Darknet及びハニーポットの比較分析に基づくマルチベクタ型DDoS攻撃の検知方法の検討

山村 翔[1,2]　神谷 和憲[2]　倉上 弘[2]

概要：複数の攻撃手法を複合したマルチベクタ型 DDoS 攻撃 (以下，マルチベクタ攻撃と呼称する.）が脅威となっている．マルチベクタ攻撃では，帯域幅消費型攻撃，リソース消費型攻撃，アプリケーションレイヤ攻撃等多数の攻撃方法が併用される．そのため，単一の攻撃方法を想定した攻撃検知・防御手法での対策だけでなく，検知・防御手法も多層的に構築する必要がある．本稿では，Darknet で観測したバックスキャッタとハニーポットログの比較により，同一攻撃先を対象としたリソース消費型攻撃，帯域幅消費型攻撃によるマルチベクタ攻撃の検知手法を提案する．評価実験により，リソース消費型攻撃と帯域幅消費型攻撃が同時または間欠的に発生していることの観測に成功した．特に間欠型攻撃は 1 時間以内に別手法による攻撃が発生する可能性が高いことが判明した．また，検知した攻撃の 14%は悪性判定されている IP アドレスへの攻撃であり，攻撃者相互における攻撃を検知した可能性がある．

キーワード：Darknet，ハニーポット，DDoS 攻撃

Discovering Multi-Vector DDoS attack by Correlation Analysis of Darknet Backscatter and Honeypot Logs

Natsuru Yamamura[1,2]　Kazunori Kamiya[2]　Hiroshi Kurakami[2]

Abstract: Multi-vector DDoS attacks have become a major threat among DDoS attacks. In multi-vector DDoS attacks, different types of attack method such as bandwidth consumptin attack, resource consumption attack and application layer attack are utilized. Still overall status of multi-vector attacks is not well analyzed and it is necessary to know how often and what types of attacks are utilized for multi-vector DDoS attacks. In this paper, we propose a method of detecting multi-vector DDoS attacks by correlation analysis of Darknet backscatter traffic and honeypot logs. Evaluation result shows that proposed method is possible to detect that resource-consuming and bandwidth- consuming attacks occur simultaneously or intermittently. Especially, intermittent attacks are likely to occur with other attack methods within one hour. In addition, 14% of detected attacks are targeting malicious IP addresses, and there is a possibility of detecting attacks among attackers each other.

Keywords: Darknet, Honeypot, DDoS attack

1. はじめに

複数の攻撃手法を複合したマルチベクタ型 DDoS 攻撃（以下，マルチベクタ攻撃と呼称する.）が脅威となっている．マルチベクタ攻撃では，DRDoS 攻撃に代表される帯域幅消費型攻撃，SYN Flood 攻撃を代表とするサーバリソース消費型攻撃，HTTP 脆弱性を利用したアプリケーションレイヤ攻撃など複数種類（マルチベクトル）の攻撃手法が併用される．

帯域幅消費型攻撃は，システムリソースないし回線規模を超過する攻撃トラフィックを生成することで，標的を

[1] 警察大学校
National Police Academy
[2] NTT セキュアプラットフォーム研究所
NTT Secure Platform Laboratories

サービス不能状態にする．DNS，NTP プロトコルなどの脆弱性を利用し攻撃規模を増幅する DRDoS 攻撃，多数の脆弱な IoT 機器を不正操作し大規模攻撃を仕掛けるものが代表的である．実際，2016 年 9 月アメリカのセキュリティ情報サイトへの最大 623Gbps の攻撃 [1]，同年 10 月多くの Web サービスが利用不能に陥ったアメリカの DNS サービスへの攻撃 [2]，2018 年 3 月のリポジトリホスティングサービス GitHub への攻撃 [3] などが報告されている．

リソース消費型攻撃は，標的サービスの TCP リソースを枯渇させることでサービス不能状態に陥らせる．SYN パケットを大量に送信し，サーバのコネクションリソースを枯渇させる SYN Flood 攻撃が代表的である．また，IPS やファイアウォールなどを標的とした TCP State Exhaustion 攻撃 [4] も報告されている．

アプリケーションレイヤ攻撃は，HTTP，SIP などのアプリケーションレイヤプロトコルの脆弱性を利用した攻撃であり，HTTP GET/POST 攻撃，SIP INVITE Flood 攻撃が代表的である．

マルチベクタ攻撃の特徴として，単一ベクタの攻撃を検知・防御したとしても，その他のベクトルの攻撃により，攻撃被害が継続・増大する．よって，検知・防御手段も多層的に構築する必要がある．しかしながら，マルチベクタ攻撃の実態・全容は明らかにされておらず，単一ベクタの攻撃の関係性を分析し，全体像を把握，複合化された攻撃を早期に発見することが対策課題の一つである．

