主要な論点リスト（案）

資料1

番号	大項目	中項目	骨格案の項番	主要な論点リスト
1	個人に対する付番、番号連携及び情報連携	基本的な考え方	第1．1．（1）	○各機関間の情報連携は情報連携基盤を通じて行わせることにより、個人情報保護に十分配慮した仕組みとすべきではないか。
2			第1．1．（2）	○情報連携基盤の構築に当たっては、住民基本台帳ネットワークシステムに係る最高裁合憲判決（最判平成20年3月6日）の判断枠組みに適合した形で個人情報保護を取り扱うシステムとすることが必要。さらに、社会保障・税に関わる番号制度及び国民ID制度においては、住基ネットより一層高度の安全性を確保することが必要ではないか。
3		情報連携の原則	第1．2．（1）	○「見える」「番号」を直接用いない情報連携 情報連携基盤においては、「番号」は「民−民−官」で広く利用される「見える番号」であることから、これをそのまま当該個人を特定する共通の識別子（「IDコード」）として用いることは、個人情報保護の観点から適切ではないのではないか。
4			第1．2．（2）	○「見えない」IDコードを用いる情報連携 IDコードはこれを認知できる者を極力最小限とする「見えない番号」とすべきではないか。その際、「住民票コードに対応した新しいコード」とすべきではないか。
5			第1．2．（3）	○情報保有機関ごとに付与されるリンクコードを用いる情報連携 「番号」を含む利用番号とIDコードの間にIDコードと対応関係のある「見えない」コード（「リンクコード」）を介在させ、原則として情報保有機関ごとに異なるリンクコードを付与し、情報保有機関はそれぞれのリンクコードを用いて情報連携基盤にアクセスすることとすべきではないか。
6		付番と番号管理	第1．3．（1）	○「番号」とIDコード・リンクコードの付番のあり方 住民票コードから「番号」を生成する方式と、住民票コードからIDコード、さらにリンクコードを生成する方式は別の方式とし、「番号」から論理的にIDコードに遡れないようなものとすべきではないか。
7			第1．3．（2）	○IDコード及びリンクコードの生成方法 住民票コードからIDコード、さらに、IDコードからリンクコードを生成する方法は、可逆暗号方式（※1）又はコード変換テーブル方式（※2）が考えられるが、個人情報保護の観点から、可逆暗号方式を採用すべきではないか。 ※1 可逆暗号方式： その都度可逆暗号によってリンクコードからIDコード、又はIDコードからリンクコードを生成する方式 ※2 コード変換テーブル方式： 乱数を用いて論理的に遡れない形でコードを変換し、変換前後のテーブルを保持する方式
8			第1．3．（3）	○「番号」の生成方法 住民票コードから「番号」を生成する方法は、IDコードを生成する方法とは異なるものとすべきであり、乱数を用いて論理的に遡れない形でコードを変換し、変換前後のテーブルを保持する「コード変換テーブル方式」を採用することが適切ではないか。その際、変換前後のテーブルは、「番号」の付番機関のみにおいて保持し、二重付番の回避、住民票コードの変更時への対応等に活用してはどうか。
9			第1．3．（4）	○「番号」とIDコード、リンクコードの管理のあり方 情報の分散管理により、漏洩時の波及リスクを最小化する観点から、「番号」とIDコードは、できる限り分離して管理することが望ましいのではないか。また、情報連携基盤においては、IDコードのみを保持することとし、リンクコードは情報連携ごとに可逆暗号で生成して、連携終了後消去することとすべきではないか。
10			第1．3．（5）	○「番号」とIDコード・リンクコードの個人への通知の必要性 「番号」については、「番号」が付番される各個人に対して安全な方法で通知されることが必要である。一方、IDコードについては、情報連携基盤においてのみ保有することとし、リンクコードについては情報保有機関においてのみ保有することとするが、セキュリティを確保するため、各個人に対しても通知されないこととすべきではないか。
11			第1．3．（6）	○「番号」とIDコード、リンクコードの変更可能性 安全性を確保する観点から、「番号」については個人からの変更請求を認めることを検討すべきではないか。 一方、IDコードとリンクコードについては、個人に通知されるものではないため、個人からの変更請求は想定されないが、万一の場合を想定し、システム上・運用上の負荷を勘案した上で、セキュリティの観点からの変更可能性について検討すべきではないか。

