http://decfamily.p1.bindsite.jp/2017/

We 25R

No.217　17/05/12

サイバー空間と法律

昨日の新聞に掲載された記事を紹介しよう。（朝日新聞DIGITAL　5月11日）

＊

サイバー防衛に自衛隊本腰
反撃なら…９条との関係課題

サイバー空間での実戦に向け、政府が本腰を入れ始めた。自衛隊のシステムをサイバー攻撃から守る模擬訓練のため攻撃要員を初めて配置。実戦で敵に反撃する能力の育成も視野に入れる。ただ、憲法との関係で課題は少なくない。

政府は今年度予算に「実戦的サイバー演習の実施体制の整備」という項目を盛り込んだ。防衛省が設立した「サイバー防衛隊」を１割増の約１１０人体制に拡充。２０１６年度とあわせ約８億円をかけ、自衛隊のシステムのダミーを使う訓練環境を省内に設ける。

「実戦的演習」では、自衛隊の中央からの指揮や全国の部隊間の通信をつかさどるシステムに、攻撃役の隊員らが侵入を図る。守備側はふだんシステム監視を担当する隊員ら。別の部屋でパソコン画面をにらみ、撃退を図る。

通常のネット環境での模擬訓練はすでに３月に初めて実施した。「不審なメールが開封された」という連絡を受けた守備側が、システム障害やウイルスを確認。攻撃役が作ったシナリオに沿った侵入を防げるかどうかを判定役の隊員らが見つめ、数時間の攻防後には研究会で検証した。

演習とは別に、「侵入テスト」にも乗り出す。実際の自衛隊のシステムをサイバー防衛隊が攻撃し、弱点を探し出す仕組みだ。同省幹部は「守りの強化には、こうした実戦的な訓練が必要だ」と説明する。

不正アクセスなどで政府への「脅威」とされたサイバー攻撃は、１５年度で６１３万件。防衛省・自衛隊への攻撃は約１００万件にのぼる。サイバー防衛隊に攻撃役を新たに置くのは、「日進月歩のサイバー攻撃に追いつく訓練シナリオを練るため」（担当者）。通信やコンピューターに詳しい自衛官を選び、国内外の大学で情報セキュリティーを学ばせた。留学先には、米国防総省と協力するカーネギーメロン大もある。

「戦争」の形を大きく変えるサイバー攻撃への備えは各国で加速。自衛隊が訓練用として育てつつある攻撃能力は、反撃にも使える。防衛省の担当者は「法的整理が追いついておらず、自衛隊が実際に他国を攻撃するのは難しい」と話す。そもそも憲法との関係の整理がまだまだだ。

政府は最近の国会などで、敵のサイバー攻撃がインフラなどに「物理的な損傷」を与えるか、ミサイル攻撃と結びつくなど「武力攻撃の一環」なら自衛権を行使できると説明している。１８年度までの中期防衛力整備計画には、「相手のサイバー空間の利用を妨げる能力保有の可能性も視野」と盛り込んだ。

だが、国境を越える匿名のサイバー攻撃はハッカーやテロリストによる犯罪だけでなく、米中ロといった大国の関与も指摘され、国際的な定義や規制は見えてこない。実際、憲法９条に基づく必要最小限の自衛権でどこまで対応できるかについて、政府は国会答弁で「一概に言えない」と言葉を濁している。

米国では政府のサイバー能力向上で監視社会の問題も浮上。犯罪捜査が通信の秘密を脅かすとの指摘は憲法２１条との関係で日本でもあり、サイバー攻撃をめぐる論点は山積している。

＊

我々が「戦争」という語でイメージする状況とは異なる事態が生まれている。監視社会の問題も含め、これからの法学には、新しい技術に向き合う視点が欠かせないようだ。