2.4.5 システムのデジタルトラスト

（1）研究開発領域の定義

サイバー空間とフィジカル空間を高度に融合したシステムによるSociety5.0では、そこに参加するステークホルダーが増加し、システムの数も膨大となる。暗号技術が組み込まれたコンピューティング技術を用いて、人を介さずに自動的に複数のステークホルダーの複数のシステム間における信頼関係を検証・確立し、信頼できるシステムによる情報サービスの提供を実現するシステムのデジタルトラストに関する研究開発を行う領域である。

（2）キーワード

TEE（Trusted Execution Environment）、リモートアテステーション（Remote Attestation）、Hardware Root Of Trust（HW RoT）、Chain Of Trust（CoT）、トラストモデル、信頼関係（Trust Relationship）、コンフィデンシャルコンピューティング、ゼロトラストアーキテクチャー、プラットフォームセキュリティー

（3）研究開発領域の概要

［本領域の意義］

サイバー空間とフィジカル空間を高度に融合したSociety5.0においては、あらゆるもののデジタル化・コネクティッド化、スマート化・自律化が進み、さまざまなステークホルダーのシステムが参加することにより社会に価値を提供すると考えられる。この際、各ステークホルダーのシステム間における信頼関係の確立が必要となる。一方で「あらゆるもののデジタル化・コネクティッド化」という観点からは、膨大な数の信頼関係の確立とその維持が必要となり、「スマート化・自律化」という観点からは、人を介さないダイナミックな信頼関係の確立が要求される。

従来の人と人との間のトラストでは、トラストする側（Trustorと呼ばれる）はトラストされる側（Trusteeと呼ばれる）を信頼するか否かをトラストされる側の信頼性により人が判断してきた。 Society5.0では、トラストされる側（Trustee）が非常に複雑なシステムとなり、その複雑なシステムをトラストする側（Trustor）もシステムとなる場合が増加している。また、これらのシステムは企業内などに閉じたシステムに留まらず、場所に捉われない多くのステークホルダーのシステムが対象となり、膨大な数の信頼関係を、人を介さずにダイナミックに構築（確立と維持）することが求められる。

近年このような信頼関係構築の要求に対して、暗号技術が組み込まれたコンピューティグ技術などの発展により、トラストされる側（Trustee）のシステムの信頼性をトラストする側（Trustor）のシステムが自動的に検証（Verify）するトラストメカニズムの技術が進化してきている。こうした技術を用いてシステム間の信頼関係を構築するのがシステムのデジタルトラストである。システムのデジタルトラストにより、システム間の信頼関係を構築することは、例えば、自動運転車が不正なシステムに接続されてしまい不正な制御をされたり、不正にデータが搾取されたりするといった問題を防ぐことに繋がる。また、人を介さずにシステム間の信頼関係をダイナミック、かつ自動的に構築することにより、複数のステークホルダーが参画する場合においてもシステムを迅速に構築することが可能となり、必要なサービスを迅速に提供することが可能となる。

このように、システムのデジタルトラストは、サイバー空間とフィジカル空間を高度に融合したデジタル社会において、ユーザーが安全・安心に利用できるサービスを迅速に提供し、そこに参画するステークホルダーに価値を提供していく上で必須である。

［研究開発の動向］

❶ 研究開発のトレンド

システムのデジタルトラストの研究開発では、近年、トラストする側（Trustor）のシステムからトラストされる側（Trustee）のシステムの信頼性（Trustworthiness[1]）をリアルタイムに検証（Verify）する技術としてリモートアテステーションが注目されている。このリモートアテステーションがさまざまなデバイス、システムに組み込まれることにより、非常に複雑なシステム全体の信頼関係の構築を自動的、自律的に行うことが可能になりつつある。

