# CYBER GRID JOURNAL

サイバー・グリッド・ジャーナル

VOL. 7

# 2020 大規模サイバー攻撃に備えよ

## 東京オリンピックに向けて

CYBER GRID JOURNAL VOL.7

TABLE OF CONTENTS

巻頭言

# 2020年 東京オリンピックに向けて 今できること！

佐藤 雅俊

サイバー・グリッド・ジャパン
ナショナルセキュリティ研究所長
初代サイバー防衛隊長
CISA（公認情報システム監査人）

サイバー空間は、インターネットの普及により今や全世界の55%の個人に利用されているといわれています。陸・海・空・宇宙の各システムは統合運用の必要性からサイバー空間で連接してデータを交換するようになり、多くのシステムがサイバー空間でつながる状態にあります。利便性が向上する反面、サイバー空間を利用した各種の攻撃は年々巧妙化し、多様化してきています。昨年策定された新たなサイバー戦略では、増大するサイバー脅威に対して、官民の情報共有やオリンピックに向けた態勢の強化等が示されていますが、実効性を高めるためには一歩先んじた対策が不可欠です。多くのシステムが連接され、ますます拡大するサイバー空間では、インシデントが発生すると瞬く間に拡散し、横に広がってしまいます。そうなると、マルウエアの種類や過去の事例に着眼した従来の手法による解析のみでは、広がりを食い止めることはできません。そこで必要になるのが、攻撃者の意図に関する分析です。これらの分析は、従来のテクニカルなアトリビューションと区別してポリティカル・アトリビューション（攻撃の背景分析）と呼ばれています。

昨年の平昌オリンピック（韓国）で発生したインシデントについて具体的な話をします。オリンピックの開会式直前に五輪組織委員会のインターネットがダウンし、予定していたドローンによる撮影が実施できなかったことは記憶に新しいと思いますが、このインシデントに際し、最初に分析結果を公表したのがセキュリティベンダーでした。複数のベンダーはテクニカル・アトリビューションにより、これらのインシデントは北朝鮮からの攻撃の疑いがある❶とレポートしましたが、その数週間後にアメリカの政府筋の話として、この攻撃は、北朝鮮からの攻撃を偽装したロシアからの攻撃であるという報道❷がなされました。後出しじゃんけんを食らったセキュリティベンダーは「十分な根拠を有さずにレポートを出すな。こん畜生！」と反論することになりますが、インシデントのファクトだけで攻撃元を特定するのは、材料として不十分だと感じます。

当時の情勢を分析すると、北朝鮮は米朝会談を前に融和ムードを演出していた時期であり、北朝鮮がオリンピックを妨害する合理的理由は少ないと考えられます。一方、ロシアについては、世界アンチドーピング機関がロシア選手のドーピングを国家的な行為と認定して、国としての出場を停止させていましたので、ロシアがオリンピックを妨害する理由は十分に考えられ、蓋然性が高いと思われます。攻撃に使用されたツール等を分析するテクニカルなアトリビューションは、点でしかありません。これらをつなぎ合わせて面にするのが、ポリティカル・アトリビューションだと考えます。

多くのシステムが連接し、拡大を続けるサイバー空間の中では、個々のインシデントを点で捉えるのではなく、面で捉えて全体を俯瞰することが重要だと考えます。1年後に東京オリンピックを控え、増大するサイバー攻撃の脅威に対しいかに備えるべきなのか。予想されるサイバー攻撃、サイバー戦の主要なアクターである中国のサイバー関連部隊の動向、そして新たな手法としての世論誘導について研究の一部を紹介したいと思います。皆さまにポリティカル・アトリビューションの必要性を感じていただければ幸いです。最後に、本誌編綴に当たり、防衛省防衛研究所の八塚正晃氏に中国のサイバー関連部隊等の動向について執筆いただきましたことを紹介するとともに感謝申し上げます。

❶ https://blog.talosintelligence.com/2018/02/group-123-goes-wild.html
❷ https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html?noredirect=on&utm_term=.1b56a21167af

# 2020
# 大規模サイバー攻撃に備えよ
## 東京オリンピックに向けて

佐藤 雅俊　サイバー・グリッド・ジャパン
ナショナルセキュリティ研究所長

## はじめに

表題を見て、ずいぶんとショッキングな言葉を使うもんだなぁと感じた方もいらっしゃると思います。我々日本人は、四方を海で囲まれ、過去に侵略された歴史がないことから、性善説で考える傾向にあります。それはそれで良い国民性なのですが、サイバー空間を利用するのは善良な人ばかりとは限りません。インターネット上では攻撃用ツールが研究目的を名目に公然と売買され、特別な知識のない組織や個人でもサイバー攻撃が可能な状況を生み出しています。当社セキュリティ監視センター「JSOC®」の観測範囲だけでも、1日当たり16億件もの不正な通信が世界各地から日本を目がけて飛んできていて、サイバー攻撃の脅威を肌で感じています。

そんな中、2020年に東京で開催されるオリンピックは、空前の訪日ブームと相まって、世界中から多くの人が集まり、メディアの注目も高いものと予想されます。純粋にオリンピックを楽しみたいという人がいる一方、オリンピックを悪用してやろうと虎視眈々と狙っている輩がいることを忘れてはいけません。過去のオリンピックにおいては、組織委員会の公式Webサイトがサイバー攻撃や金銭詐取のための偽サイトへの誘導に使われるなどの被害が報道されています。それでは、これらの攻撃から身を守るためにはどうしたらよいのでしょうか？　私は、危険を予見し、先回りした対策を取ることが必要だと感じています。

皆さまは、防犯のために自宅に鍵をかけていると思います。その上で、自宅の周りを不審者がうろついたらどうするでしょうか？きっと警察に通報したり、見回りを強化したりすると思います。サイバーセキュリティにおいても同様の対策が必要だと考えます。そこで、本稿では、2020東京オリンピックに向けてどのような攻撃が予見されるのか、また、どのような対策が必要なのか、所見を述べてみたいと思います。


## 過去のオリンピックにおけるサイバー攻撃の事例

古代ギリシャのオリンピアの祭典をもとに1896年に第１回の夏季オリンピックが開催されて以来、2020年に開催される東京オリンピックは夏季で第32回の大会となります。オリンピックの歴史を振り返ると、時代時代の情勢や各国の政治的な思惑により、オリンピックはその性格を変えてきたといえます。1968年のメキシコシティー大会では平和の祭典が黒人差別を訴える場と化し、1972年のミュンヘン大会ではパレスチナのゲリラがイスラエル選手を襲撃し、多数の犠牲者を出しました。また、1984年のロサンゼルス大会からは、オリンピックがスポンサー収益を増やすことをもくろむイベントとしての性質を強め、極度の商業主義やメダル争いに伴う競技者のプロ化が

進み、開催国の利権に絡む不正やドーピング等の問題も生起するようになりました。

オリンピックを狙ったサイバー攻撃については、2012年のロンドン大会以降に多数報道されるようになってきていますが、これらの攻撃は個々の大会の特徴や情勢に関連性が見られます。近年開催されたオリンピックにおけるサイバー攻撃の具体的な事例としては、ロンドン大会ではオリンピックの開催に反対する組織からの攻撃、リオデジャネイロ大会では、ロシアのドーピング問題をきっかけとした世界アンチドーピング機関への攻撃や開催地の脆弱なインターネットセキュリティ環境を狙った金銭目的の攻撃、さらに平昌大会においては、米朝会談を前にした政治的な世論誘導と思われる活動が報道されています。これらの攻撃と、それぞれのオリンピックの特徴は表１の通りです。

| 開催地 | 特　徴 | 攻撃事例 |
|---|---|---|
| ロンドン | 近代的で成熟した都市における洗練された大会を標榜しつつも利益を追求した商業的な傾向が強まり、オリンピック開催に反対する勢力からの反発が強まった。 | ○開会式がサイバー攻撃の標的に<br>○公式サイトに2週間で2億件以上のサイバー攻撃<br>○2週間で1万9000以上の悪意あるURLが立ち上がる |
| リオデジャネイロ | オリンピック施設建設の遅れに加え、脆弱なインターネット環境におけるホテルのセキュリティ対策の不備等が指摘された。ロシアのドーピング問題については、一部選手のドーピングが認定され、オリンピック参加が認められなかった。 | ○スポーツ仲裁裁判所へのサイバー攻撃<br>○世界アンチドーピング機関への不正アクセス<br>○政府やオリンピック関連企業に対するDDoS攻撃<br>○金銭目的のフィッシング詐欺 |
| 平昌 | 十分な予算が確保されず、オリンピック施設の建設が遅れたことに加え、大会運営環境も悪く、各国選手団からの不満も多かった。また、北朝鮮朝鮮労働党委員長と米国大統領の会談を前に、大会直前に北朝鮮と韓国の統一チームが編成されるなど政治色の濃い大会となった。ロシアのドーピング問題については国家の関与が認定され、国家としての参加が認められなかった。 | ○大会に関連する不審な文書ファイル付きメール<br>○イベントプログラムを偽装したマルウエア<br>○チケットの偽造　○世界アンチドーピング機関への攻撃<br>○開会式中のシステム障害<br>・メインプレスセンターでの映像視聴が中断<br>・公式Webサイトでの接続障害<br>・インターネットWi-Fi接続障害<br>・撮影で使われる予定のドローン飛行停止<br>○誹謗中傷<br>・大会参加選手<br>・日本 |

表1　サイバー攻撃の事例

# 日本を取り巻く情勢と2020年東京オリンピックの特徴

開催地の特性や国際情勢によりオリンピックを狙ったサイバー攻撃が異なることを述べましたが、それでは2020年の日本を取り巻く情勢や東京オリンピックの特徴はどうでしょうか？

## ① 日本を取り巻く情勢

2017年のトランプ大統領就任以来、米国で保護主義的な傾向が強まったことから、世界を巻き込む経済紛争が生起し、新規格の通信方式である5Gを巡る覇権争い等、米中の経済摩擦は先鋭化してきています。アジア地域における関係に目を向けると、2018年にトランプ大統領と北朝鮮の金正恩朝鮮労働党委員長との会談が実現し、北朝鮮の非核化や拉致問題の解決に向けた動きが期待されましたが、具体的な成果はいまだに見られていません。韓国との関係では徴用工を巡る問題や日本の哨戒機に対する射撃管制レーダーの照射問題、さらには、収束したはずの慰安婦問題にかかわる合意の破棄等、相互の信頼関係が疑われる深刻な状況にあると思われます。安全保障上の対立点である北方領土、尖閣諸島、竹島の帰属に関する問題は依然として外交上の懸念事項であり、中国・韓国・ロシアがそれぞれの思惑で行動する可能性があります。そして、公安調査庁が発表した資料によると、2018年の1月から8月までの期間に世界各地で発生したテロは50件を超えており、環境問題に関しては捕鯨に賛成する立場の日本に対する反捕鯨団体による不法な抗議活動が継続しています。