番号	大項目	中項目	骨格案の項番	主要な論点リスト
12			第1．3．（7）	○分野別に考慮すべき事項とリンクコードの付与単位 リンクコードについては、通常は、各地方公共団体を含め、情報保有機関ごとに付与されるものと考えるべきではないか。 ただし、制度上情報の共有が想定されており、現に書面又は電子的手法を通じて情報共有がなされている場合には、情報連携基盤を通じた情報連携とは異なる取扱いを行うことも検討すべきではないか。 また、特に各社会保障分野内の情報のやりとりについては、例えばサブシステムを設けて分担させ、当該分野を超えて情報連携を行う場合には当該サブシステムを経由して情報連携基盤に照会を行う仕組みにするなど、社会保障分野の特性に応じた仕組みを検討することが考えられるのではないか。 したがって、各社会保障分野におけるリンクコードの付与に当たっては、個別の情報保有機関ごとに付与すること以外の選択肢についても検討を行うことが考えられるのではないか。
13		番号連携	第1．4．（1）	○番号連携の前提としての紐付けの必要性 IDコード、リンクコードによる情報連携を可能とするためには、情報連携基盤により各情報保有機関に対して割り振られたリンクコードが、当該情報保有機関の持つ個人情報データベースに紐付くことが必要ではないか。
14			第1．4．（2）	○4情報の突合の必要性 リンクコードが情報保有機関の個人情報データベースに紐付けられるためには、情報保有機関が保有する4情報と、リンクコード、IDコードの基礎となっている住民票コードに係る住基ネットの保有する最新の4情報とを突合することが必要ではないか。 そのため、情報保有機関の責任で、情報保有機関が保有する4情報を最新のものとすることが不可欠であり、このために、住基ネットを活用できるようにすることが求められるのではないか。
15			第1．4．（3）	○リンクコードと「番号」等との対照テーブル 紐付けをした後のリンクコードと「番号」等は、4情報の突合をすることにより、各情報保有機関においてその対照テーブルを保持すべきではないか。
16			第1．4．（4）	○番号連携の流れ IDコード、リンクコード間が可逆的に変換可能となり、かつ、各情報保有機関においてリンクコードと「番号」等が紐付けられることにより、「（照会元情報保有機関の）「番号」等－（照会元情報保有機関の）リンクコード－IDコード－（照会先情報保有機関の）リンクコード－（照会先情報保有機関の）「番号」等」の順序で全ての「番号」等が紐付けられ、「番号」等間の連携が可能となるのではないか。
17		情報連携	第1．5．（1）	○法令に基づく情報連携を行う情報保有機関と情報連携対象個人情報の特定 予め法律又はこれに基づく政令によって、情報連携を行う目的、情報連携を行う情報保有機関及び情報連携の対象となる個人情報の種類及び情報連携のパターンについて、明確に定めておくべきではないか。
18			第1．5．（2）	○情報連携基盤における情報連携の承認 情報連携の条件が満たされているかどうかについては、情報連携基盤が、照会に対してその都度承認を行うこととし、その上で「（照会元情報保有機関の）リンクコード－IDコード－（照会先情報保有機関の）リンクコード」という情報連携基盤内の手順を進めることとすべきではないか。
19			第1．5．（3）	○情報連携の際の適切なアクセス制御 照会元情報保有機関、照会先情報保有機関においては、各機関におけるシステム改修の負担等も考慮しつつ、情報連携に関連する業務に携わることができる職員を予め限定し、関係する端末やデータベースへのアクセスを適切な方法により制御することにより、不正アクセスや情報漏洩を防止するとともに、事後的な当該機関内又は第三者機関等による監査の対象とすることを検討すべきではないか。
