Vol.2011-CSEC-54 No.27
Vol.2011-SPT-1 No.27
2011/7/13

国際標準 ISO/IEC15408 に基づく 匿名化処理モジュールの 匿名性評価のフレームワーク提案

松岡健[†]　五十嵐亮基[†]　羅川広行[†]
宮澤泰弘[†]　美馬正司[†]　永井康彦[†]

情報爆発時代の収集したパーソナル情報を利活用した新たなサービス創出の前提として，プライバシー確保のためにパーソナル情報を匿名化処理する技術の研究・開発が進められている．その中で，匿名化処理モジュールの妥当性や匿名化データの匿名性の評価技術も重要となる．しかし，従来の評価方法は，個別観点を評価するものは多様にあるが，実用上は，それらを組み込んだ体系的な評価方法が必要で，かつ社会的受容性や実現性を考慮して既存関連評価制度のスキーマの中で実現できることが望ましい．そこで，本稿では，国際標準 ISO/IEC15408 に基づく，体系的な匿名性評価のフレームワークを提案する．

A Proposal on Framework of Anonymity Evaluation Methodology based on the ISO/IEC15408 for Anonymization Processing Modules

Takeshi Matsuoka[†], Ryoki Igarashi[†], Hiroyuki Serikawa[†], Yasuhiro Miyazawa[†], Tadashi Mima[†] , and Yasuhiko Nagai[†]

As premise of the new service creation using personal activity information in the information explosion age, the research and development of the technique on anonymization processing of personal activity information for privacy protection. It is important technique to the validation for anonymization processing modules and the evaluation of anonymity for anonymization data. However, as for the conventional evaluation method, things evaluating an individual point of view are various, but it is desirable that the systematic evaluation method which incorporated them in the schema of the existing relative standard. In this paper, we propose the framework of systematic anonymity evaluation methodology based on the ISO/IEC15408.

1. はじめに

Web，非 Web 問わず膨大な数の多種多様な情報があふれ，収集・蓄積・解析・発信される情報爆発時代を迎えている中で，収集・蓄積した個人の生活や行動に関するパーソナル情報を利活用した新たなサービス（より適時で個人最適化されたレコメンドサービス等）の創出が期待されている．その前提としては，プライバシー確保が重要であり，情報の利活用と保護の両立を図るための技術として，暗号化やランダム化にならび，有効な技術としてパーソナル情報を匿名化処理する技術（個人の識別が困難になるよう処理する技術）の研究・開発が進められている [1)]．

その中で，サービス事業者が提供する匿名化データを用いたアプリケーションサービスの信頼性を担保するために，匿名化処理モジュールによる匿名化処理の妥当性や匿名化データの匿名性を，中立的・専門的な第三者機関にて評価できる，標準的，汎用的な匿名性評価技術・制度も重要となる．

従来から，*k*-匿名性，*l*-多様性，母集団一意性等のさまざまな指標に基づく匿名性評価方法の研究・開発が進められている [2)]．これらは，匿名化データについて，各々，匿名化データと他のデータのデータマッチングによる個人識別性（特定個人が識別される危険性），特定個人の背景知識を基にした属性推定性（特定の個人に関するプライベートな，あるいはセンシティブな属性情報が推定される危険性），母集団知識を基に個人を推測する個人識別性の観点から，確定的，確率的に評価する方法となっている．

しかしながら，従来の評価方法では，各々の観点での確定的あるいは確率的な個別評価はできるが，実用上はそれらを組み込んだ体系的な評価方法が必要になる．また，匿名性評価技術・制度の社会的受容性や実現性を考慮すると，新規に標準の匿名性評価方法や制度を立ち上げるのではなく，既存の関連する評価制度のスキーマの中で実現することが望ましい．

そこで，本稿では，従来の評価方法を組み込んだ体系的で，かつ，既存関連評価制度における評価技術と整合をとった匿名性評価方法を開発することを目標に，その第一ステップとして，匿名性評価における基準や方法のフレームワークを提案する [3)]．このフレームワークでは，匿名性におけるリスクの構成因子に従来の評価指標も組み込み，それを基に匿名化データを体系的に評価できるようにしている．また，既存関連評価技術として ISO/IEC15408（IT 製品やシステム一般の国際 IT セキュリティ評価基準）をベースにし，これと整合のとれた匿名性評価フレームワークとしている．

2. 標準的な匿名性評価方法の必要性

体系的で，既存関連評価技術・制度と整合をとった匿名性評価方法を実現するため

†（株）日立コンサルティング
Hitachi Consulting Co., Ltd.

Vol.2011-CSEC-54 No.27
Vol.2011-SPT-1 No.27
2011/7/13

の要件は以下となる．

2.1 体系的な匿名性評価方法の要件

匿名化処理モジュールを用いたアプリケーションやサービスの安全性や有効性を保証するためには，以下の事項を考慮する必要がある．

（1）多様な匿名化処理技術（個人識別性，属性推定性等に関するさまざまな匿名性を確保する匿名化処理）の中から適切な選択あるいは組合せ
（2）匿名化データへの推測による再識別リスクの評価の必要性
（3）匿名化データの母数による再識別を防ぐ技術や方法
（4）匿名化処理を行う組織自身の信頼性
（5）法律や政策などの制度による再識別行為の抑止

ここで，上記（1）～（3）が技術的な事項，(4)，(5）が組織や制度等の運用・管理的な事項となる．

従って，技術面に該当する匿名性評価方法としては，上記（1）～（3）を考慮でき，(1) についてはアプリケーションやサービスに対して，選択した匿名化処理の妥当性を検証できること，(2)（3）についてはさまざまな観点から匿名化データの匿名性を評価できること，さらに，これらを体系的に検証・評価できることが要件となる．

2.2 既存関連評価技術・制度との整合の要件

匿名性評価方法に関連する既存評価技術・制度の標準として，広く IT 製品・システムに適用できる国際 IT セキュリティ評価基準 ISO/IEC15408 と，特定分野の専門技術である暗号化処理モジュールに特化した国際評価基準 ISO/IEC19790 がある．

