新米エンジニアのための

初歩のインターネット技術

《第11回 ホストまでのメッセージ処理》

浅羽 登志也
asaba@iij.ad.jp
株式会社インターネットイニシアティブ

インターネットでは、一般のユーザーでも自分の送り出したメッセージが特定のホストに接続されるまでの仕組みを実際に確かめることができます。今回は、そのためのいくつかの便利なコマンドについて解説します。また、それを実際に使って目的地までどういう経路を通っているのか、相手ホストからなぜ応答が返ってこないのかを調べてみることにしましょう。

はじめに

この連載もついに11回目となった。過去10回で非常におおざっぱではあるが、ひととおりインターネットのアドレスやルーティングの仕組みについて解説してきたつもりである。しかし結構細かいところをすっ飛ばして進めてきているので、「これじゃなんにもわかんねーよ」と、いつか誰かに怒られるのではないかと、元来小心者の筆者は小鳩の胸をうち震わせながら毎日を過ごしている。一方、「インターネットマガジンの連載の中で1人だけハードコアで、周りからプカプカ浮いとるやんけ」とか「最初のほうは楽しいんですが、途中からよくわかんなくなります。あら、可愛い猫♪」などという声も聞く。ううむ。

それでも、「あっさばさんの記事わっかりやすいっすよー」と営業マンが励ましてくれることもある。そのニコニコ顔を見ていると、よっしゃ焼肉でも食って元気出して頑張ったろかい、という気分にもなる。とはいえ、「プロバイダーのエンジニアがこの記事読んで勉強しているらしいです」という風の噂を耳にすると、えええええええ、これ読んでもルーター1つ設定できるようになるわけじゃないのに、ええんかいなぁ…と再び不安な気持ちで胸が詰まる。

原稿はいつも夜中か休日か飛行機の中で書くことにしているのだが、最近はこんな感じで悶々としているうちに時が流れてしまうことも多い。

かくして、人は白いワニが見えるようになるのである。

運転を始める前に

ISP（Internet Service Provider）との接続が完了して人々はまず最初に何をするのだろうか？　目を輝かせながら知っている限りのURLにかたっぱしからクリック攻撃をかける？　よい時代（？）になったものである。

しかし、ちょっと待った。それで本当によいのだろうか？　もちろんそれでもよいのだが、少なくとも本稿の読者は違うと信じたい！　これはたとえば車を買ったときにまず何をするかということと似ているような気がする。つまりいきなりエンジンをかけてドライブに出かけてしまうのか、それとも、まずボンネットを開けて、よく分からないまでも、ふむふむとか言いながらひととおりあちこち触ってみたり、叩いてみたり、キャップを開けてみたりした後、さらにエンジンをかけてみて、おおあっちが動いている、こっちが回っている、なーるほどと満足そうに笑みを浮かべた後、初めてドライブに出かけていくかの違いである。

せっかくまだまだインターネットを動かしているいろいろな部分がユーザーにも比較的むき出しに見えてしまう時代なのだから、まずはいろいろ確かめてみないことには楽しみも半減するってぇもんじゃありませんか？

さて、ではいったい何が確かめられるというのだろうか？

pingコマンド

インターネットに繋がったということは、当然インターネット上のいろいろなホストにアクセスできるようになったということである。では特定のホストにインターネット経由で到達できるかどうかを調べるにはどうしたらよいだろうか？

これを確認するためにはpingというコマンドを用いればよい。pingはもともとUNIXワークステーション上のアプリケーション（Windows95にも同様のコマンドがあるし、MacにもMacTCP Pingというのがある）で、指定したホストが生きているかどうかを調べることができる。

図1はSunOS 4.1.4付属のpingコマンドを実行した例である。ベンダーやOSのバージョンによって実行の仕方やオプションに違いがあるので注意してほしい。

この図を見ると、確かにftp.iij.ad.jpというホストを指定してpingコマンドを実行すると「ftp.iij.ad.jpは生きてるよん（ftp.iij.ad.jp is alive）」という応答が返ってくる。「生きている」ということは、ftp.iij.ad.jpさんがちゃんと動いているということなんだろうが、じゃあなんで離れたところからそんなことが分かるのだろうか？

