不正アクセス❷

中央官庁への不正アクセスと米国主要サイトへのDDoS攻撃が多発

政府機関ウェブジャック事件の教訓

2000年1月24日、科学技術庁のウェブサイトが何者かによって不正アクセスを受け、コンテンツが政治的なメッセージに書き換えられるという事件が起った。これを皮切りに、総務庁、運輸省、人事院などの省庁や関連機関のウェブサイトが次々に同様の攻撃を受けて、内容を改ざんされるという事態に至った。同時期にgo.jpドメインを中心に、多くの不正アクセスを試みる行為が報告されており、特定のグループによる組織的な攻撃が試みられたものと考えられている。しかし、このような不正アクセス行為は一般にありふれたものであり、被害にあった組織では、インターネットに対して公開するサーバーへの基本的なセキュリティ対策が不十分であったといわざるを得ない。

こうした公開サーバーに対する攻撃は、典型的に、まずポートスキャンなどのクラッキングツールを使ってサーバー上で動作しているサービスを探るところから始まる。そこで使用されているソフトウェアにセキュリティホールのあるものが見つかったら、不正なデータを送りつけてアプリケーションを誤動作させてサーバー上のデータを書き換えたり、管理者権限を奪取したりする。

不正アクセスに利用されるセキュリティホールはほとんどが既知のものであり、CERT Advisoryなどのセキュリティ情報を通じてよく知られているのが普通である。したがって、OSのパッチの適用や、アプリケーションのバージョンアップ、不要なサービスの停止など、基本的なセキュリティ対策をきちんと行っていれば、やすやすと侵入を許してしまうようなことはなかったはずである。ファイアーウォールによる防御は、http以外のポートへのアクセスを遮断するという意味では有効であるが、ウェブサーバーソフトウェア自体やCGIプログラムなどの欠陥をつく攻撃を防ぐことは一般にできないので、サーバー自体をセキュアに保つことが基本と考えるべきである。

数年前と比べるとコンピュータネットワークにおけるセキュリティ対策の必要性の認識は格段に高まっている。しかし、こうした地道なセキュリティ対策とそれを継続的にメンテナンスしていくことの重要性は、いまだ正しく理解されていないことが、今回のウェブジャック事件の教訓から、最も反省すべき点であったといってよいのではないだろうか。

分散型サービス妨害攻撃（DDoS）の脅威

2000年2月7日、米ヤフーのウェブサイトが何者かによってサービス妨害攻撃を受け、約3時間にわたってほとんど使用できなくなるという事件が発生した。その後、イーベイ、アマゾンコム、CNNなどの著名サイトが次々同様の攻撃のターゲットにされ、一時的にサービスが提供できない状況に追い込まれた。この事件は、米国では、社会のインフラストラクチャーとなっているコンピュータネットワークに対する重大な挑戦として深刻に受け止められた。

この一連の攻撃で使われたのは、分散型サービス妨害（DDoS = Distributed Denial of Service）攻撃と呼ばれる手法である。サービス妨害攻撃は、サーバーやネットワークを使用できなくするのが目的で、もともと防御しづらい性質の攻撃である。DDoSの場合は、インターネット上の多数のサイトを攻撃拠点として利用し、同時協調的に大量のトラフィックを集中して送りつけるので、標的にされたサイト単独での防御は非常に困難である。

DDoSアタックの攻撃準備は、まず踏み台となるサイトを見つけ出すところから始まる。セキュリティ・ポリシーがゆるく、しかも高速のインターネット接続を持っている大学などが格好の対象とされる。踏み台サイトの不正侵入したサーバーにDDoSのツールをしかける。ツールによっては、近傍をスキャンして脆弱性を持つサーバーに自動的に攻撃をしかけ、「子ども」を増やす機能を持っている場合もある。複数の踏み台サイトでこの仕込みをした後で、攻撃者は攻撃指令を「親」プログラムに出す。指令は「子」プログラムに伝えられ、ターゲットに向けてパケットが一斉に送り出されることになる。

インターネットでは、その仕組み上、セキュリティは各サイトの自己責任によるところが大きい。また、脆弱なサイトは自らを危険にさらすだけでなく、踏み台にされることで第三者の安全をも脅かす可能性がある。今回の事件はそうした構造的な脆弱性が悪用されたものといえる。

DDoSアタックに対抗するには、プロバイダー事業者はもちろん、製品や技術・サービスを提供するベンダー、そして接続する各サイトやユーザーが協力してこれにあたる必要があり、今回の事件をきっかけとして、その方策についての活発な議論が始まっている。インターネット全体の安全は、そこに接続する無数のサイトの安全に依存しているという原点に立ち帰って、自ら果たすべき責任について考え直してみるよい機会なのではないだろうか。

（白橋明弘　ネットワンシステムズ株式会社）

Jump 01 ウェブページの改ざんに対する防衛、JPCERT/CC
http://www.jpcert.or.jp/ed/2000/ed000003.txt
サービス運用妨害攻撃に対する防衛、JPCERT/CC
http://www.jpcert.or.jp/ed/2000/ed000002.txt

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

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、データ、URL、名称など）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・図の作成者、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掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したり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される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期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。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp