# JSSM25 周年記念事業「社会への提言」提言(案) カバーシート

応募日　２０１１年　１月　２４日

提言(案)に本票を添付して応募いたします。

| | | | |
|---|---|---|---|
| 1 | 提言(案)<br>文書 | タイトル | 「情報セキュリティとプライバシー保護の観点からの国民 ID に関する提言」 |
| | | 研究会 | 個人情報の保護研究会　国民 ID 検討会 |
| | | 文書ファイル | （ファイル名：　国民ＩＤ検討会(研究会提言書.docx　） |
| 2 | 提言内容 | 主たる提言対象 | 日本国政府、各省庁、関連機関<br>・情報セキュリティやプライバシー保護の研究者および実務家<br>・国民全体 |
| | | 提言の要旨<br>(200 字程度で) | 国民 ID や共通番号制度の円滑な導入と利活用を推進するためには、ID の特性を踏まえた情報セキュリティとプライバシー保護に十分配慮した仕組みであることが国民に理解される必要がある。ID に関わる情報セキュリティとプライバシー保護の観点から認識すべき 3 つの提言とその提言を実現するための具体的な対策を提示する。 |
| | | 期待効果 | 制度と技術の両面から情報セキュリティとプライバシー保護について英知を集めた十分な議論が尽くされ、技術立国としての我が国にふさわしい国民 ID システムが構築される。 |
| 3 | 共同作成者 | 氏名／所属 | JSSM 個人情報の保護研究会　国民 ID 検討会<br>（山崎文明、畑野　元、三谷　洋、小泉雄介、原岡　望、林　隆臣、川口　元、小林　健、力　利則） |

JSSM からの提言チェックリスト

☑自分自身(つまり JSSM)への提言ではない

☑社会の発展や全体の利益につながる

☑既存の組織・団体を非難/誹謗/中傷する内容ではない

☑特定の組織・団体の価値観を押し付けるものではない

☑社会通念上求められる倫理観に添ったものである

☑提言は対象が明確で、具体的に記述されている

☑提言は事実やデータに裏付けられている

☑提言はこれまでにない独創的なものである、あるいはこれまでの取り組みを大幅に改善するものである

# 情報セキュリティとプライバシー保護の観点からの国民 ID に関する提言

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

JSSM 個人情報の保護研究会　国民 ID 検討会
山崎文明、畑野　元、三谷　洋、小泉雄介、
原岡　望、林　隆臣、川口　元、小林　健、力　利則

## はじめに

ID の活用が進んでいる国、例えば米国では他人の ID を使用して不正に社会保障サービスを受給する犯罪（ID Theft）が社会問題となっている。我が国においても国民 ID や共通番号が導入されることで同じような状況が生じることが懸念される。ID の不正使用は、クレジットカード番号やオンラインゲーム用 ID の不正使用など､すでに国内でも頻発している。コンピュータで処理される ID は、氏名と異なり重複がなく、唯一のものとしてそれだけでサービスの受給者が特定されるものである。また、ID は、容易に個人を特定できるため名寄せのためのキー（データマッチング・キー）として使用されることでプライバシーが脅かされるおそれがある。さらに、ID が一度サイバー空間上に漏えいすれば、大量の複製が作成され二度と消去できない状態となることは避けられない。一方で、ID は、氏名と異なり、新たに ID を採番し直すことも可能である。また、漏えい等の理由で不正使用されるおそれがあれば、新たに ID を採番し直すことも必要となる。

国民 ID や共通番号制度の円滑な導入と利活用を推進するためには、こうした ID の特性を踏まえた情報セキュリティとプライバシー保護に十分配慮した仕組みであることが国民に理解される必要がある。ID に関わる情報セキュリティとプライバシー保護の観点から認識すべき 3 つの提言とその提言を実現するための具体的な対策を提示する。

**提言 1　国民 ID は、ID の漏えいに強い仕組みであること**
- **(1) ID 漏えい時の再付番ルールを明示すること**
- **(2) マスターID とトランザクション ID を識別すること**
- **(3) トークナイゼーションを活用したトランザクション ID を生成すること**
- **(4) ID 漏えいの影響の極少化を考慮したセクター別トランザクション ID に分けること**

