IMES DISCUSSION PAPER SERIES

公開鍵暗号型の高機能暗号を巡る研究動向

清藤武暢(せいとうたけのぶ)・青野良範(あおのよしのり)・四方順司(しかたじゅんじ)

Discussion Paper No. 2017-J-8

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒103-8660 東京都中央区日本橋本石町 2-1-1

日本銀行金融研究所が刊行している論文等はホームページからダウンロードできます。
http://www.imes.boj.or.jp

無断での転載・複製はご遠慮下さい。

備考：　日本銀行金融研究所ディスカッション・ペーパー・シリーズは、金融研究所スタッフおよび外部研究者による研究成果をとりまとめたもので、学界、研究機関等、関連する方々から幅広くコメントを頂戴することを意図している。ただし、ディスカッション・ペーパーの内容や意見は、執筆者個人に属し、日本銀行あるいは金融研究所の公式見解を示すものではない。

IMES Discussion Paper Series 2017-J-8
2017 年 4 月

公開鍵暗号型の高機能暗号を巡る研究動向

清藤武暢（せいとうたけのぶ）*・青野良範（あおのよしのり）**・四方順司（しかたじゅんじ）***

要　旨

金融分野では、クラウド・サービス等によって業務をアウトソース化する動きが進んでいる。とりわけ、近年は、フィンテック（FinTech）企業がクラウド・サービスを通じて新しい金融サービスを提供する事例が注目を集めている。こうしたサービスでは、クラウド・サービス事業者やフィンテック企業によるデータへのアクセス等を適切に制御することが必要である。例えば、データを暗号化したまま効率的にクラウド・サービス等において取り扱うことができれば安全性の観点から望ましい。このようなニーズに対応する技術として、「高機能暗号」の研究開発が活発化している。高機能暗号に基づくクラウド・サービス等が提供されれば、金融機関はデータの安全性を確保しつつアウトソース化等を一段と進めることができると期待される。本稿では、公開鍵暗号型の高機能暗号に焦点を当てて、機能や安全性について説明する。そのうえで、金融機関の業務や新しい金融サービスに高機能暗号を適用するケースを想定し、それらの安全性や処理性能について考察する。

キーワード：クラウド・サービス、検索可能暗号、公開鍵暗号、高機能暗号、準同型暗号、属性ベース暗号、FinTech

JEL classification: L86、L96、Z00

*　日本銀行金融研究所（E-mail:takenobu.seitou@boj.or.jp）
**　情報通信研究機構サイバーセキュリティ研究所（E-mail:aono@nict.go.jp）
***　横浜国立大学大学院環境情報研究院（E-mail:shikata@ynu.ac.jp）

本稿の作成に当たっては、産業技術総合研究所研究員の松田隆宏氏から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行、情報通信研究機構あるいは横浜国立大学の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

目 次

1. はじめに

2000 年代央以後、さまざまなクラウド・サービス（いわゆる「パブリック・クラウド」）が提供されるようになった。その結果、システム開発・運用におけるコスト削減やシステム導入の迅速化、サーバ、ストレージ等のシステム・インフラの拡張性の向上等を企図して、データの処理や管理を当該サービスへアウトソースする動きが、幅広い分野において活発化するようになった。また、そうした動きに追随するように、金融分野においても、クラウド・サービスへの業務のアウトソース化の動きが広がってきている。営業支援システム、社内情報共有システム、電子メールシステム等、金融分野における活用事例は枚挙にいとまがない（金融情報システムセンター［2016］）。

金融機関がクラウド・サービスを利用する際には、マルウェア感染等によって機密性の高いデータが外部に流出するリスクに留意する必要がある。こうしたリスクは、クラウド・サービスを提供する外部事業者が適切なセキュリティ管理を行うことで制御可能である。ただし、当該外部事業者によるセキュリティ管理の状況を外部から把握する必要があり、複数の外部事業者が当該サービスの提供に関与する場合、セキュリティ管理の状況を俯瞰して把握するためには相当なコストを負担しなければならない。その結果、アウトソース化の対象は、「機密性の低いデータのみを取り扱う業務」や「暗号化したデータを保管する業務」等に限定され、金融機関は、クラウド・サービスが本来提供しうるアウトソース化のメリットを十分に享受しているとは言い難い。

このようなデータの属性に起因する業務のアウトソース化にかかる制約を解消しうる技術として、「高機能暗号」の研究開発が活発化している[1]。高機能暗号を用いれば、基本的な暗号機能（データの暗号化や復号）に加えて、「暗号化したままデータを処理する機能」、「効率的にデータを共有する機能」、「エンティティの属性に応じてデータの復号権限を制御する機能」等、高度な機能を実現することができる。今後、高機能暗号を活用したクラウド・サービスが広範に実用化されれば、当該サービスにおけるセキュリティ管理の状況に依存することなく、データの機密性等を確保しつつアウトソース化を一段と進めることができるようになると期待される。

高機能暗号は、金融分野で注目を集めている「フィンテック（FinTech）」の安全性向上にも貢献しうる。最近では、「金融機関の顧客に代わって金融機関のデータ（口座残高や送金履歴等）にアクセスし、それらを収集・加工して当該顧客に提供する」といった口座情報サービス（Account Information Service）をス

[1] 近年、クラウド・サービスでの高機能暗号の実用化に向けた研究開発が活発化しており、一部の暗号については既に製品化されている（清藤・四方［2014］、小暮・下山・安田［2015］）。

マートフォンによって提供するノンバンク企業が登場している。このように、スマートフォン等を活用し、金融機関やその顧客とデータ通信を行いつつ新しい金融サービスを提供するノンバンク企業は、「TPPs（Third Party Providers）」や「電子決済等代行業者」と呼ばれている（European Commission [2015]、金融庁［2016］、全国銀行協会［2016］）。従来、金融取引や資産に関するデータは、金融機関とその顧客によってのみ取り扱われてきた。これに対し、上記のような新しい金融サービスでは、TPPs によっても取り扱われるようになる。このため、金融取引等に関するデータへの TPPs によるアクセスをどう制御していくかが重要な課題になっている（中村［2016］）。

こうした課題への対応策の 1 つとして、高機能暗号の活用が考えられる。例えば、金融機関は、金融取引等に関するデータを高機能暗号によって暗号化して TPPs に送信し、TPPs ではそのデータを暗号化したまま統計解析等を実行する（データの機密性を高める）といった方法が想定される。また、TPPs による金融取引等に関するデータへのアクセスに関して、アクセスを許可するデータの範囲や TPPs の属性等を限定し、その範囲内でのみアクセスが可能となるように、高機能暗号によって当該データを暗号化するという方法も考えられる。筆者らが知る限り、高機能暗号を利用したサービスは、現時点では、まだ提案されていないとみられるが、今後の高機能暗号の重要な応用分野の 1 つとなる可能性がある。

高機能暗号の実用化に向けた研究開発は、今後、一段と進展していくとともに、上記のような高機能暗号の活用方法についても実現可能性が高まっていくと考えられる。将来的には、金融機関、クラウド・サービス事業者、TPPs が、より安全で効率的な業務やサービスの提供を検討していくうえで、高機能暗号が選択肢の 1 つとなる可能性がある。もっとも、現在は、既存の高機能暗号の機能等について十分に整理されているとはいえないほか、金融分野におけるアプリケーションを前提とした安全性等の評価についても研究途上にあるというのが実情である。

高機能暗号には、公開鍵暗号型と共通鍵暗号型の 2 つのタイプが存在する。公開鍵暗号型は、暗号化に用いる鍵（以下、「暗号化鍵」と呼ぶ）と復号に用いる鍵（以下、「復号鍵」と呼ぶ）が異なり、暗号化鍵を公開できるため、当事者間で事前に鍵の共有を行う必要がないという特長を有する。また、基礎技術として数学的な仕組みが用いられており、この仕組みを応用することによって、これまでにさまざまな機能が実現されている。他方、共通鍵暗号型は暗号化鍵と復号鍵が同一となり、当事者間で事前に鍵の共有を行う必要がある。また、現時点では、公開鍵暗号型と比較して、実現されている機能は少ない。一方、共通鍵暗号型は公開鍵暗号型よりも暗号処理に要する速度が高速であるという

特長を有する[2]。

こうした背景を踏まえ、本稿では、これまでにさまざまな機能が実現されている公開鍵暗号型の高機能暗号に注目し、それらの機能や安全性について説明する。合わせて、金融分野で利用可能なモデルを定義して高機能暗号の適用可能性についても考察する。2 節では 2 つのモデルを示し、3 節では、既存の高機能暗号が実現する機能と安全性について説明する。4 節では、各モデルにおいて高機能暗号の活用が想定されるケースを示し、具体的な活用方法を検討したうえで、その安全性や処理性能について考察する。

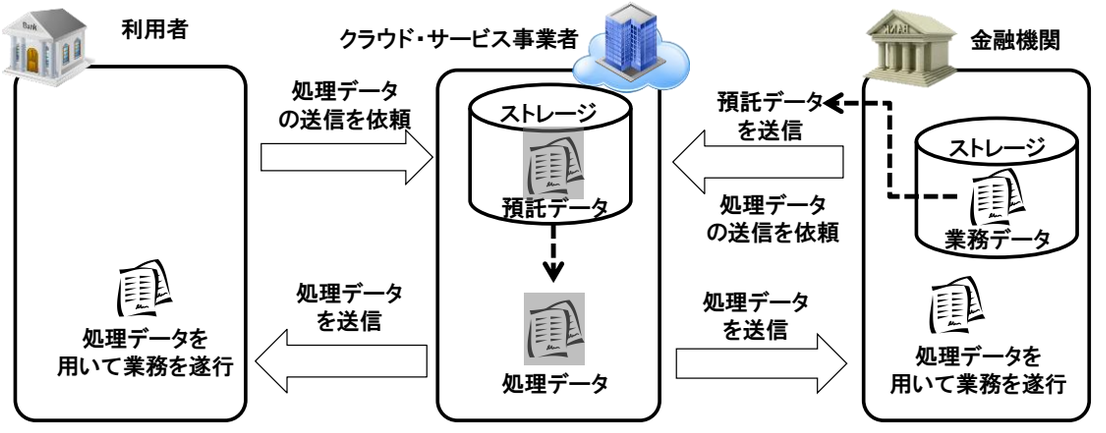
2. 金融分野において高機能暗号を適用しうる 2 つのモデル

金融分野における高機能暗号の主な利用形態として、金融機関が、①高機能暗号を実装したクラウド・サービスにおいて、既存の業務にかかる各種の情報処理をアウトソース化するケースと、②TPPs による新しい金融サービスにおいて高機能暗号を導入するケースが考えられる。本節では、まず、これらのケースの前提となる 2 つのモデルを設定する。

（1）クラウド・サービス利用モデル

クラウド・サービス利用モデルは、「金融機関が、外部のクラウド・サービス（のサーバ等の資源）を利用して自社の業務（の一部）を実現する」という状況を抽象化したものである（図表 1）[3]。

