Computer Security Symposium 2017
23 - 25 October 2017

Random Forest と K-Means 法を組み合わせたハイブリッド型攻撃検知方式の検証評価

高原　尚志[†1]

概要：インターネットに接続されたコンピュータは，日々サイバー攻撃を受ける危険と向かい合っている．既存のウイルス対策ソフトでは，過去に行われたサイバー攻撃を記したシグネチャと呼ばれる定義ファイルに掲載されている攻撃を防ぐことはできるが，過去に経験のない新たな攻撃に対応することは困難である．そこで著者らは，CSS2016 にて，人工知能の中核をなす機械学習の技術を組み合わせることによって，過去に経験のない攻撃を検知する手法(RFn5-Means)を開発し，広く知られたベンチマーク用データセットである KDD Cup 1999 Data での検証を行い報告した．しかし，KDD Cup 1999 Data は，データの冗長性が大きく実践的なデータとは言えない．そこで本稿では，KDD Cup 1999 Data を修正した NSL-KDD を用いて検証を行い，提案手法（RFn5-Means）の実践における有効性を検証する．その際，機械学習の単独手法についても検証を行い，提案手法と比較する．

キーワード：k-means，攻撃検知，NSL-KDD, KDD Cup 1999 Data, Random Forest

Evaluation of Hybrid Intrusion Detection Method combined with Random Forest and K-Means

Hisashi Takahara[†1]

Abstract: Computers on the Internet are subjected to cyber attack. Although existing anti-virus software can protect known attack, it cannot protect unknown attack. Then authors, in css2016, proposed a hybrid anomaly detection method named RFn5-Means which was combined Random Forest with K-Means. Those are machine learning methods which are core techniques of Artificial Intelligence (AI). In KDD Cup 1999 Data which is well-known dataset for benchmark of intrusion detection, authors evaluated RFn5-Means and reported. However, for that dataset have many redundant records, we cannot regard it as practical data. Thus, in this paper, we evaluate RFn5-Means with NSL-KDD which revised KDD Cup 1999 Data for practice. In consequence, we prove practicability of that method. Additionally, we evaluate some well-known machine learning methods too, and then compare them with RFn5-Means.

Keywords: K-Means, Intrusion Detection, NSL-KDD, KDD99, Random Forest

1. はじめに

1.1 背景

今日，インターネット上では，多くのサイバー攻撃が日々生み出されている．これに対応するため，サイバー攻撃の検知は大変重要である．サイバー攻撃の検知には，過去の攻撃パターン（シグネチャ）を参考に攻撃を検知するミスユース型検知と正常通信を定義してそれ以外の通信を攻撃とみなすアノマリ型検知がある[1]．ミスユース型検知では，過去の攻撃パターンによって攻撃か否かを決めるため，新たな攻撃を検知できないという課題がある．一方，アノマリ型検知では，正常通信以外は攻撃通信とするため，正常通信を正確に定義することが求められ，正常通信を攻撃とみなす誤検知率が高くなる傾向にある[2]．誤検知率を低く抑えつつ新たな攻撃にも対応した攻撃検知の方法として，機械学習を利用した方法がある．機械学習の方法には，過去の攻撃データを学習データとして参考にしながら現在の攻撃に対応する教師あり学習と学習データを用いない教師なし学習がある．教師あり学習では，過去の攻撃パターンを学習データとして，攻撃か否かを判断する．そのため，教師あり学習手法では，学習データにある攻撃（以降，学習済攻撃と称す）においては高い検知率を示すことが知られている[3][4][5]が，一方で，学習データにない攻撃（以降，非学習攻撃と称す）に対する検知率は低い[6][7]．今まで経験のない新しい攻撃に対応するためには，非学習攻撃を高い確率で検知することが求められる．

なお，既存の論文では，学習データ内に存在する攻撃を「既知の攻撃」，「known attack」，「known intrusion」などと称し，シグネチャや学習データ内に存在しない攻撃を「未知の攻撃」，「unknown attack」，「unknown intrusion」などと称している[2][8][9][10][11]が，以降，本稿では，前者を「学習済攻撃」，後者を「非学習攻撃」と称す．

1.2 動機

著者らは文献[7]の中で，広く知られた攻撃検知のためのベンチマーク用データセットである KDD Cup 1999 Data（以降，KDD99 と称す）(1.5.2)を用いて，教師なし学習の

†1 新潟県立大学
University of NIIGATA PREFECTURE

広く知られた手法である K-Means 法(1.5.1)では，学習済，非学習に関わらず攻撃を検知することができることを示した．特に，非学習攻撃の検知に関しては，教師あり手法が高々0.1 だったのに対して K-Means 法では 0.999 と極めて高い値を示した．

K-Means 法には，

「最適なクラスタ数をいくつにするか」

という課題があるが，著者らは文献[7]の中で，KDD99 の検証に限っては，攻撃検知に K-means 法を適用した場合のクラスタ数は 5 が有効であるという結論を得た．これは，KDD99 の攻撃カテゴリの数が 4 で，これに正常通信カテゴリを加えた数であり，このカテゴリ数が影響していると考えられる．

