構造化 P2P ネットワークと加法準同型暗号を用いたセキュアでスケーラブルな分散型データ集計手法の開発

代表研究者　　武　田　敦　志　　東北学院大学　教養学部　准教授

1 はじめに

通信機能を備えた安価な小型センサ端末が開発されたことにより、様々な場所にセンサ端末を配置し、インターネットを介して各センサ端末の観測データを取得することが可能となった。様々な場所にセンサ端末を設置し、これらの端末から得られる観測データを活用することにより、従来よりも安全かつ効率的な社会システムが実現できると期待されている。これらの観測データを活用するためには、個々のセンサ端末が観測したデータを収集し、平均や分散などの全体の指標となる値を集計する仕組みが必要不可欠である。現在まで、センサ端末からの観測データをクラウド環境に設置されたサーバに蓄積し、このサーバを用いて観測データの集計を行う仕組みが開発されてきた。しかし、安価で高性能なセンサ端末を様々な場所に設置し、これらのセンサ端末から膨大な量の観測データを取得する場合、すべての観測データを単一のサーバで集計することは現実的ではない。そこで、本研究課題では、各センサ端末がお互いに連携することで観測データの集計を行い、その集計結果のみを利用者やアプリケーションに送信する観測データ集計システムを開発した。このシステムでは、センサ端末をノードとする構造化 P2P ネットワークを構成し、この構造化 P2P ネットワークのルーティング情報に基づいて観測されたデータをそれぞれのノードが集計する分散型のデータ集計システムである。構造化 P2P ネットワークの仕組みを活用することにより、データを集計するために各ノードが必要とする計算量や通信データ量は $O(\log N)$ (N はネットワーク上のノードの数) となる。そのため、このデータ集計システムは従来のサーバを用いたデータ集計システムよりもスケーラビリティに優れたシステムだといえる。また、加法準同型暗号を用いることにより、暗号化されたデータを復号化せずに集計することができる。この仕組みを導入することにより、データを観測したセンサ端末と利用者端末以外で復号化する必要がなくなるため、秘密のデータを扱うことができるセキュアなデータ集計システムを構築できる。このセキュアでスケーラブルな分散型データ集計システムを用いることにより、既存手法では困難であった「広域に分散配置された大量のセンサ端末から得られる観測データの安全で効率的な集計」が可能になる。

平成 28 年度までの研究を通じて、決定的アルゴリズムに基づく構造化 P2P ネットワークを利用することにより、柔軟に制御可能でスケーラブルな分散型データ管理システムを実現できることが明らかになった。また、構造化 P2P ネットワークのルーティング情報に基づいてセンサ端末がお互いに連携することにより、従来の 20%以下の通信データ量で平均や分散などのデータ集計処理を実行可能であることが判明している[1]。さらに、センサ端末の物理的な位置を考慮した構造化 P2P ネットワークを構築することにより、一部地域のセンサ端末の観測データのみを対象とした集計処理を実現した[2]。本研究課題では、これらの研究成果をさらに発展させるため、これらのデータ集計システムで実行可能な計算処理を整理した。これにより、構造化 P2P ネットワークを用いた分散型データ集計システムが、平均や分散などの基本的なデータ集計だけではなく、t 検定や線形回帰分析などの実用的な統計分析にも対応可能であることを明らかにした。また、t 検定や線形回帰分析などの統計分析を行う場合、データ観測端末と利用者端末以外のノードに必要となる計算は加算のみであることを確認した。これにより、この分散型データ集計システムに加法準同型暗号を導入することにより、観測データを暗号化したまま集計処理を行うセキュアなデータ集計システムを実現可能であることが明らかとなった。

本研究課題では、構造化 P2P ネットワークを用いた分散型データ集計システムのプロトタイプを実装した。このプロトタイプシステムを用いて実験を行い、この分散型データ集計システムを用いることにより各ノードが持つ値の主成分分析が可能であることを確認した。また、プロトタイプシステムを用いた性能評価を行い、データ集計のために各ノードが必要とする通信データ量が $O(\log N)$ (N はネットワーク上のノード数) であることを確認した。さらに、実環境に分散型データ集計システムを実装し、このデータ集計手法が実現可能であることを確認した。

一方、実環境上に分散型データ集計システムを実装するにあたり、複数設置するセンサ端末のすべてに対してパスワード等の初期設定を行う必要があり、この設定作業が煩雑であるという問題が発生した。この問

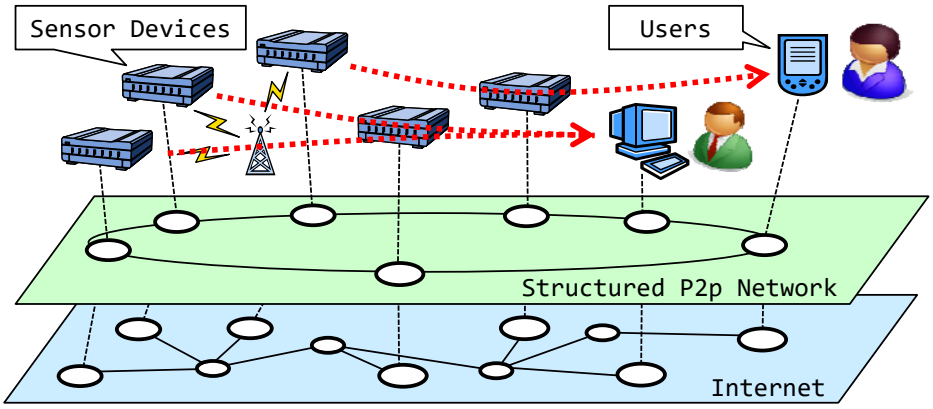

図 1　本研究課題で想定するコンピュータネットワーク

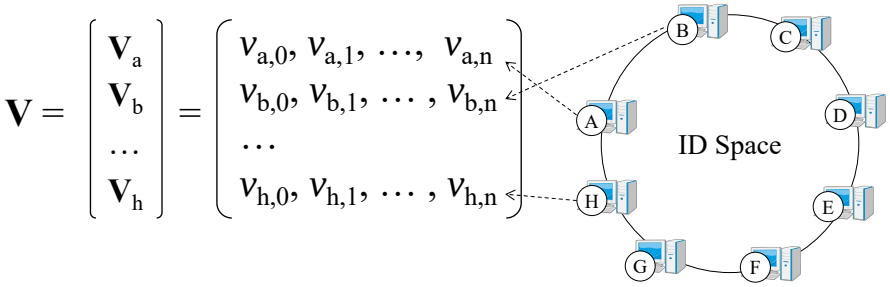

図 2　本課題で開発した分散型データ集計システムの構成

題を解決するため、センサ端末と操作端末との物理的な接触に基づく端末認証手法を開発した。この端末認証手法を用いることにより、パスワードなどの初期設定を行っていないセンサ端末に対しても操作端末から安全に接続することが可能となる。この端末認証手法のプロトタイプを実装し、実環境上で動作させることにより、センサ端末と操作端末との物理的な接触に基づく端末認証を実現できることを確認した。

本報告書では、2 章において構造化 P2P ネットワークを用いた分散型データ集計手法について説明し、その性能評価結果を示す。また、3 章では物理的接触に基づく端末認証手法について述べ、物理的接触を信頼の根拠として操作端末を認証する手順を説明する。最後に 4 章において本研究課題の成果をまとめ、この研究課題の結果を評価する。

2 構造化 P2P ネットワークを用いた分散型データ集計システム

2-1 システムの概要

近年、センサ端末で観測されたデータを集計するための仕組みが盛んに研究されており、それぞれのセンサ端末が連携することにより主成分分析などの統計処理を行う仕組みが提案されている[3, 4, 5]。しかし、これらの既存手法はセンサネットワークなどのローカルネットワークを介した通信を想定しており、広域に分散配置された膨大な量のセンサ端末を連携させることは想定していない。一方、構造化 P2P ネットワークを用いることにより、広域に分散配置された各ノードが持つ値を集計する分散型データ集計システムが提案されている[6, 7, 8, 9]。しかし、これらのシステムは合計値・平均値・最大値・最小値などの基本的な集計のみを対象としており、主成分分析や線形回帰分析などの統計分析を行うための集計は想定していない。そこで、本研究課題では、広域に分散配置されたセンサ端末が連携することにより、これらのセンサ端末によって観測されたデータの主成分分析や線形回帰分析を行うための分散型データ集計システムを開発した。このデータ集計システムが想定している利用環境を図 1 に示す。広域に分散配置された各センサ端末はインターネットを介してお互いに通信可能であり、これらのセンサ端末が連携することによりデータを集計し、その集計結果を利用者端末に送信する。本研究課題で開発した分散型データ集計システムでは、合計値や平気値などの基本的な集計だけではなく、標準偏差や共分散行列などの統計解析に必要となるデータ集計を実施できる。以下、本報告書では、このデータ集計システムの集計アルゴリズムを述べ、このデータ集計システムが主成

分分析や線形回帰分析に必要となる共分散行列を計算できることを説明する。

2-2 システムの構成

図 2 に本研究課題で開発した分散型データ集計システムにおけるノードとデータの関係を示す。従来の構造化P2Pネットワークと同様に、この分散型データ集計システムでは各ノードを仮想的なID空間上に配置し、その IS 空間上の位置に基づいてメッセージの送信先を決定する。ここで、それぞれのノードは以下の情報を管理している。

$$
\begin{aligned}
\text{node} &:= \langle\ \text{id},\ \text{value},\ \text{routes}\ \rangle \\
\text{id} &:= \text{INTEGER} \\
\text{value} &:= \{v_0,\ v_1,\ v_2,\ \cdots\} \\
\text{routes} &:= \{\text{route}_0,\ \text{route}_1,\ \text{route}_2,\ \cdots\} \\
\text{route}_i &:= \langle\ \text{node}_i,\ \text{value}_i\ \rangle
\end{aligned}
$$

