【産業競争力懇談会2010年度 プロジェクト 最終報告】

個人情報や企業情報を安全に活用するための クラウドコンピューティング基盤の整備

２０１１年３月４日

産業競争力懇談会 COCN

【エクゼクティブサマリ】

１．本プロジェクトの基本的な考え方

情報通信分野に関する国際競争力比較では、日本は高速性や利用料金といったハードウェアインフラの面では世界最先端であるにも関わらず、その普及度や電子政府といった利活用面においては低い評価となっている。つまり、ハードウェアインフラの整備は進んでいるが、それが十分に有効活用されていないことにより、消えた年金や社会保障の不正受給等、国民一人ひとりの権利が損なわれる事態を生じている。この利活用が進んでいない原因の一つに、個人情報や企業情報の有効な活用が進んでいないという課題がある。また、プライバシーと個人情報の保護が過度に強調される結果、その活用が限定的になってしまうことも懸念されている。この問題を解決するためには、個人情報や企業情報を安全に組織間で共有するための技術開発と、その活用を妨げている要因を取り除いていくことを併せて進めることが必要である。COCN は、個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤の整備について、情報の利活用を促進するために検討が必要な法制度や、開発・構築が必要な技術・システムについて提言する。

２．本プロジェクトの活動

まず、日本および海外の関連分野の状況を調査し、日本の社会システムが非効率になっている状況を再確認した。次に、医療、製品安全、金融の 3 つの分野で個人情報や企業情報を利活用する新しいサービスについて検討し、サービスを実現したときのメリット、実現するために解決しなければならない課題を議論した。サービスの実現には、個人情報や企業情報を利活用する際に国の番号制度を利用することを前提とし、その利用の課題や要件をまとめた。さらに、個人情報や企業情報を取り扱う時のセキュリティや法制度についても検討を深めた。最後に、検討した課題や要件を整理して提言とした。今後は、番号制度や法制度、セキュリティに関する議論を継続しながら、ユースケースとして検討したサービスを具体化し、実証実験でその有効性を実証していきたいと考えている。

３．実現を目指す利便性の高い新サービスとメリット

- 医療分野では、医療連携サービス、PHR 一次利用サービス、PHR 二次利用サービスの 3 つのサービスを検討した。医療連携サービスでは、各医療機関が保有している診療情報を医療機関の間で連携することで、地域で一貫した医療サービスを提供できるようになる。PHR 一次利用サービスでは、診療記録だけでなく健診記録も含めて PHR データベース環境を構築することで個人の健康維持や診療支援に役立てることができるようになる。PHR 二次利用サービスでは、個人が特定されないよう匿名化された医療情報のデータベースを構築することで、行政や医療研究機関（大学、製薬会社等）が医薬の発展に役立てることができるようになる。
- 製品安全分野では、製品リコール対応、事故未然防止、保守継続性、製品リユースにおける品質管理・保証の 4 つのサービスを検討した。製品リコール対応サービスでは、製品リコールが発生した場合に、その製品の所有者を特定し、製品の所有者に迅速に製品リコール情報を通知することができるようになる。事故未然防止サービスでは、製品の使用状況をモニタリングし、

火災等の人命に関わる事象が発生するリスクを未然に通知することで事故防止ができるようになる。保守継続性サービスでは、製品を転用する時、メーカーと異なるメンテナンス専門業者が保守を行う場合においても保守情報を継続し十分な品質管理を行うことができるようになる。製品リユースにおける品質管理・保証サービスでは、中古市場業者がその時までの使用／保守／修理情報を確認し、正確な中古製品の評価をすることでリユースを推進することができるようになる。

- 金融分野では、金融機関での本人確認、現況確認、各種証明書手続きの 3 つのサービスを検討した。本人確認サービスでは、ID カード提示や ID のネットワーク認証などにより確実な本人確認ができる。本人確認結果のデータを利用することで金融機関は確認書類の保管等の業務負荷の軽減を図ることができる。現況確認サービスでは、個人が金融機関に対し、行政情報を利用することを許諾すれば、現況確認情報を金融機関と行政機関間で直接送受信することができるようになり、本人の現況届提出の手間を省くことができる。各種証明書手続きサービスでは、例えば、納税に関わる各種書類を、個人番号を付加したデータとして、金融機関から税務署に直接データで提出することで、納税手続きにおける個人の手間を省くことができるようになる。

４．クラウドコンピューティング基盤整備に向けた提言

（１）　官の管理する個人番号、個人情報の民間活用

現在国で検討されている国民 ID や共通番号制度の個人を特定することができる番号および官の管理する個人情報（名前、生年月日、性別、住所等）を、民間のサービスにおいても個人を特定するために利用できるようにすること。

（２）　個人番号管理センターの設立

国の番号制度や国や自治体の有する個人情報を民間で利用するための機関（個人番号管理センター）の設立（これは、民間活用システムと国の番号制度のシステムの間に位置づけられ、番号や情報を安全に中継する役割を果たす機関となる）。

（３）　第三者機関の設置

個人番号管理センターにおいて個人番号や個人情報の利用が正しく行われているかを監視する第三者機関の設置の提案。個人が意図しない個人番号や個人情報の利用がされていないことを担保する機関。

（４）　関連する法制度、ガイドラインの検討

国の番号制度や官の管理する個人情報を民間活用するために見直しが必要な法制度やガイドラインについての検討や、個人番号管理センターや第三者機関を設置するための制度の制定の検討。

（５）　官民連携しての技術開発およびシステムの開発、実証

- 本人の意思を反映した情報アクセス制御が可能なシステムの開発と実証
- 大量、長期にわたる安全な情報のライフサイクル管理可能なシステムの開発と実証
- 確実に情報を匿名化する技術の開発
- 長期間（無期限で）データを安全に保存、簡単に利用できる技術の開発
- 膨大な時系列データの効率的処理技術の開発

【目　次】

【はじめに】

ブロードバンドインフラストラクチャの充実やIP化の進展に伴い、種々のサービスがインターネット上で提供されるクラウドコンピューティングの時代が到来しつつある。しかしながら、情報通信分野に関する国際競争力比較では、日本は高速性や利用料金といったハードウェアインフラの面では世界最先端であるにも関わらず、その普及度や電子政府といった利活用面においては低い評価となっている。つまり、ハードウェアインフラの整備は進んでいるが、それが十分に有効活用されていないことにより、消えた年金や社会保障の不正受給等、国民一人ひとりの権利が損なわれる事態を生じている。この利活用が進んでいない原因の一つに、個人情報や企業情報の有効な活用が進んでいないという課題がある。また、プライバシーと個人情報の保護が過度に強調される結果、その活用が限定的になってしまうことも懸念されている。この問題を解決するためには、個人情報や企業情報を安全に組織間で共有するための技術開発と、その活用を妨げている要因を取り除いていくことを併せて進めることが必要である。COCNは、個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤の整備について、情報の利活用を促進するために検討が必要な法制度や、開発・構築が必要な技術・システムについて提言する。

これからのインターネットサービスは、特定の企業が提供する特定のクラウド上で提供されるサービスではなく、金融や医療など異なる分野の企業や機関による複合的なサービスや、さらに政府や自治体といった公共機関とも連携した総合的・統合的なサービスがマルチクラウド環境で提供されていくものと考えられる。その際、クラウド間でサービスを連携するためには、それぞれのクラウドが有する情報を相互に関連付けることが重要な課題になってくる。本プロジェクトでは情報を関連付ける手段として、国の番号制度で検討されている個人を個々に識別することができる番号を、公的分野のみならず民間サービスも含めて利用することとした。この番号による情報の関連付けは、国民生活を豊かにし、より便利にする新たなサービスを生み出すと期待される。同時に、各種情報を関連付けることによるセキュリティ上の問題については十分な配慮と対策が必要である。新しいサービスについては、医療分野、製品安全分野、金融分野の3つのワーキンググループで検討した。番号制度、個人情報の取り扱いに関するセキュリティおよび関連する法制度については、それぞれ別のワーキンググループを設置し検討を深めた。

本プロジェクトが目指す、複数のクラウドが連携して、個人情報や企業情報を安全に活用することを可能にするクラウドコンピューティング基盤は、国民生活における国民負担を軽減し利便性を大幅に向上させ、様々な新たなサービスを実現する基盤となるものであり、結果として国民一人ひとりの権利を守り、公平・公正な社会を構築することに資するとともに、新産業の創出、産業の活性化を通して我が国の産業競争力強化につながるものと考えられる。官民を挙げてその実現に向けて取り組むことを期待する。

産業競争力懇談会
会長（代表幹事）
勝　俣　　恒　久

【プロジェクトメンバー】

プロジェクトリーダー：	日本電気株式会社	江村　克己	
サブ・リーダー：	日本電気株式会社	中田　登志之	
メンバー：	日本電気株式会社	青木　英司	伊東　直子
		岩本　真治	佐古　和恵
		佐治　信之	三宮　禎資
		高島　洋典	名倉　賢
		宮内　幸司	宮川　伸也
		山田　達也	山中　勝文
		吉本　明平	側高　幸治
	株式会社　日立製作所	小島　啓二	堀田　多加志
		尾内　享裕	洲崎　誠一
		赤津　雅晴	畠山　靖彦
		藤城　孝宏	佐藤　嘉則
		坂崎　尚生	安細　康介
	富士通株式会社	吉川　誠一	渋谷　俊昭
		阪井　洋之	佐々木　繁
		加藤　雅之	松田　竜太
		野村　昌弘	内藤　洋二
		五十嵐　俊哉	中川　昌彦
		御魚谷　武	下江　達二
		長谷部　高行	
	株式会社　東芝	内平　直志	西川　武一郎
	東芝ソリューション株式会社	岩崎　元一	守安　隆
		山田　朝彦	
	産業技術総合研究所	関口　智嗣	渡邊　創
		大岩　寛	田中　良夫
	第一三共株式会社	松下　泰之	古賀　貞一郎
		高鳥　登志郎	
	中外製薬株式会社	相川　仁	安達　秀樹
		佐藤　隆司	
	早稲田大学	松島　裕一	中島　徹

１．本プロジェクトの背景

現在、日本の ICT インフラは世界の主要 24 か国中総合評価で第 1 位になっている[1]。ただし、個別の指標の中では、普及率や社会基盤性（インターネットホスト数、ICT 投資割合）が低いとされている。一方世界経済フォーラム（WEF）が毎年公表している ICT 競争力ランキング[2]においては、2010 年の発表では 21 位と過去もっとも低いランキングになっている。この指標の詳細を見ると、各指標の中で個人の対応力（Individual Readiness）が 68 位、政府の対応力（Government Readiness）が 38 位と特に低くなっている。また、国際連合が発行している電子政府の世界ランキング[3]でも 17 位と低迷している（なお、WHO が電子医療に関する調査を行っている[4]が、日本は回答に応じていないため、状況は不明）。

政府は 2010 年 5 月に、「新たな情報通信技術戦略」[5]を発表した。そこでは、“「国民主権」の観点から、まず政府内で情報通信技術革命を徹底し国民本位の電子行政を実現する。加えて情報通信技術の徹底的な利活用により地域の絆を再生し、さらに新市場の創出と国際展開を図る。”とうたわれている。

この戦略には大いに期待しているが、上記データを見ても分かるとおり、現在は ICT の利活用については後進国である。特に、個人情報や企業情報の利活用が進んでいない。例えば個人が金融機関と取引をするときに、本人確認や各種証明書の入手や提示など、行政が発行する証明書や本人確認書類を必要とする場面が存在する。また、金融機関も、契約者による行政機関への証明書の提出などのために、契約者に証明書を送付している。こうしたやり取りは、手続きの際の個人の手間になっていることに加え、金融機関においても多くの業務負荷や郵送料等の業務コストの負担となっている。もし、個人－行政－金融機関（－勤務先）等の間で、個人情報を安全にやり取りできるようになれば、個人の利便性の向上、民間企業の業務効率向上が期待される。したがって、個人情報や企業情報の利活用促進が、ICT 利活用促進につながる鍵であると考える。ICT を基盤とするサービスの規模拡大に伴う個人情報や企業情報の活用形態は図 1 のように変化し、今後のサービスの規模は図 1 の一番右に示した個人情報の活用形態にあたると考えられる。

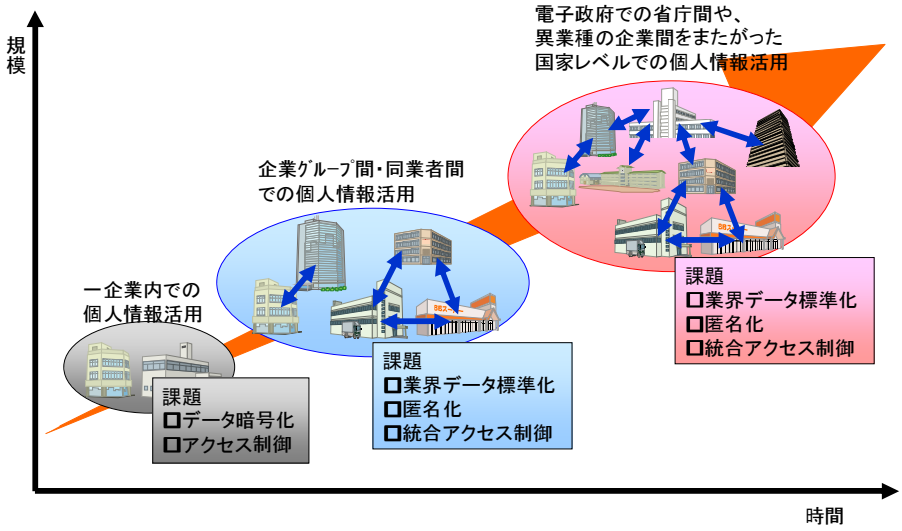


図 1　個人情報の活用形態

一方、プライバシーと個人情報の保護が過度に強調される結果、その活用が限定的になってしまうことも懸念されている。この問題を解決するためには、個人情報や企業情報を安全に組織間で共有するための技術開発と、その活用を妨げている要因を取り除いていくことを併せて進めることが必要である。

２．日本の状況と課題

２－１．日本における IT 社会への取り組み

日本での IT 社会の実現への取り組みは 2000 年 9 月に当時の森内閣総理大臣が「E-ジャパンの構想」を所信表明演説で示したところから始まる。2001 年 1 月 IT 戦略本部は e-Japan 戦略として、下記の理念に基づく IT 国家戦略を策定した[6]。

「我が国は、21 世紀を迎え、すべての国民が情報通信技術（IT）を積極的に活用し、かつその恩恵を最大限に享受できる知識創発型社会の実現に向けて、既存の制度、慣行、権益にしばられず、早急に革命的かつ現実的な対応を行わなければならない。超高速インターネット網の整備とインターネット常時接続の早期実現、電子商取引ルールの整備、電子政府の実現、新時代に向けた人材育成等を通じて、市場原理に基づき民間が最大限に活力を発揮できる環境を整備し、我が国が 5 年以内に世界最先端の IT 国家となることを目指す。」

保健医療の分野では、厚生労働省は e-Japan 戦略の一環として 2001 年 12 月に「保健医療分野の情報化に向けてのグランドデザインの策定について」を策定し、その中の工程表[7]で 2006 年度までには 1)医療施設の情報化、2)医療施設ネット化、3)医療情報の有効活用、4)EBM（Evidence-Based Medicine）支援のための施策を施し、医療情報活用の高度化を実現するとうたった。

２－２．現在の日本の状況

2010 年現在、現状を顧みると、超高速インターネット網の整備とインターネット常時接続は実現されたが、それ以外の目標に関しては、残念ながら達成したとするにはほど遠い状況にある。

例えば、2009 年 8 月に総務省が発表した「平成 20 年度における行政手続オンライン化等の状況」[8]では、国の行政機関が扱う手続きのオンライン利用率は 2007 年度 21.9%、2008 年度 34. 1%となっており、2008 年度になって 10 ポイントあがったものの、まだ 1/3 でしかない。さらに、独立行政法人等が扱う手続きのオンライン利用率は 2007 年度 7.6%、2008 年度 17.6%とまだまだ低い値である。なお、社団法人　日本経済団体連合会（以下、日本経団連）が 2008 年 11 月に出した意見書「実効的な電子行政の実現に向けた推進体制と法制度のあり方について」[9]において、「国民や企業の利便性の向上のためには、各府省庁や地方自治体の個別の申請手続きがオンラインで申請できるだけでは不十分である。また、煩雑な申請手続きを見直さず、そのまま電子化することは、逆に利便性を低下させることになる。」と指摘されている。ようやく、2008 年 6 月 4 日に次世代電子行政サービス基盤等検討プロジェクトチーム『次世代電子行政サービス（e ワンストップ）の実現に向けたグランドデザイン』が発行された。

これにより、以下に示す 26 業務がワンストップ化されることになった[10]。

表 1　ワンストップ化された 26 業務

対象業務	住民基本台帳、固定資産税、収滞納管理、後期高齢者医療、乳幼児医療、戸籍、人事給与、印鑑登録、個人住民税、国民健康保険、介護保険、ひとり親医療、住登外管理、文書管理、外国人登録、法人住民税、国民年金、児童手当、健康管理、財務会計、選挙人名簿管理、軽自動車税、障害者福祉、生活保護、就学、庶務事務

2008 年度の時点では[10]によれば実証実験のレベルにあると思われる。[11]によれば、2010 年度にシステムが稼働する自治体も存在する。一方、民間企業との連携までは実現されていないように見える。

医療分野では、2008 年度のデータで電子カルテの普及率が病院で 17.8%、診療所で 13%、歯科診療所で 82%に留まっているのが現状とされている[12]。

２－３．真の IT 社会の実現に向けて

真の IT 社会の実現に向けて検討すべき課題には、単にシステム的な問題だけではなく、規制・制度・慣行に起因するものが多くある。例えば日本経団連が出した総務省意見募集「ICT の利活用を阻む制度・規制等についての意見」[13]では、48 項目に関して阻害点を記した上で要望を述べている。その中で、本プロジェクトに関係するものを表 2 に示す。

表 2　日本経団連の「ICT の利活用を阻む制度・規制等についての意見」で本プロジェクトに関係するもの

項目	ICT 利活用を阻害する制度・規制等の根拠
(1).遠隔医療に関わる規制の見直し	・医師法第 20 条、歯科医師法第 20 条、医政局長通知（医政発第 0331020 号）「情報通信機器を用いた診療（いわゆる「遠隔診療」）について」の一部改正について（平成 15 年 3 月 31 日） ・薬事法施行令医師法第 17 条、歯科医師法第 17 条及び保健師助産師看護師法第 31 条、医政発第 0726005 号　平成 17 年 7 月 26 日 厚生労働省医政局長通知 ・健康保険法　および厚生労働省告示「健康保険法の規定による療養に要する費用の額の算定方法」
(2).特定健診の保健指導における ICT を活用した遠隔面談	・特定健康診査及び特定保健指導の実施に関する基準（平成 19 年厚生労働省令第 157 号）第 7 条及び第 8 条
(3).レセプトのオンライン請求の義務化	・「療養の給付及び公費負担医療に関する費用の請求に関する省令」（最終改正：平成二一年一一月二五日厚生労働省令第一五一号） ・「療養の給付及び公費負担医療に関する費用の請求に関する省令の一部を改正する省令の施行等について」厚生労働省保険局長通知（保発 1125 第 4 号平成 21 年 11 月 25 日）

項目	ICT 利活用を阻害する制度・規制等の根拠
(6).処方箋の電子化	民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について（平成 17 年 3 月 31 日医政発第 0331009 号、薬食発第 0331020 号、保発第 0331005 号）
(7).医療情報外部保存と 2 次利用に関する法整備	医療法（昭和 23 年法律第 205 号）第 21 条、第 22 条及び第 22 条の 2 に規定されている診療に関する諸記録
(25).住民基本台帳ネットワークの利用業務拡大および民間事業者での利用	住民基本台帳法第 11 条、11 条の 2、12 条、12 条の 2、30 条の 7
(26).公的個人認証サービスの民間事業者への利用拡大	・電子署名に係る地方公共団体の認証業務に関する法律第 1 条、3 条 4 項、17 条 ・電子署名に係る地方公共団体の認証業務に関する法律施行規則第 6 条 ・犯罪による収益の移転防止に関する法律 ・古物営業法第 15 条 ・携帯音声通信事業者による契約者等の本人確認等及び携帯音声通信役務の不正な利用の防止に関する法律施行規則
(29).自動車関連情報の利活用	・道路運送車両法 ・道路交通法 ・自動車公正競争規約

真の IT 社会を実現させるためには、上記の制度などを改善するとともに、個人、企業および行政に関わる情報を安全かつ有機的に連携させ、様々な日常サービスにおいて有効に活用できるような仕組みを構築することが必要となる。

３．個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤整備の提案

本プロジェクトでは、個人情報や企業情報を安全に活用して、複数のクラウドにより種々のサービスを提供することが可能となるクラウドコンピューティング基盤について、制度面、技術面の検討を実施した。検討したクラウドコンピューティング基盤のイメージを図 2 に示す。

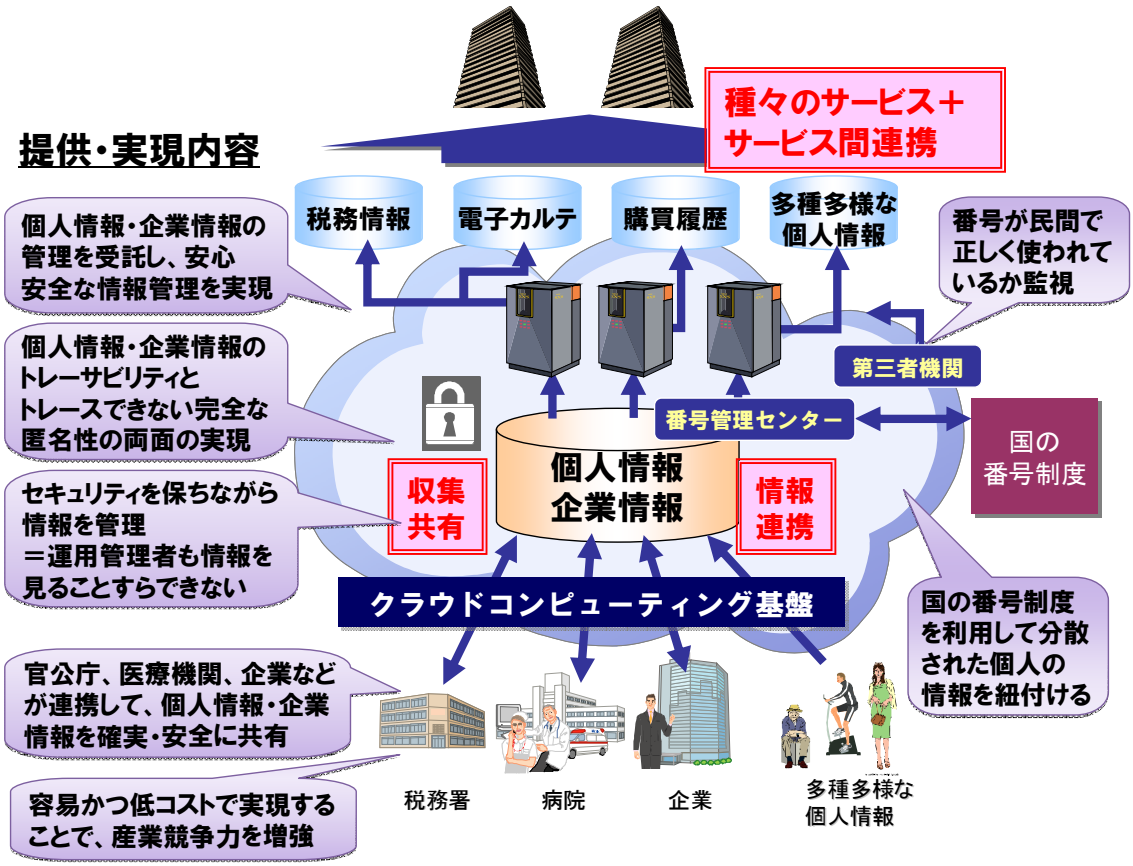


図 2　クラウドコンピューティング基盤

本プロジェクトでは、個人情報とは、元来、各自に備わっている身体的な特徴や個人の日常生活を営む際に必要となる情報、生活の活動で新たに生み出される情報であり、企業情報とは、企業名などの企業そのものを表す情報や企業が顧客にサービスを提供する際に必要な情報、企業活動の中で新たに生まれる情報であると想定している。

これからのインターネットサービスは、特定の企業が提供する特定のクラウド上で提供されるサービスではなく、金融や医療など異なる分野の企業や機関による複合的なサービスや、さらに政府や自治体といった公共機関とも連携した総合的・統合的なサービスがマルチクラウド環境で提供されていくものと考えられる。その際、クラウド間でサービスを連携するためには、それぞれのクラウドが有する情報を相互に関連付けることが重要な課題になってくる。本プロジェクト

では情報を関連付ける手段として、国の番号制度で検討されている個人を個々に識別[1]することができる番号を利用するものとした。国の番号制度を利用することにより、ID の運用に公的機関の信頼性を担保するとともに、全国民を対象とした別の仕組みを新たに作り出す無駄な投資を省くことができると考えるからである（国で検討されている番号制度によって運用される、個人を特定[2]する番号のことを以下「個人番号」と呼ぶ）。この ID による情報の関連付けは、国民生活を豊かにしより便利にする新たなサービスを生み出すと期待される。しかし、一方で各種情報を関連付けることによるセキュリティ上の問題については十分な配慮と対策が必要である。

クラウドコンピューティング基盤がこの個人番号を利用する場合、国の番号制度を運用しているシステムと民間サービスを直接接続するのではなく、個人番号の安全な取り扱いや、公的機関のもつ信頼性を保つために双方のシステムを中継する番号管理センターの設置を提案する。さらに、個人番号の民間利用が正しく行われているか監視するための第三者機関が必要だと考えている。

以降の章では、システムの形態としてはマルチクラウドシステムであること、サービス連携（情報の紐付け）のキーとして公的な番号制度を利用することを前提として、どのような有益なサービスが生み出されるかを示すとともに、それらのサービスを実現するために解決しなければならない課題について述べる。

まず４章においては、本プロジェクトにおいて提案するクラウドコンピューティング基盤上で実現できるであろう利便性の高い国民生活を豊かにするサービスについて医療、製品安全、金融の 3 つの分野で検討し、その実現に必要な要件を探った。５章では番号制度に関する検討を行い、国の番号制度を民間利用するために必要な要件についてまとめた。６章では、公的な番号制度を４章で挙げた民間サービスで利用することに対するセキュリティ上の脅威とその対策を検討した。対策について、技術だけで解決できない点については、制度的な面も併せて議論した。７章では、国の番号制度を民間利用する際に考慮が必要な法律や制度について検討した。８章では、７章までに述べた検討結果を踏まえて本プロジェクトとしての提言をまとめている。

本プロジェクトでは一年を通して議論をしてきたが、まだ十分に検討しつくしたとは言えないと考えており、それを踏まえて９章で今後の活動について述べた。なお、１０章以降の章は本プロジェクトでの検討内容に関する参考資料である。

---

[1] 識別：二人の異なる個人をそれぞれ異なるものであると判断できること。
[2] 特定：その人が誰か、氏名住所などが分かること。

４．情報利活用による利便性の高いサービスの実現

４－１．医療・健康分野のサービス

デンマーク、ドイツ、オランダ、米国などの欧米諸国では、医療サービスの充実、資源の有効利用、医療従事者間の業務プロセス支援などを目的として、予防医療、治療、遠隔地医療など様々な医療サービスの IT 化を国主導で積極的に進めている[38][39][40][41][42]。これらの国々と比較し、我が国の医療情報利活用の水準は同程度とは言い難いものの、着実に IT 化が進められており、レセプトの電子化や電子カルテの導入も進んでいる。地域の医療機関をネットワークで結び電子化された医療情報を相互に利用することで、患者の治療や地域医療の運営に役立てようという研究や実証実験等が実施されており、「ドルフィンプロジェクト」[14]や「地域医療情報連携システムの標準化及び実証事業」[15]等のように、地域の医療機関の間で治療に必要な情報を相互に参照するシステムを構築し実際の治療に利用している例もある。また、医療技術や医薬の発展、医療行政に利用することも検討されており、「健康情報活用基盤構築のための標準化及び実証事業」[16]や「日本のセンチネルプロジェクト」[17]等のように、実際に医薬品等の安全対策に利活用するために医療情報を集約し疫学研究に役立てることを目標としたプロジェクトも実施されている。

ここでは、具体的なサービスとして「医療連携サービス」、「PHR[3]一次利用サービス」、「PHR 二次利用サービス」の 3 つを検討し、それらのサービスを実現するためのシステムや社会制度を検討し課題の整理を行った。「医療連携サービス」で対象とする情報は、主に医療機関が治療や診断に使う情報を想定している。「PHR 一次利用サービス」、「PHR 二次利用サービス」については、医療機関が治療や診断に使う情報だけでなく、企業や自治体が実施している社員や住民の健康診断情報などの健康管理のための情報を、治療や健康管理に利用することを考えている。一次利用サービスとは、これらの情報を直接、本人の治療や診断に使うことを想定し、二次利用サービスとは、個人でなく集団として、性別、年代、地域といった観点からの統計的な分析などを行い、疫学研究や医療行政情報に利用することを考える。二次利用する場合は、情報が誰のものか分からないようにデータの匿名化処理を行い個人のプライバシーを守りながらデータを分析利用する。

このようなサービスを実現するシステムは、以下のような要素から構成されるとした。

- 個人番号管理センター

  個人番号管理センターは、医療情報管理機関、PHR 管理機関の要請に基づき、個人番号、個人を特定する情報を提供する。他分野と共通的に利用する個人番号を処理するセンター。個人を特定し、個人の現況確認をするために利用する。

- 医療番号管理センター

  医療番号管理センターは、医療分野に限定して使用し個人を特定する番号である医療番号を管理する。医療情報管理機関、PHR 管理機関の要請に基づき、医療番号、個人を特定する情報を提供する。

[3] PHR：Personal Health Record。個人健康記録。

医療番号は医療情報をリンクさせるために利用され、患者を一意に識別する番号と定義する。また、病気や身体的な情報である医療に関する情報の取り扱いは非常に慎重にあるべきであるという点を考慮し、医療分野内でのみ利用するものとする。

医療番号により、各医療機関、関連機関（健康管理センター等）が独自に管理する患者番号やカルテ番号等を紐付け、医療機関をまたぐ医療連携サービスや病歴等の情報の関連付けを実現する。税金や金融といった他の分野とのサービス連携のためには個人番号を利用する。このように医療分野に閉じた医療番号を定義することで、他の分野で共通的に使われる個人番号からその個人の医療情報を直接利用することを避ける仕組みを構築することができる。例えば、個人番号からその個人の医療情報を利用する場合は、医療番号管理センターを通し、紐付けすることが妥当であるか判断したのち、初めて医療番号（および各病院の患者番号やカルテ番号等）と紐付けされ情報を利用できるようになる。

- 医療情報管理機関

医療情報管理機関は、患者を識別する個人番号、医療番号から、複数の医療機関にまたがる患者の診療情報の統合利用を可能にする。各病院・医療機関が保有する情報の集約および関連付けを行う。また、病院・医療機関での保管期間を過ぎた過去の情報についても引き続き保管を行う。

- PHR 管理機関

PHR 管理機関は、様々な機関において個人番号、医療番号で管理される個人の生活・健康情報の関連付けや、収集した情報管理の他、PHR を利用する医療機関以外の事業者、行政機関に対して、情報へのアクセスを提供する。

図 3 に、システム構成を示す。

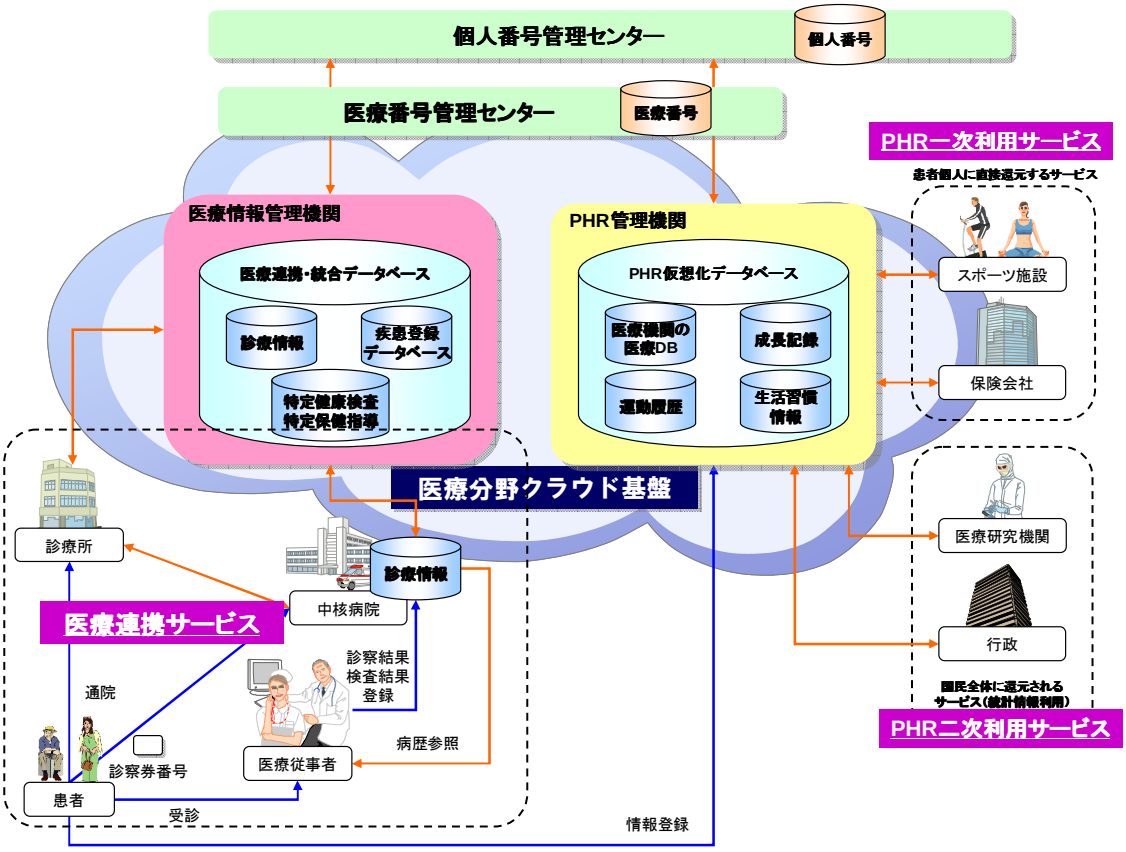


図 3　医療・健康分野に関するユースケースのシステム構成

４－１－１．医療連携サービス

（１）サービス概要

各地域において、発症から急性期、回復期を経て在宅に帰るまで、患者の様態に応じ切れ目なく医療が提供されるよう、地域の中核病院と周辺の医療機関が連携した地域医療連携の構築が求められている。電子カルテの導入を普及させ、各医療機関で持っている診療情報を医療機関の間で連携することで、複数施設の診療情報を横断的に把握でき、患者に対して地域で一貫した医療サービスを提供できるようになる。また、個人番号を患者情報として登録することで、個人番号をキーにした医療情報の連携が実現できる（図 4）。

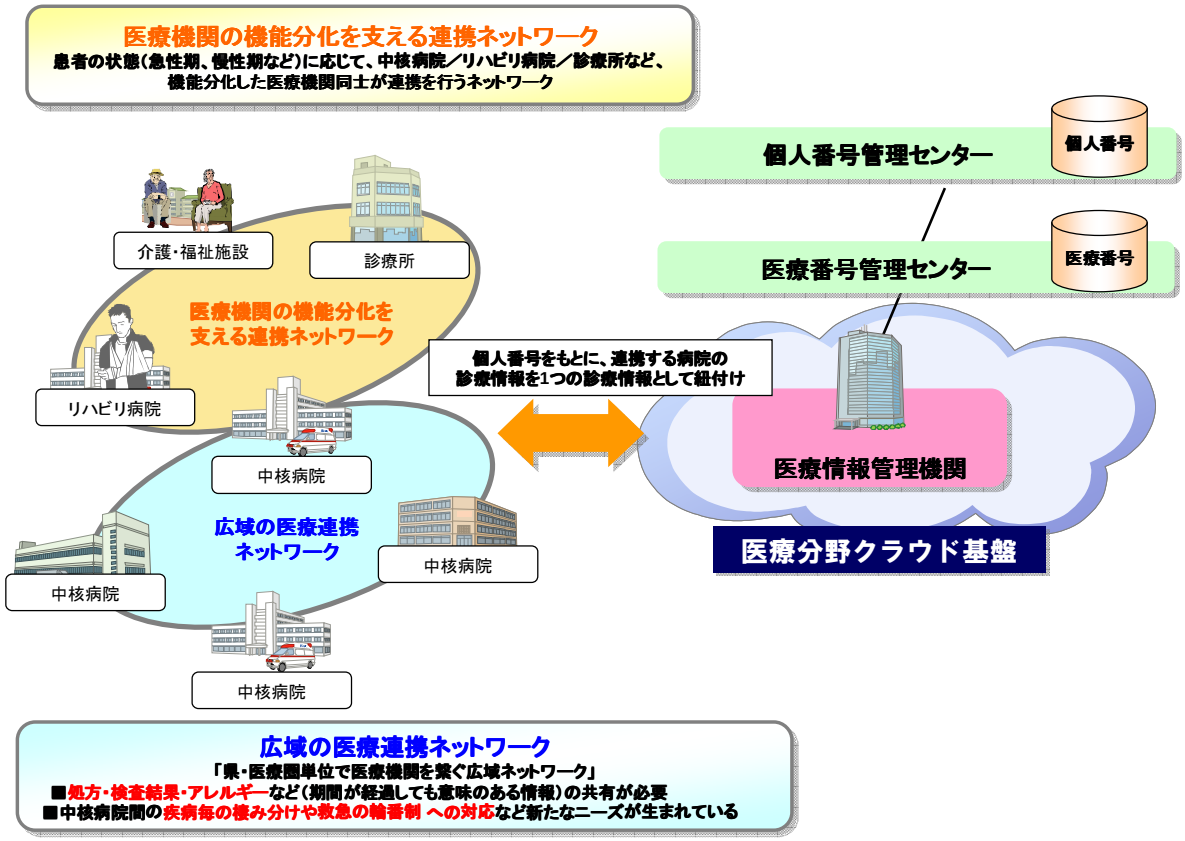


図 4　医療連携サービスのイメージ

地域医療連携を実現することにより、救急医療時の対応や医療機関を移動した場合でも、それまでの診療情報が連携できるため継続的な診療行為が可能になる。

- 医療機関で患者基本情報を登録する際、患者が個人番号を提示することで、広域医療を可能とする。
- 医療機関は、医療情報管理機関経由で当該者の患者情報を取得する。

（２）背景と目的

近年医療機関における電子カルテの導入が普及し、各医療機関で持っている診療情報を医療機関の間で連携することで、複数施設の診療情報を横断的に把握できるようになってきた。しかし、それぞれの医療機関では患者を識別するための患者番号が個別に設定されるため、医療機関同士で情報を連携するためには、連携する医療機関同士で患者番号の紐付け作業を行う必要がある。それに加えて、診療情報は重要な個人情報であるため、ミスは絶対に避けなければならず、個人を特定する作業において慎重に対応する必要があり、作業も非効率になってしまう。

また、通常医療機関で診察を受ける場合には、個人の基本情報や現病歴、既往歴、アレルギーなどの情報を申請しなければならない。しかしながら、このとき各個人が申請した情報の信頼性は保証されないまま、患者情報が登録されている。さらに、救急時に患者が申請できない状態にある場合などは、基本情報の登録ができず、さらには治療中か否か、あるいはアレルギーなどの情報も不明なまま治療しなければならず、大きなリスクを負って対処しなければならない状況にある。

個人番号による医療連携を可能とすることで、以下のようなメリットが期待できる。

（３）メリット

- 個人番号を提示してもらうことにより、個人を特定する作業が完了する。また、他の医療機関との情報連携のための手続きも軽減でき、情報の信頼性を向上させることが可能になる。
- 救急時において個人番号が分かれば、他の医療機関での診療記録が取得できる。現在治療中の病気やアレルギーなどの情報を入手することで、より迅速な対応が可能になる。
- 個人番号に紐付けされた患者の基本情報から、必要な情報を取得できるため、患者自身の申請手続きが削減できるとともに、受付担当者にとっても正確な情報を取得できるため、窓口業務の効率化と情報の信頼性が向上する。
- 平成 23 年現在、政府において「どこでも MY 病院」構想の実現が検討されている[5]。その実現の際、各病院、医療関係機関でのカルテ等の情報を患者個人単位で統合していく必要がある。本プロジェクトで提案する個人番号をキーとして情報を統合していくクラウドコンピューティング基盤をベースにして実現することができるものと考える。

（４）利用場面

＜場面１＞

患者が病院、診療所等で診察を受けるときに、これまでに掛っていた病院、診療所等の情報も踏まえて受診する場合の例を示す。

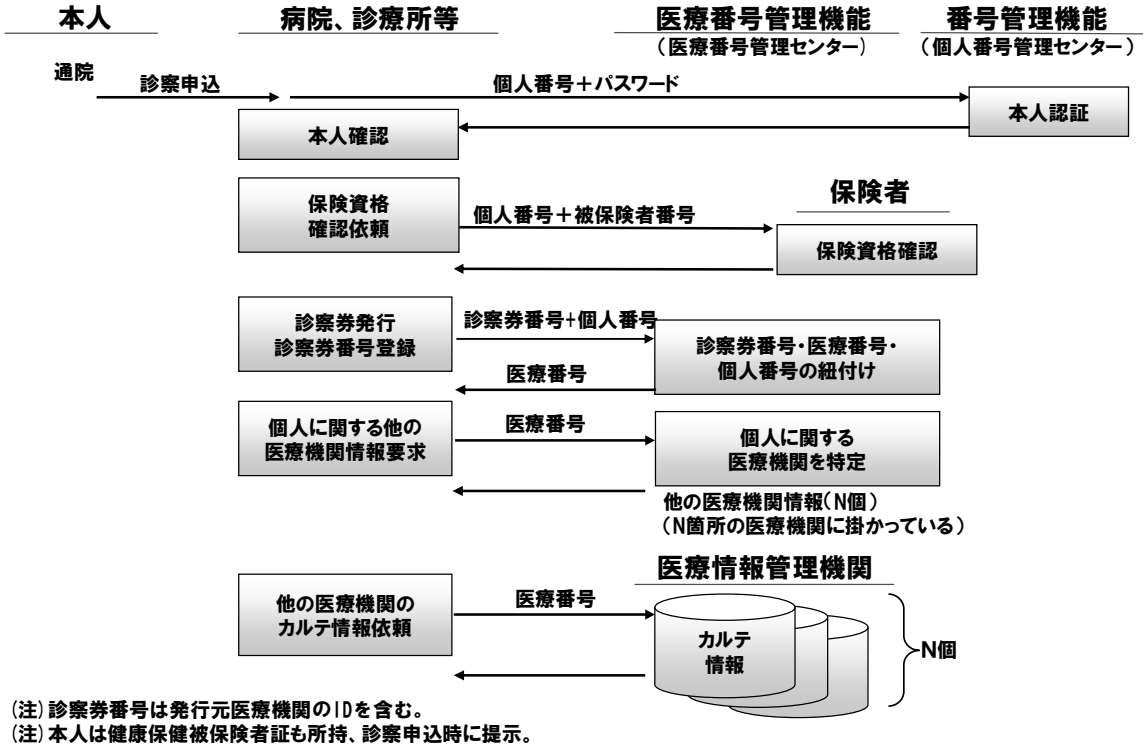


図 5　医療連携のシーケンス（カード利用可）

- 患者は、病院、診療所等で個人番号カードを用いて本人確認を行う。
- 患者の本人確認後、病院、診療所等は、患者の保険が有効であることの確認を行う。
- 病院、診療所等は、患者の診察券を発行するとともに、診察券番号を医療番号管理センターに登録する。
- 病院、診療所等は、医療番号管理センターに当該患者の医療情報を持っている医療機関の情報を要求する。
- 病院、診療所等は、受領した医療機関の情報を基に、医療情報管理機関に患者のカルテ情報を要求する（各医療機関の患者情報は、医療情報管理機関が収集する）。

＜場面２＞

上記の場面１と同様であるが、本人認証[4]のカード処理ができないときの例を示す。

[4] 認証（ユーザ認証、個人認証）：事前に発行された ID に対して、PKI（Public Key Infrastracture：公開鍵暗号基盤）やパスワードなどを使って、アクセスしてきた人がその ID で登録された本人であることを確認すること（注：認証手段をつかって、本人確認（目的）を実施することがある）。

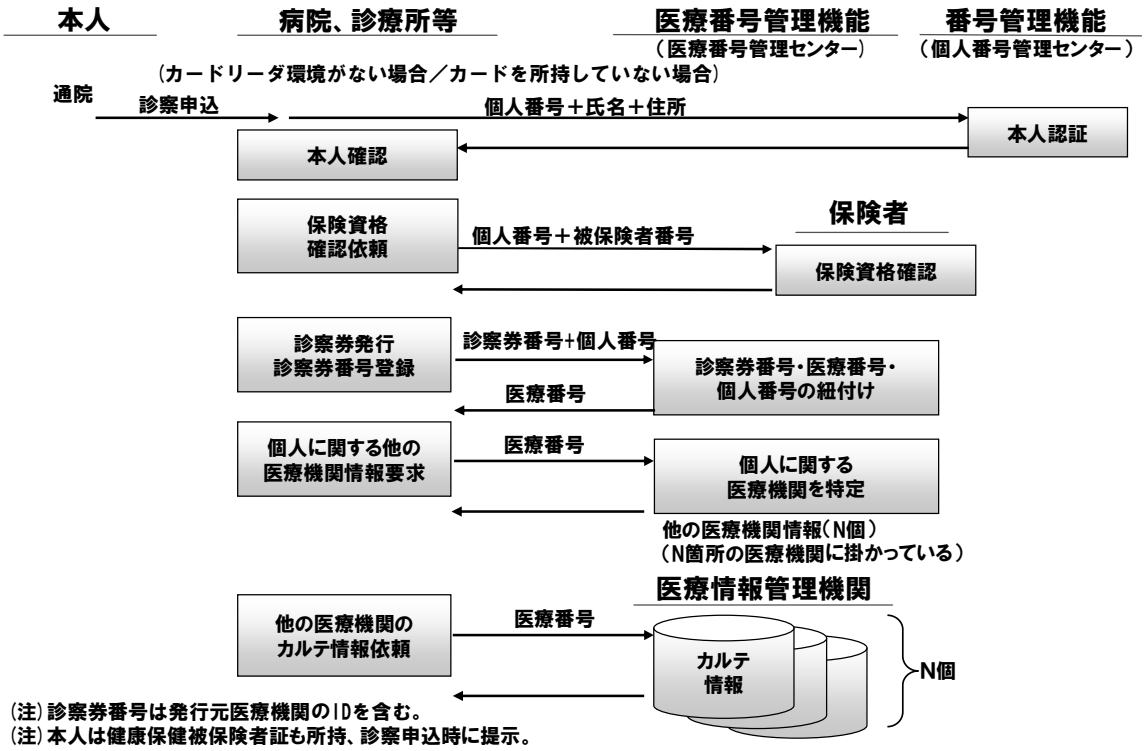


図 6　医療連携のシーケンス（カード利用不可）

- 患者は、病院、診療所等で個人番号と基本情報を提示する。
- 病院、診療所等は、その情報が正しいことと、それに加えて、窓口にて写真等で本人であることを確認する。
- 患者の本人確認以降は、場面１と同様。

４－１－２．PHR一次利用サービス

（１）サービス概要

近年、医療費の財源問題や医師不足の状況の中、個人自らが健康維持に努め、病気にならないことが求められている。生まれてから現在に至るまでの診療記録や健診記録、さらには日々の生活情報などを PHR 環境として構築することができれば、個人の生涯の健康情報を個人が自己管理でき、健康維持や診療支援に役立てることや、診療や治療に対する健康保険や傷害保険などの給付金請求を正確に、速やかに行うことが可能となり、さらには民間企業の新しいビジネスの創出につなげることが可能になる。

図 7 に、PHR 一次利用によるサービスのイメージを示す。なお、PHR 管理機関のデータは、本人の承認範囲に基づき、民間企業や行政機関に活用されることを前提としている。

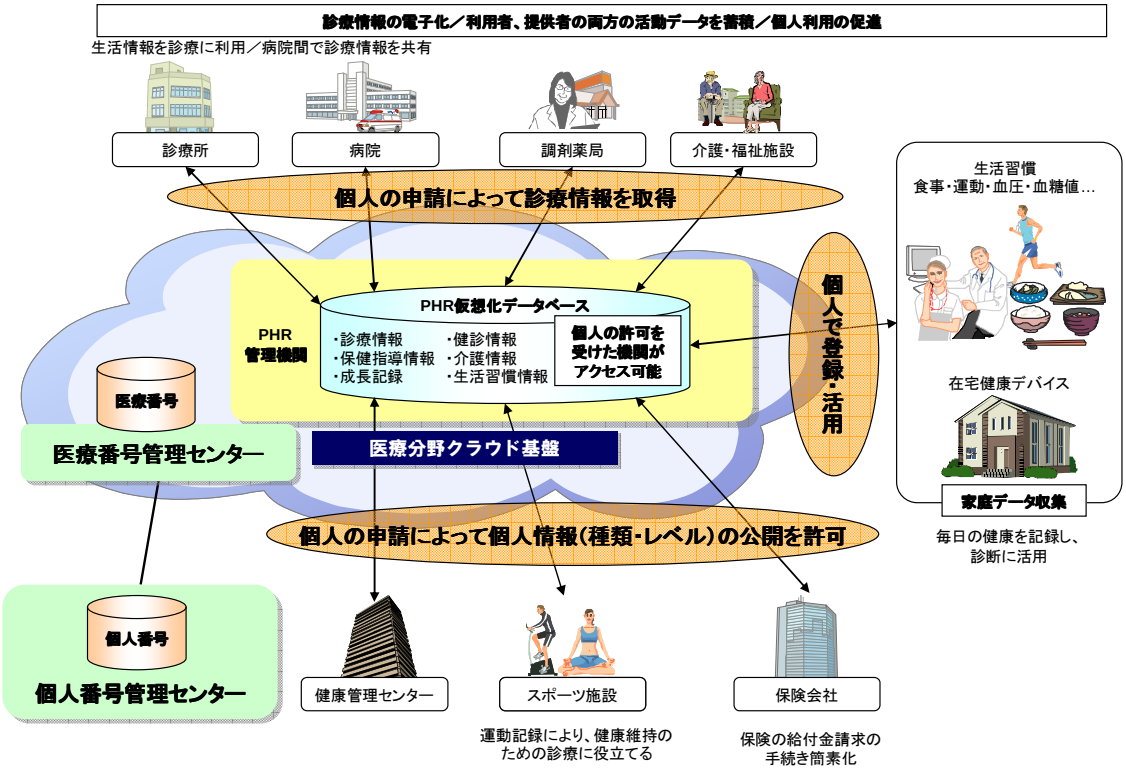
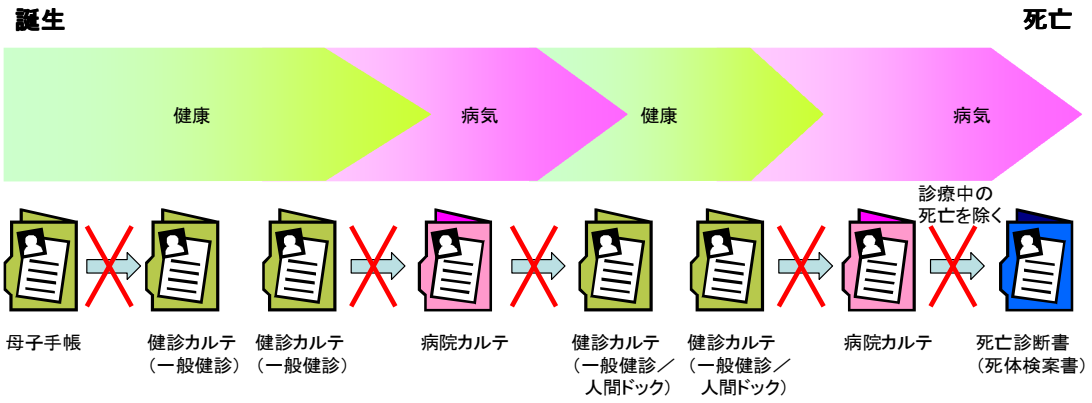


図 7　PHR 一次利用によるサービスのイメージ

例えば、図 8 に示すように、母子手帳から健診カルテ、病院カルテ、死亡診断書までを電子化し、健康なときから病気のときまで一貫して身体の情報を管理し、提供可能なサービスを実現する。これにより、健診カルテ（一般健診データ、特定健診データ）、電子カルテ（レセプトデータ、DPC[5]データを含む）のデータを連携し、個人の長期的な身体データを参照可能とすることで、個人での健康管理や医師の診断に役立てることが可能となる。

[5] DPC：Diagnosis Procedure Combination。診断群分類。



情報の断絶により病気が発症した原因を現時点の検査結果と、患者の記憶に頼らなければ診断ができない。

健診カルテと病院カルテを連携する事で、現在の検査結果と、過去の検査結果等を総合的に勘案して診断が可能。より適切な治療を可能とする。
更に、母子手帳、死亡診断書までを連結することで個人による生涯の健康状態を記録・管理可能とする。

図 8　健診・診療統合情報サービスのイメージ

（２）背景と目的

健診情報は健診システムで、診療情報は電子カルテで電子化されつつある。しかしながら、システム間での連携が不十分である。また、保険請求上で必要なデータであるレセプトデータ、DPC データについては、標準フォーマットで電子化されている。しかしながら、健診カルテの問診結果や病院カルテの問診・経過記録情報などは医療機関によりフォーマットが異なっている。このため、生まれてから現在に至るまでの診療記録や健診記録を自己管理するためには、医療機関や健診施設から情報として入手する必要がある。しかし、個人を識別するための ID は、各医療機関で個別に設定されるため、個人が過去の記録を情報として入手しようとしても、個人を確定するまでに手間がかかる。情報提供側としては重要な個人情報であるため、個人を特定する作業において慎重に対応する必要が生じ、作業も非効率になってしまう。

また、保険の給付金請求のために、診療中の、あるいは病み上がりの患者本人や入院者を抱える家族が、給付金請求のために必要な様々な書類を医療機関に申請し、相当の手数料を支払い、手続きを行っているのが現状である。これは、患者やその家族にとって多大な負担となっている。また、医療機関にとっても保険給付金請求のために必要な書類の作成・発行は、本来の業務ではなく、極めて多忙な医師や医療機関にとって負担となっている。こうした問題のために、実際には給付が十分行われない、あるいは悪意を持った申請者が不正な給付金請求を行う可能性があるなどの問題がある。

なお、レセプトデータからは、病名、薬、検査・処置項目などが、DPC データからは、レセプトデータ項目に加え、がんのステージ情報、心機能分類・重症度、日常生活活動度などが得られる。これらデータの個人への提供を検討するにあたっては、病気の告知問題を避けて通ることができない。また、データの一次利用に関し、提供範囲を個人のみとするか、親族を含めるかどうかなど、提供条件の検討も必要となる。

さらに、生涯の健康状態を個人が把握する上では、母子手帳から死亡診断書に至るまでを電子化して連携して管理できることが望ましい。しかし死亡診断書については、入院中の死亡など診療中の場合は、電子カルテで電子化されているが、診療機関の外での死亡などについては必ずしも電子化されていないのが現状である。

PHR の一次利用を可能とすることで、以下のようなメリットが期待できる。

（３）メリット

- 医師や看護師、保健師、薬剤師などから、健康維持のための総合的なアドバイスを受けることが可能になる。
- 患者にとっては、自分の健康・病気の記録をいつでも確認することができ、健康の自己管理や病気の際に医療機関に情報を提供することで適切な診断治療を受けることができる。
- 国・自治体にとっては、国民、住民の健康状態の傾向を知ることで適切な施策を打つことが可能となる。例えば健康増進プログラムのプランニングに活用できる。また個人の同意を得ることができれば、追加の健診へのレコメンデーション[6]を行うこともできる。これらの施策により労働人口維持向上と安定的な税収確保を見込める。
- 患者や家族にとっても医療機関にとっても不要な負担を強いている、医療保険や傷害保険、生命保険などの給付金請求の手続きの不便が大幅に解消される。保険会社にとっても、処理がすべて電子化されることにより大幅な省力化が図れ、事務処理の品質を向上させることができる。
- 医療保険や傷害保険、生命保険などの給付金の請求が正確になり、不正な請求の余地が小さくなる。
- スポーツ施設において、医師との連携によりその人にあった運動の指導や健康状態の管理が可能になり、個人にとって最適な健康維持のメニューの作成ができる。
- 企業は個人向けの新しいサービスビジネスを創出することができる。
- 国税電子申告・納税システム（e-Tax）を用いた確定申告を行う際に PHR の情報を利用することで、医療費控除額が入力不要となり、手続きが簡便になる。
- 政府において「レセプト情報等の活用による医療の効率化」について検討をすすめているところであるが[5]、このクラウドコンピューティング基盤は有効であると考えられる。さらにこのクラウドコンピューティング基盤が収集するデータは、出生から死

[6] レコメンデーション：recommendation。ユーザの好みに応じた情報を推薦・提供すること。

亡までの情報を想定していることから、現状検討されている内容よりさらに深い、有効なデータ活用、サービス展開の実現も考えられる。

（４）利用場面

PHR の一次利用として、医療情報、健康情報を用いて、利用者が健康アドバイスを受ける場合の利用場面を示す。

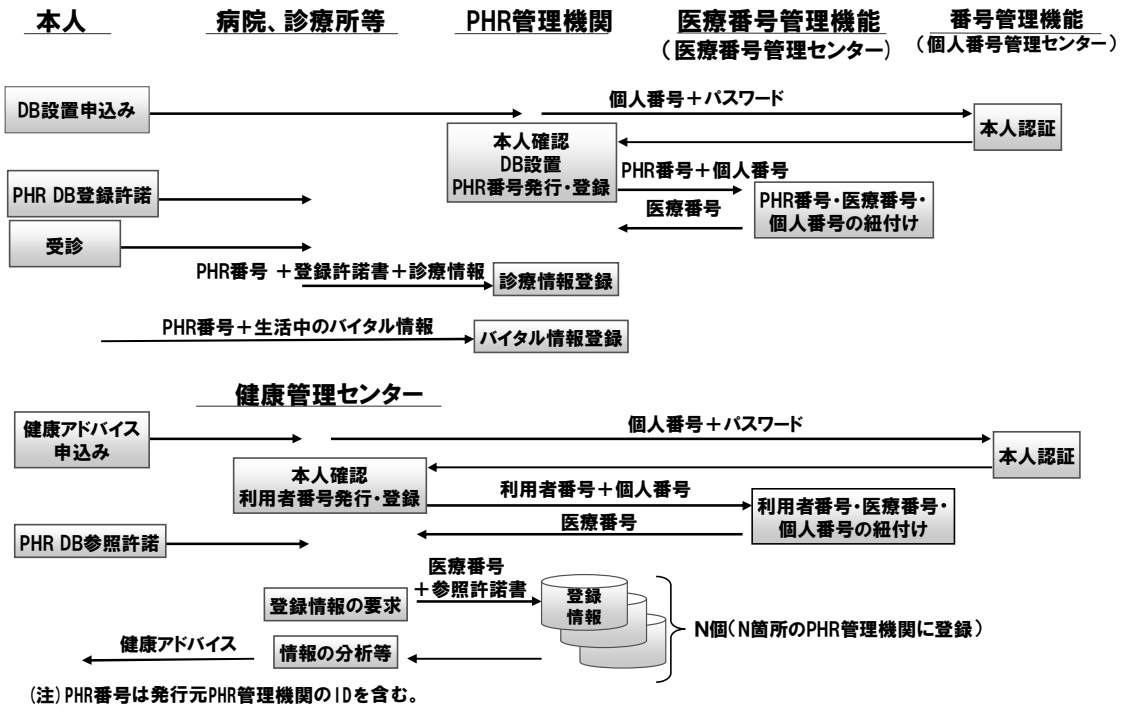


図 9　利用者が健康アドバイスを受ける場合のシーケンス

- PHR 管理機関利用者は、PHR 管理機関（複数個所の場合あり）に個人用の DB を設置する。DB 設置の申請時に個人番号カードを用いて本人確認を行う。
- PHR 管理機関は、利用者の PHR 番号と個人番号を医療番号管理センターに登録する。
- 利用者は、この PHR 管理機関に診療情報を登録することを認める病院、診療所等に対し、情報の登録許諾を行う。
- PHR 管理機関への登録を許諾された病院、診療所等は、利用者を診断する都度、診療情報を PHR 管理機関に登録する。
- 利用者は、日常生活の中でのバイタル情報を逐次（自動的に）PHR 管理機関に登録する。
- 利用者は、健康管理センターに健康アドバイスを求めるために、健康管理センターが PHR 管理機関の情報を参照することを許諾する（参照させたくない PHR 管理機関に関しては許諾しない）。

- 健康管理センターは、利用者の本人確認後、許諾を得た PHR 管理機関の情報を基に、利用者に健康アドバイスを行う。

４－１－３．PHR二次利用サービス

（１）サービス概要

医療情報データベースを構築し、患者のプライバシーを保護しながら、行政、医療研究機関（大学病院、製薬会社など）が蓄積情報を二次利用し、医療の質の向上に役立てる。ここで想定する二次利用とは、個人の健康情報を、前節の PHR 一次利用サービスのように当該個人のためだけでなく、その個人を含む公共の利益のために、個人の健康情報が収集された病院などの機関以外の外部機関（行政、医療研究機関）で利用することを指す。二次利用に際しては、前節で説明した「PHR 一次利用サービス」で構築された医療情報データベースに蓄積された情報を、外部機関に提供できるように加工したものが提供される。提供されるデータから個人を特定され、その結果として、病気などのセンシティブな情報が漏洩することを防ぐため、ここでは匿名化されたデータが提供されることを想定する。匿名化されたデータは、医療情報データベース管理機関であっても、元の個人をたどることはできない（これを、連結不可能匿名化という）。しかし、情報を提供する側の個人としては、疫学研究の結果、自分に関わる重要な知見が得られた場合には、フィードバックを受けたいという要望がある場合もあり、要望に応じて個人にフィードバックを返す必要がある。個人がフィードバックを希望しているなどの特定の条件の下であれば、医療情報管理機関において、匿名化データから元の個人を特定できるようにする仕組みを残すことも検討した（これを連結可能匿名化という）。

図 10 に PHR 二次利用によるサービスのイメージを示す。

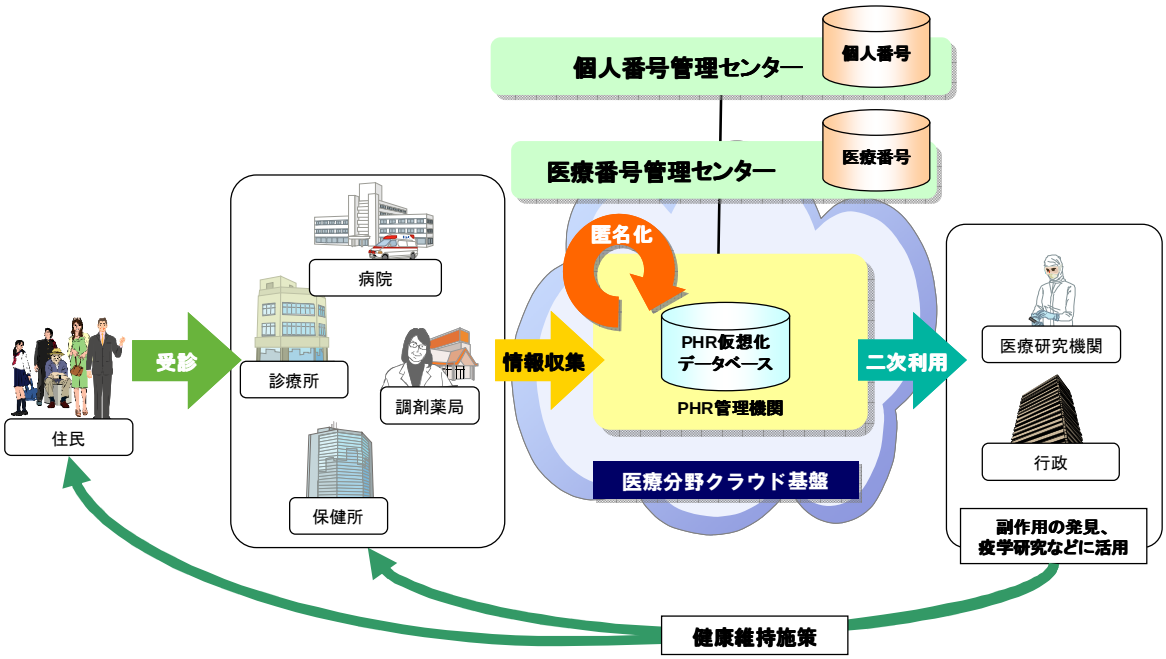


図 10　PHR 二次利用によるサービスのイメージ

【実現する事柄】

- 統合データベースの構築

  医療情報を統合的に活用できる基盤を整備する。疫学情報、臨床研究情報、健診・診療・健康保険レセプト、薬剤処方等の情報を電子化して、個人番号で連結した統合データベースを構築することにより、体系付けられた医療関連情報として、医薬品安全対策、予防医療、医療研究などへの活用が可能になる。

- 医薬品安全対策への活用

  医薬品使用後の特定の副作用（有害事象）の発生頻度（割合）を正確かつ適切な時間内にモニタし、他剤を使用した場合の副作用の発生頻度と比較することが可能になり、販売後の適切な時期にさらなる安全対策の必要性について検討し、実施することが可能となる。また、医療上必要な医薬品等の治験を実施する際の基礎的な安全性情報等をデータベースから提供することを通じ、ドラッグラグ等の解消等、医療にとって必要な医薬品等の医療技術の迅速な提供にもつながることが期待できる。

- 予防医療への活用

  予防医療は、将来の医療においてその重要性はますます高まる。健康・医療情報を相互に活用することにより、予防医療が実現できる。また、個別化医療に関しても、バイオマーカー、薬剤疫学、ゲノム研究等の研究データを他の目的別データと相互に活用することで、国民レベルでこれらの成果を享受することが可能になる。

- 医療研究への活用

  二次的データの統合的活用により、革新的医薬品・医療機器・治療技術創出を強力に推進するツールになり、新たな医療技術の開発機会が高まる。これらは高齢化社会での健康寿命延伸、疾病後の早期社会復帰に寄与するなど、超高齢時代の新たな医療システムの確立に必須である。さらに、これらの成果は世界に向けて発信することが可能であり、産業競争力の向上に資する。e-ヘルス市場の成長（ソフトウェア、初期インフラ投資、維持管理等）が期待できる。

- 医療行政への活用

  健診、診療、調剤情報などを集約し、行政が統計情報として活用する。例えばある地域で自治体が、住民に脳卒中が多いことに気づき、「塩分が多い食生活の改善を進めるキャンペーン」など、高血圧に対する施策を打つ。月毎にその自治体で「高血圧の薬を飲んでいる人数」「新しく飲み始めた人数」「薬を飲むのをやめた人数」などのデータを計測し、「新規に薬を飲む人が減り、飲むのをやめた人が増えてきた」傾向を捕え、キャンペーンの効果を判断する。

（２）背景と目的

我が国では、医療データが共有されておらず、有効な研究データの入手が困難である。一人の患者の情報が複数の病院に分散して蓄積されており、これまで利用可能な大規模な医療データベースがなく、データベースを利用した調査研究ができない状況にある。患者が転居等により転院すると、患者の予後を追跡できなくなってしまうこともある。また、自治体は単年度単位で動いているため、10 年先にしか結果が分からない事業を継続するのは難しい。食事療法などを開始して、その効果（例えば、脳卒中発症との関連性）が分かるまでには 10 年程度かかる。

上記背景から、医療情報データベースを構築し、患者のプライバシーを保護しながら、行政、医療研究機関（大学病院、製薬会社など）が蓄積情報を二次利用し、医療の質の向上に役立てる。具体的には、以下のようなメリットが期待できる。

（３）メリット

- 医療の大幅な効率化（事務、重複診断・投薬等の回避、在宅受診等）と副作用による患者負担や医療費の削減、最適医療（標準治療）提供による質の向上などが期待できる。結果として、医療に対する投資対効果が向上する。
- 予防医療・個別化医療を実現できる。
- 高齢化社会での健康寿命延伸、疾病後の早期社会復帰に寄与できる。
- 安全対策に関しては、恒常的な医薬品の安全性情報のモニタリングやリスクの早期確認が可能となり、早期の安全対策の実施や適正使用の推進、副作用被害の防止が期待できる。
- 医療技術の提供の面では、臨床研究の活性化・エビデンスの創生、革新的新薬開発分野の選定、治験・臨床試験の効率化、世界同時開発への参画、また、新規治療法の開発促進などが期待できる。
- 医療情報のデータベースを構築し、その情報の二次利用を可能とすることは、医薬品の予防的安全対策の強化や最新の医療技術の提供につながる。
- 医療情報データベースから得られる統計情報に基づいて医療関連事業の効果を測ることにより、現在よりも迅速かつ客観的に、行政が事業効果を議会あるいは住民へ説明できるようになる。ひいては、税金が効果的に使われることが期待できる。
- こうした電子化医療情報の二次利用に対しては、学会・産業界からの期待も大きく、研究・医療分野への多大な貢献が期待できる。
- 「医療情報データベースの活用による医薬品等安全対策の推進」[5]においても、この基盤は利用できるものである。収集する機関も大病院のみならず、中小の診療所や保健所、また臨床検査機関等を広い範囲で想定しているため、より精度の高い有用なデータを収集する基盤となりうると考えられる。これにより、日本人に対する効果の高い医薬品開発、治療開発の可能性や、諸外国の医薬品メーカーに対する競争力が上がるものと考えられる。

（４）利用場面

＜場面 1＞

PHR の二次利用として、病院や診療所が診療データを登録し、研究機関が研究に必要な情報として連結不可能匿名化データを使用する利用場面を示す。

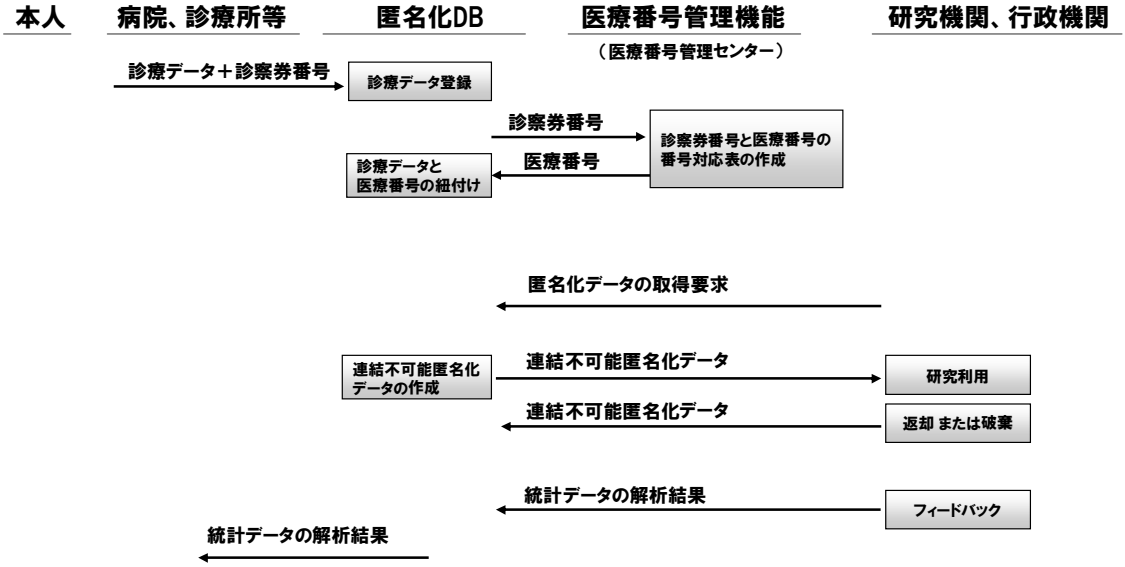


図 11　連結不可能匿名化データを使用する場合のシーケンス

- 病院、診療所等から診療データと病院での診療データ識別子（例えば診察券番号）を匿名化 DB へ送付する（匿名化 DB は仮想的な機能で、二次利用データを管理する機関がその DB 機能を有するものとする）。
- 匿名化 DB は、医療番号管理機能に診察券番号を送付し医療番号を得ることで、送付された診療データに対応する個人を一意に特定することができ、他の医療機関から送付されたその個人の診療データとマージすることが可能となる。
- 研究機関や行政機関は、統計データの解析を行う必要の都度、匿名化 DB に対して連結不可能匿名化データの取得を要求する。
- 匿名化 DB は、匿名化データから個人への追跡を行わせないために、匿名化データと個人を連結するための連結可能番号を含まない匿名化データ（連結不可能匿名化データ）を作成する。匿名化データの作成は、全データを論理的にあるいは物理的に集約してから実行する方式とする。
- 匿名化 DB は、匿名化データを格納する時には匿名化処理を実施することで匿名性の保証をする（匿名性指標には、k-匿名性[7]と l-多様性[8]を用いる）。

[7] k-匿名性：利用者情報が一つ以上の利用者を識別するための情報（住所、電話番号等。以下、準識別子）から構成されている場合に、準識別子の匿名化により、同じ準識別子が k 通り以上になることを保証する指標である。k-匿名性を満たすことによって、利用者が一人に特定されない。

- 研究機関、行政機関へは、連結不可能匿名化データが渡され、研究機関、行政機関においてデータの解析を行うことができる。
- それらの分析結果は研究や行政のデータに使われるだけでなく、病院、診療所等および国民（本人）へもフィードバックされる。

＜場面２＞

PHR の二次利用として、病院や診療所が診療データを登録し、研究機関が研究に必要な情報として情報提供者である個人の利益につながる結果が得られる可能性がある匿名化データを使用し、その結果を本人にフィードバックする利用場面を示す。

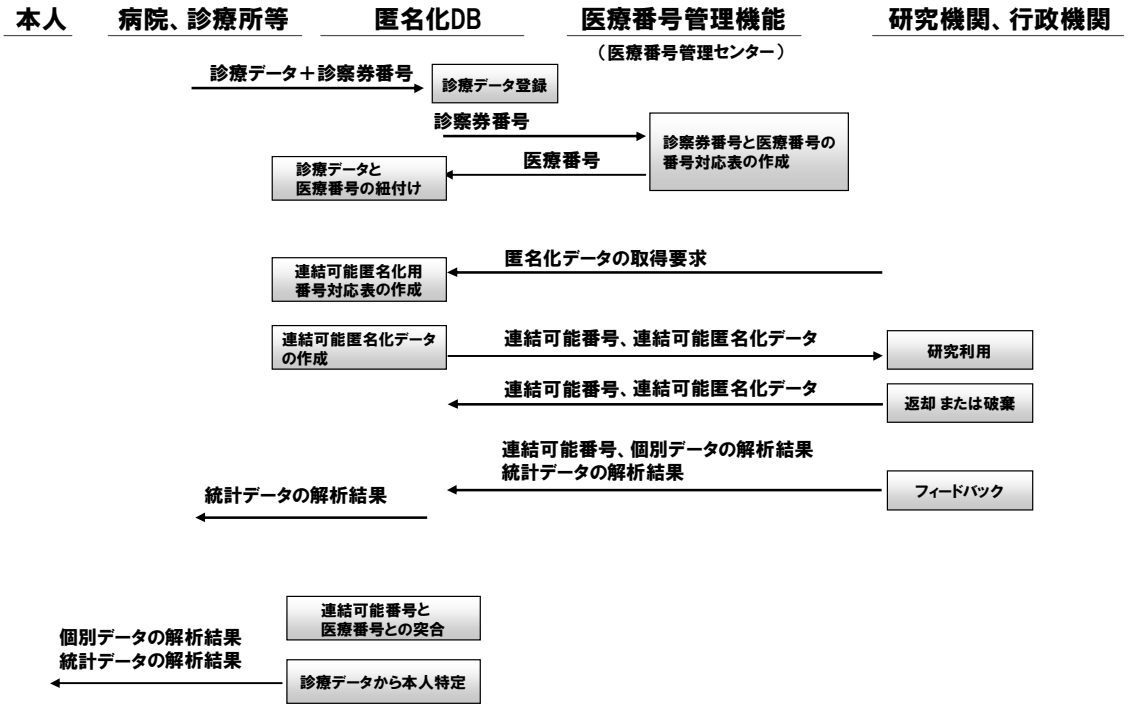


図 12　匿名化データを使用しその結果を本人にフィードバックする場合のシーケンス

- 病院、診療所等から診療データと病院での診療データ識別子（例えば診察券番号）を匿名化 DB へ送付する（匿名化 DB は仮想的な機能で、二次利用データを管理する機関がその DB 機能を有するものとする）。
- 匿名化 DB は、医療番号管理機能に診察券番号を送付し医療番号を得ることで、送付された診療データに対応する個人を一意に特定することができ、他の医療機関から送付されたその個人の診療データとマージすることが可能となる。

---

[8] l-多様性：利用者情報に機微な情報（病状、年収等。以下、センシティブ情報）が含まれている場合に、準識別子の匿名化により、同じ準識別子のセンシティブ情報が l 通り以上になることを保証する指標である。l-多様性を満たすことによって、利用者のセンシティブ情報が知られることを防止することができる。

- 研究機関や行政機関は、情報提供者である個人の利益につながる結果が得られる可能性がある場合に限り、必要の都度、匿名化 DB に対して連結可能匿名化データの取得を要求する。
- 匿名化 DB は、匿名化データから個人への追跡を可能とするために、匿名化データと個人を連結するための連結可能番号と医療番号の番号対応表を作成し、連結可能番号を含んだ連結可能匿名化データを作成する。
- 匿名化 DB は、匿名化データを作成する時には匿名化処理を実施することで匿名性の保証をする（匿名性指標には、k-匿名性と l-多様性を用いる）。
- 研究機関、行政機関へは、連結可能番号と連結可能匿名化データが渡され、研究機関、行政機関においてデータの解析を行うことができる。
- それらの分析結果は研究や行政のデータに使われるだけでなく、病院、診療所等および国民（本人）へもフィードバックされる。
- 解析の結果、ある特定の個人に重要な病気が発見される等により本人に通知が必要な場合は、匿名化 DB を通して連結可能匿名化用番号対応表により本人を特定しその個人に情報を通知可能である。

４－１－４．医療分野における提言と課題および施策

（１）医療分野における提言

散在している医療および健康関連情報を、個人番号により正確に紐付けることにより、無駄のない適切な医療の実現や、医療や新薬等の研究開発を活性化することで、国民の健康に寄与すると同時に、医療費抑制の効果を見込むことができる。このような医療情報の利活用を推進するクラウドコンピューティング基盤の早期実現を提案する。

このようなクラウドコンピューティング基盤の実現においては、様々な技術的、制度的な課題が想定されるが、技術的な課題は実証実験と新技術開発を実施しながら、実現可能を早期に見極め、一刻も早く IT による社会基盤を実現し、他国に追いつくことが必要だと考える。同時に漏洩問題が危惧される医療関連情報の取り扱いに関して、利活用可能かつ国民保護を保障する合理的な制度の検討を進める必要がある。

医療関連情報を紐付けるために必要な、個人番号および国の情報の民間活用に係る制度、およびそれらの管理運用を担うと想定される施設については「官」で、国民への利便性の高いサービスの実現は「民」で、さらに実現にあたっての知識、造詣はこの分野の有識者である「学」で、という産学官連携で進めて行くことが必要である。

（２）技術的課題と施策

- 電子化された医療関連情報の作成・保存・流通に関して、医療情報の見読性、完全性、個人認証方法の方式についての検討（カード認証、生体認証など）が必要である。
- 電子カルテシステムの導入や、医療情報をデータベース化するシステムの医療機関への導入、セキュアなインターネット環境の提供が必要となる。