ISO/IEC15408 及び ISO/IEC19790 は，いずれも既に国際的に運用実績のある評価・認証制度であり，国内でも両制度ともに，情報処理推進機構（IPA）を中心に運営されている．また，政府機関の情報セキュリティ対策のための統一基準等，IT 製品・システムの調達条件として両標準が活用されてきているところである．

ISO/IEC15408 は，IT 製品・システム非依存の汎用的な基準ライブラリと評価方法であり，基準ライブラリの中からアプリケーションに応じて適した基準を選択できるようにすることで，よりアプリケーションに適合した評価を行えるようにしている．一方，ISO/IEC19790 は，暗号化処理モジュールに特化した専門的で，かつ，アプリケーションに拠らない特定の要件に対応した評価基準となっている．

匿名化処理モジュールとしては，セキュリティ上重要で専門性が高い点は ISO/IEC19790 と同様であり匿名性に特化した評価ができることが必要だが，データやアプリケーションに応じて適した処理を選択することが重要であることから，ISO/IEC15408 のような基準構造・評価方法であることも必要である．

そこで，社会的受容性や実現性を考慮すると，新規に標準の匿名性評価方法や制度を立ち上げるのではなく，既存の関連する評価制度のスキーマの中で実現することが望ましいことから，既存両標準の匿名性評価に利用できる範囲を特定し，既存標準のスキーマの中で，ISO/IEC19790 の専門評価の特徴と ISO/IEC15408 の対象適応評価の特徴を持つよう拡張することで，匿名性評価を実現できるようにすることが要件となる．

3. 匿名性評価のフレームワークの開発アプローチと方法

体系的，標準的な匿名性評価方法の実現を目標に，その第一ステップとして，匿名性評価のフレームワークを開発する．

匿名性評価のフレームワーク開発は，まず，既存関連標準である ISO/IEC15408 及び ISO/IEC19790 から匿名性評価に利用可能な参考範囲を特定し，次に，その参考範囲から匿名化処理モジュールの妥当性検証，匿名化データの匿名性評価に対応する評価要件の抽出・匿名性評価向けに改良・不足評価要件の追加を行い，フレームワークの概要構造を検討し，その概要との整合を考慮しながら匿名化処理モジュールの妥当性検証，匿名化データの匿名性評価の基本方式を検討し，両者の基本方式からフレームワークの詳細を定義するという開発アプローチで，図 1 に示すような開発プロセスにより，実施した．各開発プロセスの概要・方法を以下に示す．

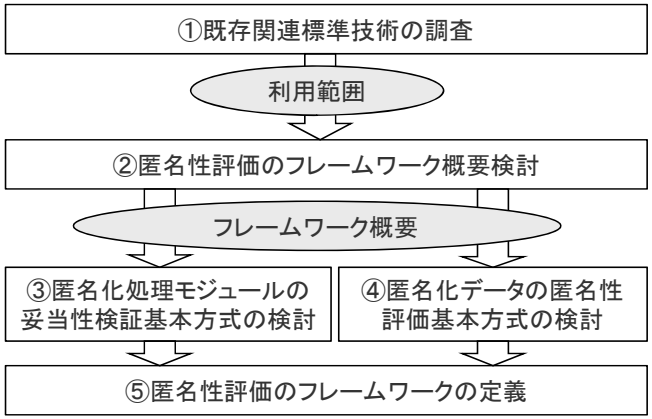

図 1　匿名性評価フレームワークの開発プロセス

① 既存関連標準技術の調査

匿名性評価に利用可能な参考範囲を特定するために，既存関連標準である ISO/IEC15408 と ISO/IEC19790 の調査を行う．

Vol.2011-CSEC-54 No.27
Vol.2011-SPT-1 No.27
2011/7/13

ISO/IEC15408 は IPA 下で現時点運用されている最新の IT セキュリティ評価基準（CC：Common Criteria）[4]と IT セキュリティ評価方法（CEM：Common Evaluation Methodology）[5]を，ISO/IEC19790 は同じく IPA 下で現時点運用されている最新の暗号モジュール評価基準[6]と暗号モジュール試験基準[7]を参照し，調査を行った．

② 匿名性評価のフレームワークの概要検討

①で特定した ISO/IEC15408 と ISO/IEC19790 における匿名性評価方法の参考範囲から，匿名化処理モジュールの妥当性検証，匿名化データの匿名性評価に対応する評価要件を抽出し，匿名性評価向けに改良し，不足要件を追加して，フレームワークの概要構造を検討する．

匿名化処理モジュールは，データ，アプリケーションに応じた評価ができる必要があることから対象適応評価ができる基準構造を持つ ISO/IEC15408 をベースに，また，匿名性専門評価が必要であることから ISO/IEC19790 の専門評価の特徴を参考にし，匿名性評価向けに要件の改良・不足要件の追加を行い，匿名性評価のフレームワーク概要構造を作成した．

③ 匿名化処理モジュールの妥当性検証基本方式の検討

②で検討したフレームワーク概要を考慮し，匿名化処理の妥当性検証の基本方式を検討する．

ISO/IEC15408 でも同様であるが，一般に開発ソフトウェアの妥当性として，用途や環境等の前提条件も含めた要求仕様に対して適した機能が設計されているか，設計どおり実装されているかを検証することが重要であることから，設計・実装の観点から匿名化処理モジュールの妥当性を検証できる基本方式を，ISO/IEC15408 と ISO/IEC19790 を分析して，作成した．

④ 匿名化データの匿名性評価基本方式の検討

②で検討したフレームワーク概要を考慮し，匿名化データの匿名性評価の基本方式を検討する．

匿名化に関するよく知られている性質に個人識別性や属性推定性といったリスクと有用性（匿名化データが，データ利活用者にとって利用価値があるという性質）がある．ここでは，個人が特定されてしまう個人識別性のリスクへの対応がまず重要であることから属性推定性よりも個人識別性を優先対象範囲とした．また，有用性の判断は申請者に拠るところが大きく申請者で対応することが妥当であると考え，評価の対象外とした．このように個人識別リスクを重点とするとともに，一般にリスクは発生の可能性と影響の大きさを考慮することから，発生の可能性と影響の大きさを構成因子とする匿名性のリスクを体系的に定義し，それを基に匿名化データの匿名性リスクを評価できる基本方式を，ISO/IEC15408 と ISO/IEC19790 を分析して，作成した．