リモートアテステーションにより信頼性の検証を可能とするためには、トラストされる側（Trustee）のシステムでは、信頼の基点（RoT：Root Of Trust）や信頼のおける実行環境（TEE：Trusted Execution Environment）[2]が用いられ、RoTには検証のための暗号鍵が組み込まれている。リモートアテステーションは、信頼のおける実行環境でRoTの暗号鍵を使って信頼性の検証を行い、システム間の信頼関係を確立する。システム間の信頼関係の繋がりはトラストチェーン（CoT：Chain Of Trust）と呼ばれており、その先のシステムの信頼性を検証していくことで、RoT を基点にCoTを拡張していくことができる。

信頼性を検証する際に必要となるRoTは信頼の基点となるものであり非常に高度なセキュリティーの実装が要求される。そのため、書き換えが容易なソフトウェアだけで達成することは困難であり、高度なハードウェアセキュリティーを施したHardware Root Of Trust（HW RoT）によりRoTを実現する取り組みが進められている。また、脆弱性を生みやすい一般的な汎用OSと分離されたTEEの実装も一般化してきており、このTEEにさまざまな Trustworthinessの検証が可能なリモートアテステーションのメカニズムを実装する取り組みも進められている（詳細は「2.4.5（4）注目動向［注目すべき国内外のプロジェクト］」に記載）。

一方、システムのデジタルトラストを考える際、デジタルトラストにより実現したいビジネスモデルとそのビジネスモデルが要求するトラストモデルの理解が不可欠であり、欧州Horizon 2020 では、マルチステークホルダーのシステム間の信頼関係構築を目指して、5Gやヘルスケア分野などのプロジェクトが進められている（詳細は「2.4.5（4）注目動向［注目すべき国内外のプロジェクト］」に記載）。

また、リモートアテステーションや信頼の基点、TEEが組み込まれたプラットフォームは、ゼロトラストアーキテクチャーやコンフィデンシャルコンピューティングでも活用されており、クラウドサービスの進化を支えている（詳細は「2.4.5（4）注目動向［新展開・技術トピックス］❶ゼロトラストアーキテクチャー、❷コンフィデンシャルコンピューティング」に記載）。

❷ 国際標準・規格

システムのデジタルトラストを実現する上で重要なリモートアテステーションは、インターネット技術の規格化を推進しているIETF（Internet Engineering Task Force）のRATS（Remote ATtestation ProcedureS）WG[1)] においてプロトコルなどの標準化が進められており、ユースケースやアーキテクチャーをまとめたドラフト文書が公開されている[2)]。米国・国立標準技術研究所（NIST：National Institute of Standards and Technology）の「NISTIR 8320 Hardware-Enabled Security」[3)] では、信頼の基点をHW RoTに実装し、TEE、リモートアテステーションを用いてCoTの範囲を拡張するセキュリティーメカニズムや、Intel、AMD、ARM、Ciscoなどによるさまざまな CoTの実装例が示されている。欧州の標準化団体である欧州電気通信標準化機構（ETSI：European Telecommunications Standards Institute）

1 Trustworthinessは、トラストされる側（Trustee）のシステムが持つ属性であり、システムのデジタルトラストでは例えばその品質などになる。トラストされる側（Trustee）のシステムがAIやIoTとした場合、それぞれに応じてTrustworthinessの意味するところが多義的になり、現在、標準化団体などによりこのTrustworthinessの定義に関する議論が盛んに行われている。

2 信頼できる実行環境は、エンクレーブ（Enclave）と呼ばれる場合もある。

の「ETSI GR SAI 006」[4] では、「Hardware security standardization ecosystem」での中でリモートアテステーションなどの標準化動向が紹介されている。

ゼロトラストアーキテクチャーについては、米国・NISTがゼロトラストアーキテクチャーの定義や原則、構成要素、ユースケース、脅威などをまとめたNIST SP800–207[5] を公開している。また、国内では、デジタル庁が「ゼロトラストアーキテクチャ適用方針」（2022年6月）を公開している。

