イントラネットセキュリティシステムにおける協調型DoS追跡技術

角田 裕[†] 太田耕平[††] 田中真一[†††]
和泉勇治[†] 加藤寧[†]
キニグレンマンスフィールド[††] 根元義章[†]

セキュリティ管理の重要性が高まる中，インターネット全体の脅威となっているDoS攻撃に対する抜本的な対策として攻撃トラヒックの追跡技術が研究されている．しかし，最終的な攻撃者の特定には，高精度追跡技術などの主要な技術とともに，多くのネットワークが協調して追跡する技術が鍵となっている．そのためには，ネットワーク管理に従事する組織が各々の知識と経験を横断的に用いて，総合的に問題解決にあたることが重要である．本論文では，インターネットにおけるDoS攻撃の追跡をネットワーク管理に必須な一要素と位置付け，産学が連携して技術開発にあたった．その結果，DoS攻撃の高精度追跡技術に加え，複数のネットワークが協調し広域にDoS攻撃を追跡する技術を統合したイントラネットセキュリティシステムを実用化した．

Collaborative DoS Traceback Technology for Intranet Security Systems

Hiroshi Tsunoda,[†] Kohei Ohta,[††] Shinichi Tanaka,[†††]
Yuji Waizumi,[†] Nei Kato,[†] Glenn Mansfield Keeni[††]
and Yoshiaki Nemoto[†]

DoS attacks pose a serious threat to the integrity of the Internet. Many countermeasures against DoS attacks have been proposed, among which traceback is a promising countermeasure. However, it is necessary to facilitate a collaborative mechanism among multiple networks in order to locate an attacker in practical situations. To develop such an effective mechanism, relevant entities from the academia, industry, and government should collaborate. As the first step towards fulfill this vision, we consider one of the important network management issues, i.e., DoS traceback, and develop a collaborative DoS traceback technology for an intranet security system via industry-university cooperation.

1. はじめに

ネットワークが社会的にも重要なインフラとなっている近年，ネットワーク管理システムの重要性が増すとともに，その役割も変化しつつある．従来の役割は自ネットワークの死活，性能，障害監視などの受動的なものが主であったが，現在はウィルス情報や脆弱性の早期把握と対策などのために，外部と連携する能動的な役割も求められるようになっている．さらに，管理の空白が致命的となるセキュリティ管理の面では，管理システム自体の安全性と信頼性の確保も重要な役割の1つとなっている．

セキュリティ管理の分野では，ネットワークに与える影響が深刻であり，既存技術での対応が困難な不正アクセスであるDenial of Service（DoS）攻撃について，抜本的な対策が必要とされている．抜本的な対策の1つとして，攻撃トラヒックの追跡による攻撃元の特定があり，多くの要素技術が提案され，部分的には実用化が進められている．しかし，インターネット全体にわたってDoS攻撃を追跡する方法は実現されておらず，追跡手法自体の改良とともに大きな課題として残っている．

そこで，本研究では，トラヒックパターンを活用した追跡方式[1)]を基盤とし，追跡方式の改良による追跡精度の向上とともに，

- 複数の組織による協調型広域追跡機能
- 安全性と信頼性

† 東北大学大学院情報科学研究科
Graduate School of Information Sciences, Tohoku University
†† 株式会社サイバー・ソリューションズ
Cyber Solutions Inc.
††† 東日本電信電話株式会社
NIPPON TELEGRAPH AND TELEPHON EAST CORPORATION

を有したイントラネットセキュリティシステムを開発する．また，安全性と信頼性の強化のために，インターネット標準の効果的な活用技術を実用化する．

実用上の追跡精度を向上させるには，実際のネットワーク運用環境に関するノウハウが不可欠である．しかし，当初は研究者に開放されていたインターネットは，近年では，社会のインフラとしての重要度を増したことで，研究目的での利用が制限されている．その結果，ネットワーク構造や利用形態の多様化，複雑化と合わせて，実用的なネットワーク技術の研究開発がますます困難になっている．従来は，いくつかの公開データ[2)~4)]に基づいて研究開発が行われてきたが，現在では新規のデータを見出すことは容易ではなく，研究開発の基礎データと実状との間に齟齬が生じつつある．この状況のもと，研究目的の実験用大規模ネットワークを構築する研究も進められ効果をあげている[5)]．しかし，ネットワーク構成だけではなく，利用状況やトラヒック特性を再現することは依然として困難な課題である．

本論文では，上記のような現状を打破し，実用的なインターネット技術の研究開発において，産学連携によるアプローチがきわめて有効であることを述べる．本研究では，文部科学省による知的クラスター創成事業の一環として，地域の大学，通信事業者，およびセキュリティ事業者が連携し，不正アクセスの中でもその対策が課題となっている DoS 攻撃を追跡する技術を核とした研究開発を進めた．追跡アルゴリズムの設計を大学が担当し，通信事業者と共同した実証実験で得られた結果をもとにアルゴリズムを改良した．そして，インターネット標準技術とイントラネットセキュリティに関する豊富な経験を有するセキュリティ事業者が中心となり，DoS 攻撃の協調追跡機能を有するイントラネットセキュリティシステムを開発した．また，その開発の過程で得られたシステムの安全性および信頼性強化技術を，製品として実用化した．

以下，2 章において，DoS 攻撃の協調追跡を実現するための課題と，解決策としての産学連携の有効性について述べる．次に，3 章ではトラヒックパターンを用いた DoS 攻撃追跡手法の概要と本研究で確立した追跡の高精度化技術を示す．そして，4 章では，本研究の目的である DoS 攻撃の協調型追跡機能を備えたイントラネットセキュリティシステムの要件を具体化し，本研究で開発したシステムについて説明する．最後に 5 章で全体をまとめる．

