情報処理学会論文誌 Vol.53 No.9 2194–2203 (Sep. 2012)

社会保障・税番号制度の民間利活用における課題の整理と解決策の検討

坂崎 尚生[1,2,a)] 側高 幸治[1,3] 長谷部 高行[1,4] 山田 朝彦[1,5] 大岩 寛[1,6]

受付日 2011年11月30日, 採録日 2012年6月1日

概要：2011 年 6 月 30 日に政府・与党社会保障改革検討本部から社会保障・税番号大綱（案）[2] が示された．社会保障・税番号制度は，社会保障や税制を一体的にとらえ，社会保障給付等の効率性・透明性・公平性を高めようという観点から導入が検討されてきた社会基盤である．上記番号制度は社会保障・税分野で利用することを目的とした制度であり，民間への利活用は現段階では検討範囲外である．そこで，産業競争力懇談会（COCN）では，民間への利活用をテーマに，番号制度が国民に安心・安全な社会基盤として受け入れられるように，番号制度の民間利用に関する脅威分析を行い，セキュリティ対策を検討した．本論文は，医療，製品安全，金融の分野での想定したユースケースを基に，課題とその課題を解決するための技術的・制度的対応策をまとめたものである．

キーワード：社会保障・税番号，マイナンバー，脅威分析，セキュリティ対策

Studies on Security in Expansion of the Use of the Social Security and Tax Number System

Hisao Sakazaki[1,2,a)] Koji Sobataka[1,3] Takayuki Hasebe[1,4]
Asahiko Yamada[1,5] Yutaka Oiwa[1,6]

Received: November 30, 2011, Accepted: June 1, 2012

Abstract: We discuss the threat analysis in expansion of the use of the social security and tax number system. In this paper, we describe security countermeasures of the number system based on the medical treatment usage, the distribution industry usage and the financial usage.

Keywords: Social Security & Tax Number, MyNumber, risk analysis, security

1. はじめに

2011 年 6 月 30 日に政府・与党社会保障改革検討本部から社会保障・税番号大綱（案）[2] が示された．社会保障・税番号制度は，社会保障や税制を一体的にとらえ，社会保障給付等の効率性・透明性・公平性を高めようという観点から導入が検討されてきた社会基盤である．上記番号制度は社会保障・税分野で利用することを目的とした制度であり，民間への利活用は現段階では検討範囲外である．番号制度の民間利用については，「2018 年を目途にそれまでの番号法の執行状況等を踏まえ，利用範囲の拡大を含めた番号法の見直しを行うことを引き続き検討する」と述べられ

1 産業競争力懇談会（COCN）
Council on Competitiveness-Nippon (COCN)
2 株式会社日立製作所
Hitachi, Ltd, Yokohama, Kanagawa 244–0817, Japan
3 日本電気株式会社
NEC Corporation, Kawasaki, Kanagawa 211–8666, Japan
4 富士通株式会社
FUJITSU LTD, Oota, Tokyo 144–8588, Japan
5 東芝ソリューション株式会社
TOSHIBA Solutions Corporation, Fuchu, Tokyo 183–8512, Japan
6 独立行政法人産業技術総合研究所
National Institute of Advanced Industrial Science and Technology, Tsukuba, Ibaraki 305–8568, Japan
a) hisao.sakazaki.qc@hitachi.com

ている．上記状況に鑑み，産業競争力懇談会（COCN）では，番号制度が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として広く民間にも利用されるために，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検討した．本論文では，政府検討の番号制度における議論との混同を避けるため，上記政府検討の番号制度とは別に仮の番号制度（以下，個人番号と称する）を想定し，医療，製品安全，金融の分野でのユースケースを基に，課題とその課題を解決するための技術的・制度的対応策をまとめた．なお，国として情報利活用を進めるための社会保障・税番号制度については，内閣官房社会保障改革担当室 [1] や国際公共政策研究センター（CIPPS）[4] 等，様々なところで議論されているので，それらの報告書を参考にされたい．