**提言 2　国民 ID は、容易に名寄せできない仕組みであること**
- **(1) 第三者機関による名寄せコントロールを可能とすること**
- **(2) ID によらない名寄せ防止を考慮した情報分散を行うこと**

**提言 3　国民 ID は、新たに出現する情報セキュリティの脅威に柔軟に対応できる仕組みであること**
- **(1) 継続的な事件・事故事例および技術動向の調査を実施すること**
- **(2) 最新動向を踏まえた情報セキュリティ対策の適用と多様性の確保、および法制度を構築すること**

## Ⅰ　国民 ID は、ID の漏えいに強い仕組みであること

### Ⅰ－１　ID 漏えい時の再付番ルールを明示すること

情報セキュリティの観点から、ID が漏えいした際の ID の変更（再付番）方針について明確にすべきである。紙媒体を基本にした行政サービスの時代には、数十件、数百件といった件数の情報漏えいを想定しておけばよかったが、電子化された行政システムでは、数十万件、数百万件、あるいは一瞬にして全件の ID が漏えいすることも見越しておく必要がある。

ID が漏えいした際にその不正使用を防止するためには、遅滞なく漏えいした当該 ID を無効と宣言した（Revocation）上で、ID を付番し直すことが情報セキュリティの基本である。

住民票コード番号は、本人の請求において変更可能とされているが、ID の漏えい事件・事故が生じた場合には、本人の希望にかかわらず、政府の責任において再付番する必要がある。「情報漏えいは起こり得ることを前提とした仕組み」として、ID 漏えい時の再付番ルールが示される必要がある。

### Ⅰ－２　マスターID とトランザクション ID を識別すること

容易に再付番できる仕組みとすることは、ID 漏えいにともなう ID の不正利用を阻止する上で重要である。ID の漏えい時に再付番を容易に行うためには、マスターID とトランザクション ID の区別が必要である（図１）。

