複数の閉域 LTE 網を用いた IoT のための秘密分散情報収集法の提案

出木原　裕　順

（受付　2019 年 5 月 31 日）

1. は　じ　め　に

近年，第四次産業革命という言葉に象徴されるように情報処理技術の発展が著しい［1, 2］。特に，人工知能（AI）や IoT（Internet of Things），ビッグデータ，ロボティクスなどの分野は第四次産業革命のコア技術として注目さている。日本では，政府が策定した第 5 期科学技術基本計画［3］の中で，これらのコア技術を用いることで「サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより，経済発展と社会的課題の解決を両立する，人間中心の社会（Society）」を目指し，新たな社会（Society5.0）の実現を提唱している［4］。Society 5.0で提唱されているような超高度情報化社会，すなわち人間の社会生活をデータ化して分析し，高度なサービスを実世界で提供するようなサイバーフィジカルシステムが発達した社会では，情報セキュリティの重要性は更に増すばかりである。しかしながら，情報セキュリティが重要視されているにもかかわらず人為的ミスによる情報漏洩が後を絶たない［5］。本研究では，IoT 分野において，生体情報やライフログなどの個人情報やプライバシー情報を収集するセンサネットワークのために，センサで取得した情報をシステムにデータとして入力してから出力されるまでのすべての工程において秘密分散法［6, 7］を用いて情報を秘匿する情報秘匿システムの開発を最終的な目標としている。その目標に向かって，本研究では研究の第一段階として，センサから取得した情報を秘密分散として複数の閉域 LTE 網を用いて分散処理する入力プロセスの構築を目的としている。