⑤ 匿名性評価のフレームワークの定義

②～④で検討したフレームワーク概要に，匿名化処理モジュールの妥当性検証基本方式，匿名化データの匿名性評価基本方式の検討結果を反映して，匿名性評価のフレームワーク詳細を定義する．

両者の基本方式から，匿名化処理モジュールの妥当性検証と匿名化データの匿名性評価を，ISO/IEC15408 と ISO/IEC19790 を分析して，どの評価要件を流用・改良あるいは要件追加して評価できるようにするのかを明確にし，フレームワークの詳細定義を行った．

4. 匿名性評価のフレームワークの開発結果

4.1 既存関連技術の調査結果概要

ISO/IEC15408 と ISO/IEC19790 を調査した結果のまとめを図 2 に示す．

ISO/IEC15408 は，IT 製品・システムの機能要件をカタログ化したセキュリティ機能コンポーネント 11 分類 134 項目と，評価における保証の深さを表す要件をカタログ化したセキュリティ保証コンポーネント 8 分類 88 項目で構成され，匿名性評価方法は匿名性を保証することを目的としていることから，セキュリティ保証コンポーネントを調査対象とした．また，セキュリティ保証コンポーネントは，クラス，ファミリと呼ばれる大項目，中項目に分類・階層化されており，コンポーネントはファミリ内の保証の深さに応じて規定されている．

調査の結果，匿名化処理モジュールの設計の妥当性検証にはセキュリティ基本設計書 ST(Security Target)を基に評価対象 IT 製品・システムの仕様を評価する ASE クラス（セキュリティターゲット評価保証クラス：Assurance class of Security target Evaluation），匿名化処理モジュールの実装の妥当性検証には，評価対象 IT 製品・システムのテスト評価を行う ATE クラス（テスト保証クラス：Assurance class of TEsts），匿名化データの匿名性評価には評価対象 IT 製品・システムの脆弱性を識別・その対策を評価する AVA クラス(脆弱性評定保証クラス：Assurance class of Vulnerability Assessment）のコンポーネントが匿名性評価開発の参考範囲となることがわかった．

一方，ISO/IEC19790 は，暗号モジュールの情報セキュリティに対する要求事項（評価要件）を全部で 11 分類 298 項目規定しており，調査の結果，匿名化処理モジュールの設計の妥当性検証には仕様や前提条件の評価を行う「1.暗号モジュールの仕様」や暗号モジュールの動作環境の評価を行う「6.動作環境」，匿名化処理モジュールの実装の妥当性検証には暗号モジュールのテスト評価を行う「9．自己テスト」，匿名化データの匿名性評価には暗号モジュールに対する攻撃方法を分析・その対処方法評価を行う「11.その他の攻撃への対処」の要求事項が参考範囲となることがわかった．

Vol.2011-CSEC-54 No.27
Vol.2011-SPT-1 No.27
2011/7/13

また, ISO/IEC15408 では保証の深さに応じてコンポーネントをパッケージ化（PKG）した評価保証レベル EAL（Evaluation Assurance Level）を定義しているが，匿名性評価のフレームワーク開発とは，匿名性評価向けの要件を保証の深さに応じてパッケージ化した匿名性評価保証パッケージを開発することである．

従って，基本的に ISO/IEC15408 の参考範囲のコンポーネントを抽出し，匿名性評価向けに改良・追加を行い，匿名性評価保証パッケージを開発し，ISO/IEC19790 の参考範囲の評価要件は，匿名性評価向けに保証コンポーネントを改良・追加する際の参考として利用した．

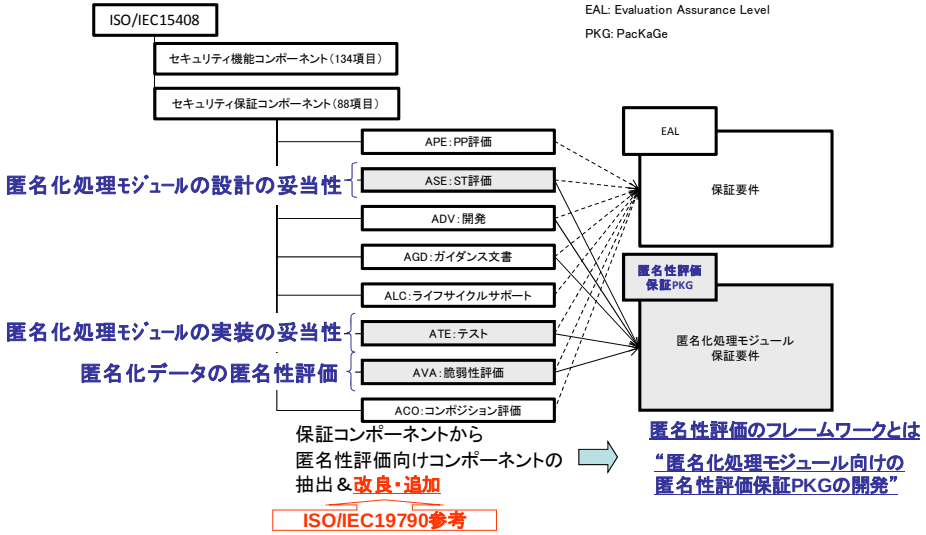

図 2　ISO/IEC15408 の特定した参考範囲と ISO/IEC19790 調査の位置付け

4.2　匿名性評価のフレームワーク概要

ISO/IEC15408 のコンポーネントを匿名性評価向けに改良・追加する方法として，詳細化（refinement）と呼ばれるコンポーネントを評価対象に合うよう具体化するパターンと拡張（extension）コンポーネントを新規に追加するパターンがある．コンポーネントの詳細化パターンは，コンポーネント追加パターンに比べ，現状のコンポーネントや評価方法を流用することができ，ISO/IEC15408 のスキーマとの整合性が高いことから，優先して利用する．