2. 産学連携による協調型 DoS 追跡技術の研究開発

2.1 協調型 DoS 追跡技術の開発における課題

DoS 攻撃は，大量のパケットを被害者に対して送信し，被害者によるサービスの提供を妨害する攻撃である．その攻撃の影響の深刻さと，ファイアウォールなどの既存技術では十分な対応が困難であることから，その対策が大きな課題となっている．DoS 攻撃の影響は，被害者のサービスが妨害されるだけにとどまらず，攻撃トラヒックにより不法に帯域を占有される途中経路のネットワークにも及ぶ．そのため，真の対策として攻撃者の特定と排除が必要であるが，攻撃パケットの送信元アドレスが改竄されているため攻撃者の特定は容易ではない．そこで，DoS 攻撃によるトラヒックの経路を逆にたどり攻撃者を発見する追跡技術の研究が行われ[6),7)]，様々な手法が提案されている[8)~11)]．著者らも，DoS 攻撃の脅威が認識され始めた当初の 1998 年より追跡技術の研究に取り組み，トラヒックパターンを用いた追跡方式を提案している[1),12),13)]．本研究では，トラヒックパターンを用いた追跡をインターネット全体にわたって実現することを目指し，産学連携によるアプローチを通じて，協調型追跡機能を有するイントラネットセキュリティシステムを開発する．

追跡技術などの実用的なセキュリティ技術の研究開発において，技術検討や評価の過程で実際のネットワーク運用環境に関するノウハウが不可欠である．そのため，MIT による取り組み[2)]に代表されるような，実際の攻撃やネットワークのトラヒックデータを収集し研究用途に広く提供する試みが行われている．MIT のデータ[2)]は，不正アクセスを実験ネットワーク上で再現して作成したデータであり，不正アクセス検知システムの性能評価の指標として多くの研究で用いられている．しかし，再現した不正アクセスは 1998 年〜2000 年当時のものであり，不正アクセスの現況とは必ずしも一致するものではない．実トラヒックを観測したデータとしては，ローレンス・バークレイ研究所が Web サーバやクライアントの入出力およびインターネットのバックボーンで収集したデータを公開しているが[3)]，公開されているデータは 2000 年までのものであり現状との乖離が大きくなっている．WIDE プロジェクトの MAWI グループが公開しているバックボーントラヒックのデータ[4)]は，つねに最新のデータが提供されていることからも非常に有益である．しかし，セキュリティ対策が立ち遅れており，今後の技術開発が重要となるイントラネットに関しては，プライ

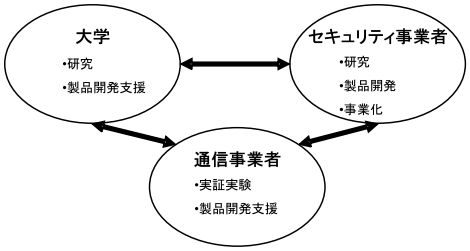

図 1 研究開発体制図
Fig. 1 Research and developement system.

バシの問題などからその情報は公開されていない．このような問題に対するアプローチとしては，ワームやウィルスの挙動を再現する実験環境 VM Nebula[14] や，仮想化技術などの活用によって様々な構成の実験ネットワークを構築可能な StarBED プロジェクト[5] などがある．しかし，追跡技術の研究で重要となるのは，ネットワークの実際の利用状況の把握および再現である．

2.2 本研究の実施体制

本研究では，文部科学省による知的クラスター創成事業の支援の下，**図 1** に示すように地域の大学，通信事業者，セキュリティ事業者の 3 者をメンバとする産学連携による技術開発を実施した．まず，研究開発の開始時点で大学が有していた DoS 攻撃追跡技術の実用的な有効性の検証と，実用に際しての問題点を明らかにするために，実際のネットワーク運用状態を反映可能な大規模な実験ネットワークを構築した．この実験ネットワークは，多数のノードやスイッチと様々な帯域のリンクを有する必要があり，その設計と管理，保守自体が研究開発における大きな課題であった．そこで，ネットワーク運用管理の実務に関して豊富な知見を有する通信事業者がトポロジ設計の段階から関わり，大学と通信事業者が連携してネットワークを構築した．その結果，実用に即した検証が可能であり，かつその保守管理のコストを考慮したネットワークの構築に成功した．実験ネットワークを利用した実験においても，大学と通信事業者が緊密に連携し，実証実験と追跡アルゴリズムの改良のサイクルを早期に繰り返すことで，高精度な DoS 攻撃追跡技術を確立した．また，セキュリティ事業者による DoS 攻撃の協調追跡機能を備えたセキュリティシステムのプロトタイプ開発においても，構築した実験ネットワークは，技術検討のフィールドおよびテスト環境として大きな役割を果たした．

DoS 攻撃の最終的な攻撃者の特定には，実用上の追跡精度に加えて，インターネット全体にわたった追跡の実現が必要であり，複数のネットワークや異なる追跡システム間の連携が不可欠である．すなわち，DoS 攻撃の追跡を実用化するにあたり，協調型追跡の実現が鍵となっている．同時に，追跡システム自体が実際の運用に耐えうる安全性と信頼性を有していなければならない．そこで，本研究では，イントラネットセキュリティ分野における豊富な実績を有するセキュリティ事業者が，その知見を生かし DoS 攻撃追跡と追跡情報交換機構をイントラネットセキュリティシステムへ実装した．IETF（Internet Engineering Task Force）における標準化活動への貢献を通じインターネット標準技術にも精通している同事業者によって，インターネット標準案[15] に準拠した追跡情報の交換機構を実現することができた．同時に，インターネット標準技術を効果的に活用する技術を確立・導入することで，システム自体の安全性と信頼性を大幅に強化することに成功した．

