Computer Security Symposium 2017
23 - 25 October 2017

変化点検知を用いた新種スキャンの早期発見手法の検討

山村 翔[1]　熊谷 充敏[2]　神谷 和憲[2]　倉上 弘[2]

概要：近年，DDoS 攻撃の大規模化が著しい．その一因として，攻撃者が公開サーバ，IoT 機器などの有する脆弱性を突き，攻撃拠点を拡大していることがあげられる．攻撃拠点の拡大にあたっては，インターネットに接続されている機器に対して，脆弱性の探索活動（スキャン）が発生する．この中で，新種のスキャンを検知することは，攻撃者の行う新たな DDoS 攻撃を早期に防止する観点から重要である．本稿では，複数拠点に設置したハニーポットから取得したログ情報に対し，変化点検知手法を適用することにより，新種のスキャンを検知する手法を提案する．評価実験の結果，提案手法は，DDoS 攻撃に関係した新種スキャンの検知においても有効であることを確認した．

キーワード：スキャン検知，変化点検知，ハニーポット

Discovering New Type of Network Scan in Early Stage by Change-Point Detection

Natsuru Yamamura[1]　Atsutoshi Kumagai[2]　Kazunori Kamiya[2]　Hiroshi Kurakami[2]

Abstract: In recent years, the volume of DDoS attack is remarkably increasing due to the fact that attackers find vulnerable servers and IoT devices to exploit them as DDoS attack sources. To defend potentially vulnerable servers and IoT devices from exploiting, it is important to catch up new type of vulnerability scans from attackers as soon as possible. In this paper, we propose a method of detecting new type of scans by applying change-point detection algorithm to analyze honeypot logs. Evaluation result shows that proposed method is possible to find unknown TCP scans and UDP scans which are turned out to be new type of vulnerability scans and potentially linked to another DDoS attack.

Keywords: Scan Detection, Change-Point Detection, Honeypot

1. はじめに

近年，サイバー攻撃は大規模化・巧妙化の傾向にある．特に DDoS 攻撃は，その攻撃規模が過去 5 年間で 12.33 倍に拡大しているとの報告 [1] がある．攻撃規模の急激な拡大の背景には，攻撃者が公開サーバ，IoT 機器などの有する脆弱性を突き，攻撃拠点を拡大していることが挙げられる．

公開サーバの脆弱性を利用した攻撃としては，DNS，NTP などのプロトコルを対象とした反射（リフレクション）攻撃が代表的である．同攻撃は，送信元情報を偽装し公開サーバに名前解決等の要求（リクエスト）を行った場合，応答（レスポンス）パケットが偽装された送信元に返信される仕組みを悪用する．応答パケットサイズは，要求パケットサイズの数十倍から数百倍 [2] に及ぶことから，同攻撃は増幅（アンプ）攻撃とも呼ばれる．攻撃者は複数の公開サーバを利用することで，簡易に大規模の DDoS 攻撃を実行可能となる．

IoT 機器の脆弱性を利用した攻撃としては，IoT 機器を不正に操作し，攻撃対象に大規模攻撃を仕掛けるもの [3] がある．IoT 機器は，処理能力等の制限から高度なセキュリティ機能の実装が難しい上，初期状態の ID，パスワードのままインターネットに接続されている機器も多数存在す

[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

ることから攻撃の対象になりやすい．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 [4]，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 [5] などが報告されている．これらの攻撃では，Mirai マルウェアに感染した数十万台の IoT 機器が攻撃拠点として使用された．

前述のような公開サーバ，IoT 機器などの有する脆弱性を突き，攻撃拠点として利用する攻撃では，攻撃者は予め新たな攻撃拠点となり得る機器を発見する必要がある．そこで，攻撃者はインターネットに接続した機器に対し，脆弱性の探索活動（スキャン）を実施する．

スキャンを早期に発見することは，その後発生する DDoS 攻撃への迅速な対策につながる．中でも，新種のスキャンを早期に検知することは，攻撃者が行う新たな DDoS 攻撃の防止の観点から重要である．新種のスキャンに関しては，未知の脆弱性を利用する可能性が高く，対策まで時間を要することから，発見の遅れが被害の拡大に直結する可能性がある．

本稿では，複数拠点に設置したハニーポットのログ情報に対し，変化点検知手法の適用により，新種スキャンを検知する手法を提案する．また，評価実験の結果から，提案手法が新種の可能性のあるスキャンの早期検知に有効であることを示す．

なお，本稿でいう新種スキャンとは，ポート番号レベルでの新たなアクセス傾向を有し，新たな攻撃との関係性が推測されるスキャンを指す．

2. 既存研究

ネットワークスキャンの分類で代表的な研究は，Darknet のトラフィック分析を行った Durumeric らの論文 [6] である．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．ハニーポットを使用したネットワークスキャンの研究としては，Krämery らの研究 [7] がある．複数のハニーポットの観測により，リフレクション DDoS 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．

