TCP/IPに係る既知の脆弱性に関する調査報告書

改訂第5版

インターネットの標準的な通信手順に知られている
セキュリティ上の弱点箇所に関する解説書

IPA
独立行政法人 情報処理推進機構 セキュリティセンター

2010年11月

登録商標等について

- Microsoft、MS、Windows、Windows 2000、Windows NT、Windows XP、Windows ロゴ、Internet Explorer、Outlook、Outlook Express などは、米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- Sun Microsystems、Sun ロゴ、Java コーヒーカップロゴ、Solaris、Java、JDK などは、米国 Sun Microsystems の米国およびその他の国における登録商標または商標です。
- その他、本文章に記載されている会社名、商品名、製品名などは、一般に各社の商標または登録商標です。
- 本書では、™、©、®などを記載しません。

本資料は、以下の URL からダウンロードできます。

TCP/IP に係る既知の脆弱性に関する調査
http://www.ipa.go.jp/security/vuln/vuln_TCPIP.html

目次

はじめに

本調査報告書は、TCP/IP に係る既知の脆弱性に関して調査した報告書です。

背景

コンピュータをはじめとしたインターネットに接続する電子機器には、インターネットの標準的な通信手順を実現するための TCP/IP ソフトウェアが組み込まれています。近年では、一般のユーザが利用する情報家電や携帯端末などの電子機器にも使われるようになり、TCP/IP ソフトウェアは広く利用されています。

これらのTCP/IPソフトウェアは、これまで多くのセキュリティ上の脆弱性が公表されてきました。脆弱性情報が公表されると、それに対応した対策情報も公表され、機器ごとに脆弱性対策が実装されてきました。これらの脆弱性は、内容を理解するためには高度な技術力を必要としますが、詳細な情報をとりまとめた資料がなく、このため、新たに開発されるソフトウェアにおいて、既に公表されている脆弱性対策が実装されていない場合が数多く見受けられます。

今回の調査報告書は、このような課題に対し、既に公表されている TCP/IP に係る脆弱性について情報を収集分析し、詳細な解説書としてとりまとめたものです。また、ソフトウェアのプログラマ向けの実装ガイド、システムエンジニアやサーバ運用者向けの運用ガイドなども、個々の脆弱性の問題ごとに記載しております。

本調査の目的

脆弱性の対策を図るためには、開発者が脆弱性についての技術的な知識を知る必要があります。

本調査報告書では、TCP/IP ソフトウェアを開発するまたは開発に関わる立場にいる人、TCP/IP ソフトウェアを運用している人を読者に想定し、TCP/IP ソフトウェアに発見される脆弱性が低減することを目指します。

本調査報告書が今後のコンピュータを初めとしたインターネットに接続する電子機器のセキュリティ対策の参考となることを期待しています。

1). TCP の初期シーケンス番号予測の問題

1)-1. 分類:TCP 【IPv4】【IPv6】

1)-2. 概要

TCP 接続において生成される、初期シーケンス番号(Initial Sequence Number:ISN)が予測可能である場合、なりすましが可能となる。

1)-3. 解説

攻撃手法とその影響

この問題を悪用して行われる攻撃は、初期シーケンス番号が予測可能であるホストに、偽造パケットを正しいパケットとして受信させることができる。この問題で行われうる攻撃の例を図 1-1 から図 1-5 に示す。

図 1-1 において、ホスト A はサーバ、ホスト B はクライアントである。ホスト A は初期シーケンス番号の予測が可能である。

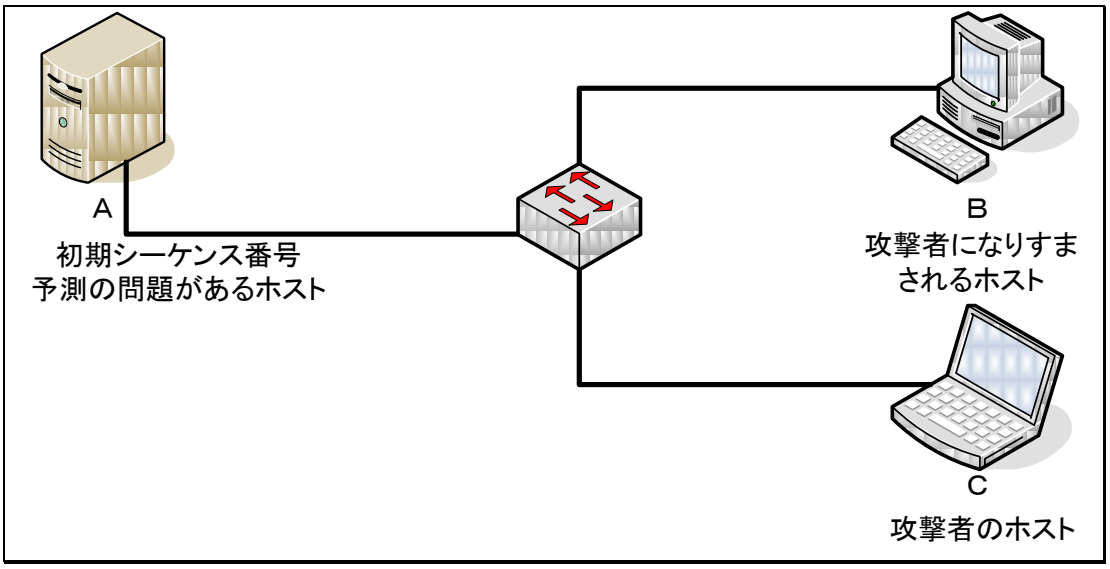


図 1-1 ターゲットネットワーク

【TCP の初期シーケンス番号予測の問題】

攻撃者はホスト C から、なりすます対象のホスト B のアドレスをソースにセットした偽造 SYN パケットを、ホスト A に送信し、ホスト A にホスト B との 3 ウェイハンドシェイクを開始させる。

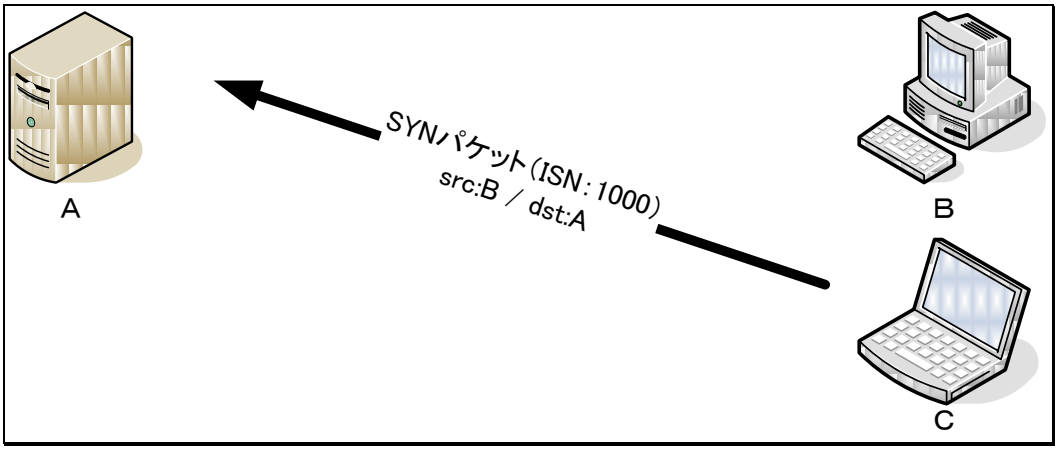


図 1-2 なりすまし TCP 接続の開始

ホスト A は、ホスト B に対して自身の初期シーケンス番号(この例では 2000)をセットした SYN/ACK パケットを送信し、ハーフオープン状態となる。(注 1)パケットはホスト B に対して送信されるため、攻撃者は直接ホスト A の初期シーケンス番号を知ることはできないが、これを推測可能である。(注 2)

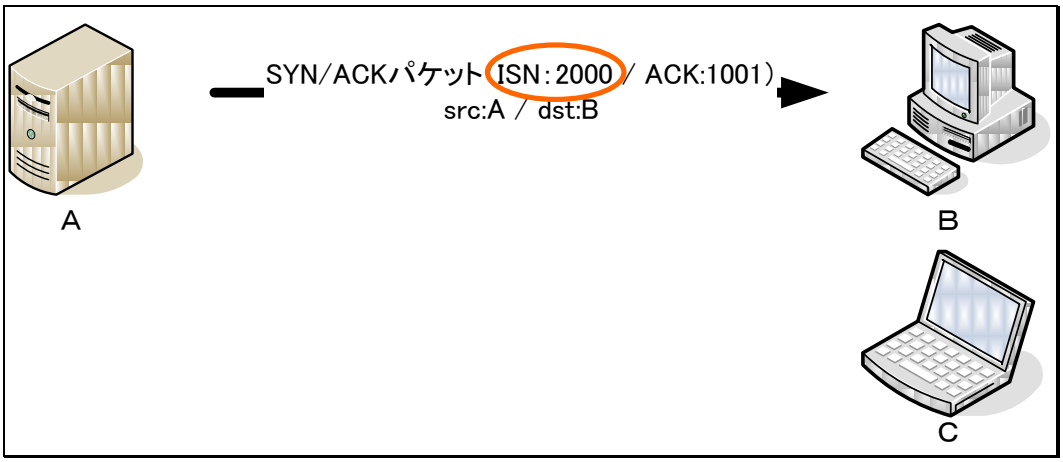


図 1-3 ハーフオープン状態

注 1:ホスト B が応答可能である場合、ホスト A に対して RST パケットが送信され、ホスト A のハーフオープン状態が終了してしまうため、攻撃者はなりすましによる 3 ウェイハンドシェイクを成立させることができない。そのため、ホスト B を何らかの方法で応答不能状態にする必要がある。(その方法として説明される例、また実例として知られているものに SYN Flood がある。)

注 2:ホスト A がアイドル状態でない場合、初期シーケンス番号の実値と推測値が異なる可能性が高くなる。

【TCP の初期シーケンス番号予測の問題】

攻撃者は、推測したホストＡの初期シーケンス番号(この例では 2000)から、対応する確認応答　番号(この例では 2001)をセットした偽造 ACK パケットをホスト A に送信する。

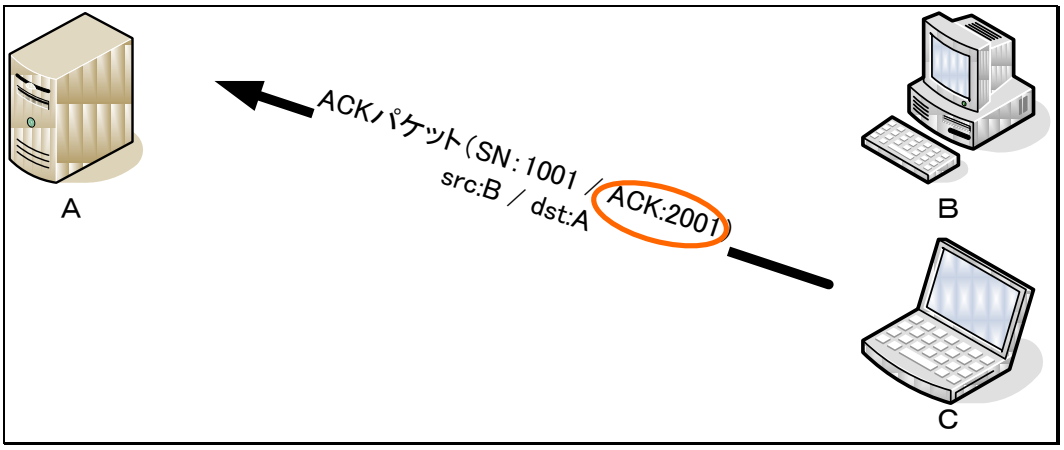


図 1-4 偽造 ACK パケットの送信

ホストＡは、ホストＢに送信した SYN/ACK パケットに対応する偽造 ACK パケットを受信したことで、ホスト B との 3 ウェイハンドシェイクが完了したと認識する。

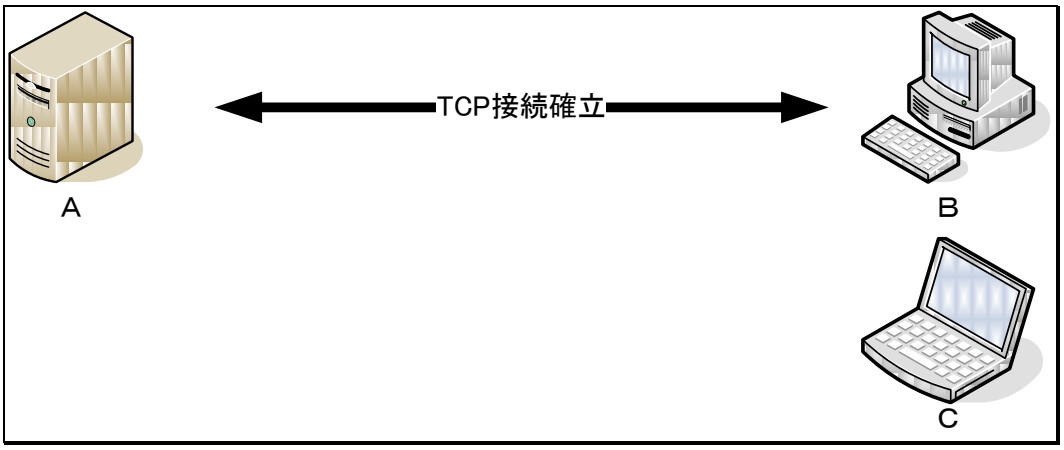


図 1-5 なりすまし TCP 接続の確立

これ以降攻撃者は、なりすます対象のホスト B のアドレスをセットした偽造パケットを作成して送信し、ホストＡにそのパケットを受信、処理させることができる。ただし、攻撃者は当該ネットワークを盗聴できる場合をのぞいて、送信した偽造パケットに対する応答パケットを受け取ることはできない。

【TCP の初期シーケンス番号予測の問題】

原因と考察

この脆弱性の原因は、初期シーケンス番号の生成方法の実装にある。シーケンス番号と確認応答番号は、TCP 接続において、接続識別子としての役割を担っている。シーケンス番号と確認応答番号に整合性が認められれば、TCP 接続中の正しいパケットとして受信され、データが処理される。そのため、シーケンス番号と確認応答番号は TCP 接続の認証において、一種のパスワードとしての役割を果たしていると言える。

シーケンス番号と確認応答番号は、初期シーケンス番号を基準として増加する値である。基準となる初期シーケンス番号は、TCP 接続開始時に行われる、3 ウェイハンドシェイクにおいて生成される。その過程を図 1-6 から図 1-9 に示す。

ホストBが、接続先のホストAにSYNパケットを送信し、3ウェイハンドシェイクを開始する。この パケットには、ホスト B が生成した初期シーケンス番号(1000)がセットされる。

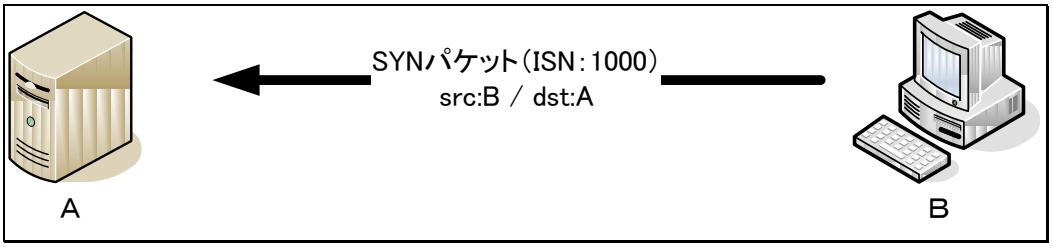


図 1-6 3 ウェイハンドシェイクの開始

ホスト A は、ホスト B の SYN パケットに対して SYN/ACK パケットを送信し、ハーフオープン状態になる。このパケットには、ホスト A からの接続開始のために、ホスト A が生成した初期シーケンス番号(2000)と、先のパケットへの応答であることを示すために、ホスト B が生成した初期シーケンス番号から計算された確認応答番号(1001)がセットされる。

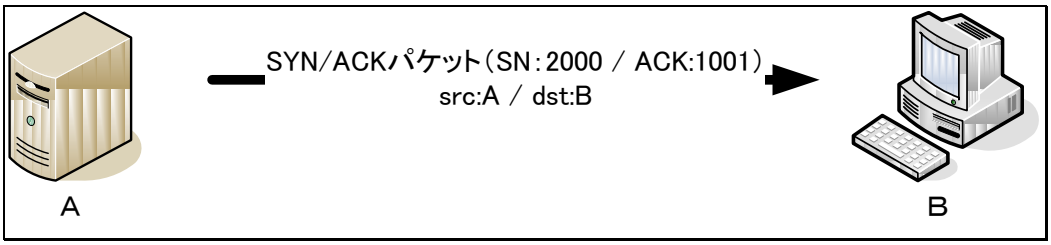


図 1-7 ハーフオープン状態

ホスト B はこのパケットによって、次の ACK パケットに必要なホスト A の初期シーケンス番号(2000)を取得する。同時に、自身が生成した初期シーケンス番号から計算される、正しい確認応答 番号(1001)がセットされているかを確認する。正しい確認応答番号を計算できるのは、ホスト B の 生成した初期シーケンス番号がセットされた SYN パケットを受け取ったホストだけである。このことから、ホスト B は SYN/ACK パケットが、自分が接続開始を要求したホスト A からの正しい応答であることを認証する。

ホスト B は、ホスト A の SYN/ACK パケットに対して ACK パケットを送信する。このパケットには、自身の初期シーケンス番号を基準として計算されるシーケンス番号(1001)と、ホスト A の初期シーケンス番号のパケットへの応答であることを示すために、ホスト A が生成した初期シーケンス番号から計算された確認応答番号(2001)がセットされる。

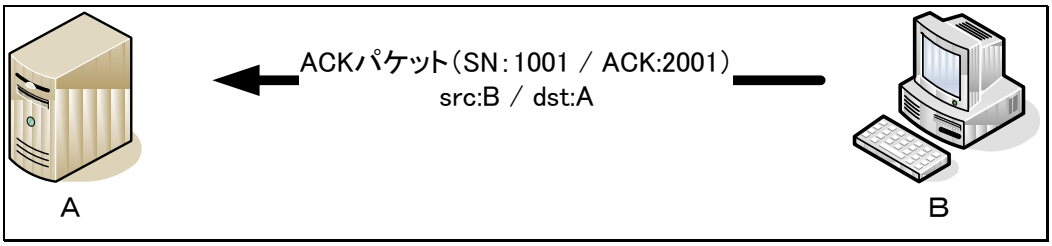


図 1-8 ACK パケットの送信

ホスト A は、ホスト B からの ACK パケットのシーケンス番号が、ホスト A からホスト B に送信した確認応答番号(1001)と一致し、また ACK パケットの確認応答番号が、自身が生成した初期シーケンス番号から計算された確認応答番号(2001)と一致するか確認する。

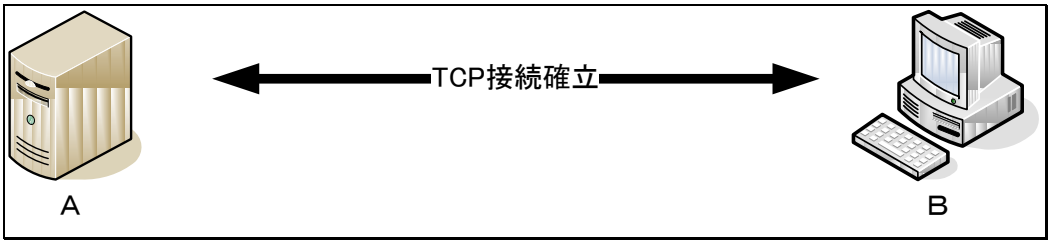


図 1-9 TCP 接続の確立

正しい確認応答番号を計算できるのは、ホスト A の生成した初期シーケンス番号がセットされた SYN/ACK パケットを受け取ったホストだけである。このことから、ホスト A は ACK パケットが、接続開始を要求してきた、ホスト B からの正しい応答であることを認証し、接続を確立する。

【TCP の初期シーケンス番号予測の問題】

IP アドレスを偽造したパケットを生成することは容易であるが、アドレスを偽造しただけでは受信ホストにパケットを受信、処理させることはできず、正しいシーケンス番号が必要となる。このシーケンス番号の計算に必要な初期シーケンス番号は、TCP 接続を確立する 2 ホストしか知り得ない情報である。しかし、初期シーケンス番号が予測可能であると、ホストが正しいパケットとして受信、処理してしまうパケットを偽造させる機会を、攻撃者に与えてしまう。

1)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題について、よく整理された情報は CERT Coordination Center(以下、CERT)が 2001 年に発行した CA-2001-09 である。この問題は、1985 年の Robert T. Morris 氏の論文「A Weakness in the 4.2BSD UNIX TCP/IP Software」において、TCP/IP の懸念点として指摘された。4.2BSD システムが、他のホストを信頼することで、認証無しにリモートからコマンドの実行が可能であり、TCP/IP の仕組みと 4.2BSD での実装の不備から、その仕組みを悪用可能であることを示した。(注 1)

1989 年には、Steve Bellovin 氏が「Security Problems in the TCP/IP Protocol Suite」の中で、Morris 氏の指摘した問題を取り上げ、対処として乱数の採用を含む、数種の方策を提案した。また 1994 年にシステムで乱数を使用する際の、疑似乱数生成機構についての RFC(Request For Comment)1750 が発行された。1995 年には CERT がインターネットにおいて、この種の攻撃が大規模に行われたという報告 CA-1995-01 を発行した。また、その 1 年前の 1994 年に、San Diego Supercomputer Center の研究員 下村 努氏のネットワークが、この問題を手段の1つとして Kevin Mitnick によって侵害された。この事件は、情報セキュリティの事例として、しばしば取り上げられており、詳細は、下村氏の著書「Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw-By the Man Who Did It」(1996 年出版 ISBN 0786862106)で述べられている。

注 1:ここでのリモートからのコマンド実行とは、rsh、rlogin 等の UNIX 由来の一連のサービス、コマンド群によって実現されるもので、r 系サービスとも呼ばれる。サーバ側で信頼するホスト(ホスト名、IP アドレス)、ユーザ(ユーザ名)を設定することで、パスワード認証を行わずにクライアントからサーバにコマンドを実行させることができる。コンピューティング環境そのものや、UNIX OS が主として学術研究者に利用されていた時代に、利便性から広く利用されていた。現在のインターネットを含むネットワーク環境においては利用しないか、ssh をはじめとする安全な手段を利用すべきである。

【TCP の初期シーケンス番号予測の問題】

1996 年、この問題に対して本質的な解決を促すために、RFC 1948「Defending Against Sequence Number Attacks」が発行された。2001 年、BindView(注 2)の Michal Zalewski は「STRANGE ATTRACTORS AND TCP/IP SEQUENCE NUMBER ANALYSIS」と題した論文において、数種類の OS の初期シーケンス番号生成について調査と相関分析を行い、多くの OS において初期シーケンス番号生成の実装は、統計的な予測が可能であるという問題があり、実装を改良することを提案した。また 2002 年には、追加の調査も行われている。同じく 5 月に CERT が CA-2001-09 を発行している。この勧告は、Morris 氏の論文を契機としたこの問題に関する主要な事柄を整理し、解決策までをまとめた。その後、各ベンダによる対策が進み、現在ではこの問題は解決されている。

注 2:BindView 社は 2005 年に Symantec 社に買収された。

1)-5. IPv6 環境における影響

この問題は TCP プロトコルの問題で、OSI 参照モデルのトランスポート層に属する問題であるため、概念的には IP プロトコルのバージョンに限らずこの問題は再現すると考えられ、IPv6 環境でも影響を受ける可能性がある。ただし、実際の IPv6 での影響についての詳細は不明である。

1)-6. 実装ガイド

CA-2001-09、RFC 1948 を参照して実装する。これらドキュメントでしばしば登場する乱数生成については、RFC 4086、NIST800-90 等が有用な参考資料となる。また、この問題に対処済みである、オープンソース OS の実装を参考とすることも有用である。(注 3)

1)-7. 運用ガイド

1. rlogin での信頼ホストの利用等、容易に偽造可能な値のみを認証に利用するサービスを削除、または停止する。
2. IPsec を例とするネットワーク層での暗号化対策を実施する。

注 3:http://lxr.linux.no/source/drivers/char/ChangeLog#L258(Linux)

http://lxr.linux.no/source/drivers/char/random.c#L1855(Linux)

http://www.openbsd.org/cgi-bin/cvsweb/src/sys/netinet/tcp_subr.c(OpenBSD)

1)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2006 年 3 月)のものである。

1981 年 RFC 793, TRANSMISSION CONTROL PROTOCOL.
http://www.ietf.org/rfc/rfc0793.txt

1985 年 TCP プロトコルにおけるセキュリティ上の懸念事項を初めて指摘した。
(Robert T. Morris 著)
http://www.pdos.lcs.mit.edu/~rtm/papers/117.pdf

1989 年 TCP シーケンスで利用するための ISN 生成機構を強固にすることを提案した。(Steve Bellovin 著)
http://www.cs.columbia.edu/~smb/papers/ipext.pdf

1994 年 RFC 1750, Randomness Recommendations for Security.
http://www.ietf.org/rfc/rfc1750.txt
http://www.ipa.go.jp/security/rfc/RFC1750JA.html
※現在は RFC 4086 の作成により廃止されている。
San Diego Supercomputer Center の研究者 下村努氏のネットワークに対して、Kevin Mitnick がシーケンス番号の推測他によって侵入した。

1995 年 CERT Advisory CA-1995-01 勧告 が出される。
http://www.cert.org/advisories/CA-1995-01.html

1996 年 RFC 1948, Defending Against Sequence Number Attacks.
http://www.ietf.org/rfc/rfc1948.txt
http://www.ipa.go.jp/security/rfc/RFC1948JA.html

1999 年 Common Vulnerabilities and Exposures CVE-1999-0077
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0077

【TCP の初期シーケンス番号予測 の問題】

2001 年　各種 OS の ISN 生成について調査、分析が行われた。(Michal Zalewski 著）
http://www.bindview.com/Services/Razor/Papers/2001/tcpseq.cfm
CERT Advisory CA-2001-09
http://www.cert.org/advisories/CA-2001-09.html
http://www.lac.co.jp/business/sns/intelligence/cert_advisory/CA-2001_09.html
Michal Zalewski が自身の調査ついて追加分析を実施した。
http://lcamtuf.coredump.cx/newtcp/

2002 年　RFC 4086, Randomness Requirements for Security.
http://www.ietf.org/rfc/rfc4086.txt
http://www.ipa.go.jp/security/rfc/RFC4086JA.html

2005 年　National Institute of Standards and Technology から乱数生成についてのセキュリティ関連資料が発行される。
http://csrc.nist.gov/publications/nistpubs/800-90/SP800-90revised_March2007.pdf

2). TCP 接続の強制切断の問題

2)-1. 分類:TCP 【IPv4】【IPv6】

2)-2. 概要

TCP 接続において、確立されている接続の送信先と送信元の IP アドレスポート番号、およびシーケンス番号(Sequence Number:SN)が推測可能、あるいは推測した SN がある範囲内である場合、偽造 RST パケットにより接続を強制切断可能となる。

2)-3. 解説

攻撃手法とその影響

この問題を悪用すると、TCP 接続を確立している 2 ホストの一方の接続を、第三者が偽造 RST パケットによって切断することが可能となる。この問題で行われうる攻撃の例を図 2-1 から図 2-3 に示す。

図 2-1 においてホスト A はサーバ、ホスト B はクライアントであり、この 2 ホスト間で TCP 接続が確立されている。

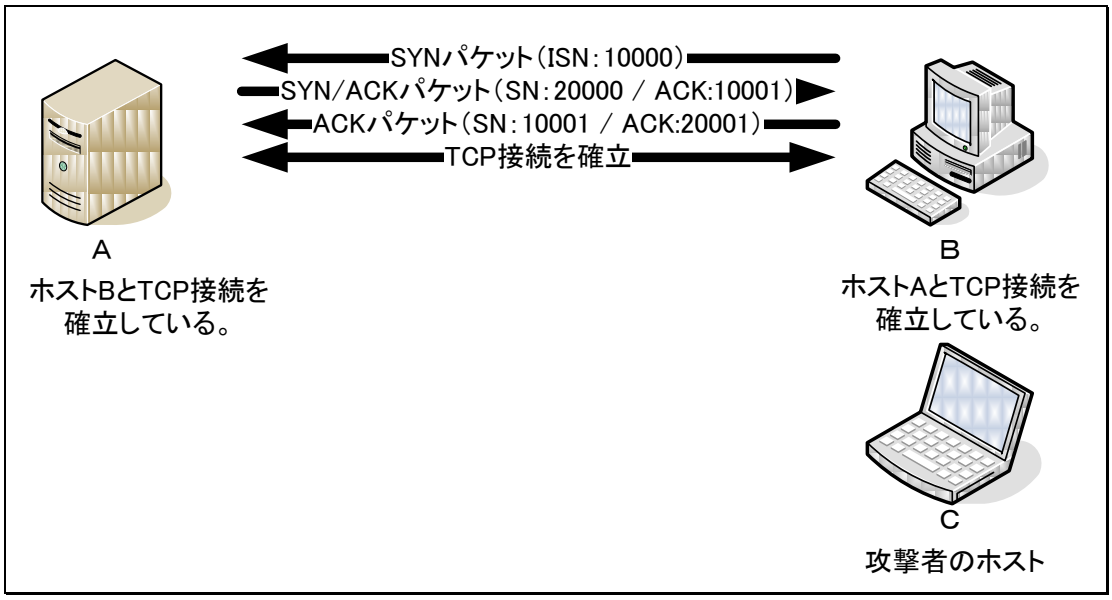


図 2-1 ターゲットとなる TCP 接続

【TCP 接続の強制切断の問題】

攻撃者は、推測したシーケンス番号をセットした RST パケットを送信する。図 2-2 では、RST パケットのシーケンス番号は 100 であるため、攻撃は失敗する。失敗した場合は、そのシーケンス番号に ウインドウサイズを加算して新しいシーケンス番号を用意し、それをセットした RST パケットを送信する。

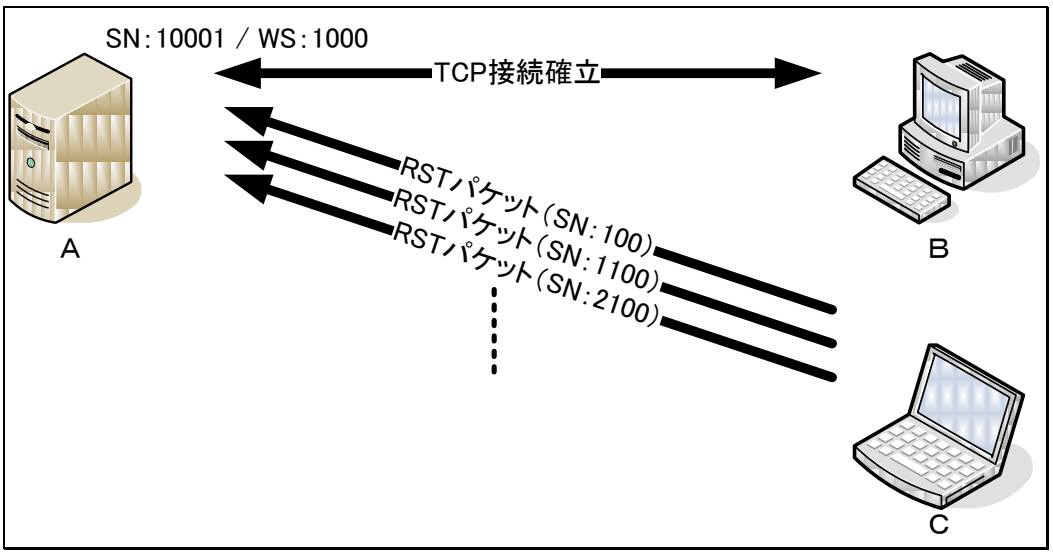


図 2-2 RST パケットの送信

攻撃者は、図 2-2 の RST パケットの送信を切断が成功するまで続ける。RST パケットのシーケンス番号は、ウインドウサイズによって増加し、やがてターゲットが受け入れて、接続を切断する範囲に到達する。この例では、ターゲットが受け入れるシーケンス番号の範囲は 10001 から 11001 である。

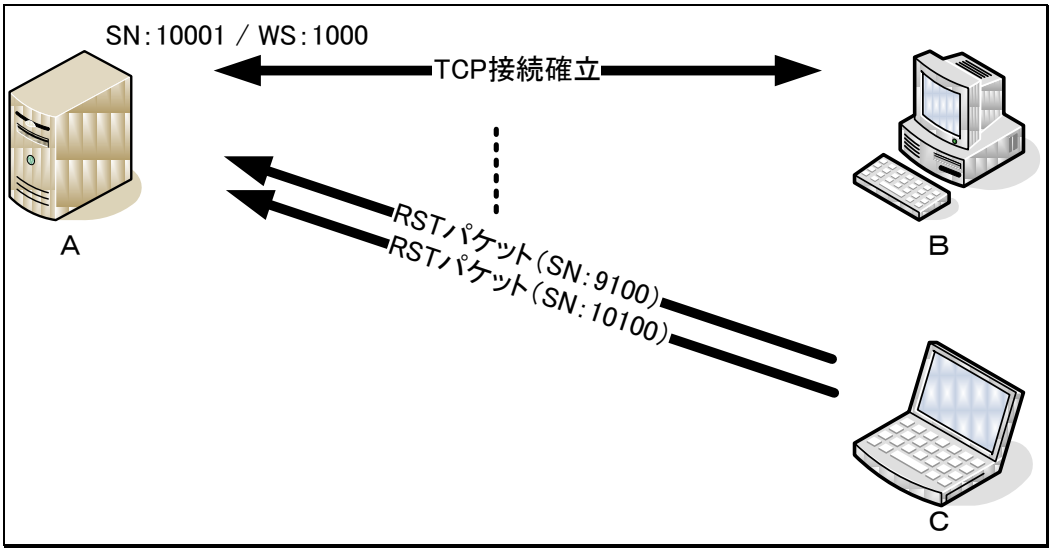


図 2-3 受け入れ範囲へ到達

【TCP 接続の強制切断の問題】

図 2-3 の最後の RST パケットで、シーケンス番号は 10100 となり、ホスト A とホスト B の接続は切断される。

原因と考察

この問題の原因は、RFC 793 で規定される TCP の仕様にある。RFC 793 の仕様では、接続を維持しているホストが RST パケットを受信した際に、そのパケットにセットされているシーケンス番号を確認して、以下の処理をする。

1. もし、RST パケットのシーケンス番号が受信ウインドウサイズより小さいか、より大きいなら、そのパケットを破棄する。
2. もし、RST パケットのシーケンス番号が受信ウインドウサイズ内なら、接続を切断する。

受信ウインドウサイズは、当該接続の次の受信シーケンス番号(Receive Next:RCV.NXT)を基点として、受信ウインドウサイズ(Receive Window:RCV.WND)を加算した範囲である。

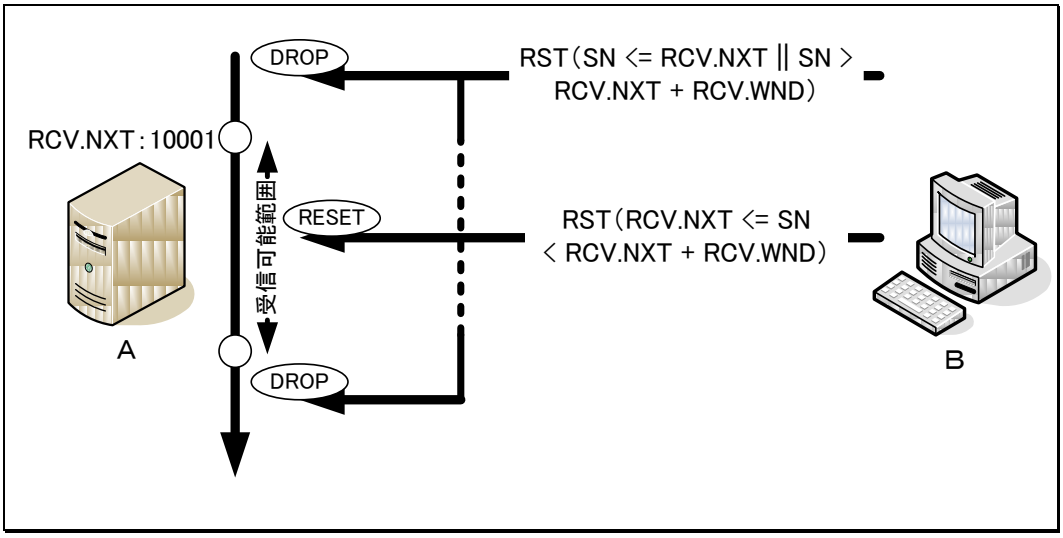


図 2-4 RFC 793 での RST パケット受信時の処理

この攻撃を成功させるには、攻撃対象接続とそのホストについて、いくつかの情報が必要である。

1. 2 ホストの IP アドレスと TCP ポート番号。(注 1)
2. RST パケットで使用するシーケンス番号。
3. 2 ホストが攻撃対象の接続で使用しているウインドウサイズ。多くの OS は、デフォルトのウインドウサイズが定められている。

注 1:一方(サーバ)のポート番号は、容易に把握可能である。もう一方(クライアント)のポート番号の推測が容易であるか否かは、対象 OS の実装に依存する。

【TCP 接続の強制切断の問題】

2)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題について、よく整理された情報は National Infrastructure Security Co-ordination Center NISCC(現在は、Center for the Protection of National Infrastructure CPNI)が 2004 年に発行した Advisory #236939 および、The Internet Engineering Task Force(以下、IETF)の TCP Maintenance and Minor Extensions Working Group が作成中の対策ドラフトである。この問題は、2003 年に Paul Anthony Watson 氏が発見し、氏の報告を受けて英国の政府系セキュリティ対策機関である NISCC が Advisory #236939 を発行した。

この種の攻撃の可能性は 1980 年代に、一部の専門家によって議論されていたが、成功させるには、接続について複数の情報が必要であり、とりわけ攻撃対象となる TCP 接続の次シーケンス番号を推測、あるいは盗聴等の手段を用いて、知る必要があることや、目標とするシーケンス番号に一致するまで、総当たりで RST パケットを送信する場合は、(2 の 32 乗／2)通りの可能性を試す必要があり、現実的ではないと考えられていた。しかし Watson 氏によって、TCP のウインドウサイズが分かれば、現実的な時間で攻撃が成立することが実証され、迅速に対策を実施すべき問題として注目された。HTTP のような、ごく短い時間で 接続が完了するアプリケーションは、この問題によって受ける影響は少ないものと考えられている。その一方で、telnet や ssh といった長時間接続を維持するアプリケーションは、この問題の影響を強く受ける可能性がある。また、Border Gateway Protocol(BGP)のようなプロトコルはネットワーク間の接続に使用されることから、影響が大きいと考えられている。

この問題に対して、各ベンダは独自の対策を実施し、この問題による影響を緩和している。問題の原因は RFC の仕様にあるため、仕様そのものの改訂も検討されている。2004 年 4 月に、IETF の TCP Maintenance and Minor Extensions Working Group が、この問題に対する対策のドラフトを作成している。このドラフトは 2006 年 3 月現在も修正が続けられており、RFC への反映は行われていない。(注 1)

IETF のドラフトでは、この問題に対して、以下の対策を提案している。

1. RST パケットのシーケンス番号がウインドウの範囲外であったなら、パケットを破棄する。
2. RST パケットのシーケンス番号が次の受信シーケンス番号に一致したなら、接続を破棄する。
3. RST パケットのシーケンス番号が次の受信シーケンス番号に一致しないが、ウインドウの範囲内であったなら、以下の確認応答(challenge ACK)を送信する。
   ＜シーケンス番号次の送信シーケンス番号:＞＜確認応答番号:次の受信シーケンス番号＞＜コントロール:ACK＞

注 1:ドラフトでは、RST、SYN、そしてデータのインジェクションの3つ問題について述べている。

2)-5. IPv6 環境における影響

この問題は TCP プロトコルの問題で、OSI 参照モデルのトランスポート層に属する問題であるため、概念的には IP プロトコルのバージョンに限らずこの問題は再現することが考えられる。マイクロソフトでは 2005 年 4 月に TCP/IPv4 の脆弱性(MS05-019)の 1 つとして、また 2006 年には TCP/IPv6 の脆弱性(MS06-064)の 1 つとして脆弱性に対処(注 1)しており、TCP/IP の実装によって IPv6 環境でも影響を受ける可能性がある。

2)-6. 実装ガイド

この問題は RFC 793 の仕様の問題であるため、仕様に従う限り、実装で回避することは出来ない。しかし、以下の実装により影響を緩和することが可能である。また、RFC が改訂された場合には、その内容に従うことを検討する。(注 2)

1. IETF のドラフトを参照し、提案されている実装に従う。
2. TCP のウインドウサイズを変更可能にする。
3. TCP のウインドウサイズを小さくする。
4. 送信時に使用するポートをランダムに選択する。

2)-7. 運用ガイド

1. IPsec を例とするネットワーク層での暗号化対策を実施する。
2. RFC 3704、RFC 3013 を参考にトラフィックのフィルタリングを実施する。(注 3)
3. 長時間接続を維持し、影響を受けると考えられるプロトコルについて暗号化等の保護を提供する拡張機能を使用する。(注 4)

注1： 双方ともに CVEID 番号 CVE-2004-0230 が割り当てられている。

注 2:この問題に関連するものとして、ISN の生成方法も強固にすべきである。

注 3:RFC 3704, Ingress Filtering for Multihomed Networks.

http://rfc.net/rfc3704.html

http://www.ipa.go.jp/security/rfc/RFC3704JA.html

RFC 3013, Recommended Internet Service Provider Security Service and Procedures.

http://rfc.net/rfc3013html

http://www.ipa.go.jp/security/rfc/RFC3013JA.html

注 4:RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option.

http://rfc.net/rfc2385.html

2)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1981 年

RFC 793, TRANSMISSION CONTROL PROTOCOL.
http://www.ietf.org/rfc/rfc0793.txt

1985 年

TCP におけるセキュリティ上の懸念事項を初めて指摘した。(Bob Morris 著)
http://www.pdos.lcs.mit.edu/~rtm/papers/117.pdf

1989 年

TCP で利用するための ISN 生成機構を強固にすることを提案した。
(Steve Bellovin 著)
http://www.cs.columbia.edu/~smb/papers/ipext.pdf

1994 年 RFC 1750, Randomness Recommendations for Security.
http://www.ietf.org/rfc/rfc1750.txt
http://www.ipa.go.jp/security/rfc/RFC1750JA.html
※現在は RFC 4086 の発行により廃止されている。

1995 年 CERT Advisory CA-1995-01
http://www.cert.org/advisories/CA-1995-01.html

1996 年 RFC 1948, Defending Against Sequence Number Attacks.
http://www.ietf.org/rfc/rfc1948.txt
http://www.ipa.go.jp/security/rfc/RFC1948JA.html

1999 年 Common Vulnerabilities and Exposures CVE-1999-0077
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0077

2001 年 ISN を生成する際の統計的弱点に見られる懸念を解説した。(Tim Newsham 著)
http://www.lava.net/~newsham/random-increments.pdf
各種 OS の ISN 生成について調査、分析が行われた。(Michal Zalewski 著)
http://www.bindview.com/Services/Razor/Papers/2001/tcpseq.cfm

【TCP 接続の強制切断の問題】

CERT Advisory CA-2001-09
http://www.cert.org/advisories/CA-2001-09.html
http://www.lac.co.jp/business/sns/intelligence/cert_advisory/CA-2001_09.html

2002 年　Michal Zalewski が自身の調査ついて追加分析を実施した。
http://lcamtuf.coredump.cx/newtcp/

2003 年　Paul Anthony Watson が TCP 接続切断の実現性について指摘した。
タイトル：SLIPPING IN THE WINDOW:TCP RESET ATTACKS

2004 年　National Infrastructure Security Co-ordination Center が Advisory を発行した。
http://www.uniras.gov.uk/niscc/docs/al-20040420-00199.html?lang=en
Common Vulnerabilities and Exposures CVE-2004-0230
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0230
United States Computer Emergency Readiness Team が Advisory を発行した。
http://www.us-cert.gov/cas/techalerts/TA04-111A.html
http://www.jpcert.or.jp/at/2004/at040003.txt
Cisco Security Advisory: TCP Vulnerabilities in Multiple IOS-Based Cisco Products
http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/cisco-sa-20040420-tcp-ios-j.shtml
Transmission Control Protocol security considerations

2005 年　http://www3.ietf.org/proceedings/05mar/IDs/draft-ietf-tcpm-tcpsecure-02.txt
マイクロソフトセキュリティ情報 MS05-019
http://www.microsoft.com/japan/technet/security/bulletin/ms05-019.mspx

マイクロソフトセキュリティ情報 MS06-064

2006 年　http://www.microsoft.com/japan/technet/security/bulletin/MS06-064.mspx

3). SYN パケットにサーバ資源が占有される問題(SYN Flood Attack)

3)-1. 分類:TCP 【IPv4】【IPv6】

3)-2. 概要

送信元アドレスを偽装した大量の不正 TCP 接続要求を受信すると、不完全な TCP 接続開始処理が大量に発生してサーバ資源が枯渇し、サービス不能状態となる。

3)-3. 解説

攻撃手法とその影響

この攻撃は、TCP における接続の確立手順として送受信ホスト間でやり取りされる 3 ウェイハンドシェイクを利用した攻撃である。

この攻撃は、基本としては図 3-1 に示すような 3 ホストで構成される。ホスト B は、不特定多数の応答しないホストであり、多くの場合、攻撃者によってランダムな IP アドレスが使用される。ホスト A は、攻撃者のホストから送信された要求に対し、応答をホスト B に返すため、ホスト B が実在する場合には、ホスト C が送信した要求と同じ数の応答が、ホスト A からホスト B 大量に送信されるため、ホスト B のトラフィックにも影響がでる場合がある。

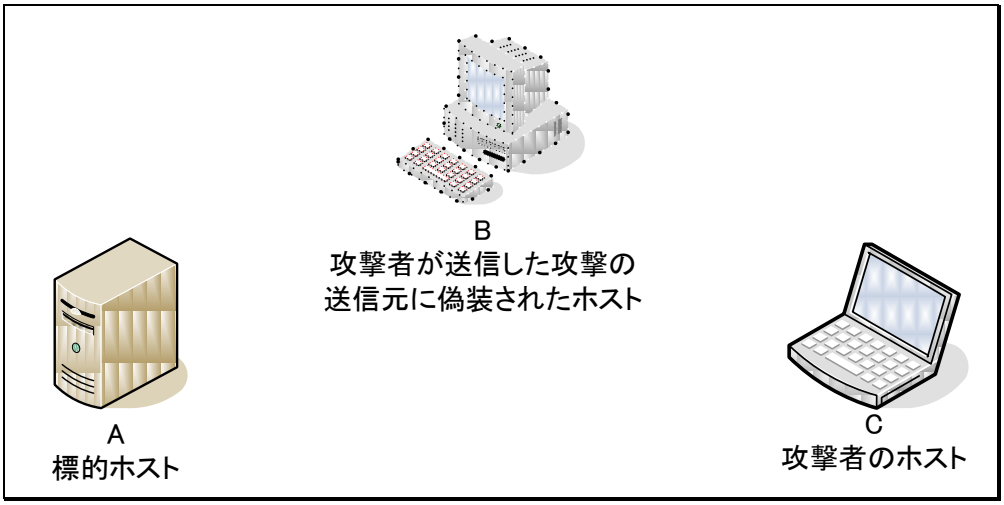


図 3-1 ターゲットネットワーク

攻撃者は、図 3-2、図 3-3 のようにホストＣから送信元アドレスをランダムに偽装した大量の不正な SYN パケットを標的となるホストＡに送信する。(説明を見やすくするために図 3-3 以降は攻撃パケットの１つについて記述するが、実際には図 3-2 のように大量の攻撃パケットが送信される)

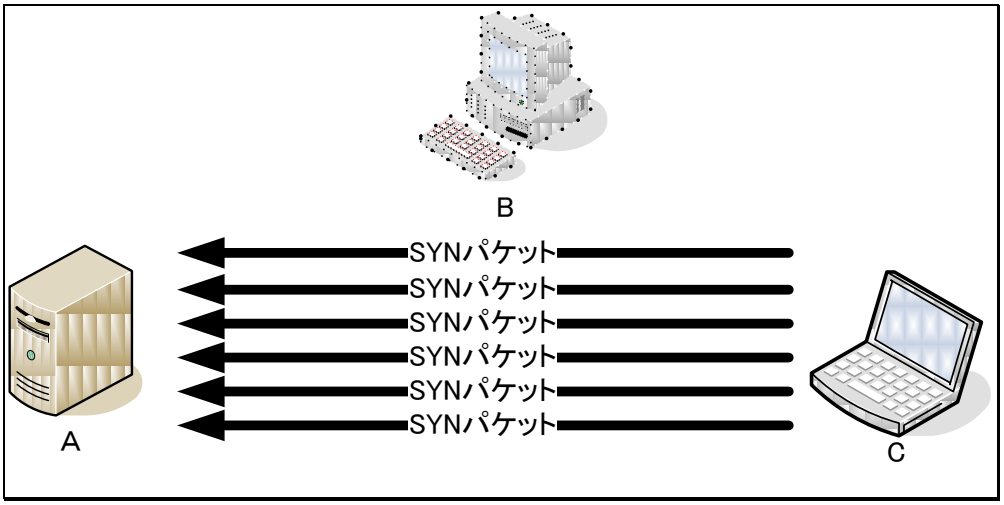


図 3-2 攻撃者は大量の SYN パケットを送信する

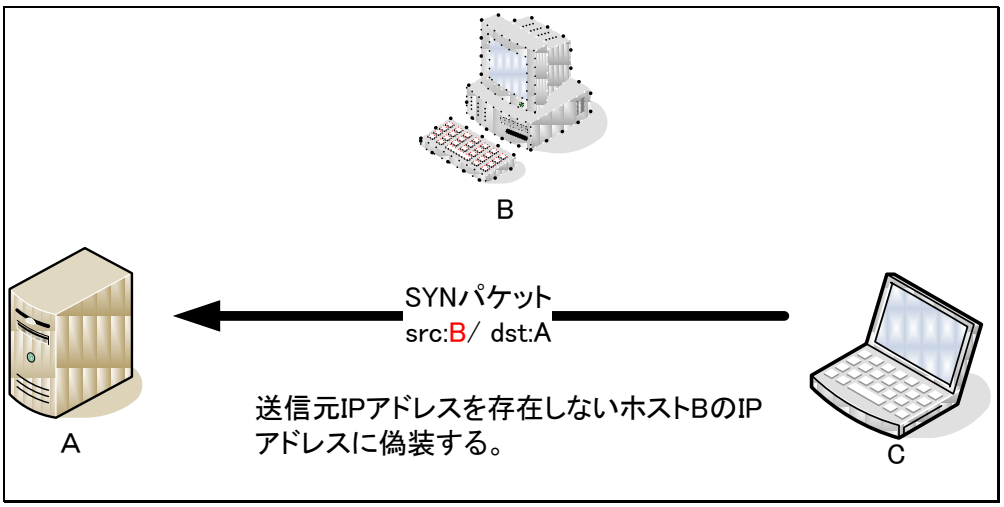


図 3-3 偽装した SYN パケットの送信

ホストＡでは不正な SYN パケットを処理し、図 3-4 に示すように SYN/ACK パケットを送信元に対して返送して、送信元からの ACK が返ってくるのを待ち続ける。大量の不正な SYN パケットを受信することによって、この ACK 待ち状態を管理するテーブルを使いきった状態になると、ホスト A 上では新たな接続要求を受けつけることが不可能となり、サービス不能状態となる。

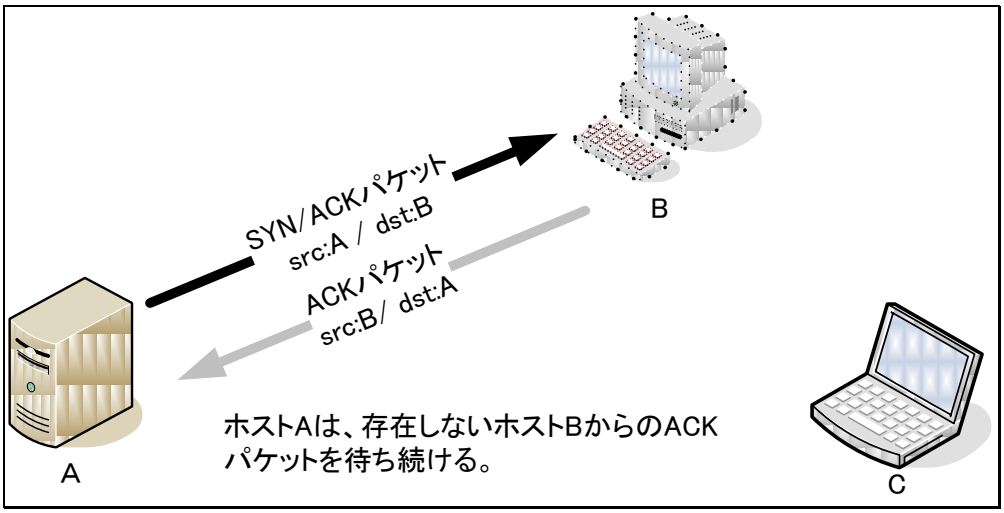


図 3-4 ACK 応答が返ってこない状態

この不完全な TCP 接続開始処理は、規定のタイムアウト時間(多くの OS に実装されている事実上の標準で約 3 分)が経過すれば破棄されるため、新たに接続要求を受け付けられる状態に復帰するが、攻撃が継続して行われている場合は再び ACK 待ち状態となるため、サービス不能状態が継続する。

また、攻撃者が、送信元アドレスをランダムではなく、存在するアドレス(ホスト B)に偽装した場合、ホスト B に対してホスト A より大量の SYN/ACK パケットが送信されるため、ネットワーク帯域が枯渇状態となり、ホスト B、および同一ネットワーク上の機器もサービス不能となる可能性がある。

原因と考察

TCP 接続を確立するために行う 3 ウェイハンドシェイクでは、送信元ホスト B は接続確立要求 SYN パケットを受信先ホスト A に送信する。次に、受信先ホスト A ではその受信した SYN パケットが到達したことを知らせ、ホスト A からの接続確立要求のために SYN/ACK パケットを送信元ホスト B に返送する。送信元ホスト A は受信先ホストからの SYN に対する確認応答 ACK パケットを返送して接続の確立が完了し、データ転送が開始される。以下の図 3-5 は 3 ウェイハンドシェイクを表したものである。

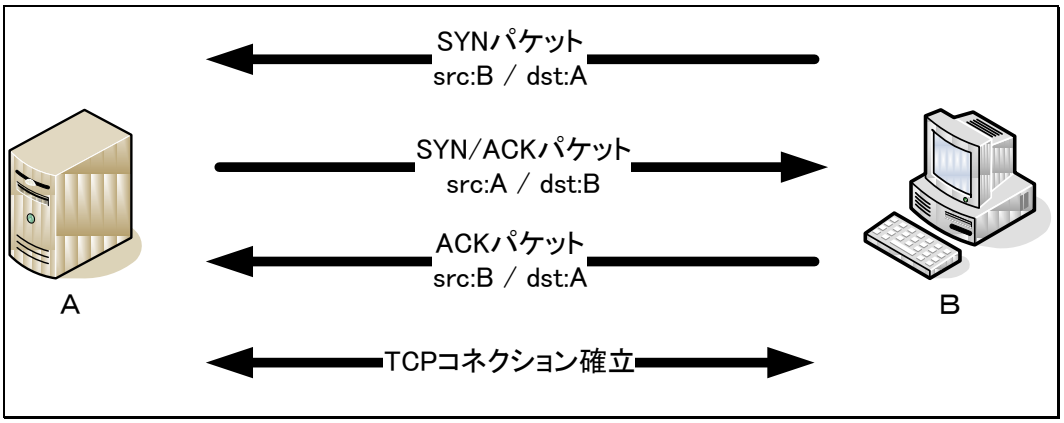


図 3-5 3 ウェイハンドシェイク

送信元を偽装された SYN パケットを受信すると、TCP 接続を確立するための接続情報は、コネクションバックログというキューに格納しつつ、偽装された送信元へ SYN/ACK を返し、送信元からの ACK を待つ。しかし、偽装された送信元からは応答は返ってこないため、応答待ち状態のバックログキューがそのまま残る。このコネクションバックログが一杯の状態になると、新たに SYN パケットを受信しても、図 3-6 のように直ちに RST を返すようになり、接続要求を拒否してしまう。たとえ正常な接続要求であっても接続が受け付けられないため、結果としてサービス不能状態となる。

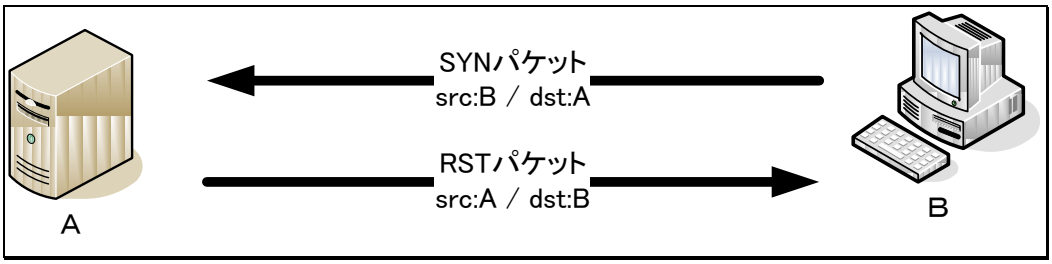


図 3-6 接続要求の拒否

バックログのサイズが小さい場合、少数の攻撃でもサービス不能となり、バックログを大きくとった場合は、少数の攻撃によってサービス不能になることはないが、短時間に多数の接続要求を受けた場合は大量のメモリを消費することによってサービス不能となる可能性がある。そのため、バックログの適切なサイズは、単に大きくすればよいものではなく、状況によって異なる。

3)-4. 発見の経緯とトピック、対策の動き、現在の動向

SYN Flood は、1996 年に CERT より CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks として注意喚起された。この問題を緩和する手段として、動的バックログ、SYN Cache, SYN Cookies などの対策があり、現在ではほとんどの主要なOSにこれらの防御機能が実装されている。

一方、現在では多くのファイアウォールで SYN Flood 攻撃の防御機能が実装されており、これらの製品によっても攻撃を緩和させることが可能である。この攻撃は、3 ウェイハンドシェイクの仕様上、完全に防御することは不可能であり、いくつかの緩和策はとられているものの根本的な対策がないまま現在に至っている。そのため、近年でも有効な攻撃手段として悪用されている攻撃である。

3)-5. IPv6 環境における影響

この問題は TCP プロトコル上の問題で、OSI 参照モデルのトランスポート層に属する問題であるため、IP プロトコルのバージョンに限らずこの問題は再現すると考えられ、IPv6 環境でも影響を受ける可能性がある。また参考情報として、linuxsecurity.com から「IPv6 approach for TCP SYN Flood attack over VoIP(IPv6 の VoIP 向け TCP SYN フラッド攻撃対策)」が公開されている。ここでは IPv6 と SYN Flood 攻撃を含む DoS 攻撃の対策、そしてパフォーマンス問題との関連性についてまとめられており、IPv6 VoIP 向けの SYN Flood 攻撃への影響が懸念されている。

3)-6. 実装ガイド

この問題は RFC 793 の仕様の問題であるため、仕様に従う限り、実装で回避することは出来ない。しかし、以下の実装により影響を緩和することが可能である。

1. 動的バックログ

   ネットワーク状況に応じてコネクションバックログのサイズを自動的に増減させる技術である。

2. SYN Cache

   バックログを生成する前の段階で、接続要求に関する最小限の情報だけを保持し、SYN Flood 攻撃によってSYN Cache が溢れた際には、不完全な接続要求を古いものから順次破棄することで、メモリの消費を抑制する技術である。

3. SYN Cookies

   SYN パケットのアドレス、ポート、初期シーケンス番号、秘密鍵から生成したハッシュ値を SYN/ACK パケットのシーケンス番号に埋め込んで返し、ACK パケットのアドレス、ポート、初期シーケンス番号、秘密鍵から算出したハッシュ値を比較することで確立中のセッションを特定し、メモリを消費せずに接続を確立する技術である。

3)-7. 運用ガイド

1. 影響を受ける製品に対して各ベンダより提供されているパッチを適用する。
2. SYN Flood 攻撃を排除するファイアウォールを含むルーティングデバイスを使用して信頼のないネットワークからの攻撃を防御する。

3)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1981 年 RFC 793, TRANSMISSION CONTROL PROTOCOL.
http://www.ietf.org/rfc/rfc0793.txt

1996 年 CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks
http://www.cert.org/advisories/CA-2000-21.html
ISS X-Force Database(135)
http://xforce.iss.net/xforce/xfdb/135
SYN cookies
http://cr.yp.to/syncookies.html

1998 年 RFC 2267, Network Ingress Filtering.
Defeating Denial of Service Attacks which employ IP Source Address Spoofing
http://www.ietf.org/rfc/rfc2267.txt
http://www.ipa.go.jp/security/rfc/RFC2267JA.html
RFC 2385, Protection of BGP Sessions via the TCP MD5 Signature Option.
http://www.ietf.org/rfc/rfc2385.txt

2000 年 マイクロソフト セキュリティ情報 MS00-091
http://www.microsoft.com/technet/security/bulletin/MS00-091.asp
http://support.microsoft.com/support/kb/articles/Q199/3/46.ASP
RHSA-2001:142-15 kernel 2.2 and 2.4: syncookie vulnerability
http://rhn.redhat.com/errata/RHSA-2001-142.html
Resisting SYN flood DoS attacks with a SYN cache
http://www.usenix.org/events/bsdcon02/full_papers/lemon/lemon_html/index.html
FreeBSD-SA-03:03.syncookies(2003-02-24)
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:03.syncookies.asc

SecurityFocus(6920)
http://www.securityfocus.com/bid/6920
Common Vulnerabilities and Exposures CVE-2003-1230
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1230

Internet server unavailable because of malicious SYN attacks(Q142641)
http://support.microsoft.com/kb/142641/en-us

2006 年 IPv6 approach for TCP SYN Flood attack over VoIP
http://www.linuxsecurity.com/content/view/121205/49/
IPv6 の VoIP 向け TCP SYN フラッド攻撃対策(パート IV)
http://opentechpress.jp/security/06/01/17/0150239.shtml
※上記タイトルの日本語版

4). 特別な SYN パケットによりカーネルがハングアップする問題(LAND Attack)

4)-1. 分類:TCP 【IPv4】【IPv6】

4)-2. 概要

送信元 IP アドレスと宛先 IP アドレスが同一に偽装された不正な SYN パケットを受信することで、自分自身に対して SYN/ACK パケットを返送してしまいサービス不能状態に陥る。

4)-3. 解説

攻撃手法とその影響

この問題は、TCP における接続の確立手順として送受信ホスト間でやり取りされる 3 ウェイハンドシェイクを悪用した攻撃である。図 4-1 に不正な SYN パケットを送信する状態を示す。

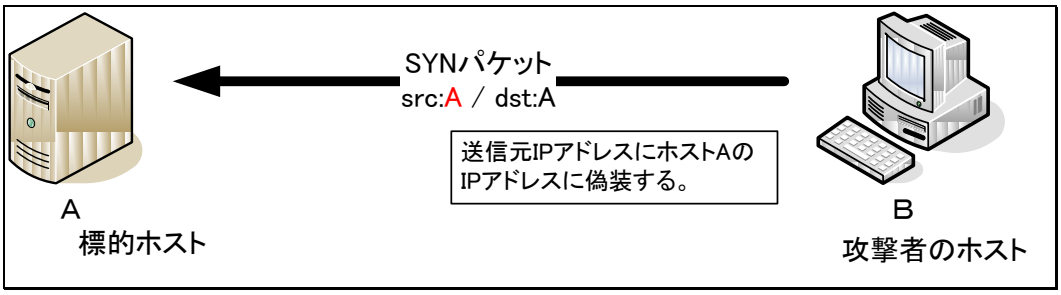


図 4-1 不正な SYN パケット

攻撃者はホスト B から送信元 IP アドレスと宛先 IP アドレスを同一に偽装した不正な SYN パケットを標的ホスト A に送信する。つまり、ここで利用する同一の IP アドレスは攻撃を試みるホスト B のものとなる。

ホスト A では、この不正な SYN パケットを受信すると自分自身が送信元であると判断してしまい、SYN/ACK パケットを自分自身に対して返送しようとする処理が行われる。図 4-2 にホスト A における処理イメージを示す。

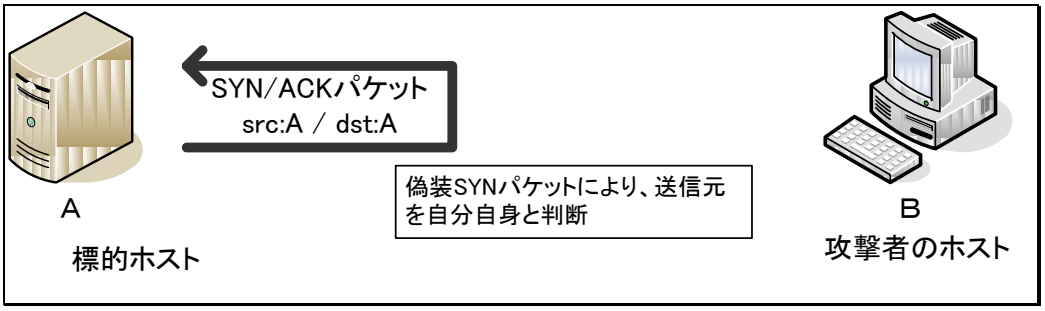


図 4-2 不正な SYN パケットを受信したホスト A での処理(イメージ図)

しかし、標的ホスト A 上では正常に処理することができず、これが原因で一定の期間(数秒から 1 分間ほど)システム負荷が高まる。攻撃者は繰り返しこのような不正な SYN パケットを送信することでシステム資源を消費して応答不能に陥らせたり、カーネルのハングアップ(フリーズ)を発生させたりすることで継続したサービス不能状態を引き起こすことが可能となる。

この問題の引き金となる不正な SYN パケットは、厳密には 2 種類確認されている。一つ目は、上記で説明したように IP アドレスの偽装にのみ着目したものである。2 つ目は IP アドレスに加えてポート番号についても着目したものである。送信元 IP アドレスを攻撃側の IP アドレスに偽装し、さらに送信元ポート番号および宛先ポート番号についても同一に偽装した SYN パケットを送信する。図 4-3 に送信元および宛先ポート番号として標的ホスト A のリッスンポートである TCP 139 番を指定した不正な SYN パケットを送信する状態を示す。

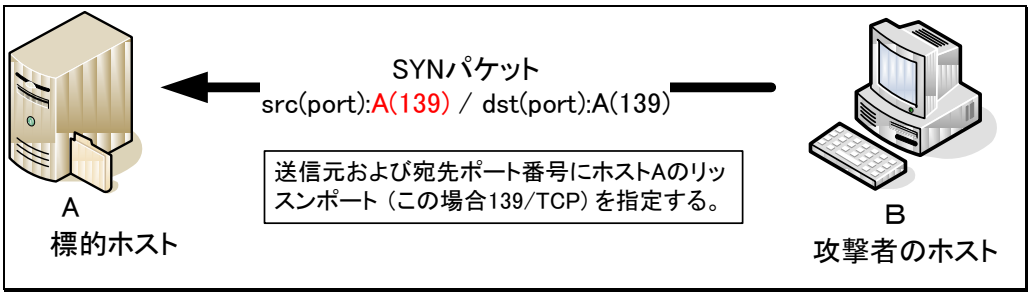


図 4-3 ポート番号も同一に偽装した不正な SYN パケット

いずれにしてもどちらの方法も送信元 IP アドレスと宛先 IP アドレスを同一に偽装することに変わりはないが、ホスト B における環境(システム資源の領域、オープンポート上で動作するサービスの実装など)や TCP の実装方法などの違いにより、それぞれの不正な SYN パケットによる影響の度合いは異なることが考えられる。

原因と考察

この問題に悪用される３ウェイハンドシェイクは、ホスト同士が TCP 接続を確立するために行われる。図 4-4 に３ウェイハンドシェイクを表したものを示す。送信元ホスト B はまず接続確立要求として SYN パケットを宛先ホスト A に送信する。次に、ホスト A ではその受信した SYN パケットが到達したことを知らせるのとホスト A からの接続確立要求のために SYN/ACK パケットをホスト A に返送する。ホスト A はホスト B からの SYN に対する確認応答 ACK パケットを返送して接続の確立が完了し、データ転送が開始される。

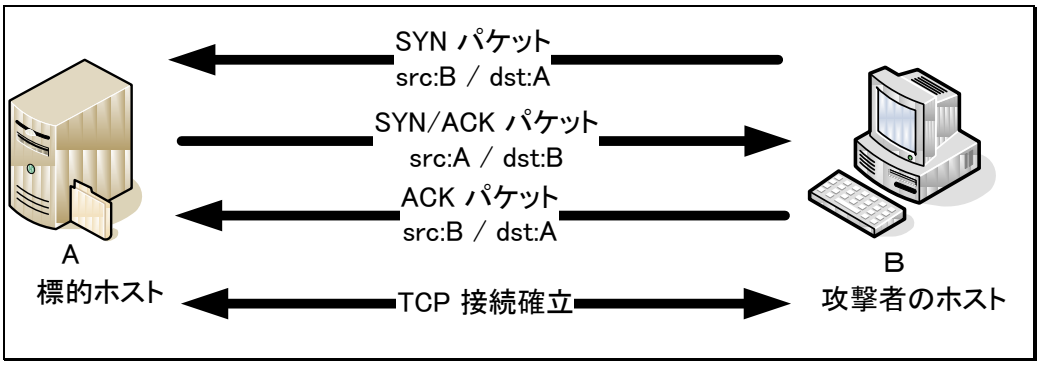


図 4-4 ３ウェイハンドシェイク

最初に送信される SYN パケットが通常の通信であれば、図 4-4 のように 3 ウェイハンドシェイク後に 2 ホスト間で TCP 接続が確立され、データ転送が開始される。そしてデータ転送が完了次第、接続の切断(4 ウェイクローズ)が行われる。しかし、この問題のように送信元の IP アドレスが標的ホスト A の IP アドレスに偽装されている場合、図 4-2 で説明したように標的ホスト A では攻撃者のホスト B 側には SYN/ACK パケットを返送せずに自分自身に対して送信しようとする処理が行われてしまうのである。

この際に利用される送信元と宛先 IP アドレスが同一である不正な SYN パケットは、通常であれば起こり得ないパケットであり、ネットワーク上にデータが流れることはない。自分自身に接続を試みる場合にはこれに該当すると言えるが、この場合自分自身を示すループバックアドレス(IPv4 の場合、127.0.0.1)と呼ばれる仮想的に割り振られた IP アドレスを使用するようになっているため、ネットワーク上には流れずにシステム上で処理されることになる。つまり、送信元 IP アドレスがループバックアドレスに偽装された SYN パケットを処理することでもこの問題と同様の攻撃が可能である。

このように送信元 IP アドレスやポート番号が偽装された、TCP の実装上想定されていない不正な SYN パケットをリモートから受信すると、受信ホストでは正常に処理することができず、これが原因となりサービス不能状態が発生することが考えられる。

4)-4. 発見の経緯とトピック、対策の動き、現在の動向

1997 年にこの問題を発見した m3lt 氏の Bugtraq メーリングリストへの投稿によりからこの脆弱性がインターネット上に公開された。同投稿には Windows 95 に対する攻撃ツール(land.c)が添付されている。このツールは送信元 IP アドレスと宛先 IP アドレスを同一にし、さらに送信元と宛先ポート番号も同一にした SYN パケットにより、数秒間システムのサービス不能(ハングアップ)状態を引き起こすというものである。この頃から自分自身に対してパケットを送り返してサービス不能を引き起こす攻撃のことを「LAND Attack」と呼んでいる。この最初に発見された LAND Attack は CVEID が割り当てられている。(CVE-1999-0016)

この後、幾つかの Exploit コードの更新を経て CERT より Teardrop Attack(注 1)と同時にサービス不能(DoS)攻撃ツールの 1 つとして LAND Attack に対する注意喚起(CA-1977-28)が行われている。影響を受ける製品の多くはこれに伴い、1998 年までにはほとんどのベンダにおいて対処済みの問題としている。また近年において LAND Attack は、ファイアウォールを含む多くのルーティングデバイスや Windows ファイアウォールなどのパーソナルファイアウォールで既知の対処済みの問題として扱われており、簡易的に装備されている DoS 攻撃の保護機能などによって一般的に排除できる攻撃となっている。

しかし、2005 年に入り Microsoft Windows に対して IPv4 および IPv6 サポートのそれぞれにおいて LAND Attack が有効であるという指摘(CAN-2005-0688, CVE-2005-1649)が報告されており、マイクロソフトではセキュリティ情報 MS05-019, MS06-064 を公開しこの脆弱性に対処している。(注 2)

上記 LAND Attack は、送信元 IP アドレスおよび宛先 IP アドレスを同一にし、さらに送信元および宛先ポート番号を同一にした SYN パケットを利用している。2003 年に発見された Windows Media サービス(TCP ポート番 7007,7778)に対する不正な SYN パケットによりサービス不能状態に陥る問題(CVE-2003-0905)が報告されているが、これについては送信元 IP アドレスのみを偽装して利用された特定のサービスに対する LAND Attack の事例の 1 つと言える。

注1：詳細については 22)「フラグメントパケットの再構築時にシステムがクラッシュする問題」 を参照

注 2：詳細については 22)-5 IPv6 環境における影響 を参照

4)-5. IPv6 環境における影響

この問題は TCP プロトコルの問題で、OSI 参照モデルのトランスポート層に属する問題であるため、概念的には IP プロトコルのバージョンに限らずこの問題は再現すると考えられ、TCP/IP の実装次第では IPv6 環境でも影響を受ける可能性がある。

LAND Attack は、2005 年に入り Windows XP および Windows Server 2003 に対しての LAND Attack(CAN-2005-0688)が有効であるという指摘が報告されており、マイクロソフトでは TCP/IPv4 の脆弱性(MS05-019)の 1 つとして対処している。この後、新たに Windows XP および Windows Server 2003、Longhorn の IPv6 における LAND Attack(CAN-2005-0688, CVE-2005-1649)が有効であるという指摘が報告されおり、マイクロソフトでは 2006 年 10 月に TCP/IPv6 の脆弱性(MS06-064)の 1 つとしてこの脆弱性に対処を行っている。

4)-6. 実装ガイド

送信元 IP アドレスおよび宛先 IP アドレスが同一のパケットは処理の対象とせず破棄するアルゴリズムを実装することで本脆弱性を排除することができる。具体的には以下のとおりである。

1. 送信元 IP アドレスおよび宛先 IP アドレスが同一のパケットをネットワーク経由で受信した場合は、そのパケットを破棄する。
2. 通常ネットワーク経由では受信することのない送信元 IP アドレスあるいは宛先 IP アドレスがループバックアドレスのパケットをリモートから受信した場合は、そのパケットを破棄する。

4)-7. 運用ガイド

ベンダよりセキュリティパッチが提供されている場合は、これを適用することで脆弱性を排除することができる。また、ゲートウェイ部分で上記実装ガイドの実装を持つファイアウォール等を使用して不正と判断したパケットをフィルタする。その他の対策を含め、具体的には以下のとおりである。

1. 影響を受ける製品に対して各ベンダより提供されているパッチを適用する。
2. LAND Attack をはじめとする DoS 攻撃を排除する製品(ファイアウォール、DoS 対策製品など)を使用する。
3. ファイアウォール等のネットワークデバイスを使用して送信元 IP アドレスおよび宛先 IP アドレスが同一であるパケット、あるいは環境によっては送信元 IP アドレスおよび宛先 IP アドレスが同一となり得る以下のようなパケットをフィルタする。
   (1)ループバックアドレス(127.0.0.1)
   (2)プライベート IP アドレス(外部からのトラフィックを扱うファイアウォールの場合)
   (3)利用する自らのグローバル IP アドレス(NAT 環境下ではない場合 など)

4)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1981 年 RFC 793, TRANSMISSION CONTROL PROTOCOL.
http://www.ietf.org/rfc/rfc0793.txt

1985 年 The LAND Attack(IPDOS)【m3lt 著】
http://www.insecure.org/sploits/land.ip.DOS.html
DoS 攻撃ツールとして land.c が公開される。
SecurityFocus 2666
http://www.securityfocus.com/bid/2666
http://downloads.securityfocus.com/vulnerabilities/exploits/land.c
Windows95 Stops Responding Because of LAND Attack
http://support.microsoft.com/kb/177539/en-us
Windows NT 4.0 で"LAND Attack"により、Windows NT の速度が遅くなる:
http://support.microsoft.com/kb/165005/ja
CERT Advisory CA-1997-28
http://www.cert.org/advisories/CA-1997-28.html
http://www.lac.co.jp/business/sns/intelligence/cert_advisory/CA-97_28.html

1997 年 Novell TID-2932511 TCP Loopback Denial-of-Service Attack
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2932511.htm

1998 年 Sun Patch Document 102010-06
http://sunsolve.sun.com/search/document.do?assetkey=102010-06
http://sunsolve.sun.com/search/document.do?assetkey=102517-05
FreeBSD advisory FreeBSD-SA-98:01
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/old/FreeBSD-SA-98:01.land.asc
HP Security Bulletin HPSBUX9801-076
http://pintday.org/advisories/vendor/hp/hpsbux9801-076.html
ISS X-Force Database land(288)
http://xforce.iss.net/xforce/xfdb/288
Cisco Security Advisory: TCP Loopback DoS Attack(land.c)and Cisco Devices
http://www.cisco.com/warp/public/770/land-pub.shtml

ISS X-Force Database cisco-land(1246)
http://xforce.iss.net/xforce/xfdb/1246

1999 年　Common Vulnerabilities and Exposures CVE-1999-0016
http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0016

2000 年　Snort.org Signature Database SID1:269
http://www.snort.org/pub-bin/sigs.cgi?sid=1-269
ISS X-Force Database land-patch(689)
http://xforce.iss.net/xforce/xfdb/689
ISS X-Force Database ver-tcpip-sys(911)
http://xforce.iss.net/xforce/xfdb/911

2003 年　Common Vulnerabilities and Exposures CVE-2003-0905
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2003-0905

2004 年　SecurityFocus 9825
http://www.securityfocus.com/bid/9825
Snort.org Signature Database SID 1:527
http://www.snort.org/pub-bin/sigs.cgi?sid=527
マイクロソフトセキュリティ情報 MS04-008
http://www.microsoft.com/japan/technet/security/bulletin/MS04-008.mspx

2005 年　Windows Server 2003 and XP SP2 LAND Attack vulnerability【Dejan Levaja 著】
http://www.securityfocus.com/archive/1/392354
http://www.securityfocus.com/data/vulnerabilities/exploits/r57windos.c
Common Vulnerabilities and Exposures CVE-2005-0688
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2005-0688
ISSX-Force Database win-server-xp-land-dos(19593)
http://xforce.iss.net/xforce/xfdb/19593
マイクロソフトセキュリティ情報　MS05-019
http://www.microsoft.com/japan/technet/security/Bulletin/MS05-019.mspx
JP Vendor Status Notes JVNTA05-102A
http://jvn.jp/cert/JVNTA05-102A/index.html

IPA セキュリティセンター 20050413-ms05-019
http://www.ipa.go.jp/security/ciadr/vul/20050413-ms05-019.html

Windows(XP, 2k3, Longhorn)is vulnerable to IpV6 Land attack.【Konrad Malewski 著】
http://www.securityfocus.com/archive/1/400188
※Windows XP/2003/Longhorn の最新バージョンにおいて IPv6 環境における LAND Attack が可能であることを指摘
SecurityFocus 13658
http://www.securityfocus.com/bid/13658
Common Vulnerabilities and Exposures CVE-2005-1649
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2005-1649
ISS X-Force Database win-server-xp-ipv6-land-dos(20629)
http://xforce.iss.net/xforce/xfdb/20629
ISS X-Force Database motorola-sb5100e-land-dos(23589)
http://xforce.iss.net/xforce/xfdb/2358

2006 年 マイクロソフトセキュリティ情報 MS06-064
http://www.microsoft.com/japan/technet/security/Bulletin/MS05-019.mspx

5). データを上書きするフラグメントパケットがフィルタリングをすり抜ける問題 (Overlapping Fragment Attack)

5)-1. 分類:TCP 【IPv4】【IPv6】

5)-2. 概要

TCP ヘッダ情報を利用するフィルタリングが実施されている場合、TCP ヘッダ情報が重複する 2 つのフラグメントパケットを受信すると、本来フィルタを通過できない TCP ヘッダ情報が上書きされ、結果としてフィルタリングを回避して通信が行われる。

5)-3. 解説

攻撃手法とその影響

攻撃者は、重複する TCP ヘッダデータ持つ 2 つのフラグメントパケットを用意し、TCP ヘッダによるフィルタリングを実施している標的ホストに対して送信することで問題を悪用する。ここで、図 5-1 に TCP ヘッダの制御フラグをチェックし TCP 接続要求(SYN=1,ACK=0)パケットを破棄するフィルタリング機器 C がホスト A の前に設置されていることを想定した構成を示す。

