

社会保障・税に関わる番号制度  
及び国民ID制度について

総務省自治行政局住民制度課  
平成 23 年 3 月 24 日

# 社会保障・税に関わる番号制度への対応①

社会保障・税に関わる番号制度に関する検討会・中間取りまとめ（平成22年6月29日）（抄）

選択肢Ⅱ～正確性・安全性からの選択～制度設計をどうする

どの番号を  
使うか

最小の費用で、  
確実かつ効率的  
な仕組み

候補

基礎年金番号

住民票コード

新たな番号  
＜住基ネットを活用  
し、新たに付番＞

- 国民全員に付番されておらず、重複もある。
- プライバシー保護の観点から、納税者番号として商取引相手などに見せるのは望ましくない。
- プライバシー保護の観点から、納税者番号として商取引相手などに見せるのは望ましくない。
- 「住民票コード」と対応させた新たな番号を付番するならば、上記のような問題を避けられ、投資コストも抑えられる。

有識者ヒアリングでの意見～選択肢の観点から～

- 新しい番号制度のシステムを立ち上げるより、住民に既に定着した住民基本台帳ネットワークを有効に活用して、無駄のないようにすべき
- 導入コストを抑えつつ、正確に国民を識別するために、住基ネットシステムを有効に活用すべき

社会保障・税に関わる番号制度に関する実務検討会・中間整理（平成22年12月3日）（抄）

＜「番号」に何を使うか＞

プライバシーの問題を回避しつつ、確実かつ効率的な仕組みを最小のコストで実現するという観点から、既存の情報システムである住基ネットを活用した（住民票コードと一対一対応した）新たな番号を使うことで検討を進める。

社会保障改革の推進について（平成22年12月14日閣議決定（抄））

2 社会保障・税に関わる番号制度について

- 社会保障・税に関わる番号制度については、幅広く国民運動を展開し、国民にとって利便性の高い社会が実現できるように、国民の理解を得ながら推進することが重要である。
- このための基本的方向については、社会保障・税に関わる番号制度に関する実務検討会「中間整理」において示されており、今後、来年1月を目標に基本方針をとりまとめ、さらに国民的な議論を経て、来秋以降、可能な限り早期に関連法案を国会に提出できるよう取り組むものとする。

## 社会保障・税に関わる番号制度への対応②

社会保障・税に関わる番号制度についての基本方針(平成23年1月31日政府・与党社会保障改革検討本部決定)(抄)

### 番号制度

#### 3つの仕組み

- 複数の機関に存在する個人の情報が**同一人の情報であること**の**確認を行うための基盤**
- 国や地方公共団体等が国民一人ひとりの情報をよりの確に把握し、国民が国や地方公共団体等のサービスを利用するための必要不可欠な手段

①付番:新たに国民一人ひとりに唯一無二の**民・民・官**で利用可能な見える「番号」を最新の住所情報と関連づけて付番する仕組み

○「番号」に何を使うか

個人:**住民基本台帳ネットワークを活用した新たな番号**  
(法人:商業・法人登記の申請に係る会社法人等番号を活用した番号)

○「番号」は誰に付番され、どの機関が付番を担うか

個人:住民票コードの付番履歴を有する**日本国民及び中長期在留者、特別永住者等の外国人住民**

※付番及び情報連携基盤を担う機関の所管は**総務省**

(法人:商業・法人登記の申請に係る会社法人等番号を有する法人、法人税の納税義務を有する人格なき団体等。付番を担う機関の所管は国税庁)

○「番号」を利用できる分野

年金、医療、福祉、介護、労働保険の各社会保障分野、国税及び地方税の各税務分野、国税及び地方税の各税務分野 ※各分野で利用されている既存の番号が当分の間並存

②情報連携:複数の機関において、それぞれの機関ごとに「番号」やそれ以外の番号を付けて管理している同一人の情報を紐付き、紐付けられた情報を活用する仕組み

○情報管理:各府省等のデータベースによる分散管理方式

○情報連携の範囲:「番号」と紐付けされた情報の最新化を図る仕組みについて検討

- ・利活用のための情報連携: 年金、医療、福祉、介護、労働保険の各社会保障分野、国税及び地方税の各税務分野
- (※将来的に幅広い分野での活用等も配慮したシステム設計を行う)

・情報連携基盤: 情報連携基盤技術ワーキンググループにおける議論を踏まえつつ検討・整理

③本人確認:個人や法人が「番号」を利用する際、利用者が「番号」の持ち主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**

○既存の**公的個人認証**及び**住民基本台帳カードを改良、活用することにより本人確認を行う**(※民・官、民・民で求められる適切な認証の在り方については今後検討)

○インターネット上にマイ・ポータル(仮称)を設置:国民が自己情報を確認し、行政機関等からのサービスを受けられるようにする

○個人情報保護の方策

○「個人情報保護WG」及び「情報連携基盤技術WG」(社会保障・税に関わる番号制度と国民ID制度に関する共同の検討の場)の設置 等

＜今後のスケジュール＞

平成23年(2011年)3月～4月「社会保障・税番号要綱」(仮称)の公表

6月「社会保障・税番号大綱」(仮称)の公表

秋以降可能な限り早期に「番号法(仮称)」案、関係法律の改正法案を提出

# 社会保障・税に関わる番号制度についての基本方針(概要) ①

## 理念

### 番号制度

- 複数の機関に存在する個人の情報が同一人の情報であることの確認を行うための基盤
- 国や地方公共団体等が国民一人ひとりの情報をよりの確に把握し、国民が国や地方公共団体等のサービスを利用するための必要不可欠な手段

## 番号制度に必要な3つの仕組み

### 付番

新たに国民一人ひとりに唯一無二の民・民・民・民・民で利用可能な見える「番号」を最新の住所情報と関連づけて付番する仕組み

### 番号制度

### 情報連携

複数の機関において、それぞれの機関ごとに「番号」やそれ以外の番号を付して管理している同一人の情報を紐付けし、紐付けられた情報を活用する仕組み

### 本人確認

個人や法人が「番号」を利用する際、利用者が「番号」の持ち主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

### ○「番号」に何を扱うか

- 個人: 住民基本台帳ネットワークを活用した新たな番号  
※「番号」の名称は国民の公募により決定
- 法人: 商業、法人登記の申請に係る会社法人等番号を活用した番号
- 「番号」は誰に付番され、どの機関が付番を担うか  
付番機関については「歳入庁の創設」の検討を進める
- 個人: 住民票コードの付番履歴を有する日本国民及び中長期在留者、特別永住者等の外国人住民  
※当分の間、付番及び情報連携基盤を担う機関の所管は総務省
- 法人: 商業、法人登記の申請に係る会社法人等番号を有する法人、法人税の納税義務を有する人格なき社団等

### 付番

### ○「番号」を利用できる分野

- 年金、医療、福祉、介護、労働保険の各社会保険分野、国税及び地方税の各税務分野
- ※各分野で利用されている既存の番号が当分の間並存

### ○情報管理

- 各府省等のデータベースによる分散管理方式

### ○情報連携の範囲

- 「番号」と紐付けされた情報の最新化を図る仕組みについて検討
- ・利活用のための情報連携
- 年金、医療、福祉、介護、労働保険の各社会保険分野、国税及び地方税の各税務分野
- ※将来的に幅広い分野での活用等も配慮したシステム設計を行う
- ・情報連携基盤  
情報連携基盤技術ワーキンググループにおける議論を踏まえつつ検討・整理

### 情報連携

### 本人確認

- 既存の公的個人認証及び住民基本台帳カードを改良、活用することにより本人確認を行う
- ※民・官・民・民で求められる適切な認証の在り方については今後検討
- ※情報連携基盤の不具合等発生時の対応を想定した制度設計等に留意が必要

- ①より公平・公正な社会の実現
- ②社会保障がきめ細やか且つ的確に行われる社会の実現
- ③行政に過剰や無駄や無駄のない社会の実現
- ④国民にとって利便性の高い社会の実現
- ⑤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

## 国民が自己情報を確認し、行政機関等からのサービスを受けられるようにする

### ○インターネット上にマイ・ポータル(仮称)を設置

- ・自己情報へのアクセス記録の確認
- ・行政機関等からの情報提供によるサービス享受



### 個人情報保護の方策

- 具体的方策について、今年5月を目的に一定の結論を得よう検討を進める
- ①自己情報へのアクセス記録の確認を法的に担保する規定の在り方、②第三者機関の在り方、③「番号」の目的外利用・提供の制限を明示、④関係法令の罰則の強化、⑤プライバシーに対する影響評価の実施とその結果の公表を行う仕組み
- 特定の分野(例えば金融、医療等)については、法律上措置すべき個人情報保護方策の有無等につき、個人情報保護WGにおける検討を踏まえ、当該制度を所管する主務官庁において今年5月を目的に一定の結論を得よう検討

### 今後の進め方

- 番号制度創設推進本部の設置(国民の理解を得ながら導入を推進)
  - ・全国47都道府県でシンポジウムを開催(平成23年度(2011年度)~24年度(2012年度))
- 地方公共団体等との連携
  - ・地方公共団体等の実情を踏まえながら、番号制度の実現に向けて議論・検討
- 法制の整備
  - ・内閣官房で「番号法(仮称)」を整備、関係府省で関係法律の改正等を実施
- ワーキング・グループの設置
  - ・「個人情報保護WG」及び「情報連携基盤技術WG」の設置
- 番号制度の導入に係る費用と便益
  - ・より精緻な費用の試算、番号制度導入の便益をわかりやすく国民に明示

### 今後のスケジュール

- 平成23年(2011年)1月 基本方針
- 3月~4月 「社会保障・税番号要綱」(仮称)の公表
- 6月 「社会保障・税番号大綱」(仮称)の公表
- 秋以降 可能な限り早期に「番号法(仮称)」案、関係法律の改正法案を提出
- ※番号制度の導入時期は制度設計や法案の成立時期により今後変わりが以下を目的とする
- 平成26年(2014年)1月 第三者機関設置
- 6月 全国民に「番号」配布(ICカードの国民への配布を検討)
- 平成27年(2015年)1月 税務分野等のうち可能な範囲で利用開始
- 以降 段階的に利用範囲を拡大

# 社会保障・税に関わる番号制度についての基本方針(概要) ②

## 一 主権者たる国民の視点に立った番号制度の構築

### 「番号」で何ができるのか

地方公共団体から提案されている意見も尊重しつつ、引き続き利用場面の拡大を目指して検討を進める

#### ○社会保障分野でできること

- ・ **高額医療・高額介護合算制度の改善**  
自己負担の上限に達した場合、立て替え払いをすることなく、以後の医療・介護サービスを受給可能
- ・ **保険証機能の一元化**  
券面に番号を記載した1枚のICカードの提示により、年金手帳、医療保険証、介護保険証を提示したものとみなす
- ・ **自己診療情報の活用**  
医療、介護サービスの現場において、本人が自分の診療情報等を容易に入手・活用できるように、地域医療連携、医療・介護連携の基盤整備が進展
- ・ **給付可能サービスの行政からの通知**  
障害のある方に対して、本人の同意に基づき利用可能な様々な施策の情報が提供される

等

#### ○年金分野でできること

- ・ **年金制度的確な運用**  
基礎年金番号の二重付番や年金手帳の二重交付の防止
- ・ **確定申告手続の簡略化**  
確定申告の際に必要な公的年金等の源泉徴収票の添付が不要となる
- ・ **所得比例年金制度の創設**  
税務の所得情報を活用した所得比例年金制度を創設するための基盤ができる

等

#### ○医療分野でできること

- ・ **確定申告手続の簡略化**  
確定申告の医療費控除に必要な領収書等の書面による添付ないし保存が不要になる

等

#### ○税務分野でできること

- ・ **所得の過少申告等の防止**  
効率的な寄せ・突合により、所得の過少申告や扶養控除のチェックが効率化し、社会保障の不正受給や税の不正還付等を防止することができる
- ・ **確定申告の際の自己情報の確認**  
e-Taxで確定申告を行う際、社会保険料控除の対象となる保険料や、医療費控除額の算出に必要な情報をマイ・ポータル（仮称）で確認することができる
- ・ **事業者負担の軽減**  
国と地方にそれぞれ記載事項が共通するものを提出する義務のある一定額以上の給与、年金の支払調書について、電子的な提出先を一か所とする

等

#### ○申請・申告等の負担が軽減できるもの(他の行政機関に出向く必要がなくなるもの)

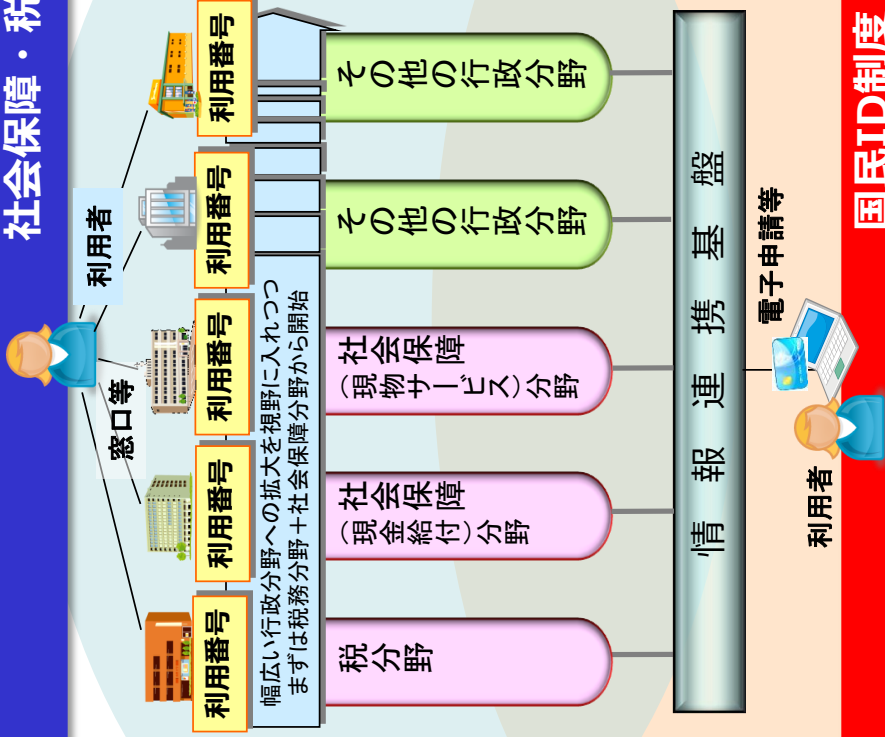
- ・ 行政機関へ申請・申告等する場合に必要な行政機関が発行する**添付書類の省略**
  - 給付等の申請  
(児童扶養手当、母子家庭自立支援給付金、特別児童扶養手当、障害者福祉手当、特別障害者手当、労災保険の年金給付)
  - 自己負担割合・自己上限負担額の決定  
(高額療養費、入院時食事療養費、入院時生活療養費の自己負担限度額、高齢者に係る医療保険の自己負担割合、養護老人ホームに係る入所者負担・扶養者負担、障害者自立支援法に基づく障害者福祉サービス・補装具等の自己負担、保育所・児童入所施設等の徴収金)
  - 国税・地方税の申告等  
(住宅ローン控除、住宅取得資金の贈与を受けた場合の贈与税の特例、居住用資産を買換えた場合の課税の特例、相続時精算課税の選択に係る届出、事業用資産を買換えた場合の課税の特例)

等

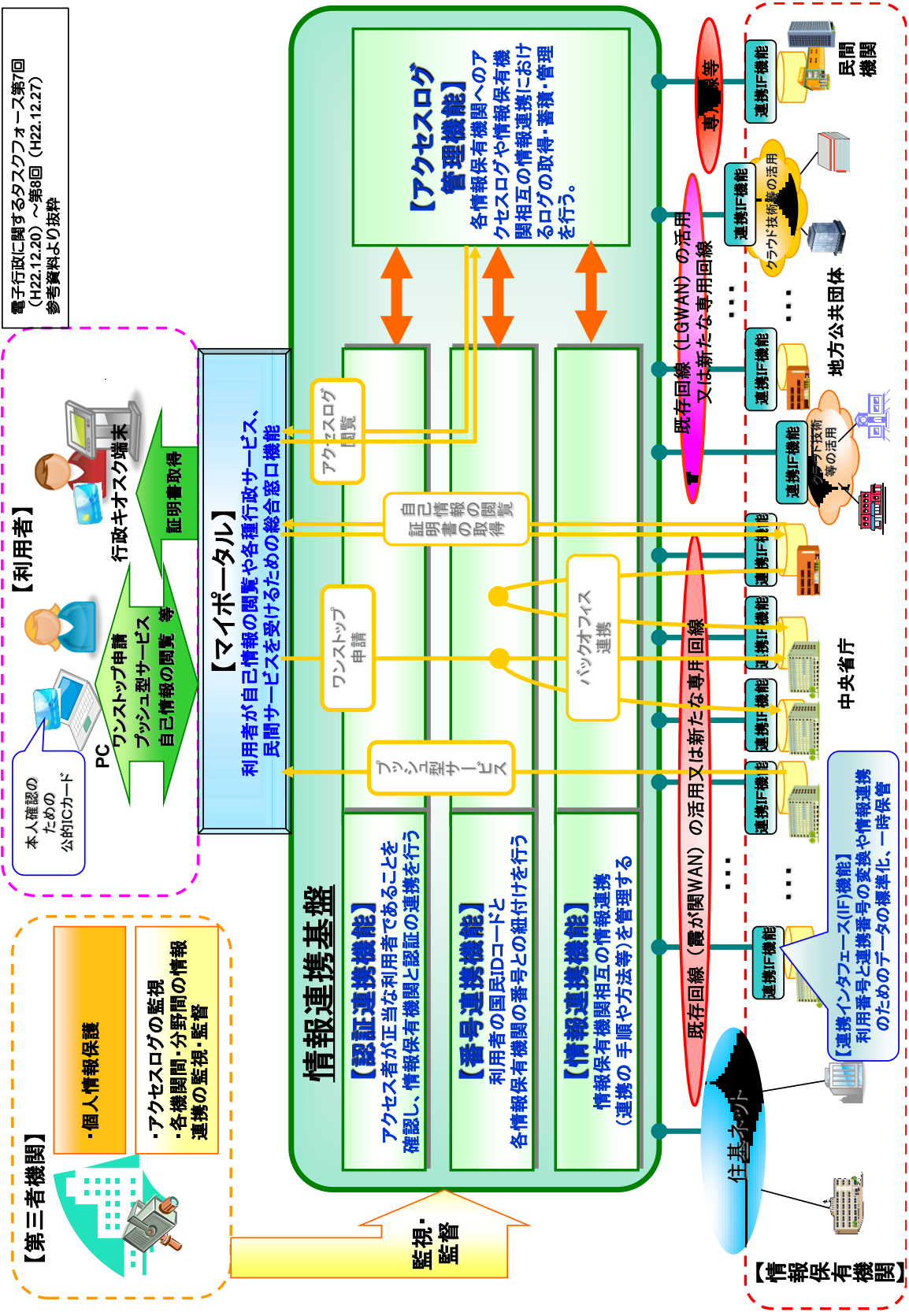
## 社会保障・税に関わる番号制度と国民ID制度の関係

情報通信による国民の利便性の向上、公平な負担、社会的弱者への確実な給付等を実現するため、国民が窓口等で利用する番号の整備（社会保障・税に関わる番号制度）と、各機関間の情報連携の仕組みの構築（国民ID制度）を一体的に進めることが不可欠。

### 社会保障・税に関わる番号制度



# 国民ID制度の全体イメージ



電子行政に関するタスクフォース第7回（H22.12.20）～第8回（H22.12.27）  
参考資料より抜粋

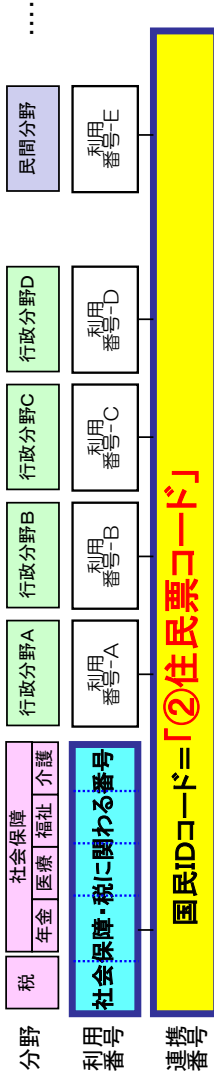
# 国民IDコードのあり方

電子行政に関するタスクフォース第7回（H22.12.20）～第8回（H22.12.27）資料より抜粋

国民IDコードに利用する番号については、一意性、悉皆性が重要な前提に立てば、「住民票コード」又は「住民票コードに対応した新しいコード」とすることが考えられるため、国民IDコードのあり方としては、次の2案が有力な選択肢。

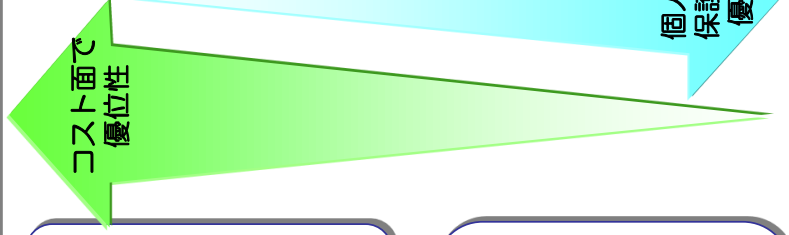
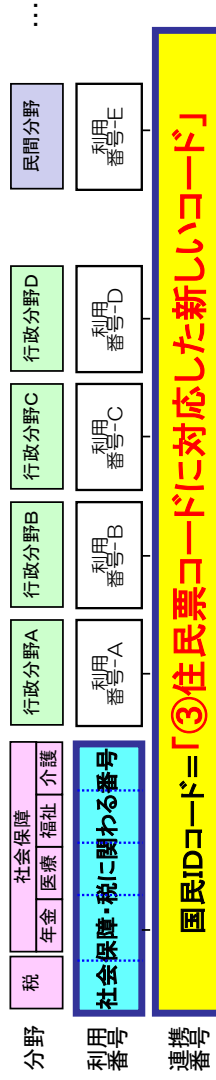
## <第1案>

