Vol.2017-CSEC-78 No.13
Vol.2017-SPT-24 No.13
2017/7/14

金融分野における高機能暗号の活用と今後の課題

宇根正志 †

概要：日本銀行金融研究所では，金融分野における高機能暗号の活用について議論するために，「第 18 回情報セキュリティ・シンポジウム」を開催した．本稿では，同シンポジウムにおける講演やパネル・ディスカッションで示された意見に加え，今後の課題についても説明する．

キーワード：金融サービス，クラウド・コンピューティング，検索可能暗号，高機能暗号，準同型暗号，属性ベース暗号，FinTech

Making Use of Advanced Cryptosystems and Research Topics in Financial Sector

MASASHI UNE†

Abstract: The Institute for Monetary and Economic Studies of the Bank of Japan held the 18th Information Security Symposium in order to discuss how to make use of advanced cryptosystems in the financial sector. This paper will summarize opinions and future research topics expressed at the presentations and panel discussion of the symposium.

Keywords: advanced cryptosystem, attribute-based encryption, cloud computing, FinTech, homomorphic encryption, searchable encryption

1. はじめに

金融サービスの提供には，情報セキュリティ技術の適切な活用が不可欠である．実際，PC やモバイル端末を利用したオンライン・バンキングでは，通信路上でやり取りされる金融取引にかかるデータの機密性や一貫性を確保したり，取引相手を認証したりするために，暗号技術が利用されている．また，ATM 等における取引では，暗号技術をキャッシュカード上で安全に実装するために，IC チップ等の暗号ハードウエア実装技術（暗号モジュール技術）が活用されている．

金融サービスのセキュリティを確保していくためには，新しい金融サービスの登場やそれに伴う環境変化にも留意することが必要である．例えば，新しいサービスにおいて，金融取引に関与する主体が多様化したり，新しい技術が活用されたりする場合，金融取引にかかる情報をどのように取り扱うか，また，新技術のセキュリティをどう評価するかといった問題が生じる．近年注目を集めている FinTech に関しても，情報セキュリティ上の課題の有無や対応について検討することが重要である．

こうした金融機関の対応を支援するために，日本銀行金融研究所は，中長期的な観点から，金融分野に関連が深い情報セキュリティ技術とその課題について研究し，情報セキュリティ対策を進める際の留意点等を示す研究論文を公表している[1]．また，学界での研究が金融業界のニーズにマッチしたものとなるように，情報セキュリティにかかる金融機関のニーズや課題についても検討し，学会で発表している[2][3]．

日本銀行金融研究所では，金融分野における高機能暗号の活用をテーマとする「第 18 回情報セキュリティ・シンポジウム」（開催日：2017 年 3 月 9 日（木），場所：日本銀行本店）を開催した．本稿は，同シンポジウムで行われた講演やパネル・ディスカッションの内容を説明し，金融分野における今後の高機能暗号の活用に向けた課題等を示す．

本稿で示されている意見は，すべて著者個人に属し，日本銀行の公式見解を示すものではない．また，あり得べき誤りはすべて著者個人に属する．

2. 第 18 回情報セキュリティ・シンポジウム

2.1 概要

第 18 回情報セキュリティ・シンポジウム（以下，単に，シンポジウムという）では，「新たな金融サービスを支えうる高機能暗号：セキュリティと利便性の両立に向けて」をテーマとして 4 件の講演とパネル・ディスカッションを行った[4]．これらの講演等のタイトルや講演者は以下のとおりである（敬称略，各参加者の所属や役職名はシンポジウム開催時点のものであることに留意されたい）．

- 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）

† 日本銀行金融研究所情報技術研究センター
Center for Information Technology Studies, Institute for Monetary and Economic Studies, Bank of Japan

ⓒ 2017 Information Processing Society of Japan

Vol.2017-CSEC-78 No.13
Vol.2017-SPT-24 No.13
2017/7/14

図 1　金融機関によるクラウド利用率の推移
（備考）参考文献[5]の図表 5-2 を引用して作成.

