平成１７年度新規委託研究テーマ研究計画書

（インターネットにおけるトレースバック技術に関する研究開発）

１．研究テーマ

「インターネットにおけるトレースバック技術に関する研究開発」

課題ア： 全体アーキテクチャの設計
課題イ： トレースバック・アルゴリズムの開発
課題ウ： トレースバック用データ収集装置（プローブ装置）の開発
課題エ： トレースバック・プラットフォームの実証実験

２．研究開発の目的

インターネットの急速な拡大と重要性の向上は改めていうまでもないところである。また、それに伴い、インターネットに対する攻撃・脅威により引き起こされうるインシデントの大きさについても年々増大の一途を辿っている。このように大規模インシデントに対する早期警戒態勢の整備が急務である。

そのような状況を受け、情報通信研究機構では平成 16 年より「広域モニタリングシステムに関する基盤技術の研究開発」を実施している。これは通信インフラ事業者や ISP 事業者の連携・協力の下で、その基礎となる広域ネットワークの監視活動を効率的かつ実効的に行うための仕組みを作るものである。具体的には監視対象から必要な情報の収集が可能なプローブ装置の開発を行うとともに、ネットワーク全体の状況監視において複数のネットワーク階層やネットワークの面的な網羅性にも十分対応できるような情報収集方式の開発を進行している。

上記の研究開発であるモニタリングは、受動的な警戒態勢であるといえる。ネットワーク上でのインシデント警戒態勢を行うためには、このような対策に加えて、能動的な警戒手段も必要であると考えられる。すなわち、ネットワーク上のある地点において攻撃の予兆を検知したときに、その攻撃がどこから行われようとしているかを探索するといった能動的な警戒態勢である。つまり、トレースバックに関する研究開発を行う必要がある。

トレースバック技術のうち、その中心となる IP レイヤにおける研究は十数年

にわたり研究が進められている。そのため、理論研究としては成熟しつつあるものの、フィールド広域に対する実装が行われている例は極めて少ない。また、IP 層よりも上位のアプリケーション層に関しては、理論研究自体まだ成熟していない状況である。

不正アクセス、DoS 攻撃、ウイルス発信等のサイバー攻撃は、攻撃パケットのソースアドレスを詐称しているため、攻撃の発信源を把握することは困難である。本件では、パケットのソースアドレスが詐称されているサイバー攻撃であっても、その発信源を把握しうるトレースバック技術を開発することを目的としている。

本件は、インターネットの実運用環境への実装を目指した研究開発を行う。具体的には、基盤となる全体のアーキテクチャの設計、トレースバック・アルゴリズムの開発、トレースバック用データ収集装置の開発、及び、それらを統合したトレースバック・プラットフォームの開発を行い、更に、当該プラットフォームの実装及び運用体制について検討し、実運用環境への実装に向けた統合試験・検証を行う。

３．研究開発期間及び平成１７年度予算

研究開発期間は、平成１７年度から平成２１年度までの５年間とする。

平成 17 年度　３００百万円程度以内

４．研究開発課題

本研究テーマにおいては、トレースバック機構に関して、以下に示す 4 つの内容を含む研究開発を行うものとする。

課題ア： 全体アーキテクチャの設計
課題イ： トレースバック・アルゴリズムの開発
課題ウ： トレースバック用データ収集装置（プローブ装置）の開発
課題エ： トレースバック・プラットフォームの実証実験

課題ア：全体アーキテクチャの設計

実運用環境への実装を想定したトレースバック・アーキテクチャおよび各コンポーネント間のプロトコルを設計する。

課題ア－１：トレースバック機構を構築する上で考慮するべき事項の網羅

トレースバック機構のアーキテクチャを構築する上で考慮するべき事項を網羅的に抽出・整理することが本研究開発の最初の課題である。考慮するべき事項のうち、トレースバック機能それ自体に関わるものとしては基本的なトレースバック方式の開発や、AS を越えてのトレースバックを実行するときの境界処理の問題等が挙げられる。また、トレースバックによりプライバシーが侵害されないようにするための工夫も要求される。

課題ア－２：基本的なトレースバック方式の開発

不正なアクセスが発見されたとき､例えその発信元が詐称されていたとしても真の発信元を明らかにすることができるような、基本的なトレースバック方式を開発するものとする。前述の通り、IP パケットトレース