図表 1. クラウド・サービス利用モデル



[2] 共通鍵暗号型の機能や安全性等の詳細については、清藤・四方［2014］、太田［2017］、芦原・清藤［2017］を参照。

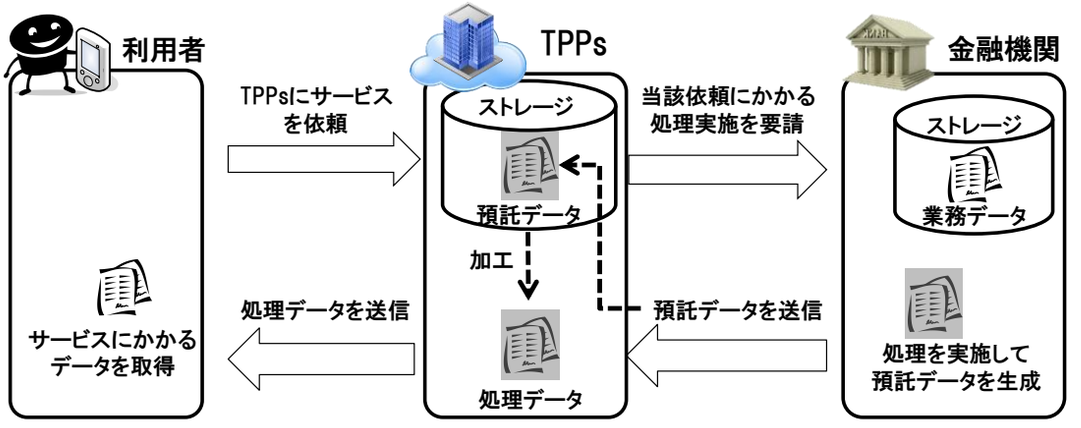
[3] 本稿で想定するクラウド・サービス利用モデルは、金融分野だけでなく他分野におけるクラウド・サービスの利用形態も包含する。

当該モデルを構成するエンティティは、「金融機関」、「利用者」、「クラウド・サービス事業者」である。まず、金融機関は、クラウド・サービスを利用して実現する業務に関するデータ（以下、「業務データ」と呼ぶ）を生成・保有するとともに、業務データをクラウド・サービス事業者に預託する（以下、預託するために一定の処理を施したデータを「預託データ」と呼ぶ）。利用者は、金融機関と連携して当該業務を遂行する。その際、クラウド・サービス事業者にアクセスして、当該データに一定の処理を施したデータ（以下、「処理データ」と呼ぶ）を入手する。金融機関が利用者となる場合があるほか、金融機関と同一の企業グループに属する企業等、当該業務に関与する主体が利用者となることもありうる。クラウド・サービス事業者は、金融機関から預託データを受信し、ストレージ上に保管して管理するとともに、金融機関や利用者の依頼に応じて当該預託データを処理し、その結果を処理データとして提供する。業務データには、当該業務の関係者以外には開示できない機密性の高いデータが含まれるものとする。

（２）TPPs 利用モデル

TPPs 利用モデルは、「TPPs が顧客の依頼に応じて（当該顧客の取引先の）金融機関にアクセスし、当該依頼に基づく各種処理を金融機関に依頼するとともに、その結果となるデータを金融機関から受信・処理して顧客に提供する」というサービスを抽象化したものである（図表 2)。例としては、TPPs が利用者に代わって金融取引にかかるデータ（口座残高や送金履歴等）を収集・加工して当該利用者に提供する口座情報サービス（Account Information Service）や、利用者が送金等の決済指図を TPPs のアプリケーション・プログラムを介して金融機関に伝達し、その結果を受信する決済指図伝達サービス（Payment Initiation

図表 2. TPPs 利用モデル



Service）等が挙げられる（European Commission [2015]）[4]。

当該モデルを構成するエンティティは、「金融機関」、「利用者」、「TPPs」である。金融機関は、利用者との金融取引において生成した「業務データ」を保管するとともに、利用者やTPPsからの依頼に基づいて各種処理を実行し、当該処理によって生成されるデータを「預託データ」としてTPPsに送信する[5]。利用者は、金融機関の顧客であり、TPPsが提供するサービスを利用する。その際、金融機関やTPPsと通信してサービスに関する依頼事項等を送信するとともに、その結果に関するデータ（処理データ）をTPPsから受信する。TPPsは、利用者からサービスの依頼を受信した後、金融機関に対して当該依頼にかかる処理の実施を要請し、当該処理の結果となる預託データを金融機関から受信・保管する[6]。また、当該預託データを加工するなどして処理データを生成し、利用者に送信する。業務データには、個人の金融取引に関する情報等、当該業務の関係者以外には開示できない機密性の高いデータが含まれているものとする。

（３）従来の暗号を利用した対策の限界

上記のモデルにおいては、マルウェア感染等によって、クラウド・サービス事業者やTPPsのシステムが取り扱うデータが外部に流出するというリスクが存在する。こうしたリスクへの対策として、業務データを暗号化してクラウド・サービス事業者等に送信することが考えられる。その際、基本的な暗号機能（業務データの暗号化や復号）のみを実現する（AESやRSA等の）既存の暗号を利用することがまず想定される。具体的には、金融機関が、暗号化鍵によって業務データを暗号化して預託データ（または処理データ）を生成し、クラウド・サービス事業者やTPPsに送信するというものである。この方法は、金融機関や利用者がクラウド・サービス事業者等に業務データの保管や転送のみを依頼する場合であれば有効といえる。しかし、利用者がクラウド・サービス事業者等に預託データに対する各種処理（キーワード検索や統計解析等）を依頼する場合、暗号化されたままでは当該処理を実施できない。そのため、利用者は、クラウド・サービス事業者等に対して預託データの復号を許可する必要がある。その結果、クラウド・サービス事業者等が（平文の）業務データを取り扱うこ

[4] 口座情報サービスは「参照・照会系」と呼ばれるサービスの1つであり、決済指図伝達サービスは「更新・実行系」と呼ばれるサービスの1つである（全国銀行協会［2016］）。

[5] 例えば、金融機関のAPI（Application Programming Interface）を通じてTPPsに提供するデータの制御（認証と認可）に関しては、「OpenID Connect」等のプロトコルが利用されるケースが多い（中村［2016］）。

[6] 一般に、口座情報サービスを提供するTPPsでは、利用者からアクセスを許可された金融機関より、口座残高や取引履歴等のデータを定期的に取得して自身のデータベースに保管し、利用者からの要求に応じて、これらのデータの加工等を行って利用者に送信する（マネーフォワード［2015］、Zaim［2015］等）。

ととなり、上記のリスクが発生する。

また、既存の暗号を利用する場合には、金融機関や利用者における暗号鍵と復号鍵の管理にかかる負担が大きくなるという課題もある。特に、TPPs 利用モデルにおいては、特定の利用者の金融取引にかかるデータを他の利用者が閲覧できないようにするために、利用者ごとに異なる暗号鍵と復号鍵を準備することになる。その結果、それらの管理にかかる負担が増加するほか、暗号化処理にかかる計算量や TPPs 等との通信量も増加する。

３．主な３つの高機能暗号の機能と安全性

本節では、既存の主な公開鍵暗号型の高機能暗号（補論 1 を参照）のうち、近年、特に研究や実用化に向けた動きが活発化している「検索可能暗号[7]」、「属性ベース暗号」、「準同型暗号」に着目し、それらが実現する機能および安全性等について説明する。特に、ここでは、2 節で定義したクラウド・サービス利用モデルおよび TPPs 利用モデルへの適用について検討するために、「登録者」、「利用者」、「外部サーバ」の 3 つのエンティティから構成されるモデルを想定する。

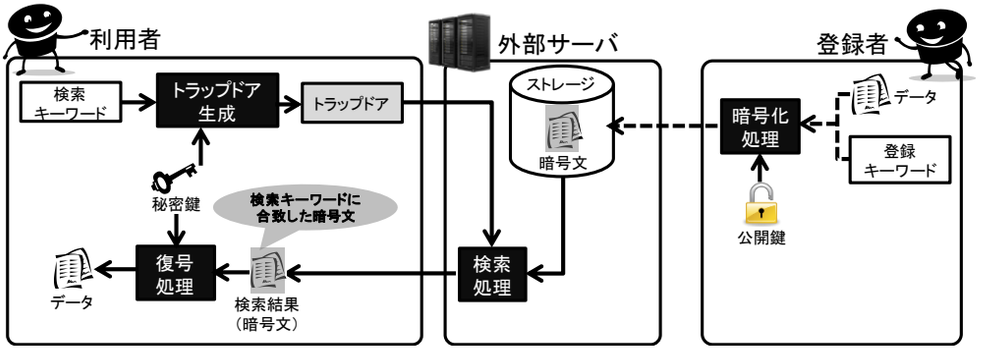
（１）検索可能暗号

イ．機能と特徴

検索可能暗号では、暗号化したデータ（以下、「暗号文」と呼ぶ）に、当該データに関連するキーワード（以下、「登録キーワード」と呼ぶ）を埋め込むことにより、データを暗号化したままキーワード検索を実行できる。検索処理時に指定するキーワード（以下、「検索キーワード」と呼ぶ）も暗号化したままでよい。

検索可能暗号のモデル（図表 3）において、登録者は、データや登録キーワードの暗号化に用いる「公開鍵」と、暗号文のキーワード検索および復号に用い

図表 3. 検索可能暗号のモデル（イメージ）



[7] 「秘匿検索暗号」と呼ばれる場合もある。

る「秘密鍵[8]」を生成し、秘密鍵を利用者に安全に配付するとともに、公開鍵は他のエンティティに公開する。そのうえで、預託するデータに関連する登録キーワードを選択した後、公開鍵を用いて登録キーワードを組み込んだデータの暗号文を生成し、外部サーバに送信する。利用者は、検索キーワードを選択した後、秘密鍵を用いて当該検索キーワードを変換し、そのデータ（以下、「トラップドア」と呼ぶ）をサーバに送信する。利用者は、検索結果として当該検索キーワードに合致した暗号文を受信し、秘密鍵を用いて復号する。外部サーバは、登録者から送信された暗号文をストレージに保管するとともに、利用者からの要求に応じて検索処理を行い、検索キーワードと同一の登録キーワードを含む暗号文を送信する。

ロ．研究開発の動向

公開鍵暗号型の検索可能暗号[9]が提案された当初は、キーワードが完全に一致しているか否かを検索する「完全一致検索」を実現する方式のみが提案された（Boneh *et al.* [2004]等）。その後、各種の検索機能を実現する方式が提案され、①キーワードの一部が一致するものの検索（「部分一致検索」、Kawai *et al.* [2015]等）、②キーワードの文字列と類似したものの検索（「類似検索」、Dong *et al.* [2013]等）、③複数個のキーワードから構成される検索条件に合致するものの検索（「AND（論理積）検索」、「OR（論理和）検索」、「NOT（否定）検索」[10]、Katz, Sahai, and Waters [2013]や Lv *et al*. [2014]等）といった、より高度な検索機能を実現する方式の研究が進められている。

また、近年では、クラウド・サービスでの利用を想定した製品開発が活発化している。例えば、リレーショナル・データベース上のデータを暗号化したままキーワード検索処理等が可能な製品等の開発および実装の事例が発表されている（NEC［2013］）。また、完全一致検索および部分一致検索が可能な製品等の開発および実証の事例も知られている（富士通研究所［2014］、三菱電機［2013、2016］）。

---

[8] 一般に、検索可能暗号は、従来の暗号（RSA 暗号や AES 等）を併用することが前提であり、データ自体の暗号化については従来の暗号を用いて行われる。本稿では、モデルを単純化するために、検索可能暗号のみでデータと登録／検索キーワードの暗号化を行うモデルを想定する。

[9] 検索可能暗号には、共通鍵暗号型の方式も存在する（Curtmola *et al* [2006]等）。共通鍵暗号型は、データおよび登録キーワードの暗号化に用いる鍵とトラップドアの生成およびデータの復号に用いる鍵が同一となり、当事者間で事前に鍵を安全に共有する必要がある。一般に、共通鍵暗号型は公開鍵暗号型よりも処理速度が高速であるため、例えば、ビッグデータ解析等のように取り扱うデータ数が多いケースでの利用に適すると考えられる。

[10] AND 検索は複数の検索キーワード全てに一致するもの、OR 検索は複数のキーワードのどれか 1 つに一致するもの、NOT 検索はキーワードに一致しないものを検索する機能である。

