セキュリティ技術の最新研究動向

Latest Trends in Research on Security Technologies

津田　宏　　鎌倉　健

あらまし

「21世紀の新たなオイル」と言われるデータを中心に，デジタル共創が進んでいる。一方，IoTの活用で激化が予想されるサイバー攻撃，パーソナルデータに関する規制への対応，AI（人工知能）に与えるデータの信頼性の確保など，新たなリスクも生まれている。セキュリティ技術は，人，データ，システムの信頼性（トラスト）を支える技術として期待が大きい。富士通研究所は，お客様のあらゆるビジネスの安心・安全を支えるために，認証・認可，データセキュリティ，サイバーセキュリティを三本柱に研究開発を進めている。

本稿では，まず富士通研究所で取り組んでいるセキュリティ技術を概説する。次に最新研究トピックスとして，ブロックチェーンを用いたデータの信頼性を担保する技術について述べる。

Abstract

Digital co-creation is underway mainly in relation to data, which is being referred to as the “new oil of the 21st century.” Meanwhile, new risks are also emerging, such as cyberattacks, which are expected to intensify due to the utilization of the IoT, compliance with regulations relating to personal data, and ensuring the reliability of data to be fed to AI. Security technologies are raising expectations as technologies that support the trust of humans, data, and systems. Fujitsu Laboratories is conducting research and development in the three core areas of authentication/authorization, data security, and cyber security for the purpose of supporting safety and security of all customer businesses. This paper first outlines the security technologies that Fujitsu Laboratories is working on. Next, as a topic of the latest research, it describes a technology to ensure the trust of data by making use of blockchain technology.

1. まえがき

2011年の世界経済フォーラムのレポートでは，「パーソナルデータは21世紀の新しいオイル」と示されている。これからのデジタルビジネスでは，産業データやパーソナルデータがオイルのように国・業界・企業をまたがり取引されていく。それらのデータが，データ解析やAI（人工知能）技術によって加工されて，新たなデジタル共創を生み出すと考えられる。こうしたデータ利活用の変化に伴って，新たな脅威・リスクに対する考慮が必要であり，以下のようなセキュリティ技術が解決すべき課題も広がっている。

(1) ボーダーレスなセキュリティ対策

データは1社で抱えるだけでなく，複数組織でデジタル共創のために用いられるようになり，サイバー攻撃対策の考え方も変わってきている。IoTの活用を含めて増加する攻撃に対して，ファイアーウォールや侵入検知および侵入防止システム（IDPS）のように，組織の境界で守る考え方には限界がある。そのため，攻撃・侵入されることを前提に，ボーダーレスで検知・対処を速やかに実行できる対策が基本となる。更に匿名化やデータ保護技術により，データが漏えいしてもリスクは最小限にする考え方が必要となる。

(2) 新たな法規制・ガイドラインへの対応

法規制やガイドラインの強化により，データの種類に応じて，組織や国をまたがり慎重に扱う必要があることは注意すべきである。米国国立標準技術研究所（NIST）では，機密レベルに応じてCI（Classified Information：国家機密レベル）やCUI（Controlled Unclassified Information：重要情報）のガイドラインが規定され（SP800-53，171），政府調達の条件にもなっている。

パーソナルデータについては，日本の改正個人情報保護法（2017年），中国のサイバーセキュリティ法（2017年），EUの一般データ保護規則GDPR（2018年）などが相次いで施行された。

(3) AIのもたらす新たなリスク

大量の学習データを利用するディープラーニングなどAI特有の課題として，学習データの信頼性が考えられる。2016年にはMicrosoftが開発したチャットボットTayが，入力データの不備により，不適切な結果を出力する事例が起きた。また，データにノイズを入れることで画像認識結果を誤判定させる技術（敵対的サンプル）も現れている。

今後，AIが組み込まれたシステムに対するデータテロのような攻撃も，リスクとして捉えておかなければならない。また，AI自体にもどのように結果が得られたかを可視化する説明可能性や，倫理的な対策が必要となってくる。更に，AIに与えるデータの信頼性や透明性の確保をセキュリティ観点で考える必要がある。

