【第１６４回】　　平成２４年１０月３０日

遠隔操作事件が露呈したサイバー安保の不備

サイバーセキュリティ研究所長　伊東寛

遠隔操作ウイルスによる冤罪事件が注目を浴びている。他人のパソコンを遠隔操作して犯罪を行った者がいる。それに対し警察が無実の人を逮捕し、一部の人はやってもいない犯罪を自白したとの報道がなされている。

真犯人と称する者からの告白文を信じれば、この犯罪は警察に恥をかかせるのが目的で、その手段としてサイバー技術を利用したということである。この犯罪が成立した要因は、現在のサイバー空間はその仕組み上、真犯人をたどることが担保されていないところにある。

今回、警察は「なりすまし」の可能性を見落としていたと言われているが、それよりも、この件は日本全体のサイバー安全保障体制が不十分であることを立証したように思う。

●戦争の引き金にも

サイバー技術が広く人々の手に入るようになった時代には何が起こり得るだろうか？例えば、尖閣諸島で中国海軍と海上自衛隊が対峙する事態が発生したとしよう。その場合、両軍は戦闘に入ることを望まないだろう。中国海軍は現在の実力では海自に勝てないだろうし、海自は日本の平和主義による束縛から抑制がかかるからだ。

ここで民間人はどう行動するだろうか。ネット上で自国の主義主張の表明、相手国の誹謗、やがて相手国へのサイバー攻撃を始める。（一般人からの攻撃を装っても、裏に中国政府がいる可能性もある。）そして、攻撃が物理的損害・人的被害を発生させた時、それまで抑制がかかっていた軍のたがが外れ、実際の戦闘の引き金を引いてしまうかもしれない。

さらに、真の攻撃者がわからないサイバー攻撃の特性を考慮すると、もっと厄介な問題がある。日中は戦争になってもお互いに何の利益もない。が、双方が攻撃し合って多額の費用を使い、それぞれの資産を失うことが、自分の利益になると考える第三国あるいは何らかの非政府主体が、なりすましのサイバー攻撃を行う可能性もあるのだ。もし中国に悪意があれば、自作自演のなりすまし攻撃さえ想定できよう。ことは極めて厄介である。

●日本は何をなすべきか

少なくともそうした事態を起こさないためには「なりすましができないような技術上の仕組み」をインターネットに加えること、及び、民間インフラに対するサイバー攻撃の禁止等を盛り込んだ国際条約を制定すること、信頼できる多数の同盟・友好国を持つこと、なにより、それにふさわしい制度や実力を日本が持つことである。これを達成するには、日本のあり方そのものも変えなければならないのではないか。今、真剣に考えるべき時が来ているように思う。

（本内容は、現時点で報道に出ていることに基づいた筆者の個人的見解であり、会社の意見を代表するものではない。）