［サイバー・ウォーズ］

応
般

⑤ ロシアのインテリジェンス機関とICT

小泉　悠 | 東京大学先端科学技術研究センター

サイバー空間で存在感を増すロシア

サイバー時代の安全保障を論じるにあたり，ロシアは台風の目となった感がある．実際，米国大統領選への介入をはじめとして，サイバー空間におけるロシアの存在感はかつてなく高まっており，メディアでもロシアのサイバー戦について目にする機会が増えた．他方，こうした領域におけるロシアの活動実態は，同国の秘密主義もあってことさらに分かりにくく，誰がどのような手段を用いているのかが今ひとつ明確に論じられていないようにも思われる．

そこで本稿では，ロシアにおけるインテリジェンス機関の活動，特に情報通信技術（ICT）を用いたそれについての解説を試みた．ロシアにはどのようなインテリジェンス機関が存在し，どのような活動を展開しているのか，その中でICTがどのような役割を果たし，どの程度のインパクを有しているのかがここでの焦点である．

「インテリジェンス」と「インテリジェンス機関」

インテリジェンス機関について論じるには，まず「インテリジェンス（Intelligence）」という言葉の意味するところを定義する必要があろう．小林の整理によれば，この言葉は主に①プロダクトとしてのインテリジェンス（政策決定者に提供される分析・加工された知識），②プロセスとしてのインテリジェンス（プロダクトを生産するための情報の要求，収集，分析，報告，フィードバックのサイクル），③組織としてのインテリジェンス（インテリジェンス活動に従事する情報機関）の3つに分類することができる[1]．

このうち，インテリジェンス活動の具体的な内容を示すのは②であり，一般的に情報収集手段別に次の4つに分類されることが多い．

- HUMINT：人的インテリジェンス（合法・非合法の人的接触によって得られた情報の分析･加工）
- SIGINT：信号インテリジェンス（通信等，電気信号の傍受によって得られた情報の分析・加工）
- IMINT：画像インテリジェンス（偵察機や偵察衛星等が撮影した画像情報の分析・加工）
- OSINT：オープンソース･インテリジェンス（公開情報の分析・加工）

ここで注意すべきは，インテリジェンス・プロセスがインテリジェンス機関の活動全体と必ずしも一致しないということである．後述するように，ロシアのインテリジェンス機関が関与する活動はきわめて幅広い分野にわたっており，狭義のインテリジェンス活動は全体のごく一部であるとさえいえる．

また，インテリジェンス機関といってもさまざまであり，広義には検察などの捜査機関や税務機関まで含まれる場合がある．しかし，本稿では論点の拡散を防ぐため，これを「ラズヴェートカ（разведка）」に従事する機関に限定したい．これは何かを探り出す行為全般を指すロシア語であり，たとえば資源業界では探鉱の意味で用いられる．一方，国家や安全保障の文脈でこの言葉が用いられる場合，その意味

するところは，狭義のスパイによる諜報活動や軍事的な偵察活動と理解することができよう．

現在のロシアにおいて，こうした文脈で「ラズヴェートカ」に従事する機関は，旧国家保安委員会（KGB）系の情報機関である連邦保安庁（FSB）および連邦対外情報庁（SVR），そしてロシア軍参謀本部直轄の情報機関である情報総局（GRU）の3つである（ちなみにGRUやSVRの「R」はこのラズヴェートカの頭文字を取ったもの）．各機関の活動内容はそれぞれの出自や任務によって異なるが，表-1はこれを「○」（各機関が主たる任務として実施しているもの），「△」（副次的任務として実施されていると推測されるもの），空欄（ごく不活発ないしまったく実施されていないと考えられるもの）に分類した．

ここから読みとれるように，GRUは三大インテリジェンス機関の中で唯一，外国における公然・非公然のHUMINT能力を有している．また，GRUは航空宇宙軍の運用する偵察衛星や偵察機，海軍の運用する情報収集艦や深海工作艇，GRU直轄の電波傍受基地等，大がかりなアセットを用いたSIGINTおよびIMINTを実施する能力を有する点でも旧KGB系機関とは一線を画す．