新種の攻撃検知の研究では，西添らの新種 DDoS 攻撃検知の検討 [8]，鐘らの新種 Web スキャンの検知の検討 [9] がある．

3. 変化点検知

3.1 概要

変化点検知は，異常検知の一種である．異常検知は，複数の入力情報の中から正常値に含まれない事象，イベント等を検知する手法全般を指すが，その中で，変化点検知は，入力された時系列情報の異常を検知することができる．時系列情報に対する他の検知手法としては，外れ値検知がある．外れ値検知は，全体のデータから逸脱したデータ値を

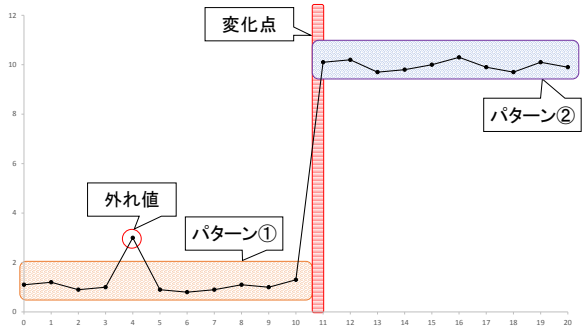

図 1 外れ値及び変化点のイメージ
Fig. 1 Image of Outlier and Change Point.

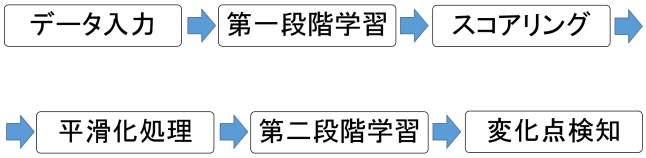

図 2 Change Finder の流れ
Fig. 2 Flow of Change Finder Method.

外れ値として検知する．外れ値検知では，入力に含まれるノイズを検知することはできるが，攻撃の増加などの変化を検知することに適していない．対して，変化点検知は，入力データのパターン（増加，減少などの傾向）が変化した時点を検知する．この特性から，攻撃の増加や，機器障害の増加などの変化を検知することに適している．そこで，著者らは，同手法が新種スキャンの検知においても適していると考えた．外れ値及び変化点のイメージを図 **1** に示す．

変化点検知では，パターンの変化を検知するために，予測モデルを定義し，予測モデルと入力データとの差異が増加した際，変化点として検知する．そのため，変化点検知の精度は，予測モデルの精度に依存する．本研究では，検知精度及び処理時間を両立した Change Finder を採用した．

3.2 Change Finder

Change Finder は，山西ら [10] により提案された手法であり，二段階学習と SDAR（Sequentially Discounting Auto Regressive learning）アルゴリズムにより，従来の AR モデル（Auto Regressive Model）を適用した手法と比較し，計算時間の短縮，非定常データへの対応，オンライン処理などの特徴を有する．変化点検知の流れを図 2 に示す．

3.2.1 SDAR アルゴリズム

Change Finder では，忘却学習アルゴリズム（SDAR アルゴリズム）により，AR モデルのパラメータを推定する．推定方法を以下に示す．

$$I = \sum_{i=1}^{t} (1-r)^{t-i} log P(x_i | x^{i-1}, \theta)$$

$\theta = (A_1, ..., A_k, \mu, \Sigma)$ とし，r は忘却パラメータ，A は AR モデルのパラメータ，k は AR モデルの次数，Σ はホワイトノイズを表す．忘却パラメータ r，AR モデルの次数 k を仮定し，t 番目の入力データ x_t が与えられたとき，I が最大となるパラメータ θ を推定する．

3.2.2 第一段階学習

入力された時系列データから AR モデルを定義し，SDAR アルゴリズムでパラメータの学習を行い，時系列データの外れ値スコアを算出する．外れ値スコア算出の計算式を以下に示す．

$$Score(x_t) = -logP_{t-1}(x_t|x^{t-1})$$

P_t は SDAR アルゴリズムにより求めた確率密度関数であり，P_t が低いほど予測値から外れていることを示す．すなわち，P_t が低ければ外れ値スコア $Score(x_t)$ が高くなり，外れ値である可能性が高い．

3.2.3 外れ値スコアの平滑化

第一段階学習により求めた外れ値スコアに対し，一定時間 T（以下，平滑パラメータという．）ごとに移動平均による平滑化処理を行う．平滑化処理の計算式を以下に示す．

$$y_t = \frac{1}{T}\sum_{i=t-T+1}^{t} Score(x_i)$$

T が大きいほど，外れ値と変化点の識別精度が高まるが，識別までの時間経過が大きくなる．

3.2.4 第二段階学習

前述の外れ値スコアを平滑化したものに対し，再度 SDAR アルゴリズムにより算出したスコアを変化点スコアとする．これにより，外れ値の影響を低減し，変化点の検知精度を向上させる．

3.2.5 変化点検知

算出された変化点スコアが大きいほど，変化点の可能性が高いことを表し，スコアが一定の閾値を超えた時点を変化点として検知する．

4. 提案手法

提案手法は，複数拠点に設置したハニーポットのログ情報に対し，変化点検知手法の適用により，アクセス傾向の変化を抽出し，新種の可能性のあるスキャンを検知するものである．提案手法の処理の流れを**図 3** に示し，以下に各機能の概要を述べる．

