情報セキュリティとプライバシー保護の観点からの ID に関する提言（素案）

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

JSSM 個人情報保護研究会　ID 検討会
ビジネスアシュアランス株式会社　山崎　文明

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 を悪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状況があり、我が国においても 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、氏名と異なり容易に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との不安がある。また、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、ID は、氏名と異なり、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可能である。

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されたシステム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 つの課題と課題解決のための提言を行う。

課題1　大量の ID の漏えいに備えること
提言　ID 漏えい時の再付番に関する方針を明確にすること
マスターID とトランザクション ID を識別すること
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
情報漏えい被害の極少化を考慮したトランザクション ID を生成すること
課題 2　情報分散を前提としたプライバシー保護の仕組みを構築すること
提言　第三者機関によるデータマッチング・コントロールを可能とすること
ID 以外のデータマッチング（名寄せ）への対処を行うこと
課題 3　変遷する情報セキュリティの脅威に対処すること
提言　継続的な事件・事故事例ならびに技術動向の調査を実施すること
最新動向を踏まえたセキュリティ対策の適用と多様性を確保すること

Ⅰ　大量の ID の漏えいに備えること

Ⅰ－ 1ID 漏えい時の再付番に関する方針を明確にすること

ID の取り扱い方針として、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しておく必要がある。紙媒体を基本にした行政サービスの時代には、数十件、数百件といったわずかな件数の情報漏えいを仮定しておけば十分であったが、電子化された行政システムでの ID の利活用を前提とするならば、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想定しておく必要がある。

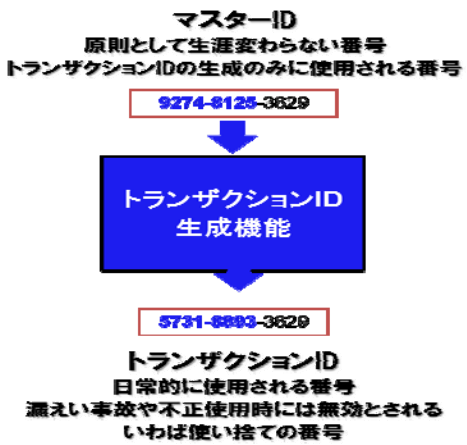
ID が漏えいした際にその不正利用を防止するためには、遅滞なく漏えいした ID を無効と宣言した（revocation）上で、新たな ID を付番することがセキュリティの基本である。

住民票コードは、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

ID の漏えいと漏えい時には再付番を行うことを前提とした場合、マスターID とトランザクション ID の区別が必要である。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、その性質上厳重に管理され、日常の行政サービスに利用されるトランザクション ID の生成にのみ使用される。マスターID は、使途が限定されており、漏えいする可能性が少ない。一方、トランザクション ID は、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性質の ID であり、漏えいが確認された場合には、マスターID から新たに生成される。メールアドレスと同様のいわば使い捨ての ID である。マスターID とトランザクション ID との組み合わせにより、トランザクション ID としての ID が漏えいした際に容易に再付番が行える仕組みが実現する。

