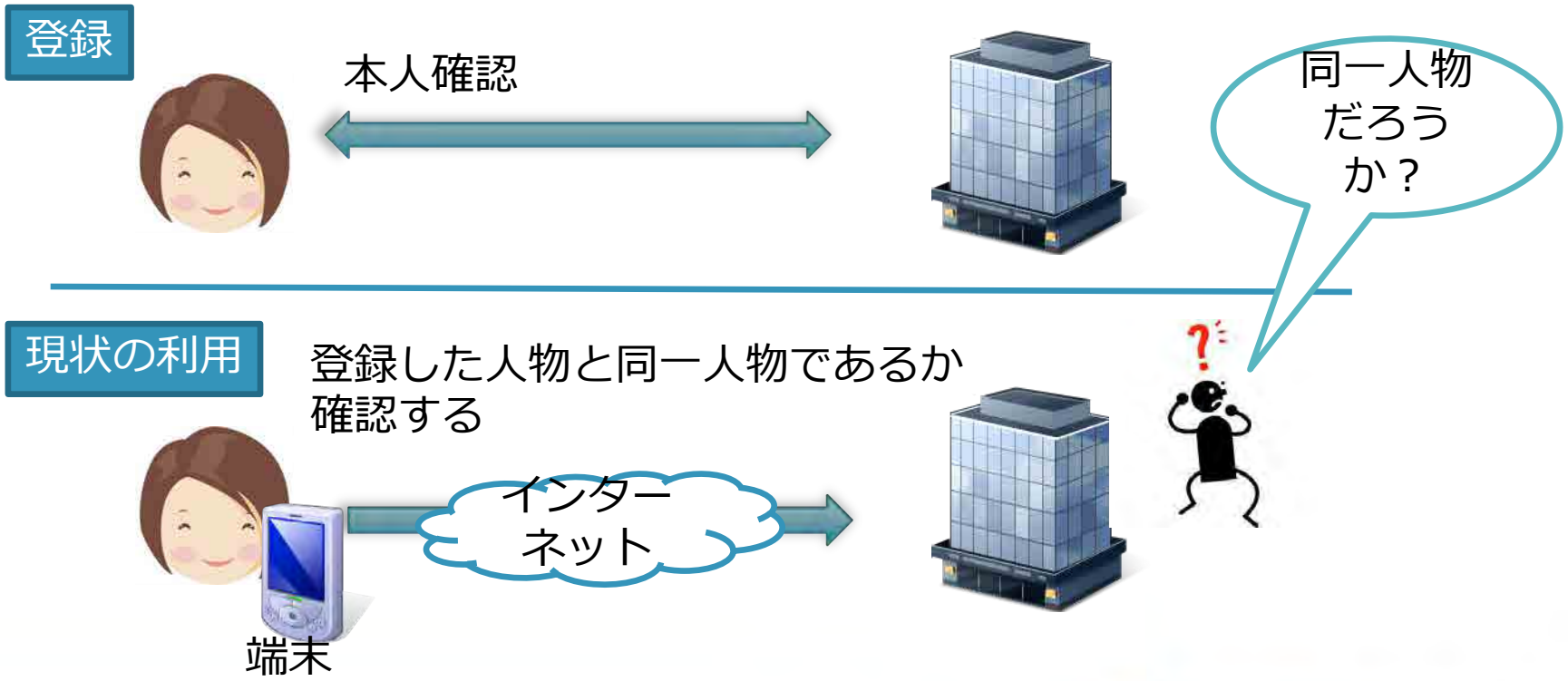
近年の個人認証の傾向

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

オンラインにおける個人認証とは

- オンライン認証とは、ある行為の実行主体と、当該主体が行った登録情報との同一性をネットワークを介した状態で検証することによって、「実行主体」が登録された人物（あるいは装置）であることの信用を確立するプロセスのこと。



同一人物だと示す方法には様々

- 認証の3要素と呼ばれる手法に加え，行動データを活用した認証などが既に活用
- 現状の個人認証システムは，安全性や利便性に問題がある
  - 知識（第１）：記憶の限界，身体的特徴（第３）生体情報に関するリスク等
- 第4の認証である行動履歴データを活用した認証

