無防備のままでは、LANの情報がダダ漏れだ！

「鉄壁 無線LAN」で

あなたの無線LANも不正アクセスにさらされている

あなたの無線LANのアクセスポイントは、きちんとセキュリティーを設定しているだろうか。「面倒くさい」「わからない」からといって、無防備なままでは、いずれ不正アクセスの被害に遭うだろう。

不正アクセスというと、下の例の「③ウイルスを送りつけられる」「④重要なファイルを消される」のような、わかりやすい被害が思いつく。しかし、本当に怖いのは「①イタズラの『踏み台』にされる」「②社内情報を盗み取られる」といったケースだ。

①の例だと、イタズラされたサイトのログ（通信記録）には、アクセスポイントの持ち主のIPアドレスが残ってしまう。持ち主は、被害を受けたサイトから犯人と疑われてしまうだろう。

②の例では、証拠を残さずに社内情報を盗み取られてしまう。社内のアクセスポイントに接続して、パスワード設定のないファイルを簡単に盗み出せる。さらに、「パケットモニタリング」を使うと、社内LANに流れている情報を盗み取ることも可能だ。盗んだデータを解析すれば、送受信されたメールなどを抽出できるのだ。

①イタズラの「踏み台」にされる

自宅のアクセスポイントを悪用されると、「オークション詐欺」や「誹謗中傷」の犯人にされてしまうことも。

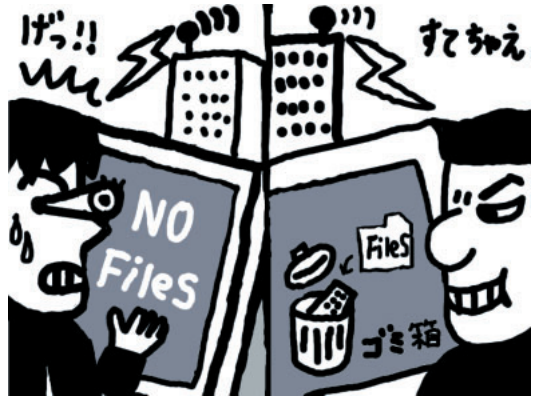
②社内情報を盗み取られる

社内LANに接続しているアクセスポイントを通して、パスワード設定されていないファイルが盗まれる。

③ウイルスを送りつけられる

通りすがりのアクセスポイントにつながっているPCに、ウイルスを送りつけることもできる。

④重要なファイルを消される



LAN内は安全と思われがちで、アクセス権の制御がされていない共有が多い。無線LANで侵入して、ファイルを全消去することも可能だ。

アクセスポイントを守る

text : 編集部　illust. : Hasegawa Takako

不正アクセスを防ぐならこのソフト

多くのアクセスポイントは、初期設定では、セキュリティー的にかなり無防備な状態のため、安全に使うにはいくつかの項目を設定しなければならない。

通信を暗号化する設定を行えば、「WEPキー」という文字列が違うと通信できなくなるので、かなり安全になる。最低限設定したい項目だ。このほかにも、MACアドレスを登録して、特定のPCだけ通信を可能にする設定や、アクセスポイントを隠して、アクセスポイントの有無すらわからなくするといった設定も有効だ。これらに対応しているアクセスポイントは限られているが、対応していれば設定しておきたい項目だ。これに加えて、ESS-IDを変更すれば、解読はさらに困難になるだろう。

これらの機能は、ブラウザーや専用の設定ソフトを使って設定するが、多数の専門用語が登場するうえ、設定項目がメニューのあちこちに分かれているため、複雑でわかりにくい機種も多い。

8月2日にソースネクストが発売した「鉄壁 無線LAN」は、アクセスポイントのセキュリティー設定を簡単にするソフトで、設定する項目を3ボタンに集約している。

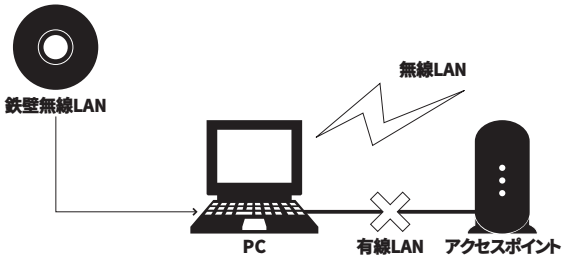
本当に3ボタンだけで無線LANのセキュリティーを確保できるのか、使い勝手も含めて編集部で検証しよう。

