Vol.2022-DPS-190 No.29
Vol.2022-CSEC-96 No.29
2022/3/11

情報銀行のセキュリティに関する一考察

清藤 武暢[1,a)]　四方 順司[1,2,b)]

概要：最近，注目されているビジネス形態の 1 つとして，情報銀行がある．情報銀行は，個人から預託された様々なデータを管理するとともに，当該個人の意思に基づき，預託されたデータを第三者（事業者等）へ提供する事業である．国内においては多くの分野で情報銀行のビジネス化にかかる検討が進められているとともに，実証実験の実施や具体的なサービスの提供等も開始されている．一方，利用する個人の観点からは，情報銀行に預託したデータの漏えいや不正な利用等のリスクに対する懸念が利用に際してのハードルになると推察される．本項では，典型的な情報銀行のモデルを定義した上で，当該モデルで想定される脅威やリスクについて整理するとともに，対策について考察する．

A Remark on the Security of Information Bank

1. はじめに

2010 年以降，個人に関するデータ（属性，行動，嗜好，医療情報等．以下，個人データと呼ぶ）は，社会へのインターネットやデジタル技術の普及によりビッグデータとして取り扱われるようになり，それに伴い，次世代の石油や通貨に例えられるなど，新たな価値を創出するデータとして取り扱われるようになった．政府はこうした個人データ活用の動きを促進させることを目的に，未来投資戦略 2017 において，情報銀行をはじめとするデータ流通プラットフォームの将来的な構築について言及するとともに，その実現にかかる各種活動を推進している [2]．その一環として，総務省と経済産業省は，2017 年から情報銀行のサービスを提供する企業が，当該サービスに求められる機能（情報信託機能と呼ばれる）を有していることを認定するスキームについての検討会を開催し，情報信託機能の認定にかかる指針を公表している [3][4]．こうした動きをうけて，最近，国内の複数の企業が情報銀行のビジネス化にむけた具体的な検討や実証実験等を行なっているほか，一部の企業ではサービス提供も開始している．

情報銀行は，個人から預託されたデータ個人データを管理するとともに，当該個人の意思に基づき，預託されたデータを第三者（事業者等）へ提供する．そして，事業者等はその提供への対価を情報銀行へ支払い，その一部をデータを預託している個人へ還元するという事業である．個人は個人データを預託することにより対価が得られること，情報銀行は預託されたデータを運用することにより利益を得ることができるなど，いろいろなメリットがあることが知られている．

一方，利用者の観点からは，個人データを預託した情報銀行やデータ提供先の企業からの情報漏えいや不正な利用等が情報銀行のサービスを利用する際の懸念となり得ることが推察される．実際，2020 年に実施された情報銀行の利用に関する意識調査においては，多くの個人データについて，利用者はどのような条件（得られる対価の種類や量等）であったとしても提供したくない割合が全体的に高いという結果が示されている [1][*1]．こうした状況を踏まえると，預託した個人データのセキュリティに対する懸念が，情報銀行サービスの普及やその利用に際してのハードルになっていると推察される．

上記の課題に対しては，情報銀行の認定スキームにおいて定められた個人データの管理ルールに従うとともに，適切なセキュリティ対策を行うことで対応が可能と考えられ

[1] 横浜国立大学 先端科学高等研究院
Institute of Advanced Sciences, Yokohama National University
[2] 横浜国立大学 大学院 環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University
[a)] seito-takenobu-bk@ynu.ac.jp
[b)] shikata-junji-rb@ynu.ac.jp

[*1] 厳密には，個人の属性や行動等がより特定されやすいデータほど提供したくないという割合が高く，一方で嗜好等についてはその割合が低い傾向が見受けられる．

る．また，当該認定スキームにおいては，個人データの提供先企業におけるセキュリティ対策の程度により，データの利用形態（例えば，閲覧のみ可能）を制御することが求められている [4]．もっとも，こうした対応には，情報銀行およびデータ提供先企業が相当なコストを負担する必要があるため，情報銀行サービスの提供や利用に対するハードルになっていることも懸念される．

