平成１４年度 社会安全研究財団委託調査研究報告書

# リアルタイムトレーシング手法に関する
# 技術動向の調査研究

平成１４年１２月
(２００２年)

コンピュータセキュリティ対策委員会
代表　清瀬 紀次

# はじめに

2001 年 9 月のアメリカ同時多発テロを機に、サイバーテロへの懸念は拍車がかかっている。市場調査会社の IDC が毎年行っている翌年の IT 動向についての予測では、「2003 年は大規模なサイバーテロが発生して経済に打撃を与え、インターネットを最低 1 日か 2 日、機能停止に陥れるだろう」と報告されていた。あくまで予測に過ぎないとはいえ、世界各地で起こる無差別テロや、国連査察を巡る米国とイラクとの関係緊張化など、不安定さを増す昨今の情勢を鑑みれば、サイバーテロへの危惧も誇張が過ぎるといえないのも事実であろう。

インターネットを通して行われる攻撃は、すでに個人のレベルはおろか、国レベルでの攻撃行為にまで変化してきていると言っても過言ではない。本邦においても、サイバー刑事法研究会報告書として、「欧州評議会サイバー犯罪条約と我が国の対応について」が 2002 年 4 月に出され、サイバー犯罪における他国との連携について議論が重ねられている現状である。

ネットワーク上の犯罪も、実世界の犯罪同様、許すべきではない反社会的な行為であることに変わりはない。しかし、攻撃者特定を行う手法、すなわち、Tracing の技術に関しては物理的、法的、社会的にさまざまな問題点があり、その技術の確立は一筋縄ではいかない現状である。

本書は、この Tracing の技術の中でも、とりわけ注目を浴びているリアルタイムでの Tracing 技術について、調査・報告したものである。リアルタイムに Tracing を行うとは技術的にいかなることであるのか、また、従来の Tracing の技術とはどのような点で違いがあるのか、ということについて述べていき、将来的に Realtime tracing による攻撃者の身元特定が可能であるのかどうかを考察することを目的とする。

委員長 清瀬 紀次

執筆者

大木 英史　株式会社ラック

森 政志　株式会社ラック

新城 直樹　株式会社ラック

目次

**第 1 章 調査目的・調査方法 ..... 1**
1. 調査目的 ..... 1
2. 調査方法 ..... 2
**第 2 章 Tracing とは ..... 3**
1. Tracing とは ..... 3
2. Tracing の技術 ..... 4
(1) OSI 参照モデルと TCP/IP ..... 4
(2) MAC アドレスに基づく Tracing ..... 16
(3) IP アドレスに基づく Tracing ..... 17
3. ログ解析 ..... 24
**第 3 章 Realtime tracing とは ..... 26**
1. Realtime tracing とは ..... 26
2. Realtime tracing の技術 ..... 27
(1) 攻撃元ホストの隠蔽 ..... 27
(2) トレースバックの 3 要素 ..... 34
(3) 自動トレースバックの種類 ..... 36
(4) Realtime tracing の効果 ..... 47
(5) Realtime tracing の利用状況 ..... 48
**第 4 章 Realtime tracing の将来 ..... 50**
1. Realtime tracing の課題 ..... 50
(1) 物理的課題 ..... 50
(2) 社会的課題 ..... 51
2. Realtime protection との関係 ..... 52
3. Realtime tracing の研究状況 ..... 54
**第 5 章 総評 ..... 58**
**第 6 章 付録 ..... 60**
＜参考資料＞ ..... 60
＜索引＞ ..... 72

# 第 1 章 調査目的・調査方法

## 1. 調査目的

インターネットが情報インフラとして確固たる地位を築いている現在、その信頼性、安全性の確保は最重要課題であると言える。しかし一方では、インターネットの性質上、連日、昼夜を問わず、不正行為や違法行為が行われている。また、ネットワーク上の不正行為や違法行為は目に見えにくく、実社会における犯罪行為に比べ社会的な反響が少ないことも影響してか、インターネット人口の増大に伴い、年々その被害規模は拡大し、内容も悪質化、巧妙化している。

セキュリティ対策の実践的な方法としては、攻撃予防・攻撃防止・攻撃検知を柱に、サイトのセキュア化実施や Firewall 及び IDS（Intrusion Detection System：侵入検知システム） 等のセキュリティ製品の導入などが挙げられるが、それらは今や当たり前のものとなり、個々における攻撃予防や攻撃防止という意識は確実に広まりつつある。しかし、不正行為や違法行為の被害を受けた後の対応方法、いわゆるインシデントレスポンス（Incident Response）に関しては、その理解やシステムの確立が十分になされているとは言えない。インシデントレスポンスの目標とするものは様々であるが、その中にはセキュリティを侵害した者、つまりネットワーク上にて不正行為や違法行為を犯した者の形跡を洗い出し、その身元を特定するという作業も含まれる。この作業は一般的に Tracing と言われ、現在の Tracing システムでは、手作業を要するステップが多く、身元特定には多くの時間と人的リソースを必要とする。つまり、結果として、インシデント発生後から侵入者特定までには時間とコストをかけざるを得ないのが実状である。

今回調査を行う Realtime tracing は既存の Tracing システムに対して正確性と即効性を寄与するものであり、Tracing における将来像とも言われている。具体的には、Realtime tracing の使用により、自動もしくは手動で即座に攻撃元を特定し、攻撃元からのアクセス遮断や法的措置のための証拠収集と言ったことが可能になると言われている。これが実現すると、Tracing にかかる時間やコストが削減できるだけではなく、インターネット上で大きなリスクを犯してまで不正行為や違法行為を行う者は減少し、年々拡大するそのような行為に歯止めをかけられるかもしれない。しかし、Realtime tracing は今だ未完成な分野であるため、体系だった資料や調査比較した資料は少ないというのが現状である。

本書では、次代のセキュリティ対策の方法となる可能性があるカテゴリーである Realtime tracing を調査し、現状をまとめた上で今後のあるべき姿を模索することを目的としている。

## 2. 調査方法

### (1) Tracing とは

現在の Tracing 作業と Realtime tracing と比較するために踏まえておくべき一般的なネットワーク用語とその技術を挙げる。また、一般的に言う Tracing の目的や技術の調査を行う。

調査対象：Tracing とは何か
　　Tracing の技術
調査手法：インターネット、書籍、雑誌などのメディアから情報を収集
調査項目：Tracing とは何か（目的）
　　Tracing の技術（TCP/IP、手法）

### (2) Realtime tracing とは

Realtime tracing とはどのようなものであるかとその効果について挙げる。また、Realtime tracing に必要とされるであろう技術の調査を行う。

調査対象：Realtime tracing とは何か
　　Realtime tracing の技術
調査手法：インターネット、書籍、雑誌などのメディアから情報を収集
調査項目：Realtime tracing とは何か（定義）
　　Realtime tracing の技術（種類、技術、効果）

### (3) Realtime tracing の将来

Realtime tracing の実現が可能であるかどうかを考察するべく、その課題や研究状況に関する調査を行う。

調査対象：Realtime tracing の課題
　　Realtime protection との関係
　　Realtime tracing の研究状況
調査手法：インターネット、書籍、雑誌などのメディアから情報を収集
調査項目：Realtime tracing の課題（Realtime tracing 実現化における障害）
　　Realtime protection との関係（内容と相違点）
　　Realtime tracing の研究状況（研究状況、種類）

# 第 2 章 Tracing とは

## 1. Tracing とは

実社会においては、「犯人は犯行現場に何かを残し、犯行現場にある何かを持ち去る」という仮説のもと、犯罪捜査が行われる。これら犯罪捜査には、個人や場所を特定するため、指紋や DNA、またさらに細かい繊維や花粉などの科学的手法が用いられる。例えば、匿名の電話主を識別するためには声紋が使用され、匿名の手紙からその書き手を特定するために筆跡やタイプライターの文字が使用されるといった具合である。

対照的に、ネットワークの世界においては、不正行為や違法行為を行う者を特定するために使用可能なものは、現実社会のものと比較するとその数は格段に少ないと言える。その理由は、クラッカーなどと呼ばれる犯罪行為を行う者たちが、個人を特定するための特徴を一切持つことないの電気的なパケットを使用して犯罪の成功を試みるからである。

このようなネットワーク上での不正行為や違法行為の調査、そしてその実行者の特定には、そのパケットがどこから、どのような経路で流れてきて、どのような振る舞いをしたか、ということを順を追ってたどっていく作業、すなわち Tracing を行うことが必要になる。Tracing の中でも、このようにパケットの発信元へさかのぼっていく行為のことを特にトレースバックと表現し、それをシステム化したものをトレースバックシステムという。トレースバックシステムでは、「人間の攻撃に対する責任の所在を明らかにする」ことを目的として、その行為に対して、いつ・どこで・誰が・何を・どのようにしたか、そしてなぜそうしたのかという情報を明確にするための調査やその情報を立証するための証拠の収集などが行われる。攻撃をもたらした部分のデータを解析し、そのデータがたどってきた経路情報などを調査する以外にも、人物調査のためのインタビューや、入室退室管理などの記録・関連する個々のシステムログ・その他ソースの精査など、責任の所在を明らかにするために行われる情報収集や調査が手作業により行われる。

