www.eai.or.kr

ADRN 이슈브리핑

일본의 디지털 영향 공작 대응 현황

이치다 카즈키 (Kazuki Ichida) (메이지대학)

EAI
동아시아연구원

ADRN 이슈브리핑

일본의 디지털 영향 공작 대응 현황

이치다 카즈키 (Kazuki Ichida)
메이지대학 사이버시큐리티연구소 객원연구원

서론

디지털 영향 공작(Digital influence operation)은 특정 국가의 대중 인식과 여론을 형성하거나 약화시키는 능력을 지니고 있다. 미국 국가정보위원회는 중국, 러시아, 이란의 경우 디지털 영향이 가져오는 인지적 효능성 때문에 이들이 사이버 공격보다 디지털 영향 공작을 더욱 우선시하고 있다고 분석한다(National Intelligence Council 2023). "디지털 영향 공작"은 인지전(cognitive warfare) 및 정보전(information warfare) 등의 용어로 다양하게 일컬어진다. 본 브리핑에서는 "디지털 영향 공작"이라는 용어를 통칭하여 사용하도록 한다.

이 글은 일본의 주요 행위자가 구사하는 대응 전략 현황을 설명한다. 일본에서는 방위성, 총무성, 외무성, 국가공안위원회, 내각 사이버시큐리티센터 등의 기관이 대응 조직을 구축하고 있다. 반면 팩트 체크 기관, 싱크탱크, 학계 등 민간 차원의 노력은 인적 자원 및 규모의 부족 등 한계에 직면해 있었다. 최근 몇 년간은 일본 정부의 지원으로 민간 차원에서의 대응 전략이 확장되는 움직임이 보인다.

일본의 디지털 영향 공작 대응은 세 가지 도전에 직면해 있다. 첫째, 지식과 인적 자원이 심각하게 부족하다. 둘째, 대응 전략은 주로 허위 정보(disinformation) 대응이나 전략적 커뮤니케이션 강화 등 일부에 국한되어 있다. 마지막으로 작전 대상 국가의 정치적 양극화를 초래할 수 있는 사이버상의 공격에 대한 문제를 해결하지 못하고 있다. 이러한 도전은 일본뿐만 아니라 유럽과 미국에서도 일반적으로 나타난다.

디지털 영향 공작 대응의 주요 행위자

유럽연합 대외관계청(European External Action Service: EEAS)은 최근 발간한 “제2차 EEAS 해외 정보 조작 및 간섭 위협 보고서”에서 정부 및 산하 기관, 사기업, 팩트체크 기구, 싱크탱크, 대학 등 디지털 영향 공작에 대응하는 주요 행위자를 적시했다(EEAS 2024). 일본의 경우, 정부 및 산하 기관의 역할이 중심적이며 다른 행위자는 상대적으로 덜 적극적인 역할을 수행한다.

1. 정부 및 산하 기관

일본의 방위성, 자위대 및 안보 관련 기관은 디지털 영향 공작에 따른 외부 위협에 대응하는 역할을 수행한다. 또한 총무성은 일본 국내의 위협 대응, 외무성은 외교적 차원의 전략적 커뮤니케이션을 각각 전담하며, 내각 사이버시큐리티센터가 전체 대응을 총괄 조정한다. 이러한 책임 배분은 2022년 발표된 국가안보전략에 규정되었으며, 각 기관이 이에 따른 세부 대응 방침을 수립하고 있다(Cabinet Secretariat 2022). 또한 형사 사건은 국가공안위원회가, 기밀 관련 사안은 내각관방, 방위성 정보본부 등이 분담하는 체계를 갖추고 있다.

국가 안보 기구: 국가안보전략은 방위성이 디지털 영향 공작에 대응하도록 명시하고 있다. 방위성 내에서는 정보 본부가 대응 업무를 전담한다(DIH n.d.). 정보본부는 직원 2,600명 이상이 속한 일본 최대의 정보 기관이다(MOD n.d.). 대중에 공개된 자료에 따르면 정보본부는 전략 커뮤니케이션을 포함한 선전 및 허위 정보 대책에 중점을 두고 있으며, 급증하는 정보의 진실성을 판단하기 위한 인공지능 시스템 개발을 계획하고 있다(MOD n.d.).

