資料４

特定個人情報保護評価指針の解説（案）に係る追加ＱＡ（案）

１．特定個人情報保護評価の実施主体について

Ｑ第３－２　地方公共団体は中間サーバーを用いて情報連携を行う予定ですが、これについてはどのように特定個人情報保護評価を行うのでしょうか。

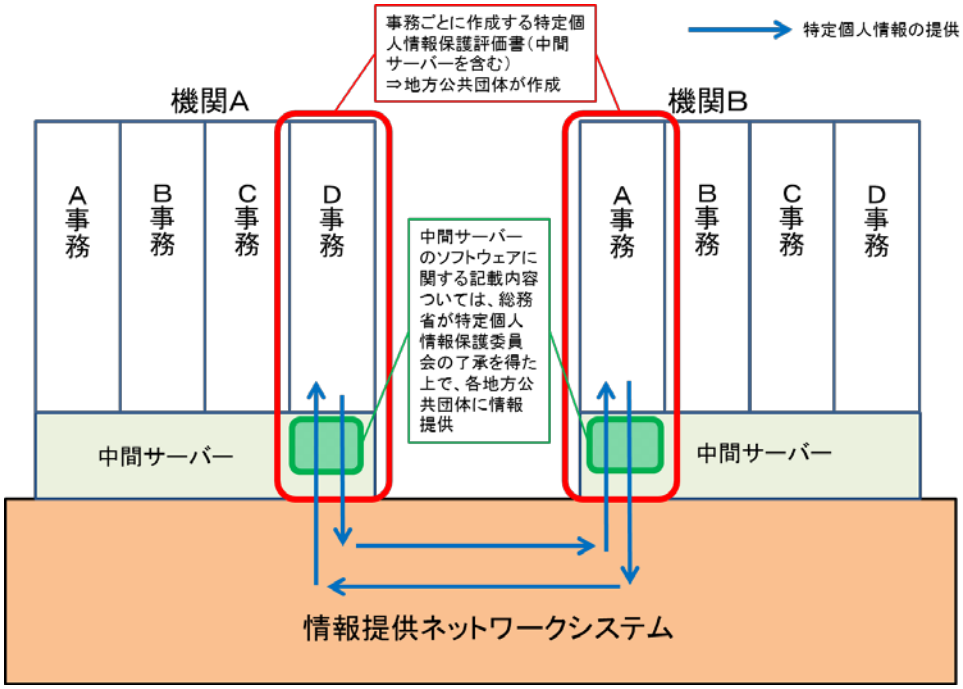
（Ａ）

○　特定個人情報保護評価の対象は、システムやサーバーそのものではなく、それらを用いて特定個人情報ファイルを取り扱う事務です。このため、システムやサーバー単独で評価するのではなく、事務ごとに作成する特定個人情報保護評価書の中において、特定個人情報の提供や移転等の方法として、地方公共団体における中間サーバーについての評価を記載することになります。

○　ただし、地方公共団体における中間サーバーのソフトウェアは、総務省が一括開発しますので、ソフトウェアに関する特定個人情報保護評価書の記載内容については、総務省が特定個人情報保護委員会の了承を得た上で、各地方公共団体に対して特定個人情報保護評価書の作成の際に必要となる情報を提供することとしています。さらに、総務省は、住民等の意見聴取及び第三者点検においても、必要に応じて地方公共団体に協力することとしています。

○　また、ハードウェアについて、「中間サーバー・プラットフォーム（仮称）」を地方公共団体が活用する場合は、当該プラットフォームに関する特定個人情報保護評価書の記載内容については、総務省が特定個人情報保護委員会の了承を得た上で、各地方公共団体に対して特定個人情報保護評価書の作成の際に必要となる情報を提供することとしています。さらに、総務省は、住民等の意見聴取及び第三者点検においても、必要に応じて地方公共団体に協力することとしています。

＜地方公共団体における中間サーバーについての特定個人情報保護評価のイメージ＞



Q第３－２　番号制度関連システム、既存住基システム、住基ネットＣＳ（コミュニケーションサーバー）、住基ネット都道府県サーバーについては、地方公共団体はどのように特定個人情報保護評価を行うのでしょうか。

（Ａ）

○　特定個人情報保護評価の対象は、システムやサーバーそのものではなく、それらを用いて特定個人情報ファイルを取り扱う事務です。このため、システムやサーバー単独で評価するのではなく、

