7 章　演習問題解答例

7.1　バイオメトリックシステムにおける脆弱性と脅威について、最低３つ挙げ、具体的な例を用い説明せよ。

（1）　脅威：センサへの偽の身体情報の提示
　　脆弱性：センサあるいは照合処理において偽造身体情報を検知できない。
　　例：　遺留指紋から、グミなど材料を用い偽造指紋を作り、指紋認証装置を不正アクセスする。
（2）　脅威：蓄積された身体情報の再入力
　　脆弱性：漏えいあるいは盗難されやすいデータ保管
　　例：　データベースに保管した暗号化されていない指紋データを盗み、偽造指紋を作成し、指紋認証装置にアクセスする。
（3）　脅威：
　　脆弱性：
　　例：

7.2　バイオメトリクス認証システムの安全性を高める技術としてキャンセラブルバイオメトリクス、生体検知技術、暗号化技術があるが、その優劣を論ぜよ。

解答例

バイオメトリック技術	内容	長所	短所
キャンセラブルバイオメトリクス	テンプレートデータを一方向関数で変換し、再発行できるようにする。	・テンプレートデータを再発行できる。	・標準化できないため、安全性の評価ができない。 ・照合精度の保存性が不明確。
生体検知	センサで身体情報を取得する時、センサあるいは照合アルゴリズムで、取得された身体情報が偽造でないことを検知する	・成りすましが防止できる基本的な機能	・検知能力を一定に保てない。つねに破られる攻撃が現れる。 ・実装すると製品が高価になる。 ・技術の標準化ができない。
暗号化技術	変換ルールを用いてデータを第三者が理解できない形にする。変換ルールが分かる者以外は、データをものに復元できない。この技術を用いてバイオメトリクスの添付レートデータを安全に保管する。	・標準化されている。 ・暗号化強度が明確。 ・ハードウエアが製品化されている。	

7.3

1. 図 1 に示すバイオメトリック認証システムの真正性について, 脅威分析を行いなさい. 真正性とは，利用者の本人性が確認できることである.
2. バイオメトリック認証システムの安全性を強化する方法として，暗号化，キャンセラブルバイオメトリクス，生体検知といった対策技術が挙げられている．なりすまし攻撃に対し，この中でどの対策技術が最も有効であるかリスク評価を行いなさい．その場合，FTA にて行いなさい.

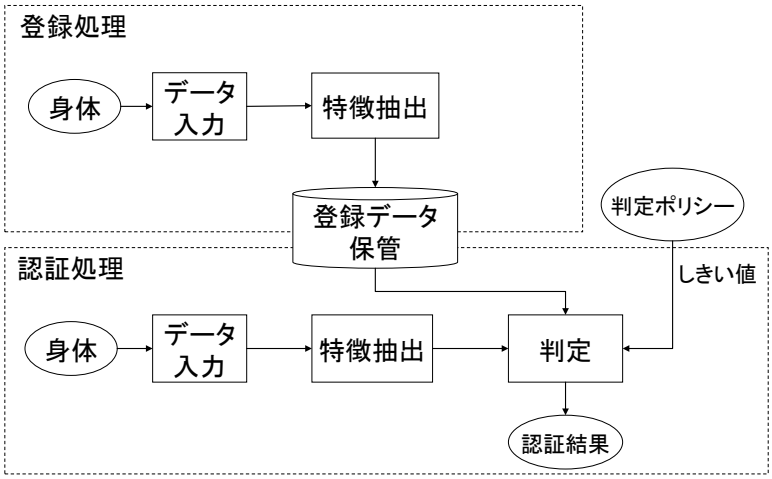

図 1 バイオメトリック認証システム

バイオメトリック認証システムの処理フローは次の通りである.

登録処理

1. 利用者から身体情報を取得する．例えば，顔認証の場合はカメラにより顔画像を，指紋認証の場合はセンサにより指紋データを取得する.
2. 入力された身体情報から個人特有の特徴を抽出する処理を行う.
3. 抽出された特徴量をテンプレートと呼ばれる登録データとしてデータベースに保管する.