このように、Tracing では人手を介しての作業が伴い、作業内容的に自動化ができないものも少なからずある。

また、実行者の特定には直接的に結びつかないが、ネットワークのセキュリティ対策には Firewall や IDS が広く利用されてきており、インターネットの規模拡大と発達に足並みを揃えるようにその技術水準も高まってきている。

Firewall は、外部からの不正侵入や破壊活動に対して、それを遮断して被害を未然に防ぐことを主眼としている。しかし、インターネット上で特定のサービスを提供している場合、そのサービスに対する外部からのアクセスを遮断することは原則的に行わないため、そこにつけいる隙があることも事実である。

IDS に関しても、これは基本的に攻撃の検知を行うことが主眼であり、前述の Firewall

と連携することによりその攻撃を遮断することは可能であるものの、その機能に関しては十分満足行くものとは言えない。このことの一因として、その攻撃検知の精度の問題がある。この問題は、誤検知と言われ、本当は攻撃ではないものを攻撃として認識してしまう積極的誤検知(FalsePositive)、逆に本当は攻撃であるにも関わらず攻撃として認識しない消極的誤検知(FalseNegative)などがある。そのような状況のため、実際に IDS を運用する際は、管理者が IDS の検知したイベント(攻撃の種類)に関して、本当の攻撃であったのかどうかを確かめる手間が生じる現状がある。IDS が検知したと同時にそのアクセスを遮断するには、現状ではまだ技術的な不安が残ると言える。

しかし、これら Firewall と IDS が保存する膨大な量のログは、攻撃者の特定に大いに寄与するものであり、このログを収集し、解析することにより、ネットワーク上での不正行為・違法行為の立証や、その実行者特定の証拠を押さえることにつながっていくのである。

インターネット上の不正行為や違法行為のもう一つの特徴として、その広域性が挙げられる。それらの行為を行う者は、遠く治権が及ばない海外に在住する者である場合も珍しくない。このような場合、不正行為や違法行為を意図するデータはその発信元からいくつもの経路をたどってきているため、正確に Tracing を行うことはより困難になる。さらに、実行者が第三者になりすます場合もありうるため、身元特定は一筋縄ではいかない。このような意味で、ネットワーク上での不正行為や違法行為は、国の内外を問わず、社会全体で協力体制を敷かなければ対応できないとも言える。各企業や通信事業者が抱えるログには、それらの行為とは関係のない大多数の人や組織のプライバシーや機密情報が含まれている。確かな規則や手続きなしに、これらの情報を共有、譲渡、あるいは公開することに対しては根強い反発があると考えられる。

直接被害を被ったネットワークに残された痕跡からだけでは、Tracing はうまくいかない。インターネットが、社会の情報インフラとして急成長したことと同様に、ネットワークのセキュリティ対策、特に Tracing が十分に機能するためには、独自のインフラ構築も必要であると言える。

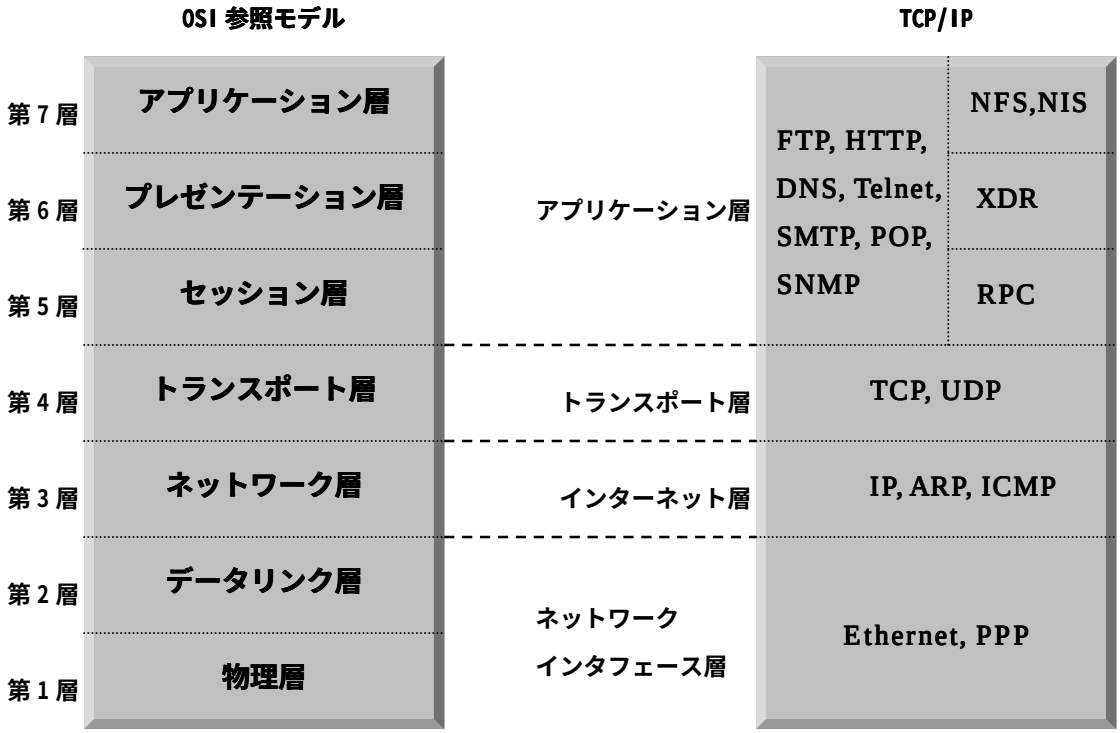
## 2. Tracing の技術

### (1) OSI 参照モデルと TCP/IP

コンピュータやネットワーク機器で相互に通信を行うためには、データの形式や送受信方法など、特定の約束事を取り決めておく必要がある。この約束事はプロトコルと呼ばれるが、それぞれのプロトコルの機能や実装方法はベンダにより異なる。このことから、ISO（International Organization for Standardization：国際標準化機構）は、1977

年より OSI（Open System Interconnection: 開放型システム間相互接続）参照モデルとして、すべてのネットワーク機器に対応する標準作成を開始した。しかしながら、OSI の開発には時間がかかりすぎることや、仕様が複雑であったことなどから、現在、インターネット上では TCP/IP が事実上の標準プロトコルとなっている。TCP/IP は、OSI 参照モデルとは独立に生まれてきたものであるが、その基本となる設計構造は同じであるため、両者はよく比較して論じられることが多い。

**表 1**




OSI 参照モデルは、機能ごとに 7 階層に分けられており、各階層は独立して扱われる。例えば、上位の階層は下位の階層に関して関知することなく機能の修正や強化が可能であるため、柔軟性のあるプロトコルの開発が行われるようになっている。TCP/IP ではTCP（Transmission Control Protocol）と IP（Internet Protocol）が主要なプロトコルであるが、これらは OSI 参照モデルの第 4 層トランスポート層と第 3 層ネットワーク層にそれぞれ対応している。また、TCP/IP は TCP/IP プロトコルスイート（Protocol Suite）と呼ばれることもあるが、これは TCP/IP が扱うプロトコルは OSI 参照モデルのすべての階層に渡るものであることを示している。TCP/IP では、機軸となるトランスポート層、

インターネット層より上位階層は一括してアプリケーション層とし、下位層はネットワークインタフェース層として、OSI 参照モデルの 7 階層に対し 4 階層のモデルとなっている。

Tracing に主に関わってくるのは、TCP/IP ではネットワークインタフェース層とインターネット層にあたる。以下では OSI 参照モデルと照らし合わせながら、TCP/IP のネットワークインタフェース層とインターネット層を解説していく。

(a). ネットワークインタフェース層

OSI 参照モデルの第 1 層「物理層」と第 2 層「データリンク層」は、TCP/IP の下位層にあたる「ネットワークインタフェース層」にあたるが、この層で最もよく利用されている媒体はイーサネット（Ethernet）である。TCP/IP とイーサネットの両者は歴史的にも強く結びついていることもあり、本書はネットワークシステムとしてイーサネットを利用していることを前提に解説していく。

第 1 層「物理層」では、通信データと電気信号との間の変換が扱われ、ハードウェア、コネクタ、ケーブル長、信号の仕様などが定義されている。例えば、あるデータを受け取った場合、それは物理層で電気信号からコンピュータが認識可能なデータの形に変換される。変換されたデータは次のデータリンク層に受け渡されることになる。（図 1 参照）