4.1 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．ハニーポットは**表 1** に示す 2 種類を使用した．ハニーポット 1，ハニーポット 2 は，上位レイヤのプロトコルには依存せず，UDP または TCP の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．特に

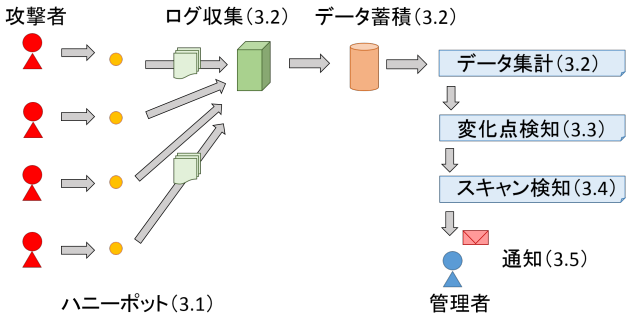

図 3 提案手法の流れ
Fig. 3 Flow of Proposed Method.

表 1 ハニーポットの条件
Table 1 Conditions of Honeypots.

ハニーポット名	動作条件
ハニーポット 1	UDP 応答有
ハニーポット 2	TCP 応答有

ハニーポット 2 に関しては，リフレクション型 DDoS 攻撃を引き込む可能性があるため，西添らの論文 [11] を参考に実装した．このように異なる条件のハニーポットから収集したログ情報を使用することで，特定の通信プロトコルの脆弱性を標的としたアクセス等を網羅する．

4.2 ログ情報の収集及び集計

データ分析にあたり，はじめにハニーポットの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，通信プロトコル，送信元 IP アドレス，送信元組織，送信元国，送信先ポート番号，アクセス数，アクセス日時，単位時間あたりの受信パケット数（以下，ppm という．），ハニーポット名を選定した．情報の概要を**表 2** に示す．ハニーポット名や ppm ついては，ハニーポットごとのアクセス傾向の比較や，スキャンと DoS 攻撃を識別する目的で分析対象に含めた．

続いて，**表 3** に示すように各ハニーポットごとに通信プロトコル，送信先ポート番号のアクセス数，ppm の最大値を集計し，変化点検知手法を適用するための時系列データを作成する．なお，検知後，送信元の関係性を確認するために，送信先ポート番号へのアクセスに含まれる送信元組織名，送信国名等の送信元情報を付与した．

4.3 Change Finder の適用による変化点検知

4.2 節で作成した時系列データを入力とし，Change Finder により，変化点スコアを算出する．変化点スコアが高い入力データは，新規のアクセスを示すものか，アクセス数が急激に増減したものである可能性が高い．新規のアクセスであれば，既存のアクセスとは異なる新たな攻撃の可能性がある．また，既存のアクセスの急増であっても，攻撃者の攻撃傾向が変化した可能性があり，共に新種の攻撃の兆

表 2　分析対象とするログ情報
Table 2　Honeypot Logs for Analyzing New Type of Network Scans.

名称	概要
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.
送信元組織名	送信元 IP アドレスから推定した当該アクセスの送信元組織.
送信元国名	送信元 IP アドレスから推定した当該アクセスの送信元国.
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.
アクセス日時	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.
ppm(packets per minute)	1 回のアクセスにおいて 1 分間に受信したパケット数.
ハニーポット名	当該アクセスを観測したハニーポット.

表 3　集計データの例
Table 3　An Example of Aggregated Data.

ハニーポット名	送信先ポート番号	アクセス日時	アクセス数	ppm の最大値	送信元情報
ハニーポット 1	TCP22	2017 年 1 月 1 日	23	4	...
	UDP53	2017 年 4 月 4 日	993	67,000	...
ハニーポット 2	TCP80	2017 年 2 月 5 日	37	3	...
	UDP1900	2017 年 7 月 19 日	110	49	...

候を検知できる可能性がある.

Change Finder のスコア計算では，前述のデータセットのほか，忘却パラメータ，AR モデル次数，平滑パラメータの設定が必要となり，各パラメータの設定値が変化点スコアの結果に影響を及ぼす.

以上により，算出した変化点スコアのうち，設定した閾値を超過したものを変化点として検知する．閾値が必要以上に高い場合は見逃しが，低い場合は誤検知が増加する．そのため，閾値の設定が検知精度に影響を及ぼす.

4.4　スキャンの検知

Change Finder の適用により変化点，すなわち，新種の可能性のある攻撃や攻撃傾向の変化を検知できる．ただし，ハニーポットへのアクセスには，DoS 攻撃も含まれており，提案手法の目的である新種スキャンの検知を実現するためには，検知した変化点から DoS 攻撃とスキャンを識別する必要がある．そこで，前述の ppm により，入力データの ppm が高ければ DoS 攻撃と，低ければスキャンと判定する処理を行う．同処理においては，ppm の閾値の設定により，DoS 攻撃とスキャンの識別精度が変化する．これにより，スキャンのみの検知が可能となる.

