Isolation Forestを用いた IoT向け異常検知手法に関する考察

菅田 大輔[1,a)]　安全 花子[1,2,†1]

概要：概要

キーワード：Isolation Forest， IoT， IDS， 異常検知

A Study on Anomaly Detection Method for IoT using Isolation Forest

Daisuke Sugata[1,a)]　Hanako Anzen[1,2,†1]

Abstract: abstract

Keywords: Isolation Forest, IoT, IDS, Anomaly Detection

1. はじめに

2. 研究方法

2.1 Isolation Forest の説明

Isolation Forest（以下, iForest）は, 外れ値検出のためのアルゴリズムである。iForest は異常データが少数であり、離れているという前提に基づいている。ランダムにデータを分割していくと、異常データは相対的に早く分離される。iForest は以下のステップで実行される。

1. データの分割

ランダムに選んだ特徴量から、ランダムに選んだ値をもとにデータを分割する。これを一定回数繰り返し、複数のツリーを作成する。

2. 異常スコアの算出

データがツリーの枝に到達するまでの平均パスをもとに、異常スコアを算出する。具体的な計算式は以下の通りである。

ここで、$E(h(x))$ はデータ点 x の平均パス長、$c(n)$ はデータセットのサイズ n に依存する定数である。

3. 異常判定

先ほど計算した異常スコアをもとに異常検知を行う。通常、トレーニングデータの異常スコアの上位 10%を閾値として設定し、それを超えたデータを異常と判定する。

2.2 IDS の概要

本研究では、小規模な IoT 環境に適した Intrusion Detection System（IDS）の設計について検討する。具体的には、Isolation Forest を用いた異常検知手法が提案され、その有効性を評価する。

2.3 全体の設計

IDS の設計は以下の 3 つのセクションに分けられる：

(1) **データの前処理**：

[1] 東京工業大学 情報理工学院 数理・計算科学系
Department of Mathematical and Computing Sciences, School of Computing, Tokyo Institute of Technology
[2] 株式会社 YY セキュリティ研究所
Security Laboratories, YY Corporation
[†1] 現在，国立研究開発法人 ZZ 研究所
Presently with National Institute of ZZ
[a)] sugata.d.aa@m.titech.ac.jp

- 入力データを適切な形式に変換する。
- 不必要な特徴量の削除やデータの標準化、ラベルエンコーディングを行う。

(2) **特徴量選択**：
- 判定に重要な特徴量を選択し、過学習を防ぎ、検知精度を向上させる。
- Random Forest を用いて特徴量の重要度を算出し、重要な特徴量を選択する。

(3) **攻撃の判定**：
- iforest を用いて通信が攻撃通信であるかを判定する。
- 特徴量の選択後、Isolation Forest で異常検知を行う。

2.4 実装

実装は以下のステップで行う：

(1) **データの前処理**：
- はじめに、不必要な特徴量の削除を行う。（データの標準化を行う必要なし？）Iforest に入力できるのは数値データだけなので、カテゴリカルデータを数値データに変換する。one-hot エンコーディングを用いてラベルのエンコーディングを行う。

(2) **特徴量選択**：
- Random Forest を用いて特徴量の重要度を算出する。その後、重要度をもとに上位 1 割の特徴量を使用する。

(3) **攻撃の判定**：
- 攻撃通信、正常通信のそれぞれでトレーニングされたサブシステムが、Isolation Forest によって異常検知を行う。
- それぞれのサブシステムの結果を 2 通りで組み合わせ、最終的な判定を行う。

3. iForest の問題点の整理

Isolation Forest を異常検知手法として使用する際，どのような問題があるのかを明らかにするため，事前実験を行った．はじめにデモデータを使用して，iForest の挙動を確認した．その考察をもとに、特徴量選択手法の提案を行なった

使用したデモデータは、(2.5, 2.5) と (-2.5, -2.5) を中心とした正常データ群と、10 から-10 の範囲に一様に分布した異常データ群からなる．二次元の場合のデモデータを図 1 に示す．

