ユーザがすべきこと
技術者がすべきこと

産業技術総合研究所 研究員

高田哲司

2006/06/04

Agenda

期待と違和感 - ユビキタス社会

携帯電話における認証

これからどうあって欲しいか

ユビキタスって?

一昔前ならSF漫画の内容が現実に!

しかし、見方を変えれば

- 誰かによって「勝手」にSensingされる世界
- しかもSensingする側はnetworkで接続されている
  - Sensingされたデータは...

とかく、この世は

利便性は声高に歌われる〜

しかし

安全性については...

なぜか多く語られない

とかくこの世は (cont.)

- 利便性は丁寧に説明される
  - なるほどね〜
- 危険性は?
  - 「大丈夫です．たいした問題ではありません」
- この技術にはどんな危険性があるのですか? と聞いてみる
  - 満足な回答が得られることは少ない

Movie

- RFID(電子タグ)が可能にする世界の例(監視カメラも活用!?)

http://chrisoakley.com/the_catalogue.html

なぜ、安全は二の次?

安全性と利便性のParadox

- 普及しない => 儲からない
- 改善しても褒められない
- でも、時に責められる(責任を問われる)

Securityとは
気を配っても、報われない領域...

どうすりゃいいの?

速報

2005/05/13 18:46 更新

日本の治安はこの2〜3年で「悪くなった」約9割

野村総研のアンケート調査によると、回答者の約9割が日本の治安はこの2〜3年で悪くなったと考えており、特にサイバー犯罪が増えたと感じている人が多い。

野村総合研究所は5月13日、治安に関する意識調査の結果を発表した。ここでは、ITmedia的な観点から注目される部分をひろっていこう。

まず、この2〜3年の間に日本の治安が「大変悪くなった」と答えた人が全体の36.4%。また、「悪くなった」と答えた53.1%を合わせると、治安の悪化を感じているのは約9割に上った。

自分の事は
自分で
守るしかない

http://www.nikkeibp.co.jp/sj/column/e/index.html

期待と違和感 - ユビキタス社会

携帯電話における認証

これからどうあって欲しいか

Net利用の主流は携帯へ

提供： TechOn!

ネット利用，「ケータイから」が「PCから」を上回る

2006年05月22日 11時1

総務省は，2005年末時点の世帯や企業における情報通信サービスの利用状況などについて調査した「通信利用動向調査」の結果をとりまとめた。これによれば，個人のインターネット利用では，携帯電話機などの移動端末からの利用者がパソコンからの利用者数を，1990年からの調査で初めて上回った。個人のインターネット利用者で移動端末を用いている人は対前年比18.8%増の6923万人，パソコンを用いる人は6601万人と推計された。なお，インターネット利用者の57%がパソコンと移動端末を併用しているとみられる。

携帯電話でのインターネット利用がPCを初めて上回る--総務省調査

目黒譲二
2006/05/22 09:52

総務省は5月19日、2005年末時点の世帯、企業および事業所における情報通信サービスの利用状況、情報通信機器の保有状況等について調査した「通信利用動向調査」の結果を取りまとめ、公表した。

通信利用動向調査は、世帯（全体、構成員）、企業および事業所を対象とし、統計報告調整法に基づく承認統計として1990年から毎年実施されている。

- 携帯電話がNetworkへの入り口に

携帯の認証方法

- 暗証番号
  - 4桁数字
- バイオメトリクス
  - 指紋認証
  - 声紋認証
  - 顔認証

生体認証が徐々に普及しつつある

が、これって便利で、かつ安全なの?

生体認証の問題I

なぜか、暗証番号との組み合わせで使われる

- 本人を排除してしまう可能性があるから
  - 0 or 1判定でない
  - 状況依存性
  - 経年変化
  - などなど…

許容しがたい特性

生体認証の問題2

製品仕様上は、精度99%以上と書かれているが...

指紋認証は「グミ指」

静脈認証は「大根指」

攻撃を想定した実験は行われていないのでは?

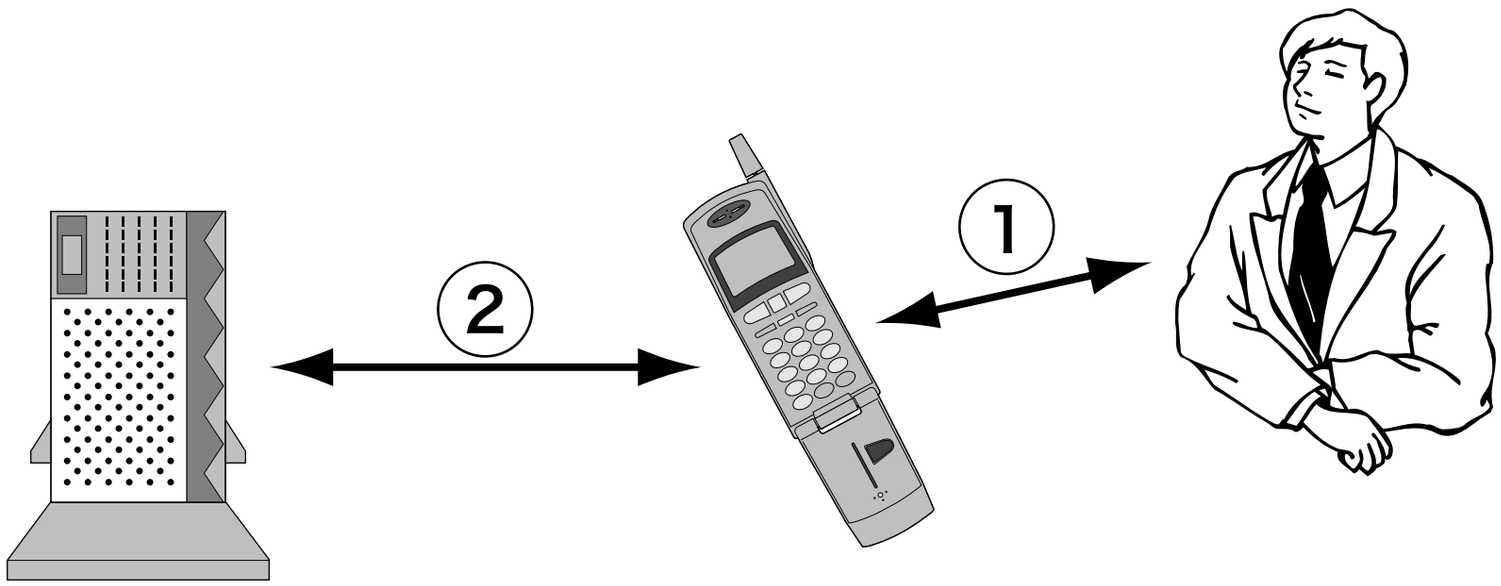
金融取引における生体認証について
http://www.fsa.go.jp/singi/singi_fccsg/gaiyou/f-20050415-singi_fccsg/02.pdfより抜粋
横浜国立大学院大学 松本勉研究室 http://www-mlab.jks.ynu.ac.jp/

