ビッグデータ利活用に向けたIoTセキュリティ
～相互認証と位置データ匿名化技術～

IoT Security for Utilization of Big Data: Mutual Authentication Technology and Anonymization Technology for Positional Data

● 新崎　卓　● 森川郁也　● 山岡裕司　● 酒見由美

あらまし

モノ（機器）のインターネットと呼ばれるIoT（Internet of Things）の普及が進むとともに，IoTによって収集されたビッグデータを解析して利活用することやアプリケーションへの活用が進んでいる。対象となるIoT機器は，センサー，自動車，家電，ウェアラブル端末など多種に及び，やり取りされるデータの種類を考慮しながら機器や使い方に応じたセキュリティ技術を適用していく必要がある。

本稿では，IoTセキュリティに求められる要件を示すとともに，富士通研究所の具体的な取組みとして，IDベース鍵共有方式をTLS（Transport Layer Security）に拡張適用して相互認証と暗号通信を同時に実現した技術を紹介する。また，位置データ利活用のための匿名化技術として，地図上の固定メッシュを多層的に使用することで，小さい領域のデータを安全により多く開示できる技術を紹介する。

Abstract

Along with the increased diffusion of the Internet, the “Internet of devices,” or Internet of Things (IoT), is becoming increasingly widespread and measures are being taken to utilize the gathered IoT data in big data analysis and applications. There is a wide range of target IoT items such as sensors, automobiles, consumer electronics and wearable devices, and this makes it necessary to apply security technologies according to the device and usage, while considering the types of data exchanged. This paper presents the requirements of IoT security. It also describes the following specific approaches of Fujitsu Laboratories: a technology that has realized mutual authentication and cryptographic communication at the same time by applying in an extended way an ID-based key agreement scheme to TLS; and a technology that allows more small-area data to be safely disclosed by having multi-tiered use of a fixed mesh on a map, which is anonymization technology for utilizing positional data.

まえがき

モノ（機器）のインターネットと呼ばれるIoT（Internet of Things）の普及が進むとともに，IoTによって収集されたビッグデータを解析して利活用することやアプリケーションへの活用が進んでいる。あらゆるものがインターネットにつながるIoTでのモノ（機器）は，工場の機器，センサー，自動車，端末機器，家電，ウェアラブル端末など多種に及ぶ。このようなモノとモノ同士が接続され，これらが提供するデータをデータベースとして扱うことで，以前とは違う新しい価値を生み出すことができる。

ユーザーが扱うこれらのIoT機器もクラウドにつながることを前提としたアーキテクチャーとなり，更に複数のクラウドがアメーバ的に連携してハイパーコネクテッド・クラウドが形成されていくと考えられる。

IoT機器は多種多様であり，やり取りされるデータも様々であることから高いセキュリティが求められる。一方で，これらの機器が持つ情報処理の能力も様々であるため，従来のパソコン，スマートフォンに使われているセキュリティ技術をそのまま利用することは難しく，機器や使い方に応じたセキュリティ技術を適用していく必要がある。

更に，IoTは様々な機器から収集されるデータの分析結果を利活用する。この中にはパーソナルデータも含まれる可能性があるため，プライバシー保護に関する技術も重要となる。

本稿では，まずIoTセキュリティに必要な技術を紹介する。次に，これらの具体的な事例として，ビッグデータ利活用に向けたIDベース暗号によるIoT機器向けの相互認証技術と，位置データ利活用のための匿名化技術を紹介する。

IoTセキュリティに必要な技術

富士通は，Fujitsu Technology and Service Vision[(1)]において，ICTがビジネスと社会のイノベーションにどのように貢献するのかについてまとめている。そのなかで，安全なICT環境を構築するための視点として「認証・認可」「データ・プライバシー保護」「セキュリティインテリジェンス」の三つの柱が重要であると定義している。これらをIoTセキュリティに当てはめてみると，「機器認証・アクセス制御」「データ保護・プライバシー保護」「機器脆弱性対策とサイバー攻撃対策」であると言える。

（1）機器認証・アクセス制御

接続される機器間の相互認証やアクセス制御を行うための技術である。機器間での相互認証を行いセキュアなデータ通信を行うことで，外部の攻撃から機器を守ることができる。また，IoT機器から送られるデータを利活用していくためには，誰のデータを計測しているのか，誰が利用しているのかといった，機器と人を結びつけるための認証技術やセンサーIDとヒトのIDを連携するための技術も必要となる。

（2）データ保護・プライバシー保護

IoT機器でやり取りされるデータを外部の攻撃から守るためには，データ保護の技術が必要である。また，やり取りされるデータの分析結果を利活用する場合は，パーソナルデータも含まれることが想定されるため，匿名化などのプライバシー保護技術が必須となる。

（3）機器脆弱性対策とサイバー攻撃対策

機器の脆弱性対策を施すとともに，起こり得るセキュリティインシデントの予兆をいち早く捉え，迅速に対処する技術も必要である。IoT機器はネットワークに接続されるため，現在のパソコンやスマートフォンのように脆弱性を悪用した攻撃を受けることが想定される。これらの攻撃に対する耐性を強化する脆弱性対策を行うとともに，攻撃に対する早期の検知，更には侵入された際の被害状況の早期確認と対策が必要である。

万が一，工場内の機器がサイバー攻撃された場合でも，マルウェアの感染・被害状況を迅速・適切に把握することで，工場の一部停止にとどめることも可能である。

IoTセキュリティは，非常に限定された環境でこれらを実現する必要がある。つまり，低い機器性能（処理能力，メモリ量，供給電力），制限されたネットワーク接続，限定的なユーザー操作などを考慮しながら，セキュリティを考えていくことが必要である。

IoTセキュリティが受ける脅威とその対策技術の概要を**図-1**に示す。

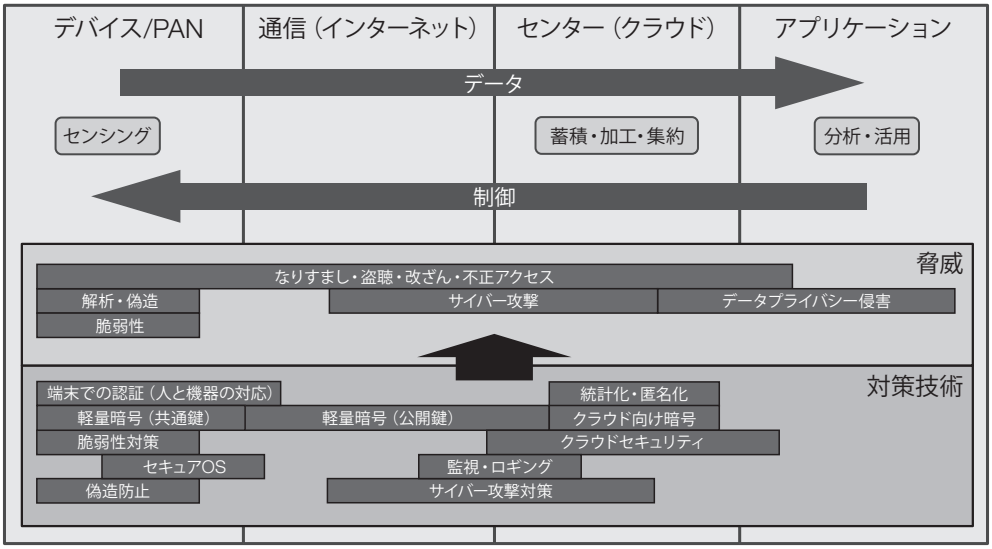


図-1　IoTセキュリティの脅威と対策技術

IoT機器向け相互認証技術

● 背景

IoTシステムの普及が進むと，機器が収集した情報の分析結果を利活用する新たなビジネスが注目されはじめた。例えば，トラクターなどの産業機械に現在の状態を通信する機能を搭載し，部品の消耗状態や交換時期を分析することで，適切な時期の部品交換が可能となる。また，BEMS（Building Energy Management System）などのエネルギー管理システムは，空調や照明をネットワーク接続することで，機器の状態や消費電力などの情報を収集可能である。更に，BEMSは収集した使用電力量のデータを分析し，その結果に基づいて機器に制御情報を送ることで，省電力化や電力の逼迫（ひっぱく）時の対応を可能とする。

