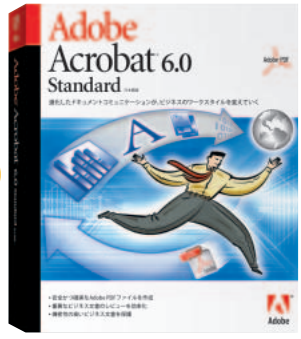
文書の電子化と共同作業を強力にサポート

Adobe Acrobat 6.0 Standard 日本語版

7月4日発売予定

アドビシステムズ

アドビストア提供価格：34,800円（通常版）、12,500円（アップグレード版）



Standardのパッケージ。ウィンドウズ版とマッキントッシュ版が用意されている。

4つの製品で構成される新Acrobatファミリー

現在、インターネットで配布される多くの文書にPDF形式が使われている。最近では納税申告書もPDF化され、国税庁のウェブサイトなどからダウンロードできるようになった。いまやPDF形式は多くのパソコンユーザーにとって必要不可欠な存在で、ほとんどのパソコンにPDFファイルを表示する「Adobe Acrobat Reader」がインストールされている。

いま書いている原稿の校正刷りも、以前はFAXで送られてきたものだが、いつのころからか電子メールにPDFファイルが添付されるようになった。Acrobat Readerでそれを印刷して修正を入れ、FAXで編集部に送り返してもいいが、「Adobe Acrobat」があれば校正作業の効率はさらにアップする。開いたPDFファイルをAcrobat上で修正し、必要に応じてコメントを付けてメールで返信するのだ。

Acrobat 6.0は、PDF化の作業がより簡便化されると同時に、こうした共同作業を行うための機能が大幅に向上した新バージョンだ。使用目的に応じて「Acrobat Professional」「Acrobat Standard」「Acrobat Elements」の3つの製品に分かれたことも、バージョン6.0の特徴だろう。名前が示すとおり「Standard」がもっとも標準的な製品で、「Professional」にはそこにより専門的な機能が追加されている。

「Adobe Reader」と名前を変えてPDFビューアーもバージョンアップ

ここでは、新Acrobatファミリーのそれぞれの製品について解説する。「Professional」では、エンジニアリングのプロ向けに「Autodesk AutoCAD」や「Microsoft Visio」などで作成した文書からワンクリックでPDFファイルを作成できる機能が加わった。また、デザインのプロ向けにはアドビの「Photoshop」や「InDesign」などのグラフィック用アプリケーションとの連係機能や色分解のプレビュー機能を備えている。

「Elements」は大量購入する企業ユーザー向けの製品だ。「Standard」からオンライン共同作業用の機能や編集・加工機能などを取り除き、マイクロソフトオフィス文書のPDF化を中心に機能が絞り込まれている。

無償でダウンロードできる「Adobe Acrobat Reader」も同時にバージョンアップした。ただし、「Adobe Reader」と名称を変更。アイコンやユーザーインターフェイスが一新されたばかりでなく、複数PDFファイルの検索機能や電子署名検証機能、eBook閲覧機能など、機能が大幅に強化されている。

必要に応じて多彩な方法で文書ファイルをPDFに変換

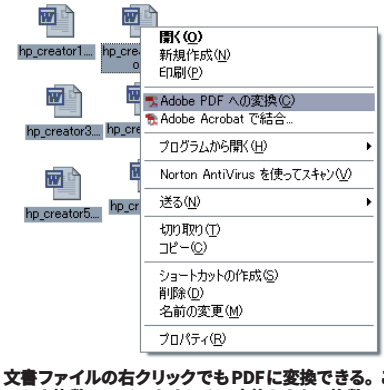
基本的に、印刷可能なアプリケーションであれば、どんなものでもPDFに変換できる。変換を行うのはAcrobatに含まれる「Distiller」というプログラムだが、ユーザーはプリンター一覧からこのDistillerを選んで印刷を実行すればいい。バージョン6.0では、このプリンターの名前がDistillerから「Adobe PDF」というわかりやすい名前に変わっている。

一部のアプリケーションに限られるが、アプリケーションのツールバーにあるPDFアイコンをクリックしてPDFファイルを作ることもできる。すでにバージョン5.0から、Word、Excel、PowerPointがこの機能に対応していたが、バ

■ Acrobat 6.0ファミリー3製品の機能比較表

機能	Elements Win版のみ※	Standard Win版/Mac版	Professional Win版/Mac版	注意事項
マイクロソフトオフィス/インターネットエクスプローラとの連係	○	◎	◎	Mac版は一部未対応
エンジニアリングユーザー向けPDF作成機能	×	×	◎	Mac版は未対応
その他のPDF作成	△	◎	◎	Mac版は一部未対応
使いやすいユーザーインターフェイス	○	○	◎	
共同作業機能（文書のチェックと注釈）	×	○	◎	Mac版は一部未対応
編集・加工	△	○	◎	
PDF文書の検索	○	○	◎	
電子フォーム	△	○	◎	
信頼性の向上・セキュリティーの強化	△	◎	◎	Mac版は一部未対応
アクセシビリティー対応	△	○	◎	Mac版は一部未対応
デザインのプロ向け機能	×	△	◎	
スキャナー/OCR機能	×	◎	◎	

◎対応　○ほぼ対応　△一部対応　×未対応
※1000ライセンス単位のライセンス販売のみ



文書ファイルの右クリックでもPDFに変換できる。このとき複数ファイルをまとめて変換したり、複数ファイルを1つのPDFファイルに変換（PDFバインダー）したりできる。

ージョン6.0からはインターネットエクスプローラ（Elementsを除く）やAutoCAD、Visioなどにも（Professionalのみ）この機能が加わった。さらに新バージョンでは、アプリケーションを起動せずに文書ファイルを直接PDFに変換することもできる。右クリックで表示されるポップアップメニューから、「Adobe PDFへの変換」を選べばいい。Acrobatウィンドウに文書ファイルをドラッグ&ドロップしても、PDFへの変換が可能だ。これら2つの方法では、複数ファイルを一度にPDFに変換することもできる。

従来のAcrobatにはなかった便利な機能に「PDFバインダー」がある。この機能を使えば、複数の文書ファイルをまとめて1つのPDFファイルにすることができる。

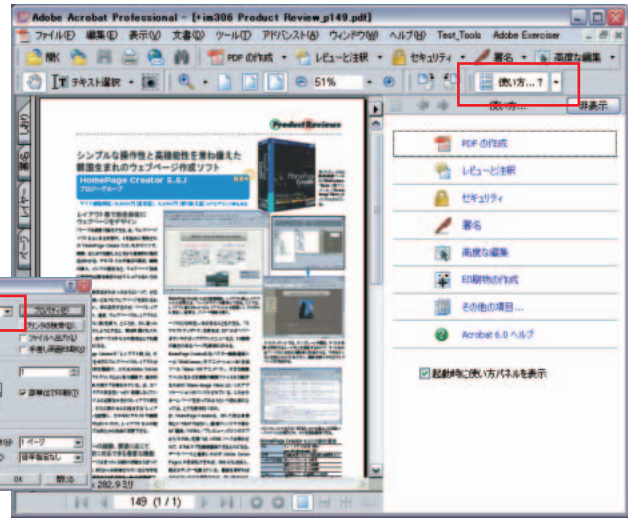
文書のオンライン共同作業とデータベース化を強力にサポート

従来のAcrobatも注釈機能を備えていたが、バージョン6.0ではそれが強化され、よりわかりやすい注釈が付けられるようになった（Elementsを除く）。たとえば、選択範囲の表現を別の言葉に置換するのか、削除するのか、あるいは他のメンバーの確認を求めるのかといったことがひと目でわかる。

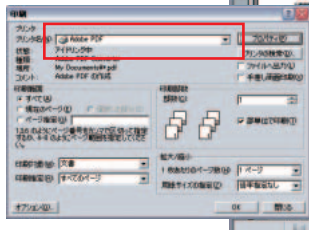
加えられた注釈は、Acrobatウィンドウ左にある「注釈」タブをクリックすれば、ウィンドウ下部にまとめて表示される。だが、共同作業に参加する人数が多くなれば、注釈の管理も煩雑になる。これを解消し、レビューを効率化してくれるのが「レビュートラッカー」機能だ（Elementsを除く）。レビュートラッカーは、PDFファイルを送ったメンバーのリストを作り、挿入された注釈に対してコメントが返されたかどうかをチェックしてくれる。PDFには「重要」「極秘」「承認済み」などのスタンプの押印やデジタル署名を付けることも可能だ。

また、スキャナーから取り込んだ画像をPDF化する機能では、バージョン6.0でさらにOCR機能が加わった（Elementsを除く）。これにより、FAXなどデジタルデータのない文書もPDF化することで検索でき、他のデジタルデータと一緒に管理できるようになる。検索の精度を上げるには手作業でデータを修正しなければならないが、OCR専用のアプリケーションを用意しなくてもこうしたことができるのはありがたい。

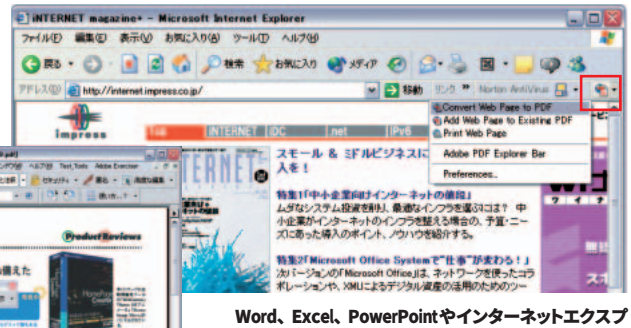
Acrobat 6.0は、さまざまな場面を想定して、数多くの機能を備えている。Acrobat 6.0を導入すれば、文書一括管理の準備は万端。成否は、利用する側がこれを十二分に使いこなせるかどうかにかかっている。（藪 暁彦）



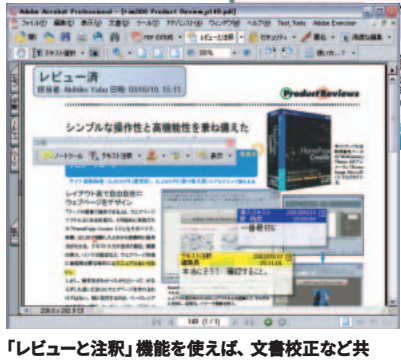
ユーザーインターフェイスも一新されたAcrobat 6.0。ツールバーの「使い方...?」をクリックすれば、ウィンドウ右にヘルプメニューが表示される。



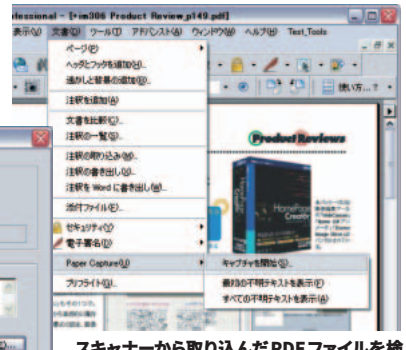
文書ファイルをPDFに変換する方法はいくつも用意されている。その1つは印刷。プリンターから「Adobe PDF」を選んで印刷すればいい。



Word、Excel、PowerPointやインターネットエクスプローラなどでは、ツールバーのPDFアイコンをクリックすればPDFに変換できる。ウェブページの変換では、CSS（カスケードスタイルシート）やフォームも取り込める。



「レビューと注釈」機能を使えば、文書校正など共同作業を電子化できる。テキストの修正、置換、挿入や、ポップアップノートに注釈も付けられる。



スキャナーから取り込んだPDFファイルを検索可能なファイルに変える方法は簡単で、「文書」-「Paper Capture」を選ぶだけでいい。

Acrobat 6.0 Standard 日本語版の動作環境

OS	ウィンドウズNT Workstation 4.0 SP6/2000 Professional SP2/XP/XP Tablet PC Edition/98SE、MacOS 10.2.2以上
CPU	Pentiumクラス、PowerPC G3以上
メモリー	64MB以上（128MB以上推奨）
ハードディスク空き容量	250MB以上（ウィンドウズ）、360MB以上（MacOS）
ディスプレイ	解像度800×600ピクセル以上
その他	CD-ROMドライブ、インターネットエクスプローラ5.0.1以上（ウィンドウズ）
参考URL	http://www.adobe.co.jp/
問い合わせ先	03-5350-0407

デュアルバンドPCカードもラインナップ 802.11g無線LANの新シリーズ

WN-G54/AXP

発売中

アイ・オー・データ機器

ダイレクトショップ価格：12,800円

WN-A54/AXPとは打って変わってごく標準的な弁当箱デザインだ。表示のLEDは側面からも見えるように光を誘導してあるが、やや暗く見づらいのが難点。ACアダプターはコンパクトでありがたい。

WN-G54/AXPは純粋なアクセスポイントなので、背面もシンプル。

802.11gでは後発だが設計には自信

アイ・オー・データ機器から、802.11g対応の54Mbps無線LAN「WN-G54」シリーズが発売された。製品ラインとしては、802.11gドラフト対応の無線LANアクセスポイント「WN-G54/AXP」、アクセスポイント内蔵ブロードバンドルーター「WN-G54/BBR」、PCカードアダプター「WN-G54/CB」が用意された。さらに802.11a/g両対応のPCカードアダプター「WN-AG/CB」が加わるほか、アクセスポイント、ルーターとPCカードのセットも用意されている。すでに発売済みの802.11a対応無線LANシリーズと合わせて、802.11a/b/gの無線LAN規格すべてに対応する製品が揃ったことになる。アイ・オー・データ機器では、これらの3つの規格をユーザーの環境に合わせて「選べる」ことを重視していく。

802.11g対応無線LANでは他社に出遅れた感があるが、そのぶん完成度は高いと見ていい。同社のニュースリリースでは「本製品『WN-G54シリーズ』は、この正式規格（IEEE802.11gのこと：筆者注）にも、確実に対応できるハードウェア設計となっています」と明記されており、設計に対する自信がうかがえる。6月に正式決定される802.11g規格への対応という点で、安心できる文言だ。もちろんWi-Fiへの対応も予定している。

上がWN-AG/CBで、下がWN-G54/CB。WN-AG/CBのほうが出っ張り部分にやや厚みがあるが、デュアルバンドだから致し方ないか。無線LANはむしろアンテナの性能がポイントだ。

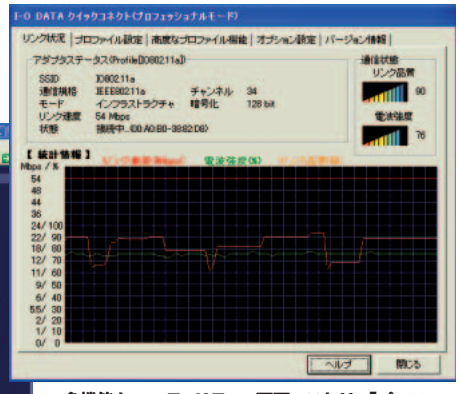
また、802.11a/b/gの3規格に対応したデュアルバンド無線LANカードが手にとりやすい価格で発売されたことにも注目したい。同社の802.11a無線LAN製品をすでに購入して使っているユーザーにも朗報だ。

設定変更も電波状態の確認も切り替え自在の「クイックコネクト」

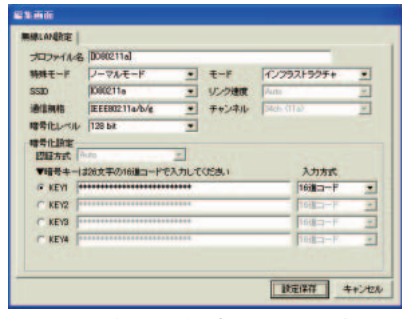
新デザインのアクセスポイント「WN-G54/AXP」は弁当箱タイプのシンプルな設計だ。1本伸びるダイバーシティーアンテナがポイントで、アクセスポイントとしては標準的なスタイルである。設定はブラウザーを使う。ウィザードなどは用意されていないため、ある程度自力で設定しなければならないが、決して難しくはない。また、他社製品に見られるような特殊な「Turboモード」などの互換性設定はない。

一方、無線LANカードは機能が豊富だ。OSのドライバーとともに、専用ユーティリティー「クイックコネクト」が付属する。SSIDやWEPなどのプロファイルを複数設定して保存でき、タスクトレイのアイコンから簡単に切り替えて使える。また、アクセスポイントの検索や、電波やリンクの状態をグラフ表示で確認できる画面もあって非常に便利になっている。欲をいえば、IPアドレスも表示してほしかった。ウィンドウズXPのユーザーはこのユーティリティーがなくても無線LANを使用できるが、ぜひとも利用をおすすめしたい。

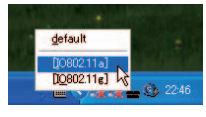
WN-G54/AXPの基本設定画面。内容はごく標準的だ。



多機能なユーティリティー画面。これは、「プロフェッショナルモード」の画面だ。電波状態など細かく状態を把握できるのがうれしい。アクセスポイントのサーチ機能もある。



SSIDやWEP暗号化などをプロファイルに設定しておくと、簡単に接続先の切り替えができる。



802.11a/gはタスクトレイの専用ユーティリティーで切り替える。802.11aとgのアクセスポイントに同じSSIDを設定してある場合は、802.11aが優先的に選ばれる。

スループットでは802.11aに軍配

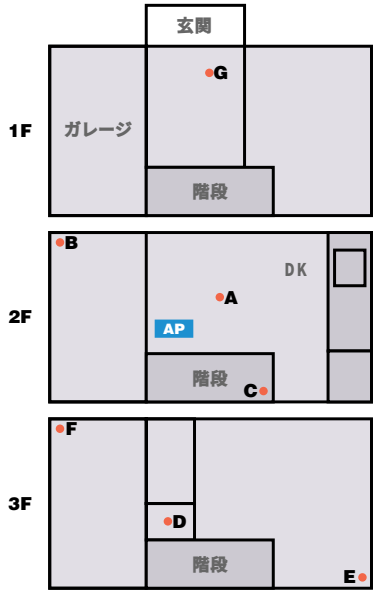
同社の802.11a対応無線LANアクセスポイント「WN-A54/AXP」と「WN-G54/AXP」を使って802.11gとaのスループット、電波の届く範囲、電子レンジの影響についてそれぞれテストした。まず、スループットの調査では、有線側のFreeBSDサーバーへftpコマンドを使って30Mバイトのファイルを送信するテストを行ったところ、802.11a（WN-A54/AXP）が2700Kバイト/秒と802.11g（WN-G54/AXP）に比べて15パーセント高いスループット値を示した。802.11gは802.11bとの互換性を担保するために、どうしても802.11aには敵わないといわれているが、まさにそのままの結果が出た。

また、3階建ての一戸建ての各所で同様のスループットを測定したのが右のグラフ。802.11aがF地点で1割程度スループットを落としているのに比べて、802.11gではわずかな低下だけだ。電子レンジの影響のテストは無線LANカードとアクセスポイントを2メートル離し、その間に電子レンジを置いて測定した。802.11aではまったく影響を受けていないのに対して、802.11gではスループットが2割程度まで落ち込んだ。全体的に、802.11aがよい結果を残している。

スループットと安定感で802.11a 通信距離と互換性で802.11g

今回の試用では、ほとんどの結果で802.11aに軍配が上がった。遮蔽物の少ない小さな家では間違いなく802.11aのほうが性能が出せるということだ。となると、802.11aを選んだほうがよいのだろうか？ 大きな一軒家や機密性が高くコンクリートの厚いマンションなどでは、今回のテスト結果とは異なり、電波の届きのよさ

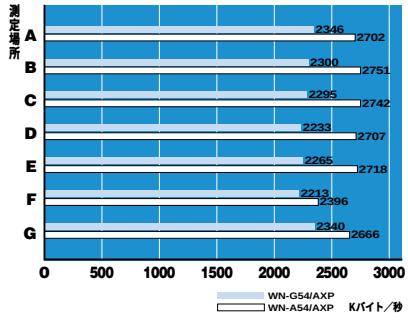
■ スループット測定の場所



という点で802.11gのほうが優れている。また、802.11gは屋外でも使用でき、無線LANスポットなどで使われている802.11bとの互換性もある。電子レンジの影響は気になるが、使用しているのは短時間だけだから問題はない。802.11aとの性能差が思ったほど大きくないこと、価格差なども考慮するなら、やはり選択肢は802.11gだ。ただ、少しでもスループットを高くしたいユーザーや、すでに家の周りにアクセスポイントのある家が多くて電波が混んでいる、802.11gと併用してスループットを稼ぎたいオフィス使用などでは802.11aを選んだほうがよいケースもある。どちらにしても、無線LANカードにはぜひともデュアルバンド（802.11a/b/g）のものを1枚買い揃えてほしい。これさえあれば、会社でも自宅でも、友人宅やホットスポットでも多様に無線LANが使いこなせることは間違いない。確実に長く使える無線LANカードになるはずだ。　（梅垣まさひろ）

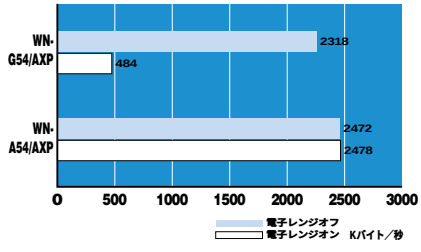
802.11aに対応したアクセスポイント「WN-A54/AXP」は、まったく異なるデザイン。アクセスポイントと電源供給ユニット、有線LANポートが分離されているので、設置の自由度も高い。

■ftpスループット結果



WN-A54/AXP（802.11a準拠）とWN-G54/AXP（802.11gドラフト準拠）を使って屋内でのスループットを比較した。A地点がアクセスポイントに一番近い。いずれもF地点でもっとも低い値が出ているが、802.11gではA地点との差はわずかだ。

■電子レンジの影響



アクセスポイントとの距離は2メートル。間に、電子レンジを置いて測定したスループットだ。802.11gは電子レンジと同じ2.4GHzの周波数のため影響を受けやすい。

WN-A54/AXP

無線LAN	802.11g（draft規格）準拠
暗号化	WEP64/128ビット
セキュリティー	MACアドレスフィルタリング
消費電流	440mA
外形寸法	幅約38×奥行き120×高さ171（mm）
重量	約300g（本体のみ）
参考URL	http://www.iodata.co.jp/
問い合わせ先	東京 03-4288-1039　大阪 06-4705-5544

■WN-G54シリーズ製品ラインナップ

種別	型番名称	販売価格
802.11g対応PCカードアダプター	WN-G54/CB	6,980円
802.11g対応無線LANアクセスポイント付きブロードバンドルーター	WN-G54/BBR	16,800円
802.11a/g/b対応PCカードアダプター	WN-AG/CB	9,180円
セット品（「WN-G54/AXP」「WN-G54/CB」）	WN-G54/AXP-S	19,200円
セット品（「WN-G54/BBR」「WN-AG/CB」）	WN-G54/BBR-S	24,500円

ルーター部を分離して置き場所を選ばない シンプルな802.11g無線LAN

PCWA-AR300

ソニー

5月31日発売予定

実売価格：25,000円程度

白色に光るアクセスポイント（右）は壁掛けもOK。ルーターユニット（左）は、WANポート1つ、LANポート3つ、アクセスポイント専用ポート1つと電源コネクターを持つ。
※本記事は開発中のもので試用

バイオの周辺機器から脱皮した無線LAN製品

ソニーのCarrierGateシリーズ無線LANに、802.11g（ドラフト規格）対応機が新たに加わった。ソニーは、802.11aから11gへ移行するのではなく、aとgの各々の利点、欠点を理解して使い分けるのがベストだと提案する。802.11aは高速なうえに電子レンジなどの干渉問題もない。一方802.11gは802.11bと互換性があり、また通信距離も伸ばせるという利点が捨てがたい。ユーザーはこれらの点を理解して環境に合った製品を選ぶべきだという考え方だ。

また、ソニーはCarrierGateシリーズをバイオの周辺機器から脱皮させ、他社製パソコンや他社製無線LANとも積極的に組み合わせられるようにサポート体制作りを進めている。バイオユーザーだけの無線LANという位置付けを打ち破る意欲だ。さらに、同シリーズのコンバーター「PCWA-DE30」を使えば、イーサネットポートを持ったネットワーク機器（たとえばPS2など）をワイヤレス化できる。

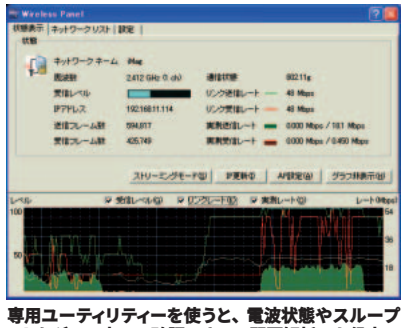
今回試用したのは、開発中のブロードバンドルーター「PCWA-AR300」とワイヤレスLANカード「PCWA-C300S」だ。PCWA-AR300のルーターユニットに802.11a対応のアクセスポイント「PCWA-A520」を接続すれば、802.11a/gのデュアルバンド対応に拡張できる。

アクセスポイントの詳細設定画面。「IEEE 802.11モード」では、「11gと11b」「11gと11b」（高マルチキャストレート）、「11gのみ」が選択できる。

スループットは約20Mbps 動画対応の小技がソニーらしい

PCカードとアクセスポイントのインストールや設定は、付属する「簡単インストールウィザード」の指示に従うだけで簡単。アクセスポイントの設定では自動的にブラウザーが開くので、「おまかせ設定」を選べば手順はスムーズだ。ルーターの設定はブラウザーを使って設定画面を開く必要があるが、こちらもシンプルで「DHCPを使った接続」「PPPoEを使った接続」「マニュアル設定」のどれかを選ぶ。

有線側に置いたFreeBSDサーバーへftpコマンドを使ったスループットの測定テストをしたところ、木造3階建てのすべての場所で約20Mbpsのスループットが得られた。以前に測定した802.11aに比べて1割程度速度は劣るが、屋内のアクセスポイントからもっとも離れた場所でも19Mbps程度だった。また、802.11bのAirMacを搭載したiBookから、サーバーにpingを飛ばしながらftpのスループットを計測したが、速度の低下はわずかだった。iBookからftpしながら測定するとスループットは半分程度になったが、同時に転送していれば帯域を半分ずつ利用することになるのでこれは問題ない。また、アクセスポイントに「11gと11b」（高マルチキャストレート）というモードがあり、これでもftpでのスループットに変わりはなかった。これは、主に動画のスループットやコマ落ちを防ぐ機能なので、ftpでの値には表れなかったのだろう。



専用ユーティリティーを使うと、電波状態やスループットをグラフ表示で確認できる。問題解析にも役立つ強力なユーティリティーだ。

左から電源アダプター、ルーターユニット、ワイヤレスユニット（アクセスポイント）。この製品から電源アダプターには電源スイッチが付いた。

ソニーならではのデザインのよさだけでなく、使い勝手、性能ともに満足できる無線LANだといっていい。なお、802.11g規格の正式決定後はファームウェアのアップデートで対応するほかWi-Fiも認定を受ける予定だ。（梅垣まさひろ）

CarrierGate 802.11g（2.4GHz）無線LANラインナップ

アクセスポイント（ブリッジタイプ）「PCWA-A320」	実売価格20,000円程度
無線LANカード「PCWA-C300S」	実売価格10,000円程度
コンバーター「PCWA-DE30」	価格未定

