

Society 5.0を支える トラスト&セキュアなサービス・システム

COVID-19や異常気象、デジタル化などによって世界の変化が加速する中、大量に発生するデータの活用、5GやAIなどのデジタル技術の活用が進展している。一方で、このような変化のスピードに対応した新たなガバナンスのあり方についても議論が始まっており、その中ではトラスト(信頼)構築の重要性が強調されている。変化が常態化するSociety 5.0ではさまざまな不測の事態が発生し得ると考えられる。

日立は、その影響を最小化する機能をサービスや社会に組み込むことで、それらのトラストの構築をめざした研究開発を進めている。本稿では、Society 5.0を支えるサービスや社会システムのトラストを系統的に構築するためのコア技術やアーキテクチャの研究開発について紹介する。

鍛 忠司 | Kaji Tadashi

高橋 由泰 | Takahashi Yoshiyasu

志村 明俊 | Shimura Akitoshi

吉野 雅之 | Yoshino Masayuki

1. はじめに

COVID-19や異常気象など、世界はここ数年過去に例を見ない急激な変化に直面している。技術に目を向けても、COVID-19を契機としてデジタル化が加速しており、大量に発生するデータの活用、5G (Fifth Generation)やAI (Artificial Intelligence)などの革新技術の活用が進展している。一方で、このような変化のスピードに従来型のガバナンスが追いつかず社会秩序を保てなくなる事例も増えつつあり、新たなガバナンスのあり方についても議論が始まっている^{1), 2)}。こうした議論の中では、トラスト(信頼)構築の重要性が強調されており、透明性・検証可能性を伴う信頼性(Trustworthiness)ベースでトラストを構築するメカニズムの必要性が議論されている。

日立はこうした動向を踏まえ、Society 5.0³⁾を支えるサービスや社会システムのトラスト(信頼)をシステム

的に構築するための研究開発に取り組んでいる。変化が常態化するSociety 5.0ではさまざまな不測の事態が発生し得るが、この影響を最小化する機能をサービスや社会そのものに組み込むことで、信頼できるサービスや社会の実現をめざしたものである。

以下、2章では信頼できるサービスの実現に向けた技術開発について、3章ではS3アーキテクチャと呼ぶ、社会全体をSociety, Service, Systemの三つの視点で捉え、データを介して同時並行的に動作する新しいアーキテクチャについて紹介する。

2. Society 5.0のサービスにおける トラスト&セキュリティ技術

2.1

二つのトラスト

Trust by Data, Trust of Data

Society 5.0のサービスは、単に安全・セキュアである

だけではトラストを勝ち取ることはできない。トラストはあるエンティティ(実体、存在などの意)が他者やサービスに対して抱く「期待」であり、主観であるからである。トラストを醸成するには、そのサービスが「信頼に足る」ことに加え、「信頼に足る」という証拠(Trustworthiness)を蓄積・周知する手段が必要である。

日立は、サービスの監視ログなどのデータからそのサービスが「信頼に足る」証拠を蓄積・開示する技術(Trust by Data) および前述のデータそのものが「信頼に足る」ことを担保する技術(Trust of Data)の研究開発を進めている(図1参照)。

以下にTrust by DataとTrust of Dataを実現するコア技術と位置付けている三つの研究を紹介する。

2.2
ビジネスのトラスト

事業を進めるうえでは、納期遅延や製品不良、コンプライアンスなど、さまざまなリスクに対処することが求められる。日立はTrust by Data技術として、IoT(Internet of Things) 機器などから収集したデータを分析することでこれらのリスクを可視化したり、制御したりする技術を開発している。本技術により、例えばサプライチェーンの品質向上のため、センサー情報や映像情報などを用いて生産工程が手順どおり行われているか確認できるようにするなど、ビジネスのトラスト向上をめざしている。