（4）注目動向

［新展開・技術トピックス］

❶ ゼロトラストアーキテクチャー

近年、企業システムのクラウド化やリモートワークの普及により、インターネットを介して場所を問わずアクセスできるモバイルデバイスやクラウド環境の活用など、アクセス手段やシステムが多様化しており、これまでの外部からの攻撃を境界線で防御し内部は暗黙的に安全であると考える「境界線防御」のリスクが高まっている。ゼロトラストアーキテクチャーは、境界、および内部の全てのシステムを信頼せず、都度検証する「Never Trust, Always Verify」の考え方に基づいており、あらゆるシステムへのアクセスを検証するという考え方である。ゼロトラストアーキテクチャーについては、米国・NISTがゼロトラストアーキテクチャーの定義や原則、構成要素、ユースケース、脅威などをまとめたNIST SP800–207[5] を公開しているが、具体的な実装仕様は利用者に委ねられている。2021年5月に起きた米国の石油パイプライン施設へのサイバー攻撃などに対応すべく指示された米国大統領令[6]（2021年5月）では、ゼロトラストアーキテクチャーを適用することが求められている。

ゼロトラストアーキテクチャーの実装においては、認証で利用する認証器やハードウェアが本物であるか、さらにアプリケーションが本物であるかを検証するためにリモートアテステーションを利用することも検討されている。また、欧州・Horizon 2020のASSUREDプロジェクト[7] では、ゼロトラストアーキテクチャーの原則を取り入れ、システムの信頼性を検証して信頼関係を確立することによって、システム全体としての信頼性を確立しようとしている。このように、システムのデジタルトラストは、ゼロトラストアーキテクチャーにおいても重要な役割を持っている。

❷ コンフィデンシャルコンピューティング

クラウドサービスでは、ストレージ内に保存されているデータやシステム間で転送されているデータは暗号化により保護することが可能であるが、CPUがデータを処理する際のメモリ上のデータは暗号化されておらず、セキュリティーリスクが存在していた。この問題に対して、近年、CPUがデータを処理する際の使用中データ（data in use）の暗号化による保護が可能なコンフィデンシャルコンピューティングが注目されている。コンフィデンシャルコンピューティングでは、CPUにはHW RoTと信頼できる実行環境であるTEE（または、エンクレーブ）が組み込まれ、リモートアテステーションにより暗号化機能の完全性を検証し、TEEにおいてCPUの使用中データを暗号化している。コンフィデンシャルコンピューティングでは、使用中データの暗号化を保証するのは、クラウド事業者ではなくプロセッサーを提供する半導体ベンダーとなる。使用中データの暗号化機能を持つプロセッサーとしては、Intel SGX, Arm TrustZone, AMD SEVなどがあり、これらを利用したコンフィデンシャルコンピューティングが注目されている。また、2019年には業界団体であるコンフィデンシャルコンピューティング・コンソーシアムが設立されている[8]。

［注目すべき国内外のプロジェクト］

❶ 欧州・Horizon 2020のプロジェクト

5G分野では、5G–PPP（5G Infrastructure Public Private Partnership）[9] の中で、システムのデジタルトラストを中心的なテーマと捉えた5G–ENSURE（2015年11月～2017年10月）[10] や5GZORRO

（2019年10月～2022年10月）[11]、INSPIRE-5Gplus（2019年11月～2022年10月）[12]、MonB5G（2019年10月～2023年4月）[13] が推進されている。5G-ENSUREでは、5Gのトラストモデルを構築する取り組みが行われ、その後、5GZORRO、INSPIRE-5Gplus、MonB5Gでは、5Gのトラストモデルをベースとして5G機能を実装する取り組みが行われた。INSPIRE-5Gplusでは「5G ネットワーク管理のためのフレームワーク」の中でTEEとリモートアテステーションが利用されている。また、5GZORROでは、そのフレームワークの中でゼロトラストアーキテクチャーの原則が議論されている。

