COLUMN
米国インターネット事情

同時多発テロとインターネットのセキュリティ

前川　徹　早稲田大学国際情報通信研究センター
E-mail: tfm@zf6.so-net.ne.jp

同時多発テロとインターネット

9月11日に米国で発生した同時多発テロ事件は，インターネットの世界にも大きな影響を与えている．

まず，事件が発生した直後から，CNNやMSNBC，ABC Newsなどの主要ニュースサイト，ハイジャックされたアメリカン航空やユナイテッド航空のウェブサイトやホワイトハウス，国防総省，FBIなどの政府機関のウェブサイトへのトラフィックが急増し，これらのサイトは一時的に麻痺状態に陥ってしまった．インターネットのパフォーマンスを調査しているKEYNOTE社は，事件が起きた当日の午前9時から10時の間は，CNN.com，NYTimes.com，ABCNew.comへのアクセスはまったく不可能だったと発表している．多くのニュースサイトは，急増したアクセスを処理するために，コンテンツをテキスト主体に変更したり（CNN.comのトップページは255KBから20KBに縮小された），回線を増強するなどの対策を行ったのだが，それでもレスポンスはかなり悪かったといわれている．

こうした現象を捉えて，緊急時にインターネットは役に立たないと考えるのは間違っている．多くの人がプライベートな電子メール，メーリングリスト，電子掲示板によって家族，友人，知人の安否を確認している．私もニューヨークからの無事を知らせる電子メールを何通も受け取った．ネット上で交換された安否確認の情報は，おそらく大変な数になったに違いない．米国では "I'm Okay" Massage Center（http://okey.prodigy.net/）のような生存者を確認できる電子掲示板がいくつも設置されたが，日本でも独立行政法人の通信総合研究所が，日本時間9月12日の午前3時から「米国同時多発テロに対する被災者支援安否情報登録検索システム」の運用を開始した．こうした緊急時の安否確認には，電話よりインターネットの方がはるかに効率がよい．

W32/Nimda

同時多発テロ事件が起きてからちょうど1週間後の9月18日，きわめて強い感染力を持った新種ウィルスが現れた．W32/Nimdaである．同時多発テロ事件発生直後に，元国防総省の専門家が，テロリストたちによるサイバー攻撃が発生する可能性があると警告していたことや，このウィルスの名称を逆さまから読むと，Admin（istration）2（to）3（rd）W（ar）となり「政府が第3次世界大戦へ」という意味にもとれることなどから，W32/Nimdaはテロリストたちが開発したコンピュータウイルスではないかと取り沙汰された．

しかし，John Ashcroft司法長官は記者会見で，「ウイルス感染と同時多発テロ事件とを結びつける証拠は現時点では得ていない」と述べ，この噂を否定している．また，この怪しげなウィルスの名称の由来についてだが，感染したパソコンがウェブサーバに送り込むファイル名がAdmin.dll（ウェブ管理用のダイナミック・リンク・ライブラリ）なので，これが名称の由来ではないだろうか（名称の由来について国内の専門家に質問したが回答は得られなかった）．また，W32はWindowsの32ビット実行ファイルのウィルスであることを示しており，それ以上の意味はない．

このW32/Nimdaに感染する恐れのあるコンピュータは，MicrosoftのInternet-ExplorerとOutlook/OutlookExpressを使用しているWindowsパソコンとMicrosoftのIISバージョン4，またはバージョン5を使用しているウェブサーバである．

W32/Nimdaはきわめて強い感染力を持っているが，それは，これまでのコンピュータウイルスと異なり，いくつもの感染パターンが組み込まれているからである．まず，最近流行のウイルスのようにメールに添付されたファイル経由でも感染する．W32/Nimdaのやっかいな点は，readme.exeという名称のファイルが添付されたメールを，Outlookの場合はメールを開いただけで，OutlookExpressの場合はプレビューしただけで感染する点である．第2の感染経路はウェブサーバからパソコンへという感染で，ブラウザでウェブページを見ただけで感染してしまう．正確にいえば，パソコンから（欠陥のあるバージョンの）InternetExplorerでW32/Nimdaによって改竄されたウェブページにアクセスすると，"readme.eml" というファイルをダウンロードさせるためのJavaScriptが動作し，パソコンにウイルスが取り込まれてしまうのである．さらにこのウイルスは，パソコンからウェブサーバにも感染する．ウイルスに感染したパソコンは，セキュ

リティホールのあるMicrosoftのIISバージョン4，またはバージョン5を使用しているウェブサーバを探して，裏口からサーバにウィルスを送り込むのである．

この強力なウィルスに関する情報や対策方法は，IPAセキュリティセンターのウェブサイト（http://www.ipa.go.jp/security/）やワクチンソフトベンダのウェブサイトを参照されたい．

