クラウドとIoTセンサを用いた不具合の原因特定

高橋 建一 [1,a)]　串田 高幸[1]

概要：設置された機器などが正常に動作しないことや原因不明のエラーなどで止まってしまうことが問題の背景である．この論文ではクラウドと IoT センサを用いて不具合の原因特定及び検知の提案をする．壊れてほしくない機器に監視用 IoT センサを設置し異常が無いか監視すること，また，不具合が起きた際の原因特定をこの監視用 IoT センサで判明しようというのが目的である．異常を検知できる方法として基準となる閾値を設定して異常検知する手法を用いる．過去のデータを参考に閾値を設定することで過去に取ったデータの範囲内を超えるものなら異常を検知できるが，極端に範囲内を超えるものに関しては対応できないという評価がある．この論文では閾値に決め方及び手法について考察し述べるものとする．

1. はじめに

現在の IoT は社会基盤や生活基盤に着実に浸透している [1]．情報通信業界をはじめ，製造，インフラ業界でその価値は高まっている．IoT に欠かすことのできないセンサーは同様にその価値を高めている．IoT の歴史は古く，その概念は 1990 年から知られている [2]．IoT の進化によって実現不可能だったものが可能になっていき人々の生活に欠かせないものとなっていった．例えるなら顧客先に設置した自社製品を今までは営業が見回って動作点検していた作業が IoT 化によって製品自体がデータを発信することによって情報のリアルタイム性が実現可能である．しかし，IoT には問題がある．それは設置した IoT 機器が確実に動作する保証が無いことだ．仮に設置した IoT 機器が動作したとしても継続的に動いてくれる保証は無い．いつ壊れるかわからない IoT 機器に対して管理体系，監視体制が必要になるという問題点が存在する．この論文では既存の管理体系，監視手法について調査し，新規に提案する監視手法との比較や相違点などを挙げて優位性があるかどうかの提案を行うものとする，この論文の 2 章は関連研究とこの論文との比較や違いを挙げる．3 章では提案内容についての説明する．4 章では実験方法についての説明をする．また，この論文では IoT とセンサを組み合わせたものを総じて IoT センサと呼ぶこととする．

2. 関連研究

異常検知の方法の 1 つにネットワークログ分析による異常検知がある [3]．これはネットワークのログ情報の分析を行い，攻撃の兆候やインシデントの調査を体系的に行える手法を提案する研究である．この方法ではネットワークの異常を検知することはできるが機器の物理的な異常や不具合を検知することはできない．この論文で提案する IoT センサを用いた不具合を検知する手法はネットワークではなくセンサを用いて検知するものである．よって，ネットワークとセンサという違いがわかる．

別の異常検知を検知する方法ではシステムの異常予兆を検知する方法がある [4]．これは機械学習によって正常時のデータを学習し，いつもと違う状態を自動的に検知するというソリューションである．この論文で提案する手法と比較すると異常予兆を検知はできるがその原因までは特定できてはいない．よって不具合を特定できるかどうかの違いがでてくる．

別の研究では IoT デバイスとクラウド環境を使用した障害検出のフレームワークがある [5]．これは IoT に組み込まれているクラウドコントロールアーキテクチャを利用した障害検出である．深層学習ベースの分析を用いて，障害検出分類を分析する．この方法との違いは IoT センサを使用しているかどうかである．IoT センサを用いたほうが物理的な不具合を検知するという面ではアプローチの方法が違うと言える．

監視手法とは別にセンサの管理手法についての研究がある．クラウドおよび霧上のセンサデータの管理方法である [6]．センサデータを高速かつ効率的に送信することができるクラウドを用いている. データを高速収集できる状態でのパフォーマンス調査について研究されている．センサの管理という面では不具合検知のシステムの状態管理に

[1] 東京工科大学コンピュータサイエンス学部
CDSL, TUT, Hachiouji, Tokyo 101–0062, Japan
[a)] C0117183

繋がる部分がある．同じ異常検知の類だがこの論文ではセンサを用いて異常検知を行うが霧上のセンサデータについては行わないという違いがある．

別の研究では安全な IoT デバイスがある．IoT デバイスの安全性やセキュリティについて考慮した安全設計についての研究である [7]．IoT デバイスやセンサの安全設計においてこの論文では不具合検知を用いて IoT デバイスの安全を保っている．