社会保障・税に関わる番号と国民IDコードを別の番号とし、国民IDコードは、住民票コードを利用。



## <第2案>

社会保障・税に関わる番号と国民IDコードを別の番号とし、国民IDコードは、住民票コードに対応した新しいコードを利用。



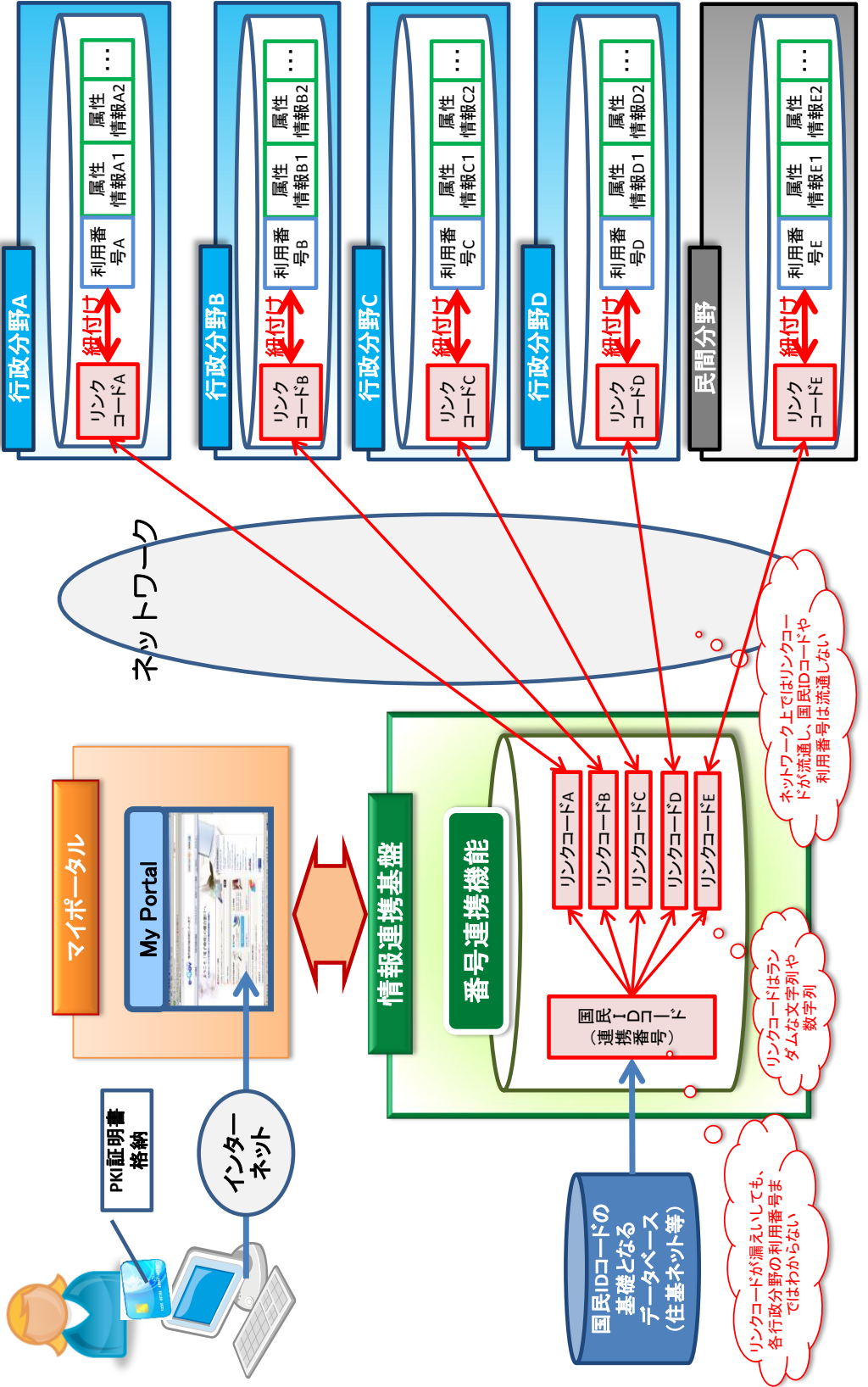
<参考> 国民IDコードと利用番号の連携は可逆（相互に検索可）の場合と、不可逆（利用番号から国民IDコードの検索不可）の場合がある。どちらも、ある分野で利用番号が溢れた場合でも別分野への不正アクセスや分野横断的な名寄せリスクを限定的なものにすることができるとは、不可逆の場合は、分野間の情報連携に当たって、その都度属性情報（氏名、住所、性別、生年月日）等により利用番号間の連携を行う（例：オーストラリアのセクター方式）などが想定され、その場合は効率性や安全性に課題があると考えられる。



# 参考. 情報連携基盤における番号連携のイメージ例

電子行政に関するタスクフォース第8回(H22.12.27)参考資料より抜粋

## 「利用番号」と「連携番号」の連携の仕方(イメージ例)



## 社会保障・税に関わる番号制度における個人情報保護方策の概要

座長試案

### 第1 はじめに

社会保障・税に関わる番号制度(以下「番号制度」という。)の導入に対しては、①国家により個人の様々な個人情報が番号をキーに名寄せ・突合されて一元管理されるのではないかとといった国家管理への懸念、②個人情報が漏えい、濫用されるのではないかとといった不正行為発生への懸念、③個人情報が、本人の知らぬ間に、かつ本人の利益に反して目的外で利用されるのではないかとといった目的外利用への懸念が指摘されている。

これらの懸念に適切に対処し、国民に安心して番号制度を利用していただくため、情報連携基盤を通じた個人情報のやり取りにおいて「番号」そのものは用いないこととするなどシステム上の安全措置を講じるほか、法制度上の措置として、目的外利用・提供等の制限等の規定を設け、番号制度における個人情報保護の観点から不当な行為を禁止するとともに、特に国家管理への懸念に対処するため、国民自らが自己情報へのアクセス記録等を確認する制度を法的に担保し、更に情報システムの導入等にあたり、プライバシーへ及ぼす影響を事前に評価し、その保護のための措置を促す仕組みを整えておく必要がある。

その上で、上記の制限等が遵守されているか、番号制度において個人情報が適切に取り扱われているか、システムが適切に稼働しているかなどといった点を、行政機関等から独立した第三者的立場で、監督する第三者機関(以下「第三者機関」という。)を設け、問題事例の発生を未然に防止するとともに、いったん問題事例が発生した場合にも、早期かつ適切に対処できるようにするほか、違法性の高い事案に対処するための罰則を整備する必要がある。

本座長試案において、以下、それぞれの法制度上の措置について、考えられる概要案を提示するものとする。

### 第2 目的外利用・提供等の制限等

#### 1 目的外利用・提供等の制限

(1) 情報保有機関(注1)に対する目的外利用・提供の制限

- 番号制度について、情報連携基盤を用いることができる事務の種類、提供される個人情報の種類及び提供先等を逐一法律又は法律の授權に基づく政省令に書き込むことで番号制度の利用範囲を特定することと

することが考えられる。

なお、情報保有機関が保有する番号に係る個人情報(注2)のうち、あらかじめ本人の同意を得て情報連携する必要がある個人情報については、その旨法律又は法律の授權に基づく政省令に記載することとしてはどうか。

また、国の行政機関、地方公共団体又は関係機関は、上記の事務に該当しない場合であっても、番号に係る個人情報の提供を受けることについて著しく異常かつ激甚な非常災害への対応など特別の理由がある場合、第三者機関の許可を受ければ、他の機関に対し、情報連携基盤を通じてこれを提供するよう求めることができ、提供を求められた機関は、これを提供することができることを法律に明記することとしてはどうか。

(注1) 番号に係る個人情報を保有し、情報連携基盤を用いて情報の連携を行う、国の行政機関、地方公共団体及び関係機関をいう。

(注2) 番号に係る個人情報とは、情報保有機関において、番号に紐づけられて保有され、情報連携の対象となる個人情報を指し、具体的には、前記のとおり、法律等により特定されることとなる。

さらに、番号そのものについては、情報保有機関等において、少なくとも他の情報と容易に照合することができ、それにより特定の個人を識別することができる形態で保有されているものと考えられることから、それ自体が個人情報に該当し、それ自体が番号に係る個人情報に含まれる。

○ 上記の範囲外の情報連携については、情報連携基盤を通じて行えないようシステム上の措置を講じる。

## (2) 閲覧、データベース作成等の制限

○ 国の行政機関、地方公共団体又は関係機関の職員等は、その職務の用以外の用に供する目的で、番号に係る個人情報を閲覧し、その全部若しくは一部を他の記録媒体に複製し、又は番号に係る個人情報が記録されたファイル若しくはデータベースを作成してはならないこととすることが考えられる。

○ 地方公共団体の職員等は、その業務に関して知り得た番号に係る個人情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはならないこととすることが考えられる(国の行政機関、関係機関の職員等については、既に、行政機関個人情報保護法7条、独立行政法人等個人情報保護法8条に同様の規定あり。)

○ 法令に基づいて番号を取り扱うことが認められている民間事業者(注)又はその従業者等は、業務に関して知り得た番号に係る個人情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはならない

こととすることが考えられる。

法令に基づいて番号を取り扱うことが認められている民間事業者又はその従業者は、正当な理由なく、番号に係る個人情報が記録されたファイル若しくはデータベースを作成してはならないこととすることが考えられる。

(注) 現時点では、金融機関、健康保険組合及び源泉徴収義務者たる事業者等が考えられる。

- 本人確認など正当な目的で番号を知り得た事業者（法令に基づいて番号を取り扱うことが認められている民間事業者及びその従業者を除く。以下同じ。）(注)又はその従業者等は、番号に係る個人情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはならないこととすることが考えられる。

本人確認など正当な目的で番号を知り得た事業者又はその従業者等は、当該番号を文書、図画又は電磁的記録に記録して保有してはならないこととすることが考えられる。

(注) 「番号」が表面記載されているＩＣカードの提示を求めて本人確認を実施する民間事業者を指し、具体的には、携帯電話事業者やレンタルビデオ業者等がこれに該当すると考えられる。

- 国の行政機関、地方公共団体、関係機関及び法令に基づいて番号を取り扱うことが認められている民間事業者以外の者は、何人も、業として、番号の記録されたファイル又はデータベースを作成してはならないこととすることが考えられる。

### (3) 告知要求の制限

何人も不当な目的で番号の告知を求めてはならないこととすることが考えられる。

## 2 再委託等に関する規制

国の行政機関が個人情報の取扱いを委託する場合には、行政機関個人情報保護法６条２項に基づき、委託を受けた者についても、保有個人情報の漏えい、滅失又はき損の防止その他の保有個人情報の適切な管理のために必要な措置を講じなければならないとされており、地方公共団体及び関係機関においても、個人情報保護条例等に基づき、同様の措置が採られているものと考えられる。また、個人情報保護法の個人情報取扱事業者が個人データの取扱いを委託する場合には、個人情報保護法２２条に基づき、委託を受けた者に対する必要かつ適切な監督を行わなければならないこととされている。