■ 無線LANのセキュリティーを高めるために必要な設定

- 無線LANの通信を暗号化
- MACアドレスの登録
- アクセスポイントを隠す
- 「ESS-ID」の変更

こうしたセキュリティーの設定は、ある程度ネットワークの知識のある人でないと難しい。「鉄壁 無線LAN」は、各種の設定を簡単にするソフトだ。

■ 無線LAN経由で設定できる



有線LANにつなぎ替えなくてもアクセスポイントの設定が可能だ

■ 対応アクセスポイント

メルコ	WLA-S11G※1
	WLAR-L11G-L
	WLA-L11G
	WLAR-128G
	WLAR-L11-S
IOデータ機器	WN-B11/BBRH
	WN-B11/BBR
	WN-A54/BBR
NEC	PA-WBR75H
	PA-WDR85FH/CE
	PA-WDR85FH/GS
コレガ	CG-WLAPRS11
	CG-WLAPR11
	CG-WLAPL11
プラネックス	BLW-03FA
	BLW-03
NTT-ME	MN7530
京セラ	KY-BR-WL100

※インターネットエクスプローラ5.5以上が必要
対応機種は8月 8日現在。新しい対応アクセスポイントは、ソースネクストのホームページに掲載される

鉄壁無線LAN

DATA

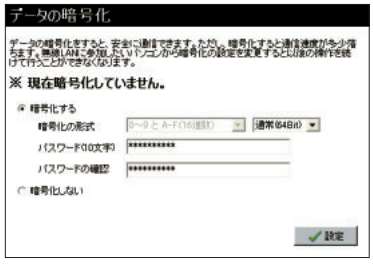
販売元	ソースネクスト株式会社
価格	6,980円
対応OS	ウィンドウズ98/98SE/2000/XP
ハードディスク	20MB以上
ブラウザー	インターネットエクスプローラ5.0以上
ドライブ	CD-ROMドライブ
問い合わせ先	03-5350-4844

N-Jump www.sourcenext.com

ボタン3つでアクセスポイントが安全になる

機種を間違えたときは
このボタンを押す

暗号化して盗聴を防ぐ



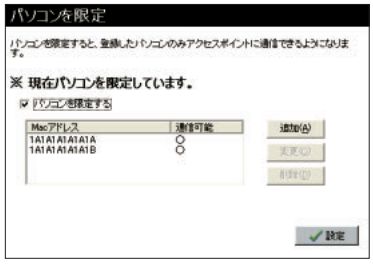
「データの暗号化」ボタンを押して、「パスワード」を設定すると、通信の暗号化が完了する。鉄壁無線LANでの「パスワード」は「WEPキー」や「ネットワークキー」と呼ばれるものだ。暗号には「64ビット」と「128ビット」の2種類があり、128ビットの方が強い。ただし、128ビット暗号はアクセスポイントと無線LANカードの組み合わせによっては通信できないことがあるので注意しよう。

WEPキーとは

WEP(Wired Equivalent Privacy)は、無線LANを暗号化して、セキュリティーを保つための仕様だ。WEPでは、10文字か26文字の「キー」を設定して通信を暗号化するが、この文字を「WEPキー」と呼ぶ。暗号化した無線LANでは、同じWEPキーを持つアクセスポイントと無線LANカードだけが通信できる。

