

気になるブログやニュースをくまなくチェック!!

Newz Crawler

ライブドア  <http://soft.livedoor.com/newzcrawler/>

「Newz Crawler」は、ブログやニュースサイトの更新情報が記録された「記事サマリーフィード」を受信して、閲覧できるウィンドウ用のソフトだ。RSSやRDFといったフィード形式に対応しており、複数のサイトから自動的に記事サマリーを収集して、読みたい記事だけを自動的にダウンロードするので、ブラウザを立ち上げずにニュースをすばやくチェックできる。

メールソフトライクな画面構成 ツリー形式でURLを管理可能

Newz Crawlerには、あらかじめ40個近い有名ブログや大手ニュースサイトが登録されており、インストール直後から数多くの更新情報を一気に集め始める。

画面はよくあるメールソフトのような構成で、左の縦長のウィンドウには登録したサイトが一覧できる。サイト名をクリックすれば、右上に取得した記事のタイトルが一覧表示され、さらに読みたい記事を

クリックすれば、その下のウィンドウに記事本文が表示されるようになっている。

記事を読んでいるときにスペースバーを押すとウィンドウがスクロールして、記事の最後に達すると自動的に次の未読記事にジャンプするので、大量のニュースを流し読みするといった使い方にも適している。

サイトの追加は、メニューから「新規ニュース配信の追加」を選択して、追加したいブログやニュースサイトのフィードのURLを入力すればOKだ。

登録した各フィードは「チャンネル」と呼ばれ、エクスプローラ形式「チャンネルツリー」で管理でき、多くのチャンネルもフォルダーでジャンルごとに整理できる。

カスタマイズ可能な閲覧モード バージョンアップに期待大

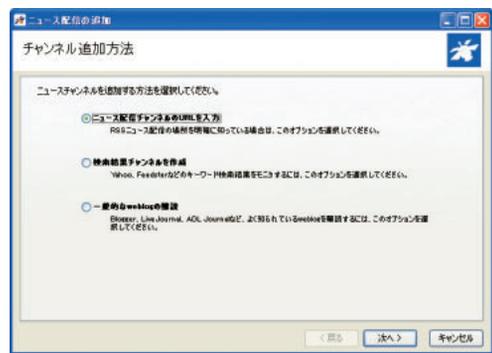
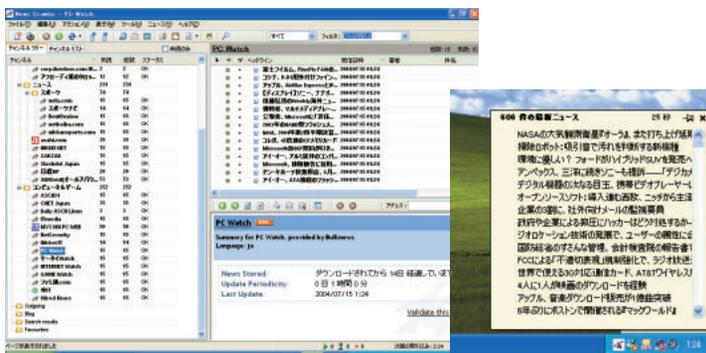
閲覧モードも豊富に備えている。「すべて」を選べば、登録されているブログやニュースサイトの記事すべてを更新時間

製品名	NewzCrawler
会社名	株式会社ライブドア
価格	2,604円(税込)
動作環境	OS: Windows XP/2000/Me、CPU: Intel Celeron 500MHz以上、メモリー: 64MB以上(Windows XPでは128MB以上 推奨)、ハードディスク: 5MB以上の空き容量(ニュース取得の件数に比例してより多くの容量が必要) 対応するフィード形式: RSS/RDF/Atom

順に閲覧でき、「今日」「2日以内」「今週」「今月」など条件分けもできる。

また、フィードの新規登録で検索サイトの結果をフィードに追加する機能や一般的なブログホスティングサービスで提供されたブログを登録する機能があるのだが、すべて英語版のみとなっていて、日本語のサイトは登録されていない。今後更新されていくと思われるが、この辺の機能が魅力的なだけに未対応なのは非常に残念だ。

すでに開発元ADC Softwareが提供する英語版では、ブログへの投稿機能などが提供されており、それらへのアップデートを含めて、今後の発展に期待の持てるソフトだ。(増田"maskin"真樹)