このように，IoTシステムはサーバが機器からデータを収集するだけでなく，サーバから機器を制御するという双方向通信のモデルとなる。こうした用途においては，収集した情報が正当な機器から送信されたかどうかの確認や，不正に機器を制御されないために，サーバのみを認証するサーバ認証ではなく，機器とサーバの双方が正当であることを確認する相互認証が必須となる。更に，2020年には接続されるデバイスが約500億個になることが予想されており，そこで使用される相互認証技術にも高い効率が求められる。富士通研究所は，IoTシステムに必要となる機器間の相互認証を効率的に行う技術を研究開発している。

現在のインターネットにおいては，TLS（Transport Layer Security）と呼ばれる認証・暗号通信技術が広く利用されている。TLSでは，相互認証を実現する機能として，事前共有鍵（PSK：Pre-Shared Key）を用いたTLS-PSKや，公開鍵暗号技術であるRSA暗号とDiffie-Hellman（DH）鍵共有を使用する認証方式TLS-DHE-RSAなどが提供されている。

TLS-PSKは，機器性能が制約される環境での利用を目的とした相互認証方式として規定されている。この方式では，相互認証する二つのエンティティが事前に秘密情報（事前共有鍵）を共有することで互いの正当性を証明する。認証処理では，共通鍵暗号のみが使用されるため，センサーネットワークなど，計算性能が制約された環境に適している。しかしこの方式では，機器の盗難・解析などにより事前共有鍵が漏えいした場合，システム全体のセキュリティが低下する危険性がある。

一方，TLS-DHE-RSAは，インターネット上のWebサービスなどで広く利用されている認証方式であり，公開鍵暗号が使用されている。一般に公開鍵暗号を使用するためには，ユーザーや機器と使用する鍵とのひも付けを保証する証明書が必要となる。相互認証する際には，まず証明書を互いに送信し，証明書検証と鍵交換と呼ばれる公開鍵

暗号処理を行う。公開鍵暗号ではエンティティごとに異なる秘密鍵を使用するため，TLS-PSKとは違い秘密鍵が漏えいしてもシステム全体のセキュリティは保たれる。しかし，この方式はシステム上の全ての機器やサーバに証明書を保持させ，公開鍵暗号処理を行うため，負荷が高いという問題がある。そのため，機器数が膨大なIoTにおいては，全機器に証明書を準備・管理する膨大な工数と，証明書を検証する暗号処理・通信量の爆発的増加が課題となる。そこで富士通研究所では，証明書を利用することなく相互認証を実現する新しい技術を開発した。[2]

● 開発技術

富士通研究所が開発した技術は，IDベース暗号技術と呼ばれる公開鍵暗号技術を活用している。これは，機器ID，メールアドレス，FQDN（Fully Qualified Domain Name）など，ユーザーや機器，サーバとひも付けされた情報（ID）を公開鍵として利用可能な技術である。従来のTLSで利用されている公開鍵暗号技術であるRSA暗号や楕円曲線暗号は，IDとは無関係に生成された乱数を鍵として利用する。そのため，事前に通信相手の証明書を入手し，その鍵（乱数）の正当性を検証する必要がある。これに対し，IDベース暗号技術では相手のIDが鍵そのもののため，証明書の事前入手や証明書を使った鍵の確認をすることなく暗号化が可能となる。この暗号技術のコンセプトは，1984年にShamirによって提案され，[3] 2000年に境らによって実用的な方式が提案された後，Bonehらによる方式が提案されるなど，[4, 5] 活発に研究が進められている。

富士通研究所の開発技術は，IDベース暗号技術の中でも，証明書を使用することなくIDにより安全な鍵の共有を実現するIDベース鍵共有技術を利用する。鍵を共有するために，まず相手の機器IDを用いて作成した部分鍵を互いに送り合う。次に，自身のIDに対応する秘密鍵を用いて，相手から入手した部分鍵から共有鍵を生成する。部分鍵の生成に使用したIDに対応する秘密鍵を保持する正当な機器のみが共有鍵を生成可能なため，この共有鍵によりその後の通信を行うことで，相互認証と暗号通信を同時に実現できる。