IoT 系の異常検知の中でも悪意のあるトラフィックの検知というものがある．その中の 1 つに 2 層次元削減および 2 層分類モデルの研究である [8]．これはユーザーからルート攻撃やリモートからローカル攻撃などの悪意のあるアクティビティを検出するように設計された，2 層の次元削減と 2 層分類モジュールに基づく侵入検知である．つまり，疑わしい動作を識別するために 2 層分類モジュールを使用するのである．この論文で提案する内容と比較すると自然的異常か故意の異常かどうか検知の違いがわかる．

IoT の異常検知に関してはネットワークだけでなく医療に関する異常検知の研究がある．医療の現場においての異常検出の重要性を研究した論文である [9]．この研究は IoT により医療データの分析を行うことでヘルスケアの分野で優れた進歩をもたらす研究を行っている. 特に心臓病の予防に特化した研究を行っており，心臓の異常検出は IoT によって手ごろに検出できるということを研究で行っている．この論文との分野は違えど行っていることは異常検知と変わりない．しかし，異常検知の対象が IoT 機器の異常か心臓の異常かの違いがある．

異常検出の軽量化という研究がある [10]．これはリソースに限りのある IoT デバイスにおいて正常なペイロードと異常なペイロードを適切に区別する研究である．また，異常検知に関しては軽量にすることでどの IoT デバイスにも実装が可能という利点がある．そのための効率的な演算や方法に関する研究を行っている．IoT デバイスとセンサを組み合わせたこの論文との研究は近い関係性があるが，異常検知のアプローチに違いがある．

IoT 向けの分散内部異常検出システムとう研究がある [11]．これは各ノードが隣接ノードを監視し，異常な動作が検出された場合に親ノードに報告するシステムである．この論文の研究と比較してノードの数の違いが挙げられる．この論文ではノードに当たるのは異常検知を行うセンサなどが当たる．ノードの数が少ないことは報告が早く遅延が少ないという利点であると言える．ノードという点では関係性があるが，異常検知の手法にはセンサを用いるかノードを複数用意するかの違いがある．

別の研究では超楕円体クラスタリングを使用したフォグ強化異常検出というのがある [12]．これはフォグコンピューティングを活用し，異常なパターンを正確かつタイムリーに検出することを行っている．また，集中型および分散型の異常検出方法の使用にたいして重大な遅延とエネルギー消費の問題を提唱している．集中型の代わりとして超楕円体クラスタリングアルゴリズムを使用することで新しい異常検出方法を提案する研究である. この論文で用いる手法は主に集中型を採用しており 1 つのコンピュータに依存している状態である．

低リソース IoT デバイス向けの軽量異常検出技術の研究がある [13]．これはリソースに制約のある小さなセンサやデバイスが取得するデータの保護を目的とする研究である．従来の検出手法やアルゴリズムを活用するとリソースの少ない IoT デバイスの負荷が多くなると懸念されている．この研究ではゲーム理論を用いることで低リソースのデバイスでも異常検出アプローチが出来るとて案されている．この論文で採用している IoT デバイスは Raspberry Pi Zero であることから低リソースのデバイスという点で関係する部分がある．

別の研究ではアルゴリズムによる行動ベースの異常検知という研究がある [14]．これはシミュレーションを使い行動モデリング侵入検知システムを使用して，スマートホームと周囲の環境を監視する研究である．抽出した行動パターンが目的の行動に一致するのか，目的の行動から逸脱した動きを示すのか区別する．この論文との違いとして異常検知の判断基準が違うと言える．この論文では閾値を設けて異常判断を行うが，これは行動モデリングを採用している．

最後にクラウド中心の IoT で異常検出とプライバシー保護の研究がある [15]．これは IoT から収集されたデータをクラウドにアップロードされた後，適切なセキュリティとプライバシー保護を行われなければ攻撃を受けやすくなる問題を提唱している．また，IoT から送られる膨大な量のデータから外れ値を引き出すことを課題として提唱している．この論文では外れ値を引き出す基準に閾値を採用している．閾値を超えたものを異常として捉えるが異常ではないデータにつていの取り扱い方に関してはサーバにデータを集約する．データの取り扱い方に違いがあるが，異常検知という分野では関係性がある．