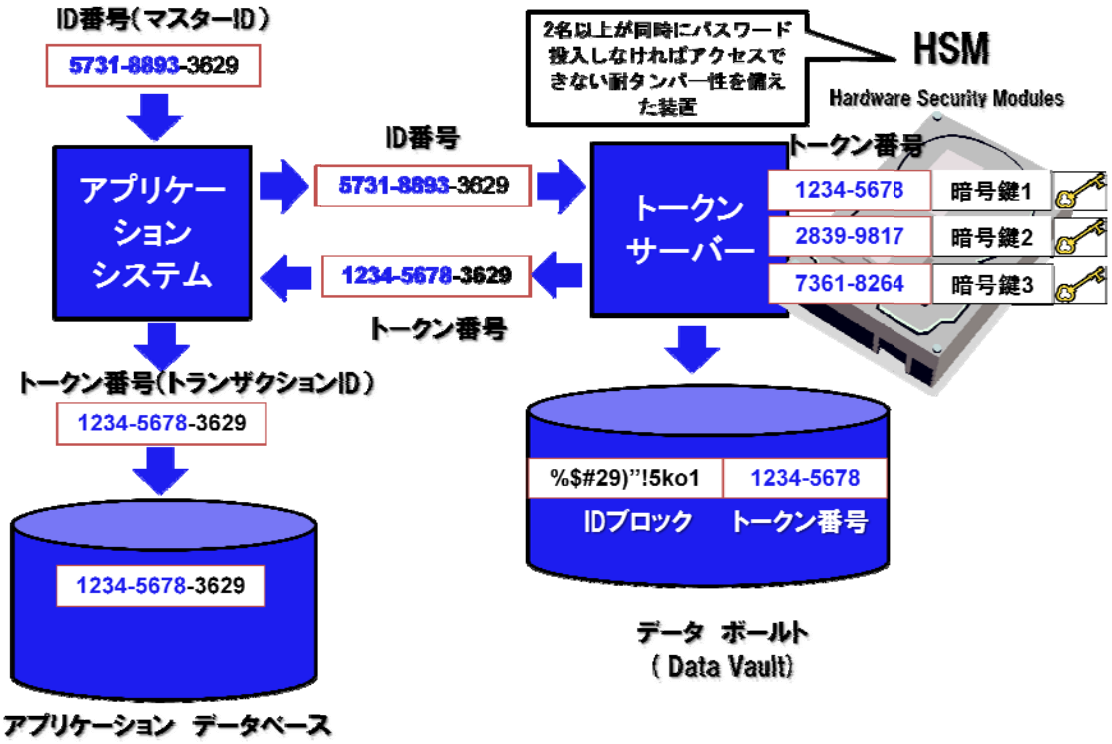
トランザクション ID とマスターID という概念に基づき国民 ID や共通番号の設計を行うとするならば、何をもってマスターID とするかが問われる。



Ⅰ－３　トークナイゼーションを活用したランザクション ID を生成すること

マスターID の秘匿化ならびにトランザクション ID の生成技術としてトークナイゼーション（Tokenization）の活用が考えられる。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」という意味がある。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 は、数学的な復号が行えないため、元の ID を特定することができない。

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 としてのトークンを生成することができる。トークナイゼーションでは、一般に HSM(Hardware Security Module)内で生成した暗号鍵を使用して元の ID(マスターID)を暗号化して保管する。「暗号化されたマスターID（ID ブロックと呼ぶ)」とその ID に対応した「トークン」とともにデータボールト（Data Vault）と呼ばれる高度にセキュリティ対策が施されたドメインに設置されたデータベースに格納し、厳重に管理する。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、格納された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。