本稿では，Darknet におけるリソース消費型攻撃の観測結果とハニーポットによる DRDoS 攻撃の観測結果を照合することにより，マルチベクタ攻撃を検知する手法を提案する．評価実験により，リソース消費型攻撃と帯域幅消費型攻撃が同時または間欠的に発生していることの観測に成功した．特に間欠型攻撃は 1 時間以内に別手法による攻撃が発生する可能性が高いことが判明した．また，検知した攻撃の 14%は悪性判定されている IP アドレスへの攻撃であり，攻撃者相互における攻撃を検知した可能性がある．

2. 関連研究

Darknet 関連研究としては，Darknet トラフィックを分析し，広域スキャンの挙動，攻撃者，攻撃対象のサービス，関連する脆弱性などを示した Durumeric らの研究 [5] がある．深澤ら [6] は異なる Darknet 観測網における相関性を示した．

一方，ハニーポット関連研究としては，複数のハニーポットの観測により，DRDoS 攻撃における送信元の情報，攻撃に使用されたマルウェアなどを示した Krämery らの研究 [7] がある．

Darknet 及びハニーポットの相関分析においては，牧田ら [8] が，DNS ハニーポットと Darknet の関係性に着目し，DRDoS 攻撃の前兆としての Darknet スキャンの可能性を示した．

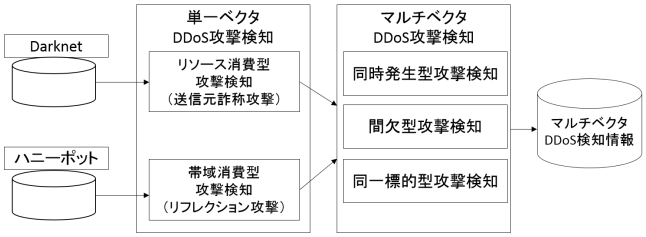

図 1 提案手法の流れ
Fig. 1 Flow of Proposed Method.

3. 提案手法

提案手法では，Darknet の観測結果とハニーポットのログ情報を照合することにより，Darknet で観測された DDoS 攻撃とハニーポットで観測された DDoS 攻撃の相関性を分析する．個々の攻撃において，異なる攻撃手法が使用されていた場合，マルチベクタ攻撃として検知するものである．

具体的には，Darknet からは，TCP プロトコルのバックスキャッタに基づき SYN Flood，FIN Flood 攻撃などのリソース消費型攻撃を，ハニーポットからは，UDP プロトコルの集中的なアクセスに基づき UDP Flood 攻撃，DRDoS 攻撃などの帯域幅消費型攻撃を検知し，各攻撃を紐付けることでマルチベクタ攻撃を検知する．

なお，提案手法では、マルチベクタ攻撃を 3.1 に示す 3 種類に分類しており，それぞれ検知の条件が異なる．

提案手法の処理の流れを**図 1** に示し，以下に各処理の概要を述べる．

3.1 マルチベクタ攻撃の分類

3.1.1 同時発生型攻撃

同一の IP アドレスを標的とした異なるベクトルの攻撃のうち，各攻撃の発生時刻が数秒から数分程度と極めて近いものを指す．ほぼ同時刻に集中的に負荷を与えることで，標的をサービス不能状態とする．

本稿では，発生時刻差が 5 分以内の攻撃を同時発生型攻撃と仮定する．

3.1.2 間欠型攻撃

同一の IP アドレスを標的とした異なるベクトルの攻撃のうち，各攻撃の発生時刻がある程度と離れているものを指す．瞬間的な負荷は同時発生攻撃に劣るが，攻撃を散発的に実施することで攻撃の検知及び全体像の把握が困難になると推測される．

本稿では，発生時刻差が 24 時間以内の攻撃を間欠型攻撃と仮定する．

3.1.3 同一標的型攻撃

同一のサービスを標的とした異なるベクトルの攻撃を指す．同一のサービスとは，特定の FQDN に紐付いた複数の IP アドレスを表す．攻撃先 IP アドレスが分散するた

表 1　Darknet の情報
Table 1　Darknet Logs for Analyzing Multi-Vector DDoS attacks.

名称	概要
観測時刻	当該アクセスを観測した日時.
通信プロトコル	当該アクセスに使用されたＴＣＰ，ＵＤＰなどの通信プロトコル.
送信元 IP アドレス	当該アクセスの送信元 IP アドレス.
送信先ポート番号	当該アクセスの送信先ポート番号.
TCP フラグ	当該アクセスの TCP フラグ情報（SYN，ACK など）.

表 2　ハニーポットの情報
Table 2　Honeypot Logs for Analyzing Multi-Vector DDoS attacks.

名称	概要
観測時刻	1 回のアクセスにおいて最初にパケットを受信した日時.
通信プロトコル	当該アクセスに使用されたＴＣＰ，ＵＤＰなどの通信プロトコル.
送信元 IP アドレス	当該アクセスの送信元 IP アドレス.
送信先ポート番号	当該アクセスの送信先ポート番号.
アクセス数	イベントの発生数．同一送信元からの一定時間内の連続イベントは 1 回とする.
total packets	同じ送信元からのアクセスにおいて受信した総パケット数.
ハニーポット名	当該アクセスを観測したハニーポット.

め，IP アドレスに基づく攻撃の検知及び全体像の把握が困難になると推測される．本攻撃を受けている FQDN を標的 FQDN と呼ぶ.