**図 1**

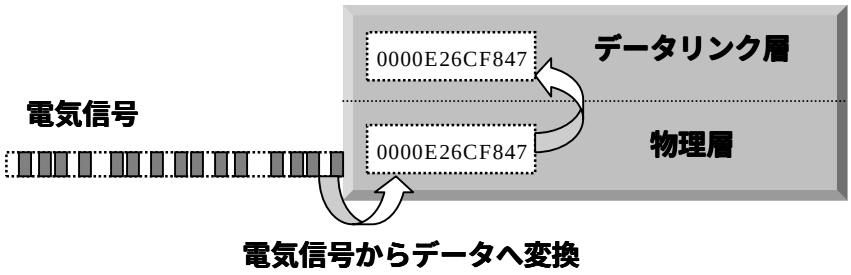
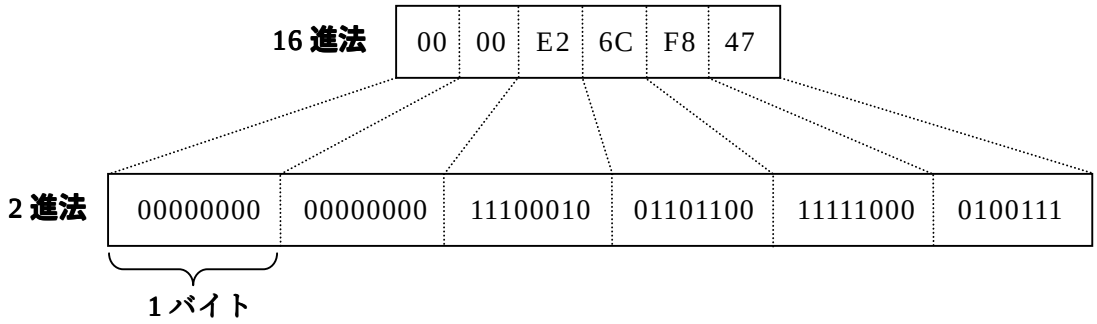


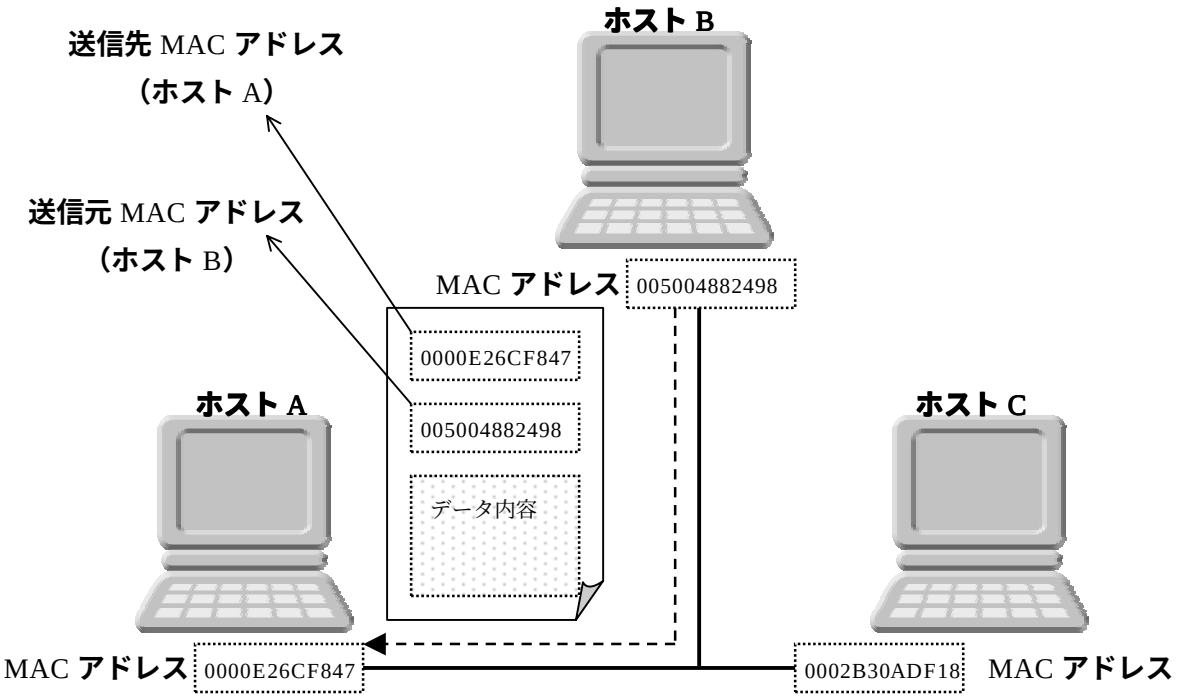
図 1 では、電気信号から変換されたデータが 16 進法で記述されているが、これを 2 進法で見ると、0 と 1 で構成される電気信号からデータへの変換が把握しやすい。（図 2 参照）

**図 2**



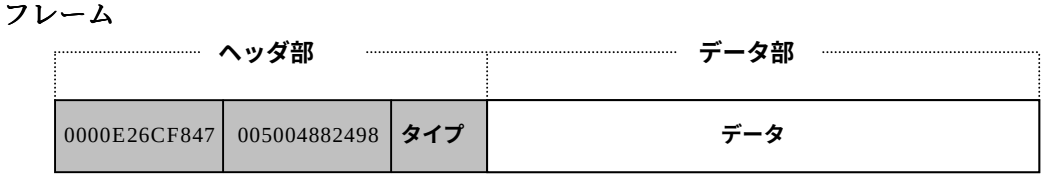

データリンク層では、一つのネットワーク上での一対一の通信が扱われる。この際、識別用に MAC アドレス（Media Access Control Address）という世界で一意の 48 ビットの値がアドレスとして用いられる。この値はネットワークカードにベンダがあらかじめ登録しているものであり、これを元にデータリンク層では、LAN 内のどのマシンからどのマシンへ送受信されたデータであるのかということが判断される。例えば、下図では、データの先頭部分に送信先としてホスト A の MAC アドレスが、送信元としてホスト B の MAC アドレスが記述されているため、そのデータがホスト B からホスト A へ送られてきたものであることがわかる。（図 3 参照）

**図 3**




データリンク層で扱われるデータは、「フレーム」と呼ばれ、先頭部分に送信先 MAC アドレス、送信元 MAC アドレス、フレームのタイプの順で記述されている。この先頭部分は MAC ヘッダ（MAC Header）と呼ばれ、これより後はデータ部として扱われる。郵便物に例えると、MAC ヘッダは郵便物の宛先と送付元、郵便の種類などにあたり、データ部は郵便物の内容と捉えることができる。（図 4 参照）

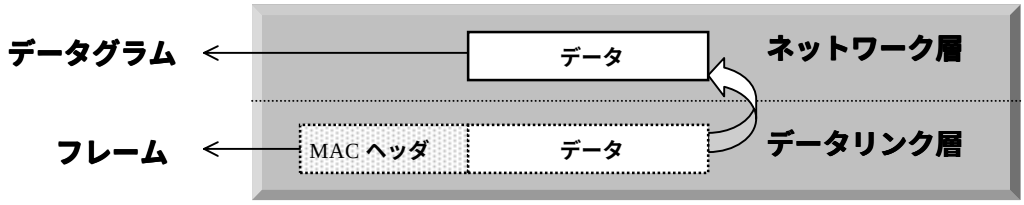
**図 4**



ただし、MAC ヘッダが道先案内の機能を果たすのはデータリンク層までであり、次のネットワーク層へは MAC ヘッダは取り除かれた形で受け渡される。ネットワーク層に渡ったデータは、データグラムと呼ばれる。

なお、フレームやデータグラムも含めたデータ一般を表わす場合に、パケットという用語も使われる。（図 5 参照）

**図 5**




(b). インターネット層

[IP アドレス]

データリンク層が MAC アドレスを元に一つのネットワーク内で一対一の通信を扱ったのに対し、インターネット層では IP アドレスを元に複数のネットワークに渡る通信を扱う。

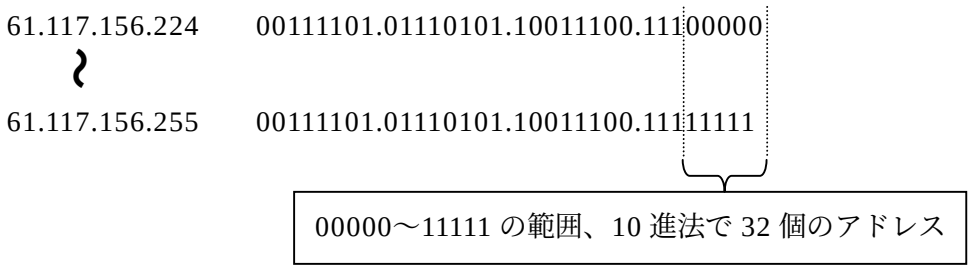
TCP/IP では、IP アドレスを用いてコンピュータの識別を行い、データのやりとりを行う。IP アドレスは、MAC アドレスと同様、世界で一意の値で、32 ビットの IPv4 が現在主に使われている。世界で一意である必要があるため、IP アドレスを獲得するためには、日本では JPNIC(Japan Network Information Center：日本ネットワークインフォメーションセンター)と呼ばれる組織に申請し、アドレスを割り当ててもらう必要がある。通常、一つの組織が IP アドレスを申請し、割り当ててもらう場合、複数の IP アドレスを割り当てられることになる。