※PCWA-DE30のみ6月28日、ほかは5月31日発売予定

PCWA-AR300

無線LAN	802.11g（draft規格）準拠
暗号化	WEP64/128ビット
セキュリティー	MACアドレス登録、SSID公開選択機能
ルーター機能	UPnP、DHCPサーバー、DHCPクライアント、PPPoE、VPNパススルー（IPsec/PPTP）
消費電力	約10W
【ワイヤレスユニット】	
外形寸法	幅98×奥行き33×高さ98（mm）
重量	約320g
【ルーターユニット】	
外形寸法	幅200×奥行き32×高さ69（mm）
重量	約340g
参考URL	http://www.vaio.sony.co.jp/Products/CarrierGate/

無線LANと指紋認証機能をPDAに標準搭載

hp iPAQ Pocket PC h5450

5月中旬発売

日本ヒューレット・パッカード

hp directplus価格：69,800円

全体的には従来のiPAQのデザインを継承している。拡張ジャケットでカードスロットを追加する「ジャケットコンセプト」も同様で、コンパクトフラッシュなどを使う場合はジャケットを別途購入する必要がある。
※製品版は多少機能が異なる可能性がある

「無線LAN機能搭載」はPDAの限られた拡張スロットを救う

2003年に入り、東芝の「GENIO e550」、カシオの「カシオペア e-3000」など、PDA用OS「Pocket PC 2002 日本語版」と、高速、低消費電力CPU「XScale PXA250/400MHz」を搭載したPDAが続々とリリースされている。そしてその最後を飾るのが、「iPAQ Pocket PC h5450」（以下h5450）だ。「GENIO e550」がデジタルカメラ機能を搭載、「カシオペア e-3000」が約30時間のずば抜けた長時間駆動という特徴を前面に打ち出しているなかで、対するh5450の最大の特徴は標準でIEEE 802.11b対応の無線LAN機能を内蔵している点だ。

従来のPDAで無線LANを利用しようとすると、コンパクトフラッシュ型の無線LANカードなどを利用し、それでなくとも少ないPDAの拡張スロットを常時1つ潰す必要があった。たとえば、コンパクトフラッシュメモリーカードなどに楽曲データを集めてPDAで聞く場合、一度無線LANカードを外して差し替えなければならず、きわめて面倒だった。無線LANの標準搭載は、空いたスロットを「メモリー専用」などに活用でき、ほかのPDAにはない最大のメリットだ。

ちなみに、OSのバージョン、CPU、液晶画面などの無線LAN機能以外のハード部分は、2002年11月に国内発売されたh3970から大きな進化はない。強いて挙げるとすれば、操作ボタンが横長のものから小さなボタンに変わった点やバッテリーが脱着式になったくらいだ。ただ、h3970はBluetooth、CPU/400MHz、64Mバイトの内蔵メモリー、240×320ドットで6万5536色のTFT液晶ディスプレイなどを装備し、現在発売されているPocket PCの中で最高スペックを誇る製品なので、「半年前の製品をベースにしていてちょっと性能が心配」ということもないだろう。

操作ボタンが横長から丸い形に変わったことで、片手での操作が若干楽になっている。指紋認証は操作ボタンの下のスキャナーで行う。

「指紋認証」など近未来PDAの標準を提示する

実際の無線LAN機能の使い勝手だが、これが非常に使いやすい。これまでPDAで無線LANを使う場合、ユーティリティーをダウンロードしてインストールするなど、実際に使えるようにするまでにハードルの高い操作が必要だった。h5450の場合、それらの操作は「iPAQ無線LAN」というソフトウェアから行う。また、ソフトウェアをメニューから立ち上げなくても、画面下のバーのアイコンをクリックするだけで設定画面が立ち上がるため、そのぶん設定の手間も省ける。さらに複数の無線LANアクセスポイントを「会社用」「フリースポット用」と登録しておけば、ツールバーからすぐに設定を変更できて便利だ。無線LAN機能のオン／オフもここで切り替えられ、通信しないときはオフにしてバッテリーを節約するという使い方もできる。

もう1つ、このマシンの特徴的な機能が、操作ボタンの下にあるスキャナーに指をこすりつけて実行する「指紋認証機能」だ。テスト機だったためか、自分の指紋の認識率が少々低かったが、モバイルユースで紛失の可能性が高いPDAには有効な機能だといえるだろう。このように先進的な機能を追加したh5450は、近未来のPDAの姿を実際の製品として提示したものと考えてもいいのではないだろうか。　（編集部）

画面下のバーからすぐに無線LANの設定や切り替え、オン／オフができる。

「指紋」の登録は表示された動画のように指をスキャナーにこすりつけて行う。うまく認識させるにはちょっとしたコツが必要。

hp iPAQ Pocket PC h5450

CPU	PXA250-400MHz
メモリー	64MB（RAM）、48MB（ROM）
バッテリー	充電式リチウムポリマーバッテリー
インターフェイス	SDメモリーカード／MMCカードスロット、赤外線
本体寸法	幅84×奥行き16×高さ138（mm）
重量	約206g（バッテリー含む）
参考URL	http://www.hp.com/jp/

クライアントの手間不要 ウィンドウズのアップデートを集中管理

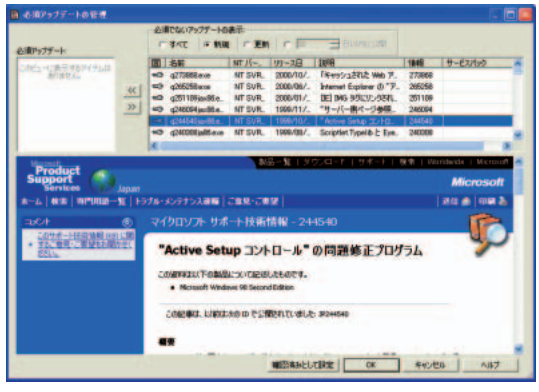
アップデート エキスパート

アップデートテクノロジー

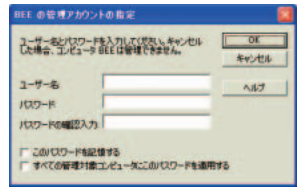
発売中

推定小売価格：268,800円（1年間／100台ライセンス）

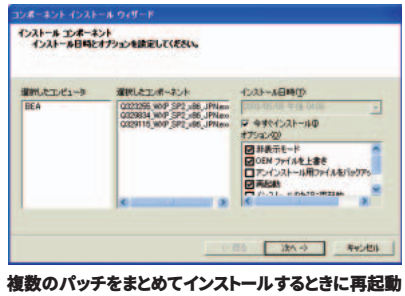
アップデートエキスパート起動画面。選択しているアップデート情報ではアップデートテクノロジーから注意を促す情報が提供されている（下ペインのブラウザー画面参照）。



必須アップデートの管理画面。マイクロソフトから特に「必須アップデート」として提供されているものをまとめて管理できる。



管理者アカウント入力画面。アップデートエキスパートでは管理者アカウントで対象となるPCにログオンして作業を行うので、あらかじめ登録しておく必要がある。



複数のパッチをまとめてインストールするときに再起動を一度に省略できる「Q Chain」と呼ばれるDOSツールがマイクロソフトから提供されているが、同様の操作がGUIで行える。

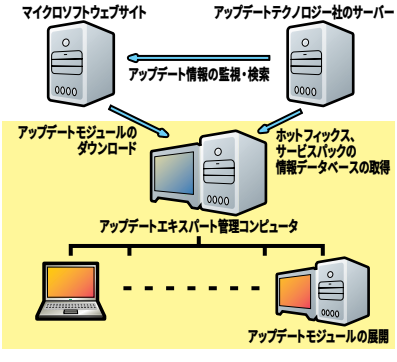
複数PCのウィンドウズアップデート作業を自動化

セキュリティー対策といえば、ウイルス対策ソフトやファイアーウォールの印象が強いが、根本的な解決はパッチやサービスパックなどで問題の原因となる“穴”をふさぐことにある。

「アップデートエキスパート」はネットワークでつながった複数のウィンドウズマシンのOSやマイクロソフトオフィスのアップデート管理を1台のPCで行うツールだ。OSやソフトの各バージョンごとのパッチやサービスパックを1か所（管理コンピュータ）にまとめてダウンロードし、管理対象のクライアントに合わせて必要なものをコピーしてインストールする。アップデート内容によっては、対話形式での応答やインストールCDが必要になるが、応答操作やインストールCDの位置をあらかじめ設定しておけば、アップデート作業を自動化できる。100台、200台のマシンに対しても、管理者は適用したいアップデートを指定して必要な設定を一度行うだけでいい。

アップデート作業では管理対象のマシン側に特別なスレーブプログラムをインストールする必要はない。またアップデートは管理者権限でログオンして行うため、アップデート作業をユーザーに止められる危険も少ない。インストール状況については失敗・成功ともにログが採れるほか、リモートでの検証もできる。

■システム構成例



パッチにも独自の検証を行う大規模システム管理者向き

アップデートエキスパートをインストールしたマシンは、アップデートテクノロジー社のサーバーから24時間体制で提供される各パッチやサービスパックに関する情報を受け取る。この情報はマイクロソフトの情報ページへのリンクやアップデートテクノロジー社独自の検証情報、カテゴリー付けなどが含まれ、パッチを導入すべきかどうかの判断を助ける内容になっている。

