Vol.2017-CSEC-78 No.14
Vol.2017-SPT-24 No.14
2017/7/14

高機能暗号の金融分野での応用に関する考察†

清藤　武暢[1]　青野　良範[2]　四方　順司[3]

概要：高機能暗号とは，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や，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を実現する暗号である．本稿では，公開鍵暗号型の高機能暗号に焦点を当てたうえで，金融機関の既存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，これらのケースにおいて期待される効果や課題等について考察する．

A Remark on Applications of Advanced Cryptosystems in Financial Sector

Takenobu Seito[1]　Yoshinori Aono[2]　Junji Shikata[3]

1. はじめに

2000 年央以後，幅広い分野においてクラウド・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，システムの開発・運用におけるコスト削減や導入の迅速化等を企図して，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，幅広い分野で活発化している．金融分野においても，同様に，クラウド・サービスへ各種業務をアウトソースする動きが広がっている [3].

また，近年はスマートフォン等の端末を活用し，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 FinTech 企業が注目を集めており，こうした企業は TPPs（Third Party Providers）と呼ばれる [7]．こうしたサービスでは，従来は金融機関のみが取り扱っていた金融取引等に関するデータが，クラウド・サービスを提供する業者（以下，クラウドサービス事業者と呼ぶ）や TPPs によっても取り扱われるようになる．そのため，これらのエンティティ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・サービス等で取り扱うことができれば，安全性の観点から望ましい．

近年，このようなニーズに対応する技術として高機能暗号が注目されており，研究開発が活発化している．高機能暗号を利用することにより，基本的な暗号機能（データの暗号化と復号）に加えて，暗号化したままデータを処理する機能や，エンティティの属性に応じて暗号化したデータへのアクセス権限を制御する機能等を実現できる．今後，この高機能暗号に基づくクラウド・サービスや新たな金融サービスが提供されれば，金融機関はデータの安全性を確保しつつ，業務のアウトソーシングや TPPs へのデータ提供を一段と進めることができると期待される．

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．その中でも，公開鍵暗号型は，構成要素として用いられているペアリングや格子の特性を活用することにより，これまでにさまざまな機能を実現する方式（検索可能暗号，属性ベース暗号，準同型暗号等）が提案されている [1].

[1] 日本銀行金融研究所
Institute for Monetary and Economic Studies, Bank of Japan
[2] 情報通信研究機構サイバーセキュリティ研究所
Cybersecurity Research Institute, National Institute of Information and Communications Technology
[3] 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

† 本稿は，[5] の内容に基づくものである．また，本稿に示されている意見は，著者たち個人に属し，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．

[1] 共通鍵暗号型の高機能暗号については，[6] や [1] を参照

Vol.2017-CSEC-78 No.14
Vol.2017-SPT-24 No.14
2017/7/14

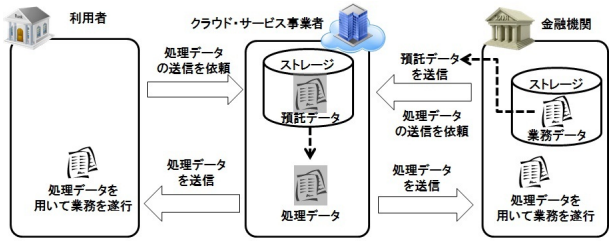

図 1　クラウド・サービス利用モデル

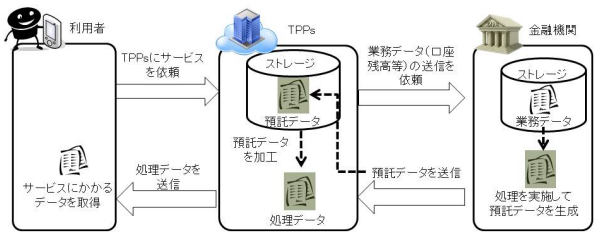

図 2　TPPs 利用モデル

本稿では，公開鍵暗号型の高機能暗号に焦点を当て，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，これらのケースにおいて期待される効果や課題等について考察する．2 節では，金融分野において高機能暗号を適用しうる 2 つのケースを定義する．3 節では，公開鍵暗号型の高機能暗号の主な 3 つの方式の概要について説明する．4 節では，各モデルにおける高機能暗号の具体的な活用方法を検討したうえで，期待される効果（メリット等），安全性や課題等について考察する．