4.5　検知後の処理

スキャン検知後の対処として，メールにより管理者に通知する．最終的には，侵入防御システムやファイアウォールなどのセキュリティ製品と連携した自動対処が望ましいが，現段階では，誤検知の可能性を排除できないことから，通知により管理者の判断を支援することとした.

4.6　提案手法の実装について

ログ情報データベースとして，全文検索エンジン Elastic Search を使用し，Elastic Search API によりデータ集計機能を実装した．また，変化点スコアの算出機能については，Python の Change Finder ライブラリ [12] を採用することとした．最後に，検知結果の通知については，検知結果をレポート化し，メールにより送付する機能を実装した.

5.　評価実験

5.1　実験条件

4 章で構築したシステムにより，データセットの条件を**表 4**，実験の各パラメータを**表 5** のとおりに設定し，評価実験を実施した．表 4 中の①，②は，それぞれハニーポット 1 及びハニーポット 2 のアクセス数を表す.

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	2016 年 8 月 1 日～2017 年 7 月 31 日
アクセス数	4,091,490 (①1,679,607，②2,411,883)

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
集計	集計間隔	1 日
Change Finder	忘却パラメータ	0.02
	AR モデル次数	1
	平滑パラメータ	7
変化点検知	変化点スコア閾値	20
スキャン検知	ppm 閾値	10

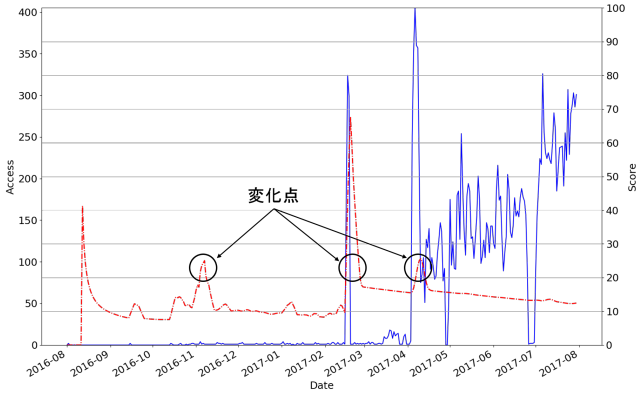

図 4　UDP389 に対する変化点検知結果
Fig. 4　Detection Result of UDP389.

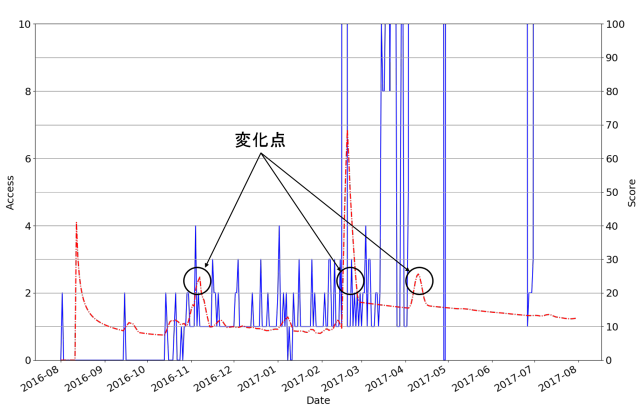

図 5　UDP389 に対する変化点検知結果を拡大したもの
Fig. 5　Deitail Figure of UDP389 Detection Result.

5.2　実験結果

表 5 の設定で実施した実験において，顕著な結果が得られた通信プロトコル，ポート番号へのアクセスを示す．各図において，左の縦軸はアクセス数，右の縦軸は変化点スコア，横軸はアクセス日時を表す．また，図中の実線はアクセス数を，破線は算出した変化点スコアを表す．

5.2.1　UDP389

ハニーポット 1 のログ情報において，UDP389 番ポート宛てのスキャンの増加を検知した結果を**図 4** に示す．アクセス数は，2 月 16 日及び 4 月 4 日に急増し，変化点スコアでは，11 月 4 日〜8 日，2 月 16 日〜25 日，4 月 7 日〜13 日の 3 つの時期に閾値を超えている．11 月については，**図 5** に示すとおり，アクセス数は少ないがスキャンが到来している．

UDP389 については，コネクションレス LDAP（CLDAP）を悪用したリフレクション攻撃 [13], [14] が報告されており，ハニーポットで取得したパケットが CLDAP のリクエストパケットであったことからも，UDP389 に関する実験結果で検知した変化点は，同攻撃に関係するスキャンの可能性がある．実際，ハニーポット 1 では，このスキャン検知の後，CLDAP を用いた DoS 攻撃を観測している．

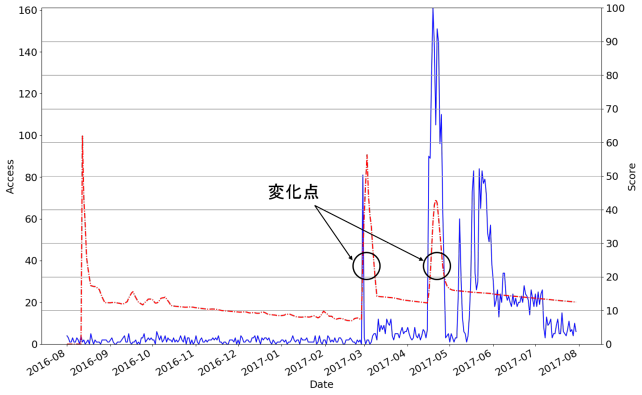

図 6　TCP81 に対する変化点検知結果
Fig. 6　Detection Result of TCP81.