3. 提案

この論文の研究テーマはクラウドと IoT センサを用いた不具合の原因特定の提案である．設置した IoT 機器には故障の可能性，不具合の可能性が潜んでいる．いつ壊れるかわからない IoT 機器に対しては不具合を検知するシステムや手法が必要である．提案内容としては壊れてほしくない IoT 機器に対して IoT センサを設置し予め決めておいた閾値を超える数値が出たら異常と判定し検知を知らせるという方法である．そしてこれは，物理的な事象に対して有効的であると考えられる．図 1 にその構成図を示す．提案内容の具体的なステップについて述べる． 1 番目に監視した

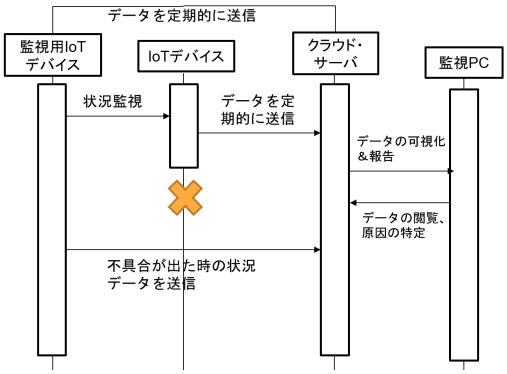

図 1　全体の構成図

```
aiueo = (temp / 16.0)
if(23¡aiueo):
   print(”Temperature:%6.2f” % aiueo),
   print(now),
(”danger too hot”)
elif(17¿aiueo):
   print(”Temperature:%6.2f” % aiueo),
   print(now),
(”danger too cold”)
if(23¡aiueo):
   print(”Temperature:%6.2f” % aiueo),
   print(now),
```

図 2　実装内容

い IoT 機器にこのレポートで提案する監視用 IoT センサを設置する．２番目に IoT 機器が故障した場合その検知を監視用 IoT センサが行う．３番目に故障時の情報をクラウドサーバに送信する．４番目にクラウドサーバから監視用 PC に報告を行う．５番目に管理者は故障時のデータを見て原因を特定する．以上の流れである．２番目と３番目の流れでは故障時の時だけでなく普段の挙動のデータを取ることになる．あらかじめ閾値を設けることで IoT 機器の怪しい挙動や動作をキャッチする為である．

4.　実装

この論文の研究で実装した部分を紹介する．この研究で使用する道具は raspberrypi zero，温度センサ (adt7410)，PC である．これらを用いて不具合検知の実装を行う．Raspberry Pi Zero を使うのは OS をインストールしてその上で Python やセンサをデプロイするのに適したコンピュータであることから使用する．数あるセンサの中から温度センサ (adt7410) を使うのはデータを取るのが単純で結果を簡潔に表すからである．センサを取り扱う上で取ったデータの最低限の理解が必要であることから，身近な温度についてデータを取ることに適する温度センサ (adt7410) を今回の研究で用いる．また，異常検知の方法は他のセンサに取り換えても遜色無いものとする．実装ではある一定の閾値を超えるとコメントで知らせるプログラムを制作した．Python で実装を行い，Raspberry Pi Zero 上でそれを実行している．実装した部分を図の 2 に示す．

閾値の変数は aiueo とする．閾値は上限 23 度，下限 17 度とした．このプログラムを実行すると温度センサが周囲の温度を把握し現在の気温を数値化する．数値が 23 度を超えるなら気温と取得した日時と”danger too hot”というコメントが出る．数値が 17 度を下回るなら気温と取得した日時と”danger too cold”というコメントが出る．もし，上限と下限の範囲内の数値ならば気温と取得した日時が表示される．以上が実装の紹介である．