WEPキーには容易に想像できる文字列や単語を使わずに、「AF083DC302」のようなアルファベットと数字を含むものにしよう。

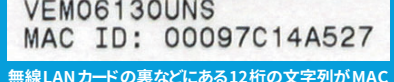
PCを制限して不正アクセスを防ぐ



「パソコンを限定」を押して、無線LANカードの「MACアドレス」を登録すると、登録された無線LANカードだけがアクセスポイントと通信できるようになる。

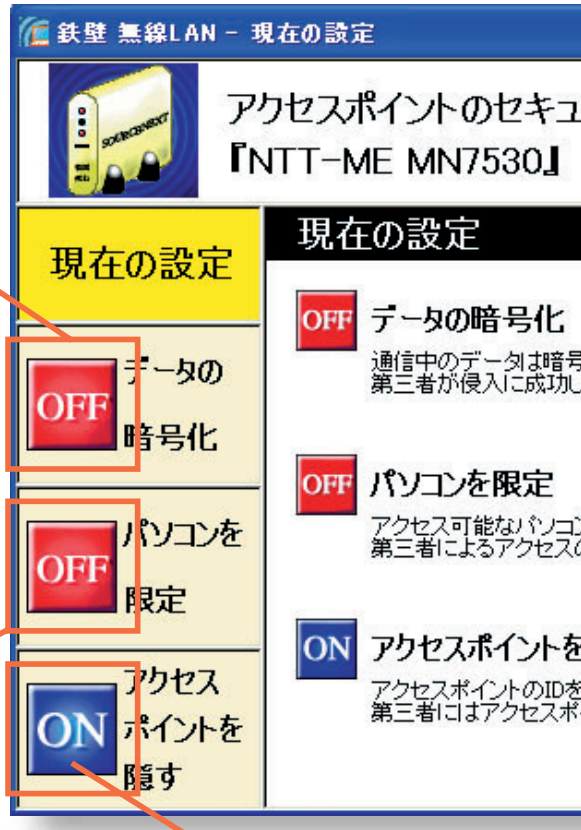
鉄壁 無線LANをインストールしたPCのMACアドレスを登録し忘れると、アクセスポイントの設定を変更できなくなってしまうので注意。

MACアドレスとは

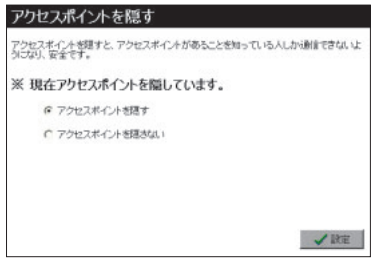


無線LANカードの裏などにある12桁の文字列がMACアドレス。メーカーによっては「MAC ID」「Node ID」と呼ばれる。

無線LANカードには「MACアドレス」という番号が割り振られている。MACアドレスは世界中で1つしかないので、MACアドレスを制限することで、特定のPCだけがアクセスポイントを使えるように設定できる。

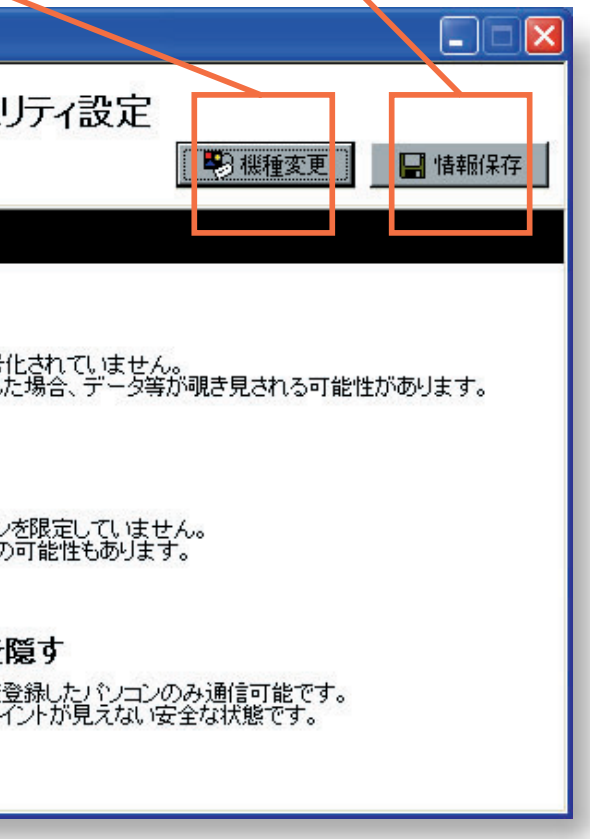


アクセスポイントを隠す



このボタンをオンにすると、ウィンドウズXPの「ワイヤレスネットワーク」からアクセスポイントを隠せるようになる。隠したアクセスポイントに接続する場合は、「ワイヤレスネットワーク」のプロパティーからESS-IDを直接入力する。

