2007 年 5 月 16 日（水）
1031060322 松本　亮介

侵入検知に関する
誤検知低減の研究動向（概略）

0 はじめに

※この資料は，参考文献を元に，参考文献の概略を作成したものです．この研究を私が実際に行ったわけではありませんので注意してください．

1 まえがき

コンピューターネットワークシステムが社会に普及していくにつれ，ネットワークセキュリティの確保が必要不可欠になった．セキュリティに関して，今まで以上に重要視されるようになったが，現実にはさまざまな被害が発生している．ワーム検知，ウィルス検知，暗号通信，セキュア OS，セキュアプロトコル等，セキュリティ確保について多方面から研究が積極的にされている．しかし，それらの多くはネットワークの末端通信ノードに何らかの変更を必要とするものであり，実利用面から早急な問題解決に対応できないという性質がある．

一方，ファイアーウォールや IDS は，末端ノードへの変更なしにネットワーク全体のセキュリティ確保を実現しようとする技術で，即効性に優れている．また, IDS の研究は国内でも盛んになってきているが，個別技術に対する研究が主体で，侵入検知全体の総合的な研究は少ない．

こういった背景から，本稿では，IDS の構成要素モデルを用いながら，誤検知低減に関する最近の研究を中心に，侵入検知全体の総合的な研究に対する必要性について述べる．

2 侵入検知システムについて

社会基盤としてのネットワークのセキュリティ確保が重要な課題であるという認識が，一般社会にまで浸透してきている．そして，セキュリティにおける安全確保の 1 つの手段として，ファイアーウォールと共に IDS（Intrusion Detection System）が利用されてきている．

IDS とは, ネットワークを流れるパケットやコンピュータ内の情報の状況を検査することにより，侵入やその前兆が発生していないかを判定するシステムである．最近では，侵入を検知すると，その通信を自動的に遮断するなどの防御手段を持つシステムもあり，これを IPS（Intrusion Prevention System）と呼ぶ．

IDS の説明のために, 構成要素としての参照モデルとして提案されている CIDF をさらに詳しく分け, 以下の 6 つに定義する．

ⅰ，データ収集機能
ⅱ，データ作成機能
ⅲ，データ解析機能
ⅳ，アクション機能
ⅴ，記録機能
ⅵ，ログ解析機能

また, IDS を構成要素と，その実現方法や方針の違いによって明確に IDS の分類を行う．

2.1 データ収集機能による分類

IDS は，データ収集機能の違いによって，ネットワーク型，分散型，ホスト型に分類される．

ネットワーク型 IDS とは，ネットワークインターフェイスをデータ収集源とし，そこを流れるパケットを監視することで，不正を検知するものである．通常は，ファイアーウォールと同様の位置に設置し，広範囲の監視を可能とする．

分散型 IDS とは，ネットワーク型 IDS の変形で，ネットワーク型 IDS のデータ収集機能を，場合によっては，データ作成機能など他の機能も含めて，複数配置したものである．広域での侵入検知や，データ解析との連携に優れている．

ホスト型 IDS とは，ホスト内のログやマシン情報などから，変更や定義外のアクセスを監視し検知するものである．ネットワーク型などと違って，個々のホストにインストールする必要があるが，ネットワーク型では収集不可能な情報まで詳細に収集することができる．バッファオーバーフロー攻撃や，不正ログインなどの検知に利用される．

2.2 データまたはログ解析機能による分類

IDS は，データまたはログ解析機能の違いにより，シグネチャマッチ型（不正検知型），アノマリディテクション型（異常検知型），ログ解析型に分類される．

シグネチャマッチ型とは，事前に定義されている不正アクセスパターンをデータベースに保存し，収集データとデータベース内のデータを，パターンマッチにより比較し不正を検出するものである．既に知られている不正アクセスやウィルスに対しては，高精度の検出を可能とするが，未知のものを検出できないという問題もある．

