個人認証に関わる周辺状況

東京大学大学院情報理工学系研究科
ソーシャルICT研究センター
山口利恵

School of Information Science and Technology, The University of Tokyo
Social ICT Research Center

現状の認証技術における問題点

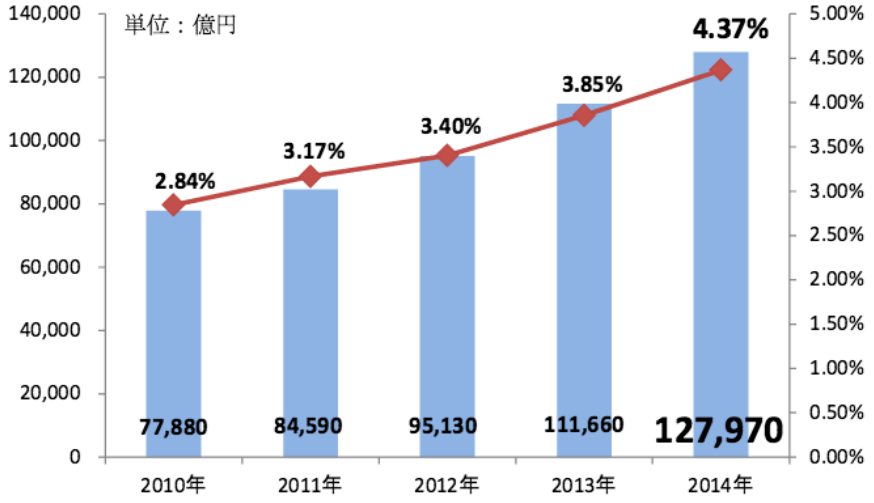
現状の分析

- ECサイト市場規模の増大
  - 2014年は前年度比，14.6%
  - 越境でのEC利用が増えるなど，不正の増加にもつながっている
- ECサイトにおける安全な決済が求められているところ，様々な不正が後をたたない

図表 1-2：BtoC-EC 市場規模および各分野の構成比率

	2013 年	2014 年	伸び率
A. 物販系分野	5 兆 9,931 億円 （EC 化率　3.85%）	6 兆 8,043 億円 （EC 化率　4.37%）	13.5%
B. サービス分野	4 兆 0,710 億円	4 兆 4,816 億円	10.1%
C. デジタル分野	1 兆 1,019 億円	1 兆 5,111 億円	37.1%
総計	11 兆 1,660 億円	12 兆 7,970 億円	14.6%

図表 1-3：BtoC-EC の市場規模および EC 化率の経年推移



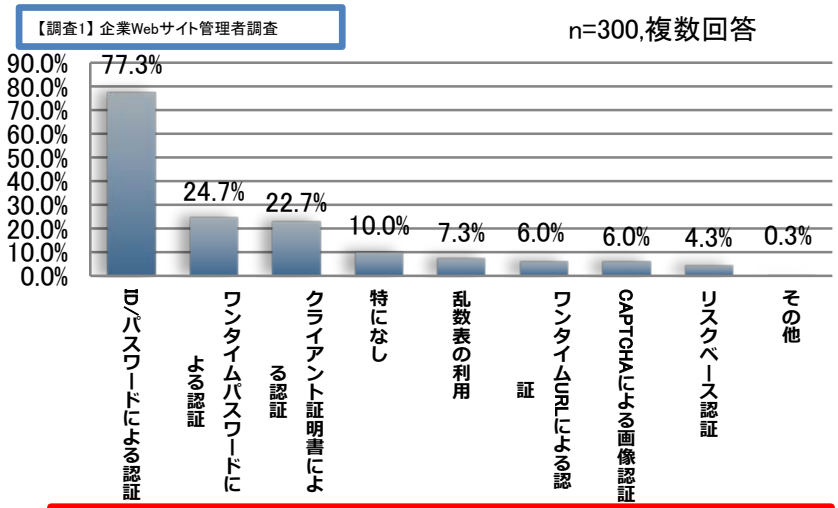
平成26年度我が国経済社会の情報化・サービス化に係る基盤整備（電子商取引に関する市場調査）
http://www.meti.go.jp/policy/it_policy/statistics/outlook/h26report.pdf

パスワードの現状

- ほとんどのサイトは、IDとパスワードに頼っている
  - 理由は、安価で使い勝手が良い。
- 一方、ユーザは、同じパスワードを使いがち

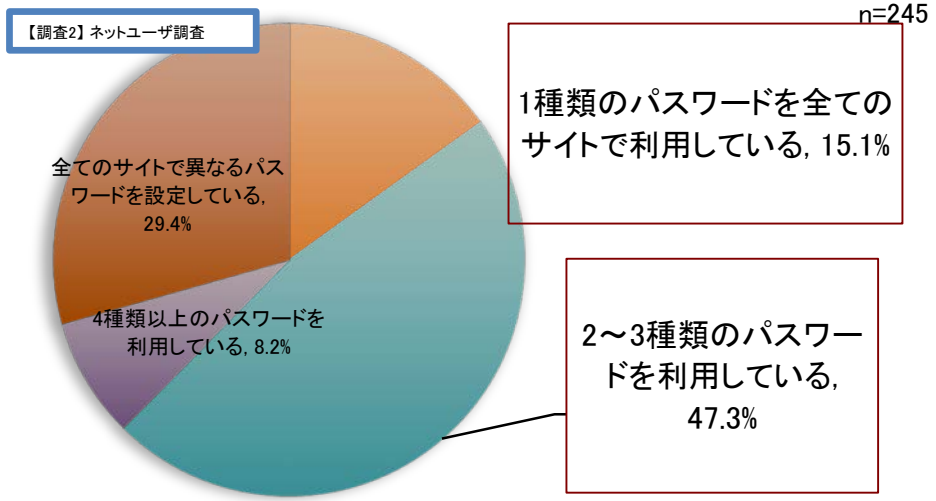
シマンテックの調査：
https://www.jp.websecurity.symantec.com/welcome/pdf/password_management_survey.pdf

現在、御社サイトでどのようなユーザ認証を実施していますか？



77%のサイトはIDとパスワードを利用

決済サービスのパスワードはそれぞれ別々に設定していますか？

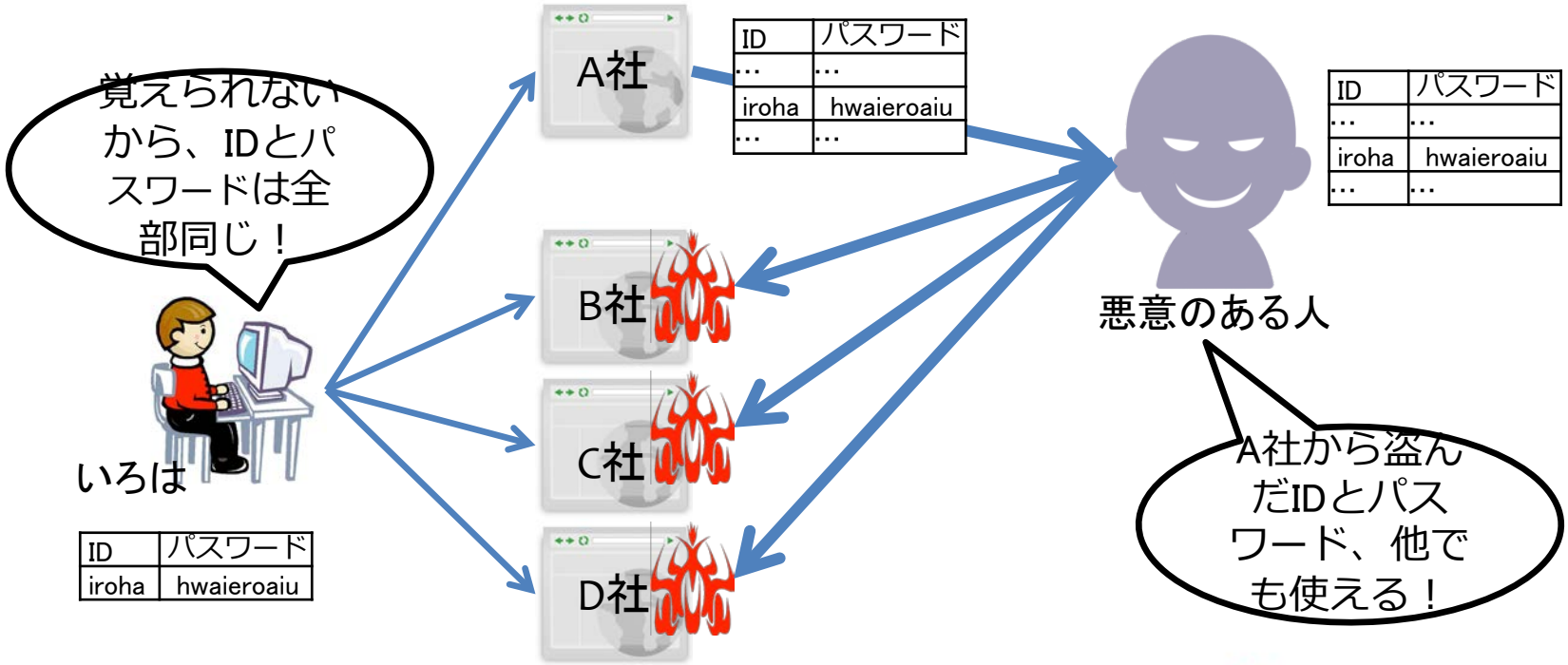


62%は1～3種類のIDとパスワードを利用

パスワードリスト攻撃

- 不正取得したIDとパスワードのリストを流用し、別のWebサイトへ不正にログインする攻撃手法
  - 攻撃成功率が高く、サイト運営者側が気づきにくい
  - サイト運営者は、ユーザーがパスワード流用しているかどうかを確認できない
- 近年、成功率は低いものの、実害が増加中