アクセスポイントの設定
を確認するときに押す



テストで使ったアクセスポイント

NTT-ME MN7530

Jump www.ntt-me.co.jp/mn/

1.5Mbpsと8Mbpsに対応したADSLモデムと、ルーター、無線LANアクセスポイントの複合機。対応しているADSLは、NTT東日本、NTT西日本の「フレッツ・ADSL」とイー・アクセスの2社。接続方式は、「PPPoE」と「PPPoA」、「IPoA」に対応する。IEEE 802.11b準拠の無線LANと、100Mbps対応の4ポートスイッチングハブを内蔵している。ADSL回線を使っていて、設置する機器を1台で済ませたい人におすすめだ。

通信規格	IEEE 802.11b
WEPキー	64/128ビット対応
外形寸法	W205×H170×D202mm
価格	4万4,800円

WLA-L11G

Jump www.melcoinc.co.jp

IEEE 802.11bに準拠した無線LANアクセスポイント。ルーター機能やADSLモデム機能は内蔵していない。64ビットと128ビットの暗号に対応しており、安全性の高い無線LANを構築できる。メーカー公称値では、屋内での通信距離が115メートル、屋外での通信距離が550メートルとなっており、広範囲で通信が可能だ。すでに有線LANでネットワークを構築していて、新たに無線LANを導入したいときに最適だ。

通信規格	IEEE 802.11b
WEPキー	64/128ビット対応
外形寸法	W205×H170×D202mm
価格	3万3,000円

セキュリティーはほぼ「鉄壁」

「鉄壁 無線LAN」を使ったセキュリティー設定は、ボタンを押して文字列を入力するだけで、意外なほど簡単だった。主要なセキュリティー機能が設定できていて、ほぼ「鉄壁」と呼べる。

唯一、「ESS-IDの変更」ができない点が気になった。ESS-IDを変更しないと、なんらかの事情で「データの暗号化」ができないときに危険なアクセスポイントになってしまうためだ。

「アクセスポイントを隠す」を設定すれば、「データの暗号化」の設定は不要かというとそうではない。アクセスポイントを隠していても、順番にすべての機種の初期設定のESS-IDを入力すれば、いずれ接続できてしまう。こういう事例は滅多にないかもしれないが、ESS-IDも「鉄壁 無線LAN」から変更できたほうがいい。

完全に「鉄壁」セキュリティーにするなら「データの暗号化」「パソコンを限定」「アクセスポイントを隠す」の3ボタンに加えて「ESS-IDの変更」を加えてほしいところだ。

■ アクセスポイントを隠せる機種

NEC
PA-WBR75H
PA-WDR85FH/CE
PA-WDR85H/GS
コレガ
CG-WLAPRS11（ファームウェア4.5.6G以上）
CG-WLAPR11（ファームウェア4.5.5G以上）
CG-WLAPL11
NTT-ME
MN7530

対応機種は8月8日現在。非対応のアクセスポイントでも、ファームウェアのバージョンアップで対応することがある

■ MN7530の設定結果

セキュリティー機能	対応
ESS-IDの変更	×
40ビットWEP	○
128ビットWEP	○
MACアドレス制限	○
アクセスポイントを隠す	○
本体ログイン名変更	×
本体パスワード変更	×

MN7530では、無線のセキュリティーは設定できたが、本体のログイン名とパスワードの変更はできなかった。

■ WLA-L11Gの設定結果

セキュリティー機能	対応
ESS-IDの変更	×
40ビットWEP	○
128ビットWEP	○
MACアドレス制限	○
アクセスポイントを隠す	—
本体ログイン名変更	—
本体パスワード変更	×