20			第1．5．（4）	○情報連携の手順 ①まず、照会元の情報保有機関において、リンクコードと「番号」等との対照テーブルを活用し、情報連携を行う対象者についてのリンクコードを用いて、入手しようとしている情報連携対象個人情報及び照会先の情報保有機関を原則として指定して、情報連携基盤に問い合わせることによって、手続が開始することとすべきではないか。 このため、照会元情報保有機関においては、情報連携を行う際に、対象者に係る4情報を、予め住基ネットの持つ最新の4情報に更新する等の方法により、可能な限り照会先情報保有機関（例えば現住所がある地方公共団体）を予め知っておくこととすべきではないか。その手法としては、第1．4．（2）の方法に準じて、住基ネットと各情報保有機関との間で行うこととすべきではないか。 なお、将来的に、日本年金機構や全国健康保険協会等住基ネットから4情報を直接提供することが可能とされているような団体以外の民間の情報保有機関が情報連携を行うことになった場合には、民間の機関の側で情報連携について本人の同意を得て本人から入手した4情報を用いて、情報連携基盤を通じて照会し、住基ネット側の4情報と合致した場合のみにリンクコードを付番するといった仕組みを検討すべきではないか。
21				②続いて、情報連携基盤においては、当該照会に係る情報連携の内容が、予め法令によって特定されたリストに含まれていることを確認し、確認できた場合には、これを承認の上、「（照会元情報保有機関の）リンクコード－IDコード－（照会先情報保有機関の）リンクコード」という手順を経て、照会先情報保有機関に対してそのリンクコードとともに情報連携対象個人情報の種類を伝達することとすべきではないか。

番号	大項目	中項目	骨格案の項番	主要な論点リスト
22				③その後、情報連携基盤より伝達を受けた照会先情報保有機関においては、当該リンクコードに係る個人の情報連携対象個人情報を付して、情報連携基盤を通じて照会元情報保有機関に対して、回答すべきではないか。 　その際、いつ、誰が、どの情報に関して、何の目的のために情報連携を行ったかといった事項に関する履歴（以下「アクセスログ」という。）を保存し、対象者である個人及び第三者機関等が事後的に閲覧できるようにすべきである。しかしながら、情報の集中管理とならないようにするため、情報連携対象個人情報そのものについては、情報連携基盤を通じて回答がされることにとどめ、情報連携基盤においては保存されないようにすべきではないか。
23		アクセスログの保存及び提供	第1．6．（1）	○アクセスログの種類と使用目的に応じた検討のあり方 　想定されるアクセスログの種類については、例えば①管理用のシリアル番号、②情報連携の照会等のアクセスを行った日時、③情報連携の根拠（法令等で予め定められた情報連携のパターン）、④照会元情報保有機関の名称、⑤照会先情報保有機関の名称、⑥情報連携対象個人情報の種類、⑦照会元情報保有機関で端末を操作した担当職員名（又は担当部署や職員名に代わる属性情報）、⑧照会先情報保有機関で端末を操作した担当職員名（又は担当部署や職員名に代わる属性情報）、⑨照会元情報保有機関において使用された端末、⑩照会先情報保有機関において使用された端末、⑪提供された情報連携対象個人情報の内容、⑫情報連携対象個人情報の用途などが考えられるが、情報の分散管理及び費用対効果の観点を踏まえつつ、アクセスログの使用目的に応じて、その保管及び提供のあり方を検討すべきではないか。 　その際、大きく分けて、個人がマイポータル等を通じて事後的に閲覧するアクセスログの範囲と第三者機関が不正アクセス・情報漏洩等を検知するために閲覧・分析を行うアクセスログの範囲とでは、後者の方がより詳細なものとして設定すべきではないか。
24			第1．6．（2）	○アクセスログの保存に係る役割分担 　アクセスログもその多くが個人情報であり分散管理すべきものであることから、全てを情報連携基盤で保存するのではなく、できる限り情報保有機関側で保存すべきものは保存するように工夫すべきではないか。
25			第1．6．（3）	○アクセスログの保存期間 　アクセスログの保存期間の検討に当たっては、その使用目的との関連で、必要最小限とし、かつ費用面で過度な負担を生じることがないよう配慮すべきではないか。 　その際、不正アクセスや情報漏洩によって犯罪を構成する可能性に鑑み、刑法第246条の2（電子計算機使用詐欺）等の公訴時効が刑事訴訟法第250条により7年と規定されていることとの関係を検討すべきではないか。