①　市町村は、住基事務の特定個人情報保護評価書の中において、既存住基システム及び住基ネット CS についての評価を記載し、

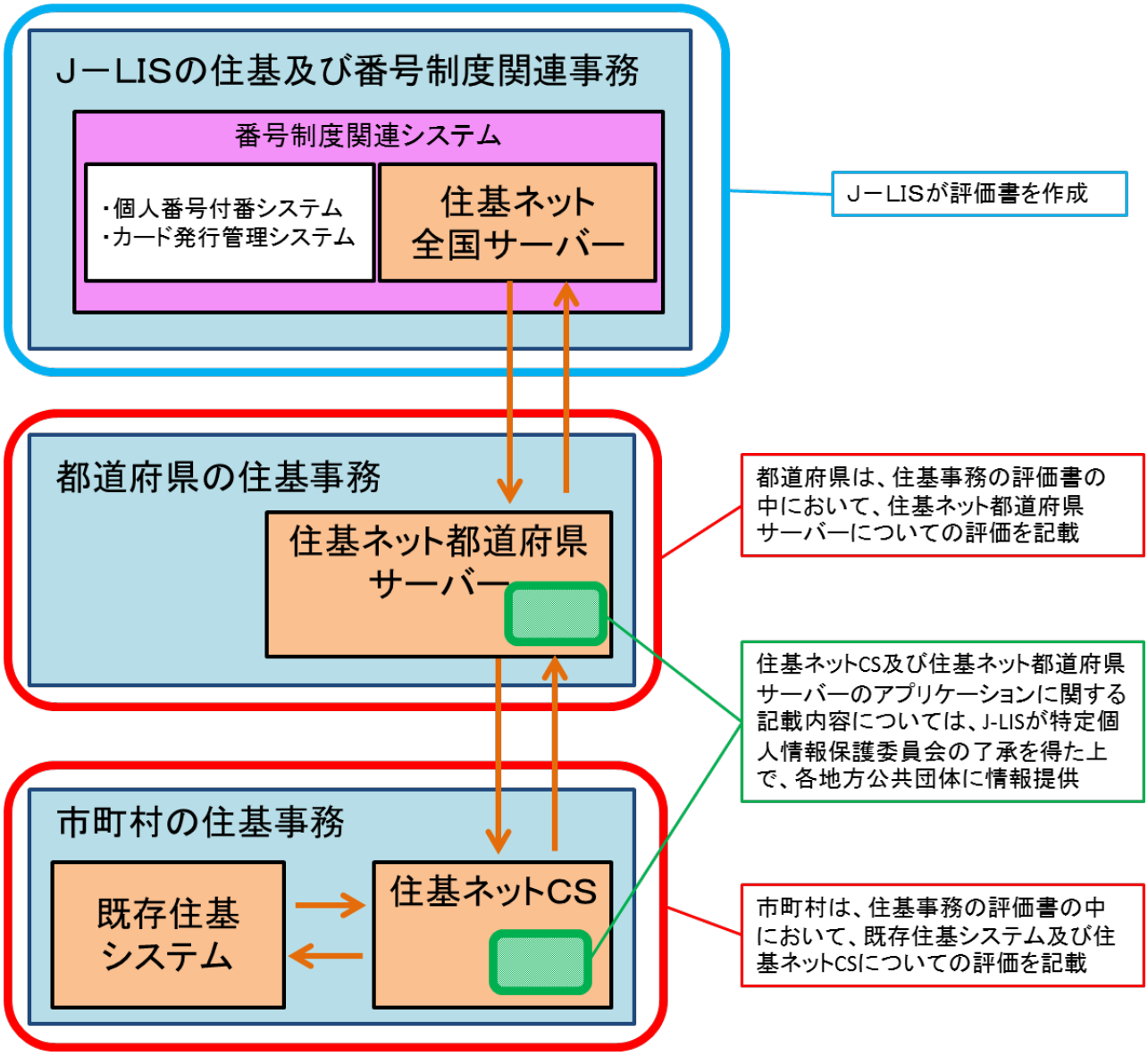
②　都道府県は、住基事務の特定個人情報保護評価書の中において、住基ネット都道府県サーバーについての評価を記載することになります。

○　ただし、住基ネット CS 及び住基ネット都道府県サーバーのアプリケーションは、地方公共団体情報システム機構（J-LIS）（※）が通常一括開発しますので、アプリケーションに関する特定個人情報保護評価書の記載内容については、J-LIS が特定個人情報保護委員会の了承を得た上で、各地方公共団体に対して特定個人情報保護評価書の作成の際に必要となる情報を提供することとしています。さらに、J-LIS は、住民等の意見聴取及び第三者点検においても、必要に応じて地方公共団体に協力することとしています。

