HITACHI
Inspire the Next

テンプレート保護と生体認証基盤

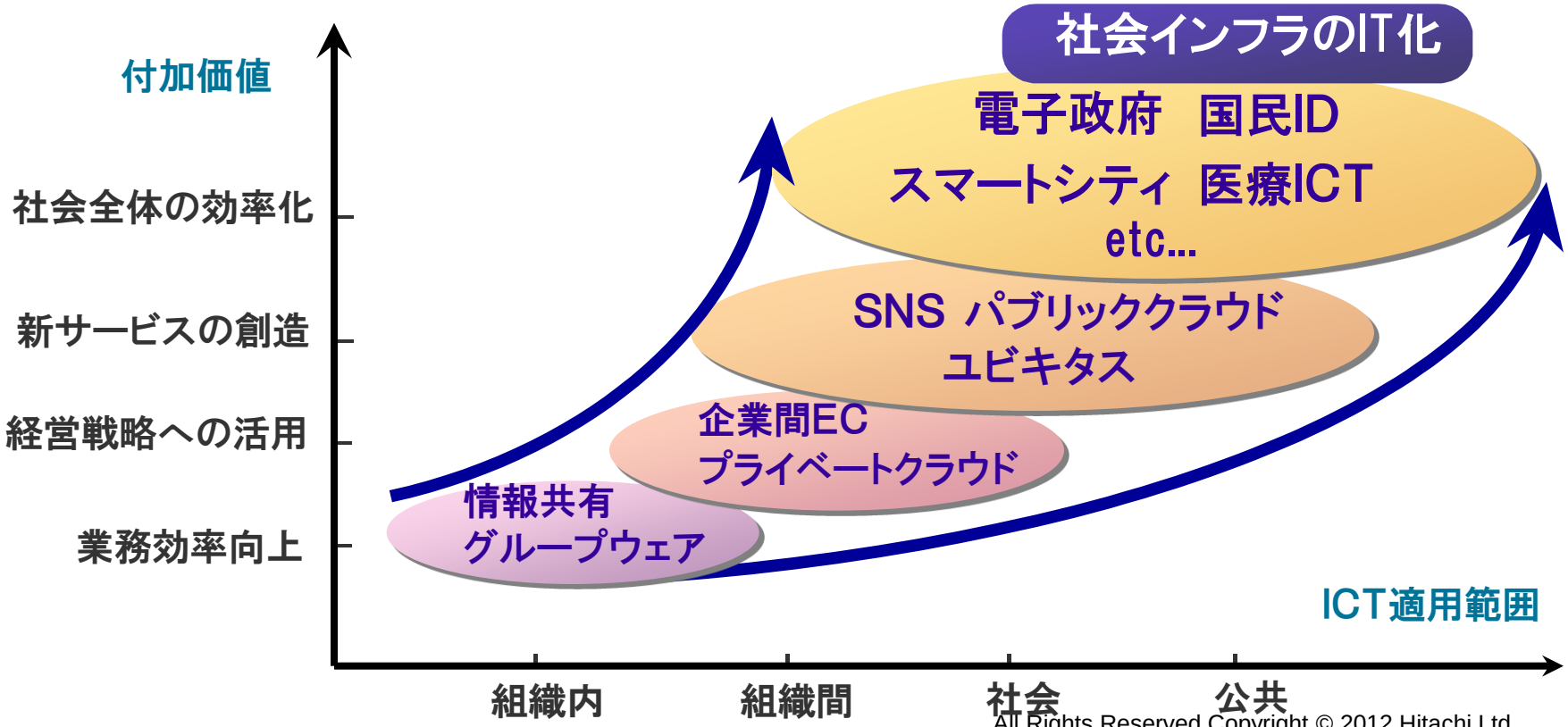
日立製作所　横浜研究所
高橋　健太

背景： 社会インフラのIT化

HITACHI
Inspire the Next

- クラウド化の進展
- 国民ID管理ニーズの高まり(先進国／途上国)
- スマートシティ，医療ICT，etc...

- ネットワーク上での**確実な本人確認に基づくセキュリティ基盤**の必要性増大



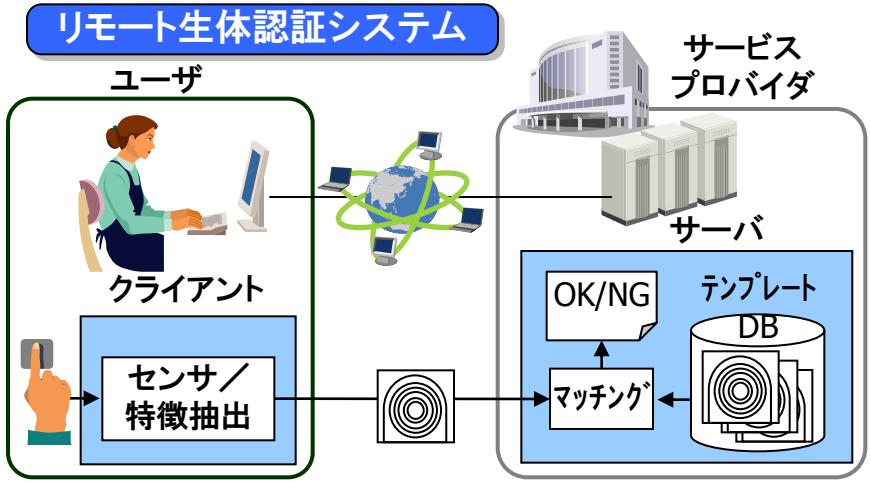
リモート生体認証への期待と課題

HITACHI
Inspire the Next

- 生体認証の利点
  - パスワードの記憶やICカードの所持が不要(高利便性).
  - ライフサイクル管理が不要(低コスト)
  - 盗用のリスクが低いく、確実な本人確認が可能(安全性)

ネットワークを介してリモートユーザを生体認証により識別する、
リモート生体認証に対する期待が高まる

- リモート生体認証の問題
  - 生体情報は・・・
    - 漏洩しても破棄・更新できない(生涯不変)
    - 個人情報／機微情報に該当
  - 生体情報の集中管理に伴う問題
    - 漏洩時の被害大
    - 内部不正の可能性
  - プライバシーの問題
    - 生体情報をサーバ管理されることへの
      ユーザの心理的抵抗感



テンプレートの厳密な保護が課題

生体情報(テンプレート)の管理モデル

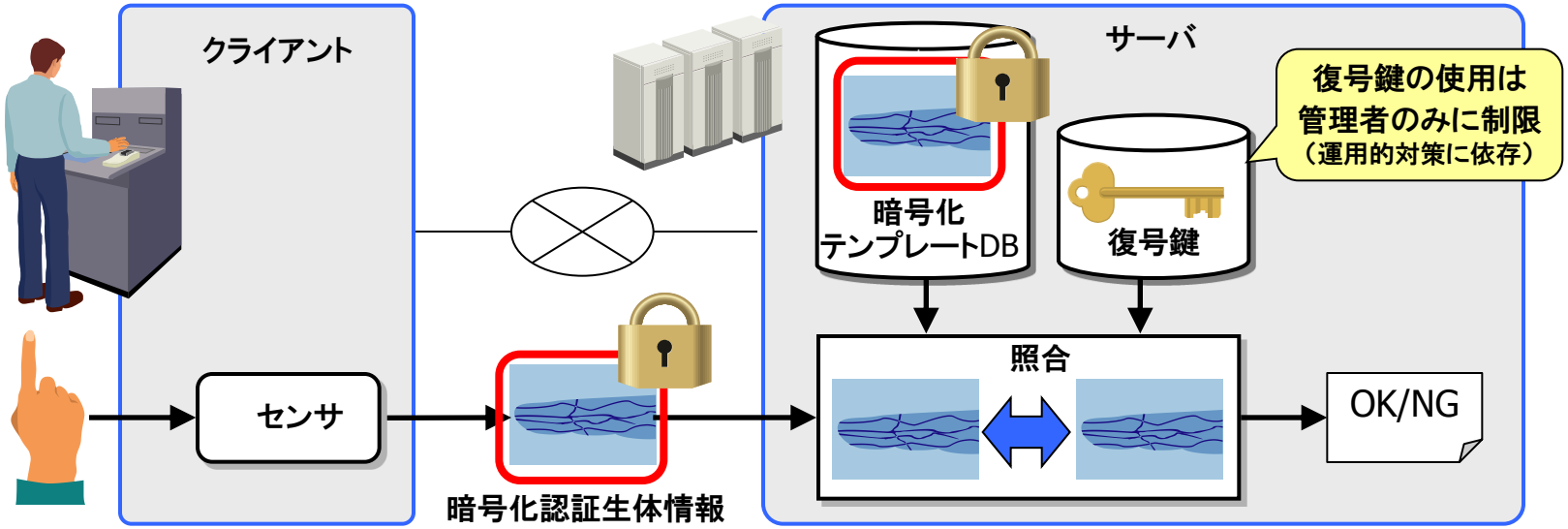
HITACHI
Inspire the Next

- Store on Card (SOC)
  - カード内に格納して，ユーザ自身が管理する.
  - 銀行ATMにおいて主流
  - 耐タンパモジュール内でテンプレートを管理・照合することで保護可能
- Store in Device (SID)
  - センサ／認証装置／認証端末(PC)内に保管
  - 小規模入退管理装置，携帯端末／PCログイン等で多く使われる
- Store on Server (SOS)
  - サーバ上で一括管理
  - 企業内情報システム，大規模入退管理等で使われる
  - クラウド化の進展等により、今後主流となる可能性