26			第1．6．（4）	○個人によるマイポータル等を通じたアクセスログの閲覧 　情報連携の対象者である個人によるアクセスログの閲覧の仕組みの検討に当たっては、マイポータルはインターネットから接続されるものであることに鑑み、閲覧を求める個人からの申請があった場合にのみ、その申請内容に応じて、アクセスログを保存する機関から提供されることとすべきではないか。 　その際、マイポータルにおいて直接閲覧できるアクセスログは、原則として情報連携基盤が保存するものに限ることとし、情報保有機関において保存すべきアクセスログのうち、例えば⑪提供された情報連携対象個人情報の内容、⑫情報連携対象個人情報の用途については、別途各情報保有機関に対して申請する手続を設け、当該手続を経た後にマイポータルにおいて閲覧するといった方策を検討すべきではないか。 　同時に、パソコンや行政キオスク端末等を使用することが困難な個人に対してもアクセスログの閲覧を可能にするため、例外的措置として、行政機関の窓口による対応等も可能とすることを検討すべきではないか。
27			第1．6．（5）	○第三者機関によるアクセスログの閲覧・分析 　第三者機関は、情報連携基盤において保存するアクセスログのみならず、情報保有機関において保存するアクセスログについても、原則として全て閲覧・分析ができるように検討すべきではないか。
28		情報保有機関の機能と既存システム・情報連携基盤間のインターフェイス	第1．7．（1）	○情報保有機関において備えるべき機能 　情報保有機関においては、照会元情報保有機関及び照会先情報保有機関としての機能、例えば、情報連携に必要なアクセス制御、アクセスログのうち情報保有機関において保存すべき情報の保存、照会を受けた際に情報連携対象個人情報を特定して一定期間内に回答する機能等を持つことが考えられるのではないか。
29			第1．7．（2）	○既存システムと情報連携基盤をつなぐインターフェイスの確保 　各情報保有機関が持つ既存システムが直接、照会元情報保有機関及び照会先情報保有機関としての機能を持つように改修することは、費用を可能な限り抑制する観点から必ずしも適切ではないのではないか。 　そこで、住基ネットにおいて用いられているコミュニケーション・サーバー方式などを参考に、既存システムの差異を吸収するインターフェイスの確保方法について、個別の既存システムの状況を踏まえた検討が必要ではないか。

番号	大項目	中項目	骨格案の項番	主要な論点リスト
30		情報連携基盤・情報保有機関間等の回線	第１．８．	○情報連携基盤・情報保有機関間等の回線 　情報連携の仕組みの構築に当たっては、情報連携基盤と各情報保有機関間等を結ぶ回線についても検討が必要である。 　その際には、できる限り既存のシステムを有効利用するという観点から、情報連携基盤と各情報保有機関を結ぶ回線については、原則として国の各行政機関間において用いられている霞ヶ関WAN並びに各地方公共団体間及び各地方公共団体と国の行政機関との間で用いられている総合行政ネットワーク（LGWAN）を改良することにより対応することを検討すべきではないか。
31	個人の本人確認（マイポータル・ICカード等）	基本的な考え方	第２．１．（１）	○高いセキュリティレベルに対応できる認証方法の必要性 　マイ・ポータル等は所得情報などセンシティブな個人情報を取り扱うこととなる。 　住基ネット訴訟に係る最高裁判決に対応するためには、マイ・ポータルにログインするための本人認証は、高いセキュリティレベルに対応できる認証方法とするなど、個人情報保護の観点や情報の一元管理を回避する厳格な仕組みが必要であり、「「番号」を利用する際、利用者が「番号」の持ち主本人であることを証明するための本人確認（公的認証）の仕組みを構築するため、既存のシステムである公的個人認証及び住民基本台帳カードを番号制度の導入に合わせて改良し、活用することにより、本人確認を行う」（基本方針P．７）。
32			第２．１．（２）	○公的個人認証サービス及び住民基本台帳カードの改良 　公的個人認証サービスや住民基本台帳カードは、もともと「番号」と「番号」を所持する者との関係を確認するために設けられたものではないことから、社会保障・税に関わる番号制度及び国民ID制度で活用していくために、いくつかの改良が必要である。
33		マイ・ポータルの利用	第２．２．（１）	○マイ・ポータルの機能 　マイ・ポータルが提供するサービスとしてには、次の４つの機能を持たせることとしてはどうか。 　①自己情報へのアクセスログを確認する機能 　②各情報保有機関が保有する自己情報を確認する機能 　③電子申請を経由する機能（ワンストップサービス） 　④行政機関等からのお知らせを表示する機能（プッシュ型サービス）
