IMES DISCUSSION PAPER SERIES

情報セキュリティ・シンポジウム（第18回）の模様：新たな金融サービスを支える高機能暗号

Discussion Paper No. 2017-J-9

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

IMES Discussion Paper Series 2017-J-9
2017 年 5 月

情報セキュリティ・シンポジウム（第 18 回）の模様：
新たな金融サービスを支える高機能暗号

要　　旨

日本銀行金融研究所は、2017 年 3 月 9 日、「新たな金融サービスを支える高機能暗号：セキュリティと利便性の両立に向けて」をテーマとして第 18 回情報セキュリティ・シンポジウムを開催した。今回のシンポジウムには、情報セキュリティ技術にかかわる金融機関の実務者や官公庁関係者、暗号学者、システム開発・運用に携わる実務家や技術者等、約 100 名が参加した。今回のシンポジウムでは、主要な「高機能暗号」である「検索可能暗号」、「準同型暗号」、「属性ベース暗号」について取り上げ、それらの技術の理解促進のために理論と実装の観点から講演を行った。また、「金融分野での高機能暗号の活用に向けて」と題したパネル・ディスカッションを行った。本稿では、今回のシンポジウムを構成するキーノート・スピーチ、講演、パネル・ディスカッションの概要を紹介する。

キーワード：検索可能暗号、高機能暗号、準同型暗号、属性ベース暗号
JEL classification: L86、L96、Z00

目　次

１．はじめに

日本銀行金融研究所情報技術研究センター（Center for Information Technology Studies：CITECS）は、2017 年 3 月 9 日、「新たな金融サービスを支える高機能暗号:セキュリティと利便性の両立に向けて」をテーマとして第 18 回情報セキュリティ・シンポジウムを開催した。

近年、FinTech 企業等と連携して新しい金融サービスを開始する金融機関が増えており、金融取引にかかるデータを FinTech 企業やクラウド・サービス事業者等の外部組織に預託するケースも増えている。その際に、外部組織に預託するデータが漏えいしたり、改ざんされたりするリスクが存在する。金融サービスの利便性低下を回避しつつ、そうしたリスクを抑制しうる技術として、「高機能暗号」と呼ばれる新しい暗号技術が注目されている。今回のシンポジウムでは、高機能暗号の理解促進と金融分野での活用に向けて、講演とパネル・ディスカッションを行った。

今回のシンポジウムには、情報セキュリティ技術にかかわる金融機関の実務者や官公庁関係者、暗号学者、システム開発・運用に携わる実務者や技術者等、約 100 名が参加した。以下では、プログラムに沿って、今回のシンポジウムの概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）[1]。

【第 18 回情報セキュリティ・シンポジウムのプログラム】

- キーノート・スピーチ「新たな金融サービスを支える高機能暗号：セキュリティと利便性の両立に向けて」
  横浜国立大学大学院　教授　松本勉
- 講演１「公開鍵暗号型の高機能暗号の研究動向」
  日本銀行金融研究所　清藤武暢
- 講演２「公開鍵暗号型の高機能暗号の実装にかかる動向」
  三菱電機情報技術総合研究所 研究員　川合豊
- 講演３「共通鍵暗号型の高機能暗号の研究動向」
  日本銀行金融研究所　芦原聡介
- 講演４「共通鍵暗号型の高機能暗号の実装にかかる動向」
  日立製作所研究開発グループ　主任研究員　吉野雅之
- パネル・ディスカッション「金融分野での高機能暗号の活用に向けて」
  モデレータ：横浜国立大学大学院　教授　松本勉
  パネリスト：横浜国立大学大学院　教授　四方順司
  金融 ISAC　理事/FS-ISAC Regional Director 鎌田敬介
  三菱電機情報技術総合研究所　主席研究員　平野貴人
  日立製作所研究開発グループ　研究員　長沼健
  日本マイクロソフトクラウドプラットフォーム技術部　廣瀬一海

[1] 文中における各参加者の所属ならびに肩書きはシンポジウム開催時点のものである。

２．キーノート・スピーチ「新たな金融サービスを支える高機能暗号：セキュリティと利便性の両立に向けて」

松本は、金融機関が外部組織によるサービスを活用し始めたことに伴うセキュリティ・リスクや、当該リスクを抑制しうるセキュリティ技術として注目されている高機能暗号について、次のとおり発表した。

