

堀部政男情報法研究会 連続シンポジウム第3回

国民IDとシステムとしての課題

—プライバシーの保護と利便性の両立を目指して—

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

2010年12月9日(日)

山崎 文明

ビジネスアシュアランス株式会社 代表取締役

発表の背景

日本セキュリティ・マネジメント学会

JSSM : Japan Society of Security Management

日本学術会議 協力学術研究団体

会長 佐々木 良一 (東京電機大学 教授)



「将来を見据えた国民ID構築のための提言」

2010年6月26日 JSSM全国大会にて発表

個人情報保護研究会国民IDのあり方検討WG

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

1. IDと名前 その特性を理解する
2. 大量の国民IDの漏えいへの備え
3. 情報分散を前提としたプライバシー保護の仕組み
4. 変遷する情報セキュリティの脅威への対処
5. おわりに

導入の趣旨

背景

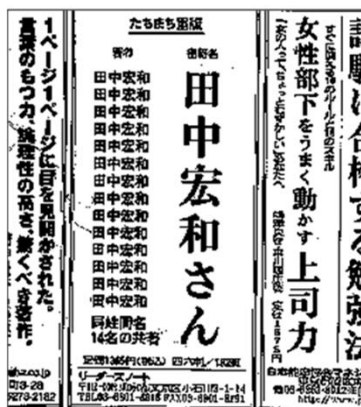
- 少子高齢化（高齢者の増加と労働力人口の減少）
- 格差拡大への不安
- 情報通信技術の進歩
- 制度・運営の効率性、透明性の向上への要請
- 負担や給付の公平性確保への要請

現在

課題

- 所得の把握や制度をまたがった事務を行う場合などにおいて、複数の機関に存在する個人の情報を同一人の情報であるということの確認を行うための基盤がないため、
- 税務署に提出される法定調書のうち、名寄せが困難なものについては活用に限界
 - より正確な所得・資産の把握に基づく柔軟できめ細やかな社会保障制度・税額控除制度の導入が難しい
 - 長期間にわたって個人を特定する必要がある制度の適正な運営が難しい（年金記録の管理等）
 - 医療保険などにおいて関係機関同士の連携が非効率
 - 養子縁組による氏名変更を濫用された場合に個人の特定が難しい 等

Business Associates Co., Ltd. **名前だけでは個人が特定できない現実**



Copyright ©2010 Fumiaki Yamasaki

5

Business Associates Co., Ltd. **ID盗用が直接の被害に結び付くサイバー空間**

多目的に利用されてしまった米国SSN

- 携帯電話の契約 アパートの賃貸契約、クレジットカードの申し込み、ゴルフ場の予約・・・

- 自分のID不正利用監視に毎月\$10

多目的に利用されてしまった韓国住民登録番号

- サイト会員登録、レンタルビデオ会員登録、・・・



Copyright ©2010 Fumiaki Yamasaki

6

Business Assurance
Co., Ltd.

ID盗用が直接の被害に結び付くサイバー空間

重要なお知らせ
【重要】ワンタイムパスワードシステム

MK-STYLEをお気に入り登録する

オンラインゲームポータル
MK-STYLE

[ニュース](#) / [初めての方へ](#) / [ショップ](#) / [サポート](#)
NEWS / BEGINNER'S GUIDE / SHOP / SUPPORT

[ニュース](#)

[TOPに飛ぶ](#)

ログイン MEMBER LOGIN

ゲストさん、ようこそ！

MK-ID

パスワード

ワンタイムパスワード

ワンタイムパスワードを利用中の方のみご入力下さい。

入力時、大文字、小文字にご注意ください。

MK-IDでログイン

MK-IDのパスワードを忘れた方

MK-ID新規会員登録

Yahoo! JAPAN ID でログイン

※現在ご利用のみで利用できます

ワンタイムパスワードを使う！

アカウント盗用被害にあわないために

お知らせ・不具合情報

お知らせ・不具合情報

日付	タイトル
2010-12-15	【重要】ID・パスワードの管理について

平素はMK-STYLEをご利用いただきありがとうございます。

以前よりMK-STYLEのお知らせにて注意を促しておりますが、インターネットサービス全体で、ID・パスワードの不正使用によるアカウントの盗用被害が多く発生しております。

他のインターネットサービスと同じID・パスワードを使用されている場合に被害に遭遇するケースが非常に多くなっております。

MK-STYLEにおいて、他のインターネットサービスと同じID・パスワードを設定されている場合は、変更いただきますようお願い申し上げます。

他企業側にて情報流出事故があったため、他のインターネットサービスと同じID・パスワードを使用されている場合、アカウントの盗用被害に遭う危険性が非常に高まります。

他のインターネットサービスと同じID・パスワードは絶対に使用しないでください。

※第三者にわかりやすいパスワードの設定は非常に危険です※

Copyright ©2010 Fumiaki Yamasaki
7

Business Assurance
Co., Ltd.

