
**この 6 月 26 日、日本で成立した著作権改正に抗議する国際的なハッカー集団アノニマスが、日本政府および関連のサイバーサイトにハッキング攻撃を仕掛け話題になっている。それに先駆けて 6 月 1 日、アメリカニューヨーク・タイムズ紙は、アメリカ／イスラエルが、国家戦略としてイランにサイバー攻撃を仕掛けていたことを明らかにした。「マルウェア」という悪意プログラムを駆使したものだが、何と言ってもショッキングなのは「アノニマス＝匿名」者によるハッキングではなく、正規の国家／政府による他国への攻撃作戦だった点である。**

## 国家主導のサイバー攻撃が明るみに

米ニューヨーク・タイムズ紙は、この 6 月 1 日付け紙面で、米国とイスラエルが共同開発した「スタックスネット」(Stuxnet)と呼ばれるマルウェア（悪意ある感染性プログラム）が、イランの核施設をサイバー攻撃して、ウラン濃縮計画を大幅に遅らせたと報じた。

このニュースが衝撃的であったのは、イランの核施設へのサイバー攻撃が、米国とイスラエルの両政府の共同によるものであることを、世界に公にしたからである。これについて、米国は認めていないがイスラエルは認めている。

このサイバー攻撃は、ブッシュ前政権時代の 2006 年に「オリンピック・ゲーム」の暗号名で計画がスタートし、2008 年には実際の攻撃が始まった。この攻撃は、現オバマ政権に引き継がれ、2010 年の大掛かりなサイバー攻撃となったのである。

2010 年 11 月、イランのアハマディネジャド大統領は、サイバー攻撃を受けたことを認めている。しかし、この時点では、どこからの攻撃かについては憶測の域に

留まっていた。

このサイバー攻撃が衝撃的だったのは、敵対国の社会・経済的インフラの機能不全を狙い、多大な戦果を挙げたという点にある。サイバー攻撃の目標が、ウェブサイトからの情報流出やパソコンの機能マヒといったレベルから、社会・経済的インフラを狙うだけでなく、特定のターゲットに的を絞って攻撃するレベルへと飛躍した点にある。

まさに、これまでの戦争の概念を根本から覆す「サイバー戦争」の戦略的兵器となったのである。ネット空間は、米国防省が名づけた、陸、海、空、宇宙に次ぐ「第5の戦場」（The Fifth Domain）の場に化してしまったのである。

このスタックスネットは誰が何の目的で開発したかは不明であったが、破壊力と目標とされた施設の危険性ゆえに、世界のマスコミが一斉に取り上げ始めた。我が国では、NHK が「21 世紀の戦争・サイバー攻撃の恐怖」（BS1 ドキュメンタリー WAVE、2011 年 11 月 26 日放送）で、核施設への攻撃の模様を紹介している。

今回のニューヨーク・タイムズ紙の報道は、国家主導によるサーバー戦争が既に始まっていることを、世界に確信させた点にある。国家によるサイバー攻撃と疑われた大規模なサイバー攻撃の最初は、2007 年のエストニアの政府機関や金融機関に対してであり、3 週間にも渡り続けられ、銀行機能そのものをマヒさせている。

このような国家主導になるサイバー攻撃は、遠い（？）中近東の話ではない。韓国では北朝鮮によるサイバー攻撃が、今年 5 月以来、重大な関心事となっている。韓国の飛行場を発着する航空機が利用する GPS（衛星利用測位システム）が狙われ、システム障害が頻発しているからである。韓国政府は、北朝鮮からの撹乱電波によるものとしている。

この 6 月には、北朝鮮の金正恩第 1 書記を侮辱した韓国の新聞社がサイバー攻撃を受けて、新聞製作のサーバーが被害を受けた。韓国と米国の両国は、ワシントンの共同会議で、サイバー攻撃の挑発が続けば報復するとのメッセージを発している。

## パンドラの箱を開けた「スタックスネット」

スタックスネットは、APT（Advanced Persistent Threat）攻撃と呼ばれる標的型攻撃の一種である。APT とは、「サイバー攻撃の一種で、特定のターゲットに対して持続的に攻撃・潜伏を行い、様々な手法を駆使して執拗なスパイ行為や妨害行為などを行うタイプの攻撃の総称である」(IT 用語辞典)。

これまでのマルウェア（malware）との基本的な違いは、特定のターゲットだけを狙って攻撃する点にある。不特定多数を狙うこれまでのマルウェアは、広範囲で発見され被害も浅く、その対策も早期に始まる。逆に、APT はターゲット以外の場所では被害が発生しないため発見されにくく、ターゲットの被害は大きくなる危険性が高い。

東京大学の坂村健教授は、このスタックスネットについて、「パンドラの箱を開けてしまったマルウェア」とその脅威を強調している。一つには、ネットに接続されていない工場や発電所をも攻撃出来ることを、初めて実証したマルウェアであるからである。

これまでは、マルウェアやコンピュータウィルスは、インターネット経由で感染するため、インターネット網から隔離しておけば安全だというのが、ネットワーク専門家の常識であった。この常識が、根本から覆されたのである。

