

バイオメトリクスセキュリティ評価に関する研究

バイオメトリクスの現状

セキュリティに関する
国際標準化の動き
(ISO/IEC 19792, 24745など)

セキュリティの
定式化、理論体系は
まだまだ発展途上

身近になった バイオメトリクス

- ▶ 銀行 ATM の預金者認証
- ▶ PC のログイン
- ▶ 従業員の勤怠管理
- ▶ 病院での従業員認証や患者認証
- ▶ 空港の出入国管理
- ▶ 試験の受験者認証 など

研究目的

第三者評価体制
の実現

セキュリティ評価技術や
理論をリードする研究

既知のセキュリティ評価に対する
検討、研究はもちろん
未知の新しいセキュリティ問題と
その評価手法の研究開発

ウルフ攻撃に対するセキュリティ研究

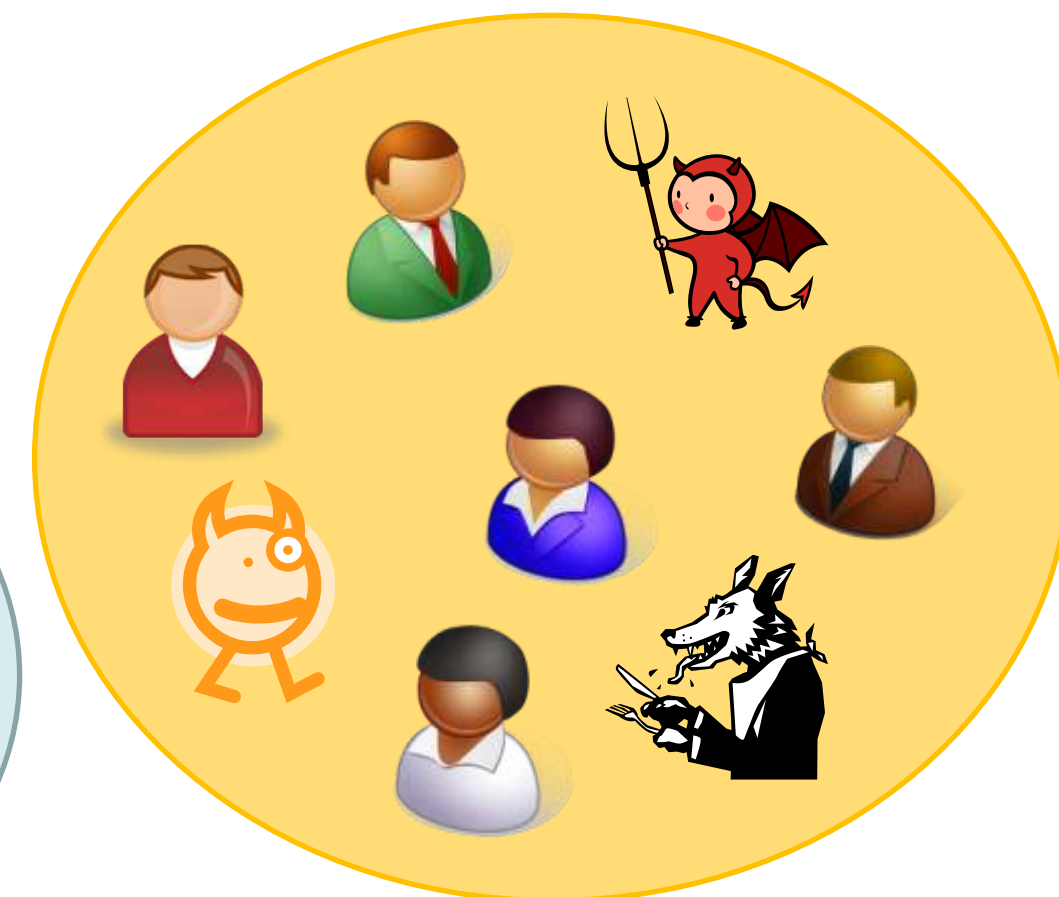
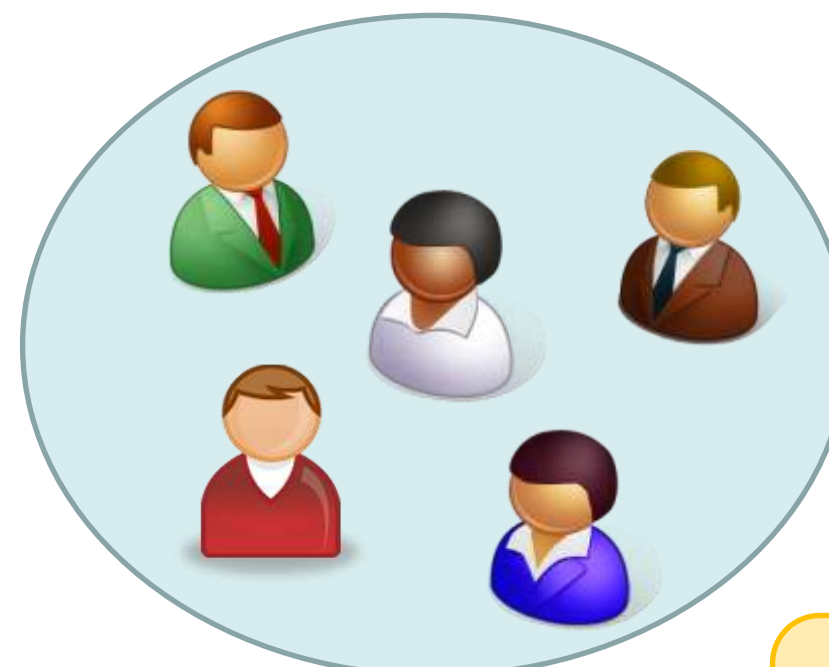
他人受入率 (FAR) だけでは故意のなりすまし攻撃
に対するセキュリティ評価ができない !!