34			第２．２．（２）	○マイ・ポータルにおける情報管理のあり方 　マイ・ポータルが取り扱う情報を内部的に管理するため、利用者の申請により各利用者固有の情報を管理する領域を確保し、利用者フォルダを開設することとし、個人情報保護の観点や情報の一元管理を回避する観点から、利用者の個人情報が利用者フォルダに過度に蓄積しないように、ログアウトの度に利用者の個人情報のうち必要のないものについては消去する仕組みとしてはどうか。
35			第２．２．（３）	○マイ・ポータルにログインするための認証 ①ログインのためのアクセスキー 　IDコードやリンクコードをICカード内に格納してマイ・ポータルにログインするためのキーにすることは、セキュリティの観点から相応しくないのではないか。 　「番号」は、他人に容易に知られてしまう「見える」番号であることから、これをキーとしてログインすることは、成りすまし等の具体的危険性が高いことから、相応しくないのではないか。 　このため、公的個人認証サービスに認証用途を付加し、認証用の電子証明書のシリアル番号識別情報（以下「認証用シリアル番号」という。）を、当該シリアル番号が流出しても、IDコード等を知ることはできないといった観点から、ログインするためのキーとして利用することとしてはどうか。 　一方で、認証用シリアル番号は電子証明書の有効期間満了により失効するものの、民間事業者も含め、各情報保有機関において蓄積されると、認証用シリアル番号を利用してデータマッチングする危険性が高まることから、認証用途以外の目的で使用することを法律上明確に禁止するといった対策を講じるべきではないか。
36				②認証用シリアル番号と認証局用リンクコードの紐付け 　認証局は、利用者の申請によりICカードに認証用の電子証明書を格納する際に取得した4情報をもって、情報連携基盤に認証局用のリンクコードの生成を要求し、生成された認証局用のリンクコードと認証用シリアル番号を紐付けしておくこととしてはどうか。
37				③マイ・ポータルへのログインの手順 　マイ・ポータルにログインする手順としては次のとおりとしてはどうか。 (a) 利用者フォルダの取得（初回にアクセスする際の対応） ⅰ）利用者は、ICカードをリーダライタにセットし、暗証番号を入力し、公的個人認証サービスの署名用の電子証明書等を利用して、利用者フォルダ取得の電子申請を行う。 ⅱ）マイ・ポータル運営機関は、利用者の電子署名付きの電子申請を受領し、認証局に対して電子証明書の有効性確認を行い、電子申請の正当性を確認する。 ⅲ）マイ・ポータル運営機関は、マイ・ポータルが取り扱う情報を内部的に管理するため、各利用者固有の情報を管理する領域である利用者フォルダを開設する。 ⅳ）マイ・ポータル運営機関は、利用者の申請による4情報をもって、情報連携基盤にマイ・ポータル用のリンクコードの付番を要求する。 ⅴ）マイ・ポータル運営機関は情報連携基盤から通知された当該リンクコードと利用者フォルダを紐付ける。

番号	大項目	中項目	骨格案の項番	主要な論点リスト
38				③マイ・ポータルへのログインの手順〔承前〕 (b) ログイン（アクセスする都度の対応） ⅰ）利用者は、マイ・ポータル上にあるログイン・ボタンをクリックした後、ICカードをリーダライタにセットし、暗証番号を入力して、公的個人認証サービスの認証用の電子証明書等を利用して、ログイン要求を行う。 ⅱ）利用者が送付する認証用の電子証明書等は暗号化してマイ・ポータル運営機関に対し送付する。 ⅲ）マイ・ポータル運営機関は、認証局とやりとりして、認証用の電子証明書の有効性を確認し、利用者の認証を行う。 ⅳ）認証がされた場合、マイ・ポータル運営機関は認証用シリアル番号を情報連携基盤へ送付する。送付後は、マイ・ポータル運営機関に認証用シリアル番号が蓄積しないよう削除する。 ⅴ）情報連携基盤は、認証用シリアル番号を認証局へ送付する。送付後は情報連携基盤に当該番号が蓄積しないよう削除する。 ⅵ）認証局は、あらかじめ認証用シリアル番号に紐付けられた認証局用リンクコードを、情報連携基盤に振り出す。 ⅶ）情報連携基盤は、当該認証局用のリンクコードからIDコードを介して、マイ・ポータル運営機関にマイ・ポータル用のリンクコードを振り出す。 ⅷ）マイ・ポータル運営機関は、当該マイ・ポータル用のリンクコードから、当該利用者の利用者フォルダを特定する。 ⅸ）マイ・ポータル運営機関は利用者に対して、ログインに成功したことを通知する。
