

総務委員会資料

陳情の審査

陳情第23号 マイナンバー制度実施の中止または延期を求める
国への意見書提出を求める陳情

資料1 「社会保障・税番号制度 概要資料（平成
27年8月版）」から抜粋

資料2 「中小規模事業者向け はじめてのマイナン
バーガイドライン」から抜粋

資料3 個人情報保護に関する法律及び行政手続
における特定の個人を識別するための番号の
利用等に関する法律の一部を改正する法律（改
正概要資料）から抜粋

平成27年10月7日

総 務 局

マイナンバー制度における安心・安全の確保

資料1

マイナンバー制度に対する国民の懸念

- ・ 個人番号を用いた個人情報の追跡・名寄せ・突合が行われ、集積・集約された**個人情報**が外部に**漏えい**するのではないかと懸念。
- ・ 個人番号の不正利用等（例：他人の個人番号を用いた**成りすまし**）等により財産その他の被害を負うのではないかと懸念。
- ・ 国家により個人の様々な個人情報が個人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懸念

制度面における保護措置

- ① 本人確認措置（個人番号の確認・身元（実存）の確認）（番号法第16条）
- ② 番号法の規定によるものを除き、特定個人情報（マイナンバーをその内容に含む個人情報）の収集・保管、特定個人情報ファイルの作成を禁止（番号法第20条、第28条）
- ③ 特定個人情報保護委員会による監視・監督（番号法第50条～第52条）
- ④ 罰則の強化（番号法第67条～第77条）
- ⑤ マイナポータルによる情報提供等記録の確認（番号法附則第6条第5項）

システム面における保護措置

- ① 個人情報を一元的に管理せず、分散管理を実施
- ② 個人番号を直接用いず、符号を用いた情報連携を実施
- ③ アクセス制御により、アクセスできる人の制限・管理を実施
- ④ 通信の暗号化を実施

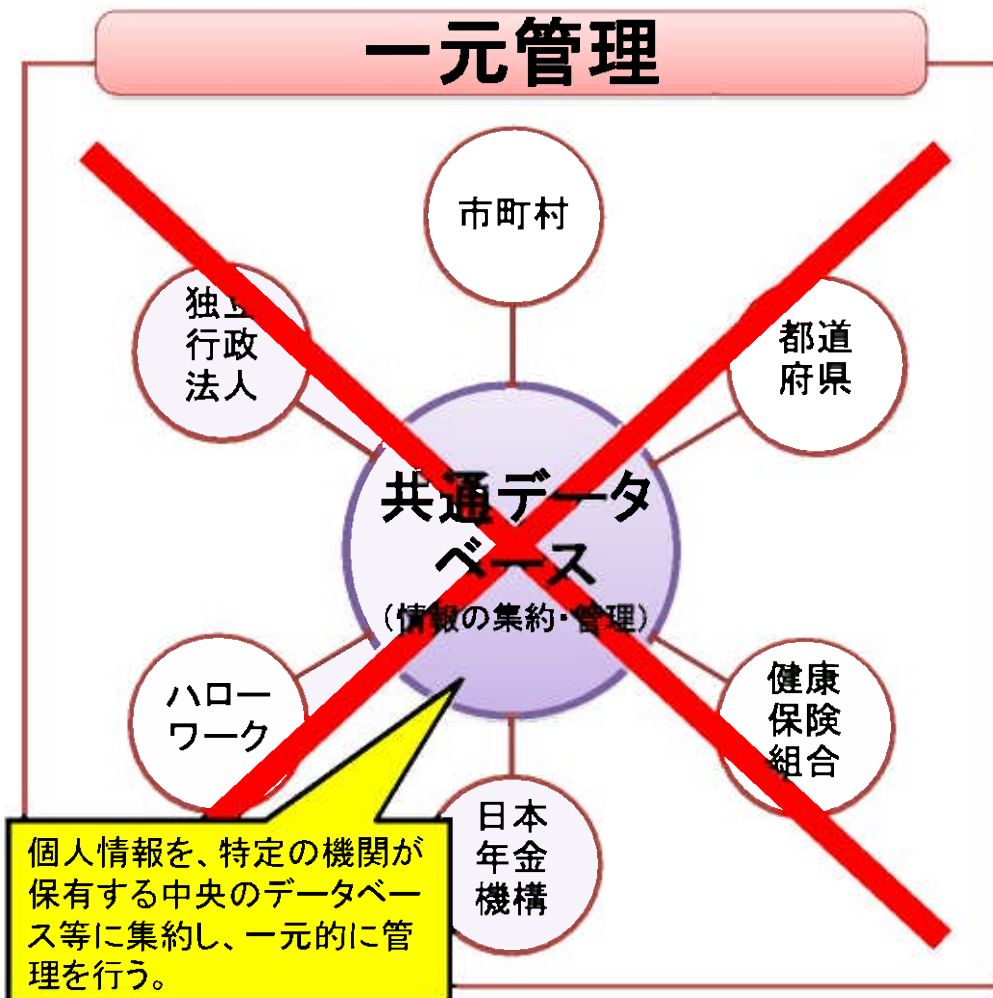


マイナンバー制度における個人情報の管理（分散管理）

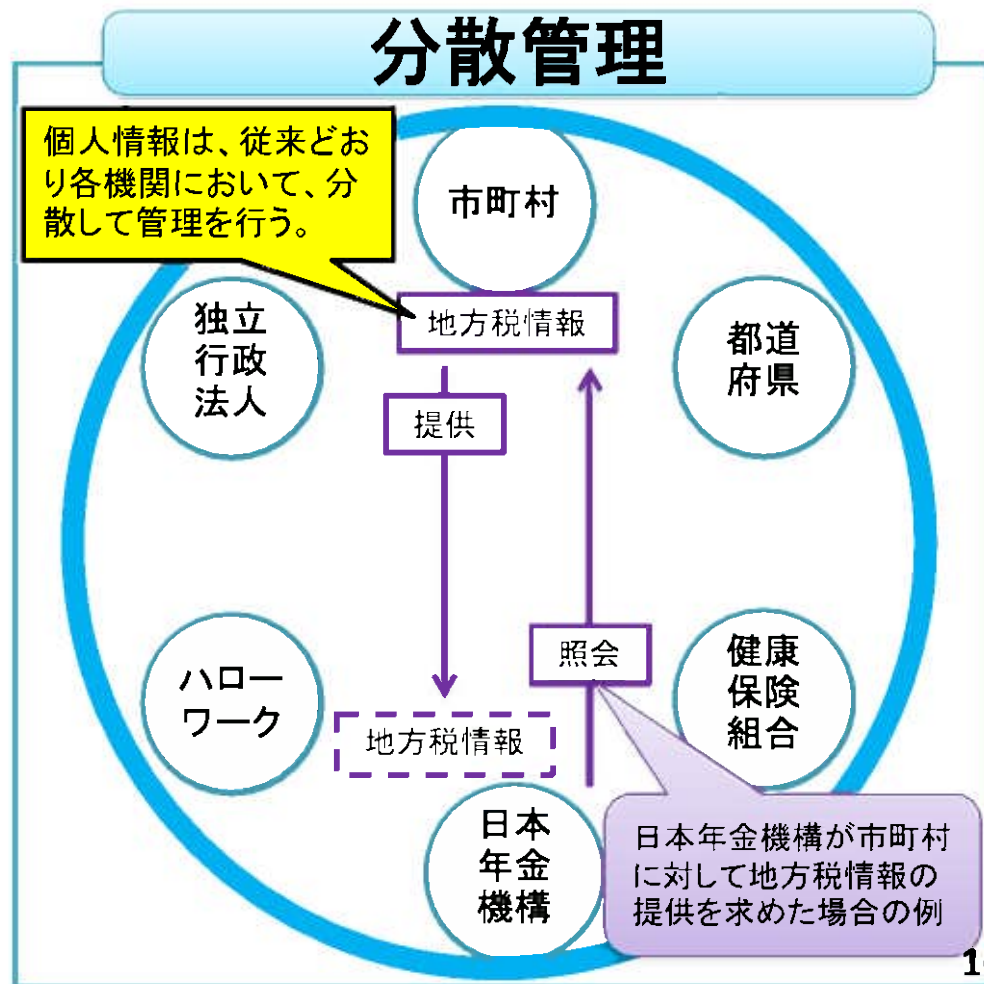
✕ 番号制度が導入されることで、各行政機関等が保有している個人情報を**特定の機関に集約**し、その集約した個人情報を各行政機関が閲覧することができる『一元管理』の方法をとるものではない。

○ 番号制度が導入されても、従来どおり個人情報は**各行政機関等が保有**し、他の機関の個人情報が必要となった場合には、番号法別表第二で定められるものにより、情報提供ネットワークシステムを使用して、情報の照会・提供を行うことができる『分散管理』の方法をとるものである。

一元管理



分散管理



個人番号・特定個人情報を保護するために、**必要かつ適切な安全管理措置**が必要です。

資料2



安全管理措置

個人番号・特定個人情報の**漏えい、滅失又は毀損の防止その他の適切な管理のために、必要かつ適切な安全管理措置**を講じなければなりません。また、**従業者に対する必要かつ適切な監督**も行わなければなりません。



- 中小規模事業者に対する特例を設けることにより、実務への影響を配慮しています。
- 中小規模事業者における対応方法は、参考資料（6ページ以降）を参照してください。



【中小規模事業者とは】

事業者のうち従業員の数が100人以下の事業者であって、次に掲げる事業者を除く事業者をいいます。

- ・個人番号利用事務実施者
- ・委託に基づいて個人番号関係事務又は個人番号利用事務を業務として行う事業者
- ・金融分野（金融庁作成の「金融分野における個人情報保護に関するガイドライン」第1条第1項に定義される金融分野）の事業者
- ・個人情報取扱事業者

「（別添）特定個人情報に関する安全管理措置」の中小規模事業者における対応方法（抜粋）

安全管理措置は、事業者の規模及び特定個人情報等を取り扱う事務の特性等により、適切な手法を採用してください。

中小規模事業者における対応方法	？ ヒント ？
<p>A 基本方針の策定 特定個人情報等の適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。</p>	<p>➤ 基本方針の策定は義務ではありませんが、作ってあれば従業員の教育に役立ちます。</p>
<p>B 取扱規程等の策定 ○ 特定個人情報等の取扱い等を明確化する。 ○ 事務取扱担当者が変更となった場合、確実な引継ぎを行い、責任ある立場の者が確認する。</p>	<p>➤ 業務マニュアル、業務フロー図、チェックリスト等に、マイナンバーの取扱いを加えることも考えられます。</p>
<p>C 組織的安全管理措置 事業者は、特定個人情報等の適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。</p>	
<p>a 組織体制の整備 ○ 事務取扱担当者が複数いる場合、責任者と事務取扱担当者を区分することが望ましい。</p>	<p>➤ けん制効果が期待できる方法です。</p>
<p>b 取扱規程等に基づく運用 c 取扱状況を確認する手段の整備 ○ 特定個人情報等の取扱状況の分かる記録を保存する。</p>	<p>➤ 例えば、次のような方法が考えられます。 ・業務日誌等において、特定個人情報等の入手・廃棄、源泉徴収票の作成日、本人への交付日、税務署への提出日等の、特定個人情報等の取扱い状況等を記録する。 ・取扱規程、事務リスト等に基づくチェックリストを利用して事務を行い、その記入済みのチェックリストを保存する。</p>
<p>d 情報漏えい等事案に対応する体制の整備 ○ 情報漏えい等の事案の発生等に備え、従業者から責任ある立場の者に対する報告連絡体制等をあらかじめ確認しておく。</p>	<p>➤ 業務遂行の基本、「ほうれんそう」（報告・連絡・相談）を確認しましょう。</p>
<p>e 取扱状況の把握及び安全管理措置の見直し ○ 責任ある立場の者が、特定個人情報等の取扱状況について、定期的に点検を行う。</p>	<p>➤ 事業者のリスクを減らすための方策です。</p>
<p>D 人的安全管理措置 事業者は、特定個人情報等の適正な取扱いのために、次に掲げる人的安全管理措置を講じなければならない。</p>	
<p>a 事務取扱担当者の監督 事業者は、特定個人情報等が取扱規程等に基づき適正に取り扱われるよう、事務取扱担当者に対して必要かつ適切な監督を行う。</p>	<p>➤ 従業員の監督・教育は、事業者の基本です。 従業員にマイナンバー4 簡条を徹底しましょう（1 ページ参照）。</p>
<p>b 事務取扱担当者の教育 事業者は、事務取扱担当者に、特定個人情報等の適正な取扱いを周知徹底するとともに適切な教育を行う。</p>	

中小規模事業者における対応方法	？ ヒント ？
<p>E 物理的安全管理措置 事業者は、特定個人情報等の適正な取扱いのために、次に掲げる物理的安全管理措置を講じなければならない。</p>	
<p>a 特定個人情報等を取り扱う区域の管理 特定個人情報等の情報漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）及び特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にし、物理的な安全管理措置を講ずる。</p>	<p>➤ 事業者の規模及び特定個人情報等を取り扱う事務の特性等によりますが、例えば、壁又は間仕切り等の設置及び覗き見されない場所等の座席配置の工夫等が考えられます。</p>
<p>b 機器及び電子媒体等の盗難等の防止 管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。</p>	<p>➤ 事業者の規模及び特定個人情報等を取り扱う事務の特性等によりますが、例えば、書類等を盗まれないように書庫等のカギを閉める等が考えられます。</p>
<p>c 電子媒体等を持ち出す場合の漏えい等の防止 ○ 特定個人情報等が記録された電子媒体又は書類等を持ち出す場合、パスワードの設定、封筒に封入し鞆に入れて搬送する等、紛失・盗難等を防ぐための安全な方を講ずる。</p>	<p>➤ 置き忘れ等にも気を付けましょう。</p>
<p>d 個人番号の削除、機器及び電子媒体等の廃棄 ○ 特定個人情報等を削除・廃棄したことを、責任ある立場の者が確認する。</p>	<p>➤ 事業者のリスクを減らすために大切です。</p>
<p>F 技術的安全管理措置 事業者は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。</p>	
<p>a アクセス制御 b アクセス者の識別と認証 ○ 特定個人情報等を取り扱う機器を特定し、その機器を取り扱う事務取扱担当者を限定することが望ましい。 ○ 機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、情報システムを取り扱う事務取扱担当者を限定することが望ましい。</p>	<p>➤ 担当者以外の者に勝手に見られないようにしましょう。</p>
<p>c 外部からの不正アクセス等の防止 情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用する。</p>	<p>➤ インターネットにつながっているパソコンで作業を行う場合の対策です。例えば、次のような方法が考えられます。 ・ウイルス対策ソフトウェア等を導入する。 ・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態にする。</p>
<p>d 情報漏えい等の防止 特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる。</p>	<p>➤ インターネットにつながっているパソコンで作業を行う場合の対策です。例えば、データの暗号化又はパスワードによる保護等が考えられます。</p>

マイナンバーの利用範囲の拡大等について

資料3

『世界最先端IT国家創造宣言』（平成26年6月24日閣議決定）等を踏まえ、さらなる効率化・利便性の向上が見込まれる分野についてマイナンバーの利用範囲の拡大や制度基盤の活用を図るとともに、マイナンバー制度の主たる担い手である地方公共団体の要望等を踏まえ、所要の整備を行う。

1. 預貯金口座へのマイナンバーの付番

- ① 預金保険機構等によるペイオフのための預貯金額の合算において、マイナンバーの利用を可能とする。
- ② 金融機関に対する社会保障制度における資力調査や税務調査でマイナンバーが付された預金情報を効率的に利用できるようにする。

2. 医療等分野における利用範囲の拡充等

- ① 健康保険組合等が行う被保険者の特定健康診査情報の管理等に、マイナンバーの利用を可能とする。
- ② 予防接種履歴について、地方公共団体間での情報提供ネットワークシステムを利用した情報連携を可能とする。

3. 地方公共団体の要望を踏まえた利用範囲の拡充等

- ① すでにマイナンバー利用事務とされている公営住宅（低所得者向け）の管理に加えて、特定優良賃貸住宅（中所得者向け）の管理において、マイナンバーの利用を可能とする。
- ② 地方公共団体が条例により独自にマイナンバーを利用する場合においても、情報提供ネットワークシステムを利用した情報連携を可能とする。
- ③ 地方公共団体の要望等を踏まえ、雇用、障害者福祉等の分野において利用事務、情報連携の追加を行う。

【参考】

『世界最先端IT国家創造宣言』（平成25年6月14日閣議決定）抄

Ⅲ. 目指すべき社会・姿を実現するための取組

3. 公共サービスがワンストップで誰でもどこでもいつでも受けられる社会の実現

(1) 利便性の高い電子行政サービスの提供

マイナンバーによる情報連携等により、更なる効率化・利便性の向上が見込まれる分野については、制度の趣旨や個人情報の保護等に配慮しつつ、マイナンバーの利用範囲の拡大や制度基盤の活用について検討を進める。