情報セキュリティ歳時記 15

まだまだ道は遠い

前川　徹
早稲田大学 国際情報通信研究センター

⊃ お粗末なセキュリティ対策

2000年1月末から2月にかけて政府や政府関連機関のウェブサイトが改ざんされる事件が起きた．クラッカーに改ざんされたのは，科学技術庁，総務庁，運輸省，人事院近畿事務局，総合研究開発機構，社団法人政府資料等普及調査会などが開設していたウェブサイトである．

この連載の第1回や第5回で取り上げたように，ウェブサイトの改ざん事件は珍しいものではない．しかし，これほどまで簡単にクラッカーの攻撃にやられてしまうとは思ってもみなかった．

今回の事件でまず指摘すべきことは，総理官邸や大蔵省，通商産業省，外務省などのウェブサイトが改ざんされていないことである（これらの省庁にも不正アクセスが試みられた形跡が発見されている）．情報処理振興事業協会（私は昨年夏まで，ここのセキュリティセンター所長だった）やネットワークセキュリティに関する緊急対応センターであるJPCERT/CCのホームページも無事だった．つまり，今回のクラッカーの腕前では，これらのサイトに侵入することはできなかったのだと考えてよいだろう．

改ざんされてしまったサイトのセキュリティ対策がどの程度のものであったかは，公式には発表されていないが，マスコミの報道などによれば，ファイアウォールで守られていないばかりか，既知のセキュリティホールも放置されていたのだという．これでは，ネット上で簡単に入手できる攻撃ツールを面白半分に実行するレベルのクラッカーでも侵入できただろう．

1月21日に，情報セキュリティ関係省庁局長等会議の決定として「ハッカー対策等の基盤整備に係る行動計画」が発表された直後だっただけに，政府の対策のお粗末さが目立った事件であった．

⊃ ファイアウォールがすべてではない

今回の事件でもう1つ心配になったことがある．それは，改ざんされたウェブサイトがファイアウォールで守られていなかったことばかりをマスコミが報道したことである．ウェブサイトはファイアウォールがなくても相当程度安全に管理することができる．逆に，ファイアウォールがあってもその設定が適切でなければ，ほとんど何の役にも立たないし，仮にファイアウォールの設定が適切であっても，ウェブサーバの設定が悪ければ，ファイアウォール越しにサーバをクラッキングされる可能性がある．

この連載の第7回で取り上げたように，インターネットで利用されている各種のソフトウェアの中にはセキュリティホールがいくつも発見されている．通常，セキュリティホールが発見されると，それを塞ぐ方法や「パッチ」と呼ばれるプログラムが公開される．また，しばらくするとその欠陥をなくした新しいバージョンが発表される．セキュリティホールの対策方法はCERT/CCやJPCERT/CCなどの緊急対応センターのウェブで公開されている．不正アクセスを未然に防ぐには，こうした情報に注意して発見されたセキュリティホールは即座に塞ぐようにしなければいけない．また，ウェブサーバでは検索やユーザ登録などの機能を付加するためにCGIスクリプトを用いることがあるが，これも作り方次第によっては不正侵入の原因となることがある．CGIスクリプトが安全であることを十分に確認しておく必要がある．

また，ウェブサーバを別のサービスにも利用している場合，そのサービスを提供しているプログラムの欠陥から不正侵入されるケースもある．できるならウェブサーバではサービスを限定し，不要なプログラムは取り除いておいた方がよい．

もちろん，その上でファイアウォールを利用すればより安全になる．外部からは決められたプロトコル（通信手順）しか通さない「DMZ（DeMilitarized Zone）」と呼ばれるゾーンにウェブサーバを配置することによって，安全性は一層高まる．

今回の事件で，改ざんされた省庁や組織にはファイアウォールがなかったことが大きく取り上げられているが，ファイアウォールがすべてではない．むしろサーバのセキュリティホール対策や，ソフトウェアの設定の方が重要である．かつてホワイトハウスのウェブサイトに侵入したgHと呼ばれるグループのメンバは，ホワイトハウスのウェブ管理者が不注意にも他のコンピュータから覗くことができるFTPサイトを介してログファイルを転送していることを発見し，これを辿ってウェブサイトに侵入したのだと語っている．管理者のほんの小さな気のゆるみからクラッカーは

侵入してくるのである．

⊃ 情報セキュリティに関する意識

(財) 日本情報処理開発協会が2000年3月に発表した「情報セキュリティに関する調査」の集計結果を見て愕然とした．数年前から情報セキュリティ関連の報道が増加しており，昨年には不正アクセス禁止法が成立したこともあり，情報セキュリティに対する関心はかなり高くなっており，企業の情報セキュリティへの取り組みはかなり進んだに違いないと思っていたのだが，どうもそうではないらしい．