こうした状況を踏まえ，本稿では，上記のように運用面での対応が想定されていたセキュリティ対策の一部を技術面で対応する方法について考察する．具体的には，典型的な情報銀行のサービス（以下，情報銀行サービスと呼ぶ）のモデルを定義した上で，当該モデルで想定される脅威とリスクについて整理する．そのうえで，それらのリスクへの対策として，高機能暗号の 1 つである準同型暗号とメッセージ認証方式を組み合わせた手法について検討し，その安全性評価を行う．

本稿の構成は以下のとおりである．2 節において典型的な情報銀行サービスのモデルとセキュリティ要件について定義し，当該モデル上で想定される脅威とリスクについて整理する．3 節においては，準備として本稿で提案する対策手法で用いる準同型暗号とメッセージ認証方式について説明する．そして，4 節において，準同型暗号を用いた情報銀行のセキュリティ対策について，その処理フローを示すとともに，セキュリティ評価を行う．最後に，5 節においてまとめと今後の課題等について述べる．

2. 情報銀行のモデルとセキュリティ要件

2.1 モデル

本項では，典型的な情報銀行サービスのモデルについて定義する．ここでは，以降の議論が明確となるように最もシンプルなモデルを考えることとする．情報銀行サービスを構成するエンティティは，情報銀行，個人，データ利用事業者である．各エンティティの役割を以下に示す．

情報銀行．個人からの委任を受けたうえで，当該個人の個人データをの預託および管理を行う．また，データ利用事業者とは，個人データの利用条件（利用対象データ，利用目的や対価等）について合意する．そのうえで，個人の許諾に基づき，予め合意した利用条件の範囲内で個人データ（または，それを統計解析等で加工したデータ）をデータ利用事業者へ提供する．当該データの提供後，データ利用事業者より対価を得るとともに，個人へ対価の一部を支払う．本モデルでは，1 つの情報銀行が存在するモデルを想定し，IB と表記する．

個人．情報銀行と自身に関する個人データの利用を許諾する範囲や対価の支払い方法等について合意した上で，当該データを情報銀行へ預託するとともに，情報銀行のデータ提供状況に応じて，対価を受け取る．本モデルでは，複数（n 人）の個人が存在することを想定し，それぞれ $P_1, P_2, \cdots, P_n$ とする．

データ利用事業者．情報銀行から，予め合意した利用条件に基づき，個人データ（または，それを演算処理等で加工したデータ）の提供を受けるとともに，その対価を情報銀行へ支払う．また，提供されたデータは利用条件で合意した期間内でのみ利用できる．本モデルでは 1 つの事業者が存在するモデルを想定し．BP と表記する．

本稿では，議論を単純化するため，対価の支払いについては，個人データの利用頻度に応じて，適切な方法また決済手段を用いて情報銀行及び個人へ支払われているものとし，以下の脅威及びリスクの検討対象外とする．

2.2 想定される脅威およびリスク

本稿で検討対象としている情報銀行サービスにおいては，一般に，情報銀行 IB に対する攻撃（脅威 1），サービス利用事業者 BP に対する攻撃（脅威 2），個人 $P_1, P_2, \cdots, P_n$ への攻撃（脅威 3），通信路への攻撃（脅威 4）が想定される，各脅威における主な攻撃手法お，よび当該攻撃が起因となるリスクの詳細を以下に示す．

脅威 1：情報銀行 IB に対する攻撃とリスク．外部の第三者が，ネットワーク機器等の脆弱性を利用して，情報銀行 IB のシステムへの不正アクセスを試行する．また，内部者の一部が，情報銀行 IB のシステムへの不正アクセスを試行する．これらの攻撃手法が行われた場合，情報銀行 IB が保有している個人データのの盗取や改ざん，サービス利用事業者 BP へ提供するデータの盗取や改ざん，および個人データに対する不正な処理等が主なリスクとして挙げられる．

脅威 2：データ利用事業者 BP に対する攻撃とリスク．外部の第三者が，ネットワーク機器等の脆弱性を利用して，データ事業利用者 BP のシステムへの不正アクセスを試行する．また，内部の一部の不正者が，データ利用事業者 BP のシステムへの不正アクセスを試行する．これらの攻撃が行われた場合，データ利用事業者 BP が保有している提供されたデータの盗取や改ざん，利用期間外でのデータの不正利用等が主なリスクとして挙げられる．

