Twitterを用いた携帯端末における個人認証の多要素化に関する研究

電気通信大学 情報理工学部 総合情報学科
1010086 高浪 悟

研究背景

1. パスワードは覚えにくい！

2. 覚えにくいので様々なサービスで使いまわす

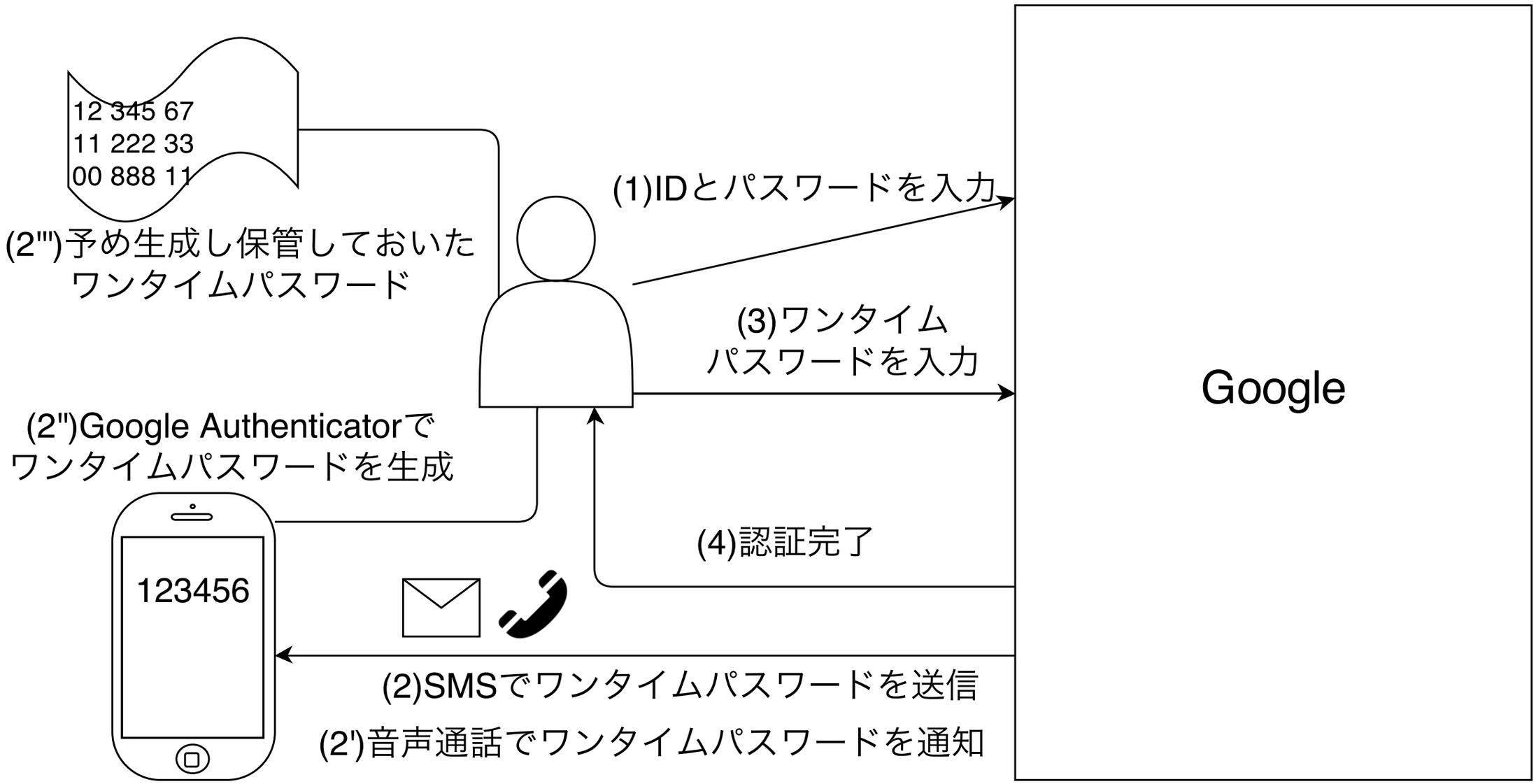
3. 一箇所で情報流出

4. 他のサービスでも不正ログイン

・ 多要素認証が金融やWebサービスの分野で普及

多要素認証

- Googleの場合



多要素認証の問題点

- **コスト**
  - サービス提供側→システムやハードウェアを導入
  - ユーザ側→ハードウェアを管理し持ち歩いたり，入力に手間がかかる
- **状況の制約**
  - SMSでワンタイムパスワード受信→携帯がオフラインの時は？
  - 指紋認証で二要素化→指を怪我したら…？

