NIDS 防衛研究所
The National Institute for Defense Studies

コンピューターウィルス Stuxnet によるイラン核関連施設攻撃
～核不拡散政策からの視点～

企画室 兼 研究部教官　須江　秀司

NIDSコメンタリー
第 20 号　2011 年 5 月 16 日

イラン・ナタンツに所在するウラン濃縮施設に対して、Stuxnet と呼ばれるコンピューターウィルスが攻撃をしかけ、同施設内に設置される遠心分離機の一部が破損したと伝えられている。核開発に邁進するイランにとり、ウラン濃縮技術は原子炉に装填する核燃料棒を生産するために必要であるとともに、核兵器製造に必要な高濃縮ウラン（HEU）生産に転用可能な技術である。Stuxnet による攻撃は、疑惑がもたれるイランの核兵器開発を標的にした米国及びイスラエルの共同オペレーションであるという報道が多いものの、その詳細は不明である。しかし、この攻撃によって「イランの核開発が数年遅れた」（ヒラリー・クリントン米国務長官）とも言われている。

イラン核関連施設に対する軍事攻撃がこれまでたびたび指摘される中、ウィルス攻撃は人的被害を伴わずに核開発を遅らせる効果を示したことから、核不拡散政策の新たなツールとしての可能性が注目され、中には「軍事攻撃に勝る」との意見もみられる。本稿では Stuxnet の概要に触れ、核不拡散政策としての役割について軍事攻撃と比較しつつ検討してみたい。

Stuxnet による被害とその侵入の手口

Stuxnet は 2009 年頃から、ナタンツのウラン濃縮施設に侵入し、同施設内に設置されている遠心分離機約 9,000 基のうち、約 1,000 基を破損させたと考えられている。国際原子力機関（IAEA）も、イランの濃縮ウラン生産量が一時期中断し、イランが破損した遠心分離機を同施設から運び出しているところを確認しているようである。イラン・アフマディネジャド大統領も Stuxnet であるとの名指しは避けたものの、ウィルスによる被害を認め西側諸国の攻撃であると非難している。

Stuxnet の特徴は二つあげられる。一点目は、Stuxnet は一端コンピュータに侵入した後、活動を開始する条件が整うまで潜伏する。実際に Stuxnet が「猛威」を振るうのは、ドイツ・シーメンス（Siemens）社の周波数変換器を使い、特定の周波数域で稼働する機器だと考えられている。Stuxnet はコンピュータを乗っ取った後、周波数を断続的に変化させるが、これに応じて遠心分離機の回転数も大幅に増減し、その結果、遠心分離機に過大な負担がかかり破損に至った模様である。二点目は、遠心分離機の稼働状況が異常を呈しているにもかかわらず、制御システムは管理者に対して稼働状況が「正常」であるというシグナルを送る機能も備えていたといわれている。

Stuxnet の被害はイランのみならずインドネシア、インド、アゼルバイジャン、パキスタン等、複数の国で報告されているが、被害件数のうち大半がイランであった。更に、Stuxnet に仕込まれた技術的特徴が、攻撃を受けたウラン濃縮施設の設計情報と一致しているという点からイラン核開発が標的であったと考えられているのである。

また、この他に注目すべき点は、当初、イラン国内で Stuxnet の被害が報告されたのは、最終的なターゲットとみられるウラン濃縮施設そのものではなく、同国内に所在する複数の企業だったことであろう。専門家の見方をまとめると、ウラン濃縮施設のコンピュータシステムを直接ウィルスによって「感染」させることは容易ではない。このため、まずは間接的にウラン濃縮施設と関係があるとみられる企業や関係者のコンピュータに Stuxnet を侵入させ、その後 USB 等の可搬記憶媒体を使ってナタンツのウラン濃縮施設への侵入を待つという手順だったとみられている。このことから、Stuxnet の製造者はイランの核開発、とりわけウラン濃縮施設に必要な関連品調達網や関係機関に関する非常に確度の高い情報を把握していたものと考えられている。

核不拡散政策の新たなツール

国家等による核兵器開発の目論みを阻止する為には、外交的手段、軍事的手段等、複数の方策を組み合わせて行われる。その中でもとりわけ米国が積極的に進めてきた拡散対抗（counterproliferation（CP））とよばれる手段は、核拡散を予防する他にも、実際に拡散してしまった場合に、これを撤去する為の措置も包含するものである。例えば、核兵器開発に使われるおそれのある懸念資材・技術の輸出管理といった政策から、海上でこれらの懸念

