ＪＳＳＭ　個人情報の保護研究会

第４回　「情報セキュリティの日」研究報告　　２０１０年2月２０日

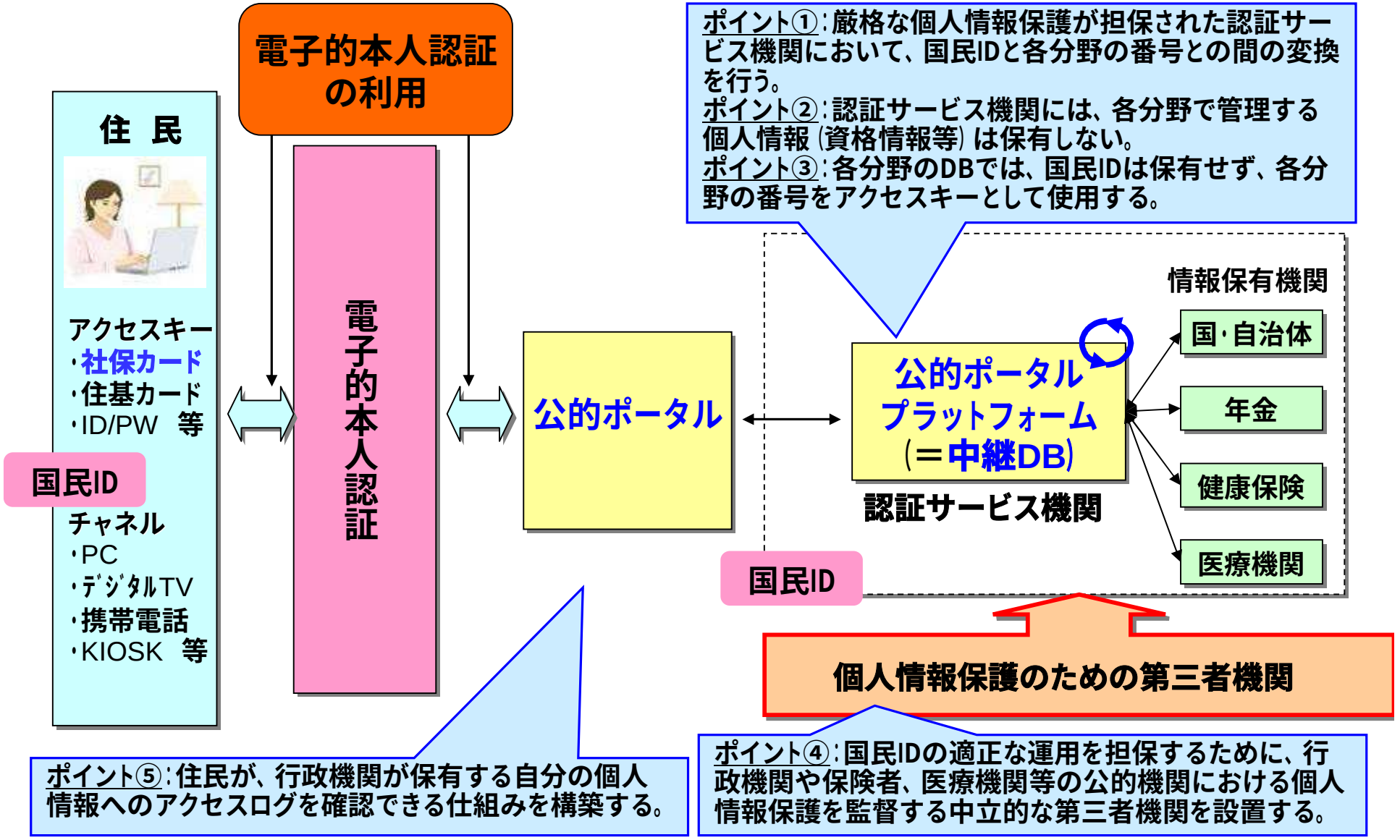
本人認証基盤の現状と課題
～クラウドコンピューティング時代を迎えて～

電子的本人認証の検討会
発表者　鵜野幸一郎（日本セキュアテック研究所）

説明順序

1. 国民的な課題：本人認証とID
2. クラウドの例　～自治体クラウド～
3. クラウドコンピューティングにおけるパスワード問題とは
   - 3-1 トークンの安全対策基準：パスワードは原則共通必須項目
   - 3-2 パスワードの悩みは世界共通
4. パスワード問題　本人認証を基礎から考える
   - 4-1 歴史鳥瞰
   - 4-2 本人認証の実行のために必要な構成要素
   - 4-3 哲学的考察
   - 4-4 心理学的考察
   - 4-5 社会工学的考察
5. 電子的本人認証技術総覧
6. 本人？　正規のユーザ？
7. 電子的本人認証基盤の課題