⇒　利便性と安全性を兼ね備えた行動履歴データの活用と多要素認証

「識別符号」って？

記憶/所持
絶対的な情報

計算量，情報量によって表現．ムーアの法則にそって安全なbit数を定義．

- パスワード
  - 利用する文字の種類や長さ
- ICカード
  - 内蔵されている暗号の種類
  - チップの安全性評価が確立

計算量的安全性に依存．

計算量での評価を行う際は，パスワード漏洩や人間のミス等については，セキュリティモデルの外として整理．数学的に表現出来ないことを外に出すことで，100%の安全性を目指す．

生体/行動
相対的な情報

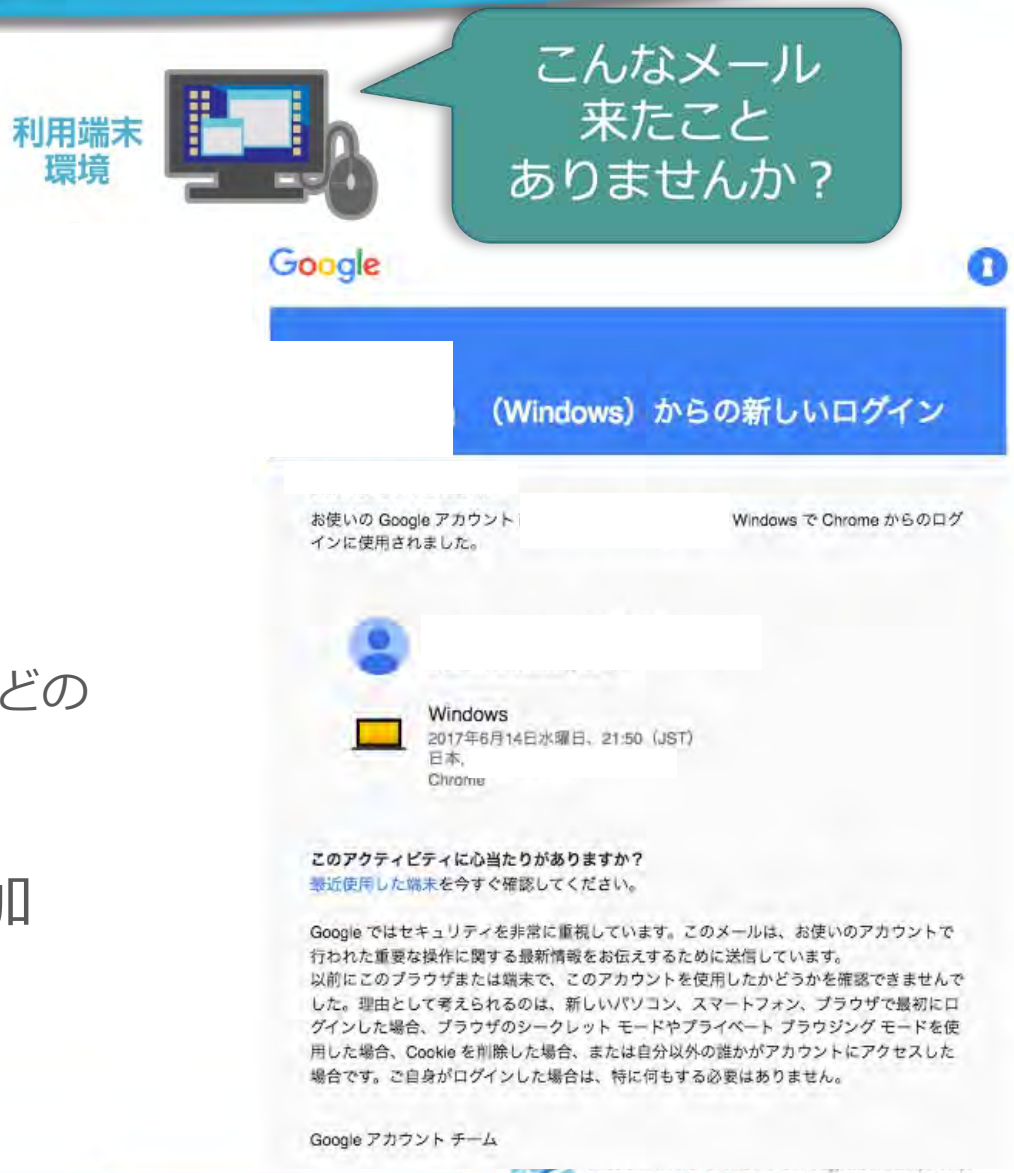
実験的，統計的に他者と区別がつくことによって評価．安全であることは経験的に評価．

