ブリーフィング・メモ

イスラエルにおける重要インフラのサイバー防衛組織と課題

政策研究部軍事戦略研究室
島津　貴治

はじめに

英国際戦略研究所(IISS)が 2021 年6月に発表した各国のサイバー能力に関する報告書(Cyber Capabilities and National Power：A Net Assessment）において、イスラエルは３段階に区分される各国の評価の中で、第 1 グループの米国に次いで、第 2 のグループに位置付けられた。イスラエルの他には、ファイブアイズの一翼を担う英国、カナダ、オーストラリアや、中国、ロシア、フランスが第２のグループと位置付けられている。イスラエルは同報告書の中で、イスラエル国家サイバー総局（INCD）の主導のもと政府機関、民間企業、学術機関、国際的なパートナーとの緊密な協力関係により、活力あるサイバーエコシステムを構築するとともに、比較的高いレベルの準備態勢と復元力をその民間セクターの中に築き上げてきたと高く評価されている[1]。

他方で、イスラエルが、今日の重要インフラ防護（CIP）を含むシビリアンのサイバー防衛態勢を整えるまでの、サイバー防衛を担う機関の変遷は多くの意見対立を反映して決して順当なものではなかった。また、現時点においてもイスラエルのサイバー安全保障政策上、法的側面、プライバシーの確保等の点から解決されるべき課題があると指摘されている。

このような状況に鑑み、本記述において、イスラエルのサイバー防衛機関の変遷にかかわる議論について時系列的にみたうえで、イスラエルのサイバー安全保障政策上の課題について述べたい。

1　イスラエルのサイバー防衛の対象としての重要インフラとは

サイバー防衛の対象となる重要インフラ（Critical Infrastructure）とは、INCD の定義によれば、「公共組織におけるセキュリティ規制法」（以下「規制法」）に記載される重要なアセットとされており[2]、この規制法では、通信、電気、水道、エネルギー、金融、交通等にかかわる重要なコンピュータシステムと、そこで扱われる情報、機密情報が保護の対象として挙げられていることから[3]、同法で、国による規制の対象とされている公共組織とその組織が管理する重要コンピュータシステム等が一般に、「重要インフラ」として認識されていると思われる。

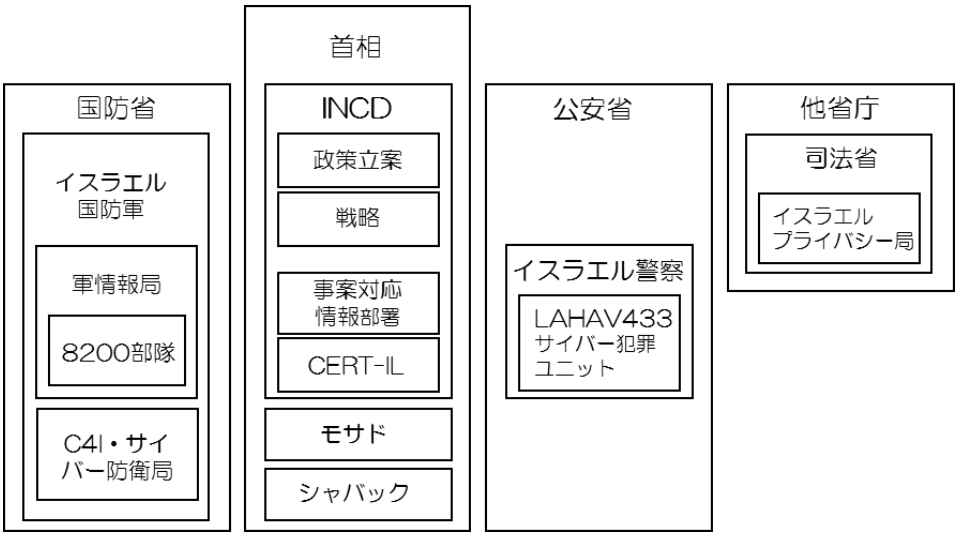
---

[1] “Cyber Capabilities and National Power：Net Assessment”, IISS, June28, 2021, p.69, https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power.
[2] Israel National Cyber Directorate, “Cyber glossary for professionals,” INCD HP, https://www.gov.il/he/departments/general/terms.
[3] “Law for Regulating Security in Public Bodies, 5758-1998,” NEVO, https://www.nevo.co.il/law_html/law01/111m1_001.htm.