はじめに、デモデータと特徴量数の関係を調査した．図 2 に示すように、特徴量数が増えるにつれて、異常検知の精度が単調に向上することがわかった．また、精度ののびは増加に反比例して緩やかになっていることもわかる。ゆえに、iForest は目標とする精度に対して十分な特徴量数が存在すると言える。

パケット通信を監視して得られたデータセットの全ての特徴が、異常検知に有効であるわけではない。iForest は特徴量同士の重みづけを行わないため、判定に有効でない特徴量が混ざると精度が低下すると考えられる。そこで、図 3 に示すように、ノイズとなる特徴量を混ぜた時の精度を調査した。この結果から、ノイズとなる特徴量が混ざると精度が低下することがわかった。また、今回の実験の場合だと、ノイズとなる特徴量が判定に有効な特徴量数の 2 倍以上になると、精度が急激に低下することがわかった。

前の実験から、データセットからノイズとなる特徴量を取り除くことが重要であることがわかった。ところで、iForest はツリーベースの異常検知手法である。そこで、同じくツリーベースの Randam Forest から特徴の重要度を算出すれば、ノイズとなる特徴量を取り除けるのではないかと考えた。図 4 は、Random Forest で算出した特徴量の重要度を表している。このグラフは、ノイズ特徴量を判別できていることがわかる。そして、実際にノイズ特徴量を取り除いた場合の精度を調査したところ、精度は???%から 0.945%まで向上した。この結果から、Feature Importance

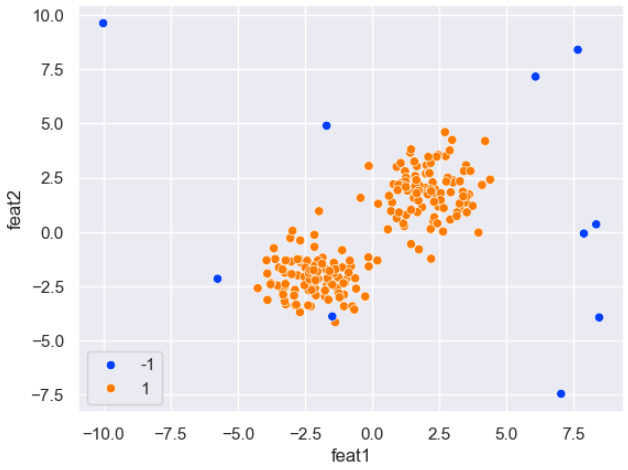

図 1 デモデータに関する図の説明（和文）
Fig. 1 Description of the dim_vs_accu figure (English).

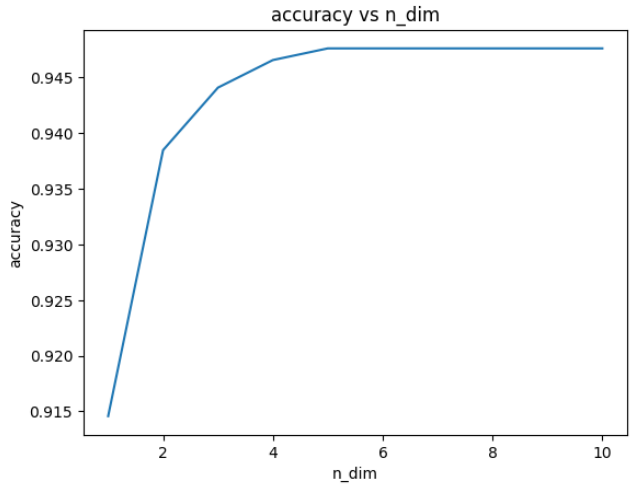

図 2 dim_vs_accu に関する図の説明（和文）
Fig. 2 Description of the dim_vs_accu figure (English).

