Holt-Winters 法を用いた侵入検知システムのログ分析手法の検討

米井 将二 †　　木村 知史 †　　稲葉 宏幸 †

† 京都工芸繊維大学大学院工芸科学研究科
605-8585　京都市左京区松ヶ崎橋上町 1
yonei07@sec.is.kit.ac.jp, kimura08@sec.is.kit.ac.jp, inaba@kit.ac.jp

あらまし　近年, ネットワークを介した情報システムが広く利用されている. しかし, サイバー攻撃による情報漏洩等の被害が多数報告されており, ネットワークセキュリティの確保は重要な問題のひとつである. 対策技術のひとつである侵入検知システム (IDS) は, 一般に膨大な量の検知アラートが発生する. この問題に対し, 著者らは Holt-Winters 法を用い, IDS の警告イベント数を予測する手法を検討してきた. 本研究では, 従来手法では予測誤差が大きかった不定期に大量の検知が発生するようなイベントに対して予測精度の向上を図る手法を検討する.

A Log Analysis of IDS Alert Events Using Holt-Winters Method

Shoji Yonei†　　Satoshi Kimura†　　Hiroyuki Inaba†

†Kyoto Institute of Technology.
1 Hashigamicho, Matsugasaki, Sakyo-ku, Kyoto-shi, Kyoto 605-8585, JAPAN
yonei07@sec.is.kit.ac.jp, kimura08@sec.is.kit.ac.jp, inaba@kit.ac.jp

Abstract　Recently, information systems using network are widely used. However, cyber-attacks as information leakage occur frequently. Therefore, ensuring network security is one of the most important issues. Intrusion detection system (IDS) which is one of countermeasure for network security outputs enormous logs for IDS alert events. For this matter, the authors have studied a method of predicting amount of IDS alert event by Holt-Winters method. In this study, we aimed to making improvements on prediction accuracy for IDS alert events which are detected in large amounts at random in comparison with previous research.

1　はじめに

昨今, コンピュータの普及に伴い, ネットワークを介した情報の伝達が増えている. そのため, ネットワーク経由の情報伝達および情報管理には最大限の注意を払う必要がある.

ネットワークセキュリティを確保する一般的な方法のひとつとして, 侵入検知システムが存在する [1]. 侵入検知システムとは, ネットワーク上のパケットをルールに基づき監視し, 異常があれば記録および管理者へ報告する技術である. 侵入検知システムの実装としては, オープンソースの侵入検知システム Snort[2] がよく知られている.

しかし, 侵入検知システムの実際の運用では, 一般に大量のログが発生し, ログ分析が困難であるという問題がある. このため, IDS ログ分析については, 様々な研究がなされている [3][4][5][6].

著者らは, 上述の問題に対し, Holt-Winters 法を利用し, Snort の各警告イベントについて検知傾向の分析と予測を行うことでログ分析を容易にする研究を行ってきた [7]. その結果, Holt-

Winters 法は, 定常的に一定量の検知が発生する警告イベントの予測に特に有効であることが分かった. しかし, 不定期に大量の検知が発生する警告イベントの予測では, 誤差が大きくなる傾向があった.

本研究では, 不定期に大量の検知が発生するような警告イベントに対し, Holt-Winters 法による予測誤差を低減する手法を提案する. まず, 2 章で従来手法について述べ, 3 章で提案手法について述べる. そして, 4 章で実験環境および結果について述べ, 考察を行う.

2 Holt-Winters 法を用いたログ分析の従来手法

2.1 Holt-Winters 法

Holt-Winters 法 [8] は, 指数平滑法の一種である. 指数平滑法は, 時系列データから将来値を予測する際に利用される代表的な時系列分析手法である. 指数平滑法における予測値は, 次の式のように定義される.

$$\hat{y}_{t+1} = \alpha y_t + (1-\alpha)\hat{y}_t \tag{1}$$

式 (1) において y_t , $\hat{y}_t$ は, それぞれ時刻 t における実測値, 予測値を表す. また, α は $0 < \alpha < 1$ の値をとるパラメータである. 式 (1) は, α によって直近のデータと過去のデータの予測への影響を調節し, 予測を行う点が特徴である.

