DNS を利用した IP トレースバック情報連携基盤の提案

佐々木 達典† 佐藤 直†

†情報セキュリティ大学院大学
221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1

あらまし 外部ネットワークから攻撃を行う際,攻撃者は送信元のIPアドレスを詐称することにより発信源の特定を著しく困難とし防御行動を阻害する.詐称時においても,攻撃経路を特定する技術がIPトレースバック技術であり,効果的な防御や抑止の手法として期待されている. しかし,実際に特定するためにはインターネットを構成する各組織間における保有情報の連携が必須であり,その連携基盤導入におけるコストや運用負担の増加等の理由から未だ普及にはいたっておらず課題となっている. 本稿では,インターネットを利用するために必須の基幹設備であるDNSを用いて組織間の情報連携を行い同課題に対処する手法を提案する.

Proposed DNS based information exchange infrastructure for IP traceback

Tatsunori Sasaki† Nao Sato†

†Institute of Information Security
2-14-1 Tsuruya-cho, Kanagawa-ward, Yokohama 221-0835, JAPAN

Abstract Generally information security attackers spoof their IP addresses so as not to be identified. Some IP traceback techniques have been developed to detect attacking routes on the Internet, but there is a problem common to the conventional techniques that related organizations such as ISPs are loaded with much cost for the IP traceback. Therefore we suggest a new method with which the organizations could perform the IP traceback with less cost in cooperative use of a DNS based information exchange infrastructure.

1 はじめに

広帯域の常時ネットワーク接続環境が一般に普及した今日において，大量のパケットを送信する等の手法によりサービス不能に陥れるいわゆる DoS 攻撃の脅威は大規模，広域化している. DoS 攻撃は，直接の攻撃対象である被害ホストのみではなく，通過する基幹ネットワークにも過大な負荷をかけ，組織における IT 活動全体や攻撃が経由する ISP におけるネットワークサービスの提供も阻害する. そのため，攻撃源に近い上流における規制等が有効な対処となりうるが，一般的に攻撃者は送信元の IP アドレスを詐称することにより発信源の特定を著しく困難化しており，効果的な対処は現実には難しいものとなっている.

送信元 IP アドレスの詐称時においても，攻撃源からの攻撃経路を特定する技術の総称が IP トレースバック技術であり，同攻撃等に対する効果的な防御や抑止力として期待されている.

図 1 に IP トレースバックの概要を示す.

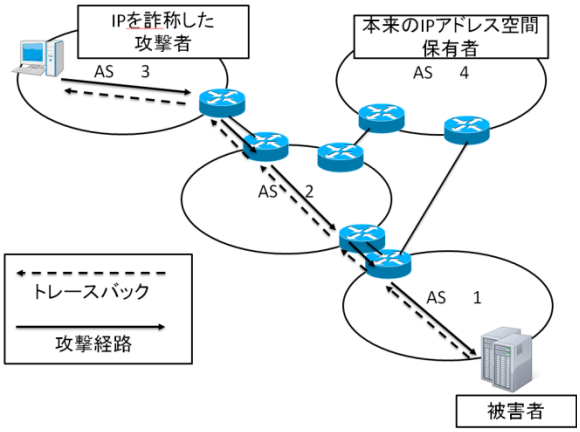

図 1　IP トレースバックの概要

IP トレースバック技術については，これまで多くの方式が提案されている．それらの手法は多種多様であるが，現在のインターネットは自律システム（AS）を単位とする各組織体の相互接続から成り立っているため，技術的手段については，各組織の実態に即して最適な手法を選択することが現実的に必要と考えられている．また，被害者から攻撃元までの攻撃経路のトレースバックを行うためには，各 AS 間で実施，取得した追跡のための情報連携の手法が必要である．この情報連携の手法が検討されているが，既存手法を具体化した仕組みを導入しようとすると，新たな機器及びアプリケーションのコストが必要となる他，それらの運用技術取得のための指導などのさまざまな対応が必要となる．特に小規模の組織においては仕組み導入に対する敷居が高い．インターネット全域に渡る普及が必須である IP トレースバックにおいて情報連携手法の導入コストは大きな課題といえる．

そこで，本稿では IP トレースバックのための情報連携手法として， DNS の分散協調動作型のデータベースを利用することにより，既存手法と比較して低コストで導入可能な手法を提案する．