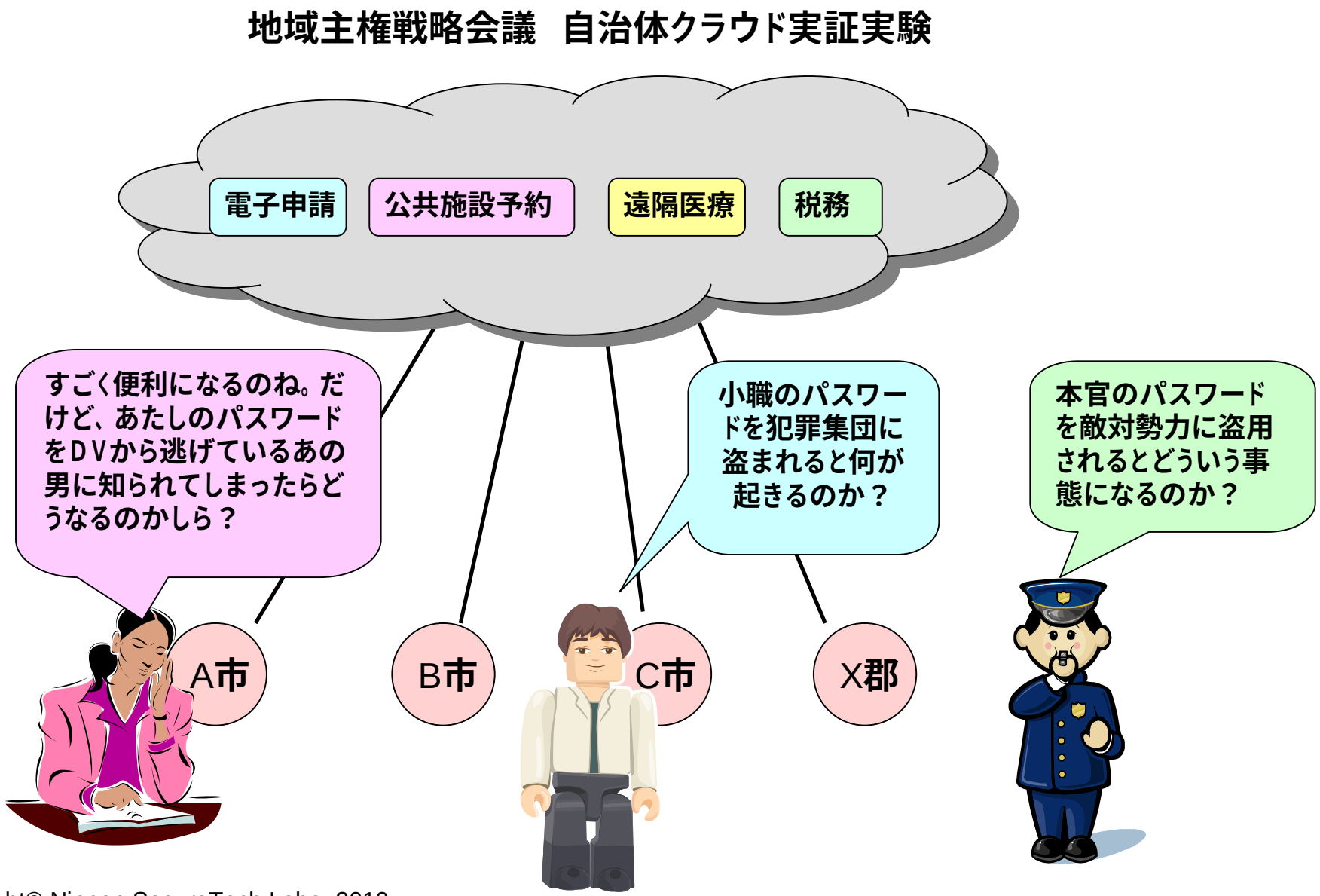
1．国民的な課題： IDと本人認証



出典：JSSM第２３回全国大会研究報告書 「次世代電子行政サービスの安全運用を支える本人認証基盤の確立に向けて」

Copyright© Institute for International Socio-Economic Studies. 2009

2．クラウドの例　～自治体クラウド～



Copyright© Nippon SecureTech Labo. 2010

3．クラウドコンピューティングにおけるパスワード問題とは

3－1　トークンの安全対策基準：パスワードは原則共通必須項目

（電子政府ガイドライン作成検討会　セキュリティ分科会発信のオンライン手続きにおけるリスク評価及び電子署名・認証ガイドラインによる定義）

トークンとは？

1．認証の対象者が認証情報を保持するための格納媒体である

2．認証要求者が所有し管理する何かであり、認証情報等の認証に用いる情報を格納または出力するハードウェア、あるいは知識等の認証情報そのもの　（パスワード等）等がある

トークンの対策基準にて、レベル1からレベル4まで全てパスワードは共通必須項目

（但し、パスワードなしトークンをレベル2で例示）

保証レベル	トークンの対策基準の実例
レベル1 低	パスワード（5桁以上）　PIN　事前登録知識の確認など
レベル2	パスワード（6桁以上）　PIN　事前登録知識の確認など　/　トークン
レベル3	パスワード ＋ トークン
レベル4 高	パスワード ＋ 耐タンパ性を有するハードウェアトークン

Copyright© Nippon SecureTech Labo. 2010

3－2　パスワードの悩みは世界共通

パスワード　覚えきれない　　本人認証の課題のNo.1

日経新聞　2009年10月27日　記事

1. 暗証番号を要求するカード

   キャシュカード　クレジットカード

2. 暗証番号を要求するネットの世界

   登録制サイト　ネット銀行　ネットショッピング　オークションサイト

自分のIDでログインするサイト数「ほぼ毎日使うサイト」「たまに使うサイト」を合わせると、　　平均13．4個

ネットで使うパスワードをわすれたことがある　　9割

利用者がメリットを感じにくい暗証番号　⇒　運転免許証　4桁暗証番号を2種

ほぼ誰でも暗証番号を忘れてしまう悲喜劇的システム(*1)