物資を運搬する船舶を拿捕するケース、そして 1981 年にイラクのオシラク原発や 2007 年にシリアの核関連とみられる施設がイスラエルによって空爆されたことに代表される軍事攻撃が顕著な事例であろう。

ここで Stuxnet が与えた影響を検討してみると、イランの核開発が遅れたことのみではない。この他にも、例えば、イランがウィルスによる「再感染」を防止するために、ウラン濃縮活動に必要な資材の調達網見直しや、核開発全般の資材供給ルートの再構築を迫られる可能性があり、核開発に要する諸々のコストが増加するという効果があるだろう。これらの点を踏まえると、Stuxnet は CP の主目的に沿ったものであり、新たな可能性を示したともいえるのではないだろうか。

軍事攻撃との比較

では果たしてウィルス攻撃が、イスラエルが実施したような軍事攻撃に勝るのか。ウィルスが持つ最大の特徴の一つは、存在が未確認の施設に対しても攻撃が場合によっては可能になるという点である。つまり、仮にイランがナタンツ以外に秘密裏の濃縮施設を保有し、ナタンツと同様のシステムで遠心分離機を稼働させていた場合、その施設にも被害が及ぶ（あるいは既に及んでいた）可能性も排除できないであろう。

更に、ウィルスによる攻撃は、犯人が特定されにくいという特徴がある他、攻撃による人的被害が出るリスクが極めて低いことも大きな利点であろう。ある試算によると、実際にイラン核施設に対する軍事攻撃に踏み切った場合、地対空ミサイル、戦闘機等による迎撃が考えられ、双方に人的被害が発生するリスクがあることは言を俟たない。

一方、デメリットであるが、ウィルス攻撃による効果の判定が難しいことではないだろうか。少なくとも、イランが保有する遠心分離機の約十分の一にダメージを与え、濃縮活動を一定期間遅らせることができたようであるが、実際の被害の状況は不明である。また、イランがウィルス攻撃から比較的早く復帰したといわれており、Stuxnet 攻撃の効果にも疑問が残る。イランは単に濃縮施設を停止させ、破損した遠心分離機のカスケード（遠心分離機が連結したもの）を隔離した模様であり、被害を最小限に食い止めることがそれ程困難ではないとも考えられていることである。

最後に、ウィルス攻撃が果たしてイランの核開発の意図を挫くことに成功したか否かという点であるが、イランのソルタニエ国際原子力機関（IAEA）担当大使は「ウィルスによって、イランのウラン濃縮活動を阻止することはできない」と述べており、また、イランがその後も濃縮活動を継続していることを考えると、この点も効果はないようである。しかしながら、空爆によって必ずしもイラク、シリアが核開発を放棄しなかった（していない）事例も同様に指摘しておくべきであろう。実際、イラクはイスラエルによる攻撃の後、少なくとも 1991 年の湾岸戦争以前までは複数のウラン濃縮活動を開始させ、核兵器開発を急速化させていたことが判明している。また、シリアも IAEA の査察に協力的な態度を示しておらず、核開発の透明性は確保されていない。

このようにウィルス攻撃は核開発を遅らせることはできたとしても、核開発の意志を放棄させることまではできないのではないだろうか。そして、少なくとも上述した点を考えるだけでも、ウィルスが「軍事攻撃に勝る」という主張を積極的に支持することは難しいかもしれない。但し、その潜在的な能力は、近年指摘されることの多い核技術・資材を融通する闇ネットワークの問題と絡めた場合、注目すべきものがあろう。同ネットワークには複数の国が関与していたため、全体像を把握し効果的な核不拡散政策を実施することは困難であることは否定できない。しかし、このことは Stuxnet の効果が、その制作者が意図した範囲を超える可能性があることもまた同様に示しているともいえるのではないだろうか。

プロフィール profile

企画室 兼 研究部

須江 秀司

専門分野：軍備管理・軍縮・不拡散

防衛研究所企画室
直 通 ： 03-3713-5912
代 表 ： 03-5721-7005（内線 6258）
FAX ： 03-3713-6149
※ 防衛研究所ウェブサイト：http://www.nids.go.jp