Vol.2018-CSEC-82 No.21
Vol.2018-SPT-29 No.21
2018/7/25

金融サービスのセキュリティに対する量子コンピュータの影響と今後の暗号の移行について

宇根正志†

概要：日本銀行金融研究所では，量子コンピュータが金融サービスのセキュリティに及ぼす影響や金融分野における今後の暗号の移行について議論するために，第 19 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を紹介する．

キーワード：暗号の移行，金融サービス，量子コンピュータ，耐量子計算機暗号

An Impact of Quantum Computing to Security of Financial Services and Future Migration of Cryptographic Algorithms

MASASHI UNE†

Abstract: The Institute for Monetary and Economic Studies of the Bank of Japan held the 19th Information Security Symposium in order to discuss an impact of quantum computing to the security of financial services and the future migration of cryptographic algorithms in the financial sector. This paper will present opinions expressed at the presentations and panel discussion of the symposium.

Keywords: financial services, migration of cryptographic algorithms, post-quantum cryptography, quantum computing

1. はじめに

安全な金融サービスを実現するうえで情報セキュリティ技術の適切な活用が不可欠であり，そのなかでも，暗号は重要な要素技術である. 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，通信路におけ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，暗号が利用されている．ATM 等における取引においても, 銀行のサーバと IC キャッシュカードとの間の通信の機密性を確保するために暗号が用いられている．金融分野における代表的な暗号は，公開鍵暗号では RSA 暗号や楕円曲線暗号が挙げられるほか，共通鍵暗号では AES が挙げられる．

金融サービスのセキュリティを確保していくためには，暗号のセキュリティの動向を継続的にフォローする必要がある．暗号に対する主な脅威として，コンピュータの処理性能や解読手法の高度化が挙げられる．コンピュータの処理性能に関しては，近年，量子力学の特性を利用した量子コンピュータの研究開発に注目が集まっている．量子コンピュータは，従来のスーパー・コンピュータよりも高速に暗号を解読することができる可能性があるといわれている. 米国連邦政府では，RSA 暗号や楕円曲線暗号を現実的な時間で解読可能な量子コンピュータが 2030 年頃に実現されうるとして，量子コンピュータにも十分な耐性を有する暗号（耐量子計算機暗号）の標準化を現在進めている[1].

こうした金融サービスを巡る環境変化への対応に関して金融機関を支援するために，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[2]．また，学界における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を検討し，学会で発表している[3][4][5].

日本銀行金融研究所では，今後，量子コンピュータの実現が金融サービスのセキュリティにどのような影響を与えうるかをテーマとする「第 19 回情報セキュリティ・シンポジウム」（開催日：2018 年 3 月 1 日，場所：日本銀行本店）を開催した[6]．本稿は，今次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紹介する．

本稿におけるシンポジウムの内容は，すべて著者の責任で取りまとめたものであり，日本銀行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著者個人に属する．

2. 第 19 回情報セキュリティ・シンポジウム

2.1 概要

第 19 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,「量子コンピュータが金融サービスのセキュリティに与える影響」をテーマとして，キーノート・スピーチ，4 件の講演，パネル・ディスカッショ