(*1) 参考：http://b-spiral.tea-nifty.com/blog/2008/03/post_8a04.html

Copyright© Nippon SecureTech Labo. 2010

パスワードの悩みは世界共通　1

米国のTechCrunch記事から　（2009年7月19日）

『ウェブ・サイトのトップページを一瞥しただけで、われわれのデジタル・ライフの管理が容易ではないということが分かる。

「パスワードを忘れたら」、「ユーザー名を忘れたら」、「ログインを続ける」、「IDを忘れたら」、「私は誰だったっけ？」といった表示がいたるところに見られる。

われわれはたった4桁の暗証番号を覚えるのにも苦労している。こうしたユーザーを相手にするウェブサービスのセキュリティーシステムは妥協の塊にならざるをえない。

ユーザーはそれぞれのアカウントごとに異なるまったくランダムな文字列などとうてい記憶できるものではない。こうして個別に見れば理屈ではそこそこ安全なサービスも、ユーザーがすべてのアカウントに同じパスワードを使い始めることによって安全性はたちまち危殆に瀕することになる。』

http://jp.techcrunch.com/archives/20090719the-anatomy-of-the-twitter-attack/

http://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/（原文）

Copyright© Nippon SecureTech Labo. 2010

パスワードの悩みは世界共通　2

朝日新聞ニュース（2010年1月22日）

「123」「abc」…安易なパスワード、5人に1人：　電子メールやオンラインショッピングを利用したりするときに入力するパスワードとして、5人に1人が「123456」とか「Password」といった安易なものを使っており、アカウントが乗っ取られる危険があることがわかった。米コンピューター・セキュリティー企業インパーバが21日、発表した。

同社は、写真投稿などのサイトrockyou.comに侵入したハッカーが利用者3200万人分のパスワードをネット上に公開するという事件が昨年12月に起きたため、分析した。その結果、利用者の20%が、名前や辞書に載っている言葉、連続した数字の羅列など、思いつきやすいパスワードを使っていた。最多は「123456」で、ほぼ110人に1人が使用。「iloveyou」「abc123」なども多かった。キーボードの字を左から順に打った「Qwerty」も20位に入った。

