印中国境衝突に係わるサイバー攻撃～我が国への教訓

執行役員　熊本　義宏

1 はじめに

インドと中国の国境を巡る衝突については、中国の攻撃的な進出行動を受けている我が国として教訓となり得る事項があると考え、本誌令和 2 年 11･12 月合併号で掲載しました。

実効支配線（ＬＡＣ）を巡る緊張から 45 年ぶりに両国は直接的な衝突に至ったわけですが、それらの行動に合わせ、中国によるサイバー攻撃が組織的に行われていたということが、米国のサイバー攻撃分析会社であるレコーデッド・フューチャー社から２０２１年２月に出された報告書により明らかになりました。我が国においても、防衛大綱においては、宇宙・電磁波・サイバーの分野が安全保障上、大きな役割を果たすことが示されており、サイバーの分野はその一つとして対応強化の必要性が強調されています。そして、その対策も着々と進められているところです。そのような状況を踏まえて、今般、緊張化する情勢の中で行われたサイバー攻撃について着目し、その態様について考察し、我が国としての教訓を得ようとするものであります。

２ ラダックを巡るインド・中国間衝突のフォローアップ

昨年 6 月にラダックのガルワン渓谷において、インドと中国との間で起きた 45 年ぶりの直接衝突については、火器そのものは使用されませんでしたが、こん棒などを使った徒手格闘の様相になり、20 名のインド軍兵士犠牲を含め双方に相当数の被害がありました。その後、両国は大規模な部隊動員がかけられ、双方の戦力が集中し事態は緊張化に向かっていました。

その中で、両国は紛争の拡大を抑制するために、将官級協議を数次にわたり行い解決の糸口を探っていました。特に、中国軍は複数個所においてＬＡＣを越えた進出が確認されており、少なくともＬＡＣ以東に後退するよう、インドは強い要求を続けていました。

3 月 1 日に行われた 11 回目の協議において、そのひとつであるパンゴン湖正面での兵力引き離しについて両国が合意し、その後、中国は同地より後退したことにより、膠着状態となっています。

３ 緊張が激化するインド・中国間情勢下でのサイバー攻撃

レコーデッド・フューチャー社の報告書によると、新型コロナウイルスの世界的な感染拡大を始めた２０２０年初頭から、中国政府が関与しているとされるサイバーグループがインド政府の各機関のシステムに対して大規模な侵入を始め､インド軍と中国軍との衝突が現実化した5月頃からは、マルウエアによるプログラムのダウンロードやデータの不正入手が激化しました。6 月に起きたガルワン渓谷での両国の衝突およびその後のＬＡＣ周辺地域における両国軍の戦力集中に呼応しつつ、水面下でサイバー攻撃は進行していたようです。

インドの電力や港湾機関のネットワークへの不正侵入が増大し、遂には 10 月にムンバイにおける大規模な停電を引き起こし、公共交通機関を含む都市機能が一時的にマヒするという重大な結果に至りました。この報告書はたいへん興味深いものであり、以下でその概要を紹介しつつ考察したいと思います。

（１）インドによる中国関係アプリ等の使用禁止措置

インド、中国両国の緊張感が高まり、２０２０年 5 月初旬以来、両国間の争いは表面化しＬＡＣ沿いの小競り合いが頻発するようになりました。そのような中で、6 月に入り、インド政府は動画配信ソーシャルメディアであるティックトックの使用を禁ずる措置を講じました。ティックトックについてはそれを運営する会社が中国テクノロジー大手のバイトダンスであり、利用者のデータ収集を行い、また、中国のサイバーセキュリティー法に基づきスパイ活動に利用されかねないとの懸念を認識し使用の禁止を決定したわけです。

さらに、両国間の紛争が混沌化する中、サイバー攻撃の進展を恐れ、11 月末までに２００以上の中国アプリが使用禁止にされました。

米国においても同様の認識の下、8 月にはトランプ政権はティックトックを使用停止にする行政命令を出しています。バイデン政権に替わり検討の結果、ティックトックとウィーチャットを禁止する行政命令の実行を停止した上で、それらアプリの安全保障上の脅威について再調査していくことを明らかにしました（6 月現在の状況）。