全OS共通のパッチは1か所で選択して一度インストールを実行すれば、選択しているマシンすべてに適用できる。OSのバージョンごとに違うパッチが提供されている場合でも、各マシンに合わせて自動的にパッチをコピーして適用してくれる。この機能は特に緊急度の高いセキュリティーのパッチをあてたいときなどに役に立つだろう。

本ソフトウェアの最大の魅力はアップデート作業の自動化だろう。筆者はウィンドウズ2000をインストールしたあとにサービスパックやパッチの適用作業で半日かかった経験がある。自動的に何もかもできればいいが、何度となくマシンは再起動して応答とCDを要求するため、マシンの前を離れられない。これらの手間を省略できるだけでもこのツールは十分に存在価値がある。指定したPCすべてに対して自動でインストールできるため、省力化効果も非常に高い。（井上繁樹）

アップデート エキスパートの動作環境

対応OS	ウィンドウズNT4.0/2000/XP Pro ※サーバー版含む
CPU	Pentium～Pentium II 300MHz以上（OSに依存）
ハードディスク空き容量	20MB以上（インストールするパッチプログラムやサービスパックに応じてさらに容量が必要）
メモリー	256MB以上
ブラウザー	インターネットエクスプローラ5.5以上
ネットワーク	TCP/IPプロトコル
ディスクフォーマット	NTFS
参考URL	http://www.updatecorp.co.jp/ ※ウェブサイトに15日間限定体験版あり

ネット経由でファイルを復元・修復・完全抹消できる

FINALDATA 2.0 エンタープライズネットワーク

発売中

アルファ・オメガソフト

定価：78,000円（パッケージ版：5エージェント付き）

法人向けには、人事異動やPCの廃棄のためにディスクを完全に抹消できる「TERMINATOR パーフェクト」をセットにしたライセンス販売も行っている。

ファイルを削除・破損から守り情報の漏洩を未然に防ぐ

「FINALDATA」シリーズは削除してしまったファイルをディスク上に残された情報をもとに復元するソフトだ。「エンタープライズネットワーク」版では、ファイルの復元以外に、破損ファイルの修復、復元不能な状態にするファイルの抹消の機能が搭載されており、ファイルに関するトラブル全般に対処できる。

フォルダー単位で、削除したファイルの自動バックアップやファイルの保護指定ができるので、不用意なファイル操作から重要なファイルを守ることができる。このほか、セクター単位でディスクイメージを圧縮保存できる。これによりいったんイメージを作成すれば別のPC上でも復元できるので、ハードウェアにトラブルがあった場合の“保険”としても有用だ。

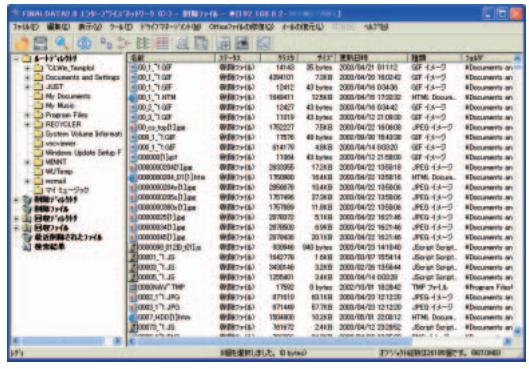
本製品はネットワークに対応しており、スレーブプログラムをインストールしたPCに対してファイルの復元・修復・抹消操作ができる。スレーブプログラムはウィンドウズ用とDOS用の2種類があり、ウィンドウズ用はTCP/IPとIPX/SPXプロトコルに、DOS用はIPX/SPXプロトコルに対応している。DOS用はIPX/SPXプロトコルをインストールしているウィンドウズでも動作は可能だ。ルーターによってはTCP/IPプロトコルのみ対応の製品もあるので、使用の際には注意したい。また、インストールCD上から直接起動できるので、本ソフトウェアのインストールのためにディスク上に残されたファイルの痕跡を壊す危険も回避できる。

データドライブは分割が必要ファイルの抹消機能は強力

「FINALDATA」ではファイルの復元前に一度ドライブ全体を走査し、復元できないものも含めてファイルリストを作成する。このため、ドライブ容量が大きいと膨大な時間がかかる。80Gバイト以上のドライブでは16時間との表示も出た。ファイルを保存しておくドライブは容量を少な目に設定しておくほうが効率的だ。走査範囲はクラスター単位で設定できるので、ファイルがどのあたりに書き込まれているかを予測できるならより効率的だ。またファイルの復元には、別途復元先のドライブが必要になるため、1ドライブ1パーティションのPCではネットワークドライブを接続するなどの工夫がいる。

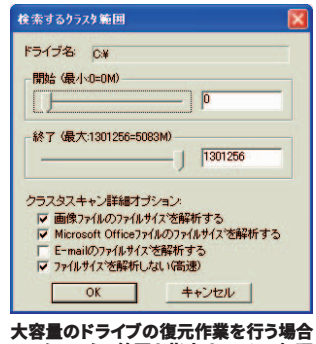
本ソフトにはいわば“盾と矛”にあたる、ファイルの復元機能と抹消機能の2つが搭載されているが、結論からいうと“矛”にあたる抹消機能のほうが強い。抹消機能は効果に応じて米国国防総省の規定準拠のものも含めて6レベルが設定されていて、初期値のレベル3でも他社の復元ソフトでは復元不能になった。

ネットワーク対応機能はスレーブプログラムを起動してパスワードを設定しておけば使える手軽なものだ。ファイアーウォールを設定していないかぎりシステムドライブも含めて内容が見えてしまうので、扱いは慎重にしたい。削除済みのインターネット一時ファイルも確認できてしまうほどだ。（井上繁樹）



ウィンドウズXP上からウィンドウズ2000のCドライブにアクセスしたところ。

プレビュー機能を使うとTXT、JPG、BMPなど対応している形式のファイルは復元前に確認できる。それ以外のファイルではダンプ表示で確認することになる。



大容量のドライブの復元作業を行う場合は、クラスター範囲を指定することで処理の高速化ができる。

ウィンドウズ用スレーブプログラムの画面。「FINALDATA」を使ってリモートアクセス中のマシン名やIPアドレスが確認できる。

FINALDATA 2.0 エンタープライズネットワークの動作環境

対応OS	ウィンドウズ95/98/Me/NT4.0（SP4以上）/2000/XP ※サーバー版含む
メモリー	64MB以上（128MB以上推奨）
ディスプレイ	解像度640×480ピクセル、256色以上
ネットワーク	TCP/IPプロトコル（DosSlave使用の場合はIPX/SPXプロトコル）
参考URL	http://www.finaldata.ne.jp/

常時接続で増える“危険”から身を守る

ファイアーウォール＆IDSを導入する

常時接続があたりまえになった現在、会社のネットワークにかぎらず、個人宅のパソコンまでもが無差別に攻撃を受けている。インターネットのセキュリティー対策は身近なもので、決して他人事ではないのだ。セキュリティーを高めようとする場合、ルーターが備えるパケットフィルタリングやウイルス対策ソフトが思い浮かぶが、それだけでは十分ではなく、不正侵入検知などの機能を持つファイアーウォールも重要になっている。（大澤文孝）

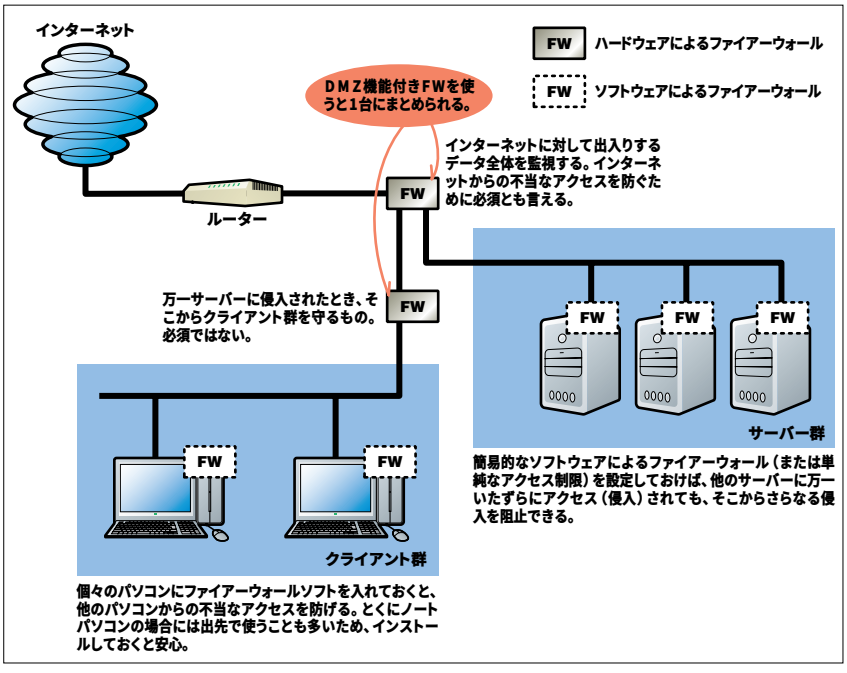
インターネットの脅威に自己防衛で対処する

改めて言うことでもないが、インターネットを使うことは危険と隣り合わせだ。パソコンをインターネットに接続した途端、知らぬ間に外部から攻撃を受け、ウイルスに感染したりパソコンが誤動作したりすることがありうる。とくに近年は、ランダムなIPアドレス宛てに、企業や個人、サーバーやクライアントの区別なく攻撃を仕掛けられることが多いため、サーバーだけでなくパソコンに対するセキュリティー対策もおろそかにできない。