いろいろなモダリティでの FAR と WAP

	指紋 (マニューシャ)	指静脈パターン	虹彩
FAR	2^{-26}	0.00145	10^{-6}
WAP	0.6	1	10^{-3}

(各数値の根拠は配布資料の参考文献をご参照ください)

FAR
正規ユーザ間の
誤一致確率



WAP

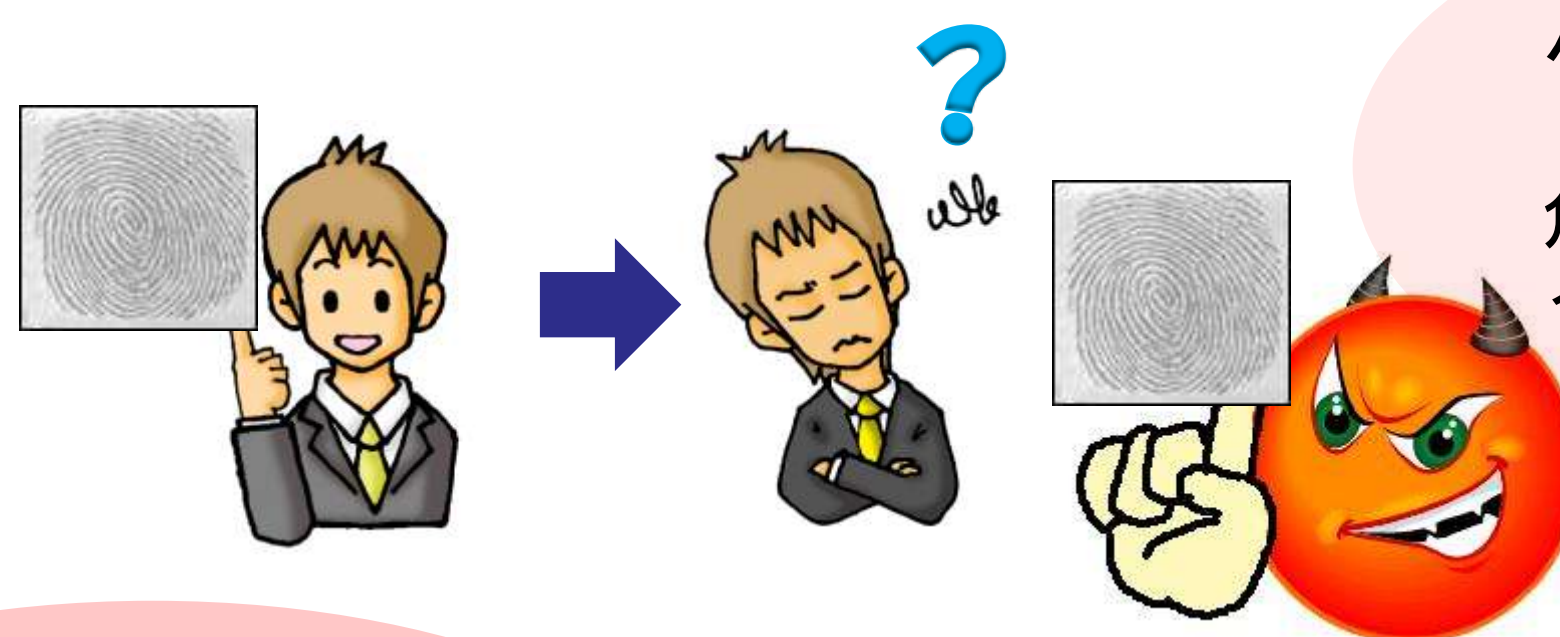