Holt-Winters 法は, 上述した指数平滑法を拡張したもので時系列データを 3 つの指標に分解し傾向を詳細に分析できることが特徴である. Holt-Winters 法の予測値は次のように定義される.

$$\hat{y}_{t+1} = a_t + b_t + c_{t+1-m} \tag{2}$$

ただし,

$$a_t = \alpha(y_t - c_{t-m}) + (1-\alpha)(a_{t-1} + b_{t-1}) \tag{3}$$

$$b_t = \beta(a_t - a_{t-1}) + (1-\beta)b_{t-1} \tag{4}$$

$$c_t = \gamma(y_t - a_t) + (1-\gamma)c_{t-m} \tag{5}$$

指数平滑法と同様に y_t, $\hat{y}_t$ は, それぞれ時刻 t における実測値, 予測値を表す. α, β, γ は $0 < \alpha$, β, $\gamma < 1$ の値をとるパラメータである. また, m は単位時間数を表し, 周期を c, 単位時間を u と定義すると $m = \frac{c}{u}$ と表せる.

ここで, a_t, b_t, c_t は表 1 のような意味を持つ. これら 3 つの指標により詳細な傾向分析を行うことが可能である.

表 1: HoltWinters 法における各指標

指標	指標が表す内容
a_t	時系列データの b_t, c_t を除いた変動
b_t	時系列データが上昇傾向か下降傾向か
c_t	時系列データの周期的な傾向

本研究では, Holt-Winters 法による分析と予測を行う際, 統計解析向けプログラミング言語 GNU R[9] を利用した. R には Holt-Winters パッケージが存在し, 式 (3), (4), (5) にある α, β, γ の値を, 予測値と実測値の差の平方の総和

$$\sum_{t=1}^{n}(y_t - \hat{y}_t)^2 \tag{6}$$

が最小となるように自動算出することができる. なお, y_t , $\hat{y}_t$ は, それぞれ時刻 t における実測値と予測値を表す.

2.2 従来手法の概要

2.2.1 従来手法の流れ

従来手法 [7] では Snort の検知データについて警告イベント毎に Holt-Winters 法を用いて分析と予測を行い, その予測値が実測値から大幅に外れた場合に管理者に警告することを想定していた.

従来手法の処理の説明に入る前に以下の定義を行っておく.

- 学習期間: Holt-Winters 法による予測に用いる入力データを取得する期間
- 検証期間: 予測値と比較を行うために, 実測値を取得する期間

上記の各期間の関係は, 図 1 のようになっている.

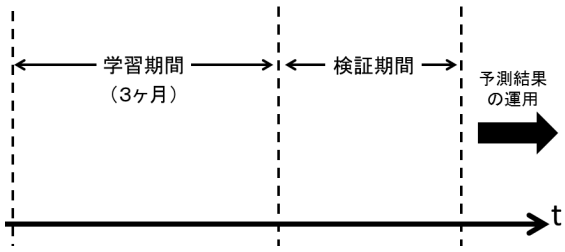

図 1: 学習期間, 検証期間の関係

従来手法の処理を以下に示す.

1. 学習期間および検証期間における Snort の検知データを取得する

2. 1. の検知データから分析対象を選定する

3. 警告イベント毎に集約時間 T を変化させて, 3-1.〜3-3. の処理を行う

3-1. 集約時間 T 時間毎に警告イベントの検知数を集約する (y_t とする)

3-2. 3-1 のデータに対し, Holt-Winters 法により集約時間単位で 48 点先までの予測値を得る

3-3. 検証期間における実測値と予測値の誤差計算を行う

4. 最小の予測誤差を与える集約時間 T を, その警告イベントの集約時間とする

ここで, 学習期間は, 検証期間をさかのぼる過去 3 か月分を対象とする. また, 集約時間 T は T=1, 2, 3, 4, 6, 8, 12[h] のいずれかとする. 検証期間は, 学習期間の終了直後から $T \times 48$ の期間となる.

2.2.2 分析対象の選定

次の方針に従い, 分析対象を選定する.

