Vol.2022-IOT-58 No.11
2022/7/12

SSHブルートフォース攻撃検知における認証時間の有効性について

小林 孝史[1,a)]　嶋田 洸希[1]　大歳 英征[1]　伊佐 眞寿[1]　武田 瑞樹[1]

概要：これまで，SSH 接続時の認証時間（パスワード要求からパスワードを入力して送信してくるまでの時間）を利用した攻撃検知の研究を行ってきた．以前の研究では，この認証時間に閾値を設定したり，時間帯や接続元 IP アドレスに依る適応的に閾値を設定して検知を行ってきたが，認証時間を用いることの有効性が明らかになっていなかった．本研究では，認証時間を用いることにより，いくつかの機械学習においても検知率の向上に寄与できることを示す．

The Effectiveness of Authentication Time in Detecting the SSH Bruteforce Attacks

Takashi Kobayashi[1,a)]　Koki Shimada[1]　Hideyuki Otoshi[1]　Shingo Isa[1]　Mizuki Takeda[1]

Abstract: We have been studying attack detection using the authentication time (the time between the password request and the password input and transmission) for SSH connections. In previous studies, we set a threshold value for the authentication time or an adaptive thresold value based on the time of day or the source IP address, but the effectiveness of using the authentication time has not been cleared. In this study, we show that the use of authentication time can contribute to improving the detection rate in several machine learning methods.

1. はじめに

インターネットサーバ上への攻撃が絶えない．Web サイトやアプリケーションを運用するにあたって，サーバを用いてコンテンツやプログラムを作成・保管・運用を行うことが主流である．そのため，インターネット上のサーバには多数の有用な情報が蓄積されており，その価値は現代の社会の中で非常に高いものとなっている．その情報が流出すると，社会的信用をなくしたり，金銭的な被害を被る可能性がある．

昨今の世界情勢を見ても，リモートワークに関係するシステムが攻撃を受けたり，情報漏えいが発生した報道が見受けられる．遠隔接続サーバへのログインについてはニュース記事になるようなことはあまりないが，日々攻撃を受けているような状況である．JPCERT/CC の報告によると，日本における SSH サーバに対する攻撃は，2020 年，2021 年に上位 5 位圏内にランクインしており，攻撃の対象となりやすいことがわかっている．最も多いのは 23/TCP で，次いで，445/TCP，22/TCP となっている．

我々が行っている研究は，その SSH サーバへのパスワードクラッキング攻撃を検知することであり，これまでに，パスワードを入力する認証時間を計測してそれを検知に用いたり [1]，時間帯や IP アドレスに基づいて適応的に攻撃かどうかを判定する仕組み [2] を開発してきた．

これらの研究においては，認証時間を攻撃検知に用いているものの，その有効性については判断していなかった．そこで，本研究では，認証時間が攻撃検知に対して有効であること，また，機械学習アプローチにおいても認証時間をパラメータとして用いることにより，より性能の良い攻撃検知が可能になることを示す．

[1] 関西大学 総合情報学部
Faculty of Informatics, Kansai University
[a)] taka-k@kansai-u.ac.jp

表 1　解析によるツールのパケット長と内容

ツール名	パケット長	パケット内容
bruteSSH	92	SSH-2.0-paramiko_1.7.7.1
Metaspoit	87	SSH-2.0-OpenSSH_5.0
Hydra	87	SSH-2.0-libssh-0.5.2
Medusa	86	SSH-2.0-MEDUSA_1.0
nCrack	86	SSH-2.0-OpenSSH_5.2
patator	92	SSH-2.0-paramiko_1.7.7.1

2. 関連研究

機械学習や深層学習アプローチを採用している研究，攻撃情報の解析についての研究について紹介する．これらの研究のいずれも，セッション全体の時間やパケット間の平均的な所要時間についての取り扱いはあるものの，本研究で取得している認証時間を識別に使用したり解析対象とはしていない．

