

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

- ・ スマートフォンやタブレット端末の普及
 - 個人情報やアプリケーションのデータが集約
→ 携帯端末における個人認証の強化が必要
- ・ 多要素認証が金融やWebサービスなどで普及
 - 携帯端末向けの多要素認証を実現する
アプリケーションも出てきている
→ 需要は存在する

携帯端末向け多要素認証例

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/iOS対応



多要素認証の問題点

- ・コスト
 - ・サービス提供側→導入コスト
 - ・ユーザ側→管理コスト, 入力負担
- ・状況の制約
 - ・生体認証や所有物認証の欠点はそのまま引き継がれるため, 使えない状況が発生しやすい

研究目的

- 携帯端末の個人認証強化
 - 多要素認証化
 - * 知識認証を活用し導入コストや制約を低減
 - * 既存のパスワード認証より手間はかかる
 - しかし覚えやすさに配慮
 - 秘密情報も作りやすく
 - 入力操作の負担に配慮

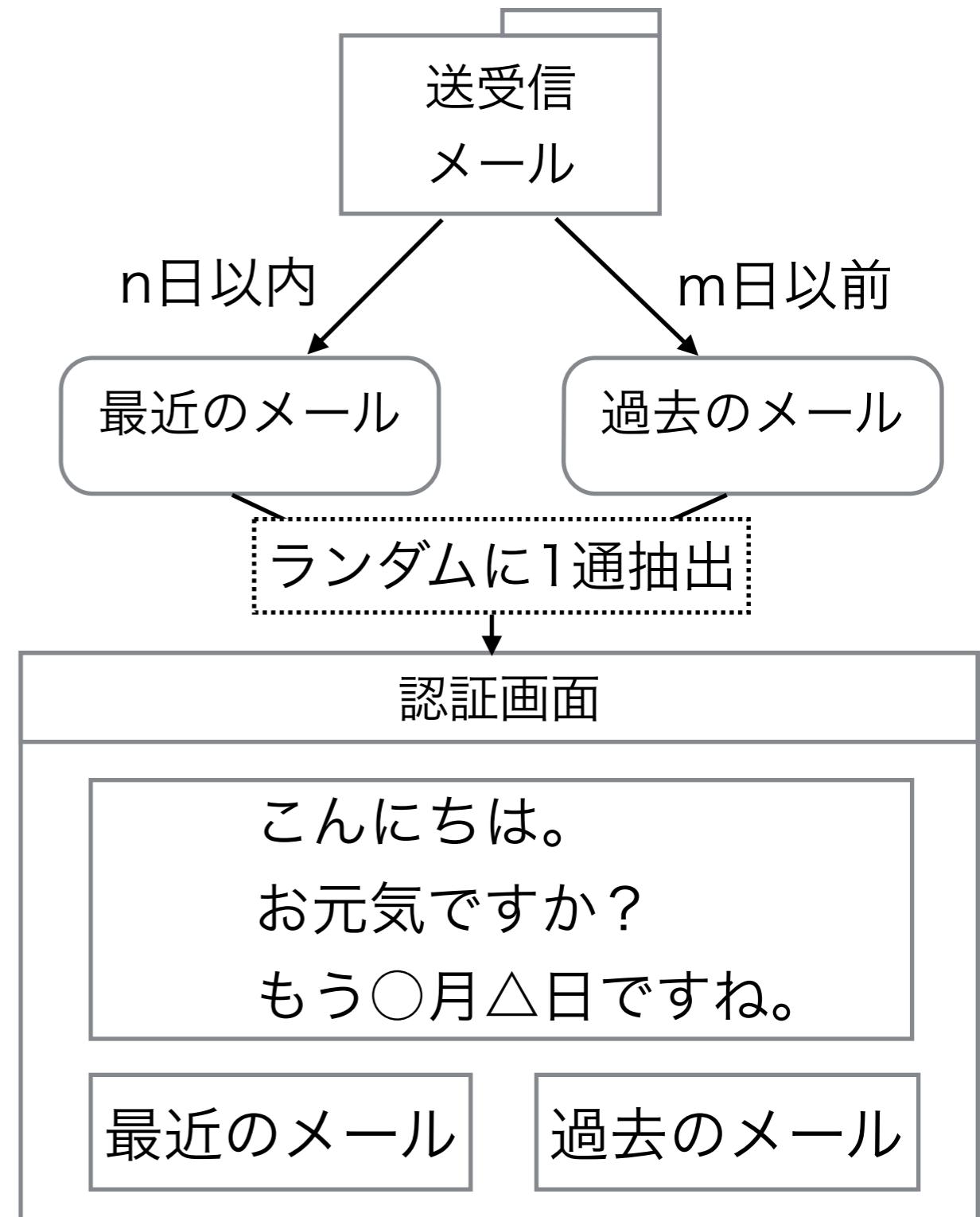
提案手法

- ・ ユーザへの記憶負担に配慮
 - 新たに覚えるのではなく既知の情報を活用
 - ライフログやSNSの情報を利用
 - Twitterの自分の投稿(ツイート)
- ・ ユーザが新たな操作を覚える負担に配慮
 - 既存操作を利用
 - iOSの通知機能とその選択動作

既存手法

ライフログとして電子メールを用いた認証

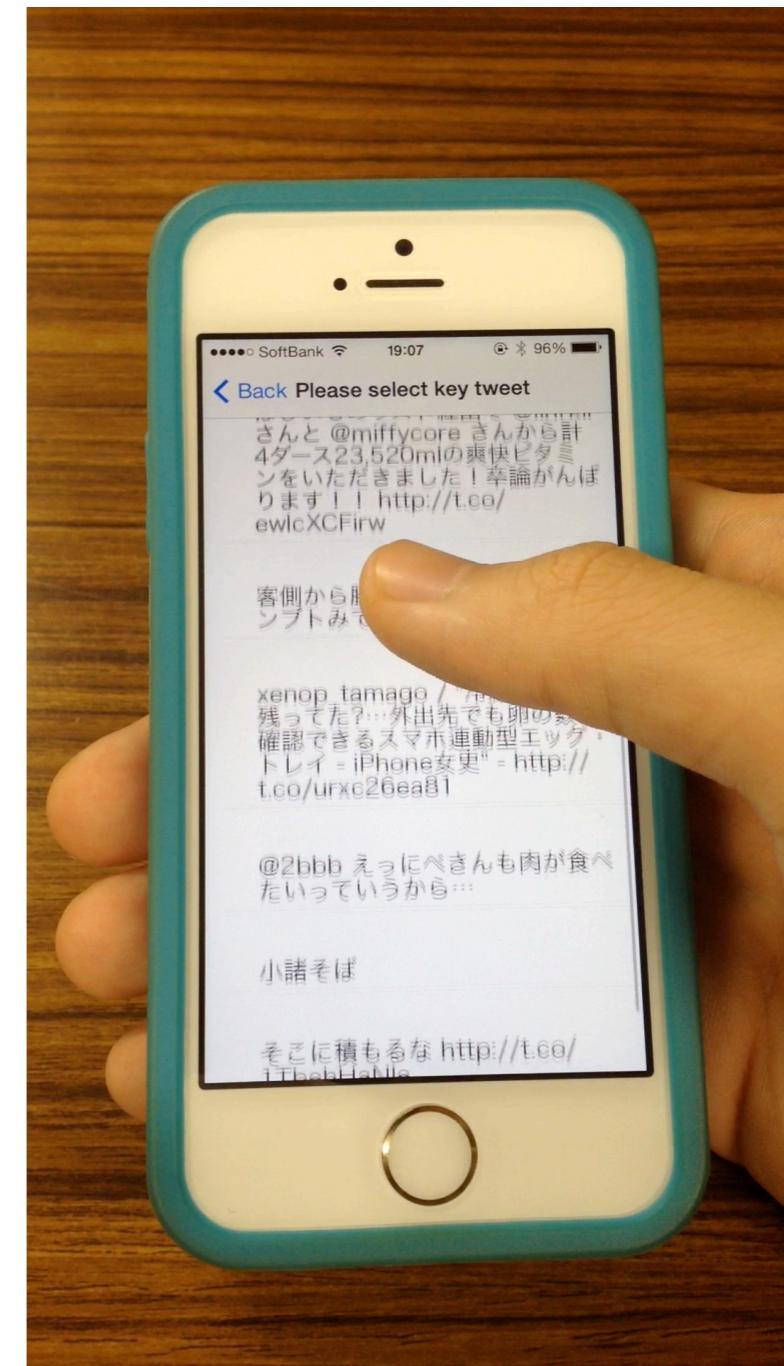
- ・ 最近のメールか過去のメールかを回答
- ・ 曖昧な時期のメールを弾くことで認証成功率を向上
- ・ 見られたくないメールが認証時に表示される恐れ



