誰でも簡単に使える暗号メール

[zixmail]登場

text：編集部

データセンターで一元管理する暗号メール

■使われない暗号メールの問題点

インターネットメールの基本的な仕組みは開発されたときからあまり変わってない。しかしインターネットが普通の社会基盤になるにつれ、議論は続くものの、メールの内容が外部に漏れる危険性についてはいまだに改善されていない。多くのユーザーが契約書やNDAなどの企業秘密などをメールでやり取りしているはずなのにだ。

もちろんメールを暗号化するためのツールとしてPGPやS/MIMEなどが一部で利用されてはいるがなかなか広まらない。その理由の1つは暗号メールをやり取りするためには、同じ暗号方式のツールを送受信者の双方が持っていなければならないことだ。相手に暗号化してメールを送りたくても、受信者が暗号ツールを導入していなければ暗号メールは成り立たない。これを説明するために、暗号メールで使われる公開鍵方式の暗号について解説しよう。

■手間とコストがかかる公開鍵方式暗号

公開鍵方式の暗号では「公開鍵」と「秘密鍵」という2つの対になった鍵が使われる。公開鍵方式を使ってメールを暗号化するには、送信者がメールの内容を受信者の公開鍵で暗号化し、受信者が自分の秘密鍵で復号するという手順を踏む（右ページ中段図）。これは公開鍵で暗号化したものはその対になる秘密鍵でしか復号できないという約束があるために成り立っている。ここで重要なのが受信者は公開鍵を送信者に届けておかなければならないことだ。公開鍵は誰に配ってもいいのでメールで送ってもかまわないが、その公開鍵が果たして送った当人のものかを証明する手立てがない。そこで一般には第三者が鍵の正当性を証明をして発行し、キーサーバーという公開鍵を管理するサーバーで保管する。このようなサービスとして、VeriSignの「デジタルID」がある。また、企業が独自にキーサーバーを構築して、社員や取引先に鍵を発行するケースもある。

デジタルIDのサービスでは、受信者の公開鍵をキーサーバーからダウンロードできるが、もし受信者の鍵がなければ暗号メールは送信できない。企業などが独自のキーサーバーを立てている場合も同様だ。

また、ほかの問題として企業などが暗号メールのシステムを導入する場合、高額な構築費を支払わなければならないといったことがある。さらに、鍵の管理にも非常にコストがかかってしまうという問題もあった。

■データセンターが持つ役割とは

こういった従来の公開鍵方式の暗号メールの問題を解決したのが、zixit社が開発した「zixmail」だ。zixmailの大きな特徴はzixitが持つセキュアデータセンター（以下、データセンター）にあるが、データセンターは次の3つの役割を持つ。

1つ目はすべてのzixmailユーザーの公開鍵を管理していることだ。公開鍵はzixmailのクライアントソフトをインストールする際に自動的にデータセンターに登録されるが、公開鍵を集中管理することで、どんなzixmailユーザーの鍵も簡単に探し出

せる。具体的には、zixmailのクライアントソフトが暗号メールを送信する際に、自動的にデータセンターから送信者の公開鍵をダウンロードするのだ。また、企業などでzixmailを導入した場合も、管理者は鍵の管理をしなくて済むし、大規模なシステムも不要になる。

2つ目はデータセンター自身がウェブメール（zixmail.netという）としての機能を持つことだ。ウェブメールの機能によって、zixmailに対応していない受信者でも暗号メールを受け取れるようになる。具体的には、zixmailのクライアントは暗号メールを送信する際に、受信者の公開鍵がデータセンターになければ、zixit社の公開鍵で暗号化したメールをデータセンターに送り、データセンターは暗号メールを預かっていることを受信者に知らせる。そして受信者は暗号メールを預かっている旨を伝えるメールを受け取ったのち、データセンターにアクセスしてパスワード（最初にアクセスしたときに設定する）を入力することで暗号メールをSSLで保護されたウェブメールとして読める。

3つ目はメッセージの署名にかかわる機能を持っていることだ。詳しくは後述するが、受信者が暗号メールを読んだかどうかを確認するための「受領証」を送信者が受け取れるといった機能を提供する。

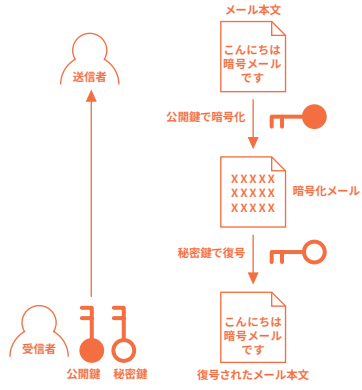
このようにzixmailは同じ公開鍵方式の暗号を使いながらも、データセンターを仲介することで、従来の欠点を補うことに成功している。zixmailのクライアントソフトとては、現在はOutlook 98/2000のプラグインソフトがある。zixmailは国内代理店としてアルファオメガが扱っており、クライアントソフトはベクターからダウンロードして5,900円で購入できる（zixmailアカウントの1年間の利用料を含む）。

zixmail
Jump www.zixmail.jp

●既存暗号メールシステムとzixmailの違い

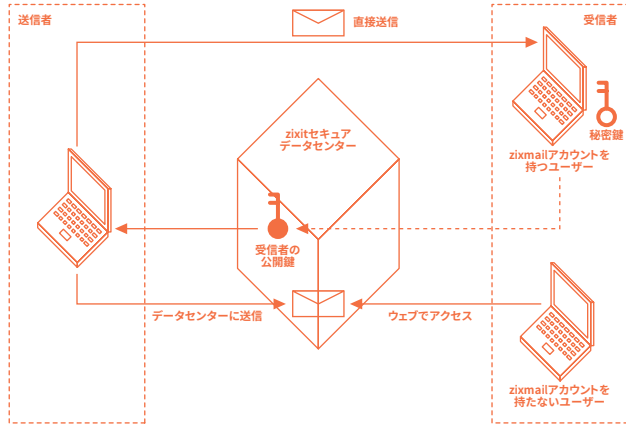
	既存の暗号メールシステム	zixmail
鍵の管理	公開鍵の管理を個人が行ったり、社内に置かれたサーバーなどで管理を行ったりするため、管理が面倒で煩雑になりコスト高になる。	公開鍵は専用のデータセンターで管理されるため鍵の管理にかかわる煩雑な作業をしなくて済む。コストも下がる。
柔軟性	送信者と受信者に対応ソフトが必要。	受信者が対応ソフトを持たなくても、データセンターに保管された暗号メールをウェブメールとして読める。
導入の容易性	企業などで全社に導入する場合は、大規模なシステム構築などが必要になる。	個人ユーザーも含む小規模な段階から導入ができる。また大規模なシステムも容易に導入できる。

●公開暗号方式のメール送受信



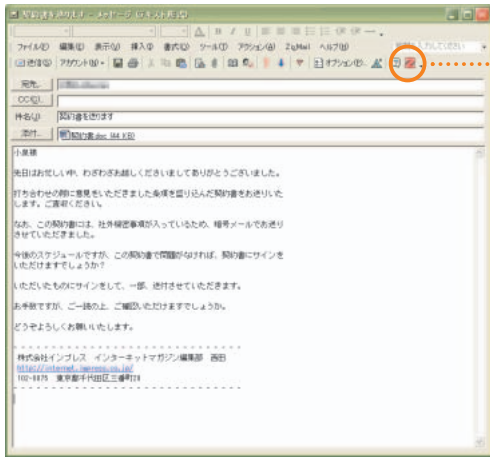
公開鍵は「公開鍵」と「秘密鍵」をペアで使って暗号と復号を行う。暗号メールの送受信は実際にはもっと複雑な手順をとるが、ここでは単純化して表現した。公開鍵で暗号メールを送受信するためには、送受信者の公開鍵を互いに交換する必要があるが、この交換手順が面倒であったり、あるいは公開鍵の管理が非常に大変で企業などで導入が遅れている。

●鍵の交換にはデータセンターを使う



zixmailクライアントはメール送信時に受信者の公開鍵をデータセンターから手に入れてメールを暗号化し、直接受信者に暗号メールを送る。もし受信者の公開鍵がデータセンターにない場合はデータセンター宛てに暗号メールを送り、データセンターが暗号メールを預かっている旨を伝えるメールを受信者に送る。受信者はそのメールを受け取ってブラウザーでデータセンターにアクセスしてウェブメールの暗号メールを読む。

zixmailの仕組みを理解して使ってみる



1 >>>送信メールを作成

送信メールは普通にメールを作成すればいい。もちろんファイルを添付して送信することもできる。なおHTMLメールを作成すると、データセンター宛てに送られる場合はデータセンター側でテキストメールに変換されるようだ。

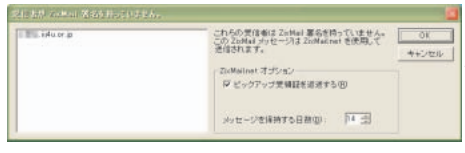
メールの作成が終わったら、Outlookのツールバーにあるzixmailのボタンを押し、暗号化に進む。

2 >>>送信メールを暗号化

暗号化手順に入ると上のようなボックスが現れる。このボックスの「電子メールアドレス」ではzixmailアカウントを持つ送信者（つまり自分）のメールアドレスを選択し、「パスワード」にはzixmailクライアントソフトのインストール時に設定した暗号化のためのパスワードを入力する。相手がメールを読んだかどうかを確認するための「受領証」を受信する場合は、チェックボックスにチェックをする。最後に「OK」を押す。

暗号化の実際のプロセスには受信者の「公開鍵」が必要になるが、この手順のときにzixmailのソフトは自動的にデータセンターから公開鍵をダウンロードする。

※データセンターに受信者の公開鍵がなかった場合（受信者がzixmailのアカウントを持っていない場合）は2'に進む。



2' >>>送信メールを暗号化（受信者がzixmailアカウントを持たない場合）

受信者がzixmailアカウントを持たない場合は、上のようなボックスが表示される。この場合、メールはデータセンターにあるzixit社の公開鍵で暗号化される。このようにzixmailではどんな場合でも暗号化してメッセージを送信できる。

3 >>>受信者へ送信

受信者がzixmailのアカウントを持っている場合は、暗号化されたメールは直接、受信者へ送信される。

受信者の公開鍵

3' >>>データセンターへ送信

受信者がzixmailアカウントをもたない場合、暗号化されたメールはデータセンターへ送信され保管される。そしてデータセンターはデータセンターに送信者のメールを保管している旨を伝えるメールを受信者に送信する。

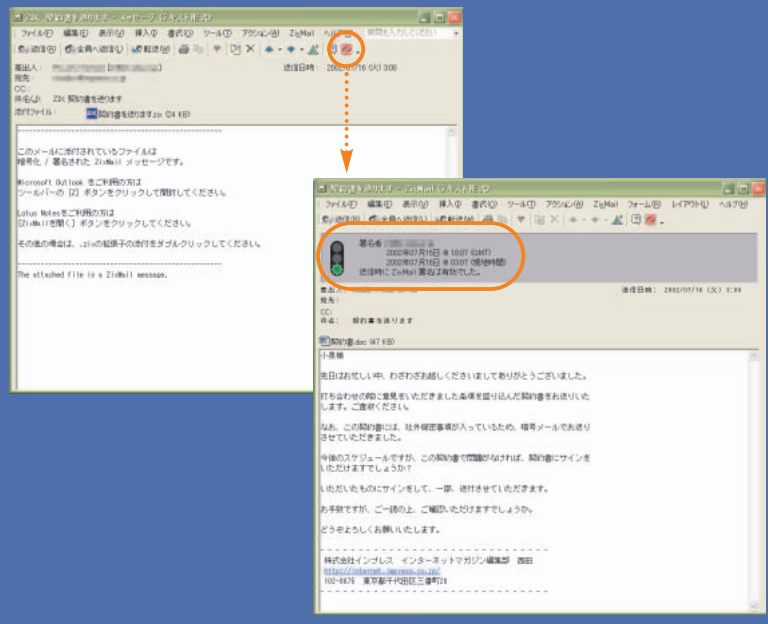
5 >>>受領証を受信

2の手順で「受領証」を受信するように設定した場合は、受信者がメールを開封するとデータセンターから受信者に「受領証」が送られる。受領証は、受信者が「メールが送られてない」あるいは「メールを読んでない」といったメール受信の否認を防ぐために使われるもので、実際には、宛先と差出人のメールアドレス、メールの受信日や開封日が記載されている。