† 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

Vol.2018-CSEC-82 No.21
Vol.2018-SPT-29 No.21
2018/7/25

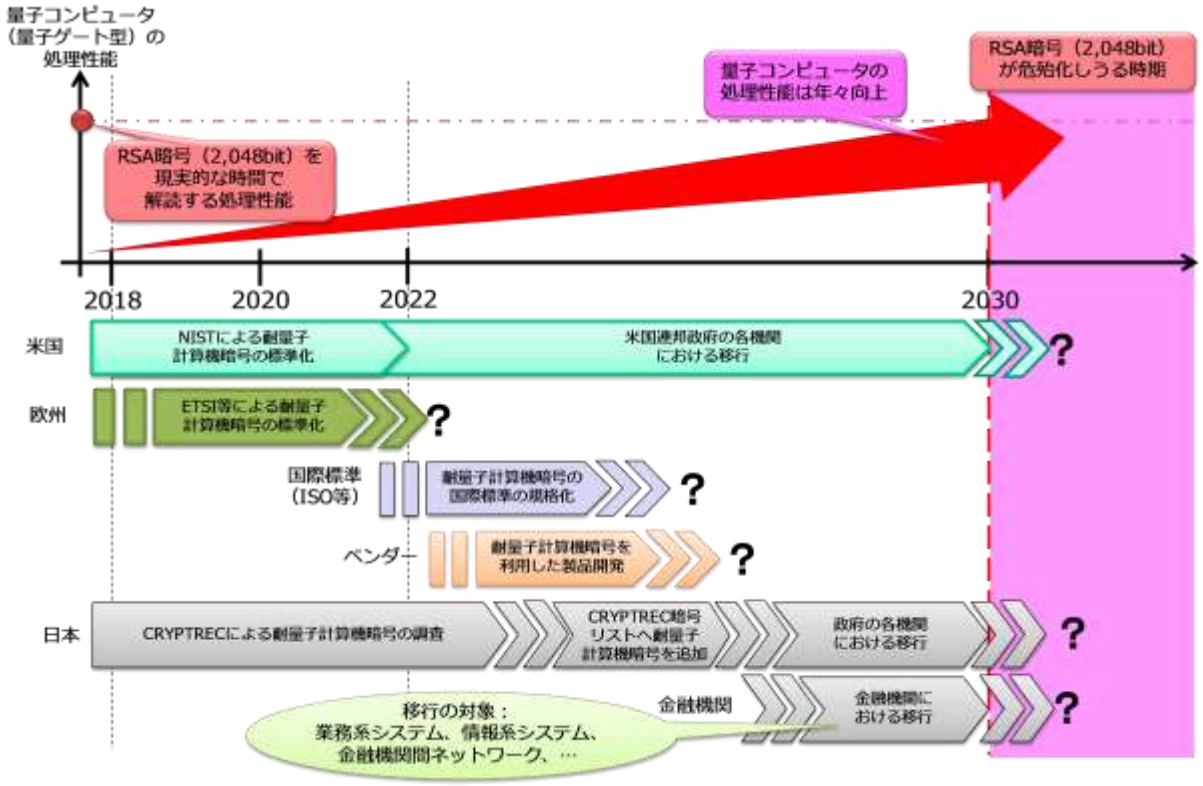

図 1　耐量子計算機暗号への移行に関する検討とスケジュール
（備考）参考文献[8]のスライド 11 を引用して作成.

ンを行った[7]. これらのタイトルや講演者・パネリスト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「量子コンピュータが金融サービスのセキュリティに与える影響」（横浜国立大学大学院教授　松本勉）
- 講演 1「超伝導量子コンピュータの仕組みと研究開発をめぐる最新動向」（東京大学先端科学技術研究センター教授　中村泰信）
- 講演 2「量子コンピュータの商用化動向」（日本アイ・ビー・エム東京基礎研究所副所長　小野寺民也）
- 講演 3「量子ゲート型コンピュータが暗号に与える影響と対策」（日本銀行金融研究所　清藤武暢）
- 講演 4「耐量子計算機暗号の標準化動向」（東京大学大学院教授　高木剛）
- パネル・ディスカッション「量子コンピュータの脅威に対して金融機関が検討すべき対策とは」

  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 専務理事 鎌田敬介
  三井住友銀行システム統括部システムリスク統括室室長代理 中山広樹
  NTT データ金融事業推進部技術戦略推進部技術戦略企画担当部長 山本英生

2.2 背景と問題意識：キーノート・スピーチ

キーノート・スピーチでは，今次シンポジウムの背景や問題意識について，以下の趣旨の発表が行われた[8].

近年，量子力学の性質を利用した情報処理技術（量子情報技術）として，量子コンピュータと量子通信の研究開発が注目されている. 量子コンピュータは, 従来のスーパー・コンピュータ（古典コンピュータ）よりも高速での演算処理が可能であり，量子通信は，より高速での通信やセキュアな鍵の配送を実現可能であるとみられている.