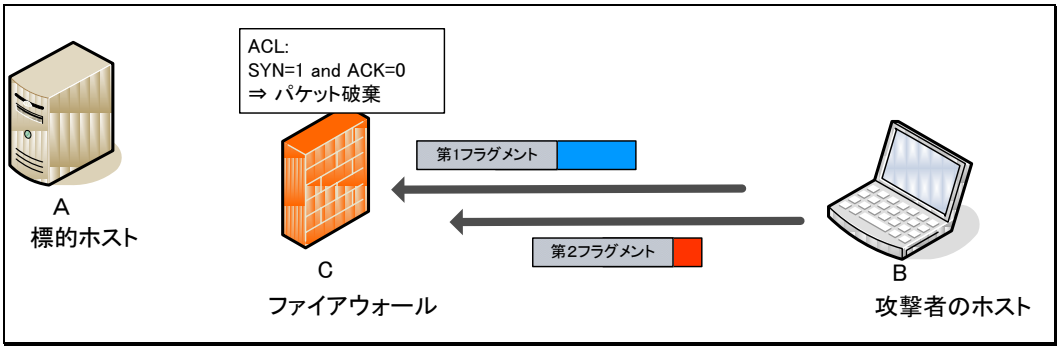


図 5-1 想定されるフラグメントフィルタとネットワーク構成

このフィルタリングを回避するために攻撃者により送信されるフラグメントパケット(第 1 フラグメント、第 2 フラグメント)を 図 5-2 にそれぞれ示す。

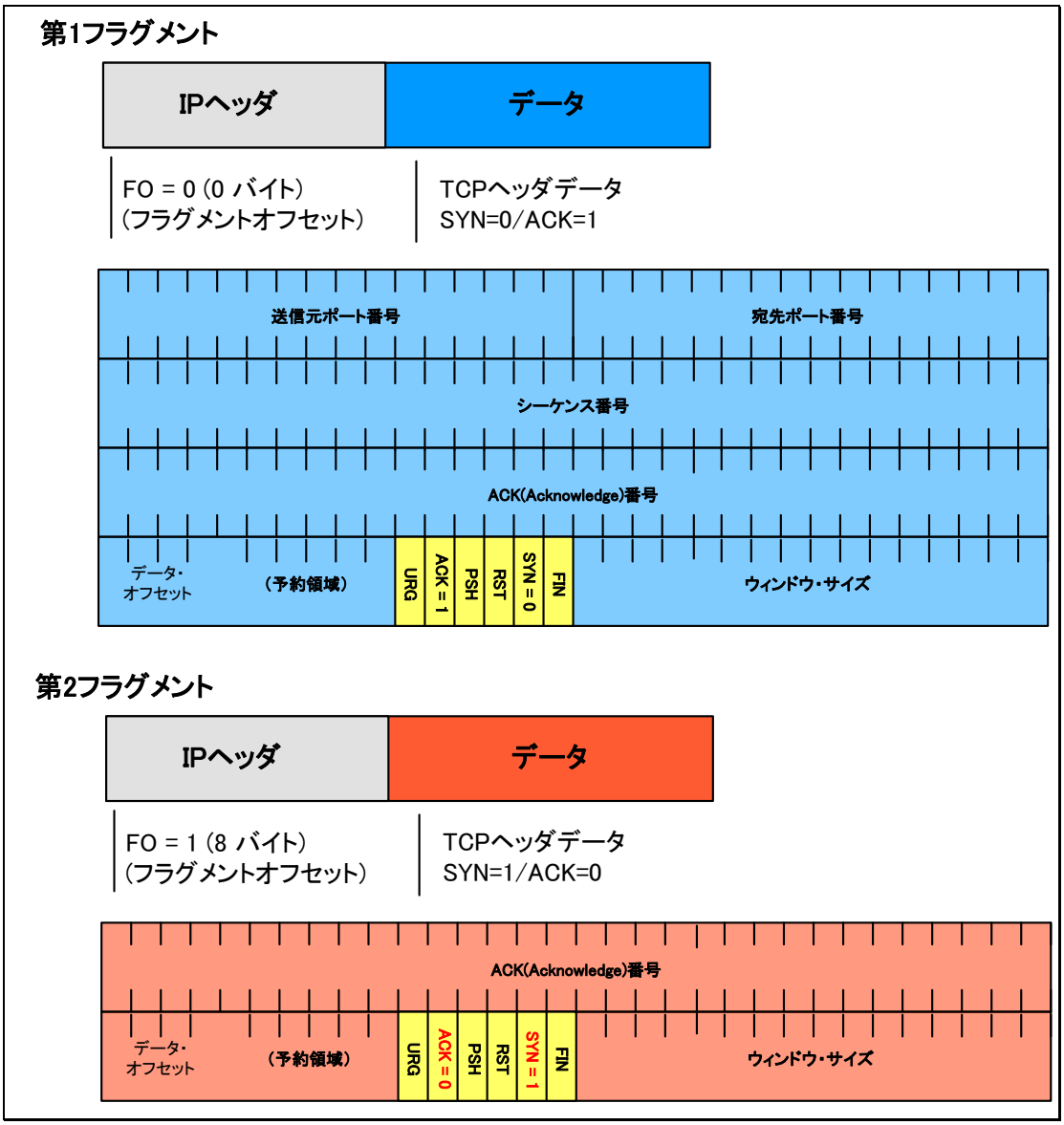


図 5-2 送信される第 1 フラグメントと第 2 フラグメント

これらのフラグメントパケットがホスト B よりホスト A に対して送信されると、ホスト A にパケットが到達する前にフィルタリング機器 C でチェックが行われる。このフィルタリング機器 C において第 1 フラグメント(FO=0)に対してのみチェックを行う実装が行われている場合、制御フラグが通過のルールに適合している第 1 フラグメントだけではなく、ルールに適合しない第 2 フラグメントもこのフィルタを通過する。

一方、受信側ホストではフラグメントパケットは分割する前のデータに再構築が行なわれる。この再構築時におけるアルゴリズムを提示する RFC 791/815 では、先に到着したフラグメントパケットのデータと後に到着したフラグメントパケットのデータで、完全にあるいは部分的に重複するデータが存在する場合は、後に到着したフラグメントパケットのデータで上書きを行うことが認められている。

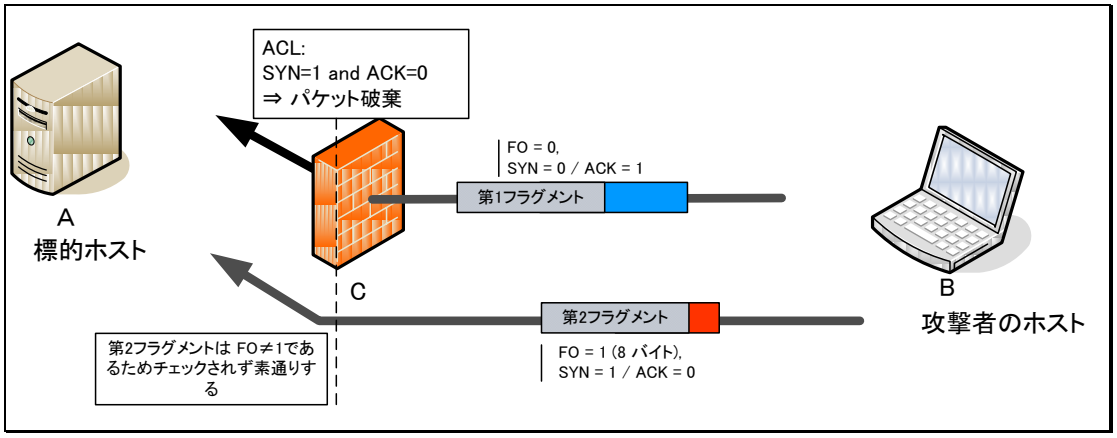


図 5-3 フィルタリングを通過する第 1 フラグメントと第 2 フラグメント

上述の第 2 フラグメントではフラグメントオフセット(FO)は 8 バイト(FO=1)が指定されているため、第 1 フラグメントにおける TCP ヘッダの先頭から 8 バイト目以降、つまり制御フラグに相当するデータ部分において重複していることになる。

そのため、フィルタリングを回避した 2 つのフラグメントパケットが、第 1 フラグメント、第 2 フラグメントの順でホスト A に到達した場合、ホスト A における再構築処理により第 2 フラグメントのデータで制御フラグデータが上書きされる。この際に再構築された TCP ヘッダを 図 5-4 に示す。つまり、最終的には TCP 接続要求パケットのデータ(SYN=1,ACK=0)として再構築され、TCP に処理が渡される。

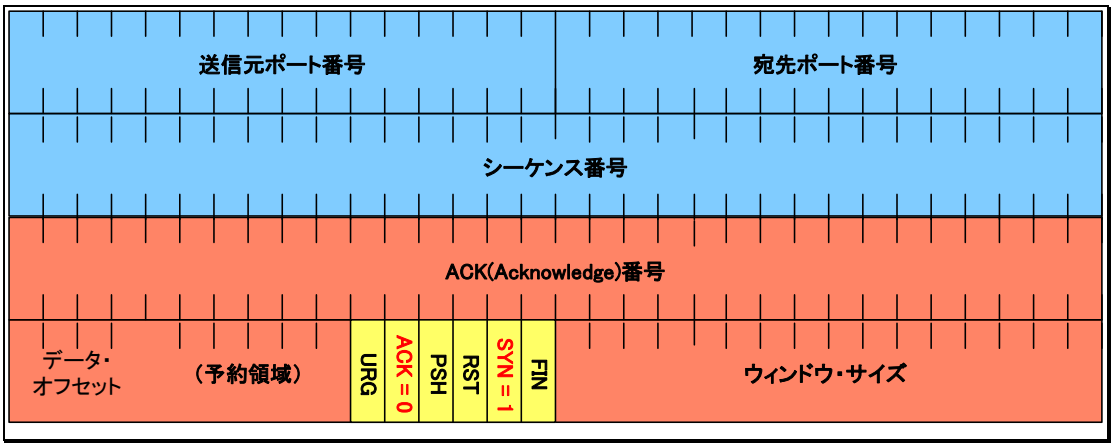


図 5-4 ホスト A 上で再構築された TCP ヘッダ

その結果、本来フィルタを通過できないはずの TCP 接続要求パケットを送信することが可能となり、フィルタリングされるべき通信が行われてしまう。

原因と考察

ネットワーク上にデータを転送するとき、ネットワークによって決められている最大伝送単位(MTU)を超えるような IP パケットは、複数の小さな IP パケットにフラグメント(分割)されて送信される。これが IP フラグメンテーション(IP の断片化)と呼ばれる機能である。Overlapping Fragment Attack は、この IP フラグメンテーション機能に関連し、フラグメントパケットのフィルタリングの実装と、受信側でのフラグメントパケットの再構築アルゴリズムにおけるデータの上書き処理に起因して発生する。

まず、一部のフラグメントフィルタリングではパケット情報の先頭にあるヘッダを元にフィルタリングを行うため、FO=0 に指定された最初のフラグメントのみチェックを行い、FO が 0 以外のフラグメントに対してはチェックしない方法が実装されているケースがある。これは、最初のフラグメントさえフィルタで破棄してしまえば、仮に以降のフラグメントパケットがフィルタを通過したとしても、IP データグラムとして成立せず破棄されるという点に基づいている。

次に、フラグメントパケットの再構築アルゴリズムを記載する RFC 791/815 では、フラグメントパケットの再構築を行う際データの上書きが認められており、複数のフラグメント間で重複するデータがあった場合には後に到着したフラグメントのデータで上書きが行われる。

この 2 つの事象が合わせて悪用された場合、フィルタリングを通過した第 1 フラグメントにおける無害なデータを、チェックが行なわれずにフィルタリングを通過した第 2 フラグメントの不正なデータで上書き可能となる。結果として TCP ヘッダデータを利用するフィルタリングを無効化して通信されてしまう。

原因の 1 つである再構築アルゴリズムに関して、後に到着したフラグメントのデータで上書きの処理を行なわないアルゴリズムを実装することを要求する標準はない。後に到着したフラグメントのデータで上書きしないような再構築アルゴリズムを実装した場合でも、意図的にフラグメントパケットの送信順番を入れ替えることで同様の攻撃を行うことが可能である。

また RFC 3128 では、Tiny Fragment Attack と Overlapping Fragment Attack を組み合わせた Tiny Overlapping Fragment Attack を悪用することで、RFC 1858 で推奨されているアルゴリズムを実装したフィルタリングを回避可能であることが報告されている。(注1)

注1 : 詳細については 6)「十分に小さいフラグメントパケットがフィルタリングをすり抜ける問題」 を参照

5)-4. 発見の経緯とトピック、対策の動き、現在の動向

この攻撃手法は 1995 年 5 月にファイアウォールメーリングリスト上での Darren Reed 氏 、Tom Fitzgerald 氏、Paul Traina 氏らの議論から発展した。そして、1995 年 10 月に示された RFC 1858 では、「IP フラグメントフィルタリングについてのセキュリティ上の考察」と題して、Tiny Fragment Attack と Overlapping Fragment Attack についての攻撃手法と、その対策として「直接的手法」と「間接的手法」の 2 つが提示された。

その後 2001 年 6 月、RFC 1858 の中で対策として提示された「間接的手法」を回避する手法が RFC 3128(Tiny Fragment Attack の変形に対する防護)で示された。この手法は前述した 2 つの攻撃手法を組み合わせた Tiny Overlapping Fragment Attack と呼ばれる攻撃手法である。 「間接的手法」による対策は、この攻撃手法に対しては不完全であり、フィルタリングが回避されてしまうため、「直接的手法」および「間接的手法」を組み合わせた対策が必要であることが示された。

これらの攻撃が可能であるかどうかは各ベンダや開発者によるパケットフィルタリングの実装方法に依存するが、近年における一般的なルータやファイアウォール製品では既知の脆弱性としての対処済みであり、影響を受けることはない。

5)-5. IPv6 環境における影響

この問題は、フィルタリング機器におけるフラグメントパケットのフィルタリングの実装方法の問題とパケット再構築アルゴリズムを悪用した攻撃である。RFC2460 に規定されているとおり、IPv6 には IPv6 拡張ヘッダとしてとしてフラグメントヘッダ(次ヘッダ値:44)が存在し、IPv6 においてもフラグメント化が許可されている。(図 5-5 にフラグメントヘッダの形式を示す。)

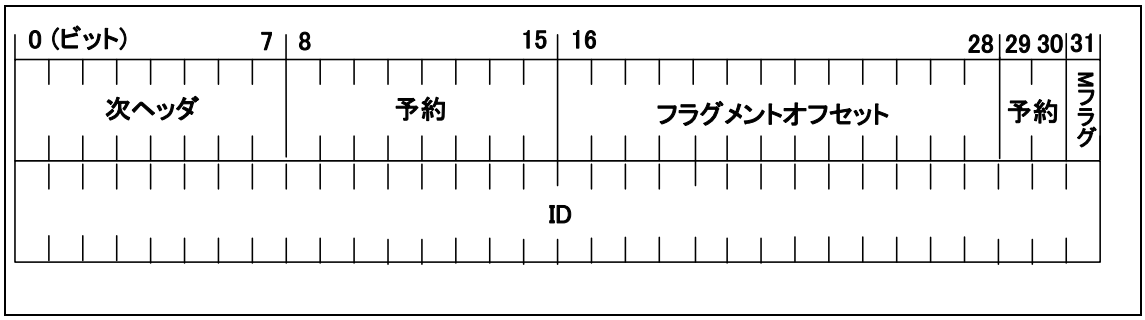


図 5-5 IPv6 フラグメントヘッダ

この IPv6 フラグメントヘッダには分割されたパケットを再構築するために必要な情報が含まれている。IPv6 におけるフラグメントの再構築は、IPv4 と異なる部分（注 2)もあるが、再構築するための情報には同じフィールド値を使用している。また、RFC2460 には現時点でフラグメント再構築時のデータ上書き等に関する制限もなく、v6ops メーリングリストの投稿で Overlapping Fragment を禁止するようにフラグメントの重複は禁止すべきとの指摘も行われている。

多くのベンダでこの問題は既知の問題として対処されているため、現在においては IPv6 でも対策済みであると考えられるが、IPv4 に類似する IPv6 フラグメントパケットのフィルタリングの実装に問題が存在する場合には、フィルタリングを通過されて通信が行われてしまう可能性がある。

また、Internet-Draft 版ではあるが 2007 年 7 月時点で IPv6 フラグメントに関する規定「Operational issues with Tiny Fragments in IPv6(IPv6 の Tiny Fragment の操作上の問題)」と「IPv6 Fragments and treatment of Tiny fragments(IPv6 Fragment と IPv6 Tiny Fragment の扱いについて)が公開されており、IPv6 においてもフラグメントの扱いに関してセキュリティの配慮が十分に必要である。

注 2: IPv6 のフラグメント化は送信元ノードだけで実行される。IPv4 のようにパケットの配送を行うルータでは実行されない。IPv6 におけるフラグメントの再構成についての詳細な手順および処理については RFC2460(セクション 4.5)を参照のこと

5)-6. 実装ガイド

RFC 3128 に提示されるフラグメントパケットフィルタリングにおけるアルゴリズムを実装することで、Overlapping Fragment Attack のみならず、Tiny Fragment Attack および Tiny Overlapping Fragment Attack によりパケットフィルタリングを回避して通信が行なわれることを防ぐことができる。また、フィルタリング機器でフラグメントパケットを実際に再構築しチェックを行う機能の実装についても、これらの攻撃に対して有効である。

1. フィルタリング機器において、RFC 3128 で提示される以下の 2 つのアルゴリズムを実装する。
   (1) FO=0、かつプロトコルが TCP、かつトランスポートヘッダの長さが指定した最小トランスポートヘッダ長(TMIN)以下であれば、そのパケットを破棄する。
   (2) FO=1、かつプロトコルが TCP であれば、そのパケットを破棄する。
2. フィルタリング機器において、フラグメントパケットを実際に再構築してパケットのチェックを行う。

5)-7. 運用ガイド

ベンダよりセキュリティパッチが提供されている場合には、これを適用することが推奨される。また、近年におけるほとんどの製品において対処済みであるため、新しい製品を導入することで本脆弱性を排除することができる。

1. 影響を受ける製品を使用している場合は各ベンダより提供されているパッチを適用する。
2. 使用している製品において、本脆弱性をチェックする機能が付属されている場合はその機能を有効にする。
3. 本脆弱性に対処済みであるファイアウォール等のフィルタリング機器を導入する。

5)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1981 年 RFC 791, Internet Protocol.
http://www.ietf.org/rfc/rfc0791.txt

1982 年 RFC 815, IP DATAGRAM REASSEMBLY ALGORITHMS.
http://www.ietf.org/rfc/rfc0815.txt

1992 年 【自動翻訳】アクセス コントロール リスト(ACL)と IP フラグメント
http://www.cisco.com/support/ja/105/acl_wp.shtml

【データを上書きするフラグメントパケットがフィルタリングをすり抜ける問題(Overlapping Fragment Attack)】

1995 年　RFC 1858, Security Considerations for IP Fragment Filtering.
http://www.ietf.org/rfc/rfc1858.txt
http://www.ipa.go.jp/security/rfc/RFC1858JA.html

1998 年　RFC2460, Internet Protocol, Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2460.txt

2001 年　RFC 3128, Protection Against a Variant of the Tiny Fragment Attack.
http://www.ietf.org/rfc/rfc3128.txt
http://www.ipa.go.jp/security/rfc/RFC3128JA.html

2004 年　IPv6 Fragment Overlap not Forbidden
http://www.ops.ietf.org/lists/v6ops/v6ops.2004/msg01497.html
ipv6-fragment-overlap(15527)
http://xforce.iss.net/xforce/xfdb/15527

2006 年　Internet-Draft, Operational issues with Tiny Fragments in IPv6
http://tools.ietf.org/id/draft-manral-v6ops-tiny-fragments-issues-02.txt

2007 年　Internet-Draft, IPv6 Fragments and treatment of Tiny fragments
http://tools.ietf.org/id/draft-manral-ipv6-fragments-00.txt

6). 十分に小さい分割パケットがフィルタリングをすり抜ける問題 (Tiny Fragment Attack、Tiny Overlapping Fragment Attack)

6)-1. 分類:TCP 【IPv4】【IPv6】

6)-2. 概要

第 1 フラグメントパケット(FO=0)の TCP パケットを 8 オクテットにフラグメントして送信することにより、制御フラグが第 2 フラグメントパケット(FO=1)に含まれるので、第 1 フラグメントパケットだけでフィルタリングしている場合、このパケットを破棄することができない。

6)-3. 解説

攻撃手法とその影響

攻撃者は意図的に TCP ヘッダ長を最小フラグメントサイズである 8 バイトにパケットをフラグメントさせた TCP 接続要求(SYN=1 と ACK=0 をもつ TCP セグメント)を送信する。その結果、 第 1 フラグメントパケットには送信元ポート番号・宛先ポート番号・シーケンス番号だけしか TCP ヘッダ情報が入らないフラグメントパケット(図 6-1 緑色部分に示す)になる。また、確認応答番号(Acknowledgement Number)以降の TCP ヘッダ情報については第 2 フラグメントパケット(FO=1)に含まれることになる。つまり、TCP の制御フラグは第 2 フラグメントパケットに含まれることになる(図 6-1 黄色部分に示す)。

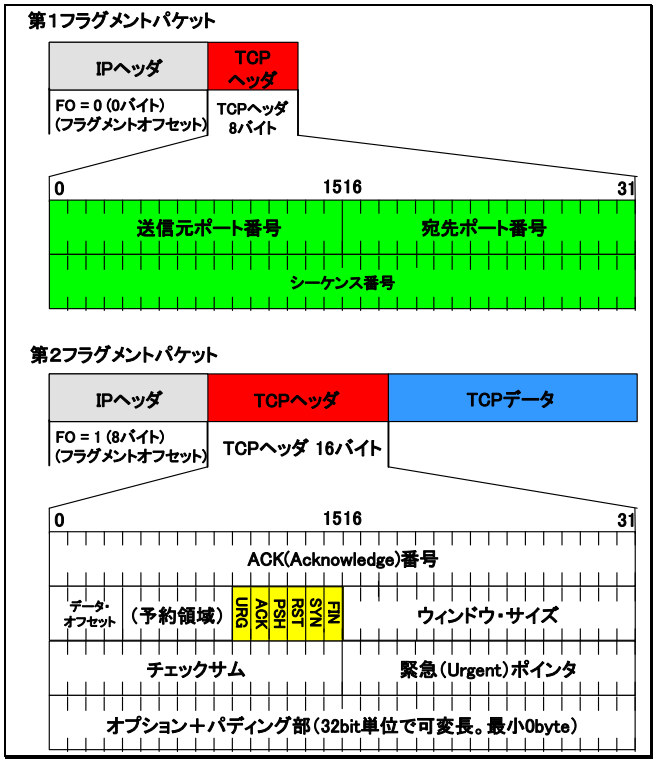


図 6-1 フラグメントパケット

このとき、フィルタリングをすり抜ける様子を 図 6-2 に示す。攻撃対象の前に設置されているパケットフィルタリング機能が第1フラグメントパケット(FO=0)しかチェックしない実装である場合、TCP 接続要求を拒否するフィルタリングをすり抜けることが可能となり、フィルタリングが無効になる。

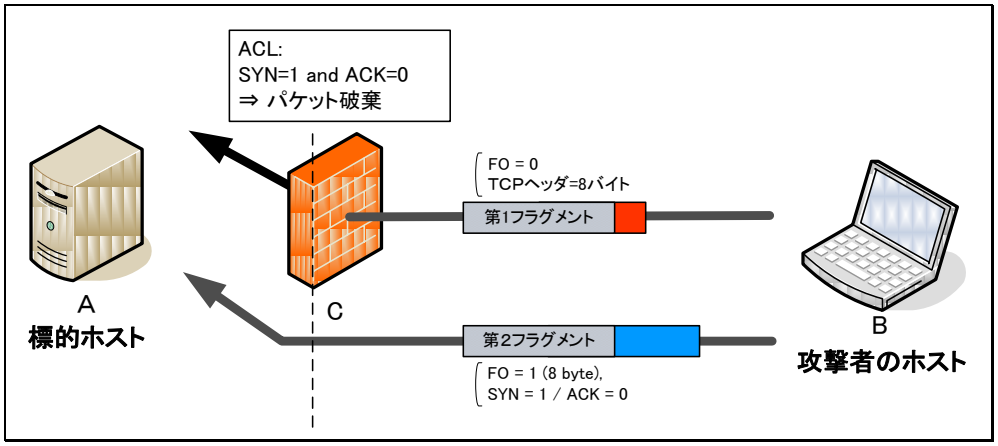


図 6-2 Tiny Fragment Attack

さらに Tiny Fragment Attack と Overlapping Fragment Attack(注1)を組み合わせた Tiny Overlapping Fragment Attack と呼ばれる攻撃手法がある。パケットフィルタリングの設定で宛先ホストに対してインバウンドでの接続を許可しており、かつ同一ホストに対してアウトバウンドでの接続のみを許可する他のポートが存在する場合、この攻撃手法が用いられると、そのアウトバウンド接続のみのポートに対してインバウンドでの接続を許可してしまうことになる。この攻撃手法が有効となる ACL の例を 表 6-1 に示す。

表 6-1 想定される ACL

No	Action	Source Port	Dest. Port	Flags	Purpose
1	Permit	>1023	SMTP	ANY	インバウンドのSMTP
2	Permit	>1023	ANY	Ack=1	FTP データ転送用 (アクティブモード)
3	Deny	ANY	ANY	ANY	破棄

注1 : 詳細については 5)「データを上書きするフラグメントパケットがフィルタリングをすり抜ける問題」 を参照

【十分に小さい分割パケットがフィルタリングをすり抜ける問題(Tiny Fragment Attack Tiny Overlapping Fragment Attack)】

攻撃者は以下の 3 つのフラグメントされたパケットを作成する。

1. フラグメント 1:(フラグメントオフセット=0、length>=16)
   TCP ヘッダの中に制御フラグが含まれている通常のフラグメントパケットである。宛先ホストに 対して、TCP 接続要求(SYN=1 と ACK=0 をもつ TCP セグメント)が許可されているポートに接続するパケットであり、パケットフィルタリングを通過する。

2. フラグメント 2:(フラグメントオフセット=0、length=8)
   TCP ヘッダには送信元ポート番号・宛先ポート番号・シーケンス番号しか含まれないフラグメントパケットであるため、パケットフィルタリングを通過してしまう(Tiny Fragment Attack)。さらにフラグメントオフセット値が 0 のため、パケット再構築時にフラグメント 1 の TCP ヘッダの送信元 ポート番号・宛先ポート番号・シーケンス番号を上書きしてしまう(Overlapping Fragment Attack)。つまり、インバウンドでの TCP 接続要求を許可しないポート番号でもパケットフィルタリングを素通りして接続が可能となる。

3. フラグメント 3:(フラグメントオフセット>=2、length=残りのパケット)
   フラグメントされた残りのパケットを送信して、パケットを完成させる。

具体的な攻撃例としては、まず 表 6-1 の想定される ACL に対して、フラグメント 1 として SMTP に TCP 接続要求パケットを送信する。次にフラグメント 2 の宛先ポート番号を TELNET(23/tcp)にして送信する。これはすべてのフィールドが FTP パケットの開始である可能性があるのでルール 2 を通過する。そして、残りのフラグメント 3 以降のフラグメントパケットは通常通りに通過する。結果として、宛先ホストでパケットが再構築されると、TELNET(23/tcp)への TCP 接続要求になってしまい、ACL で許可していない通信が可能となる。

【十分に小さい分割パケットがフィルタリングをすり抜ける問題(Tiny Fragment Attack Tiny Overlapping Fragment Attack)】

原因と考察

IP パケットの最大サイズは 64k バイト(65536 バイト)だが、実際にはこのような大きなサイズのパケットを 1 つのパケット(フレーム)として送信することができる物理ネットワーク媒体は存在しない。例えば、イーサネットでは 1500 バイト、FDDI(光ファイバ)では 4352 バイトが MTU(Maximum Transmission Unit)値として定められている。この値は物理ネットワーク媒体ごとに固有である。この値以上に大きいパケットは MTU 値ごとに分割して送信する。これが IP フラグメンテーション(IP の断片化)と呼ばれる機能である。分割された各フラグメントは、ヘッダ部(通常 20 バイト)とデータ部(可変長)からなり、データ部には TCP パケットや UDP パケットが入る。

Tiny Fragment Attack では故意にパケットを非常に小さなフラグメントに分割する。例えば、TCP パケットのヘッダ(通常 20 バイト)を 2 つのフラグメントに分割する。第1フラグメントパケットのサイズを 28 バイトにすると、20 バイトの IP ヘッダと TCP ヘッダの先頭 8 バイト(送信元ポート番号・宛先ポート番号・シーケンス番号)のみ入り、TCP ヘッダの残りの部分(SYN や ACK などの制御フラグなど)は第 2 フラグメントパケットに入る。

しかし、使用しているパケットフィルタリング機能が分割されたフラグメントのうち、第1フラグメントパケットしかチェックしない実装の場合、第 1 フラグメントパケットには SYN や ACK などの制御フラグが含まれていないためにフィルタを通過し、第 2 フラグメントパケットにある制御フラグはフィルタによるチェックなしで素通りする。

6)-4. 発見の経緯とトピック、対策の動き、現在の動向

この攻撃手法は 1995 年 5 月にファイアウォールメーリングリスト上での Darren Reed 氏 、Tom Fitzgerald 氏、Paul Traina 氏らの議論から発展して考えられた。その結果、 1995 年 10 月に「IP フラグメントフィルタリングについてのセキュリティ上の考察」と題して、Tiny Fragment Attack と Overlapping Fragment Attack についての攻撃手法ならびにその対策が RFC 1858 として示された。

その後、2001 年 6 月になって、RFC 1858 の中で対策として提示された「間接的手法」を回避する攻撃手法について RFC 3128(Tiny Fragment Attack の変形に対する防護)で示された。この手法は Tiny Fragment Attack と Overlapping Fragment Attack を組み合わせた Tiny Overlapping Fragment Attack と呼ばれる攻撃手法である。この攻撃手法が用いられた場合、「間接的手法」のみの対策では不完全であり、脆弱性を保持したままになる。そのため、「直接的手法」と「間接的手法」を組み合わせた対策が必要であることを示した。

これらの問題点は各ベンダや開発者によるパケットフィルタリングの実装方法に依存するが、近年においては既知の対処済みの問題として扱われており、ほとんどの一般的なルータやファイアウォール製品では影響を受けることはない。

6)-5. IPv6 環境における影響

この問題は Overlapping Fragment Attack と同様にフラグメントパケットのフィルタリングの実装方法における問題とパケット再構築アルゴリズムを利用した攻撃である。概念的には IPv6 でも再現すると考えられ、IPv6 環境でも影響を受ける可能性がある。既に多くのベンダでこの問題に対する対処が行われているため、現在においては IPv6 でも対策済みであると考えられるが、依然として IPv6 フラグメントパケットのフィルタリングの実装に問題が存在する場合にはフィルタを通過されてしまい、通信が行われてしまう可能性がある。

2007 年 7 月現時点で Internet-Draft 版であるが IPv6 Tiny Fragment に関する規定「Operational issues with Tiny Fragments in IPv6(IPv6 の Tiny Fragment の操作上の問題)」と「IPv6 Fragments and treatment of Tiny fragments(IPv6 Fragment と IPv6 Tiny Fragment の扱いについて)が公開されており、依然として IPv4 と同様に第1フラグメントパケットしかチェックしない実装の場合、第2フラグメントパケット以降のチェックを回避可能されてしまうとの記述もあり、IPv4と同様に十分なフラグメントパケットへの配慮が必要とされている。

6)-6. 実装ガイド

RFC 3128 に提示されるフラグメントパケットフィルタリングにおけるアルゴリズムを実装することで、Tiny Fragment Attack および Tiny Overlapping Fragment Attack のみならず、Overlapping Fragment Attack によりパケットフィルタリングを回避して通信が行なわれることを防ぐことができる。また、フィルタリング機器でフラグメントパケットを実際に再構築しチェックを行う機能の実装についても、これらの攻撃に対して有効である。

1. RFC 3128 で提示されている対策通りにフラグメントされたパケットをパケットフィルタリングにて処理する場合は以下の 2 つのアルゴリズムを実装する。
   (1) フラグメントオフセット値が 0、かつプロトコルが TCP、かつトランスポートヘッダの長さが指定した最小トランスポートヘッダ長(TMIN)以下であれば、そのパケットを破棄する。
   (2) フラグメントオフセット値が 1、かつプロトコルが TCP であれば、そのパケットを破棄する。
2. パケットフィルタリング機能を提供するデバイス上において、フラグメントされたパケットを実際に再構築して該当するパケットが問題ないかチェックする機能を実装する。

6)-7. 運用ガイド

ベンダよりセキュリティパッチが提供されている場合は、これを適用することが推奨される。また、近年におけるほとんどの製品において対処済みであるため、新しい製品を導入することで本脆弱性を排除することができる。

1. 影響を受ける製品を使用している場合は各ベンダより提供されているパッチを適用して、脆弱性を排除する。
2. 使用している製品において、本脆弱性をチェックする機能が付属されている場合はその機能を有効にする。
3. 現在、使用している製品に本脆弱性の存在が確認されているが、ベンダでのパッチ配布などのサポートがない場合、該当製品の手前に本脆弱性を排除する機器を導入する、もしくは新しい製品を購入する。

6)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1981 年 RFC 791, Internet Protocol.
http://www.ietf.org/rfc/rfc0791.txt

1992 年 【自動翻訳】アクセス コントロール リスト(ACL)と IP フラグメント
http://www.cisco.com/support/ja/105/acl_wp.shtml

1995 年 RFC 1858, Security Considerations for IP Fragment Filtering.
http://www.ietf.org/rfc/rfc1858.txt
http://www.ipa.go.jp/security/rfc/RFC1858JA.html

1999 年 Common Vulnerabilities and Exposures CVE-1999-0588
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0588

2001 年 RFC 3128, Protection Against a Variant of the Tiny Fragment Attack.
http://www.ietf.org/rfc/rfc3128.txt
http://www.ipa.go.jp/security/rfc/RFC3128JA.html

2004 年 RFC2460, Internet Protocol, Version 6(IPv6)Specification
http://www.ietf.org/rfc/rfc2460.txt

2006 年 Internet-Draft, Operational issues with Tiny Fragments in IPv6
http://tools.ietf.org/id/draft-manral-v6ops-tiny-fragments-issues-02.txt

2007 年 Internet-Draft, IPv6 Fragments and treatment of Tiny fragments
http://tools.ietf.org/id/draft-manral-ipv6-fragments-00.txt

7). PAWS 機能の内部タイマを不正に更新することで、TCP 通信が強制的に切断される問題

7)-1. 分類:TCP 【IPv4】【IPv6】

7)-2. 概要

PAWS(Protect Against Wrapped sequence numbers)機能を利用した TCP 通信中に、PAWS 機能の内部タイマを意図的に更新するようなパケットを TCP 通信中のホストに送信すると、PAWS 機能により TCP 通信が強制的に切断されてしまう。

7)-3. 解説

攻撃手法とその影響

PAWS 機能の内部タイマを意図的に更新するようなパケットを TCP 通信中のホストに送信すると、TCP 通信を強制的に切断できる。なおこの問題を利用するためには、対象となる TCP 通信の送信元の IP アドレスとポート番号、送信先の IP アドレスとポート番号を入手する必要がある。

この問題を利用した攻撃の流れを①～④で解説する。なお、①～④の TCP 通信は、PAWS 機能が有効になっていることを前提とする。

① TCP 通信を盗聴する

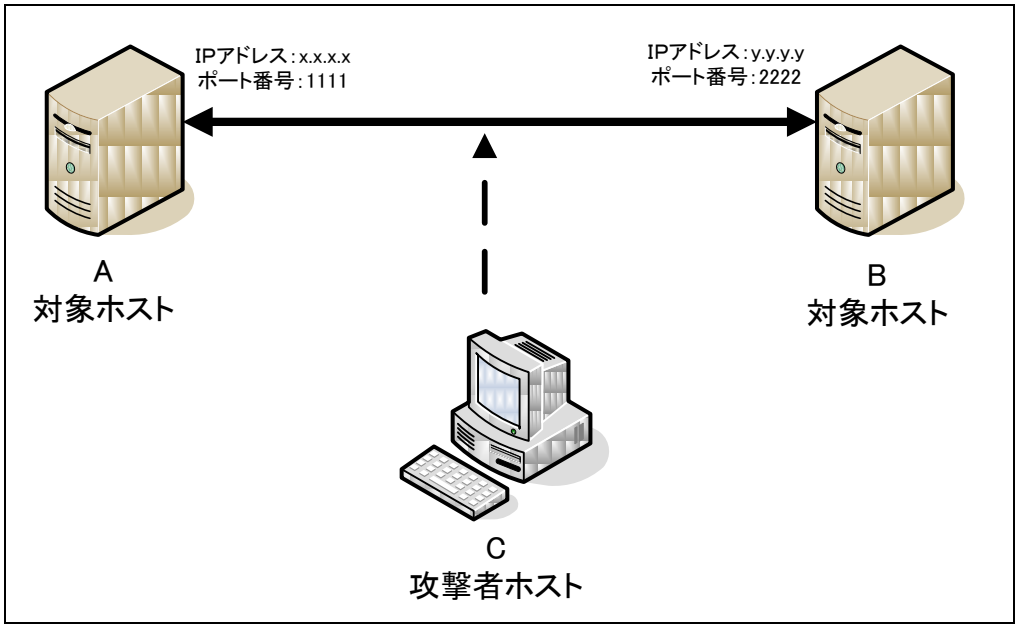


図 7-1 TCP 通信の盗聴

攻撃者は対象となる TCP 通信を盗聴し、送信元の IP アドレスとポート番号、送信先の IP アドレスとポート番号を入手する。図 7-1 では対象ホスト A、対象ホスト B 間の TCP 通信におけるそれらの情報を攻撃者ホスト C が入手すると仮定している。

② 偽装パケットを送信する

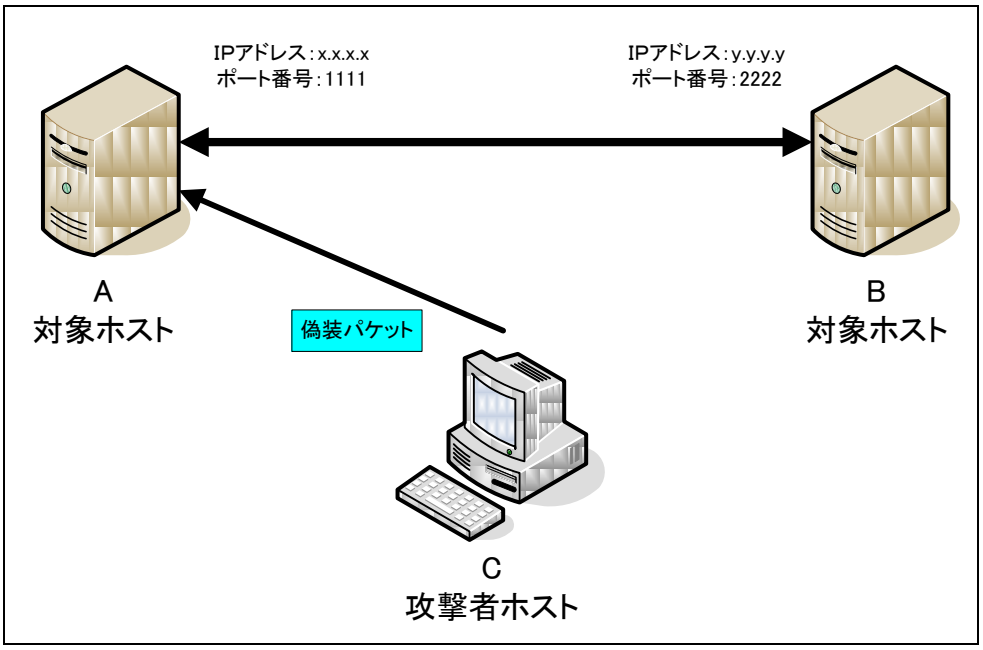


図 7-2 偽装パケットの送信

攻撃者が①で入手した情報を利用して、シーケンス番号(注 1)、Timestamps オプション値(注 2)に特定の値を設定したパケットを生成する。そのパケットを対象ホスト A に送信する。図 7-2 で送信する偽装パケットの TCP ヘッダ情報を表 7-1 で定義する。なお、攻撃者ホスト C が偽装パケットを送信した時の対象ホスト A の内部タイマを 10 とする。

表 7-1 TCP ヘッダ設定情報

TCP ヘッダ情報	設定値
送信先 IP アドレス	x.x.x.x
送信先ポート番号	1111
送信元 IP アドレス	y.y.y.y
送信元ポート番号	2222
シーケンス番号	①で盗聴した TCP 通信における、最新でないシーケンス番号とする。この例では、TCP 通信のシーケンス番号として、100、200、300 が送信されたものとし、300 より小さい 100 を設定する
Timestamps オプション値	可能な限り大きな値を設定する。この例では、内部タイマ 10 に対して極端に大きな値 10000 を設定する

注1：現在送信済みであるバイト数を表す数値である。TCP ヘッダに 32 ビットの領域が確保されている。TCP 通信においては、シーケンス番号と確認応答番号により、パケットが送信先ホストに到達したことを判断する

注 2：TCP ヘッダのオプション情報の一つである。詳細については、【原因と考察】を参照のこと

③ 偽装パケットにより、PAWS 機能の内部タイマが更新される

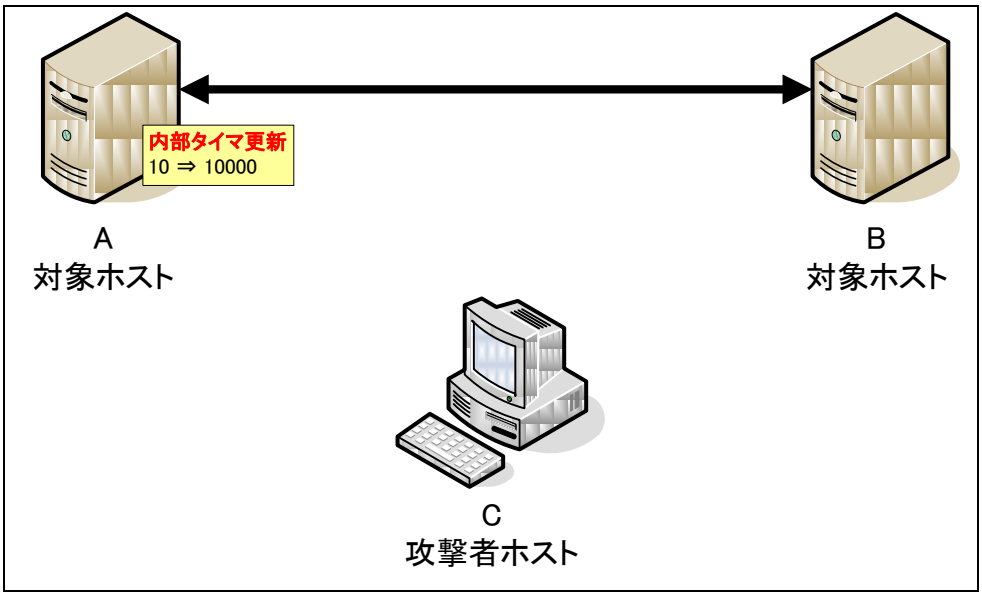


図 7-3 内部タイマ更新

対象ホスト A が②の偽装パケットを受信することで、内部タイマが更新される。図 7-3 では対象ホスト A における内部タイマが偽装パケットの Timestamps オプション値である、10000 に更新されている。

④　確立済みの TCP 通信のパケットが破棄される

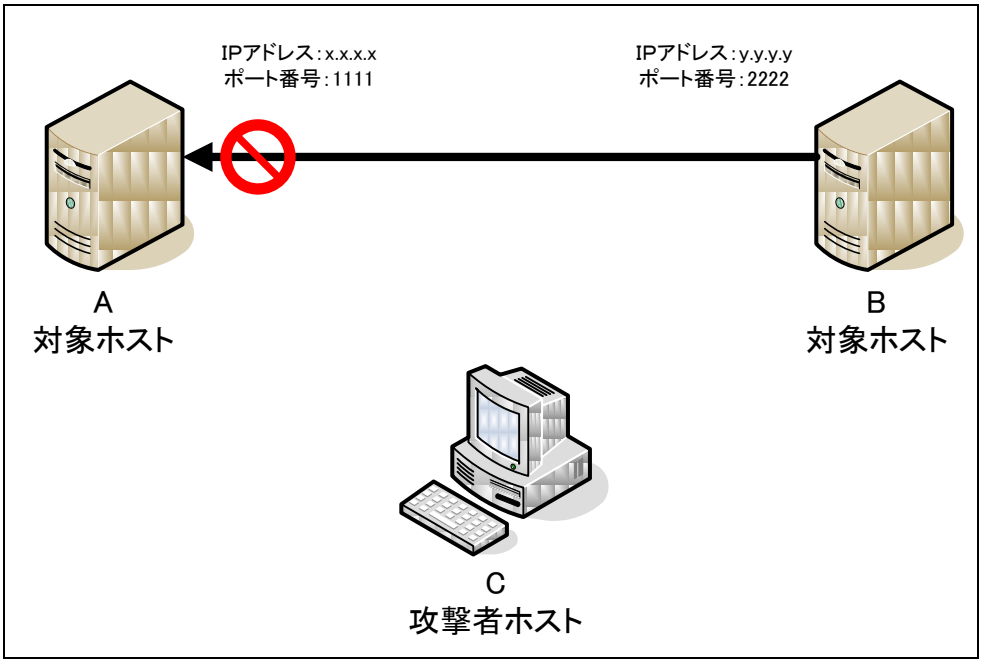


図 7-4　確立済みの TCP 通信のパケット破棄

PAWS 機能の内部タイマの仕様により、対象ホスト A が受信したパケットのうち、Timestamps オプション値が内部タイマより小さいパケットは破棄される。Timestamps オプション値には、パケット送信時に送信ホストの内部クロックを元に設定される。内部タイマが極端に大きな値に更新されたことで、Timestamps オプション値は内部タイマより小さくなる。このため、図 7-4 のように確立済みの TCP 通信のパケットも破棄され、強制的に TCP 通信が切断される。

原因と考察

この問題の原因は、PAWS 機能の内部タイマを意図的に更新できてしまう実装にある。

通常の TCP 通信においてパケットを受信した際に、受信したパケットが処理してもよいかどうかをシーケンス番号から判断している。通常の TCP 通信におけるパケット処理決定の判断手順を表 7-2 に記載する。

表 7-2 パケット処理の判断手順

手順	判断内容
1	受信したパケットのシーケンス番号が受信可能な範囲(ウインドウ)外にあった場合、そのパケットを破棄する
2	受信したパケットのシーケンス番号がウインドウ内にあった場合、そのパケットを処理する
3	受信したパケットのシーケンス番号がウインドウ外にあるが、そのパケットが再送、遅延といった特殊な条件に該当した場合、そのパケットを処理する

シーケンス番号は TCP ヘッダに 32 ビットの領域が確保されており、0~2^{32}(4294967296)の値が設定される。シーケンス番号が最大値である 2^{32} に到達したら、0 に戻る。そのため、いずれはシーケンス番号が重複するパケットが出現する。シーケンス番号が重複してしまった場合、正当なパケットであっても表 7-2 の判断手順により破棄される可能性がある。

通信回線が低速である場合、シーケンス番号が一巡して、シーケンス番号が重複するパケットが出現するまでの時間がパケットの生存時間(Time To Live: TTL)より長いため、正当なパケットが破棄される可能性は極めて低かった。しかし、通信回線が高速化していくにつれて、シーケンス番号が重複するパケットが出現するまでの時間が TTL よりも短くなった。これにより、正当なパケットが破棄されてしまう可能性が高くなった。こういった背景からシーケンス番号が重複していても Timestamps オプション値(後述)からパケットの順序を把握できるようにした、PAWS 機能が提案された。

PAWS 機能が有効となっている TCP 通信においてパケットを受信した際に、受信したパケットが処理してもよいかどうかをシーケンス番号と Timestamps オプション値から判断している。PAWS 機能を有効にした TCP 通信におけるパケット処理決定の判断手順を表 7-3 に記載する。なお、この手順は 2003 年 8 月に公開された Internet Draft である、draft-jacobson-tsvwg-1323bis-00.txt に記載されていた。赤字で記載している手順 1,2 が新たに追加された判断手順である。

表 7-3 パケット処理の判断手順(PAWS 機能を有効にしたケース)

手順	判断内容
1	受信したパケットの Timestamps オプション値(SEG.TSval)と、受信ホストの内部タイマ(TS.Recent)を比較する。比較した結果、SEG.Tsval<TS.Recent であった場合、そのパケットを破棄する
2	受信したパケットのシーケンス番号(SEG.SEQ)と受信ホストで記録していた最新の確認応答番号(Last.ACK)を比較する。比較した結果、SEG.SEQ<=Last.ACK であった場合、受信ホストの内部タイマ(TS.Recent)を受信したパケットの Timestamps オプション値に更新する
3	受信したパケットのシーケンス番号が受信可能な範囲(ウインドウ)外にあった場合、そのパケットを破棄する
4	受信したパケットのシーケンス番号がウインドウ内にあった場合、そのパケットを処理する
5	受信したパケットのシーケンス番号がウインドウ外にあるが、そのパケットが再送、遅延といった特殊な条件に該当した場合、そのパケットを処理する

表 7-3 の手順 2 において、SEG.SEQ<=Last.ACK という条件を満たすだけで、受信ホストの内部タイマを更新できる、という問題点が存在する。この問題点を利用することで、TCP 通信を確立している送信元 IP アドレスとポート番号、送信先 IP アドレスとポート番号が分かれば、意図的に小さなシーケンス番号を設定した偽装パケットを送信して、内部タイマを極端に大きな値に更新できる。内部タイマが極端に大きな値になると、表 7-3 の手順 1 により、正当なパケットまで破棄されることとなる。

●Timestamps オプション値について

パケット送信時の日時情報(TS Value)、最後に受信した応答パケットの TSval 値(TS Echo Reply)が設定される。TS Value、TS Echo Reply それぞれ 4 バイトの領域が確保される。日時情報とはいっても文字列ではなく、数値が格納される。

7)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題について、よく整理された情報は、UNITED STATES COMPUTER EMERGENCY READINESS TEAM(US-CERT)が 2005 年 5 月に発行した VU#637934、Daniel Hartmeier 氏が作成した実証コード(Proof of Concept: PoC)のコメント部分である。

インターネットの普及に伴い、ユーザが利用するインターネット回線が高速化していた。この高速化によって、TCP 通信自体のパフォーマンス、信頼性が問題になってきた。この状況を鑑み、1992 年 5 月に RFC1323 として「TCP Extensions for High Performance」が提案された。Timestamps オプション、PAWS 機能は、RFC1323 で提案されている実装である。なお、RFC1323 において、再送パケットにより内部タイマが更新されることで正当なパケットが破棄される可能性があることも記載されていた。しかし、内部タイマを更新するためには、受信したパケットのシーケンス番号(SEG.SEQ)と受信ホストで記録していた最新の確認応答番号(Last.ACK)の間に、*SEG.SEQ <= Last.ACK < SEG.SEQ+受信したパケットのパケット長*の条件を成立させる必要があった。そのため、この問題が発生する可能性は低いと考えられたため、あまり問題視されていなかった。

2003 年に RFC1323 の PAWS 機能の内部タイマを更新するアルゴリズムに問題があるとして、RFC1323 を置き換える Internet Draft(draft-jacobson-tsvwg-1323bis-00.txt)が IETF の Network Working Group から提出された。この Internet Draft では、内部タイマを更新するための条件を、*SEG.SEQ <= Last.ACK* という容易なものに置き換えている。こういった経緯により、TCP 通信を強制的に切断される問題が実現可能なものとなった。

2005 年 5 月に US-CERT を始め、各セキュリティベンダからこの問題に対するアドバイザリが公開された。また、Daniel Hartmeier 氏が作成した PoC も公開された。公開された PoC にはコメントとして、実装における問題点が詳細に記載されていた。

アドバイザリ公開後から現在に至るまで、ほとんどのネットワーク機器、OS の TCP スタックにおいて、修正プログラム、または対策方法が公開されている。

7)-5. IPv6 環境における影響

この問題はTCPプロトコル上の問題で、下位のIP層とは直接関係なく、概念的にはIPプロトコルのバージョンに限らずこの問題は再現すると考えられる。なお、この問題は偽装パケットを送付する必要があるため標的の TCP 通信の盗聴が必要になるが、IPv4 と同様に IPv6 でも TCP MD5 認証で認証や機密性を強化することで問題回避することができる。また、IPv6 の標準仕様となっている暗号化技術 IPsec 機能を使用することで IPv6 環境では実質上影響はほとんどないことが考えられる。

7)-6. 実装ガイド

PAWS 機能の内部タイマ更新条件を下記のように実装する。TCP 通信が切断される問題は、内部タイマ更新条件として、シーケンス番号を精査していないことに起因している(下記条件式の二重下線部がなかった)。そのため、内部タイマ更新条件として二重下線部を追加し、シーケンス番号を精査する。

SEG.SEQ <= *Last.ACK* <= *SEG.SEQ+SEG.LEN*

SEG.SEQ:受信したパケットのシーケンス番号
SEG.LEN:受信したパケットのパケット長
Last.ACK:受信ホストで記録していた最新の確認応答番号

実装の詳細については、オープンソース OS(FreeBSD,OpenBSD)を参考にするとよい。

http://www.freebsd.org/cgi/cvsweb.cgi/src/sys/netinet/tcp_input.c.diff?r1=1.252.2.15&r2=1.252.2.16&f=h(FreeBSD)
http://www.openbsd.org/cgi-bin/cvsweb/src/sys/netinet/tcp_input.c.diff?r1=1.184&r2=1.185&f=h(OpenBSD)

7)-7. 運用ガイド

1. ベンダ各社が提供している修正パッチをこの問題を受けるネットワーク機器およびOSに適用する
2. 必要がないのであれば、PAWS 機能および Timestamps オプションを無効にする
3. TCP 通信の盗聴防止のため、可能な通信であれば TCP MD5 認証や IPsec などを用いてパケットの認証や機密性を強化する。

7)-8. 参考情報

この問題についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 1 月)のものである。

1981 年 RFC793, TRANSMISSION CONTROL PROTOCOL.
http://www.ietf.org/rfc/rfc0793.txt

1988 年 RFC1072, TCP Extensions for Long-Delay Paths.
http://www.ietf.org/rfc/rfc1072.txt
※後に RFC1323 に置き換えられる

1990 年 RFC1185, TCP Extension for High-Speed Paths.
http://www.ietf.org/rfc/rfc1185.txt
※後に RFC1323 に置き換えられる

1992 年 RFC 1323, TCP Extensions for High Performance.
http://www.ietf.org/rfc/rfc1323.txt

1994 年 FreeBSD tcp_input.c
http://www.freebsd.org/cgi/cvsweb.cgi/~checkout~/src/sys/netinet/tcp_input.c?rev=1.1&content-type=text/plain&only_with_tag=MAIN
※この時点で Timestamps オプションは実装されていた

1995 年 OpenBSD tcp_input.c
http://www.openbsd.org/cgi-bin/cvsweb/~checkout~/src/sys/netinet/tcp_input.c?rev=1.1&content-type=text/plain
※この時点で Timestamps オプションは実装されていた

2003 年 Internet-Draft: TCP Extensions for High Performance
http://tools.ietf.org/id/draft-jacobson-tsvwg-1323bis-00.txt

2005 年 CVE-2005-0356
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-0356
Vulnerability Note VU#637934 TCP does not adequately validate segments before updating timestamp value
http://www.kb.cert.org/vuls/id/637934
JVNVU#637934 TCP の実装に不正な値で内部タイマを更新する脆弱性
http://jvn.jp/cert/JVNVU%23637934/index.html
Multiple Vendor TCP Timestamp PAWS Remote Denial Of Service Vulnerability
http://www.securityfocus.com/bid/13676/
TCP/IP timestamp denial of service
http://xforce.iss.net/xforce/xfdb/20635
TCP TIMESTAMPS Denial of Service Exploit
http://www.milw0rm.com/id.php?id=1008
※Daniel Hartmeier 氏が作成した PoC
マイクロソフト セキュリティ アドバイザリ(899480) TCP の脆弱性により、接続がリセットされる
http://www.microsoft.com/japan/technet/security/advisory/899480.mspx
※Win2000 での Timestamps オプションの無効化手順が記載されている
FreeBSD-SA-05:15.tcp
http://home.jp.freebsd.org/cgi-bin/showmail/announce-jp/1311
OpenBSD 3.6 release errata 015: RELIABILITY FIX: April 4, 2005
http://openbsd.org/errata36.html#tcp
(株)日立製作所 「TCP タイムスタンプオプションに関する脆弱性」対策について
http://www.hitachi.co.jp/Prod/comp/network/notice/VU-637934.html
※RFC 1323 の変種アルゴリズムを実装していた場合に影響を受けると明記されている

8). Optimistic TCP acknowledgements により、サービス不能状態に陥る問題

8)-1. 分類:TCP 【IPv4】【IPv6】

8)-2. 概要

TCP 通信において、意図的に応答パケットを送信し続けると、通常の TCP 通信より多くのパケットが同時に送信され続け、ネットワーク帯域が圧迫される。これにより、他のホストが通信できなくなり、サービス不能状態に陥る。

8)-3. 解説

攻撃手法とその影響

TCP 通信において、通信先ホストからのパケットの到達状況を無視して応答パケットを送信し続けることで、TCP の輻輳(ふくそう)(注1)制御を無効化できる。TCP の輻輳制御を無効化することで、対象ホスト、攻撃者ホスト間の TCP 通信が最大のウインドウサイズ(注 2)で通信を継続してしまう。この問題を利用することで、ネットワーク帯域が圧迫され、他のホストが通信できなくなり、サービス不能状態を発生させることができる。

この問題を利用した攻撃の流れを①～④で解説する。なお解説時にはウインドウサイズを cwnd*Maximum Segment Size(MSS)(注3)と定義する。

注 1:物が一箇所に集まるという意味。TCP においてはネットワークが通信過多の状態を意味する

注 2:バッファに保存できる受信パケットの最大バイト数

注 3:TCP 通信における送信可能な最大バイト数

① TCP 通信を確立する

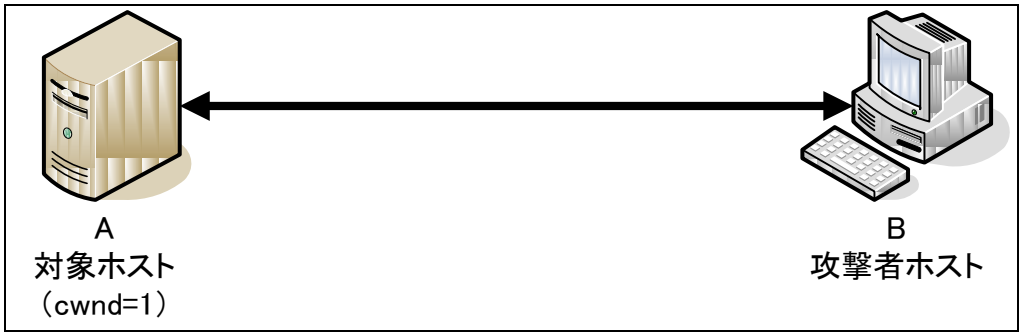


図 8-1 TCP 通信の確立

対象ホスト A と攻撃者ホスト B で TCP 通信を確立する(図 8-1 を参照)。図 8-1 において、TCP 通信確立時の対象ホスト A の cwnd を1とする。

② 攻撃者ホスト B が応答パケットを送信し続ける

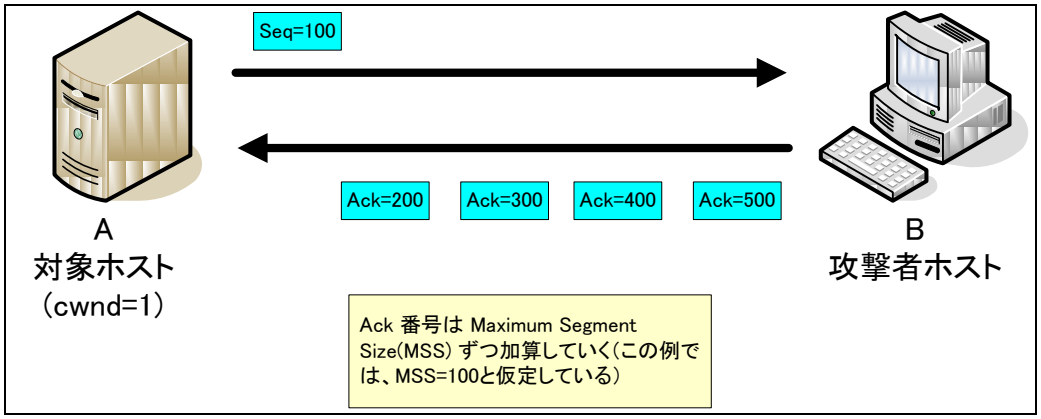


図 8-2 応答パケットの継続送信

攻撃者ホスト B が対象ホスト A から送信されるパケットを無視して、一定間隔で応答パケットを送信し続ける。応答パケットの確認応答番号(注 1)は TCP 通信確立時に設定された MSS の値ずつ加算していく。図 8-2 ではシーケンス番号(注 2)100 のパケットが到達していないにも関わらず、確認応答番号が 200, 300, 400, 500 のパケットを続けて送信している(図 8-2 では、MSS=100 と仮定している)。

注1:現在受信済みであるバイト数を表す数値である。TCP ヘッダに 32 ビットの領域が確保されている。TCP 通信においては、シーケンス番号と確認応答番号により、パケットが送信先ホストに到達したことを判断する

注 2:現在送信済みであるバイト数を表す数値である。TCP ヘッダに 32 ビットの領域が確保されている。TCP 通信においては、シーケンス番号と確認応答番号により、パケットが送信先ホストに到達したことを判断する

この応答パケット送信時、攻撃者ホストBは送信するパケットの確認応答番号が対象ホストAのウインドウサイズを越えないように注意する必要がある。確認応答番号がウインドウサイズを越えていた場合、対象ホスト A は受信したパケットをバッファに保存できないため、破棄してしまう。またその状態で応答パケットを送信し続けると、TCP 通信が切断される可能性がある。そのため、攻撃者ホスト B は確認応答番号がウインドウサイズを越えていないか、対象ホスト A の挙動から判断する必要がある(ウインドウサイズを越えていた場合、OS によって挙動が異なる)。

③　対象ホスト A のウインドウサイズが大きくなる

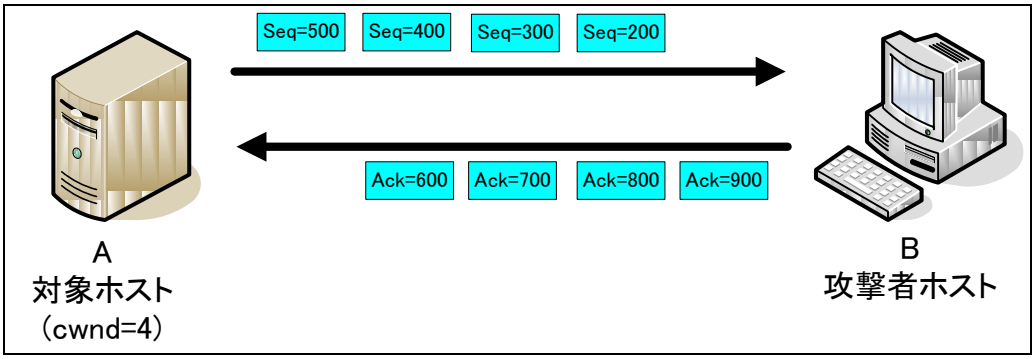


図 8-3 ウインドウサイズの増加

②において攻撃者ホスト B が応答パケットを送信し続けることで、対象ホスト A のウインドウサイズが大きくなる。対象ホスト A のウインドウサイズが大きくなることで、一度に送信される総バイト数が増加する。図 8-3 では cwnd が4となっている。

TCP 通信において、Window Scale オプション値(注1)を設定していた場合、TCP 標準の最大ウインドウサイズ(65535 バイト)よりも大きなウインドウサイズを設定できる。そのため、Window Scale オプション値を設定していた場合、この問題の影響を受けやすくなる。

注1：TCP ヘッダのオプション情報の一つである。詳細については、本項の「原因と考察」を参照のこと

④　ネットワーク帯域が圧迫され、サービス不能状態に陥る

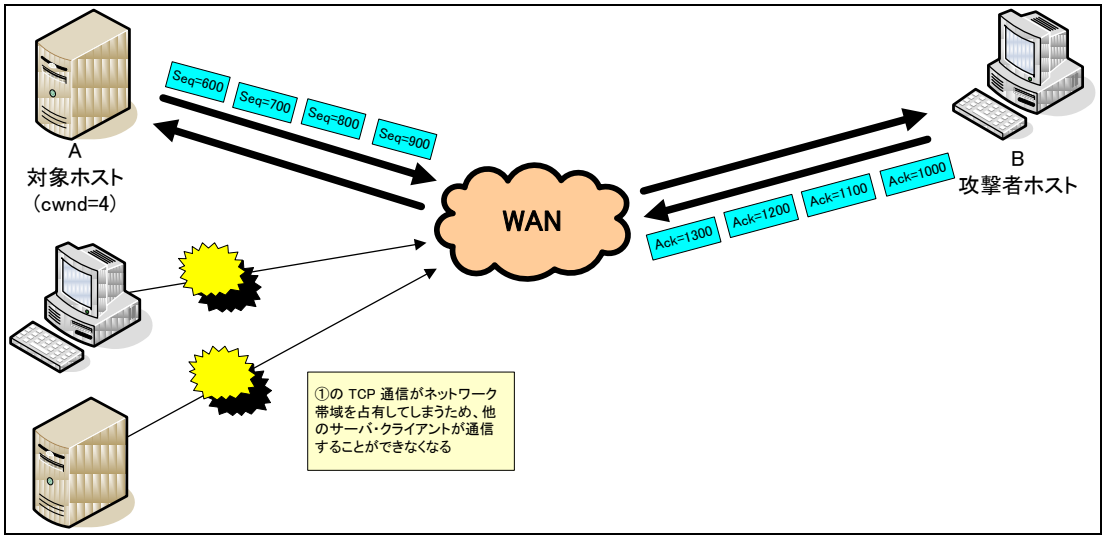


図 8-4 サービス不能状態の発生

通常であれば、ウインドウサイズが大きくなりすぎると、TCP の輻輳制御が働き、ウインドウサイズが抑制される。しかし、③においては攻撃者ホスト B が応答パケットを送信し続けているため、輻輳制御が無効化された状態となる(詳細は【原因と考察】を参照)。そのため、ウインドウサイズが大きいまま TCP 通信が継続する。これにより、図 8-4 のようにネットワーク(場合によっては、経路上のネットワークも含む)帯域が圧迫され、同ネットワークに所属するサーバ・クライアントが通信できなくなる。

原因と考察

この問題の原因は、TCP の輻輳(ふくそう)制御の実装にある。

TCP では輻輳状態が発生しないように、ウインドウサイズを制御している。この制御機構を輻輳制御と呼ぶ。この輻輳制御は、slow start アルゴリズム、avoid congestion アルゴリズム(後述)で実装されている。TCP 通信確立時は slow start アルゴリズムを利用して、ウインドウサイズに相手から通知されたウインドウサイズではなく、1MSS(イーサネットであれば、1460bytes)を設定する。これは TCP 通信確立時にネットワークが“混んでいる”可能性を考慮するためである。送信先ホストからの応答パケットを受信することで、ウインドウサイズを 1MSS 分だけ増加させる。このようにして、徐々にウインドウサイズを増やしていく。ウインドウサイズが一定値を越えたら、slow start アルゴリズムから avoid congestion アルゴリズムに推移し、ウインドウサイズの過剰な増加を抑制する。

TCP 通信中にデータの喪失(再送タイマ中に応答パケットが送信されてこない、相手からパケットの再送要求がきた等)が発生した場合、ネットワークが“混んでいる”と判断し、ウインドウサイズを減少させる。このように輻輳制御によって、ネットワーク帯域の状態に合わせて、ウインドウサイズが変更され、ネットワークが“混まない”ように制御されている。

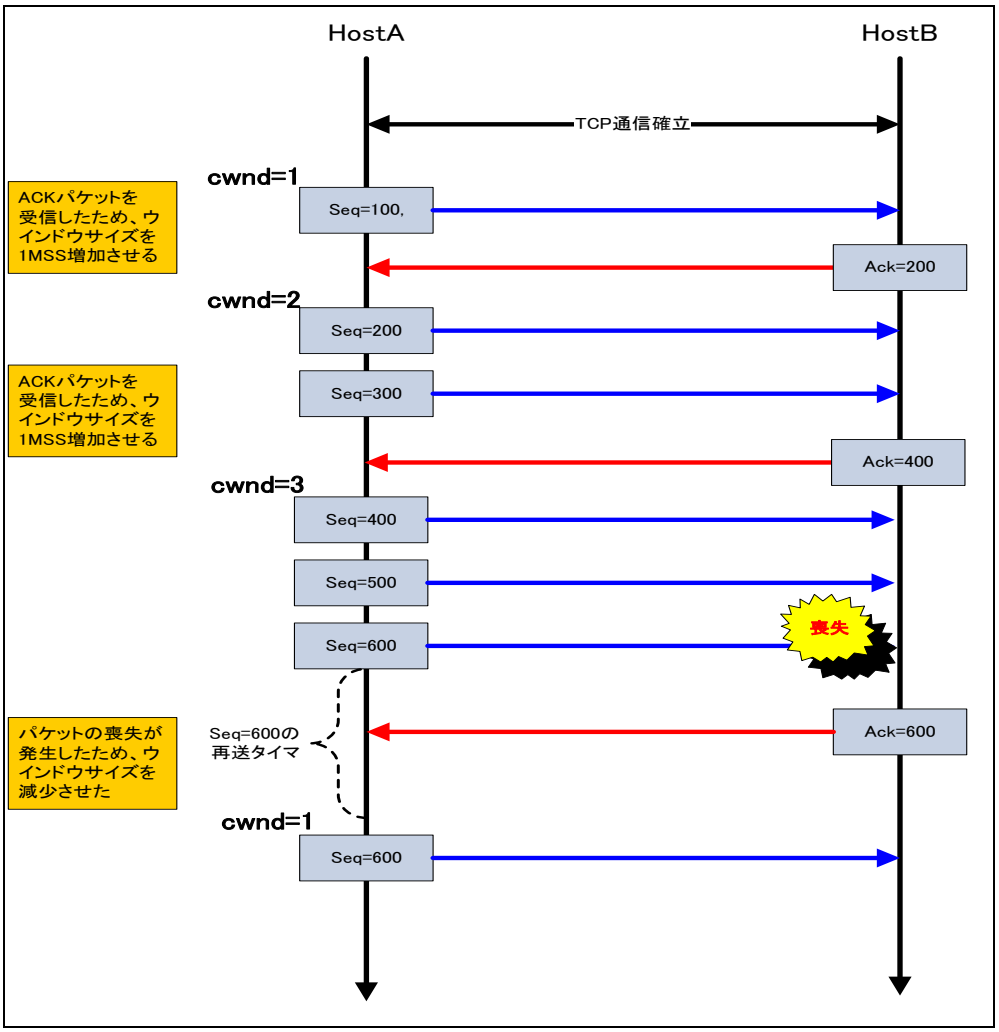


図 8-5 TCP の輻輳制御

輻輳制御の流れを図 8-5 に記載した。TCP 通信確立時にはウインドウサイズは 1MSS である(cwnd=1 と定義している)。TCP 通信で通信相手からの応答パケットを受信する度にウインドウサイズが 1MSS ずつ増加していることが分かる。ウインドウサイズが 3MSS(cwnd=3)の時にシーケンス番号 600 のパケットが経路上で喪失してしまった。これにより、再送タイマ時間を経過しても応答パケットを受信していないことから、ネットワークが"混んでいる"と判断し、ウインドウサイズを 1MSS に減少させた。ウインドウサイズ減少後、シーケンス番号 600 のパケットを再送した。このように、ネットワークの状態に応じてウインドウサイズが制御されていくこととなる。

この輻輳制御における問題点は、応答パケットを受信するだけでウインドウサイズを増加させる点にある。受信した応答パケットの確認応答番号が送信先ホストのウインドウサイズ内に収まっていれば応答パケットを処理する(ウインドウサイズ外である場合は破棄する)。しかも、送信先ホストがパケットを処理したかどうかを応答パケットのみで判断している。このことから、通信相手がパケットを処理したかどうかに関わらず、ウインドウサイズ内に収まるような応答パケットを送り続ければ、ウインドウサイズを増加させることが可能である。

通常の TCP 通信であれば、輻輳制御によりウインドウサイズが大きい状態が継続することはない。しかし、攻撃者が意図的に応答パケットを送り続けると、対象ホストはその応答パケットを処理してしまい、ウインドウサイズが大きい状態が継続してしまう。これにより輻輳制御が無効化されたことになる。ウインドウサイズが大きい状態が継続することで、ネットワーク帯域が圧迫され、サービス不能状態に陥ってしまう。なお、この問題は下記の 2 点を利用することで、さらに影響度が大きくなる。

1. 複数のホストから同時にこの問題を利用した攻撃を実行する(DDoS 攻撃)
2. TCP の Window Scale オプション値(後述)を設定する

複数のホストが同時に TCP 通信を確立し、この問題を利用した攻撃を仕掛けることで、複数のネットワーク帯域を同時にサービス不能状態に陥らせることができる。また、TCP の Window Scale オプション値を利用することで、ウインドウサイズの最大値を大きくすることができる。これにより、より過剰なトラフィックを発生させることができ、容易にサービス不能状態に陥らせることができる。

●slow start アルゴリズムと avoid congestion アルゴリズムについて

TCP 通信における転送速度は slow start アルゴリズム、avoid congestion アルゴリズムにより制御される。slow start アルゴリズム、avoid congestion アルゴリズムにはそれぞれ下記のような特徴がある。

slow start アルゴリズム:
応答パケットを受信する毎にウインドウサイズを 1MSS ずつ加算するため、転送速度が急速に上がる。

avoid congestion アルゴリズム:
応答パケットを受信する毎にウインドウサイズを(1MSS*1MSS/ウインドウサイズ)ずつ加算するため、転送速度が緩やかに上がる。

slow start アルゴリズム、avoid congestion アルゴリズムは閾値(ssthresh)によって切り替えられる。ウインドウサイズ<ssthresh であれば、slow start アルゴリズムが選択され、ウインドウサイズ>ssthresh であれば avoid congestion アルゴリズムが選択される。このようにして、一定値までは急速に転送速度を上げていき、一定値を越えたら緩やかに転送速度を上げるといった制御機構が実装されている。

●Window Scale オプション値について

TCP ヘッダの最大ウインドウサイズ(2^{16}-1)を拡張するために設定されるオプション値である。1～14 までの整数値(s と仮定)が設定され、この値を元に拡張したウインドウサイズが決定される。拡張したウインドウサイズは、TCP ヘッダのウインドウサイズ値*2^{S} となる。

8)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題について、よく整理された情報は、UNITED STATES COMPUTER EMERGENCY READINESS TEAM(US-CERT)が 2005 年11月に発行した、VU#102014 である。TCP における輻輳制御については、RFC 2581 で提案されている。この提案では送信先ホストから受信する応答パケットにより、転送速度を制御する方式を採用している。

1995 年に Stefan Savage 氏らが発表した、*"TCP Congestion Control with a Misbehaving Receiver"*において、この輻輳制御に問題があることが指摘されている。この論文で記述されている 3 つの攻撃手法のうちの 1 つが Optimistic ACKing である。Stefan Savage 氏らの論文では、サービス不能状態に陥る可能性が指摘されるだけであり、実証コード(Proof of Concept:PoC)が提示されているわけではなかった。

2005 年に Rob Sherwood 氏らが発表した、*"Misbehaving TCP Receivers Can Cause Internet-Wide Congestion Collapse"*において、Optimistic ACKing が実装され、サービス不能状態に陥る有効性も証明された。またこの論文において、この問題への対策方法がいくつか提示されており、Rob Sherwood 氏らは Randomly Skipped Segments を推奨している。

Randomly Skipped Segments とは、TCP 接続を受け付けるサーバ側が一定回数の応答パケットを受信したら、その直後サーバ側で送信する予定だったパケットを意図的に破棄するという実装方式である。パケットを意図的に破棄する際に、破棄するパケットのシーケンス番号を記録する。パケットを意図的に破棄した後、最初に受信したパケットのシーケンス番号が記録したシーケンス番号より大きいかどうかで、Optimistic ACKing 攻撃であるかを判断する。この論文では、Linux kernel 2.4.24 に対する Randomly Skipped Segments の実装方法が紹介されている。

また、Randomly Skipped Segments を実装した場合、意図的にパケットを破棄するため、パフォーマンスが低下する可能性がある。Rob Sherwood 氏らは選択確認応答(SACK: Selective ACKnowledgement)(注1)を実装することで、パフォーマンス低下を最小限に止められると述べている(Rob Sherwood 氏らの論文では実証データが記載されている)。

この問題に対してベンダ独自に対策を実施する事例もあるが、この問題自体が TCP の仕様に起因しているため、根本的な解決策はない。

8)-5. IPv6 環境における影響

この問題は TCP プロトコル上の問題で下位の IP 層とは直接関係はないため、RFC2581 の輻輳制御の仕様に準拠する実装の場合、概念的には IP プロトコルのバージョンに限らずこの問題は再現することが考えられ、IPv6 環境でも影響を受ける可能性がある。なお、一部のベンダではこの問題に対する対処が行われているが、IPv6 の影響および IPv6 の配慮が十分に行われているかについては詳細不明である。

8)-6. 実装ガイド

RFC2581 にまとめられている輻輳制御の仕様に準拠する場合、実装における回避策はない。ベンダ各社において、この問題の影響は低いと考えられているようである。

RFC2581 に準拠しない回避策として、Rob Sherwood 氏らの提示した Randomly Skipped Segments を輻輳制御に実装する方法が挙げられる(注 2)。ただし、US-CERT VU#102014 でも指摘されているが、Randomly Skipped Segments は TCP の一般的な実装ではないため、実装時はその点を理解する必要がある。

注 2:実装については、「**エラー! 参照元が見つかりません。エラー! 参照元が見つかりません。**」を参照のこと

8)-7. 運用ガイド

1. この問題を受けるネットワーク機器および OS に対する修正パッチが存在する場合、修正パッチを適用する
2. ネットワーク帯域を制限する
3. 信頼できるホストだけが接続できるよう、アクセス制御を実施する

8)-8. 参考情報

この問題についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 1 月)のものである。

1981 年 RFC793, TRANSMISSION CONTROL PROTOCOL.
http://www.ietf.org/rfc/rfc0793.txt

1992 年 RFC1323, TCP Extensions for High Performance.
http://www.ietf.org/rfc/rfc1323.txt

1999 年 RFC2581, TCP Congestion Control.
http://www.ietf.org/rfc/rfc2581.txt

TCP Congestion Control with a Misbehaving Receiver
http://www.cs.ucsd.edu/~savage/papers/CCR99.pdf

2005 年 Misbehaving TCP Receivers Can Cause Internet-Wide Congestion Collapse
http://www.cs.umd.edu/~capveg/optack/optack-extended.pdf
Vulnerability Note VU#102014 Optimistic TCP acknowledgements can cause denial of service
http://www.kb.cert.org/vuls/id/102014
JVNVU#102014 TCP プロトコルに Optimistic TCP acknowledgements による DoS が可能な脆弱性
http://jvn.jp/vn/JVNVU%23102014/index.html
ヤマハ株式会社 RT シリーズの TCP 上で DoS 攻撃を受ける可能性のある脆弱性について
http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/VU102014.html
※対策済みファームウェアを公開している
アライドテレシス株式会社 TCP(optimistic ack)の脆弱性について
http://www.allied-telesis.co.jp/support/list/faq/vuls/20051111.html
古河電気工業株式会社 TCP の Ack メッセージの処理に関する脆弱性の問題について(Optimistic Ack)
http://www.furukawa.co.jp/fitelnet/topic/ack_attacks.html

参考: マスタリング TCP/IP 入門編 第 3 版 p.189-p.205、p.210-p.215

9). Out of Band(OOB)パケットにより、サービス不能状態に陥る問題

9)-1. 分類:TCP 【IPv4】【IPv6】

9)-2. 概要

OOB パケット(注1)を受信すると、アプリケーションまたは OS が異常終了してしまい、サービス不能状態に陥る。

9)-3. 解説

攻撃手法とその影響

この問題を狙った攻撃は、OOB パケットを OS の TCP スタック(注2)が正常に処理できない点を利用している。この攻撃は WinNuke 攻撃とも呼ばれる。

攻撃者ホストが対象ホストと TCP 通信を確立し、OOB パケットを送信する。対象ホストが OOB パケットを正常に処理できない場合、アプリケーション、最悪の場合は OS が異常終了してしまう。この問題を利用した攻撃は、NetBIOS(139/tcp)サービスに対して実行された。