認証操作



iOS標準のロック解除操作



本システムの認証操作

秘密情報の設定

- ・ 設定方法は2種類
 - 手動での設定(固定)

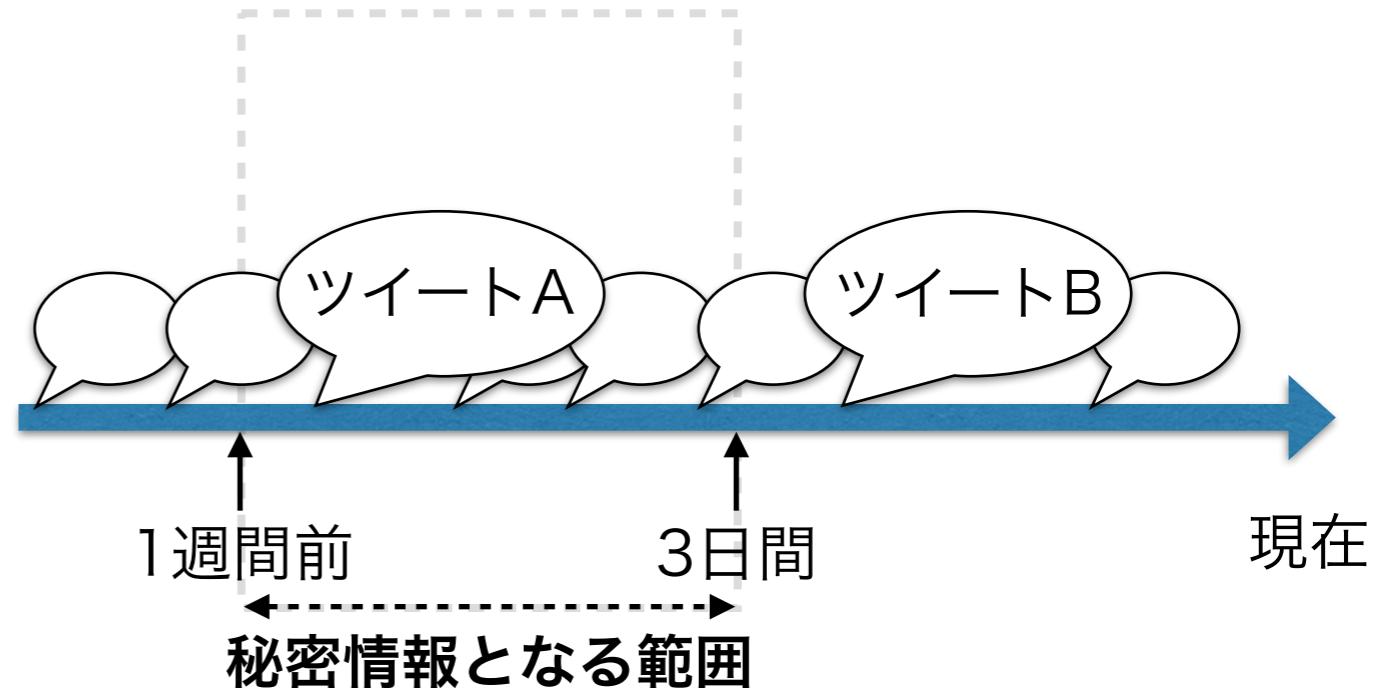
Manual Mode

- ・ 最新200件の中から固定で一つ選択
- 自動での設定(可変)
 - ・ 時系列における範囲を指定し秘密情報が可変に
→ 定期変更する必要がなくなる

秘密情報の自動設定