ニュースサイトは数あれど、実際に読めるのはその一部。それなら自分の興味や関心がある記事だけを自動的に集めてくれるこのソフトはとても便利だ。閲覧が非常に楽になるので、興味のあるサイトをドンドン登録して、必要な情報だけをチェックするという技も使える。大量のサイトを登録しても、エクスプローラ風の管理画面で整理できるのがいい。タスクトレイに常駐させておくと、定時巡回で更新されたときに画面右下のヘッドラインがポップアップウィンドウで表示される。

チャンネルの追加メニュー。基本的には「ニュース配信チャンネルのURLを入力」するが「検索結果チャンネルを作成」一般的なweblogの購読」の3パターンから行う。現在のところ、後者2つは日本語のサイトでは使えないため、登録したいサイトのフィードURLを逐一入力しよう。

ブログの更新・管理が楽になる!

ubicast Blogger

CubiCast <http://blog.ubicast.com/>

ブラウザからブログの記事を更新するのが面倒だとお悩みのブロガーにおすすめるのが「ubicast Blogger」だ。ウィンドウ上で動作するこのソフトを使えば、あたかもワープロソフトを使っているような感覚で、ブログを更新できる。もちろん画像の投稿も可能で、HTMLの知識を必要としないため初心者にも向いている。

ブログをらくらく更新 ワープロ感覚で文字を修飾

ubicast Bloggerを使うと、ブログの更新や管理が、圧倒的に楽になる。たとえば、記事を作成するときに、ワープロとまったく同じインターフェイスで、文字の種類やサイズ・色などを自由に設定できる。センタリングや段落の作成もボタン1つで、自動的にHTMLタグを挿入してくれる。

こうして作成した記事は、「投稿」ボタンを押すだけで、自動的にブログにアップロードされる仕組みだ。コメントやトラックバック、公開・非公開の設定も適宜おこなえ

る。書きかけの記事を「非公開」にして保存しておいて、必要なときに呼び出して編集するという処理もubicast Bloggerなら手軽だ。

記事執筆時点に対応しているブログツールは、サーバーインストール型のMovableTypeと、ニフティが提供するココログにしか対応していないのが残念だが、それ以外のブログツールへの対応予定もあり、またいくつかのASP型ブログサービスと交渉中だということで、それらのユーザーも対応を待ただけの価値はある。

画像もドラッグ&ドロップで投稿可 動画は独自フォーマットに変換

画像の投稿に関しても、画像ファイルを指定するだけでOKという簡便さ。マウスのドラッグ操作だけで配置やリサイズができ、アップロードも自動だ。

動画の場合も、画像と同じ手順で処理できるが、アップロードの際にオリジナル技術の“ubicast3”形式に変換される。閲

製品名	ubicast Blogger
会社名	株式会社 CubiCast
価格	無料（個人ユーザーのみ）
動作環境	OS：Windows 2000/XP、対応ブログ：MovableType（1.x、2.x）ココログ

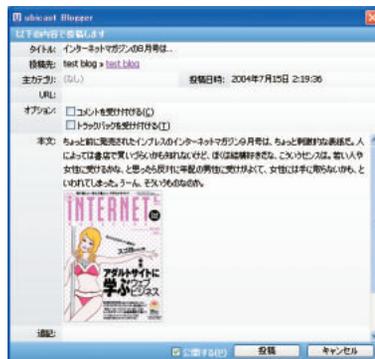
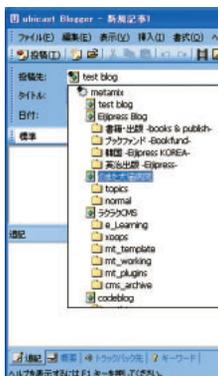
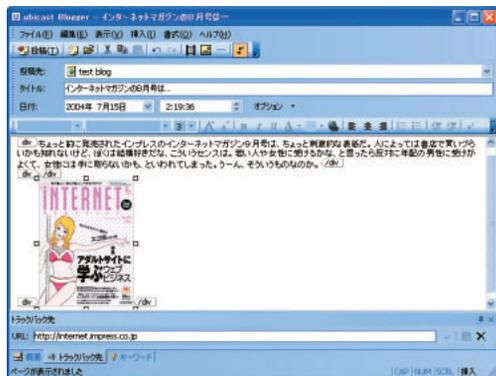
覧する際はJavaをベースにしたマルチプラットフォームの再生ソフトが自動的にダウンロードされる。どの動画ファイル形式でアップロードすべきかという悩みもなくなるはずだ。

現在、ベータ版なので一部の機能が動作しないが、すでに記事投稿機能は十分な完成度だ。複数のブログへの投稿や、過去の記事を読み込んで修正するなど、記事を投稿するという機能に限れば通常のブラウザ一経由でできることはすべてubicast Bloggerから行える。

現在のところ、正式版の公開日程は未定だが、バージョンアップされるたびに新たな機能が追加されており、今後目が離せない存在になりそうだ。

ブロガーにとって、このソフトは強い味方となるだろう。

（増田"maskin"真樹）



ワープロソフトと変わらない操作環境。文章をバラバラと入力して、ワープロのように整形し、フォントサイズや色もメニューから変えられる。画像もドラッグ&ドロップで貼り付けられて、マウスでリサイズすれば完成。この見た目そのまま、ブログに投稿される。投稿先のブログやカテゴリーは、ドロップダウンメニューから選択できる。

原稿を書き上げて「投稿」ボタンを押すと確認画面が表示される。投稿内容のプレビューのほか、コメントやトラックバックの可否といった設定もここで行う。ここでさらに「投稿」を押すと初めてブログにアップロードされる。画像も自動的にリサイズされるのが画期的。

サーバーの安全性をシールでアピール! HACKER SAFE

三和コムテック株式会社 <http://www.hackersafe.jp/>

インターネット上に公開されているサーバーは常に攻撃の危険にさらされている。その多くが既知のセキュリティーホールを狙ったもので、適切な設定がなされていなかったり、脆弱性のあるソフトウェアを利用し続けていたりするのが原因だ。

個人情報、なかでもクレジットカード番号などを扱うオンラインショップでは、攻撃による情報の流出は信用問題となるため、しっかりとしたセキュリティー対策をとるのは管理者として当然のこと。

しかしセキュリティー対策を外部に対してアピールすることには、つねに困難が付きまとう。なぜならセキュリティーとは、自ら安全性をうたっても信頼されにくく、強調しすぎれば逆に不信感を抱かせることになるものだからだ。そのためセキュリティー対策は、きちんと行っていれば外部からは何も起きていないように見え、何か起きて注目されたときは、すでに遅すぎるというジレンマがある。したがってコストに対する見返りが計りにくいのが難点だ。

脆弱性がないことを第三者が証明 ScanAlert社のHACKER SAFE

そこで登場したのが「HACKER SAFE」というサービスだ。これは米ScanAlert社が提供する、サーバーが安全であることを自らのウェブサイトにシール(GIFバナー)を貼ることで証明するサービスだ。

ScanAlert社は、サービス加入者のサーバーに対して脆弱性がないかを確かめるために、定期的な疑似攻撃を仕掛ける。そして脆弱性がないと確認されたときにだけ、加入者のウェブサイトにHACKER SAFEシールが表示される仕組みだ。

一般のユーザーは、利用したいオンラインショップにHACKER SAFEシールがあれば、ScanAlert社によって安全性が証明されたサーバーだとわかる。

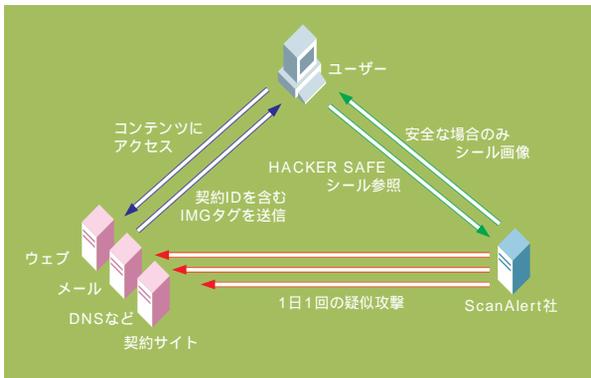
このような手法で第三者によって自社サーバーの安全性を証明できれば、セキュリティー対策とユーザーへのアピールが同時に行える。まさに一石二鳥のサービスだ。

導入は申請と簡単な作業のみ 修復までの猶予は72時間

HACKER SAFEを導入するには、利用しているサーバーのIPアドレスやOS、アプリケーションなどを申請する。そして自らのウェブページのHTMLソースに、指定されたイメージタグを挿入すれば、導入は完了だ。HACKER SAFEのシール自体は、ScanAlert社のサーバーから配信されるシステムで、常に最新の調査日がシールに表示される。

申し込みが完了すると、ScanAlert社は1日1回、サーバーに向けて疑似攻撃を仕掛けて脆弱性を調査する。調査を行うのはウェブサーバーだけでなく、データベースサーバーやメールサーバー、DNSサーバーなど、外部に公開されているすべてのネットワーク機器が対象となる。

もしもサーバーに脆弱性が発見された場合は、ただちにScanAlertから管理者に警告メールが送信される。管理者は、



自社のウェブページにはHACKER SAFEシールのIMGタグを埋め込んでおくと、シールの画像自体はScanAlert社のサーバーから配信される。ScanAlert社のサーバーは、疑似攻撃の結果、脆弱性がないときだけHACKER SAFEシールの画像を返す。



The screenshot shows the Hacker Safe seal integrated into a website. The seal features the ScanAlert logo and the text 'HACKER SAFE' with a checkmark. Below the seal, there is a detailed explanation in Japanese, including the company name 'ScanAlert社' and the date '最終検査日 4月20日'. The text explains that the seal is a proof of security provided by ScanAlert社, which performs daily simulated attacks to ensure the server is safe. It also mentions that the seal is updated with the latest check date.