一方，FSBはKGBの国内監視機関であった第2総局（VGU）を中心とし，プーチン政権下では同じく旧KGB系の国境警備機関や通信傍受機関，対テロ特殊部隊等がここに統合された．本稿のテーマとの関連においては，電話・インターネット監視システムである「即時捜査手段システム（SORM）」によってロシア国民のインターネット・トラフィックを無制限に監視・追跡し得る能力を有している点が言及されるべきであろう．これらのHUMINT/SIGINT能力は主としてロシア国内での反体制派，チェチェン等の非合法武装勢力，組織犯罪等の監視に用いられているが，一部ではこれら監視対象組織に対するインテリジェンス活動が国外でも展開されていると見られる．

SVRの前身はKGBの国外諜報機関であった第1総局（PGU）であり，いわゆるスパイ活動を主任務とする．ただ，PGUは外国に設置した電波傍受拠点を用いたSIGINTも行っていたとされ，恐らく現在のSVRも同様であろう．

まとめるならば，ソ連のGRUとKGBは共にインテリジェンス活動の一環として大規模なSIGINTを実施してきたのであり，現在のロシアがサイバー空間でICTを用いて展開している諜報活動（エスピオナージュ）はその延長上に位置付けることができよう．

ただし，ICTが持つ意味はこれにとどまらない．元々ロシアのインテリジェンス機関は狭義のインテリジェンスに限らず，多様な活動を担ってきた．GRU，FSB，SVRが国内外での暗殺や，ICTを用いたサイバー破壊活動，偽情報（フェイクニュース）の流布による情報操作といった活動（詳しくは後述）を多数実施していることはその好例である．ICTを用いたものに限って言えば，インテリジェンス機関が関与する活動は表-2のように整理することができよう．

表-1　ロシアのインテリジェンス機関とその活動内容

類型	具体的な活動内容	旧KGB系機関		ロシア軍
		FSB	SVR	GRU
HUMINT	外国における公然活動（武官派遣等）			○
	外国における非公然活動（諜報活動等）	△	○	○
	国内における反体制派等の監視	○		
	国境における出入国管理	○		
SIGINT	航空機・艦艇・人工衛星によるSIGINT	△		○
	外国における通信傍受等	○	○	○
	国内における通信傍受等	○		
	保秘通信回線等の運用	△	△	△
OSINT	外国の公開情報分析	○	○	○
	国内の公開情報分析	○	△	△
IMINT	航空機・艦艇・人工衛星によるIMINT	△		○

（出典）筆者作成

すでに述べたように，サイバー空間におけるエスピオナージュは古来から行われてきたSIGINT活動の延長にあり，これはコンプロマートも同様である．インテリジェンス機関が入手した情報を用いてターゲットの名誉を毀損したり，その可能性を示唆することで協力を強制する事例はインテリジェンスの歴史上，きわめて古くから観察されてきた．この意味では，ICTは古典的インテリジェンス活動に新たなツールを付加したものにすぎないが，そのターゲットとなる社会，経済，安全保障等がますますサイバー空間に依存するようになりつつあることは，インテリジェンス全体におけるICTの重要性を増加させているといえよう．情報操作もまた，インテリジェンス機関の活動類型としてやはり古くから存在してきたが，ICTはその影響力をかつてなく拡大する役割を果たした．ソーシャル・ネットワーキング・サービス（SNS）等，個人への伝達性が高いサイバー・メディアを用いることで，偽情報や歪曲された情報をより的確に，広範囲に流布することが可能となるためである．