2. IoT とセキュリティ

本章では，IoT の概要，IoT のセキュリティおよび情報漏洩の現状について述べる。

2.1 IoT の概要

IoT（Internet of Things）とは「もののインターネット」を意味し，第四次産業革命のコ

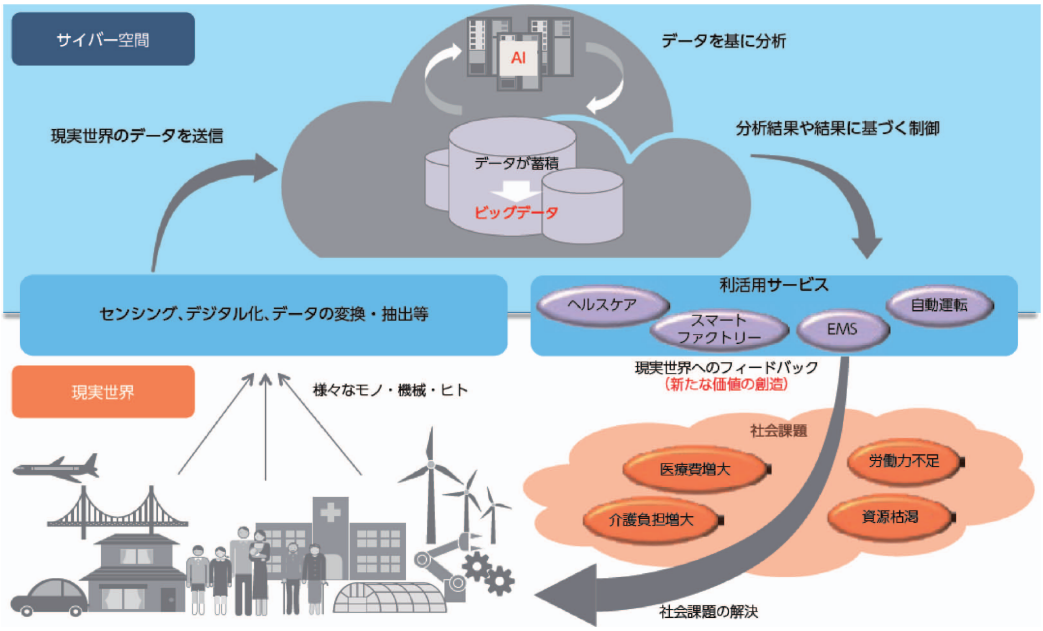


図 1　IoT・ビッグデータ・AI が創造する新たな価値
2016年版情報通信白書（総務省）より

ア技術の 1 つとして注目されており，現実世界と仮想空間をつなぐ架け橋を担っている。2016年版情報通信白書では，第四次産業革命のコア技術として挙げられる技術を一体的に捉えることで，“IoT で様々なデータを収集して「現状の見える化」を図り，各種データを多面的かつ時系列で蓄積（ビッグデータ化）し，これらの膨大なデータについて人工知能（AI）を活用しながら処理・分析等を行うことで将来を予測する”という関係を「広義の IoT」として述べている。その関係性を図式化したものを図 1 に示す。このような現実世界とサイバー空間を接続した情報システムのことをサイバーフィジカルシステム（Cyber Physical System: CPS）と呼ぶ。IoT は CPS において現実世界の情報を収集する部分と共に，サイバー空間からのフィードバックを現実空間に伝送する部分を主に担っていると言える。

2.2　IoT のセキュリティ

CPS 内で情報を伝達する役割を担う IoT は当然のことながら情報の安全性が強く求められる。日本では，経済産業省と総務省の主導のもと「IoT 特有の性質とセキュリティ対策の必要性を踏まえて，IoT 機器やシステム，サービスについて，その関係者がセキュリティ確保等の観点から求められる基本的な取組を，セキュリティ・バイ・デザインを基本原則としつつ明確化」すると共に，「産業界による積極的な開発等の取組を促すとともに，利用者が安心

して IoT 機器やシステム，サービスを利用できる環境を生み出すことにつなげること」を目的として，IoT セキュリティガイドラインが策定された［6］。そのガイドラインでは，IoT の性質を考慮した基本方針や，IoT のリスクの認識，守るべきものを守る設計，ネットワーク上での対策，安全安心な状態を維持し情報発信および共有を行う運用・保守，一般利用者のためのルールなどについて記述されている。他方，従来のセキュリティ技術はもとより，ビットコイン［7］に利用されているブロックチェーンといった新しいセキュリティ技術を IoT に応用する研究があるように［8, 9］，IoT のセキュリティは重要な課題の一つである。

2.3　情報漏洩の現状

日本ネットワークセキュリティ協会の調査では，人為的ミスによる情報漏洩が後を絶たない。日本ネットワークセキュリティ協会の2017年の調査結果を図 2 と図 3 に示す。図 2 は2017年の個人情報漏洩の概要であり，図 3 は漏洩の原因を示した円グラフである。これらの調査結果が示すように，情報漏洩の件数はまだまだ多く，またその多くが人的ミスに起因するものが多いことが分かる。そこで，本研究では，人為的ミスによる情報漏洩や内部要因による不正アクセスなどが発生した場合においても情報を秘匿することが可能な情報秘匿システムを新しく提案すると共に，その開発を研究の最終的な目標としている。本研究では研究の第一段階として，センサから取得した情報を秘密分散として複数の閉域 LTE 網を用いて分散処理する入力プロセスの構築を目的とする。

漏えい人数	519 万 8,142 人
インシデント件数	386 件
想定損害賠償総額	1,914 億 2,742 万円
一件当たりの平均漏えい人数	1 万 4,894 人
一件当たり平均損害賠償額	5 億 4,850 万円
一人当たり平均損害賠償額	2 万 3,601 円