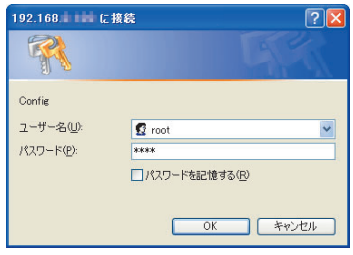
WLA-L11Gは、「アクセスポイントを隠す」と「本体ログイン名変更」にアクセスポイントが対応していない

接続が簡単になればさらによくなる

アクセスポイントには、設定を勝手に変えられないようにパスワードが設定されている。初期設定では「Admin」や「root」のように、すぐに推測できるパスワードが設定されているため、パスワードも変更しておきたい。「鉄壁 無線LAN」は、パスワード変更に対応していない。次バージョンでは、ぜひ搭載してほしい機能だ。

さらに、「鉄壁 無線LAN」からアクセスポイントに接続すると、右のような接続ダイアログが突然表示されて、ユーザー名とパスワードの入力を求められた。これでは、設定に慣れていないユーザーには不親切だ。初心者向けなら「鉄壁 無線LAN」が自動的に初期設定のユーザー名とパスワードを入力するか、初期設定のユーザー名などがマニュアルに記載されていることを、画面上でガイドすべきだろう。

■ 突然表示されたダイアログ



アクセスポイントに接続するための「ユーザー名」と「パスワード」のダイアログが突如表示された。

「鉄壁 無線LAN」で設定できるセキュリティー

- ○ 無線LANの通信を暗号化する
- ○ アクセスできるPCを制限する
- ○ アクセスポイントを隠す
- × 「ESS-ID」の変更

街にあふれる無防備アクセスポイント

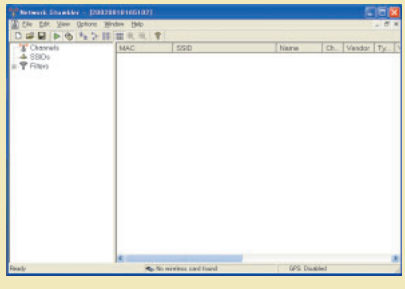
実録レポート

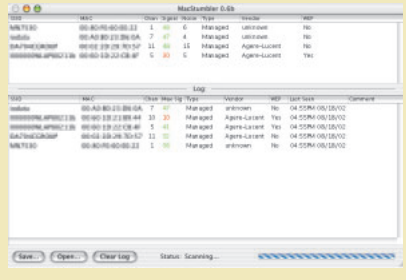
見つかったアクセスポイント：101か所
暗号化していないアクセスポイント：55か所

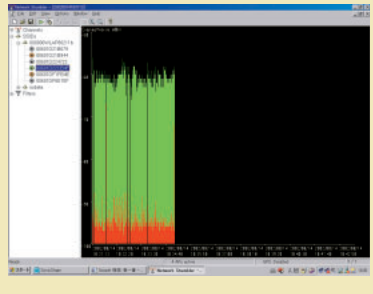
どの程度のアクセスポイントが稼働して、そのうち無防備な割合はどれだけか。東京都心と近郊で、アクセスポイントの設置数と暗号化の状態を探ってみた。

驚くべきことに、半数のアクセスポイントが暗号化の設定をしていなかった。また、暗号化はおろか、「Tsunami」「iodata」「bRoadLanner」のように、初期設定のESS-IDを変更していないアクセスポイントが10パーセントほど見つかった。まったくの初期状態で稼働しているようだ。

米国では、ノートPCを使って無防備なアクセスポイントを探す「ウォー・ドライビング」(War Driving)が問題になっている。ひょっとしたら、あなたのアクセスポイントもマニアの間で「無料ホットスポット」として、リストアップされているかもしれない。







「Net Stumbler」は、アクセスポイントの有無や暗号化の状態を検索するツール。これらのツールを使うと、無防備なアクセスポイントを簡単に発見できる。ウィンドウズ版のほか、マッキントッシュ版も出回っている。Net Stumblerを使うことで、自社オフィス内に社員が勝手にアクセスポイントを設置していないかチェックできる。