研究目的

- 多要素認証の問題点により導入しにくかった場面を多要素認証化する

➡ 携帯端末でのロック解除

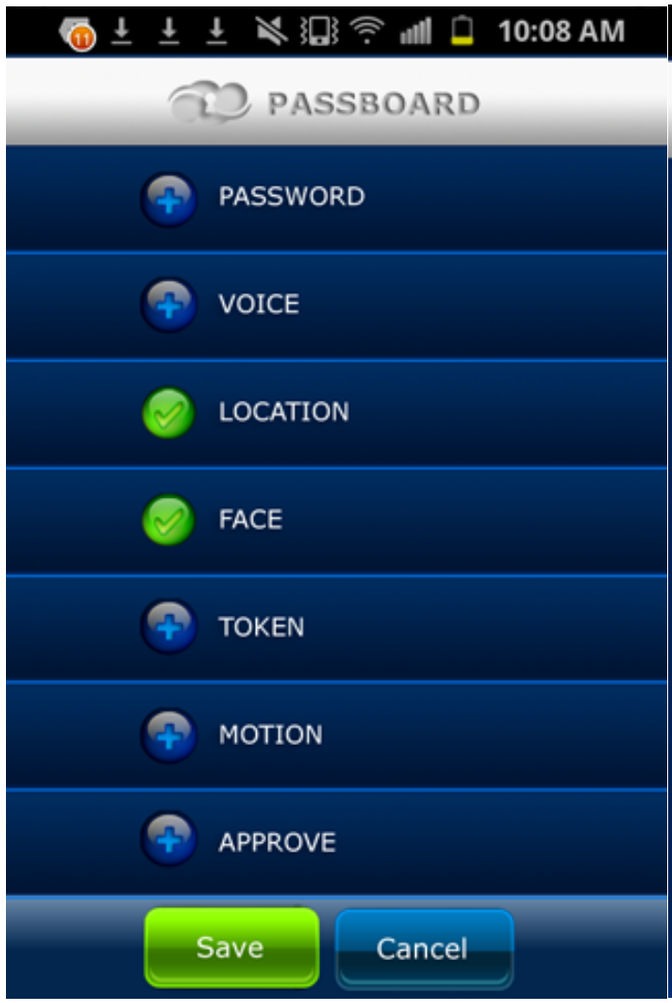
- 既存の認証よりも利便性に配慮

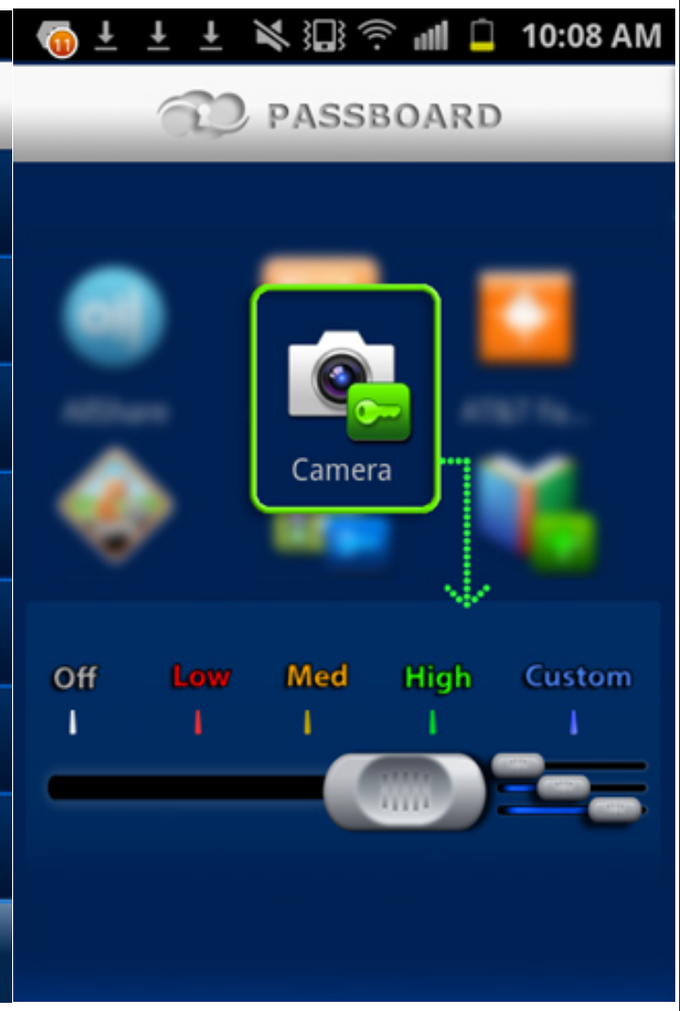
➡ ライフログやSNSが利用できるのでは？