ICMP

この仕組みは結構単純で、相手を呼んでみて一定時間以内に返事をするかどうかで判断しているのである。この相手を呼ぶという行為は、ICMP（Internet Control Message Protocol）というプロトコルを用いて行われる。ICMPはすべてのIPのソフトウェアの一部として実装されているので、用いているホストがワークステーションだろうが、MacだろうがPCだろうが、コーヒーメーカーだろうが冷蔵庫だろうが、ともかくIPを用いて通信を行うことができるものであれば必ず利用できる（はずの）プロトコルである。

ICMPにはいくつかの種類のメッセージが定義されていて、pingコマンドではこのうちのエコー要求（Echo Request）とエコー応答（Echo Reply）という2つのメッセージを用いている。ICMPのエコー要求メッセージを受け取ったホストは、送り主に対してICMPのエコー応答メッセージを返すことになっているのである。

図1　pingコマンドの例1

```
asaba:shiosai>ping ftp.iij.ad.jp
ftp.iij.ad.jp is alive
```

図2のように、pingコマンドは、指定されたホストに対してICMPエコー要求メッセージを送り、一定時間内に相手のホストからICMPエコー応答メッセージが返ってくるかどうかを調べていたわけである。

さて、ここでもうちょっと考えてみよう。送り出したエコー要求メッセージに対してエコー応答メッセージがちゃんと返ってきた場合に、いったい何が確認できたことになるのだろう？

たとえば図2で考えると、実は次の3つのことが確認できたことになる。

❶ ホストAからホストBまでICMPエコー要求メッセージがちゃんと届く
❷ ホストBのIPのソフトウェアがICMPメッセージをきちんと処理し、ICMPエコー応答メッセージを送り返す
❸ ホストBからホストAまでICMPエコー応答メッセージがちゃんと届く

つまり、相手ホストまで到達できるということと、相手ホストのIPソフトウェアが正常に動作しているということが分かるのである。おそらくISPからルーターなどのインストールをしにきた人は、ルーターを設置したあとで外部との接続性を確認するために、このpingコマンドを用いているはずである（面白がって、端末を後ろからのぞき込んだりしないように:-））。

さらに、SunOS 4.1.4付属のpingコマンドではオプション-sを指定することにより、繰り返し相手ホストに対してICMPエコー要求メッセージを送ることもできる（この動作がデフォルトであるバージョンもある）。各々のエコー要求メッセージを送り出してからエコー応答が返ってくるまでの時間を計ることにより、相手ホストとの間のRTT（Round Trip Time）を測定することができるのである。このRTTとは1組のホスト間でパケットが往復するのにかかる時間のことである。

図3の例では、shiosai.iij.ad.jpというホストからftp.iij.ad.jpというホストに対してICMPのエコー要求メッセージを繰り返し10回送っている。1行の出力が1つのエコー要求メッセージに対応している。行の右端の数字は、その回のエコー要求に対するエコー応答が返ってくるまでの時間である。一番下の2行には全体の統計情報が示されている。この出力結果もpingのバージョンによって若干異なるので注意してほしい。

このように、pingコマンド自体は単純なことしかしていないのだが、結構いろいろなことを調べられて便利である。

待てよ、では、pingコマンドが失敗したとき、つまり、ICMPのエコー要求メッセージを送ったけれども、エコー応答メッセージが返ってこなかったような場合は、いったい何が起こっているのだろうか？　この場合は上記の❶❷❸のうちどれかがうまくいっていないことになるのだが、そのどれかを特定することはできない。こういうときにどこがおかしいのかもうちょっと詳しく調べる方法はないものだろうか？

tracerouteコマンド

以前にも一度紹介したが、UNIXワークステーションで動くtracerouteというコマンドがある（Windows95にも同様のtracertというコマンドがあるし、Macにもmac tracerouteというのがある）。tracerouteコマンドはその名が示すとおり、経路（route）の追跡（trace）をするためのコマンドであった。では、さっそく試してみよう。