IDと名前

名前

名前だけでは名寄せが困難

- 同姓同名、同一誕生日

名前だけの不正行為は困難

名前は本人にとって唯一のもの

名前の変更は人生問題

ID

IDだけで名寄せが可能

- 本人が多目的に利用する可能性がある(本人による目的外利用)
- 漏えいした場合、名寄せに利用される

IDだけで成り済まされるID盗用犯罪

IDは容易に変更することができる

IDは目的に応じて作成できる

IDはIDから作り出すことができる

- マスターIDとトランザクションID
- 動的ID(Dynamic ID)

共通するのは

サイバー空間上に流出したIDや名前は永久に消去できないという事実

Copyright ©2010 Fumiaki Yamasaki
8

4

マスターIDとトランザクションIDの識別

想定される脅威に応じたID設計

- 書類ベースの手続きとインターネットを使用した手続きが向かい合う脅威が異なる
- 書類ベースの情報漏えいとインターネット経由の情報漏えいは規模や影響範囲が大きく異なる
- インターネットIDに不可欠な「使い捨てID」
韓国i-PIN (internet Personal Identification)

住基ネットを活用した新たな番号

平成22年12月3日
社会保障・税に関わる番号制度に関する実務検討会 中間整理（案）
概要 資料1

マスターID
原則として生涯変わらない番号
トランザクションIDの生成のみに使用される番号

5731-8893-3629

↓

**トランザクションID
生成機能**

↓

9274-8125-3629

トランザクションID
日常的に使用される番号
漏えい事故や不正使用時には無効とされる
いわば使い捨てのID

Copyright ©2010 Fumiaki Yamasaki

Layered Defenses と Tokenization

Layered Defenses

Data Security

Encryption
Information Masking
Truncation
Tokenization

トークン(Token)

(地下鉄・バスなどの)代用貨幣、代用硬貨
意味のない数列、
元の数と数学的関連性がない数列

データセキュリティへの応用

Copyright ©2010 Fumiaki Yamasaki

10

Data Security Architecture

Encryption (暗号化)

- データ長とデータタイプが変わってしまうことからシステムに大きな影響が出る
- CPUに対する負荷が大きい
- 復号化リスクがつきまとう

4628-\$ 6&#~'kr0-3629

Information Masking / Hash / Truncation (切り捨て)

- 元のデータに回復できない

4628-XXXX-XXXX-3629

Tokenization (トークン化)

- アプリケーションシステムへの影響は極少
- CPUに対する負荷が小さい
- 復号化リスクがない

4628-1234-5678-3629

トランザクションIDの生成

ID番号(マスターID)

5731-8893-3629

アプリケーション
システム

ID番号

5731-8893-3629

トークン番号

トークン番号(トランザクションID)