バックに関する理論的な研究は長く行われており、その成果も多い。しかし、実際にその理論をシステムに実装することについての成果はごく少数であり、要求分析・運用経験等に関する成果は存在しないのが現状である。本課題ではそのような現状を鑑み、実運用環境への実装を前提とした基本方式を開発することが必要である。

課題ア－３：トレースバックシステムの相互接続アーキテクチャの開発

世界中のあらゆるISP事業者等が同一のトレースバック方式を採用することを前提としたアーキテクチャは現実的ではない。そのような事情を鑑み、異なるトレースバック方式を採用しているISP事業者等を経由しているパケットに対しても継続してトレースバックを可能とするアーキテクチャの開発を行うものとする。

また、複数のISP事業者間でのトレースバックを考慮する際には途中NATやFirewallを経由することを想定しなければならない。そのような正規にIPアドレスを変換する機器を経由してなおトレースバックを可能とするようなアーキテクチャを開発する必要がある。

課題イ：トレースバック・アルゴリズムの開発

インターネット上に多数配置されるプローブ装置が収集するデータと市販のセキュリティ装置のログ等や、既存のネットワーク機器の設定等を利用して、ソースアドレスが詐称されたパケットによるサイバー攻撃等の発信源をリアルタイムに近い時間以内に特定しうるアルゴリズムについて研究開発を行う。その際、学術レベルですでに提案されている手法についても網羅的に調査・評価し、その採用や改良等について検討を行う。

また、IP パケットトレースバック・アルゴリズム、アプリケーショントレースバック・アルゴリズムのいずれに関してもプライバシーの保護についても既存方法についての検討を行い、盛り込むものとする。

課題イ－１：IP パケットトレースバックアルゴリズムの開発

課題アで示したアーキテクチャを実現するために、高速、正確、低負荷な IP パケットトレースバックアルゴリズムを開発するものとする。特に本課題で研究開発するアルゴリズムは実運用環境上に適用されることを考慮し、計算コスト、機器設置コスト等が現実的なものであることが要求される。それらの条件を満たすためにも、既存方式についての網羅的調査を行い、最適なアルゴリズムを選択・開発するものとする。

また､課題アで定めたアーキテクチャにおけるプライバシー保護方式に準ずるように、トレースバック・アルゴリズムにおいても利用者のプライバシーを侵害しないための工夫を盛り込む必要がある。

課題イ－２：アプリケーショントレースバックアルゴリズムの開発

アプリケーションレベルでの情報を参照するトレースバック・アルゴリズムを開発するものとする。本課題は上記イ-１で開発される IP パケットのトレースバックでは解決できない問題を解決するために実施されるものであることを考慮し、その実装効果が充分に見出せるようなプロトコル / アプリケーションに対して開発を行うものとする。

また、アプリケーションレベルでの情報を取り扱うということから、IP パケット取り扱い時以上に、トレースバックに伴う利用者のプライバシー侵害を生じさせないための工夫を盛り込む必要がある。

課題イ－３:異なるレイヤ由来の情報からトレースバック能力を向上させるアルゴリズムの開発

上記の課題イ－１で開発される IP パケットトレースバックに、イ－２で開発されるアプリケーショントレースバックを組み合わせることによって、単独実行時と比してトレースバックの精度あるいは速度が向上する、あるいは IP パケットトレースバックによっては不可能であったトレースが可能になるようなアルゴリズムを開発するものとする。その際には、アプリケーションレイヤの情報を加えることによって、最終的に得られる情報量がどの程度増加するかということを検討する必要がある。

課題ウ：トレースバック用データ収集装置（プローブ装置）の開発

トレースバック・アルゴリズムで必要となるデータをインターネットから効率的に収集すると同時に、当該データの匿名化等のデータ変換を行う装置を開発する。

本課題については「広域モニタリングシステムに関する基盤技術の研究」の中で同種の機器が開発中である。ハードウェアは「広域モニタリング研究」において開発されるものを継承し、本研究開発においては同装置上にて作動するアプリケーションのみを開発することも可能である。

本装置上で作動するアプリケーションの開発に際しては、同装置へと大量に届くパケットを効率的に処理していくことができなければならない。

課題エ：トレースバック・プラットフォームの実証実験

エ－１：実装および運用体制の検討

本研究開発における実証実験は実用になるたけ近い、複数の ISP 事業者が混在する環境を想定している。そのため、実験を行う際には複数の項目に関して合意・契約を行う必要が生ずると考えられる。