한편 자위대에서는 육상자위대 교육훈련연구본부(Training-Evaluation Education Research and Development Command: TERCOM)가 새로운 사이버전 체계를 개발하는 전담 조직을 운용하고 있으나, 그 외의 특기할 만한 대응은 많지 않다(TERCOM 2023). 미국의 사이버사령부와 달리 공작의 원점을 공격하는 선제적 대응은 논의되지 않는 것으로 보이며, 선전과 허위 정보에 대한 일본의 대응은 주로 정보의 확산 이후에 이루어진다.

총무성은 2018년부터 디지털 영향 공작 대응에 관여하여, 관련 학계 전문가와 플랫폼 기업이 참여하는 연구 그룹을 결성했다(MIC 2018). 현재 고도 정보 시스템 및 소프트웨어 분과가 허위정보 대응을 중심으로 한 이행 노력을 주도하고 있다. 다만 부처 간 권한 분담으로 인해 국가 안보 차원의 고려는 이루어지지 않고 있으며, 팩트체크와 정보 문해력 향상을 목표로 추진하고 있다.

외무성은 전략 커뮤니케이션의 차원에서 디지털 영향 공작 문제에 접근하며, 일본에 관한 잘못된 정보를 바로잡고 정확하고 긍정적인 이미지를 대외에 확산하는 것을 목적으로 한다. 이는 일본 정부의 평판 관리 기능을 수행하는 것이라 할 수 있는데, 그중 일부는 이스라엘의 평판 관리 기업에 위탁하고 있다(Intelligence Online 2023).

내각관방은 내각정보회의, 내각정보조사실, 내각 사이버시큐리티센터 등의 대응 부처를 거느리고 있다. 사이버시큐리티센터는 디지털 영향 공작 대응을 포함한 일본 정부의 전반적 대응 전략을 감독하는 역할을 수행하게 된다(Cabinet Secretariat 2022). 일본에서는 사이버 공격과 디지털 영향 공작이 각각 별개로 취급되었으나, 실제로는 양자가 상호 연계되고 대응 조직도 동일한 경우가 많다. 따라서 사이버시큐리티센터를 중심으로 한 대응 체계를 조직하려는 것이다.

그 밖에도 형사 사건을 다루는 경찰청 및 정보 사건을 다루는 공공안보 및 대외 부서들이 대응에 관여하고 있다.

상기한 바와 같이, 일본 정부의 대책은 주로 허위 정보를 탐지하여 대응하는 데 초점을 두고 있다. 그러나 디지털 영향 공작은 허위 정보 외에 감정적 조작, 타국에서 생산되는 내러티브, 인식 체계 교란 등 더 넓은 범위를 포괄한다(Myre 2020; Meta 2023). 다양한 행위자가 참여하는 종합적 대응을 전개하는 미국 등과 비교했을 때, 일본 정부의 대응은 더 좁은 범위에 특화되어 있다. 이는 지식과 인적 자원의 부족에 따른 결과라 할 수 있다. 정부 기관은 2023년부터 관련 지식을 보유한 민간 기업의 참여를 촉진하고 있다. 그러나 민간 부문도 마찬가지로 전문성과 자원의 부족을 겪고 있다. 정부가 허위 정보 대응 등을 민간 단체에 위임하고자 한다면, 이들 단체에 대한 감독 및 평가 체계가 확립되어야 할 것이다.

2. 민간 부문

유럽과 미국의 많은 사이버 보안, IT, 군사 관련 기업들은 디지털 영향 공작을 담당하는 부서를 두고 그 활동 보고서를 정기적으로 발간하고 있다. 일본의 경우, 본국의 보고서를 공유하는 외국계 기업을 제외하면 이러한 활동을 하는 사이버 보안 및 IT 기업은 많지 않다.

평판 관리 기업은 디지털 영향 공작과 관련된 민간 단체이지만, 그들의 실제 활동은 대부분 공개되지 않는다. 이들 기업에 업무를 위임하는 정부 기관의 경우도 마찬가지이다. 평판 관리 기업의 일반적인 직무 범위에 따르면, 이들은 허위 정보에 대응하고 전략 커뮤니케이션(strategic communication)을 지원한다고 추정된다. 전략 커뮤니케이션은 동맹을 강화하거나 지향하는 가치를

명확히 하기 위해 정보나 신호를 공개함으로써 국제관계를 형성하는 과정을 수반한다. 일본 정부가 관련 예산을 늘리고 체계를 강화함에 따라, 민간 기업에 대한 수요가 증가하고 사업 분야가 확장될 것으로 예상된다.