一般的に IP アドレスは 8 ビットずつ区切って 10 進法で表わす。

IP アドレス　61.117.156.228（www.npa.go.jp）

この IP アドレスは、npa.go.jp というドメイン名の中の Web サーバを指しているが、npa.go.jp のドメインは 61.117.156.224～61.117.156.255 の IP アドレスを JPNIC から割り当てられており、自由に使用することが可能である。

また、61.117.156.224 と 61.117.156.255 を 2 進法で表わすと次のようになる。




このように、JPNIC からアドレスを割り当てられて、その組織の中でさらに IP アドレスの割り当てが行われていくのであるが、内部のネットワークにおいては、プライベート IP アドレスと呼ばれる IP アドレスが用いられている。これは使用するにあたって申請も許可もせずに用いることが可能なアドレス空間であり、以下の三種類がある。

10.0.0.0 ～ 10.255.255.255（10/8）
172.16.0.0 ～ 172.31.255.255（172.16/12）
192.168.0.0 ～ 192.168.255.255（192.168/16）

これらは内部ネットワークにおいて自由に使用することが可能であるが、その場合でもホストごとの IP アドレスの割り当ては一意でなくてはならない。

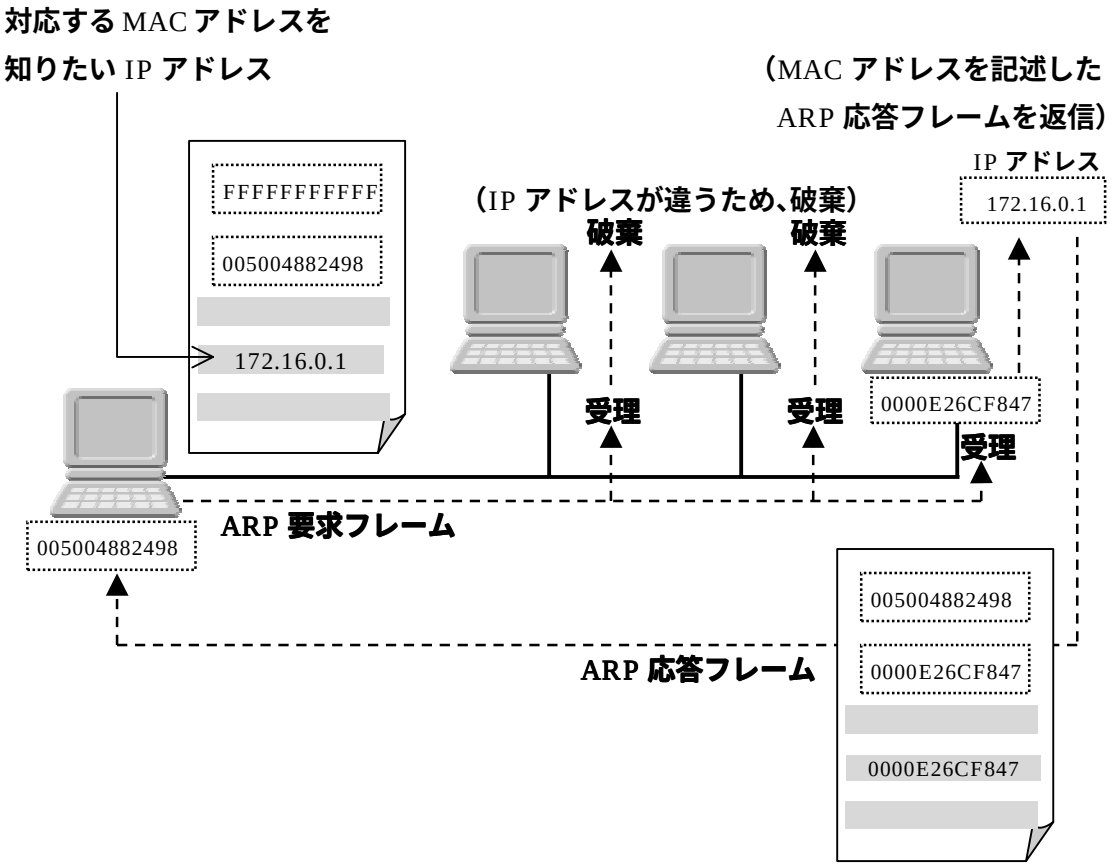
[ARP]

しかし、IP アドレスを元にデータのやりとりを行う場合も、それぞれの IP アドレスが物理的にどのマシンに対応しているかがわからなければならない。このため、TCP/IP ではインターネット層で ARP というプロトコルを用意している。

ARP は、ARP 要求フレームをブロードキャストし、同一ネットワーク内のすべてのホストに送りつける。ブロードキャストとは、ネットワーク内の不特定多数の相手にデータを送信することであり、ARP の場合、フレームヘッダで送信先 MAC アドレスを 16 進法で「FFFFFF」（2 進法ではすべて 1 のビットが立つ）とすることによってブロードキャストを行う。

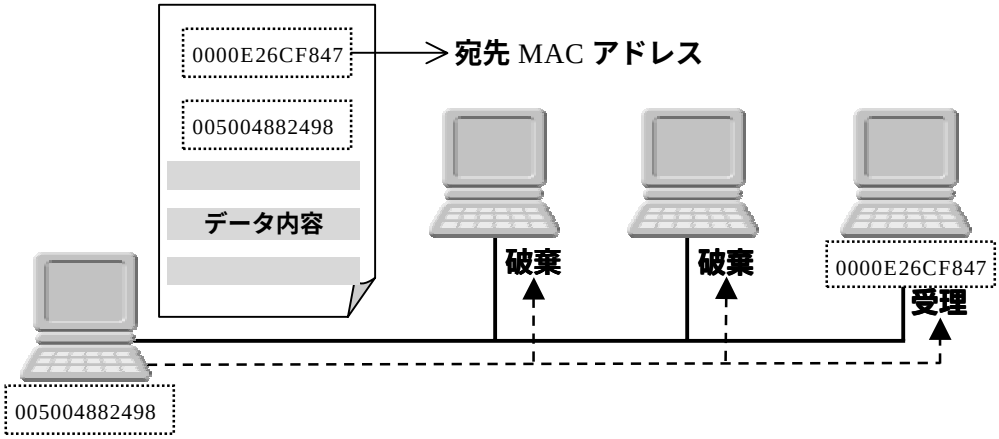
ブロードキャストでは、送られてきたフレームをすべてのホストがいったんは受理し、中身を確認する。ARP 要求フレームの中には、対応する MAC アドレスを知りたい IP アドレスが記述されており、それぞれのホストは自分がこの IP アドレスの持ち主でない場合はそのままパケットを破棄し、持ち主である場合は ARP 応答フレームという形で自分の MAC アドレスを送信元に送り返す。（図 6 参照）

**図 6**




元々、同一ネットワーク内では MAC アドレスを指定している場合でも、すべてのホストに対してフレームを送りつける。そして、この MAC アドレスの持ち主であるホストはこのフレームを受け取り、それ以外のホストはフレームを破棄する。このように特定の相手との一対一の通信をユニキャストと呼ぶ。（図 7 参照）

**図 7**

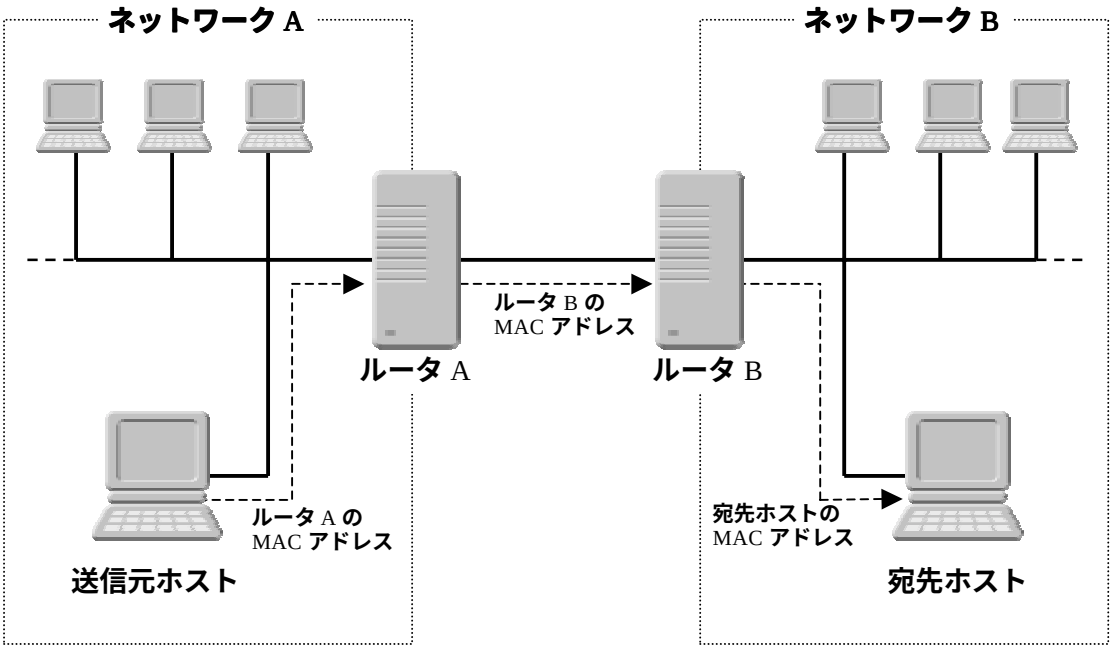



[ルータ]