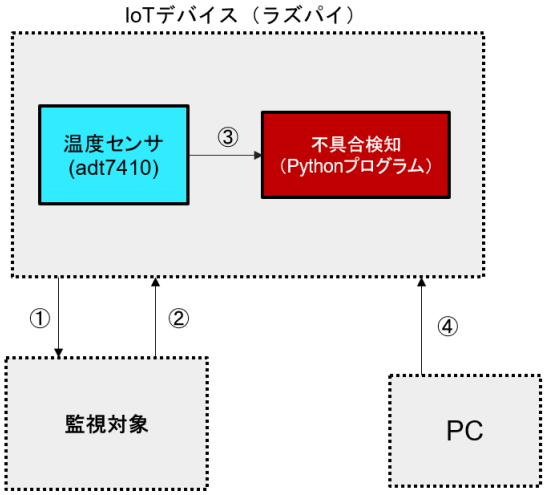

図 3　ソフトウェア構成図

5.　実験

実装の説明と同様に一定の閾値を超えると検知をコメントで知らせるプログラムを制作した．構成図の赤色の部分がこのテーマのオリジナルの部分である．なお，閾値を決める方法として一定期間内のデータから最も高かった数値と低かった数値を閾値とする手法を提案するが実装には至らなかったため今回のレポートではそれを割愛する．実験では提案内容の 2 番目の部分である IoT 機器が故障した場合の検知と閾値を超えた際の警告などの実行を実際にできるかどうかの確認を実験では行う．この実験は実際にプログラムを動かしたときに問題なく動作するかを重点に置く実験のため閾値の決め方は実験者が適当に決めるものとする．この場合は温度センサ (adt7410) が観測する温度に触れる範囲内の数値と決める．下記に実験の環境のソフトウェア構成図を示す．図の中の 1 番目の矢印は監視対象に対してデータを取るために観測している状態である．2 番目の矢印はセンサがデータを取得している状態である．3 番目の矢印は取得したデータをプログラムに送り異常が無いか検査を行っている．4 番目の矢印は異常が無いか閲覧，アクセスができる状態である．

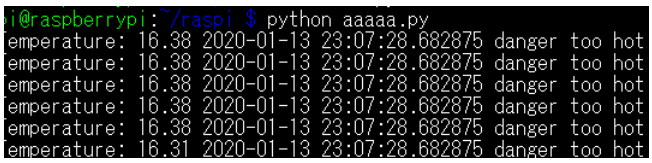

図 4 hot

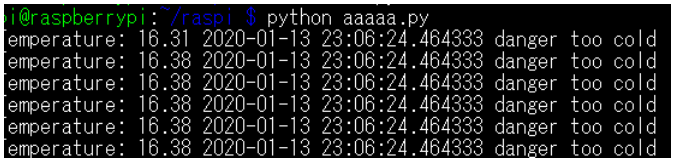

図 5 cold

6. 結果

実験の結果は成功である．プログラムでは閾値を超えたら警告がでるように表示が出来ている．上限の閾値を超えた場合に表示される内容を図の 4 に示す．下限の閾値を超えた場合に表示される内容を図の 5 に示す．2 つの図を見てわかるように閾値を超えた結果，警告が出るようになっている．これは，プログラムで設定した閾値を超えて警告が動作しているということがわかる．また，警告が動作しているということはエラーを出すことなくきちんとプログラムが動作しているということが実験の結果からわかる．

7. 考察

実験の結果からプログラムがきちんと動作すれば閾値を基準に警告を告げることが出来る．問題はその閾値をどのように判断するかである．当初の予定ではある一定期間内のデータを取り，その中から一番高い数値と低い数値を取り上げて閾値とする方式を考えた．しかし，ある一定期間内のデータの中に突発的な数値が出現しそれを閾値とした場合，再現性の低さから異常検知として役に立たないという懸念が考えられる．別の手法として記録したデータを高い順に 3 つ採用して判断する方法がある．これは，ある一定期間内のデータの中から暫定で高い数値を出したデータを 3 つ取り上げる．この 3 つを暫定の閾値として設定し，プログラムを動かした際にどの閾値が頻発して閾値を超えるかを記録する．頻発に閾値を超えるものは通常動作の際の数値だと判断できる．なぜなら，閾値というものは異常検知をするために設けるのであってそれが頻出するのならば，それは異常検知では無く通常動作の範囲内といえる．逆にある一定期間内で最も高い数値を出したのにも関わらず，以降に二度と閾値をまたぐことのない数値は特殊なケースでしか記録することができない閾値と判断し破棄する．また，高い数値の閾値だけでなく，低い数値の場合にもこの手法は有効だと考えられる．この閾値の破棄の判断で残ったものを正式な閾値として採用する手法が現段階の考察ではベストな新規手法である．しかし，この手法では暫定閾値 3 つが特殊なケースであった場合には役に立たないということがわかる．暫定する閾値の数を増やす方法があるがこれではどこまで暫定閾値を設けるかキリが無いと考えられる．閾値を設ける研究はまだ余地があるといえる．

8. おわりに

この論文では IoT 機器の異常検知を IoT センサで行うという研究を行った．異常検知のプログラムは閾値を設けることで警告を出して異常を検出することが出来た．しかし，何をもって異常とするか閾値の決め方が考察でも述べたように閾値を暫定で 3 つ決める手法では，まだ不十分である．閾値を決める方法に人工知能を使う手法が思いつくが研究テーマから逸れるため今回の研究からは外している．よって，今回の研究では閾値が設けられた場合の警告を出すプログラムはできたが，その閾値を決める手法がまだ研究の余地があるということが分かった．