ハ．脅威と安全性要件

一般に、外部サーバに暗号文の保管・検索処理を委託するケースにおいて、当該エンティティと同程度の情報（公開鍵、預託された全ての暗号文およびトラップドア）を有する攻撃者が想定される。そのうえで、データおよび登録キーワードの機密性と完全性を確保するための安全性要件が設定されている。具体的には、想定する攻撃者に対して「データが漏えいしない（安全性要件 1）」、「暗号化された業務データを意味のある異なる内容に書換えできない[11]（安全性要件 2）」、「登録キーワードが漏えいしない（安全性要件 3）」が主な安全性要件として設定されることが多い。

外部サーバに対して、検索キーワードに一致したものがあったか否かについての情報が漏えいすることも想定される。すなわち、攻撃者が検索キーワードそのものを入手できれば、暗号文の中でそれに一致するものがあるか否かの情報を得るという攻撃が可能となる。これを防止するために、攻撃者に対して「検索キーワードが漏えいしない（安全性要件 4）」も安全性要件として想定される。また、複数のトラップドアが同一か否かを識別できる場合、攻撃者はその利用頻繁を知ることができる。こうした情報を用いると、例えば、他の検索サービス等における頻度情報を参考に、検索キーワードを推測する攻撃（「頻度攻撃」と呼ばれる）が可能となる。これを防ぐために、「2 つのトラップドアが同一の検索キーワードに対応しているか否かの情報が漏えいしない（安全性要件 5）」ことが安全性要件として設定されることが多い。

（２）属性ベース暗号

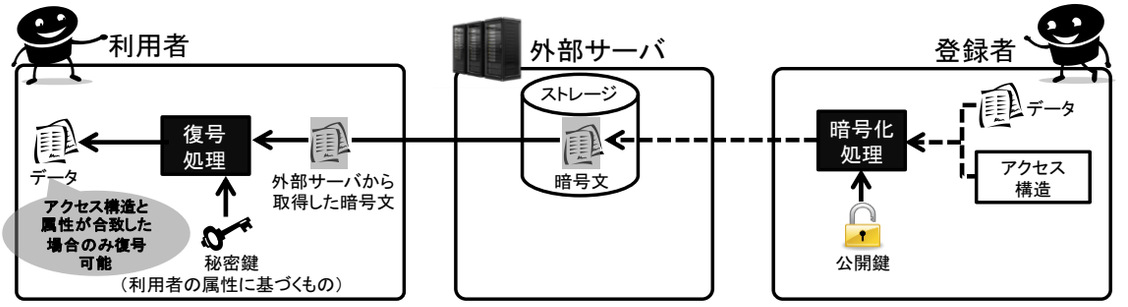
イ．機能と特徴

属性ベース暗号は、暗号文や秘密鍵に「アクセス構造」と呼ばれるデータを埋め込むことにより、暗号文を復号するエンティティを制御できる。アクセス構造とは、暗号文を復号する権限を有するエンティティの属性情報（例えば、役職、所属部署）の組合せで表現される条件文（例えば、「総務部かつ課長」や「課長または部長」）や、エンティティに復号を許可する暗号文の属性情報（例えば、邦画、アニメ）の組合せで表現される条件文（例えば、「邦画かつアニメ」や「アニメまたは SF」）である。属性ベース暗号では、エンティティと暗号文との関係がアクセス構造と合致する場合にのみ、当該エンティティは暗号文を復号できる。

属性ベース暗号は、アクセス構造を暗号文に組み込む「暗号文ポリシー型」

[11] この安全性要件は、「頑強性（Non-Malleability）」と呼ばれるものであり、厳密には「攻撃者が、あるデータの暗号文から、ある関係（例えば、復号結果がともに口座情報として取り扱われる）を満たす別のデータの暗号文を生成できないこと」を意味する（Dolev, Dwork, and Naor [1991] 等）。

図表 4. 属性ベース暗号（暗号文ポリシー型）のモデル（イメージ）



と、利用者の秘密鍵に組み込む「鍵ポリシー型」に分類される。一般に、アクセス構造の組込みは、更新の頻度が相対的に少ない情報に関して実施することが処理効率の観点から望ましい。例えば、クラウド・サービスを介してさまざまな受信者とデータを共有したい場合において、共有対象となるデータの更新頻度が相対的に少ないときは、暗号文ポリシー型が望ましい。他方、有料放送における暗号化された映像コンテンツの配信等、多様なデータを頻繁に暗号化して配付する場合において、各利用者の秘密鍵に組み込むアクセス構造の更新頻度が相対的に少ないときは、鍵ポリシー型が望ましい。

従来の暗号を利用して暗号文を復号するエンティティを制御する場合、暗号文の生成は、復号を許可するエンティティごとに、当該エンティティに配付する秘密鍵に対応した公開鍵をそれぞれ用いて行うこととなる。他方、暗号文ポリシー型の属性ベース暗号を利用する場合、復号を許可するエンティティの属性情報を表現するアクセス構造を組み込んだ暗号文を 1 つ生成すればよく、暗号化に要する手間や暗号文を保管するストレージを削減できるというメリットがある。

以下では、暗号文ポリシー型のモデルを説明する。属性ベース暗号のモデル（図表 4）において、登録者は、外部サーバを介して利用者とデータを共有するために、当該外部サーバに預託するデータ（アクセス構造を組み込んだ暗号文）を生成する。また、公開鍵と、当該公開鍵に対応する秘密鍵を各利用者の属性に応じてそれぞれ生成したうえで、各利用者にそれぞれ対応する秘密鍵を安全に配付するとともに、公開鍵は他のエンティティに公開する。利用者は、外部サーバから取得したい暗号文を受信し、秘密鍵を用いて復号する。利用者の属性とアクセス構造が合致する場合にのみ、データを復号できる。外部サーバは、登録者から送信された暗号文をストレージに保管するとともに、利用者からの要求に応じて暗号文を送信する。

ロ．研究開発の動向

暗号文ポリシー型の方式と鍵ポリシー型の方式がそれぞれ提案された当初は、属性を「論理積（AND）」と「論理和（OR）」で組み合わせた単純なアクセス構造（例えば、「課長 AND 総務部」や「（課長 OR 部長）AND（総務部）」）のみ設定可能であった[12]。その後、「否定（NOT）」を組み合わせたより複雑な条件式（例えば、「（課長 OR 部長）AND（NOT 総務部）」）を設定可能な方式が提案されているほか、設定できる属性の種類や個数等の制約を緩める研究も進められている[13]。

また、従来は、利用者の属性が所属部署の変更等により変化した場合、それに応じてアクセス構造を再定義したうえで、データの暗号化（暗号文ポリシー型）や秘密鍵の生成（鍵ポリシー型）を新たに行う必要があった。最近では、データの暗号化や秘密鍵の生成を新たに行わずに、既存の暗号文や秘密鍵に設定されているアクセス構造を効率的に変更可能な方式が提案されている（Attrapadung and Imai [2009] 、Sahai, Seyalioglu, and Waters [2012]等）。

実用化動向については、最近、クラウド・サービスを利用したファイル交換サービスに属性ベース暗号を用いてアクセス制御機能を実現するソリューションが提供されている（三菱電機ビジネスソリューションズ［2016］）。

ハ．脅威と安全性要件

アクセス構造と属性が一致しないエンティティは当該データを復号できないことが求められる。そのため、こうしたエンティティや外部サーバを攻撃者として想定したうえで、データの機密性と完全性を確保するために、本節（１）ハ．で示した安全性要件１と安全性要件２が設定されることが多い[14]。

（３）準同型暗号

イ．機能と特徴

準同型暗号は、データを暗号化したまま一定の演算処理（加算や乗算）を実

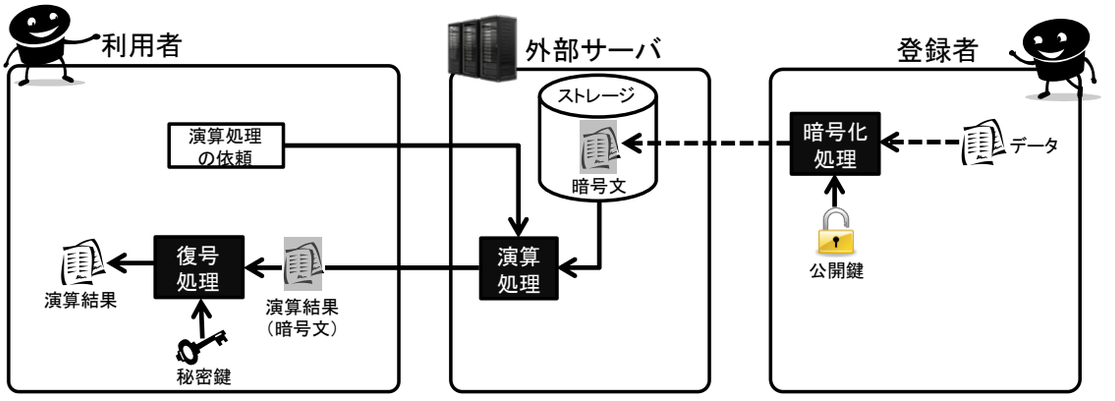
---

[12] 暗号文ポリシー型の代表的な方式として、Bethencourt, Sahai, and Waters [2007]、Waters [2011]、Rouselakis and Waters [2013]、鍵ポリシー型の代表的な方式として、Sahai and Waters [2005]、Goyal *et al.* [2006]、Rouselakis and Waters [2013]がある。

[13] 暗号文ポリシー型では、代表的な方式として、Goyal *et al.* [2008]、Okamoto and Takashima [2008]、Lewko *et al.* [2010]、Attrapadung, Hanaoka, and Yamada [2015]、Attrapadung and Yamada [2015]、鍵ポリシー型では、代表的な方式として、Ostrovsky, Sahai, and Waters [2007]、Lewko *et al.* [2007]、Okamoto and Takashima [2010]、Lewko *et al.* [2010]、Hohenberger and Waters [2013]、Gorbunov, Vaikuntanathan, and Wee [2015]、 Attrapadung, Hanaoka, and Yamada [2015]、Brakerski and Vaikuntanathan [2016]がある。

[14] 属性ベース暗号においては、安全性要件 1 のみを満たす方式を、安全性要件 1 と 2 をともに満たす方式に変換する手法が提案されている（Yamada *et al.* [2011]）。そのため、これまでに提案されている属性ベース暗号の多くは安全性要件 1 と 2 をともに満たすといえる。

図表 5. 準同型暗号のモデル（イメージ）



行できる。例えば「38」というデータの暗号文と、「62」というデータの暗号文を加算して得られた暗号文を復号すると、「100」というデータが得られる。これを利用することにより、金融機関は暗号文のままで統計解析等をクラウド・サービス事業者にアウトソース化することができると期待される。