量子コンピュータは，量子ゲート型コンピュータと量子アニーリング型コンピュータの 2 種類に大別される. 量子ゲート型コンピュータは，その処理性能が一定のレベルに達すると暗号のセキュリティに影響を及ぼすことが知られており，新たな脅威として注目されている.

米国連邦政府は，鍵長が 2,048 ビットの RSA 暗号を数時間で解読可能な量子ゲート型コンピュータが 2030 年頃までに実現しうるとして，公開鍵暗号を耐量子計算機暗号に移行する検討を進めている（図 1 を参照）. 欧州では，ETSI（European Telecommunications Standards Institute）が，耐量子計算機暗号の標準化のロードマップを 2017 年 9 月から検討している[9]. わが国では，耐量子計算機暗号の調査が CRYPTREC において進められている[10]. 金融分野でも，今後，量子ゲート型コンピュータによる暗号のセキュリティ低下に対応することが求められるようになるであろう.

2.3 各講演の概要

(1) 超伝導量子コンピュータの仕組みと研究開発の動向

講演 1 では，超伝導を用いた量子ゲート型コンピュータの仕組みと研究開発の動向について，以下の趣旨の発表が行われた[11].

量子ゲート型コンピュータの研究は，量子情報科学の理論を基に，1980 年以降，素因数分解問題を解くアルゴリズムや誤り訂正の技術等の提案を受けて急速に発展している．古典コンピュータの情報の単位であるビットは，1 つのビットで 0 か 1 のどちらかのみを表現できる．量子ゲート型コンピュータで用いられる量子ビットは，重ね合わせ状態により，1 つの量子ビットで 0 と 1 を同時に表現できることから，一種の並列処理が可能となる．

実際には，量子ビットを用いた演算処理にはノイズ等により誤りが生じ，これを訂正する必要がある．本講演時点では，理論的に誤り訂正が可能な量子コンピュータは量子ゲート型コンピュータのみであり，一部の実験によって実証されている．また，量子ビット数や量子ビットのコヒーレンス時間（量子ビットが誤りを起こさずに状態を保持することができる平均的な時間）を向上させるための研究も盛んに進められている．

量子ゲート型コンピュータの開発に関しては，グーグル社，アイ・ビー・エム社，リゲッティ・コンピューティング社等, さまざまな企業や組織から事例が報告されている．また，量子ゲート型コンピュータを動作させるソフトウェア（プログラム）を開発する企業も多数存在している．

(2) 量子ゲート型コンピュータの商用化動向

講演 2 では，アイ・ビー・エム社における量子ゲート型コンピュータの商用化動向や応用分野等について，以下の趣旨の発表が行われた[12].

2016 年 5 月，5 量子ビットの量子ゲート型コンピュータを，クラウド（IBM Cloud）を介して利用できるサービスを開始し，これまで世界中から約 6 万ユーザが利用している．2017 年 11 月には，20 量子ビットのコンピュータを開発した．今後，50 量子ビットまで拡張する計画である．量子ゲート型コンピュータ上で動作するソフトウェアの作成を支援するソフトウェア開発キット「QISKit」も提供を開始している．

量子ゲート型コンピュータの主な応用分野として，化学, 人工知能（機械学習），最適化問題が挙げられるほか，金融関係では，トレーディング戦略，ポートフォリオ最適化，リスク分析等への適用が想定される．製造業では，新素材の探索，製造プロセスの最適化等への適用が候補とみられる．今後，量子ゲート型コンピュータのユーザとなりうる企業は，量子ゲート型コンピュータを活用したサービスを速やかに提供できるように準備しておきたいと考えるであろう．主な課題となるのは，量子ゲート型コンピュータで動作するソフトウェアを新たに設計・作成するとともに，それが適切に動作することを確認・保証することである．ソフトウェアの企画，実装，検証等に相応の時間を要すると見込まれることから, 早めに着手することが求められる．

量子ゲート型コンピュータが暗号に与える影響に関しては, 鍵長が 2,048 ビットの RSA 暗号を解読するためには，誤り訂正処理を含め，約 800 万量子ビットを実現する必要があるとみられている．こうした大規模な量子ビットを有する量子コンピュータの実現は数十年先とみられている．

(3) 量子ゲート型コンピュータの暗号への影響と対応方針

講演 3 では，量子ゲート型コンピュータが公開鍵暗号や共通鍵暗号に与える影響，および，それを通じた金融サービスに関連する国際標準等への影響について，以下の趣旨の発表が行われた[13][14].

量子ゲート型コンピュータを動作させて何らかの処理を実施するためには，量子アルゴリズムが必要である．量子アルゴリズムは，量子ビットの重ね合わせ状態を維持しつつ演算処理を行うとともに，処理結果の量子ビットを観測した際に最適な解が得られるように量子ビットを操作する手順である．一部の量子アルゴリズムは，公開鍵暗号や共通鍵暗号に対する攻撃を可能にする. 具体的には, グローバーのアルゴリズム，サイモンのアルゴリズム，ショアのアルゴリズムが挙げられる．

RSA 暗号と楕円曲線暗号は，ショアのアルゴリズムによって現実的な時間で解読可能であるといわれており，これらの暗号は耐量子計算機暗号に移行することが求められる．共通鍵暗号の AES では，グローバーのアルゴリズムによって鍵を効率的に全数探索する方法が知られており，鍵長の伸長（2 倍程度）が必要とされる．さらに，AES 等にかかる一部の実装形態（暗号利用モード）では，サイモンのアルゴリズムによって鍵を効率的に推定する方法が知られており，当該アルゴリズムに対して安全な方式への移行が求められる．

RSA 暗号，楕円曲線暗号，AES は，金融サービス向けのさまざまな標準規格等に規定されている（表 1 を参照）. 例えば，金融取引における暗証番号の安全性を確保する仕組みを規定する ISO 9564-1, 2 や，金融サービスにおける利用を推奨する暗号を記載する ISO/TR 14742 が挙げられる. これらにおいては，今後，耐量子計算機暗号への移行や鍵の伸長等の対応が必要になると考えられる．

(4) 耐量子計算機暗号の標準化動向

講演 4 では，耐量子計算機暗号の標準化を巡る最近の動向について，以下の趣旨の発表が行われた[10].

NIST（National Institute of Standards and Technology）が進めている耐量子計算機暗号の標準化候補として, 69 件の応募が寄せられた. それらのうち, 格子問題に基づく暗号（格子暗号）が最も多く（24 件），符号暗号（16 件），多変数多項式暗号（10 件）と続く．各暗号は，鍵長や処理速度の観点で一長一短があり，すべての観点で優れたものはない．

表 1　金融サービスで利用されている標準規格の暗号と量子コンピュータによる影響

標準規格等	規定されている主な暗号と影響	
	公開鍵暗号	共通鍵暗号（ブロック暗号）
ISO 9564-1, 2 （暗号番号の暗号化）	RSA 暗号	【ブロック暗号】*AES*，トリプル DES 【暗号利用モード】*ECB*
ISO 11568-1, 2, 4 （鍵管理）	RSA 暗号 楕円曲線暗号	【ブロック暗号】*AES*，*トリプル DES* 【暗号利用モード】*ECB*，CBC，CFB，*OFB*，*CTR*
ISO/TR 14742 （利用を推奨する暗号）	RSA 暗号 楕円曲線暗号	【ブロック暗号】*AES*，*トリプル DES* 【暗号利用モード】*ECB*，CBC，*CTR*，CBC-MAC，*CMAC*
ISO 16609 （データの改ざん検知）	＜規定なし＞	【ブロック暗号】*AES*，*トリプル DES* 【暗号利用モード】CBC-MAC，*CMAC*
TLS （インターネット・バンキング等）	RSA 暗号 楕円曲線暗号	【ブロック暗号】*AES* 【暗号利用モード】CBC，*CCM*，GCM
EMV 仕様 （クレジットカード等の業界標準）	RSA 暗号	【ブロック暗号】*AES* 【暗号利用モード】CBC，CBC-MAC，*CMAC*

（備考）参考文献[13]のスライド 14 を引用して作成．下線の暗号と暗号利用モードは他の方式への移行が必要であることを示しているほか，斜体の暗号等は鍵の伸長が必要であることを示している．

ISO/IEC JTC1/SC27 では，耐量子計算機暗号の研究動向の調査が進められており，今後報告書が作成される予定である．IETF（Internet Engineering Task Force）では，耐量子計算機暗号の標準規格案が公表されている．

新しい暗号が提案されてから実用化されるまでに，安全性検証が行われ，一定の評価が得られることが求められる．安全性検証では，国際会議等のオープンな環境において安全性や実装性に関する検討が行われる．その結果，安全な鍵長等についてコンセンサスが得られると，当該暗号に関する標準規格の策定が開始される．企業による情報システム等への実装は，標準規格の策定が完了した後に行われることになる．

代表的な耐量子計算機暗号の 1 つである格子暗号については，現在，安全性等にかかる評価の段階にある．安全性の理論的な評価に加えて，コンピュータを用いた解読コンテストも行われている．安全性評価が今後進展すれば，安全な鍵長等にかかるコンセンサスが得られ，それらが公開・標準化された後，企業の情報システムに実装されるようになる可能性がある．

2.4 パネル・ディスカッション

「量子コンピュータの脅威に対して金融機関が検討すべき対策とは」をテーマに，金融機関が量子ゲート型コンピュータによる脅威にどのように対応していくべきかが議論された．以下では，各論点に関するパネリストやフロア参加者による主な意見やコメントを示す．

(1) 金融分野で想定される量子コンピュータのユースケースと懸念事項

【想定されるユースケース】

- 人工知能を利用した業務や与信審査，マーケット分析にかかる演算処理等に適用できるのではないか．
- 金融機関において膨大な処理時間を有する業務に活用することが有用であろう．仮想通貨のマイニング処理，人工知能（深層学習）における学習処理等への適用が期待される．

【懸念事項】

- 大規模な量子ゲート型コンピュータが実現すれば，金融分野で主流となっている暗号が危殆化する可能性がある．金融機関はさまざまなアプリケーションで暗号を利用しており，その多くのセキュリティが低下するおそれがある．とりわけ，顧客向けのアプリケーション（インターネット・バンキング等）のセキュリティ低下を回避するよう対応する必要があろう．
- 金融機関による在宅勤務のためのリモート・アクセス・システム（遠隔から行内システムにアクセスするためのシステム）のセキュリティにも影響が及ぶ可能性がある．
- 仮想通貨が暗号に依存している部分があり，万一，システム側の対策が後手に回ってしまうと，多くの利用者が仮想通貨を失いかねない．
- 仮想通貨が改ざん防止にハッシュ関数を利用している場合，量子コンピュータによりハッシュ関数のセキュリティが低下すると，取引内容が改ざんされるおそれがある．特に，パブリック型のブロックチェーンを利用する仮想通貨では，不特定多数の利用者による合意形成が前提となることから，インパクトが大きくなる可能性がある．

(2) 量子コンピュータの脅威が顕在化する際の状況

- 量子ゲート型コンピュータは，莫大な開発コストや維

持管理コストが必要となることから，当初は国家や大手 IT 企業，国から援助を得ている研究機関において利用可能となると想定される．

- 量子ゲート型コンピュータの実機を保有しているのはごく一部の企業や研究機関に限定されているとみられるものの，開発している事実を公表していない企業や研究機関が存在する可能性は否定できない．
- 量子ゲート型コンピュータは，利用者が設備として調達して利用するのではなく，IT 企業等が当該コンピュータの計算資源をクラウドとして提供し，そうしたサービスをネットワーク経由で使用するという形態になるであろう．
- 金融機関は，自前で量子コンピュータを調達・保有することは考えにくく，クラウド経由での利用になる可能性が高い．