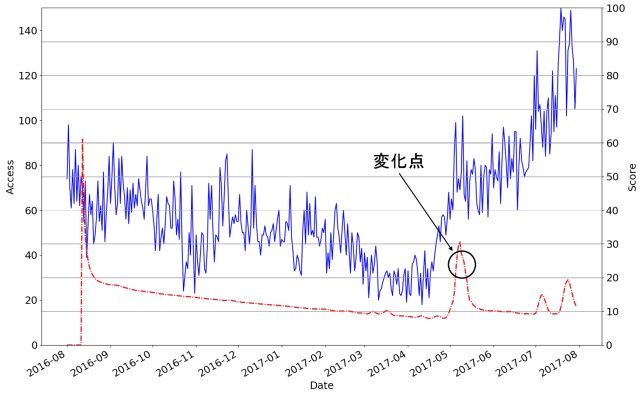

図 7　TCP445 に対する変化点検知結果
Fig. 7　Detection Result of TCP445.

5.2.2　TCP81

ハニーポット 2 のログ情報において，TCP81 番ポート宛てのスキャンの増加を検知した結果を**図 6** に示す．アクセス数が 2 月 28 日，4 月 16 日に急増し，変化点スコアは，2 月 28 日〜3 月 8 日，4 月 17 日〜27 日の 2 つの時期に閾値を超えている．

TCP81 については，同時期に IP カメラ等の脆弱性を標的としたマルウェア「PERSIRAI」に関係するアクセス [15] が報告されており，本攻撃に関するスキャンを検知した可能性がある．PERSIRAI は感染後各種 DDoS 攻撃を実施することから，前兆となるスキャンの検知は，DDoS 攻撃の阻止において有効である．

5.2.3　TCP445

ハニーポット 2 のログ情報において，TCP445 番ポート宛てのスキャンの増加を検知した結果を**図 7** に示す．アクセス数については，4 月中旬より増加傾向にあり，5 月 5 日に急増し，変化点スコアは，2017 年 5 月 5 日〜12 日の時期に閾値を超えている．

TCP445 については，4 月以降に「WannaCry」等の複数のマルウェアで利用される SMB の脆弱性を標的としたアクセスの増加 [16] が報告されており，同攻撃に関するスキャンを検知した可能性があるが，関連性については十分

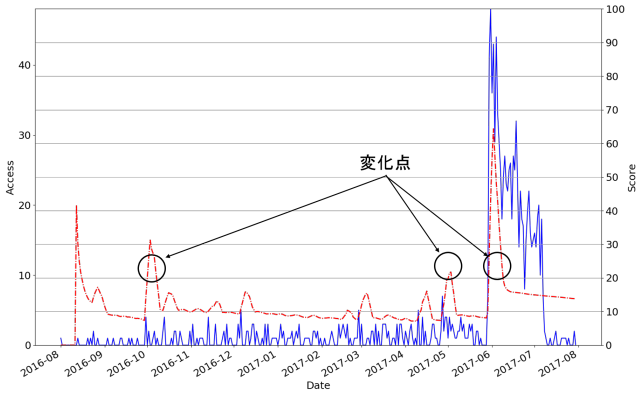

図 8　TCP9000 に対する変化点検知結果
Fig. 8　Detection Result of TCP9000.

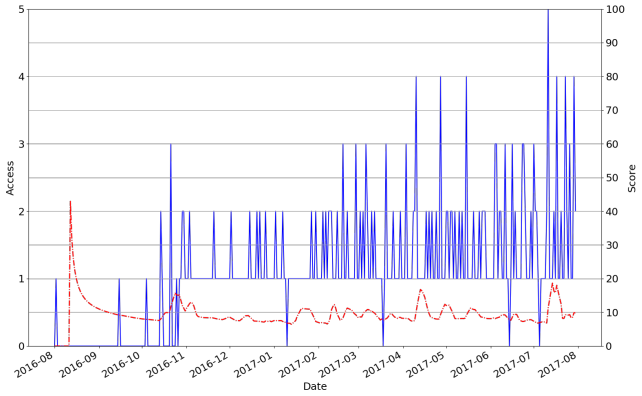

図 9　UDP389 におけるハニーポット変更時の影響
Fig. 9　UDP389 Detection Result in Different Honeypot.

