第 11 章　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―

山添　博史

はじめに

2020 年 12 月、米国でサイバー情報窃取を可能にするマルウェア（ウイルスを含む、悪意のソフトウェア）SUNBURST が、SolarWinds 社のネットワーク管理ソフトウェアを利用する多くの組織に拡散した事案が公になり、ロシアによる深刻なサイバー攻撃として大きく報道されている。しかし米国もロシアも事態の全容を明らかにするとは限らず、世界のサイバーセキュリティの実態を理解するのは困難を極める。サイバーセキュリティ問題について安全性を高めていくには、公的組織が発表する事案の状況に限らず、多様な場面で論じられているサイバーセキュリティの動向や過去の事例も交えて、厳密ではなくても趨勢を理解し、必要な措置を講じる継続的な努力が必要だろう。本章では、ロシアのサイバーセキュリティの考え方の手がかりとして「情報セキュリティドクトリン」の概要を検討し、その理解を交えつつ、SUNBURST の事案で生じている問題を取り扱う。

1. ロシアの情報セキュリティの概念

2016 年 12 月、ロシアのプーチン大統領は「ロシア連邦情報セキュリティドクトリン」（以下、「情報セキュリティドクトリン」）に署名した[1]。これは、2000 年の文書を更新したもので、事前に草案を公表して意見を聴取したうえでの決定であった。大きな変化の一つは、外国による情報空間の操作により社会の安定が脅かされるという脅威認識を書き込んだことである。

その変化は、2014 年の危機を経て国家安全保障の脅威認識が先鋭化した動向に沿ったものと言える。2014 年 12 月の「ロシア連邦軍事ドクトリン」の更新では、「軍事的危険」として、ロシア国内の愛国的伝統を損なう宣伝など、軍が本来対処するものではないような情報空間における問題を挙げている。2015 年の「ロシア連邦国家安全保障戦略」でも同様の趣旨の記述が追加された[2]。2016 年の「情報セキュリティドクトリン」も、この「ロシア連邦国家安全保障戦略」を根拠文書の一つに挙げており、上記 2 つの文書と同様に、国家の安全を守るための重要な場として情報空間を論じている。

2014 年 12 月の「ロシア連邦軍事ドクトリン」では、非核抑止システムとして、「ロシア連邦への侵略を非核手段で予防するための、対外政策・軍事・軍事技術手段の複合物」を用いると定めている。これは、2014 年のウクライナ政変を外国によるロシアの国益への攻撃とみなし、それに対する手段として核抑止は有効ではなく、非核手段によるべきだという議論があったからである。2011 年のリビアにおいて政権反対運動が広がり、外国による軍事介入につながり、その結果政権が崩壊し国家が分裂したという理解がロシアでは有力であり、ロシア軍は非軍事手段と軍事手段を交えたものが現代の戦争だと認識している。そして、このような軍事に限らない脅威に対して抑止を行うことを「戦略的抑止」と述べるようになってきた[3]。

「情報セキュリティドクトリン」も、このような戦争観において国益を情報空間で防衛す

るという趣旨が強いものである。これは第3部「脅威」の構成からも見えてくる。まず第10条で、地政学的目的、テロリズム、犯罪で国際平和と戦略的安定性を損なうものを脅威としている。以下、脅威として挙げるのは、外国が軍事目的のために情報インフラに影響を与えること（第11条）、外国諜報機関が主権を侵害し伝統的価値や若者に悪影響を与えること（第12条）、テロ・過激派組織の情報空間利用（第13条）、個人情報犯罪（第14条）などである。このように、テロ組織や犯罪者よりも、外国がロシアの情報セキュリティに脅威を与えていることが主要な問題として扱われている。

ロシア政府による「情報セキュリティ」（информационная безопасность）の用語の選択も、「サイバーセキュリティ」（кибербезопасность）の語とは異なり、このような考え方を背景に持っていると考えられる。サイバー空間において不正アクセスの脅威からいわゆるCIA、すなわち機密性（confidentiality）、完全性（integrity）、可用性（availability）を守って情報システムを運用するという論点よりも、ここでの「情報セキュリティ」は広く政治・社会に影響する情報空間全般を対象とし、一方で政府が社会を管理するという立場に強く結びついている。合法的手段を用いた情報通信であっても、「情報セキュリティ」への脅威にはなりうる。