富士通研究所は，TLSを拡張してIDベース鍵共有方式を適用した技術を開発した。開発方式と従来TLSの認証手順の比較を**図-2**に示す。TLS拡張では，既定のTLSプロトコルに適合するように，IDベース鍵共有技術による共有鍵の生成に対し，整形・最適化を行った。特に，従来のTLSでは，証明書の交換なしには機器IDとしてIPアドレスやドメイン名などしか利用できない制約があった。しかし，送信者の情報を通信開始時に効率的に伝達する拡張を行うことで，任意の情報を機器IDとして利用可能にした。この拡張により，これまでのTLS利用と同等の簡便さで，機器IDによる相互認証技術の利用が可能となる。

● 評価

開発技術の効果を評価するため，TLSのOSS（Open Source Software）として広く利用されているOpenSSLに開発技術を実装し，性能評価を行った。評価では，サーバが機器からデータを収集する状況を想定し，クライアントを小型のシングルボードコンピュータ，サーバを汎用パソコンに実装した。その結果，従来のTLS-DHE-RSAと比較して通信量を約1/6，処理時間を約1/5に短縮することに成功した（**図-3**）。開発技術により，軽量に機器間の相互認証が可能となり，IoTにおいてもWebサービスなどと同等のセキュリティを実現できることが確認できた。

本研究で開発している認証技術は，IoTの基盤部分で利用される。今後，数百億個の機器がネットワークでつながるIoTの時代に相互接続性を確保するためには，富士通だけではなく，他社もしくは他研究機関との協力が重要となる。そのため現在，東大グリーンICTプロジェクト（GUTP：Green University of Tokyo Project）と共同でBEMS向け通信規格IEEE 1888[6]への本認証技術の導入を進めている。IEEE 1888は，東京大学や中国の企業・大学が共同で標準化を進めた通信プロトコルであり，2011年に国際標準化された。このプロトコルでは，HTTPとXMLによる通信方式を採用しており，ZigBeeやビル・オートメーションと制御ネットワークの通信規格であるBACnet（Building Automation and Control Networking protocol）などの様々な通信規格の統合管理を実現している。このプロトコルは，機器からのデータ収集だけでなく，機器への制御通信もサポートしている。こ

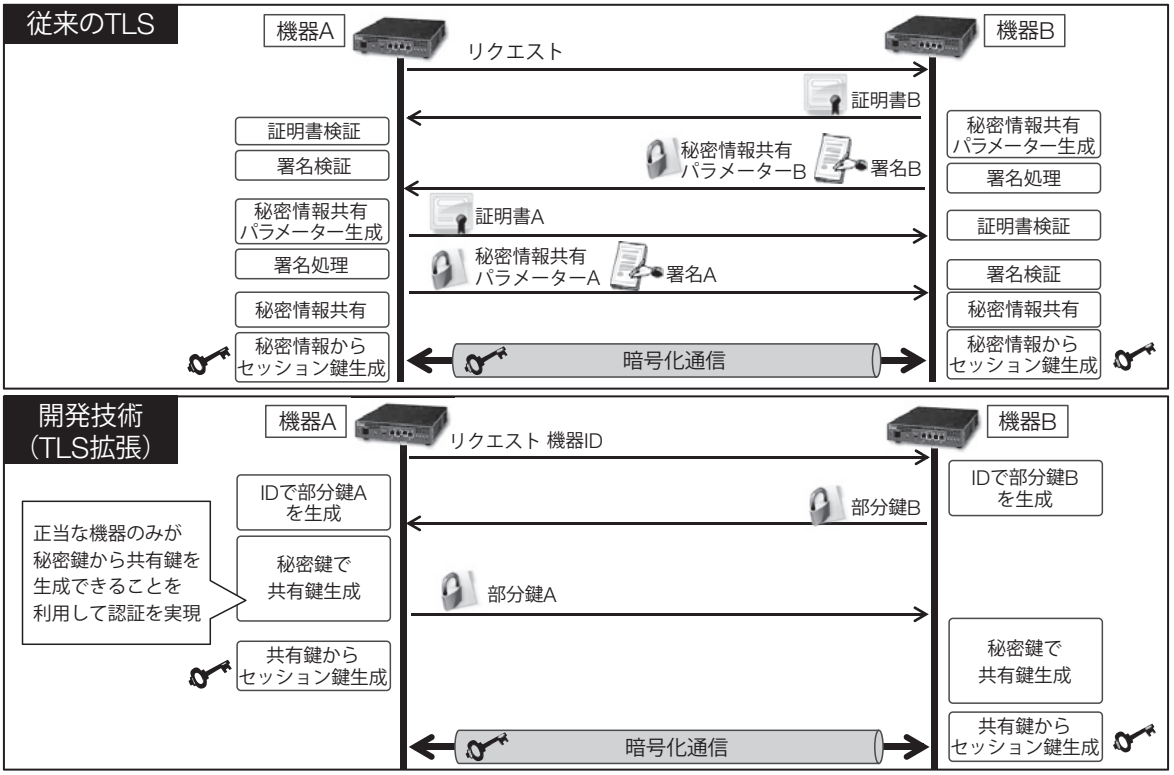


図-2　開発技術と従来のTLSとの比較

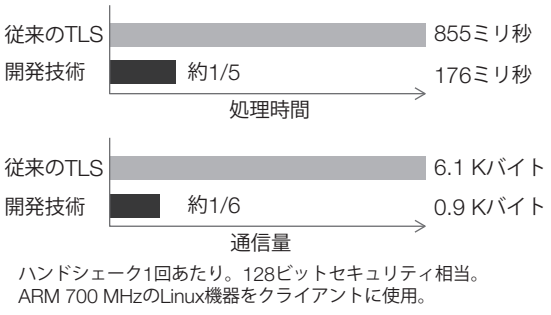


図-3　性能評価結果

のため，開発技術がターゲットとしている双方向通信モデルとなっている。今後は，GUTPとの実証実験を通じて相互接続性検証・課題抽出とその解決を進め，本プロジェクトでの採用およびIEEE標準化を目指す。

位置データ利活用のための匿名化技術

本章では，位置データ利活用のための匿名化技術への取組みについて説明する。

● 背景

近年，GPS受信機能を持つカーナビやウェアラブルデバイスがインターネットを通じて位置データを収集者に提供し，収集者が加工して第三者に開示する状況が見られるようになった。例えば，東日本大震災の被災地域において，走行する多数の自動車（提供者）の位置データを企業（収集者）が収集し，地図上にプロットして開示することで，第三者（活用者）が通行実績情報を得られるようにしたサービスが注目を集めた。(7)

昨今，パーソナルデータの適正な利活用に向けて個人情報保護法が改正されるなど，位置データの第三者提供はIoTの隆盛とともに今後ますます盛んになると考えられる。

しかし，位置データは提供者のプライバシーや機密を含む場合がある。例えば，訪れた店や施設などが知られると，他人に知られたくない個人の嗜好や状況などが推定されてしまう場合がある。したがって，収集者は提供者のプライバシーや機密を活用者から守るため，位置データを匿名化して開示する必要がある場合が多い。このような時代背景から，富士通研究所では様々なデータに関する匿名化技術の研究開発に取り組んできており，位置データについてもその対象としている。

● 開発技術

本稿で紹介する位置データは，提供者ID（identifier）と緯度・経度情報を持つレコードの集まりとする。また，各提供者は短い時間間隔でレコードを継続的に提供しているとする。例えば，前述の通行実績情報サービスでは，提供者IDは自動車（カーナビなど）のID，緯度・経度は自動車の位置となる。また，各IDにつき，例えば走行中に1秒間隔でレコード群が収集されている。