2　イスラエルのサイバー防衛組織

イスラエルのサイバー防衛組織等の概要を下図に示す。

イスラエルのサイバー防衛組織等の概要



（出所）Israel's National Cybersecurity and Cyberdefense Posture Policy and Organizations, Center for Security Studies (CSS), ETH Zürich, p.14 より執筆者作成。

現在、イスラエルのシビリアンのサイバー防衛を主に担っているのは、首相直轄の INCD と国内治安機関のシャバック（Shabak：英語名 Israel Security Agency）である[4]。以下、それぞれについて説明する。

（1）INCD

INCD は、シャバック、モサド等と並ぶ首相府の組織であり、首相の指揮監督の下、イスラエルのサイバー防衛面で重要な役割を果たしている[5]。INCD が今日の位置付けになった背景は次章に譲るが、その主だった任務は、シビリアンの分野におけるサイバー防衛の全ての側面を責任範囲とし、政策の策定や技術力の構築からサイバー空間における実際の防衛活動までもカバーする[6]。

また、INCD の活動を支える実行組織としてイスラエルサイバー緊急事態対応チーム（CERT-IL）を運営しており、CERT-IL は、イスラエル国家全土に亘る、INCD と官民の公共組織体との間の 24 時間体制の通報メカニズムを維持する責任を有している[7]。

このような INCD が所掌する公共組織体は、規制法附則第５の中で規定されており、イスラエル

---

[4] その他のサイバー防衛機関として、国防省・イスラエル国防軍情報局 8200 部隊や C4I・サイバー防衛局、イスラエル警察の LAHAV433 サイバー犯罪ユニットがある。Jasper Frei, "Cyberdefense Report Israel's National Cybersecurity and Cyberdefense Posture Policy and Organizations," Center for Security Studies, ETH Zurich, September,2020, p.15, https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf.

[5] Ibid., p.7.

[6] IISS, "Cyber Capabilities and National Power" p.73.

[7] Israel National Cyber Directorate, "The Israeli Cyber Emergency Response Team （CERT)," INCD HP, June5,2019, https://www.gov.il/en/departments/news/119en.

銀行、イスラエル天然ガスルート会社、石油・エネルギーインフラ会社、水道会社、イスラエル電力公社、イスラエル郵便会社、ベングリオン空港、イスラエル鉄道会社、イスラエル放送会社、財務省、鉄道・交通・安全省、航空局等がその対象となっている[8]。

（2）シャバック

シャバックは、イスラエルの国内治安機関であり、対テロ活動を担っているが、INCD と並んで首相直属の機関としてサイバー防衛の任にあたっている[9]。

シャバックは、重要な通信インフラに対する責任をもってサイバー防衛にかかわっており、シャバックによる規制対象組織として、上記規制法の附則第 4 に、イスラエルの主要通信事業者であるベゼック社（固定回線、移動通信、ISP 等を運営）、地中海ノーチラス・イスラエル社（海底ケーブルを運営）、ペレフォン・コミュニケーション社（携帯電話事業を運営）、ホット・テレコミュニケーション・システム社（ケーブルテレビ、ブロードバンド通信事業を運営）等の事業者があげられている[10]。

3　サイバー防衛機関の変遷にかかわる議論

（1）強権的な国家情報セキュリティ局の活動と中小規模事業等へのサイバー脅威増大

コンピュータ社会の発展に伴い生じてきた脅威に対し、既存の国家組織による対策に不満を覚えたイスラエル政府は、国家安全保障評議会（NSC）に対し、これらの脅威に対処するための戦略を策定するよう命じ、2002 年 12 月 11 日、政府特別決議 B/84 号「イスラエルにおけるコンピュータシステム防護の責任」が決定された[11]。この決議の中で、シビリアンのコンピュータインフラを防護する政府組織の創設が義務付けられ、その結果利害関係機関の代表による運営委員会と国家情報セキュリティ局（National Information Security Authority（ヘブライ語名：Re′em））が創設されシャバックの内部に置かれた[12]。

Re′em は、当時、「重要（Critical）」と定義された組織体における IT セキュリティを監視し、指示を与え、その実行を監督し、Re′em によって義務化された指示に違反する者に対する制裁を課す権限まで与えられていた[13]。また、指示の確実な順守と、新たなリスク因子の評価のために、関連する組織体の保有するいかなる情報や資産に対してもアクセスすることが許容された[14]。他方で、21 世紀の初めの 10 年間は、Re′em によって重要と判断されないような、中小規模事業、NGO、一般国民といった人口の大半は、サイバー・セキュリティのない状況に置かれることとなり、技術の進歩と脅威の拡大の中、何等の手当てもされない状況が続いた[15]。

---

[8] “Law for Regulating Security in Public Bodies, 5758-1998.”.

[9] Shabak（又は、Shin Bet）は、Shirut HaBitahon HaKlali（General Security Service のヘブライ語訳）の略称である。Shabak HP, https://www.shabak.gov.il/english/pages/about.html#=1.

[10] “Law for Regulating Security in Public Bodies, 5758-1998.”

[11] Lior Tabanski & Isaac Ben Israel, *Cybersecurity in Israel*, Springer, 2015, p.35.

[12] Ibid.

[13] Ibid.

[14] Tabanski & Ben Israel, *Cybersecurity in Israel*, p.38.

[15] Ibid .; Lior Tabanski, “Critical Infrastructure Protection against Cyber Threats.”

（2）初のシビリアンのサイバー防衛機関 INCB の設立とシャバックとの対立

2010 年、当時のベンヤミン・ネタニヤフ（Binyamin Netanyahu）イスラエル首相は、イスラエル科学省の研究開発国家評議会議長であった、イサク・ベンーイスラエル（Isaac Ben-Israel）退役将軍に現状の政策の見直しを命じ、同年、「国家サイバー構想」が提出された[16]。これを受け、2011 年８月７日、政府決議第 3611 号「サイバー空間における国家の能力の推進」が決定された[17]。

政府決議第 3611 号の主要な内容は、イスラエルにおける公共または民間の利害関係者にかかわるサイバー分野の活動を率いて、政策面での調整を図る専門の政府機関の設立であり、具体的には、イスラエル国家サイバー局（Israel National Cyber Bureau：INCB）を創設することであった[18]。INCB の主な任務は、首相、政府、政府委員会に対しサイバー分野における政策を推奨し、包括的な国家サイバー戦略を起草することとされた[19]。しかし、他の利害関係機関との間の意見の不一致が解消されなかったため CIP 活動における変革を推進するまでには至らなかった[20]。

（3）Re′em からの CIP 任務の移管とシビリアンのサイバー防衛機関 INCD の創設

ネタニヤフ首相は、2010 年の国家サイバー構想を策定させた、ベンーイスラエル退役将軍に、サイバー・セキュリティ政策を巡る手詰まり状態を解決するためのロードマップを作成するよう命じた[21]。結果として、ベンーイスラエル退役将軍がネタニヤフ首相に提出した提言が政策変更の基礎となり[22]、2015 年２月 15 日、政府決議第 2443 号「サイバー防衛にける国家の規制と政府のリーダーシップの促進」が決定され[23]、その中でシビリアン側におけるサイバー・セキュリティを進展させるための新たな機関の創設が決定された[24]。

その新たな機関は、「国家サイバー・セキュリティ局（National Cyber Security Authority：NCSA）」とされ、サイバー防衛力整備とその維持を担う INCB と並んで、首相府に置かれ、運用をつかさどる機関とされた[25]。同様に、2015 年２月 15 日の政府決議第 2444 号「サイバー防