図4は、urayasu.iij.ad.jpというホストからftp.iij.ad.jpに対してtracerouteコマンド

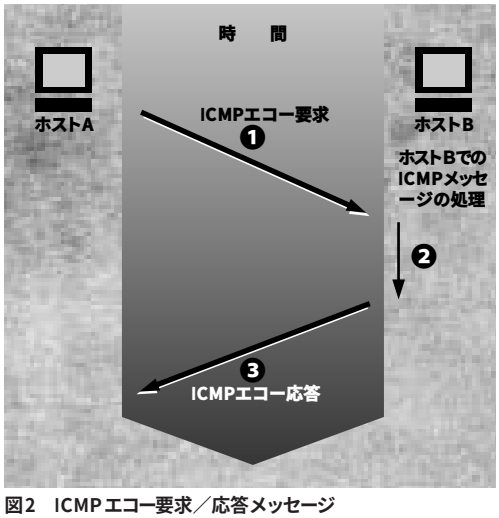

図2　ICMPエコー要求／応答メッセージ

```
asaba:shiosai>ping -s ftp.iij.ad.jp
PING ftp.iij.ad.jp: 56 data bytes
64 bytes from ftp.iij.ad.jp (192.244.176.50): icmp_seq=0. time=7. ms
64 bytes from ftp.iij.ad.jp (192.244.176.50): icmp_seq=1. time=7. ms
64 bytes from ftp.iij.ad.jp (192.244.176.50): icmp_seq=2. time=6. ms
64 bytes from ftp.iij.ad.jp (192.244.176.50): icmp_seq=3. time=8. ms
64 bytes from ftp.iij.ad.jp (192.244.176.50): icmp_seq=4. time=6. ms
64 bytes from ftp.iij.ad.jp (192.244.176.50): icmp_seq=5. time=7. ms
64 bytes from ftp.iij.ad.jp (192.244.176.50): icmp_seq=6. time=6. ms
64 bytes from ftp.iij.ad.jp (192.244.176.50): icmp_seq=7. time=6. ms
64 bytes from ftp.iij.ad.jp (192.244.176.50): icmp_seq=8. time=6. ms
64 bytes from ftp.iij.ad.jp (192.244.176.50): icmp_seq=9. time=6. ms
^C
---- ftp.iij.ad.jp PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 6/6/8
```
図3　pingコマンドの例2（オプション-sを指定した場合）

を実行したときの結果である。これにより、urayasu.iij.ad.jpからftp.iij.ad.jpに到達するまでどういうルーターを経由していくのかが分かる。

まず1行目は、最初に経由するルーターがmaihama.iij.ad.jpという名前のルーターであることを示している。さらに行の右側の3つの数字がurayasuからmaihamaまでのRTTを示している。なぜ3つ表示されるかは後で詳しく述べることにしよう。

2行目は、maihamaの次に、sanbancho-fw.iij.netというルーターを経由することを示している。行の右側の3つの数字は1行目と同様、urayasuからsanbancho-fwまでのRTTを示す数字である。

以下同様に、otemachi-bb0.iij.net、otemachi-gate0.iij.netというルーターを経由して最後5行目にftp.iij.ad.jpというホストに到達していることが分かる。このように、経路上にあるすべてのルーターを経由する順番に示してくれるのである。しかも、各ルーターまでのRTTまで分かってしまうのだ。なるほど、面白い。しかし、どうしてこんなことが分かるのだろう？

実はtracerouteコマンドもICMPを用いているのである。しかし、pingコマンドと違って結構複雑なことをしている。tracerouteコマンドの動作を理解するためには、実はいままですっ飛ばしてきた細かい部分を理解する必要がある。

IPデータグラムの構造

インターネット上でやりとりされるデータの単位は、IPデータグラムという。これは連載の前のほうでも解説したと思う。すべてのデータグラムは、データグラムヘッダーを持ち、ここにデータグラムの配送を制御するための情報が書き込まれている（図5）。

これはちょうど葉書や封書を送るときには、表に宛先や送り主の住所を書いたり、場合によっては速達と書いたりするのと同じことである。これを見て郵便屋さんはそれをどこに届けるのか、届かなかったときにはどこに送り返すのか、速達扱いで送るべきかどうか、などを判断するのである。

IPのデータグラムヘッダーには、宛先や送り主の住所に相当するIPアドレスや、TOS（Type Of Service）のような、配送の質を示す情報（これはたとえば郵便に普通の郵便と速達があるようなものである。だがTOSは現在あまり使われていない）などが記されている。