(4) 新たなトラストモデルの必要性

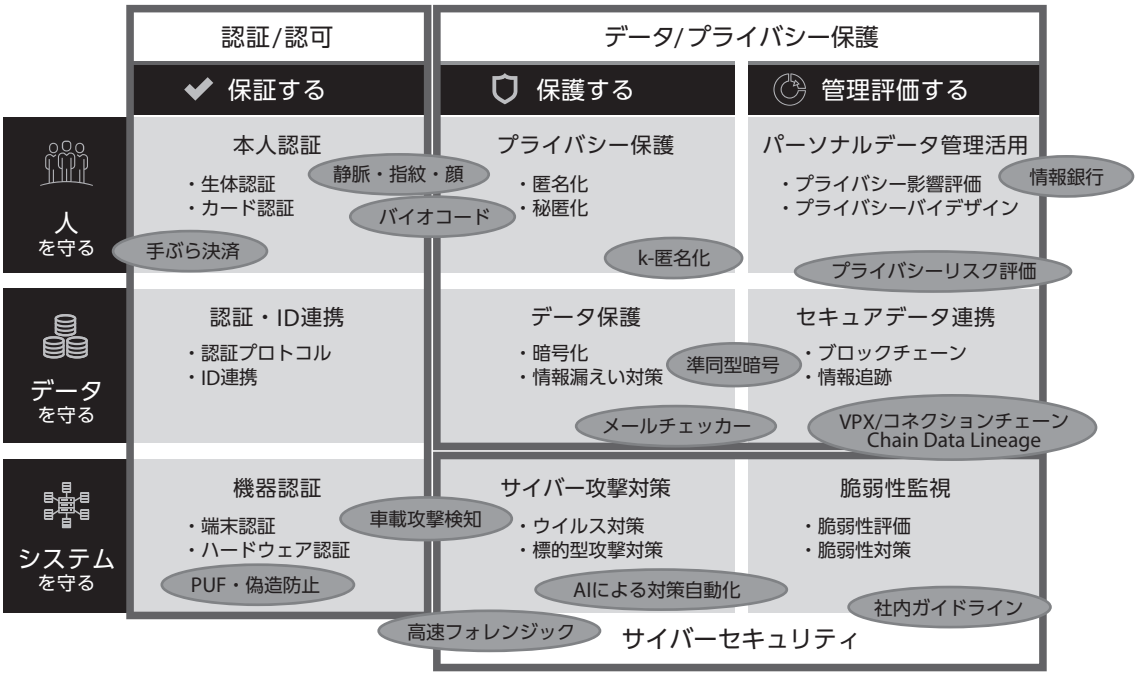
国を越えて複数の組織がデジタル共創活動するために，人や組織における信頼（トラスト）の考え方も変わり始めている。従来は，PKI（Public Key Infrastructure）などの技術で信頼できる第三者を仮定して信頼を担保していたのに対して，ブロックチェーンのように参加者が相互に信頼を支援するような仕組みも国や業界をまたがるサプライチェーンでは有効になっている。

こうした脅威やリスクの多様化に対して，セキュリティ技術は大きく二つの方向による対策が期待されている。一つは，サイバー攻撃対策を支えるセキュリティ人手不足も叫ばれている中で，それらの対応を含めたAIや自動化技術を活用して，効率良く守るための技術である。もう一つは，AIや法規制など新たなリスクを低減し，デジタル共創を可能にする攻めの技術である。

本稿では，富士通研究所のセキュリティの守りと攻めの技術を概説し，AI技術を活用したサイバーセキュリティ，およびデジタル共創を支えるデータセキュリティの二つの観点から先端技術を紹介する。

2. デジタルビジネスを支えるセキュリティ

富士通研究所では，セキュリティ技術を，人やモノの保証を行う「認証・認可技術」，人やデータの保護や管理を行う「データ保護技術」，システムの保護や管理を行う「サイバーセキュリティ技術」の三つに大別している。富士通研究所が取り組んでいるセキュリティ技術の全体像を図-1に示す。縦方向