このようにして ARP は、目的の IP アドレスに対応する MAC アドレスを取得することが可能であるが、同一ネットワーク内にその IP アドレスを所有するホストがいない場合、そのネットワークのルータ（Router）に対して問い合わせを行う。

ルータは、ネットワーク上を流れるデータを他のネットワークへ中継する装置である。前に、「データリンク層が MAC アドレスを元に一つのネットワーク内で一対一の通信を扱ったのに対し、インターネット層では IP アドレスを元に複数のネットワークに渡る通信を扱う」と述べたが、この「一つのネットワーク」の意味するところは、ルータにより区切られた範囲ということになる。ネットワークを単純化して図示すると、ネットワーク A からネットワーク B のホストに対してデータを送信する場合、送信元のホストはトポロジー上、まずネットワーク A のルータにデータを送信しなければならない。（図 8 参照）

**図 8**



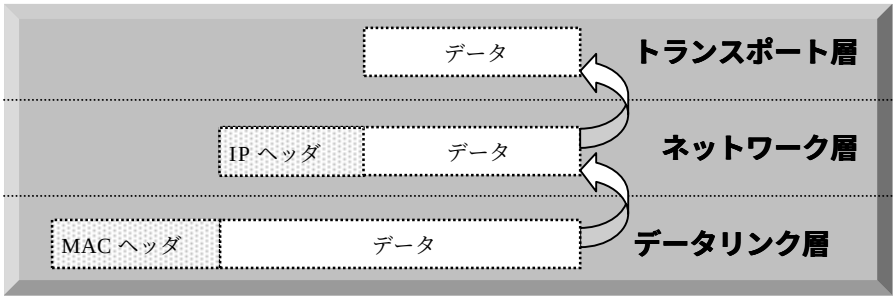

送信元ホストはまずルータ A の MAC アドレスを宛先としてフレームを送信する。一般的に、ルータ A の MAC アドレスは送信元ホストにおいてキャッシュされている。ルータは、どの IP アドレスがどのルータを経由することにより到達可能かといった情報を、経路制御表（Routing Table）として持っており、これに基づいてルータ A はフレームの送り先をルータ B とする。そして、ルータ B の IP アドレスを元にその MAC アドレスを特定し、フレームを送信する。ここでも同じく、一般的には、ルータ A の ARP テーブルにルータ B の MAC アドレスがキャッシュされている。最終的に、ルータ B から宛先ホストの MAC アドレス宛にフレームが送られる。

このように、データリンク層で「MAC アドレスを元に一つのネットワーク内で一対一の通信」が行われ、送信元ホストが宛先ホストの MAC アドレスを得ることができないにも関わらず、宛先ホストの IP アドレスを指定すればデータを送り届けることが可能である。IP、すなわちインターネットプロトコルが、このエンド・トゥ・エンドの通信や、経路制御をつかさどる。

インターネット層のデータは、IP ヘッダを取り除いて次のトランスポート層に渡される。インターネット層では IP アドレスに基づいて宛先までの経路の制御を行ったが、これはデータが確実に宛先に届けられることを保証してはいない。ネットワークが混雑し

ている場合や、何かしら障害が起きた場合などにデータ到達の信頼性を制御するのはトランスポート層である。トランスポート層の細かな説明は省くが、これまでと同じようにトランスポート層からアプリケーション層などの上位層へは TCP ヘッダが取り除かれて渡されていくことになる。これはデータを受信する側の動きだが、逆にデータを送信する場合も、上位層から各層においてヘッダを付け足していき、最終的にデータリンク層でフレームを作り上げていくことになる。（図 9 参照）

**図 9**

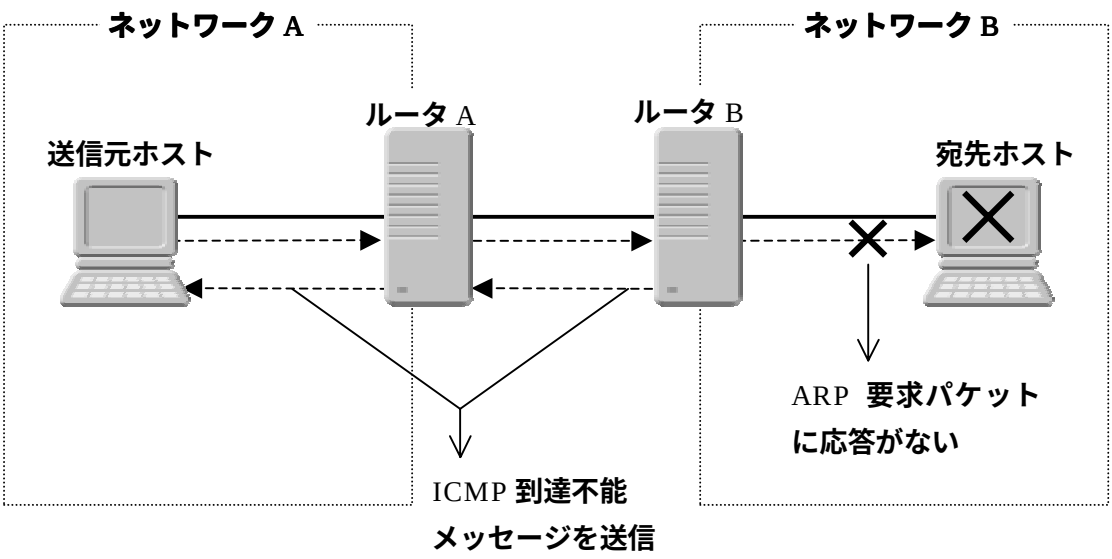



[ICMP]

次にインターネット層のプロトコルの一つである ICMP の説明を行うが、このプロトコルは、IP データグラムがネットワーク上の何らか障害により宛先へ到達できなかった場合に、その障害の通知を行うプロトコルである。また、能動的にネットワークの診断を行う場合にも用いられる。

例として、宛先となるネットワーク B のホストが電源を落としている、もしくは、障害により通信不能である場合を考えてみる。この場合、送信元ホストから送信されたデータはルータ B まで順調に届けられるが、ルータ B から宛先ホストに対して ARP 要求パケットを送信しても応答がない状態となる。数度にわたって ARP 要求パケットを送信した後、ルータ B は送信元ホストに対して、データが宛先ホストへ到達できなかった旨を ICMP により通知する。（図 10 参照）

**図 10**




ICMP でネットワーク診断を行う場合、最もよく使われるものが PING コマンドである。これは、宛先ホストとの通信が可能な状態であるかを判断する場合に用いられるが、先ほどと同じく宛先ホストが通信不能である場合は、ICMP 到達不能メッセージが返される。宛先ホストとの通信が順調に行われれば、ICMP エコー応答メッセージが届く。

ICMP には次のように様々なタイプのメッセージがある。

**表 2**

**主な ICMP メッセージ**

| タイプコード | 内容 |
|---|---|
| 0 | **エコー応答**（Echo Reply） |
| 3 | **到達不能**（Destination Unreachable） |
| 4 | **始点抑制**（Source Quench） |
| 5 | **リダイレクト**（Redirect） |
| 8 | **エコー要求**（Echo Request） |
| 9 | **ルータ通知**（Router Advertisement） |
| 10 | **ルータ選択**（Router Selection） |
| 11 | **時間超過**（Time Exceeded） |
| 17 | **アドレスマスク要求**（Address Mask Request） |
| 18 | **アドレスマスク応答**（Address Mask Reply） |

ICMP のこれらのメッセージは、IP データグラムの IP ヘッダではなく、そのデータ部に組み込まれているため、見かけ上は TCP や UDP のトランスポート層に見えるが、実際はインターネット層であり、IP の一部である。

(2) MAC アドレスに基づく Tracing

[ARP テーブル]

UNIX と Windows に標準装備されている arp コマンドを用いてそのマシンの ARP テーブルを確認することが可能である。Windows では、arp コマンドにオプションとして a を指定すると ARP テーブルの内容が表示される。次は IP アドレス 172.16.0.1 の Windows マシンで arp コマンドを実行した例である。

```
C:¥>arp -a

Interface: 172.16.0.1 on Interface 0x1000003
  Internet Address      Physical Address      Type
  172.16.0.2            00-c0-f6-90-a2-5b     dynamic
  172.16.0.3            00-c0-f6-b3-0a-17     dynamic
```