（※）平成 26 年 4 月 1 日に、財団法人地方自治情報センター（LASDEC）が、地方公共団体情報システム機構（J-LIS）に移行。

○　なお、番号制度関連システム（住基ネット全国サーバー、個人番号付番システム及びカード発行管理システム）については、J-LIS が特定個人情報保護評価を実施することとなります。

＜市町村、都道府県、J-LIS の事務についての特定個人情報保護評価のイメージ＞



２．特定個人情報ファイルについて

Ｑ第４－３　既存番号で連携しているデータベースやテーブルについては、全て特定個人情報ファイルに該当するのでしょうか。

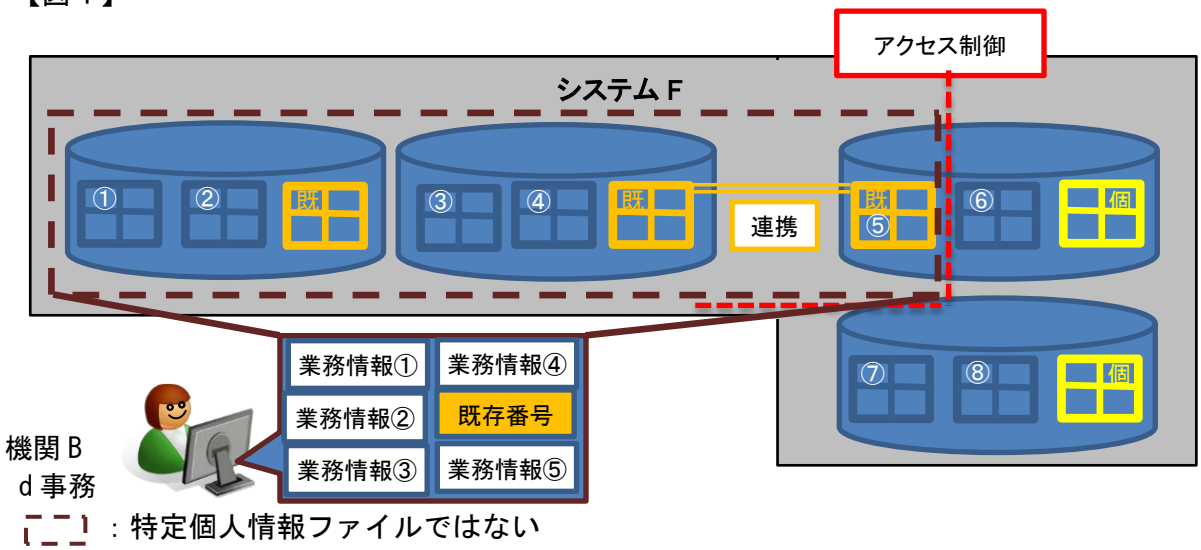
（Ａ）

○　特定個人情報ファイルに該当するか否かは、個人番号と紐づけてアクセスできるかどうかで判断します。したがって、既存番号で連携している場合であって、アクセス制御により、個人番号そのものにはアクセスできず、個人番号以外の情報にのみアクセスできるように制御されている場合は、特定個人情報ファイルには該当しません。これは、データベース間にアクセス制御を設ける場合もテーブル間にアクセス制御を設ける場合も同じです【図１参照】。

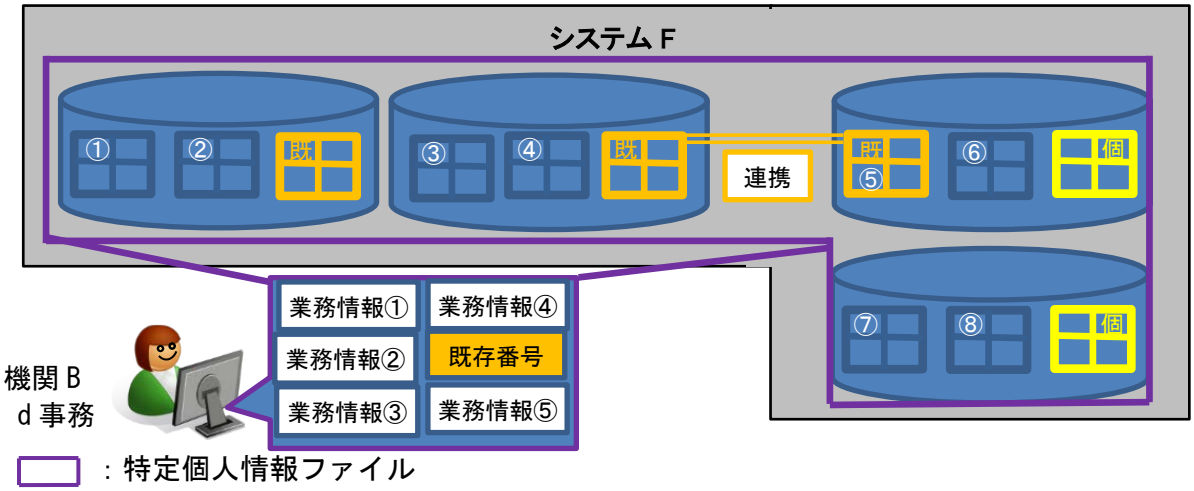
一方、既存番号で連携している場合であっても、アクセス制御がされておらず、個人番号そのものにアクセスできる場合は、特定個人情報ファイルに該当することになります【図２参照】。

