Vol.2020-DPS-182 No.7
Vol.2020-CSEC-88 No.7
2020/3/12

暗号資産のセキュリティに関する研究動向と課題

井上紫織† 宇根正志†

概要：日本銀行金融研究所では，暗号資産のセキュリティを巡る最新の研究動向や，そうした研究成果を暗号資産の実務に活用するうえで解決すべき課題について議論するために，第 21 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：暗号資産，金融サービス，ブロックチェーン，セキュリティ対策

Recent Research Trends and Challenges on the Security of Crypto-Assets

SHIORI INOUE† MASASHI UNE†

Abstract: The Institute for Monetary and Economic Studies of the Bank of Japan held the 21st Information Security Symposium in order to discuss recent research trends on the security of crypto-assets and how to apply research results to security practices in crypto-asset businesses. This paper will present opinions expressed in the presentations and panel discussion of the symposium.

Keywords: blockchain, crypto-asset, financial service, security countermeasure

1. はじめに

近年，改ざん不可能な取引履歴の記録手段として，金融分野をはじめとするさまざまな分野でブロックチェーンの活用可能性が検討されている．金融情報システムセンターが実施したアンケート調査によると，ブロックチェーンまたは分散型台帳技術への取組み状況について「実用化済」，「準備段階」または「検討中」と回答した金融機関の割合は 25.5%となっている．そのうち，「地域通貨・電子通貨」を活用目的に挙げる金融機関の割合は 28.9%となっており，ビットコインやイーサリアムといった既存の暗号資産に留まらず，新たな暗号資産の活用可能性が注目されていることが伺われる（図 1 参照）．

利用者が安心して暗号資産を取引するためには，当該取引のセキュリティが確保されていることが求められる．最近では，暗号資産の用途や利用者のニーズを考慮したセキュリティ対策手法に関する研究が進展しており，実際にそうした対策を講じた暗号資産も開発されている．今後，暗号資産をより多様な環境や用途において安全に活用するためには，学術的な研究成果をフォローしつつ，暗号資産のセキュリティ特性やセキュリティ上の課題について正確に理解しておくことが重要である．

こうした観点を踏まえて，日本銀行金融研究所では，「暗号資産のセキュリティ」をテーマとする「第 21 回情報セキュリティ・シンポジウム」（開催日：2020 年 12 月 9 日，場所：日本銀行本店）を開催した[1][2]．本稿では，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．

なお，本稿におけるシンポジウムの内容は，すべて著者たち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たちに属する．

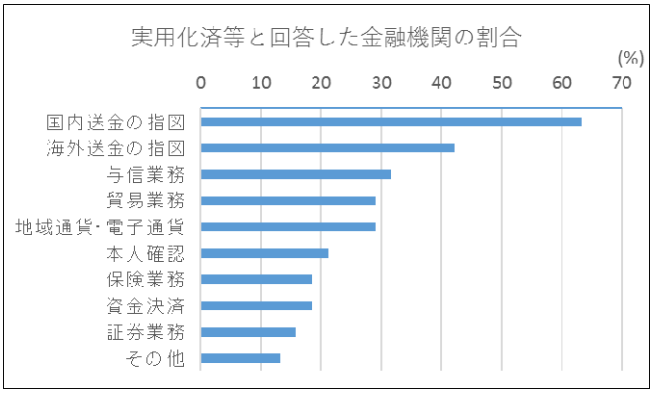

図 1 ブロックチェーンまたは分散型台帳技術の活用目的
（備考）参考文献[3]の図表 1-14 をもとに作成

2. 第 21 回情報セキュリティ・シンポジウム

2.1 概要

第 21 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，キーノート・スピーチ，2 件の講演，パネル・ディスカッションを行った．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（ジョージタウン大学 リサー

† 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), Institute for Monetary and Economic Studies (IMES), Bank of Japan

チ・プロフェッサー　松尾真一郎）

- 講演 1「暗号資産のセキュリティを巡る最新動向(1)」（筑波大学准教授　面和成）
- 講演 2「暗号資産のセキュリティを巡る最新動向(2)」（日本銀行金融研究所　宇根正志）
- パネル・ディスカッション「暗号資産のセキュリティに関する研究成果を実務へ活用していくうえでの課題」

モデレータ：ジョージタウン大学 リサーチ・プロフェッサー　松尾真一郎
パネリスト：筑波大学准教授　面和成
金融 ISAC 専務理事/CTO　鎌田敬介
メルペイ取締役/CTO　曾川景介

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，以下の趣旨の発表が行われた．

代表的な暗号資産のひとつとして知られるビットコインは，サトシ・ナカモトの論文に基づき設計されたブロックチェーンを用いて運用が開始された[4]．この論文において，ビットコインは，信頼された第三者機関を必要とせず，二重支払いを防止する仕組みを具備した支払いシステムとして提案された．

しかし，近年では，法定通貨との交換取引等，支払い以外の用途に応用されている．その結果，サトシ・ナカモトの論文において想定されていなかったセキュリティ上のリスクが発生することとなった．例えば，取引所から暗号資産が流出する事件がこれまでに発生したが，それらは，支払い以外の処理や取引所の運用におけるセキュリティ対策が不適切であったことに起因しているとみられている．

こうした点を踏まえると，暗号資産は，安全なエコシステムを形成するために必要なセキュリティ対策が十分に確立されないまま，商用化され流通しているのが実情であるといえる．暗号資産の基盤技術であるブロックチェーンのセキュリティを確保することに加えて，それ以外の構成要素のセキュリティも十分に検討し，対策を講じることが必要である．

まず，ブロックチェーンのセキュリティを考えるうえで，その技術の成り立ちを理解することが有用であろう．ブロックチェーンは，近年新たに開発された技術というわけではなく，①暗号，②プライバシー保護，③デジタル化現金（digitalized cash），④コストとゲームの理論（cost and game theory），⑤分散処理（decentralization）といった技術・学問分野の知見が結実した技術といえる．

暗号に関しては，ビットコインにおけるデータの連鎖構造にハッシュ関数が用いられているが，これはタイムスタンプ方式やヒステリシス署名における連鎖構造と類似している．もっとも，既存の方式は信頼できるサーバを要する点でブロックチェーンと異なっている．

プライバシー保護の技術も暗号資産やブロックチェーンの発展を後押ししている．米国政府は，1990 年代，米国以外による強力な暗号の利用を制限するために暗号の輸出を規制していたほか，米国政府のみが復号可能な専用のハードウェア（クリッパー・チップ＜Clipper Chip＞）の使用を義務付けるなどの政策を推進していた．これらの政策によって，米国政府が個人間の通信の内容を閲覧できるようになる可能性があった．こうした動きに対抗するために，プライバシー保護の技術に関する研究が活発化し，グループ署名，ミックスネット，オニオン・ルーティング等が開発された．これらは，暗号資産の匿名性を高める手段として利用されるケースがある．

デジタル化現金については，モンデックスや日本銀行・NTT 電子現金方式等，これまでにさまざまな方式の研究開発が行われており，それらの知見が暗号資産の取引に活用されている．また，コストやゲームの理論は，継続的なマイニングのためのインセンティブ・メカニズムの設計に不可欠となっている．分散処理に関しては，インターネットにおける情報通信において，信頼できる第三者機関を仮定しなくても，一部のサーバの故障や不正行為に対して頑健性を確保する手法が開発されており，ブロックチェーンにも活かされている．

上記のとおり，暗号資産は暗号アプリケーションの 1 つとして捉えることができる．暗号アプリケーションにおいては，データの機密性や一貫性の確保は鍵管理の問題に変換される．したがって，すべての参加者が秘密の鍵を適切に管理することが求められる．もっとも，鍵管理を適切に行ったとしても，暗号は計算機の性能向上や（未知の）脆弱性の発見によって危殆化しうることから，例えば，ブロックチェーンに用いられる暗号が危殆化した場合を想定したうえで，長期署名フォーマット等を活用して強力な暗号に更新する方法を検討しておくことも必要である[5][6].

また，暗号資産のセキュリティを理論的に評価する手法の開発も重要である．最近では，暗号資産のセキュリティ特性を定義するとともに，一定の条件のもとでそれらが満たされることを証明する手法の研究が活発化しており，そうした手法によってマイニング・プロトコルを評価した結果が報告されている．

マイニング・プロトコルを実装する際には，プログラムのバグにどのように対処するかについて検討が必要である．イーサリアムにおける DAO 事件では，スマート・コントラクトのプログラムのバグが悪用され，大量の暗号資産が流出した．作成したプログラムをどのように検証するか，そして，バグを発見した際にそれをどのように修正・対応するかが大きな課題となっている．

このように，暗号資産のセキュリティを確保するうえで，技術面の対応だけでは十分とはいえず，分散環境において

も技術を適切に活用し問題を解決するための仕掛けが必要である．暗号資産のエコシステムにおいて各参加者が適切に行動するようにインセンティブを付与する仕組みや，規制の導入についても検討が必要となりうる．こうした点を踏まえると，暗号の研究者や技術者のコミュニティだけでなく，暗号資産に関するサービス事業者，経済学や法律学の専門家，規制当局の実務者も関与しつつ検討を進めることが必要であろう．

2.3 各講演の概要

(1) 「暗号資産のセキュリティを巡る最新動向（1)」

講演 1 では，暗号資産のシステムがネットワーク上の攻撃に悪用されるリスクに関する最新の研究動向について，以下の趣旨の発表が行われた．

ブロックチェーンを用いた暗号資産は，耐改ざん性と高可用性という 2 つの特徴を有する．耐改ざん性は，ハッシュ関数とコンセンサス・アルゴリズムにより，ブロックチェーンに格納されたデータを改ざんすることが実質的に不可能であるという性質である．高可用性は，すべての参加者が同じブロックチェーンを所持することにより，一部の参加者が活動を停止した場合であっても，残りの参加者によりシステム全体が稼動し続けることができるという性質である．

暗号資産には，こうした特徴に起因するリスクが存在する．まず，耐改ざん性に起因するリスクとして，不正なデータが格納された場合に，当該データが格納され続ける（「ブロックチェーン汚染」という）リスクが挙げられる．2018 年に，ビットコインのブロックチェーンを調査した結果が発表され，書籍や論文等，著作権侵害に当たると考えられるデータのほか，個人的な写真やメール，第三者機関から流出したとみられる電話番号や住所，銀行口座，パスワード等，秘匿性が高くプライバシー侵害に当たると考えられるデータが格納されていることが報告されている[7]．また，イーサリアムのブロックチェーンについて調査を実施したところ，画像ファイル等の非金融データに加え，マルウェアとみられる悪質なファイルが埋め込まれていることが判明した[8]．

ブロックチェーン汚染により，ボットネットを用いたサイバー攻撃の脅威が高まる可能性を示す研究結果も報告されている[9][10]．ボットネットは，特定のマルウェアに感染した複数のコンピュータ（ボット）で構成されるネットワークのことであり，攻撃者は，特定のサーバから各ボットに攻撃の命令を送信してボットを遠隔操作する．こうしたサーバは C&C（command and control）サーバと呼ばれる．従来のボットネットにおいては，攻撃の命令（C&C 命令と呼ばれる）はボット間の通信によって伝達されることから，1 つのボットを特定することができれば，そのボットの通信から芋蔓式に他のボットを追跡・特定することが可能となり，ボットネットの全容を解明して攻撃を停止させることが可能であった．

しかし，ブロックチェーンのトランザクションに C&C 命令が埋め込まれると，各ボットはブロックチェーンから直接 C&C 命令を読み込むことになる．その結果，攻撃に際してボット間で通信する必要がなくなり，ボットネット全体を把握することが困難となる．

ビットコインやイーサリアムといった主な暗号資産においては，それらのブロックチェーンの一部がある程度信頼されているウェブサイト上にエクスプローラー（explorer）として転用されており，誰もが簡単にアクセス可能である．攻撃者が暗号資産のブロックチェーンにマルウェア等の悪意のあるデータを埋め込むと，それらが一部のウェブサイトに転用される可能性がある．そうしたウェブサイトに（ブロックチェーンに参加していない）一般のユーザーがアクセスした場合，悪意のあるデータを読み込んでしまい，ブロックチェーン汚染がさらに拡大する危険性がある．

ブロックチェーンの高可用性については，サービスを停止することが適当な場合においても容易にシステムをダウンさせることができないというリスクにつながる．例えば，特定の暗号資産が使用されなくなり，その価値が失われてしまった場合，その暗号資産のシステムを停止させ，サービスを終了させることが望ましいと考えられる．実際に，価値を有しない暗号資産のブロックチェーンを調べると，一部の暗号資産では，参加者が特定の地域に偏っていることが判明した[11]．これらのブロックチェーンは，それらの地域の特定の参加者によって，暗号資産という本来の目的とは異なる用途で使用されている可能性が高いと考えられる．このような望ましくない状態においても，ブロックチェーンのサービスを停止させることができず，攻撃に悪用されるリスクがある点に留意が必要である．

(2) 「暗号資産のセキュリティを巡る最新動向（2)」

講演 2 では，暗号資産のセキュリティに関する主な研究事例を紹介するとともに，それらを実務に活用する際の課題について，以下の趣旨の発表が行われた．

暗号資産のシステムは，主に，①暗号，②ネットワーク，③基盤プロトコル（ブロックチェーン），④応用プロトコル（合意形成等），⑤ソフトウェア／ハードウェア，⑥運用（セキュリティ管理等）によって構成される．これらに関して，脆弱性やそれを悪用する攻撃に関する研究をサーベイすると，暗号，応用プロトコル，ソフトウェアを対象とするものが目立つ．暗号に関しては，ハッシュ関数や署名の危殆化についての研究が挙げられる．応用プロトコルについては，非公開のフォークによる攻撃（利己的マイニング），大量のマイニング・パワーを用いる攻撃（51%攻撃），暗号資産による支払いの返金（リファンド）を悪用する攻撃（リ

ファンド攻撃）に関する研究が挙げられる．また，ソフトウェアについて，秘密鍵（署名生成用）の推定やプログラムのバグに関する研究が挙げられる．

具体的には，ハッシュ関数や署名の安全性が低下した場合，ブロックチェーン上の取引データの改変や二重使用が発生する可能性が指摘されている[12]. また，対策として，過去の取引データ等を，安全性が高いハッシュ関数等による新しいブロックチェーンに順次格納し，過去の取引データを保護する手法が提案されている[13].

利己的マイニングは，攻撃者が自分のフォークを公表しないでマイニングを続け，公開されているブロックが確定する直前に自分のフォークを公開し，マイニングの報酬の独占と暗号資産の二重使用を試みる攻撃である．攻撃者が全マイニング・パワーの 25%以上を有する場合，善良なマイナーよりも多くの報酬を獲得しうるとの研究が報告されている[14]．対策については，基盤プロトコルの変更等が必要であり，適用は容易でないとみられている（例えば，[15][16]）.

51%攻撃は，攻撃者が全マイニング・パワーの半数以上を用いてマイニングを行い，その報酬を独占するとともに，利己的マイニングと同様にフォークを秘匿して二重使用を試みる攻撃である．攻撃しやすい暗号資産にマイニング・パワーを振り向けたり，クラウドからリソースを調達したりする手法が知られている[17]．こうした攻撃により，攻撃者は，善意のマイナーよりも多額の報酬等を得る場合があるとのシミュレーション結果が示されている．

リファンド攻撃は，商取引での支払いを暗号資産の移転によって行うプロトコルにおいて，取引のキャンセル等に伴う返金先（リファンド用のアドレス）の検証を店舗が実施困難な場合に発生しうる攻撃である[18]．例えば，悪意を有する顧客が（結託した）第三者のアドレスをリファンド用として店舗に伝え，その第三者が暗号資産を入手すると同時に，店舗に伝えたアドレスを「自分が伝えたものではない」と主張して顧客自らも暗号資産の入手を試みることが想定される．対策としては，リファンド用のアドレスに顧客の署名を付与するなど，店舗がその正当性を検証できるようにすることが挙げられる．

秘密鍵の推定に関しては，ユーザーが選んだパスフレーズから秘密鍵を生成するケース（ブレイン・ウォレット）において，秘密鍵を高速に探索する手法が提案されている[19]．これをビットコインに適用すると，クラウドのリソースを約 56 ドルで調達して 18,000 個以上の秘密鍵を発見できた旨が報告されている．また，取引データに付与する署名の生成に乱数（ナンス）を用いるケースでは，ナンスの分布に偏りが生じると秘密鍵が容易に推定されうることが知られている[20].

プログラムのバグ等に関しては，イーサリアムのスマート・コントラクトのプログラムの脆弱性とその影響の分析結果が発表されている[21]．例えば，不適切な関数の呼出しによるフォールバックや，処理の繰返しによる無限ループ等が発生しうることが指摘されている．

今後も，暗号資産に関する脆弱性や攻撃が新たに発見・検知される可能性がある．仮に，そうした脆弱性等が深刻なリスクにつながりうるものであった場合，暗号資産のサービスを停止し，脆弱性を解消したうえで，新方式を周知・実装しつつ暗号資産のサービスを再開することが求められる．こうした点を踏まえると，脆弱性等に関する情報を関係者の間で適切に共有し，脆弱性の解消に向けた対応のあり方を予め検討しておくことが重要である．

脆弱性等に関する情報の共有やその後の対応については，金融分野をはじめとする重要インフラ分野において，情報を共有する関係者の特定，情報の流れの整備，実際の対応にかかる訓練等が既に行われている．暗号資産における脆弱性等の対応を検討する際には，こうした知見も有用であると考えられる．

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，暗号資産に特有のリスク，研究者と技術者との間の情報共有や連携のあり方について議論された．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) 伝統的な金融サービスと比較した暗号資産のセキュリティ面の特性と課題

- 暗号資産も伝統的な金融サービスも，利用者のアカウントや秘密鍵の管理が重要であるという点で共通している．一方，暗号資産には，耐改ざん性と高可用性によるリスクが存在する点が異なる．つまり，暗号資産の不正な取引が検知された場合等において，それに関するデータをブロックチェーン上で遡及的に修正することができないほか，システムを停止することができないという問題がある．
- 暗号資産に関するサービスは利便性が優先される傾向が強く，伝統的な金融サービスと比べてセキュリティ管理の運用に問題が発生するケースが多い．利便性を犠牲にすることなくセキュリティを確保するための工夫を行っている企業のノウハウを，暗号資産に関連するサービス事業者のコミュニティにおいてどの程度共有できるかが，重要な論点の 1 つであろう．
- 暗号資産の取引は匿名性が高く，不正に取得した暗号資産の資金洗浄が比較的容易であることから，従来の金融サービスのシステムに比べて攻撃者に狙われやすい．こうしたリスクを軽減させる目的で取引の匿名性を低下させると，取引に関する各利用者のプライバシーは低下してしまうため，リスクとプライバシーの両方をいかにバランスさせるかが課題である．

(2) 暗号資産における脆弱性対応

（信頼できる第三者や中央集権的な仕組みの必要性）

- かつて，ビットコインのブロックチェーンにおいて，予め設定されていた発行上限を超える額のビットコインを発行できてしまう脆弱性が明らかになった．それを解消するためのパッチを適用する際に，適用タイミングによって各ノードにおける処理が異なってしまう可能性が課題となった．そこで，ビットコインの全ノードの過半数のノード群が協力し，特定のタイミングで同時にパッチを適用することとなった．本事例では，同時にパッチ適用を行ったノード群があたかも「信頼できる第三者」のように行動しており，信頼できる第三者が存在しなくても適切に動作するというビットコインの設計指針と矛盾しているだろう．
- 何らかの不具合を解消するために暗号資産の仕様を後から変更することは容易でない．脆弱性対応を円滑に行うためには，暗号資産に中央集権的な仕組みを導入することも視野に入れてはどうか．
- ウェブ・アプリケーションやソフトウェア製品の脆弱性への対応として，脆弱性やインシデントに関する情報の共有や，脆弱性解消に向けたソフトウェア・ベンダーとの連携等に関して，JPCERT コーディネーション・センター等による国際的な枠組みが整備された．暗号資産における脆弱性の対応についても，こうした既存の枠組みを活用することができるのではないか．

（ソフトウェアの開発やメンテナンスにおけるインセンティブ・メカニズム）

- ビットコインのプログラム開発はビットコイン・コア等の技術者のコミュニティによって進められるものの，それらのコミュニティやそれを構成する技術者は，作成したプログラムに対する責任を法的に負っているわけではない．脆弱性に関する情報が寄せられたとしても，対応するか否かは各技術者の善意に委ねられることになるだろう．
- マイニングに対しては報酬が準備されている一方，安全なソフトウェアの開発やメンテナンスについては報酬が準備されておらず，インセンティブ・メカニズムとして不十分ではないかとの意見も聞かれる．プログラムのバグに関する情報を受け付ける主体や，そのバグや修正プログラムをテスト・検証する主体を準備することが必要であるとともに，メンテナンス等への対応に報酬を支払うシステムの導入が有用であろう．
- 報酬システムにおいては，悪意を有する参加者の存在を前提としたうえで，善意の参加者が安全に報酬を受け取ることができるように設計する必要がある．
- 報酬の原資の確保に関して，OpenSSL の事例では，当初は資金が乏しく十分なメンテナンスを期待できない状況であったが，その後，大手ベンダーによる支援によって適切なメンテナンスが行われるようになったように，暗号資産においても，将来，大手のカストディ事業者がこうした役回りを引き受けるようになる可能性もある．

(3) 研究者と技術者の情報連携

（情報連携に関する課題）

- 暗号資産の脆弱性に関する研究成果が日々研究者によって公表されているものの，研究者と（暗号資産のサービスに携わる）技術者との間で十分に共有されていないのではないか．
- 研究者の立場としては，学術的な成果をさまざまな場で発信していくことが必要であるが，研究集会での発表だけでは，企業の実務者や技術者に伝わらない場合もある．
- 研究者，技術者，実務者，規制当局の担当者等，暗号資産に関わる利害関係者が一堂に会し，暗号資産やセキュリティに関する用語や概念について認識を共有したうえで，最新の研究成果をどのようにビジネス・モデルや規制に反映させていくかを検討する枠組みが必要ではないか．
- 研究と実務の両方を理解し，研究者と技術者の橋渡し役として機能する人材や組織が必要である．例えば，暗号資産の不正な取引を検知した際に，疑わしい（暗号資産の）複数のアカウントや（そのアカウントの所有者の）銀行口座を凍結するか否かを判断することが必要になりうるが，暗号資産に関するサービス事業者と金融機関の双方の事情に精通している人材が議論に加わらないと対処が難しいであろう．

（CGTF の活動）

- 暗号資産の分野においても，各事業者において責任ある立場の人材が自主的に集まり，研究者との対話や情報共有の仕組みの整備を含め，業界としての対応を検討することができる場が必要であろう．そうした場の 1 つとして，わが国では，暗号資産やセキュリティの学識経験者らが中心となって CGTF（Cryptoassets Governance Task Force）が立ち上げられ，暗号資産に関するセキュリティ対策のあり方やベスト・プラクティスについて調査・研究が開始されている．
- 現時点では，CGTF 等の活動が一般に広く認知されておらず，活動内容の情宣を強化し，賛同者や協力者を増やしていくことが必要である．そのうえで，金融 ISAC のような体制を整備することができれば理想的ではあるものの，直ちに実現させることは困難であり，徐々に規模を拡大させながら内容の充実を図っていくことが求められる．

(4) 暗号資産のセキュリティにかかる研究課題と今後の展望

（デバイスや鍵の管理）

- 暗号資産のセキュリティを確保していくうえで，ウォレットに保管されている秘密鍵を保護することが重要である．秘密鍵は，利用者自身が自分のデバイス（ハードウェア・ウォレット等）で保護・使用するケースと，取引所等に保管を依頼するケースがあるが，前者については，利用者が自分で適切にデバイスを管理することが求められる．
- 専門家でない利用者からは，「暗号資産のサービスに関しては，馴染みの薄い専門用語が多くて理解しづらい」との声が聞かれることもあり，利用者によるデバイスや鍵の管理が適切に実施されない可能性がある．
- 既知の脆弱性に対しては，暗号資産の場合でも一般的な情報システムの場合と同様のセキュリティ対策を適用することができる．例えば，利用者の秘密鍵の管理については，中央集権型ではあるが，公開鍵暗号基盤における認証局業者の管理・運用体制やセキュリティ・プラクティスが参考になる．
- 多様なアプリケーションにおける本人確認にパスワードが使用されているが，アプリケーションごとに異なる（強力な）パスワードを覚えて使用することは困難となっている．例えば，利便性を考慮して，生体認証をパスワードと組み合わせて活用するなどの対応が有効ではないか．こうした対応を実現するために活用するソリューションについてもセキュリティ管理についてルール等を設けたうえで，適切に運用していくことが求められる．

（テストや検証）

- 近年，システムの設計書や仕様書を作成せずに直接プログラミングを行うケースが多いが，そうしたケースでは，完成したシステムのセキュリティの検証が難しくなるのではないか．
- 規模が比較的小さい組織の場合，テストや検証を行うためのドキュメントを作成し，それらを用いてプログラム等の品質を管理する対応が困難である場合も想定され，テスト等を外部の業者に委託することも選択肢として考えられる．
- システムの品質は開発に携わった技術者のレベルに依存することから，技術者のスキルを向上させることが重要であり，中長期的に技術者の教育をどのように進めるかを議論することが必要である．
- これまでに電子決済システムの研究開発において研究者や技術者として活躍していた人材の多くが，現在，企業等の要職にあり，第一線の研究者や技術者に直接ノウハウを伝授することが難しくなってきている．こうしたノウハウをどのように継承していくかが大きな課題である．
- 暗号資産の各ステークホルダーが，セキュリティ対策に関してそれぞれどのような役割を担い，それらをどの程度達成しているかについて現状を整理し，課題を明確にすることがまず必要である．そのうえで，これまでの研究成果の知見をどのように活用できるかを検討することが重要である．

（標準化）

- ビットコインやイーサリアムにおける技術仕様がそれぞれ BIP（Bitcoin Improvement Proposals），EIP（Ethereum Improvement Proposals）として作成・公開されているものの，個々のドキュメントにおける記述の粒度等が区々であるなど，ドキュメントの品質向上が必要になっている．RFC のように，ドキュメントの記述レベル等を標準化することがまず必要であろう．
- セキュリティに関する標準化を検討する際には，一般に，①（個々の）要素技術，②実装，③運用という 3 つのレイヤーに分けて考える必要がある．暗号資産やブロックチェーンの標準化においても，各レイヤーに関与する主体が相互に連携しつつ標準化のあり方を議論していくという姿勢が重要である．
- ブロックチェーンに関連する国際標準化が ISO/TC307 において審議されており，ブロックチェーンのセキュリティ，取引所やカストディ事業者におけるセキュリティも対象になっている．ブロックチェーンに関連する技術分野の研究開発のスピードが非常に速く，国際標準としてコンセンサスが得られる状況に至っていないことから，当面は，技術報告書として取りまとめたうえで，内容を定期的にアップデートすることになるであろう．
- 汎業界向けのセキュリティに関する国際標準化を担当する ISO/IEC JTC1/SC27 において，情報システムのセキュリティ管理に関する国際標準 ISO/IEC 27002 が標準化されており，こうした既存の国際標準を活用することができる．

3. おわりに

第 21 回情報セキュリティ・シンポジウムでは，暗号資産のセキュリティを巡る最新の研究動向が紹介されたほか，パネル・ディスカッションでは，そうした研究成果を暗号資産の実務に活用するうえで解決すべき課題についてさまざまな意見が示された．現時点では，暗号資産のセキュリティ対策には多くの課題が残されているが，安全なエコシステムを形成していくためには，これらの課題や最新の研究動向を十分に認識したうえで，適切な対策を講じたり用途を検討したりすることが望まれる．今後も，最新の研究

