平成１７年度経済産業省　産業技術研究開発委託事業－１
生体情報による個人識別技術（バイオメトリクス）を
利用した社会基盤構築に関する標準化

# 第５部　バイオメトリクスを可搬型メディアに応用するための技術調査

平成１８年３月

財団法人ニューメディア開発協会

## ５　バイオメトリクスを可搬型メディアに応用するための技術調査

### （１）　調査研究の目的

近年、重要施設に対する職員のアクセスを厳密にする目的で、可搬型メディアにバイオメトリクス情報を搭載し、それを用いて本人認証を行うニーズが高まっている（例：空港職員や原子力発電所職員など)。セキュリティを強化する目的でバイオメトリクス認証を用いる場合には、バイオメトリクス認証システム全体でのセキュリティ要件の検討が必要であるが、現状では個別システムに対しての検討が盛んであり、アーキテクチャや安全性の根拠に統一性がない。また、セキュリティシステムではその機能だけではなく運用も併せた検討が必要であるが、セキュリティ機能の検討に関してはバイオメトリクス認証の第一の課題である認証性能（認証精度やスループット）の確保といった点に注力されているうえ、運用に対する検討はそれ自体希少であるので、システム全体でのセキュリティについては体系的な議論があまりなされていないのが現状である。

一方、システム全体でのセキュリティを検討するためには、ＩＳＯ／ＩＥＣ １５４０８やＩＳＯ／ＩＥＣ ２７０００シリーズといった手法を用いるのが最適であるが、これらの各標準は現状ではまだシステム設計者に浸透していないだけでなく、個別のシステム毎に一から分析していくのは大変な労力を必要とする。

そこで以下の２点を目的とし、システム全体に対する機能要件と運用要件の両方を併せ持ったセキュリティ要件として「セキュリティプロファイル」を作成すること。および、セキュリティプロファイルを国際標準化の場に提案することで国際貢献することを目的とする。

- ＩＳＯ／ＩＥＣ １５４０８やＩＳＯ／ＩＥＣ ２７０００シリーズなどの標準的手法を組み合わせて分析・整理することで、セキュリティ要件のシステム全体での網羅性を確保する。
- 個別システム設計者が、本セキュリティプロファイルを採用することによって、各種標準手法に詳しくなくとも専門家が設計するのと同様な効果が得られるようにする。

平成１６年度はセキュリティプロファイル検討における基礎的な部分を実施したが、今年度は、平成１６年度の成果を引き継ぎ、以下の内容を検討した。

（ａ）セキュリティプロファイルの仕様拡充

平成１６年度はトークンを使用した職員認証システム（バイオメトリクスによる検証機能）を適用対象としたセキュリティプロファイルを策定したが、今年度はその適用範囲を広げ、バイオメトリクステンプレートを生成しトークンに格納するバイオメトリクス登録システムのためのセキュリティ仕様を検討した。

（ｂ）国際規格素案の策定と業界内の意見集約・合意形成

平成１６年度成果と上記（ａ）による仕様拡充部分の国際標準案を策定し、国内外標準化機関へ提案した。また標準案策定にあたり、バイオメトリクスセキュリティコンソーシアム運用仕様策定部会ホームランドセキュリティタスクフォース内のセキュリティプロファイルサブワーキンググループを継続して活用し、業界有識者のコメント収集及び合意形成を行った。

（2）　委員会

本調査はバイオメトリクス・セキュリティ・コンソーシアム（以下ＢＳＣ）運用仕様策定部会のホームランドセキュリティタスクフォースのサブワーキンググループ（以下ＳＷＧ）において、以下の通りレビューを受けた。

1）　ＳＷＧメンバ

表 5-1 ＳＷＧメンバ

| | 氏名 | 所属 |
|---|---|---|
| 主査 | 梅田　伸明 | （株）NTT データ |
| 委員 | 道坂　修 | （株）NTT データ |
| 委員 | 白方　貴史 | （株）NTT データ |
| 委員 | 磯部　義明 | （株）日立製作所 |
| 委員 | 新崎　卓 | （株）富士通研究所 |
| 委員 | 坂本　静生 | 日本電気（株） |
| 委員 | 笹川　耕一 | 三菱電機（株） |
| 委員 | 星　佳典 | 沖電気工業（株） |
| 委員 | 松本　泰 | セコム（株） |
| 委員 | 平野　誠治 | 凸版印刷（株） |
| 委員 | 半田 富己男 | 大日本印刷（株） |
| 委員 | 植村　泰佳 | ECSEC |

| | 氏名 | 所属 |
|---|---|---|
| 委員 | 池野　修一 | BSC 基盤技術部会長 |
| オブザーバ | 滝沢　俊男 | （財）ニューメディア開発協会 |
| オブザーバ | 林　義昭 | （財）ニューメディア開発協会 |

２）　レビュー日程

表 5-2 レビュー実施日程

| 回数 | 日程 | レビュー実施場所 |
|---|---|---|
| 第１回 | 平成１７年３月１８日 | （財）ニューメディア開発協会会議室 |
| 第２回 | 平成１７年４月１５日 | |

## ５．１　セキュリティプロファイルの仕様拡充

### ５．１．１　今年度取り組み概要

平成１７年度は平成１６年度における取り組みを継続し、可搬型メディアとバイオメトリクスの組み合わせによる本人認証システムにおけるセキュリティ機能要件と運用要件の検討を一通り終えることができた。具体的には以下の検討を実施した。

- 昨年度検討した本人確認部のプロテクションプロファイルを元に機能要件を抽出した。
- 昨年度定義したシステム要件を元に運用要件を検討・整理した。
- 機能要件と運用要件をマージしセキュリティプロファイル ver1.0 として要件をまとめた。
- 本人確認部での検討手順に従い、未検討であったアカウント登録部に関しても同様の検討を行った。
- アカウント登録部における検討結果を、セキュリティプロファイル ver1.0 へマージし、セキュリティプロファイル ver2.0 として要件をまとめた。

以上の検討を通して、これまでに類のない機能面と運用面の両面からのセキュリティ要件を検討・整理することができた。具体的なセキュリティプロファイルの検討結果に関しては、 次節以降で詳しく記述する。

５．１．２　　検討の範囲

バイオメトリクス認証システムにおいて考慮すべきセキュリティ脅威としては、主に「なりすまし」「個人情報漏洩」「システム停止」などが挙げられる。従って、これら全ての脅威に対してセキュリティ要件を検討する必要があるが、重要施設に対する職員のアクセスを厳密にする目的での本人認証において最大の脅威は「なりすまし」であり、正当な職員になりすまされることで重大な被害をこうむることとなる。そこで、本セキュリティプロファイルでは、「なりすまし」防止に絞って検討することとした。

ただし、「なりすまし」と密接な関係がある認証精度に関しては、システム毎に使用する製品が異なるとともに、製品選定においてある程度解決できることから、本セキュリティプロファイルでは、認証精度以外の脆弱性を利用した「なりすまし」を対象として対策を検討した。

５．１．３　　検討のアプローチ

一般に、セキュリティ要件（機能要件、運用要件）を検討する際には、ＩＴシステムの機能要件の検討方法の世界標準であるＩＳＯ／ＩＥＣ　１５４０８の手法と、情報セキュリティの運用管理方法の事実上の標準であるＩＳＯ／ＩＥＣ　２７０００シリーズの手法を利用して検討する方法が考えられる。ＩＳＯ／ＩＥＣ　１５４０８とＩＳＯ／ＩＥＣ　２７０００シリーズの組み合わせ方は様々な方法があるが、本セキュリティプロファイルの検討では、ＩＳＯ／ＩＥＣ　１５４０８をベースにした上で運用要件を詳細化する部分でＩＳＯ／ＩＥＣ　１７７９９（将来ＩＳＯ／ＩＥＣ　２７００２となる予定）から抜粋する方法を採った。具体的には以下の手順で分析した。

手順１：　脅威分析

ＩＳＯ／ＩＥＣ　１５４０８に従い、検討対象とする業務概要・守るべき資産・システム構成・関連するプレイヤ・周辺環境、を可能な限り定義し、起こりうる脅威を分析する。

手順２：　機能要件検討

分析した脅威への対策方針を検討し、ＩＳＯ／ＩＥＣ　１５４０８のｐａｒｔ２より機能要件を抜粋することで対策方針を詳細化する。

手順３：　運用要件検討

機能要件検討と平行で実施し､機能要件で対策できない脅威に対する運用による対策方針を検討する。ＩＳＯ／ＩＥＣ　１７７９９より管理策を抜粋することで対策方針を詳細化する。また、脅威への対策だけでなく、脅威分析の際に前提と

した周辺環境とするための要件もＩＳＯ／ＩＥＣ １７７９９の管理策によって詳細化する。

上記の手順で検討した後、機能要件と運用要件を組み合わせることで、「なりすまし」を防止するためのセキュリティ要件としてまとめた。

### ５．１．４　　対象とするシステムの定義

#### （１）　　業務概要

本セキュリティプロファイルでは「職員の厳密な本人確認を必要とする業務全般」を想定し、万が一のテロ行為などで重大な被害が起こりうる可能性のある、基幹インフラ、機密情報、重要施設におけるアクセスが限られた職員およびそれに準じる従業員に対する認証業務とする。

また、想定環境としては、守るべき資産が存在するエリアに対する物理的なアクセス制御のためのゲート施設での職員認証とし、ゲート数は数十程度とする。このような環境における職員の具体的な例としては、空港職員、航空会社クルー、原子力発電所職員などがある。

職員およびそれに準じる従業員を認証するにあたり、本セキュリティプロファイルでは、トークンデバイスに格納した指紋データを用いた指紋認証を行うことを想定する。また、関連する業務としては、本来の目的である入退室管理を行うために必要な「本人確認業務」と、事前準備として実施される「アカウント登録業務」が存在する。

#### （２）　　システム基本定義

ゲート数が数十程度の規模を想定することから、本人確認部はゲートごとに設置することとし、外部ネットワークで接続された認証用サーバ等は想定しない。

生体テンプレート格納方式はトークンデバイスに格納する方式とし、検証行為毎にキャプチャされる検証用指紋データと、トークンデバイスから読み出した生体テンプレートを、トークンデバイスの外部で比較することで照合スコアを計算する方式とする。

各種ゲートは単独で動作しており、ゲート間やオープンなネットワークなどとは接続されておらず、クローズドなシステムとする。

生体認証システムは、関連する国際標準に準拠して作成されており、API や生体テンプレートフォーマット等はオープンであることとする。例えば、バイオメトリクスに関してはＩＳＯ／ＩＥＣ １９７８４、ＩＳＯ／ＩＥＣ １９７９４－２もしくはＩＳＯ／

ＩＥＣ １９７９４－４には最低限準拠しているものとする。また、トークンデバイスに関しては接触型の場合はＩＳＯ／ＩＥＣ ７８１６、非接触型の場合にはＩＳＯ／ＩＥＣ １４４４３に最低限準拠しているものとする。

（３） システム構成

以下の図 5-1 に本セキュリティプロファイルが対象とする範囲を示す。入退室管理システムは、大きくアカウント登録部、本人確認部、アクセス制御部、職員情報管理部、ゲート開閉部に分けられる。この５つの機能ブロックの中で、生体認証処理に関するものは、アカウント登録部および本人確認部の２つである。以降、本セキュリティプロファイルでは、特にアカウント登録部と本人確認部を合わせて生体認証システムと呼び、生体認証システムに対するセキュリティプロファイルを策定していく（アクセス制御部、職員情報管理部、ゲート開閉部は、本セキュリティプロファイルの対象外とする）。

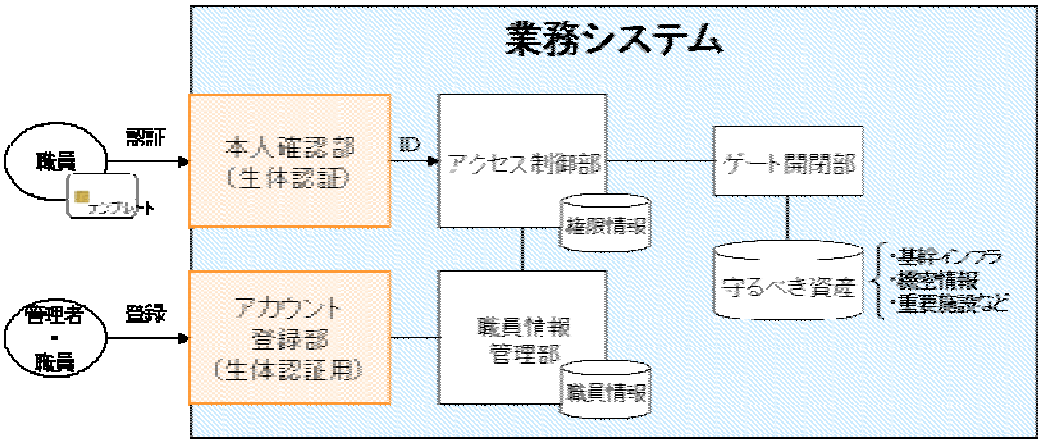


**図 5-1 対象とするシステム**

以下にそれぞれの部位に関する説明を記述する。

１） アカウント登録部

ゲートを通過する権限を与える職員およびそれに準じる従業員から、テンプレートとなる指紋情報を採取し、認証トークンに格納する部分である。

２） 本人確認部

職員からライブで採取した指紋情報と認証トークン内に格納している職員のテンプレート情報を照合し、職員の本人性を確認する部分である。

３）　アクセス制御部

本人確認部の結果を受けて、本人であると判定された職員が、ゲートを通過する権限を持っているかどうかを判定する部分である。アクセス制御部は、ゲートごとに通過可能な職員の権限情報を持っている。本検討の対象外。

４）　職員情報管理部

認証トークンと職員の紐付け情報や、その他氏名など、職員に関する情報を管理する部分である。本検討の対象外。

５）　ゲート開閉部

アクセス制御部の結果を受けて、物理的にゲートを開閉する部分である。本検討の対象外。

（４）　守るべき資産

セキュリティプロファイルを検討する上で想定する保護対象資産は、前述した本人確認部によって職員が識別・確認され、その後アクセス制御部などによって通過が制限されているエリアに存在するもの全てとする（これをプライマリ資産と呼ぶ)。また、本人確認部およびアカウント登録部が正常に動作するために必要なデータや設備も保護対象とした（これをセカンダリ資産と呼ぶ)。以下にそれぞれの定義を記述する。

【プライマリ資産】

セキュリティプロファイルの対象である生体認証システムの範囲内にはプライマリ資産は存在しない

つまり、通過が制限されているエリアに存在する資産は紙文書、金庫、国土、国民などが挙げられるが、生体認証システム（本人確認部およびアカウント登録部）は入退室管理システムにおける本人確認を担う部分であるので、生体認証システムの管轄内には保護対象資産は存在しない。ここで対象とする生体認証システムは、本人確認を確実にすることで資産の保護に貢献することが目的となる。

【セカンダリ資産】

- 指紋認証システムに特化した静的情報（例：閾値、認証用パラメータなど）
- システム動作中の動的生成データ（例：指紋画像など）
- システム監査のための情報（例：監査ログ、日付情報など）

（5）　ファシリティ

本セキュリティプロファイルで前提とする物理環境は、高セキュアな環境とする。具体的なイメージとしては、守るべき資産が納められている領域へアクセスするためには、生体認証を用いた本人認証システムを通過しなければならない。また、本人認証システムおよびアカウント登録施設に到達するまでには、一つまたは複数のゲート（例えば、守衛が立っている場合や、物理的な鍵が設置されている場合がある）を通過していなければならない。すなわち、本人認証システムには、不特定多数の人物ではなく、一般職員および特定職員のみしか到達できないような環境を前提とする（Fig. 4-3: Facilities Assumed for the Security Profile
）。

また、ファシリティ要件に関しては本プロファイルのスコープ外であるので、特に想定しないが、充分なセキュリティを保っているものとする。

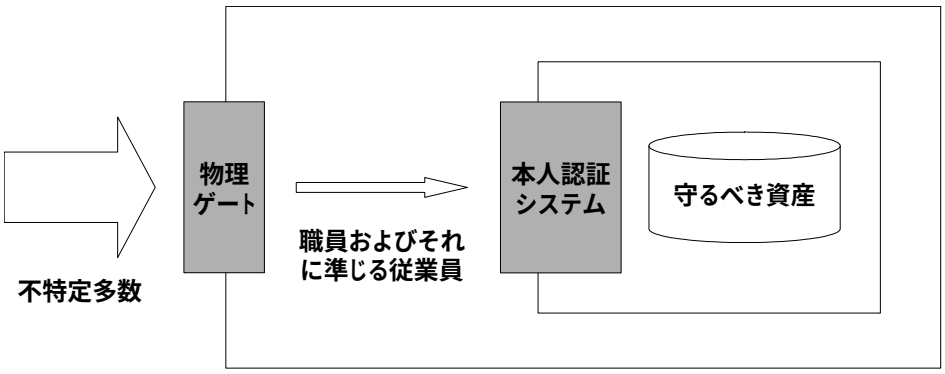


**図 5-2　想定する物理環境**

５．１．５　　本人確認部、アカウント登録部に共通なセキュリティ運用要件の検討

本節では、前節にて記述した対象とするシステムにおける基本的セキュリティ要件について検討した結果を記述する。基本的要件としては運用管理が主体となるため、運用要件のみを検討した。次節以降ではここで定義した運用が行われていることを前提とした上で脅威分析、セキュリティ要件検討を行った。なお、運用要件の策定にあたっては、ＩＳＯ／ＩＥＣ　１７７９９：２０００を参考にした。

運用要件は本節と次節以降において以下のように大きく３つの観点で検討・定義した。従って、各運用要件には下記３つのセクションを大分類として、さらにその下に中分類・

小分類を設け運用管理の対象を詳細化し、さらに小分類ごとには具体的管理策（コントロール）を設定した。なお、各管理策には一意の番号を付与している（Fig. 6-2: Numbering Rule of Operational Profiles
）。この管理策には、必須項目とオプション項目を設定しており、オプション項目は、実アプリケーションにおいて、守るべき資産と対策未実施のリスクを評価し、費用対効果を検討した上で適用を判断するべき項目とした。

- 基本事項
  生体認証システムを、セキュリティを確保しながら運用していく場合に必要となる基本的な要件を策定する。
- アカウント登録時のセキュリティ
  職員情報の登録時に必要となる運用要件を策定する。システム構成図におけるアカウント登録部に焦点を当てる。
- 本人確認時のセキュリティ
  職員の本人確認時に必要となる運用要件を策定する。システム構成図における本人確認部に焦点を当てる。

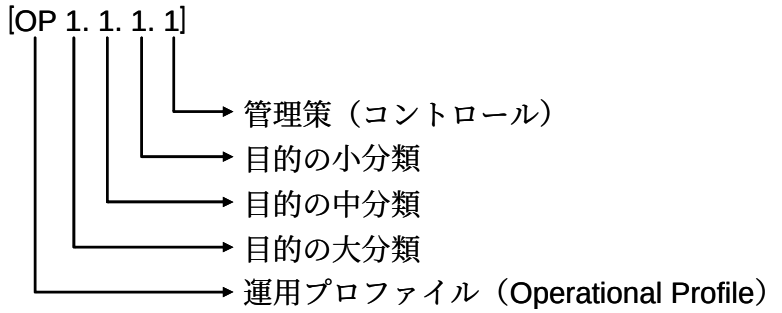


**図 5-3 運用要件での番号規則**

運用要件は具体的には、生体認証システムをセキュリティを確保した状態で運用していくために必要な「生体認証システム基本方針」の確立、その基本方針を遵守して運用していくための「組織のセキュリティ」に関する枠組み、職員の役割に関する「人的セキュリティ」、およびシステム運用管理に関する「通信および運用管理」である。以下に検討結果である要件の詳細を記述する。

（1） 生体認証システム基本方針

生体認証システムを、セキュリティを確保した状態で運用していくために、そのセ

キュリティ方針を明確化し、全職員に対して意識させる必要がある。そこで、生体認証システムの運用に対し、組織内にて生体認証システムの管理責任者を置き、生体認証システムのセキュリティ方針を文書化することが望ましい。

[OP 1.1.1.1] 生体認証システム基本方針文書を作成し、生体認証システムの運用管理責任者によって承認され、適当な手段で、全職員に公表し、通知すること。【必須】

[OP 1.1.1.2] 生体認証システム基本方針は、定められた見直し手続きに従って、基本方針の維持および見直しが行われること。【必須】

（２） 組織のセキュリティ

１） 情報セキュリティ基盤

生体認証システムを運用する組織内において、情報セキュリティを導入し、その実施状態を統制するための管理上の枠組みを確立することが望ましい。

[OP 1.2.1.1] セキュリティを主導するための明瞭な方向付けのための、運営委員会を設置すること。【必須】

[OP 1.2.1.2] 運営委員会は、適切な責任分担および十分な資源配分によって、セキュリティを促進すること。【必須】

[OP 1.2.1.3] 個々の資産の保護に対する責任および特定のセキュリティ手続きの実施に対する責任を、明確に定めること。【必須】

[OP 1.2.1.4] 新しい情報処理設備に対する運営委員会による認可手続きを確立すること。【オプション】

[OP 1.2.1.5] 専門家による情報セキュリティの助言を内部または外部の助言者から求め、組織全体を調整すること。【オプション】

２） 第三者によるアクセスのセキュリティ

特定職員以外の第三者が、業務上、資産が納められている領域へアクセスすることが必要となる場合、セキュリティとの関連を明確化するためにリスクアセスメントを実施し、セキュリティの要求事項が記載されている契約を組織と第三者が取り交わし、資産のセキュリティを維持することが望ましい。

[OP 1.2.2.1] 施設への第三者のアクセスに関連づけてリスクを評価し、適切な管

理策を実施すること。【必須】

（3）　資産の管理

生体認証システムを導入することによって保護しようとする資産が何であるかを明確にし、適切な保護を確実にすることが望ましい。

[OP 1.3.1.1]　生体認証システムそれぞれに関連づけて、重要な資産について目録を作成し、維持すること。【必須】

（4）　人的セキュリティ

1）　職務定義および雇用におけるセキュリティ

人による誤り、盗難、不正行為、または設備の誤用のリスクを軽減するために、職員を採用する段階からセキュリティの責任について言及し、その採用候補者を十分に審査することが望ましい。また、セキュリティ責任を雇用契約に盛り込み、雇用中はその監視を行うことが望ましい。

[OP 1.4.1.1]　セキュリティの役割および責任は、生体認証システム基本方針で定められたとおりに、適切に文書化すること。【必須】

[OP 1.4.1.2]　職員は、雇用条件の一部として、機密保持契約書または守秘義務契約書に署名すること。【必須】

2）　職員の訓練

情報セキュリティの脅威および懸念に対する職員の認識を確実なものとし、通常の業務の中で職員が生体認証システム基本方針を維持していくことを確実にし、生じうるセキュリティリスクを最小とするために、生体認証システムを利用する職員を訓練することが望ましい。

[OP 1.4.2.1]　生体認証システム基本方針および手順について、組織のすべての職員および関係する外部利用者を適切に教育し、並びに定期的に更新教育を行うこと。【必須】

3）　セキュリティ事件・事故および誤動作への対処

セキュリティ事件・事故および誤動作による損害を最小限に抑えるため、並びに

そのような事件・事故を監視してそれらから学習するために、セキュリティに影響を及ぼす事件・事故が発生した場合の報告、およびシステムの弱点の報告を職員に徹底させることが望ましい。また、組織は、セキュリティ違反を犯した職員に正式な懲罰手続きを確立することが望ましい。

[OP 1.4.3.1] セキュリティ事件・事故は、適切な連絡経路を通して、できるだけ速やかに報告すること。【必須】

[OP 1.4.3.2] 生体認証システムの利用者に対して、システムのセキュリティの弱点、またはそれらへの脅威に気づいた場合若しくは疑いをもった場合は、注意を払い、かつ報告するよう要求すること。【必須】

[OP 1.4.3.3] ソフトウェアの誤動作を報告する手順を確立すること。【必須】

[OP 1.4.3.4] 事件・事故および誤動作の種類、規模並びに費用の定量化および監視を可能とする仕組みを備えていること。【オプション】

[OP 1.4.3.5] 生体認証システム基本方針および手順に違反した職員に対する、正式な懲戒手続を備えていること。【必須】

（５） 通信および運用管理

１） 運用手順および責任

生体認証システムの正確、かつ、セキュリティを保った運用を確実にするために、全ての情報処理設備の管理・運用の責任および手順を確立することが望ましい。

[OP 1.5.1.1] 生体認証システム基本方針の付属とするセキュリティ個別方針によって明確化した操作手順は、文書化して維持していくこと。【必須】

[OP 1.5.1.2] 生体認証システムの変更について管理すること。【必須】

[OP 1.5.1.3] セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うことができるように、事件・事故管理の責任および手順を確立すること。【必須】

[OP 1.5.1.4] 情報若しくはサービスの無認可の変更または誤用の可能性を小さくするために、ある種の職務若しくは責任領域の管理または実行の分離を考慮すること。【オプション】

２） 悪意のあるソフトウェアからの保護

ソフトウェアおよび情報の完全性を保護するために、悪意のあるソフトウェアの侵入を防止し、検出するための、予防の措置を行うことが望ましい。

[OP 1.5.2.1] 悪意のあるソフトウェアから保護するための検出および防止の管理策、並びに利用者に適切に認知させるための手順を導入すること。【必須】

3） システムの維持管理

生体認証システムの完全性および可用性を維持するために、データのバックアップの取得およびその復元、並びに作業記録を残すことが望ましい。

[OP 1.5.3.1] 極めて重要な業務情報およびソフトウェアのバックアップは、定期的に取得し、かつ検査すること。【必須】

[OP 1.5.3.2] 運用担当者は、自分の作業の記録を継続すること。【必須】

[OP 1.5.3.3] 運用担当者の記録は、定期的に独立した検査をうけること。【オプション】

[OP 1.5.3.4] 障害については報告を行い、是正処置をとること。【必須】

4） ネットワークの管理

ネットワークにおける情報の保護、およびネットワークを支える基盤の保護を確実にするために、ネットワークのセキュリティ管理を行うことが望ましい。

[OP 1.5.4.1] ネットワークにおけるセキュリティを実現し、かつ維持するために、一連の管理策を実施すること。【必須】

5） 媒体の取り扱いおよびセキュリティ

資産に対する損害および事業活動に対する妨害を回避するために、媒体を管理し、物理的に保護することが望ましい。

[OP 1.5.5.1] 取り外し可能な付属媒体（例えば、テープ、ディスク、カセット）および印刷された文書の管理手順があること。【必須】

[OP 1.5.5.2] 媒体が不要となった場合は、安全、かつ、確実に処分すること。【必須】

[OP 1.5.5.3] 認可されていない露呈または誤用から情報を保護するために、情報

の取り扱いおよび保管についての手順を確立すること。【必須】

[OP 1.5.5.4]　認可されていないアクセスから生体認証システムに関する文書を保護すること。【必須】

## ５．１．６　　アカウント登録部における脅威分析およびセキュリティ要求仕様の検討

本節では、５．１．４節で定義したシステムにおいて、５．１．５節で検討した基本的な運用がなされているものと前提した上で、アカウント登録部における脅威分析およびセキュリティ要件検討を行った結果を記述する。

### （１）　　アカウント登録業務想定

**アカウント登録業務は、新規登録・再発行・生体テンプレート更新の３つの場合が考えられるが、業務フローは全て** Fig. 4.1: Task Workflow

に示す手順で実施されるものとする。

| 事前確認業務 | 指紋テンプレート採取業務 |
|---|---|
| 【新規登録・再発行・テンプレート更新】<br>申請書作成 → 申請 → 申請内容チェック → | 指紋採取 → トークン格納 → トークン発行 |

**図 5-4　業務フロー**

アカウント登録業務フローをバイオメトリクス認証に特化するかどうかで二つに分割し、バイオメトリクス認証に特化しない申請内容チェックまでを事前確認業務と呼び、バイオメトリクス認証に特化する指紋採取以降を指紋テンプレート採取業務と呼ぶことにする。また、以下にそれぞれのフローに関する説明を記述する。

【申請書作成】

新規作成･再発行･テンプレート更新のそれぞれにおいて､必要な書類を作成し、また、必要に応じて身分を証明する書類を用意する。

【申請】

申請受付窓口などで申請書や身分証明書､使用中の認証トークン等を提出し申請する。

【申請内容チェック】

申請受付窓口の受付担当者等が申請内容のチェック・申請者の本人確認・認証トークンのチェックなどを実施する。ただし、バイオメトリクス認証技術による１：N照合は想定しない。

【指紋採取】

申請内容チェックをパスした申請者から指紋データを採取し､テンプレートを作成する。

【トークン格納】

生成したテンプレートをトークンデバイスへ格納する｡テンプレートだけでなく、業務上必要なデータも格納し、認証トークンとして完成させる。(必要に応じてトークン表面への印刷なども実施)

【トークン発行】

作成した認証トークンを申請者へ受け渡す。本セキュリティプロファイルでは、その場で発行することを想定し、後日引き渡すパターンは想定しない。従って、引渡しの際の本人確認はないものとする。

（２）　脅威分析

１）　脅威の考え方

脅威を検討するにあたり、本人確認部と同様に攻撃者が正当な職員に「なりすます」ことに関する脅威のみを分析した。よって、以下のようなセキュリティ脅威は対象外とした。

【サービス停止および登録未対応によるシステム利用不可】

⇒ 「なりすまし」目的の登録時の不正にはサービス停止や登録未対応は脅威とはならず、また、未対応者への代替措置は検討の対象外とする

【プライバシ情報（生体情報など）の漏洩】

⇒ 別途プライバシ情報の保護対策としてプロファイルを定義すべき

2）　システム構成要素分析

アカウント登録部におけるシステム構成要素としては、以下の４つの要素から構成されるものとした。

【指紋読み取り機能】

アカウントを登録する際に、認証トークンに格納する指紋情報を読み取るための機能であり、指紋センサ、指紋センサドライバソフトなどから構成される。

【トークン書き込み機能】

アカウントを登録する際に、職員から採取した指紋のテンプレートとＩＤを認証トークンに書き込むための機能であり、トークンリーダ、トークンリーダドライバソフトなどから構成される。

【職員情報入力機能】

アカウントを登録する際に、職員の各種情報（氏名・役職など）を入力するための機能であり、キーボード、ディスプレイ装置、入出力ソフトなどから構成される。

【テンプレート生成機能】

アカウントを登録する際に、指紋読み取り機能で読み取った職員の指紋情報を、認証トークンへ格納するテンプレート情報に変換する機能であり、指紋特徴の抽出処理、エンコーディング処理などから構成される。

3）　プレイヤ分析

アカウント登録部に関わるプレイヤとしては、４種の職員が想定され、それぞれ以下に示すような特徴を持っているものとした。

**表 5-3 想定プレイヤ**

| 役割 | 説明 | 想定 | 例 |
|---|---|---|---|
| 部外者 | 守るべき資産を保有する組織に所属しておらず、資産へのアクセス権だけでなく、あらゆる権限を持っていない。 | 資産へのアクセス権を得るために不正を行う可能性を持つ。テロ組織や犯罪組織へ所属している可能性も考慮する。 | ・犯罪者<br>・テロリスト |

| 役割 | 説明 | 想定 | 例 |
|---|---|---|---|
| 一般職員 | 守るべき資産を保有する組織に所属しているが、資産へのアクセス権を持たない職員。資産以外へのアクセス権は持っている。 | 資産へのアクセス権を得るために不正を行う可能性を持つ。過去にテロ組織等に所属していた可能性も考慮する。 | ・一般社員<br>・アルバイト |
| 特定職員 | 守るべき資産を保有する組織に所属しており、かつ、資産へのアクセス権を持っている職員。 | 一般職員や部外者が資産へアクセスできるよう結託して不正行為を実施する可能性を持つ。過去にテロ組織等に所属していた可能性も考慮する。 | ・管理職<br>・特定業務担当者 |
| 登録担当者 | 守るべき資産を保有する組織に所属しており、資産へのアクセスするための認証トークンを発行する業務に従事する職員。 | 悪意はなく、他のプレイヤと結託することはない。 | － |

4）　攻撃発生箇所分析

最後に、プレイヤが攻撃する箇所についての分析を行った結果、以下の図 5-5 のような結果となった。

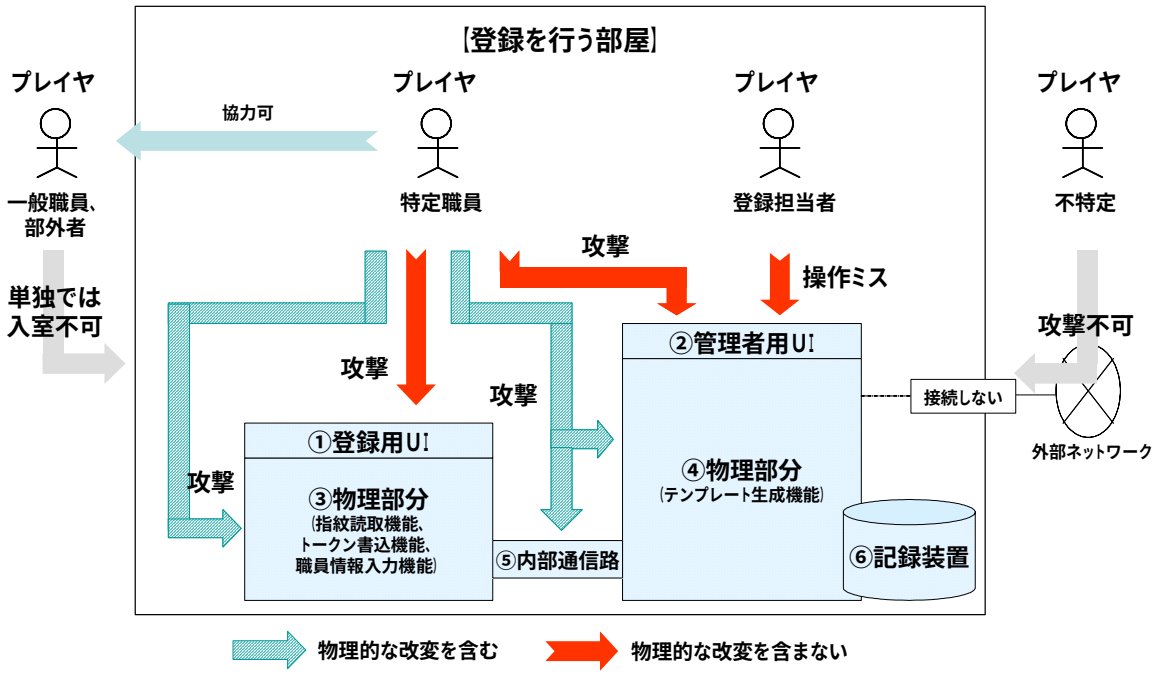


**図 5-5 プレイヤと攻撃発生箇所（アカウント登録部）**

5） 脅威詳細

前述した１）～４）の分析を元に、脅威を検討し抽出した結果を以下に記述する。ただし、事前確認業務と指紋テンプレート採取業務でそれぞれ独立して検討を実施した。

（a） アカウント登録部（事前確認業務時）

アカウント登録業務のなかで、生体認証に特化しない事前確認業務時における脅威は以下のものとなった。

| | |
|---|---|
| 脅威 | 特定職員に成りすまして登録する |
| 識別子 | T.Pre_Impersonate |
| 内容 | 本脅威は、資産の存在する部屋に入ることが許された特定職員になりすまして認証トークンを作成する脅威とする。一般職員が特定職員になりすますものと、部外者が特定職員になりすますものが想定される。 |

| | |
|---|---|
| 脅威 | 不適切な人物を登録する |
| 識別子 | T.Pre_Suspicious_Staff |

| | |
|---|---|
| 内容 | 本脅威は、たとえ業務上は資産へのアクセス権限を持っている特定職員であったとしても、セキュリティ上では不適切な（過去にテロ組織等に属していた等）人物が登録を行い、認証トークンを作成する脅威とする。特定職員の中に危険な思想をもった者が居る可能性は否定できない。 |

| | |
|---|---|
| 脅威 | テンプレート更新時に他の特定職員の認証トークンを使って更新する |
| 識別子 | T.Pre_Fake_Token |
| 内容 | 本脅威は、なんらかの方法で入手した特定職員の認証トークンを使い、テンプレート更新を行うことで、更新完了後に自分の認証トークンとして使えるようにする脅威とする。 |

（b） アカウント登録部（指紋テンプレート採取業務時）

アカウント登録業務のなかで、生体認証に特化する指紋テンプレート採取業務時における脅威は以下のものとなった。なお、脅威を想定する上で、前述した事前確認業務時の脅威はここでは発生しないものと前提した。また、脅威の記述にあたっては、その特性によって本人確認部と同様に以下の３種に分類した。

- 生体認証に特化した脅威
- 本人認証システムに共通な脅威
- ＩＴシステムに共通な脅威

ａ） 生体認証に特化した脅威

| | |
|---|---|
| 脅威 | 人工物を使って任意の指紋を登録する |
| 識別子 | T.Bio_Artifact_Enroll |
| 内容 | 本脅威は、特定職員がキャプチャデバイスに対して物理的な人工物を使って任意の指紋を登録する脅威とする。他人の指紋を登録することによって、登録された指紋の持ち主が不正に入室権限を得ることができる。 |

| | |
|---|---|
| 脅威 | 低品質のテンプレートを登録する |
| 識別子 | T.Bio_Poor_Enroll |
| 内容 | 本脅威は、特定職員が故意または偶然に低品質のテンプレートを登録することで、本人認証時に他人が成りすませる可能性が高くなる脅威とす |

| | |
|---|---|
| | る。一般に低品質のテンプレートが他人受入率を高くするとは言えないが、その可能性は否定できない。 |

ｂ）　本人認証システムに共通な脅威

| | |
|---|---|
| 脅威 | 登録担当者のミスで別人の認証トークンを発行する |
| 識別子 | T.Authsys_Wrong_Enroll |
| 内容 | 本脅威は、登録担当者が登録業務を行う際に、入力ミス等によって登録申請者とは別の職員の認証トークンとして発行してしまう脅威とする。別人の認証トークンとして発行された場合、本人認証時に別人になりすますことが可能となる。 |

ｃ）　ＩＴシステムに共通な脅威

| | |
|---|---|
| 脅威 | 登録担当者権限を不正獲得する |
| 識別子 | T.ITsys_Usurp_Admin |
| 内容 | 本脅威は、登録担当者でないものが登録機能を実行可能になる脅威とする。登録機能を悪用することによって、不正に認証トークンを発行することが可能となる。 |

| | |
|---|---|
| 脅威 | 不正行為や攻撃を検出できないことにより被害が拡大する |
| 識別子 | T.ITsys_Undetect |
| 内容 | 本脅威は、様々な攻撃や不正行為の痕跡が残らないことで、上記脅威の発生の検知がおくれ、被害が拡大してしまう脅威とする。攻撃を受けたことに気づかないだけでなく、操作ミスなのか攻撃を受けたのかの判別もつかなくなる。 |

（３）　セキュリティ要件検討

１）　機能要件

本節では、前述の脅威に対しＩＴ機能で対応すべきセキュリティ要件の検討結果を記述する。要件の策定にあたっては、ＩＳＯ／ＩＥＣ １５４０８ Ｐａｒｔ２を参考にした。

機能要件は本節と次節以降において以下のように大きく２つの観点で検討･定義した。従って、各機能要件には下記２つのセクションを大分類として、さらにその下に中分類・小分類を設け、機能を詳細化した。なお、機能要件には一意の番号を付与している（図 5-6)。この機能要件には、必須項目とオプション項目を設定しており、オプション項目は、実アプリケーションにおいて、守るべき資産と対策未実施時のリスクを評価し、費用対効果を検討した上で適用を判断するべき項目とした。

- アカウント登録部のセキュリティ機能
  職員情報の登録時に利用されるＩＴシステムに必要となる機能要件を策定する。システム構成図におけるアカウント登録部に焦点を当てる。
- 本人確認部のセキュリティ機能
  職員の本人確認時に利用されるＩＴシステムに必要となる機能要件を策定する。システム構成図における本人確認部に焦点を当てる。