SOSモデルにおける従来の生体情報保護

HITACHI
Inspire the Next

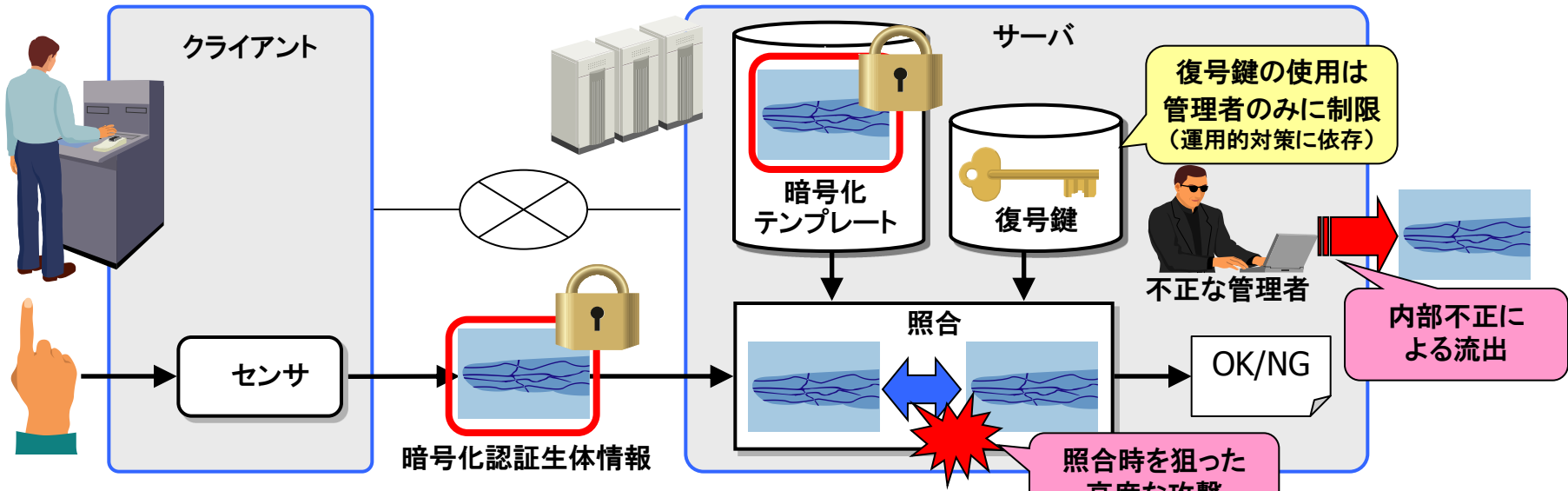
- 暗号化＋運用管理
  - テンプレートを暗号化しサーバ側DBで集中管理．復号鍵はサーバ側で管理．
  - 照合時にはテンプレートと認証生体情報をサーバ側の鍵で復号して比較．
- SOC, SID に対する利点
  - テンプレートの管理をサービス提供者側でコントロール可能．
    - サーバへのアクセス制御，管理者の教育等の運用による保護が可能．
  - ICカードの発行、管理コストが不要



「サーバ認証＋暗号化」の問題点

HITACHI
Inspire the Next

- 安全性の問題点
  - 不正な管理者がテンプレートを復号化し、漏洩／なりすましに利用可能
    - サーバ管理者権限を盗用した攻撃者も同様の攻撃が可能
  - 一旦事故が発生すると，大規模漏洩に繋がる可能性あり
- 運用上の問題点
  - テンプレートの安全性が鍵管理／サーバ運用・保守に大きく依存するため、管理者やオペレータの強固な認証が必要となるなど、運用上の負担が大きい



SOSにおける新たな生体情報保護

HITACHI
Inspire the Next

テンプレート保護型生体認証技術

- 生体情報をサーバに対して秘匿したまま認証
  - サーバ管理者の過失・内部不正による生体情報漏洩を防止
  - 利用者のプライバシを保護
- 生体情報の安全性をアルゴリズムレベルで確保
  - ⇔ カード内照合： 安全性をハードウェア（耐タンパチップ）に依存
  - ⇔ 暗号化＋運用管理： 安全性をサーバの運用管理に依存

研究アプローチ

- 既存研究は大きく3つのアプローチに分類可能

1. キャンセラブルバイオメトリクス
   - 生体情報を変換（暗号化・ハッシュ化）して秘匿し，元に戻さず照合
2. バイオメトリック暗号
   - 生体情報を用いて秘密鍵を生成し，暗号技術を利用して認証
3. ゼロ知識証明ベース
   - 生体情報の「近さ」をゼロ知識証明

金融機関における生体情報保護の必要性

HITACHI
Inspire the Next

- FISCガイドライン
  『金融機関等コンピュータシステムの安全性対策基準・解説書第8版』(2011/3)

  - 【技35-1】生体認証の特性を考慮し、必要な安全対策を検討すること。
    生体認証の導入と運用にあたっては、技術の最新動向等に留意し、その特性を十分考慮し、必要な安全対策を検討すること。

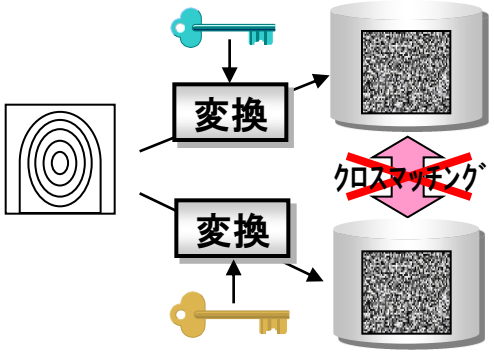
    考慮すべき特性：
    1. 認証精度
    2. 代替措置手続き
    3. 否認防止
    4. 不正認証（なりすまし）等防止
    5. テンプレート保護技術
       「取り消し可能なバイオメトリクス認証」(Cancellable biometrics)
       など技術動向を考慮することが望ましい。

テンプレート保護型生体認証の要件 [Jain,et.al., 2009]

HITACHI
Inspire the Next

- Performance
  - 変換によって照合精度が劣化しないこと
- Secrecy
  - 変換生体情報から元の情報が復元できないこと

- Diversity
  - （複数のアプリに対し）同一の生体情報から複数のテンプレートを作成できること
  - テンプレート間のクロスマッチングができないこと

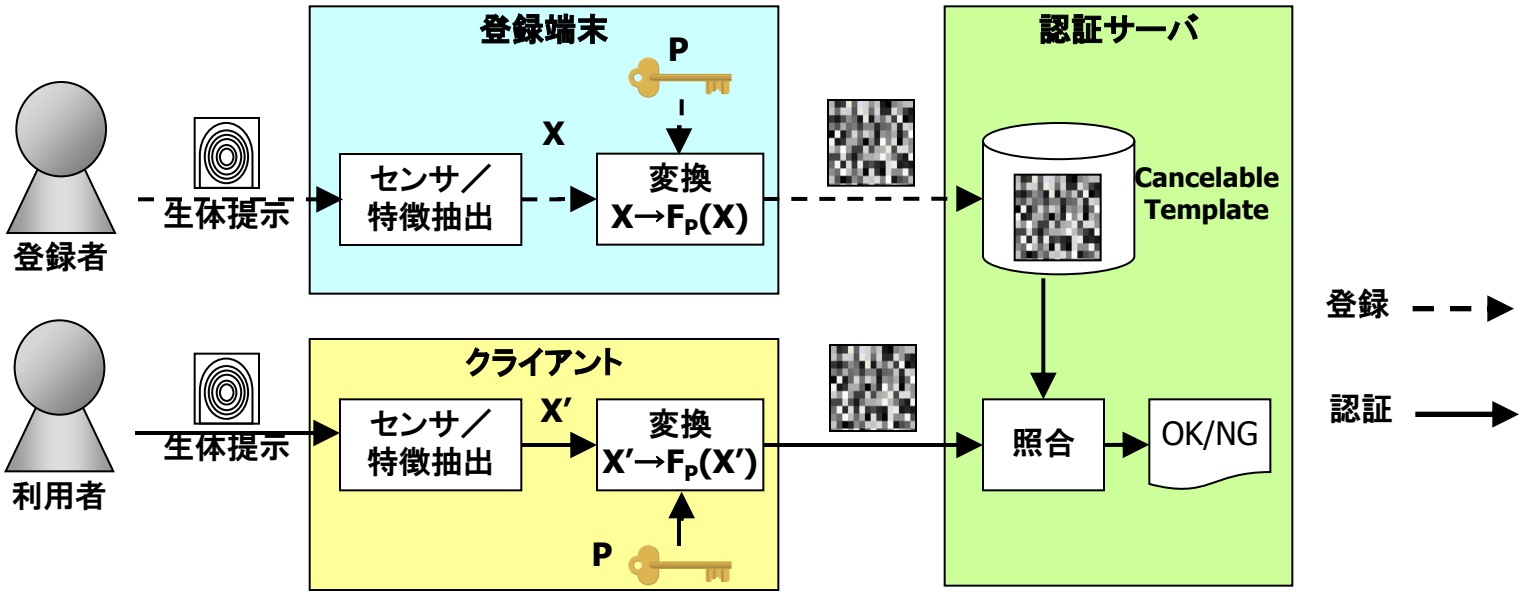


- Revocability
  - 漏洩したテンプレートを容易に破棄・更新できること

キャンセラブルバイオメトリクス

HITACHI
Inspire the Next

- 生体情報を変換(暗号化)したまま登録・照合
  - 登録時:
    - 変換パラメータP(暗号鍵に相当) をランダムに生成して登録者に発行.
    - 登録生体情報を X → $T=F_P(X)$ と変換(暗号化に相当)してサーバに登録(Cancelable Template)
  - 認証時:
    - 照合生体情報を X′ →$V= F_P(X')$ と変換し, 変換したまま T と照合(元に戻さない)



