

将来を見据えた 国民ID構築のための提言

Proposal for establishing a national ID scheme
– from the viewpoint of security, privacy and architecture

2010年6月26日(土)

個人情報保護研究会

国民IDのあり方検討会

山崎文明、畑野元、三谷洋、小泉雄介、原岡望、
芦田勝、林隆臣、川口元、小林健、力利則

Agenda

1. 本研究の目的と問題提起
2. 国民IDの検討経緯と状況
3. ID付番の代表的な方式
4. セキュリティとプライバシーからみた課題
5. アーキテクチャからみた課題
6. まとめ

1.本研究の目的と問題提起

本研究の目的: **提言**

現在検討が進んでいる国民IDの構築において、
将来を見据えて十分な議論を尽くしたうえで、
制度作りや方式設計を進めるべきである

<十分に議論すべきポイント>

- ・セキュリティに関する議論
- ・プライバシーに関する議論
- ・アーキテクチャに関する議論

2.1 国民IDの検討推移と状況

- 国民IDとは
 - 社会基盤の運営や、行政サービス等を利用する際等に個人を識別する識別子



- 政策の転換
 - 納税者管理番号から社会保障番号へ
 - 行政分野・地方自治まで横断する共通基盤

1.1 国民IDの構築の現状

- 2013年の導入を予定
 - 主な導入目的
 - 国や地方自治体等の行政サービスの利便性の向上、業務の効率化
 - 電子政府の構築に関する安全な社会の形成等
- 懸念事項
 - セキュリティ、プライバシーに関する議論は十分か
 - 諸外国の**既存の**方式を参考に行っている
 - 将来にわたって有効な技術を取り入れるように検討されているか

1.2 検討・議論の主な不足事項

1. セキュリティに関する議論

- マスターIDとトランザクションIDの識別
- IDの再付番をどのように行うかの検討
- セキュリティリスクを想定した検討

2. プライバシーに関する議論

- 名寄せの問題（容易に名寄せが可能となるリスク）
- 自分で自分をどう証明するか

3. アーキテクチャに関する議論

- 安全面、制度面、運用面の検討
- 将来にわたる有効性の確認

- 技術力や法制整備、方式設計等に関する先進国となり得るか、安全でより便利な社会を築けるかを左右するもの
- 拙速に導入を進めるのではなく、十分な議論を尽くすことが必要