1234-5678-3629

1234-5678-3629

アプリケーション データベース

2名以上が同時にパスワード
投入しなければアクセスできな
い耐タンパー性を備えた装置

HSM

Hardware Security Modules

トークン番号

1234-5678

暗号鍵1

2839-9817

暗号鍵2

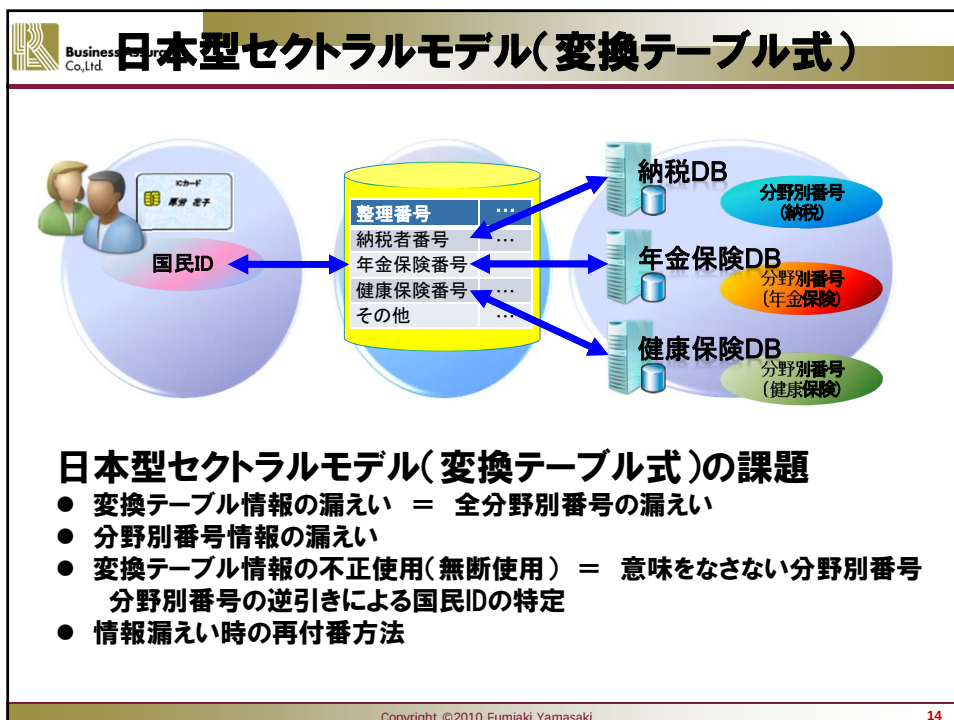
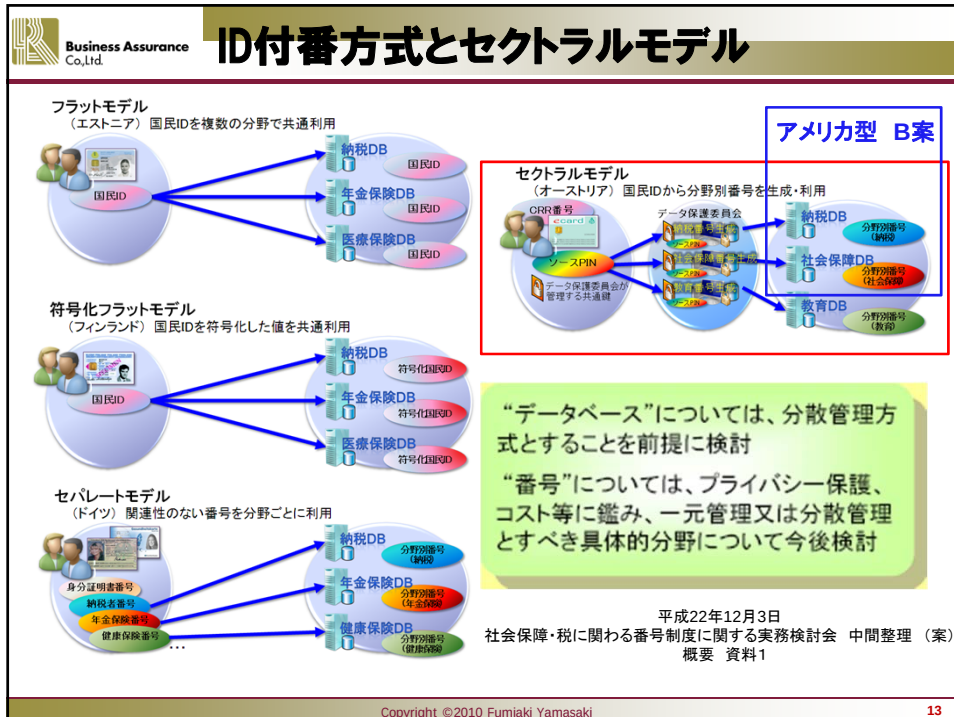
7361-8264

