RCIS
Research Center for Information Security

情報セキュリティ研究センター

Research Center for Information Security
井沼　学 **Manabu Inuma**

バイオメトリクスのセキュリティに関する研究

バイオメトリクスの現状

身近になったバイオメトリクス

- 出入国管理
- ATM の預金者認証
- 住居の入出管理
- 病院での従業員認証や患者認証　など

安全性評価理論や評価技術はまだ確立していない。

研究目的

■ 安全性評価手法の研究

安全性要件を定式化し、種々の認証アルゴリズムや攻撃に対する安全性を第三者が定量的に確認できる評価手法を研究、開発する。

■ 安全で高性能な認証方式の研究

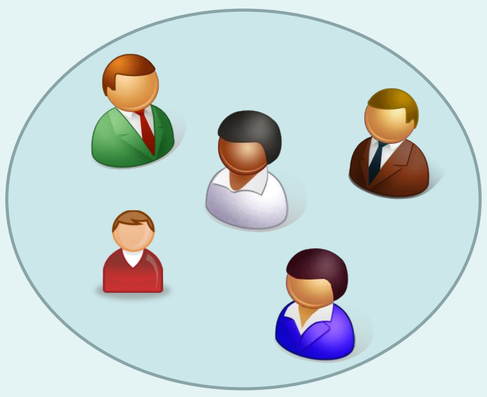
確立した手法によって安全性が定量的に評価できる高性能な認証方式の開発を行う。

ウルフ攻撃に対するセキュリティの研究

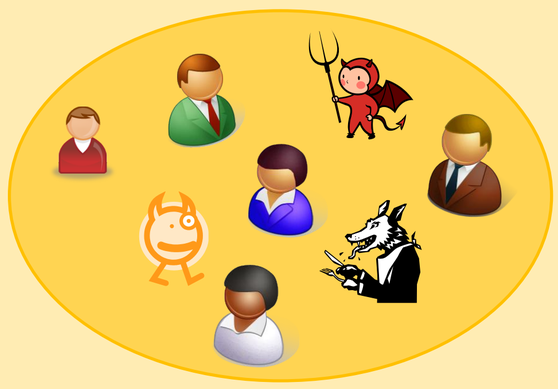
RCIS はウルフ攻撃確率（WAP）を提案し、従来の他人受入率（FAR）では捉えられなかった脆弱性の発見に成功した。

	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}

FAR
正規ユーザ間の誤一致確率



WAP
あらゆるサンプルによるなりすまし攻撃の成功確率の最大値

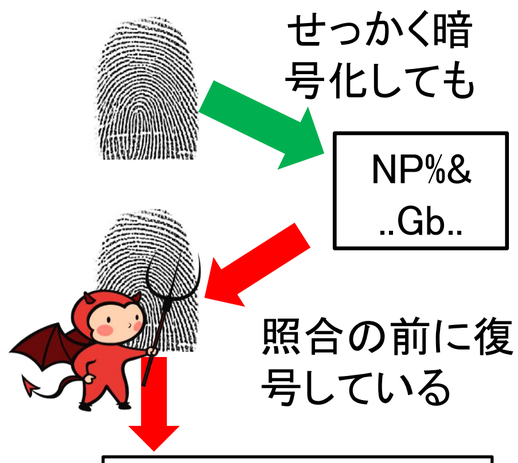


- ウルフ攻撃の理論研究や安全で効率のよい照合アルゴリズムの研究
- 評価技術確立のためのウルフ攻撃実験

キャンセラブルバイオメトリクスの研究

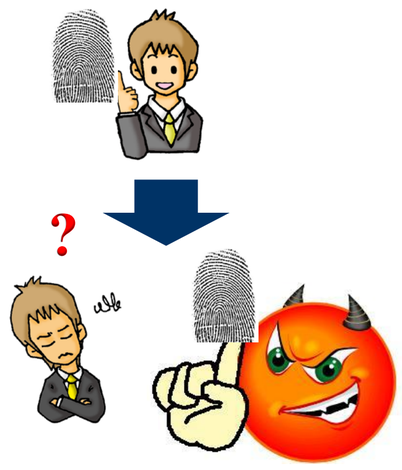
生体情報漏洩の問題

生体データを暗号化しても、照合の時には、元の生体データに復号して照合するため、不正な管理者などに生体情報を盗み取られる危険性がある。



更新困難性の問題

生体情報は本人と強く結びついた情報であり取り替えができないため、漏洩の危険にさらされた時に、自由に更新することができない。



いったん漏洩すると更新が自由にできない

■ 生体情報の保護と更新可能性を達成するバイオメトリクス認証方式の研究開発

- ■ 現実的な仮定のもとで実用的な安全性要件の定式化を行った。
- ■ 暗号理論と符号理論を用いた手法を提案した。

■ 国民が安全して利用できる国民認証インフラの実現

- ■ 登録情報からは生体情報が復元できない。
- ■ カードを落とすなど、万が一、秘密情報が漏洩しそうな場合には更新によって安全性を回復できる。