この問題を利用した攻撃の流れを①～③で解説する。

① TCP 通信を確立する

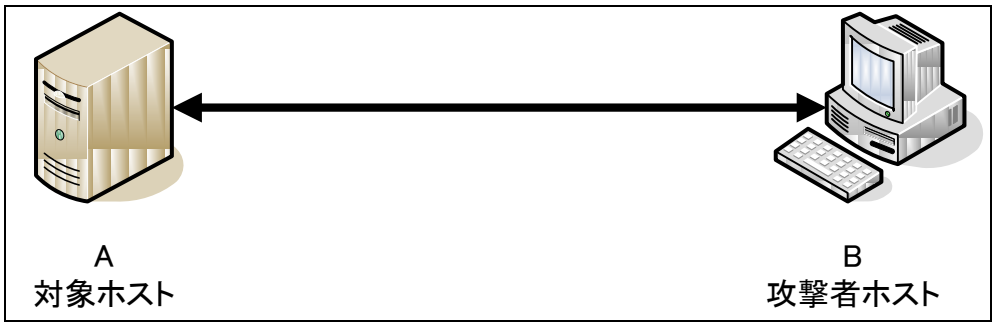


図 9-1 TCP 通信の確立

図 9-1 のように、対象ホスト A と攻撃者ホスト B で TCP 通信を確立する。

注1:緊急に処理する必要があるデータを含むパケット

注 2:TCP パケットを処理する、OS の内部プログラム

② OOB パケットを対象ホストに送信する

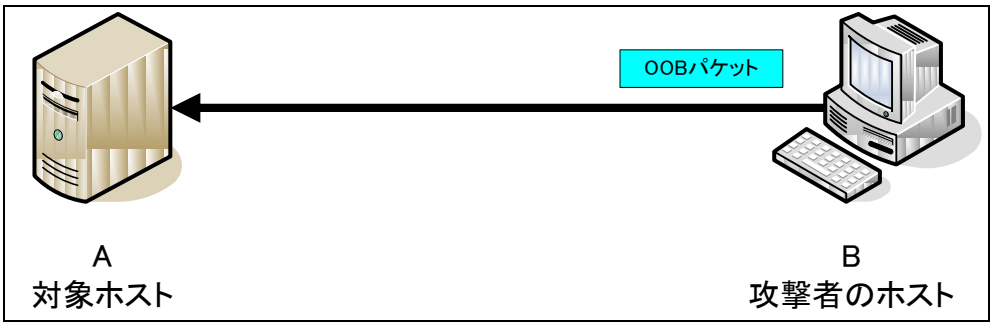


図 9-2 OOB パケットの送信

図 9-1 で確立した TCP 通信において、攻撃者ホスト B から OOB パケットを対象ホスト A に送信する(図 9-2 を参照)。なお、OOB パケットは 1 バイト以上のデータを含む必要がある。

③ アプリケーションまたは OS が異常終了する

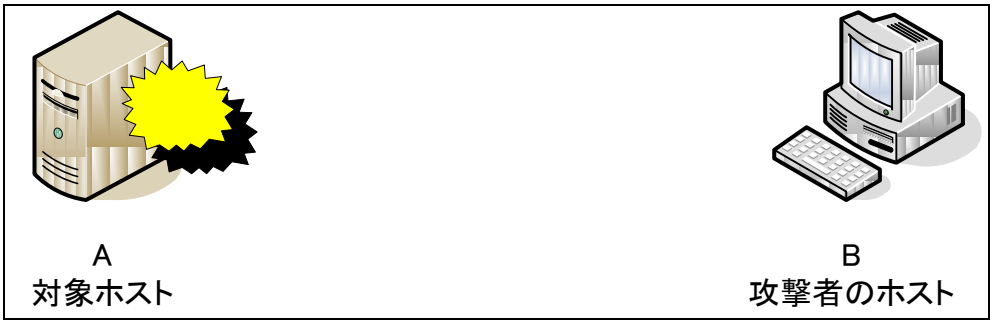


図 9-3 アプリケーションまたは OS の異常終了

対象ホストが図 9-2 で送信されたパケットを受信する。対象ホストが OOB パケットを正常に処理できないため、①の TCP 通信を確立していたアプリケーション、最悪の場合は、OS 自体が異常終了してしまう(図 9-3 を参照)。

原因と考察

この問題の原因は、OOB パケットにおける緊急データの取り扱いにあるとされているが、詳細な技術情報については公開されていない。

この問題については、Microsoft 社が公開している WindowsNT の技術情報で解説されている。なお、この問題は TCP の仕様ではなく、実装によって発生している。そのため、影響範囲が特定の OS に限定されることに注意していただきたい(対象 OS については、参考情報を参照のこと)。

WindowsNT の技術情報によると、WindowsNT の TCP スタックでは、OOB パケット(後述)において、緊急に処理してほしいデータの後にも通常データが続くことを想定して実装されている(図 9-4 を参照のこと)。この問題を引き起こす OOB パケットのように緊急データのみが格納されているパケット(図 9-4 の斜線部のないパケット)の場合でも、通常データがあるものとして TCP スタックが処理してしまう。これにより、例外エラーが発生してしまい、OS またはアプリケーションが異常終了してしまう。

この問題を受ける Windows95 において、レジストリを編集し、OOB パケットの処理方法を Berkeley Software Distribution(BSD)形式(後述)から RFC1122 形式(後述)に変更すると、この問題の影響を受けなくなる。このことから、緊急ポインタ情報の取り扱いにおいて、問題があると推測される。しかし、図 9-4 のような正常に処理されると考えられるパケットを受信した場合でも、WindowsNT が異常終了することが確認できた(Windows95 同様にレジストリを編集し、OOB パケットの処理方法を RFC1122 形式に変更しても同様だった)。この問題について詳細な情報が公開されていないため、詳細な原因について言及することはできない。

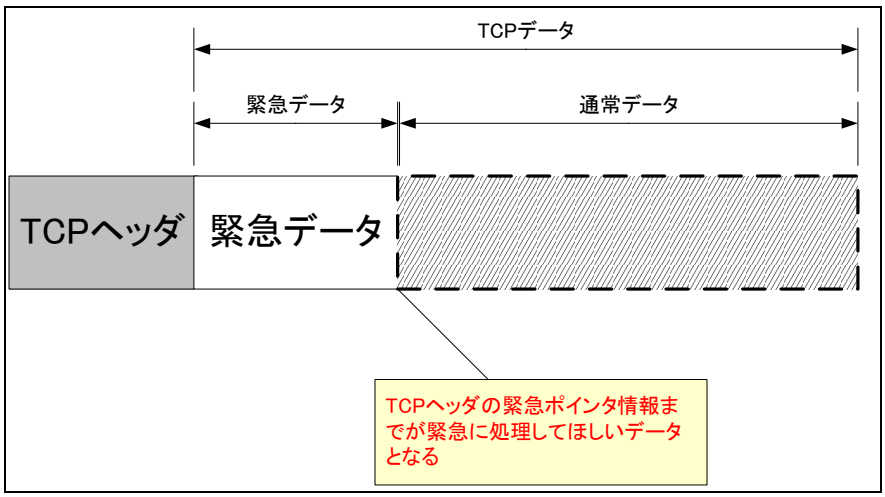


図 9-4 OOB パケットの取り扱い

●OOB パケットについて

OOB パケットは、TCP ヘッダにおいて URG フラグ(後述)、緊急ポインタ情報(後述)が設定されたパケットのことである。受信ホストで緊急に処理してほしいデータがある場合、送信ホストは URG フラグ、緊急ポインタ情報を設定し、OOB パケットとして送信することで、受信ホストに緊急に処理するデータがあることを通知できる(ただしそのデータが実際にすぐに処理されるかどうかは、各アプリケーションの実装に依存する)。この時、受信ホストは”緊急モード”状態であるとされる。緊急ポインタ情報がしるす終了データを受信するまでは、受信したデータは緊急データとして取り扱われる。緊急ポインタ情報がしるす終了データを受信したら、”緊急モード”状態が終了する。OOB パケットを利用するプロトコルとしては、telnet、rlogin、ftp 等が挙げられる。また、OOB パケットを送信する場合、少なくとも最低 1 バイトのデータを送信しなければならない。

●URG フラグについて

URG フラグは、TCP ヘッダのコードビット(Code Bit)と呼ばれる設定情報の一つである。

TCP ヘッダには、コードビット(Code Bit)と呼ばれる 6 ビットの情報が定義されている。このコードビットのそれぞれ 1 ビットがフラグと呼ばれる設定情報を意味し、このフラグによって TCP パケットがどんな役割を担うかが決定される。コードビットの各 1 ビットに 1 を設定すると、各フラグ情報が有効となり、0 を設定すると無効となる。

URG フラグが有効となっているパケットは、OOB パケットであることを意味する。なお URG フラグが有効になった場合のみ、TCP ヘッダの緊急ポインタ情報が利用される。

●緊急ポインタ情報について

緊急ポインタ情報は TCP ヘッダにおける設定情報の一つであり、OOB パケットにおいて緊急に処理しなければならないデータの位置情報である。位置情報として、シーケンス番号で構成される TCP データのうち、どの部分までが緊急に処理しなければならないデータであるかを表す、オフセット情報が設定される。

緊急ポインタ情報の実装には、2 通りの方法が存在している。TCP の実装の多くは、RFC 1122 形式よりも BSD 形式を採用していると言われている。

- 緊急ポインタ情報が緊急データ直後の通常データの最初をしるす、BSD 形式
- 緊急ポインタ情報が緊急データの最後のデータをしるす、RFC 1122 形式

9)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題が発覚した発端は、1997 年 5 月に_eci 氏が Bugtraq メーリングリストに投稿したメールである。_eci 氏のメールには、実証コード(Proof of Concept:PoC)も記載されており、この PoC を試した有志により、実際にこの問題への攻撃が成功することが確認された。この問題が WinNuke 攻撃と呼ばれることとなった原因は、_eci 氏が投稿した PoC が winnuke.c という名前だったためと推測される。_eci 氏の投稿を受けて、有志により VC++、Perl といった別の言語での PoC も作成された。

この問題に対するパッチが提供されるまでに、有志によりいくつかの回避策が提示されている。回避策として挙げられていたのは、下記の 2 つである。

- NetBIOS サービスの無効化
- レジストリ編集による、OOB パケット処理方法の変更

_eci 氏の投稿から数日後に Microsoft 社は Windows3.1、NT4.0 用の Hotfix をリリースした。しかしこの Hotfix を適用しても、この問題の影響を受けるとの報告があり、さらにその数日後 Microsoft 社は Hotfix を再リリースしている。なお、Windows95 用の Hotfix は、2 度目の Hotfix のリリースと同時期にリリースされている。WindowsNT4.0 においては、ServicePack4 以降ではこの問題への対策が施されている。

この問題は Windows だけではなく、NetBIOS ベースのサービスが稼動している OS で影響を受ける。SCO OpenServer 5.0、AppleShare IP 6.1 Web & File Server もこの問題の影響を受ける。現在は各ベンダより修正プログラムが提供されており、この問題は解決している。

9)-5. IPv6 環境における影響

この問題は TCP プロトコル上の問題で下位の IP 層とは直接関係はないため、概念的には IP プロトコルのバージョンに限らず影響があると考えられ、IPv6 環境でも影響を受ける可能性がある。しかし、多くのベンダでは既にこの問題の対処が行われているため、影響を受ける製品の TCP/IP の実装方法にもよるが、現在は IPv6 でも影響は存在しないものと考えられる。

9)-6. 実装ガイド

この問題は TCP の実装によるものであるか、アプリケーションの実装によるものであるか、情報が少なく断定することはできない。RFC1122 において、OOB パケットの取り扱いが必須であることと、その取り扱い方法が規定されているものの、TCP の OOB パケットの実装には、BSD 形式と RFC1122 形式の 2 通りが混在しているのが実情である。下記の実装により、この問題の発生を軽減することができる。

1. OOB パケットを取り扱うプロトコル(telnet、ftp、その他独自プロトコル)を利用しない場合には、OOB パケットを取り扱う実装をしない。または、それを取り扱わない機能を用意する
2. OOB パケットの取り扱いにおいて、BSD 形式と RFC1122 形式のどちらを利用するか、切り替える機能を用意する

9)-7. 運用ガイド

ベンダが修正パッチを提供している場合、その修正パッチを適用する。修正パッチが提供されていない、もしくは適用できない場合、下記の対策を実施することで、この問題の影響度を低くすることができる。

1. ファイアウォールで不要な通信をブロックする
2. アプリケーション側で信頼できるホストからのみ接続を許可するよう、アクセス制御を実施する

9)-8. 参考情報

この問題についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 1 月)のものである。

1981 年 RFC793, TRANSMISSION CONTROL PROTOCOL.
http://www.ietf.org/rfc/rfc0793.txt

1989 年 RFC1122, Requirements for Internet Hosts -- Communication Layers.
http://www.ietf.org/rfc/rfc1122.txt

1997 年 Bugtraq mailing list archives: Windows 95/NT DoS
http://www.security-express.com/archives/bugtraq/1997_2/0203.html
※この問題の発端となった投稿
Bugtraq mailing list archives: OOB Quick Fix
http://www.security-express.com/archives/bugtraq/1997_2/0211.html
※NetBIOS サービスを無効化する手順が投稿された
Bugtraq mailing list archives: New Win95 OOB fix allows Netbios to be used
http://www.security-express.com/archives/bugtraq/1997_2/0231.html
※レジストリを編集して、OOB パケットの処理方法を修正する方法が投稿された

Bugtraq mailing list archives: WinNT 4.0 OOB Hotfix
http://www.security-express.com/archives/bugtraq/1997_2/0232.html
※Microsoft 社がリリースした Windows3.1、NT4.0 用の Hotfix についてのアドバイザリが転載されている
Bugtraq mailing list archives: Update to Windows 95 TCP/IP to Address Out-of-Band Issue
http://www.security-express.com/archives/bugtraq/1997_2/0326.html
※Microsoft 社がリリースした Windows95 用の Hotfix についてのアドバイザリが転載されている
H-57: Windows NT/95 Out of Band Data Exploit
http://ciac.llnl.gov/ciac/bulletins/h-57.shtml
Out of Band(OOB)data denial of service
http://xforce.iss.net/xforce/xfdb/173
Multiple Vendor "Out Of Band" Data Denial Of Service Vulnerability
http://www.securityfocus.com/bid/2010
Multiple Vendor Out Of Band Data DoS(WinNuke)
http://www.osvdb.org/1666

1998 年 IP-based Denial of Service Attacks
http://www.securityfocus.com/advisories/1411

1999 年 CVE-1999-0153
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0153
AppleShare IP Web & File 6.1.1 Update Read Me
http://docs.info.apple.com/article.html?artnum=58287

2003 年 [NT]Out Of Band(OOB)データ受信時の TCPIP.SYS の Stop 0A
http://support.microsoft.com/kb/143478/ja

2006 年 Out-of-Band 問題に対する Windows 95 TCP/IP の更新プログラム
http://support.microsoft.com/kb/168747/ja
Windows NT および Windows 2000 での TCP/IP および NBT の設定
http://support.microsoft.com/kb/120642/ja

2007 年　Windows TCP/IP Registry Entries
http://support.microsoft.com/kb/158474
Protocol-Independent Out-of-Band Data
http://msdn2.microsoft.com/en-us/library/ms740102.aspx

参考　詳解 TCP/IP<Vol.1>　p.330-p.334
マスタリング TCP/IP　入門編　第 3 版　p.189-p.205、p.210-p.215
ネットワーク侵入解析ガイド
侵入検知のためのトラフィック解析法　p.243-p.247

10).ウインドウサイズ 0 の TCP 接続過多により、サービス不能状態に陥る問題

10)-1. 分類:TCP 【IPv4】【IPv6】

10)-2. 概要

RFC793 等で規定されている TCP の実装には、TCP 接続確立後のデータ送受信の際にウインドウのサイズを 0 に設定した ACK パケットを大量に送信し続けることにより、サービス不能状態に陥る可能性がある。

10)-3. 解説

攻撃手法とその影響

この問題を悪用すると、TCP 接続が確立されたホストのリソースが大量に浪費され、第三者のホストからの正規の接続が不能となる。この問題を利用した想定される攻撃の例を図 10-1 から図 10-2 に示す。以下に示す攻撃手法は標的のホスト A から、攻撃者のホスト B がデータを取得することを前提とする。

図 10-1 において、攻撃者のホスト B から標的のホスト A への接続を確立するために 3 ウェイハンドシェイクを成立させる。

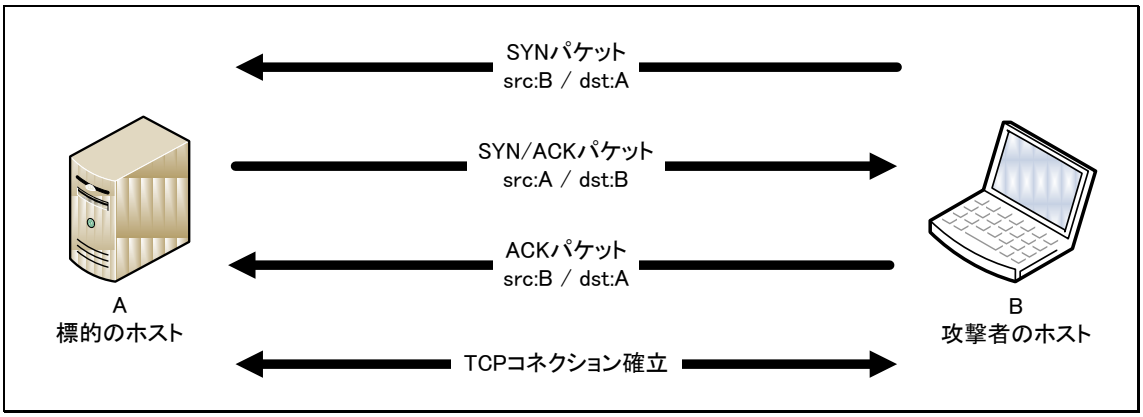


図 10-1 3 ウェイハンドシェイクによる TCP セッション確立

図 10-2 のように、3 ウェイハンドシェイクの成立後、標的のホスト A から攻撃者のホスト B に対しデータが送信される。その際に送信されるデータサイズは、ACK パケットのウインドウサイズで指定される。なお、このウインドウサイズは攻撃者のホスト B のみ指定可能である。このとき、ウインドウサイズを 0 にして ACK パケットを送信すると標的のホスト A からのデータ送信は中断し、TCP セッションは維持されたままの状態(ESTABLISHED 状態)となる。

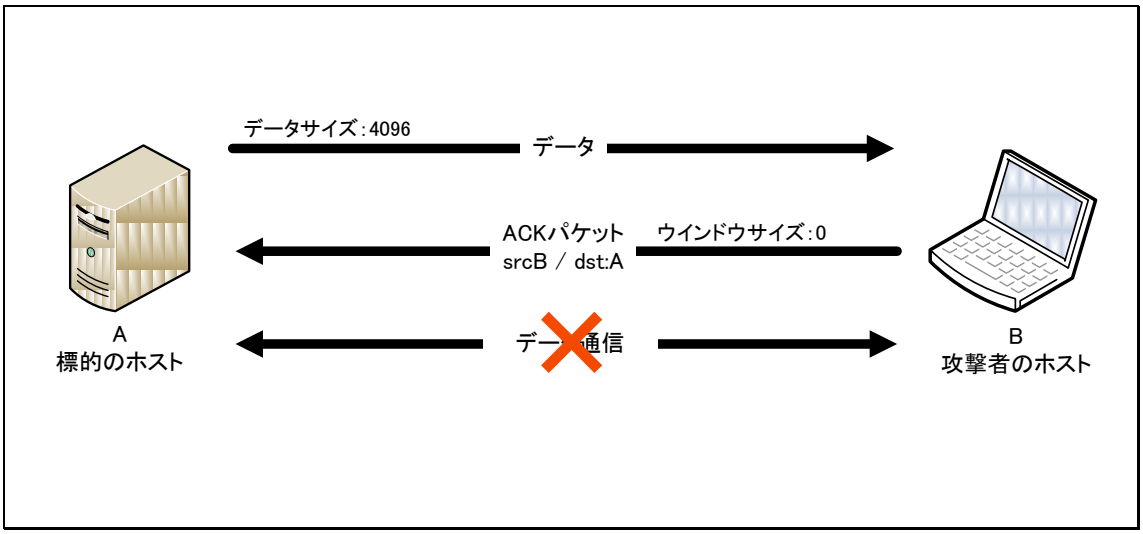


図 10-2 ウインドウサイズを利用したフロー制御

この状態を大量に生成し、攻撃者はウインドウサイズを 0 に指定した ACK パケットを大量に送信する。ウインドウサイズ 0 の影響でデータの転送は行われないため、ネットワーク帯域を圧迫することなく、標的のホスト A のメモリリソースを浪費させる。これにより図 10-3 に示すように、標的のホスト A に対する第三者のホスト C からのアクセスができなくなる。

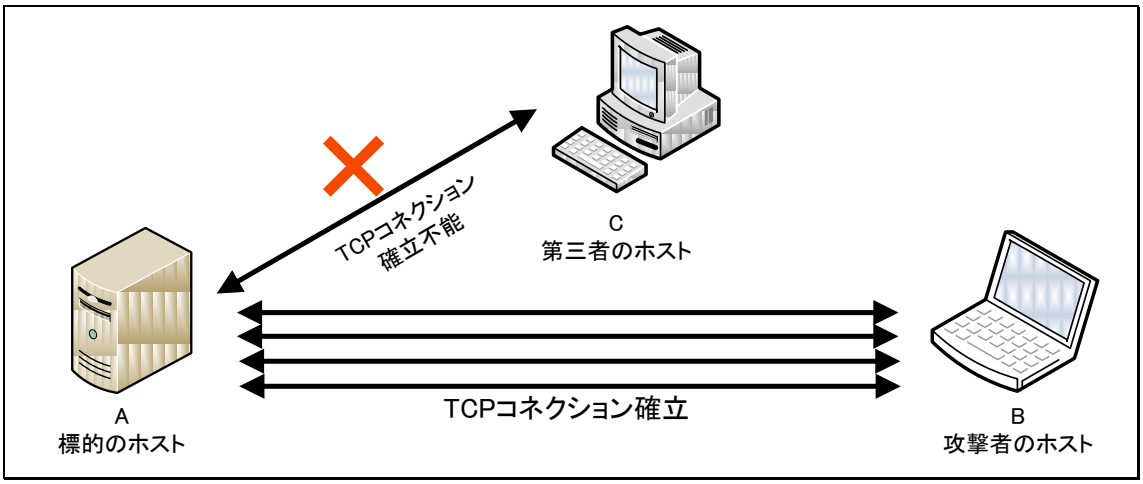


図 10-3 メモリリソース不足による第三者からのアクセス不能状態

原因と考察

まず、ウインドウサイズについて説明する。TCP ではセッション確立後、送信ホストの都合でデータを送信する。つまり受信ホストの都合に関係なくデータパケットが送信されるため、負荷が大きいときにはデータを受信しきれなくなる可能性がある。(注 1)これを防ぐため、TCP では受信ホストが送信ホストに受信可能なデータサイズを通知する仕組みが存在する。この仕組みがウインドウサイズである。

ウインドウサイズは受信ホストのみが指定でき、図 10-4 に示すように、TCP ヘッダ内にウインドウサイズを指定する領域(16 ビット)が存在する。受信ホストは、受信可能なサイズをこのウインドウサイズの領域に入れて送信する。

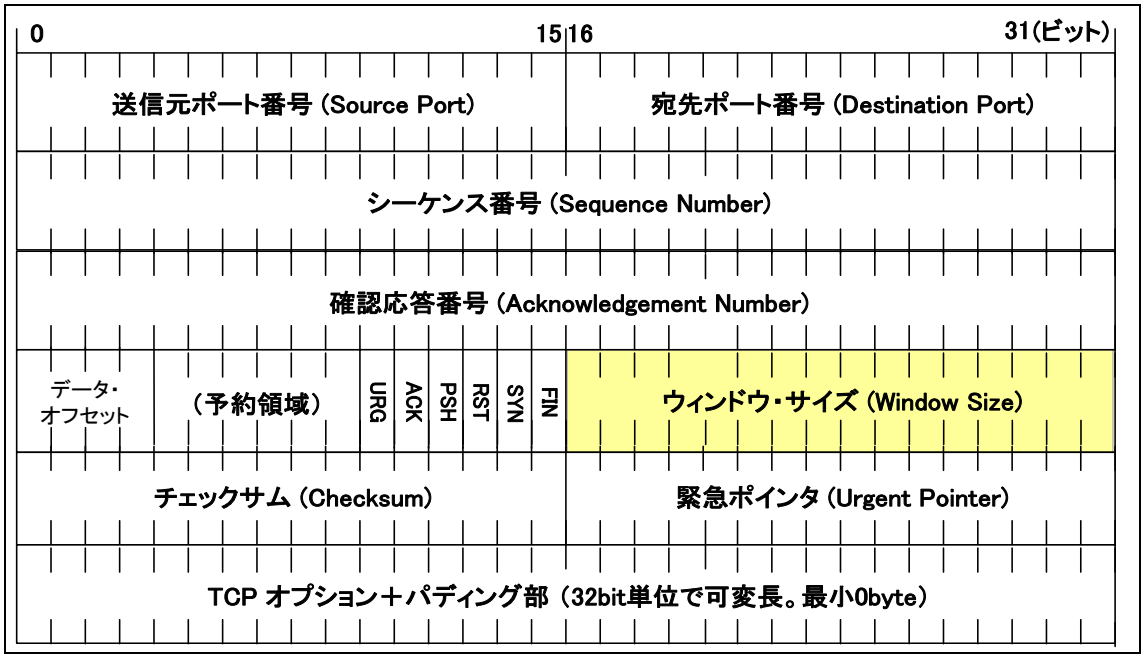


図 10-4 TCP ヘッダ

注 1:データを受信できなかった場合は、同じデータを再送する仕組みになっている。また、送信ホストから送信されるデータ量が受信ホストの処理できるスピードを上回ると、SWS(Silly Window Syndrome)という現象が起こる。これは、受信ホストが少しでも処理が完了したことを ACK で受信できるウインドウサイズを送信ホストに伝えてしまうことによって、常にごくわずかなデータ量を送信する現象に陥ることを指す。

RFC793 に規定されている TCP の仕様では、受信ホストでデータの受信処理が間に合わない場合、一旦データ通信を中断する要求を出す。その際に通知するものがウインドウサイズ 0 であり、このパケットを受信した送信ホストはデータの送信を中断する。その後、定期的に受信ホストのウインドウサイズの最新情報を取得するために、送信ホストはウインドウプローブというパケットを受信ホストに対して送信する。

図 10-5 に示すように、ウインドウプローブは受信ホストから応答が返ってくる限り理論上無限に繰り返されるため、セッションは維持されたままとなる。このウインドウサイズ 0 に指定した ACK パケットを大量に送信し、いつまでもデータの送受信が行われないセッション状況を大量に引き起こすことで、サービス不能状態に陥る。なお、発見元である Outpost24 がこの問題を確認するために作成したツール名が Sockstress であることから、本問題は Sockstress という名で広く知られている。

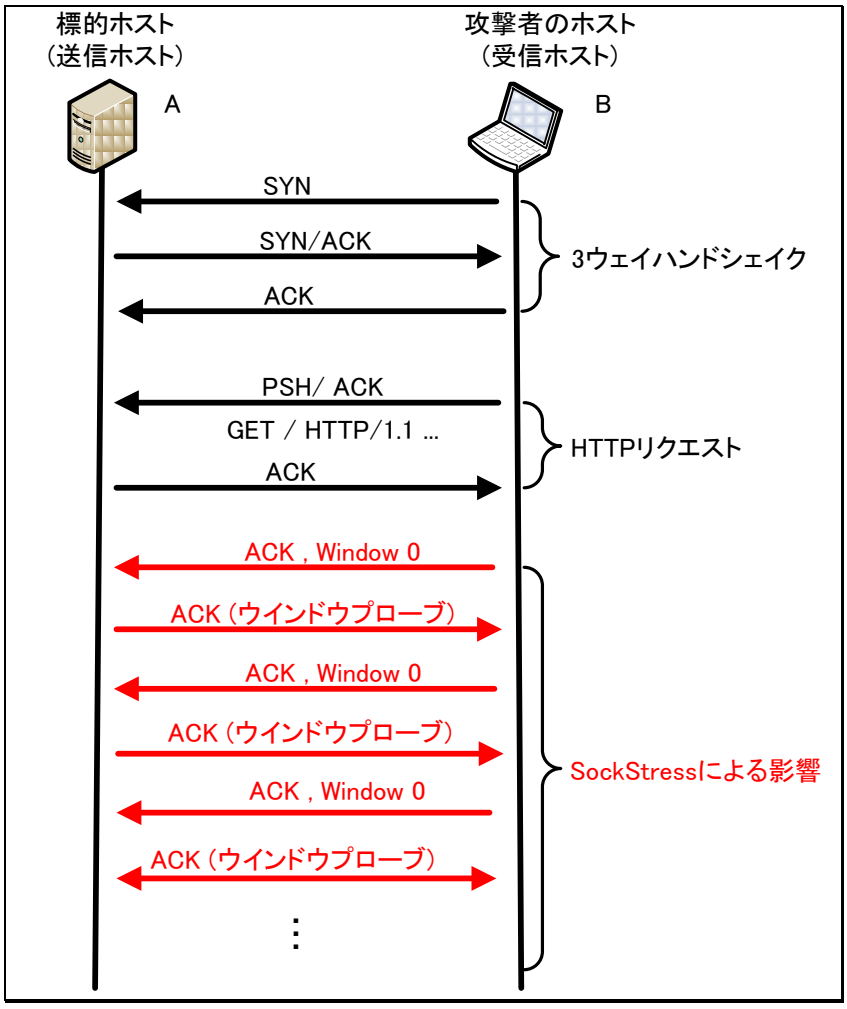


図 10-5　Sockstress 使用時の攻撃イメージ

10)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題についてよく整理された情報は、Finnish Computer Emergency Response Team(CERT-FI)が 2009 年 9 月 8 日に発表した、CERT-FI Advisory on the Outpost24 TCP Issues である。

この問題は、2008 年 10 月 2 日に Outpost24 の研究者である Jack C. Louis 氏、および同社の Robert E. Lee 氏によって指摘され、2009 年 9 月 8 日に CERT-FI の協力の下に詳細情報が公開された。「UnicornScan」というポートスキャンツールを使用中に発見したもので、その後問題を確認するために「Sockstress」というツールを開発した。このツールを使用することで本問題を悪用する TCP 接続を試行することが可能であるが、一般公開はされていない。この問題の影響は、Windows OS、Linux、BSD 系 Unix、Cisco 製品、およびその他 OS を含む広範囲に渡り、TCP を実装するシステムが影響を受ける可能性がある。CERT-FI からこの問題の詳細が公表されると、各ベンダにて対応策が公開された。ただし、本問題に関して TCP 接続が正当なものか、否かを判断することが困難であるため、一部のベンダからは対策が未だに公開されていない。詳細に関しては、各ベンダから提供されている情報を参照のこと。

なお、IETF の TCPM Working Group においてウインドウサイズ 0 に指定された ACK パケット受信時の実装に関連するセキュリティ議論が行われている(Internet Draft Clarification of sender behaviour in persist condition.)。しかし、RFC793 にて規定されている TCP の仕様に問題が存在するため、現在においても根本的な解決策はなく、本問題を回避または影響を緩和することで対応しているというのが実情である。

10)-5. IPv6 環境における影響

この問題は TCP プロトコルの問題で、OSI 参照モデルのトランスポート層に属する問題であるため、概念的には IP プロトコルのバージョンに限らずこの問題は再現すると考えられ、IPv6 環境でも影響を受ける可能性がある。ただし、実際の IPv6 環境における影響についての詳細は不明である。

10)-6. 実装ガイド

1. ホストのリソースが復元するまで新しい TCP 接続の数を制限する。
2. ウインドウサイズ 0 の ACK をある一定水準以上受信した際、対象のセッションを切断する。

10)-7. 運用ガイド

1. 各ベンダから提供されているパッチや修正バージョンを適用する。
2. 使用できる TCP セッション数を管理、あるいは制限する。
3. 信頼できない送信元アドレスからのパケットを破棄するために、限られたアクセスのみに限定する。

10)-8. 参考情報

この問題についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本問題調査時点(2010 年 5 月)のものである。

1981 年 RFC793, TRANSMISSION CONTROL PROTOCOL.
http://www.ietf.org/rfc/rfc0793.txt

1982 年 RFC813, WINDOW AND ACKNOWLEDGEMENT STRATEGY IN TCP
http://www.ietf.org/rfc/rfc0813.txt

1989 年 RFC1122, section-4.2.2.17, Probing Zero Windows
http://www.ietf.org/rfc/rfc1122.txt

2006 年 Vulnerability Note VU#723308 TCP may keep its offered receive window closed indefinitely(RFC 1122)
http://www.kb.cert.org/vuls/id/723308

2008 年 Outpost24 TCP Vulnerability Found
http://www.outpost24.com/news/news-2008-10-02.html
Common Vulnerabilities and Exposures CVE-2008-4609
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4609
IETF Internet Draft: Clarification of sender behaviour in persist condition
http://tools.ietf.org/id/draft-ananth-tcpm-persist-00.txt

2009 年 CPNI TECHNICAL NOTE 3/2009
http://www.cpni.gov.uk/Docs/tn-03-09-security-assessment-TCP.pdf
Outpost24 Unicornscan
http://www.unicornscan.org/
Cisco Security Response: Cisco Response to Outpost24 TCP State Table Manipulation Denial of Service Vulnerabilities Document ID: 108167
http://www.cisco.com/en/US/products/products_security_response09186a0080a15120.html
JPCERT/CC Alert JPCERT-AT-2009-0019
http://www.jpcert.or.jp/at/2009/at090019.txt
JVNVU#943657 複数の TCP の実装におけるサービス運用妨害(DoS)の問題
http://jvn.jp/cert/JVNVU943657/index.html

2009 年

マイクロソフト セキュリティ情報 MS09-048
http://www.microsoft.com/japan/technet/security/bulletin/ms09-048.mspx
turbolinux TCP プロトコルの問題について(CVE-2008-4609)
http://www.turbolinux.co.jp/support/document/knowledge/829.html
Cisco Advisory ID: cisco-sa-20090908-tcp24
http://www.cisco.com/en/US/products/products_security_advisory09186a0080af511d.shtml
McAfee CVE-2008-4609 にて報告された TCP プロトコルの問題について
問題番号 EW09092801
http://www.mcafee.com/japan/pqa/aMcAfeeEws.asp?ancQno=EW09092801&ancProd=McAfeeEws
redhat レッドハット ナレッジベース CVE-2008-4609 の問題
http://kbase.redhat.com/faq/docs/DOC-18964
NEC 複数の TCP の実装におけるサービス運用妨害(DoS)の問題 NV09-014
http://www.nec.co.jp/security-info/secinfo/nv09-014.html
SECLISTS.ORG [security bulletin] HPSBMI02473 SSRT080138 rev.1
http://seclists.org/bugtraq/2009/Nov/131
JVNDB-2009-002092
Microsoft Windows におけるサービス運用妨害(DoS)の問題
http://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-002092.html
CERT-FI Advisory on the Outpost24 TCP Issues
https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html

2010 年

ヤマハ RT シリーズのセキュリティに関する FAQ
TCP の実装におけるサービス運用妨害(DoS)の脆弱性について
http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/VU943657.html
JVNDB-2009-002090
複数の TCP の実装におけるサービス運用妨害(DoS) の問題
http://jvndb.jvn.jp/ja/contents/2009/JVNDB-2009-002090.html
富士通 複数の TCP の実装におけるサービス運用妨害(DoS) の問題
http://software.fujitsu.com/jp/security/vulnerabilities/vu943657.html

参考:

詳解 TCP/IP Vol.1 プロトコル [新装版] p320-322

マスタリング TCP/IP 入門編 第 4 版 p.213-214

11).TCP 接続状態を操作し維持させることにより、サービス不能状態に陥る問題 (Naptha Attack)

11)-1. 分類:TCP 【IPv4】【IPv6】

11)-2. 概要

存在しない架空のホストと標的のホストの間に大量のセッションを確立させ、TCP 接続の状態を意図的に維持させることにより、標的のホストのリソースが枯渇しサービス不能状態に陥らせることが可能となる。

11)-3. 解説

攻撃手法とその影響

この問題は、RFC793 に記載されている TCP の状態遷移における仕様上の問題を利用した攻撃である。標的のホストと架空のホスト間で TCP セッションを確立し、攻撃者が ESTABLISHED や FIN-WAIT-1 等の TCP 接続の状態(ステート)を意図的に維持/操作することで、サービス不能状態を引き起こす。この問題を利用した攻撃の流れを図 11-1 から図 11-9 で説明する。

図 11-1 に示すように、攻撃者のホスト B は送信元 IP アドレスを架空のホスト C の IP アドレスに偽装し、標的のホスト A に TCP 接続の 3 ウェイハンドシェイクを行うための SYN パケットを送信する。この際、攻撃者のホスト B は架空のホスト C を操作し、大量の SYN パケットを送信する。また、攻撃者のホスト B は後述する標的のホスト A から架空のホスト C に送信されるパケットを受信するために、プロミスキャスモードを有効にする。

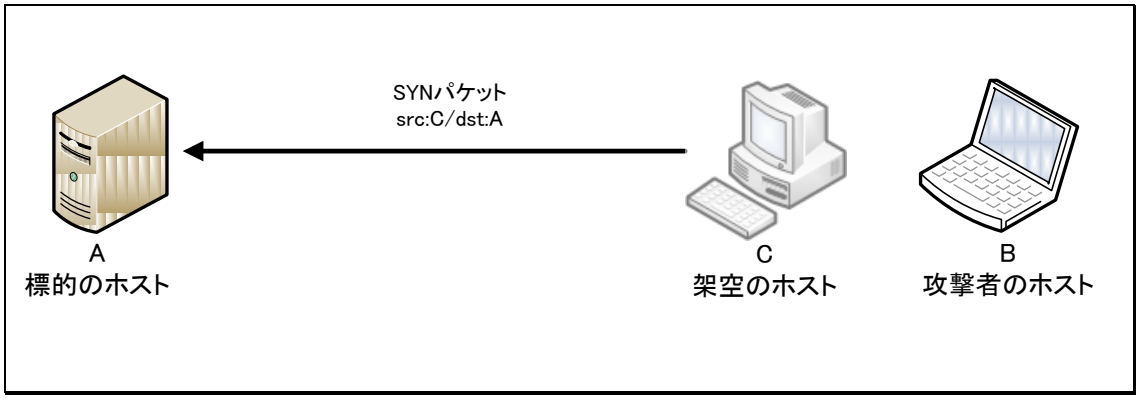


図 11-1 架空のホストからの SYN パケット送信

なお、架空ホスト C に偽装するのは攻撃者の追跡を困難にすることに加え、攻撃者のホスト B 自身のリソースを最小限にして使用することを目的としている。

偽装された SYN パケットを受信した標的のホスト A は、図 11-2 に示すように架空のホスト C に SYN/ACK パケットを送信する。攻撃者は架空のホスト C に送信された SYN/ ACK パケットを攻撃者のホスト B で受信する。

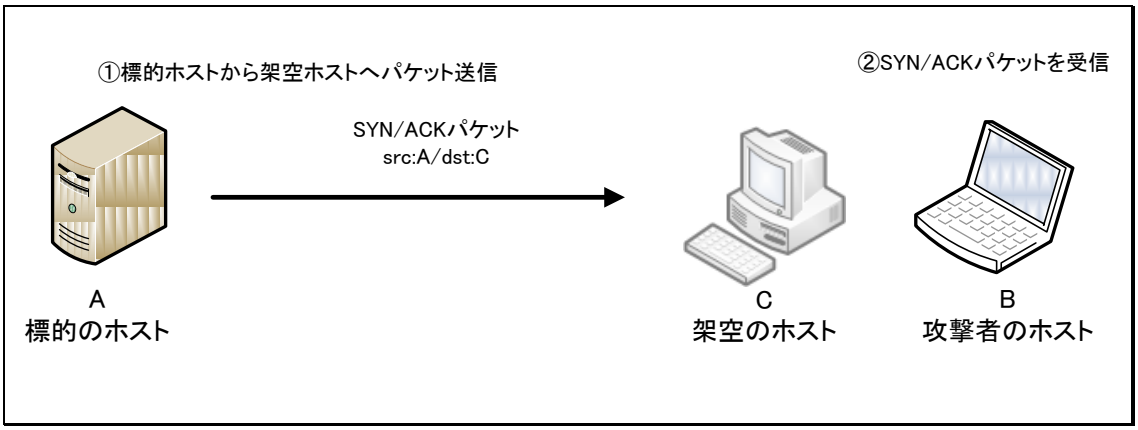


図 11-2 SYN/ACK パケットの受信

図 11-2 の状態後、3 ウェイハンドシェイクを完了させるために攻撃者のホスト B は図 11-3 に示すように送信元 IP アドレスを架空のホスト C に偽装して ACK パケットを標的のホスト A に送信し、TCP セッションを確立させる。

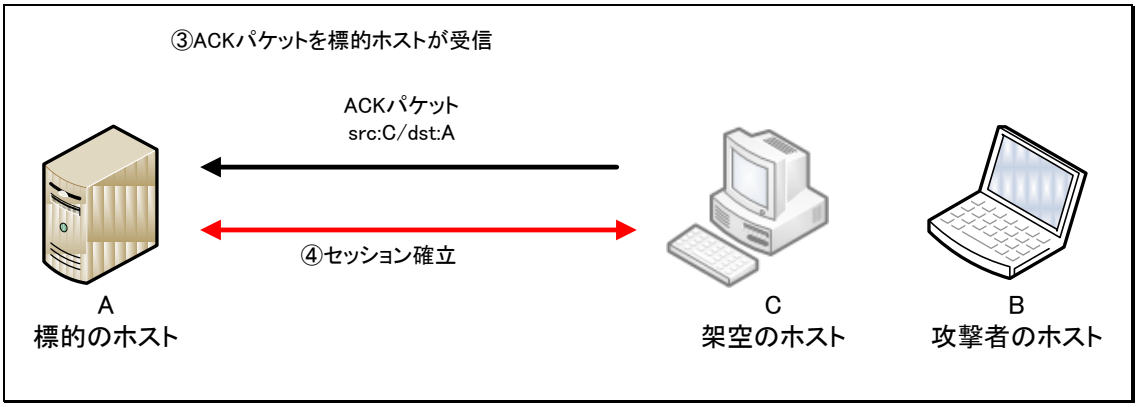


図 11-3 3 ウェイハンドシェイクによるセッションの確立

図 11-1 から図 11-3 では、標的のホスト A および架空のホスト C 間で 3 ウェイハンドシェイクを行い、TCP セッションを確立する。この際の TCP 状態遷移のイメージを以下に示す。

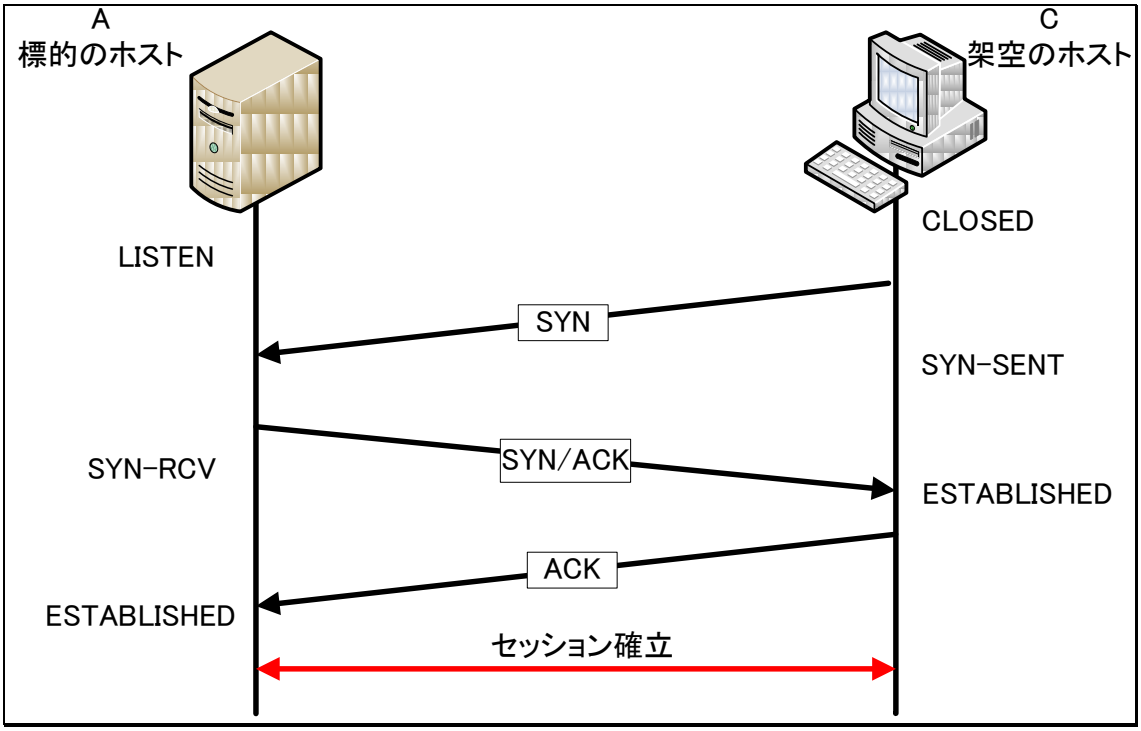


図 11-4　3 ウェイハンドシェイク

標的のホスト A が SYN-RCV 状態から ACK パケットを受信すると、ESTABLISHED 状態に遷移し架空のホスト C との TCP セッションが確立する。この際、本来は個別の接続に関するデータを保持するために、TCB の割り当てや子プロセスの生成を行い、双方ホストではリソースを浪費する。しかし、Naptha Attack では架空のホスト C は攻撃者が作成した実在しないホストのため、標的のホスト A のみが ESTABLISED 状態を維持されたままとなり、リソースを浪費してしまう。

攻撃者は、上記の図 11-1 から図 11-3 の状態を多く作り出して標的のホスト A のリソースをより浪費させるために、図 11-5 のように大量の架空のホストを装い、それぞれの架空のホストが図 11-1 から図 11-3 の手順を繰り返し行えるような環境を用意する。攻撃者のホスト B は、標的のホスト A と架空のホスト C 群での ESTABLISHED 状態が標的ホストの最大セッション数に達するまで SYN パケットを送信し続ける。

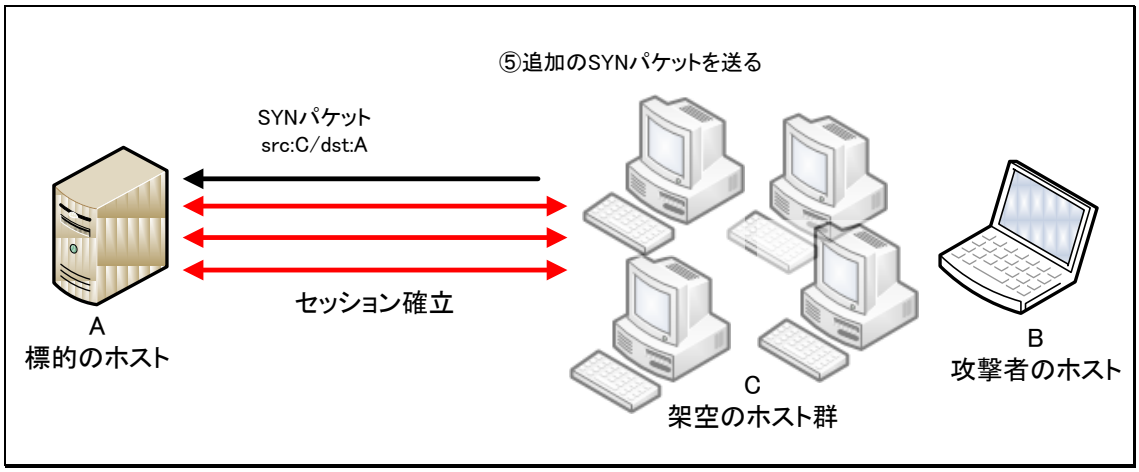


図 11-5　標的のホスト A と架空のホスト C との大量のセッション確立

図 11-6 に示すように標的のホスト A では大量のセッションが確立されているため、リソースが浪費される、あるいはネットワーク帯域が枯渇され、結果としてサービス不能状態に陥る可能性がある。また、標的のホスト A での最大セッション数に達した場合等、製品や標的のホストの設定/環境等によってはハングアップや新たに正常な接続を受け付けられないといった状態に陥る可能性がある。

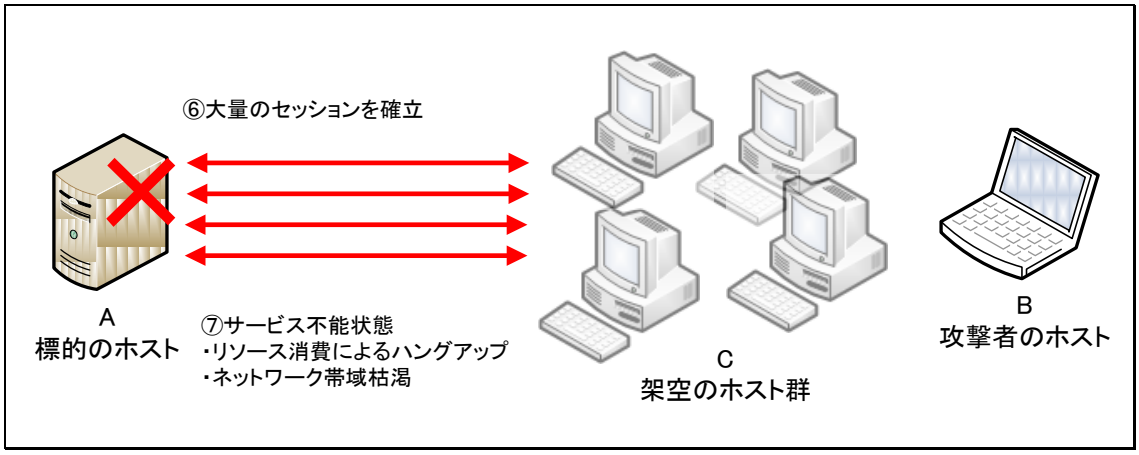


図 11-6　サービス不能状態

ただし、このような状態が標的ホスト側で永久に維持されることを避けるために、OS や製品によっては Keep-Alive という機能が用意されている。

Keep-Alive 機能はまだセッションが有効であるか、セッションを維持すべきなのかを確認するために Keep-Alive パケットを定期的に送信する。通信相手からこのパケットに対する応答(ACK)がなければ、そのセッションを切断して新たな接続を受け付けることができるようになる。
しかし、次に示すような方法で攻撃者はセッションを維持させ、クローズ処理といった次の状態に遷移することを避けることが可能となる。

図 11-7 は標的のホスト A と架空のホスト C 間でセッションが確立された後の状態である。標的のホスト A は自身の Keep-Alive の設定によって、通信相手の架空のホスト C に Keep-Alive パケットを送信する。架空のホスト C に対する通信を受信可能な攻撃者のホスト B は、受信した Keep-Alive パケットの応答として、図 11-3　3 ウェイハンドシェイクによるセッションの確立図 11-3 と同様に送信元 IP アドレスを架空のホスト C の IP アドレスに偽装して ACK パケットを返す。攻撃者は Keep-Alive パケットを受信する度に ACK パケットによる応答を行い、攻撃者は標的のホスト A と架空のホスト C 間のセッションを維持することで攻撃対象のネットワーク帯域の枯渇、リソースの浪費を引き起こすことが可能となる。

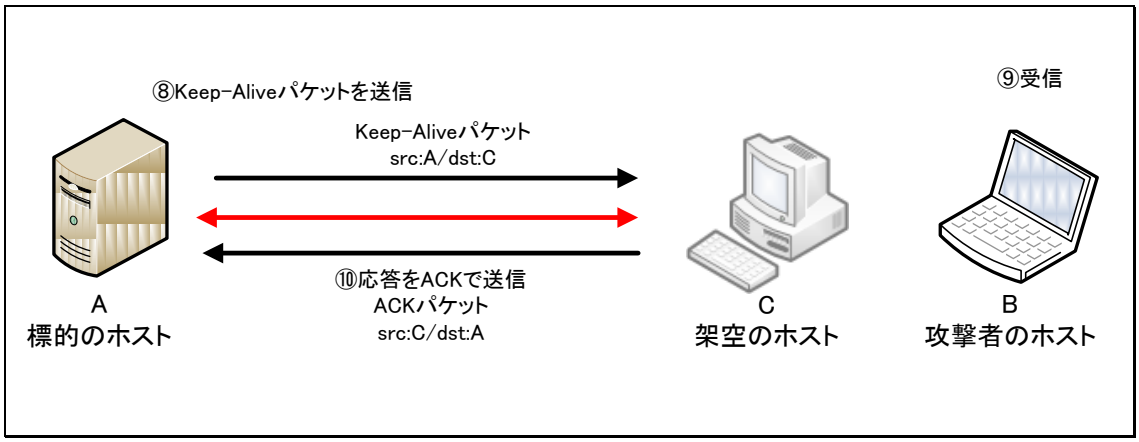


図 11-7　標的のホスト A から架空のホスト C への Keep-Alive パケットの受信

これまでに解説した図 11-1 から図 11-7 までの攻撃手法では、ESTABLISHED 状態を大量に生成し、それを維持させることを試みている。図 11-8 以降では ESTABLISHED 状態後の FIN-WAIT-1 の状態を利用した手法について解説する。

FIN-WAIT-1 とは、セッションを切断(CLOSED)しようとするホストが FIN パケットを送信し、通信相手から ACK パケットが返送されるまで待機している状態のことを指す。TCP セッション切断のイメージを図 11-8 に示す。

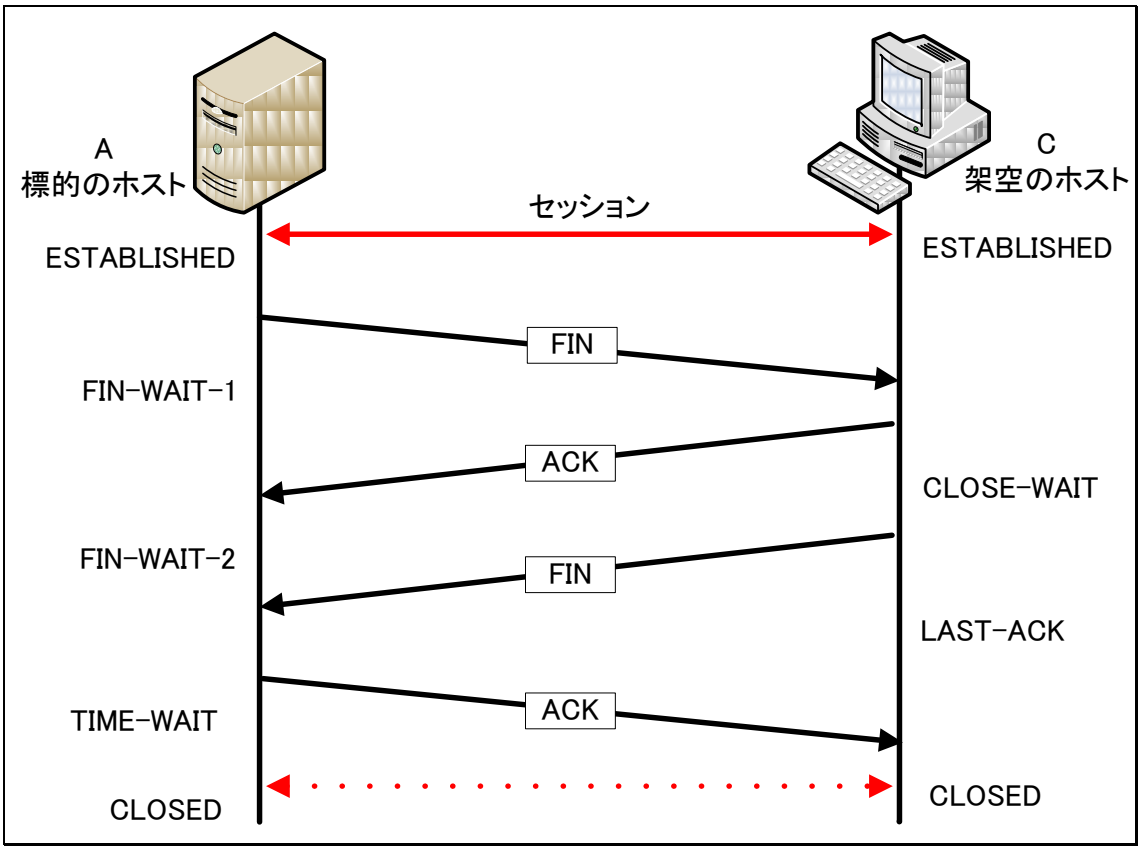


図 11-8　TCP セッション切断

標的のホスト A がセッションを切断するために FIN パケットを架空のホスト C へ送信すると、FIN-WAIT-1 状態に遷移する。その際、架空のホスト C として ACK パケットで応答しないでいると、標的のホスト A は FIN-WAIT-1 状態のまま応答を待つことになる。そして、接続がタイムアウトするまで大量のセッションを確立しておくことで、標的のホスト A の待機状態はリソースを浪費してしまう。このイメージを図 11-9 に示す。

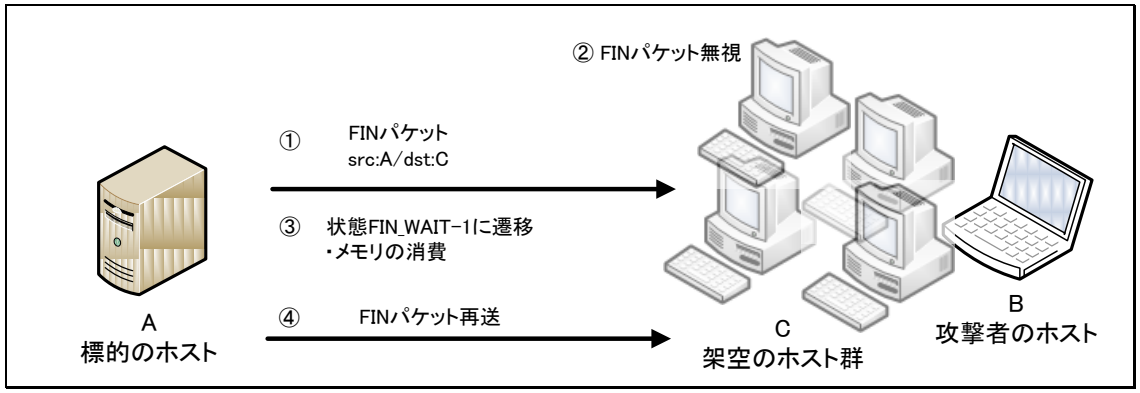


図 11-9 セッション切断要求

ここでは 2 つの TCP 接続状態(ESTABLISHED と FIN-WAIT-1)を利用した攻撃について説明した。TCP/IP スタックの実装によっては、他の TCP 接続状態を利用することで同様のサービス不能状態を引き起こすことが可能となる。それぞれの状態を利用した攻撃に対する影響は TCP/IP スタックの実装によって違いが出るため、製品によっては両方に影響がある製品もあれば、片方のみに影響がある製品も存在する。

原因と考察

この問題は偽装パケットであっても TCP 接続状態を維持させることができてしまう TCP の状態遷移の実装に原因がある。上記では 2 つの TCP 接続状態(ESTABLISHED、FIN-WAIT-1)を使用した解説をしているが、攻撃者はこの状態を維持するため、標的のホストに対し TCP の状態遷移に沿った TCP フラグおよびシーケンス番号を含む偽装パケットを送信する必要がある。これ以外に FIN-WAIT-2 状態を使用する等、他の待機状態の維持を試みることでも同様の攻撃は成立することが考えられる。

ESTABLISHED 状態の維持による影響については、Keep-Alive の実装によって影響度が左右される。TCP の状態遷移の実装において、Keep-Alive は必須の実装として RFC には規定されていないものの、実際に TCP を実装する多くの製品が TCP/IP スタックや TCP サービスのレベルで用意している。Keep-Alive が有効な TCP 実装の場合、この問題の影響は、CPU やメモリリソース、TCP のタイムアウト値や再送回数、最大同時接続数等の他にも、Keep-Alive 関連の設定値(有効な TCP サービスの範囲かどうか、Keep-Alive タイマや Keep-Alive パケットの送出回数および間隔)や RST パケットの送信タイミング等にも関係があると考えられる。このように、如何に実在しないホストとTCP 接続状態を維持するかがこの問題の要点であり、標的のホストの設定や状況等によって影響度が大きく変化するものと考えられる。

11)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題は、米国 BindView 社のセキュリティチーム RAZOR Security Team に所属する Bob Keyes 氏によって 2000 年に報告された問題である。同氏は、ESTABLISHED および FIN-WAIT-1 の 2 つの TCP 接続状態を使用して当時の主要な OS への影響について報告している。この問題の総称として Naptha と名付けており、CERT Advisory CA-2000-21. "Denial-of-Service Vulnerabilities in TCP/IP Stacks"としても注意喚起が行われている。当時は、同じ TCP 接続状態を使用する SYN Flood Attack と比べ、少ないリソースで効果的に DoS 攻撃を試行できる、他の脆弱性との組み合わせや DDoS 攻撃に応用できる、匿名性を持った攻撃が試行できるといった点から、新たな DoS 攻撃として注目を集めた。また 2001 年に入り、同氏によって学習および解説目的として検証用ツールが公開されている。

当時の RAZOR Security Team の報告によると、Naptha Attack で影響を受ける OS は、Compaq 社の Tru64 UNIX V4.0F、FreeBSD 4.0-REL、Linux Kernel 2.0、Hewlett-Packard 社の HP-UX 11.00、Microsoft 社の Windows 95、98、98SE(注 1)と Windows NT 4.0 SP6a がある。なお、NT 以外の Windows は FIN-WAIT-1 のみ、Windows NT は ESTABLISHED および FIN-WAIT-1、それ以外は ESTABLISHED のみを使用した攻撃に影響があると報告されている。一部ベンダからパッチが提供されているが、その他影響を受けるベンダの対応状況について詳細は不明である。

また現在の主要な OS バージョンへの影響については詳細不明であるが、TCP の仕様上この問題を完全に排除することはできていないため、影響を受ける可能性がある。しかし、一方では Keep-Alive の実装や TCP タイムアウト値、再送設定等については依然議論されており、TCP/IP スタックや TCP サービスにおいて、一般的な DoS 攻撃の対策と共に設定値の最適化や改良が検討されているものと考えられる。

注 1: MicroSoft セキュリティ情報「不完全な TCP/IP パケットの脆弱性に対する対策(MS00-091)」において、Windows Me 用の対処策も公開されている。

11)-5. IPv6 環境における影響

この問題は TCP プロトコル上の問題で、OSI 参照モデルのトランスポート層に属する問題であるため、IP プロトコルのバージョンに限らずこの問題は再現すると考えられ、IPv6 環境でも影響を受ける可能性がある。

11)-6. 実装ガイド

この問題は RFC793 で規定されている TCP の状態遷移の実装による問題であるため、仕様に従う限り、この問題を完全に排除することは出来ない。しかし、次のような実装や設定項目を導入検討することにより、問題を回避あるいは影響を緩和することが可能である。ただし、正常な通信との区別が困難であることや標的のホスト側のパフォーマンス等にも影響があることから、実装には十分な注意が必要である。

1. 想定されていない送信元 IP アドレスからのパケットを破棄する。
2. サーバのリソースが復元するまで新しい TCP 接続の数を制限する。
3. 実在しない IP アドレスからの大量の TCP セッションの確立や維持を試みる通信を異常と判断するアルゴリズムを実装し、不要な通信を破棄/制限する。なお、設定値を可能な限り小さくすることで影響が緩和することが可能となる。
   - TCP セッションの各状態における、タイムアウト値や再試行の回数等。
   - Keep-Alive パケットの送信間隔や送信回数。
   - 製品自体、あるいは同一の送信元 IP アドレスから接続可能な最大セッション数。

11)-7. 運用ガイド

1. 影響を受ける製品に対して各ベンダより提供されているパッチの適用や問題が修正されたファームウェアにバージョンアップする。

2. 発見者によって提示されている次のような対策を実施する。
   - 不要な TCP サービスを停止する。
   - ファイアウォール等で TCP ポートに対するパケットフィルタリングを実施する。
   - UNIX における inetd 等の、サービス制御ツールを使用して TCP 接続の受け付けにおいて TCP サービスの接続数の制限や許可/拒否の制御を実施する。
   - RFC 2827 において示されているような、送信元 IP アドレスを偽装した DoS 対策を実施する。
   - TCP タイムアウトの時間を短くする、Keep-Alive タイマを短く設定し、Keep-Alive パケットの送信間隔を短くする。

11)-8. 参考情報

この問題についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本問題調査時点(2010 年 5 月)のものである。

1981 年 RFC793, TRANSMISSION CONTROL PROTOCOL.
http://www.ietf.org/rfc/rfc0793.txt

1998 年 RFC2827, Network Ingress Filtering:
Defeating Denial of Service Attacks which employ IP Source Address Spoofing
http://www.ietf.org/rfc/rfc2827.txt

2000 年 The NAPTHA DoS vulnerabilities
http://www.packetstormsecurity.org/0012-exploits/bindview.naptha.txt
マイクロソフト Microsoft Security Bulletin(MS00-091)
http://www.microsoft.com/technet/security/bulletin/ms00-091.mspx
Beyond Security The NAPTHA DoS vulnerabilities
http://www.securiteam.com/securitynews/6B0031F0KA.html
NEOHAPSIS NAPTHA Advisory Updated Bind View RAZOR
http://archives.neohapsis.com/archives/win2ksecadvice/2000-q4/0105.html
CERT Advisory CA-2000-21 Denial-of-Service Vulnerabilities in TCP/IP Stacks
http://www.cert.org/advisories/CA-2000-21.html

2000 年 Common Vulnerabilities and Exposures CVE-2000-1039
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2000-1039
NIST Vulnerability Summary for CVE-2000-1039
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1039

2006 年 Guardian Security IPv6 approach for TCP SYN Flood attack over VoIP, Part II
http://www.linuxsecurity.com/content/view/121124/49/

2009 年 CPNI TECHNICAL NOTE
http://www.cpni.gov.uk/Docs/tn-03-09-security-assessment-TCP.pdf
Naptha TCP State Exhaustion Testing With Network Expect
http://netexpect.org/wiki/Naptha
Security Focus Multiple Vendor TCP/IP Resource Exhaustion Vulnerability
http://www.securityfocus.com/bid/2022

12).パケット再構築時にバッファが溢れる問題(Ping of death)

12)-1. 分類:ICMP 【IPv4】【IPv6】

12)-2. 概要

フラグメント化された ICMP Echo パケットを再構築する際に、データサイズのチェックを行っていない場合、バッファオーバーフローが発生する恐れがある。

12)-3. 解説

攻撃手法とその影響

この問題を悪用して行われる攻撃は、フラグメント化される程充分に大きい ICMP Echo パケットを攻撃対象のホストに送信することにより攻撃を行うことができる。

この問題で行われ得る攻撃の流れを、図 12-1 から図 12-4 に例示する。

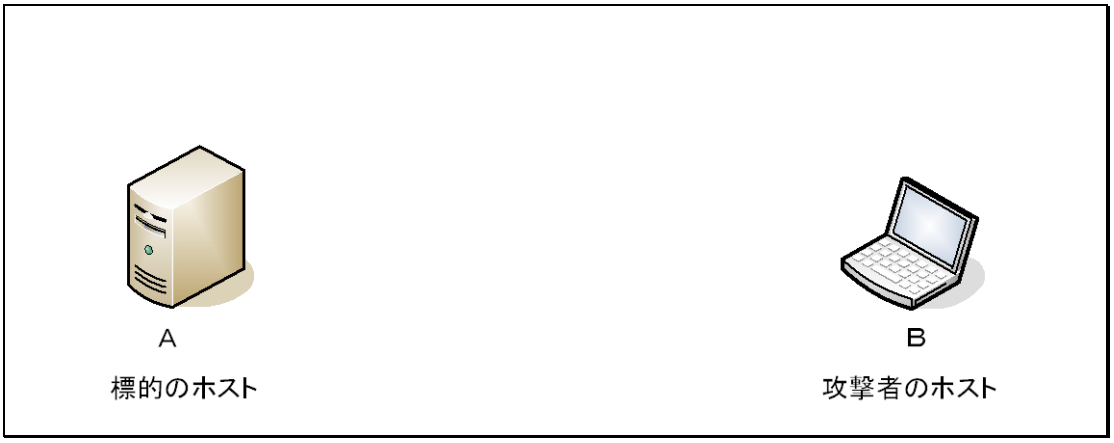


図 12-1 ターゲットネットワーク

攻撃者は、ホストBからフラグメント化される程充分に大きい ICMP パケットを、攻撃対象のホストAに対して送信する。

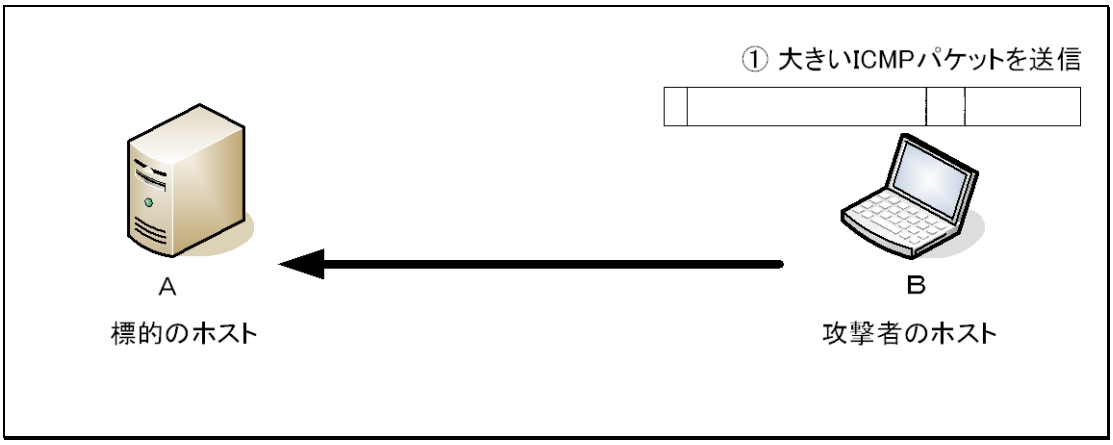


図 12-2 攻撃 ICMP パケットの送信

送信された ICMP パケットはフラグメント化され、攻撃対象のホストAに到達する。

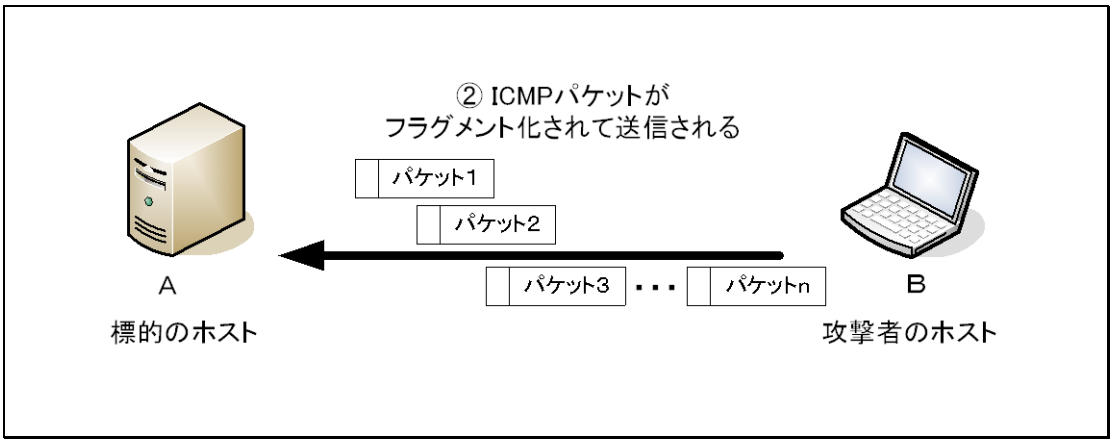


図 12-3 ICMP パケットのフラグメント化

攻撃対象のホストAはフラグメント化されたICMPパケットを再構築しようとする。この時、バッファが溢れシステムクラッシュ、リブートなどが起きる。

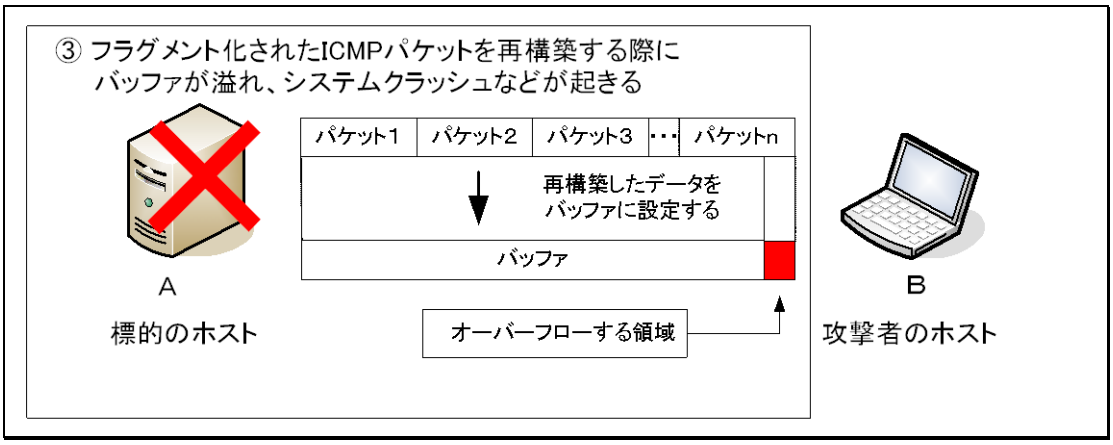


図 12-4 ICMP パケットの再構築

原因と考察

この問題は多くで利用されているRFC791のパケット再構築のアルゴリズムを利用した攻撃である。ネットワーク上にデータを転送するとき、ネットワークによって決められている最大伝送単位(MTU : Maximum Transmission Unit)を超えるようなIPパケットは、複数の小さなIPパケット(フラグメント)に分割して送信先ホストに送信される(図 12-6 を参照)。フラグメント処理はMTUの長さで分割して届けられ、受信ホストでは全てのフラグメントパケットが届くまでフラグメントデータは確保されたバッファ(キュー)に格納される。

IPパケット再構築(Reassembly)処理については RFC 791 と RFC 815 に示されている。RFC791のパケット再構築処理は、各フラグメントパケットのIPヘッダ中のフラグメント・フラグ(More Fragment: MF)とフラグメントオフセット(Fragment Offset: FO)、パケット長を使用する。図 12-5 を参照)

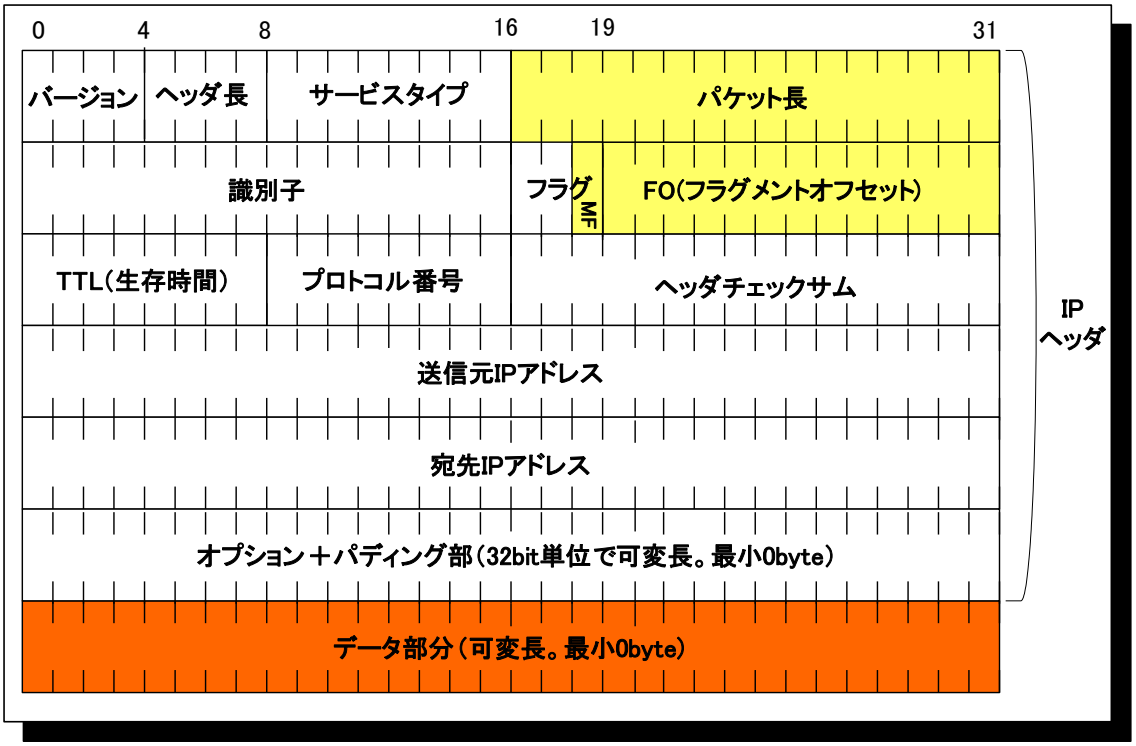


図 12-5 IP データグラムフォーマット

IP パケットを受け取ると、まず MF、FO からフラグメントパケットかどうかが確認され、上位プロトコルにデータを渡すために幾つかの手順を経てパケットの再構築処理が行われる。

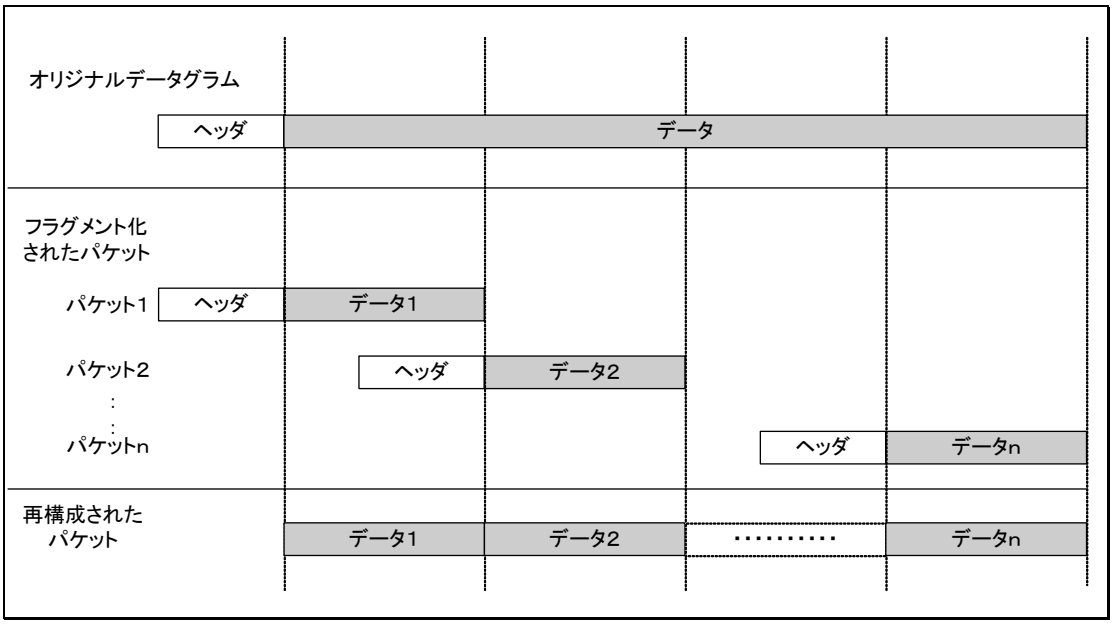


図 12-6 フラグメント処理状態遷移

IP パケットのデータ領域としての最大許容可能サイズは、IP パケットの最大サイズからヘッダ情報のサイズを差し引いたものとなる。IP パケットに含まれるヘッダ情報は次のとおりとなっており、IP オプションが特に指定されていない場合は IP パケットには 20 オクテットのヘッダが含まれている。(RFC791)また ICMP Echo リクエストには 8 オクテットの ICMP ヘッダ情報が含まれている。(RFC792)よって、データ領域の最大の許容できるサイズは 65535-20-8 = 65507 オクテットとなる。

これより、ICMP リクエスト送信からバッファ溢れまでの過程を図 12-7 から図 12-9 に例示する。ホストBがホストAに、65507 オクテットを超えるサイズの ICMP Echo リクエストのパケットを送ることにより、パケットがフラグメント化されてホストAに送信される。(図 12-7 を参照)

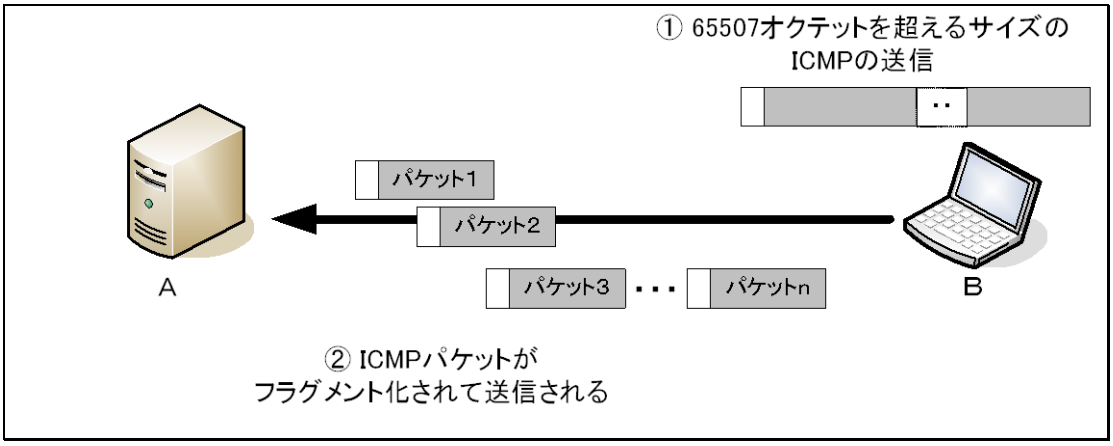


図 12-7 パケットのフラグメント化

受信ホストAではフラグメント化されたパケットを再構築しようとする。再構築の位置はパケット中のオフセット値を元に、個々のフラグメント化されたパケットがどの場所かを決定する。(図 12-8 を参照)