Military and Strategic Affaires Volume 3, No. 2, INSS, November,2011, pp.72-73, https://www.inss.org.il/wp-content/uploads/2017/01/Military-Strategy-volume-3-no.2.pdf

[16]この構想で、2015 年までにイスラエルを世界のトップ５の一つとしての地位を固めるべくサイバー技術開発の動機付けをいかに行うか、サイバー技術開発にあたってどのインフラが必要とされるか、そしてサイバー空間の危険や脅威に最も適切に対処するにはいかなるアレンジメントが必要か、について提議された。Tabanski & Ben Israel, *Cybersecurity in Israel*, p.43.

[17] Lior Tabanski, "Israel Defense Forces and National Cyber Defense," The Quarterly Journal, Volume 19, Issue 1, Jan19,2019, p.49, https://isij.eu/article/israel-defense-forces-and-national-cyber-defense.

[18] Ibid.; Prime Minister's Office, "Government Resolution 3611, Promoting National Capacity in Cyberspace," Prime Minister's Office , July8,2011, https://www.gov.il/he/departments/policies/2011_des3611.

[19] Tabanski & Ben Israel, *Cybersecurity in Israel*, p.52.

[20] Ibid., p.57.

[21] Ibid.

[22] Ibid.

[23] Prime Minister's Office, "Government Resolution2443, Promoting National Regulation and Government Leadership in Cyber Defense," Prime Minister's Office, February 15, 2015, https://www.gov.il/he/Departments/policies/2015_des2443.

[24] Tabanski & Ben Israel, "Cybersecurity in Israel," p.58.

[25] Ibid.

衛のための国家の準備態勢の促進」[26]によって NCSA は、CIP 任務をこれまで遂行してきたシャバックの隷下組織である Re'em を吸収することとなり、同任務はシャバックから NCSA に移管されることとなった[27]。翌 2016 年に重要なコンピュータシステムを所管する責任の移管が完了し、先に述べた規制法に従い、通信事業者に関する責任はシャバックに残されることとなり、同法によって、NCSA が、同法附則第 5 に規定されるその他のコンピュータシステムと組織体を管轄することとされた[28]。

また、これらの決議により NCSA 内に CERT-IL が設立され、サイバー・セキュリティ・インシデント管理やそれへの対処の中心的拠点として、サイバー脅威に対する国家の復元力の強化に努めることとなった[29]。同時に、上記の政府決議第 2444 号において、イスラエル国家サイバー総局（Israel National Cyber Directorate：INCD）の創設も決定されていた[30]。

（4）国家サイバー・セキュリティ戦略の策定とシビリアンのサイバー防衛態勢の確立

2017 年 12 月 17 日の政府決議第 3270 号[31]で、INCB と NCSA は、INCD に統合されることとなり、政策の策定、技術力の構築、サイバー防衛活動に至るまで、INCD がシビリアンの分野におけるすべてのサイバーの局面の責任を負うこととなった[32]。2018 年 12 月 27 日、イスラエル国会であるクネセットが、規制法の修正法を可決し、上記の INCB と NCSA の INCD への統合について、法的な根拠を与えることとなった[33]。

なお、2017 年 9 月にはイスラエルは、同国として初の「国家サイバー・セキュリティ戦略（Israel National Cyber Security Strategy in brief）[34]」（以下「サイバー戦略」）を公表しており、INCD[35]の果たすべき役割や運用概念、能力構築の考え方等について明らかにされており、現状では、INCD は、政策やガイダンスの発出等を行っている[36]。