受信側▷

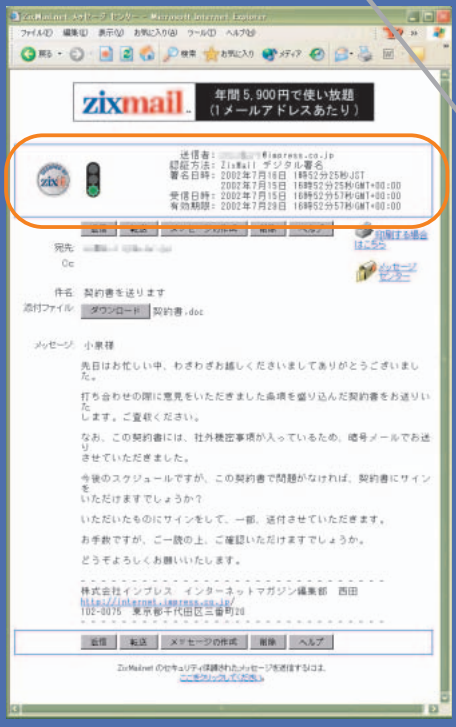
4 >>>受信したメールを読む（受信者がzixmailアカウントをもつ場合）

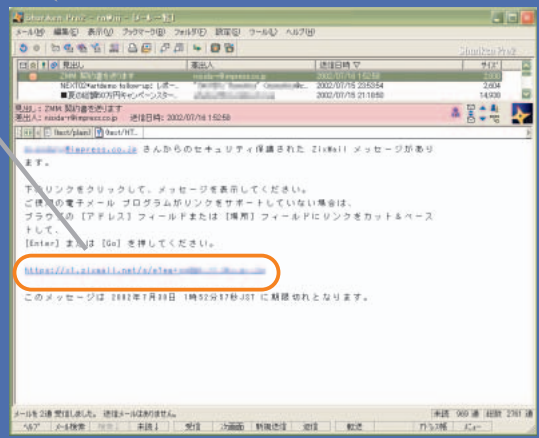
受信したzixmailの暗号メールは、送信時と同じようにzixmailボタンを押すことで復号される。復号されたメッセージには、送信者や署名日時（メールを暗号化した日時）、受信日時、改ざんがあったかどうかのアイコンが証明書として表示される。



zixitセキュアデータセンター

受信者の公開鍵はアカウント発行時にデータセンター内に保管される





4' >>>受信したメールを読む（受信者がzixmailアカウントをもたない場合）

zixmailアカウントをもたない場合、受信者は、上（右）のようなデータセンターにメールを保管している旨をメールとして受け取る。メールに記載されているURLにジャンプすると、メールアドレスとパスワードを入力するように促される（最初にデータセンターにアクセスする場合は、パスワードを設定するように促される）。入力が済むとブラウザー上に保管されているメールが表示される（左）。表示される内容は、4と同じように、送信者や署名日時、受信日時などが証明書として表示される。

zixmailのより高度な仕組みに迫る

■送受信時間もデータセンターで管理

zixmailが従来の公開鍵方式の欠点を解決していることは理解いただけただろう。しかし、いままで説明した以上にzixmailは高度な仕組みを持っている。

181ページでzixmailのデータセンターの役割の1つにメッセージの署名にかかわる機能について触れた。署名とは送られたメールの正当性を証明するもので、たとえば「このメールは誰がいつ誰に送ったもの」ということと「このメールの内容は改ざんされていない」ということを証明する。183ページ4の右上にある受信者が復号したメールの画面を見てほしい。信号の形をしたアイコンと署名者、送信日時が表示されているが、これはメールに付加された署名による情報を表示している。

署名は一般の公開鍵方式の暗号でも使われるが、暗号化した本人（送信者）の正当性とメールの内容が改ざんされていないかを検証するときのみに用いられるのが普通である。一方、zixmailの場合は暗号メールを送信する際に、データセンターで「トランザクション証明書」というものが発行される。このトランザクション証明書には、データセンター内にあるルビジウム時計から得られる非常に正確なタイムスタンプとメールの送信者や受信者の情報などが含まれている。この証明書に最終的に送信者の署名が添付される。このため時間に対して非常にシビアなメールのやり取りでも十分に効力を持つ（左下図）。

