

重要インフラ監視容認を



有識者に聞く



慶大教授 土屋 大洋氏

つながら。
米国の一部企業は政府の情報収集や偵察に協力する。犯罪集団や国家によるサイバー攻撃から利用者を守る。通信事業者は政府の通信傍受に協力しなければならぬと定める法律がある。

米中が対立する局面では陸海空の戦いと同時に、サイバー攻撃が起こりうる。米国と同盟関係にある日本は社会インフラが狙われて混乱する状況下で、領空・領海への侵犯が起こる可能性もある。

英シンクタンクの国際戦略研究所（IISS）が6月に発表した各国のサイバー能力に関する報告書は、日本を最下位のグループに位置づけた。米国や中国、ロシアなどと比べると日本は最下位どころかランク外と言えるほど大きな差がついているのが実態だ。

米国は安全保障上の理由や自国企業の利益を守る目的で、平時から外国のネットワークにひそかに侵入して秘密情報を得ているとされる。「積極的な防衛体制（アクティブ・ディフェンス）」と呼ばれる手法だ。

潜在的な攻撃者を平時から監視し、兆候をつかんだ場合は攻撃防止策をとる。攻撃主体を特定し、時には政治的・経済的制裁を加える。攻撃する代償は大きいと認識させることが抑止に

な「積極的な防衛体制」をとりにくい。プライバシー侵害への懸念があり、平時から無制限に監視する仕組みを導入するのはハードルが高い。サイバー空間を防衛するために重要インフラなどを例外的に監視する措置を検討する必要がある。

たとえば一般国民の監視ではなく、五輪などサイバー攻撃を受けやすい大規模イベントの期間中や、重要なインフラに限って保護する方法が考えられる。電力や鉄道などの基幹インフラを担う企業に絞って政府に情報提供を可能にするような仕組みも選択肢となる。

◇ 世界共通の課題であるサイバー防衛は岸田政権でも対応が急務となる。有識者に意見を聞いた。