報道資料

平成21年11月26日
日本電気株式会社
国立大学法人奈良先端科学技術大学院大学
パナソニック電工株式会社
株式会社クルウィット
財団法人日本データ通信協会
株式会社KDDI研究所
独立行政法人情報通信研究機構

サイバー攻撃源の逆探知システムの開発と実験に成功

～ 世界初、広域インターネット環境下で逆探知を実証 ～

日本電気株式会社※①、国立大学法人奈良先端科学技術大学院大学※②、パナソニック電工株式会社※③、株式会社クルウィット※④、財団法人日本データ通信協会※⑤、株式会社KDDI研究所※⑥は、インターネットでのサイバー攻撃源を逆探知するトレースバック*1技術を開発しました。また、実際に稼働中のインターネット環境（以下「実インターネット環境」）で逆探知実験を行い、有効性と実用性を実証しました。

不正アクセス等のサイバー攻撃は発信源を隠蔽、詐称することが通常です。本技術では、そのような攻撃であってもパケットの痕跡をたどり、発信源を素早く突き止めることが可能です。また、今回のような実インターネット環境における、複数のインターネット接続事業者*2（以下「ISP」）にまたがるトレースバック実験は世界初の試みです。

なお、本研究の成果は、独立行政法人情報通信研究機構※⑦（以下「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開発」にて得られたものです。

【背景】

近年、コンピュータウイルスやDoS（Denial of Service：サービスの妨害）攻撃*3、DDoS（Distributed DoS：分散型サービス妨害）攻撃*4など、インターネット上の犯罪や事故は増大しており、社会インフラとしての安全対策が求められています。しかし、インターネット上の住所であるIPアドレスの書き換えなど、発信源が隠蔽、詐称されている場合には特定が困難であり、対策が望まれています。

これに対しNICTでは、平成17年度から平成21年度まで「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」を実施しています。IPアドレスが詐称されている状態で攻撃元を特定するには、どこからどのような経路で通信が行われているのかを把握する必要があります。また、セキュリティポリシーやプライバシーポリシーの異なる複数のISPが連携し、通信の秘匿性を確保する必要もあります。

【今回の成果】

本トレースバックの研究では、以下の技術を開発し、システム構成や運用手順を策定して実験を行いました。

- サイバー攻撃に関連するパケット情報を匿名化するなど、通信の秘匿性を確保しながら、そのパケットの痕跡をたどっていくことを可能とする技術
- 膨大な痕跡の中から追跡すべきパケットの情報を効率良く探し出し、迅速な事案対処を可能とする技術
- 複数ISP間で協力するには運用面や制度面での課題があるが、これらを考慮したシステム構成や運用手順の検討

今回の実証実験では、北海道から沖縄まで全国に所在する15社のISPの協力を基に、発信源のIPアドレスが詐称されたパケットによる模擬サイバー攻撃を発生させ、逆探知に成功しました。このような実インターネット環境において、複数のISPにまたがるトレースバック実験は、海外においても例がなく世界で初めての試みです。

【今後の展望】

本研究開発は、複数のISPの管理するネットワークを超えて、不正アクセスの発信源を追跡し逆探知が可能なことを実証しました。これにより、発信源への迅速な対処が可能になるとともに、サイバー攻撃に対する大きな抑止効果となり、より安全で安心なインターネット環境の実現につながります。

トレースバック相互接続システムのソフトウェアを、以下のURLにおいてオープンソースとして公開しています。

［トレースバック相互接続システムソフトウェア(名称:InterTrack)公開URL］
http://intertrack.naist.jp/

＜ 本件に関する 問い合わせ先 ＞
日本電気株式会社
知的資産 R&D 企画本部 広報グループ
http://www.nec.co.jp/contact/

＜ 報道関係 問い合わせ先 ＞
日本電気株式会社
コーポレートコミュニケーション部　山梨
Tel:03-3798-6511
E-mail:r-yamanashi@bc.jp.nec.com