動向や国際標準化の動向をフォローするとともに，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] 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 21 回情報セキュリティ・シンポジウム 暗号資産のセキュリティ」，2019 年（https://www.imes.boj.or.jp/citecs/symp/21/index.html，参照 2020-02-05).
[2] 日本銀行金融研究所,「情報セキュリティ・シンポジウム（第 21 回）の模様：暗号資産のセキュリティ」，IMES Discussion Paper Series, no. 2020-J-2，日本銀行金融研究所，2020 年
[3] 金融情報システムセンター,「令和元年度金融機関アンケート調査結果」，金融情報システム，no.347，金融情報システムセンター，2019 年，p.60.
[4] Nakamoto, Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008 (https://bitcoin.org/bitcoin.pdf，参照 2019-12-20).
[5] European Telecommunications Standards Institute, EN 319 122-1, V 1.1.1, Electronic Signatures and Infrastructures (ESI); CAdES Digital Signatures; Part 1: Building Blocks and CAdES Baseline Signatures, European Telecommunications Standards Institute, 2016.
[6] Sato, Masashi, and Shin'ichiro Matsuo, Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography, Proceedings of International Conference on Computer Communication and Networks (ICCCN) 2017, IEEE, 2017, pp.1-8.
[7] Matzutt, R. et al., A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin, Proceedings of International Conference on Financial Cryptography and Data Security (FC) 2018, Lecture Notes in Computer Science, 10957, Springer-Verlag, 2018, pp.420-438.
[8] Sato, Teppei, Mitsuyoshi Imamura, and Kazumasa Omote, Threat Analysis of Poisoning Attack against Ethereum Blockchain, presentation at International Conference on Information Security Theory and Practice (WISTP) 2019, 2019.
[9] Ali, S. T. et al., ZombieCoin: Powering Next-Generation Botnets with Bitcoin, Proceedings of International Conference on Financial Cryptography and Data Security (FC) 2015, Lecture Notes in Computer Science, 8976, Springer-Verlag, 2015, pp. 34-48.
[10] Ali, S. T. et al., ZombieCoin 2.0: Managing Next-Generation Botnets Using Bitcoin, International Journal of Information Security, 17 (4), Springer-Verlag, 2018, pp. 411-422.
[11] 田口 涉・今村光良・面 和成,「ブロックチェーン技術の分散性による無停止メカニズムのリスク分析」, 情報処理学会研究報告，2019-CSEC-86 (4)，情報処理学会，2019 年，pp.1-6.
[12] Giechaskiel, Ilias, Cas Cremers, and Kasper B. Rasmussen, On Bitcoin Security in the Presence of Broken Cryptographic Primitives, Proceedings of European Symposium on Research in Computer Security (ESORICS) 2016, Lecture Notes in Computer Science, 9879, Springer-Verlag, 2016, pp.201-222.
[13] Sato, Masashi, and Shin'ichiro Matsuo, Long-Term Public Blockchain: Resilience against Compromise of Underlying Cryptography, Proceedings of International Conference on Computer Communication and Networks (ICCCN) 2017, IEEE, 2017, pp.1-8.
[14] Eyal, Ittay, and Emin Gün Sirer, Majority Is Not Enough: Bitocoin Mining Is Vulnerable, Communications of the ACM, 61(7), Association for Computing Machinery, 2018, pp.95-102.
[15] Pass, Rafael, and Elaine Shi, Fruitchains: A Fair Blockchain, Proceedings of ACM Symposium on Principles of Distributed Computing (PODC) 2017, Association for Computing Machinery, 2017, pp.315-324.
[16] Zhang, Ren, and Bart Preneel, Publish or Perish: A Backward-Compatible Defense against Selfish Mining in Bitcoin, Proceedings of Cryptographers' Track at the RSA Conference (CT-RSA) 2017, Lecture Notes in Computer Science,10159, Springer-Verlag, 2017, pp.277-292.
[17] Han, R. et al., Sucker Punch Makes You Richer: Rethinking Proof-of-Work Security Model, Cryptology ePrint Archive: Report 2019/752, International Association for Cryptologic Research, 2019.
[18] McCorry, Patrick, Siamak F. Shahandashti, and Feng Hao, Refund Attacks on Bitcoin's Payment Protocol, Proceedings of International Conference on Financial Cryptography and Data Security (FC) 2016, Lecture Notes in Computer Science, 9603, Springer-Verlag, 2017, pp.581-599.
[19] Courtois, Nicolas, Guangyan Song, and Ryan Castellucci, Speed Optimizations in Bitcoin Key Recovery Attacks, Tatra Mountains Mathematical Publications, 67, De Gruyter, 2016, pp.55-68.
[20] Breitner, Joachim, and Nadia Heninger, Biased Nonce Sense: Lattice Attacks against Weak ECDSA Signatures in Cryptocurrencies, Proceedings of International Conference on Financial Cryptography and Data Security (FC) 2019, Lecture Notes in Computer Science, 11598, Springer-Verlag, 2019, pp.3-20.
[21] Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli, A Survey of Attacks on Ethereum Smart Contracts SoK, Proceedings of International Conference on Principles of Security and Trust, Lecture Notes in Computer Science, 10204, Springer-Verlag, 2017, pp.164-186.

