3H−05

パケット情報と通信ログ情報を用いた侵入経路追跡の検討*

北澤繁樹，藤井誠司，大越丈弘，小林信博，河内清人，勝山光太郎†
三菱電機株式会社 情報技術総合研究所‡

1　はじめに

システムへの侵入を検知した場合の対抗手段の一つとして，これまで多くの侵入経路追跡技術が提案されている．しかしながら，追跡結果を正確かつ効率的に導く手法はこれまで提案されていない．本稿では，既存の複数の侵入追跡手法を併用することにより，正確かつ効率的に侵入経路追跡を可能とする追跡手法を提案する．これにより，検知された侵入に対する早期対策が可能となる．

2　侵入経路追跡

これまでに，多くの侵入経路追跡を行うシステムが提案されている [1, 2]．既存のシステムは，大きく分けて (1) IP パケットの発信元 IP アドレスを元にする方式（以後，これをホストレベル追跡と呼ぶ）と，(2) Ethernet アドレスを元にする方式（以後，これをルータレベル追跡と呼ぶ）がある．

ホストレベル追跡では，発信元 IP アドレスを元に，finger コマンド，whois コマンド，ping コマンド，traceroute コマンドなどにより，不正アクセスパケットの発信元を特定する．したがって，一般的には短時間で追跡が終了するが，発信元 IP アドレスを詐称された場合に対応できないため，追跡結果の正確性に乏しい．一方，ルータレベル追跡では，ローカルネットワーク上のパケットログをルータ上で取得し，そのパケットの流れをルータごとにたどることで，発信元までの不正アクセスパケット中継経路と発信元を特定する．これにより，発信元 IP アドレスを詐称された場合でも侵入経路を特定可能である．しかしながら，経路上のルータとして特殊なハードウェアを想定する必要があり，また，追跡処理中に各機器が通信を行いながら逐次処理を行うため，追跡処理に遅延が発生してしまう．

これらの方式は追跡対象とする階層は異なるものの，パケットの情報を用いているという点では，共通した方式である．また，お互いの利点によってお互いの欠点を補完可能な関係にあることが分かる．したがって，どちらか一方の方式を選択するより，双方を採用した方が効率的に追跡が行えると言える．

本稿では，攻撃者が身元を隠すために踏み台ホストを用いている場合にも対応するため，踏み台ホストの通信履歴やプロセス情報を元にホスト内部を追跡する方式（以後，この方式をホスト内部追跡と呼ぶ）を提案し，ホストレベル追跡およびルータレベル追跡と組み合わせてスケジューリングする．これにより，複数の踏み台ホストを含む侵入経路を正確かつ効率的に追跡することが可能となる．

3　システム構成

図 1 は，提案システムの全体図を表している．

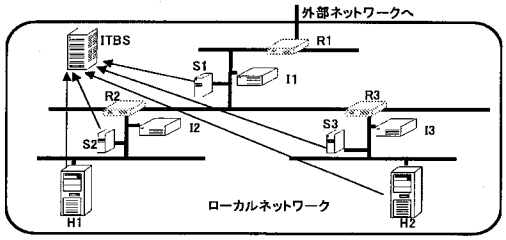

図 1: 侵入経路追跡システム概略

図中の各記号はそれぞれ以下の機器を表している．

侵入経路追跡サーバ（ITBS）
侵入経路追跡サーバ（ITBS : Intrusion Trace Back Server）は，ローカルネットワーク上に存在するパケットログ収集装置から送られてくるパケット情報，および対象ホストから送られてくるプロセス情報と通信履歴ログをデータベースに格納しておき，侵入検知システムから受け取った不正アクセスパケットの情報を元にデータベースを解析することで，侵入経路追跡を行う．

パケットログ収集装置（S1，S2，S3）
パケットログ収集装置は各サブネットに 1 つ存在し，サブネットを流れる全てのパケットに関するパケット情報（取得日時，Ether，IP，ICMP，TCP，UDP などヘッダ情報など）を収集する．

対象ホスト（H1，H2）
対象ホストは，攻撃者の攻撃目標となるサーバや踏み台として利用されうるサーバを表す．対象ホスト上では，そのホストで生成されたプロセスに関する情報（プロセス ID，親プロセス ID，実ユーザ ID など），およびリモートとの通信履歴（通信先 IP アドレス，ポート番号，通信プロセスのプロセス ID など）に関する情報を収集する．これらの情報は，対象ホストが攻撃パケットを送出した経緯の特定に用いる．

ルータ（R1，R2，R3）
一般的に設置されているルータまたはゲートウェイを表しており，パケットのルーティングなどを司る．

侵入検知システム（I1，I2，I3）
ネットワーク上を流れるパケットを監視し，不正アク

---

* A Trace Back System Using Packet Information and Communication Histry

† Shigeki KITAZAWA, Seiji FUJII, Takehiro OKOSHI, Nobuhiro KOBAYASHI, Kiyoto KAWAUCHI, Kotaro KATSUYAMA
‡ Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1, Ofuna, Kamakura, Kanagawa, 247-8501, Japan

セスパケットを検知した場合には，検知したパケットと警告を侵入経路追跡サーバへ通知する．

4 ログ解析アルゴリズム

提案する侵入経路追跡サーバでは，(1) ホストレベル追跡，(2) ルータレベル追跡，(3) ホスト内部追跡という3つの異なる経路解析を行いながら，侵入経路を特定する．これは，解析する1つの侵入経路を異なる視点から解析することで，正確かつ効率的に侵入経路を特定するためである．ここでは，特に提案システムにおけるルータレベル追跡について触れ，ホスト内部追跡手法について詳細を述べた後，侵入追跡のスケジューリングについて説明する．