サイバーフィジカルシステム分野のASSURED（2020年9月～2023年8月）[7] では、ユースケースとしてスマート工場、スマートシティー、スマート宇宙、スマート衛星通信などが想定されており、自律的なサイバーフィジカルシステムの構築が目指されている。ここではセキュリティーやプライバシーを考慮して自律的にシステムのデジタルトラストを構築するためのフレームワークが提案されており、さまざまな箇所でリモートアテステーションのスキームが幅広く適用されている。また、ASSUREDでは、ゼロトラストアーキテクチャーの原則が採用されており、システム間の信頼関係を構築することによって、システム全体としての信頼性（Trustworthiness）を確立しようとしている。

IoTプラットフォーム分野では、接続時における「ゼロタッチ」コンフィギュレーションや、サービスを利用する際の自動的な信頼性（Trustworthiness）の検証など、膨大な数のIoTデバイスに対応するスケーラブルなデジタルトラスト構築のためのメカニズムをテーマとしたプロジェクトが推進されている。例えば、RAINBOW[14] では、ユースケースとして製造における人とロボットのコラボレーションや、都市モビリティのデジタル化、電力網の監視などが想定されており、IoTサービスをスケーラブルかつ安全に利用できるオープンで標準化されたリモートアテステステーション技術の研究開発が推進されている。また、ARCADIAN-IoT[15] では、ユースケースとして産業用制御システム、緊急警戒システム、医療IoTデバイスなどが想定されており、IoTにおけるセキュリティー、プライバシー管理の向上を目指し、IoTデバイスまたはゲートウェイ、スマートフォンなどのデバイスが機密性の高い情報やサービスにアクセスする際に、デバイスのセキュリティーやプライバシーなどの機能の信頼性（Trustworthiness）をリモートアテステーションにより検証する研究開発が推進されている。

ヘルスケア分野では、2022年5月にEU域内統一ルールとして公開された欧州ヘルスデータスペース規則案（EHDS：European Health Data Space）に関連する研究開発プロジェクトが推進されており、プライバシー保護が重要な要件となっている。例えば、ASCLEPIOS[16] では、コンフィデンシャルコンピューティングを用いて、ユーザーデータのプライバシーを保護するクラウドベースのデジタルヘルスフレームワークが開発されている。このフレームワークでは、クラウドサービスにおける暗号化などの信頼性（Trustworthiness）を検証するためや、利用者が医療デバイスを使用する前に医療デバイスの完全性を検証するために、リモートアテステーションが利用されている。

これら以外にも、プライバシーに配慮したリモートアテステーションメカニズムの研究や、AI分野でも学習データや学習済みモデルの保護、複数のAIエッジとクラウドとの間でフェデレーション学習を行う際のデータの保護のためにTEEやリモートアテステーションを用いる研究が推進されている。

❷ 欧州・Horizon Europeのプロジェクト

モビリティ分野で将来の自動運転車の安全性を高めるための研究（CCAM：Cooperative, Connected and Automated Mobility）が進められており、CONNECT（Continuous and Efficient Cooperative Trust Management for Resilient CCAM）（2022年9月～）[17] では、車両からMEC（Multi-access Edge Computing）、クラウド環境に至るシステム全体のトラストチェーンを確立して、転送中、保管中、使用中のデータを保護するとともに、データやリソースへアクセスする際には、都度、認証を行うゼロトラストアーキテクチャーの考え方を適用する研究開発が推進されている。

（5）科学技術的課題

ここでは「（3）研究開発領域の概要、（4）注目動向」に関する科学技術的課題を紹介する。

❶ リモートアテステーションの相互運用性の確立

リモートアテステーションは、システムのデジタルトラストを構築する上で重要な技術であるが、これまで、プロセッサーに実装されたHW RoTなどを元にボトムアップに発展してきた経緯がある。このためプロセッサーのアーキテクチャーへの依存性が強く、異なるプロセッサーとの間での相互運用性の確保が課題となっている。インターネット技術の規格化を推進しているIETFのRATS WG[1)]においてリモートアテステーションの相互運用性を確保すべくプロトコルなどの標準化が進められている。