---

[26] Prime Minister's Office, "Government Resolution2444, Promoting National Preparedness for Cyber Defense," Prime Minister's Office, February 15, 2015, https://www.gov.il/he/Departments/policies/2015_des2444.
[27] Tabanski, "Israel Defense Forces," p.52.
[28] Israel National Cyber Directorate, "Government decisions and the law regulating security in public bodies," INCD HP, July16,2018, https://www.gov.il/he/Departments/news/govdecisions.
[29] Tabanski & Ben Israel, "Cybersecurity in Israel," p.58.
[30] Tabanski, "Israel Defense Forces," p.53.
[31] Prime Minister's Office, "Government Resolution3270. 1. Consolidation of units of the national cyber system 2. Granting an exemption from a tender for the position of head of the national cyber system 3. Addition of the position of head of the national cyber system to the addendum under section 23 of the Civil Service Law (Appointments) 4. Determination of salary and terms of service," Prime Minister's Office, December17,2017, https://www.gov.il/he/departments/policies/dec_3270_2017.
[32] Tabanski, "Israel Defense Forces," p.53.
[33] Global Legal Monitor, "Israel: Knesset Passes Amendment Law Recognizing Role of National Cyber Directorate in Protecting Cyberspace", Library of Congress, July 22, 2019, https://www.loc.gov/item/global-legal-monitor/2019-07-22/israel-knesset-passes-amendment-law-recognizing-role-of-national-cyber-directorate-in-protecting-cyberspace/.
[34] Israel National Cyber Directorate," Israel National Cyber Security Strategy in brief," Prime Minister's Office, September, 2017, https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.
[35] 公表当時はまだ INCD に統合されておらず、サイバー戦略文書上は NCSA の役割とされている。
[36] Israel National Cyber Directorate, "Israel National Cyber Directorate," ttps://www.gov.il/en/departments/israel_national_cyber_directorate/govil-landing-page.

4　イスラエルのサイバー安全保障政策上の課題

（1）INCD みずからの活動の根拠となる法律の未整備

これまで見てきたとおり、政府決議 B/84 号、第 3611 号、第 2443 号、第 2444 号、第 3270 号でイスラエルにおけるシビリアンのサイバー・セキュリティに関する体制及び態勢については形作られ、2017 年にはサイバー戦略も策定され、運用コンセプトも明らかにされてきた。この間、INCD が政策や推奨を発出し、民間企業に対する指導的役割を果たしつつ、CERT－IL を運用し日々のインシデントへの対応を行ってきた。

しかしながら、シビリアンのサイバー・セキュリティの実行機関としての INCD は、その職責を果たすための法的根拠となる「サイバー防衛法（仮称）」が未整備であるため（2021 年 12 月 17 日現在）、INCD の任務、機能、権限について法律で規定されていない状況である[37]。そして、サイバー・セキュリティ活動の実施にあたり、法執行機関のような強制力や調査権限も有していないとされる[38]。INCD のイガル・ウンナ（Yigal Unna）長官は、2018 年法案の提出に先立ち、同法案について、「それは今日、自分たちが行っていることを正式化するものであり、イスラエルの民間と政府機関が、サイバー・セキュリティのために何を行っているべきか、についての枠組みを構築するものである。」と述べている[39]。この発言からも、INCD が法的な根拠のないまま実態として「推奨」、「ポリシー策定」等を実施している状況がうかがえる。

（2）INCD の権限強化のためのサイバー防衛法（仮）立法化への動きとそれへの懸念

現実のサイバー脅威の高まりを受け、サイバー防衛に関する法律を整備する必要があるとして、2018 年以降、立法化の動きが進められてきたが[40]、国内での強い反対にあい立法化には至らなかった[41]。2018 年法案に関する主な反対の理由は、①INCD の権限の広さ（裁判所命令なしに私有地への立ち入り、物件押収可）、②プライバシー保護の不十分さ、③INCD の活動に対する監視メカニズムの貧弱さ等が指摘されていたほか、④シャバックなどの法執行機関、情報機関、軍等の権限との干渉等があったとされる[42]。

コロナ禍でのテレワークの拡大や、デジタル化の進展に伴うサイバー・セキュリティ上のリスク

---

37 Global Legal Monitor, “Israel: Knesset Passes Amendment Law.”

38 Tabanski, “Israel Defense Forces,” p.52、NCSA には、法執行活動を行う権限は与えられなかったのは、2015 年当時、2013 年のエドワード・スノーデンによる米国の NSA 等の活動等に関する暴露の余波を受けて慎重に熟慮した結果であったとみられている。

39 Shoshanna Solomon, “Winter is still coming,’ cyber chief warns on hacking threats,” Times of Israel, June20, 2018, https://www.timesofisrael.com/winter-is-still-coming-cyber-chief-warns-on-hacking-threats/.

