特定個人情報保護評価書（案）に対する意見募集の結果

No.	提出された意見の概要	意見に対する考え方
1	事務の内容において「情報提供ネットワークシステムにて一元管理しないものとする。」とあるが、実際にはJ-RISによりクラウド型の中間サーバが用意され、個人情報が一元管理されることになっている。 例え自治体ごとにDBが分けられるにしても、J-RISまたはそこからの受託者がシステムを管理するのであれば、一元管理そのものではないか。ベネッセの事例を考えれば、そこから大規模な情報漏えいが起きる可能性は十分に想像できるのではないか。	地方公共団体情報システム機構（J-LIS）が地方公共団体向けに提供する予定の中間サーバー・プラットフォームは、クラウド型のサービスで整備することとしていますが、論理的には各機関ごとに専用サーバが割り当てられ、データは各機関別に区分管理されております。 また、機構や受託者が特定個人情報に係る業務にはアクセスできないよう管理するなど、セキュリティについては十分な対策をとることとしております。
2	連携用符号についてですが、セキュリティの向上のため、連携用符号をいったん生成したらずっとそのまま使い続けるというのではなく、定期的に生成しなおして変更するべきだと思います。	情報提供ネットワークシステムにおいては、住民票コードから連携用符号を生成し、連携用符号から情報提供用個人識別符号を生成します。 連携用符号は本システムから外に出ることはないため、住民票コードから情報提供用個人識別符号が推測される、もしくは情報提供用個人識別符号から他の情報提供用個人識別符号が推測されるリスクは基本的にはありません。暗号化方式の危殆化等に対しては、計画的に符号を生成し直すこととしております。
3	番号法は賛成ですが、現在の検討内容は、日本国政府と官庁の都合によるところが大きいと思います。国と国民がWin-Winであるべきと思います。憲法前文では、国民のための政治が歌われています。役所の事務の都合による政治ではいけないと思います。小学校の時、先生から習いました！そもそも国政は、国民の厳粛な信託によるものであって、その権威は国民に由来し、その権力は国民の代表者がこれを行使し、その福利は国民がこれを享受する。これは人類普遍の原理であり、この憲法は、かかる原理に基づくものである。フィンランドでは、電子カルテ「KanTa」があり、連携しています。日本国も、学ぶべきかと思います。税金を絞ることに知恵を絞るのでは、人として、少し、悲しくありませんか。家族や祖父祖母の末永い健康、暖かい気持ちの国にしたくありませんか。 まとめますが、「医療（カルテ、処方箋）」と連携してください。 そうすれば、日本の人が、喜ぶと思います。よろしくお願いします。 Intelligenceが高くても、Wisdomが低いと、人を幸せにできないです。アイデアとイノベーションを大切にしてください。	今後の個人番号の利用拡大検討の際の参考とさせていただきます。
4	「7. 特定個人情報の保管・消去」 リスク1： 特定個人情報の漏えい・滅失・毀損リスク （6）技術的対策 具体的な対策の内容 上記に関して、参考になると思われる、知識として、「IPA（独立行政法人情報処理推進機構）」のサイト内検索を用いて、「有線LAN暗号化」で検索したところ、「検索結果」に「盗聴」という語句がありました。URL 「https://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/snif.html」 「soho」向けの知識とはいうものの、かなり「有益」かつ「情報セキュリティに関する教育・啓蒙活動」に資すると考えられるので、この度、「意見」として、送信することにいたしました。どうぞよろしくお願い申し上げます。 1.7 盗聴 盗聴は映画や現実の世界でワイヤレスマイクを主体として行われるものや、電話の盗聴などを連想します。ネットワーク上での盗聴は、こうした音声盗聴とは違い、基本的に「データを盗み見る行為」または「データを抜き取る行為」を言います。 ・ネットワーク内部の社員等が、ネットワークのパケットを抜き取って他人の通信内容を盗み見る ・内部の社員等のIDとパスワードを盗み、なりすましてメール等の通信内容を閲覧したり、改竄したりする ・外部のクラッカがインターネットから社内LANのサーバや端末に侵入し、侵入した器材の権限を使ってデータを盗み見る	情報ありがとうございます。本システムは、セキュリティについて十分考慮した構成としており、盗聴できる環境とはなっておりません。 具体的な対策として、無線LAN経由でのアクセスは禁止します。また、利用の際に適切なユーザ認証を行うとともに、通信の暗号化を行います。