既存手法(1)

Passboard

- 複数の認証要素を組み合わせられる
- アプリごとにロックを設定可能
- 外部環境(明るさや騒音)などによって認証の要素を変化
- Android/iPhone対応

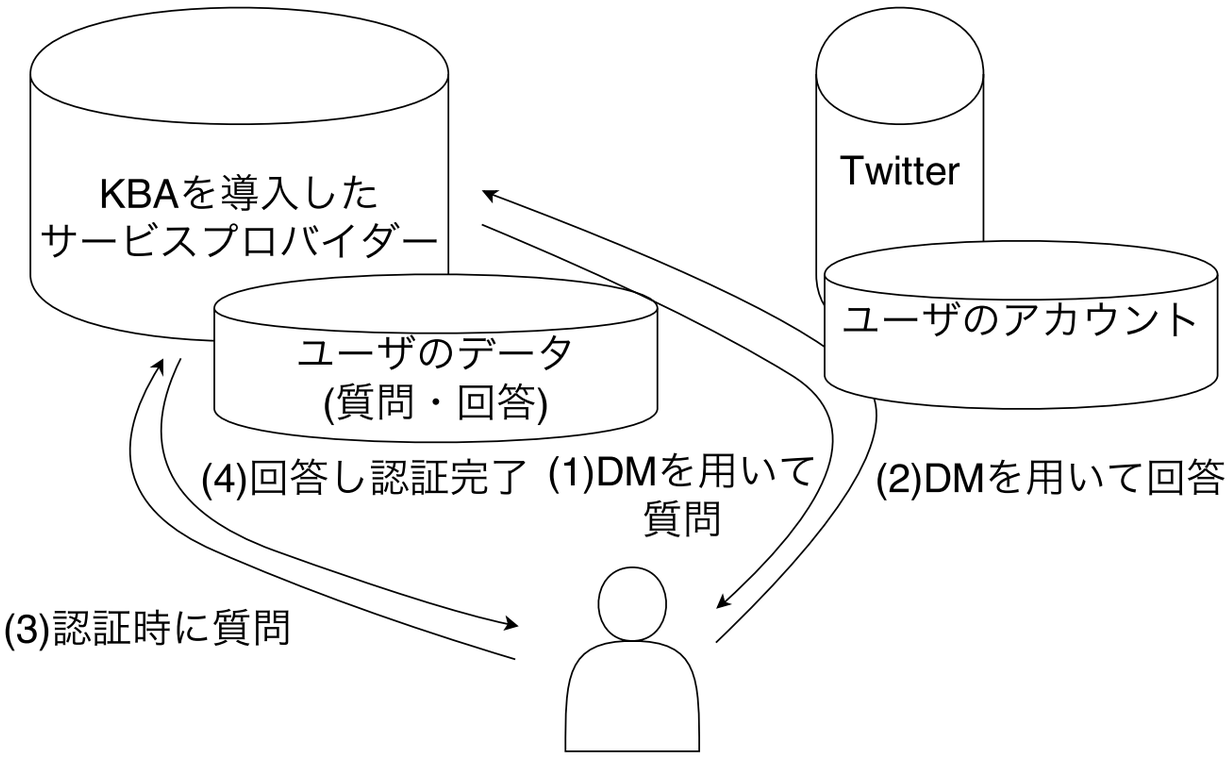




既存手法(2)