技術立国の礎とすべき

2.国民IDの検討経緯と状況

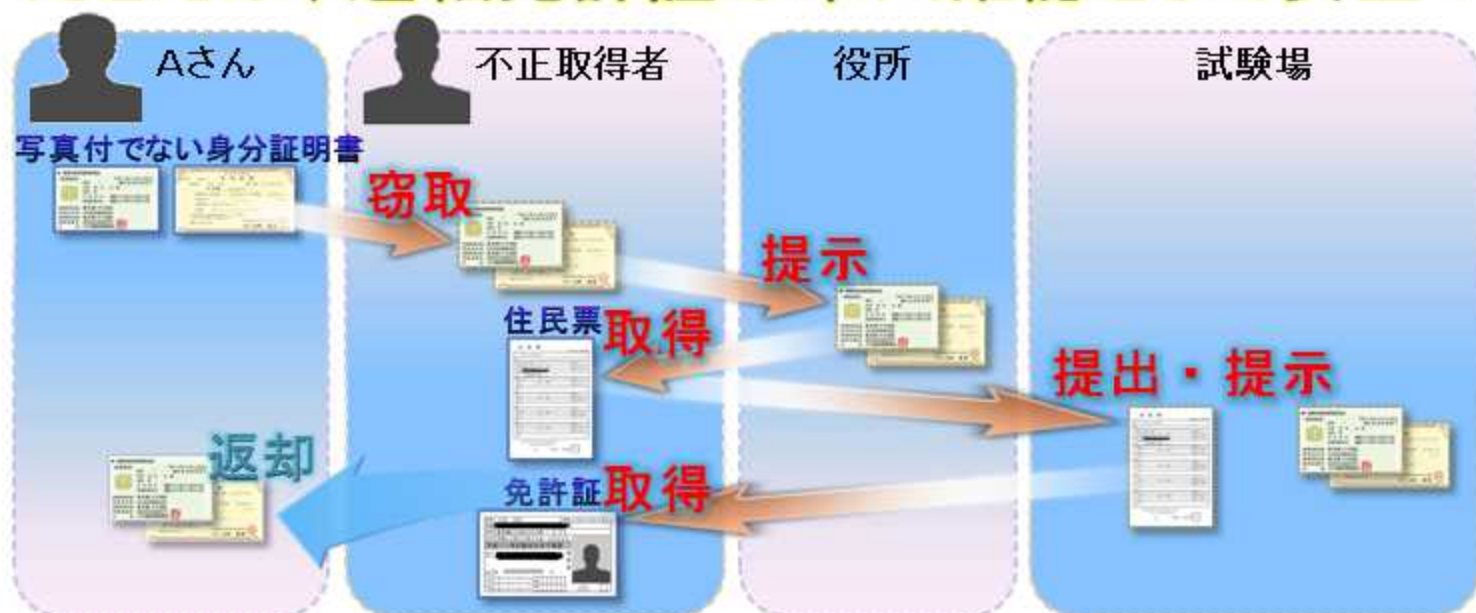
2.2 プライバシー問題

- 従来の行政分野別番号の見直し
 - 1968年 各省庁統一個人コードの検討開始
 - 1979年 納税者番号の検討開始
 - 2001年 社会保障番号の検討開始
- 「国民総背番号制」への不安
 - 1994年 住基ネットの検討開始
 - ・ 当初、住民票コードの行政分野横断、民間利用も検討
⇒ プライバシー上の不安による批判が集中
 - 住民の居住関係の確認のみの利用に限定
 - 民間利用は禁止

