5E-3

定点観測による不正アクセス分析システムの提案[1]

榊原裕之[2]　藤井誠司[3]　北澤繁樹[4]　平井規郎[5]　鹿島理華[6]　東辰輔[7]
三菱電機株式会社　情報技術総合研究所[8]

1. はじめに

近年 DoS 攻撃，ワーム等のネットワーク経由の不正アクセスが増加しており社会的な問題となっている．従来の代表的な不正アクセスの検知方法にシグネチャベースの Signature based Network IDS(以下 S-NIDS)[1]があるが，未知の不正アクセスに対しては対応するシグネチャの適用に遅延が発生するため，その間は監視対象のネットワークが攻撃にさらされる課題がある．

本稿ではネットワーク上のトラフィックを定点観測・分析することで不正アクセスを早期に検知するシステムの提案を行う．S-NIDS と提案システムを併用することにより S-NIDS の課題を補完する．

2. S-NIDS の特徴と課題

S-NIDS の特徴と課題について述べる．

○　特徴

S-NIDS では，不正アクセスに特有のパケットデータを検知条件にするため，パケットの特徴が明らかになっている不正アクセスに対しては確実に検知可能である．

また，ネットワーク（以下 N/W）のパケットをスニッフィングし検知する方式のため，N/W に接続された計算機に専用のソフトウェア（以下 S/W）をインストールする等の変更を加える必要が無い．

○　課題

シグネチャの開発と適用は不正アクセスの方法/パケットが特定された後になる．また，亜種が発生した場合は既存のシグネチャを修正する場合がある．このため，未知や亜種の不正アクセスに対してはシグネチャが開発/修正・適用されるまでの間は，監視対象のシステムが攻撃にさらされていても検知できない．

従って，S-NIDS を使用する場合は未知/亜種の不正アクセスに対する早期対策が課題となる．N/W の管理者は脆弱性情報を常時チェックし S/W のパッチの適用や設定の変更等を行い未知/亜種の不正アクセスに備える必要があるが，全ての計算機に迅速にこれらの処置を実施できるとは限らない．よって，シグネチャの開発・適用前の早期の段階で不正アクセスを検知し，N/W 管理者の管理下にある N/W 機器で通信を遮断する等の補完的な対策を行う必要がある．

1 An Intrusion Detection System based on network stationary monitoring,　2 Hiroyuki Sakakibara 3 Seiji Fujii 4 Shigeki Kitazawa 5 Norio Hirai 6 Rika Kashima 7 Shinsuke Azuma　8 MITSUBISHI ELECTRIC CORPORATION, INFORMATION TECHNOLOGY　R&D CENTER

3. 定点観測による不正アクセス分析システムの提案

本稿では S-NIDS の課題を補完するため，定点観測に基づく不正アクセス分析システムを提案する．

3.1. 目標

監視対象の N/W においてパケットをリアルタイムに観測・分析し不正アクセスを早期に検知すること，及び検知した不正アクセスに対する対策の指標を示すことを目標とする．

不正アクセスを受けている環境においては，正常なパケットと不正アクセスのパケットが混在しているが，攻撃方法/パケットが特定されシグネチャが開発される前の段階で不正アクセスのパケットの存在を検知することができれば，S-NIDS の課題を補完することが可能である（図 1）．

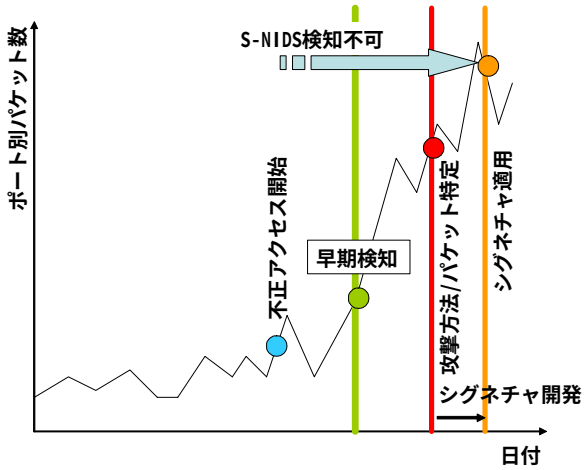

図 1　不正アクセスの早期検知の概念

3.2. 監視対象と定点観測データ

既存の定点観測システム [2][3]では，インターネット上の複数の箇所で観測を行っているが，提案するシステムでは，企業等の特定の組織に属する N/W を監視対象とする．ファイアウォール（以下 F/W），S-NIDS からのパケットログ（定点観測データ）を提案システムに入力し，リアルタイムに分析を行う．S-NIDS 等のログの情報が分析に不足している場合や機器自体が設置されていない箇所には，スニッフィング形式のパケット収集装置を設置しパケットを収集する（図 2）．N/W 上の定

