ネットワーク部会研究（3）

新潟県立看護大学における Linux・Apache における不法アクセスの監視

橋本明浩
新潟県立看護大学（情報科学）

A study on Statistical Access Check and Monitoring of Web Server

Akihiro Hashimoto
Niigata College of Nursing (Information Science)

キーワード：　リナックス（Linux）アパッチ（Apache）監視（monitoring）

要旨
Linux 上の Apache の稼動集計を元に統計的解析をおこない不法アクセスを監視できることを示す.

はじめに

WWW のサーバとして Microsoft 社の提供する IIS（Internet Information System）以上に広く使用されているプログラムに Apache(アパッチ)がある．Apache は無料で提供されているおり，高い機能を備えている．稼動の OS も Windows，Mac OS，Linux，Solaris 等と幅広く，セキュリティ面でも高く評価されている優れたソフトウェアである．加えて，利用の説明等も（http://www.apache.jp/）完備しているので，簡単に WWW サーバとしての利用が可能である．本報告では，Linux で稼動している本学の Apache でのアクセスの監視の報告をおこない，簡単なアクセス統計からの考察を行う．図 1 図 2 図 3 に本学サーバ装置を示す（写真提供 信越情報システム　平井氏）

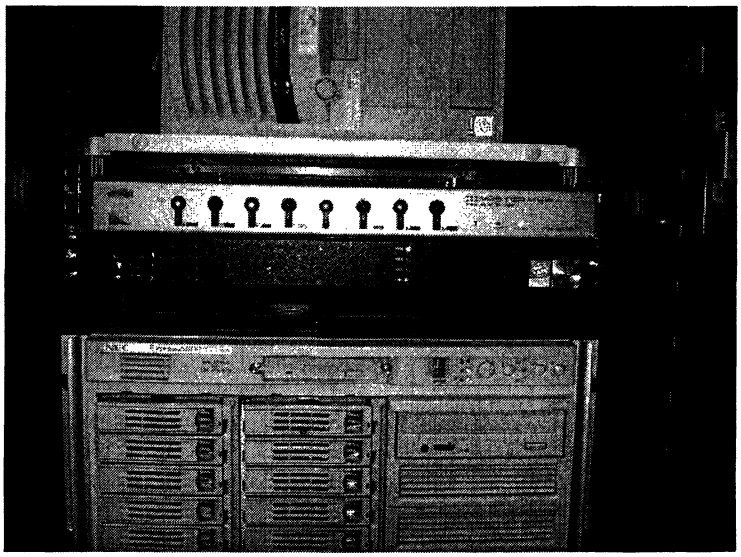

図 1　Linux サーバ機（平成 15 年度作成，写真中央，Proside 社製）

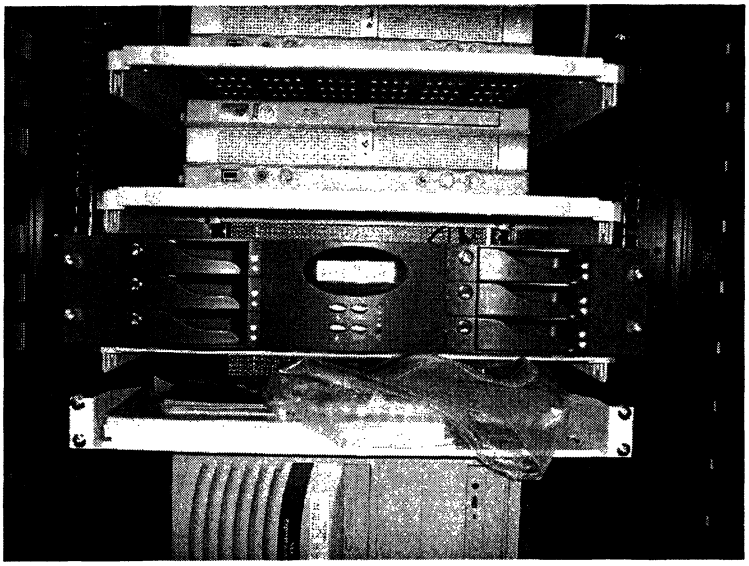

図 2 大容量高信頼性ディスク装置(平成 14 年度作成 写真中央, Infotrend 製)