このように，本研究においては，大学，通信事業者，セキュリティ事業者が相互に協調するとともに，要素技術の開発，実証実験および製品化支援，実用化システム開発というそれぞれの役割を果たすことで，DoS 攻撃の広域協調追跡機能を備えた総合的なセキュリティシステムのプロトタイプを開発した．以下，3 章と 4 章において，基盤となるトラヒックパターンを用いた DoS 攻撃の追跡方式と，協調型広域追跡機能を有するイントラネットセキュリティシステムについて，その技術の詳細と効果をそれぞれ述べる．

3. DDoS 攻撃の高精度追跡技術

本章では，まずトラヒックパターンの類似性を利用した DoS 攻撃追跡方式の概要を述べる．次いで，DoS 攻撃が複数の地点から分散して行われる Distributed DoS（DDoS）攻撃を高精度に追跡するための，追跡アルゴリズムの改良について述べる．

3.1 トラヒックパターンを用いた DoS 攻撃追跡方式の概要

トラヒックパターンを用いた DoS 攻撃追跡は，各リンクで観測したトラヒックパターンの形状を比較することで行う[1),12),13)]．トラヒックパターンはリンクを通過したパケット数の時間的推移であり，**図 2** に示すように，観測ウインドウ内のタイムスロットごとのパケット数によってその形状が定まる．そのため，形状が類似したパターンが 2 つのリンクで観測された場合には，それらのリンクを同じトラヒックが通過したと推定する．形状の類似性の評価指標としては，2 つのパターン間の相関係数を用いる．

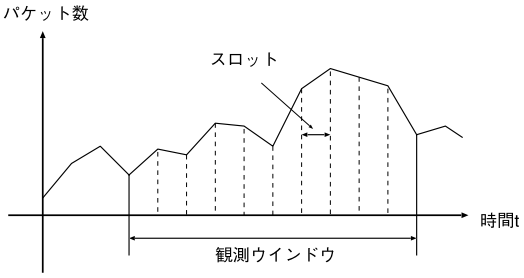

図 2 トラヒックパターン
Fig. 2 Traffic pattern.

トラヒックパターンを用いた追跡は，用いる追跡情報が単純な量的情報のみであるため，送信元 IP アドレス改竄の影響を受けない．また，個々のパケットのペイロード情報を精査しないため，大容量の DoS 攻撃にも容易に対応可能であるとともに，通信のプライバシも保護することができる．

しかし，DDoS 攻撃の場合には，複数の攻撃トラヒックの合流によるパターン形状の変化や，個々の攻撃トラヒックの規模が他のトラヒックと比較して相対的に小さくなることで，正確な追跡が困難となる．そこで，次節では DDoS 攻撃の高精度追跡を実現するための追跡アルゴリズムを説明する．

3.2 DDoS 攻撃に対応した追跡アルゴリズム

複数の地点から DoS 攻撃が分散して行われる DDoS 攻撃の場合，複数の攻撃トラヒックの合流によってトラヒックパターンの形状が変化しうる．そのため，単純な 1 対 1 のパターン比較では正確な追跡が困難である．

この問題を解決し，DDoS 攻撃の追跡精度を向上させる手法として，著者らは 2 次計画法に基づいたトラヒックパターンの比較による追跡方式[16] を提案している．この方式では，ネットワークの合流地点を想定し，合流地点に入力するパターンと，その地点から出力されるパターンの比較過程を 2 次計画問題として扱う．そして，その 2 次計画問題を解くことで，各入力トラヒックが出力トラヒックに含まれる割合を算出し，その割合に基づいて攻撃に関連する入力リンクを判断する．従来手法では攻撃の合流数が増えるにつれて追跡精度が低下するが，2 次計画法に基づいたパターンの比較によって追跡精度が大幅に向上することが確認されている．

DDoS 攻撃の追跡におけるもう 1 つの課題として，合流前の個々の攻撃トラヒックはパターン形状の特徴的な変化として現れにくいことがあげられる．これは，合流したトラヒックで攻撃することが前提である DDoS 攻撃では，個々の攻撃トラヒックは比較的小規模であり，他のトラヒックとの量的な差異が生じにくいことが原因である．この問題に対し，著者らは独立成分分析を用いた追跡手法[17]，トラヒックの最小流量に着目したフィルタリングをパターンに施す手法[18),19)] を提案している．

独立成分分析を用いた手法では，各パターンを複数の独立な成分に分解し，分解後の成分に基づいて類似性を評価する．そのため，パターンの形状を直接的に比較する場合と比べて高解像度な比較が可能となる．また，成分に分解する過程で対象リンクの過去の通信状況を考慮に入れるため，追跡時点のトラヒック量の変化だけではなく，通常状態との差異をもとに評価することができる．

一方，トラヒックの最小流量に着目したフィルタリング手法は，比較対象のパターンに含まれる短期間のトラヒック変動の影響を除去することを目的とする．具体的なフィルタリングは，パターンに対して一定幅のウインドウを適用し，各ウインドウ中の単位時間あたりの最小トラヒック量を要素とするパターンを生成することで行う．そして，フィルタリング後のパターンの類似性を相関係数を用いて比較する．DoS 攻撃による変動は長期的な変動であるため，フィルタリング処理により結果的にパターンに含まれる DoS 攻撃の部分が際立ち，追跡精度の向上につながる．

