Vol.2018-DBS-167 No.3
Vol.2018-IFAT-132 No.3
2018/9/12

相関関係の変化を利用した内部ネットワークの異常検知手法

高畑 孝輝[1]　新美 礼彦[2]

概要：情報システムでは，マルウェアなどの動作により正常通信とは異なる通信が行われる場合がある．そのような通信に対して，近年，組織内部のネットワークに着目した内部対策が注目されている．本研究では，異常検知手法のひとつである密度比推定の相関変化検知を使用して，内部ネットワーク中の異常検知を行うことを提案する．実験では，正常データを加工し，攻撃を含んでいると想定した相関関係の変化部分を含んだデータを用意し変化検知を行い，変化部分を検知できることを確認した．

1. はじめに

監視している対象から自動的に異常を検知するという目的で異常検知研究がされている．異常検知の多くの手法では，正常とされているデータから確率分布などを用いて正常状態をモデル化し，新たに入力されたデータが正常からどれだけ離れているかを異常スコア値として算出し，予め定めた異常スコア値を超えた場合に異常として検知する．

異常検知研究の 1 つとして，構造変化検知という手法が提案されている．構造変化とはデータに内在する変数間の相関関係を抽出する手法であり，変数間の相関関係から正常状態を定義することによって，相関関係の崩れを異常スコアとして算出し，異常検知を行うことができる．

構造変化検知では，監視する変数を独立であると仮定した際に検出できないような変数間の関係を抽出することができ，同様に変数間の相関を利用した主成分分析と比較すると，どの変数同士の関係が崩れたかを行列として出力するので，検出後に原因を特定しやすい利点がある．

本論文では，このような異常検知をネットワークセキュリティの分野に適用し，内部ネットワークでの通信挙動の変化を，構造変化検知を用いて検出することを確認する．システムへの攻撃やマルウェアの動作には，機密情報の奪取，感染の拡大，踏み台とした DDoS 攻撃や SPAM メールの送信などを目的に，ネットワーク内部で通信を行う挙動をするものがある．そのような内部ネットワークでの通信から相関関係を持つようなトラフィックを想定し，相関変化検知によって異常検知ができるかを確認することが本論文の目的である．

論文構成について説明する．2 章では関連研究ついて記述し，3 章で提案手法を記述する．4 章では使用するデータセットへの処理と特徴分析について記述し，5 章では使用するデータセットに加工を加えたものに対して変化の検出を行う実験についてと結果の考察を述べる．最後に 6 章で結論を述べる．

[1] 公立はこだて未来大学大学院 システム情報科学研究科
Future University Hakodate, Graduate School of System Information Science
[2] 公立はこだて未来大学 システム情報科学部
Future University Hakodate, Faculty of System Information Science

2. 関連研究

構造変化検知についての研究と，内部ネットワークに着目した研究について記述する．また，密度比推定と密度比推定による構造変化検知について説明する．

2.1 内部ネットワークに注目した研究

内部ネットワークに着目した異常検知を行う手法は既に多数研究されている．

永山らは，内部ネットワークをグラフ構造と考えて，ホスト間の通信コミュニティ分析を行い，正常状態を作成し，正常状態との比較をすることで異常状態を検出するという研究を行っている [1]．arp 通信のみでグラフ構造を定義していることが特徴的である．また，井出らは，ネットワークの構造分析を，Web システムでのサーバ間のトラフィックに適用し，データベースサーバ，Web アプリケーションサーバとの通信頻度の分布変化により，サーバの異常部位を検出するという方法を提案している [2]．村上らは，ボットネットの協調通信により，ホスト同士の通信頻度の相関が変化することを想定し，ベイジアンネットを用いて検出することを提案している [3]．このように内部ネットワークに着目し，トラフィックからの分析を元にしたさまざまな手法が研究されている．

これら研究と同様のアプローチであるが，本論文ではホ

スト間の通信をホストを変数として扱うのではなく，通信の時系列データに含まれる HTTP 通信や DNS 通信のような相関関係を持ったデータを対象にする．

2.2 構造変化検知に関する研究

データの変数間の相関を抽出する最も簡単な手法として，データが正規分布に従っていると考え精度行列を求める手法がある．この手法では，標本から共分散行列を求め，その逆行列を計算することによって精度行列を求める．共分散行列の逆行列である精度行列は，変数間の直接的な相関を示すことが証明されているため，精度行列の変化を求めることによって構造変化検知を行う．