- 生体情報（特徴点）
  - なるべく多くの人を被験者としてデータを取得し，評価
  - 指紋などが，世界中と誰とも一致していないと誰も証明できない
- 行動データ
  - IPアドレスや位置情報など，他の人と区別できるだけの情報を利用し，多要素認証することが多い．

経験的な安全性で表現しているので，100% になることはない．

昨今の行動データを活用した認証

- リスクベース認証
  - 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
- 行動ログデータを活用した
  認証
  - 周辺のWifi情報やBluetoothなどの
    情報を活用
- 研究としても様々議論が増加
  - 最近の様々な学会においても,
    論文が出てきている



実証実験（ステップ1.5　ぷちコン）

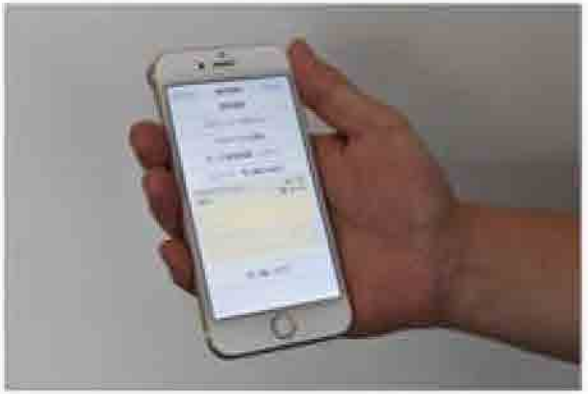
▽実験に使用する菓子販売ボックス

①利用者が近づくと自動で扉が解錠

②あとは商品を手にとって・・・

③扉を閉めると決済完了

④アプリ上で利用内容を確認できる



出典　http://info.cr.mufg.jp/news/down2.php?attach_id=349&seq=1548&category=1&page=1

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

（例）

  - 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

難しい．．．
言い出したらキリがない．．．

リスクの表現を内に含めるか，外とするか．
できない場合には，経験的に評価するので，100%にはならない

まとめ

- 個人認証の問題は多く語られてきたが，抜本的な解決に至っていない
  - パスワード漏洩等のセキュリティ問題事例が沢山あるが，利用は減っていない
  - ICカードは，オンライン個人認証においては利用がすすんでいない
- クレジットカードは，安全性よりも利便性重視
  - 不正があった際，保険などによってカバー．安全性をお金で表現.
  - 限度額の高いゴールドカードでは搭載チップが高額で有効期限が短く，限度額が低いデパートカードは安いチップで有効期限が10年.
- 経験的なリスク判定を元に，現実的な手法をとることが増えてくるであろう
  - 想定しているモデルの外のセキュリティ事例が増加し続ける

おまけ

- 行政の無謬性と現実解をどこにとるか

- 以下，参考

情報セキュリティだけに目を向けない

- セキュリティの専門家：
  「セキュリティを完全に」

  その中で，
  「利便性が高い」

  というものを求めがち

コストを考えると．．．

- 導入コスト
- ユーザの負担コスト
- 等

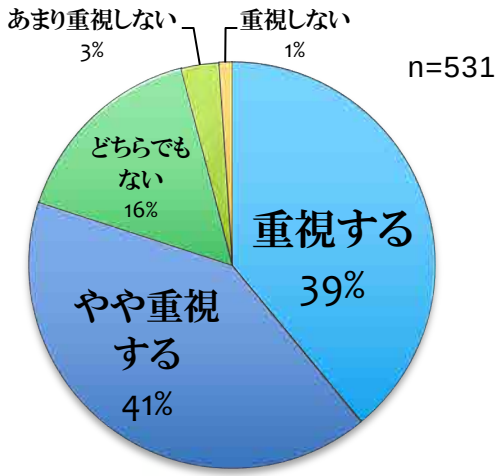
なぜ導入がすすまないか

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

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

安全安心に対するパラダイムシフト

- 従来の情報セキュリティの考え方
  - 「セキュリティをICT内で完全に」　その中で，「利便性が高い」
  - でも，全然利便性が高くない！
- クレジットカードの世界では？　→　費用対効果を重視
- この世界観でセキュリティを高めることで，
  保険料が安くなる上に，ユーザの利便性をあげる
  ことにつながる

