コンピュータセキュリティ　6－5
（1999．7．9）

不正なTCPコネクション確立に関する一考察

寺田真敏†　甲斐　賢†　熊谷仁志‡
†(株)日立製作所システム開発研究所　‡日立ソフトウェアエンジニアリング(株)

要旨

不正アクセスによって引き起こされる情報システムへの被害は多大なものであるため、不正アクセス（データ破壊、改ざん、侵入、システム自身の稼動停止）の対策が重要な課題となってきている。しかし、不正アクセスは、目に見えにくいものであり、定量的なデータが少ないためにセキュリティ対策を進めていく上で、脅威度分析、被害や対策コスト計算をしにくいものとなっている。本稿では、「不正アクセス自体がどの程度起こりやすいものなのか？」ということを定量的な情報として提示することを目的として、限られた条件下ではあるが、TCPコネクションの偽造を対象とした実験を行うと共に、コネクション確立の成功度やパケットキャプチャ数での定量化の可能性を示す。

Study of TCP spoofing connection establishment

Masato Terada†　Kai Satoshi†　Hitoshi Kumagai‡
†System Development Laboratory, Hitachi Ltd.
‡Hitachi Software Engineering Co., Ltd.

Abstract

Because unauthorized access causes a lot of damage to the information system, the countermeasure against the unauthorized access (data destruction, alteration, invasion, system's own suspension of operation) has been being an important subject. But unauthorized access can be hard to be seen in the eyes and there are a few quantitative data. So it is hard to wear the menace occasion analysis, the damage estimate, and the countermeasure cost calculation when proceeding with the security countermeasure. The purpose of this study is presenting a quantitative information such as "How much does unauthorized access itself happen easily?" It is reported because an experiment targeting the forgery of the TCP connection was done though it is under the condition limited.

1. 緒言

近年、ネットワーク環境においては、計算機資源への不正アクセス（データ破壊、改ざん、侵入、システム自身の稼動停止）の問題が重要になってきている。特にインターネットの普及により、遠隔からネットワークを経由して攻撃対象となる計算機への侵入や停止を目的とする不正アクセスが増えている。不正アクセスの手法としては、

- パスワードを強制的に解析するパスワードクラッキング
- ネットワーク上を流れるデータを盗聴するパケットスニファリング
- 計算機上で稼動しているサービスやサービ

ス上の弱点を探しだすスキャンニング
- プログラムに過大な負荷を掛けたり、異常終了させるサービス提供不能攻撃
- IP アドレス、電子メールアドレスの送信元を偽るなりすまし

など様々な手法がある。また、不正アクセスによって引き起こされるコンピュータ、データとネットワークへの被害は多大なものであるため、これらの不正アクセスから計算機を守ることは重要な課題である。しかし、不正アクセスは、目に見えにくいものであると共に、「不正アクセス自体がどの程度起こりやすいものなのか？」「対策や被害発生後の回復にどのくらいの工数がかかるものなのか？」など定量的なデータが少ないためにセキュリティ対策を進めていく上で、脅威度分析、被害や対策コスト計算をしにくいものとなっている。

本稿では、まず「不正アクセス自体がどの程度起こりやすいものなのか？」ということを定量的な情報として提示することを目的として、限られた条件下ではあるが、TCP コネクションの偽造を対象とした実験に基づく検討結果を報告する。

2. TCP コネクションの偽造に関する研究と不正アクセス

2.1 TCP コネクションの偽造

TCP の実装に伴う脆弱性については、1985 年 Robert T. Morris が「4.2BSD Unix では TCP コネクションの初期シーケンス番号の類推が可能である」と報告している。また、TCP/IP 環境における脆弱性については、Steve Bellovin が「TCP コネクションのシーケンス番号の推測、ルーティング上の問題、アプリケーション(Finger, SMTP, FTP, SNMP など)の問題」を報告している[1][2]。

特に、TCP の実装に伴う脆弱性については、1995 年 Kevin Mitnick によって、この脆弱性を利用した不正アクセスの試みが行われたことは記憶に新しい[3]。Kevin Mitnick が利用した手法は、図 2.1に示すように、
- ターゲット計算機と通信を通して、TCP コネクションの初期シーケンス番号の推測を行う。
- 負荷を増大させるデータや、ネットワーク応答性を阻害するデータを送付することにより、正規の計算機をサービス提供不能(DoS: Denial of Service)状態に陥れる。
- 偽造 TCP/IP パケットを用いて TCP コネクションを仮想的に確立する。