番号に係る個人情報の取扱いについては、より厳格な規制が必要と考

えられることから、地方公共団体及び法令に基づいて番号を取り扱うことが認められている民間事業者等による委託について、現行の行政機関個人情報保護法又は個人情報保護法における規制と同様の規制を課すこととすることが考えられる。

また、現行法制上、規制が存しない再委託、再々委託等については、主に、以下のような規制を行うことが考えられる。

(1) 行政機関が保有する番号に係る個人情報の取扱いについて

- 国の行政機関、地方公共団体又は関係機関が保有する番号に係る個人情報の取扱いの再委託、再々委託等について、同行政機関、地方公共団体又は関係機関の許可を要することとすることが考えられる。
- 上記の再委託、再々委託等を受けた者は、番号に係る保有個人情報の漏えい、滅失又はき損の防止その他の番号に係る保有個人情報の適切な管理のために必要な措置を講じなければならないこととすることが考えられる。
- 上記の再委託、再々委託等における受託業務の従事者等(労働者派遣法に規定する派遣労働者を含む。以下同じ。)は、その職務の用以外の用に供する目的で、番号に係る個人情報を閲覧し、その全部若しくは一部を他の記録媒体に複製し、又は番号に係る個人情報が記録されたファイル若しくはデータベースを作成してはならないこととすることが考えられる。

また、上記の再委託、再々委託等における受託業務の従事者等は、その業務に関して知り得た番号に係る個人情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはならないこととすることが考えられる。

(2) 民間事業者が保有する番号に係る個人情報の取扱いについて

- 法令に基づいて番号を取り扱うことが認められている民間事業者が保有する番号に係る個人情報の取扱いの全部又は一部の再委託、再々委託等について、同事業者の明示的な許諾を要することとすることが考えられる。
- 上記の再委託、再々委託等を受けた者は、その取り扱う番号に係る個人データの漏えい、滅失又はき損の防止その他の個人情報の安全管理のために必要かつ適切な措置を講じなければならないこととすることが考えられる。
- 上記の再委託、再々委託等を受けた者又はその受託業務の従事者等は、業務に関して知り得た番号に係る個人情報の内容をみだりに他人

に知らせ、又は不当な目的に利用してはならないこととすることが考えられる。

上記の再委託、再々委託等を受けた者又はその受託業務の従事者等は、正当な理由なく、番号に係る個人情報記録されたファイル若しくはデータベースを作成してはならないこととすることが考えられる。

### **3 守秘義務**

- 番号を取り扱う事務に従事する国の行政機関、地方公共団体若しくは関係機関の職員等又は委託(再委託、再々委託等を含む。)を受けた者若しくはその受託業務の従事者等は、職務に関して知り得た番号に係る個人情報の電子計算機処理等に関する秘密を漏らしてはならないこととすることが考えられる。

## **第3 本人による個人情報へのアクセス及びアクセス記録の確認**

### **1 本人による個人情報へのアクセスについて**

- 国の行政機関が保有する番号に係る個人情報のうち、不開示情報に該当しないことが事前に確定でき、かつマイポータル上で開示を行っても事務の適正な遂行に支障を及ぼすおそれがない情報については、マイポータル上で開示できることとすることが考えられる。
- 地方公共団体が保有する番号に係る個人情報についても、不開示情報に該当しないことが事前に確定でき、かつマイポータル上で開示を行っても事務の適正な遂行に支障を及ぼすおそれがない情報については、当該地方公共団体の判断によりマイポータル上で開示できることとすることが考えられる。
- 上記に該当しない情報についても、マイポータル上で、本人が保有個人情報の開示請求手続を行えるようにすることが考えられる。また、訂正請求手続及び利用停止請求手続についてもマイポータル上で行えるようにすることが考えられる。
- マイポータルへのアクセスの際には、I Cカードを用いた公的個人認証を活用し、成りすましを防止することが考えられる。

### **2 アクセス記録の確認について**

#### (1) アクセス記録を確認できる対象範囲

- 情報連携基盤を通じた各府省、地方公共団体、関係機関による個人情報のやりとりについて、アクセス記録を確認できることとすることが考えられる。

#### (2) 除外事由

- 行政機関個人情報保護法 14 条及び個人情報保護法 25 条に規定される除外事由を踏まえ、必要に応じて除外事由を設けることとすることが考えられる。
- (3) 本人が確認できる項目
  - アクセスの日時、アクセスの主体、アクセスの対象となった情報の種類、情報連携の根拠のほか、情報連携基盤技術WGにおける検討を踏まえた項目を確認できることとすることが考えられる。
- (4) 確認方法
  - マイポータルを通じた確認のほか、情報連携基盤技術WGにおける検討を踏まえて、インターネット接続が困難な者等も確認できるようなその他の仕組みを設けることが考えられる。その場合も、マイポータルへのアクセス同様、成りすましを防止する本人認証の仕組みが必要と考えられる。

#### **第4 プライバシーに対する影響評価(P I A)等**

番号に係る個人情報適切に取り扱われているかを確認するためには、システム上においても個人情報保護に配慮した設計がきちんとなされているか確認する必要がある。そこで諸外国で採用されている P I A の手法を取り入れ、事前にかかる確認を行うことが考えられる。

一般的に、P I A とは、情報システムの導入等にあたりプライバシーへ及ぼす影響を事前に評価し、その保護のための措置を促す仕組みをいう。P I A の具体的な実施方法としては、個人情報の収集目的や収集方法、利用方法、管理方法などを検討し、そのシステムがプライバシーに配慮した設計となっているか確認することが考えられる。P I A の実施時期としては、プライバシーへ及ぼす影響に大幅な手戻りなく対応できるようにするため、システム設計の変更が可能であるシステム開発前が適当と一般的に考えられている。

##### **1 各機関に対する P I A**

- 国の行政機関は、番号に係る個人情報を扱うシステムの構築又は改修にあたり、P I A を実施し、その結果を第三者機関に報告し、その承認を受けること(法律による義務付け)とすることが考えられる。
- 第三者機関は、国の行政機関向けのガイドラインや地方公共団体又は民間事業者が P I A を実施する場合のガイドラインを作成するとともに、P I A の実施についての助言、指導等を行うことができることとすることが考えられる。

- 番号制度開始と同時に運用に供される情報連携基盤等のシステムについては、第三者機関が設立される予定の2014年1月より前に開発が行われることが想定されるため、第三者機関ではPIAを開発前に承認することができないこととなる。したがって、かかるシステムに対するPIAの承認は、PIAワーキンググループ(仮称)において行うこととしてどうか。

## **2 情報連携基盤の監視等**

第三者機関は、(立入検査やアクセスログの確認等により)情報連携基盤を随時監視することとすることが考えられる。

# **第5 第三者機関**

## **1 業務範囲**

### (1) 監督の対象とする機関等

国の行政機関のほか、地方公共団体、関係機関及び番号を取り扱う民間事業者(注)についても監督の対象とすることが考えられる。

(注) 法令に基づいて番号を取り扱うことが認められている民間事業者及び本人確認など正当な目的で番号を知り得た民間事業者を指す。

### (2) 監督の対象とする分野

当初は、上記機関等における社会保障及び税分野の番号に係る個人情報の取扱い等を監督の対象とし、将来的に対象の拡大を目指すこととすることが考えられる。

## **2 機能・権限**

最低限、次の(1)記載の機能・権限を有することとすることが考えられるほか、(2)記載の点について、更に検討を進める。

なお、機能・権限についても、必要に応じて、将来的に、更に必要なものがあるかについて検討を行う。

### (1) 最低限必要な機能・権限

#### ア (普及啓発)

番号制度に係る個人情報保護について普及啓発を行うこととすることが考えられる。

#### イ (番号に係る個人情報の取扱いに関する調査等)

監督対象機関等(注)に対し、番号に係る個人情報の取扱いに関する事務の実施状況について、定期的に又は必要に応じて調査を実施し、資料の提出及び説明を求めることができることとすることが考えられる。

(注) 第三者機関による監督の対象となる国の行政機関、地方公共団体、関係機関及び番号を取り扱う民間事業者をいう。以下、同じ。



ウ (苦情処理)

監督対象機関等による番号に係る個人情報取扱いに関する苦情について、相談に応じ、苦情に係る事情を調査することができることとすることが考えられる。

苦情の解決について必要があると認めるときは、監督対象機関等に対し、文書若しくは口頭による説明を求め、又は資料の提出を求めることができることとすることが考えられる。

エ (民間事業者等に対する立入検査等)

番号法(仮称)の施行に必要な限度において、番号を取り扱う民間事業者及び関係機関に対し、番号に係る個人情報取扱いに関し、報告させ、第三者機関の職員に、番号に係る個人情報取扱いに関係ある事務所、事業所その他その事業を行う場所に立ち入り、当該取扱いに関する帳簿、書類その他の物件を検査させ、又は関係者に質問させることができることとすることが考えられる。

オ (国の行政機関、地方公共団体に対する実地検査)

番号法(仮称)の施行に必要な限度において、国の行政機関及び地方公共団体の番号に係る個人情報(ただし、犯罪の予防、鎮圧又は捜査、公訴の維持、刑の執行その他の公共の安全と秩序の維持等一定の事由を目的として保有されている場合は除く。)の取扱いに関する事務の実施状況について実地の検査をすることができることとすることが考えられる。

カ (監督対象機関等に対する助言・指導)

監督対象機関等に対し、番号に係る個人情報取扱い状況や取扱いについてのルール(本人確認規定等)の策定などに関し必要な助言・指導をすることができることとすることが考えられる。

キ (監督対象機関等に対する勧告)

監督対象機関等が番号法(仮称)等の規定に違反した場合、監督対象機関等に対し、違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができることとすることが考えられる。

ク (民間事業者等に対する命令)

番号を取り扱う民間事業者及び関係機関が正当な理由がなく勧告に係る措置をとらなかったとき又は緊急に措置をとる必要があると認めるときは、当該民間事業者及び関係機関に対し、その勧告に係る措置又は必要な措置をとるべきことを命ずることができることとすることが考えられる。

ケ (地方公共団体に対する是正の要求の勧告)

第三者機関は、地方公共団体の番号に係る個人情報の取扱いに関する事務の処理が法令の規定に違反していると認めるとき、又は著しく適正を欠き、かつ、明らかに公益を害している認めるときは、内閣総理大臣(注)に対し、地方自治法245条の5に基づき当該地方公共団体に対して当該事務の処理について違反の是正又は改善のため必要な措置を講ずべきことを求めるよう勧告することができることとすることが考えられる。

(注) ここでいう内閣総理大臣とは、内閣府の長としての内閣総理大臣を指す。

コ (行政機関の長に対する措置要求)

内閣総理大臣は、番号に係る個人情報を保有する国の行政機関の長に対し、前記キの規定による措置が速やかに実施されることが必要であると認めるときは、当該措置の速やかな実施を求めることができることとすることが考えられる。