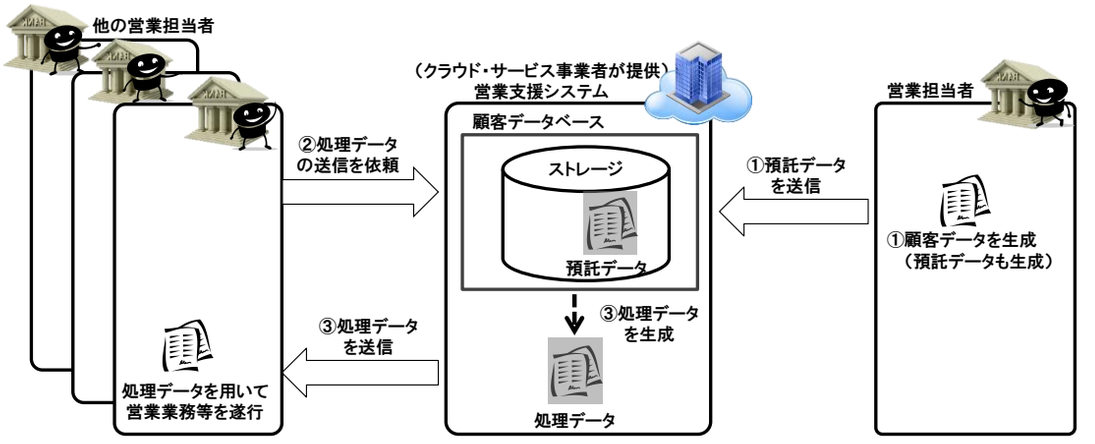
準同型暗号のモデル（図表 5）において、登録者は、公開鍵と秘密鍵を生成し、利用者に秘密鍵を安全に配付するほか、公開鍵は他のエンティティに公開する。また、外部サーバに預託するデータ（暗号文）を生成する。利用者は、外部サーバに対して暗号文への演算処理を要求し、その処理結果（暗号文）を受信した後、秘密鍵を用いて復号する。外部サーバは、登録者から送信された暗号文をストレージに保管するとともに、利用者からの要求に応じて暗号文に対する演算処理を行い、その結果を送信する。

ロ．研究開発の動向

データを暗号化したまま演算するというアイデアは 1970 年代から知られていた（Rivest, Adleman, and Dertouzos [1978]）。当初は、乗算または加算の一方のみを演算可能な方式（以下、「単一演算型」と呼ぶ）が提案されており、統計解析等の複雑な演算を実現するのは困難であった。その後、加算と回数制限のある乗算が可能な方式が提案された後（Boneh, Goh, and Nissim [2005]）、2009 年に乗算と加算の両方を回数に制限なく演算できる方式（以下、「完全型」と呼ぶ）が発表された（Gentry [2009]）。完全型については、処理速度が単一演算型と比較して遅いことが実用上の課題となっており、処理の高速化を目的とした研究が行われている（Gentry, Sahai, and Waters [2013]等）。このほか、一般的な準同型暗号では、同じ公開鍵を用いて生成した暗号文同士の演算のみ可能であったが、近年、異なる公開鍵による暗号文同士の演算も可能な方式が提案されている（López-Alt, Tromer, and Vaikuntanathan [2012]、Brakerski and Perlman [2016]等）。

実用化動向としては、前述のとおり、統計解析等をクラウド・サービス事業

図表 6. 営業支援システムへの高機能暗号の適用例（イメージ）



者にアウトソース化することを企図した研究開発が知られている（富士通研究所［2013］、情報通信研究機構［2016］等）。

ハ．脅威と安全性要件

外部サーバに暗号文の保管および演算処理を委託するケースにおいては、当該エンティティと同程度の情報（公開鍵、預託された全ての暗号文）を有する攻撃者に対してデータの機密性を確保するために、本節（１）ハ．で示した安全性要件１が設定されることが多い。データの完全性に関する安全性要件２に関しては、暗号文への正当な演算処理と、攻撃者による不正な演算処理を識別困難であることから原理的に満たされない。学界では、この課題を解決するための研究も盛んに行われている（Gennaro, Gentry, and Parno [2010]、Fiore, Gennaro, and Pastro [2014]等）。

４．２つのモデルへの高機能暗号の適用に関する考察

本節では、2 節で定義したクラウド・サービス利用モデルと TPPs 利用モデルへの高機能暗号の適用について検討し、各モデルにおいて高機能暗号が果たしうる役割（期待される効果や安全性等）について考察する。

（１）クラウド・サービス利用モデルへの適用

イ．想定される高機能暗号の適用例

クラウド・サービス利用モデルに高機能暗号を適用する例として、検索可能暗号、属性ベース暗号、準同型暗号をそれぞれ適用した「（クラウド・サービス

図表 7. 営業支援システムに高機能暗号を適用する目的と期待される効果

高機能暗号	目的	期待される効果
検索可能暗号	営業担当者が、顧客データベース上で、預託データを復号しないでそのままキーワード検索を実行すること。	・ キーワード検索を可能とするという意味で、営業担当者の利便性を向上させる。 ・ クラウド・サービス事業者からの情報漏えいリスクが軽減される（鍵管理によって制御）。
属性ベース暗号	顧客データへのアクセスを暗号（アクセス構造が埋め込まれる）によって制御すること。	・ 顧客データを共有する際の鍵管理や暗号処理に要するコストが軽減される。 ・ クラウド・サービス事業者からの情報漏えいリスクが軽減される（鍵管理によって制御）。
準同型暗号	預託データを暗号化したまま統計解析等をクラウド・サービス事業者に委託すること。	・ 顧客データの演算処理を可能とするという意味で、営業担当者の利便性が向上する。 ・ クラウド・サービス事業者からの情報漏えいリスクが軽減される（鍵管理によって制御）。

事業者が提供する）営業支援システム」を想定する[15]（図表 6）。営業支援システムは、多くの金融機関によって利用されている情報系システム[16]の 1 つである。このシステムは、営業活動の効率性向上を企図して、営業担当者が保有する顧客情報や営業の進捗状況等に関する情報をデータベースに蓄積・管理し、必要に応じて共有するものである（金融情報システムセンター［2015］）。ここでの営業支援システムは、金融機関の営業担当者が、顧客データ等を随時生成し、クラウド・サービス事業者のデータベース（以下、「顧客データベース」と呼ぶ）に預託するとともに、それらを他の営業担当者と当該データベースを通じて活用することを実現するシステムとする。

上記の営業支援システムに高機能暗号を適用する目的、および期待される効果を図表 7 にまとめる。高機能暗号を利用することにより、クラウド・サービス事業者からの情報漏えいリスクを軽減しつつ、営業担当者の利便性の向上（利用できる機能の追加や鍵管理等のコスト軽減）が期待される。

各暗号を適用する際の各エンティティにおける処理の概要を図表 8 にまとめる（各処理の詳細については、補論２（１）を参照）。

---

[15] 検索可能暗号は、属性ベース暗号や準同型暗号と組み合せて適用できる。例えば、営業担当者は、クラウド・サービスを利用して、顧客データベース上の預託データについて、検索処理を行って絞り込んだうえで、復号しないでそのまま、特定の営業担当者と共有したり（検索可能暗号と属性ベース暗号の組合せ）、分析を委託したり（検索可能暗号と準同型暗号の組合せ）することが可能となる。検索可能暗号における顧客データの暗号化自体は既存の暗号（RSA 暗号等）を用いて行われるため、これの代わりに属性ベース暗号や準同型暗号を利用することで、組み合わせて利用することができる。一方、属性ベース暗号と準同型暗号は、それぞれが顧客データの暗号化に関わる処理を行うため、両者を組み合わせることは、現時点では困難と考えられる。

[16] 情報系システムは、金融機関における預金・為替・融資等の勘定処理業務以外の各種業務に資することを目的として、データ分析や共有を行うことを目的としているシステムである（金融情報システムセンター［2015］）。

図表 8. 営業支援システムにおける各エンティティにおける処理の概要

高機能暗号	各エンティティにおける処理		
	①営業担当者による鍵生成[17]と預託データの生成	②営業担当者による依頼	③営業支援システムによる処理データの生成と送信
検索可能暗号	・顧客データの共有を受ける各営業担当者は、公開鍵と秘密鍵を生成。公開鍵は顧客データを預託する全営業担当者に公開し、秘密鍵は自身で安全に保管。 ・顧客データを預託する営業担当者は、顧客データと登録キーワードを、顧客データの共有を受ける各営業担当者が公開鍵を用いて暗号化し、預託データとして営業支援システムに送信。	顧客データの共有を受ける営業担当者は、検索キーワードから、自分の秘密鍵を用いてトラップドアを生成し、営業支援システムに送信。	顧客データの共有を受ける営業担当者からの依頼に応じて預託データを検索し、検索条件に合致したものを処理データとして当該営業担当者に送信。
属性ベース暗号	・1 つの公開鍵と、顧客データの共有を受ける各営業担当者の属性に応じた秘密鍵（個数は属性のバリエーションに依存）を生成。公開鍵はデータを預託する全営業担当者に公開し、秘密鍵は、顧客データの共有を受ける各営業担当者が自身で安全に保管。 ・データを預託する営業担当者は、顧客データの共有を受ける営業担当者の属性に基づいてアクセス構造を設定した後、顧客データを、公開鍵によって当該アクセス構造を組み込んで暗号化し、預託データとして営業支援システムに送信。	顧客データの共有を受ける営業担当者は、営業支援システムに預託データの送信を依頼。	顧客データの共有を受ける営業担当者からの依頼に応じて預託データを処理データとして送信。
準同型暗号	・顧客データの共有を受ける各営業担当者は、公開鍵と秘密鍵を生成。公開鍵は顧客データを預託する全営業担当者に公開し、秘密鍵は自身で安全に保管する。 ・データを預託する営業担当者は、顧客データを、顧客データの共有を受ける各営業担当者の公開鍵を用いて暗号化し、預託データとして営業支援システムに送信。	顧客データの共有を受ける営業担当者は、営業支援システムに預託データの統計解析等を依頼。	顧客データの共有を受ける営業担当者からの依頼に応じて預託データの統計解析等を行い、その結果を処理データとして当該営業担当者に送信。

ロ. 脅威・リスクおよび安全性

営業支援システムにおける攻撃者は、全営業担当者（登録者および利用者に相当）以外のエンティティとし[18]、クラウド・サービス事業者の内部者の一部と

[17] 本稿では、モデルを単純化するため、検索可能暗号と準同型暗号については、営業担当者が鍵生成を行う処理フローを想定するが、例えば、当該営業担当者が所属する金融機関のシステム担当部署が鍵生成等を行う場合もありうる。

[18] 本稿は、金融機関がクラウド・サービス事業者に業務の一部をアウトソース化する際の安全性について考察することを主な目的としている。そのため、営業担当者が利用する端末および所属する組織内の情報システムやネットワーク機器に関して、不正侵入の防止・検知対策や当該環境内で処理される業務データの厳密な管理が実施されているとする。

図表 9. 営業支援システムにおける主な脅威・リスクと安全性要件

主な脅威	攻撃方法	安全性に関するリスク	安全性要件
クラウド・サービス事業者への攻撃	ネットワーク機器等の脆弱性を悪用し、営業支援システムへの侵入を試行する。	顧客データが外部に流出する、あるいは、改ざんされるリスク。	・顧客データが漏えいしない（安全性要件 A-1）。 ・暗号化された顧客データを意味のある異なる内容に書換えできない（安全性要件 A-2）。
通信路上での攻撃	当該通信路において、顧客データの盗聴や改ざんを試行する。	顧客データが通信路上で盗聴される、あるいは、改ざんされるリスク。	

結託する場合も想定する。主な脅威としては、クラウド・サービス事業者への攻撃と、各エンティティ間を接続する通信路上での攻撃[19]が想定される。各攻撃対象において起こりうる攻撃方法とリスク、および安全性要件は、図表 9 のとおりである。

各暗号において、顧客データの機密性（安全性要件 A-1）と完全性（安全性要件 A-2）が満たされるか否かを評価すると（評価の詳細は補論 2 を参照）、準同型暗号においては、安全性要件 A-1 が満たされるものの、安全性要件 A-2（完全性にかかる要件）が満たされない。検索可能暗号と属性ベース暗号については、両要件がともに満たされる。営業支援システムにおける顧客データの保管時やエンティティ間での送受信時に顧客データが改ざんされたとしても、準同型暗号のみではそれを検知困難であるといえる。暗号化された顧客データ（預託データ）の完全性を確保するために、例えば、営業担当者が改ざんの有無を適宜検証できる仕組み[20]（Fiore, Gennaro, and Pastro [2014]等）の併用等が考えられる。