国立大学法人奈良先端科学技術大学院大学
企画総務課 広報渉外係　藤里
Tel:0743-72-5026　E-mail:s-kikaku@ad.naist.jp

パナソニック電工株式会社
広報部　吉田
Tel:06-6909-7187
E-mail:kyosida@panasonic-denko.co.jp

株式会社クルウィット
担当　国峯
E-mail:inquiry@clwit.co.jp

財団法人日本データ通信協会
トレースバック担当
E-mail: tracebackkoubo@telecom-isac.jp

株式会社 KDDI 研究所
営業企画グループ　前川
Tel:049-278-7545　E-mail:inquiry@kddilabs.jp

独立行政法人情報通信研究機構
総合企画部 広報室 担当　廣田
Tel:042-327-6923　E-mail:publicity@nict.go.jp

＜各企業・研究機関＞

※①　日本電気株式会社（本社：東京都港区、代表取締役執行役員社長：矢野 薫）
※②　国立大学法人奈良先端科学技術大学院大学（奈良県生駒市、学長：磯貝 彰）
※③　パナソニック電工株式会社（本社：大阪府門真市、代表取締役社長：畑中 浩一）
※④　株式会社クルウィット（本社：東京都三鷹市、代表取締役：国峯 泰裕）
※⑤　財団法人日本データ通信協会（本部：東京都豊島区、理事長：森 清）
※⑥　株式会社KDDI研究所（埼玉県ふじみ野市、代表取締役所長：秋葉 重幸）
※⑦　独立行政法人情報通信研究機構（本部：東京都小金井市、理事長：宮原 秀夫）

＜各研究機関の成果と要素技術等の解説＞

日本電気株式会社、株式会社 KDDI 研究所による成果
パケット収集システム

接続ポイントを通過したパケットを識別できるように、パケットヘッダーの一部から算出したハッシュ値[*5]をメモリ上に保持するシステム。トレースしたいパケットのハッシュ値が分かれば、そのパケット収集システムが接続しているポイントを通過したかどうかが分かる。

パナソニック電工株式会社、株式会社クルウィットによる成果
トレースバックコントロールシステム

パケット収集システムからのハッシュ値を集約し、サイバー攻撃と関連付けるシステム。関連付けは、研究開発したトレースバックアルゴリズムにより、サイバー攻撃に対して実用的な速度で検出が可能。

国立大学法人奈良先端科学技術大学院大学による成果
トレースバック相互接続システム

ISP を超えてトレースバックコントロールシステムの相互連携を実現するシステム。隣接する ISP のトレースバック相互接続システムにトレース対象と同一のハッシュ値を持つパケットが通過したかどうかを問い合わせ、これを繰り返すことによって得られるパケットの経路情報をトレースバック管理センターへ保存する。また、異なるトレースバック方式の差異吸収も行う。

株式会社 KDDI 研究所による成果
トレースバック検索システム

各 ISP の担当者からの要求により、トレースバック管理センターが逆探知を行うための検索システム。ISP 間で直接情報交換することなくトレースできる機能を実現している。

財団法人日本データ通信協会による成果
実インターネット環境における実証実験の実施

開発された各システムの構成や運用ルールの制定を運用面や制度面での課題を考慮して行い、実インターネット環境での模擬攻撃を使用した実証実験を実施した。

＜用語 解説＞

*1　トレースバック

トレースバックとは追跡のことを指し、インターネットにおけるトレースバックでは、実際にどこからパケットが送られてきたのか、通信経路を追跡して発信源をつきとめること。

*2　インターネット接続事業者（ISP）

インターネット接続事業者（Internet Service Provider:ISP）とは、電話回線や光ファイバー回線などを通じて、インターネットへの接続を提供する事業者のこと。