第4部「情報セキュリティ保障のための戦略目的」が挙げる対策では、まず第21条に軍事政策を記載している。第22条で国家、社会、人権、情報インフラを守る行動を挙げる。第23条ではイデオロギー、外国エージェントに注意する。第25条で、経済分野として技術向上、外国依存の減少を目指す。第29条は、戦略的安定性と戦略的パートナーシップ、主権の確保、脅威から守るための国際協力、国際法を挙げる。

このようなロシアの情報セキュリティ観でいえば、民間企業や一般行政機構をサイバー犯罪から守り社会のサイバー空間利用の安全性を高めるよりも、外国による政権転覆につながる情報空間全体の管理が重要課題になる。それに関連して、国内でのテロ組織のみならず、野党の組織的運動を制御するための情報空間の管理・活用にロシアの政権は取り組んでいる。

「情報セキュリティドクトリン」第29条に挙げている国際協力として、ロシアは上海協力機構加盟国、特に中国との協力を重視している。国連では中国、ロシア、タジキスタン、ウズベキスタンが「テロリズム、分離主義、過激主義を助長し政治、経済、社会の安定を損なう情報の流布」をとどめるための規則づくりを提案している。2015年に習近平国家主席とプーチン大統領が「情報セキュリティ協力」の文書に署名した。両国は共通の脅威認識を示し、協力枠組みの構築に努めている一方、サイバー攻撃手段におけるノウハウを共有せず、互いに対する諜報活動は続けていると見られる[4]。

2. サイバー攻撃をめぐる米露関係

（1）SolarWinds社製品を通じたサイバー攻撃事案

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）CEOが、訓練用のサイバー攻撃ツールに対する不正アクセスを発見し、最高レベルの政府組織能力によるサイバー攻撃だとみなして、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[5]。発見のきっかけは、不正ユーザーがFireEye社の多要素認証メカニズムにおいてアクセスを許可する端末として自分のものを新たに登録したとき、管理者に警告が通

知され、正当なユーザーに確認したところ本人ではないと判明したことだった[6]。

同社は調査を継続し、12 月 13 日に続報を発表した。SUNBURST と名づけたマルウェアが、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いうものだった[7]。同日、米国国土安全保障省のサイバーセキュリティ・インフラセキュリティ庁（CISA: Cybersecurity and Infrastructure Security Agency）が緊急通達を出した[8]。日本の内閣サイバーセキュリティセンター（NISC）も 14 日に政府機関に注意喚起を行い、また一般への注意喚起を公表した[9]。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のダウンロードがあったという[10]。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。

さらに、SolarWinds 社への侵入経路も調査されている。その可能性の一つとして、『ニューヨーク・タイムズ』紙は JetBrains 社のソフトウェア開発ツール TeamCity を報じた。それが事実なら全世界で SolarWinds 社のようなバックドアを何千も設置することを可能にするという[11]。しかし、SolarWinds 社の調査でも TeamCity が侵入の原因になってはいないと、JetBrains 社は説明している[12]。

いずれにしても、何らかの入り口から、SolarWinds 社の Orion Platform という広く使われているシステムにバックドアが設置され、それを利用する多くの組織が情報窃取の被害を受ける可能性があるため、「サプライチェーン攻撃」と呼ばれることが多い。攻撃者は、認識されるような損害を多く出せば発覚のリスクが増えるため、対象を絞って慎重な情報収集をしてきたようである。それでも、最終目的に関する情報を持つ関連企業は情報窃取の対象になる。このように、サプライチェーンを狙う今回の事案の特徴として、米国政府機関のみならず多くの関連企業が窃取の被害を受けることになり、多くの組織で対策をとらねばならないことになる。政府の立場からは、オンプレミス（組織敷地内に設置するシステム）だとしても、それを運営するためのソフトウェアを提供する企業や、その開発の過程のすべてからバックドアを排除し続けなければ、窃取できる出入り口を許してしまうことになる。

しかも 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アップデートの中に潜む 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（例えば Orion 上のモジュール Network Performance Monitor はネットワーク上の通信状況を把握する[13]）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[14]。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な攻撃であり、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[15]。

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%、英国が6%、オーストラリアが4%で、その他21%のうち少数だが日本のものもあった[16]。