3.2　Darknet の条件

Darknet には膨大なトラフィックが到達するため，その全てを記録，分析するには多くのリソースが要求される．提案手法では，実施時の負荷を考慮し，サンプリングデータを用いることとした．また，相関分析では送信元 IP を使用するが，Darknet 観測結果の送信元 IP には悪性ホストも含まれる．そこで，後述する条件により，攻撃を受けているホスト（以下，標的ホストという.）の可能性が高いバックスキャッタの送信元 IP のみを抽出する.

なお，Darknet トラフィックを元に検知できる DDoS 攻撃は，送信元 IP アドレスを詐称した攻撃かつ詐称した IP アドレスが Darknet の観測範囲（未使用 IP アドレス帯）の攻撃に限られる.

3.3　ハニーポットの条件

提案手法では，複数のハニーポットのログ情報を用いる．使用するハニーポットは，上位レイヤのプロトコルには依存せず，TCP または UDP パケットを受信した際に，ランダムなペイロードを付加して応答するものである．UDP パケットへの応答に関しては，DRDoS 攻撃を引き込む可能性があるため，西添らの論文 [9] を参考に実装した．プロトコルに依存しないハニーポットのログ情報を使用することで，複数の通信プロトコルを併用するマルチベクタ攻撃に起因するアクセスを網羅する.

3.4　データセットの収集及び整形

データの分析にあたり，はじめに Darknet 観測システム及びハニーポットからログ情報を定期的に収集し，蓄積，集計できるデータベースに登録する．分析対象とする情報として，Darknet 観測システムからは，観測時刻，通信プロトコル，送信元 IP アドレス，送信元ポート番号，TCP フラグを，ハニーポットからは，観測時刻，通信プロトコル，送信元 IP アドレス，送信先ポート番号，送信元から受信した全パケット数（total packets），ハニーポット名を選定した．情報の概要を**表 1**，**表 2** に示す．ハニーポット名はハニーポット毎の特性の分析，total packets はスキャンと DoS 攻撃を識別する目的で対象に含めた.

3.5　リソース消費型攻撃の検知

Darknet の情報から TCP プロトコルのバックスキャッタのみを抽出する．バックスキャッタの識別には，Liu らの論文 [10] を参考とし，TCP フラグに SYN-ACK，ACK，RST，RST-ACK のいずれかを含むものを選択した.

3.6　帯域幅消費型攻撃の検知

ハニーポットの情報から UDP プロトコルを標的とした攻撃を抽出する．攻撃の識別には，total packets を指標とした．total packets が閾値を超えたアクセスはリフレクション攻撃などの帯域幅消費型攻撃，閾値未満のアクセスはスキャン活動と想定し，前者のみを検知する.

3.7　マルチベクタ攻撃の検知

送信元 IP 及び観測時刻の 2 つのパラメータに基づき 3.5 のリソース型攻撃及び 3.6 の帯域幅消費型攻撃の双方の検

表 3　マルチベクタ攻撃検知例
Table 3　Parameter Setting of Experiments.

標的 IP	攻撃種別	観測時刻	観測点	UDP 攻撃プロトコル	TCP 攻撃プロトコル
A	同時発生型	2018/1/31 21:00	Darknet，ハニーポット A	udp123	tcp80
B	同時発生型	2018/3/11 20:55	Darknet，ハニーポット A	udp11211	tcp80
C	間欠型	2018/4/30 00:00	Darknet，ハニーポット B	udp123	tcp8403

知結果を紐付ける．

バックスキャッタの送信元 IP は攻撃を受けるホストであり，ハニーポットの送信元 IP も同様に DRDoS 攻撃の標的となるホストである．本稿ではこれらの IP を標的 IP と呼ぶ．そのため，標的 IP に基づき照合することで，同じ標的ホストに対する攻撃手法を抽出することができる．

ただし，マルチベクタ攻撃の検知においては，攻撃発生の時刻差も分析対象となる．同一の標的 IP に対する攻撃であっても数週間，数ヶ月を隔てて実行された場合は，別個の攻撃と考えられる．したがって，提案手法では，観測時刻も紐付けに使用することとした．しかし，観測時刻をそのまま使用した場合，検知漏れが多数発生するおそれがある．そこで，観測時刻に一定のマージン（以下，観測区間という．）を設定することで，観測区間以下の観測時刻の差を吸収し，攻撃を検知できるようにした．アルゴリズムを Algorithm1 に示す．

Algorithm 1 マルチベクタ攻撃検知方法
Input: DDoS 検知結果 $_{darknet}$,DDoS 検知結果 $_{honeypot}$
Output: マルチベクタ攻撃情報
```
if 標的 IP_darknet = 標的 IP_honeypot then
  if 観測区間 ≦5 分間 then
    同時発生型マルチベクタ攻撃
  else if 観測区間 ≦24 時間 then
    間欠型マルチベクタ攻撃
  end if
end if
if 標的 FQDN_darknet = 標的 FQDN_honeypot then
  同一標的型マルチベクタ攻撃
end if
```