*3　DoS（Denial of Service：サービスの妨害）攻撃

サーバなどのネットワークを構成する機器に対して、サービスの提供を不能な状態にする攻撃のこと。

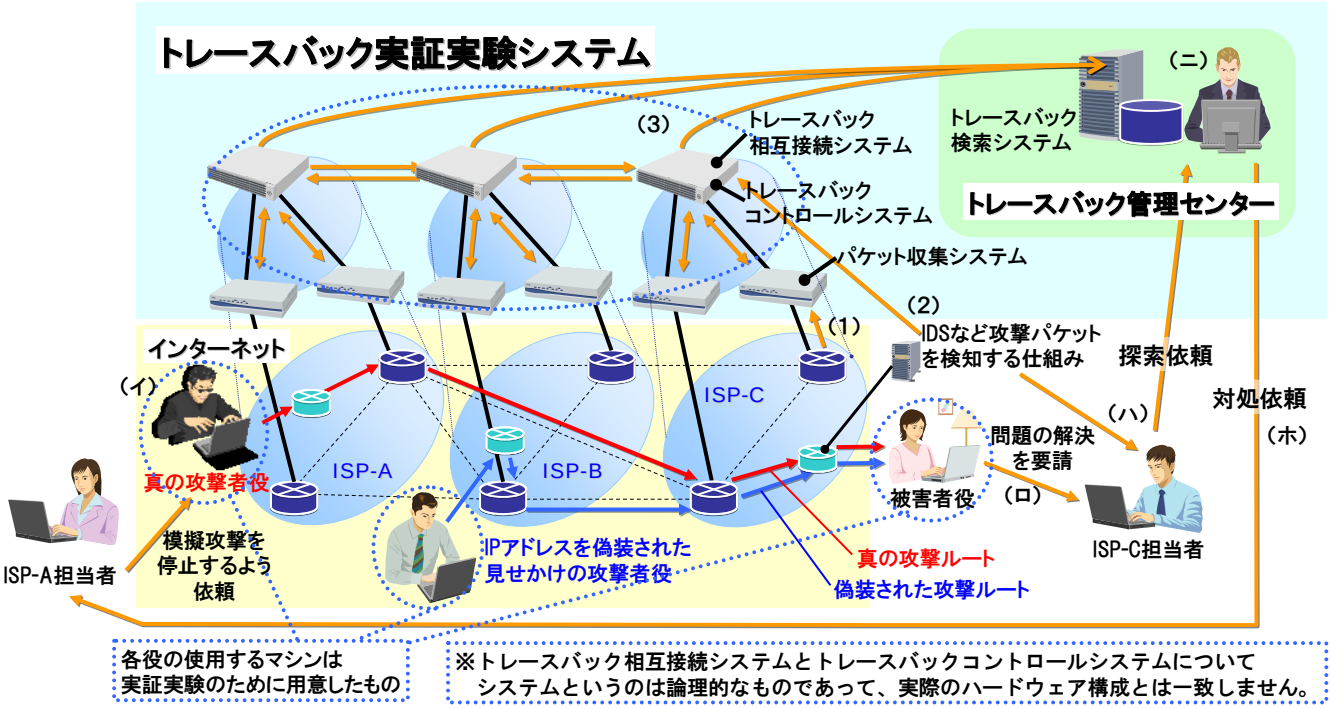
*4　DDoS（Distributed DoS：分散型サービス妨害）攻撃

複数のコンピュータにより、標的とされたサーバ等に行う DoS 攻撃のこと。

*5　ハッシュ値

加工前の情報（パケットヘッダー情報）から特定の処理を行うことで算出された値。データ量が縮減されるとともに、不可逆性・匿名性を持つ。

補足資料



トレースバック実証実験の動作概要

システムの動作概要（実証実験の開始により以下の動作が開始される）

（１）パケット収集システムによるハッシュ値の算出と保管を開始する。

（２）IDS(Intrusion Detection System)が模擬攻撃パケットの検出を開始する。模擬攻撃パケットを検出した場合、模擬攻撃パケットのハッシュ値を算出し、トレースバック相互接続システムへ提供する。

※IDS：ネットワークを流れるパケットを監視して、不正アクセスと思われるパケットを発見した場合に管理者に通報するシステム。

（３）トレースバック相互接続システムは提供されたハッシュ値をもとにトレースバック相互接続システム間で問い合わせを行い、その結果得られた模擬攻撃パケットの経路情報をトレースバック管理センターのトレースバック検索システムへ登録する。

実証実験参加者のオペレーション概要

（イ）ISP-A の真の攻撃者役が発信元の IP アドレスを ISP-B の見せかけの攻撃者役の IP アドレスに詐称して、ISP-C の被害者役宛の模擬攻撃パケットの送出を開始する。

（ロ）被害者役が模擬攻撃を検知し、ISP-C の担当者に問題の解決を要請する。

（ハ）ISP-C の担当者は被害者役からの要請により、模擬攻撃パケットのハッシュ値を確認し、トレースバック管理センターに模擬攻撃パケットの探索を依頼する。

（ニ）探索依頼を受けたトレースバック管理センターは、トレースバック検索システムを利用して模擬攻撃元を探索し、ISP-A であることを特定する。

（ホ）模擬攻撃元を特定したトレースバック管理センターは、模擬攻撃元の ISP-A の担当者に模擬攻撃の停止の対処依頼をする。ISP-A の担当者が真の攻撃者役に対して模擬攻撃パケットの送出を停止するように依頼する。

参考)

パケットヘッダーにある発信元の IP アドレスでトレースするのではなく、通過したパケットのハッシュ値を痕跡としてトレースをするので、発信元の IP アドレスが詐称されていても発信源を特定することが可能となっている。