一方，ICTはインテリジェンス機関の活動に新たな領域，すなわちサイバー・サボタージュを作り出した．ブッシュ（George W. Bush）政権およびオバマ政権においてサイバー安全保障担当の大統領補佐官を務めたリチャード・クラーク（Richard A. Clark）らが述べるように，コンピュータで制御される産業・金融インフラやオフィス機器は，それが閉鎖型ネットワークであるか否かを問わず，敵対勢力にとって格好の攻撃対象となる[2]．社会の中に広く，膨大に存在しているコンピュータ制御機器が暴走すれば，大規模な火災や爆発が発生し，社会活動を大混乱させ，経済を崩壊させることも不可能ではないためである．これは，かつて破壊工作員や戦略爆撃機が担っていた任務をサイバー空間経由で実施するものと位置付けられよう．

ロシアはサイバー空間で何をしているか

概念的整理は以上のとおりとして，今度はロシアのインテリジェンス機関が実際にどのようなオペレーションを展開しているのかを見ていこう．

まずは概況である．米国の戦略・国際研究所（CSIS）は，政府機関，軍需企業およびハイテク企業が標的となったサイバー攻撃および100万ドル以上の損害を出したサイバー攻撃を「顕著なサイバー事案」と定義し，2006年から事例を収集してきた．これによると，ロシアは中国に次いで世界第2位のサイバー攻撃発信地であり，2019年前半までの約13年間で合計100件近い事例が確認されている[3]．この中には国家が関与しないサイバー犯罪も含まれていようが，その多くは軍や情報機関が実施ないし実施の指令・調整を担当する国家的なサイバー活動であると考えられる．

しかも，ICTを用いたロシアのインテリジェンス機関の活動は，表-2で示した諸類型をほぼ完全にカバーする，フルスペクトラムなものである．以下，過去の事例から主要なものを挙げてみたい．

エストニアに対するサイバー・サボタージュ

2007年4月，旧ソ連のエストニアでロシア系住民による大規模な暴動が発生すると，その翌日からエストニアの政府機関，メディア，銀行システムなどが一斉にDDoS攻撃を受け始め，社会システム

表-2　ICTを用いたインテリジェンス機関の活動

類型	内容
諜報（エスピオナージュ）	サイバー空間における情報の窃取
名誉毀損（コンプロマート）	入手した情報の流布による名誉毀損またはその脅し
情報操作	事実に基づかないものを含めた情報の流布・歪曲による民心の捜査
破壊活動（サボタージュ）	サイバー空間を経由した物理的・非物理的打撃

（出典）筆者作成

が麻痺状態に陥った．のちに「タリン事件」と呼ばれるこの出来事は，サイバー攻撃が一国の首都機能を麻痺させた初の事例とされ，北大西洋条約機構（NATO）によるサイバー防衛卓越研究拠点（NATO CCDCOE）の設置やサイバー攻撃に対する対処指針（「タリン・マニュアル」）の策定につながった．

ところで，この攻撃はそれまで知られていたDDoS攻撃のような一過性のものではなく，数週間に渡る継続的な攻撃であった点が注目される．また，攻撃には世界50カ国のコンピュータ100万台以上が参加していたが，多くのコンピュータの所有者は攻撃に参加したという自覚はなく，何者かにコンピュータを乗っ取られて「ゾンビ」化させられていた．これだけ大規模なサイバー攻撃を誰が行ったのかは現時点でも明らかでないが，ロシア政府が何らの音頭を取った疑いは濃厚とされている．

グルジア戦争：同時進行する軍事作戦とサイバー戦

2008年8月，グルジアの分離独立地域であるアブハジアおよび南オセチアをめぐってロシアの間で戦争が発生したが，この最中にグルジア政府は間断ないDDoS攻撃を受けた．地上戦が始まる数時間前，StopGeorgia.ruというフォーラムがネット上に出現し，同フォーラムがグルジア政府機関のサーバ一覧を表示してDDoS攻撃を行うようにネットユーザ達に呼びかけたのである．この結果，グルジア政府機関のサーバは軒並みダウンし，ネットを使用した情報収集や連絡・調整，対外広報などが行えなくなってしまった．

当然，StopGeorgia.ruにはロシア政府の関与が伺われる．実際，StopGeorgia.ruに75.126.142.110というIPアドレスを提供していたIT企業Steady-HotをWHOIS検索してみると，その所在地が参謀本部情報総局のすぐ隣のブロックであることが判明したとの報道がある．