記号について

本論文では以下の記号を用いて脅威/要件/対抗策を整理している．

T = Threat（脅威）
R = Requirements（要件）
C = Countermeasures（対抗策）

2. 番号制度の民間利用について

番号制度の民間利用について定義する．本論文では「民間利用」とは，民間企業が特定の利用目的で顧客等に個人番号の告知を求め，同番号を個人情報と紐付けて利用することと定義する．こうした民間利用の範囲は個人番号の利用目的に応じて大きく法定的利用と商用的利用に分けることができる．法定的利用とは，法律で定まった業務を行う際に個人番号を使うことが義務付けられている場合であり，税務分野でいえば，雇用主による給与所得の源泉徴収票の提出や，金融機関による配当所得等の支払調書の提出といった法律の規定により提出が義務付けられている業務に対して，個人番号を利用する場合である．一方，商用的利用とは，法令の求めで行うのではなく，営業上の利用であり，医療分野における診療情報の共有や，製品安全分野におけるリコール案内通知，金融分野における契約者の現況確認といったサービスで個人番号を利用する場合である．なお，社会保障・税分野における法定的利用に関しては，主に政府において検討されており，本論文では，主に後者の商用的利用を検討している．

番号制度を民間利用するということは，様々な用途で商用的利用することを想定しているため，個人情報が独り歩きする可能性が高まると考えられる．また，番号制度に携わる組織や人の数も多くなり，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等，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 [1] や CIPPS [4] 等での検討事項に加え，民間利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．本論文では，上記状況に鑑み，番号制度の民間利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[*1]．

3. 番号制度の民間利用における脅威分析

3.1 脅威分析手法

脅威分析を行う手法の 1 つとして，5W1H 脅威分析法がある．5W1H 脅威分析法は「いつ（when）[*2]」「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 脅威分析法を採用し，3.2 節に示す医療，製品安全，金融のユースケースに沿って，「何を（what）」「誰が（who）」を定義し，各ユースケースにおける脅威を分析した．具体的には，「個人の情報」を保護すべき資産（what）ととらえ，「(A) 個人番号」，「(B) 基本情報（氏名，性別，住所，生年月日，ほか）」，「(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) 管理機関等の権限保有者（悪意を持った内部犯，または過失の内部者）」の 2 通りに分類し，脅威分析を行った（**表 1**）．

3.2 民間利用ユースケース

本検討では番号制度を民間利用した際，利便性が高く国民の生活が豊かになると思われる医療，製品安全，金融の 3 分野を例にあげ 9 個のユースケースを設定した [3]．**表 2** に各ユースケースの概要を示す．なお，本節では，上記 9 個のユースケースのうち，代表的な 4 つのユースケースを紹介する（**図 1**）．

表 1 保護対象資産と脅威の主体
Table 1 property and subject.

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，ほか） (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) 管理機関等の権限保有者 （悪意を持った内部犯，または過失の内部者）

[*1] 政府検討の社会保障・税番号制度でも，社会保障分野，特に医療分野等において取り扱われる情報には，個人の生命・身体・健康等に関わる情報をはじめ，特に機微性の高い情報が含まれていることから，個人情報の漏洩が深刻なプライバシ侵害につながる危険性があるとして医療分野等の個別法を検討している．

[*2] 「いつ（when）」に関して，本検討では，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．

表 2 ユースケース概要
Table 2 Use cases.

医療分野	
EHR 医療連携サービス	各医療機関で持っている診療情報を医療機関の間で個人番号を媒介して連携させ，患者に対し地域で一貫した治療を施すためのサービス
PHR 一次利用サービス	母子手帳から健診カルテ，死亡診断書までを電子化し，健康時から病気の時まで一貫して身体の情報を管理し，健康維持や診療支援をするサービス
PHR 二次利用サービス	医療研究機関等が当事者のためだけでなく，公共の利益のために蓄積情報をプライバシを保ちつつ二次的に利用し，医療の質向上に役立てるサービス
製品安全分野	
製品リコールサービス	製品リコールが発生した場合に，製品番号と個人番号を連携して製品の所有者情報を取得し，製品リコール情報を所有者に通知するサービス
事故未然防止サービス	製品の使用状況をインターネット経由でモニタリングし，リスクを未然に通知するサービス
保守継続性サービス	製品を中古で転用する場合やメーカと異なる業者が保守を行う場合において，必要な保守情報を継承し継続性のある品質管理を支援するサービス
製品リユースにおける品質管理・保障サービス	製品が中古市場等で取引される場合に，製品番号と個人番号を用いて必要な情報を入手し適正価格を算出するとともに，製品情報と一緒に売買することを支援するサービス
金融分野	
本人確認サービス	口座開設時の本人確認において，身分証の提示の代わりに，個人番号カードの認証機能等より個人番号に紐付いた本人確認を実施するサービス
現況確認サービス	結婚や引越等で氏名・住所が変更となった場合に金融機関側で個人番号より住民登録情報を参照することで変更届提出等の手間を削減するサービス