IPAの調査：https://www.ipa.go.jp/security/txt/2013/08outline.html



Webサイトの認証

多様な認証方法が存在

1. ワンタイムパスワード
   導入例：国内外銀行、社内LANログイン等

トークン（ワンタイムパスワード専用表示端末）
http://www.mizuhobank.co.jp/direct/info/onetimeo803.html

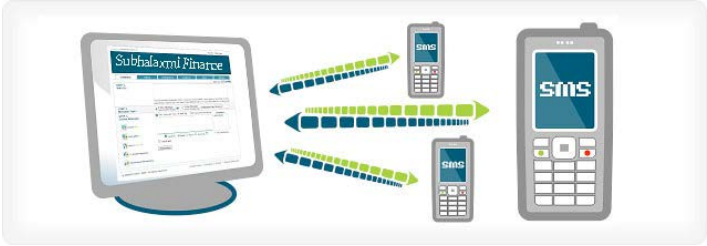
2. PassFaces
   導入例：国外銀行、等

http://www.passfaces.com/

3. ICカード
   導入例：国外銀行、等

http://www.gemalto.com/emv/online_security.html

4. SMS
   導入例：国外銀行、等

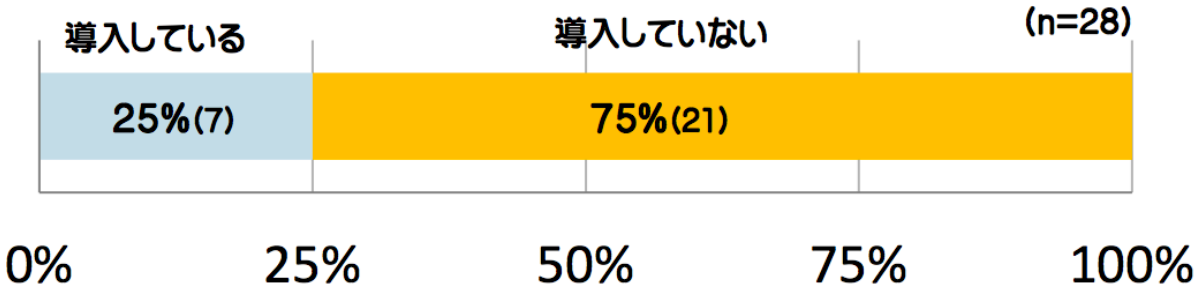


http://www.shubhalaxmifinance.com.np/smsBankingAtm.php

高度な認証手段の導入具合

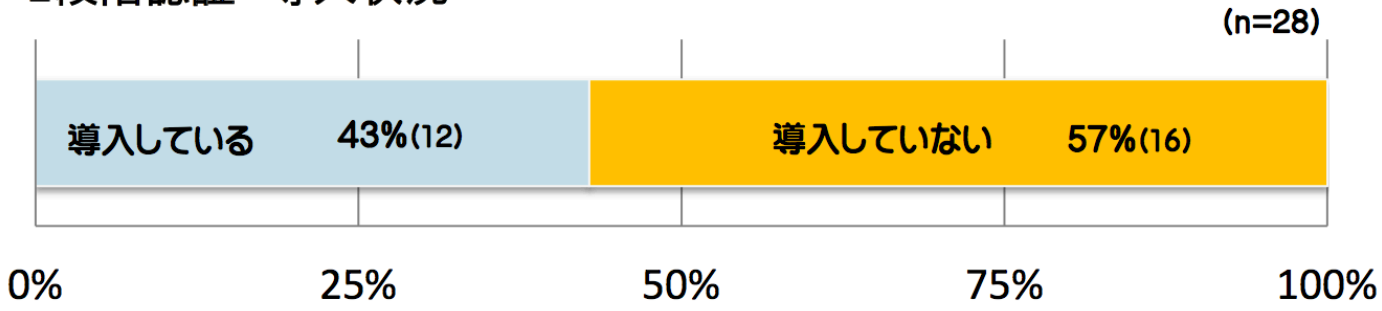
- リスクベース認証

■リスクベース認証を導入しているか



- 二段階認証

■2段階認証　導入状況



総務省：**「ウェブサービスに関するID・パスワードの管理・運用実態調査結果」**
2015年7月30日　http://www.soumu.go.jp/main_content/000370853.pdf

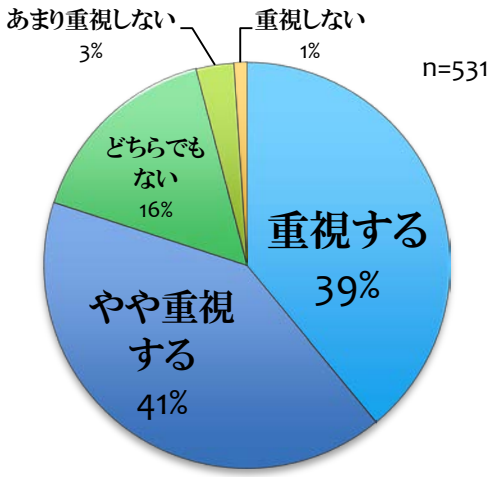
なぜ導入がすすまないか

各種機関がこの問題に対してアンケートを実施

- ＩＰＡ「オンライン本人認証方式の実態調査」*1：
  - コストが安い
  - 他の手段は利用率の低下に繋がるという懸念

  ⇒　サービス事業者はユーザへの負担を考えて，新たな方式にうつりにくい
- 富士通総研「インターネットバンキングに関するセキュリティ意識調査」*2：
  - 8割が使い勝手を重視

「インターネットバンキング」に関する意識調査



*1 https://www.ipa.go.jp/security/fy26/reports/ninsho
*2 http://www.ffri.jp/news/release_20131205.htm