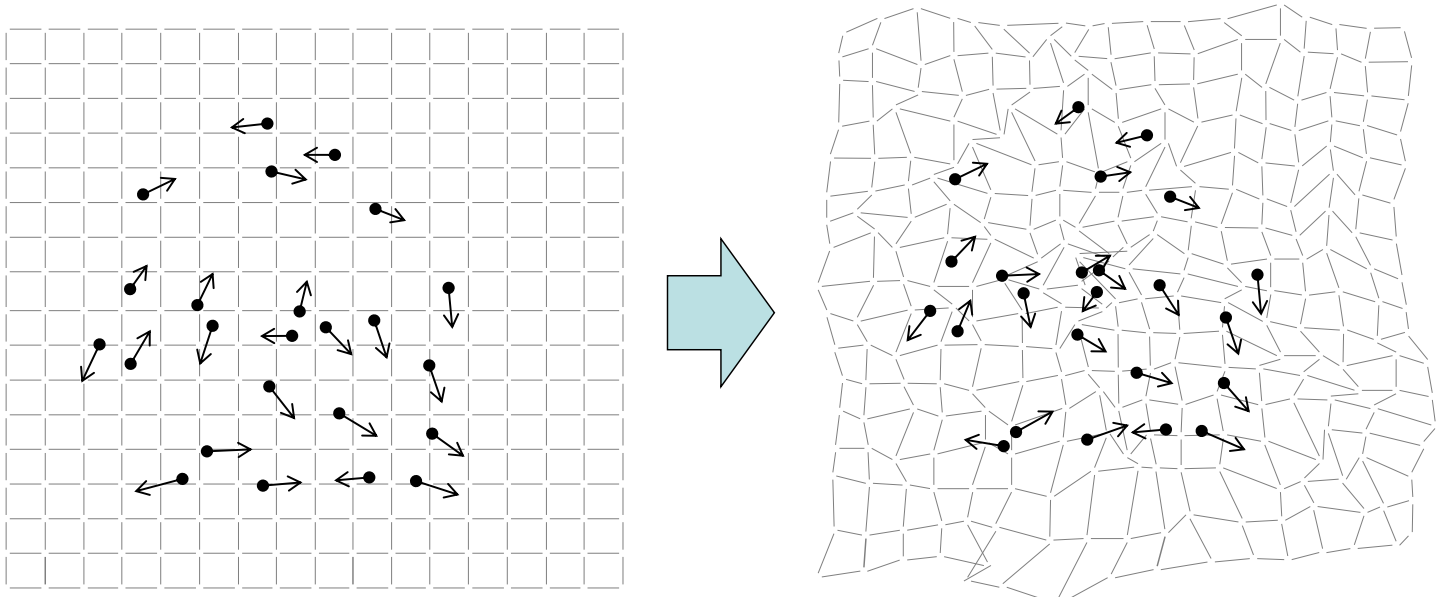
キャンセラブルバイオメトリクスの研究例
Cancelable Biometrics

HITACHI
Inspire the Next

- N.K.Ratha,et,al. (IBM)
  - 生体情報を秘匿したまま認証し，取替え可能とする概念を提唱 (2001)
  - 幾何的変換に基づく指紋特徴量の変換関数を提案 (2007)

- 指紋特徴量（マニューシャ）の幾何的変換：

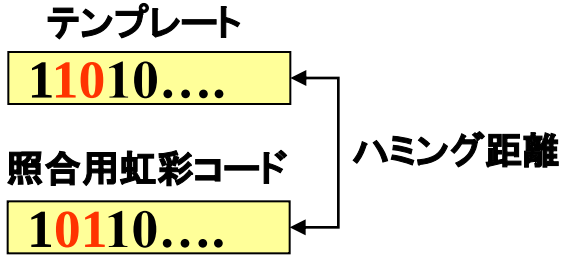
$$x' = x + f(x, y),$$
$$y' = y + g(x, y),$$
$$\theta' = \theta + h(x, y) \bmod 2\pi$$



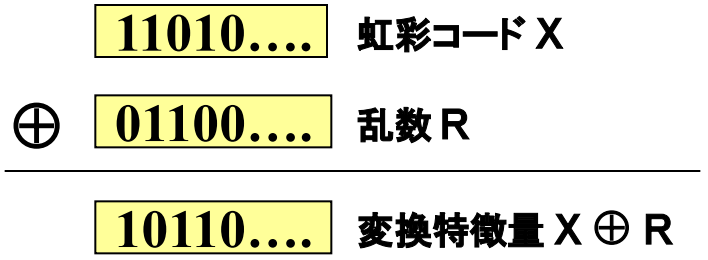
キャンセラブル虹彩認証

HITACHI
Inspire the Next

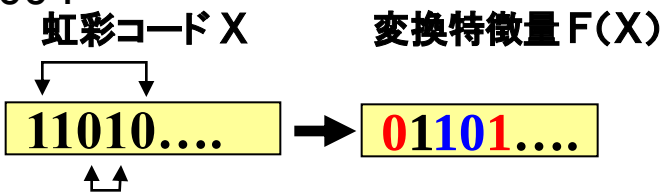
- 虹彩照合
  - 特徴量：虹彩コード(2048bit)
  - 距離：虹彩コード間のハミング距離 Hd
    - 厳密にはシフトずれを考慮した最小ハミング距離



- M.Braithwaite, et. al. (Iridian)
  "Application specific biometric templates", 2002
  - 変換関数： マスキング
    - 虹彩コードXと乱数RとのXOR(虹彩)
    - F(X)＝X⊕R (R: 2048bit)
  - ハミング距離不変
    - Hd(F(X), F(X'))＝Hd(X, X')



- 太田 他 (KDDI)
  "虹彩コードを秘匿する虹彩認証方式の提案", 2004
  - 変換関数： マスキング＋ビット置換
  - ハミング距離不変



Biohashing (Random Projection)

HITACHI
Inspire the Next

- Teoh, et.al. : Biohashing (2006)
  - LSH (Locally Sensitive Hashing) で使われている Random Projection (RP) を利用
  - RP: ランダムな基底への射影と量子化による変換
- **変換関数**
  - **特徴量 x: m 次元実数ベクトル**
  - K: n×m **実数行列** (n<m)
    - **各要素は正規分布** N(0,1)**に従ってランダムに決定**
  - **変換:**

$$f : \mathbb{R}^m \to \{0,1\}^n,$$

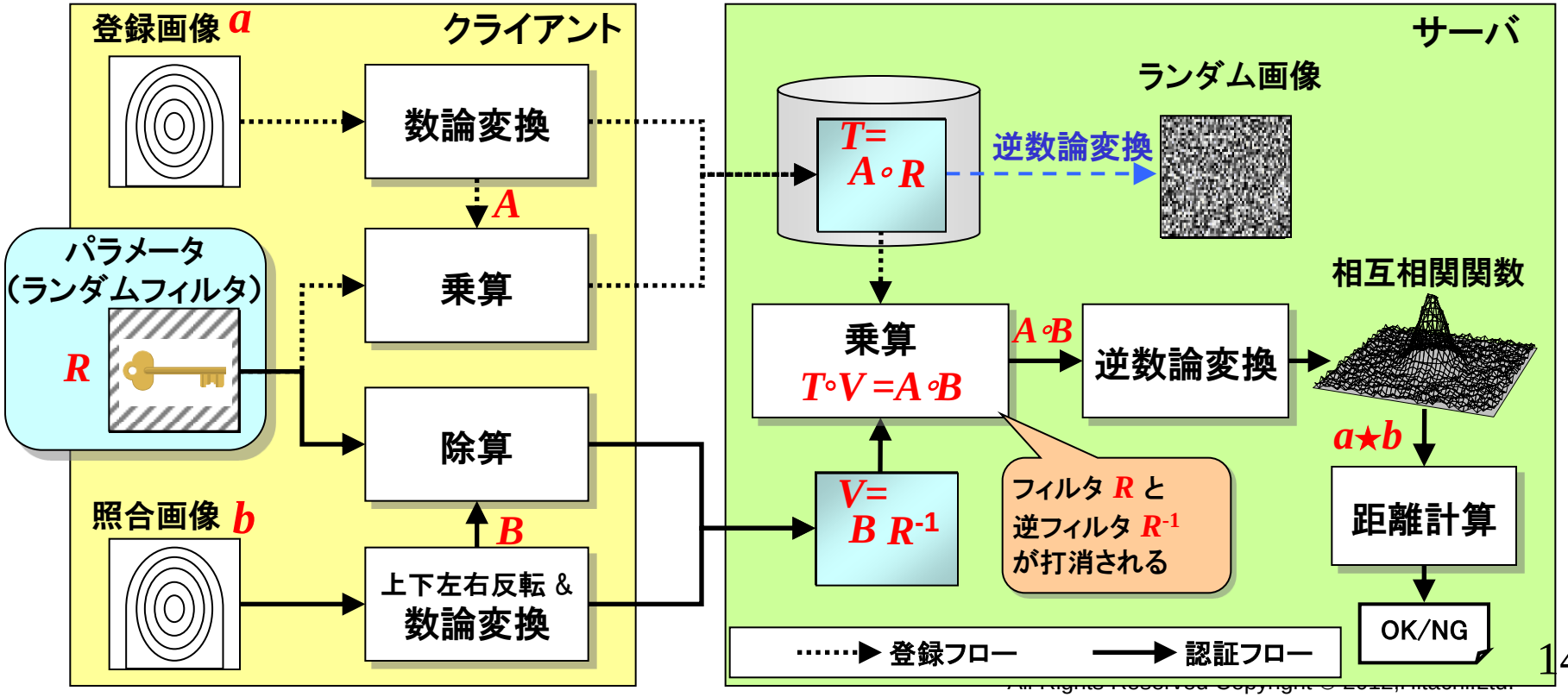
$$\boldsymbol{x} \mapsto \boldsymbol{t} = \mathrm{Sig}(K\boldsymbol{x} - \tau \cdot \mathbf{1})$$

$$\mathrm{Sig}((y_1, \cdots, y_n)^T) = (t_1, \cdots, t_n)^T, \quad t_i = \begin{cases} 0 & (y_i \leq 0) \\ 1 & (y_i > 0) \end{cases}.$$