アノマリディテクション型とは，正しい利用状況におけるシステムやユーザーの挙動のプロファイルを作成し，収集したデータとこのプロファイルを比較し不正を検出するものである．理論上は，未知のものを検出するとされているが，現状では特定の状況下（バッファオーバーフローなど）で効果を発揮するのみにとどまっている．また，プロファイルを作成するのにも時間がかかってしまう．

ログ解析型とは，異常検知を目的としており，アノマリディテクション型の解析対象が，ホスト上のユーザーの利用プロファイルそのものであるのに対し，ログ解析型はシグネチャマッチ型 IDS 等が出力するログを用いて検出するものである．異なるアルゴリズムを持つ複数のデータ解析部から出力されるログを分析対象にするため，現時点では False Positive 低減に最適なアプローチとされている．

2.3 アクション機能による分類

IDS はアクション機能により，狭義の IDS と IPS に分類できる．狭義の IDS とは，不正アクセスの通知とログ記録機能のみを有し，防御機能のないもののことである．

3 誤検知低減に関する研究動向

IDS を運用する際に，誤検知による大量のログ出力が大きな課題となっている．つまり，False-Positive（正常を異常と検出）によって，正常状態におけるログを大量に出力してしまうためである．それらの大量のログの内，実際に攻撃を受けているログは 4%程度という報告もある．2.2 で述べたログ解析型 IDS では，大量のログが発生することが前提とされているが，このログの存在自体が False-Positive であるともいえる．しかし，ログ解析型 IDS では，このログを統計的に解析し不正行為のログを選別することで，大量のログ出力による問題を解決しようとしている．

3.1 シグネチャ設定の難しさ

False-Positive の解決が IDS 実運用での課題とされる中，シグネチャマッチ型 IDS も大量の False-Positive を発生させてしまう．この誤検知問題の原因として、False-Positive は不正行為以外の通信に現れるパターンを含んでしまっている．また，False-Negative は不正行為の通信に現れるパターンをシグネチャにできていないためだと考えられる．

実際に，これらのシグネチャを正しく記述できれば解決するが，この 2 つの要素を一致させることは難しい．これを解決するために，攻撃と応答の関係を表現する方法，攻撃と応答両方の検知を監視する方法，複数の通信を関連づけてシグネチャマッチさせる方法，などが提案されているが完全な解決には至っていない．

3.2 プロファイル作成の難しさ

アノマリディテクション型 IDS によるプロファイルの作成が非常に困難とされており，実用に至っていないのが現状である．しかし，最近の研究では，被害の頻度が高いバッファオーバーフロー攻撃に対しては効果があるとして，研究が盛んに行われている．検証関数というものを関数呼び出しの始まりと終わりに挿入し，プログラムの制御フローを変更することで，異常を検知する手法などがある．

4 その他の研究と研究課題

IDS の研究には，まだまだ問題点が多く挙げられている．それは，異なる IDS 種別ごとのログ・運用点順の統合問題，既存分析ツールには攻撃傾向の把握に適している項目に関する分析機能がないこと，大量ログによりかすかな痕跡を見逃してしまうこと，既存頻度分析機能では未知の攻撃に対応できないこと，などが挙げられる．

以上の研究課題は，今のところ積極的には研究されていないが，今後の IDS 誤検知低減に必要不可欠な問題を挙げる．それは，個別環境にあった IDS パラメータの設定手法の研究である．パラメータ設定は非常に難しいが，設定によって検出精度が大きく

左右されるため，避けては通れない課題である．

もう 1 つ必要不可欠な課題は，シグネチャ更新の更なる高速化とそれに伴う IDS のパフォーマンス向上である．

その他 IDS とは違う研究課題としては，インシデントカウントの基準や，IDS の評価方法，IDS 熟練運用者の確保，などが挙げられる．

参考文献

[1] 藤田直行，“侵入検地に関する誤検知低減の研究動向”