2.3 本人確認の重要性

- 本人確認手段の信頼性確保が必要
 - 「不正な信用の連鎖」を招かないようにする
 - 国民IDの発行時の本人確認を厳密に行う

たとえば、運転免許証は本人確認として安全？



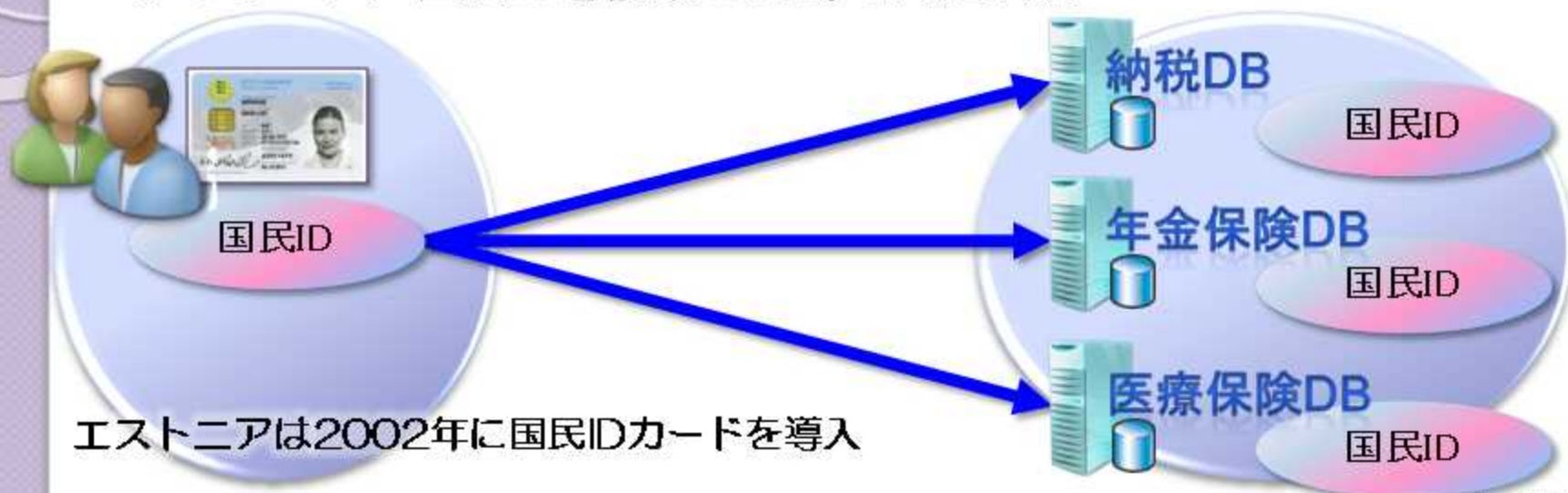
3. ID付番の代表的な方式

- フラットモデル (エストニア)
- 符号化フラットモデル (フィンランド)
- セパレートモデル (ドイツ)
- 変換テーブル式セパレートモデル
(日本で導入検討中)
- セクトラルモデル (オーストリア)

3.1 ID付番の代表的な方式①

フラットモデル

(エストニア) 国民IDを複数の分野で共通利用



メリット

- 分野別番号・行政サービスの統合、ワンストップ化が容易

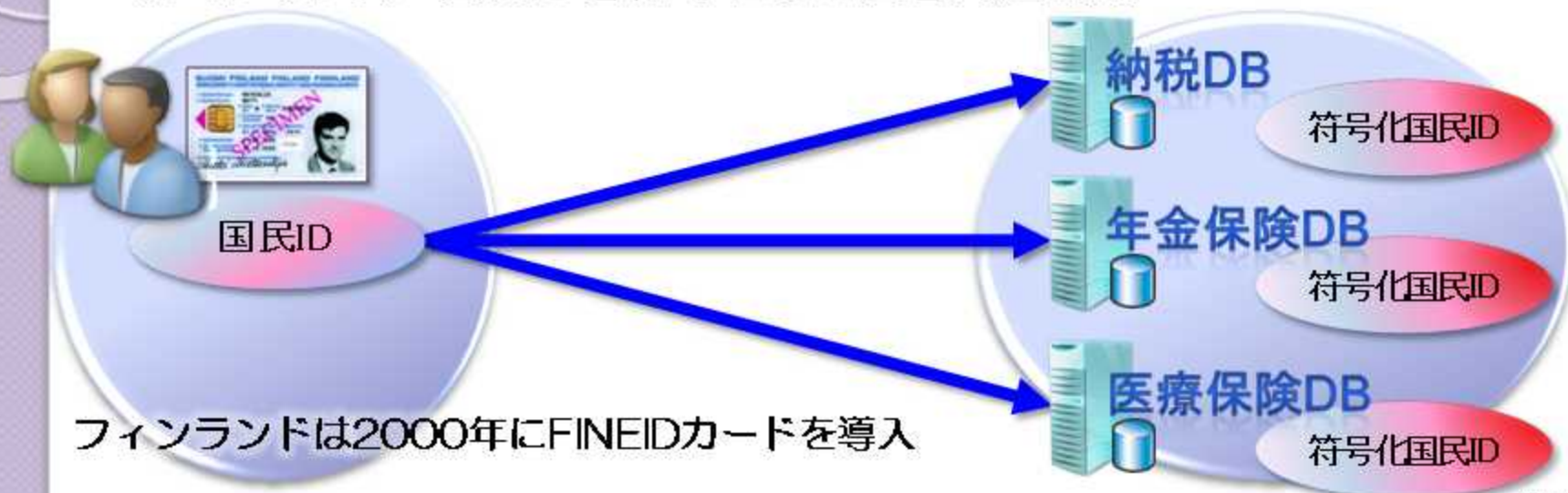
デメリット

- 個別データベースから情報漏えいした場合、国民IDをすべて再付番する必要がある
- 不正利用や情報漏えい時のデータマッチングのリスクが高い

3.2 ID付番の代表的な方式②

符号化フラットモデル

(フィンランド) 国民IDを符号化した値を共通利用



メリット

- 分野別番号・行政サービスの統合、ワンストップ化が容易
- 個別データベースから情報漏えいした場合も、すべての国民IDを再付番する必要はない

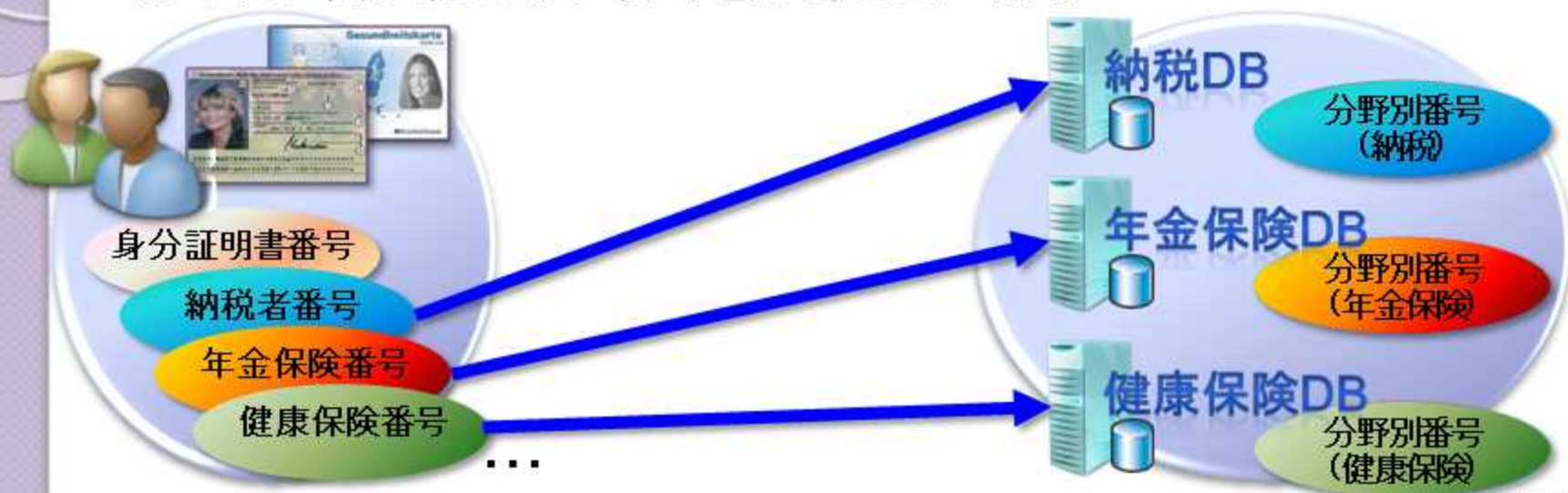
デメリット

- 不正利用や情報漏えい時のデータマッチングのリスクが高い

3.3 ID付番の代表的な方式③

セパレートモデル

