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」の模様

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、2019 年 12 月 9 日、「暗号資産のセキュリティ」をテーマとして、第 21 回情報セキュリティ・シンポジウムを開催した。

近年、ビットコインをはじめとする、ブロックチェーンを利用した暗号資産が注目を集めている。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、今回のシンポジウムでは、暗号資産のセキュリティを巡る最新の研究動向について講演を行うとともに、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パネル・ディスカッションを行った。当日は、情報セキュリティ技術にかかわる金融機関関係者、暗号資産に関連するサービスを提供する企業等の実務者、研究者、システム開発・運用に携わる技術者等、約 90 名が参加した。本稿では、下記のプログラムに沿って、シンポジウムにおける議論の概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）[1]。

本稿に示されている意見はすべて発言者たち個人に属し、その所属する組織の公式見解を示すものではない。

1 文中の各参加者の所属と肩書きはシンポジウム開催時点のものである。

【第 21 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「暗号資産に関するセキュリティの概観と研究動向」
  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
- 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. キーノート・スピーチ「暗号資産に関するセキュリティの概観と研究動向」

松尾は、暗号資産のセキュリティにかかる最近の研究動向や課題について、以下のとおり発表した。

(1) 暗号資産の用途とセキュリティ

代表的な暗号資産の 1 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（Nakamoto [2008]）。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。

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。

(2) 暗号資産を構成する要素技術

暗号資産やそれを構成する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い。むしろ、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[2]。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[3]。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。

2 タイムスタンプ方式は、データが特定の時刻に存在していたことや、データ系列におけるデータの存在の順序関係を証明することを目的とする暗号プロトコルであり、ブロックチェーンと同様に、ハッシュ関数を用いて一連のデータの前後関係を証明する方式も提案されている（Haber and Stornetta [1991]）。ヒステリシス署名（hysteresis signature）は、デジタル署名付きデータの改変の有無を長期間証明可能にするための暗号プロトコルであり、署名付きデータをハッシュ化し、その後に生成された署名付きデータにハッシュ値を埋め込むことによって、署名付きデータの系列に連鎖構造を持たせる点が特徴である（洲崎・松本［2002］）。

3 グループ署名は、署名を生成したユーザーが特定の署名者のグループに含まれていることを確認できるものの、どのユーザーが署名者かを特定することができないという署名方式である。ミックスネット（mix-net）は、データの送信者の匿名性を高めた通信路（匿名通信路）を実現する手法の 1 つであり、通信路上の複数のサーバがデータに暗号処理を施すとともに、データの送信順序を入れ替えることによって、送信者を特定困難にするものである。オニオン・ルーティング（onion routing）は、ミックスネットを改良した匿名通信路の実現手法であり、データの送信順序の入替えを行う代わりに、ダミーのデータを送信するなどによって、より高速での双方向通信を可能としている。オニオン・ルーティングは、トーア（Tor）と呼ばれることもある。

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[4]。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。

(3) 暗号資産のセキュリティ上の課題

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（European Telecommunications Standards Institute [2016]、Sato and Matsuo [2017]）[5]。

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

4 モンデックス（Mondex）は、ナショナル・ウエストミンスター銀行とモンデックス・インターナショナル社が 1990 年に開発した方式であり、利用者間で金銭的価値を転々流通させることができる点が特徴である。日本銀行・NTT 電子現金方式は、こうした転々流通性に加えて、データの流通経路を事後的に追跡する機能を実現している点が特徴である（森畠ほか［1997］）。

5 長期署名フォーマットは、デジタル署名付きデータに関して、それを生成したユーザーや改変の有無を 10 年以上の長期間にわたって確認できるようにするためのデータ・フォーマットであり、欧州における電気通信技術の標準規格を策定する欧州電気通信標準化機構（European Telecommunications Standards Institute: ETSI）によって標準化されている。

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。

3. 講演 1「暗号資産のセキュリティを巡る最新動向（1）」

面は、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、以下のとおり説明した。

(1) 暗号資産における 2 つの特徴

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。

(2) ブロックチェーン汚染のリスクとその影響

イ. ブロックチェーン汚染

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）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、機密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（Matzutt *et al.* [2018]）。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（Sato, Imamura, and Omote [2019]）。