ハッカーは、パスワードを当てずっぽうで自動生成して高速入力するプログラムを使い、アカウントを乗っ取ろうとするが、安易なパスワードを候補に使えば、「当たり」の確率が飛躍的に上がる。同社は、現代の通信環境とコンピューターの能力から、ハッカーがその気になれば、毎秒1回のペースで乗っ取りが可能と指摘。例えば「This little piggy went to market」という文の単語の頭文字などから「tlpWENT2m」とするなど、ハッカーが想像しにくいパスワードを使うよう強く勧めている。

http://www.asahi.com/national/update/0122/TKY201001220267.html

http://www.imperva.com/news/press/2010/01_21_Imperva_Releases_Detailed_Analysis_of_32_Million_Passwords.html

Copyright© Nippon SecureTech Labo. 2010

本当に厄介なパスワードの悩み

簡単に覚えられるパスワードは簡単に破られる。

破られない長大な難解パスワードを3組以上も覚えられる人は稀。

「This little piggy went to market」という意味のある文章から作ったものであっても「tlpWENT2m」のようなもの文字列をIDと一緒に何組も覚え続けていられる人は多くない。

キャッシュカードの暗証番号を携帯電話や他の用途にも使い回すのは銀行の基準では過失に準ずる扱い。

頻繁に変更を要求されるとメモ/手帳への依存しか選択肢がない。

ところが、

屋外でのパスワード記載メモ/手帳の携帯は銀行の基準では【過失】

Copyright© Nippon SecureTech Labo. 2010

実は大きなパスワード運用コスト

文字パスワードシステムの調達コストは無料で導入コストも非常に安い

しかし

強固なパスワードを強制、更に頻繁な変更も実施すると

失念・混乱によるヘルプデスク・再発行の費用が発生する

ヘルプデスク・再発行の費用を抑制するには

メモ / 手帳依存を許可 / 黙認する（セキュリティ犠牲）
あるいは
簡単に破られる脆弱パスワードを許可/黙認する（セキュリティ犠牲）

Copyright© Nippon SecureTech Labo. 2010