また、送信者が受領証を受け取ると設定した場合は、さらに受信者が受け取った暗号メールを復号する際にもデータセンターからトランザクション証明書が発行される。このトランザクション証明書に受信者の署名が添付されてデータセンターに送り返され、最終的に受領証が送られる。このため開封時の時間もサーバー側で正確に把握することができるのだ（右下図）。

受信者がメールを読んだかどうかと同時にいつメールを読んだかといった情報が重要な場面もビジネスなどでは想定される。それを完全に解決できる仕組みもzixmailは持ち合わせている。

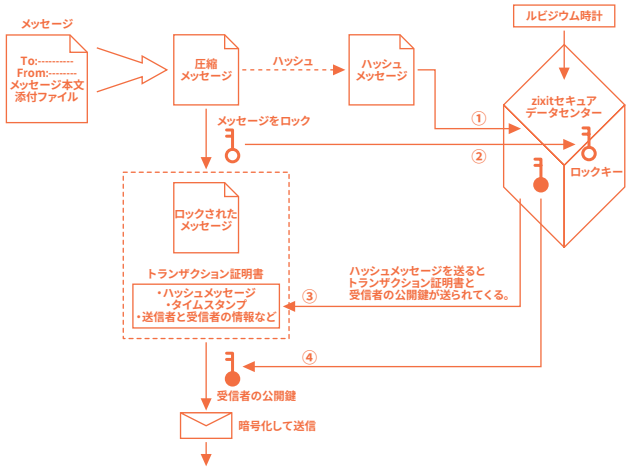
■企業では一括した導入もできる

さて、いままではzixmailの仕組みについて解説してきたが、最後にzixmailのシステム構成についても触れておきたい。

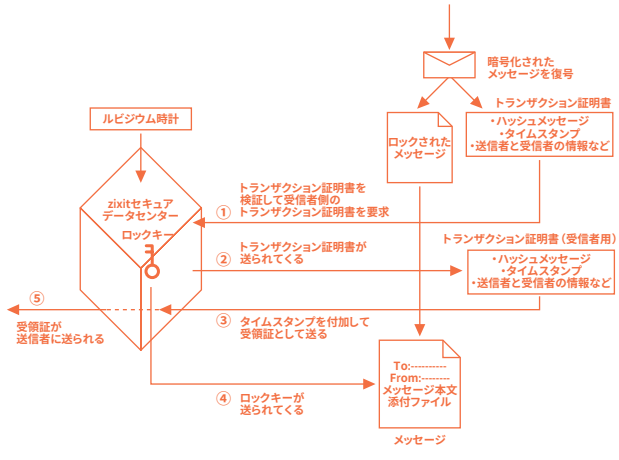
zixmailのクライアントソフトとしてはOutlook98/2000に対応しているが、現時点ではメールソフトとしてはそれのみである。実際、企業などで導入する場合には、Outlookの対応だけではシステムとしては非力である。そこで、zixmailでは大規模ユーザー向けにzixvpmというハードウェアのソリューションを用意している。zixvpmはOSにSolarisを採用したハードウェアで、企業のネットワーク上に置くことで一括してメールの暗号化と復号を行えるようにしている。

zixvpmを使うとクライアントのメールソフトとして何を利用しても自動的にメールが暗号化あるいは復号がなされ、zixmail

●受領証付きメッセージの送信



●受領証付きメッセージの受信



※ここでの説明は簡略化しています。実際にはさらに厳密な公開鍵暗号の手順を踏んでいます。

のクライアントソフトを持っていなくもzixmailに対応できる。zixvpmでは、メールアドレスに含まれるドメイン名やサブジェクト(件名)に書かれるキーワードで暗号化する／しないを設定できる。具体的には、「@impress.co.jp」宛てのメールはすべて暗号化したり、サブジェクト内に「重要」という文字が含まれているメールはすべて暗号化したり、あるいは特定の送信元のメールは必ず暗号化したりするといった設定が可能だ。もちろんzixvpmを使う場合も鍵の管理はzixit社のデータセンターで行われるため、システム管理者は不要な作業を強いられることはない(下図)。