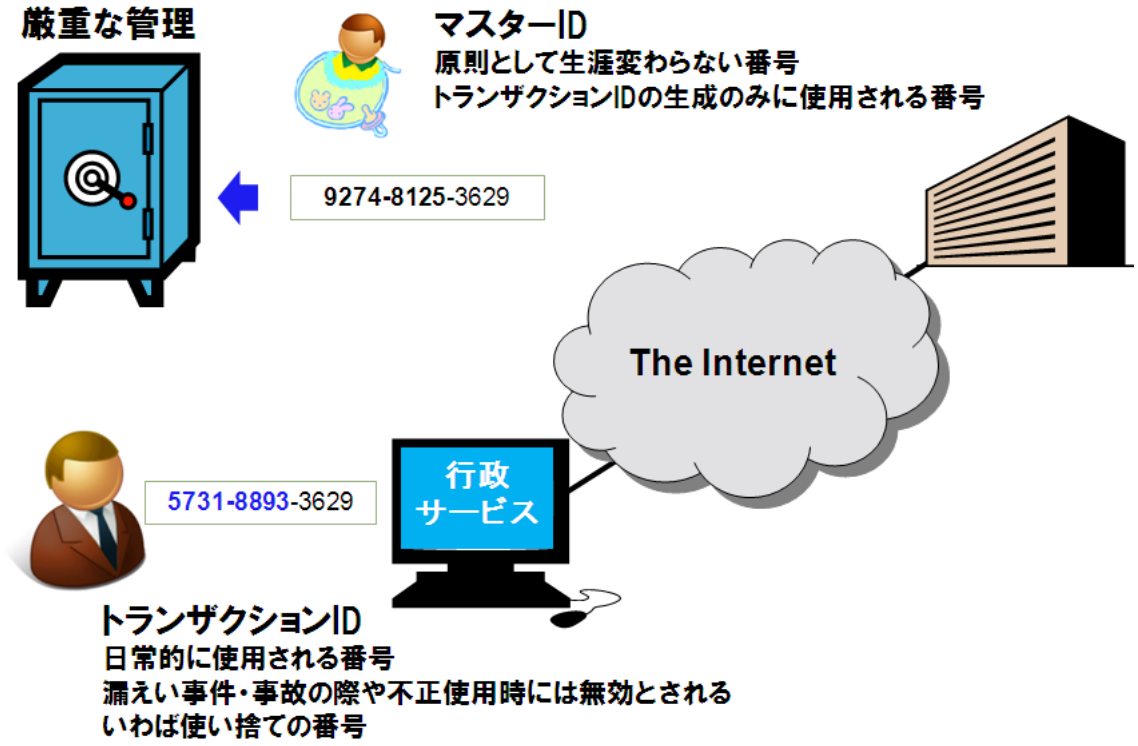


図１　マスターIDとトランザクションID

マスターID とは、原則として変更（再付番）されない普遍的な ID を指す。マスターID は、その性質上厳重な管理が必要であり、日常の行政サービス等に利用してはならない。マスターID は、用途をトランザクション ID の生成に限定し、漏えいする可能性を最小限とする必要がある。一方、トランザクション ID は、マスターID から生成される ID で、事業体やサービスなどの複数のシステム間で頻繁にやり取りされることから、常に漏えいの脅威にさらされるという性質を持つ。トランザクション ID の漏えいが確認された場合には、マスターID から新たにトランザクション ID が生成される。トランザクション ID はいわば使い捨ての ID である。

住民票コード番号自体は、すでにトランザクション ID として使用されていることから、マスターID としての要件を満たしておらず、漏えいリスクが付きまとうという点が懸念される。したがって、現行の住民票コード番号を元に（下記のトークナイゼーション技術を利用して）新たな ID を生成し、この新たな ID を国民 ID のマスターID とするといった一過性の手続きも検討する必要がある（図 2)。

トランザクション ID とマスターID という概念に基づき国民 ID や共通番号の設計を行うとするならば、何をもってマスターID とするかについて十分な検討が望まれる。

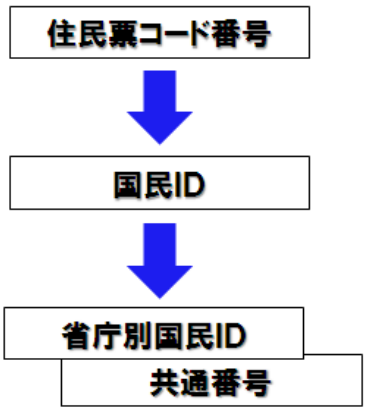


**図2　住民票コード番号からの国民IDの生成**

### Ｉ－３　トークナイゼーションを活用したトランザクション ID を生成すること

マスターID の秘匿化およびトランザクション ID の生成方式として、オーストリアではハッシュ関数による暗号化方式が用いられている。しかし、暗号化による生成方式を採用する場合には、暗号アルゴリズムが危殆化した際の影響についても考慮しておく必要がある。そこで、トランザクション ID の生成方式として、トークナイゼーション(Tokenization)の活用を提言したい。トークナイゼーションとは、トークン化するという意味で、トークンとは「意味のない数列」や「引換券」という意味があり、情報セキュリティ分野では、元の ID を数学的な関連性がない別の数列等に置き換える技術を指す。暗号化と異なりトークナイゼーションされた ID から数学的な解析によって元の ID を求めることはできない。