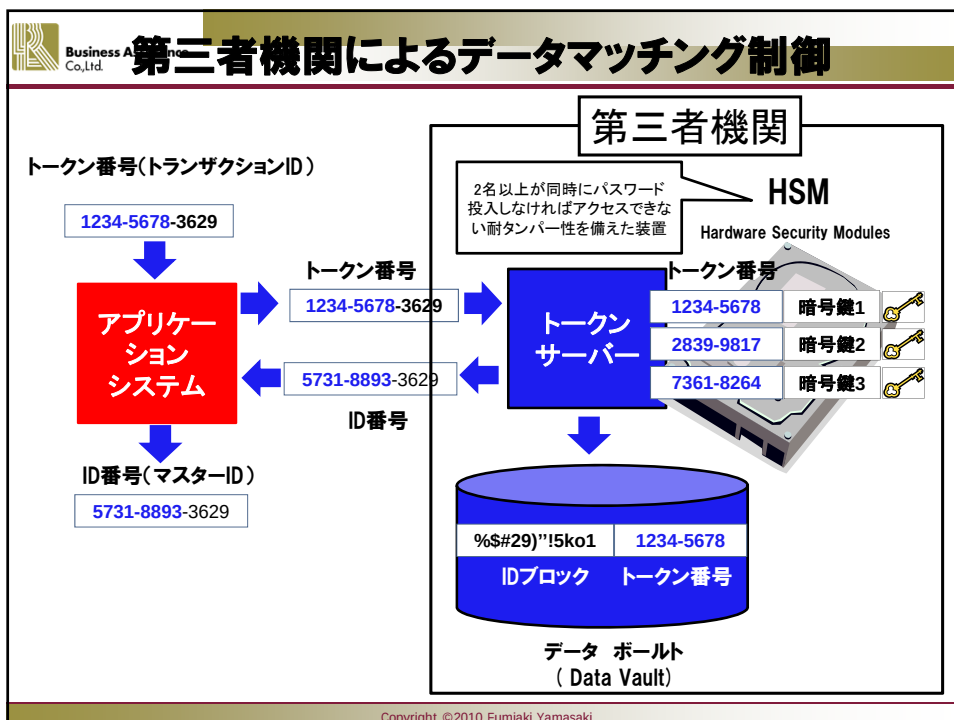
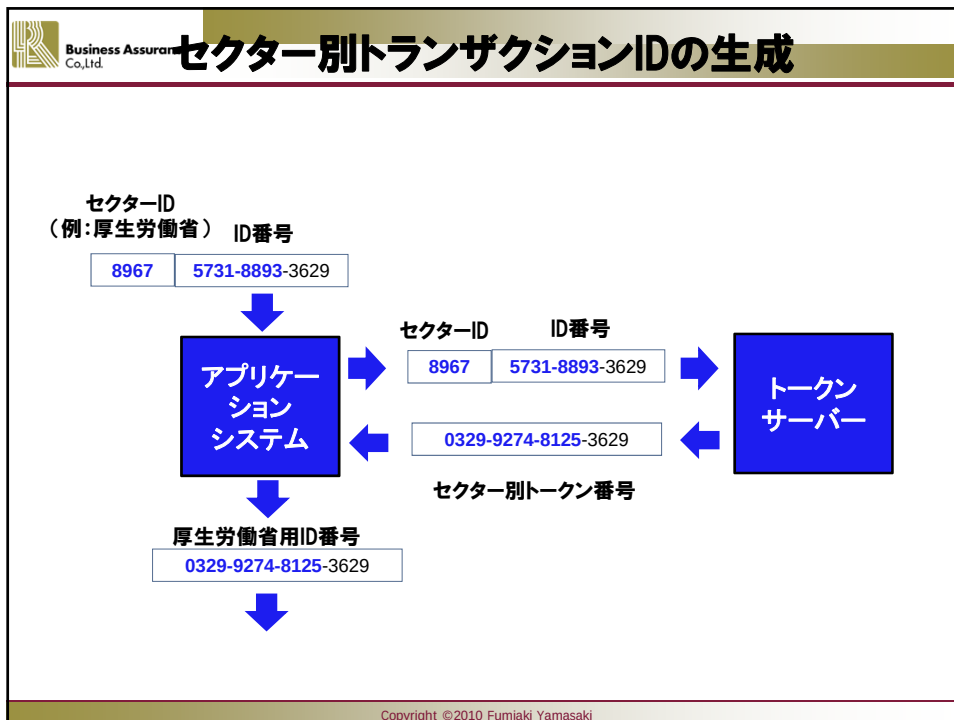
暗号鍵3

トークン番号

%\$#29)!5ko1 1234-5678
IDブロック トークン番号

データ ボールト
(Data Vault)