脅威 3：個人 $P_1, P_2, \cdots, P_n$ に対する攻撃とリスク．外部の第三者が，ある個人の端末（スマートフォン等）にマルウェア等を感染させるなどして，当該端末への不正なアクセスを試行する．また，個人の一部が，他の個人が端末内に保有する個人データの盗取や改ざんを試行する．これらの攻撃が行われた場合，ほかの正当な個人が端末等で管理している個人データの盗取や改ざんが主なリスクとして挙げられる．

脅威 4：通信路に対する攻撃とリスク．外部の第三者が，各

エンティティ間の通信路上でやり取りされている情報の盗取や改ざんを試行する．この攻撃が行われた場合，通信路上でやり取りされる情報の盗取や改ざん等が主なリスクとして挙げられる．

2.3 セキュリティ要件

本項では，前項において整理した脅威とリスクを踏まえ，情報銀行サービスに求められるセキュリティ要件について整理する．情報銀行サービスにおいては，情報銀行へ個人が預託した個人データの盗取や改ざんを防ぐことが，サービスを安全に利用する上で重要となる．また，データ利用事業者が利用条件に基づき処理されたデータを正しく受け取ることができることも必要となる．さらに，情報銀行がデータ利用事業者へ提供するデータの内容について，個人が予め許諾したもの以外は提供されないように個人が制御できることも重要と考えられる．これらの観点に基づき，情報銀行サービスのセキュリティ要件を以下のように定義する[*2]．

個人データの機密性．ある個人 P_i の個人データが漏えいしない．

提供データの機密性．情報銀行 IB がデータ利用事業者 BP へ提供するデータが漏えいしない．

個人データの完全性．ある個人 P_i の個人データが改ざんされない．

提供データの完全性．情報銀行 IB がデータ利用事業者 BP へ提供するデータが改ざんされない．

個人の制御可能性．情報銀行 IB およびデータ利用事業者 BP により，ある個人 P_i が許諾した利用条件とは異なるデータの提供および利用はされない．

3. 準備：準同型暗号とメッセージ認証方式

本項では，後述する情報銀行サービスの実現手法で利用する高機能暗号の 1 つである準同型暗号とメッセージ認証方式の概要について述べる．

3.1 準同型暗号

高機能暗号は，基本的な暗号機能（暗号化，鍵共有，改ざん検知）に加えて，さらに高度な機能を実現する暗号技術の総称であり，その 1 つに準同型暗号がある．準同型暗号は，公開鍵暗号を拡張した暗号技術であり，暗号化されたデータを復号することなく（暗号文のままで），元のデータの演算処理（統計解析や機械学習等）が可能な技術である．そのため，データに対する演算処理時に元のデータを復号する必要がないため，データ管理者またはデータ解析者による不正や，システムへの不正アクセス等に対しても元のデータの機密性を確保できる．

準同型暗号は，実現できる演算処理のタイプにより，単一演算型，Somewhat 演算型，完全型に分類される [6]．単一演算型は，暗号化したデータ同士の加算または乗算のどちらか一方のみ可能な方式である．Somewhat 型は，加算と乗算を組み合わせた演算が可能であるが，乗算の回数に制限のある方式である．完全型は，加算と乗算を組み合わせた演算が可能であり，かつ乗算の回数に制限のない方式である．一般に，加算と乗算を組み合わせることにより任意の演算処理を実現できることが知られているため，Somewhat 型または，完全型はさまざまなアプリケーションで有用となる汎用的な技術と考えられる．

本稿では，完全型の準同型暗号のうち，佐藤らにより提案された方式に注目する [5]．本方式は，特定の演算処理を行った結果（暗号文）のみ復号可能な復号鍵が存在するという性質を有するモデルとなっている．そこで，この性質を利用して，情報銀行サービスにおける各種データの機密性および個人の制御可能性を満たす対策手法の実現を行う．佐藤らが提案した完全型の準同型暗号（以下，完全準同型暗号と呼ぶ）のアルゴリズムとセキュリティ要件の概要を以下に示す[*3]．

