5E-01

秘密分散法を用いた情報秘匿システムの開発

出木原　裕順†
広島修道大学†

１．はじめに

近年，IoT（Internet of Things）によって現実世界の情報を取得して新しいサービスや製品を生み出すことが注目されている．他方，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[1]．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[2, 3]を用いて情報を秘匿する情報秘匿システムの開発を目的としている．本稿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分散処理する入力プロセスを Arduino と sakura.io モジュールを用いて構築した．

２．IoT

IoT は第四次産業革命のコア技術の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である．本研究では，IoT は実世界をセンシングして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情報を蓄積してビックデータ化する情報システムと定義している（図１参照）．

本稿では，IoT デバイスとして Arduino[4]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[5]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 2(a)参照）．また，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 2(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ー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．

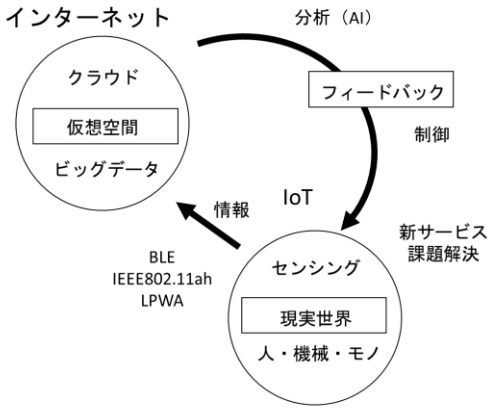


図１ IoT による現実世界と仮想空間の接続

(a)Arduino　(b)sakura.io モジュール

図２　Arduino と sakura.io モジュール

３．提案法

本研究では，IoT のデバイスが取得したデータを秘密分散を使って分割し，分散処理することでヒューマンエラー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の開発を目的としている．図 3 に提案法の全体像と本稿で構築した開発部分を示す．提案法では，センシングによって取得した情報を秘密分散で複数のデータに分割し，それらの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．そのうち，キーとなる情報をユーザ自身が保持することができる。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も可能になる．

Development of Secure Information System using Secret Sharing
†Hiroyuki Dekihara・Hiroshima Shudo University

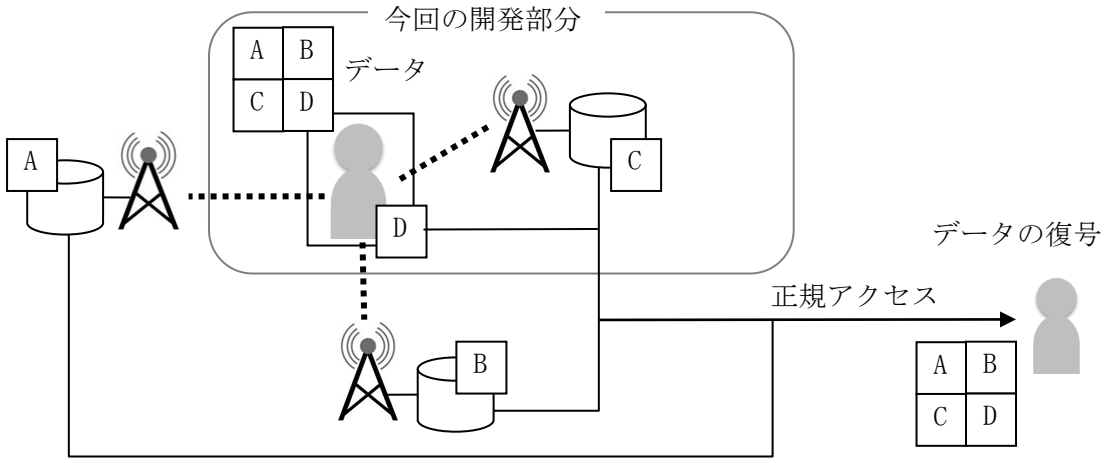
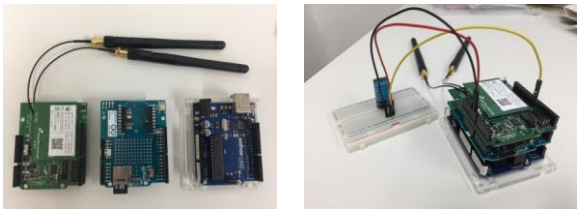


図３　提案法の全体像と今回の開発部分

４．実装実験

本稿では，研究の第一段階として，IoT デバイスと単一の通信経路上で，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 4(a)右参照），sakura.io モジュール(LTE)と sakura.io シールド for Arduino（図 4(a)左参照），Arduino ワイヤレス SD シールドを使用した（図 4(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．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（図 4(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した．



(a)IoT デバイス機器　(b)センシングの外観

図４　実験用 IoT デバイス

５．おわりに

本稿では，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蓄積した．今後の課題としては，IoT デバイスから複数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としての運用が期待できる．

参考文献

[1]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
（2019.1.11 閲覧）

[2]G. R. Blakley: “Safeguarding cryptographic keys”, Proc. of the National Computer Confer-ence, Vol.48, pp.313-317, 1979.

[3]A. Shamir , How to share a secret, Communications of the ACM, Vol.22, No.11, pp.612-613, 1979.

[4]Arduino
https://www.arduino.cc/ (2019.1.11 閲覧)

[5]sakura.io
https://sakura.io/ (2019.1.11 閲覧)