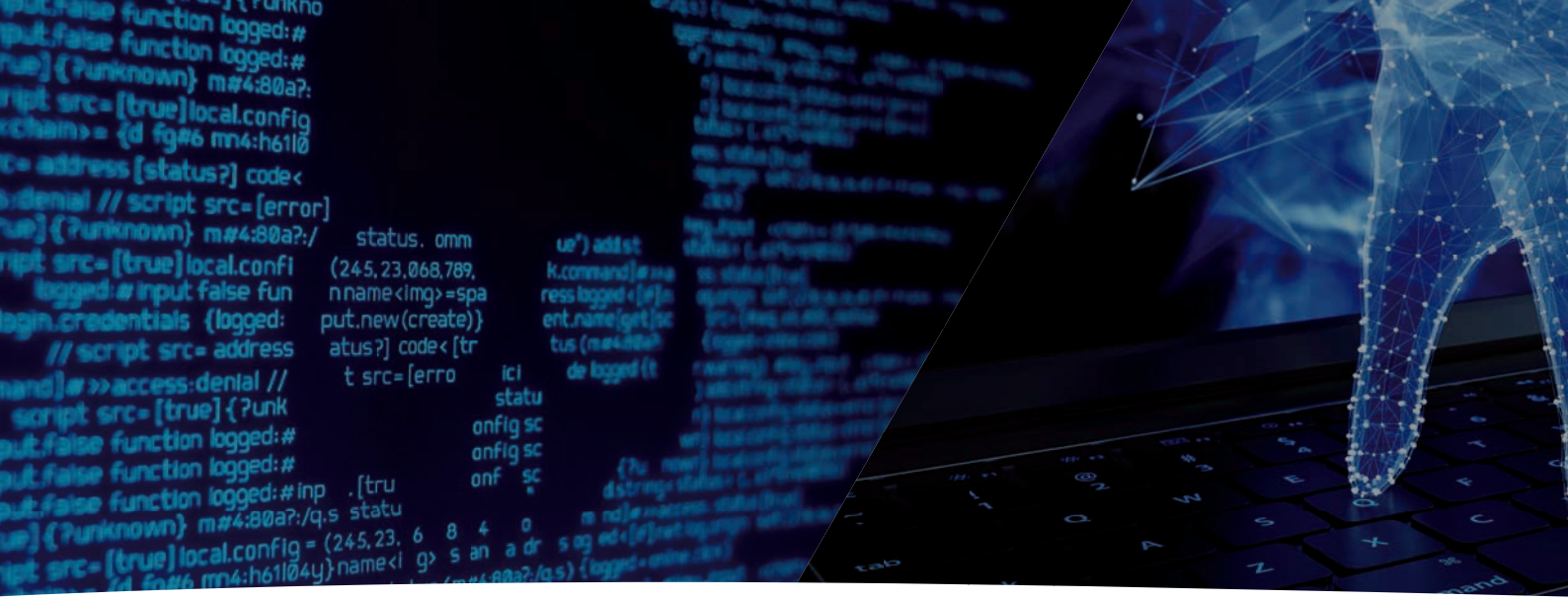
保護貿易を巡る懸念、安全保障上の対立、歴史問題にかかわる認識の相違、テロ活動、反捕鯨関連活動等、日本を取り巻く情勢は引き続き厳しく、警戒を続ける必要があります。

## ② 東京オリンピックの特徴

東京オリンピックの特徴を考えてみましょう。オリンピック組織委員会では、“スポーツには世界と未来を変える力がある。”をビジョンとして掲げ、①全員が自己ベスト②多様性と調和③未来への継承―の３つを基本コンセプトとして、史上最もイノベーティブで、世界にポジティブな改革をもたらす大会とすることを目標としています。[1] 大会会場は選手村を中心として2つのゾーンで構成され、大部分の競技はこのゾーン内で行われます。それ以外の競技は周辺の自治体で行われますが、野球やサッカーは東日本大震災からの復興をアピールするために、福島、宮城、茨城で行われます。これらを見ると、東京オリンピックは東京の優れたインフラや交通網といった都市機能を生かし、イノベーティブでダイナミックな大会を目指していること、そして東京以外でも一部の競技が行われることがわかります。

一方、オリンピックの商業主義化や競技者のプロ化の傾向は続くと予想され、金銭を狙った攻撃やオリンピック委員会やアンチドーピング組織に対する攻撃は継続されるものと考えられます。また、オリンピックが世界的に注目されるイベントであることから、組織をアピールする活動が数多く企画され、相反する組織との間で衝突する事態も発生する可能性があります。さらにオリンピックの開閉会式には世界各国の要人が参列し活発な外交が行われるのが通例であることから、活発な諜報活動が行われるものと予想します。

1 https://tokyo2020.org/jp/games/vision/



# 予想されるサイバー攻撃

敵の可能行動を見積もる軍事的な手法として情報見積というものがあります。情報見積では、味方の任務の遂行に影響を及ぼす敵の意図と能力を分析し、敵の可能行動及び採用公算の順位を明らかにするのですが、サイバー攻撃における能力や意図の分析では、サイバー空間の特性を踏まえる必要があります。サイバー攻撃には①多様性②匿名性③隠密性④攻撃側の優位性⑤抑止の困難性等の特性[2]があるといわれています。また、近年の兵器システムは従来のクローズされた環境から、サイバー空間を通じて連接しデータを交換する図１のようなクロスドメイン[3]の環境へと移行しています。

通常戦は物理的な破壊（ハードキル）を目的としているため、対峙する兵器の質や量、兵力

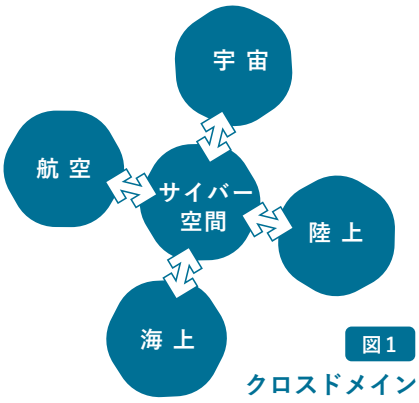



図1 クロスドメイン

の配備が戦局に重大な影響を与えます。一方、サイバー戦では情報通信ネットワークや情報システム等の悪用によって流れるデータを妨害、欺瞞、詐取する（ソフトキル）ことを目的とするため、世の中に出回っていないマルウエアの作成能力やシステムの脆弱性・組織の重心を探るインテリジェンスが能力分析の鍵となります。

次に、意図に関する分析ですが、国家が主体となる攻撃では、政治的な意思が攻撃のトリガーとなりますので、要人の発言や国家戦略から意図をある程度推察することが可能です。他方、組織や個人からの攻撃は、夜道に前触れもなく現れる辻斬りのようなもので、犯罪としての性格が強くなります。そこで使われる刀は最新のものではなく破壊力も小さいかもしれませんが、急所にはまるとシステム停止や大規模なインシデントを引き起こす懸念があります。これらの主体ごとに攻撃能力や意図、インテリジェンスの概要を整理すると表2の通りになります。

表2 主体別特性

| 主体 | 意図 | | 攻撃能力 | | インテリジェンス |
|---|---|---|---|---|---|
| 国家主体 | 国家による意思、政治的意図 | 要人発言や戦略等から推察 | 高い | 組織的な情報詐取や高度な攻撃ツールの開発が可能、制御系や重要システムの停止をもたらす可能性もある | 保有 |
| 犯罪組織 | 組織の意思 | 犯行声明、犯罪心理から推察 | 中程度 | 金銭詐取、サイトの改竄等には一般的な手法を用いるほか、一部のマルウェアについて亜種を作成し使用する可能性がある | 一般的には保有しないが、独自の情報網を保有する可能性 |
| 個人 | 個人の意思 | 犯罪心理から推察 | 低い | 金銭詐取、サイトの改竄等には一般的な手法が用いられる | 保有しない |

### ① 国家による政治的意図を持った攻撃

国家を背景としたサイバー攻撃は、サイバー攻撃単独というよりも、それ以外の諜報・調略活動等と並行して行われるものと考えられます。これらの活動で得られた情報は外交の一手段として実行されます。優れた人材と予算を使うことができるため、攻撃は巧妙かつ組織的です。

**I. アンチドーピング組織に対する妨害活動**

ロシアの選手が行ったドーピングに国家が関与したという世界アンチドーピング機構の認定を背景に、国際オリンピック委員会は、2018年の平昌オリンピックへのロシアの国としての参加を認めない決定をしました。この決定に対してロシアは不満を持っていることから、

2 平成24年9月、「防衛省・自衛隊によるサイバー空間の安定的・効果的な利用に向けて」
3 http://www.mod.go.jp/j/yosan/2019/setsumei.pdf

# 2020 大規模サイバー攻撃に備えよ

## 東京オリンピックに向けて

平昌オリンピックと同様の妨害活動は継続するものと予想されます。

### II.日本の地位向上に対する妨害活動

オリンピックは日本の技術力をアピールする絶好の機会であるとともに、オリンピックの成功は世界規模のイベントを履行しうる国として、組織運用能力や治安維持能力の評価を高めることに貢献します。しかしながら、地域のパワーバランスという観点から日本の地位向上を喜ばない国も存在し、これらの国からの妨害や反日活動が行われる可能性は排除できません。開会式等のセレモニーでお披露目される最先端の技術が失敗すれば、日本の技術力への期待を失墜させることになります。

### III.情報詐取のための活動

オリンピックは各国の首脳が集まる外交の場でもあります。この祭典期間中は多くの首脳級要人により世界的な問題や2国間の懸案等が話し合われます。多くの国がその内容に注目していて、中国、ロシア、米国等の主要な国は伝統的に、これらの情報を収集するための活動を行うものと考えられます。まさに情報戦の主戦場といえます。