本課題では、そのような複数事業者が混在する環境におけるトレースバックを実施する際にどのような項目についての取り決めが必要であり、それぞれの取り決めはどのような書面あるいはそれ以外の手続きによって実施されるのか、ということについて明らかにするものとする。具体的な検討項目としては、情報管理体制、トレースバック開始の要件等が考えられる。

エー２：攻撃パターンの想定

本実証実験では、実運用環境上にて実際に生じている攻撃をその観測対象とする。それに先立ち、想定される攻撃パターンをリストアップすることとする。ネットワーク上で実際に観測される攻撃パターンは送信パケットの種類やパケット送信期間の長短など多種多様であり、それらそれぞれに対応できるかどうかについて検討することが必要である。

エー３：動作検証

トレースバック・プラットフォームを実運用環境に実装し、エー１で規定された条件に基づいて不正アクセスに対するトレースバックを行う。その上で、以下の各項目に対してトレースバック結果の評価を実施するものとする。評価すべき主たる項目はトレースバックに要した時間、各ノードへの負荷、トレースバックの成功度合いとする。

５．研究テーマ選定の背景、研究開発の必要性及び他で実施されている類似研究との切り分け、標準化の動向

１）当該研究テーマを取り巻く現状

近年、不正アクセス、ウイルス、ワーム、DoS 攻撃などによる被害が世界中で多発しており、サイバー空間における脅威が今後もますます増加する傾向にあると見られている。このようなインシデントに対しては、ISP 事業者及び通信インフラ事業者などテレコム業界の相互の連携・協力の下で、広域ネットワーク上の多次元的・多面的な情報を収集し、それらの統合的な分析を通して、インシデント発生時等において早期の対策・対応を可能とする仕組みの構築が求められている。

このような社会的要請の高まりを受け、情報通信機構委託研究「広域モニタリングシステムに関する基盤技術の研究開発」が国内 ISP 事業者の連携のもと、進行中である。これはインシデント発生時の情報収集が迅速かつ網羅的に実施されるようにするための研究開発である。

モニタリングにより収集された情報は活用されなくてはならない。その活用例のうち極めて有効なものがトレースバック技術であるといえる。トレースバック技術のうち、IP パケットに関する理論研究は十数年に渡り実施されているが、大規模ネットワーク上でその有用性が検証された例は少ない。また、アプリケーショントレースバック技術に関しては、理論研究自体まだ未成熟な段階である。

本研究開発においては、現在進行中の広域モニタリングシステムとの協調を行いながら、トレースバック技術の研究・実装を行っていくことが求められる。

２）研究開発の必要性

ウイルス・ワームに係る感染機会の拡大は、インターネットが社会経済活動の基盤として発展していく上で制約要因となることが懸念される。このため、各利用者が自身の考え方に立って、セキュリティ意識を高めていくことはもちろんのこと、ISP 事業者や通信インフラ事業者等においても、利用者に対してインターネットの安全・安心な利用環境を提供していくことがますます重要となっている。

このような利用環境を提供していくためには広域なネットワークにおけるインシデント警戒体制がとられていることが必要である。また、そのような警戒態勢を実現するためには、受動的警戒態勢である広域モニタリングだけではなく、能動的警戒態勢である不正パケット送信に対するトレースバックの双方が実現される必要があると考えられる。

インターネット上でトレースバックを実施する際、多くの ISP 事業者・通信事業者の連携による方が、より精度の高いトレースバックを実現することができるのは明らかである。そうした点からも、本研究開発は複数の ISP 事業者、通信事業者の協力を踏まえて実施されてこそ意味があるものであるといえる。

３）他で実施されている類似研究との切り分け

情報通信研究機構（NiCT）委託研究**「大規模ネットワークセキュリティ確保に向けた研究開発」**（以下、大規模ネットセキュリティ研究）においては、分散化・階層化された様々なネットワーク機器等の情報（稼動状況、通信のやり取りを記録したデータ、アクセスログ等）の集中的な管理と不正データの発信源探査を基盤とする統合的なセキュリティシステムを構築し、さらに、大規模なネットワーク環境をフィールドとして、その実効性を検証することを目的に研究開発が行われている。