(ドイツ) 関連性のない番号を分野ごとに利用



メリット

- 不正利用や情報漏えい時のデータマッチングのリスクは比較的低い

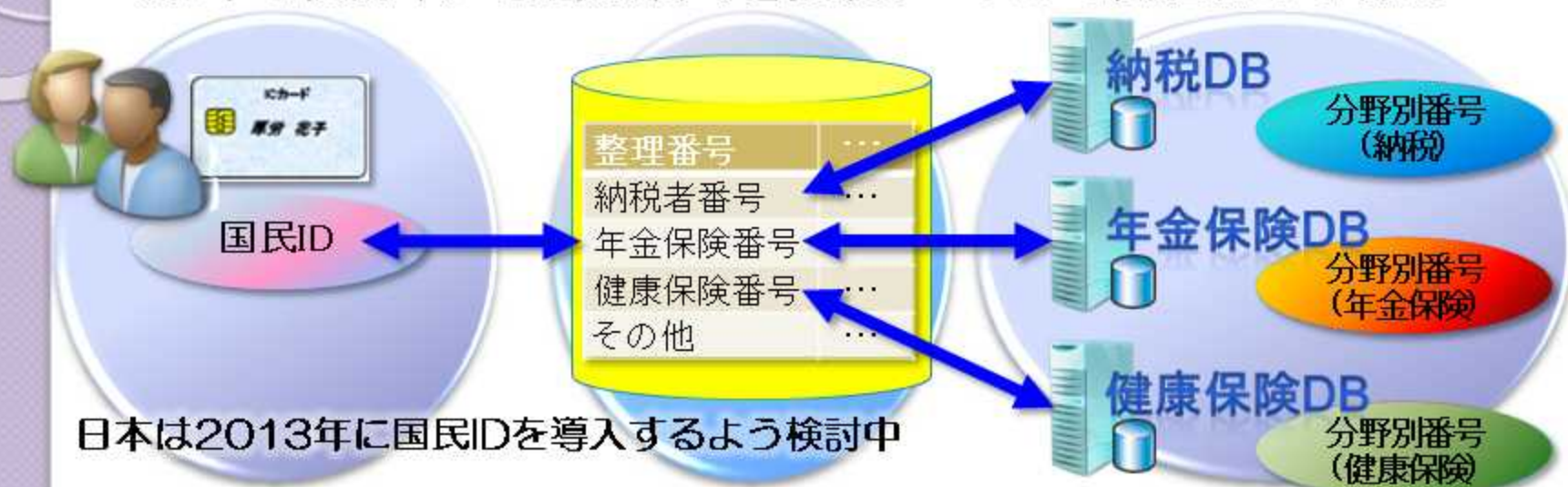
デメリット

- 各種行政サービスの統合、ワンストップ化は困難

3.4 ID付番の代表的な方式④

変換テーブルモデル

(日本で検討中) 分野別番号を変換テーブルで関連付けて利用



メリット

- 各種行政サービスの統合、ワンストップ化が可能

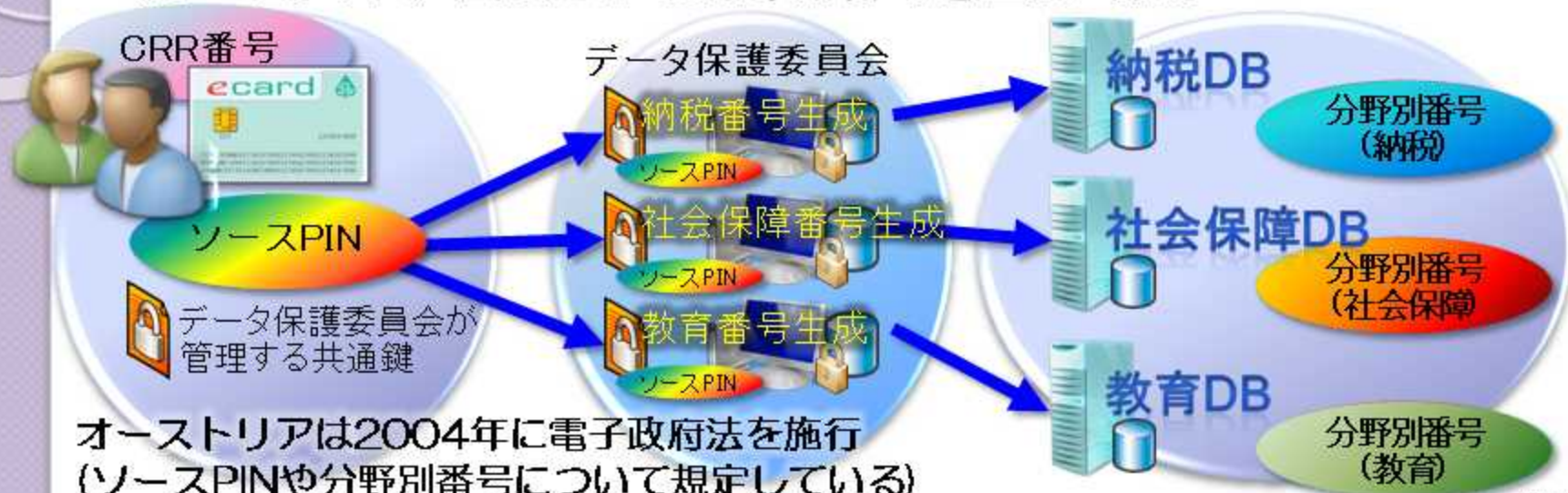
デメリット

- 不正利用・情報漏えい時に、すべての分野別番号が漏えいするリスクが高い

3.5 ID付番の代表的な方式⑤

セクトラルモデル

(オーストリア) 国民IDから分野別番号を生成・利用



メリット

- 個人データを分野間で交換することが比較的容易
- カードには1つの番号を記録するのみでよく、変更・追加等不要
- 不正利用や情報漏えい時のデータマッチングのリスクが低い

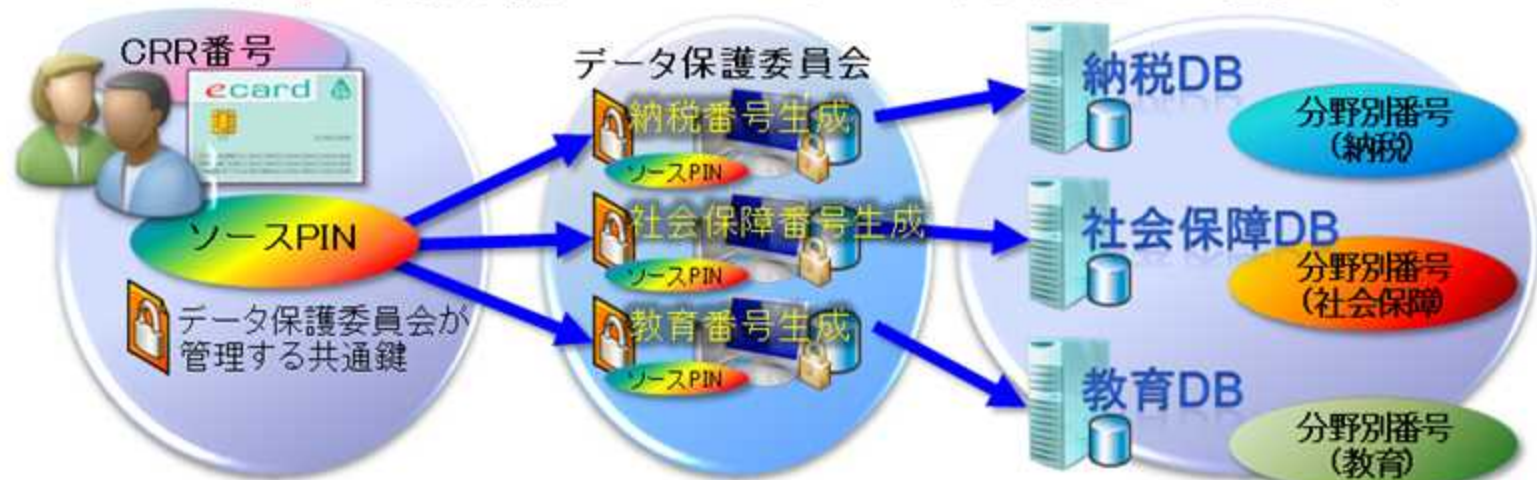
デメリット

- 分野別番号を体系的に付番する際、手間がかかる

4. セキュリティとプライバシー からみたID付番の課題

4.1 セキュリティの確保

- マスターIDは変更(再付番)しない
 - マスターIDは日常的には使用しない
 - 何をマスターIDにするか十分に議論する
 - マスターIDとランザクシオンIDは区別する
- 短期間で再付番できるように検討しておく
 - セグメント化して、1回で漏えいするIDを少なくする
 - 短期間で再付番できるようにID発行窓口を多くする



4.2 プライバシーの確保

- 容易にデータマッチングできないようにする
 - 同じIDを複数の行政サービスで使用すると名寄せが容易になる
 - ・ ドイツは納税者番号を税務処理の利用に限定
 - 利便性との調和を図ることも必要
 - ・ 国民が複数のIDを管理し使い分ける煩わしさ
 - 名寄せができないことを悪用されるおそれ
 - ・ 特定の条件を満たした場合に名寄せを可能とする余地を残す
 - ☞ 本人の同意を得た場合、第三者機関の審査を経た場合