著者らは文献[6]の中で，

(特徴 1) 教師あり学習である Random Forest は学習済攻撃の検知率が高い(検知率 0.910)

(特徴 2) 教師なし学習である K-Means は非学習攻撃の検知率が高い（検知率 0.999）

ということを示し，Random Forest において学習済攻撃をスクリーニングした後，K-Means で非学習攻撃を検知するというハイブリッド方式を提案し，KDD99 で検証した．その結果，すべての攻撃を検知することができた（検知率 1.000）．

しかし，KDD99 は

・意図的に冗長データを挿入している

・正常通信と攻撃通信のバランスが実践的ではない（攻撃通信の比率が多過ぎる）

・データ容量が大きい

などの指摘があり，KDD99 のみの評価をもって，上記手法（以降，RFnK-Means と称す）が有効であるとは言えない．

そこで本稿では，KDD99 を実践的なデータセットとしての修正した NSL-KDD(1.5.2)を用いて，RFnK-Means について評価を行い，実践に耐え得るか否かを検証する．また，教師あり学習の各手法や教師なし学習の K-Means 法といった単独手法の評価も合わせて行い，RFnK-Means の結果と比較した．

1.3 先行研究

著者らは文献[6]の中で RFnK-Means を提案し，KDD99 によって検証を行い，すべての攻撃を検知することに成功した．ここでは，先行研究として，著者らが文献[P40]の中で提案した手法である RFnK-Means について紹介する．

RFnK-Means は，1.2 の中で示した 2 つの特徴

(特徴 1) 教師あり学習である Random Forest は学習済攻撃の検知率が高い(検知率 0.910)

(特徴 2) 教師なし学習である K-Means は非学習攻撃の検知率が高い（検知率 0.999）

に基づいて，これを組み合わせることにより，学習済攻撃，非学習攻撃を検知するという手法である．

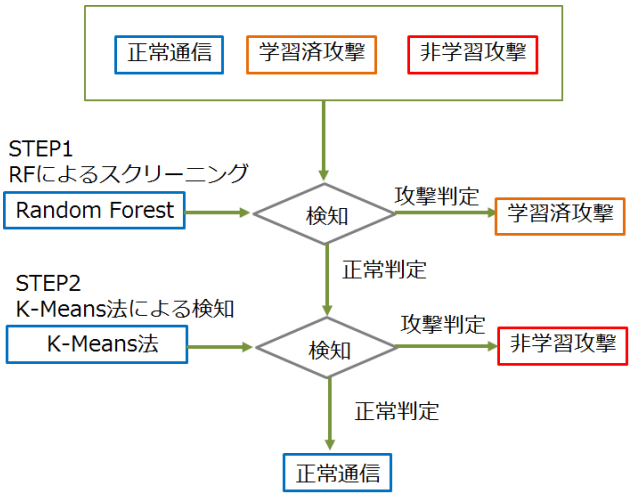

図 1 RFnK-Means 方式の攻撃検知フロー

Figure1 Anomaly Detection Flow on RFnK-Means Method

著者らは文献[6]において，KDD99 では，検知率 1.000 を達成し，攻撃検知においては，KDD99 での検証に限って，目標を達成した．また，K-Means のクラスタ数についても，KDD99 での検証において，5 が有効であるということも合わせて示した（以降，クラスタ数 5 の K-Means を 5-Means と称し，文献[6]での提案手法を RFn5-Means と称す）．

1.4 研究課題と貢献

文献[6]で RFn5-Means についての検証に用いたデータセットは KDD99 である．KDD99 は，攻撃検知のベンチマーク用データセットとして広く知られているが，一方で

・意図的に冗長データを挿入している

・正常通信と攻撃通信のバランスが実践的ではない（攻撃通信の比率が多過ぎる）

などの指摘があり，KDD99 のみでの検証で実践に有効であると結論付けることはできない．

そこで本稿では，KDD99 を実践用修正したデータセットである NSL-KDD を用いて更なる検証を行い，RFn5-Means が，実践にも耐え得る手法であることを示すことにより，実践的なサイバー攻撃検知の観点からの学術的貢献を目指す．

1.5 関連研究

1.5.1 機械学習手法

本稿では，機械学習の手法として，提案方式で用いられる RF，K-Means 法以外にも，比較のため決定木（Decision Tree =DT），Naïve Bayes(NB)，Support Vector Machine(SVM)などの手法を用いて検証を行った．関連研究として，各手法について，ここで説明する．

***K-Means 法**

K-Means 法は，1967 年に J. MacQueen によって命名された[12]．学習データを用いない，教師なし機械学習手法の

ひとつであるクラスタリングの代表的な手法で，アルゴリズムは次の通りである[13][14][15][16][17][18].