特定個人情報保護評価書（案）に対する意見募集の結果

5	1.7.1 パケットスニッフィング スニッフィングはネットワークを流れるパケットを収集し、その中身を解析、閲覧する盗聴手法です。そこに流れているデータを抜き取るので、本来アクセス権限のないデータも見ることができます。 盗聴を行うためのソフトウェアの入手は簡単です。OSに添付されている場合もあります。そもそも、ネットワーク管理を目的としたものですが、悪用することによってネットワーク上のデータを盗聴することができます。 たとえば、Windows 2000のネットワークモニタや、UNIXシステムで広く使用されているtcpdump等が代表的な例です。これらを使用すると、管理のためにパケットを見ていても、どこからどこに対してtelnetし、ログインなどのやりとりまでも見えてしまいます。もちろん、これが見えなければ障害などの原因究明ができないため、実行には管理者の権限が必要になっているので盗聴することによって得られる情報は、ネットワーク上を流れる全てのデータとなります。その中で攻撃する側にとってメリットがあるものは限られているでしょう。 ・ユーザ名とパスワード ・メールの内容 ・クレジットカードの情報 ・住所や電話番号等の個人情報 telnetでシステムにログインする際、ユーザ名やパスワードを入力します。このときのデータは、ネットワーク上を平文で流れます。もちろん、suコマンドを使用したときのパスワードも全て平文です。つまりtelnetを使用した場合、全ての操作は見られていると考えて良いでしょう。 また、メールシステムとしてSMTP/POPを使用している場合、POPのユーザ名やパスワードはもちろん、取り込んだメールやSMTPで送信しているメールも全て盗聴可能です。たとえば、関係者以外には漏らせないような機密事項をSMTPで送信するということは、SMTPを使用している時点で機密ではなくなるのです。	情報ありがとうございます。本システムは、セキュリティについて十分考慮した構成としており、盗聴できる環境とはなっておりません。 具体的な対策として、無線LAN経由でのアクセスは禁止します。また、利用の際に適切なユーザ認証を行うとともに、通信の暗号化を行います。
6	1.7.2 スニッフィングの手法 盗聴のためのパケット収集を同一LAN内から行うには、ホストに何らかのモジュールを仕込む必要はありません。特に、リピータハブを使用しているネットワークであれば、盗聴を行うためのパソコンが1台あれば十分です。そのパソコンを近くにあるハブの空いているポートに刺すだけで同一セグメント内での他の端末のやり取りが盗聴可能になります。 スイッチングハブがセットされているネットワークの場合、リピータハブの要領でのスニッフィングは不可能ですが、上位機種のスイッチングハブには管理者がネットワーク状態監視をするためのミラーリングポートがついているので、そこへ盗聴器材を接続すれば同一セグメント内のスニッフィングが実行できます。また、ミラーポートのついていないスイッチングハブではセグメント内全体の盗聴は無理ですが、スイッチングハブがMACアドレスで配信の識別をしている点を利用して、セグメント内ホストのMACアドレスを偽造して信号を出していれば、ホストに配信されるはずのパケットを受信することができます。	情報ありがとうございます。本システムは、セキュリティについて十分考慮した構成としており、盗聴できる環境とはなっておりません。 具体的な対策として、無線LAN経由でのアクセスは禁止します。また、利用の際に適切なユーザ認証を行うとともに、通信の暗号化を行います。
7	1.7.3 無線LANのスニッフィング 有線LANの場合、前項で述べたとおりパケットスニッフィングを行うためには、器材を物理的にネットワークに接続する必要があります。すなわち、内部の人間がこっそりと設置するか、外部の人間であれば、そのLAN環境に忍び込まなければならなりません。 しかし無線LANは本来使用すべき環境の外部でも電波検出が可能な場合がほとんどで、まったくセキュリティが施されていない場合を仮定すれば、LAN環境の外部で電波を傍受し、そこに流れているパケットを収集して中身を見れば盗聴は完了します。 また、出荷時のデフォルト状態で無線LANルータを使用している人が多く、部外者でも電波の範囲内に無線LANカードを装備したノートPCを持ち込みさえすれば、ネットワークの使用者と同じ条件でLANへの接続が可能になり、ネットワーク内の他の器材へ不正アクセスされる危険性があります。	情報ありがとうございます。本システムは、セキュリティについて十分考慮した構成としており、盗聴できる環境とはなっておりません。 具体的な対策として、無線LAN経由でのアクセスは禁止します。また、利用の際に適切なユーザ認証を行うとともに、通信の暗号化を行います。

