L-004

バイオメトリック認証システムに対するFTAによるリスク分析
Risk Analysis for Biometric Authentication Systems using FTA

清水 將吾† 瀬戸 洋一†
Shogo Shimizu Yoichi Seto

1. はじめに

バイオメトリック認証システムの安全性を確保するためには，データの漏えいによるプライバシー問題や漏えいデータの再利用によるなりすましの問題がある．これらの問題への対策として，データ暗号化，生体検知，キャンセラブルバイオメトリクスが開発されている．バイオメトリクスデータはもともと露出したものが多く，安全性確保においては，なりすまし対策が重要である．個々の技術は別々にその効果を論じられており，システム全体の安全性の確保の観点から，対策技術の適用効果や効果的な組合せについての検討がなされていない．本稿では，代表的な信頼性解析手法であるフォールトツリー分析（以下，FTA）を用いて，バイオメトリック認証システムの安全性に対するリスク分析を行う．本分析において作成したフォールトツリー（以下，FT）をもとに，各対策技術の有効性を定量的に評価することができる．

2. 脅威と対策技術

本稿で対象とするバイオメトリック認証システムの処理モデルを図 1 に示す．認証システムの内外の様々な箇所に脆弱性が存在し，これを利用した脅威が発生する．バイオメトリック認証システムの脆弱性と脅威は文献[1]に基づく．

なりすまし攻撃に対する一次的な対策技術として生体検知が挙げられるが，その他にも，物理的セキュリティ，認証アルゴリズムの精度改善，暗号化，電子署名，生体検知，チャレンジ&レスポンス型の認証プロトコル，キャンセラブルバイオメトリクス等，複数の技術が関係する（表 1 参照）．キャンセラブルバイオメトリクスは生体情報の特徴量を秘匿化するとともに，テンプレートが漏洩した際にそれを何度でも無効化・再発行可能にする技術であり，近年，多くのアルゴリズムが提案されている．

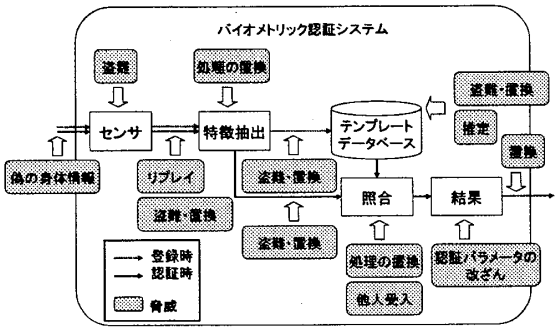

図 1 処理モデル

†公立大学法人首都大学東京産業技術大学院大学，
Advanced Institute of Industrial Technology, Tokyo Metropolitan University

表 1 なりすまし攻撃に対する対策技術

対策技術	概要
生体検知	センサに偽造した生体情報を提示する攻撃に対して有効（一次的な対策）
認証アルゴリズムの精度改善	偶発的な他人受入が起こるまで繰り返し入力を行う攻撃に対して有効
暗号化	転送部やテンプレートデータベースから元の生体情報や特徴量を盗む攻撃に対して有効
電子署名	データや処理，認証パラメータ，照合結果の不正な置換えに対して有効
物理的セキュリティ	センサやテンプレートデータベースからの不正なデータ持ち出しに対して有効
チャレンジ&レスポンス型の認証プロトコル	以前に入力された生体情報を再利用するリプレイ攻撃に対して有効
キャンセラブルバイオメトリクス	転送部やテンプレートデータベースから元の生体情報や特徴量を盗む攻撃に対して有効 生体情報の数を超えて再発行可能（可用性）

バイオメトリック認証システム全体の安全性の確保を目的としたとき，攻撃者には様々な手段があり，一つの対策技術では十分ではない．例えば，暗号化やキャンセラブルバイオメトリクスによりテンプレートの内容を保護しても，露出した残留指紋等から生体情報を復元され，システムに有効なテンプレートを生成される可能性がある．また，バイオメトリック認証システムを構築したり技術開発を行う場合，すべての機能を実現することは費用対効果の観点から現実的ではない．このため，各対策技術およびそれらの組合せについて安全性に関してどの程度の効果が得られるのかを見極め，実装に優先順位を付ける必要がある．次節では，対策技術の有効性の定量的評価を支援するための一手法について考察する．

3. 対策技術の有効性の評価

対策技術の有効性の評価を行うために，まず，バイオメトリック認証システムのリスク分析を行う．リスク分析の手法として，FTA を採用する．FTA は故障解析に広く用いられており，また，情報システムのセキュリティ対策立案等にも応用されている[2]．次に，FTA の結果から対策技術の有効性を評価する方法について述べる．

3.1 FTA によるリスク分析

FTA では，脅威の発生過程の因果関係を表した FT と呼ばれる木構造の論理図を作成し，この論理図を基に脅威の発生確率を算出してリスク評価を行う．FTA の網羅性を明確にするために事象分割型の FTA 手法[2][3]が提案されており，本稿でも同様の方針で行う．

まず，who（攻撃の行為者），when（脅威が発生する時点），where（脅威が発生する場所），what（攻撃の目的）の組合せによってすべての事象を抽出する．それぞれの項目の具体的な事象を以下に示す．