39			第2．2．（4）	○自己情報へのアクセスログを確認する機能 アクセスログを確認する手順としては次のとおりとしてはどうか。 ⅰ）マイ・ポータルにログイン後、利用者が、自己情報へのアクセスログの確認をマイ・ポータル運営機関に要求する。 ⅱ）マイ・ポータル運営機関は、利用者フォルダと紐付いているリンクコードを通じて、情報連携基盤等に問い合わせをする。 ⅲ）情報連携基盤は、情報連携基盤に記録されているアクセスログの情報を、マイ・ポータル用のリンクコードを通じて、マイ・ポータルの利用者フォルダに送付する。 ⅳ）利用者がマイ・ポータルからログアウトすると同時に、利用者フォルダに一時的に保存されているアクセスログの情報は削除する。
40			第2．2．（5）	○各情報保有機関が保有する自己情報を確認する機能 情報保有機関が保有する自己情報は、情報保有機関において適切に管理するべきものであり、マイ・ポータルに蓄積することは極力回避するべきではないか。 マイ・ポータルは、情報保有機関と認証連携を行い、情報の閲覧は、情報保有機関が有するサイトから行うこととすべきではないか。 既存の技術を活用しつつ、マイ・ポータルへログインした際の認証結果を情報保有機関に引き継ぐ方法を検討してはどうか。 自己情報を確認する基本的な手順としては次のとおりとしてはどうか。 ⅰ）利用者は、マイ・ポータルにログイン後、情報保有機関が保有する自己情報を確認することをマイ・ポータル運営機関に対して要求する。 ⅱ）マイ・ポータル運営機関は、利用者フォルダに紐付いているマイ・ポータル用のリンクコードを通じて、情報連携基盤に問い合わせる。 ⅲ）情報連携基盤は、マイ・ポータル用のリンクコードをIDコードに変換し、さらに、情報保有機関のリンクコードを振り出して、情報保有機関に伝達をする。 ⅳ）情報保有機関は、当該リンクコードから、情報保有機関が保有する利用番号を通じて、必要な情報を取り出し、当該情報を情報連携基盤を通じて、マイ・ポータルに送信をする。 ⅴ）マイ・ポータル運営機関は、利用者フォルダに個人情報を一時的に保存して、マイ・ポータルに表示する。 ⅵ）利用者がマイ・ポータルからログアウトすると同時に、利用者フォルダに一時的に保存されている情報保有機関の情報を削除する。
41			第2．2．（6）	○電子申請を経由する機能（ワンストップサービス） 利用者は、マイ・ポータルに公的個人認証サービスの認証用の電子証明書等によりログインすることとなるが、社会保障や税の分野における電子申請のように、センシティブな個人情報を取り扱うことが想定されている場合には、あらためて公的個人認証サービスの署名用の電子証明書等で申請を行う必要があるのではないか。 情報保有機関に対する電子申請については、文書の真正性の推定効が働くことや改ざんを防止する必要があることから、情報保有機関の責任において署名検証を行う必要があるのではないか。 必要な手続きはマイ・ポータルのトップページから、各情報保有機関のサイトにリンクを張り認証連携することで、利用者が各手続きの電子申請を行うこととするが、典型的なサービスについて、一度、電子申請をすれば、申請が必要な全ての情報保有機関に送付され処理される仕組み（ワンストップサービス）も検討することとしてはどうか。

番号	大項目	中項目	骨格案の項番	主要な論点リスト
42			第２．２．（７）	○行政機関等からのお知らせを表示する機能（プッシュ型サービス） 情報保有機関が利用者に対してお知らせする事項がある場合には、当該情報は、マイ・ポータルの利用者フォルダに送付する仕組みとしてはどうか。 お知らせを表示する手順としては次のとおりとしてはどうか。 ⅰ）情報保有機関が利用者に対して伝達事項がある場合には、情報保有機関のリンクコードを通じて、情報連携基盤に必要なお知らせ情報を送付する。 ⅱ）情報連携基盤は、情報保有機関のリンクコードをIDコードに変換し、さらにマイ・ポータル用のリンクコードを振り出して、マイ・ポータルの利用者フォルダに、お知らせ情報を送付する。 ⅲ）利用者がマイ・ポータルにログインするまで、当該情報は利用者フォルダに保存することとし、利用者がマイ・ポータルにログインした際、当該お知らせ情報を表示する。なお、当該お知らせ情報には、リンクが張られており、必要な電子申請等を行うことができるようにする。 ⅳ）利用者が閲覧した場合や、当該情報を表示する期限が切れた場合には、当該情報が利用者フォルダから削除される。