10年以上，問題点を指摘しながら解決できていない

- IDとパスワードは限界に来ている
  - 記憶に頼るパスワードはどうしても脆弱になりがちである
    - ユーザリテラシーの向上は、非常に息の長いプロジェクト
  - 暗号鍵を活用したシステムは専用ソフトやハードウェアが必要
    - 普及が進んでいない
- 「セキュリティが高く利便性が高い認証が必要」という台詞はここ10年間言われてきたが変わってこなかった
  - セキュリティが高い、利便性が高い、という点だけではない何かが必要
- 新たな攻撃は次々に起きている
  - 写真から指紋が収集される時代がくる
    (https://allabout.co.jp/gm/gc/467302/)

⇒ **ドラスティックに社会全体を変革する必要がある**

指紋認証に問題が見つかる

最近のオンライン認証

リスクベース認証

- こんなメール
  来たこと
  ありませんか？

- 端末のOS, ブラウザ
  IPの位置情報などの
  情報から
  通常のアクセスと
  違うかで判断

利用端末
環境

Google

「Chrome」（Windows）からの新しいログイン

会 様

お使いの Google アカウント i　　ic.jp が Windows で Chrome からのログインに使用されました。

ACM　　2017
icpc201

Windows
2017年6月14日水曜日、21:50（JST）
日本, 茨城県つくば市*
Chrome

このアクティビティに心当たりがありますか？
最近使用した端末を今すぐ確認してください。

Google ではセキュリティを非常に重視しています。このメールは、お使いのアカウントで行われた重要な操作に関する最新情報をお伝えするために送信しています。
以前にこのブラウザまたは端末で、このアカウントを使用したかどうかを確認できませんでした。理由として考えられるのは、新しいパソコン、スマートフォン、ブラウザで最初にログインした場合、ブラウザのシークレット モードやプライベート ブラウジング モードを使用した場合、Cookie を削除した場合、または自分以外の誰かがアカウントにアクセスした場合です。ご自身がログインした場合は、特に何もする必要はありません。

Google アカウント チーム

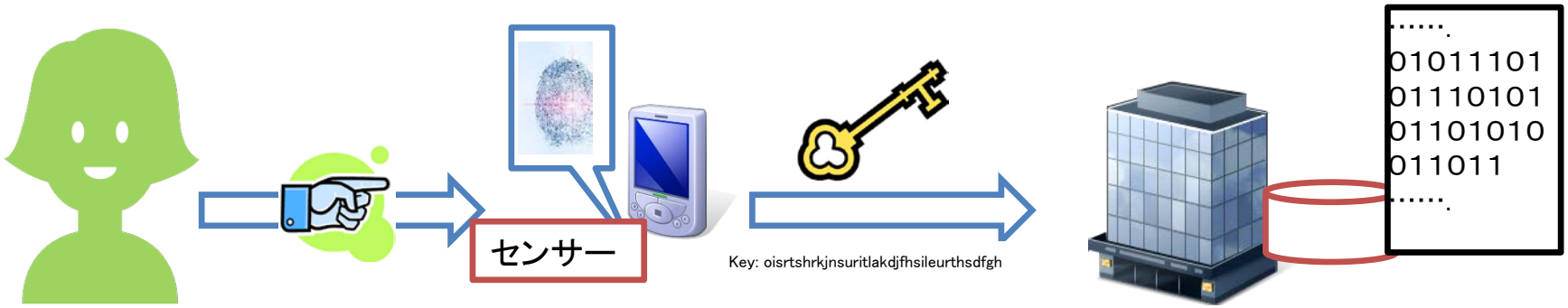
生体認証の普及

- 最近は，携帯電話等において生体認証が使われる動き
- しかし，生体認証単独だけでの利用は少ない
  - 理由：
  - 生体情報のセキュリティ強度が安定していない
    - 最近は技術が進みつつあるので、急激にすすむ可能性はある
  - 生体情報のオンライン上プライバシーの問題が解決できていない
    - 現状の技術の多くは，手元の端末に生体情報を格納

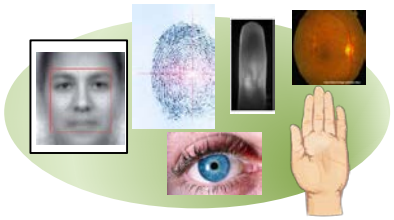
http://www.samsung.com/jp/promotions/galaxys5/
http://www.appbank.net/2013/09/12/iphone-news/666217.php
http://appllio.com/20150302-6219-fujitsu-saikou-ninsho

生体認証の利用シーン

- ユーザの手元はいろいろな認証技術を活用（生体認証含む）
  - FIDO、Apple Pay
- 生体情報とのやりとりは，端末．端末とサーバのやりとりは暗号
  - 生体認証だけでのオンライン認証はリスクが高い



生体情報を端末に提示　　生体情報と照合　　利用端末情報と照合



スマートフォンの生体認証

- ロック解除に使われる生体認証
  - 指紋認証
    - iPhone(TouchID)
  - 顔認証
  - 虹彩認証
- なりすまし
  - Apple iPhone
    - Touch ID
  - Samsung Galaxy S8
    - NTTドコモ、auから6月上旬発売

速報

2017年05月24日 10時33分 更新

「Galaxy S8」の虹彩認証、「写真でだませた」と独ハッキンググループ

かつて「iPhone 5s」の指紋認証を破ったハッキンググループCCCが、今度は「Galaxy S8」の虹彩認証を、Samsungのプリンタで出力した目の写真とコンタクトレンズでだませたとして動画を公開した。