○　なお、個人番号そのものにアクセスできる場合とは、事務を行う権限を有する者が個人番号とともに見ることができる場合のみでなく、システムの内部処理で個人番号と連携する場合もこれに該当します。

【図１】



【図２】



※画面には業務情報①～⑤と既存番号しか表示されない場合であっても、システムの内部で業務情報⑥～⑧と個人番号にアクセスできる場合には、紫の実線が特定個人情報ファイルに該当することとなる。

Ｑ第４－３　アクセス制御を行えば特定個人情報ファイルには該当しないとのことですが、アクセス制御とはどのようなものでしょうか。

（Ａ）

○　事務を行う権限を有する者が個人番号を画面や帳票などで見ることができる場合や、システムの内部処理において個人番号を用いる場合は、特定個人情報ファイルに該当することになりますが、アクセス制御がされており、個人番号を画面や帳票で見ることができず、システムの内部処理においても用いていない場合には、特定個人情報ファイルに該当しません。アクセス制御の手法としては、次のような手法が考えられます。

①　画面・帳票における制御

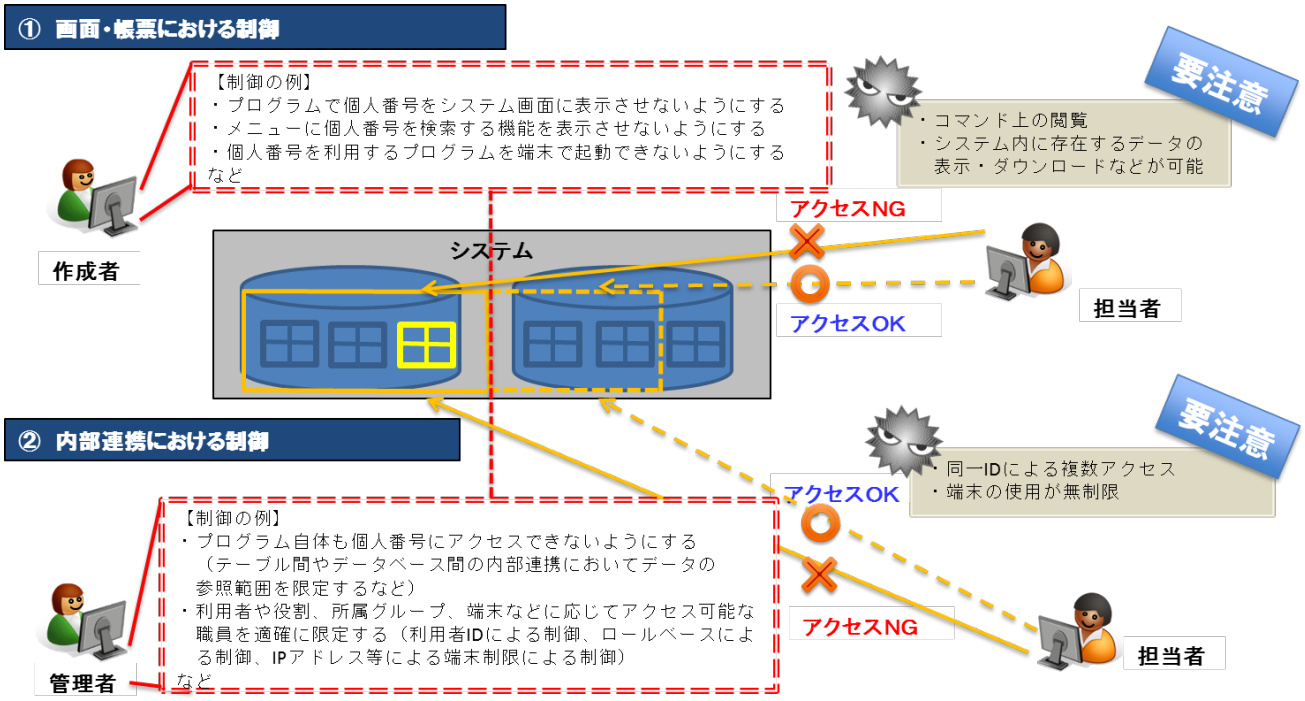
事務を行う権限を有する者が個人番号を画面や帳票などで見ることができないようアクセス制御する手法としては、プログラムにより個人番号をシステム画面に表示させないようにすること、メニューに個人番号を検索する機能を表示させないようにすること、個人番号を利用するプログラムを端末で起動できないようにすることなどが考えられます。