ロ．ボットネットによる攻撃と影響

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（Ali *et al.* [2015, 2018]）。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）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。

ハ．ブロックチェーン汚染の拡大容易性

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[6]。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。

(3) ブロックチェーンの無停止性のリスク

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（田口・今村・面［2019］）。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

6 ここでのエクスプローラーは、ブロックチェーン上のデータを検索するエンジンである。

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。

4. 講演 2「暗号資産のセキュリティを巡る最新動向（2）」

宇根は、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とおり発表した。

（1） 暗号資産の構成要素と脆弱性・攻撃

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。

（2） 主な研究事例

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ある（Giechaskiel, Cremers, and Rasmussen [2016]）。対策としては、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（Sato and Matsuo [2017]）。

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、善意の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（Eyal and Sirer [2018]）。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、Pass and Shi [2017]、Zhang and Preneel [2017]）。

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（Han *et al.* [2019]）。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（McCorry, Shahandashti, and Hao [2016]）。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（Courtois, Song, and Castellucci [2016]）。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（Breitner and Heninger [2019]）。

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（Atzei, Bartoletti, and Cimoli [2017]）。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。

(3) 暗号資産の脆弱性に関する情報の共有と対応

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[7]。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。

5. 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」

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を行った。これらの議論を行ううえでの参考情報として、まず、鎌田は、金融分野における脆弱性の情報共有やインシデント対応に関する活動を行っている金融 ISAC について紹介したほか、曾川は、電子決済のサービスを提供するシステムの開発・運用にかかる事例や経験を説明した[8]。その後の議論の概要は以下のとおりである。

(1) 伝統的な金融サービスと暗号資産におけるセキュリティの差異

まず、モデレータの松尾は、伝統的な金融サービスと暗号資産を比較した際に、セキュリティ対策上のポイントやリスクに関してどのような違いがあるかをパネリストに問うた。

面は、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と述べたうえで、講演 1 において紹介したように、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と説明した。すなわち、暗号資産の不正

7 わが国では、重要インフラ分野の事業者間における脆弱性等の情報の共有や分析、訓練等を担う枠組みとして、セプター（Capability for Engineering of Protection, Technical Operation, Analysis and Response: CEPTOAR）が分野ごとに整備されている。金融分野においては、銀行、証券、生命保険、損害保険の各分野にセプターが整備されている。

8 金融 ISAC は、わが国の金融分野においてサイバーセキュリティに関する情報の共有・分析、安全性の向上のための協働活動を行い、金融サービスの利用者の安心・安全を継続的に確保することを目的する一般社団法人であり、2014 年に設立された。

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と指摘した。

鎌田は、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との見方を示した。また、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という面があると説明した。セキュリティ管理の運用に関して、鎌田は、暗号資産に関連するサービス事業者のなかには、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も少なくなく、そうしたノウハウを同業者のコミュニティにおいてどの程度共有できるかが、セキュリティ管理に関する問題を解消していくうえで重要な論点の 1 つであろうと述べた。

曾川は、鎌田や面の意見に賛意を表したうえで、攻撃の対象になりやすいという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と説明し、こうしたリスクとプライバシーの両方をどのようにバランスさせるかが課題になるとの見方を示した。

(2) 暗号資産における脆弱性への対応

暗号資産における脆弱性への対応のあり方に関連して、松尾は、まず、過去のビットコインにおけるプログラムのバグ対応の事例を紹介した。そのバグは、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というものであり、それを解消するためのパッチが準備されたものの、パッチ適用の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といった問題が発生しうることが判明した。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を決め、適用した直後に当該バグの存在を公表した。この事例に関して、松尾は、パッチ適用のタイミング等を決定し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のではないかとの見方を示した。

これを受けて、面は、松尾が示した事例が「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が容易でない」という教訓を残したといえると述べた。そのうえで、脆弱性への対応を円滑に行うために、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との見方を示した。また、ブロックチェーンのプログラムに脆弱性が発見された場合、全参加者がプログラムを修正