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するケースと，(2)TPPs による新しい金融サービスに高機能暗号を導入するケースが考えられる．本節では，これらのケースを抽象化した 2 つのモデルを定義する．

2.1 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を利用して自社の業務を実現するという状況を抽象化したものである（図 1）．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．金融機関は，業務に関するデータ（以下，業務データと呼ぶ）を生成・保管するとともに，当該データに一定の処理を施したデータ（以下，預託データと呼ぶ）をクラウド・サービス事業者に預託する．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．金融機関や当該金融機関と同一の企業グループに属する企業等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，ストレージ上で保管・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．

2.2 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 2）．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．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．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．

2.3 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，金融機関において業務データを暗号化したものを預託データとして，クラウド・サービス事業者や TPPs に送信することが考えられる．その際，従来の暗号（RSA 暗号等）を利用する方法がまず想定される．この方法は，金融機関がクラウド・サービス事業者に業務データの保管や転送のみ依頼する場合には有効である．しかし，金融機関や利用者がクラウド・サービス事業者等に各種処理（キーワード検索や統計解析等）を依頼する場合には，暗号化したままでは当該処理を実施できない．そのため，金融機関や利用者は，クラウド・サービス事業者や TPPs 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・サービス事業者や TPPs が（平

文の）業務データを取り扱うこととなり，上記のリスクが発生する．

また，金融機関や利用者が，業務や金融サービスにおいて連携するエンティティが預託データを復号できる権限を制御するためには，各エンティティごとに異なる鍵が準備される必要がある．その結果，鍵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各エンティティ間で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のうち，近年，特に研究開発が活発化している検索可能暗号，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と安全性について説明する．以下では，2節で定義したモデルへの適用について検討するために，登録者，利用者，外部サーバから構成されるモデルを想定する．

3.1 検索可能暗号

3.1.1 機能

検索可能暗号では，暗号化したデータ（暗号文）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良い．

検索可能暗号のモデルにおいて，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当該データの復号に用いる秘密鍵を生成し，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）を外部サーバに送信する．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，利用者からの依頼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．

公開鍵暗号型の検索可能暗号は，完全一致検索を実現する方式が提案された後 [9]，より高度な検索機能（部分一致検索，類似検索，複数キーワード検索等）を実現する方式が提案されている（[17]，[12]，[16]，[18] 等）．

3.1.2 安全性

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（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．さらに，検索キーワードの機密性を確保するために，検索キーワードが漏えいしない（安全性要件 4），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．

3.2 属性ベース暗号

3.2.1 機能

属性ベース暗号は，暗号文や秘密鍵にアクセス構造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．この暗号では，エンティティの属性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．特に，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，利用者からの依頼に

応じて暗号文を送信する．

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 AND と OR で組み合わせた単純なアクセス構造のみ設定可能であった [8][22]．その後，NOT を組み合わせたより複雑な条件式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（[20]，[15]，[19]，[11] 等）．

3.2.2 安全性

属性ベース暗号においては，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，3.1.2 節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．

3.3 準同型暗号

3.3.1 機能

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）を実行できる．準同型暗号のモデルにおいて，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．

準同型暗号の機能である，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 [21]．当初は，乗算または加算の一方のみを演算可能な方式が提案されており，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 [10]，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が発表された [14]．

3.3.2 安全性

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，3.1.2 節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．

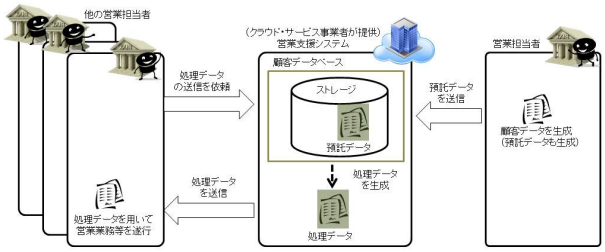

図 3 想定する営業支援システム

表 1 営業支援システムに高機能暗号を適用した際に期待される効果

高機能暗号	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（暗号文）を復号しないでそのままキーワード検索を実行可能．
属性ベース暗号	顧客データの復号権限を営業担当者が効率的に制御可能．
準同型暗号	顧客データを暗号化したまま外部サーバで統計解析等を実施可能．