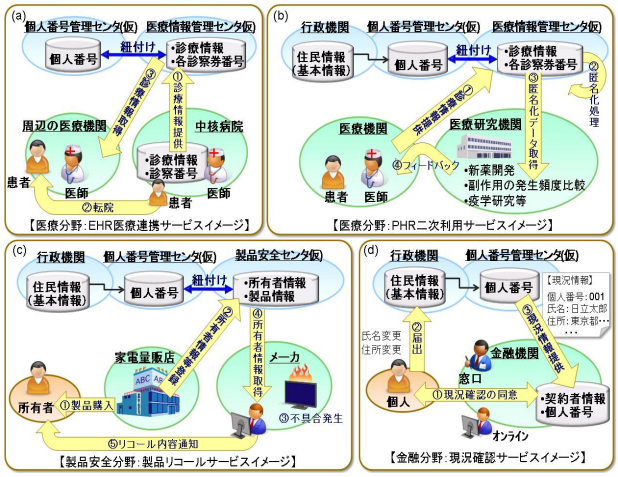

図 1 ユースケース
Fig. 1 Use cases.

本ユースケースでは，以下のセンタを仮設定している．
【個人番号管理センタ】主に個人番号を管理し，個人を特定する情報を提供する．
【医療情報管理センタ】電子化された医療情報を相互に利用するためのセンタであり，主に各医療機関から提供される診療情報および各医療機関で利用されている診察券番号等を管理する．
【商品安全センタ】製品安全に関するサービスを提供するためのセンタであり，主に製品に付けられた製品番号・製品情報と，その製品に関する所有者情報を管理する．

3.2.1 医療分野：EHR（Electronic Health Record）医療連携サービス

患者の様態に応じて切れ目なく医療が提供されるように地域の中核病院と周辺の医療機関が患者の診療情報等を共有する地域医療連携サービス．具体的なサービスシーンは以下．① 中核病院は医療情報管理センタに患者の診療情報・診察券番号・個人番号等を提供する．医療情報管理センタでは提供された診療情報等を個人番号と紐付けて管理する．② 患者は様態に応じて中核病院から周辺の医療機関に転院する．③ 医療機関は転院してきた該当患者の診療情報を個人番号を媒介にして医療情報管理センタから取得し治療を施す（図 1 (a)）．

3.2.2 医療分野：PHR（Personal Health Record）二次利用サービス

医療研究機関（大学病院，製薬会社等）が当事者のためだけでなく，公共の利益のために蓄積された医療情報を患者のプライバシを保護しながら二次利用し，医療の質の向上に役立てるサービス．具体的なサービスシーンは以下．① 医療機関から診療情報・診察券番号・個人番号等を医療情報管理センタに提供する．② 医療情報管理センタでは提供された診療情報等を個人番号と紐付けて管理し，医療研究機関へ患者のプライバシを保護しながら情報提供するために，匿名化処理を行う．③ 医療研究機関は，匿名化データを取得し，医薬品使用後の特定の副作用発生頻度調査や新薬開発，疫学研究等に利用する．④ 分析結果は研究に使われるだけでなく，各医療機関へも医療情報管理セン

タを経由してフィードバックされる．なお，情報を提供する側の個人としては，疫学研究等の結果，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る場合もある．その際，医療情報管理センタは，情報提供時の本人の了解の下，個人番号を介して個人番号管理センタ・行政機関と連携し，本人にその結果をフィードバックする（図 1 (b)）．

3.2.3 製品安全分野：製品リコールサービス

製品リコールが発生した場合に，メーカが製品安全センタ経由で該当製品の所有者情報を取得し，製品リコール情報を所有者に通知するサービス．具体的なサービスシーンは以下．① 所有者が家電量販店等で製品を購入する．② 家電量販店は，所有者の個人番号を取得し，製品番号・製品情報等と合わせて製品安全センタに登録する．③ 不具合が発生する．④ メーカは製品安全センタに問い合わせ，該当製品の所有者情報を取得する．⑤ メーカは取得した所有者情報を基にリコール内容を通知する．なお，所有者が転居等で連絡がとれない場合，メーカは再度製品安全センタに問い合わせ，製品安全センタは情報登録時の本人の了解の下，必要に応じて，個人番号管理センタ・行政機関と個人番号を介して連携し，メーカに最新の所有者情報を知らせる（図 1 (c)）．

3.2.4 金融分野：現況確認サービス

個人と金融機関での同意の下，結婚や引越しに関わる氏名，住所の変更情報や現況確認を，金融機関と行政機関間で個人番号を媒介にしてやりとりすることで，個人からの変更届提出や現況届提出等の手間を削減するサービス．具体的なサービスシーンは以下．① 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る．② 個人が結婚や引越し等に関わる氏名変更や住所変更を市町村役所に届け出る．③ 金融機関は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個人番号管理センタに問い合わせる（図 1 (d)）．

3.3 各ユースケースにおける脅威分析

本検討では，3.2 節のユースケースごとに 5W1H 脅威分析法を用いて脅威分析を行い，110 個の脅威を洗い出した [3]．ここでは，ユースケースより導き出された主な脅威を紹介する（**図 2**）．

例 1. 悪意の第三者が不正アクセスにより医療情報管理センタや個人番号管理センタから個人の診療情報や個人番号等の個人情報を漏洩・改竄する（図 2 (a1)）．

例 2. 本人が了承していないのにもかかわらず，病院どうしで勝手に診療情報等を共有し，本人にとって知られたくない情報が流通してしまう（図 2 (a2)）．

例 3. PHR 二次利用目的で個人を特定する基本情報等を匿名化したつもりが，一部のデータは，個人を推定できるものになっていて，そこから個人が推定される．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，そこから個人が推定される（図 2 (b)）．

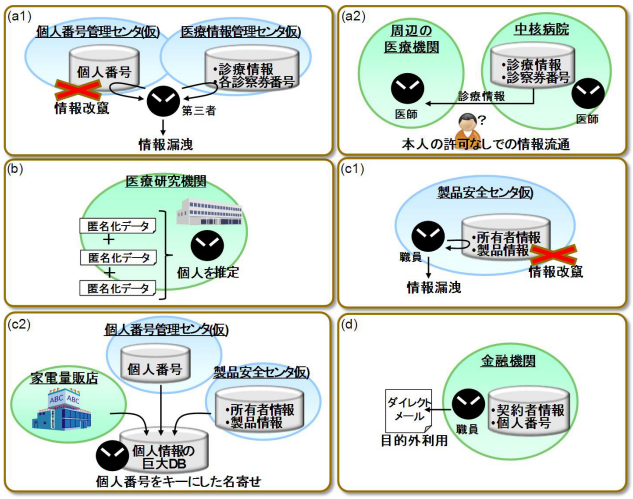

図 2 主な脅威
Fig. 2 Threat.

例 4. 製品安全センタの職員が所有者情報を不正に漏洩・改竄する（図 2 (c1)）．

例 5. 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，本人の知らないところで個人情報に関する巨大 DB が作られる．（図 2 (c2)）．

例 6. 利用者が希望していないのに，個人番号または個人番号を媒介に入手した基本情報等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（図 2 (d)）．

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竄
- **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推定

T2：権限保有者による脅威[*3]
- **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竄
- **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推定
- **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

また，これら **T1**～**T3** の脅威は，以下のような攻撃手段（how）で引き起こされる．

なお，一般的に攻撃は下記 (1)，(2) の順で引き起こされ

[*3] 「T2：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．

表 3 脅威と攻撃手段（how）
Table 3 Relation between threat and attack.

脅威	攻撃手段（how）	
	情報へのアクセス手段	情報アクセス後の処理
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	不正な情報取得等
T1-2：悪意の第三者による情報改竄	不正アクセス，成りすまし等	不正な情報処理等
T1-3：個人番号をキーとした名寄せ	不正アクセス，ネットワーク盗聴，公開データの取得等	番号をキーとした情報収集等
T1-4：匿名化データからの個人推定	不正アクセス，ネットワーク盗聴，公開データの取得等	データ分析等
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	（権限保有者であることの認証）	不正な情報持出し，誤操作等
T2-2：権限保有者による情報改竄	（権限保有者であることの認証）	不正な情報処理，誤操作等
T2-3：番号をキーとした名寄せ	（権限保有者であることの認証），公開データの取得等	番号をキーとした情報収集等
T2-4：匿名化データからの個人推定	（権限保有者であることの認証），公開データの取得等	データ分析等
T2-5：権限保有者による目的外利用	（権限保有者であることの認証）	不正な情報処理等
T2-6：本人の許可なしでの情報流通	（権限保有者であることの認証）	不正な情報処理等
T3：その他の脅威		
T3-1：情報消失等でサービス不履行	天災等によるデータの消滅等	

るが，権限保有者はすでに情報にアクセスできる権限を保有しているため，(2) から始めることができる．

(1) 情報へのアクセス手段

【不正アクセス】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等を悪用してアクセス権を取得する．

【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等により，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す．

【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．

【公開データの取得】公開されている情報からデータを取得する．

(2) 情報アクセス後の処理

【不正な情報取得・持出し】システムへのアクセス権を持っている者が，不正に情報を取得・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，保護対象資産に改竄の危害を加えたり，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竄等の危害を加える．

【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，何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，個人を推定する．

(3) その他

【その他】天災等によるデータの消滅等．

なお，**表 3** は，各脅威と，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．

4. 安心安全な情報利活用のためのセキュリティ対策

一般的にセキュリティ対策は，技術的対策と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，制度的対策は運用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，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．本検討では各ユースケースから抽出した番号制度の民間利用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制度面の両面からセキュリティ対策を検討する．

4.1 セキュリティ要件

3 章で，番号制度の民間利用における脅威とその脅威の攻撃手法が洗い出された．特に攻撃手法が分かれば，その攻撃を成功させないための要件を導くことができる．ゆえに

表 4 技術的対策・制度的対策の概要
Table 4 Solution.

技術的なセキュリティ対策	
攻撃を防止する対策	効果
C1 端末認証	利用できる機器を制限することができる．
C2 ユーザ認証	利用者を認証することで，成りすましを防止することができる．
C3 アクセス制御	ユーザがシステム上で行える処理を制御することができる．
C4 通信路の暗号化	ネットワークを流れる情報の盗聴を防止することができる．
C5 本人の承諾による処理技術	本人了承なしの情報流通を防止することができる．
C6 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．
C7 匿名化技術	データの二次利用の際，匿名化により個人推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	効果
C8 アクセスログ管理	権限保有者が行った処理をログとして管理し監査することで，権限保有者による目的外利用を抑止することができる．
C9 マイ・ポータル技術	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	効果
C10 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．
C11 電子署名	万が一，保護対象資産を書き換えられた場合でも改竄を検知し，改竄されたことを証明することができる．
C12 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．
C13 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．
C14 分散管理技術	クレジットカード仕様の PCIDSS [5] 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，情報流出した時に被害を最小化することができる．
C15 バックアップ技術	複製をあらかじめ作成し，例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．
制度的なセキュリティ対策	
制度的対策	効果
C16 第三者機関の設置	個人番号を利用する組織を認定する機関および，個人番号を利用する組織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．
C17 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・人を認定する制度を策定する．これにより闇金融等，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．
C18 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を策定する．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．
C19 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を策定．これにより不正に対する抑止効果が期待できる．
C20 補償制度策定	番号制度に関連し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を策定．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．
C21 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．
C22 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，主務大臣への報告やそれにともなう改善措置に従わない等，適切な対処をしなかった場合に刑事罰が科される．

表 5 セキュリティ要件と対策
Table 5 Requirements and solution.

要件	必要なセキュリティ対策	
	技術的対策	制度的対策
R1 第三者からのアクセスを防止できること	**C1** 端末認証 **C2** ユーザ認証 **C3** アクセス制御	**C21** 不正アクセス禁止法
R2 成りすましを防止できること	**C2** ユーザ認証	
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	**C2** ユーザ認証 **C3** アクセス制御	
R4 カードの盗難・紛失の際，カード利用を停止できること		**C13** カード失効・再発行
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	**C10** 蓄積データの暗号化	**C22** 個人情報保護法
R6 保護対象資産がネットワークから漏洩しないこと	**C4** 通信路の暗号化	**C22** 個人情報保護法
R7 保護対象資産の改竄を検知できること	**C11** 電子署名	
R8 万一危害があった場合，可能な限り補償がされていること		**C20** 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	**C1** 端末認証 **C2** ユーザ認証 **C3** アクセス制御	**C16** 第三者機関の設置 **C17** 認定制度策定
R10 権限保有者を認証できること	**C1** 端末認証 **C2** 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	**C12** 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	**C10** 蓄積データの暗号化	**C22** 個人情報保護法
R13 権限保有者が行った処理を確認できること	**C8** 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	**C6** 複数人による操作 **C8** アクセスログ管理	**C16** 第三者機関の設置 **C18** 監査制度策定 **C19** 罰則制度策定 **C22** 個人情報保護法
R15 本人または第三者により，自己情報を確認できること	**C9** マイ・ポータル技術	**C18** 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		**C19** 罰則制度策定
R17 限保有者の誤操作が起きにくい仕組みにすること	**C6** 複数人による操作	
R18 本人の許可なしでは情報が流通しないこと	**C5** 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		**C18** 監査制度策定
R20 個人番号とほかの情報が分割管理されていること	**C14** 分散管理技術	
R21 二次利用する際，データが匿名化されていること	**C7** 匿名化技術	
R22 複数の匿名化データを集めても個人が推定できないこと	**C7** 匿名化技術	
R23 バックアップがとられていること	**C15** バックアップ技術	

本検討では，3 章で洗い出した結果から，それらの脅威に対抗するためのセキュリティ要件を導いた．以下にその結果を記す．**R1**〜**R23** が導かれたセキュリティ要件である．

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（本人性を証明できること）
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 個人番号カード紛失等の際，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 万一危害があった場合，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竄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と（本人性を証明できること）

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 個人番号カード紛失等の際，カード利用を停止できること
R7 保護対象資産の改竄を検知できること
R8 万一危害があった場合，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/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推定に対するセキュリティ要件
R21 データを二次利用する際，データが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推定できないこと
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 万一危害があった場合，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竄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 保護対象資産の改竄を検知できること
R8 万一危害があった場合，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/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推定に対するセキュリティ要件
R21 データを二次利用する際，データが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推定できないこと
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[*4]
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
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 情報消失等で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

[*4] 医療分野ユースケースの緊急を要する場合については要検討．

4.2 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，制度的な対策は，より安心安全な番号制度を実現するために技術的な対策を補完するものである．本検討では，上記観点のもと，主要な技術的対策と制度的対策を整理し，4.1 節であげた要件を満たすためのセキュリティ対策について検討を行った．以下，技術的対策と制度的対策の概要をそれぞれ**表 4** にまとめる．また，**表 5** で 4.1 節であげたセキュリティ要件と表 4 のセキュリティ対策との関係を示す．

5. 安心安全な番号制度の民間利用の実現に向け，さらに検討すべき技術的対策と制度的対策

政府検討の社会保障・税番号制度では，番号の利用目的が法律または法律の授権に基づく政省令に規定され，不正行為に対し罰則を設けるため，原則として本人同意を前提としない方向で進んでいるが，本検討の番号制度の民間利用では，様々な用途での利用を想定しており，このままでは，個人情報が独り歩きする可能性が高くなると考える．また，個人番号と紐付く情報が，医療分野における診療情報や金融分野での契約者情報等，よりセンシティブな情報を扱う場合もあるため，それによる被害も高くなると考える．それゆえ，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する対策として，国民が自らの意思で同意した場合に限り，その同意した利用範囲内のみで個人番号を利用できる仕組みが必要と考える．

さらに，サービスが多様化するにつれ，金銭がらみの被害も多くなると考えられ，個人番号を騙った成りすましによる脅威の対策を強化することも重要と考える．また，匿名化データによる個人推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，さらなるセキュリティ対策を講じる必要がある．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】

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．それ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」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等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・ポータル技術の確立（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）
●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】

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いだいている．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？」等，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，医療分野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．

●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】

番号制度の民間利用において，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，成りすまし等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？」等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，携帯電話等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
●携帯電話等，他のデバイスを用いた本人確認方式
●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推定の脅威に対するセキュリティ対策】

医療分野ユースケース（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推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推定できてしまっては，匿名化の意味をなさない．それゆえ，たとえ複数の匿名化情報が集まっても個人を推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推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】