画像マッチングに対するキャンセラブル方式

HITACHI
Inspire the Next

- S.Hirata and K.Takahashi (2009), in ICB2009
  - 数論変換(有限体上のフーリエ変換)に基づく畳み込み計算を利用
  - 精度保存性を有する
- K.Takahashi (2011), in IJCB2011
  - 2変数多項式環上の剰余乗算に基づく畳み込み計算を利用
  - 精度保存性と情報理論的安全性を有する



キャンセラブルバイオメトリクスの長所・課題

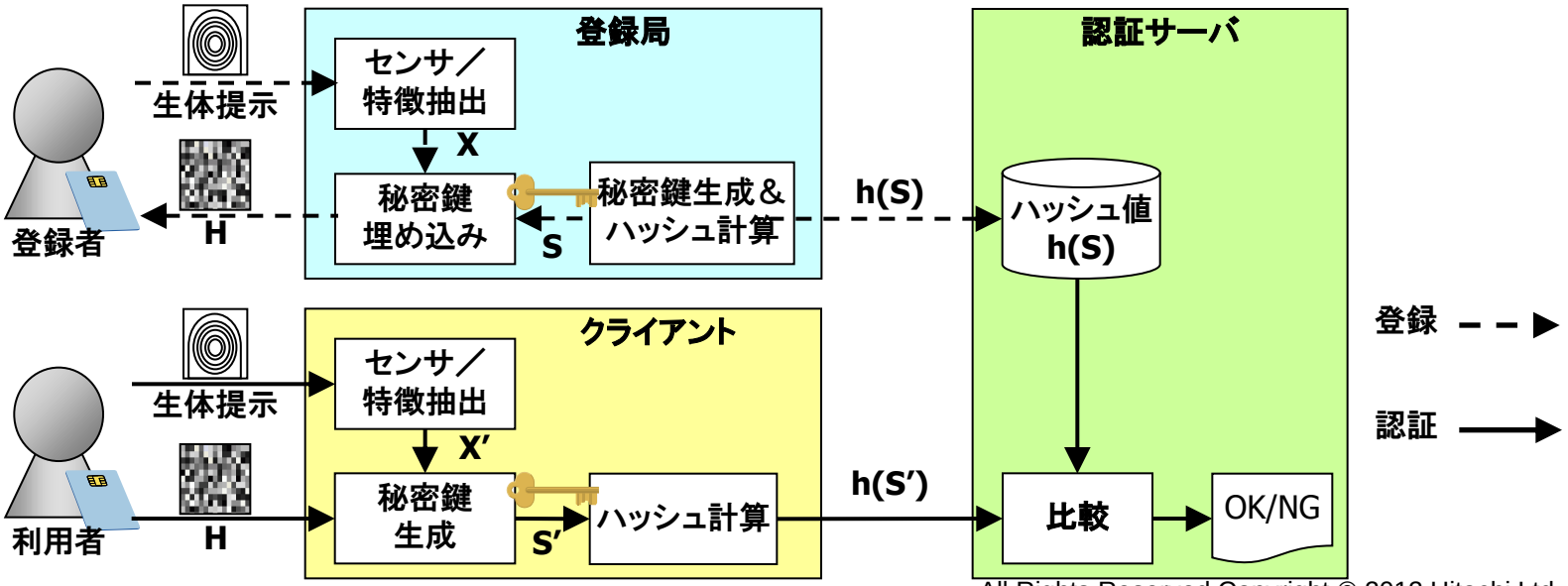
HITACHI
Inspire the Next

- 長所
  - 従来の照合アルゴリズムの認証精度を保ったまま実現可能な方式が知られている
  - 一般に処理が軽く，実用に適している
- 課題
  - より高度な攻撃に対する安全性証明
    - [Braithwaite02],[Takahashi11] などは1つのキャンセラブルテンプレートからの生体情報解読に対して情報理論的安全性を有するが、同一パラメータで変換された複数のキャンセラブルテンプレートからの解読攻撃に対する厳密な安全性証明はついていない
  - テンプレート漏洩時のなりすまし対策
    - キャンセラブルテンプレート漏洩時に、これと照合成功する認証用変換特徴量を容易に計算可能.
    - 変換パラメータのゼロ知識証明を組合わせることで対処可能

      高橋 他,「セキュアなリモート生体認証プロトコルの提案」, 情報処理学会論文誌, 2008.

バイオメトリック暗号

- 概要
  - 生体情報に秘密鍵を埋め込み／復元し，暗号技術を利用して認証
  - 登録時：
    - 秘密鍵Sを生体情報Xに埋め込んで補助情報Hを作成し、登録者に発行．
      - HからS,Xは復元できない
    - ハッシュ値 h(S) を認証サーバに登録
  - 認証時：
    - 利用者の生体情報 X′ を用いて H から S′ を取り出す
      - X′がXに十分近いときのみS′=S
    - ハッシュ値 h(S′) をサーバに送信．サーバは　h(S′)、h(S) を比較

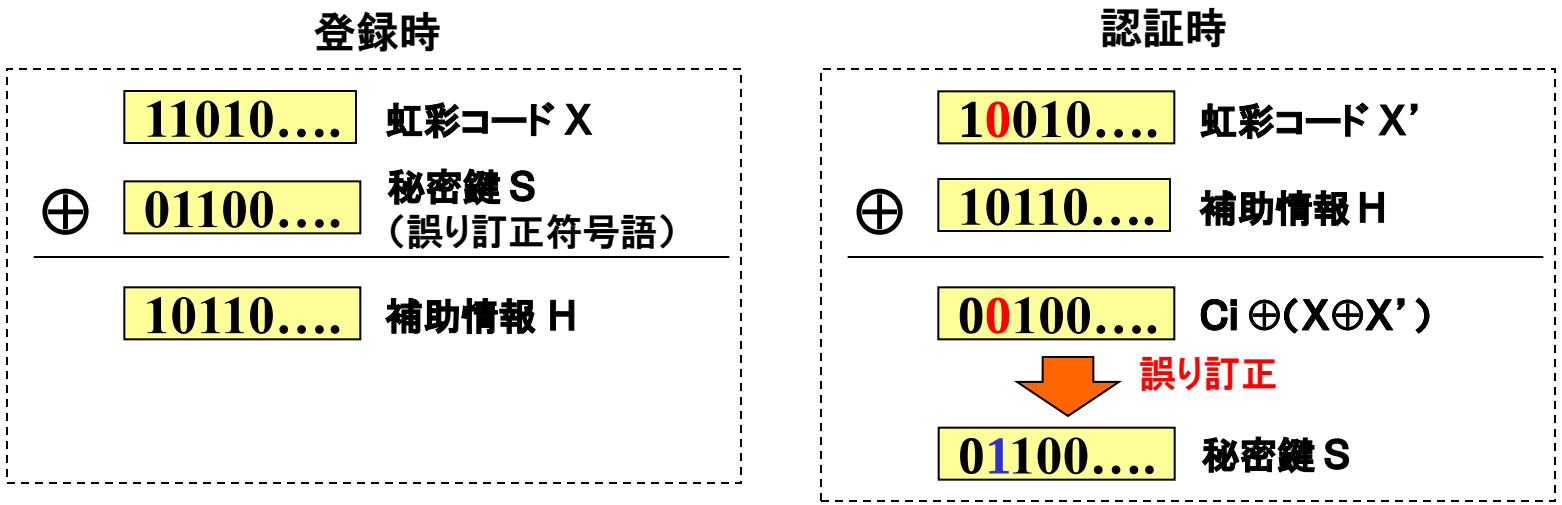


Fuzzy Commitment

HITACHI
Inspire the Next

- A.Juel, et. al. (RSA), "A fuzzy commitment scheme", 1999
  - 特徴量X，X'の距離がハミング距離で与えられる場合に，誤り訂正符号を用いて秘密鍵を生成するアルゴリズム．
  - 登録時：
    - Xと同じビット長の誤り訂正符号C＝{Ci}から符号語をランダムに選択し秘密鍵Sとする
    - 補助情報： H＝X⊕S
  - 認証時（鍵復元時）：
    - X'⊕H＝S⊕(X⊕X') を誤り訂正してSを生成