あらゆるサンプルを用いたなりすまし
攻撃を考慮した攻撃成功確率の最大値

なりすまし攻撃に対するより強いセキュリティ評価のための評価尺度
ウルフ攻撃確率 (WAP) は RCIS より提案されました。

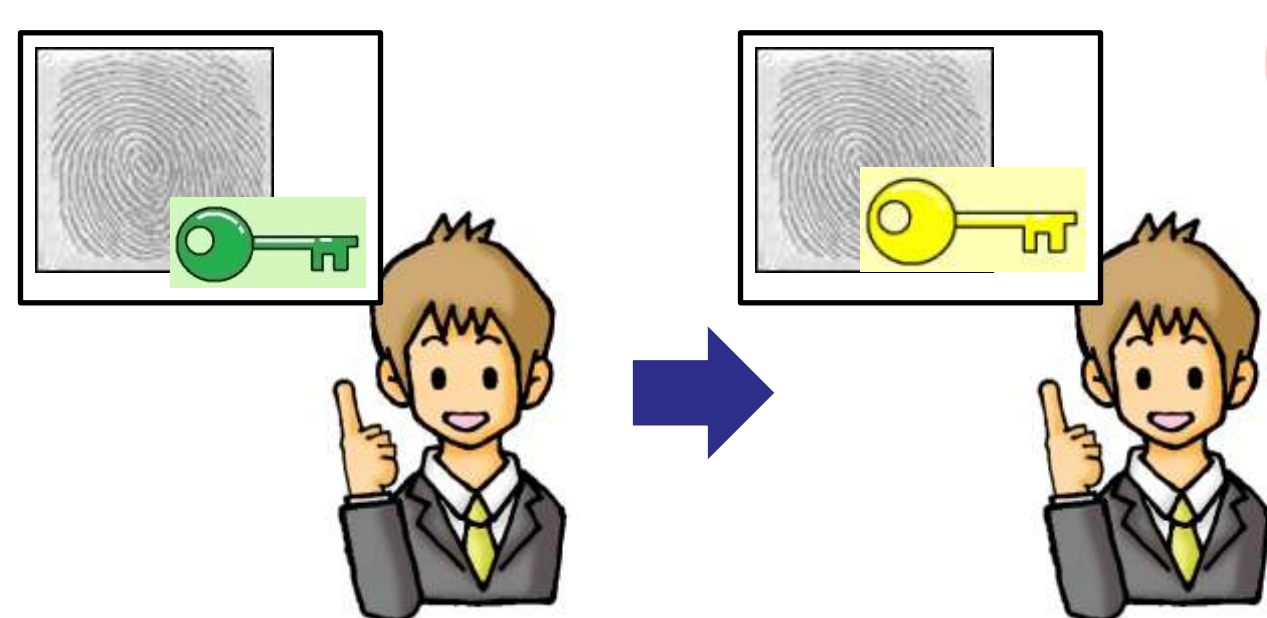
ウルフ攻撃に対して安全で、かつ高精度、高速なバイオメトリクス認証の研究、開発を行っています。