匿名性評価向けにコンポーネントごとのパターンの適合性を検討した結果を以下に示す．

- ASE クラス（新規クラス定義によるコンポーネント追加パターン）
  ISO/IEC19790 でも「1.暗号モジュールの仕様」の評価要件があるように，セキュリティ上重要で専門的である匿名化処理モジュールにおいても，匿名化処理を対象とした専門の仕様の評価要件があることが適当である．しかしながら，ISO/IEC15408 での仕様に該当する ST は IT 製品・システムについて汎用的な評価が実施できるように記述項目が多岐にわたり，その作成が開発者に大きな負担となっている．そこで，匿名化処理モジュールの設計の妥当性検証においては，匿名化処理の範囲に限定した検証で良いことから，従来の ST を簡易化した構成の匿名化処理モジュール基本設計書を定義し，開発者にかかる負担を軽減する．また，この匿名化処理モジュールに特化した基本設計書の構成に沿った評価を行うため，ASE クラスに換えて新規にクラスを定義し，コンポーネントを追加する．
- ATE クラス（コンポーネント詳細化パターン）
  匿名化処理モジュールの実装の妥当性では，従来のテスト評価を実施することと同様で良いため，基本的に既存コンポーネントを流用し，テスト項目の妥当性に関する部分を詳細化する．
- AVA クラス（コンポーネント詳細化パターン）
  従来のコンポーネントを匿名化データの匿名性評価ができるように詳細化して利用する．

以上を踏まえ検討した匿名性評価のフレームワークの概要を図 3 に示す．

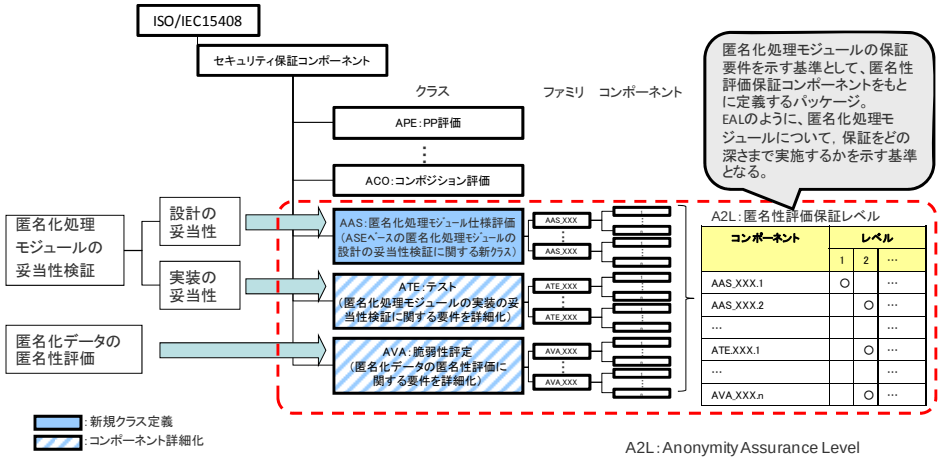

図 3　匿名性評価のフレームワークの概要

Vol.2011-CSEC-54 No.27
Vol.2011-SPT-1 No.27
2011/7/13

匿名化処理モジュールの設計の妥当性検証は，ASE クラスを参考に AAS クラス（匿名化処理モジュール仕様評価クラス：Assurance class of Anonymization processing module Specifications evaluation）を新規に定義し，コンポーネントを追加する．匿名化処理モジュールの実装の妥当性検証，匿名化データの脆弱性評価については， ATE クラスとの AVA クラスコンポーネントを匿名性評価向けに詳細化する．また，上記の匿名性評価保証コンポーネントを，匿名性の保証の深さに応じてパッケージ化し，匿名性評価保証レベル（A2L：Anonymity Assurance Level）として定義する．

4.3 匿名化処理モジュールの妥当性検証基本方式の検討結果概要

ST の構成を参考に，匿名化処理モジュール基本設計書：AT（Anonymization Target）を定義した．この基本設計書では，匿名化処理モジュールの対象/方針・要件・仕様や，その対応，申請者が取得したい A2L のレベル（目標 A2L）とその根拠を記述する構成となっている．この基本設計書を基に匿名化処理モジュールの設計の妥当性を，ASE 同様に各章単位で記述内容の妥当性を見ることで検証する．

また，匿名化処理モジュールの実装の妥当性検証については，ISO/IEC15408 のテスト評価と同様で良いことから，ATE クラスのコンポーネント，すなわち ATE_COV（カバレージ），ATE_DPT（深さ），ATE_FUN（機能テスト），ATE_IND（独立テスト）ファミリのコンポーネントを基本的に流用し，テスト項目の妥当性検証に関する部分を詳細化する．

4.4 匿名化データの匿名性評価基本方式検討結果概要

匿名化データの匿名性評価は，現状 *k*-匿名性や *l*-多様性，母集団一意性等のような多様な匿名性の評価指標があるが，実用上はそれらを組み込んだ体系的な評価方法が必要になることから，一般的なリスクの概念である発生の可能性と影響の大きさを構成因子とする匿名性のリスクを体系的に定義し，構成因子に従来の評価指標も組み込み，その基で評価が行える方法を検討した．以下にその検討結果を示す．

4.4.1 匿名性リスクの定義

匿名性リスクの定義とその構成因子を図 4 に示す．

匿名性リスクは，一般的なリスクの概念から，再特定の可能性と特定された場合の影響の大きさを積算する形式を採り，「再特定の可能性（従来の個人識別リスク）」と「特定された場合の影響の大きさ」を構成因子とする．「再特定の可能性」は，内的要因と外的要因で構成され，内的要因は対象データの特徴として，外的要因は環境条件と攻撃者のタイプとして定義した．ここで，対象データの特徴の中に，従来の *k*-匿名性，*l*-多様性，母集団一意性等の従来の匿名性評価指標も組み込んだ構成としている．一方，「特定された場合の影響の大きさ」は，開示による申請者への影響と利用者や登録者といった個人への影響で構成される．