ハ. コストにかかる評価

ここでは、N+1 人の営業担当者が存在し、ある営業担当者が他の N 人の営業担当者と一定のサイズの顧客データを共有する際に必要となるコストを考える。その際、このコストを左右する主なパラメータは「公開鍵の個数」、「顧客データの暗号化処理の回数」、「公開鍵のサイズ」、「暗号化した顧客データ（預託データ）のサイズ」であり、これらを評価項目とする。

---

[19] 本稿では、高機能暗号を適用した際の安全性に関する議論を整理しやすくするために各エンティティ間において相手認証は適切に行われており、「第三者によるなりすまし」は行われないものとする（TPPs 利用モデルにおいても同様）。

[20] 暗号化したまま演算したデータに対する認証子（データの完全性を保証するデータ）を、当該データを復号することなく生成するメッセージ認証方式（「準同型ハッシュ関数」と呼ばれる技術を利用した方式）により、意図したエンティティによりデータが演算されたことを利用者が検証できる仕組みである。

検索可能暗号においては、顧客データを預託する営業担当者は、顧客データの共有を受ける各営業担当者が生成した公開鍵で顧客データをそれぞれ暗号化する必要があるため、処理に要する公開鍵の個数と暗号化処理の回数は、ともに従来の暗号（RSA 暗号）と同じく N となる。公開鍵のサイズは、従来の暗号（RSA 暗号等）と同程度となるほか、預託データのサイズは、一般に、従来の暗号における暗号文のサイズに、登録キーワードの個数に比例するデータのサイズを加えたものとなり、従来の暗号における暗号文のサイズの高々数倍程度となると考えられる。

属性ベース暗号について、仮に従来の暗号を用いて N 人の営業担当者と顧客データを共有する場合、公開鍵の個数と暗号化処理の回数は N となる一方、属性ベース暗号を適用した場合は、顧客データの共有を受ける営業担当者の属性（アクセス構造）を暗号文に組み込むことで暗号文を復号可能な営業担当者の範囲を制御できる。そのため、公開鍵の個数と暗号化処理の回数はともに 1 となる。公開鍵のサイズと預託データのサイズは、一般に、少なくとも従来の暗号の場合の数倍程度のサイズに留まると考えられる。

準同型暗号においては、顧客データを預託する営業担当者は、顧客データの演算処理結果の共有を受ける各営業担当者が生成した公開鍵で顧客データをそれぞれ暗号化する必要があるため、公開鍵の個数と暗号化処理の回数は従来の暗号と同じく N となる。公開鍵のサイズと預託データのサイズは、実現できる演算の種類により異なる。乗算または加算のどちらか一方のみを演算可能な単一演算型の方式を利用する場合、一般に、公開鍵のサイズと預託データのサイズは従来の暗号と同程度のサイズとなる。一方、乗算と加算の両方を演算可能な完全型の方式を利用する場合は、公開鍵のサイズと預託データのサイズは、一般に、少なくとも従来の暗号の場合の数百倍から数千倍のサイズとなると考えられる[21]。

（２）TPPs 利用モデルへの適用

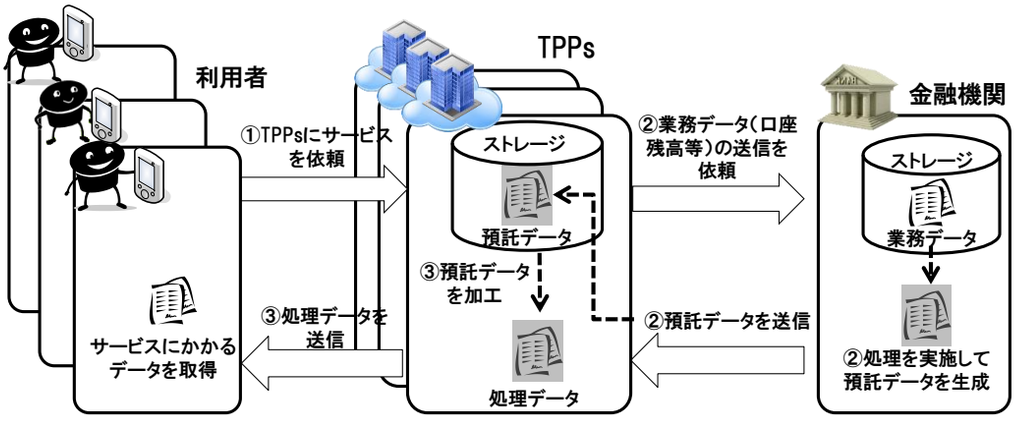
イ．想定される高機能暗号の適用例

２節（３）で説明した TPPs 利用モデルに高機能暗号を適用するケース、として検索可能暗号、属性ベース暗号、準同型暗号をそれぞれ適用した「口座情報サービス[22]」を想定する（図表 10）。口座情報サービスでは、準備として、高機能暗号用の公開鍵や秘密鍵の生成・配付を行ったうえで、①利用者（金融機関

[21] 近年、これらのサイズを大幅に削減しうる準同型暗号が提案されており、活発に研究が行われている。ただし、安全性の観点において解決すべき課題が残っているため、今後の研究動向に注目する必要がある（詳細については、Peikert [2016]等を参照）。

[22] 口座情報サービスの概要については、本稿 2 節または European Commission [2015]や金融庁［2016］を参照。

図表 10. 口座情報サービスへの高機能暗号の適用例（イメージ）



の顧客）が TPPs にサービスを依頼し、②TPPs が金融機関から預託データ（暗号化された口座残高等）の収集を行うとともに、③預託データを加工して処理データを生成し、利用者に提供することとする。

上記の口座情報サービスに高機能暗号を適用する目的、および期待される効果を図表 11 にまとめる。高機能暗号を利用することにより、TPPs からの情報漏えいリスクを軽減しつつ、当該サービスの利便性の向上が期待される[23]。

図表 11. 口座情報サービスに高機能暗号を適用する目的と期待される効果

高機能暗号	目的	期待される効果
検索可能暗号	TPPs が預託データを復号しないでキーワード検索を実施すること[24]。	・ TPPs からの情報漏えいリスクが軽減される。 ・ 預託データを検索可能という意味で、利用者の利便性が向上する。
属性ベース暗号	金融機関が、各 TPPs にアクセスを許可する預託データの範囲等を効率的に制御すること[25]。	・ 金融機関が、預託データを復号できる TPPs を柔軟に設定できる。 ・ 金融機関が預託データを提供する際の鍵管理や暗号処理に要するコストを削減できる。
準同型暗号	TPPs が預託データを暗号化したまま統計解析等を実施すること。	・ TPPs からの情報漏えいリスクが軽減される。 ・ 預託データの統計解析等を実施可能という意味で、利用者の利便性が向上する。

[23] 営業支援システムの事例と同様に、検索可能暗号と属性ベース暗号、準同型暗号を組み合せて適用することも考えられる。例えば、預託データを検索キーワードによって絞り込んだうえで、準同型暗号の機能によって統計解析等を行う（検索可能暗号と準同型暗号の組合せ）ことが考えられる。

[24] 例えば、登録キーワードとして「取引の種類」や「取引の日付」等を設定し、当該期間内に実施された、特定の種類のデータのみを抽出するといった処理が可能になると考えられる。

[25] 属性ベース暗号により、TPPs が処理データへのアクセスを許可する利用者を効率的に制御することも想定される。例えば、複数の利用者が処理データを共有するサービスに利用することが考えられる。もっとも、現時点では、著者らの知る限り、こうしたサービスの提供事例は少ない。

図表 12. 口座情報サービスにおける各エンティティの処理の概要

高機能暗号	各エンティティにおける処理			
	（準備）鍵生成	①利用者による利用依頼	②金融機関による預託データの生成・送信	③TPPs による処理データの生成・送信
検索可能暗号	各利用者は、公開鍵と秘密鍵を生成。公開鍵は TPPs にデータを預託する金融機関に公開し、秘密鍵は自身が安全に保管。	検索キーワードから、自らが生成した秘密鍵を用いてトラップドアを生成し、TPPs に送信。	・ TPPs からの定期的な預託データ送信依頼を受けて、業務データと登録キーワードを、各利用者が生成した公開鍵を用い暗号化して、預託データを生成。 ・ TPPs に預託データを送信。	利用者からのトラップドアに応じて預託データを検索し、検索条件に合致したものを処理データとして、当該利用者に送信。
属性ベース暗号	金融機関は、1 つの公開鍵と、預託データの送信を受ける TPPs の属性ごとの秘密鍵（個数は属性のバリエーションに依存）を生成。公開鍵は公開し、秘密鍵は預託データの送信を受ける各 TPPs に安全に配付。	TPPs に処理データの送信を依頼。	・ 利用者からの依頼に応じた TPPS からの預託データ送信依頼を受けて、預託データの送信を受ける TPPs の属性をアクセス構造として設定した後、業務データを、公開鍵を用い、当該アクセス構造を組み込んで暗号化し、預託データを生成[26]。 ・ 預託データを TPPs に送信。	利用者からの依頼に応じて、金融機関に預託データの送信を依頼した後、当該データを受信。預託データを復号し業務データとした後、必要に応じ加工して処理データを生成し、利用者に送信[27]。
準同型暗号	各利用者は、公開鍵と秘密鍵を生成。公開鍵は TPPs にデータを預託する金融機関に公開し、秘密鍵は自身が安全に保管。	TPPs に預託データの統計解析等を依頼。	・ TPPs からの定期的な預託データ送信依頼を受けて、業務データを、各利用者が生成した公開鍵を用いて暗号化し、預託データを生成。 ・ TPPs に預託データを送信。	利用者からの依頼に応じて預託データの統計解析等を行い、その結果を処理データとして当該利用者に送信。

上記の各暗号をそれぞれ適用する際の各エンティティにおける処理の概要を図表 12 にまとめる（各処理の詳細は補論２（２）を参照）。

[26] この暗号化処理については、TPPs からの依頼の都度行うのではなく、アクセスを許可する TPPs の属性を設定したうえで予め暗号化して預託データを生成し、事前にストレージに保管しておくという方法も考えられる。この場合、TPPs からの依頼があれば、当該 TPPs の属性に合致する預託データを抽出して送信すればよい。

[27] 利用者へ処理データを送信する際、既存の暗号等を利用して安全性を確保する必要がある。

図表 13. 口座情報サービスにおける主な脅威・リスクと安全性要件

主な脅威	主な攻撃方法	安全性に関するリスク	安全性要件
TPPs への攻撃	ネットワーク機器等の脆弱性を悪用し、口座情報サービスを提供する情報システムへの侵入を試行する。	TPPs が保管する業務データが外部に流出する、あるいは、改ざんされるリスク。	・ 業務データが漏えいしない（安全性要件 B-1）。 ・ 暗号化された業務データを意味のある異なる内容に書換えできない（安全性要件 B-2）。
利用者への攻撃	利用者の端末にマルウェアを感染させるなどして、当該利用者が保管する情報（秘密鍵、業務データ等）の盗取を試行する。	利用者が保管する情報が外部に流出する、あるいは、改ざんされるリスク。	
通信路上での攻撃	当該通信路において、業務データの盗聴や改ざんを試行する。	業務データが通信路上で盗聴される、あるいは、改ざんされるリスク。	

ロ. 脅威・リスクおよび安全性

上記の口座情報サービスにおける攻撃者は、金融機関（登録者）以外のエンティティとするが[28]、TPPs の内部者の一部や利用者の一部と結託する場合も想定する。主な脅威としては、①TPPs への攻撃、②利用者への攻撃、③各エンティティ間を接続する通信路上での攻撃を想定する。各攻撃対象において起こりうる攻撃方法とリスク、および安全性要件は図表 13 のとおりである。