Darknet 及びハニーポットの検知結果を対象に，標的 IP または標的 FQDN が一致する攻撃を抽出し，観測時刻の差が観測区間以内であれば，マルチベクタ攻撃と判定する．さらに，観測区間の値により，同時発生型攻撃などの分類を行う．

以上の処理により，リソース消費型攻撃及び帯域幅消費型攻撃によるマルチベクタ攻撃を検知する．マルチベクタ攻撃検知結果の例を**表 3** に示す．UDP 攻撃プロトコルはハニーポットで検知した攻撃プロトコルを，TCP 攻撃プロトコルは Darknet で検知した攻撃プロトコルを表す．検知結果から標的 A は，2018/1/31 21:00 から 5 分以内に udp123（NTP を用いた帯域幅消費型攻撃）及び tcp80（HTTP を対象としたリソース消費型攻撃）を併用した同時発生型マルチベクタ攻撃を受けた可能性が高いといえる．

検知情報については，通知やデータベース化といった形での使用を想定している．

4. 評価実験

4.1 実験条件

データセットの条件を**表 4**，実験パラメータの条件を**表 5** に示す．

4.2 実験結果

観測区間を調整し，同時型攻撃及び間欠型攻撃の検知を実施した．観測期間全体での標的 IP 数及び検知比率を**表 6** に示す．検知比率は，ハニーポットにおいて検知した帯域消費型攻撃の標的ホストがマルチベクタ攻撃を受ける比率を表し，1 式で求められる．

$$\text{検知比率} = \frac{\text{マルチベクタ攻撃の標的 IP 数}}{\text{帯域幅消費型攻撃の標的 IP 数}} \quad (1)$$

マルチベクタ攻撃の標的 IP 数及び検知比率については，同時発生型攻撃 199IP(検知比率 0.23%)，間欠型攻撃 781IP(検知比率 0.92%) となり，同時発生型攻撃よりも間欠型攻撃の検知数が多い結果となった．したがって，マルチベクタ攻撃においては，同時発生型攻撃よりも間欠型攻撃の標的となる可能性が高いといえる．

観測区間ごとの標的 IP 数を**図 2** に示す．図中の棒グラフは各観測区間で検知した標的 IP 数を，破線は観測区間

表 4　データセット条件
Table 4　Conditions of Data Sets.

パラメータ名	設定値
集計期間	2018 年 1 月 1 日〜6 月 30 日
Darknet アクセス数	4,484,358 (サンプリング済み)
ハニーポットアクセス数	1,806,520

表 5　実験パラメータ設定
Table 5　Parameter Setting of Experiments.

機能	パラメータ名	設定値
ハニーポット	tp 閾値	10,000
同時発生型攻撃検知	観測区間	5 分間
間欠型攻撃検知	観測区間	1 時間，2 時間，6 時間，12 時間，24 時間

表 6　マルチベクタ攻撃における標的 IP 数及び検知比率

Table 6　Number of Victim IP and Detection Ratio in Multi-Vector Attack.

	同時発生型攻撃	間欠型攻撃	全攻撃
全期間	199(0.23%)	781(0.92%)	980(1.16%)
1 日平均	1.48(0.25%)	5.65(0.90%)	7.19(1.18%)
1 週間平均	8.62(0.25%)	34.35(0.94%)	42.96(1.19%)
1 ヶ月平均	34.67(0.24%)	137.50(0.92%)	172.17(1.16%)

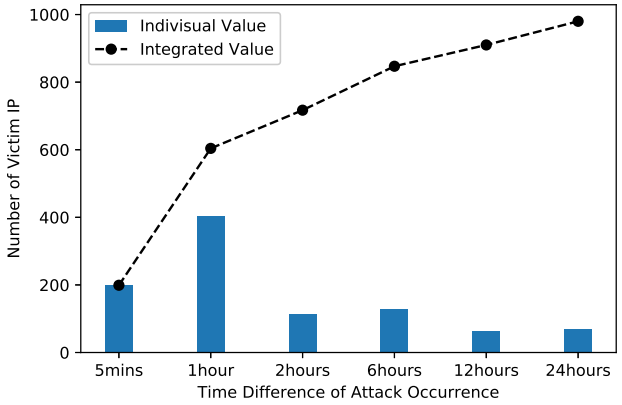

図 2　観測区間ごとの標的 IP 数

Fig. 2　Trend of Number of Victim IP by Time Difference.

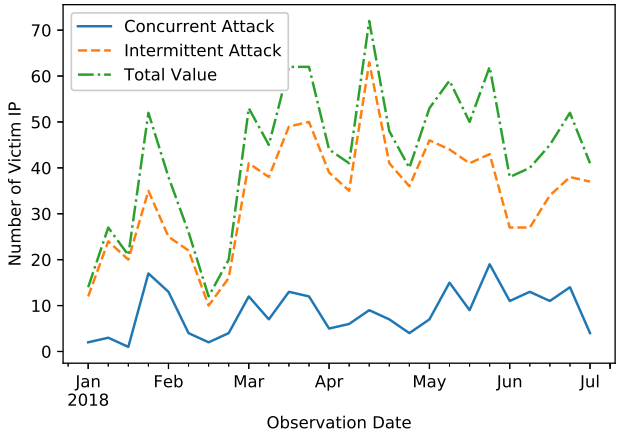

図 3　標的 IP 数の推移

Fig. 3　Trend of Number of Victim IP by Multi-Vector Attack.

