パネルディスカッション

司会：菊池　浩明（東海大）

パネラー

- 利用者認証研究者
  - 西垣 正勝（静岡大学）
- 暗号理論家
  - 尾形 わかは（東京工業大学）
- 生体情報研究者
  - 高橋 健太（日立製作所）
- 個人情報保護専門家
  - 新保 史生（筑波大学）

本パネルの目的

- 脅威に対する共通の問題意識を持つこと
- 様々なアプローチの長短所を認識すること
- 来るべき生体情報（の漏洩）時代に向け，
  今なすべきことの方向を明らかにすること

菊池の予言1

- ○年以内に，
  国内初の生体情報漏洩事件が起きる

理由1.

- 生体情報の導入が促進

理由2.

- 個人情報の付加価値が高まっている

個人情報流出問題で記者会見する
ソフトバンクグループの孫正義代表
http://www.asahi.com/special/yahoobb/TKY200402270346.html

理由3.

- なのに，誰も気がついていない
  （ここに参加している我々を除いて！）

  - そもそも，生体情報は個人情報なのか？

議題2.

- 生体情報はどこで記憶するべきか？

	ユーザ	サーバ
例	ICキャッシュカード 静脈をPINの代わり	図書館・空港 静脈をカード代わり
利点	漏洩のリスクがない	デバイス不要
欠点	デバイス所有	漏洩リスク

ユーザが持つべき派の言い分

- 漏洩のリスクがない
- 低いコスト（高速ネットワークが不要）で
  高い精度（他人とマッチする必要がない）
- 紛失は利用者のリスク

サーバが持つべき派の言い分

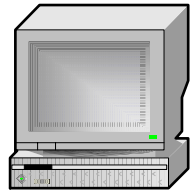
- 生体情報を格納する耐タンパーは本当に信用できるのか？（Felica脆弱性事件）
- 持ち物不要で認証できるべきだ（城県那珂市市立図書館）
- 貴重品を持てない子供でも使える（米国の給食にて活用）

議題3.

- では，一体どの方式が一番安全なのか？
  - どの仮定が現実的か？
  - 比較は困難: 対象とする脅威が異なる

生体情報におけるリスク

証明者 P



検証者 V

生体情報 x’

x = x’

x
比較x = x’

補助記憶デバイス

x

登録データベース

脅威の分類 [尾形，菊池，西垣SITA 2006]