### IV.領土・領海問題に起因する活動

日本が公式に発表している領土問題は、北方領土と竹島の間の問題です。表向きは尖閣諸島を巡る問題は存在しないという立場ですが、尖閣諸島周辺では、中国の領海侵犯等の実質的な紛争があります。世界中の記者が集まるオリンピックは、これらの国が自己の主張をアピールする好機であり、オリンピックに合わせて中国が尖閣諸島周辺への領海侵入を行い、マスメディアを利用して日中間の領土問題をアピールしようとする可能性があります。また、韓国による竹島の不法占領行動がエスカレートしたり、ロシアが北方領土付近での活動を活発化する可能性があります。

### V.歴史問題を悪用した世論誘導

中国、韓国、北朝鮮は機会あるたびに歴史問題を悪用したキャンペーンを行う等、オリンピック期間中にも仕掛けてくる可能性があります。

### VI.米中情報戦の激化に触発された活動

米中の経済摩擦を背景とした情報戦はますます激化し、米国の国防権限法の制定に伴い新通信規格である5Gや各国の政府調達から中国企業を排除する等の動きが加速しています。日本は日米同盟の重要性から米国の主張に沿って動くこととなりますが、中国の民兵や愛国者の一部が、中国製品排除に対抗して、中国以外の製品に対してピンポイントで攻撃を仕掛けてくる可能性は排除できません。

## ② 金銭目的の攻撃

### I.偽サイト等に誘導し、金銭を詐取するフィッシング攻撃

オリンピックに便乗する標的型攻撃は、最も効率的で汎用的なだましの手口であると考えられます。攻撃者がフィッシング等により銀行口座やクレジットカードの番号等を入手し、不正にログインして金銭を詐取するか代金を送金させておいて身をくらます手口です。「オリンピックの無料チケット提供」をうたう日本語の偽メールが複数送信され、メッセージから不正サイトに誘導する攻撃が確認されたとの報道[4]があることから、これらの攻撃はすでに始まっていると考えるべきです。

### II.宿泊客や訪日外国人等の個人情報詐取を狙った偽Wi-Fiスポットの設置

多くの訪日外国人は宿泊施設でインターネットを利用するものと考えられますが、大半のホテルでは設置が容易でコストが安いWi-Fiスポットを採用しています。ところが、Wi-Fiシステムの暗号強度はそれほど高くはありません。また、Wi-Fiは無線を使っていることから、スプーフィングといわれるなりすまし型の盗聴が簡単にできてしまいます。さらに偽のルーターを設置すれば、簡単にスポットを乗っ取ることも可能です。過去のオリンピックではWi-Fiを使った情報の詐取が多発したことから、米国等は自国民の渡航に際し、ホテルでのWi-Fi接続の危険性に注意喚起しています。[5]

## ③ ハクティビストによる主義主張のための攻撃

### I.オリンピック開催に反対する抗議活動

オリンピックは多額な予算が必要であることから、これらの予算執行に対して不満を持つ組織がオリンピック組織委員会等に対して反対活動を行う可能性があります。

### II.主義主張を拡散するためのメディアに対するハッキング

さまざまな主張を持つ組織が、メディアをハッキングまたは誘導して自己の主張を行う可能性があります。

### III.LGBTの理解促進活動に伴う衝突

東京オリンピックのコンセプトの一つに多様性と調和があり、LGBTに対する理解促進活動を進めている組織等では、東京オリンピックをLGBTに対する理解を広める好機と考えていると思われることから、これらの多様性に対して批判的な組織との衝突や妨害が発生する可能性があります。

### IV.反捕鯨活動

日本の捕鯨に反対する組織は、日本のIWC

4 http://www.security-next.com/097615
5 https://www.us-cert.gov/ncas/current-activity/2018/02/01/Pyeongchang-2018-Staying-Cyber-Safe-during-Olympics

脱退を受けて活動を活発化させる可能性があります。特にメディアの注目が高いオリンピックは彼らの活動をアピールする好機であり、これまで観測されているような「オペレーション・キリングベイ」といわれるDDoS攻撃に加えて、IWC脱退に関わった組織や捕鯨関係者、イルカ漁を行っている漁村等を直接狙ってくることも考えられます。

**④ テロ集団による勢力誇示と拡大のための攻撃**

テロ集団は無差別な殺りく行為により自己の勢力誇示を行う可能性があります。世界中から多くのメディアが集まるオリンピックはテロリストにとって絶好の見せ場であり、東京オリンピックでテロを行う可能性は排除できません。サイバー空間における活動としては情報収集やプロパガンダ、そしてWebサイト等へのハッキングが主なものと考えられますが、近年のIoTやドローン技術がテロに悪用される可能性もあります。

**I.地方のイベントを狙った攻撃**

開閉会式会場や要人の宿泊ホテル、そして競技会場周辺は全国から動員された警察官により厳重な警備が行われることと予想されますが、地方や周辺のイベント会場の警備は手薄になる恐れがあり、これらのイベントを狙ったテロが生起する可能性があります。

**II.交通システムを狙った攻撃**

公共交通網は都内いたるところに整備され、観客の移動や大会運営を支える要となります。これらのシステムはGPS等の位置情報を利用して列車の運行状況を把握し過密なトラフィックを正確にさばいていますが、優れた運行システムには単一障害点（その箇所が動作しないとシステム全体に障害が起きてしまうポイント）が複数存在することが知られています。都心から遠く離れた場所の信号機故障が路線全てに影響し、全体が遅延や運休となるケースはたびたび発生していますし、運行システムに古いOSがいまだに使われているケースも確認されています。

昨年の8月27日に発生したゲリラ豪雨では、鉄道が落雷に伴う停電のために運行を見合わせる事態に陥りましたが、この際、京王井の頭線渋谷駅の運行状況を表示するモニターにWindows2000のロゴが現れて話題になりました❻。クローズドなシステムである制御系システムであっても、インターネットに接続している事務用の端末や監視カメラ等のIoT機器を通じてマルウエアを仕込む事例もあることから警戒が必要です。

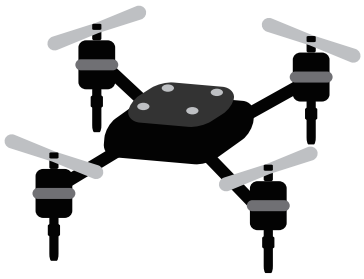
**III.電力システムを狙ったサイバー攻撃と大規模停電**

電力システムは、発電に関わるシステムや送電に関わるシステム等、複数のシステムで構成され、かつ電力の需給バランスの上に成り立っています。2018年に発生した北海道胆振東部地震の際にそのバランスが崩れて大規模な停電が発生したように、複雑なシステムには多くの障害点が存在します。電力システムそのものでなくても、関連するシステムを物理的、またはサイバー攻撃により制御不能にすることでこのバランスを崩すことが可能です。

2013年に発生した米国のダムシステムに対するサイバー攻撃では、ダムの水門を制御するシステムが攻撃を受け、攻撃者による制御が可能な状況にあったと報道❼されています。電力システムの停止は市民生活に多大な影響を与えることから、これらの攻撃に際しても運用の継続を求められます。バックアップ・システムの設置や運用等、国家レベルでの対応が不可欠だと考えます。

**IV.ドローンによる開閉会式の妨害**

開会式においてドローンの編隊飛行や空飛ぶ車がお披露目されるのではないかという噂はすでに広まっていますが、ドローンはほとんどの場合、遠隔地から無線でコントロールされています。この周波数を乗っ取れば、ドローンは簡単にハックすることが可能です。乗っ取らないまでも、命令伝達のための電波を妨害すればドローンはアンコントロール状態になり墜落するかもしれません。開閉会式でのドローンを使ったデモ展示の妨害に加え、南米ベネズエラで発生したようなドローン攻撃❽にも警戒が必要です。



今や攻撃兵器としても
利用されているドローン

## 大規模サイバー攻撃への備え

**① 100%安全なシステムなどありません**

（情報保証から任務保証の考え方へシフト）

Winnyに代表される、P2Pのファイル共有ソフトによる情報漏えいをきっかけに制度化された情報保証の考え方は、情報を漏えいさせないための対策が主眼で、漏えいした場合の罰則が厳しく規定されています。多くの官庁には、この原則に基づき、情報保証責任者の責務として情報を守ることが義務付けられています。

しかしながら、システムにはセキュリティホールが存在し、脆弱性も日々発見されています。そのため、大規模なサイバー攻撃に備えるためには、サイバー攻撃によるシステムの停止や、情報の漏えいを想定した対策が必要です。特に重要なインフラシステムについては、いかに任務を担保するかという任務保証の考え方へのシフトが不可欠です。

**② あなたの会社は24時間戦えますか？**

（SOP❾の承認と関係者への情報の共有）

多くの企業は、国の基準に基づき最高情報セキュリティ責任者（CISO）を配置していることと思われます。しかしながら、優秀な情報セキュリティ責任者の管理下であっても、サイバー空間は世界中とつながり多くの攻撃が日々襲ってきます。サイバー攻撃は情報セキュリティ担当者の勤務時間に合わせてはくれませんので、担当する部署は24時間での対応を迫られます。しかもインシデントはいつ発生するかわかりません。意思決定者と連絡が取れない場合もあります。このため、インシデント発生の都度意思決定者の指示を受けるのでは対応が間に合いません。それを解決するためには、必要な処置をマニュアル化し、事前に責任者の承認を得ておくことが有効だと考えます。

**③ 人材の育成は一朝一夕にはできません**

（適切なキャリアパスと人的資源の有効活用）

セキュリティ人材は2020年には19万人不足

⑥ https://www.excite.co.jp/News/it_g/20180829/Slashdot_18_08_29_0444227.html ⑦ https://www.cnn.co.jp/tech/35075354.html
⑧ https://www.bbc.com/japanese/45079899 ⑨ SOP：Standard operation procedure

# 2020 大規模サイバー攻撃に備えよ

## 東京オリンピックに向けて

するとのデータ⑩がありますが、これらの人材は一朝一夕には育成できません。現場で対処の責任者を任せるためには相当程度のセキュリティの知識と経験が必要です。当社でもある程度の仕事を任せられるようになるには、適性を含めて3年程度のOJT⑪が必要とされています。人材の育成には当然、時間とお金がかかります。この貴重な人材を有効に活用するためには、それらの技能を有する人材が適切に管理され、昇進するキャリアパスが必要になります。そうしないと、これらの人材は外資系の企業に高収入で引き抜かれることにつながります。