図 2　個人情報漏洩インシデントの概要
2017年　情報セキュリティインシデントに関する調査報告書【速報版】より

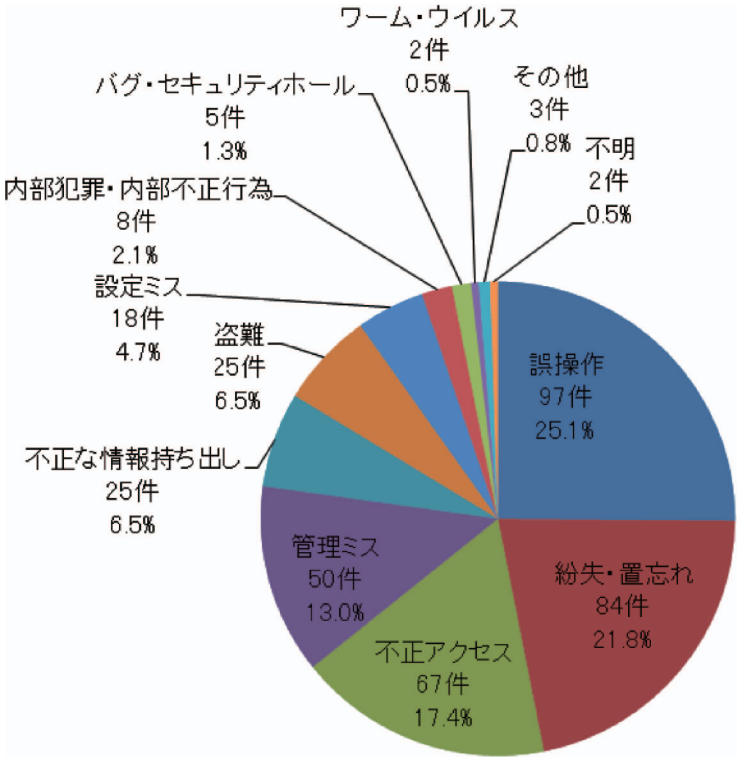


図 3　個人情報漏洩の原因
2017年　情報セキュリティインシデントに関する調査報告書【速報版】より

3. 提　　案　　法

本章では，提案法の概要，IoT のデバイスおよび秘密分散法について述べる。

3.1　提案法の概要

本研究で提案する情報秘匿システムは，IoT で実世界をセンシングして情報を収集し，集めた情報をクラウドコンピューティングなどのインターネット上の仮想空間に蓄積してビックデータ化し，そのビッグデータを AI などで分析して現実世界にフィードバックするサイバーフィジカルシステム（CPS）の一種である。提案する情報システムのデータの流れ図を図 4 に示し，その概要を図 5 に示す。図 4 は図 1 を簡略化したものであり，本研究では IoT でセンシングした情報をインターネットに伝達する部分の手法を提案している。また，提案法では，図 5 に示すように，複数の伝達経路を使ってデータをインターネットに運搬し，インターネット上の複数のクラウドコンピューティング上に分散して蓄積される。そして主キー