特定個人情報保護評価書（案）に対する意見募集の結果

8	「7. 特定個人情報の保管・消去」 リスク1： 特定個人情報の漏えい・滅失・毀損リスク （6）技術的対策 具体的な対策の内容 上記に関して、参考になると思われる、知識として、「IPA（独立行政法人情報処理推進機構）」のサイト内検索を用いて、「有線LAN暗号化」で検索したところ、「検索結果」に「盗聴」という語句がありました。URL「https://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/snif.html」 「soho」向けの知識とはいうものの、かなり「有益」かつ「情報セキュリティに関する教育・啓蒙活動」に資すると考えられるので、この度、「意見」として、送信することにいたしました。どうぞよろしくお願い申し上げます。 1.7.4 盗聴を防ぐには スニッフィングを防御するには、インフラ面でなるべくスイッチングハブを導入し、それぞれのハブの管理を行うことが必要です。また、パケットについては、可能な限り暗号化をして送受信するべきでしょう。無線LANについては、MACアドレスによるアクセスポイントの接続制限や、WEPや802.1Xで通信を暗号化する必要があります（詳しくは5.通信機器の設定方法を参照ください）。 昨今、街中やホテルロビー等で提供されているホットスポット・サービスの中には、セキュリティ設定が皆無に等しく盗聴や侵入を許すサービスもあるので、ホットスポットのサービスデベロッパは慎重に選択するべきでしょう。	情報ありがとうございます。本システムは、セキュリティについて十分考慮した構成としており、盗聴できる環境とはなっておりません。 具体的な対策として、無線LAN経由でのアクセスは禁止します。また、利用の際に適切なユーザ認証を行うとともに、通信の暗号化を行います。
9	・25、34ページ 「職員・運用者ごとにIDを発行し、共有IDは使用しない」とあるが、ある人のIDでログインし、そのまま他の人もシステムを使うこと（犯罪事件に関係し報道されていた市役所の実状の例）を物理的に防ぐ対策が示されていない。もし、職員・運用者への研修やモラル徹底以外に方法がないのであれば、リスク管理の弱点として認識すべきである。 ・12、19、27、36ページ 「原則として再委託は行わないこととする」と言いながら、再委託が必要となる状況について何か例外的な場合という限定はなく、再委託契約に必要な事項を盛り込み、安全管理措置を講じていれば広く再委託できる内容になっているのは、リスク管理として十分でない。 国民等は、委託先については公表等により確認可能だが、再委託先は確認できないことや、また、民間会社で発生した再委託先からの大規模な情報漏洩事件の例に見るリスクを考えて、再委託しない事業者を委託先とするなどを検討するべきである。	・重要な機能を利用する際は、入力・更新等の権限を分離した複数人によるシステム操作を必須とする機能（デュアルロック機能）を採用します。また、内部職員を統制する運用規程等を定め、これにより職員・運用者の適正なIDの利用を徹底いたします。 ・原則再委託は行わないこととしていますが、一部業務について再委託が必要となる場合には、番号法第１０条及び第１１条の趣旨を踏まえ、かつ、内部職員を統制する運用規程等に基づき、再委託者に対しても監督や教育を徹底するなどの人的安全管理措置を講じます。