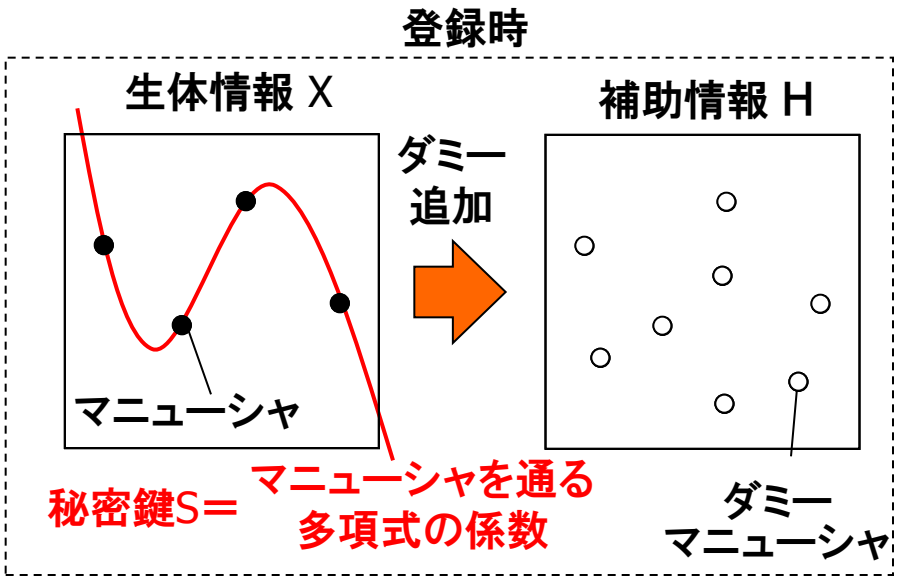
ハミング重み小（X,X'が近い）
なら正しく誤り訂正可能

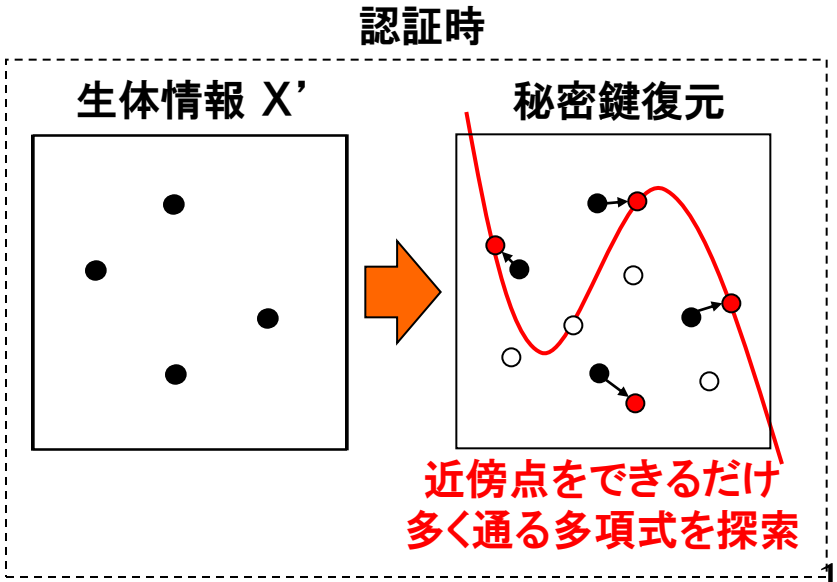


Fuzzy Vault

HITACHI
Inspire the Next

- A.Juels, et.al. (RSA), "A fuzzy vault scheme", 2002
  - 生体情報X，X'が集合として表現され，その距離がset difference(共通要素の数)で与えられる場合に，
  - 誤り訂正理論を応用して一意のデータ(秘密鍵)を埋込み／復元するアルゴリズム
- T. Clancy, et.al. (Univ. of Meryland)
  "Secure smartcard-based fingerprint authentication", 2003
  - Fuzzy Vault を指紋に適用
  - 生体情報X: マニューシャ(特徴点)の集合
- その後，多くの研究グループにより改良研究が進められている





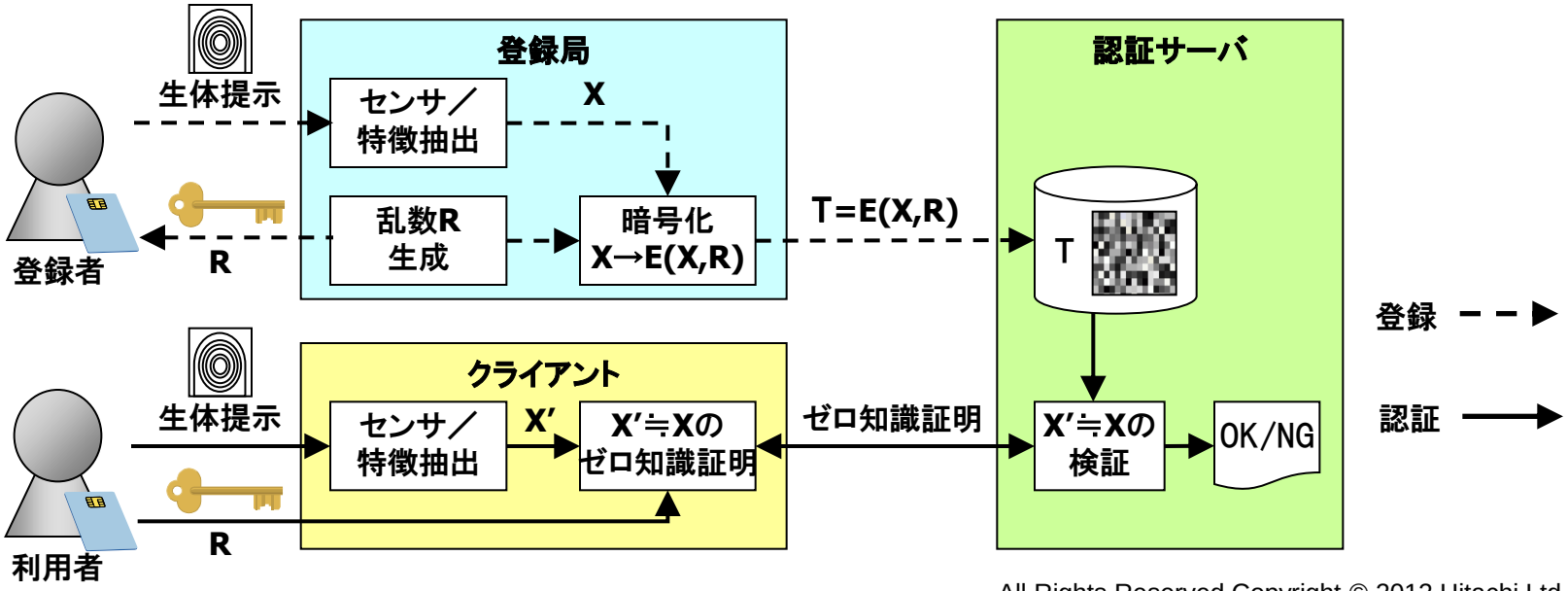
バイオメトリック暗号の長所・課題

HITACHI
Inspire the Next

- 長所
  - 既存の暗号プリミティブに基づく認証プロトコルとの融合が容易
    - ハッシュ関数に基づくパスワード認証、公開鍵暗号ベースの認証(PKI等)、etc…
- 課題
  - 安全性の厳密な証明
    - 補助情報漏洩時に、生体情報や秘密鍵を推定する攻撃(Secrecyの脆弱性)やクロスマッチング攻撃(Diversityの脆弱性)が多数発見されている
      e.g., S. Hidano, et.al., "Evaluation of Security against Biometric Guessing Attack in Biometric Cryptosystem using Fuzzy Commitment Scheme," BIOSIG2012, 2012.
  - 認証精度の向上
    - 認証精度が誤り訂正能力に依存.
      このため誤り訂正符号の各種限界の制約を受け、認証精度の向上が困難.

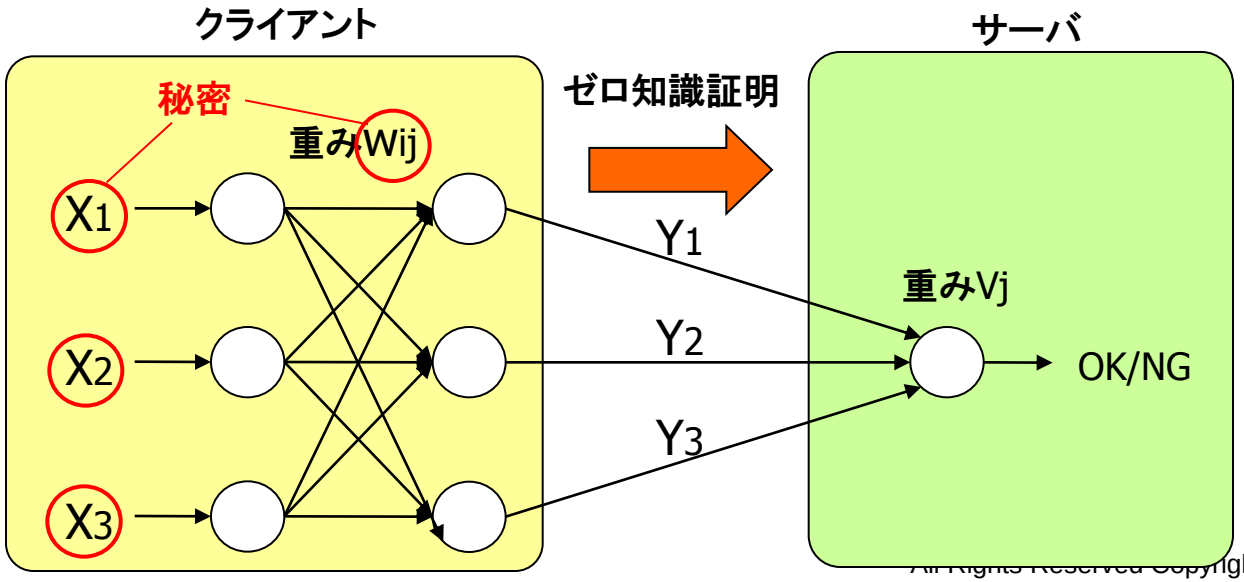
ゼロ知識証明ベース

- 概要
  - クライアントが認証サーバに対し，Xに十分近いX′の知識をゼロ知識証明
    - 認証の結果，サーバはXとX′が十分近いか否かの2値情報のみを得，それ以外の情報は得ない．
  - 登録時：
    - 生体情報 X の暗号文（又はコミットメント） T=E(X,R) をサーバに登録
    - 乱数 R を登録者に発行
  - 認証時：
    - 利用者の生体情報 X′ が X に十分「近い」ことをゼロ知識証明
- 長所
  - 既存の暗号理論に基づく安全性証明が可能