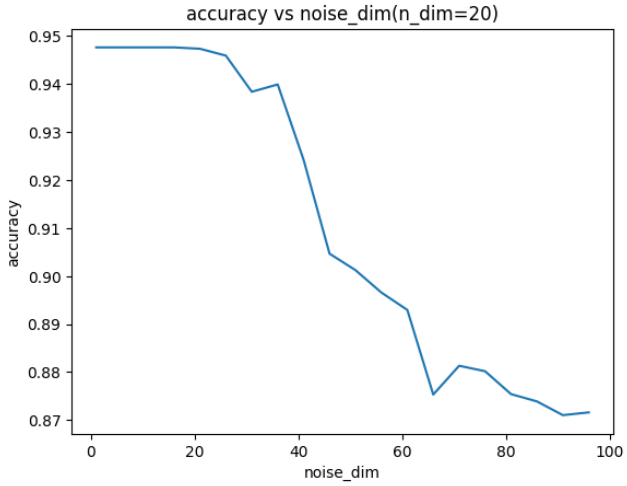

図 3　noise_accu に関する図の説明（和文）
Fig. 3　Description of the noise_accu figure (English).

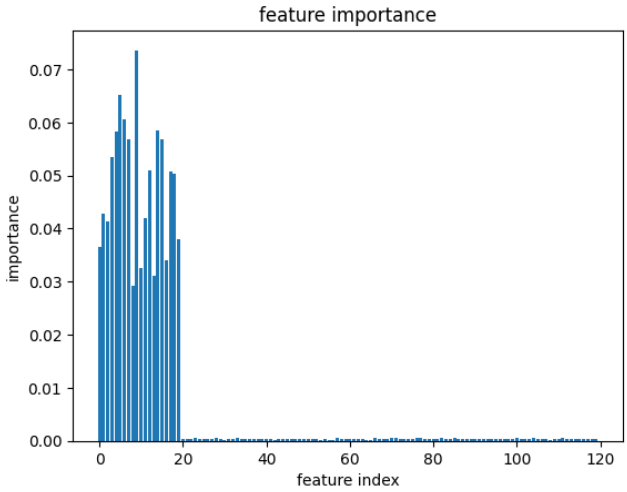

図 4　select_noise に関する図の説明（和文）
Fig. 4　Description of the select_noise figure (English).

による特徴量選択手法は精度の向上に有効ではないかと考えた。

3.1　より効果的な異常判定について

4.　結果と考察

4.1　実験方法

4.1.1　実験環境

(1) **特徴量エンジニアリングの比較：**

- Random Forest を用いた特徴量選択手法
-
-

(2) **判定の組み合わせアルゴリズムの比較：**

- 2 つのサブシステムの結果を組み合わせる手法
- k-means クラスタリングを用いて判定を行う手法
- Rogistic Regression を用いて判定を行う手法

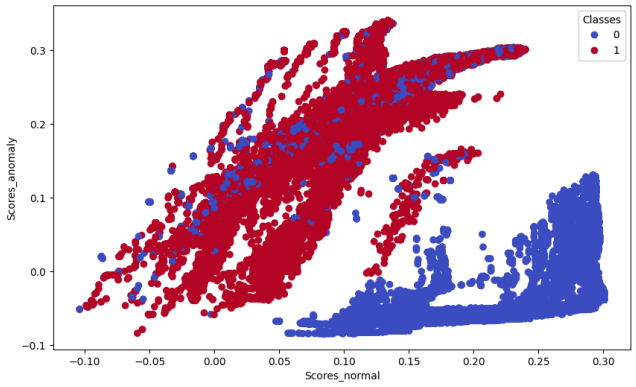

図 5　classes_UNSW に関する図の説明（和文）
Fig. 5　Description of the classes_UNSW figure (English).

実験は Mac Book Pro 2017 2.3GHz Intel Core i5, 8GB RAM で行った。また、実験に用いたプログラムは Python3.10.4 で実装した。Isolation Forest や Random Forest の実装には、scikit-learn のライブラリを用いた。

4.1.2　データセット

使用したデータセットの概要とその妥当性について述べる。

(1) **NSL-KDD**：KDDCUP99 の問題点を解決するために提案されたデータセットであり、データの冗長性や攻撃データの割合を調整したもの。

(2) **UNSW-NB15**：既存のデータセットの問題点を解決し、現代のネットワークトラフィックと低フットプリント攻撃を包括的に反映するために作成されたデータセット。

4.1.3　評価指標

使用した評価指標とその妥当性について述べる。

(1) **Accuracy**：正確度を示し、予測が実際のクラスと一致する割合を示す。

(2) **F1-score**：Precision（適合率）と Recall（再現率）の調和平均を示す。

4.2　結果

4.3　考察

5.　おわりに

おわりにを書く.

