特集／米国の規制を巡る動向

〈6〉米国の2023会計年度ジェイムス・M.・インハーフ国防授権法におけるサイバーセキュリティ関連の重要規定とその概要

法政大学　人間環境学部　教授　永野　秀雄

Ⅰ　はじめに

2023会計年度ジェイムス・M.・インハーフ国防授権法（James M. Inhofe National Defense Authorization Act for Fiscal Year 2023: 2023 NDAA）は、2022年12月23日にバイデン大統領の署名により成立した。本法に名前が冠せられたジェイムス・M.・インハーフ氏は、オクラホマ州選出の共和党上院議員として1994年から同職にあり、2023年1月に引退されることが決まっていた。

さて、同法は、昨年度より約1割り増しの約8579億ドル（約114兆円）の国防支出を認める巨大な立法となった。また、文書としても4408頁と厚く、サイバーセキュリティについても、歴史上、最も多い規定が置かれている。

本稿では、2023NDAAに規定されたサイバーセキュリティ関連条文のうち、わが国にとって参考になるものや、重要性が高い規定に限って概説する。このため、国防総省の部門・役職等の権限変更や人工知能関連の規定等は、原則として対象としなかった。また、仮訳と書かれていない場合には、各条文のまとめであることをお断りしておきたい。

以下では、まず、2023NDAAの中で、サイバーセキュリティについて中心的に規定する第15編「サイバー及び情報作戦事項」に関して全条文を概説した後、サイバーセキュリティに関するその他の重要規定について説明する。条分数が多いことから、興味のある内容にだけ目を通して頂ければ幸いである。

なお、本年度も、国防授権法の法案に関して党派間の対立点が多く、年末になってようやく本法案が成立した。このため、通常は同法の立法者意思を示すものとして公表される両院協議会報告書（Conference Report）は作成されず、昨年度に引き続き、簡略式の両院合意書を締結するという方法が採用された。したがって本稿において立法者意思について言及する場合には、この簡略式の両院合意書である2023会計年度ジェイムス・M.・インハーフ国防授権法に関する両院合同付帯説明書（Joint Explanatory Statement to Accompany the James M. Inhofe National Defense Authorization Act for Fiscal Year 2023）のことを意味している[1]。

[1] 本稿では、該当箇所で直接引用している文献を除き、以下の英語文献を参照した。なお、本稿では、紙幅の関係から、サイテーションによりネット上で文献を特定できる場合には、URLの表示を省略している。Alexander O. Canizares & Brenna D. Duncan, *The FY 2023 National Defense Authorization Act: Key Provisions Relevant to Defense Contractors*, Perkins Coie LLP (Dec. 29, 2022).

II　2023NDAA 第 15 編「サイバー及び情報作戦事項」

A　はじめに

2023NDAA において、サイバーセキュリティについて多くの規定を置いている第 15 編「サイバー及び情報作戦事項」は、第 A 章「サイバー関連事項（Cyber Matters）」（第 1501 条から第 1514 条）、第 B 章「情報作戦（Information Operations）」（第 1521 条から第 1526 条）、第 C 章「人事（Personnel）」（第 1531 条から第 1541 条）、及び、第 D 章「報告及びその他の関連事項（Reports and Other Matters）」（第 1551 条から第 1560 条）から構成されている。見て頂いて分かるように、これらの条文番号は、日本の法律のように連番にはなっていないものの、全体としてはかなりの条文数になる。

以下では、この章立ての順序に従って、各条文を概説していく。

B　第 A 章「サイバー関連事項」

1　第 1501 条「主席サイバーアドバイザーの向上」

第 15 編「サイバー及び情報作戦事項」第 A 章「サイバー関連事項（Cyber Matters）」の最初の条文は、第 1501 条「主席サイバーアドバイザーの向上（Improvements to Principal Cyber Advisors）」であり、２つの事項について規定している。

まず、その最初のものが、2014 会計年度国防授権法第 932 条「連邦サイバー軍の権限、機能及び監督（Authorities, capabilities, and oversight of the United States Cyber Command）第 (c) 項「主席サイバーアドバイザーの向上」を改正する条項であり、その内容は、予算関係とその手続、議会への報告等となっている。また、第２の内容が、国防長官の主席サイバーアドバイザー、同副サイバーアドバイザー及び各軍長官の主席サイバーアドバイザーに関して、関連する合衆国法典や国防授権法の規定の細部を改正する内容となっている。ここでは、いずれの規定についても、説明を省略する。

2　第 1502 条「各軍による連邦サイバー軍への支援についての年次報告書

第 1502 条「各軍による連邦サイバー軍への支援についての年次報告書（Annual reports on support by military departments for United States Cyber Command）」は、合衆国法典第 10 編第 19 章第 391 条「運用において重要な請負人及びその他の一定の請負人のネットワーク及び情報システムに関するサイバーインシデントに関する報告（Reporting on cyber incidents with respect to networks and information systems of operationally critical contractors and certain other contractors）」の後に、新たに第 391a 条「各軍による連邦サイバー軍への支援についての年次報告書（Annual reports on support by military departments for United States Cyber Command）」を追加することを規定した条文である。