2.3
個人データのトラスト

今日、金融、医療、旅行などのさまざまな領域でユーザーの個人データの提示が求められる。プライバシー保

護を求める世論の高まりに応じて、欧州のGDPR(General Data Protection Regulation) や米国のCCPA (California Consumer Privacy Act) など、個人情報を含む個人データ管理に関する規制強化の動きが顕著である。これらの動向を受け、特定の管理主体に依存せず、ユーザー自らが個人データを管理可能な自己主権型管理形態であるSSI (Self-sovereign Identity) が議論されている。SSIの実現手段としては、ブロックチェーン上に記載された個人データの開示をユーザーが制御する分散型ID (Identification) が議論されている。

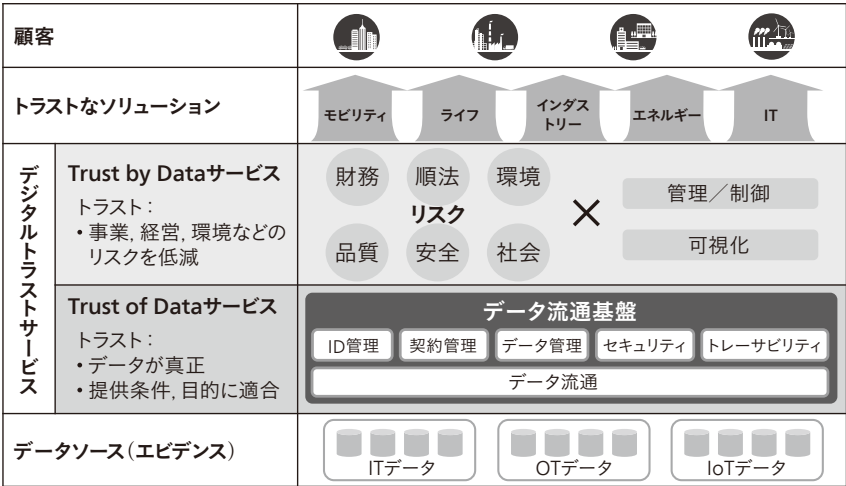
ブロックチェーンでは、記述された個人データとユーザーの関係の確認に電子署名を用いるため、秘密鍵を管理する必要がある。一方、この鍵管理の煩雑さが運用上の課題となっている。日立は、この鍵管理という課題自体を排除することに成功した。すなわち、生体情報から電子署名を生成するPBI (Public Biometrics Infrastructure) 技術である。PBIを利用することで、生体情報を秘密鍵として利用できるため、ユーザーは秘密鍵を管理の手間を省けるだけでなく、秘密鍵の紛失や漏洩リスクも同時に解消できる⁴⁾ (図2参照)。本技術は、個人データを対象としたTrust of Data技術と位置づけられるものである。

2.4
データ利用のトラスト

価値の源泉がデータの利活用に移行し、フィールドのIoT機器が生み出す多様なデータを流通させ、利用することが期待されている。一方で、データが機密性を含む可能性がある場合、データ流通や利用の履歴管理が必要になるなど、データ利活用のハードルが高い。

図1| Trust by DataとTrust of Data

データにより信頼に足ることを示すTrust by Dataとデータそのものが信頼に足ることを保証するTrust of Dataがある。



注：略語説明
ID (Identification), OT (Operational Technology), IoT (Internet of Things)

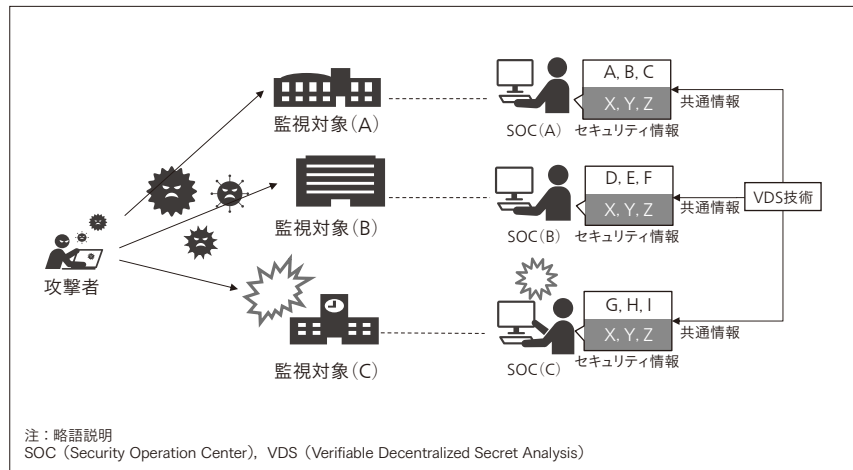
図2| 公開型生体署名PBI

PBIは、生体情報を秘密鍵として利用する電子署名技術（公開鍵認証）である。秘密鍵をどこにも保存せず、秘密鍵管理を必要としない。



図3| VDS技術のSOCへの適用例

それぞれのSOCが保有しているセキュリティログから共通情報だけを抽出し、サイバー攻撃を検知する。



日立は、データを流通させて利用するのではなく、処理をデータのある場所で行うことにより、データ利活用のハードルを下げることに成功した。すなわち、高機能暗号と分散処理を組み合わせたVDS (Verifiable Decentralized Secret Analysis) と呼ばれる技術である。VDSでは、例えば、複数のSOC (Security Operation Center) が保有する機微なセキュリティ情報から暗号化したままで共通する情報のみを抽出し、サイバー攻撃を早期検知することができる^{5), 6)} (図3参照)。これにより、共有するセキュリティ情報を必要最小限に抑制し、安全性を向上する。本技術は、機密データ利用におけるTrust of Data技術と位置づけられるものである。

3. Trusted Serviceから Trusted Digital Societyへ

Society 5.0が安全・安心でより豊かな暮らしを実現する社会であるためには、2章で述べた技術を組み込んだトラストなデータ流通基盤上で、革新技術の開発と社会実装ならびにガバナンスが有機的につながり、社会に対して有効に機能しなければならない。日立は、その規範となるアーキテクチャの研究開発に取り組んでいる。図4はこれからのシステム構築の考え方を示したもので

ある。法によって定められたルールに基づいてオペレーションを実行する従来型のシステム構築では、変化が常態化する社会において多様なニーズに応え続けることは困難である。サービスに関わるステークホルダーどうしで合意形成しながらゴールを柔軟に設定しつつ (Society), 新たなサービスのTrustworthinessを迅速に確保し (Service), レジリエントにオペレーションを変更可能な (System), Society, Service, Systemの三つのビュー (視点) から社会を捉えたアーキテクチャが必要である。これをS3アーキテクチャと呼ぶ (図5参照)。データ流通基盤を介した信頼できるデータに基づいて社会のゴールやデータを共有し, Society, Service, Systemで試行と評価を繰り返すことでFuture Proofな社会を実現していく。そのためには以下に示す機能を各ビューが備えておくことが必要であり、現在開発を推進中である。

3.1

Societyビュー

Society 5.0では人間中心の社会をめざすことが求められており、例えば経済的成長と、人々の暮らしにおける質的側面の向上の両立が重要である。国や自治体といったガバナーは、マクロな指標で目標を定めるだけでなく、デジタル技術によってそれらを実現する主体であること

図4|システム構築の考え方

法によって定められたルールに基づいてオペレーションを実行する従来型のシステム構築では、変化が常態化する社会において多様なニーズに応え続けることは困難であり、システムからゴールやサービスを分離することが必要である。

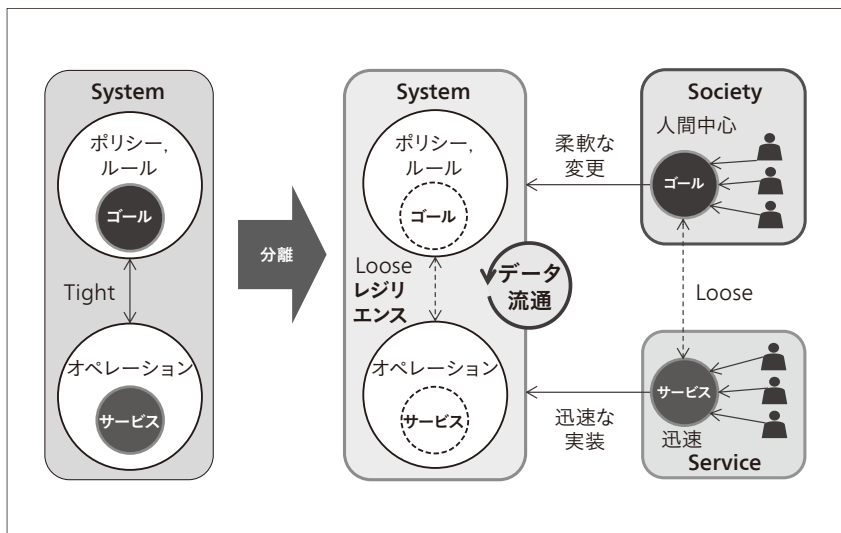
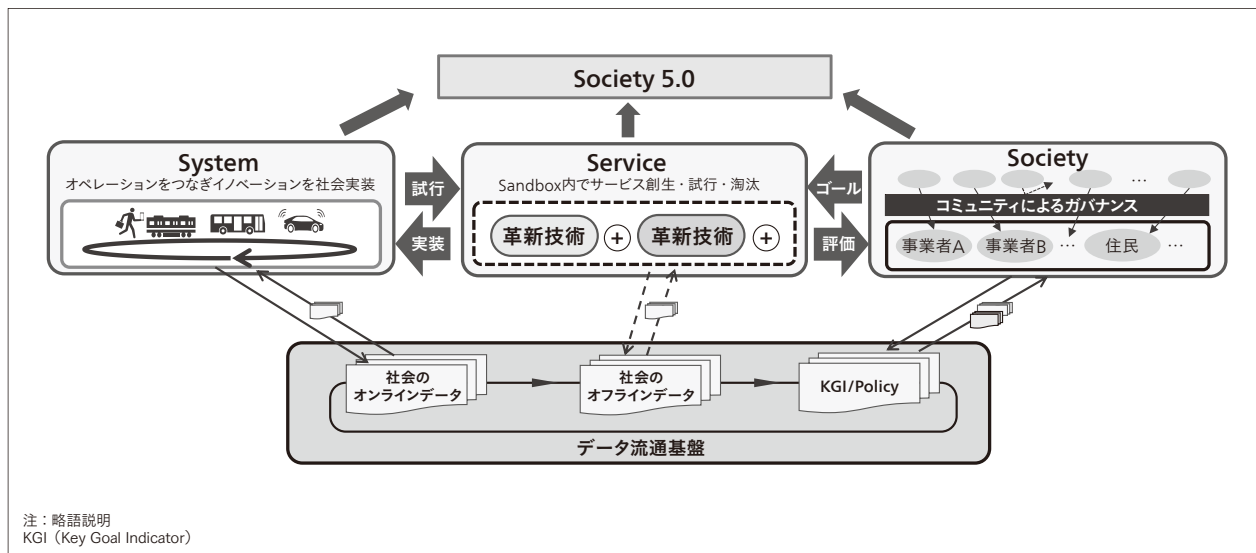


図5|S3アーキテクチャ

トラストなデータ流通を介して社会のゴールやデータを共有し、Society、Service、Systemで試行と評価を繰り返すことでFuture Proofな社会を実現していくアーキテクチャを示す。



が求められる。

日立は、ガバナーが交通や輸送の状況、人々の健康状態、設備の状態などさまざまな側面で社会を評価する際に、QoL (Quality of Life) の考え方をうい、その評価に人間中心という理念を埋め込むことを検討している。これにより、人間中心をめざすガバナーの意思決定を、サービスの設計や運用に反映しやすくなる。社会の多様性に着目し、多主体を捉えたKPI (Key Performance Indicator) モデルの評価方法を用いて、ガバナーの意思決定、すなわち政策と社会サービス開発を連動させることができる。

3.2

Serviceビュー

デジタル技術の進化は、企業や自治体が所有する各種

システムの連携を促し、人や社会に役立つ多様なイノベーションの迅速な創生を可能にする。同時に、異種・異業種間システム連携時の安全性検証や可用性確保がネックとなり、その社会実装の妨げとなるという課題が生じる。

S3アーキテクチャでは、実社会のシステム状態、オペレーション(制御)状態、生活者状況などの多層的なデータをリアルタイムに収集・分析し、CPS (Cyber Physical System) や実フィールド上において、サービスやオペレーション機能の安全性や可用性を検証する動的サービス検証基盤 (Sandbox) を備えている。イノベーションを動的に試作・検証し、SocietyビューやSystemビューと連携して、検証完了した機能から順次段階的な社会実装を可能とすることにより、QoL向上をもたらすアジャイルなサービスインを実現する。

3.3

Systemビュー

変化が常態化すると予測されるSociety 5.0の社会においては、社会実装・提供を迅速に行う必要がある。よって時間のかかる社会インフラ整備を待たず、既存の社会インフラが持つ機能を活用し、新たなサービスに転用していくことがより重要になる。そのためには機能のアンバンドル、リバンドルを容易にし、変化に対してレジリエントに社会インフラとしてのオペレーションを継続し続けられることが必要である。それには既存の社会インフラが提供している機能をサイバー空間上にソフトウェアモデルとして実装し、実装した複数のソフトウェアモデルをつなぐ仕掛けが求められる。日立はこれをオペレーション仮想化技術と呼び、現在、開発に取り組んでいる。本技術により、例えば社会インフラがトラブルなどで停止した際も、ソフトウェアモデルとして実装されている代替社会インフラを活用することでサービスを継続させることができ、サービス全体のレジリエンスを向上させることができる。具体的には、生産・流通の分野において、天災などの理由により一部工場の生産量が下がった場合、複数の別工場を連携させた新たな代替バリューチェーンを迅速に実現させるなど、トラブルに強いレジリエントなサービス提供が可能になると考えている。

4. おわりに

本稿では、Society 5.0を支えるサービスや社会システムのトラストをシステム的に構築するための研究開発について紹介した。

今後、本稿で紹介した技術も含め、実際のサービスや社会システムへトラスト構築の機能の実装を進めていく。同時に、本研究開発や社会実装で得た知見を踏まえ、そもそもSociety 5.0におけるトラストはいかにして構築すべきなのか、といったコンセンサスの形成についても貢献していきたい。

参考文献など

- 1) 経済産業省：GOVERNANCE INNOVATION Society5.0の実現に向けた法とアーキテクチャのリ・デザイン、<https://www.meti.go.jp/press/2020/07/20200713001/20200713001-1.pdf>
- 2) 世界経済フォーラム 第四次産業革命日本センター、アジャイルガバナンス、<https://jp.weforum.org/centre-for-the-fourth-industrial-revolution-japan/agile-governance>
- 3) 内閣府：Society5.0、https://www8.cao.go.jp/cstp/society5_0/index.html
- 4) 長沼健，外：PBIを用いたブロックチェーン向け鍵管理技術，SCIS2019，2G4-5（2019.1）
- 5) 西嶋克哉，外：セキュリティ・オペレーションにおける秘匿データ分析システムの提案，DICOMO2020，2G-1（2020.6）
- 6) 日立ニュースリリース：複数組織で観測したダークネット通信を分析することでサイバー攻撃の予兆を検知，被害の未然防止に貢献（2019.6），<https://www.hitachi.co.jp/New/cnews/month/2019/06/0618.html>

執筆者紹介



鍛 忠司

日立製作所 研究開発グループ
システムイノベーションセンタ 所属
現在、サイバーセキュリティやトラストに関する研究開発に従事
博士（情報科学）
IEEE CS会員



高橋 由泰

日立製作所 研究開発グループ システムイノベーションセンタ
システムアーキテクチャ研究部 所属
現在、OR・数理技術の研究開発に従事
博士（工学）
情報処理学会会員，日本オペレーションズ・リサーチ学会会員



志村 明俊

日立製作所 研究開発グループ システムイノベーションセンタ
システムアーキテクチャ研究部 所属
現在、社会インフラを対象としたシステムアーキテクチャの研究開発に従事
博士（工学）
計測自動制御学会会員



吉野 雅之

日立製作所 研究開発グループ システムイノベーションセンタ
セキュリティ研究部 所属
現在、暗号と情報セキュリティに関する研究開発に従事
博士（科学）
情報処理学会会員，電子情報通信学会会員，
日本医療情報学会会員