｐ１５　Ⅲ3リスク４

（事前質問内容）

バックアップファイル以外にファイルを作成しないとある。また、保守作業においての操作履歴を残すことにしているのか。

（回答）

これについては、保守作業における操作履歴については残るということになっている。その操作履歴については、自動的にバックアップされて保存されるという仕組みになっている。

・４つめの質問について　Ｐ１５　Ⅲ3

（事前質問内容）

スクリーンセーバー項目における長時間とは具体的にどれほどか。また、それはきちんと客観的な根拠のある数値設定になっているのか。

（回答）

操作中については、基本的には離席しないということになっているが、ログオフしないままで離席してしまうことにより長時間、画面に個人情報が表示され続けるということは不適切であるので、スクリーンセーバーとかパスワードロックの起動については、５分で設定をしている。それについて客観的な根拠のある数値設定であるかどうかということであるが、さきほど話をしたチェックシートによる自己チェックをする際の指針として、住基ネットのセキュリティ対策に関する指針が示されているが、それにおいても具体的に定められていないので、客観的ということでは答えきれない部分があるが、５分ということで設定しているという実情である。

・５つめの質問について　Ｐ１５　Ⅲ3

（事前質問内容）

ハードコピーの取得とあるが、ハードコピーが可能なシステムであるということか。ハードコピーの流出は大きな懸念事項であるが、操作ログにきちんと残るのか。デジタルカメラで画面を撮ることもハードコピーであるが、そのような行為に対する規律はあるのか。

（回答）

委託先の地方公共団体情報システム機構及びＹＳＫ－ｅＣＯＭについては、そもそも本人確認情報にアクセスできないので、ハードコピーは取得できない。職員による画面のハードコピーについては、取ることはできる状況になっているが、基本的にそのような行為は禁止している。特別な必要があれば、セキュリティ責任者が各部署にいるので、申請してもらって許可を得てからということになると思う。そして終了後には、セキュリティ責任者がハードコピーの確認をするということになる。

・６つめの質問について　Ｐ１５　Ⅲ3

（事前質問内容）

保存を禁ずるとあるが、そもそも保存が可能なシステムなのか。ベネッセにおける漏洩事件の根本原因であったが、教育以外にきちんと技術的な（運営を人間に頼らない）対策が取られているのか。

（回答）

委託先においては画像データを保存することはない。システム自体では画像データを保存するという設定はしていない。

・　７つめ、８つめの質問について　（共に）Ｐ１７　Ⅲ4

（事前質問内容）

委託先従業員に対する監督・教育とあるが、これはしかるべき水準を満たす知識・技術・倫理観を持つということを明確に規定しているのか。一言訓示を聞いただけでも教育を受けたことになる、情報取扱者の国家基準である「ＩＴパスポート試験」の合格者など客観的な基準を定めないと安心できない。

（回答）

機構については直接個人情報にアクセスすることができない。ＹＳＫ－ｅＣＯＭについても、ＹＳＫ－ｅＣＯＭに権限設定されている業務は、月次の住民基本台帳人口の統計処理ということで、それは直接個人情報を見るということはできない。それ以外の業務としては、システムに直接携わることのないウィルスパターンファイルの反映をしてもらっている。委託契約書に、個人情報取扱特記事項というものを定めており、委託先は受託業務従事者に対する教育、研修を義務づけられている。これは、特記事項の内容とか、個人情報の守秘義務、目的外使用の禁止、個人情報保護条例の罰則の対象になるということについて、委託先の方で必要な教育、研修を行わなければならないことを定めている。ＹＳＫ－ｅＣＯＭにおいては、社内に情報管理の資格者として、情報セキュリティスペシャリストという資格を持つ者が２名いるということで、そのような資格者の管理のもとで、代表端末機器の運用、管理を行っている。

・９つめの質問について　Ｐ２０　Ⅲ7リスク１④

（事前質問内容）

年金機構の問題で、この点（安全管理体制・規定の職員への周知）の不十分さが明らかになっている。この項目は「特に力を入れて」という水準でなければ危機意識を持っているとは言えないのではないか。