スタックスネットの仕組みの狡猾性については、坂村健教授が分かりやすく簡明に説明しているので、ここにそのまま紹介させてもらう（毎日新聞　2012 年 6 月 19 日付け）。

「スタックスネットはミサイルと言われるぐらい悪質で、標的を確認し破壊効果をおよぼす弾頭部と、その弾頭を敵陣に届ける運搬部に分けられる。

運搬部はさまざまなシステムの抜け道を組み込んだハッキングツールの集大成になっていてインターネットだろうが USB メモリーだろうが、あらゆる方法を試し、外に自分のコピーを送りつけようとする。攻撃対象にたどり着いたと弾頭部が判断すると、実際の破壊工作を開始する」。

スタックスネットの分かりやすく詳しい説明、感染の経緯や技術的仕組みなどについては、一般社団法人 JPCERT／CC の小熊信孝氏による「Stuxnet—制御システムを狙った初のマルウェア」が、参考になるので参照されたい。(2011 年 2 月 18 日付け、パワーポイントで図解、www.jpcert.or.jp/ics/2011/20110210-oguma.pdf )

さて、問題は脅威となるマルウェアはこれだけではなく、次々と新種が発見されている点にある。すでに、「デューク」（Duqu）と Flame といったマルウェアが発見されている。デュークは 2011 年 10 月に発見され、スタックスネットとコードが似ており、スタックスネットから派生したもの見られている。

Flame は、先月の 2012 年 5 月に発見されており、これまでに発見されたマルウェアの中で、最も高度で洗練されたものと言われている。米ワシントン・ポスト紙（2012 年 6 月 19 日）は、イランの核燃料濃縮処理を妨害するサイバー攻撃に向けて、米国とイスラエルの両政府が共同開発したものだという証言を伝えている。

## APT 攻撃の脅威にどう対処するか

我が国では、関西電力の大飯原子力発電所の再開が決定し、他の原子力発電所も再開に向けて動き始めている。地震や津波対策だけが問題視されているが、核施設関連へのサイバー攻撃に対して、国家レベルでの対策が早急にかつ真剣になされる必要がある。

福島原発事故では、チェルノブイリやスリーマイルの原発事故の教訓を生かせなかった。イラクの核施設へのサイバー攻撃の教訓が、軽視されるようなことは絶対

にあってはならないといってよい。

すでに、我が国でも衆議院や大企業などでウィルスやマルウェアによる被害が報告されている。2011 年 8 月には、三菱東京 UFJ 銀行や北海道銀行などのネットバンキングに対する攻撃も発覚している。

同じ 8 月には、三菱重工業の国内 11 拠点でサーバーPC83 台がマルウェアに感染し、翌 9 月にマスコミに公表され、大きな騒ぎになったことは、記憶に新しい。原子力企業や金融機関といった産業界のインフラ企業が、狙われ始めている。

この原稿を書いている現在も、財務省や裁判所、自民党・民主党などのウェブサイトがサイバー攻撃を受け、内容の書き換えや閲覧不能といった被害が、6月26日から発生している。国際的なハッカグループ「アノニマス」が犯行声明を出しており、28日も攻撃を続行すると予告している。

このようなサイバー攻撃に対して、監督官庁の防衛省（2007 年設立）も、平成 23 年版防衛白書（2011 年 8 月発行）の「サイバー空間をめぐる動向」( 第 I 部、第 1 章、第 1 節)の「2.サイバー空間における脅威の動向」で、スタクスネットの脅威について報告している。

しかし、具体的な防衛体制は、あまりにもお粗末である。2005 年 3 月に、陸上自衛隊通信団の下に「システム防護隊」が設置されたのが、最初である。これは 2000 年に発生した中央官庁のホームページ改竄事件を受けて設立されたものである。ただし、陸上自衛隊の電算機システムをサイバー攻撃から防護すること及びサイバー関連情報に関する調査研究を任務とするに過ぎない。

本格的なサイバー部隊の設置については、来年の 2013 年度末に、陸海空 3 自衛隊の統合部隊である「サイバー空間防衛隊」が新設される予定になっている。この部隊では、「各省庁や出先機関、防衛関連企業のシステムなどの防御も検討している」という（産経ニュース、2012 年 1 月 21 日付け）。

最大の問題は、わが国ではサイバー戦争時代に対応できる国家軍事戦略が、欠如している点にある。我が国は戦後一貫して「専守防衛」を国家戦略としてきている。このため、自衛隊は、相手国とその物理的破壊攻撃が確認できない限り、防衛措置は取れない。

すなわち、未確認の相手国からのサイバー攻撃に対して、自衛隊は何らの対処も出来ないのが実情といってよい。この問題は、政治家の意思決定の問題である。核施設へのサイバー攻撃を視野に入れた国家戦略の見直しが、急務といってよい。

つい最近、「サイバー攻撃に自衛権行使可能、外務省が見解」（読売新聞、2012年5月15日）という報道があつた。外務省がサイバー空間について、国連憲章など現行の国際法が適用されるとの見解をまとめ、4月26日に開かれた政府の情報セキュリティ政策会議に提示していたという。この会議は、関係閣僚が集まってレベルに過ぎず、今後の進展を望む次第である。

（ TadaakiNEMOTO ）