公益財団法人日本国際問題研究所

研究レポート

「大国間競争時代のロシア」研究会 FY2021-1 号　2021 年 6 月 8 日

米露関係における SolarWinds 社サイバーセキュリティ事案

山添博史（防衛研究所主任研究官）

はじめに

2021 年 4 月 13 日、米国のジョー・バイデン大統領はロシアのウラジーミル・プーチン大統領と電話会談し、米露関係の障害となっている複数の事案を話し合った。その 2 日後の 15 日、ホワイト・ハウスはロシアの有害な活動にはコストを与えるとして、経済制裁などの報復措置を発表した。このなかで比較的詳細に述べているのは、2020 年 12 月に発覚した、SolarWinds 社の製品を通じたサイバー攻撃事案であり、この報復措置発表と同日の 2021 年 4 月 15 日には米英両国の情報機関が、ロシア対外諜報庁(SVR)に責任があると初めて公式に指名した[1]。本稿では、この SolarWinds 社製品をめぐる事案をとりあげ、米露関係におけるサイバーセキュリティ問題の一端を論じる。なお、本稿は日本国際問題研究所のロシア研究会報告書中の拙稿(2021 年 2 月執筆)[2]の一部を用い、4 月～5 月の情勢をもって加筆したものである。

SolarWinds 社サイバー攻撃事件の発覚

2020 年 12 月 8 日、セキュリティ企業 FireEye のケヴィン・マンディア(Kevin Mandia)が、不正アクセスを検出し、そこから最高レベルの政府組織能力によるサイバー攻撃が米国の多くの機関に対して行われていると発見して、米国政府やマイクロソフトと協力して調査中と発表した。FireEye 社は 12 月 13 日の続報において、同社が SUNBURST と名づけたマルウェア(ウイルスを含む、不正行為のプログラム)が、SolarWinds 社が提供し幅広く使われているネットワーク管理ソフトウェア Orion Platform の更新ファイルの形をとって全世界の多数のシステムに広がり、バックドア(侵入のための裏口)をつくって慎重に情報窃取を行っていたと指摘した[3]。

トレンドマイクロ社によると、SUNBURST が検出されたと 12 月 16 日までに通知してきた事例のうち、米国が 53%、カナダが 9%、アルゼンチンが 7%、英国 6%、オーストラリア 4%で、その他 21%のうち少数だが日本のものもあった[4]。報道では、米

国政府機関として財務省、商務省、国防総省、国土安全保障省、国務省、司法省、エネルギー省などが被害を受けた組織のリストに挙がっている[5]。いくつかのメールアカウントが不正アクセスされたとの情報は出ているが、決して知られるべきでない機密がどの程度の被害を受けたのか、政府機関は明らかにしていない。

SolarWinds 社によるその後の調査により、2019 年 9 月に不正アクセスがあり、2020 年 3 月から SUNBURST マルウェアの拡散が始まっており、18,000 件程度の更新ファイルダウンロードがあったという。最大で 9 ヶ月ほど、見つからずに情報窃取が進んでいた可能性がある。

この事案の顕著な特徴は、非常に有利な立場をマルウェアが巧妙に利用して活動しており、問題発見が非常に難しかったというものである。Orion Platform の中に仕込まれたバックドアとして、SUNBURST は気づかれずに活動できる立場をもっていた。通常、被害を出したマルウェアはセキュリティ企業に分析され、そのシグネチャー(署名)が広く出回る。各システムにおけるマルウェア対策ソフトウェアがマルウェアのシグネチャーリストを更新し、新たなリストに合致するソフトウェアがあればマルウェアと判断し排除する。もし未知のマルウェアが、「ゼロデイ」と呼ばれる未知の脆弱性を利用して侵入した場合は、EDR(Endpoint Detection and Response)の機能を持つセキュリティソフトウェアが稼働していれば、データの流れなどを監視し、不審な大量送信や特殊データへの不審なアクセスを検出し、マルウェアの存在の特定につなげる。しかし Orion Platform の正規のデジタル署名を持つ更新プログラムの中に潜む SUNBURST は、正規の Orion が行うと認知されている広範なネットワーク監視の行動の中に紛れて情報を収集するため、Orion が不審な行動をとっていると判定するのは非常に難しいという特徴がある。しかも SUNBURST は、端末セキュリティツールの多くを無効化していた。

このように SUNBURST は、従来の手段と比べても非常に巧妙に開発され運用された高度の攻撃であり、マイクロソフトのプレジデント、ブラッド・スミス(Brad Smith)は、これは史上最も広範で洗練された攻撃で、1,000 人以上のエンジニアを必要とすると推測している[6]。