2　既存の IP トレースバック技術

本章ではまず，IP トレースバックの個々の技術に関する既存研究をリンク調査型，逆探知パケット型，マーキング型，ダイジェスト型の４つに大別して概要を紹介し，連携が必要な理由とそこにある課題を述べる．

2.1　リンク調査型

被害ノードにおいて攻撃を観測した際に，プロトコル種別やポート番号など攻撃パケットの特徴を抽出し，ルータにてフィルタ機能を用いてパケットが流入及び流出するインターフェース及び，隣接ルータを特定する手法である．同一管理組織内での運用を前提とするため，組織間の連携が必須となる．また，攻撃が実行されている間でなくては特定できない，手動調査のためネットワーク管理者に多大な負担がかかる，という課題がある．

2.2　逆探知パケット型

攻撃経路の特定に，専用の逆探知用パケットを用いる手法である．IETF-ITRACE-WG により ICMP を利用したトレースバック手法[1]が提案されている．同方式では，ICMP メッセージに新たなメッセージ種別である Traceback を規定し，同メッセージ内に追跡のための情報を記載する．ルータでは，パケットが通過する際に一定の確率で同メッセージを作成し，送信する．被害ノード側では，攻撃発生時に平行して送信される同メッセージから追跡のための経路情報を得る．本来のパケットとは別に逆探知用のパケットを生成することから，通信量が増加する懸念があり，またそれを抑制するために ICMP メッセージの生成確率を低下させると，DDoS 攻撃に見られるように，少量多数の送信元からの攻撃時にメッセージが生成されず，トレースバック品質が低下する問題等がある．

2.3 マーキング型

追跡情報を流れている IP パケット自体の内部に格納する方式. 被害ノードでは攻撃パケットの内部から追跡情報を抽出し, 復元することにより逆探知を行う. 前述の逆探知パケット方式とは異なり, 追跡のための追加パケットを必要としないため, ネットワークへの追加負荷をかけない. Savage ら[2]の論文では, 追跡のための情報を IP ヘッダ内の Identification フィールドに格納することを提唱している. 同フィールドを使用した場合, 本来の用途であるフラグメントパケットの再構築ができなくなる等の弊害の発生や, IPsec 等の利用に支障をきたす場合がある. また, データの復元時に多大な計算を必要とするという課題がある.

2.4 ダイジェスト型

ルータをパケットが通過する際にパケットの内容を記録することで, 逆探知用のパケットの利用や, パケットへのマーキングをすること無しにトレースバックを行う手法. パケットの内容を単純に記録するだけでは記録容量を多大に消費し保持可能上限数に影響が生じることから, MD5 や SHA-1 などの一方向性ハッシュ関数を用いて, パケットの経路上で不変な箇所やペイロードの先頭部等からハッシュ値を生成, 記録し保存する. 記録に際して充分なリアルタイム処理性能や, 大きな記録容量の確保を必要とする問題があるが, ハッシュ値を用いてパケットそのものを保持しないため通信情報の秘匿の観点からは利点がある. また, 同一管理組織内での運用を前提とするため, 組織間の連携が別途必須となる.

2.5 トレースバック情報の連携

これまでに述べたように, IP トレースバックには多数の既存手法が存在しているが, 冒頭でも述べた通り, 現在のインターネットは自律システム(AS)をひとつの単位とする各組織体の相互接続から成り立っているため, トレースバックを実際に行う技術的手段についても, 各組織の実態に即して最適な手法を選択することが現実的である. 被害ノードから攻撃元までの攻撃経路を追跡するためには, 各 AS 間で採取した追跡情報を相互接続し連携するための手段が必要となる. その際は, 他事業者に対して追跡要求を発することとなるため, パケットの内容はハッシュ関数等を使用し, 秘匿することが望ましい. この場合各 AS 内において攻撃パケットを元に生成されたハッシュ値を照合して自 AS 内外を切り分ける機能を具備することにより, AS 間におけるトレースバック情報の相互接続が実現できる.

2.6 連携に関する既存研究と課題

ここでは, 2009 年に国内の ISP15 社と検証実験[3]を行う等, IP トレースバックの相互接続を行うにあたって最も有力な実装形態である InterTrack を既存研究例として紹介する.