生体認証の問題点3

生体認証 = 所有物認証

- 変更不能な身体情報
  - 拒否したい時はどうしたらいい?
  - 本人自身に危害を加えられる恐れ

所有物認証の問題



所有物認証だとPath Ⅰの部分の認証が不明確

情報を持っている人が本人かどうかは確認できない

認証とは?

- 何かしらの知識をもとに、対象の正当性を確認する行為

from wikipedia.
http://ja.wikipedia.org/

- 私はMr.Aです、私の秘密情報はこれです.
なのでこの処理をお願いします
- 私はこの口座のためのCashCardを持っています
そして暗証番号はxyzaです. 処理をお願いします

アクセス制御と認証

- アクセス制御 (識別)
  - 所有/許可(資格)/特徴の確認
- 認証
  - ユーザの意思の確認

生体認証ではなく、**生体識別**である

生体認証の誤解とは

生体認証は

認証の利便性向上を実現しているが、
安全性向上とは言い切れない

本人の意思確認が必要ならば

知識または能力照合型認証しかない

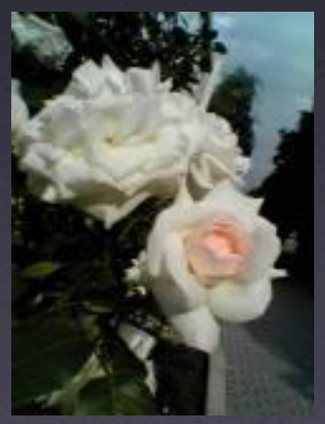
で、画像認証

あわせ絵

- ユーザの写真を利用
- 安全性向上
- 暗証番号と同等の利便性
- 通知によるPDCAサイクル

まずはじめに...