- 学習期間において検知数が 300 件以下の警告イベントを解析対象から外す
- 検証期間において検知数が 0 件の警告イベントを解析対象から外す

これは, 過去 3 か月において検知数が 300 件以下の警告イベントは, 特に管理者の負担にはならず, 分析する必要がないと判断したためである. また, 検証期間において検知数が 0 件の警告イベントについては, 予測精度の計算が行えないことから分析対象から外している.

2.2.3 予測誤差の計算

予測結果の精度を表す尺度として, 相対平均二乗誤差 (Relative-Mean Squared Error, RMSE) と呼ばれる統計量を用いる.

RMSE は, 予測値と予測値に対応する実測値 (以下, 検証値) の平均二乗誤差を, 検証データの平均検知数で正規化したものである.

Holt-Winters 法による予測値を $\hat{y}_t$, その検証値を Z_t とすると, 平均二乗誤差 MSE は次の式で定義される.

$$MSE = \frac{\sum_{t=1}^{48}(\hat{y}_t - Z_t)^2}{48} \tag{7}$$

検証値の平均検知数を $\bar{Z}_t$ とすると, 式 (7) から RMSE は次の式で定義される.

$$RMSE = \frac{MSE}{\bar{Z}_t} \tag{8}$$

2.3 従来手法による結果

学習期間を 2013/3/1〜2013/5/31, 検証期間を 2013/6/1 以降とした時の従来手法による予測結果を図 2〜4 に示す. なお, 表 2 にシグネチャ番号と警告イベントの対応を示す.

表 2: シグネチャ番号と警告イベントの対応

シグネチャ番号	警告イベントの内容
8	WEB-MISC robots.txt access
21	WEB-MISC SSLv2 openssl get shared ciphers overflow attempt
167	WEB-CLIENT CyberLink PowerDVD playlist file handling stack overflow attempt

図 2 がシグネチャ8 に対する予測結果であり, RMSE=2.77 である. また, 図 3 がシグネチャ21

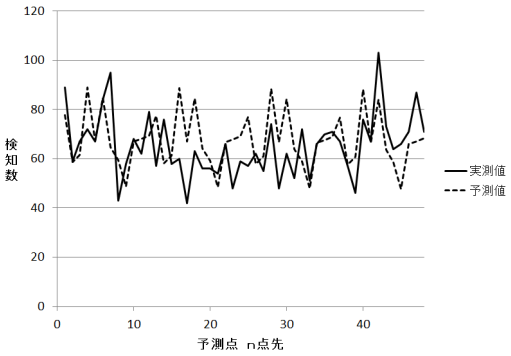

図 2: Holt-Winters 法による予測 (シグネチャ番号:8 集約時間:2[h])

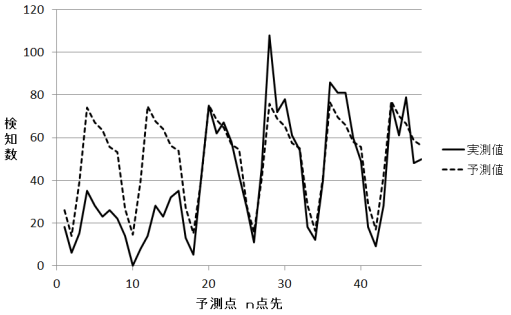

図 3: Holt-Winters 法による予測 (シグネチャ番号:21 集約時間:3[h])

に対する予測結果であり, RMSE=10.15 である. 図 2, 3 共にある程度の予測ができていることがわかる.

一方, 図 4 はシグネチャ167 に対する予測結果であり, RMSE は RMSE=118.57 となっている.

図 4 のように不定期に大量の検知が発生する警告イベントに対して, 予測誤差が大きくなる傾向があることがわかる.

この例の他にも, 学習期間や検証期間で不定期に大量の検知が起きる警告イベントの特徴を調べた結果, 次の 2 種類のものがあることが分かった.