2.1 Delwar らの研究

Delwar らの研究 [3] では，CICIDS2017 データセットを用いて，SSH と FTP に対する bruteforce 攻撃の検知を行っている．このときに LSTM（Long Short-Term Memory）による深層学習アプローチを用いている．加えて，機械学習による識別器を用いた識別と有効性の評価も行っており，その結果，LSTM モデルが 99.88%という性能を示した．

2.2 Kahara Wanja らの研究

Kahara Wanja らの研究 [4] では 5 つの基礎的な機械学習アルゴリズムと CNN（畳み込みニューラルネットワーク）を用いて比較検証をしている．CICIDS2018 データセットを用いて行われている．CNN を用いるため，特徴量のデータを画像データと同じ 2 次元配列に変形して学習を行っている．

CNN を用いた検知の判定結果は，Accuracy: 0.943，Precision: 0.925，Recall: 0.978，F-measure: 0.918 という非常に高い検知結果になっている．また，他の 5 つのアルゴリズムと比較しても，ほぼ同値か CNN がわずかに上回る結果になった．

2.3 ムイデンらの研究

ムイデンらの研究 [5] では SSH サーバへの認証を手入力でなく自動で認証するツールに対してのツールごとにどのような差があるのかということを検証している研究になっている．この研究では，攻撃者が用いる自動認証ツールはツールによって違いがあることに着目して，ハニーポットを用いログファイルを出力し，分析を行なっている．SSH サーバとクライアント間でバージョン交換を行う際に発生するパケットの長さとペイロードを Wireshark を用いて解析を行っている．SSH サーバとクライアント間でコネクションが確立されると，SSH プロトコルとしての通信が開始され，サーバはクライアントに対してバージョン情報の送信を行う．例として,，SSH サーバソフトウェアの代表的な OpenSSH バージョン 8.4p1 では，“SSH-2.0-OpenSSH_8.4p1” という文字列を送信し，それに対してクライアント側はそれに対応したバージョン情報を返信する．解析結果としてツールによってペイロードの長さとペイロードの内容の違いを分析した．分析の結果は表 1 のように示されている．表の数字はパケット長である．ツールによって実装されているソフトウェアバージョンが異なることが発見された．なお，現在，当研究室で観測しているソフトウェアバージョンの比率については，この表とは異なるものとなっている．

3. 本研究で使用している認証情報について

これまでに行った研究で用いていた認証情報として，OpenSSH サーバのソースコードに手を加え，ログイン試行ごとにアクセスの時間，ログを取得した SSH サーバの IP アドレス，SSH サーバのバージョン，SSH サーバのプロセス id，認証の成否，アクセス元 IP アドレス，パスワードの入力を求めてからパスワードを含むパケットが返ってくるまでの時間，悪性/正規の判断，SSH プロトコルの通信から計算された RTT，マイクロ秒までを含むアクセスの時間，アルゴリズムの交渉が終わった時間，鍵交換が完了した時間を含んだ情報を取得している．

OpenSSH サーバ自体への改変は，公式サイトでの最新バージョンのリリースに合わせて，認証情報の取得部分を組み込んでいる．これまでのところ，8.x 系のマイナーバージョンでのアップデートが主体であったため，ソースコードが大きく変化していないことから，多くの作業は発生していない．

認証情報の例

```
Nov 8 20:59:41 localhost sshd4 [6409]: Fail,
726f6f74, 7a68656e7275696463, 60.173.195.191,
44422, 0.136092, Normal, 106.016872,
1636372781, 075988, 109.678610, 102.355134
[preauth]
```

3.1 認証時間

本研究では，キーボード入力を伴う正規ユーザのパスワード入力時間に比べ，攻撃者はログイン処理を自動化することから，坂東・上原の研究 [1] と同様に，パスワード入力時間が短くなる傾向がある性質を利用した検知を行う．そのため，クライアントのパスワード入力時間を計測する必要がある．本研究ではクライアントにパスワード入力要求を出し，その応答が返ってくるまでの時間を認証時間と