일본의 양대 팩트체크 기관은 팩트체크 이니셔티브(http://fij.info) 및 일본팩트체크센터(https://www.factcheckcenter.jp/)이다. 여타 선진국에 비하면 팩트체크 기관의 수와 활동은 적은 편이며, 영향력도 여전히 제한적이다. 막대한 허위 정보가 쉽게 생산되는 환경에서 팩트체크 활동의 확장성은 도전 받고 있으며, 팩트체크 결과는 허위 정보에 비하면 제한적 범위에 확산되는 데 그친다. 이는 세계 각국의 팩트체크 기관이 직면한 도전이기도 하다. 싱크탱크 중에서는 일본국제문제연구소(https://www.jiia.or.jp/)와 사사카와평화재단(https://www.spf.org) 등이 디지털 영향 공작 관련 연구를 수행하고 있지만, 그 수와 범위가 제한적이고 보고서 대부분이 기존 문헌 및 조사 자료를 재구성하는 수준이다.

정치학, 사회학, 미디어 등 다양한 분야의 학계 연구자들은 각 분야와 디지털 영향 공작 간의 연관성을 탐구하고 있다. 이들 중 일부는 일본 정부의 지원을 받기도 한다. "국가안전보장전략 개정을 향한 제언"이나 "건전한 언론 플랫폼을 향하여" 등 다양한 분야의 연구자와 실무 종사자가 참여한 야심찬 연구 프로젝트가 진행되기도 했다(ROLES 2022; Toriumi and Yamamoto 2023). 전자는 국가 안전 보장의 모든 영역을 다루었으며, 디지털 영향 공작 대응의 획기적인 참고 자료가 되었다. 한편 후자는 연구 자금의 원천이 불투명하였고, 여론 조작 가능성에 관한 우려를 일으킨 바 있다.

요컨대 일본의 학문 공동체는 유럽과 미국만큼 광범위한 분야를 다루고 있지는 않다. 다만 가까운 장래에 정부의 재정 지원이 증가한다면, 학계의 활성화를 촉진할 수도 있을 것이다.

일본의 디지털 영향 공작 대응의 문제점

일본의 디지털 영향 공작 대응은 지금까지 부진했다. 총무성이 연구를 적극 진행하기는 하였으나 시민사회, 학계, 팩트체크 기관 및 민간 기업의 관여는 제한적이었다. 2023년 일본 정부는 이 문제를 중요하게 다루기로 하고, 예산 및 조직을 확충하여 민간 기업과 연구 기관의 영향력을 증진하기로 하였다. 비록 지식과 인적 자원의 부족 문제가 여전히 있지만, 일본은 본격적 대응의 출발점에 있다고 할 수 있다.

현재 일본의 대응에는 크게 세 가지 문제점이 있다. 첫째, 지식과 인적 자원의 부족은 가장 중대한 걸림돌이다. 둘째, 대응책이 주로 허위 정보 대처, 정보 문해력 향상, 전략 커뮤니케이션 강

화 등에 국한되어 있다. 최근 카네기 국제평화재단이 발간한 보고서는 다면적인 대응책 마련의 중요성을 강조하며 정책, 미디어, 교육 등을 망라하는 10가지 대응책을 제시한 바 있다(Bateman and Jackson 2024).

끝으로, 유럽이나 미국과 마찬가지로 일본에서도 국내 차원의 위험 요소는 상당 부분 경시되고 있다. 외부에서의 디지털 영향 공작은 대상 국가 내부의 양극화를 악화시키는 경우가 많아, 국내 대응과 국제적 대응 간 상호 연계가 필요하다. 가령 미국의 음모론 집단인 큐어넌(QAnon)의 주장은 종종 러시아나 중국과 동조하기도 한다(Kayali and Scott 2022; Soufan Center 2021; Butler and Martin 2022; Graziosi 2022).

해외에서의 방해에만 대처하는 접근법은 위협의 실체에 접근하지 못한다. 대내적으로 디지털 영향 공작을 전개하는 국가의 수는 타국에 대한 방해를 전개하는 국가보다 많다(Martin et al. 2020; Meta 2022; Bradshaw et al. 2020). 대내적인 공작은 민주주의에 더 심각한 위협을 초래한다. 또한 해외에서의 방해가 대상 국가의 정치적 양극화를 활용하는 경우도 잦다. 즉 대상 국가에 존재하는 정치적 문제를 활용하는 공작을 전개하는 것이다. 디지털 영향 공작 대응이 국내 여건과 외부 개입 간 연계를 고려하지 못한다면, 민주주의를 지키는 효용성은 제한적일 것이다. 미국 국가정보위원회에 따르면 중국, 러시아, 이란은 미국 국내의 양극화를 이용하는 전략을 중점 추진한다(National Intelligence Council 2022). 디지털 영향 공작에 대한 대응은 국내 및 대외 차원에서 함께 이루어져야 한다.