InterTrack は情報通信研究機構(NICT)の委託研究「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」[4]にて奈良先端科学技術大学院大学で開発されたトレースバックアーキテクチャの参照実装である. 追跡の効率性と詳細情報の他者流出を防止する観点から, 攻撃 AS 経路の特定と関連 AS 内の詳細経由ルータ調査を個別に行う段階的なトレースバックを志向するアーキテクチャであり, 共通のハッシュ関数と入力フォーマットによって, パケットのハッシュ値を作成するものに限定されるが, トレースバック技術間の相互接続を実現している.

InterTrack では, ITM と呼ばれるコンポーネントが主として連携基盤構築の役割を担っている. ITM を各 AS に一ヵ所設置の上, BGP4 のような相互接続ネットワークを構築し, ルータを通過したパケットが自 AS の外から送信されていた際は, 相互接続された ITM を介して他 AS に追跡要求を発出する. この追跡要求を受けた AS は, 要求元と同様に自 AS からの送信かどうかの判定を行い, 自 AS からの送信パケットであった場合はその旨を回答し, 自 AS 外からの送信パケットであった場合は, さらに隣接する他 AS

のITMに探査要求を転送する. この動作を再帰的に送信元を特定するまで繰り返し実施し, 特定後, 得られた探査結果を要求元へ回答する. なお, 経路に関連するASに対しては, 経由ルータ等の詳細調査を行うため, ITM から該当するASに詳細調査を依頼する. この動作は前述の関連するAS探査と同時並行的に実施されるが, AS 内の詳細構成情報となることから, この情報については探査結果を回答する必要は無い.

前述の通り, InterTrack は有力な実装形態であるが, 現状では未だ広範に浸透しているとは言い難い状況であると考える. DoS 等の攻撃の脅威が続き, 早期に対策が求められる中, 普及に時間を要している理由としては, 通信の秘密に関する法的面の整備が不十分である他, トレースバック連携基盤を構築するための機器やアプリケーションの導入費用や運用負担が大きいことがある. すなわち, InterTrack においては, ITM コンポーネントが主として連携基盤構築の役割を担っており, 同アプリケーションの導入とそれを動作させるハードウェアは原則として通信に必要なルータ等の機器とは別に用意する必要がある. そして, その初期設定や運用に際しては個別の知識が新たに要求されることとなり, 相互接続対向先との連携のような恒常的なオペレーションも追加的に発生する.

これらの負担が導入に際しての敷居を高めているという側面は否定できず, 普及するために継続検討しなければならない課題である.

3 DNSを用いた連携基盤の提案

3.1 DNS方式の利点

既存トレースバック連携手法が持つ課題への対処として, 本稿では同連携に際して新たな専用の機構を導入するのではなく, インターネットを提供するISP等の組織においては既に導入済みのDNS(Domain Name System)の仕組みを用いた連携基盤の構築を提案する.

DNS はインターネットを使った階層的な分散型データベースシステムであり, 現在ではおもにインターネット上のホスト名や電子メールに使われるドメイン名と, IP アドレスとの対応づけを管理するために使用されている. 各ドメインはゾーンと呼ばれる管轄に分けてゾーン毎に権威DNSサーバと呼ばれるホストで管理される. 上位から権限を適切に下位の権威 DNS サーバに委譲することにより階層的な構造を持ち, ルート DNS を頂点とする一個の巨大な木構造をなす. これによりインターネットに接続される全てのコンピュータに関する情報を, 複数の分散された権威DNSサーバが保持する情報を協調連携させることによって, 集中管理することなく取得できる仕組みを実現している.

DNS を連携に用いる利点としては以下が挙げられる.

(1) 元来 DNS は異なるドメインが持つ情報を分散保持し, 協調動作する仕組みであるため, AS ごとに分散保持されるトレースバック情報を連携する用途に適している.
(2) レイヤ4プロトコルにUDPを採用しており, 大量の問い合わせに高速な応答をする方向で設計されたシステムであるため, 迅速性が要求される攻撃対処にあたって応答性が高い.
(3) インターネット利用に必須のシステムであることから, 各ASにて充分な運用実績をもっており運用が容易である. また, 既存利用設備を流用することも可能である.
(4) DNSSEC 利用により, 情報提供元 DNS サーバの出自が保証されるため, 虚偽のトレースバック情報を流されて追跡の品質が落ちることがなくなる.