3.3 追跡精度の評価

提案しているそれぞれの DDoS 攻撃追跡手法について，シミュレーションによって追跡精度を評価する．

まず，ネットワークの合流点への入力リンク数を 10，出力リンク数を 1 として**図 3** のようにネットワークの合流点をモデル化する．次にネットワーク運用の知見に基づいて通常トラヒックのパターンを決定し，各リンクに割り当てる．そして，k 個の入力リンクに人工的に作成した DoS 攻撃のパターンを付加して，合流数 k の DDoS 攻撃をシミュレートした．

他のトラヒックに埋もれるような小規模の DoS 攻撃を想定し，合流前の攻撃トラヒックの単位時間あたりのパケット数を通常トラヒックのパケット数の 1/2 程度に設定した．また，DoS 攻撃のパターンを付加する時間をずらすことにより，攻撃開始時間が異なった DDoS 攻撃を再現した．

上記の条件で各リンクに通常トラヒックと攻撃トラヒックをランダムに割り当て，合流数 k ごとに 100 回ずつシミュレーションを行い，判定成功率の平均を算出した．判定成功率は，全入力リンク数と判定成功した入力リンク数の比によって定義され，総合的な追

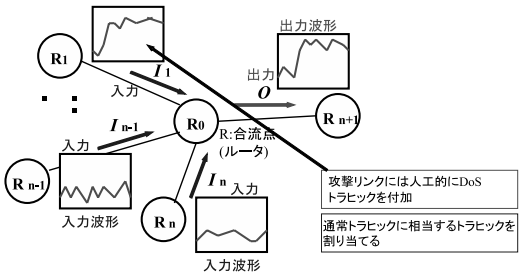

図 3 ネットワークの合流点のモデル
Fig. 3 Model of network confluences.

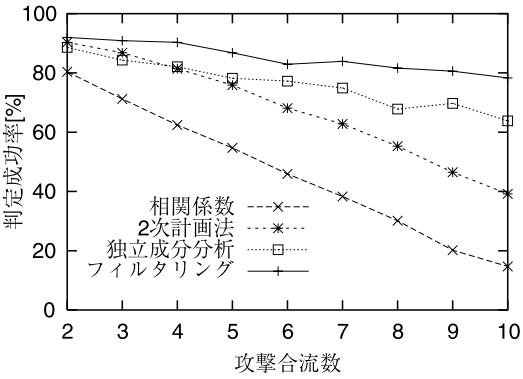

図 4 各種追跡方式の追跡精度
Fig. 4 Accuracy various traceback methods.

跡性能を表す．**図 4** に，各手法における合流数と判定成功率の関係を示す．

図 4 より，合流数の増加にともなってすべての手法で判定成功率が低下することが分かる．手法ごとの追跡精度を比較すると，相関係数を判定基準とする手法が最も精度が低く，DDoS 攻撃に対応した追跡方式では追跡精度が向上している様子が分かる．特に，最小値に着目しフィルタリングを行う手法[18),19)] は，合流数の増加による精度の低下度合いが最も小さく，全体を通して最高の性能を示している．この結果から，追跡アルゴリズムの改良によって，トラヒックパターンを用いた追跡を DDoS 攻撃に対応させるとともに，大幅な高精度化を実現できたといえる．次章では，このトラヒックパターンを用いた高精度 DoS 攻撃追跡をインターネット全体にわたって広域で実施する，協調型の追跡機能を有したセキュリティシステムの実用化について述べる．

4. DoS 攻撃の協調追跡機能を有するイントラネットセキュリティシステム

本章では，研究開発の目的である協調型の DoS 攻撃追跡機能を有した高信頼性イントラネットセキュリティシステムにおける要件を整理し，本研究で確立し

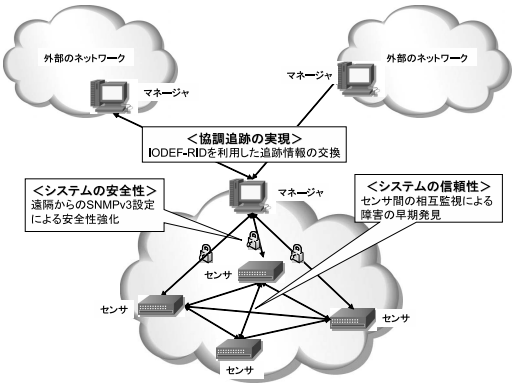

図 5 DoS 攻撃の協調追跡機能を有するイントラネットセキュリティシステム
Fig. 5 An intranet security system with collaborative Dos traceback technology.