- 暗号化鍵生成アルゴリズム **FHEEKGen**．セキュリティパラメータ 1^λ を入力として与えられたとき，すべての個人に対する暗号化鍵（$ek_1, ek_2, \cdots, ek_n$）を出力するアルゴリズムである．
- 演算鍵・復号鍵生成アルゴリズム **FHEKpairGen**．演算処理を表現した回路 F とすべての個人の秘密鍵 $(ek_1, ek_2, \cdots, ek_n)$ を入力として与えられたとき，回路 F に基づく演算処理を実行するための演算鍵 evk_F とその演算結果の暗号文のみ復号できる復号鍵 dk_F を出力するアルゴリズムである．
- 暗号化アルゴリズム **FHEEnc**．データ m_i と暗号化鍵 ek_i（$1 \leq i \leq n$）を入力として与えられたとき，暗号文 C_i を出力するアルゴリズムである．
- 演算アルゴリズム **FHEEval**．回路 F，演算鍵 evk_F と暗号文の組（$C_1, C_2, \cdots, C_n$）を入力として与えられたとき，回路 F に基づく演算結果（暗号文）C_F を出力するアルゴリズムである．
- 復号アルゴリズム **FHEDec**．回路 F に基づく演算結果（暗号文）C_F と復号鍵 dk_F を入力として与えられたとき，演算結果 $F(m_1, m_2, \cdots, m_n)$ を出力するアルゴリズムである．

上記の方式は，無限の計算能力を有する攻撃者に対して安全性を確保することが可能な情報理論的安全性を有

[*2] 前述のとおり，本項では各エンティティ間での対価支払いにかかる手続きについては検討対象外としていることから，対価支払いにかかるセキュリティ要件については除外している．

[*3] ここでは，本稿で想定する情報銀行サービスを実現するために必要最低限の定義等について述べるとともに，参考にした佐藤らの論文とは表現が異なる部分があることに留意されたい．厳密な定義や表現等については提案論文 [5] を参照．

する方式となっている．そのため，暗号化鍵生成アルゴリズム **FHEKpairGen** と演算鍵・復号鍵生成アルゴリズム **FHEKpairGen** は，信頼できる第三者機関（Trusted Authority，以下，TA と呼ぶ）が実施することを前提とする[*4]．

上記の完全準同型暗号においては，攻撃者として暗号文 $(C_1, C_2, \cdots, C_n)$，演算後の暗号文 C_F と演算鍵 evk_F を所持する（無制限の計算能力を有する）攻撃者を想定したうえで，当該攻撃者が元のメッセージ（$m_1, m_2, \cdots, m_n$）関する情報を得られないこと（データの機密性）をセキュリティ要件として定義している（以下，セキュリティ要件 1 と呼ぶ）．

3.2 メッセージ認証方式

前項で述べた完全準同型暗号は，データの機密性を確保することは可能であるが，暗号文への正当な演算処理と，攻撃者による不正な改ざんを識別するのが困難であるために，原理的にデータの完全性を確保することができない．そのため，情報銀行システムに前述の完全準同型暗号のみを利用した場合，各種データの完全性を確保できないことになる．したがって，データの完全性を確保するために，改ざん検知機能を有するメッセージ認証方式を利用する．ここで，前述の完全準同型暗号は情報理論的安全性を有する方式であるため，セキュリティレベルを揃えるために，情報理論的に安全なメッセージ認証方式である認証符号（Authentication-code，以下 A-code と呼ぶ）を利用する [7][8]．典型的な A-code のアルゴリズムとセキュリティ要件の概要を以下に示す[*5]．

- 鍵生成アルゴリズム **AKGen**．セキュリティパラメータ 1^λ を入力として与えられたとき，認証鍵 ak と検証鍵 vk を出力するアルゴリズムである．
- 認証子生成アルゴリズム **AAuth**．メッセージ m，認証鍵 ak を入力として与えられたとき，認証子 α を出力するアルゴリズムである．
- 認証子検証アルゴリズム **AVer**．メッセージ m，認証子 α，検証鍵 vk が与えられたとき，メッセージ m が改ざんされていない場合には $true$，そうでない場合には $false$ を出力するアルゴリズムである．