認証処理

1. 利用者から身体情報を取得する.
2. 身体情報から個人特有の特徴を抽出する処理を行う．ここまでは登録処理と同じである.
3. 利用者を特定する利用者識別子を入力し，対応するテンプレートをデータベースから

選定する．選定されたテンプレートと上のステップにおいて抽出された特徴量との間の類似度を求める．この類似度が判定ポリシーで指定されたしきい値以上である場合は，認証に成功したと判定して，アプリケーションの利用権限を与える．

（参考）

FTA（Fault Tree Analysis）[1]

FTA とは，システムの信頼性解析をするための代表的な定量的リスク評価手法である．FTA では，(1) FT（Fault Tree）と呼ばれる，脅威の発生原因の因果関係を表した論理図を作成し，(2) 作成した FT に発生確率を付与することでリスクの定量分析を行う．

以下に，ある脅威に対する，FTA によるリスク分析手順を示す．

1. 解析対象とする脅威を FT の頂上事象に設定する．
2. 頂上事象の直接原因となる事象を頂上事象の下位に AND または OR 論理ゲートで関連付けて展開する．
3. 上で展開された事象（中間事象） を同様の方法でさらに下位に展開し，これ以上分解できないレベルの事象（末端事象）まで展開したら FT の作成を終了する．FT の例を図 2 に示す．

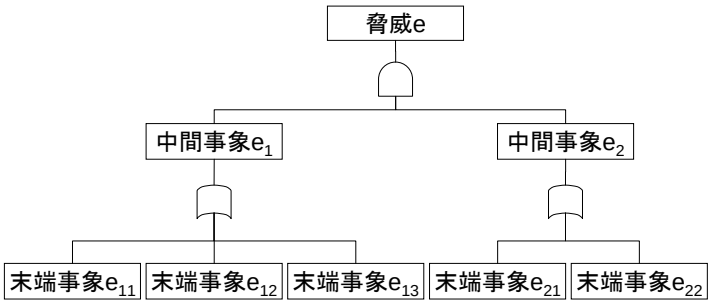

図 2 FT の例

4. 各末端事象に発生確率を付与し，計算式にしたがって頂上事象の発生確率を算出する．

なお，発生確率の計算式は以下の通りである．上位事象を e，e の下位事象を $e_1,\ldots,e_n$ とする．

AND ゲートの場合，$p(e)= p(e_1)\times p(e_2)\times\ldots\times p(e_n)$

OR ゲートの場合，$p(e)=1-(1- p(e_1)) \times(1-p(e_2))\times\ldots\times(1-p(e_n))$

5. 脅威の発生確率にその脅威の影響の大きさを表した数値を掛け合わせることで，リスク値を計算する．

リスク=発生確率×影響度

キャンセラブルバイオメトリクス[2]

バイオメトリクスは究極の個人情報であると同時に，身体の一部であり変更ができないという性質がある．この問題への対策として，キャンセラブルバイオメトリクスと呼ばれるテンプレート保護技術が提案されている．キャンセラブルバイオメトリクスは，元のバイオメトリック情報を復元不可能な手法で撹乱することによってテンプレートを生成する．また，テンプレートが漏洩した場合でも，再登録を行うことで元のテンプレートを無効化できる．この方式は非可逆変換を使用して元のバイオメトリック情報を歪曲するため，変換方式とテンプレートが既知の場合でも，元の身体情報に復元することは難しい．

生体検知[3]

生体検知は，特徴情報が生きている人間から取得されたものであるかどうかを確認する技術である．例えば，静電容量を利用した方式や光の反射を利用した光学方式等が提案されている．生体検知機能が搭載されたバイオメトリック認証システムでは，人工物等を用いて特徴情報を偽造することは困難である．