この他にもデータグラムヘッダーには、データグラムに振られたシーケンス番号や、データグラムの生存時間（TTL: Time To Live）や、途中でデータグラムがさらに細かく分割されたかどうかを示す情報などが含まれている。データグラムヘッダーの詳細については、別の機会に譲ることにして、ここではtracerouteを理解するために必要なものだけ解説しよう。

データグラムの最長生存時間

すべてのIPデータグラムには必ず最長生存時間（TTL）というものが定義されている。これは実際には8ビットの整数値であり、インターネット上に送り出されたデータグラムが生存し続けられる最長時間を秒数で表したものである。TTLの値は、ルーターがデータグラムを配送する際に、その処理にかかった秒数だけ減じられる。通常はルーターでのデータグラムの処理は、数ミリから数十ミリ秒程度しかかからない。しかし、TTLの値は少なくとも1ずつ減らさないといけない（さもないと、永遠にTTLの値は減らない）ので、ルーターを通過するたびに1ずつ減っていくと考えればよいだろう。

こうしてルーターを経由するたびにTTLは1ずつ減じられ、0になった時点でデータグラムは廃棄される。これにより、たとえばルーティング・ループなどが生じた場合にも、データグラムが永遠にループすることを防止できるのである。

しかし、人様のデータグラムを廃棄してしまうわけなので、ただ黙って捨ててしまうわけにもいかない。そのデータグラムの送り手に自分がデータグラムを廃棄してしまったことをお知らせするのが礼儀というものである。さて、どうしよう？

大丈夫。困ったときのICMPということで、ちゃんとそのためのメッセージが用意

```
toshiya:urayasu>traceroute ftp.iij.ad.jp
traceroute to ftp.iij.ad.jp (192.244.176.50), 30 hops max, 40 byte packets
1 maihama (192.244.184.33)  2.105 ms  1.975 ms  1.937 ms
2 sanbancho-fw.iij.net (192.244.191.45)  36.426 ms  33.858 ms 32.502 ms
3 otemachi-bb0.iij.net (202.232.0.33)  43.935 ms  39.508 ms  41.499 ms
4 otemachi-gate0.iij.net (192.244.176.14)  38.911 ms  37.909 ms 37.232 ms
5 ftp (192.244.176.50)  47.307 ms  37.76 ms  37.296 ms
```

図4　tracerouteコマンドの例

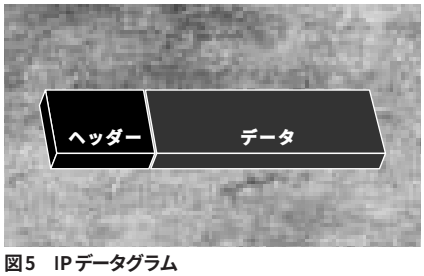

図5　IPデータグラム

されているのである。この場合のデータグラム廃棄の通知には、ICMPの時間切れ（Time Exceeded）メッセージを用いることができる。

図6では、ホストAからホストBに向けてデータグラムをTTL=6で送り出したが、経路上のルーター1でTTLの値が0となり、データグラムが廃棄される。ルーター1は、データグラムを廃棄したことを通知するためにホストAにICMP時間切れメッセージを送る。

これを受け取ったホストAでは、「ああ、TTLが0になっちゃったのかぁ…」とデータグラムが廃棄された原因を知ることができるのである。

宛先到達不可

tracerouteコマンドを説明するためには、さらにいくつかのICMPメッセージについて説明しておかないといけない。あともう少しだけ我慢しよう。

データグラムが途中で廃棄されるのは、TTLが0になったときだけではない。経路上のルーターやデータグラムのデスティネーションホストが、受け取ったデータグラムをどう処理してよいのか分からずに困ってしまうことがある。

ルーターであれば、宛先ホストに対する経路情報を持っていないため、次にどこに転送してよいのやら分からなくなったり、宛先ホスト自体がいなかったりした場合である。ホストであれば、確かに自分宛のデータグラムだけれども、それを渡すべきアプリケーションがないような場合である。