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．

4.1 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・サービス事業者が提供する）営業支援システムを想定する （図 3）．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 [2] 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 [2]．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，当該顧客データを暗号化したうえでクラウド・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した際に期待される効果を表 1 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（当該サービス上で利用できる機能の追加や鍵管理等のコスト削減）

[2] 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 [2]．

が期待される．

4.1.1 各エンティティにおける処理の概要

営業支援システムに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は以下のとおりである（各処理の詳細については [5] を参照）．

検索可能暗号を適用した際の処理

1. 営業担当者による鍵生成と預託データの生成：顧客データを共有する各営業担当者は，公開鍵と秘密鍵を生成する．その後，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．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する．
2. 営業担当者による依頼：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する．
3. 営業支援システムによる処理データの生成と送信：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する．

属性ベース暗号を適用した際の処理

1. 営業担当者による鍵生成と預託データの生成：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）を生成する．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する．顧客データを預託する営業担当者は，当該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，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する．
2. 営業担当者による依頼：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する．
3. 営業支援システムによる処理データの生成と送信：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処理データとして送信する．

準同型暗号を適用した際の処理

1. 営業担当者による鍵生成と預託データの生成：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する．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する．
2. 営業担当者による依頼：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する．
3. 営業支援システムによる処理データの生成と送信：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する

表 2 営業支援システムにおける主な脅威・リスク

主な脅威	攻撃方法	安全性に関するリスク
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．
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．

4.1.2 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，クラウド・サービス事業者の内部者の一部と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を表 2 にまとめる．

上記の脅威・リスクを想定したうえで，顧客データの機密性と完全性を確保するために，顧客データが漏えいしない（安全性要件 A-1）と，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）を，安全性要件として定義する．

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 [5] 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 [13] の併用等が考えられる．

4.1.3 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

表 3　口座情報サービスに高機能暗号を適用した際に期待される効果

高機能暗号	期待される効果
検索可能暗号	TPPs が，預託データ（暗号文）を復号しないでそのままキーワード検索を実行可能.
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可能.
準同型暗号	TPPs が預託データを復号しないでそのまま統計解析等を実施可能.

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．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，ともに従来の暗号と同じく N となる．公開鍵のサイズは，従来の暗号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．

4.2　TPPs 利用モデル

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を想定する（図 4）．

口座情報サービスは，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）を金融機関から収集・加工して当該利用者に提供するサービスである．ここでの口座情報サービスでは，高機能暗号用の公開鍵や秘密鍵の生成・配付が行われているもとで，利用者（金融機関の顧客）が TPPs にサービスを依頼し，TPPs 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，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．

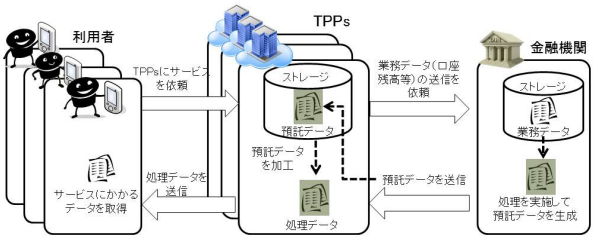

図 4　想定する口座情報サービス

上記の口座情報サービスに高機能暗号を適用した際に期待される効果を表 3 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．

4.2.1　各エンティティにおける処理の概要

口座情報サービスに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は以下のとおりである（各処理の詳細については [5] を参照）．

検索可能暗号を適用した際の処理

1. 各エンティティによる鍵生成：各利用者は，公開鍵と秘密鍵を生成する．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する．
2. 利用者による利用依頼：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 に送信する．
3. 金融機関による預託データの生成・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，預託データを生成する．その後，TPPs に預託データを送信する．
4. TPPs による処理データの生成・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，当該利用者に送信する．

属性ベース暗号を適用した際の処理

1. 各エンティティによる鍵生成：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）を生成する．その後，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 に安全に配付する．
2. 利用者による利用依頼：TPPs に処理データの送信を

依頼する．

3. 金融機関による預託データの生成・送信：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，公開鍵を用いて，業務データに当該アクセス構造を組み込んで暗号化したうえで，預託データを生成する．その後，預託データを TPPs に送信する．
4. TPPs による処理データの生成・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，当該データを受信する．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，利用者に送信する [3]．

