# 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

坂崎 尚生 ‡,†　　側高 幸治 ‡,††　　長谷部 高行 ‡,†††　　山田 朝彦 ‡,††††
大岩 寛 ‡,†††††

‡ 産業競争力懇談会 (COCN)
100-8280 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

†(株) 日立製作所
hisao.sakazaki.qc@hitachi.com
†† 日本電気株式会社
k-sobataka@bx.jp.nec.com
†††(株) 富士通研究所
hasebe.takayuki@jp.fujitsu.com
†††† 東芝ソリューション (株)
Yamada.Asahiko@toshiba-sol.co.jp
††††† 独立行政法人産業技術総合研究所
y.oiwa@aist.go.jp

**あらまし** 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捉え，社会保障給付の効率性・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。本論文では，医療，金融，製品安全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為の技術的・制度的対応策を纏めたものである。

# Inter-cloud Information Sharing Foundation for Secure Utilization of Personal and/or Enterprise Information

Hisao Sakazaki‡,†　　Koji Sobataka‡,††　　Takayuki Hasebe‡,†††
Asahiko Yamada‡,††††　　Yutaka Oiwa‡,†††††

‡Council on Competitiveness-Nippon(COCN)
Nippon Life Marunouchi Building, 1-6-6, Marunouchi, Chiyoda-ku, Tokyo-to, 100-8280

†Hitachi, Ltd
hisao.sakazaki.qc@hitachi.com
††NEC Corporation
k-sobataka@bx.jp.nec.com
†††FUJITSU LABORATORIES LTD.
hasebe.takayuki@jp.fujitsu.com
††††TOSHIBA Solutions Corporation
Yamada.Asahiko@toshiba-sol.co.jp
†††††National Institute of Advanced Industrial Science and Technology
y.oiwa@aist.go.jp

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

# 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捉え，社会保障給付の効率性・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」と述べられている。上記状況を鑑み，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為に，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為，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，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為の技術的・制度的対応策を纏めた。尚，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。

# 2　番号制度の民間活用について

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。従って，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為には，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。それ故，本論文では，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。

表 1: 保護対象資産と脅威の主体

| | |
|---|---|
| 保護対象資産 (what) | (A) 個人番号<br>(B) 基本情報 (氏名，性別，住所，生年月日，他)<br>(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)<br>(b) 管理機関等の権限保有者<br>（悪意を持った内部犯，または過失の内部者） |

# 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一つとして，5W1H 法がある。5W1H 法は「いつ (when)[1]」「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，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)」「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。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 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 分野を例に挙げ 10 個のユースケースを設定した [3]。表 2 にて各ユースケースの概要を示す。

[1]「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

| | |
|---|---|
| **医療分野** | |
| 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為のサービス |
| 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為だけでなく，公共の利益の為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ー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 |
| 各種証明書手続サービス | 個人が税務署に提出する各種証明書類を個人番号を用いて金融機関から税務署に直接提出することで個人での証明書の管理を軽減させるサービス |

### 3.3 各ユースケースにおける脅威分析

本検討では，3.2 節のユースケース毎に 5W1H 法を用いて脅威分析を行い，118 個の脅威を洗い出した [3]。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[2]
- **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

[2]「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。

また，これら **T1**〜**T3** の脅威は，主に以下のような手段 (how) で引き起こされる。

【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し，システムに侵入して保護対象資産に漏洩や改竄等の危害を加える。
【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竄等の危害を加える。
【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，個人を特定する。
【その他】天災などによるデータの消滅等。

尚，表 3 は，3.3 節の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上記攻撃手段 (how) との対応関係を纏めたものである。

## 4 安心安全な情報利活用の為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

表 3: 脅威と攻撃手段 (how)

| 脅威 | 攻撃手段 (how) |
|---|---|
| **T-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 |
| **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 |
| **T1-3**:個人番号をキーとした名寄せ | 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 | データ分析等 |
| **T2-1**:権限保有者による情報漏洩 | 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<br>**T2-3**:番号をキーとした名寄せ | 不正な情報処理, 誤操作等<br>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 | データ分析等 |
| **T2-5**:権限保有者による目的外利用 | 不正な情報処理等 |
| **T2-6**:本人の許可なしでの情報流通 | 不正な情報処理等 |
| **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 |

リティを守る為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，時には利便性が悪化する場合もある。従って，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 章にて，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。特に攻撃手法がわかれば，その攻撃を成功させない為の要件を導くことができる。故に本検討では，3 章で洗い出した結果から，それらの脅威に対抗する為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。

**T1-1 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繋がらないこと）
**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
**T2-1 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繋がらないこと）
**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[3]
**R15** 本人又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
**T3-1 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

## 4.2 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

[3]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

表 4: 技術的対策の概要

| 攻撃を防止する対策 | 効果 |
|---|---|
| **C1** 端末認証,<br>**C2** ユーザ認証,<br>**C3** 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。 |
| **C4** 通信路の暗号化 | ネットワークを流れる情報の盗聴をを防止することができる。 |
| **C5** 自己情報コントロール技術<br>**C6** 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。 |
| **C7** 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。 |
| **C8** 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** |
| **C9** アクセスログ管理<br>**C10** 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為に，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** | **効果** |
| **C11** 蓄積データの暗号化<br>(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。 |
| **C12** 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。 |
| **C13** ロールベース<br>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。 |
| **C14** 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。 |
| **C15** 分散管理技術 | クレジットカード仕様の PCIDSS [5] が推奨している様に，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。 |
| **C16** 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。 |

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為に技術的な対策を補完するものである。本検討では，上記観点の基，主要な技術的対策と制度的対策を整理し，4.1 節で挙げた要件を満たす為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 4,5 に纏める。また，表 6 にて 4.1 節で挙げたセキュリティ要件と表 4,5 のセキュリティ対策との関係を示す。

表 5: 制度的対策の概要

| 制度的対策 | 効果 |
|---|---|
| **C17** 第三者認定機関<br>・監査機関の設置 | 個人番号を利用する組織を認定する機関及び，個人番号を利用する組織を監査する機関を設置する。<br>これにより番号制度に則った正しい運用を実現できる。 |
| **C18** 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。 |
| **C19** 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。<br>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。 |
| **C20** 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。 |
| **C21** 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。<br>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。 |
| **C22** 不正アクセス禁止法<br>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。 |
| **C23** 個人情報保護法<br>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伴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。 |

# 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

表 6 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，情報改竄に関する脅威 (R1〜R7) は，現在確立されている技術的・制度的対策により概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 (R13〜R19) 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 (R2,R3) や匿名化データによる個人推定の脅威 (R21,R22) 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。それ故，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〜R17)】**

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

表 6: 技術的対策と制度的対策の概要

| 要件 | 現在確立されている対策 | | さらに検討すべき対策 | |
|---|---|---|---|---|
| | 技術的対策 | 制度的対策 | 技術的対策 | 制度的対策 |
| **R1** | C2,C3 | C22 | | |
| **R2** | C2 | | C2 | |
| **R3** | C2 | | C2 | |
| **R4** | | C14 | | |
| **R5** | C11 | C23 | C11 | |
| **R6** | C4 | C23 | | |
| **R7** | C12 | | | |
| **R8** | | | | C21 |
| **R9** | C2 | | | C18 |
| **R10** | C1,C2 | | | |
| **R11** | C13 | | | |
| **R12** | C11 | C23 | C11 | |
| **R13** | | | C9 | |
| **R14** | | C23 | C7,C9 | C19,C20 |
| **R15** | | | C10 | C19 |
| **R16** | | | | C20 |
| **R17** | | | C7 | C21 |
| **R18** | | C23 | C5,C6 | |
| **R19** | | | | C19 |
| **R20** | C15 | | | |
| **R21** | C8 | | C8 | |
| **R22** | C8 | | C8 | |
| **R23** | C16 | | | |

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為には，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」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。それ故，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（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。それ故，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。

● 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及び制度設計
● 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，成りすましなど第三者による不正を防止する為に，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為，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（R21〜R22)】**

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，匿名化の意味を成さない。それ故，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 (R12)】**

個人情報や企業情報の民間活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（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為，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。それ故，最終利用者が予め決まっていなくても，医療情報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 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 (以下，個人番号と称する) 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為の技術的・制度的対応策を纏めた。具体的には 5W1H 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，保護対象資産及びその管理場所，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。更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纏めた。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, 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, 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, http://www.cocn.jp/common/pdf/thema30.pdf

[4] 共通番号制度の早期実現に向け 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, http://www.cipps.org/img/news/100701/ID number proposals.pdf

[5] PCIDSS, PCI Security Standards Council, https//www.pcisecuritystandards.org/