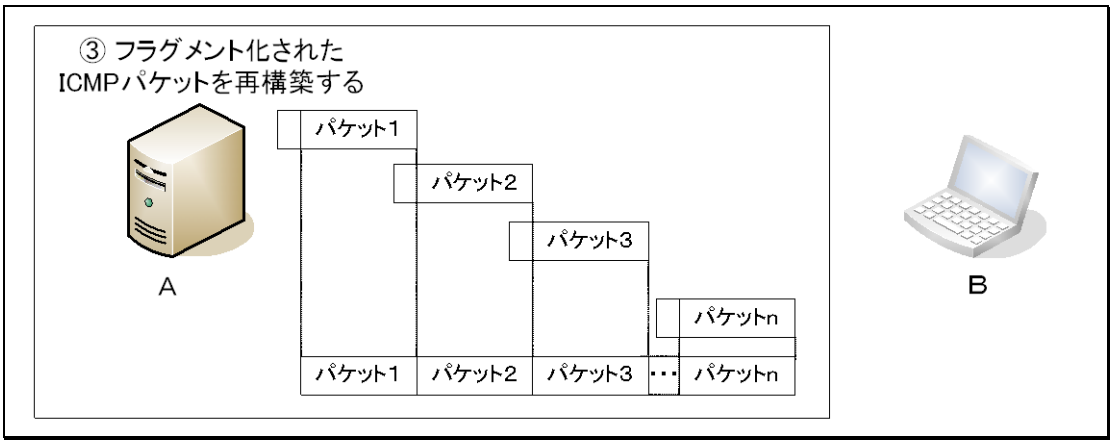


図 12-8 パケットの再構築

最後の断片に含まれるオフセット値に基づいて再構成した時に、断片化されたサイズ(offset + datasize)が 65535 より大きいサイズに結合されてしまうことで 16 ビットの内部変数がオーバーフローし、システムクラッシュ、リブートやカーネル・ダンプのような事態が引き起こされる。(図 12-9 を参照)
この問題はプロトコルスタックの実装のバグを利用した攻撃と言える。

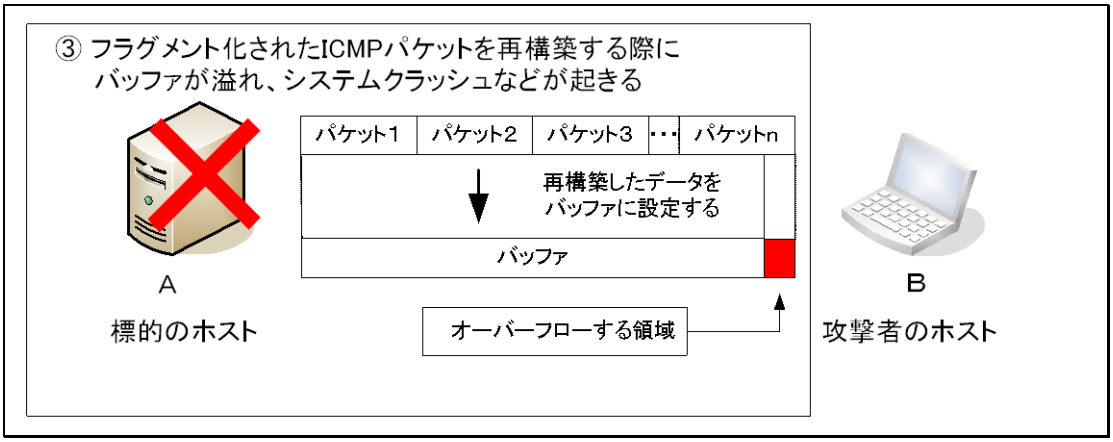


図 12-9 バッファの溢れ

12)-4. 発見の経緯とトピック、対策の動き、現在の動向

Ping of death は、1996 年に CERT Advisory CA-1996-26 Denial-of-Service Attack via ping として注意喚起されている。この攻撃手法により Windows のみならず、マッキントッシュや、UNIX を使ったシステムやファームウェアにも多くの被害をもたらした。

現時点では、ほとんどの OS 等で対応策が取られている。ただし、バージョンの古い OS 等ではパッチが必要な場合もある。

12)-5. IPv6 環境における影響

IPv6 のパケット再構築のアルゴリズムは、IPv4 とのパケット構造やフラグメント化の方法が異なり違いはあるが、IPv4 同様にパケットのサイズチェック(IPv6 最大のペイロードサイズ(注 1)) を超える ICMP Echo パケットを破棄する対処が行われていない場合は IPv6 環境でも影響を受ける可能性がある。しかし、既にほとんどの OS で IPv4 の対応策が取られていることから、IPv6 サポートの時点で既に脆弱性は排除されている製品も存在すると考えられる。

なお、IPv6 では RFC 1883 で示されているように長いペイロードを持つ IPv6 パケットを送るために使われるオプション(注 2)が用意されており、通常の 65535 より大きなペイロードを持つ IPv6 パケットをジャンボグラム(注 3)と呼んでいる。ジャンボグラムを IPv6 でサポートする場合には、この扱いについても TCP/IP 実装面において十分な配慮が必要であると言える。

注 1: IPv6 の最大ペイロードサイズは、IPv6 拡張ヘッダと上位層プロトコル データ単位を合わせたものとなり、通常は 65,535 オクテットのペイロードとなる

注 2: Jumbo Payload(ジャンボペイロード)オプションといい、IPv6 の拡張ヘッダであるホップバイホップオプションヘッダ中に含まれる

注 3: ジャンボグラムについては RFC 2675 で示されており、65,536 オクテットから 4,294,967,295 オクテットのペイロードを持つ IPv6 パケットの転送を許す

12)-6. 実装ガイド

1. パケットのサイズチェックを行う。65507 オクテットを超えるサイズの ICMP Echo パケットが送られてきた場合は破棄する。
2. パケットサイズを規定し、規定したサイズより大きいパケットは破棄する。パケットを破棄したら送信元に対し ICMP でエラーを通知する。

12)-7. 運用ガイド

1. 影響を受ける製品を使用している場合は各ベンダより提供されているパッチを適用して、脆弱性を排除する。
2. 使用している製品において、本脆弱性をチェックする機能が付属されている場合はその機能を有効にする。
3. 現在、使用している製品に本脆弱性の存在が確認されているが、ベンダでのパッチ配布などのサポートがない場合、該当製品の手前に本脆弱性を排除する機器を導入する。

12)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1981 年 RFC 791, Internet Protocol.
http://www.ietf.org/rfc/rfc0791.txt
RFC 792, Internet Control Message Protocol.
http://www.ietf.org/rfc/rfc0792.txt

1989 年 RFC 1122, Requirements for Internet Hosts - Communication Layers.
http://www.ietf.org/rfc/rfc1122.txt
RFC 1812, Requirements for IP Version 4 Routers.
http://www.ietf.org/rfc/rfc1812.txt
RFC 2644, Changing the Default for Directed Broadcasts in Routers.
http://www.ietf.org/rfc/rfc2644.txt
http://www.ipa.go.jp/security/rfc/RFC2644JA.html
Insecure – Ping of Death
http://www.insecure.org/sploits/ping-o-death.html
CERT Advisory CA-1996-26
http://www.cert.org/advisories/CA-1996-26.html

1995 年 RFC 1883, Internet Protocol, Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc1883.txt
RFC 2675, IPv6 Jumbograms
http://www.ietf.org/rfc/rfc2675.txt

1997 年　ISS X-Force Database(95)
http://xforce.iss.net/xforce/xfdb/95
Common Vulnerabilities and Exposures CVE-1999-0128
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0128
Common Vulnerabilities and Exposures CVE-1999-0345
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0345
Linux.com - IP パケットのフラグメント
http://japan.linux.com/kernel/internal24/node227.shtml
SecurityFocus 1240
http://www.securityfocus.com/bid/1240
ISS X-Force Database(4532)
http://xforce.iss.net/xforce/xfdb/4532

2003 年　ISS X-Force Database(12555)
http://xforce.iss.net/xforce/xfdb/12555

2006 年　Cisco - アクセス コントロール リスト(ACL)と IP フラグメント
http://www.cisco.com/support/ja/105/acl_wp.shtml

年代不明 ISS X-Force Database(13828)
http://xforce.iss.net/xforce/xfdb/13828

参考　　マスタリング TCP/IP IPv6 編 第 1 版　p.49-p68

13).ICMP Path MTU Discovery 機能を利用した通信遅延の問題

13)-1. 分類:ICMP 【IPv4】【IPv6】

13)-2. 概要

Path MTU Discovery 機能を悪用し、偽装された ICMP パケットにより 2 点間の通信の MTU 値が変更されることで、通信にスループットの低下による通信遅延が発生する恐れがある。

13)-3. 解説

攻撃手法とその影響

Path MTU Discovery 機能は、あらかじめ経路 MTU(PMTU: Path Maximum Transmission Unit)を発見し、送信元ホストで Path MTU の大きさにデータを分割してから送信する方法で、RFC 1191 にて規定されている。この方法を悪用し、送信元ホストに細工された Path MTU を設定させることで、通信に影響を与える可能性がある。

攻撃は以下のパターンで行われる。図 13-1 および図 13-2 に攻撃の概要を示す。

1. IP レベルで通信可能な 2 つのホスト A,B が存在する。
2. 攻撃者 C は、B に対し、送信元 IP を A に偽装し、ICMP echo request パケットを送信する。
3. B はハッシュテーブルに新しいエントリを作成する。

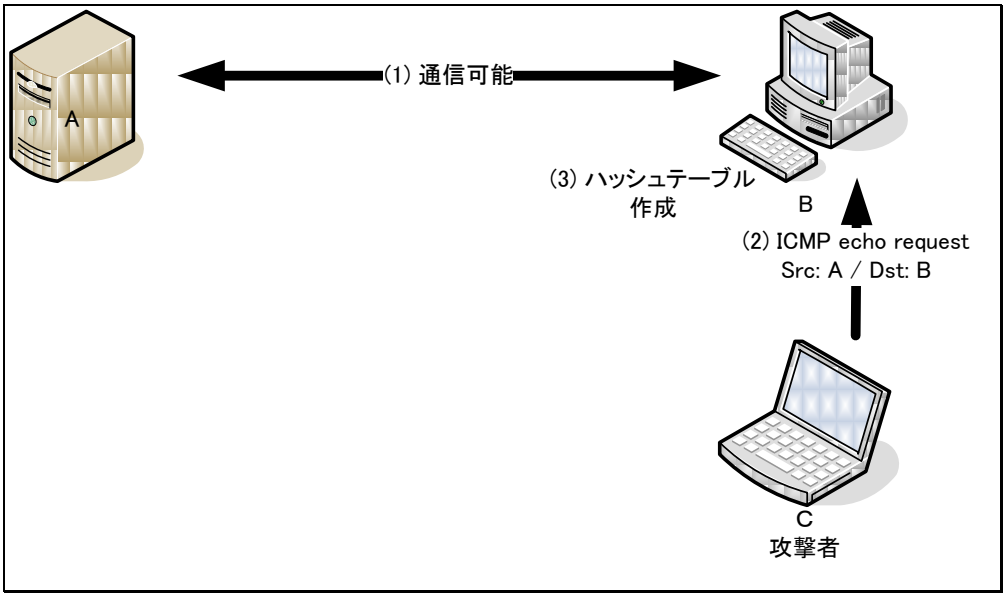


図 13-1 ICMP Path MTU Discovery を利用した通信遅延(第一段階)

4. C は B に対し、送信元 IP を A に偽装し、ヘッダ長+α 程度の小さい MTU 値の情報を持った ICMP “Fragmentation Needed and Don’t Fragment was Set”(Type = 3, Code = 4) パケットを送信する。
5. B は受信した ICMP パケットを元に新しい MTU 値を設定する。

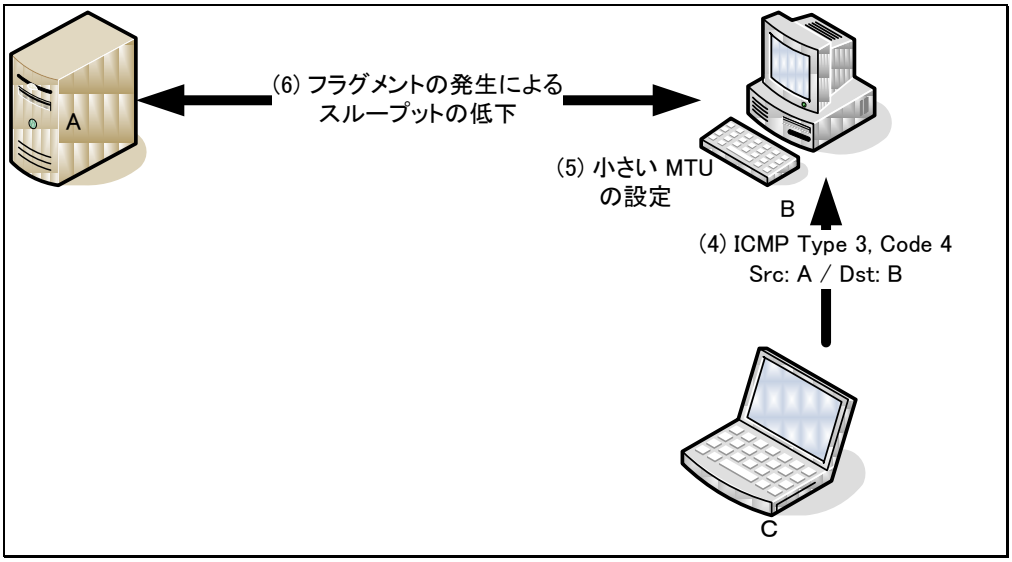


図 13-2 ICMP Path MTU Discovery を利用した通信遅延(第二段階)

この結果、MTU 値がクリアされないようにこれらのパケット送信を繰り返すことにより、A-B 間の通信で大量の断片化が発生するなどでスループットが非常に低下し、タイムアウト等が発生する可能性がある。

原因と考察

Path MTU Discovery は以下のように処理される。処理の流れを図 13-3 に示す。

1. IP ヘッダ中の分割化禁止フラグを設定しパケットを送信する。
2. 途中のルータは、分割処理が必要となっても分割処理を行わず、パケットを破棄する。
3. 同時に、ICMP(type = 3、code = 4)パケットにより次の MTU 値が送信元に通知される。
4. ICMP により通知された MTU 値を、Path MTU 値として利用し、その値をもとに送信元ホスト上で分割化処理が行われる。
5. RFC 1191 では、Path MTU 値は約 10 分間キャッシュすることになっている。

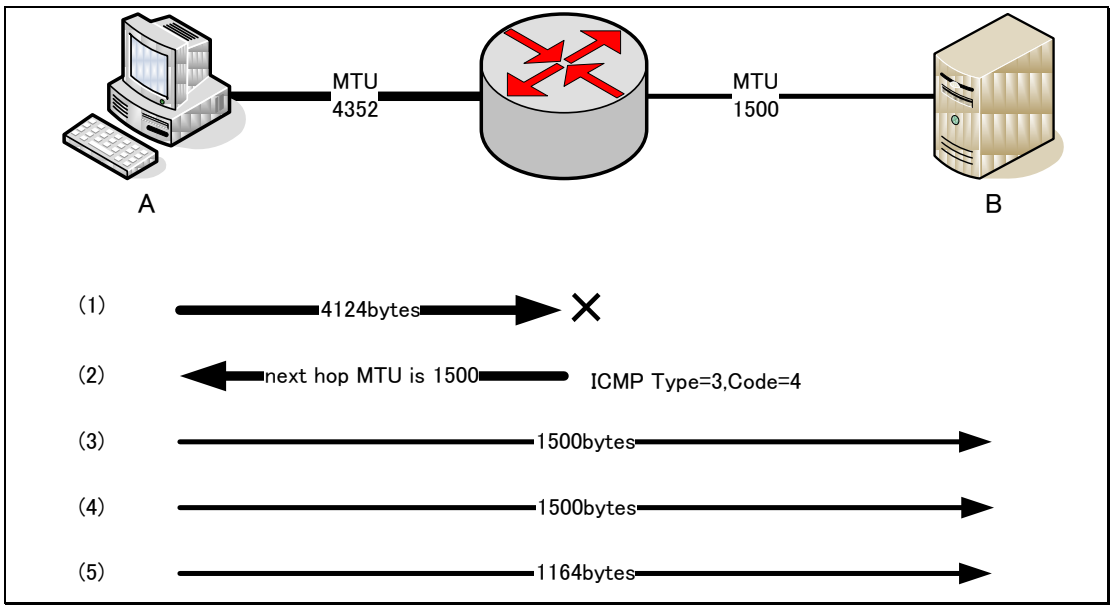


図 13-3 Path MTU Discovery の仕組み

通信が発生している間に ICMP パケットを受信すると、MTU が ICMP パケットに指定された値に変更され、以降通信が継続する。例えば、MTU 値がヘッダ長+α 程度に小さい場合には IP パケットが大量に分割化し、通信速度の低下や通信のタイムアウトが発生する恐れがある。

13)-4. 発見の経緯とトピック、対策の動き、現在の動向

1990 年に RFC 1191 が提案されたが、この時点で攻撃の可能性が指摘されていた。2001 年に Bugtraq メーリングリスト上で antirez がこの問題を指摘した。2004 年に Gont により攻撃への対策が提示された。2005 年に各製品ベンダが他の問題に対する対策を含めたパッチをリリースした。

13)-5. IPv6 環境における影響

この問題は、ICMPv4 のハードエラーメッセージ “Fragmentation Needed and Don’t Fragment was Set”(Type = 3, Code = 4)を利用してPath MTUを変更し、不要なフラグメントによって通信遅延を発生させる問題である。ICMPv6 には上記 ICMPv4 エラーメッセージ(Type = 3, Code = 4)に相当するメッセージとして ICMPv6 エラーメッセージ”Packet too Big”(Type = 2, Code =0)がある。

IPv6 の Path MTU Discovery は RFC1981 に規定されており、IPv4 とは異なる。IPv6 では RFC 中継点のルータでパケットの分割はさせないことにし、送信ノード(ホスト)でパケット分割が行われるが、ICMPv6 エラーメッセージ”Packet too Big”は中継点のルータが自分に設定された MTU よりも大きなパケットが来た場合に発信元に通知され、Path MTU が設定し直してからパケットを再送する仕組みになっている。ICMPv4 のハードエラーメッセージと同様に偽装した ICMPv6 エラーメッセージ”Packet too Big”を利用することで Path MTU が置き換えられる可能性があるため、IPv6 においても ICMPv6 エラーメッセージにより通信遅延の影響を受ける可能性があり、一部のベンダにおいては ICMPv4 の修正と併せて ICMPv6 での対処が行われている。

13)-6. 実装ガイド

仕様上の問題であり、実装上で対策する手段がない。

13)-7. 運用ガイド

1. MTU 値の下限を決め、それ以下のサイズにパケットが分割されないようにする。RFC 1191 では 68 バイトを最小値としている。
2. ホスト上で Path MTU Discovery 機能を無効化する。
3. ファイアウォールまたはルータで、不要な ICMP パケットを遮断する。
4. OS によっては、ベンダよりパッチ等がリリースされているので、適用する。

13)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1990年 RFC 1191, Path MTU Discovery.
http://www.ietf.org/rfc/rfc1191.txt

1996年 RFC 1981, Path MTU Discovery for IP version 6
http://www.ietf.org/rfc/rfc1981.txt

2001年 ICMP fragmentation required but DF set problems.【antirez 著】
http://archives.neohapsis.com/archives/bugtraq/2001-01/0231.html.
New Denial of Service attack exploits special ICMP flags
http://www.securiteam.com/securitynews/5AP0D2A35U.html.
ISS X-Force Database icmp-pmtu-dos(5975)
http://xforce.iss.net/xforce/xfdb/5975
Common Vulnerabilities and Exposures CVE-2001-0323
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0323

2004年 ICMP attacks against TCP【Gont 著】
http://www.gont.com.ar/drafts/icmp-attacks-against-tcp.html
Common Vulnerabilities and Exposures CVE-2004-1060
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1060

2005年 NISCC Vulnerability Advisory ICMP – 532967
http://www.cpni.gov.uk/docs/re-20050412-00303.pdf?lang=en

Cisco Security Advisory: Crafted ICMP Messages Can Cause Denial of Service
http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml
[security bulletin] SSRT4743, SSRT4884 rev.1 - HP Tru64 UNIX TCP/IP remote Denial of Service(DoS)
http://marc.theaimsgroup.com/?l=bugtraq&m=112861397904255&w=2
[security bulletin] SSRT4884 HP-UX TCP/IP Remote Denial of Service(DoS)
http://www.securityfocus.com/archive/1/archive/1/418882/100/0/threaded
マイクロソフトセキュリティ情報 MS05-019

http://www.microsoft.com/japan/technet/security/bulletin/MS05-019.mspx
Open Vulnerability and Assessment Language OVAL2188
http://oval.mitre.org/oval/definitions/data/oval2188.html
Open Vulnerability and Assessment Language OVAL3826
http://oval.mitre.org/oval/definitions/data/oval3826.html
Open Vulnerability and Assessment Language OVAL780
http://oval.mitre.org/oval/definitions/data/oval780.html
TCP 実装の ICMP エラーメッセージの処理に関する脆弱性の問題について
(古川電工)
http://www.furukawa.co.jp/fitelnet/topic/icmp_attacks.html

2006 年　TCP Remote ICMP Denial Of Service Vulnerabilities
ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2006.4/SCOSA-2006.4.txt
SCO OpenServer ICMP Message Handling Denial of Service
http://secunia.com/advisories/18317

参考　マスタリング TCP/IP　入門編　第 3 版　p.134
マスタリング TCP/IP　IPv6 編　第 1 版　p.68-81

14).ICMP リダイレクトによるサービス応答遅延の問題

14)-1. 分類:ICMP 【IPv4】【IPv6】

14)-2. 概要

ホストやルータに対し、偽装された ICMP リダイレクトメッセージ(Type = 5)が送信されることにより、ルーティングテーブルが書き換わり、サービス不能状態になる。

14)-3. 解説

攻撃手法とその影響

ICMP リダイレクトメッセージ(Type = 5)はルータやホストに対してルーティング変更を指示するメッセージである。これを悪用することで、ルータやホストのルーティング情報を書き換えることが可能である。ICMP リダイレクトメッセージを悪用した攻撃には次の 2 種類の攻撃手法が想定される。

1つ目は、攻撃者はからホスト A に対して通信を全てホスト A 自身へ通信が行われるように不正な ICMPリダイレクトメッセージ送信する。これによりルーティング情報が書き換えられたホストAは通信を全て自身宛てに送信する。その後も、定期的に不正な ICMP リダイレクトメッセージを送信することで、このルーティング情報が解除されない限りホスト A は通信不能な状態となる。攻撃イメージを図 14-1 攻撃のイメージに示す。

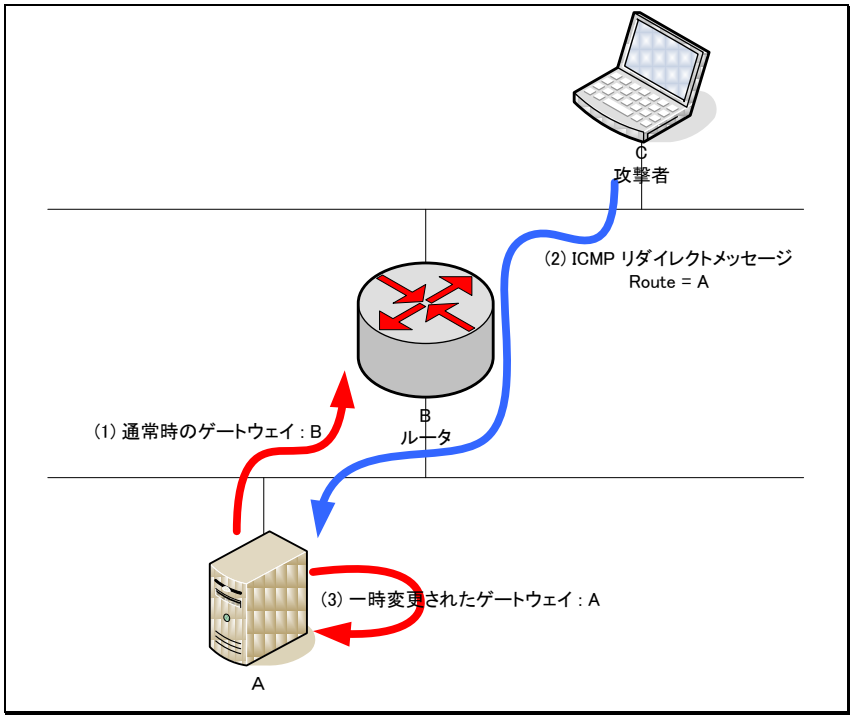


図 14-1 攻撃のイメージ

2 つ目については、攻撃者は ICMP リダイレクトメッセージを大量にホスト A へ送りつけることでルーティングテーブルを肥大化させ、ホスト A のリソースを枯渇させることができる。攻撃者は不正な ICMP リダイレクトメッセージを送信し続けることにより、ホスト A を動作不能状態にすることが可能である。

原因と考察

ICMP リダイレクトメッセージはパケットの経路情報をやり取りするために利用され、以下のように一時的にルーティングテーブルを追加することができる。

1. ホスト A からホスト B へパケットを送信する。
2. ホスト A のデフォルトゲートウェイはルータ 1 と設定されているため、パケットをルータ 1 へ送信する。
3. ルータ 1 はパケットを受け取るがホスト B がルータ 2 の先にあるため、ルータ 2 へパケットを転送する。
4. ルータ 1 はホスト A へ ICMP リダイレクトメッセージを利用し、今後ホスト B へパケットを送信する際はルータ 2 を利用するよう指示する。
5. ホスト A は ICMP リダイレクトメッセージを受け取り一時的にこの経路情報をルーティングテーブルへ追加し、その後に同じ送信先へパケットを送る際にこの情報を利用する。

以上の通信の流れを図 14-2 に示す。

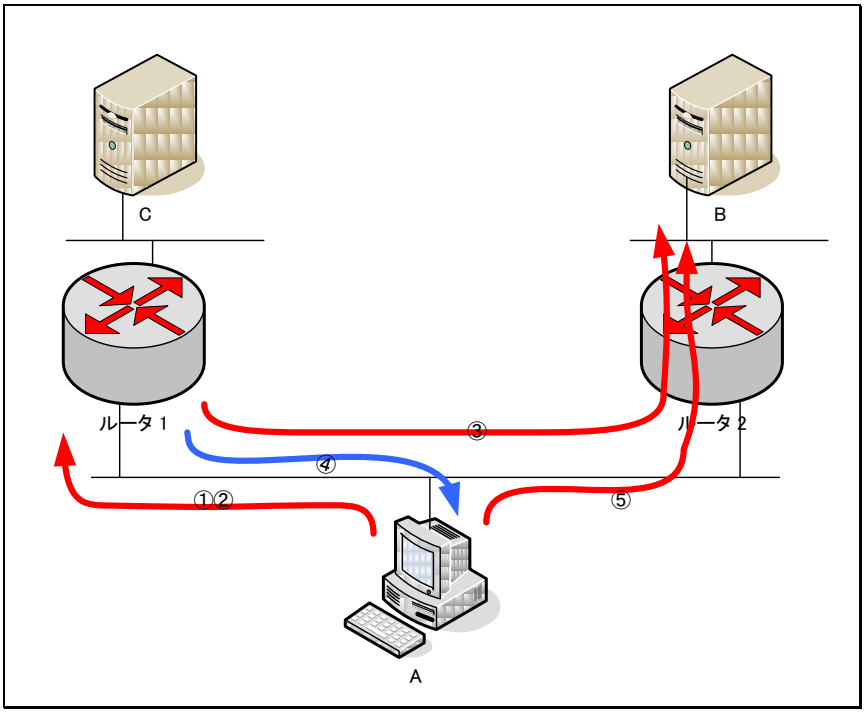


図 14-2 ICMP リダイレクトメッセージの仕組み

もし ICMP リダイレクトメッセージが不正な場合、ルーティング情報が不適切に書き換わることに起因し、通信が不能になる恐れがある。また、古いルータ製品などでは、ルーティング情報の保持領域にサイズ制限がないことから、ルーティング情報が肥大化しリソースが枯渇する恐れがある。

14)-4. 発見の経緯とトピック、対策の動き、現在の動向

ICMP リダイレクトメッセージの仕様は ICMP プロトコル自体とともに 1981 年に決められた。 1999 年にルーティングを変更する攻撃ツールである Winfreeze が公開された。2002 年にルーティングテーブル肥大化によるリソース枯渇の問題が公開された。

14)-5. IPv6 環境における影響

IPv6 における IPv4 の ICMP リダイレクトメッセージに相当する機能は、RFC2461 に規定されている近隣探索プロトコル(NDP:Neighbor Discovery Protocol)で提供される。近隣探索は、ICMPv6 を使用して 3 種類 5 タイプのメッセージで機能を実現し、その中の 1 つのメッセージタイプに ICMPv6 リダイレクトメッセージ(Type =137)がある。概念的には IPv4 と同じ手法での攻撃が可能であり、IP プロトコルのバージョンに限らず問題が再現すると考えられ、IPv6 環境でも影響を受ける可能性がある。

補足資料

IPv6 環境では IPv4 での対策に加え、以下のような対策を施すことで IPv6 のセキュリティの向上を図ることができる。

・ルータを超えて送られる近隣探索パケットを破棄する

IPv4 ではルータを超えて別ノードから ICMP リダイレクトメッセージを送ることが可能であるが、IPv6 の近隣探索パケットは、IPv6 ヘッダ内における最大ホップ数として 255 という特別な値が使われる。(注 1)これは、別ノードから送られる近隣探索パケットであることを表す。図 12-3 に IPv6 ヘッダを示す。

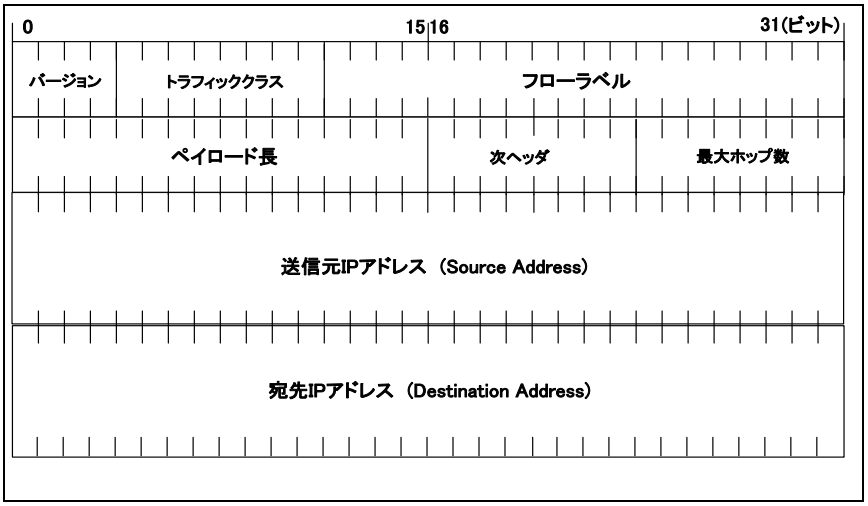


図 14-3 IPv6 ヘッダ

そのため、最大ホップ数の値を調べることでルータを超えた近隣探索パケットであるかを容易に判別することができ、これにより外部からの ICMP リダイレクトメッセージを破棄することができる。ただし、同一ノードからの攻撃には有効な対策ではない。

・SEND(SEcure Neighbor Discovery) を利用する

SEND は、RFC 3971 に規定される近隣探索プロトコルをセキュリティ上の脅威から保護するための仕組みである。SEND ではルータとの信頼関係の構築やパケットの改ざんと送られるメッセージの妥当性を判断できるため、この仕組みを利用することで偽装された ICMP リダイレクトメッセージの処理を無効化できる。

14)-6. 実装ガイド

仕様上の問題であり、実装上で対策する手段がない。

14)-7. 運用ガイド

1. 自分自身に対するルーティング変更要求は無視する。
2. ルーティング情報の保持領域をサイズ制限する。
3. ICMP リダイレクトメッセージの処理を無効化する。
4. ファイアウォールやルータで、不要な ICMP パケットを遮断する。
5. OS によっては、ベンダよりパッチ等がリリースされているので、適用する。

14)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1981 年 RFC 792, Internet Control Message Protocol.
http://www.ietf.org/rfc/rfc792.txt

1998 年 RFC2460, Internet Protocol, Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2460.txt
RFC 2461, Neighbor Discovery for IP Version 6(IPv6)
http://www.ietf.org/rfc/rfc2461.txt
RFC 2463, Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2463.txt

1999年 WinFreeze, a Denial of Service attack against Windows
http://www.securiteam.com/exploits/2ZUQ5QAQKO.html

Winfreeze.c for Solaris
http://packetstormsecurity.org/9903-exploits/Winfreeze-sparc.c
Winfreeze EXPLOIT Win9x/NT
http://marc.theaimsgroup.com/?l=ntbugtraq&m=92099515709467&w=2
ISS X-Force Database win-redirects-freeze(1947)
http://xforce.iss.net/xforce/xfdb/1947

2002年 Common Vulnerabilities and Exposures CVE-1999-1254
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-1254

2005 年 RFC 3971, SEcure Neighbor Discovery(SEND)
http://www.ietf.org/rfc/rfc3971.txt

参考 マスタリング TCP/IP 入門編 第 3 版 p.144
マスタリング TCP/IP IPv6 編 第 1 版 p.84-116

15).ICMP リダイレクトによる送信元詐称の問題

15)-1. 分類:ICMP 【IPv4】【IPv6】

15)-2. 概要

ホストやルータに対し偽装された ICMP リダイレクトメッセージ(Type = 5)が送信されることにより、ルーティングテーブルが書き換わり、盗聴や侵入が可能になる。

15)-3. 解説

攻撃手法とその影響

ICMP リダイレクトメッセージ(Type = 5)はルータやホストに対してルーティング変更を指示するメッセージである。これを悪用し、ルータやホストのルーティング情報を書き換えることで特定ホストに成りすますことが可能である。

この問題で行われうる攻撃の例を図 15-1 に示す。通信可能なホスト A、B が存在し、攻撃者 C がホスト B になりすましてホスト A と通信しようと試みる。

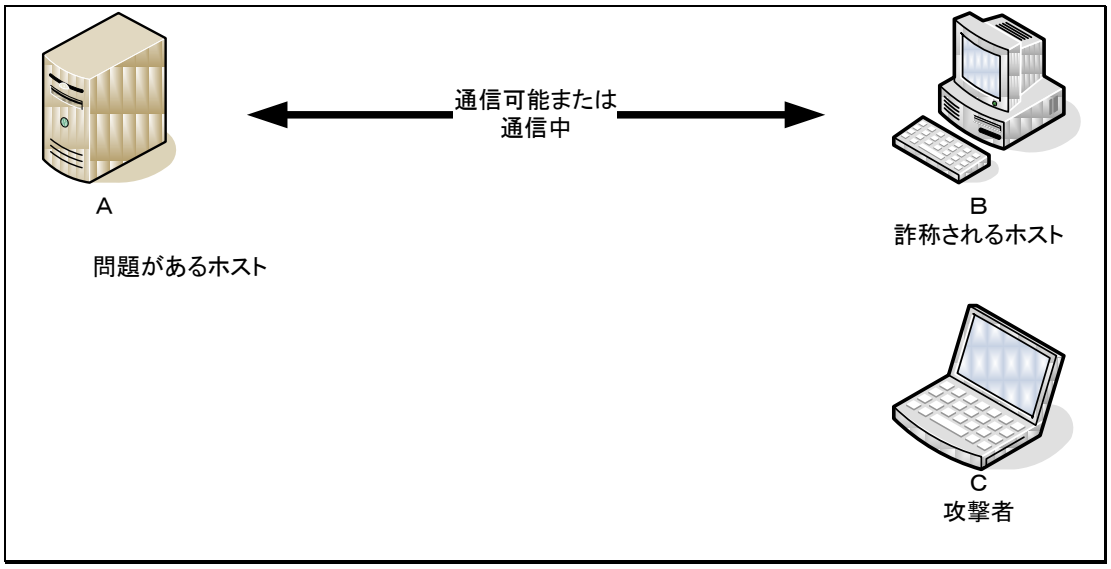


図 15-1 攻撃手法(第 1 段階)

攻撃者 C は図 15-2 に示すようにホスト A(または途中経路のルータ)に対して、ホスト B へのルーティングをホスト C に向けるよう ICMP リダイレクトメッセージを送信する。ホスト A は受信した ICMP リダイレクトメッセージに従い、ルーティング情報を更新する。

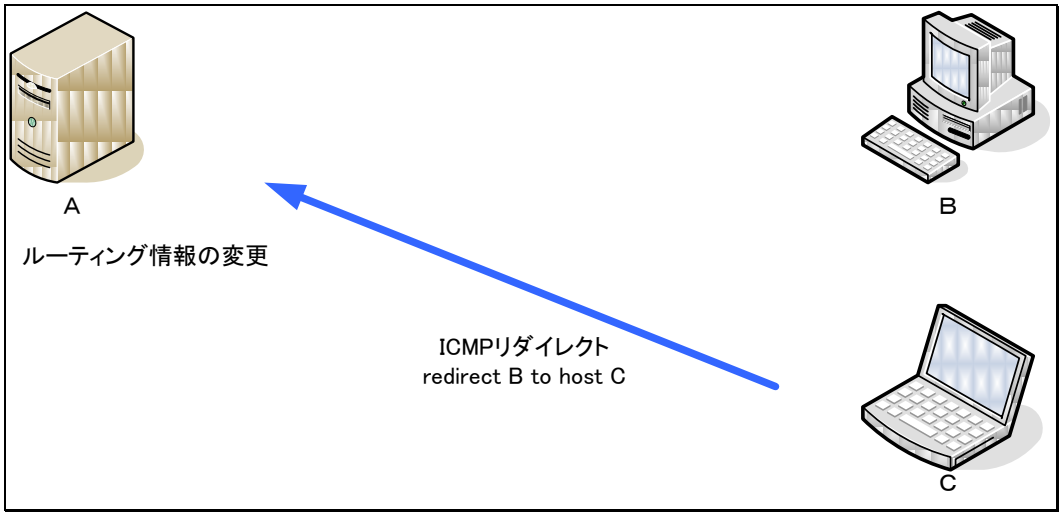


図 15-2 攻撃手法(第 2 段階)

図 15-3 に示すように、ホスト A は更新されたルーティング情報に従い、ホスト B に対する通信をホスト C に対して送信する。

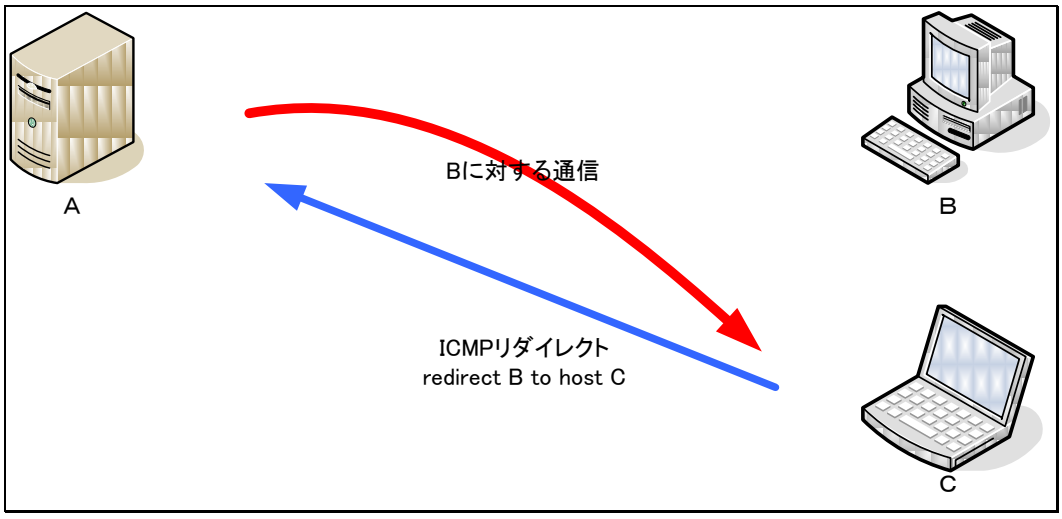


図 15-3 攻撃手法(第 3 段階)

この手法により、本来 A-B 間で発生すべき通信が A-C 間で発生し、攻撃者 C は B になりすますことが可能である。

【ICMP リダイレクトによる送信元詐称の問題】

この問題の脅威として、以下が考えられる。

- A-B 間で通信が発生している場合 A から B への通信を C に変更させることにより、C は A-B 間の通信の盗聴が可能である。
- A-B 間にホストレベルの信頼関係がある場合、C は rlogin 等を利用し、権限を奪取することが　可能である。

原因と考察

ICMP リダイレクトメッセージはパケットの経路情報をやり取りするために利用され、以下のように一時的にルーティングテーブルを追加することができる。

1. ホスト A からホスト B へパケットを送信する。
2. ホスト A のデフォルトゲートウェイはルータ 1 と設定されているため、パケットをルータ 1 へ送信する。
3. ルータ 1 はパケットを受け取るがホスト B がルータ 2 の先にあるため、ルータ 2 へパケットを転送する。
4. ルータ 1 はホスト A へ ICMP リダイレクトメッセージを利用し、今後ホスト B へパケットを送信する際はルータ 2 を利用するよう情報を送信する。
5. ホスト A は ICMP リダイレクトメッセージを受け取り一時的にこの経路情報をルーティングテーブルへ追加し、その後に同じ送信先へパケットを送る際にこの情報を利用する。

以上の通信の流れを図 15-4 に示す。

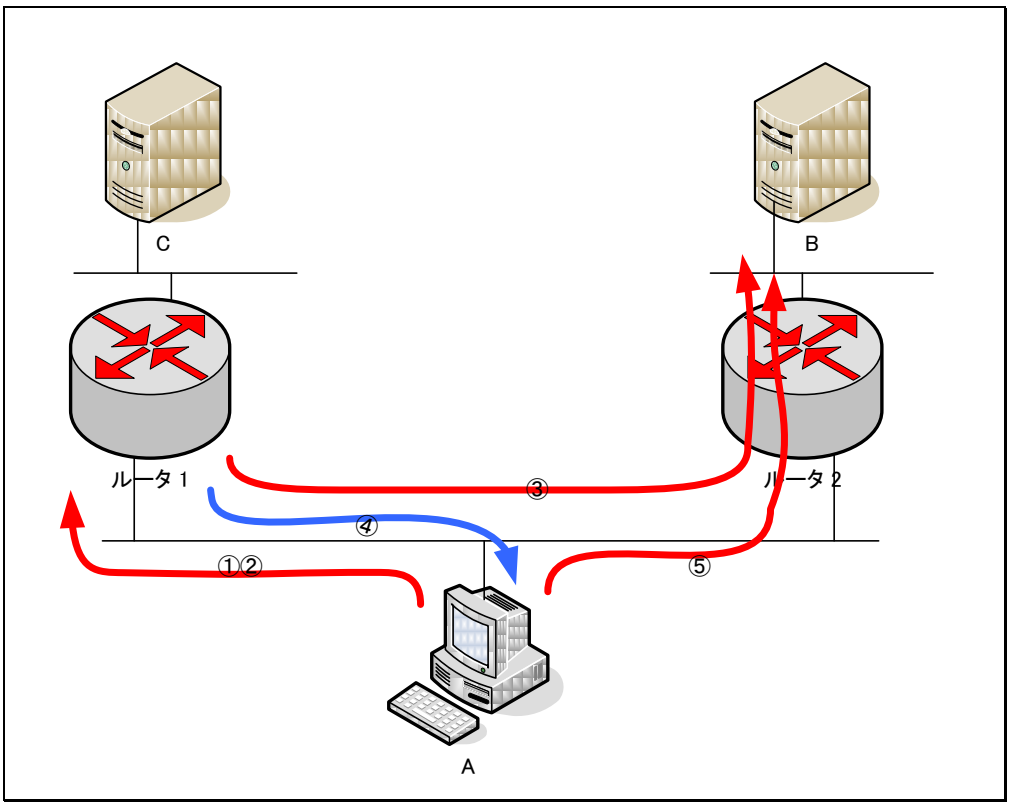


図 15-4 ICMP リダイレクトメッセージの仕組み

もし ICMP リダイレクトメッセージが不正な場合、ルーティング情報が不適切に書き換わることに起因し、通信が意図しない IP に対して発生する恐れがある。

15)-4. 発見の経緯とトピック、対策の動き、現在の動向

ICMP リダイレクトメッセージの仕様は ICMP プロトコル自体とともに 1981 年に決められた。1989 年および 1995 年に、ホストおよびルータの要件として、RFC 1122 および RFC 1812 が提案された。

15)-5. IPv6 環境における影響

IPv6 における IPv4 の ICMP リダイレクトメッセージに相当する機能は、RFC2461 に規定されている近隣探索プロトコルで提供される。近隣探索は、ICMPv6 を使用して 3 種類 5 タイプのメッセージで機能を実現し、その中の 1 つのメッセージタイプに ICMPv6 リダイレクトメッセージ(Type =137)がある。概念的には IPv4 と同じ手法での攻撃が可能であり、IPv6 環境でも影響があると考えられる。(注 1)

注 1:IPv6 環境では IPv4 での対策に加え、IPv6 のセキュリティの向上を図ることができる。詳細については 12)-5 の補足資料を参照のこと

15)-6. 実装ガイド

この問題は ICMP リダイレクトメッセージの仕様上の問題であるが、RFC 1122 および RFC 1812 に従い実装することである程度回避可能である。要点を以下に示す。

1. 送信元 IP アドレスと転送先 IP アドレスが同一ネットワークでない ICMP リダイレクトメッセージは処理しない。
2. ルーティングプロトコルを使用しているルータは ICMP リダイレクトメッセージを処理しない。
3. 転送先 IP アドレスが自分自身の存在するネットワーク上に無い場合は、処理しない。
4. 送信元アドレスがデフォルトゲートウェイで無い場合は、処理しない。

15)-7. 運用ガイド

1. ICMP リダイレクトメッセージの処理を無効化する。
2. ファイアウォールやルータで、ICMP パケットを遮断する。
3. OS によっては、ベンダよりパッチ等がリリースされているので、適用する。

15)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1981年 RFC 792, Internet Control Message Protocol.
http://www.ietf.org/rfc/rfc792.txt

1998 年 RFC2460, Internet Protocol, Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2460.txt
RFC 2461, Neighbor Discovery for IP Version 6(IPv6)
http://www.ietf.org/rfc/rfc2461.txt
RFC 2463, Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2463.txt

1989 年 RFC 1122 Requirements for Internet Hosts -- Communication Layers
http://www.ietf.org/rfc/rfc1122.txt

【ICMP リダイレクトによる送信元詐称の問題】

1995 年　RFC 1812, Requirements for IP Version 4 Routers.
http://www.ietf.org/rfc/rfc1812.txt
RFC 3971, SEcure Neighbor Discovery(SEND)
http://www.ietf.org/rfc/rfc3971.txt

参考　マスタリング TCP/IP　入門編　第 3 版　p.144
マスタリング TCP/IP　IPv6 編　第 1 版　p.84-116

16).ICMP 始点抑制メッセージ による通信遅延の問題

16)-1. 分類:ICMP 【IPv4】

16)-2. 概要

IPv4 において、ICMP 始点抑制メッセージを受け取ったホストは、そのメッセージを受け取らなくなるところまでパケット送出の速度を落とすため、通信が遅延してしまう。

16)-3. 解説

攻撃手法とその影響

ICMP 始点抑制メッセージ(Source Quench; Type = 4)は、ネットワーク上で発生した輻輳を緩和するために送信されるメッセージである。特定のホストに ICMP 始点抑制メッセージを送信し続けることによって、そのホストの通信が阻害される恐れがある。

この問題で行われうる攻撃の例を図 16-1 に示す。この攻撃が行われホスト A とホスト B が通信を行っているものとする。

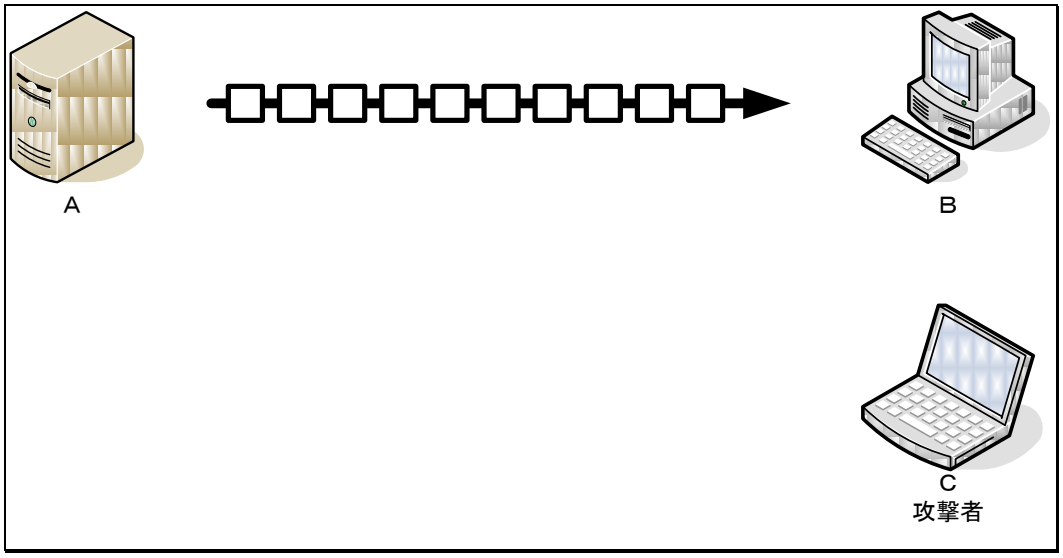


図 16-1 ICMP 始点抑制メッセージによる転送遅延(第一段階)

【ICMP 始点抑制メッセージ による通信遅延の問題】

攻撃者 C が ICMP 始点抑制メッセージをホスト A に対して送信し続けた場合、ホスト A はネットワークに混雑が発生していると判断し、図 16-2 のように送信間隔を空ける。この結果、ホスト A からホスト B への通信が遅延してしまう可能性がある。

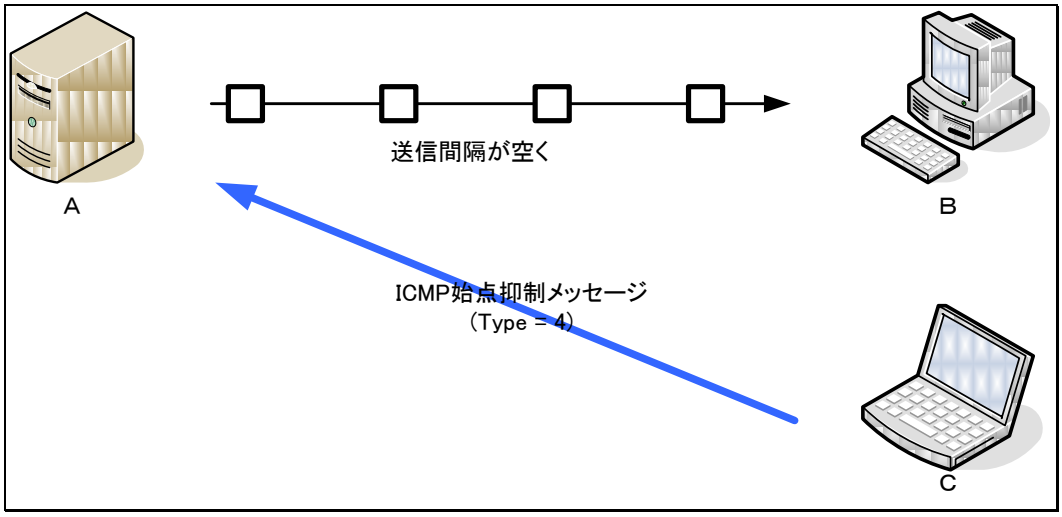


図 16-2　ICMP 始点抑制メッセージによる転送遅延(第二段階)

原因と考察

ICMP 始点抑制メッセージは、ネットワーク上で発生した輻輳を緩和するために送信されるメッセージである。TCP/IP の実装や使用するトランスポート層プロトコルにより本メッセージに対する反応は異なるが、 RFC 1122 において、TCP を使用するホストは ICMP 始点抑制メッセージを受信した場合、スロースタート処理を行うことが推奨されている。 また、RFC 2001 では近年の TCP の実装に用いられるスロースタートと即時再転送に関することが記述されている。

このメッセージは、ネットワーク機器におけるキューの残りがゼロになったとき(パケットを廃棄しなければならない状況に陥ったとき)に送出される。メッセージを受け取ったホストは、ネットワーク上のどこかが混雑していることを認識し、TCP 通信におけるウインドウサイズの調整を行いパケットの送出速度を遅くする。そのため、意図的に特定ホストに対してメッセージを送り続けることにより、そのホストの通信を阻害することが可能となる。

このメッセージは本来、ネットワーク輻輳の対応としてかつて試みられたものであるが、現在ではこの状況の対応としては効果的な方法でないことが認識されており、本メッセージはほとんど使用されていない。

16)-4. 発見の経緯とトピック、対策の動き、現在の動向

ICMP 始点抑制メッセージの仕様は ICMP プロトコル自体とともに 1981 年に決められた。2004 年に Gont により"ICMP Attacks Against TCP"が公開された。2005 年には NISCC より、アドバイザリ(Vulnerability Issues in ICMP packets with TCP payloads)が公開された。

16)-5. IPv6 環境における影響

この問題には ICMP 始点抑制メッセージ(Source Quench; Type = 4)を利用するが、ICMPv6 にはこれに相当するメッセージは存在しないため、IPv6 環境においてはこの問題の影響を受けない。

16)-6. 実装ガイド

仕様上の問題であり、実装上で対策する手段がない。

16)-7. 運用ガイド

1. ファイアウォールやルータで、ICMP メッセージに対するアクセス制御を実施する。
2. ICMP 始点抑制メッセージの受入れを拒否あるいは無視する。
   Windows XP のインターネット接続ファイアウォール機能では、「発信元の抑制を許可する」を無効にする。

16)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2006 年 3 月)のものである。

1981年 RFC 792, Internet Control Message Protocol.
http://www.ietf.org/rfc/rfc792.txt

1989 年 RFC 1122, Requirements for Internet Hosts -- Communication Layers.
http://www.ietf.org/rfc/rfc1122.txt

1995 年 RFC 1812, Requirements for IP Version 4 Routers.
http://www.ietf.org/rfc/rfc1812.txt

2001年 RFC 2001, TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms.
http://www.ietf.org/rfc/rfc2001.txt

2004年　ICMP attacks against TCP【Gont 著】
http://www.gont.com.ar/drafts/icmp-attacks-against-tcp.html
Common Vulnerabilities and Exposures CVE-2004-0791
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0791

2005年　NISCC Vulnerability Advisory ICMP – 532967
http://www.uniras.gov.uk/niscc/docs/al-20050412-00308.html?lang=en
[security bulletin] SSRT4743, SSRT4884 rev.1 - HP Tru64 UNIX TCP/IP remote Denial of Service(DoS)
http://marc.theaimsgroup.com/?l=bugtraq&m=112861397904255&w=2
[security bulletin] SSRT4884 HP-UX TCP/IP Remote Denial of Service(DoS)Dec 07 2005 06:39PM
http://www.securityfocus.com/archive/1/archive/1/418882/100/0/threaded
RHSA-2005:016-13
http://rhn.redhat.com/errata/RHSA-2005-016.html
SUNALERT:101658(formerly 57746)
http://sunsolve.sun.com/search/document.do?assetkey=1-26-101658-1
TCP 実装の ICMP エラーメッセージの処理に関する脆弱性の問題について(古川電工)
http://furukawa.jp/fitelnet/topic/icmp_attacks.html

2006 年　TCP Remote ICMP Denial Of Service Vulnerabilities
ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2006.4/SCOSA-2006.4.txt

SCO OpenServer ICMP Message Handling Denial of Service
http://secunia.com/advisories/18317

参考　マスタリング TCP/IP　入門編　第 3 版　p.146

17).ICMP ヘッダでカプセル化されたパケットがファイアウォールを通過する問題 (ICMP トンネリング)

17)-1. 分類:ICMP 【IPv4】【IPv6】

17)-2. 概要

ICMP パケットの通過を許可するファイアウォールやルータには、ICMP でカプセル化された TCP や UDP のパケットを ICMP パケットとみなして通過させてしまう問題がある。

17)-3. 解説

攻撃手法とその影響

データを ICMP ヘッダでカプセル化することにより、ICMP パケットの通過を許可しているファイアウォールやルータをデータが通過してしまう問題がある。これを悪用して、ファイアウォールで許可されていない TCP/IP の通信に ICMP ヘッダを付加(カプセル化)することによりファイアウォールを通過させることが可能である。

例として、telnet が許可されていないファイアウォールに telnet の通信を通過させることを想定する。ファイアウォール外側のホスト C が内側のホスト A に対して送信した telnet は、図 17-1 のようにファイアウォール B で遮断される。

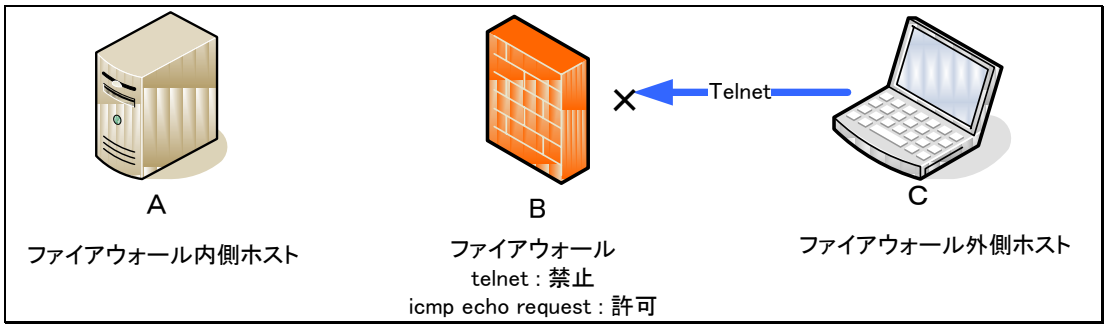


図 17-1 ファイアウォールによる telnet の遮断

しかし、telnet のパケットの先頭に ICMP ヘッダを付加した上で送信した場合、ファイアウォール B は ICMP パケットとみなし、通過させる(図 17-2)。ICMP パケットを受信したホスト A は脱カプセル化により ICMP ヘッダを外した上で、telnet パケットとして処理する。

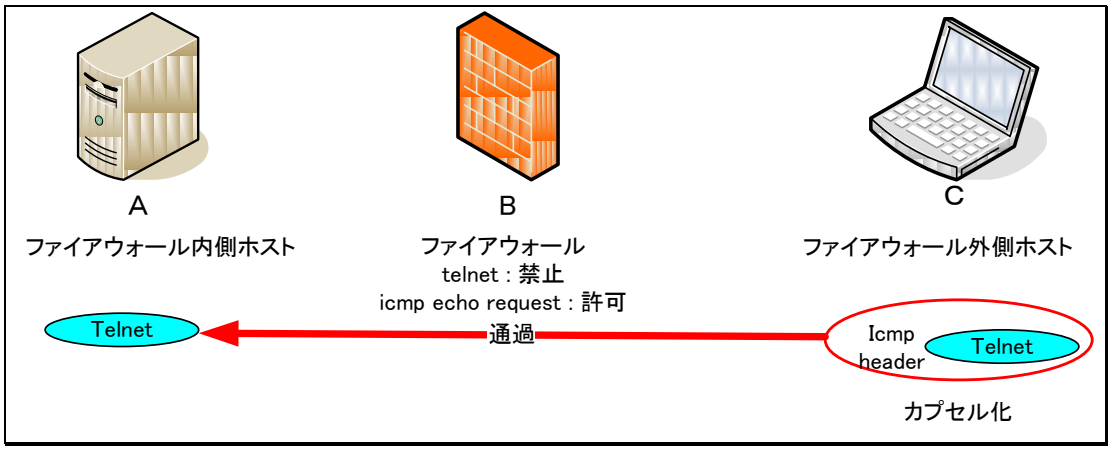


図 17-2 カプセル化したパケットの通過

この手法を成功させるには、送信側ホスト、受信側ホスト双方に同様のカプセル化および脱カプセル化の仕組みを実装する必要がある。そのため、この問題を利用してファイアウォール内側への侵入を試みるには、あらかじめファイアウォール内側のホストにカプセル化および脱カプセル化を行う仕組みを用意する必要がある。

原因と考察

多くのファイアウォールやルータは、IP アドレス、プロトコル、ポート番号のチェックのみを行っており、データ部分(ペイロード)のチェックを行っていない。また、ICMP の仕様では、データの長さに制限がない。そのため、ICMP パケットのペイロード部分に TCP パケットをそのまま埋め込むことが可能となっている。

ICMP パケットにサイズ制限を設定するよう仕様を変更することにより、脅威を軽減することが可能と考えられる。

なお、同様の問題が UDP にも存在する。特に DNS(53/udp)は名前解決のため多くのファイアウォールで許可しているため、悪意のあるデータを UDP ヘッダでカプセル化し、ファイアウォールを通過させることが可能である。

17)-4. 発見の経緯とトピック、対策の動き、現在の動向

1997 年に、オンライン出版物である Phrack にて Loki バックドアが公開された。これはクライアント/サーバプログラムであり、侵入しようとするホスト上の Loki サーバと攻撃元ホスト上の Loki クライアントとの間で ICMP または UDP トラフィックを介して rcmd/rsh に相当するセッションを行うものである。

17)-5. IPv6 環境における影響

RFC2463 に規定される ICMPv6 の仕様においてもデータ部分は可変長でありサイズやカプセル化の制限は要求されていないため、概念的には IP プロトコルのバージョンに限らずこの問題は再現すると考えられ、IPv6 環境でも影響を受ける可能性がある。

17)-6. 実装ガイド

ICMP の仕様上の問題であり、実装上で対策する手段はない。

17)-7. 運用ガイド

1. ファイアウォールやルータで ICMP パケットを遮断する。
2. ICMP パケットのサイズ制限を行うことにより、大きな ICMP パケットを通過させないようにする。ただし、この方法では、正規の ICMP パケットも通過できなくなる恐れがある。

17)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007年 7 月)のものである。

1981 年 RFC 792, Internet Control Message Protocol.
http://www.ietf.org/rfc/rfc0792.txt

1997 年 Phrack Magazine, Volume 7, Issue 49, Article 06 of 16
http://www.phrack.org/issues.html?issue=49&id=6&mode=txt
Phrack Magazine, Volume 7, Issue 51, Article 06 of 17
http://www.phrack.org/issues.html?issue=51&id=6&mode=txt
ISS X-Force Database loki(1452)
http://xforce.iss.net/xforce/xfdb/1452

1998 年 RFC 2463, Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc0792.txt

18).ICMP エラーにより TCP 接続が切断される問題

18)-1. 分類:ICMP 【IPv4】【IPv6】

18)-2. 概要

TCP の実装の中には、偽装された ICMP 到達不能メッセージ(Type = 3)を受信すると、既存の TCP 接続を切断してしまう問題がある。

18)-3. 解説

攻撃手法とその影響

IP パケットをあて先に転送できない場合、送信元ホストに対して ICMP 到達不能メッセージ(ICMP Destination Unreachable; Type = 3)が送信される。ホストによっては、ICMP 到達不能メッセージを受信すると TCP 接続を切断するため、ICMP 到達不能メッセージを悪用して、偽装した ICMP 到達不能メッセージを送信することで TCP 接続を切断させることが可能な場合がある。

この問題で行われうる攻撃の例を図 18-1 に示す。ホスト A およびホスト B 間で TCP 通信を行っているものとする。

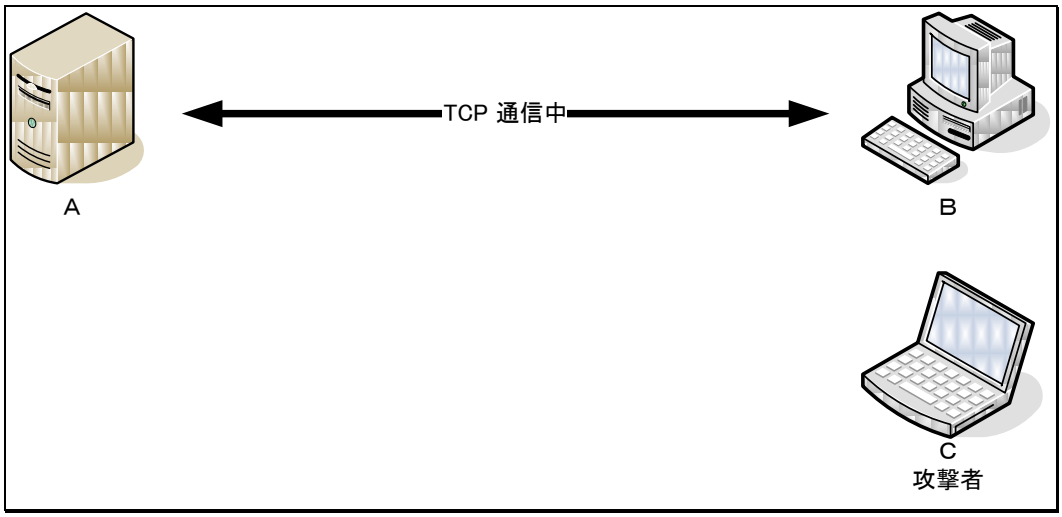


図 18-1 ICMP 到達不能メッセージによる TCP 通信の切断(第一段階)

図 18-2 に示すように、攻撃者 C はホスト A がホスト B に対して送信したパケットの IP ヘッダ部分をデータ(ペイロード)として持つ ICMP Protocol Unreachable(Type = 3, Code = 2)あるいは ICMP Port Unreachable(Type = 3, Code = 3)を A に対して送信する。この結果、ホスト A およびホスト B 間の通信が切断される可能性がある。

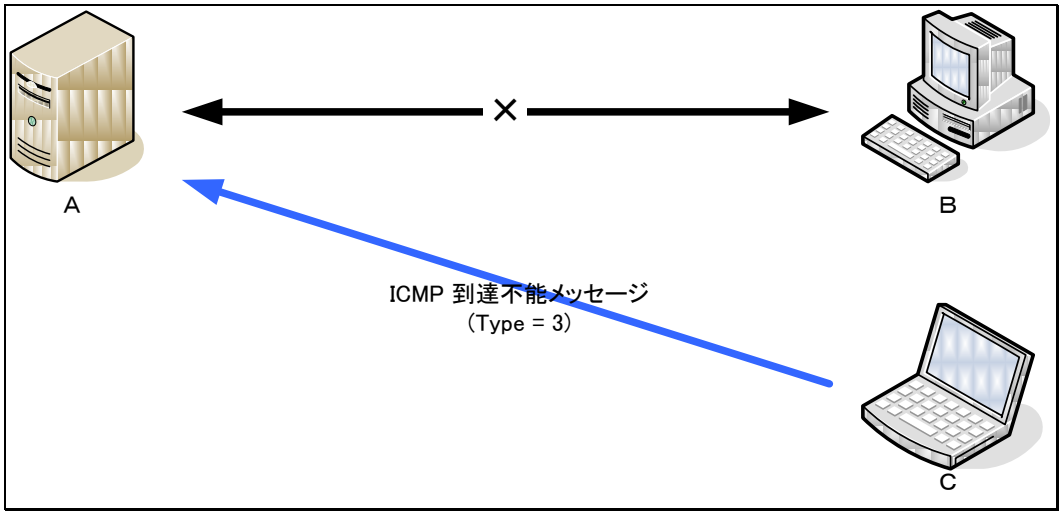


図 18-2　ICMP 到達不能メッセージによる TCP 通信の切断(第二段階)

原因と考察

ICMP 到達不能メッセージのデータ構造は RFC 792 にて規定されている。ICMP 到達不能メッセージのデータ構造を図 18-3 に示す。

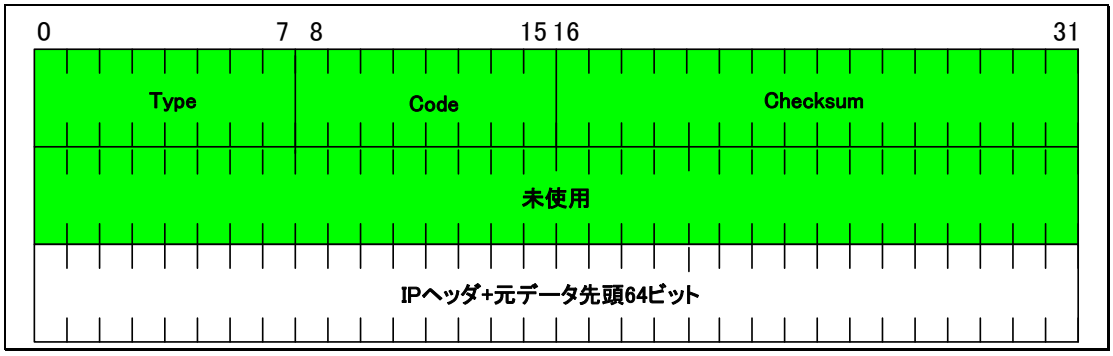


図 18-3 ICMP 到達不能パケットの構造

データ部分には元となるパケットのヘッダ部分とデータ部分の先頭 64 ビットが含まれており、元の TCP 通信を発生させたプロセスを特定するために使用される。TCP 通信に対する到達不能メッセージの場合、データ部分にポート番号に関するデータが含まれている。

また、ICMP 到達不能メッセージは表 18-1 に示すものが規定されている。

表 18-1 ICMP 到達不能メッセージ

Code 番号	ICMP 到達不能メッセージ
Code 0	Network Unreachable
Code 1	Host Unreachable
Code 2	Protocol Unreachable
Code 3	Port Unreachable
Code 4	Fragmentation Needed and Don't Fragment was Set
Code 5	Source Route Failed
Code 6	Destination Network Unknown
Code 7	Destination Host Unknown
Code 8	Source Host Isolated
Code 9	Communication with Destination Network is Administratively Prohibited
Code 10	Communication with Destination Host is Administratively Prohibited
Code 11	Destination Network Unreachable for Type of Service
Code 12	Destination Host Unreachable for Type of Service

RFC 1122 では、Code2、3、4 のメッセージをハードエラー(hard error)と規定し、メッセージを受信した場合には TCP 接続を中止すべきとしている。

以上の仕様により、ICMP 到達不能メッセージを受信したホストは、そのペイロードにある IP アドレス、ポートのデータを元に該当する TCP 通信を特定し、TCP 接続を切断する。なお、IP データ部分の先頭 64 バイトには、TCP シーケンス番号のフィールドが含まれている。そのため、ICMP 到達不能メッセージのペイロードに含まれる TCP シーケンス番号を確認し、正当性を確認すべきと提案されている。

18)-4. 発見の経緯とトピック、対策の動き、現在の動向

1981 年に ICMP の仕様である RFC 792 が発行されたが、この時点では ICMP 到達不能メッセージを受信した場合の挙動について規定されていなかった。1985 年に発行された RFC 1122 にて、Code2、3、4、の到達不能メッセージを受信した際には TCP 接続を切断すべき(SHOULD)の見解が示された。2004 年に Gont により、ペイロードに含まれる TCP シーケンス番号を確認する提案がなされた。

18)-5. IPv6 環境における影響

この問題は、偽装した以下の ICMPv4 到達不能メッセージを利用して TCP 通信の切断を発生させる問題である。

・“Protocol Unreachable“(Type = 3, Code = 2)

・“Port Unreachable“(Type = 3, Code = 3)

ICMPv6 については上記 ICMPv4 エラーメッセージに相当するメッセージとして以下の ICMPv6 不到達メッセージ(注 1) があり、この 2 つの ICMPv6 不到達メッセージを利用することで IPv6 においても TCP 通信切断の影響がある。

・“communication with destination administratively prohibited”(Type=1,Code =1)

・“port unreachable”(Type = 1, Code = 4)

なお、TCP 実装の ICMP エラーメッセージの処理に関する脆弱性(NISCC-532967)より、ステータスが「該当製品あり」のベンダ情報を見ると、ICMPv4 および ICMPv6 の両方をサポートする一部のベンダでは、この問題の影響に関する情報が記述されている。マイクロソフトでは 2005 年 4 月に TCP/IPv4 の脆弱性（MS05-019）の 1 つとして、また 2006 年には TCP/IPv6 の脆弱性(MS06-064) の 1 つとして脆弱性の対処を行っており、ICMPv4 および ICMPv6 の両方の修正が行われている。また、影響を受けないベンダでは ICMPv4 および ICMPv6 ともに影響を受けないという報告が行われている。

注 1: ICMPv6 不到達メッセージは ICMPv6 エラーメッセージの 1 つとして RFC2463 に規定されている。

18)-6. 実装ガイド

1. ICMP エラーの対象となる接続を特定する際に、ペイロードに含まれる IP アドレス、ポート番号だけではなく、TCP シーケンス番号の妥当性を調査することで、偽装パケットによる攻撃に反応する機会を減少させることができる。

18)-7. 運用ガイド

1. ホスト上で ICMP 到達不能パケットの処理を無効化する。
2. ファイアウォールまたはルータで、ICMP パケットを遮断する。
3. OS によっては、ベンダよりパッチ等がリリースされているので、適用する。

18)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1981年 RFC 792, Internet Control Message Protocol.
http://www.ietf.org/rfc/rfc0792.txt

1989年 RFC 1122, Requirements for Internet Hosts -- Communication Layers.
http://www.ietf.org/rfc/rfc1122.txt

1998年 RFC2463, Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2463.txt

2004年 Common Vulnerabilities and Exposures CVE-2004-0790
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-0790
ICMP attacks against TCP【Gont 著】
http://www.gont.com.ar/drafts/icmp-attacks-against-tcp.html

2005年 NISCC Vulnerability Advisory ICMP – 532967
http://www.uniras.gov.uk/niscc/docs/al-20050412-00308.html?lang=en
[security bulletin] SSRT4743, SSRT4884 rev.1 - HP Tru64 UNIX TCP/IP remote Denial of Service(DoS)
http://marc.theaimsgroup.com/?l=bugtraq&m=112861397904255&w=2
TCP 実装の ICMP エラーメッセージの処理に関する脆弱性 NISCC-532967
http://jvn.jp/niscc/NISCC-532967/index.html
[security bulletin] SSRT4884 HP-UX TCP/IP Remote Denial of Service(DoS)
http://www.securityfocus.com/archive/1/archive/1/418882/100/0/threaded
マイクロソフトセキュリティ情報 MS05-019
http://www.microsoft.com/japan/technet/security/bulletin/MS05-019.mspx
Open Vulnerability and Assessment Language OVAL57746
http://oval.mitre.org/oval/definitions/data/oval57746.html
Open Vulnerability and Assessment Language OVAL3458
http://oval.mitre.org/oval/definitions/data/oval3458.html

Open Vulnerability and Assessment Language OVAL1910
http://oval.mitre.org/oval/definitions/data/oval1910.html
Open Vulnerability and Assessment Language OVAL4804
http://oval.mitre.org/oval/definitions/data/oval4804.html
TCP 実装の ICMP エラーメッセージの処理に関する脆弱性の問題について(古川電工)
http://www.furukawa.co.jp/fitelnet/topic/icmp_attacks.html

2006年 SCO OpenServer ICMP Message Handling Denial of Service
http://secunia.com/advisories/18317
TCP Remote ICMP Denial Of Service Vulnerabilities
ftp://ftp.sco.com/pub/updates/OpenServer/SCOSA-2006.4/SCOSA-2006.4.txt
マイクロソフトセキュリティ情報 MS06-064
http://www.microsoft.com/japan/technet/security/Bulletin/MS06-064.mspx

参考 マスタリング TCP/IP 入門編 第 3 版 p.143-144
マスタリング TCP/IP IPv6 編 第 1 版 p.69

19).ICMP Echo リクエストによる帯域枯渇の問題 (Ping flooding, Smurf Attack, Fraggle Attack)

19)-1. 分類:ICMP,UDP 【IPv4】【IPv6】

19)-2. 概要

送信元アドレスを攻撃対象に偽装した ICMP Echo リクエストを中継ホストに送信すると、中継ホストは偽装された送信元へ ICMP Echo 応答を返す。攻撃対象のネットワークにその応答が大量に送信された場合、攻撃対象のネットワークの帯域が枯渇してしまう問題である。

19)-3. 解説

攻撃手法とその影響

Ping flooding

Ping flooding は、図 19-1 に示す 3 台のホストで攻撃が構成される。

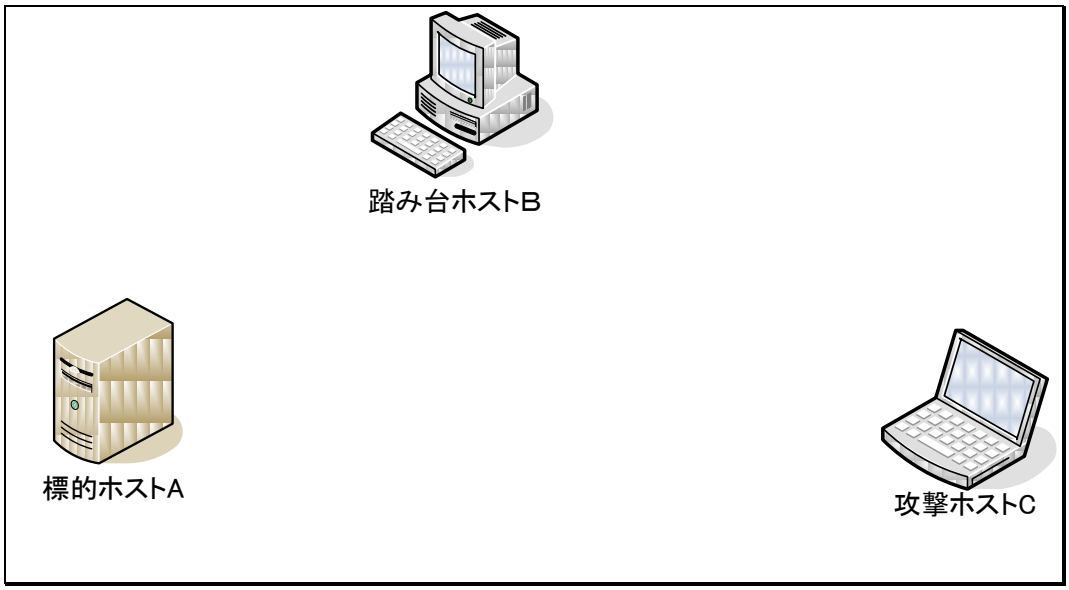


図 19-1 攻撃ネットワーク構成

攻撃ホスト C は図 19-2 に示すように送信元を標的ホスト A に偽装した ICMP Echo リクエストを踏み台ホスト B に大量に送信する。

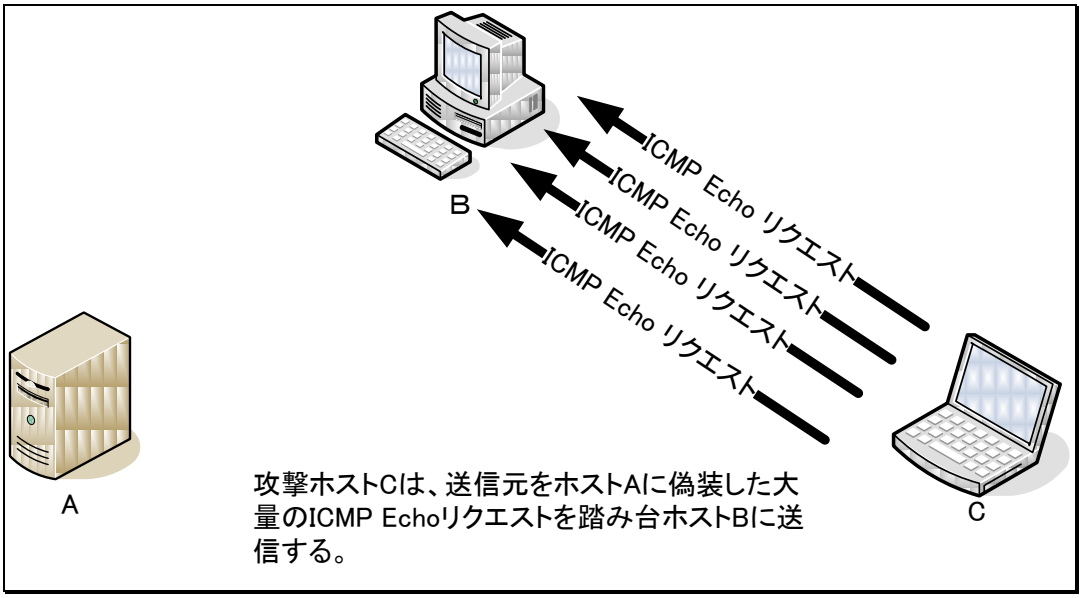


図 19-2 Ping flooding 送信

踏み台ホスト B は、図 19-3 に示すように偽装された送信元である標的ホスト A に ICMP Echo 応答を大量に送信する。

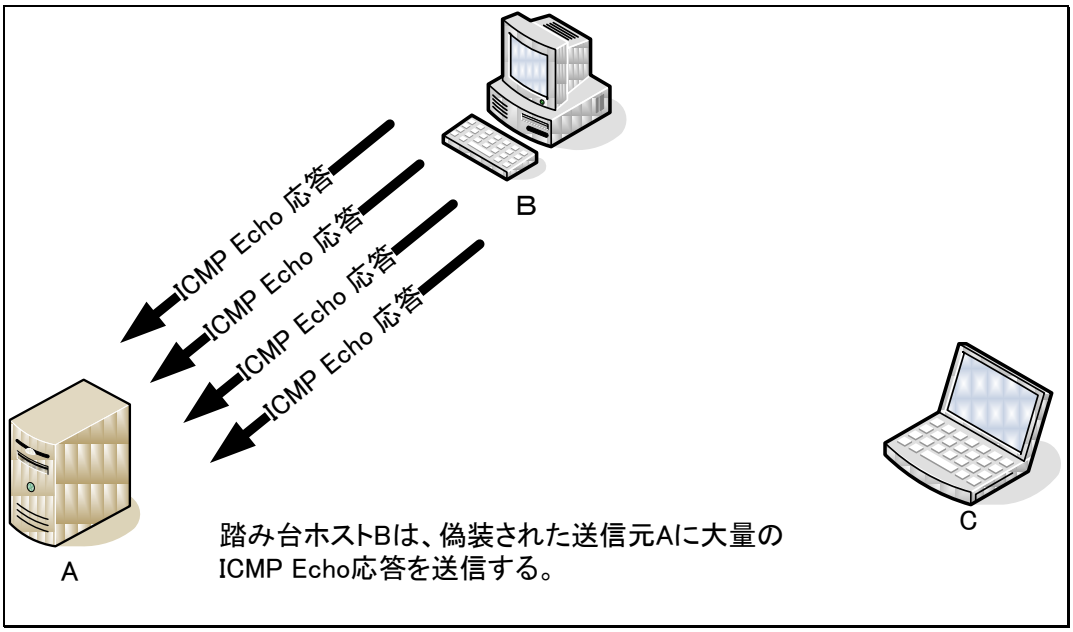


図 19-3 Ping flooding 応答

これによって、攻撃対象ネットワークの帯域を枯渇してしまうという攻撃である。この攻撃では、攻撃ホスト C が送信した ICMP Echo リクエストと標的ホスト A のネットワークに送信される ICMP Echo 応答は同数であり、標的ネットワークに与える負荷と同じ負荷が攻撃側にも生じることになる。