ここで，前述の完全準同型暗号と同様，鍵生成アルゴリズム **AKGen** は，信頼できる第三者機関 TA が実施することを前提とする．

A-code においては，一般に，攻撃者としてメッセージ m とその認証子 α を有している攻撃者を想定したうえで，異なるメッセージ m' に対する正当な認証子 α' を生成することができないこと（メッセージの正当性）を安全性要件として定義している（以下，セキュリティ要件 2）と呼ぶ．

4. 情報銀行サービスの実現手法

本項では，2.3 項で定義したセキュリティ要件を満たす情報銀行サービスの実現手法について検討する．先にも述べたとおり，本手法は前節で示した特殊な完全準同型暗号と A-code を組み合わせて構成しているものである．また，2.1 項で定義した情報銀行サービスのエンティティに加えて，鍵生成に関する処理を行う信頼できる第三者機関 TA の存在を想定する．実現手法の具体的な構成は以下のとおりである．

1 初期設定フェーズ． 信頼できる第三者機関は，暗号化鍵生成アルゴリズム **FHEEKGen** と鍵生成アルゴリズム **AKGen** を用いて，個人 $P_1, P_2, \cdots, P_n$ に対する暗号化鍵と認証鍵の組（ek_1, ak_1），（ek_2, ak_2），…，（ek_n, ak_n）を生成し，各個人に安全な通信路を用いて配付する（検証鍵（$vk_1, vk_2, \cdots, vk_n$）は信頼できる第三者機関 TA において一時保管する）．また，情報銀行 IB は，データ利用事業者と利用条件について合意し，個人から個人データの利用条件について合意を得たうえで，各個人の認証子に対する検証鍵，当該利用条件にある演算処理 F に対する演算鍵 evk_F と復号鍵 dk_F，および認証鍵と検証鍵の組の生成を信頼できる第三者機関 TA へ依頼する．信頼できる第三者機関 TA は情報銀行からの依頼を受け，すべての個人へ演算処理 F に関する同意を改めて確認し[*6]，予め合意を得ていたことが確認された場合には演算鍵・復号鍵生成アルゴリズム **FHEKpairGen** を用いて evk_F と dk_F を生成し，また生成アルゴリズム **AKGen** を用いて，認証鍵と検証鍵の組（ak_{IB}, vk_{IB}）を生成したのち，保管していた（$vk_1, vk_2, \cdots, vk_n$），ak_{IB} と evk_F を情報銀行 IB，vk_{IB} と dk_F をデータ利用事業者 BP へそれぞれ安全な通信路を用いて配付する．ここでは，議論を簡単にするため，すべての個人 $P_1, P_2, \cdots, P_n$ がデータ利用事業者 BP の利用条件に合意したものとする．

2 個人データの預託フェーズ． 個人 $P_i (i = 1, 2, \cdots, n)$ は，暗号化鍵 ek_i と暗号化アルゴリズム **FHEEnc** を用いて，自身の個人データ m_i の暗号文 C_i を生成したのち，認証鍵 ak_i と認証子生成アルゴリズム **AAuth** を利用して，暗号文 C_i の認証子 α_i を生成する．その後，暗号文と認証子の組（C_i, α_i）を暗号文情報銀行 IB へ送付する．情報銀行 IB は，受信した暗号文と認証子の組（C_i, α_i）に対して，検証鍵 vk_i と認証子検証ア

[*4] 情報理論的安全性の枠組みでは，鍵生成については信頼できる第三者機関 TA が実施するのが一般的である．

[*5] ここでは，完全準同型暗号と同様，A-code についても情報銀行サービスの実現に必要最低限の定義等について述べることとする．

[*6] 信頼できる第三者機関が個人へ演算処理 F に関する同意の確認をする方法としては，個人の端末（スマートフォン等）に承認用アプリをインストールし，当該アプリケーションを介して確認するなどの方法が考えられる．ここでは，適切な方法が存在することを前提とする．