- 通常, 一定量の検知が発生するが, 不定期に大量の検知が発生する
- ほとんどの検知量が 0 であり, 稀に大量検知が発生する

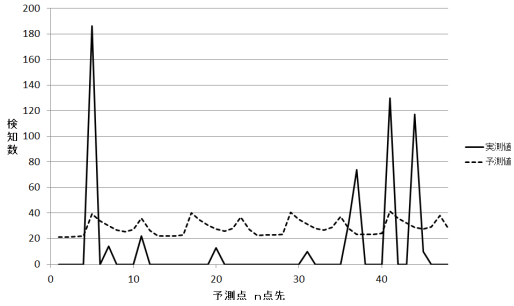

図 4: Holt-Winters 法による予測 (シグネチャ番号:167 集約時間:2[h])

前者では, 不定期に発生する大量検知を除けば, 何らかの検知傾向があると考えられるので, このような警告イベントに対して, Holt-Winters 法による検知数の予測精度を改善することを考える.

3 提案手法

前節で述べたように検知データの一部に大量の検知が含まれる場合には, Holt-Winter 法による予測精度が大きく劣化してしまう. そのことを確認するために, 大量の検知が含まれた入力データを Holt-Winters 法により学習する際の予測値のふるまいを調べたものが図 5 である. これは図 4 の予測に先んじて行われた Holt-Winters 法による学習過程を示すものである.

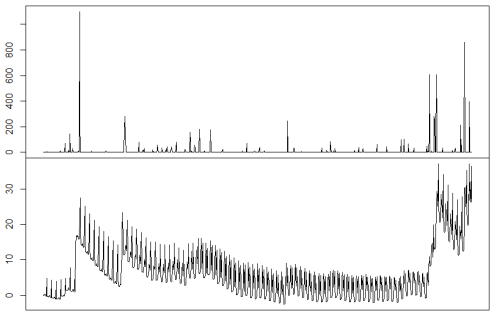

図 5: 従来手法による予測時の学習過程の様子 (シグネチャ167 集約時間 2[h])

図の上段が, Holt-Winters 法に入力される時系列データであり, 下段が入力データに対する Holt-Winters 法の予測値を示す時系列データである. 図 5 を参照すると, 大きな検知数が得られた時点で予測値も大きく上昇していることがわかる. また, 大量検知の影響による予測値の上昇はその後しばらくの間, その影響が残ることも確認できる.

そのため, 図 5 の終盤で大量検知により上昇した予測値の影響が, 図 4 における予測開始時にも残っており, 本来予測されるべき値よりも大きな予測値となっていることがわかる. 従って, 学習期間中に大量検知を修正することで, 大量検知を含むような警告イベントについても予測精度を向上させることができると考えられる.

本研究では, 不定期に発生する大量検知を検知数の時系列データ上の外れ値として考え, これを取り除くことで予測への影響を無くすことを考える. 具体的には, 外れ値と判定されるデータを, 該当する警告イベントの平均検知数に置き換えることで予測精度の向上を図る.

最初に, 処理手順の説明で用いる, 記号および用語の定義を行っておく.

- y_t: 集約時間 T ごとに集約した検知数 (2.2.1 節で定義済み)
- μ: $\{y_t\}$ の平均値
- σ: $\{y_t\}$ の標準偏差
- 外れ値: $\{y_t\}$ において, $y_t > \mu + 3\sigma$ または $y_t < \mu - 3\sigma$ を満たすもの
- S: 外れ値を除く $\{y_t\}$ の合計
- N: 外れ値を除く $\{y_t\}$ の個数

外れ値に対する処理手順を以下に示す.

1. $\{y_t\}$ から $\mu \pm 3\sigma$ を求め, 外れ値となる y_t を決定する.
2. S と N を求める
3. 警告イベントの外れ値を除いた平均検知数 $E = \frac{S}{N}$ を求める
4. 1. で外れ値と判定されたデータの値を E に置き換える

以上の処理を適用した上で, 再度, Holt-Winters 法を適用し, 予測誤差の計算を行う.