トークナイゼーション技術を使用してマスターID からトランザクション ID を生成する手順は次の通りである（図 3)。

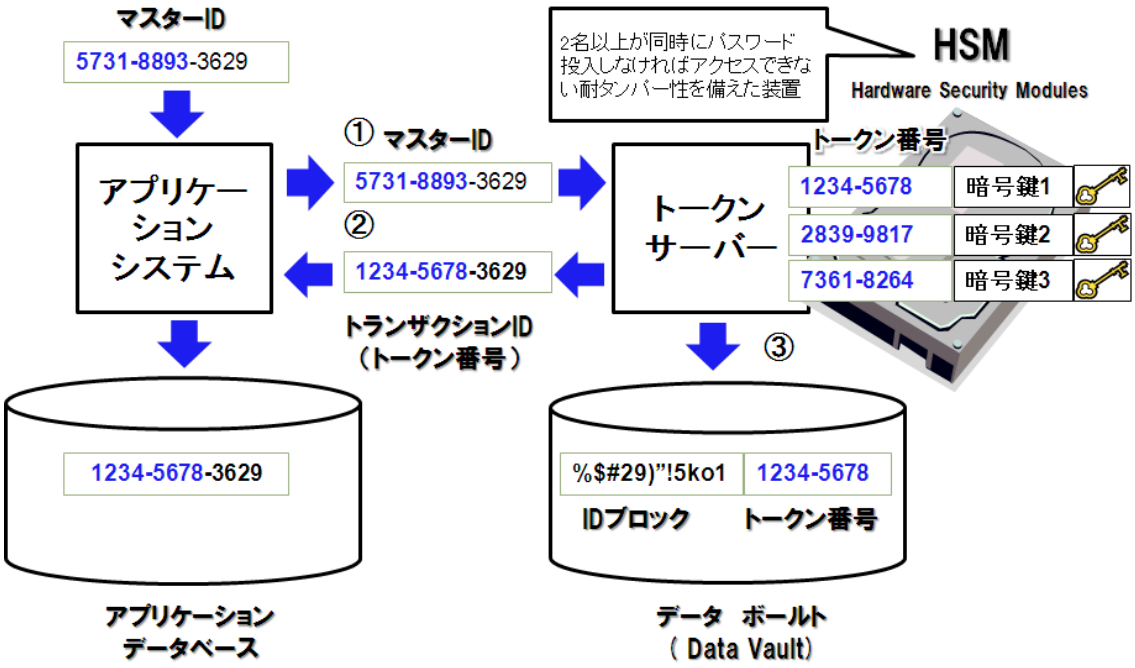


**図3 マスターIDからトランザクションIDを生成する手順**

① マスターID を読み込んだアプリケーションシステムは、トークンサーバーに搭載されたトークナイゼーション・プログラムを呼び出し、マスターID をトークナイゼーション・プログラムに引き渡す。

② マスターIDを受け取ったトークナイゼーション･プログラムは､マスターIDの全数列、もしくは一部（図 3 では上 8 桁）の数列をトークンに置き換えトランザクション ID を生成して、アプリケーションシステムへ返す。

③ トークンサーバーは、生成したトークンとマスターID を HSM(Hardware Security Module )に引き渡す。マスターID は、HSM 内で生成された暗号鍵で暗号化され（暗号化されたマスターID は ID ブロックと呼ばれる)、対応するトークンとともにデータボールト（Data Vault）と呼ばれる厳重に管理されたデータベースに保管される。

HSM は、耐タンパー性（無理にこじ開けようとするとデータが消滅する）を備えた装置であるため、物理的に盗難されてもデータが漏えいする可能性は、極めて低い。また、格納されている暗号鍵にアクセスするためには 2 名以上のアクセス権を持った者がそれぞれのパスワードを同時に入力しなければならないため、パスワードを知っている者同士が結託しない限り、暗号鍵が知られることはない。

データボールトとは、一般のアプリケーションシステムとは隔離された高度に情報セキュリティ対策が施されている領域（ドメイン）に設置されたデータベースのことで、

厳重なアクセス制御が行われる。データボールトに格納されるデータは、暗号化されたマスターID（ID ブロック）とマスターID に対応したトークンであり、仮にデータボールトのデータが漏えいしたとしても ID ブロックが解読され復号されない限り、マスターID が漏えいすることはない。さらにトークン番号がマスターID の一部の桁数でしかない場合は、トランザクション ID としての意味も持たないことから、極めてデータ漏えいに強い仕組みといえる。

### Ⅰ－4 ID 漏えいの影響の極少化を考慮したセクター別トランザクション ID に分けること

ID の不正使用を防止するため、ID の漏えいが確認された場合は、すみやかに当該 ID が失効される必要がある。したがって ID の失効による影響範囲を極少化する仕組みが不可欠である。行政サービス単位や共通管理単位ごとにトランザクション ID を異なるものにすることでトランザクション ID の漏えいにともない発生する影響範囲を行政サービス単位や共通管理単位に限定することができる。

セクトラルモデルを採用しているオーストリアの事例にみられるように、行政サービス単位や共通管理単位ごとにセクターID を付番し、それぞれのセクターID とマスターID を組み合わせた数列（もしくは文字列）に対してトークナイゼーションを行うことで、セクターごとに異なったトランザクション ID が生成される（図 4）。