（1）予めクラスタ数 k を決め，各クラスタに対する代表値を設定する.（初期の代表値を決める方法としては，与えられたデータをランダムに k 個選んで，各クラスタの代表値とする方法などがあるが，本稿では，ランダム関数を用いて初期値を発生させる方法を用いた.）

（2）各ノードに対して各クラスタの代表値からの距離を測定して，最も短いクラスタに対象ノードを所属させる.

（3）所属したノードの平均値を計算して，改めてクラスタの代表値とする.

（4）代表値が変わらなくなるまで，（2），（3）を繰り返す.

（5）代表値が変わらなくなった時点で，クラスタリングを終了し，各ノードの所属を決定する.

K-Means 法には, 球形のクラスタを形成する傾向がある, クラスタの大きさや濃度を均等にしようとする，外れ値の影響を受けやすいなどの課題が指摘されている[19].

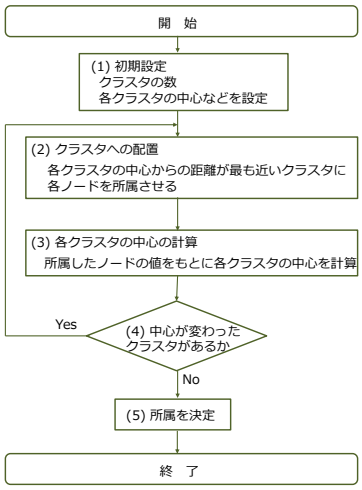

図 2 K-Means 法のフローチャート
Figure2 Flow Chart of K-Means

***Decision Tree (DT)**

DT は決定木とも呼ばれ, 提案方式で用いる RF は複数の DT を組み合わせて用いるアンサンブル手法であるが，そのもととなる DT は，特徴値ごとに条件を設定して，最も分類効率が大きな特徴値から順に分類を行うことにより，ノードの所属カテゴリを予測する手法である[20][21].

***Random Forest (RF)**

RF は, 2001 年に Leo Breiman によって提案された[22][23], 複数の DT を用いて分類を行うアンサンブル手法[21]である．各 DT において，ランダムに抽出された特徴量の中から分類能力の高い特徴量から順に分類を行うことを繰り返す．攻撃検知に応用した場合，高い分類能力を示すことが広く知られている[3][4][5].

***Naïve Bayes (NB)**

NB は，各特徴量が独立であると仮定して，事前に与えられる学習データから尤度を推定し，評価データが所属するカテゴリを求める方法である[21][24].

***Support Vector Machine (SVM)**

SVM は, 学習データをもとに各データを分離する超平面の中でマージンを最大化するものを求めてモデルを形成して，評価データを識別する手法である．1963 年に V. N. Vapnik らによって線形モデル[25]が，1992 年に Bernhard E. Boser らによって非線形モデル[26]が提案された.

1.5.2 データセット

***KDD99**

KDD99 は，1998 DARPA Intrusion Detection Evaluation Data Set（以降，DARPA98 と称す）[27][28]の通信データ（TCP dump データ）をセッション単位のデータとして加工したデータセットであり, データが古い, 冗長的である, データサイズが大きいなどの短所もあるが，現在でも多くの攻撃検知の研究で検証用データセットとして用いられている[29][30][31]．KDD99 には，4,893,980 件のデータからなるフルデータ(kddcup.data)とその内の約 10％の 494,020 件のデータを抽出したデータ(kddcup.data_10_percent), そして 311,029 件のデータからなる評価用データ(corrected)などが収められている．本稿では，学習データとして kddcup.data_10_percent，評価データとして corrected を用いる．kddcup.data_10_percent の中には，97,277 件（19.69%）の正常通信と 396,743 件（80.31%）の攻撃通信が収められている．攻撃通信は 22 種類の攻撃からなり，これが DoS, Probe，U2R，R2L の 4 つのカテゴリに分かれている．corrected の中には, 60,593 件（19.48%）の正常通信と 250,436 件（80.52%）の攻撃通信が収められている[30]．攻撃通信は 37 種類の攻撃からなり[30]，この内，20 種類は kddcup.data_10_percent と共通の攻撃で，残りの 17 種類は新たな攻撃である．KDD99 における検証実験では，kddcup.data_10_percent を教師あり学習の学習データとして用い，corrected を評価データとして用いるが，学習データである kddcup.data_10_percent に含まれる攻撃を学習済攻撃，評価データである corrected に含まれる攻撃の内 kddcup.data_10_percent には含まれない攻撃を非学習攻撃と称す．corrected の全攻撃通信 250,436 件の内，171,114 件（68.33%）は学習済攻撃，79,322 件（31.67%）は非学習攻撃である.