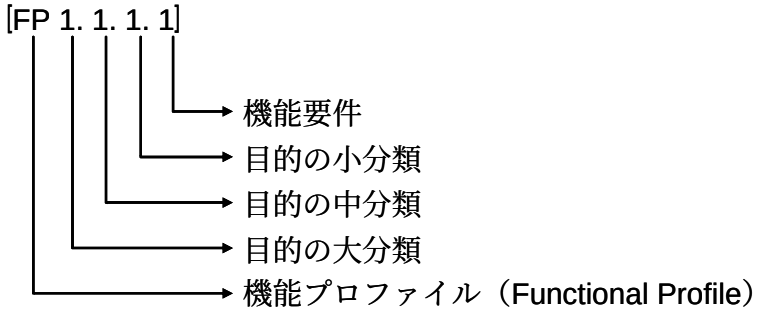


**図 5-6 機能要件での番号規則**

（ａ） 識別・認証

ａ） 利用者認証

[FP 1.1.1.1] 登録担当者としての認証が成功するまでは管理機能は何も実行できないようにすること。【必須】

[FP 1.1.1.2] 登録担当者を認証する際には、複数の認証機構を使用すること。【オプション】

ｂ） 偽造されない認証

[FP 1.1.2.1] 偽造された人工指によるキャプチャ行為を検出できること。【オプション】

ｃ） 利用者識別

[FP 1.1.3.1] 登録担当者としての識別が成功するまでは管理機能は何も実行できないようにすること。【必須】

ｄ） 認証失敗

[FP 1.1.4.1] 認証行為の失敗回数がある一定回数を超えた場合にはそれを検出し、また、管理者に対してその旨を通知すること。【必須】

[FP 1.1.4.2] 認証行為の失敗回数がある一定回数を超えた場合にはそれを検出し、それ以降一定期間の間は当該利用者の利用を停止すること。【必須】

（ｂ） セキュリティ監査

ａ） セキュリティ監査データ生成

[FP 1.2.1.1] 以下の監査対象事象の監査記録を生成できること。【必須】

a) 監査機能の起動と終了
b) 認証トークン発行
c) 登録担当者ログイン・ログアウト
d) 登録担当者認証失敗がある一定回数を超えた場合
e) その他セキュリティ侵害と考えられる事象

[FP 1.2.1.2] 各監査記録において少なくとも以下の情報を記録すること。【必須】

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)
b) その他の監査関連情報

[FP 1.2.1.3] 各監査対象事象を、その原因となった利用者の識別情報に関連付けること。【必須】

ｂ） セキュリティ監査事象格納

[FP 1.2.2.1] 監査証跡が事前に定義された限界を超えた場合、管理者に対して警

告を発すること。【オプション】

[FP 1.2.2.2] 監査証跡が意図せず消失しないように記録媒体の二重化によって防止すること。【オプション】

[FP 1.2.2.3] 監査証跡が意図せず消失しないように格納媒体を Read Only にすること。【オプション】

（ｃ） セキュリティ管理

ａ） セキュリティ属性の管理

[FP 1.4.1.1] 目的精度をみたす指紋データの品質である指紋データだけが登録されること。【オプション】

ｂ） 管理機能の特定

[FP 1.4.2.1] 指紋キャプチャ時に指紋データの品質確認プロンプト表示を行うこと。【必須】

[FP 1.4.2.2] 指紋キャプチャ時に指紋画像の確認プロンプト表示を行うこと。【オプション】

[FP 1.4.2.3] 認証トークン発行時に記録内容の確認プロンプト表示を行うこと。【必須】

[FP 1.4.2.4] 誤って認証トークンを発行したことが判明した場合には、アクセス制御部へ直ちに通知を行うこと。【必須】

（ｄ） タイムスタンプ

[FP 1.5.1.1] 時刻サーバへ問い合わせて、時刻情報を補正できること。【オプション】

[FP 1.5.1.2] 高精度時計を内蔵し、正確な時刻情報を利用すること。【オプション】

２） 運用要件

本節では、前述の脅威に対し人による運用で対応すべきセキュリティ要件の検討結果を記述する。要件の策定にあたっては、ＩＳＯ／ＩＥＣ １７７９９：２０００を参考にしたが、生体認証に特化したものなどについては新たに作成した。なお、番号付与方法に関しては、５．１．５章における図 5-3 に従った。

（ａ）　人的セキュリティ

ａ）　職務定義および雇用におけるセキュリティ

人による誤り、盗難、不正行為、または設備の誤用のリスクを軽減するために、職員を採用する段階からセキュリティの責任について言及し、その採用候補者を十分に審査することが望ましい。

[OP 2.1.1.1]　職員採用時の応募資料の検査において、公的証明書（パスポート又は同種の文書）の検査をすること。【必須】

[OP 2.1.1.2]　職員採用時の応募資料の検査において、履歴書の検査をすること。【必須】

[OP 2.1.1.3]　請負業者及び臨時職員に対しても同様の審査手続きを実施すること。【必須】

[OP 2.1.1.4]　かなりの権限を持つ地位に就く職員については、この調査を定期的に行うこと。【オプション】

[OP 2.1.1.5]　職員採用時に、組織は応募者に対して信用調査を行うこと。【オプション】

[OP 2.1.1.6]　職員採用時に、組織は応募者に対して要注意人物リストとの照合を行うこと。【オプション】

（ｂ）　物理的および環境的セキュリティ

ａ）　セキュリティが保たれた領域

業務施設および業務情報に対する認可されていないアクセス、損傷および妨害を防止するために、セキュリティ境界を明確にし、識別されたリスクに対応した保護対策を施すことが望ましい。

[OP 2.2.1.1]　テンプレート登録業務を実施する部屋を保護するために、幾つかのセキュリティ境界を利用すること。【必須】

[OP 2.2.1.2]　登録申請者だけにアクセスを許すことを確実にするために、適切な入退管理策によってテンプレート登録業務を実施する部屋を保護すること。【必須】

[OP 2.2.1.3]　テンプレート登録業務を実施する部屋のセキュリティを強化するために、その領域での作業のための管理策（複数人による監視など）

および指針を追加すること。【必須】

ｂ）　装置のセキュリティ

資産の損失、損傷または劣化、および業務活動に対する妨害を防止するために、装置は、セキュリティに対する脅威および環境上の危険から物理的に保護されることが望ましい。

[OP 2.2.2.1]　テンプレート登録用装置は、環境上の脅威および危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置または保護すること。【オプション】

[OP 2.2.2.2]　データ伝送または情報サービスに使用する電源ケーブルおよび通信ケーブルの配線は、傍受または損傷から保護すること。【オプション】

[OP 2.2.2.3]　テンプレート登録用装置についての継続的な可用性および完全性の維持を確実とするために、テンプレート登録用装置の保守を正しく実施すること。【オプション】

（ｃ）　アクセス制御

ａ）　アクセス制御に関する業務上の要求事項

情報へのアクセスおよび業務手続きは、業務およびセキュリティの要求事項に基づいて管理する必要があり、この場合、情報を伝える範囲およびアクセスの認可に対する個別方針を定義することが望ましい。

[OP 2.3.1.1]　アクセス制御についての業務上の要求事項を定義し、文書化すること。【必須】

[OP 2.3.1.2]　テンプレート登録端末へのアクセスは、安全なログオン手続を経て達成されること。【必須】

[OP 2.3.1.3]　全ての職員（一般職員・特定職員）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（職員 ID）を保有すること。【必須】

[OP 2.3.1.4]　脅迫の標的となり得る職員のために、脅迫に対する警報（duress alarm）を備えることを考慮すること。【オプション】

ｂ）　利用者のアクセス管理

認可されていないアクセスを防止するために、アクセスを許可するための、正規の利用者登録手続があることが望ましい。

[OP 2.3.2.1]　事前確認業務において、申請者が資産を含む領域へのアクセスに対して、システムの実務管理者から認可を得ているかを検査すること。【必須】

[OP 2.3.2.2]　事前確認業務において、申請者の本人確認書類を用いた本人確認をすること。【必須】

[OP 2.3.2.3]　事前確認業務において、申請者に対して要注意人物リストとの照合をすること。【オプション】

[OP 2.3.2.4]　テンプレートを更新する際には、事前確認業務において、申請者の所持する認証トークン内に格納された情報または認証トークン表面に印刷された情報を使用して本人確認すること。【必須】

[OP 2.3.2.5]　テンプレートを更新する際には、事前確認業務において、申請者の所持する認証トークンを用いて、指紋認証による本人確認をすること。【オプション】

[OP 2.3.2.6]　テンプレート登録業務において、採取された指紋データの品質が十分かどうかを確認すること。【必須】

[OP 2.3.2.7]　登録担当者に対して、テンプレート登録時のミスを防ぐよう適切にテンプレート登録方法に関して教育し、ならびに定期的に更新教育すること。【必須】

[OP 2.3.2.8]　テンプレート登録業務において、十分な品質の指紋データが採取できない場合には、指紋データの品質が向上するような措置（指紋採取用クリームを使用するなど）を講じること。【オプション】

ｃ）　システムアクセスおよびシステム使用状況の監視

許可されていない活動を検出するために、アクセス制御方針からのずれを検出し、セキュリティ事件・事故の場合に証拠となるようにするとともに、監視可能な事象を記録するために、システムを監視することが望ましい。

[OP 2.3.3.1]　例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査およびアクセス制御の監視を補うために、合意された期間保存すること。【必須】

[OP 2.3.3.2] 生体認証システムの使用状況を監視する手順を確立すること。【必須】

[OP 2.3.3.3] 監視の結果は、定期的に見直すこと。【オプション】

[OP 2.3.3.4] システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること。【オプション】

[OP 2.3.3.5] コンピュータの時計は正しく設定すること。【必須】

[OP 2.3.3.6] コンピュータの時計は定期的に確認すること。【必須】

（d） 利用環境のセキュリティ

特定職員の指紋データを採取する場合は、その採取環境は本人確認時と同一にすることが望ましい。また、採取時には、採取対象となるモダリティの特徴を変形または隠すような行動、その他要因を制御することが望ましい。さらに指紋データを採取するセンサの時間経過による劣化にも随時対処することが望ましい。

ａ） 指紋データ採取環境の管理

[OP 2.4.1.1] 指紋データの採取環境は、生体認証システム基本方針で定められたとおりに、適切に文書化すること。【必須】

[OP 2.4.1.2] 指紋データの採取環境は、利用する製品に応じて適切に設定されること。【必須】

ｂ） 利用者環境の管理

[OP 2.4.2.1] テンプレート登録時の行動に関する指針を文書化すること。【必須】

[OP 2.4.2.2] 特定職員および登録担当者に対して、生体特徴の変形を促すような行動、およびその他影響があるであろう要因を防ぐよう適切に教育し、テンプレート登録時には適宜指導すること。【必須】

[OP 2.4.2.3] 登録担当者に対して、人工指に関するセキュリティ脅威に関して教育し、ならびに定期的に更新教育すること。【必須】

[OP 2.4.2.4] テンプレート登録時の行動を適宜監視すること。【必須】

ｃ） 生体センサの管理

[OP 2.4.3.1] 指紋データを採取するためのセンサは、継続的な可用性および完全性の維持を確実とするために、常に一定の環境となるように保守を行うこと。【必須】

[OP 2.4.3.2] 指紋センサは、電源異常から保護すること。【オプション】

[OP 2.4.3.3] データ伝送に使用する通信ケーブルの配線は、傍受または損傷から保護すること。【オプション】

（ｅ） 代替手段

アクセスの認められた特定職員が、利用するモダリティの怪我、喪失、その他要因により生体認証システムを利用できない場合、業務上の必要性により、代替手段を提供しなければならない。また、そもそも組織の決定したモダリティを持ち合わせていない特定職員を資産にアクセスさせる必要がある場合、生体認証システム以外の代替手段による本人認証が必要になる。

ａ） 生体が損傷した時の代替手段

[OP 2.5.1.1] 指紋が怪我、喪失、その他要因によって利用できない場合の代替手段に関する要求事項を定義し、文書化すること。【必須】

[OP 2.5.1.2] 代替手段を利用した特定職員を管理すること。【オプション】

ｂ） 未対応者への代替手段

[OP 2.5.2.1] 未対応者に対する代替手段に関する要求事項を定義すること。【必須】

ｃ） 代替手段の見直し

[OP 2.5.3.1] 代替手段は、定められた見直し手続きに従って、維持および見直しが行われること。【必須】

（ｆ） 認証トークンの盗難・紛失

特定職員が認証トークンを盗難された場合、または紛失した場合に、当該認証トークンに対するテンプレート情報の更新処理は行わないことが望ましい。

ａ） 認証トークン盗難・紛失時の管理策

[OP 2.6.1.1] 認証トークンの盗難･紛失時の要求事項を定義し、文書化すること。【必須】

[OP 2.6.1.2] 盗難・紛失が判明している認証トークンによるテンプレート更新は行わないこと。【オプション】

## ５．１．７　本人確認部における脅威分析およびセキュリティ要求仕様の検討

本節では、５．１．４節で定義したシステムにおいて、５．１．５節で検討した基本的な運用がなされているものと前提した上で、本人確認部における脅威分析およびセキュリティ要件検討を行った結果を記述する。

### （１）　本人確認業務想定

本人確認時の業務フロー等については特に想定せず、物理的な施設に設けられたゲート施設に設置された指紋認証装置を使って、職員が認証を行うものとした。

### （２）　脅威分析

#### １）　脅威の考え方

脅威を検討するにあたり、攻撃者が正当な職員に「なりすます」ことに関する脅威のみを分析した。よって、以下のようなセキュリティ脅威は対象外とした。

【サービス停止および登録未対応によるシステム利用不可】

⇒ システムが利用不可状態になっても、「なりすまし」はできない、また、登録未対応者などへの救済措置として、運用での対処がされるはずであるが、代替システムに対するセキュリティ侵害は対象外とする

【プライバシ情報（生体情報など）の漏洩】

⇒ 別途プライバシ情報の保護対策としてプロファイルを定義すべき

#### ２）　システム構成要素分析

本人確認部におけるシステム構成要素としては、以下の３つの要素から構成されるものとした。

【指紋読み取り機能】

認証を受けようとする者が本人確認部に対して指紋情報を入力するための機能であり、指紋センサ、指紋センサドライバソフトなどから構成される。

【トークン読み取り機能】

認証を受けようとする者が本人確認部に対して認証トークンを入力するための

機能であり、トークンリーダ、トークンリーダドライバソフトなどから構成される。

【指紋情報の照合、本人性判定機能】

指紋読み取り機能から出力された指紋情報と、トークン読み取り機能から出力された指紋テンプレートを比較照合し、その照合結果と本人性の判断基準となる閾値とをさらに比較し、その結果によって本人かどうかを判定する機能である。

指紋特徴の抽出処理、指紋情報の照合処理、本人性判定処理などから構成される。

3）　プレイヤ分析

本人確認部に関わるプレイヤとしては、３種の職員が想定され、それぞれ以下に示すような特徴を持っているものとした。

**表 5-4 想定プレイヤ**

| 役割 | 説明 | 想定 | 例 |
|---|---|---|---|
| 一般職員 | 守るべき資産を保有する組織に所属しているが、資産へのアクセス権を持たない職員。資産以外へのアクセス権は持っている。 | 一般職員や部外者が資産へアクセスできるよう結託して不正行為を実施する可能性を持つ。 | ・一般社員<br>・アルバイト |
| 特定職員 | 守るべき資産を保有する組織に所属しており、かつ、資産へのアクセス権を持っている職員。 | 一般職員や部外者が資産へアクセスできるよう結託して不正行為を実施する可能性を持つ。 | ・管理職<br>・特定業務担当者 |
| 管理者 | 生体認証システムの運用管理を行う職員。 | 悪意はなく、他のプレイヤと結託することはない。 | － |

4）　攻撃発生箇所分析

最後に、プレイヤが攻撃する箇所についての分析を行った結果、以下の図 5-7 のような結果となった。

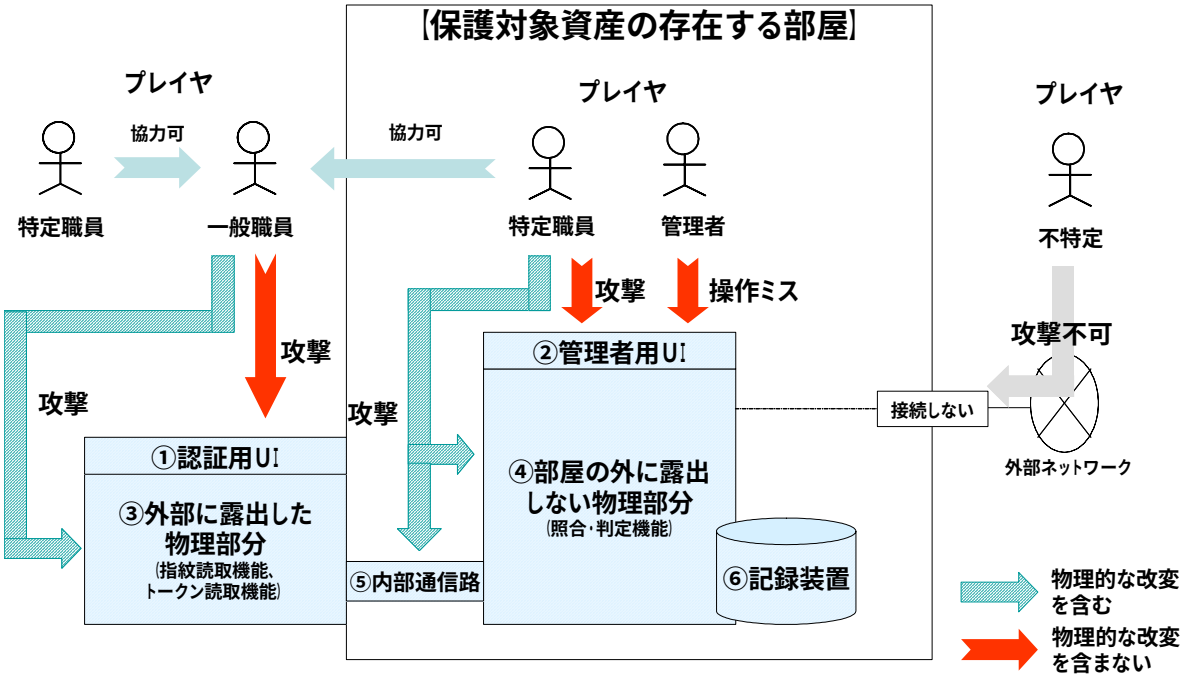


図 5-7　プレイヤと攻撃発生箇所（本人確認部）

５）　脅威詳細

前述した１）～４）の分析を元に、脅威を検討し抽出した結果を以下に記述する。脅威の記述にあたっては、その特性によって以下の３種に分類した。

- 生体認証に特化した脅威
  攻撃方法が指紋認証のみに有効であると考えられる「なりすまし」脅威。
- 本人認証システムに共通な脅威
  本人認証の方式（生体認証、パスワード認証、持ち物認証など）に関わらず、人を認証するシステムに共通に発生する「なりすまし」脅威。
- ＩＴシステムに共通な脅威
  ＩＴシステムに一般的に存在する攻撃手法によって、結果的に生体認証システムの「なりすまし」につながる脅威。