HACKER SAFEシールは、サイズや色によって複数のパターンがある。また携帯電話向けのHACKER SAFEシールも用意されている。ユーザーは、HACKER SAFEシールをクリックすると、どのように安全なのか、その詳細な情報をポップアップウィンドウで見ることができる。

HACKER SAFEのウェブからアカウントごとに用意された管理ページにログインし、どのような脆弱性かといったことだけでなく、対処の方法まで確認できる。

管理ページは完全に日本語化されており、脆弱性の種類や対処方法などのセキュリティに関するさまざまな情報が掲載されているため、ネットワーク管理者にとっては大変有効な情報源となる。

ただし、脆弱性への対処方法がわかったからといって、ノンビリはしてられない。警告メールが届いたあと、サーバーに対策がされないまま72時間を経過すると、そのサイトは安全でないと判断されてしまい、HACKER SAFEシールの配信がストップする。当然、ウェブページに表示されなくなり、これはユーザーの立場から見れば、信頼を損なう効果がある。脆弱性が報告されたなら、ただちに修正すべきだ。

日本総代理店となっている三和コムテック株式会社では、有償で脆弱性修正の相談ができるヘルプデスクサービスを提供しているので、すばやい対応をするためには、このサービスを併用するのもよいだろう。

なお、自社管理ではないレンタルサーバーであっても、HACKER SAFEの契約は

可能だ。ただしサーバーの管理者権限がないと対処できないことも多いため、その場合にはレンタルサーバー業者にも同時に脆弱性が報告される。

米ではクレジットカード会社が推奨 HACKER SAFEの知名度が鍵

米国でスタートしたHACKER SAFEは、導入件数が飛躍的に増えており、5月末時点で約5万5000サイトに採用されているという。この背景には、米国では個人情報情報を扱うためには、法的な義務が課されていることがある。とくにクレジットカード決済を採用するサイトに厳しく、VISAやMaster Cardといったカード会社も、それぞれ独自にセキュリティ要件を定めている。それを満たさないサイトは、決済取引が停止されてしまうほどのものだ。しかしHACKER SAFEを導入すると、それによってカード会社のセキュリティ要件を満たしたと見なされるという事情も手伝って、とくにショッピングサイトで導入が進んでいるようだ。

一方、日本国内では、まだサービスがまったばかりのため、知名度が低い。そのためユーザーがHACKER SAFEシール

サービス名	HACKER SAFE
国内代理店	三和コムテック株式会社
価格	年額29万8,000円(1ドメイン/3デバイスまで)+ 初期導入費3万円

を見ても意味が伝わらず、安全性のアピールという目的を果たすには不十分な状況だ。しかし今後多くのサイトで利用されるようになれば、ユーザーに対する知名度も上がり、安全性の指標として信頼されるだろう。

しかしながら、HACKER SAFEの知名度が低い現在の段階でもメリットはある。

ネットワーク管理者は、日々脆弱性の情報を追って、その都度修復をするのが基本だが、すべての情報を追いかけることはかなりの労力をともなう。しかしHACKER SAFEを導入すれば、日々自動的にチェックがされるため、日常の管理業務にかかる負担は大幅に減るだろう。

HACKER SAFEシールは、ユーザーに安全性をアピールするためのシンボルとだけ考えると、ショッピングサイトなどの安心感が売り上げにつながるサイトでしかメリットがないと思いがちだ。しかし実際には、それだけに留まらない効果があるので、多くのサイトで導入する価値があるだろう。

(大澤文隆)



管理ページでは、サーバーがどのような脆弱性をもつかが一覧表示される。左にある1~5までの数字が危険度のランクを表し、大きいほど危険性が高い。

それぞれの脆弱性について詳細な解説ページが用意されており、また解説はすべて日本語化されている。それぞれの脆弱性について、具体的な解決方法まで指示されているため、サーバーの管理者にとっては大変便利である。



[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の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