3.2 提案手法の概要

3.2.1 連携ドメインの権限委譲

DNS を利用する前提として, トレースバックに関する情報を各 AS から申請受付, 登録するトレースバックルート DNS の管理組織を設け,

トレースバック情報連携用のドメインを準備する．ここでは仮に同ドメインを iptraceback.org とし，同組織は本ドメインの権威 DNS サーバを運用管理することとする．そしてトレースバック情報を連携する ISP は同情報連携用ドメインから AS 番号名のサブドメインを権限委譲され，各 AS は各々が保有する権威 DNS サーバにおいて同サブドメインを運用する．これは通常の DNS におけるドメインの運用と同様である．

今，AS1 における同サブドメインを as1.iptraceback.org と定義する．図 2 にルート DNS サーバから権限移譲する流れを示す．

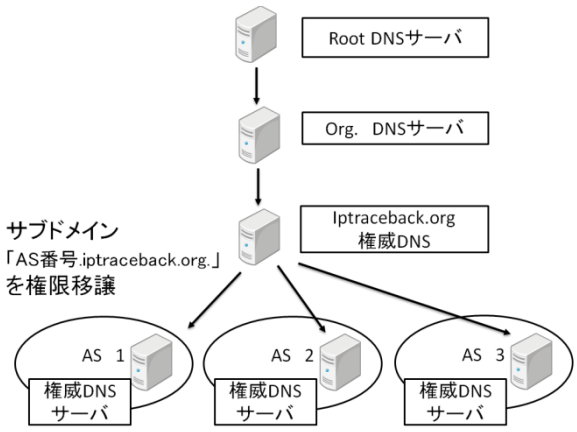

図 2　DNS 権限委譲の流れ

3.2.2 通過パケットハッシュ値の登録

各 AS においては攻撃の発生や追跡要求の必要有無を問わず常時ルータを通過するパケットの特徴をハッシュ値として取得することとする．その際，隣接 AS からの流入パケットであった場合は流入したインターフェースから対向 AS を判別し，流入元 AS 番号を取得する．また，自 AS のエンドユーザが接続するエッジルータにて同エンドユーザからの通信を収容しているインターフェースからの通信であった場合はその旨を示す ORIGIN フラグを設定することとする．

取得したハッシュ値と流入元 AS または ORIGIN フラグの組を DNS リソースレコードとして，情報管理用ドメインから権限委譲された組織体内管理用サブドメインを管理する権威 DNS サーバに登録する．ここではトレースバック情報専用のリソースレコード TB を定義し利用することとする．DNS サーバアプリケーションである BIND9.6-ESV-R6[5]でのレコード設定例を以下に示す．1 行目と 3 行目の例は外部 AS からの流入であること，2 行目は同 AS が送信元である ORIGIN フラグを表す．

```
13a5e313d2d144fa23633412dabf09eb  IN TB 65521
896c6c8e90435ac281c659fd35a2c6c5  IN TB ORIGIN
db324788f6a568d98bfbb67b5f17846c  IN TB 65521
```

3.2.3 被害ノードからの追跡情報の要求

トレースバック追跡要求は IDS（Intrusion Detection System）等の要求元機器のスタブリゾルバから自組織のキャッシュ DNS サーバに対して TB レコードに関する DNS 問い合わせを行い，通常の DNS の仕組みと同様の方式で各 AS の権威 DNS サーバから回答を受領する形で行う．具体的な流れは下記の通りである．

（1）攻撃パケットのハッシュ値の取得
　攻撃発生時，被害ノード近傍において攻撃パケットを採取し，ハッシュ値を生成する．

（2）送信元の自組織内外判定
　自組織からの発信かの判別のため，
　攻撃パケットのハッシュ値.自 AS 番号.iptraceback.org
の TB レコードを自組織のキャッシュ DNS サーバに問い合わせを行う．自組織の AS 番号は既知情報であるため，この問い合わせは実現可能であり，また通常の DNS の動作に従って，ルート DNS を起点とした再帰的問い合わせが行われ，自組織の権威 DNS サーバで自ずと回答されることとなる．ここで TB レコードに対する回答が ORIGIN フラグであった場合は，自組織からの攻撃と判別される．また，流入元 AS 番号が回答された場合は，同 AS からの流入パケットであることが判明するため次項以降を実施する．