山本（以下 山）：いきなり本題ですけど、鉄壁 無線LANは「買い」ですか。

三柳（以下 三）：アクセスポイントの設定ができていない人には、有無を言わさず買わせたい。よく無線LANのセキュリティーを設定しに、友達の家に出張することがあるけど、今後はこのソフトを奨めるよ。

山：正直に言うと、ソースネクストっていうので、機能も「初心者向け」かと思っていたんですよ。でも、実際に使ってみた感想は、ソフトはよくできいますよ。でも、初心者向けにはまだハードルを感じる。

三：ボタン3つで設定できるんだから、あれ以上簡単にはならないんじゃないの？

山：問題は設定画面ではなく、アクセスポイントに接続するときにあるんですよ。今回は、あえて「鉄壁 無線LAN」とアクセスポイントのマニュアルを読まないでテストしました。セキュリティーの設定は元々面倒だから、マニュアルを読まなくてもいいぐらい簡単じゃないと使う人は少ないと思って。が、アクセスポイントを選択して接続するときに、アクセスポイントにログインするユーザー名とパスワードを入力するのダイアログが出て困っちゃいました。結局、マニュアルの巻末にある初期設定のユーザー名とパスワードを探しましたよ。

本誌デスクの三柳英樹。ADSLからバックボーンまでインフラに深い知識を持つ

三：このソフトって、初期設定で使っている人が対象だとすれば、極力簡単に設定できたほうがいいね。初期設定のユーザー名は自動で入力してほしかったな。で、「鉄壁 無線LAN」上で名前とパスワードを変更するほうが便利だし、セキュリティーもより強固だよね。

山：いきなり注文を付けちゃいましたけど、非常によくできてる点があって、メルコのWLA-L11Gでのテストですが、アクセスポイントに接続している無線LANカードのMACアドレスを自動で読み取ってリストに表示するんですよ。リストの中から、登録したいMACアドレスにだけチェックを入れて「設定」ボタンを押すと、MACアドレス制限ができちゃう。

「鉄壁」には一歩足りないが無防備な人は今すぐ使うべき

三：MACアドレス制限は、設定の中でも特に面倒だからね。この機能に対応したアクセスポイントが増えるといいなぁ。

次のバージョンアップでぜひ！

山：「WEPキーの設定」と「MACアドレス登録」「アクセスポイントを隠す」など、主要なセキュリティー機能が設定できていました。ほぼ「鉄壁」と呼んでいいと思いますよ。だけど、ESS-IDが変更できない点と、アクセスポイント自体のパスワード設定ができないのは、ちょっと物足りない。「鉄壁」と言うからには、次のバージョンではこの辺の設定までカバーしてほしい。

三：対応のアクセスポイントはどうかな？

山：徐々に増えると思うけど、発売時に対応しているアクセスポイントは、まだまだ数が少ない。アップデートで対応アクセスポイントを増やす予定というから、サポートをがんばってほしいところですね。

三：無線LAN以外の部分のセキュリティー設定もやってほしいなぁ。無線LANとブロードバンドルーターの複合機では、ルーター部分のセキュリティー設定もできると、さらに良くなるね。

山：シリーズで「鉄壁 ホットスポット」ができるといいですね。ホットスポットの中には、ほかのコンピュータが見えてしまうところもありますし。

交差点ごとにアクセスポイント発見

三：それにしても、思ったよりも無線LANって普及してるんだねぇ。

山：毎月、数十の無線ホットスポットを回ってますが、「意図しない無線ホットスポット」が多数見つかりますよ。無線LANで使われている電波（2.4ギガヘルツ帯/802.11b）って、壁とか天井みたいな遮蔽物があるとすぐ減衰するけど、遮蔽物がなければ意外と遠くに飛ぶ。1階の窓際にアクセスポイントを置いている人は要注意。

三：たぶん、まだ危機意識すらないんだと思う。この前、バスに乗ってるときにアクセスポイントを探してみたけど、交差点でとまるたびにアクセスポイントが見つかるような状態だった。中には会社っぽい無防備なアクセスポイントがあったけど、非常に危険。社員が勝手にアクセスポイントを立てるのは厳禁だね。

無線LAN、ホットスポット担当の山本浩司。日本各地の無線ホットスポットを取材して回る

［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