しかし，この手法は多くの場合，共分散行列が正則でなければ逆行列を求められないという問題や，精度行列の結果として出力される数値がどの数値から相関があると考えるかを閾値などで手動で決める必要があるという問題がある．

そこで，精度行列を直接求めると同時にできるだけ行列を疎に近づける手法としてグラフィカルラッソが提案されている [4]．グラフィカルラッソでは，精度行列の推定に L1 正則化を行うことによって疎な解を実現している．

グラフィカルラッソによる手法は，異常検知に使用する場合，2 つ標本から精度行列を求め，精度行列の差によって変化検出を行うが，精度行列の差を直接推定する密度比推定を用いた手法が Liu らによって提案されている [5]．この手法でも，精度行列の差分を直接推定し，グラフィカルラッソと同様に L1 正則化や Elastic Net によって疎な解を得る．

論文では，グラフィカルラッソと密度比推定を使い異常状態を検知する手法である．

2.3 密度比推定について

密度比推定とは，2 つの標本の確率密度関数の比を直接推定する手法のことを指す．

2 つの標本を $D = \{\boldsymbol{x}_1, ..\boldsymbol{x}_N\}$，$D' = \{\boldsymbol{x}'_1, ..\boldsymbol{x}'_N\}$ とし，それぞれのデータの元になる確率密度関数を $p_D(\boldsymbol{x})$，$p_{D'}(\boldsymbol{x})$ とする．ここで，式 (1) のように，確率密度関数の比を定義したときに，直接，密度比 $r(\boldsymbol{x})$ を求めるような推定法を密度比推定と呼ぶ．

通常，2 つの標本の確率密度関数の比を求める場合，まずそれぞれの標本から確率密度関数である $p_D(\boldsymbol{x})$，$p_{D'}(\boldsymbol{x})$ を推定し，2 つの推定された確率密度関数から比 $r(\boldsymbol{x})$ を求めるという手法をとる．この手法をとった場合，特に分母が 0 に近い値で誤差が発生した際に，比が大きく変化するという問題がある．そこで，比を直接推定することによって，このような比を計算する際の数値の変化が発生しないという利点がある．

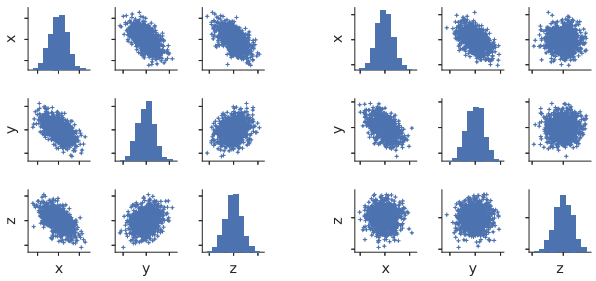
$$r(x) = \frac{p_D(\boldsymbol{x})}{p_{D'}(\boldsymbol{x})} \tag{1}$$

2.4 相関検知への応用

密度比推定による相関変化問題を解くことによって，2 つの異なる時刻のそれぞれのデータ標本から正規分布の精度行列の差を求めることができる．

例として図 1 のような 2 つの散布図行列を示す．左側の分布では，変数 x，変数 z の間に相関があるが，右の分布では相関がなくなっていることがわかる．このような相関の変化を，差分の形で直接求めることができる．

具体的には，それぞれの標本が正規分布から得られたデータと考え，正規分布の比を直接推定することによって，相関を得る手法を取る．この手法は正規分布の比と相関行列の比が比例していることを利用している．



変化前の相関　　変化後の相関

図 1 相関の散布図行列

3. 提案手法

本章では，グラフィカルラッソと密度比推定による構造変化を検知する異常検知手法を記述する．

3.1 手法の概要

本論文では，構造変化を相関関係の変化と考える．相関関係の変化を検出する手法を，ネットワークトラフィックの時系列データに含まれる相関のある変数群から，相関が崩れることを検出することに応用することによって，異常検知を行う手法を提案する．