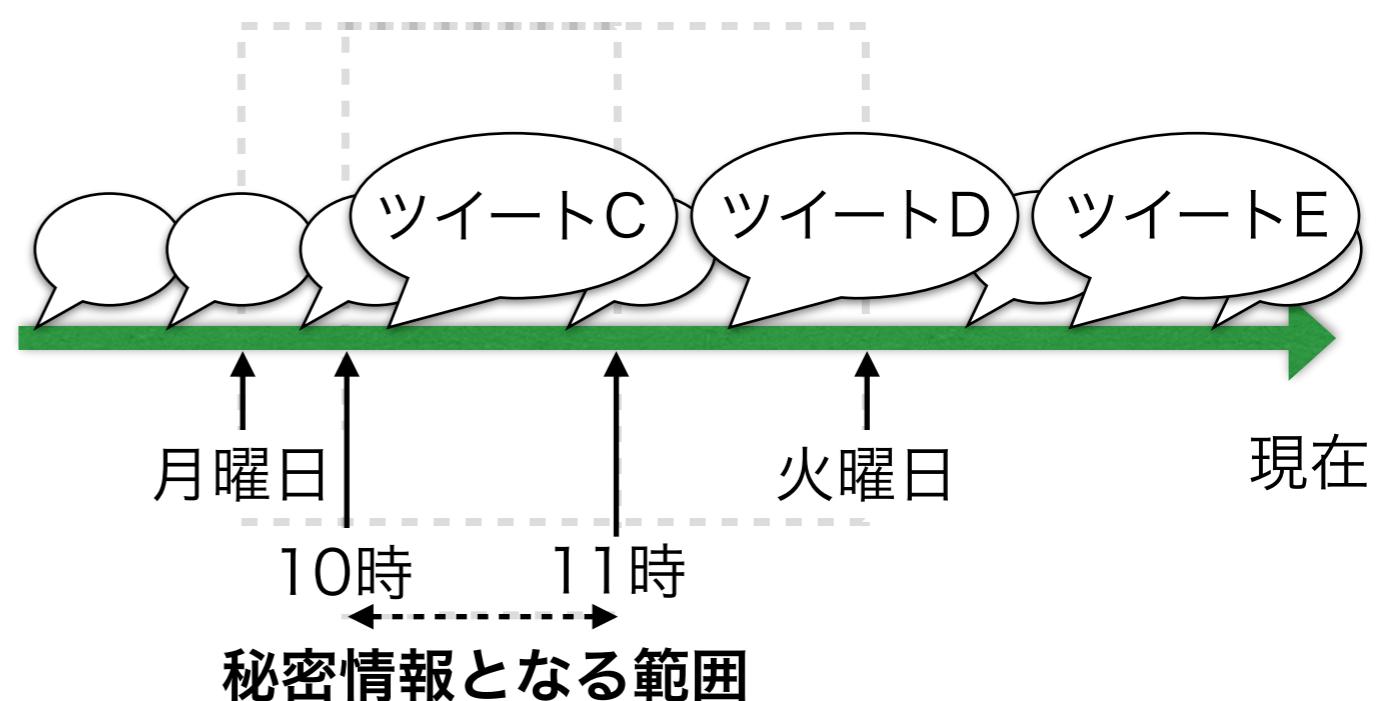
Auto Mode Type Term

- どのくらい前から
どのくらいの期間



Auto Mode Type Cycle

- 曜日と時間

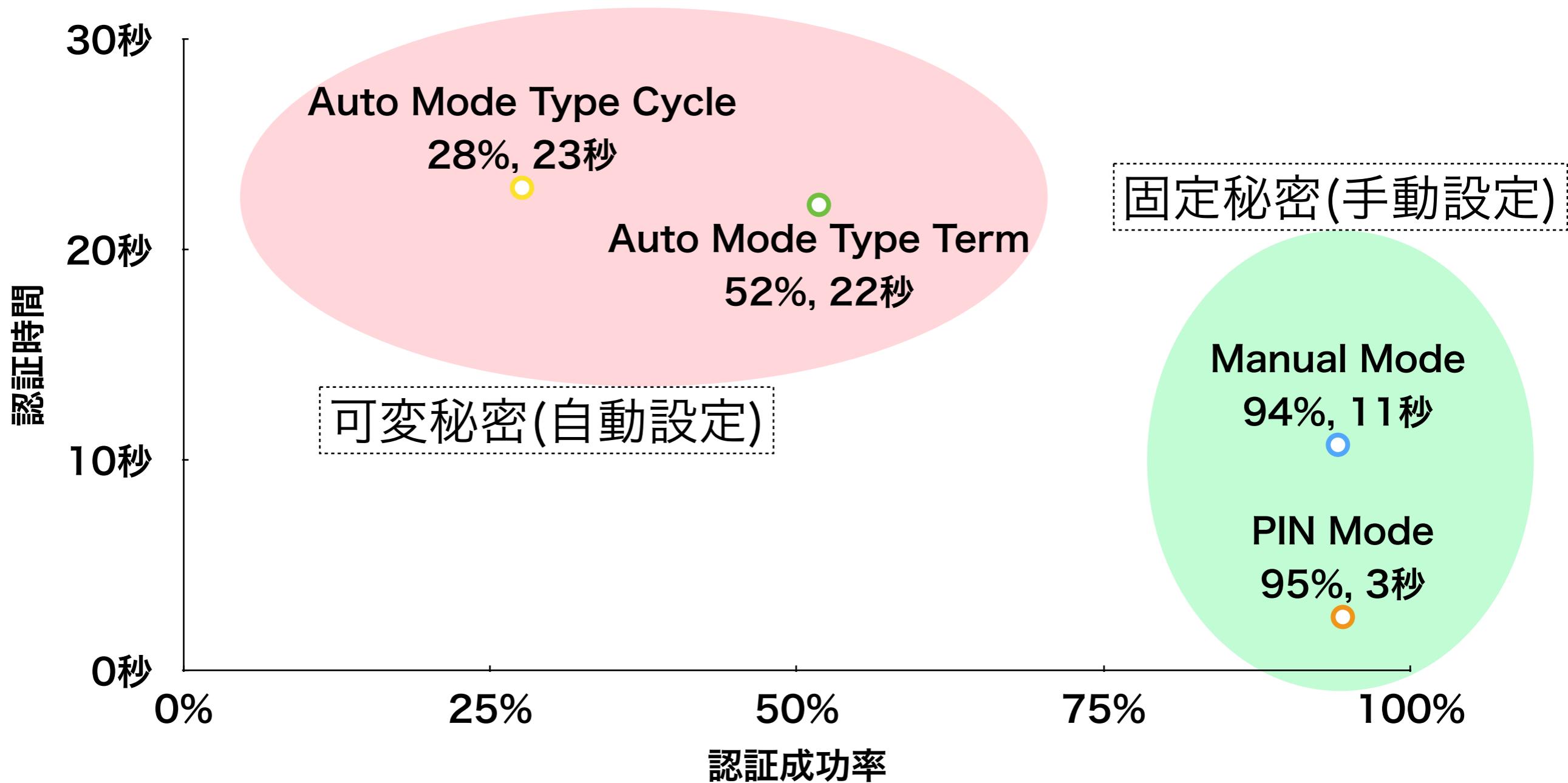


実験方法

- ・ 4パターンの秘密
 - ・ 3種類の設定方法+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
- ・ 被験者数は15人

	男性	女性
20歳代	10人	1人
30歳代	1人	2人
40歳代	1人	-

実験結果



考察

- Manual Mode
 - 5桁のPIN認証と同程度の認証成功率
 - 被験者アンケートでは体感時間や利便性についてPIN認証と同等の評価
- Auto Mode
 - 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
 - 既存手法と同様に、曖昧なものを取り除く