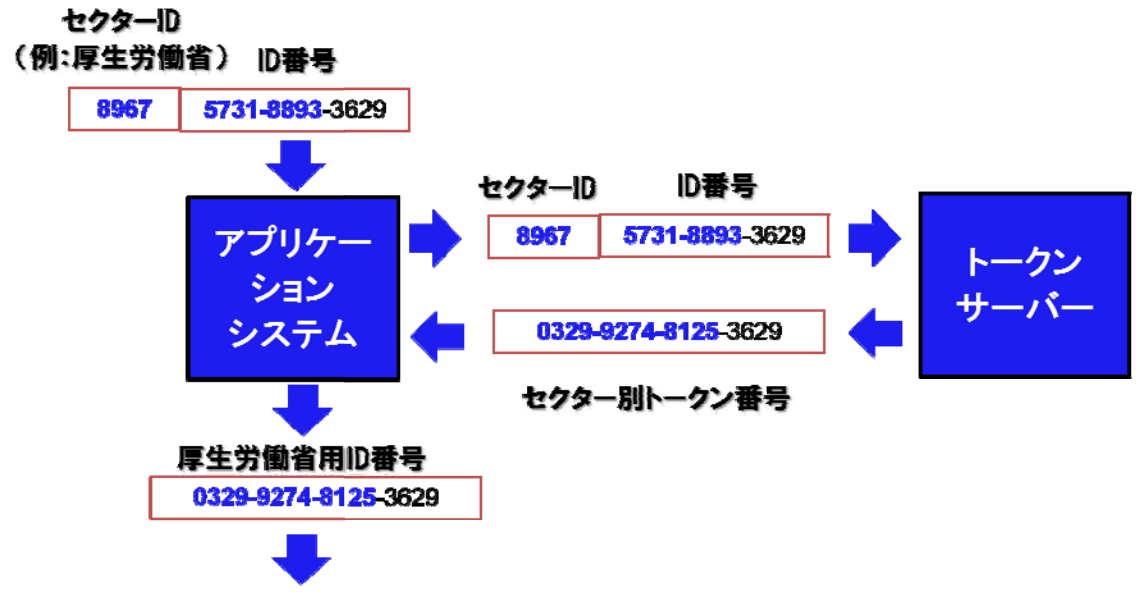


Ⅰ-4　情報漏えい被害の極少化を考慮したトランザクション ID を生成すること

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被害範囲を行政サービス単位や共通番号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番号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。

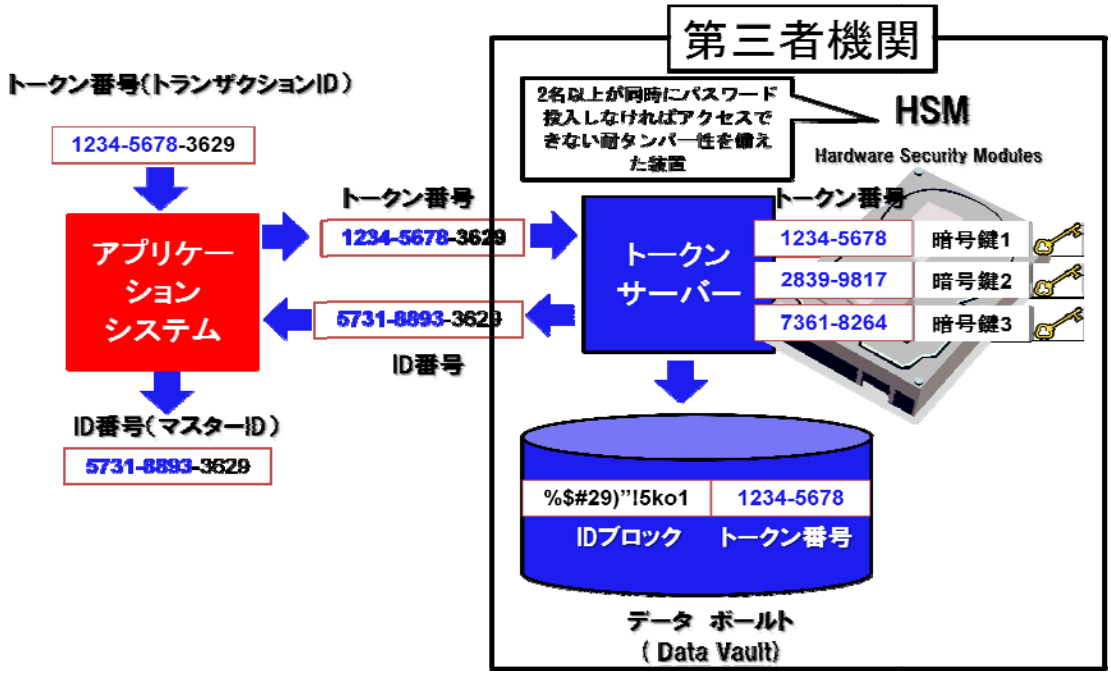
特定のセクターで使用されている ID が漏えいした場合には、当該セクターのセクターID を再付番し、新たに付番されたセクターID とマスターID の組み合わせからトランザクション ID を生成することで再付番が完了する。ID 漏えい被害範囲を極小化するとともに迅速に被害を予防し、回復するという観点からの方式設計が期待される。