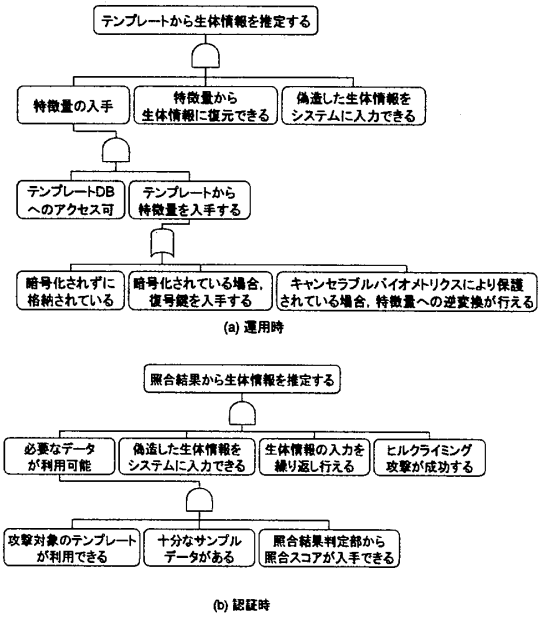

図 2　生体情報の推定によるなりすましの FT

- who：システム管理者，利用者
- when：登録時，運用時
- where：センサ，特徴抽出部，テンプレートデータベース，照合部，転送部，認証結果判定部，システム外部
- what：本人の生体情報と登録済みテンプレート以外の組合せを使用して認証に成功する，または，そのためのバックドアを生成する．

これら 4W の組合せを考慮して，なりすましが起こる事象を抽出する．抽出される脅威の例を以下に示す．

- 利用者が認証時に転送部でデータの改ざんができれば，センサでは本人の生体情報を入力し，通信路上で他人の生体情報またはテンプレートに置き換えることによって他人になりすますことができる．
- 管理者が運用時にテンプレートデータベースから他人のテンプレートを盗み出し，それを生体情報に復元して認証に使用することによってなりすましが行える．

次に，抽出された各事象を頂上事象として，脅威の発生過程に基づいて中間事象，基本事象に分割することで FT を作成する．例として，who=利用者，when=運用時，where=テンプレートデータベースの場合の FT を図 2(a)に，who=利用者，when=認証時，where=認証結果判定部の場合の FT を図 2(b)に示す．なお，図 2(b)の FT は文献[4]を参考に定義した．例えば，図 2(a)においてテンプレートから生体情報に復元するには，テンプレートから特徴量を入手でき，かつ，特徴量から生体情報に復元でき，かつ，偽造した生体情報をシステムに入力できる必要がある．他の FT も同様に作成する．

3.2 対策技術の有効性に関する考察

作成した FT の葉にあたる各基本事象に発生確率を与え，論理和・論理積の計算を頂上事象に向かって行うことで脅威の発生確率を求められる．リスクは脅威の発生確率に被害額を掛けることで定量化される．対策技術の適用は，基本事象の発生確率を低下させることに相当する．例えば，図 2(a)において，テンプレート保護にキャンセラブルバイオメトリクスを適用した場合，テンプレートから特徴量を入手できる確率を下げることにつながる．従って，対策技術の有効性は，それらを適用した場合の事象発生確率に基づくリスク評価値と適用しない場合の事象発生確率に基づくリスク評価値との差分によって測られる．この値を新たに必要な技術開発費や実装費と比較することによって，開発効果やシステム構成をより定量的に判断できる．また，利用者にシステムとしての安全性を説明する場合にも使用できる．発生確率の見積が難しい場合は相対的な発生頻度を与えるによって対策技術の効果に優先順位を付けることができる．

評価の例として，生体検知技術の有効性を考える．生体検知が有効であるのは，センサに偽生体情報が提示され，かつ生体検知機能が有効に機能する場合である．更に，前者は以下の二つの事象の論理和である．

(1) システム内部から他人のテンプレートを入手し，テンプレートから生体情報に復元し，復元した生体情報をシステムに提示する．
(2) システム外部から残留指紋等を入手し，それを元に作成した人工指等の生体情報をシステムに提示する．

テンプレートの暗号化やキャンセラブルバイオメトリクスは元の特徴量を秘匿化する機能をもち，上記(1)の中間事象であるテンプレートから生体情報の復元を困難にするが，(2)の事象に対しては有効ではない．一方，生体検知技術はいずれの場合にも有効であり，センサに偽生体情報が提示されるという脅威に関しては特徴量を秘匿化する技術よりも効果的であると言える．

また，テンプレートの盗難は安全性を阻害する脅威である他に，個人情報の漏洩というプライバシーの問題がある．しかし，テンプレートに格納されている情報は指紋や静脈等の画像特徴量であり，名前等の個人を特定する情報と関連付けられなければ秘匿化されていなくても問題にならないと考える．

4. おわりに

本稿では，バイオメトリック認証システムの安全性について FTA を用いてリスク分析を行った．本分析によって作成した FT に基づき，なりすまし攻撃に対する対策技術の有効性を定量的に評価することができる．

今後の課題としては，可用性に対するリスク分析と対策技術の評価が挙げられる．

参考文献

[1]瀬戸洋一編著, “ユビキタス時代のバイオメトリックセキュリティ”, 日本工業出版(2003).
[2]織茂昌之, 津原進, 山本倫子, 佐々木良一, “情報システムにおけるセキュリティ対策立案のための計画手法”, 情報処理学会論文誌, Vol.41, No.1, pp.177-187, (2000).
[3]臼井佑真, 間形文彦, 勅使河原可海, 佐々木良一, 西垣正勝, “事象分割型 FTA を用いたセキュリティ対策評価モデルの提案”, 2008 年暗号と情報セキュリティシンポジウム (SCIS2008), 4B1-4, (2008).
[4]A. Adler, “Sample image can be independently restored from face recognition template”, Can. Conf. Electrical Computer Eng., Vol.2, pp.1163-1166,(2003).