シリーズ　サイバーセキュリティとデジタル化戦略を考える④

デジタル化戦略の要であるサイバーインテリジェンスとセキュリティクリアランス

慶應義塾大学 特任教授
手塚　悟

はじめに

本シリーズも最後の第４回目となった。第３回では「わが国の国家安全保障におけるサイバーセキュリティとデジタル化戦略」を論じ、日米同盟の下、米国に遅れているデジタル化をいかに推進し、追いつくかについて述べてきた。今回はより具体的に「デジタル化戦略の要であるサイバーインテリジェンスとセキュリティクリアランス」について検討する。

サイバーインテリジェンスのデジタル化

わが国に国家レベルでのサイバーインテリジェンスシステムがないことは、前回で述べた。それが日米同盟やFive Eyes等との情報連携において、極めて問題であることも指摘した。

図１のように、Five Eyesにわが国が加わってSix Eyesになるためには、インテリジェンス情報のGive & Takeの関係が加盟国同士で成立していなければならないことを第２回目で述べた。わが国がFive Eyesのメンバーになるためには、少なくともわが国からGiveできるインテリジェンス情報を収集できなければならない。つまりOSINT（Open Source Intelligence）情報等の情報収集・分析・解析が、平時から常に実施できるだけの環境がなければならないのである。

図２は第１回でも掲載した、わが国におけるサイバー分野の全体像である。この全体像に対して、サイバーインテリジェンスのデジタル化を実現するためには、どのように機能がマッピングされるかを整理するのが極めて重要である。

図３は、サイバーインテリジェンスシステム

●わが国は、ファイブアイズのGive&Take情報共有の枠組みへの参画が必要である
●ファイブアイズの枠組みに参加するためには、わが国において未整備の国家サイバーインテリジェンスシステムを可及的速やかに構築する必要がある

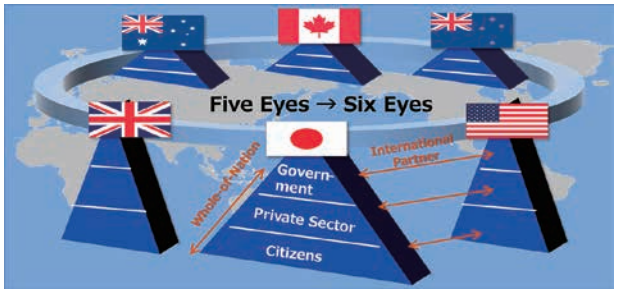

図１

●わが国におけるサイバー分野の全体像

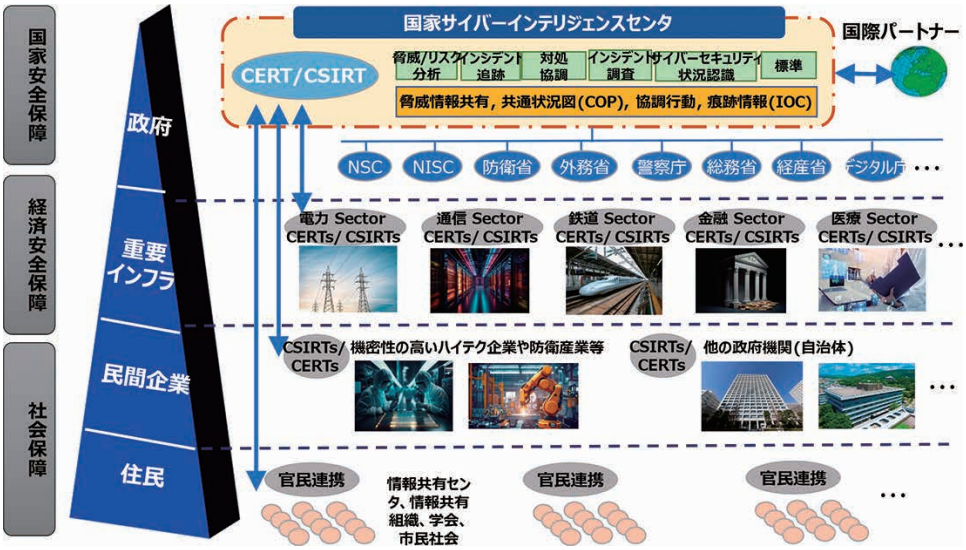

図２

●サイバーインテリジェンスシステムの機能

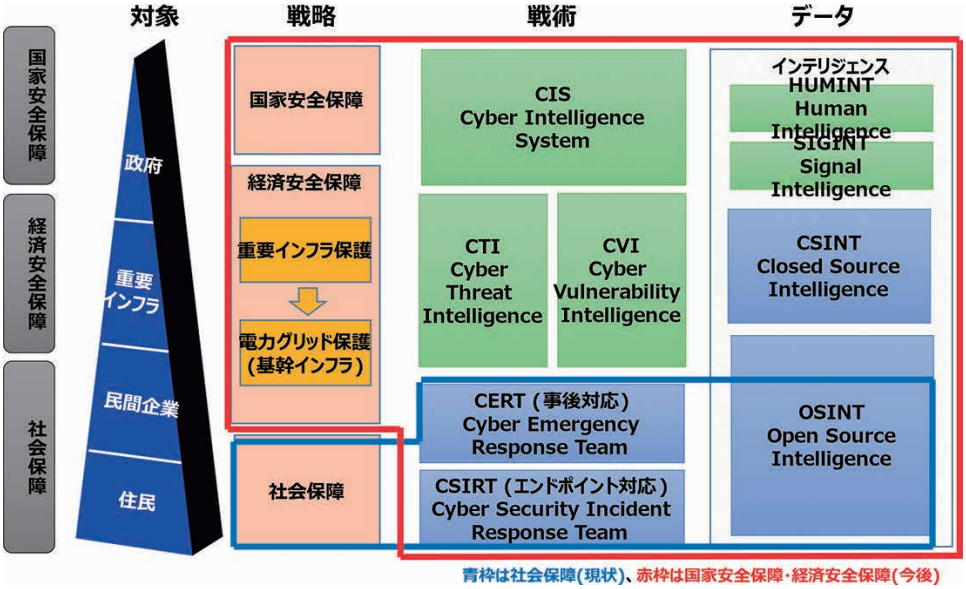

図３

の機能を示したものである。縦軸に国家安全保障、経済安全保障、社会保障、横軸に対象、戦略、戦術、データと分類を整理し、それぞれに当てはまる機能をマッピングしている。各分野で必要とするサイバーインテリジェンス機能は、青枠で囲まれた社会保障においては既に構築されている。青枠を含めた赤枠全体を国家安全保障、経済安全保障においては今後構築する必要がある。

構築すべきサイバーインテリジェンスシステ