3.2 手法の構成

提案手法の構成を簡易的に示すと，図 2 のようなスイッチングハブによって接続されるコンピュータ同士のネットワークを対象としている．スイッチングハブには，通信内容を集計して監視サーバに転送するプロトコルである SNMP や NetFlow を実装してる機器があり，それらの機器を使用することで，ネットワーク内部で動作するホストが行うトラフィックからスイッチングハブを通るトラフィックを収集，集計し，監視サーバで分析することを想定して

いる．

監視サーバでは転送された集計データを入力として，リアルタイムに異常検知を行う．異常検知は構造変化検知をグラフィックラッソ及び密度比推定によって計算する手法によって行う．

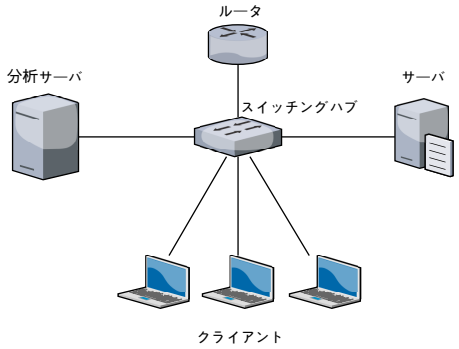


図 2 提案手法の全体像

3.3 相関を持つ属性について

本論文では，以下の相関についてのデータを処理することを提案する．

- HTTP 通信と DNS 通信の相関
- TCP 通信の TCP ヘッダに含まれる syn と synack の相関

HTTP 通信と DNS 通信は，HTTP で特定のドメインのホストにアクセスする際に，DNS に IP アドレスを問い合わせることから，2 つの通信間に相関関係があることを期待した．DNS を利用したトンネリング攻撃や，DomainFlux のような複数のドメインへの通信を行う際に，相関が崩れるという想定をした．

TCP ヘッダに含まれる syn と synack については，本来 2 つの通信が要求，応答のセットで通信されるため，頻度の相関が存在している．この際，SynFlooding 攻撃のような特定の通信量が偏って増加する攻撃がされた場合に相関が崩れると想定した．ただし，ack についてはスリーウェイハンドシェイクだけではなく，データの受信を確認するたびに，ack フラグが送られるため，ack 単体ではなく，synack に集計し，syn は synack ではない単体のものに限って集計した．

3.4 時系列データへの応用

2 つの標本の相関変化を時系列のデータに応用することを考える．図 3 のように，現在時刻を t_0 とし，現在時刻から時間窓サイズ s だけ前の時刻を t_{-1}，さらに時間窓サイズ s だけ前の時刻を t_{-2} とする．t_0 から t_{-1} までの標本を D_1，t_{-1} から t_{-2} までの標本を D_2 とし，2 つの標本 D_1，D_2 から得られる相関の差分を求めるという問題に置き換えることにより，時系列のデータの相関変化を求めることができる．

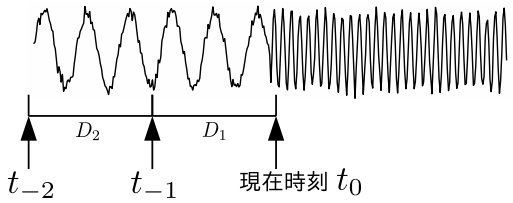


図 3 時間窓の指定

4. 実験で使用するデータの処理の流れと特徴分析

本章では，実験で使用するデータである NCD DATAset について記述する．また，データの処理に使用したツールと処理方法について記述する．

4.1 使用するデータ

実験では，コンピュータセキュリティシンポジウムで行われるワークショップの 1 つである MWS(Malware Work-Shop) が提供している MWS DATAset に含まれる NCD in MWS Cup 2014 を使用する [6]．このデータセットは MWS で行われる MWS Cup 2014 の際に、会場内で流れたトラフィックを無線アクセスポイントを集約するスイッチングハブ上で約 80 分程度の時間キャプチャしたものであり，複数のホストの通信をログとして取得している．このデータを正常なデータとして使用する．