自分のパス画像(Pass-Image)を決定しておく



複数毎を推奨、しかし最低1枚でも運用可能

いざ、認証

照合画像には0 or 1枚のPass-Imageが含まれる

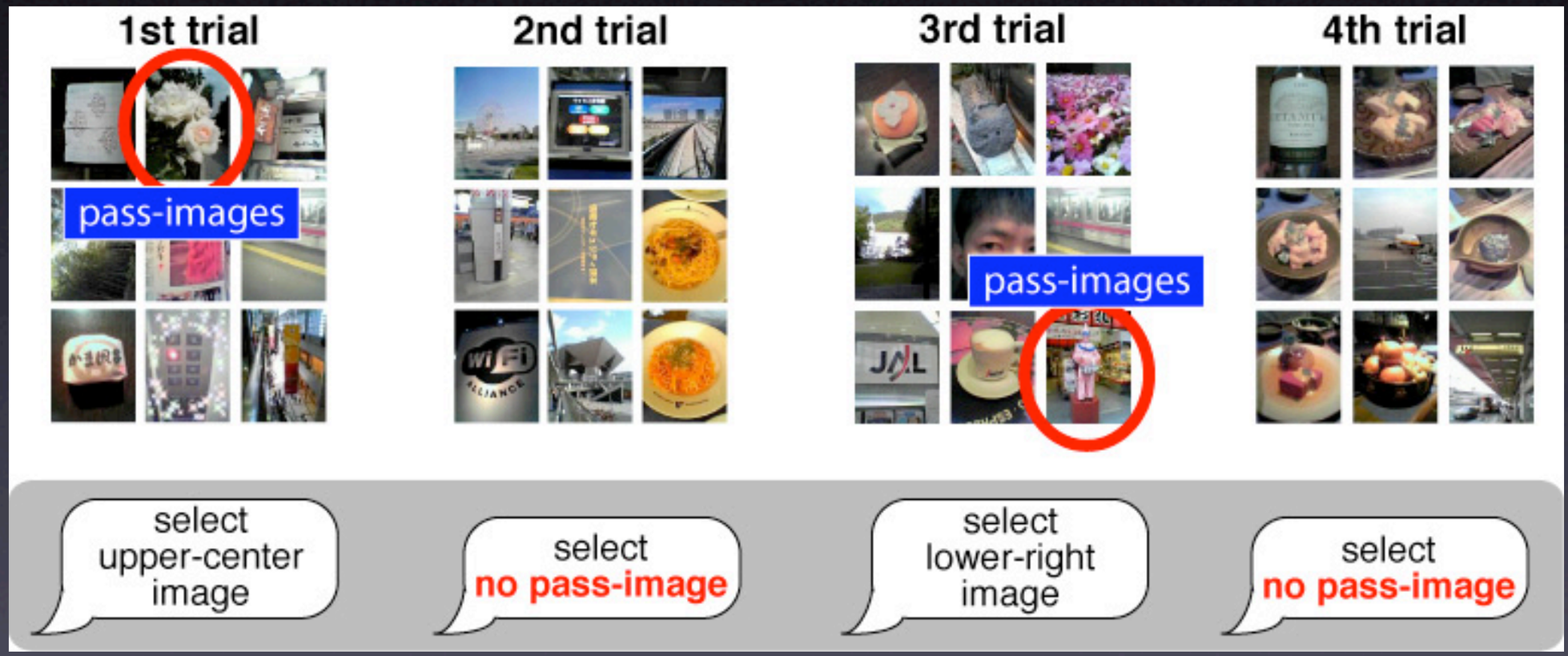
パス画像なし

パス画像なし

- ある場合は Pass-Imageを選択する
- ない場合は「Pass-Imageなし」と回答

認証方法

全ての写真はunique



すべての回答が正解であれば
試行者を正規のユーザとして認める

利点

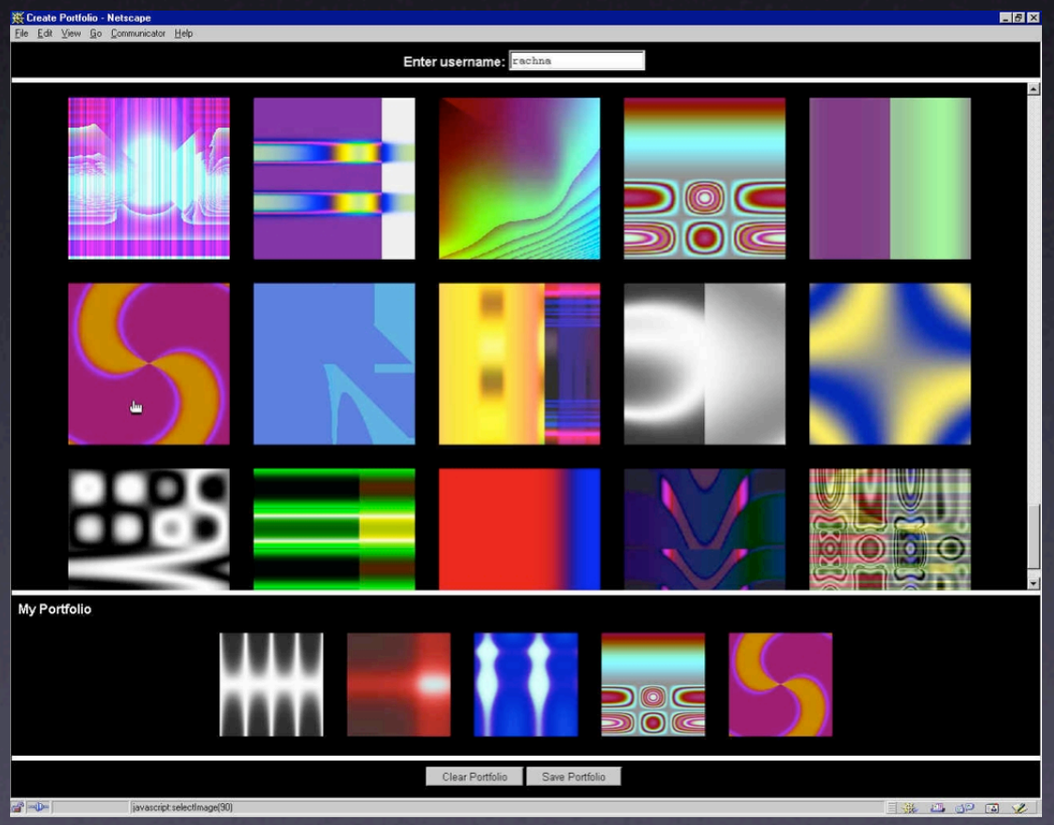
- 自分が撮影した写真の利用
  自分がすでに知っている情報を利用
- 回答候補の提示
  思い出す(想起)可能性
- 簡単操作
  想起/入力から認識/選択へ