（１）金融サービスを提供する環境の変化

スマートフォン等のモバイル端末やクラウド・サービスが普及し、サービス利用者の利便性を向上させる情報技術（オープン API、ブロックチェーン等）を活用した新しい金融サービスである「FinTech」が注目されている。こうしたサービスの増加に伴い、金融取引にかかるデータを FinTech 企業やクラウド・サービス事業者等の外部組織に預託するケースも増えている。例えば、サービス利用者が取引する複数の金融機関から自分の口座に関するデータを取得し、それらを集計・加工して当該サービス利用者に提供するサービス（口座情報サービス）が開始されているほか、証券決済等の金融インフラにおけるブロックチェーンの活用を企図した検討が進められている。

（２）新たな金融サービスに求められる情報セキュリティ

金融機関は、金融取引等にかかるデータを外部組織に預託する際にそれを暗号化しているが、当該データを外部組織に加工させる場合、外部組織内で一度復号する必要がある。その際に、データが漏えいしたり、改ざんされたりするリスクが存在する。また、連携するデータを暗号化する都度異なる鍵を用いる必要があることから、鍵の管理負担が増加し、金融機関側の「利便性低下」が生じうる。こうしたリスク増加と利便性低下の両方を抑制しうる技術として、「高機能暗号」が注目されている。高機能暗号は、基本的な暗号機能（データの暗号化と復号など）に加えて、高度な機能を実現する暗号技術の総称であり、データを暗号化したままさまざまな処理を行うことができるものがある。また、高機能暗号にはデータの機密性確保に用いられるものだけでなく、データの作成者の認証や完全性確保に用いられる技術もある。

高機能暗号のうち、検索可能暗号は、既にクラウド・サービスを利用した電子メールシステムに適用されている。これは、クラウド・サーバ上に暗号化されたメールを格納し、暗号化したまま検索を行うというものである。また、API を利用した口座情報サービスに対して、高機能暗号である属性ベース暗号や準同型暗号を適用することが考えられる。属性ベース暗号はエンティティの属性に応じて暗号化したデータの復号権限を効率的に制御することができる方式で

あり、準同型暗号はデータを暗号化したまま統計解析等の演算処理を実現する方式である。これらを用いて、口座情報等のデータへのアクセス制御を効率的かつ柔軟に実施したり、当該データを暗号化したまま加工したりすることが、今後、想定される。

（３）今回のシンポジウムの狙い

今次シンポジウムのテーマは「新たな金融サービスを支える高機能暗号」である。今回のシンポジウムでは、高機能暗号のうち、検索可能暗号、準同型暗号、属性ベース暗号を取り上げる。シンポジウムを通して、高機能暗号の正確な理解を促進するために、高機能暗号で実現される機能や課題について理論と実装の両面から議論したい。また、高機能暗号が活用できる分野や、実際に活用する際の課題を技術面と運用面の双方の観点から検討したい。

３．講演１「公開鍵暗号型の高機能暗号の研究動向」

清藤は、高機能暗号のなかで公開鍵暗号型に分類される主な方式（準同型暗号、属性ベース暗号）に焦点を当てて、実現される機能や安全性、当該方式を金融分野で活用した際に期待される効果と課題について、次のとおり発表した。

（１）公開鍵暗号型の高機能暗号

公開鍵暗号型の高機能暗号には、基礎技術として数学的な仕組み（「ペアリング関数[2]」や「格子[3]」等）が採用されており、これまでにさまざまな機能を実現する方式（準同型暗号、属性ベース暗号等）が提案されている。安全性については、属性ベース暗号は、従来の暗号（RSA 暗号等）と同程度の安全性を確保できる。一方、準同型暗号については、データの機密性を確保できるものの、データの完全性を確保することが原理的に困難である[4]。

（２）金融分野で活用した際に期待される効果と課題

既にクラウド・サービスとして提供されている「営業支援システム」と、FinTech 企業等を介して利用できる新たな金融サービスである「口座情報サービス」に、それぞれ準同型暗号と属性ベース暗号を活用するケースを考える。営業支援シ

---

[2] 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性質を有する関数である。

[3] 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、点同士の四則演算が可能な性質を有する。

[4] 一般に、準同型暗号では、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することが原理的に困難である。