攻撃の対象となるのは、セキュリティー的に脆いサーバーやクライアントマシンだ。サーバーやクライアントマシンが利用しているOSやアプリケーションのなかには、“セキュリティーホール”と呼ばれるセキュリティー上の弱点を持つものも多く、これが標的になりやすい。インターネット上には、セキュリティーホールに対する攻撃を自動化するツールも存在し、これを使うと技術がなくても誰でも簡単に攻撃できてしまうのが実態だ。このため、ウィンドウズアップデートなどを頻繁に確認してセキュリティーホールをふさぐことがもっとも根本的な防衛策になるのだが、サーバーやパソコンの台数が多いとすべてを管理するのは難しく、また未知のセキュリティーホールが存在する場合には対応できない。

そこで重要となるのが、インターネットと通信するデータを常に監視し、不正なデータを流さないようにする仕組みだ。この仕組みを持つものを総合的に「ファイアーウォール」と呼ぶ。以降では、ファイアーウォールの導入のしかたや種類について解説しよう。

■ ファイアーウォールの設置例



ルーターの直後や部署間の接続点に配置する

ファイアーウォールを置く場所は、「管理下にある安全を保ちたいネットワーク」と「管理下にない外部のネットワーク」との間となる。インターネットに接続している場合には、自分のパソコンが接続しているLANと、LANの外部にあるインターネットとの間だ。つまり、基本的にはルーター部分とLANまたは自分のパソコンとの間にファイアーウォールを導入すればよい。またルーター本体やルーター機能付きのモデムを使わずにブリッジ型のADSLモデムなどをインターネットに接続している場合には、パソコン自身にファイアーウォールソフトをインストールすることでも対応できる。

企業の場合には、さらに別の場所にファイアーウォールを置くこともある。たとえば、部署間のデータ漏洩を防ぐために部署間の接続点にファイアーウォールを導入するとか、無線LANアクセスポイントの前にファイアーウォールを設けて、第三者が無線LANを使って入り込めなくするといった対策がある。また、サーバーを設置している場合には、万一サーバーに入り込まれたときに、内部のLANに入り込めないよう、二重のファイアーウォールを備えることもある。

ファイアーウォールを置く場所は、1つとは限らない。最低限インターネットとの接続点には置くべきだが、それ以外にも配置し、二重三重にファイアーウォールを構えることも多い。

データの出入りを監視するファイアーウォールの導入

TCP/IPのネットワークではデータをパケット単位で転送する。このパケットには「(TCPやUDPなどの)プロトコル種別」「IPアドレス」「ポート番号」などのヘッダー情報が記載されている。これらの情報を使って通過させるか拒否するかを決めるのがパケットフィルタリング方式のファイアーウォールだ。

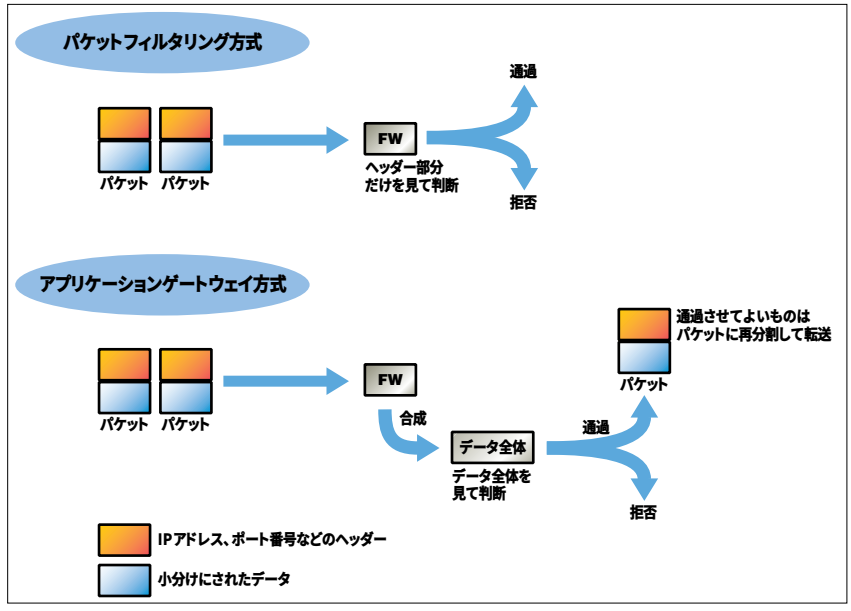
パケットフィルタリング方式は構成が簡単なので、ルーターなどのネットワーク機器にも搭載されている。とくにブロードバンドルーターで使われるIPマスカレード機能は、「LANからインターネットへの通信はできるが、要求がないかぎりインターネットからLANへはデータを送らない」という一種のパケットフィルタリング的な機能も果たす。このため、IPマスカレードでインターネットに接続していれば、比較的安全な状態になっていると言える。

しかしパケットフィルタリング方式では、データの内容を判断材料としないため、不正な命令やデータが含まれているかどうかで通過／拒否を決めるといったことはできない。これに対して、アプリケーションゲートウェイ方式のファイアーウォールでは、データの内容まで調べて通過／拒否を決める。このためウイルスなどの不正な命令やデータが含まれているかどうかの判断ができ、さらには不正なデータ部分を除去して通過させることもできる。

アプリケーションゲートウェイ方式は、データの流れ全体を判断する必要があるため、大がかりなものとなる。よって、専用のハードウェアやソフトウェアで構成される。ちなみにパソコンにインストールして使うウイルス対策ソフトは、アプリケーションゲートウェイ方式のファイアーウォールの一種だ。

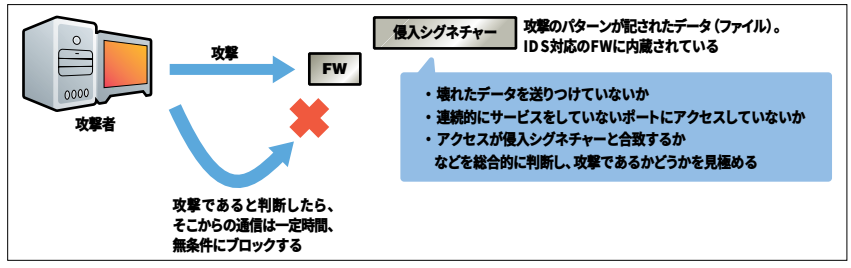
パケットフィルタリング方式では、外部からの直接の攻撃を抑えることはできるが、メールの受信やウェブの参照など、すでに接続が確立された状態で不正なデータが入っていても、それを阻止できない。そこで、アプリケーションゲートウェイ方式も併用し、不正なデータが入り込むのを防ぐようにするのが望ましい。

■ ファイアーウォールの種類



パケットフィルタリング方式ではヘッダー部分だけを見て判断する。しかし、アプリケーションゲートウェイ方式ではデータの内容まで見て判断する。

■ IDS機能の概念



IDSは攻撃パターンを調べ、攻撃と判断したら、それ以上はパケットの解析をせずに無条件にブロックするので、ファイアーウォールの負担が減る。ネットワーク資源を大量に使わせて、システムをダウンさせる攻撃に強い。

不正アクセスを検知するIDSの役割

クラッカーの攻撃手法はさまざまだが、多くの場合、TCP/IPの通信の仕組みである「3ウェイハンドシェーク」と呼ばれる構成を悪用して、接続したあとに応答を返さずに相手側のネットワーク資源を消費させるものや、セキュリティーホールに対して攻撃をするものが多く、攻撃パターンがある程度決まっている。

そこで攻撃パターンを感知し、攻撃されたと判断したら、そこからの接続を一切受け取らないようにするのも防御策として有効だ。その仕組みがIDS(Intrusion Detection System)だ。

IDSは、TCP/IPのコネクション状態を把握し、特定の接続元から尋常ではない量の接続を受け取ったときや、ある攻撃パターンと同等の接続動作が行われたときに、一定時間、その接続元からの通信を無条件に拒否する。このため、負荷が少ないのがIDSの利点だ。IDS機能を備えていなくてもパケットフィルタリングなどによって不正アクセスを阻止できるが、この場合1つ1つパケットを調査するため、攻撃が続くとファイアーウォールに負荷がかかってしまう。またIDSは単一の接続ではなく攻撃全体の流れで調査するので、攻撃パターンの変化にも対処できる。負荷がかかったり侵入されたりする前に食い止めるという点で、インテリジェントなファイアーウォール機能だと言えるだろう。

個人向けの手軽に使える ファイアーウォール＆IDS

ファイアーウォールと言うと、何やら高価なハードウェアが必要にも思えるが、最近は安価なファイアーウォールソフトもあり、個人でも導入は容易だ。個人向けのファイアーウォールソフトは、初期設定で適切なセキュリティー設定が施されているため、インストールするだけでも簡単にセキュリティーを強化できる。