確認されていない．この結果からは，早期スキャン検知により，必ずしも DDoS 攻撃には関連しないが，マルウェア感染のキャンペーンなどを観測できる可能性を示している．

5.2.4　TCP9000

ハニーポット 2 のログ情報において，TCP9000 番ポート宛てのスキャンの増加を検知した結果を**図 8** に示す．アクセス数については，5 月 30 日に急増し，変化点スコアは，2016 年 10 月 2 日〜6 日，2017 年 5 月 2 日〜3 日，5 月 30 日〜6 月 8 日の 3 つの時期に閾値を超えている．

TCP9000 については，海外製デジタルビデオレコーダの脆弱性を標的としたアクセス [18] が報告されており，同攻撃を検知した可能性がある．現在，TCP9000 のスキャンと DDoS 攻撃の関係性を示唆する報告はないが，今後，感染機器を悪用した DDoS 攻撃が発生する可能性は否定できない．

6.　考察

6.1　スキャンの検知効果

ハニーポット 1 及びハニーポット 2 のログ情報に対して，提案手法を適用した結果，UDP389，TCP81，TCP445，TCP9000 への攻撃に関係性のあるスキャンの検知が可能であった．これらの実験結果において，提案手法による検知時期は，関係機関の発見時期と概ね同時期であり，公表時期よりも数日から数ヶ月早いことを確認した．ここで，発見時期は各機関が最初にスキャンを観測した時期を，公表時期は注意喚起のため観測結果を発表した時期を表す．提案手法による検知時期と公開情報との比較を**表 6** に示す．

表 6　提案手法による検知時期と公開情報との比較
Table 6　Comparison between Detection Timing by Proposed Method and Public Information.

ポート番号	検知時期	発見時期	公表時期
UDP389	11 月 4 日	10 月中旬 [14]	11 月 29 日 [14]
TCP81	4 月 17 日	4 月 [15]	5 月 9 日 [15]
TCP445	5 月 5 日	4 月 19 日 [16]	5 月 15 日 [16]
TCP9000	5 月 30 日	5 月 29 日 [18]	7 月 31 日 [18]

以上の結果から，提案手法が新種攻撃のスキャンの早期検知において効果的であることを確認できた．

しかし，データセットやパラメータの設定条件によって，変化点検知の効果が変化する可能性があるため，追加実験を実施した．実験結果及び考察を以下に述べる．

6.2　ハニーポットの動作条件が及ぼす影響

ハニーポットの動作条件による検知への影響を検証するため，ハニーポット 1 の代わりにハニーポット 2 の UDP389 へのアクセスに対して，提案手法を適用した結果を**図 9** に示す．各ハニーポットの動作条件は表 5 のハニーポット条件のとおりである．ハニーポット 2 の結果では，UDP389 番ポートに対するアクセス数が少なく，変化点スコアは閾値を超えなかった．ハニーポット 1 と比べ，ハニーポット 2 のログ情報では，提案手法による検知が効果的ではなかった．原因としては，アクセス数が少ないためであると考えられる．ハニーポット 2 は，UDP アクセスへの応答を停止しており，CLDAP リフレクション攻撃への利用価値が低いことから，ハニーポット 1 ほどアクセスが増加せず，大きな変化が生じなかった可能性がある．

実験結果から，ハニーポットによって，ログ情報の傾向が異なり，提案手法の適用結果も異なることが確認できた．単一のハニーポットからのログ情報では，新種スキャンを検知できない可能性があり，可能な限り，異なる条件のハニーポットのログ情報を複合的に利用することが重要である．

6.3　Change Finder のパラメータ設定が及ぼす影響

Change Finder のパラメータを変更した際の検知への影響を検証するため，各パラメータを**表 7** のとおり変更し追加実験を実施した．忘却パラメータを変更した実験 I の結果を**図 10** に，平滑パラメータを変更した実験 II の結果を**図 11** にそれぞれ示す．

実験 I において，忘却パラメータを最大に設定した r=0.5

表 7　Change Finder パラメータの設定
Table 7　Parameter Setting of Change Finder.

実験名	パラメータ名	設定値
実験 I	忘却パラメータ	0.02, 0.1, 0.5
	AR モデル次数	1
	平滑パラメータ	7
実験 II	忘却パラメータ	0.02
	AR モデル次数	1
	平滑パラメータ	3, 7, 20

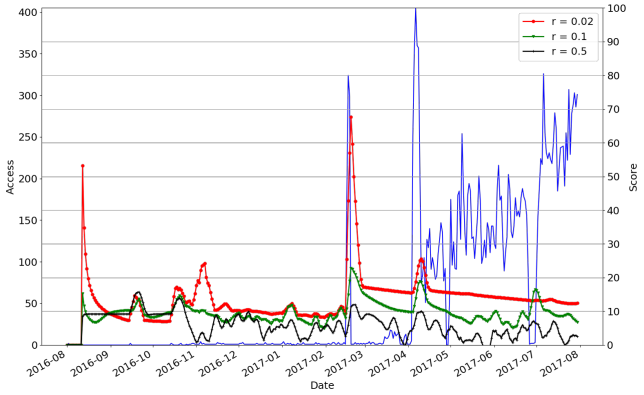

図 10　UDP389 における忘却パラメータ変更時の影響
Fig. 10　Difference in UDP389 Detection Result by Change Finder Parameter.