ここで、172.16.0.4 から 172.16.0.1 へ ping を打ち、その直後に再び arp コマンドを実行してみる。

```
C:¥>arp -a

Interface: 172.16.0.1 on Interface 0x1000003
  Internet Address      Physical Address      Type
  172.16.0.2            00-c0-f6-90-a2-5b     dynamic
  172.16.0.3            00-c0-f6-b3-0a-17     dynamic
  172.16.0.4            00-02-b3-3a-28-d0     dynamic
```

このように 172.16.0.4 の MAC アドレスが ARP テーブルに追加されたことが確認可能である。しかしこの場合、この新たに追加された MAC アドレスの情報は数分以内には消去されてしまう。仮に攻撃を受けた場合、その時点でアクセスがあったマシンの MAC アドレスをおさえておくためには、MAC アドレスをログに記録させる設定にしてログを収

集しておかなくてはならない。

IDS においては、攻撃検知の際に MAC アドレスをログとして記録することが可能である。MAC アドレスをログとして残すことの理由として、例えば、組織内部において IP アドレスが固定で割り当てられている場合、単純に自分のマシンに他人の IP アドレスを設定することにより詐称が可能であるが、MAC アドレスをログとして残しておくことにより、IP アドレスの詐称を行って不正を働いたマシンやユーザを特定することが可能となる。また、ネットワークに接続した際に DHCP サーバ[注]により IP アドレスが割り当てられる場合、DHCP サーバのアクセスログには、割り当てられた IP とその IP に対応するホストの MAC アドレスが記録される。DHCP を使用して不特定多数の人間がネットワークを利用することが可能であると、IP アドレスだけではマシンやユーザの特定は困難であるため、この場合には MAC アドレスに基づく監視が必要となってくる。

(3) IP アドレスに基づく Tracing

[nslookup コマンド]

nslookup コマンドは IP アドレスを FQDN（Fully Qualified Domain Name：完全修飾ドメイン名）へ、FQDN を IP アドレスへ変換するコマンドで、UNIX、Windows ともに装備されている。インターネット上では、IP アドレスの代わりに www.npa.go.jp といったドメイン名を用いることが可能だが、これは DNS（Domain Name System）により IP アドレスとドメイン名の変換（Mapping）が行われることにより実現している。このドメイン名は階層構造を成しており、www.npa.go.jp では、jp というトップレベルドメイン下に go というセカンドレベルドメインがあり、その下にサードレベルドメインとして npa があり、さらにその下に www という名前のホストがあることを表わしている。仮に npa.go.jp に属するホストから、単に www と指定するとそれは www.npa.go.jp を表わすことになる。FQDN とは、www といった省略したドメイン名の指定ではなく、www.npa.go.jp といったトップレベルドメインからのすべての情報を指定したもののことである。IP アドレスと FQDN の変換を名前解決と呼ぶが、nslookup コマンドは本来 DNS で正しく名前解決ができているかどうかを確認するためのコマンドである。

nslookup コマンドにより、ログに残っている IP アドレスから FQDN を、あるいは逆

---

注 DHCP は Dynamic Host Configuration Protocol の略で、クライアントに IP アドレス等のネットワークに必要な設定を提供するサービスであり、この DHCP サービスを提供するサーバを DHCP サーバと呼ぶ。TCP/IP を利用して通信する場合，それぞれのコンピュータに IP アドレスやデフォルト・ゲートウエイのアドレスなどを設定する必要があるが，DHCP サーバでは IP アドレスやデフォルト・ゲートウエイのアドレスを登録しておき、クライアントから起動時にリクエストがくると、IP アドレスを割り当てる。

に FQDN から IP アドレスを得ることにより Tracing の基礎的な準備が始まる。FQDN に記述されている各ドメイン名からは、不正行為や違法行為の実行者がどのような国、地域、組織に属しているかが大まかにではあるが推測可能である。当然ながら、ログに残っている IP アドレスや FQDN で示されるホストは、攻撃の中継地点にすぎない、あるいはなりすまされている可能性もある。

[whois]

whois は Whois データベースに問い合わせを行うことにより、DNS ドメインの管理組織、管理者代表者、連絡先などの情報を得ることを可能とするコマンドであり、UNIX では標準装備されている。Whois データベースは様々なものがあるが、日本国内のものとしては whois.nic.ad.jp などがある。whois コマンドは Windows では標準装備されていないため、サードパーティーのアプリケーションか、whois サービスを提供している Web サイトを利用することになる。次は http://whois.nic.ad.jp/cgi-bin/whois_gw で whois を実行してドメイン情報を得た結果である。

| | |
|---|---|
| Domain Information: [ドメイン情報] | |
| a. [ドメイン名] | NPA.GO.JP |
| e. [そしきめい] | |
| f. [組織名] | 警察庁 |
| g. [Organization] | National Police Agency |
| k. [組織種別] | 政府関連法人 |
| l. [Organization Type] | Government |
| m. [登録担当者] | KT287JP |
| n. [技術連絡担当者] | TH218JP |
| p. [ネームサーバ] | okfm.npa.go.jp |
| p. [ネームサーバ] | ns2.ttnet.ad.jp |
| y. [通知アドレス] | osimabuku01@npa.go.jp |
| [状態] | Connected (2003/05/31) |
| [登録年月日] | 1996/05/30 |
| [接続年月日] | 1996/06/12 |
| [最終更新] | 2002/06/01 02:27:13 (JST) |
| | form@domain.nic.ad.jp |

IP アドレスに対応する FQDN がない場合でも、Whois データベースを利用して IP アドレスの管理組織や所有者を確認することが可能である。nslookup コマンドでは、IP アドレスに対応する FQDN が登録されていなければマッピングを行えないが、Whois データベースは IP アドレスの管理情報に関するものであるため、FQDN の有無に左右されない。また、その組織や所有者がどこからどこまでの IP アドレスを管理しているかといった IP アドレス空間の情報を得ることも可能である。次は、IP アドレス空間などのネットワーク情報を得た結果である。

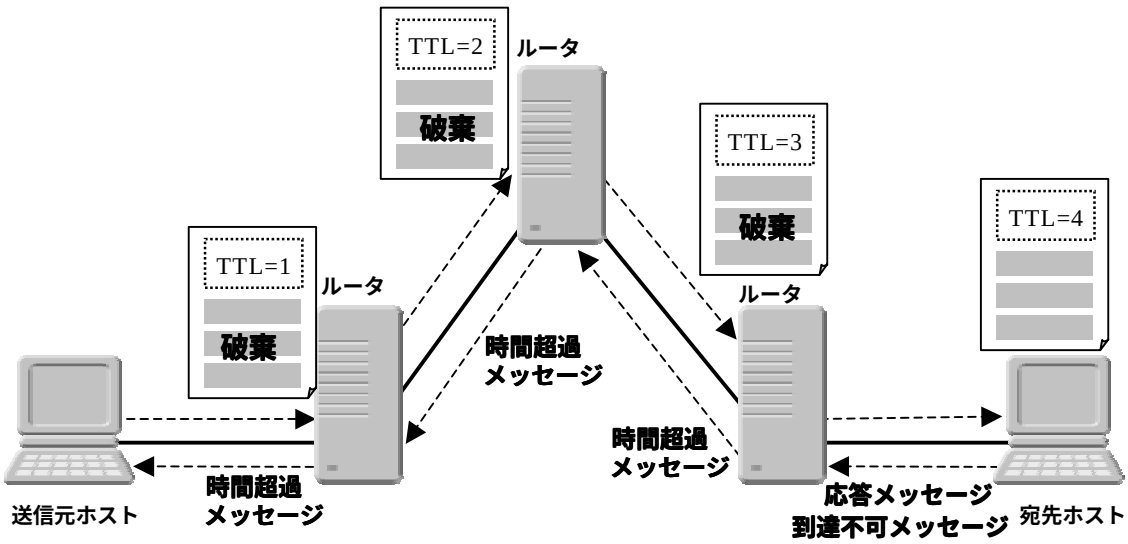
| | |
|---|---|
| Network Information: [ネットワーク情報] | |
| a. [IP ネットワークアドレス] | 61.117.156.224/27 |
| b. [ネットワーク名] | NPA |
| f. [組織名] | 警察庁 |
| g. [Organization] | National Police Agency |
| m. [運用責任者] | KT287JP |
| n. [技術連絡担当者] | HN2216JP |
| y. [通知アドレス] | hniikura99@npa.go.jp |
| [割当年月日] | 2001/03/05 |
| [返却年月日] | |
| [最終更新] | 2001/03/05 15:56:32 (JST) |
| | ip-alloc@nic.ad.jp |

[traceroute・tracert コマンド]