5 分間から 24 時間までの累積の標的 IP 数を表す．傾向として，観測区間 5 分間及び 1 時間における検知 IP 数が特に多く，これらを合計した 1 時間以内の標的 IP 数はマルチベクタ攻撃を受けた標的 IP 数の 61.63%に及んだ．このことから，攻撃の実行間隔に変動はあるものの，一度攻撃を受けた標的ホストの半数以上は 1 時間以内に別手法による攻撃を受ける傾向にあると推察される．

時間軸上の標的 IP 数の推移を**図 3** に，マルチベクタ攻撃検知比率の推移を**図 4** にそれぞれ示す．共に実線は同時発生型攻撃を，破線は間欠型攻撃の標的 IP 数を表す．標的 IP 数に関しては，間欠型攻撃の IP 数が恒常的に同時発

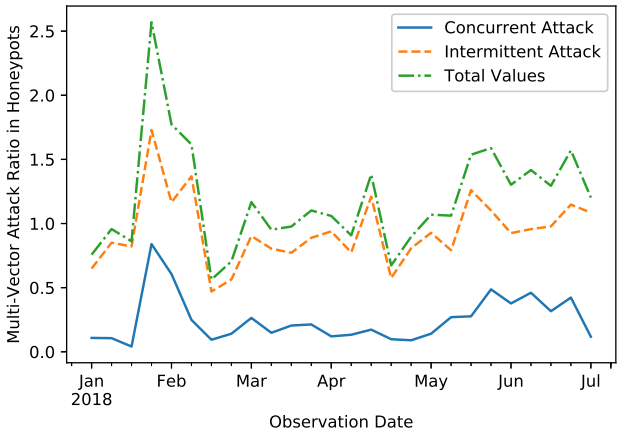

図 4　マルチベクタ攻撃検知比率の推移

Fig. 4　Trend of Multi-Vector Attack Ratio in Honeypots.

生型攻撃の IP 数を上回っている．マルチベクタ攻撃検知比率においても同様の傾向を示している．6 ヶ月間の推移からはマルチベクタ攻撃の増加，減少などの傾向は確認できず，継続的に発生しているものと推測される．

4.2.1　同時発生型攻撃の検知結果

5 分以内に観測された同一 IP に対する攻撃は，同一攻撃者による同時発生型マルチベクタ攻撃の可能性が高い．同攻撃における標的ホストは，1 日平均 1.48IP，1 ヶ月平均 34.67IP であった．

検知頻度上位のプロトコルを**表 7** に示す．攻撃に使用された UDP プロトコルは，udp123(NTP), udp389(CLDAP), udp11211(memcached), udp5093(sentinel), udp9987(VoIP) などの DRDoS 攻撃に使用されるものが上位であった．TCP プロトコルは，tcp80(HTTP)，tcp8043(不明)，tcp25461(不明)，tcp22(SSH)，tcp443(HTTPS) などが上位であった．UDP 及び TCP プロトコルの組合せとしては，特に udp123，udp389 と tcp80，tcp8403 の併用が多く確認された．

観測期間における UDP プロトコルの推移を**図 5** に示す．udp123 は恒常的に多い傾向にある．udp389 は 5 月以降増加の傾向が見られる．udp11211 に関しては，3 月に突如観測され始めた．これは同年 3 月初旬に発生した memcached の脆弱性に基づく DRDoS 攻撃 [3] の影響であり，単一ベクタ攻撃と同様にマルチベクタ攻撃においても，攻撃手法の変遷があると推測される．

同期間における TCP プロトコルの推移を**図 6** に示す．tcp80 は常に多く，tcp8403 は 4 月以降に急増している．

複数のリフレクタを用いた同時発生型マルチベクタ攻撃の検知例を**表 8** に示す．本攻撃では，tcp80 と udp123 が併用されている．udp123 による攻撃が複数のハニーポットにおいて同じ間帯に観測されたことから，DRDoS 攻撃による帯域幅消費型攻撃とリソース消費型攻撃を組み合わせたマルチベクタ攻撃と推測される．

表 7　マルチベクタ攻撃における使用プロトコル
Table 7　Protocols in Multi-Vector Attacks.