表 1　高機能暗号の主な実現方式

暗号方式	機能
準同型暗号	データを秘匿したまま，四則演算が可能
属性ベース暗号	データを秘匿したまま，復号するエンティティの属性に合わせてアクセス制御が可能
検索可能暗号	暗号化されたままデータ検索が可能
代理再暗号化	暗号文の指定復号者を変更する際に，暗号文を別の暗号文に復号しないで変換可能
放送暗号	データを秘匿したまま，復号するエンティティのアクセス制御が可能
しきい値暗号	しきい値以上のデータにより復号可能
漏洩耐性暗号	鍵が漏えいしても解読を防止することが可能
タイムリリース暗号	時刻による復号制御が可能

（備考）参考文献[6]のスライド 13 を引用して作成.

- 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　鎌田敬介
  三菱電機主席研究員　平野貴人
  日立製作所研究員　長沼健
  日本マイクロソフト　廣瀬一海

2.2 問題意識

近年，金融分野において，FinTech と総称される新しい金融サービスが注目を集めているほか，金融機関によるクラウド活用も徐々に広がってきている（図 1 を参照）[a]. こうした金融環境の進展を背景として，今回のシンポジウムでは，FinTech やクラウドで取り扱われる金融取引データ等のセキュリティと利便性を両立させるための技術として「高機能暗号」を取り上げた．高機能暗号は，データを暗号化したまま（復号せずに）四則演算を実行可能であるなど，通常のデータの暗号化／復号に加えて，より高度かつ多彩な機能を実現する暗号の総称である（表 1 を参照）. 今後，FinTech やクラウド活用の拡大に伴い，金融機関やその顧客以外のエンティティ（FinTech 企業やクラウド事業者等）が金融取引データ等を取得し処理する場面が増えてくると予想される. その結果, サイバー攻撃等によって，第三者のエンティティから金融取引データ等が流出するリスクも高まる．その際，金融機関が高機能暗号によって金融取引データ等を暗号化し，そのままクラウド事業者等に渡して処理を依頼することができれば，そうしたリスクの低減につながる．加えて，クラウド事業者等がデータを処理する際に当該データの復号が不要となるなど，データの処理性能が向上する可能性もある.

シンポジウムでは，金融分野において高機能暗号を活用する際のモデルケースが提示されたほか，高機能暗号にかかる最新の研究や製品・サービス化の動向を踏まえつつ，金融分野における高機能暗号活用の可能性が議論された.

2.3 各講演の概要

(1) 公開鍵暗号型の高機能暗号の研究動向

第 1 の講演では，高機能暗号のうち，公開鍵暗号型を取り上げ，「準同型暗号」と「属性ベース暗号」に関して，それらの特徴や安全性要件，高機能暗号の適用が想定されるアプリケーションについて説明が行われた[7]. 具体的には，高機能暗号の適用が想定されるアプリケーションとして，FinTech における代表的なサービスのひとつである「口座情報サービス（account information services)」のモデルと，クラウドを利用した「営業支援システム」のモデルが取り上げられた[8].

口座情報サービスのモデル では，ノンバンク（FinTech 企業等）が金融機関の顧客の要望に応じて当該金融機関から口座情報（口座残高，取引履歴等）を取得し，それらを加工して顧客に提供するというケースを想定した（図 2 を参照）. 金融機関は, ノンバンクに口座情報を送信する際に，それを高機能暗号で暗号化する．ノンバンクは，暗号化さ

a) シンポジウム参加者を対象に実施したアンケートで，金融機関の実務者からの回答をみると，FinTech やクラウドのセキュリティに高い関心が寄せられていることが読み取れる．同アンケートについては付録を参照されたい.