SIPRNetへの侵入

2008年10月には，米国の機密ネットワークである「秘密インターネットプロトコル・ネットワーク（SIPRNet）」がロシアによる侵入を受けた．SIPRNetは国防総省が機密情報を扱うために構築した「防衛情報システムネットワーク（DISN）」の一部であり，インターネットには接続されていない孤立型システムであったため，外部からの侵入はそれまで一度も確認されていなかった．のちの調査によると，ロシアの情報機関は米軍基地などあちこちにバックドアを仕込んだUSBメモリを放置し，それを拾った米側職員がSIPRNetに差し込んだことで侵入を許したとされる．

ウクライナ危機とサイバー戦

2014年2月，ウクライナで政変が発生すると，ロシアは軍事介入に踏み切り，これと同時に大規模なサイバー攻撃を展開した．ウクライナ危機におけるサイバー戦の特徴は，敵対国の双方が激しいサイバー攻撃の応酬を展開している点にある．これは敵対国同士が言語を共有しているという特殊性に原因が求められようが，サイバー攻撃が双方向的な応酬として実施された事例は珍しいのではないかと思われる．双方ともに最も多いのはDDoS攻撃で，Webサイトの改ざん等がこれに次ぐが，このほかにもマルウェアを用いてウクライナの送電網管理システムへの攻撃が行われ，大規模な停電が発生した事案（2015年）や，会計ソフトの脆弱性を衝いた広範な政府機関・企業への攻撃で重要インフラが機能不全に陥る事案（2017年）など，烈度の高いサイバー・サボタージュ事例も少なくない．

他方，ウクライナのハッカーグループ「サイバー・フンタ」は，ロシアのウラジスラフ・スルコフ（Владислав Сурков）大統領補佐官（プーチン（Владимир Путин）大統領のブレーンとして知られる）のメールサーバに侵入して大量のメールを窃取し，公開するという攻撃を行った．暴露さ

れた情報は1ギガバイトにもおよび，その中にはロシアによるウクライナ介入の具体的な計画やこれを主導した人物などに関する情報が多数含まれていた．ICTによるエスピオナージュと情報戦の融合事例といえよう．

ロシア・ゲート

2016年の米国大統領選に対するロシアの介入疑惑，いわゆる「ロシア・ゲート」疑惑についてはすでに多くの著作や研究成果があるので，ここでは詳しくは触れない．

ただ，「ロシア・ゲート」が複合的な性格を有していることだけは指摘しておこう．すなわち，①トランプ（Donald Trump）陣営が大統領選を戦うにあたってロシア側となんらかの協力（共謀）を行っていたという疑惑，②ロシアが民主党全国委員会（DNC）等にハッキングを仕掛けてメール類を摂取していたという疑惑，③ロシアがSNSやインターネット広告を用いて大量の偽情報を発信していた疑惑，の三重構造であり，このうち，本稿のテーマに強く関連するのは②であろう．

当時，DNCのサイバーセキュリティはきわめて杜撰であり，ロシアによる侵入は純粋に技術的にみてさほど困難であったとは思われない．侵入が発覚してからの連邦捜査局（FBI）による対応が鈍かったことも，ロシアによる継続的な侵入を許すことにつながった．逆にいえば，ロシアは比較的初歩的なハッキング技術できわめて大きな政治的効果を得たわけであり，サイバー戦の非対称性を示す典型例といえよう．

ハッカーとインテリジェンス機関

プーチン大統領は2017年，「ハッカーというのはフリーのアーティスのようなものだ」と述べたことがある．つまり，ハッカーはそれぞれ自分の興味や愛国心にしたがってハッキングを行っているのであって，政府がそれを統制することはできないという理屈である．