解答例

(1) バイオメトリック認証システムの脅威分析

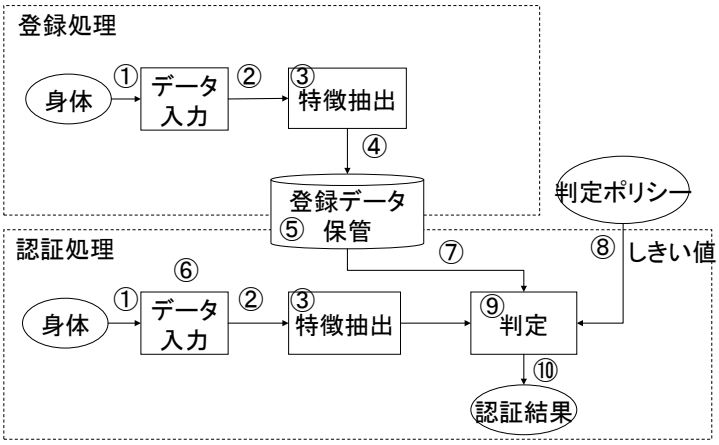

図 3 バイオメトリック認証システムの脅威

図 3 に示す箇所で以下のような脅威が発生する．

① センサへの偽の身体情報の提示

偽造の指，偽の署名，顔写真を貼った覆面等をセンサに提示する．

② センサから特徴抽出処理への転送部に対する攻撃

ネットワークまたはバスを攻撃して，センサから取得した身体情報を別の情報に置き換える．

③ 特徴抽出処理の置換え
特徴抽出処理に対してトロイの木馬等による攻撃を行い，任意の特徴を設定する．
④ 身体の特徴を示す情報の不正変換
入力信号から抽出された身体の特徴を示す情報を偽造した情報に置き換える．
⑤ 蓄積されたテンプレートの改ざん
認証用のテンプレートを格納したデータベースを改ざんし，不正な利用者に認証を与える，または正規の利用者を否認する可能性を引き上げる．
⑥ 蓄積された身体情報の再入力
センサを介さずに，センサ機器等に残存する身体情報を再入力する．
⑦ テンプレート格納機器から照合処理への転送部に対する攻撃
データベース上に保管されたテンプレートが通信チャネルを経由して照合処理部に送られる
ときにテンプレートを不正に変更する．
⑧ 照合閾値の置換え
判定ポリシーを書き換えることにより，照合閾値を任意の値に設定する．
⑨ 照合処理への攻撃
照合処理が行われる場所を攻撃し，照合処理の結果を任意のスコアに置き換える．
⑩ 最終決定のすり替え：認証の判定結果をすり替える．

上記の攻撃に対して，表 1 に示すような対策技術の適用が考えられる．

表 1 バイオメトリック認証システムの脅威と対策技術

	脅威	対策技術
①	センサへの偽の身体情報の提示	生体検知
②	転送中のデータの盗難・置換え	暗号化
③	特徴抽出処理の置換え	電子署名
④	身体の特徴を示す情報の不正変換	暗号化，キャンセラブルバイオメトリクス
⑤	テンプレートの盗難・置換え	物理的セキュリティ， キャンセラブルバイオメトリクス
⑥	残存した身体情報の再入力	生体検知，チャレンジレスポンス
⑦	転送中のテンプレートの盗難・置換え	暗号化，キャンセラブルバイオメトリクス
⑧	認証パラメータの変更	暗号化
⑨	本人拒否・他人受入の発生 照合処理の置換え	判定閾値の変更 電子署名
⑩	照合結果の改ざん	電子署名

(2) FTA による対策技術の有効性の評価

なりすまし攻撃に対する FT の例を図 4 に示す.