関連研究

Deja Vu

5枚選択/20枚

4桁数字入力と
同程度の安全性



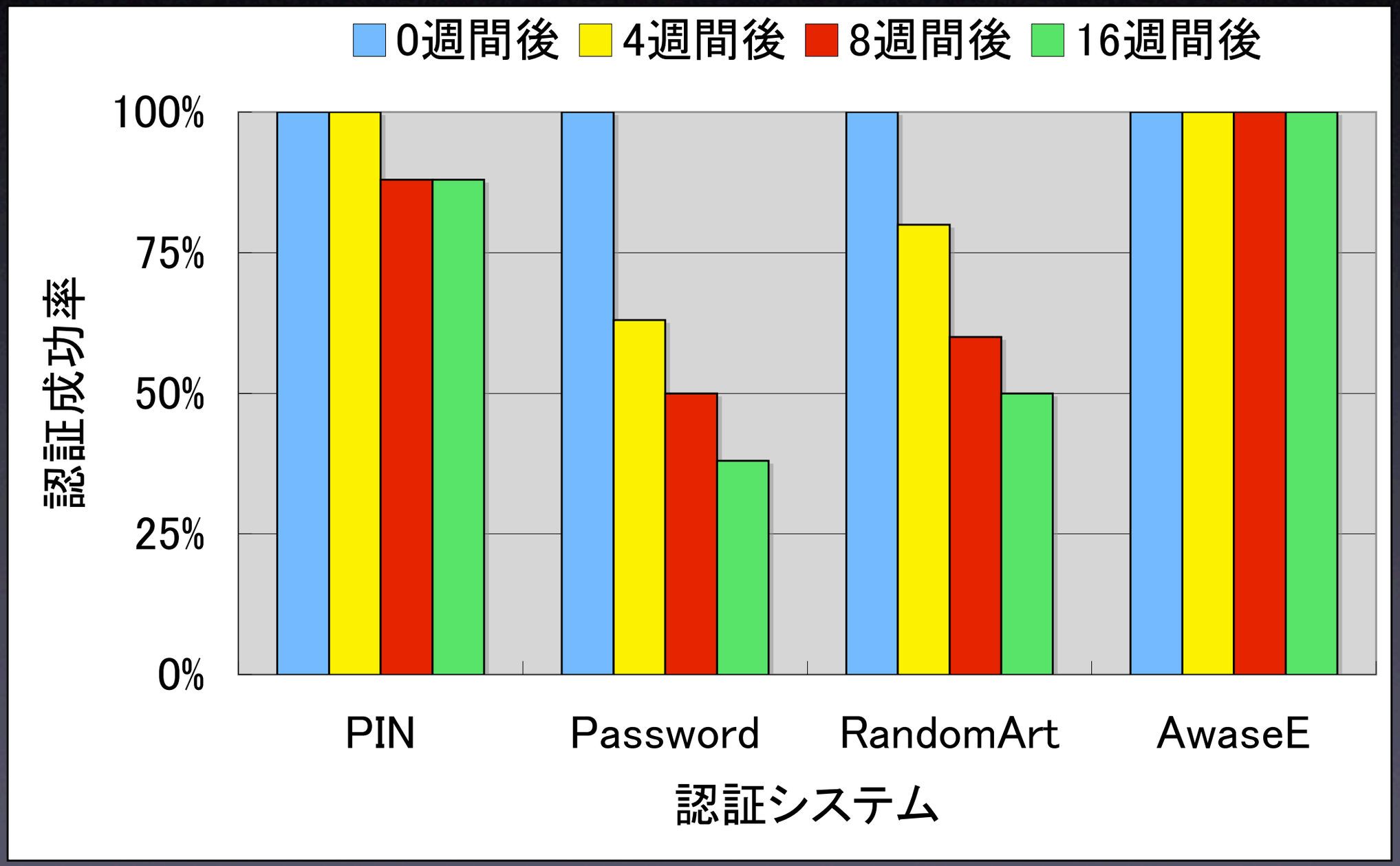
http://www.sims.berkeley.edu/~rachna/dejavu/

提示選択型認証方式

他の手法との比較

issues / method	input	memory and recall	generate and change
Text-based password	✗	✗	✗
System assigned image	○	△	✗
User's favorite photo	○	○	○

長期記憶評価


0週間後
4週間後
8週間後
16週間後
100%
75%
50%
25%
0%
認証成功率
PIN
Password
RandomArt
AwaseE
認証システム

理論的安全性

10個の選択肢 x 4回の照合回数
= 10,000通り

しかし全ての照合において
”パス画像なし”の回答だけは認めない

10000 - 1 = **9999** 通り

4桁暗証番号による認証とほぼ同等

問題点

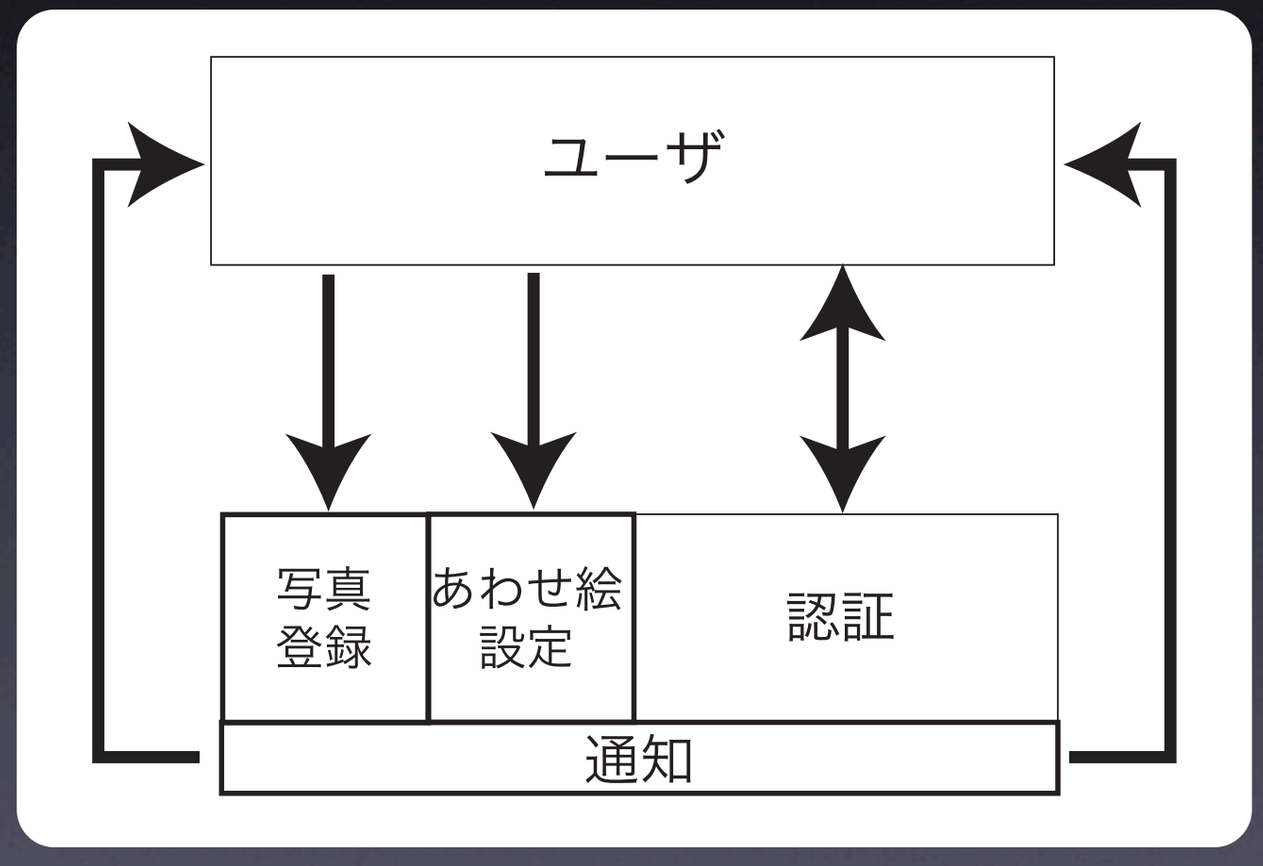
候補が表示されている事による脅威

- Intersection攻撃
  - 答えが常に表示される事を悪用
- 推測攻撃
  - 知識や視覚的特徴を基に推測
- あぶりだし攻撃
  - 出現頻度を基に推測