（２）両国のサイバースパイ活動の活発化

また、両国によるサイバースパイ活動が活発化しました。インド系グループのサイドワインダーは、中国軍や政府機関を標的にしたサイバー活動を行っていましたが、一方で、中国系グループは、5 月の軍事行動に呼応してプラグＸ・マルウエア指令サーバーを活発化させインドの公共機関や軍事組織を標的とする活動に指向しました。このように、ＬＡＣ周辺での衝突の収拾を模索しつつ、有利な条件の作為を狙いとしてスパイ活動やマルウエアなどによるサイバー活動が水面下で続けられていたわけです。

（３）レッドエコーによるインド政府機関等へのサイバー侵入

活動報告書によると、中国が後援する脅威グループであるレッドエコーは、サイバー活動を大規模に行っているとのことです。　中国が後援するグループとしては、他に、ＡＰＴ41、トントチーム、キーボーイ、ティックなどが確認されていて広範な活動に関連しています。

レッドエコーはなりすましドメイン構成の手法でインドの発電所や送電所に侵入していきました。標的とされた機関は、10 個の発電・送電機関および 2 個の港湾機関であることが特定されました。それらは、インド国家重要情報施設防護センター（ＮＣＩＩＰＣ）が重要施設として指定している機関です。特定にあたっては、21 のＩＰアドレスが 12 機関を標的としている状況を把握したとのことです。

レッドエコーは、インドの電力機関の中で、全国に５個ある地域電力配分センター（ＲＬＤＣ）のうち、少なくとも４個のセンターや２個の州電力配分センター（ＳＬＤＣ）を標的として、疑わしいネットワーク侵入を行っていることが確認されています。これら機関は電力の供給と需要のバランスを図り、安定した電力を維持する重要な責任を有しています。さらに地域のメディアの報道によると 10 月に起きたムンバイにおける停電については、近郊の町パドハに所在するＳＬＤＣのシステムに埋め込まれたマルウエアとの関連があるとしています。停電とマルウエアとの関連性は、裏付けが得られていませんが、インド電力配分センターが標的とされていることは確かであることから、

関連性があるとの見解を示しています。
　インド電力機関に対するレッドエコーの侵入としては、他に、高圧変電所や石炭火力発電所を標的にしたものもあります。また、２個のインドの港湾機関（ムンバイ港およびＶ・Ｏ・チダンバラナール港）についても、レッドエコーの標的となっていることも確認されています。

（４）レッドエコーの手法

ア シャドウパッドの使用

　それでは、どのような手口で当該機関への侵入を成し得たのでしょうか。それには、シャドウパッドというバックドアが使われています。バックドアは、直訳すれば「裏口」または「勝手口」のことですが、コンピュータの機能を不正に利用するために設けられた通信接続の機能のことを言います。
　シャドウパッドはその一つであり、２０１７年に起きた不正アクセス事案で初めて明らかにされたものです。この事案は、世界的大手企業にサーバー管理ツールを提供しているネットサラング・コンピュータ社配信のソフトウェアパッケージに埋め込まれたバックドアであるシャドウパッドが発見されたというものです。