(3) 推奨される暗号の移行パターン

- RSA 暗号等から耐量子計算機暗号への移行パターンとして，暗号鍵を伸長した後（例えば，RSA 暗号の鍵長を 2,048 ビットから 3,072 ビットに伸長），耐量子計算機暗号に移行するというもの（パターン 1）と，暗号鍵の伸長を行わずに耐量子計算機暗号に移行するというもの（パターン 2）が考えられる．
- 金融機関は，システムの更改時期に合わせて暗号を移行することが多く，システム更改の検討開始の時点で最適な暗号が選択可能な状態になっていることが求められる．したがって，更改時期に耐量子計算機暗号が選択可能な場合にはパターン 2 を採用しうるが，そうでない場合にはパターン 1 となるであろう．
- 移行対象のシステムにおいて暗号処理がモジュール化されている場合には，パターン 1 よりもパターン 2 の方が効率的となる場合がある．
- 金融サービスの顧客は耐量子計算機暗号への移行が困難な端末を利用している場合がある．そうした端末への対応（レガシー対応）が必要か否かは，どちらのパターンを採用するかを検討するうえで重要である．
- パターン 1 では，古典コンピュータの攻撃手法だけでなく，量子ゲート型コンピュータの実用化動向も考慮して鍵長の伸長度合いを決めるべきである．この場合，過去のケースに比べて，鍵長を大幅に伸長しなくてはならない可能性にも留意する必要がある．
- 認証局の一部では，既にパターン 1 による移行（鍵長を 3,072 ビットに伸長）を進めている．これまで，新しい暗号が標準化されてから普及するまでに 20～30 年を要してきたことから，今回の暗号移行においても長期的な移行計画を立案することが望ましい．

(4) 耐量子計算機暗号への移行やシステム実装に際しての課題や留意点

- 金融機関は，量子ゲート型コンピュータの開発動向をフォローすることに加え，セキュリティ・ベンダーによる耐量子計算機暗号のソリューションの提供動向についてもフォローすることが必要である．
- 暗号の移行に際して，重要度の低いシステムで試行し，信頼性や可用性に関する検証を行った後に，信頼性・可用性の要求度合いが高いシステムから移行していくことになるであろう．
- DES や AES の標準化等，米国連邦政府による過去の暗号移行のケースでは，標準化された暗号が世界各国で広く利用されるようになっている．こうした点を踏まえると，今後，米国連邦政府によって標準化される耐量子計算機暗号は，2030 年頃に世界各国で主流の暗号となっている可能性もある．こうした状況についても考慮しておくことが重要である．
- 現時点で耐量子計算機暗号のソリューションが提供されていないのであれば，金融機関による 2030 年までの移行対応の完了は困難かもしれない．その場合，移行が完了しないリスクを許容できるか否かを検討し，許容できない場合の代替策を検討することが求められる．
- 金融機関のシステムにおいて，顧客との通信を行う際に暗号が利用されるケースが多い．したがって，顧客の OS やブラウザが耐量子計算機暗号に対応していることが耐量子計算機暗号への移行の前提となる．逆に，顧客の OS 側での対応が進めば，金融機関側でも対策を進めざるをえなくなる可能性がある．
- 移行を開始する時期を決定するうえで，暗号のセキュリティ低下の損失と量子ゲート型コンピュータの利用にかかるコストのバランス（費用対効果）を見極めることが重要である．
- 現時点では，移行に時間を要するシステム構成が主流となっているが，今後のシステム構築では，ソフトウェア等に有効期限を設けるなど，暗号移行を実施しやすい設計とするという考え方がありうる．
- 金融機関においては，暗号の移行以外にもシステム面で解決すべき課題が山積している．それらの課題と耐量子計算機暗号への移行のバランスをとることも重要である．