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[17]。機密情報が盗まれたことを確認したとは明らかにされていない。攻撃者や報道機関などによる機密情報のリークも確認されておらず、本当に重要な機密情報が盗まれたとはまだ言えない。また、政府機関がFireEye社よりずっと早く攻撃内容を把握していたが秘匿していたという可能性も低い[18]。もし秘匿していたのであれば、政府機関が多くの民間企業、しかも政府機関に関わる企業への被害拡大を許していたことになるので、考えにくいだろう。

（2）ロシアの関与に関する言説

2020年12月にSolarWinds社製品を通じたサイバー攻撃が知られるようになってすぐ、これはロシア政府によるものと報道されるようになったが、米国政府機関はその根拠を明確に示していない。そのような具体的な情報源を秘匿するのは通例のことである。

マイク・ポンペオ国務長官は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[19]。2021年1月5日の連邦捜査局（FBI）、サイバーセキュリティ・インフラセキュリティ庁（CISA）、国家情報長官室（ODNI）、国家安全保障局（NSA）の合同声明によれば、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「高度で持続的な脅威」（APT）で、ロシア起源の可能性があると述べている[20]。

APTとは“Advanced Persistent Threat”であり、技量が高く組織的な成果でサイバー攻撃を行う集団のことである。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。組織力があり、犯罪の利益よりも特定の国益に整合する動機の一貫性があることで、このようなAPTの多くは政府の指示を受けた組織によるものと考えられている。FireEye社は主要なAPTの紹介として、イラン、中国、北朝鮮、ロシア、ベトナムの政府によると考えられる組織を挙げている[21]。

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、SUNBURSTはAPT29別名“Cozy Bear”、ロシアの対外諜報庁（SVR）に所属するサイバー攻撃集団によるものとされている[22]。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[23]。ほかに、ロシアの軍参謀本部諜報総局（GRU）に属するとされるAPT28別名“Fancy Bear”によるサイバー攻撃も複数知られている。ロシアでの報道では概して、米国におけ

るロシア関与の言説や米露関係の悪化について報じているが、ロシアの関与を否定するための主張はそれほど強くない[24]。当の APT28 や APT29 も、発覚した際には自らが何者かを示す痕跡を残しており、民間のセキュリティ企業が秘密の情報源なしに攻撃者を特定できた[25]。互いに競争して実績を示しているか、あるいはロシアの能力への恐怖を煽る趣旨が考えられよう。

しかし我々が公開情報で得られる根拠だけで、ある APT が特定政府の指揮下にあると確信することは難しい。また、ある単一の集団が脆弱性を利用して攻撃するとも限らない。2021 年 2 月 3 日のロイターの報道によると、SolarWinds 社製ソフトウェアの別の脆弱性を利用して米国政府機関に侵入した事案が見つかり、これは侵入の特徴から中国のものであるとされているという[26]。

SUNBURST が特定組織に限定した情報窃取を目的とするものだとして、その被害の重大性を検証するのは難しい。もし、広範囲の被害が想定されうる攻撃にもかかわらず、米国の民間セキュリティ企業と政府組織がこれを発見し、機密情報の窃取や基幹システムの破損に及んでいないのが事実であれば、米国のサイバー防御能力が高いことを示しているとも言える。逆に、米国政府機関が確認できない、あるいは確認しても公表しない、甚大な機密情報窃取が行われた可能性もあり、この場合は SUNBURST が米国政府を打ち負かしたことになろう。1940 年代にソ連はワンタイムパッド（1 回限り暗号表）を用いた高度な暗号通信を利用し、長らく誰にも破られていないとされていたが、実は米国の VENONA プロジェクトが暗号を解読し活用したことを秘匿していたことが、1990 年代に明らかになった[27]。このように秘密諜報活動でどちらがどのように上回ったのか、明らかになるまで長い時間がかかる、あるいは明らかになることがないという可能性もある。

米国ではロシアへの報復が議論されている。米国政府がこれをロシアによる諜報活動とみなし、ロシアに対して同様に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、それを報復の証として公表するとは限らない。実際に、2020 年 10 月に FBI がサイバー攻撃の犯人としてロシア GRU の職員の顔写真を公表したが、これはロシアに対する諜報活動あるいは対諜報活動（カウンターインテリジェンス）の成果の一部であろう。あるい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。さらに、損害を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、このようなエスカレーションでは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[28]。