ここで対象とされている「ログの蓄積と不正データの発信源追跡」という研究開発課題については本研究開発と同様な目標であるものの、その実施方法に大きな差が見られる。すなわち、「大規模ネットセキュリティ研究」においてはそのシステムの検証をシミュレータ環境で実施している一方で、本研究開発では同様の検証を複数のISP事業者のネットワークが接続されたリアルの大規模なネットワーク環境への適用することによって実施することを指定している。

旧通信・放送機構（TAO）委託研究**「不正アクセス発信源追跡技術に関する研究開発」**（平成11年度～13年度。以下、不正アクセス追跡研究）は課題名にもあるように、トレースバックに関する研究開発である。「不正アクセス追跡研究」は主として三つの項目を対象としている。すなわち、どのように不正アクセスを検知するか、不正アクセス検知後にその発信源をどのように追跡するか、そしてそれらの検知・追跡技術が不正利用されることを防ぐための防御技術の研究開発である。

「不正アクセス追跡研究」についても興味の対象としている部分については同様である。また、追跡技術の悪用を防ぐといった重要項目についても考慮に入れた意義深い研究開発であるといえる。しかしながら「不正アクセス追跡研究」も前述の「大規模ネットセキュリティ研究」と同様、その検証を実運用環境において実施するには至っていない。この点において本研究の独自性が発揮される。

また、上記の二つの研究課題との大きな違いとして、本研究開発においてはトレースバックを IP レイヤーだけではなくアプリケーションレイヤにおいても実施することも挙げられる。アプリケーション・トレースバックアルゴリズムに関する研究は世界的にみても挑戦的な課題であり、その研究を行う意義は大きい。

「広域モニタリングシステムに関する基盤技術の研究開発」（以下、広域モニタリング基盤研究）は大規模な実用ネットワーク環境におけるインシデント警戒体制の実効性検証を目的としている点は本研究と同様であるものの、その実現方法がモニタリングに特化しておりトレースバックに言及していないという点において本研究の独自性が発揮される。

６．研究開発の到達目標

課題ア：全体アーキテクチャの設計

課題ア－１：トレースバック機構を構築する上で考慮するべき事項の網羅

（１）先行研究の網羅的調査を踏まえ、考慮するべき事項を一通りリストアップする。それらに対して優先順位を設定し、本研究開発においてはどの項目をどの程度考慮するのかを明らかにする。

課題ア－２：基本的なトレースバック方式の開発

（１）既存のトレースバック方式についての網羅的な調査を行う。本調査は、実運用環境に導入することを前提に行われるべきであり、各方式がその目標を達成することが可能であるか、可能とするためにはどのような改善を加えるべきであるかを明らかにする。
（２）また、実際に運用する上で非現実的なスピードや負荷が発生しないか、という点についても明らかにする。特に、ネットワーク上の一部のノードに対して極端な負荷がかかるような可能性については明確にしておく必要がある。

課題ア－３：トレースバックシステムの相互接続アーキテクチャの開発

（１）NAT、Firewall など「正規に IP アドレスを変化する」機器を越えてのトレースバックを行う方法についてその基本方式を検討する。本目標についても実運用環境への実装という視点に立ち、網羅的な先行研究調査を行うものとする。

（２）また、異なるトレースバック方式との連携や、国際的な標準化などに備え、十分な拡張性を備えた相互接続アーキテクチャを開発するものとする。

課題イ：トレースバック・アルゴリズムの開発

課題イ－１：IP パケットトレースバックアルゴリズムの開発

（１）トレースバックに要する時間は数分から 10 分までを目安とする。同時に、目安となる時間を超えて行われるトレースバックについては、ネットワーク全体にかかる負荷を考慮しつつ実施されるよう考慮する。
（２）また IP パケットトレースバック・アルゴリズムとしてマーキング方式を採用した場合には、意味のあるトレースバックとなるために必要なマーク率はどの程度であるか算出する。
（３）トレースバックする過程で不用意にプライバシーを漏らすような方式にならぬことを保証する。

課題イ－２：アプリケーショントレースバックアルゴリズムの開発

（１）どのアプリケーション/プロトコルに対して適用するのが良いのかを網羅的に検討し、本研究開発において実際に開発するべき対象を絞り込む。その際、SMTP（電子メール)、HTTP（Web)、FTP（ファイル転送）の三つに関しては必須項目とする。それ以外のものを開発対象とする場合にも、汎用的に用いられているアプリケーション/プロトコルを対象とする。
（２）開発されたプライバシー保護技術がトレースバック精度を一定に保持しつつ、プライバシーを守ることができるということを明らかにする。