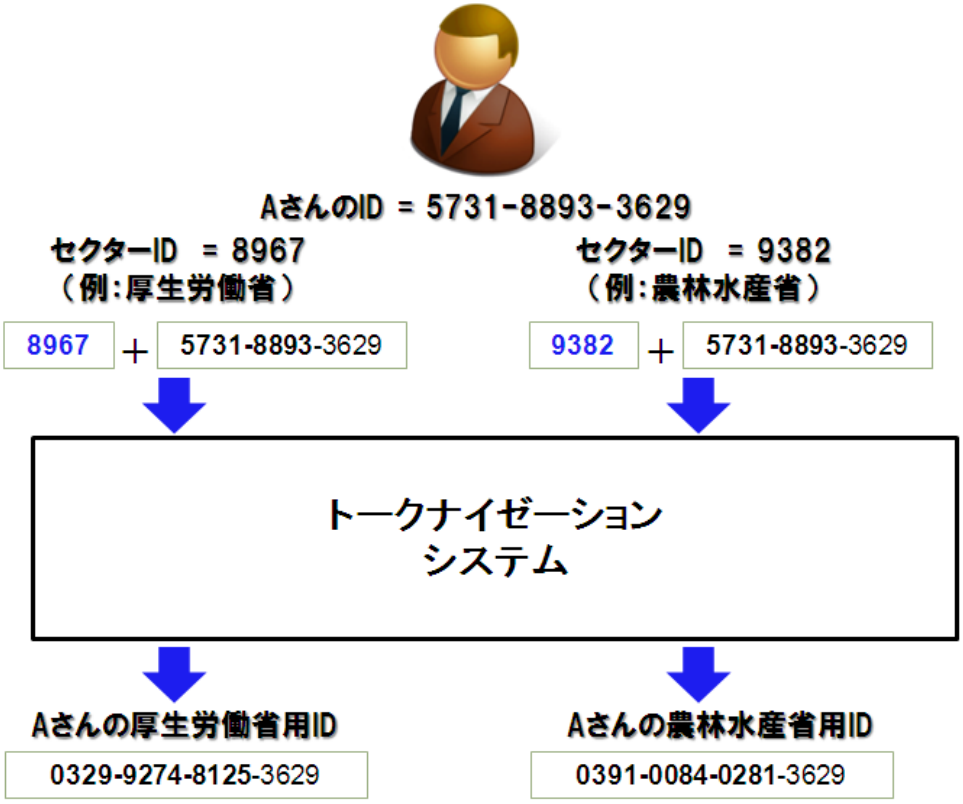


図4 セクター別トランザクションIDの生成

特定のセクターで使用されている ID が漏えいした場合には、当該セクターのセクターID を再付番し、新たに付番されたセクターID とマスターID の組み合わせからトランザクション ID を生成することで再付番が完了する。ID 漏えいの影響範囲を極少化するとともに被害の発生を適切に予防し、回復するという観点からの方式設計が期待される。

１つのセクター別トランザクション ID から、用途によって複数のサブトランザクション ID を生成することも可能であり、同一セクター内でサービスごとに ID を使い分ける方式に応用することもできる（図 5)。