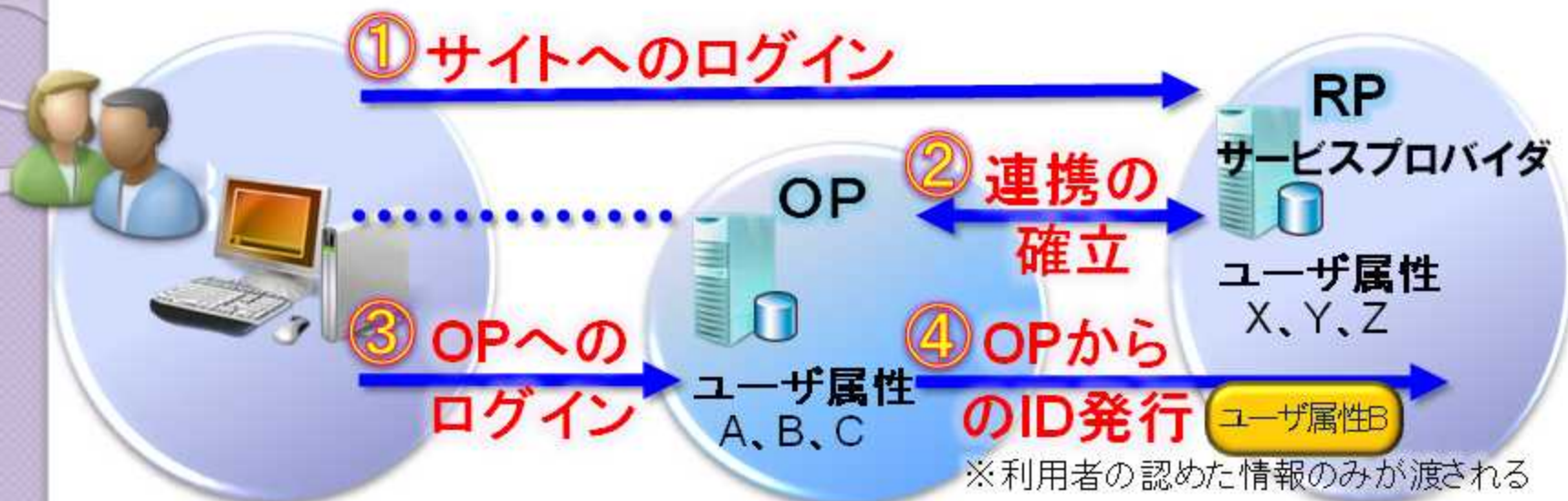
5.アーキテクチャからみた課題

5.1 要件を満たす方式(ダイナミックID)



- 認証にはマスターIDは使用せず動的に生成されたIDを利用する方式
- マスターIDを直接利用しないことでマスターIDの漏えいを防止(再付番の必要性を排除)
- 認証時に使用されたIDは毎回変わるので認証時のIDによる名寄せはできない