4.1 ルータレベル追跡

ルータレベル追跡では，不正アクセスパケット情報に含まれるパケット取得日時とIP TTL値を除く全てのパケット情報が一致するパケットをデータベースから検索する．ここで得られる検索結果には，侵入経路上の各ルータ間で送受信されたパケットに加え，不正アクセスパケットとパケット情報は一致しているが，不正アクセスパケットとは無関係なパケットが含まれている可能性がある．したがって，不正アクセスパケットとは無関係なパケットを取り除き，正確な不正アクセスパケット中継経路を特定するため，検索結果に含まれる各パケットのIP TTL値によるソートを行った後，ルータのEthernetアドレスによる侵入経路の構成処理を行う．

4.2 ホスト内部追跡

ホスト内部追跡では，不正アクセスパケットを生成し，送出したプロセスを特定するとともに，そのプロセスの親プロセスをたどり，親プロセスの中に外部と通信しているプロセスがある場合は，その対象ホストが踏み台とされている可能性があるとみなし，さらに追跡を継続する．

ホストレベル解析もしくは，ルータレベル解析が既に行われており，その解析の結果，パケットは対象ホストの通信ポートYから送信されたことが特定されているものとする．このとき，そのパケット取得日時を検索キーとしてデータベースを検索し，通信履歴からその時間にその対象ホストの通信ポートYを使用していたプロセス（パケット生成プロセス）に関する情報を得る．検索の結果得られたプロセスが外部と通信を確立していた場合は，そのプロセスの通信履歴を検索キーとして，データベースを検索し，外部装置から受け取ったパケットを特定する．パケット生成プロセスが外部装置からの接続による通信を確立していなかった場合は，同様の処理を親プロセスに対して行う．

パケット生成プロセスが外部装置からの接続による通信を確立していたプロセスが見つかるか，親プロセスが定義されないプロセス（オペレーティングシステムの特別なプロセス）にたどり着くまで，上記の処理を繰り返し行う．親プロセスが定義されないプロセスにたどりついた場合には，そのホストを攻撃者が直接利用したコンピュータであると断定する．

4.3 侵入経路追跡スケジューリング

図2は，侵入経路追跡スケジューリングをそれぞれの追跡時系列上に表したものである．図2において，各追跡時系列上の長方形は，その追跡が実行中であることを示しており，網掛けがされているものは，提案システムにおける実質的な追跡の流れを表す．

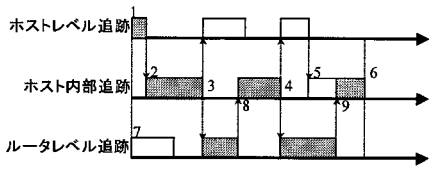

図 2: 侵入経路追跡スケジューリング

まず，初期動作として，侵入検知システムから侵入検知通知を受け取った場合には，ホストレベル追跡とルータレベル追跡を平行して開始する（図2の1，7）．

ホストレベル追跡終了時，そのホストレベル追跡と同時に開始されたルータレベル追跡が未終了の場合（図2の2）のみ，ホストレベル追跡の入力としたパケットの情報を元にホスト内部追跡を開始する．これは，ルータレベル追跡の結果の方がホストレベル追跡よりも正確であると考えられるからである．この理由から，ルータレベル追跡終了時，そのルータレベル追跡と同時に開始されたホストレベル追跡が未終了である場合（図2の8）や，ルータレベル追跡により特定された発信元がホストレベル追跡で特定された発信元と異なる場合（図2の9）は，ルータレベル追跡で特定された発信元のホスト内部追跡を行う．ここで，図2の9のように先にホストレベル追跡の結果によるホスト内部追跡（図2の5）が実行中の場合は，図2の5で開始されたホスト内部追跡を終了させてから新たにルータレベル追跡で特定された発信元のホスト内部追跡を行う．

ホスト内部追跡終了時，ホスト内部追跡の入力としたパケットを生成したプロセスが，ネットワークを経由した外部装置からの命令を受信していた場合には，その命令を伝達したパケットを特定し，特定したパケットを入力とするホストレベル追跡およびルータレベル追跡を同時に開始する（図2の3，4）．その他の場合はホストレベル追跡，ルータレベル追跡ともに開始しない（図2の6）．

5 まとめ

本稿では，ホストレベル追跡，ルータレベル追跡，およびホスト内部追跡という異なる追跡手法を組み合わせることにより，複数の踏み台を含む侵入経路を正確かつ効率的に特定するための侵入経路追跡システムと，侵入経路追跡スケジューリング方法を提案した．侵入経路追跡スケジューリング方法では，正確性が保証されないホストレベル追跡の結果をルータレベル追跡の結果で裏付けしながら追跡を継続していく．したがって，ホストレベル追跡のみの場合よりも正確に，また，ルータレベル追跡のみの場合よりも効率的に，侵入経路を特定可能となる．

参考文献

[1] 浅香 緑，“モバイルエージェントによる侵入検出システムのための情報収集方式”，電子情報通信学会論文誌，Vol.J81-D-I No.5，pp532-539，1998.

[2] 竹爪他，“不正アクセス発信源追跡アーキテクチャの一検討”，情報処理学会第60回全国大会，6Q-06，2000.