上記の各暗号について、顧客データの機密性（安全性要件 B-1）と完全性（安全性要件 B-2）が満たされているか否かを評価すると（評価の詳細は補論 2 を参照）、準同型暗号においては、安全性要件 B-1 が満たされるものの、安全性要件 B-2 が満たされない。検索可能暗号と属性ベース暗号においては両要件がともに満たされる。営業支援システムと同様に、準同型暗号を適用する際に預託データや処理データの完全性を確保するためには、改ざんの有無を適宜検知できる仕組み（Fiore, Gennaro, and Pastro [2014]等）を併用することが考えられる。

ハ. コストにかかる評価

ここでは、N_1 人の利用者と N_2 個の TPPs が存在する場合に、金融機関が各 TPPs に預託データを提供する際に必要となるコストを考える。このコストを左右する主なパラメータは「公開鍵の個数」、「（業務データの）暗号化処理の回数」、「公開鍵のサイズ」、「預託データのサイズ」であり、これらを評価項目とする。公開鍵のサイズと預託データのサイズについては、本節（1）ハ. の議論と同様であるため、ここでは省略する。

[28] 本稿は、利用者が TPPs の提供する口座情報サービスを利用する際の安全性について考察することを主な目的としている。そのため、金融機関の情報システムやネットワーク機器に関して、不正侵入への対策や、業務データの厳密な管理が実施されているものとして対象外とする。

検索可能暗号においては、金融機関は、各利用者が生成した公開鍵で業務データをそれぞれ暗号化する必要があるため、公開鍵の個数は従来の暗号（RSA 暗号等）と同様に N_1 となる。また、暗号化処理の回数は、全利用者の預託データ（各利用者の預託データ数を k とする）について一斉に暗号化処理を行う必要が生じた場合を想定すると、従来の暗号と同様に、$k \times N_1$ となると考えられる。

属性ベース暗号については、仮に従来の暗号を用いて預託データを生成する場合、公開鍵の個数、暗号化処理の回数ともに N_2 となる[29]一方、属性ベース暗号の場合は、業務データへのアクセスを許可する TPPs の属性をアクセス構造として設定することにより、公開鍵の個数は 1 となる。また、暗号化処理の回数は、最大で TPPs の属性のバリエーションの数となると考えられる（例えば、TPPs の属性が 3 種類あれば 3 回となる）。

準同型暗号においては、金融機関は、各利用者が生成した公開鍵で業務データをそれぞれ暗号化する必要があるため、公開鍵の個数は従来の暗号と同様に N_1 となる。また、暗号化処理の回数は、従来の暗号と同様に、全利用者の預託データ（ただし、各利用者の預託データ数は k とする）について一斉に暗号化処理を行う必要が生じた場合を想定すると、$k \times N_1$ となると考えられる。

（３）高機能暗号を適用する際の留意点

検索可能暗号を適用する際の留意点としては、検索処理の精度を保つために、業務データ（顧客データや口座残高等）の暗号化処理時の登録キーワードの設定を適切に行う必要があることが挙げられる。対策としては、例えば、業務データから登録キーワードを自動的に抽出する仕組みの利用が考えられる[30]。また、TPPs 利用モデルにおいては、暗号化した業務データを復号しないで統計解析等を実施することはできないという点に留意する必要がある。対策としては、準同型暗号との併用等が考えられる。

属性ベース暗号を適用する際の留意点としては、営業担当者や TPPs の属性が人事異動等により変化した場合、新しいアクセス構造に基づいて預託データ（または秘密鍵）を新たに生成する必要があることが挙げられる。最近では、既存の預託データ（または秘密鍵）に設定されているアクセス構造を効率的に変更する方式の研究が進められており、こうした方式の利用について検討すること

[29] 属性ベース暗号における暗号文へのアクセス制御と類似の機能は、OpenID Connect の認可の機能を利用することにより実現できる。ただし、業務データの暗号化や鍵管理については、OpenID Connect では従来の暗号の利用が前提となっており、暗号化や鍵管理にかかるコストは、従来の場合が当てはまる。

[30] 例えば、「重要」や「至急」等の単語を登録キーワードの候補として予めデータベースに登録しておき、業務データ内に当該単語が一度でも出現した場合に、登録キーワードとして設定する方法等が考えられる。

が考えられる（Attrapadung and Imai [2009]、Sahai, Seyalioglu, and Waters [2012]等）。

準同型暗号を適用する際の留意点としては、一般的な準同型暗号の場合、異なる営業担当者が（異なる公開鍵を用いて）生成した預託データ同士の演算ができないことが挙げられる。対策としては、異なる公開鍵で暗号化した顧客データ同士でも演算処理が可能な方式が提案されはじめており、今後、こうした方式の利用が考えられる（Brakerski and Perlman [2016][31]等）。

また、上記の高機能暗号を利用する際には、「ペアリング関数[32]」や「格子[33]」と呼ばれる数学的な仕組みを利用した演算が必要となる。そのため、金融機関、営業担当者や利用者の端末、クラウド・サービス管理者や TPPs の情報システムに当該演算を処理するための環境（ソフトウェア・ライブラリや専用ハードウェア等）を準備する必要がある。

５．おわりに

本稿では、既存の金融業務や新たな金融サービスの安全性と利便性を両立しうる公開鍵暗号型の高機能暗号に注目し、実現される機能や安全性について説明するとともに、既存の金融業務や新たな金融サービスを抽象化したモデルへの適用による効果や留意点等について考察を行った。

高機能暗号については、実用化に向けた研究開発が活発化している一方、従来の暗号と比較すると、一般に、暗号鍵（公開鍵、秘密鍵）や暗号文のサイズが大きいことや、暗号化処理に要する時間が長いことなど、技術的な面で多くの課題が残されている。特に、金融業務や金融サービスへの適用を想定した場合には、高機能暗号を実装したシステムの信頼性や処理性能を向上させることが必要と考えられる。現在の研究開発の動向を前提とすると、金融業務や金融サービスにおける活用については、まずは他の分野や業務において相応の実績を有するサービス事例から導入を開始するのが望ましいと考えられる。実装にあたっては、高機能暗号の処理に対応するために、新たなソフトウェア・ライブラリの導入等が必要となることから、既存のシステムを改修する必要が生じることとなる。したがって、改修に伴うコスト負担が発生するほか、信頼性や

[31] この方式は、①暗号化できるデータのサイズに制約があること、②暗号文のサイズが大きいこと、③暗号文を復号する際には、複数の秘密鍵が必要となること等が課題として残っており、今後の研究の進展に期待したい。

[32] ペアリング関数は、特殊な曲線（例えば、楕円曲線）上の点の加算を整数の乗算に変換する「双線形」と呼ばれる性質を有する関数である。

[33] 格子とは、「ベクトル空間上に規則正しく並んでいる点の集合」であり、点同士の四則演算を行うことが可能な性質を有する。

可用性の観点から問題が生じないかについて厳密に検証することも求められる。

こうした技術的な課題に加えて、相互運用性も確保する必要がある。すなわち、多くの金融機関、TPPs、利用者が高機能暗号を利用できる環境を整備するために高機能暗号にかかる標準化の推進も重要な課題であるといえる。

今後、金融分野における高機能暗号の活用によって、金融機関をはじめとする関係者がどのようなメリットを享受できるかについて、技術的な課題への対応状況等を踏まえながら検討を進めていくことが有用であろう。

以　上

参考文献

太田和夫、「共通鍵暗号による秘匿検索暗号のセキュリティ」、『日本銀行金融研究所ディスカッション・ペーパー・シリーズ』2017-J-05、日本銀行金融研究所、2017 年

芦原聡介・清藤武暢、「共通鍵暗号型の検索可能暗号の処理性能について」、『日本銀行金融研究所ディスカッション・ペーパー・シリーズ』2017-J-07、日本銀行金融研究所、2017 年

金融情報システムセンター、『平成 28 年版金融情報システム白書』、金融情報システムセンター、2015 年

――――、「平成 28 年度金融機関アンケート調査結果」、『金融情報システム』No.341、金融情報システムセンター、2016 年

金融庁、「金融制度ワーキング・グループ報告 ― オープン・イノベーションに向けた制度整備について ―」、2016 年

小暮淳・下山武司・安田雅哉、「暗号化したまま検索が可能な秘匿検索技術」、『電子情報通信学会誌』Vol.98、No.3、電子情報通信学会、2015 年、202-206 頁

情報通信研究機構、「暗号化したままデータを分類できるビッグデータ向け解析技術を開発」、2016 年

清藤武暢・四方順司、「高機能暗号を活用した情報漏えい対策『暗号化状態処理技術』の最新動向」、『金融研究』第 32 巻第 3 号、日本銀行金融研究所、2014 年、93～132 頁

全国銀行協会、「オープン API のあり方に関する全銀協の検討状況」、第 3 回金融審議会・金融制度ワーキング・グループ資料、2016 年

中村啓佑、「金融分野の TPPs と API のオープン化：セキュリティ上の留意点」、『日本銀行金融研究所ディスカッション・ペーパー・シリーズ』2016-J-14、日本銀行金融研究所、2016 年

富士通研究所、「世界初！暗号化したまま統計計算や生体認証等を可能とする準同型暗号の高速化技術を開発」、2013 年

――――、「暗号化したまま検索が可能な秘匿検索技術を開発」、2014 年

マネーフォワード、「家計簿『マネーフォワード』4 つの特徴」、2015 年

三菱電機、「『秘匿検索基盤ソフトウェア』を開発」、2013 年

――――、「『部分一致対策秘匿検索基盤ソフトウェア』を開発」、2016 年

三菱電機ソリューションズ、「関数型暗号とクラウドサービスを利用した機密情報ファイル交換サービス『パッケージプラス(R)トランスポーター』の提供開始」、2016 年

NEC、「NEC、世界初、データベースの情報を暗号化したまま処理できる秘匿計

算技術を開発」、2013 年
Zaim、「Zaim と金融機関の連携」、2015 年
Albrecht, Martin R, Rachel Player, and Sam Scott, “On the Concrete Hardness of Learning with Errors,” *Journal of Mathematical Cryptography*, 9(3), 2015, pp.169-203.
Attrapadung, Nuttapong, and Hideki Imai, “Attribute-Based Encryption Supporting Direct/Indirect Revocation Modes,” *Proceedings of Cryptography and Coding 2009*, LNCS 5921, Springer-Verlag, 2009, pp.278-300.
———, Goichiro Hanaoka, and Shota Yamada, “Conversions Among Several Classes of Predicate Encryption and Applications to ABE with Various Compactness Tradeoffs,” *Proceedings of ASIACRYPT2015*, LNCS 9452, Springer-Verlag, 2015, pp.191-208.
———, and Shota Yamada, “Duality in ABE: Converting Attribute Based Encryption for Dual Predicate and Dual Policy via Computational Encodings,” *Proceedings of CT-RSA2015*, LNCS 9048, Springer-Verlag, 2015, pp.87-105.
Baek, Joonsang, Reihaneh Safavi-Naini, and Willy Susilo, “Public Key Encryption with Keyword Search Revisited,” *Proceedings of International Conference on Computational Science and Its Application (ICCSA) 2008*, LNCS 5027, Springer-Verlag, 2008, pp.1249-1259.
Bethencourt, John, Amit Sahai, and Brent Waters, “Ciphertext-Policy Attribute-Based Encryption,” *Proceedings of IEEE Symposium on Security and Privacy (SP) 2007*, 2007, pp.321-334.
Blaze, Matt, Gerrit Bleumer, and Martin Strauss, “Divertible Protocol and Atomic Proxy Cryptography,” *Proceedings of EUROCRYPT’98*, LNCS 1403, Springer-Verlag, 1998, pp.127-144.
Boneh, Dan, Giovanni Di Crescenzo, Rafael Ostrovsky, and Giuseppe Persiano, “Public Key Encryption with Keyword Search,” *Proceedings of EUROCRYPT2004*, LNCS 3072, Springer-Varlarg, 2004, pp.506-522.
———, Eu-Jin Goh, and Kobbi Nissim, “Evaluating 2-DNF Formulas on Ciphertext,” *Proceedings of Theory of Cryptography Conference (TCC) 2005*, LNCS 3378, Springer-Verlag, 2005, pp.325-341.
———, and Brent Waters, “Conjunctive, Subset, and Range Queries on Encrypted Data,” *Proceedings of Theory of Cryptography Conference (TCC) 2007*, LNCS 4392, Springer-Verlag, 2007, pp.535-554.
Brakerski, Zvika, and Renen Perlman, “Lattice-Based Fully Dynamic Multi-key FHE with Short Ciphertexts,” *Proceedings of CRYPTO2016*, LNCS 9814, Springer-Verlag,

2016, pp.190-213.