4．　パスワード問題　本人認証を基礎から考える

4－1　歴史鳥瞰

4－2　本人認証の実行のために必要な構成要素

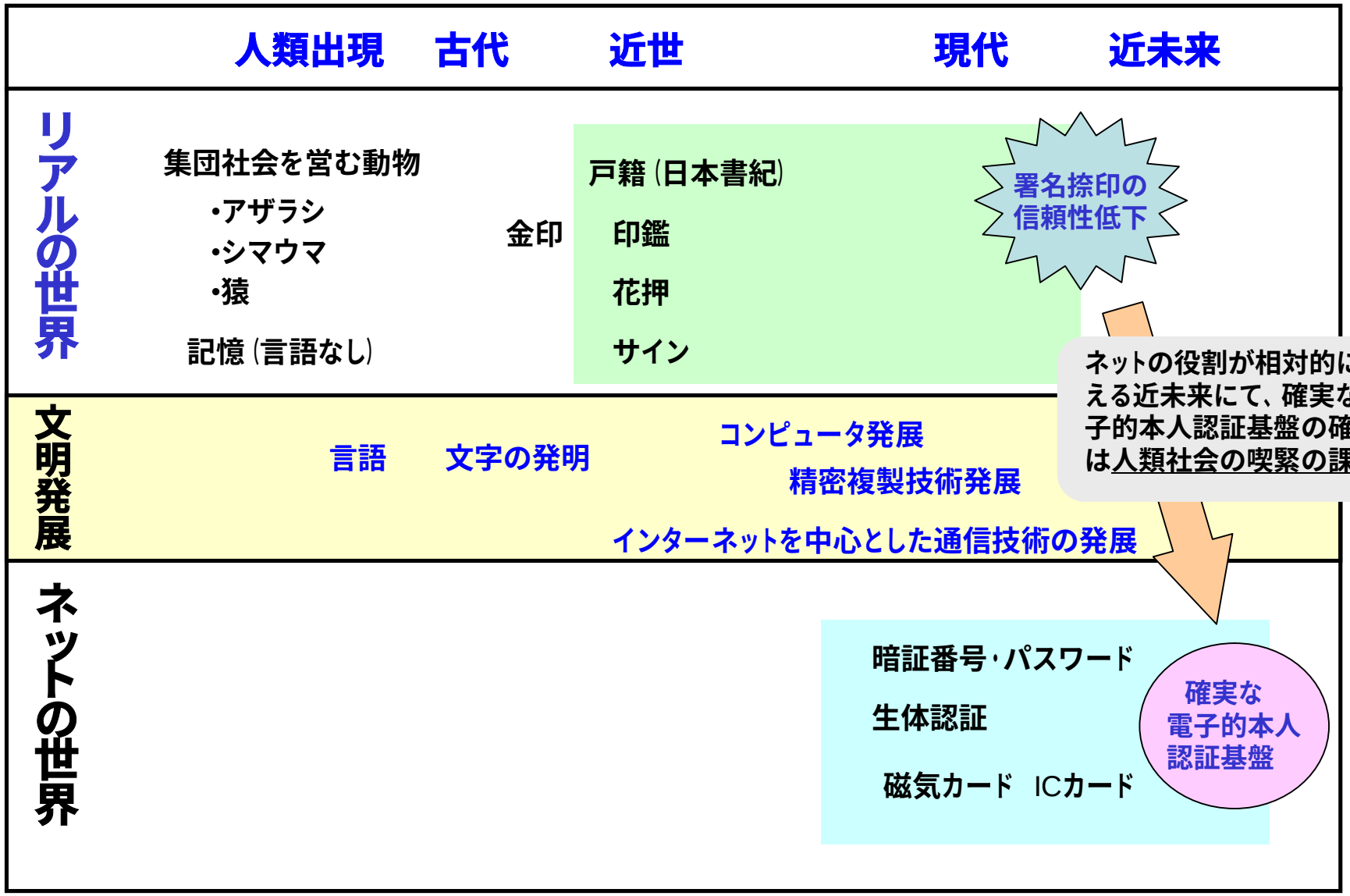
4－3　哲学的考察

4－4　心理学的考察

4－5　社会工学的考察

Copyright© Nippon SecureTech Labo. 2010

4－1 本人認証を基礎から考える 歴史鳥瞰



精密複製技術の発展により印影や手書きサインを含む重要文書の複製が近年容易になっている

Copyright© Nippon SecureTech Labo. 2010

4－2　本人認証を基礎から考える本人認証の実行のために必要な構成要素

：認証する人の介在が必須

：認証する人の不介在が許されている

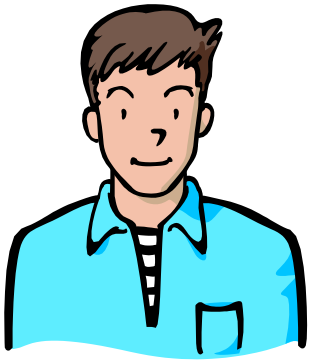
	登録	発行･管理	トークン保有	本人認証プロセス
文字以前	親が子･嫁を酋長へ紹介	祭で面通し、祭りの最中に腕にイレズミ	イレズミ 	イレズミが彫られた手･腕の検視
アナログ時代（署名捺印）	役所にて戸籍確認印鑑登録	役所にて印鑑証明発行	登録済印鑑保有 	印鑑証明書添付つき押印済印影を検視
デジタル時代	認証対象者の身元確認	身元確認の結果に基づいて認証情報･トークンの発行	格納媒体 ･記憶 ･生体 ･所有物	身元識別情報との同一性を検証

Copyright© Nippon SecureTech Labo. 2010

4－3 本人認証を基礎から考える 哲学的考察

人間とは？　本人を本人と確実に認証するとは？

本人　＝　正規のユーザ



悪意も善意も同時にもつことができるやっかいな生き物：人間

本人認証とは、権利や義務の主体確定プロセス

- 本人認証
- 個人識別
- 本人確認
- 本人証明
- 認可
- Identification
- Certification
- Authentication
- Authorization
- この人は誰ですか
- おれはオレに相違ない

Copyright© Nippon SecureTech Labo. 2010

【本人認証】

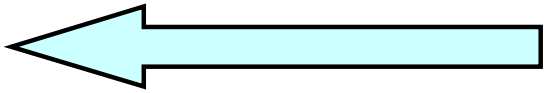
当事者ですか？
(Is he/she the person who claims to be?)