というものである。

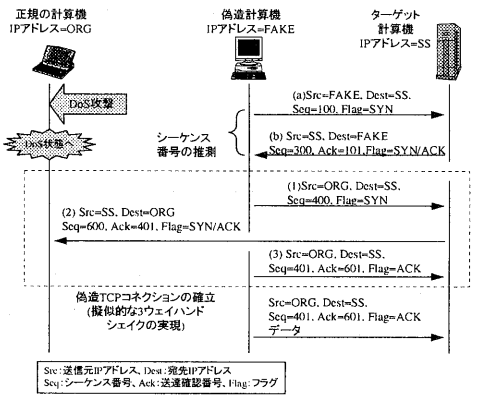


図 2.1 シーケンス番号推測による擬似 TCP コネクションの確立

また、最近の CERT/CC の不正アクセスの動向報告によれば、偽造 IP アドレスとパケットスニファリング技術を利用した TCP コネクションの偽造により、セキュリティ脆弱性探査も行われていると報告されている[4]。

2.2 脆弱性に関する指標

現在、不正アクセス対策においては、不正アクセスの要因となる脆弱性(セキュリティホール)を、危険度とか、リスクと呼ぶ「その問題の相対的な深刻さ」を表す定性的基準を利用して表現している場合が多い(表 2.1)。

このような定性的基準を用いている理由と

しては、脆弱性の引き起こす被害が、システム構成、運用形態(特に対象となる計算機の位置づけ)などにより大きく変わるため、一意の定量的なデータとして提示しにくいことがあげられる。

しかし、不正アクセス対策においては、脆弱性に関する基準は、定量情報の方が望ましい。そこで、TCP コネクションの偽造を対象に、まずは、「不正アクセス自体がどの程度起こりやすいものなのか？」の定量化の可能性を実験を基に調査、検討した。

表 2.1 脆弱性に関する指標の例

危険度/リスク	ケース 1 (A 社の場合)	ケース 2 (F 政府組織の場合)
高	管理者権限を不正取得できる。管理者権限でプログラムを起動できる。システムファイルを操作できる。	管理者(sysadmin, root)権限を不正取得できる(例：リモートから不正アクセスにより、計算機のコマンドプロンプトを利用することができるなど)。
中	DoS 攻撃などのサービス妨害や、管理者以外のユーザ権限を不正取得できる。	管理者以外のユーザ権限を不正取得できる(設定ミスにより、パスワードファイルを取得できるなど)。
低	ローカルのハードディスクの内容やブラウザのクッキーなどを不正に取得される。	DoS 攻撃などのサービス妨害

3. 実験概要

本章では、TCP コネクションの偽造に関する実験の概要について述べる。

3.1 TCP コネクションの偽造

実験においては、「TCP コネクションの偽造だけで、対象とする計算機からどれだけの情報を引き出せるのか？」を定量的に示すために、以下のような前提条件を設定した。

(1) 正規の計算機をサービス提供不能(DoS: Denial of Service)状態に陥れることはしない。

(2) 図 3.1に示すように、偽造 IP アドレスとパケットキャプチャ技術を利用した TCP コネクションの偽造を行う(初期シーケンス番号の類推による TCP コネクションの偽造は行わない)。

なお、前提条件(2)により、常に、偽造計算機を正規の計算機とターゲット計算機の通信データが通過するネットワーク上に設置し、さらに、その通過データをキャプチャできなければならないが、対象とする計算機から確実に情報引き出しを行うことができるため、この前提条件を設定することとした。

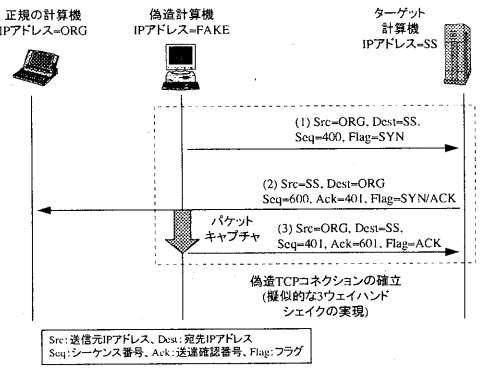


図 3.1 実験で使用した偽造 TCP コネクションの形態

3.2 TCP コネクション利用可能時間

TCP のデータ転送制御では、不当な TCP パケットを受信した場合、この不当なパケットに関連する TCP コネクションを無効とするためのリセット(RST)パケットを送付することとなっている。

このため、前提条件(1)により、偽造計算機が利用可能な TCP コネクションの時間は、正規の計算機の送信する RST パケットがターゲット計算機に到着するまでの時間となる(図 3.2)。すなわち、