UNIX の traceroute コマンド、Windows の tracert コマンドは、特定の宛先ホストへ到達するためにどのルータを通過していくのかを確認するコマンドである。これは ICMP の時間超過（Time Exceeded）メッセージを利用することにより実現されており、本来ネットワーク障害の際に用いられるコマンドである。時間超過とあるが、実際には、一つのネットワークからルータによって別のネットワークへルーテイングされる回数であるホップ数の制限の意味である。IP ヘッダには TTL（Time To Live：生存時間）と呼ばれる 8bit のフィールドがあり、ルータを通過するたびにその値を一つずつ減らしていき、値が 0 になった時点でそのデータを破棄し、送信元へ ICMP 時間超過メッセージを通知する仕組みになっている。これは、途中にあるルータのルーティング情報が間違っていたりした場合、データがネットワークを永遠にループしてしまう可能性を防ぐためのものである。TTL 値は小さすぎると、目的のネットワークへたどりつくまでにデータが破

棄される可能性があるため、一般的に大きめに設定される。traceroute・tracert コマンドでは、宛先ホストの IP アドレスを指定したデータの TTL 値を 1 に設定して送信する。送信されたデータは一番初めに通過するルータで TTL が 0 になるため、データを破棄し、ICMP 時間超過メッセージを送り返す。そして TTL 値を一つずつ増やしたデータを送信し続け、ルータを通過するたびにそのルータからメッセージを受けていくことにより、データがたどる経路を把握していく。（図 11 参照）

**図 11**




前述したように、traceroute・tracert コマンドはネットワーク障害の際の経路確認のためのコマンドであるため、ある特定のデータが複数ある経路の中のどの経路をたどってきたかを確認することはできない。

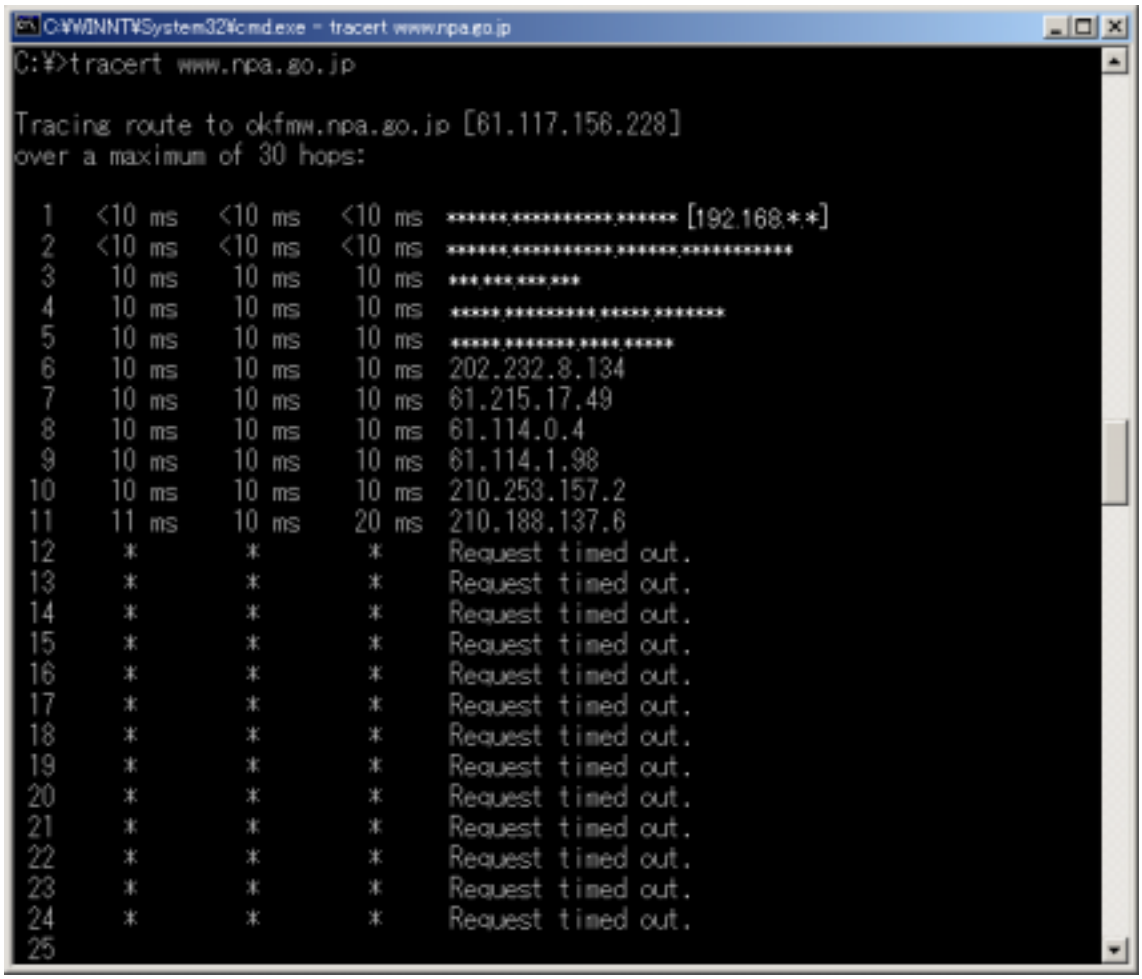
しかし、経路にあたるネットワークの管理組織からの協力を得ることの困難さもそうであるが、それ以上に traceroute・tracert コマンドでは経路情報の確実性の点で問題がある。traceroute・tracert コマンドは、宛先ホストに到達するまでに多くのパケットをやり取りするため、行きと帰りのパケットが違う経路をたどる可能性もある。このような問題を解決するため、1993 年に RFC1393 [注]が提案され、経路変更の問題の解決が図られたが、この RFC に対応していないルータもあるため、依然問題は残る。また、

[注] RFC（Request For Comment）は、インターネットに関する技術の標準化を行う組織である IETF が発行している文書である。RFC1393 は、題目が「Traceroute Using IP Option」となっており、IP トレースルートオプションと、個々のルータが通知する ICMP トレースルートメッセージのフォーマットや手順が規定されている。

traceroute・tracert コマンドは時間超過メッセージなどの ICMP の機能を利用するが、ルータによってはセキュリティの観点からこのようなメッセージを返さない設定にしている場合も少なくない。その場合、Tracing は経路途中で打ち切られることになる。

図 12 は、http://www.npa.go.jp/へ tracert コマンドでトレースした結果であるが、途中で ICMP のメッセージが返らなくなっており、トレースが順当に行われなかった例である。