攻撃者が情報窃取を行っていたとして、情報空間での攻撃がそこで終わっているとは限らない。他国政府に内情を知られる以上に、政治・社会に損害をもたらす方法がある。例えば、2014 年のウクライナ問題に際して、米国務省のヴィクトリア・ヌーランドは電話の会話で、自らの断固たる外交姿勢に対応が追いついていない EU 側の姿勢を非難する表現を用いた。彼女はロシアが盗聴しうることを認識していたが、それで米国の本気の態度をロシア当局が確信するなら構わないと考えていた。しかし問題は、プーチン政権がヌーランドの率直な会話の内容（すでに公になっている政策）を知ったことではなく、その音声が加工されて YouTube に現れ、米国が下品な言葉で EU を罵り、ウクライナをめぐって無様な仲間割れをしている印象が広まったことだった。これはロシアの「積極工作」の転機

だった[29]。

すなわち、秘密であるべき空間の情報が関係者以外に知られたという問題のみならず、それを根拠として公開空間で信頼性を損なう言説が猛威を振るうという現象が深刻さを増してきたのである。捻じ曲げているとはいえ、そこに根拠があるために、米国のような公開空間では「捏造されたプロパガンダである」という主張が通りにくく、やはり信頼性は損なわれてしまう。

類似例で著名なのは、2016年の大統領選挙における民主党内部情報の暴露である。民主党選挙対策本部のメールが盗まれ、7月22日にウィキリークスから公開された中の一例によると、選挙スタッフがバーニー・サンダース候補に不利になるような質問を用意する謀議をめぐらせており、ヒラリー・クリントン候補陣営による不正の印象が広まった[30]。すなわち、政府中枢の最高機密情報でなくても、秘密の通信から公開空間に持ち出す内容と方法によっては、政治プロセスに重大な被害が及ぶのである。そのあと2017年1月、米国情報機関はロシアが行った工作だと断定したが、それでも米国の大統領選挙が歪められたという認識は消え去るものではなく、米国の民主プロセスが受けた損害は大きかった。さらに、根拠のない「フェイク・ニュース」でも、恐怖や怒りの感情を利用して広まっていけば、社会言論空間に大きな混乱をもたらすことが可能である。

上記のような事例が、ロシアが意図して実行したものとするならば、それは第1節で述べたような、ロシアの情報セキュリティにおける脅威の概念と整合性が高いものである。すなわち、国際関係において対象国を圧迫し、あるいは政情不安や軍事紛争を引き起こす手段として、その社会の政治プロセスに大きく作用する形で情報空間を操作するというものである。もしクレムリンが、2011年のロシア国内反政権デモの広がりや2014年のウクライナ政変を、情報セキュリティへの脅威を通じた米国によるロシア攻撃とみなし、それを繰り返させないための手段の一環として、米国社会の情報セキュリティの脆弱性を利用した攻撃を実行しているとすれば、それは「非軍事手段による戦略的抑止」としても理解しうるものである。攻撃がロシア発であるという認識が広まる根拠を攻撃者が残していることも、それと整合する。それであれば、サイバー／情報空間における重大な事件がさらに発生していくことを、我々は予期せねばなるまい。

おわりに

サイバーセキュリティ上の脅威は日々高まっており、本章で見たように非常に巧妙な手法も現れている。これらの問題は日常生活を脅かすのに加えて、国際関係を複雑化させ、大きな危険もはらむものである。サイバー脅威を根絶することができなくても損害を低減するために重要なのは、サイバー攻撃を行った側が得られる利益が少なく、要するコストが大きくなることであろう。2019年頃から猛威を奮っているマルウェアEmotetに関しては、ウクライナやオランダの警察機関が自国内の攻撃拠点を物理的に制圧し、そこのサーバーを通じてEmotetマルウェア除去の措置をとったため、かなりの程度損害の拡大は止まり、また加害者が利益を得ることも妨げられた[31]。このような犯罪組織も政府系集団も、安価に利益を得るか損害を与えられるのであればサイバー攻撃を頻発させるが、それが難しくなれば頻度は下がるだろう。