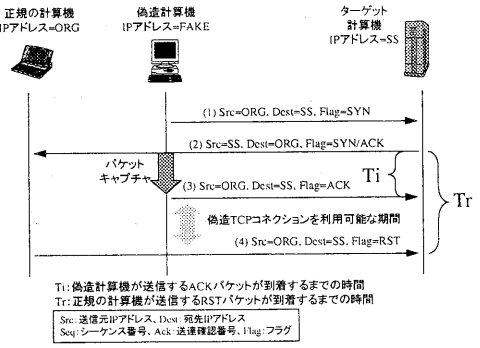
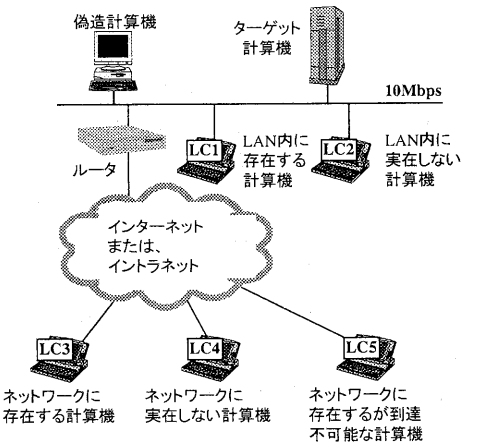


図 3.2 TCP コネクション利用可能時間

TCP コネクション利用可能時間
=(Tr：正規の計算機の送信する RST パケットが到着するまでの時間)−(Ti：偽造計算機の送信する ACK パケットが到着するまでの時間)

となり、この時間差が大きいほど、偽造計算機は、ターゲット計算機との間で多くのデータ交換を行うことが可能となる。

また、この TCP コネクション利用可能時間は、ネットワーク構成 (計算機のネットワーク上の配置)の影響を受けることとなるため、図3.3に示すような実験構成をとることとした。なお、図中の LC＊は、模擬する正規の計算機を示している。



項番	トポロジ	経由ルータ数	ping応答時間
LC1	LAN内の既存マシンを模擬	0	8.9ms
LC2	LAN内の実在しないマシンを模擬	0	応答なし
LC3	LAN外の既存マシンを模擬	14	56.6ms
LC4	LAN外の実在しないマシン模擬	10以上	応答なし
LC5	LAN外のホスト（ネットワーク）到達不可能のマシンを模擬	5	ICMPエラー[*]

ping 応答時間：ターゲット計算機から正規の計算機への ping 応答平均時間
通過ルータ数：ターゲット計算機から正規の計算機間に存在するルータ数
[*] ICMP Destination Unreachable エラー

図 3.3 実験構成

3.3 測定内容

偽造計算機として、UNIX[1]を搭載した PC を使用し、実験用にパケットキャプチャ機能とパケット送信機能を備えたツールを作成した。

測定内容は、以下の通りである。

- 偽造 TCP コネクション確立の成功度
- 偽造 TCP コネクションを利用した HTTP アクセスに伴う取得可能データ量

4. 実験結果

(1) 偽造 TCP コネクション確立の成功度

偽造計算機の送信する ACK パケットが到着するまでの時間 (Ti) は平均すると約 46ms である。この時間は、偽造計算機上でのツール処理時間 (ターゲット計算機の送信する SYN + ACK パケットをキャプチャしてから ACK パケットを送信するまでの時間)にほぼ等しい。このため、表 4.1に示すように、前提条件(1)の下では、同一 LAN 上にいる計算機を模擬することはほとんど不可能であった。一方、ping 応答時間とツール内部処理時間がほぼ等しいネットワークに設置された計算機 LC3 を模擬する場合、3 割前後の確率で偽造 TCP コネクションを確立することができた。また、同一 LAN 以外の実在しない計算機 LC4, LC5 を模擬

[1] UNIX は、X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。

するのであれば、100%確実に偽造 TCP コネクションを確立することができることが分かった。

表 4.1　偽造 TCP コネクション確立の成功度

項番	Ti 平均値	Tr 平均値	成功確率
LC1	47.2ms	0.9ms	0%
LC2	——	——	0%
LC3	43.7ms	41.8ms	36%
LC4	50.6ms	——	100%
LC5	42.3ms	——	100%

Ti：偽造計算機が送信するACKパケットが
　到着するまでの時間
Tr：正規の計算機が送信する RST パケットが
　到着するまでの時間
成功確率：偽造 TCP コネクション確立の実現確率

(2) 偽造 TCP コネクションを利用した HTTP アクセス

偽造 TCP コネクションを利用して HTTP アクセスを行った結果、ping 応答時間とツール内部処理時間がほぼ等しいネットワークに設置された計算機 LC3 を模擬した場合、1 パケット(約 1.5KB)分の Web データを収集することができた。また、同一 LAN 以外の実在しない計算機 LC4, LC5 を模擬するのであれば、アクセスしたページの全てのデータを取得することができる。

表 4.2　実験結果 (HTTP サーバアクセス)