キャンセルラブルバイオメトリクスのセキュリティ研究

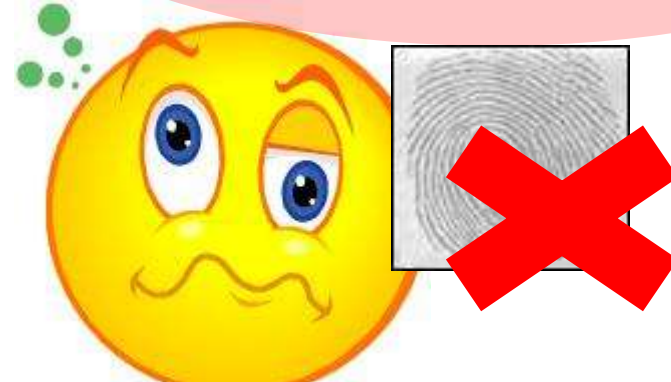
個人から切り離せないバイオメトリクス
情報はパスワードやトークンのような
自由な更新が困難であるという問題が
あります。



バイオメトリクス情報
が盗まれたり、その
危険性が高まった場
合など更新が困難。



バイオメトリクス情報を
暗号化して登録するなど
の工夫により、更新可能
な認証方法を実現。



バイオメトリクス情報を用いながらも、パ
スワードやトークンのように入力情報や
登録情報を更新できる (キャンセルラブル
な) 認証技術とそのセキュリティを研究し
ています。

バイOMETRICSのセキュリティ評価 に関する研究

井沼 学

■ 身近になったバイOMETRICS認証

- 銀行ATM
- PCログイン
- 出入国管理
- 病院の職員、患者認証
など

■ セキュリティ評価は発展途上

- セキュリティの定式化、理論体系の整理
- セキュリティ要件や評価手法の標準化
- 第3者評価機関設立などの評価体制の構築

バイOMETRICSセキュリティ 研究の主な目的とテーマ

主な研究目的

- 評価技術と理論をリードする研究
 - 既存手法のセキュリティ評価はもちろん、新しいセキュリティの問題の発見、評価手法の研究
 - バイOMETRICS情報の特性を生かした、安全で利便性の高い個人認証技術の開発

主な研究テーマ

- なりすまし攻撃に対するセキュリティ
 - ウルフ攻撃に対するセキュリティの研究
- バイOMETRICS情報の漏えいに対するセキュリティ
 - キャンセラブルバイOMETRICSのセキュリティの研究

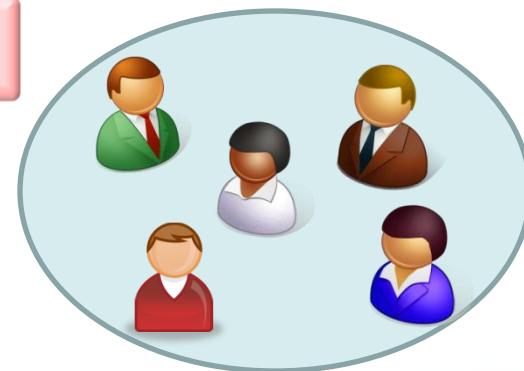
ウルフ攻撃に対する セキュリティの研究

既存の他人受入率 (FAR) による評価では不十分!

	指紋 (マニューシャ)	指静脈 パターン	虹彩
FAR	2^{-26}	0.00145	10^{-6}
WAP	0.6	1	10^{-3}

(各数値の根拠は配布資料の文献を参照ください)

- 新しい評価尺度 **ウルフ攻撃確率(WAP)** の提案
FAR ではとらえきれない脆弱性の存在が示唆されています
- ウルフ攻撃に対して安全なアルゴリズム構成の枠組みを提案
- 安全で、高精度で、高速なバイオメトリクス認証の研究開発



FAR: 正規ユーザ間の誤一致確率



WAP

あらゆるサンプルを用いたなりすまし攻撃の成功確率の最大値

キャンセラブルバイオメトリクス のセキュリティの研究

バイオメトリクス情報は更新が困難!

個人から切り離せないバイオメトリクス情報は、パスワードやトークンのような自由な更新が困難であるという問題があります

■ 安全かつ更新可能なバイオメトリクス認証技術の研究開発

- 認証モデル、セキュリティの定式化
- 暗号理論、符号理論を用いる手法を提案し、安全性を証明

■ 指紋、虹彩、署名など各モダリティに対する応用手法の開発

■ ID 連携技術への応用