ただし、通常使用するシステム画面に個人番号が表示されなくても、コマンド上では個人番号が閲覧できるようになっている場合なども考えられますので、このような場合には、コマンド実行権限の制限などの措置も必要となります。また、通常使用するシステム画面には個人番号が表示されなくても、システムの機能により、システム内に存在するデータの表示・ダウンロードなどが可能であり、その中に個人番号が含まれる場合が考えられます。このような場合には、システム画面以外についても個人番号を表示・ダウンロードさせないよう制限するなどの措置が必要となります。

② 内部連携における制御

システムの内部処理において個人番号を用いないようアクセス制御するには、データベース・テーブル・ファイルの参照を制限したり、プログラムやコマンドの実行権限を制限することなどが考えられます。具体的には、システムのプログラム自体も個人番号にアクセスできないようにすること、データベース等の設定により利用者や役割、所属グループ、端末などに応じてアクセス可能な職員を適確に限定すること（利用者 ID による制御、ロールベースによる制御、IP アドレス等による端末制限による制御）などが考えられます。

ただし、同一 ID による複数アクセスなど本来 ID を使ってはいけない者が ID を使って個人番号にアクセスする場合や、IP アドレス等による端末制限をしてもその端末が誰でも使用可能な状態になっている場合は、アクセス可能な職員を適確に限定しているとは言えません。



３．しきい値判断における対象人数について

Ｑ第５－２　対象人数は、どのように考えればよいですか。

（Ａ）

○　規則において、対象人数は「特定個人情報ファイルを取り扱う事務において保有する全ての特定個人情報ファイルに記録される本人の数の総数」をいうとされています。一般に、その事務において経常的に取り扱う特定個人情報の本人数をいうと考えられます。

○　なお、本人とは、個人番号によって識別される特定の個人をいい、当該事務における受給者、被保険者等に限定されません。例えば、医療保険の場合であれば、その被保険者だけではなく、被扶養者等についても個人番号を保有するのであれば、被保険者の数だけでなく、被扶養者等の数も対象人数に含まれます。

Ｑ第５－２　特定個人情報保護評価を実施する事務において、最初に保有している個人情報には個人番号が紐づかないものの、個人番号に紐づく個人情報が徐々に増え、対象人数が徐々に増えていくような場合、対象人数をどう考えたらよいですか。

（Ａ）

○　個人番号の利用開始時点において保有する特定個人情報の本人数を対象人数とするのではなく、その事務において取り扱う特定個人情報の本人数を合理的に推測して、対象人数を記載してください。これまでその事務において経常的に取り扱ってきた個人情報の本人数のうち個人番号と紐づくと考えられる数、その事務において今後経常的に取り扱うことが予測される個人情報の本人数のうち個人番号と紐づくと考えられる数、特定個人情報の保存期間の予測等により推測することが考えられます。システム設計上又は予算上想定している人数があれば、それを記載することも考えられます。給付申請やデータの削除時期が集中することなどにより、対象人数が期間によってばらつきがある場合は、これまでその事務において経常的に取り扱ってきた特定個人情報の本人数のピークの水準等により、対象人数を合理的に推測することとなります。

Ｑ第５－２　地方公共団体の宛名システムのような個人番号と既存番号の対照テーブルを参照できる場合は、対象人数をどのようにカウントすべきですか。

（Ａ）

○　対象人数は、事務において経常的に取り扱う特定個人情報の本人数をカウントする必要があり、特定個人情報ファイルの範囲と直接結びつくとは限りません。以下、具体例を用いて説明しますが、ケース①からケース③までのいずれの場合も、A給付事務において、経常的に取り扱う特定個人情報の本人数は１１万人ですので、対象人数は１１万人ということになります。

○　ただし、番号法においては、個人番号を利用することができる事務が限定されており、個人番号を利用できるのは当該事務の処理に当たって必要な限度であるとされています。したがって、A給付事務に携わる職員が当該事務の処理以外の目的で特定個人情報の検索等を行うことは法令上禁止されていることから、検索等が行われないよう、厳格に管理する必要があります。