すでに米国ではデュポンやセブンイレブンなどの企業が導入をしており、国内でも給与明細などの情報を社員に暗号メールで送信するために導入をしている企業もあるという。

■プロバイダーなどの導入で広がる

zixvpmは企業向けの製品であり、個人ユーザーにとっては直接メリットがないようにも思える。ただ、今後、zixvpmがプロバイダーなどに導入されると個人ユーザーでもメールソフトに左右されることなく、暗号メールを利用できるようになることも想定できる。たとえば、暗号メールを送りたい相手のメールアドレスやドメイン名、あるいはサブジェクトに入力するキーワードをプロバイダーのウェブから登録しておくことで、どんなメールソフトでもzixmailに対応できるだろう。実際、米国ではヤフーのウェブメールのオプションとしてzixmailが採用されている。

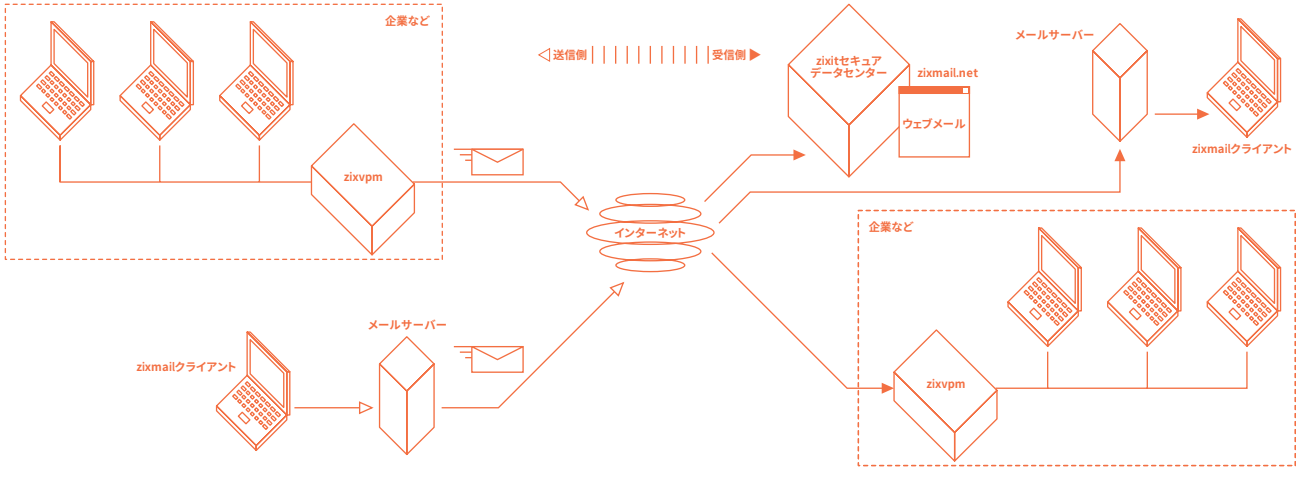
クライアントソフトとしては、Outlookのみしか対応していないが、今後それ以外のメールソフトに対応するかは、現時点では未定だという。一方、zixmail未対応のユーザー向けに使われるウェブメールのzixmail.netでは、米国では暗号メールを送受信できるプランもあり、個人ユーザーとしてこれを利用することも可能だ。

ともあれ、いままでこれだけ柔軟性を持って利用できる暗号メールはなかったはずだ。メールの暗号化の方式についてはまだまだ改善の余地はあるが、zixmailが提示する仕組みはその回答の1つであることは間違いない。

zixvpmサーバーの実機。OSはSolarisを使用しているが、今後はLinux対応版も出るという。企業などでこのサーバーを導入すれば、サーバー上で暗号と復号が自動的に行われるので、Outlook以外のクライアントも使用できる。価格はハードとソフト込みで98万円。これ以外にユーザーライセンス料が必要になる。販売代理店はアルファオメガ。

建設に5,000万ドルもかけたというzixitセキュアデータセンターの監視システムの様子。このデータセンターは、200万回／時の公開鍵の配送、100万通／時のメール保管、1億3000万個以上のメールアドレスに対応する公開鍵保管といった能力を持つという。

●専用クライアント、専用ハードウェア、データセンターをうまく組み合わせるzixmail



［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