実用化した技術について説明する．

図 5 は，本研究開発で実用化したイントラネットセキュリティシステムが有する機能の概要を示している．各ネットワークは，ネットワーク内での追跡動作を管理するマネージャと，トラヒックパターンを観測するセンサによって構成されている．まず，ネットワークどうしの協調による広域追跡を実現するために，各ネットワークのマネージャに追跡情報の交換機能を実装する．また，マネージャとセンサ間の通信の安全性を強化するために，複数センサへの SNMPv3 一括設定技術を導入し，SNMPv3 による安全なセンサ管理を実現する．そして，センサ間の相互監視によって，センサで発生した障害の早期検知を実現し，システム自体の信頼性を強化する．

以降では，DoS 攻撃の協調追跡と，システムの安全性と信頼性の強化に関して，それぞれ 4.1 節と 4.2 節で述べる．

4.1 DoS 攻撃の協調型追跡の実現

DoS 攻撃の追跡において，一部の方式を除いて共通の課題として残されているのが，いかにして広域な追跡を実現するか，という問題である．追跡には経路上のトラヒックの観測情報が必要であるが，通常，管理権限のない外部からの観測情報の参照は許可されておらず，広域追跡は事実上不可能となっている．この現状を打破するには複数のネットワークの協調が不可欠であり，そのためには標準化された通信によって追跡情報を交換することが必須となる．

そして，この追跡情報の交換においては，

- 追跡情報の記述方式とトランスポートプロトコル
- 追跡情報の正規化アルゴリズム

を定める必要がある．まず，追跡情報は協調するすべ

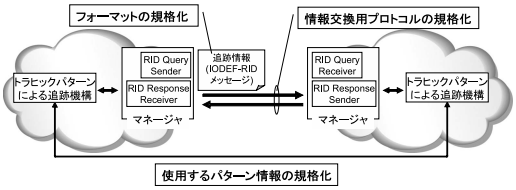

図 6 DoS 攻撃の協調追跡におけるシステム構成
Fig. 6 Architecture of a collaborative Dos traceback system.

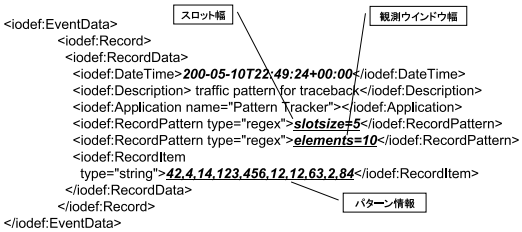

図 7 トラヒックパターン情報を記述した IODEF メッセージ
Fig. 7 IODEF message including traffic pattern information.

てのマネージャが理解可能な方式で記述されており，交換時に使用するトランスポートプロトコルが取り決められていなければならない．また，異なる追跡システム間で追跡情報を相互に利用するためには，送受信する追跡情報を正規化するアルゴリズムについて双方の合意が必要である．

4.1.1 追跡情報の記述方式とトランスポートプロトコル

ウィルスへの対策や脆弱性の早期把握などのために重要な技術となっているセキュリティインシデント情報の交換は，IETF（Internet Engineering Task Force）でも INCH（Incident Handling）WG によって議論が行われ，著者らはその基本要件を提案している[20]．INCH WG では，情報交換フォーマット IODEF（Incident Object Description and Exchange Format）[21] の標準化を進めており，IODEF で交換する情報の 1 つとして DoS 攻撃の追跡情報に着目している．そして，追跡情報の交換方式を定めた IODEF-RID（Real-time Internet Defense）[15] が提案されている．本論文ではこの IODEF-RID を用いて協調型の追跡システムを実現し，DoS 攻撃の追跡に残された最後の大きな課題を克服する．

図 6 は協調追跡を実現するシステム構成を示している．各組織はそれぞれ任意の方式によって内部の追跡を行うとし，マネージャは外部との連携のために IODEF-RID に準拠した通信機能を備える．この構成によって，個別の追跡技術に依存しない方式で，広域追跡を実現する．

トラヒックパターン情報を記述した IODEF メッセージの例を**図 7** に示す．1 つのトラヒックパターンは，生成時のスロット幅，観測ウインドウ幅とともに，CSV 形式で記述した各スロットのパケット数によって表現されている．

IODEF メッセージは XML（eXtensible Markup Language）がベースであることから，その交換には SOAP（Simple Object Access Protocol）の使用が検討されており，下位のトランスポートプロトコルは HTTP（Hyper Text Transfer Protocol）あるいは SMTP（Simple Mail Transfer Protocol）となる．協調追跡は，あるマネージャから外部のマネージャへの追跡依頼と，外部のマネージャからの追跡結果の応答によって成り立つ．このとき，外部のネットワークの追跡結果が判明するまでには，外部ネットワーク内の追跡処理のために一定の時間が必要であり，追跡の依頼と結果の応答は同期しない可能性が高い．そこで，より非同期通信に適した SMTP を介した IODEF-RID メッセージの送受信機構を実装した．

4.1.2 トラヒックパターン情報の正規化アルゴリズム

追跡情報として使用するトラヒックパターンはトラヒックの流量を直接反映するものであり，パターン生成時の適切なスロット幅，観測ウインドウ幅（図 2 参照）はネットワークごとの利用状況や利用形態によって異なる．パラメータ設定の違いは，生成されるトラヒックパターンの形状の違いにつながるため，異なるネットワークから追跡情報として送信されたトラヒックパターンをそのまま自ネットワークでの追跡に使用できるとは限らない．トラヒックパターンを用いた追跡における基本的な判断基準はパターン形状の類似性であり，形状の類似性を正しく評価するためには双方のシステムが追跡情報として利用できるようにパターンを正規化する必要がある．

図 8 にパターン情報の正規化の例として，2 つのネットワークを 250 秒間観測したトラヒックパターン A と B の形状を比較する場合を示している．トラヒックパターン A は，スロット幅 5 秒でパケット数をカウントした，観測ウインドウ幅 50 スロットのパターンである．一方，トラヒックパターン B は，スロット幅 1 秒でカウントした，観測ウインドウ幅 250 スロットのパターンである．このとき，スロット幅および観測ウインドウ幅が異なるため，正規化なしでは 2 つのトラヒックパターンの形状を正しく比較できない．

本システムでは，この問題を考慮し，双方のシステ

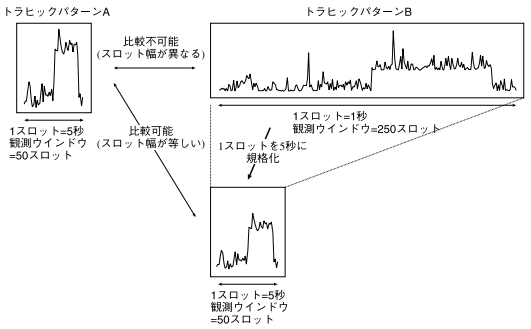

図 8 トラヒックパターンの正規化
Fig. 8 Normalization of traffic pattern.