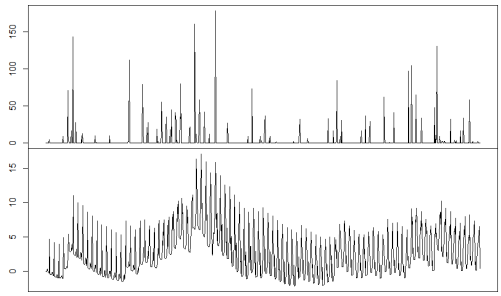

図 6: 提案手法適用後の学習過程の様子

図 5 の時系列データに提案手法を適用した結果が, 図 6 である. 図 6 では, 大量検知の影響が取り除かれ, 図 5 よりも予測精度が向上していることがわかる. なお, 図 5 と図 6 とでは縦軸のスケールが大きく異なっているので注意されたい.

4 提案手法の適用と評価

4.1 実験環境

提案手法の効果を確認するため, 一定量の検知が発生しつつ, 不定期に大量の検知が発生する警告イベントとして, 表 3 に示す警告イベントを用いる.

表 3: 不定期に大量検知が発生する警告イベント

学習期間	検証期間	対象シグネチャ番号
2012/2/1 ～2012/4/30	2012/5/1～	27
2013/3/1 ～2013/5/31	2013/6/1～	167

関連して, 表 3 の警告イベントの詳細を簡単に説明する. 各シグネチャと警告イベントの内容は, 表 4 に示すとおりである. シグネチャ27 は, SNMP マネージャーによる TCP 通信にお

表 4: 実験に用いる警告イベントの内容

シグネチャ番号	警告イベントの内容
27	SNMP trap tcp
167	WEB-CLIENT CyberLink PowerDVD playlist file handling stack overflow attempt

ける SNMP トラップの発行を検知したものである. また, シグネチャ167 は, CyberLink 社の PowerDVD8.0 が持つスタックオーバーフローの脆弱性を不正利用する試みを検知したものである.

これらのデータに対して, 提案手法の適用前後における RMSE を比較し, 予測精度の改善の度合いを明らかにする.

なお, RMSE を適切に比較するために, 従来手法と提案手法の双方について検証期間に含まれる大量検知についても 3 章で述べた方法で修正した後に RMSE を計算している.

4.2 結果および考察

表 3 のデータに対する提案手法の適用結果を表 5,6 および図 7,8 に示す.

表 5: シグネチャ27 に対する予測誤差

従来手法		提案手法	
集約時間 [h]	RMSE	集約時間 [h]	RMSE
1	36.06	1	1.94
2	76.70	2	7.55
3	137.24	3	29.01
4	127.78	4	54.01
6	214.69	6	104.56
8	250.48	8	103.05
12	170.98	12	56.21

表 5, 6 を参照すると, ほとんどの集約時間で RMSE の低下が確認でき, 提案手法により予測精度が向上していることがわかる. 表 5, 6 では, 共に集約時間 T=1[h] で提案手法の RMSE が最小となっており, それぞれRMSE=1.93, RMSE=14.17 となっている. それぞれ適用前の RMSE と比較すると, シグネチャ27 は約 $\frac{1}{18}$ の値, シグネチャ167 は約 $\frac{1}{15}$ の値になっており, 大幅な予測精度の向上が実現できていることがわかる.

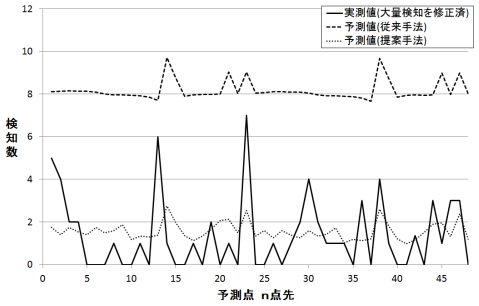

図 7: 提案手法適用前後の予測値と修正実測値 (シグネチャ27 集約時間 1[h])

表 6: シグネチャ167 に対する予測誤差

従来手法		提案手法	
集約時間 [h]	RMSE	集約時間 [h]	RMSE
1	222.03	1	14.72
2	147.88	2	66.80
3	149.21	3	157.53
4	183.32	4	143.01
6	156.95	6	186.81
8	466.13	8	371.57
12	947.55	12	336.29