Business Alliance Co., Ltd. 国民ID以外のデータマッチングへの対処

国民ID以外のマッチング(名寄せ)キー

- 氏名、性別、生年月日、住所、電話番号(携帯電話番号)、メールアドレス等
- プッシュ型の行政サービスに不可欠なメールアドレス

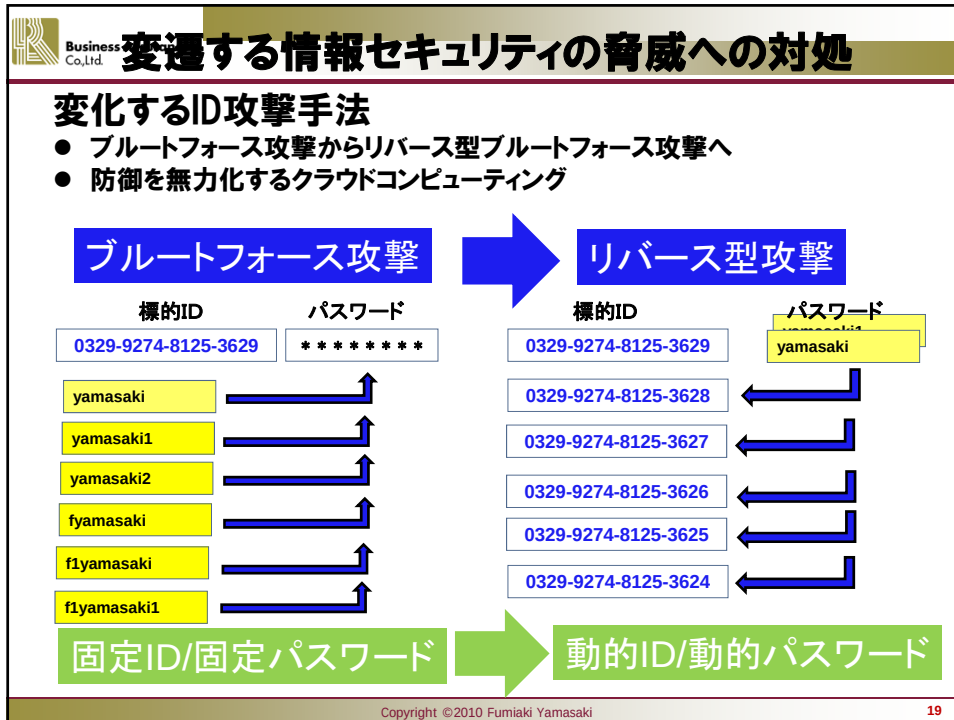
Copyright ©2010 Fumiaki Yamasaki 17

Business Alliance Co., Ltd. 政府、第三者機関、民間に跨る分散管理方式

“データベース”については、分散管理方式とすることを前提に検討
 “番号”については、プライバシー保護、コスト等に鑑み、一元管理又は分散管理とすべき具体的分野について今後検討

平成22年12月3日
 社会保障・税に関わる番号制度に関する実務検討会
 中間整理 (案) 概要 資料1

Copyright ©2010 Fumiaki Yamasaki



Business Assurance Co., Ltd. **まとめ**

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・事事故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

Copyright ©2010 Fumiaki Yamasaki 20

国民IDの構築は

- 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

自己紹介



価格：2,940円
判型：B5変形判/247ページ
ISBN：4-8222-5223-5
発行：日経BP社
発売：日経BP出版センター
2008年4月14日発行



ADR: Alternative Dispute Resolution
「裁判外紛争解決手続の利用の促進に関する法律」

山崎 文明(やまさき ふみあき)
PCI SSC PO Japan 連絡会 会長
ビジネスアシュアランス株式会社 代表取締役社長
ネットワンシステムズ株式会社フェロー
IT-ADRセンター 専門ADR委員

システム監査技術者(経済産業省)/医療情報技師
英国規格協会 BS7799情報セキュリティ・スペシャリスト
システム監査、ネットワークセキュリティ、セキュリティポリシーに関する専門家。大手
会計監査法人にてシステム監査に永年従事。

【各種委員会委員就任加盟歴】

内閣官房 安全保障危機管理室 情報セキュリティ対策推進室WG委員

警察庁不正アクセス犯罪等対策専科講師

学校セキュリティ検討委員会委員

経済産業省サイバーテロ実験評価委員

警察庁不正プログラム調査研究委員会委員

警察庁サイバーセキュリティ調査研究委員会委員 他

【加盟学会】

警察政策学会正会員

日本安全保障・危機管理学会正会員

日本セキュリティ・マネジメント学会正会員

【著書】

「PCIデータセキュリティ基準 完全対策」(日経BP社)

「すべてわかる個人情報保護」(日経BP社)、「情報セキュリティハンドブック」(オーム社)、「情報セキュリティと個人情報保護 完全対策」(日経BP社)、「システム

監査の方法」(中央経済社)、「コンティンジェンシー・プランニング」(日経BP社)、「

セキュリティマネジメント・ハンドブック」(日刊工業新聞社)等。



ビジネスアシュアランス株式会社

お問い合わせ先

E-mail: toiawase@biz-assure.co.jp

電話: 03-5462-0698 (代表)