❷ システムのデジタルトラストのフレームワーク構築

システムのデジタルトラストを構築するためには、対象とするビジネスモデルとそのビジネスモデルが要求するトラストモデルを理解した上で、そのフレームワークを構築する必要がある。例えば、5G分野で紹介したINSPIRE–5Gplusでは、「複数のドメインにまたがるネットワークスライス（クロスドメインスライス）の利用を前提に5G ネットワーク管理のためのフレームワーク」の構築を目指している。また、ヘルスケア分野で紹介したASCLEPIOSでは、TEEなどを利用したコンフィデンシャルコンピューティングにより、ユーザーのプライバシーを保護した上で攻撃を防ぐクラウドベースのデジタルヘルスフレームワークが開発されている。この様に、さまざまなビジネスモデルに対応するためには、そのフレームワークの構築が求められている。

（6）その他の課題

❶ ハードウェアセキュリティーとソフトウェアセキュリティーの研究開発の融合

システムのデジタルトラストの構築のためには、HW RoTやTEEなどに関するハードウェアセキュリティーの研究とそれらを利用するソフトウェアセキュリティーの研究を合わせたプラットフォームとしてのセキュリティーの研究が重要となる。プラットフォームとしてのセキュリティーの研究を進めるためには、ハードウェアやソフトウェアを含めシステム全体を見渡せる幅広い知識を持ったセキュリティー人材が必要となる。文部科学省において実施された補助事業「成長分野を支える情報技術人材の育成拠点の形成（enPiT）」（第2期）で取り組まれていたように、今後、さらなる人材育成が求められている。（「2.4.1 IoTシステムのセキュリティー（6）その他の課題 ❷人材育成」にも記載）

❷ 技術と制度

デジタルトラストは、技術だけでなく、法制度によりその法的有効性が担保される必要がある。欧州FP7のプロジェクトであるOPTET（2012年11月～2015年10月）[18)]では、デジタルトラストの定義や、関連する技術、法制度が社会経済に及ぼす影響について幅広く検討されている。例えば、OPTET–法的統合モデルやソフトローのあり方、欧州連合における一般データ保護規則（GDPR：General Data Protection Regulation）やeIDAS（electronic Identification and Authentication Service）規則[3]などのハードローがシステムのデジタルトラストに果たす役割などが考察されている。わが国においても、OPTETのようにデジタル社会におけるトラストに関する基礎研究がなされ、その上で取り組むべき制度、技術を検討していく必要がある。

3 eIDAS規則については「2.4.6 データ・コンテンツのデジタルトラスト（3）研究開発領域の概要［研究開発の動向］」を参照いただきたい。

（7）国際比較

国・地域	フェーズ	現状	トレンド	各国の状況、評価の際に参考にした根拠など
日本	基礎研究	○	→	・HW Root Of Trust の基礎となるハードウェアセキュリティーの研究は盛んに行われている一方、トラストの重要性が認識されてきているが、コア技術の研究開発までに至っていない。
	応用研究・開発	△	→	・現状、関連する活動は少ない。
米国	基礎研究	○	↗	・各半導体ベンダーIntel、AMD、NVIDIA、Qualcomm、プラットフォーマー（Apple、Google、Amazon、Microsoft）がHW Root Of Trust を組み込んだセキュリティチップの研究開発を盛んに行っている[19), 20), 21)]。
	応用研究・開発	◎	↗	・プラットフォーマーがリモートアテステーションサービスを自社のプラットフォームに組み込みつつある。半導体ベンダーもIntel のProject Amberなど、リモートアテステーションの組み込みを推進している[22)]。
欧州	基礎研究	◎	↗	・過去からFP6、FP7、HORIZON 2020などのR&Dプログラムにおいて、多くのプロジェクトがトラストをテーマに取り上げており、その中で「システムのデジタルトラスト」の概念が構築されている[23)]。
	応用研究・開発	○	↗	・5G分野などを中心に、マルチステークホルダーで構成されるシステムにおいて、デジタルトラストの研究開発が盛んに行われている[11), 12), 13)]。
中国	基礎研究	○	↗	・米国と同様、中国のプラットフォーマーであるAlibabaなどが、コンフィデンシャルコンピューティングなどの分野で多くの論文を発表している[24)]。
	応用研究・開発	◎	↗	・米国と同様、中国のプラットフォーマーが、自社のサービスにアテステーションサービスを組み込みコンフィデンシャルコンピューティングなどのサービスを展開している[25)]。
韓国	基礎研究	△	→	・目立った動きは少ない
	応用研究・開発	○	→	・サムソンが、HW RoT, TEE, リモートアテステーションなどをベースにして、クラウド、スマートデバイスの垂直統合的なサービスを提供している[26)]。