PUF：Physically Unclonable Function
VPX：Virtual Private digital eXchange

図-1　セキュリティ技術マトリクス

に守る対象として，人，データ，システムを置き，横方向に3種類の守り方を置いている。例えば，本人認証する技術として手のひら静脈認証のような生体認証技術，データを保護する技術として暗号化や匿名化，データを管理する技術としてブロックチェーンなどがある。

2.1 多様化する守りのセキュリティ

初期のサイバー攻撃対策では，ファイアーウォールなどを用いて組織内を攻撃させないようにする入口対策が中心であった。しかし，標的メール攻撃を始めとしサイバー攻撃が高度化する中で，全てのサイバー攻撃を入口でブロックすることは不可能であり，マルウェアに感染した場合を想定した事後対策の重要性が増している。

経済産業省のサイバーセキュリティ経営ガイドライン[(1)]においても，サイバー攻撃を受けた場合に備えた体制構築の必要性が指摘され，対応体制・復旧体制の整備が推奨されている。

お客様の業務継続を支える守りのセキュリティでは，今後IoTへの対応は必須である。あらゆるモノがインターネットにつながるIoTでは，適用場面に合わせて，従来のサイバー攻撃とは異なる考え方が必要となる。

IoTを活用したシステムの構築においては，様々なベンダーのセンサーを組み合わせるとともに，全体としてセキュリティを担保することが求められる。IoT機器の脆弱性を検出するために，富士通研究所はIoT機器を対象としたファジング技術を開発した。詳細は，本誌掲載の「システムに潜む未知の脆弱性を検出するセキュリティテスト技術」を参照されたい。

モビリティ（コネクテッドカー）においては，第一に走行中の車に対してリアルタイムな攻撃への対処が求められる。富士通研究所は，車載ECU（Electronic Control Unit）において，車載ネットワークであるCAN（Controller Area Network）に挿入される攻撃メッセージをリアルタイムに検知する技術を開発した。[(2)] モビリティにおいては，こうした車載機器における応急処置的な対策と，各車両の情報を集約して車種ごとのオンラインアップデートなどにつなげるセンター側における長期的な対策

の両立が必要となる。

また，工場や産業制御システムにおいても，OT（Operational Technology）による自動制御が進む一方で，OT部門へのサイバー攻撃も健在化している。工場では，生産ラインを止めるとビジネス損失に直結する。このため，必ずしもマルウェアに感染した機器をすぐに停止するということはできず，慎重な対応が必要となる。こうした，攻撃対処も専門家の作業を助けるAI技術の期待は高い。

2.2 デジタル共創に向けた攻めのセキュリティ

異なる組織間におけるデジタル共創活動では，相手が本人であるかどうか，認証の信頼性をどう保証するかが求められる。セキュリティ技術はこうした課題を解決し，新たなビジネスを創造する「攻め」にも使うことができる。

本人認証の信頼性については，富士通の独自技術である手のひら静脈認証をはじめとする，生体認証技術を開発している。従来の手のひら静脈認証では，1万人規模から一人を認証することが可能であったのに対して，顔認証も組み合わせることで，100万人規模から本人を認証することができるようになった。これにより，大規模イベントなどにおいても，スマートフォンやカードなどの機器が不要な手ぶら認証や決済が可能となった。詳細は，本誌掲載の「生体データの保護や管理を容易にできる生体認証技術」を参照されたい。

データのセキュリティは，C（Confidentiality：秘匿性），I（Integrity：完全性），A（Availability：可用性）の三つの観点から考える必要がある。中でも，ブロックチェーンは特にIとAを実現する技術として期待が高い。ブロックチェーン技術を活用した，企業にまたがるデータの来歴を管理する技術については3章で述べる。また，ブロックチェーン間を連携するコネクションチェーン技術については，本誌掲載の『ブロックチェーンを安全につなげるセキュリティ技術「コネクションチェーン」』を参照されたい。