従って，従来の匿名性指標と相違する匿名性リスクの特長は，「再特定の可能性」（従来の個人識別リスク）において，*k*-匿名性や *l*-多様性等の従来の匿名性指標も構成因子として組み込んだ体系的な構成となっていること，さらに，「再特定の可能性」に加え，「特定された場合の影響の大きさ」も考慮した評価ができることである．

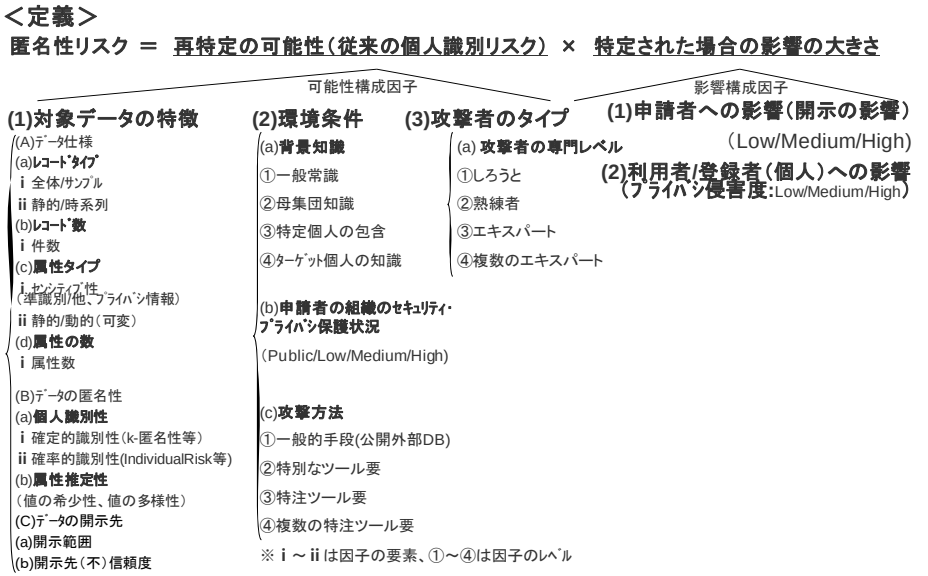

図 4　匿名性リスクの定義と構成因子

4.4.2 匿名性リスクを基にした匿名性評価フロー

匿名性リスクを基に評価を行うためのフローを図 5 に示す．

図 5 の上部は，ISO/IEC15408 の脆弱性評価を行う際のフローで，下部はそれを踏まえて開発した匿名性評価のフローである．

ISO/IEC15408 では評価を行う際に，まず評価対象 IT 製品・システム（以下 TOE と呼ぶ）に関連しそうな潜在脆弱性を洗い出し，TOE に該当するか否か，対策がされているかについて検証を行う．検証後，TOE に該当しない，又は十分な対策がされていない場合は，残存脆弱性として特定し，その脆弱性を攻撃するのに必要な攻撃能力を評価することにより残存脆弱性のリスクを評価する．その残存リスクが目標 EAL に対して許容レベル内であれば合格となり，許容レベル外であれば不合格となり，脆弱性を克服する対策が必要とみなされる．

Vol.2011-CSEC-54 No.27
Vol.2011-SPT-1 No.27
2011/7/13

匿名性評価についても同様に，潜在脆弱性の洗い出しとして，匿名性リスクの構成因子を基に，匿名化対象データの匿名性リスクを評価する．その後，リスク対策の検証として，匿名化対象データの匿名性リスク評価結果を基に，匿名化により各構成因子について，どれほどリスクを軽減できたかを確認する．確認した結果を基に匿名化後の未対策因子を残存脆弱性として特定するとともに，匿名化データの匿名性リスクを評価する．匿名化データの匿名性リスクが目標 A2L の許容レベル内にあれば合格となり，許容レベル外であれば不合格となり，より高度な匿名化を行うなど未対策因子への対策を行う．

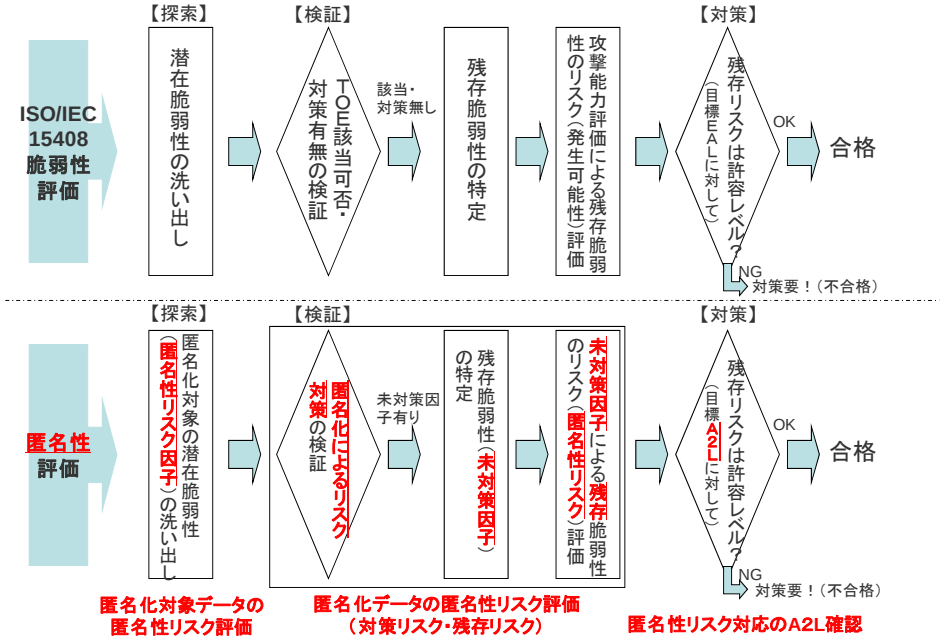

図 5　匿名性評価フロー

4.4.3 匿名性リスク評価方法

匿名性リスクの各構成因子の程度を測るパラメータ値を規定し，表 1 に示す構成因子パラメータ表を作成し，このパラメータ値を用いて匿名性リスクを評価する方法を開発した．各構成因子のパラメータ値は，リスクの低いほうから高いほうへと昇順に並べており，パラメータ値ごとに得点付けしている．