	同時発生型攻撃			間欠型攻撃		
	UDP	TCP	組合せ	UDP	TCP	組合せ
1	udp123 (64.07%)	tcp80 (40.67%)	udp123&tcp80 (27.86%)	udp123 (61.29%)	tcp80 (42.69%)	udp123&tcp80 (29.18%)
2	udp389 (16.99%)	tcp8403 (24.23%)	udp123&tcp8403 (17.27%)	udp389 (14.37%)	tcp8403 (5.97%)	udp389&tcp80 (5.72%)
3	udp11211 (6.13%)	tcp25461 (3.34%)	udp389&tcp8403 (5.85%)	udp11211 (10.70%)	tcp443 (4.60%)	udp11211&tcp80 (3.92%)
4	udp5093 (2.79%)	tcp22 (2.51%)	udp389&tcp80 (5.57%)	udp111 (1.80%)	tcp22 (1.80%)	udp123&tcp8403 (2.86%)
5	udp9987 (2.51%)	tcp443 (2.51%)	udp11211&tcp80 (2.79%)	udp9987 (1.31%)	tcp8080 (1.24%)	udp123&tcp443 (2.68%)

表 8　複数のリフレクタによる同時発生型マルチベクタ攻撃
Table 8　Example of Concurrent Multi-Vector Attack by Distributed Reflectors.

標的 IP	攻撃種別	観測時刻	観測点	UDP 攻撃プロトコル	TCP 攻撃プロトコル
X	同時発生型	2018/6/14 4:30	Darknet，ハニーポット A	udp123	tcp80
X	同時発生型	2018/6/14 4:30	Darknet，ハニーポット B	udp123	tcp80

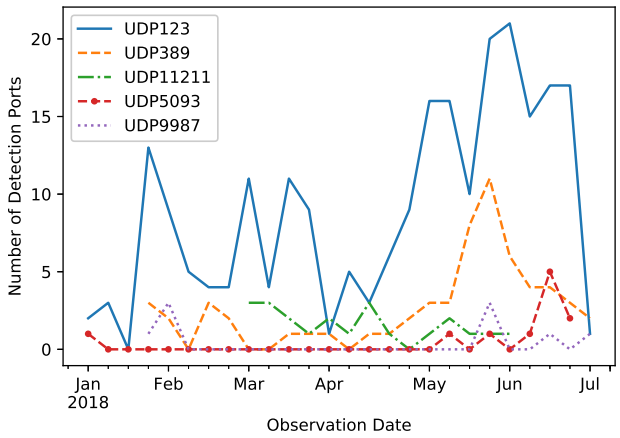

図 5　同時発生型攻撃における UDP プロトコルの推移
Fig. 5　Trend of UDP Protocol in Concurrent Attack.

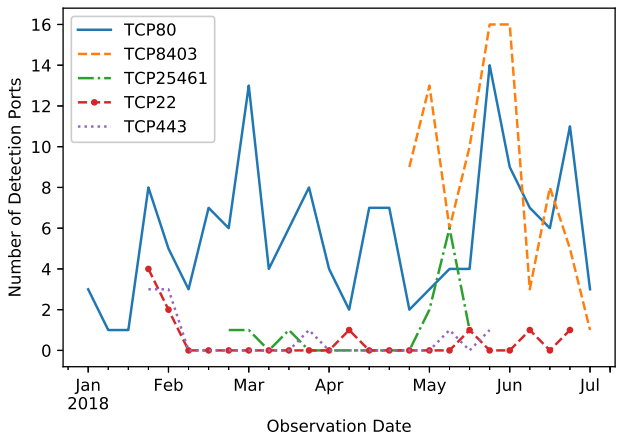

図 6　同時発生型攻撃における TCP プロトコルの推移
Fig. 6　Trend of TCP Protocol in Concurrent Attack.

複数の UDP プロトコルを用いた同時発生型マルチベクタ攻撃の検知例を**表 9** に示す．本攻撃では，udp123，udp389 とハニーポットごとに異なる UDP プロトコルが攻撃に使用された．tcp80 へのリソース消費型攻撃を実施しつつ，異なるプロトコルのリフレクタを用いることで，攻撃の成功率を高めたマルチベクタ攻撃と推測される．

4.2.2　間欠型攻撃の検知結果

24 時間に観測された同一 IP に対する攻撃は，間欠型マルチベクタ攻撃の可能性がある．同攻撃における標的ホストは，1 日平均 5.65IP，1 ヶ月平均 137.50IP であった．ハニーポットで観測したプロトコル及び Darknet で観測したプロトコルは，観測区間 5 分間時と概ね同様であったが，検知数及び使用プロトコルの増加が確認された．

間欠型攻撃の検知例を**表 10** に示す．本攻撃では，標的ホストに対して数日間，プロトコルを変更しながら攻撃が継続されている．

4.2.3　同一標的型攻撃の検知結果

標的ホストと見られる IP アドレスのドメイン情報を比較し，マルチベクタ攻撃を受けやすい FQDN の有無を分析した．標的ホストには同時発生型攻撃の標的 IP アドレスを，FQDN の参照には Virus Total の Passive DNS 情報を使用した．結果を**表 11** に示す．Virus Total の照会結果に対して，2 式により悪性スコアを求め，悪性スコア > 0 の IP を悪性ホスト，悪性スコア ≤ 0 の IP を良性ホストとして定義した．悪性情報件数及び良性情報件数は，標的 IP の照会結果に含まれる**表 12** の情報の件数を表す．

$$\text{悪性スコア} = \text{悪性情報件数} - \text{良性情報件数} \times 3 \quad (2)$$

Passive DNS に登録されていたホスト 151 件は全てユニークな FQDN と紐付いており，共通する FQDN を標的とした攻撃は確認できなかった．悪性スコアに基づき IP を判定した結果，29IP(検知した標的 IP の 14.57%) が悪性ホストと判定された．悪性スコア判定よりも誤検知の可能性は高くなるが，悪性登録件数 > 0 を悪性ホストとした場合の悪性ホスト数は 61IP(30.65%) であった．

表 9　複数の UDP プロトコルによる同時発生型マルチベクタ攻撃
Table 9　Example of Concurrent Multi-Vector Attack by Multiple UDP Protocols.