　レコーデッド・フューチャー社の報告書では、シャドウパッドは後に、ファイアーアイがＡＰＴ41（バリウムやウインティなどのグループと部分的に一致）による侵入に使われていると解析しています。ＡＰＴ41 のみならず､中国系グループにより２０１９年後半から広く使われるようになり、中国国家セキュリティー省や人民解放軍でも広く使われているとのことです。　現段階で、中国系の少なくとも 5 つのグループ（ＡＰＴ41、トントチーム、アイスフォッグ・クラスター、キーボーイ、ティック）がシャドウパッドを使っていることがわかっています。最近ではそのインフラがモンゴルでのビジネス管理会社ともつながり、中国系グループであるＴＡ４２８やラッキーマウスと関連してさらに広がっているようです。
　昨年 9 月には、ＡＰＴ41 の運用者 5 人が米政府に訴追され、ダミー会社である成都４０４ネットワークテクノロジーとつながっていたことが判明しました。また、中国の民間契約者やダミー会社が中国国家セキュリティー省のためにサイバースパイ活動を実施している実態も浮き彫りになり、そのつながりが明らかになりました。
　また、トントチームは遼寧省の省都瀋陽に所在する人民解放軍の軍事地域技術偵察局と深く係わっています。シャドウパッドは中国系グループがサイバースパイ活動をするために広く活用されている最新の手段だと分析しています。
　シャドウパッド感染のために利用されているネットワークインフラは AXIOMATICASYMPTOTE(以下、「Ａ」と言う）として特定されています。Ａサーバーは、ネットワークインフラ検知、ドメイン分析やネットワーク伝送分析の能力を有していて、レッドエコーがインド電力機関を標的とした大規模な行動に使われています。

イ レッドエコーインフラの戦術・技術・手順

　レッドエコーが使う「Ａ」サーバーはいくつかのインド発電所や送電所のなりすましドメインを

構成しました。それには、インターネットユーザーがウエブブラウザにドメインを入力する際に犯す打ち間違いを利用するタイポスクワティングが使われています。ユーザーが誤ったドメインを偶然に入力すると、なりすましドメインに導かれるというわけです。

レッドエコーの識別された侵入行為における運用インフラの手口としては、聞きなれない当局サーバーネームをドメインとして登録、中国ドメインの再販、フーイズ・プライバシー・プロテクション・サービスの利用、「A」インフラが他社をホスト、インド機関やインドに関連した文字列のなりすましドメインを使用、共通したドメインである.com を使用、ダイナミック・ドメイン・ネーム・システム（ＤＤＮＳ）を使用、といった特性を有します。

これらはレッドエコーに特有のものではありませんが、全般的な分析により、レッドエコーの行動であるとみなしています。これらの手法を基礎として、関連する更なるドメインの識別を行っています。

ウ レッドエコーの関与

少なくとも３個のＩＰアドレスが、２０２０年 11 月にインドの石油・ガス関連機関を標的としたＡＰＴ41 の関連が疑われている活動の中で確認されています。さらに、多数のドメインをホストする 2 つの「A」サーバーが、多くのＩＰアドレスと交信するのが確認されています。この行為は、ＡＰＴ41 による行為とも一致し、また、レッドエコーの行為にも通じるものです。また、インドの石油・ガス・エネルギー企業を標的にしていたトントチームとの関連性があることも重要な点です。

このように相互関連性はわかっていますが、このことで特定のインド電力機関への関与に対する十分な証拠になるとは言い切れません。従って、引き続き継続的に追跡をして、レッドエコーと深く関連している、もしくは、明白であるとの確証を得たいと考えているようです。

４ 被害の軽減策

レッドエコーに関連した行動を見つけ、被害を軽減するために、①侵入監視・防止システムなどの防護メカニズムを利用して疑わしい不正ドメインとの接続行為をブロック、②フィルタリング機能を利用して侵入行為や疑わしい当局ドメインをブロック、③レコーデッド・フューチャー社の脅威情報モジュールなどの活用によりレッドエコーや「A」サーバーのような中国系の脅威グループによる侵入行為などを識別・分析しリアルタイム監視、④タイポスクワティングのようなドメイン悪用の監視などによる対策の強化を推奨しています。

５ 今後の見通し、展望

この調査で、インド電力機関に対して、２０２０年中旬以降、一連の疑わしい標的侵入が行われていたことが判明しました。　この侵入は、中国系の行動グループであるレッドエコーにより行われました。このグループは、シャドウパッドの指令サーバーを構成するインフラである「A」サーバーを集中的に使用していました。そして、このサーバーは、ＡＰＴ41、 トントチーム、アイスフォッグ・クラスター、キーボーイ、ティックといった中国の脅威活動グループの間で共有されています。