ロシア政府も情報セキュリティへの脅威を減らすため、外交手段も用いている。冷戦

時の核軍備管理や保健問題のように、対立する国際関係においても協力が成立する余地はあり、サイバー問題についても可能性は慎重に検証していく必要があろう。ロシアは、最近ではフランスや日本と情報／サイバーセキュリティの協議を行っている。2019 年 11 月の日本との第 3 回サイバー協議では、ロシアのアンドレイ・クルツキフ（Андрей Владимирович Крутских）情報セキュリティ国際協力担当大統領特別代表・外務省特任大使や日本の赤堀毅外務省総合外交政策局参事官兼サイバー政策担当大使らが、情報空間に関する互いの戦略、多国間協力、テロ・犯罪組織対策、重要インフラ防護などについて話し合った[32]。

米国に対しては、ロシアはプーチン大統領の声明を発表し、情報セキュリティ分野でのハイレベル対話の再開、1972 年の米ソ海上事故防止協定（INCSEA）に類似した行動規範の合意、国内問題への相互不干渉の合意などを呼びかけた[33]。一方、2021 年 1 月に成立した米国のバイデン政権は、新 START 条約の延長は速やかに進めたものの、ロシアとの重大問題の一つにサイバー問題を挙げている。米露間において、情報／サイバーセキュリティをめぐっての立場の相違や互いの行動に対する不信感は根強く、国際協力の実体化はまだまだ難しいだろう。

国際協力が進みにくい間は、セキュリティ脅威を発見し共有して各組織が強靭性を高めていく努力が一層重要になろう。いくら防御を高めていても、サイバー攻撃は日常的に行われてその手法は極めて速く高度化していく。本章で扱った SolarWinds 社の事案は、その顕著な事例であり、このようなことが進行し続けるならば、多くの組織は気づかないままに情報窃取の被害に遭ったり、いつ何時でも破壊活動が始まりうる拠点を抱えることになる。しかし、組織の最重要の情報システムが被害を受ける前に、より一般的な情報システムにおいて脅威を発見できれば、その損害を限定し、かつ攻撃者に利益を与えることを拒否することができる。アルペロヴィチは、常に侵入が行われうることを仮定して、損害を限定する措置をとるほかないと指摘している[34]。侵入されることを前提として、システム内部のすべての情報アクセスを疑って検証することで、問題検出の機会を極大化する「ゼロトラスト」の考え方などをうまく活用し、サイバー空間の品質を不断に高めていく努力が必要だろう。

―注―

1　2016 年 12 月 5 日ロシア大統領令第 646 号による。http://kremlin.ru/acts/bank/41460 ;『ロシア新聞』にも掲載、«Доктрина информационной безопасности Российской Федерации,» *Российская Газета*, December 6, 2016, https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html ; 英語版はロシア外務省が unofficial translation として掲載。https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

2　「ロシア連邦国家安全保障戦略」「ロシア連邦軍事ドクトリン」の邦訳は、小泉悠『軍事大国ロシア：新たな世界戦略と行動原理』（作品社、2016 年）を参照。

3　「戦略的抑止」の概念をめぐる動きと「軍事ドクトリン」にかかる議論については小泉悠『軍事大国ロシア』を参照。本章筆者による関連の記載は、山添博史「ロシアの国際闘争手段としての核兵器：『戦略的抑止』における最終手段、紛争局限手段、言説攻勢手段」『国際政治』第 203 号（2021 年 4 月）。

4　Adam Segal, “Peering into the Future of Sino-Russian Cyber Security Cooperation,” War on the Rocks, August 10, 2020, https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/

5 Kevin Mandia, “FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community,” FireEye, December 8, 2020, https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html 筆者マンディアは、米軍のコンピュータ・セキュリティ担当将校を経てセキュリティ事業の Mandiant 社を創業し、FireEye との統合後も経営職を務める。

6 「SolarWinds 事件を詳しく解説：ユーザー ID とパスワード認証ではサイバー攻撃を避けられない」CloudGate, 2021 年 1 月 22 日、https://www.cloudgate.jp/blog/2021/1/solarwinds-cyber-attack-cause-and-how-to-avoid.html?gclid=EAIaIQobChMI1pP0lcq67gIVEQRgCh0fUwuQEAAYAiAAEgLY7fD_BwE

7 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

8 https://cyber.dhs.gov/ed/21-01/

9 「SolarWinds 社製 SolarWinds Orion Platform ソフトウェアに関する政府機関等への注意喚起の発出について」内閣サイバーセキュリティセンター、2020 年 12 月 16 日。 https://www.nisc.go.jp/active/general/pdf/chuikanki201216.pdf

10 「1 年以上も検出できなかった『史上最大級の高度な攻撃』、同じ弱点は世界中に」ITmedia News, 2021 年 1 月 25 日、https://www.itmedia.co.jp/news/articles/2101/25/news064.html

11 Nicole Perlroth, David E. Sanger and Julian E. Barnes, “Widely Used Software Company May Be Entry Point for Huge U.S. Hacking,” *New York Times*, January 6, 2021.