ケース①　事務システムと、個人番号と既存番号（ここでは宛名番号という。）の対照テーブルを有するシステム（ここでは宛名システムという。）が別々のシステムであるケース

○　下図のケース①は、次のようなケースを表しています。

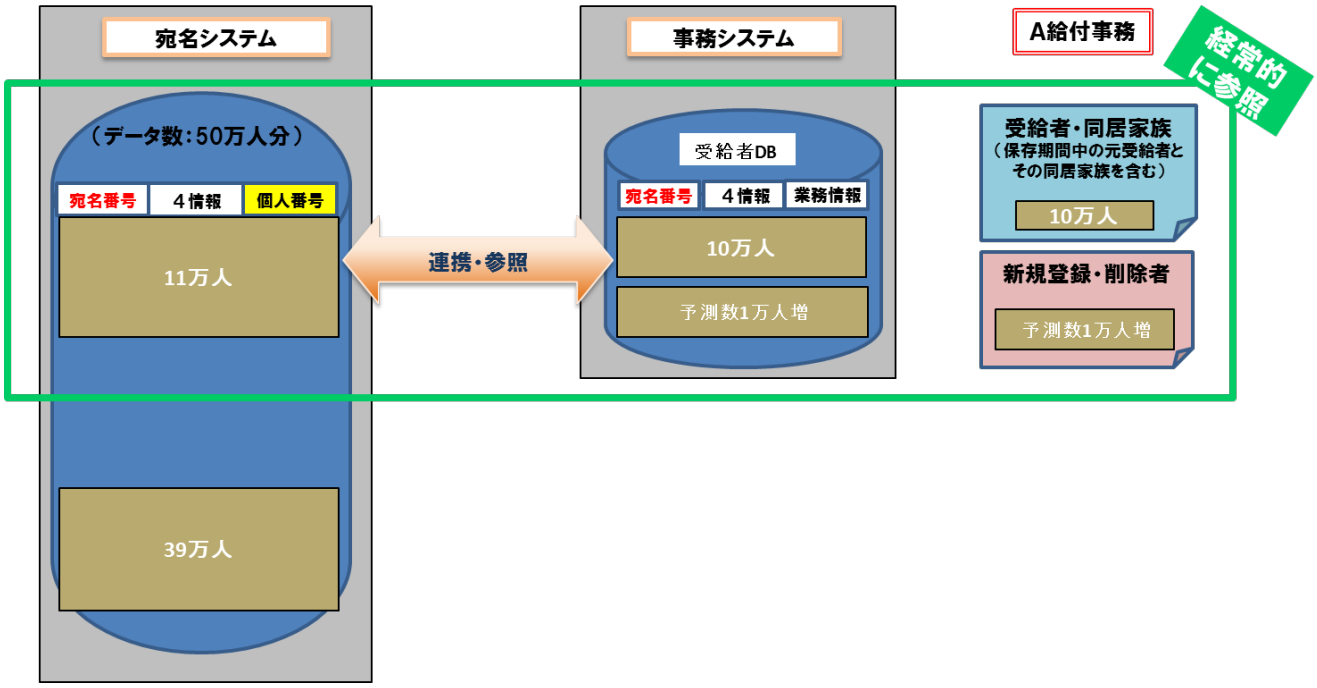
・　A給付事務を処理するために必要な情報として、評価実施機関では、受給者・同居家族（保存期間中の元受給者とその同居家族を含む。以下同じ。）の特定個人情報ファイルを取り扱っています。

・　A給付事務では、その時点における受給者・同居家族のデータとして、既に１０万人分のデータを事務システムの受給者DBに格納しています。

・　A給付事務における今後の増減分を、新規登録によって増加する数と保存期間の満了等により削除される者の数（以下「新規登録・削除者数」という。）を基に合理的に予測すると、約１万人分のデータが増加することが予測され、この増加分についても受給者DBに格納される見込みとなっています。

・　事務システムと宛名システムは別々のシステムですが、A給付事務を処理するに当たっては、事務システム（１１万人分）の情報だけでなく、宛名番号をキーとして宛名システム（５０万人分）の個人番号にアクセスし、個人番号に紐づく情報を参照します。