ルゴリズム **AVer** を利用して検証を行い，その結果が $true$ の場合にのみ自身のストレージへ保管する．

3 個人データの演算処理フェーズ． 情報銀行 IB は，データ利用事業者 BP から個人データへの処理依頼を受けて，個人データの暗号文（$C_1, C_2, \cdots, C_n$），演算鍵 evk_F と演算アルゴリズム **FHEEval** を用いて，演算処理の結果（暗号文）C_F を生成する．その後，認証鍵 ak_{IB} と認証子生成アルゴリズム **AAuth** を用いて認証子 α_{IB} を生成したうえで，（C_F，α_{IB}）をデータ利用事業者 BP へ送信する．

4 データ利用フェーズ． データ利用事業者 BP は，情報銀行 IB から受信した（C_F，α_{IB}）に対して，検証鍵 vk_{IB} と認証子検証アルゴリズム **AVer** を利用して検証を行い，その結果が $true$ の場合にのみ復号鍵 dk_F と復号アルゴリズム **FHEDec** 利用して，演算結果 $F(m_1, m_2, \cdots, m_n)$ を復号する．

5. 安全性評価

本項では，前節で検討した情報銀行サービスの実現手法の安全性評価を行う[*7]．

5.1 脅威 1 に対する安全性評価

ここでは，情報銀行 IB のシステムへ不正侵入した第三者および情報銀行 IB の内部者の一部が攻撃者となることを想定する．この場合，攻撃者は個人データの暗号文 $(C_1, C_2, \cdots, C_n)$，$vk_1, vk_2, \cdots, vk_n)$，$ak_{IB}$ と演算鍵 evk_F を入手している．当該攻撃者に対して，各セキュリティ要件を満たすかについて評価する．

5.1.1 個人データの機密性

個人データはすべて完全準同型暗号を用いて暗号化されたうえで，情報銀行 IB に預託されている．ここで，完全準同型暗号がセキュリティ要件 1 を満たしている場合，演算鍵 evk_F を入手している攻撃者であっても，暗号文から元の個人データに関する情報を得ることは難しい．したがって，完全準同型暗号がセキュリティ要件 1 を満たすとき，個人データの機密性は満たされる．

5.1.2 提供データの機密性

情報銀行 IB により個人データを演算処理した結果は暗号化されている．ここで，完全準同型暗号がセキュリティ要件 1 を満たしている場合，演算鍵 evk_F を入手している攻撃者であっても提供データに関する情報を得ることは難しい．したがって，完全準同型暗号がセキュリティ要件 1 を満たすとき，提供データの機密性は満たされる．

5.1.3 個人データの完全性

個人データの暗号文に対しては，A-code の認証子が生成・付与されている．ここで，A-code がセキュリティ要件 2 を満たしている場合，検証鍵（$vk_1, vk_2, \cdots, vk_n$）と検証鍵 ak_{IB} を入手している攻撃者であっても，暗号化された個人データの内容を改ざんすることは難しい．したがって，A-code がセキュリティ要件 2 を満たすとき，個人データの完全性は満たされる．

5.1.4 提供データの完全性

個人データの演算結果(提供データ)に対しては, A-code の認証子が生成･付与されている．ここで, A-code がセキュリティ要件 2 を満たしている場合, 検証鍵（$vk_1, vk_2, \cdots, vk_n$）と検証鍵 ak_{IB} を入手している攻撃者であっても，演算結果の内容を改ざんすることは難しい．したがって，A-code がセキュリティ要件 2 を満たすとき，演算結果の完全性は満たされる．ただし，当該評価は，どのような状況においても情報銀行 IB は演算処理を正しく処理することが前提であり，もし，攻撃者が演算処理のプロセスを改ざんできる場合には，当該セキュリティ要件を必ずしも満たされないことに留意する必要がある．そのため，こうした状況においては，情報銀行 IB における演算処理が正しく行われたことを第三者が検証する仕組みの導入等を検討する必要がある．

5.1.5 個人の制御可能性

演算処理 F に対する演算鍵を信頼できる第三者機関 TA が生成する際，事前に個人に対して合意の確認が行われる．ここで，信頼できる第三者機関 TA と個人の間で確認にかかる処理が適切に行われている場合，合意したものとは異なる演算処理 F' に対する演算鍵を得ることは難しい．したがって，信頼できる第三者機関 TA と個人の間で確認にかかる処理が適切に行われているとき，個人の制御可能性は満たされる．