- 医療情報データベースの実現に際しては、情報活用のベネフィットとリスクを踏まえた制度設計、導入すべき情報セキュリティ技術の選定が必要となる。
- 匿名化、セキュリティ、運用体制、医療情報の電子化の促進、データベースの標準化と変換基準の開発・普及が必要である。
- PHR の情報を管理するための公的データセンターの整備や、個人情報を収集する仕組み（分散 DB 連携）が必要である。
- 識別子を削除する、というレベルでの医療データの匿名化処理、いわゆる「連結不可能な匿名化」は実施されているが、識別子ではない複数の情報の組み合わせにより個人を特定できてしまうリスクへの配慮がなされていない。このようなリスクに対処するには、組み合わせにより情報が推測されないレベルまで、情報の粒度を粗く、抽象化して提供するといった仕組みが必要である。
- 一人の患者が複数の医療機関にかかっている場合、複数の医療機関のデータ間で同一患者のデータを関連付けることで、より多角的なデータ解析ができる。しかし、複数の医療機関で蓄積されているすべての医療情報を統合するということは、特定の患者のすべての情報を個々の医療機関に知られてしまう可能性がある。さらには、患者の一部の情報が漏洩した場合、より多くのプライバシー情報の漏洩につながる危険性が高い。したがって、個人が特定されないようにして複数の医療機関のデータを連携・統合できる仕組みが必要である。
- 同一人（患者）の医療情報を統合するための個人番号の基盤の整備が必要であり、かつ個人番号の連携規約と連携情報標準化も必要となる。
- 個人の医療・診療情報が保険の給付金請求以外の目的に利用されないための対策も必要である。

（３）制度および慣習に基づく課題と施策

- 医療情報の収集や二次利用に対する医師、国民からの理解を得る必要がある。特に、患者のプライバシーへの配慮が不可欠であり、まず社会的コンセンサスの形成が前提となる。その上で、医療情報の二次利用や個人を識別する情報の第三者利用に関する法令、ガイドラインの整備が必要となる。実際に情報を収集・活用するにあたっては本人同意の取得方法についての検討も必要である。
- 医療機関が管理する医療情報に個人番号を付与するような法令、ガイドラインの整備が必要である。
- 個人情報保護法および関連法令と、医療情報データベースの関係の明確化が必要である。
- 医療情報データベースの構築、運用にかかるコストをどのように分担するかについての検討が必要である。
- 健診カルテと病院カルテの連携が可能な標準化の整備推進が必要であり、また標準化普及のために、標準化に対応した健診システム、電子カルテシステム等への助成措置の実施が必要と考えられる。

- 医療情報を集約するためには、医療情報を持っている医療機関や患者自身がその情報を出すことに意義を持ち、情報提供したことに対するインセンティブ（例えば、患者にとっては高度な治療が得られる、治療費が安くなる等の、病院にとっては診療報酬を高く設定する等の直接的なメリット）が得られるようにするか、社会制度として強制的に情報を集められるようにすることを考えないと、十分な情報の集約は難しい。

４－２．製品安全分野のサービス

製品の所有・使用情報のポインタ[9]を「製品安全センター」で一元的に管理し、製品の所有・使用情報を製品リコール対応、事故未然防止、保守継続性、製品リユースにおける品質管理・保証などの、製品の安全性の確保および安心を増すためのサービスに利活用する。具体的には、下記のサービスを実現する。

- 製品リコール対応
- 事故未然防止
- 保守継続性
- 製品リユースにおける品質管理・保証

本ユースケースでは、下記の三種類の識別番号が必要となる。

- 個人番号：個人を識別する番号。製品の所有者が個人の場合の識別に使われる。
- 法人番号：法人を識別する番号。製品の所有者が法人の場合の識別に使われる。
- 製品番号：製品を識別する番号。製品番号に関しては、ISO（ANSI）や GS1 でシリアル番号が決まっており、グローバルでのユニーク性を確保されている（発番機関コード＋国コード＋企業コード＋製品コード＋シリアル番号）。
- 間接認識番号：間接的に個人番号あるいは法人番号を特定できる番号。具体的には、クレジットカード番号、免許番号、韓国の i-PIN（参考資料）などであり、間接識別番号管理者に問い合わせることで、個人番号あるいは法人番号を取得できる。

本ユースケースを実現するためのシステムは以下の構成要素が必要である。

- 製品情報管理機関

  製品情報管理機関は製品を製造したメーカー、保守専門業者、リサイクル業者などである。また輸入製品等について国内で管理体制を維持できない場合など、その機能をアウトソーシングできる情報管理専門業者もあると仮定する。製品情報管理機関は、製品番号で識別される製品の所有者の情報（個人番号、法人番号、あるいは間接認識番号）およびその製品の使用状況や保守／修理に関する情報（以下「製品情報」と呼ぶ）を保有する。その情報は、製品安全センターの指示があった場合に開示、移管しなければならない。また、所有者から情報削除要請があった場合には削除しなければならない。製品情報管理機関は、製品安全センターから認証を受ける必要がある。
- 製品安全センター

  製品安全センターは、製品に付けられた製品番号から、その製品に関する所有・使用情報がどの製品情報管理機関にあるかのポインタ情報を持っている。メーカーやサービス業者から、製品情報の開示要請があった場合に、その妥当性を判断し、製品情報管理機関に開示・移管を指示できる。さらに、個人番号・法人番号管理センターに問い合わせ、製品所有者の現住所を取得、製品情報管理機関に開示できる。また、製品情報管理機関の認証も行い、認証された製品情報管理機関が持つ

[9] ポインタ：情報がどこにあるかを示す情報。

製品情報へのポインタ情報を一元管理する。

製品安全センターはリコール対象製品の一覧や、企業別のリコール発生件数を取りまとめる機能も有する。現状では、各企業の Web サイトでリコール製品の情報を個別に情報発信しているが、企業毎に分かれて開示されても、製品利用者個人としては不便である。企業横断的な情報は、消費者庁（リコール情報ポータルサイト）や国民生活センターが独自に企業の発信した情報を収集し整理しているが、優良企業が自主的に製品不具合情報を開示する場として製品安全センターを活用できれば、個人・法人双方にとってメリットがある。

- 個人番号・法人番号管理センター

個人番号・法人番号管理センターは、個人番号・法人番号と現住所など基本情報を紐付けるための情報を持っている。製品安全センターの要請に基づき、基本情報を提示する。

図 13 に、システム構成を示す。

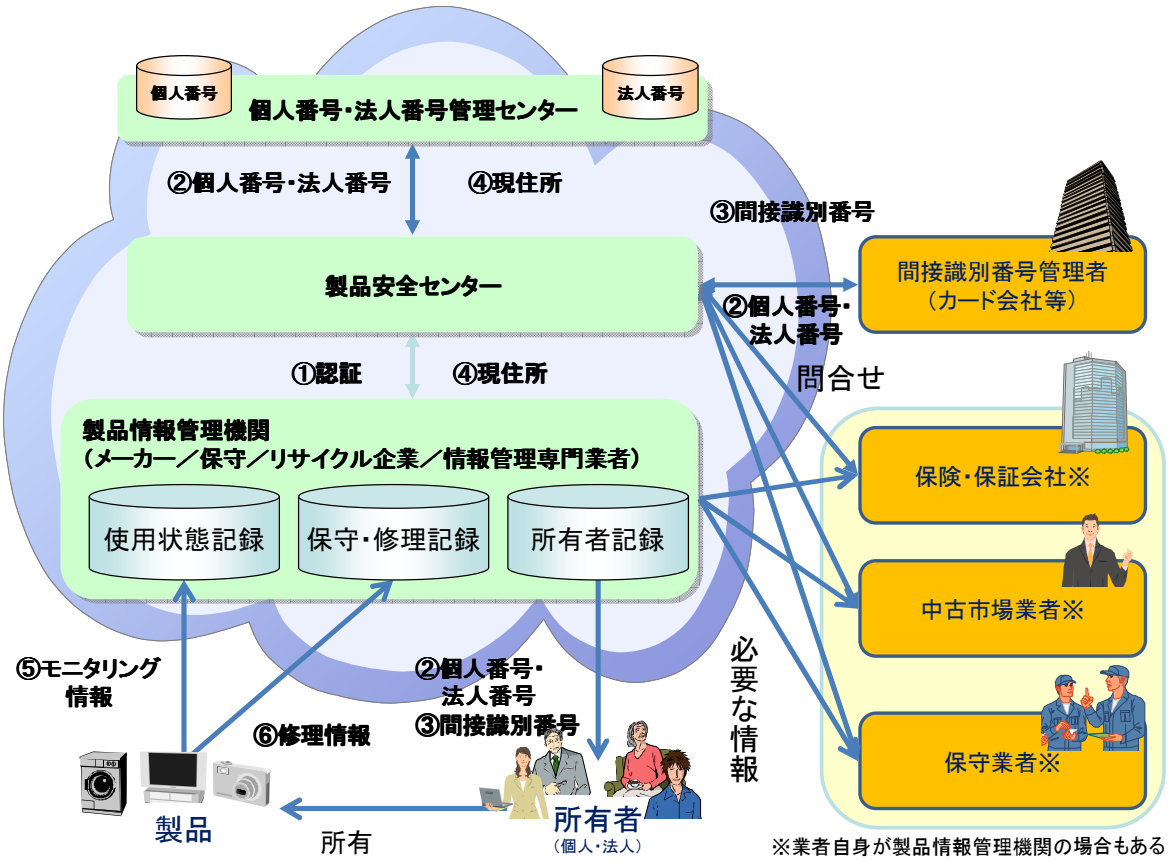


図 13　製品安全のシステム構成

ここで、2010 年 10 月時点での製品所有・使用情報の管理に関する既存の取り組みについて以下に示す。以下に示すユースケースの作成に関しては、これらの既存の取り組みを参考にしつつ、番号制度の利活用の視点を組み込んだ。また、ユースケースの実現にあたっては、これらの既存の取り組みと連携することが望ましい。

- 家電電子タグコンソーシアム（家電コンソ）[21]

　家電の電子タグの標準化を目的として、2005 年に家電電子タグコンソーシアムが設立された。構成員は大手家電メーカー各社で、事務局はみずほ情報総研である。電子タグ運用指針第一版（2006 年）、第二版（2008 年）を作成しており、2010 年度に第三版を完成させ、コンソーシアムは終了予定となっている。

　電子タグの利用が前提で、製品のライフサイクル[10]の管理の効率化を目的としている。なお、製品のライフサイクルでの電子タグのユースケースに関しては、電子タグ運用指針第二版にて詳細に検討されている。また、電子タグの国際標準化組織「EPCglobal」とも連携し、国際標準化を目指すとしている。

- 電気・電子情報連携推進協議会（IPPC）[22]

　電気・電子業界の製品安全・消費者保護・環境・リサイクル対策のための、企業・業種・業界の壁を超えた情報共有のインフラ整備を目的として、2007 年に設立された。2010 年度に最終報告をまとめ、完了する予定である。現在、会員数 38。事務局は（財）家電製品協会である。

　製品安全部会、製品リサイクル部会、製品含有物質部会とシステム技術委員会から構成される。2010 年度は、製品トレーサビリティ部会と製品安全部会に再編し、報告書をまとめる。特に、製品安全部会では製品所在把握と事故未然防止の検討を行っており、本ユースケースでも製品安全部会の検討結果を参考にした。

　事故未然防止に関しては、製品リコール回収率の向上や事故の再発防止を目的に、通信ネットワークを介してリコール情報を対象機器に直接通知する「リコール情報告知システム」の検討を行っている。

　製品所在把握に関しては、リコールなどの有事の際にメーカーや販売店が所有する情報を交換する「製品ライフサイクルトレースシステム」の検討を行っている。また、製品ライフサイクルトレースシステムとリコール情報告知システムとの連携が必要となるとしている。

４－２－１．製品リコール対応

（１）サービス概要

　製品リコールが発生した場合に、製品情報管理機関が、製品安全センター経由で製品の所有者（個人、法人）の住所を迅速かつ正確に把握でき、製品リコール情報を製品の所有者に通知できる（以下の箇条書きに登場する丸数字は、図 14 に記載のものに対応する）。下記の例ではメーカーを製品情報管理機関としたが、家電量販店などの販売店を製品情報管理機関とし、販売店がメーカーの依頼を受けて製品リコール情報の通知を行う場合もある。

- メーカーは製品安全センターから製品情報管理機関としての①認証を取得する。認定が得られないメーカーは、専門の製品情報管理機関に製品情報管理を委託することが可能である（製品情報管理専門業者のクラウドサービスを利用すると考えることもできる）。

[10] 製品のライフサイクル：生産、物流、在庫管理、修理、リサイクルの流れ。

- メーカーは販売時に②個人番号／法人番号または代替の間接識別番号を取得する。その際、製品安全センターで登録内容の確認をするか否かを明示（例えば、記入された個人番号と氏名が一致しているかの確認のみ行う。IC カードのように電子化されていれば不要）する。
- 事故発生・リコールなどの有事の際に、メーカーは対象機器の使用者の③のリストを製品安全センターに送付する。
- 製品安全センターは、④に関しては間接識別番号管理者に問い合わせ、⑤個人番号／法人番号を取得する。
- 製品安全センターは、⑥のリストを個人番号・法人番号管理センターに送り、⑦現住所を入手し、メーカーに提示する。
- メーカーは⑧現住所に基づき使用者に⑨事故発生・リコールの内容を通知する。

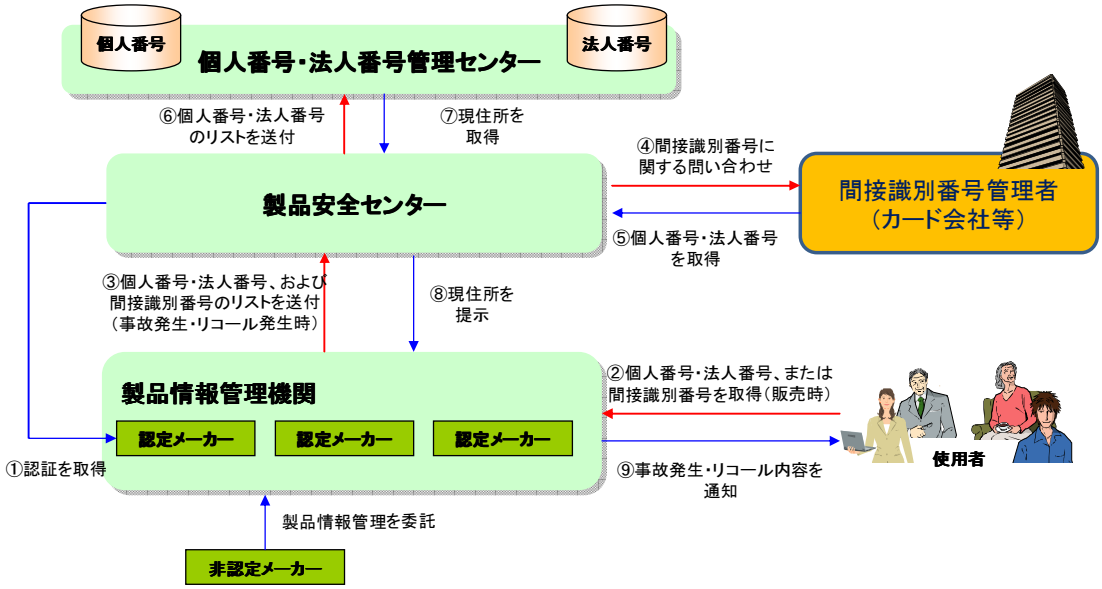


図 14　製品リコール対応のユースケース

（２）背景と目的

製品リコールや自主回収の時には製品の所在を把握する必要がある。特に、人命に関わる不具合が発生する可能性が高く、製品の所在が確認できない場合には、国内全戸に郵便物で通知するなどの対応を行う事例も発生している。

製品情報管理機関と製品安全センターが連携することで製品所有者の割り出しが容易となり、製品リコール対応の効率化が期待される。また、様々な理由でメーカーが製品リコール対応できない場合も、製品情報が販売店等で管理されていれば行政側で対応することも可能となる。

（３）メリット

現状の製品の所在把握率は必ずしも高くない、把握されていても一元管理されていない、などの理由で製品リコールや自主回収が不十分となりリコール後も事故が発生する場合がある。本ユースケースは、製品所有者にとって事故のリスクを低減できるメリットがある。同時に、メーカー側の製品リコールや自主回収のコストを大幅に削減できる。

４－２－２．事故未然防止

（１）サービス概要

不具合による製品リコールや商品回収ではない場合でも、メーカーが設計時に想定していなかった長期間の利用や悪環境での利用により火災等の人命に関わる事象が発生する場合がある。製品の使用状況を製品情報管理機関がモニタリングし、リスクを未然に通知することで事故の未然防止ができる(以下の箇条書きに登場する丸数字は､図 15 に記載のものに対応する)。

- 製品がインターネットや電話回線等のネットワークで常時あるいは定期的に接続されていることを前提とする。また、製品の固体毎にユニークな「製品番号」があるとする。
- 製品情報管理機関は、インターネットや電話回線経由で製品の使用状況をモニタリングする[11]。
- 製品が危険な状況にある場合には、ネットワークで接続された製品上でなんらかの表示を行うとともに、製品安全センターに①通知し、使用者の②現住所を獲得する。
- メーカーは現住所に基づき使用者に事故発生・製品リコール・商品回収の③内容を通知する。

[11] スケーラビリティの観点から、製品情報管理機関側のサーバーにおけるモニタリング情報の縮約技術が重要となる。また、製品内部にビルトインテスト機能を持たせ、診断結果のみを送信する方法も有効である。

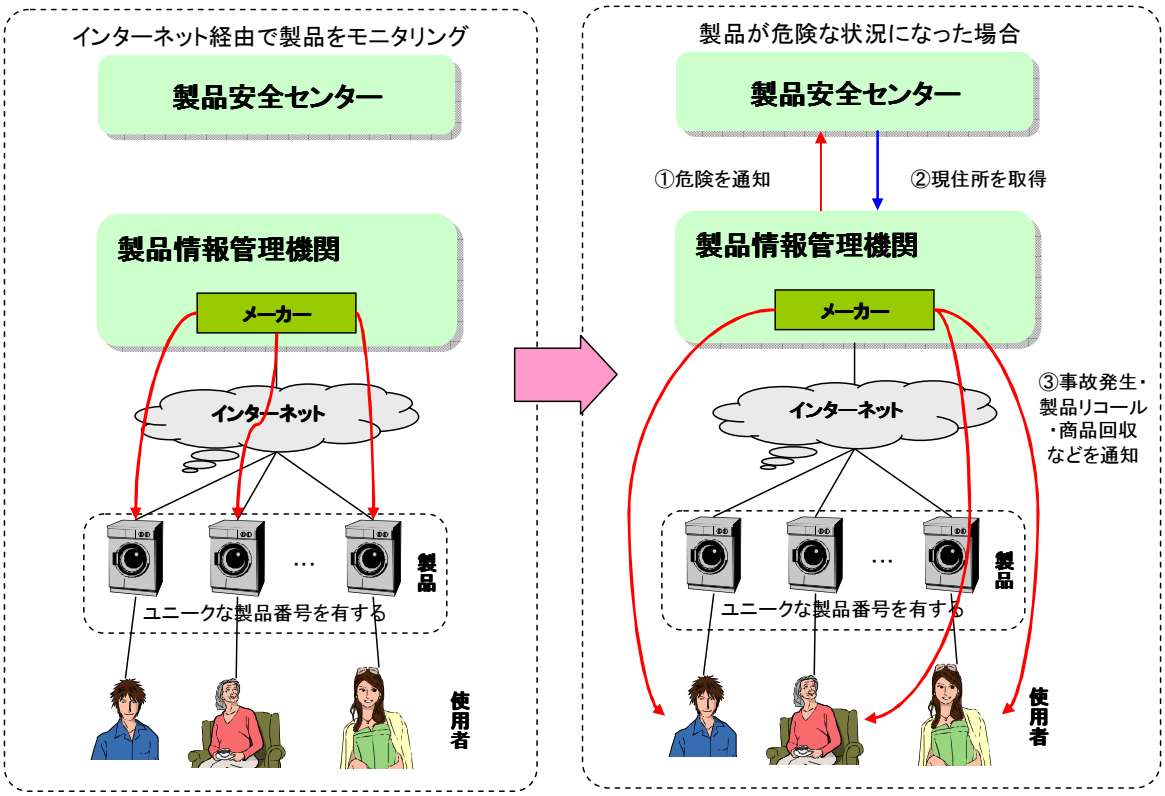


図 15　事故未然防止のユースケース

（２）背景と目的

不具合による製品リコールでない場合でも、設計の想定外の長期間の利用や悪環境での利用により火災等の人命に関わる事象が発生する場合もある（湯沸器、乾燥機、扇風機などの例）。最近は耐用年数などを表示するようになっているが（長期間使用製品安全点検・表示制度）、一般家庭では必ずしも耐用年数が厳守されるとは限らない。

製品番号により個々の製品をモニタリング可能とすることで、利用方法に関わらず、事故を未然に防ぐ効果が期待される。

なお、遠隔の製品モニタリングは、業務用の機器では従来から行われてきたが、インターネットの普及により近年はコンシューマ機器（パソコン、テレビ、掃除機など）でもモニタリングが可能になってきている。今後は、スマートグリッドの普及に伴い、製品が省エネ制御などの目的でネットワークに常時接続されるようになり、製品モニタリングの環境は一層整備されることが予想される。

（３）メリット

製品所有者にとって事故のリスクを低減できるメリットがある。メーカー側は、製品事故を未然防止できると同時に、製品の使用状況を把握し、より安全な製品の設計にフィードバックできる。また、ネットワーク経由での製品上での表示だけでは、製品の設置場所などによっては製品所有者が気付かないなど、通知が不十分な可能性も考えられる。この点について、個人番号・法人番号を用いた現住所への通知により、より確実な通知を担保することができる。

４－２－３．保守継続性

（１）サービス概要

製品を中古で転用する場合、メーカーと異なる保守専門業者が保守を行う場合、また保守業者が変わる場合、必要な保守情報を継承することで継続性のある品質管理ができる。

保守業者が変わる場合などは、使用者の了解の下、製品安全センター経由で製品情報管理機関から必要な情報を引き継ぐ。製品情報管理機関は、製品安全センターから指示があった場合には、所定の製品情報を渡さなければならない。製品毎に引き継ぐべき情報は、業界団体と製品安全センターで決定する（以下の箇条書きに登場する丸数字は、図 16 に記載のものに対応する）。

- 保守業者が変わる場合、①保守の引き継ぎが必要になる。新しい保守業者は、製品所有者の了解の下、製品安全センター経由で製品情報管理機関（以前の保守業者の場合が多い）から③必要な使用／保守／修理情報（必ずしもすべての情報ではない）を引き継ぐことができる。
- 製品情報管理機関は、製品安全センターから指示があった場合には、②所定の使用／保守／修理情報を新しい保守業者に渡す。
- 新しい保守業者は、引き継いだ使用／保守／修理情報を活用して④適切な保守を行う。実施された保守情報は製品情報管理機関（新しい保守業者自身の場合が多い）に登録される。

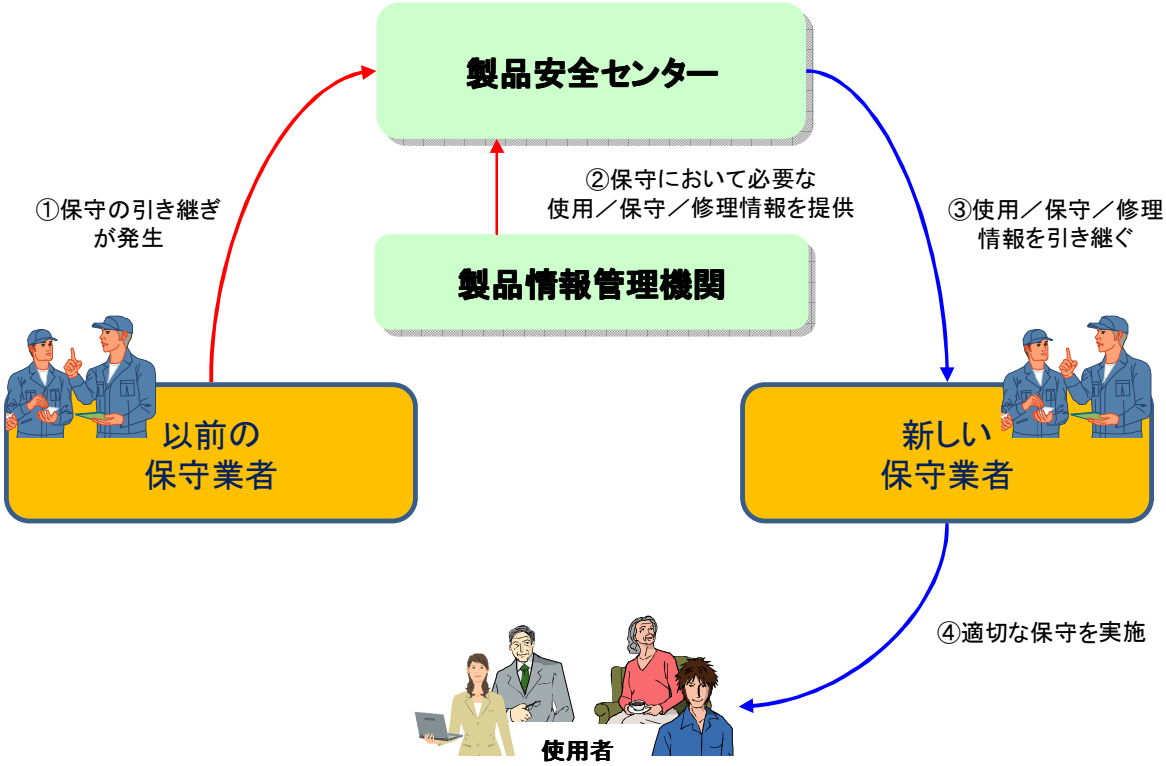


図 16　保守継続性のユースケース

（２）背景と目的

製品を中古で転用する場合、メーカーと異なるメンテナンス専門業者が保守を行う場合、また保守業者が変わる場合、現状では保守情報が継続されないケースがあり、十分な品質管理ができないことがある。

製品安全センター経由で製品情報管理機関から必要な情報を引き継ぐことにより、中古製品の保守継続性を担保できるようにする。

（３）メリット

製品所有者にとって、適切な保守を継続的に受けることができ、事故のリスクを低減できるメリットがある。保守業者側は、製品の使用や修理状態に即した効率的な保守（Condition Based Maintenance）を実施できる。

４－２－４．製品リユースにおける品質管理・保証

（１）サービス概要

自動車の中古市場やリサイクルショップなどで外観だけでは中古製品の品質が見積もれない場合でも、中古市場業者が製品情報管理機関から入手した使用／保守／修理情報（一種の保証書）を確認することで、正確な中古製品の評価ができ、リユースを推進できる。

製品が中古市場やリサイクルショップで取引される場合は、使用者の了解の下、中古市場業者が製品安全センター経由で製品情報管理機関から必要な情報を入手し、適切な価格を算出するとともに、製品情報と一緒に売買する。

さらに、使用情報を確認することで製品の状態を正しく評価でき、三年間無償修理保証などの保険・保証サービスを合理的な価格で受けることができる。すなわち、保険・保証会社は、使用者の了解の下、製品安全センター経由で製品情報管理機関から必要な情報を入手し、合理的な保険・保証料金でサービスを提供できる（以下の箇条書きに登場する丸数字は、図 17 に記載のものに対応する）。

- 製品が中古市場で取引される場合は、使用者（旧所有者）の了解の下、中古市場業者が製品安全センターへの①問い合わせを行い、その製品の②使用／保守／修理情報を管理している製品情報管理機関を特定する。使用者の了解を得るために、個人番号・法人番号による現住所確認が必要な場合もある。
- 製品情報管理機関から必要な③情報を入手し、④適切な価格あるいは価格決定の参考になる品質指標（優／良／可などの品質ランク、品質項目のチェックリストなど）を提示し、売り手および買い手に提示する。
- 売買時には使用／保守／修理情報も新しい所有者（あるいは所有者が依頼した製品情報管理機関）に引き継がれる。
- 売買が成立した場合には、製品情報管理機関に新しい所有者が個人番号・法人番号、もしくは間接識別番号とともに登録される。

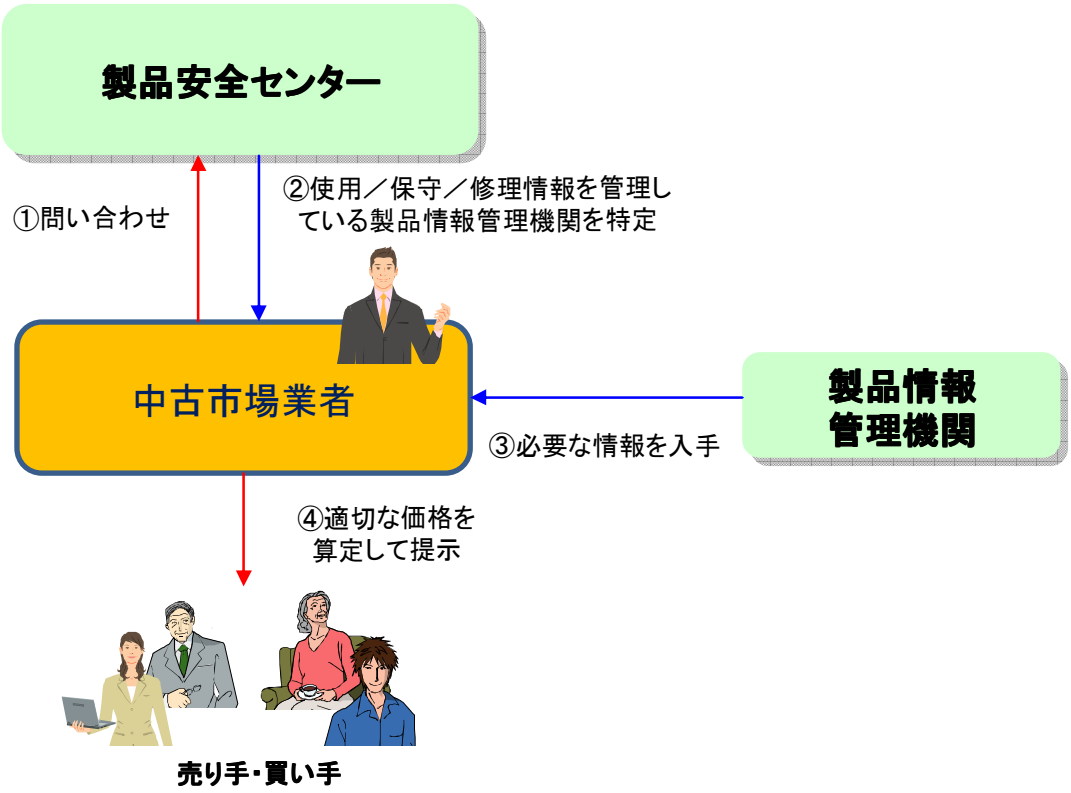


図 17　製品リユースにおける品質管理・保証のユースケース

（２）背景と目的

中古市場・リサイクルショップや保険・保証サービスなどで外観だけでは品質が見積もれない場合、製品品質に関するモラルハザードが発生し、リユースや保険・保証サービスが適切に運用できない場合があった（レモン市場問題）。

（３）メリット

製品情報管理機関から中古製品の情報を提供することにより、中古製品の適正な評価や品質保証を可能とすることで、製品購入者が安心して購入でき、中古市場の活性化が期待される。また、情報提供に付随して、売買時の所有者情報の移行管理もできる。中古市場の活性化は、地球環境問題にも良い影響を与える。

４－２－５．サービスを実現するにあたっての課題と施策

（１）技術的課題と施策

- 製品所有・使用情報に関する標準化が必要である。標準化は、すべての製品に共通な部分と、業界や製品毎に異なる部分があると思われる。このため、業界団体との連携が必要である。特に、製品使用状態モニタリングに関しては、スマートハウス／スマートグリッド関連の標準化への提案も必要である。

- 多量の時系列データの収集・蓄積・分析技術が必要である。特に、製品使用情報をモニタリングする場合のスケーラビリティの確保が課題である。
- モニタリングデータなどから事故を未然防止するための異常検出、故障・事故予測技術の開発が必要である。
- 保守や修理情報から製品の品質の劣化を推定し、中古市場における売買の参考にする品質ランク（場合によっては適正価格）を算出する技術が必要である。

（２）制度および慣習に基づく課題と施策

- 製品安全センターおよび個人番号・法人番号管理センターは、公平性および信用性が重要であり、公的機関が運営することが望ましい。製品安全に関する情報収集や広報に関しては、消費者庁、国民生活センター、国土交通省自動車交通局技術安全審査課、独立行政法人製品評価技術基盤機構などで行われている。製品安全センターとこれらの機関との関係を整理する必要があるとともに、民間側の製品情報管理機関とのインターフェースの確立が必要である。
- 自動車やエレベータ等の法定点検など安全確保の視点から義務化されているものは適用可能だが、法的制約のない一般の家庭製品所有者が情報を登録するインセンティブを与えられるかは課題である。特に、製品を譲渡・転売した場合の新しい所有者による登録はトレーサビリティ確保のために必要である。製品安全に関する「権利」と「義務」の関係を整理し、場合によっては法制度を変える必要もある。
- 家電メーカーや販売店等が自社ユーザ DB を構成し、アフターサービスに活用するのは営利活動であり、そこに公的な機関を経由して個人情報を紐付けるためには合理性が必要である。
- 製品の所有・使用情報は個人情報・企業情報であるが、どのような場合の共有が許容されるかに関するプライバシー保護の議論が必要である。
- 製品の所有・使用情報を共有することでメーカーの競争力が低下するという危惧に対してどのように答えるかが課題である。
- 製品情報管理機関が倒産等で消滅した場合の対応が課題である。間接識別番号の場合も、クレジット会社との契約が切れると無効になってしまい、トレーサビリティが途切れる可能性がある。
- 個人番号は住民基本台帳をベースに考えられるが、法人番号は現状では、登記所の「会社法人等番号」、電子商取引推進センターの「標準企業コード」、流通システム開発センターの「JAN 企業コード」、帝国データバンクや東京商工リサーチの企業 ID などがあり、国際的にも、GS1（Global Standard One）の企業コード（GLN: Global Location Number）などがあり統一はされていない[12]。IT 戦略本部の国民 ID に関する工程表においても、「企業コードの導入」は、2011 年度までに課題抽出と制度整備を完了するとしている。政府

[12] ISO6523 や UN/EDIFACT3055 等で、企業コードのユニークなナンバリングの仕組みはあるが、現状は、1 つの企業がコード発行機関ごとのユニークな企業コードを持っている状況である。

の「社会保障・税に関わる番号制度についての基本方針（案）」では、法人番号は「会社法人等番号」をベースにし、付番機関の所管は国税庁としているが、製品所有者の所在把握の視点で十分かの検討が必要である。また、製品番号の企業コードとの整合性を取る必要性の検討も必要である。

- どのような事態が発生した場合（リコールなど）に製品安全センターが対応するかの判断基準とその担保方法（例えば、経済産業省に届け出たリコールについてのみ問い合わせる、など）についての検討が必要である。また、リコール関連法令（消費生活用製品安全法、電気用品安全法、道路運送車両法、ガス事業法、液化石油ガスの保安の確保及び取引の適正化に関する法律）との整合性、さらには関連法令の改定が必要である。
- 携帯音楽プレーヤーと石油ファンヒーターでは、危険度が異なるが、このような製品の特性によって、個人番号や法人番号との関連付けに関しての考え方を変えるのかどうかの検討が必要である。
- 製品所有・使用情報の管理は、参入障壁（製品所有・使用情報の管理ができない製品の締め出し）となる場合もある。国際競争力の視点からの検討が必要である。
- 個人番号・法人番号管理センターに関しては、他のユースケースと共通フレームワークとして提言する。
- 製品の所有・使用情報のポインタを管理する公的な製品安全センターを設立する。製品安全センターの運営形態としては、国民生活センターと同様の独立行政法人化が考えられる。
- 製品安全に関する法律には製造物責任法（PL 法）に加えて電気用品安全法や道路運送車両法など各種リコール関連法令がある[32]。今回の新しい仕組みに関して、既存の製品安全に関する「権利」と「義務」の関係を整理し、場合によっては法制度を変える必要もある。

４－３．金融分野のサービス

個人が金融機関と取引をするときに、本人確認や各種証明書の入手や提示など、行政が発行する証明書や本人確認書類を必要とする場面が存在する。また、金融機関も、契約者による行政機関への証明書の提出などのために、契約者に証明書を送付している。こうしたやり取りは、手続きの際の個人の手間になっていることに加え、金融機関においても多くの業務負荷や郵送料等の業務コストの負担となっている。個人－行政－金融機関（－勤務先）等の間で、個人情報を安全にやり取りできるようになることで、個人の利便性の向上、民間企業の業務効率向上、新たなサービスの実現が期待される。

具体的には、個人と金融機関とのやり取りは、犯罪収益移転防止法や預金保険法などの法制度によって厳格な本人確認や現況確認が実施されている。本人確認や現況確認のために、本人であることを証明する書類や現在の氏名や住所を証明する書類について、主として行政機関が発行する免許証や住民票などの証明書が活用されている。また、税務申告や契約時においては行政機関への証明書の提出や行政機関が発行する各種書類が必要となる。こうした各種証明書を入手し、提出する作業は、金融機関窓口と役所を行き来せざるを得ず、個人にとって負担となっている。また、民間の終身年金保険などの金融商品においては、毎年の現況確認届の提出が必要なものもあり、こうした手続きを忘れたために、保険料が払われないなど、個人にとって不利益が発生している。一方、金融機関も契約者との契約内容に基づく義務の履行のために、本人確認業務や契約内容の確認業務を強化しており、業務上の負荷増加につながっている。

個人の本人確認や現況情報の確認、さらに各種証明書のやり取りにおける負荷軽減を図ることで、契約者の正確な権利の履行、利用者、および企業の負荷軽減が期待される（図 28）。

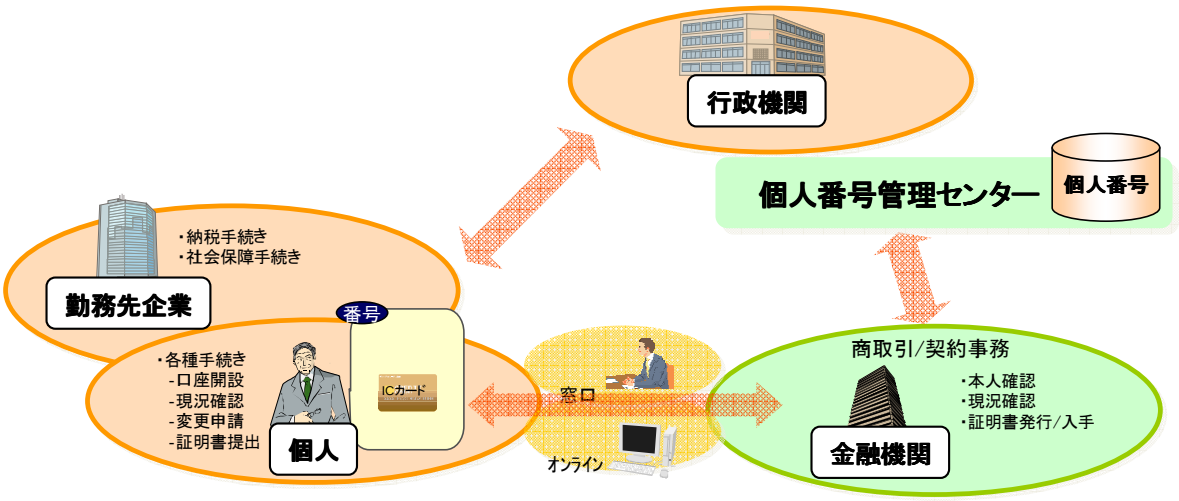


図 18　ユースケースの全体像

４－３－１．本人確認

（１）サービス概要

個人の口座開設時の本人確認において、窓口での ID カード提示および金融機関によるその写しの取得（コピー）や、郵送での本人確認が可能な書類のコピーなどの送付が行われている。それに代わり、ID カード提示や ID のネットワーク認証などにより、紙のやり取りやコピーの送付を行うことなく確実な本人確認を実施する。また、データとして本人確認結果を取得することにより、バックオフィスにおける本人確認書類の保管等の業務負荷軽減を図る（図 19）。