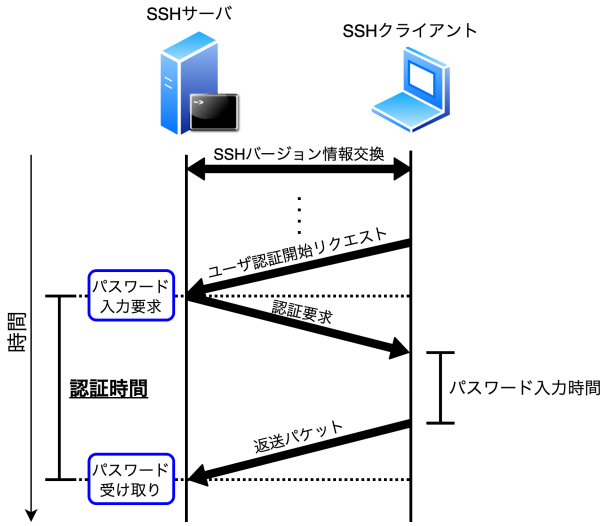

図 1 パスワード入力時間と認証時間の違い

する．

一般に，コンピュータ間の通信は，双方のコンピュータが置かれたネットワーク環境や，地理的距離，時間帯によるネットワーク帯域の混雑具合などにより，通信の遅延が発生する．そのため，この認証時間は，クライアントのパスワード入力時間とは異なる点を留意しなければならない．パスワード入力時間と認証時間の違いのイメージを図 1 に示す．

本研究で使用した認証時間は，SSH サーバのソースコードに手を加え，パスワード入力要求とパスワードを受け取る箇所の間の時間を計測している．もちろん，この時間にはパケットを転送するための時間も含まれているため，送信元によって異なる時間になることは明白である．我々の研究 [2] においては，この傾向も分析する必要があると考え，時間帯や IP アドレスによる個別プロファイリングを用いた検知を行っていた．

4. データセットと前処理

本研究で用いているデータセットは，当研究室の SSH サーバで収集したパケットデータを Canadian Institute for Cybersecurity が提供している CICFlowMeter[6] というネットワークトラフィック解析ツールによって得られた特徴量（78 種類）で構成されている．使用したデータは，2021 年 11 月 1 日から 11 月 7 日の間に収集した 61125 件の攻撃の認証情報ログ，パケットデータを用いる．また，正規ユーザーの遠隔接続時のデータも必要であるため，研究室内の被験者によって作成された認証情報・パケットデータ 1424 件分を加えている．運用データとしては 2021 年 12 月 1 日から 12 月 21 日までの 21 日間のデータと使用する．

この特徴量には，そのパケット（セッション）のラベルも含まれているが，本研究ではそのラベルは使用していない．また，他にも 6 つの特徴量，FlowID，SourceIP，DestinationIP，SourcePort，DestinationPort，Protocol もあるため，これらの特徴量を含めた全 84 種類の特徴量でデータセットを構成している．

4.1 認証情報データとの結合

認証時間については，我々の過去の研究活動において実装を行った SSH サーバによって取得している．CICFlowMeter によるデータセットとこの認証時間を結合する必要があるが，そのときの基準になるのは，送信元 IP アドレスとポート番号である．ハニーポットサーバでは，1 つのセッションに対して最大 3 回の認証が行われているので，その解析データに対して最大 3 つの認証情報データを結合している．

正規のログイン試行については，ハニーポットデータと比較して圧倒的に少なくなっているため，ハニーポットデータで収集した数と同じになるように，重複したデータを持たせている．

4.2 データの正規化と不要データの削除

データセットは機械学習で利用しやすいように，すべて数値化されたデータが格納されている．特徴によっては，非常に小さい値のデータや非常に大きな値のデータが入る可能性があるので，正規化を行うことで絶対値の大きい数値の要素に依存するようなことのないようにしている．

4.3 GeoIP 情報

GeoIP とは，広義には IP アドレスを元に，地球上の場所を特定する技術のことを指す．本研究においても，これまでの研究と同様に，MixMind 社が提供している，GeoLite2 Databases[7] を用い，IP アドレスから位置情報を取得して認証情報に含め，地理的距離と認証時間の関係性の解析に用いている．

5. 機械学習の設定と識別結果

本研究において使用した機械学習アルゴリズムは，ニューラルネットワーク（MLP），LightGBM および畳み込みニューラルネットワーク（CNN）である．

5.1 ニューラルネットワークを用いた学習

ニューラルネットワーク（MLP）は 3 層構成（入力層・隠れ層・出力層）とし，学習パラメータは表 2 のとおりである．ニューラルネットワークのモデル作成には，Python ライブラリである Keras を用いている．認証時間である `authtime` 含むデータセットと含まないデータセットを用いて学習を行った結果を表 3 に示す．

`authtime` を含むデータセットでの学習が 4 つの評価指標すべてで含まないデータを上回っている．これにより，ニューラルネットワークでは `authtime` を含めることで検

表 2 ニューラルネットワークのパラメータ

パラメータ	値
Activation	ReLU
Loss function	binary_crossentropy
Optimization algorithm	Adam
Epochs	20
Batch size	10

表 3 ニューラルネットワークを用いた学習結果

	authtime 含む	authtime 含まない
Accuracy	0.9995	0.9990
Precision	0.9904	0.9901
Recall	0.9810	0.9525
F1	0.9856	0.9709

表 4 LightGBM を用いた学習結果

	authtime 含む	authtime 含まない
Accuracy	0.9999	0.9999
Precision	1.0	0.9969
Recall	0.9969	0.9969
F1	0.9984	0.9969

知率の向上につながることが確認できた．

5.2 LightGBM を用いた学習

LightGBM は決定木アルゴリズムに基づいた勾配ブースティング（Gradient Boosting）の機械学習フレームワークである．モデル訓練にかかる時間が非常に短い，計量値をヒストグラムとして扱うためにメモリーの効率が高い，などの利点がある一方，ハイパーパラメータを適切に設定しないと過学習が起こりやすい，という特徴がある．

LightGBM を用いた学習には，Python のライブラリで実装したプログラムによりモデル化する．このアルゴリズムでも認証時間である authtime を含むデータでの学習と含まない CICFlowMeter の解析結果のみの学習の二つの対比実験をおこなった．さらに，このアルゴリズムでは認証時間のみ，ソフトウェアバージョンを含んだデータでの学習も行った．認証時間の有無での学習の結果は表 4 となった．この結果から Precision，F1 では authtime を含むデータのほうが少し高いスコアを得られた．

LightGBM ではモデル作成に決定木を使用しているため，決定木の作成時に特徴量をさまざまな箇所で利用することがある．その決定木のノードとして使用された回数により重要度を測ることができる．表 5 は使用回数の上位 10 件を示したものである．

また，決定木のノードを通った際に，目的関数にどの程度の改善が見られたかを計算している．その改善度合いについてもその特徴量の重要性を示すことになる．表 6 はその改善値の上位 10 件を示している．

決定木を作成する際の特徴量の使用回数と特徴量による目的関数の改善度合いにより，その特徴量の重要性が示

表 5 特徴量の使用回数による重要度上位 10 件

feature	importance
authtime	0.1500
Fwd IAT Min	0.1137
Flow IAT Min	0.1049
Src Port	0.0767
Idle Mean	0.0690
Init Fwd WinByts	0.0422
Fwd Pkts/s	0.0411
Bwd IAT Min	0.0380
Flow Duration	0.0366
Bwd Pkts/s	0.0338