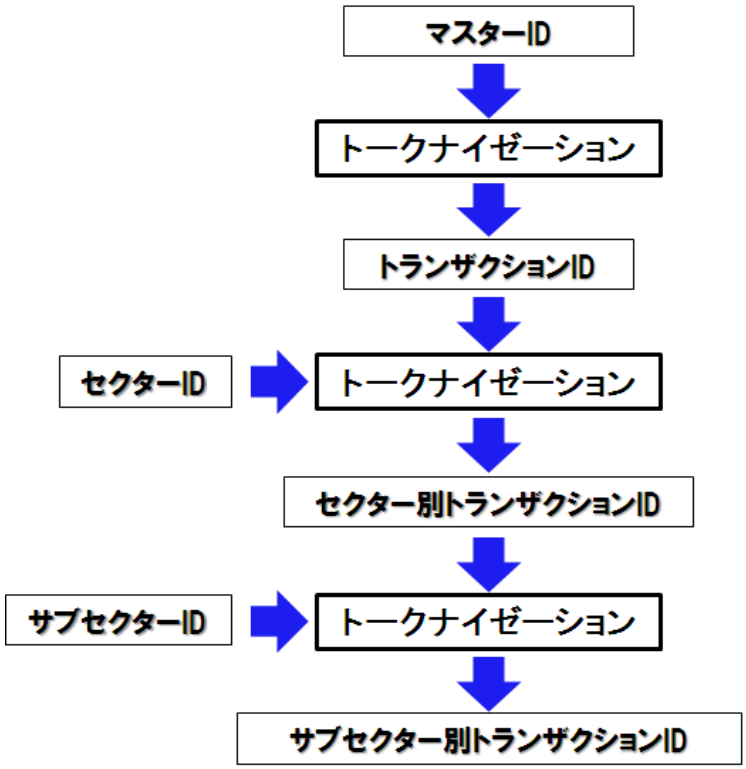


**図5　行政サービス分野ごとのトランザクションIDの生成**

## Ⅱ　国民 ID は、容易に名寄せできない仕組みであること

### Ⅱ－１　第三者機関による名寄せコントロールを可能とすること

異なるトランザクション ID を用いている行政サービス間での名寄せは、それぞれのトランザクション ID をトークナイゼーションされる前の状態（マスターID）に戻さない限り不可能である。トークナイゼーションされた ID を元のマスターID に戻すためには、データボールトのデータと HSM 内に格納された暗号鍵が必要になる。したがって、データボールトと HSM、もしくは HSM のアクセス権を有効にするパスワードを第三者機関が管理することで許可されない名寄せを防止することができる（図 6)。欧州のプライバシー・コミッショナー制度に見られるような政府によるプライバシー侵害を監視したり、通報を受け付けたり、

名寄せ行為の妥当性を審査する第三者機関もしくは別途の第三者機関が、トークンサーバーを管理下に置くことで、政府等による無許可の名寄せを確実に阻止することが可能となる。