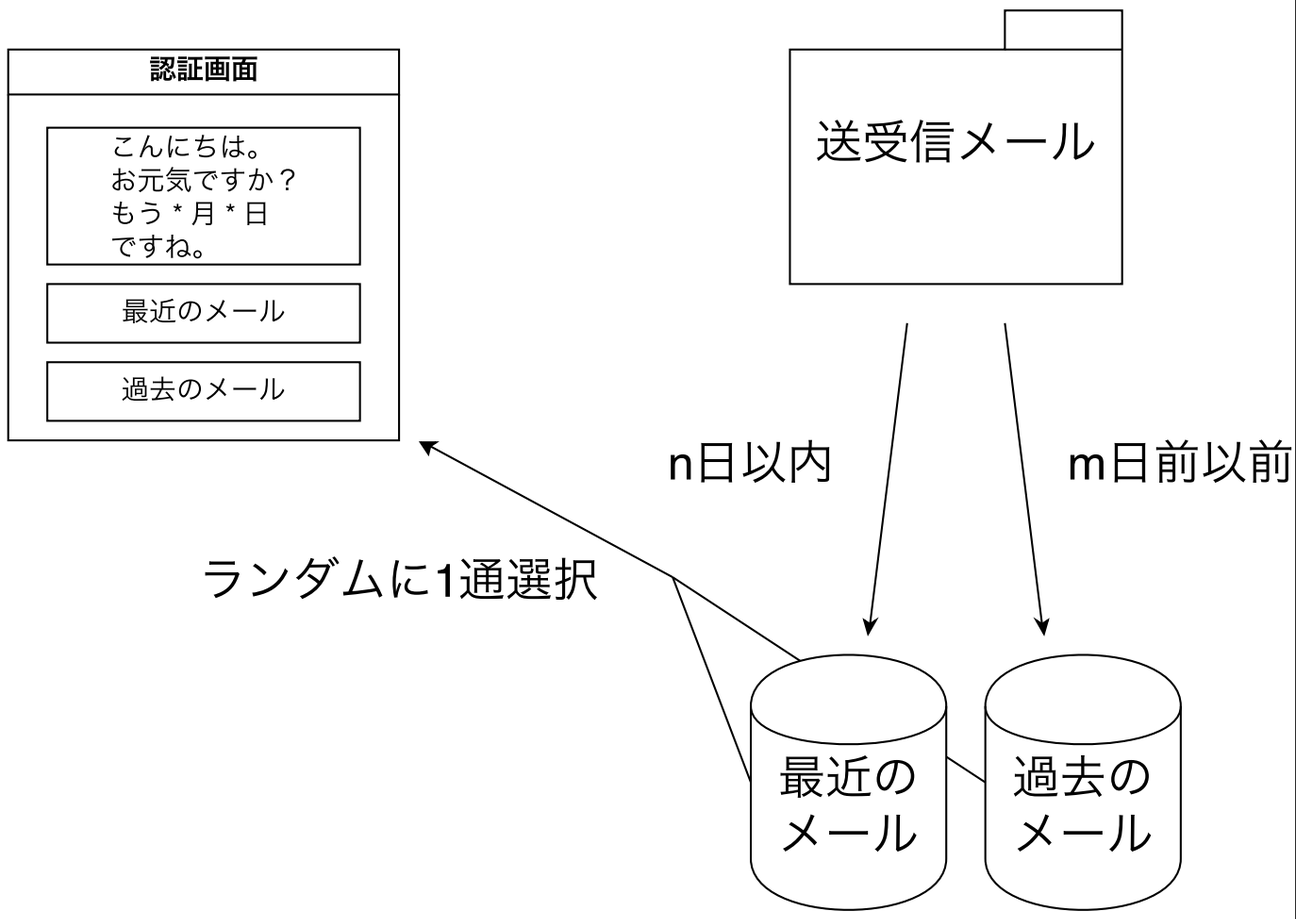
KBA(Knowledge Based Authentication)

- Twitterのメッセージ機能を利用し，秘密の質問を定期的に更新
- 質問内容は「○月△日にランチは何を食べたか」といったもの
- Twitterを使う理由が希薄，答えるのが面倒



既存手法(3)

- メールを用いた認証
- 「最近の」メールか「過去の」メールかを回答させる
- 最近とも過去ともいえる曖昧な時期のメールを弾くことで認証成功率を向上
- 見られたくないメールが認証時に表示されてしまう恐れ