4.2 データの処理に使用したツール

パケットキャプチャファイルからコネクションごとのバイト数，パケット数や DNS 通信を抽出するアプリケーションである Bro[7] や，Python のパケット解析ライブラリである dpkt[8] を使用して，pcap から必要な属性を抽出した．

本論文では，実時間での実行や，実際のシステムでの評価を含まないため，フロー情報を実際のフロー収集システムから実装する必要はないと考え，データの分析部分は処理済みの csv ファイルに対して，Python のライブラリ群でアルゴリズムを実装し，その上で分析を行った．

4.3 データの処理の流れ

データの処理は以下の手順で行った．頻度を集計する時間間隔については相関があると想定するデータが分離しない程度の時間を考慮し，1 分とした．

(1) 解析ツールを用いて，パケットキャプチャファイルから必要な属性を取り出す．
(2) 特定時間ごとの通信頻度の合計値を集計して，それを 1 つのデータとする．
(3) 集計されたデータを時系列データとして，異常検知を

行う．

4.4 処理されたデータの可視化

図 4 は上記の処理により，パケットキャプチャファイルから TCP ヘッダのフラグである syn と synack の頻度を 1 分ごとに集計し，時系列で可視化したものである．このような複数属性の時系列データの分析を行う．

図 5 は上記の処理により，DNS 通信と HTTP，HTTPS 通信の合計値の頻度を 1 分ごとに集計し，時系列で可視化したものである．ただし，これら 2 つの通信では，平均のパラメータを潰すために，z-score 正規化を行っている．

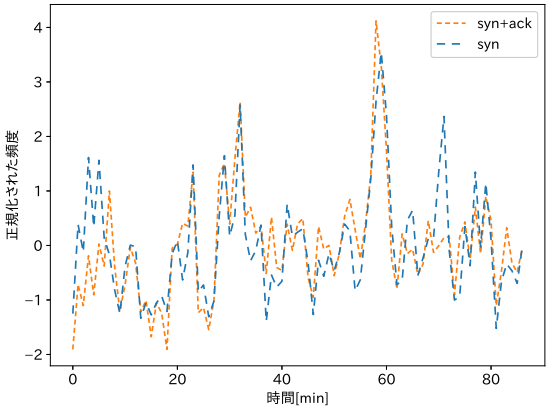


図 4 正常通信の TCP ヘッダに含まれる
syn と synack の 1 分ごとの頻度の変化

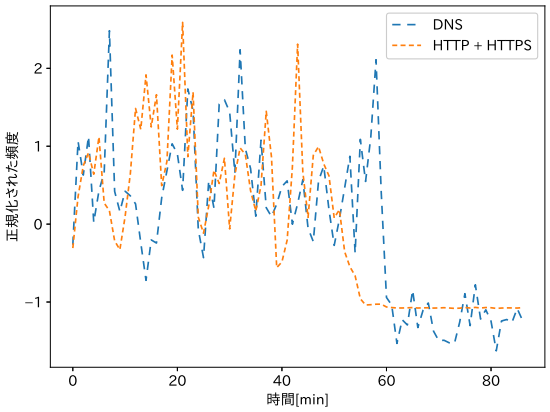


図 5 正常通信に含まれる
DNS 通信と HTTP 通信の 1 分ごとの頻度の変化

また，図 6 は，TCP 通信上の syn 通信と synack 通信，図 7 は HTTP 通信と DNS 通信の頻度を 2 次元平面にマッピングしたものである．データ全体で相関係数を算出したところ，syn 通信と synack 通信では相関係数は 0.79，HTTP 通信と DNS 通信では相関係数は 0.56 となった．