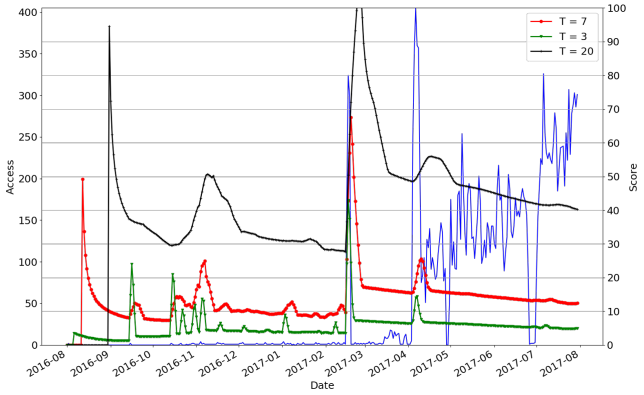

図 11　UDP389 における平滑パラメータ変更時の影響
Fig. 11　Difference in UDP389 Detection Result by Smoothing Parameter.

では，変化点スコアが全体的に低く，アクセス数の増減に対応し，細かく変動している．また，r=0.1 も r=0.02 と比べ，全体的なスコアが低い結果となった．

実験 II において，平滑パラメータを大きく設定した結果ほど，変化点スコアが高くなり，データセットに発生したごく短時間の増減（外れ値）の影響を受けやすいことが確認できた．一方で，設定値が大きいほど，検知時期が実際のアクセス数の変化よりも遅延している．

実験 I，II の結果から，忘却パラメータを高く設定した場合，変化点スコアが低下した上，外れ値の影響を受けやすくなることが判明した．今回の実験結果からは，検知精度を高めるためには，忘却パラメータを 0.1 未満に設定する必要があるといえる．

平滑パラメータを小さく設定した場合，スコアの低下及び外れ値の影響を受ける傾向が確認できた．ただし，高く設定した場合，検知時間の遅延が発生する可能性があるため，条件に応じて適切に設定する必要がある．

表 8　集計期間及び集計間隔の設定
Table 8　Parameter Setting of Aggregation Period and Aggregation Interval.

パラメータ名	設定値
集計期間	2017 年 4 月 1 日〜4 月 30 日
集計間隔	1 時間

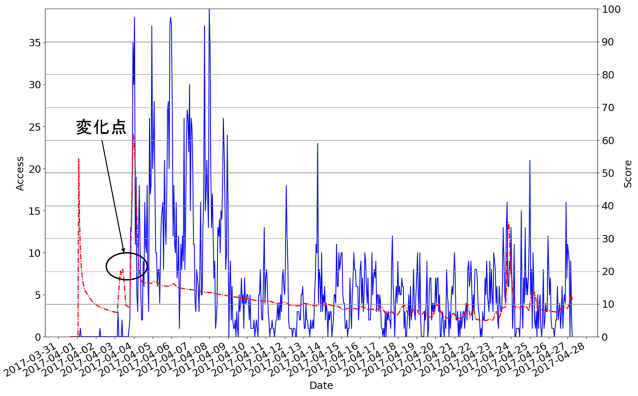

図 12　UDP389 に対する集計間隔変更時の検知結果
Fig. 12　UDP389 Detection Result in Different Aggregation Interval.

6.4　早期検知に関する考察

ここまでの実験において，スキャンを検知することはできたが，平滑化処理の影響により，実際のスキャン発生日時と検知日時の間に時間差が発生していた．今回の実験では，ハニーポットのログ情報を 1 日単位で集計していたため，時間差が 1 日〜3 日程度となった．

そこで，集計間隔の変更による検知への影響を検証するため，集計期間及び集計間隔を**表 8** の条件に変更し，実験を行った． 同実験における UDP389 番ポートへのアクセスに提案手法を適用した結果を**図 12** に示す．アクセスは 4 月 4 日 6 時から急増し，変化点スコアは 4 月 4 日 6 時において閾値を超えた．これは集計間隔を短時間に設定することで，検知日時の時間差を低減できることを示している．

以上の結果から，短期的なログからリアルタイムでの検知処理を実行する場合には，集計間隔を数分から数時間と短く設定することにより早期検知が可能となる．また，スキャンの有無が不明な場合は，はじめに集計間隔を数日単位で設定した検知により，スキャンの時期を絞り込み，その後，集計期間を短く設定し，再度検知することにより，正確な発生日時を特定する方法が効率的である．

6.5 運用に関する考察

試作システムについては，研究の一環として運用しており，過去 24 時間に検知した新種の可能性のあるスキャンのリストが，毎日管理者・研究者宛に送信される．ログ情報の集計から通知までの処理はハニーポット 1 台あたり 1 分以内で終了し，定期実行の負担も軽微である．スキャンの最終確認は目視だが，1 度に報告される新種スキャンの候補は概ね 10 件程度と目視により確認できる範囲であり，新たな攻撃兆候の分析に効果を発揮している．