ステムでは、金融機関の営業担当者間でクラウド・サービス事業者のデータベースを介して顧客情報等を共有する。口座情報サービスでは、サービス利用者は（複数の）金融機関における自分の口座残高等のデータを集計・確認する。ここでは、営業担当者および金融機関のデータがクラウド・サービス事業者やFinTech企業に預託される際の暗号化処理に準同型暗号と属性ベース暗号を適用することを想定する。

これらのサービスに準同型暗号と属性ベース暗号を適用することによって、クラウド・サービス事業者等からのデータ漏えいリスクの軽減が可能となる。これに加えて、準同型暗号の適用によって、クラウド・サービス事業者等に、暗号化されたデータに対する統計解析等の委託が可能となる。また、属性ベース暗号によって、データを暗号化する営業担当者や金融機関における鍵管理コストの軽減が可能となる。

他方、準同型暗号と属性ベース暗号を活用する際には、従来の暗号と比較して暗号処理に要するコストが増加する場合がある。また、準同型暗号については、データの完全性を確保するための技術を別途利用する必要がある。

４．講演２「公開鍵暗号型の高機能暗号の実装にかかる動向」

川合は、公開鍵暗号型の高機能暗号のうち、検索可能暗号と属性ベース暗号にかかる実装の現状、講演 1 で想定した高機能暗号活用のケースにおける実装面の課題について、次のとおり発表した。

（１）公開鍵暗号型の高機能暗号の開発動向

検索可能暗号は、データを暗号化したままキーワード検索を実行する機能を実現する方式である。三菱電機では、データベースに公開鍵暗号型の検索可能暗号を実装するためのソフトウェアの研究開発を行っている。これは、サービス利用者の端末に組み込む「暗号化・復号用ソフトウェア」とクラウド・サービス事業者のサーバに組み込む「検索用ソフトウェア」で構成される。

また、三菱電機グループでは、属性ベース暗号を用い、企業間での安全なデータ共有サービスを提供している。このサービスにおいては、データを暗号化する企業の担当者は、アクセスを許可するデータの開示範囲や担当者の属性を効率的に制御することができる。また、属性ベース暗号と準同型暗号を組み合せて機能の実用性を向上させる方式についても研究開発を進めている。

（２）公開鍵暗号型の高機能暗号の実装上の留意点

検索可能暗号と属性ベース暗号をシステムに実装する際には、各エンティティにおける秘密鍵の安全な管理方法を検討することが重要である。また、既

存のシステムへの適用を検討する場合には、当該システムとの親和性やコストを抑えられるような導入方法を検討する必要がある。

属性ベース暗号の暗号化や復号処理は、現状十分な処理速度を達成している。一方でシステムに適用する際の留意点としては、各エンティティの秘密鍵を生成する機関の選定方法の検討が挙げられる。秘密鍵を生成できる権限は、エンティティの参加認否を決定するという非常に強力な権限であるため、この権限をどの機関が有し、秘密鍵を生成するための情報（秘密鍵生成用の鍵や各エンティティの属性等）をどのように管理するのかを予め検討する必要がある。同様の検討は、検索可能暗号をシステムに適用する際にも必要となる。ただし、これらの検討は、システムやその用途、およびコストによって適した管理方法が異なるため、個々のアプリケーションごとに、設計段階からセキュリティ分析を行ったうえで導入する必要がある。

５．講演３「共通鍵暗号型の高機能暗号の研究動向」

芦原は、高機能暗号のなかで共通鍵暗号型として分類される方式のうち、検索可能暗号に焦点を当てて、その機能、安全性要件、処理性能の評価について、次のとおり発表した。

（１）共通鍵暗号型の検索可能暗号のモデル

検索可能暗号は、講演１および２で発表された公開鍵暗号型の方式のほかに、共通鍵暗号型の方式が存在する。公開鍵暗号型の方式では、不特定多数のエンティティがクラウド・サービス事業者へデータを預託可能である。共通鍵暗号型の方式では、クラウド・サービス事業者内のサーバ上で大量のデータを効率良く検索可能である。