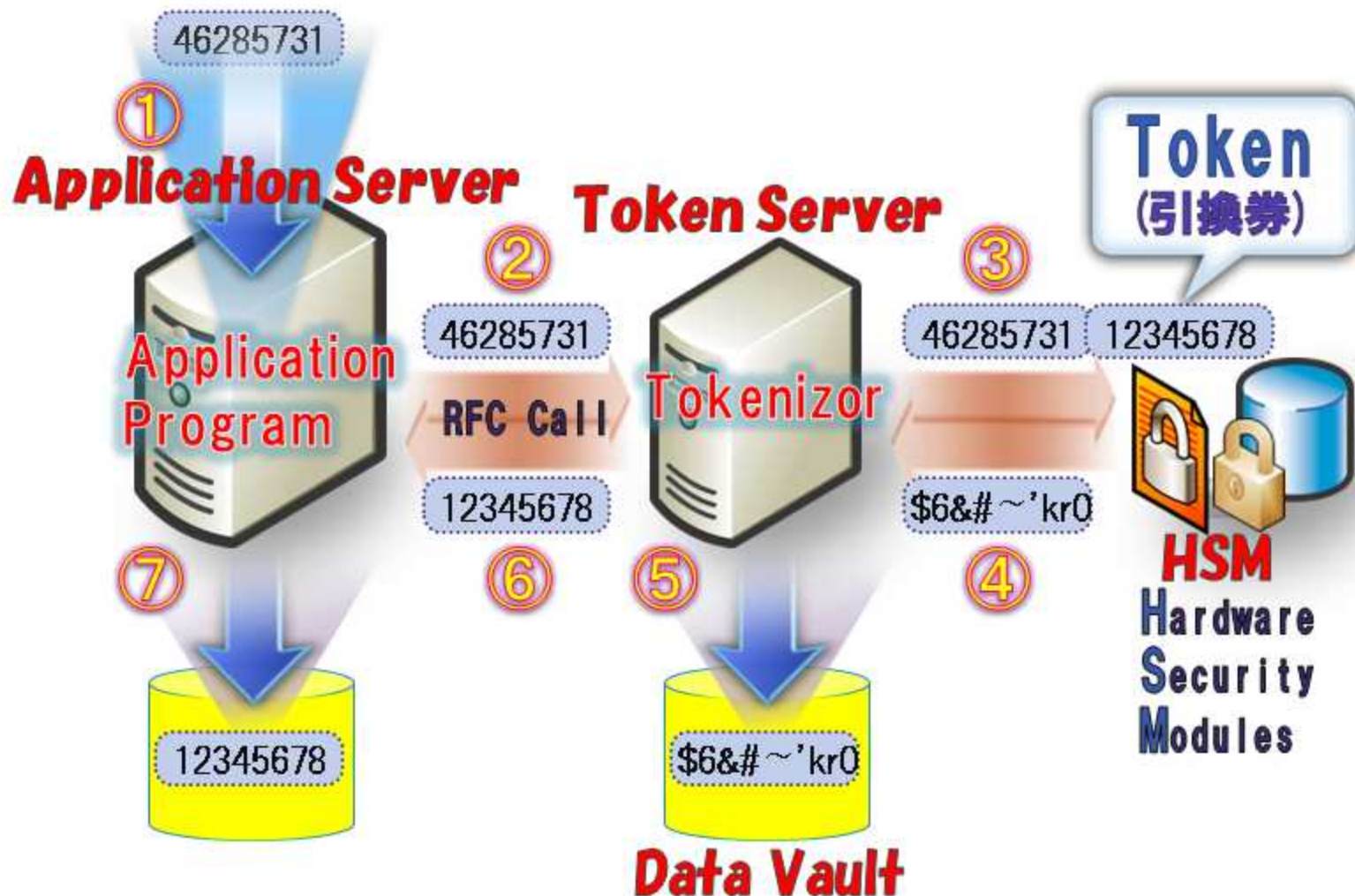
5.2 要件を満たす方式(OpenID)



- 利用者は登録したOP (OpenID Provider) による認証で、他のサービスプロバイダのサービスが利用できる
- サービスプロバイダでのサービス利用は、OPにより渡されるURL形式のOpenIDで行われ、マスターIDの漏えいを防止できる
- サービスプロバイダへ渡されるIDは仮名で行われるため名寄せはできない

5.3 トークナイゼーション

保護されるべきIDを無意味な数列(Token)に置き換えて処理



5.4 実現に向けた課題

- 情報が漏えいしても悪用できない仕組み
 - IDやパスワードのワンタイム化 (Dynamic Data/Unique Transaction)
 - トークナイズによる漏えい情報の無意味化
- 情報漏えい被害範囲の局所化
 - セクトラルモデルによる漏えい被害の局所化
 - セクターID変更による容易な再付番
- 第三者機関の審査の下での名寄せ
 - 第三者による暗号鍵の保管と使用許諾審査



6. まとめ

国民ID導入の先駆者である豪州の事例

- 1986年→2006年→2009年と3回にわたって、方式設計を見直し、新技術を導入
- さらに次の点について、議会を中心とする国民的な議論を行っている

- ✓ 付与対象者やその強制付与の範囲
- ✓ IDデータベースの登録項目や認証媒体の保有情報の内容
- ✓ 中央管理システムの保管データやネットワークへのアクセス権の明確化
- ✓ 民間部門のID利用の限定方法
- ✓ 登録情報への本人の開示請求・修正権 等

国民ID構築は

- 日本が将来に向けて技術力や法制整備、方式設計等に関する先進国となり得るためのものである
- 安全でより便利な社会を築けるか左右するものである
- 拙速に進めるのではなく、十分な議論を尽くすことが必要である

将来を見据えた 国民ID構築のための提言

Proposal for establishing a national ID scheme
– from the viewpoint of security, privacy and architecture

質疑・ご意見を
お願いいたします