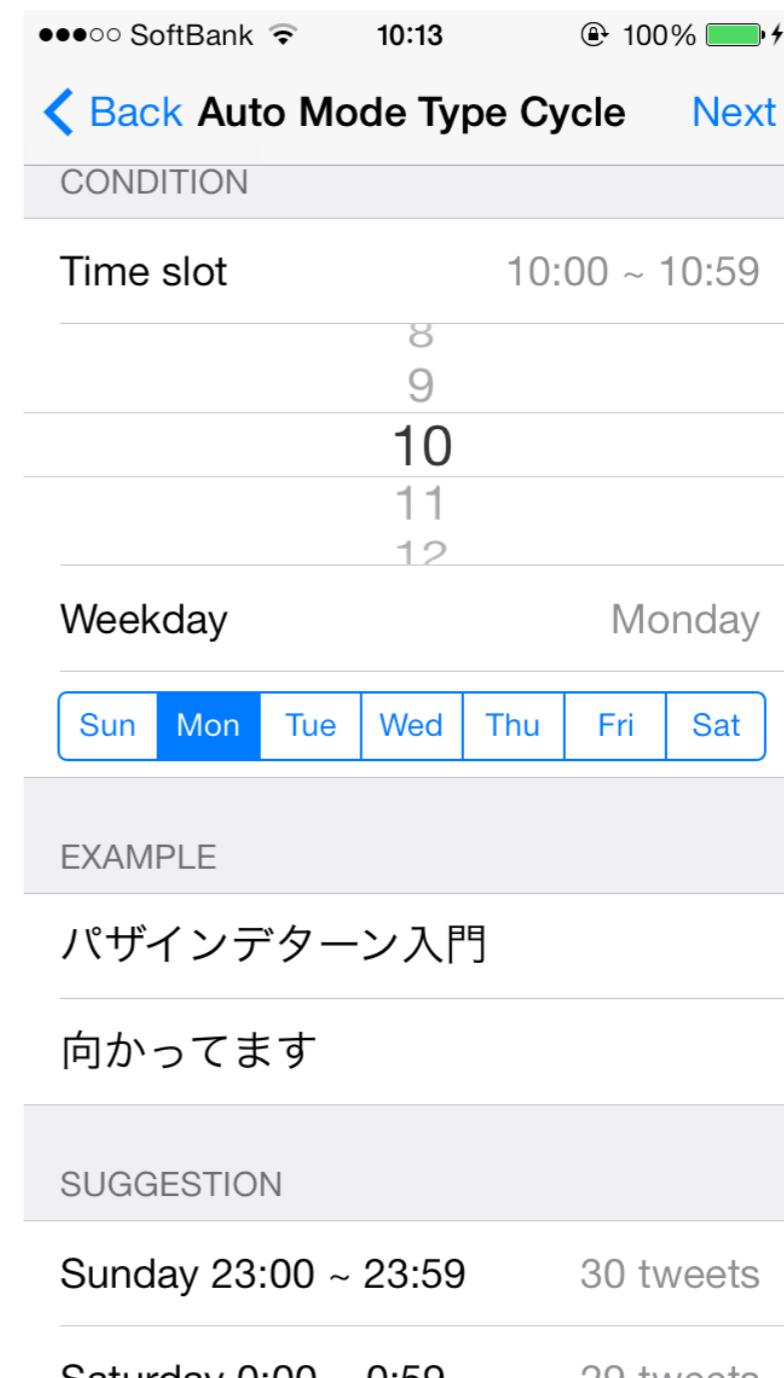
まとめ

- ・ 高機能な携帯端末が普及
 - 個人認証を強化する必要
- ・ 携帯端末における個人認証の強化を目指した知識と知識による二要素認証の提案
 - 能動的に発信した情報と既存の携帯端末に存在する操作で利用者の負担に配慮
 - 固定秘密であればPIN認証と比べて遜色のない結果
- ・ 学会発表
 - ・ Computer Security Symposium 2013でポスター発表

参考文献

- [1] PASSBAN, 2014-01-25. [http://www.passban.com/.](http://www.passban.com/)
- [2] 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.

自動方式2種の設定画面



実験結果(表)

	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	94.34	2.56