点を通過するパケットを分析するため，サーバ／PC への専用の S/W の導入は不要である．

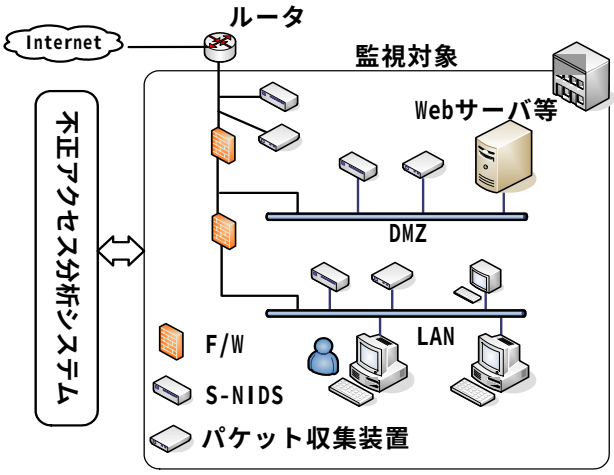

図 2　提案システムと監視対象

3.3.　機能構成

図 3に提案システムの機能の概要を示す．

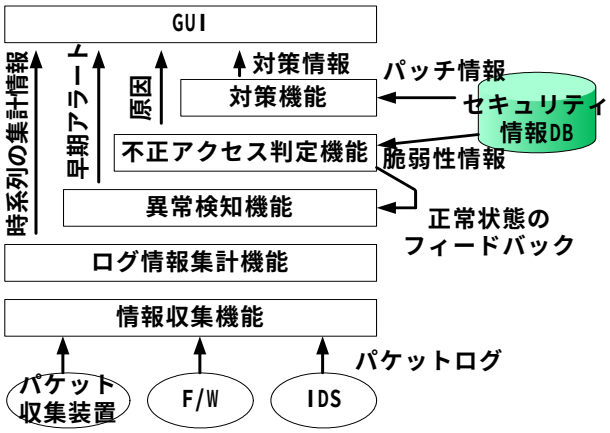

図 3　提案システムの機能構成

・　情報収集機能

F/W，IDS，パケット収集装置のパケットログを定期的に収集する．

・　ログ情報集計機能

情報収集機能で集められたパケットログから不正アクセスの検知に必要なパケットの情報を集計する．例えば，単位時間当たりの送信元 IP アドレス毎パケット数，送信先ポート毎パケット数，或いはパケット長等の集計を行う．

・　異常検知機能

ログ情報集計機能により集計されたデータをもとに異常な N/W トラフィックを検知し早期アラートを出力する．筆者らは，異常状態のリアルタイムな検知の手法として Singular Value Decomposition (SVD)を利用した主成分分析が有効であると判断している．当手法によれば異常状態の発生は正常状態からの距離の逸脱で検知され，検証の結果，不正アクセスの報告（及びシグネチャの開発）よりも早期の段階で異常検知に成功している[4]．

・　不正アクセス判定機能

異常検知機能においてトラフィックの異常状態が検知された場合，不正アクセスが原因であることを判定する機能である．ログ情報集計機能において複数の分析視点での集計を行い，各々に対する異常検知機能の検知の結果を総合的に判断し不正アクセスが原因であることを確定する．

また，セキュリティ情報 DB に格納された既知の脆弱性情報も判定に利用する．例えば，異常検知機能において特定のサービス（ポート）へのパケットの分析結果で異常が検知されており，直近に同サービスの脆弱性が公開されていたのであれば，同脆弱性を悪用した不正アクセスの可能性があると判定できる．

誤検知と判定された場合はその情報を正常状態として異常検知機能にフィードバックする．

・　セキュリティ情報 DB

S/W の最新の脆弱性情報・パッチ情報を管理するデータベースである[5]．

・　対策機能

不正アクセス判定機能により不正アクセスが確定された場合，特定ポートへのアクセスの制限，パッチの適用等の指示等，対策の指針を出力する機能である．ネットワーク管理者はこの出力を参考に対策を行う．

・GUI

早期アラート，不正アクセスの原因，対策情報を表示する．

4.　おわりに

未知/亜種の不正アクセスの早期検知・早期対策を目標とし，定点観測で得られたパケットデータに SVD による分析を適用した不正アクセス分析システムを提案した．提案システムと S-NIDS を併用することでより確実な不正アクセスの検知・対策が実現できると考える．今後は不正アクセス判定機能の具体的な実装方法を検討し，システムの実装・評価を行う予定である．

参考文献

[1] Snort, http://www.snort.org
[2] TALOT2 http://www.ipa.go.jp/security/
[3] ISDAS http://www.jpcert.or.jp/isdas/
[4] 定点観測による不正アクセス分析システムの提案-ワーム攻撃による異常検出のためのネットワークログ分析手法,平井，鹿島，東 他，IPSJ 68 回全国大会予稿集
[5]セキュリティ情報センターの開発，榊原，藤井 他，IPSJ 67 回全国大会予稿集