特定個人情報保護評価書（案）に対する意見募集の結果

10	I 基本情報 1．特定個人情報ファイルを取り扱う事務の2）事務事務の内容について。 事務の目的の記載は修正すべきである。 番号制度の目的として「評価書」は冒頭、「社会保障・税番号制度は、効率的な情報の管理・利用、迅速かつ安全な情報の連携を実現することを目的として導入されるもの」としている。この認識は、番号制度の目的が行政にとっての国民管理の効率化であるという本音を吐露したものである。 この番号制度はそもそも何のための制度かが問題視され、番号法制定の国会審議においても論議となり法の目的規定が修正されてきた経緯があるが、この「評価書」の記述はその修正もふまえずに一面的な目的を表明している。 「社会保障・税番号大綱」では、社会保障制度や税制を一体的に捉え、社会保障給付の効率性・透明性・公平性を高めるために導入するとしていたが、番号法の第一条目的には「税・社会保障制度」という文言もなく、何にでも使える制度に変質しつつある。番号法の施行令では、警察などが治安管理のために特定個人情報を利用することまで認めている。 特定個人情報保護評価は、番号制度制度が内包する基本的人権侵害の可能性をふまえて、 （1）事前対応による個人のプライバシー等の権利利益の侵害の未然防止 （2）国民・住民の信頼の確保 を目的に実施されるものであり、そのためには利用目的の限定と明確化が必要である。何に使われるかわからない制度を信頼することはできず、プライバシー侵害の防止を期待することはできない。 事務の（メリットとしてでなく）目的として、少なくとも「社会保障・税番号大綱」が番号制度により実現する社会として説明してきた ・より公平・公正な社会 ・社会保障がきめ細やかかつ的確に行われる社会 ・行政に過誤や無駄のない社会 ・国民にとって利便性の高い社会 ・国民の権利を守り、国民が自己情報をコントロールできる社会 の理念を明記すべきである。	ご意見を踏まえ事務の目的の記載を修正いたします。 「社会保障・税番号制度は、複数の機関に存在する個人の情報を同一人の情報であることの確認を行うための基盤であり、社会保障・税制度の効率性・透明性を高め、国民にとって利便性の高い公平・公正な社会を実現することを目的とした制度である。個人番号の利用は、社会保障がきめ細やかかつ的確に行われる社会、行政に過誤や無駄のない社会、国民にとって利便性の高い社会、国民の権利を守り、国民が自己情報をコントロールできる社会の実現を旨として行うものである。」
11	I 基本情報 1．特定個人情報ファイルを取り扱う事務の2）事務事務の内容について。 番号制度における情報連携の仕組みをわかりやすく国民に示すべきである。 この情報連携の仕組みは、特定個人情報の一元管理・把握の防止を図ることで住基ネット最高裁判決で住基ネットが合憲とされた要件を確保するいう意味をもち、仕組み次第では違憲となるものである。 今回の「評価書」は、番号制度における情報連携のうち、情報提供ネットワークシステムのコアシステムの部分だけを対象としている。インターフェースシステムによる外部機関との連携や、さらに別機関で行う個人番号（マイナンバー）の付番システムなどを含めた番号制度の全体像は、特定個人情報保護評価という仕組みの限界として明らかでない。 これでは「特定個人情報の一元管理・把握の防止」や「番号法上認められた情報連携以外はシステム上連携しないなど、不正な情報連携の防止」が図られているのか判断できず、「特定個人情報ファイルを取り扱う者が、入手する特定個人情報の種類、使用目的・方法、安全管理措置等について国民・住民に分かりやすい説明を行い、その透明性を高める」という保護評価の目的は達成されず、個人のプライバシー等の権利利益が侵害されることへの懸念を払拭することはできない。 番号制度全体の情報連携の仕組みを、詳細かつわかりやすく国民・住民に示したうえで、特定個人情報保護評価を実施すべきである。	特定個人情報保護評価は、番号法第27条に基づき、評価実施機関が特定個人情報を取り扱う事務を対象に、指針に基づいて評価をするものであり、本評価書は情報提供ネットワークシステム（コアシステムおよびインターフェイスシステム）の運営にかかる事務を対象に評価を行ったものです。番号制度全体に関する情報については、内閣官房のWebページ等から、引き続き国民に分かりやすく提示していきます。