디지털 영향 공작에 대한 국가의 관여는 네 가지 유형으로 나눌 수 있다(Nyst and Monaco 2018; Ichida 2018; Woolley 2023). 현재 유럽, 미국, 일본은 그 중 두 가지 유형에 대처하고 있다. 정부가 공작을 조장하고 지원하는 세 번째와 네 번째 유형은 특히 대응이 어려우며, 대상 국가의 양극화를 활용하는 경우 더욱 그러하다.

유형 1. 정부의 집행(Government Execution): 정부 또는 산하 기관이 직접 공작을 시행한다.

유형 2. 정부의 지원 및 조정(Government Support and Coordination): 정부가 공작 계획을 세우되, 그 시행은 외부 행위자에게 위임한다.

유형 3. 정부의 조장 및 지원(Government Incitement and Support): 정부가 온라인 사용자로 하여금 정부에 비판적인 개인 및 단체를 공격하도록 부추겨 여론을 조작하는 유형으로, 가장 심각한 위험을 초래한다.

유형 4. 정부의 승인 및 지원(Government Approval and Support): 정부가 공작 대상에 대한 비난과 공격을 하기 쉬운 환경을 조성한다.

다만 일본 정부는 마지막 유형에 대응하는 데 잠재적인 강점을 갖고 있다. 현 집권당인 자유민주당은 2009년 민주당에 정권을 내준 이후 온라인 홍보 활동을 전담하는 'T2'라는 조직을 운영했다(Koguchi 2016). T2는 IT 및 홍보 기업의 지원을 받아 기업의 평판 관리와 유사한 활동을 수행했다. 이러한 사실은 일본 정부가 국내에서의 디지털 영향 공작에 관한 정책적 배경을 갖고 있음을 시사한다. 정부의 활동을 대중에게 알리고 논의를 활성화하며, 투명성을 증대하는 노력이 수반된다면 일본 정부는 민주적인 대응 태세를 구축할 수 있을 것이다. ■

참고 문헌

Bateman, Jon, and Dean Jackson. 2024. “Countering Disinformation Effectively: An Evidence-Based Policy Guide.” Carnegie Endowment for International Peace. January 31. https://carnegieendowment.org/2024/01/31/countering-disinformation-effectively-evidence-based-policy-guide-pub-91476 (Accessed February 8, 2024)

Bradshaw, Samantha, Hannah Bailey, and Philip N. Howard. 2021. “Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation.” Oxford University Programme on Democracy & Technology. https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/ (Accessed February 8, 2024)

Butler, Josh, and Sarah Martin. 2022. “Australian online anti-vaccine groups switch to Putin praise and Ukraine conspiracies.” *The Guardian*. March 1. https://www.theguardian.com/australia-news/2022/mar/02/australias-anti-vaccine-groups-switch-focus-to-putin-praise-and-ukraine-conspiracies (Accessed February 8, 2024)

Cabinet Secretariat. 2022. “National Security Strategy of Japan (Provisional Translation)” December 2022. https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf (Accessed February 8, 2024)

Defense Intelligence Headquarters: DIH. n.d. “情報本部の任務・活動.” https://www.mod.go.jp/dih/company.html (Accessed February 8, 2024)

European External Action Service: EEAS. 2024. “2nd EEAS Report on Foreign Information Manipulation and Interference Threats.” January 23. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en (Accessed February 8, 2024)

Graziosi, Graig. 2022. “Anti-vax conspiracy theorists in US turning to antisemitic pro-Putin propaganda, report says.” *The Independent*. March 2. https://www.independent.co.uk/news/world/americas/us-politics/putin-propaganda-usa-conspiracy-theorist-b2027230.html (Accessed February 8, 2024)

Ichida, Kazuki. 2018.『フェイクニュース　新しい戦略的戦争兵器』. Tokyo: Kadokawa Shinsho.