提案手法

- ライフログやSNSの情報を利用
  - Twitter：ライフログであり緩い繋がりを持つSNSでもある
    - 自分の投稿(ツイート)を利用した3種類の秘密情報の設定方法
- 携帯端末への導入
  - Apple iOSで実装

手動で秘密情報を設定

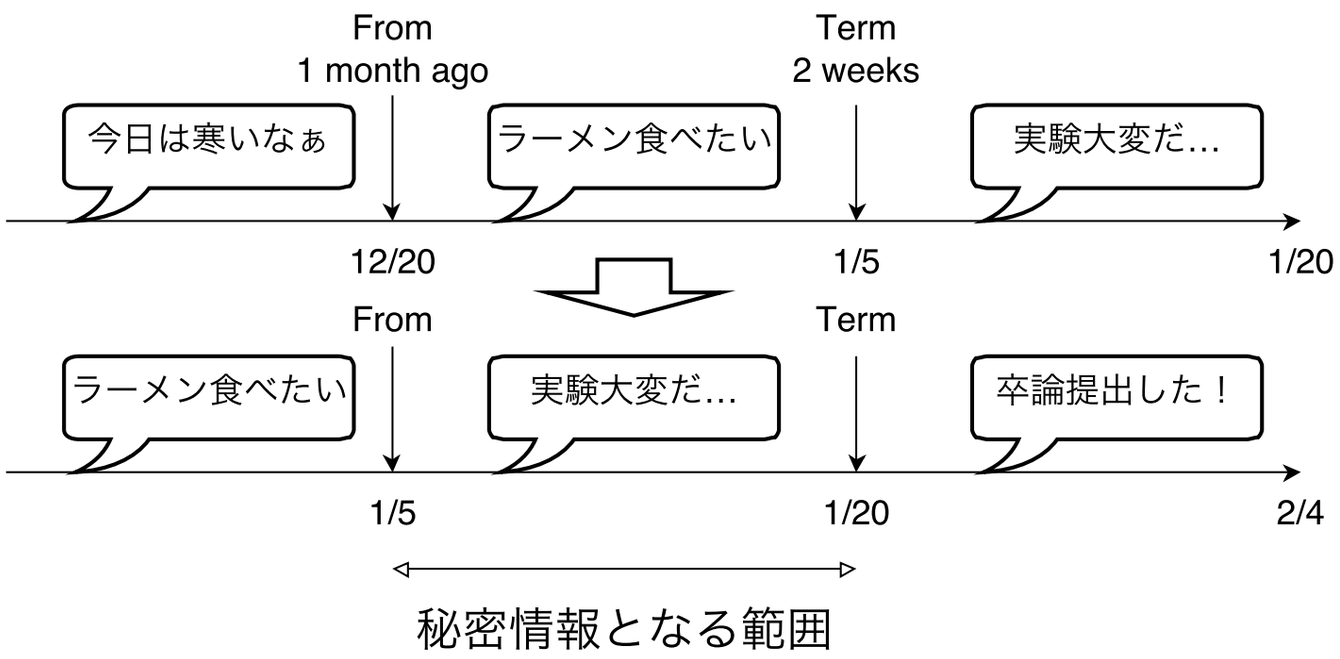
Manual Mode

- 最新200件の中から固定で一つ選択

自動で秘密情報を設定(1)