個人情報や企業情報の民間利用に関す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を管理する機関で管理し，必要に応じて診療情報を復号して利用することを想定しているが，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，医療情報管理センタ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が必要となってくる．

【プライバシ影響評価（PIA）：Privacy Impact Assessment】

諸外国では，情報システムの導入等にあたりプライバシへ及ぼす影響を事前に評価し，その保護のための措置を講じる仕組みである PIA [7] が採用されている．PIA を実施することにより，事前にプライバシに対する影響やリスクを軽減するための合理的措置を講じることができる．ま

た，個人番号に係る個人情報の取扱いやシステムに対する透明性が増し，「各機関がどのような情報を収集し，どのように使用するのか」，「安心安全な情報の利活用がどのように実現されるか」について，国民に分かりやすい説明を行うことができる．それゆえ，上記，技術的・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することも重要と考える．

6. まとめ

本論文では，政府検討の番号制度とは別に仮の番号制度を想定し，医療，金融，製品安全の分野でのユースケースを基に，課題とその課題を解決するための技術的・制度的対応策をまとめた．具体的には 5W1H 脅威分析法を用いて，各ユースケースにおける脅威分析を実施し，各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，サービスシーン等により，様々な脅威が存在することが分かった．さらに我々はそれらの脅威に対して，セキュリティ要件を導き出し，技術的面と制度面の両面から対策をまとめた．また，安心安全な番号制度の民間利用の実現に向けさらに深堀りすべき技術的対策と制度的対策を検討した．

参考文献

[1] 社会保障・税に関わる番号制度，内閣官房，入手先 ⟨http://www.cas.go.jp/jp/seisaku/bangoseido/index.html⟩.
[2] 社会保障・税番号大綱，政府・与党社会保障改革検討本部，入手先 ⟨http://www.cas.go.jp/jp/seisaku/bangoseido/pdf/110630/honbun.pdf⟩.
[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の整備プロジェクト，産業競争力懇談会，入手先 ⟨http://www.cocn.jp/common/pdf/thema30.pdf⟩.
[4] 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，入手先 ⟨http://www.cipps.org/img/news/100701/ID number proposals.pdf⟩.
[5] PCIDSS, PCI Security Standards Council, available from ⟨https//www.pcisecuritystandards.org/⟩.
[6] 社会保障・税の共通番号制度の導入と民間利用のあり方，金融税制・番号制度研究会，2010 年 11 月，入手先 ⟨http://www.japantax.jp/teigen/file/20101127.pdf⟩.
[7] 瀬戸洋一，伊瀬洋昭，六川浩明，新保史生，村上康二郎：プライバシー影響評価 PIA と個人情報保護，中央経済社．

坂崎 尚生

1999 年北陸先端科学技術大学院大学情報科学研究科博士後期課程修了．博士（情報科学）．同年（株）日立製作所システム開発研究所（現，横浜研究所）入所．セキュリティ・プライバシに関する研究開発に従事．

側高 幸治

1999 年中央大学大学院理工学研究科電気電子工学専攻博士前期課程修了．同年日本電気（株）入社．現在，同社情報・ナレッジ研究所主任．暗号，PKI，匿名化技術等，セキュリティ基盤技術の研究開発に従事．

長谷部 高行

現所属：富士通株式会社フィールイノベーション本部．1985 年（株）富士通研究所に入社，コンテンツ保護システム等のセキュリティシステムの研究開発に従事．電子情報通信学会会員．

山田 朝彦 （正会員）

東芝ソリューション株式会社 IT 技術研究所主任研究員，理学博士．バイオメトリクスの情報セキュリティに関する国際標準化を中心に，システムに関わる情報セキュリティ技術の研究・開発に従事．

大岩 寛 （正会員）

2005 年 3 月東京大学大学院情報理工学系研究科コンピュータ科学専攻博士課程修了．博士（情報理工学）．同年 4 月に産業技術総合研究所に入所，2012 年 4 月より同研究所セキュアシステム研究部門高信頼ソフトウェア研究グループ長．プログラミング言語・安全なソフトウェア構築手法，インターネット上のプロトコル，認証・ID 連携等，ソフトウェアとそれで実現されるシステム全般のセキュリティ向上に関する研究に従事．