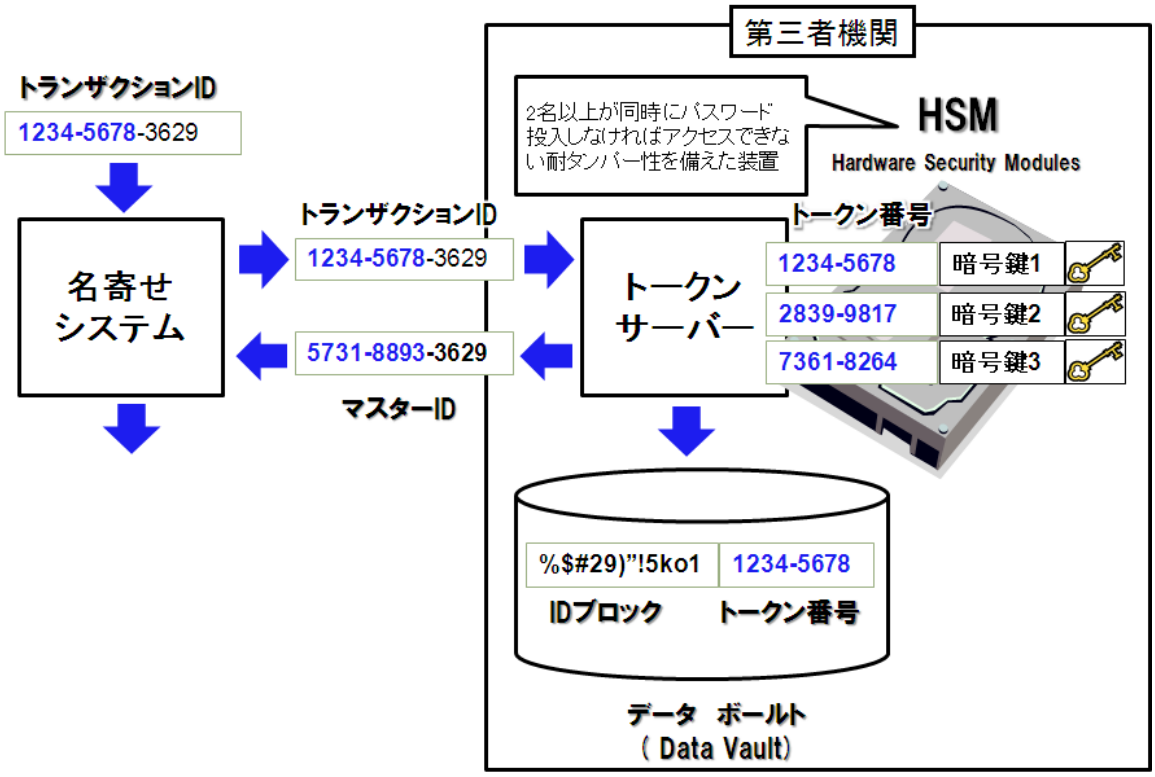


**図6 第三者機関による名寄せコントロール**

### Ⅱ－２ IDによらない名寄せ防止を考慮した情報分散を行うこと

仮にセクトラルモデルが採用されIDによる名寄せが、第三者機関の承認のもとにしか行えない仕組みが構築されたとしても氏名、性別、生年月日、住所、電話番号（携帯電話番号）、メールアドレス、銀行口座番号、送金カード番号（クレジットカード番号等）などを使用すれば名寄せを行うことは不可能ではない。したがって、これらID以外の情報による名寄せの防止を考慮した情報分散を行うことが必要である。特に積極的に国民に情報を発信するプッシュ型の行政サービス（免許の更新時期、未納金の督促、受給資格の通知など）を念頭に置いた場合、メールアドレスの登録は不可欠である。メールアドレスによる名寄せを防止するためには、行政サービスごとに異なるメールアドレス（エイリアス）の登録が必要である。エイリアスの管理は、国が行うのではなく、民間のISP(インターネット接続事業者)等の既存のエイリアス・メールアドレスサービスやオープンIDの仕組みを利活用することで「国（政府)」、「第三者機関」、「民間」という3つの組織間での情報分散が実現する（図7)。