[佐藤由紀子，ITmedia]

印刷／PDF　220 ツイート　49 いいね！　49 シェア　6 B! Bookmark　22 Pocket　1 G+1　通知

PR ソフトバンクがつくった大学ご存知ですか？今だけ入学金０円

ドイツのハッキンググループ「Chaos Computer Club」（CCC）は5月22日（現地時間）、韓国Samsung Electronicsの最新フラッグシップ端末「Galaxy S8」に搭載された虹彩認証を、印刷した写真でだませたと発表した。

デジタルカメラで撮影した顔の写真から目の部分を拡大し、Samsungの高解像度プリンタで印刷したものに、カーブをつけるために普通のコンタクトレンズを載せ、あらかじめその目の持ち主の虹彩を登録してあるGalaxy S8のカメラに向けたところ、ロックが解除された様子を動画で公開した。

デジタルカメラで顔を撮影

http://www.itmedia.co.jp/news/articles/1705/24/news072.html

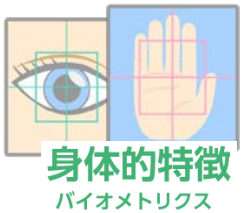
生体認証利用シーン

- オンラインでは，生体認証に暗号鍵の情報を組み合わせたケースが多い
- 現状の技術において，生体認証だけでの認証シーンとは？
  - 入国管理での利用
  - 建物に認証

→　人や防犯カメラが介在しているような場面での利用が多い
（不正があった場合には，随時指摘，もしくは，後から追跡が可能）

認証結果の利用方法

- 個人認証技術の多くが，０，１の組み合わせ
  - 知識：
    パスワード入力，ＰＩＮの正しさ，誤り
  - 所持：端末ＩＤの確認
  - 身体的特徴：閾値を超えたかどうか
  - ２段階認証や多要素認証であっても，
    「○」か「×」の組み合わせ



認証の3要素＋行動認証

- 認証の3要素だけでは語れなくなってきた
- 行動を活用した認証
  - 人々の行動履歴情報を活用した認証
- 多要素認証
  - 複数の認証を組み合わせて，より精度が高く利用しやすい認証手段の提案を行う

行政サービス向けの
認証とはどういうものか

オンラインと対面の違い

- 申請
  - 対面/紙
    - 書面を作成し，本人確認をして提出
  - オンライン
    - セッションごとに本人確認をしてチェックアウト
    - E-tax の場合は，最初に本人確認，提出書面を作成，署名を付与
- 買い物
  - 対面
    - 購入物品を選別し，レジでお金ととりかえ
  - オンライン
    - 購入物品を選別し，本人確認をしてチェックアプト
- 意思確認
  - 対面/電話…電話を呼ぶ声？
  - オンライン… ？

リスク 対 利便性

- クレジットカード
  - 購入時点
    - 金額が小さい場合には，サインレス
    - 突然違う買い物を行う場合には，電話での本人確認
  - カードの有効期限
    - ゴールドカードの有効期限は3年
    - デパートカードのようなカードの有効期限は10年のものもある

→　カード中に暗号鍵が入っており，リスクに応じて鍵の安全性を考慮している

不正があった場合には，保険（金銭）でカバーする社会的な枠組みが構築されている

リスク評価をどうするのか

- クレジットカードの場合は，保険でカバーする枠組みが存在している
  - 金銭で後から処理できる
- 個人情報の漏洩が犯罪につながった事例など，取り返しのつかない場合にはどうしたらよいのか
- 行政の無謬性をどのようにとらえるか