特定個人情報保護評価書（案）に対する意見募集の結果

12	I 基本情報　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の、(1)符号の生成について、以下を明確にされたい。 [1]「・情報照会者等から、住民基本台帳ネットワークシステムを介して、情報提供用個人識別符号生成の対象者の住民票コードを受領する。」とあるが、これは情報照会者等に住基ネットから住民票コードが提供され、それを情報照会者がコアシステムに送るという意味か。だとしたら情報照会者に住民票コードを提供できる法的根拠は何か。 [2]「・住民票コードを基に、暗号演算により、対象者ごとに異なり、情報提供用個人識別符号等の生成の基となる全ての情報照会者等に共通の連携用符号を生成し、連携用符号発行管理ファイルに保存する。住民票コードは連携用符号生成後に直ちに削除する。」について。 　この連携用符号発行管理ファイルにより、連携用符号の重複作成を防止する（5頁）とされ、このファイルの記録項目は「個人番号対応符号」と「連携用符号発行管理情報」とされている（9頁、15頁）。 　住民票コードは任意に変更できるため、変更された場合、暗号演算の結果としての連携用符号は異なる値になると思われるが、それを同一人の連携用符号であると識別するのはどのような方法によるのか。記録項目以外の個人識別情報はないのか。 [3]「・連携用符号に暗号演算による変換を行うことにより、情報照会者等ごとに異なる情報提供用個人識別符号を生成し、依頼元の情報照会者等へ送信する。情報提供用個人識別符号は情報提供ネットワークシステムに保存しない。」について。 　これは情報提供用個人識別符号を可逆暗号により連携用符号から生成し、情報連携の際には、その都度、情報提供用個人識別符号から連携用符号に変換し、さらに照会先機関の情報提供用個人識別符号に変換するという処理を行うということか。 　そうだとすると、情報連携の都度膨大な演算処理が発生するが、演算が100%正確に行われていることをどうやって確認するのか。またシステムはこの演算処理の負荷に耐えられるのか。万一、演算に誤りが起きれば、別人の情報が連携されることにならないか。	[1] 符号発行時、情報照会者等は住民基本台帳ネットワークシステムに対して個人番号（マイナンバー）を送付し、住民基本台帳ネットワークシステムで個人番号から住民票コードを取得し、情報提供ネットワークシステムへ送付します。そのため、情報照会者へ住民票コードは提供されません。 [2] 住民票コード変更時には、新旧の住民票コードから生成される連携用符号の対応を管理します。これにより、同一人の連携用符号であることを識別します。また、記録項目以外の個人識別情報はございません。 [3] 連携用符号から情報提供用個人識別符号を生成した際は、都度検算を行い、正確性を確保しています。また、想定される情報連携の処理件数等を基に、負荷に対応できるシステム構成といたします。
13	I 基本情報　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の、(2)情報連携の媒介について、以下を明確にされたい。 [1]「・情報提供者は、情報照会者に対し、特定個人情報の提供を行う。情報提供は、コアシステムを介さず、インターフェイスシステムを介して行われる。」について。 　このアクセストークン方式では、コアシステムに特定個人情報が蓄積されることを防止するメリットはある一方で、個人情報そのものは情報照会者と情報提供者の間で直接送られることになるが、実際に提供された個人情報が番号法にて認められる範囲を逸脱していないことをどうやって確認するのか。 [2]「・情報照会が、番号法にて認められる範囲（番号法第21条第2項）かどうか確認を行い、情報提供用個人識別符号により情報提供者へ送信する。」について。 　この情報提供の媒介は、一連のシステム処理にて自動的に行われるとなっている。 　この番号法第21条第2項に該当するか否かを、どのような仕組みで自動的に行うのか。 [3]この情報提供は自動的に行われるとなっている。しかし番号法第21条第2項に該当する事務であったとしても、個別には提供を避けなければならない場合があると思われる（ドメスティック・バイオレンスやストーカーの被害者の住所情報が提供先から加害者に伝わる可能性が想定される場合や、差別的な利用をされるおそれが予想される場合など）。 　そのような場合に、提供の可否を情報提供者側が判断し選択する仕組みは、どのように保障されるか。	[1] 情報連携において、情報提供者が提供する特定個人情報については、番号法別表第2に基づき主務省令で定められています。情報照会者からの番号法で認められる範囲であることを確認された情報照会に対し、情報提供者は、主務省令に定められる特定個人情報を提供することとなっており、各機関の既存システムについても適切なアクセスコントロールを確保し、適正な事務遂行の範囲内でのみ運用されるものと考えます。 [2] コアシステムに、番号法別表第2の内容を電子化した情報（マスターデータ）を保持します。情報照会者から情報照会要求が行われる都度、マスターデータと照合を行い、当該情報照会が番号法で認められる範囲であるかを確認します。 [3]情報提供を行う仕組みとしましては、即時提供を行う機能に加えて事後提供とする機能を設けており、提供の可否については情報提供者が行うことになります。