表 6 特徴量の目的関数の改善による重要度上位 10 件

feature	importance
Tot Fwd Pkts	6.2485
Fwd Pkts/s	0.8791
authtime	0.6676
Init Fwd Win Byts	0.5989
Idle Max	0.5385
Idle Mean	0.5038
Bwd Pkt Len Min	0.2854
Flow IAT Min	0.1878
Fwd IAT Min	0.0225
Src Port	0.0158

表 7 authtime のみの結果

評価方法	スコア
Accuracy	0.9876
Precision	0.6204
Recall	0.2623
F1	0.3687

されている．表 5 および 6 のどちらにも認証時間を示す `authtime` が含まれていることから，認証時間という指標は，悪性と良性の接続を区別するために重要な要素となっていることがわかる．

また，認証時間とソフトウェアバージョンのみを判定要素として用いた LightGBM による決定木の作成も行った（結果は表 7）．認証時間のみを用いた場合，これまでの研究で得られた正答率と同等の結果となったが，再現率は低いものとなった．この結果は，認証時間の情報のみでは，2 つのクラス（攻撃と正規の接続）を区別することは難しいということを示している．正規のユーザーによる接続時のパスワード入力においても，場合によっては非常に短い時間で入力できてしまう状況も容易に想像でき，攻撃者によるパスワード入力ほどではないにしろ，認証時間が比較的短くなる．

もうひとつのソフトウェアバージョンを用いた学習であるが，これは評価用データとして認証時間に加えてソフトウェアバージョンを含めたものを使った学習を行っている．ソフトウェアバージョンとは，SSH サーバとの接続時に交

表 8　CNN のパラメータ

パラメータ	値
Activation	softmax
Loss function	binary_crossentropy
Optimization algorithm	Adam
Epochs	20
Batch size	10
Dropout	0.2

換される文字列 SSH-protoversion-softwareversion のうちの softwareversion のことである [8]．この文字列には，クライアントで使用しているソフトウェアやライブラリの名称等が記述されており，どのようなクライアントから接続されているかを知る指標にもなる．この実験で使用したソフトウェアバージョンは tshark によって抽出された文字列を用いている．

ソフトウェアバージョンと認証時間を用いた LightGBM による決定木モデルの作成では，4 つの指標すべてで 1.0 という結果を得た．このときに用いている正規利用者のクライアントソフトウェアとしては，全員が特定の SSH クライアントを使用している．2021 年 11 月 1 日〜7 日のデータセットの場合，収集したパケットデータはすべて攻撃由来のものであり，その中で，特定の SSH クライアントを使っていると考えられる，ソフトウェアバージョンがその特定の SSH クライアントと同一のものである接続試行は合計で 339 件で，全件数の約 0.5%に当たる．つまり，攻撃ツールのほとんどがその特定の SSH クライアント以外を使用していることになり，かつ，認証時間は短くなっている．逆に，通常利用の場合にはほとんどの場合が特定の SSH クライアントを用いており，かつ，認証時間も長くなっている．このようにソフトウェアバージョンと認証時間には強い相関が見られるため，識別性能も非常に高い結果を示したといえる．この傾向は，このデータセットを作成した時期から 6 ヶ月を経た 2022 年 6 月現在でもほぼ同等の傾向を示している．

5.3　CNN を用いた学習

Python のライブラリである，Keras を用いて畳み込みニューラルネットワーク（CNN）のモデルを作成する．認証時間である authtime を含むデータでの学習と含まない CICFlowMeter の解析結果のみの学習の二つの対比実験をおこなった．CICFlowMeter による特徴の 77 種類を用いる．また，authtime を含むデータでは 78 種類を用いる．また，CNN を用いるにあたって特徴量のデータを画像化する処理を行なった．authtime を含まないデータは 7×11 の形に，authtime を含むデータでは 6×13 に画像化を行なった．表 8 に使用したパラメータを示す．この学習は accuracy のみの判定をおこなった．学習結果は表 9 となった．CNN による学習では Accuracy の指標は他の手法に比べて低くなっていることに加えて，認証時間の有無は学習結果にさほどの影響を及ぼしていないことがわかる．