Smurf Attack

Smurf Attack は 図 19-4 に示す2台のホストと踏み台ネットワークで構成される。

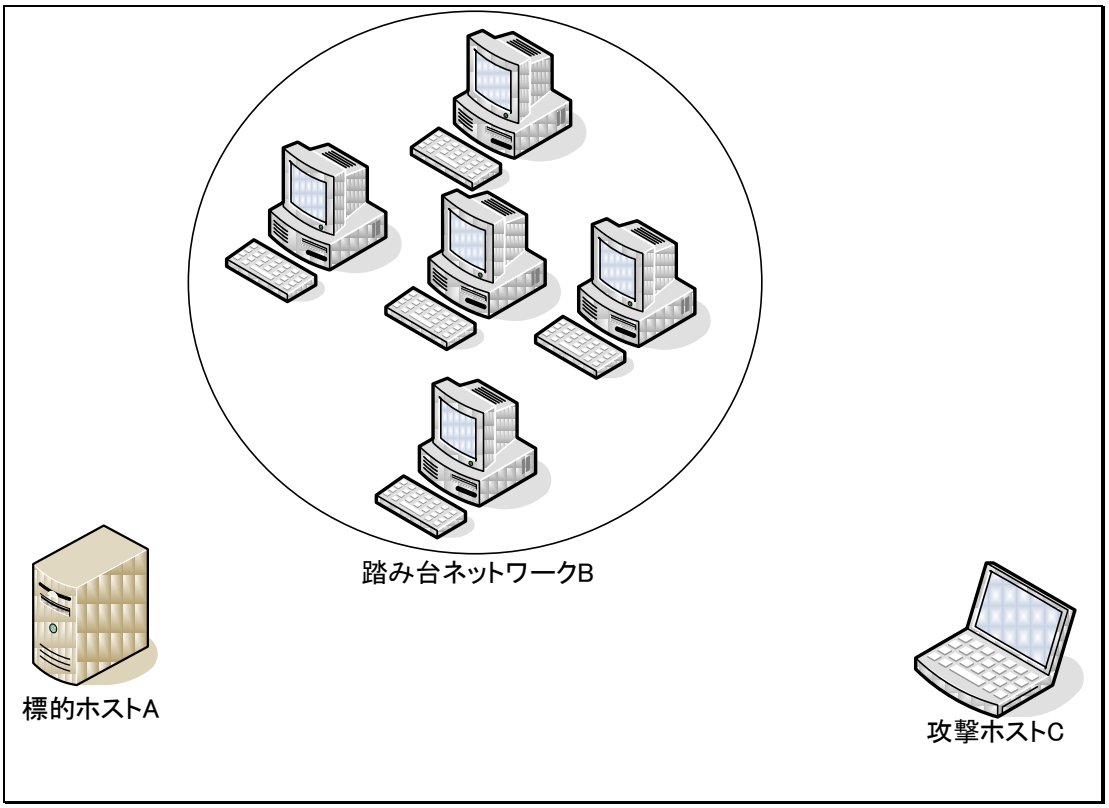


図 19-4　Smurf Attack 攻撃ネットワーク構成

攻撃ホスト C は図 19-5 に示すように、送信元アドレスを標的ホスト A に偽装し、送信先を踏み台ネットワーク B のブロードキャストアドレスに設定した ICMP Echo リクエストを送信する。

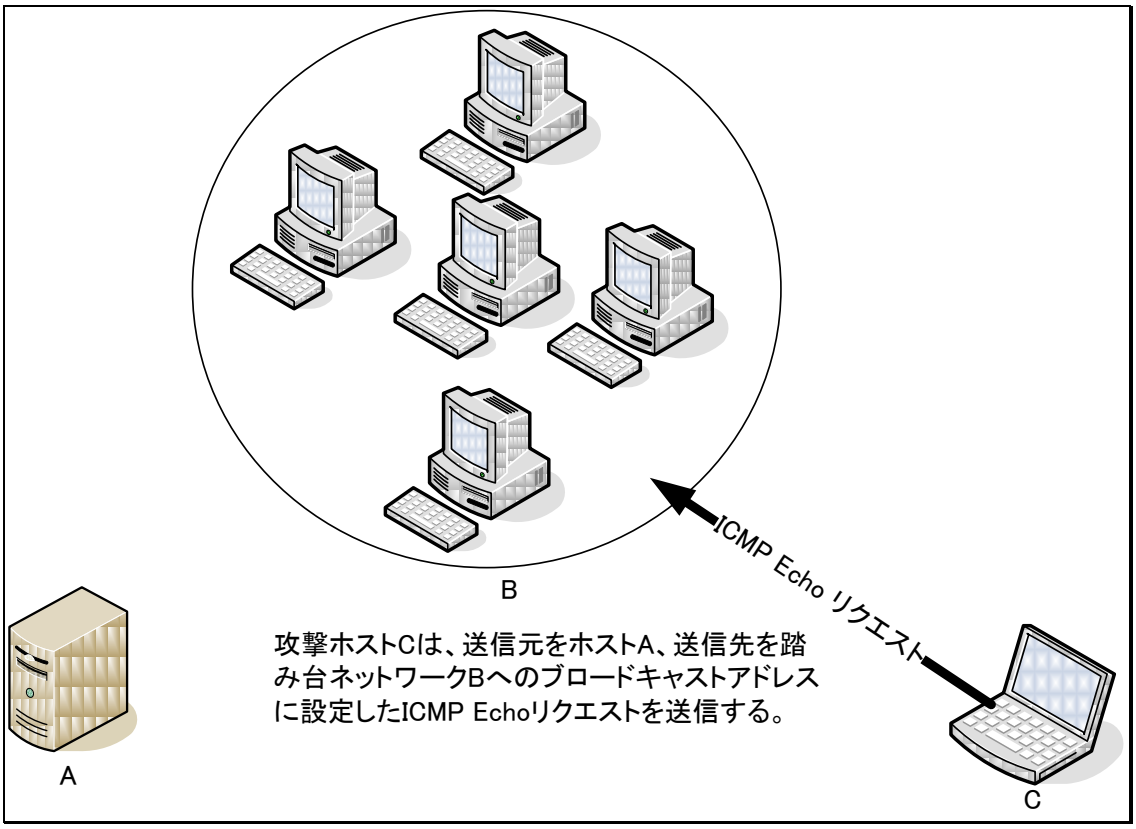


図 19-5　Smurf Attack 送信

図 19-6 に示すように送信先に設定された踏み台ネットワーク B に属する全ホストが ICMP Echo リクエストを受け取り、それらのホストは、偽装された ICMP Echo リクエストの送信元であるホスト A に ICMP Echo 応答を送信する。

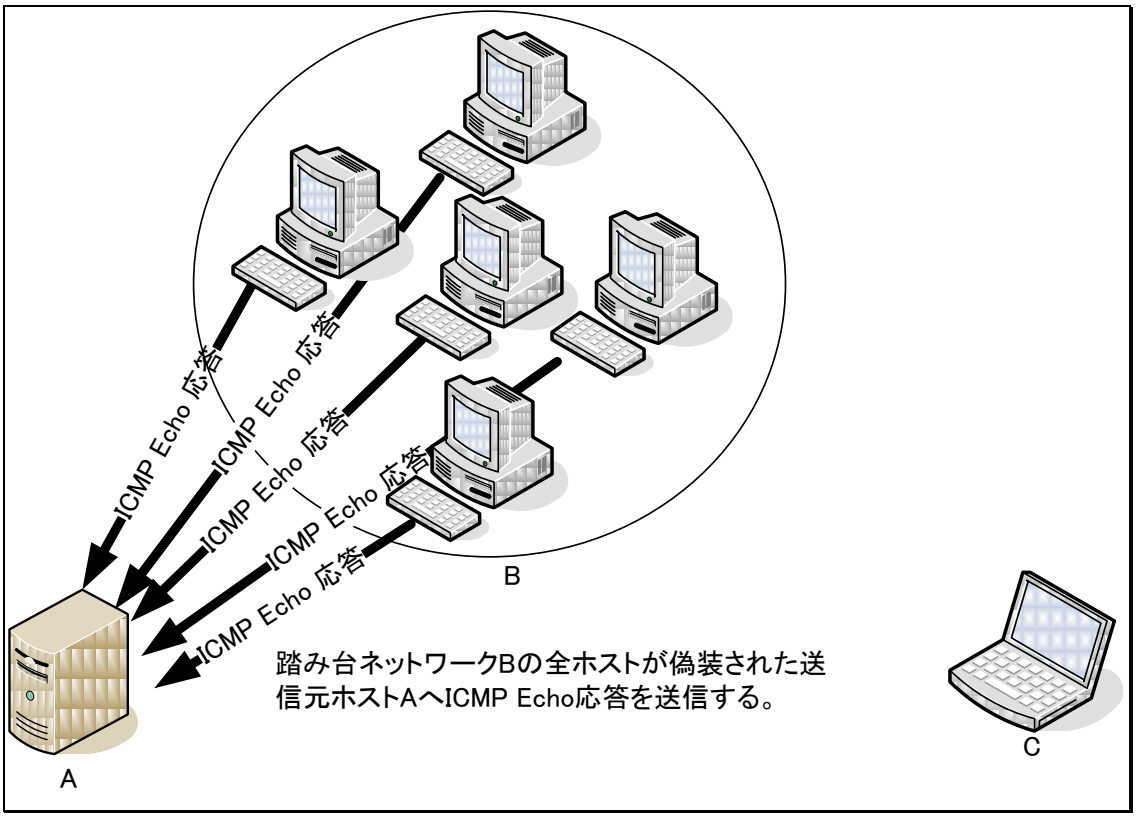


図 19-6 Smurf Attack 応答

この攻撃では、攻撃ホスト C が送信した 1 つの ICMP Echo リクエストが、送信先に設定された踏み台ネットワーク B で増幅された ICMP Echo 応答となって標的ホスト A に送信されるため、攻撃側に比べ、踏み台ネットワークと標的ネットワークには大きな負荷が生じることになり、ネットワーク帯域が枯渇する結果となる。

Fraggle Attack

Smurf Attack と同様に送信元アドレスを攻撃対象ホストに偽装し、送信先をブロードキャストアドレスに設定した攻撃で、UDP の echo(7)、daytime(13)、qotd(17)、chargen(19)の応答を利用して攻撃対象ネットワークの帯域を枯渇させるものである。

原因と考察

ICMP Echo は、ネットワーク上のホストが動作しているか否かを確認するために使われるもので、ICMP Echo リクエストパケットを送信先ホストが受け取ると、ICMP Echo 応答パケット送信元ホストへ返送する。ICMP Echo リクエストの送信元アドレスが偽装されると、ICMP Echo リクエストの送信先のホストは偽装された送信元に応答を返すため、攻撃者は送信先アドレスに指定した第三者のホストを利用して攻撃することが可能である。攻撃を受けた側から見ると、攻撃の送信元ホストは攻撃者とは異なる第三者のものであるため、本来の攻撃者を特定することは困難である。

送信先をブロードキャストに設定した(ダイレクト・ブロードキャスト)パケットは、送信先のネットワークのサブネットに属するすべてのホストに届く。そして、そのすべてのホストから応答が帰ってくるため1つのリクエストが、ホストの台数分の応答に増幅されて返ってくる結果となる。

この2つの問題を組み合わせて、送信元を偽装し、送信先をブロードキャストアドレスの ICMP Echo リクエストを使用したものが Smurf Attack で、攻撃者が送信した1つの ICMP Echo リクエストが踏み台ネットワーク上の台数分の応答に増幅された ICMP Echo 応答が標的ホストに送信されることになり、そのトラフィックによって踏み台ネットワークと標的となるネットワークの帯域が枯渇させられることになる。

Smurf Attack の変種である Fraggle Attack では、ICMP Echo のかわりに、UDP の echo(7)、daytime(13)、qotd(17)、chargen(19)を使用する。これらのサービスは、ICMP Echo と同様に UDP のリクエストを送信すると、送信者に応答を返すものであるため、送信元を偽装し、送信先をブロードキャストアドレスにしたリクエストを踏み台ネットワークに送信すると、偽装されたアドレスに踏み台ネットワーク上のホストの台数分の応答に増幅された応答が標的ネットワークに送信される。

なお、Fraggle Attack において、踏み台ネットワークＢを構成するホストが攻撃者のリクエストに該当する UDP のサービスを提供していない場合は UDP の応答は送信されないが、そのかわりに RFC 792 に従い ICMP の Port Unreachable を偽装されたアドレスに送信してしまうため、当該ホストが UDP のサービスを提供していない場合も攻撃に利用される結果となる。

これらの攻撃は、標的ネットワーク側では攻撃パケットから本来の攻撃元を特定できないため対策をとることが難しく、攻撃を受けた場合は標的ネットワークの上位 ISP や踏み台となっているネットワークに攻撃の遮断や攻撃者の特定を要請するといった対応が必要である。

一方、踏み台ネットワークに送信されるダイレクト・ブロードキャストは、Smurf Attack, Fraggle Attack などの攻撃以外の目的で一般に使用されることはないため、踏み台として悪用されることを防ぐために、ルータ上でこれをブロックすることが有効な対策である。これは、RFC 2644 でルータ機器のデフォルト設定の要件として規定されている。

19)-4. 発見の経緯とトピック、対策の動き、現在の動向

Smurf Attack は、1996 年に CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks として注意喚起され、CVE-1999-0513 が作成されている。

Fraggle Attack は、Smurf Attack の変種で CVE-1999-0514 が作成されている。

これら攻撃に共通する、ダイレクト・ブロードキャストに関する問題の対策として 1999 年 8 月に RFC 2644 が発行され、ルータ機器のデフォルト設定の要件としてダイレクト・ブロードキャストをブロックすることが規定された。

ホスト側においてもダイレクト・ブロードキャストに応答しないことをデフォルト設定とするベンダは増加する傾向にあるが、これを強制する規定は存在しないため、すべての製品で対策がとられているわけではない。

19)-5. IPv6 環境における影響

Ping flooding については、概念的に IP プロトコルのバージョンに限らずこの問題は再現することが考えられる。IPv4 のブロードキャストアドレスを悪用する Smurf Attack、Fraggle Attack については、IPv6 の場合は攻撃者側の事前準備の方法が異なるため、影響を受けるシナリオに違いがある。

IPv6 にはブロードキャストアドレスが存在しないため、代わりにリンクローカル・オールノードマルチキャストアドレス(FF02::1)(注 1)というリンク上の全ノード宛の通信が可能となる、永久的に割り当てられるマルチキャスト IPv6 アドレスを送信先アドレスに設定することで悪用されることが考えられる。マルチキャストアドレスの形式を図 17-7 に示す。

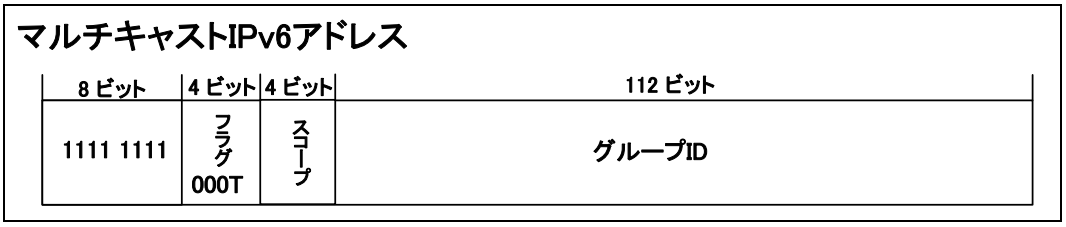


図 19-7 マルチキャスト IPv6 アドレスの構造

このリンクローカル・オールノードマルチキャストアドレスは同一リンクに対しての通信でのみ利用されることが想定されており、IPv4 のブロードキャストのようにルータを超えて利用することはできない。そのため、IPv4 の場合概念的にルータを超えた他のネットワークを指定して踏み台ネットワークとして利用することが可能であったが、IPv6 の場合は他のネットワークを指定することができなくなる。図 17-5 と比較して IPv6 の場合を示すと図 17-8 のようになり、攻撃ホスト C はネットワーク B 上のノードである必要がある。

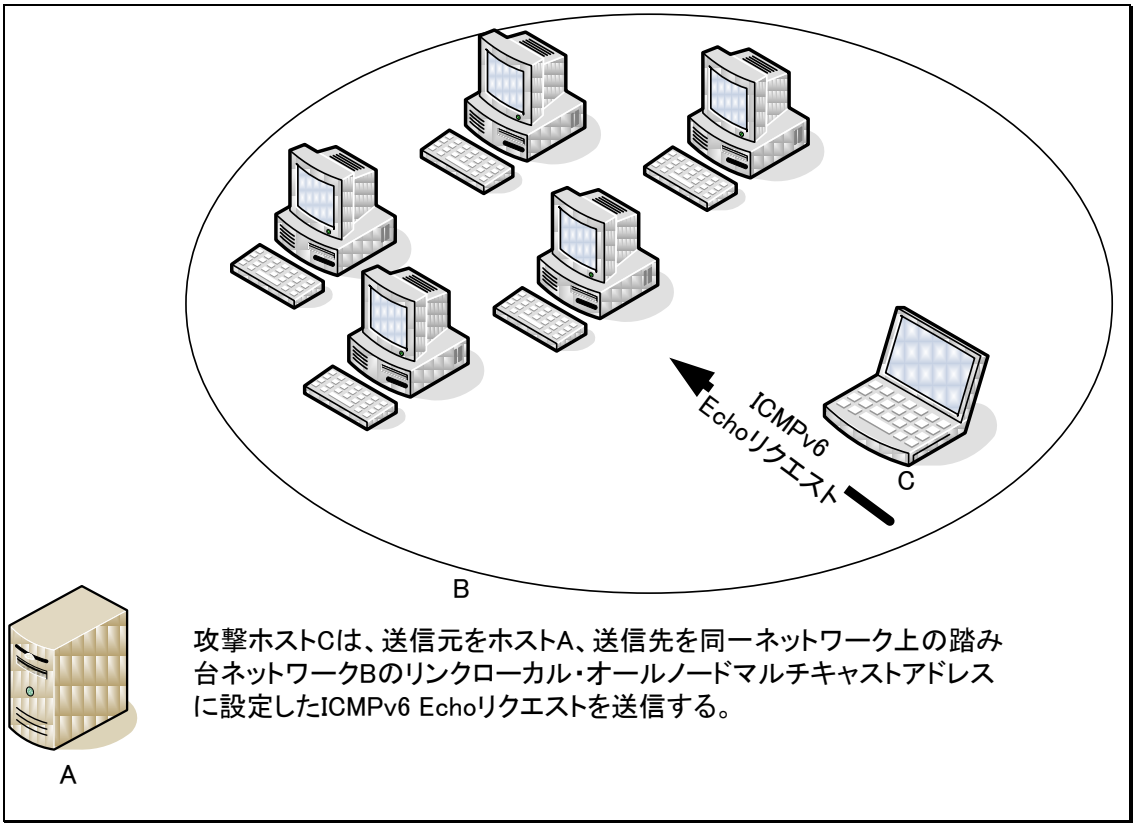


図 19-8　Smurf Attack 送信(IPv6 環境での想定されるシナリオ)

19)-6. 実装ガイド

1. 送信先 IP アドレスがブロードキャストである ICMP Echo には応答しないように設定可能にする。
2. 送信先 IP アドレスがブロードキャストである UDP の echo(7)、daytime(13)、qotd(17)、chargen(19)には応答しないように設定可能にする。

注 1: リンクローカル・オールノードマルチキャストアドレス(FF02:0:0:0:0:0:0:1)は RFC2375 において割り当てられている。図 17-7 に示すマルチキャストアドレスの形式に従い、マルチキャストアドレスの先頭の 8 ビットが全て 1 で Scope = 2、Group ID = 1 となる。

19)-7. 運用ガイド

1. 送信先 IP アドレスがブロードキャストである ICMP Echo には応答しない。
2. 送信先 IP アドレスがブロードキャストである UDP の echo(7)、daytime(13)、qotd(17)、chargen(19)には応答しない。
3. ファイアウォールを含むルーティングデバイスで、送信先 IP アドレスがブロードキャストであるパケットを遮断する。

19)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1997 年 Cisco Systems Technical Tips, "Smurfing": The Latest in Denial of Service Attacks
http://www.pentics.net/denial-of-service/presentations/19971027_smurf_files/frame.htm
ISS X-Force Database(13828):
http://xforce.iss.net/xforce/xfdb/588

1998 年 CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks
http://www.cert.org/advisories/CA-1998-01.html
http://www.lac.co.jp/business/sns/intelligence/cert_advisory/CA-98_01.html
CIAC Information Bulletin I-021a, "smurf" IP Denial-of-Service Attacks
http://www.ciac.org/ciac/bulletins/i-021a.shtml
FreeBSD, Inc. Security Advisory FreeBSD-SA-98:06, smurf attack
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/old/FreeBSD-SA-98:06.icmp.asc
ISS X-Force Database(815):
http://xforce.iss.net/xforce/xfdb/815

RFC 2375, IPv6 Multicast Address Assignments
http://www.ietf.org/rfc/rfc2375.txt

1999 年 Common Vulnerabilities and Exposures CVE-1999-0513
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0513
Common Vulnerabilities and Exposures CVE-1999-0513
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0513
RFC 2644, Requirements for IP Version 4 Routers.
http://www.ietf.org/rfc/rfc2644.txt
http://www.ipa.go.jp/security/rfc/RFC2644JA.html
[NT]Simple TCP/IP サービスへの攻撃に対しサービスを拒否する
http://support.microsoft.com/kb/q154460/

20).ICMP タイムスタンプ要求/ネットマスク要求への応答による問題

20)-1. 分類:ICMP 【IPv4】

20)-2. 概要

ICMP のタイムスタンプ要求およびネットマスク要求に応答してしまうことにより、システムのネットワーク構成情報ならびに時間情報を取得され、更なる攻撃に悪用されてしまう可能性がある。

20)-3. 解説

攻撃手法とその影響

この問題は、RFC に基づく ICMP の仕様によるものであるが、悪意ある第三者が対象のホストを攻撃する際に情報収集することを助長してしまう。なお、ICMP のタイムスタンプ要求およびネットマスク要求に関して直接的な関係性はないため、それぞれの問題について個別に説明する。

ICMP タイムスタンプ要求(Type:13)/応答(Type:14)

図 20-1 のように、攻撃者のホスト B から標的のホスト A に ICMP タイムスタンプ要求(Type = 13)を送信する。

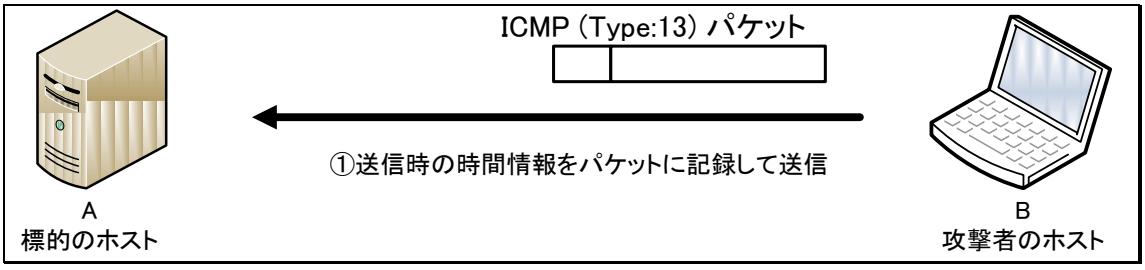


図 20-1 ICMP タイムスタンプ要求

図 20-2 のように、攻撃者のホスト B から送信されたパケットを受信した標的のホスト A は、後述する ICMP メッセージの受信タイムスタンプに受信した時間情報を記録する。

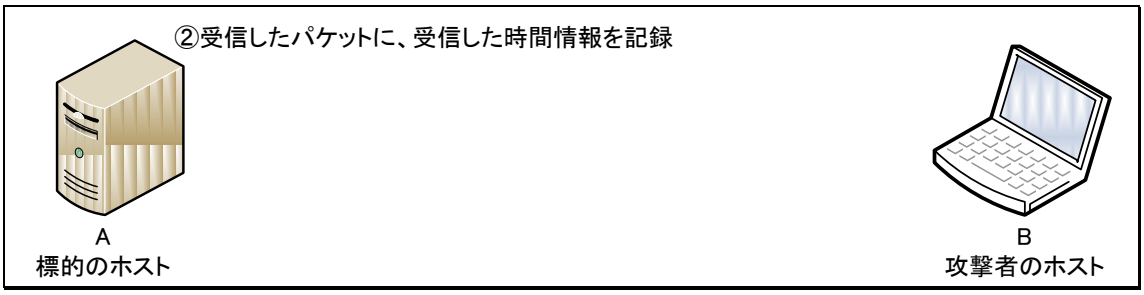


図 20-2 パケットの受信時間情報の記録

攻撃者のホスト B から ICMP タイムスタンプ要求(Type = 13)を受信した標的のホスト A は、図 20-3 のように攻撃者のホスト B に対してタイムスタンプ応答(Type = 14)を送信する。

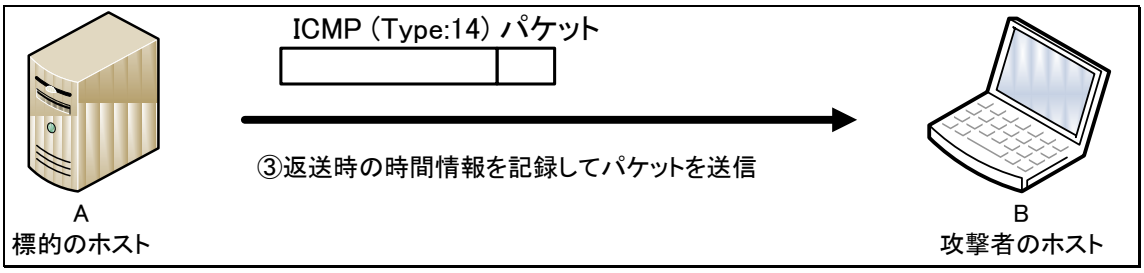


図 20-3 ICMP タイムスタンプ応答

図 20-1 から図 20-3 の手順で、攻撃者は標的のホスト A の時間情報を取得することができる。なお、この応答パケットに含まれる時間情報は、GMT(Greenwich Mean Time)の午前 0 時から経過したミリ秒で示される。

ICMP ネットマスク要求(Type:17)/応答(Type:18)

手順は ICMP タイムスタンプ要求/応答と同様であるが、使用する ICMP のタイプおよび取得できる情報が異なる。

図 20-4 のように、攻撃者は攻撃者のホスト B から標的のホスト A に ICMP ネットマスク要求(Type = 17) を送信する。

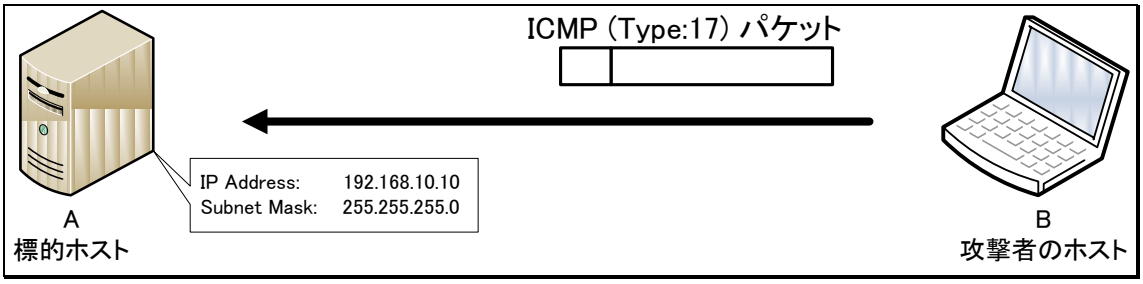


図 20-4 ICMP ネットマスク要求

攻撃者のホスト B から ICMP ネットマスク要求(Type = 17)を受信した標的のホスト A は、図 20-5 のように攻撃者のホスト B に対して ICMP ネットマスク応答(Type = 18)を送信する。

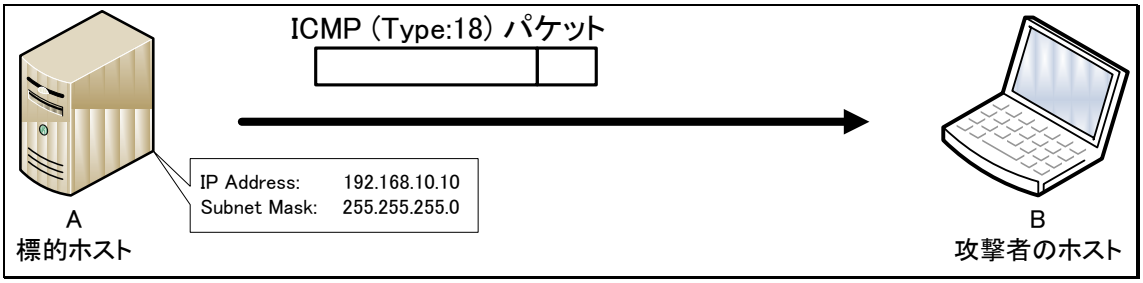


図 20-5 ICMP ネットマスク応答

上記の手順で、攻撃者は標的のホスト A のサブネットマスク情報を取得することができる。ICMP のタイムスタンプ要求およびネットマスク要求から得られる情報は単体としての情報量は豊富ではないが、攻撃者はこのような情報収集をした後に更なる攻撃を仕掛けるため、不必要に ICMP での要求に応答することは危険となる場合がある。

原因と考察

この問題は ICMP の仕様によるものであるため、まず ICMP の概要について説明する。

ICMP は、TCP/IP プロトコルスタックにおけるネットワーク層に属するプロトコルの 1 つであり、主な役割は情報取得である。同階層プロトコルの IP には、エラーの報告、送信元ホストに制御メッセージの送信、適切なルートの取得等の手段が存在しないため、ICMP はこのような機能を実現するために規定された。

ここで解説する ICMP タイムスタンプ要求は RFC792 に、ネットマスク要求は RFC950 に規定されている。

図 20-6 に示すものは、IP ヘッダと ICMP メッセージとの関係であるが、IP ペイロード部に ICMP メッセージが続くことになっている。IP ヘッダのプロトコルにて ICMP のプロトコル番号が 1 であれば、IP ペイロードのデータ部には ICMP メッセージが入る。

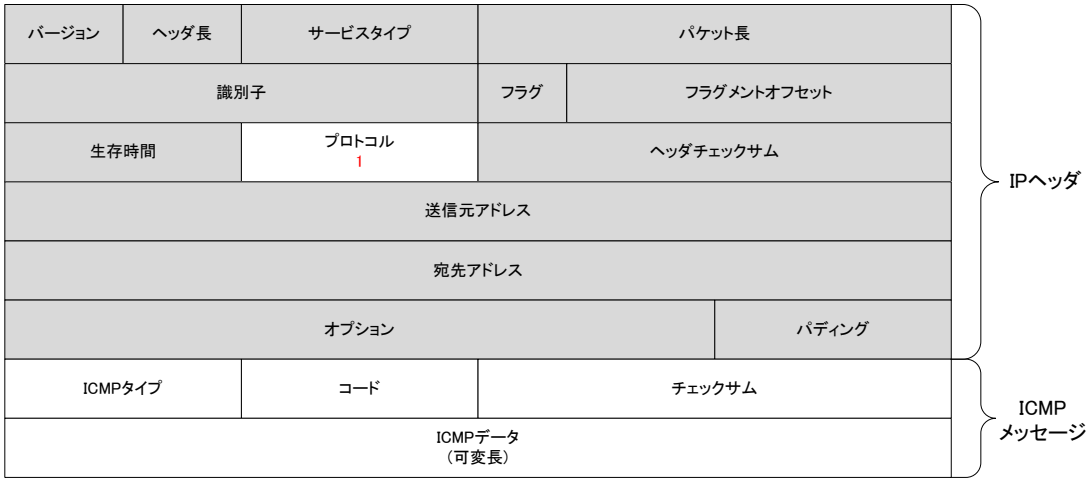


図 20-6 IP ヘッダと ICMP メッセージの構造上の関係性

ICMP メッセージにはそれぞれ、ICMP タイプ、コード、チェックサム、ICMP データの数値が入る。なお、ICMP のデータ領域は ICMP のタイプによって含まれるデータが変化する。

表 18-1 に示すように、ICMP のメッセージタイプには、エラーメッセージと、問い合わせメッセージの 2 つに大別される。エラーメッセージは、宛先到達不能(Type:3)、始点抑制(Type:4)、リダイレクト(Type:5)、データグラムの時間超過(Type:11)、およびデータグラムのパラメータ異常(Type:12)がこれにあたる。対して、問い合わせメッセージは、エコー要求(Type:8)/応答(Type:0)、タイムスタンプ要求(Type:13)/応答(Type14)、情報要求(Type:15)/応答(Type:16)、およびネットマスク要求(Type:17)/応答(Type:18)がある。(注 1)

表 20-1　ICMP タイプ一覧

タイプ	メッセージタイプ	内容
0	問い合わせ	エコー応答
3	エラー	宛先到達不能
4	エラー	始点抑制
5	エラー	リダイレクト
8	問い合わせ	エコー要求
11	エラー	データグラムの時間超過
12	エラー	データグラムのパラメータ異常
13	問い合わせ	タイムスタンプ要求
14	問い合わせ	タイムスタンプ応答
15	問い合わせ	情報要求　＜使用されなくなっている＞
16	問い合わせ	情報応答　＜使用されなくなっている＞
17	問い合わせ	ネットマスク要求
18	問い合わせ	ネットマスク応答

応答時のコードにはエラーメッセージのエラー番号が入るが(注 2)、問い合わせメッセージの場合は常に 0 が入ることになっている。また、チェックサムは、データ受信時に分割されたパケットに不足がないか確認するためのものである。受信したパケットを再計算して本領域の数値と一致しているか確認する。

注 1:タイプが不明な ICMP メッセージを受信した場合、そのメッセージは破棄される。これは ICMP 自体に問題が発生した場合のことを考慮し、ICMP エラーメッセージ処理を繰り返し行わないような仕組みになっているためである。

注 2:タイプ 3-5 および 11-12 のエラーメッセージはさらに種類が分類される。より細かく種類を指定するためにコードが利用されるが、問い合わせメッセージはタイプでの分類以上に種類が細かくないため一律で 0 となる。

次に、ICMP タイムスタンプおよび ICMP ネットマスクについて考察する。ICMP タイムスタンプ(要求/応答)は、図 20-7 に示すような ICMP メッセージ部を持つ。送信時のタイムスタンプ要求は ICMP タイプ 13 であり、返送時のタイムスタンプ応答は ICMP タイプ 14 である。また、エラーメッセージではないため、コードは常に 0 となる。開始タイムスタンプには、ICMP タイムスタンプ要求が送信された時間情報が入る。その後、タイムスタンプ要求を受信したホストは、それを受信した時間情報と送信元へ返送する時間情報を記憶し、それぞれの時間情報を受信タイムスタンプおよび送出タイムスタンプに入れて送信元ホストをタイムスタンプ応答として送信する。

図 20-7 ICMP タイムスタンプメッセージ

攻撃者はタイムスタンプ応答に含まれる受信タイムスタンプ、あるいは送出タイムスタンプの時間情報から、対象ホストで設定されている時刻を推測することができる。この結果、対象ホストの物理的な場所を特定することや、対象ホストにおいて時刻ベースの認証方式が使用されている場合、タイムスタンプを調べることで不正接続やなりすましが行われる可能性がある。

ICMP ネットマスク(要求/応答)は、図 20-8 に示すような ICMP メッセージ部を持つ。なお、送信時のネットマスク要求は ICMP タイプ 17 であり、再送時のネットマスク応答は ICMP タイプ 18 である。また、ICMP タイムスタンプと同様にエラーメッセージではないため、コードは常に 0 となる。

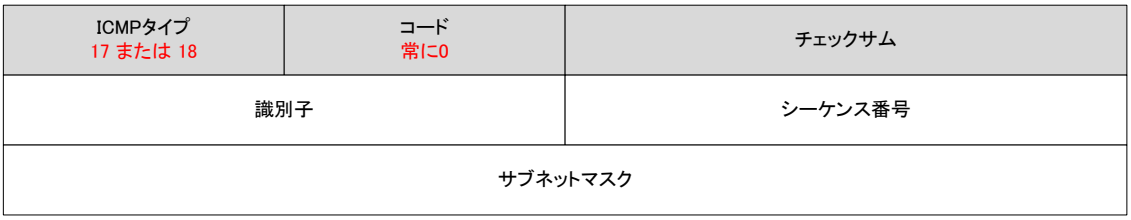


図 20-8 ICMP ネットマスク要求/応答メッセージ

前述のとおり、ICMP ネットマスク(要求/応答)のメッセージフォーマットは、RFC950 で規定された。送信元ホストがブロードキャストする ICMP ネットマスク要求では、32 ビットのサブネットマスクの値は 0 に設定される。ICMP ネットマスク要求(Type:18)を受信した対象ホストは、サブネットマスクに自分が属するネットワークのサブネットマスク情報を入れ、ICMP タイプを 18 に変更した後に当該メッセージをローカルユニキャストで返送する。なお、識別子およびシーケンス番号は 1 つのネットワークに 1 つのサブネットマスクしか存在しないため、使用されないことが多い。

この ICMP ネットマスク要求/応答を悪用して、攻撃者は不正に対象ホストが属するネットワークのサブネットマスクを取得する。これにより、なりすましや対象ホストに接続して更なる攻撃が行われる可能性がある。

上記で説明した問題は ICMP の仕様上、あるいは ICMP 要求に応答してしまう限り防ぐことはできない。また、Ping Flood 攻撃や PING(ICMP エコー要求)と同様の目的として、ICMP タイムスタンプや ICMP ネットマスクの要求/応答を悪用されることで、サービス不能攻撃やホストの生存確認にも利用されてしまう危険性も考えられる。

20)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題は、1999 年に Common Vulnerabilities and Exposures(CVE)においてセキュリティ問題として取り上げられた。当時はデフォルトで ICMP 要求に応答してしまう製品が多く、ファイアウォール等を使用したパケットフィルタリングによるセキュリティ対策が十分に浸透していなかった。詳細は不明であるが、ICMP 要求の応答を許可する環境に対して注意を促す意図があって公開されたものと考えられる。

また 1997 年頃からリリースされた Nmap や Nessus 等の多くのセキュリティスキャナーには ICMP プロトコルのタイプ別にメッセージを送信し、対象ホストの生存状況等を確認する機能が実装されており、ICMP はネットワークセキュリティにおける基本的な概念として考えられている。現在では ICMP 機能を有効にすることはセキュリティ上好ましくないという考えから、ファイアウォール機能等を利用してデフォルトで ICMP 要求に応答しないように設定された製品も多く存在している。

しかし、環境や用途、運用方法によって ICMP は不可欠な存在として利用されている。タイプ別に ICMP 要求への応答を許可するか否かを設定できる機能が実装されたものや、デフォルトで全ての ICMP 要求に応答する製品も存在する。このように、ベンダや製品利用目的等によって ICMP の扱いに対する考え方は様々で利用用途によって ICMP の実装は考えられており、対策もそれに従って考えられている。

20)-5. IPv6 環境における影響

本問題には ICMP タイプ 13、14 および 17、18 を利用するが、ICMPv6 にはこれに相当するメッセー

ジは存在しないため、IPv6 環境においてはこの問題の影響を受けない。

しかし、ICMPv6 においても多岐に渡るリクエストの種類があるため、本問題に関わる問題以外のリクエストで重要な情報を取得されてしまう等の影響がある。このため、ICMPv6についてもICMPと同様の考え方が必要と言える。

20)-6. 実装ガイド

1. 信頼できる送信元からのみ ICMP タイムスタンプ要求およびネットマスク要求に応答を返すよう実装する。

20)-7. 運用ガイド

1. ICMP タイムスタンプ要求およびネットマスク要求に対して応答を返さないように設定を変更する。
2. ファイアウォール等のフィルタリング機器を使用して、ICMP パケットを破棄する。

20)-8. 参考情報

この問題についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本問題調査時点(2010 年 5 月)のものである。

1981 年 RFC792, Internet Control Message Protocol
http://www.ietf.org/rfc/rfc792.txt

1985 年 RFC950, Internet Standard Subnetting Procedure
http://www.ietf.org/rfc/rfc950.txt

1994 年 RFC1700、 Assigned Numbers
http://www.ietf.org/rfc/rfc1700.txt

1999 年 Common Vulnerabilities and Exposures CVE-1999-0524
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0524

2001 年 SecureScout ICMP Timestamp Reply Vulnerability
http://descriptions.securescout.com/tc/11010
SecureScout ICMP Netmask Reply Vulnerability
http://descriptions.securescout.com/tc/11011
WHITEHATS.CA Netmask-based ICMP Echo Request Smurf Broadcast Scanning with Crafted ICMP Payloads using SendIP
http://www.whitehats.ca/main/members/Jeff/gcia_assign_2/gcia_assign_2.html

2009 年 VMware Security Response to CAN-1999-0524:
http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1434

参考: マスタリング TCP/IP 応用編 p.106-120

21).IPv6 実装における Forwarding Information Base の更新に関する問題

21)-1. 分類:ICMP 【IPv6】

21)-2. 概要

一部の IPv6 製品における近隣探索（NDP:Neighbor Discovery Protocol）の実装に問題があり、細工された近隣要請(Type:135)を受信することで、経路情報である Forwarding Information Base（以後、「FIB」と記載する）が汚染されて適切に通信を転送できない状態となり、結果として意図しない通信が行われる可能性がある。

21)-3. 解説

攻撃手法とその影響

現在の TCP/IP を実装する多くの製品では、目的のホストまで最適な経路でかつ高速にパケットの送受信や転送が行われるように実装されており、そのために必要となる経路情報や IP アドレス対応表といった、パケットを送出するために必要な情報が各ノードで管理されている。IPv6 において各ノード間でこのような情報をやり取りし、パケット送信のために必要なことが近隣探索であり、近隣探索は IPv6 ルーティングと密接な関係にある。本問題は、偽装された近隣探索メッセージを利用することで IPv6 ルータの経路情報を汚染させることができる問題である。

本問題を攻撃者に利用されることで、結果的に通信の妨害(サービス不能状態)や盗聴などの影響を受ける可能性がある。本問題を利用した攻撃手法について図 21-1 から図 21-9 に示す。なお、本問題は影響がある製品の最適な経路の決定に関連があると考えられるが、この経路決定方法については影響を受ける製品ベンダにおいて詳細情報が公開されていない。このため、本問題が再現する攻撃手順や影響を受ける仕組み、再現状況については詳細不明ではあるが、ここでは考えられる一例として解説を進める。

図 21-1 にこの攻撃の説明に使用する環境を示す。問題となるのは、複数のインタフェースを持ち、IPv6 ルータ機能を実装する標的のゲートウェイ A である。ここでは第三者のホスト X から第三者のホスト C への通信を攻撃者のホスト B に転送して盗聴する方法について解説する。

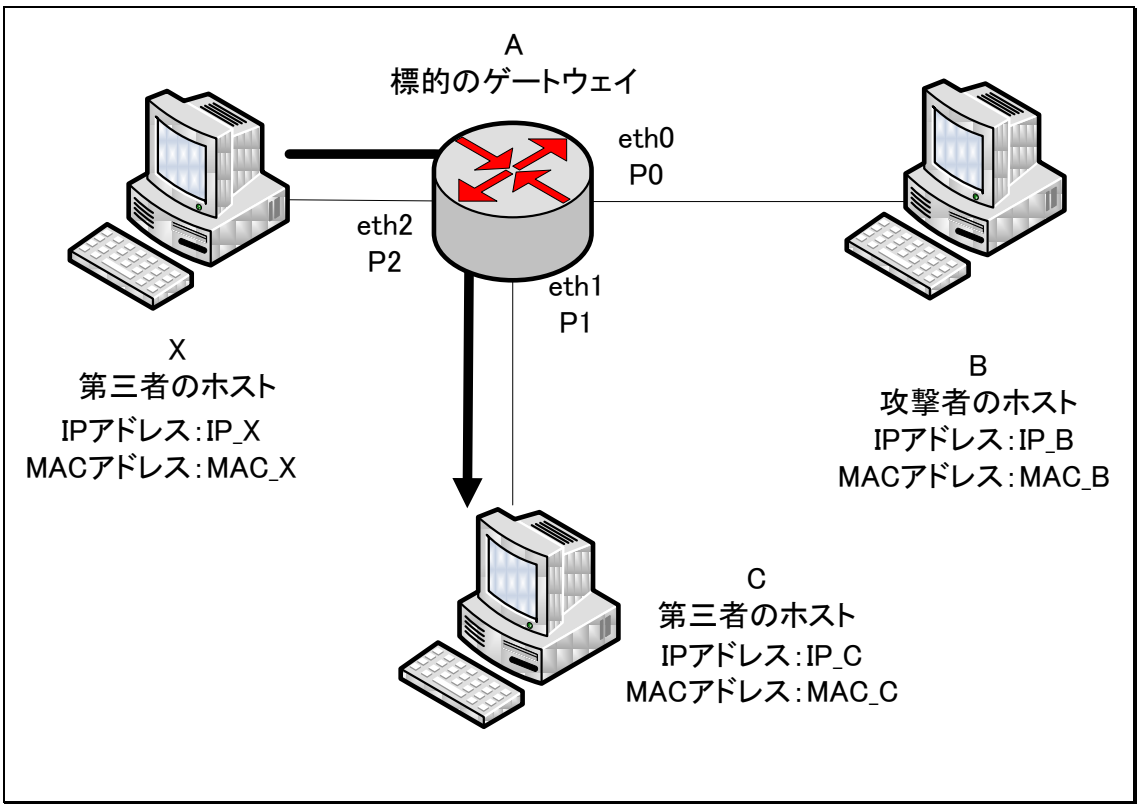


図 21-1 ターゲットネットワーク

図 21-2 に示すように、まず攻撃者は攻撃者のホスト B から問題がある標的のゲートウェイ A に対して、送信元 IP アドレスを偽装した近隣要請(Type：135)を送信する。ここで、送信元 IPv6 アドレスは第三者のホスト C のアドレス IP_C に偽装する。問題が再現する条件として、攻撃者は送信元 IP アドレスが on-link ではないプレフィックスを持つ IPv6 アドレスを使い、偽装する必要がある。(注 1)

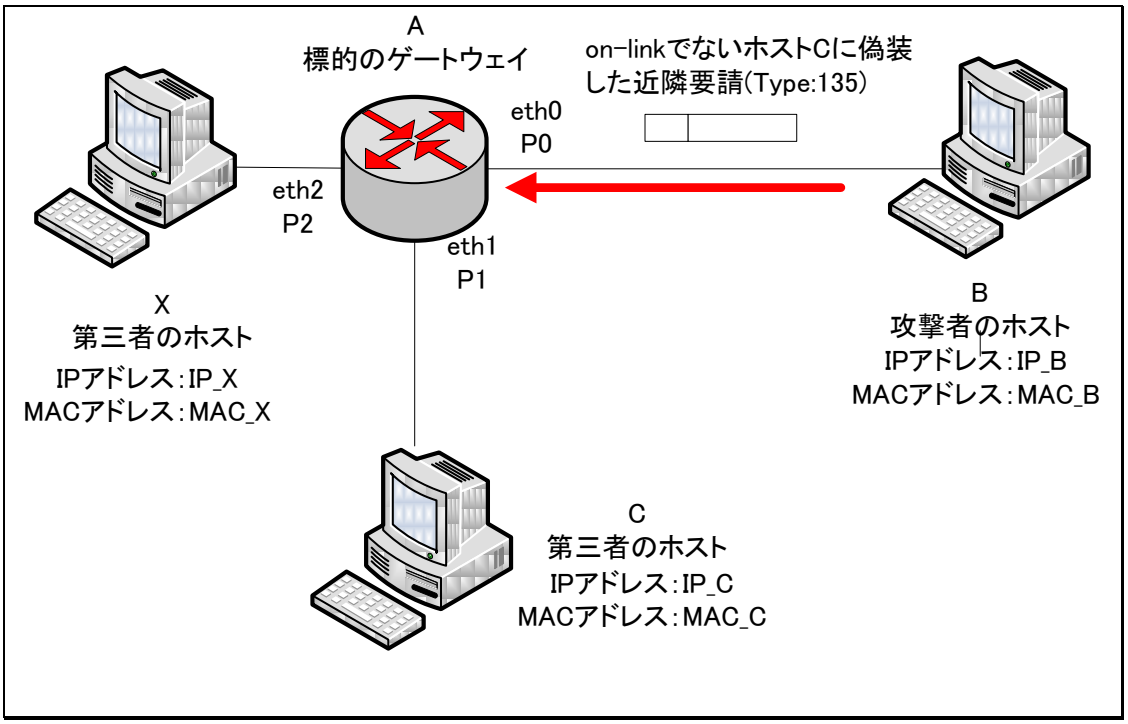


図 21-2 近隣要請(Type：135)の送信

注 1:プレフィックスとはリンク上のインタフェースに割り当てられないアドレスであり、近隣探索が届かない状態のこと。プレフィックスは IPv6 のアドレス構造で IPv4 のネットワーク部分に相当する部分を指す。ここでは攻撃者のホスト B 上が配置されたインタフェースに全ての IPv6 アドレスのプレフィックスが一致している状態とする。

この時に標的のゲートウェイ A が受信する近隣要請メッセージの構造は図 21-3に示すとおりである。近隣探索では、ICMPv6(プロトコル番号:58)メッセージを利用しており、IPv6 ヘッダ内の次ヘッダ領域に 58 が指定される。また近隣探索の機能はタイプ 133 から 137 の 5 つのメッセージタイプがあり、このうち本問題に利用される近隣要請はタイプ 135 に相当するため、ICMPv6 ヘッダのタイプ領域には 135 が指定される。

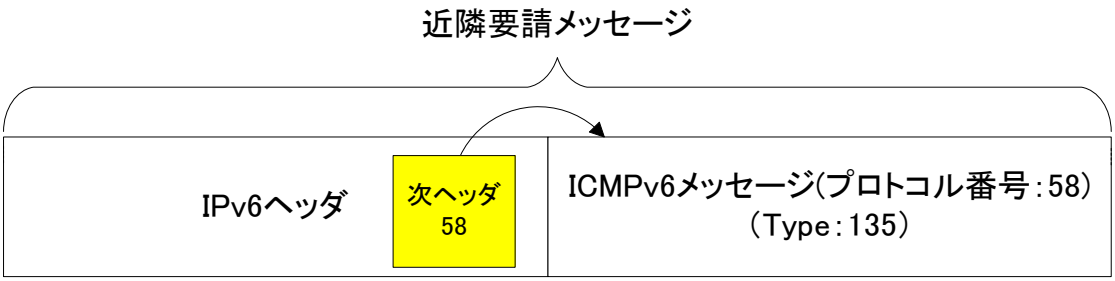


図 21-3 近隣要請メッセージの構造

近隣要請(Type:135)は、同一リンク内のルータを含むノードのアドレス解決(IPv4 における ARP に相当する)、到達可能かどうかの確認、重複アドレス検出を目的に送信されるが、ここではアドレス解決を目的としたメッセージ構造に沿った近隣要請(Type:135)を送信する。このため、図 21-3 における IPv6 ヘッダ内は図 21-4 のようになる。

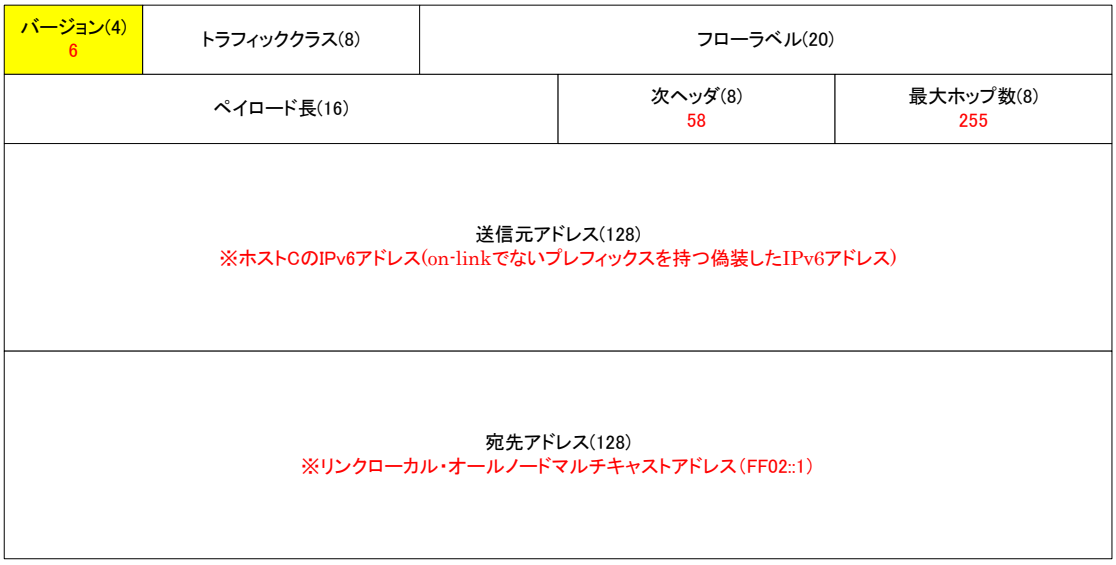


図 21-4 近隣要請(Type:135)メッセージにおける IPv6 ヘッダ内

送信元アドレスは本来攻撃者のホスト B となるが、この場合第三者のホスト C のアドレス（on-link でないプレフィックスを持つ偽装した任意の送信元 IPv6 アドレス）を指定する。また、近隣要請(Type：135)の最大ホップ数にはルータを超えた転送を禁止するという意味の 255、宛先アドレスには送信先の IPv6 アドレスが入る。なお、アドレス解決を目的とした場合には、IPv4 におけるブロードキャストアドレスに相当するリンクローカル・オールノードマルチキャストアドレス（FF02::1）を指定することになる。

つまり、図 21-5 に示すようにここでの想定では近隣要請(Type：135)は同一リンク内の全ノードに送信されることになる。

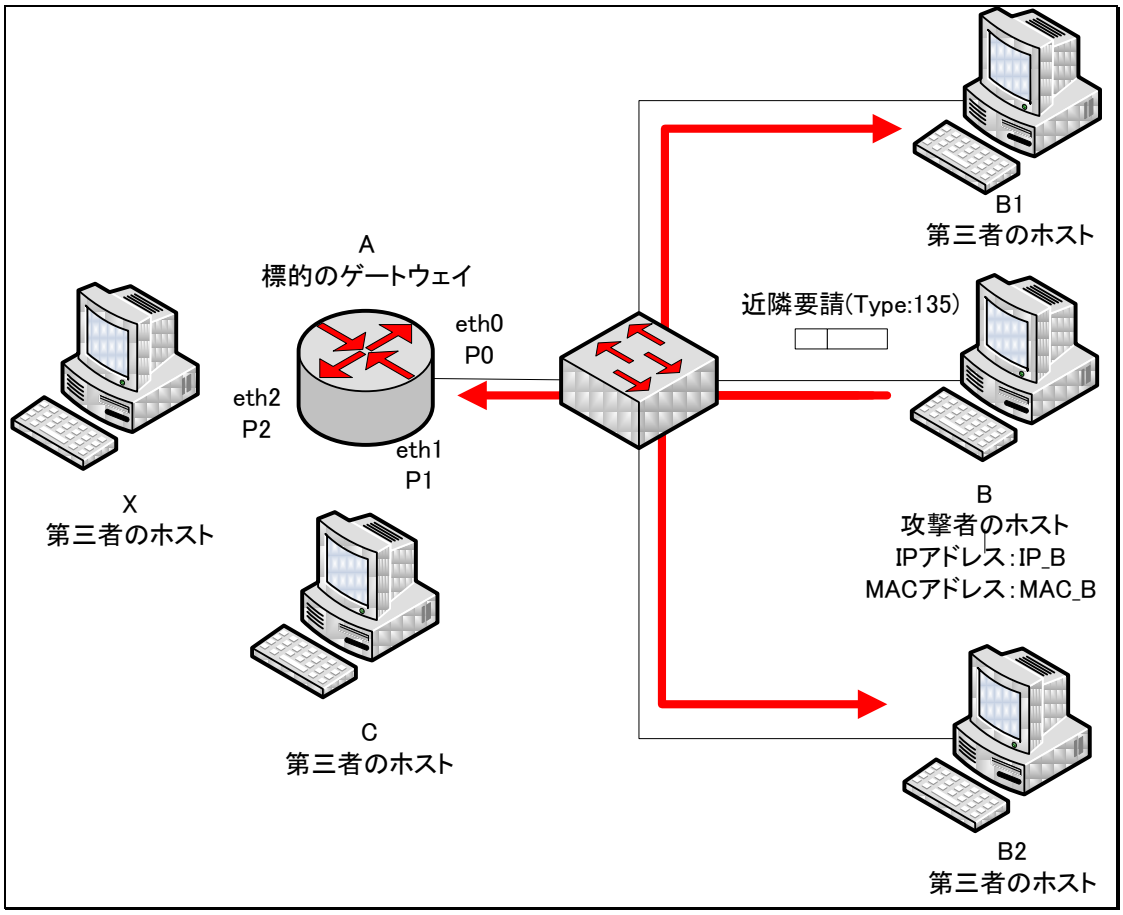
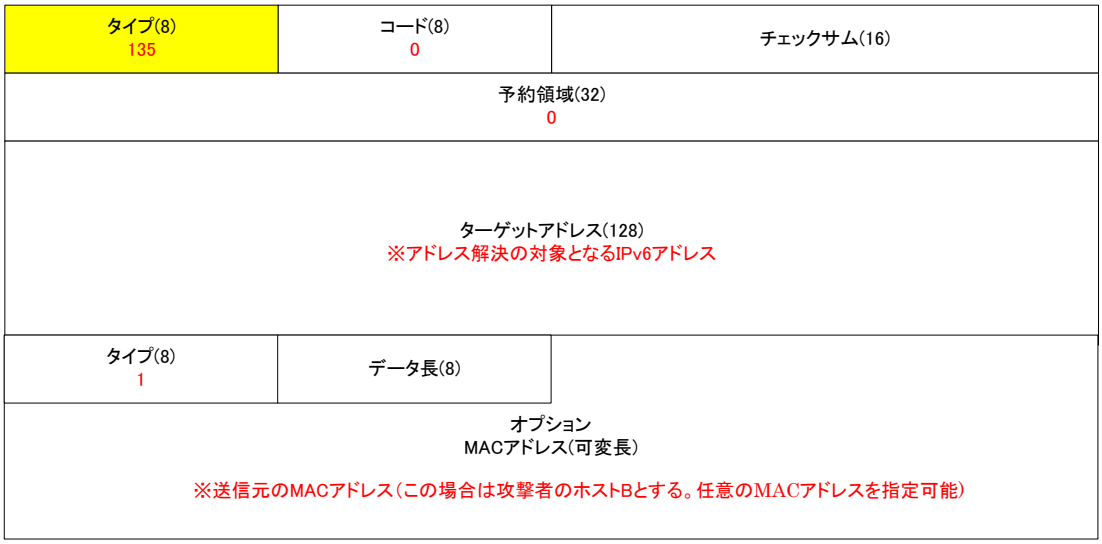


図 21-5 近隣要請（Type:135）をリンクローカル・オールノードマルチキャストアドレスに送信する

さらに図 21-3 の ICMPv6 ヘッダ内は図 21-6 のようになる。近隣要請(Type:135)の構成上、タイプ領域には 135、コード領域には 0 が設定される。また、予約領域は 0 であり、ターゲットアドレスには本来の近隣要請(Type:135)メッセージの構造ではアドレス解決の対象となる IPv6 アドレスの指定となるため、ここでは、近隣キャッシュの汚染を試みる標的のゲートウェイ A の IPv6 アドレスとする。

また、アドレス解決の場合にはオプション領域に送信元 MAC アドレスの指定が必須になるため、ここでは攻撃者のホスト B の MAC アドレスを指定する。ただし、攻撃者はこの領域に任意の MAC アドレスを指定可能である。



※( )内はビット数

図 21-6 近隣要請(Type:135)メッセージにおける ICMPv6 ヘッダ内

上述したオプション領域に MAC アドレスを含んだ近隣要請(Type:135)を標的のゲートウェイ A が受信すると、この偽装された情報を基に IP アドレスと MAC アドレスの対応表である近隣キャッシュの更新を試みる。近隣キャッシュ内に該当するエントリが無い場合は新たに作成され、既存のエントリと受信した MAC アドレスが異なる場合には、エントリが更新される。(注 2)

注 2:ここでは、アドレス解決を目的としたメッセージ構成で近隣要請(Type:135)を送信し、近隣キャッシュが更新されることにしているが、他のメッセージ構造でも近隣キャッシュが更新される。

この結果、図 21-7 に示すようなイメージでインタフェース eth0 において第三者のホスト C の IPv6 アドレスをキーとするエントリが近隣キャッシュに保持される。(注 3)

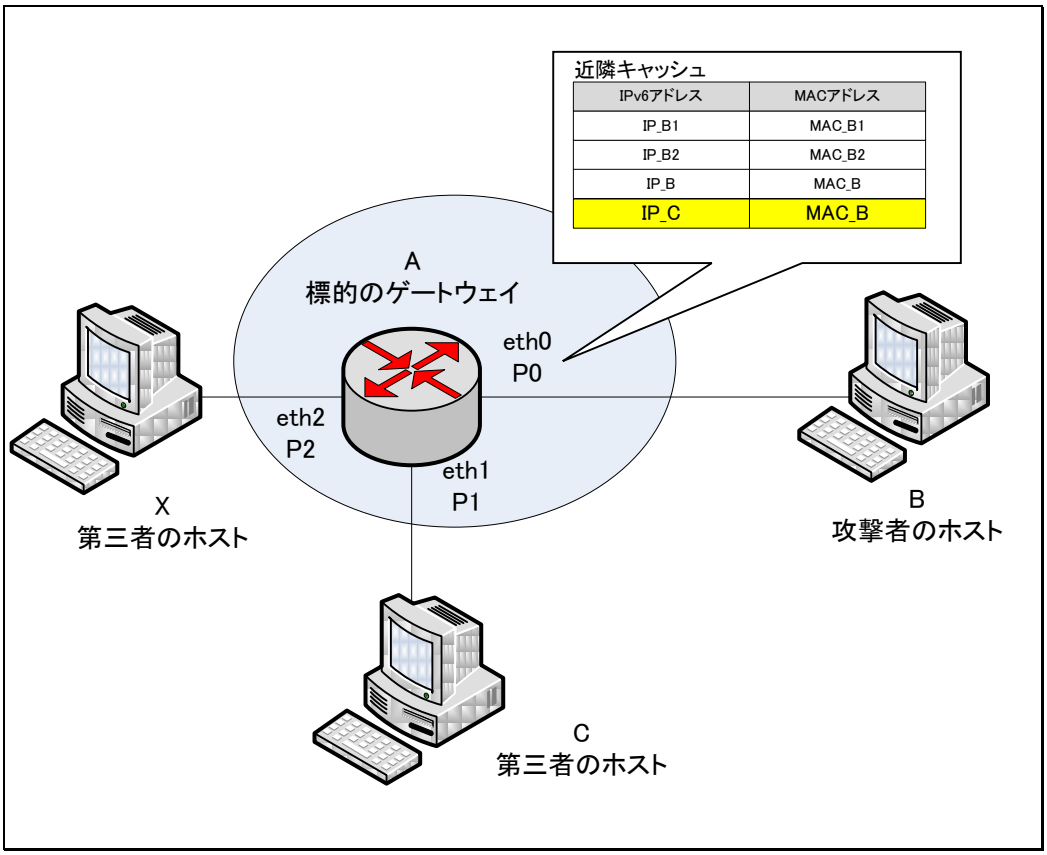


図 21-7 近隣キャッシュの更新

ここで、幾つかのルータ機能を持つ IPv6 製品では、受信した送信元 IPv6 アドレスに IP_C、送信元 MAC アドレスに MAC_B が指定された近隣要請(Type:135)によって作られた近隣キャッシュの保持データを基に、そのまま FIB という経路情報の更新を試みてしてしまう可能性がある。FIB は宛先プレフィックスや次ホップ、インタフェースなどの情報を持ち、パケットを最適な経路で高速に転送するために利用されもので、ルータは FIB の情報を基に経路を決定する。

注 3:近隣要請(Type:135)を受信したゲートウェイ A は、その後メッセージの送信元に対して近隣広告を送信することで近隣キャッシュが更新されたことを通知し、攻撃者が近隣広告のターゲット MAC アドレスを自身の近隣キャッシュに書き込み、更新する。

このように、問題がある標的のゲートウェイ A は汚染された近隣キャッシュを基に FIB を更新してしまい、この結果図 21-8 のように標的のゲートウェイ A はホスト C への通信が正常に通信できなくなる FIB を保持することになる。(注 4)

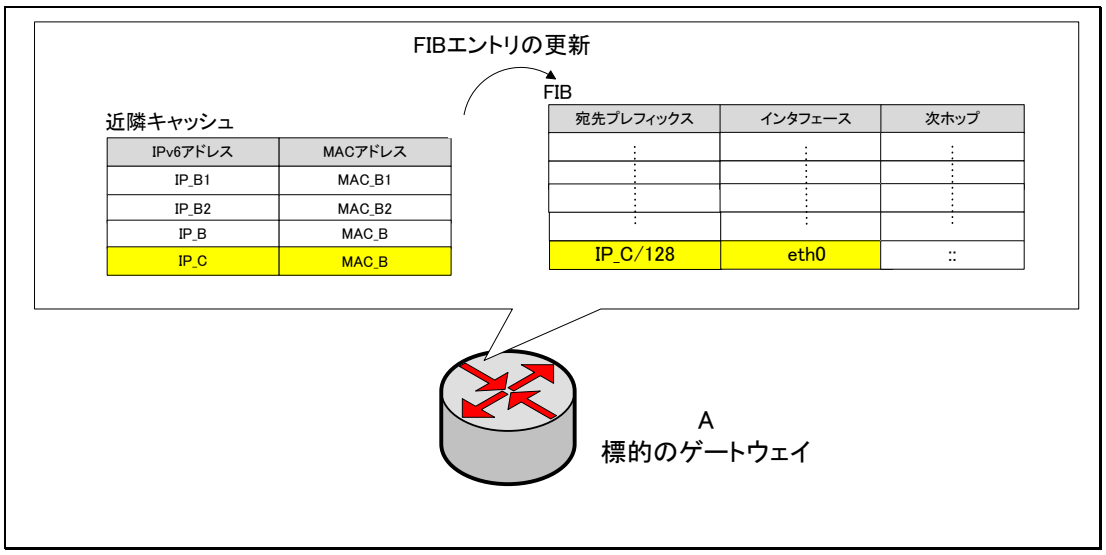


図 21-8 汚染された近隣キャッシュを基に FIB を更新

標的のゲートウェイ A の状態が図 21-8 に遷移した後は図 21-9 のような状態となり、第三者のホスト X から第三者のホスト C への通信を標的のゲートウェイ A が受信すると、ルーティング処理により汚染された FIB を参照してしまい、本来転送されるインタフェース eth1 ではなく eth0 に転送され、正常にルーティングすることができなくなる可能性がある。さらに、近隣キャッシュを参照すると影響を受ける通信の送信先ホストであったホスト C は攻撃者のホスト B の MAC アドレス(MAC_B)として対応付けられているため、標的のゲートウェイ A はホスト X からホスト C への通信内容をホスト B に転送してしまう可能性があり、これにより攻撃者はホスト B 上で通信を傍受できる可能性がある。

注 4:この問題の影響を受ける一部ベンダにおいて、ホスト経路相当の情報が経路情報として登録されるという記述がある。

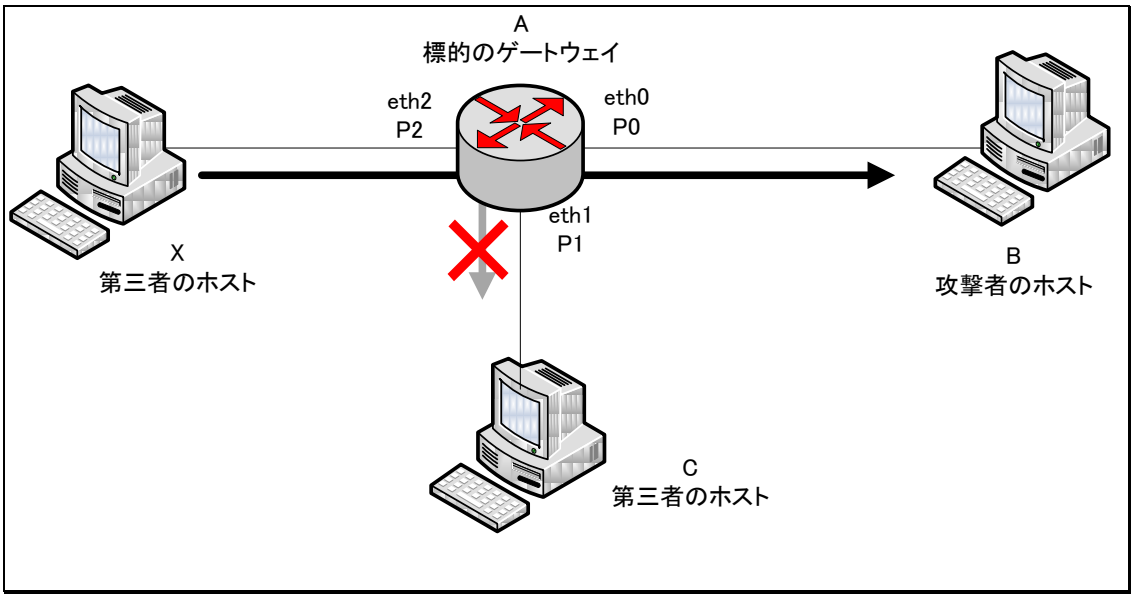


図 21-9 標的のゲートウェイ A での意図しない通信の発生

この問題を利用することで、攻撃者は on-link ではないプレフィックスを持つ送信元 IP アドレスを使用した近隣要請(Type:135)を問題があるルータに送信することにより、任意の IPv6 アドレスと任意の MAC アドレスを近隣キャッシュにエントリさせることが可能となり、この結果がルーティングに影響を及ぼす可能性がある。このため、同じルータ上で物理的に異なるネットワークに配置されたホスト間の通信経路を操作できる可能性があり、任意の IPv6 アドレスや MAC アドレスを指定することで盗聴の他にも、通信の妨害やさらには第三者のホストへのなりすましが行われる可能性がある。

なお、この攻撃を成立させるためには攻撃対象のホストの IPv6 アドレスを把握する必要があると考えられる。またこの攻撃が成立している状況下においては、状況次第で経路情報が元の状態に戻りルーティングが正常な状態に戻ることも考えられる。この場合、攻撃者がこの汚染した経路情報を維持するためには、定期的に偽の近隣要請メッセージを送る必要がある。

原因と考察

この問題は、次の 2 つの事象によって生じる問題であると考えられる。

1. 偽装された近隣要請(Type：135)を受信し、自身の近隣キャッシュにエントリを追加あるいは更新する（近隣キャッシュの汚染）。
2. 汚染された近隣キャッシュを基に FIB を更新する。

まず 1. については、近隣キャッシュの保守方法および近隣探索の仕様に関係がある。近隣キャッシュの実装および保守方法については OS や IPv6 製品を提供するベンダ等によって異なることが考えられるが、近隣キャッシュの汚染に関する脅威は本問題が発見される以前から既に指摘されている。

近隣探索に関わる様々なセキュリティ脅威については RFC 3756「IPv6 Neighbor Discovery(ND) Trust Models and Threats」で論じられており、ここでは本問題と類似する脅威として近隣要請(Type:135)/近隣広告(Type:136)のなりすましによる脅威が指摘されているなど、偽装した近隣探索メッセージを利用した攻撃の 1 つとして考えられる。近隣探索のメッセージタイプは表 21-1 に示すとおりである。これらを利用した近隣キャッシュのエントリに関わる攻撃はこの他にも指摘されており、偽装した近隣探索メッセージの扱いについては近隣探索の実装上、根本的な対策がなく対応が困難であると考えられる。

表 21-1 近隣探索のメッセージ

名称	タイプ	送られる方向	内容
ルータ要請	133	ホスト → ルータ	ホストがリンク内のルータを探索するためにルータへ送信する。
ルータ広告	134	ルータ → ホスト	ルータがホストに自分の存在を知らせるために送信する。このメッセージにはアドレス自動生成、経路設定、通信パラメータ設定に必要な情報が含まれる。
近隣要請	135	ノード → ノード	ノードがアドレス解決の要請、到達可能かどうかの確認、重複アドレス検出のために送信する。
近隣広告	136	ノード → ノード	ノードが近隣要請(Type:135)への応答として返す。
リダイレクト	137	ルータ → ホスト	ルータがホストに、より適切な次ホップを教えるために送信する。

また 2. については、FIB を更新する際に何も考慮されていないために生じる問題と考えられるが、FIB の性質上、妥当性をチェックする処理を追加することが開発および実装の目的上困難であると推察される。また、冒頭でも述べたとおり、製品によって FIB の保守方法やルーティングの実装方法が異なることも考えられ、1.と同様に 2.についても製品の実装上、対応が困難であると考えられる。

なお、本問題の影響がないと報告しているベンダも存在しており、ルーティングや FIB 保守の方法など、経路決定に関する各製品の実装設計の段階によって影響有無が変わることが推察される。

21)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題は David Miles 氏により発見され、UNITED STATES COMPUTER EMERGENCY READINESS TEAM(US-CERT)によって 2008 年 10 月に VU#472363 として公開された。本問題が公開された以降、影響を受ける IPv6 製品を提供する多くのベンダにおいて影響有無に関する情報やアドバイザリが公開されており、パッチや修正バージョン、回避策等が示されている。現在では多くのベンダで既にこの問題の対処が行われているが、一部のベンダでは対策を検討している。詳細については、各ベンダが公開するアドバイザリを参照のこと。

また本問題を利用した攻撃を完全に防ぐには、SEND(SEcure Neighbor Discovery)や認証機能、パケットの正当性検証の実装といった IPv6 近隣探索へのセキュリティ配慮が求められるが、SEND の普及や設定の複雑さの観点から、未だ現実的な解決策は無いのが現状である。そのため、on-link ではないプレフィックスを持つ送信元アドレスを受信しなければ本問題の影響がないため、これを基に対策方法を提示しているベンダが多く見受けられており、例えば偽装された近隣要請(Type:135)を受信しないように修正されたパッチの適用やバージョンアップ、設定変更の対策を推奨している。

21)-5. IPv4 環境における影響

この問題は IPv6 近隣要請を利用した近隣キャッシュに関わる問題であるため、IPv4 では影響がない。ただし影響範囲が異なるが、IPv4 においては近隣キャッシュと同等の役割を担う ARP キャッシュの汚染に関する問題が既に指摘されている。詳細については 23)「ARP テーブルが汚染される問題」を参照のこと。

21)-6. 実装ガイド

1. uRPF(unicast Reverse Path Forwarding)機能を実装し、本来受信するインタフェースからのみ受信する。
2. SEND を実装する

21)-7. 運用ガイド

ベンダよりセキュリティパッチが提供されている場合には、これを適用することが推奨される。修正パッチが提供されていない、もしくは適用できない場合、下記の対策を実施することで、影響を少なくすることができる。

1. インタフェースに設定された IPv6 アドレスのプレフィックス以外の送信元アドレスを持つ近隣要請(Type:135)をフィルタ等で破棄する。
2. インタフェースにおいて本来受信するプレフィックスが指定された送信元 IPv6 アドレスのからのみ受信するように設定する。
3. 盗聴対策として https 通信等のアプリケーション層の暗号化を利用する。

21)-8. 参考情報

この問題についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本問題調査時点(2010 年 4 月)のものである。

2004 年 IPv6 Neighbor Discovery(ND) Trust Models and Threats(RFC 3756)
http://www.ietf.org/rfc/rfc3756.txt

2005 年 SEcure Neighbor Discovery(SEND)(RFC3971)
http://www.ietf.org/rfc/rfc3971.txt

2007 年 Neighbor Discovery for IP version 6(IPv6)(RFC4861)
http://www.rfc-editor.org/rfc/rfc4861.txt

2008 年 Vulnerability Note VU#472363 IPv6 implementations insecurely update Forwarding Information Base
http://www.kb.cert.org/vuls/id/472363
Common Vulnerabilities and Exposures CVE-2008-2476
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2476
Common Vulnerabilities and Exposures CVE-2008-4404
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4404
IPv6 Neighbor Discovery Protocol routing vulnerability
http://security.freebsd.org/advisories/FreeBSD-SA-08:10.nd6.asc
Multiple Vendors IPv6 Neighbor Discovery Protocol Implementation Address Spoofing Vulnerability(Juniper Networks)
http://www.juniper.net/security/auto/vulnerabilities/vuln31529.html

JVNVU#472363 IPv6 実装における Forwarding Information Base のアップデートに関する問題
http://jvn.jp/cert/JVNVU472363/
JVNDB-2008-001801 IPv6 NDP 実装における Neighbor Discovery メッセージの送信元検証処理に関する脆弱性
http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001801.html
IPv6 実装における Forwarding Information Base のアップデートに関する問題(日本電気株式会社)
http://www.nec.co.jp/security-info/secinfo/nv08-011.html
AX-VU2008-04「IPv6 近隣探索プロトコルに存在する脆弱性」に関するご報告(アラクサラネットワークス)
http://www.alaxala.com/jp/techinfo/security/20081003.html
「IPv6 近隣探索プロトコルに存在する脆弱性」に関するご報告(株式会社 日立製作所)
http://www.hitachi.co.jp/Prod/comp/network/notice/IPv6ND.html
FreeBSD Security Information IPv6 Neighbor Discovery Protocol routing vulnerability
http://security.freebsd.org/advisories/FreeBSD-SA-08:10.nd6.asc
Multiple vendor IPv6 NDP implementation denial of service(IBM Corporation)
http://xforce.iss.net/xforce/xfdb/45601
JVNDB-2008-001802 IBM zSeries 上の IPv6 NDP 実装における Neighbor Discovery メッセージの送信元検証処理に関する脆弱性
http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001802.html

2009 年 Common Vulnerabilities and Exposures CVE-2008-4404
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4404

2010 年 IPv6 実装における Forwarding Information Base のアップデートに関する問題(ネットワーク製品)(富士通株式会社)
http://fenics.fujitsu.com/products/support/2010/ipv6_02.html

参考: マスタリング TCP/IP IPv6 編 p.68-79、p.84-94、p.99-104

22).フラグメントパケットの再構築時にシステムがクラッシュする問題 (Teardrop Attack)

22)-1. 分類:IP 【IPv4】【IPv6】

22)-2. 概要

2 つのフラグメントパケット間においてデータが重複するようにフラグメントオフセット値が設定されているフラグメントパケットを受信すると、このフラグメントパケットを正常に再構築できないシステムでは、サービス不能状態に陥る。

22)-3. 解説

攻撃手法とその影響

攻撃者は不正に作成された 2 つのフラグメントパケットを、標的ホスト A に送信し攻撃を行なう。送信される 2 つのフラグメントパケットを第 1 フラグメント、第 2 フラグメントとして、図 22-1 にその様子を示す。この際、第 2 フラグメントのフラグメントオフセットを、最初に送信される第 1 フラグメントのデータサイズよりも意図的に小さく設定する。ホスト B においてこれらのフラグメントパケットを再構築させることで、問題を発生させる。