ⓒ 2017 Information Processing Society of Japan

Vol.2017-CSEC-78 No.13
Vol.2017-SPT-24 No.13
2017/7/14

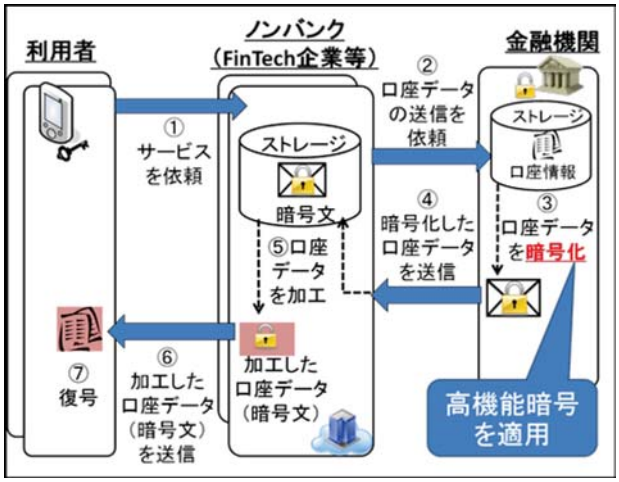

図 2　口座情報サービスへの高機能暗号の適用例（概念図）
（備考）参考文献[7]の図表 10 を引用して作成.

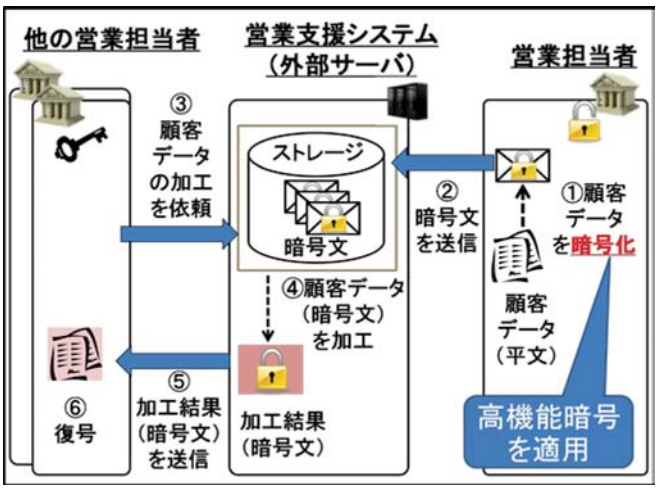

図 3　営業支援システムへの高機能暗号の適用例（概念図）
（備考）参考文献[7]の図表 6 を引用して作成.

れた口座情報をそのまま加工し，その結果となるデータを利用者に送信する. 利用者はそれを復号し, 加工された（平文の）口座情報を得る.

営業支援システムのモデル では, 金融機関の営業担当者がクラウドに顧客データを預託し，閲覧権限を有する他の営業担当者と共有・活用するというケースを想定した（図 3 を参照）. 営業担当者は，顧客データを高機能暗号で暗号化したうえでクラウドに預託する. 他の営業担当者がクラウドに預託された（暗号化済みの）顧客データを加工・入手したい場合，クラウドは暗号化された顧客データをそのまま加工して送信する. 当該営業担当者はそれを復号し，加工済みの（平文の）顧客データを得る.

上記のモデルでは，暗号化されたデータの四則演算を準同型暗号によって実現するほか，データの復号権限の制御を属性ベース暗号によって効率的に実施することを企図している. 本講演では，高機能暗号を利用した場合，通常の暗号と比較して，情報流出リスクや鍵管理のコストを軽減できる反面，暗号化処理にかかるコストが増加する可能性があるという分析結果が示された.

(2) 公開鍵暗号型の高機能暗号の実装にかかる動向

第 2 の講演では，第 1 の講演で取り上げられた準同型暗号や属性ベース暗号について，実装状況と取り組むべき課題が示された. 準同型暗号 については，既に，暗号文に対する回帰分析やハミング距離計算等が実施可能となっているが，分析処理が複雑であり，データ件数によっては処理性能が低下する可能性があるとの説明があった. とはいえ，この分野でも，属性ベース暗号との組合せなど，実用化に向けた研究は着実に行われている.

属性ベース暗号 については, 暗号化データベースに同暗号を実装するサービスが既に提供されており，処理速度等の性能面でも実用レベルに達している事例が紹介された. また，運用上の留意点として，秘密鍵が復号権限の制御に用いられることから，秘密鍵の生成や管理にかかる権限の運用を，従来の公開鍵暗号の場合以上に厳格に実施する必要があるとの見方が示された.