課題イ－３：異なるレイヤ由来の情報からトレースバック能力を向上させるアルゴリズムの開発

（１）アプリケーショントレースバックを実装することにより享受されるメリットと、実装することによって発生するコストについて、両者の関係が妥当なものであるかを検証する。ここでのメリットとはトレースバック成功までに要する時間の短縮等を意味する。また、コストとはネットワークおよびネットワーク上の各種機器への負荷を意味する。

課題ウ：トレースバック用データ収集装置（プローブ装置）の開発

（１）各プローブ装置が単位時間あたりに処理するべきデータ量を想定し、効率良く、遅延無く処理が行われるものとする。
（２）上記の目標がインターネット上のデータ流通量が急増しても耐えうるしくみを目指す。

課題エ：トレースバック・プラットフォームの実証実験

課題エ－１：実装および運用体制の検討

（１）これ以降の課題項目が滞りなく実施できる体制を事業者間で構築するために定型契約書類を一式作成する。
（２）本研究開発で構築されたトレースバック体制に関して、外部公開用ポリシーを策定する。本ポリシーの策定は、一般ユーザへの広告と同時に、新規事業者が参加しやすくなるようにするためという意義を有する。

課題エ－２：攻撃パターンの想定

（１）本研究開発が想定している範囲において、現在想定可能な攻撃パターンをできるたけ網羅するように想定攻撃パターンを策定する。ここでいう攻撃パターンとは、特定のサーバに対する集中攻撃（DoS, DDoS 等）、網羅的なスキャンによる脆弱なホストの発見および攻撃（Scanning 等）、およびネットワークの輻輳攻撃（ICMP, DNS の不正使用等）といった攻撃形態の抽象的なモデルを意味する。

課題エ－３：動作検証

（１）プローブ装置を実運用環境上に実装し、実際の攻撃に対してトレースバックを行う。
（２）不正アクセス到着時から 12 時間以内であれば、当該アクセスに対してのトレースバックを実行できるものとする。

課題全体として：

（１）実運用環境上において、定められた運用ポリシーに準じて、高速かつ正確にトレースバックを実施すること。
（２）インターネット上でのトレースバックは協力者が多ければ多いほど、その価値が増す。類似最新動向の調査、国際標準化への積極性、そのためにも高い拡張性を有した設計とするべきである。

７．期待される波及効果

広域モニタリングによって構築される ISP・通信事業者を横断するインシデント警戒体制に加えて、本研究開発の成果であるトレースバックが補完されることによりこの警戒態勢はより堅牢なものとなる。

また、本研究開発が目的とするような広範囲を対象としたトレースバックが可能となれば、それだけでネットワーク上での不正アクセスに対して一定の抑止力とすることができるのである。

さらに、前項でも示したとおり実運用環境上において大規模な実験を早期に行うことにより、国際標準化関与時にイニシアチブをとることにつながると考えられる。

８．研究開発スケジュール

本研究テーマの研究開発期間は、平成 17 年度から平成 21 年度までの５年間であり、スケジュールは概ね以下のとおりである。

研究開発項目	平成 17 年	平成 18 年	平成 19 年	平成 20 年	平成 21 年
課題ア： 全体アーキテクチャの設計					
（ア-1）トレースバック（TB）機構を開発する上で考慮するべき事項の網羅	→	→			
（ア-2）基本的な TB 方式の開発		→	→		
（ア-3）TB システムの相互接続アーキテクチャの開発			→	→	
課題イ： TB アルゴリズムの開発					
（イ-1）IP パケットト TB アルゴリズムの開発	→	→			
（イ-2）アプリケーション TB アルゴリズムの開発	→	→			
（イ-3）異なるレイヤ由来の情報から TB 能力を向上させるアルゴリズムの開発		→	→	→	

（次ページに続く）

（前ページからの続き）

研究開発項目	平成 17 年	平成 18 年	平成 19 年	平成 20 年	平成 21 年
課題ウ： TB 用データ収集装置の開発					
課題エ： TB プラットフォームの実証実験					
（エ-1）実装および運用体制の検討					
（エ-2）攻撃パターンの想定					
（エ-3）動作検証