通知機能

認証システムで発生した事象をユーザへ通知

- 写真登録
- パス画像設定/更新
- 認証開始
- 認証結果

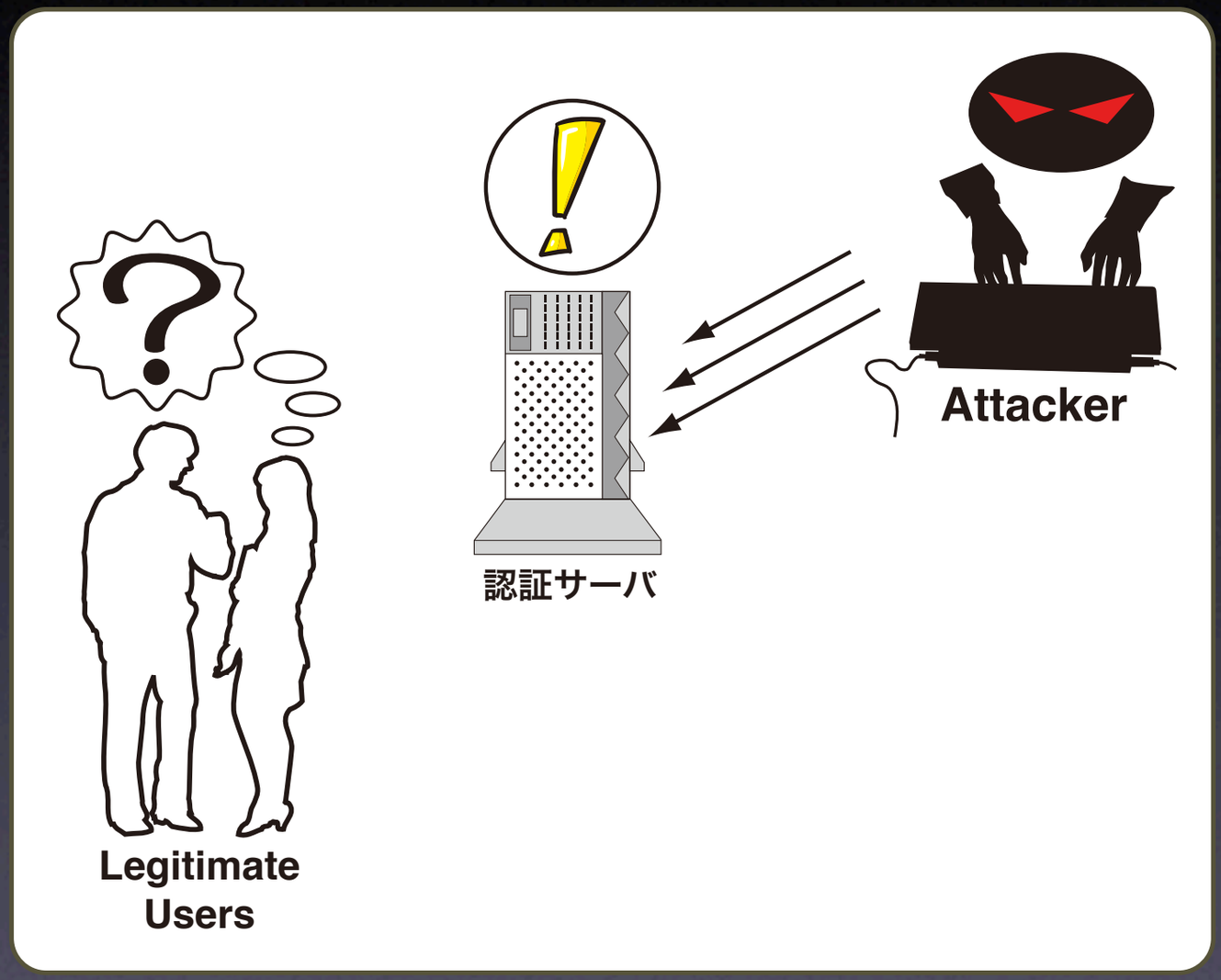


あくまで通知のみ
対応は実世界でユーザが行う

通知すると...

目的

- 正常稼働確認
- 脅威の存在をユーザへ
  - 現実を認識
  - ユーザが対応可能
- 抑止力効果



ユーザをWeakest Linkにしないための仕組み

ユーザも希望

オンライン・バンキング利用者を対象とした
セキュリティ意識調査結果を発表

現在行われているクレジットカード取引監視と同様に、銀行に対してオンライン・バンキング利用時の監視（変則的な行為またはその兆候の検知）を希望すると回答。【回答者の 89%】
不審な行為が検知されたときには、銀行から連絡があることを希望する。【回答者の 59%】

RSA Security press release (2006/03/24)
http://www.rsasecurity.co.jp/news/data/20060324l.html

現実に始まりつつある

主要 >> 記事一覧

シティバンク、ＡＴＭでの取引を今秋からメール通知

シティバンクは12日、偽造カードなどによる不正引き出しに対応するため、入出金などの取引がＡＴＭであった場合、顧客の携帯電話やパソコンに電子メールで通知するサービスを秋から始めると発表した。