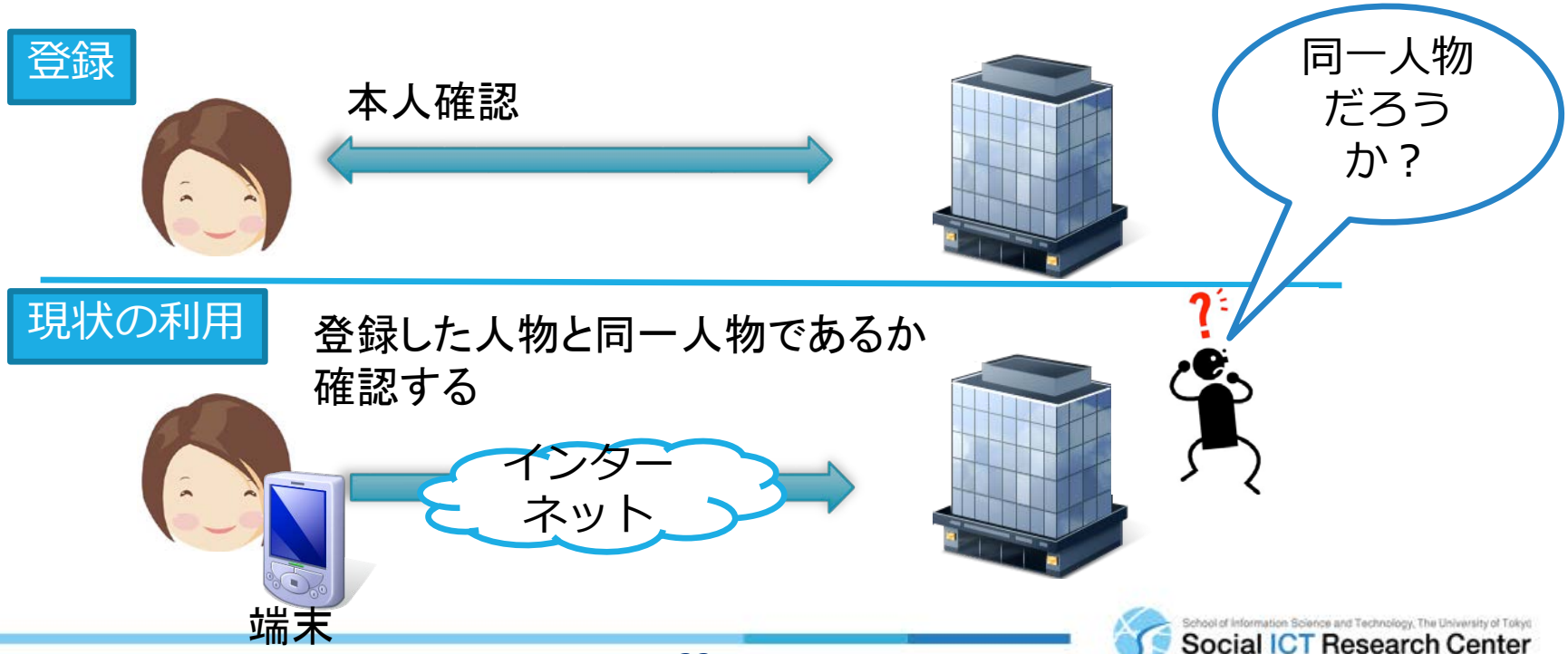
認証の基本プロセス

登録

利用

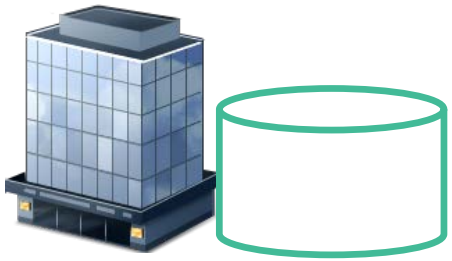
- 身元識別情報の特定
- 認証情報の保持の検証
- 意思確認
- 権限付与

サービス提供



登録処理

- 登録作業の時点でも実は何らかの認証処理が行われている
  - 対面の場合は写真を利用したりするが，間違うケースも
- バッグエンドIDを発行し，IDを振り分ける
  - 政府系の場合は，４情報との整合性をキーにしている

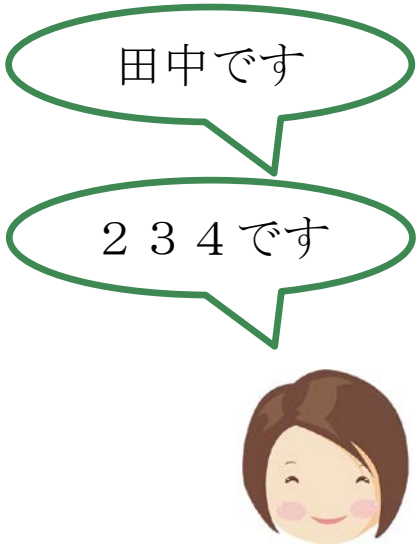


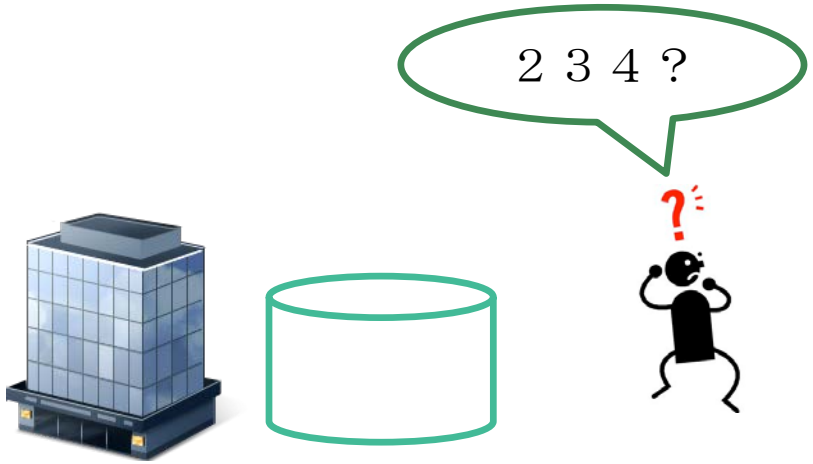
IDを付与

ID	名前	…	何で確認したのか
２３４	田中	…	運転免許証

認証

- バッグエンドIDとの紐付け
  - 一部事例は，IDをつけて，後から紐付けているケースも
- Identity Proofing
  - どの属性で確認するのか





ID	名前	…	?
２３４	田中	…	32429

どこでもリスクがおきうる

- どこででもリスクはある
  - 割合の高い低いの問題
- 登録時
  - カード発行時点
    - 対面での確認が不十分なケース
  - 生体の登録が不完全
- 認証時
  - データの改ざん
  - パスワードリスト攻撃
  - 偽造生体情報
  - 不正カードの利用