（ａ）　生体認証に特化した脅威

| 脅威 | 人工指紋によるなりすまし |
|---|---|
| 識別子 | T.Bio_Artifact |

| | |
|---|---|
| 内容 | 本脅威は、キャプチャデバイスに対して物理的な人工物を使ってなりすましを試みる脅威とする。人工物は、検証時にキャプチャされた指紋情報やテンプレートから作成されるかもしれないし、なりすまし対象者の日常生活から取得した情報から作成されるかもしれない。 |

| | |
|---|---|
| 脅威 | 指紋センサやメモリ上の残留情報によるリプレイ攻撃によるなりすまし |
| 識別子 | T.Bio_Replay |
| 内容 | 本脅威は、物理的に指紋キャプチャデバイスのセンサ面などに付着した指紋情報をそのまま利用してなりすましを試みる脅威と、ＩＴ機器のメモリなどに残留しているデジタル情報をそのまま利用してなりすましを試みる脅威とする。 |

| | |
|---|---|
| 脅威 | テンプレートの改変・偽造によるなりすまし |
| 識別子 | T.Bio_Fake_Template |
| 内容 | 本脅威は、テンプレートの改変・偽造・すり替えなどによって、正当なテンプレートではなく攻撃者のテンプレートを使用させることによってなりすましを試みる脅威とする。テンプレートはテンプレート格納部と比較照合部との通信路で攻撃にあうかもしれないし、テンプレート格納部そのものを偽造・改ざんするかもしれない。 |

| | |
|---|---|
| 脅威 | 閾値などを改変することによるなりすまし |
| 識別子 | T.Bio_Wrong_Parameter |
| 内容 | 本脅威は、閾値などの認証パラメータを改変することによって、本人性判定結果を狂わせ、なりすましを試みる脅威とする。認証パラメータはパラメータ変更機能で改変されるかもしれないし、直接記録デバイスへアクセスして改変されるかもしれないし、パラメータ格納部と処理モジュールの転送路で改変されるかもしれない。 |

| | |
|---|---|
| 脅威 | 認証精度に起因するなりすまし |
| 識別子 | T.Bio_Accuracy |
| 内容 | 本脅威は、指紋認証の認証精度が 100%ではないことや、個別の指紋認証製品や使用環境によって認証精度が変化するなどの脆弱性を利用してなりすまされる脅威とする。(例:特徴の似た人 Wolf・Sheep などの特性)。 |

| | |
|---|---|
| 脅威 | 想定外環境での使用によるなりすまし |
| 識別子 | T.Bio_Bad_Condition |
| 内容 | 本脅威は、システムが設置される環境が指紋センサやトークンリーダが推奨する環境から逸脱し、誤動作を起こすことによってなりすまされる脅威とする。 |

（b） 本人認証システムに共通な脅威

| | |
|---|---|
| 脅威 | ブルートフォース攻撃によるなりすまし |
| 識別子 | T.Authsys_Bruteforce |
| 内容 | 本脅威は､特に工夫も無く何度も繰り返し検証行為を行うことによって、なりすましを試みる脅威とする。わずかな試行回数でたまたま認証精度との兼ね合いでなりすまされる脅威は含まず、あくまでも膨大に検証行為を試みる場合とする。 |

| | |
|---|---|
| 脅威 | 共連れによるなりすまし |
| 識別子 | T.Authsys_Piggyback |
| 内容 | 本脅威は正当な利用者が認証行為を行って、第三者を入室させるピギーバック攻撃によってなりすます脅威とする。正当な利用者が故意に行う場合と、攻撃者に脅迫されて行う場合がある。 |

| | |
|---|---|
| 脅威 | 代替手段を利用したなりすまし |
| 識別子 | T.Authsys_Fallback |
| 内容 | 本脅威は、攻撃者が意図的に本人拒否や入力未対応（ＦＴＡ）を引き起こして、弱い代替手段でなりすます脅威とする。通常、未対応者や本人拒否を高い確率で発生する利用者（Goat）に対して用意されていることが多い。 |

（c） ＩＴシステムに共通な脅威

| | |
|---|---|
| 脅威 | 管理者権限の不正獲得による管理者機能の不正実行 |
| 識別子 | T.ITsys_Usurp_Admin |

| | |
|---|---|
| 内容 | 本脅威は、管理者権限を持たない者が維持管理機能を実行可能になる脅威とする。維持管理機能を悪用することによって、様々な不正行為（閾値の改変、試行回数制限の解除など）が可能となり、他の脅威への対策が十分機能しなくなる。 |

| | |
|---|---|
| 脅威 | 不正行為や攻撃の不検出 |
| 識別子 | T.ITsys_Undetect |
| 内容 | 本脅威は、様々な攻撃や不正行為の痕跡が残らない脅威とする。痕跡が残らないことにより、攻撃を受けたことに気づかず的確な対応ができなかったり、維持管理機能の実行記録が無いことにより、設定ミスなのか攻撃を受けたのかの判別もつかなくなる。 |

| | |
|---|---|
| 脅威 | プログラムの改変による不正行為の実行 |
| 識別子 | T.ITsys_Modify_Program |
| 内容 | 本脅威は、システムの構成要素であるソフトウェアモジュールの改変・すり替えなどによって動作を狂わせ、なりすましを試みる脅威とする。例えば判定モジュールをすり替えて必ずＯＫを返すようにすれば誰でもなりすましが可能となる。 |

| | |
|---|---|
| 脅威 | 物理的な改変による不正行為の実行 |
| 識別子 | T.ITsys_Physical_Attack |
| 内容 | 本脅威は、物理的な構成要素を不正なものに取り替えたり、ケーブルを繋ぎ変えたりすることによって不正なデータを入力し、誤動作させることでなりすます脅威とする。 |

| | |
|---|---|
| 脅威 | 事故・故障による誤動作 |
| 識別子 | T.ITsys_Fault |
| 内容 | システムの構成要素となるＩＴ機器（ハードディスク装置やネットワーク装置など）が動作に支障をきたすような故障などの動作不良を起こすことによって、誤動作した結果なりすまされる脅威とする。 |

| | |
|---|---|
| 脅威 | コンピュータウィルスなどによる誤動作 |
| 識別子 | T.ITsys_Bad_ITenvironment |

| | |
|---|---|
| 内容 | システムの構成要素となるＯＳや装置などに関する構成要素単体の脆弱性を利用して誤動作を起こさせる脅威とする。 |

| | |
|---|---|
| 脅威 | 不必要な機能による脅威 |
| 識別子 | T.ITsys_Unnecessary_Function |
| 内容 | システムがパーソナルコンピュータなどの汎用機器で構成されている場合に、プログラミング環境などの不必要なソフトウェアやＵＳＢなどの機能拡張インタフェースを利用して、システムを誤動作させる脅威とする。 |

（3）　セキュリティ要件検討

1）　機能要件

本節では、前述の脅威に対しＩＴ機能で対応すべきセキュリティ要件の検討結果を記述する。要件の策定にあたっては、ＩＳＯ／ＩＥＣ １５４０８ Ｐａｒｔ２を参考にした。なお、番号付与方法に関しては５．１．６章における図 5-6 に従った。

（a）　識別・認証

a）　利用者認証

[FP 2.1.1.1]　管理者としての認証が成功するまでは管理機能は何も実行できないようにすること。【必須】

[FP 2.1.1.2]　管理者を認証する際には、複数の認証機構を使用すること。【オプション】

[FP 2.1.1.3]　生体認証システムの機能を停止させる際には再度認証を実施すること。【オプション】

b）　偽造されない認証

[FP 2.1.2.1]　偽造された人工指による認証行為を検出または防止できること。【オプション】

[FP 2.1.2.2]　センサ面に残留した指紋かどうかを検出できること。【オプション】

[FP 2.1.2.3]　偽造された認証トークンによる認証行為を検出または防止できること。【オプション】

ｃ） 利用者識別

[FP 2.1.3.1] 管理者としての識別が成功するまでは管理機能は何も実行できないようにすること。【必須】

ｄ） 認証失敗

[FP 2.1.4.1] 認証行為の失敗回数がある一定回数を超えた場合にはそれを検出し、また、管理者に対してその旨を通知すること。【必須】

[FP 2.1.4.2] 認証行為の失敗回数がある一定回数を超えた場合にはそれを検出し、それ以降一定期間の間は当該利用者の利用を停止すること。【オプション】

（ｂ） セキュリティ監査

ａ） セキュリティ監査データ生成

[FP 2.2.1.1] 以下の監査対象事象の監査記録を生成できること。【必須】

a) 監査機能の起動と終了

b)上記以外の個別に定義した監査対象事象

[FP 2.2.1.2] 各監査記録において少なくとも以下の情報を記録すること。【必須】

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報、事象の結果(成功または失敗)

b) その他の監査関連情報

[FP 2.2.1.3] 各監査対象事象を、その原因となった利用者の識別情報に関連付けること。【必須】

ｂ） セキュリティ監査事象格納

[FP 2.2.2.1] 監査証跡が事前に定義された限界を超えた場合、管理者に対して警告を発すること。【オプション】

[FP 2.2.2.2] 監査証跡が意図せず消失しないように記録媒体の二重化によって防止すること。【オプション】

[FP 2.2.2.3] 監査証跡が意図せず消失しないように格納媒体を Read Only にすること。【オプション】

（ｃ） データ保護

ａ） 完全性転送保護

[FP 2.3.1.1] 認証トークンに格納された指紋テンプレートの転送において、改変、消去、挿入、リプレイが生じたかどうかを検出できること。【必須】

ｂ） 機密保護

[FP 2.3.2.1] 指紋情報等の重要なデータが別々のパーツ間で送られる場合、データを暴露から保護できること。【オプション】

ｃ） データ認証

[FP 2.3.3.1] 指紋テンプレートの内容の真正性を検証できること。【必須】

[FP 2.3.3.2] 認証トークンの真正性を検証できること。【オプション】

（ｄ） セキュリティ管理

ａ） セキュリティ属性の管理

[FP 2.4.1.1] 各種設定値は正常な値だけが値として設定されること。【オプション】

[FP 2.4.1.2] 各種設定値を変更する機能を運用開始以降は誰も使用できないようにすること。【オプション】

ｂ） 管理機能の特定

[FP 2.4.2.1] 設定内容変更時の確認プロンプト表示を行うこと。【必須】

[FP 2.4.2.2] 生体認証システムの機能を停止させる場合に、運用管理者に通知をすること。【オプション】

（ｅ） タイムスタンプ

[FP 2.5.1.1] 時刻サーバへ問い合わせて、時刻情報を補正できること。【オプション】

[FP 2.5.1.2] 高精度時計を内蔵し、正確な時刻情報を利用すること。【オプション】

２）　運用要件

本節では、前述の脅威に対し人による運用で対応すべきセキュリティ要件の検討結果を記述する。要件の策定にあたっては、ＩＳＯ／ＩＥＣ １７７９９：２０００を参考にしたが、生体認証に特化したものなどについては新たに作成した。なお、番号付与方法に関しては、５．１．５章における図 5-3 に従った。

（ａ）　物理的および環境的セキュリティ

ａ）　セキュリティが保たれた領域

業務施設および業務情報に対する認可されていないアクセス、損傷および妨害を防止するために、セキュリティ境界を明確にし、識別されたリスクに対応した保護対策を施すことが望ましい。

[OP 3.1.1.1]　資産を含む領域を保護するために、幾つかのセキュリティ境界を利用すること。【必須】

[OP 3.1.1.2]　認可された者だけにアクセスを許すことを確実にするために、適切な生体認証技術を用いた入退管理策によってセキュリティの保たれた領域を保護すること。【必須】

[OP 3.1.1.3]　セキュリティが保たれた領域の選択および設計においては、火災、洪水、爆発、騒擾、その他の自然または人為的災害による損害の可能性を考慮すること。【オプション】

[OP 3.1.1.4]　セキュリティが保たれた領域のセキュリティを強化するために、その領域での作業のための管理策および指針を追加すること。【必須】

ｂ）　装置のセキュリティ

資産の損失、損傷または劣化、および業務活動に対する妨害を防止するために、装置は、セキュリティに対する脅威および環境上の危険から物理的に保護されることが望ましい。

[OP 3.1.2.1]　指紋認証装置は、環境上の脅威および危険からのリスク並びに認可されていないアクセスの可能性を軽減するように設置または保護すること。【必須】

[OP 3.1.2.2]　指紋認証装置は、停電、その他の電源異常から保護すること。【オプション】

[OP 3.1.2.3] データ伝送または情報サービスに使用する電源ケーブルおよび通信ケーブルの配線は、傍受または損傷から保護すること。【オプション】

[OP 3.1.2.4] 指紋認証装置についての継続的な可用性および完全性の維持を確実とするために、装置の保守を正しく実施すること。【オプション】

[OP 3.1.2.5] 取扱いに慎重を要する情報を保持する記憶装置の処分は、物理的に破壊するかまたは、確実に上書きすること。【必須】

（b） アクセス制御

a） アクセス制御に関する業務上の要求事項

情報へのアクセスおよび業務手続きは、業務およびセキュリティの要求事項に基づいて管理する必要があり、この場合、情報を伝える範囲およびアクセスの認可に対する個別方針を定義することが望ましい。

[OP 3.2.1.1] アクセス制御についての業務上の要求事項を定義し、文書化すること。【必須】

[OP 3.2.1.2] 全ての職員（一般職員、特定職員、管理者）は、その活動が誰の責任によるものかを後で追跡できるように、各個人の利用ごとに一意な識別子（職員 ID）を保有すること。【必須】

[OP 3.2.1.3] 脅迫の標的となり得る職員のために、脅迫に対する警報（duress alarm）を備えることを考慮すること。【オプション】

b） システムアクセスおよびシステム使用状況の監視

許可されていない活動を検出するために、アクセス制御方針からのずれを検出し、セキュリティ事件・事故の場合に証拠となるようにするとともに、監視可能な事象を記録するために、システムを監視することが望ましい。

[OP 3.2.2.1] 例外事項、その他のセキュリティに関連した事象を記録した監査記録を作成して、将来の調査およびアクセス制御の監視を補うために、合意された期間保存すること。【必須】

[OP 3.2.2.2] 生体認証システムの使用状況を監視する手順を確立すること。【必須】

[OP 3.2.2.3] 監視の結果は、定期的に見直すこと。【オプション】

[OP 3.2.2.4]　システムが直面する脅威とそれらの起こり方を理解するために、記録を検証すること。【オプション】

[OP 3.2.2.5]　コンピュータの時計は正しく設定すること。【必須】

[OP 3.2.2.6]　コンピュータの時計は定期的に確認すること。【必須】

（ｃ）　生体認証システムの開発及び保守

ａ）　暗号による管理策

リスクがあると考えられる情報の機密性、真正性または完全性を保護するために、暗号技術を用いた管理策を利用することが望ましい。

[OP 3.3.1.1]　組織の情報を保護するための暗号による管理策の使用について、個別方針を定めること。【必須】

ｂ）　システムファイルのセキュリティ

生体認証をセキュリティが保たれた方法で実施されることを確実にするために、システムファイルの実行を管理することが望ましい。

[OP 3.3.2.1]　生体認証システムでのソフトウェアの実行を管理すること。【オプション】

[OP 3.3.2.2]　試験データを保護し、管理すること。【オプション】

（ｄ）　利用環境のセキュリティ

特定職員の指紋データを採取する場合に、その採取環境はアカウント登録時に採取した環境と同一にすることが望ましい。また、採取時には、採取対象となるモダリティの特徴を変形または隠すような行動、服装、その他要因を制御することが望ましい。さらに指紋データを採取するセンサの時間経過による劣化にも随時対処することが望ましい。

ａ）　指紋データ採取環境の管理

[OP 3.4.1.1]　指紋データの採取環境は、生体認証システム基本方針で定められたとおりに、適切に文書化すること。【必須】

[OP 3.4.1.2]　指紋データの採取環境は、利用する製品に応じて適切に設定される

こと。【必須】

[OP 3.4.1.3] 指紋データの採取環境は、常に一定の状態を保つこと。【必須】

ｂ） 利用者環境の管理

[OP 3.4.2.1] 生体認証システム利用時の行動に関する指針を文書化すること。【必須】

[OP 3.4.2.2] 特定職員に、生体特徴の変形を促すような行動、およびその他影響があるであろう要因を防ぐよう適切に教育し、並びに定期的に更新教育を行うこと。【必須】

[OP 3.4.2.3] 生体認証システムの利用時の行動を定期的に監視すること。【必須】

ｃ） 生体センサの管理

[OP 3.4.3.1] 指紋データを採取するためのセンサは、継続的な可用性および完全性の維持を確実とするために、常に一定の環境となるように保守を行うこと。【必須】

[OP 3.4.3.2] 指紋センサは、電源異常から保護すること。【必須】

[OP 3.4.3.3] データ伝送に使用する通信ケーブルの配線は、傍受または損傷から保護すること。【必須】

（ｅ） 共連れの禁止

特定職員の本人確認が終了し、守るべき資産が納められている領域への物理的なゲートが開いた場合に、アクセスの認められていない人物が、共に侵入しようとすることは禁止するべきである。

ａ） 利用環境の管理

[OP 3.5.1.1] 生体認証システムによって、資産が納められた領域に入退できると認められる特定職員は、一度の認証時に一人だけとすること。【必須】

ｂ） 職員の訓練

[OP 3.5.2.1] 共連れによるセキュリティ上のリスクに関して、特定職員に認知させるための手順を導入すること。【必須】

[OP 3.5.2.2] 共連れを行った場合の、正式な懲戒手続きを備えること。【必須】

（ｆ）　代替手段

特定職員が認証トークンの不携帯または利用するモダリティの怪我、喪失、その他要因により生体認証システムを利用できない場合、業務上の必要性により、代替手段を提供しなければならない。また、そもそも組織の決定したモダリティを持ち合わせていない特定職員を資産にアクセスさせる必要がある場合、生体認証システム以外の代替手段による本人認証が必要になる。

ａ）　認証トークン不携帯時の代替手段

[OP 3.6.1.1]　資産の納められている領域にアクセスすることが認められた特定職員が認証トークンを忘れた場合の代替手段に関する要求事項を定義し、文書化すること。【必須】

[OP 3.6.1.2]　代替手段を利用した特定職員を管理すること。【オプション】

[OP 3.6.1.3]　認証トークンを携帯しなかった特定職員に対する、正式な懲戒手続きを備えていること。【オプション】

ｂ）　モダリティ損傷時の代替手段

[OP 3.6.2.1]　モダリティが怪我、喪失、その他要因によって利用できない場合の代替手段に関する要求事項を定義し、文書化すること。【必須】

[OP 3.6.2.2]　代替手段を利用した特定職員を管理すること。【オプション】

ｃ）　未対応者への代替手段

[OP 3.6.3.1]　未対応者に対する代替手段に関する要求事項を定義すること。【必須】

ｄ）　代替手段の見直し

[OP 3.6.4.1]　代替手段は、定められた見直し手続きに従って、維持および見直しが行われること。【必須】

（ｇ）　認証トークンの盗難・紛失

特定職員が認証トークンを盗難された場合、または紛失した場合に、その職員に係わるアクセス権限の変更、および当該認証トークンの利用停止を行うことが望ましい。

ａ）　認証トークン盗難・紛失時の管理策

[OP 3.7.1.1] 認証トークンの盗難･紛失時の要求事項を定義し、文書化すること。【必須】

[OP 3.7.1.2] 認証トークンの盗難・紛失は、適切な連絡経路を通して、できるだけ速やかに報告すること。【必須】

[OP 3.7.1.3] 認証トークンを盗難・紛失した特定職員のアクセス権限は一定期間剥奪すること。【必須】

[OP 3.7.1.4] 認証トークンの盗難、紛失後の代替手段に関する要求事項を定義し、文書化すること。【必須】

[OP 3.7.1.5] 認証トークンを紛失した特定職員に対する、正式な懲戒手続きを備えていること。【必須】

（ｈ） 生体認証技術に特有のセキュリティ

ａ） 類似性

生体認証には、例えば双子の顔のように、類似した生体情報を持つ他の利用者が存在する可能性があるため、この生体情報の類似性に関する管理策を設定することが望ましい。

[OP 3.8.1.1] 類似性に関する生体認証システムへの要求事項を定義し、文書化すること。【必須】

ｂ） 特異性

生体認証では、Ｗｏｌｆ（なりすましやすい生体情報を持つ人物)、Ｌａｍｂ（なりすまされやすい生体情報を持つ人物)、Ｇｏａｔ（極端に誤拒否が大きい生体情報を持つ人物）などにより、高確率で誤拒否や誤受入が発生する可能性があるため、この特異性に関する管理策を設定することが望ましい。

[OP 3.8.2.1] 特異性に関する生体認証システムへの要求事項を定義し、文書化すること。【必須】

ｃ） 習熟

特定職員が生体認証装置の使用方法を習熟していない場合、生体情報の採取失敗による誤拒否が発生してしまう可能性があるため、この習熟に関する管理策を設定することが望ましい。

[OP 3.8.3.1]　習熟に関する生体認証システムへの要求事項を定義し、文書化すること。【必須】

## ５．２　国際規格素案の策定と業界内の意見集約・合意形成

昨年度及び今年度の検討成果を国際標準へ反映する為に、ＩＳＯ／ＩＥＣ　ＪＴＣ１　ＳＣ３７WG４に対し、セキュリティプロファイルのコンセプトやその概要を提案した。また同WGのプロジェクトである２４７１３－２（空港従業員の物理アクセスコントロールの為のバイオメトリクスプロファイル）にセキュリティプロファイルを寄稿し、２４７１３－２への仕様反映方法を提案した。

本セキュリティプロファイルの提案先としては、関連のあるＳＣとして、ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ１７（ＩＤカード)、ＳＣ２７（セキュリティ)、ＳＣ３７（バイオメトリクス）と３つの候補があったが、以下の理由によりＳＣ３７が最適と判断した。

- セキュリティプロファイルは可搬型メディア一般を対象としておりＩＣカードに特化していないことから、ＳＣ１７は適さないと思われる点
- セキュリティプロファイルはセキュリティ評価の一般的な方法論を定義するものではなく、バイオメトリクスを使用するアプリケーションのセキュリティ要件であることから、ＳＣ２７は適さないと思われる点
- セキュリティプロファイルの関わるセキュリティ仕様は、バイオメトリクスを使用するアプリケーションに依存し、キーとなるポイントがバイオメトリクス（ＳＣ３７）に集約される点

また、ＳＣ３７の提案先WGとしては、アプリケーションのプロファイルに関しての検討の場であるＳＣ３７WG４が適当であると判断した。

### ５．２．１　ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ３７ WG４における標準化動向

セキュリティプロファイルの提案先であるＳＣ３７WG４では、開発中の標準はただ一つであり、プロジェクト番号は２４７１３となっている。タイトルは「Biometric Profiles for Interoperability and Data Interchange」であり、他のWGにおいて策定された仕様を組み合わせて、具体的アプリケーションにおける要件を定義することで、アプリケーションレベルにおける相互運用性を確保するための規格である。

２４７１３は基本的な定義の部分と、各種アプリケーションに特化した部分とでパートを分ける方式を採っており、パート１が共通アーキテクチャ、パート２以降は具体的アプリケーション毎に作成されている。パート２は空港従業員の物理アクセスコントロールが対象であり、パート３は船員の身分証明書を用いた船員認証が対象となっている。以降それぞれの現在の動向を簡単に説明する。

（1）　２４７１３－１（Biometric System Reference Architecture）

２４７１３－１では、２４７１３シリーズにおける共通アーキテクチャを定義しており、主にバイオメトリクス認証における生体情報取得（キャプチャ）、特徴抽出、照合、判定などの処理フローとシステムにおける概念上の実装方法を規定している。２００５年6月の南アフリカ会議にてＦＣＤに昇格、２００６年1月の京都会議では、主にWG１における用語定義との調和等を課題として、ＦＣＤに残留、以降現時点に至っている。

（2）　２４７１３－２（Physical Access Control for Employees at Airports）

２４７１３－２では、２４７１３－１で定義する共通アーキテクチャを基本として、空港施設に従事する職員に対し、バイオメトリクス認証を用いた物理アクセスコントロール（例えば、ゲート制御システムなど）におけるプロファイルを規定している。セキュリティプロファイルの前提とするアプリケーションと近いシステムモデルであり、本セキュリティプロファイルの寄稿先として、このプロジェクトを選択した。２００５年１１月のパリ会議以降、ＣＤに残留、現時点に至っている。

（3）　２４７１３－３（Biometric Profile for Seafarers）

２４７１３－３では、２４７１３－１の共通アーキテクチャと２４７１３－２のプロファイルを基本として、ＩＬＯの定める船員の身分証を用いたバイオメトリクス認証のプロファイルを規定している。２４７１３－３はＩＬＯの定める船員の身分証に関する改正国際条約第１８５号の技術仕様であるＳＩＤ－０００２の国際標準化を目的に、ＩＬＯより正式にプロファイル作成を依頼されて発足した。２００５年１１月のパリ会議以降、WDから発展せず、現在に至っている。

５．２．２　　活動詳細

昨年度及び今年度の成果の国際標準提案に至っては、下記の活動を通じて国内関係者及びＩＳＯ／ＩＥＣ　ＪＴＣ１　ＳＣ３７国内委員会の承認を得た。

**表 5-5 標準化活動一覧**

| 会議名 | 日程 | 内容 |
|---|---|---|
| SC37WG4 国内小委員会 | 2005 年 5 月 13 日 | 南ア会議における日本からの寄稿内容の審議 |
| SC37 国内専門委員会 | 2005 年 5 月 24 日 | 南ア会議において日本から寄稿することに関する審議 |
| SC37 国際会議（南ア） | 2005 年 6 月 28 日 | セキュリティプロファイルの内容紹介と必要性の合意形成 |
| SC37WG4 国内小委員会 | 2005 年 10 月 31 日 | 京都会議における日本からの寄稿内容の審議 |
| SC37 国内専門委員会 | 2005 年 11 月 10 日 | 京都会議において日本から寄稿することに関する審議 |
| SC37 国際会議（京都） | 2006 年 1 月 9 日 | 24713-2 へのセキュリティプロファイルの具体的適用方法の提案 |

上記において、特に国際への提案活動として、以下を報告する。

（1）　ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ３７ 国際会議（南アフリカ共和国）

ＳＣ３７WG４のWG会議にて、セキュリティプロファイルの国際標準提案にあたり、そのコンセプトと概要を中心にプレゼンテーションを実施した。提案にあたっては、プレゼンテーション資料を事前に送付（Ｎ１１６５）し、国際主査とプレゼンテーションの為の時間を用意してもらうよう調整を図り、ＷＧ４会議のアジェンダ（Ｎ１１３８）の１３項 Other Business のセッションにて発表を行なった。発表では、セキュリティプロファイルのスコープと国際標準における新規性、またＳＣ３７WG４における検討の妥当性を説明し、また２４７１３－２における適合性をアピールした。会議では、特にイギリスよりその必要性に同意するコメントがあった他、国際主査より京都会議にて完成版の寄稿を期待する等のコメントが得られ、セキュリティプロファイルの必要性の合意形成を行った。

（2）　ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ３７ 国際会議（京都）

前回の提案結果を受け、ＳＣ３７WG４の京都会議において、セキュリティプロファイルの完成版の寄稿と、２４７１３－２への具体的反映方法を提案した。京都会議

では、WG会議のアジェンダ（Ｎ１４２７）における２４７１３－２の議論のメインパートとして、６．１項「日本の寄書に対する取り扱い」が挙げられ、日本の寄書に対する議論の時間が割り当てられた。

日本は南アフリカ会議にて紹介したセキュリティプロファイルのコンセプトを再度説明し、既存の標準規格との関連や２４７１３－２の対象とする従業員のプロファイルに対しそのセキュリティ仕様としてどのような考えで策定し、どのような内容を仕様化したのか、これをどのように２４７１３－２に反映していくのか等１０分程度のプレゼンテーションを行なった。特に２４７１３－２への反映方法としては、日本から下記の２通りの反映方法を提案した。

- ケースＡ：ＣＤ本文にセキュリティ要件の節を起し、セキュリティプロファイルのサマリを提示、セキュリティプロファイルの本文を Normative Annex とする案
- ケースＢ：「２４７１３－３のラポータグループのプロファイル開発の進め方」（Ｎ１１２１）におけるプロファイルの項目のうち、セキュリティに関連する部分についてセキュリティプロファイルから抽出、セキュリティプロファイルの本文を Informative Annex とする案

これに対して、イギリス／南アフリカ／ドイツ／アメリカ／フランスから意見が出た。イギリス、南アフリカからは好意的な意見が出たが、特に南アフリカからは２４７１３の新規パートとしたらどうか、等の意見も出て国際主査も前回ＮＰが成立しなかった２４７１３－４として検討しても良いのではないかとの発言もあった。一方、フランスからは内容的には合意できるもののＳＣ３７およびWG４のスコープ外であると発言した。ドイツからは２４７１３－２以外のパート、具体的には２４７１３－３に対してはどのように反映していくのかという問いかけについて、パート３のエディタは「必ずしも必要でないが、２４７１３－３に対してはケースＢのような寄稿を歓迎する」と発言、セキュリティ仕様はシステムに依存するため、パート毎に考えていくべきという結論になった。また２４７１３－２のエディタはイギリス／シンガポールの Annex 追加の作業もあり、日本の提案によって更に Annex が増える点に対しては否定的であり、ケースＡにおける Annex の Editing は誰がメンテナンスをするのか、また Annex に添付するセキュリティプロファイルの量も４７頁もありこれは Annex としては不適切である等と難色を示していた。これに対して、日本は日本担当分のメンテナンスは日本が対応する、分量としては Annex にふさわしくなるよう適宜修正するなど回答した。

以上の議論を経て、日本の寄書の扱いは、２４７１３－２のＣＤ再投票に対し２４

７１３－２への反映方法を加味したコメントとして再度寄稿することとなった。上記に示す通り、２４７１３－２のエディタを除き、寄書の内容には参加国すべてが好意的であり、２４７１３－２のＣＤ投票結果に対する議論が行なわれる次回ロンドン会議にて更なるレビューを受ける予定である。

### ５．２．３　　活動まとめ

今年度は５．１章にて詳述したセキュリティプロファイルを国際標準として提案、日本におけるバイオメトリクス分野でのセキュリティ検討に関するプレゼンスを向上させることができた。国際提案にあたっては２回のＳＣ３７国際会議を通して、セキュリティプロファイルの必要性・有用性が認知されることができたと共に、現在開発中の２４７１３－２に対する要件の反映方法について国際会議に先立って具体案を検討し提案することで、その仕様反映方法、内容共に多くの国の賛同を得ることが出来た。

今後は２４７１３－２に対する適応性を向上させ、次回国際会議に向けた寄稿提出を目指し、更なる検討を進めていく予定である。

## ５．３　　調査研究結果まとめ

５．１章および５．２章において今年度の活動を報告したが、最後に、平成１６年度から２ヵ年にわたって実施してきた本調査研究の結果と課題についてまとめる。

### ５．３．１　　調査研究計画の達成度合い

本調査研究では、当初以下に挙げる検討を通して可搬型メディアとバイオメトリクスを組み合わせた本人認証システムにおけるセキュリティ要件を定義することが目的であり、更には、その成果物を用いて国際標準化において日本から貢献することを目指していた。

１）　ＩＣカードとバイオメトリクスの組み合わせによる本人認証システムのモデルの整理
２）　１）のセキュリティ分析とセキュリティ要求仕様（ＰＰ）の検討
３）　２）で策定したＰＰを元とするセキュリティ機能と運用仕様（セキュリティプロファイル）の策定

４）　3）に対するフィージビリティスタディの実施とプロファイルの検証

平成１６年度においては、上記１）～２）を通して現状の技術・製品・標準に関する調査を行い、２）～３）において職員認証業務における検討項目の明確化および検討スキームの確立を行った。ただし、２）と３）の検討途中において、利用シーンを本人確認時とアカウント登録時に分離して検討するという方針へ変更し、まずは本人確認時をターゲットとしたセキュリティ脅威の抽出までにとどまり、具体的なセキュリティ対策の検討までは着手できなかった（一部運用要件は除く）。また、４）のフィージビリティスタディの適用先については残念ながら適当な案件が見つからず、１６年度は実施することはできなかった。

平成１７年度においては、２）と３）の検討を継続し、本人確認時のセキュリティ要件をまとめることができ、また、本人確認時だけでなくアカウント登録時におけるセキュリティ検討も実施し、当初の予定通り２）および３）を完遂し、機能要件と運用要件を併せたセキュリティプロファイルを完成させることができた。また、４）に関しては１７年度も案件が見つからず実施することができなかったが、実フィールドでの評価の代わりに、国際標準化活動を通して国内だけでなく海外の有識者からのレビューを受けることができたことにより、完成度を高めるという意味では十分な活動ができたと考える。

５．３．２　　調査研究を通して得られた知見

本調査研究を進めていく上でいくつかの重要な知見を得られたが、それらは以下の２点である。

- ＩＳＯ／ＩＥＣ １５４０８とＩＳＯ／ＩＥＣ １７７９９の組み合わせ手法
- セキュリティ検討における認証精度の考え方

以下にそれぞれについて得られた知見の詳細を記述する。

（1）　　ＩＳＯ／ＩＥＣ １５４０８とＩＳＯ／ＩＥＣ １７７９９の組み合わせ手法

本調査研究では、本人認証システムのＩＴセキュリティ機能とセキュリティ運用を検討し、要件としてまとめることが目的であったが、それぞれに特化した検討手法や雛形となる用件のリストなどが標準化されており、それらを用いて検討することが必要不可欠であると考えた。即ち、ＩＴセキュリティ機能要件の検討において

は、ＣＣ（Common Criteria）をベースにＩＳＯ化されたＩＳＯ／ＩＥＣ １５４０８を用い、セキュリティ運用の検討においてはＢＳ（British Standard）７７９９がベースとなったＩＳＯ／ＩＥＣ １７７９９を用いる方法である。しかし、本来は別々で検討することを念頭に規格化されたものであるため、それぞれを組み合わせる際に工夫が必要となった。

組み合わせ手法としてまず思いつく方法としては、ＩＳＯ／ＩＥＣ １５４０８に基づいた検討を行い、脅威分析を通して対策すべきと判断した脅威に対する要件を定義する際に、「ＩＴ機能要件」に関してはＩＳＯ／ＩＥＣ １５４０８のパート２を用い、「非ＩＴ機能要件」に関してはＩＳＯ／ＩＥＣ １７７９９を用いる方法がある。こうすることで、ＩＳＯ／ＩＥＣ １５４０８単独で検討した際には通常あまり具体的に定義することがない「非ＩＴ機能要件」についても詳細な定義が可能となり、単独の場合よりも完成度の高いものが作成可能となる。

しかし、ＩＳＯ／ＩＥＣ １５４０８に基づいた検討においては、想定される運用環境などを「前提条件」として定義した上で脅威分析・対策検討を行い、ＩＴ機能では対策できない（しない）脅威に対して「非ＩＴ機能要件」を定義していく方法を採るが、「前提条件」の設定如何によっては非ＩＴ機能要件がほとんど必要なくなり、運用による対策はあまり必要ないというように見えてしまう場合がある。だが実際に運用要件を検討する際には、非ＩＴ機能要件として定義された部分だけでなく、前提条件として「すでに実現されていると仮定した運用」を実現するような運用方法（運用要件）というのも重要な検討対象となる。

そこで、本調査研究においては、ＩＳＯ／ＩＥＣ １５４０８に基づいた検討方法をメインとしつつも、脅威分析・対策検討の結果として定義した「非ＩＴ機能要件」だけでなく、「前提条件」を満たすための運用もＩＳＯ／ＩＥＣ １７７９９を用いて要件定義することにより、より完成度が高くなるよう工夫した。その結果、運用要件の網羅性が向上するだけでなく、ＩＴ機能要件を検討する際の前提条件がより具体的になることで、脅威分析の精度も向上させることができた。また、ＩＴ機能と運用を同時に検討する際の有効な手法であることが本検討を通して確認することができたので、可搬型メディアとバイオメトリクスの組み合わせだけでなく、一般的なセキュリティ検討の際にも広く活用ができる手法であることがわかった。

（２）　セキュリティ検討における認証精度の考え方

バイオメトリクス認証システムを設計する際にＩＳＯ／ＩＥＣ １５４０８を適用する場合、他の一般的なＩＴシステムと同様にセキュリティを確保する範囲を明

確に定め、その範囲内で想定される脅威や守るべき資産を定義していくことになる。

その際、バイオメトリクス認証特有の考慮すべき点として、バイオメトリクス認証が１００％の認証精度ではないというが挙げられる。バイオメトリクス認証はパスワード認証などの方式と違いＦＡＲやＦＲＲといった認証精度に起因して一定確率で誤認識が発生するため、いくら完璧なセキュリティを確保していても一定確率で他人によるなりすましの脅威が発生してしまう。だが、この特性は他の認証方式と比べてセキュリティ強度が低いとは一概には言えない（例えば４桁の数字によるパスワード認証では理論上１／１００００の一定確率でなりすますことが可能である）。

バイオメトリクス認証におけるＦＡＲと、パスワード認証におけるなりすまし成功率は、それぞれパーセンテージで表すことができるが、例えパーセンテージが同じであっても、それぞれの方式のセキュリティ強度は同じとはいえない。なぜなら、パスワードであれば任意に好きな数字や文字を入力することができるが、バイオメトリクス認証においては、システムへ入力可能な生体特徴の数が制限されてしまうので（例：指紋であれば攻撃者一人あたりの指は最大１０本となる）、なりすまし成功率がパーセンテージでは同じであったとしても、バイオメトリクス認証の方がセキュリティ強度が高いと考えられる。このようなバイオメトリクス認証の精度とセキュリティ強度の関係については、現在研究段階であり、明確な定義はされていないので、適用する業務によって個別の判断をしているのが現状である。

また、セキュリティ対策は、脅威を１００％排除することが必ずしも良策とは言えず、コスト対効果を勘案し必要十分なセキュリティを確保することが重要であるので、業務で求められるセキュリティがどの程度のなりすまし成功率であれば許容できるかということに帰着する。

以上のことから、ＩＳＯ／ＩＥＣ １５４０８に基づいてセキュリティ設計・評価を行う際には、認証精度に起因する脅威は対象外とし、その他の脅威への対策に注力すべきであり、ＦＡＲ／ＦＲＲといった認証精度やＷｏｌｆやＧｏａｔといったアルゴリズムの特性に関しては無理に評価対象とはせず、ＩＳＯ／ＩＥＣ １５４０８の評価とは別途実施する手法が現実的ではないかと考える（これは暗号製品における暗号アルゴリズム評価と類似しており、ＩＳＯ／ＩＥＣ １５４０８では暗号アルゴリズム評価は対象外としている）。

以上のことをまとめると、本調査研究の範疇を超えているが、バイオメトリクス認証システムにおけるセキュリティを検討する上では以下のような課題が残っており、今後更なる研究が必要であることがわかった。

【課題】 セキュリティ強度とＦＡＲの対応が不明であるため、システム設計の際にどの程度のＦＡＲとなることを目指せばよいか判断が難しい。

この課題を解決するにはいくつかのハードルがあり、一つは生体認証製品によってＦＡＲの算出方法がまちまちであるということがある。だがこれに関しては、現在ＩＳＯ／ＩＥＣ ＪＴＣ１ ＳＣ３７ ＷＧ５での活動（１９７９５関連の取り組み）で統一されつつあるので、今後解消するものと考える。二つ目は、セキュリティ強度の分析手法が現段階では確立されていないというものである。これは生体認証方式によってＦＡＲの値の判断は異なることと、精度に起因する脆弱性の存在も考慮する必要があり、基準認証事業の１テーマである「バイオメトリクスセキュリティ評価基準の開発」の研究成果やＩＳＯ／ＩＥＣ １９０９２などの国際標準、Biometrics Evaluation Methodology といった各種関連成果物を組み合わせて解決していく必要があるが、今後学会等においても認証アルゴリズムのセキュリティ強度に関する研究発表などに期待したい。

### ５．３．３　　今後の課題

今後は標準化活動に関して次回ロンドン会議に向けて以下の追加検討を実施していく必要があり、平成１８年度以降も継続して活動を展開していく予定である。

- ２４７１３－２に対する親和性を向上
- 規格上の齟齬がないか等のチェック
- 国際標準になった場合の準拠度合いの評価方法の検討

５．４　　付録

５．４．１　ＩＳＯ／ＩＥＣ　ＳＣ３７への寄書（Security Profile 英語版）

# Security Profile

# for Token and Biometrics Based

# Staff Identity Verification Systems

November, 2005
Japan National Body

## 1. Introduction

Recent years has seen growth in demand to perform personal identity verification using token devices[1] that carry biometric information, for the purpose of enforcing stringent control over the access of staff to important facilities. In order to use biometric authentication to reinforce security, security requirements pertaining to the entire biometric authentication system need to be examined. However, current studies are mostly focused on individual systems, and the architecture and basis of security lacks integrity. Furthermore, while security systems require studies not only of their function but also of their operation, studies of security functions are centered on the main subject of biometric authentication, which is, how to ensure authentication capability (authentication precision, throughput etc.). And with studies of operations themselves being very scarce, systematic discussion of the security of a system as whole is rare.

On the other hand, while it would be best to use methods such as ISO/IEC 15408 or BS 7799 to investigate the security of a system as a whole, these standards are still not widely adopted by system architects, and it would require tremendous effort to analyze each system individually from scratch.