標的 IP	攻撃種別	観測時刻	観測点	UDP 攻撃プロトコル	TCP 攻撃プロトコル
Y	同時発生型	2018/1/23 23:40	Darknet，ハニーポット A	udp123	tcp80
Y	同時発生型	2018/1/23 23:40	Darknet，ハニーポット B	udp389	tcp80

表 10　間欠型マルチベクタ攻撃
Table 10　Example of Intermittent Multi-Vector Attacks.

標的 IP	攻撃種別	観測時刻	観測点	UDP 攻撃プロトコル	TCP 攻撃プロトコル
Z	間欠型	2018/3/27	Darknet，ハニーポット A	udp11211，udp123，udp389	tcp0，tcp80
Z	間欠型	2018/3/29	Darknet，ハニーポット A	udp123，udp389	tcp80，tcp8600
Z	間欠型	2018/3/30	Darknet，ハニーポット A	udp123	tcp8600
Z	間欠型	2018/4/1	Darknet，ハニーポット A	udp123，udp389	tcp8600
Z	間欠型	2018/4/2	Darknet，ハニーポット A	udp123	tcp8600，tcp9987
Z	間欠型	2018/4/3	Darknet，ハニーポット A	udp123	tcp80，tcp8600
Z	間欠型	2018/4/4	Darknet，ハニーポット A	udp11211，udp123，udp389	tcp8600

表 11　同一標的型攻撃の検知結果
Table 11　Result of Service-Based Detection.

種別	件数	比率
標的ホスト	199	100%
未登録ホスト	48	24.12%
登録ホスト	151	75.88%
重複する FQDN	0	0.00%
良性ホスト	170	85.43%
悪性ホスト	29	14.57%

表 12　ホストの判定に使用する情報
Table 12　Information to Classify Host Type.

種別	情報名
良性情報	undetected_downloaded_samples
	undetected_communicating_samples
	undetected_referrer_samples
悪性情報	detected_urls
	detected_downloaded_samples
	detected_communicating_samples
	detected_referrer_samples

5. 考察

5.1 攻撃傾向に関する考察

観測期間内の各プロトコルの傾向から，帯域幅消費型攻撃では udp123 が，リソース消費型攻撃では tcp80 が最も使用されるものの，udp11211，tcp8403 の急増などが観測された．このことから，マルチベクタ攻撃においても攻撃者は，時事の脆弱性，高効率の攻撃手法などを採用しているものと推測される．

加えて，検知した攻撃の中には，表 9 に示したように NTP 及び CLDAP などの複数のプロトコルによる同時攻撃や，ハニーポットごとに異なるプロトコルを使用している状況も確認できた．攻撃者は，目的や状況に応じて，プロトコルやリフレクタなどを使い分けている可能性がある．

5.2 同時発生型攻撃及び間欠型攻撃の相違に関する考察

使用されるプロトコルに大きな違いは見られず，使用率上位のプロトコルはほぼ同様であった．対して，攻撃の標的ホスト数では，同時発生型攻撃よりも間欠型攻撃が多いという結果になった．このことから，時間差を設けてマルチベクタ攻撃を実行する攻撃者が多い可能性がある．特に観測区間 1 時間以内における標的 IP 数が全標的 IP 数の 60%程度であったことから，1 時間以内に再度攻撃を実施する攻撃者が多い可能性も考えられる．

その他の差異として，一度の攻撃に使用される TCP 及び UDP プロトコルの数も間欠型攻撃がより多い傾向にあることを確認した．表 10 に示したように間欠型攻撃では複数の UDP，TCP プロトコルが併用される．同時発生型攻撃においても複数のプロトコルを使用するケースは確認されたが，攻撃者の目的が異なる可能性がある．同時型攻撃が瞬間的な負荷上昇のために複数プロトコルを使用するのに対し，間欠型攻撃では時間差かつ攻撃プロトコルの適宜変更により攻撃検知を遅らせるためだと推測される．

5.3 悪性ホストへの攻撃に関する考察

同一標的型攻撃に関する実験結果から，同一の FQDN を対象とする攻撃を確認することはできなかった．一方で，表 11 に示したようにマルチベクタ攻撃の標的として検知したホストのうちの約 14%が悪性ホストであることが判明した．誤検知の可能性を考慮したとしても，悪性ホストを標的としたマルチベクタ攻撃が実行されている可能性は高い．このことから，マルチベクタ攻撃においても攻撃者相互での攻撃活動は行われており，悪性ホストという一つのカテゴリも同一標的型攻撃の対象となり得ると推測される．