テロリストの暗号利用

一方，同時多発テロ事件の容疑者たちの痕跡がインターネット上で数多く発見されている．報道によれば，何人かの容疑者はフロリダ州のキンコーズに置かれている有料のインターネット端末を使って，トラベルサービスサイトにアクセスしており，米国No.1のトラベルサイトであるTravelocityは，2人の容疑者が同社のサービスを利用して航空券を予約していることを確認している．

実は，事件が起きる前から，テロリストたちがインターネットを利用しているという報道もあった．2001年2月6日のUSA Todayは，米国および外国の当局筋からの情報として，今回の同時多発テロ事件の首謀者だとされている「ビン・ラディン氏のグループが，スポーツ関係のチャットルームのメッセージやポルノサイトの写真の中に，次のテロ活動の計画やテロリストたちへの指示を暗号化して隠している」と報道している（http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm）．

写真などのコンテンツにメッセージを隠す技術はステガノグラフィー（Steganography）と呼ばれる．もちろん巧妙に隠されているので，目を皿のようにして写真を眺めてもメッセージを見つけることはできない．これに対してメッセージを鍵と演算したり並べ替えたりして意味不明のデータにする方法が暗号である．メッセージが暗号化され，さらに写真などのコンテンツに埋め込まれてしまえば，メッセージの解読はおろか発見さえも困難になってしまう．前述のUSA Todayの記事によれば，暗号技術はイスラム過激派にとって日常の道具になっているという．今回の同時多発テロ事件の容疑者たちがステガノグラフィーや暗号を利用していた証拠が見つかったというニュースはまだ流れていないが，その可能性は十分あるだろう．

そんな中，同時多発テロ事件が起きたため，連邦政府や議会では，暗号利用を禁止あるいは規制すべきであるという声が高まっている．

Zimmermann氏の涙？

2001年9月20日のワシントンポスト紙は，およそ10年前に暗号ソフト“PGP”を開発したPhil Zimmermann氏が，同時多発テロ事件以来，罪の意識に打ちのめされて毎日泣いているという記事を掲載した（http://www.washingtonpost.com/wp-dyn/articles/A1234-2001Sep20.html）．つまり，同時多発テロ事件の容疑者たちが，テロの実行計画を進める上で彼が開発した暗号を利用した可能性があり，彼らの通信が暗号化されていたために，テロを未然に防止できなかった可能性がある．それでZimmermann氏が罪の意識にさいなまれているというストーリーなのである．

しかし，9月24日，Zimmermann氏はPGP ver.7.0.3の電子署名付きの声明を発表し，PGPを開発したことで後悔はしていないことを明らかにした（http://www.philzimmermann.com/text/PRZ_Response_WashPost.txt）．この声明によれば，9月17日にワシントンポスト紙の記者のインタビューに答えたのは事実だが，その時に記者が読み上げてくれた記事原稿には，「罪の意識に打ちのめされて毎日泣いている」という表現もそんなニュアンスの文章もなかったのだという．おそらく，長い記事原稿を短くするという編集の段階で間違った表現が採用されたのだろうとZimmermann氏は推測している．

暗号利用規制論争の行方

どうやら，同時多発テロ事件を契機に暗号利用を禁止，または規制しようという動きが活発になっているようである．この問題は1990年代を通して何度も議論されてきた経緯がある．当時と比べて，連邦政府の次世代暗号が決定したなどの状況の変化はあるが，本質的な変化はない．

過去の米国の暗号規制論争については，本誌1999年6月号掲載の解説記事「緩和される暗号輸出規制　米国の暗号政策をめぐる論争を考える」Vol.40, No.6（pp.600-605）を参照いただきたいが，暗号の利用規制や輸出規制を行っても，犯罪者やテロリストによる強力な暗号の利用を阻止できるわけではない．すでに多くの暗号アルゴリズムは公知のものとなっているし，既知のアルゴリズムを利用した暗号ソフトウェアの開発に天才的なプログラマは必要ない．また，すでに強力な暗号ソフトは世界中にばらまかれてしまっているのである．利用できる暗号をキーエスクロー機能付きのものに制限し，それ以外の暗号利用を禁止することによって，（犯罪者やテロリストによる）容易に解読できない暗号の利用を阻止できるのではないかと考える人もいるかもしれない．しかし，暗号化したメッセージを写真などのコンテンツに埋め込むステガノグラフィーを用いれば，そんな規制は何の役にも立たないだろう．

おそらく結論は変わらないだろう．暗号利用の規制は実効性に乏しく，個人のプライバシー侵害の可能性を高め，情報技術産業の足を引っ張ることにしかならないのだから．

（平成13年10月4日受付）