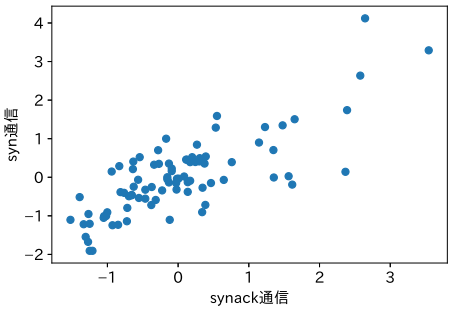


図 6 正常通信に含まれる
syn 通信と synack 通信の 1 分ごとの頻度の散布図

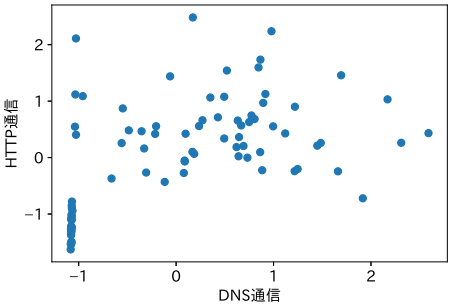


図 7 正常通信に含まれる
DNS 通信と HTTP 通信の 1 分ごとの頻度の散布図

図 4 では，syn と synack は正常であれば，送信に対して応答するという特性からほとんど同じタイミングで頻度の上下をしている．一方で，DNS と HTTP，HTTPS の通信を見ると，通信頻度が多い 0〜60 分と 60〜80 分では大きく上下しているところから全体を見ると相関はあるが，部分的に見ると必ずしも相関が発生しているとは言えない．DNS は HTTP に限らず名前解決に使用していることや，HTTP の通信が行われるごとに対応して DNS 通信が行われるとは限らないため，完全な相関にならないと考えられる．

これら通信の相関の崩れを監視することによって異常検知を実現できるかを検証する．syn 通信と synack 通信は、もともと相関関係が高い通信の例，DNS と HTTP，HTTPS 通信はもとの相関関係があまり高くない通信の例の実験データとして取り上げる．

5. 実験

本章では，行った実験の目的，実験方法，評価方法について記述する．

5.1 実験目的

本論文では，相関検知の変化を検出する手法を，ネットワークトラフィックの時系列データに含まれる相関のある変数群から，相関が崩れることを検出することによって，異常検知を行う手法を提案している．そのため，相関関係

が変化するデータに対して，相関検知手法の一種であるグラフィカルラッソ及び密度比推定を使用して，相関関係の変化の検出が可能であるかを検証する．

前章で分析したデータに対して，構造検知手法であるグラフィカルラッソ及び密度比推定を使用した方法で異常状態を検知できるかを確認し，性能を評価することを目的とする．密度比推定の利点として，異なる確率密度関数の相関の差を疎性を持ったまま直接推定できるという点がある．それを確認するために，独立に確率密度関数の相関を求める手法であるグラフィカルラッソと比較し，密度比推定でも検出できるかを確認する．

5.2 実験方法

正常データとして，データ分析の際に使用した正常データを使用する．異常状態での検知を想定するために，攻撃を想定して恣意的にデータの変更を行う．

前章で 1 分ごとに区切り頻度を集計したデータを 60 分時点で一定の値に変更するという変更を行う．このように変更することで，データ間の相関が崩れることを予想する．

syn と ack のデータには，SynFlood 攻撃のような syn の値が異常に増加する場合を想定する．変更を行った後のデータは図 8 のようになる．

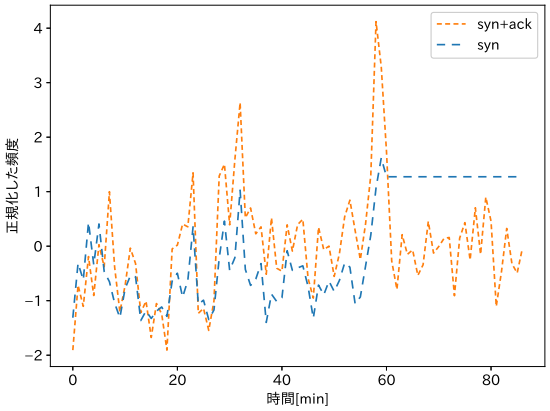


図 8 正常通信と異常通信の TCP ヘッダに含まれる syn と synack の 1 分ごとの頻度の変化

DNS 通信と HTTP 通信の相関については，DNS の通信頻度が通常より多くなることを想定する．変更を行った後のデータは図 9 のようになる．相関変化を求めるために一定に固定するが，実際の攻撃上では固定にはならないと考えられるために，実データとのこの実験がどのように関連しているかが今後の課題となる．