その侵入行為は、同様に「A」サーバーを使って２０２０年に中国の脅威活動グループにより行

われたインドのエネルギーインフラを標的としたものと同様の特性を表しています。
　したがって、インドの電力機関を標的とした狙いは、インドのエネルギーインフラへのアクセスという戦略的企図を有していると考えられます。ＲＬＤＣへのネットワークアクセスそのものは、スパイ活動を目標としたものとしてはそれほど大きな経済的利益は得られなかったようです。しかしながら、以下の様な成果を得るために、事前配置的に潜ませ、潜在的な手段として保持しておくという戦略的利益にはつながりました。
① 軍事的示威活動として強固なメッセージを伝える
② 外交的に対峙している時に、世論に揺さ振りをかけ得る行動となる
③ 重要なインフラへの将来的な破壊的サイバー行動を後押しする
　両国の緊張が高まり続けるならば、レッドエコーのような中国系グループが国家的な戦略利益と調和して行うサイバー作戦も増加し続けることになります。新型コロナウイルスのパンデミックを受け、それからの経済的回復は両国にとって優先事項であるため、このように国境問題での修辞的・動的なエスカレーションは、両国間に不信感や不確実性を高めていくことになります。さらに、中国が一帯一路（ＢＲＩ）投資プログラムで支援を続ける国々に対する影響力を行使し続けるであろうと思われます。このことは、さらなる戦略的利益を追求するサイバー作戦が増えていくだろうということを示しています。

６ インド・中国両国間の衝突激化の要因

　報告書によると、インド、中国という大きな人口を有する両国は、近年、敵対心を強め、経済的・地政的な野望を背景にその競争は激化し、２０２０年 5 月 5 日以来、両国は、その境界において小競り合いを続けてきました。これら両国の衝突激化の要因として 2 つの点を列挙しています。
　一つ目は、新型コロナウイルス感染拡大に対する国際的圧力を受け中国がより積極的になったこと、二つ目は、インドによるＬＡＣ沿いに延びる幹線道路の建設であるとしています。

（１）新型コロナウイルス感染拡大への対応

　一つ目の点については、２０１９年 12 月頃、中国武漢での肺炎の集団発生が起きているとのニュースが報じられ、２０２０年に入り中国での感染拡大、そして全世界に広がっていったわけであり、各国が感染拡大への対応としてロックダウンなどの措置を取る中で、その感染源である中国に対して厳しい目を向けていたのは確かであり、中国および中国国民はその圧力を重く受け止めていたと推察できます。外からの圧力をかわすための方策として、隣接国との国境問題への積極的姿勢というのは十分に妥当性があると考えます。

（２）幹線道路建設の影響

　二つ目の点については、インドはＬＡＣの情勢に対してより的確な対応を可能にすることを目的として、近接が可能で、年間を通して通行が確保できる幹線道路の建設を進めていました。　ラダックは、標高３０００ｍを越える高地に、地形険峻なため、アクセスに制限を受けているので、ダルバックーショック―ＤＢＯ（ＤＳＤＢＯ）幹線道路の建設は非常に重要です。
　ショック川沿いに延びるこの道路は従来から使用されてきましたが、河川沿いに通る従来の道路

は、雪解け水で水かさが増したことによりショック川が氾濫するため、夏季の 3 か月間は使うことができず、対応上の大きな問題であると認識されていました。そのため、氾濫時においても通行が確保できるように川からの高さを保つような新ルートの建設を進めており、２０１９年になって完成し、首都レーからの近接を含むＬＡＣへの部隊展開や後方連絡線の確保能力が向上しました。

一方で、中国側としては、ＤＳＤＢＯ幹線道路およびＤＢＯ近隣に建設された飛行場の整備は、シンチャン・ウイグル幹線道路および中国・パキスタン経済回廊（ＣＰＥＣ）に対する脅威であると主張し、迅速な対応が必要であるとの認識を持つようになりました。