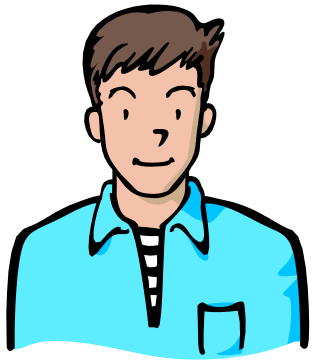
本人認証は当人が死亡していても意識不明であっても実行できてしまえるものでないことが望ましい

本人の頭脳
(本人の記憶と意思)

コンピュータのCPU
(機械の記憶と意思)

私は鈴木であると主張(自称)します。
その証拠としてパスワードを入力します

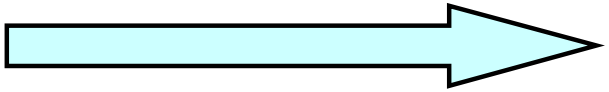




記憶照合

あなたを鈴木と認めます。なぜなら
パスワードを正しく入力したから

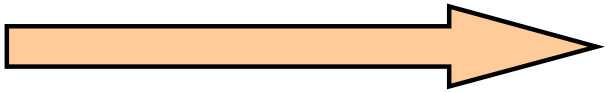
YES



Yes/No

NO

あなたは鈴木と認めることはできません
なぜならパスワードが誤りだから



YES/NOしかない

権利義務の主体確定プロセスである本人認証は、当人の意思的行為を以て成立

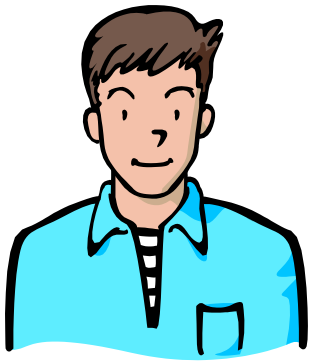
Copyright© Nippon SecureTech Labo. 2010

因みに、本人確認のもう一つの構成要素である個人識別については

【個人識別】　**この人は誰ですか？**
(Who is this person?)

コンピュータのCPU
(機械の記憶と意思)

この人は誰ですか？
・指紋をチェックします
(あるいは)
・社員証をチェックします



生体照合　所有物照合

本人認証は当人が死亡していても意識不明であっても実行できてしまえるものでないことが望ましいが、個人識別はあえて実行できる

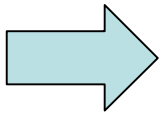
生体照合や所有物照合だけでは本人の意思の有無の確認をできない
悪意側からのなりすまし、複写、模倣、窃盗等の攻撃対応という課題あり

Copyright© Nippon SecureTech Labo. 2010

４－４　本人認証を基礎から考える　本人認証の心理学的考察

パニックや興奮状態でもリアルの相手との対面等では可能な本人認証だが、
相手が見えないネット環境での電子的本人認証は、より困難が予想される。

1. **激しい怒りや悲しみの最中**
2. **緊張で心が張り詰めた中**
3. **激しい運動の後**
4. **上司や顧客の叱責の渦中**
5. **病いの状況にて（腹痛、頭痛、・・・）**
6. **戦場における攻防の中　等**



常態でない心理状態に耐える電子的本人認証

Copyright© Nippon SecureTech Labo. 2010

４－５　本人認証を基礎から考える　本人認証の社会工学的考察

人	大人 子供 高齢者 障害者 悪意の人	•高齢者でもストレスなく本人認証できること •障害者でも容易に本人認証プロセスができること •不正使用者の排除が強力なこと
環境条件	屋内･屋外 宇宙･深海 高熱･厳寒 騒音･静寂 手袋　ゴーグル着用 手足拘束	•屋外で本人認証プロセスができること •高温多湿、厳寒強風でもできること •手袋、ゴーグル着用でもできること
悪意側のプロセス	嘘 脅迫　恐喝 賄賂 フィッシング＋マルウェア	•フィシング詐欺の対策が可能なこと •キーロガーなどのマルウェアを無効化できること •本人認証の権限を分散できること
対象物･情報	国家機密情報 個人機微情報 ログ･認証情報	•運用管理者の悪意･裏切りに耐えること •ビッグブラザーに対抗できること

Copyright© Nippon SecureTech Labo. 2010

5．電子的本人認証技術総覧

☆ 本人を認証する方式

記憶認証

- パスワード
- マトリックス
- 画像
- 対話型

短期記憶と長期記憶

記憶の再生と対象の再認

所有物認証

- ICカード･磁気カード
- USBトークン
- OTP
- クライアント証明書
- 乱数表
- メールアドレス認証

生体認証

- 指紋　静脈　虹彩　網膜　顔　掌
- サイン　音声　まばたき　腕の振り　所作動作
- DNA

☆ 本人認証の補完

- リスクベース認証：アクセス端末、場所、時刻等からリアルタイムでリスクを評価して必要時のみ　追加認証を要求するパッシブ型認証
- パスワード集中管理：シングルサインオン、パスワードマネジャー

Copyright© Nippon SecureTech Labo. 2010

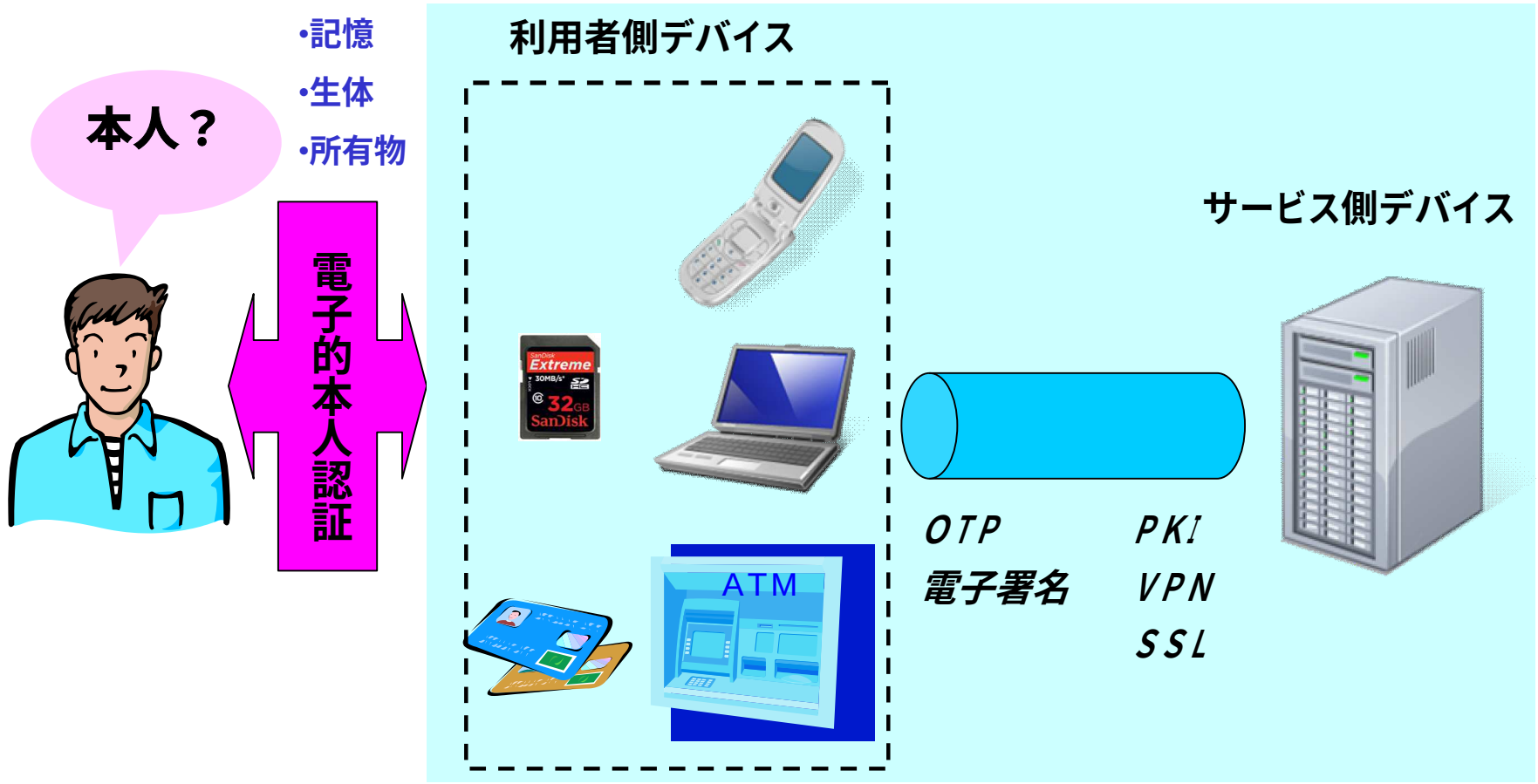
6．本人？　正規のユーザ？

***電子的本人認証における*End to end**

利用者を含めたEnd to end securityの範囲

デバイスのEnd to end securityの範囲

正規のユーザ？ | 正規のデバイス！ | 正規のサーバ！



Copyright© Nippon SecureTech Labo. 2010

7．電子的本人認証の課題　（その1）

《未だ懸案の電子的本人認証の課題》

1. 利用者は、サービス毎に本人認証が必要なため、ID・パスワードの管理が煩雑
2. 本人認証に関する統一基準がない（強度、利用、運用管理、など）
3. 利用者情報の漏洩事件や事故が多発している
4. 本人認証はサービス・プロバイダにとって大きな負担となっている
5. 異なるトラストドメイン間での連携は実現されておらず、サービス・プロバイダによるサービス提供が制限される

上記出典：電子認証ビジネスモデル策定報告書（JIPDEC　平成18年3月）

Copyright© Nippon SecureTech Labo. 2010

7．電子的本人認証の課題　(その2)

ワンストップ行政サービスを提供できる電子政府実現を念頭に

《電子的本人認証の検討会で考えた課題》

1. 全ての国民が安全につかいこなせる本人認証手段