受付開始は29日。シティバンクのホームページを通じて利用の申し込みをすると、ＡＴＭでの取引がある度に顧客にメールで通知が届く。シティバンクのカードが利用可能なＡＴＭでのすべての取引が通知対象となっている。日本国内だけでなく、海外のＡＴＭも対象としている。

通知には入出金や振り込みなどの取引の内容と取引額が記載されている。通知された取引に覚えがない場合、シティバンクに連絡をすると、ＡＴＭでの取引が停止される。（23:13）

Citibank アラートサービス

http://www.citibank.co.jp/service/alert/index.html

期待と違和感 - ユビキタス社会

携帯電話の認証

これからどうあって欲しいか

ユーザがすべき事

- 性悪説を前提に技術を見よう
- 危険性を予測する
  - 直感(本能)的に「これって危なくない?」と思ったものは使わない
- 聞いてみる / 調べてみる
  - 詳しそうな人、メーカー、キャリア、Google(?), ブログ(?)に聞いてみる

疑問を持つ事、自分で調べる事は大切

予想は現実になる


BBC
Home
News
Sport
Radio
TV
Weather
Languages
BBC NEWS
UK version
International version
About the versions
Low graphi
News Front Page
Africa
Americas
Asia-Pacific
Europe
Middle East
South Asia
UK
Business
Health
Science/Nature
Technology
Entertainment
Have Your Say
Last Updated: Thursday, 31 March, 2005, 10:37 GMT 11:37 UK
E-mail this to a friend
Printable version
Malaysia car thieves steal finger
By Jonathan Kent
BBC News, Kuala Lumpur
Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.
The car, a Mercedes S-class, was protected by a fingerprint recognition system.
Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.
The gang, armed with long machetes, demanded the keys to his car.

予想は現実になる 2

詐欺：住基カード偽造、容疑で逮捕

福岡県警八幡東署は18日、他人名義の住民基本台帳カードを作らせたとして北九州市八幡東区祝町1、無職、森下寿子容疑者（56）を詐欺などの容疑で逮捕した。森下容疑者は「携帯電話が料金滞納で使えなくなり、別人名義で加入申し込みをしたかった」などと話しているという。

調べでは、森下容疑者は05年10月4日、八幡東区役所
住民票を勝手に自分の住所に異動させ9日後、住基カー
どを記入し、自分の写真を添付して提出。住基カードを

森下容疑者は女性の住民票異動を届ける際、自分で作
申請時には、女性名義の郵便貯金キャッシュカードを提
下容疑者が住基カードを使って金融機関から借金してい

2006年5月19日

北海道斜里町の職員、住基ネットのパスワードなどをWinny流出

P2Pファイル共有ソフト「Winny」のネットワーク上に、北海道斜里町の行政情報などが流出していることがわかった。同町の男性職員の自宅PCがウイルスに感染して流出したもの。水道料金や町税の未払い者など642人分の個人情報のほか、住民基本台帳ネットワーク（住基ネット）の接続パスワードなども流出した。

流出した情報は全部で1,813件で、そのうち1,624件が行政情報だった。個人情報が含まれていたものは54件（642人分）で、斜里町によれば「業務上のやり取りで、水道料金や町税未払い者の入金額を事務連絡する資料などが含まれていた」という。

このほか、3年前のパスワードではあるが住基ネットのパスワードも流出。住基ネット全国センターが全国の自治体に送った告知文なども流出した。ただし、住基ネット関連の個人情報は流出していない。また、パスワードも毎年変更しており、流出したパスワードは現在利用していないという。

2006/03/29

実は本人次第

- 携帯電話もITも**道具**
  - それは自分にとって必要なのか?
  - 何が問題で、それを解決/改善してくれるのか?
  - 利便性をとるか、安全をとるのか?
  - そこにあるRiskは許容できるのか?

見極めが重要

技術者がすべきこと

- 安全性に関する情報提示/開示
- 初期設定は、安全を優先した設定に
- 選択の自由(安全性 or 利便性)をユーザに
- User Interfaceの必要性
  - 今、何が起きているかを明確に提示
  - 安全に関する選択を可能に

これではいけない


顔認証機能

P33

ケータイを開くだけで自動的に*
持ち主の顔を識別できる安心機能。

サブカメラを使い事前に顔認証用画像を登録しておけば、顔の特長で使用者を判別し、第三者による不正利用を防止します。万一紛失したり、盗難にあった場合に、電話帳データやメールアドレス・送受信したメールなど、プライバシーを保護できます。

※初期登録が必要です。●顔認証技術は完全に本人認証を保証するものではありません。当社では、本製品を第三者に使用されたこと、または顔認証により使用できなかったことによって生じる、いかなる損害に対しても一切責任を負いかねますのであらかじめご了承ください。また顔認証を設定していても、ボーダフォンライブ!FeliCa は使用できますのでご注意ください。

安全性に関する
excuseは下に
小さく書いてある

FeliCaの危険性とその対策

モバイルSuicaから改善可能

- 初期設定: Suica機能を無効にしておく
- ユーザがいつでも有効/無効化可能にする
- 有効/無効化のためのSwitchと、現在の状態を示すUser Interface(UI)を提供