シンチャン・ウイグル幹線道路については、中国としては非常に関心の高い 2 つの地域を結ぶ主要道路としてその価値を認識しているところですが、ラダック正面では、この道路からいくつもの道路がアクサイ・チンを横切ってＬＡＣに向かい整備されており、部隊展開や後方連絡線として活用されています。特に、デプサン高原へは良好な近接経路が整備されていて、機甲戦力の展開も可能であるとの分析もなされています。

また、中国としては、ＤＳＤＢＯ幹線道路がカラコルム峠やシンチャン・チベット幹線道路を越えてカラコルム幹線道路まで迫っているとの認識を示し、ひいてはＣＰＥＣへの脅威であるとの主張もされています。そのため、このインドによるＤＳＤＢＯ幹線道路建設をトリガーにアクサイ・チンやＬＡＣ沿いへの戦力展開を急進的に進めてきたとしています。このような国内的な交通路整備でさえも、中国は脅威と捉え対外活動の口実としてしまう現実を十分に留意する必要があります。

７ サイバー攻撃に関する分析

今般の中国によるサイバー攻撃が、ラダックの国境衝突事案に与えた影響を考察したいと思います。

中国の狙いは、インドが整備したＤＳＤＢＯ幹線道路の活用を制限することが目的のひとつであるので、その一つとしてガルワン渓谷での要点進出だったと考えられます。この場合、パトロール強化により仮設物建設を含めた中国軍の進出状況を把握する必要がありますが、２０２０年初頭から急激に増加したサイバー攻撃は、ちょうど新型コロナウイルスの感染拡大で混乱を来している中で、インド側の国内での状況把握や指揮連絡を大きく阻害することになったと考えられます。

また、エネルギーや港湾など政府の機関に対する大規模なサイバー攻撃は社会全体に影響を及ぼすことになり、戦略的な意味を成したものと思われます。また、戦術的に見ても、拠点での活動を妨害することとなり、動向の把握や前線における局地的な指揮連絡のみならず、中央との指揮連絡にも制約を加えることになったと考えられます。このことは、中国軍が、ＬＡＣよりインド側に進出していることを承知したる後の部隊進出や 6 月のガルワン渓谷での直接衝突に際しての先行的な対応に少なからず影響を与えたものと推察されます。

じ後の事態の収拾にあたっては、継続的なサイバー攻撃とともに、マルウエアの事前配置を匂わすことにより、以降の作戦に対する潜在的な脅威を認識させることとで、条件の有利化を狙っていたと考えられます。さらに、ムンバイにおいては実際に停電を起こし、社会生活に多大な影響を与えたことから、サイバー攻撃の有効性が深く認識されたものと思われます。

８ 結論

今般、インドと中国間の領域闘争にあたっては、新型コロナウイルス感染拡大における政府の対応や社会の混乱に乗じ、特に、中国によるサイバー攻撃がさらなる混乱を与え、作戦の有利化に繋げていった状況が露呈しました。このように、サイバー攻撃は複合的に指向することによりさらなる成果を期待することができます。また、その範囲も前線に限定することなく、広範な区域に拡大させることも可能であることから、その影響力を至当に認識する必要あります。

サイバー攻撃は、インドの例の通り、有事には至ってはいないグレーゾーンの段階からその規模を増大させ、条件の有利化を図り、領土拡張などの行動に結び付けているものであります。この場合、社会インフラへの攻撃やマルウエアの埋め込みなどによる潜在的脅威を継続によりその成果を確実なものとするように指向されています。

また、平時においても、香港の例のように、抗議行動への対策として、香港大学にサイバー攻撃を行い活動の無効化を図るような試みも行われています。

今般、我が国はサイバーセキュリティー戦略を改訂し、9 月に新設のデジタル庁が目指す「国民目線の利便性向上」とサイバーセキュリティーの両立の必要性を指摘するとともに、デジタル社会の実現に向け、サイバー空間の信頼性向上やセキュリティー対策に関する「環境づくりに努める」と明記しました。このように平時における対策は講じられつつありますが、南西諸島を中心に進出する中国の動きの中にあって、安全保障の観点から、その対処の中で、サイバー攻撃への対策を講じていく必要性が大きいということを指摘したいと思います。