Auto Mode Type Term

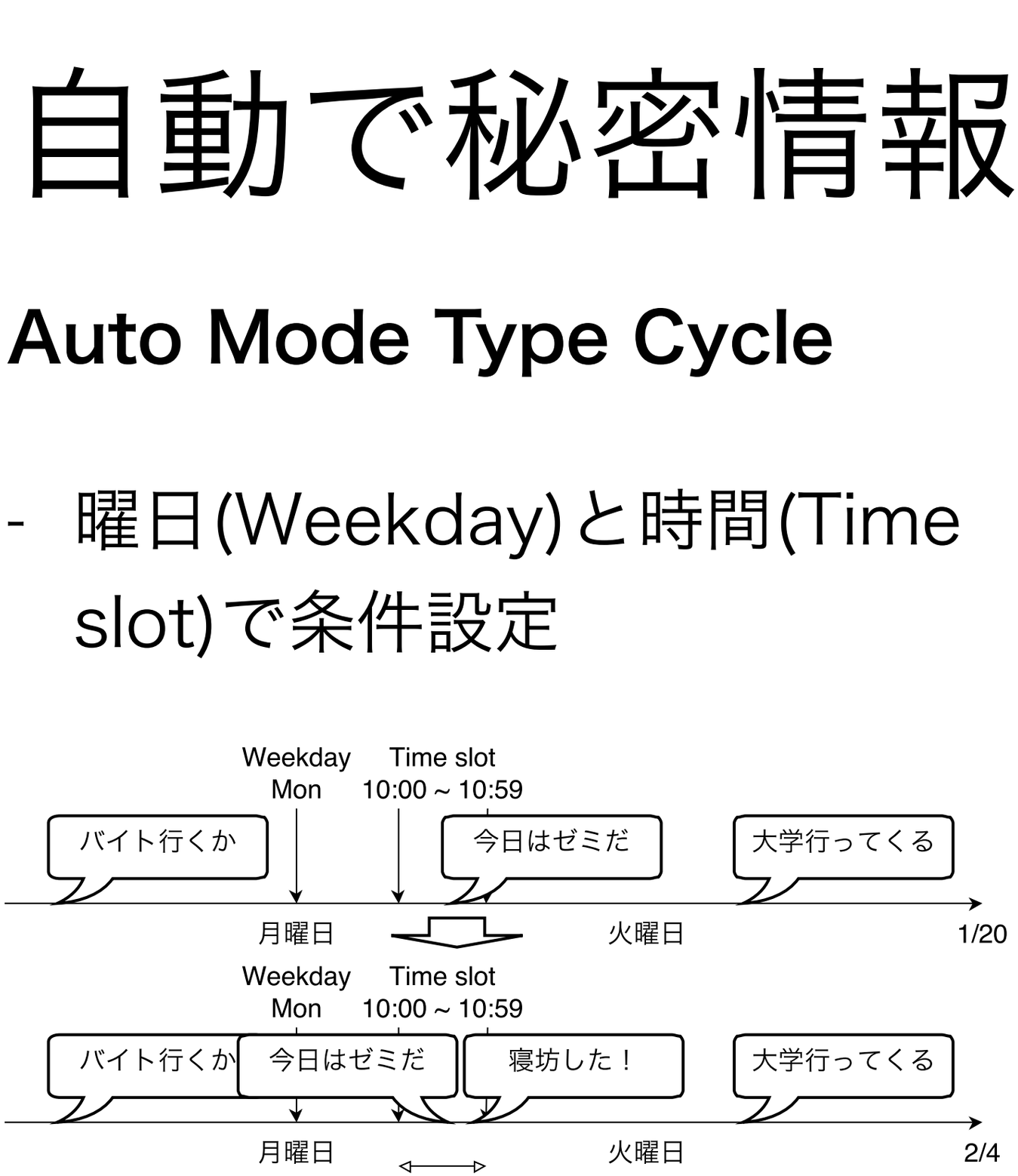
- 何日前(From)から何日間(Term)で条件設定



自動で秘密情報を設定(2)