ムにおけるスロット幅の最大公約数を新たなスロット幅として用いてパターンを整形する．そのために，図 7 に示すように，追跡依頼時に送信する追跡情報の一部にトラヒックパターン生成時のスロット幅および観測ウインドウ幅を含めている．正規化処理は基本的に受信側で行い，受信したパターンと自ネットワークのパターンのいずれかまたは双方を正規化した後に，自ネットワーク内の追跡を実施する．図 8 では，双方のスロット幅の最大公約数は 5 秒であるため，パターン B をスロット幅 5 秒のパターンに正規化することにより，パターン A と B を正しく比較できる．

この正規化アルゴリズムの問題として，パターンの整形によって，正規化前の本来のパターンが有している細かな形状が失われることが予想される．この問題は，双方のスロット幅の差が非常に大きい場合に顕著となり，類似性の評価に悪影響を及ぼすことが懸念される．しかし，トラヒックパターンによる追跡の対象は数分間以上継続する DoS 攻撃であり[16]，そのような攻撃の形状をとらえるための必要なスロット幅の範囲は自ずと限定される．したがって，複数の追跡システム間でスロット幅の設定が大幅に異なることは考えにくく，本節で述べた正規化アルゴリズムは有効に機能すると考えられる．

4.2 システムの安全性と信頼性の確保

ネットワーク管理におけるセキュリティ管理の重要性が高まるにつれて，管理システム自体の安全性，信頼性への要求もますます厳しいものとなっている．ここでは，セキュリティシステムに実用的な安全性と信頼性をもたらす技術として，

- 安全な管理プロトコル SNMPv3[22)~29)]
- 分散管理のための管理情報ベース DISMAN MIB[30)]

の導入について述べる．

4.2.1 SNMPv3 の導入による安全性の強化

ネットワーク管理プロトコルである SNMP（Simple Network Management Protocol）は，今やネットワーク管理に不可欠な技術となっている．しかし，現在エンドユーザまで広く普及しているバージョン（SNMPv1 および v2）は通信内容の暗号化をサポートしておらず，認証機能も貧弱であるため，SNMP の持つ有効性を十分に利用できていない．たとえば，認証のためのコミュニティ名が平文でネットワークを流れることから，遠隔からの機器設定の変更など外部からの書き込みを許可するような運用は，その利便性以上のリスクをともなうために推奨されていない．この問題に対して，セキュリティ面を強化した最新のプロトコルである SNMPv3 がすでに標準化されているが[22)~29)]，その重要性からベンダによる実装は進んでいるものの，導入時の複雑さからエンドユーザへの普及は依然として進んでいない[31)]．近年では，普及の進まない原因は SNMP が独自の技術体系をとっていることであるという認識から，より一般的に知られている技術による実装の標準化も議論されている[32)]．

そこで，本システムでは，最もコストのかかる SNMPv3 の初期設定を遠隔から安全に実施する技術を開発し，実装した．本技術により，SNMPv3 を大規模ネットワークに速やかに導入することが可能となり，結果としてこれまで使用されていなかった SNMP による書き込みを安全に実現できるようになった．本システムは，この技術を利用することで，パターン情報収集に関する設定などを遠隔から動的に変更可能となり，安全性強化と利便性向上の双方を実現した．

4.2.2 センサの相互監視による信頼性の強化

システム全体の信頼性，可用性向上の第 1 歩は，システムの稼働状況をつねに監視し，発生した問題を見逃すことなくいち早く対処することである．本システムでは，トラヒックを監視するセンサの可用性確保が重要である．現在の多くのシステムでは，マネージャが定期的に各センサへの到達性や応答性を確認することで稼働状況を監視している．しかし，この方法では，マネージャ自身に障害が発生した場合には，その他の障害を検知できず対応が遅れてしまう．この一点障害性を回避し障害の早期発見を実現するために，本システムではセンサへの到達性，応答性を他の複数のセンサが確認する．このセンサどうしの相互監視は，既存システムにおけるマネージャ部分の一点障害性の回避につながり，障害の発見と対策を迅速に行うことができるためにシステムの信頼性を強化できる．

本システムでは，この相互監視を実用的なフレー

ムワークとして実現するために，IETF の DISMAN（DIStributed MANagement）WG によって標準化された管理情報ベース（MIB：Management Information Base）である DISMAN MIB を活用した．本システムでは，DISMAN MIB を実装したセンサに対して，前節で述べた SNMPv3 によってそれぞれの監視対象を安全に設定することが可能であり，以後は各センサが自動的に相互監視する．通常時には特定の中央マネージャが不要であるため，マネージャ自身がクリティカルポイントになるリスクもなく，監視トラヒックの集中も発生しない．そして，1 つのセンサを複数のセンサから監視することで，特定のマネージャの障害による問題の見逃しを未然に防止できる．本技術を活用したセンサ管理システムは，多くのセンサによってネットワークを監視するシステムに導入され，実用化されている．