本人ぽい証拠の積み上げ

- リスクベース認証をはじめ，1箇所にこだわらない認証手法の出現してきた
  - 本人っぽい証拠の積み上げ
- 認証時に提出する別添書面（オンラインも含む）において，本人っぽい情報が積み上がるケースも
  - 納税の場合は，源泉徴収票での金額が正しければ？
  - 民間の会社から別途書面が提出されれば？
  - 育児関連の書面を複数出す場合は？

セッション管理

- オンラインの場合は，セッション管理が難しい
  - 購入等を入力した人と，決済作業を行う人が同一人物かどうか

海外事例

- ドイツ/米国：二次トークンの活用　（１次アカウント，２次アカウント）
  - 米国の場合は，利用しているGoogle アカウントを政府の番号に紐付ける登録を後から行う
- Credential を先に渡してから本人確認を後から（米，英，加，ニュージーランド，オーストラリア）
- 対面，犯罪収益移転防止法（免許番号），携帯電話でのID

実際に生きている（freshな）IDに対して，別のIDとの紐付けをする

海外でうまくいっている事例の理由

- ICカードでうまくいっている事例
  - 国民全員に強制的に配布
- 窓口が少ない国がオンライン化がうまくいく
  - 銀行の窓口がない
  - （日本は？）　対面インフラが充実している
- 生活に欠かせない場面から行政サービス
  - オンラインバンキングでの利用からの行政サービス
    - エストニア
  - eID Wallet
    - 決済手段との連動

行政への期待

- 行政の無謬性
- 本人確認/実在性確認
- 社会的慣習
- 対面インフラが充実している
  - 他国と比較すると，日本は対面サービスが多い，特に行政
- ユニバーサルサービスをどこまで頑張るか
  - リテラシーが低い人をどうしていくのか
  - 生体認証が利用出来ない人をどうしていくのか

どこまでシステム/インフラ投資をするべきかが難しい
（システムには，人の動きも含まれる）

電子申請に関わる項目

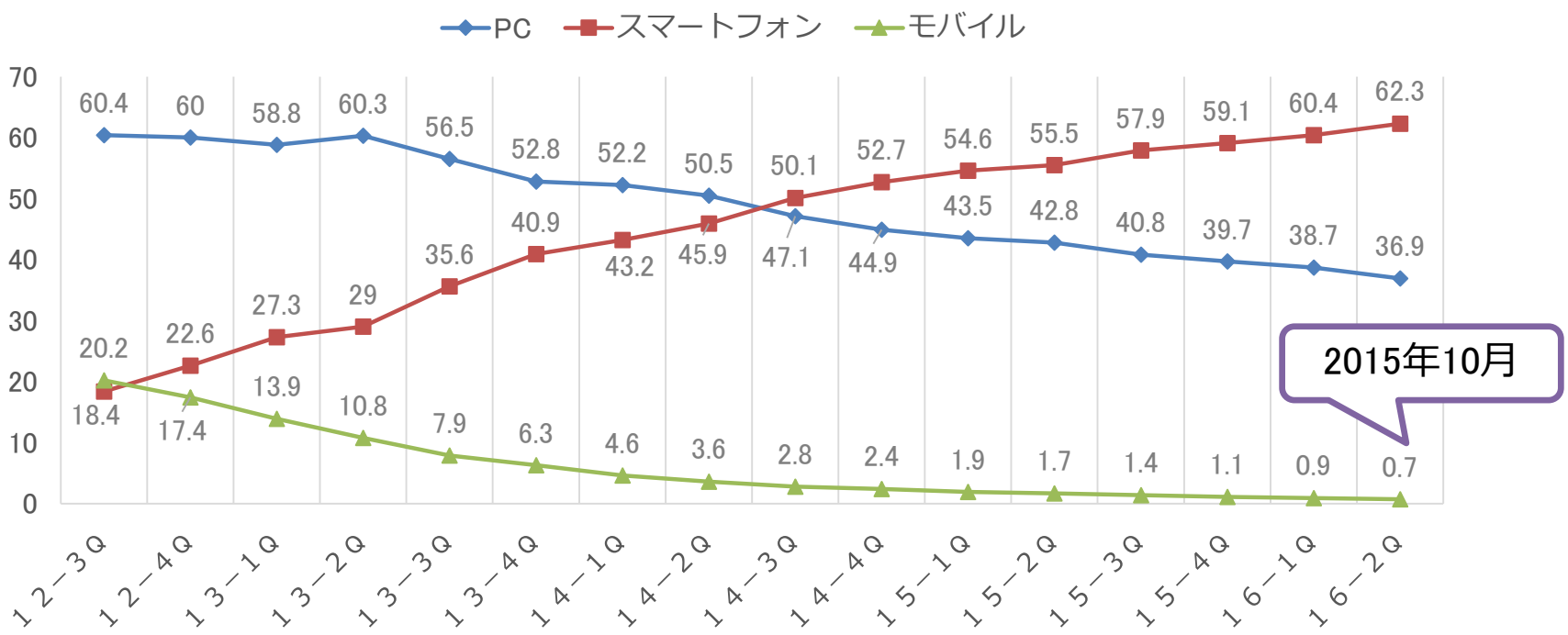
- 制度設計のあり方
  - 時代に即応しなければならない
- 利用環境
  - 時代時代ですぐに変わる
    - OSや実装周りが難しい
  - 現状，スマートフォンがプライマリー
    - なくしたらすぐにわかる
    - おかしな利用があった場合の対処が比較的容易
- 利用頻度/時効
  - そのIDが利用し続けられたものなのか，あまり利用されていないものなのか
    - 利用されていないIDは不正に利用されるリスクを伴い，また，ユーザの利用が慣れにくい
  - その申請が一生に1度か

周辺環境：機器の経年変化

- EC利用に利用した機器，2013年中頃にスマートフォンとPCが逆転

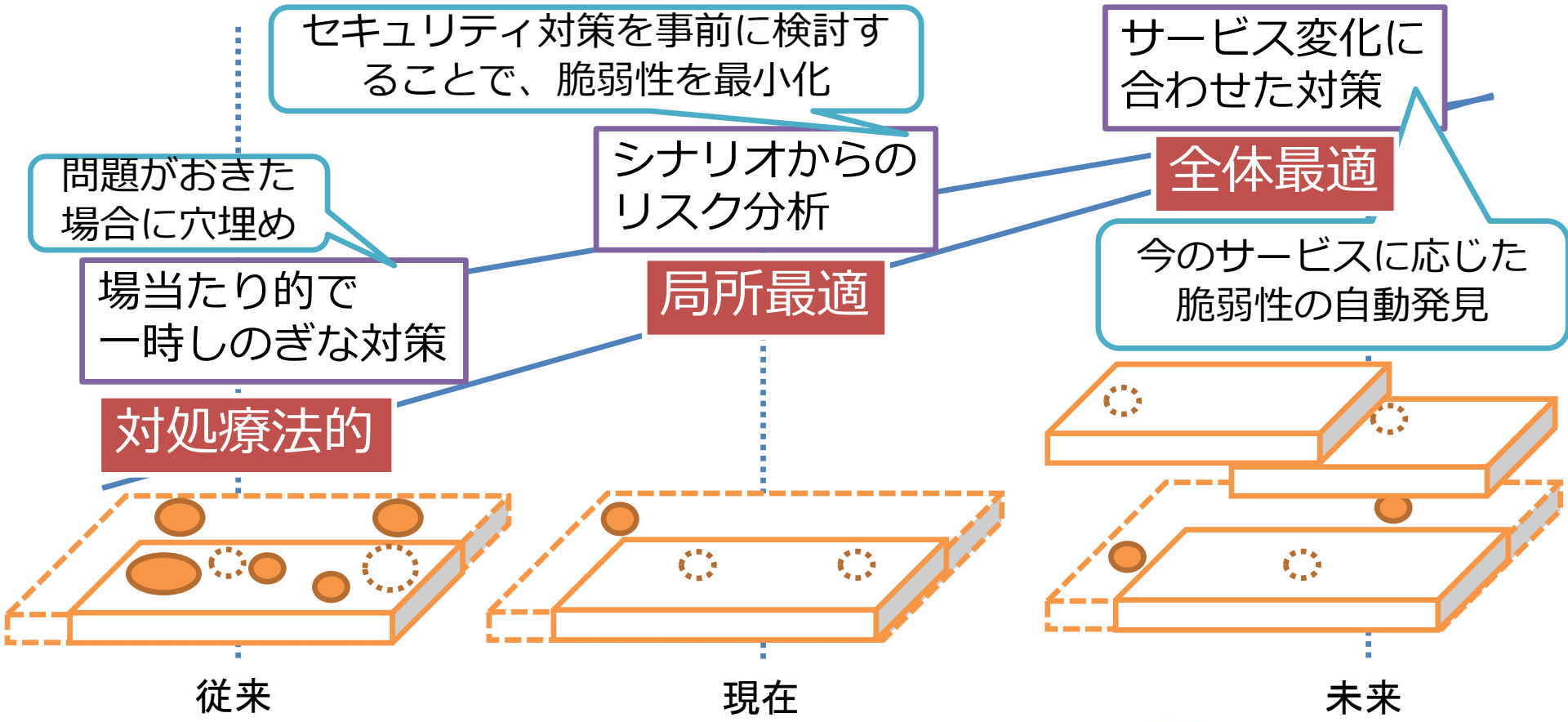
経済産業省：平成26年度我が国情報経済社会における基盤整備(電子商取引に関する市場調査 ）内の市場トレンドより，「スタートトゥデイ デバイス別出荷比率」

http://www.meti.go.jp/policy/it_policy/statistics/outlook/h26report.pdf
http://www.starttoday.jp/wp-content/uploads/2014/04/ir20140430-jp.pdf
http://www.starttoday.jp/wp-content/uploads/2015/10/CFM2.0.pdf



ビッグデータ/IoTを利用した未来の対策

- 今後はビッグデータを活用することで、自動的に脆弱性が発見可能な枠組みの実現



セキュリティの問題を新時代での解決を

- オンラインでのセキュリティリスクは紙ベースより大きいので，配慮が必要
- サービスの現状把握が必須
  - 1年に1度しか使わないサービスにおいて，複雑な作業を求めても
- 1箇所でのセキュリティ対策の限界
  - 複数の場で対策を多段階にしていかなければ
- 新たな社会技術を活用して，セキュリティ題を解決
  - 多段階をどのように実現したら良いのか