5.2 脅威 2 に対する安全性評価

ここでは，データ利用事業者 BP のシステムへ不正侵入した第三者およびデータ利用事業者 BP の内部車の一部が攻撃者となることを想定する．この場合，攻撃者は vk_{IB} と dk_F を入手している．当該攻撃者に対して，各セキュリティ要件を満たすかについて評価する．

5.2.1 個人データの機密性

データ利用事業者は個人データの演算結果のみ得られ，元の個人データの暗号文等を入手するのは困難である．したがって，個人データの機密性は満たされる．ただし，演算結果の内容（統計解析の種類等）によっては，演算処理に利用された個人データに関する情報が得られる場合がある[*8]．そのため，こうした状況においては，演算結果から

[*7] 前節で検討した実現手法は，構成要素として情報理論的に安全な方式を利用している．したがって，これらを利用した実現手法も情報理論的に安全であるため，量子コンピュータによる解読への耐性を有する．もっとも，この点については本稿の趣旨と異なるため，詳細な議論は省略する．

[*8] 例えば，複数の数値の平均値と利用されたデータの一部を得られた場合，残りのデータに関する情報が得られることが知られてい

元のデータを推測困難にする仕組みの導入等を検討する必要がある．

5.2.2 提供データの機密性

データ利用事業者 BP は，提供データ（演算結果）を得ることができる権限を有しているため，当該セキュリティ要件については検討対象外とする．

5.2.3 個人データの完全性

データ利用事業者は BP は，個人データおよびその暗号文にアクセスすることは困難であるため，セキュリティ要件は満たされる．もっとも，個人データの機密性における議論と同様，演算処理の種類によってはその結果から元のデータに関する情報を得ることができ，得られた情報を改ざんすることが可能となる．したがって，演算処理の結果から元データを推測困難にする仕組みの導入等のを検討する必要がある．

5.2.4 提供データの完全性

個人データの演算結果（提供データ）に対しては，A-code の認証子が付与されている．ここで，A-code が安全性要件 2 を満たしている場合，vk_{IB} と dk_F を入手している攻撃者であっても，演算結果の内容を改ざんすることは難しい．したがって，A-code がセキュリティ要件 2 を満たすとき，提供データの完全性は満たされる．

5.2.5 個人の制御可能性

脅威 1 における議論と同様であるため，ここでは省略する．

5.3 脅威 3 に対する安全性評価

ここでは，外部の第三者や個人の一部が攻撃者となることを想定する．この場合，攻撃者は（ek_j, ak_j）を入手している．当該攻撃者に対して，各セキュリティ要件を満たすかについて評価する．

5.3.1 個人データの機密性

第三者や個人の一部が，他の個人の端末に格納されている個人データを盗取することは困難である．したがって，他の個人の個人データの機密性は満たされる．もっとも，攻撃者が，マルウェア等を感染させて不正アクセスを行うことも想定され，その場合には当該端末内に保管されている個人データの機密性は満たされない．そのため，当該セキュリティ要件を満たすためには端末内にセキュアな領域を構築するなどの対策が必要がある．

5.3.2 提供データの機密性

第三者や個人の一部が，提供データへアクセスすることは想定モデルにおいては困難である．したがって，提供データの機密性は満たされる．

5.3.3 個人データの完全性

第三者や個人の一部が，他の個人の端末に格納されている個人データを改ざんすることは困難である．したがって，他の個人の個人データの完全性は満たされる．もっとも，攻撃者による端末への不正アクセスが可能な場合には，個人データの完全性は満たされない．したがって，個人データの機密性における議論と同様，セキュアな領域の構築が必要となる．

5.3.4 提供データの完全性

第三者や個人の一部が，提供データへアクセスすることは想定モデルにおいては困難である．したがって，提供データの完全性は満たされる．

5.3.5 個人の制御可能性

個人は演算処理 F の内容を制御する権限を有していることと，個人と信頼できる第三者機関 TA の間で適切な合意の確認にかかる処理が適切に行われている場合，第三者により合意したものと異なる演算処理 F に対する演算鍵を信頼できる第三者機関 TA に生成させることは困難である．したがって，信頼できる第三者機関 TA と個人の間で確認にかかる処理が適切に行われているとき，個人の制御可能性は満たされる．

5.4 脅威 4 に対する安全性評価

第三者は公開情報のみ入手できるため，当該攻撃者にかかる安全性の議論はより多くの情報を得られる情報銀行 IB における安全性の議論に包含されるため，ここでは省略する．

6. まとめ

本項では，最近注目されている情報銀行サービスについて，典型的なモデルを定義するとともに，セキュリティの観点に注目したうえで必要となる要件について整理した．また，当該セキュリティ要件を満たす実現手法について検討し，安全性評価を行った．ここでは，完全準同型暗号と A-code をシンプルに構成した手法について安全性評価を行ったため，一部の脅威に対しては他の仕組みを利用する必要があることが明らかとなった．また，対価の支払いについては本項では検討対象外としたが，具体的なビジネスモデルについて検討する場合には，支払いにかかる方法についてもセキュリティを考慮する必要がある．さらに，ビジネスモデルの内容によっては，追加のセキュリティ要件が必要になることも推察される．

ここで，本稿では通信路として安全ではないチャネル（通信路上でやり取りされるデータに対する第三者による盗取・改ざんが可能）を想定したうえで，やり取りされるデータの完全性を確保するために A-code を利用した．しかし，個人と情報銀行間の通信路が authenticated channel（通信路上でやり取りされるデータに対する第三者による改竄が困難な通信路）となった場合，個人データの暗号文に認証子が不要となる．また，利用するメッセージ認証方

る．

式について，今回は準同型暗号とセキュリティレベルを揃えるために A-code を利用したが，計算量的安全性の枠組みで検討する場合には，Message Authentication Code を利用しての同様の安全性を確保できる[*9]．さらに，情報銀行の実現手法に利用した準同型暗号について，本稿では，佐藤らが提案した方式の適用を考えたが，情報理論的安全性を必要としない場合には，特定の演算処理を行った結果のみ復号可能な復号鍵を生成できる性質を有する準同型暗号を利用しても，同様のセキュリティ要件を満たす手法を実現できる．

今後の課題としては，具体的なビジネスモデルを想定したうえで，より詳細なセキュリティ要件や，これらのセキュリティ要件を満たす実現手法を高機能暗号をはじめとする暗号技術等を利用することにより実現することや，計算量的安全性の枠組みのもと，佐藤らの方式と同様の性質を有する準同型暗号の実現等が挙げられる．こうした研究が，情報銀行サービスのセキュリティ確保，利便性向上とコスト削減の推進に資することを期待したい．

謝辞　本研究は，総務省の「電波資源拡大のための研究開発（JPJ000254）」における委託研究「安全な無線通信サービスのための新世代暗号技術に関する研究開発」の成果の一部である．また，本研究の一部は JSPS 科研費 JP18H03238 の助成を受けたものである．

参考文献

[1] NTT データ経営研究所：情報銀行の利用に関する一般消費者の意識調査，NTT データ経営研究所・ニュースリリース（2020）
[2] 大和総研：2019 年度，情報銀行が本格開業へ，大和総研レポート（2019）
[3] 総務省・経済産業省：「情報信託機能の認定スキームの在り方に関する検討会」の開催，総務省・報道資料（2017）
[4] 総務省・経済産業省：「情報信託機能の認定スキームの在り方に関する検討会とりまとめ（案）」に対する意見募集の結果、とりまとめ及び「情報信託機能の認定に係る指針 ver2.1」の公表，総務省・報道資料（2021）
[5] 佐藤慎吾，四方順司：情報理論的に安全な完全準同型暗号に関する考察，情報処理学会研究報告・コンピュータセキュリティ研究会（2021）
[6] 四方順司：量子コンピュータの脅威を考慮した高機能暗号：格子問題に基づく準同型暗号とその応用，日本銀行金融研究所・金融研究（2019）
[7] E. N. Gilbert, F.J.MacWilliams and N.J.Slone : Code which Detect Deception, Bell System Technical Journal(1974)
[8] G.J.Simon : Authentication Theory/Coding Theory, CRYPTO(1984)

[*9] Message Authentication Code は，共通鍵暗号を利用してメッセージの改ざん検知機能を実現する技術である．