5. おわりに

本論文では，実用的なセキュリティ技術の開発における産学連携の有効性を，Denial of Service（DoS）攻撃の追跡に関する実際の技術開発およびシステム開発を通して述べた．インターネットにおける DoS 攻撃の追跡を実現するためには，追跡精度の向上だけでなく，複数のネットワークに設置された追跡システムの連携による協調型追跡が必要となる．また，同時に，追跡システム自体が実用に耐えうる安全性と信頼性を有していなければならない．本研究では，大学，通信事業者，およびセキュリティ事業者が連携し，DoS 攻撃の協調追跡技術を有する総合的なイントラネットセキュリティシステムを確立した．システム上で動作する追跡技術は，従来のトラヒックパターンを用いた追跡方式をさらに改良し，DDoS 攻撃をも高精度に追跡可能となっている．協調追跡のための情報交換には，標準化が進められている IODEF-RID 方式を採用しており，DoS 攻撃の広域追跡のさらなる実用化を進めるうえで，他の追跡方式を採用しているシステムとの協調も容易に実現可能であるといえる．また，インターネット標準を効果的に活用する技術を実用化したことにより，利便性を損ねることなく，システム自体の安全性と信頼性を実用的なレベルで確保することができる．

本研究開発によって確立した技術は，段階的に製品化されており，現段階では SNMPv3 の導入技術とセンサの相互監視技術がセキュリティ事業者の製品に組み込まれている．システムの信頼性の大幅な向上と，安全な管理プロトコルの最大限の活用が可能となったこの製品は，独創性・市場性に富んだ新製品・新技術・新ソフトウェアを表彰するコンテストにおいて，優秀賞および産学連携特別賞を受賞している[33]．このことからも，本研究は，産学連携の有効性を十分に生かし，実用的なセキュリティ管理技術の確立に貢献したといえる．

謝辞 本研究は，文部科学省による知的クラスター創成事業の援助を受けて実施された．また，東日本電信電話株式会社の與那原亨氏，大森孝雄氏，佐藤良信氏には実証実験に際して多くのご協力をいただいた．ここに感謝する．

参考文献

1) Mansfield, G., Ohta, K., Takei, Y., Kato, N. and Nemoto, Y.: Towards Trapping Wily Intruders in the Large, *Computer Networks*, Vol.34, pp.659–670 (2000).
2) MIT Lincoln Laboratory — DARPA Intrusion Detection Evaluation. http://www.ll.mit.edu/IST/ideval/
3) The Internet Traffic Archive. http://ita.ee.lbl.gov/
4) MAWI Working Group Traffic Archive. http://tracer.csl.sony.co.jp/mawi/
5) Miyachi, T., Chinen, K. and Shinoda, Y.: Automatic Configuration and Execution of Internet Experiments On An Actual Node-based Testbed, *Tridentcom 2005*, pp.274–282 (2005).
6) Belenky, A. and Ansari, N.: On IP Traceback, *IEEE Communications Magazine*, Vol.41, No.7, pp.142–153 (2003).
7) Gao, Z. and Ansari, N.: Tracing Cyber Attacks from the Practical Perspective, *IEEE Communications Magazine*, Vol.43, No.5, pp.123–131 (2005).
8) Bellovin, S.: The ICMP Traceback Message, Internet Draft (2000). http://www.research.att.com/~smb/papers/draft-bellovin-itrace-00.txt
9) Snoeren, A., Partridge, C., Sanchez, L., Jones, C., Tchakountio, F., Schwartz, B., Kent, S.T. and Strayer, W.T.: Single-Packet IP Traceback, *IEEE/ACM Trans. Networking*, Vol.10, No.6, pp.721–734 (2002).
10) Savage, S., Wetherall, D., Karlin, A. and Anderson, T.: Practical Network Support for IP Traceback, *IEEE/ACM Trans. Networking*, Vol.9, No.3, pp.226–237 (2001).
11) Belenky, A. and Ansari, N.: Tracing Multiple Attakers with Deterministic Packet Marking (DPM), *Proc. IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pp.49–52 (2003).