(3) 共通鍵暗号型の高機能暗号の研究動向

第 3 の講演では，共通鍵暗号型の高機能暗号のうち，暗号化したままファイルのキーワード検索を実現する「検索可能暗号」に焦点を当てて，安全性要件や処理性能評価について説明が行われた[9]. 検索可能暗号を用いると，機密性を有するファイルをクラウドに預託する際，当該ファイルを事前に暗号化しておくことで，クラウド事業者に対してファイルの内容を秘匿しつつ，閲覧したいファイルをキーワード検索して入手することができる. 検索可能暗号には，共通鍵暗号型のほか公開鍵暗号型も存在するが，共通鍵暗号型の方が公開鍵暗号型に比べて高速での処理が可能であるため，膨大なデータの検索・演算に向いている.

本講演では，こうした「ビッグデータ解析での検索可能暗号の利用」を想定し，クラウドに預託されるファイル数の増加に伴って計算量やデータサイズがどう変化するかを代表的な実現方式（7 件）に関して評価・比較した. その結果，計算量やデータサイズなど複数の評価尺度の間でトレード・オフ関係が存在し，すべての評価尺度において最適な方式は現時点では提案されていないとの説明があった.

(4) 共通鍵暗号型の高機能暗号の実装にかかる動向

第 4 の講演では，共通鍵暗号型の検索可能暗号における実装状況と処理性能評価の留意点が示された. 実装状況に関しては，検索エンジンに検索可能暗号を適用するソフトウエアが提供されていることや，医療分野において，クラウド上で検索可能暗号を実装し，患者の情報を暗号化して

ⓒ 2017 Information Processing Society of Japan

Vol.2017-CSEC-78 No.13
Vol.2017-SPT-24 No.13
2017/7/14

当該クラウドに預託・管理するサービスの事例等が紹介された.

処理性能の評価は，実装方式だけでなく，どの検索エンジンを利用するかといった点にも依存する場合がある．このため，実際に処理性能を評価する際には，検索エンジンの種類についても考慮する必要があるとの見方が示された.また，第 3 の講演で取り上げられた「預託されるファイル数」以外のパラメータが処理性能を左右するケースもある.このため，実現方式の特性やアプリケーションの要件等を理解しつつ，どの評価尺度を重視するかを検討する必要があるとの説明があった.

2.4 パネル・ディスカッション

パネル・ディスカッションでは,「金融分野での高機能暗号の活用に向けて」をテーマに，高機能暗号の活用が金融分野に与える影響や今後の活用に向けた課題を主な論点として議論した．以下では，各論点に関するパネリストの主な意見やコメントを示す.

(1) 高機能暗号を活用するメリット・デメリット

【メリット】

- ノンバンクやクラウド事業者等の「データの受け手」が復号用の鍵を管理するのではなく，「データの出し手」である金融機関が鍵を管理しデータの機密性を自ら制御可能となる.
- 管理する必要がある鍵の種類が減少するなど，鍵の管理にかかる負担が通常の暗号に比べて低減する場合がある.
- 使用する計算リソースに応じて課金されるクラウド・サービスの場合，金融機関がデータを暗号化することでクラウド事業者等における暗号化等の処理量が削減され，計算リソース使用量低下によってクラウド・サービスの利用料金も低下する可能性がある.

【デメリット】

- 高機能暗号では，一般に，暗号化や復号にかかる計算量等が通常の暗号に比べて増加する傾向がある.
- 既存の金融サービスや金融機関業務のシステムに高機能暗号を適用する場合，それらのシステムやデータベースを改修する必要が生じ，そのコストやシステムのディグレードが発生する可能性がある.

(2) 高機能暗号の主なアプリケーション

金融分野において高機能暗号の活用が想定されうるアプリケーションとして，第 1 の講演で説明された営業支援サービスや口座情報サービスに加えて，以下のアプリケーションが挙げられた.

- ATM 取引等で利用される生体認証（生体情報を秘匿したまま照合・判定）
- 分散台帳上のトランザクション処理（トランザクションを暗号化したまま検証）やノードのアクセス制御（鍵管理等の負担軽減）
- 金融機関が取扱うデータのマスキングやデータベースへのアクセス制御（鍵管理等の負担軽減）

(3) 今後の高機能暗号の活用に向けた課題

今後，金融分野において高機能暗号を活用していく際の主な課題として，以下の意見が出た.