3. デジタル共創を支えるデータセキュリティ

本章では，デジタルデータの信頼性を支えるデータのプライバシー保護を中心としたセキュリティ技術について述べる。

3.1 デジタル共創に向けたデータ流通技術

産学官などの異なる組織が相互につながり，新たな価値やサービスを作り出すデジタル共創では，デジタルデータがサイバー空間内を流通し，データのサプライチェーンが形成される。更にAI技術の活用においては，AIに与えるデータの信頼性が重要である。加工食品の信頼性を担保するため原材料表記が必須なように，これからはデータにも来歴が必要になると考えられる。そのためには，データが誰によってどのようなデータからどのような処理によって作られたかを確認できる必要がある。また，活用するデータがパーソナルデータを含む場合には，きちんと本人同意を取って収集されたものかを確認できることも重要な要件となる。

このような背景をもとに，富士通研究所ではデータの出所や経路などの来歴を一元的に把握可能なデータの来歴管理技術を開発した。[3] 以下，分散する個人データの同意管理を一元化し，本人同意に基づいた個人データの簡単かつ安全な流通を可能にする技術について説明する。

(1) 課題

企業間で個人データを流通する際の関連標準には，権限認可を行う「OAuth」やOAuthに基づいたアクセス管理プロトコル「UMA（User-Managed Access）」がある。これらはいずれも，個人を対象として設計されている。例えば，患者本人の同意を得ることによって診療情報を別の医療機関に提供することはできる。しかし，企業が既に所有している個人データを一括して他組織に移転する用途には，新たな設計が必要である。

OAuth，UMAの典型的な構成を図-2に示す。UMAは，利用者単位でデータを認可して第3者に提供するモデルである。各サーバやクライアント間で発生する複数の通信を，そのまま人数分繰り返す