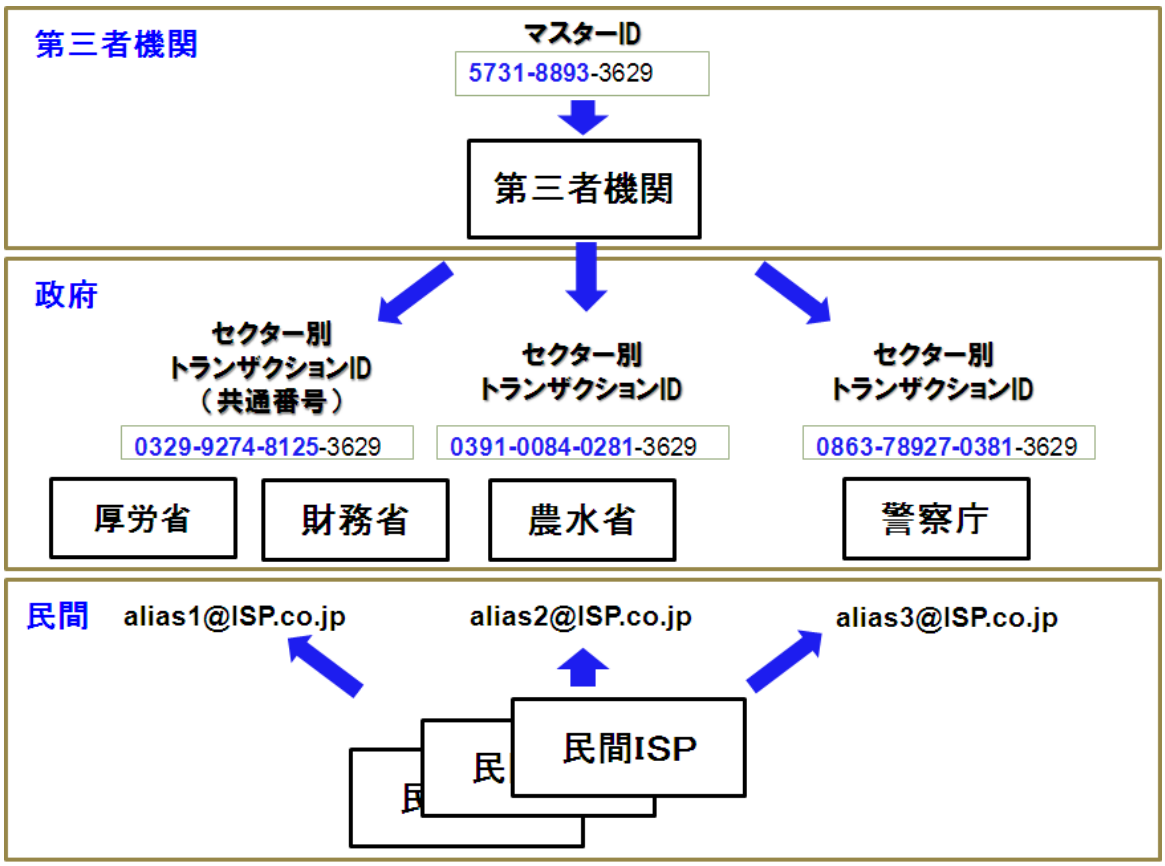


**図7　第三者機関、政府、民間への情報分散**

## Ⅲ　国民 ID は、新たに出現する情報セキュリティの脅威に柔軟に対応できる仕組みであること

### Ⅲ- 1　継続的な事件・事故事例および技術動向の調査を実施すること

コンピュータ処理速度の向上やクラウドコンピューティングの登場は、情報セキュリティに対する従来とは異なった脅威をもたらす。例として、今後懸念される脅威の 1 つにレインボー攻撃が挙げられる。コンピュータの能力の向上は、現行の通信経路の暗号化技術を無力にする恐れがあるだけでなく、一般に広く使用されている固定パスワードに依存した本人認証を無力化し、「成りすまし」を容易にする懸念があるとされている。従来行われてきたパスワードの解析は、特定の ID に対して様々なパスワードを試行してパスワードを探り当てるブルートフォース攻撃（Brute Force Attack/Brute Force Password Cracking）と呼ばれる手法が主流であったが、現在懸念されている新たな脅威は、パスワードを固定し、ID を次から次に変更して ID とパスワードの組み合わせを探り出すリバースタイプのブルートフォース攻撃である。国民 ID のように発行されている ID の数が膨大であればあるほど ID とパスワードが一致する可能性が高まることから、シンガポール政府など ID の利活用が進んでいる国で懸念されている脅威の 1 つである。こうした脅威に対抗するためダイナミック ID やワンタイムパスワードといった動的に ID やパスワードを伝送のたびに異なるデータに変換する技術が主流となりつつある。

情報セキュリティに対する脅威は、技術の進歩によってそのありようが変化する点に特徴がある。変遷する情報セキュリティの脅威に対処し続けるためには、米国をはじめとするID利活用の先進国における犯罪事例を収集し、分析することで常に情報セキュリティの脅威を把握することが重要である。

### Ⅲ- 2　最新動向を踏まえた情報セキュリティ対策の適用と多様性の確保、および法制度を構築すること

最新の脅威を把握したうえで、その脅威に対抗するための技術的対策を常に最新のものとして維持する仕組みが不可欠である。また、1つの技術に依存することは、新たな脅威の出現によって一瞬にして情報セキュリティ対策が無効となる危険性がともなう。したがって何重にも対策を張り巡らせる多層防御（Defense in Depth）の考え方と多様な対策技術の採用が重要である。このことを踏まえ、諸外国の例をそのまま転用するのではなく、最新の技術を盛り込んだ仕組みを構築することが望まれる。

また、国民ID法（仮称）のような根拠法の制定にあたっては、情報セキュリティに配慮して必要以上の情報開示をしないことが重要である。住民票コード番号は、住民基本台帳法施行規則第1条第2号の規定に基づき官報で番号体系が告示（2002年7月25日総務省告示第436号）されており、実在する住民票コード番号を簡単に作り出すことができることからリバースタイプのブルートフォース攻撃を容易に行い得る状況としてしまっている。こうした反省を踏まえ、情報セキュリティの要となるアルゴリズムなどが公開されることがないよう切望する。さらに最新技術を適用しようとした場合に制約を受けることがない法制度として工夫がなされることを期待する。

## Ⅳ　まとめ

紙ベースの業務手続きとWebコンピューティングベースの手続きが混在することは、避けられない。それぞれの手続きに対する情報漏えいや不正利用などの脅威は異なった形で存在する。したがって、想定される個々の脅威に応じた適切な情報セキュリティ対策が実施されることが望まれる。

また、法制度を含む国民ID制度の設計は、システム開発に例えるならば要件定義や外部設計に該当する。したがって、まず、はじめに情報セキュリティやプライバシー保護に対する要件を的確に定義することが重要である。要件定義および外部設計をしっかり行い、実現方式を検討する内部設計フェーズでは、豊富なシステム開発経験者や情報セキュリティに対する知見を備えた専門家を交えた議論が行われることが重要である。

制度と技術の両面から情報セキュリティとプライバシー保護について英知を集めた十分な議論が尽くされ、技術立国としての我が国にふさわしい国民IDシステムが構築されることを期待する。