ただし，サイバー戦の実施主体に民間の個人ないし集団が含まれていることはまったくの嘘ではない．多くのケースにおいてGRU，FSB，SVRといった政府機関はサイバー攻撃を自ら実施するのではなく，金銭や愛国心を動機とする民間のハッカーを「サイバー民兵」として組織化し，その実行に当たらせていると見られている[☆1]．

他方，大規模かつ継続的なサイバー戦の実施には相当の金銭的・人的リソースを必要とすることから，サイバー攻撃のすべてが「サイバー民兵」に委託されていることもまた想定しにくい．ロシア発の「先進的かつ継続的な脅威（APT：Advanced Persistent Threat）」としては，APT28やAPT29が知られているが，前者についてはその正体がGRU所属の2つの組織（第26165軍事部隊および第74455軍事部隊）であることが明らかにされている．このほか，継続的なサイバー戦を行っている主要なハッカーグループは，なんらかの形でロシア政府機関と一体ないし密接な関係にあるものと考えられよう．**表-3**は，以上の関係性を整理したものである．

では，こうした広範な活動を展開するインテリジェンス機関同士は，どのような関係にあるのだろうか．つまり，彼らは相互に協力しあっているのか，それとも独立に活動しているのだろうか．

結論を先に述べるならば，各インテリジェンス機関は同一の目標を追求しつつも相互に連携する関係にはない可能性が高い．この点を裏付けるのが，サイバー・インテリジェンス企業Check Point Researchがマルウェア分析ツールの開発企業Intezerと合同で行った調査である．両社は，ロシアのインテリジェンス機関が用いているとされるマルウェアのサンプルを大量に収集し，これを構成するモ

☆1 ジェフリー・カー（Jeffrey Carr）は，グルジアに対するサイバー攻撃に関して，クレムリン（ロシア政府）が「ナーシ」のような官製青年運動にサイバー攻撃任務を与え，「ナーシ」はさらに一般のハッカーを雇って実際のサイバー攻撃部隊にするという三層のモデルを描いている[4]．

ジュールやソースコード間の類似性を独自開発したツールで分析するという手法により，各インテリジェンス機関間の関係性を割り出すことに成功した．以下，両社の報告書[5]の主要な知見のサマリーから，本稿との関連において重要な部分を転載する．

- 本調査は，この種のものとしては初であり，かつ最も包括的である．

  きわめて強力な国家における異なったサイバー諜報機関間の繋がりをマッピングするために，数千のサンプルが初めて収集され，分類，分析された．
- 多くのケースにおいて，ロシアのアクターはほかのアクターとコードを共有していない．

  各アクターは異なったオペレーションのために異なったマルウェア・ファミリー間でコードを使いまわしているが，各アクター間で共有されているツール，ライブラリ，フレームワークは存在しない．
- ロシアにおいて APT に分類されるアクターないし組織は，それぞれ独自のマルウェア開発チームを有しており，長年に渡って似たようなマルウェア・ツールキットとフレームワークを別個に開発してきた．これら多くのツールキットが同じ目的に用いられていることを考えると，これら別個の活動には冗長性があるということになろう．
- これらの発見は，ロシアがオペレーションを安全に行うために多大の努力を図っていることを示している．

  異なる組織が広範なターゲットに対して同じツールを使い回すのを避けることにより，彼らはあるオペレーションが露見してもほかのオペレーションが危険に曝されないようにすることができる．

要するに，ロシアのインテリジェンス機関は独自のマルウェア開発部門を抱え，似たような目的のためであってもほかの機関が開発したマルウェアを流用することはしていない（あるいはそうした協力を行う関係にはそもそもない）ということである☆2．

☆2 問題の報告書によると，異なるインテリジェンス機関のマルウェア間にも共通性が存在するケースが稀にではあるが観察される．ただし，これはダーク Web 等で配布されたオープンソースを用いた結果であり，インテリジェンス機関間の連携の結果ではないとされている．