する必要があるため、脆弱性を悪用した攻撃が実行される前に修正を進める方法を検討することが求められると述べた。

鎌田は、2000 年代初より、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、脆弱性に関する情報の受付窓口を設置することが必要であるとの機運が高まり、その後、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（Japan Computer Emergency Response Team）コーディネーションセンター等によって国際的な枠組みが整備された経緯を紹介した[9]。そのうえで、暗号資産における脆弱性への対応についても、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と述べた。

松尾は、ホワイト・ハッカーや学界の研究者が脆弱性を発見すると、一般的な情報システムの場合であれば、それを開発ベンダーに連絡し、開発ベンダーが修正プログラムを作成してセキュリティを確保する道筋が確立した後に、関連する論文を発表する、「責任ある開示（Responsible Disclosure）」と呼ばれる標準的な手続きが存在すると述べた。ビットコインの場合には、プログラムの開発はビットコイン・コア（Bitcoin Core）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く、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のではないかとの見方を示した。

これに関して、曾川は、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と説明した。そして、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と述べた。さらに、そうした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と説明した。報酬の原資の確保に関して、OpenSSL の事例を紹介し、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として、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との見方を示した[10]。

9 JPCERT コーディネーションセンターは、インターネットを介して発生するセキュリティ・インシデントに関して、国内における報告の受付、対応の支援、発生状況の把握、手口の分析、対策の検討・助言等を行っている非営利団体である。海外の CERT とも連携し、インシデントに関する情報の国際的な共有等も行っている。

10 OpenSSL は、インターネット・バンキング等で用いられる暗号通信プロトコル TLS（Transport Layer Security）等を実装するための代表的な暗号ライブラリである。

フロア参加者から、暗号資産においては、運用における脆弱性が顕在化して生じたインシデントが多いようにみられるが、セキュリティ管理の運用において、従来の金融サービスと暗号資産とでどのような点が異なっているかとの質問があった。

これに対して、曾川は、従来の金融サービスでは、実績のあるソフトウェアを比較的多く使用する傾向にあるほか、運用に関する知見の蓄積も多いとの認識を示した。もっとも、いかなるプログラムにも脆弱性が存在する可能性を否定できず、従来の金融サービスと暗号資産のいずれにおいても、脆弱性が顕在化することを想定したうえで、その被害を最小限に留めるように対処方法を予め検討しておくことが求められると説明した。

(3) 研究者と技術者の情報連携

松尾は、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との問題を提起した。そのうえで、研究者と技術者の情報連携のあり方についてパネリストに問うた。

面は、研究者の立場として、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り、国内であれば、電子情報通信学会主催の「暗号と情報セキュリティシンポジウム」や情報処理学会主催の「コンピュータセキュリティシンポジウム」等、大勢の研究者が集まる研究集会で発表することが多いと説明した。もっとも、こうした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との見方を示した。

曾川は、研究者、技術者、実務者、規制当局の担当者等、暗号資産にかか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と述べた。

鎌田は、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との見方を示した。例えば、暗号資産の不正な取引を検知した際に、疑わしい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のではないかと述べた。そのうえで、金融 ISAC の会員となっている金融機関についてみると、IT 関連の企業やセキュリティ・ベンダー等、金融業界以外から金融機関へ転職してきた、IT に詳しい人材が橋渡し役となって活躍しているケースが多いと説明した。

これを受けて、松尾は、暗号資産の分野においても、金融 ISAC のように、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はないかとの見方を示した。また、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ことを紹介した[11]。

曾川は、現時点では、CGTF 等の活動が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との見方を示した。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と述べた。

(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

松尾は、暗号資産のセキュリティを確保していくうえでどのような研究を優先的に進めるべきかについて、パネリストに意見を求めた。

面は、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との見解を示した。秘密鍵は、利用者が自分のデバイス（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と述べた。もっとも、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、生成方法が煩雑であるという理由から「安全性の高いパスワードがあまり使用されていない」という事例と同様に、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と指摘した。

鎌田は、暗号資産の各利害関係者が、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と述べた。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との見方を示した。

研究成果の知見の活用に関して、松尾は、これまでにさまざまな電子決済システムの研究開発が進められ、その知見が蓄積されたとしたうえで、以前、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