謝辞　謝辞を書く.

参考文献

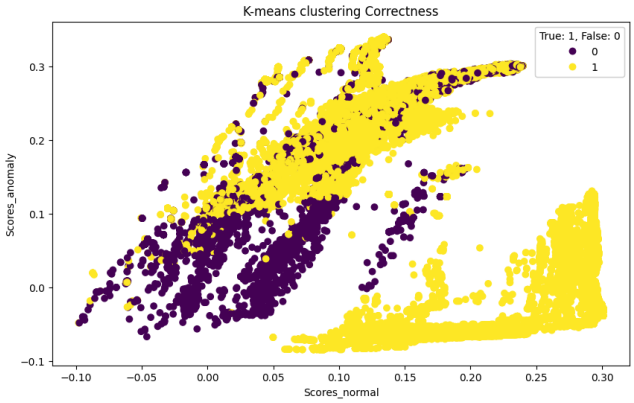

図 6　collectness_UNSW に関する図の説明（和文）

Fig. 6　Description of the collectness_UNSW figure (English).

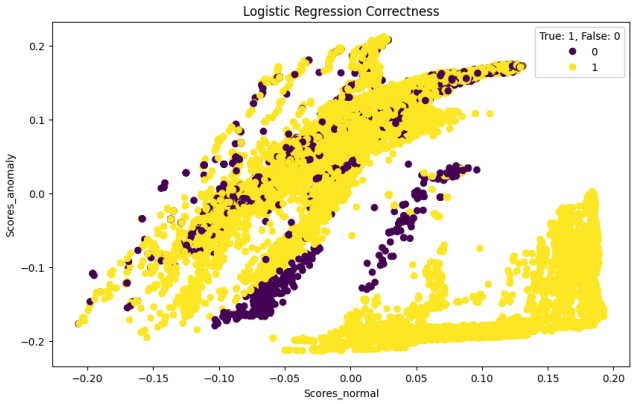

図 7　collectness_UNSW2 に関する図の説明（和文）

Fig. 7　Description of the collectness_UNSW2 figure (English).

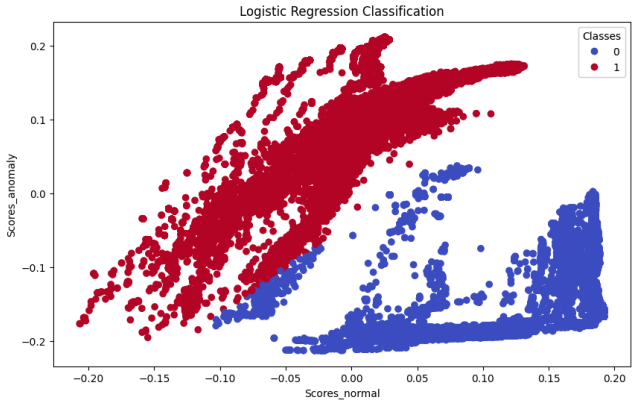

図 9　predict_classes_UNSW2 に関する図の説明（和文）

Fig. 9　Description of the predict_classes_UNSW2 figure (English).

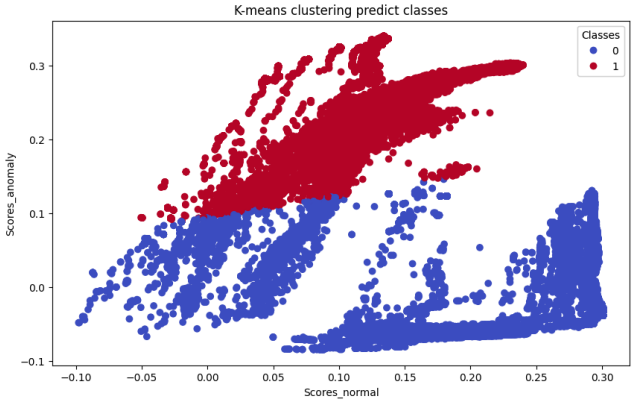

図 8　predict_classes_UNSW に関する図の説明（和文）

Fig. 8　Description of the predict_classes_UNSW figure (English).