- 高機能暗号の導入にかかるコスト，既存の暗号等に基づくシステムと比較した際のメリット・デメリット，サービス利用者や金融機関にとっての利便性等を明確にすることなしに，金融分野での活用を検討することはできない.
- CRYPTREC 暗号リストのような信頼できる暗号リストに加えるといったことを通じて，高機能暗号に対する信頼感を醸成していくことが重要である．そのためには，安全性等の観点から高機能暗号の評価手法を検討・確立していくことが求められる.
- 金融分野では，高機能暗号がどのようなものかについての認識がまだ薄いのが実情である．金融機関と研究者が意見を交わし，高機能暗号の特徴やメリットに関する情報を共有し理解を深めるための場を整備することも有用である.
- 金融機関の既存のシステムを高機能暗号導入のために改修するのはハードルが高い．新しいサービスを提供するために新しいシステムを導入することがあれば，それに合わせて高機能暗号の採用を検討する，あるいは，既存のシステムの大規模な改修を実施する際に採用を検討することが現実的である.
- 高機能暗号は，既に，クラウド・サービス上で活用されており，現時点での主な活用分野は医療分野である.今後，金融分野において高機能暗号の活用を検討していく際には，医療分野で先行活用されている事例を参考にすることが有用である.
- 長期的な利用を想定する場合，量子コンピュータの実現に留意し，格子暗号等，量子コンピュータに耐性を有する方式の採用を検討することが必要である.

3. 今後の課題

講演やパネル・ディスカッションでの議論を踏まえると，高機能暗号の活用に向けた今後の課題として，まず，高機能暗号の安全性やコスト面での評価手法の開発 が挙げられる．現在，さまざまなタイプの高機能暗号が提案されているが，既存の暗号方式との横並びでの比較を可能とする評価手法は筆者の知る限りまだ存在しないようである．また，長期的な利用を想定する場合，量子コンピュータへの耐性の評価 も必要であると考えられる.

こうした手法による評価結果に基づく 高機能暗号の標準化 も課題となるといえる．CRYPTREC 暗号リストへの高機能暗号への掲載等，一定の安全性等を有する暗号として位置づけられることになれば，金融機関をはじめとする

ⓒ 2017 Information Processing Society of Japan

暗号利用者の信頼感が醸成されるようになると期待される．標準化を進めるにあたっては，暗号利用者側のニーズも踏まえた検討が必要であり，金融機関と研究者との間で情報共有等を進めていくことも重要である．

4. おわりに

本稿では，高機能暗号をテーマとする第 18 回情報セキュリティ・シンポジウムでの議論の内容を紹介した．講演やパネル・ディスカッションでは，金融分野で活用が想定されうるアプリケーションや高機能暗号の実装動向が紹介されたほか，高機能暗号のメリット・デメリット，今後の高機能暗号の活用に向けた課題について議論された．今回示された課題への対応等について引き続き注目していきたい．

参考文献

[1] 日本銀行金融研究所，「日本銀行金融研究所ホームページ」，2017 年（URL：http://www.imes.boj.or.jp/citecs/, 参照 2017-03-31）．
[2] 井澤秀益，「金融業界において注目されている情報セキュリティ上の課題について」，コンピュータセキュリティシンポジウム 2015 予稿集，情報処理学会，2015 年．
[3] 中村啓佑・宇根正志，「金融業界において注目されている情報セキュリティ上の研究課題：認証技術に焦点を当てて」，『情報処理学会研究報告』vol. 2016-CSEC-74，no. 15，情報処理学会，2016 年．
[4] 日本銀行金融研究所，「日本銀行金融研究所情報技術研究センター 第 18 回情報セキュリティ・シンポジウム 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」，2017 年（URL：http://www.imes.boj.or.jp/citecs/symp/18/ index.htm，参照 2017-03-31）．
[5] 金融情報システムセンター，「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．
[6] 松本勉，「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”」，第 18 回情報セキュリティ・シンポジウム配付資料，日本銀行金融研究所，2017 年（URL：http://www.imes.boj.or.jp/citecs/symp/18/ref2_matsumoto.pdf，参照 2017-03-31）．
[7] 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」，IMES Discussion Paper Series，no. 2017-J-8，日本銀行金融研究所，2017 年．
[8] 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」，IMES Discussion Paper Series，no. 2016-J-14，日本銀行金融研究所，2016 年．
[9] 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」，IMES Discussion Paper Series，no. 2017-J-7，日本銀行金融研究所，2017 年．