このような高度なサイバー攻撃を行う集団は「高度で持続的な脅威」(APT: Advanced Persistent Threat)と呼ばれている。未知の脆弱性を発見し、それを利用する方法を開発し、露見しにくいよう慎重に運用するには、相当の組織力が必要である。サイバー犯罪も高度化しているが、犯罪者が利益を得ようとするために被害者が損害を認識する機会は比較的多い。これに対し APT の多くは、特定の国益に整合する動機の一貫性をもって露見を回避して行動を続けているため、政府の指示を受けた組織と考えられている。主要な APT には、イラン、中国、北朝鮮、ロシア、ベトナムの政府に属すると考えられる組織が挙げられている。

実際に SUNBURST は、最大 9 ヶ月もの間、検出されずに広範囲に侵入し、少数特定の組織において情報窃取を行っており、相当の技術力を投入して実現したもので、一般のサイバー犯罪集団より格段に高い水準の攻撃である。報道では早くから、SUNBURST はロシアの対外諜報庁(SVR)に所属する APT29(ほかに"Cozy Bear"などいくつかの通称でも呼ばれる)によるものとされていた。セキュリティ専門家のドミトリー・アルペロヴィチ(Dmitri Alperovitch)は、状況証拠は SVR によることを示唆しており、破壊活動よりも諜報活動に特化した集団だと述べている[7]。

米国による報復をめぐる問題

このように 2020 年 12 月に SolarWinds 社事案が広く知られるようになってすぐ、報道などではロシア政府によるものと指摘されるようになったが、米国政府機関が公式にロシアを名指しするには時間がかかった。

事案が公になった直後の米政府高官のコメントとしては、マイク・ポンペオ国務長官がロシアによる攻撃と発言したのに対し、ドナルド・トランプ大統領は中国の可能性もあるとツイートした。2021 年 1 月 5 日の米国情報機関の合同声明は、最大で 18,000 の組織が影響を受けた可能性があるが、ごく少数の組織で実際の諜報活動があってその内容をなお調査しており、加害者は APT で、ロシア起源の可能性があると述べるにとどまった [8]。

米国ではロシアへの報復が議論されるようになったが、諜報活動やサイバー空間にまつわる特有の難しさがある。諜報活動に対する報復としては、諜報員と疑われる外交官を追放するという古典的な報復手段があるが、これはサイバー諜報活動能力を弱める効果的な反撃には見えない。また、ロシアに対して同様にサイバー諜報活動を行うのが報復だとすれば、これはすでに行っているはずであり、米国政府がそれを報復の証として公表するとは限らない。それであれば、公共空間では「サイバー被害を受けたのに米国の現政権は報復をしていない」と認識されることになる。

さらに、損害が目に見えるようにサイバー破壊活動を行うことは、分かりやすい報復の選択肢になるが、これは諜報活動から破壊活動へのエスカレーションであり、段階が上がった反撃を覚悟する必要がある。サイバー空間で反撃を受ける脆弱なところは米国に無数にあり、米国社会が受けるダメージが大きいため、これを覚悟して報復することは相当難しいと考えられており、例えばオバマ政権は何度も考慮しつつも実行は見送った [9]。

しかしロシアの米国に対するサイバー攻撃は高度化し継続しているため、何らかの報復手段をとるべきという主張も高まってきている。戦略国際問題研究所(CSIS)のジェームズ・ルイス(James Lewis)戦略技術研究部長は、コストを与える報復を考案することを提案する。例えばロシアでの腐敗を暴き、国民の不満が政権に向かうようになれば、政権がコストを感じることになるという [10]。

ただし、この例も実際に行うには難しい問題がある。もし誰が腐敗を暴いたのか分からないのなら、米国がロシアに報復を成功させたとは認識しにくい。一方、仮に誰がやったか不明でも、腐敗を告発する人々は何らかの形で北米・西欧の人々とつながり声援を受けているので、クレムリンは米国が仕掛けた重大な攻撃と認識するであろう。もともと、「ロシア連邦情報セキュリティドクトリン」などに見られるロシアの情報空間における安全観によれば、米国がロシア社会の脆弱性を攻撃し政治を不安定化させようとしていると考えるので、それをやめさせるための措置をとるという発想がある。例えば、ロシアの仕業とされた、2016 年の大統領選挙期間中の内部情報の暴露や SNS の不正利用を通じた対立感情の増幅は、先にロシアやウクライナに対して米国が工作を仕掛けてきたという認識にもとづく、米国に痛みを与えて思いとどまらせるような報復、ないし広義の「抑止」の手段として理解することもできる。いまロシアの情報空間を混乱させ政治・社会に影響する事件がおこれば、「やはり米国はロシアを攻撃している」という認識・言説は強まり、ロシアによると思われる新たな様相の攻撃も発生する可能性がある。そうなれば、米国はそれでもさらにロシアに打撃を与える姿勢を示すのか、エスカレーションの度合いを制御するための手段をとるのか、難しい問題が生じるだろう。