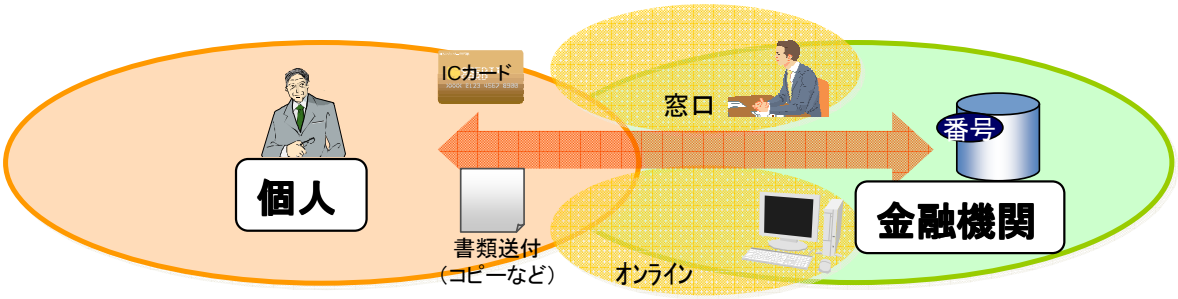


図 19　本人確認のユースケース

（２）背景と目的

近年、マネーロンダリングや振込み詐欺等の防止に向けて、金融口座開設時の本人確認業務が厳格化され、口座開設や契約手続きにおいて、運転免許証や健康保険証、パスポート、住民基本台帳カード（氏名、住所、生年月日の記載があるもの）などの本人確認が可能な書類の提示が必要となっている。口座開設等の取引時に本人を確認できる書類を提示する必要があるが、運転免許証を返却した高齢者などは、常時携帯できる本人確認が可能な書類等がないため、住民票の取得、提出などが必要となり、行政機関と金融機関双方に行く必要があるなど不便な状況となっている。

一方、金融機関においても、窓口における書類の確認および、その写し（コピーや番号の記載）の取得、管理が必要となっており、窓口およびバックオフィスにおける作業負荷の増大につながっている。

本人確認を円滑に実施できるインフラがあることで、個人の本人確認にかかる手間の解消および金融機関の業務効率化につながることが期待される。

（３）メリット

個人側のメリットは以下となる。

- 口座開設時の個人の本人確認書類の携帯の不便性の解消
- 本人確認書類を所持しない個人が、住民票等の行政機関発行の証明書を取得、提出する手間の解消

金融機関側のメリットは以下となる。

- 窓口における本人確認業務の時間短縮
- バックオフィスにおける本人確認書類の管理事務の削減
- 本人確認の確実性の向上

（４）利用場面

本人確認は、金融機関における口座開設時や新規契約時、各種取引において法令もしくは監督官庁のガイドラインに定められている。

図 20 に概要を示す。

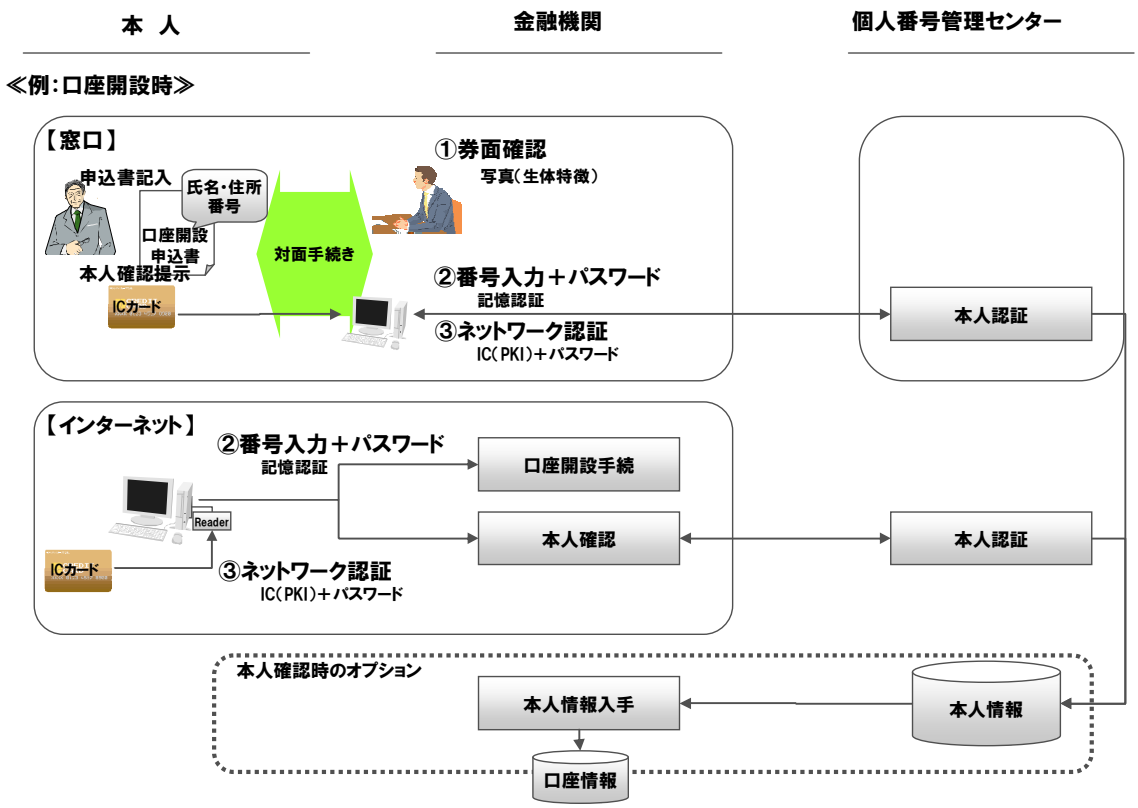


図 20　本人確認の概要

金融機関における本人確認を求めている法令には、犯罪収益移転防止法（マネーロンダリング法）、預金保険法（ペイオフ法）などがある。犯罪収益移転防止法では、振り込め詐欺等の犯罪において本人の不特定な口座が利用されるのを防ぐことを目的としている。預金保険法では、ペイオフの発動において、顧客の預かり資産である口座を確実に顧客に戻すため、および、ペイオフの対象を特定するために、同一本人の名寄せにより複数口座を有する個人の資産を合算することを目的としている。このため、金融機関では、口座開設や新規契約時に本人確認書類の提示を顧客に求めている。

本人確認では、複数のバリエーションが考えられる。ここではいくつかの代表的な場面を抽出し、それぞれの場面による必要機能の割り出しを行うこととする。

（ア）身分証となるカード媒体を利用した場合

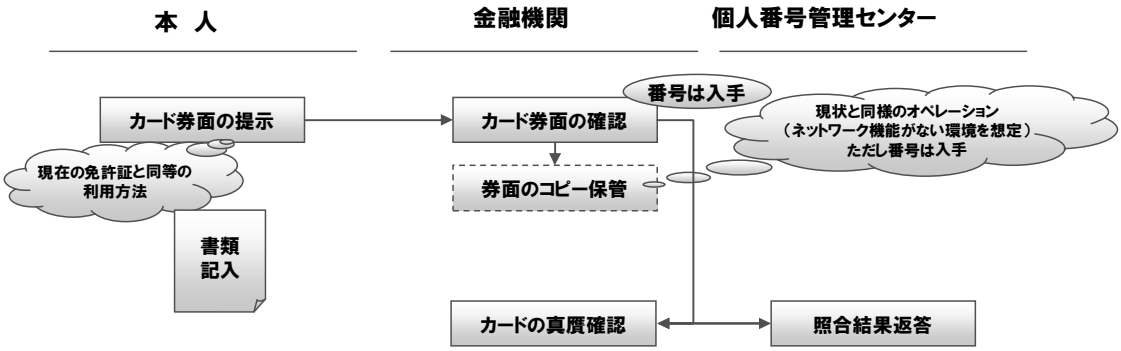


図 21　本人確認のシーケンス（オフライン）

①ID カードにより窓口で本人確認を行う

- 公的機関が発行したカード媒体の券面に本人を特定する生体特徴（写真等）や氏名、住所が記載されていること
- カードの偽造対策として、カードの真贋確認が行える仕組み

（イ）個人番号＋パスワード認証を利用した場合

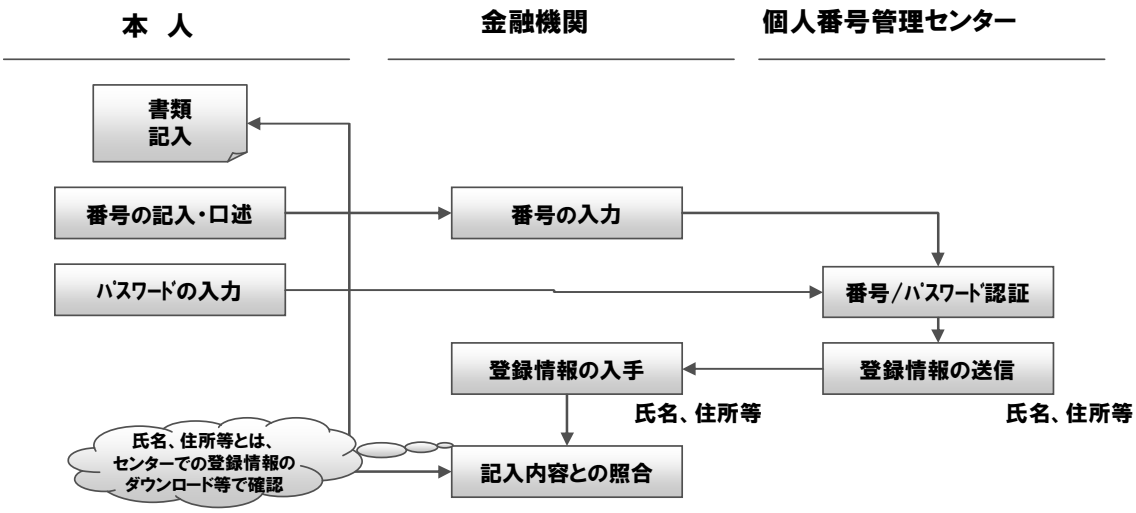


図 22　本人確認のシーケンス（個人番号とパスワード使用）

①番号の記入・口述を行い、クレジットカードのパスワード認証と同様、本人の入力が他人に分からない状態でのパスワード入力を行う

②番号＋パスワードの照合結果によって本人であることを確認する。また、本人であることが確認されると、あらかじめ登録してある氏名、住所等の情報が表示される

- この際、氏名、住所は最新のものである必要がある

（ウ）本人が番号管理センターを通じて本人確認情報を金融機関に提供する場合

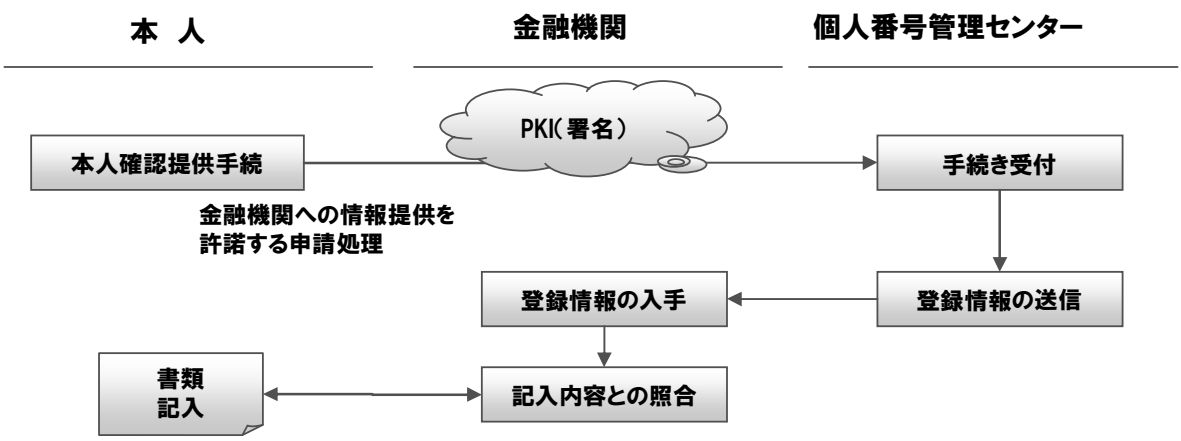


図 23　本人確認のシーケンス（PKI 使用）

①本人が金融機関で個人番号管理センターにアクセスし、本人確認を行った上で、本人の情報を金融機関へ提供するよう依頼する

②個人番号管理センターは、本人の依頼に基づき、当該金融機関へ本人の情報を開示（もしくは送付）する

４－３－２．現況確認

（１）サービス概要

個人が、契約先の金融機関に対し、行政情報を利用することを許諾すれば、結婚や引越に関わる氏名、住所の変更情報や現況確認を、金融機関と行政機関間でやり取りすることができる。これにより、個人からの変更届や現況届を金融機関に提出する手間が削減される（図 24）。

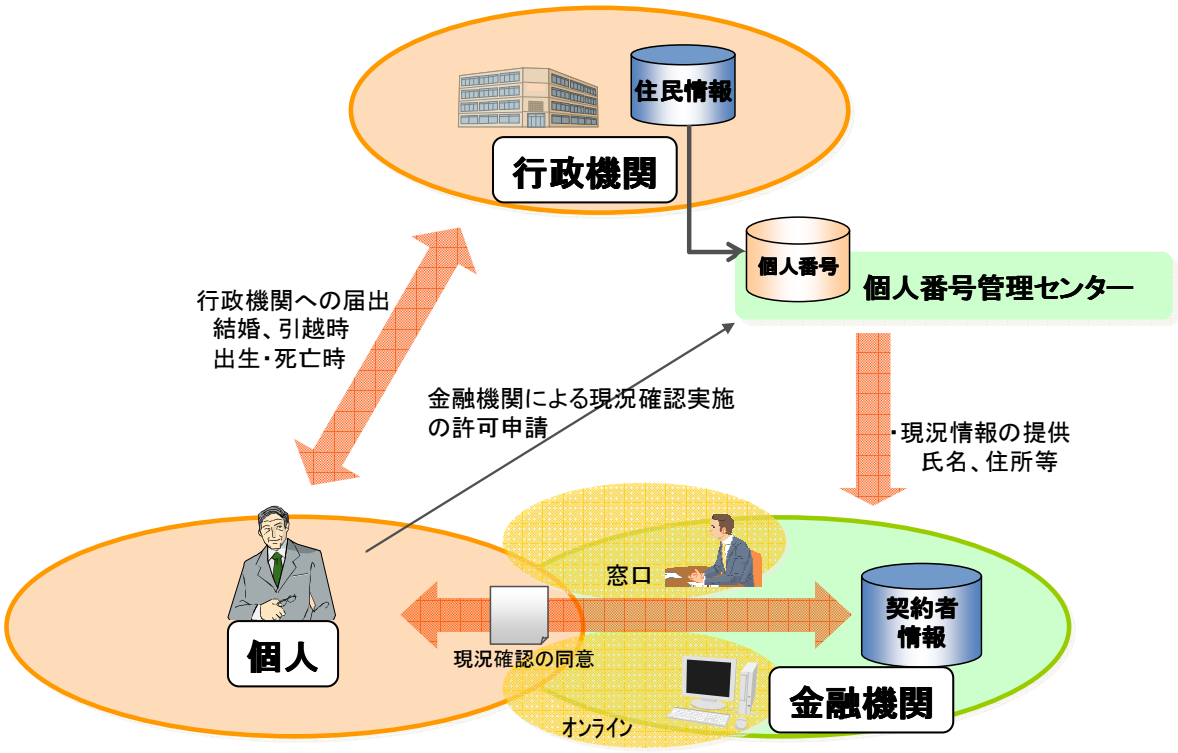


図 24　現況確認のユースケース

（２）背景と目的

銀行口座や保険証券等の金融商品取引では、契約者が結婚や引越などによって氏名、住所等を変更した際には、変更届を提出する必要がある。しかし、個人からの申し出によって行われるため、手続きを忘れてしまうケースも発生する。

口座開設や保険証券の契約といった金融商品の取引では、口座契約者本人が契約内容を適正に把握できていないことにより不正な取引が行われる問題や、金融機関が正確に契約者を把握できていないことによる保険金の不払い問題など、個人の不利益が発生している。例えば、民間保険における終身年金商品では、契約条件によっては、毎年現況届を提出することを義務付けている商品も存在するが、契約者本人の高齢化等により手続きそのものが負担となっているケースや、さらには申請を忘れたことにより、未払いになるケースが発生している。

一方、金融機関においても、預金保険法や犯罪収益移転防止法などの法令順守はもちろんのこと、契約の確実な履行を実施するために契約者の現況調査などを実施しているが、郵送した郵便物が未達になり、営業担当者による訪問が必要になるなど、確認作業に伴う金融機関の業務負担が増加している。

行政機関が保有している現況情報を本人の同意のもと民間企業が利用できるようになれば、結婚や引越等による氏名、住所の変更届や、毎年の現況届の提出の手間が軽減され、現況が確認できないことによる保険金の未払い問題等の契約不履行の発生を防ぐことができる。また、金融機関においても、現況確認にかかる業務負荷の軽減につながる。

（３）メリット

個人側のメリットは以下となる。

- 氏名・住所の変更届や現況届の提出に関わる手間の削減
- 適正な権利履行の実現（未払い、過払いの防止）

金融機関側のメリットは以下となる。

- 契約者情報の正確性向上
- 現況確認業務に関わる業務負荷の低減

（４）利用場面

現況確認とは、結婚や引越などにより氏名、住所が変更となった場合や、金融商品の契約条項によって定められた事由により、現在の氏名、住所が正しいかどうかの確認を行うことである。図 25 に概要を示す。

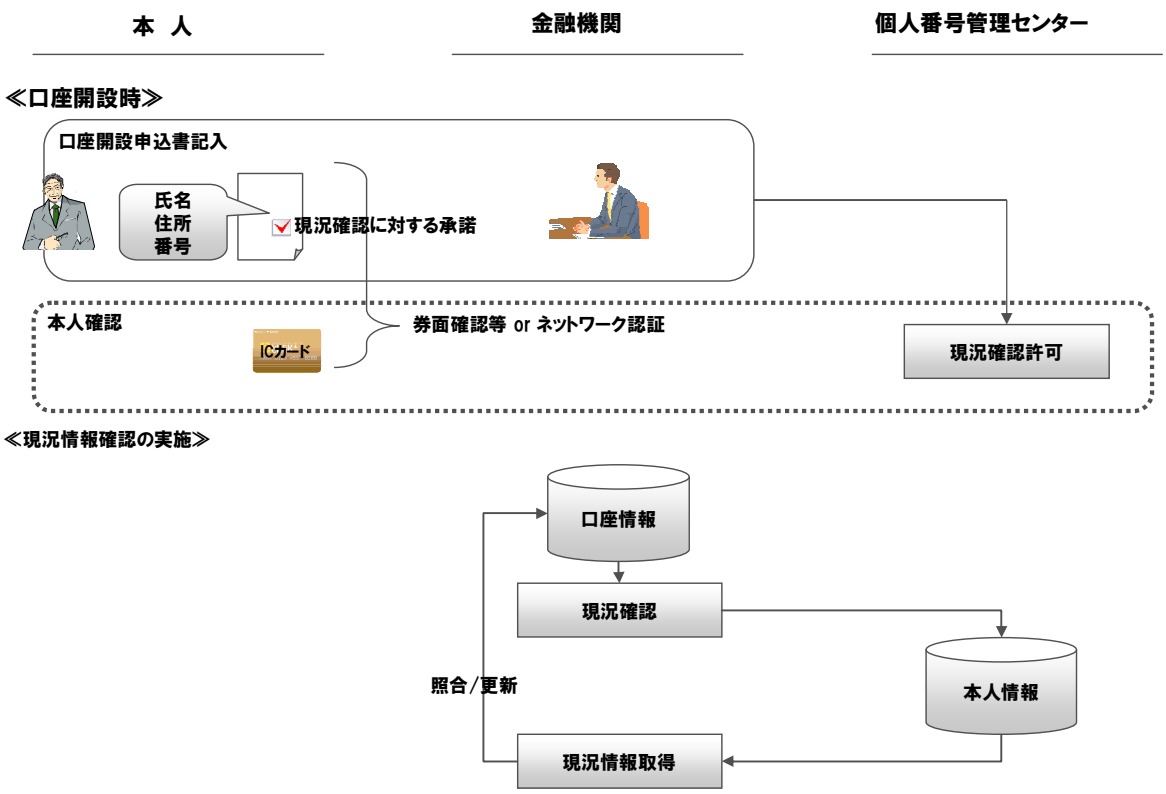


図 25　現況確認の概要

現況確認は、本人確認と同様に、犯罪収益移転防止法や預金保険法に基づき、口座や契約者を正確に把握可能とするために行う。契約者は、結婚や引越により氏名や住所が変更となった際、変更届を提出することが求められている。また、終身年金保険等において、保険の該当者の生存を確認するために、毎年、公的機関の発行する住民票などの証明書の提出と請求書の申請を契約条項において個人に義務付けているものもある。近年の保険金不払い問題にあるよう

に、本来給付の権利があるにもかかわらず、申請漏れ等によって保険会社で支給漏れが起きるケースもあり、保険会社では契約内容の確認作業などを徹底させる等によって作業負荷の増加につながっている。

金融機関は、口座開設時や契約時に現況情報の確認を金融機関が行うことの承諾を個人より受け、個人番号管理センターにて本人情報の確認を行うことにより、現況確認ができる。

現況確認では、複数のバリエーションが考えられる。ここではいくつかの代表的な場面を抽出し、それぞれの場面による必要機能の割り出しを行うこととする。

（ア）契約時等に現況確認の承諾を行い、承諾に基づき金融機関が確認作業を実施

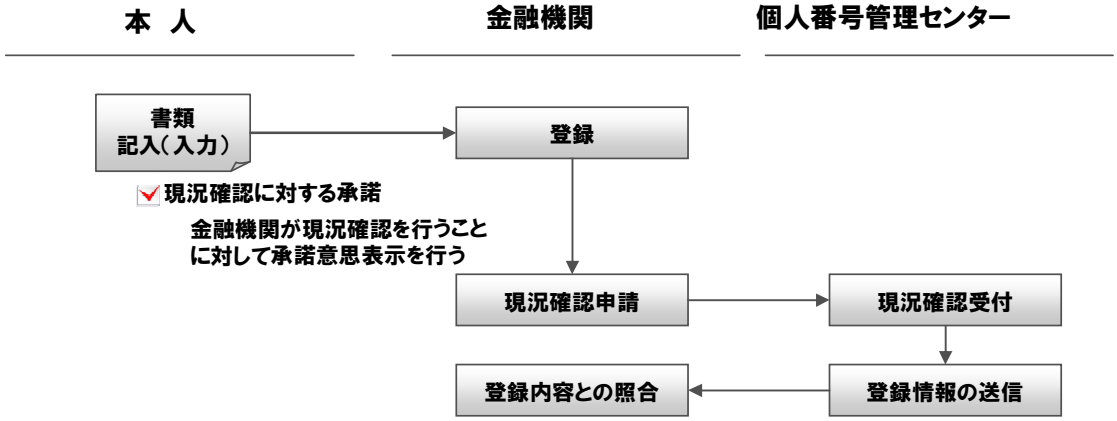


図 26　現況確認のシーケンス（金融機関が個人番号管理センターに問い合せることを許可）

①本人が金融機関による現況確認を承諾する

②金融機関は承諾された範囲で個人番号管理センターへ確認作業を行い、最新情報を入手する

（イ）本人が個人番号管理センターを通じて現況確認情報を金融機関に提供する場合

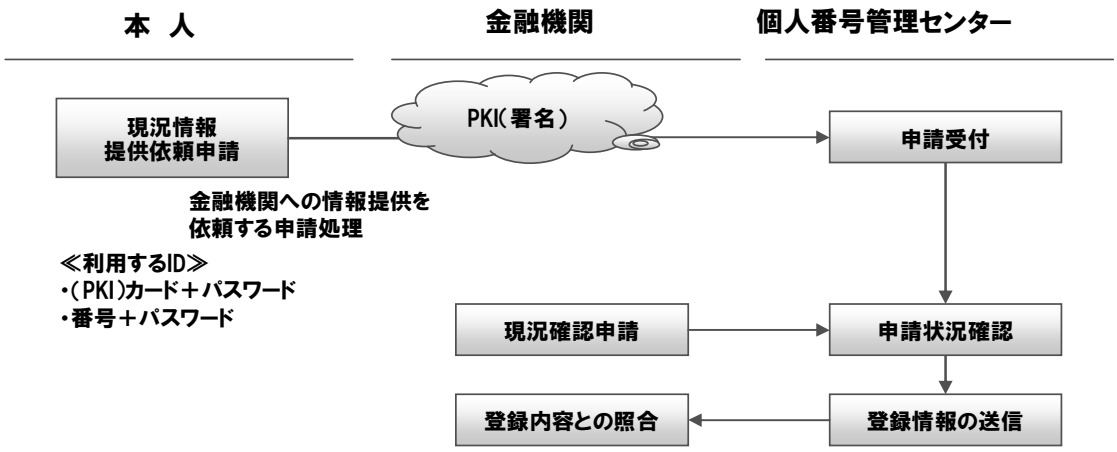


図 27　現況確認のシーケンス

（金融機関からの問い合せを個人番号管理センターが受付けることを許可）

①本人が金融機関で個人番号管理センターにアクセスし本人確認を行った上で、本人の現況情報を金融機関へ提供することの依頼・許諾を行う

②個人番号管理センターでは、本人の依頼・許諾に基づき、当該金融機関からの現況情報確認依頼に対し、現況情報の提供を行う

４－３－３．各種証明書手続き

（１）サービス概要

金融機関から個人に送付し、個人が税務署（多くの会社員においては勤務先企業）に提出していた納税に関わる各種書類を、個人番号を付加したデータとして、金融機関から税務署に直接データで提出することで、個人では証明書の入手・管理の手間の軽減が、金融機関では送付コストの削減が、税務署では納税者からの申告情報と紐付けることが、それぞれ可能となる（図28）。

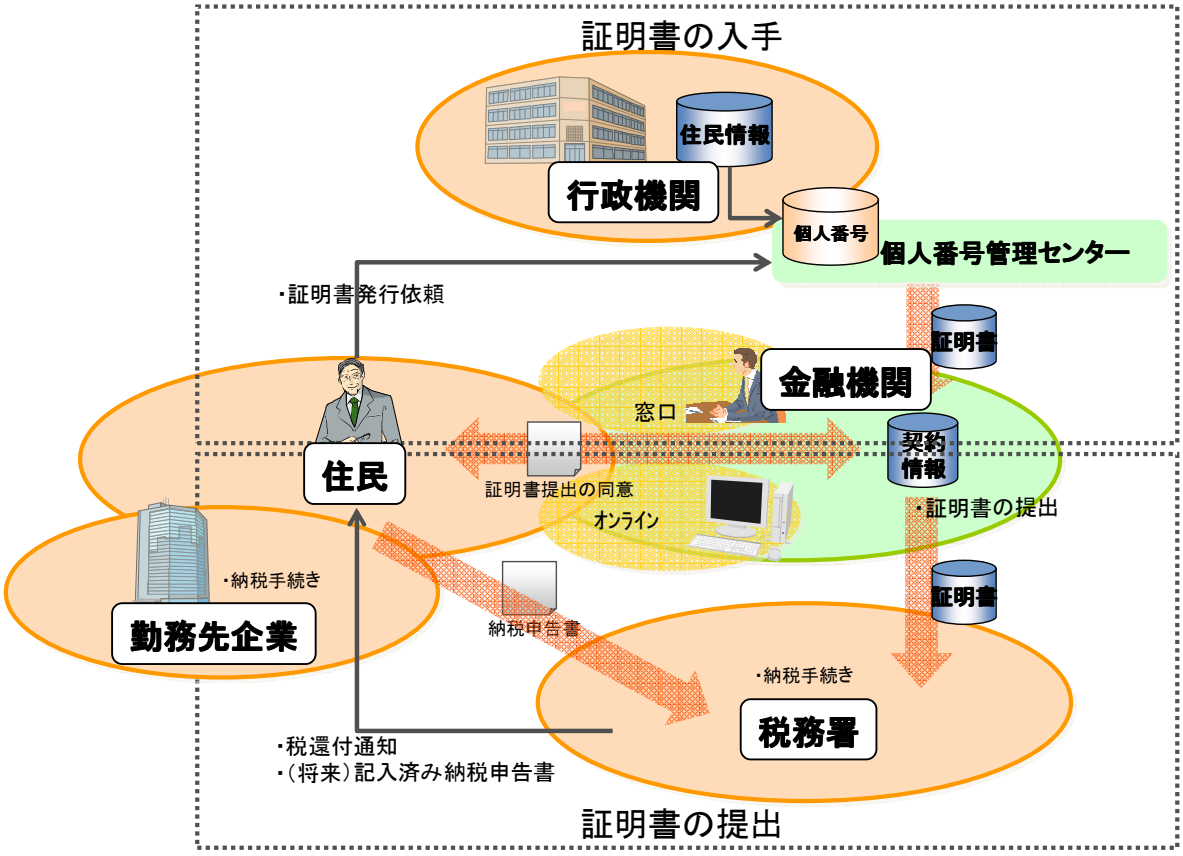


図 28　各種証明書手続きのユースケース

（２）背景と目的

納税申告時、個人は配当・利子所得や住宅ローン控除、保険料支払証明書などの証明書を添付し、申告している。そのため、主に個人との間で納税に係る各種証明書の発行を行っている

金融機関は、契約者に対し、住宅ローン残高証明書や保険料支払証明書などを、毎年、発行・郵送している。個人は、毎年の納税申告時に、これらの証明書の保管、提出を行っているが、書類の紛失等によって再発行の依頼などが煩雑になっている。また、納税者の大多数を占めるいわゆるサラリーマンの処理は、勤務先が一括して事務処理を行う特別徴収にて処理されているが、勤務先である企業の作業負荷となっている。同様に、金融機関においても全契約者に対する証明書の発行・提出業務は負担となっている。

近年、給付付き税額控除や記入済み税額申告書など、納税と給付のあり方に対する議論や納税者の負担軽減策などが検討されており、それに伴い、納税に関わる付帯情報の電子化が求められている。

これらの情報の電子化および税務署との直接データ連携ができるようになることで、納税者による証明書の入手および添付等の処理の手間、金融機関の紙の証明書の発行および郵送コストの削減が期待される。また、税務署においても納税情報の管理業務の効率化が期待される。

一方、個人と金融機関との取引において、本人確認や現況確認、さらにローン契約時等では住民票や印鑑証明、収入証明など公的機関が発行する証明書の提出が必要な取引が多く存在している。個人は、ローン契約手続きの際に行政機関に行って各種証明書を入手の上、金融機関との手続きを行う。同様に、金融機関においてもこうした書類のやり取りおよびバックオフィスにおける確認作業や保管作業に多大な業務負荷が発生している。

（3）メリット

個人側のメリットは以下となる。

- 行政機関に対する各種証明書の提出負荷の軽減
- 行政機関発行の証明書の入手の手間の軽減

金融機関側のメリットは以下となる。

- 証明書の発行および郵送コストの削減
- 契約者より入手した各種証明書の確認・保管作業の負荷軽減

企業（勤務先）側のメリットは以下となる。

- 従業員から提出される、特別徴収に関わる証明書等の管理、提出業務負荷の軽減

税務署側のメリットは以下となる。

- 納税者が提出する書類チェックの手間の軽減

（4）利用場面

各種証明書手続きは、本人および金融機関では、行政機関への証明書提出と行政機関が発行する証明書の入手がある。

主なユースケースを表 3 に示す。

表 3　各種証明書手続きの主なユースケース

タイプ	ユースケース	状況	証明書の例	実現したい状況
行政への書類送付	納税時の各種証明書	納税に当たって保険会社や金融機関から各種証明書を入手（送付）の上、勤務先、税務署へ提出。	・源泉徴収票 ・保険控除証明書 ・住宅ローン残高証明書	・番号が添付された情報が金融機関や保険会社から直接送付される。
	生活保護の申請や相続財産の調査等	相続時の相続財産調査において残高証明書や取引明細書が必要。	・残高証明書 ・取引明細書	・番号が添付された情報が金融機関から直接送付される（もしくは本人意思のもと情報提供される）。
行政からの書類入手（金融機関への証明書提出）	各種契約手続き	各種契約手続きにおいて、公的機関発行の証明書の提出をしている。 貸金法改正により、ローン契約時に収入の証明が義務付けられたため、収入証明等の提示が必要。	・住民票 ・収入証明 ・印鑑証明書	・金融機関の窓口等において、行政保有の情報を入手できる。
	住宅ローン契約時	住宅ローン借り入れ時には、各種証明書の提出が必要となり、行政機関および勤務先企業からの各種証明書の取得が煩雑。	・身分証明書類（住民票） ・源泉徴収票/納税証明書 ・印鑑証明書 ・勤続証明書 ・借入金証明書	（契約窓口で） ・行政機関や勤務先にアクセスし、必要情報を入手（もしくは金融機関へ送付）し、手続きを一括して実施する。 （自宅からインターネットで） ・必要書類の手続きをする。

（ア）行政機関への証明書提出

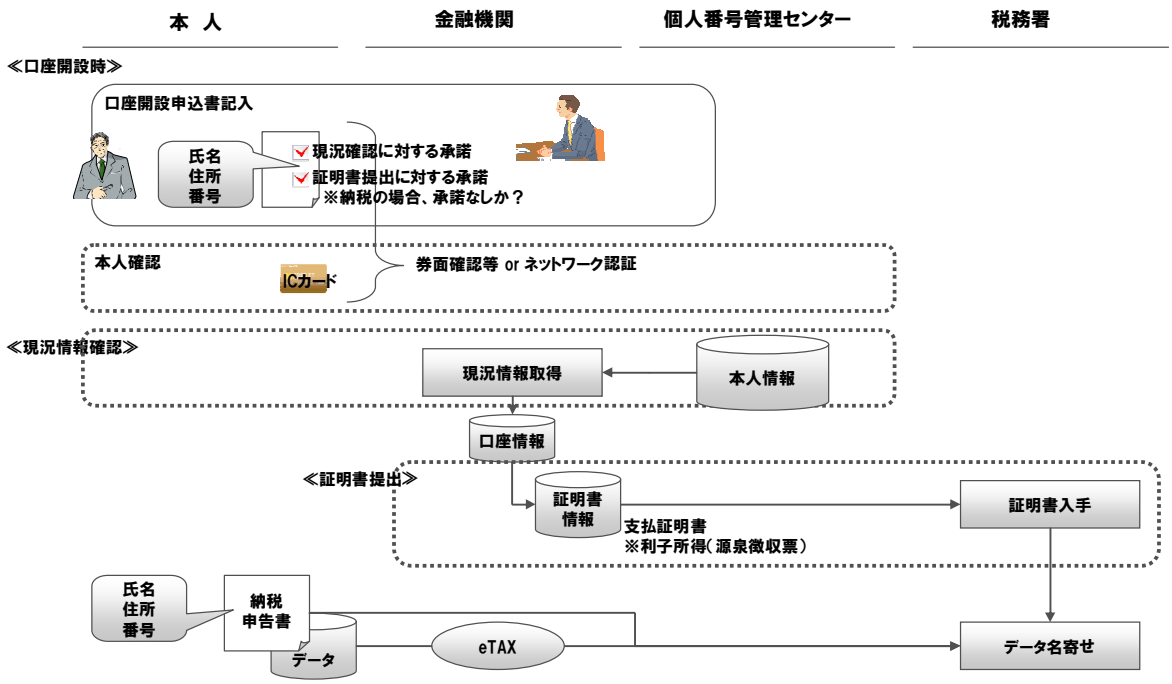


図 29　税務関連書類提出の場合のシーケンス

番号制度の導入に伴い、行政機関に証明書を提出するものとして、納税申告関連書類に番号を記載し直接提出するものが挙げられる。金融機関が発行する納税申告関連の書類としては、表 4 に主だったものを掲載する。

表 4　金融機関が発行する主な納税申告関連の書類

証明書類	証明書の必要な場合	現状	今後（想定）
利子所得 （源泉徴収票）	源泉分離課税によって一律所得税 15%、住民税 5%を徴収する。控除額が所得税額を上回る場合には、確定申告を実施することにより控除対象となる。	源泉徴収票を入手し、確定申告書とともに税務署へ提出する。 ※e-TAX では、本人保管	番号付番された源泉徴収票が税務署に提出される。 税務署にて番号による申告との名寄せ（番号で）を行い、税額計算して納付・還付。
雑所得における源泉徴収票	講師謝礼等で受けた所得は源泉徴収され、支払企業より源泉徴収票が送付される。これを税務署に提出する。	講師謝礼等で、給与所得等とは別の所得を受けた場合、雑所得として計上する。その際、支払企業より源泉徴収票が送付され確定申告時に添付する。	番号付番された源泉徴収票が支払企業より直接税務署に提出される。 税務署にて番号による申告との名寄せ（番号で）を行い、税額計算をして納付・還付。

証明書類	証明書の必要な場合	現状	今後（想定）
保険料控除証明書	保険料については一定金額が控除対象となるため、証明書を添付書類として提出する。	契約している保険会社より保険料控除証明書が送付されてくるため、これを特別徴収であれば勤務先、確定申告であれば税務署に添付書類として提出する。	番号付番された証明書が保険会社から直接税務署へ提出される。 税務署にて番号による申告との名寄せ（番号で）を行い、税額計算して納付・還付。
借入金残高証明書	住宅ローン控除を受ける際、残高証明書を添付書類として提出する。	契約している金融機関より証明書が送付されてくる。これを特別徴収であれば勤務先、確定申告であれば税務署に添付書類として提出する。	番号付番された証明書が保険会社から直接税務署へ提出される。 税務署にて番号による申告との名寄せ（番号で）を行い、税額計算して納付・還付。

（イ）行政機関からの証明書入手

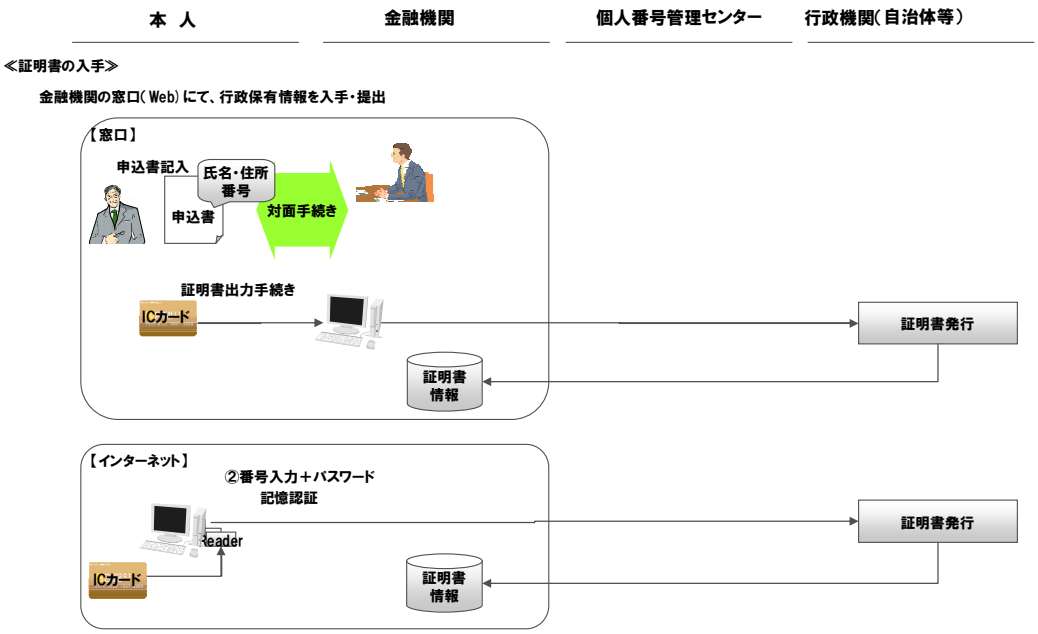


図 30　行政機関からの証明書入手の場合のシーケンス

①本人認証をした上で、証明書の発行手続きを行う

金融機関窓口における証明書の提出やインターネット等による手続きのときに、行政機関からの証明書の入手が必要になる。近年、コンビニで各種証明書の発行をしている自治体もあるが、同様に金融機関窓口においても発行できるようになれば、紛失等のト

ラブルも避けられる。また、最終的には、直接データによるやり取りが想定され、コピーの取得や書類の保管等の手間の削減にも効果を発揮する。

４－３－４．サービスを実現するにあたっての課題と施策

民間分野での番号制度の利用に係る課題としては、①利用者の受容性、②既存の口座、契約への番号付け、③不正な手段による情報漏洩対策、④個人情報の目的外利用の制限、⑤本人の承諾の証明が挙げられる。

① 利用者の受容性

番号制度を民間で利用する際にもっとも重要な観点は、利用者に番号制度の民間利用を受容してもらえるか否かにある。たとえ法制度上利用が認められていたとしても顧客である利用者が不信感を持ったり、利用を拒んだりするときに無理強いすることはできない。企業としても顧客離れにつながるようなリスクを抱え込むことは営業上避けるべきである。