40 Global Legal Monitor, “Knesset Passes Amendment Law.”

41 Deborah Housen-Couriel, Tal Mimran, Yuval Shany, “Israel’s Version of Moving Fast and Breaking Things: The New Cybersecurity Bill,” LAWFARE, May 7, 2021, https://www.lawfareblog.com/israels-version-moving-fast-and-breaking-things-new-cybersecurity-bill.

42 Amir Cahane, “The New Israeli Cyber Draft Bill – A Preliminary Overview,” The Federmann Cyber Security Research Center, 2018, https://csrcl.huji.ac.il/new-israel-cyber-law-draft-bill；実際、法案が公表される 1 年前に、サイバー・セキュリティの強化に関するネタニヤフ首相の構想に関し、軍等が反対したことがメディアにリークされた事案があった Jacob Magid, “Security chiefs slam Netanyahu over planned cyber defense body,” Times of Israel, April24,2017, https://www.timesofisrael.com/security-chiefs-slam-netanyahu-over-planned-cyber-defense-body/.

の高まり、そして、イスラエル企業に対する度重なるサイバー攻撃を踏まえ、速やかにこれらに対処するために、2021 年２月、ネタニヤフ首相は、「サイバー・セキュリティ及び国家サイバー総局」という新法案を公表した[43]。新法案の内容は、2018 年法案の省略版と見られ、時限立法として起案されている[44]。

新法案は、専門的な見地からサイバー・セキュリティ・ガイダンスを政府機関等公共機関と民間機関に対し提供するにあたっての、INCD の機能と権限を法で定めることをねらいとしているが、2018 年の法案でもそうであったように、民間のコンピュータネットワークにおけるサイバー防衛活動にあたって、例外のない侵入権限（Intrusive powers）を INCD に認めることについて、深刻な疑念が指摘されている。たとえば、民間企業が協力しない場合には、企業の同意を要せずして、企業のサーバーにアクセスすることを INCD に許すための裁判所命令を、INCD が求めることができるようになっておりまた、収集したデータの、政府機関同士の共有も許容されていて、それによるデータの保護や漏洩、プライバシーの確保、知的財産権の保護に関する懸念も生じている[45]。

おわりに

イスラエルは、サイバー分野において世界でも有数のハイテク国家として、サイバー・セキュリティをリードする実力を有するがゆえに、冒頭で述べた IISS のサイバー能力に関する報告書で第２グループに属することが可能となっているのであろう。

イスラエルのサイバー空間における安全保障上の国益を防護するために、INCD に対して新しい法的なツールを速やかに提供することは、イスラエルとイランとの高まる緊張関係のゆえ、サイバー攻撃のリスクが高まっている現在のタイミングで、より一層急を要するものとなっている[46]。しかし、シビリアンのサイバー・セキュリティに関し、いまだサイバー防衛法（仮称）が未制定で、その着地点を見いだせていない状況にある。

重要インフラ防護を含めサイバー防衛に関しては、世界では国家の関与を強める趨勢にあると思料するが、治安維持、国益保護の名のもとに個人や民間企業の活動への関与と行き過ぎた監視が、民間の自発的な取り組みを阻害し、新技術の開発の動機を損なう恐れがあることも懸念される。それゆえにこのようなサイバー防衛機関の運営にあたっては、個人や民間企業への配慮と、サイバー防衛機関の活動が適正に行われていることを確保する体制も併せて整備していく必要があろう。

[43] Deborah Housen-Couriel, “Israel’s Version of Moving Fast and Breaking Thing.”
[44] Ibid.
[45] Ibid.
[46] Ibid.