43			第２．２．（８）	○自宅以外でのマイ・ポータルの利用 マイ・ポータルは、自宅のパソコンで利用できることはもちろん、自宅にパソコンがない場合であっても、例えば、現在は証明書等の発行に利用されている行政キオスク端末で利用が可能となる仕組みとするべきではないか。 そのためには、コンビニエンスストアなど、既存のインフラやサービスを有する民間事業者と連携を図ることを検討してはどうか。
44		窓口等における本人確認	第２．３．（１）	○書面により本人確認及び「番号」確認を行う場合 ① 本人がICカードを所持していない場合 法令等で「番号」を確認することが認められている機関の窓口等（以下「窓口等」という。）においては、利用者に対し、本人確認書類（運転免許証等）の提示を求め、本人であることを確認した上で、「番号」の申告を求め、本人から申告された「番号」を書面に記載することとしてはどうか。 ② 本人がICカードを所持している場合 ICカードのICチップ内に「番号」を安全に格納し、窓口等において確認できる仕組みとしてはどうか。
45			第２．３．（２）	○電子的に本人確認及び「番号」確認を行う場合 窓口等が書面を使わず電子的に本人確認及び「番号」確認を行う場合には、公的個人認証サービスの仕組みを活用して本人確認をした上で、ICカードから「番号」を取り出す仕組みとしてはどうか。 なお、窓口等の体制が未整備の場合は、ICカードに記載された「番号」を書面に記載することも考えられるか。
46		公的個人認証サービスの改良	第２．４．（１）	○認証用途の付加の必要性 不正データに誤って電子署名をするリスクを回避するため、認証用途の付加を行う必要があるのではないか。 認証用の電子証明書は、署名用の電子証明書と異なり、文書の真正性の推定効が働かないことから、特に検証者に対しては、署名用の電子証明書と適切に使い分ける義務を課した上で、システムとしてその実行を担保する仕組みとしてはどうか。
47			第２．４．（２）	○鍵ペア 認証用途として利用した鍵ペアを、署名用途として利用した鍵ペアとして利用するリスクを回避するため、ICカードのICチップ内には、署名用途の鍵ペアと認証用途の鍵ペアを別々に格納するなどの措置を講じることとしてはどうか。
48			第２．４．（３）	○電子証明書の発行 現在、公的個人認証サービスについては、市町村が発行する住民基本台帳カードに市町村の窓口において厳格な本人確認を行った上で、都道府県知事が電子証明書を発行しており、このことが信頼性の担保となっていることから、同様の方法で発行することとすべきではないか。
49			第２．４．（４）	○電子証明書の記録事項 署名用の電子証明書は、現行と同様に、4情報、署名用シリアル番号、有効期間の満了日等を記録し、認証用の電子証明書には、4情報は記録せず、認証用シリアル番号、有効期間の満了日等を記録することとしてはどうか。
50			第２．４．（５）	○電子証明書の有効期間・更新 電子証明書の有効期間については、暗号方式を強化した上で、５年間に延長することとしてはどうか。 利用者がオンラインで失効した電子証明書を更新できる仕組みを検討してはどうか。
51			第２．４．（６）	○ICカード以外のデバイス ICカード以外の媒体の利用を希望する場合においては、公的個人認証サービスを格納するICカードを所持し、かつ、本人の同意がある場合に限り、セキュリティが確保されることを前提に、当該媒体に公的個人認証サービスを格納することを可能とする仕組みを検討することとしてはどうか。
52			第２．４．（７）	○署名検証者の拡大等 将来的に、署名検証者について民間事業者にも拡大することとしてはどうか。 その際、認証用シリアル番号のセキュリティを確保した上で、民間事業者が共同で署名検証を行う仕組みを検討してはどうか。

番号	大項目	中項目	骨格案の項番	主要な論点リスト
53		ICカード（住民基本台帳カードの改良）	第２．５．（１）	○ICカードの交付 国民に対して自己情報へのアクセス記録を確認する権利を保障する観点から、自己情報へのアクセス記録を確認する者に対しては、ICカード及び電子証明書を発行し、交付すべきではないか。 法定代理人や任意代理人による取得については、住基カードの取得の手続きと同様に、代理人の本人確認等の手続きを適切に行うことを検討してはどうか。