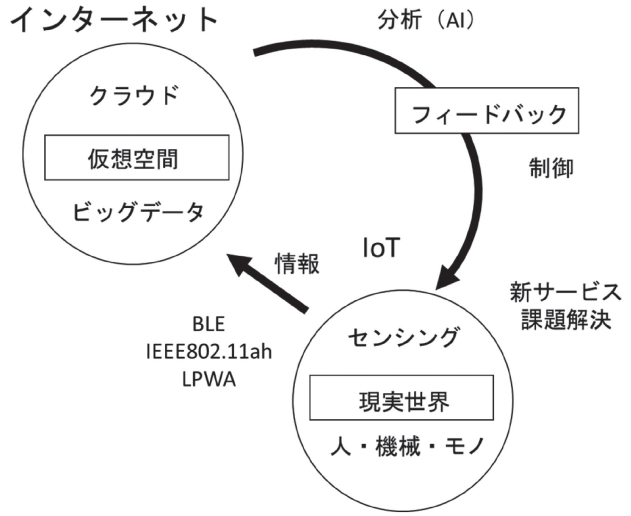


図 4　CPS におけるデータの流れ

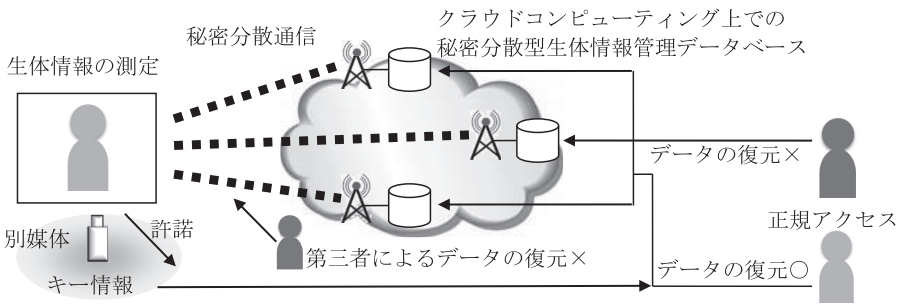
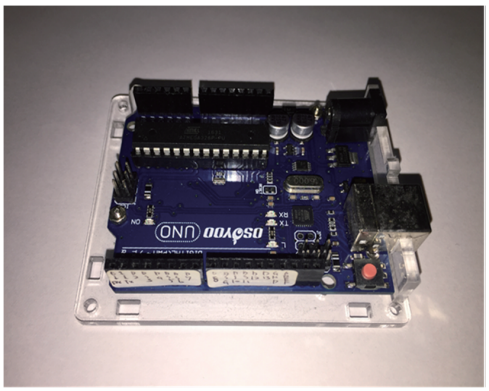


図 5　提案する情システムの概要

となるデータを本人もしくは第三者機関が管理することにより，悪意ある第三者のような情報システムの外部要因はもとより，人為的ミスといった情報システムの内部要因に起因するインシデントにも本人もしくは第三者機関の許諾がなければアクセスできないような情報秘匿システムの開発を目指している。

3.2　IoT のデバイス

本研究では，IoT デバイスとして Arduino［10］を利用し，通信モジュールとしてさくらインターネットの sakura.io モジュール［11］を採用した。Arduino は，一枚のプリント基盤の上に電子部品と入出力がついたマイクロコンピュータであり，センサやモジュールを接続し，C++ のようなプログラミング言語で制御することができる（図 6（a）参照）。また，



(a) Arduino

(b) sakura.io モジュール

図 6　Arduino と sakura.io モジュールのデバイス

sakura.io モジュールは，Arduino や Raspberry Pi に装着可能な通信モジュールである（図 6（b）参照)。LTE 通信を用いた閉域網を使ってデータをインターネット上のクラウドコンピューティングであるさくらインターネットデータセンタにデータを蓄積できると共に，外部サービスとの連携も可能である。

3.3　秘密分散法に基づいた秘匿情報の分散管理

本研究では，人為的ミスや不正アクセスなどで一部のデータが漏洩したとしても情報が守られる情報秘匿システムを実現するために，秘密分散法［12, 13］を採用した。秘密分散法は暗号化方式の一種で，(k, n) しきい値法とも呼ばれている。ある秘密情報 s を暗号化する場合，定数項が s となる $k-1$ 次多項式 $f(x)$ を用意する。次に，$f(x_i)$ のグラフ上を通る点 $(x_i, f(x_i))$ $(i = 1, 2, \cdots, n)$ を導出し，それぞれの点情報をシェアとする。このシェアが暗号化されたデータ群となり，通常分散して保持する。逆に，シェアから秘密情報 s を復号したい場合は，k 個以上のシェアから $f(x)$ を導出する。この $f(x)$ の導出過程で求められる定数項が復号したい秘密情報 s と同値となる。秘密分散法を採用した提案法の手順の大まかな流れを以下に示す。

①取得した情報に秘密分散法を適用してデータを分割（暗号化）
②復元のキー情報はユーザ（第三者機関等）が管理
③分割したデータを複数の経路で伝達
④クラウドコンピュータ上にデータを分散して蓄積
⑤キー情報とクラウド上のデータを用いて情報を復元（復号）