ファイアーウォールは、インターネットからの攻撃を守るだけでなく、LANからインターネットに向けて不正なデータが漏れないようにする役割もある。たとえばトロイの木馬と呼ばれる種類のウイルスに感染すると、勝手にインターネットと通信し始め、外部から自分のパソコンがコントロールされてしまうことがある。そこでファイアーウォールソフトでは、あらかじめ指定したプログラムしかインターネットと通信できないようにセキュリティーの条件を設定できるようになっている。その機能を使えば、知らぬ間にソフトが起動し、勝手にインターネットと通信してしまう事態を防げる。

なおファイアーウォールソフトをインストールすると、正常な通信もが拒絶され、いくつかのソフトが利用できなくなることもある。その場合には、ファイアーウォールを緩和する設定が必要となるが、何から何まで緩和するとセキュリティーは脆くなるので注意してほしい。

ファイアーウォールで通信速度が低下する

ファイアーウォールソフトは、すべての通信状態を監視するものなので、インストールするとどうしても通信速度が低下する。とはいえ、近年のパソコンのCPUは高速なため、計測してみないとわからないほどの微々たる低下だ。しかし特定のソフトがやけに遅いと感じることがあるかもしれない。これは必要な通信がファイアーウォールによって妨害され、タイムアウトまで待たされているケースだ。そのような場合には、ファイアーウォールの設定を緩和して通信を許可することで対応できる。

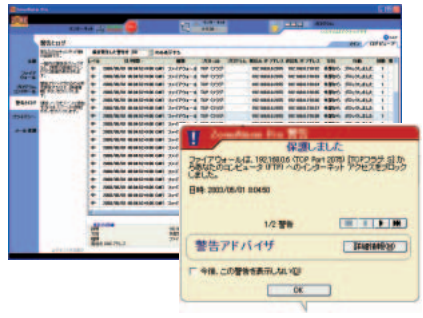
※ここで紹介する2製品は読者プレゼント対象。P59へGO！

ZoneAlarm PRO 3

フォーベル クリエーティブ　URL http://www.forval-c.co.jp/

価格：6,800円

設定が簡単なファイアーウォールソフト。通信先を「イントラネット」や「インターネット」のようにグループ化して設定するため、初心者でもわかりやすい。反面、上級者が欲する、手動での高度な設定の柔軟性には乏しい。あらかじめ指定したプログラムしか通信できないようにしたり、Cookieを遮断してプライバシーを守ったり、メールの添付ファイルを除去したりする機能も備える。IDS機能には対応していない。

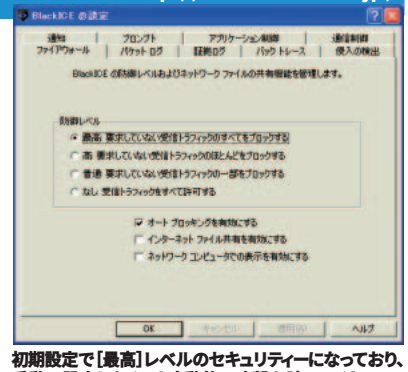


BlackICE PC Protection

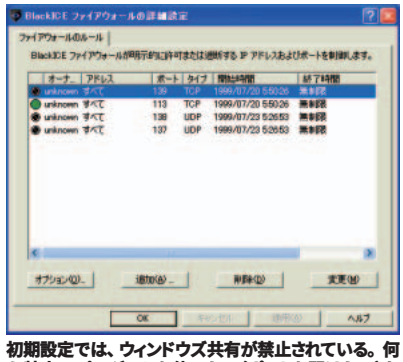
アクト・ツー　URL http://www.act2.co.jp/

価格：9,800円

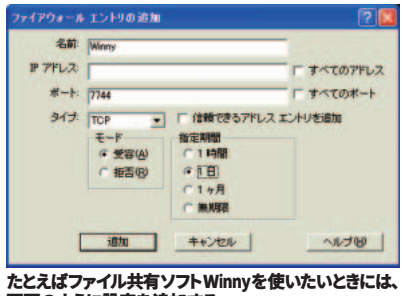
IDS機能を搭載したファイアーウォールソフト。IDS機能とパケットフィルタリングの組み合わせでパソコンを守る。あらかじめ指定したプログラムしか通信できないようにすることもできるが、初期設定はオフになっている。初期設定では、ネットワークからの接続はすべて禁止されて安全だが、一部のソフトが利用できないこともある。その場合には、設定をカスタマイズし、特定のプログラムのみ使えるようにする（ポートを開ける）ことで対応できる。



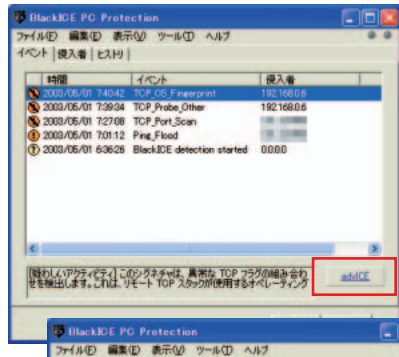
初期設定で［最高］レベルのセキュリティーになっており、手動で設定しなくても自動的に攻撃を防いでくれる。



初期設定では、ウィンドウズ共有が禁止されている。何か特定のプログラムを使いたい（ポートを開けたい）ならば、ここで設定する。



たとえばファイル共有ソフトWinnyを使いたいときには、画面のように設定を追加する。



IDS機能により、疑わしいアクセスは拒否されてログに残る。［advICE］ボタンを押すと、攻撃の詳細や対処法を見ることができる。

ウイルス対策ソフト付属のファイアーウォール機能

近年は、ウイルス対策ソフトでも、ファイアーウォール機能を備えたものが多い。ウイルス対策ソフトは、メールやウェブに含まれるウイルスを監視する機能を備えており、それをさらに強力にして一般的なファイアーウォール機能まで搭載するのは自然の流れだとも言える。

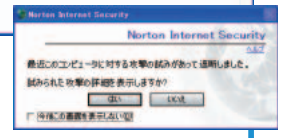
なかでもNorton Internet Security 2003は、ウイルス対策ソフトのNorton Antivirus 2003とファイアーウォールソフトのNorton Personal Firewallで構成される。しかもNorton Personal Firewallは、IDS機能も備えた本格的なファイアーウォールだ。1本でウイルス対策だけでなく攻撃からも守れるという点で重宝する。

ウィンドウズXP標準機能も場合によっては有効

ウィンドウズXPの「ネットワークのプロパティ」で、「インターネット接続ファイアーウォール機能」を有効にすると、ファイアーウォール機能が有効になる。機能的には、ルーターを使ってインターネットに接続しているのと同程度（IPマスカレードと同等）で、外部から入ってくるパケットはすべて遮断し、内部から出ていくパケットとそれに対する応答はすべて許可する。それ以外に細かな設定はできないが、ファイアーウォールソフトをインストールしていないのであれば、この機能を有効にしておきたい。有効にしておけば、無線LANスポットや携帯電話からの接続など、ルーターがないところでインターネットを使うときにも安心だ。

Norton Internet Security 2003

IDSに対応し、侵入しようとしていると判断した場合には、初期設定で30分間、そこからの通信を遮断する。

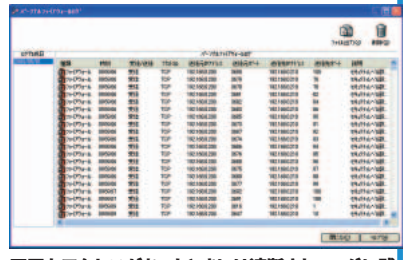


攻撃があるとログに記録され、どこからどのような攻撃が仕掛けられているのかがわかる。[対処方法]を参照すれば、どのようにして対応すればよいのかもわかる。

攻撃を受けた場合には、どこから攻撃されているのか、地図上で把握することもできる。

ウイルスバスター2003リアルセキュリティ

IDS機能は備えないが、あらかじめトロイの木馬などで使われるポートが遮断されるように設定されている。



不正なアクセスがあったときには遮断され、ログに残る。IDS機能は備えないので、パケット単位での遮断となる。

■ ファイアーウォールソフト機能比較

製品名	ZoneAlarm PRO 3	BlackICE PC Protection	Norton Internet Security 2003	ウイルスバスター2003リアルセキュリティ
				
IDS	×	○	○	×
Cookie除去	○	×	○	○
ウイルス除去	×	×	○	○
通信先をゾーンでグループ化しての設定	○	△（ネットワークアドレス単位での登録）	○	○
特定プログラムのみの通信許可	○	○	○	○

専用ファイアーウォール機器を使うメリット

本格的にセキュリティーを高める場合には、専用のファイアーウォールBOXを用いる。ソフトウェアによるファイアーウォールだと、個々のサーバーやクライアントにインストールして設定する手間がかかるためだ。

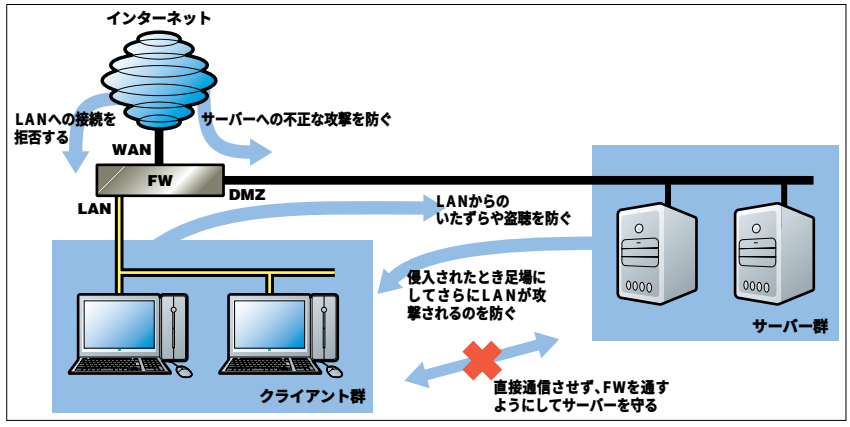
またファイアーウォールBOXで攻撃を防いでおけば、不正なデータが個々のサーバーやクライアントに届かないため、サーバーやクライアントの負荷を抑えることができる。とくにネットワーク資源を消費させる攻撃の場合、ソフトウェアによるファイアーウォールだと、OS自身が負荷に耐えられなくなることもあるためだ。さらにファイアーウォールBOXには、異常があったときに管理者に通知する機能や統計をとる機能もあるので、管理しやすいというメリットもある。

サーバーの運用にはDMZを用意する

サーバーを運用する場合には、サーバーの前にもファイアーウォールを設けることが多い。とくにファイアーウォールBOXには、「WAN」「DMZ」（DeMilitarized Zone：分離区域）「LAN」の3つのポートが付いている製品があり、「インターネット」「サーバー群」「クライアント群」の3つのゾーンに分け、それぞれに別のセキュリティーを施せる。

サーバーを分離するのは、サーバーに万一侵入されたときに、そこを足場としてLANに入り込むのを防ぐためだが、それだけでなくLAN内にいる不届き者がサーバーをいたずらしないようにしたり、サーバーが送受信するデータをクライアントが盗聴できないようにしたりする目的もある。

■ DMZの構成

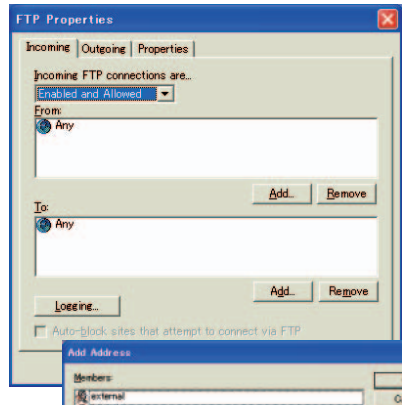


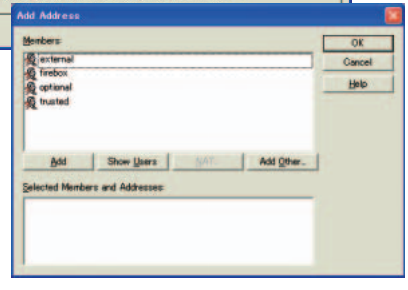
図はDMZ機能付きのファイアーウォールBOXを示しているが、2台のファイアーウォールに分けて構成してもよい。

Firebox 500では、ファイアーウォールの設定をサービスごとに指定する。この画面に示したサービスのアイコンは一部で、ほかにもいくつかのサービスが存在し、それらも追加できる。

「WatchGuard Firebox 500」の背面。EXTERNALがWAN、TRUSTEDがLAN、OPTIONALがDMZを示す。

現在のトラフィックや、誰がどこと通信しているのかを見ることもできる。

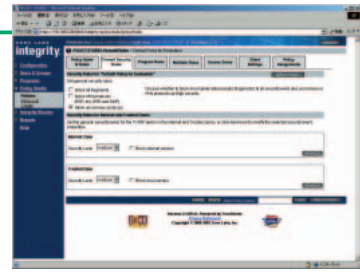




各サービスの設定では、どこからどこ宛ての通信を許すのか、もしくは拒否するのかを設定する。ポート単位での設定のほか、IPアドレスやネットワークアドレス、さらにはファイアーウォール本体やNTドメイン、RADIUSサーバーなどで認証したユーザー単位での設定もできる。

企業のネットワークセキュリティーを集中管理するソフトウェア

VPNなどを用いてリモートから会社に接続する場合には、クライアントを足場にして社内LANに入り込まれる可能性がある。そんなときは、個々のクライアントにファイアーウォールソフトを導入すると安心だ。しかし、全クライアントに設定するのは大変だし、セキュリティーポリシーの変更の際には、迅速に対応しにくい。そこで活用されるのが、セキュリティーを集中管理するソフトウェアだ。



セキュリティーを集中管理できるZONE LABS Integrity。この製品は、Server版とClient版からなる。個々のクライアントにClient版をインストールしておけば、Serverで設定したセキュリティー設定が有効となり、セキュリティー設定をサーバーで統括管理できる。

サーバー向け・クライアント向けで使い分ける

ファイアーウォールBOX製品は、サーバー向けのものとクライアント向けのもの、そして両者をサポートするものに分けられる。サーバー向けのものには、IDS機能、帯域制御機能など、サーバーに負荷がかからないように工夫されているものが多い。これに対してクライアント向けのものは、アダルトなどのコンテンツのフィルタリングやJavaScriptなどの除去、利用時間の制限、プロキシーによるユーザー認証、モバイルからのVPNアクセス、さらにはオプションでウイルス駆除機能を備えるものもある。両者をサポートするものは、DMZ機能を装備し、サーバーのゾーンとクライアントのゾーンを分離できるようになっている。機能がもっとも充実しているのは、両者をサポートするものだが、価格もそのぶん高くなる。

規模と機能で選ぶハードウェア製品

ファイアーウォールBOX製品を選ぶときに、まず重要なのが、何台まで接続するかという点だ。ほとんどの製品は、ライセンス販売となっており、無制限にサーバーやクライアントを接続できるわけではない。サーバー向け製品の場合にはIPアドレス数、クライアント向け製品の場合には同時アクセス数やユーザー認証として登録可能なユーザー数などで価格が異なることが多い。また、IDS機能やウイルス対策機能を持つ製品は、侵入シグネチャーやウイルス定義ファイルのライセンスを1年単位で更新するというものも多く、台数やユーザーが多いほど、ランニングコストも膨らんでくる。よって、多ければいいというものでもない。

また当然、通信速度も重要だ。安価な製品だと接続インターフェイスが10BASE-Tにしか対応していないこともあり、FTTH環境で接続している場合にはこれでは力不足だ。

また、ネットワークの規模が大きければ、リモートからのメンテナンスができるかどうか、通知機能は充実しているかといった管理面での機能の充実もファイアーウォールBOXを選ぶときのポイントとなる。

WatchGuard Firebox 500

価格：350,000円　URL http://www.watchguard.co.jp/

DMZを装備した多機能ファイアーウォール。WAN、DMZ、LANのそれぞれに別のIPアドレスを設定する以外に、同一IPを割り当てて利用するブリッジモードもサポートする。プロキシー機能を備えており、ユーザー認証によるアクセス権制御やコンテンツのフィルタリングもできる。またVPNによるモバイルからのアクセスサーバーとしても活用できる。ユーザー数、接続台数ともに無制限だが、モバイルVPNは標準で5ユーザーまで。ウイルス駆除にも対応する。

SonicWALL PRO100

価格：478,000円(初年度保守費含む)　URL http://www.sonicwall.com/japan/

小規模なネットワークに向く、コンパクトなファイアーウォール。DMZを装備し、サーバーも守れる。WANとLANのそれぞれに別のIPアドレスを設定して利用する。接続台数は無制限。管理画面はウェブベースで、初心者でも容易に管理できる。設定は、IPアドレスやポート番号単位が基本となるので、複雑な設定をしたい場合には設定項目がおのずと多くなる。プロキシー機能は備えないが、URLフィルタリングやコンテンツフィルタリングには対応する。オプションで、VPNやウイルス駆除にも対応。

■ ファイアーウォールBOX機能比較

製品名	サーバーおよびクライアント向け		クライアント向け		
	WatchGuard Firebox500	SonicWALL PRO 100	WatchGuard Firebox S6	SonicWALL SOHO3	NetScreen 5XT
スループット(非VPN時)	75Mbps(プロキシー時15Mbps)	75Mbps	75Mbps	75Mbps	70Mbps
DMZポート数	1	1	0	0	0
IDS機能	○	○	○	○	○
VPN拠点間接続	×	オプション	オプション	オプション	○
VPNトンネル数	—	50	オプション(最大6)	オプション(10)	10
VPNリモートクライアント接続	5ユーザー(最大50)	オプション	オプション(最大10)	オプション	○
帯域制御	×	×	×	×	○
NAT、IPマスカレードなどアドレス変換	○	○	○	○	○
DHCPサーバー	○	○	○	○	○
DHCPクライアント	○	○	○	○	○
PPPoE	○	○	○	○	○
最大接続数	無制限(認証ユーザー数は250)	無制限	10(最大25または50まで追加可能)	10または50	10または無制限
プロキシー機能	○	×	×	×	×
ウイルス駆除	5ライセンス付き(1年間)	オプション	1ライセンス付き(1年間)	オプション	なし

［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