———, and Vinod Vaikuntanathan, “Circuit-ABE from LWE: Unbounded Attributes and Semi-Adaptive Security,” *Proceedings of CRYPTO2016*, LNCS 9816, Springer-Verlag, 2016, pp.363-384.

Canneti, Ran, Shai Halevi, and Jonathan Katz, “A Forward Secure Public Key Encryption Scheme, ” *Journal of Cryptology*, 20(3), 2007, pp.265–294.

Curtmola, Reza, Juan Garay, Seny Kamara, and Rafail Ostrovsky, “Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions,” *Proceedings of the ACM Conference on Computer and Communication Security (CCS) 2006*, 2006, pp.79-88.

Desmedt, Yvo, “Threshold Cryptography,” *Transactions on Emerging Telecommunications Technologies*, 5(4), 1994, pp.449-458.

Dodis, Yevgeniy, Jonathan Katz, Shouhuai Xu, and Moti Yung, “Key-Insulated Public Key Cryptosystems,” *Proceedings of EUROCRYPT2002*, LNCS 2332, Springer-Verlag, 2002, pp.65-82.

Dolev, Danny, Cynthia Dwork, and Moni Naor, “Non-Malleable Cryptography,” *Proceedings of ACM Annual Symposium on the Theory of Computing (STOC) 1991*, 1991, pp.542-552.

Dong, Qiuxiang, Zhi Guan, Liang Wu, and Zhong Chen, “Fuzzy Keyword Search over Encrypted Data in the Public Key Setting,” *Proceedings of International Conference on Web-Age Information Management (WAIM) 2013*, LNCS 7923, Springer-Verlag, 2013, pp.729-740.

Emura, Keita, Goichiro Hanaoka, Go Ohtake, Takahiro Matsuda, and Shota Yamada, “Chosen Ciphertext Secure Keyed-Homomorphic Public-Key Encryption,” *Proceedings of Public-Key Cryptography (PKC) 2013*, LNCS 7778, Springer-Verlag, 2013, pp.32-50.

European Commission, “Payment Services Directive: frequently asked questions,” 2015 (http://europa.eu/rapid/press-release_MEMO-15-5793_en.htm?locale=en).

Fiore, Dario, Rosario Gennaro, and Valerio Pastro, “Efficiently Verifiable Computation on Encrypted Data,” *Proceedings of the ACM Conference on Computer and Communication Security (CCS) 2014*, 2014, pp.844-855.

Gennaro, Rosario, Craig Gentry, and Bryan Parno, “Non-interactive Verifiable Computing: Outsourcing Computation to Untrusted Workers,” *Proceedings of CRYPTO2010*, LNCS 6223, Springer-Verlag, 2010, pp.465-482.

Gentry, Craig, “Fully Homomorphic Encryption using Ideal Lattices,” *Proceedings of ACM Annual Symposium on the Theory of Computing (STOC) 2009*, 2009,

pp.169-178.

———, Ami Sahai, and Brent Waters, "Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based," *Proceedings of CRYPTO2010*, LNCS 8042, Springer-Verlag, 2013, pp.75-92.

Gorbunov, Sergey, Vinod Vaikuntanathan, and Hoeteck Wee, "Attribute-Based Encryption for Circuits," *Journal of the ACM*, Vol 62(6), 2015.

Goyal, Vipul, Abhishek Jain, Omkant Pandey, and Amit Sahai, "Bounded Ciphertext Policy Attribute-Based Encryption," *Proceedings of International Colloquium on Automata, Languages, and Programming (ICALP) 2008*, LNCS 5126, Springer-Verlag, 2008, pp.579-591.

Goyal, Vipul, Omkant Pandey, Amit Sahai, and Brent Waters, "Attribute-based encryption for fine-grained access control of encrypted data," *Proceedings of the ACM Conference on Computer and Communication Security (CCS) 2006*, 2006, pp.89-98.

Hohenberger, Susan, and Brent Waters, "Attribute-Based Encryption with Fast Decryption," *Proceedings of Public-Key Cryptography (PKC) 2013*, LNCS 7778, Springer-Verlag, pp.162-179, 2013.

Hwang, Yong Ho, and Pil Joong Lee, "Public Key Encryption with Conjunctive Keyword Search and Its Extension to a Multi-user System," *Proceedings of Pairing 2007*, LNCS 4575, Springer-Verlag, 2007, pp.2-22

Katz, Jonathan, Ami Sahai, and Brent Waters, "Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products," *Journal of Cryptology*, 26(2), 2013, pp.191-224.

Kawai, Yutaka, Takato Hirano, Yoshihiro Koseki, and Tatsuji Munaka, "SEPM: Efficient Partial Keyword Search on Encrypted Data," *Proceedings of Cryptology and Network Security (CANS) 2015*, LNCS 9476, Springer-Verlag, 2015, pp.75-91.

Lewko, Allison, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, and Brent Waters, "Bounded Ciphertext Policy Attribute-Based Encryption and (Hierarchical) Inner Product Encryption," *Proceedings of EUROCRYPT2010*, LNCS 6110, Springer-Verlag, 2010, pp.62-91.

López-Alt, Adriana, Eran Tromer, and Vinod Vaikuntanathan, "On-the-fly Multiparty Computation on the Cloud via Multikey Fully Homomorphic Encryption," *Proceedings of Annual ACM symposium on the Theory of computing (STOC) 2012*, 2012, pp.1219-1234.

Lv, Zhiquan, Cheng Hong, Min Zhang, and Dengguo Feng, "Expressive and Secure Searchable Encryption in the Public Key Setting," *Proceedings of Information*

Security Conference (ISC) 2014, LNCS 8783, Springer-Verlag, 2014, pp.364-376.

Naor, Moni, and Gil Segev, "Public-Key Cryptosystems Resilient to Key Leakage," *Society for Industrial and Applied Mathematics (SIAM) Journal of Computing*, 41(4), 2012, pp.772-814.

National Institute of Standards and Technology, "Recommendation on Key Management," Special Publication (SP) 800-57, National Institute of Standards and Technology, 2012.

———, "Report on Post-Quantum Cryptography," NIST Internal/Interagency Reports (NISTIR) 8105, National Institute of Standards and Technology, 2016.

Okamoto, Tatsuaki, and Katsuyuki Takashima, "Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption," *Proceedings of CRYPTO2010*, LNCS 6223, Springer-Verlag, 2010, pp.191-208.

Open Data Institute, "Open Banking Standard," Open Data Institute, 2016.

Ostrovsky, Rafail, Amit Sahai, and Brent Waters, "Attribute-Based Encryption with Non-Monotonic Access Structures," *Proceedings of the ACM Conference on Computer and Communications Security (CCS) 2007*, 2007, pp.195-203.

Peikert, Chris, "A Decade of Lattice Cryptography," *Foundations and Trends in Theoretical Computer Science*, 10(4), 2016, pp.283-424.

Peng Xu, and Hai Jin, "Public-Key Encryption with Fuzzy Keyword Search: A Provably Secure Scheme under Keyword Guessing Attack," *IEEE Transactions on Computers*, 62(11), 2012, pp.2266-2277.

Rivest, Ronald, Leonard Adleman, and Michael L. Dertouzos, "On Data Banks and Privacy Homomorphisms," *Foundations of Secure Computation*, Academia Press, 1978, pp.169-177.

Rouselakis, Yannis, and Brent Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," *Proceedings of the ACM Conference on Computer and Communication Security (CCS) 2013*, 2013, pp.463-474.

Sahai, Amit, Hakan Seyalioglu, and Brent Waters, "Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption," *Proceedings of CRYPTO2012*, LNCS 7417, Springer-Verlag, 2012, pp.199-217.

——— and Brent Waters, "Fuzz Identity-Based Encryption," *Proceedings of EUROCRYPT2005*, LNCS 3494, Springer-Verlag, 2005, pp.457-473.

Waters, Brent, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," *Proceedings of Public-Key Cryptography (PKC) 2011*, LNCS 6571, Springer-Verlag, 2011, pp.53-70.

Yamada, Shota, Nuttapong Attrapadung, Goichiro Hanaoka, and Noboru Kunihiro,

"Generic Constructions for Chosen-Ciphertext Secure Attribute Based Encryption," *Proceedings of Public Key Cryptography (PKC) 2011*, LNCS 6571, Springer-Verlag, 2011, pp.71-89.

補論１．主な高機能暗号とその機能

これまでに提案されている各種の主な高機能暗号（公開鍵暗号に基づく方式）と、各方式が実現する機能を図表 A-1 にまとめる。

図表 A-1. これまでに提案されている主な高機能暗号とその機能

方式の名称		機能の概要		主な参考文献
検索可能暗号		データを暗号化したままキーワード検索を実行。		Boneh *et al.* [2004]
準同型暗号	単一演算型	データを暗号化したまま演算を実行。	加算または乗算のどちらか一方のみ可能。	Rivest, Adleman, and Dertouzos [1978]
	完全型		加算と乗算が可能。	Gentry [2009]
代理人再暗号化方式		データを暗号化したまま、復号権限を有するエンティティを変更。		Blaze, Bleumer, and Strauss [1998]
属性ベース暗号	鍵ポリシー型	データを復号できるエンティティを制御。	属性に基づくアクセス構造を秘密鍵に組み込む。	Sahai and Waters [2005]
	暗号文ポリシー型		属性に基づくアクセス構造を暗号文に組み込む。	Bethencourt, Sahai, and Waters [2007]
鍵漏えい耐性暗号	フォワード・セキュア（Forward-Secure）型	秘密鍵を定期的に更新することによって、あるタイミングで秘密鍵が漏洩した際に、そのタイミングよりも前に生成された暗号文の安全性を保証。		Canneti, Halevi, and Katz [2007]
	鍵隔離（Key-Insulated）型	秘密鍵を定期的に更新することによって、あるタイミングで秘密鍵が漏洩した際に、それ以外の秘密鍵で生成された暗号文の安全性を保証。		Dodis *et al.* [2002]
	リーケージ・レジリエント（Leakage-Resilient）型	秘密鍵の一部が漏洩しても暗号文の安全性を保証。		Naor and Segev [2012]
しきい値暗号		暗号文の復号権限を複数のエンティティに分割。一定数（しきい値）以上のエンティティが協力することにより暗号文を復号可能。		Desmedt [1994]