秘匿ニューラルネット

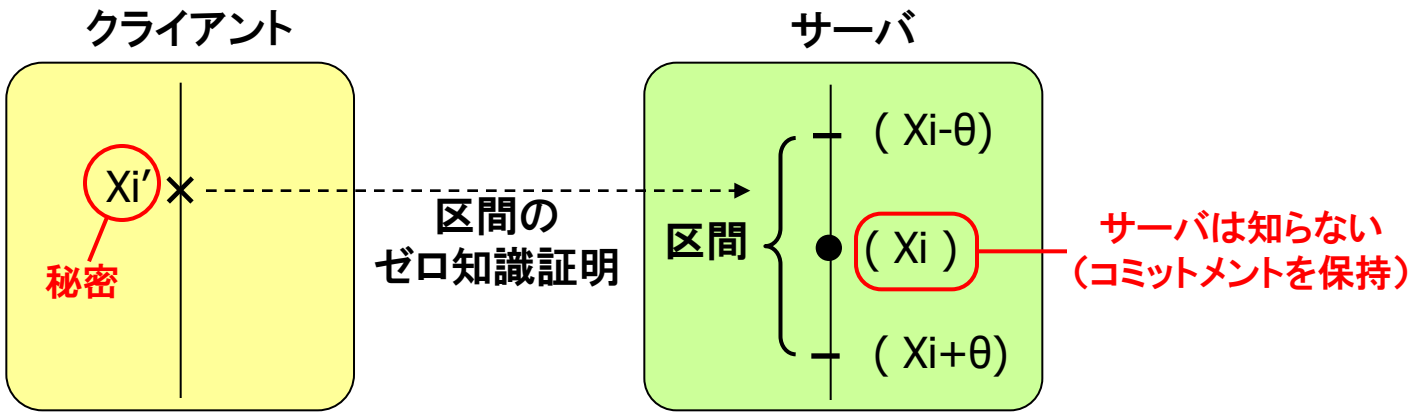
- 菊池, “非対称生体認証”, 2005
  - ニューラルネットワーク(NN)を用いて照合可能な生体認証方式を対象
  - 登録時:
    - 登録生体情報を受理するNNを学習
      - 中間層ノードの重み Wij をクライアントが保持
      - 出力層ノードの重み Vj と，Wij の暗号文 E(Wij, R) をサーバが保持
    - 乱数 R を登録者に発行
  - 認証時:
    - クライアントがNNの中間層までを計算し，その出力 Yj をサーバへ送信
    - NNの秘密計算により入力ベクトル(生体情報)Xiを秘匿したまま，Yiの正しさをゼロ知識証明
    - 中間層ノード数に比例した回数のゼロ知識証明が必要
- 指紋への適用報告あり(永井 他, 2006)
  - FAR 8.3%,　FRR 9.8%



「近さ」のゼロ知識証明

HITACHI
Inspire the Next

- 尾形, 菊池, 西垣
  “リモートバイオメトリクス認証に有効な「近い」ことを示す零知識証明プロトコル”, 2006
  - 対象とする生体認証方式
    - 生体情報： ベクトル $X=(X_1,X_2,\cdots,X_n)$
    - 生体情報X,Yが「近い」 $\equiv \max(|X_i - Y_i|) \leqq m$
  - 登録時：
    - 登録生体情報 $X=(X_1,\cdots,X_n)$ のコミットメント $\{E(X_i,R_i)\}$ をサーバに登録
    - 乱数 $\{R_i\}$ を利用者に発行
  - 認証時：
    - 照合生体情報 $X' = (X_1',\cdots,X_n')$ の各 X_i' が区間 $[X_i-\theta,X_i+\theta]$に含まれることをゼロ知識証明(「区間のゼロ知識証明」を利用)
    - クライアントは X_i を知らないため, $X_i \in \{X'-\theta,\cdots,X'+\theta\}$ を総当りで試す
    - $n\theta$ 回の区間のゼロ知識証明が必要



ゼロ知識証明ベースの長所・課題

HITACHI
Inspire the Next

- 長所
  - 厳密な安全性証明が可能
- 課題
  - 計算量・通信量の削減
    - 準同型暗号やゼロ知識証明プロトコルを多用するため、一般に膨大な計算量・通信量が必要となる
  - 認証精度の向上
    - 特徴量形式や距離関数に強い制約が課される場合が多く、実際の生体情報へ適用した際に認証精度が大幅に劣化する可能性が高い.

研究開発動向

HITACHI
Inspire the Next

研究動向

- ここ10年余り，企業・大学等の研究機関において研究開発が活発化
- 欧州ではEP7(第7次枠組計画)において，テンプレート保護技術の研究開発を目的としたTURBINEプロジェクト(2008/2～2011/1)が実施

製品化動向

- 既に実用化フェーズに入りつつある
- 日立： キャンセラブルバイオメトリクスを用いたクラウド型指静脈認証サービス(2010～)
- 蘭 GenKey(PrivID)： Fuzzy Commitmentに基づく(?)テンプレート保護型指紋認証
- 米 Securics： コロラド大 Boult 教授らによるテンプレート保護技術

標準化動向

- ISO/IEC JTC1/SC37: 24745 Biometric template protection
- ITU-T/SG17: X.gep(1091) A guideline for evaluating telebiometric template protection techniques

生体情報のエントロピー問題

HITACHI
Inspire the Next

- オフライン解読攻撃
  - どのような(一方向性)変換を用いても、パラメータや補助情報が既知の場合、変換後のテンプレートを入手した攻撃者は O(1/FAR) 回の総当りで、認証の成功するような生体情報を復元可能
  - 認証サーバに問い合わせずに実行可能(オフライン攻撃)
- 既存の生体認証技術の精度と攻撃空間

モダリティ	FAR	攻撃空間 (bit)
指紋	10^{-4}～10^{-6}	13～20
静脈	10^{-6}	20
虹彩	10^{-6}～10^{-8}	20～27

  - 一般的な暗号鍵の空間(例:128bit)と比べて極めて小さく、容易に解読可能
- テンプレート保護技術の現実的な使い方
  - テンプレートと変換パラメータ(または補助情報、乱数)は分散管理
  - いずれのデータも管理主体が安全に管理し、漏洩時には速やかに破棄・更新

FAR: False Acceptance Rate

集中型から分散型の認証モデルへ

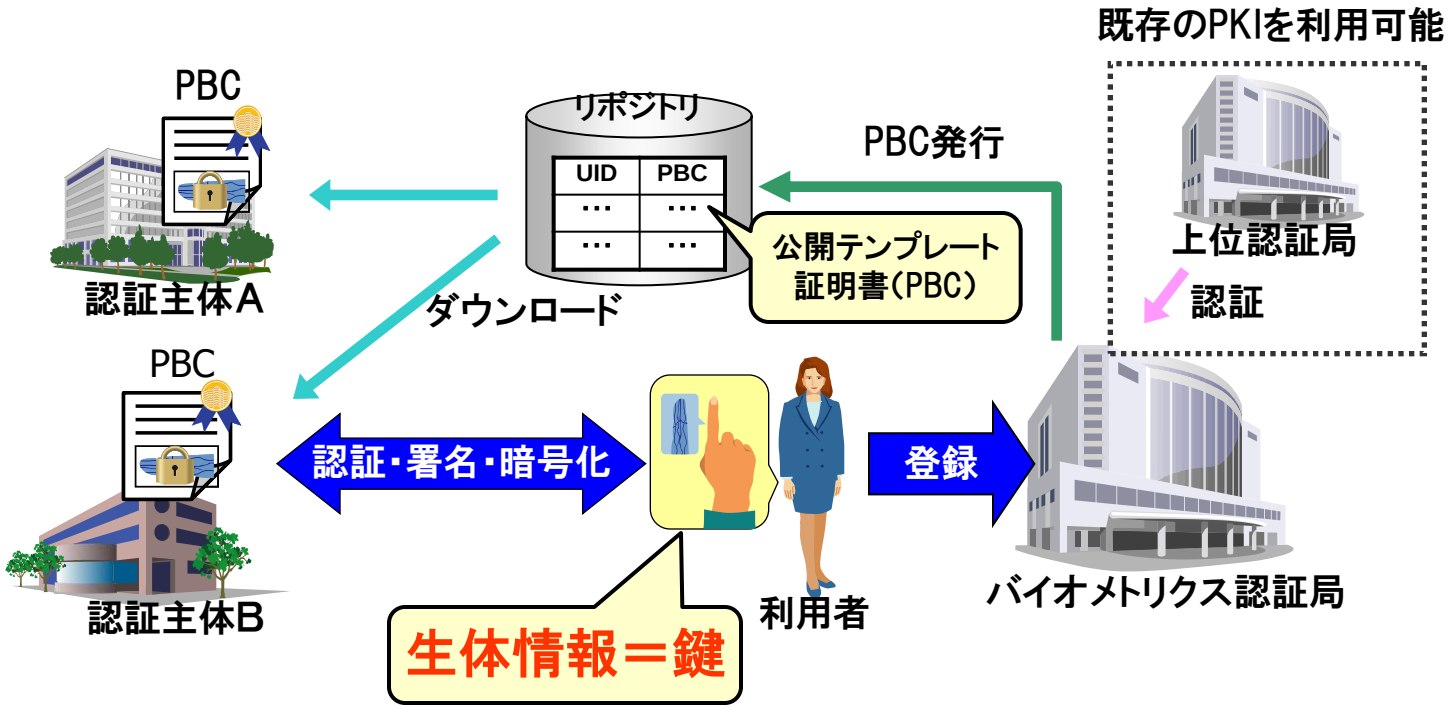
HITACHI
Inspire the Next

- 今後の研究の方向性
  - センサ・特徴抽出技術の向上、マルチモーダル化などにより、生体情報のエントロピーは増加
  - 生体情報を、自身のエントロピーで秘匿できる可能性
    ⇒テンプレート公開可能