5.3 パラメータ設定

提案手法にはいくつかの事前に設定するパラメータが存在するが，本実験では最も疎な結果を得ることができた表

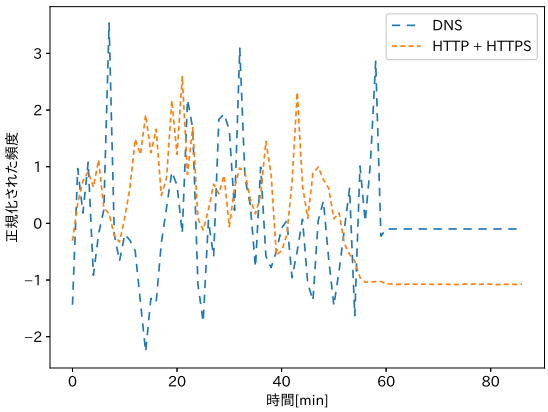


図 9 正常通信と異常通信の TCP ヘッダに含まれる DNS 通信と HTTP 通信の 1 分ごとの頻度の変化

1，表 2 のパラメータを使用した．標本として利用する時間窓のサイズについては同様の理由で $s = 10$ とした．

表 1 syn，synack で使用したパラメータ群

パラメータ名	パラメータ
密度比推定の L1 ノルム	1.1
グラフィカルラッソの L1 ノルム	0.017

表 2 HTTP 通信，DNS 通信で使用したパラメータ群

パラメータ名	パラメータ
密度比推定の L1 ノルム	0.4
グラフィカルラッソの L1 ノルム	0.8

5.4 実験結果

評価した結果，syn，synack 間の通信と DNS，HTTP 間の通信では，それぞれ図 10，図 11 のようになった．横軸は 1 分ごとに区切った時間，縦軸は推定した相関の差分である．左右で，グラフィカルラッソによる推定の結果と密度比推定による推定の結果を示している．それぞれの結果を確認すると，syn，synack のデータと両手法において異常が発生させた 60 分以降に相関の差分が変化していることがわかる．

実験結果から，実験の目的であるグラフィカルラッソと密度比推定で相関の変化を検知することができることを確認できた．

5.5 考察

相関の算出結果については正常の通信であっても，データ送受信の失敗や，別通信との関係する通信の発生などにより，ノイズが発生するため，相関の算出結果にブレが生じてしまい，従って相関の差分にもブレが生じてしまう．実験では相関の高い通信と高くない通信を使い，もとの相

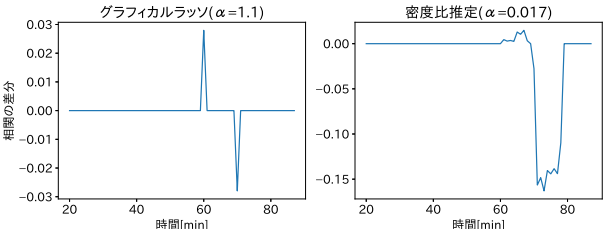


図 10 正常通信と異常通信に含まれる
syn 通信と synack 通信の 1 分ごとの頻度の変化

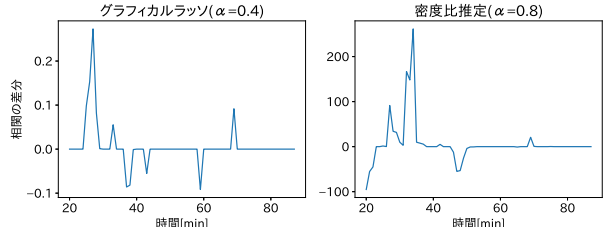


図 11 正常通信と異常通信に含まれる
DNS 通信と HTTP 通信の 1 分ごとの頻度の変化

関関係の高さと変化の大きさの関係を考察する．パラメータを調整することによって，syn，synack については異常を発生させた時刻に相関の差分が上昇していることから，相関の変化を用いることで，異常の検知ができていることがわかる．HTTP 通信と DNS 通信については正しく検知することができなったと言える．改変させたデータ以上に，元データの相関変化が大きかったため取り出すことができなかったことが原因と考える．しかし，より相関を得られるように IMAP など DNS を使用する通信を加算することにより，改善できる可能性がある．