（註1）フェーズ

基礎研究：大学・国研などでの基礎研究の範囲

応用研究・開発：技術開発（プロトタイプの開発含む）の範囲

（註2）現状　※日本の現状を基準にした評価ではなく、CRDS の調査・見解による評価

◎：特に顕著な活動・成果が見えている　　○：顕著な活動・成果が見えている

△：顕著な活動・成果が見えていない　　×：特筆すべき活動・成果が見えていない

（註3）トレンド　※ここ1～2年の研究開発水準の変化

↗：上昇傾向、→：現状維持、↘：下降傾向

参考文献

1) Internet Engineering Task Force（IETF）, “Remote ATtestation ProcedureS（rats）,” https://datatracker.ietf.org/group/rats/about/,（2023年2月25日アクセス）.

2) Henk Birkholz, et al., “Remote ATtestation procedureS（RATS）Architecture, 2. Reference Use Cases,” Internet Engineering Task Force（IETF）, https://datatracker.ietf.org/doc/draft-ietf-rats-architecture/,（2023年2月25日アクセス）.

3) Michael Bartock, et al., “NISTIR8320 Hardware-Enabled Security : Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases,” National Institute of Standards and Technology（NIST）, https://csrc.nist.gov/publications/detail/nistir/8320/final,（2023年2月25日アクセス）.

4）European Telecommunications Standards Institute（ETSI）, “ETSI GR SAI 006 V1.1.1（2022-03）: Securing Artificial Intelligence（SAI）; The role of hardware in security of AI,” https://www.etsi.org/deliver/etsi_gr/SAI/001_099/006/01.01.01_60/gr_SAI006v010101p.pdf,（2023年2月25日アクセス）.
5) Scott Rose, et al., “NIST Special Publication 800-207: Zero Trust Architecture,” National Institute of Standards and Technology（NIST）, https://csrc.nist.gov/publications/detail/sp/800-207/final,（2023年2月25日アクセス）.
6) Joseph R. Biden Jr., “Executive Order on Improving the Nation’s Cybersecurity,” The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/,（2023年2月25日アクセス）.
7) ASSURED Project, https://www.project-assured.eu,（2023年2月25日アクセス）.
8) Confidential Computing Consortium, https://confidentialcomputing.io,（2023年2月25日アクセス）.
9) 5G Infrastructure Public Private Partnership（5G-PPP）, https://5g-ppp.eu,（2023年2月25日アクセス）.
10) Mike Surridge, et al., “3 State of the Art in Trust Modelling,” in 5G Enablers for Network and System Security and Resilience（5G-ENSURE）, D2.5 Trust model（final）v2.2, 5G ENSURE, 15-29., http://5gensure.eu/sites/default/files/5G-ENSURE_D2.5 Trust model（final）v2.2 inc history.pdf,（2023年2月25日アクセス）.
11) Gregorio Martínez Pérez, et al., “2.1.1 Design Updates,” in 5GZORRO Grant Agreement No. 871533, D4.4: Final Design of Zero Touch Service Management with Security and Trust Solutions, 5GZORRO, 14-21., https://www.5gzorro.eu/wp-content/uploads/2022/06/5GZORRO_D4.4_v1.1_Final-withWM.pdf,（2023年2月25日アクセス）.
12) Milon Gupta, “Trust mechanisms for 5G environments - INSPIRE-5Gplus deliverable D4.1,”INtelligent Security and PervasIve tRust for 5G and Beyond（INSPIRE-5Gplus）, https://www.inspire-5gplus.eu/trust-mechanisms-for-5g-environments-inspire-5gplus-deliverable-d4-1/,（2023年2月25日アクセス）.
13) MonB5G, https://www.monb5g.eu,（2023年2月25日アクセス）.
14) European Commission, “HORIZON 2020: AN OPEN, TRUSTED FOG COMPUTING PLATFORM FACILITATING THE DEPLOYMENT, ORCHESTRATION AND MANAGEMENT OF SCALABLE, HETEROGENEOUS AND SECURE IOT SERVICES AND CROSS-CLOUD APPS, https://cordis.europa.eu/project/id/871403,（2023年2月25日アクセス）.
15) Autonomous Trust, Security and Privacy Management Framework for IoT（ARCADIAN-IoT）, https://www.arcadian-iot.eu,（2023年2月25日アクセス）.
16) Advanced Secure Cloud Encrypted Platform for Internationally Orchestrated Solutions in Healthcare（ASCLEPIOS）, https://www.asclepios-project.eu,（2023年2月25日アクセス）.
17) European Commission, “Continuous and Efficient Cooperative Trust Management for Resilient CCAM,” https://cordis.europa.eu/project/id/101069688,（2023年2月25日アクセス）.
18) Laura German, et al., “2. OPTET Trust and Trustworthiness Model,” in D2.5 Consolidated report on the socio-economic basis for trust and trustworthiness, University of Southampton Institutional Research Repository, 9-15., https://eprints.soton.ac.uk/410774/1/OPTET_WP2_D2_5_v1_0.pdf,（2023年2月25日アクセス）.
19) Alon Jackson, “Trust is in the Keys of the Beholder: Extending SGX Autonomy and Anonymity,”