ここで、id はそのノードの ID 空間上の位置であり、value はそのノードが管理しているデータである。また、routes はそのノードのルーティングテーブルであり、各ノードはメッセージの送信先ノードの一覧をルーティングテーブルとして管理する。また、この分散型データ集計システムでは、それぞれのノードはメッセージの送信先ノードの情報だけではなく、そのノードから受け取った部分的な集計結果である $value_i$ もルーティングテーブルの値として管理する。この部分的な集計結果 $value_i$ は、ID 空間上で $node_i$ と $node_{i+1}$ の間に存在するノードが持つデータの集計結果であり、そのノードのルーティングテーブルが更新されるときに送信先ノードから取得する値である。それぞれのノードが定期的にルーティングテーブルの更新処理を実行することにより、メッセージの送信先の情報だけではなく、部分的な集計結果も更新する。このルーティングテーブルの更新に必要となる通信メッセージは Chord[10]などの構造化 P2P ネットワークと同じであり、それぞれのノードがルーティングテーブルを更新するために必要とうなる通信データ量は O(log N) (N はネットワーク上のノード数) となる。一方、この部分的な集計結果を集めて集約することにより、すべてのノードが持つデータの集計結果を得る。部分的な集計結果を集めるための通信メッセージはChordなどの構造化P2Pネットワークにおける探索メッセージと同じであり、ノードが部分的な集計結果を集めるために必要とする通信データ量も O(log N)となる。

2-3 データ集計手順と共分散行列の計算

本研究課題で開発した分散型データ集計システムは、センサ端末で観測されたデータを集計し、その集計結果を利用者端末に表示する。この集計手順は以下の３つのステージに分けることができる。

(1) センサ端末による計算
(2) 構造化 P2P ネットワークによるデータ集計
(3) 利用者端末による計算

センサ端末による計算と利用者端末による計算では、単一のノードにあるデータのみを用いて必要な計算を実行するため、四則演算だけではなく、データの分割や変形などの複雑な計算を実行できる。一方、構造化 P2P ネットワークによるデータ集計では、2-2 で述べた手順でデータ集計を行うため、ここでは総和・総乗・最大値・最小値の計算のみ実行可能である。そのため、この分散型データ集計システムを用いて主成分解析や線形回帰分析を行うためには、このシステムに適した計算順序を開発する必要がある。

ネットワーク上のノード $node_i$ 保持しているデータを $\mathbf{V}_i$ とし、そのネットワークのすべてのノードが保持しているデータを $\mathbf{V}=(\mathbf{V}_0, \mathbf{V}_1, \cdots, \mathbf{V}_n)^T$ とし、ネットワーク上のノードの数を N とすると、共分散行列 Cov(**V**) は

$$\mathrm{Cov}(\boldsymbol{V}) = \frac{1}{N}\boldsymbol{V}^T\boldsymbol{V} - \overline{\boldsymbol{V}}^T\overline{\boldsymbol{V}}$$

となる。この共分散行列の計算を行うためには１つのノードにすべてのデータを集める必要があるため、共分散行列の計算に必要となる通信データ量は O(N)となる。そこで、この共分散行列の式の計算順序を変更し、

$$\mathrm{Cov}(\boldsymbol{V}) = \frac{1}{N}\sum \boldsymbol{V}_i^T\boldsymbol{V}_i - \frac{1}{N^2}\left(\sum \boldsymbol{V}_i\right)^T\sum \boldsymbol{V}_i$$

とする。この計算順序であれば、2-2 で述べた手順でデータ集計を行うことが可能となるため、この共分散

行列の計算に必要となる通信データ量は O(log N)となる。これにより、膨大な数のセンサ端末が大量の観測データを持っていたとしても、現実的な計算時間で共分散行列を計算することができる。共分散行列の計算結果を用いることで、データの主成分分析や線形回帰分析が可能となる。すなわち、本研究課題で開発した分散型データ集計システムを用いることで、膨大な数のセンサ端末が観測したデータの主成分分析や線形回帰分析を行うことが可能となる。

分散型データ集計システムを用いて共分散行列を計算する場合、部分的な集計結果を得るために必要となる計算は加算のみである。そこで、Paillier 暗号などの加法準同型暗号を用いて集計対象のデータを暗号化することにより、部分的な集計を行う他のノードにデータの内容を見られることなく共分散行列の計算を行うことができる。すなわち、本研究課題で開発した分散型データ集計システムは、秘密にしたい観測データやプライバシーに関わる登録データを安全に集計することができる。

2-4 プロトタイプシステムの実装と性能評価

本研究課題で開発した分散型データ集計システムの機能を検証するため、このデータ集計システムのプロトタイプシステムを実装した。また、このプロトタイプシステムを用いて分散型データ集計システムの性能評価を行った。プロトタイプシステムは 1 台のサーバを用いた実験を想定しており、複数のノードが 1 個のプロセスとして動作する。ただし、それぞれのノードは別スレッドで動作しており、データの共有は行っていない。ノード間でデータを交換する必要がある場合は、ループバックインタフェースを介してメッセージデータを送受信する。このプロトタイプシステムを用いて、分散型データ集計システムが正しく共分散行列を計算し、主成分分析を実施できることを検証した。また、それぞれのノード間で送受信されるメッセージの通信データ量を計測し、分散型データ集計システムのスケーラビリティを評価した。

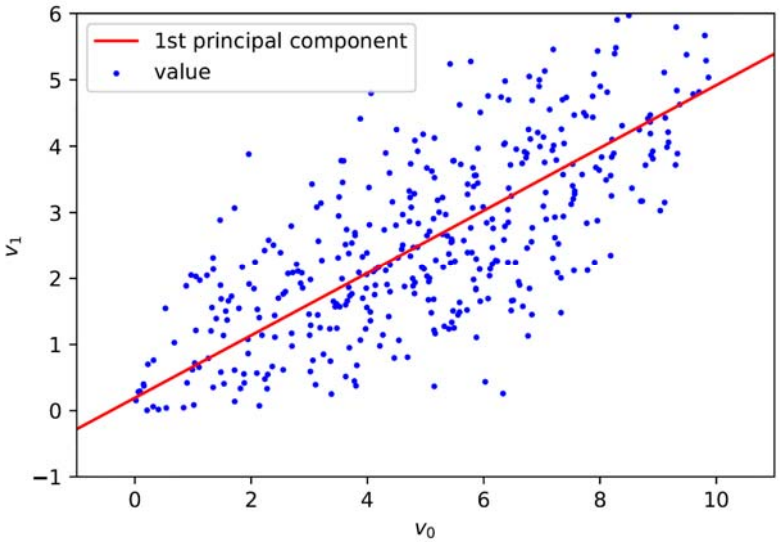

図 3　分散型データ集計システムを用いた主成分分析の計算結果

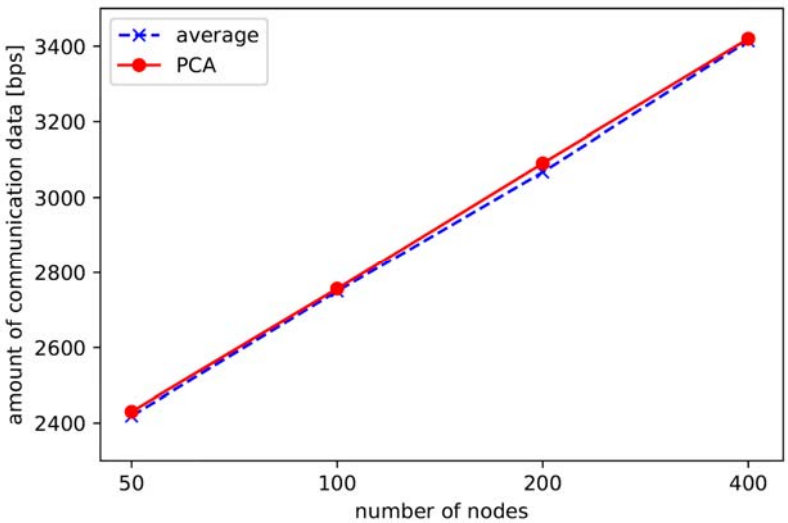

図 4　データ集計に必要となる通信データ量

図 3 に分散型データ集計システムを用いて実施した主成分分析の結果を示す。この実験では、構造化 P2P ネットワーク上に 400 個のノードを作成し、それぞれのノードに異なる 2 次元ベクトルの値を設定した。この条件下で、すべてのノードに設定されたベクトル値の共分散行列を 2-2 及び 2-3 で述べた手順で計算し、その共分散行列の計算結果よりこれらのベクトル値の第 1 主成分を導出した。図 3 より、本研究課題で開発した分散型データ集計システムを用いることにより、それぞれのノードが持つベクトル値の主成分分析を実施できていることがわかる。これは、2-3 で述べたとおり、分散型データ集計システムがこれらのベクトル値の共分散行列を正確に計算できるためである。

図 4 に分散型データ集計システム用いてデータ集計を行ったときに 1 個のノードで送受信された通信デー

タ量を示す。この実験により、この分散型データ集計システムでは、データ集計を行うために各ノードに必要となる通信データ量は O(log N)であることを確認した。これは、本研究課題で開発した分散型データ集計システムがスケーラビリティに優れたシステムであることを示している。一方、この実験では、この分散型データ集計システムを用いて平均値の計算と主成分分析を実行した。これらの計算に必要となる通信データ量に大きな差は見られなかった。構造化 P2P ネットワークではルーティングテーブルの維持のための多くの通信メッセージを必要する。そのため、データ集計のためのメッセージに比べてルーティングテーブル維持のための通信メッセージが多いため、データ集計の複雑さが変化しても送受信する通信データ量に大きな変化は見られなかったものと考えられる。

2-5 実環境で動作する集計ソフトウェアの実装と検証

実環境における実験を行い、本研究課題で開発した分散型データ集計システムが実際のネットワーク上においても動作することを検証した。この実験では、8 個の Raspberry PI に室温センサを接続し、これらをセンサ端末として動作させた。また、1 個のノート PC を利用者端末とし、この利用者端末から室温センサの観測データの集計要求を発行するようにした。さらに、これらの端末を無線 LAN に接続し、相互に通信可能な状態とした。以上の条件で、室温の平均値の計算を実行し、分散型データ集計システムが実環境において実用的な時間(0.7 秒)以内で室温の平均値を計算できることを確認した。

3 物理的接触に基づいた端末認証手法

3-1 端末認証手法の概要

実環境上に分散型データ集計システムを実現するためには、多くのセンサ端末を複数の場所に設置し、それらのセンサ端末がお互いに通信できる状態に設定する必要がある。一般的に、センサ端末はネットワーク接続以外の入出力装置を持たないため、操作端末を用いてネットワーク経由でセンサ端末の初期設定を行う。操作端末からセンサ端末を操作するためには、センサ端末に接続するための IP アドレスやパスワードなどの情報を操作端末に入力する必要がある。しかし、多数のセンサ端末を設置する場合、個々のセンサ端末に接続するための情報を操作端末に入力する作業が煩雑となる。

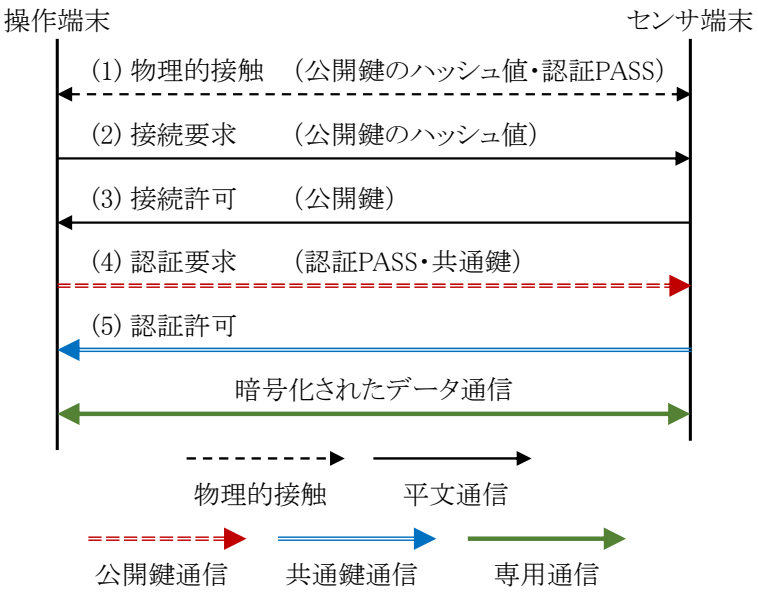

図 5　物理的接触に基づいた端末認証手順

そこで、本研究課題ではこの問題を解決するため、センサ端末と操作端末との物理的な接触に基づく端末認証手法を開発した。この端末認証手法では、センサ端末と操作端末が物理的に交換した情報を用いて相互に認証することにより、IP アドレスやパスワードなどの接続情報を入力していない操作端末からでもセンサ端末に接続できる。また、センサ端末にパスワードなどの認証情報を設定する必要がないため、初期設定を行っていないセンサ端末に対しても操作端末から安全に接続することが可能となる。

図 5 に物理的接触に基づいた端末認証手法の認証手順を示す。この端末認証手法では、センサ端末に接続するために必要となる IP アドレスなどの情報を操作端末に入力していない環境を想定している。そのため、操作端末は、ネットワーク上に存在する複数のセンサ端末の中から、接続対象であるセンサ端末を識別する必要がある。そこで、この端末認証手法では、操作端末がセンサ端末との物理的な接触により接続に必要となる情報を取得し、この情報を用いて接続対象となるセンサ端末を検索する。具体的には、QR コードや NFC などのマーカからセンサ端末の公開鍵のハッシュ値を取得し、IP ブロードキャストや IP マルチキャストを用いて取得したハッシュ値の公開鍵を持つセンサ端末を検索する。また、QR コードや NFC などのマーカから認証パスワードを取得し、公開鍵のハッシュ値と認証パスワードを用いることで操作端末とセンサ端末の相

互認証を実現する。この端末認証手法では、操作端末は公開鍵のハッシュ値を物理的接触によって取得しているため、ネットワーク上の他の端末による公開鍵の改竄やなりすましを防ぐことができる。また、公開化鍵暗号方式を用いて認証 PASS を暗号化するため、認証 PASS の盗聴を防ぐことができる。この端末認証手法を用いることにより、初期状態のセンサ端末に対しても操作端末から簡単かつ安全に接続することが可能となる。また、センサ端末は物理的に接触可能な操作端末にのみ接続許可を与えるため、初期状態のセンサ端末をインターネットに接続したとしても悪意のある利用者にのっとられることはない。

3-2 端末認証手法の認証手順

この端末認証手法では、以下の認証手順を経ることにより、操作端末とセンサ端末が相互に認証する。

（１）物理的接触

操作端末とセンサ端末が物理的に接触することにより、操作端末はセンサ端末に接続するための情報を取得する。具体的には、操作端末は、QR コードや NFC などのマーカから、センサ端末の公開鍵のハッシュ値と認証のためのパスワード（認証 PASS）を取得する。ここでは、それぞれのセンサ端末には個別の公開鍵と認証 PASS が設定されているものとする。これらのデータはセンサ端末が製造されたときに設定された値であり、センサ端末に付属しているQRコードやNFCなどのマーカから読み取ることができる。この端末認証手法では、公開鍵や認証 PASS の情報を用いて操作端末とセンサ端末の相互認証を行う。そのため、公開鍵や認証 PASS が悪意のある利用者に知られるのを防ぐため、これらの値は十分に安全な長さを持つ必要がある。具体的には、公開鍵は 2048 ビット以上、公開鍵のハッシュ値は 256 ビット以上、認証 PASS は 256 ビット以上の長さが必要と考えられる。

（２）接続要求

操作端末は IP ブロードキャストや IP マルチキャストを用いて通信可能なセンサ端末すべてに対して接続要求メッセージを送信する。この接続要求メッセージには、操作端末が物理的接触によって取得したセンサ端末の公開鍵のハッシュ値が含まれている。そこで、このメッセージを受信したセンサ端末では、そのセンサ端末が持つ公開鍵のハッシュ値と接続要求に含まれるハッシュ値を比較し、これらの値を一致した場合のみ操作端末に対して接続許可メッセージを送信する。

（３）接続許可

接続対象となるセンサ端末は、接続要求メッセージに含まれる公開鍵のハッシュ値を確認し、操作端末に対して接続許可メッセージを送信する。この接続許可メッセージにはセンサ端末の公開鍵が含まれている。このメッセージを受信した操作端末では、この公開鍵のハッシュ値と物理的接触によって取得した公開鍵のハッシュ値が同じ値であることを確認する。

（４）認証要求

接続許可メッセージを受信した操作端末はセンサ端末に対して認証要求メッセージを送信する。この認証要求メッセージには、操作端末がセンサ端末との物理的接触により取得した認証 PASS とこのメッセージ以降の通信で使用する共通鍵が含まれている。この認証要求メッセージは接続許可メッセージにより取得した公開鍵を用いて暗号化されているため、接続許可メッセージを送信したセンサ端末だけが認証要求メッセージの内容を復号化できる。このメッセージを受信したセンサ端末はメッセージに含まれる認証 PASS を確認し、正しい認証 PASS を確認できた場合は操作端末に対して接続許可メッセージを送信する。

（５）接続許可

正しい認証 PASS を確認できたセンサ端末は操作端末に対して接続許可メッセージを送信する。この接続許可メッセージには、セッション番号などのデータ通信に必要となる情報が含まれる。センサ端末は、認証要求メッセージによって取得した共通鍵を用いて接続許可メッセージを暗号化するため、操作端末のみが接続許可メッセージを復号化できる。接続許可メッセージの送受信を終えた操作端末とセンサ端末は共通鍵で暗号化したデータの送受信を開始する。

3-3 安全性

この端末認証手法では、すべてのメッセージに対して必要な暗号化や電子署名が用いられている。そのため、以下の通り、悪意のある利用者による盗聴・改竄・なりすましを防ぐことが出来る。

（１）物理的接触の安全性

操作端末はセンサ端末と物理的に接触することにより、認証に必要となる公開鍵のハッシュ値と認証 PASS を取得する。この手順はインターネットなどのコンピュータネットワークを介さず行われるため、悪意のある利用者がネットワークを介して盗聴・改竄・なりすましを行うことはできない。一方、悪意のある利用者

が物理的にセンサ端末に接触することにより、認証のための情報を不正に取得する可能性がある。しかし、悪意のある利用者がセンサ端末に物理的に接触できる場合、いかなる方法を用いてもセンサ端末の安全を確保することはできない。そのため、この端末認証手法では悪意のある利用者がセンサ端末に物理的に接触する状況を想定していない。

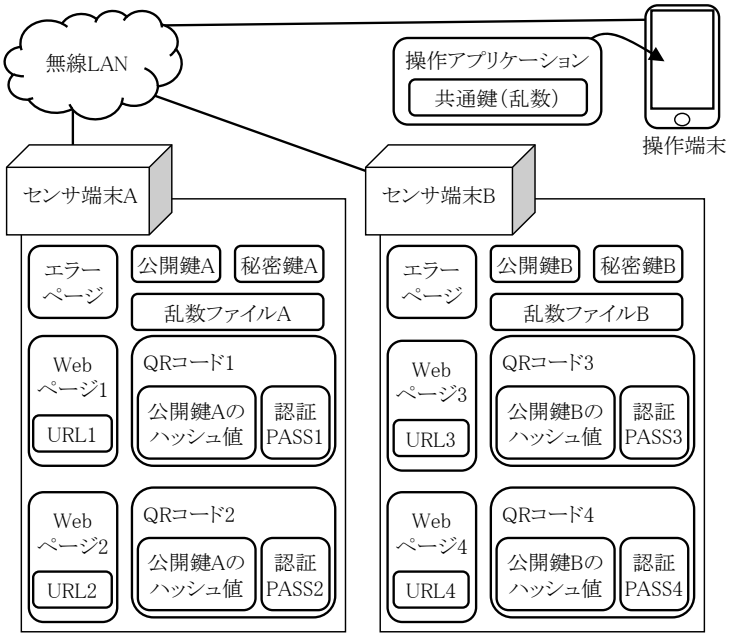

図 6　物理的接触に基づく端末認証のプロトタイプ実装

（２）接続要求の安全性

接続要求メッセージは平文で送信されるため、このメッセージを盗聴することにより公開鍵のハッシュ値を取得できる。そのため、悪意のある利用者が、公開鍵のハッシュ値を用いて操作端末になりすましを行う攻撃が想定される。しかし、操作端末とセンサ端末が相互認証するためには物理的接触によって取得する認証 PASS が必要となる。そのため、悪意のある利用者が操作端末になりすましたとしても、その利用者は認証 PASS を持っていないため、センサ端末が悪意のある利用者を認証することはない。一方、悪意のある利用者が接続要求メッセージを改竄し、意図しないセンサ端末との認証に誘導するという攻撃が想定される。この攻撃の場合、操作端末の接続要求メッセージは意図しないセンサ端末へ送信される。しかし、接続要求メッセージの応答にあたる接続許可メッセージにはセンサ端末の公開鍵が含まれており、操作端末は接続許可メッセージに含まれる公開鍵と物理的接続によって取得した公開鍵のハッシュ値を比べることにより、意図したセンサ端末と通信していることを確認できる。そのため、悪意のある利用者が接続要求メッセージを改竄して意図しないセンサ端末に通信を誘導したしても、操作端末はその改竄を検知することが可能である。

（３）接続許可の安全性

接続許可メッセージは平文で送信されるため、悪意のある利用者によって改竄やなりすましによる攻撃が想定される。しかし、操作端末は物理的接触によってセンサ端末の公開鍵のハッシュ値を取得しているため、悪意のある利用者により接続許可メッセージの改竄やなりすましが行われたとしても、そのメッセージに含まれる公開鍵が意図したセンサ端末の公開鍵でないことを検知することが可能である。

（４）認証要求の安全性

操作端末が送信する認証要求メッセージはセンサ端末の公開鍵を用いて暗号化されるため、秘密鍵を持つセンサ端末だけが認証要求メッセージを復号化できる。そのため、ネットワーク上に悪意のある利用者がいたとしても、認証要求メッセージの盗聴・改竄・なりすましのいずれも実行不可能である。

（５）接続許可の安全性

センサ端末が送信する接続許可メッセージは認証要求メッセージによって共有された共通鍵によって暗号化されるため、共通鍵を持っている操作端末とセンサ端末だけが接続許可メッセージを復号化できる。そのため、ネットワーク上に悪意のある利用者がいたとしても、接続許可メッセージの盗聴・改竄・なりすましのいずれも実行不可能である。

3-4 実装

この端末認証手法の実現可能性を検証するため、この端末認証手法を導入したセンサ端末と操作端末のプロトタイプを実装した。図 6 にプロトタイプ実装の概要を示す。このプロトタイプでは、Raspbian Stretch 搭載の Raspberry Pi 3 をセンサ端末とし、Android 6.0 搭載のスマートフォンを操作端末とした。センサ端末によって観測されたデータはコンピュータネットワークを介して Web ページとして取得できるが、それぞれの Web ページにはアクセス制限が設定されており、物理的接触に基づく端末認証を経ることでこれらの Web ページを取得できるように実装した。また、それぞれのセンサ端末には QR コードが印刷されており、これらの QR コードを読み込むことによりセンサ端末の公開鍵のハッシュ値と認証 PASS を取得できる。操作端末と

センサ端末は同一の無線 LAN に接続しており、IP アドレスは DHCP により自動的に割り当てられている。ただし､操作端末とセンサ端末にはお互いの IP アドレスや接続されている端末の数などの認証のための設定は一切行われてない。このプロトタイプ実装を用いて、物理的接触に基づく端末認証手法の実験を行い、この端末認証手法が実現可能であることを確認した。また、物理的接触が発生してから認証が完了するまでの時間を計測し、QR コードの画像認識を含めて 2 秒以内に認証を完了できることを確認した。

4 まとめ

本研究課題では、構造化 P2P ネットワークを用いた分散型データ集計システムの設計、及び、このデータ集計システムを用いた主成分分析や線形回帰分析などの統計分析手法を論文としてまとめ、ネットワークソフトウェアに関する国際会議 NBiS-2017 においてこの研究成果を発表した。また、物理的接触を根拠とした端末認証手法については、その認証手順と安全性を研究報告としてまとめ、国内の研究会である MBL 研究会（情報処理学会）においてその研究成果を発表した。以上の通り、本研究課題では、構造化 P2P ネットワークと加法準同型暗号を用いたセキュアでスケーラブルな分散型データ集計システムの実現を達成し、その研究成果を国内外に向けて発信した。そのため、本研究課題は研究目標を概ね達成できたと評価できる。

【参考文献】

[1] Takeda, A., Oide, T., Takahashi, A., Suganuma, T.: Accurate Data Aggregation on Unstable Structured P2P Network, Proceedings of the 29th IEEE International Conference on Advanced Information Networking and Applications, 542–549 (2015).

[2] 生出拓馬, 武田敦志, 高橋晶子, 菅沼拓夫: ネットワークアウェアな P2P 型安否情報共有システムの提案. 情報処理学会論文誌, vol.55, no.2, 607–618, (2014).

[3] Macua, S.V., Belanovic, P., Zazo, S.: Consensus-based distributed principal component analysis in wireless sensor networks. Proceedings of the 11th International Workshop on Signal Processing Advances in Wireless Communications (2010)

[4] Liang, Y., Balcan, M.F.F., Kanchanapally, V., Woodruff, D.: Improved distributed principal component analysis. Advances in Neural Information Processing Systems 27, 3113–3121 (2014)

[5] Alsheikh, M.A., Lin, S., Niyato, D., Tan, H.P.: Machine learning in wireless sensor networks: Algorithms, strategies, and applications. IEEE Communications Surveys & Tutorials 16(4), 1996–2018 (2014)

[6] Shafaat, T.M., Ghodsi, A., Haridi, S.: A practical approach to network size estimation for structured overlays. Lecture Notes in Computer Science 5343, 71–83 (2008)

[7] Graffi, K., Stingl, D., Rueckert, J., Kovacevic, A., Steinmetz, R.: Monitoring and management of structured peer-to-peer systems. Proceedings of the 9th International Conference on Peer-to-Peer Computing (P2P '09), 311–320 (2009)

[8] Schulz, S., Blochinger, W., Hannak, H.: Capability-aware information aggregation in peer-to-peer grids. Journal of Grid Computing 7(2), 135–167 (2009)

[9] Abe, K., Abe, T., Ueda, T., Ishibashi, H., Matsuura, T.: Aggregation skip graph: A skip graph extension for efficient aggregation query over p2p networks. International Journal On Ad-vances in Internet Technology 4(3), 103–110 (2012)

[10] Stoica, I., Morris, R., Liben-Nowell, D., Karger, D.R., Kaashoek, M.F., Dabek, F., Balakrishnan, H.: Chord: A scalable peer-to-peer lookup protocol for internet applications. IEEE/ACM Transactions on Networking 11(1), 17–32 (2003)

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Scalable Distributed Data Analysis on Structured P2P Network	Proceedings of the 20th International Conference on Network-Based Information Systems (NBiS2017), Springer	2017 年 8 月
物理的接触を根拠とした IoT デバイスのためのアクセス制御手法	研究報告モバイルコンピューティングとパーベイシブシステム（MBL），vol.2017-MBL-85，no.24	2017 年 11 月