共通鍵暗号型の検索可能暗号では、サービス利用者は、事前に秘密鍵を用いて、預託するデータの暗号化と「暗号化インデックス」の生成を行い、それらをクラウド・サービス事業者のサーバに送信する[5]。キーワード検索を行う際には、サービス利用者は、検索キーワードを秘密鍵で暗号化し、「トラップドア」と呼ばれるデータを生成してサーバに送信する。サーバは、トラップドアと暗号化インデックスを用いて暗号化したまま検索処理を実行し、その結果（検索キーワードを含む暗号化されたデータ）をサービス利用者に送信する。サービス利用者は、それを復号し検索キーワードを含むデータ（平文）を得る。

安全性については、クラウド・サービス事業者に預託したサーバ内のデータ

[5] 暗号化インデックスは、サーバに対してデータやキーワードを秘匿したまま効率的に検索処理を実行するために用いられる。

全てを入手できる攻撃者を想定する場合が一般的である。そのうえで、「当該攻撃者が、①預託されているデータの内容、②各データに含まれるキーワードや検索キーワード、③データとキーワードの対応関係を推測することができない」というデータの機密性にかかる安全性要件を設定し、それを満たす方式が数多く提案されている。データの完全性については、別途、データの改ざんを検知する手段を利用する必要がある。

（２）処理性能の評価

検索可能暗号を利用する際には、データ登録やキーワード検索の処理にかかる計算量やデータのサイズが実用的な範囲内におさまる必要がある。各処理にかかる計算量とデータのサイズのうち、①暗号化インデックスのサイズ、②トラップドアのサイズ、③検索処理にかかる計算量を、処理性能の代表的な評価尺度とみなすことができる。

大量のファイルを検索可能暗号によってキーワード検索するケースを想定し、国際会議等で近年提案された 7 つの実現方式について、預託するファイル数の増加に対し、上記の各評価尺度の値がどのように変化するかを分析した。その結果、全ての評価尺度において性能の良い方式は存在しなかった。検索可能暗号を使用する際には、想定する用途に適した方式を採用し、効率良く実装することが重要である。

６．講演４「共通鍵暗号型の高機能暗号の実装にかかる動向」

吉野は、クラウド・サービス事業者における共通鍵暗号型の検索可能暗号の実装例と当該事例の処理性能について、次のとおり発表した。

（１）検索可能暗号の実装

クラウド・サービス上で共通鍵暗号型の検索可能暗号を実装する際には、サービス利用者の端末やクラウド・サービス事業者のサーバへの負担に配慮する必要がある。日立製作所では、既存の検索エンジンに共通鍵暗号型の検索可能暗号を適用するソフトウェアを提供している[6]。この製品は、サービス利用者やサーバへの負担を抑えつつ、既存の検索エンジンの機能を暗号化したまま利用可能とするものであり、現在、マイクロソフト社のクラウド・サービス「Microsoft

[6] 検索エンジンとは、与えられた文書のデータに対してキーワード検索の機能を提供するソフトウェアである。ここで紹介された検索可能暗号は、既存の検索エンジンの構成要素のひとつとして組み込まれる。例えば、代表的なオープンソースの検索エンジンとして知られる「Apache Solr」に適用することで、ワードやエクセル、パワーポイント等のファイルに含まれる単語をキーワードとして検索する機能を有する。

Azure」上で即時に利用を開始できる状態で提供している。こうしたサービスの他にも、患者情報をクラウド上で安全に保存・検索するサービスを医療機関に提供した事例もある。

（２）実装された方式の処理性能

日立製作所の検索可能暗号では、既存の検索エンジンを用いて各データとキーワードの対応関係を示すデータを生成し、秘密鍵を用いて暗号化インデックスを生成する。暗号化したデータとともに暗号化インデックスをクラウド・サービス事業者に預託することで、クラウド・サービス上で安全かつ効率的にキーワード検索を実行することができる。

この方式の処理性能は、「Apache Solr」等の検索エンジンの性能に依存する。また、暗号化インデックスのサイズや検索処理にかかる計算量は、預託するデータ全体に含まれるキーワードのバリエーションの総数に依存する。クラウド・サービス事業者に大量のデータを預託している場合、使用頻度の高いキーワードの大半は既に暗号化インデックスに含まれていると考えられる。預託するデータの数がさらに増加しても、新規登録が必要となるキーワードは使用頻度の低いものに限定されることから、暗号化インデックスのサイズの増加が抑えられる。したがって、預託するデータ量に対してスケーラブルで実用的な方式といえる。

７．パネル・ディスカッション「金融分野での高機能暗号の活用に向けて」

冒頭、**廣瀬**は、Microsoft Azure 上で安全にデータ交換を行う仕組みにかかる研究動向や、高機能暗号（主に準同型暗号）を巡る研究開発の動向について発表した。そのうえで、高機能暗号の活用が金融分野に与える影響や活用に際しての課題等について以下のとおり議論が行われた。

（１）高機能暗号の活用が金融分野に与える影響

モデレータの**松本**は、金融分野の高機能暗号を活用しうる分野や事例について、パネリストに意見を求めた。

鎌田は、ブロックチェーン技術や講演 1 で示されたクラウド・サービスを利用した業務等が想定されるとの見解を示した。特に、ブロックチェーン技術での活用については、当該技術を検討しているコミュニティにおいて認知されつつあると補足した。また、金融機関におけるデータ管理に高機能暗号を適用し、システム構成のスリム化や効率性の向上を実現できるとすれば、これも金融分野でのニーズとして挙げられるのではないかと説明した。

長沼は、金融分野では、クラウド・サービスを利用した電子メール・システムのようなバックエンドのシステムで検索可能暗号のニーズがあると述べた。また、医療分野において、電子カルテ等を管理するシステムで検索可能暗号のニーズがあり、既に導入事例もあると付言した。

平野は、金融機関の ATM 等で利用される生体認証に応用する（暗号化したまま生体情報の照合を行い認証する）というニーズがあるのではないかと述べた。

廣瀬は、ブロックチェーンのトランザクションを準同型暗号で暗号化したうえで、暗号化したままトランザクションの検証処理を行うなどの実験をマイクロソフト社で行っていると説明した。また、ブロックチェーンに属性ベース暗号を活用することにより、電子カルテや登記簿等を複数の組織間で分散管理するとともに、閲覧権限者を柔軟に制御できると述べた。

ブロックチェーンへの活用に関して、**長沼**は、準同型暗号と属性ベース暗号を組み合わせてブロックチェーンに適用し、従来のアクセス制御サーバを用いずにブロックへのアクセスを制御することが可能になるとの見方を示した。

ここで、**フロア参加者**より、高機能暗号はクラウド・サービス事業者が行う処理を効率化するという観点からのニーズがありうるとの発言があった。クラウド・サービス事業者は、サービス利用者から預託されたデータは原則暗号化する必要があり、その処理にかかるコストを高機能暗号の利用により削減できる可能性があると説明した。クラウド・サービスで処理されるデータのサイズと計算量を高機能暗号を用いて削減できれば、使用するリソースに応じて課金するタイプのサービスにおいては、サービス利用者はより安い料金でサービスを受けられる可能性もあるとの見方を示した。

これに対して、**長沼**は、高機能暗号は従来の暗号と比較して鍵や暗号文のサイズが大きいことや、演算処理に必要な計算量が相応に発生することから、コストや料金の低下につながるとは必ずしも言えないとコメントした。

鎌田は、ニーズについて調査することは重要であるが、高機能暗号の利用を所与とするべきではないと指摘した。さらに、高機能暗号を利用することによるセキュリティの効果は、従来の暗号と運用面での対策を組み合せることでも実現できることが多く、セキュリティ・レベルの向上や運用コスト削減等のメリットを金融機関に対して具体的に示すことが必要であると説明した。

こうした考え方に対して、**長沼**は、高機能暗号活用のメリットを一般的かつ定量的に示すことが現時点では難しく、導入を検討する企業のニーズに応じてメリットを説明するとともに、機能や運用方法等を調整する場合が多いと説明した。

平野は、クラウド・サービスが提供され始めた当初は、業務にどのように活用できるかが明確ではなかったが、その後、多様なニーズが生まれ、さまざま

なエコシステムに組み込まれるようになったと説明した。高機能暗号についても、今後ニーズが明確になってくるのではないかと述べた。

以上の議論を踏まえて、**松本**は、金融分野ではブロックチェーンやクラウド・サービスを用いるさまざまなエコシステムで高機能暗号のニーズがありうると説明した。また、金融分野でのニーズをより具体化していく過程において、他分野（医療分野等）での導入事例を参考にすることが有用であると述べた。他方、ニーズを検討する際には、高機能暗号の利用を前提とするのではなく、従来の暗号等を利用した場合と比較して、その効果を具体的に整理する必要があると述べた。

（２）高機能暗号を活用することのメリットとデメリット

松本は、高機能暗号を利用することのメリットやデメリットについてパネリストに意見を求めた。

廣瀬は、準同型暗号（特に完全準同型暗号[7]）には、暗号処理に要する計算量が相対的に大きいというデメリットがあるものの、クラウド・サービスでは活用する際に計算リソースを柔軟に拡張できるため、このデメリットは解消される可能性があると述べた。

平野は、暗号処理コストは運用を工夫することによって削減することができると補足した。すなわち、全てのデータに対して高機能暗号を用いて暗号化を行うのではなく、データの重要度を整理し、必要なデータを絞り込んだうえで暗号化することによって、計算量を削減することが考えられると述べた。

松本は、高機能暗号で大規模なデータを処理するためには、暗号処理コストの削減だけではなく、当該処理に要するエネルギーの削減も重視されるとの見解を示した。これらの削減を十分に行うためには、ソフトウェア実装だけでは困難であることから、ハードウェア実装が必要となる点を説明したうえで、横浜国立大学では、このハードウェア実装に関する研究を進めており、現在、世界最高水準の暗号処理速度を達成できていると補足した。

一方、**長沼**は、企業による導入が進まない要因として、高機能暗号を既存のデータベースに実装する際に、当該データベースの改修が必要となることが挙げられると述べた。

これに対して、**鎌田**は、金融分野で既に稼働している既存のシステムを改修して新しい仕組みを実装することは、安定性等の観点から容易ではないと指摘

[7] 完全準同型暗号とは、暗号化したデータに対して加算と乗算の両方を、回数に制限なく演算できる方式である。

した。そのうえで、システム更改のタイミングにおいて、設計段階から高機能暗号を実装するという対応が有効であると説明した。

四方は、クラウド・サービス上で高機能暗号を利用するメリットは、構造上、預託したデータのセキュリティ（プライバシー保護等）を保ちつつ、クラウド・サービス事業者から、鍵の生成・管理を安全に切り分けることが可能な点にあると説明した。このことは、クラウド・サービス事業者は鍵の運用コスト削減、サービス利用者は信頼できる機関等に鍵を安全に預託可能というメリットがある。この点から、高機能暗号の活用がさらに広がることが期待できるのではないかと述べた。

ここで、**松本**は、これまでの議論が主に公開鍵暗号型の高機能暗号を対象としたものであることを説明したうえで、共通鍵暗号型の高機能暗号のメリットとデメリットについて意見を求めた。

長沼は、共通鍵暗号型は公開鍵暗号型と比較して暗号処理が高速であるというメリットがあると説明した。もっとも、データの暗号化は秘密鍵を持つエンティティのみが可能であるという性質上、その用途は限定的とならざるを得ないとの見解も示した。

（３）高機能暗号の共通化や標準化

松本は、ベンダー等が個別に高機能暗号を開発すると、競争によるイノベーションが期待できる反面、高機能暗号の標準化が進まない可能性があるとの問題提起を行った。そのうえで、この問題を解決する方法について、パネリストに意見を求めた。

廣瀬は、多くの金融機関が同一の高機能暗号を利用できるようにする方法として、クラウド・サービス事業者が高機能暗号が実装されたソフトウェア開発キット（Software Development Kit：SDK）を開発・配付するという方法が考えられると説明した。

鎌田は、共通の高機能暗号を各金融機関が採用すれば、それらが保有している暗号化データの全てを対象とした、横断的な検索や統計処理等が実現する可能性があるとコメントした。

四方は、高機能暗号は、ある方式から別の方式を実現できるという関係性（例えば、準同型暗号から検索可能暗号を実現できる）を有することが知られていると説明した。そのため、異なった高機能暗号の方式を複数の金融機関が採用したとしても、方式間の差異を補足・変換するツールを利用することによって、横断的な検索や統計処理を実現することは理論的には可能であると述べた。

ここで、**フロア参加者**から、高機能暗号を普及させるためには、CRYPTREC暗号リストに選定されるとか、金融業界全体で統一の選定基準を策定するなどの対応が必要ではないかとの質問が寄せられた。

鎌田は、金融分野で高機能暗号の利用を検討するうえで、そうした信頼できるリストに選定されているとか、評価基準が整備されていることが望ましいとの見解を示した。

平野と**長沼**は、現在、ベンダーが高機能暗号の開発競争を行っている段階であることから、標準化には相応の時間が必要であると述べた。そのうえで、各ベンダーは、自社の方式をデファクト・スタンダードとすることを目指しているのが実情であると説明した。

鎌田は、学界やベンダーが金融業界のニーズを確りと把握できるようなフレームワークの構築が欠かせないとしたうえで、金融業界と研究者がディスカッションや実験を行う場を整備し相互の理解を深めていることが重要ではないかとの見解を示した。具体的なアプリケーションでの導入・運用コスト、セキュリティ・リスクの分析結果を踏まえた総合的な判断が必要であり、そうした評価を可能とする手法の検討も重要であるとコメントした。

ここで、**鎌田**は、パネリストに対して、高機能暗号が標準化され実際に利用されるようになるには今後どの程度の期間が必要かと質問した。

松本は、金融業界のニーズの強さによって標準化が実現する時期は変化すると述べた。

廣瀬は、マイクロソフトの研究部門においては、高機能暗号のハードウェア実装に関する研究が主流であるとしたうえで、機械学習への適用事例等を鑑みると、3 年以内に実用化の時期が判明するのではないかとの見方を示した。もっとも、それは技術的な観点からの見通しであり、サービスとして提供されるようになるか否かとは別問題であると述べた。そして、金融分野で高機能暗号のニーズが存在し、クラウド・サービス上での提供を望むのであれば、そうした要望を表明していく必要があるのではないかとの見方を示した。

松本は、以上の議論を総括して、技術的には近い将来、実用に耐えうる方式が開発され、標準化や共通化に先行して、個々の企業によって高機能暗号が徐々に利用されるようになっていく可能性が高いのではないかと説明した。

（４）量子コンピュータの脅威への対応

松本は、現行の暗号方式から高機能暗号への移行時期やその際に使われる暗号方式の選定基準をどのように考えたら良いのか、との問題提起を行った。

四方は、現在の高機能暗号の構成にあたっては、ペアリング関数、または格子と呼ばれる数学的な仕組みが主に利用されていると説明した。そのうえで、

ペアリング関数を利用する場合のメリットは、格子を利用するよりも効率が良く、高い実用性が実現できることであると述べた。一方、格子を利用する場合のメリットは、耐量子性（量子コンピュータでも容易に解くことができない性質）や完全準同型暗号等の一部の高機能暗号を容易に実現できることであると述べた。そのうえで、どちらを利用した方が良いかは、量子コンピュータの実用化時期がひとつのポイントになると付言した。その具体的な時期を推測するのは困難であるが、現在、米国政府は、量子コンピュータに耐性のある公開鍵暗号（耐量子暗号）の標準化活動を進めており、わが国もこの動向を注視すべきであると指摘した。さらに、移行時期や暗号方式を検討する際には、暗号化するデータのセキュリティを担保したい期間やセキュリティのレベルも考慮すべきであると指摘した。例えば、長期間に亘り機密性を確保したいのであれば、耐量子性のある格子型の高機能暗号を選択することが考えられると述べた。

これを受けて、**長沼**は、量子コンピュータの実現が公表される時期を、事前に予測することは困難であり、ある日突然公表される可能性もあるとの見方を示した。そのうえで、耐量子暗号に速やかに移行できるよう準備を今から開始することが必要であるとの見解を示した。

全体の議論を総括して、**松本**は、金融業界において、高機能暗号を活用するニーズが存在するといえるものの、実際に高機能暗号を活用した金融サービスを実現させていくためには、具体的なニーズや金融機関にとってのメリットを明確にしていく必要があると説明した。そのうえで、研究者、ベンダーおよび金融機関がディスカッションできる場を構築していくなどの環境構築が重要であるとの見方を示した。さらに、今後、高機能暗号の導入を考える際には、データの機密性を保持する期間を考慮し、量子コンピュータに対して耐性を有する高機能暗号の導入を検討することも必要であると述べて、パネル・ディスカッションを締め括った。

以　上