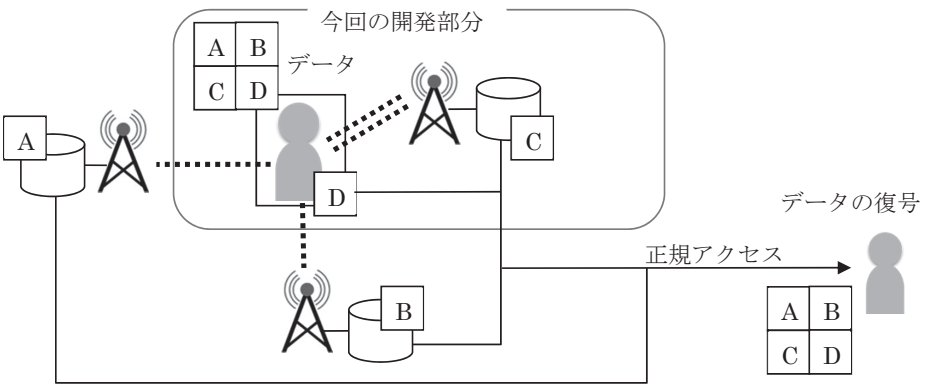
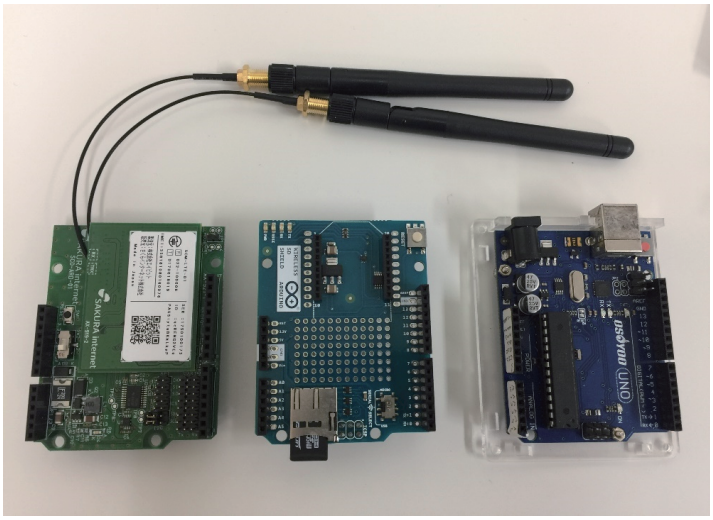


図 7　提案法の全体像における本研究の開発部分

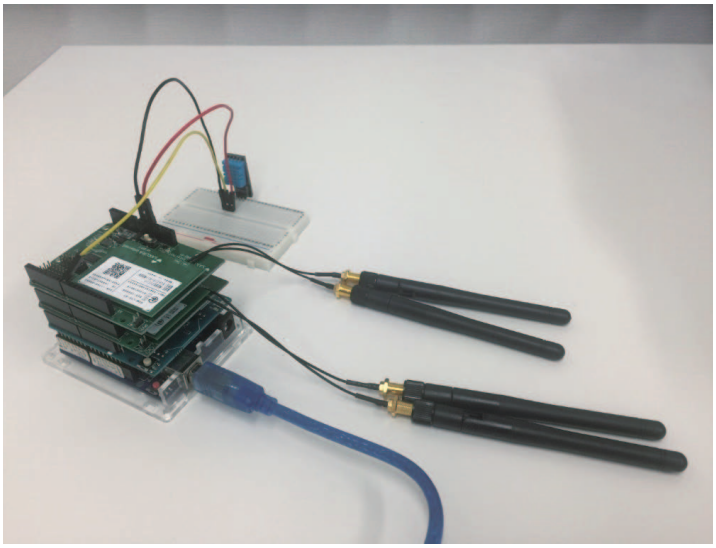
提案法では，IoT のデバイスが取得したデータを秘密分散法のアルゴリズムを使って暗号化（分割）して分散させ，分散させたデータを複数の経路を使ってインターネットなどのネットワーク上に分散させて蓄積させる。この過程の中で，キーとなる情報をユーザ自身が保持したり第三者に委託管理させたりすることができる。これにより，正規アクセス時のみ閲覧を許可するなどの処理が可能となる。提案法の全体像における本研究の開発部分を図 7 に示す。

4. 実　装　実　験

本研究では研究の第一段階として，提案手法の試験的な実装実験を行った。IoT デバイスで収集したセンサデータを複数の閉域 LTE 通信経路を使って，ユーザ自身とクラウド上にデータを分割するシステムを構築した。実験用の IoT デバイスとして，Arduino UNO rev.3 と完全互換の Osoyoo UNO Borad（図 8（a）右参照），sakura.io モジュール（LTE）と sakura.io シールド for Arduino（図 8（a）左参照），Arduino ワイヤレス SD シールドを使用した（図 8（a）中央参照）。また，センサには温湿度センサモジュール（DHT11）を使用した。実装時には，Arduino に各ボード類を装着し，ジャンパーワイヤでセンサと接続した。なお，複数経路を実現するために sakura.io モジュールは 2 つ使用した（図 8（b）参照）。取得したデータは，ユーザ管理用の分割データは microSD カードに蓄積し，その他のデータは sakura.io の IoT プラットフォーム上に蓄積できることが確認できた。



(a) IoT デバイス機器



(b) センシングの外観

図 8　実装した IoT デバイス

5. お　わ　り　に

本研究では，IoT のための情報秘匿システムの開発に向けて，その第一段階として，IoT デバイスで取得したデータをユーザ自身とクラウドコンピューティング上に分散させて蓄積す

るシステムを開発した。具体的には，ユーザは IoT デバイスに装着した SD カードにデータを蓄積し，その他のデータはさくらの IoT プラットフォームに複数の閉域 LTE 網の経路を使って伝達させて蓄積した。今後の課題としては，IoT デバイスから異なる複数の経路を使った物理レイヤでの秘密分散通信の実現やデータの秘密分散演算処理法，データの閲覧処理法の開発などが挙げられる。これらが実現できれば，情報システムの中のほぼすべての工程で情報が秘密分散法に基づいて分散処理されるため，万が一どこかの工程でデータの一部が漏洩したとしても情報を復元することが困難であることから，情報が完全に秘匿される完全型情報秘匿システムの実現が期待できる。

謝　　辞

本研究の一部は，広島修道大学ひろしま未来協創センター2018年度調査研究費（ひろみら特別研究）の助成を受けたものである。

参 考 文 献

［1］ クラウス・シュワブ（著），世界経済フォーラム（翻訳），第四次産業革命：ダボス会議が予測する未来，日本経済新聞出版社，2016.
［2］ クラウス・シュワブ（著），小川敏子（翻訳），「第四次産業革命」を生き抜く ダボス会議が予測する混乱とチャンス，日本経済新聞出版社，2019.
［3］ 内閣府，第 5 期科学技術基本計画，2016.
［4］ 内閣府 Society 5.0
https://www8.cao.go.jp/cstp/society5_0/index.html（2019.05.31閲覧）
［5］ JNSA セキュリティ被害調査ワーキンググループ，2017年情報セキュリティインシデントに関する調査報告書【速報版】，日本ネットワークセキュリティ協会，2018年.
https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_ver1.1.pdf（2019.05.21閲覧）
［6］ IoT 推進コンソーシアム，総務省，経済産業省，IoT セキュリティガイドライン ver1.0，2016.
https://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf（2019.05.31閲覧）
［7］ Satoshi Nakamoto，Bitcoin: A Peer-to-Peer Electronic Cash System, The Bitcoin Foundation.
https://bitcoin.org/bitcoin.pdf（2019.05.31閲覧）
［8］ M. Samaniego and R. Deters, Blockchain as a Service for IoT, Proc. of IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, pp. 433–436, 2016.
［9］ Dorri, Ali, Kanhere, Salil, Jurdak, Raja, Gauravaram, Praveen, Blockchain for IoT Security and Privacy: The Case Study of a Smart Home., Proc. of IEEE PerCom workshop on security privacy and trust in the Internet of Thing, 10.1109/PERCOMW.2017.7917634, 2017.
［10］ Arduino
https://www.arduino.cc/（2019.1.11閲覧）
［11］ sakura.io
https://sakura.io/（2019.1.11閲覧）
［12］ G. R. Blakley: “Safeguarding cryptogra-phic keys”, Proc. of the National Computer Confer-ence, Vol. 48, pp. 313–317, 1979.
［13］ A. Shamir, How to share a secret, Communications of the ACM, Vol. 22, No. 11, pp. 612–613, 1979.