また，日々の運用を通して，ChangeFinder を用いた検知において，以下のような場合に誤検知や見逃しが生じることが分かった．まず，元々アクセス数が少ないポート番号へのスキャンは，少量の増加であったとしても誤検知する可能性がある．次に，アクセス数が徐々に増加する場合，僅かな傾向変化を検知することができず見逃す可能性がある．最後に，トラフィックが急激に減少した場合も誤検知する可能性がある．提案手法においては，これらの制約が生じるため，現状では目視確認が必要である．

7. おわりに

DDoS 攻撃は近年大規模化しており，その背景には，攻撃者による攻撃拠点の拡大がある．本稿では，攻撃者が攻撃拠点を拡大するための公開サーバ，IoT 機器等を標的とした脆弱性のスキャン，特に新たな攻撃の前兆となる新種のスキャンの早期発見を目的とし，複数のハニーポットのログ情報に対する変化点検知手法の適用による新種スキャンの検知手法を提案した．さらに提案手法の評価実験により，新種スキャンの検知が可能であることを確認した．その一方で，分析対象となるログ情報の傾向や各種パラメータの設定値の影響により，誤検知や見逃しが発生するなどの課題も判明した．今後は，課題の解決と検知精度の向上を目指すこととする．

参考文献

[1] ArborNetworks: ARBOR NETWORKS' 12TH ANNUAL WORLDWIDE INFRASTRUCTURE SECURITY REPORT FINDS ATTACKER INNOVATION AND IOT EXPLOITATION FUEL DDOS ATTACK LANDSCAPE, ArborNetworks.com (online), available from ⟨https://www.abornetworks.com/arbor-networks-12th-annual-worldwide-infrastructure-security-report-finds-attacker-innovation-and-iot-exploitation-fuel-ddos-attack-landscape⟩ (accessed 2017-08-15).

[2] Rossow, C.: Amplification Hell: Revisiting Network Protocols for DDoS Abuse, *Proc. NDSS* (2014).

[3] 中里純二，牧田大佑，島村隼平，井上大介：ダークネット観測による IoT 機器の脅威，*2017 Symposium on Cryptography and Information Security* (2017).

[4] 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).

[5] 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).

[6] 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).

[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] 西添友美，牧田大佑，吉岡克成， 松本勉：プロトコル非準拠ハニーポットを用いた新種の DRDoS 攻撃の早期検知，電子情報通信学会技術研究報告，Vol. 116, No. 522, pp. 13–18 (2017).

[9] 鐘揚，折原慎吾，谷川真樹， 嶋田創， 村瀬勉，高倉弘喜，大嶋嘉人：URI の共起性検知に基づく Web スキャンの実態調査，電子情報通信学会技術研究報告，Vol. 115, No. 488, pp. 25–30 (2016).

[10] Takeuchi, J. and Yamanishi, K.: A Unifying Framework for Detecting Outliers and Change Points from Time Series, *IEEE Transactions on Knowledge and Data Engineering*, Vol. 18, No. 4, pp. 482–492 (2006).

[11] 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).

[12] Sunsuke, A.: changefinder, Argmax.jp (online), available from ⟨http://argmax.jp/index.php?changefinder⟩ (accessed 2017-08-14).

[13] AkamaiTechnologies: Threat Advisory: CLDAP Reflection DDoS, Akamai.com (online), available from ⟨https://www.akamai.com/jp/ja/multimedia/documents/state-of-the-internet/cldap-threat-advisory.pdf⟩ (accessed 2017-08-14).

[14] 警察庁：リフレクター攻撃の踏み台となる機器の探索行為と考えられるアクセスの増加等について，@police（オンライン），入手先 ⟨https://www.npa.go.jp/cyberpolice/important/2016/19552.html⟩（参照 2017-08-22）.

[15] TrendMicro: Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras, TrendLabs Security Intelligence Blog (online), available from ⟨http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/⟩ (accessed 2017-8-14).

[16] 警察庁：攻撃ツール「Eternalblue」をはじめとするソフトウェアの脆弱性を悪用した攻撃等と考えられるアクセスの観測について，@police（オンライン），入手先 ⟨https://www.npa.go.jp/cyberpolice/detect/pdf/20170525.pdf⟩（参照 2017-08-14）.

[17] JPCERT/CC: ランサムウェア"WannaCrypt" に関する注意喚起，JPCERT/CC（オンライン），入手先 ⟨https://www.jpcert.or.jp/at/2017/at170020.html⟩（参照 2017-08-14）.

[18] 警察庁：海外製デジタルビデオレコーダの脆弱性を標的としたアクセスの観測等について，@police（オンライン），入手先 ⟨https://www.npa.go.jp/cyberpolice/detect/pdf/20170731.pdf⟩（参照 2017-08-14）.