特定個人情報保護評価書（案）に対する意見募集の結果

14	Ⅰ 基本情報　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の、(3)情報提供等の記録の管理について、 Ⅱ 特定個人情報ファイルの概要　2. 情報提供等記録ファイルについて 情報提供等の記録は、個人の手続きを通してどのような社会生活を営んでいるかが把握できるプライバシー情報であるが、その提供の仕組みを明確すべきである。 [1]「・情報提供等記録開示システムを介して本人から開示請求を受信した際に、該当する情報提供等の記録を抽出し、インターフェイスシステムを介して情報提供等記録開示システムへ送信する。」について。 情報提供等記録は、「連携用符号」から生成された「情報提供等記録用符号」によって個人識別できるようになっていると思われるが、その符号を本人は知らない。情報提供等記録ファイルでは個人番号対応符号しか記録項目がないが、情報提供等記録開示システムから本人が開示請求をする際に、どのような仕組みで本人識別するのか（住所氏名等によるのか、個人番号によるのか、公的個人認証によるのか、その他か）。またその識別された本人と「情報提供等記録用符号」をどのように紐付けするのか。 [2]「・番号法第52条第1項の規定により、特定個人情報保護委員会から報告を求められた場合には、番号法第19条第11号の規定により、特定個人情報を提供することと規定されており、この規定に基づき、特定個人情報保護委員会から情報提供等の記録の提供の求めがあった場合には、情報提供等の記録を提供する。」について。 この場合、特定個人情報保護委員会が提供を求めた個人の情報提供等記録を、どのような仕組みでその個人のものであると識別し抽出するのか。 またこの仕組みにより、本人申請以外でもその人の情報提供等記録を抽出することが可能になるが、そうすると番号法第19条第12号の規定とその政令別表により刑事事件捜査や破防法その他の治安立法に基づき個人の情報提供等記録を抽出・提供も可能になるのではないか。 さらに本人からの開示請求の場合は、その記録が情報提供ネットワークシステムに残るが、特定個人情報保護委員会からの依頼は書面等によることになっており(38頁)、刑事事件捜査等への提供を本人が確認できなくならないか。	[1] 情報提供ネットワークシステムでは、情報提供等記録開示システムで公的個人認証による本人確認後、機構から提供される住民票コードから連携用符号及び情報提供等記録用符号を生成し、利用者と紐付けることとしています。 [2]番号法第52条第1項の規定に基づく 特定個人情報保護委員会への報告については、犯罪捜査を目的としたものではありません。
15	Ⅱ 特定個人情報ファイルの概要の1. 連携用符号発行管理ファイルについて。 このファイルの法的根拠として、番号法第2条第14項、第19条第7号、第21条第2項があげられている（9頁、10頁）。 しかしこれらの条文は、情報提供ネットワークシステムにより情報連携を行うことが規定されているだけで、それを「符号」により行うことはどこにも規定されておらず、連携用符号発行管理ファイルを保有する法的根拠にならない。 番号法の中に、情報連携は（マイナンバーや住民票コードなどではなく）符号により行うことを明記すべきである。 Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策について [1]委託について 連携用符号発行管理ファイル、情報提供等記録ファイルとも、バックアップ取得や運用管理で委託（さらには再委託）を行い、またその際特定個人情報は消去されない（12頁、19頁、27頁、36頁）。 しかしこれらファイルは他の事務や一般の個人情報と異なり、他のあらゆる個人情報の紐付けを可能にする情報であり、一元管理とならないためにとして複雑なシステムが検討されているものである。 それを委託し万一悪用・漏えいした場合は、このような仕組みの効果そのものを損なう危険があり、委託はせずに行政がみずから責任を持って管理すべきである。 [2]特定個人情報の提供・移転について 連携用符号発行管理ファイルについては（委託や情報提供ネットワークシステムを通じた提供を除く）提供・移転はしないとされ、リスク評価は行われていない（29頁）。 しかし番号法第19条第12号とその政令別表により刑事事件捜査や破防法その他の治安立法に基づき特定個人情報の利用が認められており、連携用符号や情報提供用個人識別符号の提供が求められることが起こらないのか。このような提供を求められた場合、どう対応するのか、明らかにすべきである。	Ⅱ　番号法施行令第21条に、情報照会者による特定個人情報の提供の求めの際には、情報提供用個人識別符号を用いることが定められております。 Ⅲ [1] 本システムの運用を行うに当たり、基幹的な業務や重要な業務は行政が自ら実施するものの、高度かつ専門技術が要求される等の理由から、定型的な業務等については、委託による外部リソースの活用が必要となる場合があります。委託を行う際には、番号法第11条の趣旨を踏まえ、取り扱う特定個人情報の安全管理が確保されるよう、当該委託を受けた者に対する必要かつ適切な監督や教育を徹底いたします。 [2] 連携用符号発行管理ファイルについては、本システムでデータを保存しますが、情報提供用個人識別符号については保存しません。犯罪捜査等にあたり、裁判所の命令やしかるべき法令に基づいて、連携用符号発行管理ファイルを提出するケースがあるか否かは、本評価書が対象とする事務の範疇に含まれないことから本評価書に記載できるものではございません。