付録　金融機関の実務者からのアンケート

シンポジウム当日の参加者（約 100 名）を対象にアンケート（無記名，所属組織の業態のみを選択）を実施し，金融機関の実務家から 19 件の回答を得た（全体では 66 件）．

アンケートの主な質問事項は，今後の情報セキュリティ・シンポジウムで取り上げてほしいテーマを問うもの（質問イ），足許の情報セキュリティ上の課題を問うもの（質問ロ），金融サービスを提供するシステムにおいて先行き攻撃対象となりうる部分を問うもの（質問ハ）の 3 項目である．具体的には，各質問は以下のとおりである．

- 質問イ：今後シンポジウムで取り上げてほしいトピックを選択肢から 3 つ以内でお選びください．
- 質問ロ：日本ネットワークセキュリティ協会による「JNSA 2016 セキュリティ十大ニュース」の各種ニュースにおいて，貴社においても同様の課題があると思われる項目や，貴社にも影響が大きいと思われる項目を選択肢から 3 つ以内でお選びください．
- 質問ハ：今後貴社においても脅威となりえると考えられる項目（金融サービスを提供するシステム全体における攻撃箇所に着目した整理）を選択肢から 3 つ以内でお選びください．

これらの質問の選択肢，金融機関の実務者からの回答を集計した結果は，以下のとおりである（表 A-1 を参照）．

(1) 今後取り上げてほしいトピック：FinTech とクラウド

質問イ（今後シンポジウムで取り上げてほしいトピック）では，「FinTech の最新動向およびセキュリティ（**イ-1**）」が最も高い回答率（58%）であった．これに次いで高い回答率（37%）となったのが，「クラウドのセキュリティ（**イ-3**）」であった．

(2) 2016 年のニュース：AI のセキュリティ分野への影響

質問ロ（最近の情報セキュリティ上の課題）では，「AI 技術のセキュリティ分野への影響（**ロ-7**）」が最も高い回答率（53%）となった．次いで，「IoT 機器による DDoS 攻撃（**ロ-1**）」と「ランサムウェア攻撃の蔓延（**ロ-3**）」が共に高い回答率（42%）となった．

(3) 今後の脅威となり得る対象：顧客端末（PC，スマホ）

質問ハ（先行き攻撃対象となりうる対象）では，「顧客端末（PC, スマホ）への攻撃（**ハ-1**）」が最も高い回答率（53%）となった．また，「社員の端末（行員の PC やタブレット）への攻撃（**ハ-6**）」と「対外接続系システム（WEB サーバ，インターネット・バンキング）への攻撃（**ハ-3**）」が共に高い回答率（42%）であった．

上記を踏まえると，金融機関の実務家が最も関心を寄せていたのは FinTech のセキュリティであるといえる．質問イでは，「FinTech の最新動向およびセキュリティ」，質問ロでは「AI 技術のセキュリティ分野への影響」がそれぞれ最も高い回答率であった．AI 技術は，FinTech で活用される技術の 1 つとみられており，質問ロにおける上記の選択肢も FinTech に関するものといえる．

また，質問ハでは，「顧客端末（PC，スマホ）への攻撃」が最も高い回答率となったが，FinTech ではスマートフォンのアプリによるサービス提供が注目されていることも影響しているとみられる．「対外接続系システム（WEB サーバ，インターネット・バンキング）への攻撃」も高い回答率となったが，同様に，API のオープン化を巡る議論の活発化が影響している可能性がある．なお，これらの選択肢