この論文の研究では異常検知を行う IoT センサを行った．しかし，この IoT センサ事態が故障してしまった場合のケースを考えると異常検知という面ではまだまだ不十分であるということが今回の研究で新たに分かった．監視用 IoT センサやデバイスが故障した際の対策として今回提案する異常検知のシステムの外側に監視用 IoT を監視するシステムが対策として考えられる．これは異常検知のシステムの外側に設置することでたとえ監視対象の IoT デバイスと監視用の IoT センサが故障して異常検知が不能になったとしても外側の監視用 IoT センサを監視するプラットフォームを設けることで不意の故障に備えるものだ．

最後に本研究では IoT センサを用いて異常検知の研究を通じて，異常検知の方法や構築について考察を行った．その結果，異常検知を行う上で何をもって異常と判断するのか閾値の決め方が本研究では重要だということが分かった．また，IoT センサが壊れた際の予備体制が必要があることも本研究では判明した．閾値を決める最適な方法や手法の研究，不意の故障に備えてのシステムの予備などが今後の課題である．

参考文献

[1] 三宅 常之:IoT の現在と次の 10 年、日本写真学会誌、81 巻、第 2 号 (2018)
[2] P.Suresh, J.Vijay Daniel, Dr.V.Parthasarathy, et al.:A state of the art review on the Internet of Things(IoT) , Proc. IEEE-32331(2014)
[3] 関谷 勇司:ネットワークログ分析による異常検知の可

能性について、「マルチメディア, 分散, 協調とモバイル (DICOMO2017) シンポジウム」(2017)
[4] 花森　利弥、西村　利浩:システムの異常予兆を検知するリアルタイム監視ソリューション (2016)
[5] Hyunsoo, L:Framework and development of fault detection classification usingIoT device and cloud environment, Jornal of Manufacturing Systems(2017)
[6] Euripide G.M. Petrakis, Stelios, S, Theodoros, S, et al.: Internet of Things as a Service (iTaaS): Challenges and solutions for management of sensor data on the cloud and the fog, Internet of Things(2018)
[7] Stefano, T, Jorn, M, Nikolaos, T, Rajkumar, R:Secure IoT Devices for the Maintenance of Machine Tools, ScienceDirect(2017)
[8] H.H. Pajouh, R. Javidan, and R. Khayami:A Two-Layer Dimension Reduction and Two-Tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks, IEEE transactions on emerging topics in computing(2016)
[9] Arijit, U, Soma, B, Chetanya, P, et al.: IoT Healthcare Analytics: The Importance of Anomaly Detection, IEEE 30th International Conference on Advanced Information Networking and Applications(2016)
[10] Douglas, H.S, Kenneth, M.Z and Yu, C:Ultra-Lightweight Deep Packet Anomaly Detection for Internet of Things Devices, IEEE(2015)
[11] Nanda, K.T, Ethiopia, N, Rejeev, K.K, et al.: Distributed Internal Anomaly Detection System for Internet-of-Things, Proc. IEEE Annual Consumer Communications(2016)
[12] Lingjuan, L, Graduate, S.M, Jiong, J, et al.: Fog-Empowered Anomaly Detection in IoT Using Hyperellipsoidal Clustering, IEEE INTERNET OF THINGS JOURNAL, Vol.4, No.5(2017)
[13] Hichem, S, Sidi, M.S, Mohamad, A.: A Lightweight Anomaly Detection Technique for Low-Resource IoT Devices: A Game-Theoretic Methodology, Proc. IEEE ICC 2016 - Mobile and Wireless Networking Symposium(2016)
[14] Briana, A, LiEsa, B, Rahmira, R, Albert, E.: Behavioral Modeling Intrusion Detection System (BMIDS) using Internet of Things (IoT) Behaviorbased Anomaly Detection via Immunity-inspired Algorithms, Proc. International Conference on Computer Communication and Networks(2016)
[15] Ismail, B, Burak, K, Melike, E.: Anomaly detection and privacy preservation in Cloud-Centric Internet of Things, Proc. IEEE ICC 2015 - Workshop on Security and Privacy for Internet of Things and Cyber Physical Systems(2015)