### ④ 訓練なくして実行なし

（想定外を不測事態へ）

インシデント発生後の記者会見で「想定外の事象で対応できなかった」との言い訳を聞きますが、インシデントは想定していないところに発生するのが常であり、これを言い訳にすることは危機管理を担当する部署として本質を理解していないと疑わざるを得ません。想定外の事象を不測事態として対応するためには、可能性をしらみつぶしに当たり、スタディする必要があります。より多くの訓練を行うことで、対処の幅が広がります。訓練なくして実行なし、想定外を不測事態として対処するための継続した訓練が不可欠です。

### ⑤ 情報モラルに関する啓発活動

（「不正を正当化」させない教育）

「不正のトライアングル」という理論を聞いたことのある方も多いと思います。この理論は米国の犯罪学者であるD.R.クレッシー（1919-1987）が実際の犯罪者を調査して人が不正行為を実施する仕組みに導き出した理論⑫で、人が不正を行うのは「機会」「動機」「正当化」の不正リスクが全て揃ったときだというものです。「機会」とは不正行為を実行する客観的環境、「動機」とは不正行為を実行しようとする主観的事情、「正当化」とは不正行為の実行を是認しようとする主観的事情のことです。つまり、この3要素のうちの1つでも無くすことができれば、不正は起こらないことになります。客観的な環境である「機会」はインターネットが存在する限り無くすことはできませんが、主観的事情である「動機」と「正当化」は無くすことは可能です。そのための有効な手段の一つが情報モラルに関する教育になります。

2017年6月に中学生がインターネット上の情報をもとに身代金要求型のマルウエアを作成したとして逮捕されたこと⑬は世間を驚かせましたが、インターネットを通じた活動はリアルな現実と乖離しているために罪を犯しているという意識がなかったり、身元を特定されるとは考えずに悪事や危険な行為を行ったりしてしまうケースが散見されます。将来の日本を担う若者たちがトラブルに巻き込まれないように、情報モラルに関する啓発活動は不可欠です。


## おわりに

自衛隊のブルーインパルスが大空に五輪の輪を描いた1964年東京オリンピックから55年が経過し、高度経済成長を経た東京はロンドン、ニューヨークに次ぐ世界第3位の成熟した都市⑭といわれています。お台場や東京スカイツリー、そして浅草といった名所には多くの外国人が訪れにぎわっています。発達した公共交通システムや美しいビルの風景、そして昔ながらの日本の文化とのコントラストには絶妙な趣があり、お台場のテラスでレインボーブリッジを見ながら食事を取ると、都会にいながらにしてリゾートでくつろいでいるような錯覚に陥ります。その風景に浸りながら、日本に生まれてよかったとつくづく感じています。

2020年には、いよいよ待望のオリンピックが東京や被災地を含む各地で開催されます。多くの日本人は期待に胸を膨らませ、待ち遠しく感じていると思います。この大切なイベントを、サイバー空間を悪用する攻撃者の思うがままにさせるわけにはいきません。オリンピックを通じて、日本の良き伝統が若い人たちに引き継がれ、感動が思い出として残るように、我々にはなすべきことを実行する義務があります。安全は与えられるものではなく、自らが獲得すべき事項です。我々には、主体的な取り組みが求められています。

⑩ http://www.meti.go.jp/press/2016/06/20160610002/20160610002.html　⑪ On the job training　⑫ https://www.d-quest.co.jp/internalcontrol/fraud_triangle/
⑬ https://japan.cnet.com/article/35102749/　⑭ http://mori-m-foundation.or.jp/ius/gpci/index.shtml

# サイバーセキュリティと中国の情報化戦争

八塚 正晃
防衛省 防衛研究所 地域研究部
中国研究室　教官・研究員

※本稿における見解は、所属機関を代表するものではありません

## 1. はじめに

中国は、今や世界最大の情報化社会を抱える国家といえます。中国の公式データである『中国インターネット発展状況統計報告2018』によれば、中国のインターネットユーザーの数は8億人（普及率約58%）を超え、昨年の中国におけるインターネット小売売上高は4兆人民元（日本円で約65兆円）に達しています[1]。習近平国家主席は就任以来、政治、経済、文化、社会、軍事の各領域で情報化の推進やサイバーセキュリティに注力しており、中国を「サイバー強国」にすることを国家目標に掲げています。また、中国政府は、インターネット、ビッグデータ、人工知能（AI）等の情報化を今後の経済発展のための重要なエンジンと位置付けています[2]。2017年6月には、サイバーセキュリティ法を施行したことも注目を集めました。

2019年にG20やラグビーワールドカップ、2020年に東京オリンピック・パラリンピックなどの大きな国際イベントを主催する日本にとっても、中国のサイバーセキュリティの動向は大きな関心事です。そこで、本稿では、中国のサイバーセキュリティに対する取り組みを主に軍事面から紹介します。サイバーセキュリティに注力する中国政府の背景として情報化社会と中国共産党の微妙な関係を解説した上で、中国軍が将来の戦争の形態として対応を進める情報化戦争という概念を読み解き、中国軍のサイバー戦の在り方とその作戦を担う組織の動向を中心に紹介したいと思います。

## 2. 情報化社会と中国共産党体制の微妙な関係

情報化社会の進展は、中国の執政党である中国共産党にとって、歓迎するものである一方で、警戒するべき事象でもあります。中国共産党政権にとっての最重要課題は、自らの安定的な統治と発展です。こうした観点から、①中国共産党の独裁体制と相いれない思想や価値の中国社会への浸透②中国共産党の統治に不満を持つ国内の政治勢力の糾合③中国経済の不安定化を招く投機的な金融投資活動や経済犯罪――に対して、中国共産党指導部は警戒しています。情報化社会の進展は、こうした個々の不安材料をサイバー空間を介して瞬時につなぎ合わせることで中国共産党の統治を揺るがす大きな圧力を生み出しかねません。こうした理由から、中国政府は情報化社会の進展を警戒し、サイバーセキュリティに注力しています。

しかし、中国共産党にとって悩ましいのは、サイバー空間に対する規制を強化すれば体制が安定するという単純な話でないことです。たしかに、情報の規制を強化すれば、経済犯罪や中国共産党独裁体制に対して不満を持つ勢力の取り締まりは容易になるでしょう。ただし、サービス産業・消費主導の経済構造に移行を目指す中国では、こうした情報化社会の大勢を拒否することは、中国の安定的な経済発展を阻害する可能性があります。

1 中国互聯網絡信息中心『中国互聯網絡発展状況報告』（2018年7月）
2 中共中央網絡安全和信息化委員会弁公室「発揮大数据経済発展的駆動作用」2018年12月4日（http://www.cac.gov.cn/2018-12/04/c_1123803079.htm）

サイバー空間に関する規制を強化すれば、情報技術のイノベーションの源泉である市民の自由な発想を圧迫してしまうからです。

したがって、情報化が社会に浸透する中で中国共産党の一党独裁体制を維持するためには、サイバーセキュリティに関する統治と発展の間の微妙な関係をうまく管理しなければいけないのです。つまり、中国共産党に求められているのは、サイバー空間の効果的活用と党の統治能力の維持・強化を両立するサイバー空間のガバナンスです。中国政府のサイバーセキュリティに関する取り組みは、その適切なガバナンスの模索に他なりません[3]。

国際関係の観点から、中国政府、なかんずく中国共産党政権のサイバー空間のガバナンスに大きな影響を与えうるのは、外国からのサイバー空間を介した内政干渉や外国軍からのサイバー攻撃です。こうした観点から、中国共産党の軍である人民解放軍は、サイバー戦を含む情報化戦争への対応を急速に進めています。以下では、この情報化戦争という概念を説明します。

## 3. 中国軍の情報化戦争の概念

中国政府は、2015年の国防白書（中国の軍事戦略）において、「世界の新軍事革命が発展し、戦争形態は情報化戦争への変化を加速している」との認識を示し、中国軍が将来の戦争形態と考える情報化戦争への対応を急速に進めています。情報化戦争とは、中国軍によれば「ネットワーク化された情報システムに基づき、情報化された武器装備及び関連する作戦方法を利用し、陸・海・空・宇宙・サイバー・電磁等の空間及び認知領域において、システム対抗を主な形式として進む戦争」と定義されます[4]。この定義はやや難解なので、以下でいくつかの特徴を手掛かりに解読しましょう。

情報化戦争の第一の特徴は、戦争における情報の役割を極めて重視することにあります。現代の軍は、その指揮命令系統や武器装備がサイバー空間を介して高度にネットワーク化され、これが統合的なシステムを構成しているため、現代の戦争においては、情報が全領域・作戦行動に影響を与え、戦争の結果を左右します。情報の支配が死活的に重要なのです。情報化戦争においては、相手の作戦・情報システムの急所に対して正確な攻撃を行うことがとても重要です。当然ながら、相手も同様の作戦を取ります。つまり、情報化戦争は、自軍のシステムと相手軍のシステムの戦いであり、中国軍はこれを「システム対抗」と呼んでいます。

情報化戦争の第二の特徴は、戦争コストの抑制です。改革開放以降、中国共産党は、持続的な経済発展を自らの統治の正当性にしています。ところが、現代の戦争は、戦争を実施するコストが上昇しており、ひとたび戦争が勃発すれば、社会や国民を巻き込み、自国の経済を犠牲にするため、共産党統治にとって致命的な損失を生起しかねません。したがって、他国との戦争が発生したとしても、経済への波及を回避することが鍵となります。すなわち、情報化戦争で重視されるのは、戦争の局地化とエスカレーション管理です。そのために、サイバー空間を利用した相手国に対する情報戦、国際社会への戦略的な情報発信などを通じて、戦争の戦線拡大、長期化、国際化を回避することを目指します。情報化戦争とは、中国共産党統治の持続の観点から発想されている概念なのです。

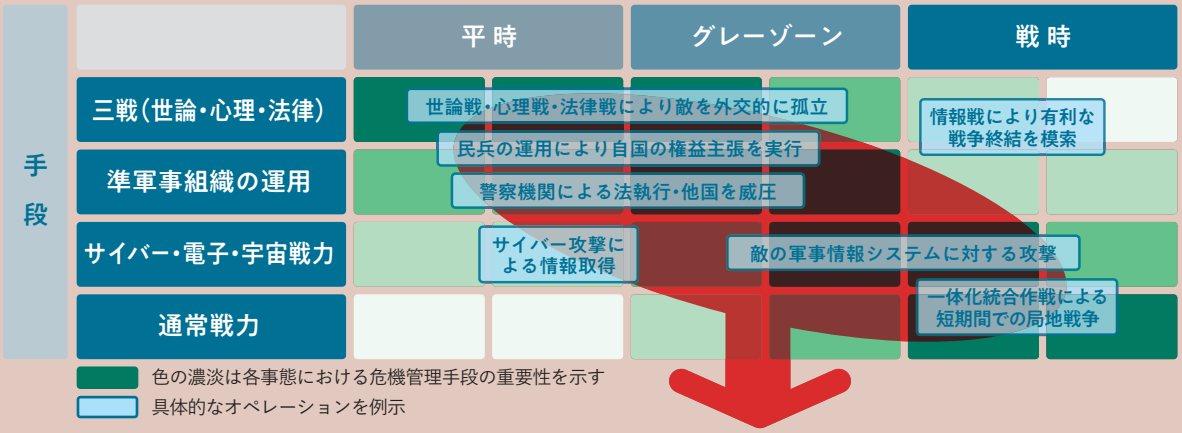
情報化戦争の第三の特徴は領域横断的であり、とりわけ新たな戦略領域が重視されることです。中国軍は、

3 中国のサイバーセキュリティに関するガバナンスの模索については、拙論「中国のサイバー安全保障政策と日本への影響」『東亜』2018年1月号をご参照ください

4 『中国人民解放軍軍語（全本）』（軍事科学出版社、2011年）、48頁

# サイバーセキュリティと中国の情報化戦争

**図1　情報化局地戦争の概念図** ※1




**中国軍が将来戦で想定する情報化局地戦争の範囲**

※1『戦略学2013年版』等を参考に筆者作成

図1の通り、平時とも戦時ともつかないグレーゾーンを含めて平時から戦時まであらゆる段階において、陸海空等の通常戦力と準軍事組織、さらには宇宙・サイバー・電磁等の新たな戦略領域を一体的に組み合わせながら運用する「一体化統合作戦」の実施を目指しています。他方で、情報化戦争においては、先述のように、相手のネットワーク化された情報システムを瓦解させるために戦争の主導権を奪取することが重要です。この主導権をめぐる闘争は戦争の準備期間から始まります。準備段階においては、戦争のエスカレーションを招く通常戦力に比べ、宇宙・サイバー・電磁等の空間及び認知領域等の新たな戦力を利用したオペレーションが大きな役割を果たします。

以上でも分かるように、中国の情報化戦争においては、どの局面においても、サイバー空間のオペレーションは極めて重要な位置づけにあります。それでは、中国軍はサイバー戦をどのように考えているのか、次に見てみましょう。

## 4. 中国のサイバー戦

サイバー戦は、中国軍によれば、「情報戦」の一部とされます。情報戦とは、広義には、敵対する双方が政治、経済、科学技術、外交、文化、軍事などの領域において、情報技術を利用して進める主導権をめぐる争いのことを指し、狭義には、軍事行動における情報の優位を確立するための情報対抗と定義されます[5]。その中において、サイバー戦は、サイバー空間の中で、攻撃においては相手のサイバーシステム等を破壊・弱体化させ、防御においては自身のサイバーシステムやサイバー情報を保護することを指します[6]。

より具体的には、中国軍のサイバー領域における作戦は、①サイバー空間を介した偵察行動②サイバー攻撃・防御作戦③サイバー能力を部分的に開示することによる抑止行動――の3つに分けられます（図2）[7]。中国軍の理解によれば、これら3つの作戦を状況に応じて組み

5 葉征『信息化作戦概論』（軍事科学出版社、2007年）、第6頁　6 『中国人民解放軍軍語（全本）』（軍事科学出版社、2011年）、286頁
7 軍事科学院軍事戦略研究部『戦略学（2013年版）』（軍事科学出版社、2013年）192-193頁

合わせながら実施することで、自国に有利な環境で情報戦を進めることができるとされます。

なお、サイバーに隣接した領域として、電子戦があります。これも情報戦の一つですが、主に、電磁エネルギー、指向性エネルギー、音響エネルギーなどの電磁スペクトラムの手段を利用して、相手の情報設備、情報システムや関連する装備を物理的に攻撃し、弱体化・破壊することを指します[8]。中国軍の場合、両者を作戦の中で有機的に結びつけて実施します。これを「網電一体戦（サイバー・電子一体戦）」と呼びます[9]。すなわち、情報に対してサイバー攻撃をする「ソフトキル」と、情報設備そのものに対して物理的に電磁攻撃をしかける「ハードキル」を合わせて実施する攻撃が想定されます。

**図2　中国のサイバー戦の種類と方法**※2

**サイバー偵察**
- 相手のサイバーのパスワードを解読
- 有線、無線、電磁ルートを通じたアクセス
- 相手システムのバグを利用した潜入

**サイバー攻撃・防御作戦**
- 情報に対して攻撃を行うソフトキル
- 電磁手段を用いたハードキル

**サイバー抑止**
- 平時における能力誇示
- シミュレーションや演習の実施
- 高度な演習の実施
- 限定的な攻撃的オペレーションの実施

※2 Dean Cheng, Cyber Dragon: Inside China's Information Warfare and Cyber Operations, Santa Barbara: Praeger, 2016等を参考に筆者作成

## 5. サイバー戦を担う組織

中国は習近平政権で進めている大規模な軍改革の一環で2015年末に人民解放軍に新たな軍種を設けました。その新軍種こそ「戦略支援部隊」であり、宇宙・サイバー・電磁の領域を担い、中国軍の「情報戦」の中核となる組織です。これら3つの領域を跨いで主管する軍種は世界でも例はなく、大きな注目を集めています。

中国軍の透明性は他国と比べて極めて低いうえに、現在も大規模な軍改革が続いているため、戦略支援部隊がどの程度の規模であり、いかなる組織構造を持っているのかは公式に明らかにされていません。これまでさまざまな分析がされていますが、軍改革前に総参謀部や中央軍事委員会等に散らばって情報戦を担っていた各組織を再編して戦略支援部隊を創設したと見られています。また、サイバーセキュリティを担う人材の教育・確保が難しいともいわれており、同部隊の体制整備が完了するまで相当な時間がかかると見られます。

なお、今回の軍改革において、陸、海、空、ロケット軍、戦略支援部隊等の各軍種は主に軍隊建設を担い、東西南北中の5つに分けられた各戦区は主に軍事作戦を担うという整理がなされました。したがって、軍種である戦略支援部隊は、サイバー、電子、宇宙空間における作戦を担う人材の育成、軍事能力の向上に従事し、作戦時に各戦区に情報戦に従事する人員や部隊を提供するフォース・プロバイダーとしての役割を担うと考えられます。

また留意すべきこととして、情報化戦争においては戦争準備の段階から情報戦が実行されうると先述しましたが、中国軍の中でこの作戦を担うのは戦略支援部隊だと推測されます。すなわち、同部隊は、平時における

8 『中国人民解放軍軍語（全本）』（軍事科学出版社、2011年）、第263頁
9 葉征『信息化作戦概論』（軍事科学出版社、2007年）、28頁

# サイバーセキュリティと中国の情報化戦争


PROFILE

**八塚 正晃（やつづか・まさあき）**

1985年生まれ。2008年慶應義塾大学総合政策学部卒。慶應義塾大学法学研究科後期博士課程単位取得退学。日本学術振興会特別研究員（DC1）、香港総領事館専門調査員、外務省国際情報統括官組織専門分析員などを経て、2016年から現職。その間、北京大学留学（2009-2010年）。専門は、中国政治外交（史）、東アジア国際関係論、国際安全保障論。


「三戦（世論戦・心理戦・法律戦）」にもなんらかの役割を担う可能性があります。ただし、平時における情報戦については、中国共産党の中央宣伝部傘下の党メディア、国家安全部、公安部などの国家の情報機関が存在しているので、これらの組織とどのように役割分担をするのかは定かではありません。

また、同様の観点から、サイバー民兵にも注意する必要があります。中国では、各地の地方政府の中に、市民を動員して民兵を組織する部署（人民武装部）があり、この中にサイバー作戦を担当するサイバー民兵部隊（中国語では「サイバー作戦分隊」ないし「ネットワーク作戦分隊」と記述）が存在します。こうしたサイバー民兵は、サイバー技術専門教育機関の教師、研究機関の専門家、情報技術を学ぶ大学院生等によって構成されるようです[10]。彼らは、戦時には軍の指揮下に入り、相手国に対するハッカー攻撃、電波妨害、ウイルス攻撃、サイバー偵察、宣伝工作等に従事し、自らが所属する組織の情報システムの保護・管理・復旧等の任務を負います[11]。なお、サイバー民兵は、平時において諜報活動に従事する明確な証拠はありませんが、中国の民間の情報技術企業に情報戦に携わるサイバー民兵の人材が在籍している可能性は考えられます[12]。

## 6. おわりに

以上で見たように、中国のサイバーセキュリティに係る取り組みは、急速な展開を見せています。日本政府は、こうした中国の取り組みを含む国際的なサイバーセキュリティ環境の複雑化を受けて、積極的にサイバーセキュリティに係る施策を進めています。

本稿における情報化戦争の解読からも分かるように、中国軍は平時から戦時にかけてシームレスに情報戦を実施する体制の構築を図っているため、日本もそれに対応したオールジャパンのサイバーセキュリティを講じることが求められます。平時における情報戦への不備は、戦時の脆弱性に直結します。情報戦の対象には政府部門だけでなくメディアや重要インフラ管理業者など民間企業も含まれると考えられ、また、情報関連機器の導入・運用の過程でマルウエアやバックドアが埋め込まれる可能性もなしとしません。政府・民間を問わず情報インフラ施設の防護強化、サイバー攻撃を受けた際の代替設備・施設の確保、サプライチェーンのスクリーニング等を通じてレジリエンスを高めることが求められます。

サイバー攻撃は、攻撃側に圧倒的に有利なために先制攻撃への誘因が強くなります。また、脆弱な部分から狙われるため、中央だけでなく地方自治体や地方の自衛隊基地においても、サイバーセキュリティに係る情報共有や関連研修の実施、設備導入を通じたサイバー防衛能力の底上げが重要となります。こうした施策はサイバー攻撃を無力化する拒否的抑止といえます。

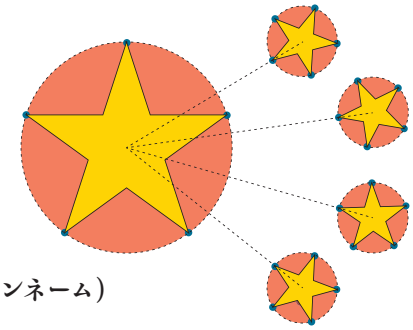
また、拒否的抑止能力に加えて、サイバー攻撃の発信源を特定するアトリビューション能力を高めつつ、報復能力を示すことで相手に攻撃を思い留まらせる懲罰的抑止能力の保有も議論することは、日本のサイバーセキュリティを充実させることにつながります。この観点からも、防衛省が2018年12月に改訂した「防衛計画の大綱（防衛大綱）」において、サイバー、宇宙、電磁波に力点を置き領域横断作戦の実現を目指し、「相手方によるサイバー空間の利用を妨げる能力等」の抜本的強化を図ることが明記されたことは、日本のサイバー抑止能力の向上につながると期待されます。

10 張志倫「軍分区如何精編訓網絡戦民兵分隊」『西南民兵』（2007年10月5日）

11 李国強・陳偉・呉愛軍「民兵網絡戦分隊的任務、建設与運用」『国防』（2006年第8期）、40頁

12 Robert Sheldon and Joe Mcreynolds, “Civil-Military Integration and Cybersecurity,” China and Cybersecurity, Oxford University Press: Oxford, 2015, p.190.

# 中国による サイバー心理戦



サイバー・グリッド・ジャパン　長田 真知（ペンネーム）

## 不戦而屈人之兵（戦わずに人の兵を屈服させる）

これは、紀元前500年頃に軍事思想家の孫武が説いたとされる「孫子の兵法」❶の一節で、この考え方を政策に組み込んだものが中国の「三戦」です。三戦とは、世論戦、心理戦、法律戦の3つを指します。本稿では、三戦の中でもっとも長い歴史を持つ心理戦に焦点をあて、その歴史的発展経緯とサイバー空間へと拡大したサイバー心理戦について述べます。

## 中国の三戦

三戦は、2003年12月、中国人民解放軍の法規である「中国人民解放軍政治工作条例（政工条例）」に初めて明記されました❷。人民解放軍はこの三戦を実施することで、敵国の組織を崩壊させ、敵国による心理的な攻撃に対抗し、法律に関する工作を展開することが規定されています。人民解放軍は、これら三戦を組み合わせて互いに補い、根拠を与えながら目標の達成を目指します❸ 図1。


図1　中国の三戦

このうち、心理戦は人民解放軍の軍事用語辞典である「中国人民解放軍軍語」において、以下のように定義されています❹。

> 戦略意図と作戦任務に基づき、政治、軍事闘争の目的を実現するために、特定の情報やメディアを運用し、目的対象の心理及び行動に対し影響を与える作戦行動。

この定義に基づき、人民解放軍は国外向けの攻勢心理戦 表1 と国内向けの防勢心理戦を展開するとされています。

| 種　類 | 例 |
|---|---|
| 威嚇・恫喝 | 日本の領海や領空識別圏への侵入、経済的制裁、歴史問題 |
| 懐柔・暗黙 | 経済的支援、動物のレンタル、他国報道に乗じた情報公開 |
| 誇　示 | 軍事パレードの開催、先進軍事技術の公開、領有権の主張 |
| 欺瞞・離間 | 日本政府と国民の対立を煽動、日本が国際的に孤立するよう宣伝・支援 |
| 教育・醸成 | 親中派・国際的支持者の獲得、中華思想や歴史観の普及 |

表1　攻勢心理戦の事例


❶ 金谷治（2001）『孫子』岩波書店
❷ 土屋貴裕（2013）「中国の軍制と工作条例の変遷：政治と財務の視点から」,『問題と研究：アジア太平洋研究専門誌』42(3), p.115-148, 国立政治大学国際関係研究センター
❸ 航空自衛隊幹部学校戦略研究グループ（2016）「中国による三戦の定義等およびエア・パワーに関する三戦の事例」,『エア・パワー研究第2号』, p.113-124
❹ 『中国人民解放軍軍語（全本）』（2011）軍事科学出版社

例えば、中国は1992年に公布した国内法である「中華人民共和国領海及び接続水域法（領海法）」に、尖閣諸島が中国の領土であることを明記しました（法律戦）。中国は、これをメディアで公言し、尖閣諸島が係争地であることを国内外に印象付けました（世論戦）。そして、それを証明するため、尖閣諸島の接続水域では中国公船が定期的に航海しています（心理戦）。では、このような心理戦は一体いつから行われていたのか？　その歴史的な発展経緯について掘り下げていきます。

## 心理戦の歴史

中国における心理戦の歴史は長く、その最たるものが冒頭で紹介した「孫子の兵法」です。中国共産党で敵軍工作の指導をしていた毛沢東も愛読者の一人であり、著書『持久戦論』において、「戦争における決定的な要因は武器ではなく人である」と主張しました。

1927年、毛沢東指導下の中国共産党では当時対立していた国民党対策として、敵は国民党の指導者であり兵士として駆り出された貧しい民衆ではないとする対敵2分法を提唱しました❺。この対敵2分法を日本に対して実戦的に応用したのが、1937年の日中戦争です。毛沢東は、日本人を日本軍国主義者と日本人民に分け、日本人民を抗日勢力に取り込むことで日本人同士の対立を狙いました。この工作のために組織された国民革命軍第八路軍は、精神的に敵軍民の戦闘意思を瓦解させることを目的に、対日プロパガンダを行いました。つまり、1930年代には対日本心理戦の土壌ができていたのです。

## サイバー空間への拡大

心理戦をより効率良く展開する方法として、中国はサイバー空間に注目しました。そのきっかけは、1991年湾岸戦争における米軍のハイテク利用による武力戦・宣伝戦でした。当時、人民解放軍所属の喬良と王湘穂は、1999年の著書『超限戦』において、これからは武力戦だけではなく、貿易戦、金融戦、新テロ戦、生態戦、心理戦、密輸戦、メディア戦、麻薬戦、ハッカー戦、技術戦、仮想戦、資源戦、経済援助戦、文化戦、国際法戦といった戦法を組み合わせ、同一時間帯に異なる空間で行動を展開することにより、あらゆる場所が戦場になると考察しました❻。

2000年の全軍心理戦研究会ではハイテクの利用により戦わずして勝つことが可能になったことが強調され、2002年石家荘陸軍指揮学院で開催された勉強会にて、ITを利用し平時から心理戦を展開することが提唱されました❼。中央指導部は国家の「情報化」を推進するとし、情報化条件下の局地戦に勝利し得る軍隊を創設するよう人民解放軍へ指示しました❽。中国は、有事における情報優勢を確立するため❾、平時からの情報収集と情報操作に取り組んでいるのです 図2 。

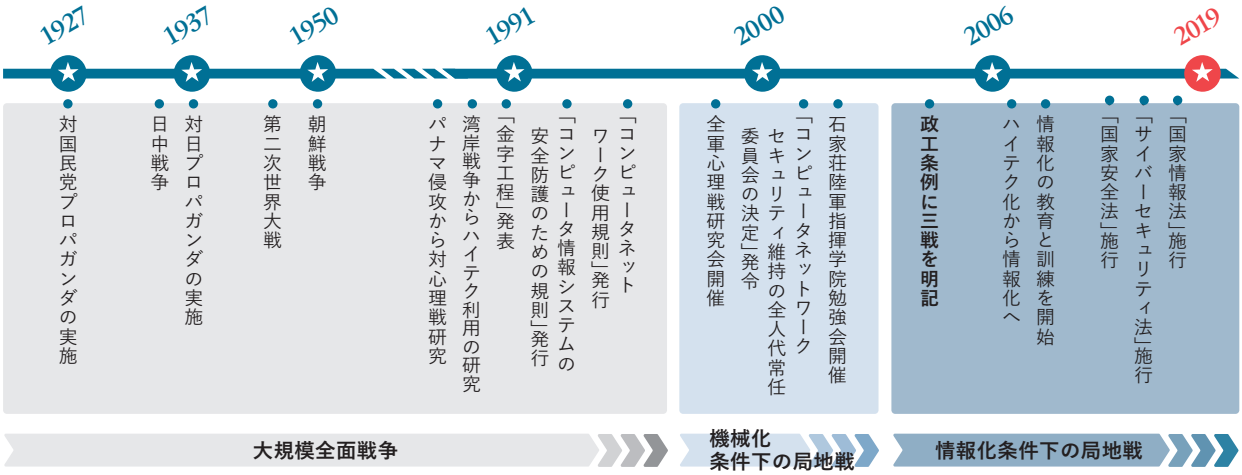



図2 心理戦とサイバー関連政策の抜粋

❺ 趙新利（2010）『日中戦争期における中国共産党の対日プロパガンダ戦術・戦略-日本兵捕虜対応に見る「2分法」の意味-』早稲田大学出版部
❻ 喬良著・王湘穂著（2001）『超限戦』坂井臣之助監修，劉琦訳，共同通信社
❼ 齊藤良（2010）「中国の三戦（輿論戦、心理戦、法律戦）と台湾の反三戦」，『陸戦研究』58(681)，p.23-54，九段社
❽ ジョー・マクレイノルズ（2017）『中国の進化する軍事戦略』五味睦佳ほか訳，原書房
❾ ディーン・チェン（2018）『中国の情報化戦争：情報心理戦からサイバー戦、宇宙戦まで』五味睦佳ほか訳，原書房

# サイバー心理戦（威嚇→情報窃取→世論誘導）

サイバー空間における心理戦は、人へ心理的操作を試みる直接的なものと、コンピューターへの攻撃を通して心理的効果を生み出す間接的なものがあります。本稿では、サイバー攻撃と、それに付随して展開される直接的・間接的心理戦 表2 について考察していきます。

| 手　法 | | 目的と心理的作用 |
|---|---|---|
| 威嚇・妨害 | DDoS攻撃、機能停止 | ・標的国の目的遂行を妨げる<br>・標的国内のインフラを制御不能にさせ孤立させる<br>・かく乱している間に異なる目的を達成する |
| | Webページ等の改ざん | ・標的国の政策の誤りや違法性を誇示する |
| 情報窃取 | APT攻撃 | ・標的を心理誘導して機密情報を窃取する |
| | サーバーや機器の乗っ取り | ・機密情報を窃取し、悪用することで加害者にする |
| 世論誘導 | プロパガンダ | ・標的国内における味方の醸成と対立の促進<br>・標的国の国際的孤立を促進 |
| | フェイクニュース | ・偽情報によるかく乱 |
| | 非公開情報の暴露 | ・標的国の国際的な評価を下げる |
| | 公開情報の威力的変更 | ・国際上の黙認を確立し、政策を有利に進める |