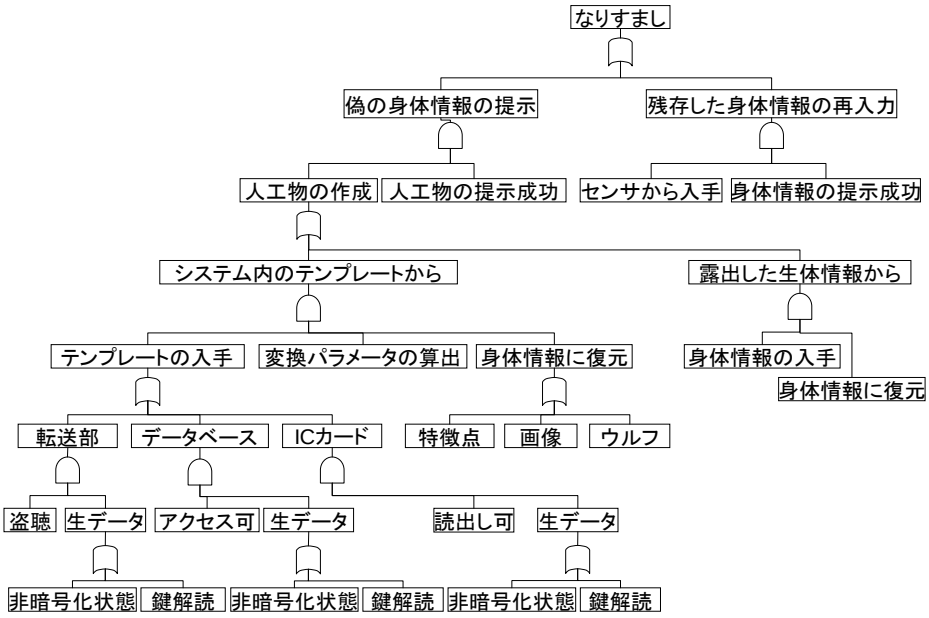

図 4 なりすまし攻撃に対する FT

暗号化とキャンセラブルバイオメトリクスは，システム内から漏洩したテンプレートを利用したなりすまし攻撃を防止するのに有効である．生体検知技術はシステム内から漏洩したテンプレートを利用したなりすまし攻撃，および，センサに遺留した指紋等の露出した生体情報を利用したなりすまし攻撃の両方に対して有効である.

以下に末端事象の発生確率の一例を表 2 に示す.

表 2 末端事象の発生確率の例

末端事象	発生確率（対策が適用されている場合）			
	なし	暗号化	キャンセラブル バイオメトリクス	生体検知
センサに残存する身体情報の入手	0.1	0.1	0.1	0.1
露出した生体情報の入手	0.3	0.3	0.3	0.3
露出した生体情報から身体情報に復元	0.3	0.3	0.3	0.3
キャンセラブルバイオメトリクスにおける変換パラメータの算出	-	-	0.1	-
特徴点から身体情報に復元	0.1	0.1	0.1	0.1
画像から身体情報に復元	0.3	0.3	0.3	0.3
ウルフから身体情報に復元	0.2	0.2	0.2	0.2
鍵の解読	-	0.01	-	-
データが暗号化されていない状態	1.0	0	1.0	1.0
通信の盗聴	0.1	0.1	0.1	0.1
データベースへのアクセス可	0.2	0.2	0.2	0.2
ICカード内データの不正読出し可	0.1	0.1	0.1	0.1
生きていない身体情報の提示が成功	1.0	1.0	1.0	0

次に，バイオメトリック認証システムに対して，暗号化，キャンセラブルバイオメトリクス，生体検知のそれぞれを適用した場合，および，いずれも適用しない場合について，対応する対策技術が既に適用されているという仮定のもとでの脅威（頂上事象）の発生確率を計算する．これらをもとに，例えば，中間事象である「露出した生体情報から人工の身体情報に復元できる」確率は次のように計算できる．

（露出した身体情報から人工の身体情報に復元できる確率）

=（露出した身体情報を入手できる確率）×（人工の身体情報に復元できる確率）

=0.3×0.3=0.09

同様の計算を頂上事象に達するまで繰り返し行う．損害をいずれの場合も同程度とすると，リスクの度合は脅威の発生確率により評価できる．それぞれの対策技術の有効性は，どの対策技術も適用しないときを基準としたときのリスク評価値の下降幅により，表 3 のように測ることができる．

表 3 脅威の発生確率

適用する対策技術	なし（基準）	暗号化	キャンセラブル バイオメトリクス	生体検知
脅威の発生確率	0.33	0.18	0.20	0.0
発生確率の下げ幅	-	0.15	0.13	0.33

この結果，これらの対策技術の中では生体検知技術が最も有効性が高いと結論できる．