特定個人情報保護評価書（案）に対する意見募集の結果

16	[1] 情報提供等記録ファイル（P.23） 【意見】 保持項目には以下を追加していただきたい。 ・情報照会処理者端末ID（もしくはMACアドレス） ・情報提供処理者端末ID（もしくはMACアドレス） ・提供媒体名 [2] 3. 特定個人情報の使用（P.25） リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク ユーザ認証の管理「具体的な管理方法」 について″ 【意見】パスワード変更の定期的なアラートとあるが、さらに加えて、パスワードの有効期間を設定して、期間満了時は変更を必須（使用不可）とすることで、定期的な変更を強制していただきたい。また、変更するパスワードは過去一定期間に使っていないものとさせる、同一数字、連続数字を使わない、英数字や大文字、小文字、特殊文字の混合などの強度にするなど、セキュリティポリシーについても言及していただきたい。 [3] 3. 特定個人情報の使用（P.25） リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発行・失効の管理「具体的な管理方法」 について″ 【意見】「定期的に対応表を見直し、アクセス権限の発行・失効管理が正しく実施されていることの確認を行う。」 とあるが、システム上定期的に失効させ、次の期間のアクセス権限は改めて申請するようにして、不適切な権限継続の看過を防止していただきたい。 [4] 3. 特定個人情報の使用（P.25） リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク「その他の措置の内容」 について 【意見】「システムにログインするパスワードは、システム上暗号化されて保管される。」とあるが、端末とサーバーとの間の通信時、パスワードは暗号化して通信し、（突合等で必要な場合は受信後に複号するなどして、）暗号化された状態で保管する方式とすることを明記していただきたい。	[1] 情報照会者等における情報照会・提供の処理方式は、職員が端末から入力する、業務システムにて自動的に行う等、情報照会者等毎に様々な方式が想定されます。そのため、情報提供等の記録に端末情報や提供媒体名を保持することは想定しておりません。 [2] 特定個人情報へのアクセスの際には、ID・パスワード認証に加え、生体認証を行う仕様としています。また、パスワードに関し、有効期限の設定や文字種の混在等の考え方について、ご意見を踏まえ追記いたします。 [3] 運用性を考慮し、アクセス権限をシステム上定期的に失効させることなどは想定しておりませんが、運用規程等に基づき、アクセス権限の発行・失効管理を徹底し、不適切な権限継続を防止いたします。 [4] 端末とサーバとの間の通信において、パスワードは暗号化して通信を行います。
17	4. 特定個人情報ファイルの取扱いの委託（P.27） 委託契約書中の特定個人情報ファイルの取扱いに関する規定 「規定の内容」 について 【意見】不法行為（故意または過失による権利侵害）により損害が発生した時の委託先に対するペナルティ内容を定める規定（事象単位の金額、指名停止期間）を含んだサービスレベルアグリーメントを取り交わす旨を追加していただきたい。 4. 特定個人情報ファイルの取扱いの委託（P.27） 再委託先による特定個人情報ファイルの適切な取扱いの確保 「具体的な方法」 について 【意見】不法行為（故意または過失による権利侵害）により損害が発生した時の再委託先に対するペナルティ内容（事象単位の金額、指名停止期間）を含んだサービスレベルアグリーメントを取り交わす旨を明記していただきたい。 4. 特定個人情報ファイルの取扱いの委託（P.36） 委託契約書中の特定個人情報ファイルの取扱いに関する規定 「規定の内容」 について 【意見】不法行為（故意または過失による権利侵害）により損害が発生した時の委託先に対するペナルティ内容を定める規定（事象単位の金額、指名停止期間）を含んだサービスレベルアグリーメントを取り交わす旨を追加していただきたい。 4. 特定個人情報ファイルの取扱いの委託（P.36） 再委託先による特定個人情報ファイルの適切な取扱いの確保 「具体的な方法」 について 【意見】不法行為（故意または過失による権利侵害）により損害が発生した時の再委託先に対するペナルティ内容（事象単位の金額、指名停止期間）を含んだサービスレベルアグリーメントを取り交わす旨を明記していただきたい。	契約書作成の際の参考とさせていただきます。