Intelligence Online. 2023. “Japan turns to Israel’s 9500 Group to counter Chinese Fukushima disinformation.” September 12. https://www.intelligenceonline.com/corporate-intelligence/2023/09/12/japan-turns-to-israel-s-9500-group-to-counter-chinese-fukushima-disinformation,110042325-art (Accessed February 8, 2024)

Kayali, Laura, and Mark Scott. 2022. “Anti-vax conspiracy groups lean into pro-Kremlin propaganda in Ukraine.” *POLITICO*. March 17. https://www.politico.eu/article/antivax-conspiracy-lean-pro-kremlin-propaganda-ukraine/ (Accessed February 8, 2024)

Koguchi, Hidehiko. 2016.『情報参謀』. Tokyo: Kodansha.

Martin, Diego A. Jacob N. Shapiro, and Julia G. Ilhardt. 2020. “Online Political Influence Efforts Dataset.” Princeton University Empirical Studies of Conflict Project. Last Updated May 11, 2023. https://esoc.princeton.edu/publications/trends-online-influence-efforts (Accessed February 8, 2024)

Meta. 2022. “Recapping Our 2022 Coordinated Inauthentic Behavior Enforcements, Meta.” December 15. https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/ (Accessed February 8, 2024)

_____. 2023. “THIRD QUARTER Adversarial Threat Report.” November 3. transparency.fb.com/ja-jp/metasecurity/threat-reporting/ (Accessed February 8, 2024)

Ministry of Internal Affairs and Communications: MIC. 2018. “プラットフォームサービスに関する研究会 (Study Group on Platform Services)”. https://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/index.html (Accessed February 8, 2024)

Ministry of Defense: MOD. n.d. “Integrated Information Warfare with Special Regard to the Cognitive Dimension.” https://www.mod.go.jp/en/d_architecture/infowarfare/index.html (Accessed February 8, 2024)

Myre, Greg. 2020. “A ‘Perception Hack’: When Public Reaction Exceeds The Actual Hack.” *NPR*. November 1. https://www.npr.org/2020/11/01/929101685/a-perception-hack-when-public-reaction-exceeds-the-actual-hack (Accessed February 8, 2024)

National Intelligence Council. 2022. “Foreign Threats to the 2022 US Elections” December 23. https://www.odni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf (Accessed February 8, 2024)

Nyst, Carly, and Nicholas Monaco. 2018. “State-Sponsored Trolling.” July 19. Institute for the Future. https://legacy.iftf.org/statesponsoredtrolling/ (Accessed February 8, 2024)

Research Center for Advanced Science and Technology Open Laboratory for Emergence Strategies: ROLES. 2022. “国家安全保障戦略改訂に向けた提言(Recommendations for the Revision of the National Security Strategy).” October 31. https://roles.rcast.u-tokyo.ac.jp/publication/20221031 (Accessed February 8, 2024)

Soufan Center. 2021. “Quantifying The Q Conspiracy: A Data-Driven Approach to Understanding the Threat Posed by QAnon.” April 21. https://thesoufancenter.org/research/quantifying-the-q-conspiracy-a-data-driven-approach-to-understanding-the-threat-posed-by-qanon/ (Accessed February 8, 2024)

TERCOM (陸上自衛隊の新たな戦い方検討チーム). 2023. “陸上自衛隊の新たな戦い方コンセプトについて” October 3. https://www.mod.go.jp/gsdf/tercom/img/file2320.pdf (Accessed February 8, 2024)

Thomas, Elise. 2022. “QAnon goes to China – via Russia”, Institute for Strategic Dialogue. March 23. https://www.isdglobal.org/digital_dispatches/qanon-goes-to-china-via-russia/ (Accessed February 8, 2024)

Toriumi, Fujio, and Tatsuhiko Yamamoto. 2023. “KGRI Working Papers No.1 健全な言論プラットフォームに向けて ver2.0 (Toward a Healthy Platform for Discussion).” May 2023. https://www.kgri.keio.ac.jp/docs/S0120230529.pdf (Accessed February 8, 2024)

Woolley, Samuel. 2023. *Manufacturing Consensus: Understanding Propaganda in the Era of Automation and Anonymity*. New Haven: Yale University Press.

■ 이치다 카즈키(Kazuki Ichida)_메이지대학 사이버시큐리티연구소 객원연구원.

■ 담당 및 편집: 박한수_EAI 연구원

문의: 02-2277-1683 (ext. 204) hspark@eai.or.kr

발행일 2024년 2월 16일
“일본의 디지털 영향 공작 대응 현황” 979-11-6617-712-5 95340

재단법인 동아시아연구원
03028 서울특별시 종로구 사직로7길 1
Tel. 82 2 2277 1683 Fax 82 2 2277 1684

Email eai@eai.or.kr Website www.eai.or.kr