- 生体情報を秘密鍵とした公開鍵暗号・署名技術に基づく認証基盤
  - テンプレート公開型生体認証基盤
    Public Biometric Infrastructure (PBI) の実現

PBIシステムモデル

- PBIシステムの最小構成
  - バイオメトリクス認証局： 公開テンプレート証明書(PBC)の発行
  - リポジトリ： PBCを登録・公開
- PKIとの違い
  - 秘密鍵 → 生体情報
  - 公開鍵証明書 → 公開テンプレート証明書(PBC)

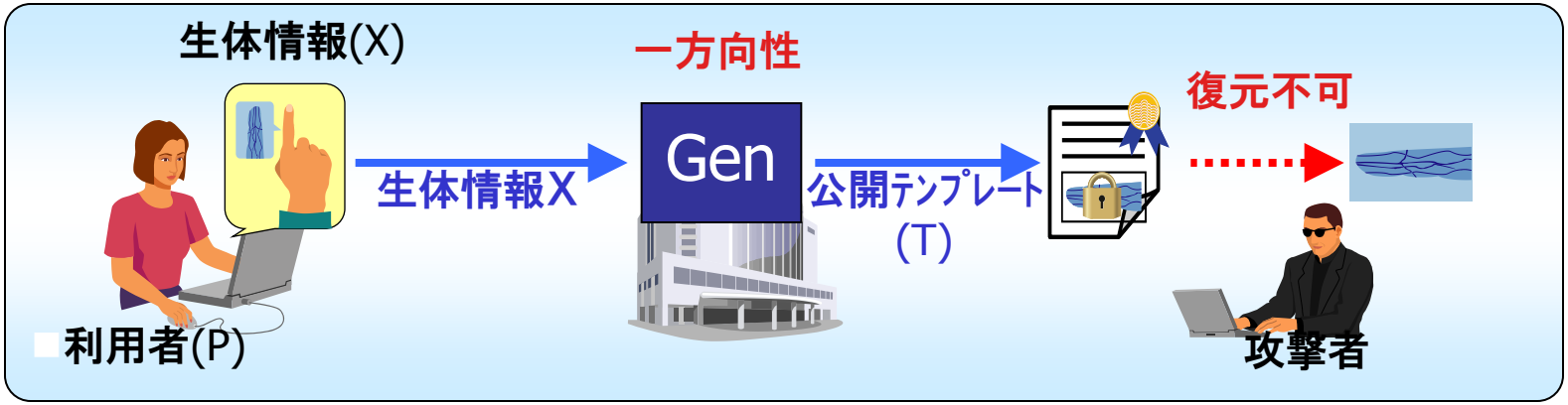


PBC:Public Biometrics Certificate

PBIの機能要件

- PBIの機能：
  - 登録／認証／署名／公開鍵暗号

- 登録機能
  - 生体情報 X を入力とし，公開テンプレートTを出力するPPTA
    - T=Gen(X)
  - 一方向性：T から X を復元・推定することができない．

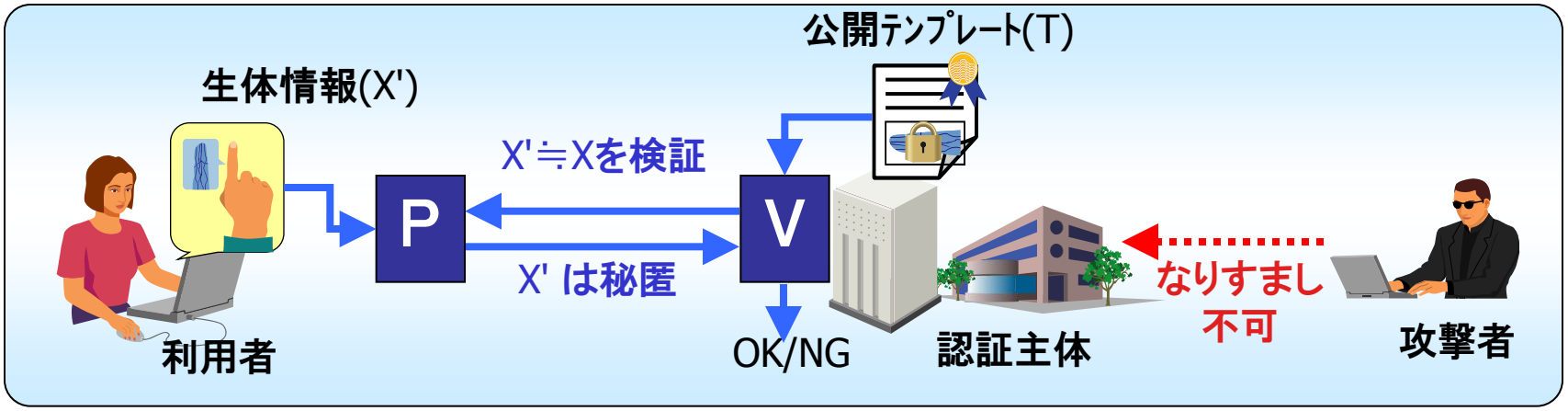


PPTA：Probabilistic Polynomial Time Algorithm

PBIの機能要件

HITACHI
Inspire the Next

- **認証機能**
  - Prover P（入力：生体情報X'), Verifier V（入力：T)からなる認証プロトコル:
    - ＜P(X'),V(T)＞ = "OK" or "NG"
  - **正当性**：X'≒Xなら(圧倒的確率で) "OK"を出力 (※)
  - **安全性**：X'(≒X)を知らない攻撃者は認証成功できない

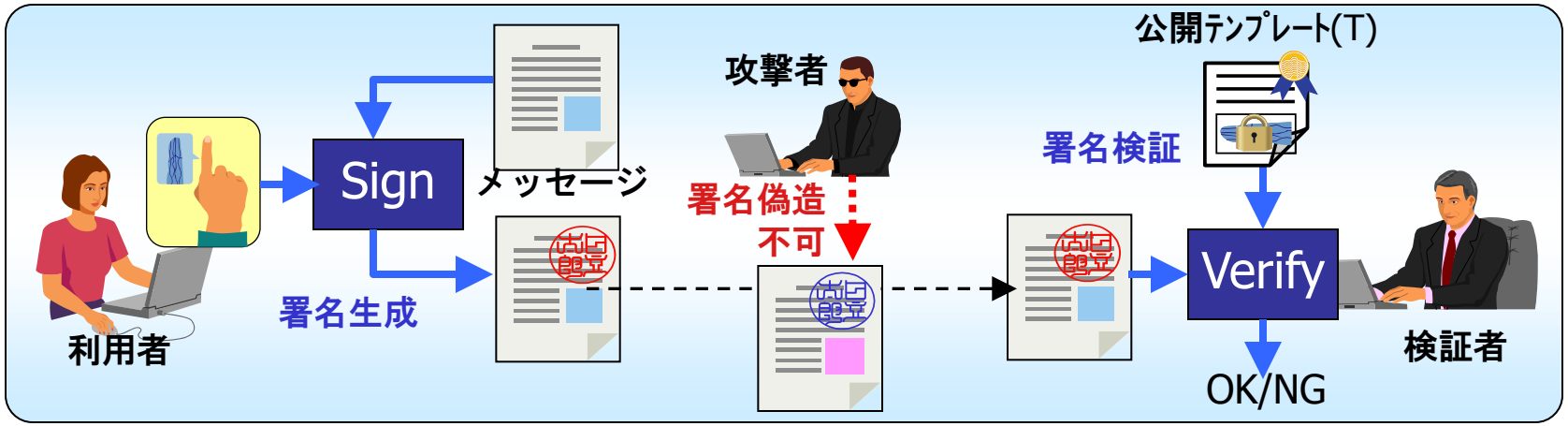


※ 生体情報空間にはある距離関数 d(・,・) が定義されているとし,
所定の閾値 t に対し X'≒X ⇔ d(X',X)≦t と定義.