準同型暗号を適用した際の処理

1. 各エンティティによる鍵生成：各利用者は，公開鍵と秘密鍵を生成する．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する．
2. 利用者による利用依頼：TPPs に預託データの統計解析等を依頼する．
3. 金融機関による預託データの生成・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，預託データを生成する．その後，TPPs に預託データを送信する．
4. TPPs による処理データの生成・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する．

4.2.2 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，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，TPPs への攻撃，利用者への攻撃，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を表 4 にまとめる．

上記の脅威・リスクを想定したうえで，業務データの機密性と完全性を確保するために，業務データが漏えいしない（安全性要件 B-1）と，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）を，安全性要件として定義する．

上記の各暗号について，業務データの機密性（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 [5] 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 [13] の併用等が考えられる．

[3] 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．

表 4 口座情報サービスにおける主な脅威・リスク

主な脅威	攻撃方法	安全性に関するリスク
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．
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．

4.2.3 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，営業支援システムの議論と同様であるため，ここでは省略する．

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．

5. おわりに

本稿では，公開鍵案型の高機能暗号を既存の金融業務（営業支援システム）や新たな金融サービス（口座情報サービス）へ適用した際の効果や課題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，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．また，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．

参考文献

[1] 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-7，日本銀行金融研究所，2017 年．
[2] 金融情報システムセンター，“平成 28 年度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．
[3] 金融情報システムセンター，“平成 28 年度版金融情報システム白書，”金融情報システム，No.341，2016 年．
[4] 清藤武暢，青野良範，四方順司，“量子コンピュータの解読に耐えうる「格子暗号」の最新動向，”金融研究，第 34 巻第 4 号，pp.135-170，2015 年．
[5] 清藤武暢，青野良範，四方順司，“公開鍵暗号型の高機能暗号を巡る研究動向，”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-8，2017 年．
[6] 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 33 巻第 4 号，日本銀行金融研究所，pp.93-132，2014 年．
[7] 中村啓祐，“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-14，2016 年．
[8] Bethencourt, John, Amit Sahai, and Brent Waters, “Ciphertext-Policy Attribute-Based Encryption,” Proceedings of IEEE Symposium on Security and Privacy (SP) 2007, pp.321-334, 2007.
[9] Boneh, Dan, Giovanni Di Crescenzo, Rafael Ostrovsky, and Giuseppe Persiano, “Public Key Encryption with Keyword Search,” Proceedings of EUROCRYPT2004, LNCS 3072, Springer-Varlarg, pp.506-522, 2004.
[10] Boneh, Dan, Eu-Jin Goh, and Kobbi Nissim, “Evaluating 2-DNF Formulas on Ciphertext,” Proceedings of Theory of Cryptography Conference (TCC) 2005, LNCS 3378, Springer-Verlag, pp.325-341, 2005.
[11] Brakerski, Zvika, and Renen Perlman, “Lattice-Based Fully Dynamic Multi-key FHE with Short Ciphertexts,” Proceedings of CRYPTO2016, LNCS 9814, Springer-Verlag, pp.190-213, 2016.
[12] 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, pp.729-740, 2013.
[13] 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, pp.844-855, 2014.
[14] Gentry, Craig, “Fully Homomorphic Encryption using Ideal Lattices,” Proceedings of ACM Annual Symposium on the Theory of Computing (STOC) 2009, pp.169-178, 2009.
[15] 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, pp.579-591, 2008.
[16] Katz, Jonathan, Ami Sahai, and Brent Waters, “Predicate Encryption Supporting Disjunctions, Polynomial Equations, and Inner Products,” Journal of Cryptology, 26(2), pp.191-224, 2013.
[17] 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, pp.75-91, 2015.
[18] 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, pp.364-376, 2014.
[19] 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, pp.195-203, 2007
[20] Okamoto, Tatsuaki, and Katsuyuki Takashima, “Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption,” Proceedings of CRYPTO2010, LNCS 6223, Springer-Verlag, pp.191-208, 2010.
[21] Rivest, Ronald, Leonard Adleman, and Michael L. Dertouzos, “On Data Banks and Privacy Homomorphisms,” Foundations of Secure Computation, Academia Press, pp.169-177, 1978.
[22] Sahai, Amit and Brent Waters, “Fuzz Identity-Based Encryption,” Proceedings of EUROCRYPT2005, LNCS 3494, Springer-Verlag, pp.457-473, 2005.