12 「SolarWinds 社関連の報道に対する続報」JetBrains, January 8, 2021, https://blog.jetbrains.com/ja/blog/2021/01/08/an-update-on-solarwinds-ja/

13 “Orion Platform,” SolarWinds, https://www.solarwinds.com/ja/orion-platform , accessed on February 10, 2021.

14 Matt Bromiley, Andrew Rector, Robert Wallace, “Light in the Dark: Hunting for SUNBURST,” FireEye, February 16, 2021, https://www.fireeye.com/blog/products-and-services/2021/02/light-in-the-dark-hunting-for-sunburst.html

15 “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/

16 「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

17 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。

18 David E. Sanger, Nicole Perlroth and Eric Schmitt, “Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit,” *New York Times*, December 14, 2020.

19 Rachel Sharp, “Trump slams Pompeo for blaming Russia for huge cyber attack as he breaks his silence to say CHINA could be responsible and that voting machines may have been hit - but claims it is 'well under control',” *Daily Mail*, December 20, 2021.

20 “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

21 「APT 攻撃グループ」FireEye, https://www.fireeye.jp/current-threats/apt-groups.html , 2021 年 2 月 17 日アクセス。

22 例えば、「米政府機関、ハッキング被害で情報流出　ロシアの集団が関与か」CNN.co.jp、2020 年 12 月 14 日、https://www.cnn.co.jp/tech/35163799.html ; Ellen Nakashima and Craig Timberg, “Russian government hackers are behind a broad espionage campaign that has compromised U.S. agencies, including Treasury and Commerce,” *Washington Post*, December 15, 2020.

23 “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。

24 «Дональд Трамп затоптал русский след,» *Kommersant*, December 21, 2020, https://www.kommersant.ru/doc/4624966 ; «"Холодная война" США с Россией стала цифровой,» *MK*, January 27, 2021, https://www.mk.ru/politics/2021/01/27/kholodnaya-voyna-ssha-s-rossiey-stala-cifrovoy.html

25 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）第 9 章、位置 No. 4755。ロシア政府系とされるサイバー事案の多くを参照するには、廣瀬陽子『ハイブリッド戦争　ロシアの新しい国家戦略』（講談社、2021 年）第 2 章。

26 “Exclusive: Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources,” Reuters, February 3, 2021, https://www.reuters.com/article/us-cyber-solarwinds-china/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-u-s-payroll-agency-sources-idUSKBN2A22K8

27 ジョン・アール・ヘインズ、ハーヴェイ・クレア『ヴェノナ：解読されたソ連の暗号とスパイ活動』（PHP 研究所、2010 年）。

28 サンガー『サイバー完全兵器』「はじめに」、位置 No. 221。

29 サンガー『サイバー完全兵器』第 8 章、位置 No. 4167。

30 小川聡、東秀敏『トランプ　ロシアゲートの虚実』（文藝春秋、2018 年、Kindle 版）、第 5 章、位置 No. 2149。

31 “World’s Most Dangerous Malware Emotet Disrupted Through Global Action,” EUROPOL, January 27, 2021, https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

32 “Press Release on the Outcome of the Third Round of the Japan-Russia Interagency Consultations on International Information Security,” Ministry of Foreign Affairs of Russian Federation, November 21, 2019, https://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/3908177 ; 「第 3 回日露サイバー協議の開催」外務省、2019 年 11 月 20 日、https://www.mofa.go.jp/mofaj/press/release/press4_008022.html ; なお、2020 年 1 月 23 日には第 2 回日ウクライナサイバー協議が行われた。

33 «Заявление Президента Российской Федерации В.В.Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности,» Ministry of Foreign Affairs of Russian Federation, September 25, 2020, https://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/4350560?p_p_id=101_INSTANCE_UsCUTiw2pO53&_101_INSTANCE_UsCUTiw2pO53_languageId=ru_RU

34 “SolarWinds Breach: An RSAC Interview with Dmitri Alperovitch” RSA Conference.