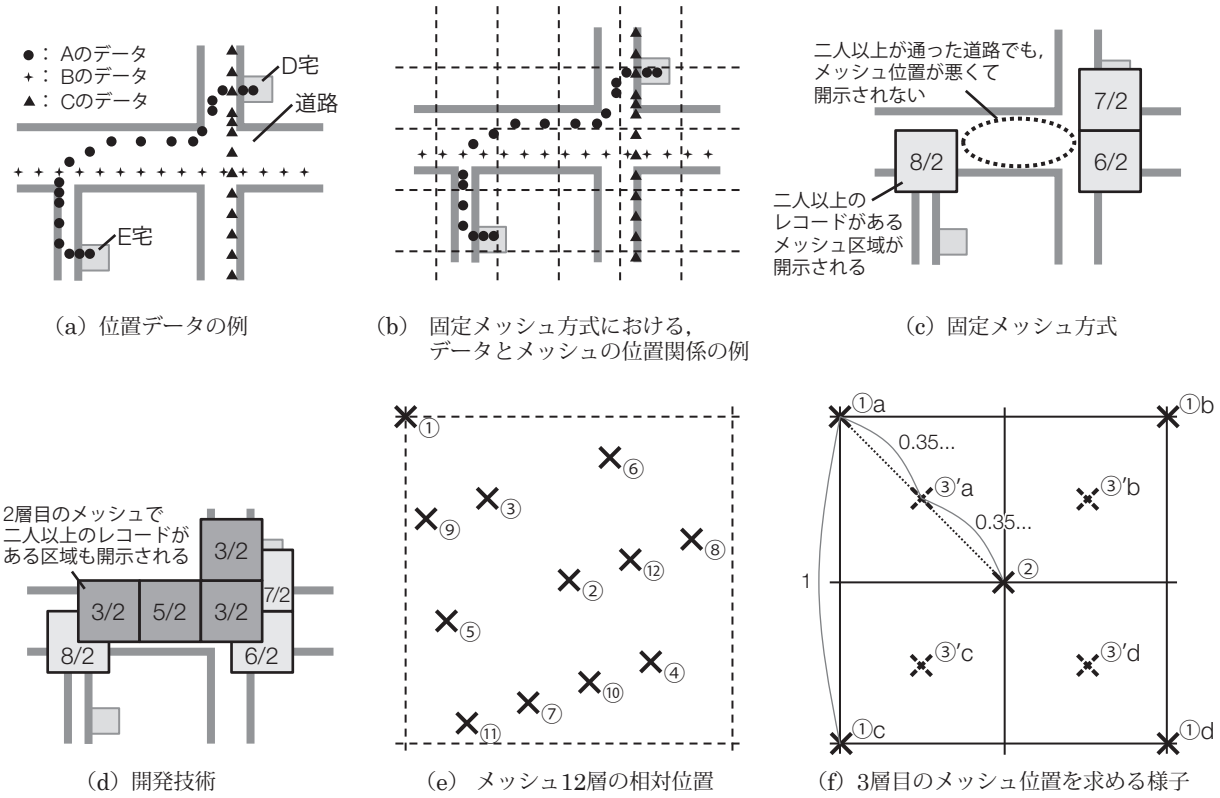
図-4（a）は，ある日の位置データを地図上にプロットした例である。提供者AはE宅からD宅へ自動車で移動しているが，D宅に寄ったことはE宅の主人Eに知られたくないと思っているとする。しかし，もしEが活用者であり，その日E宅に入った自動車がAだけと知っていた場合，このデータよりEはAがD宅に寄ったことが分かる。これはプライバシーの漏えいである。

位置データからのプライバシー・機密漏えいを防ぐためには，提供者が誰だか分からなくすること，つまり匿名化が効果的である。活用者は，特定の個人や企業の情報を知る必要はなく，多くの市民や商用車などの全体的な傾向が分析できれば良い場合も多い。例えば，前述の通行実績情報サービスがそれに該当する。

簡単な匿名化方式としてIDの削除があり，無名化と呼ばれる。無名化により，データが多い位置ではプライバシー・機密漏えいを軽減できる。しかし，そうでない位置では効果は限定的になる。例えば，図-4（a）を無名化すると，Eはどの点がAのものか確信できなくなるが，点の間隔や軌跡から容易に推定できる。

別の方式に，地図情報を使ってフィルタリングする方式がある。例えば，前述の通行実績情報サービスでは，幹線道路における情報のうち位置データがあった部分を開示したと言われている。生活道路の情報はプライバシー・機密漏えいになりやすいため，この方式は幹線道路以外に適用しづらいという問題がある。

また，位置データに対しよく用いられる別の方式に，あらかじめ決められた大きさで空間をメッシュに分け，各区域に含まれるレコード数を計上する方式がある。本稿では，これを固定メッシュ



（a）位置データの例　（b） 固定メッシュ方式における，データとメッシュの位置関係の例　（c）固定メッシュ方式

（d）開発技術　（e） メッシュ12層の相対位置　（f）3層目のメッシュ位置を求める様子

図-4　位置データ利活用のための匿名化技術

方式と呼ぶ。固定メッシュ方式では更に，含まれるID数が少ない区域の情報はプライバシー・機密保護のために開示しないことが多い。日本の総務省統計局は，地域メッシュ統計として固定メッシュ方式を使っており，区域の大きさとして約80 km四方から約250 m四方の5段階を定め，各区域にコードを割り当てている。しかし，例えばどの道路であるかを大まかに区別するためには，20 m四方程度の，より細かいメッシュを使う必要がある。

図-4（a）のデータに図-4（b）に示すメッシュを用いた固定メッシュ方式を適用し，ID数が2以上の区域を残した例を図-4（c）に示す。各区域内に記載の「n/v」はレコード数nとID数vを示しており，例えば「8/2」は二人の提供者の計8レコード分のデータがその区域中にあることを示している。元の48レコード中，本例では27レコードを開示できず，削除している。

固定メッシュ方式は計算量が少なく，ID数が少ないメッシュを開示しなければプライバシー・機密漏えいを軽減できる優れた方式である。しかし，細かいメッシュでは，図-4（c）で中央の道路内のレコードがほとんど開示されていないように，運悪く道路内にメッシュの境界が来るなどの場合に，開示されるデータが激減する問題がある。そこで，富士通研究所は小さい領域のデータを安全により多く開示できる新しい技術を開発した。

開発技術は，固定メッシュを多層的に使用することで，開示できる領域を増やす。図-4（d）は，図-4（c）で使用した1層目のメッシュに加え，2層目のメッシュを使用することで開示できる領域が増えた様子を示したものである。2層目のメッシュにより新たに14レコードを開示できている。一般的に，メッシュ層数が多いほど開示できるレコード数が増える。計算量は層数に応じてほぼ線形に比例するが，1層あたりの計算量が少ないため問題になりにくい。

更に，メッシュを効果的に配置する方法を開発した。新しいメッシュの位置は，既に使用したどのメッシュからも離れている方が効果が高い。そこで，既存メッシュの全ての辺から最も遠い点のうち，既存メッシュの全ての頂点の中からより近い頂点がより遠い点を新しいメッシュの頂点とすることにした。12層までのメッシュ頂点の相対位置を図-4（e）に示す。例えば3層目のメッシュ頂点の位置を求める様子を図-4(f)に示す。図-4(f)で，全ての辺から最も遠い点は③′a ～ dの四つであり，③′aに近い点は①aと②である。それらとの距離は，メッシュ区域の大きさを1四方とするといずれも0.35...であり，③′b ～ dも同様で，③′a ～ dは差がつかないため新しいメッシュの頂点は③′a ～ dのいずれかとする。この方法は3次元以上にも応用可能であり，緯度・経度のほかに高度や時刻を含めたデータの匿名化にも適用できる。

● 評価

以下に示す実際のデータに適用したところ，固定メッシュ方式に比べて開発技術は約7％レコードを多く開示できた（**図-5**）。

・経度・緯度単位が0.1秒（約3 m）
・自動車約1000台分の毎秒走行位置データ1週間分
・地域メッシュコード5339-36内（東京都江東区有明周辺，約300万レコード）

区域の大きさは24 m四方とし，ID数が3以上の区域のみ開示した。開発技術ではメッシュを8層使用した。処理速度は，一般的なパソコンで固定メッシュ方式約6秒に対し開発技術約90秒であり，十分実用的な性能と言える。