Reichman University, https://www.runi.ac.il/media/151p1eou/jackson-msc-thesis.pdf,（2023年2月25日アクセス）.
20) Advanced Micro Devices, Inc., “AMD Secure Encrypted Virtualization（SEV）,” https://developer.amd.com/sev/,（2023年2月25日アクセス）.
21) Andrés Lagar-Cavilla, Prabhu Jayanna and Bryan Kelly, “Caliptra: An open source, reusable silicon IP block for a Root of Trust for Measurement（RTM）,” Open Compute Project, https://146a55aca6f00848c565-a7635525d40ac1c70300198708936b4e.ssl.cf1.rackcdn.com/images/6dadf83e9f93ca89efaf3b93ab076cea8f9ac747.pdf?utm_source=thenewstack&utm_medium=website&utm_content=inline-mention&utm_campaign=platform,（2023年2月25日アクセス）.
22) Intel Corporation「インテル コーポレーション、クラウドからエッジ、オンプレミス環境での信頼性を保証するProject Amberを発表」https://www.intel.co.jp/content/www/jp/ja/newsroom/news/vision-2022-project-amber-security.html,（2023年2月25日アクセス）.
23) European Commission, “HORIZON 2020: Enablers for Network and System Security and Resilience（5G-ENSURE5G）,” https://cordis.europa.eu/project/id/671562,（2023年2月25日アクセス）.
24) Alibaba Cloud, “TEE-based confidential computing,” https://www.alibabacloud.com/help/en/container-service-for-kubernetes/latest/tee-based-confidential-computing-tee-based-confidential-computing,（2023年2月25日アクセス）.
25) Alibaba Cloud, “Use confidential containers to implement remote attestation in TEE-based ACK clusters,” https://www.alibabacloud.com/help/en/container-service-for-kubernetes/latest/use-confidential-containers-to-implement-remote-attestation-in-tee-based-ack-clusters,（2023年2月25日アクセス）.
26) SAMSUNG Knox, “The Big Picture,” https://docs.samsungknox.com/dev/common/knox-ecosystem.htm,（2023年2月25日アクセス）.