② 既存の口座、契約への番号付け

税務分野に番号制度が導入された際、源泉分離課税における利子所得を示す源泉徴収票が発行されるときに番号を記載することが想定される。また、保険料支払に対する控除においても、保険料支払証明書に番号を記載して発行されることが想定される。納税分野であるため、法制度に則った運用が求められるが、実際には、顧客一人ひとりから番号を入手し、既に開設された口座や契約のデータベースに登録していく作業は、多大な手間と時間を要する。

③ 不正な手段による情報漏洩対策

本人確認のときに偽造された個人番号カードが用いられる、あるいは本人確認、現況確認、証明書の入手において不正なアクセスが行われて個人情報が漏洩することを防止する手段が必要である。

④ 個人情報の目的外利用の制限

番号制度および現況確認や証明書の入手、提出において、今までは本人の了解の下、手間がかかりながらも実施していた業務が、情報連携によって実施可能になる反面、目的外の利用制限も必要となる。この際、いかに目的外の利用制限を確実かつ正しい方式で実行するかが求められる。

⑤ 本人承諾の証明

現況確認等は、本人の承諾の下で実施されることが望ましい。その際、本人から得た承諾をどのように証明するかが問題となる。仮に悪意を持った主体が存在した際、悪意ある行為を排除する仕組みが必要となる。

上記③～⑤に関し、詳しくは６章で記述するが、サービスを実現するにあたっての課題とそれらに対する、技術的・制度的施策の概要を表 5 に示す。

表 5　主な技術的・制度的課題と施策

課題	技術的施策	制度的施策
本人確認における本人を証明する個人番号カードの偽造対策	偽造できない（困難にする）仕組みおよび偽造を発見する仕組み 例）透かし、IC チップ、認証	偽造等に対する罰則等の整備 損害補償の整備
本人確認や現況確認、証明書の入手における不正アクセスの防止	不正アクセスを排除する仕組み 例）端末認証、ユーザ認証、アクセス制御	不正行為に対する監視および罰則等の整備 損害補償の整備
目的外利用の発見および排除	―	第三者機関による監査、罰則等の整備 損害補償の整備 金融機関の認定、ガイドライン制定
本人承諾を受けていないアクセスの発見および排除	本人の意思確認の仕組み、アクセス権管理、アクセスログ管理	第三者機関による監査、罰則等の整備 損害補償の整備 金融機関の認定、ガイドライン制定

５．民間利用を前提にした番号制度の実現

この章では、４章のユースケース検討から抽出された、個人番号を民間利用する際に番号制度に求められる要件を整理し、番号制度のあり方についての COCN としての考え方を示す。

５－１．番号制度によって実現したい要件

５－１－１．個人番号と個人情報、各機関情報の関係

まず、個人番号、個人を特定する基本情報、さらに行政機関や企業が業務によって取得したその他の個人に関する情報について、図 31 に整理した。

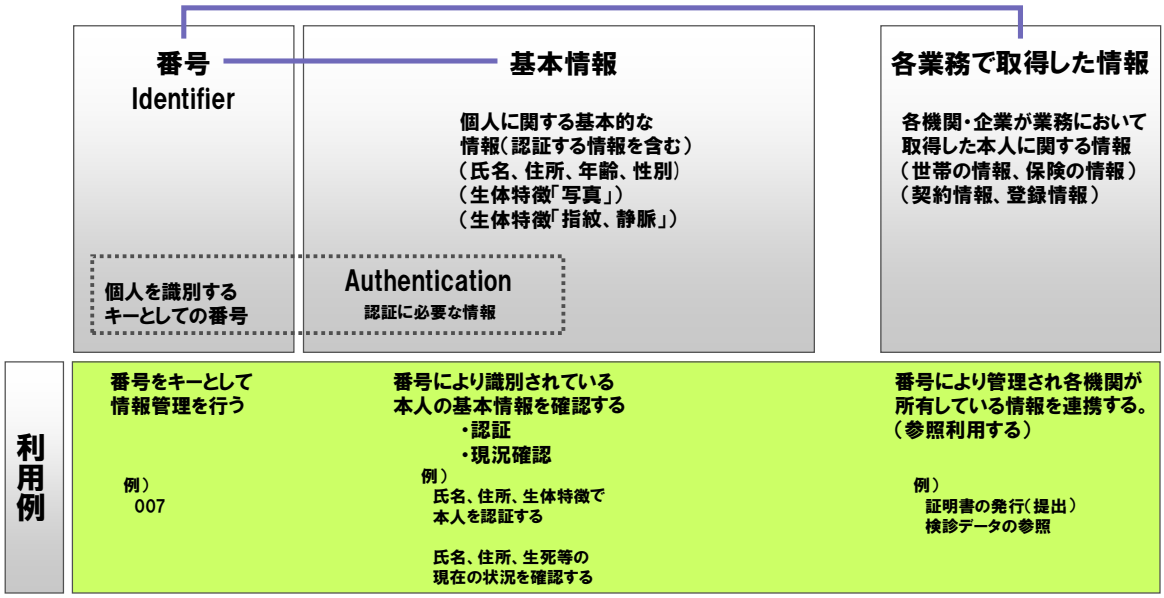


図 31　個人番号の位置づけ

個人番号は、対象を識別する識別子＜Identifier＞である。すなわち、個人番号が異なれば、それは別の個人であり、同一であれば同じ個人であると判断できるものである。しかし、個人番号からは、氏名などの本人を特定する情報が類推できないため、個人番号単独では個人を特定できる情報とはみなされない。一方、個人番号と合わせてその人の氏名や住所が格納されたデータベースの基本情報を参照することが可能であれば、個人番号から本人を特定することができる（Authentication）。その他の各業務で取得した個人に関する情報は、それぞれの機関が個別に管理するものであって、番号が一元管理されていることによって、個人に関する情報が一元管理されることになるわけではない。

上記の整理を念頭に置きつつ、以下に民間企業が番号制度によって実現したいことを提示する。

（１）個人一人ひとりが識別できること

個人一人ひとりに付番された番号によって、一人ひとりが識別できることにより、個人番号をキーとして、一人ひとりを重複なく識別することが可能となる。そのためには、個人一人ひとりに一つの番号が付番され、その番号は他人に付番されないことが必要である。このことに

より、本人のものとして提示された個人番号によって紐付けを行い、民間企業が管理する情報について個人別の情報として管理することが可能となり、本人の情報の名寄せなどが確実に行えるようになる。こうしたことは、金融機関における本人確認や複数の口座の所有者の名寄せ、および、医療現場において、転職などによって保険証が変更された患者の情報管理に活用されることが期待される。

（２）本人確認ができること

個人一人ひとりに付番された番号とその個人の氏名や住所、生年月日、生体特徴などの本人を特定する情報を結び付けることによって、確実な本人確認が可能となる。番号制度の導入と同時に、本人を認証できる個人番号カードやPKI認証などの本人確認手段を整備することによって、本人確認が必要な場面において確実な本人確認が可能となる。具体的には、預金保険法や犯罪収益移転防止法などに定められた金融機関における本人確認手続きなどでの活用が期待される。

（３）個人一人ひとりの現況確認ができること

行政機関に登録されている本人の氏名や住所、現在の状態（生死等）の最新情報を確認することが可能となり、本人の氏名、住所などを常に最新の状態に保つ必要がある業務が簡素化される。具体的には、金融機関での本人確認や現況確認が必要な業務において、最新の情報の把握のために、現在は免許証のコピー（住所変更された場合には裏書も含め）や住民票などにより確認作業が行われているが、これを本人の承諾を前提に、民間企業が個人番号管理センター（後述）にアクセスしてネットワークで本人の現況を確認できるようにすることによって、証明書の入手、提出における利用者の負担軽減につながることが期待される。

（４）情報連携ができること

一人ひとりに付番された番号に紐付く、各機関、各企業が保有している情報を、本人の意思（許諾）に基づき、しかるべき機関、企業の間で直接に情報連携できることにより、個人と企業間における権利と義務の確実な履行や、情報連携に係る本人の負担の削減が可能となる。具体的には、金融機関における口座開設やローン審査等において必要な各種証明書のやり取りや、今後税務分野での申告における証明書情報の連携等において、利用者の利便性向上が期待される。

５－２．番号制度で実現すべき機能

５－２－１．実現機能

民間企業が番号制度を利用することを前提に、番号制度で実現すべき機能を表 6 に示す。

表 6　番号制度で実現すべき機能

実現機能	概要
本人確認を実現する媒体	券面にて本人確認が可能なカード。 ・券面に本人を特定する情報が記載されているもの 　－顔写真 　－氏名、住所等 ・認証手段 　－ID・パスワードによる認証 　－PKI・パスワードによる認証 　－生体認証（指紋、静脈等）
ネットワークを活用した本人確認機能	ネットワークアクセスにより上記認証手段を活用して本人確認が行える機能。
現況確認が行える仕組み （ネットワークの活用）	本人および本人から承諾を受けた民間企業がネットワークアクセスにより、現況情報の確認ができる仕組み。 （行政機関が保有する氏名、住所等の最新情報を入手できる）
現況確認等において、本人が民間企業に対して承諾したことを証明する仕組み	民間企業が本人承諾のもと現況確認を実施する際、その企業が本人承諾を得ていることを証明する仕組み。 この仕組みがない場合、悪意を持った主体が、本人承諾があることを偽り、不正に現況確認をすることが可能となる。
目的外での利用を排除する仕組み	現況確認等において、本人から承諾を受けた目的利用以外でのアクセスを排除する仕組み。 これには、目的の確認以外に、利用する権限のない者からのアクセスを排除する仕組みが必要となる。
行政保有の証明書情報を入手する仕組み	現行のコンビニにおける証明書発行と同様に、本人が操作することを前提に、民間企業において紙の証明書を入手する仕組み。
証明書情報を電子媒体として入手・管理する仕組み	行政発行の証明書を、紙であるのと同様に、電子情報として民間企業が入手する仕組み。 これにより、手続き上の取り扱いおよび保管作業の削減が期待される。

５－２－２．安心して利用できる番号制度

番号制度を民間で利用するにあたっての大前提は、利用する個人が安心して利用できることであり、この要件を満たさずして番号制度そのものの導入および民間利用はありえない。また、利用者にとって安心かつ便利でなければ結果として利用しにくいもの＝利用されないものとなってしまう。法律的根拠に基づき利用が義務付けられる行政分野と同様に、民間での利用も番号制度の安全性及び利便性が確保されないと、利用者および企業の積極的な利用は進まない。そのため、各ユースケースでの番号の利用場面で、考えられる課題およびリスク要因についての検討を行い、課題およびリスクの回避策、さらに実現すべき新たな機能や制度の抽出を行った。

（１）課題およびリスク分析

各ユースケースにおける脅威を洗い出し、整理すると以下のようなものがある。

- 情報の漏洩
- 情報の改ざん
- 情報の目的外利用
- 情報の本人了承なしの流通
- 匿名化された関連情報による個人の特定

（２）必要機能

番号制度を運営するシステムでは、上記の脅威が起きないようにする機能が必要である。

洗い出された脅威を阻止する技術的対策について検討を行ったところ、多くの脅威は現在確立されている技術で対抗することができる。しかし、番号制度の民間利用でのセキュリティ要件を満足するためには、さらに技術的、制度的検討を深める必要がある。

これら（１）（２）に関する詳細は、６章セキュリティについての検討を参照のこと。

５－３．番号制度に対する提言

COCN における番号制度の民間分野での活用の各ユースケースの検討を踏まえ、番号制度に関して以下のとおり提言する。

すでに政府内において検討されているように、番号制度の導入は、国民一人ひとりの権利を守り、弱者に対して積極的な支援が実施される公平・公正な社会を実現することが最大の目的である。さらに、番号制度の導入により、国民生活における国民の負担を軽減し、利便性を大幅に向上させることで、社会全体の効率化を実現し、新たなサービス、新産業の創出、産業の活性化を通して我が国の産業競争力強化につなげていくことが求められる。

５－３－１．番号制度に求められる要件

COCN が考える番号制度のあるべき姿について、番号のあり方、番号の利用方法、番号制度を支える制度・仕組みについて以下に述べる（番号制度は、個人を対象にした個人番号と、法人を対象にした法人番号の 2 つがあるが、今回の検討は個人番号に焦点を当てて記述する）。

（１）番号のあり方　～どんな番号であるべきか～

（ア）全員付番

番号制度の対象となる個人が付番対象となる。具体的には、日本国籍を有する者または日本に居住する外国人で、住民登録を行い、納税等の義務や行政サービスを享受する者が対象となる。

番号は、出生時（住民登録時）に付番され、一生涯保持される。番号を利用する業務によっては、死亡後も情報管理の必要性があるため、死亡後も番号を保持する。

（イ）「見える番号」であること

番号は、ヒューマンリーダブル[13]とすべきである。諸外国の犯罪等の事例やかつての番号議論において、番号の盗難に対するリスクの懸念が挙げられているが、納税用の番号でも検討されているように、「見える番号」が必要である。

また、番号を利用する際に、本人が口述・記述できるものであるべきであり、その際、記憶が可能な番号表現方法であることもひとつの要件として挙げられる。番号が記載された媒体を常時携帯せずに利用できる利便性に加え、番号盗難リスクの低減策としても有効である。また、本人が暗唱できる番号を付番するために、個人番号の一意性を維持しつつ、本人が覚えやすい番号（例えば、携帯電話番号、郵便番号、本人・家族の生年月日等を組み合わせた番号）を設定可能とする制度設計が求められる。

（ウ）番号の一貫性と変更可能性

番号によって本人を特定するための基本的要件として、本人の番号が変更されないことが望まれる。そのため、番号は変更できないものとすべきである。しかし、本人の番号が犯罪に利用されるなど、個人番号が汚染された場合等を想定すると番号を変更せざるを得ない状況も不可避である。そのため、番号の一貫性を担保するための仕組みを具備することが必要となる。具体的には、「見える」かつ変更できる番号と「見えない（見せない）」かつ変更できない番号の組み合わせによって、見える番号が汚染され変更せざるを得ない状況となった際に、見えない番号によって本人の番号管理の一貫性を担保しつつ、見える番号を変更するなどの仕組みが考えられる。

---

[13] ヒューマンリーダブル：Human Readable。人が認識可能なこと。

（エ）個人番号カード（ID カード）

民間活用のユースケースからも抽出されたように、番号制度の導入によって実現する重要な機能の１つとして、本人特定、すなわち身分証明の機能として、公的機関が発行した身分証明書の機能を持つカード（個人番号カード）の利用が挙げられる。近年の犯罪防止などの対策として、金融機関をはじめ、携帯電話等の契約時や本人特定郵便の受け取り時に本人確認が行われているが、その媒体に求められる機能には、本人を特定できる情報としての生体特徴である写真、本人を特定する氏名、住所などが必要となる。そのため、番号の導入に付帯して身分証明書となるカードの発行をすべきである。さらにカードの導入では、偽造等による成りすまし防止など本人特定を確実にする仕組みも合わせて導入すべきである。

公的機関が発行する個人番号カードは、券面に個人番号、氏名、住所、顔写真を記載した身分証明書として活用できるタイプ、公的認証基盤を活用した電子証明書を内蔵したタイプ、さらには、セキュリティの強度を上げるために生体認証機能を搭載したタイプ、個人の携帯電話の内蔵カードに電子証明書を内蔵したタイプ等々、安全性を維持しながら利便性を保証できる形で、複数のタイプの個人番号カードが選択できるように制度設計することが求められる。

（２）利用方法　～どのような利用方法があるか～

（ア）利用の必須／任意

番号制度は、付番については全員必須であるが、利用については必須である分野と任意である分野を設けるべきである。税務分野等については必須であるが、民間利用をはじめ、その他の分野では基本的には本人の意思を尊重した利用が可能な制度とすべきである。特に民間分野では、本人の意思に基づいて利用されることが前提であり、加えて、番号がなければ今以上の不利益を被る事態の発生は断じてあってはならない。そのため、番号の任意利用に関して、サービスを提供する民間企業は、現状業務維持を前提として必ず代替手段を提供するなどの手立てが必要である。

（イ）利用手段

番号の利用方法は、利便性とセキュリティの兼ね合いによって、複数の手段を用意すべきである。

番号が記載されたカードを誰もが常時携帯する状況は想定しにくく、カードがなければサービスが受けられないという状況は避けなければならない。そのため、番号のみの利用、すなわち本人が自らの番号を記憶して利用する手段も用意すべきである。その際の本人認証手段としては、個人番号＋記憶認証としてのパスワード等が考えられる。

番号の利用に関するセキュリティ強度についても本人確認の厳密性やアクセスする情報の機密性等要求されるセキュリティ強度に応じて複数段階のセキュリティ手段を用意すべきである。本人記憶認証としての個人番号＋パスワードでの認証や、IC チップを活用した PKI＋パスワードによる認証、生体認証などが考えられる。

また、番号の利用対象業務については、ユニバーサルサービスの観点から、必ずしも番号を利用しなくても同様のサービスが受けられるように複数の利用手段を提供すべきである。番号制度やWeb等による番号利用手段の普及に伴い、デジタルデバイドを感じる情報弱者を生み出してしまうことは本末転倒である。

（3）番号制度を支える制度・仕組み

（ア）付番・配付の実施方法

個人番号の付番は、本人の特定を伴い実施されることが必要であるため、個人と密接に関わっている機関（基礎自治体）において実施されることが必要である。

個々人への付番についてはある時点をもって一括して行い、その後は、出生の届け時に実施していくことが想定される。本人に対する本人の番号（カード）の配布は、本人に対する番号（カード）の所持に対するインセンティブが必要であろうと想定される。そのため、制度導入に併せた配付などの工夫が必要である。

（イ）既存インフラの有効活用

番号制度を支える仕組みの構築においては、住基ネット等の既存インフラを有効に活用すべきである。番号の付番・管理は、対象者全員に対応するための全国ネットワークが必要となるため、新たな仕組みを構築することは膨大な費用がかかることから現実的とは言えない。

また、既存インフラの中でも、役割が重複するものについては、全体を見据えた再検討が必要である。

（ウ）法制度上考慮すべき要件

民間企業における個人情報利用は、個人情報保護法などの法制度やプライバシーマークなどの管理基準の認定などが整備されたことによって、保護が徹底されるようになってきた。番号制度の利用にあたっては、こうした既存の法制度や管理基準等についても再点検を行い、必要な制度の見直しが求められる。

また、個人番号管理センター（後述）の設立、運用に関連して、住民基本台帳法その他の関連法制の見直しが必要となる。

さらに、行政および民間企業が正しく番号制度の利用をしているか否かについて、第三者機関を設立し、監視する機能を確立すべきである。

（エ）安全性を担保する仕組み

情報セキュリティには絶対安全であるということが事実上ないことを踏まえれば、セキュリティを脅かす攻撃が日々進化していくことを念頭に安全性担保には万全の対策を講じるべきである。

番号および番号に係る情報連携の状況を監視し、不正行為が見受けられる場合には、調査を行い、実際に発生してしまった事件・事故に対しては、被害者を救済する機関や

仕組みが必要となる。特に行政の内部機関による不正利用については、独立した第三者機関等による監視・監査が求められる。

（オ）情報漏洩・犯罪行為への対応

いかに管理を徹底しても、悪意のある第三者による番号に係る犯罪行為をすべて防ぐことは難しい。また、ドメスティックバイオレンス等の親族による犯罪行為等により、継続的に同一番号を利用することで不利益を被る事態が発生することもありえる。こうした犯罪行為や自身の番号がなんらかの原因により継続的に利用することが好ましくない事態が発生したときの対処が不可欠である。具体的には、犯罪行為等に利用されて汚染されてしまった番号をしかるべき手続きによって変更できることが求められる。

（カ）ユニバーサルサービスを担保する仕組み

番号制度および番号制度を支える仕組みは、ICT を活用した利用者の利便性を高める仕組みとして期待される一方、デジタルデバイドといった情報弱者を生み出す危険性をはらんでいる。民間サービスでの利用は、効率性を重視するあまり、ICT 利用による手段提供のみといった、情報弱者が著しく不当な不利益を被る可能性を否定できない。あくまでも ICT 活用は便利な機能としての手段の 1 つであり、利用しない、できない人に対する他の手段の提供が担保されている必要がある。

５－３－２．個人番号管理センター

番号制度の民間利用において、個人番号および本人を特定する情報の利用による本人確認、現況確認の実施については、行政内システムとは切り離した機能を新たに設定し、実施すべきである。COCN の検討では、個人番号管理センターを新たに設置し、番号制度の民間利用に必要な機能を一元的に提供することを前提に検討を行った。特に現況確認などの個人番号に紐付く本人を特定する情報の利用において、適正な情報管理体制を有すると認定された特定の民間企業、分野別番号管理センターに対して適正な手続きにて情報の提供が実施されるためには、集中的な対応が必要である。

≪制度全体（仮説）の中での位置づけイメージ図（案）≫

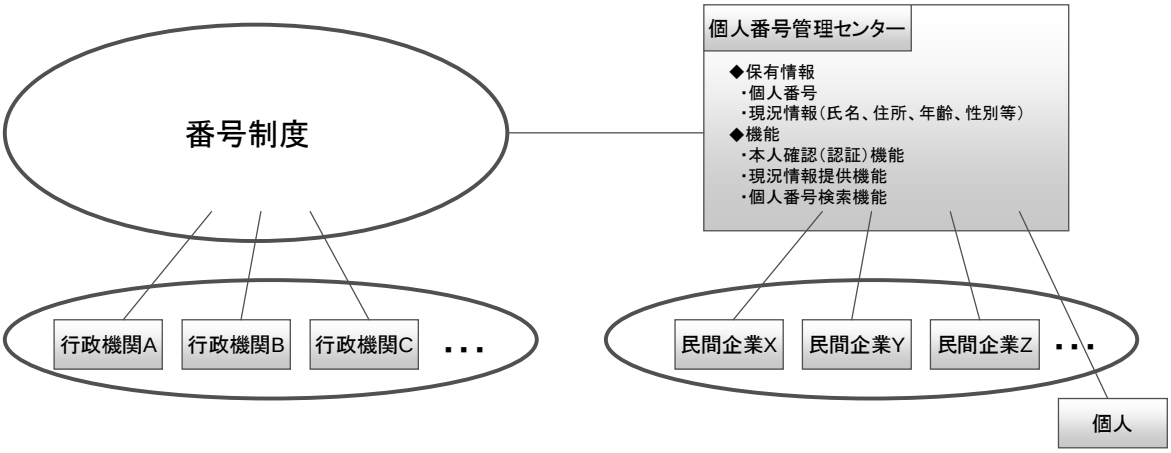


図 32　個人番号管理センターの位置づけイメージ

個人番号管理センターは、政府内で検討されている番号制度と連携した公的機関として設置され、民間利用に必要な情報およびサービス機能を提供するとともに、番号制度を運用する行政内のシステムに民間企業が直接アクセスすることを遮断するために設置される。

医療機関、金融機関等、個人番号を活用する民間企業、分野別番号管理センターが顧客サービスを行うにあたり、個人番号管理センターは以下の機能を持つ必要がある。

（１）顧客が個人番号カードに記載された本人であることを確認できる機能

- 顧客が個人番号カードを使用し、その個人がパスワード入力や生体認証することで本人であることを確認する。
- 個人番号カードを所持していない場合、個人番号とパスワードの入力により本人であることを確認する。

（２）顧客の現況を確認できる機能

- 認定された特定の民間企業、分野別番号管理センターが、個人番号の判明している顧客の個人番号を提示することで、その顧客の現住所、生死を確認する。
- 個人番号が変更されている場合、過去に個人番号の有効性を確認した時の個人番号と確認時の年月日を提示することで現在の個人番号を検索し、その個人番号に基づき個人の現住所、生死を確認する。

（３）顧客の個人番号を検索できる機能

- 認定された特定の民間企業の窓口にきた顧客が、個人番号カードを所持しておらず、個人番号も記憶していない場合、窓口において免許証等で本人が確認できたことを条件に、その顧客の個人番号を検索し、提供する。
- 認定された特定の民間企業からの過去の本人特定情報に基づき、現在の個人番号を検索し、提供する。（例：銀行口座の口座開設時や病院の初診時の年月日、およびその時の本人特定情報（氏名、住所、生年月日、性別）に基づき、現在の個人番号を検索し、提供する）。

上記以外の番号制度の各論について、平成 23 年 1 月に発表された社会保障・税に関わる番号制度についての基本方針（案）及び平成 22 年 12 月に発表された社会保障・税に関わる番号制度に関する実務検討会の中間整理（案）の内容を下敷きに、COCN の考え方を１０－１．の表 20 に示す。

６．セキュリティについての検討

６－１．番号制度の民間利用におけるセキュリティについて

本プロジェクトで提案している「個人情報や企業情報を安全に活用するためのクラウドコンピューティング基盤」が、社会基盤として広く利用されるためには、適切な法制度の下で国民にとって安心・安全を感じられる基盤として構築され、正しく運用される必要がある。そのためには、基盤の構築・運用に関して網羅的・体系的な脅威分析を行い、その脅威に対して効果的なセキュリティ対策を施すことが重要である。この脅威分析・対策の品質が高まるほどに、国民に不安を抱かせるようなセキュリティ事故を未然に防ぐことができるようになるとともに、国民にも本基盤が安心・安全な社会基盤として受け入れられるようになると考える。

この章では上記問題意識の下、個人情報や企業情報を利活用するために解決しなければならないセキュリティ上の課題（脅威）について、４章で検討した各分野でのユースケースを例として議論し、その議論から出てきた課題とその課題を解決する技術的・法制度的な対応策をまとめた。

また、技術的・法制度的な対策を講じることはもちろん、それらの対策により、「安心安全な情報の利活用がどのように実現されるか」ということを分かりやすく説明し、国民の理解を得られるようにしなければならない。それゆえ、本章では、国民が抱く不安に対する回答として、国民目線での説明も記載した。

６－１－１．共通番号に関するセキュリティ対策検討の状況

国として情報利活用を進めるための共通番号制度については、内閣官房社会保障改革担当室[33]や国際公共政策研究センター（CIPPS）[34]等、様々なところで議論されている。CIPPS では、国民が抱く不安について、「国家管理への懸念」「不正行為のリスク」「目的外利用のリスク」の 3 つに分類し、それらの不安を払拭するために、第三者機関の設置や法整備などの制度面と、システム設計やデータベース分散管理など技術面からの対策を講じている。それら国として情報利活用を進めるための共通番号制度については、前述の内閣官房社会保障改革担当室[33]や CIPPS[34]などの報告書を参考にされたい。

表 7　共通番号制度に対して予想される反対論やリスクとその対策

予測される反対論やリスク		対応策（制度面）	対応策（技術）
国家管理への懸念	国家による国民の監視・監督 国民の個人情報の支配	・政府外に第三者機関設置。監視体制強化。 （行政権力との分離、準司法的機関）	・自己情報の管理監視システム （自己情報へのアクセスログ確認機能）
	国（行政）に対する不信感 （職員による情報の盗み見、不正閲覧、持ち出しなどの流出）	・職員研修・教育の徹底。情報取扱者については採用基準設置、職員のモラル/意識向上を図る ・罰則規定、懲戒免職等	
不正行為のリスク	不正アクセス、なりすまし	・不正行為に対する罰則規定 ・国民に対するモラルの教育 ・海外まで含めた情報収集と対策の徹底	・強固なシステム設計 ・公的認証基盤の構築による正確な本人確認
	情報漏洩、改ざんの懸念		・情報の正当性確認措置システム導入 ・データベース分散管理 ・中継データベースによる連携
目的外利用のリスク	個人情報を利用した逆選択 （保険会社の加入の逆選択　等）	・法による規制強化 （逆選択の禁止規定及び罰則規定）	―
	許可無い個人情報の利用 （民間企業での勝手な利用　等）	・目的外利用の厳密な禁止規制 ・目的外利用（提供者・利用者）の罰則規定	―

（「共通番号制度の早期実現に向けて」CIPPS　2010 年 7 月 1 日[34]）

６－１－２．番号制度の民間活用におけるセキュリティの重要性

番号制度を民間利用するということは、番号制度に携わる組織や人の数も多くなることから、一般的にセキュリティの脅威が増大する。また、情報の利用範囲も広くなることから、個人情報の漏洩、プライバシー侵害という問題だけでなく、犯罪への情報利用や金銭がらみの被害など、脅威の種類・程度も多種多様化し、リスクも大きくなると考えられる。したがって、番号制度を民間利用し、個人情報や企業情報の利活用を図っていくためには、内閣官房社会保障改革担当室[33]や CIPPS[34]等での検討事項に加え、民間活用による新たな脅威に対する対策を講じ、番号制度の民間利用における障害を取り除いていくことが重要である。それゆえ、本報告では、民間活用により生じる新たな脅威とその対策を中心に検討する。

６－２．番号制度の民間活用におけるセキュリティ脅威

個人情報や企業情報の民間活用を図っていくためには、６－１－１．で検討されている国民の不安を取り除く対策に加え、民間活用による新たな脅威や国民の不安が生じないように対策を講じる必要がある。

脅威分析を行う手法として、5W1H 法がある。5W1H 法は「いつ（when）」「どこで（where）」「誰が（who）」「何を（what）」「どのように（how）」「何を目的とした（why）」被害であるかを洗い出す手法である。本検討では 5W1H 法を採用し、まず、「何を（what）」「だれが（who）」を定義し、各ユースケースにおける脅威を分析した。なお、「いつ（when）」に関しては、個人情報および企業情報の民間利用時全体を対象にしている。

具体的には、「個人の情報」を保護すべき資産（what）と捉え、「（A）個人番号」、「（B）基本情報（氏名、性別、住所、生年月日、他）」、「（C）その他紐付けられた関連情報」の 3 つを保護すべ

き資産とし、番号制度の民間利用における脅威を分析した。

また、脅威を引き起こす可能性のある主体（who）としては、「(a) 悪意の第三者（悪意を持った外部犯)」、「(b) 個人番号管理センターやその他民間管理機関の権限保有者（悪意を持った内部犯、または過失の内部者)」の二通りに分類し、脅威分析を行った（表 8)。

表 8　保護対象資産と脅威の主体

保護対象資産（what）	(A) 個人番号 (B) 基本情報（氏名、性別、住所、生年月日、他） (C) その他、紐付けられた関連情報
脅威の主体（who）	(a) 悪意の第三者（悪意を持った外部犯） (b) 個人番号管理センターやその他民間管理機関の権限保有者 （悪意を持った内部犯、または過失の内部者）

番号制度を民間利用した際、国民が受ける可能性のある被害として、以下のものが考えられる。

- 情報漏洩により、本人の知られたくない情報（住所、病歴、資産情報、購買情報など）が、他人に知られてしまう
- 成りすましや情報の改ざんなどにより、金銭的な被害を受ける
- 成りすましにより、不正に銀行口座を開設され、犯罪に利用される
- 情報を改ざんされることにより、番号制度活用によるメリットである本来受けられるべきサービス（健康情報サービス（医療ユースケース)、リコール情報（製品安全ユースケース)、住宅ローン控除サービス（金融ユースケース）等）が受けられなくなる
- 本人の知らないところで、勝手に自分の情報が流されてしまう
- 名前、住所等の個人情報をデータベース化されプライバシーが丸裸にされてしまう
- 名前、住所等の個人情報が名簿化されて、名簿業者などで売買されてしまう
- 匿名化された情報や分散化された情報を寄せ集めて、本来特定できないはずの個人情報が特定されてしまう

このように番号制度の民間利用により国民は様々な不安を抱くことと思われる。それゆえ、番号制度の民間利用における脅威を正しく分析し、適切な制度設計・セキュリティ設計を施すことが重要である。

本プロジェクトでは、医療、製品安全、金融のそれぞれのユースケースに沿って、そこで発生する脅威が、「いつ（when)」「どこで（where)」「誰が（who)」「何を（what)」「どのように（how)」「何を目的とした（why)」ものであるかを具体化し、詳細な脅威分析を行った。なお、ユースケース毎の分析結果の詳細については、１０－２．各ユースケースにおけるセキュリティ脅威分析（詳細）を参考にされたい。

６－２－１．各ユースケースにおける脅威分析

本プロジェクトでは、医療、製品安全、金融のそれぞれのユースケース毎に脅威分析を行い、その結果、保護対象資産およびその管理場所、脅威の主体者、サービスシーンにより、様々な脅威が存在することが分かった（「１０－２．各ユースケースにおけるセキュリティ脅威分析（詳細)」参照)。

これらの脅威は、脅威の主体者により大きく T1～T3 に大別することができ、さらに詳しくは以下のようにまとめることができる。

T1：悪意の第三者による脅威
- T1-1：悪意の第三者による情報漏洩
- T1-2：悪意の第三者による情報改ざん
- T1-3：個人番号をキーにした名寄せ
- T1-4：匿名化データからの個人特定

T2：権限保有者による脅威
- T2-1：権限保有者による情報漏洩
- T2-2：権限保有者による情報改ざん
- T2-3：個人番号をキーにした名寄せ
- T2-4：匿名化データからの個人特定
- T2-5：権限保有者による目的外利用
- T2-6：本人の許可なしでの情報流通

T3：その他の脅威
- T3-1：情報の劣化･消失によるサービス不履行

なお、T2 の権限保有者による脅威には、「組織による脅威」と「組織内のある権限保有者による脅威」とがある。

また、これらの脅威は以下のような手段（how）で引き起こされる。

【不正アクセス】

システムへの正規のアクセス権を持たない人が、ソフトウェアの不具合などを悪用してアクセス権を取得し、システムに侵入して保護対象資産に漏洩や改ざん等の危害を加える。

【成りすまし】

個人番号を記載したカードの盗難･紛失、あるいは個人番号の盗み見などにより、第三者に個人番号を取得され、その者がその個人番号を使って本人に成りすまし、本人の保護対象資産に対して漏洩や改ざん等の危害を加える。

【ネットワーク盗聴】

ネットワークを流れるデータを盗聴することにより、不正に個人番号や基本情報、関連情報等の保護対象資産を取得する。

【不正な情報持ち出し】

システムへのアクセス権を持っている者が、不正に情報を持ち出すことにより、保護対象資産に漏洩の危害を加える。

【不正な情報処理】

システムへのアクセス権を持っている者が、不正に情報を処理することにより、保護対象資産に改ざんの危害を加えたり、目的外の利用を行ったりする。

【誤操作】

システムへのアクセス権を持っている者が、誤操作により保護対象資産に漏洩や改ざん等の危害を加える。

【個人番号をキーとした情報の収集】

公開されている情報やネットワークを流れるデータ等、正規/不正に限らず、個人番号をキーとして個人情報を収集する。

【データ分析】

公開されている情報やネットワークを流れるデータ等、正規/不正に限らず、なんらかの手段でデータを大量に取得し、それらのデータを分析することにより、個人を特定する。

【その他】

天災などによるデータの消滅など。

表 9 は、ユースケースから導かれた脅威に対し、その脅威を引き起こす攻撃手段（how）との対応関係をまとめたものである。

表 9　脅威と攻撃手段（how）

分類番号	脅威	攻撃手段（how）	被害の例
T1	**悪意の第三者による脅威**		
T1-1	悪意の第三者による情報漏洩	不正アクセス、 成りすまし、 ネットワーク盗聴等	（医療ユースケースの例） 悪意の第三者からの不正アクセス、成りすまし、ネットワーク盗聴などにより、医療情報管理機関等から個人の診療記録などの医療情報が漏洩される。
T1-2	悪意の第三者による情報改ざん	不正アクセス、 成りすまし等	（金融ユースケースの例） 悪意の第三者が個人番号を騙り、他人に成りすますことにより、勝手に口座が開設され犯罪等に利用される。
T1-3	個人番号をキーとした名寄せ	個人番号をキーとした情報収集等	（製品安全ユースケースの例） 個人番号をキーにして個人情報が収集され、個人情報の名簿が作られる。
T1-4	匿名化データからの個人特定	データ分析等	（医療ユースケースの例） 匿名化したつもりの情報が、個人を特定できるものになっていて、そこから個人が特定され

分類番号	脅威	攻撃手段（how）	被害の例
			る。あるいは同一人物に関する複数の匿名化データを集め分析することにより、そこから個人が特定される。
T2	**権限保有者による脅威**		
T2-1	権限保有者による情報漏洩	不正な情報持ち出し、誤操作等	（金融ユースケースの例） 金融機関の職員が資産情報を不正に持ち出し、そこから情報が漏洩する。
T2-2	権限保有者による情報改ざん	不正な情報処理、誤操作等	（金融ユースケースの例） 金融機関の職員による資産情報改ざんにより、金銭被害を受ける。
T2-3	番号をキーとした名寄せ	個人番号をキーとした情報収集等	（製品安全ユースケースの例） 個人番号をキーにして個人情報が収集され、個人情報の名簿が作られる。
T2-4	匿名化データからの個人特定	データ分析等	（医療ユースケースの例） 匿名化したつもりの情報が、個人を特定できるものになっていて、そこから個人が特定される。あるいは同一人物に関する複数の匿名化データを集め分析することにより、そこから個人が特定される。
T2-5	権限保有者による目的外利用	不正な情報処理等	（医療ユースケースの例） 個人番号が本来の医療情報連携に用いられず、保険会社加入審査などの目的で勝手に個人番号が利用される。
T2-6	本人の許可なしでの情報流通	不正な情報処理等	（医療ユースケースの例） 本人が了承していないのにも関わらず、病院同士で勝手に情報を共有し、本人にとって知られたくない情報が流通してしまう。※ただし、緊急を要する場合、本人の承諾なしで診療記録を連携できる仕組みについても検討が必要。
T3	**その他**		
T3-1	情報の劣化･消失によるサービス不履行	天災などによるデータの消滅等	個人情報を管理しているシステムの故障等により個人情報が消滅し、本来受けられるサービスが受けられなくなる。

６－３．安心安全な情報利活用のためのセキュリティ対策

本節では、各ユースケースから抽出した脅威に対抗するために必要となる、セキュリティ要件と対策について検討する。

一般的にセキュリティ対策は、技術的対策と法制度的対策に大別することができる。技術的対策はセキュリティを守るための直接的な対策であり、法制度的対策はセキュリティを守るための管理面における間接的な対策である。セキュリティ対策というと技術的対策ばかりが注目される傾向にあるが、技術的セキュリティ対策は強化すればするほど費用がかさみ、ときには利便性が悪化する場合もある。したがって、技術的対策だけでなく、法制度的な対策も強化し、両方でバランスの良い対策をとることが重要である。本検討では番号制度における脅威に対してセキュリティ要件を定義し、その要件に対して技術的面と法制度面の両面から対策を講じている。

６－３－１．セキュリティ要件

ここではまず、前節から導かれた脅威に対して、セキュリティ要件を定義する。

T1　：悪意の第三者による脅威に対するセキュリティ要件

T1-1：悪意の第三者による情報漏洩に対するセキュリティ要件

- R1：第三者からの不正アクセスを防止できること
- R2：成りすましを防止できること（本人であることを証明できること）
- R3：本人または本人が許可した者以外は利用できないこと
- R4：個人番号カード等の盗難･紛失の際、カード利用を停止できること
- R5：保護対象資産が管理されている DB から漏洩しないこと
- R6：保護対象資産がネットワークから漏洩しないこと
- R8：万が一、保護対象資産に危害があった場合、可能な限り補償がされていること

T1-2：悪意の第三者による情報改ざんに対するセキュリティ要件

- R1：第三者からの不正アクセスを防止できること
- R2：成りすましを防止できること（本人であることを証明できること）
- R3：本人または本人が許可した者以外は利用できないこと
- R4：個人番号カード等の盗難･紛失の際、カード利用を停止できること
- R7：保護対象資産の改ざんを検知できること
- R8：万が一、保護対象資産に危害があった場合、可能な限り補償がされていること

T1-3：個人番号をキーとした名寄せに対するセキュリティ要件

- R20：個人番号と基本情報、関連情報とは、分割管理されていること
  （個人番号漏洩がダイレクトに個人情報漏洩につながらないこと）

T1-4：匿名化データからの個人特定に対するセキュリティ要件

- R21：統計データなどの二次利用に用いる際、個人が特定されないように匿名化されていること
- R22：複数の匿名化データを集めても個人が特定できないこと

T2　：権限保有者による脅威に対するセキュリティ要件

T2-1：権限保有者による情報漏洩に対するセキュリティ要件

- R9：提供サービスを利用できる組織･人を認定できること
- R10：権限保有者を認証できること
- R11：権限保有者の役割（ロール）を定義できること
- R12：必要最小限のデータを除き、秘匿（暗号化）すること
- R17：権限保有者の誤操作が起きにくい仕組みにすること
- R8：万が一、保護対象資産に危害があった場合、可能な限り補償がされていること

