interview

NETSCAPE

本誌先月号の緊急レポートでも紹介したように、ついにネットスケープナビゲーター2.0のベータ版がリリースされた。そこで、ネットスケープ社の日本法人である日本ネットスケープコミュニケーションズのカントリーマネージャー杉原信一氏に、その目指すところをうかがってみた。

インタビュアー：本誌編集長　井芹昌信

「2.0の最大の特長はマルチメディアという言葉を意識した付加価値を入れていることですね。」

ネットスケープ社の規模だとか、売り上げだとか、何人いらっしゃるかとか、まずその辺から教えてください。

杉原：現在米国のネットスケープ社では、従業員が500人以上になりました。8月に上場しましたでしょ。それでわっと広まった感じがあるんですけど。売り上げに関しては第3四半期の数字が初めて公開後に出たんですけど、2000万ドル以上を計上しました。上場して、最短距離で第3四半期で初めて黒字に転換して、これもまた1つの記録だと思うんですけど、おかげさまで順調にいっています。プロダクトも順調に普及していると言えるんじゃないでしょうか。ただ、ナビゲーターのセールスがまだ多くて、サーバーは伸びてますけど30から35パーセントくらいですね。
去年の12月にバージョン1.0が初めて出て、このあいだ発表したのが2.0。ちょうど1年後にメジャーバージョンアップという意味で2.0を出そうと、今むこうはすごく忙しくやっている状況です。

日本語版のほうは？

杉原：日本語版のナビゲーターは8月のあたまに初めてできまして、それまで英語版のセールスだったんですけど。8月の下旬くらいからやっと日本語版のパッケージが出始めて、今では正直申しまして何万本という単位で出ていっています。
日本でのナビゲーターのシェアは、一説によりますと65パーセントとか書いてあるんですけど、もっといってるんじゃないかなと思います。マックに関しましては、100パーセント近く出ていますけどもね。そういう意味では、日本でもインターネットの普及に貢献しているんじゃないかと思いますね。

ナビゲーターは、お店で売れているんですか？

杉原：売れ始めています。秋葉原セールスが大変重要になってきていてもっと力を入れていきたいと思っていますが、今はなんといってもコーポレートユーズですね。それが一番大きなシェアをもってまして。やはり、エンタープライズレベルでまだインターネットに入ってないところが多いものですから、そっちのほうに普及させて。インターネットの1つの問題の中にアクセスのチャージが高いというのがあるんですね。ですから個人ももちろんだいぶ入ってますけど、企業がまず最初に入っていくという形になっていく気がしますね。

ナビゲーターの2.0のほうなんですけど、製品版の出荷予定はいつ頃ですか？

杉原：アメリカでの出荷の予定が12月の末くらいと言われておりまして、もっと早まる可能性もありますけども、それが最新のスケジュールですね。今、ベータ版を出しておりますけども、たぶんベータ1、ベータ2という形で出ていって、12月には出すことがわかっていますけども。日本語版はそれからローカライズしますので、来年の第1四半期という見方をしています。

それでは、2.0のセールスポイントを。

杉原：やはりマルチメディアという言葉を意識した付加価値を入れているということですよね。筆頭はHOT JAVAですね。それから動画を入れ込むためのマクロマインドディレクターであるとか、そういった本来のマルチメディアと言われてきたテクノロジーとの融合が図られています。それにセキュアーなE-mailも入れておりますし。その辺では、オールインワン的なパッケージになったと言ってもいいと思いますね。

私はとくに電子メールの部分に興味があって、たとえば電子メールとブラウザーのコンビネーションによるいろいろな使い方があるんじゃないかなと思っていたんですけど。インターネットの利用者はネットスケープ立ち上げておけばほとんどのことができるということですか？

杉原：それじゃないと、本来のインターネ

日本ネットスケープコミュニケーションズ株式会社
カントリーマネージャー

杉原信一

ット上でのマルチメディアとは言えないんですよね。

アクロバットの機能というのは、今回はどうですか？

杉原：アドビのアクロバットですよね。これはサードパーティーのものですから、私どもがローカリゼーションするわけじゃないもので。むずかしいかな、というところはあるんですけどね。

すると、アクロバットなしで日本語版を出してしまうということもありえるということですか？

杉原：サードパーティーに関して遅れた場合には、その機能をつけずにということもあるかもしれません。これは12月くらいにならないとわからないですね。

ほかに2.0で大きく変わった機能というと何がありますか？。

杉原：クライアントの認証ですね。これまでのバージョンではサーバーの認証しかやってませんでしたが、2.0からはクライアントの認証を入れます。要するに、クライアントに対しても認証機関がサーティフィケート、つまり本人であることの証明書を出すわけですね。そうすることによって、サーバーとクライアントがお互いに本人であることの確認ができるようになるわけです。

具体的に、オンラインショッピングをするようなケースで、どういうふうに利用されることになるんですか。

杉原：サーバーとクライアントの間で、ショッピングをする前にお互いにサーティフィケートを交換して本人であることを確認し合うわけです。
まずサーバーに対して、たとえば「本当にインプレスのサーバーですか」と尋ねると、サーティフィケートが送られてきて「私はインプレスのサーバーですよ」というのがわかる。同じようにしてサーバー側もクライアントが本人であることを確認できるわけです。