   信頼できる本人認証手段なくして信頼できるサービスなし

2. 公平と平等の原則

   サイバー世界における民主主義の成立要件　高齢者　障害者もネット国民

3. モバイル環境での利用

   いつでも、どこでも、誰でもストレスなく利用できることが要件

4. 意思行為原則：　権利義務の主体確定プロセスである本人認証は、当人が死亡しても意識不明であっても実行できてしまえるものでないことが望ましい

   意思的行為＝本人しか知りえない秘密情報の意思的提示が有効

5. 本人認証技術とデバイス認証技術の再整理と本人認証に関する誤解（優良誤認）の解消

   ワンタイムパスワード、電子署名、PKIは、あくまでデバイス認証技術

6. 本人認証は、未だ最先端のIT知識と悪知恵に長けた悪意集団の執拗な攻撃に耐える強靭さを有していない

Copyright© Nippon SecureTech Labo. 2010

電子的本人認証の検討会　開催中！

確実な電子的本人認証基盤の確立に向けて「電子的本人認証の検討会」開催中

【国民にとって】

次世代電子行政サービス実現の最大の鍵が確実な本人認証

【企業団体にとって】

「モバイル機器持ち出し禁止としたいが、社員の業務効率低下を招く」
というジレンマを解決する最大の鍵が確実な本人認証

国民と行政の双方にとって使い易く実現可能性の高い本人認証基盤を考察し、
下記に寄与するため「電子的本人認証の検討会」にて活動中です。

- デジタル社会・ネットワーク社会における国民の安全・安心な
  社会活動への寄与
- 企業団体において安全・安心でかつ自由闊達な活動への寄与

Copyright© Nippon SecureTech Labo. 2010

電子的本人認証の検討会有志

氏名（五十音順）	
伊東寛	株式会社シマンテック
内田順一	JSSM先端技術・情報犯罪とセキュリティ研究会
鵜野幸一郎	日本セキュアテック研究所
大井正浩	中央大学
加藤美治	富士通株式会社
川口元	キヤノンマーケティングジャパン株式会社
久良知健	株式会社インフォセック
小泉雄介	日本電気株式会社
小林健	株式会社ＯＳＫ
力利則	日本電気株式会社
浜田良樹	東北大学
林隆臣	日本電気株式会社
林簡	株式会社インフォセック
原岡望	JSSM個人情報の保護研究会
廣島彰彦	原沢製薬工業株式会社