***NSL-KDD**

NSL-KDD[32] は，カナダの UNB(University of New Brunswich)において，KDD99 の冗長性や容量の多さなどの欠点を修正したデータセットである．主な特徴は，KDD99

の冗長性の除去や各手法の評価結果の差を大きくすることによって，手法ごとの特徴を見出せるようになっている．また，データ量を少なくする（学習データで KDD99 の約 29.0%，学習データで KDD99 の約 7.2%）（表 1）ことにより，評価実験ごとにデータを抽出する必要がなくなり，常に同一データによって評価実験を行うことができるため，結果が抽出に依存することがなくなり，評価結果の比較に信頼性を得ることができる．

また，実践データと比べて攻撃通信の多さが指摘されていた KDD99（約 2:8（正常通信:攻撃通信））に対して，NSL-KDD では，攻撃通信の割合を大幅に減らして（約 6:4（正常通信:攻撃通信））実践データに近づけるための修正が行われている（表 1）．

表 1 攻撃通信と正常通信の比率
(KDD99 vs. NSL-KDD)
Table1 Ratio between Attack and Normal
(KDD99 vs. NSL-KDD)

		Normal	Attack	Total
KDD99	Train	19.7% (97,277 件)	80.3% (396,743 件)	434,020 件
	Test	19.5% (60,593 件)	80.5% (250,436 件)	311,029 件
NSL-KDD	Train	53.5% (58,630 件)	46.5% (67,343 件)	125,973 件
	Test	43.1% (9,711 件)	56.9% (12,833 件)	22,544 件

その他にも，京都大学で開発された Kyoto[33][34][35]やオーストラリアのニューサウスウエールズ大学で開発された UNSW-NB15[36][37][38]などのデータセットがあるが，本稿では，特徴量の選択による影響を考慮して，KDD99 と同じ特徴量をもつ NSL-KDD での検証を行った．

2. RFn5-Means の検証評価

ここでは，1.5.1 で示した機械学習の各手法（単独手法）と RFn5-Means について，KDD99 と NSL-KDD を用いて検証を行い，その結果について考察を加える．

2.1 準備

2.1.1 評価指標

本稿では，検証の評価指標として，検知率（DR）と誤検知率（FAR）を用いた．以下に混同行列(Confusion Matrix)（表 2）をもとにした，各指標の定義式（式 1，式 2）を示す[1][21][39][40].

表 2 混同行列
Table2 Confusion Matrix

	予測(Positive)	予測(Negative)
正解 (Positive)	TP (True Positive)	FN (False Negative)
正解 (Negative)	FP (False Positive)	TN (True Negative)

$$\mathrm{DR} = \frac{TP}{TP+FN} \quad \text{(式 1)}$$

$$\mathrm{FAR} = \frac{FP}{FP+TN} \quad \text{(式 2)}$$

ここで TP (True Positive)は, Positive と正しく予測されたノード数，FP (False Positive)は，実際は Negative であるが Positive と予測されたノード数，FN (False Negative)は，実際は Positive であるが Negative と予測されたノード数，TN (True Negative)は Negative と正しく予測されたノード数である．本稿では，Positive を Attack（攻撃通信），Negative を Normal（正常通信）と読み替えるものとする．

2.1.2 ソフトウエア

本稿では，機械学習用ソフトウエアとして，オーストラリアの Waikato 大学から配布されている WEKA[41][42]を用いる．WEKA は，機械学習用のフリーソフトであり，現在，多くの機械学習を用いた攻撃検知の研究で用いられている[42].

本稿における各手法に対する WEKA の設定は, 以下の通りである．

*SVM

WEKA の SMO アルゴリズムを用い，カーネル関数として exponent 1 の Poly kernel を用いた．

*DT

ID3 アルゴリズム[43][44]の拡張である C4.5 の WEKA における実装である J48 を用いた．

*NB

WEKA における実装である NaïveBayes を用いた．

*RF

選択する特徴量の数は，全特徴量数 m に対して，log2m+1 として検証実験を行った．これは，WEKA のデフォルト値である．また，今回の検証実験では，決定木数を 5 としたが, 決定木数 3 から 20 では, 各指標の標準偏差は高々0.012 であった. なお, 特徴量の選択は, WEKA の random number generator に RF におけるデフォルトの seed 値 1 を与えて行った．

*K-means 法

WEKA の実装である SimpleKMeans にて検証を行った．初

期値は, WEKA の random number generator に SimpleKMeans におけるデフォルトの seed 値 10 を与え，クラスタの数は 5 として検証を行った.

2.1.3 データセット

検証に用いるデータセットは以下の通りである.

*KDD99

学習データ…kddcup.data_10_percent_corrected

評価データ…corrected

*NSL-KDD

学習データ…KDDTrain+

評価データ…KDDTest+

2.2 前処理

2.2.1 特徴量の選択

KDD99 には 41 個の特徴量がある．KDD99 を修正した NSL-KDD にも同様に 41 個の特徴量がある．特徴量の選択は攻撃検知にとって重要な課題であり，Gini 係数[21]や Information Gain[21]を用いたものがあるが，本稿では上記 41 個の特徴量の内, テキストデータである protocol_type と service と flag を除いた 38 個の特徴量を選択した.

2.2.2 正規化

検証実験を行うにあたって，データを正規化[21]した．また， KDD99 及び NSL-KDD には全部で 41 個の特徴量があるが，この内，検証には，テキストデータである Protocol_type，Service，Flag の 3 つの特徴量を除外した 38 個の特徴量を用いた．各特徴量は，正規化（normalization）して(式 3), 最大値 1, 最小値 0 の範囲に収まるようにした.

$$\text{正規化後の値} = \frac{\text{もとの値} - \text{最小値}}{\text{最大値} - \text{最小値}} \qquad \text{（式 3）}$$

更に，評価データ（KDD99 の場合 corrected，NSL-KDD の場合 KDDTrain+）に含まれる 37 種類の攻撃の内，学習データ（KDD99 の場合 kddcup.data_10_percent_correctd，NSL-KDD の場合 KDDTest+）に含まれる攻撃を学習済攻撃（以降，EXIST と称す）とし，含まれない攻撃（17 種類）を非学習攻撃として，正常通信と非学習攻撃のみのデータ（以降，NEW と称す）を作成し，非学習攻撃の検知の検証を行う際の評価データとした.

2.3 評価結果と分析及び考察

単独手法及びハイブリッド手法（RFn5-Means）の KDD99 及び NSL-KDD による評価結果は以下の通りである（表 3）.

表 3 評価結果(KDD99 vs. NSL-KDD)

Table3 Results of Evaluation (KDD99 vs. NSL-KDD)

*KDD99

	DR	FAR
5-Means	0.957	0.297
SVM	0.902	0.016
DT	0.907	0.017
NB	0.900	0.026
RF	0.910	0.005
RFn5-Means	1.000	0.478

*NSL-KDD

	DR	FAR
5-Means	0.807	0.573
SVM	0.603	0.068
DT	0.669	0.078
NB	0.646	0.160
RF	0.597	0.078
RFn5-Means	0.952	0.160

上記の結果, KDD99 では教師あり学習の各手法の DR は 0.900 以上であるが，NSL-KDD では DT の 0.669 が最も高い値であり，KDD99 の場合と比べて，0.2～0.3 ポイント程度低くなっている．教師なし学習である 5-Means でも DR は 0.15 ポイント低くなっている．これに対して，RFn5-Means は, 約 0.05 ポイントの下落に抑えられている.

更に FAR に関しては，教師あり学習の各手法が 0.05 ポイント以上上昇しており，教師なし学習の 5-Means でも，約 0.3 上昇している．これに対して，RFn5-Means では，約 0.3 低く抑えることができている.

上記の結果から，教師あり学習の各手法は，実践データである NSL-KDD に対しては, 検知率が下がってしまうが, RFn5-Means は実践データでも検知率の低下を 0.05 ポイント程度に抑えることができ，NSL-KDD での検証結果を見る限り，実践に耐え得る手法であることが分かった.

以降，上記の結果となった要因について，考察（分析）する．上記結果を分析するにあたり，各手法の学習済攻撃及び非学習攻撃の検知率を測定した（表 4，表 5）.

表 4 学習済攻撃の評価（KDD99 vs. NSL-KDD)

Table4 Results of Evaluation for Known Attack (KDD99 vs. NSL-KDD)

*KDD99

	DR	FAR
5-Means	0.826	0.014
SVM	0.968	0.016
DT	0.974	0.020
NB	0.964	0.026
RF	0.976	0.006

*NSL-KDD

	DR	FAR
5-Means	0.818	0.243
SVM	0.730	0.068
DT	0.778	0.088
NB	0.702	0.162
RF	0.756	0.078

表 5 非学習攻撃の評価（NSL-KDD)

Table5 Results of Evaluation for Unknown Attack (KDD99 vs. NSL-KDD)

*KDD99

	DR	FAR
5-Means	0.999	0.619
SVM	0.091	0.016
DT	0.082	0.017
NB	0.099	0.026
RF	0.100	0.005

*NSL-KDD

	DR	FAR
5-Means	0.993	0.593
SVM	0.301	0.068
DT	0.404	0.,078
NB	0.568	0.160
RF	0.200	0.078

その結果，NSL-KDD では，学習データがあるにも関わらず，教師あり学習の各手法の学習済攻撃に対する検知率は，0.756(RF の検知率)に留まった．また，各手法とも KDD99 の場合に比べて，NSL-KDD では，検知率が 0.2～0.25 程度下がっている．これは，KDD99 には冗長データが多く，これを除去した NSL-KDD では，学習データにある攻撃であってもまったく同じ特徴量の値を示すとは限らないことが要因のひとつではないかと考えられる．つまり，実践においては，学習データ（シグネチャ）があっても，特徴量の値がまったく同じでない場合，機械学習の手法では検知できない学習済攻撃が存在することを意味している．このことは，学習済攻撃の亜種も，教師あり学習では検知するのは難しいということを意味していると考えられる．一方で，RFn5-Means の STEP1 で RF（教師あり学習）を用いた学習済攻撃の検知率が低下したとはいえ，70%～80%程度の学習済攻撃は検知でき，検知した攻撃を除去（スクリーニング）した後の攻撃通信と正常通信の割合は，NSL-KDD でも 0.634:0.366(正常通信:攻撃通信)で，KDD99 の場合（0.727:0.273）と比べても割合で 0.09 ポイント程度の差に留まるため（表 6）RFn5-Means の STEP2 である 5-Means の段階では攻撃通信の数が減少しており，KDD99 の場合と同様に攻撃通信と正常通信に分類しやすくなっているものと考えられる．

表 6 RF スクリーニング後の攻撃通信と正常通信の割合（KDD99 vs. NSL-KDD）

Table6 Ratio between attack and normal after RF Screening (KDD99 vs. NSL-KDD)

	Normal	Attack
KDD99	0.727	0.273
NSL-KDD	0.634	0.366

また NSL-KDD において，KDD99 の場合と比べて，誤検知率が 0.478 から 0.016 へと 0.36 ポイント程度改善されているのは, KDD99 では人工的に冗長データを多く挿入していたため, 正常通信を誤って攻撃通信と判定してしまうと，冗長データとして挿入された周辺データも誤検知してしまったためと考えられる．

従って RFn5-Means は, NSL-KDD で検証評価した範囲ではあるが，誤検知率の観点からも，実践データに対して対応できる可能性がある手法であると考えられる．

3. まとめ

本稿では，著者らが文献[6]にて提案した RFn5-Means について, KDD99 を実践データとして修正した NSL-KDD を用いて，単独の機械学習手法と比較しながら，評価検証した．その結果，教師あり学習手法では，NSL-KDD においては検知率が 0.7 に達しなかったのに対して，RFn5-Means では 0.952 という結果を得た．このことから，

・教師あり学習手法は，単独手法では，実践で用いるには課題がある

・RFn5-Means は，実践でも用いることができる可能性がある

ということが分かった．

更に，KDD99 において，RFn5-Means 手法を実践で用いるための課題となっていた誤検知率の高さも実践データでは 0.160 に抑えることができ，誤検知率の観点からも RFn5-Means が実践に用いることができる可能性があることが分かった．

しかし，NSL-KDD は 1999 年の KDD99 のデータセットを修正したものであるため，データが古いという指摘がある．そのため，今後，2015 年時点のデータを有する Kyoto や UNSW-NB15 などの近年のデータを含むデータセットにて検証を行う予定である．ただし，Kyoto や UNSW-NB15

などのデータセットは，KDD99 や NSL-KDD と特徴量の数や種類が異なるため，上記データセットを用いる場合には特徴量の選択についての研究も同時に進める必要があると考えられる．

現時点で，サイバー攻撃検知に関して，以下の課題が考えられる．

・最適な特徴量の選択[45][46]
・状況に応じたパラメータチューニング
・本稿の手法である RFn5-Means（RF+K-Means）以外の組み合わせによるハイブリッド手法との比較[47][48]
・検知率及び誤検知率の向上
・最適な評価用データセットの検討[49][50]

今後，上記課題について，丁寧にひとつひとつ取り組んで行く予定である．

謝辞 本研究は JSPS 科研費 JP17K00187 の助成を受けたものです。

本稿の執筆にあたり，九州大学の櫻井幸一先生と YAOKAI FENG 先生にご指導頂きました．ここに感謝の意を表します．

参考文献

[1] 山田明: ネットワーク侵入検知システムの高度化に関する研究，*東北大学博士学位論文* (2009).
[2] Reda M. Elbasiony, Elsayed A. Sallam, Tarek E. Eltobely, Mahmoud M. Fahmy: A hybrid network intrusion detection framework based on random forests and weighted k-means, *Ain Shams Engineering Journal*, Volume 4, Issue 4, pp.753-762, (2013).
[3] Jiong Zhang, Mohammad Zulkernine, and Anwar Haque: Random-Forests-Based Network Intrusion Detection Systems, *IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and Reviews*, Vol.38, No.5, pp.649-659 (2008).
[4] Saint Murat GIRAY, Aydin Goze POLAT: Evaluation and Comparison of Classification Techniques for Network Intrusion Detection, *Proc. 13th International Conference on Data Mining Workshops (ICDMW 2013)*, pp.335-342 (2013).
[5] Sundus Juma, Zaiton Muda, M.A. Mohamed, Warusia Yassin: Machine Learning Techniques for Intrusion Detection System: A Review, *Journal of Theoretical and Applied Information Technology (JATIT)*, vol.72, no.3, pp.422-429 (2015).
[6] 高原尚志: Random Forests と K-Means 法によるハイブリッド式アノマリ検知方式，*コンピュータセキュリティシンポジウム 2016 (CSS2016)論文集*, pp.1019-1026(2016).
[7] 高原尚志: K-Means 法による攻撃検知　ー教師あり学習手法との比較ー，*電子情報通信学会技術研究報告*, Vol.116, No.300, pp.207-214(2016).
[8] 山田明，三宅優，竹森敬祐，田中俊昭: 学習データを自動生成する未知攻撃検知システム，*情報処理学会論文誌*, vol.46, no.8., pp.1947-1958 (2005).
[9] Jungsuk SONG, Hiroki TAKAKURA, Yasuo OKABE, and Yongjin KWON: Unsupervised Anomaly Detection Based on Clustering and Multiple One-Class SVM, *IEICE TRANS. COMMUN.*, Vol.E92-B, No.6, pp.1981-1990, (2009).
[10] Gisug Kim, Seungmin Lee, Sehun Kim: A novel hybrid intrusion detection method integrating anomaly detection with misuse detection, *Expert Systems with Applications*, Volume 41, Issue 4, pp.1690-1700 (2014).
[11] 村井光，正代隆義：効果的なネットワークインシデント検知のための半教師ありデータスクリーニング，*火の国情報シンポジウム 201 論文集 5*, 2B-3, pp.1-8, 佐賀大学 (2015).
[12] J. MacQueen: Some methods for classification and analysis of multivariate observations, *Proc. Fifth Berkeley Symp. on Math. Statist. and Prob.*, vol. 1, pp. 281-297 (1967).
[13] 松田一孝，筧一彦，胡振江，武市正人: データマイニングのアルゴリズム記述を容易にする拡張行列演算の提案．*情報処理学会論文誌 プログラミング.*, vol.46, no.SIG 11 (PRO 26), pp.1-15 (2005).
[14] 上田達也，安倍広多，石橋勇人，松浦敏雄: P2P 手法によるインターネットノードの階層的クラスタリング，*情報処理学会論文誌*, vol.47, no.4, pp.1067-1076 (2006).
[15] Jain, Anil K.. Data clustering: 50 years beyond K-means, *Pattern Recognition Letters*, Vol. 31, No. 8, pp.651-666 (2010).
[16] Supreet Kaur, Usvir Kaur: A Survey on Various Clustering Techniques with K-means Clustering Algorithm in Detail, *International Journal of Computer Science and Mobile Computing*, vol.2, no.4, pp.155-159 (2013).
[17] Mukesh Kumar Choudhar, Mandeep Singh Saini: Palvee. Classification by K-Means Clustering, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, vol.2, no.5, pp.1684-1688 (2013).
[18] Johannes Blömer, Christiane Lammersen, Melanie Schmidt, Christian Sohler: Theoretical Analysis of the k -Means Algorithm - A Survey (online), available from <https://arxiv.org/pdf/1602.08254v1> (accessed 2016-05-21).
[19] Tan,Steinbach, Kumar: K-Means Cluster Analysis (online), available from <https://www.yumpu.com/en/document/view/26521444/k-means-cluster-analysis-chapter-3-3-ppdm-cl-ass> (accessed 2016-05-21).
[20] Kotsiantis, S B.: Decision trees: a recent overview, *Artificial Intelligence Review*, vol. 39, no. 4, pp.261-283 (2013).
[21] 荒木雅弘: フリーソフトで始める機械学習入門，*森北出版株式会* (2014).
[22] LEO BREIMAN: Random Forests, *Machine Learning*, vol.45, no.1. pp.5-32 (2011).
[23] RandomForest　(online), available from <http://weka.sourceforge.net/doc.dev/weka/classifiers/trees/RandomForest.html> (accessed 2016-05-21).
[24] George H. John, Pat Langley: Estimating continuous distributions in Bayesian classifiers, *Proc. the Eleventh conference on Uncertainty in artificial intelligence* (UAI'95), pp.338-345 (1995).
[25] V. N. Vapnik and A. Ya. Lerner: Pattern Recognition Using Generalized Portrait Method, *Automation and Remote Control.*, vol.24, no.6, pp.774-780 (1963).
[26] Bernhard E. Boser, Isabelle M. Guyon, Vladimir N. Vapnik: A Training Algorithm for Optimal Margin Classifiers, *Proc. the fifth annual workshop on Computational learning theory* (COLT '92). , pp.144-152 (1992).
[27] Lincoln Laboratory, Massachusetts Institute of Technology (online), available from <https://www.ll.mit.edu/ideval/data/1998data.html> (accessed 2016-05-21).
[28] Mahbod Tavallaee, Ebrahim Bagheri, Wei Lu, and Ali A. Ghorbani: A Detailed Analysis of the KDD CUP 99 Data Set, *Proc. the 2009 IEEE Symposium on Computational Intelligence in Security and Defense Applications* (CISA 2009), pp.53-58 (2009).
[29] Martina Troesch and Ian Walsh: Machine Learing for Network Intrusion Detection, *Final Report for CS 229*, Stanford University (2014).
[30] Atilla Ozgur, Hamit Erdem: A review of KDD99 dataset usage in

intrusion detection and machine learning between 2010 and 2015 (online), available from <https://peerj.com/preprints/1954/> (accessed 2016-05-21).
[31] Saffa O. Al-mamory, Firas S. Jassim: Evaluation of Different Data Mining Algorithms with KDD CUP 99 Data Set, *Journal of Babylon University, Pure and Applied Sciences*, vol.21, no.8, p.2663-2681 (2013).
[32] S. Revathi, A. Malathi: A Detailed Analysis on NSL-KDD Dataset Using Various Machine Learning Techniques for Intrusion Detection, *International Journal of Engineering Research & Technology (IJERT)*, vol.2, Issue 12, p.1848-1853 (2013).
[33] Jungsuk SONG, Hiroki Takakura, and Yasuo Okabe: Description of Kyoto University Benchmark Data (online), available from < http://www.takakura.com/Kyoto_data/BenchmarkData-Description-v5.pdf> (accessed 2017-08-23).
[34] Song, J., Takakura, H., Okabe, Y., Eto, M., and Inoue, D., and Nakao, K. "Statistical analysis of honeypot data and building of kyoto 2006+ dataset for NIDS evaluation," *in Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security* (BADGERS'11), pp.29–36 (2011).
[35] 多田竜之介, 小林良太郎, 嶋田創, 高倉弘喜: 新 Kyoto2006+ データセットの作成に関する検討と評価, 電子情報通信学会技術研究報告, Vol.116, No.328, pp.21-26 (2016).
[36] The UNSW-NB15 data set description (online), available from < https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/cybersecurity/ADFA-NB15-Datasets/> (accessed 2017-08-23).
[37] Nour Moustafa, Jill Slay: UNSW-NB15: a comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set), *Military Communications and Information Conference* (MilCIS) (2015).
[38] Moustafa, Nour, and Jill Slay: The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set, *Information Security Journal: A Global Perspective*, Volume 25, pp.18-31 (2016).
[39] Natesan, P, Balasubramanie, P, Gowrison, G.: Improving the attack detection rate in network intrusion detection using adaboost algorithm, *Journal of Computer Science*, Vol. 8, No. 7, pp.1041-1048 (2012).
[40] Chordia Anita S.: Sunil Gupta. An Effective Model for anomaly IDS to Improve the Efficiency, *Proc. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, p.190-194 (2015).
[41] Mark Hall, Eibe Frank, Geoffrey Holmes, Bernhard Pfahringer, Peter Reutemann, Ian Witten: The WEKA data mining software: an update, *ACM SIGKDD Explorations Newsletter*, vol.11, no.1, p.10-18 (2009).
[42] The University of Waikato: Weka 3 - Data Mining with Open Source Machine Learning Software in Java (online), available from <http://www.cs.waikato.ac.nz/ml/weka/> (accessed 2016-05-21).
[43] Kotsiantis, S B.: Decision trees: a recent overview, *Artificial Intelligence Review*, vol. 39, no. 4, p.261-283 (2013).
[44] 市野将嗣, 市田達也, 畑田充弘, 小松尚久：トラフィックの時系列データを考慮した AdaBoost に基づくマルウェア感染検知手法, *情報処理学会論文誌*, Volume 53, No.9, pp2062-2074, （2012）.
[45] Chidanada Murthy P., Dr. A. S. Manjunatha, Anku Jaiswal: Building Efficient Classifiers for Intrusion Detection with Reduction of Features, International Journal of Applied Engineering Research, Volume 11, Number 6, pp.4590-4596 (2016).
[46] Elaheh Biglar Beigi, Hossein Hadian Jazi, Natalia Stakhanova, and Ali A. Ghorbani: Towards Effictive Feature Selection in Machine Learing-based Botnet Detection Approches, *Communications and Network Security* (CNS) (2014).
[47] Muhammed Kabir Gmbo, Azman Yasin: Hybrid Approach for Intrusion Detection Model Using Combination of K-Means Clustering Algorithm and Random Forest Classification, *The International Journal of Engineering and Science* (IJES), Volume 6, Issue 1, pp.93-97 (2017).
[48] Kailas S. Elekar, Prof. M. M. Waghmare: Effective Intrusion Detection System Using Combination of Data Mining Techniques, *Forth Post Graduate Conference* (iPGCON-2015) (2015).
[49] Iman Sharafaldin, Amirhossein Gharib, Arash Habibi Lashkari: Towards a Reliable Intrusion Detection Benchmark Dataset, *Software Networking*, Vol. 2017, Issue 1, pp.177-200 (2017).
[50] Monowar H. Bhuyan, Dhruba K. Bhattacharyya, and Jugal K. Kalita: Towards Generating Real-life Datasets for Network Intrusion Detection, *International Journal of Network Security*, Vol.17, No.6, pp.675-693 (2015).