54			第２．５．（２）	○ICカードの発行 現在、住民基本台帳カードは、市町村の窓口において厳格な本人確認を行った上で発行しているが、同様の方法で発行することとすべきではないか。 現行の住民基本台帳カードは、①住民が転入届の特例を受け、②全国の行政機関で本人確認を行い、③住民の日常生活において民間事業者との契約等の手続の場面での本人確認を行うことを可能とするとともに、市町村が様々なサービスにICカードを活用できるようにすることを目的として設けられたものであることから、ICカードに当該機能も併せて持つこととしてはどうか。
55			第２．５．（３）	○券面記載事項 ４情報及び顔写真を券面に記載することとしてはどうか。 「番号」の持ち主であることを証明するため、カード券面に「番号」を記載することとし、偽変造防止のための技術的な工夫を施すべきではないか。 カード券面に「番号」を記載することを望まない者に対する対応についてどう考えるか。
56			第２．５．（４）	○ICチップ記録事項 ICカードの券面に記載されている「番号」が偽変造されていないことを確かめるため、ICチップ内に「番号」を安全に記録し、窓口等は、ICカードの券面記載事項（４情報、顔写真及び「番号」等）をリーダライタ及びソフトウエアで確認することができるようにしてはどうか。 ICチップ内の「番号」を確認するためのソフトウエアについては、カードを利用して本人確認をする必要がある者に対して交付するものとしてはどうか。 ICチップ内の「番号」は、法令等で「番号」を確認することが認められている機関が「番号」を確認する場合に限り、システム上加工可能なデータとして取り出せることを検討してはどうか。
57	法人に対する付番	付番対象	第３．１．	法人に対して付番する「番号」の付番対象は、会社法人等番号を有する法人本店のほか、登記のない法人、国及び国税等の納税義務を有する人格なき社団等など付番機関の長が適当と判断したもの（以下「登記のない法人等」という。）とし、登記のない法人等については、付番機関が独自の「番号」を付することとしてはどうか。 法人の事業所に関しては、必ずしも会社法人等番号を有しないこと等から「番号」の付番は困難であるが、国税と地方税とで源泉徴収又は特別徴収を行う給与支払事務所の範囲が重複しており、これらに関しては部内番号等の情報を共有していくこととすべきではないか。
58		登記のない法人等に対する付番方法	第３．２．	番号の基礎となる会社法人等番号は、登記所コード４桁＋登記簿種別２桁＋個別番号６桁の計１２桁の整数で構成されているが、登記のない法人等に対しては、既存の登記所コードと重ならない番号を使用して付番することとしてはどうか。
59		番号の変更	第３．３．	会社法人等番号は平成２４年度以降、管轄登記所外への移転登記又は組織変更の登記を行っても会社法人等番号が変更されない仕組みとなる予定であり、「番号」についても同様に、変更しないこととしてはどうか。 また、重複付番を避けるためにも一度使用した番号は再利用しないこととしてはどうか。
60		番号の通知	第３．４．	法人は公的認証の利用または券面に表示された番号を提示して税又は社会保障サービスを受けることを想定していないことから、番号の通知は紙により行うこととしてはどうか。
61		検索及び閲覧	第３．５．	法人等に対する付番機関においては、法人等の基本３情報（商号又は名称、本店又は主たる事務所、会社法人等番号）の検索、閲覧ができるサービスをホームページで提供することを基本としてはどうか。
62	その他	企業コードについて	第４．１．	IT戦略本部電子行政に関するタスクフォースにおいては、行政の電子化によって企業の利便性の向上や行政の業務効率の向上を図る観点から、企業コードの整備及びその活用のための施策について検討している。 検討の方向性としては、ニーズの把握、費用対効果の検証を前提として、例えば、番号制度により付番される法人番号と他の行政分野や民間分野で使用されている法人の識別番号との紐付け・置換の推進、行政機関間での企業情報の相互参照による行政手続における公的添付書類の削減、民間の電子商取引等においても信頼性が保たれた企業のアイデンティティを表す属性情報の参照の充実、用途・利用者・利用場所等を考慮した企業認証の整備等が考えられるのではないか。