5.4 検知効果に関する考察

実験結果から，提案手法により同時発生型攻撃及び間欠型攻撃の検知に成功した．検知した標的ホスト数は 1 日あたり 2 件程度，ハニーポットで検知した攻撃内のマルチベクタ攻撃の比率は 0.2%程度であった．今後，さらなるマルチベクタ攻撃の検知を目指す場合，2 つのアプローチが想定される．

1 点目は，標的情報の多角的検討である．同一標的サービス型攻撃で取り上げた FQDN など個々の IP アドレス以外に着目することにより，マルチベクタ攻撃の検知率が上昇すると考えられる．

2 点目は，分析対象の拡張である．本稿では，Darknet 及びハニーポットに相関する攻撃のみを検知対象としたが，ハニーポットのみ，Darknet のみの観測結果においても，複数プロトコルによるマルチベクタ攻撃を確認した．したがって，Darknet 及びハニーポットの個別の観測結果に対して提案手法を適用することでも，新規のマルチベクタ攻撃を検知できると推測される．

以上 2 点の検討によって，検知効果の向上が期待できる．

5.5 運用に関する考察

攻撃検知結果のデータベース，検知システムなどへの反映を考慮する場合，検知精度及び即時性が重要となる．検知精度に関しては，同時型攻撃検知よりも間欠型攻撃検知により検知される攻撃が多いことが判明した．一方、即時性に関しては，数分単位での検知となる同時発生型攻撃検知が優れている．双方の検知結果は利点が異なるため，検知処理を並列化させ，複数の検知結果を利用することで，高精度かつ即時の攻撃検知が可能となる．

検知結果の活用方法としては，同時発生型攻撃のアラートを元にリアルタイムの対策を講じつつ，間欠型攻撃のアラートを元に数時間後に発生する攻撃に備えるといったものが考えられる．

6. おわりに

複数の攻撃手法を併用した DDoS 攻撃であるマルチベクタ攻撃は脅威となっている．本稿では，帯域幅消費型攻撃及びリソース消費型攻撃を併用したマルチベクタ攻撃の早期検知を目的として，Darknet 及びハニーポットの観測結果の相関分析によるマルチベクタ攻撃検知手法を提案した．評価実験により，リソース消費型攻撃と帯域幅消費型攻撃が同時または間欠的に発生していることの観測に成功した．特に間欠型攻撃は 1 時間以内に別手法による攻撃が発生する可能性が高いことが判明した．したがって，実網での DDoS 攻撃対策においては，一つの DDoS 攻撃を検知・防御した後も，次の攻撃への対策に取り組むことが重要である．また，検知した攻撃の 14%は悪性判定されている IP アドレスへの攻撃であり，攻撃者相互における攻撃を検知した可能性がある．今後は，検知精度の向上，機能拡張などを目指すこととする．

参考文献

[1] AkamaiTechnologies: akamai's [state of the internet] /security Q3 2016 report, Akamai.com (online), available from ⟨https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf⟩ (accessed 2017-08-15).

[2] York, K.: Dyn Statement on 10/21/2016 DDoS Attack, Dyn.com (online), available from ⟨https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack⟩ (accessed 2017-08-15).

[3] skottler: February 28th DDoS Incident Report, GitHub Engineering (online), available from ⟨https://githubengineering.com/ddos-incident-report/⟩ (accessed 2018-08-14).

[4] Verisign: Types of DDoS Attacks, Verisign (online), available from ⟨https://www.verisign.com/en_US/security-services/ddos-protection/types-of-ddos-attacks/index.xhtml⟩ (accessed 2018-08-14).

[5] Durumeric, Z., Bailey, M. and Halderman, J. A.: An Internet-Wide View of Internet-Wide Scanning, *Proc. 23rd USENIX Security Symposium (USENIX Security 14)*, USENIX Association, pp. 65–78 (2014).

[6] 深澤成孝， 佐藤直：ダークネットトラフィックの相関分析，研究報告マルチメディア通信と分散処理（DPS），Vol. 2015, No. 20, pp. 1–7 (2015).

[7] Krämery, L., Kruppy, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K. and Rossow, C.: AmpPot: Monitoring and Defending Against Amplication DDoS Attacks, *Research in Attacks, Intrusions, and Defenses. Lecture Notes in Computer Science*, Vol. 9404, pp. 615–636 (2015).

[8] 牧田大佑，吉岡克成， 松本勉，中里純二，島村隼平，井上大介：DNS アンプ攻撃の事前対策へ向けた DNS ハニーポットとダークネットの相関分析，情報処理学会論文誌，Vol. 56, No. 3, pp. 921–931 (2015).

[9] 西添友美，牧田大佑，吉岡克成， 松本勉：プロトコル非準拠のハニーポットによる DRDoS 攻撃の観測，*SCIS2015 The 32nd Symposium on Cryptography and Information Security* (2015).

[10] JUN, L. and KENSUKE, F.: An Evaluation of Darknet Traffic Taxomony, *Journal of Information Processing*, Vol. 26, pp. 148–157 (2018).