T2-2：権限保有者による情報改ざんに対するセキュリティ要件

- R9：提供サービスを利用できる組織･人を認定できること
- R10：権限保有者を認証できること
- R11：権限保有者の役割（ロール）を定義できること
- R17：権限保有者の誤操作が起きにくい仕組みにすること
- R7：保護対象資産の改ざんを検知できること
- R8：万が一、保護対象資産に危害があった場合、可能な限り補償がされていること

T2-3：個人番号をキーとした名寄せに対するセキュリティ要件

- R20：個人番号と基本情報、関連情報とは、分割管理されていること
  （個人番号漏洩がダイレクトに個人情報漏洩につながらないこと）

T2-4：匿名化データからの個人特定に対するセキュリティ要件

- R21：統計データなどの二次利用に用いる際、個人が特定されないように匿名化されていること
- R22：複数の匿名化データを集めても個人が特定できないこと

T2-5：権限保有者による目的外利用に対するセキュリティ要件

- R13：権限保有者が行った処理を確認できること
- R14：権限保有者の目的外利用を抑止できること
- R15：本人または第三者により、自己に関する情報を確認できること
- R16：権限保有者の不正行為に対して罰則があること

T2-6：本人の許可なしでの情報流通に対するセキュリティ要件

- R18：本人の許可なしで情報が流通しないこと[14]
- R19：本人が承諾していることを証明できること

T3　：その他の脅威に対するセキュリティ要件

T3-1：情報の劣化･消失によるサービス不履行に対するセキュリティ要件

- R23：バックアップがとられていること

[14] 医療ユースケースの緊急を要する場合等については要検討。

６－３－２．セキュリティ対策

セキュリティ技術の進歩により、今日では様々な技術的対策が存在する。これらセキュリティ技術による対策は、主に「攻撃を防止することを目的とした技術」、「抑止効果を狙った技術」、「被害を最小化するための技術」の 3 つに大別することができる。

また、法制度的な対策は、技術的な対策を補完するものであり、より安心安全な番号制度を実現することができる。表 10 は、主な技術的対策と法制度的対策の概要をまとめたものである。

表 10　技術的対策と法制度的対策の概要

分類	対策の種別	セキュリティ対策	効果
技術的対策	攻撃を防止する対策	端末認証、ユーザ認証（IC カードを使った PKI/生体認証）、アクセス制御	利用者を認証し、成りすましを防止することができる。 悪意の第三者等から、保護対象資産への不正アクセスを防止することができる。
		通信路の暗号化	ネットワークを流れる情報（保護対象資産）の盗聴を防止することができる。
		自己情報コントロール技術 本人の承諾による処理技術	本人に関わる情報を本人がコントロールし、本人了承なしの情報流通を防止することができる。
		複数人による操作	権限保有者単独での誤操作を防止することができる。
		匿名化技術	データの二次利用の際、匿名化により個人特定ができないようにすることができる。
	攻撃を抑止する対策	アクセスログ管理 マイポータル技術	権限保有者による目的外利用を抑止するために、権限保有者が行った処理をログとして管理する。また、国民自身が本人に関する情報に対し、権限保有者が行った処理を確認することができる。
	被害を最小化する対策	蓄積データの暗号化 （保護対象資産の暗号化）	万が一、第三者が保護対象資産にアクセスできた場合でも、データ自身を暗号化することで、情報漏洩を防止することができる。
		電子署名	万が一、保護対象資産を勝手に書き換えられた場合でも、改ざんを検知し、改ざんされたことを証明することができる。
		ロールベースアクセス制御	各権限保有者のアクセス権限をロール（役割）に応じた必要最低限のものとし、権限以上の不正アクセスを防止することができる。
		カード失効・再発行	新たな個人番号を発行する仕組みを整備し、問題の発生した個人番号を無効化することができる。
		分散管理技術	クレジットカードの仕様で PCI-DSS[35]が推奨しているように、個人番号と基本情報、関連情報とを分割管理することで、万が一、情報が流出した時に、被害を最小化することができる。

分類	対策の種別	セキュリティ対策	効果
		バックアップ技術	複製（コピー）をあらかじめ作成し、たとえ問題が起きてもデータを復旧できるように備えておく。
法制度的対策	法制度による対策	第三者認定機関・監査機関の設置	個人番号管理センターと個人番号を利用する組織を認定する機関、およびそれらを監査する機関を設置する。これにより、番号制度に則った正しい運用を実現できる。
		認定制度策定	番号制度を利用することを認められた組織、および人を認定する制度の策定。これにより、闇金融など不特定多数の組織への番号提供、および情報提供を防止することができる。
		監査制度策定	認定制度が正しく運用されているかを監査する監査制度の策定。個人番号の目的外利用等の履歴を監査することで権限保有者による目的外利用を抑止することができる。
		罰則制度策定	権限保有者が不正（目的外利用、情報漏洩等）を行った場合の罰則規定の策定。これにより不正に対する抑止効果が期待できる。
		補償制度策定	番号制度に関連して、情報管理側の不備により被害（金銭被害、情報漏洩）が生じた場合の補償規定の策定。これにより、国民は万が一の被害に対して補償を受けることができる。
		不正アクセス禁止法 平成 11 年 8 月 13 日法律 128 号	インターネット等のコンピュータネットワーク等での通信において、不正アクセス行為とその助長行為を規制する。
		個人情報保護法 平成 15 年 5 月 30 日法律 57 号	個人情報を個人情報データベース等として所持している事業者に対して、主務大臣への報告やそれに伴う改善措置に従わない等の適切な対処を行わなかった場合に、刑事罰が科される。

また、表 11 は６－３－１．のセキュリティ要件に関して重複を考慮してまとめ、そのセキュリティ要件に対して、上記セキュリティ対策を「現在確立されている技術的・法制度的対策」と、「安心安全な番号制度の民間活用の実現に向けさらに検討すべき技術的・法制度的対策」に分けてまとめたものである。

表 11　主なセキュリティ対策

セキュリティ要件		現在確立されているセキュリティ対策		さらに検討すべきセキュリティ対策	
		技術的対策	法制度的対策	技術的対策	法制度的対策
R1	第三者からのアクセスを防止できること	ユーザ認証、アクセス制御	不正アクセス禁止法		
R2	成りすましを防止できること	ユーザ認証（IC カードを使った PKI/生体認証）		本人確認方式の高度化	
R3	本人または本人が許可した者以外は利用できないこと	ユーザ認証（IC カードを使った PKI/生体認証）		本人確認方式の高度化	
R4	カードの盗難･紛失の際、カード利用を停止できること		カード失効・再発行		カード運用ガイドライン策定
R5	保護対象資産が管理されている DB から漏洩しないこと	蓄積データの暗号化	個人情報保護法	蓄積データの完全なエンドツーエンド暗号化	
R6	保護対象資産がネットワークから漏洩しないこと	通信路の暗号化	個人情報保護法		
R7	保護対象資産の改ざんを検知できること	電子署名			
R8	万が一の場合、補償がされていること				補償制度策定
R9	提供サービスを利用できる組織･人を認定できること	ユーザ認証			認定制度策定
R10	権限保有者を認証できること	端末認証、ユーザ認証			
R11	権限保有者の役割（ロール）を定義できること	ロールベースアクセス制御			
R12	必要最小限のデータを除き、秘匿（暗号化）すること	蓄積データの暗号化	個人情報保護法	蓄積データの完全なエンドツーエンド暗号化	
R13	権限保有者が行った処理を確認できること			アクセスログ管理	
R14	権限保有者の目的外利用を抑止できること		個人情報保護法	アクセスログ管理 複数人による操作	監査制度策定 罰則制度策定
R15	本人または第三者により、自己情報を確認できること			マイポータル技術	監査制度策定
R16	権限保有者の不正行為に対して罰則があること				罰則制度策定
R17	権限保有者の誤操作が起きにくい仕組みにすること			複数人による操作	補償制度策定
R18	本人の許可なしでは情報が流通しないこと		個人情報保護法	自己情報コントロール技術 本人の承諾による処理技術	
R19	本人が承諾していることを証明できること				本人承諾制度の設計
R20	個人番号と他の情報が分割管理されていること	分割管理技術			
R21	個人が特定されないように匿名化すること	匿名化技術		匿名化技術の高度化	
R22	複数の匿名化データを集めても個人が特定できないこと	匿名化技術		匿名化技術の高度化	
R23	バックアップがとられていること	バックアップ技術			

６－３－３．安心安全な番号制度の民間活用の実現に向けさらに検討すべき技術的対策と法制度的対策

表 11 から分かるように、悪意ある第三者からの不正アクセス等による情報漏洩、情報改ざんに関する脅威は、現在確立されている技術的･法制度的対策によりおおむね対抗することができる。しかし、権限保有者による目的外利用や本人の許可なしでの情報流通に関する脅威に関しては、必ずしも対策が確立されているとは言えず、それが国民の不安につながっていると考える。

また、個人番号を騙った成りすましによる脅威や匿名化データによる個人特定の脅威も個人番号を民間利用した個人情報利活用の特徴的な脅威であり、現在のセキュリティ対策で十分とはいいきれない。

それゆえ、安心安全な番号制度の民間利用の実現に向けて、以下のセキュリティ対策の検討を深めることが重要と考える。

【権限保有者による目的外利用に対するセキュリティ対策（R13～R16)】

権限保有者の認証などは現在の技術で確立できるが、権限保有者による目的外利用や誤操作による脅威が残っている。権限保有者による目的外利用を抑止するためには、利用履歴を記録していることを知らせることが効果的である。そのためには、対象となるシステムに対してどのようなログを取得･管理すべきかを検討し、権限保有者が行った処理を確認できる仕組みが必要である。また、権限保有者による不正がないことを国民に証明するために、第三者監査機関を設置し、第三者による監査を行うことが重要である。また、第三者による監査だけでなく、国民自身が自己の情報に関する処理を確認できる仕組みを確立することで、国民が安心して番号制度を利用できるようになる。このような仕組みは、本人に関する情報を集約したサイト、「マイポータル（仮称)」をインターネット上に設け、個人情報が利用された履歴を自身で把握できるようにすることで実現できる。しかし、このようなマイポータルを設置するだけでは、自分の情報が目的外利用されていないかどうかを国民が日々チェックしなければならず、国民にとって負担となる可能性がある。それゆえ、自動的に目的外利用の疑いがある処理を監視し、その結果を本人に通知する仕組みなども考慮されるべきと考える。

主な検討課題を以下に示す。

- 第三者監査機関の設立、監査制度の策定
- 監査用ログの取得・管理方法の検討
- 権限保有者の不正行為に対する罰則制度の策定
- 国民自身が個人情報の利用履歴を確認できるマイポータル技術（自動的に目的外利用の疑いがある処理を監視し、その結果を本人に通知する仕組みを含む）の確立
- 万が一の被害に対する補償のあり方の検討

【本人の許可なしでの情報流通に関する脅威に対するセキュリティ対策（R18、R19)】

国民は、本人の知らないところで自分の情報が流通することに対して不安を抱いている。それゆえ、本人の許可なしでは情報流通ができない仕組みについて検討する必要がある。また、サー

ビス提供者側の説明の不備で、よく分からないうちに承諾してしまうケースも考えられる。「国民は何に対して了承したのか？」、「承諾しなければどうなるのか？」、「紙面による承諾書か？電子による承諾システムか？」など、どのようにして本人が承諾したのかを証明できるような制度設計が必要である。

一方、本人の許可なしで情報が流通することは問題ではあるが、医療ユースケースにおける緊急を要する場合のように、本人の承諾なしで診療記録を連携できる仕組みについても検討が必要である。したがって、このような例外のケースも考慮し、柔軟な制度設計をすることが重要である。

主な検討課題を以下に示す。

- 国民自身が自己の情報を管理できる自己情報コントロール技術の確立
- 本人の承諾による処理方法の検討および制度設計
- 例外処置の検討

【悪意の第三者による脅威（個人番号を騙った成りすましによる脅威）に対するセキュリティ対策（R2～R5）】

番号制度の民間活用において、本人が個人番号を提示して各サービスを受ける場合がある。その際、成りすましなど第三者による不正を防止するために、本人が本人であることを証明することが重要になってくる。現在、IC カード等の認証技術を用いて本人確認をすることができるが、「IC カードインフラのない場所での使用はどうするのか？」、「IC カードが盗難された場合どうなるのか？」「万が一、成りすましによる被害があった場合、どうなるのか？」など国民が不安に感じる課題が残されている。また、本人確認方法を IC カードによる認証ではなく、携帯電話などを用いて認証する方法も考えられる。番号制度の利便性向上のため、それらのデバイスでの本人確認方法についても今後検討する必要がある。

主な検討課題を以下に示す。

- カード運用ガイドラインの策定（カード失効･再発行の手順およびカード利用方法の確立）
- カードインフラのない場所での本人確認方式の検討
- 携帯電話等、その他のデバイスを用いた本人確認方式の検討
- 万が一の被害に対する補償のあり方の検討

【匿名化データによる個人特定の脅威に対するセキュリティ対策（R21～R22）】

医療ユースケース（PHR 二次利用）に見られるように、個人情報を統計情報として扱う場合もある。このように個人情報を集め統計情報として利用する場合、収集された情報から個人が特定されないように匿名化処理を施すことが重要である。また、名前や住所等、直接個人を特定する情報を削除しても、そこに含まれる情報を分析することで個人を特定できてしまっては、匿名化の意味を成さない。それゆえ、たとえ複数の匿名化情報が集まっても個人を特定できないような匿名化技術が望まれる。

主な検討課題を以下に示す。

- 匿名化方式の検討

- 複数の匿名化情報が集まっても個人を特定できないような匿名化技術

【その他特記すべきセキュリティ対策（R12)】

個人情報や企業情報の民間活用に関して、各センターにおける新たな情報漏洩対策として、蓄積データの完全なエンドツーエンド暗号化（プロキシ再暗号化技術など）が必要となってくる。通常､情報漏洩対策としてはデータの暗号化が一般的であるが､医療連携やPHR一次利用等では、現在普及している暗号技術だけでは要件を満たさない。医療連携やPHR一次利用では、診療情報等を暗号化して医療情報管理機関やPHR管理機関で管理し、必要に応じて医療連携やPHR一次利用に用いるが、暗号化する時点では、その診療情報等を次に利用する病院や医師等は決まっていない。つまり、通常の暗号化技術は、相手の暗号化鍵で暗号化し情報共有をするが、医療連携やPHR一次利用等では、次にそれらの診療情報を利用する相手が決まっていないため、診療情報を暗号化するための暗号化鍵を定めることができない。それゆえ、最終利用者があらかじめ決まっていなくても、医療情報管理機関やPHR管理機関等で診療情報等が復号されることなく、最終利用者に暗号化データを送付することが可能な暗号化技術（プロキシ再暗号化技術など）が必要となってくる。

主な検討課題は以下である。

- プロキシ再暗号化技術（暗号化したままで別の復号鍵に付け替えられる技術）

６－４．国民の不安に対する回答

本章の冒頭で述べたとおり、個人情報や企業情報を利活用していくためには、技術的・法制度的なセキュリティ対策を講じることはもちろん、それらの対策により、安心安全な情報の利活用をどのように実現できるかということを国民に分かりやすく説明し、理解を得られるようにしなければならない。

本節では、国民が抱く不安に対する回答として、６－３．で述べたセキュリティ対策と対比させながら、国民の理解を得られるような国民目線での回答例を示す（表 12)。

表 12　国民の不安に対する回答

	想定される国民の不安	回答	関連番号
1.	偽造、成りすましによって、不正に個人情報がのぞき見されるのではないか？	基本的にICカードを利用したユーザ認証（PKI、生体認証など）により偽造・成りすましを防止することができます。しかし、ICカードインフラがない場合で本人確認が必要なケースなどもあり、そのような状況も鑑み、サービスレベルに応じた様々なケースにおける本人確認手段の検討が必要です。	R2
2.	他人の個人番号を使って､銀行口座開設やクレジットカードの発行、携帯電話購入（電話開設)、借金、買い物などをされる危険性があるのでは？	COCNではサービスレベルに応じて本人認証が必要なサービスと必要のないサービスがあることを想定しています。銀行口座開設やクレジットカード発行などの利用には、本人確認を必要とします。具体的にはICカードを利用したユーザ認証（PKI、生体認証など）などにより本人確認を行います。それゆえ、他人の個人番号を騙るだけでは、銀行口座開設、クレジットカードの発行などはできない仕組みとなります。	R2

	想定される国民の不安	回答	関連番号
3.	自分の個人番号カードを落としてしまったらどうなる？再発行してもらえるのか？落としたカードは無効にしてもらえるのか？	たとえ第三者が紛失したカードを拾っても、上記のとおり、ユーザ認証しないと、そのカードは使うことができません。また、COCNでは、個人番号の民間利用において、利用者が個人番号カードを紛失した場合、カードを無効にして、新たなカードを再発行することを想定しています。ゆえに、たとえ第三者が紛失したカードを拾ってもそのカードは使うことができません。	R4
4.	個人番号は変更できるのか？他人に知られた番号は使いたくない。	個人番号は生涯不変の番号であることが望ましいのですが、COCNでは、個人番号が犯罪等に悪用された場合等、一定の条件の下では、個人番号を変更できる仕組みを検討しています。また、個人番号を利用するには本人確認が必要となるため、個人番号が他人に知られただけでは他者が悪用することができない仕組みとなっています。本人確認が可能な認証情報が個人番号と一緒に他人に知られてしまった場合は、認証情報を更新するか、もしくは新しい個人番号を再発行する必要があります。	R4
5.	個人情報が改ざんされたりしないか？	個人情報は、電子署名技術などにより、改ざんを検知することができます。また、個人情報の改ざんに限らず、間違った個人情報が登録されてしまうケースも考えられます。この様なケースも考慮し、自己の情報を自分で確認できる仕組みが必要です。また、万が一、個人情報が改ざんされ被害が生じた場合に備え、補償のあり方の検討も今後の課題です。	R7 R8 R15
6.	他人が個人番号を悪用して損害を受けたら、誰が補償してくれるのか？	個人番号を悪用した者に対して損害賠償請求をすることが原則ですが、現在のクレジットカードの仕組みのように、発生した損害に対して保険会社により補償するケースも考えられます。それらの状況も踏まえ、番号制度の民間活用において損害が発生した場合の補償のあり方の検討も今後の課題です。	R8
7.	民間企業にてプライバシーの侵害はおこらないか？	第三者機関による監査制度を策定し罰則制度を設けることで、民間企業による目的以外の利用を抑止することができます。また、利用する情報によっては、個人番号制度を利用できる民間企業を認定する制度も策定し、違反が発生した場合の罰則の強化や認定の取り消しの仕組みも必要です。	R9 ～ R16
8.	職員による盗み見、不正閲覧、個人情報の持ち出しに使われないか？	職員の業務内容に応じて必要最低限の情報しか閲覧できないようにする仕組みにより盗み見、不正閲覧を防止することができます。また、盗み見、不正閲覧、個人情報の持ち出しのような不正行為に対しては法律により、厳しい罰則が科せられます。また、職員の不正行為を抑止するために、職員が行った操作はすべてログに取り、第三者機関により監査される仕組みが必要と考えます。	R10 ～ R16
9.	誰が悪用したのか見つけることはできるのか？	個人情報へのアクセスはすべてログに取り、第三者機関により監査される仕組みが必要です。これにより、いつ、誰が、何の情報にアクセスし、どのような処理を行ったのか調べることができます。	R13 R15
10.	個人情報を目的外に使われないか？	第三者機関による監査制度に基づき、職員が行った操作はすべてログに取り、第三者機関により監査されます。また個人番号制度を利用できる民間企業を認定する制度を策定し、目的外利用があった際には認定を取り消す仕組みも必要です。これらの対策により、個人番号を利用してダイレクトメールを送るなど、目的外の利用を抑止することができます。また、情報を集約するセンターでは、そこで行われる機能を最小化し、その機能を実現するために必要な情報以外の情報は暗号化し、上記センターにおいては復号することなしにその機能を実行します。これによって、そもそも情報を集約することを目的とする機関における不正を予防します。	R13 ～ R15
11.	国家による国民の監視、個人情報の支配に使われるのでは？	民間が扱う情報に関して、本人が望む目的以外では利用できない仕組みが必要です。国民の監視につながるような目的で利用できないような仕組みを実現するために、第三者監査機関を設置することが重要です。また、「その第三者監査機関としての要件は何か？」「どのように何を監査するのか？」「不正が発覚した場合どうするのか？」等、監査制度や罰則制度の策定が必要です。	R13 ～ R16

	想定される国民の不安	回答	関連番号
12.	民間に広く個人番号が流通すると、どのような形で自分の個人番号が悪用されるのかが分からないので不安である。	この様な国民の不安を解消するために、本人の許可なしでは情報が流通しない仕組みが必要です。また、自分の情報が何処にあり、どのように扱われているのかを自分で確認し制御できる仕組み（自己情報コントロール）を確立することにより不安を取り除くことができると考えます。	R13 R14
13.	個人番号によって様々な個人情報が集約できてしまう。一つの個人情報が漏れるとすべての情報が漏れてしまうリスクがあるのでは？	個人番号は、基本情報や関連情報などとは別々に管理されることが重要です。また関連情報は、医療、製品安全、金融など分野毎に分散管理することも重要です。さらに、個人情報にアクセスする人を認証する仕組みも必要です。この様な仕組みにより、個人情報を誰もが個人番号により集約できるわけではなく、また、たとえ一つの個人情報が万が一漏洩してもすべての個人情報に影響が出るわけではありません。	R20
14.	医療：統計、治験情報の共有によるプライバシー漏洩は起こらないか。	統計や治験情報に医療情報を活用する場合における匿名化技術の確立が重要です。統計等に用いる場合、匿名化を施すことで個人情報の漏えいによるプライバシーの侵害は起こりません。この様な匿名化技術は、たとえ複数の匿名化情報を集めても個人を特定できないことが求められます。	R21 R22

７．法律や制度についての検討

番号制度の民間活用を行うためには、国として情報利活用を行う上での法制度の整備に加え、下記の法的、制度的検討が必要となる。

（１）　番号制度の民間利活用を機能的に実現するための法整備

①個人番号管理センターの設置

②民間利用するための法規制の緩和および新たな法制度・ガイドラインの規定

（２）　番号制度の民間利活用を安心安全に運用するための法整備

①第三者機関（認定・監査機関）の設置

②国民のセキュリティ上の不安を取り除くための法制度策定

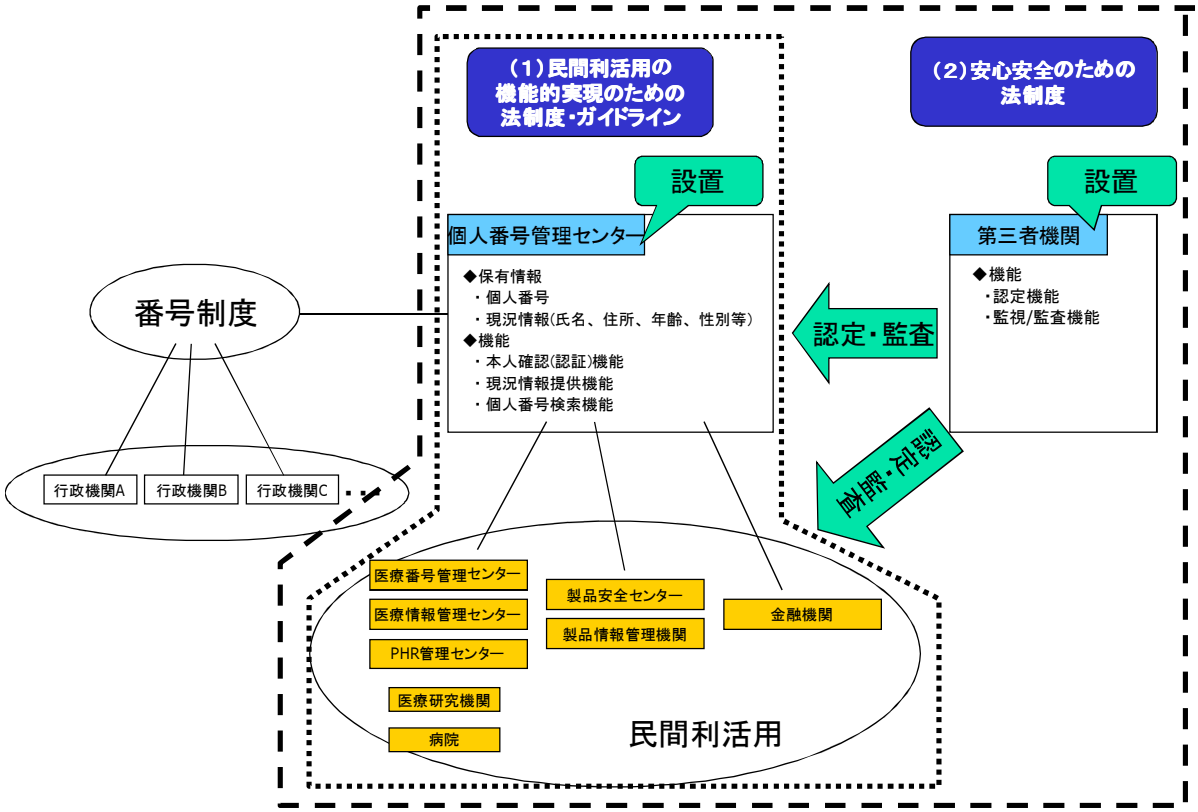


図 33　必要となる法制度イメージ

本検討では、上記に示した民間活用を図る上で変更または新規に必要となる法制度などについて検討を行う。

７－１．変更または新規に必要となる法制度の検討

本節では、５章で述べた番号制度による情報の民間利活用を実現していく上で、変更または新規に必要となる法制度についての検討結果について示す。

７－１－１．番号制度の民間利活用を機能的に実現するための法整備

番号制度を用いた情報の利活用を機能的に実現するためには、番号にかかる民間利用の機能を一元的に提供する個人番号管理センターの設置が必要となる。また、ユースケース毎の検討では現状の法規制の枠を超えた新たなサービスによる民間活用も想定しているため、法規制の緩和および新サービスの枠組みを規定する新たな法制度・ガイドラインの規定も必要となる。

（１）個人番号管理センターの設置

番号制度の検討の中で、民間利用において、番号および本人を特定する情報の利用による本人確認、現況確認の実施を行う、行政内システムとは切り離した機能を有する「個人番号管理センター」の設置を必要としている。また、個人番号管理センター設置の根拠となる法制度も必要になると考えられる。

表 13　設置が必要な機関

項目	機能
個人番号管理センターの設置	行政内システムとは切り離された番号管理を行う機関。 本人確認（認証）機能と現況情報提供機能と個人番号検索機能を備える

（２）民間利用するための法規制の緩和および新たな法制度・ガイドラインの規定

今回、番号制度による情報の民間活用を進める上でユースケース毎に新たなサービスの検討を行った。このサービスを機能的に実現するためには、現状の法規制の枠を超えたものもあるため、法規制の緩和が必要となるものがある。また、新たなサービスを実現するためにはその枠組みを規定する新たな法制度・ガイドラインの規定も必要となる。以下では、各ユースケースで必要となる法規制の緩和と新たに必要となる法制度・ガイドラインについて示す。

表 14　ユースケース共通の実現機能と法制度

実現したい 機能・サービス	法規制の緩和・変更が 必要な法令	内容
番号制度を利用した本人確認および現況確認の実施	住民基本台帳法	個人番号管理センターにおいて、個人番号と認証情報（パスワード等）を用いて、基本四情報の照会を可能とする。
公的個人認証を民間で活用	行政手続きオンライン三法	個人番号管理センターにおける本人確認サービスにおいて、公的個人認証制度の活用を可能とする。

表 15　医療ユースケースの実現機能と法制度

実現したい 機能・サービス	法規制の緩和・変更が 必要な法令	関連ガイドライン	内容
医療情報および PHR 情報を本人了承の下に番号制度により紐付けて利活用	医療法	個人情報の管理に関する指針について（総務省） 総務省、経産省、厚労省のガイドライン等	医療情報および PHR 情報を病院などで利用する上での規定・ガイドラインの策定。
匿名化した医療情報を二次利用	個人情報保護法 医療法 統計法 外為法（海外利用時）	個人情報の管理に関する指針について（総務省） 疫学研究に関する倫理指針（文科省・厚労省） 総務省、経産省、厚労省のガイドライン等	確実な情報の匿名化を行うことを条件に、研究機関などで医療情報を統計利用することを可能とする。 研究機関などで医療情報を、プライバシーを保護した状態で統計利用するための、情報の確実な匿名化を行う規定、情報取り扱い・廃棄のルールを定めたガイドラインの策定。

表 16　製品安全ユースケースの実現機能と法制度

実現したい 機能・サービス	法規制の緩和・変更が 必要な法令	関連ガイドライン	内容
製品リコールおよび保守引き継ぎに番号制度を利用	消費生活用製品安全法 製造物責任法（PL 法） 電気用品安全法（PSE）		製品リコールおよび製品の保守継続性において、個人番号制度を活用することを可能とする制度の策定、および関連制度の変更。

表 17　金融ユースケースの実現機能と法制度

実現したい 機能・サービス	法規制の緩和・変更が 必要な法令	関連ガイドライン	内容
番号制度を利用した本人確認を口座開設時に利用	銀行法 保険業法 犯罪収益移転防止法	金融庁ガイドライン	個人番号管理センターにおける本人確認サービスを用いて、銀行口座開設時等で必要となる本人確認を可能とする制度の策定、および関連制度の変更、ガイドラインの策定。
金融機関と行政機関の間で、本人に関する証明書類等のバックオフィス連携	所得税法（納税証明書）		金融機関の発行する電子的な各種証明書を用いて、税務処理を行うことを可能とする制度の策定、および関連制度の変更。

７－１－２．番号制度の民間利活用を安心安全に運用するための法整備

番号制度による情報の民間利活用を安心安全に行うには、「セキュリティについての検討」にて述べたとおり、セキュリティ上の問題（脅威）に対抗するため、第三者機関の設置と、組織の認定制度、罰則制度、補償制度の策定が必要となる。

（１）第三者機関（認定・監査機関）の設置

罰則や番号制度を活用する組織や権限保有者の認定を行い監視・監査を行う第三者機関の設置が必要となる。第三者機関の設置は、番号制度のグローバル展開を見据えた上でも、必要不可欠な要件である。これは、EU 個人情報保護指令として、「個人データの第三国への移転は、この指令に従って採択された国内規定の順守を損なうことなく、当該第三国が十分なレベルの保護措置を確保している場合に限って行うことができることを定めなければならない」との規定があり、十分な保護措置の要件として第三者機関の設置を求めているためである。また、第三者機関設置の根拠となる法制度も必要になると考えられる。

表 18　設置が必要な機関

項目	機能
第三者機関の設置	個人番号管理センターおよび個人番号を利用する公的組織・民間組織の認定、監視、監査を行う機能を備える

（２）国民のセキュリティ上の不安を取り除くための法制度策定

民間活用を行う上で、国民のセキュリティ上の不安を取り除くため、「セキュリティについての検討」にて述べたとおり、認定制度、罰則規定、補償制度の整備も必要となる。

表 19　規定が必要な制度

必要となる制度	内容
個人番号管理センターの認定制度	第三者機関により、個人番号管理センターが個人番号および現況情報（基本四情報）を適切に管理・運用していることを認定する制度。 監視、監査の規定も必要。
個人番号を利用する公的組織・民間組織の認定制度	第三者機関により、個人番号を利用する公的組織・民間組織（医療番号管理センター、医療情報管理機関、PHR 管理機関、製品安全センター、製品情報管理機関、金融機関など）が、個人番号および現況情報（基本四情報）を適切に管理・運用していることを認定する制度。 監視、監査の規定も必要。
不正行為の罰則や責任範囲を定める制度	番号制度に関連して、不正（目的外利用、情報漏洩）を行った場合の罰則規定の策定、および権限保有者の責任範囲の規定。
国民の被害を補償する制度	国民が具体的な被害（金銭被害、情報漏洩、情報改ざん）を受けた場合に、補償を行うための制度の整備。

８．クラウドコンピューティング基盤の整備に向けた提言

（１）官の管理する個人番号、個人情報の民間活用

現在国で検討されている国民 ID や共通番号制度の個人を特定することができる番号、および官の管理する個人情報（名前、生年月日、性別、住所等）を、民間のサービスにおいても個人を特定するために利用できるようにすることを提案する。民間サービスにおいて住民票、戸籍等で行っていた本人確認が容易かつ信頼性の高いものとなり、サービスの提供者、利用者双方にメリットが大きい。また民間および官民連携の新たな利便性の高いサービスを生み出す基盤となると考えられる。

（２）個人番号管理センターの設立

国の番号制度や官の管理する個人情報を民間で利用するための機関（個人番号管理センター）を設立することを提案する。このセンターは、クラウドコンピューティング基盤がこの個人番号を利用する場合、国の番号制度を運用しているシステムと民間サービスを直接接続するのではなく、個人番号や個人情報の安全な取り扱いや、国や自治体等の公的機関のもつ信頼性を保つために双方のシステムを中継する機関である。

（３）第三者機関の設置

本プロジェクトで提案するクラウドコンピューティング基盤やその上で実現されるサービスにおいて、個人番号や個人情報の利用が正しく行われているかを監視する第三者機関の設置を提案する。その機関の持つ機能は、番号の取り扱いの監視をする役割であり、個人番号および個人情報について個人が意図しない利用がされていないことを担保する機関である。

（４）関連する法制度、ガイドラインの検討

国の番号制度や官の管理する個人情報を民間活用するために見直しが必要な法制度やガイドラインについての検討が必要であると考える。そのなかでは、個人番号や個人情報の不正行為に対する罰則や個人番号を扱う担当者の責任範囲を定める制度の制定に関連する検討も必要である。また、それに加えて個人番号管理センターや第三者機関を設置するための制度の制定が必要であると考える。

（５）官民連携しての技術開発およびシステムの開発、実証

サービスを実現する上での技術課題については、技術開発を進めていくことやシステムの実現性を実証する実証実験を実施して解決していく必要がある。

- 本人の意思を反映した情報アクセス制御が可能なシステムの開発と実証
- 大量、長期にわたる安全な情報のライフサイクル管理可能なシステムの開発と実証
- 確実に情報を匿名化する技術の開発
- 長期間（無期限で）データを安全に保存、簡単に利用できる技術の開発
- 膨大な時系列データの効率的処理技術の開発

９．今後の活動

今後は以下に示す検討活動を継続し、提言の実現フェーズの活動へ移行できるよう議論と準備を進めていく。

（１）本年度の検討内容をより深く、より具体的にする

本報告書では、医療、製品安全、金融に関わる分野でのユースケースを検討した。継続してこれらのユースケースの検討を深め、より具体的な内容にしていく。また分野を統合するクラウドシステム全体のアーキテクチャやシステム要件、クラウド間で交換される情報の標準化などの検討を進める。必要に応じて、新メンバーの加入や関連した検討を行っている他の団体や組織と連携を取り議論を広げ深めていく。同時にシステムやサービスの具体化を進め実証実験の実施を目指す。また、必要に応じて新たなユースケースも検討する。

（２）番号制度に関する検討

2011 年 1 月 31 日、政府から「社会保障・税に関する番号制度についての基本方針」が示され、社会保障・税に関する番号制度の 2015 年の利用開始までの道筋が示された。2015 年の番号制度開始の時には、本報告書で検討した民間利用するための番号制度に対する要件が反映されているように、活動および番号制度に関する議論を継続していく。

（３）セキュリティに関する検討

本報告での脅威分析とセキュリティ対策の検討結果を踏まえ、今後は、本報告により明らかになったセキュリティの課題について深堀し、安心安全な番号制度の民間活用の実現に向けて更なる検討を進める。

（４）実証実験に向けた検討

本報告書のユースケースで述べたサービス、またこれから検討を進めるユースケースのサービスは、いずれも今までにないものである。よって、これらのサービスを実現し普及させていくためには、想定できない様々な問題点が出てくると考えられる。そのため、実証実験によりフィージビリティの確認を行うことは必須であると考えられることから、今後は実証実験を検討する場を設けて議論を進めていく。

（５）関係省庁、地方自治体への働きかけ

本報告書で提示した、個人情報と企業情報を安全に共有できる仕組みは、国の行政や企業活動の基盤となるものであり、国民生活をより利便性を高め充実させるものである。しかし、実現に際しては、多くの技術的課題、制度的課題がある。これらの課題には、企業だけでは解決が困難なものも含まれており、産学官の連携と協力が必要であると考えている。プロジェクトでの検討を進めながら、並行して各関連機関に働きかけていく。

（６）サービスのグローバル展開のための検討

クラウドコンピューティング基盤上で実現される新サービスが、グローバルに展開するために解決が必要な技術的な課題や、考慮しなければならない EU 指令等の法制度の課題への対応等について検討していく。

１０．別紙

１０－１．番号制度に関する COCN の考え方

表 20　番号制度に関する COCN の考え方

項目	COCN の考え方	基本方針案（一部中間整理案）
利用範囲	・民間企業でも利用可能 ・民－民－官の関係で利用可能なことはもちろん、民－民においても利用可能であること ※ただし、利用できる民間企業は、高い情報セキュリティレベルを維持できると認定された特定企業、団体に限定すべき	・まずは、社会保障分野（年金、医療、福祉、介護、労働保険）と税務分野（国税、地方税） ・将来的には、幅広い行政分野、国民同意に限定した民間サービス ・民－民－官の関係で利用可能なこと
番号対象者	・番号制度の対象となる個人 ・法人についても番号制度が必要 ※法人の番号制度については別途検討が必要	・日本国民及び中長期在留者、特別永住者等の外国人
番号の存在	・番号は本人を一意に特定できる番号とする ・「見える番号」と「見えない番号」が存在する	・全員が唯一無二の番号を持っていること ・行政機関間等で利用される情報連携 ID とは同一である必要はない（中間整理）
番号の表現形式	＜見える番号＞ ・見える番号は、人間が記憶などにより、口述や記述ができるものとして存在 （本人が記憶できる仕様であることが望ましい） ＜見えない番号＞ ・見えない番号は、番号制度のアンカーとして厳重管理され、見せない番号として存在	・目で見て確認できる番号であること ・情報連携 ID は、目で見て確認できることは不要（中間整理）
番号の変更可否	＜見える番号＞ ・基本的に変更は不可。ただし、個人番号の使用に不都合がある場合、家庭裁判所等の手続きを経て変更を認める等の配慮が必要 ＜見えない番号＞ ・変更不可	
保持期間	・個人番号を利用するサービスの制度が求める期間保持（基本的イメージとして、出生時に付番） ・将来見える番号が再利用されることも視野に、見えない番号によって追跡性を担保する等の仕組みの検討が必要	

項目	COCN の考え方	基本方針案（一部中間整理案）
氏名・住所等の情報との関係	・番号と連携する本人を特定する情報（氏名、住所等）が関連付けられていること ・氏名、住所等は最新の情報と関連していること ・住基四情報に加えて、死亡年月日の情報が必要	・最新の住所情報が関連付けられていること
番号の管理方式	・各分野別の番号とは番号間で連携 ・新しい番号を利用する分野（既存番号を置き換える分野等）は、各分野の要件、プライバシー等を鑑み要検討	・プライバシー保護、コスト等を鑑み、一元管理または分散管理とすべき。分散管理の場合の具体的分野について今後検討（中間整理）
付番機関	・番号制度を広い分野で利用すべきとの要件が満たされるような性格を持った機関の設置を検討すべき ・実際の付番業務、個人番号カードの発行業務は基礎自治体が担うことが現実的	・歳入庁の創設の検討を進める ・個人の付番：当面は総務省 ・法人の付番：当面は国税庁
データベースの管理	・データベースについては、分散管理方式とすべき	・データベースについては、分散管理方式とする
個人情報保護の徹底	・本人が自らの情報（番号）への行政機関によるアクセス記録を確認できる手段を提供すべき ・民間企業からのアクセスについても同様 ・第三者機関を設置すべき ・目的外利用を禁止する法令および罰則等にて不正利用を防止すべき ・民間利用については、情報セキュリティおよび個人情報管理の運用が確立されている企業、団体に限定すべき。例えば、P マーク等の認証制度等と同様の利用企業の認証制度を確立すべき	・最低限、「自己情報へのアクセス記録の確認」、「第三者機関の設置」、「目的外利用防止に係る具体的原則明示」、「関係法令の罰則強化」を実施する方向で検討