表2 サイバー攻撃と心理的作用の例

## (1) 威嚇

中国発のサイバー攻撃が初めて報じられたのは、1999年5月コソボ紛争におけるNATO軍中国大使館誤爆事件です。中国ではNATO軍の誤爆は故意であったとの見方があり、中国人ハッカー集団が米国政府のWebサイトを改ざんしました⑩。その翌年、2000年1月には日本の中央官庁や外郭団体のWebページが改ざんされる事件が起こりました⑪。これは、中国外務省の抗議を聞き入れず強行開催された大阪のイベントへの報復とする見方があります。

このように、初期の中国によるサイバー攻撃は、抗議活動として万人に見える形で行われるものでした。この威嚇によるサイバー攻撃は、2012年の尖閣諸島国有化をピーク⑫に、減少傾向にあります⑬。理由は、反日デモの暴徒化をはじめ、威嚇は海外投資の撤退や国際的評価の低下を招くためと推測します。

## (2) 情報窃取

初期のサイバー攻撃は有志のハッカーによるものでしたが、2002年には民兵を活用した「人民解放軍情報戦民兵部隊」が創設されました⑭。そして、米国ではこの頃から人民解放軍61398部隊が関与したとするAPT1を確認しています⑮。

2004年、日本では金銭の窃取を目的としたフィッシング詐欺が流行しました。その容易さと成功率から「メールから人を誘導する」攻撃手法が以後増加します。2005年10月には、実在の外務省職員になりすました標的型メールが観測されるようになりました⑯。本攻撃の攻撃元は不明ですが、メール件名「小泉首相の靖国神社参拝速報」に関心がある層からの情報窃取を狙っています。

前述の通り、中国は情報優勢を確立するために平時から情報収集をしています。標的周辺で窃取した情報は信頼性が高く、

⑩ Ellen Messmer (1999)「Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says」, <http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/ >
⑪ 情報処理推進機構(2000)「情報セキュリティの現状 2000年版」, <https://www.ipa.go.jp/security/fy12/sec2000/sec2000.pdf >
⑫ 株式会社ラック(2012)「攻撃件数の増加について」, <https://www.lac.co.jp/lacwatch/alert/20120918_000158.html >
⑬ 株式会社ラック(2016)「JSOC INSIGHT Vol.10」, < https://www.lac.co.jp/lacwatch/pdf/20160106_jsoc_j001w.pdf >
⑭ 財団法人防衛調達基盤整備協会(2010)「中華人民共和国のサイバー戦とコンピュータ・ネットワーク・エクスプロイテーション能力」, < https://ssl.bsk-z.or.jp/kakusyu/pdf/22-5%20shousassi.pdf >
⑮ FireEye(2004)「APT1－Exposing One of China's Cyber Espionage Units」, <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf>
⑯ 情報処理推進機構(2011)「IPAテクニカルウォッチ 標的型攻撃メールの分析に関するレポート」, <https://www.ipa.go.jp/files/000024771.pdf>

サイバー攻撃の成功率を高め、さらなるサイバー攻撃の足掛かりとして利用できます。そして、収集した情報をもとに先手を打って宣伝・暴露することで中国に有利な世論を形成します。

### (3) 世論誘導

中国が世論誘導の活動を開始したのは、1989年天安門事件後と考えられています[17]。この頃に、欧米諸国のメディアに中国の国際的なイメージが低下するような批判的な記事が掲載されました。そのため、中国は文化交流を通じて現地の国民や世論に直接働きかける広報文化外交の一環として、対外宣伝を強化してきました。

中国による対外宣伝は、文化大革命前にその戦略思想が既にでき上がっています[18]。この戦略思想に基づき、対外宣伝を制御することで心理的効果を狙っています。

1.対外宣伝に関する管理思想は対内宣伝に従う
2.対外宣伝の内容は、中国のプラスイメージと功績を宣伝し、マイナス報道を回避する
3.対内宣伝と対外宣伝を区別して報道する

対外宣伝におけるプラスとマイナスの使い分けの根本は、1942年に毛沢東が中国共産党内へ向けたスピーチ「懲罰と治療法の基本原則」に基づく思想改造にあるものと考えます[19]。思想改造の構造は、自己批判により自らの過去と現在における罪に気付かせて認めさせる「告白」と、中国共産党にとって理想的な人物に造り変える「再教育」の二段階に大別されます[20]。

第一段階の「告白」を対外宣伝に置き換えると、歴史問題において日本人は加害者であるとマイナス宣伝を繰り返すことで、日本人が自発的に反省するように促すという手法に該当します。国際的な信憑性の有無にかかわらず、反復して主張することで中国に有利な世論を形成し、日本と周辺諸国において反日感情を醸成します。

第二段階では「再教育」として、中国は善でそれ以外は悪という理論を形成します。例えば、1950年の朝鮮戦争では捕虜の不幸や困難は資本主義のせいであるとし、共産主義の素晴らしさを説きました[21]。対外宣伝に応用すると、中国の一帯一路政策における発展途上国へのインフラ整備支援のようなプラス宣伝に該当します。このプラス宣伝の効果を高めるためには、それと相反するマイナス宣伝を制御する必要があります。中国内においては、検閲による情報統制や五毛党(インターネット上で中国政府のプラス情報を大量に書き込み、マイナス情報を埋もれさせる集団)による世論誘導が知られていますが、諸外国に対してもジャーナリストを拘束する等でマイナス宣伝を制御しています[22]。

## これからのサイバー心理戦

本誌のP4～9(2020大規模サイバー攻撃に備えよ)で国家による政治意図を持った攻撃が述べられている通り、心理戦を有利に進めるための情報窃取や世論誘導は引き続き行われる可能性があります。中国の目標は、中国の国際的な地位を向上させ、日本の国際的な信頼や地位を低下させることです。そのために、諸外国における親中派を増やし、各国で国内対立を促し、反中派を国際的に孤立させます。中国は、これを実現するためにサイバー空間を用いて心理戦を展開します。

中国が日本から窃取しようとしている情報の種類とその背景、ニュース等により世論を誘導する意図、つまりポリティカル・アトリビューションにより、サイバー空間を用いた日本への攻撃を分析・対処することが今後ますます重要になってくるでしょう。

---

17 高井潔司(2011)『中国文化強国宣言批判』, 蒼蒼社
18 雷紫(2014)「グローバル時代における中国の対外宣伝戦略に関する考察」,『国際広報メディア・観光学ジャーナル』18, p.137-155
19 ロバート・J・リフトン(1979)『思想改造の心理:中国における洗脳の研究』小野泰博訳, 誠信書房
20 Hunter Edward(1956)『BRAINWASHING: The Story of the Men Who Defied it』New York, Farrar, Straus and Cudahy
21 Edgar H. Schein(1960)『BRAINWASHING』Massachusetts institute of technology University Press
22 Elana Beiser(2017)「Record number of journalists jailed as Turkey, China, Egypt pay scant price for repression」, Committee to Protect Journalists <https://cpj.org/reports/2017/12/journalists-prison-jail-record-number-turkey-china-egypt.php>

ラックの顔

第7回


# 仕事を通じて「国を衛る」。サイバーセキュリティの技術で政府に貢献

「国を衛る」。これは、ラックの社長である西本逸郎が事業に対して掲げる信念だ。その熱い思いはラックで働く社員にも受け継がれており、仕事を通じて国や政府に貢献しようと考える社員は少なくない。サイバーセキュリティという事業が、どのような形で国を衛ることにつながるのか。国への貢献を積極的に進めようとラック社内の環境整備が整いつつある今、それぞれのやり方でそれを実現している二人の社員に、その動機とやりがいを聞いた。

## 仕事を続けながら技術を生かせる点が魅力だった「予備自衛官等制度」

ラックの前身であるエー・アンド・アイ システムに入社してから、一貫してシステム開発に携わっていた芝村が、サイバーセキュリティ事業へと足を踏み入れたのは2013年のことだ。システムインテグレーションサービスからセキュリティ分野への転向は、IT業界の中でも珍しい部類に入る。

「正直に言うと、当時セキュリティ事業に対してそこまで深い理解はありませんでした。たまたまセキュリティに関する本を読んでいたタイミングで、サイバーセキュリティ事業部のサイバー救急センター❶への社内公募があったので、興味を持って応募しました（芝村）」

セキュリティ事業へと軸足を移し、技術を磨いていた芝村が、「予備自衛官等制度」を知ったのはそれから1年ほど経った2014年のこと。陸上自衛隊東京地方協力本部の隊員がラックに来社し、説明会を行ったのがきっかけだ。

「陸上自衛隊出身の同僚に、『刺激になるから』と参加を勧められ、説明会に参加しました。国際情勢が緊迫していることは個人的にも以前から気になっていて、何か家族のためにできることはないかと漠然と考えてはいたんです。とはいえ、仕事を辞めることはできませんし、体力にそこまで自信があるわけでもない。予備自衛官等制度は、仕事を続けながら、自分の技術を生かせるという点が、自分の考えや環境に合っていたので応募しました（芝村）」

予備自衛官等制度とは、平時には日常生活を送りながら、自衛官として必要とされる素養を訓練で維持し、有事の際には防衛召集や災害召集などに応じて自衛官として活動する人員を確保する予備役制度だ。災害復旧や警備などの一般公募に加えて、語学や医療、整備といった特殊な技術を持つ人を募集する技能公募のコースがあり、芝村は後者で任務に当たっている。予備自衛官等制度に

❶ セキュリティに関わる緊急事態に対して支援を行う緊急対応サービスを提供する部門

おける技能には、サイバーセキュリティという分野は規定されていないことから、「情報処理」技能の中の技術として応募している。

技能公募の場合、初年度に予備自衛官補として10日間の訓練を受け、その後予備自衛官として年5日間の訓練を毎年続けることになる。部隊の統制をするための基本動作や射撃、救命救急など、一般公募と同様の訓練のほか、配属された部隊が有する技術についての職務訓練も行っているという。早朝から深夜に及ぶ訓練、しかも10日間という短い期間で陸上自衛官に求められる基本的な所作を身につけることはかなり過酷だ。そのため、宿営舎で寝食をともにしながら濃密な時間を過ごした他のメンバーとは自然と深い絆が生まれると芝村は言う。