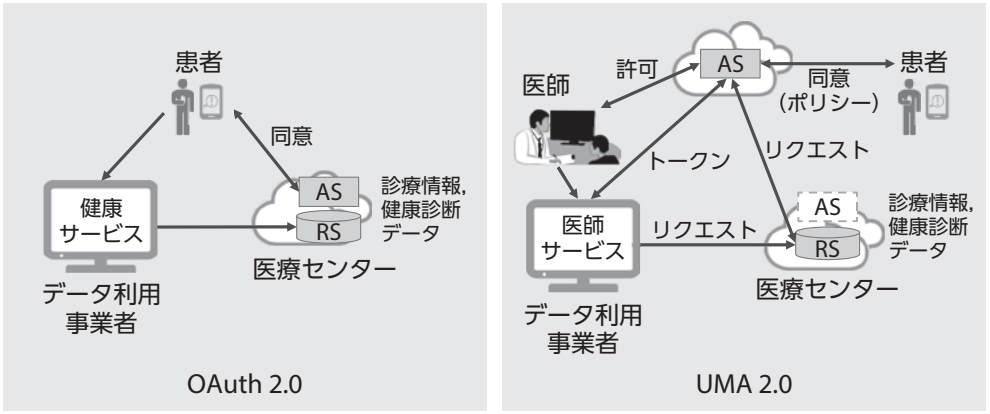


図-2　OAuth，UMAの構成例

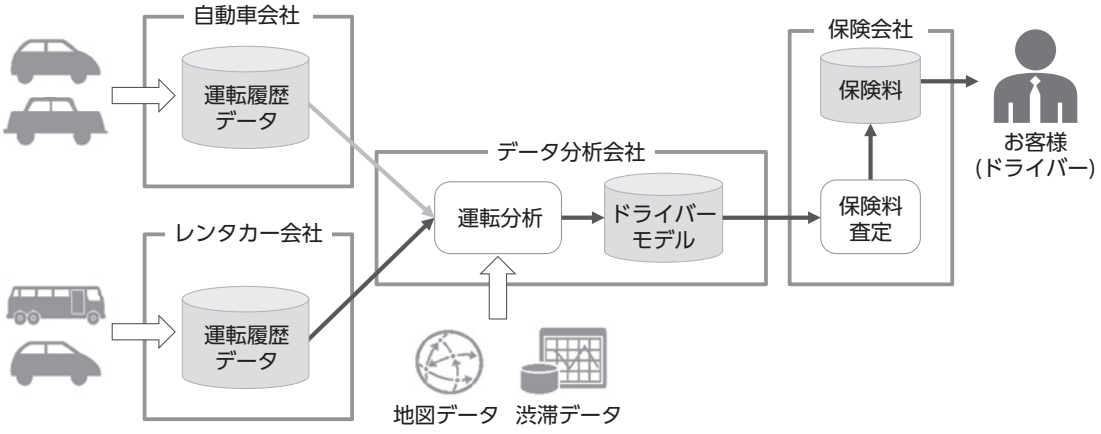


図-3　運転履歴に基づく自動車保険

と，メッセージ数が莫大な量となり，それに伴う処理量や通信量を抑えることが課題である。

(2) 開発技術

上記課題に対して，UMAを拡張しデータフォーマットや属性指定を埋め込めるようにすることにより，複数のデータ群を仮想的に一人分のデータとして扱い，このデータ群をトークンに割り付ける手法を考案した。これにより，UMAが本来備えるアクセス制御の安全性を活かしながら，取得する人数に関わらず2回分のシーケンスで複数名のデータを一括取得できるようになった。ただし，この拡張によって標的型メールなどで不正なリンクを送り，データを取得する攻撃に対する脆弱性が生じる。そこでトークンの検証機能も追加した。

3. 2　開発技術がもたらす効果

UMAでは，認証サーバで同意結果の確認を行っているため，企業間でデータを一括取得する際も同意されたデータのみが転送される。認証サーバに保持された同意情報や個人データのアクセス履歴は，ブロックチェーンで管理されるため改ざんすることは困難である。なおこの管理においては，富士通のブロックチェーンクラウドサービス「FUJITSU Intelligent Data Service Virtuora DX データ流通・利活用サービス」を利用している。

また，本人同意を取得する際に利用可能な同意ポータルも試作した。これにより，サービス提供者は独自の同意取得アプリケーションや同意情報の管理システムを構築しなくても良い。また，利用観点

から操作を一元化することで扱いやすくなっている。

本技術の応用例として，例えば，データ分析会社が，自動車会社やレンタカー会社から取得した運転履歴データの活用も考えられる（図-3）。この運転履歴データに地図データや渋滞データなど運転分析に必要なデータを加えて，ドライバーの運転モデルを作成し，それに基づいて保険料を算出する個人特化型の自動車保険（テレマティクス保険）のサービスが考えられる。ユーザーは，自身が提供に同意したいずれのデータから保険料が算定されたかといった根拠を確認することができる。

4. むすび

本稿では，デジタルビジネスを支える，富士通研究所が考える守りと攻めのセキュリティの最新技術について述べた。

データの法規制，個人情報の漏えい，AIに与えるデータの信頼性といった新たなリスクに加えて，IoTを含めたサイバー攻撃も増大し被害も大きいものとなっている。その一方で，セキュリティ専門家が足りないという現実がある。本稿で述べた，AIやブロックチェーンを活用した新たなセキュリティ技術は，こうしたセキュリティ専門家の能力を拡張し，人・データ・システムのトラストを実現する技術である。引き続き実用化に向けた研究開発を進めていく。

参考文献

(1) 経済産業省：サイバーセキュリティ経営ガイドライン.
http://www.meti.go.jp/policy/netsecurity/mng_guide.html
(2) 富士通研究所：車載ネットワークでのサイバー攻撃を検知する技術を開発.
http://pr.fujitsu.com/jp/news/2018/01/24-1.html
(3) 富士通研究所：業種業界を超えたデータ流通の信頼性を向上する技術を開発.
http://pr.fujitsu.com/jp/news/2018/09/20-1.html

著者紹介

津田　宏（つだ　ひろし）
(株) 富士通研究所
セキュリティ研究所
データセキュリティやブロックチェーンの研究開発に従事。

鎌倉　健（かまくら　けん）
(株) 富士通研究所
セキュリティ研究所
データセキュリティやブロックチェーン応用の研究開発に従事。