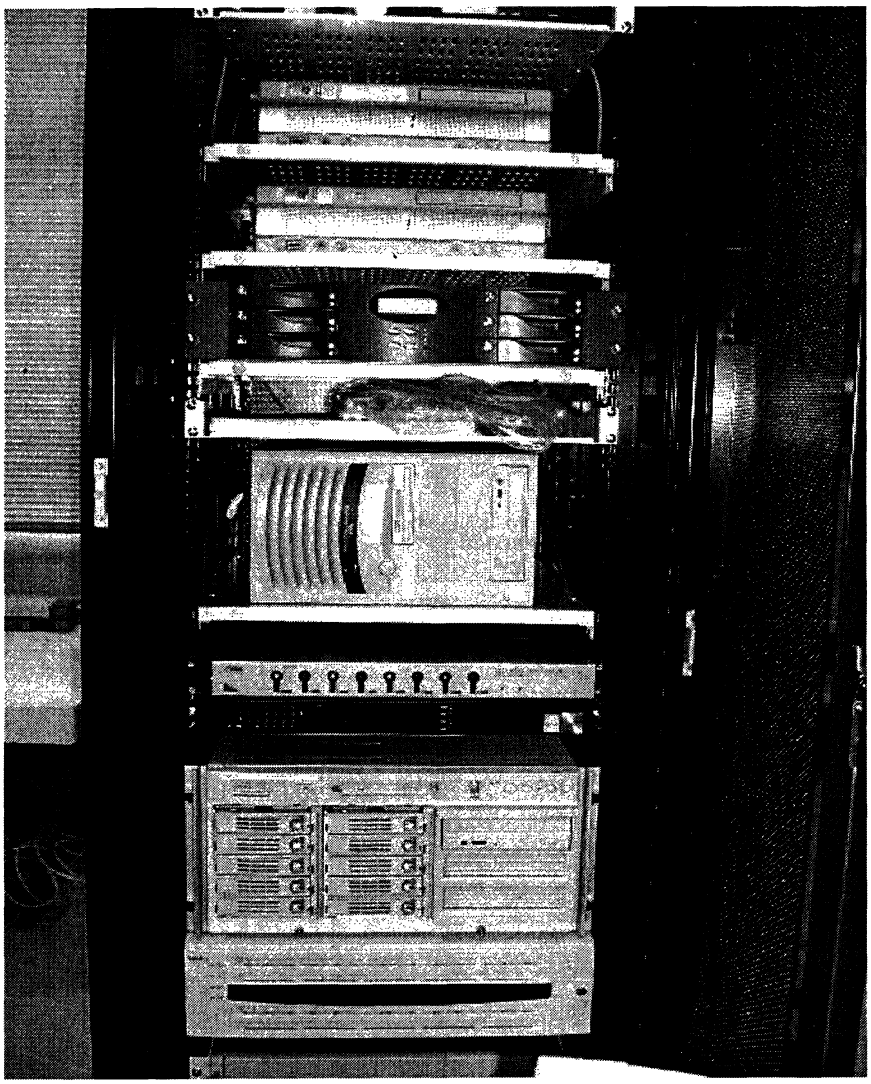

図 3 サーバ装置全景

ログファイルの実際と背景

Linux での Apache の標準設定(Version 2.0.40)では，以下にログのファイルが存在する

Apache の稼動ログ(アクセスログ)　　/var/log/httpd/access_log ,
Apache のエラーログ　　　　　　　　/var/log/httpd/err_log

侵入を試みる場合は，最初に必ず失敗をともなうので，上記のログに記録が残る場合が多く，典型的なウォームは特定の犯行の軌跡を残す．新聞紙上で騒がれるウォーム，ウィルスは爆発的な感染を引き起こし，しばらくして絶滅したかのように思われている．しかし，電子メールに添付されたファイルを後日開く場合，新規に Windows NT, Windows2000 を導入するなどの場合もあり，ウォーム感染，不正アクセスのバックドア開放に結びつく．加えて Internet の接続は国境を越えて行われており，日本以外の国々からの侵入も多く根絶は困難である．

