



## サイバー・テロの脅威

3月15日夜、成田空港の航空管制用の電波が、北朝鮮から発射された同一周波数の妨害電波で4時間近く混信した。

同様の混信は3月9日、11日、14日にも確認されており、いずれも「会話の際に耳障りな程度」で管制システムに大きな混乱は生じなかったが、今少し強度な電波が発射された場合には航空管制業務が混乱し、重大事故に至る可能性があったという（今までにも平成17年3月に、北朝鮮からの同じ周波数の電波によって管制通信が不能となって、成田空港や航空機のチャンネルの変更を余儀なくされたことがあった）。

総務省では、国際電気通信連合（ITU）に今回の無線妨害を通報して、北朝鮮の混信排除を要請することを検討しているとのことである。

しかし、事は重大であり、単なる要請の検討にとどめず、関係省庁が一体となって、監視体制を強化して、航空管制の混乱を狙うサイバーテロの予防の充実強化に努めるべきであろう。

我が国では、現実に重大な事態が発生しているにもかかわらず、そのことの国民への周知徹底を図ることが怠られがちであって、平和ボケした国民と関係当局はいずれもが、自分だけは安全と決め込んで「いざ鎌倉」の場合への準備はついに整備されないままに終わることが多い。

他方、米国では、国防総省が3月5日に2008年版の「中国の軍事力に関する年次報告書」を米議会に提出し、その中で、最大の懸念として、中国の宇宙軍拡と核ミサイル増強を挙げ、特に米政府機関へのハッカー攻撃に警鐘を鳴らしている。

具体的には、2007年において中国を発信地とする国防総省など米機関のコンピューターへのハッカー攻撃による侵入が相次いでいると指摘し、中国が、米軍の軍事行動が依拠している偵察衛星や通信衛星によるNCWシステム（ネットワーク中心の戦争）の破壊を企てているとしている。

こうした事柄についての米国の厳しい認識と対処は我が国も共有すべきであって、いたずらにイージス艦の衝突事故の責任追及にのみ明け暮れていていいものではない。

北朝鮮や中国のサイバーテロ能力は、右に挙げた彼等の実際の行動事例に徴すれば、かなり高度なレベルに達していると思わなければならない。我が国もまた、いつ彼等のハッカー攻撃にさらされるかもしれない。いや、既にさらされているのだ。

因みに警察庁が毎年まとめている「情報技術解析年報」の平成19年度版では、全国の警察施設のインターネットコンピューターに対する外国からの無差別攻撃件数は年間8万件を超えていると報告されている。

このことから推定すれば、民間の重要インフラ事業者のインターネット上で発生しているであろう同様の事案はかなり数多いものと思われる。

警察庁が提言している数々の予防措置を早急に講じなければ、情報セキュリティ侵害事業の被害を防止することはかなり困難である。

今こそ、平和ボケを払拭して、来るべきサイバーテロの危険に対して、官民の緊密な連携による対策の充実を図ることが喫緊の急務であることを強く自覚すべきである。