（平成２７年１０月５日資料）

資料３

全項目評価書の主な修正事項（4事務共通部分）

◆千葉市の評価書（4事務）のレベルを合わせて、標記を統一すべきである、という指摘を受けての修正事項です。

◆評価書項目の、「Ⅰ」は基本情報、「Ⅱ」は特定個人情報ファイルの概要、「Ⅲ」は特定個人情報ファイルの取扱いプロセスにおける対策、です。

No.	評価書の項目		該当ページ	指摘事項	内　容	対　応　（　修　正　等　）
1	Ⅰ-1	Ⅰの「1．特定個人情報ファイルを取り扱う事務」の「②事務の内容」欄	高齢・・P3 国保・・P3 年金・・P3 介護・・P3	「※」の説明書き	「※」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。	様式のルール上、欄外には入力ができないため、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。 なお、表題「Ⅲ　特定個人情報ファイルの取扱いプロセスにおける対策」の右横にある「※（7．リスク1⑨を除く」の表記については、全国統一の、様式の一部である。
2	Ⅰ-2	Ⅰの「2．特定個人情報ファイルを取り扱う事務において使用するシステム」	高齢・・P5 国保・・P5 年金・・P4 介護・・P4	業務共通システム （庁内連携システム/宛名システム）	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。	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。
3	Ⅰ 別添1	Ⅰの（別添1）「事務の内容」	高齢・・P7～10 国保・・P7～14 年金・・P5 介護・・P7	構成図	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。	対応済（※詳細は各評価書を参照） 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。 ・業務共通システムとの連携についてすべて記載。 ・情報の流れの凡例について、「特定個人情報の流れ」と「特定個人情報以外の流れ」に統一。 ・住民基本台帳ネットワークシステムを使用する場合は記載し、システムと接続しているわけではないので、「目視で確認」していることを表示。
4	Ⅱ-3	Ⅱの「3．特定個人情報の入手・使用」の「①入手元」欄、「②入手方法」欄	高齢・・P12 国保・・P16 年金・・P7 介護・・P9、31、49、68、81	①（入手元）、②（入手方法）の確認	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。	対応済（※各評価書を参照）
5	Ⅱ 別添2	Ⅱの（別添2）「特定個人情報ファイル記録項目」	高齢・・P18 国保・・P24 年金・・P12 介護・・P86	記録項目の記載の順番	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記載すること。）	対応済（※各評価書を参照）
6	Ⅲ－2	Ⅲの「2．特定個人情報の入手」の「リスク1」欄及び「リスク3」欄	高齢・・P19、20 国保・・P38 年金・・P13 介護・・P87	個人番号・本人確認方法	確認の方法を統一すべきである。	確認書類として、「個人番号カード、通知カード、運転免許証、旅券」の4つについては、基本的に記載することとした。
7	Ⅲ－2	Ⅲの「2．特定個人情報入手」の「リスク4：入手の際に特定個人情報が漏えい・紛失するリスク」の「リスクに対する措置の内容」欄	高齢・・P21 国保・・P39 年金・・P13 介護・・P88	紙媒体に対する措置、電子データに対する措置	・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。 ・また、国民健康保険の評価書で、「電磁的記録媒体を極力使用しない」という表現の意味が分かりにくい。 ・統一して記載すること。	下記内容について、追加、修正を行った。 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。 【紙媒体に対する措置】 ・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。** 【電子データに対する措置】 ・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。 【業務共通システムに対する措置】 ・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。

No.	評価書の項目		該当ページ	指摘事項	内　容	対　応　（　修　正　等　）
8	Ⅲ－３	Ⅲの「３．特定個人情報の使用」の「リスク１」の「その他の措置の内容」欄	高齢・・P21 国保・・P39 年金・・P14 介護・・P88	外部ネットワークとの分離	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。	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。
9	Ⅲ－７	Ⅲの「７．特定個人情報の保管・消去」の「リスク１」の「⑥技術対策」欄	高齢・・P28 国保・・P46 年金・・P19 介護・・P97	同上	同上	【不正アクセス対策】 ・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。
10	Ⅲ－３	Ⅲの「３．特定個人情報の使用」の「リスク２：権限のない者によって不正に使用されるリスク」の「特定個人情報の使用の記録」欄	高齢・・P23 国保・・P39 年金・・P14 介護・・P89	アクセスログの確認	アクセスログを記録しているだけでは不十分。定期的に確認することが必要である。	【〇〇システムにおける措置】 ・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。 【業務共通システムにおける措置】 ・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。
11	Ⅲ－３	Ⅲの3の「リスク3：従業者が事務外で使用するリスク」の「リスクに対する措置の内容」欄	高齢・・P23 国保・・P40 年金・・P15 介護・・P89	同上	同上	・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。
12	Ⅲ－４	Ⅲの「４．特定個人情報ファイルの取扱いの委託」の「特定個人情報ファイルの取扱いの記録」欄	高齢・・P25 国保・・P40 年金・・P16 介護・・P90	同上	同上	同上
13	Ⅲ－５	Ⅲの「５．特定個人情報の提供・移転」の「リスク１」の「その他の措置の内容」欄	高齢・・P26 国保・・P41 年金・・P17 介護・・P91（※提供・移転しない）	同上	同上	同上
14	Ⅲ－４	Ⅲの「４．特定個人情報ファイルの取扱いの委託」の「情報保護管理体制の確認」欄	高齢・・P25 国保・・P40 年金・・P16 介護・・P90	委託先、再委託先への罰則規定	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。	次の下線部分を追加した。 ・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。
15	Ⅲ－４	Ⅲの「４．特定個人情報フィルの取扱いの委託」の「特定個人情報の消去のルール」欄	高齢・・P25 国保・・P41 年金・・P16 介護・・P90	消去のルール	消去のルールについて、統一して記載すること。	・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。