Ⅱ　情報分散を前提としたプライバシー保護の仕組みを構築すること

Ⅱ－１第三者機関によるデータマッチング・コントロールを可能とすること

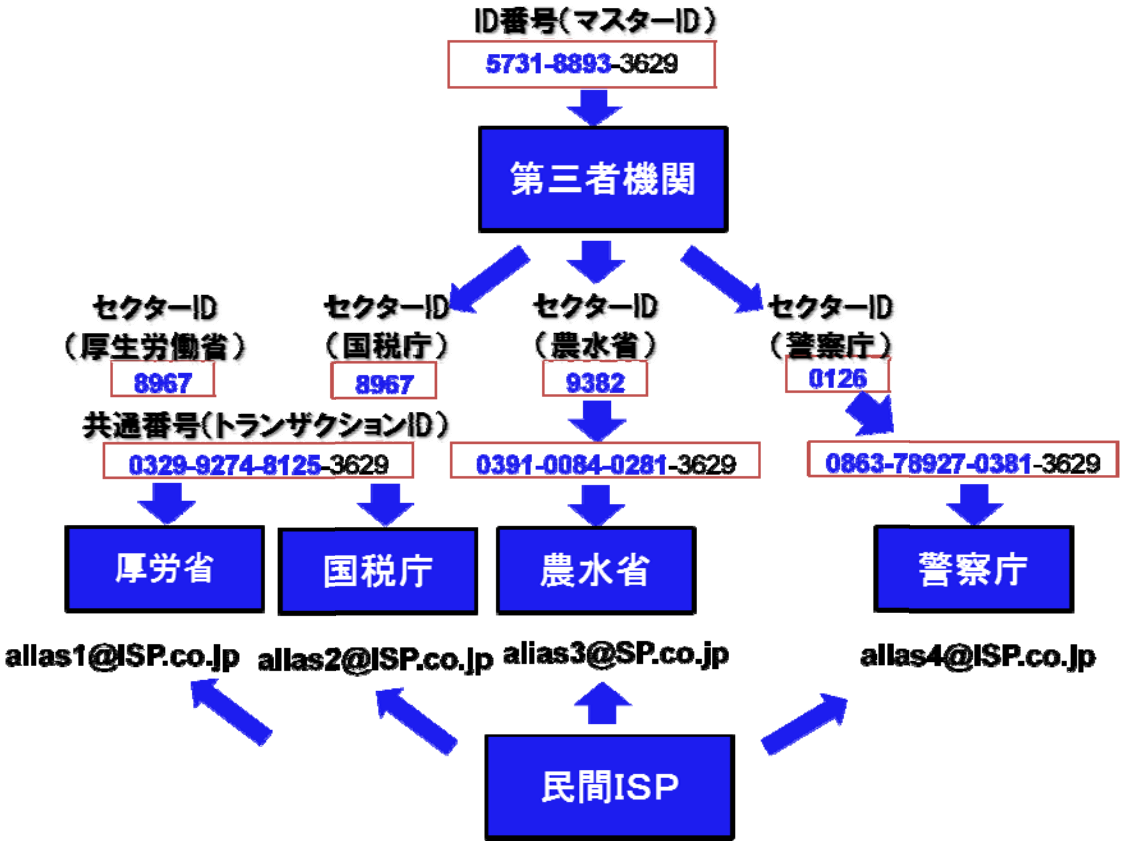
トークナイゼーションを行って生成されたトランザクション ID は、トークナイゼーションされる前の状態（マスターID）に戻すことでデータマッチング（名寄せ）が可能となる。トークナイゼーションされた ID を元のマスターID に戻すためには、データボールトのデータと HSM 内に格納された暗号鍵が必要になる。したがって、データボールトと HSM、もしくは HSM のアクセス権を有効にするパスワードを第三者機関が管理することで許可されないデータマッチングを防止することができる。



Ⅱ－２　ID 以外のデータマッチング（名寄せ）への対処を行うこと

仮にセクトラル方式が採用され 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が可能である。

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 事業者等のサービスを利用することで「国（政府）」、「第三者機関」、「民間」という 3 つの組織間での秘密分散が実現する。



Ⅲ　変遷する情報セキュリティの脅威への対処

Ⅲ- 1　継続的な事件･事故事例ならびに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、従来とは異なったセキュリティ上の脅威をもたらす。例として、今後懸念される脅威の一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ア攻撃（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アタックである。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一つである。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。

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セキュリティ対策の適用と多様性を確保すること

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のが望ましい。

Ⅳ　まとめ

ユビキタスな社会インフラが整うまで、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セキュリティ対策が実施されることが望まれる。

また、ID制度の制度設計は、システム開発に例えるならば外部設計や要件定義に該当する。したがって、セキュリティやプライバシー保護に対する要件を、まず、はじめに定義することが重要である。外部設計としての要件定義をしっかり行い、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相応しいIDシステムが構築されることを期待する。