項番	キャプチャパケット数 (取得情報サイズの割合 *)	HTTP アクセスログ
LC1	0 個 (0%)	記録なし
LC2	0 個 (0%)	同上
LC3	1.0 個 (25%)	記録あり
LC4	4.5 個 (100%)	同上
LC4	4.2 個 (100%)	同上

キャプチャパケット数：偽造計算機でキャプチャできた
　パケット数
HTTP アクセスログ：ターゲット計算機上の HTTP アクセス
　ログへの偽造 IP アドレス記録の有無
*) アクセスページのサイズ(6KB)に対して取得することの
　できたページサイズの割合

(3) 考察

実験により、限られた条件下ではあるが、TCP コネクション偽造を対象とした不正アクセスの実現性を定量的に示した。

まず、偽造 TCP コネクションに関する、その影響度をわかりやすく表現するために、インターネット上での ping の応答時間を指標として提示する。表 4.3は、都内にある ISP で実測した ping 応答時間である。実験と同じ環境をインターネット上に構築することができるならば、50ms を越える ping 応答時間のサイトに対しては、3 割前後の確率で偽造 TCP コネクションを確立することができると思われる。

表 4.3　ping 応答時間の実測値

対象ホスト	応答性能(ms)
ISP 内	2
東京	11
大阪	27
広島	37
宮城	**50**
北海道	**50**
沖縄	**100**
米国	**110 (日本-米国間で 100ミリ秒)**

注) ping 応答時間は、都内の ISP から上記地域に置かれた特定の計算機に対しての実測値である。従って、上記地域に置かれた全計算機との応答時間を保証するものではない。

次に、アプリケーションから見た偽造 TCP コネクションの利用しやすさを提示する。表 4.4は、代表的なインターネットアプリケーションプロトコルが、データ転送(本文となるデータ参照・書込み)までに必要とする処理をまとめたものである。HTTP では、TCP コネクション確立後にデータ転送フェーズに入れるため、偽造 TCP コネクションを利用しやすいプロトコルの 1 つであると言える。その他のプロトコルでは、データ転送処理までに何ステップかの処理を必要とする分、偽造 TCP コネクションを利用しにくい。

特に認証処理は、リプレイ攻撃による不正を回避できるのであれば、以下の偽造 TCP コネクションを利用した不正を防ぐ手法として有効であると思われる。

- 実在しない計算機を模擬する。
- サービス提供不能にある計算機を模擬する。

表 4.4　プロトコル処理の概要

サービス名	TCP コネクション確立後の データ転送までの処理
HTTP	**データ転送**
SMTP	SMTP 通信開始処理(送受信先指定など) データ転送
NNTP	NNTP 通信開始処理(グループ選択など) データ転送
rsh	エラー用ポート番号通知 ユーザ名/コマンド 入出力/エラー用のコネクション接続 データ転送
TELNET	TELNET のオプション折衝 ユーザ名/パスワード データ転送
FTP	ユーザ名/パスワード データ転送用の TCP コネクション接続 データ転送
POP	ユーザ名/パスワード データ転送

5. 結論および今後の課題

本稿では、限られた条件下ではあるが、TCP コネクションの偽造を対象とした「不正アクセス自体がどの程度起こりやすいものなのか？」ということを偽造 TCP コネクション確立の成功度やパケットキャプチャ数を用いることにより定量化できることを示した。不正アクセスは、目に見えにくいものであるため、従来の危険度のような定性的基準だけではなく、このような定量的な情報を提示することで、その危険度を認識してもらうことがより効果的、効率的対策を立てる上で必要であると考えている。

一方、不正アクセス対策においては、情報提供方法(内容、表現方法など)も重要な課題の 1 つであると認識している。そこで、今後は、不正アクセスに関する分析や評価のための定量的なデータ収集、効率的・効果的対策の研究と合わせ、不正アクセスの危険性を一般利用者にも理解してもらえるような情報提供の検討も進めていく。

参考文献

1) Morris, R.T. : "A Weakness in the 4.2BSD UNIX TCP/IP Software",. Computing Science Technical Report No. 117, AT&T Bell Laboratories, Murray Hill, New Jersey (1985), ftp://ftp.research.att.com:/dist/internet_security/117.ps.Z

2) Steve Bellovin : “Security Problems in the TCP/IP Protocol Suite”, Computer Communication Review vol. 19, no. 2 (April 1989) pages 32-48, ftp://ftp.research.att.com:/dist/internet_security/ipext.ps.Z

3) http://www.cert.org/advisories/CA-95.01.IP.spoofing.attacks.and.hijacked.terminal.connections.html

4) “Probes with Spoofed IP Addresses”, http://www.cert.org/incident_notes/IN-98-05.html