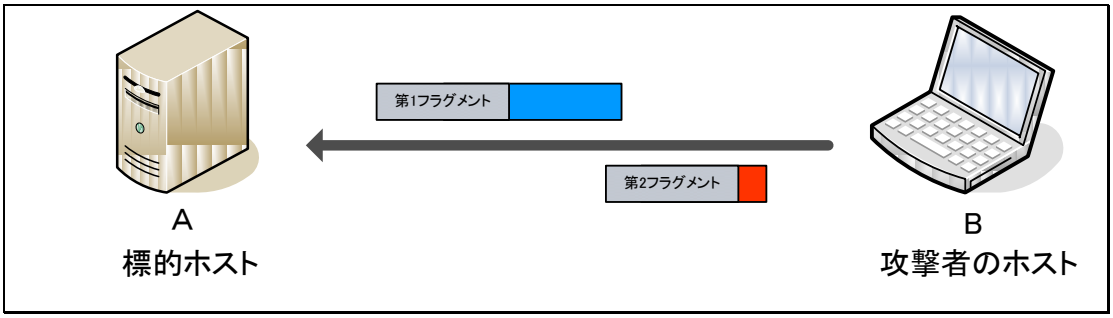


図 22-1 送信されるフラグメントパケット

問題を発生させるフラグメントパケットの具体的な例として、第 1 フラグメントおよび第 2 フラグメントにおける各値を図 22-2 に示す。

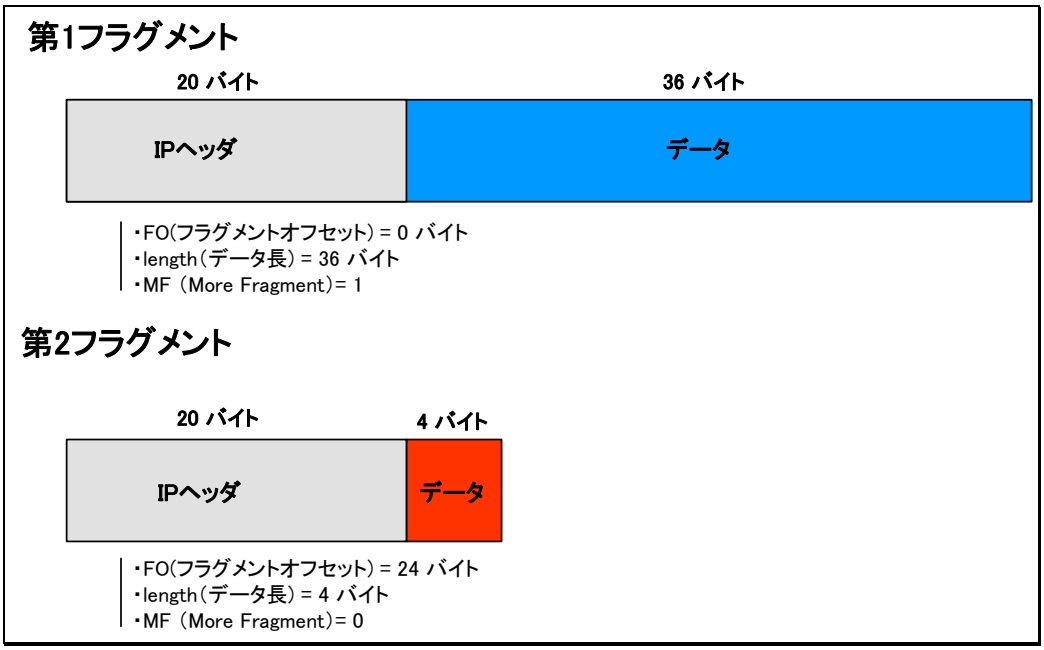


図 22-2 第 1 フラグメントと第 2 フラグメントの各値

通常のフラグメントデータでは、第 1 フラグメントのデータの後には第 2 フラグメントのデータが続く。そのためには、第 2 フラグメントのフラグメントオフセット値には、第 1 フラグメントのデータの終端である 36 バイトが指定されていなければならない。

しかし攻撃に利用されるフラグメントパケットでは、第 2 フラグメントのオフセット値は 24 バイトが指定されている。つまり第 2 フラグメントのデータは、第 1 フラグメントのデータの終端よりも前の位置となるデータであることを指し示している。フラグメントパケットを受信し再構築の処理を行なうホスト A では、第 1 フラグメントのデータ中に第 2 フラグメントのデータが重複する形のデータであるとして解釈される。

この際の送信されたフラグメントパケットが再構築された際のデータ配置を図 22-3 に示す。尚、図中(a)は通常想定されるフラグメントオフセットにより再構築された場合のデータ、(b)は一方のデータが他方のデータに内包されるようにフラグメントオフセット値が設定されている場合のデータを示している。

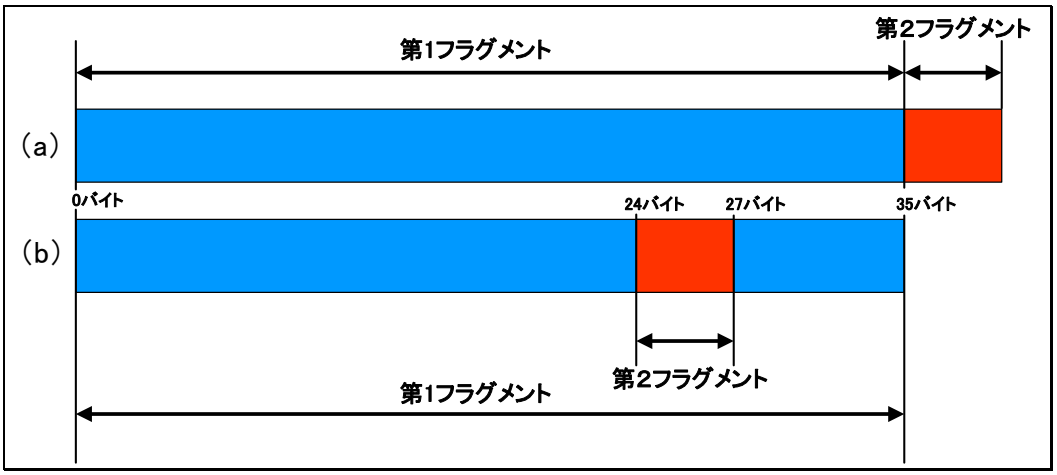


図 22-3 再構築後のフラグメントデータ

ホスト B において、このようにデータが重複するフラグメントパケットを正常に処理できないという TCP/IP の実装上の問題を保持していた場合、システムのクラッシュやリブート、ハングアップといった事象が発生し、結果としてサービス不能状態に陥る。

原因と考察

ネットワーク上にデータを転送するとき、ネットワークによって決められている MTU(Maximum Transmission Unit)を超えるような IP パケットは、複数の小さな IP パケット(フラグメントパケット)に分割して送信される。OS によって詳細な箇所は異なるが、Teardrop Attack の原因は、データが重複しているフラグメントパケットの再構築時における処理の不備によるものである。

例えば、Linux Kernel 2.0.32 未満におけるフラグメント再構築の実装では、フラグメントデータのサイズのチェックの処理で、過度に大きい値であるかどうかのチェックは行なわれていたが、小さい値であるかどうかのチェックが行なわれていなかったことに起因している。また、フラグメントデータが重複する場合のアルゴリズムでは、フラグメントデータサイズの計算方法が適切ではなかったため、データサイズを表す特定の変数に負の値が格納される。その後の処理において、フラグメントデータサイズ分のメモリ領域を割り当てるため、memcopy()関数にこの変数が渡されると、符号なしの過大な正の値として処理され、結果としてリブートやシステムの停止が発生しサービス不能状態に陥ってしまう。

22)-4. 発見の経緯とトピック、対策の動き、現在の動向

1997 年 11 月、この問題を発見した G P R 氏の Bugtraq メーリングリストへの投稿により脆弱性がインターネット上に公開された。メールには Linux Kernel および Windows NT 4.0 / Windows 95 を対象とした Exploit コード「teardrop.c」が記載されており、以降この問題による攻撃は Teardrop Attack としてサービス不能(DoS)攻撃としては代表的な 1 つに挙げられている。

同年 12 月には CERT Advisory CA-97.28 が公開され、TCP/IP 実装に起因する、同じく代表的な DoS 攻撃の 1 つである LAND Attack と同時に注意喚起が行なわれている。

1997 年に最初の Teardrop Attack が報告されて以来、1998 年には bonk、boink、newtear、2000 年には Teardrop2 というように、いくつもの変種の攻撃が報告されている。影響としてはいずれもサービス不能状態を発生させるものである。Teardrop Attack とこれらの複数の変種の違いは送信フラグメントのサイズによるものであり、根本的な部分については Teardrop Attack と同様である。

近年においては、既知の問題として各 OS で修正済みであり、類似した手法による攻撃は一般的な機能を持つ IDS/IPS やファイアウォールでも検知・防御を行なうことが可能である。

22)-5. IPv6 環境における影響

Teardrop Attack はパケット再構築処理において重複するフラグメントパケットを正常に処理できないという実装上の問題を利用した DoS 攻撃である。RFC2460 に規定されているとおり IPv6 には IPv6 拡張ヘッダとしてとしてフラグメントヘッダ(次ヘッダ値:44)(注 2)が存在し、フラグメント化が許可されている。そのため、IP プロトコルのバージョンに限らずパケットの再構築処理は行われる。(注 3) また、RFC2460 ではフラグメントの重複を禁止するような記述も無いため、概念的には IPv6 環境でもこの問題は再現すると考えられる。

さらに、既に多くのベンダではこの問題に対する対処が行われているため、現在においては IPv6 でも対策済みであると考えられるが、IPv4 と同様に IPv6 の重複するフラグメントパケットを正常に処理できない問題が実装上にある場合には、影響を受ける可能性がある。ただし、IPv4 において各製品のフラグメント再構築の実装方法によって再現性および影響は異なっているため、実際に IPv6 において影響があるかどうかは不明である。

また、Internet-Draft 版ではあるが 2007 年 7 月時点で IPv6 フラグメントに関する規定「Operational issues with Tiny Fragments in IPv6(IPv6 の Tiny Fragment の操作上の問題)」と「IPv6 Fragments and treatment of Tiny fragments(IPv6 Fragment と IPv6 Tiny Fragment の扱いについて)が公開されており、IPv6 においてもフラグメントの扱いに関して十分なセキュリティの配慮が必要とされている。

注 2: IPv6 フラグメントヘッダの形式については、図 5-5 を参照のこと

注 3: IPv6 のフラグメント化は送信元ノードだけで実行される。IPv4 のようにパケットの配送を行うルータでは実行されない。IPv6 におけるフラグメントの再構成についての詳細な手順および処理については RFC2460(セクション 4.5)を参照のこと

22)-6. 実装ガイド

フラグメント再構築の処理において、適切なアルゴリズムを実装することで本脆弱性を排除することができる。

1. フラグメントデータサイズのチェックを適切に行う。
2. フラグメント間でデータが重複する場合のフラグメントサイズの算出を適切に行う。

22)-7. 運用ガイド

ベンダよりセキュリティパッチが提供されている場合は、これを適用することで脆弱性を排除することができる。その他の対策を含め、具体的には以下のとおりである。

1. 影響を受ける製品に対して各ベンダより提供されているパッチを適用する。
2. ネットワークのゲートウェイ部分で、一般的な機能を持つ IDS/IPS やファイアウォールを導入し、同種の攻撃に対する検知・防御を行う。

22)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年7月)のものである。

1981 年 RFC 791, Internet Protocol.
http://www.ietf.org/rfc/rfc0791.txt

1997 年 SecurityFocus 124
http://www.securityfocus.com/bid/124
無効な ICMP データグラムフラグメントによる Windows NT、Windows 95 のハングアップ

http://support.microsoft.com/kb/154174/ja

CERT Advisory CA-1997-28

http://www.cert.org/advisories/CA-1997-28.html

http://www.lac.co.jp/business/sns/intelligence/cert_advisory/CA-97_28.html

Caldera Security Advisory SA-1997.29

http://packetstormsecurity.org/advisories/caldera/SA-1997.29.txt

1998 年 The "Bonk" NT/Win95 fragmentation attack 【bendi 著】

http://www.insecure.org/sploits/95.NT.fragmentation.bonk.html

・ DoS 攻撃ツールとして bonk.c が公開される。

Windows NT Teardrop2 Attack 【Jiva DeVoe 著】

http://www.windowsitpro.com/Articles/Index.cfm?ArticleID=9290&DisplayTab=Article

・ DoS 攻撃ツールとして boink.c が公開される。

ISS X-Force Database teardrop-mod(343)

http://xforce.iss.net/xforce/xfdb/343

・ DoS 攻撃ツールとして newtear.c が公開される。

RFC2460, Internet Protocol, Version 6(IPv6) Specification

http://www.ietf.org/rfc/rfc2460.txt

1999 年 Common Vulnerabilities and Exposures CVE-1999-0015

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0015

Common Vulnerabilities and Exposures CVE-1999-0104

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0104

Common Vulnerabilities and Exposures CVE-1999-0258

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0258

2000 年 変種の teardrop Attack により Windows NT 4.0 から STOP 0x0000000A, 0x00000019 エラーが発生する

http://support.microsoft.com/default.aspx?scid=kb;ja;179129

23).パケット再構築によりメモリ資源が枯渇される問題(Rose Attack)

23)-1. 分類:IP 【IPv4】【IPv6】

23)-2. 概要

IP 分割パケットの最初のパケット(第 1 フラグメントパケット)と最後のパケット(最終フラグメントパケット)を送信することで、受信ホストではこの不完全なフラグメントパケットを破棄するまでの間、パケットデータを確保するためにメモリ領域を占有してしまうため、正常なフラグメントパケットを受け付けなくなる。

23)-3. 解説

攻撃手法とその影響

Rose Attack は、IP フラグメンテーションにおけるパケット再構築(Reassembly)処理の仕組みとその実装方法を巧妙に利用した攻撃である。図 23-1 に 2 種類のフラグメントパケットを送信する様子を示す。

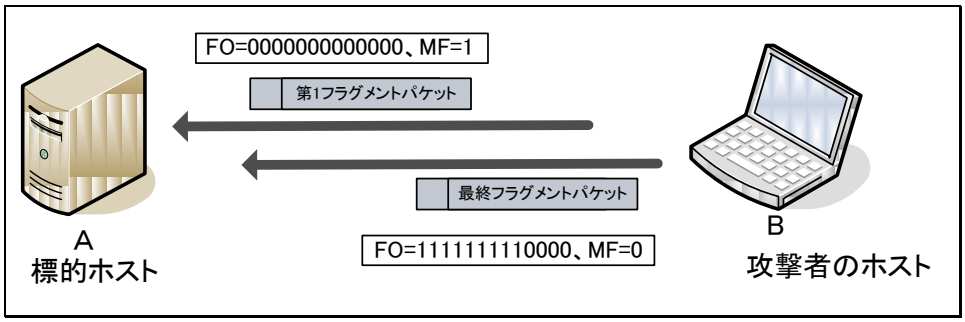


図 23-1 Rose Attack の 2 種類のフラグメントパケット

攻撃者は、ホスト B からフラグメントオフセット(FO)が 0 の第 1 フラグメントパケット(FO=0、MF=1)を標的ホスト A に送信し、続けてホスト B から FO が大きい最終フラグメントパケット(例えば FO=8176、MF=1。FO を 2 進数で表すと 1111111110000 となる。)を標的ホスト A に送信する。そしてこれを利用して可能な限り大きいサイズを装ったフラグメントパケットを送りつけることでメモリ領域を大量に占有することが可能となる。

最初と最後の 2 種類のフラグメントパケットを受信した標的ホスト A では、パケット再構築のために途中のフラグメントパケットが全て送信されるまでは不完全なフラグメントパケットとしてメモリ領域に確保される。このフラグメントパケットはタイムアウトになるまで、あるいは全てのフラグメントパケットが送信されない限りは破棄されない仕組みとなっている。攻撃者はこれを悪用して繰り返し不完全なフラグメントパケットを送りつけることで、標的ホスト A 上に確保されたメモリ領域を大量に消費させることが可能である。この状態が続くホスト A では正当なフラグメントパケットを受信できなくなってしまったり、システム負荷が高まったりしてしまう。その結果サービス不能状態に陥ってしまう可能性がある。

また Rose Attack に類似するフラグメント処理を悪用した New Dawn Attack と名付けられている攻撃手法がある。図 23-2 にこの攻撃で用いるフラグメントパケットを送信する様子を示す。

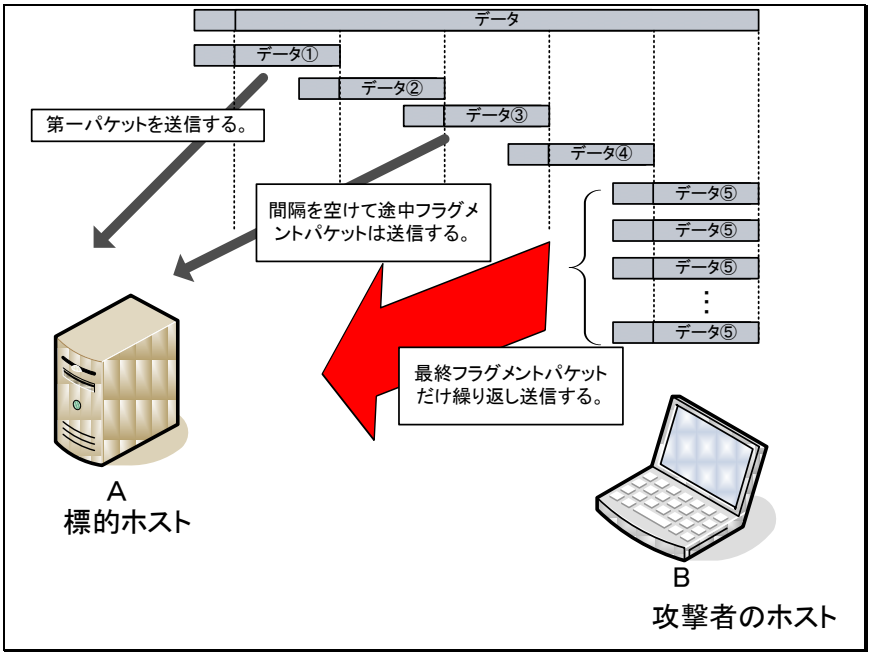


図 23-2 New Dawn Attack で使用するフラグメントパケット

まず攻撃ホスト B から第 1 フラグメントパケットをホストに送信する。次いで、完全なパケットにならないように間隔を空けて中間のフラグメントパケットを幾つか送信し(図 23-2 ではデータ③のみ)、最後に最終フラグメントパケットを標的ホスト A に送信する。

Rose Attack 同様に不完全なフラグメントパケットを送信することに違いはないが、この攻撃は最終フラグメントパケットを繰り返し送りつける。標的ホスト A では受け取った全てのフラグメントパケットに対してパケット再構築を試みるため、この処理により CPU 資源が大量に消費される。この結果 CPU 使用率が急上昇し、システムクラッシュや再起動してしまうなどのサービス不能状態に陥ってしまう。

パケット再構築はメモリと CPU 時間に大きな負担を課すが、標的ホスト A における影響の度合いについてはそれぞれの攻撃手法の違い、マシンスペックや OS の違い、そして送信されるフラグメントパケットの総数などの違いによって異なることが考えられる。

原因と考察

問題の引き金となっている IP パケット再構築(Reassembly)処理については RFC 791 と FRC 815 に示されている。この問題は多くの TCP/IP の実装で利用されている RFC 791 のパケット再構築のアルゴリズムを利用した攻撃である。FRC791 のパケット再構築処理は、各フラグメントパケットの IP ヘッダ中のフラグメント・フラグ(More Fragment: MF)とフラグメントオフセット(Fragment Offset: FO)、パケット長に加え、タイマを使用する。図 23-3 に IP データグラムのフォーマットを示す。

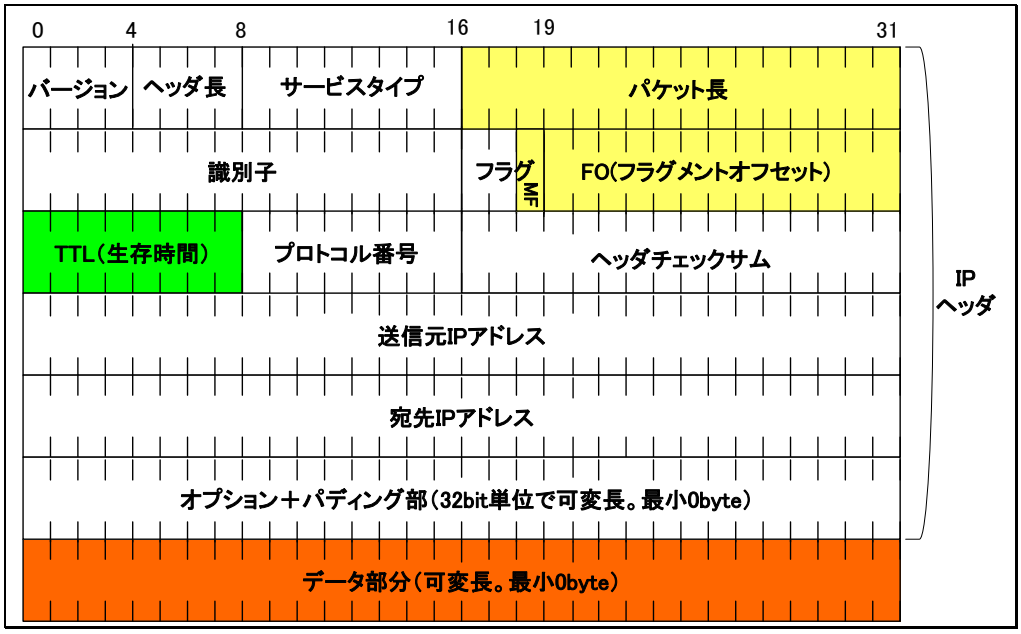


図 23-3 IP データグラムフォーマット

タイマはパケットの再構築を放棄するためのタイムアウト時間のことで、タイムアウト時間を過ぎると全ての再構築処理が停止しパケット全体が破棄される。RFC 791 によるとタイムアウト時間は初期値に 15 秒を設定することが推奨されており、この現在のタイマ値と到着したフラグメントパケット中の TTL(Time To Live:生存時間(図 23-3 緑色部分に示す))を比較して大きい値に再設定される。つまりタイマの最大値は TTL の最大値(225 秒)となる。

IP パケットを受け取ると、まず MF、FO からフラグメントパケットかどうかが確認され、フラグメントパケットであれば上位プロトコルにデータを渡すために幾つかの手順を経てパケットの再構築処理が行われる。しかし、タイムアウト時間を過ぎても全てのフラグメントパケットが揃わずに不完全な場合、パケットデータ全体が破棄される。

ネットワーク上にデータを転送するとき、ネットワークによって決められている最大伝送単位(MTU : Maximum Transmission Unit)を超えるような IP パケットは、複数の小さな IP パケット(フラグメント)に分割して宛先ホストに送信される。フラグメント処理は MTU の長さで分割して届けられ、受信ホストでは全てのフラグメントパケットが届くまでフラグメントデータは確保されたバッファ(キュー)に格納される。

Rose Attack の場合、攻撃者は 2 つのフラグメントパケットを意図的に送信し、このうち最終フラグメントパケットは IP ヘッダ中の MF を 1 に設定する。本来最終フラグメントパケットの MF には、後続のデータが存在しないことを示すゼロ(0)を指定するが、後続の IP パケットが存在するかのように見せてその到着を待たせるために 1 を設定する。到着を待たせている間により多くのバッファを占有しておくため、可能な限り大きいサイズでパケットを送る必要がある。IP プロトコルで運べるパケットの最大サイズは 64k バイト(65536 バイト)だが、実際にはこのような大きなサイズのパケットを 1 つのパケットで送信することができる物理ネットワーク媒体は存在しない。

フラグメントパケットの最大生存時間は 255 秒だが、RFC 791 では変更しても良いことになっており、発見者の報告によると Windows 2000 は 2 分、Sun Solaris は 4 分、Mandrake Linux は 30 秒などというように OS によってタイムアウト設定値が異なる。そのためメモリ資源を枯渇させる Rose Attack は OS によって影響の度合いが大きく異なると考えられる。また RFC 791 ではパケット再構築待ちとなるフラグメントパケットの取り扱いやタイムアウト時のパケット破棄については言及していない。

一方で New Dawn Attack については Rose Attack とは異なり、IP フラグメント処理のタイムアウトには起因せずに発生する。このため、OS に関わらず影響が及ぶ可能性がある。Rose Attack がパケット再構築における不完全なフラグメントパケットを破棄する仕組みを利用してメモリ資源の枯渇を引き起こすのに対し、New Dawn Attack は通常では起こり得ない無駄な処理を繰り返し引き起こすことでシステム負荷を高める。発見者が公開するサイトには Rose Attack と New Dawn Attack の Exploit コードを利用した幾つかのテストパターンの検証結果が公開されている。(注 1)

この結果を見ると、この攻撃はマシンスペックや送信されるフラグメントパケットの総数に加えて影響が異なることがわかる。また、標的ホストの OS によっても異なっており、特に Microsoft Windows に対しての攻撃が効果的であると見受けられる。

この攻撃は応答要求を受け取る必要の無いことから IP 偽装が可能であり、TCP 以外の UDP、ICMP プロトコルでも利用可能である。また、IPv6 環境下でこの問題が再現する可能性についても指摘されている。

注 1: Attack Results for all attacks http://digital.net/~gandalf/Rose_Frag_Attack_Explained.htm#item4

23)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題は 2003 年に William K. Hollis 氏が SANS Institute の GIAC GCFW 認定試験での課題論文を作成する際に考え出した攻撃である。論文の記述で発見者によって"Rose Attack"と名付けられている。その後、発見者自身によって BUGTRAQ メーリングリストにこの問題が投稿される。 ここで別のユーザによって幾つかの Exploit コードが公開され、より効果的な攻撃手法が提唱された。

New Dawn Attack を含め、この問題は TCP/IP を実装する多くの製品が影響を受ける可能性があるが、発見者によって影響を受けると報告されている OS のうち、一部を除いては 2004 年から 2005 年までの段階で既に修正が行われている。Microsoft Windows、IBM AIX については明確に修正されたことを示す情報については未確認だが、一部のセキュリティポータルサイトでは AIX がこの問題が解消されているなどの報告もあり、これ以降に発見された類似する問題やその他の TCP/IP の脆弱性と併せてこの問題が修正されている可能性も考えられ、一概には未解決であるとは言えない。

23)-5. IPv6 環境における影響

Rose Attack はパケット再構築処理を利用した攻撃である。RFC2460 に規定されているとおり IPv6 には IPv6 拡張ヘッダとしてとしてフラグメントヘッダ(次ヘッダ値:44)が存在し(図 5-5 を参照)、フラグメント化が許可されている。そのため、IP プロトコルのバージョンに限らずパケットの再構築処理は行われる。(注 2)この点から、概念的には IPv6 環境でもこの問題は再現すると考えられる。この問題が BUGTRAQ メーリングリストに投稿された際にも IPv6 での影響有無について議論が行われており、投稿者および閲覧者の間で IPv6 にも影響があると指摘されている。

ただし、Rose Attack は TCP/IP の実装方法によって大きく影響が異なり、また IP プロトコルのバージョンの違いによってパケット再構築を放棄する時間(タイムアウト値)や再構築の手順に違いがある点を考慮すると、IPv6 において攻撃を IPv4 と同様に効果的に実現できるのかどうかは不明である。

注 2: IPv6 のフラグメント化は送信元ノードだけで実行される。IPv4 のようにパケットの配送を行うルータでは実行されない。

注 3: IPv6 におけるフラグメントの再構成についての詳細な手順および処理については RFC2460(セクション 4.5)を参照のこと

23)-6. 実装ガイド

IP パケットの再構築処理において利用される IP ヘッダ中の値とタイマ値から不正なフラグメントパケットと判断するチェックを厳密に行うため、以下のアルゴリズムを実装する。

1. IP パケットの再構築処理において、以下のパラメータに対して制限を行う。
   (1)最大パケットサイズ
   (2)最小フラグメントサイズ
   (3) IP パケットの最大長
2. IP パケットの再構築処理におけるタイムアウト値を減少する。
3. パケット再構築を試みる回数を設定する。
4. IP パケットの再構築処理において、保持する最大フラグメント数を制限する。

23)-7. 運用ガイド

ベンダよりセキュリティパッチが提供されている場合は、これを適用することで脆弱性を排除することができる。また、ファイアウォール等を使用して不完全と判断したフラグメントパケットについては破棄するなど、緩和策を含めてネットワークおよびシステム全体での対策を必要とする。

1. 影響を受ける製品に対して各ベンダより提供されているパッチを適用する。
2. 上記実装ガイドに基づくチェックが行えるファイアウォール等を使用して不適切と判断したフラグメントパケットをフィルタする。
3. メモリやシステム資源を可能な限り確保することで、この問題を利用する攻撃を緩和する。

23)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2006 年 3 月)のものである。

1981 年 RFC 791, Internet Protocol.
http://www.ietf.org/rfc/rfc0791.txt

1998 年 RFC2460, Internet Protocol, Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2460.txt

2003 年 GIAC Enterprises Network Security GCFW V2.0【William K. Hollis 著】
http://www.giac.org/certified_professionals/practicals/gcfw/0462.php
http://digital.net/~gandalf/Rose_Frag_Attack_Explained.htm

2004 年 IPv4 fragmentation --> The Rose Attack(3/31)【Gundalf 著】
http://www.securityfocus.com/archive/1/359144
Rose Attack の説明および、検証が公開される。
Re: IPv4 fragmentation --> The Rose Attack(4/8)【Paul Starzetz 著】
http://www.securityfocus.com/archive/1/359863
ISS X-Force Database macos-tcp-ip-dos(16946)
http://xforce.iss.net/xforce/xfdb/16946
Common Vulnerabilities and Exposures CAN-2004-0744
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0744
Rose_Frag_Attack_Explained
http://digital.net/~gandalf/Rose_Frag_Attack_Explained.txt
Rose Attack および New Dawn Attack の詳細情報が公開される。
http://docs.info.apple.com/jarticle.html?artnum=300667
HP Security Bulletin HPSBUX02087
http://www1.itrc.hp.com/service/cki/docDisplay.do?docId=c00579189
Common Vulnerabilities and Exposures CVE-2005-4316
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4316
SecurityFocus 11258
http://www.securityfocus.com/bid/11258

Microsoft Windows IPv6 Packet Fragmentation Handling DoS
http://skateboard.osvdb.org/displayvuln.php?osvdb_id=10456&print

2005 年 IBM APAR - POTENTIAL DOS IN IP STACK
http://www-1.ibm.com/support/docview.wss?uid=isg1IY63365
http://www-1.ibm.com/support/docview.wss?uid=isg1IY63364
http://www-1.ibm.com/support/docview.wss?uid=isg1IY63363

24).IP 経路制御オプションが検査されていない問題(IP Source Routing 攻撃)

24)-1. 分類：IP 【IPv4】【IPv6】

24)-2. 概要

始点経路制御オプション(Source Route）は、ネットワークの経路(中継点)を設定するための IP オプションである。このオプションを使用すると、宛先アドレスが中継点のアドレスで順次置き換えられる。このことを利用して、始点経路制御オプションを検査していないフィルタを不正に通過できる可能性がある。

24)-3. 解説

攻撃手法とその影響

図 24-1 に、この攻撃の説明に使用する環境を示す。攻撃者のホストEは、自分の管理下にある攻撃元ルータDを経由して、攻撃対象ホストBと不正に通信を行うことを試みる。攻撃対象ホストBは、信頼ホストAからの通信のみを受け付けるように設定されている。

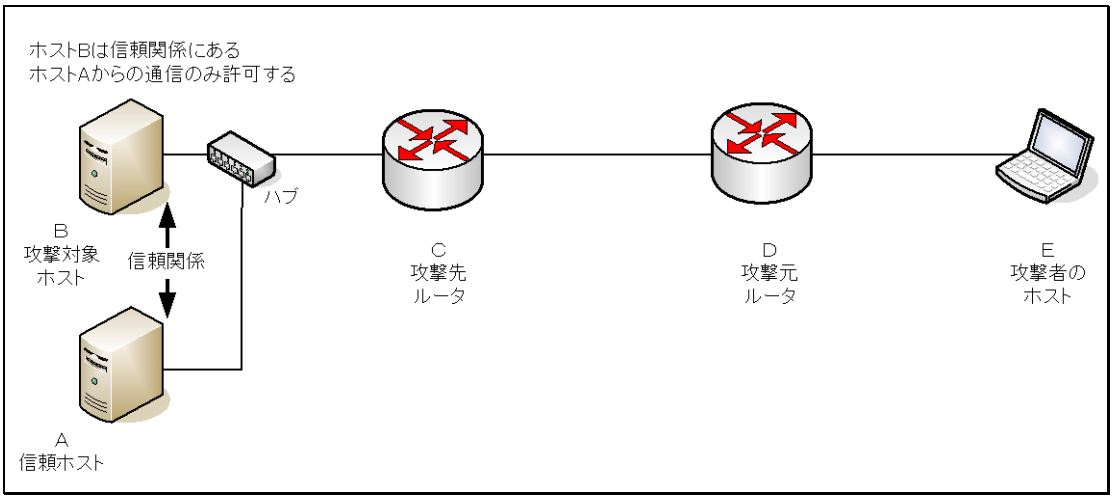


図 24-1 ターゲットネットワーク

図 24-2 は、攻撃者のホストEから攻撃対象ホストBへの経路を説明している。この攻撃では、ターゲットネットワークに、中継点として指定したルータ以外のルータが介在するため、経路オプションとして LSRR(Loose Source and Record Route）を利用する。

1. 攻撃者のホストEは送信先を攻撃元ルータD、中継点を攻撃対象ホストB、送信元を信頼ホストAのアドレスに指定したパケット送出する。
2. 攻撃元ルータDでは、中継点と送信先の入れ替えが行われる。
3. 攻撃先ルータCは、始点経路制御オプションを検査していない。そのため、この時点でこのパケットは、送信先が攻撃対象ホストB、送信元が信頼ホストAであるように見える。
   このパケットは、このまま攻撃対象ホストBに到達し、信頼ホストAからのように見えるパケットを攻撃対象ホストBは受け入れる。

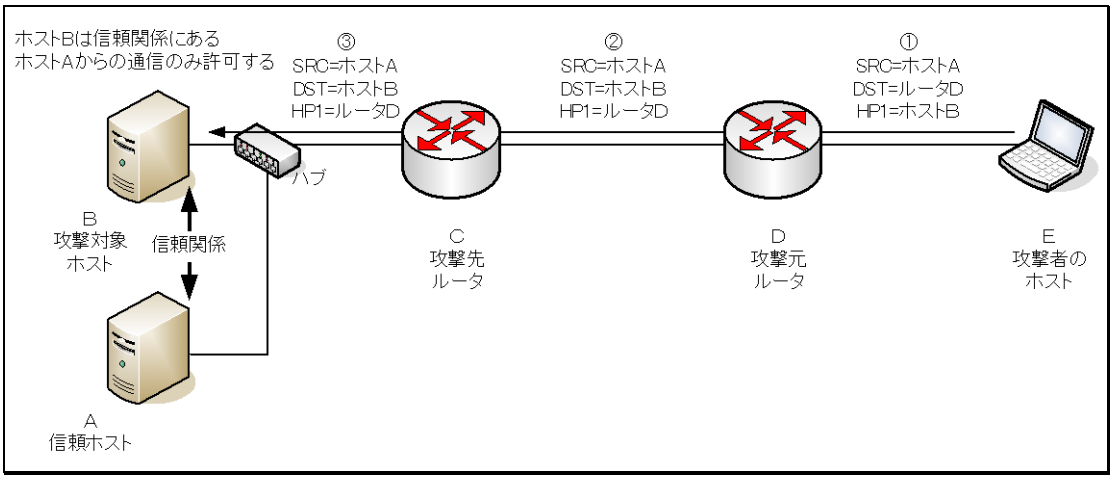


図 24-2 攻撃対象への攻撃

図 24-3 は、攻撃対象ホストBから攻撃者のホストEへの応答の経路を説明している。

4. 攻撃対象ホストBは、中継点と送信先を入れ替え、送信先を攻撃元ルータD、中継点を信頼ホストAに指定したパケット送出する。
5. 攻撃先ルータCは、このパケットをそのまま通過させる。
6. 攻撃元ルータDは、中継点と送信先を入れ替え、送信先が信頼ホストAとなる。このルータは、攻撃者の管理下にあるので、あらかじめ信頼ホストA宛のパケットが攻撃者のホストEに届くように設定しておく。

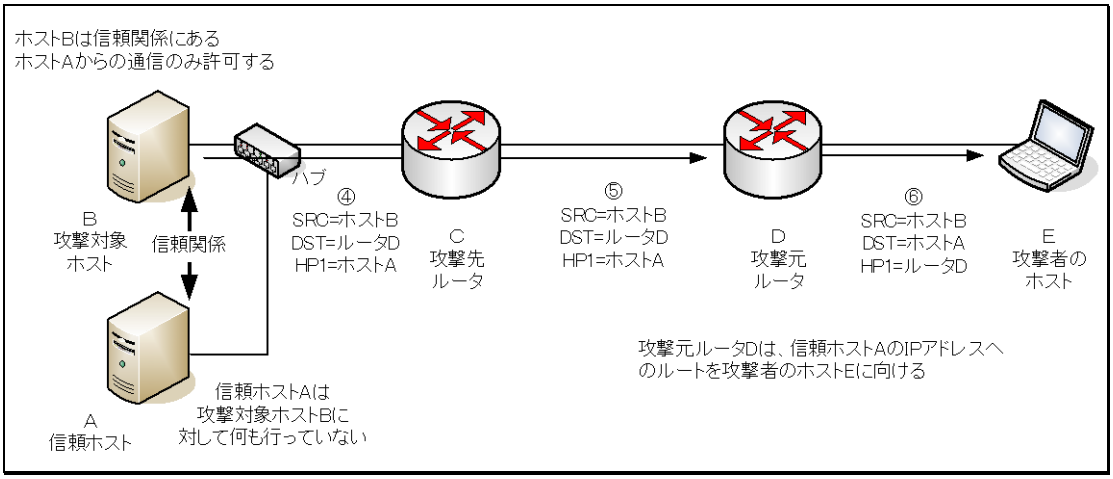


図 24-3 攻撃対象の応答

原因と考察

図 24-4 にソース・ルーティングの概要を示す。ホスト D は、送信先をルータ C で、中継点1にルータ C、中継点2にルータ B、中継点3にホスト A を設定して送信する。ルータ C は、送信先をルータ B に置き換えて送信する。ルータ B は、送信先をホスト A に置き換えて送信する。これらのパケットを、始点経路制御オプションを検査しない機器が受け取ると、中継点が送信先のように見えてしまう。

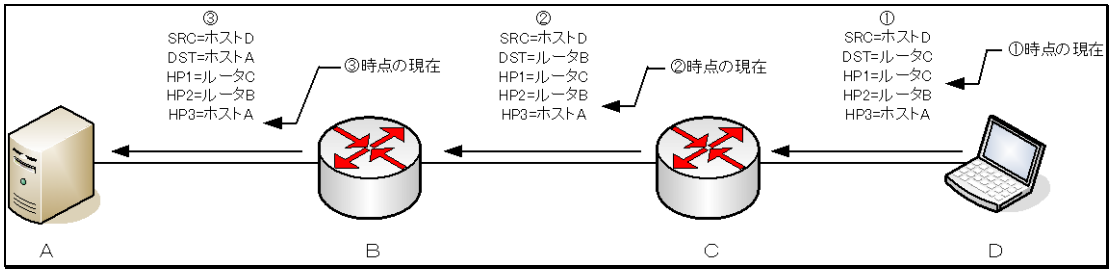


図 24-4 ソース・ルーティングの概要

始点経路制御オプションには、SSRR(Strict Source and Recorded Route)と、LSRR(Loose Source and Recorded Route)の２つのタイプがある。これらのオプションは図 24-5 のIPデータグラムヘッダ構造のオプション部に値が設定される。

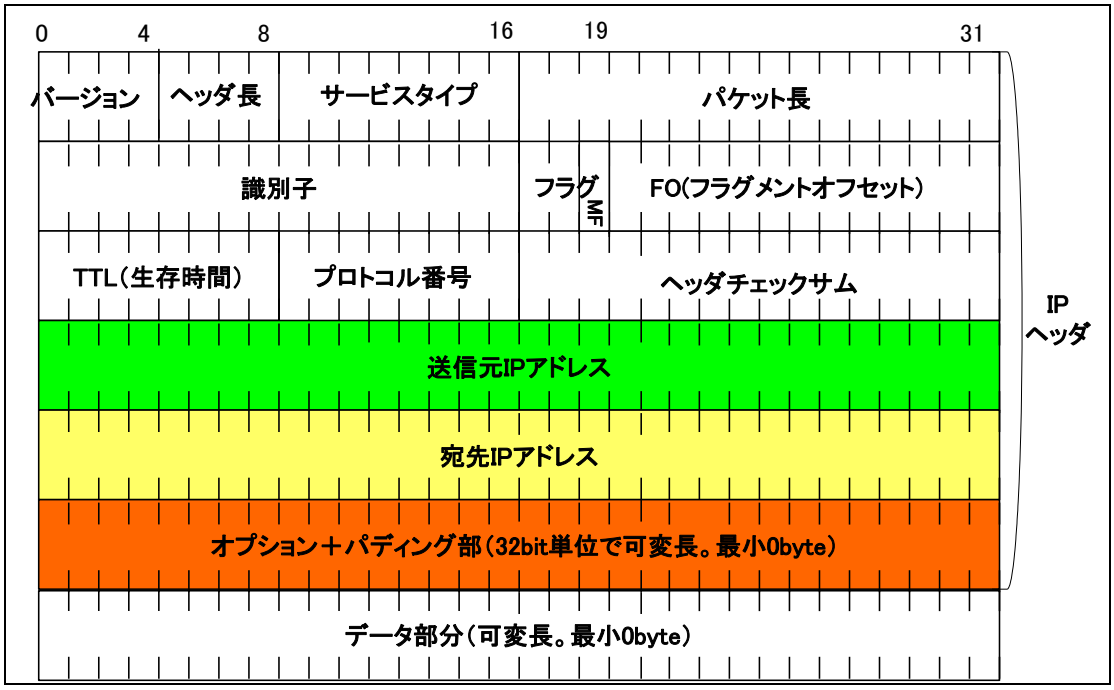


図 24-5 IPデータグラムヘッダ構造

LSRR(Loose Source and Recorded Route)

このオプションを使用する場合、必ず通らなければならない中継点を指定する。終点にたどり着くまでに、指定されていない中継点を経由しても良い。本オプションを使用する場合は図 24-6 のタイプフィールドに 131(10000011)を設定する。

タイプ	長さ	ポインタ	第１中継点IPアドレス（HP1）	第２中継点IPアドレス（HP2）	・・・・

図 24-6 ルーティングオプションの構造

SSRR(Strict Source and Recorded Route)

このオプションを使用する場合、指定された中継点以外のルータを経由することができない。中継点が SSRR に従うことが出来ない場合は、データグラムは破棄される。本オプションを使用する場合は図 24-6 のタイプフィールドに 137(10001001)を設定する。

LSRR、SSRR ともに、ポインタには中継点データ(route data)の先頭が、オプション相対ポインタとして設定されている(最小の初期値は4）。宛先(Destination）アドレスに到着し、かつポインタが長さより大きくない場合、ソースルートにある次のアドレスが宛先アドレスになり、そのとき使用している送信元アドレスを記録経路のアドレスに入れ、ポインタを 4 増加させる。

24)-4. 発見の経緯とトピック、対策の動き、現在の動向

IP Source Routing 攻撃は、1993 年に CERT Advisory CA-1993-07 Cisco Router Packet Handling Vulnerability として注意喚起された。

近年においては既知の問題として多くが対応済みであり、また同様の手法による攻撃は一般的な機能を持つファイアウォールでも防御を行なうことが可能である。

24)-5. IPv6 環境における影響

この問題はIPv4のソース・ルーティング機能を利用して送信元IPアドレスを詐称したパケットの送信により不正侵入を試みる攻撃であるが、IPv6 においてはソース・ルーティングに代わる機能として、拡張ヘッダのルーティングヘッダ(次ヘッダ値:43)が使用される。概念的には Type 0 ルーティングヘッダ(注 1)を使用することで IPv6 環境でもこの問題は再現すると考えられる。ルーティングヘッダの形式を図 20-7 に示す。

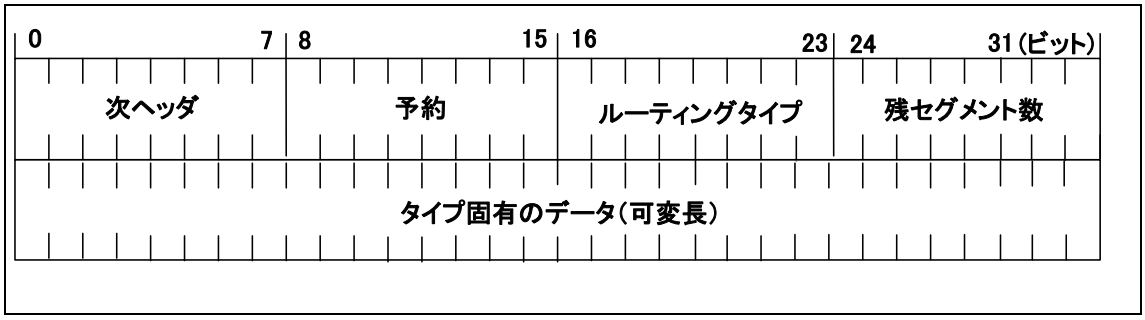


図 24-7 IPv6 ルーティングヘッダ

Type 0 ルーティングヘッダは、IPv4 の Loose Source Routing に相当する機能であり、宛先アドレスに到着すると特定の手順での経由地に向けてパケットを送付する処理が行われる。(注 2)ここでは後続ヘッダの処理への移行判断やパケットの整合性確認や条件に満たないパケットの破棄などが行われる。ここで、IPv4 の始点経路制御オプションが検査されない問題のように、この処理を含むルーティングヘッダの処理や実装等に問題があると、同様に不正にフィルタを通過されてしまうなどの影響を受ける可能性がある。IPv4 では既知の問題として対処されているため、現在においては IPv6 でも対策済みであると考えられるが定かではない。なお、IPv6 ノードにおいて Type 0 ルーティングヘッダの転送を無効にすることでこの問題の影響は受けない。

注 1: ルーティングタイプに 0 が指定されたルーティングヘッダ。ヘッダの形式と処理が RFC2460 で規定されており、現在はこの他タイプ 2(Mobile IPv6 の利用目的)が定義されている。

注 2: 詳細な手順および処理については RFC2460(セクション 4.4)を参照のこと

24)-6. 実装ガイド

1. フィルタリングの評価を行う際に、始点経路制御オプションの内容を考慮する。(注 3)
2. 始点経路制御オプションを伴うパケットを転送しない機能を用意する。(注 3)

24)-7. 運用ガイド

1. 始点経路制御オプション伴うパケットを転送しない設定にする。(注 3)

注 3: IPv6 の場合は、始点経路制御オプションの代わりに Type 0 ルーティングヘッダの処理への考慮が必要になる。

24)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月）のものである。

1981 年 RFC 791, Internet Protocol.
http://www.ietf.org/rfc/rfc0791.txt
RFC 793, TRANSMISSION CONTROL PROTOCOL.
http://www.ietf.org/rfc/rfc0793.txt

1998 年 RFC2460, Internet Protocol, Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2460.txt

1993 年 CERT Advisory CA-1993-07
http://www.cert.org/advisories/CA-1993-07.html

1995 年 ISS X-Force Database(514)
http://xforce.iss.net/xforce/xfdb/514
CERT Advisory CA-1995-01
http://www.cert.org/advisories/CA-1995-01.html
CERT Advisory CA-1996-21
http://www.cert.org/advisories/CA-1996-21.html

1999 年 Common Vulnerabilities and Exposures CVE-1999-0909
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0909
SecurityFocus 646:
http://www.securityfocus.com/bid/646/discuss
ISS X-Force Database(3251)
http://xforce.iss.net/xforce/xfdb/3251
マイクロソフト セキュリティ情報 MS99-038
http://www.microsoft.com/japan/technet/security/Bulletin/MS99-038.mspx

2002 年 SecurityFocus 4016
http://www.securityfocus.com/bid/4016
ISS X-Force Database(10108)
http://xforce.iss.net/xforce/xfdb/10108

2003 年 Symantec - Loose_Source_Route
http://service1.symantec.com/support/INTER/entsecurityjapanesekb.nsf/jp_docid/20031010150838949?OpenDocument&dtype=corp
Symantec - Strict_Source_Route
http://service1.symantec.com/support/INTER/entsecurityjapanesekb.nsf/jp_docid/20031010190205949?OpenDocument&dtype=corp
Unixcities.com - Source routing
http://www.unixcities.com/dos-attack/index.html
SecurityFocus 10707
http://www.securityfocus.com/bid/10170

SecurityFocus 10599
http://www.securityfocus.com/bid/10559
SecurityFocus 10551
http://www.securityfocus.com/bid/11551
Common Vulnerabilities and Exposures CVE-2004-2597
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2597
Common Vulnerabilities and Exposures CVE-2004-2598
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-2598

2007 年 Deprecation of Type 0 Routing Headers in IPv6
http://tools.ietf.org/id/draft-jabley-ipv6-rh0-is-evil-00.txt
IPv6 Type 0 Routing Header Processing
http://tools.ietf.org/id/draft-savola-ipv6-rtheader-00.txt

25).IP ヘッダオプションのデータ長が 0 のパケットの問題

25)-1.　分類：IP 【IPv4】【IPv6】

25)-2.　概要

IP ヘッダオプションのデータ長(オプション長)が 0 のパケットを処理することで、デバイスがフリーズしたりクラッシュしたりしてしまう問題がある。結果として攻撃者はデバイスに対するサービス不能状態を引き起こすことができる。

25)-3.　解説

攻撃手法とその影響

この問題は、IPv4 ヘッダのオプションフィールドを利用する。開発段階において十分にテストされていない製品が IP オプションのデータ長が 0 を示す特定のパケットを処理してしまうことで生じてしまう問題である。この問題の影響を受ける製品の多くは、処理エラーによりサービス不能状態に陥ってしまう。影響を受ける製品に応じてサービス不能状態の状況や再現方法が若干異なるが、図 25-1 において Linksys VPN Router の問題(CVE-2006-0309)を例にして攻撃の流れを示す。(注 1)

注 1: CVE-2006-0309 の場合、発見者の情報によるとローカルネットワーク内からインターネット上のホストに対して検証を実施したとの報告がある。

攻撃者は図 25-1 のようにホスト B から IP オプションを含む意図的に作成した不正パケットを問題のある標的のルータ A に対して送信する。あるいは別のホスト C に対して標的のデバイス A を介すように不正パケットを送信する。そして、送信された不正パケットをルータ A が受信することで、不正パケットを適切に処理することができず、デバイスはクラッシュしてしまう。同類の問題が存在する別の製品でも、システムの再起動や無限ループが発生し、応答が停止してしまうなど、サービス不能状態に陥ってしまい、正常な通信を妨害される可能性がある。

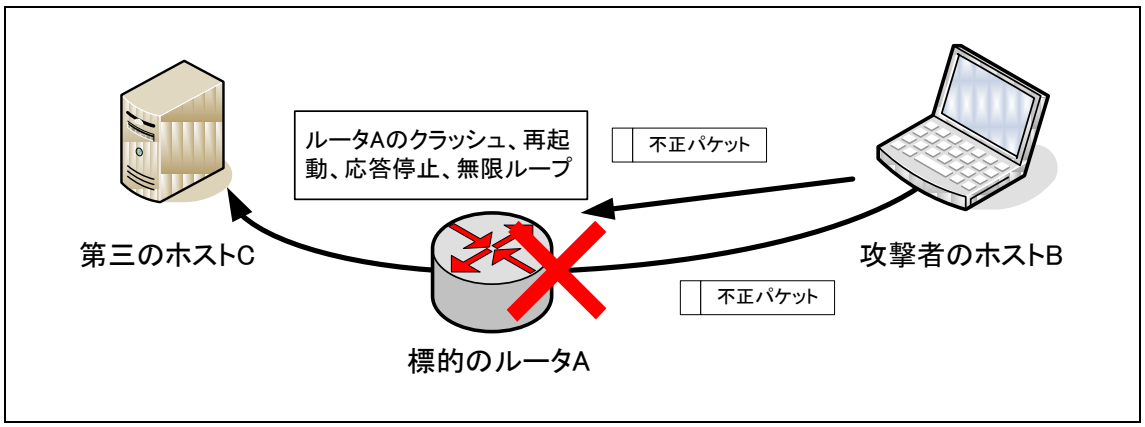


図 25-1 標的のルータ A での不正パケットの受信

ここで、この問題で利用される IP オプションを含む不正パケットについて解説する。以下図 25-2 に IP ヘッダの構造を示す。

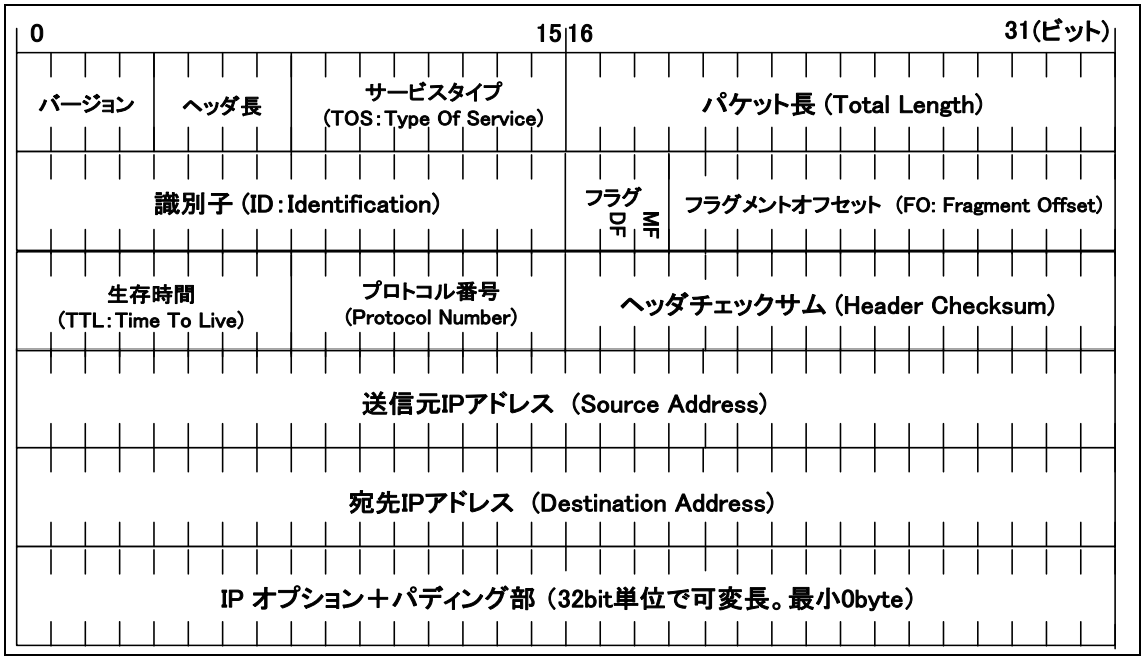


図 25-2 IP ヘッダ

IPv4 が定義されている RFC791 では、このように IP ヘッダのオプションフィールドは可変長であり、必ず含まれる情報ではないとしている。(IP オプションの複数指定は可能) またオプションフィールドは次のフィールド値であるパディングを含めて 32 ビット単位での指定が必要になる。

IP オプションで指定される形式は図 21-3 のように分割されている。先頭の 1 バイト目はオプションタイプで、オプションの種類などを表す。次の 1 バイトのオプション長には 1 つのオプション全体の長さを示す値が格納される。1 つのオプションを取り出して処理する際には、データサイズが可変長である点もありこの値が見られる。その次のオプションデータにはオプションによって様々な情報が格納される。

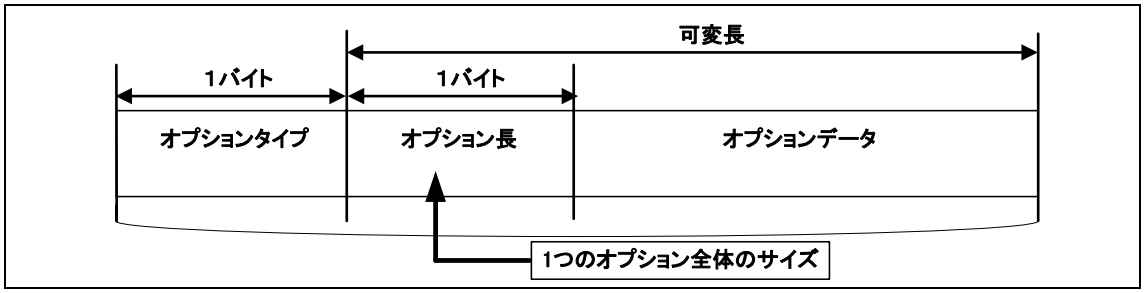


図 21-3 IP オプションの形式

さらに、オプションタイプの形式を図 25-4 に示す。図 21-3 の先頭の 1 バイト目にあるオプションタイプは図 21-4 のように左からコピーフラグ(1 ビット)、オプションクラス(2 ビット)、オプション番号(5 ビット)の 3 つで構成され、それぞれの値は表 25-1 から表 25-3 のように定義されている。

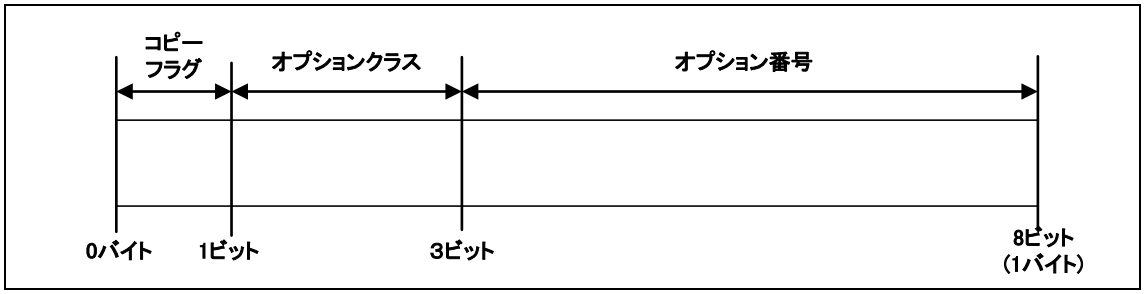


図 21-4 オプションタイプの形式

表 25-1 コピーフラグ

値(2 進数表記)	説明
0	コピーしない
1	コピーする

表 25-2 オプションクラス

値(2 進数表記)	説明
00	通常(制御用)
01	予約(注 2)
10	デバッグと計測用
11	予約(注 2)

注 2: 予約は将来の使用の為に確保されていたもので、現在は使用されていない。

なおオプション番号ではオプションの種類を指定するフィールドで 8 つが定義されている。オプションタイプは表 25-3 のように前の値であるコピーフラグとオプションクラスとの組み合わせで決められており、コピーフラグとオプションクラスはインターネットオプションのタイプ分けをする上でのオプション番号を補う情報としても考えることができる。

【IP ヘッダオプションのデータ長が 0 のパケットの問題】

表 25-3 オプション番号

コピー	クラス	オプション番号	タイプ(()内は 2 進数表記)	オプション長	説明
0	0	0	0(0 00 00000)	なし	End of Option list
0	0	1	1(0 00 00001)	なし	No Operation
1	0	2	130(1 00 00010)	11	Security
1	0	3	131(1 00 00011)	可変	Loose Source Routing
0	2	4	68(0 10 00100)	可変	Internet Timestamp
0	0	7	7(0 00 00111)	可変	Record Route
1	0	8	136(1 00 01000)	4	Stream ID
1	0	9	137(1 00 01001)	可変	Strict Source Routing

* 各インターネットオプションの詳細は RFC791 [Page 15]を参照のこと

* 表 21-3 の項目「タイプ」は、コピーフラグ、オプションクラス、オプション番号で構成されるオプションタイプをタイプ値として示したもの

上記の内容および発見者の情報(注 3)を参考にして今回問題となる不正パケットの内容を示すと図 25-5 のようになる。

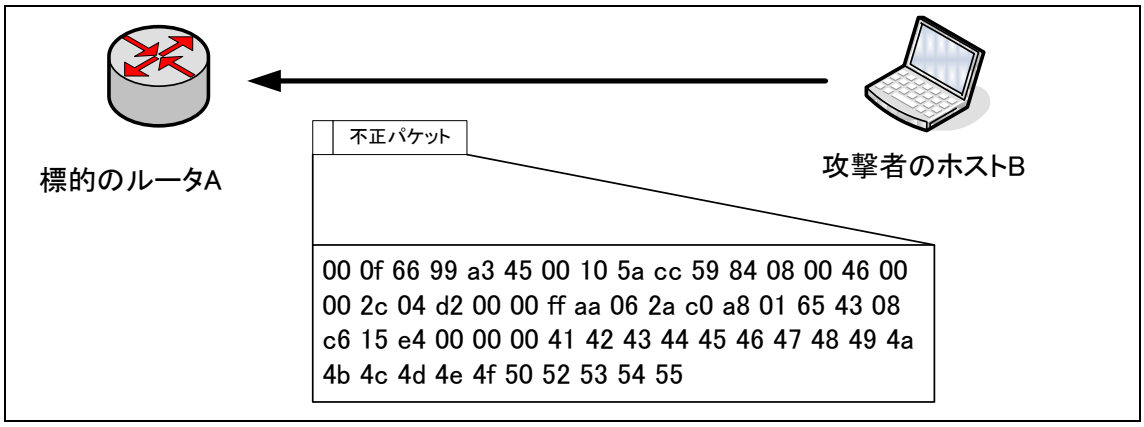


図 25-5 不正パケットの中身

注 3: http://www.securityfocus.com/archive/1/archive/1/421929/100/0/threaded

また、この不正パケットの内容を図 25-6 に示す。(注 4)内容を確認するとプライベートの IP アドレス 192.168.1.101(16 進数表記で c0 a8 01 65)の攻撃ホスト B からグローバル IP のルータ A に向けて不正パケットを送信していることがわかる。Ethernet ヘッダ、IP ヘッダ、IP データ部で構成されるこの不正パケットの IP データ部には、文字列(ABCDEFGHIJKLMNOPQRST)が含まれており、上位プロトコルが何かを示す 8 ビットで構成される IP ヘッダ中の⑨プロトコルには「aa」(10 進数表記で 170)が指定されている。

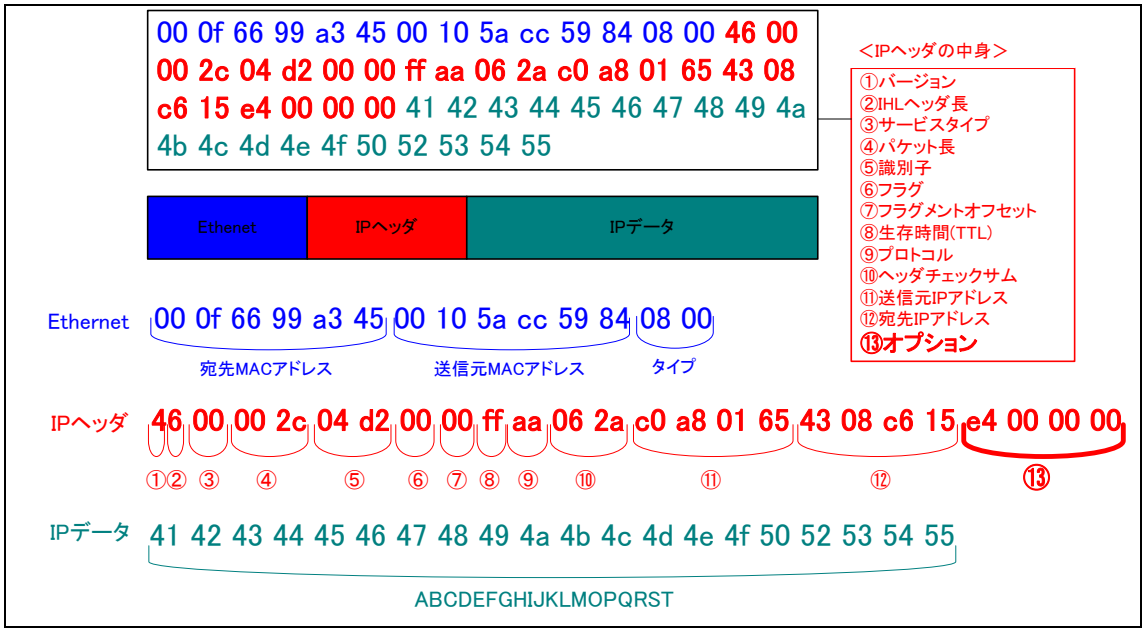


図 25-6 不正パケットの詳細

注 4: パケットの中身は 16 進数表記となっている。

さらに今回問題となっている ⑬オプション のフィールドを見ると、「e4 00 00 00 00」となっており、この部分を 2 進数で示すと図 25-7 のようになる。

16進数	e4	00	00	00
2進数	1110 0100	0000 0000	0000 0000	0000 0000

図 25-7 不正パケットの IP オプション部(16 進数と 2 進数表記)

この図を図 21-3 の IP オプションの形式と図 21-4 のオプションタイプの形式に当てはめてみると、先頭の e4 の部分がオプションタイプを示すことになり、コピーフラグが 1、オプションクラスが 11(10 進数で 3)、オプション番号に 00100(10 進数で 4)が指定され、それ以降が「00 00 00」のため、オプション長およびオプションデータにゼロ「0」が指定されていることになる。

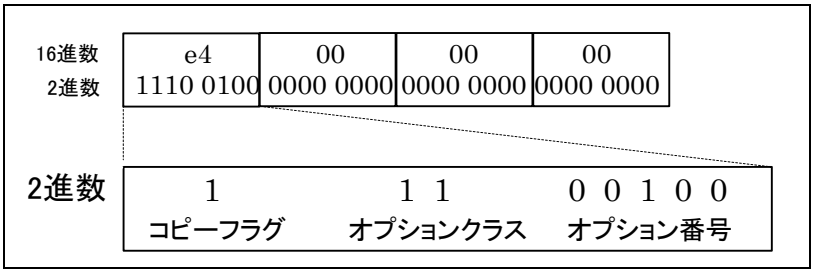


図 21-8 不正パケットのオプションタイプ

表 25-3 のオプション番号との組み合わせと比較してみても、このオプションタイプ 0xe4(2 進数表記で 11100100、10 進数表記だと 224)でオプションのデータ長がゼロの組み合わせは定義されておらず、RFC791 規格外のインターネットオプションが指定されていることになる。このような通常でないパケットを図 25-1 のように標的のルータ A に処理させることで、攻撃者はサービス不能状態を引き起こすことが可能となる。

今回の問題を引き起こす不正パケットは、その他の製品でも影響を受けることが既に確認されており、今回解説した不正パケットの処理により、幾つかの製品が影響を受ける可能性がある。(注 5)

注 5: 脆弱性スキャナ Nessus では、これら 2 つの問題に対しての検査項目(3com RAS 1500 DoS, pluginID:11475、URL; http://www.nessus.org/plugins/index.php?view=single&id=11475)が作成されている。

【IP ヘッダオプションのデータ長が 0 のパケットの問題】

原因と考察

この問題は、IP オプション処理部における製品設計上の不備に起因する問題であると考えられる。各ベンダからの詳細な情報が公開されていないため詳細は不明であるが、今回の調査から考えると、オプションタイプ 0xe4 に限らず、RFC で定義されていない IP オプションタイプ(定義済みの 8 つの IP オプション以外)の指定によって同じような影響を受ける可能性がある。そのため、”オプションタイプのデータ長が 0 に指定されたパケット”という、単にデータの長さを示すフィールドの処理部分に問題があるのではなく、オプションタイプ(コピーフラグ、オプションクラス、オプション番号)とデータ長 0 の組み合わせや各フィールドで示す種類、処理するデータフィールドが可変長であること、予約値や識別番号の存在など、単体のフィールドを処理するだけでも設計上考慮が必要なパターンが局部的に数多く存在しているという点が、今回のような問題を引き起こす大きな要因になっているのではないかと考えられる。このことから、設計→開発→テスト という開発プロセスにおいて考慮すべきパターンが増大することで作業が増大し、設計段階での不備やテストの欠落などにより、今回のような製品の品質に影響を及ぼす問題が作られやすくなってしまうのではないかと推察する。

なお、今回解説した Linksys VPN Router の問題(CVE-2006-0309)と同じ不正パケットを送信することで同様の影響を受けてしまう製品が他にも存在することが既に確認されている。また、IP オプションフィールドの処理部に限らず、例えば IP よりも上位プロトコルである TCP ヘッダ中のオプションフィールドの処理部などでも今回と類似する問題が幾つか報告されている。その他、オプションフィールド内に限らずとも、その他様々なヘッダフィールドにおいて通常ではあり得ない規格外の値や形式を含むパケットを適切に処理できずにサービス不能状態に陥ってしまう問題は数多く存在する。

つまり、このような TCP/IP パケットにおける特定のフィールド値とその組み合わせや無効な形式によってサービス不能状態に陥る問題は、IP ヘッダのオプションフィールドに限った問題ではない。開発者は、単体のフィールド処理を設計するだけでも、処理部分によっては破棄や各フィールドとの関連性など、様々な視点を持ち品質面への影響を十分考慮した上でパケット処理や TCP/IP スタック全体の設計を行うことが求められる。

表 25-4 に今回例に挙げた CVE-2006-0309 の問題に類似し、同じような設計上の不備によって DoS 攻撃が成立すると考えられる問題の一部を示す。これらの問題についても送信元で指定可能な要素は IP オプションフィールドと同様に多いため、処理側では考慮しなければならないパターンが比較的多い部分で頻繁に発生している。

【IP ヘッダオプションのデータ長が 0 のパケットの問題】

表 25-4 CVE-2006-0309 に類似する DoS 問題(一部)

製品名	説明
Axent Raptor 6.0	IP オプションのデータ長が 0 の不正パケットにより DoS となる。 http://www.securityfocus.com/bid/736
rp-pppoe PPPoE	TCP オプションのデータ長が 0 の不正パケットにより DoS となる。 http://nvd.nist.gov/nvd.cfm?cvename=CVE-1999-0193
Ascend/3com ルータ製品	TCP オプションのデータ長が 0 の不正パケットにより DoS(再起動)となる。 http://nvd.nist.gov/nvd.cfm?cvename=CVE-2000-0580
Norton Internet Security, Norton Personal Firewall 2003/2004	SACK オプションなど、幾つかのオプションのデータ長が 0 の TCP パケットにより、DoS となる。 http://nvd.nist.gov/nvd.cfm?cvename=CVE-2004-0375
Kerio Personal Firewall 4.1.1 以前	IP オプションのデータ長が 0 の不正パケットにより DoS となる。CVE-2006-0309 と同じ不正パケットを利用。 http://nvd.nist.gov/nvd.cfm?cvename=CVE-2004-1109
3Com SuperStack II RAS 1500	IP オプションのデータ長が 0 の不正パケットにより DoS となる。CVE-2006-0309 と同じ不正パケットを利用。 http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-2577
Wyse Winterm 1125SE	IP オプションフィールドのデータ長が 0 の不正パケットにより DoS となる。CVE-2006-0309 と同じ不正パケットを利用。 http://www.securityfocus.com/bid/14536
TIBCO Rendezvous 7.5.2 – 7.5.4	データ長フィールドに 0 が指定された特定のパケットにより DoS となる。 http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-4158
3Com IntelliJack Switch NJ220 2.0.23 未満	データ長フィールドに 0 が指定されたループバックパケットにより DoS となる。 http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-3533

25)-4. 発見の経緯とトピック、対策の動き、現在の動向

インターネット上で調査した限りでは、最も古く発見された IP オプションのデータ長 0 に関連する問題は、1999 年に公開された Axent Raptor 6.0 の問題である。この問題を利用する Exploit コードについても併せて公開されている。以後、類似する問題が他のルータ製品でも報告されたり、脆弱性スキャナ Nessus にこの問題の検査項目が追加されたりしており、設計上の不備に起因する問題としては代表的な問題の 1 つである。

TCP/IP スタックを実装し IP オプションの処理が必要な製品を開発する上では、このような問題は現在でも注意しなければならない点であるが、過去と比べ、技術的な進歩と開発者の意識のもとで製品の設計開発における品質の改善が進んでおり、このような設計上の不備の問題は徐々に減りつつあると考えられるが、近年では類似した問題の報告が少ないのが事実であり、実際にこのような問題の対策が進んでいるかどうかの詳細は不明である。

25)-5. IPv6 環境における影響

IPv4 ではヘッダは 20 オクテットから 60 オクテットの可変長であったが、IPv6 は 40 オクテットの固定長のヘッダとなり、IP のオプションデータは拡張ヘッダにまとめられてペイロードの先頭に配置される形式となっている。

IPv6 の拡張ヘッダの種類は表 21-5 に示す種類があり、複数ヘッダが存在する場合は IPv6 ヘッダの後に拡張ヘッダの部分につなぎ合わせて配置される。それぞれのヘッダの形式は図 21-9 のルーティングヘッダの形式の例にあるように、各拡張ヘッダには表 21-5 のプロトコル番号を示す次ヘッダやヘッダ全体の長さを示すヘッダ長、さらにルーティングタイプのように各拡張ヘッダの中でもさらにタイプ分けされる場合はそれを示すフィールドなどが用意されている。また、拡張ヘッダは 8 オクテットの倍数の長さである必要があり、8 オクテットに満たない場合のために IPv4 と同様に Pad オプションが用意されている。

表 25-5 IPv6 拡張ヘッダの種類

名前	プロトコル番号 (タイプ値)	概要
ホップバイホップオプションヘッダ	0	途中のノードで利用される情報が含まれる。
ルーティングヘッダ	43	経由するノードを指定する。
フラグメントヘッダ	44	フラグメントの情報が含まれる。
認証ヘッダ(AH)	50	IPSec の AH が含まれる。
ESP ヘッダ	51	IPSec の ESP が含まれる。
終点オプションヘッダ	60	最終の宛先で利用される情報が含まれる。
Mobile IPv6 用ヘッダ	135	Mobile IPv6 で利用される情報が含まれる。

図 21-9(参考)ルーティングヘッダの形式

このように IPv6 では IPv4 と比べ、拡張ヘッダの出現に伴いヘッダ構造の違いや利用用途の拡張が見受けられるが、IP のオプションを示す部分は存在し、さらにタイプやヘッダ長などを示すフィールドも存在する。

そのため、IPv4 と同様に IPv6 でも IP のオプションが示される拡張ヘッダの取り扱いには十分な配慮が必要となり、IPv6 の場合には拡張ヘッダの種類(次ヘッダ値)やヘッダ長の取り扱い、また場合によってはヘッダが可変長であることやヘッダの配置順と処理順の関係など、それぞれの拡張ヘッダの処理条件については IPv4 と同じような設計段階での注意が必要であり、IPv6 でも拡張ヘッダの取り扱いには十分に注意しなければ類似の問題が発生してしまうことが考えられる。さらに IPv6 の拡張ヘッダによりオプション部で表現される機能が増えたために、IPv6 は IPv4 よりも注意すべき箇所が増えていると推測され、開発側はより厳密な注意が必要であると考えられる。

25)-6. 実装ガイド

1. IP オプション(IPv6 の場合は拡張ヘッダ)の取り扱いにおいて、例えば以下の項目について妥当性の確認を怠らず、仕様上問題はないものの、通常では処理の対象になり得ないような場合でも製品の設計開発の段階で条件定義を行う。そして、不適切なものは適切に破棄されるようにするなどの処置を検討する。
    - オプションの識別値やデータ長などの各フィールド自身の値や内容のチェック
    - 各ヘッダやフィールド間の関係や組み合わせに対するチェック
    - 各フィールドで示されるデータ長の値と実データサイズとの関係のチェック(例えばオプション長で示される値と実際のオプションフィールドのサイズとの関係)

2. RFC などの規格外のパケットは処理せずに破棄するようなアルゴリズムを実装する。

25)-7. 運用ガイド

3. 影響を受ける製品に対して各ベンダより提供されているパッチの適用や問題が修正されたファームウェアにバージョンアップする。

4. IP オプションで提供される機能が不要、あるいは無効にしても良い場合、ファイアウォールを含むルーティングデバイスや IDS/IPS 等で IP オプションを含むパケットを破棄する。

5. ファイアウォールを含むルーティングデバイス等の機能において、流れる IP オプションを含むパケットが特定の時間内に一定のパケット量に達した場合に、そのパケットを破棄できるような機能を利用する。

25)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2008 年 8 月)のものである。

1995 年 IETF RFC1812: Requirements for IP Version 4 Routers
http://www.ietf.org/rfc/rfc1812.txt

1998 年 IETF RFC791: Internet Protocol
http://www.ietf.org/rfc/rfc791.txt

IETF RFC2460: Internet Protocol, Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2460.txt

IETF RFC2463: Internet Control Message Protocol(ICMPv6) for the Internet Protocol Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2463.txt

1999 年 SecurityFocus 736
http://www.securityfocus.com/bid/736

Common Vulnerabilities and Exposures CVE-1999-0905
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0905

2003 年 3com RAS 1500 Remote vulnerabilities【Piotr Chytla 著】
http://www.securityfocus.com/archive/1/316043

SecurityFocus 7175
http://www.securityfocus.com/bid/7175

Nessus Plugin ID 11475
http://www.nessus.org/plugins/index.php?view=single&id=11475

2004 年 KERIO Security Advisories KSEC-2004-11-04-01
http://www.kerio.com/security_advisory.html#0411

Kerio Personal Firewall Multiple IP Options Denial of Service
http://research.eeye.com/html/advisories/published/AD20041109.html

SecurityFocus 11639
http://www.securityfocus.com/bid/11639

Common Vulnerabilities and Exposures CVE-2004-1109(KERIO)
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1109

2005 年 Remote DOS on Wyse thin client 1125SE 【Josh Zlatin-Amishav 著】
http://www.securityfocus.com/archive/1/407903
SecurityFocus 14536
http://www.securityfocus.com/bid/14536
Common Vulnerabilities and Exposures CVE-2005-2577
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2577

2006 年 Linksys VPN Router(BEFVP41) DoS Vulnerability 【paul14075@gmail.com 著】
http://www.securityfocus.com/archive/1/archive/1/421929/100/0/threaded
SecurityFocus 16307
http://www.securityfocus.com/bid/16307
Common Vulnerabilities and Exposures CVE-2006-0309
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-0309

【IP ヘッダオプションのデータ長が 0 のパケットの問題】

2007 年　Cisco Security Advisory: Crafted IP Option Vulnerability
http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/cisco-sa-20070124-crafted-ip-option-j.shtml
http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml

参考　　マスタリング TCP/IP　入門編　第 1 版　p.158-162
マスタリング TCP/IP　IPv6 編　第 1 版　p.49-99

26).IP 経路制御機能(ソース・ルーティング機能)により、サービス不能状態に陥る問題

26)-1. 分類:IP 【IPv4】【IPv6】

26)-2. 概要

IP プロトコル仕様における経路制御機能(以下、ソース・ルーティング機能とする。パケットの通過経路を送信者が指定する方式を指す。IPv4 の場合ソース・ルーティング オプション、IPv6 の場合は Type 0 ルーティングヘッダに相当)のセキュリティ上の欠陥により、特定の経路情報を含む IP パケットを処理することでネットワーク帯域が枯渇して通信遅延が発生する、あるいはパケットを処理するデバイスのクラッシュにより通信が停止してしまう問題がある。結果として攻撃者はネットワークやデバイスに対するサービス不能状態を引き起こすことができる。

26)-3. 解説

攻撃手法とその影響

> 本項では、特に問題視されている IPv6 プロトコルにおける問題(IPv6 Type 0 ルーティングヘッダの問題)をメインに取り上げて解説を行う。IPv4 プロトコルに関しては、後述の 22)-5 において解説している。

IPv6 プロトコルにおいて、ソース・ルーティング機能はルーティングヘッダ(次ヘッダ値:43) として扱われる部分である。IPv6 のルーティングヘッダは拡張ヘッダの１つとして RFC2460 に規定されている。図 26-1 にルーティングヘッダの形式を示す。

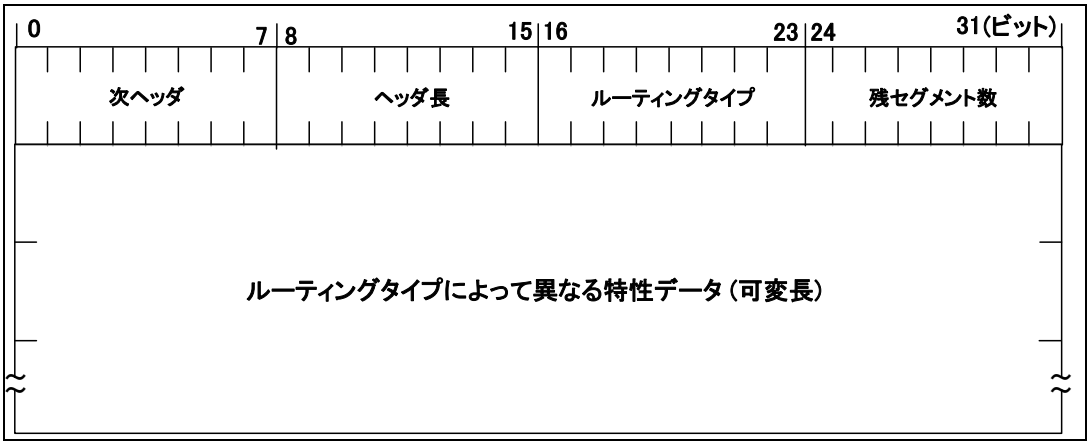


図 26-1 IPv6 におけるルーティングヘッダの形式

図 22-1 に示されるルーティングタイプは調査時点(2008 年 8 月)においてタイプ「0」とタイプ「2」の 2 種類が定義されている。(注 1) タイプ「2」は Mobile IPv6 で利用するために後から定義されたタイプである。今回問題となるタイプ「0」はパケットの配送経路を指定するために利用され、特性データには経由する宛先アドレス一覧が含まれる。ルーティングタイプが 0 に指定されたルーティングヘッダ(以下、RH0 とする)の形式を図 26-2 に示す。