12) Ohta, K., Mansfield, G., Takei, Y., Kato, N. and Nemoto, Y.: Detection, Defense, and Tracking of Internet-Wide Illegal Access in a Distriuted Manner, *Proc. INET2000* (2000).
13) 武井洋介，太田耕平，加藤 寧，根元義章：トラヒックパターンを用いた不正アクセス検出及び追跡方式，電子情報通信学会論文誌 B，Vol.J84-B, No.3, pp.1464–1473 (2001).
14) 三輪信介，大野浩之：再現実験環境「VM Nebula」を用いたウィルス・ワームの解析，インターネットコンファレンス 2003 (2003).
15) Moriarty, K.M.: Incident Handling: Real-time Inter-network Defense, Internet Draft (2005).
16) 坂口 薫，和泉勇治，太田耕平，加藤 寧，根元義章：2 次計画法に基づいたトラヒックパターンの比較による DoS の追跡，電子情報通信学会論文誌 B，Vol.J85-B, No.8, pp.1295–1303 (2002).
17) 佐藤 徹，和泉勇治，根元義章：独立成分分析を用いたトラヒックパターン解析による DoS 攻撃経路追跡手法の提案，電子情報通信学会技術研究報告 NS2004-101 (2004).
18) 内海宏律，角田 裕，和泉勇治，根元義章：トラヒックの最小流量に着目したトラヒックパターンのフィルタリングによる DDoS 追跡の高精度化，電子情報通信学会技術研究報告 NS2005-110 (2005).
19) Utsumi, H., Tsunoda, H., Waizumi, Y. and Nemoto, Y.: Traffic Pattern Filtering Based on Lower Bounds of Traffic Volume for DDoS Traceback, *21st Annual Computer Security Application Conference, Works in Progress Session* (2005).
20) Mansfield, G., Danyliw, R. and Demchenko, Y.: Requirements for the Format for Incident Information Exchange (FINE), Internet Draft (work in progress) (2006). http://www.ietf.org/internet-drafts/draft-ietf-inch-requirements-07.txt.
21) Danyliw, R., Meijer, J. and Demchenko, Y.: The Incident Object Description Exchange Format Data Model and XML Implementation, Internet Draft (2006).
22) Harrington, D., Presuhn, R. and Wijnen, B.: An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, RFC3411 (2002).
23) Case, J., Harrington, D., Presuhn, R. and Wijnen, B.: Message Processing and Dispatching for the Simple Network Management Protocol (SNMP), RFC3412 (2002).
24) Levi, D., Meyer, P. and Stewart, B.: Simple Network Management Protocol (SNMP) Applications, RFC3413 (2002).
25) Blumenthal, B.W.U.: User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), RFC3414 (2002).
26) Wijnen, B., Presuhn, R. and McCloghrie, K.: View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP), RFC3415 (2002).
27) Presuhn, R.: Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), RFC3416 (2002).
28) Presuhn, R.: Transport Mappings for the Simple Network Management Protocol (SNMP), RFC3417 (2002).
29) Presuhn, R.: Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), RFC3418 (2002).
30) White, K.: Definitions of Managed Objects for Remote Ping, Traceroute, and Lookup Operations, RFC2925 (2000).
31) Deployment Report by IESG. http://www.ietf.org/IESG/Implementations/2571-2575-Deployment.txt
32) Integrated Security Model for SNMP (ISMS) WG. http://www.ietf.org/html.charters/isms-charter.html
33) りそな中小企業振興財団と日刊工業新聞社共催の第 18 回中小企業優秀新技術・新製品賞. http://www.nikkan.co.jp/sanken/18singizyutu.html

(平成 18 年 5 月 23 日受付)
(平成 18 年 9 月 14 日採録)

角田 裕（正会員）

平成 12 年東北大学工学部情報工学科卒業．平成 14 年同大学大学院情報科学研究科修士課程修了．平成 17 年同研究科博士課程修了．同年同大学情報科学研究科助手，現在に至る．博士（情報科学）．在学時より，衛星ネットワークの構築，管理，ネットワークセキュリティ等の研究に従事．電子情報通信学会会員．

太田　耕平

平成 5 年東北大学工学部情報工学科卒業．平成 7 年同大学大学院情報科学研究科修士課程修了．平成 10 年同研究科博士課程修了．同年（株）サイバー・ソリューションズ入社．現在に至る．平成 17 年より IPA 研究員．博士（情報科学）．在学時よりインターネット管理，セキュリティ管理等の研究に従事．

田中　真一

平成元年日本電信電話株式会社入社．平成 8 年東海大学工学部通信工学科卒業．平成 15〜17 年東日本電信電話株式会社研究開発センタ所属．ネットワークシステム，インターネットセキュリティシステムの研究開発やネットワーク運用管理の研究に従事．電子情報通信学会会員．

和泉　勇治

平成 8 年東北大学工学部情報工学科卒業．平成 10 年同大学大学院情報科学研究科修士課程修了．平成 13 年同研究科博士課程修了．同年同大学情報科学研究科助手，平成 15 年同講師，現在に至る．博士（情報科学）．ニューラルネットワーク，文字認識，コンピュータネットワークの構築，管理等の研究に従事．電子情報通信学会会員．

加藤　　寧

昭和 63 年東北大学大学院修士課程修了．平成 3 年同大学院博士課程修了．同年同大学大型計算機センター助手，平成 7 年同大学大学院情報科学研究科助手，平成 8 年同助教授，平成 15 年同教授，現在に至る．工学博士，コンピュータネットワークの構築，管理，文字認識，ニューラルネットワーク等の研究に従事．電子情報通信学会，IEEE 各会員．

キニグレン マンスフィールド

昭和 52 年インド工科大学大学院修士課程修了．昭和 54 年インド理科大学大学院修士課程修了．昭和 63 年東北大学大学院工学研究科博士課程修了．以来，インターネット関連研究に従事．現在，東北大客員研究員．(株) サイバー・ソリューションズ代表取締役．工学博士（東北大学）．IETF の活動にも貢献．Internet Society，IEEE，ACM 各会員．

根元　義章（フェロー）

昭和 43 年東北大学工学部通信工学科卒業．昭和 48 年同大学大学院博士課程修了．同年同大学助手，昭和 59 年同大学電気通信研究所助教授，平成 3 年同大学大型計算機センター教授，平成 7 年同大学大学院情報科学研究科教授，工学博士．マイクロ波伝送路回路，コンピュータネットワーク，情報伝送システム，画像処理，文字認識等の研究に従事．昭和 56 年 IEEE・MTT・Micro Wave Prize 受賞．平成 17 年 IEEE 衛星通信貢献賞受賞．平成 18 年文部科学大臣表彰科学技術賞受賞．平成 18 年情報通信月間総務大臣表彰受賞．電子情報通信学会フェロー，IEEE シニアメンバー．