5E-1

Webアプリケーションの AID(Anomaly Intrusion Detection) に対する評価項目の提案

吉田　剛，河内　清人，藤井　誠司†
三菱電機株式会社　情報技術総合研究所†

1. はじめに

バッファオーバーフロー，クロスサイトスクリプティングなど，Web アプリケーション上において悪意のあるユーザの攻撃による情報の改ざんや漏洩が大きな問題となっている．現在，その対策の一つとして侵入検知システムがあり，不正検知と呼ばれる手法が広く用いられている．しかし，不正検知は既知の攻撃に対しては非常に有効であるが，未知の攻撃には効果がなく，常に新しい攻撃やその亜種に対応し続ける必要がある．一方で，異常検知（AID）という手法が検討されている．AID では，対象とするネットワークの通常のアクセス状況を学習し，それと大きく異なるアクセスを攻撃と判断する．そのため，AID は未知の攻撃にも対応できると期待されているものの，学習の精度，効率に関する評価項目についてはまだ検討が不十分である．

そこで本稿では，学習に焦点を当てた評価項目について検討を行い，その有用性を明らかにするために，その尺度に基づいて文献[1]で挙げられている 6 つの AID 手法を組み合わせた 1 つの AID 手法を試作し評価することで，その課題を抽出した．

2. 学習に関する評価項目の検討

AID では，より少ない学習サンプル数および学習に必要な計算量で，より高い検知精度を得られるものが優れていると言える．ここで，検知精度が高いとは，異常検知率が高く，誤検知率が低いことを指す．そこで，本稿では以下の評価項目を設定した．

① 十分な学習サンプル数を与えた場合の最終的な検知精度.
② 検知精度が収束するのに必要な学習サンプル数.
③ 学習サンプル数に対する処理時間の変動量.
④ 学習データが変化した場合の①～③の変化の大きさ.

各項目は AID の利用用途や環境によって評価基準が異なる．①からは AID の検知精度の限界を，②からは AID の適応の早さを，③からはある時間内に学習できるサンプル数を知ることができる．

また，④からは同じ環境における学習データの変化への対応能力を知ることができる．同じ環境でも学習データの到着の仕方により①～③の変化の度合いは異なり，その変化が小さい AID ほど導入時の効果が予め予測しやすい．これは AID 導入において重要な評価項目となる．

そこで，ここで挙げた評価項目に対して以下のように評価を行う．

3. 既存手法の評価

文献[1]に基づいて AID を試作し，上記評価項目①～④について評価を行った．試作した AID は 6 つの手法を組み合わせて異常の検知を行う．しかし，そのうち Structural Inference については今回利用した実験用データを入力するとヒープ領域が足りなくなるため用いなかった．

評価は，学習量の増加に対する検知精度の推移の測定から①，②を，学習量に対する学習・検知時間の推移の測定から③を評価した．さらに，④の有用性を検証するためにこれらの測定を異なる複数の入

Evaluation methods for Anomaly Intrusion Detection
Go YOSHIDA, Kiyoto KAWAUCHI, Seiji FUJII
Mitsubishi Electric Corporation Inforamtion Technology R&D Center, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501, Japan

力データを用いて行い, その変化の度合いを調べた. ここで, 評価用のデータには社内の Web ベースのワークフローに対するリクエストデータを用いた. 評価の手順は次のとおりである. まず, 取得した 1395 リクエストのデータから評価用に 600 リクエストをランダムに抽出する. さらに, 残りのデータから学習用に500 リクエストをランダムに抽出する. 今回は上記の方法で抽出したデータA, Bを用いて 10 サンプルずつ学習量を増加させて評価を行った. しかし, このデータには攻撃が含まれないため, 検知精度については異常を検知した時を誤検知として誤検知のみを評価した. また, 評価用マシンの仕様は以下のとおりである.

OS	CPU	メモリ	実装言語
WindowsXP Professional	Pentium4 3.2GHz	1GB	Java SDK ver.1.5.0_02

3.1. 学習サンプル数に対する誤検知率の推移の評価

図 1 は学習サンプル数の増加に伴う誤検知率の推移を表している. データAは緩やかに収束し, 130 サンプル時点でほぼ収束し, 最終的に誤検知率が 0.001 まで減少した. 一方データBは 30 サンプルを境に急激に誤検知率が減少し, 40 サンプルでほぼ収束し, 最終的に 0.003 まで減少した.

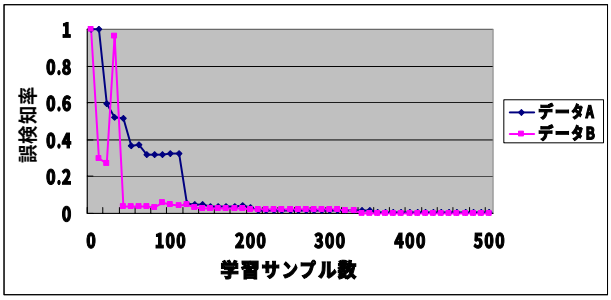

図 1 学習サンプル数における誤検知率の推移

3.2. 学習サンプル数に対する学習・検知時間の推移の評価

図 2 は学習サンプル数の増加に伴う学習時間と検知時間の推移を表している. 図から学習時間は学習サンプル数の増加に伴ってほぼ線形に増加していることが分かる. 検知時間はデータAに関しては学習サンプル数の増加に対して検知時間の変動がほとんどないが, データBに関しては 330 個のサンプルを学習した時点で検知時間が 300[msec] 減少している.

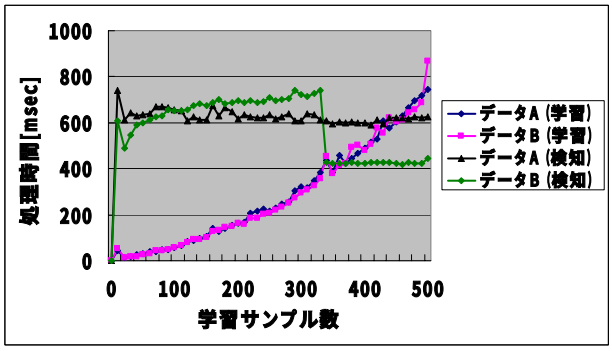

図 2 学習サンプル数における学習・検知時間の推移

4. 考察

学習サンプル数に対する誤検知率の推移の評価から, 対象 AID は学習用データの選び方によって誤検知率の減少の度合いや収束の早さが異なる. 今回の評価では, 収束の早さで約 100 サンプル, 割合として約 3 倍の違いが出ていることが分かる.

また, 学習サンプル数に対する学習・検知時間の推移の評価においても, 学習データを変化させることで検知時間に 200[msec], 割合として 50%もの影響が表れていることが分かる.

以上の結果から, 2 章で我々が提案した評価項目④は AID の評価において重要な項目であると言える.

5. おわりに

本稿では, Web アプリケーション上における攻撃に対する侵入検知システムについて, AID 手法の学習に焦点を当てた評価項目について検討を行い, その尺度に基づいて文献[1]で挙げられている AID を試作し評価することで, 評価項目の有用性を示した.

今後は, 他の AID との比較や新たな観点における評価項目の検討, 評価を行う.

6. 参考文献

[1] C. Kruegel and G. Vigna. Anomaly detection of web-based attacks. In Proceedings of 10th ACM Conference on Computer and Communications Security (CCS'03), October 2003.