注 1:ルーティングタイプが 0 の場合、このリストと宛先アドレスにはマルチキャストアドレスを指定することはできない。

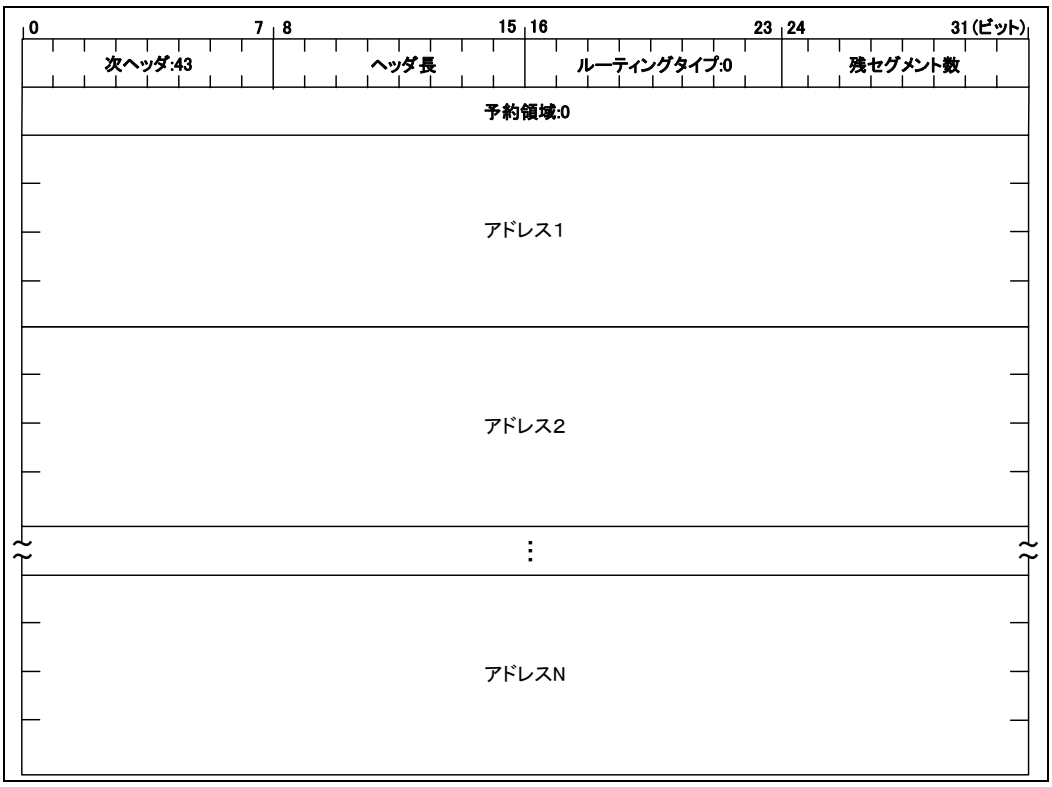


図 26-2 ルーティングタイプが 0 に指定されたルーティングヘッダ(RH0)の形式

ルーティングタイプが 0 の場合、可変長のデータ部の先頭 32 ビットは予約領域でゼロ「0」が含まれ、次に続くアドレス 1～N に経由する順番にノードのアドレスのリストが指定される。(注 1)宛先アドレスにパケットが到着するとルーティングヘッダの内容を調べ、IPv6 ヘッダに指定される宛先アドレスを変更する処理が行われる。

次にルーティングヘッダの処理について示す。図 26-3 は送信元アドレス A のホストから宛先アドレス B のホストに向けたパケット配送が行われ、経路がノード R1、R2、R3 の順で指定されているときの様子を示している。

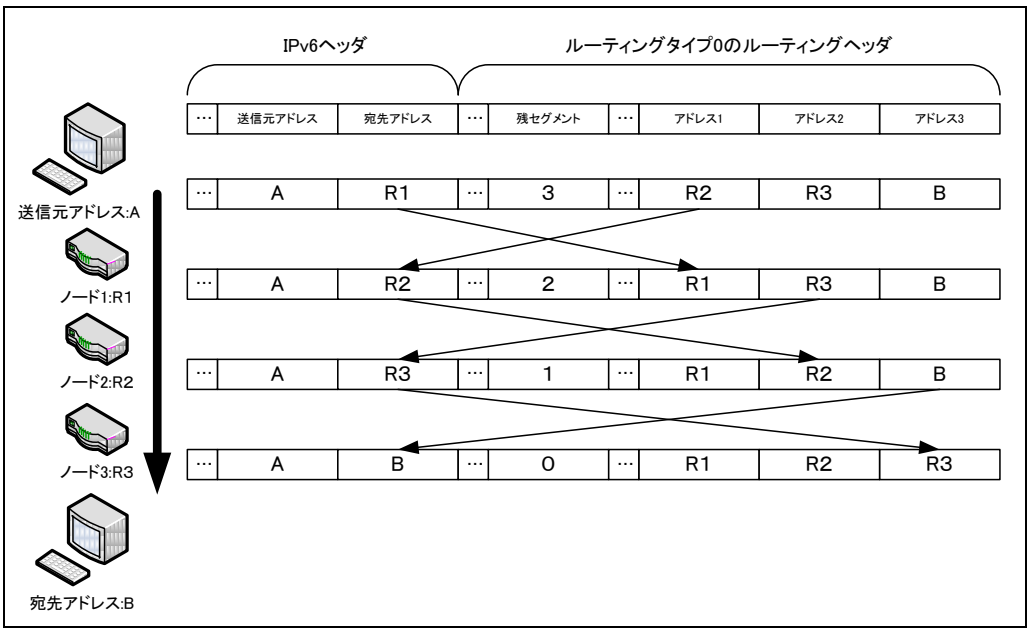


図 26-3 ルーティングヘッダの処理

RFC2460 ではこの RH0 に対するセキュリティの配慮が十分に行われていないため、RFC2460 に準拠するホストやルータ製品が RH0 を処理することで、ネットワーク帯域枯渇やデバイスのクラッシュにより通信の遅延や停止を引き起こす可能性がある。

RH0 を利用した不正パケットの流れは以下の図 26-4 のようになる。ここで示される攻撃の流れ①～④について解説する。

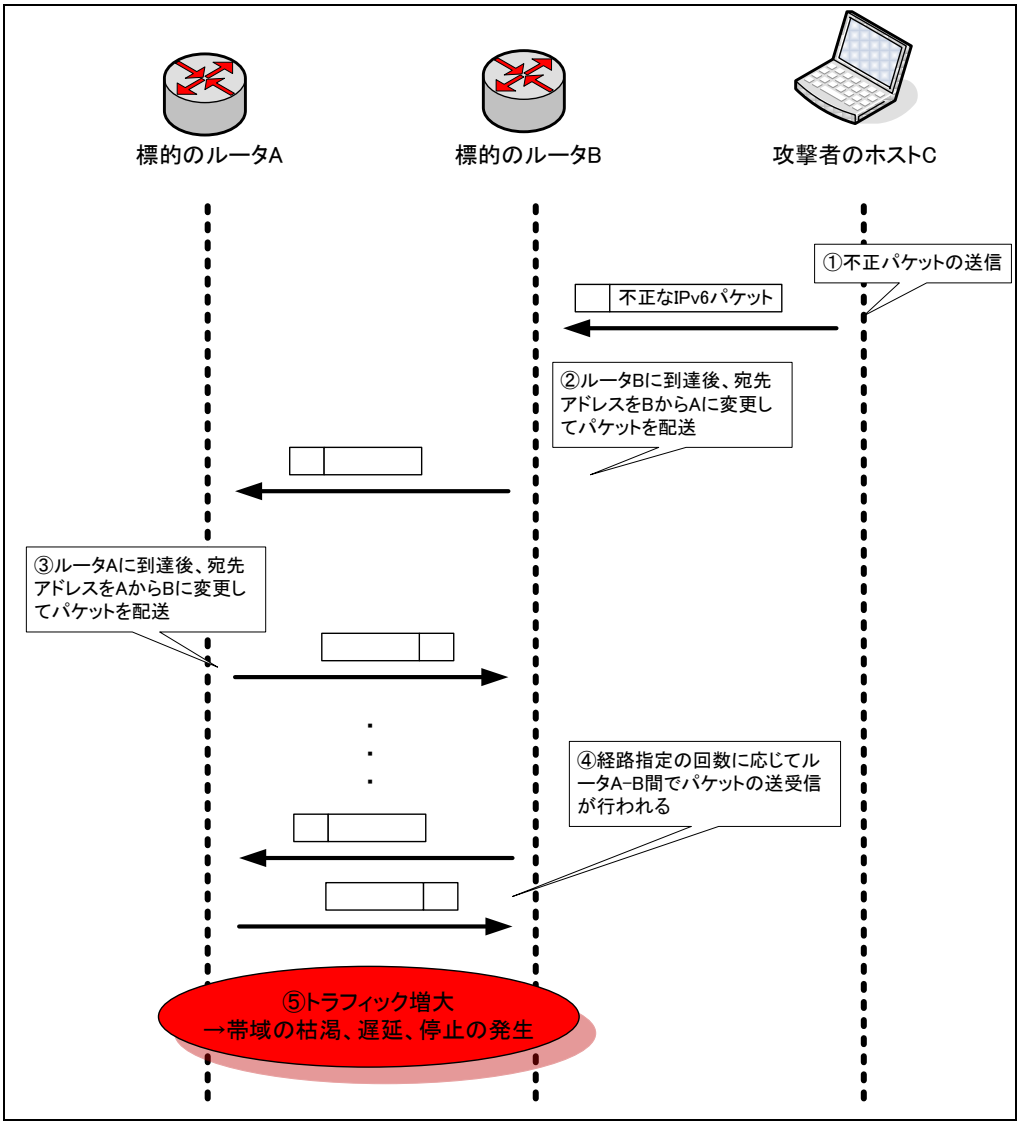


図 26-4 RH0 を含む不正な IPv6 パケットの流れ

＜図 26-4 での不正パケットの遷移＞

① まず、攻撃者は標的とするこの問題に脆弱な同一リンク上に存在する標的のルータ B と標的のルータ C の IPv6 アドレスを特定し、ホスト C の攻撃者は図 26-5 のようにルータ A とルータ B 間で繰り返し経路指定が行われた RH0 を含む不正な IPv6 パケットを標的のルータ B に送信する。

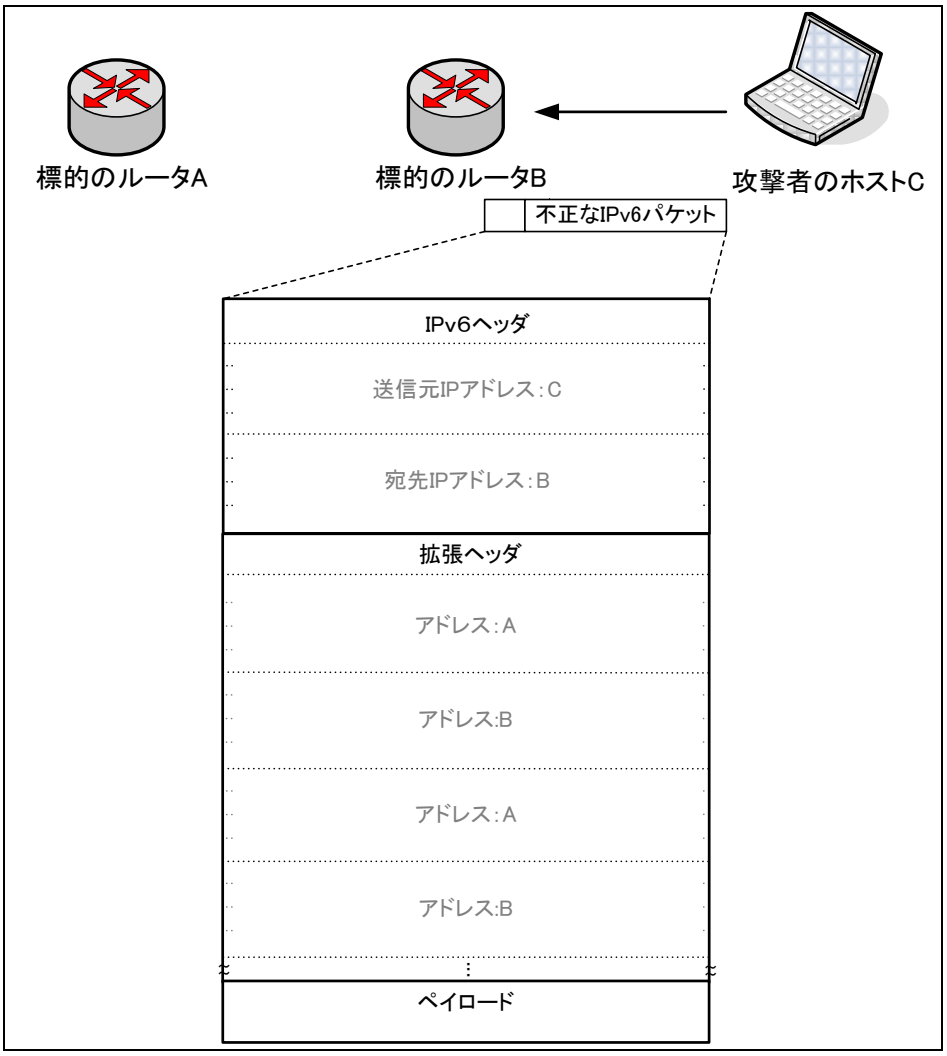


図 26-5 RH0 を含む不正な IPv6 パケットの構成

② ルータ B に到達した不正な IPv6 パケットは RH0 で経路指定されたとおりルーティングヘッダの処理に準じて、経路上次の配送先に指定されたルータAのアドレスを宛先アドレスに変更してパケットを配送する。この際、RFC2460 では RH0 中に指定可能な IPv6 アドレス数の制限や自分のアドレスが後方に存在するかなどのチェックなど、セキュリティ上十分な制約について定義されておらず、単体の IPv6 パケットだけで RFC2460 に準拠して RH0 を処理する脆弱なルータ A とルータ B の間で繰り返しパケットを配送する指定が可能になってしまう。

③ ルータAに到達したパケットは先ほどの②と同じように、RH0 で次に経路指定されているルータ B のアドレスを宛先アドレスとし、パケットを送り返す形でルータ B にパケットを配送する。

④ 以降、RH0 でルータ A とルータ B のアドレスの指定回数に応じてルータ A-B 間でパケット送受信の繰り返しが続けられる。結果として、攻撃者はルータ A-B 間でループ状態を作り出すことができる。

⑤ 攻撃者は①～④を繰り返す RH0 を含む IPv6 パケットを何度も何度も送信することで、ルータ B とルータ C 間のトラフィックを増大させることができる。これにより、ネットワーク帯域が枯渇してしまい、他の通信が妨害されてしまう可能性がある。あるいは、ルータ上での処理過程やネットワーク構成、トラフィック量等によっては標的のルータ自体がクラッシュし、通信が停止してしまう可能性がある。

原因と考察

この問題の原因は、RFC2460 に規定されている IPv6 プロトコルの仕様にある。ルーティングヘッダの取り扱いに関して RFC2460 に準拠する製品はリストに指定可能なアドレスの数に制限がなかったりリストに含まれるアドレスチェックを行わなかったりするため、ループ状態を作り出すように意図的に作成された RH0 を含む IPv6 パケットを破棄せずにそのまま処理してしまうのが原因である。

この問題を成立させるためには、攻撃者は同一リンク上にある脆弱なホストやルータの IPv6 アドレスを把握する必要がある。広く知られており、重要かつ高速なネットワーク回線に接続されている IPv6 ノードは、特に標的になる可能性が高いと考えられている。

また Cisco Systems の情報によると、TCP、ICMP、UDP 等のパケットタイプには依存しないため、偽装されたパケットによって攻撃を受ける可能性があると報告されている。

26)-4.　発見の経緯とトピック、対策の動き、現在の動向

RH0 の問題は 2007 年 4 月にカナダで開催されたセキュリティカンファレンス CanSecWest 2007 で EADS の Arnaud Ebalard 氏と Philippe Biondi 氏が発表した "Fun with IPv6 routing headers"(資料タイトル「IPv6 Routing Header Security」)(注 1)で公表された。この発表では RH0 を利用した以下 4 タイプの攻撃手法が発表されており、この中の DoS を引き起こす問題 3.-1) として発表された問題が RH0 の代表的な問題として知られている。

1.Advanced Network Discovery
RH0 によって提供される経路指定を強要することで、通常では選択されない経路のネットワーク探索に使うことができる問題

2. Bypassing filtering devices
RH0 を使用してファイアウォール等で施されている IPv6 フィルタリングルールを回避する問題

3. DoS
1) RH0 を使用して2つの中継ノード間でルーティングループを引き起こし、ネットワーク帯域を枯渇させる問題 2) 1)での通信遅延により、増幅された TCP SYN パケットが送出される問題

4. Defeating Anycast
RH0 を使用して特定のエニーキャストアドレスの全インスタンスを識別可能なため、エニーキャストの効力を無効にすることができる問題。発表ではエニーキャストアドレスのルート DNS に対する脅威

なお Cisco Systems から「IPv6 Routing Header Vulnerability」というアドバイザリが公開されているが、CanSecWest 2007 での発表で RH0 の問題との関連性が公表されている。CanSecWest 2007 での発表以降、Cisco Systems 以外でも OS やルータ製品を取り扱うベンダが続けてセキュリティアップデートを発表しており、現時点では影響範囲が広範囲に及んでいる。(注 2)

注 1: http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf

注 2: 影響を受ける製品を取り扱うベンダの多くは、公表する問題箇所は上記 3.-1)の問題のみに言及している。それ以外の問題に関する情報については詳細不明である

多くのベンダで採用されたこの問題対策のほとんどが以下の対策である。この対策は 2007 年 5 月に RH0 の問題の対策として公開された 2 つのドラフト版として公開されたものである。

1. draft-jabley-ipv6-rh0-is-evil-00(注 3):
    - RH0 を含む IPv6 データグラムは転送しないようにする

2. draft-savola-ipv6-rtheader-00(注 4):
    - IPv6 仕様においてデフォルトでは RH0 を無効にする
    - IPv6 仕様においてデフォルトでは RH0 を無効にし、IPv6 仕様のオプション部分として取り扱うようにする
    - IPv6 仕様において RH0 の実装を削除する

注 3: http://tools.ietf.org/id/draft-jabley-ipv6-rh0-is-evil-00.txt

注 4: http://tools.ietf.org/draft/draft-savola-ipv6-rtheader/draft-savola-ipv6-rtheader-00.txt

その後、2007 年 12 月には IPv6 において RH0 を実装しないとする RFC5095 が制定された。これにより、基本としては IPv6 仕様において RH0 を実装しないように変更が行われている。また RFC5095 では RH0 の実装を無効にするまでの間の問題の緩和策として、RFC2827 と RFC3704 で推奨されているフィルタリングを実施する事が示されている。

また、Type 0 のルーティングヘッダの取り扱いを多くの製品で無効にする中で、幾つかのベンダでは RH0 の機能は有効のままとし、特定の条件を満たす場合のみにパケットを破棄するような対策なども考えられている。

26)-5. IPv4 環境における影響

IPv6 の RH0 は、IPv6 からの機能であるため、IPv4 には RH0 の問題は存在しない。しかし、IPv4 には RH0 で提供される機能に相当するソース・ルーティング機能が存在する。双方とも送信者が経路を指定する際に利用される機能である。

IPv6 の RH0 については今回の RH0 の問題が発表される以前から潜在的なセキュリティ問題として不安視されていた面があったが、この IPv4 のソース・ルーティング機能についてもセキュリティ上不安視されていたのは同様で、ソース・ルーティング機能における既に報告済みの問題「20. IP 経路制御オプションが検査されていない問題(IP Source Routing 攻撃)」が発見されているなど、IPv4 のソース・ルーティング機能でも十分なセキュリティの配慮が必要な機能であるといえる。

本項の問題についても概念的には IPv4 でもこの問題は再現すると考えられるが、IPv4 のソース・ルーティング機能は IPv6 の RH0 に比べて中間ノードのアドレスを指定できる数が少なく、危険性も IPv4 の方が低いと考えられている。さらに IPv4 においては IP Source Routing 攻撃の対策が有効と考えられるが、調査時点(2008 年 8 月)では既に IP Source Routing 攻撃の対策が有効な状態で運用されている機器が多いと考えられ、現状 IPv4 においては多くの環境下において現実的に有効な攻撃にはならないと推察する。

なお Cisco Systems の情報によると、IPv6 プロトコルを IPv4 にトンネリングさせるようなネットワーク環境下の場合で、脱カプセル化（Decapsulation）後の宛先アドレスに IPv6 アドレスが利用されるような場合は、RH0 の問題として影響を受ける可能性があるとしている。その他、IPv6 環境にて使用される Type 2 ルーティングヘッダは影響を受けないことが報告されている。

26)-6. 実装ガイド

1. RFC5095 に示されるように RH0の実装を無効とし、以下のようなパケットは処理せずに破棄する。(注 5)
    - Type 0 のルーティングヘッダを持つ IPv6 パケット
    - Type 0 のルーティングヘッダの中で自身(問題のあるデバイス)のアドレスがセットされている IPv6 パケット
    - IPv6 通信が不要な場合、IPv6 パケットの全て

2. RH0 の実装は有効とするものの、パケット処理において以下のような制限を設ける。制限を超えた場合は対象のパケットを破棄し、攻撃を受けた場合でもある一定以上の影響(例えば帯域の消費など)を受けないようにする。
    - 自身のアドレスがセットされている Type 0 のルーティングヘッダを持つ IPv6 パケットで、RH0 の中で指定されているアドレス数に制限を設ける
    - Type 0 のルーティングヘッダを持つ IPv6 パケットの処理数に制限をかける

3. Type 0 のルーティングヘッダの処理をデフォルトで無効とし、ユーザ自身が必要に応じて利用できるように機能を実装する。

注 5: パケット破棄の処理の際、破棄に加えてエラー応答(例えば ICMPv6 を利用した Parameter Problem のエラー応答)を送信するような実装も考えられている。

26)-7. 運用ガイド

1. 影響を受ける製品に対して各ベンダより提供されているパッチの適用や問題が修正されたファームウェアにバージョンアップする。

2. ファイアウォール等のフィルタリング機器を使用してデバイスの手前で以下のようなパケットを破棄する。
   - Type 0 のルーティングヘッダを持つ IPv6 パケット
   - Type 0 のルーティングヘッダの中でデバイス自身のアドレスがセットされている IPv6 パケット
   - IPv6 通信が不要な場合、IPv6 パケットの全て

26)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2008 年 8 月)のものである。

1998 年 IETF RFC2460: Internet Protocol, Version 6(IPv6) Specification
http://www.ietf.org/rfc/rfc2460.txt
Security of IPv6 Routing Header and Home Address Options
http://tools.ietf.org/html/draft-savola-ipv6-rh-ha-security-00.txt

2000 年 IETF RFC2827: Network Ingress Filtering
http://www.ietf.org/rfc/rfc2827.txt

2004 年 IETF RFC3704: Ingress Filtering for Multihomed Networks
http://www.ietf.org/rfc/rfc3704.txt

2006 年 IETF RFC4294: IPv6 Node Requirements
http://ietf.org/rfc/rfc4294.txt

2007 年 Cisco Security Advisory: IPv6 Routing Header Vulnerability
http://www.cisco.com/warp/public/707/cisco-sa-20070124-IOS-IPv6.shtml
http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/cisco-sa-20070124-IOS-IPv6-j.shtml
US-CERT Vulnerability Note: VU#274760
http://www.kb.cert.org/vuls/id/274760

SecurityFocus 22210
http://www.securityfocus.com/bid/22210
Common Vulnerabilities and Exposures CVE-2007-0481
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0481
JP Vendor Status Notes　JVNTA07-024A
http://jvn.jp/cert/JVNTA07-024A/
JP Vendor Status Notes　JVNVU#274760
http://jvn.jp//cert/JVNVU274760/index.html
JPCERT/CC Alert　JPCERT-AT-2007-0002
http://www.jpcert.or.jp/at/2007/at070002.txt
OPENBSD SECURITY FIX: April 23, 2007
http://openbsd.org/errata39.html#022_route6
http://openbsd.org/errata40.html#012_route6
SecurityFocus 23615
http://www.securityfocus.com/bid/23615
ISS X-Force Database openbsd-ipv6-type0-dos(33851)
http://xforce.iss.net/xforce/xfdb/33851
US-CERT Vulnerability Note VU#267289
http://www.kb.cert.org/vuls/id/267289
IPv6 Routing Header Security.(Philippe BIONDI and Arnaud EBALARD　著)
http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf
Common Vulnerabilities and Exposures CVE-2007-2242
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2242
Linux Kernel ChangeLog 2.6.20.9
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.20.9
Linux Kernel ChangeLog 2.6.21
http://www.kernel.org/pub/linux/kernel/v2.6/ChangeLog-2.6.21
FreeBSD-SA-07:03
http://security.freebsd.org/advisories/FreeBSD-SA-07:03.ipv6.asc
KAME project's action on Type 0 Routing Header issue
http://www.kame.net/newsletter/20070502/index.ja.html
Deprecation of Type 0 Routing Headers in IPv6 draft-jabley-ipv6-rh0-is-evil-00
http://tools.ietf.org/id/draft-jabley-ipv6-rh0-is-evil-00.txt

IPv6 Type 0 Routing Header Processing draft-savola-ipv6-rtheader-00.txt
http://tools.ietf.org/draft/draft-savola-ipv6-rtheader/draft-savola-ipv6-rtheader-00.txt
RHSA-2007:0347-2 kernel security and bug fix update
https://rhn.redhat.com/errata/RHSA-2007-0347.html
sun security community SECURITY BLOG 16 May 2007　IPv6 Routing Header Issues
http://blogs.sun.com/security/entry/ipv6_routing_header_issues
draft-ietf-ipv6-deprecate-rh0-01-candidate-00(Joe Abley 著)
http://www.ietf.org/mail-archive/web/ipv6/current/msg07313.html
http://www.ietf.org/mail-archive/web/ipv6/current/msg07499.html
JVNDB-2007-000387 IPv6 Type0 ルーティングヘッダの問題
http://jvndb.jvn.jp/contents/ja/2007/JVNDB-2007-000387.html
JVNVU#267289 IPv6 Type0 ルーティングヘッダの問題
http://jvn.jp//cert/JVNVU267289/index.html
【AX-VU2007-01】「IPv6 Routing Header Type 0 の問題」に関するご報告
http://www.alaxala.com/jp/support/security/20070628.html
About the security content of AirPort Extreme Base Station with 802.11n Firmware 7.2.1
http://docs.info.apple.com/article.html?artnum=306375
IPv6 Type0 ルーティングヘッダの問題
http://software.fujitsu.com/jp/security/vulnerabilities/vu267289.html
Release Note -- SEIL/neu 2FE Plus version 1.81-162(Fillin5)
SEIL シリーズ セキュリティ&脆弱性情報 : [影響:あり] IPv6 プロトコル仕様の脆弱性
http://www.seil.jp/download/seilseries/doc/plus_relnote_v181.txt
http://www.seil.jp/seilseries/news/snote/snote_200705_01.html
FITELnet : IPv6 プロトコルの Type 0 ルーティングヘッダに関する脆弱性について
http://www.furukawa.co.jp/fitelnet/topic/vulnera_20070614.html
ヤマハ RT シリーズのセキュリティに関する FAQ ： タイプ 0 のルーティングヘッダが付いた IPv6 が DoS 攻撃に使われる可能性のある脆弱性について
http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/VU267289.html
NEC 製品セキュリティ情報 : NV07-001
http://www.nec.co.jp/security-info/secinfo/nv07-001.html
BUGTRAQ:20070615 rPSA-2007-0124-1 kernel xen
http://www.securityfocus.com/archive/1/471457

USN-486-1: Linux kernel vulnerabilities
http://www.ubuntu.com/usn/usn-486-1
About the security content of the Mac OS X 10.4.10 Update CVE-2007-2242
http://docs.info.apple.com/article.html?artnum=305712
MANDRIVA:MDKSA-2007:171
http://www.mandriva.com/security/advisories?name=MDKSA-2007:171
SUSE:SUSE-SA:2007:051
http://www.novell.com/linux/security/advisories/2007_51_kernel.html
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6
http://www.ietf.org/rfc/rfc5095.txt
IPv6 拡張ヘッダの Type0 ルーティングヘッダに関する脆弱性について
http://www.allied-telesis.co.jp/support/list/faq/vuls/20071025.html

参考　　マスタリング TCP/IP　IPv6 編　第 1 版　p.46-59

27).IPv6 IPComp パケットの処理によりサービス不能状態に陥る問題

27)-1. 分類:IP 【IPv6】

27)-2. 概要

KAME プロジェクト(注 1)の IPv6 パケットを処理する IPsec スタック(以後、「IPv6 IPsec スタック」と記載する。)に IPv6 IPComp パケットを正常に処理できない問題が存在するため、不正に細工された IPv6 IPComp パケットを受信するとシステムの停止、または再起動に陥る可能性がある。

27)-3. 解説

攻撃手法とその影響

攻撃者は、細工を施した IPv6 IPComp パケットを、KAME プロジェクトの IPv6 IPsec スタックが実装するシステムに対して送信することでこの問題を悪用できる。この問題を悪用した攻撃例を図 27-1 から図 27-4 に示す。

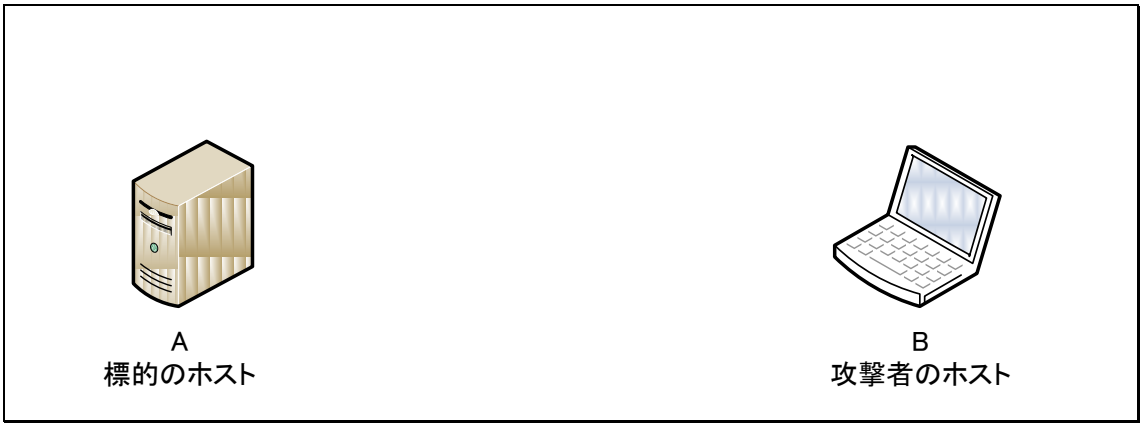


図 27-1 ターゲットネットワーク

注 1:株式会社インターネットイニシアティブ、日本電気株式会社、株式会社東芝、株式会社日立製作所、富士通株式会社、横河電機株式会社による共同研究プロジェクト。FreeBSD、 OpenBSD、 NetBSD といった BDS 系と呼ばれる OS 上に IPv6 を中心としたインターネット技術の標準コードを実装することを目的として、1998 年に発足した。BSD ライセンス下でフリーソフトウェアとして公開され、現在までに各 BSD UNIX の IPv6 スタックとして採用されており、さらにルータ等の組み込み製品等にも採用されている。http://www.kame.net/

攻撃者は、ホスト B から細工した IPv6 IPComp パケットを標的のホスト A に送信する。図 27-2 にその様子を示す。

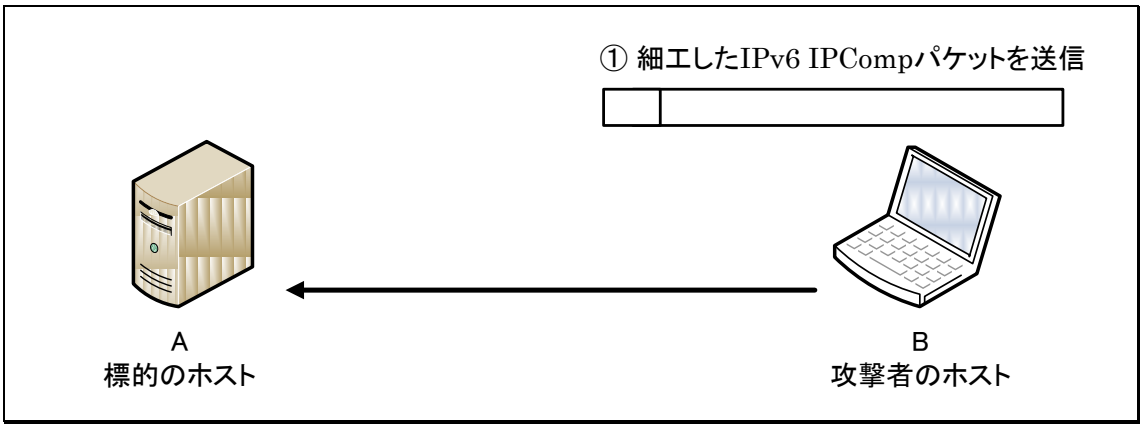


図 27-2　細工した IPv6 IPComp パケットの送信

図 27-3 に示すように攻撃者のホスト B から送信された IPv6 IPComp パケットが標的のホスト A に到達し、標的のホスト A は、受信した IPv6 IPComp パケットを IPv6 IPsec スタックで処理しようとする。

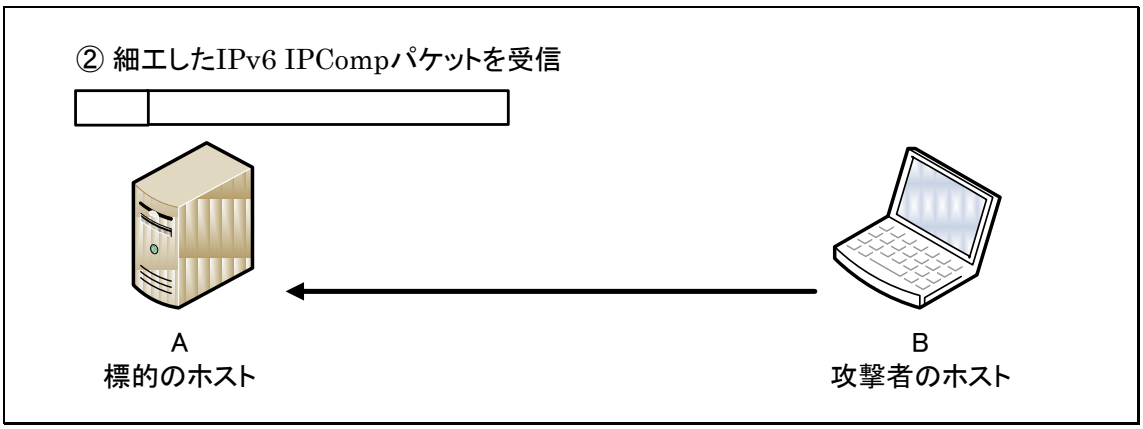


図 27-3　IPv6 スタックでの受信

このとき、IPv6 IPsec スタックにおいて攻撃者のホスト B から送信された IPv6 IPComp パケットを正しく処理することできず、図 27-4 に示すように標的のホスト A においてシステムの停止、または再起動が起こり、その結果サービス不能状態に陥ってしまう可能性がある。

図 27-4　IPv6 スタック処理不能

ここで IPv6　IPComp パケットの構造について説明する。IPComp は RFC3173 にて規定されている IP パケットのトランスポート層を圧縮するプロトコルであり、VPN のスループット改善のために IPSec と組み合わせて使用されることが多い。IPv6 ヘッダおよび IPComp ヘッダの構造と関係を図 27-5 および図 27-6 に示す。

図 27-5 は、IPv6 IPComp パケットの構成図である。IPv6 IPComp パケットは、IPv6 ヘッダを先頭に、拡張ヘッダ(注 2)、IPComp ヘッダ、上位層ヘッダ、ペイロードと続くことで構成されている。拡張ヘッダはパケットの先頭から処理され、ノードは IPv6 ヘッダや拡張ヘッダ内の次ヘッダの値によって、以降のヘッダの処理が必要かどうかを判断している。なお、RFC3173 により、IPComp ヘッダは IPv6 においてはペイロードの一部とみなされているため、中継点(ホップバイホップオプションヘッダ)、経路制御(ルーティングヘッダ)、および断片(フラグメントヘッダ)という拡張ヘッダの前に配置してはならないと規定されており、図 27-5 に示すような位置に IPComp ヘッダは配置される。

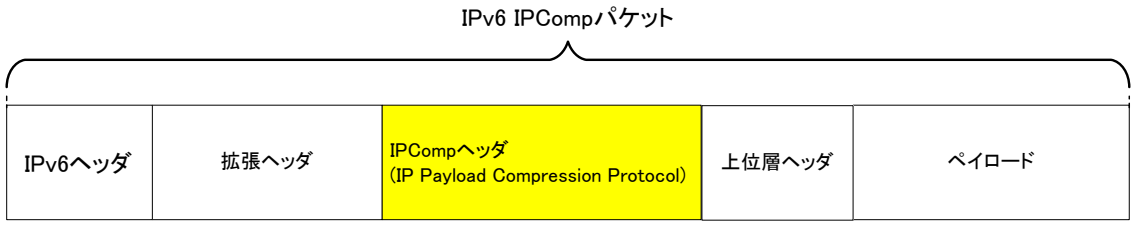


図 27-5　IPv6 IPComp パケットの構成概要

注 2:IPv6 では、全パケットに共通かつ必須の情報のみを IPv6 ヘッダで定義し、その他のオプション情報は拡張ヘッダとして扱うこととしている。拡張ヘッダはホップバイホップオプションヘッダ、終点オプションヘッダ、ルーティングヘッダ、フラグメントヘッダ、AH(Authentication Header)、ESP(Encapsulation Security Payload)ヘッダ、Mobile IPv6 用ヘッダ等が存在する。全てのヘッダは次ヘッダ領域を保持しており、プロトコル番号を指定することで次に続くヘッダを実現している。なお、拡張ヘッダは推奨される配置順があり、Mobile IPv6 用ヘッダを除き、上記に示したヘッダ名順に並ぶことが望ましい。

図 27-6 のように、IPv6 ヘッダおよび拡張ヘッダには次ヘッダという 8 ビットの領域が存在し、次に続くヘッダのタイプを示している。この次ヘッダに入る数値はプロトコル番号であり、IPComp ヘッダを示す場合には 108 を指定する。次ヘッダに 108 を指定することで次に続くヘッダのタイプが IPComp ヘッダとして扱われ、IPComp ヘッダ以降はペイロードと見なされ圧縮処理が行われる。なお、IPComp のプロトコル番号が 108 であることは、RFC1700 にて規定されている。

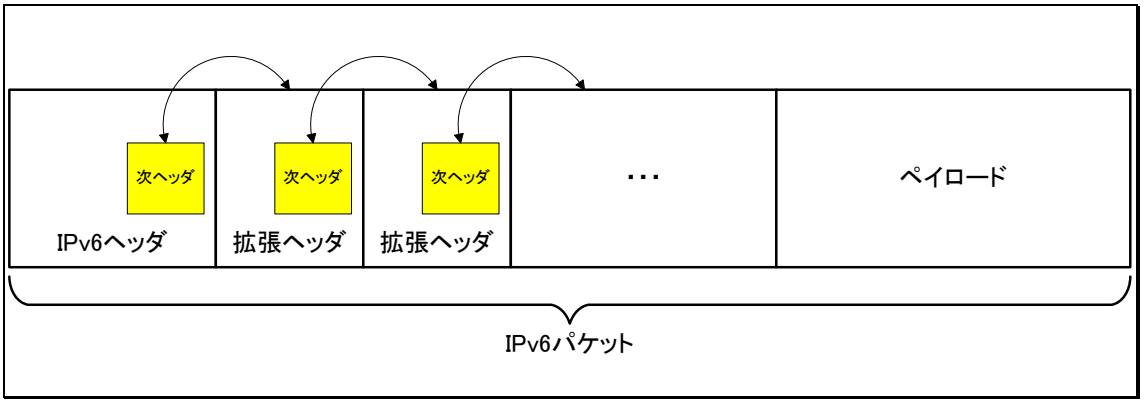
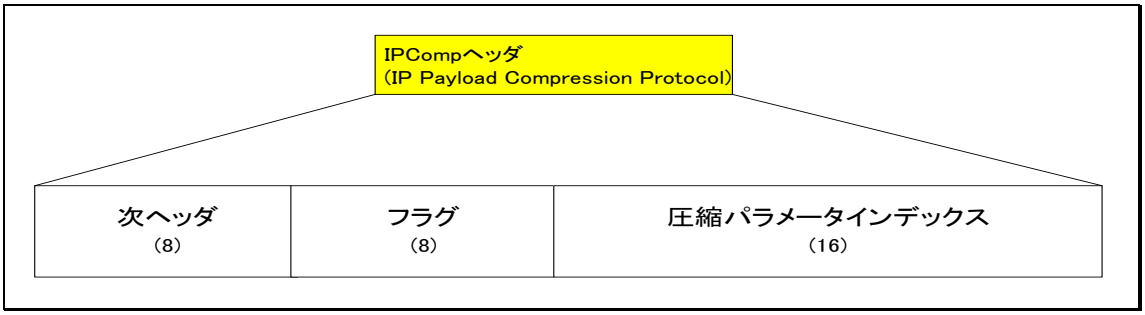


図 27-6　次ヘッダと IPv6 パケットの関係図

IPComp ヘッダの構造は図 27-7 に示すような構造を持つ。次ヘッダは 8 ビットのセレクタであり、次に続くプロトコル番号を指定することができる。フラグは 8 ビットの領域であるものの、この領域の値は 0 にしなければならないと RFC3173 にて規定されている。

また、受信側のノードはこのフラグを無視することとなっている。圧縮パラメータインデックスは 16 ビットの領域を保持しており、主に圧縮アルゴリズムに関する情報を保持する領域となっている。



※( )内の数字はビット数

図 27-7　IPComp ヘッダの構造

このように RFC に準拠した IPv6 IPComp パケットの取扱いについては、通常の他のヘッダ処理でも行われていることと同様に次ヘッダの値(108)、IPComp ヘッダ内の構造に加え、拡張ヘッダ間の配置関係や圧縮ペイロード部との位置関係についても規定されている。

原因と考察

この問題は KAME プロジェクトで作成された IPv6 スタックの問題を利用したものである。KAME プロジェクトが作成した IPv6 IPsec スタックには ipcomp_input.c におけるコーディングミスが存在し、ipcomp_input6( )内の m_pulldown( )関数の戻り値チェックが適切でないため、この問題が存在すると考えられる。今回の調査により一部製品を対象とした Exploit コードが公開されているため、この攻撃が成立するための仕組みを考察する上での有益な情報源の１つとして、Exploit コードが生成する攻撃パケットについて解説する。

Exploit コードは、図 27-8 に示すような IPv6 ヘッダを持つパケットを送信するコードになっている。

バージョン(4) 6	トラフィッククラス(8) 0	フローラベル(20) 0	
ペイロード長(16) 0		次ヘッダ(8) 108	最大ポップ数(8) 102

※( )内はビット数

図 27-8　Exploit コードが送信する不正な IPv6 パケットの構造

公開されている Exploit コードを、IPv6 ヘッダの構造(送信元アドレス、および送信先アドレスは省略)に当てはめると、次ヘッダの領域にプロトコル番号 108、ペイロード長に 0 が指定されていることがわかる。しかし、IPComp はペイロードを圧縮する性質上、ペイロード長が 0 にはなり得ない。また、IPComp ヘッダに関する記述はこのコード内には含まれておらず、図 27-8 に示すパケットはこれまで説明してきたような通常の IPv6 IPComp パケットの構成とは異なっていることがわかる。

つまり、この Exploit コードからは IPComp ヘッダ自体の処理に問題が存在するのではなく、IPv6 ヘッダで次ヘッダに IPComp ヘッダを指定しつつも、IPComp ヘッダが存在しないために正常に処理が出来ずにサービス不能状態に陥ると考えられる。

図 27-9 は、図 27-8 の Exploit コードによる影響を受ける範囲を示したものである。本脆弱性の原因である ipcomp_input.c は、図 27-9 に示す条件下でのみ再現性があり、IPv6 IPComp パケットでも受信する側のホストが IPsec を有効にしていなければ本脆弱性による障害は発生しないと推測される。なお、IPsec のデフォルト設定(有効/無効)は製品ごとに異なっている。

IPComp			
IPsec なし		IPsec あり	
IPv4	IPv6	IPv4	IPv6
脆弱性なし	脆弱性なし	脆弱性なし	脆弱性あり

図 27-9 IPv6 IPsec スタックの実装における本脆弱性の存在箇所

IPComp は IPv6 において拡張ヘッダとの配置順や圧縮されるペイロード部の位置関係等、複雑な条件処理が必要な IP オプションの 1 つであると言える。

27)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題は、2008 年 2 月頃に KAME プロジェクトのメンバーの一人である坂根 昌一 氏により注意喚起がなされている他、同メンバーの曽我部 崇 氏からも IPA へ情報提供がなされており、KAME プロジェクトに由来する IPv6 IPsec スタックを実装するシステムに影響がある可能性について告知した。その後、当該スタックを実装した製品を提供しているベンダにおいてこの問題の影響に関する報告が行われている。また、この脆弱性を利用した Exploit コードがインターネット上に公開されている。

なお、現時点では影響を受ける多くのベンダにおいて修正済みのバージョンや対策方法が提供されている。詳細については、各ベンダが提供する情報を参照のこと。

27)-5. IPv4 環境における影響

IPComp は IPv4 においても使用可能であるが、この問題は IP プロトコルの実装上の問題ではないため、IP プロトコルのバージョンに関わらず影響はない。これは KAME プロジェクト由来の IPv6 IPsec スタック特有の問題であり、当該スタックを実装する製品にのみ影響がある。

27)-6. 実装ガイド

3. 通常では処理の対象になりえないような場合でも、製品の設計開発の段階で以下のような項目について対応を検討し、不適切なものを適切に破棄されるようにする等の処置を行う。
   (ア) 想定外のパケットを洗い出し、パケット処理部における厳密なテスト項目の作成等
   (イ) 破棄する対象の条件定義の実施
4. IPComp を使用しない場合、IPv6 IPComp パケットは処理せずに破棄する。(次ヘッダ値:108 を持つ IPv6 IPComp パケットを破棄する。)
5. ペイロードの圧縮プロトコルを IPComp ではなく他の圧縮プロトコルを利用する。

27)-7. 運用ガイド

1. 影響を受ける製品ベンダから公開されているパッチを適用する。
2. ファイアウォール等のパケットフィルタリングで各ヘッダの持つ次ヘッダのプロトコル番号 108(IPComp のプロトコル番号)がセットされている IPv6 IPComp パケットを破棄する。
3. IPsec を利用しない場合は、IPsec が無効になっているか確認する。

27)-8. 参考情報

この問題についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本問題調査時点(2010 年 5 月)のものである。

1994 年 RFC1700、 ASSIGNED NUMBERS
http://www.ietf.org/rfc/rfc1700

2001 年 RFC3173、 IP Payload Compression Protocol(IPComp)
http://www.ietf.org/rfc/rfc3173

2007 年 kame/kame/sys/netinet6/ipcomp_input.c (The KAME project)
http://www.kame.net/dev/cvsweb2.cgi/kame/kame/sys/netinet6/ipcomp_input.c.diff?r1=1.36;r2=1.37

CVS log for src/sys/netinet6/ipcomp_input.c(NetBSD)
http://cvsweb.netbsd.org/bsdweb.cgi/src/sys/netinet6/ipcomp_input.c?f=u&only_with_tag=netbsd-3-1

2008 年 Common Vulnerabilities and Exposures CVE-2008-0177
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0177
KAME IPv6 Stack Can Be Crashed By Remote Users Sending an IPv6 Packet Containing an IPComp Header
http://securitytracker.com/alerts/2008/Feb/1019314.html
Secunia Advisory SA28788
http://secunia.com/advisories/28788
KAME Project IPv6 IPComp Header Denial Of Service Vulnerability
http://www.securityfocus.com/bid/27642
JP Vendor Status Notes JVNVU#110947
http://jvn.jp/cert/JVNVU110947/
IIJ SEIL Series 脆弱性情報 偽造された IPv6 パケットに対する受信処理の問題
http://www.seil.jp/seilseries/security/2007/12181268.php
JPCERT/CC REPORT 2008-02-14
http://www.jpcert.or.jp/wr/2008/wr080601.txt

2008 年 FreeBSD-SA-08:04.ipsec
http://security.freebsd.org/advisories/FreeBSD-SA-08:04.ipsec.asc
Apple Mac OS X xnu <= 1228.3.13 ipv6-ipcomp Remote kernel DoS PoC
http://www.milw0rm.com/exploits/5191
※mu-b@digit-labs.org により作成された PoC
SecurityTracker Alert ID: 1019314
http://securitytracker.com/alerts/2008/Feb/1019314.html
Secunia Advisory SA28816
http://secunia.com/advisories/28816
APPLE-SA-2008-05-28 Security Update 2008-003 and Mac OS X v10.5.3
http://lists.apple.com/archives/security-announce/2008//May/msg00001.html
Secunia Advisory SA29130
http://secunia.com/advisories/29130

Apple セキュリティアップデート 2008-003 / Mac OS X 10.5.3 の
セキュリティコンテンツについて
http://support.apple.com/kb/HT1897?viewlocale=ja_JP
APPLE-SA-2008-07-11 iPhone 2.0 and iPod touch 2.0
http://lists.apple.com/archives/security-announce/2008//Jul/msg00001.html
JVNDB-2008-001083 KAME プロジェクトの IPv6 スタックにおける IPComp パケットの処理にサービス運用妨害(DoS)の問題
http://jvndb.jvn.jp/ja/contents/2008/JVNDB-2008-001083.html
National Cyber-Alert System Vulnerability Summary for CVE-2008-0177
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-0177

2009 年

Secunia Advisory SA31074
http://secunia.com/advisories/31074
US-CERT Vulnerability Note VU#110947
KAME project IPv6 IPComp header denial of service vulnerability
http://www.kb.cert.org/vuls/id/110947
ヤマハ RT シリーズのセキュリティに関する FAQ　TCP の実装におけるサービス運用妨害(DoS)の脆弱性について
http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/VU943657.html
ヤマハ RT シリーズルータ IPComp の仕様
http://www.rtpro.yamaha.co.jp/RT/docs/ipsec/ipcomp.html
CENTURY SYSTEM　NXR シリーズ技術情報 NXR シリーズでの IPv6 の実装におけるサービス運用妨害(DoS)の脆弱性について(JVN#75368899)
http://www.centurysys.co.jp/support/nxr_common/JVN75368899.html
NEC 製品セキュリティ情報 NV09-014 複数の TCP の実装におけるサービス運用妨害(DoS)の脆弱性
http://www.nec.co.jp/psirt/secinfo/nv09-014.html
古川電エネットワーク 技術情報インデックス TCP の実装におけるサービス妨害の脆弱性について
http://www.furukawa.co.jp/fitelnet/topic/vulnera_20091009.html
富士通 複数の TCP の実装におけるサービス運用妨害(DoS) の脆弱性に関する対応について(ネットワーク製品)
http://fenics.fujitsu.com/products/support/2009/tcp_11.html

参考:

マスタリング TCP/IP IPv6 編 p.49-68

28).ARP テーブルが汚染される問題

28)-1.　分類：ARP 【IPv4】【IPv6】

28)-2.　概要

イーサネットアドレス解決(ARP)プロトコルには、ARP パケットの真正性を保証する仕組みが無いため、不正な ARP パケットにより、ARP テーブルが汚染される問題が存在する。この問題によって通信のリダイレクトが発生する。

28)-3.　解説

攻撃手法とその影響

この問題を悪用して行われる攻撃は、トラフィックのリダイレクトを引き起こし、通信内容の盗聴を可能とする。この問題で行われうる攻撃の流れを、図 28-1 から 図 28-2 に示す。

図 28-1 において、攻撃者のホスト C と、攻撃者に盗聴されるホスト B は同一のローカルエリアネットワーク(LAN)にスイッチで接続されており、LAN 外への通信はゲートウェイ A によって中継される。

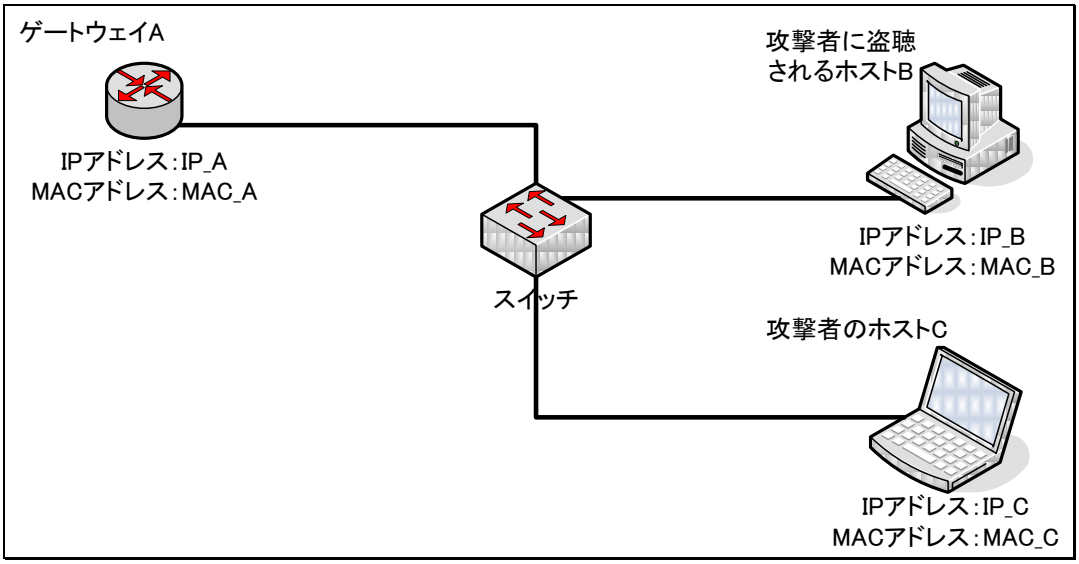


図 28-1 ターゲットネットワーク

【ARP テーブルが汚染される問題】

攻撃者は、ゲートウェイ A とホスト B に対して、不正な ARP パケットを送信して、それぞれの ARP テーブルを汚染する。

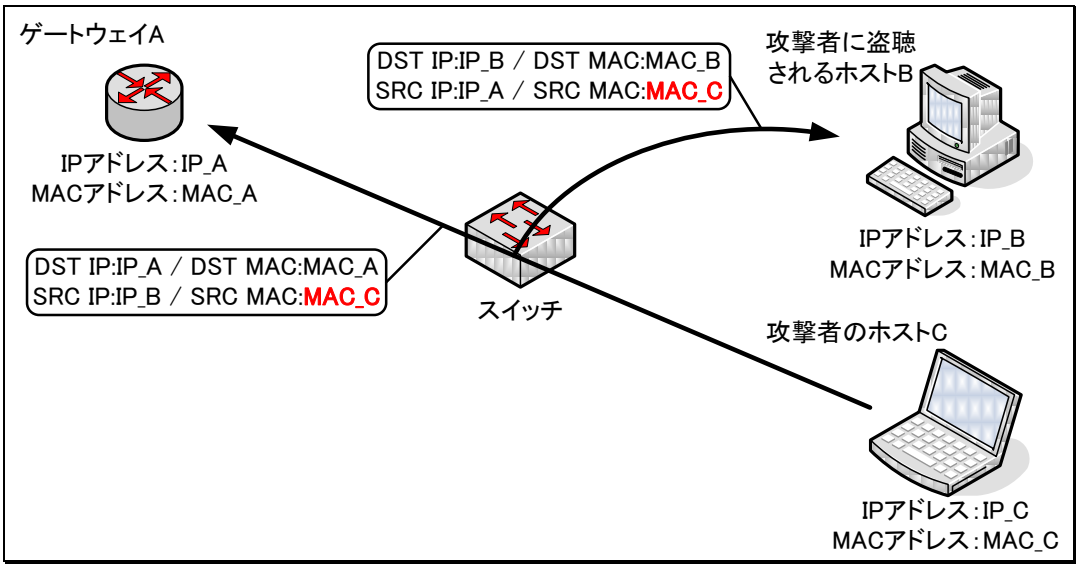


図 28-2 ARP テーブルの汚染

攻撃者からの不正な ARP パケットによって、各ホストの ARP テーブルは、表 28-1 の正常な状態から 表 28-2 の汚染された状態に変化する。また、攻撃者は、ゲートウェイ A とホスト B の ARP テーブルが、正常な状態に戻るのを防ぐため、不正な ARP パケットを定期的に送信し続ける。

表 28-1 正常な ARP テーブル

ホスト	ARP キャッシュエントリ	
	IP アドレス	MAC アドレス
ゲートウェイ A	IP_B	MAC_B
ホスト B	IP_A	MAC_A

表 28-2 汚染された ARP テーブル

ホスト	ARP キャッシュエントリ	
	IP アドレス	MAC アドレス
ゲートウェイ A	IP_B	**MAC_C**
ホスト B	IP_A	**MAC_C**

表 28-2 の状態で、ホスト B がゲートウェイ A に対してパケットを送信すると、ARP テーブル上のゲートウェイ A の MAC アドレスが攻撃者の MAC アドレス(MAC_C)となっているため、ゲートウェイ A 宛のパケットでありながら、攻撃者のホストにパケットが届く。

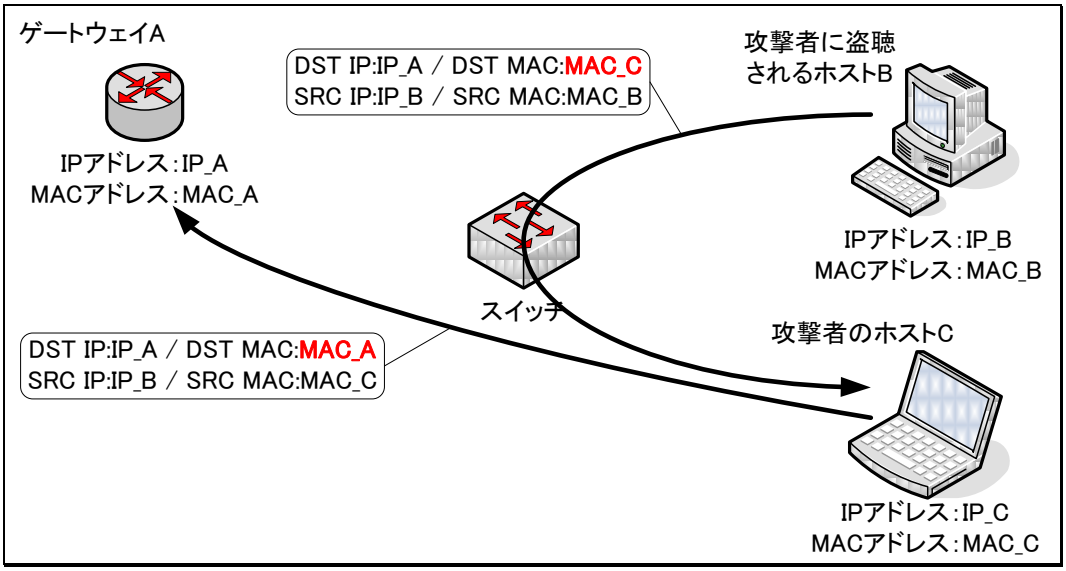


図 28-3 ARP 汚染による通信のリダイレクト：ホスト B

攻撃者のホストは、受信したゲートウェイ A 宛のパケットを盗聴し、さらにそのパケットの送信先 MAC アドレスを正しい MAC アドレス(MAC_A)に書き換えて、送信する。

また、ゲートウェイ A がホスト B に対してパケットを送信した場合においても、ARP テーブル上のホスト B の MAC アドレスが攻撃者の MAC アドレス(MAC_C)となっているため、ホスト B 宛のパケットでありながら、攻撃者のホストにパケットが届く。

【ARP テーブルが汚染される問題】

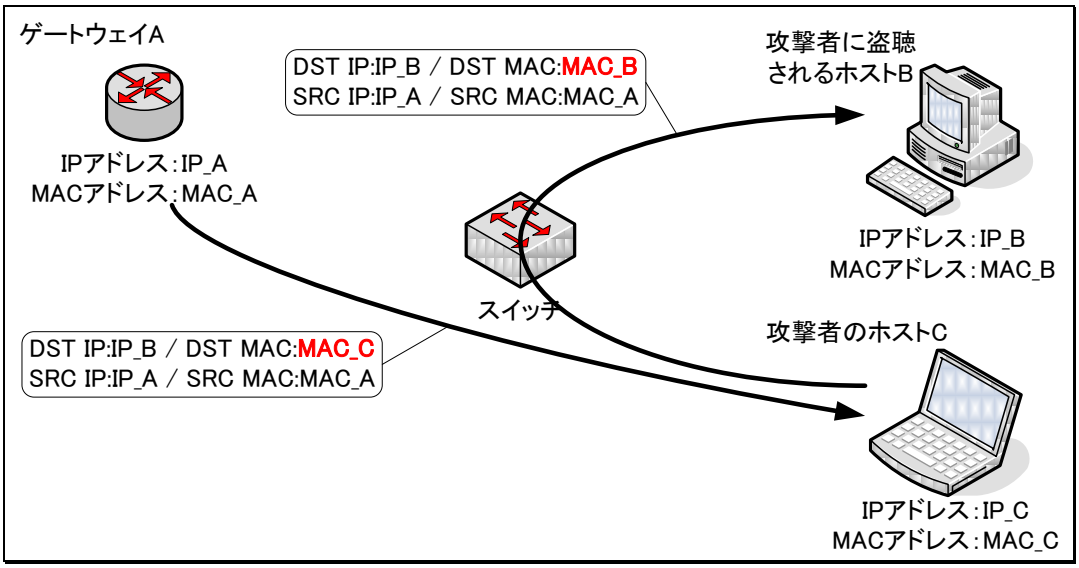


図 28-4 ARP 汚染による通信のゲートウェイ A

攻撃者のホストは、受信したホスト B 宛のパケットを盗聴し、さらにそのパケットの送信先 MAC アドレスを正しい MAC アドレス(MAC_B)に書き換えて、送信する。この一連の流れによって、ゲートウェイ A とホスト B の間の全ての通信は、攻撃者のホスト C を中継して行われ、その内容は攻撃者の知るところとなる。

この攻撃は、攻撃者が通信を行うホストの中間に介在し、セキュリティを侵害する。この種の攻撃手法を総称して、中間者攻撃(Man-In-the-Middle Attack：MIM Attack)と呼ぶことがある。

原因と考察

この脆弱性の原因は、RFC 826 で規定されている ARP の仕様にある。仕様では ARP パケットが偽造されて、テーブルが汚染されることについて考慮されていない。

イーサネットと IP で構成されるネットワークにおいて通信を行うには、データリンク層のアドレスである MAC アドレスと、ネットワーク層のアドレスである IP アドレスの組み合わせが必要となる。それらは、各ホストが ARP テーブルで管理している。

ホストが ARP テーブルを作成する仕組みを、図 28-5 から図 28-7 に示す。

【ARP テーブルが汚染される問題】

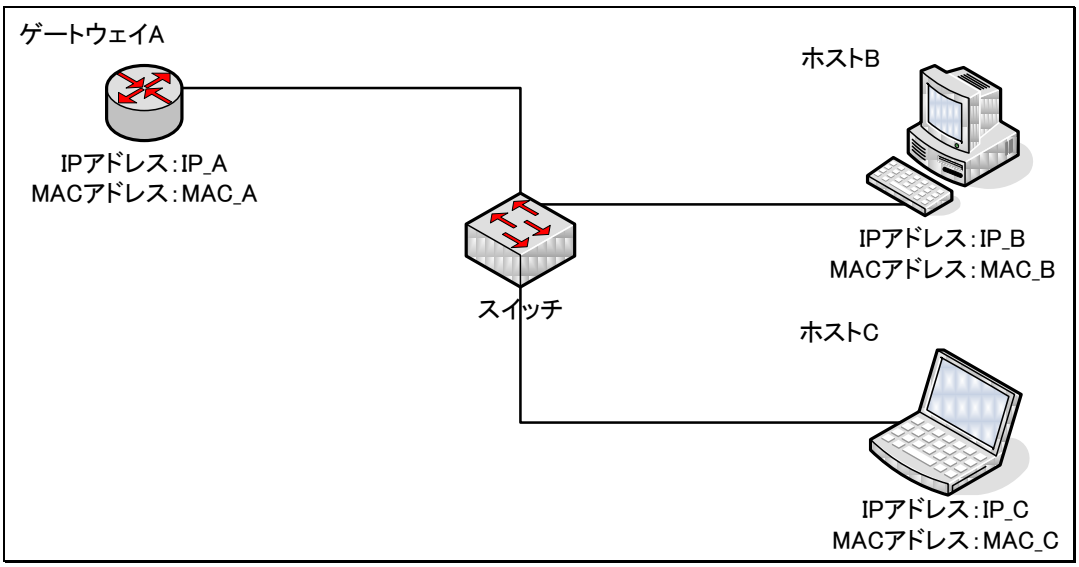


図 28-5 ローカルエリアネットワーク

図 28-5 において、各ホストの ARP テーブルは表 28-3 に示すとおりである。

表 28-3 図 28-5 の 3 ホストの ARP テーブル

ホスト	ARP キャッシュエントリ	
	IP アドレス	MAC アドレス
ゲートウェイ A	—	—
ホスト B	—	—
ホスト C	—	—

ホスト B がゲートウェイ A と通信する場合には、ホスト B は自身の ARP テーブルを参照し、ゲートウェイ A のエントリがあるかを確認する。そのエントリは存在しないため、ホスト B は「IP アドレス：IP_A のホストは、MAC アドレス：MAC_B に応答せよ」という内容のパケットをブロードキャストする。これを ARP リクエストという。

【ARP テーブルが汚染される問題】

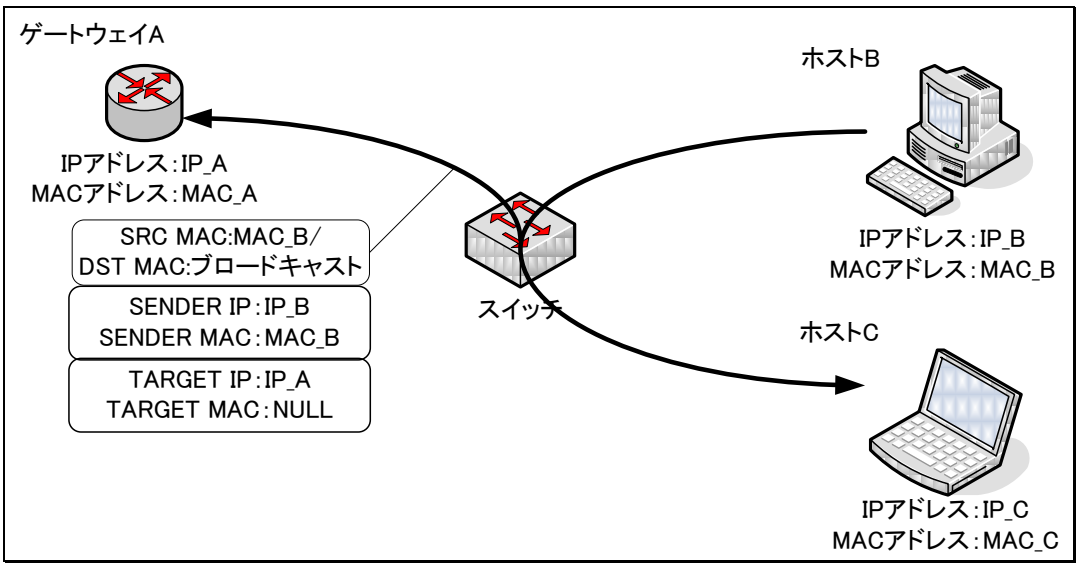


図 28-6 ARP リクエスト

ホスト B が問い合わせた IP アドレス(IP_A)を持つゲートウェイ A は、ホスト B に「IP アドレス：IP_A の MAC アドレスは MAC_A」という内容のパケットを、ユニキャストで送信する。これを ARP リプライという。

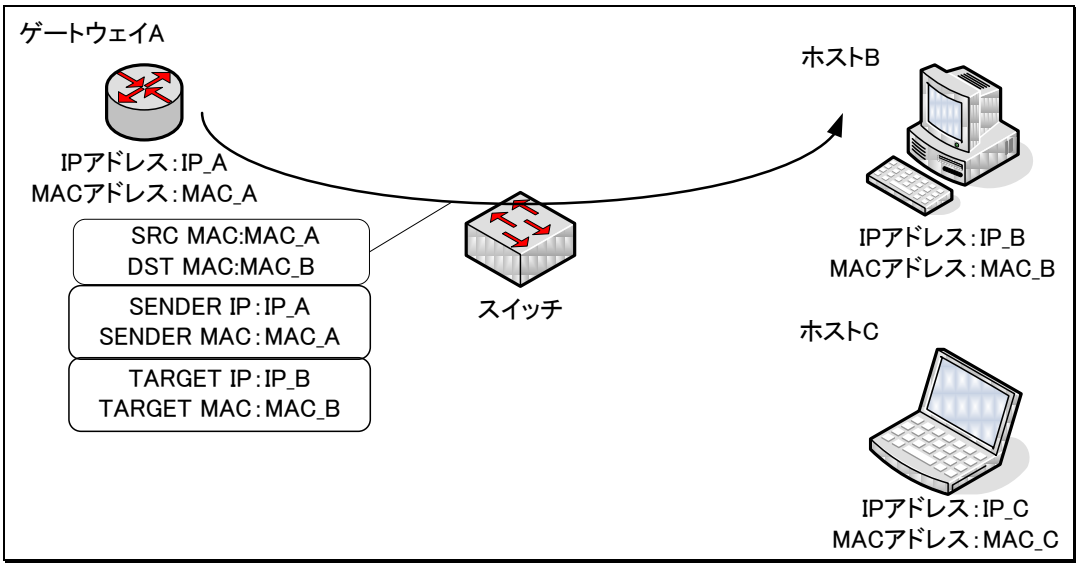


図 28-7 ARP リプライ

図 28-6 と図 28-7 に示した、ARP リクエストと ARP リプライによって、ホスト B とゲートウェイ A の ARP テーブルは表 28-4 に示す内容となる。これによって、ホスト B はゲートウェイ A と通信を行うことが可能となる。

【ARP テーブルが汚染される問題】

表 28-4 ARP テーブル

ホスト	ARP キャッシュエントリ	
	IP アドレス	MAC アドレス
ゲートウェイ A	IP_B	MAC_B
ホスト B	IP_A	MAC_A
ホスト C	―	―

ゲートウェイ A、ホスト C についても同様であり、図中の3つのホストが、他の全てのホストと通信を行う場合、これらの ARP テーブルは表 28-5 に示す内容となる。

表 28-5 ARP テーブル

ホスト	ARP キャッシュエントリ	
	IP アドレス	MAC アドレス
ゲートウェイ A	IP_B	MAC_B
	IP_C	MAC_C
ホスト B	IP_A	MAC_A
	IP_C	MAC_C
ホスト C	IP_A	MAC_A
	IP_B	MAC_B

この一連の仕組みによって、論理アドレス(IP アドレス)と物理アドレス(MAC アドレス)の組み合わせである ARP テーブルをホストが作成、参照することで、通信が可能となる。

しかし、ARP テーブルは、すでにエントリされている IP アドレスから ARP リプライが送られた場合、送信元の真正性を確認することなく、その内容で ARP テーブルが更新される。また、エントリに無い IP アドレスを送信元とする ARP リプライが送られた場合においても、送信元の真正性を確認することなく ARP テーブルに新たにエントリするため、送信元アドレスを偽造した ARP リプライによって、ホストの ARP テーブルを不正な MAC アドレスで汚染されてしまう危険がある。

RFC 826 では、ARP パケットの真正性の保証について明確に考慮していない。障害等で発生しうる不正なエントリを考慮して、タイムアウトやエージングの機能について記述されているが、真正性への対処ではない。(なお、RFC 1122 では古いキャッシュエントリを消去する仕組みを備えるべき、としている。)また、攻撃を継続された場合は、それらを実装したとしてもこの問題を根絶することは困難である。

【ARP テーブルが汚染される問題】

28)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題が最初に論じられたのがいつであるかは、本調査では確証を得られていないが、1997 年に Yuri Volobuev 氏の BUGTRAQ への投稿(Subject: Redir games with ARP and ICMP)において、この問題について記述がある。また、Common Vulnerabilities and Exposures(CVE)において、ARP 汚染によって、IP スプーフィングや DoS を引き起こせるとして、CVE-1999-0667 の番号が割り振られている。

この問題は ARP の仕様上の問題であるため、修正プログラム等の対策は提供されていない。この問題を悪用した攻撃手法は「arp poisoning」や「arp spoofing」として、広く知られておりツールも多数存在する。多くの場合、この問題単体を利用するものではなく、機能の一つとして提供されている。

28)-5. IPv6 環境における影響

IPv6 では、IPv4 の ARP のように別のプロトコルを定義してリンク層アドレス(イーサネットの場合は MAC アドレス)を取得するのではなく、RFC 2461 に規定される ICMPv6 の一部として動作する近隣探索によってアドレス解決が行われる。近隣探索ではアドレス解決の際に利用される近隣キャッシュという、ARP テーブルのような IP アドレスとリンク層アドレスの対応表の管理が行われる。IPv4 における ARP テーブルの汚染は、IPv6 ではこの近隣キャッシュの汚染に相当する攻撃として考えられるが、概念的には送信元を偽造した近隣広告メッセージ(注 1)を送信することによって同様の問題が発生し、IPv6 環境でもこの問題に類似した影響を受ける可能性がある。

このような近隣キャッシュのエントリに関する問題を含む近隣探索に関するセキュリティ脅威については既に懸念されており、RFC3756 においてその近隣探索に関連する幾つかの脅威について示されている。

また、このような状況における対策として、近隣探索をセキュリティ上の脅威から保護するために RFC 3971 に規定される SEND(SEcure Neighbor Discovery)という安全に近隣探索を行える仕組みが作られている。SEND では、ルータとの信頼関係の構築やパケットの改ざんと送られるメッセージの妥当性の判断ができるため、この仕組みを利用することでこの問題のように信頼のないホストから送られる偽造メッセージの無効化を実現できること考えられる。

注 1:MACアドレスを調べるために IPv4 の ARP では ARP リクエストと ARP リプライを使うが、IPv6 の場合は近隣要請メッセージ(Type=135)と近隣広告メッセージ(Type=136)を使う。

28)-6. 実装ガイド

この問題は RFC 826 の仕様の問題であるため、仕様に従う限り実装で回避することは出来ない。

28)-7. 運用ガイド

この問題による影響を緩和する手段として、以下の方法がある。

3. ローカルエリアネットワークの物理セキュリティ、あるいはその集線装置を管理し、不正なホストの接続を防止する。
4. ARP テーブルを静的テーブルとし、不正な ARP パケットによるテーブルの汚染を防止する。エントリする IP アドレスと MAC アドレスの正しいペアのリストが必要であり、大規模なネットワークでは管理負担が増加する。
5. ネットワーク型やホスト型 IDS 等により、不正な ARP パケットの検知し、対応する。IP アドレスと MAC アドレスの正しいペアのリストが必要であり、大規模ネットワークでは管理負担が増加する。

28)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1982 年 RFC 826, An Ethernet Address Resolution Protocol.
http://www.ietf.org/rfc/rfc0826.txt

1988 年 RFC2461, Neighbor Discovery for IP Version 6(IPv6)
http://www.ietf.org/rfc/rfc2461.txt

1989 年 RFC 1122, Requirements for Internet Hosts -- Communication Layers.
http://www.ietf.org/rfc/rfc1122.txt

1995 年 RFC 1868, ARP Extension - UNARP
http://www.ietf.org/rfc/rfc1868.txt

1997 年 ARP の問題についての意見が BUGTRAQ へ投稿される。(Yuri Volobuev)
http://www.insecure.org/sploits/arp.games.html

1999 年 Common Vulnerabilities and Exposures CVE-1999-0667
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0667

2004 年 RFC3756, IPv6 Neighbor Discovery(ND) Trust Models and Threats
http://www.ietf.org/rfc/rfc3756.txt

2005 年 RFC 3971, SEcure Neighbor Discovery(SEND)
http://www.ietf.org/rfc/rfc3971.txt

29).ARP テーブルが不正なエントリで埋め尽くされる問題

29)-1. 分類:ARP 【IPv4】【IPv6】

29)-2. 概要

イーサネットアドレス解決(ARP)プロトコルには、ARP パケットの真正性を保証する仕組みが無いため、不正な ARP パケットにより、ホストの ARP テーブルが埋め尽くされる問題が存在する。この問題によって通信が妨げられる問題が発生する。

29)-3. 解説

攻撃手法とその影響

この問題を悪用して行われる攻撃は、イーサネットネットワークでのアドレス解決を妨害し、通信の使用不能状態を引きおこす。この問題で行われうる攻撃の流れを、図 29-1 から図 29-2 に例示する。

図 29-1 において、攻撃者のホスト C と、攻撃者に通信を妨害されるホスト B は同一のローカルエリアネットワーク(LAN)にスイッチで接続されており、LAN 外への通信はゲートウェイ A によって中継される。

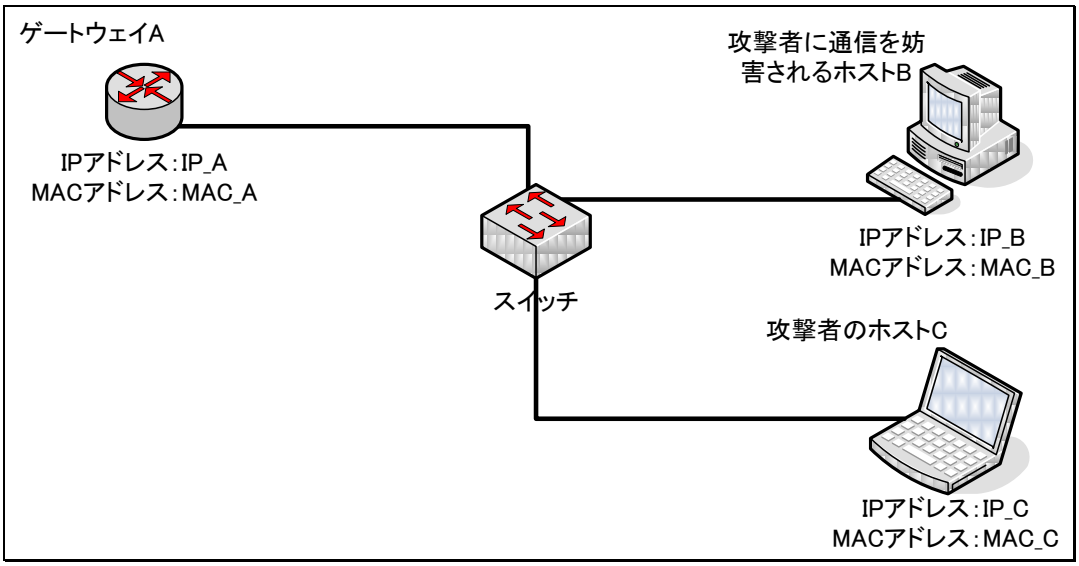


図 29-1 ターゲットネットワーク

【ARP テーブルが不正なエントリで埋め尽くされる問題】

また、このときホスト B の ARP テーブルは表 29-1 のとおりであり、最大 10 のエントリが格納できるものとする。

表 29-1 ホスト B の ARP テーブル

	ARP キャッシュエントリ	
	IP アドレス	MAC アドレス
①		
②		
・ ・ ・		
⑩		

攻撃者は、ホスト B に対して、不正な MAC アドレスがセットされた ARP リプライを大量に送信して、ARP テーブルを不正なエントリで埋め尽くす。

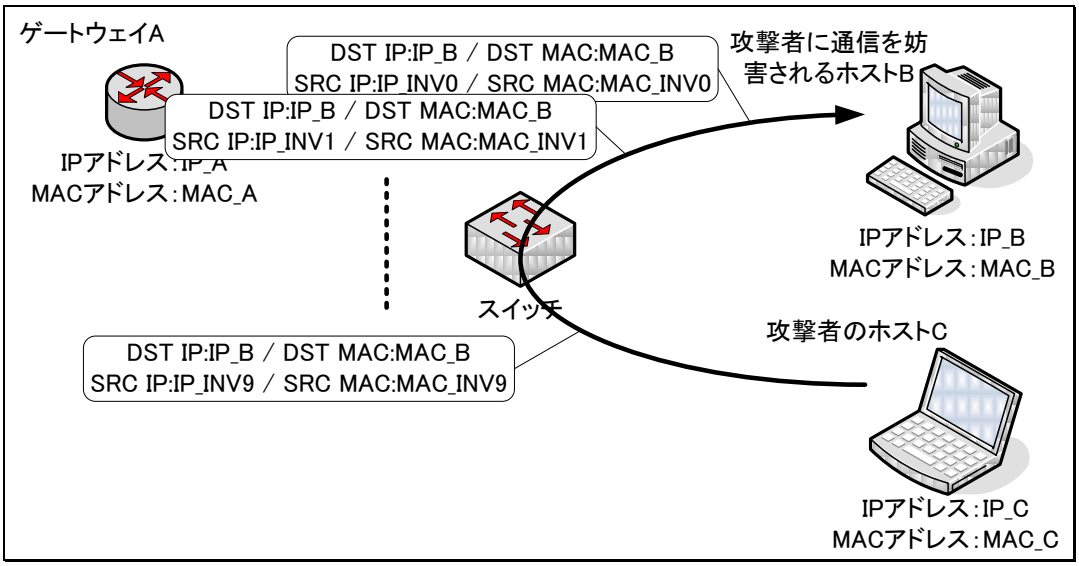


図 29-2 ARP テーブルの汚染

攻撃者からの不正な ARP パケットによって、ホスト B の ARP テーブルは、表 29-1 の正常な状態から、表 29-2 の汚染された状態に変化する。また、攻撃者は、ARP テーブルが、他の要因で正常な状態に戻るのを防ぐため、不正な ARP パケットを定期的に送信し続ける。

表 29-2 汚染されたホスト B の ARP テーブル

	ARP キャッシュエントリ	
	IP アドレス	MAC アドレス
①	IP_INV0	MAC_ INV 0
②	IP_ INV 1	MAC_ INV 1
. . .	. . .	. . .
⑩	IP_ INV 9	MAC_ INV 9