Network 管理者は，専門家の責務として安全なネットワーク環境を保全する努力を怠ってはならないと言われている([1],[2])．ログの解析，統計的，科学的分析を行い，アクセス傾向を見ることは，早期に異常を発見し，未然に不正なアクセスを防止することができる可能性も高いと思われる．被害を受けた PC は，踏み台として，次の加害者になることを心に刻むべきであり，無作為の怠慢は，管理責任者としての咎を受ける可能性もあると思われる．

LOG の解析から見るウォームの傾向

典型的なウィルスは WWW サーバを対象として攻撃を加える．多くの侵入パターンは WWW サーバとしての機能を利用して不正な侵入を試みる．(詳細は ttp://www.cert.org)

以下に典型的なウィルスの侵入攻撃パターンを示す．

1. Code Red　(CERT Advisory CA-2001-19) と
   Buffer　Overflow を狙ってくるので，以下のアクセス Log が残る．
   ```
   GET/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
   NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
   NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
   NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
   NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
   NNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u
   6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53
   ff%u0078%u0000%u00=a　HTTP/1.0
   ```
2. Code Red II と sadmind/IIS ワーム (CERT　Incident Note IN-2001-09)
   Code Red と同様であるが，以下のアクセス Log が残る．
   ```
   GET/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
   XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
   ```

XXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a

3. W32/Nimda Worm（CERT® Advisory CA-2001-26 Nimda Worm）
以下の16個の連続アクセスが残る.

GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET/msadc/..%5c../..%5c../..%5c/..¥xc1¥x1c../..¥xc1¥x1c../..¥xc1¥x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..¥xc1¥x1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..¥xc0/../winnt/system32/cmd.exe?/c+dir
GET /scripts/..¥xc0¥xaf../winnt/system32/cmd.exe?/c+dir
GET /scripts/..¥xc1¥x9c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir

本学への不法侵入を狙った侵入統計からみた傾向

米国法では，Computer Fraud and Abuse Act (CFAA) 47 U.S.C. 1030 et seq[1]. により，コンピュータへの侵入は，試みただけでも違法となっている．日本でも不正アクセス行為の禁止等に関する法律（平成１３年１月６日施行）により，不正アクセスの実行は禁止されているが，捜査方法に関する適切な取り締まり方法が無いために，事前検挙の例はない．いずれも，国内犯だけを対象にしているために，国外でのウォーム作成，国外からのウォームの投入は野放しであり，ウォームによるバックドアの開放は2次犯罪に結びつく．

ウィルスおよびウォームには一定の時期に流行する．簡単な統計をとり，不正アクセスの発生時期を統計解析することは，管理者にとって重要な任務である．

前節で示したパターンをもとに，簡単な Shell Script で，不正アクセス統計ファイルをEXCEL で解析可能である．(付録参照)

前述の不正アクセスの統計を表 1 不正アクセスの分類と期間 に示す．表にみるようにNimda によるアクセスは消滅していないこと，そして以前の猛威を振るった Code Red II ではなく，CodeRED が再度復活していることに注意をするべきである．

[1] http://www.usdoj.gov/criminal/cybercrime/1030_new.html

表 1 不正アクセスの分類と期間

期間	CodeRED	CodeREDII	Nimda
2001/8/1 以前	0	0	0
～2001/9/1	134	4046	0
～2001/10/1 まで	0	1763	2115
～2001/11/1	4	0	1217
～2001/12/1	3	0	738
～2002/1/1	26	0	507
～2002/2/1	16	0	452
～2002/3/1	28	0	302
～2002/4/1	28	0	496
～2002/5/1	39	0	484
～2002/6/1	24	0	285

2002 年 5 月のアクセス回数をエラー! 参照元が見つかりません。に示す．比較のためにウォームが発生した 2001 年 9 月のアクセス回数を図 5．2001 年 9 月のアクセス回数 に与える．

基本的なアクセス回数は過去の時系列解析により、季節変動、循環変動、傾向変動に分解される．しかし，9 月のアクセスはこの不規則変動(ノイズ部分)が検定上，５％有意規準（P=0.00）で棄却されている．