表 -3　ロシアの主要なハッカーグループと政府機関との関係

グループ名	別名	想定される上位・関連組織	主要な活動
APT28	Pawn Storm, Fancy Bear, Sofacy, Tsar Team, Strontium, Sednit	GRU	・米大統領選挙への介入（2016 年） ・欧州諸国・国際機関に対する侵入 ・その他多数
APT29	Dukes, Cozy Bear, Monkey	FSB または SVR	・米大統領選挙への介入（2016 年） ・米国を含む世界各国の国家機関に対する侵入 ・その他多数
Turla	Snake, Venomous Bear, Uroburos, Group 88, Waterbug	FSB	・スイス国防省・軍需企業に対する侵入 ・東欧諸国の領事館に対する侵入 ・韓国政府機関に対する侵入
Black Energy	Sandworm, Voodoo Bear, Electrum	不明（GRU ？）	・グルジアへの DDoS 攻撃（2008 年） ・ウクライナの電力網に対するマルウェア攻撃（2015 年）
Koala	Energetic Bear, Dragonfly, Group 24, Crouching Yeti	不明（ロシア政府が関与）	・エネルギー，原発，水，航空，重要製造業等に対する侵入（2014 年～）
TEMP.Armaggedon	-	不明（ロシア政府が関与）	・ウクライナの保安・法執行機関に対する攻撃
TEMP.Isotope	Dragonfly 2.0, Energetic Bear	不明（ロシア政府が関与）	・米国の電力網に対する侵入
TEMP.Veles	-	中央化学機械研究所（TsNIIKhM）	・産業用制御システム（ICM）に対する侵入

（出典）筆者作成

サイバー時代におけるロシアとの向き合い方

本稿の主な結論は次のとおりである．

第1に，ICTは，インテリジェンス機関が古典的な活動を新たな手段で継続するためのツールであり，しかもその効果はICTの普及によってきわめて大きくなっている．ことにロシアのインテリジェンス機関がSNSを用いて米国のような先進国の社会を大きく揺るがせたことは，今後の安全保障を構想する上で大きなインパクトを有しているといえよう．

第2に，ICTを用いたインテリジェンス機関の活動は物理領域にも及ぶようになっている．戦時の破壊活動や限定的な暗殺に限らず，きわめて低コストかつ短時間で社会や政治に混乱や破壊をもたらす能力をロシアのインテリジェンス機関は有するようになった．これは狭義のインテリジェンスという観点からのみロシアのインテリジェンス機関を理解することがますます困難になりつつあることを意味する．

第3に，ロシアのインテリジェンス機関は相互に独立して任務を遂行しており，単独の事案を阻止しても同じような事案が別の手段で遂行される可能性が高い．ここまで述べてきたことを併せて考えるならば，Check Point ResearchとIntezerが用いたような大規模な計量的手法によってロシアのインテリジェンス機関が有する能力を全体として把握し，抑止・対処戦略へとつなげる必要があろう．

参考文献

1) 小林良樹：インテリジェンスの基礎理論，立花書房，pp.6-8 (2011).
2) リチャード・クラーク，ロバート・ネイク：世界サイバー戦争，徳間書店（2011）．（原題：Richard A. Clark and Robert K. Knake : CYBER WARFARE : The Next Threat to National Security and What to Do About It, Harper Collins, 2010）．
3) CSIS, Significant Cyber Incidents, https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity
4) Carr, J. : Inside the Cyber Warfare : Mapping the Cyber Underground, O'Reilly, pp.118-119 (2011).
5) Cohen, I. and Bassat, O. B. : Mapping The Connections Inside Russia's APT Ecosystem, Check Point Research and Intezer (2019), https://research.checkpoint.com/2019/russianaptecosystem/

（2020年3月25日受付）

小泉　悠　nuclearblue1982@gmail.com

1982年千葉県生まれ．早稲田大学大学院政治学研究科修了（修士）．民間企業勤務，外務省専門分析員，ロシア科学アカデミー客員研究員，（公財）未来工学研究所特別研究員等を経て2019年より現職．ロシアの軍事・安全保障政策を専門とし，『「帝国」ロシアの地政学』（東京堂出版）等の著書がある．