１０－２．各ユースケースにおけるセキュリティ脅威分析（詳細）

ここでは、各ユースケースにおける詳細なセキュリティ脅威分析について記載する。ここで挙げられる脅威は、既に各分野の組織においてセキュリティ対策が施され、現実にはその様な脅威が発生する確率が極めて低いものもある。

（１）医療ユースケースにおける脅威

医療ユースケースにおいて、保護対象資産（what）が適切な管理下にある時に存在しうる場所（where）を以下の表 21 に示す。

表 21　医療ユースケースにおける保護対象資産とその管理場所

場所（where）	保護対象資産（what）		
	個人番号	基本情報	関連情報
個人番号管理センター	○	○	○　（認証用情報）
医療番号管理センター	○	―	○　（医療番号、病院情報）
医療情報管理機関	○	○	○　（医療番号、医療情報）
PHR 管理機関	○	○	○　（医療番号、PHR 情報）
病院･診療所	○	○	○　（医療番号、医療情報）
研究機関	―	―	○　（匿名化医療情報）
上記の場所間のネットワーク上	○	○	○　（上記情報）

（凡例　○：存在する　―：存在しない）

これらの保護対象資産に対し、医療ユースケースにおいて具体的にどのような脅威があるかを分析した。表 22 は、医療ユースケースから導かれた脅威をまとめたものである。

表 22　医療ユースケースにおける脅威一覧

サービスシーン	脅威/課題	具体的な被害(why)	脅威主体(who)		保護対象資産(what)				攻撃手段(how)
			悪意の第三者	権限保有者	場所(where)	個人番号	基本情報	関連情報	
共通	番号管理センターから、個人番号/基本情報/認証情報が漏洩する	情報の入手により、情報の悪用、プライバシーの侵害が発生する	●		番号管理センター	●	●	●	不正アクセス、成りすまし等
共通	医療番号管理センターから、個人番号/医療番号等が漏洩する		●		医療番号管理センター	●		●	不正アクセス、成りすまし等
共通	病院から、個人番号/基本情報/医療情報等が漏洩する		●		病院	●	●	●	不正アクセス、成りすまし等
PHR 一次利用	PHR 管理機関から、個人番号/基本情報/PHR 情報等が漏洩する		●		PHR 管理機関	●	●	●	不正アクセス、成りすまし等
PHR 二次利用	医療情報管理機関から、個人番号/PHR 情報等が漏洩する		●		医療情報管理機関	●		●	不正アクセス、成りすまし等
共通	番号管理センター/病院/医療番号管理センター/PHR 管理機関の間のネットワーク上で、個人番号/基本情報/関連情報が漏洩する		●		ネットワーク上	●	●	●	ネットワーク盗聴等
共通	番号管理センターから、個人番号/基本情報/認証情報が漏洩する			●	番号管理センター	●	●	●	不正な情報持ち出し等
共通	医療番号管理センターから、個人番号/医療番号等が漏洩する			●	医療番号管理センター	●		●	不正な情報持ち出し等

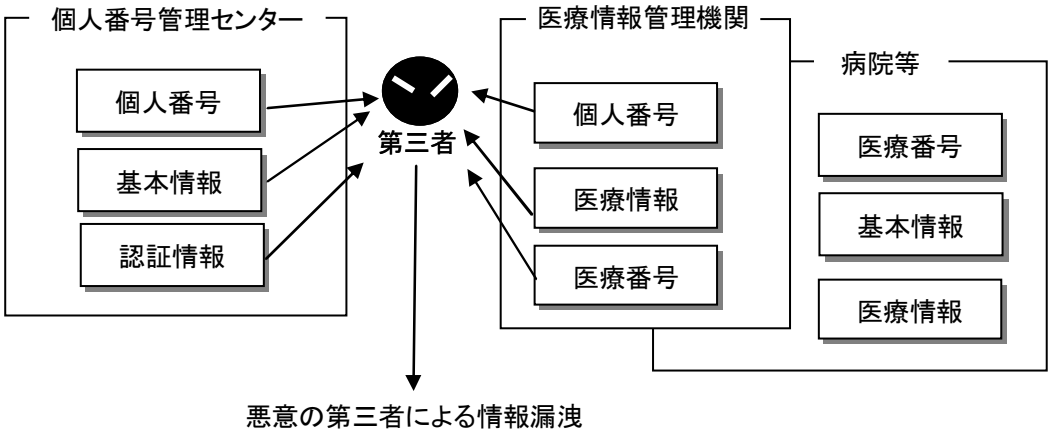
サービスシーン	脅威/課題	具体的な被害(why)	脅威主体(who)		保護対象資産(what)				攻撃手段(how)
			悪意の第三者	権限保有者	場所(where)	個人番号	基本情報	関連情報	
共通	病院から、個人番号/基本情報/医療情報等が漏洩する			●	病院	●	●	●	不正な情報持ち出し等
PHR 一次利用	PHR 管理機関から、個人番号/基本情報/PHR 情報等が漏洩する			●	PHR 管理機関	●	●	●	不正な情報持ち出し等
PHR 二次利用	医療情報管理機関から、個人番号/PHR 情報等が漏洩する			●	医療情報管理機関	●		●	不正な情報持ち出し等
共通	情報漏洩された個人番号/基本情報/関連情報を収集し、番号を基に名簿化する	名簿化され、情報が売買されることでより広範囲に情報が漏洩	●		管理外	●	●	●	個人番号をキーとした情報収集等
共通	病院/医療情報管理機関/PHR 管理機関の関連情報を改ざんする	改ざんにより、本来受けられるはずのサービスが受けられなくなる	●		病院/管理機関			●	不正アクセス、成りすまし等
共通	病院/医療情報管理機関/PHR 管理機関の関連情報を改ざんする			●	病院/管理機関			●	不正な情報処理、誤操作等
共通	病院/医療情報管理機関/PHR 管理機関の個人番号/基本情報/関連情報を目的外利用する	診療記録等を保険会社に転売される		●	病院/管理機関	●	●	●	不正な情報処理等
共通	本人了承なしに病院/医療情報管理機関/PHR 管理機関の間で個人番号/基本情報/関連情報が流通する	本人了承なしに知られたくない情報が流通してしまう		●		●	●	●	不正な情報処理等

サービスシーン	脅威/課題	具体的な被害(why)	脅威主体(who)		保護対象資産(what)				攻撃手段(how)
			悪意の第三者	権限保有者	場所(where)	個人番号	基本情報	関連情報	
PHR 二次利用	基本情報（準識別子）を匿名化したつもりが、一部のデータは個人を特定できるものになっている、あるいは匿名化したつもりの基本情報をキーとして名寄せできる	不完全な匿名化により、個人が特定されてしまう	●	●	研究機関		▲	●	データ分析等
PHR 二次利用	破棄または返却するはずの匿名化データが、されないままになっている	個人が特定されてしまう可能性が高まる		●	PHR 管理機関		▲	●	誤操作等

表 22 から分かるように医療ユースケースにおいて、保護対象資産およびその管理場所、脅威の主体者、サービスシーンにより、様々な脅威が存在するが、これらを脅威の種別に着目すると、以下のように分類できる。

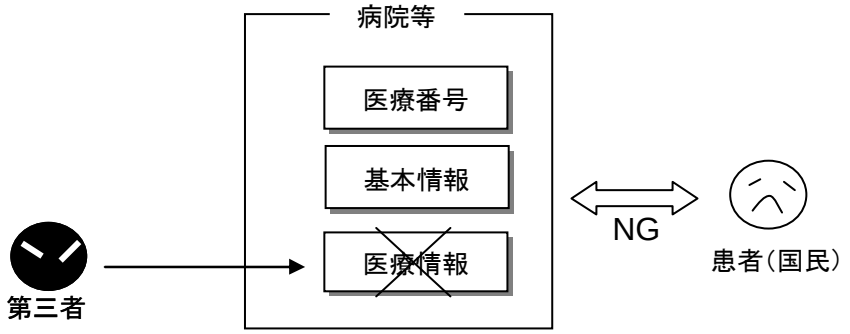
【T1】悪意の第三者による脅威

【T1-1】悪意の第三者による情報漏洩



例）悪意の第三者からの不正アクセスにより医療情報管理機関等から個人の診療記録などの医療情報が漏洩する。

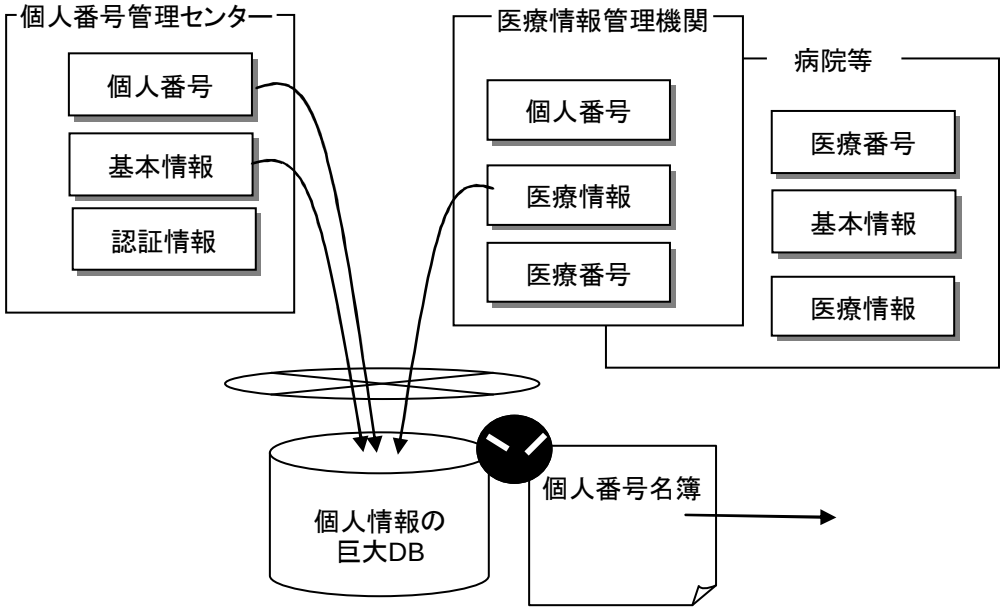
【T1-2】悪意の第三者による情報改ざん



医療データ情報が改ざんされ，正常な健康・医療サービスに支障

例）悪意の第三者からの不正アクセスにより病院等の医療情報が改ざんされ、正しい診断ができなくなる。

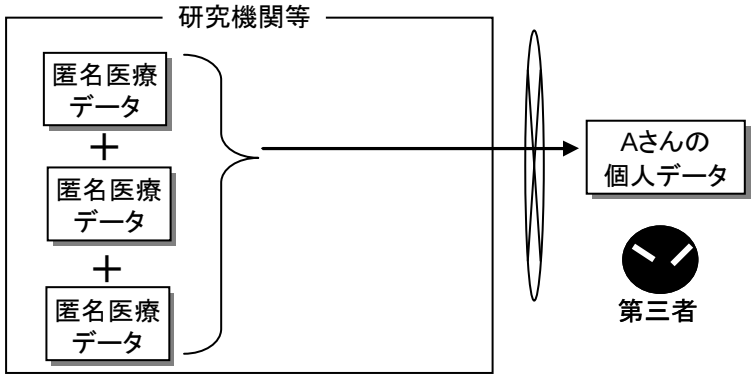
【T1-3】個人番号をキーにした名寄せ



個人番号をキーにして個人情報を収集し、巨大DBが作られる
個人番号の名簿が作られ，医療情報の売買に使われる

例）個人番号をキーにして、あらゆるところから個人情報が収集され個人情報に関する巨大 DB が作られる。また、それらの情報から名簿が作られ、個人の診療記録などの医療情報を欲しがる組織に売買される。

【T1-4】 匿名化データからの個人特定

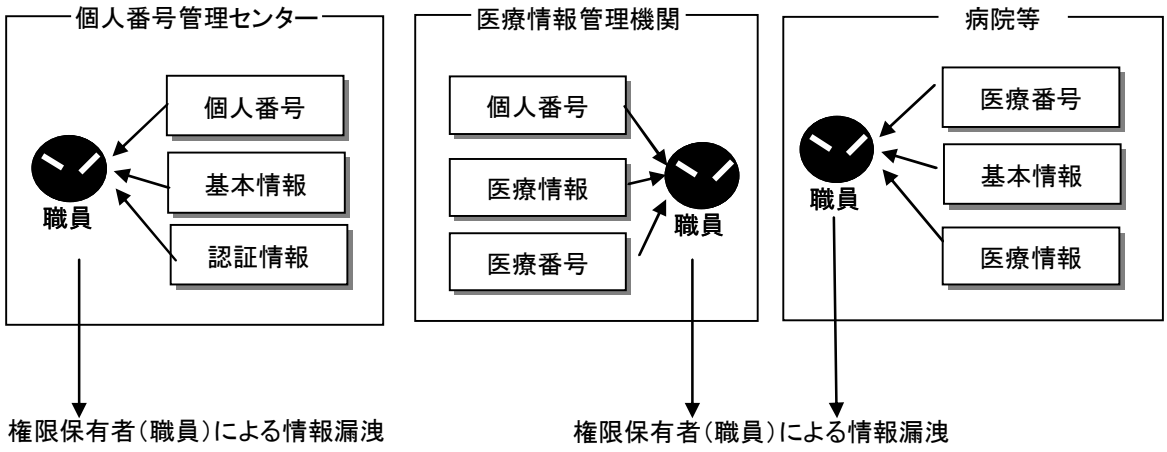


匿名化された医療データを入手し，個人を特定

例）PHR 二次利用目的で個人を特定する基本情報を匿名化したつもりが、一部のデータは、個人を特定できるものになっていて、そこから個人が特定される。あるいは同一人物に関する複数の匿名化データを集めることにより、そこから個人が特定される。

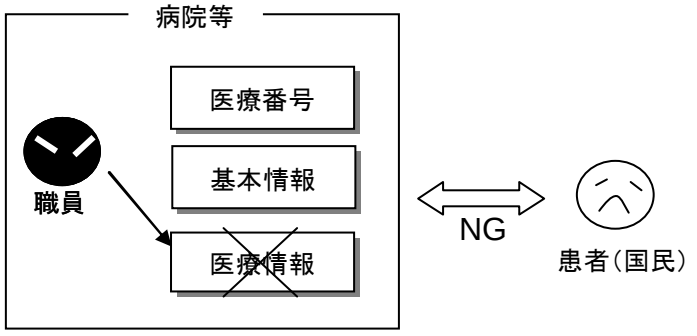
【T2】権限保有者による脅威

【T2-1】権限保有者による情報漏洩



例）医療情報管理機関等の職員が診療記録などの医療情報を不正に持ち出し漏洩する。

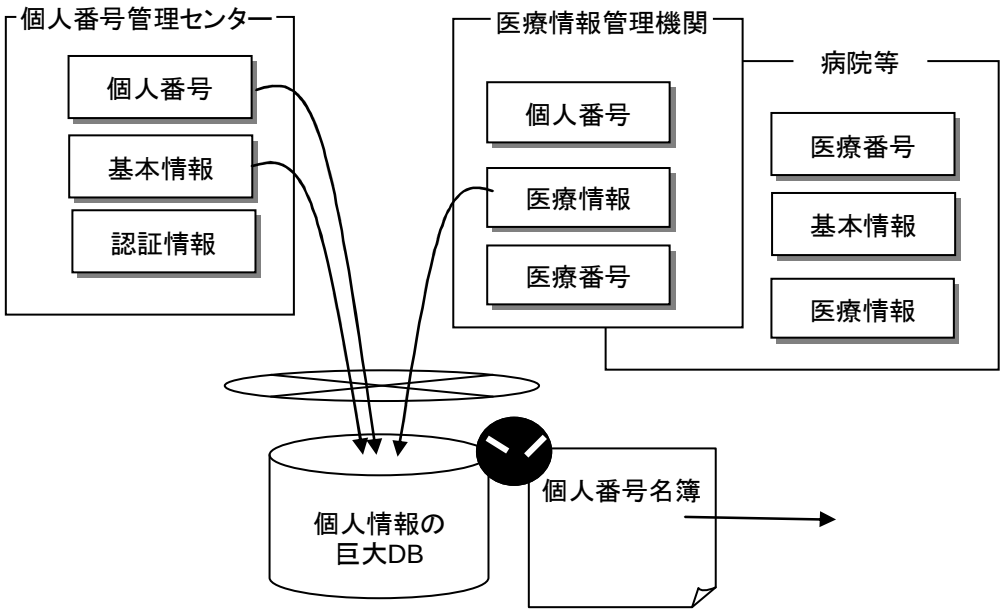
【T2-2】権限保有者による情報改ざん



医療データ情報が改ざんされ，正常な健康・医療サービスに支障

例）病院の職員が医療情報を改ざんし、正しい診断ができなくなる。

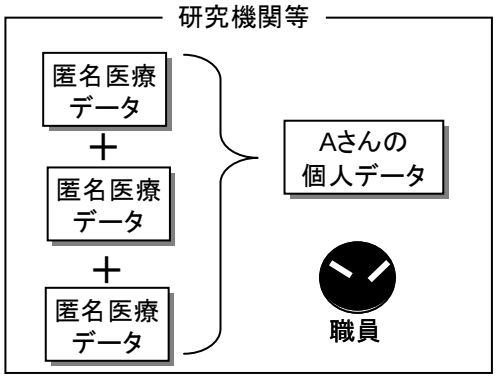
【T2-3】個人番号をキーにした名寄せ



個人番号をキーにして個人情報を収集し、巨大DBが作られる
個人番号の名簿が作られ，医療情報の売買に使われる

例）個人番号をキーにして、あらゆるところから個人情報が収集され個人情報に関する巨大 DB が作られる。また、それらの情報から名簿が作られ、個人の診療記録などの医療情報を欲しがる組織に売買される。

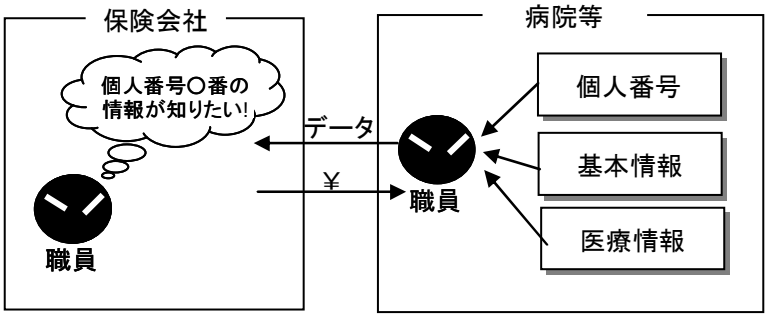
【T2-4】 匿名化データからの個人特定



匿名化された医療データを入手し，個人を特定

例）PHR 二次利用目的で個人を特定する基本情報を匿名化したつもりが、一部のデータは、個人を特定できるものになっていて、そこから個人が特定される。あるいは同一人物に関する複数の匿名化データを集めることにより、そこから個人が特定される。

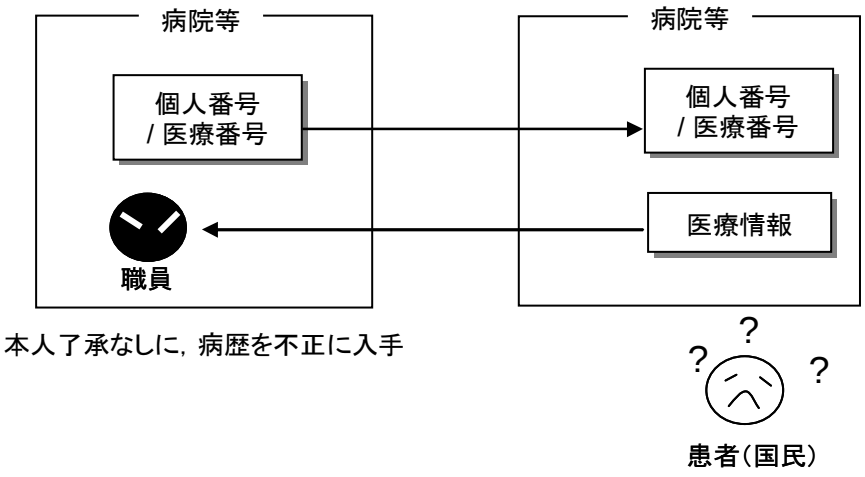
【T2-5】権限保有者による目的外利用



診療記録等を保険会社の加入審査に利用される

例）利用者が希望していないのに、保険会社加入審査などの目的で個人番号が利用される。

【T2-6】本人の許可なしでの情報流通



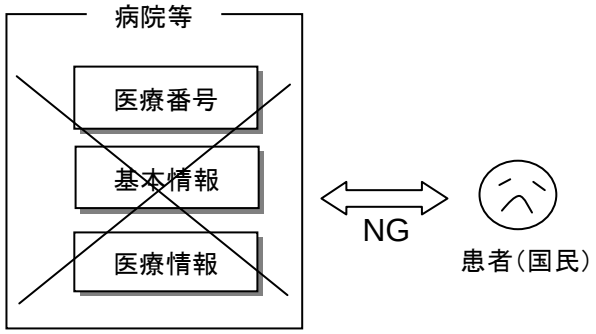
本人了承なしに，病歴を不正に入手

患者(国民)

例）本人が了承していないのにも関わらず、病院同士で勝手に情報を共有し、本人にとって知られたくない情報が流通してしまう。
ただし、緊急を要する場合、本人の承諾なしで診療記録を連携できる仕組みについても検討が必要。

【T3】その他

【T3-1】情報の劣化･消失によるサービス不履行



例）個人情報を管理しているシステムの故障や地震等の天災により個人情報が消滅し、本来受けられるサービスが受けられなくなる。

（２）製品安全ユースケースにおける脅威

製品安全ユースケースにおいて、保護対象資産（what）が適切な管理下にある時に存在しうる場所（where）を以下の表 23 に示す。

表 23　製品安全ユースケースにおける保護対象資産とその管理場所

場所（where）	保護対象資産（what）		
	個人番号	基本情報	関連情報
個人番号管理センター	○	○	○　（認証用情報、法人番号）
製品安全センター	○	○	○　（製品番号、法人番号、顧客所有物データ）
製品情報管理機関	○	○	○　（製品番号、法人番号、顧客所有物データ、モニタリングデータ）
上記の場所間のネットワーク上	○	○	○　（上記情報）

（凡例　○：存在する　―：存在しない）

これらの保護対象資産に対し、製品安全ユースケースにおいて具体的にどのような脅威があるかを分析した。表 24 は、製品安全ユースケースから導かれた脅威をまとめたものである。

表 24　製品安全ユースケースにおける脅威一覧

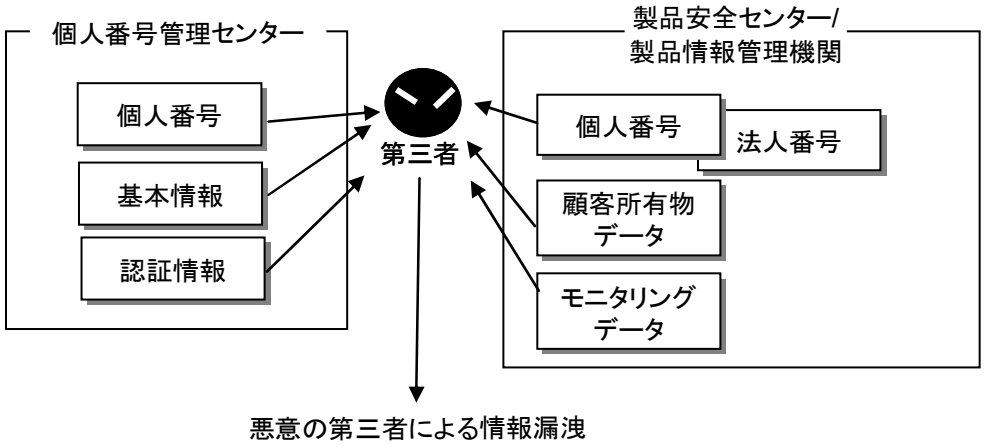
サービスシーン	脅威/課題	具体的な被害(why)	脅威主体(who)		保護対象資産(what)				攻撃手段(how)
			悪意の第三者	権限保有者	場所(where)	個人番号	基本情報	関連情報	
共通	個人番号・法人番号管理センターから、個人番号/基本情報/認証情報等が漏洩する	情報の入手により、情報の悪用、プライバシーの侵害が発生する	●		番号管理センター	●	●	●	不正アクセス、成りすまし等
共通	製品安全センターから、個人番号/基本情報/製品番号等が漏洩する		●		製品安全センター	●	●	●	不正アクセス、成りすまし等
共通	製品情報管理機関から、個人番号/基本情報/製品番号等が漏洩する		●		製品情報管理機関	●	●	●	不正アクセス、成りすまし等
共通	個人番号･法人番号管理センターと製品安全センター/製品情報管理機関の間のネットワーク上で､個人番号/基本情報/関連情報が漏洩する		●		ネットワーク上	●	●	●	不正アクセス、成りすまし等
共通	個人番号・法人番号管理センターから、個人番号/基本情報/認証情報等が漏洩する	情報の入手により、情報の悪用、プライバシーの侵害が発生する		●	番号管理センター	●	●	●	不正な情報持ち出し等
共通	製品安全センターから、個人番号/基本情報/製品番号等が漏洩する			●	製品安全センター	●	●	●	不正な情報持ち出し等
共通	製品情報管理機関から、個人番号/基本情報/製品番号等が漏洩する			●	製品情報管理機関	●	●	●	不正な情報持ち出し等

サービスシーン	脅威/課題	具体的な被害(why)	脅威主体(who)		保護対象資産(what)				攻撃手段(how)
			悪意の第三者	権限保有者	場所(where)	個人番号	基本情報	関連情報	
保守継続性	製品情報管理機関で、引き継ぎ時に、不要な個人番号/基本情報/製品番号等が漏洩する			●	製品情報管理機関	●	●	●	不正な情報処理、誤操作等
事故未然防止	製品情報管理機関から、個人番号/基本情報/モニタリング情報が漏洩する			●	製品情報管理機関	●	●	●	不正な情報持ち出し等
共通	情報漏洩された個人番号/基本情報/関連情報を収集し番号を基に名簿化する	名簿化され、情報が売買されることでより広範囲に情報が漏洩	●		管理外	●	●	●	個人番号をキーとした情報収集等
共通	製品安全センター/製品情報管理機関の関連情報を改ざんする	改ざんにより、本来受けられるはずのサービスが受けられなくなる	●		製品安全センター/製品情報管理機関			●	不正アクセス、成りすまし等
共通	製品安全センター/製品情報管理機関の関連情報を改ざんする			●	製品安全センター/製品情報管理機関			●	不正な情報処理、誤操作等
共通	製品安全センター/製品情報管理機関の関連情報を目的外利用する	購入記録を転売される		●	製品安全センター/製品情報管理機関			●	不正な情報処理等
製品リコール対応	うそのリコール情報を流され、メーカーおよび購入者が混乱に陥れられる	改ざんにより、本来受けられるはずのサービスが受けられなくなる	●		製品情報管理機関、ネットワーク上			●	成りすまし、情報改ざん等
事故未然防止	モニタリング情報が改ざんされ、保守が正しく行われない			●	製品情報管理機関、ネットワーク上			●	不正な情報処理

表 24 から分かるように製品安全ユースケースにおいて、保護対象資産およびその管理場所、脅威の主体者、サービスシーンにより、様々な脅威が存在するが、これらを脅威の種別に着目すると、以下のように分類できる。

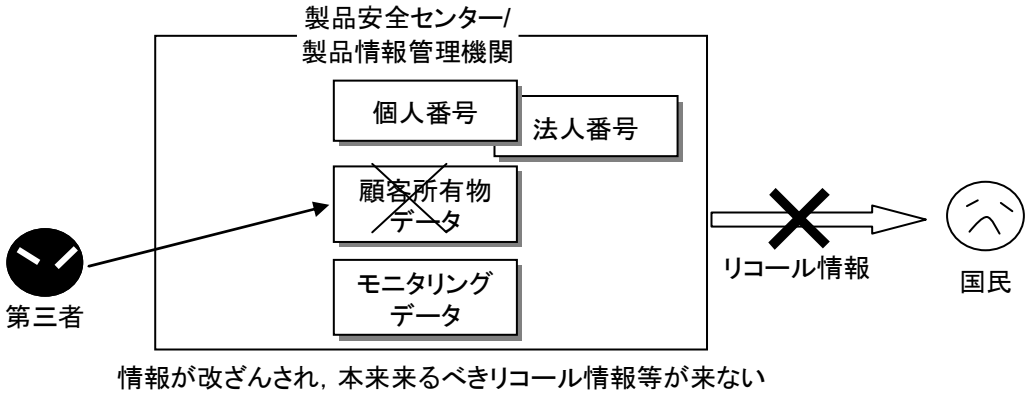
【T1】悪意の第三者による脅威

【T1-1】悪意の第三者による情報漏洩



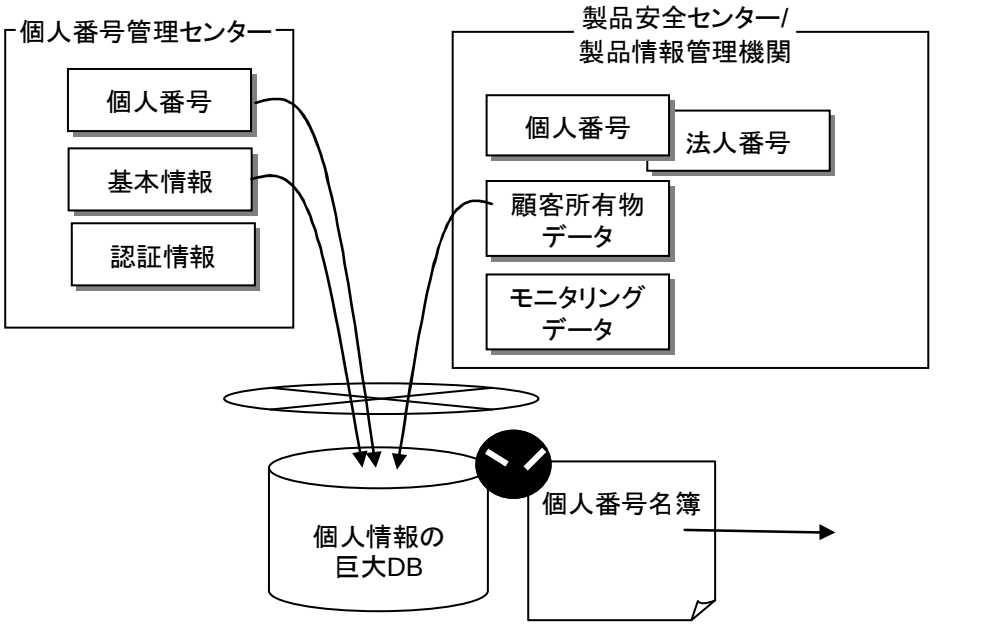
例）悪意の第三者からの不正アクセスにより製品情報管理機関等から個人の購入記録など顧客所有物データや購入製品の使用状況モニタリングデータなどが漏洩する。

【T1-2】悪意の第三者による情報改ざん



例）悪意の第三者からの不正アクセスにより製品情報管理機関等の顧客所有物データが改ざんされ、本来来るべきリコール情報等が来ない。
偽のリコール情報を流され、メーカーおよび購入者が混乱に陥れられる。

【T1-3】個人番号をキーとした名寄せ

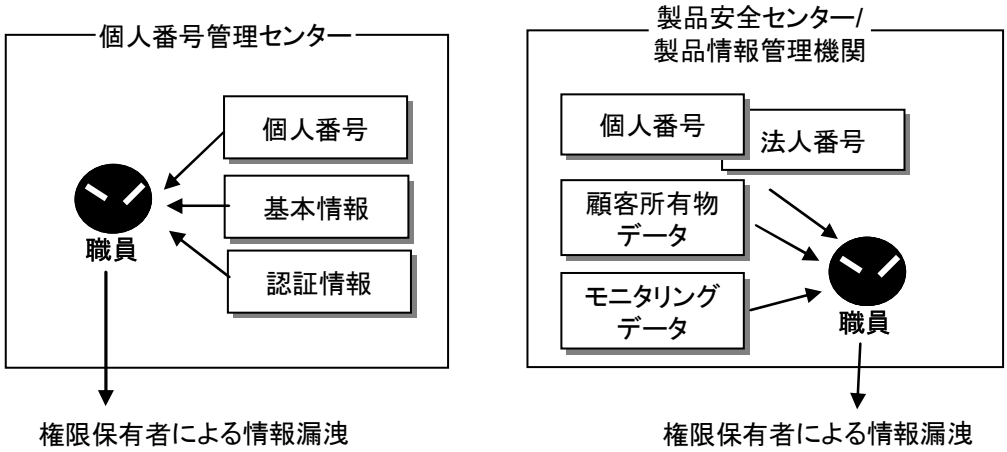


個人番号をキーにして個人情報を収集し、巨大DBが作られる
個人番号の名簿が作られ，個人の所有物に関する情報の売買に使われる

例）個人番号をキーにして、あらゆるところから個人情報が収集され個人情報に関する巨大 DB が作られる。また、それらの情報から名簿が作られ、個人の購入行動などのマーケティング情報として売買される。

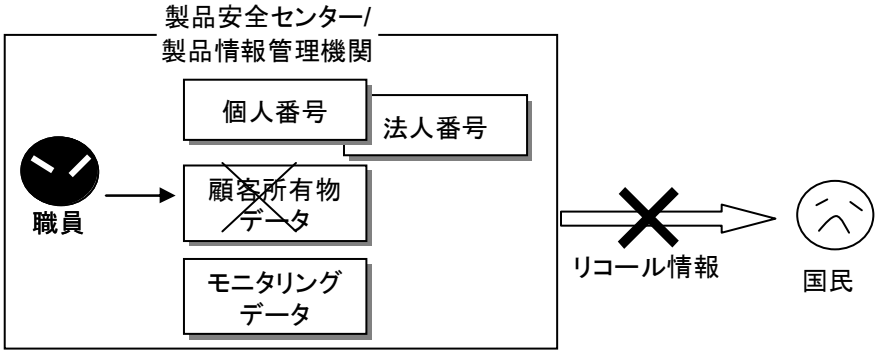
【T2】権限保有者による脅威

【T2-1】権限保有者による情報漏洩



例）製品情報管理機関等の職員が顧客所有物データを不正に持ち出し漏洩する。

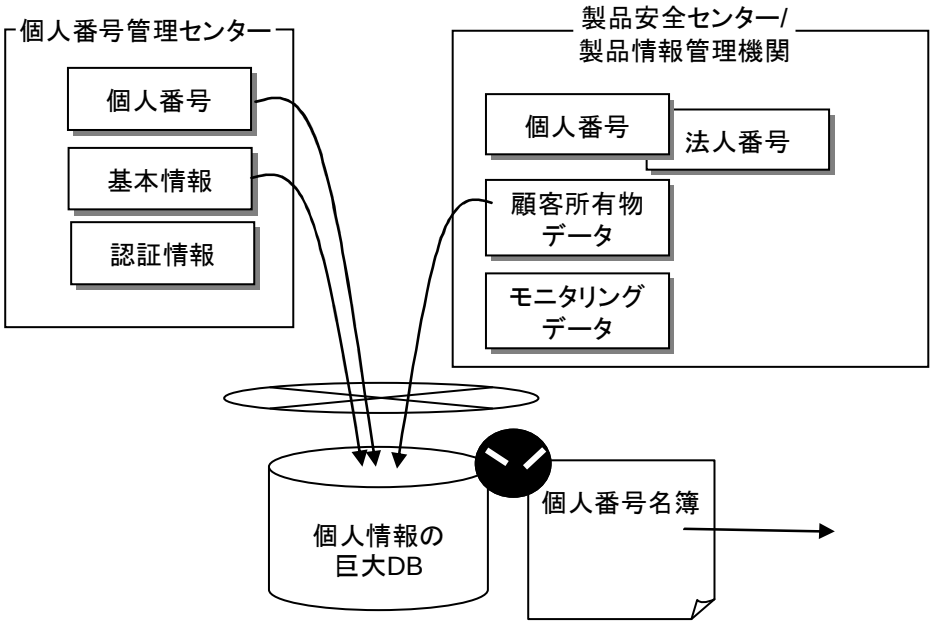
【T2-2】権限保有者による情報改ざん



情報が改ざんされ，本来来るべきリコール情報等が来ない

例）製品情報管理機関の職員が顧客所有物データを改ざんし、リコール情報が来なくなる。

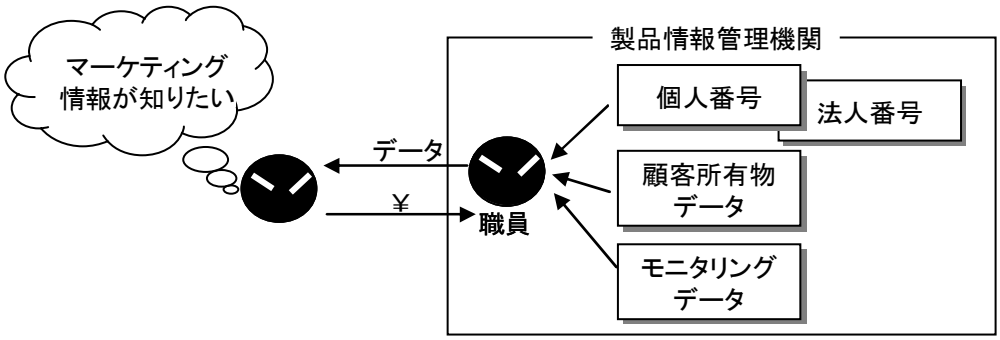
【T2-3】個人番号をキーとした名寄せ



個人番号をキーにして個人情報を収集し、巨大DBが作られる
個人番号の名簿が作られ，個人の所有物に関する情報の売買に使われる

例）個人番号をキーにして、あらゆるところから個人情報が収集され個人情報に関する巨大 DB が作られる。また、それらの情報から名簿が作られ、個人の購入行動などのマーケティング情報として売買される。

【T2-5】権限保有者による目的外利用

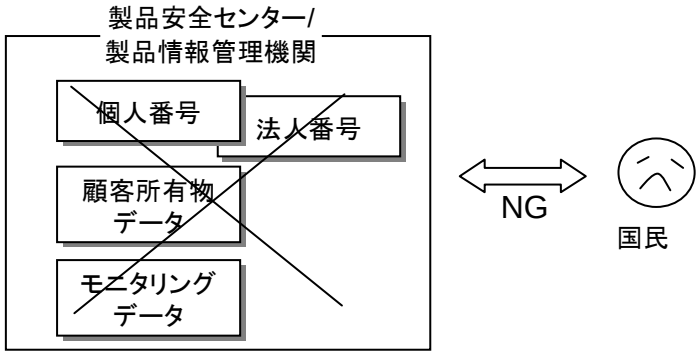


マーケティング情報として利用される

例）利用者が希望していないのに、メーカーのマーケティング情報を収集する目的で個人番号が利用される。

【T3】その他

【T3-1】情報の劣化･消失によるサービス不履行



例）個人情報を管理しているシステムの故障や地震等の天災により個人情報が消滅し、本来受けられるサービスが受けられなくなる。

（３）金融ユースケースにおける脅威

金融ユースケースにおいて、保護対象資産（what）が適切な管理下にある時に存在しうる場所（where）を以下の表 25 に示す。

表 25　金融ユースケースにおける保護対象資産とその管理場所

場所（where）	保護対象資産（what）		
	個人番号	基本情報	関連情報
個人番号管理センター	○	○	○　（認証用情報）
金融機関	○	○	○　（口座番号、資産情報、各種証明書）
行政機関	○	○	○　（各種証明書）
上記の場所間のネットワーク上	○	○	○　（上記情報）

（凡例　○：存在する　―：存在しない）

これらの保護対象資産に対し、金融ユースケースにおいて具体的にどのような脅威があるかを分析した。表 26 は、金融ユースケースから導かれた脅威をまとめたものである。