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 90 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，金融機関の実務者から 27 件の回答を得た（全体では 65 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今後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：情報処理推進機構による「情報セキュリティ 10 大脅威 2019」の各項目において，貴社においても同様の課題があると思われる項目や，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，貴社において脅威となりうると考えられる項目（金融サービス等を提供する情報システム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 とキャッシュレス決済

質問イでは，「FinTech（オープン API 等）」が最も高い回

答割合（52%）であった．これに次いで高い回答率（41%）となったのが「リテール金融取引（QR コード決済等キャッシュレス決済)」であった．

(2) 足許の情報セキュリティ上の課題：標的型攻撃による被害と内部不正による情報漏えい

質問ロでは，「標的型攻撃による被害」や「内部不正による情報漏えい」が高い回答率（それぞれ 44%，41%）となった．

(3) 今後脅威となりうる対象：顧客の端末とクラウド上のシステム

質問ハでは，「顧客の端末（PC，スマホ）への攻撃」や「クラウド上のシステムへの攻撃」が高い回答率（それぞれ 48%，44%）となった．

表 A-1　シンポジウムでのアンケート集計結果

	金融機関 (27)	ベンダー (12)	大学・研究機関等(7)	その他 (19)	全体 (65)
イ．今後取り上げてほしいトピック（数字は回答割合）					
FinTech（オープンAPI等）	52%	50%	43%	74%	57%
暗号技術（高機能暗号、暗号の移行等）	11%	17%	29%	16%	15%
リテール金融取引（QRｺｰﾄﾞ決済等ｷｬｯｼｭﾚｽ決済）	41%	33%	29%	37%	37%
サイバー攻撃	4%	42%	14%	11%	14%
認証技術（生体認証等）	19%	42%	43%	16%	25%
クラウド	37%	25%	43%	26%	32%
インターネット・バンキング	37%	50%	29%	42%	40%
IoT機器	33%	42%	43%	11%	29%
分子・DNAを活用する情報技術・ｺﾝﾋﾟｭｰﾃｨﾝｸﾞ	7%	17%	14%	5%	9%
モバイル端末	15%	17%	14%	0%	11%
ロ．「情報セキュリティ10大脅威2019」のうち、貴組織においても課題があると思われる事項（数字は回答割合）					
標的型攻撃による被害	44%	8%	29%	42%	35%
ビジネスメール詐欺による被害	22%	25%	14%	16%	20%
ランサムウェアによる被害	19%	0%	14%	16%	14%
サプライチェーンの弱点を悪用した攻撃の高まり	26%	8%	14%	16%	18%
内部不正による情報漏えい	41%	42%	0%	16%	29%
サービス妨害攻撃によるサービスの停止	30%	0%	0%	11%	15%
インターネットサービスからの個人情報の窃取	33%	25%	14%	26%	28%
IoT機器の脆弱性の顕在化	7%	8%	14%	21%	12%
脆弱性対策情報の公開に伴う悪用増加	4%	17%	14%	0%	6%
不注意による情報漏えい	19%	42%	14%	26%	25%
ハ．今後脅威となりうると考えられる事項（数字は回答割合）					
顧客の端末（PC、スマホ）への攻撃	48%	17%	14%	16%	29%
金融機関対外接続系システム（WEBｻｰﾋﾞｽ、ｲﾝﾀｰﾈｯﾄ･ﾊﾞﾝｷﾝｸﾞ等）への攻撃	37%	17%	29%	16%	26%
金融機関情報系システム（電子メール、EPR等）への攻撃	15%	8%	29%	21%	17%
クラウド上のシステムへの攻撃	44%	33%	14%	26%	34%
社員の端末（行員のPCやタブレット等）への攻撃	33%	17%	14%	53%	34%
金融機関勘定系システムへの攻撃	7%	8%	0%	0%	5%
金融機関の設備制御系システム（空調、監視ｶﾒﾗ、IoT機器等）への攻撃	0%	0%	0%	5%	2%
FinTech企業への攻撃	37%	17%	14%	26%	28%
AIを用いたサービスに対する攻撃	19%	8%	14%	16%	15%

（備考）表中の括弧内の数字は、各分野における回答者数を示す。