Auto Mode Type Cycle

- 曜日(Weekday)と時間(Time slot)で条件設定

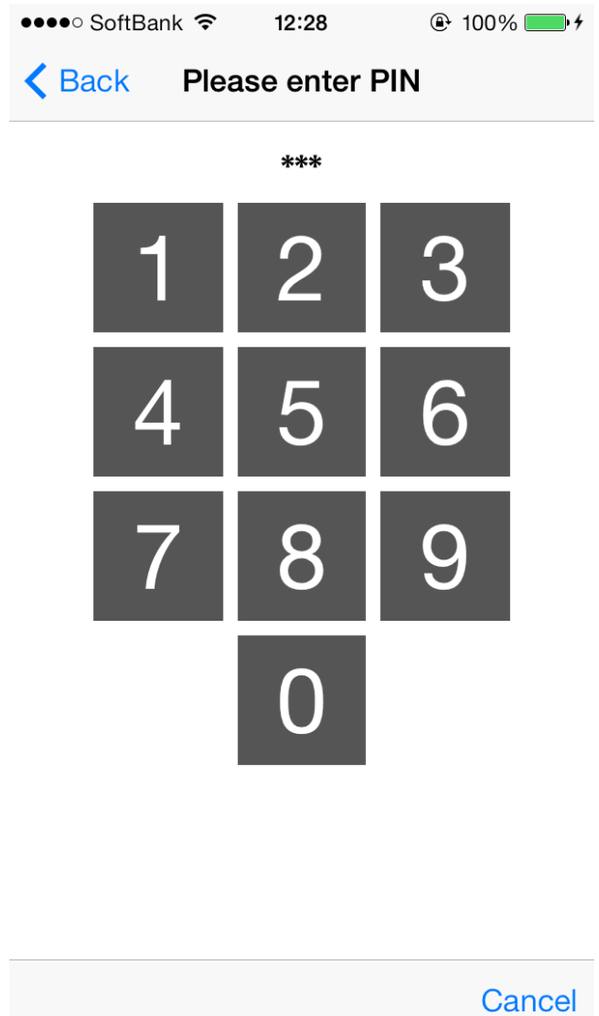


秘密情報となる範囲

認証操作

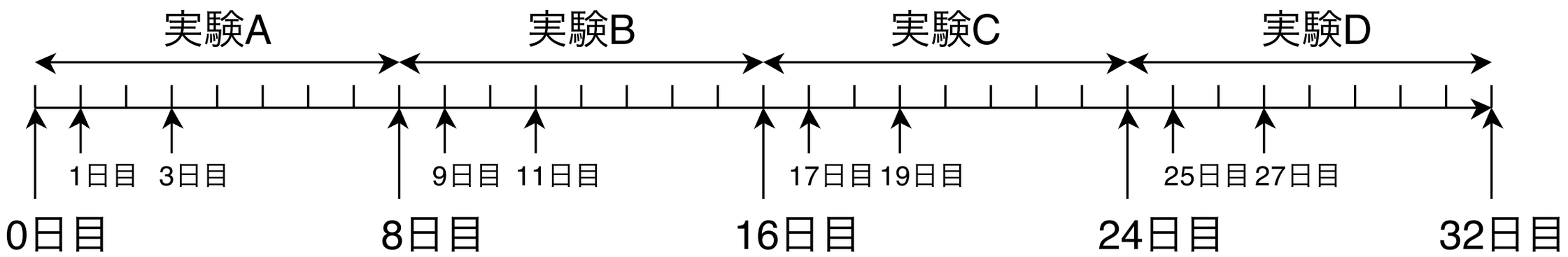
- iOSのロック解除操作を利用(実験用に再現)
  - ユーザが既に慣れている操作を使用

スライドで選択
+遷移



実験方法

- 3種類の設定方法(パターン)+5桁のPIN認証で実験
  - 1パターンにつき8日間(設定した日から0，1，3，8日目に実施)
  - それぞれのパターンが重複しないように，順番に偏りがないように実施



スケジュール例

実験結果

・ 被験者数15人(男性12人，女性3人)

	認証成功率(%)	認証時間(秒)
Manual Mode	94.12	10.74
Auto Mode Type Term	51.79	22.14
Auto Mode Type Cycle	27.59	22.95
PIN	96.08	2.55

考察

- 手動で設定(Manual Mode)では，5桁のPIN認証と同程度の認証成功率

- 自動で設定の2種はどちらも認証成功率が低い

  - 設定条件は覚えているものの，当てはまるツイートを思い出せない人が多数

- 認証時間ではPIN認証に遠く(5-10倍)及ばず…

今後の課題

- 設定は覚えているが当てはまるツイートが分からない

  ➡ 既存手法と同じように，曖昧なものを取り除く

- 認証時間の長さ

  ➡ 2択のような答えやすい選択肢を複数回繰り返す

まとめ

- 多要素認証が普及
  - しかしコストと利用できる環境に問題有り
- 安全性と利便性の両立を目指した多要素認証の提案
  - PIN認証と比較して安全性を向上可能
  - 自動での秘密情報設定は改善の余地あり
- CSS2013でデモ発表済み

参考文献

[1] PASSBAN, 2014-01-25. http://www.passban.com/.

[2] Tomofumi Nemoto, Kyohei Furukawa, and Manabu Okamoto. Poster: Knowledge-Based Authentication using Twitter. Symposium On Usable Privacy and Security 2011, 2011.

[3] 西垣 正勝 and 小池 誠. ユーザの生活履歴を用いた認証方式 : 電子メール履歴認証システム (ネットワークセキュリティ). 情報処理学会論文誌, 47(3):945–956, mar 2006.