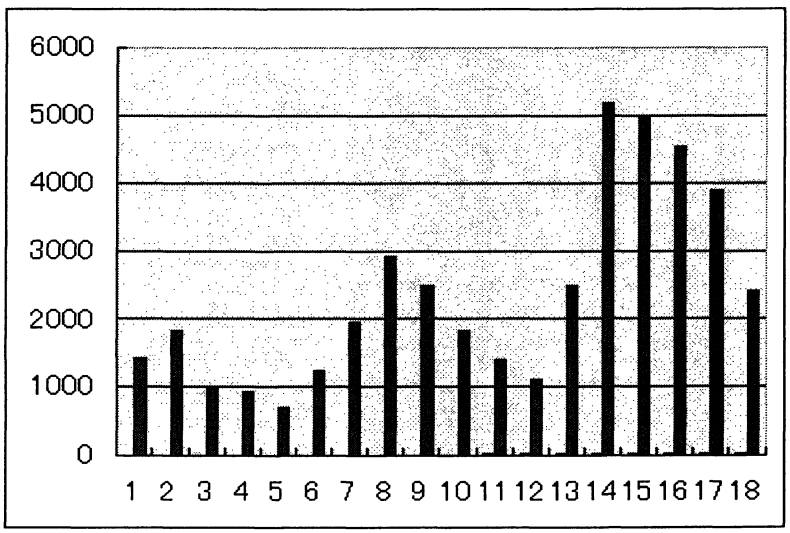

図 4．2002 年 5 月のアクセス回数

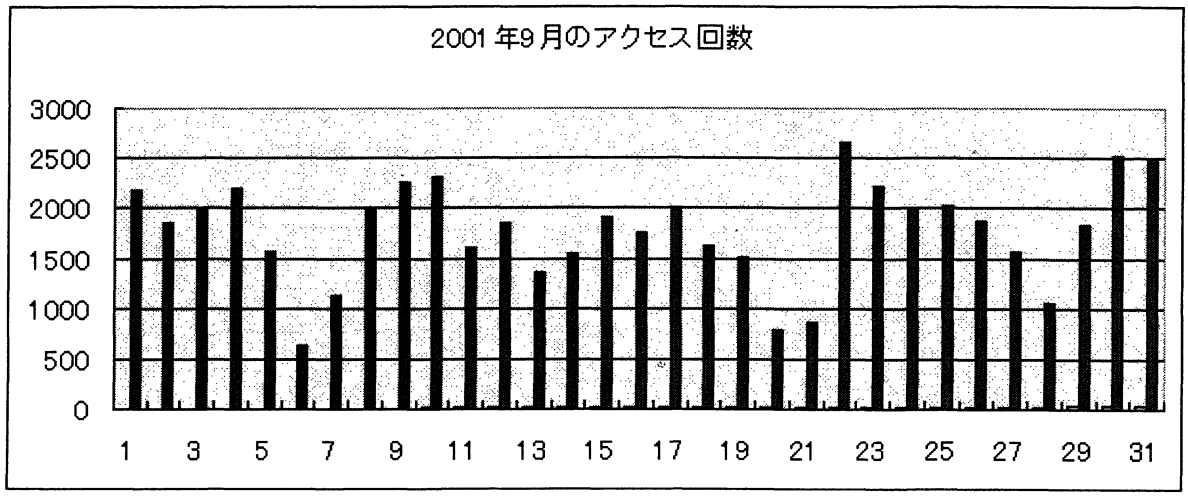

図 5. 2001年9月のアクセス回数

以上の例から不正アクセス対策として，サーバのプログラムの定期的な更新，瑕疵修正を行うのは当然として，Log の統計学的解析，多変量解析，時系列的な高度な解析を行えば早期に不正アクセスは発見可能と思われる．

まとめ

ウォーム等による不正アクセスの頻度は，流行性感冒の発生頻度に類似している．爆発的な流行の後，激減し，さらに復活を遂げる．

本学のウィルス発見頻度でも同様な傾向を示している．管理者が常に監視の目を Computer Network と Computer に向けるのは当然のことであるが，一般の利用者も常に過去のウィルス，ウォームの警戒をといてはいけないのである．1つの PC の不用意な操作が，所属する部署 NETWORK，そして世界の Internet への加害者になりうるからである．