11 CGTF は、暗号資産の利用者を保護するために、暗号資産の取引等に関するリスク管理のための安全対策基準の策定を目的として 2018 年に設立された研究会である。セキュリティ技術の専門家や暗号資産の交換業者の実務者等によって構成されている。

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として、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と説明した。

曾川は、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と説明した。例えば、秘密鍵の管理に関しては、利用者が取引所等に管理を委託するケースであれば、委託先がそうした管理を適切に実行することが利用者から期待される。こうした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との見方を示した。また、面が示したパスワードに関する問題について、曾川は、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と指摘したうえで、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と述べた。さらに、こうした対応を実現する際には、なんらかのソリューションを活用することになるが、その場合も、ソリューションにおけるセキュリティ管理についてルール等を設けたうえで、それらに沿って適切に運用していくことが求められると付言した。

松尾は、近年、システムの設計書や仕様書を作成しないで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と述べたうえで、どのような対応が考えられるかをパネリストに問うた。

これに対して、曾川は、自社では、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していると説明した。もっとも、規模が比較的小さい組織の場合、そうした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と述べた。また、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と述べた。

設計書等のドキュメントについて、松尾は、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という問題意識を示した。そのうえで、RFC（Request for Comments）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と補足した[12]。

12 RFC は、インターネット上で使用される各種の技術仕様を規定する標準規格であり、技術者らによる任意団体である IETF（Internet Engineering Task Force）において策定されている。

最後に、フロア参加者から、ブロックチェーンのセキュリティに関する標準化を今後どう進めていくべきかについて質問があった。

鎌田は、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としたうえで、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との見解を示した。

松尾は、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と説明した[13]。そのうえで、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との見方を示した。また、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と述べ、パネル・ディスカッションを締め括った[14]。

13 ISO/TC307 は、ブロックチェーンと電子分散台帳技術に関する国際標準化を担当する専門委員会である。

14 ISO/IEC 27002 は、企業等における情報システムのセキュリティ管理の枠組み（情報セキュリティ・マネジメント・システム）やそのベスト・プラクティスを規定する国際標準である。

参考文献

洲崎誠一・松本　勉、「電子署名アリバイ実現機構―ヒステリシス署名と履歴交差」、『情報処理学会論文誌』、第 43 巻第 8 号、情報処理学会、2002 年、2381～2393 頁

田口　渉・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」、『電子情報通信学会技術研究報告』、第 119 巻第 140 号、電子情報通信学会、2019 年、23～28 頁

森畠秀実・阿部正幸・藤崎英一郎・中山靖司、「電子現金方式」、1997 年暗号と情報セキュリティシンポジウム発表論文、電子情報通信学会、1997 年

Ali, Syed Taha, Patrick McCorry, Peter Hyun-Jeen Lee, and Feng Hao, "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.

———, ———, ———, and ———, "ZombieCoin 2.0: Managing Next-Generation Botnets Using Bitcoin," *International Journal of Information Security*, 17(4), Springer-Verlag, 2018, pp. 411–422.

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.

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.

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.

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.

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.

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.

Haber, Stuart, and Wakefield Scott Stornetta, “How to Time-Stamp a Digital Document,” *Journal of Cryptology*, 3(2), 1991, pp. 99–111.

Han, Runchao, Zhimei Sui, Jiangshan Yu, Joseph Liu, and Shiping Chen, “Sucker Punch Makes You Richer: Rethinking Proof-of-Work Security Model,” Cryptology ePrint Archive: Report 2019/752, International Association for Cryptologic Research, 2019.

Matzutt, Roman, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Müllmann, Oliver Hohlfeld, and Klaus Wehrle, “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.

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, 2016, pp. 581–599.

Nakamoto, Satoshi, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008 (available at https://bitcoin.org/bitcoin.pdf、2019 年 12 月 20 日).

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.

Sato, Teppei, Mitsuyoshi Imamura, and Kazumasa Omote, “Threat Analysis of Poisoning Attack against Ethereum Blockchain,” *Proceedings of IFIP International Conference on Information Security Theory and Practice (WISTP) 2019*, *Lecture Notes in Computer Scienc*e, 12024, Springer-Verlag, 2019, pp. 139–154.

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.

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 Scienc*e, 10159, Springer-Verlag, 2017, pp. 277–292.