## 訓練で直接身につけること以上に多くの経験が得られる制度

さまざまな技能を持った人たちが集う技能公募の訓練。サイバーセキュリティとは無縁の職種の人たちだからこそ、「一緒に過ごせた時間は貴重だ」と芝村は話す。

「自動車や工場の機器を整備する技術者、現役の医師やこれから防衛省に入省するという大学生など、職業も年齢も普段出会う機会のない人と交流することはとても刺激になります。警備会社で警備員の指導をしているという警備のスペシャリストの方に、私の自宅の写真を見ながら泥棒に入られないための警備のポイントを教えてもらったりと、日常生活に役立つ知識を得られることもあるんですよ（笑）。訓練が終わったあとも、SNSでコンタクトを取ったり、一緒にお酒を飲みに行ったり、家族ぐるみでお付き合いをしている人もいます（芝村）」

また、陸上自衛官とのコミュニケーションにも大きな影響を受けたという。

「陸上自衛官としての心構えや普段考えていることを聞いているうちに、日本が置かれている状況を意識して考えるようになりました。国際情勢に関する新聞記事を読むときにどういった点に着眼すればよいかといった視点も、以前に比べて鋭くなったように思います（芝村）」

さらに、訓練のためだけに費やす5日間という時間そのものが、芝村にとっては特別なものとなっているともいう。訓練の期間は駐屯地に入って、外に出ることはほぼない。完全に隔離された状況に置かれることで、自分自身を改めて見つめ直す時間を持てるからだ。

「家族のことも考えますし、仕事についても次に何をしようか、そのために何が必要か、といったことをゆっくり考えられるんです。訓練は、いろいろな意味で自分にとって大切な時間になっていると思います（芝村）」

## 新規事業の立ち上げで見えてきた課題を解決するための出向

比較的異動の少ない芝村と異なり、初田の業務経験はバラエティに富んでいる。新卒でラックに入社後、JSOC（Japan Security Operation Center／ラックのセキュリティ監視・運用サービス拠点）でアナリストに就任、技術者としてのキャリアをスタートさせた初田は、ペネトレーションテスト（脆弱性診断）やコンピューターが侵害を受けた際に顧客とともに復旧対応の支援を行うインシデントレスポンス、コンピューターフォレンジックといわれる調査業務、そしてそのトレーニングトレーナーなど、ラックの事業に広く関わってきた。「自分自身でも、いろいろな業務を経験させてもらったと思っている」と話す初田が日本サイバー犯罪対策センター（JC3）に出向する転機となったのが、2013年に行った

# 芝村　崇

takashi shibamura

マルウエア・脅威分析チームの立ち上げだ。

「当初は、“サイバーセキュリティを生業とする企業としてラックは脅威分析をきちんとできているのだろうか”という不安の中で始まったプロジェクトでした。1年ほど続けたところで“思ったよりも悪くはないな”という感触が得られ、技術レポート『CYBER GRID VIEW』の第1号を発行することもできた。マルウエアや脅威分析に対する手応えを感じ始めていた、そんな矢先の辞令でした（初田）」

自らが手がけた新チームがようやく軌道に乗り始め、事業拡大が見えてきたというタイミングで初田が出向の話を承諾したのは、なぜか。その理由を本人はこのように話す。

「マルウエアや脅威分析で犯罪者を追いかけていけばいくほど、我々が得られる情報というのはパズルのピースにすぎないということを痛感していました。日本政府や大企業への侵入による情報窃取など、国益が損なわれるような攻撃については以前から懸念を持っていたのですが、そういったレベルの事案は、もはや個人ではなく、海外諸国が主体、もしくはスポンサーとなって攻撃を行っている可能性もあります。スケールの大きな事案に対応し、犯罪者に近づくためには、一企業であるラックが持っている情報だけでは全然足りないんです。情報共有の必要性を強く感じていたときに、まさに情報共有を促進する組織が設立されると聞き、面白そうだ、チャレンジしてみたい、と思いました（初田）」

ともにマルウエア・脅威分析チームを立ち上げた上司でもある担当役員は、初田の出向をうれしく思う半面、寂しさも感じたと話す。それほどに高い能力を持つ人材を外部組織へ出向させる、そういった人事にも、「国を衛る」というラックの思いが見え隠れしているといえるだろう。

## 無理や負担のない情報共有が、継続的なサイバーセキュリティに寄与する

JC３は2014年11月に業務を開始した、産学官の連携組織だ。その背景には、警察庁が主体となり、サイバーセキュリティに精通した民間の有識者等を集めて開催していた「総合セキュリティ対策会議」の存在がある。同会議の議論では、産学官連携の重要性がしばしば叫ばれていた。アメリカでは2002年にNCFTA（National Cyber-Forensics and Training Alliance／産学官の連携によりサイバー犯罪に関する情報共有や無力化に向けた活動に取り組んでいる非営利団体）という組織が設立され、サイバー犯罪の予防や摘発などの成果を上げていた。そこで日本でも、NCFTAをモデルとした組織を立ち上げ、情報の集約や分析した情報の共有により、脅威の大本を特定・軽減・無効化していこうというのがJC3設立の趣旨である。

JC３の立ち上げは、官民から集まったわずか6人の人間でスタートした。

「当初はとにかく“何でも”やりました。規定類の作成や物品の受発注といった総務的なことはもちろん、カンファレンスの開催など、みんなで議論して協力してやっていくといった状況でした。官には官の慣習がありますし、民には民のルールがある。また、会員等のステークホルダーもたくさんいます。当然のことながら、ラックで経験してきたスピード感そのままで仕事を進めることはできませんでした（初田）」

一見焦りが募りそうな状況下にあったものの、初田は「無理をしない」ことを念頭に業務に当たっていたという。

「“Focus on what you can share and are comfortable sharing”――共有をしても差し支えない情報の共有、互いに負担のない情報共有――これはNCFTAのポリシーの一つであり、JC３もそれを踏襲しています。情報の共有に関しては、積極的な組織もあれば保守的な組織もある。それぞれの立場を尊重し、できるところから少しずつ取り組もうというスタンスがこの課題に対しては非常に重要。情報共有は継続して

# 初田淳一

junichi hatta

実現できなければ意味ありません。数十年先まで続けて活動できる組織を作るために、まずは土台をしっかり固めようという気持ちで臨んでいました(初田)」

初田をはじめとする設立メンバーの努力が実り、設立から5年目を迎えたJC3の活動は、その範囲を大きく拡大させつつある。「私は2017年9月に出向を終えましたが、私が在籍していたときよりも会員も増え、情報共有が格段に進み、すさまじい勢いで組織が成長していると感じています。後任には語学が堪能で優秀な若手社員が派遣されているので安心です」と初田は安堵の表情を見せた。

## 外から得られた経験が社内に還元され、再び国への貢献につながる

異なるアプローチでありながらも、「仕事を通じて国を衛る」というラックのポリシーを実現している芝村と初田。外部の組織に身を置いたことで得たものも多いというが、そういった経験はラックでの業務にどのように生きているのか。

「業務上で防衛関連の方々にお会いする機会があったときに同じ目線で話ができるので、打ち解けやすくなりますし、話がスムーズに進むことが多くなったと感じています。また、今受けている訓練は一般的な内容が多く、それほどサイバーセキュリティに特化したものではありませんが、近い将来、サイバーセキュリティの専門家として訓練を受けることができるようになると聞いています。実際に召集がかかったときに自分の技術を生かしてどんな貢献ができるか、そのために自分に不足しているものは何か、常に自分を振り返ることが、技術の向上や仕事に対するモチベーションにつながっていると実感しています。訓練の日は有給休暇とは別に特別休暇を取得できるなど、会社も予備自衛官等制度への応募を後押ししてくれていますので、社内で興味を持ちそうな人がいたら、積極的に声をかけています(芝村)」

「情報共有は、一言で言ってしまえば信頼関係に尽きる。NCFTAには、“Focus on what you can share and are comfortable sharing”に加えて“One team, One goal” “Face to face” “Industry first”という4つのポリシーがありますが、JC3へ出向した3年間でこれを体感できたことは非常に大きいと感じています。“信頼”は目に見えるものではありませんから、信頼関係を構築するのは容易ではありません。ですが、このポリシーを頭だけでなく身をもって理解できたことで、業務上の信頼関係を築きやすくなったと感じています。また、NCFTAのスタッフとは月に1度のペースでテレカンファレンスでの情報交換をしていますし、年に1度はFace to faceでのミーティングも行っています。具体的な内容は話せませんが(笑)、彼らとのコミュニケーションで得られるグローバルの最新情報は業務に大いに役立っています(初田)」

ラックを離れたことで見えてきた多様な視点や人脈、知識。そういったものが再びラックへと還元され、それが国への貢献へとつながる糧となる。そういった好循環がこれからも多く生まれることを期待したい。

**芝村 崇**
takashi shibamura

サイバーセキュリティ事業部
Advanced Cyber Threat Research Center(ACTR)
Threat Hunting Team

1998年、ラックの前身であるエー・アンド・アイ システム入社。システム構築業務を経て、2013年よりサイバーセキュリティ事業部に在籍。サイバー救急センターでフォレンジックやマルウエア解析等に携わった後、現在はACTRにてスレットインテリジェンス(脅威情報)に関わる業務を担当。「子供たちにパパと同じ仕事がしたいと言われ喜びましたが、PCを占拠され微妙な心境です」

**初田 淳一**
junichi hatta

サイバーセキュリティ事業部
Advanced Cyber Threat Research Center(ACTR)
Threat Hunting Team チームリーダー
兼 サイバー・グリッド・ジャパン 次世代技術開発センター

2002年ラック入社。JSOCにてアナリストを経験後、ペネトレーションテストやインシデントレスポンス、フォレンジックなど幅広い業務に携わる。2014年12月より一般財団法人日本サイバー犯罪対策センター(JC3)へ出向、同法人の設立に参画。2017年9月より現職。最近は妻とポケモン探しを楽しんでいる。

# CYBER GRID JOURNAL VOL.7

サイバー・グリッド・ジャパンは株式会社ラックの研究開発部門です。
サイバー攻撃や各国のセキュリティ事情、セキュリティ防御技術などに関する最先端の研究のほか、
複数のセキュリティ企業との連携や新たな製品・サービスの開発、各種啓発活動などにより
日本のセキュリティレベルと情報モラルの向上に貢献しています。



**株式会社ラック サイバー・グリッド・ジャパン**
〒102-0093 東京都千代田区平河町 2-16-1 平河町森タワー
E-MAIL：sales@lac.co.jp　https://www.lac.co.jp/

株式会社ラック
サイバー・グリッド・ジャパン