(3)流入元 AS の再帰的問い合わせ

続いて入手した流入元 AS 番号から,

攻撃パケットのハッシュ値.流入元 AS 番号.iptraceback.org

の TB レコードを自組織のキャッシュ DNS サーバに問い合わせを行う. この問い合わせも同様に通常の DNS の動作に従って, ルート DNS を起点とした再帰的問い合わせが行われ, 流入元組織の権威 DNS サーバで回答される. これを ORIGIN フラグが回答されるまで再帰的に繰り返し行い, 都度入手した AS 番号を記録する. ORIGIN フラグが回答された場合は, 送信元 AS が特定できたため, 問い合わせを終了する. この過程で入手した流入元 AS 番号を送信元から列記することで AS 単位での攻撃経路が特定される.

提案手法を用いることで, 2 章にて紹介した, InterTrack と同様の連携を既存の DNS の仕組みを用いて自動的に攻撃 AS の経路を特定することができる. DNS を用いた連携の流れを図 3 に示す.

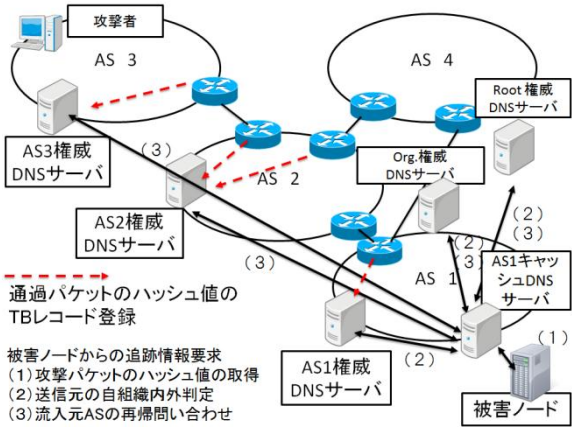

図 3 DNS を用いた連携の概要

4. まとめ

本稿では最初に IP トレースバックの必要性を述べ, トレースバック手法は各組織の実状に応じて選択されるべきであることから, 各組織毎に収集した追跡のための情報を相互接続し連携する仕組みが必要であることを述べた. 次に, 既存の実装方法を導入するには導入や運用を行う負担が生じ, この負担が既存手法の普及を妨げる要因となっていると考え, 同課題を解消するため DNS を利用する手法を提案し, 実現の可能性を示した.

本稿では該当 AS を特定した後に,具体的にそこを経由したルータ単位での経路追跡方法について言及しておらず, それについても今後検討が必要であるが, 同様の DNS を用いた方法に, 内部情報であるネットワーク構成情報を無制限に外部に公開することを保護するための適切なアクセス規制等を施すことによって実現が可能と考えている. また, 提案方式を使用した場合, ルータトラフィックを逐一 DNS のレコード登録する際に想定される負荷が現実的に処理可能な範囲に収まるかといったような性能面の確認も必要である. そのため, 今後は提案方式を検証するための試験モデルを構築し, 有効性と性能面について検証を行っていく予定である.

参考文献

[1]S.Bellovin, ICMPTracebackMessages, http://tools.ietf.org/html/draft-ietf-itrace-04 (2012 年 8 月確認).

[2]S.Savage, D.Wetherall, A.Karlin and T.Anderson, PracticalNetwork Support for IP Traceback, Proc. of SIGCOMM'00. pp.295-306, 2000.

[3]奈良先端科学技術大学院大学プレスリリース,サイバー攻撃源の逆探知システムの開発と実験に成功,http://www.naist.jp/pressrelease/detail_j/topics/772/ (2012 年 8 月確認).

[4] 門林雄基,櫨山寛章,宮本大輔,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, http://itaku-kenkyu.nict.go.jp/seika/h20/seika/95/95_naist.pdf (2012 年 8 月確認).

[5] BIND 9.6-ESV-R6 ,Internet Systems Consortium,http://www.isc.org/software/bind (2012 年 8 月確認).