3. おわりに

第 19 回情報セキュリティ・シンポジウムでは，量子コンピュータの開発や商用化，耐量子計算機暗号の標準化にかかる最新動向が紹介されたほか，金融分野での量子コンピュータのユースケースや懸念事項，耐量子計算機暗号への移行のスケジュール，課題や留意点に関して議論が行われた．量子コンピュータの開発や耐量子計算機暗号の標準化の動向を引き続きフォローするとともに，今回示された課題への金融機関における対応等に注目していきたい．

参考文献

[1] National Institute of Standards and Technology, Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization, Call for Proposals Announcement, 2016.
[2] 日本銀行金融研究所,「日本銀行金融研究所ホームページ」, 2018 年（URL：https://www.imes.boj.or.jp/citecs/，参照 2018-03-31）.
[3] 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.
[4] 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.
[5] 宇根正志,「金融分野における高機能暗号の活用と今後の課題」,『情報処理学会研究報告』vol. 2017-CSEC-78, no. 13, 情報処理学会, 2017 年.
[6] 日本銀行金融研究所,「情報セキュリティ・シンポジウム（第 19 回）の模様：量子コンピュータが金融サービスのセキュリティに与える影響」, IMES Discussion Paper Series, no. 2018-J-6, 日本銀行金融研究所, 2018 年.
[7] 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 19 回情報セキュリティ・シンポジウム量子コンピュータが金融サービスのセキュリティに与える影響」, 2018 年（URL：https://www.imes.boj.or.jp/citecs/symp/19/index.htm, 参照 2018-03-31）.
[8] 松本勉,「キーノート・スピーチ：量子コンピュータが金融サービスのセキュリティに与える影響」, 第 19 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.
[9] European Telecommunications Standards Institute, Quantum-Safe Cryptography (QSC); Limits to Quantum Computing Applied to Symmetric Key Sizes, ETSI GR QSC, 006, 2017.
[10] 高木剛,「耐量子計算機暗号の標準化動向」, 第 19 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, 2018 年.
[11] 中村泰信,「超伝導量子コンピュータの仕組みと研究開発をめぐる最新動向」, 第 19 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, 2018 年.
[12] 小野寺民也,「量子コンピュータの商用化動向」, 第 19 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, 2018 年.
[13] 清藤武暢,「量子ゲート型コンピュータが暗号に与える影響と対策」, 第 19 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, 2018 年.
[14] 清藤武暢・四方順司,「量子コンピュータが共通鍵暗号の安全性に与える影響」, IMES Discussion Paper Series, no. 2018-J-2, 日本銀行金融研究所, 2018 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 120 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 30 件の回答を得た（全体では 81 件）.

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**）である．各質問の内容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 2017 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.

質問の選択肢や回答の集計結果を表 A-1 に示す．主な結果を整理すると，以下のとおりである.

(1) 今後取り上げてほしいトピック：FinTech と AI

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（分散台帳技術等）の最新動向（**イ-9**）」が最も高い回答率（50%）であった．これに次いで高い回答率（37%）となったのが「人工知能（AI）や機械学習のセキュリティ（**イ-3**）」であった.

(2) 2017 年のニュース：ランサムウェア攻撃の蔓延

質問**ロ**（最近の情報セキュリティ上の課題）では，「ランサムウェア攻撃の蔓延（**ロ-2**）」が最も高い回答率（53%）となった．次いで，「大規模な個人情報の漏洩（**ロ-4**）」と「国家によるサイバー攻撃の常態化（**ロ-7**）」が高い回答率（それぞれ 30%，23%）となった.

(3) 今後の脅威となりうる対象：対外接続系システム

質問**ハ**（先行き攻撃対象となりうる対象）では，「対外接続系システム（ウェブ・サーバ，インターネット・バンキング・システム）への攻撃（**ハ-2**）」が最も高い回答率（50%）となった．次いで，「顧客端末（PC，スマホ）への攻撃（**ハ-1**）」，「社員の端末（行員の PC やタブレット）への攻撃（**ハ-5**）」，「FinTech 企業への攻撃（**ハ-8**）」が共に高い回答率（27%）となった.