【ケース①の図】



＜ケース②　事務システムの中に受給者DBと住民情報DBが存在するケース＞

○　下図のケース②は、次のようなケースを表しています。

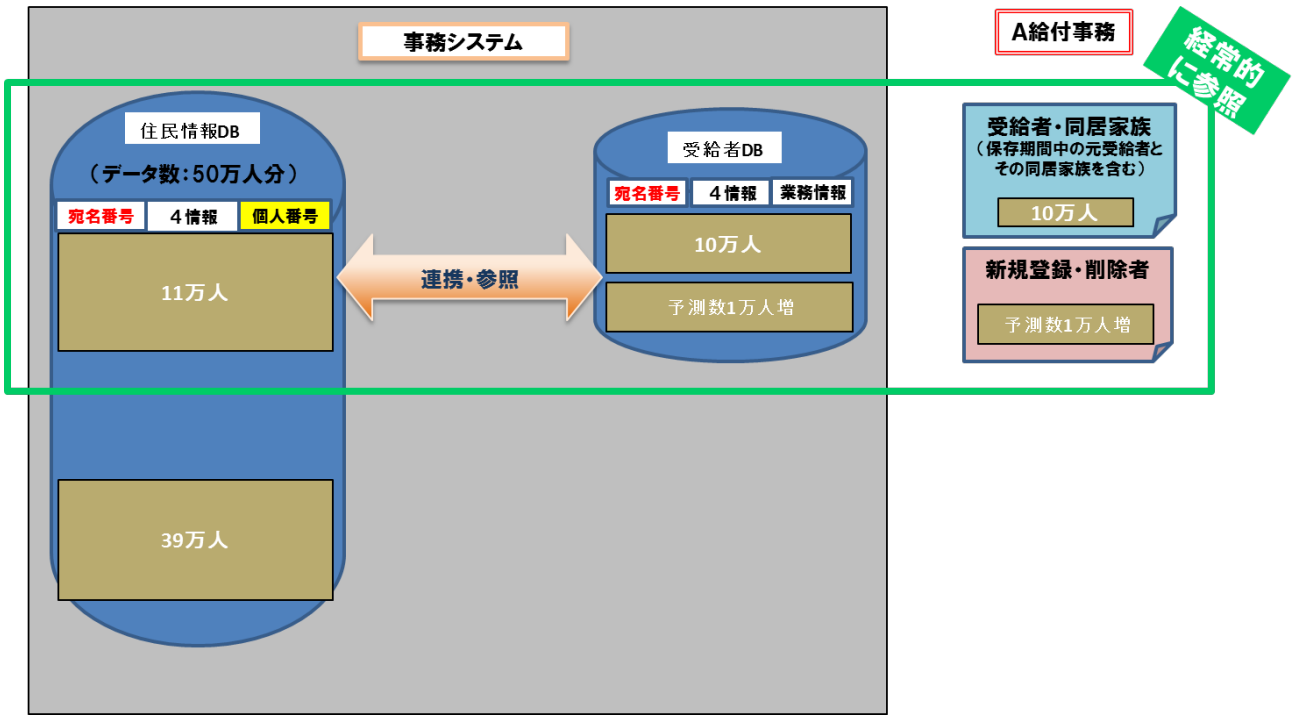
・　A給付事務を処理するために必要な情報として、評価実施機関では、受給者・同居家族の特定個人情報ファイルを取り扱っています（ケース①と同様）。

・　A給付事務においては、その時点における受給者・同居家族のデータとして、既に１０万人分のデータを事務システムの受給者DBに格納しています（ケース①と同様）。

・　A給付事務における今後の増減分を、新規登録・削除者数を基に合理的に予測すると、約１万人分のデータが増加することが予測され、この増加分についても受給者DBに格納される見込みとなっています（ケース①と同様）。

・　事務システムの中に受給者DBと住民情報DBが存在しますが、A給付事務を処理するに当たっては、受給者DB（１１万人分）の情報だけでなく、宛名番号をキーとして住民情報DB（５０万人分）の個人番号にアクセスし、個人番号に紐づく情報を参照します。