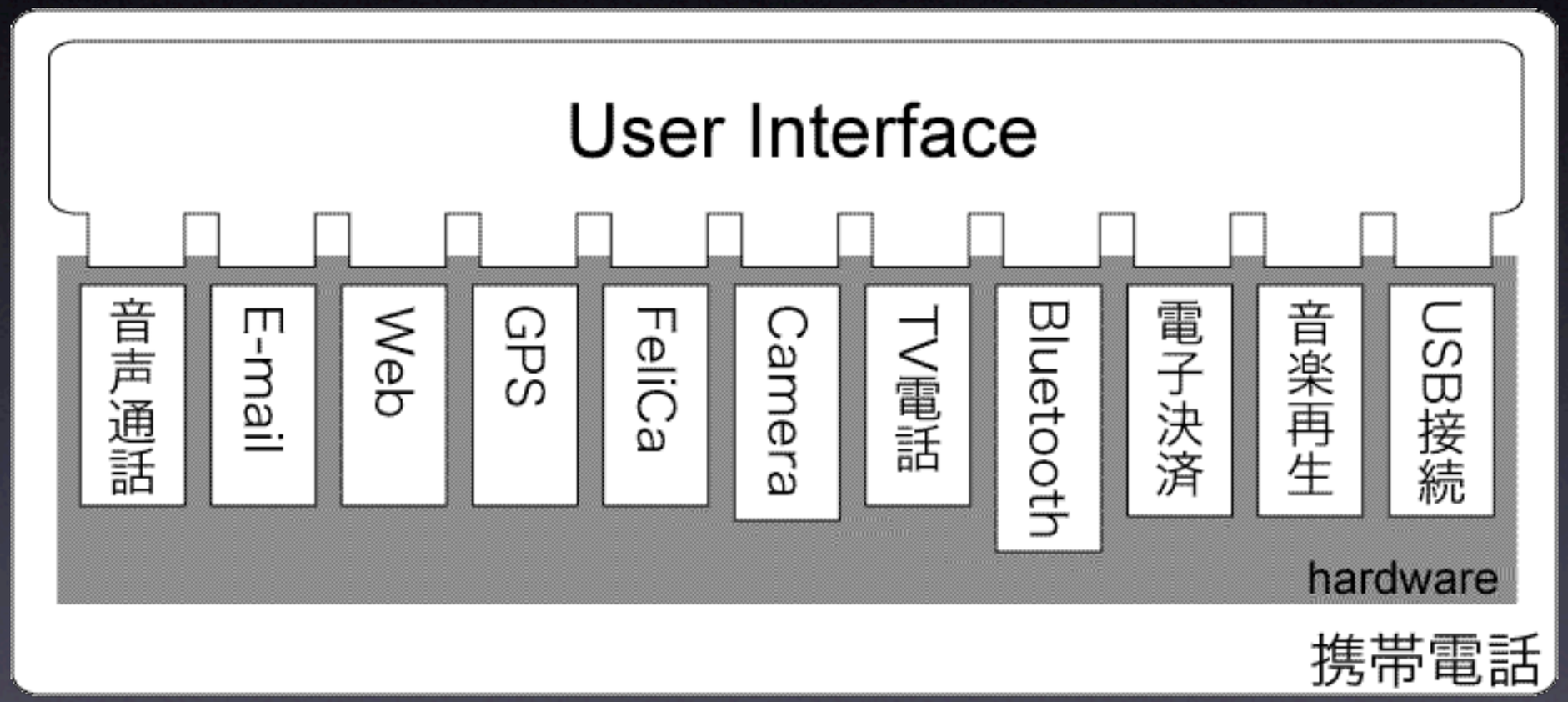
携帯電話とFeliCaの組み合わせなら
十分に対策は可能なはず

実はある (au W32S)

- FeliCaキー
  - FeliCaロック
- FeliCaサイン

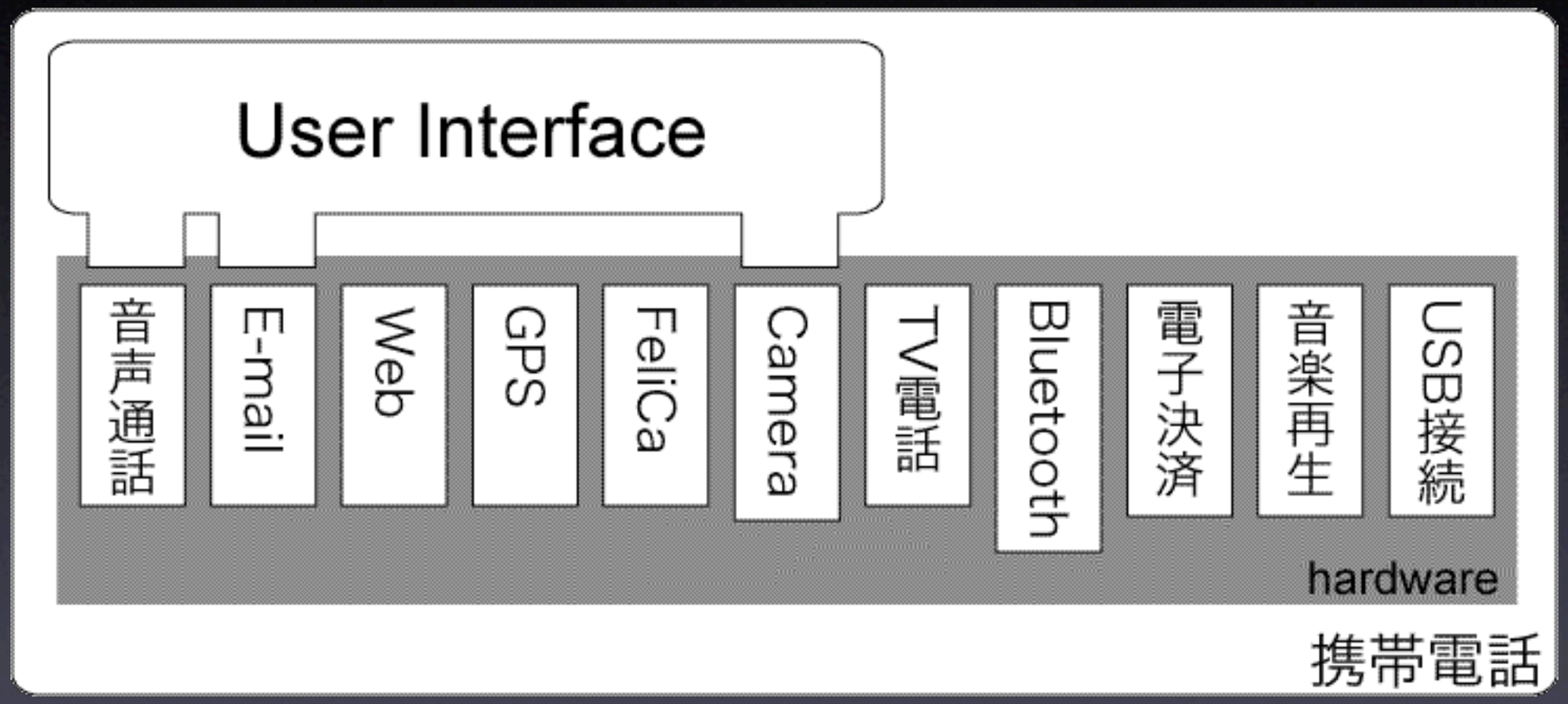
http://arena.nikkeibp.co.jp/rev/20051125/114434/index2.shtml