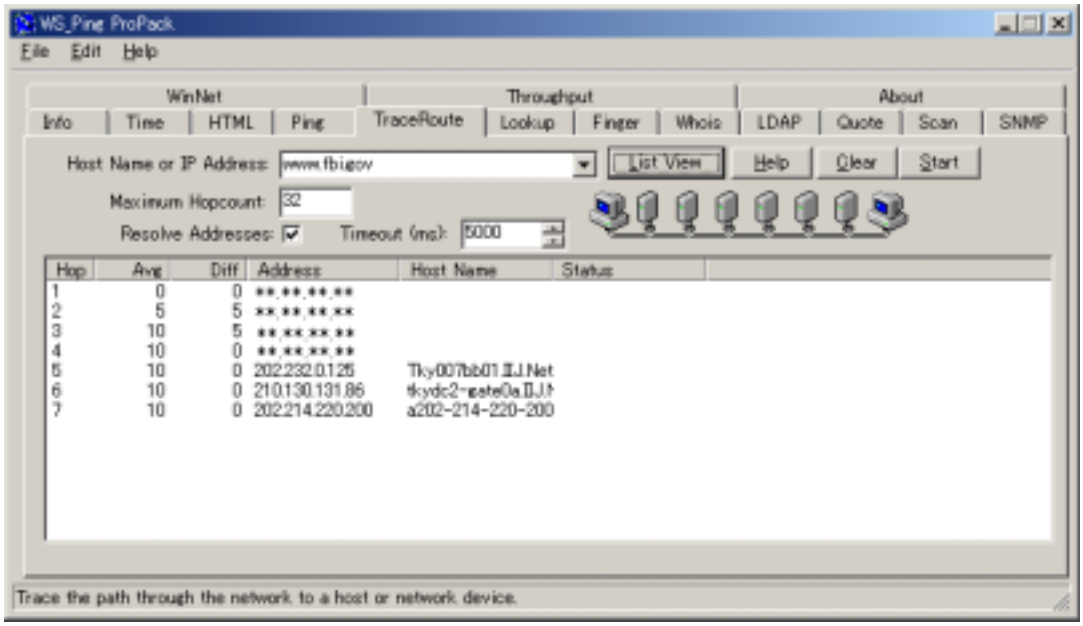
**図 12**




この traceroute・tracert コマンドを GUI 化し、さらに nslookup や whois の機能を加えたツールがいくつか開発されている。

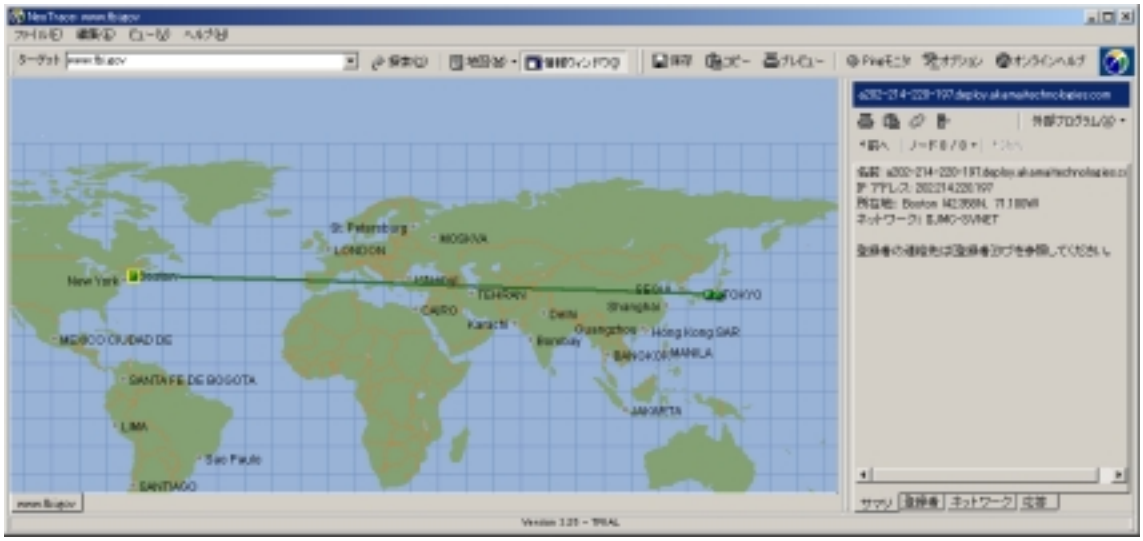
図 13 は、Ipswitch 社の WS_Ping ProBack というソフトで、UNIX 上で使用されるコマンドが Windows 上で簡単に利用できる。図 13 では、東京から FBI（合衆国連邦捜査局）の Web サイト（http://www.fbi.gov/）へ経路探索を行っている。

**図 13**



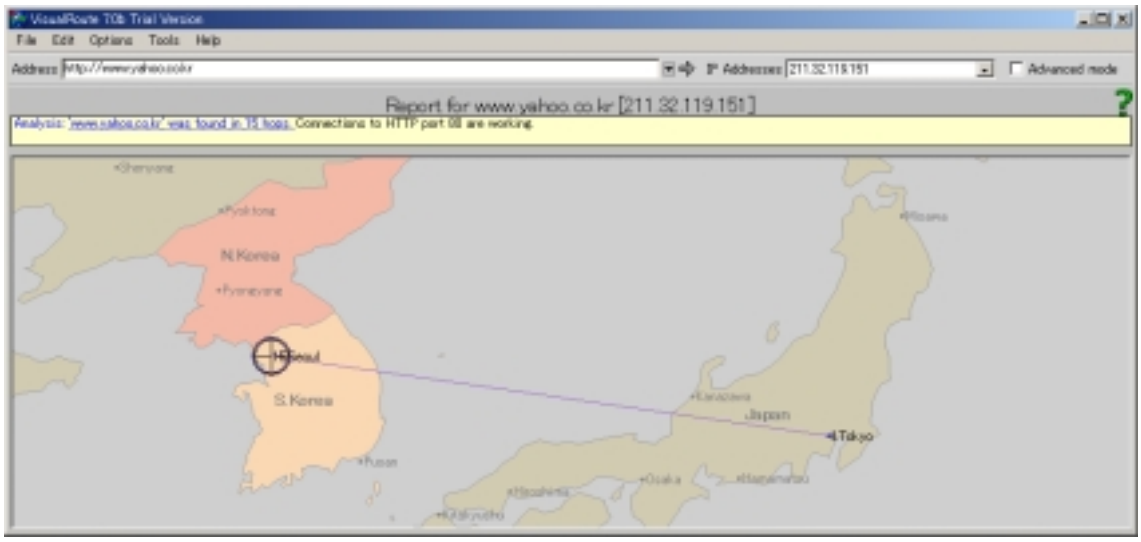

NeoWorx 社が開発したインターネット経路探索ソフト NeoTrace Pro では、経由地点を世界地図にマッピングし、国外へのトレースにおいても視覚的な把握が容易になるよう設計されている。図 14 では、同じく、東京から FBI（合衆国連邦捜査局）の Web サイト（http://www.fbi.gov/）へ経路探索を行った結果画面である。

**図 14**



NeoTrace Pro と同じく、世界地図によって視覚的な経路情報把握が行えるソフトとして Visualware 社の VisualRoute というソフトがある。図 15 は、Visual Route を用いて、Yahoo! Korea のサイト（http://www.yahoo.co.kr/）へトレースした結果画面である。

**図 15**



## 3. ログ解析

Firewall や IDS、各サーバなどのネットワーク経路上の位置するホストに蓄積されたログを収集し、解析することで総合的に Tracing を行うことが可能である。ログの形式はシステムにより様々であるが、基本的には、日付、時刻、ソース IP アドレス、ターゲット IP アドレス、どのサービスに対してアクセスがあったかを示すポート番号、パケットの種類などの情報が集められる。定期的に、あるいは常時ログ解析を行うことにより攻撃を早期に発見することができる。ただし、攻撃の種類によってはその痕跡がログに残らない場合もあるため、攻撃が行われたことが明らかになった直後にログ解析によって Tracing を行うということもありうる。

Firewall では、基本的に攻撃のログは記録されない。記録されるログは、Firewall がパケットの通過を許可したか、拒否したかの記録だけであり、通過を許可したログと拒否したログの持つ意味は異なる。

通過を許可したログにより、ポートスキャンなどの攻撃前の調査行為を解析できる可能性がある。ポートスキャンは、ターゲットとなるネットワークにおいて、どの IP アドレスのマシンがどのサービスを提供しているかどうかを調査する行為である。インターネット上で Web や FTP などの特定のサービスを提供している場合、そのマシンのサービスへのアクセスは Firewall では拒否しない。そのため、Firewall が通過を許可したアクセスのログの中には、このような調査行為の痕跡が残っている可能性がある。ポートスキャンなどの調査では、そのサービスへアクセス可能かどうかの確認を行っているため、発信元を偽造している可能性はきわめて低いと言える。また、大半の攻撃者は攻撃を行う前に事前に調査を行うため、この段階で、調査行為を行っている発信元をリストアップして記録に残しておくことは有用である。

Firewall が通過を拒否したログからは、その Firewall が守っているネットワークのホストが攻撃された場合、その攻撃元を解析できる可能性がある。攻撃されたホストのログは改竄や消去が行われている可能性があるため、その信頼性に問題がある。また、攻撃者が一回の攻撃で Firewall をくぐり抜け、内側のホストへの攻撃に成功した場合は、当然 Firewall にその発信元に関するログは残されないが、通常攻撃は数度に渡って試みられて成功する。その場合、攻撃の前後で Firewall に残されたログを解析することにより発信元が解析できることになる。

IDS は攻撃の検知を主眼としているため、比較的軽微な攻撃や悪戯行為などの場合は、すぐさま検知アラートを出し、管理担当者に通知して、的確に対処することが可能である。この検知アラート自体がログ解析とも捉えることができるのであるが、問題点も多々ある。IDS の弱点としてよく挙げられるのが、DoS 攻撃（Denial of Service：サービス不能攻撃）に弱いということである。DoS 攻撃は、大量のトラフィックを送信し続けることによりターゲットの機能を停止させる攻撃である。元々ネットワーク内のトラフィ

ックを大量に処理している IDS はこの負荷に対処することが難しいと言える。DoS 攻撃によって IDS の検知機能が停止させられた場合、ログをとることもできなくなる可能性がある。さらに、IDS のログ解析においては誤検知によるログと実際の攻撃によるログの見極めが必要になる。また、未知の攻撃手法に対して IDS は機能しないため、このような攻撃が行われた際にはログ自体が存在しない可能性もある。IDS はあくまで攻撃の検知を行い、それを人間に知らせることが主な機能であり、その攻撃からホストやネットワークを守ることはできない。この意味で、IDS はそれを取り付けたから安全性が増すというものではなく、その運用が最も重要であり、様々な事態に対応可能な専門的な知識や人員が必要であると言える。ログ解析においても、単純にログを貯めていけばいいということではなく、状況により柔軟に対応していくことが求められる。

ログ解析や IDS の運用には、専門的な知識と技術が必要となるため、すべての組織が行えることではないとも考えられる。しかし、ネットワーク上で犯罪が行われた場合、ほとんど唯一の証拠となるログをどのように管理し、有効に扱っていくかということは今後ますます重要な課題となっていくであろう。