【ケース②の図】



＜ケース③　事務システムの中の住民情報 DB において、受給者の情報を一括管理するケース＞

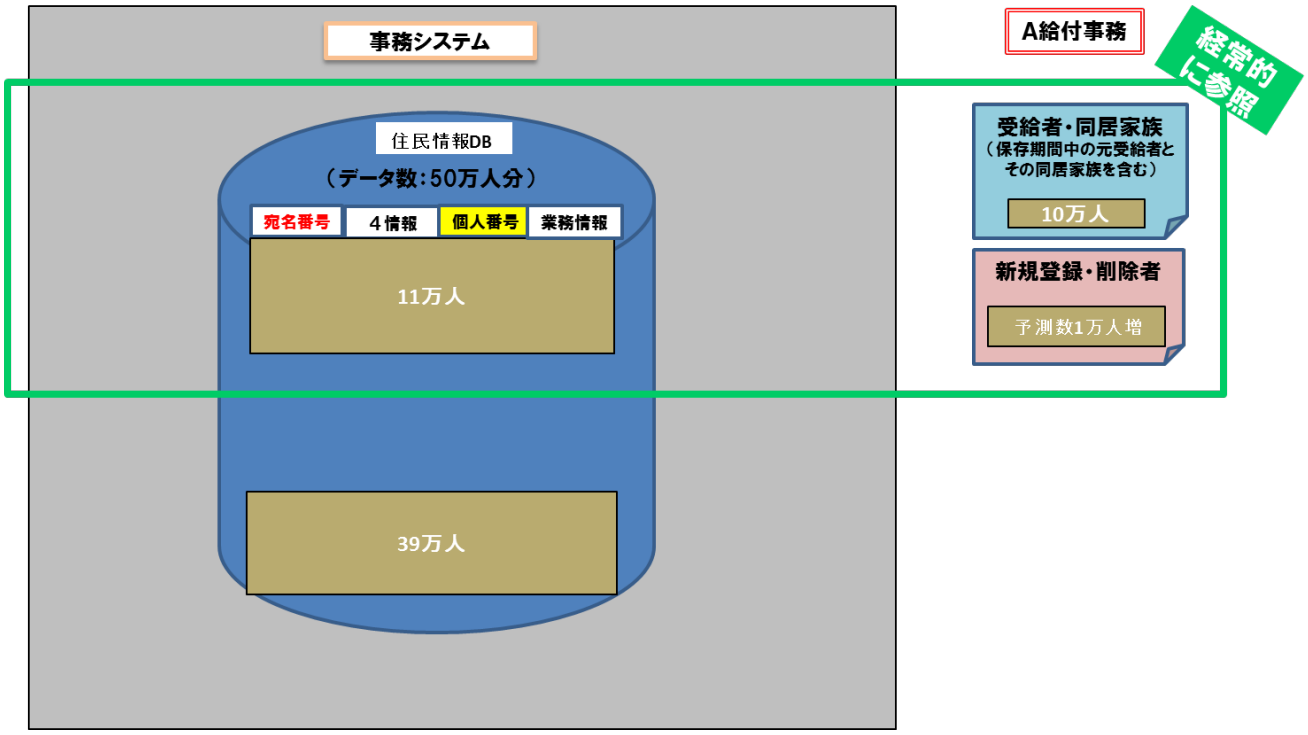
○　下図のケース③は、次のようなケースを表しています。

・　A給付事務を処理するために必要な情報として、評価実施機関では、受給者・同居家族の特定個人情報ファイルを取り扱っています（ケース①と同様）。

・　住民情報DBには、全住民のデータ（５０万人分）が格納されており、A給付事務においては、住民情報DBにおけるその時点の受給者・同居家族のデータ（１０万人分）及び下記増加分のデータ（１万人分）のみ参照しています。また、業務情報も直接住民情報DBに格納しています。

・　A給付事務においては、今後の増減分を、新規登録・削除者数を基に合理的に予測すると、約１万人分のデータが増加することが予測され、この増加分についても直接住民情報DBを参照することになります。

【ケース③の図】



４．実施時期について

Ｑ第６の１　指針第６の１（１）ウで定められた経過措置の場合、特定個人情報ファイルを保有する前に特定個人情報保護評価を実施することが求められますが、運用開始前までに実施すればよいのでしょうか。それともテスト段階までに実施する必要がありますか。

（Ａ）

○　経過措置適用の場合における特定個人情報保護評価の実施時期は、テスト段階で特定個人情報ファイルを保有するか否かによって異なります。

○　特定個人情報ファイルとは、①個人番号そのものをその内容に含む個人情報ファイル、②個人番号そのものを含まないものの、個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む個人情報ファイルをいいます（番号法第２条第９項）。②とは、例えば、情報提供ネットワークシステムを使用した情報提供の求め又は情報提供の際に用いられる符号や個人番号を部分的に修正したもので、個人番号と一対一で対応するものなどを含む個人情報ファイルをいいます。

○　したがって、テストデータに個人番号そのものが含まれている場合は、テストデータであっても、当該データは特定個人情報ファイルに該当しますので、当該データを保有する前に特定個人情報保護評価を終わらせる必要があります。

○　テストデータとしてダミーの番号を用いる場合は、当該ダミーの番号が、個人番号と全く関係ないものであれば、特定個人情報保護評価の対象とはなりません。一方、ダミーの番号が上記②に該当する場合には、当該データは特定個人情報ファイルに該当しますので、このような場合には、当該データを保有する前に特定個人情報保護評価を終わらせる必要があります。