また, 図 7 および図 8 は, 従来手法と提案手法についてその予測値の変化を比較したものである. 図 7 はシグネチャ27 について RMSE が最小となる集約時間 T=1[h] の場合の予測値をプロットしている. 図 7 から, 提案手法では, 大量検知を除いた部分の傾向をよく予測していることが明らかである. 図 8 は, シグネチャ167 について集約時間 T=2[h] の場合の予測値をプロットしている. 提案手法では, T=2[h] の場合の RMSE は最小値を与えていないが, 同じ条件で比較するために従来手法で RMSE の最小値を与える T=2[h] を用いている. 図 8 においても提案手法の方が実測値をうまく予測していることがわかる.

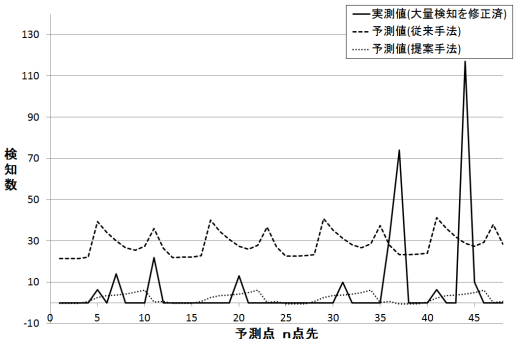

図 8: 提案手法適用前後の予測値と修正実測値 (シグネチャ167 集約時間 2[h])

5 おわりに

本研究では, Holt-Winters 法を利用した侵入検知システムの警告イベント検知数の予測精度を従来よりも精度よく予測する方法について検討した.

従来手法では, 定常的に一定量の検知数が得られる警告イベントに対しては, 精度の高い予測を行えていたが, 不定期に大量検知を含む警告イベントに対する予測精度は高くなかった.

本研究では, 不定期な大量検知を含む警告イベントの特徴を分析し, 一定量の検知が発生しつつも不定期に大量検知が発生する警告イベントに対しては, 大量検知の影響を Holt-Winters 法による予測時にあらかじめ取り除くことで予測精度の向上を図っている.

提案手法では, 不定期な大量検知を外れ値とみなし, それらを該当警告イベントの平均検知数に置換した上で, 再度, Holt-Winters 法による予測を行った. その結果, 従来よりも予測精度が向上することが確認できた.

今後の課題として, 本研究で使用した以外の警告イベントについても提案手法を適用し, 予測精度の向上が見られるかを検証していきたい.

参考文献

[1] 藤田 直行, "侵入検知に関する誤検知低減の研究動向", 電子情報通信学会論文誌, vol.J89-B, no.4, pp.402-411, April. 2006.

[2] Snort 公式ホームページ
http://www.snort.org/

[3] 竹森 敬祐, 三宅 優, 田中 俊昭, 笹谷 巌, "攻撃イベント数に関する調査および理論統計分布へのモデル化", 電情報通信学会技術研究報告, vol.103, no.691, pp.171-174, March 2004.

[4] 竹森 敬祐, 三宅 優, 中尾 康二, 菅谷史昭, 笹谷 巌, "Security operation center のための IDS ログ分析支援システム", 電情報通信学会論文誌, vol.J87-A, no.6, pp.816-825, June 2004.

[5] T. Itoh, H. Takakura, A. Sawada, and K. Koyamada, "Hierarchical visualization of network intrusion detection data", IEEE Computer Graphics and Applications, vol.26, no.2, pp.40-47, March 2006.

[6] K. Abdullah, C .Lee, G. Conti, J.A Coeland, and J.Stasko, "IDS rain storm: Visualizing IDS alarms", Workshop on Visualization for Computer Security(VizSEC'05), pp.1-10, Oct. 2005.

[7] 戸田 剛司 , "警告イベントの時系列予測に基づく侵入検知システムのログ分析手法に関する研究", 京都工芸繊維大学大学院工芸科学研究科修士論文, (2012).

[8] J.D Brutlag, "Aberrant behavior detection in time series for network monitoring", USENIX 14th Systems Administration Conference(LISA), pp.139-146, Dec. 2000.

[9] The R for Statistical Computing
http://www.r-project.org.