この条文からは、連邦サイバー軍の編成、配員、訓練等が容易でないことが分かる。

（仮訳）
第 391a 条「各軍による連邦サイバー軍への支援についての年次報告書」
第 (a) 項「報告書」
連邦サイバー軍司令官は、国防長官が当該会計年度の国防予算関連資料を連邦議会に提出してから 15 日が経過する前に、連邦議会上下両院の軍事委員会に対して以下の内容を含んだ報告書を提出しなければならない。
第 (1) 号　国防総省の各軍の省（military department）が、連邦サイバー軍司令官により策定され、国防長官室によって承認された要件を遵守し、2023 会計年度国防授権法第 1534 条（「サイバー任務部隊における即応態勢の未達に関する是正」）に基づく計画を効果的に実施し、かつ、同法の第 1533 条（「サイバースペース作戦部隊の総戦力の生成」）の定める要件を遵守しているのか否かに関する評価。
第 (2) 号　上記第 (1) 号において評価された各軍の省につき、(A) 同省が、上記の要件を満たしているとする認証、又は、(B) 同省が、上記の要件をどのように満たしていないかに関する詳細な説明。
第 (b) 項「評価要素」
本条第 (a) 項第 (1) 号における個別評価において、

評価対象となる各軍の省については、以下の各号の内容が含まれていなければならない。

第 (1) 号 サイバー任務部隊（Cyber Mission Force）内における人員配置、訓練及び装備要員の採用に関する指針、手続及び執行。

第 (2) 号 サイバー任務部隊又はサイバースペース作戦部隊（cyberspace operations forces）内の部隊（unit）のいずれかに配属される者に対する訓練カリキュラムの十分性及び安定性、並びに、それが当該軍の省における訓練基準に適合しているのか否か。

第 (3) 号 陸軍、海軍、空軍、海兵隊又は宇宙軍の構成員をサイバー任務部隊に配員する際の任務及び任期に関する指針及び手続が適正なものであるか否か。

第 (4) 号 当該軍の省が、サイバー任務部隊内の重要な職務を有効に満たしているのか否か。これには、文民、軍人及び請負人から出向した個人がうまく組み合わされているのか、及び、連邦サイバー軍司令官が策定し、国防長官室によって承認された要件を満たすのに必要な手法が取られているのか否かという点も含まれる。

第 (5) 号 サイバーに特有な科学技術の向上に関する投資の適切性（特に、サイバー任務部隊の能力開発に関するもの）。

第 (6) 号 サイバー作戦に責任を有する要員に関する軍における職務上の専門分野、指名者、評定又は空軍専門性分類（Air Force specialty code）ついての指針、手続及び投資が十分なものであるか否か。なお、これには、重要な職務に対して熟達した専門要員を必要とされる人数を揃えて勤続させるための諸指針が有機的に機能しているのかの評価も含まれ、その要素としては、勤続年数、ボーナスや特別手当、通常とは異なる俸給メカニズム、及び、本人が希望する職務に継続して勤務することを認めることが含まれる。

第 (7) 号 サイバースペース活動に関して国防総省と共通して利用すべき用語集に関して、国防長官の主席サイバーアドバイザーと連携して、当該軍の省による同用語集の利用に関する評価を行うこと。

第 (8) 号 サイバー任務部隊及びサイバー作戦部隊に従事している要員が、割り当てられた使命を完遂するための準備ができているのか否か。

第 (9) 号 過去の年度における評価結果に対応して当該軍の省により当該評価期間の間に取られた措置が、適切であったか否か。

第 (10) 号 連邦サイバー軍司令官が関係があると決定したその他の事項。

第 (c) 項「最初の報告書」

連邦サイバー軍司令官は、2024 会計年度の国防予算関連資料が連邦議会に提出された日からできる限り速やかに、連邦議会上下院の軍事委員会に対して、合衆国法典第 10 編第 391a 条に基づいて最初の報告書を提出しなければならない。

３　第 1503 条「戦略的サイバープログラムに関して主たる責任を負う部局の変更

第 1503 条「戦略的サイバープログラムに関して主たる責任を負う部局の変更（Modification of office of primary responsibility for strategic cybersecurity program）」は、2018 会計年度国防授権法第 1640 条「戦略的サイバーセキュリティプログラム」第 (c) 項「責任」第 (2) 号「システム及びインフラの審査」を改定し、同号を「主たる責任を負う部局」と変更して、国防長官官房に責任者の室を設けるとともに、その業務・権限について記述したものである。本条は、組織変更に関する内容であることから、これ以上の記述は省略する。

なお、この戦略的サイバープログラム（2018 会計年度国防授権法第 1640 条第 (c) 項第 (1) 号に規定されている）とは、国防長官が国家情報長官と協議して策定するプログラムであり、その担当者は、連邦政府の①攻撃サイバーシステム（Offensive cyber systems）、②長距離打撃システム（Long-range strike systems）、③核抑止システム（Nuclear deterrent systems）、及び、④国防総省重要インフラ（Critical infrastructure of the Department of Defense）に関するサイバーセキュリティを向上させる責任を負うとともに、これらの既存のシステムとインフラ及びこれらの新規調達計画の審査についての責任を負っている。

４　第 1504 条「目的適合的なサイバースペース作戦機関」

第 1504 条「目的適合的なサイバースペース作戦機