表 26　金融ユースケースにおける脅威一覧

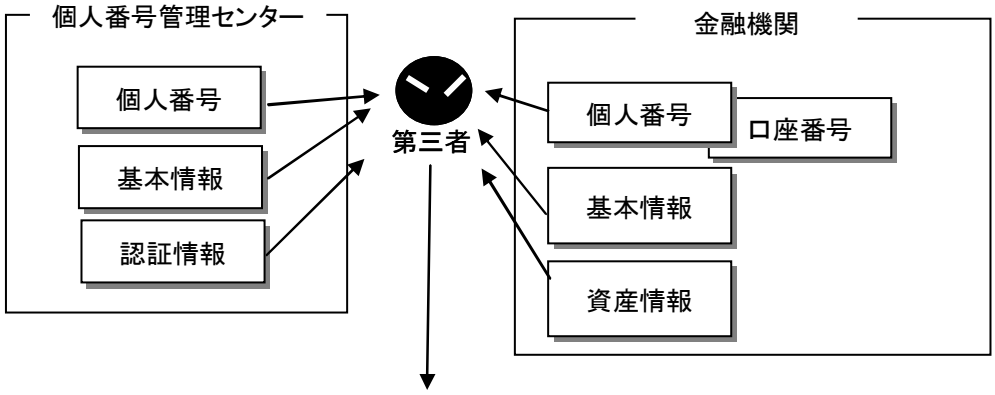
サービスシーン	脅威/課題	具体的な被害(why)	脅威主体(who)		保護対象資産(what)				攻撃手段(how)
			悪意の第三者	権限保有者	場所(where)	個人番号	基本情報	関連情報	
共通	番号管理センターから、個人番号/基本情報/認証情報等が漏洩する	情報の入手により、情報の悪用、プライバシーの侵害が発生する	●		番号管理センター	●	●	●	不正アクセス、成りすまし等
共通	金融機関から、個人番号/基本情報/資産情報等が漏洩する		●		金融機関	●	●	●	不正アクセス、成りすまし等
共通	行政機関から、個人番号/基本情報/関連情報が漏洩する		●		行政機関	●	●	●	不正アクセス、成りすまし等
本人確認業務	IC 付きカードの盗難＋パスワードの盗難/偽造による、本人成りすまし行為		●		金融機関	●	●	●	不正アクセス、成りすまし等
各種証明書手続き業務	行政機関と金融機関の間のネットワーク上で、個人番号/基本情報/資産情報等が漏洩する		●		ネットワーク上	●	●	●	ネットワーク盗聴等
共通	番号管理センターから、個人番号/基本情報/認証情報等が漏洩する			●	番号管理センター	●	●	●	不正な情報持ち出し等
共通	金融機関から、個人番号/基本情報/資産情報等が漏洩する			●	金融機関	●	●	●	不正な情報持ち出し等
共通	行政機関から、個人番号/基本情報/資産情報等が漏洩する			●	行政機関	●	●	●	不正な情報持ち出し等
共通	情報漏洩された個人番号/基本情報/関連情報を収集し番号を基に名簿化する	名簿化され、情報が売買されることでより広範囲に情報が漏洩	●		管理外	●	●	●	個人番号をキーとした情報収集等

サービスシーン	脅威/課題	具体的な被害(why)	脅威主体(who)		保護対象資産(what)				攻撃手段(how)
			悪意の第三者	権限保有者	場所(where)	個人番号	基本情報	関連情報	
共通	金融機関の資産情報等を改ざんする	改ざんにより、金銭的な被害を受ける	●		金融機関			●	不正アクセス、成りすまし等
共通	金融機関の資産情報等を改ざんする			●	金融機関			●	不正な情報処理誤操作等
共通	金融機関の資産情報を目的外利用する	資産情報が転売される		●	金融機関			●	不正な情報処理等
各種証明書手続き業務	本人了承なしに金融機関/行政機関の間で個人番号/基本情報/資産情報/資産情報等が流通する	本人了承なしに知られたくない情報が流通してしまう		●	金融機関 行政機関	●	●	●	不正な情報処理等
現況確認業務	第三者が現況確認情報を不正に取得する	知られたくない情報が知られてしまう	●		番号管理センター	●	●		不正アクセス、成りすまし等
現況確認業務	承諾を受けていない金融機関による現況確認の実施	知られたくない情報が知られてしまう		●	番号管理センター	●	●		不正な情報処理等

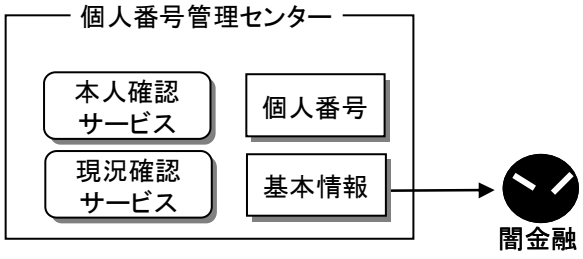
表 26 から分かるように金融ユースケースにおいて、保護対象資産およびその管理場所、脅威の主体者、サービスシーンにより、様々な脅威が存在するが、これらを脅威の種別に着目すると、以下のように分類できる。

【T1】悪意の第三者による脅威

【T1-1】悪意の第三者による情報漏洩

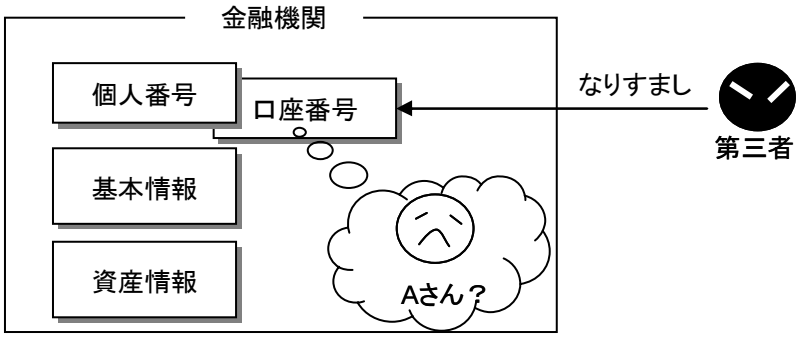


例）悪意の第三者からの不正アクセスにより、金融機関から個人の資産情報が漏洩する。



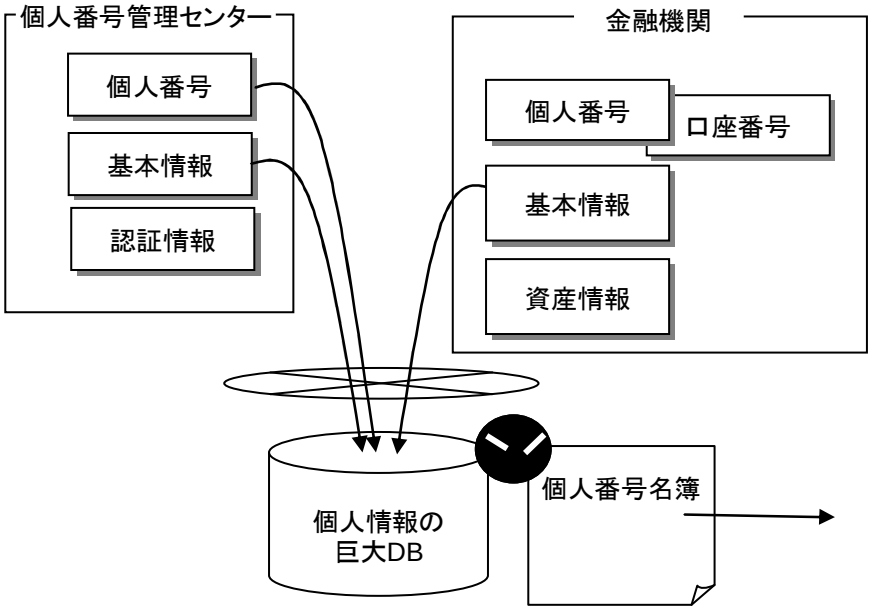
例）金融機関が現況確認等に用いるための本人確認・現況確認サービスを使って、闇金業者に住所情報を取得され、強引な取立てをされる。

【T1-2】悪意の第三者による情報改ざん



例）悪意の第三者が個人番号を騙り他人に成りすますことにより、資産が奪われる。
悪意の第三者が個人番号を騙り他人に成りすますことにより、勝手に口座が開設され、犯罪等に利用される。

【T1-3】個人番号をキーとした名寄せ

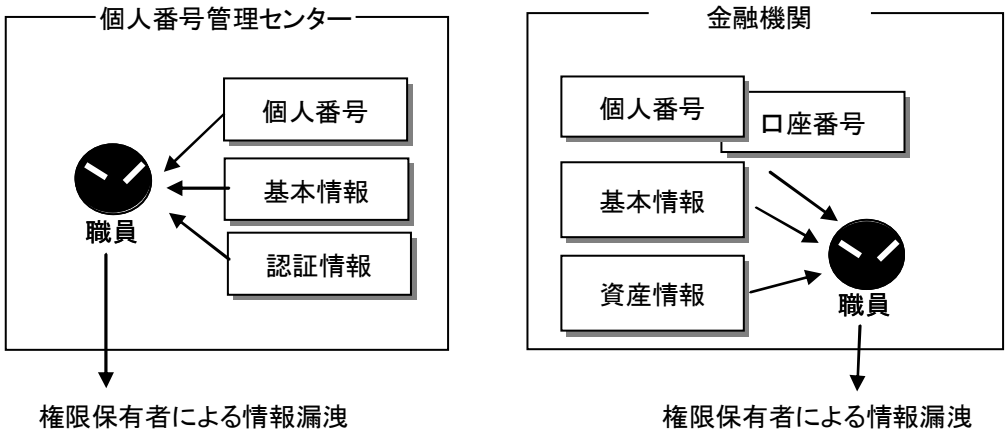


個人番号をキーにして個人情報を収集し、巨大DBが作られる
個人番号の名簿が作られ，個人の資産に関する情報が売買される

例）個人番号をキーにして、あらゆるところから個人情報が収集され個人情報に関する巨大 DB が作られる。また、それらの情報から名簿が作られ、個人の資産情報が売買される

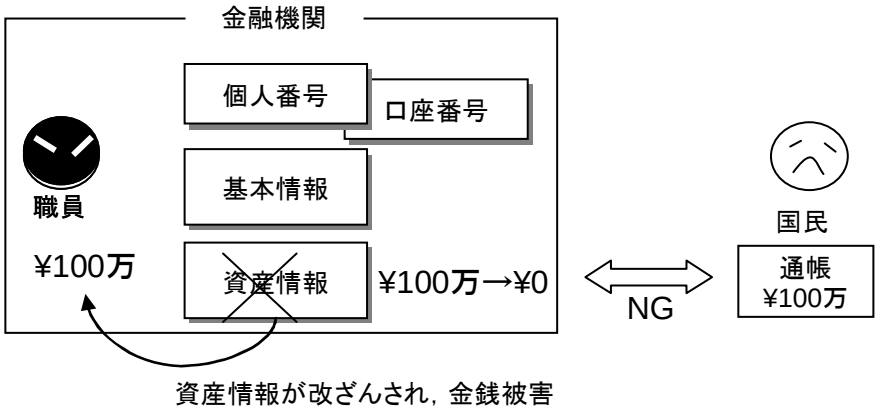
【T2】権限保有者による脅威

【T2-1】権限保有者による情報漏洩



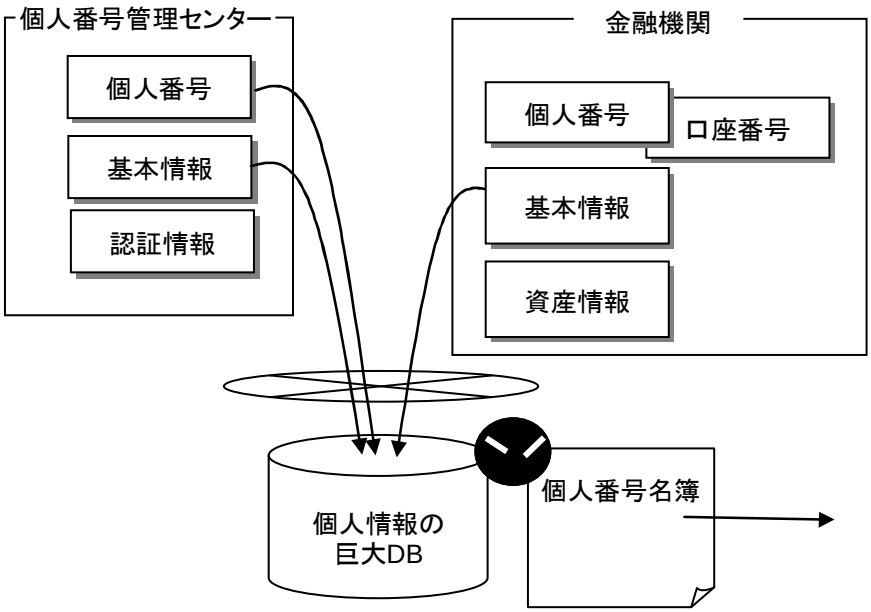
例）金融機関の職員が資産情報を不正に持ち出し漏洩する。

【T2-2】権限保有者による情報改ざん



例）金融機関の職員による資産情報改ざんにより、金銭被害を受ける。

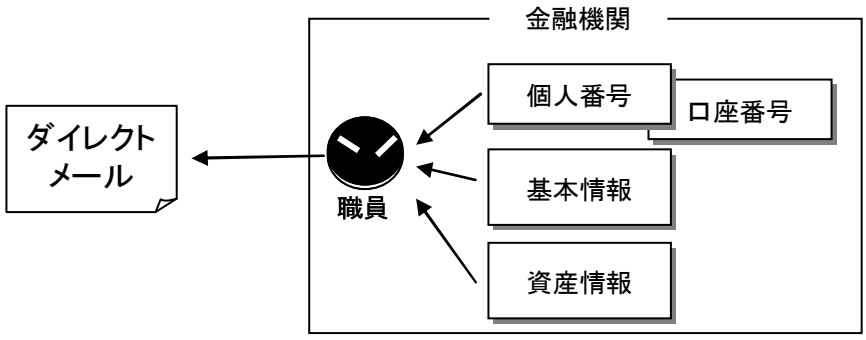
【T2-3】個人番号をキーとした名寄せ



個人番号をキーにして個人情報を収集し、巨大DBが作られる
個人番号の名簿が作られ，個人の資産に関する情報が売買される

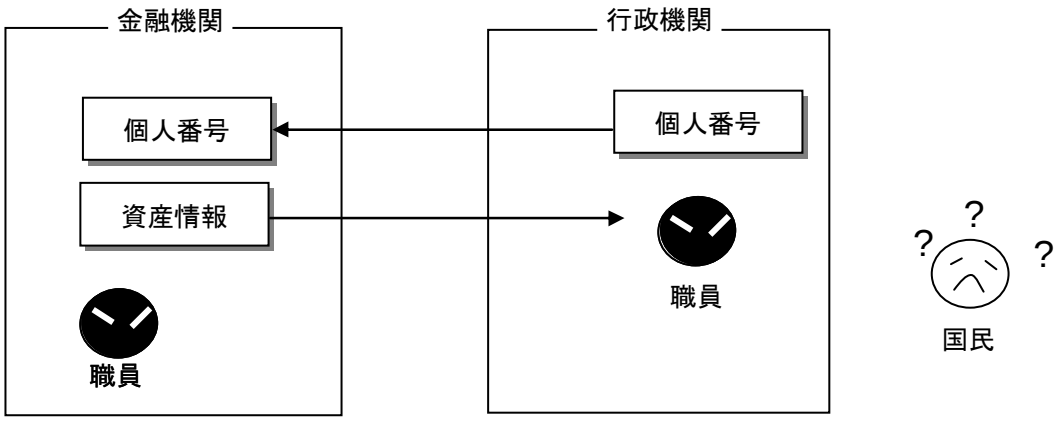
例）個人番号をキーにして、あらゆるところから個人情報が収集され個人情報に関する巨大 DB が作られる。また、それらの情報から名簿が作られ、個人の資産情報が売買される

【T2-5】権限保有者による目的外利用



例）利用者が希望していないのに、個人番号が新たな金融商品を通知するダイレクトメール等に利用される

【T2-6】本人の許可なしでの情報流通に関する脅威

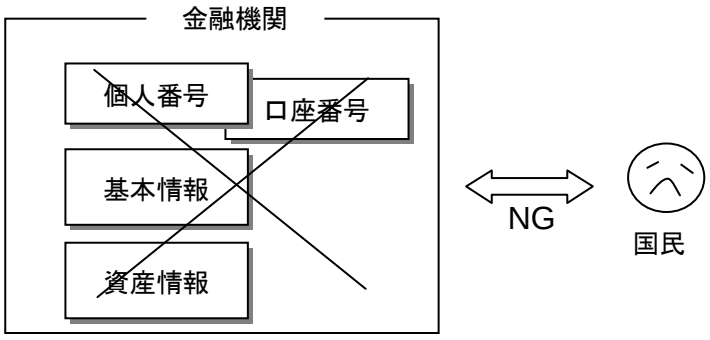


資産情報等が本人了承なしに流通してしまう

例）本人が了承していないのにも関わらず、金融機関と行政機関とで勝手に情報を共有し、本人にとって知られたくない情報が流通してしまう。
控除申告や社会保障の手当てのため、一度は行政機関に資産情報を提供することを承諾したが、それ以降も行政機関に資産情報が共有されてしまい本人にとって知られたくない情報が流通してしまう。

【T3】その他

【T3-1】情報の劣化･消失によるサービス不履行



例）個人情報を管理しているシステムの故障や地震等の天災により個人情報が消滅し、本来受けられるサービスが受けられなくなる。

１１．参考資料：世界の状況

１１－１．各国の住民データベースに関して

１１－１－１．韓国の住民データベースと電子政府の仕組み[36][37]

[3]に示した電子政府の世界ランキングにおいて 1 位とされた韓国では、5,300 種類の行政サービスの詳細をインターネットで調べることができ、そのうち 720 種類のサービスを電子申請により行うことができる。また、28 種類の証明書を自宅で発行することが可能となっている。

電子申請、インターネットバンキング、インターネットショッピングなど、民間も含めたあらゆるインターネットサービスで住民登録番号が使用されている。しかし、住民登録番号が盗まれた場合に、成りすましの危険性の高いことが問題になっている。その対策として、i-PIN と呼ばれる番号を取得し、住民登録番号の代わりに使用する制度が設けられている。利用者は民間登録機関から i-PIN を取得し、自分で番号を変更して使用することが可能である。

１１－１－２．オーストリア、エストニア、ドイツの住民データベースと電子政府の仕組み[38][39]

（１）オーストリア

オーストリアでは三層構造の識別番号を運用することで、個人情報の保護と効率的な行政事務を両立している。インターネット上での署名・認証用のカードとして「市民カード」というものが用いられている。ただし、これは住基カードのような専用カードではなく、健康保険カード、銀行カード、学生証などの IC カードや電子 ID カード、携帯電話等が用いられる。市民カードを利用した住民向けサービス事例を表 27 に示す。

表 27　オーストリアの市民カードを利用した住民向けサービス

サービス名称	概要
Finanz Online	・インターネット上の確定申告・納税システムであり、電子申告や納税額の確認等を行うことができる。
住民登録確認	・自分の住民登録データをオンラインで確認できる。
犯罪記録確認	・就職時などに必要な、自分に関する無犯罪証明書をオンラインで発行申請し、手数料も支払うことができる。
help.gv.at	・電子政府ポータルサイトであり、様々な行政手続きを行うことができる。
電子配達サービス	・公文書を電子的に受け取ることができる。
社会保険システムでの利用	・自分の社会保険記録の詳細をオンラインで確認できる。 ・年金の受給申請をオンラインでできる。 ・自分の医療記録を閲覧できる（将来）。 ・自分の医療記録に誰がアクセスしたか確認できる。また自分の医療記録にアクセスできる医療従事者を制限できる（将来）。

（２）エストニア

エストニアでは、15 歳以上の国民に対して IC チップ付きの電子身分証明書（国民 ID カード）が発行される。

この国民 ID カードが、生活に根ざした種々の公共サービスや電子行政サービスを利用するためのツールとなっている。具体的な利用方法は表 28 に示すように、①物理的な身分証明書としての利用、②電子マネーとしての利用、③オンラインでの身分証明書としての利用（電子署名、認証機能）に分類される。

表 28　エストニアの国民 ID カードの利用方法

①物理的な身分証明書としての利用
■運転免許証の代替
■健康保険証の代替
■EU 域内でパスポートの代替
②電子マネーとしての利用
■公共交通機関の乗車券
■駐車料金支払い
③オンラインでの身分証明書としての利用（電子署名、認証機能）
■電子申請
■インターネット投票
■インターネットバンキング
■市民ポータルへのログイン　等

（３）ドイツ（2010 年 10 月時点の調査内容）

ドイツでは ID 番号は、前述のエストニアと異なり、行政分野毎に異なる個人識別番号を付番しており、分野毎の識別番号の間には何らの関連性もない（1976 年に一度提案されたが、連邦憲法裁判所が分野横断的な個人識別番号は違憲との見解を示したため）。ドイツでは 2010 年 11 月に電子 ID カードの発行が予定されている。これは現行の紙の身分証明書に切り替わるものである。電子 ID カードを用いて、下記のようなサービスが予定されている。

電子 ID カード利用による住民向けサービス例（予定）

- 自動車登録（新規、移転）：新たなナンバーをインターネットで登録して受け取れる
- 無犯罪証明書：就職時などに必要だが、インターネットで調べて書類を取り寄せられる
- 住民登録：引越し時など、直接自宅から手続きできる
- オンラインバンキング：電子 ID カードの本人認証で口座開設などができる
- 年齢認証：タバコの自動販売機や、年齢制限があるオンライン販売で年齢認証できる
- 市民ポータル：電子 ID カードを使って社会保障情報や納税情報にアクセスできる

電子 ID カードの利用にあたっては、カードのみで OK、カード＋PIN 入力など、セキュリティレベルによっていくつかの認証方法を使い分けることが可能となっている。

以上、諸外国の ID 方式と公的認証サービスを俯瞰してきた。

海外諸国では、公的認証サービスを使って、各種の行政手続き（電子申請、電子申告等）を行えることは当然として、住民登録データベースや、納税、社会保障、教育など各分野のデータベースに記録された自分の情報を閲覧したり、一定の項目については自ら更新したりすることができる。また、公共性の高い分野など、民間企業のサイトでも公的認証サービスを利用することが可能である[39]。

１１－２．諸外国での電子医療の状況

１１－２－１．オランダの電子医療の状況[40]

オランダでは、電子投薬記録（EMD）と電子代診記録（WDH）をまずは実現している。EMD では、各病院などに存在する患者の投薬記録に対して、薬局、病院、医者などがアクセスすることが可能となっている。WDH では、主治医を代行する医師が、主治医の電子カルテにアクセスすることを可能とするものである。

１１－２－２．米国のセンチネルイニシアティブ[41]

米国では医薬品の安全モニタリングのために、複数の情報源から得られた医療データのリンク・解析を可能とするために、患者のプライバシーを確保しながら異なる情報源へのアクセスの確保、そして市販後のリスクを同定し、解析するためのシステムを構築することとした。2012 年までに 1 億人規模のデータ利用を可能とすることを目的としている。

１１－２－３．オーストリアの電子医療の状況[38]

オーストリアの「電子医療記録システム（ELGA）」は全国的な電子医療記録ネットワークシステムである。電子化によって、連邦、州、および独立の社会保険機関の医療制度を統合し、患者と医者との間の情報伝達を円滑化することを目的としている。ELGA 上では、患者データは様々な病院医療従事者、開業医、あるいは患者自身によって、入力が可能である。患者データの内医療記録は末端の個別の情報システムに保存される。データ利用の権限を与えられた者はデータ保護の観点から一定の安全性を確保していれば、患者データを参照できる。

ELGA では、公共医療や保険制度向けに患者の匿名化された医療記録を生成することが可能である。

１１－２－４．ドイツの電子医療の状況[38][39]

ドイツでは 2006 年より電子健康保険カード（eGK）が導入された。PIN による本人のコントロール、PC 等でカード内のデータを閲覧できる。また、医師や薬剤師向けには処方箋などに電子署名する機能を備えた「医療専門家カード（HBA）」が導入された。電子保険健康カードプロジェ

クトの主たる目的は、医療分野における様々な手続きに電子的なサポートを与えることである。全体のシステム像を下記に示す[39]。

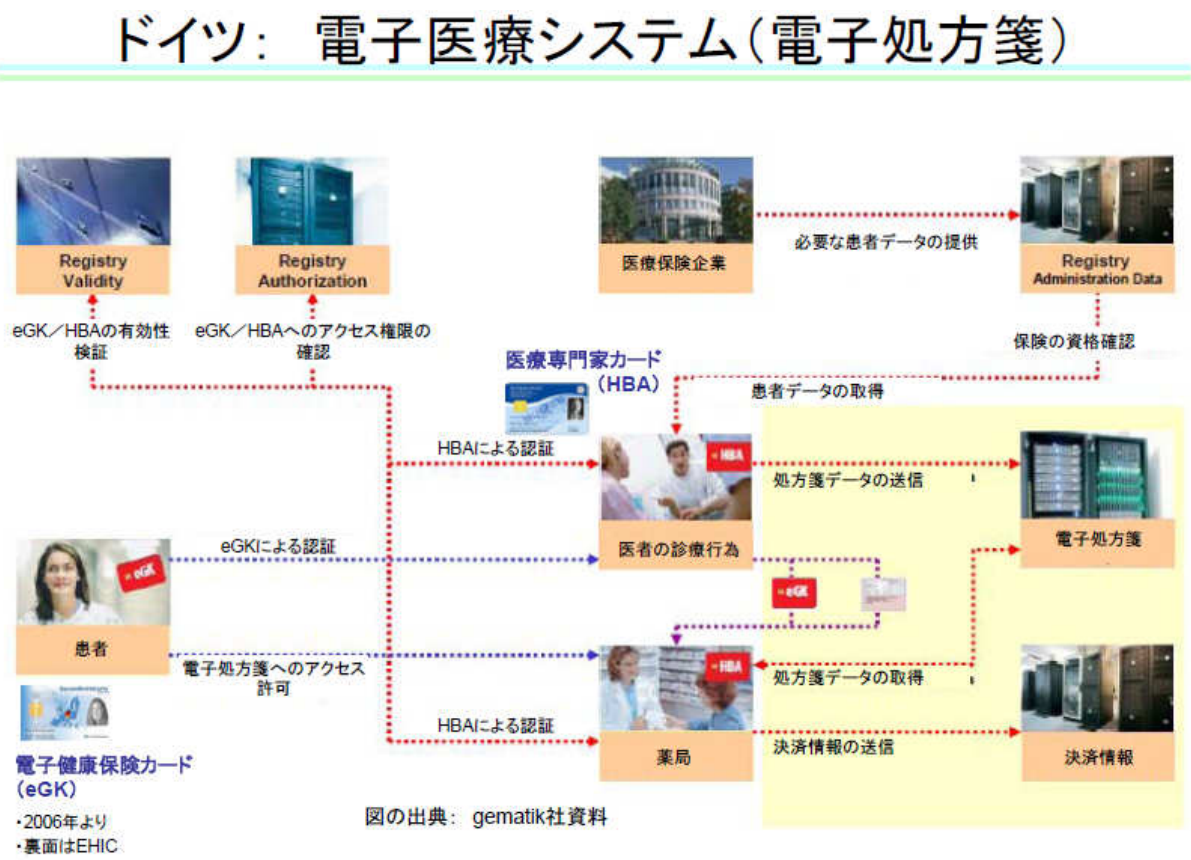


図 34　ドイツでの電子医療システム像

１１－２－５．デンマークの電子医療の状況[42]

デンマークの医療関連サービスは、費用の 85%が税金でまかなわれる公的サービスの 1 つであり、予防医療、治療、遠隔地医療まで含めた様々な医療サービスの IT 化を、電子政府計画の一環として進めている。

デンマークの中心的な医療情報システムは、患者の電子カルテシステムである EPJ（Electronic Patient Journal：Elektroniske patientjournaler）である。EPJ は 1990 年代から、各医療サービス単位である県単位で構築されてきた。2002 年には標準化規格である電子カルテ基本構造（G-EPJ）の開発と EPJ が医療情報化の中心課題として位置付けられ、現在に至っている。また、デンマークでは、国民すべてが保有する 10 桁の CPR と呼ばれる個人 ID 番号をもとに全国患者インデックス（the National Patient Index）が作られる。この全国患者インデックスが、個人情報のインデックスの役割を果たしている。

医療情報システムの中心である EPJ に加え、その他にも複数のデータベースが構築されている。例えば、各地で開発や試験利用が始まったデータベースには、患者の薬剤情報の一括管理システム、予約管理システムといった、各種医療情報のデータベースがある。

また、全国の医療機関の開院時間、担当医、医院のホームページのリンクなどが記載されたクリニカルデータベースや、疾患の徴候、治療方法が記載された疾患データベースといった全国をカバーするデータベース構築も進行中である。

１２．参考文献

[1] 総務省　2009 年 8 月「日本の ICT インフラに関する国際比較評価レポート」
http://www.soumu.go.jp/main_content/000034706.pdf

[2] World Economic Forum　“The Global Information Technology Report 2009-2010”、
http://www.weforum.org/en/initiatives/gcp/Global%20Information%20Technology%20Report/index.htm

[3] United Nations “United Nations E-Government Survey 2010”
http://unpan1.un.org/intradoc/groups/public/documents/un/unpan038851.pdf

[4] World Health Organization: “Global Survey for E-health”
http://www.who.int/goe/data/en/

[5] 首相官邸 :「新たな情報通信技術戦略」
http://www.kantei.go.jp/jp/singi/it2/100511honbun.pdf

[6] http://www.kantei.go.jp/jp/it/network/dai1/1siryou05_2.html

[7] http://www.mhlw.go.jp/shingi/0112/s1226-1c.html

[8] http://www.soumu.go.jp/main_content/000031924.pdf

[9] http://www.keidanren.or.jp/japanese/policy/2008/082/index.html

[10]http://www.kantei.go.jp/jp/singi/it2/nextg/meeting/dai5/siryou6.pdf

[11]http://www.soumu.go.jp/main_sosiki/joho_tsusin/top/tiiki_kosin.pdf

[12]http://www.work-master.net/news_jDpSFni9d.html

[13]http://www.keidanren.or.jp/japanese/policy/2010/080.html

[14]http://www.ehr.or.jp/activity/index.html

[15]http://www.jahis.jp/tiikirenkei_pj/tiikirenkei_top.html

[16]https://microsite.accenture.com/meti/Pages/default.aspx

[17]http://www.mhlw.go.jp/stf/shingi/2r9852000000mlub.html

[18]「活力ある高齢社会に向けた研究会中間提言」（東京大学･COCN 共同研究・2010 年 2 月）
http://pari.u-tokyo.ac.jp/policy/policy4_cocn_100215.pdf

[19]「バイオ成長戦略」提言書（日本バイオ産業人会議・2010 年 8 月）
http://www.jba.or.jp/jabex/pdf/20100826teigen.pdf

[20]「新たな情報通信技術戦略」（IT 戦略本部・2010 年 5 月）医療分野施策
http://www.kantei.go.jp/jp/singi/it2/100511honbun.pdf

[21]家電電子タグコンソーシアム、家電業界における電子タグ運用標準化ガイドライン（2.0 版）～電子タグを活用した製品ライフサイクル管理の実現に向けて～、2008 年 10 月

[22]電気・電子情報連携推進協議会（IPPC）平成 21 年度（2009 年度）活動報告書

[23]内平ほか、「信用情報共有基盤における財務情報開示・流通・利用支援機能に関する考察」、経営情報学会 2004 年度秋季全国研究発表大会、2004

[24]文書の電磁的保存等に関する検討委員会報告書
http://www.meti.go.jp/policy/it_policy/e-doc/kentouiinkai_houkokusyo.pdf

[25]「医療情報システムの安全管理に関するガイドライン 第 4.1 版」 に関する Q&A

http://www.mhlw.go.jp/shingi/2010/02/dl/s0201-3a.pdf
[26]医療情報システムの安全管理に関するガイドライン　第 4.1 版（平成 22 年 2 月）
http://www.mhlw.go.jp/shingi/2010/02/dl/s0202-4a.pdf
[27]保健医療福祉分野 PKI 認証局認証用（組織）証明書ポリシ（平成 21 年 11 月）
http://www.mhlw.go.jp/shingi/2009/11/dl/s1106-7c.pdf
[28]保健医療福祉分野 PKI 認証局認証用（人）証明書ポリシ（平成 21 年 11 月）
http://www.mhlw.go.jp/shingi/2009/11/dl/s1106-6c.pdf
[29]厚生労働省において保健医療情報分野の標準規格として認めるべき規格について（平成 22 年 2 月）
http://www.mhlw.go.jp/shingi/2010/01/dl/s0125-12a.pdf
[30]平成 22 年度版死亡診断書（死体検案書）記入マニュアル
http://www.mhlw.go.jp/toukei/manual/index.html
[31]高度情報通信ネットワーク社会推進戦略本部（第 54 回）
http://www.kantei.go.jp/jp/singi/it2/dai54/gijisidai.html
[32]身崎成紀　製品の安全性確保に向けたリコール法制度、情報開示・報告制度のあり方に関する調査研究　社会技術研究論文集　Vol.2、313-320、Oct. 2004.
[33]社会保障・税に関わる番号制度、内閣官房、
http://www.cas.go.jp/jp/seisaku/bangoseido/index.html
[34]共通番号制度の早期実現に向けて～国民本位の社会基盤づくり～、国際公共政策研究センター共通番号制度に関する研究会、2010 年 7 月 1 日
http://www.cipps.org/img/news/100701/ID%20number%20proposals.pdf
[35]PCI-DSS、 https://www.pcisecuritystandards.org/
[36]首相官邸： 韓国電子政府について
http://www.kantei.go.jp/jp/singi/it2/nextg/pdf/siryou_21.pdf
[37]e-Government of Korea http://www.korea.go.kr/html/files/publications/eGov_2009.pdf
[38]株式会社国際社会経済研究所：海外住民データベースの状況と、地方情報化の進展
http://www.candc.or.jp/cyosa_kenkyu/pdf/2007/2007report_01.pdf
[39]株式会社国際社会経済研究所（発表当時は NEC 総研） 海外事例住民データベースを活用した電子政府のあり方オーストリア・エストニア・ドイツ
http://www.candc.or.jp/cyosa_kenkyu/pdf/2007/080306_soken.pdf
[40]http://www.ehealth-era.org/database/documents/factsheets/Netherlands.pdf
[41]“The Sentinel Initiative National Strategy for Monitoring Medical Product Safety”
http://www.fda.gov/downloads/Safety/FDAsSentinelInitiative/UCM124701.pdf
[42]「デンマークの医療の効率化と IT」（JETRO ユーロトレンド 2006.9）
http://www.jetro.go.jp/world/europe/eurotrend/pdf/0609R3.pdf

１３．付録 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 意見提出

国家戦略室を中心とする社会保障・税に関わる番号制度に関する検討会（会長：菅首相）が 2010 年 2 月に発足し、6 月に中間報告を発表した。COCN では、この中間報告に対して、同年 8 月にパブリックコメントとして意見書を提出している。提出した意見書を次ページ以降に掲載する。

（別 添）

「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」
意見提出

氏名・団体名
産業競争力懇談会（ＣＯＣＮ）
会長 勝俣恒久
（東京電力株式会社　取締役会長）
住所
東京都千代田区丸の内一丁目６番６号
日本生命丸の内ビル（株式会社日立製作所内）
電話番号　　０３－４５６４－２３８２

１．選択肢Ⅰ　「利用範囲をどうするか」

※①～④のうち最も望ましいと考える選択肢番号を**１つのみ**選択し、
記載してください。 → ④＋α

① Ａ案　（ドイツ型：税務分野のみで利用）
② Ｂ－１案（アメリカ型：税務分野、社会保障は現金給付分野のみに利用）
③ Ｂ－２案（アメリカ型：税務分野、社会保障は現金給付分野に加え、社会保障情報サービスにも利用）
④ Ｃ案　（スウェーデン型：幅広い行政分野で利用）

【選択理由】

(1) 税務、社会保障に限らず、幅広い行政分野で利用できること、さらに本人の了解を前提にして、民間企業を含めて、幅広く産業利用ができるようにすべきです。そのことによって、国民にとってのメリット(利便性)は大きく向上し、情報管理のリスク・コストも社会全体として大きく減少させることが可能になると考えています。

(2) 「電子政府評価委員会 平成 20 年度報告書」等でも述べられているとおり、オンライン利用を促進するためには利用者目線での業務サービス改革が必須であり、その実現に向けては、国、地方自治体のみならず、民間企業も含めたシステム連携が必要です。そのため、本番号の利用範囲に対する制限はできるだけ少ないものが望ましいと考えます.

(3) 利便性の具体的な例として、例えば住所変更があった場合を考えてみますと、民間のサービスと公的な番号制度との連携が取れているとした場合、住所変更に関連した行政手続きと民間のサービス(銀行やクレジット会社等)の手続きとを一括して行うことが可能になります。

(4) また、企業が自社製品・サービスの契約ユーザーの現況を確認するために、公的な共通番号による情報提供が可能となれば、消費者の権利保護が促進されます。たとえば、本人が契約段階で了解している場合、保険会社、金融機関が直接本人の最新住所の確認ができるようになりますし、製造業での製品リコール対応も迅速化できます。

(5) 社会のリスクを軽減する例として、オンラインでの電子商取引の本人確認手段として、セキュリティの高い公的な共通番号による認証手段を使うことにより、今までパスワード認証などセキュリティが低いため起きていた、なりすましや、不正なサービスの利用などを防止することができると考えられます。さらに、プライバシー保護が重要課題である電子カルテ等の個人の医療情報を、本人が収集する際の本人確認手段としての利用も考えることができます。

(6) また、行政だけでなく民間利用も想定した場合、利用者の不安を払拭するために、アクセスログの管理を含めてシステムが正しく運用されていることを監視する第三者機関の設置が必要だと考えます。

２．選択肢Ⅱ　「制度設計をどうするか」

【番号に何を使うか】

※①～③のうち最も望ましいと考える選択肢番号を**１つのみ**選択し、
記載してください。 → ③

① 基礎年金番号
② 住民票コード
③ 新たな番号

【選択理由】
共通番号は、住基ネットを活用し、「新たな番号」を付番することが良いと思います。さらに、共通番号は、目に見える番号であること、国民全員に一人一番号を付与することが必要だと考えます。「新たな番号」は、既に実績のある住基ネットを活用して付番することとし、既存の住民票コードとの対応関係を維持することにより生成されることが必要だと考えます。そうすることで、最小の費用で、確実かつ効率的な仕組みが構築できます。住民票コードと同等の「新たな番号」を新規に作り出すことは、番号管理や運用に関連する新たなシステムの開発が必要となり、コスト増となるので反対です。

【情報管理をどうするか】

※①・②のうち最も望ましいと考える選択肢番号を１つのみ選択し、
記載してください。 → ②

※次頁に続きます。

① 一元管理方式（各分野の番号を一本に統一し、情報を一元的・集中的に管理）
② 分散管理方式（情報を各分野で分散管理し、中継データベースを通じて、
共通番号を活用して連携）

【選択理由】
情報管理に関しては、情報漏洩のリスクを小さくするために、各分野で分散管理する方式が優れていると思います。そのことにより、各分野の既存システムをベースに、共通番号で連携を図る効率的なシステムを構築していくべきだと考えます。既存システムがそれぞれ個別の番号で運用されている中、番号を一つに統一することは負担が大きすぎると考えます。

３．選択肢Ⅲ　「保護の徹底をどうするか」

（複数回答可能）

※①～③のうち望ましいと考える選択肢番号を選択し、
記載してください。 → ①②③

① 国民自らが情報活用をコントロールできる
② 「偽造」「なりすまし」等の不正行為を防ぐ
③ 「目的外利用」を防ぐ

【選択理由】
(1)「国民自らが情報活用をコントロールできる」ことを最優先に考えるべきだと思います。国、地方の公的分野での利用に関しては法令により「目的外利用」を規制する必要がありますが、本人が希望する民間利用、産業利用に関しては、過度の制約がつかないようにすることが大切です。
(2)1968 年の「各省庁統一個人コード」や 1980 年の「グリーンカード」など、過去、いくつかの番号制度が検討・実施されましたが、その都度、プライバシー等に対する懸念から普及しませんでした。本番号制度において、そのような国民の不安を払しょくするためには、①自己情報へのアクセス記録を確認できるなど国民自らが情報活用をコントロールできる仕組みを導入すること、②IC カード等を利用した確実な本人確認により「偽造」「なりすまし」等の不正行為を防ぐこと、③法令等を整備することにより「目的外利用」を防ぐこと、の全てを実施するとともに、国民に対する普及・啓もう活動にも力を入れるべきと考えます。

御意見ありがとうございました

産業競争力懇談会（ＣＯＣＮ）

東京都千代田区丸の内一丁目６番６号　〒100-8280
日本生命丸の内ビル（株式会社日立製作所内）
Tel：03-4564-2382　Fax：03-4564-2159
E-mail：cocn.office.aj@hitachi.com
URL：http：//www.cocn.jp/
事務局長　中塚隆雄