手段＼不正	生体情報漏洩	なりすまし
サーバ内部班	A	
ICカードの盗難	B	C
通信路盗聴		D

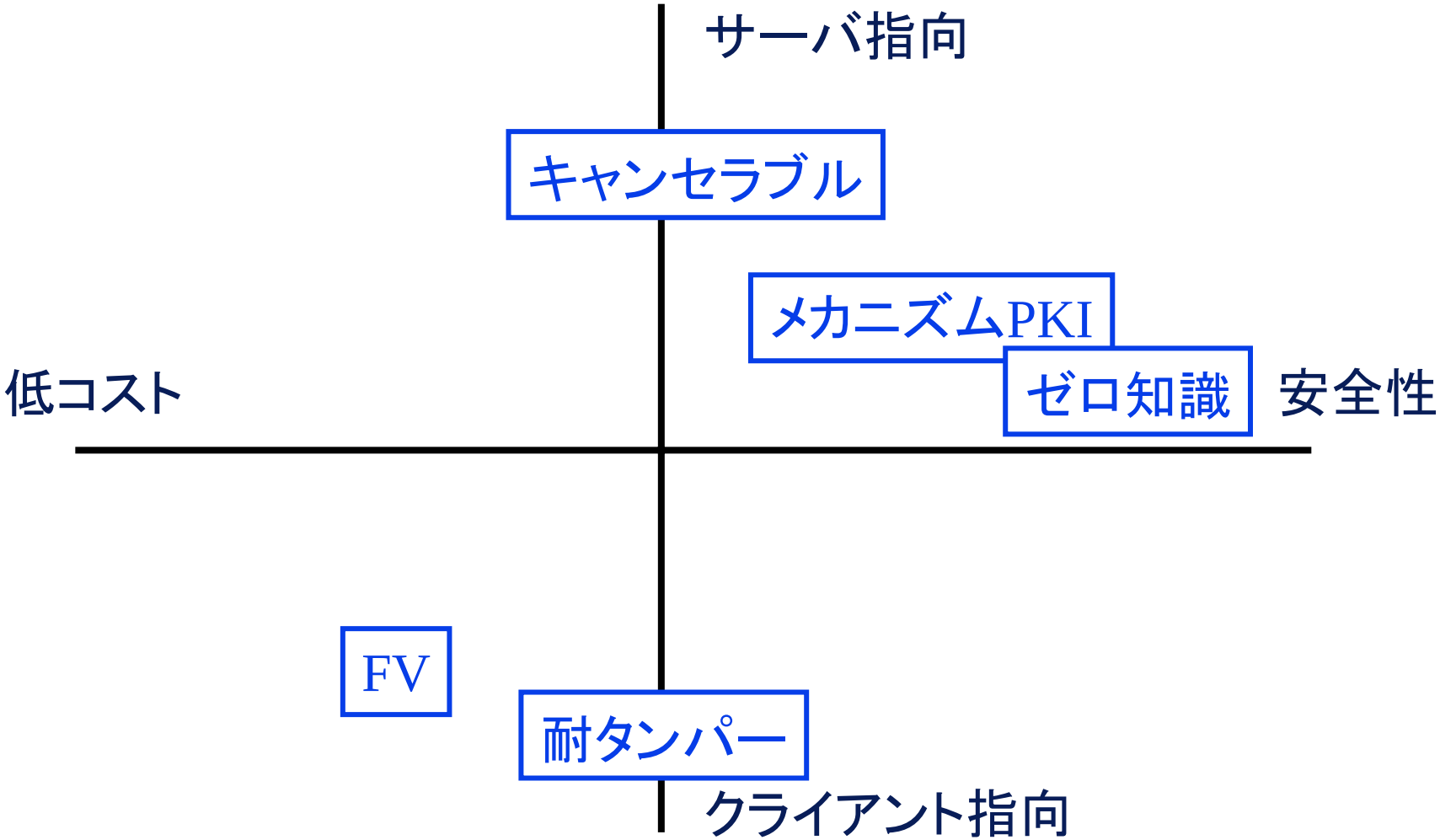
セキュリティ技術

- 1. 耐タンパーデバイス
  - デバイス内に生体情報格納・検証
- 2. キャンセラブル
  - 乱数で生体情報を変換（マニューシャ等長変換）
- 3. ランダマイズ（Fuzzy Vault）
  - チャフ（偽特徴点）を混在させ，誤り訂正
- 4. メカニズムベースPKI
  - 生体情報を種に動的に秘密鍵生成
- 5. ZeroBIO
  - 生体情報の保有をゼロ知識証明

セキュリティ技術とその安全性

	A. 内部班漏洩	カード紛失		D. 通信路盗聴
		B情報漏洩	Cなりすまし	
1. 耐タンパ	耐タンパ性	耐タンパ性	生体情報FRR	暗号
2. キャンセラブル	統計的情報漏えい	乱数のみ	失効リスト	暗号
3. FV	偽情報の数			偽情報の数
4. メカニズムPKI	公開鍵暗号の安全性	スケールのみ	失効リスト	暗号
5. ゼロ知識	コミットメントの安全性	情報理論的	失効リスト	暗号

議題3のまとめ　（仮置きです）



結論

- 生体情報漏洩事件は　　年内に起きる
- 生体情報は　　に管理するべきだ
- 最も安全な方式は　　だ.
- だから，これからは　　を研究するべきだ