（回答）

安全管理体制とか、職員への周知については、年１回、１～２時間程度、総務省又は機構が作成した全国の統一的なテキストにより、総務省、機構の職員を講師として住基ネット担当職員向けの研修を実施している。その研修会後には、総務省が作成した全国一律のチェックリストにより自己点検を実施している。また、職員は情報政策課が実施している情報セキュリティ研修も受けている。

・１０個めの質問について　Ｐ２２　Ⅳ2

（事前質問内容）
「ネットワークの利用について」は「必要な知識の習得」とあるのに対し、「セキュリティ」に関しては「意識の向上」としか記述されていない。意識は「自覚をもつ」「気を付ける」といった精神的な話である。セキュリティ対策において、知識もなく意識だけ向上しても様々な問題の発生を防止することはできない。知識に関する教育はどうなっているのか。
（回答）
先ほど話をした研修会の資料中では、セキュリティ対策について、標的型攻撃の脅威や事例とか住基ネットにおける対策などセキュリティに関する知識の習得に重点を置いた内容となっている。また、情報政策課で実施している一般の職員向けに実施している情報セキュリティ研修についても同様に標的型攻撃の脅威や事例をかなり掲げている。なお、記載ぶりについては、ご指摘のとおりと思う。ただ、中身については、知識の向上ということももちろん重要だと考えている。

（議長）
ただいま回答をいただいたが、補充的にさらに質問があればお願いしたい。

（委員）
どこに対するという話ではなく、いやなことを言うつもりで話をするが、山梨県が全国基準よりも厳しい取り組みをしてはいけないというルールはないのだということを考えてほしい。特にパブリックコメントの意見が全くなかったという現状は危険ではないかと思う。というのは、意見がなかったから反対がなかったということではないと思う。そんなことがあることも知らなかったということならまだしも、問題があった時に、県とか我々側としては、パブリックコメントを求めたのに何も答えなかったではないか、と言いたくなることもあるかもしれないが、そんなことは関係なく、矢面に立たされると思う。そういった時に、例えば、神奈川県藤沢市の市役所の関係でニュースになっていたが、職員に攻撃を仕掛けたら、何割かが平気でファイルを開いてしまったということである。藤沢市も、多分、全国で実施しているチェックリストをやっているはずである。それでもこうだということを考えていると、おそらく、完璧に教育が行われているということ自体を想定してはいけないということになると思う。それゆえに、ＩＴパスポートの資格試験は国家試験なので、国が情報取扱者は国民全員であるということを言って始めている試験なので、それくらいの知識がなければならない。例えば、ファイルの拡張子という概念を知らない人間が添付ファイルを開く開かないの判断ができるわけはないし、標的型攻撃という話を聞いていても実際にやられた時に全く理解していない。私は学生に攻撃を仕掛けることを授業でやっているが、７割は引っかかる。なので、残念ながら、知識がある人間は避けられるが、ない人間は避けられない。そういった授業型の研修では限界があるということは、私も教育をやっているので感じる。こればっかりは、山梨県は他の県よりも一段階厳しい教育をやっているよ、と言えるくらいにやらないといけない。授業のような研修を増やすのではなくて、資格を取ってこい、というくらいのことでなければならないと思う。責任者がＩＳＯの規格くらいの研修に行っているのは知っているが、おそらく、業務端末を使う方は責任者ではないので、そうではないと思う。例えば、職場にスマートフォンを置いてある、とかデジカメを身に付けながら仕事をしている状態で、それも規制されていない。また、アルバイトの職員がマイナンバーが記載された書類を目にすることができるということ自体に問題があると思う。ということで、もう一段階踏み込んで、他の県とか、国がどうのこうではないということで考えてほしい。

（議長）
その他に何かあるか。

（委員）
　パスポートセンターなど、業務端末のある場所には、監視カメラは設置されているのか。

（市町村課）
　監視カメラの設置はない。

（委員）
　人的管理が難しいということは実感できるので、そういうところの管理ももっとしてもらえればと思う。

（委員）
　評価書のＰ５の備考欄の（注２）にある媒体連携とは、具体的には何をさすのか。

（市町村課）
　先ほど、税の話をした。税務課については他部署に該当するが、住基ネットの本人確認情報の提供として、１件ごとに確認する場合と、一括で１００件とかのデータを抽出するという機能もある。ここで言っているのは、一括提供の場合ということであるが、媒体連携というのは、住基ネット自体が他のネットワークとつながっていないので、ＣＤなどの媒体でやりとりするということになる。これとの対比概念とすれば、ネットワーク連携ということになるが、セキュリティを確保したうえで、ネットワーク連携を取ることもできるということで、他県ではそういうところもある。媒体連携をすると手間がかかり、ネットワークにつなぐと便利だけれども危険性がある。本県では、媒体連携でやろうということで、方針を決めている。そのことを記載している。一括提供の方式により本人確認情報の提供を行う場合には、その情報連携に電子記録媒体を用いるということである。

（委員）
　多分、そういうことだと思っていた。そこで、オンラインのセキュリティについてはよく書いてあるが、そのような媒体に記録された情報のことについてはどのように保護措置が執られているのか。

（市町村課）
　媒体連携に関しては、Ｐ２０の７⑤に記載している。入退室管理を行っているサーバー室の中で行うこととしている。媒体連携は、税務のサーバーからデータを落として住基のサーバーに読み込ませることになり、その媒体に関してもサーバー室内のラックにきちんと保管するということになっている。外へは持ち出さない。入退室管理を行っているサーバー室内にサーバーを置き、その中で処理を行う。

（委員）
　これは意見である。一つは、私は業務端末が都道府県サーバにつながっていると思っていなかった。代表端末が乗っ取られるということは想定していないし、住基ネットの専用の回線が乗っ取られるということも考えていない。一番考えられるのは、業務端末における違法な取扱いということが一番危険性が高いと思う。業務端末に関する管理というものは、もう少ししっかりやってもらった方がいいのではないかと思う。
　もう一つは、Ｐ１５のリスク４のところで、「システム上管理権限を与えられた者以外は、情報

の複製は行えない仕組みとする」となっているが、おそらく、成りすましがあれば複製できてしまうのではないかと思う。そういう意味では業務端末のところが危険ではないかと思う。

それから、評価書の内容について一点確認させてほしい。内部点検結果表の２ページ目の一番下から２つ目の７２のところである。「７２．特定個人情報を取り扱う従業者等に対しての教育・啓発や」のあとに「違反行為をした従業者等に対する措置」ということが書いてあるが、評価書には後半の部分が書かれていない。ここの部分を、評価書に書き加えた方がいいと思う。

（委員）

先ほど委員が言った、記録媒体の件である。記録媒体をラックに保存するということを言っていたが、そのサーバ室への入退室は入退室カードでやっていて、代表端末は生体認証でやっているということだが、記録媒体については当然個人情報が入っているが、それを部屋から持ち出す行為は掌認証を経ない。これについてはセキュリティが一段低くなる。ということで、記録媒体を部屋の中に少しでも残しておくのならば、部屋自体に掌認証を入れないと、全体のレベルが下がってしまう。

（議長）

最終的には答申という形でまとめることになるが、事務局に答申案を作成してもらい、委員から意見をもらうということにしたい。最終の答申については、その結果を踏まえて、次回の審議会で確定させるということにしたい。

（議長）

その他に何かあるか。

（各委員）

なし。

（議長）

それでは、「特定個人情報保護評価（住民基本台帳ネットワークシステムに係る本人確認情報の管理及び提供等に関する事務の第三者点検）」は以上とする。

(3)その他　　平成２６年度山梨県個人情報保護条例の施行状況について

（議長）

その他として何かあるか。

（事務局）

「平成２６年度山梨県個人情報保護条例の施行状況について」説明する。

（事務局）

－　資料に基づき、平成２６年度山梨県個人情報保護条例の施行状況について説明　－

（議長）

以上の説明について、質問等はあるか。

（各委員）

なし。

（議長）

以上をもって議事を終了する。