困ったときには、そのまま持っていても仕方がないので「ええい捨てちゃえ！」となるのだが、この場合もやはり黙って捨ててしまうのは礼儀に反する。

このような場合のために、3つのICMPメッセージが用意されている。ネットワーク到達不可（Network Unreachable）メッセージ、ホスト到達不可（Host Unreachable）メッセージ、ポート到達不可（Port Unreachable）メッセージである。ちょっと待ってよ。最初の2つは分かるけど、最後の「ポート」って何なのよ？　うーむ困った。筆者もここで原稿を捨てちゃいたくなるのだが、そうすると畳の上で寝られなくなってしまう人がいるので、そうもいかない。とりあえずここでは、ポートはアプリケーションを表すと思ってほしい。

これでやっと材料が揃った。

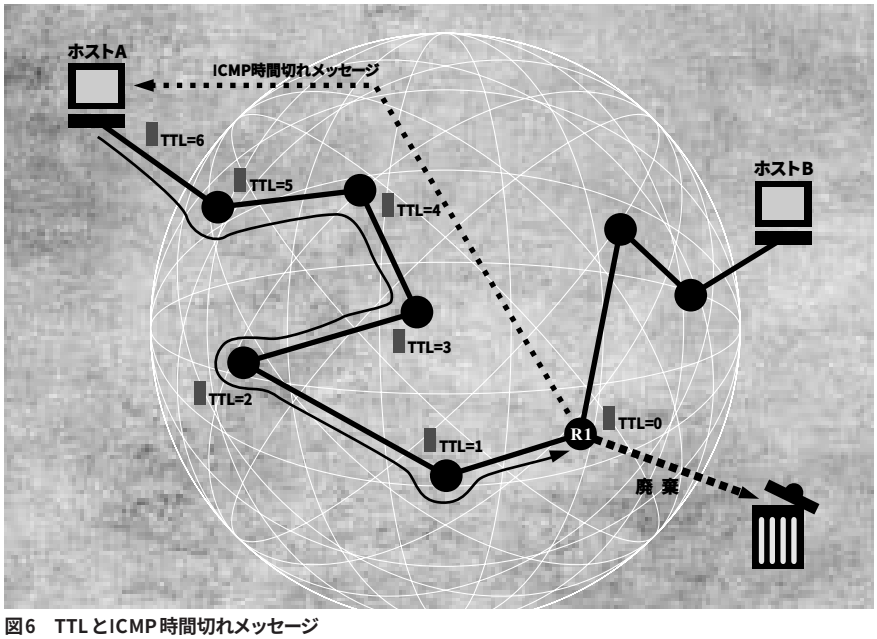

図6　TTLとICMP時間切れメッセージ

tracerouteコマンドの仕組み

tracerouteコマンドは、図7に示すように、これまでに説明したいくつかのICMPメッセージをうまく利用して、経路上のルーターを調べていく。

ホストAからホストBまでの経路を調べたい場合、まずホストAは、ホストB上に存在しない（と思われる）アプリケーション宛にデータグラムを送る。ただしこのときTTLの値を1にして送るのである。

するとそのデータグラムを受け取ったルーター1は、データグラムの転送の処理をする際にTTLの値を1減らす。もともとTTLが1だったものを、1減らしてしまうと0になるので、「おっとぉ、ざーんねんでした捨てちゃうもんね」とデータグラムを廃棄する。

だがこのとき礼儀正しいルーター1は、ICMP時間切れメッセージをホストAに送り返して、自分がいみじくもデータグラムを廃棄してしまったことを通知する。これによりホストAは、最初のルーターがルーター1であることが分かる。なぜ分かるかって？　ふっふっふ、まだまだ甘いな明智君。送られてきたICMPメッセージのソースアドレスを見ればよいのだよ。

次にホストAは、最初と同じデータグラムを再び、しかし今度はTTLの値を2にして送り出す。すると今度はルーター1でTTLが1減らされてもまだ0にはならず、ル

ーター2にめでたく転送される。だがルーター2で残念ながらTTLは0となり、今度はルーター2がデータグラムを廃棄する。ルーター2も礼儀正しい良い子なので、ホストAに捨てちゃってごめんなさいと、ICMP時間切れメッセージを送る。これでホストAは、2番目のルーターがルーター2であることをまんまと知ることができるのである。

あとは、これを繰り返していけばよい。ホストAは、ICMP時間切れメッセージを受け取るたびに、TTLの値を1つ増やして前と同じデータグラムを送り出す。こうすることにより、データグラムが転送されていく経路上の順番どおりにどういうルーターがあるのかがホストAにばれていくのである。しかもホストAでは、ICMP時間切れメッセージが送り返されてくるまでの時間を計っているので、図4のようにRTTまでばれてしまう。

これを繰り返していくと、いつかはホストBまでデータグラムが届くようになる。しかし、せっかくホストBにデータグラムが届いても、ホストBにはそのデータグラムを処理するアプリケーションがいない。良い子のホストBは「せっかく頂いたんですけどねぇ」と言いながらもデータグラムを廃棄するのだが、ホストAに対してICMPポート到達不可メッセージを送り返すことを忘れない。

ホストAでは、ICMPポート到達不可メッセージが送り返されると、「おお、やっとホストBに届いたか」と言いながら、tracerouteコマンドの実行を終了するのである。

おわりに

こうして、pingコマンドやtracerouteコマンドを用いれば、特定の相手に到達できるのかどうか、また、そこに至るまでにどういう経路を経由するのかを調べることができる。これだけでもいろいろ楽しめること請け合いである。

あれ？　でも、ちょっと待ってよ。tracerouteコマンドで、もし万が一データの宛先として指定されているアプリケーションがホストB上に存在していたらどうなるの？　思惑通りにICMPポート到達不可メッセージは返ってこないんじゃないかしら？　うーむ、良い質問だ。

ふっふっふ。ぬかりはない。そのためにtracerouteコマンドは、データグラムを3つ同時に、それぞれ異なるアプリケーション宛に送り出しているのである。これが図4で、RTTが3つずつ表示されている理由である。またこれによって、同じルーターに対するRTTを3回測定していることになるので、1回だけ測定するよりもよいデータが得られるのである。どうだまいったか？

うーん、でもでも、もしその3つの異なるアプリケーションがたまたますべて存在していたらどうなるの？ ねぇどうなるの？

うっうーむ。再び良い質問だ……　おっとぉ、そろそろ時間だぁ！ ふっふっふっふ。さらばじゃ明智君！ また会おう！

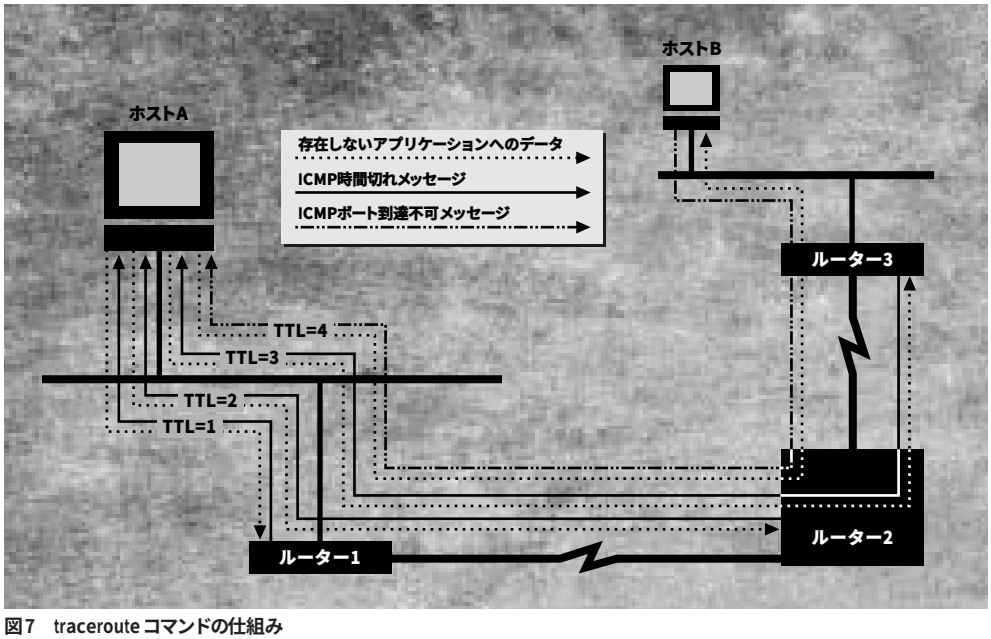

図7　tracerouteコマンドの仕組み

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp