

平成27年10月26日

千葉市情報公開・個人情報保護審議会
会 長 稲 垣 総 一 郎 様

特定個人情報保護評価部会
部会長 多 賀 谷 一 照

特定個人情報保護評価部会における調査審議の結果について（報告）

当部会にて、調査審議した結果、下記のとおり報告します。

記

1 審議事項

行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号。以下「番号法」という。）第27条第1項に基づく特定個人情報保護評価について

- (1) (新) 福祉システム（後期高齢者医療事務）
- (2) 新国民健康保険システム（国民健康保険に関する事務）
- (3) 国民年金システム（国民年金に関する事務）
- (4) 介護保険システム（介護保険に関する事務）

2 調査審議の内容

- (1) 上記システムに係る全項目評価書（案）を確認した。
- (2) 部会での意見と意見に対する主な対応状況は、別紙1から別紙3までのとおり。

3 部会の意見

番号法、特定個人情報保護評価に関する規則、特定個人情報保護評価指針、千葉市個人情報保護条例等の規定に照らし、慎重に調査審議した結果、現段階における評価としては妥当なものと認められる。

なお、広域連合のセキュリティを確保する仕組みについては、今後とも引き続き検討及び改善を進められたい。

4 審議経過

- (1) 平成27年 8 月 27 日 第5回部会
- (2) 平成27年10月 5 日 第6回部会

部会での意見と意見に対する主な対応状況について（全システム共通）

NO.	部会での意見	対応状況
1	<p>「※」の説明書きについて</p> <p>「※」の表記は、全国統一の様式の一部であるとしても、その説明書きを書かないと、市民は分かりにくい。</p>	<p>対応済み</p> <p>様式のルール上、欄外には入力できないため、Iの1-②「事務の内容」の一番下に、1行空けて【凡例：「※」重要事項】と記入することとした。</p>
2	<p>業務共通システムの取扱いについて</p> <p>業務共通システムは、4つ事務のシステムすべてに連携するのであれば、すべての事務において、評価の対象とすべきである。</p>	<p>対応済み</p> <p>4つの評価書すべてに、取り扱うシステムの一つとして、業務共通システムの概要（名称、機能、接続）を同一内容で記載することとした。</p>
3	<p>構成図の記載について</p> <p>構成図に盛り込む内容については、必要に応じて、統一すること。</p>	<p>対応済み</p> <p>特定個人情報ファイルを使用するシステムや、特定個人情報の入手元についてすべて記載し、取得、収集、保管、利用、提供といった情報の流れを分かるようにするとともに、記載方法の統一を行った。</p>
4	<p>入手元・入手方法の再確認について</p> <p>例えば、「②入手方法」欄に「情報提供ネットワーク」が含まれているのであれば、当然、「①入手元」欄に、国の機関や他の自治体が含まれると思われるので、このようなことを含めて再確認すること。</p>	<p>対応済み</p> <p>再確認を行い、必要に応じて評価書を訂正した。</p>
5	<p>記録項目の記載方法について</p> <p>セキュリティの観点から、記録項目をランダムに並べて記載すること。（実際のファイルレイアウトと異なる順番での記載）</p>	
6	<p>個人番号・本人の確認方法について</p> <p>確認の方法を統一すべきである。</p>	<p>対応済み</p> <p>個人番号カード、通知カード、運転免許書、旅券の4つは基本的に記載することとし、記載方法の統一を図った。</p>

7	<p>紙媒体・電子データに対する漏えい・紛失に関する措置について</p> <p>紙をいつまでも保管していると漏えいのリスクが高まるので廃棄のルールを定めて、できるだけ早く廃棄すること。</p> <p>意味が分かりにくい表現が見受けられるので記載方法を統一すること。</p>	<p>対応済み</p> <p>下記内容について記載することとし、必要に応じて評価書の追加、修正を行った。</p> <p><内容></p> <p>特定個人情報の入手に関しては、次の点について職員等に対する教育を徹底する。</p> <p>【紙媒体に対する措置】</p> <ul style="list-style-type: none"> ・特定個人情報を記録した紙媒体は定められた保管場所で施錠管理等を行い、漏洩・紛失を防止する。 ・紙媒体を窓口で受け取り後、事務処理が完了したら、速やかに保管場所で管理するよう徹底する。 ・保存期間が終了するなど、保有する必要がなくなった個人情報については、速やかに廃棄する。 <p>【電子データに対する措置】</p> <ul style="list-style-type: none"> ・特定個人情報が記録された電子データについては、電磁的記録媒体を用いた連携を極力行わないこととし、記録媒体を使用する場合は定められた担当者のみが作業することとする。事務が完了したら速やかに記録媒体から電子データを消去し、作業状況を記録する。 ・情報の入手はインターネットにつながるネットワークでは行わない。 <p>【業務共通システムに対する措置】</p> <ul style="list-style-type: none"> ・業務共通システムについては、情報の暗号化を実施し、また各業務システムの専用回線とのみ情報をやり取りすることで、漏洩・紛失のリスクを防止している。
8	<p>外部ネットワークとの分離について</p> <p>外部ネットワークとの分離について、すべてのシステムで対応しているかを確認し、その旨を統一して記載すること。</p>	<p>対応済み</p> <p>外部ネットワークと分離していることが確認できたので、下記内容について記載することとし、必要に応じて評価書の修正を行った。</p> <p><内容></p> <p>インターネットを扱う端末と業務システムを扱う端末を分けており、業務システムで使用する端末については外部と接続していない。</p> <p>【不正アクセス対策】</p> <ul style="list-style-type: none"> ・インターネットなどの外部ネットワークと分離し、外部ネットワークからの不正アクセスを防止する。 ・データに対する不正アクセスを防止するため、サーバ上のデータ保管フォルダに対してアクセス制限及び暗号化を行う。

9	<p>アクセスログの確認について</p> <p>アクセスログを記録しているだけでは不十分であるので、定期的に確認すること。</p>	<p>対応済み</p> <p>下記内容について記載することとし、必要に応じて評価書の追加、修正を行った。</p> <p><内容></p> <p>情報システム責任者がログ記録を取得し定期的に確認を行う。特に一定時間ログオンを継続した者について、定期的に所属課あてに通知し、利用目的等を報告させるなど、不正な利用の牽制を行う。</p> <p>【〇〇システムにおける措置】</p> <ul style="list-style-type: none"> ・情報システム責任者がログ記録を取得し定期的に確認を行う。特に一定時間ログオンを継続した者について、定期的に所属課あてに通知し、利用目的等を報告させるなど、不正な利用の牽制を行う。 <p>【業務共通システムにおける措置】</p> <ul style="list-style-type: none"> ・システムのアクセスログ管理機能により、職員の認証ログの管理を行うことにより、いつ、誰がシステムにアクセスしたかをログに記録する。 ・記録したログについては、一定の期間保管し、定期的に確認を行う。
10	<p>委託先、再委託先への罰則規定について</p> <p>契約を締結する際の確認として、委託先、再委託先への罰則の適用に係る明記について、統一して記載すること。</p>	<p>対応済み</p> <p>下記内容について記載することとし、必要に応じて評価書の追加、修正を行った。</p> <p><内容></p> <p>契約時においては、契約業者に個人情報管理責任者を設置させ、個人情報の適正な管理をさせることとするほか、目的外の利用禁止、複写の禁止など、個人情報保護条例等に基づき事務の委託・再委託を行う場合に、その業務を行う者が講じなければならない事項を定めた個人情報取扱特記事項や関係法令の罰則規定を明記した契約書により、契約締結する。</p>
11	<p>消去のルールについて</p> <p>委託時の消去等のルールについて、統一して記載すること。</p>	<p>対応済み</p> <p>下記内容について記載することとし、必要に応じて評価書の追加、修正を行った。</p> <p><内容></p> <ul style="list-style-type: none"> ・委託が終了した場合、個人情報を委託元に返還、破棄、もしくは消去しなければならない。 ・委託元の求めに応じ、破棄、消去の方法、完了日等を報告する旨を規定し、必要に応じて、職員がその内容を確認する。

部会での意見と意見に対する主な対応状況について
(後期高齢者医療事務（広域連合の標準システムの取扱いについて）)

NO.	部会での意見	対応状況
1	<p>再委託の必要性について</p> <p>現在、再委託をしている再委託先について、その必要性について確認すること（また、今後、新たに再委託をする場合は、その確認を慎重に行うこと。）。</p>	<p>対応済み</p> <p>委託先の契約は5年契約で、前回は平成24年度に契約を行っていること、契約の方法は公募型プロポーザル方式で、委託先と再委託先も含めた履行体制や業務内容・価格を含んだ提案書を審査し決定された契約であること、従って、事前に仕様に適合した再委託先の選定が行われ、再委託先の技術を要することにより業務全体が行える委託契約であることを確認した。</p>
2	<p>委託先、再委託先の社員の作業場所について</p> <p>委託先、再委託先の社員が作業を行う場合、広域連合の施設内や、広域連合が契約しているデータセンターに来て作業を行うのか、あるいは、社内にデータを持ち帰って作業をするのか確認をすること。</p>	<p>対応済み（一部については今後確認）</p> <p>個人情報を取り扱う業務を行う場所はデータセンター内、及び広域連合内のみ制限しており、それ以外の外部で個人情報を取り扱う業務を行わないこと、委託先・再委託先の会社内で行う業務はプログラム構築など、個人情報を取り扱わない業務に限定していることまでは報告されているので、今後、その証拠の確認を行い、その内容によっては、さらなる検討及び改善を求めることとする。</p>
3	<p>サーバーの設置場所について</p> <p>広域連合のサーバーは、広域連合の施設の中にあるのか、あるいは、データセンターにあるのか。データセンターにある場合、データセンターとの契約関係はどうなっているのかを確認すること。</p>	<p>対応済み</p> <p>広域連合のサーバーについては、経費節減のため国保連合会が契約する県内の外部施設（データセンター）と同じ場所で共同運用していること、データセンターの運用・管理業務委託は、「広域連合電算処理システム運用業務委託」の再委託先として契約していること、また、その他にサーバーの共有部分の使用料については国保連合会と賃貸借契約を行っていることを確認した。</p>

4	<p>セキュリティ監査を行う職員について</p> <p>委託先、再委託先に対して、広域連合の職員によるセキュリティ監査を年に一回行っている、とのことであるが、その職員はセキュリティについて十分な知識を持っているのか。また、どんな監査をしているのかを確認すること。</p>	<p>対応済み</p> <p>セキュリティ監査には2種類あり、1つは年に1回、データセンター、委託先に対して、広域連合の管理職、及び電算担当職員が情報セキュリティポリシー等により契約書の確認等を行う事務的な監査であること、また、その他、2～3年に一度、広域連合の委託による情報監査業者による、広域連合、委託先、データセンターに対する外部監査を行っていることを確認した。</p>
5	<p>外部ネットワークとの分離について</p> <p>インターネットなどの外部ネットワークと分離し、外部ネットワークからの不正アクセスを防止する必要があるが、広域連合のシステムでは対応できているのかを確認すること。</p>	<p>対応済み（一部については今後確認）</p> <p>標準システムについて、外部ネットワークとは物理的に分離しているとのことまでは報告されているので、今後、その証拠の確認を行い、その内容によっては、さらなる検討及び改善を求めることとする。</p>
6	<p>再々委託先等の履行確認について</p> <p>再々委託や再々々委託の相手方との契約関係について、甲が乙に対して要求していることと同じような状況になっているのかを確認すること。</p>	<p>改善を求める</p> <p>1の契約書等の確認時に、再々委託先や再々委託先に対する承諾書に形式的な不備があった件等を踏まえ、今後、引き続き再委託状況の確認を進めるとともに、さらなる検討及び改善を求めることとする。</p>
7	<p>再委託先等に対する監査について</p> <p>再委託先に対する監査を行っているとのことであるが、どのような監査を行っているのか、システム面だけでなく、契約書等（承諾書や特記事項、承認申請書、履行体制図など）のチェックまで含めて行っているのかを確認すること。</p>	<p>改善を求める</p> <p>今後、外部監査の実施状況を確認を進めるとともに、さらなる検討及び改善を求めることとする。</p>

部会での意見と意見に対する主な対応状況について
(中間サーバー・ソフトウェアのアクセスログを確保する仕組みについて)

NO.	部会での意見	対応状況
1	<p>中間サーバーについて</p> <p>中間サーバー・ソフトウェアのアクセスログを監視する仕組みについて、千葉市において適切な監視が行えるよう検討を進めること。</p>	<p>対応済み</p> <p>中間サーバーのアクセスログ監視については、国に対し、ログの仕様等の提示を求めている状況であり、国から回答が得られた段階で、その内容を踏まえ、ログ監視等適切な対応を行う。</p> <p>なお、中間サーバーのアクセスログ監視と併せて、千葉市独自で行うログ監視の仕組みについても検討を行っている。職員が端末から行った操作内容について、アクセスログを取得し、監視を行う仕組みを整備する予定である。</p>