最初に登録が必要なのですか？

杉原：認証機関に登録してサーティフィケートを発行してもらうわけです。

具体的にはどういう構想になるんですか。

杉原：認証機関は今はベリサインという会社がやっているんですけど。サーバーを立ちあげたときに、これが本当にあなたのものですねということを確認したうえで、認証機関がサーティフィケートを発行するわけです。サーティフィケートといってもデジタルな番号ですが、それを入れることによって初めてサーバーの中の公開鍵と秘密鍵が使えるようになるという仕組みです。

クライアント側も事前に登録してキーをもらうわけですか？

杉原：そうです。それは当然デジタルでくるわけですけれども、それをナビゲーターの中に入れておくわけです。

ところで、サーバーの2.0はどんな製品になりそうですか？

杉原：われわれは「セキュアクーリエ」という言い方をしているんですけど、アプリケーションレベルでのセキュリティー機能を持たせるかたちになります。本来のRSAのセキュリティーはネットワークレイヤーにSSLとして入っていますが、それに対してセキュアクーリエというのはアプリケーションレイヤーに入れているんです。これはどういうコンセプトかと言いますと、エレクトリックコマースで、消費者と、マーチャントと、アクワイヤーすなわちカード会社や銀行の間でのセキュリティーを実現するものなんです。
このシステムでは2つの電子封筒をつくります。たとえば、何かの買い物をするとしますね。そうしますと、1つの封筒には購入関係のマーチャントが知らなければならない情報、もう1つの封筒には個人のクレジットカード番号とかパーソナリティー・アイディンティフィケーション・ナンバーですとかを入れます。つまりマーチャントのところでは個人的なクレジットカード番号と

かの情報は開かせないようにさせるんです。マーチャントのところで必要なのは、何を買ったか、いくらだったかということだけなんです。どうしてこういうふうにするかというと、もし悪いマーチャントがいたら、クレジットカード番号を盗んで悪用する可能性があるからです。あくまでもアクワイヤーのところ、要するにカード会社や銀行のところにきて初めて個人の情報が開けられるわけです。アクワイヤーでオーソライゼーションされたならば、オーソライゼーションの封筒を新たにつくって、マーチャントと個人に戻してやることになります。
しかも、これに使われるのアルゴリズムのビット長は、80ビット以上の承認がとれそうだということなんですけど。

それは基本的には、RSAみたいな技術をそこでも使っているんですか。

杉原：そうです。ポイントは、こうすることによって個人の情報が守られるということです。これは2.0のコンセプトで、クライアントのほうにはすでにあるんですけれど、当然2.0のサーバーが出てこないと使えません。これは、来年の春以降ではないかと思いますけれど。

話は変わりますが、このあいだキーを破られましたね。あのあとの対策というのは？

杉原：2つ破られましたよね。
まず40ビットのキーが破られたことに関しては、2つの主張をしておりまして、1つにはアメリカ国防省に対して「40ビットはやっぱり破られます。いくらスーパーコンピューター2台とワークステーション120台を使って8日間かかると言っても、破られるものは破られます」ということ。ただ「40ビットでもこんなに手間がかかるんです」ということもありますよね。ネットスケープのサーバーはセッションを100秒ごとに区切ってキーのアルゴリズムを変えていますから、あの40ビットを破ったのに関しましては、100秒間のデータしかないわけです。そこに、もし重要な情報があったら終わりですけども、もし重要な情報がなかった場合には、ほかの100秒をまた8日間かけて破らなければならないということなんですね。われわれの言っていることは「やっぱり40ビットは手間ひまかければ破られてしまいますよ。ですからインターナショナルにおいても、もっとビット長を長くすべきですよ」ということで、アメリカの司法省や安全保障局もだいぶ緩和してきているんですけどね。もう1つの主張は「40ビットと言えどもこれだけ時間がかかるので、今のカタログショッピングなどに比べたらはるかにセキュアーですよ」ということ。ハイテクであるがゆえにハッカーが挑戦するわけです。今、アメリカではMCIのショッピングモールとか、あちこちでもやり始めていますけれども、それによる被害は一切ありませんしね。それが1つ。
もう1つの話というのは、キーを生成するときのアルゴリズムがリバースエンジニアリングで解けてしまったということです。これに対しては、ネットスケープは認めておりまして、この生成のときのコンビネーションのビット長が30ビットであったのは甘かったということで、それを300ビットに変えて今はもうアップグレードされています。

今の2.0でもされていますか。

杉原：もちろんされています。1.0に関しましても、このパッチは出ております。

輸出のほうですけども、48ビットまでOKになっているとか。

杉原：まだ、正式には聞いていないのですが、いずれそういうのは出てくると思います。かなりプレッシャーをかけていますから。

40ビットとか48ビットとか、バージョンの違いによるキーの互換性の問題はないんですか？

杉原：問題ないです。サーバーにアクセスするときに、たとえば「私は40ビットですよ」という信号を出すんです。そうすると「じゃあ、40ビットでやりましょう」ということになるんです。じつは今のクライアントには128ビットの機能が入っているんですが、今は40ビットしか使えないようになっています。ですから、それを伸ばすことは簡単にできるんです。

では、最後に読者の方に何か言っておきたいことがあればお願いします。

杉原：みなさんセキュリティーをものすごく心配されているのはわかるんですけれども、今のテレビショッピングとかテレフォンショッピングとか、そういうところでクレジットカード番号が公開されているのに比べれば、はるかにセキュアーであるということをご理解いただければ、もう少しこのエレクトリックコマースというものを早めに実用化できるのではないかと思いますね。

どうもありがとうございました。

［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