COLUMN

ひしぬま・ひろゆき◎情報通信研究機構欧州連携センター長。1991年、郵政省（現総務省）に入省し、2011年7月から現職

欧州ICTレポート

サイバー攻撃に対抗する法規範と技術

菱沼宏之

2007年のエストニアに対するサイバー攻撃、2010年のイラン核施設に対するサイバー攻撃などを契機として、世界的にも、サイバーセキュリティ（情報通信セキュリティ）、とりわけ、サイバー犯罪やサイバー戦争に注目が集まっている。我が国においても、2011年に多くのサイバー攻撃が報告されたのは、読者の皆様もご承知の通りである。

このため、これまで陸・海・空を主な戦闘空間として考えてきた各国の防衛関係者の間でも、宇宙空間とサイバー空間を、第4・第5の戦闘空間として捉え始めている。

サイバー犯罪については、欧州評議会を中心にして、2001年に成立し、2004年に発効した「サイバー犯罪に関する条約」（いわゆるブダペスト条約）が知られており、欧州以外の国にも一部広がりを見せている。

サイバー犯罪にとどまらないサイバー戦争については、一説によれば、国際連合憲章第7章（平和に対する脅威、平和の破壊及び侵略行為に関する行動）が適用され、また、戦時国際法としての1949年のジュネーブ条約が、兵器を限定していないことから、適用されると言われている。

近年、サイバーセキュリティの観点から、インターネットガバナンスフォーラム、OECD、G8サミット、New World 2.0（2011年10月、フランス）、ロンドンサイバー国際会議（同年11月）などで活発な議論が行われているのは、本連載の諸氏が指摘している通りである。

このようなサイバーセキュリティに関する議論の中で、私が注目しているのは、法規範と技術による対応である。

サイバー犯罪に関する条約は、その成り立ちが欧州中心であるにせよ、欧州以外の国でも採択可能であるという点で、現実的な選択肢となり得る。これを超えて新たな条約を策定しようとすると、一からの議論となって、あるフランスの外交関係者によれば、議論だけで50年もかかりかねず、条約ができた時点でサイバー犯罪の水準ははるか先を行っていることになろう。この点で、上海協力機構などが提唱するサイバーセキュリティやサイバー犯罪に関する国際的な法的枠組みについては、疑問なしとしない。技術進展が早く、自由な情報流通が民主主義や経済・社会活動を支える本分野においては、せいぜい、拘束力の弱い行動規範のようなものにより対応すべきであろう。

また、情報通信分野のセキュリティには、サイバー攻撃がネットワーク上で技術的に行われる以上、規範による対応だけでは限界があり、技術的対応が重要である。筆者が最近参加したフランス国防高等研究所の研修における講演では、サイバーセキュリティ対応には、例えば、アドミニストレータ（ネットワークの管理者）が毎日パッチを当てるようなインセンティブを持つことが必要であるところ、安全なシステムを維持するためのコストについて所属する会社の経営層から必ずしも十分な理解が得られず、会社や政府から必要なコストがかけられていないとの指摘があった。

筆者の所属する情報通信研究機構では、「nicter」というインシデント分析システム（ネットワーク攻撃可視化・分析技術）を研究開発しており、サイバー攻撃に起因したセキュリティインシデントの早期発見、原因究明、対策法の導出を目指している。このような技術的対応をもとに国際協力を進めていくのが有力な現実的選択肢であろう。

※本稿は、筆者の個人的見解である。

※本コラムは欧州在住の6氏によるリレー連載です。