また、公開鍵暗号型の検索可能暗号によって実現されている検索機能について整理すると、以下の図表 A-2 のとおりである。

図表 A-2. 公開鍵暗号型の検索可能暗号で実現されている検索機能

検索機能	概要	主な文献
完全一致検索	検索キーワードと同じ登録キーワードを有する登録データを検索。	Boneh *et al.* [2004]、Abdlla *et al.* [2005]、Bellare, Boldyreva, and O'Neill [2007]
部分一致検索	検索キーワードが文字列の一部に含まれる登録キーワードを有する登録データを検索。この検索機能には、前方（後方）一致検索も含まれる。	吉田・小田・小林［2010］、Kawai *et al.* [2015]
AND 検索	複数個の検索キーワードの全てに合致する登録キーワードを有する登録データを検索。	Boneh and Waters [2007]、Baek, Safavi-Naini, and Susilo [2008]、Katz, Sahai, and Waters [2013]
OR 検索	複数個の検索キーワードの少なくとも 1 つと完全に一致する登録キーワードを有する登録データを検索。	Baek, Safavi-Naini, and Susilo [2008], Katz, Sahai, and Waters [2013]
AND 検索と OR 検索の組合せ	AND 検索と OR 検索を組み合わせた検索条件に一致する登録キーワードを有する登録データを検索。	Katz, Sahai, and Waters [2013]
OR 検索と NOT 検索の組合せ	OR 検索と NOT 検索を組み合せた検索条件に一致する登録キーワードを有する登録データを検索。	Lv *et al.* [2014]
類似検索	検索キーワードの文字列と類似した登録キーワードを有する登録データを検索。	Xu and Jin [2012]、Dong *et al.* [2013]

備考：清藤・四方［2014］図表 9 を最新動向に基づき加筆・修正したもの。

補論２．２つのモデルに高機能暗号を適用した際の処理と安全性評価

（１）営業支援システムへの高機能暗号の適用

イ．検索可能暗号の適用

（イ）処理フロー

処理フローとして、鍵生成、登録、検索の 3 つのフェーズを想定する。鍵生成フェーズにおいて、顧客データの共有を受ける各営業担当者は公開鍵と秘密鍵を生成したうえで、公開鍵は顧客データを預託する全ての営業担当者が利用できる形で公開し、秘密鍵は自身で秘密に保管する。登録フェーズにおいて、顧客データを預託する営業担当者は、顧客データの共有を受ける各営業担当者が生成した公開鍵を用いて、顧客データおよび（当該顧客データに関連する）登録キーワードを暗号化して預託データを生成する。その後、クラウド・サービス事業者に送信する。クラウド・サービス事業者は、預託データを顧客データベースに保管する。検索フェーズにおいて、顧客データの共有を受ける営業担当者は取得したい顧客データにかかる検索キーワードを選択する。そのうえで、自らが生成した秘密鍵を用いて当該検索キーワードからトラップドアを生成した後、クラウド・サービス事業者に送信する。クラウド・サービス事業者は、トラップドアを用いて検索処理を行い、検索キーワードに合致するものを抽出して処理データとして当該営業担当者に送信する。顧客データの共有を受ける営業担当者は、自らが生成した秘密鍵を用いて処理データを復号し、顧客データを取得する。

（ロ）安全性の評価

攻撃者は、「全ての公開鍵」、「全ての預託データ」、「全てのトラップドア」を入手していると想定する。検索可能暗号が安全性要件 1 と 3 を満たしている場合、預託データ（暗号文）から顧客データ（平文）に関する情報は漏えいしない。また、安全性要件 4、5 を満たす場合、トラップドア（変換処理された検索キーワード）から検索キーワードに関する情報は漏えいしない。この結果、検索可能暗号が安全性要件 1、3、4、5 を満たす場合には、安全性要件 A-1 が満たされる。また、検索可能暗号が安全性要件 2 を満たしている場合、暗号化された顧客データ（預託データ）を異なる内容に書き換えることができないため、安全性要件 A-2 が満たされる。

ロ．属性ベース暗号の適用

（イ）処理フロー

処理フローとして、鍵生成、登録、共有の 3 つのフェーズを想定する。鍵生成フェーズにおいて、公開鍵および顧客データの共有を受ける営業担当者の属性ごとの秘密鍵が生成され、秘密鍵は顧客データの共有を受ける各営業担当者に安全に配付する。公開鍵は、顧客データを預託する全ての営業担当者が利用可能な形で公開する。登録フェーズにおいて、顧客データを預託する営業担当者は、他の営業担当者と共有したい顧客データについて、共有を許可する営業担当者の属性をアクセス構造として設定する。その後、公開鍵を用いて暗号文（預託データ）を生成し、クラウド・サービス事業者に送信する。クラウド・サービス事業者は、預託データを顧客データベースに保管する。共有フェーズにおいて、顧客データの共有を受ける営業担当者は顧客データの取得要求をクラウド・サービス事業者に送信する。クラウド・サービス事業者は、当該取得要求に応じて、該当する預託データを抽出し処理データとして当該営業担当者に送信する。顧客データの共有を受ける営業担当者は、秘密鍵を用いて処理データを復号する。

（ロ）安全性の評価

攻撃者は「公開鍵」、「全ての預託データ」を入手していると想定する。属性ベース暗号が安全性要件 1 を満たす場合、預託データから顧客データに関する情報は漏えいしない。また、安全性要件 2 を満たす場合、暗号化された顧客データを異なる内容に書き換えることはできない。したがって、属性ベース暗号が安全性要件 1、2 を満たす場合、安全性要件 A-1 と A-2 が満たされる。

ハ．準同型暗号の適用

（イ）処理フロー

処理フローとして、鍵生成、登録、演算の 3 つのフェーズを想定する。鍵生成フェーズにおいて、顧客データの共有を受ける各営業担当者は、公開鍵と秘密鍵を生成し、秘密鍵は自身で安全に保管するとともに、公開鍵は顧客データを預託する全ての営業担当者が利用できる形で公開する。登録フェーズにおいて、顧客データを預託する営業担当者は、顧客データの共有を受ける各営業担当者が生成した公開鍵を用いて顧客データを暗号化して預託データを生成した後、クラウド・サービス事業者に送信する。クラウド・サービス事業者は、預託データを顧客データベースに保管する。演算フェーズにおいて、顧客データの共有を受ける営業担当者はクラウド・サービス事業者へ預託データに対する演算処理要求を送信する。クラウド・サービス事業者は、当該演算処理要求に

応じて、預託データに対する演算処理を行い、その結果（処理データ）を当該営業担当者に送信する。顧客データの共有を受ける営業担当者は、秘密鍵を用いて処理データを復号し、演算処理された業務データを得る。

（ロ）安全性の評価

攻撃者は「公開鍵」、「全ての預託データ」を入手していると想定する。準同型暗号が安全性要件 1 を満たす場合、これらのデータから業務データに関する情報は漏えいせず、安全性要件 A-1 が満たされる。一方、準同型暗号は暗号化された業務データを異なる内容に書き換えられた場合、それを検知することが原理的に困難であり、安全性要件 A-2 は満たされない。

（２）口座情報サービスへの高機能暗号の適用

イ．検索可能暗号の適用

（イ）処理フロー

処理フローとして、鍵生成、収集、提供の 3 つのフェーズを想定する。鍵生成フェーズにおいて、各利用者は、公開鍵と秘密鍵を生成し、秘密鍵を自身で安全に保管するとともに、公開鍵は TPPs にデータを預託する金融機関が利用できる形で公開する。収集フェーズにおいて、TPPs は、利用者に関する業務データ（口座残高等）の取得要求を、定期的に金融機関に送信する。金融機関は、当該取得要求に応じて業務データを抽出し、当該業務データにかかる登録キーワードを設定したうえで、各利用者が生成した公開鍵を用いてこれらのデータを暗号化し預託データを生成する。金融機関は、TPPs に預託データを送信する。TPPs は、預託データをストレージに保管する。提供フェーズにおいて、利用者は、入手したい業務データ（口座残高等）に関する検索キーワードを設定し、自らが生成した秘密鍵を用いてトラップドアを生成した後、業務データの提供依頼として TPPs に送信する。TPPs は、提供依頼（トラップドア）を用いて預託データの検索処理を行い、検索キーワードに合致するものを処理データとして利用者に送信する。利用者は、自らが生成した秘密鍵を用いて処理データを復号し、業務データを取得する。

（ロ）安全性の評価

攻撃者は、「公開鍵」、「全ての預託データ」、「全てのトラップドア」、「（攻撃者と結託した）一部の利用者の秘密鍵」を入手していると想定する。検索可能暗号が安全性要件 1、3 を満たしている場合、預託データから業務データに関する情報は漏えいしない。また、安全性要件 4、5 を満たす場合、トラップドアから検索キーワードに関する情報は漏えいしない。この結果、検索可能暗号が安

全性要件 1、3、4、5 を満たす場合には、安全性要件 B-1 が満たされる。また、検索可能暗号が安全性要件 2 を満たす場合、暗号化された業務データを異なる内容に書き換えることができず、安全性要件 B-2 が満たされる。

ロ．属性ベース暗号の適用

（イ）処理フロー

処理フローとして、鍵生成、提供の 2 つのフェーズを想定する。鍵生成フェーズにおいて、金融機関が、公開鍵と、預託データの送信を受ける TPPs の属性ごとの秘密鍵を生成し、安全な手段を用いて各 TPPs に配付する。公開鍵は、利用者等に対して公開する。提供フェーズにおいて、利用者は自身の口座情報等の取得要求を TPPs に送信する。TPPs は、取得要求を金融機関に転送する。金融機関は、当該取得要求に応じて、当該利用者の業務データを抽出した後、預託データの送信を受ける TPPs の属性をアクセス構造として設定し、公開鍵を用いて当該アクセス構造を組み込んだ暗号文（預託データ）を生成して TPPs に送信する。TPPs は、金融機関から配付を受けた秘密鍵を用いて預託データを復号し、業務データを入手する。その後、TPPs は、利用者からの依頼に基づき、当該業務データに必要に応じ統計解析等の加工を行って処理データを生成し、利用者に送信する。

（ロ）安全性の評価

攻撃者は「公開鍵」、「全ての預託データ」、「攻撃者と結託した一部の（金融機関から預託データへのアクセスを許可されていない）TPPs の秘密鍵」を入手していると想定する。属性ベース暗号が安全性要件 1 を満たす場合、攻撃者は業務データに関する情報を得られない。安全性要件 2 を満たす場合、攻撃者は暗号化された業務データを異なる内容に書き換えることができない。この結果、属性ベース暗号がこれらの安全性要件を満たしている場合には、安全性要件 B-1 と B-2 が満たされる。

ハ．準同型暗号の適用

（イ）処理フロー

処理フローとして、鍵生成、収集、提供のフェーズを想定する。鍵生成フェーズにおいて、各利用者は公開鍵と秘密鍵を生成し、秘密鍵を自身で安全に保管するとともに、公開鍵は TPPs にデータを預託する金融機関が利用可能な形で公開する。収集フェーズにおいて、TPPs は利用者に関する業務データ（口座残高等）の取得要求を、定期的に金融機関に送信する。金融機関は、当該取得要求に応じて業務データを抽出した後、当該業務データから各利用者が生成した公

開鍵を用いて暗号文（預託データ）を生成して TPPs に送信する。TPPs は、預託データをストレージに保管する。提供フェーズにおいて、利用者は預託データに対する演算処理要求を TPPs に送信する。TPPs は、当該演算処理要求に応じて預託データ（暗号文）に対する演算処理を行い、その結果を処理データとして利用者に送信する。利用者は、自らが生成した秘密鍵を用いて処理データを復号し、演算処理された業務データを取得する。

（ロ）安全性の評価

攻撃者は「公開鍵」、「全ての預託データ」、「（攻撃者と結託した）一部の利用者の秘密鍵」を入手していると想定する。準同型暗号が安全性要件 1 を満たす場合、これらのデータから業務データに関する情報は漏えいせず、安全性要件 B-1 が満たされる。ただし、暗号化された業務データが異なる内容に書き換えられた場合、それを検知することが原理的に困難であるため、安全性要件 B-2 は満たされない。