表 29-2 の状態で、ホスト B がゲートウェイ A に対してパケットを送信する場合、ARP テーブルにはゲートウェイ A のエントリが存在しないため、通信を行えない。また、この状態で ARP リクエストによってゲートウェイ A のエントリを取得しても、ARP テーブルは格納可能なエントリ数の上限に達しており、エントリを追加できないため、通信を行えない。

この状態が続く限り、ホスト B は一切のホストと通信ができず、通信不能となる。

【ARP テーブルが不正なエントリで埋め尽くされる問題】

原因と考察

この脆弱性の原因は、RFC 826 で規定されている ARP の仕様にある。仕様では ARP パケットが偽造されて、テーブルが不正なエントリで意図的に埋め尽くされることについて考慮されていない。

イーサネットとIPで構成されるネットワークにおいて通信を行うには、データリンク層のアドレスで あるMACアドレスと、ネットワーク層のアドレスであるIPアドレスの組み合わせが必要となる。それらは、各ホストが ARP テーブルで管理している。

ホストが ARP テーブルを作成する仕組みを、図 29-3 から図 29-5 に示す。

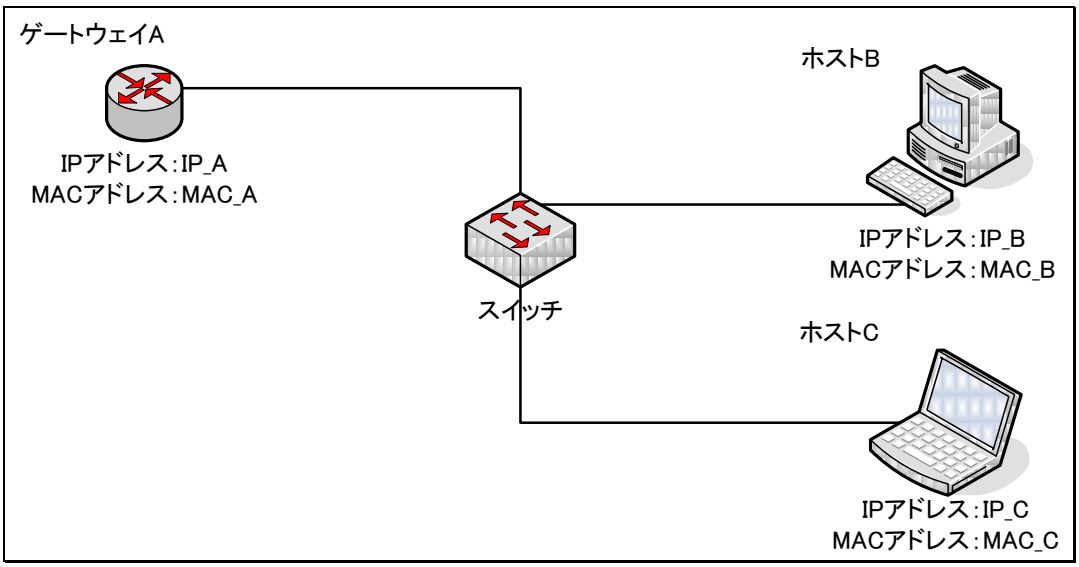


図 29-3 ローカルエリアネットワーク

図 29-3 において、各ホストの ARP キャッシュエントリは表 29-3 に示すとおりである。

表 29-3 図 29-3 の 3 ホストの ARP テーブル 1

ホスト	ARP キャッシュエントリ	
	IP アドレス	MAC アドレス
ゲートウェイ A	—	—
ホスト B	—	—
ホスト C	—	—

ホスト B がゲートウェイ A と通信を開始する場合には、ホスト B は自身の ARP キャッシュエントリを参照し、ゲートウェイ A のエントリがあるかを確認する。そのエントリは存在しないため、ホスト B は「IP アドレス：IP_A のホストは、MAC アドレス：MAC_B に応答せよ」というパケットをブロードキャストする。これを ARP リクエストという。

このリクエストでゲートウェイ A とホスト C はホスト B の IP アドレスと MAC アドレスのペアを ARP テーブルにエントリする。

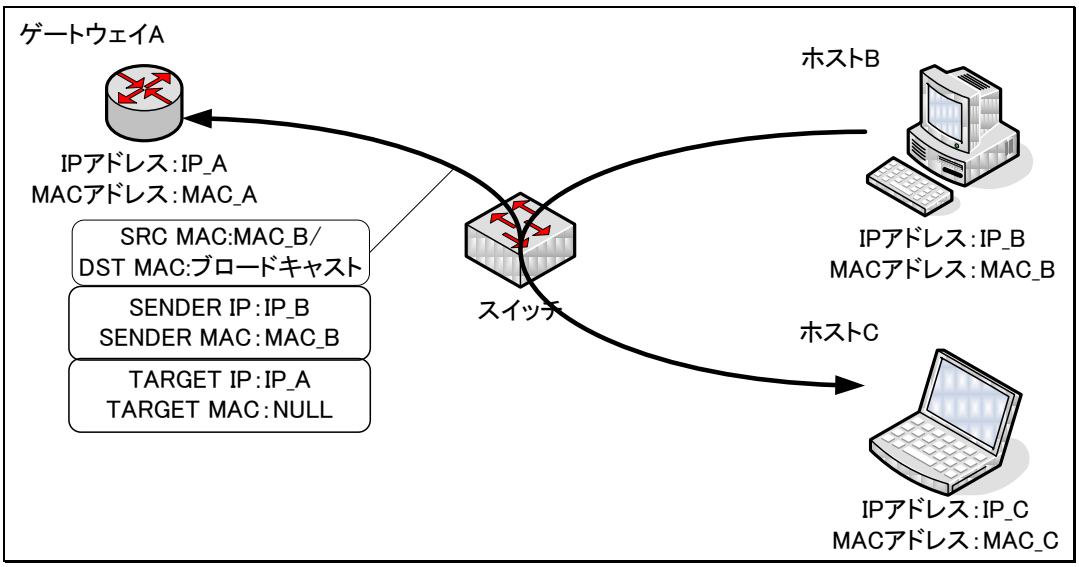


図 29-4 ARP リクエスト

ホスト B が問い合わせた IP アドレス(IP_A)を持つゲートウェイ A は、ホスト B に「IP アドレス：IP_A の MAC アドレスは MAC_A」という内容のパケットを、ユニキャストで送信する。これを ARP リプライという。このリプライでホスト B はゲートウェイ A の IP アドレスと MAC アドレスのペアを ARP テーブルにエントリする。

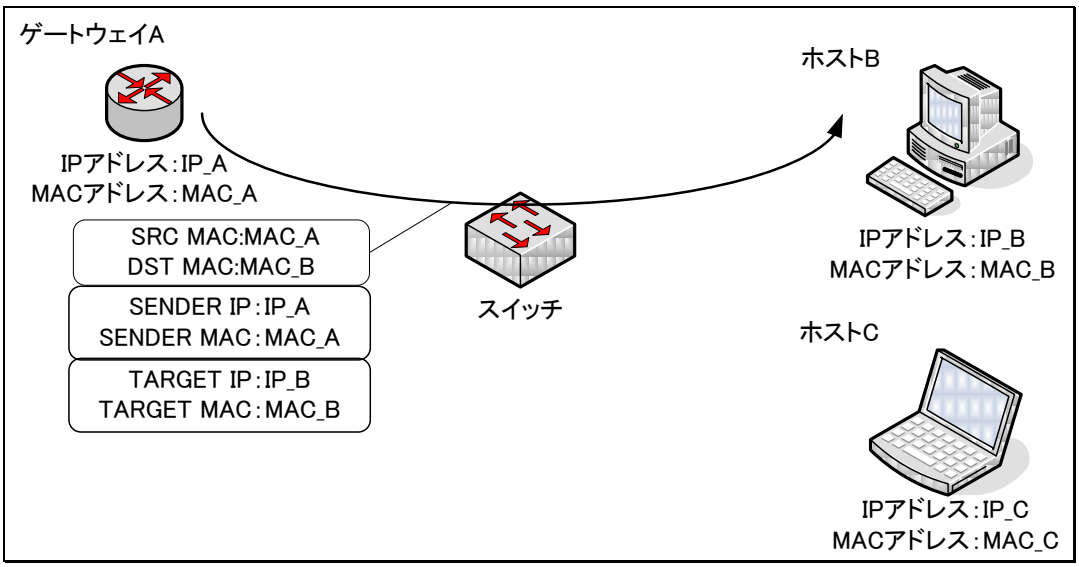


図 29-5 ARP リプライ

図 29-4 と図 29-5 に示した、ARP リクエストと ARP リプライによって、ホスト B とゲートウェイ A の ARP テーブルは表 29-4 に示す内容となる。これによって、ホスト B はゲートウェイ A と通信を行うことが可能となる。

表 29-4 図 29-5 の 3 ホストの ARP テーブル 2

ホスト	ARP キャッシュエントリ	
	IP アドレス	MAC アドレス
ゲートウェイ A	IP_B	MAC_B
ホスト B	IP_A	MAC_A
ホスト C	IP_B	MAC_B

ゲートウェイ A、ホスト C についても同様であり、図 29-4 で示された 3 つのホストが、他の全てのホストと通信を行う場合、これらの ARP キャッシュエントリは表 29-5 に示す内容となる。

表 29-5 図 29-5 の 3 ホストの ARP テーブル 3

ホスト	ARP キャッシュエントリ	
	IP アドレス	MAC アドレス
ゲートウェイ A	IP_B	MAC_B
	IP_C	MAC_C
ホスト B	IP_A	MAC_A
	IP_C	MAC_C
ホスト C	IP_A	MAC_A
	IP_B	MAC_B

この一連の仕組みによって、ホストが論理アドレス(IP アドレス)と物理アドレス(MAC アドレス)の 組み合わせである ARP テーブルを作成、参照することで、通信が可能となる。

しかし、ARP テーブルは、すでにエントリされている IP アドレスから ARP リプライが送られた場合、送信元の真正性を確認することなく、その内容で ARP テーブルが更新される。また、エントリに無い IP アドレスを送信元とする ARP リプライが送られた場合においても、送信元の真正性を確認することなく ARP テーブルに新たにエントリするため、送信元アドレスを偽造した大量の ARP リプライによって、 ホストの ARP テーブルが埋め尽くされる危険がある。

RFC 826 では、ARP パケットの真正性の保証について明確に考慮していない。しかし、障害等で発生しうる不正なエントリを考慮して、テーブル内のエントリについて、タイムアウトやエージングの機能を備えることが望ましい、としている。また、RFC 1122 では古いキャッシュエントリを消去する仕組みを備えるべき、としている。

タイムアウト等の機能を実装した場合においても、この攻撃を継続、あるいはネットワーク内にこの攻撃を行うウィルス、ワーム等が拡散した場合は、攻撃元を根絶する必要がある。

29)-4. 発見の経緯とトピック、対策の動き、現在の動向

この問題が最初に論じられたのがいつであるかは、本調査では確証を得られていないが、1997 年に Yuri Volobuev 氏の BUGTRAQ への投稿(Subject: Redir games with ARP and ICMP)において、この問題について記述がある。1999 年、Common Vulnerabilities and Exposures(CVE)に おいて、ARP 汚染によって、IP スプーフィングや DoS を引き起こせるとして、CVE-1999-0667 の番号が割り振られている。

この問題は古典的な攻撃手法の1つとされ、タイムアウト機能等による緩和策が提案されており、多くの OS で実装されている。しかし、1999 年の CVE-1999-0667 から現在に至るまで、各種 OS に 依然としてこの問題があることが報告されており、留意すべきであると思われる。

また、この問題は ARP 汚染による攻撃手法の一つとして、広く知られており、ツールも多数存在する。多くの場合、この問題単体を利用するものではなく、機能の一つとして提供されている。

29)-5. IPv6 環境における影響

IPv6 では、IPv4 の ARP のように別のプロトコルを定義してリンク層アドレス(イーサネットの場合は MAC アドレス)を取得するのではなく、RFC 2461 に規定される ICMPv6 の一部として動作する近隣探索(Neighbor Discovery)によってアドレス解決が行われる。近隣探索ではアドレス解決の際に利用される近隣キャッシュという、ARP テーブルのような IP アドレスとリンク層アドレスの対応表の管理が行われる。IPv4 における ARP テーブルの汚染は、IPv6 ではこの近隣キャッシュの汚染に相当する攻撃として考えられるが、概念的には送信元を偽造した大量の近隣広告メッセージ(注 1)を送信することによって、近隣キャッシュを埋め尽くされ、通信を妨げられるというシナリオが IPv6 でも考えられ、この問題の類似した影響を受ける可能性がある。

このような近隣キャッシュのエントリに関する問題を含む近隣探索に関するセキュリティ脅威については既に懸念されており、RFC3756 においてその近隣探索に関連する幾つかの脅威について示されている。RFC 2461 では近隣キャッシュにおける制限、ガーベジコレクションとタイムアウトの関係についても触れられている。

また、このような状況における対策として、近隣探索をセキュリティ上の脅威から保護するために RFC 3971 に規定される SEND(Secure Neighbor Discovery)という安全に近隣探索を行える仕組みが作られている。SEND では、ルータとの信頼関係の構築やパケットの改ざんと送られるメッセージの妥当性の判断ができるため、この仕組みを利用することでこの問題のように信頼のないホストから送られる偽造メッセージの無効化を実現できること考えられる。

注 1:MACアドレスを調べるために IPv4 の ARP では ARP リクエストと ARP リプライを使うが、IPv6 の場合は近隣要請メッセージ(Type=135)と近隣広告メッセージ(Type=136)を使う。

29)-6. 実装ガイド

この問題は RFC 826 の仕様の問題であるため、仕様に従う限り実装で回避することは出来ない。しかし ARP テーブルにタイムアウトやエージングの機能を実装することで、問題による影響を緩和することができる。

RFC 826 では、ARP テーブル内のキャッシュエントリを削除する機能について述べ、さらなる検討が必要としている。

RFC 1122 では上記を備えるべきとし、それがタイムアウトによる場合はタイムアウト値が設定可能である事が望ましい、としている。

29)-7. 運用ガイド

この問題による影響を緩和する手段として、以下の方法がある。

1. 利用している OS 等に、この問題が報告された場合は、直ちに修正プログラムを適用する。
2. ローカルエリアネットワークの物理セキュリティ、あるいはその集線装置を管理し、不正なホストの接続を防止する。

29)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1982 年 RFC 826, An Ethernet Address Resolution Protocol.
http://www.ietf.org/rfc/rfc0826.txt

1989 年 RFC 1122, Requirements for Internet Hosts -- Communication Layers.
http://www.ietf.org/rfc/rfc1122.tx

1995 年 RFC 1868, ARP Extension - UNARP.
http://www.ietf.org/rfc/rfc1868.txt

1997 年 ARP の問題についての意見が BUGTRAQ へ投稿される。(Yuri Volobuev)
http://www.insecure.org/sploits/arp.games.html

1998 年 RFC 2461, Neighbor Discovery for IP Version 6(IPv6).
http://www.ietf.org/rfc/rfc2461.txt

1999 年　Common Vulnerabilities and Exposures CVE-1999-0667
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0667

2000 年　Common Vulnerabilities and Exposures CVE-2000-0914
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0914

2001 年　Common Vulnerabilities and Exposures CVE-2001-1055
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-1055

2002 年　Common Vulnerabilities and Exposures CVE-2002-0438
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0438

2003 年　Common Vulnerabilities and Exposures CVE-2003-0804
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0804

2004 年　RFC3756, IPv6 Neighbor Discovery(ND) Trust Models and Threats
http://www.ietf.org/rfc/rfc3756.txt

2005 年　Sun Solaris に同種の脆弱性が報告される。
http://secunia.com/advisories/14286/

RFC 3971, SEcure Neighbor Discovery(SEND)
http://www.ietf.org/rfc/rfc3971.txt

2006 年　Cisco の無線アクセスポイントに同種の脆弱性が報告される。
http://www.cisco.com/warp/public/707/cisco-sa-20060112-wireless.shtml

30).通常でないパケットへの応答によって OS の種類が特定できる問題 (TCP/IP Stack Fingerprinting）

30)-1. 分類:TCP,IP,ICMP 【IPv4】【IPv6】

30)-2. 概要

特定のパケットを送信することで返される応答パケットを解析し相違点を調べることで、対象ホストの OS の種類を特定されてしまう問題がある。

30)-3. 解説

攻撃手法とその影響

本項では TCP/IP スタックフィンガープリンティング(TCP/IP Stack Fingerprinting)の解説を行うが、基礎知識として OS フィンガープリンティング(OS Fingerprinting)全体から解説を行う。、必要に応じて関連する項目も補足する。

OS Fingerprinting

OS Fingerprinting は、古くから知られているリモートのオペレーティングシステム(以下、OS)を特定する手法のことである。異なる OS 間では、機能やサービスの特長、応答の仕方に違いがあり、そこに着目して対象ホストの OS の種類とバージョンを特定したり、絞り込みを行えたりすることができる。OS Fingerprinting は以下に示すとおり、「能動的」と「受動的」の 2 種類の手法に大きく分類される。

表 30-1 OS Fingerprinting の分類

Active OS Fingerprinting(能動的 OS フィンガープリンティング): 対象ホストに向けて特定のパケットを送信してその応答を解析対象とし、OS を特定する手法。		
	Application Fingerprinting	アプリケーションから得られる情報から OS を特定する手法。TELNET や FTP、HTTP などのサービスにアクセスした際に返されるバナーで判別する手法(Banner Grabbing)や、ポートの開閉状況(port probe)、特定のサービスでの対話的なアプローチによって得られる情報など、アプリケーションから OS 判定に関連する情報は多く存在する。
	TCP/IP Stack Fingerprinting	OS ごとにある TCP/IP スタックの実装の違いに着目し、OS を判定する手法。プローブパケット(probe packet)を送信してその応答を解析、特定のヘッダ値や応答有無の違いから OS を判定する。
Passive OS Fingerprinting(受動的 OS フィンガープリンティング): 対象ホストがネットワーク上に流れるトラフィックをスニファしたものを解析対象とし、OS を判定する手法。現在この手法は攻撃の検出・分析・防御するための機能として IDS やハニーポットシステム、ファイアウォール等で利用されている。		

また、Active OS Fingerprinting と Passive OS Fingerprinting の相違点としては、Active OS Fingerprinting は対象ホストにパケットを送信することが必要になるのに対し、Passive OS Fingerprinting は対象ホストに対して何らかのアクションを何も起こす必要がない点である。ただし、OS 判定における基本的な仕組みは同じである。取得した OS Fingerprint と既知の OS Fingerprint とを照合し、一致するものがあった場合は OS に関する情報を出力するというもので、Nmap(注 1)などの OS フィンガープリントツールのほとんどは照合元となる既知の OS Fingerprint をデータベース化して用意している。このデータの蓄積量と各フィンガープリントの詳細度合いが OS 判定の精度に影響を及ぼす大きな 1 つの要因となっている。

注 1:Nmap は、TCP/IP Stack Fingerprinting による OS 判定機能を備える代表的なネットワーク検査ツールの 1 つである。OS 判定には、照合用データベースとなる 2 つのテキスト形式のファイル(nmap-os-db と nmap-os-fingerprints)が用意されている。ソース stable(安定)版の最新バージョン Nmap 4.20(2007 年 8 月 13 日ダウンロード時点)には、合計で 1900 件以上の様々な OS やデバイス(汎用機、ルータ、スイッチ、ゲーム機など)の OS Fingerprint が蓄積されている。

ここで、主な OS Fingerprinting ツールを以下に示す。

表 30-2 主な OS Fingerprinting ツール

ツール	URL	OS 判別タイプ	使用プロトコル
Queso	http://www.apostols.org/projectz (リンク切れ)	Active	TCP
Nmap	http://insecure.org/nmap/	Active	IP, TCP, UDP, ICMP
Xprobe	http://xprobe.sourceforge.net/	Active	UDP, ICMP
Ring	http://www.planb-security.net/wp/ring.html	Active	TCP
Siphon	http://siphon.datanerds.net/	Passive	TCP, IP
P0f	http://lcamtuf.coredump.cx/p0f.shtml	Passive	TCP, IP
SinFP	http://www.gomor.org/cgi-bin/sinfp.pl	Active / Passive	TCP, IP

TCP/IP Stack Fingerprinting

TCP/IP Stack Fingerprinting の具体的な OS 判定の解説例として、Nmap で使われる Active OS Fingerprinting の手法と攻撃の流れを例として図 25-1 から図 25-4 に示す。

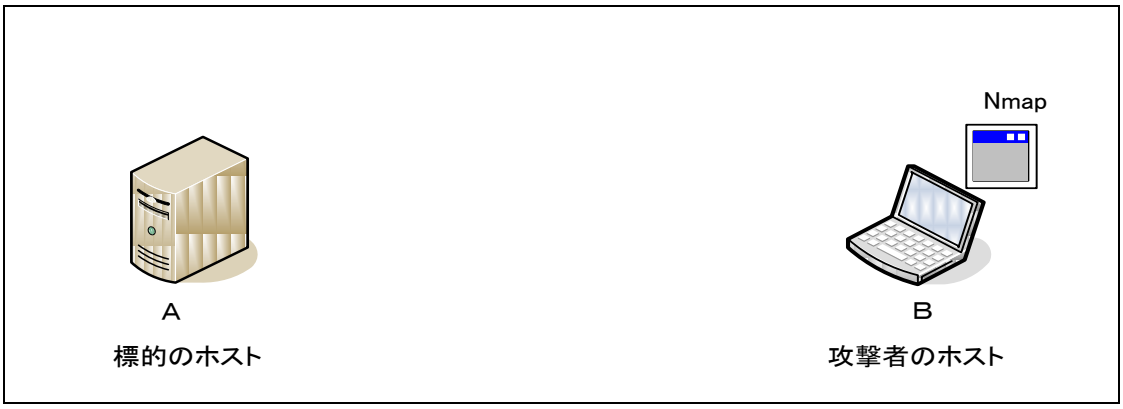


図 30-1 ターゲットホスト

攻撃対象のホスト A の OS を判定するために、攻撃者のホスト B で実行された Nmap は、複数のプローブパケット(最大で 15 個の TCP,UDP,ICMP パケット)をホスト A に送信する。表 30-3 にその主なプローブパケットの種類を示す。(図 25-5、図 25-6、図 25-7 にはパケットの構造を示す。)

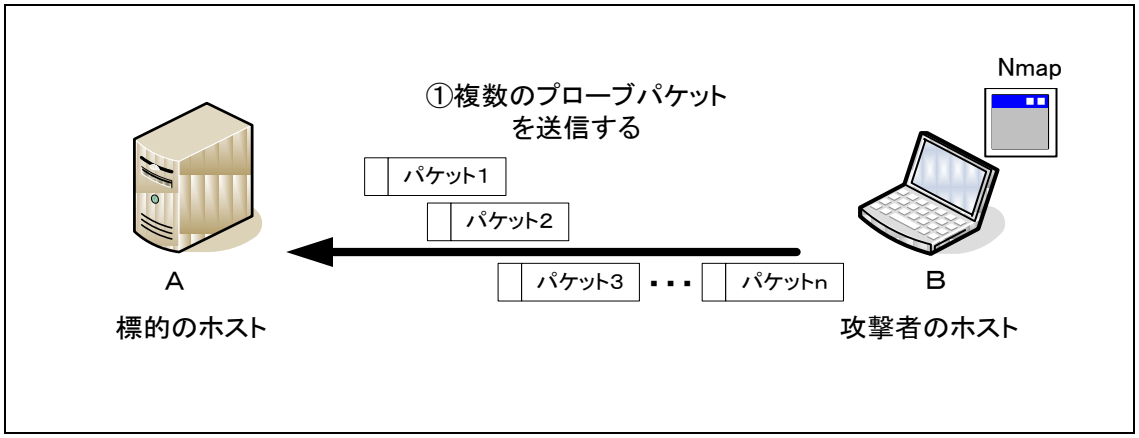


図 30-1 プローブパケットの送信

攻撃者のホスト B 上の Nmap は、プローブパケットを送信した後、攻撃対象のホスト A からの、それぞれのプローブパケットに対する応答パケットを待つ。応答パケットの有無、また返ってきた場合には各プロトコルに応じた特定のヘッダフィールドの値を解析・記録する。

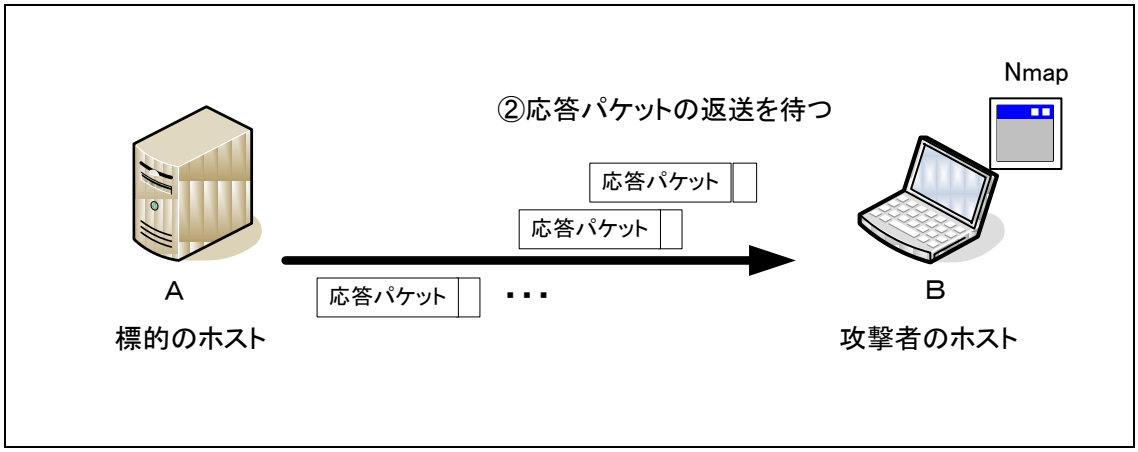


図 30-2 標的ホストからの応答パケットの返送

ここで、攻撃対象のホスト A で動作する OS 次第によって、応答状況に違いが見られる。Nmap はこれに注目し、予め用意されているデータベース化された既知の OS Fingerprint と先ほど解析・記録して得られた情報との照合を行い、OS を判定しその結果を出力する仕組みになっている。(注 2)

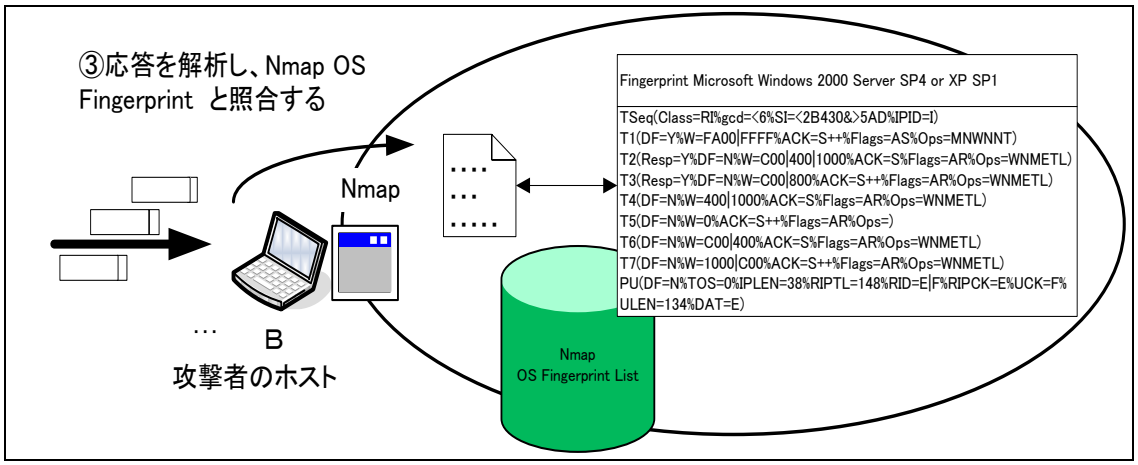


図 30-3 応答パケットと Nmap OS Fingerprint List との照合

注 2:Nmap の詳細については、「TCP/IP Fingerprinting Methods Supported by Nmap」を参照(以下 URL)

http://insecure.org/nmap/osdetect/osdetect-methods.html

表 30-3　Nmap の主なプローブパケットの種類

プローブパケット(注 3)	説明
TCP SYN パケット (SEQ,OPS,WIN, and T1)	TCP オプションや TCP ウインドウフィールドにそれぞれ別の値がセットされた複数の SYN パケットをプローブパケットとして送信し、その応答となる SYN/ACK パケットから得られる複数の情報(応答パケット間のウインドウサイズの違いなど)を OS 判定の材料にする。Nmap では 6 つの異なる SYN パケットをプローブパケットとして利用する。
ICMP Echo リクエスト ￥(IE)	ICMP echo リクエストの特定のフィールドに値をセットしてプローブパケットとして送信する。ICMP echo リプライが返ってくるかどうか、ICMP echo リプライのコード値や、IP ヘッダ中の type of service(TOS)フィールド値などを比較し、OS 判定の材料にする。Nmap では 2 つの異なる ICMP echo リクエストをプローブパケットとして利用する。
TCP ECN(ECN フラグがセットされた SYN パケット) (ECN)	対象ホスト上の TCP スタックが explicit congestion notification(ECN)に対応するかどうかに注目する。ECN フラグ(CWR や ECE フラグを含む)がセットされた SYN パケットをプローブパケットとして対象ホストのオープンポートに対して送信し、その応答となる SYN/ACK パケットの有無や、応答があった場合の time-to-live(TTL)や Don't Fragment(DF)ビットの値、ECN サポートに関するフラグの有無などを比較し、OS 判定の材料にする。
TCP パケット(注 4) (T2-T7)	IP DF ビットのセット有無や TCP ウインドウフィールドの値に違いをつけた、複数の TCP パケット(SYN,ACK,FIN フラグのセット状況もそれぞれ異なる)をプローブパケットとしてオープン・クローズポートに対して送信し、その応答パケットの有無から TCP フラグやオプション、TCP ISN(イニシャルシーケンス番号)、TCP シーケンス番号、TCP Acknowledgment Number(確認応答番号)、RST が返された際のエラーメッセージのデータのチェックサムなどを比較し、OS 判定の材料にする。Nmap では 6 つの異なる TCP パケットをプローブパケットとして利用する。
UDP パケット (U1、PU)	クローズポートに特定の UDP パケットを送信する。完全に対象ホストのポートが閉じている場合には、応答パケットとして ICMP ポート不到達メッセージが返される。この ICMP ポート不到達メッセージのヘッダ部や IP ID 値、IP Total Length 値や IP Checksum 値、メッセージ自体の有無などを比較・確認し、OS 判定の材料にする。

注 3: 各プローブパケットの() 内に示される略語は、照合用データベース(nmap-os-db と nmap-os-fingerprints)内で使用されているものである。2 つの照合用データベース内で利用されるテスト項目もあれば片方でのみ利用されるテスト項目もある

注 4: 6 つの TCP プローブパケットについては図 30-4 を参照

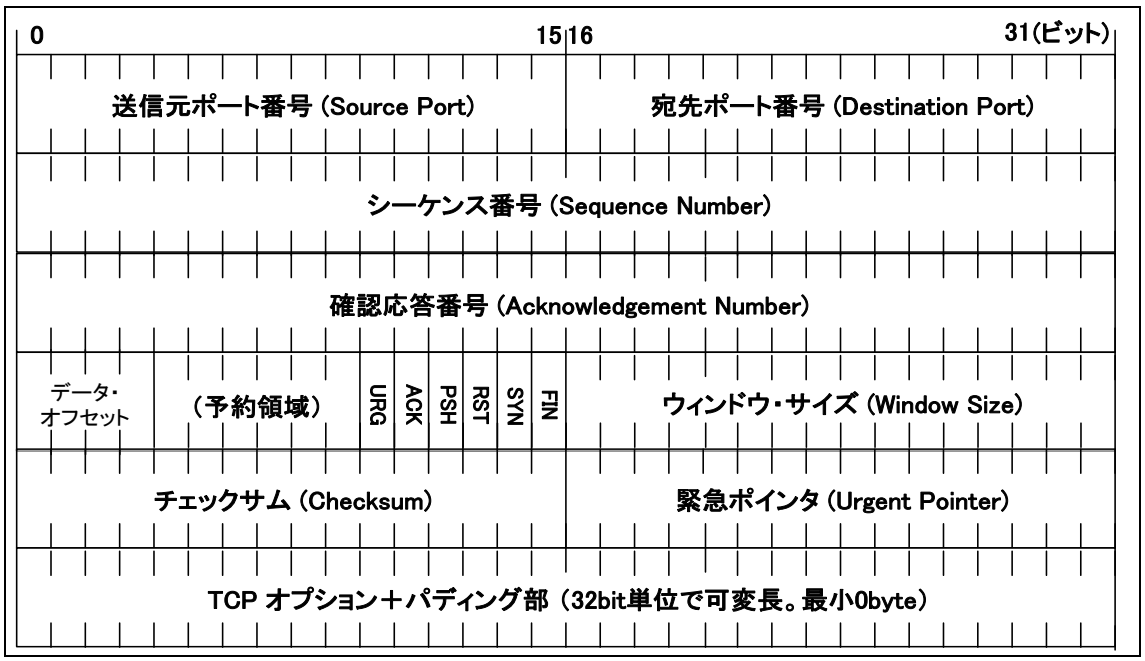


図 30-5 TCP ヘッダ

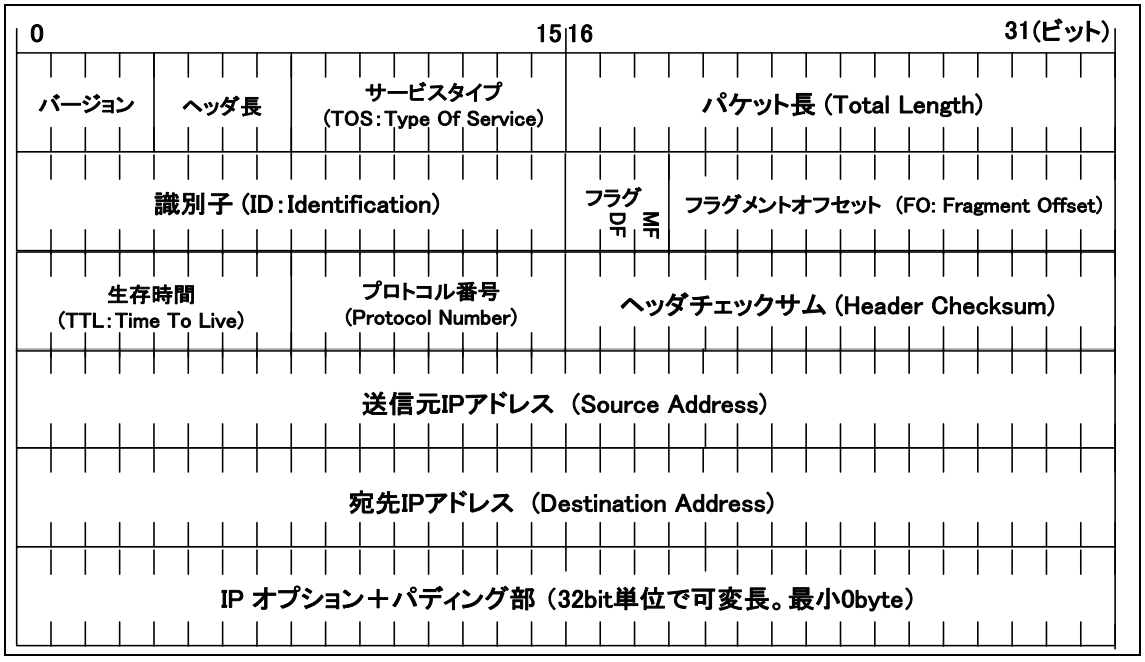


図 30-6 IP ヘッダ

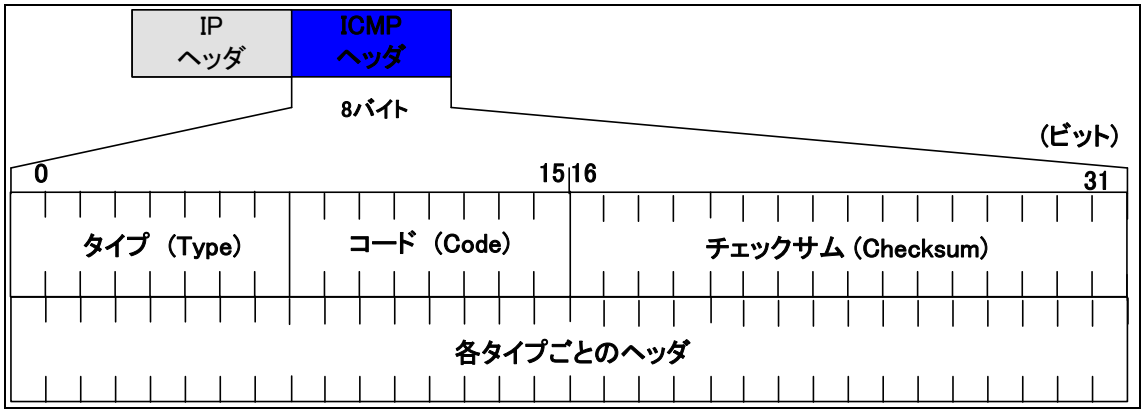


図 30-7 ICMP ヘッダ

プローブパケットの一例として、表 25-3 で紹介した多くの OS Fingerprint で使用される 6 つの TCP パケット(T2-T7)が送信されるイメージ図を以下の図 25-8 に示す。

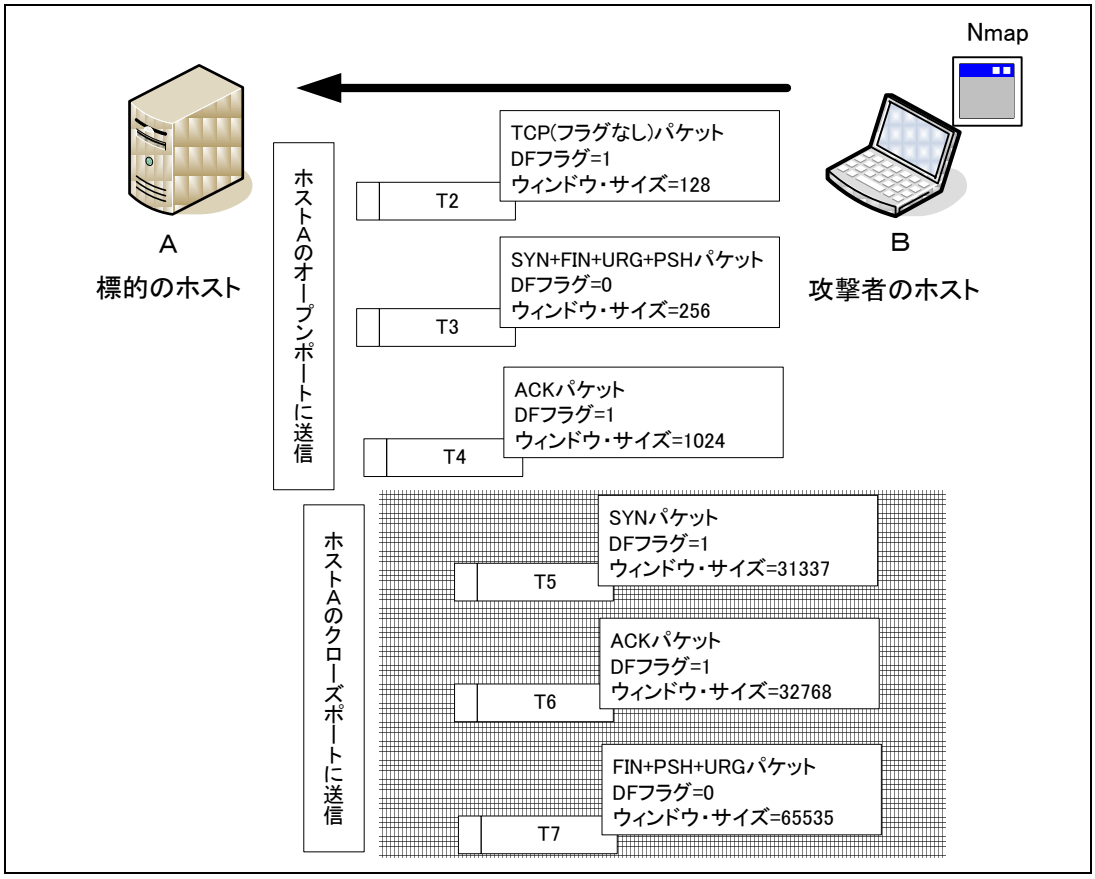


図 30-8 プローブパケットとして送信する 6 つの TCP パケット(T2-T7)

原因と考察

この問題の原因は、各 OS の製品開発ベンダによって使用される TCP/IP スタックの実装に違いがあることに由来する。

情報が公表されにくい部分であるため詳細については不明だが、例えば TCP/IP スタックの開発時において、製品開発ベンダによって RFC の解釈に違いが出たり、十分に RFC に準拠していない部分が開発過程で出てきたりしてしまう結果、TCP/IP の実装が微妙に異なってきてしまい、得られる値(OS Fingerprint)に変化が出るという点が考えられる。また、RFC の要件を満たす製品や同製品であっても、バージョンが異なることで OS Fingerprint に違いが出ているのが現状であり、TCP/IP スタックに直接的に関係しない部分であっても、関連する機能拡張や修正などの処理部分の違いによっても影響があると考えられる。

以上より、各ベンダとも対策が難しい問題であり、この問題による影響と品質面などを考慮するとあまり重要視されていない問題として考えられているようである。

30)-4. 発見の経緯とトピック、対策の動き、現在の動向

Active OS Fingerprinting の手法は、古くから知られているバナーから OS の種類とバージョンを取得するなどの Application Fingerprinting から始まったが、その後 Savage 氏が開発した Queso をはじめとして TCP/IP Stack Fingerprinting の手法をベースにして作られた簡易的なプログラムが幾つか公開されている。これらプログラムはテスト数がとても限られおり、OS バージョンの絞り込みの精度が十分ではなかった。

1998 年になると、Nmap の作者 Fyodor 氏によって「Remote OS detection via TCP/IP Stack FingerPrinting」が公表され、TCP/IP Stack Fingerprinting における多くの OS 判別方法を実装した Nmap がリリースされ、よりOSの判定精度を上げたツールが出た。この頃の Nmap は主に TCP パケットのヘッダフィールドを解析対象としていたが、その後、複数の ICMP パケットの組み合わせを送信することによって、その応答パケットの IP ヘッダを基に OS を判定する Fyodor 氏および Arkin 氏が開発した Xprobe がリリースされている。

2002 年には、新たな TCP/IP Stack Fingerprinting ツール Ring がリリースされた。この Ring は TCP の再送タイムアウト(RTO: Retransmission TimeOut)をベースに OS 判定するツールである。まずオープンポートに対して SYN パケットを送信する。次に、返される SYN/ACK パケットをドロップし、3 ウェイハンドシェイクに必要な最後の ACK パケットを送らない状態にする。SYN Flooding はこの状態を繰り返すために、SYN パケットを大量に送りつけて DoS 攻撃を試みるが、Ring の場合はそれぞれの次に SYN-ACK パケットが再送されるまでの時間に注目するというものである。

一方、Passive Fingerprinting は 2000 年に Lance Spitzner 氏によってその概念が公開されており、Craig Smith 氏が作成した検証用ツール(passfing.tar.gz)と併せて公開されている。この他受動的フィンガープリントツールとしては、subterrain crew が作成した siphon や Michael Zalewski と Bill Stearns 氏によって作成された p0f などがリリースされている。Passive Fingerprinting ツールでは、主に TTL、Window Size、Don't Fragment(DF)ビット、Type of Service(TOS)の値から OS 判定を行う。

また 2005 年には GomoR によって作成された SinFP が登場した。このツールは Active および Passive OS Fingerprinting の両方の機能を持つ。また、ヒューリスティックな解析アルゴリズムを用いることで特定の TCP オプションやウインドウサイズなどの、特定の判別要因に対する追加更新をする必要がなく、また Nmap では障害となり得る PAT/NAT が設定されたファイアウォールなどのデバイスを超えての OS Fingerprint 調査を実現可能にした。

現在では、IDS やハニーポットシステム、ファイアウォール等で広く OS Fingerprinting 技術の応用が行われているが、多くのツールではバージョンアップが行われておらず、既知の OS Fingerprint のデータ更新と蓄積が停止している状態にある。現実的に利用されているツールは Nmap などの一部のツールに限られているようである。

30)-5. IPv6 環境における影響

本問題は IPv6 環境にも影響がある。TCP/IP Stack Fingerprinting ツールである Nmap や SinFP などの一部のツールは既に IPv6 環境に対応している。また、2006 年には eEye Digital Security の研究チームによって、IPv6 環境での ICMPv6 を利用した OS 判定の研究(PacSec 2006 ー「IPv6 マッピング」より)が行われており、今後も IPv6 環境での OS の判別ができる範囲とその精度向上についての動きがあることが予想される。

30)-6. 実装ガイド

本問題は製品開発ベンダ間で TCP/IP スタックの実装に違いがあるために生じている問題であり、TCP/IP スタックの開発方法に違いがある(開発者や工程、考え方)などの、根本部分が問題となっている。そのため、実装上での対策方法は考えにくいが、偽装した OS Fingerprint を返す機構を実装することで OS の判別を誤らせる方法(注 2)がある。またこれをツール化した Morph(注 3)というツールが BSD ライセンスで公開されている。しかし、TCP/IP スタックに対するパフォーマンスや信頼性への影響、ツールの信頼性の欠如は否めないため、実際の製品開発に導入することは現状困難であるといえる。

また、設定変更や修正プログラムの適用、ネットワーク環境などで TCP/IP スタックの振る舞いが変わり、一部のヘッダフィールド値が変わる結果、OS Fingerprint が変わるということもあり、現在の TCP/IP Stack Fingerprinting の手法では攻撃者は OS とそのバージョンを完全に判別することは難しく、製品開発ベンダ各社としても本問題を重要視していないと考えられる。

注 2:2002 年に奈良先端科学技術大学院大学 情報科学研究科の研究チームによって研究・実証が行われている。(「OS Fingerprint 対策手法の実装と評価」より)

注 3:Morph: http://www.synacklabs.net/projects/morph/

30)-7. 運用ガイド

nmap や Xprobe などの TCP/IP Stack Fingerprinting ツールは、ホストやネットワーク環境などで条件が揃った場合でないとOS判定を適切に実行することができない。そのため、完全な対策ではないが返す情報を極力無くしたり偽ったりすることで、本問題を回避することが出来る。

1. 不要なポートは閉じる。
2. ファイアウォール等のフィルタリング機器を導入する。

Active OS Fingerprinting に関しては、プローブパケットをブロックすることでOS判定を防ぐことができる。全てのプローブパケットを防ぐにはフィルタリングのルール作成に時間を要することになるが、オライリーより出版されている「Network Security Hacks」では、OpenBSD などの BSD 系 OS の pf を使用し、TCP フラグの無効な組み合わせに着目をして Nmap が送信する一部のプローブパケットをブロックし不完な OS Fingerprint を提供することで、攻撃者を困惑させる情報を返す方法が示されている。

30)-8. 参考情報

当該脆弱性についての情報を得るにあたって、有益と思われる情報源を以下に列挙する。なお、下記情報は本脆弱性調査時点(2007 年 7 月)のものである。

1981 年 INTERNET CONTROL MESSAGE PROTOCOL(RFC 792)
http://www.ietf.org/rfc/rfc792.txt
http://www.ietf.org/rfc/rfc793.txt

1998 年 Remote OS detection via TCP/IP Stack FingerPrinting(Fyodor 著)
http://insecure.org/nmap/nmap-fingerprinting-article.txt

2000 年 Remote OS detection via TCP/IP Stack FingerPrinting(日本語訳)
http://insecure.org/nmap/nmap-fingerprinting-article-jp.html
Defeating TCP/IP Stack Fingerprinting
http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/smart/smart_html/index.html
Remote Operating System Fingerprinting Library - The libOS Release
(Fred Trotter 著)
http://packetstormsecurity.org/defcon10/dc10-fred-trotter/RemoteOperatingSystemFingerprintingLib.html
X - Remote ICMP based OS Fingerprinting Techniques
(Fyodor Yarochkin, Ofir Arkin 著)
http://www.sys-security.com/archive/papers/X_v1.0.pdf
TCP/IP Stack Fingerprinting Principles(Thomas Glaser 著)
http://www.sans.org/resources/idfaq/tcp_fingerprinting.php
Passive Fingerprinting : IDing remote hosts, without them knowing
(Lance Spitzner 著)
http://www.securityfocus.com/infocus/1224
Passive Host Fingerprinting(Max Vision 著)
http://www.ouah.org/fingerpr.html
What is p0f and what does it do?
http://www.sans.org/resources/idfaq/p0f.php

2001 年 Xprobe Remote ICMP Based OS Fingerprinting Techniques(Ofir Arkin 著)
http://www.blackhat.com/presentations/bh-europe-01/arkin/bh-europe-01-arkin.ppt
ICMP を使って対象サイトの OS を特定する「Xprobe」(ITpro)
http://itpro.nikkeibp.co.jp/members/ITPro/SEC_CHECK/20010921/1/

2002 年 Ring out the old, RING in the New:OS Fingerprinting through RTOs
(Tod Beardsley 著)
http://www.planb-security.net/wp/ring.html
Know Your Enemy: Passive Fingerprinting(日本語訳)
http://www.vogue.is.uec.ac.jp/honeynet/papers/finger.html
奈良先端科学技術大学院大学「OS Fingerprint 対策手法の実装と評価」
http://iplab.naist.jp/~daisu-mi/miyamoto-wit2001.pdf

Xprobe v2.0 A "Fuzzy" Approach to Remote Active Operating System Fingerprinting (Fyodor Yarochkin, Ofir Arkin 著)
http://www.sys-security.com/archive/papers/Xprobe2.pdf

2003 年 Port 0 OS Fingerprinting(Ste Jones 著)
http://www.networkpenetration.com/port0.html
A practical approach for defeating Nmap OS-Fingerprinting
(David Barroso Berrueta 著)
http://www.zog.net/Docs/nmap.html
Analysis of Remote Active Operating System Fingerprinting Tools(Ryan Spangler)
http://www.packetwatch.net/documents/papers/osdetection.pdf
Honeyd A OS Fingerprinting Artifice(2003)
http://citeseer.ist.psu.edu/743374.html
Demystifying Remote Host(Abhisek Datta 著)
http://www.hackinthebox.org/modules.php?op=modload&name=News&file=article&sid=7947&mode=thread&order=0&thold=0
OS Fingerprinting with ICMP
http://www.securitypronews.com/securitypronews-24-20030929OSFingerprintingwithICMP.html

2004 年 The Art of(Application)Fingerprinting
http://www.ccc.de/congress/2004/fahrplan/files/196-the-art-of-fingerprinting-slides.pdf
Frustrating OS Fingerprinting with Morph
http://www.synacklabs.net/projects/morph/Wang-Morph-Notacon2004.pdf
Passive visual fingerprinting of network attack tools
(Gregory Conti, Kulsoom Abdullah 著)
http://portal.acm.org/citation.cfm?id=1029216
Passive OS fingerprinting.(Evgeniy Polyakov 著)
http://tservice.net.ru/~s0mbre/old/?section=projects&item=osf
Passive OS Fingerprinting: Details and Techniques(Toby Miller 著)
http://www.ouah.org/incosfingerp.htm

2005 年 NTP Fingerprinting Utility
http://www.securiteam.com/tools/6F00Q20EKY.html

Reconnaissance and OS Fingerprinting(Suku Nair 著)
http://engr.smu.edu/~nair/courses/8349/reconnaissance.ppt
New OS fingerprinting tool(SinFP)
http://archives.neohapsis.com/archives/sf/pentest/2005-06/0175.html
SinFP - A New Approach to OS Fingerprinting
http://www.securiteam.com/tools/5QP0920IKM.html

2006 年 Remote OS Detection via TCP/IP Fingerprinting(2nd Generation)(Fyodor 著)
http://insecure.org/nmap/osdetect/
Nmap 4.00 with Fyodor
http://www.securityfocus.com/columnists/384/1
Passive OS Fingerprinting With P0f And Ettercap(Video)
http://www.irongeek.com/i.php?page=videos/passive-os-fingerprinting
Nmap vs SinFp
http://www.computerdefense.org/?p=173
PacSec 2006 - IPV6 マッピング(Yuji Ukai,Ryan Permeh,Ryoji Kanai 著)
http://pacsec.jp/psj06/psj06yukai-e.ppt
http://pacsec.jp/psj06/psj06yukai-j.ppt

2007 年 Enhanced Operating System Identification with Nessus
http://blog.tenablesecurity.com/2007/05/enhanced_operat.html

用語集

Access Control(アクセス制御)

情報セキュリティ分野において、ユーザがコンピュータシステムの資源にアクセスすることができる権限・認可をコントロールすることをいい、典型的にはオペレーティングシステムにおいて ACL(Access Control List: アクセスコントロールリスト)として実装される。MAC(Mandatory Access Control)方式、DAC(Discretionary Access Control)方式がある。

また、インターネットセキュリティにおいて、送信元／宛先の IP アドレスとポートに対するパケットの通過の可否をコントロールするリストも ACL(Access Control List: アクセスコントロールリスト)と呼ばれる。また、分散オブジェクト上にも ACL は実装されている。何らかのコンピュータ／ネットワーク資源へのアクセスをコントロールすることを表現する広範な内容を表現するようになってきている。

ACK(ACKnowledgement) パケット

コンピュータ間通信において、送信元ホストから送信されたデータが受信ホストに正常に到達したときに返すパケット。受信に誤りがあった場合に再送処理を行う NACK(Negative ACKnowledgement)や、一部データだけ受け取ったことを示す SACK(Selective ACKnowledgement)という応答信号もある。TCP ヘッダにおいて ACK パケットは制御フラグフィールドの 2 ビット目が 1 であるパケットを示す。

ACL(Access Control List: アクセスコントロールリスト)

「Access Control(アクセス制御)」参照。

ARP(Address Resolution Protocol)

アドレス解決プロトコルという。イーサネット上の機器間の通信では、物理アドレス(MAC アドレス)によって通信が行なわれる。そのため、IP アドレスと MAC アドレスの対応を調べる処理が必要となる。ARP はその際に IP アドレスからイーサネットの物理アドレスを特定するために使用される。一方、物理アドレスを元に IP アドレスを特定するプロトコルは RARP(Reverse ARP)と呼ばれる。

Buffer Overflow(バッファオーバーフロー)

プログラムにおいて入力データや処理の途中で使用する作業用のデータ記憶場所をバッファ領域という。 通常バッファ領域の大きさは、あらかじめ決められた一定量のデータを処理できるように確保し、万が一、一定量を超えるデータがあった場合は、エラーとする。 しかし、一定量のチェックをしていなかったり、チェック方法が間違っていたり等の原因により、バッファ領域の外までデータを記憶してしまうことがあり、これをバッファオーバーフローという。 バッファオーバーフローが発生すると、プログラムの記憶場所や他のデータの記憶場所を書き換えてしまい、プログラムが異常終了したり、

思ってもいない動作をしたりすることになる。このようなセキュリティ脆弱性をもったプログラムを攻略すると、任意のプログラムを、当該プログラムが動作していた権限で動かすことができてしまう。Buffer Overrun と同義語。

CCP(Compression Control Protocol)

PPP 通信に使用されるネットワーク制御プロトコル(NCP)のオプション機能である圧縮制御プロトコルのこと。RFC1962 に規定されている。

CERT(Computer Emergency Response Team)

米国カーネギーメロン大学(CMU)に置かれているコンピュータ緊急対応チーム。インターネットセキュリティに関する技術研究や情報収集・発信、啓蒙活動を行っている。1988 年に組織化され、CERT/CC(Computer Emergency Response Team/Coordination Center)となった。同組織が 2003 年までに発行した CERT Advisory は以下 URL で確認できる。なお、同アドバイザリの情報発信機能は現在米国土安全保障省のコンピュータ緊急対応チーム（US-CERT）に引き継がれている。
http://www.cert.org/advisories/

Exploit コード(Exploit Code)

実証コードとほぼ同義語で使われる。「実証コード(PoC: Proof of Concept)」参照。

FIB(Forwarding Information Base)

パケットを高速に転送するため、必要な情報をツリー状に変換して目的地までの最短経路を選択するために実際のパケット転送判断で使われるテーブル。一般的に RIB(Routing Information Base)と呼ばれる経路情報を基に構築され、宛先プレフィックス、インタフェースや次ホップのアドレスなどの情報で構成されている。

Firewall(ファイアウォール)

特定のネットワークセグメントを他のネットワークとの接続部分において防護するソフトウェアないしハードウェアである。外部のインターネットから内部のイントラネットを防護するのが典型的である。インターネットファイアウォールの場合、通常インターネットサーバーも運用されるので、単純な外部と内部をコントロールする関係にはならない。外部インターネットと内部イントラネットの間に DMZ(スクリーンドサブネット。非武装地帯ともいう。)と呼ばれる境界ネットワークを構築することがある。ファイアウォールの考え方には、このような DMZ の構築も含まれる。

ファイアウォールを実現するための技術には、パケットフィルタリングやアプリケーションゲートウェイ等がある。これらは、組み合わされて実装されることがある。また、ネットワークベース IDS によるミスユース検出、IP マスカレード等の技術も利用されることがある。

GMT(Greenwich Mean Time)

イギリスのロンドンにあるグリニッジ天文台で観測される平均太陽時をもとに決められる時刻である。日本時間は、「GMT+09:00」と表される。以前は GMT が世界標準時刻であったが、現在は UTC が主流である。

ICMP(Internet Control Message Protocol)

TCP/IP プロトコルの機能を補完するためのプロトコル。TCP/IP パケットの転送中に発生した各種エラーの通知や動作確認など、ホストやネットワーク機器間での状態確認を行なうために利用される。

IETF(Internet Engineering Task Force)

インターネット技術の標準化を行う国際組織のこと。技術プロトコル仕様文書のほか情報提供文書は、RFC(Request For Comments) として発行される。セキュリティ分野においてもワーキンググループが複数ある。

IP(Internet Protocol)

インターネットやイントラネットにおいて情報を伝達するために、IP アドレスで定められた受信先に情報を運ぶ役割を担うプロトコル。OSI 参照モデルの第 3 層(ネットワーク層)に相当する。上位のプロトコルである TCP や UDP などとあわせてネットワークを形成する。現在 IP プロトコルのバージョンは IPv4 と IPv6 の 2 つがある。

IPsec(Security Architecture for Internet Protocol)

IP 層(ネットワーク層)の通信における暗号化や改ざん防止など、セキュリティ確保を実現するプロトコルであり、仮想プライベートネットワーク(VPN)のセキュリティ技術として現在では主に利用されている。IPsec では IP パケット単位で暗号化してデータの送受信を行い、TCP や UDP などの上位層のプロトコルを利用するアプリケーションでは、IPsec による暗号通信が行われていることを意識する必要がなくセキュリティの確保が可能になる。IPv4 ではオプションとして IPsec を使用することができるが、IPv6 では標準で実装される。

IPv4(Internet Protocol Version 4)

現在世界中で最も広く普及しているインターネットプロトコル(IP)。「IP(Internet Protocol)」参照。

IPv6(Internet Protocol Version 6)

インターネットの急速な普及に伴い、IPv4 アドレスの枯渇問題が浮上しているが、その解決策として開発された次世代のインターネットプロトコル。IPv4 と比べアドレス空間が拡大されたほか、セキュリティ機能の標準での実装やルータの負荷低下などが図られた仕様となっている。現在では国内をはじめ IPv6 に対応するネットワーク機器やアプリケーション、サービスが増えてきており、今後の普及が期待されている。

IP フラグメンテーション(IP fragmentation)

IP パケットを分割して送信し、受信側でパケットを再構成(reassemble)すること。IP フラグメント(IP fragment)ともいう。IPv4 では、1 つの IP パケットで最大 64K バイトまでのデータを送信することができるが、実際のネットワーク構成(ルータなどの機器や回線設備)のサイズによって一度に送信できるサイズはもっと小さいため、このサイズに収まるようにパケット分割を実行し送信する作業を行う。このサイズを最大転送ユニット(MTU:「MTU(Maximum Transmission Unit)」参照。)といい、ルーティングの経路途中でこの MTU の値が小さいたびにパケット分割を実行し、その次のルータが受け取ったパケットを組み立て直して送信するという作業が繰り返される。一方 IPv6 では、ルータの負荷軽減が考慮されており、ルータによってパケット分割は実行されず、送信元のホストでのみパケット分割が実行される仕組みになっている。

JVN(Japan Vulnerability Notes)

経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」を受けて、日本国内の製品開発者の脆弱性対応状況を公開するサイトとして、有限責任中間法人 JPCERT コーディネーションセンター(JPCERT/CC)と独立行政法人 情報処理推進機構(IPA)が共同で運営するサイト。

Keep-Alive

ネットワーク通信において、通信路やセッションが有効かどうかを確認するために定期的に行われる通信のこと。Keep-Alive は様々なプロトコルで使用されている。TCP の接続では相手のセッション状態が有効か、経路上の異常等で終了していないか確認する方法がないため、通信終了の合図がないと永久にセッションを閉じられなくなってしまう。
接続中に無通信状態が続くと一定時間おきに一定回数の Keep Alive パケットが送信される。双方のセッションが有効であれば ACK パケットで応答を返す。セッションが有効でなければ ACK パケットを返すことができないので、セッション終了とみなし強制的にセッションが切断される。

Kernel(カーネル)

デバイスやディスク、メモリの管理や CPU の制御などを行う OS(オペレーティングシステム)の中核となる部分。

MAC アドレス(Media Access Control address)

コンピュータやネットワーク機器を相互接続するために設定されるハードウェア固有のアドレス。OSI 参照モデルの第 2 層(データリンク層)で利用される。イーサネットでは、全世界で製造されるネットワークインタフェースカード(NIC)1 枚それぞれに対して出荷時に固有のアドレスが設定されている。

Nessus

Tenable Network Security, Inc.が提供する代表的なネットワーク脆弱性スキャナ(脆弱性検査ツール)。バージョン 2 では GPL ライセンスの下で提供されていたが、バージョン 3 から新しいライセンスの下で提供されている。これにより、使い方によっては無償のままで利用できるがソースが非公開となった。ネットワークを介してホストの脆弱性の有無を効果的に確認することができる。
http://www.nessus.org/nessus/

NIST(National Institute of Standards and Technology:米国国立標準技術研究所)

科学技術分野における計測と標準に関する研究を行う米国商務省に属する政府機関。情報技術に関する研究も行われており、その中でコンピュータセキュリティに関して研究を行い情報セキュリティ関連文書も多く発行している。

Nmap

Insecure.Org によってオープンソースで提供されている代表的なネットワーク調査およびセキュリティ監査を行うためのネットワークスキャナ(ネットワーク検査ツール)。高機能なポートスキャナとして知られており、様々な手法でのポートスキャンの他、OS の判定やサービス/アプリケーションのバージョン判定を行うことができる。

OSI 参照モデル

国際標準化機構(ISO)により制定された、異機種間のデータ通信を実現するためのネットワーク構造の設計方針。OSI(Open Systems Interconnection)に基づき、コンピュータなどの通信機器が持つべき機能を 7 つの階層に分割したモデル。上からアプリケーション層、プレゼンテーション層、セッション層、トランスポート層、ネットワーク層、データリンク層、物理層 となる。

Packet Filtering(パケットフィルタリング)

ファイアウォールの一方式で、ゲートウェイホストやチョークルータに実装することができるネットワークアクセス制御技術のひとつ。TCP/IP パケットのヘッダ情報をもとに、当該パケットの通過／却下を制御する。

FTP プロトコルのように、管理プロトコルとデータプロトコルが別のポートを利用するプロトコル等は、1 セッション内で両ポートを相互に関連づけて解釈する必要があるため、 プロトコルのコマンドを理解して制御する機能を備えるようにパケットフィルタリング機能を拡充したものがあり、これは「ダイナミックパケットフィルタリング」と呼ばれている。 これに対して、従前の基本的なパケットフィルタリング機能は、「スタティックパケットフィルタリング」と呼ばれることがある。

Pad オプション(パッドオプション)

用意したデータがある一定の固定長に満たないとき、あるいは短いデータを固定長にするときにゼロを埋め込んでその固定長にすること。パディング、ゼロパディングとも呼ばれる。

Patch(パッチ)

ソフトウェアに見つかった脆弱性を修正するプログラム。「フィックス」と呼ばれることもある。ベンダは、セキュリティ脆弱性の発見に対応して、パッチを提供する。ユーザは、それらをコンピュータ システムにインストールすることで脆弱性を除去できる。

Path MTU Discovery

パケット送信時において、予め経路上の最小 MTU 値を発見し送信時の MTU を最適化してパケット送信すること。この機能により、中継ルータでのパケットの分割を避けることができ、ルータの負荷を軽減させる。現在では多くのオペレーティングシステムにおいて有効化されている機能で、IPv6 の場合ルータでのパケット分割が禁止されているため、ほぼ必須の機能になっている。

Personal Firewall(パーソナルファイアウォール)

エンドユーザが使用するパーソナルコンピュータ上で、ネットワークへのアクセスコントロールを行うソフトウェアは「パーソナルファイアウォール」と呼ばれている。典型的には、パケットフィルタリング機能が実装され、ファイル共有のポートを塞ぐような設定がなされる。

Probe(プローブ、探査)

攻撃・侵入の前段階に行われる標的サイトについての調査。(機種やバージョンの同定等。)

RFC(Request for Comments)

IETF によって公表される、インターネットに関する技術の標準等の検討がまとめられた一連の文書。1969 年に発行が開始されており、インターネット標準の仕様のみならず、現時点における最善の実践(BCP)、FYI(For Your Information)を含む情報提供、実験的なもの、および歴史的なものがあり、広範にわたる。

RH0(Type 0 Routing Headers)

IPv6 における”ルーティングタイプにゼロが指定されたルーティングヘッダ”を指す。”タイプ 0 のルーティングヘッダ(Type 0 Routing Headers)” とも呼ばれ、RFC 5095 では「Type 0 Routing Headers」の略語として RH0 を定義して文書中で利用している。

SEND(SEcure Neighbor Discovery)

SEND は、CGA(Cryptographically Generated Addresses)を用いて IPv6 の近隣探索の様々な機能を安全に実装するための仕組みであり、RFC 3971 に規定されている。(CGA は RFC 3972)近隣探索は非常に便利で高機能である反面、偽ルータや偽ホストを装って ICMPv6 メッセージを利用することで通信妨害、なりすましや盗聴を行うことができてしまい、ローカルネットワークでの問題がある。このような脅威からの保護をするために、SEND はホスト間の公開鍵とそれを使用して生成された IPv6 アドレス、そして RSA 電子署名を使用してのパケット送受信により、パケットの改ざんの検出やアドレス詐称を防止する仕組みとして考えられた。また、電子証明書を使用してのルータとの信頼関係の構築やタイムスタンプを使用しリプレイ攻撃の防止策としても SEND を利用することができ、近隣探索におけるセキュリティ向上を図ることができる。しかし、利用に関する権利上の問題や設定が複雑になるなどの問題から、現在 SEND はまだ普及には至っていないようである。

SYN(SYNchronization) パケット

コンピュータ間通信において、データのやり取りを行うための接続の際に最初に送信されるパケット。TCP 通信におけるセッション確立時に接続要求として SYN パケットが送信される。

TCP(Transmission Control Protocol)

インターネットやイントラネットにおいて情報を伝達するためのプロトコルの 1 つ。情報伝達を確実に行うためにコネクション型通信を行う。ネットワーク層のプロトコルである IP の補完の役割として使われることで TCP/IP ネットワークを形成する。TCP は、OSI 参照モデルの第 4 層(トランスポート層)に相当し、第 5 層以上(セッション層)の上位プロトコル(HTTP、FTP、SMTP など)の橋渡しをする役割を持つ。

TCP/IP スタック

TCP/IP ネットワーク通信を行う際に必要となる通信プロトコルに関するプログラムを階層化してまとめた1つのプログラム群。

UDP(User Datagram Protocol)

TCP と同様にインターネットやイントラネットにおいて情報を伝達するためのプロトコルの 1 つで、ネットワーク層の IP とセッション層以上の上位プロトコル(HTTP、FTP、SMTP など)の橋渡しをする役割を持つ。TCP とは対照的に、コネクションレス(非接続)型の通信方式で再送や送達確認などは行われないため、信頼性がない。しかしその分、TCP と比べ高速通信が可能であり、画像や音声のストリーム配信で利用されることが多い。DNS における名前解決は、やり取りされるデータが小さく高速な処理が求められるため、問い合わせと応答に UDP 通信が一般的に利用される。

uRPF(Unicast Reverse Path Forwarding)

送信元アドレスの偽装を防ぐための機能。ルータが受信したパケットの送信元アドレスを、ルータ自身が保持する経路表から経路として存在するか調べる。経路表から経路情報が見つかればそのまま送信し、見つからなければパケットを削除する。IETF(Internet Engineering Task Force)から推奨されている。

Vulnerability(脆弱性)

システム、ネットワーク、アプリケーション、または関連するプロトコルのセキュリティを損なうような、予定外の望まないイベントにつながる可能性がある弱点の存在、設計もしくは実装のエラー。オペレーティングシステムの脆弱性である場合もあれば、アプリケーションシステムの脆弱性である可能性もある。またソフトウェアの脆弱性以外に、セキュリティ上の設定が不備である状態においても、脆弱性があるといわれることがある。俗に、セキュリティホール(security hole)と呼ばれることもある。

近年ソフトウェアの脆弱性について、広い語感を与える Vulnerability を整理し、予定されたセキュリティ仕様を満たさないものを狭義の Vulnerability とし、仕様上のセキュリティの欠如を Exposure(露出)として区別する動きがある。このほかにも、広義には vulnerability もしくは security hole と呼ばれながらも、ソフトウェア自体の問題ではない論点には、弱いパスワード等の本人認証の回避問題、設定ミスによる問題がある。

エニーキャストアドレス(Anycast Address)

IPv6 において複数のインタフェースに同じグローバルユニキャストアドレス(IPv4 のグローバルアドレスと同等)を割り当てて一つのアドレスを共有して利用するアドレス。このエニーキャストの仕組みにより、送信元から最も近いインタフェースと通信が行われることになり、負荷分散と冗長化を実現するためにこのアドレスが使われる。

オクテット(octet)

情報通信の分野で使われる、8 ビットの情報を表す情報量の単位。

近隣キャッシュ(Neighbor Cache)

近隣ノードの IP アドレスと MAC アドレスの対応表である。最近通信した近隣ノードの情報を保有している。IPv4 の ARP キャッシュに相当するものであり、RFC2461 にて規定されている。

近隣探索(ND: Neighbor Discovery)

近隣探索は、IPv6 の根幹であり必須である 5 つの ICMPv6 メッセージ(ルータ要請、ルータ広告、近隣要請、近隣広告、リダイレクト)を利用し、同一リンク内で IPv6 パケットを送信するために必要な機能を提供する。IPv4 における ARP や ICMP ルータ探索、ICMP リダイレクトに相当する機能を実現し、さらに IPv4 では提供されていなかった追加機能を備えている。

最大転送ユニット(MTU: Maximum Transmission Unit)

1 つの IP パケットで送信できるデータの最大値。

サービス妨害攻撃(DoS attack: Denial of Service attack)

コンピュータ資源やネットワーク資源が、本来のサービスを提供できない状態に陥れる攻撃。例えば、インターネットサーバーによって提供されている各種サービスを標的として妨害する攻撃が、一般に入手可能なツールを利用して行われている。このような DoS 攻撃には、 次の種類がある。:

- インターネットプロトコルの特性を悪用して、ネットワークに接続されたコンピュータに過剰な負荷をかけ、サービスを提供することをできなくする攻撃。(SYN フラッド攻撃)等。
- ネットワークの帯域を渋滞させる攻撃: Smurf attack(Smurf 攻撃)等。
- サーバーアプリケーションの脆弱性を悪用し、アプリケーションに例外エラーの処理を発生させてサービスを提供することをできなくする攻撃

参考:CERT アドバイザリ(English) CA-1996-01, CA-1998-01, CA-1999-17, CA-2000-01, CA-2000-21

実証コード(PoC: Proof of Concept)

ソフトウェア等の脆弱性を利用して問題の再現性の確認、攻撃が可能であることを実証するプログラム。研究材料や脆弱性が修正されたかどうかを確認・検証するプログラムとして使用される。検証用に作られたコードではあるが、容易に悪意あるプログラムを作成されてしまう。

侵入検知システム(IDS: Intrusion Detection System)

システムに対する侵入/侵害を検出・通知するシステム。 システムを監視し、セキュリティポリシーを侵害するような行為を検出した場合に、その行為を可能な限り早く管理者に伝えるとともに、調査分析の作業を支援するために必要な情報を保存・提供することが目的である。

IDS は大きくネットワークベース IDS と、ホストベース IDS に分類されることがある。その分類法は、検査対象がネットワークパケットの情報かホスト内で生成する情報かによる場合がある。

IDS の機能を拡張し、侵入を検知したら接続の遮断などのリアルタイム防御を行なうものを侵入防止システム(IPS: Intrusion Prevention System)と呼ばれる。

セキュリティパッチ

「Patch(パッチ)」参照。

脱カプセル化(Decapsulation)

ある方式の通信パケットを他の方式の通信パケット内に包んで送信することをカプセル化といい、受信側で再びカプセルから取り出すように元のパケットを取り出し、組み立て直すことを脱カプセル化という。IPv4－IPv6 間でのトンネリングや VPN などの技術で利用されている。

転送制御ブロック(TCB:Transmission Control Block)

TCP の実装において、TCP 接続の状態を保持するために利用される内部データ構造のこと。遷移状態、タイマ、ウインドウサイズ、送受信シーケンス番号、セッションの優先度等、TCP 制御に関する情報が格納される。

ノード(Node)

ネットワークを構成するホスト、ルータやハブなどのネットワーク機器のこと。

パケット(Packet)

コンピュータ通信において、ヘッダ(送信先アドレスやパケットの種類などの制御情報)を付加したデータの最小単位。

ファームウェア(Firmware)

ルータやスイッチなどのハードウェアに組み込まれた基本的な制御を行なうためのソフトウェア。ハードウェアとソフトウェアの中間に位置するものであるため、こう呼ばれている。

フィルタリング(Filtering)

(情報を)選別、遮断すること。ルータやファイアウォールが持つフィルタリング機能は、基本機能の一つであり、パケット配送を検査して通過を許可するかを判断する役割を持つ。

フィールド(Fields)

例えば TCP ヘッダや IP ヘッダの構造などを示すときに利用する場合、あるヘッダの内側の部分示し、ヘッダを構成する各要素、という意味で使われる。

フィンガープリント(Fingerprint)

「指紋」または「拇印」というという意味で、証明書などが改ざんされていないことを証明するデータ(ハッシュ値)のことを指す。OS フィンガープリントとは、OS のフィンガープリント(指紋)という意味で、OS を特定するための特徴があるデータのことを指す。

輻輳(ふくそう)

物が一箇所に集まるという意味。TCP においてはネットワークが通信過多の状態を意味する。輻輳の状態にならないよう通信を制御することを輻輳制御という。

ブロードキャスト(Broadcast)

同一ネットワーク上の全てのノード(不特定多数のノード)に対してデータを送信すること。IPv4 では、ブロードキャストアドレスという特殊なアドレスに対してデータを送信することで、全ノードに対してデータ送信が行われる。IPv6 については、「リンクローカル・オールノードマルチキャストアドレス(Link-local All Node Multicast Address)」参照。

分散型サービス妨害攻撃(DDoS attack: Distributed Denial of Service attack)

インターネットプロトコルの特性を攻略して、ネットワークに接続されたコンピュータに過剰な負荷をかけて、サービスを提供することをできなくしてしまう種類の攻撃がある。このような DoS 攻撃の攻撃元が複数で、標的とされたコンピュータがひとつであった場合、その標的とされるコンピュータにかけられる負荷は、より大きなものになる。このような攻撃が DDoS(Distributed Denial of Service:分散型サービス妨害)攻撃と呼ばれている。攻撃元は、攻撃者(人間)自身であるとは限らない。むしろ、攻撃者が事前に標的以外の複数サイトに、攻撃プログラムを仕掛けておいて、遠隔から の操作をきっかけとして一斉に DoS 攻撃をしかける手法の方が広く知られている。

ペイロード(Payload)

通信パケットにおけるヘッダ部分(制御情報)を除いたデータ本体の部分を指す。ペイロード部分のデータの大きさのことをペイロード長(Payload length)という。

ヘッダ(Header)

データ本体の先頭に付加される、データ本体に関する制御情報。通信パケットにおいては、付加されているヘッダには、宛先アドレスや送信先アドレス、パケットの種類などのパケット送受信において重要となるデータが含まれている。

マルチキャスト

同一ネットワーク上の複数の指定したノードに対して同じデータを送信すること。パケットを送る際に、経路上でルータがデータをコピーするので、効率的にパケットを送信できる。

ユニキャスト(Unicast)

ネットワーク内において、単一のノードを指定してデータを送信すること。複数のノードを指定してデータを送信するマルチキャスト、特定多数の相手にデータを送信するブロードキャストなどの対比の用語。

リンク(Link)

OSI 参照モデルの第 2 層(データリンク層)を通じてノード同士が直接通信できるメディアや通信装置のこと。同一リンク上のノード同士は直接通信を行う。

リンクローカル・オールノードマルチキャストアドレス(Link-local All Node Multicast Address)

IPv6 において永久的に割り当てられるリンクローカルアドレス(特定のリンク内でのみ有効なアドレス)をアドレスの有効範囲(スコープ)とする、全ノード宛のマルチキャスト IPv6 アドレス(FF02:0:0:0:0:0:0:1 あるいは FF02::1 と表記)のこと。IPv4 のブロードキャストアドレスに相当するアドレスであり、同一リンク内の全ノードへのデータ送信に利用される。

TCP/IP に係る既知の脆弱性に関する調査報告書

－ インターネットの標準的な通信手順に知られているセキュリティ上の弱点箇所に関する解説書 －

［発　　行］ ２００６年　５月３０日 第１版
２００７年　４月１２日 改訂第２版 第１刷
２００７年　５月２４日 改訂第２版 第２刷
２００８年　１月　８日 改訂第３版
２００９年　１月　８日 改訂第４版
２０１０年　１１月１日 改訂第５版
独立行政法人 情報処理推進機構 セキュリティセンター
［執　　筆］ 株式会社ラック
［協　　力］ 株式会社インターネットイニシアティブ(IIJ)
一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)
日本電気株式会社
パナソニックコミュニケーションズ株式会社
株式会社 日立製作所
富士通株式会社
パナソニック株式会社
ヤマハ株式会社

情報セキュリティに関する届出について

IPA セキュリティセンターでは、経済産業省の告示に基づき、コンピュータウイルス・不正アクセス・脆弱性関連情報に関する発見・被害の届出を受け付けています。

ウェブフォームやメールで届出ができます。詳しくは下記のサイトを御覧ください。
URL: http://www.ipa.go.jp/security/todoke/

コンピュータウイルス情報

コンピュータウイルスを発見、またはコンピュータウイルスに感染した場合に届け出てください。

不正アクセス情報

ネットワーク(インターネット、LAN、WAN、パソコン通信など)に接続されたコンピュータへの不正アクセスによる被害を受けた場合に届け出てください。

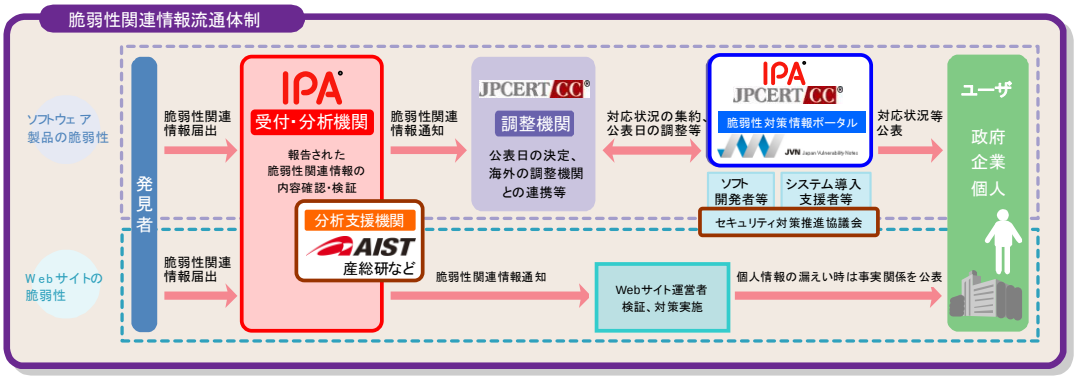
ソフトウエア製品脆弱性関連情報

OSやブラウザ等のクライアント上のソフトウエア、ウェブサーバ等のサーバ上のソフトウエア、プリンタやICカード等のソフトウエアを組み込んだハードウエア等に対する脆弱性を発見した場合に届け出てください。

ウェブアプリケーション脆弱性関連情報

インターネットのウェブサイトなどで、公衆に向けて提供するそのサイト固有のサービスを構成するシステムに対する脆弱性を発見した場合に届け出てください。

脆弱性関連情報流通の基本枠組み「情報セキュリティ早期警戒パートナーシップ」



※JPCERT/CC：有限責任中間法人 JPCERT コーディネーションセンター、産総研：独立行政法人 産業技術総合研究所

独立行政法人 情報処理推進機構
〒113-6591
東京都文京区本駒込二丁目28番8号
文京グリーンコートセンターオフィス16階
http://www.ipa.go.jp

セキュリティセンター
TEL: 03-5978-7527 FAX 03-5978-7518
http://www.ipa.go.jp/security/