実際にバイデン政権が 2021 年 4 月 15 日に発表した報復措置も、このような問題を検討したうえでのものだっただろう。ホワイト・ハウスの声明は SolarWinds 社事案の責任者をロシアの SVR に属する APT29 と公式に名指しし、この件を詳述して、米国が問題視しているというメッセージを発している。声明全体としては、2020 年米国大統領選挙に際しての違法な情報流布、クリミア半島占領を含むウクライナへの攻撃・圧力、アフガニスタンでのタリバンへの教唆、SolarWinds 社製ソフトウェアを通じ

たサイバー諜報活動といった多くの問題をとりあげており、それらに対する対抗措置として、財務省による対象企業に対する経済制裁、ロシア外交官 10 名の追放、同盟国とのサイバーセキュリティ協力の強化を挙げた[11]。

このような報復措置は、米国としては慎重にしたものという評価がある[12]。実際、ロシア政府に協力するいくつかのテクノロジー企業に対する経済制裁は行うものの、SVR の中核に対する大きなダメージは意図していないようである。上記で述べたような問題点を勘案して、サイバーセキュリティ問題における報復はエスカレーション制御をしやすい手法と程度にとどめるという配慮もあろう。また、米国にとって長期的で深刻な挑戦は中国に関するものなのでそれを優先し、ロシアとは低いレベルでもある程度の安定した関係を望むという動機も考えられよう。バイデン政権は、4 月の声明でもロシアとの安定的な関係を望むと述べ、5 月の北極評議会で外相会談を行い、6 月に首脳会談を予定している。そのような安定化の努力も、それでも抑えられないサイバー空間での攻防も、米露両国はしばらく継続することになるだろう。

---

1 "Russian Foreign Intelligence Service Exploiting Five Publicly Known Vulnerabilities to Compromise U.S. and Allied Networks," National Security Agency, April 15, 2021, https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2573391/russian-foreign-intelligence-service-exploiting-five-publicly-known-vulnerabili/

2 山添博史「ロシアをめぐるサイバー問題―ロシアの情報セキュリティ概念と SolarWinds 社事案―」『大国間競争時代のロシア』(日本国際問題研究所、2021 年)、https://www.jiia.or.jp/research/JIIA_russia_research_report_2021.html

3 Kevin Mandia, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor," FireEye, December 13, 2020, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

4 「SolarWinds 社製品を悪用、米政府などを狙う大規模サプライチェーン攻撃」トレンドマイクロ、2020 年 12 月 16 日。https://blog.trendmicro.co.jp/archives/26849

5 セキュリティ専門家による日本語のまとめとしては「SolarWinds のサプライチェーン攻撃についてまとめてみた」piyolog, 2020 年 12 月 20 日、https://piyolog.hatenadiary.jp/entry/2020/12/20/045153 , 2021 年 2 月 5 日アクセス(1 月 30 日最終更新)。筆者 piyokango 氏は 2017 年 5 月、迅速・的確なインシデント解説記事の発信により公共のセキュリティ向上に貢献したとして、「サイバーセキュリティに関する総務大臣奨励賞」を受けている。

6 "SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments," CBS News, February 14, 2021, https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/

7 "SolarWinds Breach: An RSAC Interview with Dmitri Alperovitch About Who, How and Why," RSA Conference, December 14, 2020, https://www.rsaconference.com/industry-topics/video/solarwinds-breach-dmitri-alperovitch . アルペロヴィチはロシア出身で、中国による Google 等へのサイバー攻撃を特定し、CrowdStrike 社の共同創立者となったセキュリティ専門家である。

8 "Joint Statement By The Federal Bureau Of Investigation (FBI), The Cybersecurity And Infrastructure Security Agency (CISA), The Office Of The Director Of National Intelligence (ODNI), And The National Security Agency (NSA)," CISA, January 5, 2021, https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

9 デービッド・サンガー『世界の覇権が一気に変わる サイバー完全兵器』(朝日新聞出版、2019 年、Kindle 版)「はじめに」、位置 No. 221。

10 "Cybersecurity experts say U.S. needs to strike back after SolarWinds hack," CBS News, February 14, 2021, https://www.cbsnews.com/news/solarwinds-60-minutes-2021-02-14/

11 "FACT SHEET: Imposing Costs for Harmful Foreign Activities by the Russian Government," U.S. White House, April 15, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

12 "US imposes sanctions on Russia over cyber-attacks," BBC, April 16, 2021, https://www.bbc.com/news/technology-56755484