表 9　CNN を用いた学習結果

	authtime 含む	authtime 含まない
Accuracy	0.9767	0.9767

これは特徴量を画像にマッピングする際，画像サイズが非常に小さいことに加えて，特徴量の関連性を考慮せずに畳み込み層を構築していることもあり，CNN 内のフィルターの学習がうまくいっていないことが考えられる．本研究においてはその検討に取り掛かっていないため，今後の研究課題としておきたい．

6.　検証

以上の比較の結果，本データセットでは LightGBM のモデルが最も高い検知率を発揮したため，LightGBM のモデルを使って検証した．2021 年 11 月 1 日から 11 月 7 日の 7 日間で学習したモデル（以下モデル A）を，ハニーポットサーバで取得している 2021 年 12 月 1 日から 12 月 21 日までの 21 日間の運用データを使用して攻撃の検知結果を検証した．運用はハニーポットサーバで行っているため，運用に用いたデータは全て攻撃者による認証である．12 月 1 日から 7 日の間の認証数は 48566 件，14 日までは 49651 件，21 日までは 48981 件である．その結果を表 10 に示す．検知率としては 12 月 1 日から 12 月 7 日では 97.08%，12 月 8 日から 12 月 14 日では 99.66%，12 月 15 日から 12 月 21 日では 97.02%であった．

また，学習期間を 11 月 1 日から 11 月 7 日の 7 日間から増やし，11 月 1 日から 11 月 14 日の 14 日間（以下モデル B），11 月 1 日から 11 月 21 日の 21 日間（以下モデル C）にしてモデルを作成して検証をおこなった．検証には 7 日間と同様にハニーポットサーバで取得している 2021 年 12 月 1 日から 12 月 21 日までの 21 日間のデータを使用して検証を行なった．結果を表 11，表 12 に示す．また，検知率としては表 11 の 14 日間の学習では，12 月 1 日から 12 月 7 日で 95.76%，12 月 8 日から 12 月 14 日で 99.08%，12 月 15 日から 12 月 21 日で 96.21%であった．また，表 12 の 21 日間の学習では 12 月 1 日から 12 月 7 日で 0.25%，12 月 8 日から 12 月 14 日で 0.27%，12 月 15 日から 12 月 21 日で 0.10%であった．

この結果から，LightGBM のモデルを利用して攻撃を検知することは有効である．ただ，LightGBM の特徴として挙げられる過学習の起こりやすさから 21 日間の大量のデータを学習することによって過学習を起こし検知率が低くなっていると考えられる．そのため，検証にあたっては過学習を起こさないためのアプローチが必要である．

過学習の原因として，LightGBM の学習を行う際に，決定木の深さに対して制限をかけておらず，データの増加に

表 10 モデル A を適用した結果

日程	攻撃と判断	正規ユーザと判断	検知率
12 月 1 日〜7 日	47150	1416	97.08%
12 月 8 日〜14 日	49486	165	99.66%
12 月 15 日〜21 日	47526	1455	97.02%

表 11 モデル B を適用した結果

日程	攻撃と判断	正規ユーザと判断	検知率
12 月 1 日〜7 日	46509	2057	95.76%
12 月 8 日〜14 日	49199	452	99.08%
12 月 15 日〜21 日	47526	1455	96.21%

表 12 モデル C を適用した結果

日程	攻撃と判断	正規ユーザと判断	検知率
12 月 1 日〜7 日	122	48444	0.25%
12 月 8 日〜14 日	1381	48276	0.27%
12 月 15 日〜21 日	51	48930	0.10%

表 13 モデル D を適用した結果

日程	攻撃と判断	正規ユーザと判断	検知率
12 月 1 日〜7 日	43559	5007	89.69%
12 月 8 日〜14 日	49549	102	99.79%
12 月 15 日〜21 日	47439	1542	96.81%

よってより深く学習していたと考えられる．そこで，決定木の深さ制限を設けることでデータが増加しても過学習を起こしにくくするアプローチを行なった（制限として深さを 5 以下とした）．2021 年 11 月 1 日から 11 月 28 日までの 28 日間のデータを使用して学習をおこない，モデルを作成した（以下モデル D）．モデル D を 2021 年 12 月 1 日から 12 月 21 日の 21 日間で検証した結果を表 13 に示す．

検知率としては，12 月 1 日から 12 月 7 日では 89.69%，12 月 8 日から 12 月 14 日では 99.79%，12 月 15 日から 12 月 21 日では 96.81%であった．以上のことから，LightGBM を用いて学習を行うことで高い攻撃検知率を示すことがわかる

7. 結論と今後の課題

本研究では機械学習を用いた手法での認証時間の有無による検知率の変化を確認し，閾値による判定だけでなく，機械学習においても悪性接続の検知に寄与できることを示した．本研究で用いた 2 つの機械学習アルゴリズム（MLP，LightGBM）において，認証時間を含むデータセットの方が判断指標として用いた 4 つの評価数値でいずれも向上することがわかった．これにより認証時間は閾値による攻撃検知だけでなく，機械学習を用いた手法でも有効的な結果が得られるという結論が得られた．

また，畳み込みニューラルネットワークを用いた学習の場合には，認証時間を使用してもさほどの性能向上は見られなかった．この原因については，特徴量の画像変換に際して，生成する画像サイズが小さいことと，畳み込みそうにおける特徴量間の関連性について考慮していないことから，CNN 内のフィルターの学習がうまくいっていないことが考えられる．特徴量を考慮した畳み込み層の構成については，今後検討していきたいと考えている．

本研究では，CICFlowMeter による解析結果を機械学習のデータセットとして用いているが，データサイズや ACK パケット受信回数など，1 セッションのパケットデータから得られる情報によりデータセットを構成しているため，攻撃者からの接続時にリアルタイムに検知する用途には用いにくい特性がある．したがって，リアルタイム検知に適したデータセットの構築方法についても検討していく必要がある．

参考文献

[1] 坂東翼, 上原拓也, 小林孝史：認証時間に基づいた SSH パスワードクラッキング攻撃検知手法の提案, 第 16 回情報科学技術フォーラム, pp. L–015 (2017).
[2] 小林孝史, 嶌岡柊也, 唐心悦, 嶋田洸希, 小川綾雅：パスワード認証情報を収集する SSH サーバの構築および運用とそれを活用した bruteforce 攻撃の検知手法, 研究報告インターネットと運用技術 (IOT), Vol. Vol.2021-IOT-53 No.16, (2021).
[3] Hossain, M. D., Ochiai, H., Fall, D. and Kadobayashi, Y.: SSH and FTP brute-force Attacks Detection in Computer Networks: LSTM and Machine Learning Approaches, *Proceedings of the 5th IEEE International Conference on Computer and Communication Systems (ICCCS 2020)* (2020), Accepted.
[4] Wanjau, S. K., Wambugu, G. M. and Kamau, G. N.: SSH-Brute Force Attack Detection Model based on Deep Learning, *International Journal of Computer Applications Technology and Research* (2021).
[5] Mardan, M., 篠田伸夫：SSH における攻撃ツールの識別, 情報処理学会第 76 回全国大会 (2014).
[6] CICFlowMeter, `https://www.unb.ca/cic/research/applications.html`.
[7] GeoLite2 Free Geolocation Data MaxMind Developer Site, `https://dev.maxmind.com/geoip/geoip2/geolite2/`(Accessed on 01/24/2021).
[8] T. Ylone, E., C. Lonvick: The Secure Shell (SSH) Transport Layer Protocol, https://tools.ietf.org/html/rfc4253 (2006), (accessed on June 20, 2022).