UIはSecurity向上に貢献



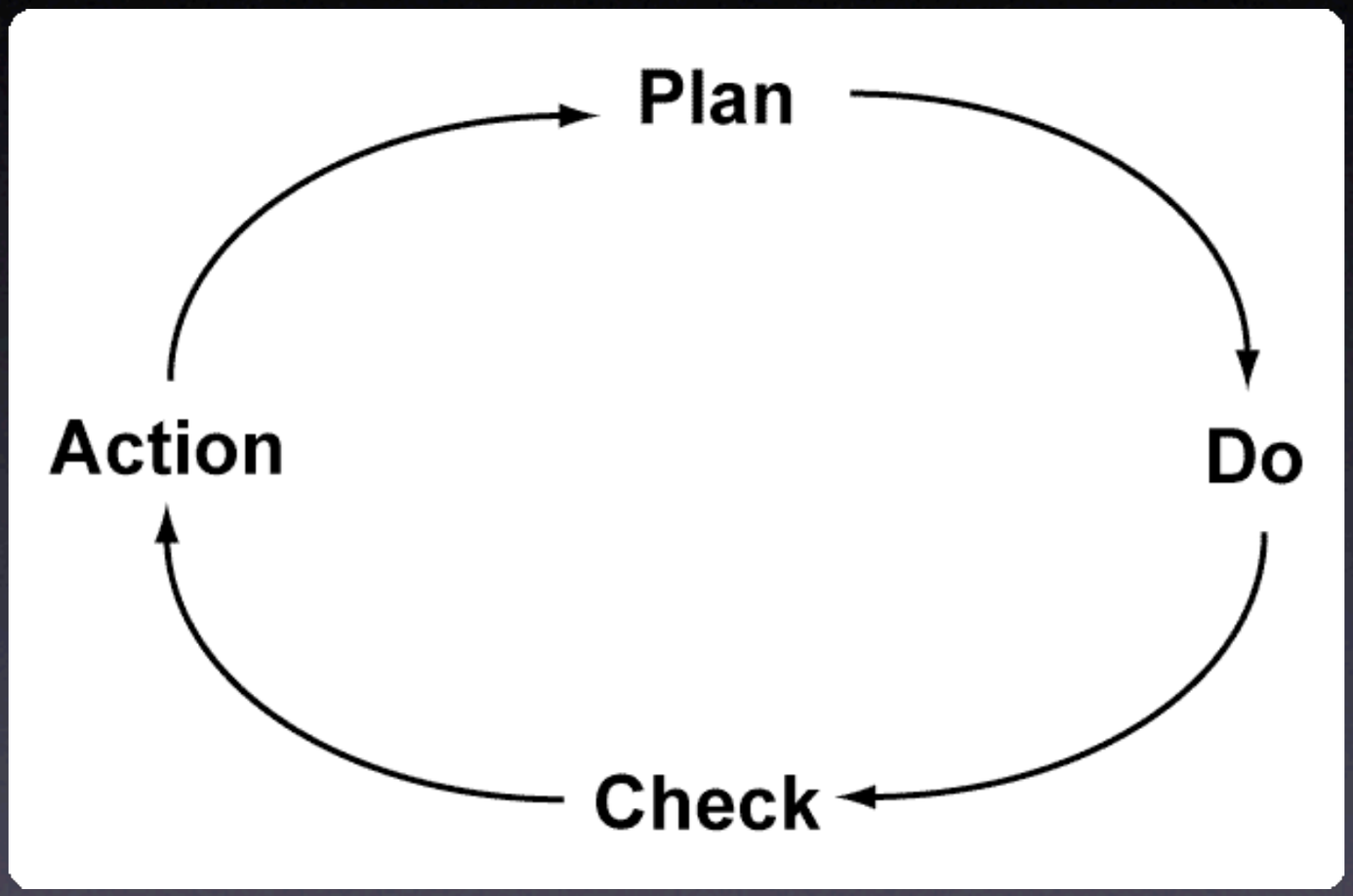
最近の携帯電話はテンキーで、端末が持つ
すべての機能を操作可能にしているため、複雑に

UIはSecurity向上に貢献(2)



User interfaceを入れ替え可能にし、ユーザの要望に応じた、機能の選択(無効化)を可能にして欲しい

PDCAサイクル



終わりはない．継続していく事が重要

Information Security Management System: ISO27001

参考文献

- 携帯電話関係の情報
  - http://netaro.ddo.jp/~zetaka/news/rlan/news.html
- 情報セキュリティ関連情報
  - http://www.csrs.is.uec.ac.jp/~zetaka/zetaka/news/sec/news.html
- ITは人を幸せにするか 全22章
  - http://kodansha.cplaza.ne.jp/digital/it/2003_06_11/index.html
- はびこる奇怪論理とその考察
  - http://www.mneme.co.jp/data/thesis.html