Hence, this "Security Profile" has been developed as security requirements that combine functional requirements and operational requirements for an entire system for the following two purposes:

- Analyze and organize using standard methods such as ISO/IEC 15408 and BS 7799 to ensure coverage of security requirements of the entire system;
- Through the use of this Security Profile, enable architects of individual systems who lack detail knowledge of the various standardized methods, to achieve the same effect as systems designed by expert architects.

## 2. Scope

The major threats that biometric authentication systems should consider include "impersonation", "personal information leakage", and "system halt". Thus, while security requirements of all these threats need to be examined, the largest threat to

[1] IC chips, 2D barcodes, magnetic stripes, etc.

personal authentication for the purpose of enforcing stringent control over access of staff to important facilities is "impersonation", which means serious damage would be caused by impersonation of an authentic staff. Therefore, the discussion of this Security Profile focuses on prevention of "impersonation".

However, for authentication accuracy which is closely related to "impersonation", the products used are different among systems, and issues may be resolved through product selection. Thus, measures pertaining to vulnerabilities other than authentication accuracy are discussed in this Security Profile.

## 3. Approaches

Generally, in order to discuss security requirements (functional requirements, operational requirements), one way would be to use ISO/IEC 15408 which is the global standard for reviewing functional requirements of an IT system, and BS 7799 which is the de-facto standard for considering operation management methods of information security. While there are various ways to combine the methods of ISO/IEC 15408 and BS 7799, this Security Profile has based its discussion on ISO/IEC 15408 while using parts of BS 7799 part 1 (ISO/IEC 17799) when detailing the operational requirements. Specifically, the following procedure was used for analyzing.

(1) Threats analysis

Defined the target business outline, assets to protect, system configuration, relevant players, and peripheral environment as much as possible, and analyzed potential threats.

(2) Study of functional requirements

Examined countermeasures towards threats that have been found through the analysis, and detailed the countermeasures by applying the functional requirements from part 2 of ISO/IEC 15408.

(3) Study of operational requirements

Performed in parallel with the review of functional requirements, and discussed operational countermeasures towards threats that cannot be prevented with functional requirements. Countermeasures were detailed by applying management measures from ISO/IEC 17799. Along with the countermeasures

towards threats, requirements of the peripheral environment which is the basis for the threats analysis was also detailed by applying management measures from ISO/IEC 17799.

After studying using the above procedures, the functional and operational requirements were combined to produce the security requirements to prevent "impersonation".

# 4. The Target System

## 4.1. Business Overview

This Security Profile assumes "all tasks that require strict personal identity verification of the staff" as its target, and addresses authentication tasks towards staff and employees who have limited access to backbone infrastructures, sensitive information and classified facilities that may suffer significant damage by terrorist activities.

Furthermore, the assumed environment is a gate facility with several dozen gates where access to areas that contain protected assets is physically controlled by performing staff identity verification. Airport staff, airline crew, and staff of atomic power plants are examples of staff of the assumed environment.

For the purpose of authentication of staff and employees, this Security Profile assumes performing fingerprint authentication with fingerprint data stored on token devices. Furthermore, related tasks would include "personal identity verification tasks" which is required to perform the primary task of entry/exit management, and "account registration tasks" which is performed as a preparation task.

### 4.1.1. Account Registration

Three account registration tasks are assumed. The three are new registration, re-issuing, and updating biometric templates. However, the workflow of these tasks all follow the procedure outlined in Fig. 4.1.

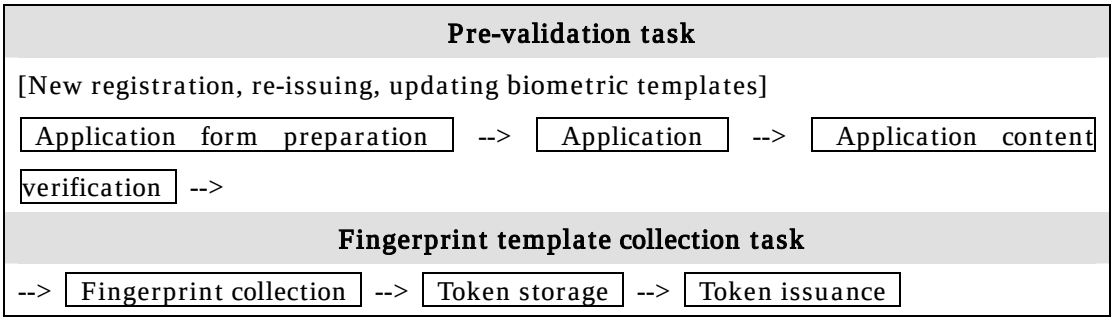


Fig. 4.1: Task Workflow

The account registration workflow shall be divided into two parts depending on whether biometric authentication specific actions are required. The part that does not require biometric specific actions shall be called "pre-validation task", and the part beginning from fingerprint collection which require biometric specific actions shall be called "fingerprint template collection task". Furthermore, the following are descriptions of each workflow.

[Application form preparation]

Create required documents for each new registration, re-issuing, and biometric template updates, and prepare personal identity documents if necessary.

[Application]

Apply by submitting the application form, identification documents, authentication token, etc. at the application desk.

[Application content verification]

The personnel at the application desk performs verification of application content, personal identification, authentication token, etc. However, 1 to N collation verification through biometric authentication technology is not assumed.

[Fingerprint collection]

Collect fingerprints from applicants that have passed application content verification, and create biometric templates.

[Token storage]

Store generates biometric templates to the token devices. In addition to the templates, other data required by the business shall also be stored to complete the authentication token. (Other processes such as printing onto the surface of the token shall also be performed if necessary.)

[Token issuance]

Hand over the created authentication token to the applicant. This Security Profile assumes issuing tokens on the spot, and does not consider handing over tokens at a later date. Thus, no personal identity verification will be performed when handing over the token.

#### 4.1.2. Personal Identity Verification

No task workflow is specified for personal identity verification, and authentication shall be performed by staff using fingerprint authentication devices that are installed at gate facilities established in the physical facility. The physical environment and roles of staff are described later in this document.

### 4.2. System Overview

#### 4.2.1. Basic Definition

Since this Profile assumes facilities with several dozen gates, the personal identity verification part shall be set up at each gate, and authentication servers connected through an external network is not assumed.

The biometric template shall be stored in a token device, and verification shall be performed by calculating a collation score. The collation score shall be calculated by comparing externally from the token device, the fingerprint data for verification that is captured at each verification occasion, with the biometric template that is read from the token device.

The gates shall be a closed system where they operate independently and no connections exist between the gates and/or with an open network.

The biometric system shall be built in compliance with the relevant International Standards, and the API and biometric template formats shall be open to the general

public. For example, the biometrics portion shall at least comply with ISO/IEC 19784, ISO/IEC 19794-2 or ISO/IEC 19794-4. For token devices, if the tokens are contact type tokens, they shall at least comply with ISO/IEC 7816, and for contactless tokens, they shall at least comply with ISO/IEC 14443.

### 4.2.2. System Structure

Fig 4-2 shows the scope of this Security Profile. The entry/exit management system is mainly divided into the following parts: account registration, personal identity verification, access control, staff information management, and gate open/close. Of these five functional blocks, the parts relevant to biometrics authentication processing are the account registration and personal identity verification parts. Hereafter, within this Security Profile, the account registration and personal identity verification parts will collectively be referred to as biometrics authentication systems and the Security Profile for this biometrics authentication system shall be defined (the access control, staff information management, and gate open/close parts are beyond the scope of this Security Profile).

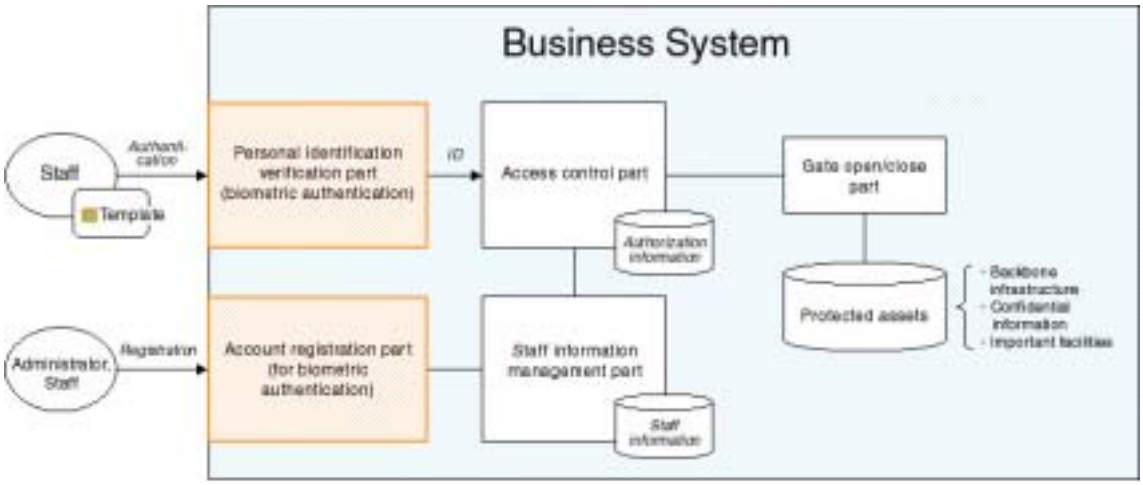


Fig. 4-2: The System Structure

The following are descriptions of each part.

(ㅁ) (1) Account Registration

This part collects from the staff and employees that will be given privilege to pass the gate, fingerprint information for creating biometric templates, and stores the information onto authentication tokens. This part contains the following functions:

[Fingerprint Reading Function]

The function to read fingerprint information stored on an authentication token when registering an account. This function consists of fingerprint sensors, driver software for fingerprint sensors, and other items.

[Token Writing Function]

The function to write the biometric template of the fingerprint collected from the staff and the ID onto an authentication token in order to register an account. This function consists of token writers and driver software for the token writers.

[Staff Information Input Function]

The function to enter various staff information (name, title, etc.) when registering an account. This function consists of keyboards, display devices, and input/output software.

[Biometric Template Generation Function]

The function that converts staff fingerprint information read from a fingerprint collection device into biometric template information to be stored on an authentication token. This function consists of fingerprint minutiae extraction, encoding, and other processes.

(ㅅ) (2) Personal Identity Verification

This part verifies that the staff is indeed the person who he/she claims to be by checking that the fingerprint information collected from the staff on the spot, matches the biometric template information of the staff that is stored on the authentication token. This part contains the following functions:

[Finger Print Reading Function]

The function used by the authenticated person to enter fingerprint information into

the personal identity verification part. This function consists of fingerprint sensors, driver software for fingerprint sensors, etc.

[Token Reading Function]

The function used by the authenticated person to enter an authentication token into the personal identity verification part. This function consists of token readers, driver software for the token readers, etc.

[Fingerprint Information Verification and Authenticity Validation Function]

The function that compares fingerprint information output from the fingerprint reading function with the biometric template output from the token reading function, then compares the result to a threshold value that determines the authenticity, and then judges its authenticity depending on the results.

This function consists of fingerprint minutiae extraction, fingerprint information comparison, and authenticity judgment processes.

(ニ) (3) Access Control

This part determines whether the staff whose identification was verified as a result of the personal identity verification, has the appropriate privileges to pass the gate. The access control part holds privilege information of the staff that are allowed to pass for each gate. Outside of the scope of this Security Profile.

(ホ) (4) Staff Information Management

This part manages information about the staff, such as information that binds the biometric template with the staff, and the staff's names, that are used when performing verification. Outside of the scope of this Security Profile.

(ヘ) (5) Gate Open/Closure

This part performs the physical gate open/closure activities based on the results of the access control part. Outside of the scope of this Security Profile.

## 4.3. Players

In order to examine security threats with regard to access control over "assets that

require protection" such as backbone infrastructure, sensitive information, and important facilities that may incur severe damage from possibilities of acts such terror attacks.

### 4.3.1. Account Registration

Table 4-1: Players in Account Registration

| Role | Description | Assumption | Examples |
|---|---|---|---|
| Outsider | A person who does not belong to the organization that owns the assets that require protection, and who does not have any rights including rights to access the assets. | The person may perform illegal acts to obtain access rights to assets. The person may belong to terrorist or criminal organizations. | Criminal, Terrorist |
| General staff | A person who belongs to the organization that owns the assets that require protection, but who does not have any rights to access the assets. The person has access rights to things and places other than the assets. | The person may perform illegal acts to obtain access rights to assets. The person may have belonged to terrorist or criminal organizations. | General staff, Part time worker |
| Specified staff | A person who belongs to the organization that owns the assets that require protection, and who does have the access rights to assets. | General staff or outsiders may collude to perform illegal acts to obtain access rights to assets. The person may have belonged to terrorist or criminal organizations. | Management, Personnel for specific tasks |
| Registratio | A person who belongs to the | The person has no | N/A |

| | | | |
|---|---|---|---|
| n operator | organization that owns the assets that require protection, and who perform the tasks to issue authentication tokens that are required to access the assets. | malicious intentions and will not collude with other players. | |

### 4.3.2. Personal Identity Verification

Table 4-2 Players in Personal Identity Verification

| Role | Description | Assumption | Examples |
|---|---|---|---|
| General staff | A person who belongs to the organization that owns the assets that require protection, but who does not have any rights to access the assets. The person has access rights to things and places other than the assets. | The person may perform illegal acts to obtain access rights to assets. | General staff, Part time worker |
| Specified staff | A person who belongs to the organization that owns the assets that require protection, and who does have the access rights to assets. | General staff or outsiders may collude to perform illegal acts to obtain access rights to assets. | Management, Personnel for specific tasks |
| Administrator | Staff that performs operational management of the biometrics authentication system. | The person has no malicious intentions and will not collude with other players. | N/A |

## 4.4. Facilities

This Security Profile assumes a highly secure environment as its physical

environment. Specifically, in order to access an area where protected assets are located, staffs are required to pass a personal identity verification system that use biometrics authentication. Furthermore, the person must pass one or more gates (for example, where a guard is posted or a physical key is installed) to reach the personal identity verification system. Thus, the personal identity verification system assumes an environment where only general staff members or specified staff can reach and not an area where any person can approach (see Fig.4-3).

Furthermore, no facility requirements are assumed since it is beyond the scope of this Profile. However, appropriate security shall be maintained.

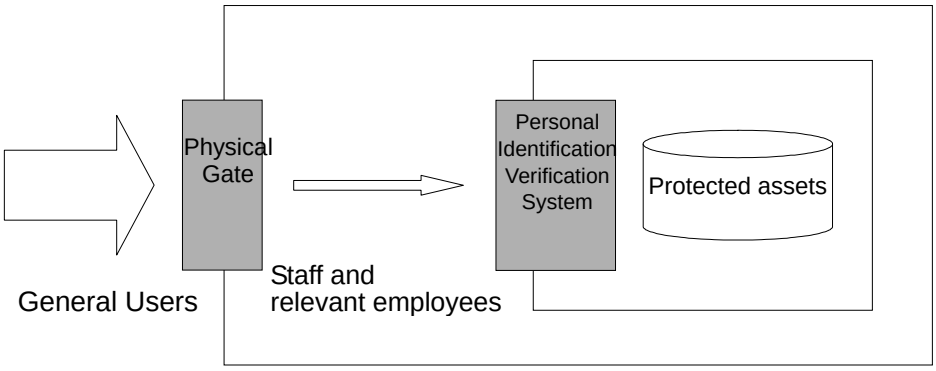


Fig. 4-3: Facilities Assumed for the Security Profile

# 5. Assumed Threats

This chapter describes the threats assumed in this Security Profile for the system defined in the previous chapter.

## 5.1. Considerations of Threats

Since the purpose of this Security Profile is to define security requirements that prevent attackers from “impersonating” specified staff members (legitimate users), the threats assumed will also be limited to threats related to “impersonation.” Thus, security threats such as the following are excluded.

[System Unavailable to Goats and FTA Users]

=> It is expected that alternative steps will be in place as fallbacks. However, security breaches of alternative systems are excluded.

[Availability Degradation]

=> Impersonation shall be impossible even in event of system unavailability. Security breaches of alternative systems when availability degradation is observed is also excluded as noted above.

[Private Information (Biometrics Information, etc) Leakage]

=> A profile for private information protection should be defined separately.

## 5.2. Threat

This section describes the threats identified based on the considerations described in the previous section. The descriptions of the threats are divided into the following three types according to their characteristics.

- Threats Specific to Biometric Authentication

  Threats where the attacking method is considered to be effective only to biometric authentication. This Security Profile covers only threats specific to authentication that use fingerprints.
- Threats Common to All Personal Identity Verification

  “Impersonation” threats common to systems that authenticate people, irrelevant of the authentication method (biometrics authentication, password authentication, possessed item authentication, etc.)
- Threats Common to IT Systems

  Threats that lead to “impersonation” in biometrics authentication systems through existing common attacks that target IT systems.

### 5.2.1. Account Registration (When Performing Pre-Validation Tasks)

Within the account registration tasks, for pre-validation tasks which do not require biometric specific actions, the following threats are assumed.

| Threat | Registration of impersonated specified staff |
|---|---|
| Identifier | T.Pre_Impersonate |

| | |
|---|---|
| Description | Threats where a specified staff that is permitted to enter the room where assets are kept, is impersonated to create an authentication token. A general staff or outsider may impersonate a specified staff. |

| | |
|---|---|
| Threat | Registration of inappropriate staff |
| Identifier | T.Pre_Suspicious_Staff |
| Description | Threats where a specified staff that has access rights to assets for the purpose of his/her task but is inappropriate for security reasons (for example, because he/she belonged to a terrorist organization in the past), registers and creates an authentication token. Possibilities of existence of specified staff with dangerous thoughts cannot be denied. |

| | |
|---|---|
| Threat | Biometric template updated using authentication token of a different specified staff |
| Identifier | T.Pre_Fake_Token |
| Description | Threats where a person updates his/her biometric template using a different specified staff's authentication token obtained through some method, enabling the person to use the authentication token for himself/herself. |

### 5.2.2. Account Registration (When Performing Fingerprint Template Collection Tasks)

Within the account registration tasks, for fingerprint template collection tasks which require biometric specific actions, the following threats are assumed. Note that in examining the threats, the threats listed in the pre-validation tasks section are assumed not to happen here.

(ト) (1) Threats Specific to Biometric Authentication

| | |
|---|---|
| Threat | Registration of arbitrary fingerprints using artifacts |
| Identifier | T.Bio_Artifact_Enroll |
| Descriptio | Threats where specified staff uses physical artifacts towards a |

| | |
|---|---|
| n | capture device to register arbitrary fingerprints. By registering fingerprints of another person, the person with the registered fingerprints will be able to illegally obtain entry rights. |

| | |
|---|---|
| Threat | Registration of low quality biometric templates |
| Identifier | T.Bio_Poor_Enroll |
| Description | Threats where specified staff deliberately or by accident, registers a low quality biometric template, increasing the possibility of successful impersonation by another person when performing personal identity verification. Generally speaking, we cannot say that low quality biometric templates will increase the possibility of accepting somebody else, but the possibility cannot be denied. |

(チ) (2) Threats Common to All Personal Identity Verification

| | |
|---|---|
| Threat | Issuance of an authentication token of another person due to mistake by registration operator |
| Identifier | T.Authsys_Wrong_Enroll |
| Description | Threats where a registration operator issues an authentication token of a person different from the registration applicant due to mistakes such as entry errors when performing registration task. The authentication token issued for a different person may be used to impersonate the other person when performing personal identity verification. |

(リ) (3) Threats Common to IT Systems

| | |
|---|---|
| Threat | Illegal acquirement of registration operator privileges |
| Identifier | T.ITsys_Usurp_Admin |
| Description | Threats where a person who is not a registration operator would become able to perform registration functions. By taking advantage of the registration function, the person will be able to issue an authentication token illegally. |

| | |
|---|---|
| Threat | Expanding of damage due to inability to detect illegal acts or attacks |
| Identifier | T.ITsys_Undetect |
| Description | Threats where damages expand due to the delay of detecting the previous threats because of the lack of evidences left of various attacks and inappropriate actions. Not only will attacks be unnoticed but will also be indistinguishable from operational errors. |

### 5.2.3. Personal Identity Verification

#### (ㅈ) (1) Threats Specific to Biometric Authentication

| | |
|---|---|
| Threat | Impersonation with artificial fingerprints |
| Identifier | T.Bio_Artifact |
| Description | Threats where an attacker will use a physical artificial item towards a capture device in an attempt to impersonate a legitimate user. The artificial item may be created based on fingerprint information or biometric templates that have been captured when performing verification, or may be created based on information obtained from a daily life of an impersonation target. |

| | |
|---|---|
| Threat | Impersonation through replay attack using residual information on fingerprint sensors or memory |
| Identifier | T.Bio_Replay |
| Description | Threats where physical residual fingerprint information on sensors of fingerprint capture devices or residual digital information in memory areas of IT devices are directly used in an attempt to impersonate a legitimate user. |

| | |
|---|---|
| Threat | Impersonation through tampering/counterfeiting |
| Identifier | T.Bio_Fake_Template |
| Descriptio | Threats where an attacker uses his/her own biometric template |

| | |
|---|---|
| n | instead of a legitimate biometric template by tampering with, counterfeiting, or replacing a biometric template in an attempt to impersonate a legitimate user. The biometric template may be attacked at its communication path between the biometric template storage part and the comparison part, or the biometric template storage part itself may be counterfeited or tampered with. |

| | |
|---|---|
| Threat | Impersonation through alternation of thresholds |
| Identifier | T.Bio_Wrong_Parameter |
| Description | Threats where an attacker tampers with authentication parameters such as thresholds and making the identity verification function to come up with a false judgment, in an attempt to impersonate a legitimate user. The authentication parameter may be changed by the parameter alternation function, or through direct access to storage devices, or may be tampered with at the transmission path between the parameter storage part and the processing module. |

| | |
|---|---|
| Threat | Impersonation attributed to authentication accuracy |
| Identifier | T.Bio_Accuracy |
| Description | Threats where vulnerabilities are exploited in an attempt impersonate a legitimate user. Vulnerabilities include the fact that fingerprint authentication is not 100% accurate, or that its accuracy varies depending on the fingerprint authentication product or usage environment. (Example: people with similar minutiae, Wolf, Sheep characteristics.) |

| | |
|---|---|
| Threat | Impersonation due to use in unexpected environments |
| Identifier | T.Bio_Bad_Condition |
| Description | Threats where a system malfunction occurs due to installation of fingerprint sensors and token readers into environments other than those recommended, allowing impersonation. |

### (ル) (2) Threats Common to All Personal Identity Verification

| | |
|---|---|
| Threat | Impersonation through brute force attacks |
| Identifier | T.Authsys_Bruteforce |
| Description | Threats where impersonation is attempted by repetitively performing verification numerous times without utilizing any elaborate methods. This only applies to cases where verification is performed numerous times, and does not include cases where impersonation is achieved by chance after only a few attempts with regard to the accuracy of authentication. |

| | |
|---|---|
| Threat | Impersonation through piggyback attacks |
| Identifier | T.Authsys_Piggyback |
| Description | Threats where impersonation is achieved by piggyback attacks in which a legitimate user performs authentication and a third party enters the room by going in with the legitimate user. There may be cases where the legitimate user does this on purpose, or is forced to do so because he/she is threatened by an attacker. |

| | |
|---|---|
| Threat | Impersonation by taking advantage of alternative procedures |
| Identifier | T.Authsys_Fallback |
| Description | Threats where an attacker causes a false rejection or failure to acquire (FTA) on purpose, in order to use a vulnerable alternative method thereby achieving impersonation. Normally, applies to users that generating false rejections or failure to acquire at a high rate. |

### (ヲ) (3) Threats Common to IT Systems

| | |
|---|---|
| Threat | Illegal execution of administrative function by illegally obtaining administration privileges |
| Identifier | T.ITsys_Usurp_Admin |

| | |
|---|---|
| Description | Threats where a person who does not posses administrative privileges becomes able to execute administrative functions. Various inappropriate actions (altering thresholds, removing limits to the number of retries, etc.) will become possible by maliciously using administrative functions, thereby allowing insufficient countermeasures towards other threats. |

| | |
|---|---|
| Threat | No detection of inappropriate actions and attacks |
| Identifier | T.ITsys_Undetect |
| Description | Threats where no evidences of various attacks and inappropriate actions are left. Disables the ability to appropriately handle attacks due to the lack of evidences and not knowing of the attack, or since there are no execution logs of the administrative functions, deprives the ability to identify whether an event was due to configuration errors or attacks. |

| | |
|---|---|
| Threat | Information leakage |
| Identifier | T.ITsys_Disclose_Info |
| Description | Threats where information is intercepted by certain means from components of the system and leaked to an unauthorized external person. Leaked information may hint methods to breach security, adding to an attacker's potential. |

| | |
|---|---|
| Threat | Execution of illegal actions by altering programs |
| Identifier | T.ITsys_Modify_Program |
| Description | Threats where an attacker tampers with or replaces a software module that comprises a system causing malfunctions in an attempt to impersonate a legitimate user. For example, if a verification module is replaced with a module that always returns an OK, everybody will be able to impersonate anybody. |

| | |
|---|---|
| Threat | Execution of illegal actions by physical tampering |
| Identifier | T.ITsys_Physical_Attack |

| | |
|---|---|
| Description | Threats where unauthorized data is entered by replacing physical components with malicious components or rearranging connection of communication cables to cause malfunction in an attempt to impersonate a legitimate user. |

| | |
|---|---|
| Threat | Malfunction due to accidents or failures |
| Identifier | T.ITsys_Fault |
| Description | Threats where malfunction such as failures that hamper proper behavior of IT devices components (hard drives, network devices, etc.) that comprise the system occurs, thereby allowing impersonation. |

| | |
|---|---|
| Threat | Malfunction due to computer viruses |
| Identifier | T.ITsys_Bad_ITenvironment |
| Description | Threats where vulnerabilities of individual system components such as operating systems and devices are exploited to cause malfunction. |

| | |
|---|---|
| Threat | Threats due to unnecessary functions |
| Identifier | T.ITsys_Unnecessary_Function |
| Description | Threats where unnecessary software such as programming environments or function enhancements such as USBs are exploited in systems that are comprised of general purpose devices including personal computers, thereby causing malfunctions. |

# 6. Security Requirements

This chapter describes the security requirements for threats mentioned above, dividing the requirements into functional requirements and operational requirements.

## 6.1. Functional Requirements

This section defines the security requirements to be addressed with IT functions by

dividing the requirements into an account registering part and personal identity verification part. ISO/IEC 15408 was used as basis in defining the requirements.

- Security functions of the account registration part

  Defines functional requirements that are required for IT systems used for registering staff information. Focuses on the account registration part of the system configuration diagram.
- Security functions of the personal identity verification part

  Defines functional requirements that are required for IT systems used for personal identity verification of staff. Focuses on the personal identity verification part of the system configuration diagram.

Using the above two sections as the major category, the functions are detailed in lower level categories. The requirements measures have mandatory items as well as optional items. Optional items are defined as items which employment to actual applications shall be decided upon evaluating the assets to protect and the risks that may arise when not employing them, and considering cost-effectiveness.

Furthermore, the functional requirements are assigned unique numbers (Fig. 6-1).

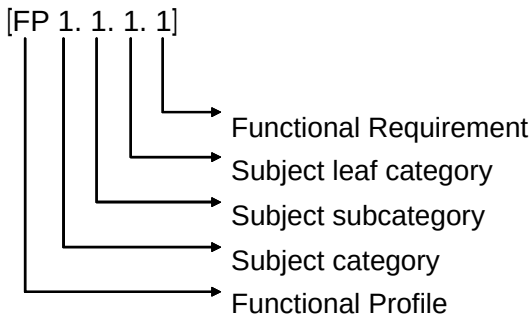


**Fig. 6-1: Numbering Rule of Operational Profiles**

### 6.1.1. Account Registration

(ワ) (1) Identification and Authentication

(a) User Authentication

[FP 1.1.1.1] No administrative functions shall be executable until authentication as registration operator is successful. [MANDATORY]

[FP 1.1.1.2] Multiple authentication mechanisms shall be used when authenticating registration operator. [OPTIONAL]

(b) Unforgeable Authentication

[FP 1.1.2.1] The function shall be capable of detecting capture operations that use counterfeited artificial fingers. [OPTIONAL]

(c) User Identification

[FP 1.1.3.1] No administrative functions shall be executable until identification as administrator is successful. [MANDATORY]

(d) Authentication Failures

[FP 1.1.4.1] The function shall detect that an authentication failed after a certain number of retries, and shall notify the administrator as such. [MANDATORY]

[FP 1.1.4.2] The function shall detect that an authentication failed after a certain number of retries, and shall cease use of the failed account for a certain period [MANDATORY]

(**カ**) (2) Security Audit

(2) Security Audit Generation

[FP 1.2.1.1] The function shall be capable of recording an audit of the following audit target events. [MANDATORY]

a) Starting and stopping audit functions
b) Authentication token issuance
c) Registration operator's login and logout
d) Registration operator authentication failure exceeding a specified number of times
e) Other events that may be considered as security breaches

[FP 1.2.1.2] Each audit record shall record at least the following information. [MANDATORY]

a) Date and time of the event, the type of event, subject identification information, and event results (success or failure)

b) Other audit related information

[FP 1.2.1.3] Each audit target event shall be associated with the identification information of the user that caused the event. [MANDATORY]

(b) Security Audit Event Storage

[FP 1.2.2.1] The administrator shall be notified when an audit trail exceeds a defined threshold. [OPTIONAL]

[FP 1.2.2.2] Audit trails shall be protected from accidental loss by storing them in redundant storage media. [OPTIONAL]

[FP 1.2.2.3] Audit trails shall be protected from accidental loss by making the storage media read-only. [OPTIONAL]

(ヨ) (3) Security Management

(a) Management of Security Attribute

[FP 1.3.1.1] Only fingerprint data that satisfy the target precision of fingerprint data quality shall be registered. [OPTIONAL]

(b) Specification of Management Functions

[FP 1.3.2.1] Fingerprint data quality confirmation prompts shall be displayed when capturing fingerprints. [MANDATORY]

[FP 1.3.2.2] Fingerprint image confirmation prompts shall be displayed when capturing fingerprints. [OPTIONAL]

[FP 1.3.2.3] Record content confirmation prompts shall be displayed when issuing authentication tokens. [MANDATORY]

[FP 1.3.2.4] The access control part shall be notified immediately when it is found that an inappropriate authentication token had been issued. [MANDATORY]

(タ) (4) Time stamps

[FP 1.4.1.1] The system shall be capable of querying a time server and adjusting its own time information accordingly. [OPTIONAL]

[FP 1.4.1.2] The system shall have a highly accurate clock built-in and shall use

accurate time information. [OPTIONAL]

6.1.2. Personal Identity Verification

(レ) (1) Identification and Authentication

(a) User Authentication

[FP 2.1.1.1] No administrative functions shall be executable until authentication as administrator is successful. [MANDATORY]

[FP 2.1.1.2] Multiple authentication mechanisms shall be used when authenticating an administrator. [OPTIONAL]

[FP 2.1.1.3] Authentication shall be performed again when halting a function of the biometrics authentication system. [OPTIONAL]

(b) Unforgeable Authentication

[FP 2.1.2.1] The function shall be capable of detecting or preventing use of counterfeited artificial fingers when performing authentication. [OPTIONAL]

[FP 2.1.2.2] The function shall be capable of identifying whether a fingerprint is a residual fingerprint on the surface of a sensor. [OPTIONAL]

[FP 2.1.2.3] The function shall be capable of detecting or preventing use of counterfeited tokens when performing authentication. [OPTIONAL]

(c) User Identification

[FP 2.1.3.1] No administrative functions shall be executable until identification as administrator is successful. [MANDATORY]

(d) Authentication Failures

[FP 2.1.4.1] The function shall detect that an authentication failed after a certain number of retries, and shall notify the administrator as such. [MANDATORY]

[FP 2.1.4.2] The function shall detect that an authentication failed after a certain number of retries, and shall cease use of the failed account for a

certain period [OPTIONAL]

(ソ) (2) Security Audit

(a) Security Audit Generation

[FP 2.2.1.1] The function shall be capable of recording an audit of the following audit target events. [MANDATORY]

a) Starting and stopping audit functions

b) Other individually defined audit target events.

[FP 2.2.1.2] Each audit record shall record at least the following information. [MANDATORY]

a) Date and time of the event, the type of event, subject identification information, and event results (success or failure)

b) Other audit related information

[FP 2.2.1.3] Each audit target event shall be associated with the identification information of the user that caused the event. [MANDATORY]

(b) Security Audit Event Storage

[FP 2.2.2.1] The administrator shall be notified when an audit trail exceeds a defined threshold. [OPTIONAL]

[FP 2.2.2.2] Audit trails shall be protected from accidental loss by storing them in redundant storage media. [OPTIONAL]

[FP 2.2.2.3] Audit trails shall be protected from accidental loss by making the storage media read-only. [OPTIONAL]

(ツ) (3) Data Protection

(a) Data Transfer Protection

[FP 2.3.1.1] When transferring biometric templates stored on an authentication token, the function shall be able to detect alternation, deletion, insertion, and replay. [MANDATORY]

(b) Data confidentiality protection

[FP 2.3.2.1] Important data such as fingerprint information shall be protected from exposure when transmitting between individual parts. [OPTIONAL]

(c) Data Authentication

[FP 2.3.3.1] The function shall be capable of verifying the authenticity of the contents of a biometric template. [MANDATORY]

[FP 2.3.3.2] The function shall be capable of verifying the authenticity of a token. [OPTIONAL]

(ネ) (4) Security Management

(a) Management of Security Attribute

[FP 2.4.1.1] Only valid values shall be set as values for the various configuration settings. [OPTIONAL]

[FP 2.4.1.2] The function for changing the various configuration setting values shall be made unusable when actual operation of the system begins. [OPTIONAL]

(b) Specification of Management Functions

[FP 2.4.2.1] Confirmation prompts shall be displayed when changing settings. [MANDATORY]

[FP 2.4.2.2] Operation administrator(s) shall be notified when halting a function of the biometrics authentication system. [OPTIONAL]

(ナ) (5) Time stamps

[FP 2.5.1.1] The system shall be capable of querying a time server and adjusting its own time information accordingly. [OPTIONAL]

[FP 2.5.1.2] The system shall have a highly accurate built-in clock and shall use accurate time information. [OPTIONAL]

## 6.2. Operational Requirements

This part divides the Operational Requirements into the following three major

sections. ISO/IEC 17799:2000 was used as basis in defining the requirements, and areas pertaining to biometrics authentication were newly established.

- Basic Items

  This defines the basic requirements necessary to operate biometric authentication systems while ensuring its security.
- Security During Account Registration

  This defines operational requirements necessary during registration of staff information. Focuses on the account registration part of the system configuration diagram.
- Security During Personal Identity Verification

  This defines operational requirements necessary for personal identity verification of the staff. Focuses on the personal identity verification part of the system configuration diagram.

Using the above three sections as major categories, the operation management targets are detailed in lower level categories. Furthermore, management measures (controls) are defined for each lowest level category. The management measures have mandatory items as well as optional items. Optional items are defined as items which employment to actual applications shall be decided upon evaluating the assets to protect and the risks that may arise when not employing them, and considering cost-effectiveness.

Furthermore, the Operational Requirements are assigned unique numbers (Fig. 6-2).

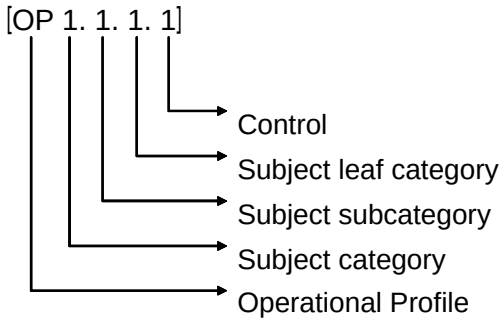


Fig. 6-2: Numbering Rule of Operational Profiles

### 6.2.1. Basic Operation Requirements

Basic security requirements for operational requirements of biometric authentication systems are defined below. The targets of the requirements definition are establishment of “biometric authentication system basic policy,” “organizational security” framework for enforcing and operating the basic policy, “personnel security” of roles of staff, and "communication and operational management" regarding operational management of the system, which are required in operating biometric authentication systems while ensuring security.

#### (ラ) (1) Security Policy

In order to operate biometric authentication systems while ensuring security, security policies must be clearly defined and all staff members must be made aware of the policies. Thus, considering the operation of biometric authentication systems, it is desirable to designate a person responsible for managing the biometric authentication system within the organization, and document the security policies of the system.

[OP 1.1.1.1] An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties. [MANDATORY]

[OP 1.1.1.2] The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. [MANDATORY]

#### (ム) (2) Organizational Security

(a) Information Security infrastructure

It is desirable for an organization that operates a biometric authentication system to introduce information security, and establish a management framework to govern its operation conditions.

[OP 1.2.1.1] An operations committee shall be established to define clear directions for leading security initiatives. [MANDATORY]

[OP 1.2.1.2] The operations committee shall promote security by designating

appropriate responsibilities and allocating sufficient resource. [MANDATORY]

[OP 1.2.1.3] Clearly define the responsibilities towards each individual asset to protect and the responsibilities to enforce the individual security procedures. [MANDATORY]

[OP 1.2.1.4] An authorization procedure by the operations committee for new information processing facilities shall be established. [OPTIONAL]

[OP 1.2.1.5] Advice regarding information security shall be sought from internal or external expert advisors and shall be coordinated with the entire organization. [OPTIONAL]

(b) Identification of risks from third party access

For cases where access by a third party other than specified staff members to areas where assets are located is required, it is desirable to perform risk assessment in order to clarify the consequences to security and to have the third person sign an agreement listing the security requirements with the organization as well as to maintain the security of the assets.

[OP 1.2.2.1] Risks associated with the access by a third party to the facility shall be evaluated and appropriate management measures shall be executed. [MANDATORY]

(**ウ**) (3) Asset classification and control

Assets that are to be protected by the biometric authentication system should be clarified and appropriate protection should be ensured.

[OP 1.3.1.1] For each biometric authentication system, a catalogue of important assets shall be associated and maintained. [MANDATORY]

(**ヰ**) (4) Personnel Security

(a) Security in Job Definition and resourcing

In order to reduce the risk of human error, theft, illegal acts, or misuse of facilities, staff candidates should be informed of security responsibilities at the time of

recruitment, and the candidates should be screened thoroughly. Furthermore, security responsibilities should be included in employment agreements and the persons' adherence to the agreement should be monitored.

[OP 1.4.1.1] Security roles and responsibilities shall be documented appropriately as specified in the biometric authentication system basic policy. [MANDATORY]

[OP 1.4.1.2] Employed staff shall sign a security agreement or a non-disclosure agreement as one of the conditions for employment. [MANDATORY]

(b) User Training

Staff that will use the biometric authentication system shall be trained in order to ensure their awareness towards the threats and considerations of information security and ensure that the staff will comply with the biometric authentication system basic policies while they work, and to minimize any security risks that may occur.

[OP 1.4.2.1] All staff members of the organization as well as relevant external users shall be trained appropriately of the biometric authentication system basic policy and procedures, and update training shall be performed regularly. [MANDATORY]

(c) Responding to security incidents and Malfunctions

In order to minimize the damage from security incidents and malfunctions, and to monitor and learn from such incidents. Staff members should be enforced to report occurrence of events and accidents that may effect security as well as report vulnerabilities of the system. Furthermore, organizations should establish formal punitive procedures for staff members that violate security.

[OP 1.4.3.1] Security events and accidents shall be reported as soon as possible using appropriate communication paths. [MANDATORY]

[OP 1.4.3.2] Require the users of the biometric authentication system to pay attention to and to report of vulnerabilities of the system's security, and of threats or possibilities of threats. [MANDATORY]

[OP 1.4.3.3] Establish procedures to report software malfunctions.

[MANDATORY]

[OP 1.4.3.4] Mechanisms that allow quantification and monitoring of types of events, accidents, or malfunctions as well as scale and cost shall be implemented. [OPTIONAL]

[OP 1.4.3.5] Formal provisions of disciplinary procedures shall be in place to reprimand staff members that have violated biometric system basic policies and procedures. [MANDATORY]

(ノ) (5) Communications and Operations Management

(a) Operational Procedures and Responsibilities

In order to ensure accurate and secure operation of biometric authentication systems, management and operation responsibilities and procedures for all information processing facilities should be established.

[OP 1.5.1.1] Operation procedures clarified by the individual security policies accompanying the biometric authentication system basic policy shall be documented and maintained. [MANDATORY]

[OP 1.5.1.2] Changes of the biometric authentication system shall be managed. [MANDATORY]

[OP 1.5.1.3] Responsibilities and procedures for events and accidents management shall be established in order to ensure quick, effective, and organized actions towards security events and accidents. [MANDATORY]

[OP 1.5.1.4] In order to minimize possibilities of unauthorized changes or misuse of information or services, separation of management or execution of certain duties or responsible areas shall be considered. [OPTIONAL]

(b) Protection Against Malicious Software

In order to protect the integrity of software and information, preventive measures should be taken to prevent and detect intrusion of malicious software.

[OP 1.5.2.1] Detection and prevention management measures to protect against malicious software as well as procedures to make the users aware of them shall be implemented. [MANDATORY]

(c) Housekeeping

In order to maintain the integrity and availability of biometric authentication systems, data should be capable of being backed up and restored and records of the work performed should be logged.

[OP 1.5.3.1] Highly important work information and software shall be backed up regularly and checked. [MANDATORY]

[OP 1.5.3.2] Operators shall keep recording their own work record. [MANDATORY]

[OP 1.5.3.3] Records of operators shall be regularly inspected independently. [OPTIONAL]

[OP 1.5.3.4] Failures shall be reported and corrective actions shall be performed. [MANDATORY]

(d) Network Management

Network security management should be preformed in order to protect the information on the network and to ensure protection of infrastructure supporting the network.

[OP 1.5.4.1] Management measures shall be performed to achieve and maintain network security. [MANDATORY]

(e) Media Handling and Security

Media should be managed and physically protected to avoid damage to assets and interruption of business.

[OP 1.5.5.1] Management procedures for removable media (such as tapes, disks, cassettes) and printed documents shall be prepared. [MANDATORY]

[OP 1.5.5.2] Media no longer required shall be deposited safely and securely. [MANDATORY]

[OP 1.5.5.3] Information handling and storage procedures shall be established to protect information from unauthorized exposure or misuse. [MANDATORY]

[OP 1.5.5.4] Documents pertaining to biometric authentication systems shall be protect from unauthorized access. [MANDATORY]

### 6.2.2. Operation During Account Registration

Operational requirements of biometric authentication systems necessary for account registration of specified staff are defined here.

#### (**オ**) (1) Personnel Security

(a) Security in Job Definition and resourcing

In order to reduce the risk of human error, theft, illegal acts, or misuse of facilities, staff candidates should be informed of security responsibilities at the time of recruitment, and the candidates should be screened thoroughly.

[OP 2.1.1.1] Official certificates (passports or similar documents) shall be inspected when reviewing application materials that have been submitted by recruited staff candidates. [MANDATORY]

[OP 2.1.1.2] Curricula vitae shall be inspected when reviewing application materials that have been submitted by recruited staff candidates. [MANDATORY]

[OP 2.1.1.3] Contractors and temporary workers shall also be subject to equivalent screening procedures. [MANDATORY]

[OP 2.1.1.4] This survey shall be performed regularly for staffs that assume a capacity with substantial authority. [OPTIONAL]

[OP 2.1.1.5] When recruiting staff, the organization shall perform background checks of applicants. [OPTIONAL]

[OP 2.1.1.6] When recruiting staff, the organization shall check applicants against blacklists. [OPTIONAL]

#### (**ク**) (2) Physical and Environmental Security

(a) Secured Areas

In order to prevent unauthorized access, damage, and interruption to working facilities and work information, security boundaries should be made clear and protection measures towards identified risks should be in place.

[OP 2.2.1.1] Multiple security boundaries shall be used to protect rooms where biometric template registration tasks will be performed. [MANDATORY]

[OP 2.2.1.2] In order to ensure access grants to registration applicants only, the room where biometric template registration tasks will be performed shall be protected by appropriate entry/exit management measures. [MANDATORY]

[OP 2.2.1.3] In order to reinforce security of the rooms where biometric template registration tasks will be performed, management measures, such as supervision by multiple people, and policies shall be added. [MANDATORY]

(b) Equipment Security

In order to prevent loss, damages, or degradation of assets and interruption of work activities, devices should be physically protected from security threats and environmental dangers.

[OP 2.2.2.1] Biometric template registration devices shall be installed or protected to minimize risks arising from environmental threats or danger as well as possibilities of unauthorized access. [OPTIONAL]

[OP 2.2.2.2] Wiring of power cables and communication cables that are used for data transfer or information services shall be protected from interception and damages. [OPTIONAL]

[OP 2.2.2.3] In order to ensure the biometric template registration devices' continuous availability and integrity, maintenance of the devices shall be performed properly. [OPTIONAL]

(ヤ) (3) Access Control

(a) Business requirement for access control

Access to information and business procedures need to be managed based on business and security requirements, and in this case, individual policies for scope of information conveyance and authorization of access should be defined.

[OP 2.3.1.1] Business requirements for access control shall be defined and documented. [MANDATORY]

[OP 2.3.1.2] Access to biometric template registration terminals shall be achieved through secure logon procedures. [MANDATORY]

[OP 2.3.1.3] Each staff (general staff and specified staff) shall have a unique identifier (staff ID) so that their activities can be traced later to know who is responsible. [MANDATORY]

[OP 2.3.1.4] Consider preparing duress alarms for staff that may become target of threats. [OPTIONAL]

(b) Access Control of Users

In order to prevent unauthorized access, there should be an official user registration procedure to permit access.

[OP 2.3.2.1] When performing pre-validation tasks, applicants shall be checked whether they have obtained access permission from the system's business management to the areas containing assets. [MANDATORY]

[OP 2.3.2.2] When performing pre-validation tasks, personal identification of the applicant shall be verified using personal identification documents. [MANDATORY]

[OP 2.3.2.3] When performing pre-validation tasks, the applicant shall be checked against blacklists. [OPTIONAL]

[OP 2.3.2.4] When updating a biometric template, in the pre-validation task, information stored in the authentication token owned by the applicant or information printed on the authentication token surface shall be used to verify personal identification of the applicant. [MANDATORY]

[OP 2.3.2.5] When updating a biometric template, in the pre-validation task, the

authentication token owned by the applicant shall be used to verify personal identification through fingerprint authentication. [OPTIONAL]

[OP 2.3.2.6] When performing biometric template registration tasks, the collected fingerprint data shall be checked to see whether the quality is sufficient. [MANDATORY]

[OP 2.3.2.7] Registration operator shall be trained in biometric template registration methods to prevent mistakes from occurring when registering biometric templates, and update training shall be performed regularly. [MANDATORY]

[OP 2.3.2.8] When performing biometric template registration tasks, if fingerprint data of sufficient quality cannot be collected, measures to improve fingerprint data (for example, using fingerprint collection cream) shall be implemented. [OPTIONAL]

(c) Monitoring System Access and Use

In order to detect unauthorized activities, deviation from access control policies should be detected so that it can be used as evidence of security events and accidents, and in order to record events that can be monitored, the system should be monitored.

[OP 2.3.3.1] Audit records which record exceptions and other security related events shall be saved for an agreed period for future investigations and to supplement monitoring of access controls. [MANDATORY]

[OP 2.3.3.2] Monitoring procedures for account registration systems shall be established. [MANDATORY]

[OP 2.3.3.3] Monitoring results shall be reviewed periodically. [OPTIONAL]

[OP 2.3.3.4] Records shall be verified to understand the risks that the system faces and how they occur. [OPTIONAL]

[OP 2.3.3.5] The clock of the computer shall be set correctly. [MANDATORY]

[OP 2.3.3.6] The clock of the computer shall be checked periodically. [MANDATORY]

(ङ) (4) Security of Usage Environment

When capturing fingerprint data from specified staff, the capturing environment

should be the same as the environment used for capturing when performing personal identity verification. Also, when performing a capture, actions and other factors that may skew or hide the characteristics of the target modality should be controlled. Furthermore, fatigue degradation of sensors that capture biometric information should also be taken care of at appropriate times.

(a) Management of Fingerprint Data Capturing Environment

[OP 2.4.1.1] Fingerprint data capturing environments shall be documented appropriately as specified in the biometric authentication system basic policy. [MANDATORY]

[OP 2.4.1.2] Fingerprint data capturing environments shall be configured appropriately according to the product used. [MANDATORY]

(b) Management of user behavior

[OP 2.4.2.1] Guidance for actions when performing biometric template registration shall be documented. [MANDATORY]

[OP 2.4.2.2] Appropriate training shall be performed for specified staff and registration operator to prevent actions that may prompt deformation of biometric characteristics and other factors that may have impact, and update training shall be performed periodically. [MANDATORY]

[OP 2.4.2.3] Registration operator shall be trained in threats regarding artificial fingers, and update training shall be performed regularly. [MANDATORY]

[OP 2.4.2.4] Actions when registering biometric templates shall be monitored periodically. [MANDATORY]

(c) Management of Biometric Sensor

[OP 2.4.3.1] To ensure continuous availability and integrity, sensors for capturing fingerprint data shall be maintained so that they always sustain a certain environment. [MANDATORY]

[OP 2.4.3.2] Fingerprint sensors shall be protected from electrical power anomalies. [OPTIONAL]

[OP 2.4.3.3] Wiring of communication cables that are used for data transfer shall be protected from interception and damages. [OPTIONAL]

### (ケ) (5) Alternative Methods

When an authorized specified staff's modality to be used is unavailable for the biometric authentication system due to injury, loss, or other factors, for the necessity of business, alternative methods should be provided. Furthermore, in order to allow specified staff who originally lack the modality that has been decided for the organization to access assets, personal identity verification through alternative methods other than biometric authentication systems will be required.

(a) Alternative Method for Damaged Modality

[OP 2.5.1.1] Requirements for alternative methods when fingerprint cannot be used due to injuries, loss or other factors, shall be defined and documented. [MANDATORY]

[OP 2.5.1.2] Specified staff members that have used alternative methods shall be managed. [OPTIONAL]

(b) Alternative Methods for FTE Users

[OP 2.5.2.1] Requirements for alternative methods for FTE users shall be defined. [MANDATORY]

(c) Reexamination of alternative methods

[OP 2.5.3.1] The alternative methods shall be maintained and revised according to revision procedures defined. [MANDATORY]

### (フ) (6) Theft and Loss of Authentication Tokens

When a specified staff is stolen or has lost his/her authentication token, the update processing of biometric template information of the person's authentication token should not be performed.

(a) Management Measures on the Event of Authentication Token Theft and Loss

[OP 2.6.1.1] Requirements regarding occasions of authentication token theft and loss shall be defined and documented. [MANDATORY]

[OP 2.6.1.2] Biometric templates shall not be updated with authentication tokens that are known to be stolen or lost. [OPTIONAL]

6.2.3. Operation During Personal Identity Verification

Operational requirements of biometric authentication systems necessary for personal identity verification of the staff are defined here.

(ㄱ) (1) Physical and Environmental Security

(a) Secured Areas

In order to prevent unauthorized access, damage, and interruption to working facilities and work information, security boundaries should be made clear and protection measures towards identified risks should be in place.

[OP 3.1.1.1] Multiple security boundaries shall be used to protect areas including those where the assets a located. [MANDATORY]

[OP 3.1.1.2] In order to ensure access grants to only those authorized, secured areas should be protected by entry/exit management measures that use biometric authentication technology. [MANDATORY]

[OP 3.1.1.3] When selecting and designing secured areas, considerations shall be given to possibilities of damages due to fire, flood, explosions, civil disorder, and other natural or human-caused disasters. [OPTIONAL]

[OP 3.1.1.4] In order to reinforce security of secured areas, management measures and guidance shall be added for work to be done in such areas. [MANDATORY]

(b) Equipment Security

In order to prevent loss, damages, or degradation of assets and interruption of work activities, devices should be physically protected from security threats and environmental dangers.

[OP 3.1.2.1] The fingerprint authentication device shall be installed or protected to minimize risks arising from environmental threats or danger as well as possibilities of unauthorized access. [MANDATORY]

[OP 3.1.2.2] The fingerprint authentication device shall be protected from power failure and other power anomalies. [OPTIONAL]

[OP 3.1.2.3] Wiring of power cables and communication cables that are used for data transfer or information services shall be protected from interception and damages. [OPTIONAL]

[OP 3.1.2.4] In order to ensure the fingerprint authentication devices' continuous availability and integrity, maintenance of devices shall be performed properly. [OPTIONAL]

[OP 3.1.2.5] Storage devices that store information which require discreet handling shall be disposed by physically destructing it or by making sure everything is overwritten. [MANDATORY]

(工) (2) Access Control

(a) Business requirement for access control

Access to information and business procedures need to be managed based on business and security requirements, and in this case, individual policies for scope of information conveyance and authorization of access should be defined.

[OP 3.2.1.1] Business requirements for access control shall be defined and documented. [MANDATORY]

[OP 3.2.1.2] Each staff (general staff, specified staff, administrators) shall have a unique identifier (staff ID) so that their activities can be traced later to know who is responsible. [MANDATORY]

[OP 3.2.1.3] Consider preparing duress alarms for staff that may become target of threats. [OPTIONAL]

(b) Monitoring System Access and Use

In order to detect unauthorized activities, deviation from access control policies should be detected so that it can be used as evidence of security events and accidents, and in order to record events that can be monitored, the system should be monitored.

[OP 3.2.2.1] Audit records which record exceptions and other security related events shall be saved for an agreed period for future investigations and to supplement monitoring of access controls. [MANDATORY]

[OP 3.2.2.2] Monitoring procedures for biometric authentication systems shall be established. [MANDATORY]

[OP 3.2.2.3] Monitoring results shall be reviewed periodically. [OPTIONAL]

[OP 3.2.2.4] Records shall be verified to understand the risks that the system faces and how they occur. [OPTIONAL]

[OP 3.2.2.5] The clock of the computer shall be set correctly. [MANDATORY]

[OP 3.2.2.6] The clock of the computer shall be checked periodically. [MANDATORY]

(テ) (3) Systems Development and Maintenance

(a) Cryptographic controls

In order to protect secrecy, authenticity, or integrity of information that may pose risks, management measures that employ encryption technology should be used.

[OP 3.3.1.1] Individual policies shall be determined of usage of management measures to protect the organization's information through encryption. [MANDATORY]

(b) Security of System Files

In order to ensure that biometric authentication is performed securely, execution of system files should be managed.

[OP 3.3.2.1] Execution of software within the biometric authentication system shall be managed. [OPTIONAL]

[OP 3.3.2.2] Test data shall be protected and managed. [OPTIONAL]

(ア) (4) Security of Usage Environment

When capturing fingerprint data from specified staff, the capturing environment should be the same as the environment used for capturing when performing account

registration. Also, when performing a capture, actions, clothes, and other factors that may skew or hide the characteristics of the target modality should be controlled. Furthermore, fatigue degradation of sensors that capture biometric information should also be taken care of at appropriate times.

(a) Management of Fingerprint Data Capturing Environment

[OP 3.4.1.1] Fingerprint data capturing environments shall be documented appropriately as specified in the biometric authentication system basic policy. [MANDATORY]

[OP 3.4.1.2] Fingerprint data capturing environments shall be configured appropriately according to the product used. [MANDATORY]

[OP 3.4.1.3] Fingerprint data capturing environments shall always maintain a certain condition. [MANDATORY]

(b) Management of user behavior

[OP 3.4.2.1] Guidance for actions when using biometric authentication systems shall be documented. [MANDATORY]

[OP 3.4.2.2] Appropriate training shall be performed to prevent actions that may prompt deformation of biometric characteristics and other factors that may have impact, and update training shall be performed periodically. [MANDATORY]

[OP 3.4.2.3] Actions when using biometric authentication systems shall be monitored periodically. [MANDATORY]

(c) Management of Biometric Sensor

[OP 3.4.3.1] To ensure continuous availability and integrity, sensors for capturing fingerprint data shall be maintained so that they always sustain a certain environment. [MANDATORY]

[OP 3.4.3.2] Fingerprint sensors shall be protected from electrical power anomalies. [MANDATORY]

[OP 3.4.3.3] Wiring of communication cables that are used for data transfer shall be protected from interception and damages. [MANDATORY]

(サ) (5) Prohibiting Piggy Back Entry

After personal identity verification for a specified staff is completed and the physical gate to the area where the protected assets are located is opened, other unauthorized persons should be prohibited from entering with the authorized person.

(a) Management of usage Environment

[OP 3.5.1.1] Specified staff that enter or exit the area where protected assets are located shall be permitted one person at a time by the biometric authentication system. [MANDATORY]

(b) Staff Training

[OP 3.5.2.1] Procedures to make the specified staff members aware of security risks due to piggy back entry shall be implemented. [MANDATORY]

[OP 3.5.2.2] Formal provisions of disciplinary procedures shall be in place to reprimand those who performed piggy back entry. [MANDATORY]

(キ) (6) Alternative Methods

When a specified staff member has forgotten his/her authentication token or the modality to be used is unavailable for the biometric authentication system due to injury, loss, or other factors, for the necessity of business, alternative methods should be provided. Furthermore, in order to allow specified staff who originally lack the modality that has been decided for the organization to access assets, personal identity verification through alternative methods other than biometric authentication systems will be required.

(a) Alternative Method for Lack of Authentication Token

[OP 3.6.1.1] Requirements for alternative methods that will be used when specified staff members that are authorized to access areas where assets are located have forgotten to bring along their authentication token, shall be defined and documented. [MANDATORY]

[OP 3.6.1.2] Specified staff members that have used alternative methods shall be managed. [OPTIONAL]

[OP 3.6.1.3] Formal provisions of disciplinary procedures shall be in place to reprimand specified staff members that have forgotten to bring along their authentication token. [OPTIONAL]

(b) Alternative Method for Damaged Modality

[OP 3.6.2.1] Requirements for alternative methods when fingerprint cannot be used due to injuries, loss or other factor, shall be defined and documented. [MANDATORY]

[OP 3.6.2.2] Specified staff members that have used alternative methods shall be managed. [OPTIONAL]

(c) Alternative Methods for FTE Users

[OP 3.6.3.1] Requirements for alternative methods for FTE users shall be defined. [MANDATORY]

(d) Reexamination of alternative methods

[OP 3.6.4.1] The alternative methods shall be maintained and revised according to revision procedures defined. [MANDATORY]

(ב) (7) Theft and Loss of Authentication Tokens

When specified staff member is stolen or has lost his/her authentication token, the said staff should have his/her access permissions changed and use of the applicable authentication token should be stopped.

(a) Management Measures on the Event of Authentication Token Theft and Loss

[OP 3.7.1.1] Requirements regarding occasions of authentication token theft and loss shall be defined and documented. [MANDATORY]

[OP 3.7.1.2] Authentication token theft and loss shall be reported as soon as possible using appropriate communication paths. [MANDATORY]

[OP 3.7.1.3] Specified staff members whose authentication token was stolen or lost shall have their access rights revoked for a certain period. [MANDATORY]

[OP 3.7.1.4] Requirements regarding alternative methods that are used in the event of authentication token theft and loss shall be defined and documented. [MANDATORY]

[OP 3.7.1.5] Formal provisions for disciplinary procedures shall be in place to reprimand the specified staff members that have lost their token.

[MANDATORY]

(✗) (8) Security Specific to Biometrics Authentication Technologies

(a) Similarities

With biometric authentication, since there are possibilities where persons with similar biometric information exist (for example, faces of a twin), management measures for similarities of biometric information should be established.

[OP 3.8.1.1] Requirements for biometric authentication systems regarding similarities shall be defined and documented. [MANDATORY]

(b) Sheep and Goats

Since there is a high possibility of false accepting or rejecting of people when using biometric authentication due to Wolf (a person with biometric information that allows the person to impersonate someone else easily), Lamb (a person with biometric information that make the person easy to impersonate) and Goat (a person with biometric information who's rejection rate is extremely high) characteristic persons, management measures to handle such uniqueness should be established.

[OP 3.8.2.1] Requirements for biometric authentication systems regarding uniqueness shall be defined and documented. [MANDATORY]

(c) Familiarization

Since false rejections may occur due to failure of capturing biometric information when the specified staff member is not familiar with the usage of biometric authentication devices, management measures for familiarization should be established.

[OP 3.8.3.1] Requirements for biometric authentication systems regarding familiarization shall be defined and documented. [MANDATORY]