PBIの機能要件

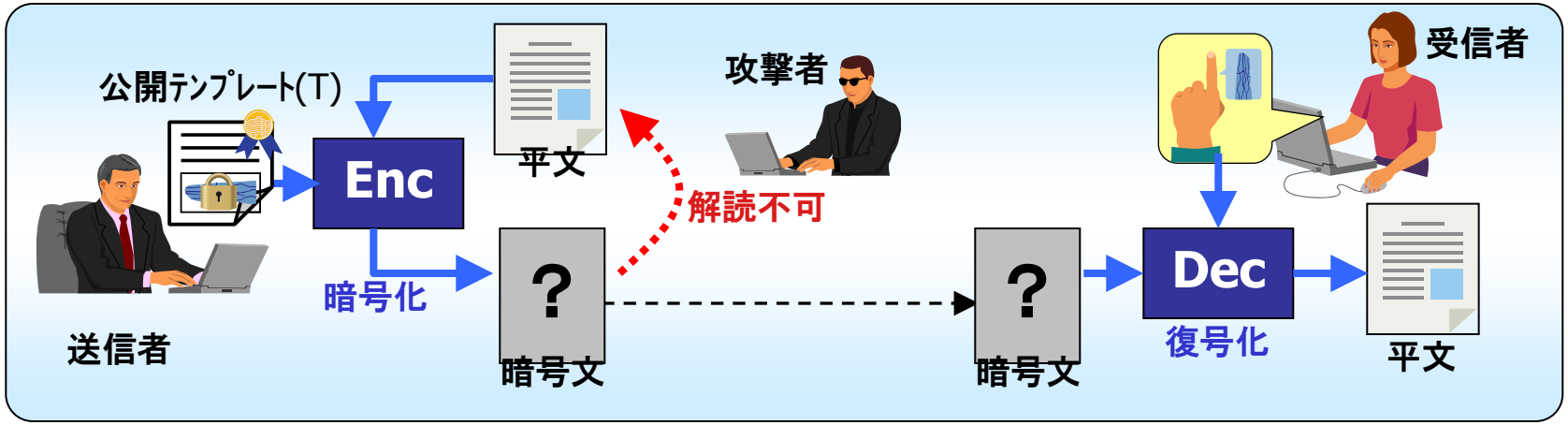
HITACHI
Inspire the Next

- 署名機能
  - 署名生成：メッセージ M，生体情報 X' を入力，署名文σを出力とするPPTA
    - σ=Sign(M,X')
  - 署名検証：メッセージ M，署名文σ，公開テンプレートTを入力とするPPTA
    - Verify(M,σ,T)="OK" or "NG"
  - **正当性**： X'≒X なら(圧倒的確率で) "OK" を出力
  - **安全性**： X'(≒X)を知らない攻撃者は署名を偽造できない



PBIの機能要件

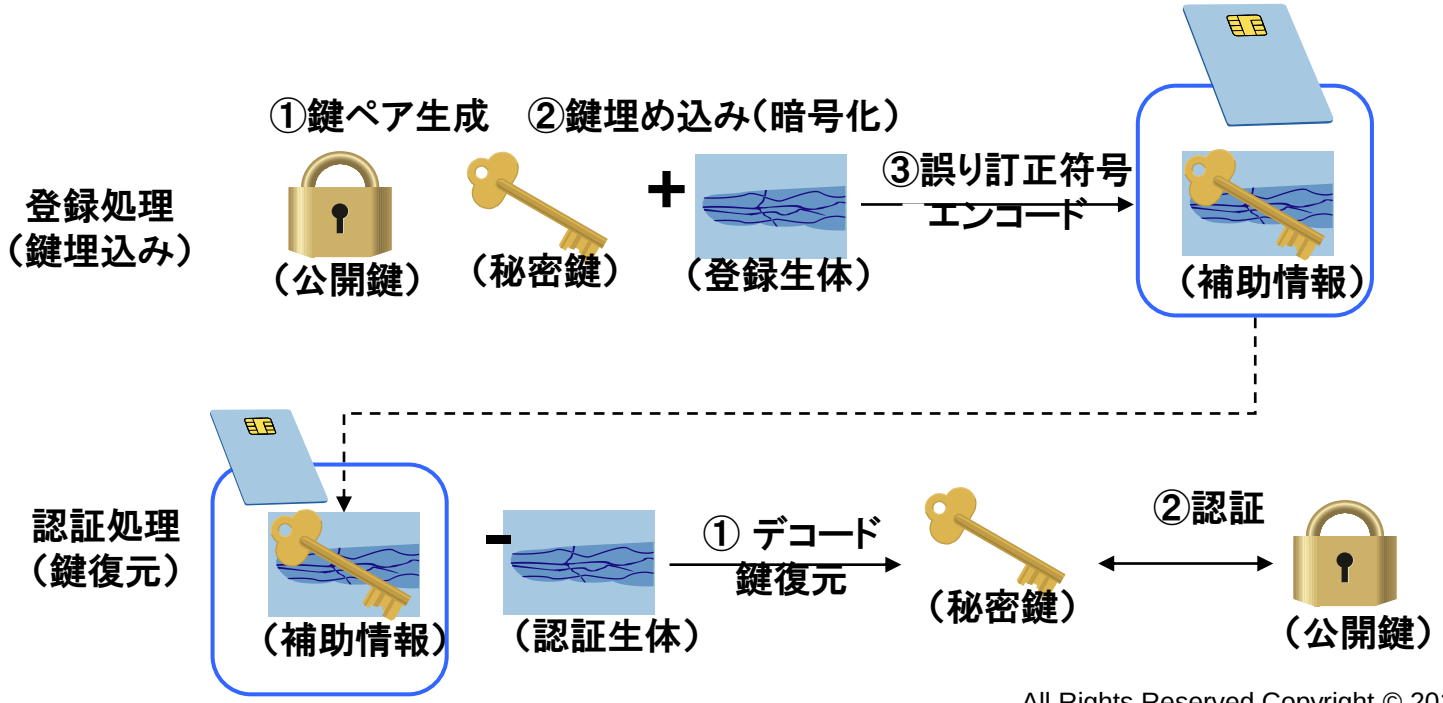
- （公開鍵）暗号機能
  - 暗号化：平文M，公開ﾃﾝﾌﾟﾚｰﾄTを入力，暗号文Cを出力とするPPTA
    - C=Enc(M,T)
  - 復号化：暗号文 C，生体情報 X' を入力，平文 M' を出力とするPPTA
    - M'=Dec(C,X')
  - **正当性**： X'≒X なら（圧倒的確率で） M'=M.
  - **安全性**： X'（≒X）を知らない攻撃者はMの部分情報を得ることができない.



要素技術の検討

HITACHI
Inspire the Next

- 既存技術： バイオメトリック暗号
  - 生体情報(曖昧な情報)を「共通鍵」とした共通鍵暗号
  - (公開鍵暗号の)「秘密鍵」を，生体情報で暗号化／復号化することで PBIの認証機能，暗号機能を実現可能
    - 生体情報で暗号化した「秘密鍵」の暗号文： 補助情報
  - 署名機能は実現不可
    - 署名生成アルゴリズムの入力として(メッセージ，生体情報に加えて)補助情報が必要



要素技術の検討

HITACHI
Inspire the Next

- その他の既存技術：
  - キャンセラブルバイオメトリクス，ZeroBIO
    - いずれも署名，暗号機能を実現できない

新たな要素技術（バイオメトリック署名）が必要

機能＼技術	Biometric Cryptosystems	Cancelable Biometrics	ZeroBIO
認証	○	△	○
署名	×	×	×
公開鍵暗号	○	×	×

バイオメトリック署名

HITACHI
Inspire the Next

- Fuzzy Signature (FS)
  - 秘密鍵に誤差を許す電子署名方式
  - 整数格子上のFuzzy Commitment と Schnorr署名を融合
- バイオメトリック署名：
  - 生体情報を鍵とする電子署名．特徴抽出器＋FS で実現可能

バイオメトリック署名

HITACHI
Inspire the Next

- Fuzzy Signature (FS)
  - 秘密鍵に誤差を許す電子署名方式
  - 整数格子上のFuzzy Commitment と Schnorr署名を融合(SCIS2012)
- バイオメトリック署名：
  - 生体情報を鍵とする電子署名．特徴抽出器＋FS で実現可能
  - バイオメトリック署名，バイオメトリック暗号の組み合わせにより
    認証・署名・暗号を全て実現 ⇒ PBIを実現可能

機能＼技術	Biometric Cryptosystems	Cancelable Biometrics	ZeroBIO	バイオメトリック署名
認証	○	○	○	○
署名	×	×	×	○
公開鍵暗号	○	×	×	×

まとめ

HITACHI
Inspire the Next

- テンプレート保護型生体認証技術
  - 生体情報は漏洩しても取り替えられない　⇒　厳密な保護が必要
  - 研究アプローチ
    - キャンセラブルバイオメトリクス
      - 生体情報を暗号化したまま照合
    - バイオメトリック暗号
      - 生体情報の誤差を誤り訂正符号等により補正し、秘密鍵を抽出して暗号プロトコル利用
    - ゼロ知識証明ベース
      - ゼロ知識証明プロトコル、準同型暗号等を用いて生体情報の「近さ」を証明
  - 既に実用化フェーズに入りつつある
  - 但し生体情報のエントロピーは現状小さく、データの分散管理が必須
- テンプレート公開型生体認証基盤（PBI）
  - 十分なエントロピーが確保できるなら、テンプレートを公開可能
    - 集中型（テンプレート保護）　⇒　分散型（PBI）
  - PBI：　生体情報を「鍵」とする認証，署名，公開鍵暗号基盤
    - バイオメトリック署名技術 ⇒ PBI の実現可能性