表 1　匿名性リスク構成因子パラメータ表

匿名性リスク						パラメータ値	備考	得点
	再特定の可能性							
		(1)対象データの特徴	(A)ﾃﾞｰﾀ仕様	(a)ﾚｺｰﾄﾞﾀｲﾌﾟ	ｉ 全体/ｻﾝﾌﾟﾙ	サンプル(一部)	サンプリング比0.2程度	1
						サンプル(部分)	サンプリング比0.5程度	2
						全体		4
					ii 静的/時系列	静的		1
						時系列(時折)	月次程度	3
						時系列(頻繁)	日次程度	4
				(b)ﾚｺｰﾄﾞ数	ｉ 件数	件数大	数百万件以上	1
						件数中	数十万件	3
						件数小	数万件	4
				(c)属性タイプ	ｉ ｾﾝｼﾃｨﾌﾞ性（準識別/他、ﾌﾟﾗｲﾊﾞｼｰ情報）	Low	プライバシ情報を含まない	1
						Medium	プライバシ情報を含み、かつ、準識別属性数5以下	3
						High	プライバシ情報を含み、かつ、準識別属性数6以上	4
					ii 静的/動的（可変）	静的属性のみ		1
						動的属性数少	動的属性が5以下	3
						動的属性数大	動的属性が6以上	4
				(d)属性の数	ｉ 属性数	属性数小	5属性以下	1
						属性数中	6属性以上9属性以下	2
						属性数大	10属性以上	4
			(B)ﾃﾞｰﾀの匿名性	(a)個人識別性	ｉ 確定的識別性(k-匿名性等)	Low	再特定リスク<＝0.05(k>＝20)	1
						Medium	再特定リスク>0.05(k<20) 再特定リスク<0.33(k>3)	3
						High	再特定リスク>＝0.33(k<＝3)	4
					ii 確率的識別性(IndividualRisk等)	Low	再特定リスク<＝0.05	1
						Medium	再特定リスク>0.05 再特定リスク<0.33	3
						High	再特定リスク>＝0.33	4
				(b)属性推定性（値の希少性、値の多様性）		Low	リスク<＝0.05 （再特定リスクにあわせて0～1の範囲でオーダリング）	1
						Medium	リスク>0.05 リスク<0.33 （再特定リスクにあわせて0～1の範囲でオーダリング）	3
						High	リスク>＝0.33 （再特定リスクにあわせて0～1の範囲でオーダリング）	4
			(C)ﾃﾞｰﾀの開示先	(a)開示範囲		範囲小	部門内	1
						範囲中	グループ内	2
						範囲大	コミュニティ内	3
						公開	パブリック	4
				(b)開示先（不）信頼度		Low	学術系機関	2
						Medium	政府系機関	3
						High	民間系機関	4
		(2)環境条件		(a)背景知識		④ﾀｰｹﾞｯﾄ個人の知識		1
						③特定個人の包含		2
						②母集団知識		3
						①一般常識		4
				(b)申請者の組織のｾｷｭﾘﾃｨ・ﾌﾟﾗｲﾊﾞｼｰ保護状況		High		1
						Medium		2
						Low		3
						Public		4
				(c)攻撃方法		④複数の特注ツール要		1
						③特注ツール要		2
						②特別なツール要		3
						①一般的手段（公開外部DB）		4
		(3)攻撃者のタイプ		(a)攻撃者の専門レベル		④複数のエキスパート		1
						③エキスパート		2
						②熟練者		3
						①しろうと		4
	特定された場合の影響の大きさ							
		(1)申請者への影響（開示の影響）				Low		1
						Medium		2
						High		3
		(2)利用者/登録者（個人）への影響（プライバシ侵害度）				Low		1
						Medium		2
						High		3

Vol.2011-CSEC-54 No.27
Vol.2011-SPT-1 No.27
2011/7/13

定義した匿名性リスクを算出する方法を図 6 に示す．また，以下に方法の手順を示す．

①：構成因子パラメータ表の各構成因子について該当するパラメータ値を選択する．

②・③：選択したパラメータ値が対応する得点を「再特定の可能生」と「特定された場合の影響の大きさ」ごとに合計し，合計得点に対応する「再特定の可能生」と「特定された場合の影響の大きさ」の値を算出する．

④：「再特定の可能性」の値と「特定された場合の影響の大きさ」の値を積算して匿名性リスクの値を算出する（図 6 ④の匿名性リスク値の網掛けはリスクが高すぎるため，保証できない範囲）．なお，このような準定量的なリスク算出方法は，ISO/IEC27001（ISMS）：情報セキュリティ管理の分野で代表的に利用されている方法である [8]．

⑤：匿名性リスクの値を基に対応する A2L レベルを算出し，この値が目標 A2L 以上となれば，匿名化により目標 A2L 相当か，それ以上にリスクが軽減されている（残存するリスクが目標 A2L の許容レベル内）とみなされ，匿名性リスク評価は合格となる．

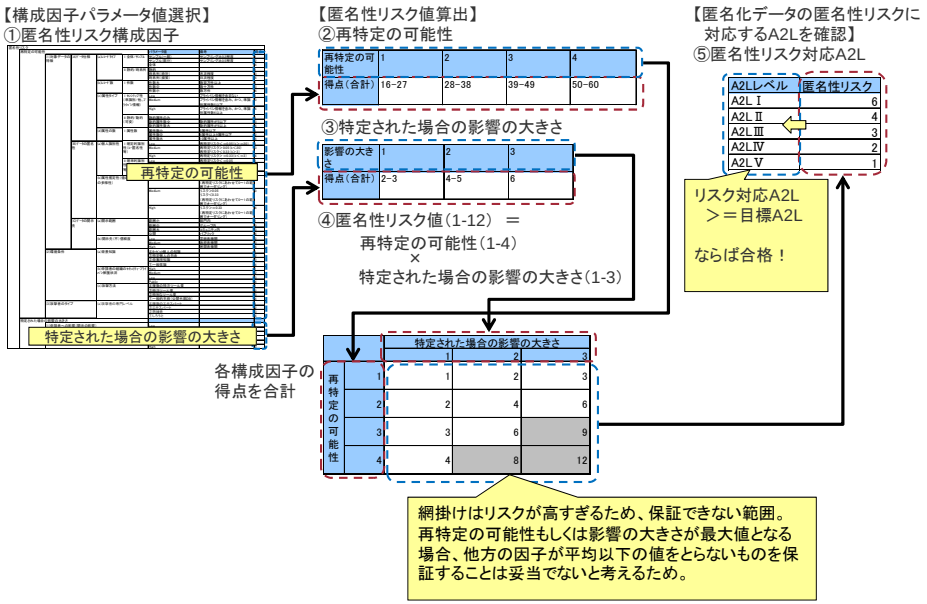

図 6　匿名性リスク評価方法

4.5 匿名性評価のフレームワークの開発結果概要

4.2 節のフレームワーク概要に 4.3 節，4.4 節の基本方式を反映して開発した匿名性評価のフレームワークは，以下の評価基準とその評価基準に基づく評価方法となる 2 つの検証・評価基本方式から構成される．

- 匿名性評価保証コンポーネント群から構成され，匿名性評価のフレームワークとなる匿名性評価保証パッケージ（匿名性評価の評価基準）
- 匿名化処理モジュール基本設計書(AT)による設計の妥当性検証を特徴とする匿名化処理モジュールの妥当性検証基本方式
- 匿名性リスク評価方法を特徴とする匿名化データの匿名性評価基本方式

匿名性評価保証パッケージ（A2L）を図 7 に，表 2 に匿名性評価保証コンポーネントの一覧を示す．

ISO/IEC15408 の保証の深さを表す EAL は商用の最高保証レベルがレベル 5 を目安としていること，ISO/IEC15408 の評価手法 CEM の規定もレベル 5 までとなっていることから，A2L の匿名性保証の深さを Ⅰ から Ⅴ の 5 レベルとした．

AAS クラスは，匿名化処理モジュールの設計の妥当性検証のために，ASE クラスを参考に新規に定義したクラスである．匿名化処理モジュール基本設計書（AT）の章ごとに妥当性を検証するように，各章ごとにファミリを定義した．ISO/IEC15408 では，評価対象の基本仕様のチェックが，以降の EAL に応じた多様な評価の前提になることから，まず ST 評価を行い，ASE クラスにおいて EAL に拠らず，同じ記述・評価レベルを求めるものとなっている．匿名性評価においても同様に，目標 A2L がどのレベルでも AT に同じ記述・評価レベルを求めるものとし，AAS クラスの各ファミリ内の保証コンポーネントをレベル共通のコンポーネントとした．

ATE クラスは，匿名化処理モジュールの実装の妥当性検証を評価する．匿名性評価においても ISO/IEC15408 と同様のテスト評価を実施するため，A2L は EAL と同じである．

AVA クラスは，匿名化データの匿名性評価を行う．匿名化データの匿名性評価基本方式は，匿名性リスクを一般的評価レベル（個人識別情報（各個人をそれ単体で一意に識別可能な情報）の削除あるいは加工（ID 化）をチェック）と体系的評価レベルで評価することから，それぞれのレベルでの評価は AVA_VAN.2（脆弱成分）と AVA_VAN.4（系統的脆弱性分析）が該当する．A2L と保証コンポーネントの対応は，平均より低い保証レベル（A2L Ⅰ，Ⅱ）は AVA_VAN.2 で評価し，平均以上の保証レベル（A2LⅢ以上）は AVA_VAN.4 で評価することとした．

Vol.2011-CSEC-54 No.27
Vol.2011-SPT-1 No.27
2011/7/13

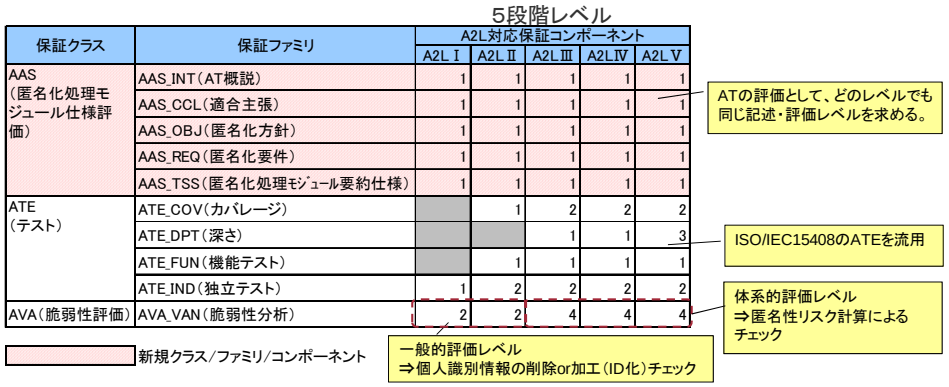

図 7　匿名性評価保証パッケージ（匿名性評価保証レベル：A2L）定義

表 2　匿名性評価保証コンポーネント定義

保証クラス	保証ファミリ	保証コンポーネント	コンポーネント概要	参考既存保証コンポーネント
AAS（匿名化処理モジュール仕様評価）	AAS_INT（AT概説）	AAS_INT.1（AT概説）	AT参照、TOE参照にて、AT及び匿名化処理モジュールが正しく識別されているかどうかを決定する。 また、TOE概要が対象となる匿名化処理モジュールの使用方法、匿名化機能、動作環境、設置環境について正しく記述しているかを決定する。	ASE_INT.1（ST概説）
	AAS_CCL（適合主張）	AAS_CCL.1（適合主張）	対象なる匿名化処理モジュールの目標A2Lを確認する。	ASE_CCL.1（適合主張）
	AAS_OBJ（匿名化方針）	AAS_OBJ.1（匿名化方針）	匿名化処理モジュールの方針として、前提環境/条件、匿名化対象データの仕様と匿名化範囲、開示範囲と匿名化実施レベル、関連するコンプライアンスに関する記述がの妥当かどうかを決定する。	ASE_SPD.1（セキュリティ課題定義） ASE_OBJ.2（セキュリティ対策方針）
	AAS_REQ（匿名化要件）	AAS_REQ.1（匿名化要件）	匿名化処理モジュールの要件や運用環境の要件の妥当性を確認するとともに、各要件に対応するAAS_OBJ.1（匿名化方針）で記述された方針が、要件の根拠として妥当かを決定する。 また、目標A2Lが妥当かも決定する。	ASE_REQ.2（派生したセキュリティ要件）
	AAS_TSS（匿名化処理モジュール要約仕様）	AAS_TSS.1（匿名化処理モジュール要約仕様）	匿名化処理モジュールの仕様として、採用匿名化機能/アルゴリズム、入出力データ仕様の妥当性及び、必要な運用ガイダンス（利用マニュアル、規約類）が用意されているかを決定する。 また、各仕様に対応するAAS_REQ.1（匿名化要件）で記述された要件が、仕様の根拠として妥当かを決定する。	ASE_TSS.1（TOE要約仕様）
ATE（テスト）	ATE_COV（カバレージ）	ATE_COV.1（カバレージの証拠）	開発者が匿名化機能をテストしたかどうか、及び開発者のテストカバレージ証拠がテスト証拠資料に識別されているテストとATの仕様に記述されている匿名化機能との対応を示していることを決定する。	-
		ATE_COV.2（カバレージの分析）	開発者がすべての匿名化機能をテストしたかどうか、及び開発者のテストカバレージ証拠がテスト証拠資料に識別されているテストとATの仕様に記述されている匿名化機能との対応を示していることを決定する。	-
	ATE_DPT（深さ）	ATE_DPT.1（テスト：基本設計）	開発者が匿名化機能を機能仕様と比較してテストしたかどうかを決定することである。	-
		ATE_DPT.3（テスト：モジュール設計）	開発者が全匿名化機能と内部の詳細機能を機能仕様と比較してテストしたかどうかを決定することである。	-
	ATE_FUN（機能テスト）	ATE_FUN.1（機能テスト）	開発者がテスト証拠資料におけるテストを正しく実行し、証拠資料として提出したかどうかを決定する。	-
	ATE_IND（独立テスト）	ATE_IND.1（独立テスト−適合）	匿名化機能のサブセットを独立にテストすることにより、匿名化処理モジュールがATの仕様に特定されているとおりにふるまうかどうかを決定する。	-
		ATE_IND.2（独立テスト−サンプル）	匿名化機能のサブセットを独立にテストすることにより、匿名化処理モジュールがATの仕様に特定されているとおりにふるまうかどうかを決定する。 また、開発者のテストのサンプルを実行することにより開発者のテスト結果において確信を得る。	-
AVA（脆弱性評価）	AVA_VAN（脆弱性分析）	AVA_VAN.2（脆弱性分析）	公知・一般的な脆弱性探索レベルとして、個人識別情報から個人が直接特定できないことを決定する。	-
		AVA_VAN.4（系統的脆弱性分析）	系統的分析による脆弱性探索レベルとして、匿名化データの匿名性リスクが目標A2Lに対する許容レベルにあるかを決定する。	-

新規クラス/ファミリ/コンポーネント　　※下線部は匿名性評価向けにISO/IEC15408/保証コンポーネントを詳細化する部分

5. おわりに

本稿では，社会的受容性や実現性を考慮して既存の国際標準 ISO/IEC15408 をベースに開発した匿名性評価のフレームワークを提案した．本フレームワークは，匿名性評価の評価基準となる匿名性評価保証レベル：A2L，匿名化処理モジュール基本設計書（AT）による設計の妥当性検証を特徴とする匿名化処理モジュールの妥当性検証基本方式，匿名性リスク評価方法を特徴とする匿名化データの匿名性評価基本方式から構成され，匿名化処理モジュールを標準的，体系的に評価することができる．

今後，本稿にて開発した匿名性評価のフレームワークに基づき，定義した匿名性評価保証コンポーネントの内容を具体化し，匿名性評価方法原案を開発する．また，開発原案を基にモデルケースに適用して方法の妥当性・有効性評価を行い，洗練させていく予定である．

謝辞

本研究は，経済産業省　平成 22 年度産業技術研究開発委託費による「次世代高信頼・省エネ型 IT 基盤技術開発事業（行動情報活用型クラウドサービス振興のためのデータ匿名化プラットフォーム技術開発事業）」の一環として行われた．この場を借りて，関係各位に感謝の意を表する．

参考文献

1) 経済産業省：情報大航海プロジェクト　個人情報匿名化基盤, http://www.meti.go.jp/policy/it_policy/daikoukai/igvp/cp2_jp/common/024/010/post-9.html（参照 2011-06-03）．
2) Aggarwal, C. and Yu, P.: Privacy-Preserving Data Mining: Models and Algorithms, Springer-Verlag (2008).
3) 経済産業省：平成 22 年度次世代高信頼・省エネ型 IT 基盤技術開発事業報告書「行動情報活用型クラウドサービス振興のためのデータ匿名化プラットフォーム技術開発事業」, http://www.meti.go.jp/policy/mono_info_service/joho/cloud/2010/index.html（参照 2011-06-03）．
4) IPA（独立行政法人 情報処理推進機構）JISEC（IT セキュリティ評価及び認証制度)：情報技術セキュリティ評価のためのコモンクライテリア,バージョン 3.1 改訂第 3 版［翻訳第 1.0 版］,（2009.7）．
5) IPA JISEC：情報技術セキュリティ評価のための共通方法,バージョン 3.1 改訂第 3 版［翻訳第 1.0 版］,（2009.7）．
6) IPA JCMVP（暗号モジュール試験及び認証制度）：暗号モジュール評価基準 第 0.1 版,（2005.3）.
7) IPA JCMVP：暗号モジュール試験基準 第 0.1 版,（2005.3）．
8) JIPDEC（一般財団法人日本情報経済社会推進協会 情報マネジメントシステム推進センター）：情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項,ISO/IEC27001:2005 対訳版,(2005).