その上で、第三者機関は、国の行政機関において前記の措置が速やかに実施されることが必要であると認めるときは、内閣総理大臣に対し、当該国の行政機関の長に対して当該措置の速やかな実施を求めるよう勧告することができることとすることが考えられる。

サ (個人情報ファイルの保有等に関する事前通知)

国の行政機関が番号に係る個人情報ファイルを保有しようとするときは、当該行政機関の長は、あらかじめ、第三者機関に対し、行政機関個人情報保護法10条2項の各号に該当する場合のうち必要なものを除き、同条1項に掲げる事項を通知しなければならないこととすることが考えられる。

シ (情報連携基盤の監視等)

情報連携基盤及びそのインターフェース部分を、その稼働前に監査するとともに、(立入検査やアクセスログの確認等により)情報連携基盤を随時監視することとすることが考えられる。

ス (PIAの助言・指導・承認)

第三者機関は、国の行政機関がプライバシーに対する影響評価(PIA)を実施するに際し、助言・指導できるとともに、国の行政機関が提出するプライバシーに対する影響評価報告書を承認することができることとすることが考えられる。

セ (意見の陳述)

必要があると認めるときは、番号制度又は同制度における個人情報

保護のための方策に関する重要事項について、内閣総理大臣に意見を述べるができることとすることが考えられる。

ソ (国際協力)

(番号制度に係る)個人情報保護について国際協力を行うこととすることが考えられる。

(2) 更に検討すべき機能・権限

○ 課徴金等の制裁措置を実施できることとするか。

(→ 個人情報の不正利用等により、例えば、独禁法違反の事案のように、はく奪すべき程度の経済的利得が得られる事例は乏しいと思われることから、課徴金制度を設けることは現実的ではなく、他に実効性のある制裁措置は認めがたいのではないか?)

○ 救済申立ての手續に第三者機関が関わることとするか、関わることとする場合、どのように関わることとするか。

→ 番号に係る個人情報の不開示決定等に対する不服申立てについて、行政機関個人情報保護法42条の規定により諮問をした行政機関の長は、第三者機関に対し、諮問をした旨を通知しなければならないこととしてはどうか。

そして、第三者機関は、同通知を端緒とし、必要に応じて、上記権限等を用いて調査等を行い、行政機関の長に助言・指導等を行うこととしてはどうか。

### 3 法的形式と組織形態

○ 内閣府の外局として置かれる、いわゆる三条委員会（内閣府設置法49条1項）とすることが考えられる。

○ 委員長及び委員を国会の同意を得て内閣総理大臣が任命することとすることが考えられる。

○ 委員長は、会務を総理し、対外的にコミッショナーとして委員会を代表することとすることが考えられる。

委員長は、緊急に対処すべき事態が生じた場合、必要があれば、いつでも委員会を招集できることとすることが考えられる。

○ 第三者機関は、国に設置される機関であるが、地方公共団体も監督の対象にすることが考えられるため、委員の構成として、地方公共団体の関係者を含めることが考えられる。

○ 第三者機関は、毎年、業務の状況を国会に報告することとすることが考えられる。

## 第6 罰則

罰則の強化は、基本的に、以下の罰則を創設することにより対応することとすることが考えられる。

### 1 国の行政機関、地方公共団体、関係機関の職員等を主体とするもの

#### (1) 不正利用等

- 国の行政機関、地方公共団体若しくは関係機関の職員等又は受託業務(再委託、再々委託等における受託業務を含む。)の従事者等(以下「国の行政機関の職員等」という。)が、正当な理由がないのに、番号に係る個人情報のうち個人の秘密に属する事項が記録されたデータベース(その全部又は一部を複製し、又は加工したものを含む。)を提供した行為に対し、刑罰を科すこととすることが考えられる(行政機関個人情報保護法53条より罰則を引き上げることを検討)。

(注) 第2の1(1)記載のとおり、その具体的な範囲は法律で規定されることとなる。以下、同じ。

- 国の行政機関の職員等が、正当な理由がないのに、その業務に関して知り得た番号に係る保有個人情報を提供し、又は盗用した行為に対し、刑罰を科すこととすることが考えられる(行政機関個人情報保護法54条より罰則を引き上げることを検討)。

※ 上記二つの規定については、国外犯処罰規定を設けることとすることが考えられる。

#### (2) 不正取得等

- 国の行政機関、地方公共団体又は関係機関の職員がその職権を濫用して、専らその職務の用以外の用に供する目的で、番号に係る個人情報のうち個人の秘密に属する事項が記録された文書、図画又は電磁的記録を収集した行為に対し、刑罰を科すこととすることが考えられる(行政機関個人情報保護法55条より罰則を引き上げることを検討)。

※ 上記の規定については、国外犯処罰規定を設けることとすることが考えられる。

#### (3) その他

- 前記第2の3の規定に違反して秘密を漏らした者に対し、刑罰を科すこととすることが考えられる。

その際、国、地方、その他の機関間で情報連携が行われることにかんがみれば、前記第2の3の規定に違反して秘密を漏らした者に対する刑罰は、秘密を洩らした者の身分等にかかわらず同一の行為に対して同一の量刑とすることが考えられる。

(参考)

国家公務員法第 109 条（国家公務員の守秘義務違反に対する罰則）：「1 年以下の懲役又は 50 万円以下の罰金」

地方公務員法第 60 条（地方公務員の守秘義務違反に対する罰則）：「1 年以下の懲役又は 3 万円以下の罰金」

国税通則法第 126 条（国税職員の守秘義務違反に対する罰則）：「2 年以下の懲役又は 100 万円以下の罰金」

## 2 国の行政機関、地方公共団体の職員等以外の者も主体となり得るもの

### (1) 不正利用等

- 番号を取り扱う民間事業者若しくはその従業者等又は同事業者が保有する個人データの取扱いの全部若しくは一部の委託(再委託、再々委託を含む。以下同じ。)を受けた者又はその委託業務の従事者等(以下「番号を取り扱う民間事業者等」という。)が、正当な理由がないのに、番号に係る個人情報のうち個人の秘密に属する事項が記録されたデータベース(その全部又は一部を複製し、又は加工したものを含む。)を提供した行為に対し、刑罰を科すこととすることが考えられる。
- 番号を取り扱う民間事業者等が、正当な理由がないのに、その業務に関して知り得た番号に係る個人情報を提供し、又は盗用した行為に対し、刑罰を科すこととすることが考えられる。

※ 上記二つの規定については、国外犯処罰規定及び両罰規定を設けることとすることが考えられる。

### (2) 不正取得等

- 詐欺等行為(人を欺き、人に暴行を加え、又は人を脅迫する行為をいう。)又は管理侵害行為(財物の窃取、施設への侵入、不正アクセス行為(不正アクセス禁止法3条に規定する不正アクセス行為をいう。)その他の保有者の管理を害する行為をいう。)により、番号に係る個人情報を取得した者に対し、罰則を科すこととすることが考えられる(なお、同罪の法定刑によって更に対象となる行為を検討する必要あり。)

### (3) その他

- 法令に基づいて番号を取り扱うことが認められている民間事業者が保有する番号に係る個人情報ファイル又はデータベースに虚偽の記録をした者に対し、罰則を科すこととすることが考えられる。
- 前記第5の2(1)クの規定による命令に違反した者に対し、罰則を科すこととすることが考えられる。
- 前記第5の2(1)エの規定による報告をせず、若しくは虚偽の報告をし、又は立入検査を拒み、妨げ、若しくは忌避し、若しくは質問に対して陳述をせず、若しくは虚偽の陳述をした者に対し、罰則を科すこととすることが考えられる。

※ 上記二つの規定については、両罰規定を設けることとすることが考えられる。

### **3 第三者機関の委員長等の守秘義務違反**

- 第三者機関の委員長、委員又は職員等が職務上知り得た秘密を漏らした行為に対し、罰則を科すこととすることが考えられる(通常为国家公務員の守秘義務違反より罰則を引き上げることとすることが考えられる。)

## **第7 死者の識別情報**

国の行政機関、地方公共団体、関係機関又は法令に基づいて番号を取り扱うことが認められている民間事業者が、番号に係る死者の識別情報について、保存年限の規定等により保存している場合には、個人情報と同等の安全管理措置を講ずるものとして考えられる。

**社会保障・税に関わる番号制度における個人情報保護方策  
(本人確認・法人番号)**

1. 本人確認・認証、番号の真正性確保の論点

- 券面に番号を記載した公的個人認証に対応した顔写真付きのICカードを現行の住民基本台帳カードを改良の上、国民に配布し、対面での本人確認やオンラインでの認証に活用することが考えられる。
- 上記ICカードの配布方法については、その配布対象者が当該対象者であることを確認し、かつ、配布対象者に確実に配布されるよう法令で規定し、成りすまし防止を徹底する必要があると考えられる。
- 番号を取り扱う機関において、本人であることの証明手段がないまま、本人の申告による番号で本人確認が行われれば、成りすましの温床となり、制度そのものの根幹を揺るがしかねないことから、本人確認を行う際は、番号を本人確認の手段としない取り扱いとする必要がある。
- また、番号を取り扱う個別具体の手続きにおける本人確認のあり方については、その手続きごとに要求される本人確認の厳密さのレベルが異なることから、統一のルールを作成せず、引き続き個別のルールに基づき本人確認を行うことが考えられる。
- 上記ルールの作成・改定・運用等に当たっては、第三者機関が設置された後は、第三者機関が助言、指導等を行うことができることとすることが考えられる。
- なお、本人確認・認証が徹底されても、告知を受ける番号そのものの真正性を担保するものではないことから、法律に真正な番号を告知する義務を規定することが考えられる。
- 仮に真正性に疑わしい番号が判明した場合には、
  - ①番号を取り扱う国、地方公共団体は 付番機関又は付番機関から委託等を受けた機関に真正な番号を照会・確認を可能とすること、併せて、
  - ②真正な番号が判明した場合に、番号を取り扱う国、地方公共団体は、真正でない番号の削除又は真正な番号へ書き換えを可能とすることを法令等に規定することが考えられる。

2. 法人番号の論点

- 法人に関する情報については、現行の個人情報保護法制の射程外であり、法人番号に紐付けられる法人等の特定に必要な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)はいずれも公開されている情報であることから、法人番号については番号にかかる個人情報保護方策の射程外と考えられる。

# 本人確認

私はAです。



## 【本人確認】

- ①Aさんは架空の人物ではないか(実在性確認)
- ②Aさんは他人の成りすましではないか(同一性確認)



## 【本人確認の主な手法】

- (1)本人確認書類の提示等  
本人特定事項(氏名、生年月日、性別、住所、顔写真等)と申請書等との記載内容や本人の特徴とを照合
- (2)面談等による確認  
本人しか知れない事項を口頭質問し、確認者側の記録と照合
- (3)郵送を利用した確認  
証書などとの関係書類を転送不要郵便で送付し、返送されずに送達されたことをもって「同一性」を確認
- (4)公的個人認証の活用

○番号の有無で各種既存の手続きに求められる本人確認のレベルは変わらないか

○現に求められる本人確認のレベルは個別に定められている。

⇒ 従来どおり、個別法又は個別のルールで対応してはどうか

○仮に番号のみで本人確認が行われれば成りすましの温床になるおそれがある

⇒ 法律で明示的に禁止してはどうか



# 番号の真正性確保

私(A)の番号は1234です。



## 【本人確認】

- ①Aさんは架空の人物ではないか(実在性確認)
- ②Aさんは他人の成りすましではないか(同一性確認)

## 【真正性確認】

- ③Aさんの番号は1234で間違いないか



## 【真正性確認の主な手法】

- (1)窓口で本人による手続き  
券面に番号が記載された顔写真付きICカードを提示
- (2)オンラインによる手続き  
ICカードを活用
- (3)郵送や代理人による手続き  
本人確認+番号が記載されたICカードの券面の写し

○番号の真正性確保は本人確認・認証と不可分

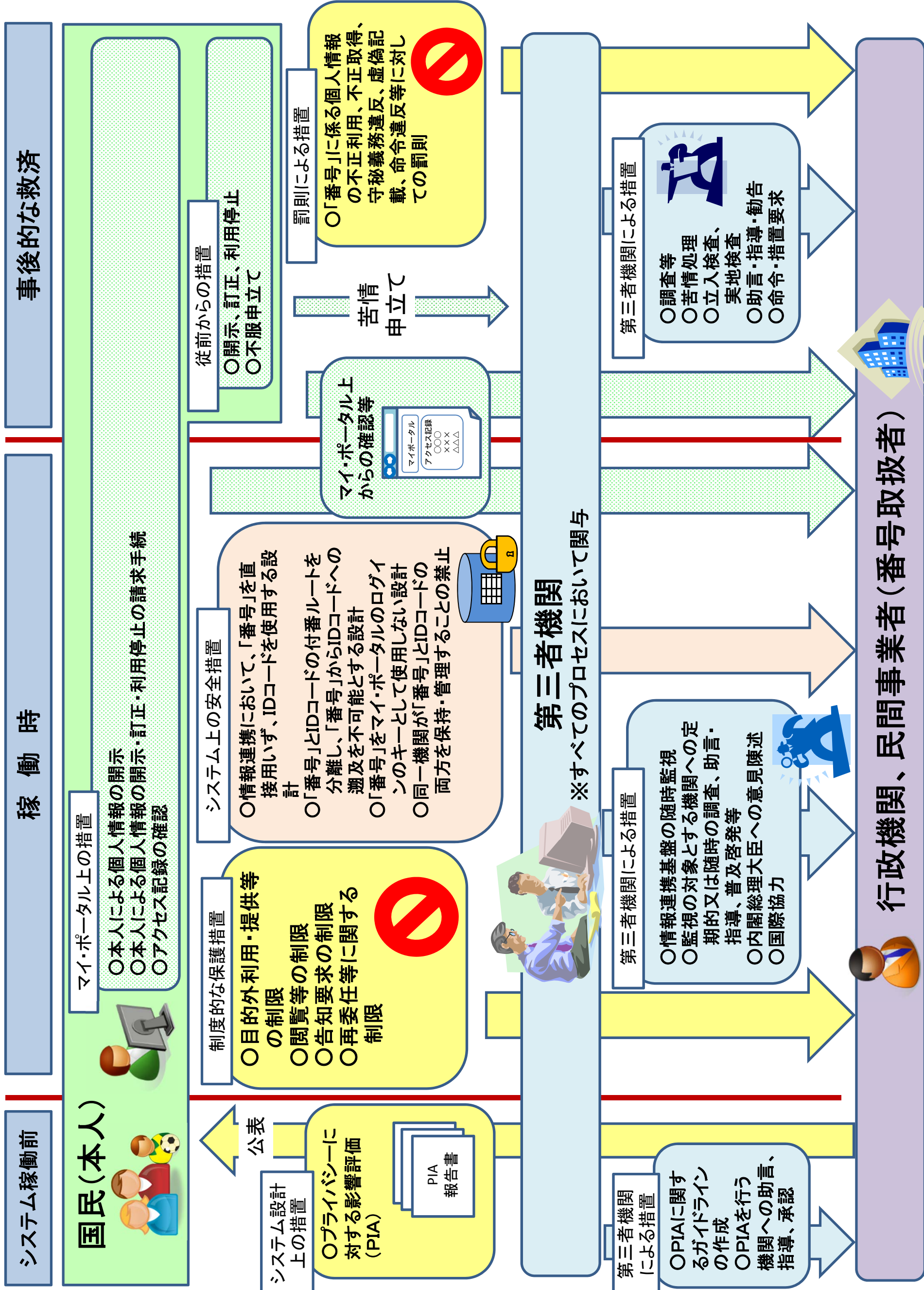
⇒ 本人確認と同様に、個別法又は個別のルールで対応してはどうか

○郵送や代理人による大量の手続きで逐一番号の真正性を担保することは困難

⇒ 国民の利便性にかんがみ郵送や代理人による手続きは存置せざるをえない。法律で虚偽の告知を禁止してはどうか。

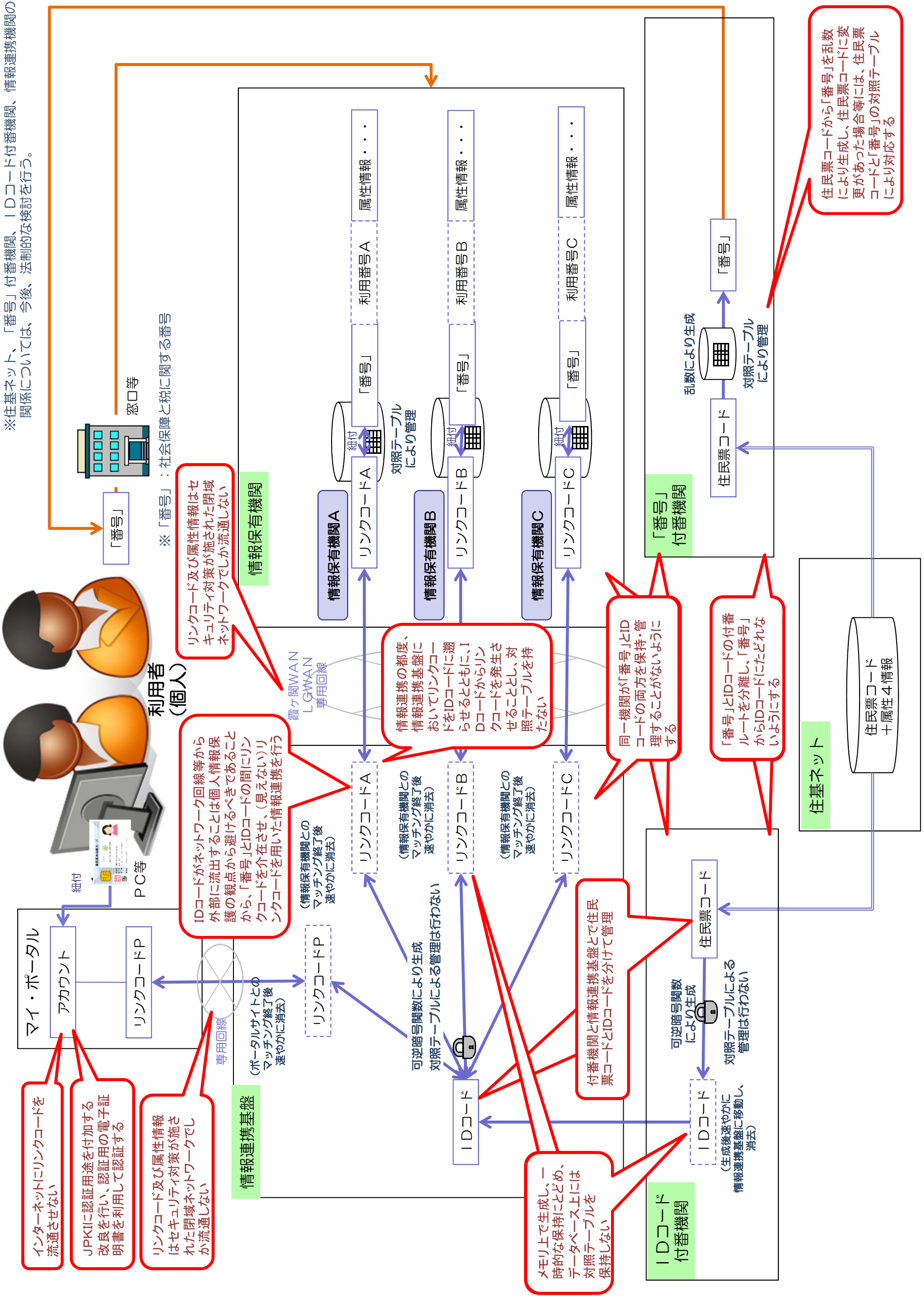
⇒ 仮に真正性に疑わしい番号が判明した場合、付番機関等に真正な番号を確認のうえ、真正でない番号の削除や真正な番号への書き換えを可能としてはどうか

# 社会保障・税に関わる番号制度における個人情報保護の方策



# 番号制度 番号連携イメージ

※住基ネット、「番号」付番機関、IDコード付番機関、情報連携機関の  
関係については、今後、法制的な検討を行う。



## 社会保障・税に関わる番号制度及び国民ID制度における 情報連携基盤技術の骨格案(その1)

平成23年3月4日  
情報連携基盤技術ワーキング・グループ

### 第1 個人に対する付番、番号連携及び情報連携

#### 1. 基本的な考え方

- (1) 「番号制度構築に当たっては、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、情報連携基盤がデータのやり取りの承認やアクセス記録の保持を行い、国民が自己情報へのアクセス記録を確認できるようにするなど、個人情報保護に十分配慮した仕組みとする」(基本方針P. 6) 必要がある。
- (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(以下「住基ネット」という。)に係る最高裁合憲判決(最判平成20年3月6日)で示された個人情報を一元的に管理することができる機関又は主体が存在しないこと、何人も個人に関する情報をみだりに第三者に開示又は公表されない自由を有することなどの判断枠組みに適合した形で個人情報を取り扱うシステムとすることが必要である。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、取り扱う個人情報が、住基ネットの本人確認情報よりも格段に秘匿性の高い社会保障・税に係る情報を中心としており、かつ、住基ネットが行わないこととしているデータマッチングを行うこととするものであることから、より一層高度の安全性を確保することが求められるのではないか。

#### 2. 情報連携の原則

##### (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、異なる情報保有機関等が有する同一人の情報を連携するためには、当該個人を特定する共通の識別子(以下「IDコード」という。)を用いることとなるが、「番号」は「民一民一官」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ないのではないか。

##### (2) 「見えない」IDコードを用いる情報連携

したがって、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、従来の電子行政タスクフォースにおける国民ID制度の検討においては、①「住民票コード」又は②「住民票コードに対応した新しいコード」の2案が選択肢として示されていたが、個人情報保護の観点をより重視し、IDコードを認知できる者を極力最小限とすることが必要であるということを前提とすれば、住民票に記載されている住民票コードではなく、②「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。

### (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

IDコードは情報連携基盤において管理されることとなるが、仮にこれを情報保有機関も共有し、それで情報連携基盤にアクセスさせることとすると、万一漏洩した際にはその影響が他の情報保有機関にも波及する可能性がある。そこで、「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別の「見えない」コード（以下「リンクコード」という。）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。

## 3. 付番と番号管理について

### (1) 「番号」とIDコード・リンクコードの付番のあり方

前述の最高裁判決で指摘された個人情報の一元管理を避け、「番号」を含めた「見える」利用番号から情報連携に用いるIDコードに直接アクセスできないようにするという観点から、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。

### (2) IDコード及びリンクコードの生成方法

異なる情報保有機関同士の情報連携を図るためには、それぞれの情報保有機関ごとに付与されたリンクコードからIDコードに遡ることができ、また、IDコードからリンクコードに遡ることができることとする必要がある。このためには、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（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）又は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）が考えられる。コード変換テーブル方

式は、同一の機関において住民票コードとIDコードのリストの一元管理を行う必要があり、その場合、万一漏洩した際の影響範囲が広がる可能性があることから、可逆暗号方式を採用すべきではないか。

### (3) 「番号」の生成方法

3.(1)で述べた観点から、住民票コードから見える「番号」を生成させる方法は3.(2)とは異なる方法とすべきであり、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。

### (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コードのみを保有することとし、リンクコードは情報連携ごとに可逆暗号で生成して、連携終了後直ちに消去することとすべきではないか。

### (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、個人が行政機関等の窓口や申告書への記入等の方法により使用されるものであるため、「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。

### (6) 「番号」とIDコード・リンクコードの変更可能性

住民票コードについて個人による変更請求が認められており、かつ、「番号」については個人にも通知され、見える番号として様々な手続に用いられるものであることから、その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・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、変更請求は想定されない。しかしながら、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。

#### (7) 分野別に考慮すべき事項とリンクコードの付与単位について

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（例：地方税法第45条の3では、前年分の所得税について所得税法上の確定申告書を提出した場合には、原則として地方税法上の申告書が提出されたものとみなす仕組みを採用）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、年金、医療、福祉、介護、労働保険の各社会保障分野については、基本方針において、本ワーキング・グループ及び個人情報ワーキング・グループによる検討経過を踏まえ、社会保障分野における具体的な措置について検討するサブ・ワーキング・グループにおいて検討が進められることとされている。

その際には、特に各社会保障分野においては、よりセンシティブな個人情報が含まれていることや医療機関や薬局等情報保有機関が極めて多数に上る分野が存在すること等に鑑み、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、そ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。

## 4. 番号連携について

### (1) 番号連携の前提としての紐付けの必要性

リンクコードと「番号」及びその他の利用番号（以下「番号」等という。）は、セキュリティの観点から論理的関連性を持たないものとなる。これを前提として、2. 及び3. で述べた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（対象者についての「番号」等と属性情報等から構成されたデータベース）に紐付けられることが必要となる。

これによって、各情報保有機関の持つ属性情報が、リンクコード・IDコ

ードを通じて他の情報保有機関の持つ属性情報と連携されることとなる。

#### (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利用番号の属性情報として管理される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ある。

そのためには、情報保有機関の責任で、情報保有機関の保有する4情報を最新のものとするのが不可欠であり、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と。

#### (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.(2)により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と。

#### (4) 番号連携の流れ

3.(2)により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、4.(1)～(3)によって、各情報保有機関においてリンクコードと「番号」等と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。

### 5. 情報連携について

#### (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

基本方針においては、「当面の情報連携の範囲は、年金、医療、福祉、介護、労働保険の各社会保障分野と国税・地方税の各税務分野とする」とされているが、1.(2)に述べた観点から、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と。

#### (2) 情報連携基盤における情報連携の承認

5.(1)により定められた情報保有機関及び情報連携対象個人情報のリス



トの中に、照会元情報保有機関による情報連携の照会が含まれることが情報連携の条件となるが、そ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)リンクコードーIDコードー(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。

### (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。

### (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、4.(3)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、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。

② 続いて、情報連携基盤においては、5.(2)に述べたように、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)リンクコードーIDコードー(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。

- 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、6. で述べるように、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。

## 6. アクセスログの保存及び提供

### (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としては、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かつ広範囲なものとして設定すべきではないか。

### (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。

そこで、例えば、6.(1)に示したリストの中では、5.(4)③の考え方も踏まえ、①～⑥までは情報連携基盤で、⑦・⑨・⑪・⑫については照会元情報保有機関で、⑧・⑩・⑫については照会先情報保有機関で保存をすることが考えられるのではないか。

### (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に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。

### (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6.(1)の⑪・⑫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。

### (5) 第三者機関によるアクセスログの閲覧・分析

第三者機関の役割は、個人情報保護ワーキング・グループにおいて検討されているところであるが、情報連携に関しては、アクセスログの閲覧・分析等により、情報連携基盤及び情報保有機関の情報連携に係る個人情報の取扱いを監視・調査する権限等を有することが想定される。

したがって、6.(1)の考え方を踏まえ、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。

## 7. 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

### (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持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。

### (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

情報連携に関わる業務分野について、各情報保有機関が持つ既存システムには様々な種類があり、これらを直接7.(1)に例示したような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と。

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と。

## 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と。

## 第2 個人認証とマイポータル・ICカード等の活用

## 第3 法人に対する付番

## 第4 その他

## 社会保障・税に関わる番号制度及び国民ID制度における 情報連携基盤技術の骨格案(その2)

平成23年3月23日  
情報連携基盤技術ワーキング・グループ

### 第2 個人の本人確認(マイポータル・ICカード等)

#### 1. 基本的考え方

##### (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

「当面の情報連携の範囲は、年金、医療、福祉、介護、労働保険の各社会保障分野と国税・地方税の各税務分野とする」(基本方針P.6)ことから、マイ・ポータル等は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)。

##### (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

一方、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。

具体的には、マイ・ポータルにログインするために、公的個人認証サービスに認証用途を付加すること、電子証明書の有効期間の延長など公的個人認証サービスの利便性を高めること、法令等で「番号」を確認することが認められている民間事業者が電子的に本人確認を行うことができるよう署名検証者を民間事業者に拡大すること、住民基本台帳カードの券面に「番号」を記載することを検討すること等が考えられるのではないかと。

## 2. マイ・ポータルの利用

### (1) マイ・ポータルの機能

マイ・ポータルには、次の4つの機能を持たせることとしてはどうか。

自己情報へのアクセスログを確認する機能

各情報保有機関が保有する自己情報を確認する機能

電子申請を経由する機能(ワンストップサービス)

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)

### (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(マイ・ポータルの利用者に情報提供するためのシステム上の作業領域で、個人とはリンクコードのみで紐付けられ管理されているもの。)を開設する((3)参照)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極力蓄積しないように、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。

### (3) マイ・ポータルにログインするための認証

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、情報連携のための共通の識別子であるIDコードやリンクコードがインターネット上を流通することになり、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」番号であり、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(4.(1)参照)、署名用の電子証明書とは別に認証用の電子証明書を発行することとし、認証用の電子証明書のシリアル番号(以下「認証用シリアル番号」という。)を、次の観点から、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。

(a) 「番号」やIDコードとは論理的な関連性はなく、仮に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こと

(b) 電子証明書等は暗号化して送付するが、仮に認証用シリアル番号が盗まれたとしても、秘密鍵自体は本人しか有しないため、当該認

証用シリアル番号だけでは、認証することはできないこと

- (c) 現行の公的個人認証サービスの署名用の電子証明書のシリアル番号（以下「署名用シリアル番号」という。）と同様に、認証用シリアル番号は一意性があるものとするができること

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、次の対策を講じるべきではないか。

- (a) 現行の公的個人認証サービスと同様に、認証用途以外の目的で使用するを法律上明確に禁止すること
- (b) 認証用シリアル番号は認証局（公的個人認証サービスの電子証明書を発行する機関をいう。以下同じ。）においてのみリンクコードと紐付けが行われることとし、マイ・ポータル運営機関の利用者フォルダや情報保有機関の管理する各利用番号と認証用シリアル番号との紐付けは行わないこと
- (c) 電子証明書が本人のものであるかどうかは認証局に問い合わせることとし、当該認証局はマイ・ポータル運営機関又は各情報保有機関に対し、情報連携基盤を通じて、当該者のリンクコードを伝達する仕組みとすること

#### 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。

#### 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）
- ）利用者は、ＩＣカードをリーダーライタにセットし、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（４情報が含まれている。４．（４）参照）等を利用して、利用者フォルダ取得の電子申請を行う。
- ）マイ・ポータル運営機関は、利用者の電子証明書を付した電子申請を受領し、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。

- ) 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。
- ) 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。
- ) 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。

(b) ログイン（アクセスする都度の対応）

- ) 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カードをリーダーライタにセットし、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（4.参照）を利用して、ログイン要求を行う。
- ) 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。
- ) 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。
- ) 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。
- ) 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。
- ) 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（2.(3)参照）を、情報連携基盤に振り出す。
- ) 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。
- ) 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。
- ) 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。

(4) 自己情報へのアクセスログを確認する機能

マイ・ポータルで確認できるアクセスログについては、第1の6.のと



おりである。

アクセスログを確認する手順としては次のとおりとはどうか。

）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。

）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、情報連携基盤に問い合わせをする。

）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。

）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。

#### (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も検討してはどうか。この際、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はどうか。

）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。

）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。

）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。

）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。

）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。

）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。

( 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、申請書の文書の真正性を推定する効果が働くことや改ざんを防止する必要があることから、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、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。

なお、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。

( 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。

) 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。

) 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。

) 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。

) 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。

( 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。

### 3．窓口等における本人確認

法令等で「番号」を確認することが認められている機関は、書面又は電子的な方法により、本人確認をした上で、「番号」を確認する必要がある。

#### (1) 書面により本人確認及び「番号」確認を行う場合

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。

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し利用できる仕組みとしてはどうか（5.(4)参照）。

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。

#### (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」を取り出す仕組みを検討してはどうか。

### 4．公的個人認証サービスの改良

#### (1) 認証用途の付加の必要性

社会保障・税に関わる番号制度及び国民ID制度において求められる本人確認は、文書を伴わないアクセスであり、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。

なお、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。

( 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。

( 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、同様の方法とするべきではないか。

( 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。

( 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、現在３年間とされているところであるが、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。

現在、失効した電子証明書を更新する場合には、利用者は、住所地市町村の窓口に出向き、本人確認を受けた上で電子証明書の発行を申請する必要があるが、利用者の利便性を高めるため、利用者がオンラインで電子証明書を更新できる仕組みを検討してはどうか。

( 6 ) ＩＣカード以外のデバイス

携帯電話等ＩＣカード以外の媒体については、それのみでは当該媒体が真に本人のものであるかどうかの確証が得られないことから、ＩＣカード以外の媒体の利用を希望する場合には、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。

#### (7) 署名検証者の拡大等

3.(2)のとおり、法令等で「番号」を確認することが認められている民間事業者が電子的に本人確認を行えるようにするため、また、将来的に、情報連携する範囲を民間事業者に拡大するためには、民間事業者において、より安全に本人確認を行う取引環境を整えることが前提となることから、署名用途及び認証用途に係る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、署名用シリアル番号や認証用シリアル番号のセキュリティを確保した上で、検証者側のコスト負担を軽減するため、民間事業者が共同で検証を行う仕組みも検討してはどうか。

### 5. ICカード（住民基本台帳カードの改良）

#### (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等に対しては、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。

#### (2) ICカードの発行

ICカードの発行にあたっては、現在の住民基本台帳カードが、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、同様の方法とすべきではないか。

また、ICカードの機能については、現行の住民基本台帳カードが、住民が転入届の特例を受け、全国の行政機関で本人確認を行い、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カードは当該機能も併せて持つこととしてはどうか。

#### (3) 券面記載事項

現行の住民基本台帳カードについては、タイプA（氏名のみ、顔写真無し）及びタイプB（4情報、顔写真あり）があるが、取引における本

人確認を厳格に行うため、ICカードは、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、IC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。

IC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。

#### (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ェ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ェアについては、IC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。

### 第3 法人に対する付番

#### 1. 付番対象

基本方針においては、「法人等に対して付番する「番号」については、商業・法人登記の申請に係る会社法人等番号を活用した番号とする。会社法人等番号を有しない法人等に対して付番する「番号」については、今後検討する」(基本方針p.5 1.(1))とされている。

会社法人等番号は、商業・法人登記の申請にかかる会社法人等に対して各法務局から付与される番号であるが、登記を要しない法人・国・地方公共団体・人格なき社団等など、一部の法人等に対しては付与されていない。

このため、付番対象は、会社法人等番号を有する法人本店のほか、登記を要しない法人、国・地方公共団体、国税・地方税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。

なお、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。

## 2．登記のない法人等に対する付番方法

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。

## 3．番号の変更

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。

## 4．番号の通知

法人は公的認証の利用又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。

## 5．検索及び閲覧

「法人等に対して付番する「番号」は、広く一般に公開されるものであり、自由に流通させることができ、官民を問わず様々な用途で利活用するものとする。」(基本方針p.5 1.(1))とされている。

このため、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。

## 第4 その他

### 1．企業コードについて

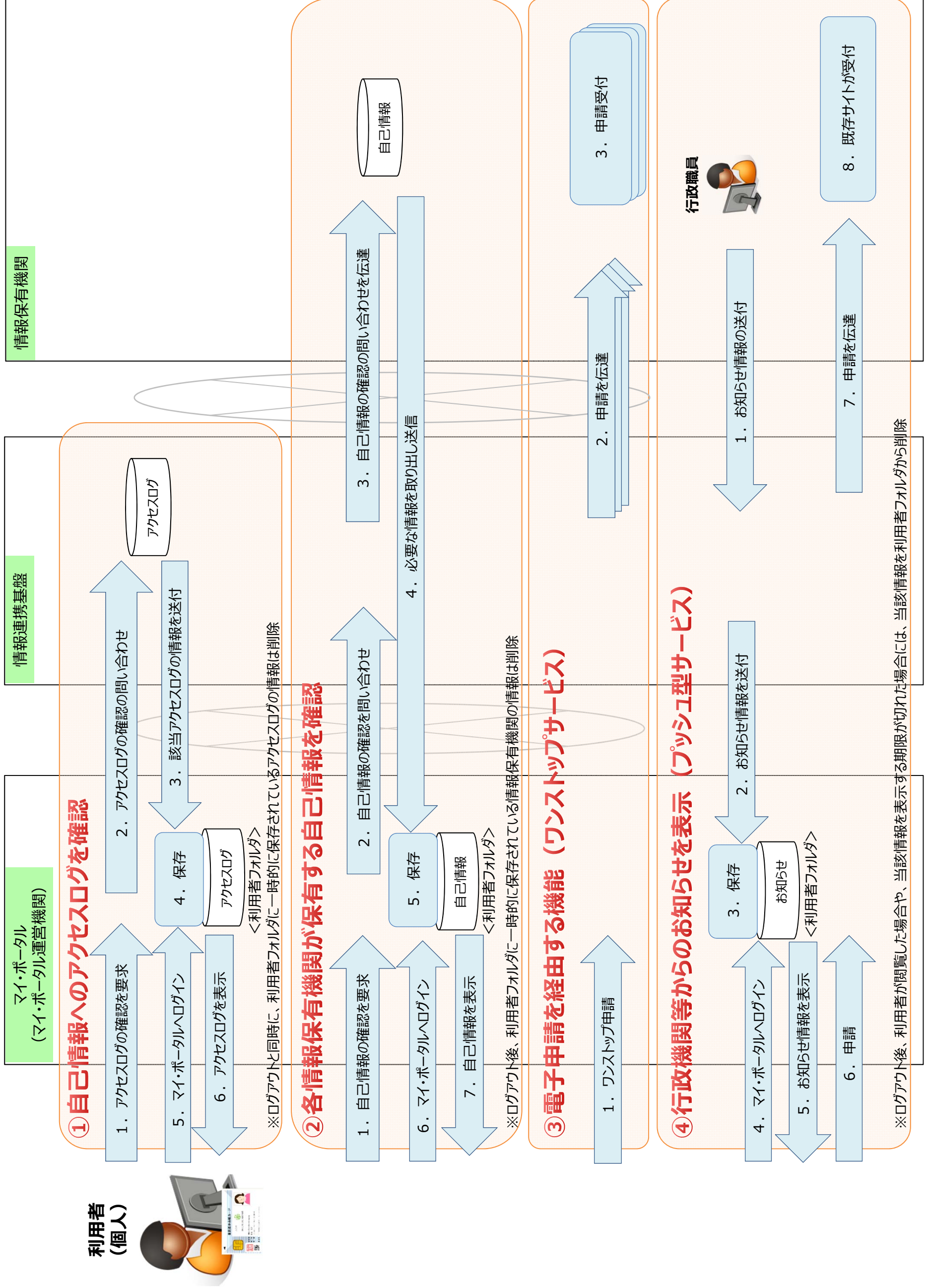
IT戦略本部電子行政に関するタスクフォース（以下「タスクフォース」という。）においては、行政の電子化によって企業の利便性の向上や行政の業務効率の向上を図る観点から、企業コードの整備及びその活用のための施策について検討している。

今後の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と。

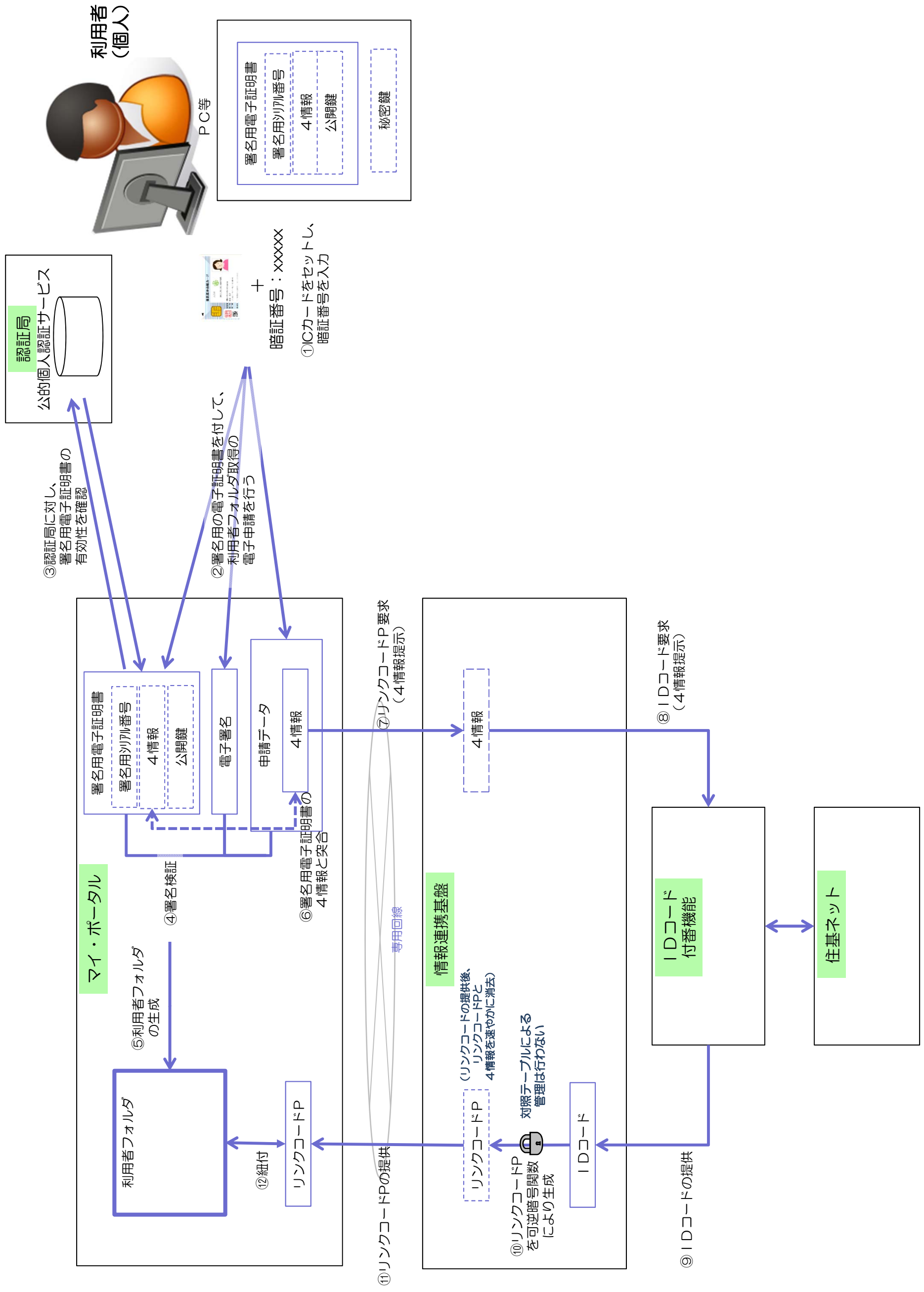
また、企業コードには、網羅性（法人等に対して網羅的に付与）、一意性（法人等に対して重複なく付与）、一貫性（法人等の商号変更、移転等が生じてもコードは不変）、非再利用性（法人等が消滅しコードに空きが生じても他に割当しない）、開放性（誰でも利用可能）、参照可能性（コードの公開）、非譲渡可能性（企業の所有権や商号が譲渡可能されても、コードは譲渡されない）等の性質が備わっていることが望ましいと考えられるが、上記のような施策を推進するに当たっては、番号制度により付番される法人番号を活用し、その上で、求められる性質を満たすための仕組みをタスクフォースにおいて検討することが考えられるのではないかと。



## 第2 2. (1) マイ・ポータル機能



## 第2 2. (3) ③マイ・ポータルへのログインの手順 (a) 利用者フォルダ取得のフロー



## 第2 2.(3) ④ マイ・ポータルへのログインの手順 (b)ログインフロー