ⓒ 2017 Information Processing Society of Japan

Vol.2017-CSEC-78 No.13
Vol.2017-SPT-24 No.13
2017/7/14

表 A-1　シンポジウムでのアンケート集計結果

			金融機関 (19)	ベンダー (24)	大学・研究機関等 (8)	その他 (15)	全体 (66)
イ．今後取り上げてほしいテーマ（数字は回答割合＜%＞）							
	イ-1	**FinTech の最新動向およびセキュリティ**	**58**	71	50	53	61
	イ-2	スマホ・タブレットのセキュリティ対策	21	17	13	27	20
	イ-3	**クラウドのセキュリティ**	**37**	38	0	20	29
	イ-4	インターネット・バンキングのセキュリティ対策	16	17	13	27	18
	イ-5	サイバー攻撃の最新動向	21	8	13	20	15
	イ-6	海外金融機関のセキュリティ対策	26	25	13	47	29
	イ-7	内部犯を考慮したセキュリティ対策	32	8	0	13	15
	イ-8	暗号技術の最新動向	5	42	13	40	27
	イ-9	IoT のセキュリティ対策	21	33	25	40	30
	イ-10	マルウェアの最新動向および対策	16	8	13	13	12
ロ．2016 年ニュースで同様の課題があると思われるものは？（数字は回答割合＜%＞）							
	ロ-1	IoT 機器による DDoS 攻撃	42	54	50	40	47
	ロ-2	自衛隊情報システムへのオープン・システムからの踏み台攻撃	11	13	13	7	11
	ロ-3	ランサムウェア攻撃の蔓延	42	13	0	40	26
	ロ-4	解消されないセキュリティ人材不足	32	33	50	20	32
	ロ-5	NISC が位置情報ゲームに注意喚起	5	0	0	20	6
	ロ-6	不正アクセスの低年齢化（教育委員会からの情報窃取）	0	0	13	13	5
	ロ-7	**AI 技術のセキュリティ分野への影響**	**53**	42	38	40	44
	ロ-8	巧妙化する標的型メール攻撃（JTB からの情報漏洩）	37	29	25	33	32
	ロ-9	IPA が「情報処理安全確保支援士」を新設	11	13	13	7	11
	ロ-10	EU プライバシー規制の採択（個人データ管理の厳格化）	16	21	38	27	23
ハ．今後脅威となり得ると考えられるものは？（数字は回答割合＜%＞）							
	ハ-1	**顧客端末（PC，スマホ）への攻撃**	**53**	42	38	40	44
	ハ-2	POS 端末や ATM への攻撃	0	29	25	20	18
	ハ-3	**対外接続系システム（WEB サーバ，インターネット・バンキング）への攻撃**	**42**	33	50	47	41
	ハ-4	勘定系システムへの攻撃	11	8	25	20	14
	ハ-5	情報系システム（電子メール，ERP）への攻撃	37	17	13	20	23
	ハ-6	**社員の端末（行員の PC やタブレット）への攻撃**	**42**	38	0	27	32
	ハ-7	クラウド上のシステムへの攻撃	32	38	0	40	32
	ハ-8	設備制御系システム（空調，監視カメラ，IoT 等）への攻撃	21	25	25	27	24

（備考）表中の括弧内の数字は，回答者の各分野におけるサンプル数（回答数）を示す．

は，昨年度開催した第 17 回情報セキュリティ・シンポジウムでのアンケートにおいても相対的に高い回答率（それぞれ 54%, 61%）となっており，今回のアンケートに限らず，近年注目度が高まっていることがうかがわれる[3].

質問イにおいて FinTech のセキュリティに次いで高い回答率となった クラウドのセキュリティ も，比較的高い関心が寄せられていたといえる．背景として，わが国の金融機関におけるクラウド活用の進展が挙げられる．金融情報システムセンターが実施したアンケート調査結果によれば，わが国の金融機関におけるクラウドの利用率（「利用中」との回答の割合）は，2015 年度に 36.5%であり，2011 年度（16.5%）と比較すると増加傾向が読み取れる（図 1 を参照）．クラウドを活用する金融機関が徐々に増えるなかで，クラウドのセキュリティにかかる問題意識も高まっていると考えられる．

ⓒ 2017 Information Processing Society of Japan