パラメータ設定について考察する．グラフィカルラッソ，密度比推定の両方の手法において，相関の差をパラメータを細かく設定することによって，検知することができた．通信種類によってパラメータを正確に調整しながら適用することが重要であると考えられる．

時間窓のパラメータについては，窓サイズを小さくしすぎると，標本数が少なくなるため誤差が大きくなると考えられる．一方で，窓サイズを大きくしすぎると，処理時間が増加することや，変化が誤差として丸められるため，適切なサイズを設定する必要があると考える．

6. 結論

本論文では，相関関係の変化によりネットワークの異常検知を行う手法を提案した．提案手法をグラフィカルラッソと密度比推定による相関関係の変化を検知する手法により実装し，相関の高い通信と高くない通信に対して，相関関係の変化を検知できるかを実験により確かめた．

密度比推定の特徴を確認することができたと共に，ネットワークの異常検知という問題に対して，時系列の相関関係の変化検知によって，部分的に検知することができた．

本研究では，実験として 2 変数の相関関係の変化を検知する方法を実行したが，グラフィカルラッソや密度比推定は多変数での変数間の相関関係の変化を検出することができるため多変数での変化を検出するか確認する展望がある．その際には，ひとつの異常スコアとして集約する方法が課題になると考えられる．

また，その異常スコアのどの値が異常として判断するかを考える必要がある．本論文では，グラフに可視化することによって検知できているかを確認したが，自動的に検知するという点から見ると，閾値を設定することや，確率統計によりアラートを出すタイミングが必要になると考える．

実験に使用したデータについては，攻撃手法が恣意的に正常なデータを加工したものであったため，実際の攻撃を環境下で実行し，その攻撃を検知することで，実際の攻撃に応用する展望がある．

今後の展望としては，これら課題を解決することを含め，キャプチャされたファイルを処理する方法ではなく，実環境下での動作したデータを集計し，異常検知することが望まれる．相関変化検知により数間の関係を抽出することができ，変数同士の関係が崩れたかを理解することによって，数多くあるネットワークセキュリティにおけるネットワーク異常検出のひとつになると考える．

参考文献

[1] 長山弘樹, 胡　博, 小山高明, 三好　潤: 通信コミュニティ分析に基づく標的型攻撃の LAN 内侵入拡大の検知, 研究報告セキュリティ心理学とトラスト（SPT）, Vol. 2017-SPT-22, No. 27, pp. 1–6 (2017).

[2] IDÉ, T. and KASHIMA, H.: Eigenspace-based Anomaly Detection in Computer Systems, *Proceedings of the Tenth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, KDD '04, New York, NY, USA, ACM, pp. 440–449 (2004).

[3] 村上慎太郎，濱崎浩輝，川喜田雅則，竹内純一，吉岡克成，大介井上，将史衛藤，康二中尾: 確率的依存関係に基づくボットネット検知の検討 (高度インシデント分析を支える要素技術, インターネットセキュリティ, 一般)，電子情報通信学会技術研究報告. ICSS, 情報通信システムセキュリティ， Vol. 109, No. 86, pp. 1–6 (2009).

[4] Friedman, J., Hastie, T. and Tibshirani, R.: Sparse inverse covariance estimation with the graphical lasso, *Biostatistics*, Vol. 9, No. 3, pp. 432–441 (2008).

[5] Liu, S., Quinn, J. A., Gutmann, M. U., Suzuki, T. and Sugiyama, M.: Direct Learning of Sparse Changes in Markov Networks by Density Ratio Estimation, *Neural Computation*, Vol. 26, No. 6, pp. 1169–1197 (2014).

[6] 神薗雅紀，秋山満昭，笠間貴弘，村上純一，畑田充弘，寺田真敏: マルウェア対策のための研究用データセット〜MWS Datasets 2015〜，研究報告コンピュータセキュリティ（CSEC），Vol. 2015-CSEC-70, No. 6, pp. 1–8 (2015).

[7] Bro: The Bro Network Security Monitor, https://www.bro.org/.

[8] dpkt: dpkt: fast, simple packet creation / parsing, with definitions for the basic TCP/IP protocols (2018).