情報セキュリティと保険やリスク評価を
組み合わせた新たな社会システムの確立

10年以上，問題点を指摘しながら解決できていない

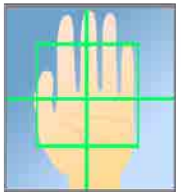
- IDとパスワードは限界に来ている
  - 記憶に頼るパスワードはどうしても脆弱になりがちである
    - ユーザリテラシーの向上は、非常に息の長いプロジェクト
  - 暗号鍵を活用したシステムは専用ソフトやハードウェアが必要
    - 普及が進んでいない
- 「セキュリティが高く利便性が高い認証が必要」という台詞はここ10年間言われてきたが変わってこなかった
  - セキュリティが高い、利便性が高い、という点だけではない何かが必要
- 新たな攻撃は次々に起きている
  - 写真から指紋が収集される時代がくる
    (https://allabout.co.jp/gm/gc/467302/)

⇒ **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

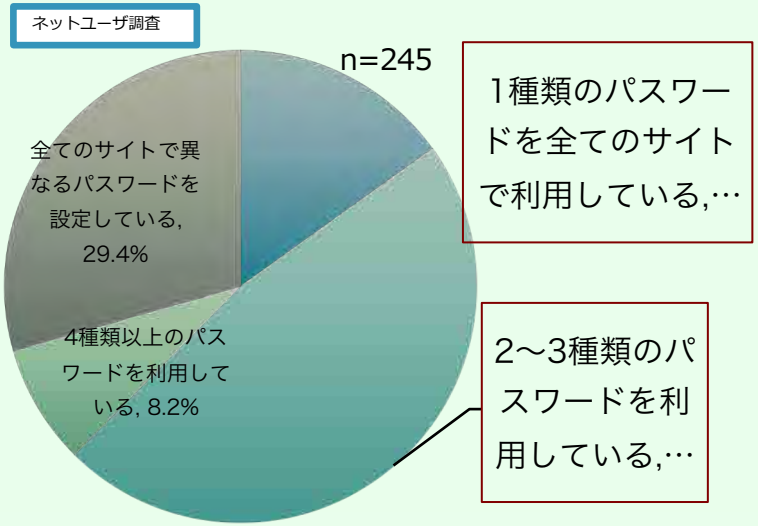
現状の個人認証システムの問題点

- 認証の3要素の問題点
  - 知識（第１）：記憶の限界
  - 所持（第２）：ハードウェアは素人には難しい
  - 身体的特徴（第３）生体情報に関するリスク



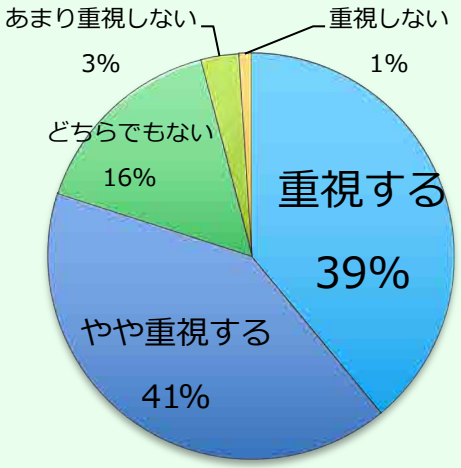
⇒　現状の個人認証システムは，安全性や利便性に問題がある

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

「インターネットバンキング」に関する意識調査



80%が**使い勝手を重視**

Social ICT Research Center

https://www.jp.websecurity.symantec.com/welcome/pdf/password_management_survey.pdf　http://www.ffri.jp/news/release_20131205.htm