以上のように，富士通研究所は，小さい領域の位置データを安全により多く開示できる新技術の開発に成功した。これにより，例えば通行実績情報サービスを幹線道路以外にも適用できる可能性が高まった。今後は，開発技術により開示される

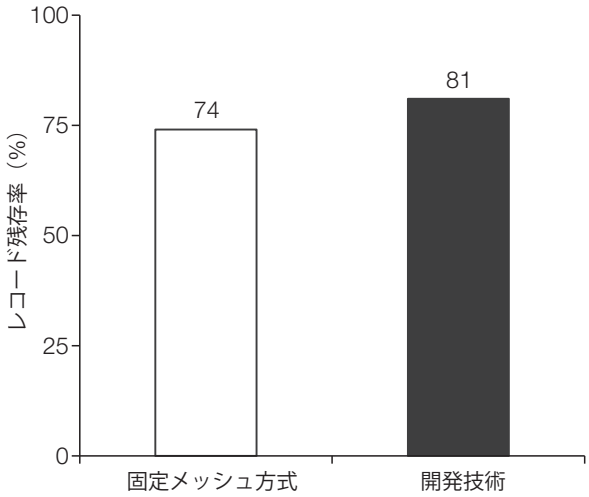


図-5　開発技術の効果

レコード数の増加による効果を実際の活用場面で評価したい。

むすび

本稿では，IoTセキュリティとビッグデータの利活用に関する富士通研究所の取組みを紹介した。

IoTセキュリティでは,「機器認証・アクセス制御」「データ保護・プライバシー保護」「機器脆弱性対策とサイバー攻撃対策」技術が重要である。富士通研究所の具体的な取組みとして，IDベース鍵共有方式をTLSに拡張適用して相互認証と暗号通信を同時に実現する技術と，位置データ利活用のための匿名化技術として地図上の固定メッシュを多層的に使用することで小さい領域のデータを安全により多く開示できる技術を紹介した。

今後，IoT機器はクラウドにつながることを前提としたアーキテクチャーになると考えられる。大量のIoT機器がクラウドにつながり，更に複数のクラウドがアメーバ的に連携してハイパーコネクテッド・クラウドが形成されていくと考えられる。

富士通研究所では，IoTの将来を見据えて，ハイパーコネクテッド・クラウドを想定したIoTセキュリティ技術の研究開発を進め，クラウドやIoTプラットフォームへの適用を推進していく。更には，これらのプラットフォーム上で，安心・安全にIoTデータを収集し，データを利活用するための仕組みの研究開発を進めていく。

参考文献

(1) 富士通：Fujitsu Technology and Service Vision. http://www.fujitsu.com/jp/vision/

(2) 酒見由美ほか：IDベース認証機能付鍵交換のTLS適用とその実装評価．暗号と情報セキュリティシンポジウム（SCIS）2016，2016.

(3) A. Shamir：Identity-based cryptosystems and signature schemes．CRYPTO 1984，Springer，LNCS 196，p.47-53，1984.

(4) R. Sakai et al.：Cryptosystems based on pairing. SCIS2000，2000.

(5) D. Boneh et al.：Identity-based Cryptography Standard（IBCS）#1．CRYPTO 2001，Springer，LNCS 2139，p.213-229，2001.

(6) 落合秀也：IEEE 1888プロトコル教科書，インプレスジャパン，2012.

(7) 須藤三十三ほか：広域的な災害発生後のプローブ情報の活用－東日本大震災での事例を通して－．情報システム学会誌，Vol.8，No.1，p.30-41（2012）.

著者紹介

新崎　卓（しんざき　たかし）
知識情報処理研究所
次世代・認証認可プロジェクト 所属
現在，認証技術に関する研究開発に従事。

山岡裕司（やまおか　ゆうじ）
知識情報処理研究所
データ・プライバシー保護プロジェクト 所属
現在，データ・プライバシー保護技術に関する研究開発に従事。

森川郁也（もりかわ　いくや）
知識情報処理研究所
次世代・認証認可プロジェクト 所属
現在，認証技術に関する研究開発に従事。

酒見由美（さけみ　ゆみ）
知識情報処理研究所
次世代・認証認可プロジェクト 所属
現在，認証技術に関する研究開発に従事。