特定個人情報保護評価書（案）に対する意見募集の結果

18	該当箇所：Ⅲ特定個人情報ファイルの取り扱いプロセスにおけるリスク対策（全般） 意見内容１：対策の有効性についての確認ができるように改良していただきたい。 理由１：対策に関する記述が項目の列挙にとどまっており、その必然性や導入後の運用などを正しく行うための施策などについての記述がみられないため、これらの対策が「十分である」「力を入れている」といった漠然とした記載に対する立証が困難です。こうした対策は一時の評価ではなく継続的な評価が必要で有り、適切な運用体制が不可欠であることから、当該組織における管理体制、運用体制について確認できる内容を追加していただきたいと考えます。 意見内容２：システムの開発、保守に関するリスクとその対策も記載していただきたい。 理由２：「別添１」記載の内容は、単なる「方式説明」にすぎず、これらのシステム開発において、こうした方式が正しく実装され、試験され、また、導入後の運用において発見された問題点などをどのように適切に修正するのかといった点がまったく不明です。昨今のオープンソースソフトウエアの脆弱性などを顧みるに、実装面での脆弱性によって安全が脅かされる例が多発しており、大きなリスクとなっています。 意見内容３：技術的対策を記述した部分について、不十分もしくは不正確な記述が見られるので、読者が誤解する恐れのない表現としていただきたい。 理由３：たとえばP25「その他の措置の内容」に記載されたパスワードに対する「暗号化」は正確には「ハッシュ化」であり不可逆なものでなくてはなりません。鍵により復号可能な暗号化方式を採用した場合、内部者により情報が盗用されるリスクが発生する可能性があるので、「ハッシュ化」と明記すべきと考えます。また同ページの「ユーザ認証の管理／具体的な管理方法」では、パスワードの変更通知について書かれていますが、通知のみでなく、確実に変更させる仕組みやパスワードポリシー（文字数、文字種、再利用制限など）をシステム的に強制することで実効性を担保する必要があるなど。	１．運用時の管理は、全項目評価書Ⅱ３⑦の通り、総務省大臣官房企画課個人番号企画室が実施する予定です。本システムの運用に係る項目は現在検討中であり、管理体制、運用体制については、今後整備する運用手順書や運用規程等にて記載します。 ２．本評価書や調達仕様に基づきシステムの開発を行い、試験を通じて各方式が正しく実装されていることを確認します。なお、本評価書は、指針に基づき、特定個人情報を取り扱う事務を対象にリスク評価を行っています。運用・保守における手順は、今後整備する運用手順書や運用規程等にて記載します。 ３．ご指摘ありがとうございます。ご指摘を踏まえ、評価書に追記いたします。