上記を踏まえると，アンケートに回答した金融機関の実務家が最も関心を寄せていたのは，前回のシンポジウムのアンケートと同様に，FinTech のセキュリティであるといえる[5]．質問**イ**では，「FinTech（分散台帳技術等）の最新動向」に次いで「人工知能（AI）や機械学習のセキュリティ」が高い回答率であったが，AI や機械学習は FinTech で活用される技術の 1 つである．また，質問**ハ**において，「FinTech 企業への攻撃」が今後脅威となりうるものとして比較的高い回答率となっている.

セキュリティ対策上の課題や今後の脅威としては，外部のネットワークからの攻撃が引き続き注目を集めているといえる．質問**ハ**において，「対外接続系システム（ウェブ・サーバ，インターネット・バンキング・システム）への攻撃」が高い回答率となったほか，質問**ロ**において，「ランサ

Vol.2018-CSEC-82 No.21
Vol.2018-SPT-29 No.21
2018/7/25

表 A-1　シンポジウムでのアンケート集計結果

		金融機関 (30)	ベンダー (19)	大学・研究機関等(10)	その他 (22)	全体 (81)
イ．今後取り上げてほしいテーマ（数字は回答割合＜%＞）						
イ-1	モバイル端末のセキュリティ（セキュア・エレメント、TEE、SIM の安全性等）	27	16	10	9	17
イ-2	クラウドのセキュリティ	30	21	20	14	22
イ-3	**人工知能（AI）や機械学習のセキュリティ**	**37**	53	70	41	46
イ-4	IoT のセキュリティ対策	10	32	40	41	27
イ-5	認証技術の安全性（モバイル端末での認証、生体認証等）	23	37	0	23	23
イ-6	暗号技術の最新動向（高機能暗号、耐量子計算機暗号）	17	47	40	18	27
イ-7	**海外金融機関のセキュリティ対策**	**33**	21	10	9	21
イ-8	インターネット・バンキングのセキュリティ対策	30	5	0	0	12
イ-9	**FinTech（分散台帳技術等）の最新動向**	**50**	32	50	45	44
イ-10	量子コンピュータとその影響	23	16	30	32	25
ロ．2017 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	20	42	40	45	35
ロ-2	**ランサムウェア攻撃の蔓延**	**53**	37	10	32	38
ロ-3	SNS による不正確な情報拡散の影響	20	5	0	14	12
ロ-4	**大規模な個人情報の漏洩**	**30**	26	30	9	23
ロ-5	改正個人情報保護法の全面施行	13	21	0	18	15
ロ-6	インターネットの安定性への不安	7	16	20	18	14
ロ-7	**国家によるサイバー攻撃の常態化**	**23**	47	30	55	38
ロ-8	不正アクセスの低年齢化	3	5	0	9	5
ロ-9	セキュリティ専門家自身による不正行為の不安	10	5	10	9	9
ロ-10	IPA「情報処理安全確保支援士」の登録の伸悩み	0	0	0	0	0
ハ．今後脅威となりう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**	**27**	42	20	14	26
ハ-2	**対外接続系システム（ウェブ・サーバ、インターネット・バンキング・システム）への攻撃**	**50**	26	10	23	32
ハ-3	情報系システム（電子メール等）への攻撃	23	16	10	14	17
ハ-4	クラウド上のシステムへの攻撃	20	21	20	14	19
ハ-5	**社員の端末（行員の PC やタブレット）への攻撃**	**27**	37	10	14	23
ハ-6	勘定系システムへの攻撃	7	5	0	18	9
ハ-7	設備制御系システム（空調、監視カメラ、IoT 等）への攻撃	10	11	30	18	15
ハ-8	**FinTech 企業への攻撃**	**27**	21	20	18	22
ハ-9	AI を用いたサービスに対する攻撃	13	21	30	27	21

（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．

ムウェア攻撃の蔓延」と「大規模な個人情報の漏洩」が比
較的高い回答率となったことから伺われる．