さて，Computer Network と Computer 全体に管理と監視を行う管理者の労力は大きく，加えて対策の業務，報告書，計画立案と業務に関しては枚挙の暇がない．加えて，新種の不正アクセス，ウォーム,等は次々と発見されるだけでなく，本報告で示したように過去の不正アクセスが再流行するのである．行政のスリム化が叫ばれる今日ではあるが，必要な部署には適切な人材と人員の配置が必要であることを本報告のまとめとしたい．

謝辞

本学ネットワークシステムを献身的に保守監視している株式会社信越情報サービスの皆さん，企画立案の支援をしていただいている本学看護研究交流センターの皆様に深く感謝の意を表します．

参考文献,資料

1) ACM Council: "ACM Code of Ethics and Professional Conduct", http://www.acm.org/constitution/code.html. 1992.

2) 情報処理学会:" 情報処理学会倫理綱領", http://www.ipsj.or.jp/gaiyo/ipsjcode.html 2001

3) 北岡，園田:" 不正アクセスと刑法", 関西大学法学論集,第４７巻,第６号,47--. 1998

付録

例　CodeRED のアクセス統計を/tmp/C1.DAT というファイルに集計する例.

（1）UNIX に Login した後に以下の操作を行う.

grep　NNNNNNNNNNN　/var/log/httpd/access_log | cut -d¥[-f2 | cut -d¥] -f1 | cut -d: -f1 > & /tmp/C1.DAT

（2）UNIX にある/tmp/C1.DAT というファイルを Windows にファイル転送（FTP 等）を行った後に EXCEL で開く．読み込まれたデータが A 列となっているので，A 列全体の書式を「日付」の「2001/8/2」の形式に変更する.

	A	B
1	4-Aug-01	
2	4-Aug-01	
3	4-Aug-01	
4	4-Aug-01	
5	4-Aug-01	
6	5-Aug-01	
7	5-Aug-01	
8	5-Aug-01	
9	5-Aug-01	
10	5-Aug-01	
11	5-Aug-01	
12	5-Aug-01	
13	5-Aug-01	
14	5-Aug-01	
15	5-Aug-01	
16	5-Aug-01	
17	5-Aug-01	
18	5-Aug-01	
19	5-Aug-01	
20	5-Aug-01	

図 6　EXCEL でデータを開いた画面

	A
1	2001/8/4
2	2001/8/4
3	2001/8/4
4	2001/8/4
5	2001/8/4
6	2001/8/5
7	2001/8/5
8	2001/8/5
9	2001/8/5
10	2001/8/5
11	2001/8/5
12	2001/8/5
13	2001/8/5

図 7　日付を書式を変更した表示結果

（3）B 列に同様に日付の書式で階級の区切りを入力する.

	A	B
1	2001/8/4	
2	2001/8/4	2001/8/1
3	2001/8/4	2001/9/1
4	2001/8/4	2001/10/1
5	2001/8/4	2001/11/1
6	2001/8/5	2001/12/1
7	2001/8/5	2002/1/1
8	2001/8/5	2002/2/1
9	2001/8/5	2002/3/1
10	2001/8/5	2002/4/1
11	2001/8/5	2002/5/1
12	2001/8/5	2002/6/1
13	2001/8/5	
14	2001/8/5	

図 8　階級の区切りの日付を入力した画面

（4）EXCEL ではツールをアドインを指定し，「分析ツール」にチェックを入れる.

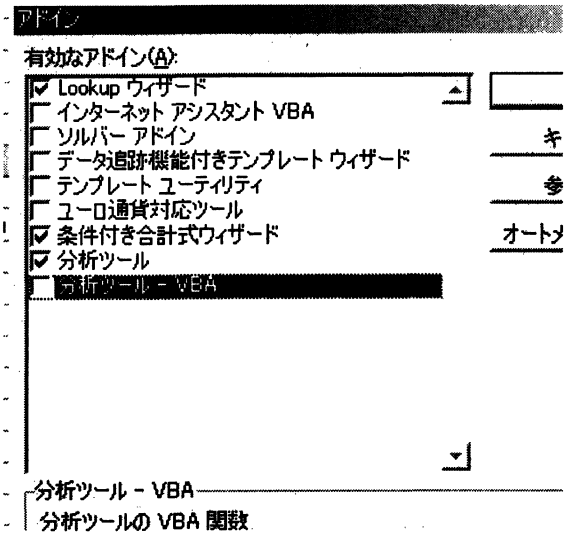

図 9 分析ツールを有効にした状態.

さらにツール⇒分析ツールを指定し，ヒストグラムを指定する.

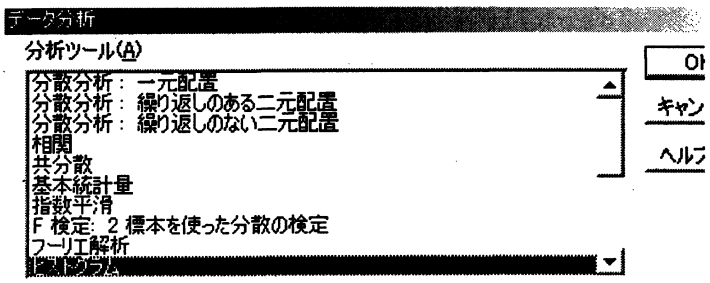

図 10　分析ツールのヒストグラムを選択する画面

ヒストグラムの対象を A 列全体（$A:$A）とし，区間のデータ（ここでは，B2：$B12）の範囲をしてし，出力先のセル（ここでは，$C$2）を指定し，OK を押す．

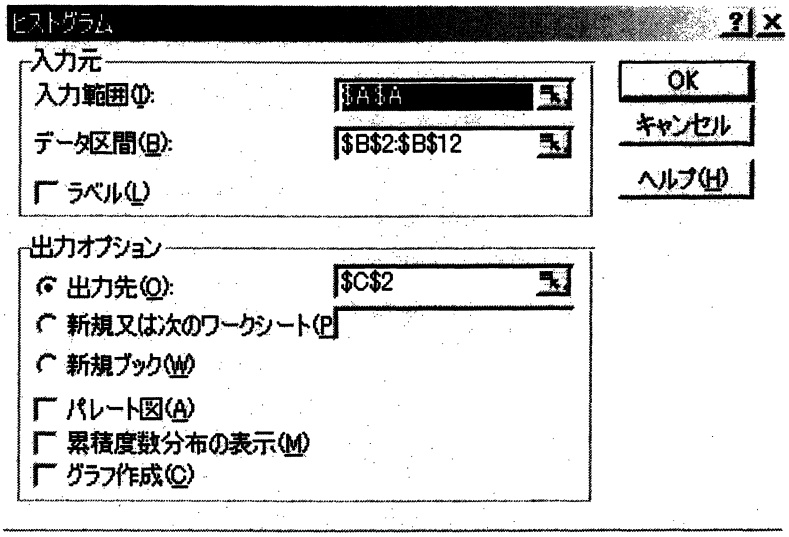

図 11　ヒストグラム作成画面

1.dat

	A	B	C	D
1	2001/8/2			
2	2001/8/2	2001/8/1	データ区間	頻度
3	2001/8/2	2001/9/1	2001/8/1	0
4	2001/8/2	2001/10/1	2001/9/1	134
5	2001/8/2	2001/11/1	2001/10/1	0
6	2001/8/2	2001/12/1	2001/11/1	4
7	2001/8/2	2002/1/1	2001/12/1	3
8	2001/8/2	2002/2/1	2002/1/1	26
9	2001/8/2	2002/3/1	2002/2/1	16
10	2001/8/2	2002/4/1	2002/3/1	28
11	2001/8/2	2002/5/1	2002/4/1	28
12	2001/8/2	2002/6/1	2002/5/1	39
13	2001/8/2		2002/6/1	24
14	2001/8/2		次の級	0
15	2001/8/2			
16	2001/8/2			

図 12　ヒストグラム作成結果

この例では 2001 年 8 月 1 日以前のアクセス結果は 0 であるが，2001 年 8 月から 9 月にかけて，134 件の不正アクセスがあったことになる．