この調査は，企業の情報システム部門を対象として，昨年11月から年末にかけて実施されたアンケート調査（発送数は4,714通，回答数は876通）である．

コンピュータウイルス被害や不正アクセス被害の届出機関として情報処理振興事業協会（IPA）が指定されていることは6割前後の回答者が「知っている」と答えているが，不正アクセスの手口の分析を行い，再発防止策の検討と助言を行っているJPCERT/CCについて，約3分の2の回答者は「知らない」と答えている．また，すでにセキュリティポリシーを定めているところは20%弱で，約35%が作成中か検討中，40%以上の企業が「定めていない」と答えており，6割以上の企業には，専任のセキュリティ管理者または担当者がいない．さらに，不正アクセス対策では，従業員に対するパスワード管理を含むセキュリティ教育が必須であるにもかかわらず，なんと8割以上の企業が不正アクセス対策について従業員向けの教育・訓練の機会を設けていないと答えている．

どうもセキュリティ対策が十分でないのは官公庁だけではないらしい．

⊃ ECサイトへのサービス妨害攻撃

日本の官公庁のウェブサイトが攻撃された直後の2月始め，今度は米国の有名なECサイトがクラッカーに襲われた．襲われたのはポータルサイトのYahoo!やオークションサイトのeBay，書籍や音楽CD等のネット販売で有名なAmazon.comなどである．

クラッカーが利用した手法は，サービス妨害攻撃（DoS：Denial of Service，一般的には「サービス拒否攻撃」と呼ばれることが多い）の一種である「分散型サービス妨害攻撃（DDoS：Distributed Denial of Service）」であり，ウェブの改ざんではなく，標的となるサーバに処理能力を超える情報を一方的に送りつけることによって，サービスを不能にしてしまうという攻撃だった．つまり，データを盗んだり，改ざんしたりすることはできないが，サーバのサービスを不能にするという嫌がらせである．この連載の第8回で紹介したように，この種の攻撃を防ぐのはきわめて難しい．しかし，だからといってまったく対策がないわけではない．

DDoS攻撃を行うために，クラッカーはまず複数のコンピュータに，DoS攻撃を行うプログラムを仕掛ける．そのプログラムを一斉に動かすことによって，標的となるコンピュータを麻痺させるのである．つまり，DDoS攻撃のためには，踏み台となる複数のコンピュータに不正にアクセスして攻撃用のプログラムを植え付けるか，コンピュータウイルスのようにメールの添付書類などの形で送り込むという準備作業を必要とする．したがって，インターネットに接続されているすべてのコンピュータが十分な不正アクセス対策，コンピュータウイルス対策をとっていれば，DDoS攻撃を仕掛けることはできなくなるのである．

火災や地震などの物理的脅威に対するセキュリティ対策の場合は，対策を怠って被害が生じても，ネットワークで接続された遠方のコンピュータに被害が及ぶことはまずないだろう．しかし，このDDoS攻撃にみられるように，不正アクセス対策やコンピュータウイルス対策を怠れば，被害者ではなく，加害者になる可能性がある．

これはDDoS攻撃に限定される話ではない．たとえば，ウイルス対策が十分でなければ，取引先などにウイルス感染している文書ファイルを送り，相手のコンピュータに被害を与える可能性がある．また不正アクセス対策が十分でないために，SPAMと呼ばれる迷惑メールの発信サイトとして利用されたり，不正アクセスのための踏み台に利用されることもある．

情報セキュリティ対策は，もはや自分の情報資産を守るためだけに必要なものではない．ネットワークでつながった世界（サイバースペース）全体の安全を守るために必須のものといってよいだろう．自分が管理しているサイトにはさほど重要な情報は入っていないからセキュリティ対策が不十分でも問題ないと思っている管理者がいるかもしれないが，それは大間違いである．インターネットに接続するならば，セキュリティ対策を行うのは社会的義務なのである．

⊃ おわりに

どうも長い間ご愛読いただきありがとうございました．情報セキュリティ関連の技術標準の話や電子マネー，デジタル音楽配信と暗号の話などまだまだ取り上げるべき話題はあるのですが，「情報セキュリティ歳時記」は今回で終了させていただきます．次号からは別テーマでコラムを連載する予定になっておりますので，お楽しみに．では，また次号で．

今月の参考文献等
1)「情報セキュリティに関する調査」集計結果，(財) 日本情報処理開発協会 (Mar. 2000).

(平成12年4月12日受付)