日本大学大学院総合社会情報研究科紀要　No.13, 001-012 (2012)

ロシアのサイバー戦略
―「サイバー戦コンセプト」を中心に―

佐々木　孝博
日本大学大学院総合社会情報研究科

An Analysis of Russian Notion of Cyber Strategy
-In Reference to the Document "Conceptual Views Regarding the Activity of the Armed Forces of Russian Federation in the Information Space"-

SASAKI Takahiro
Nihon University, Graduate School of Social and Cultural Studies

This paper is concerned with latest trends in Russian military strategy which culminates in the notion of information space (cyber space). The author aims at making clear today's Russian way of thinking about Cyber Space and its meaning for the defense system of Russia. In the first place, Russian official documents concerning cyber issues are examined, and announcements and comments made by high-ranking officials are surveyed. The announcement made in March, 2012 by Deputy Prime Minister Dmitry Rogozin about a plan to set up a cyber-security command can be regarded as the most representative statement. Next, and more importantly, a thorough-going theoretical analysis of the document "Conceptual Views Regarding the Activity of the Armed Forces of Russian Federation in the Information Space" will be made, and the political and military world views underlying the document inquired into.

はじめに

2012 年 3 月 21 日、ドミートリー・オレゴヴィッチ・ロゴジン（Дмитрий Олегович Рогозин）ロシア副首相（防衛担当）は、ロシア軍の指揮管制システム及び軍事ネットワークを防護するために、米国はじめ西側主要国と同様にサイバー戦を統括する組織として「サイバーコマンド」を創設することを表明した。これに相前後してロシア国防省のホームページに、2011 年に制定された 14 ページからなる「情報空間（サイバー空間[(1)]）におけるロシア軍の活動に関するコンセプト（以後、〔ロシア軍〕サイバー戦コンセプトという）[(2)]」の全文が掲載された（発表年は同コンセプトの表紙に 2011 年との記載があるが、HP への掲載年月日は不詳）。これは、ロシア国防省が初めて発表したサイバー戦コンセプトである。これらの動きは、近年ロシアが情報安全保障（特にサイバー戦）を重要視し、各種施策を実行しつつあることを示すものである。

本稿においては、ロシアの情報安全保障に関する公文書体系を概観するとともに、国防省（軍）がサイバー戦コンセプトを制定することになった背景を考察していく。また、サイバー戦コンセプトを制定した時期に前後して確認された情報安全保障（特に

(1) 後述するプーチン首相（当時）の大統領選公約とも言える安全保障論文「強くあれ－ロシアの国家安全保障」(『ロシア新聞』2012 年 2 月 20 日）において、「情報空間」と「サイバー空間」をほぼ同義語として使用している。したがって、本稿においては必要に応じ「情報（空間）」と「サイバー（空間）」を併記、または読み替えることとする。

(2) 国防省「情報空間（サイバー空間）におけるロシア軍の活動に関するコンセプト」『国防省 HP』2011 年 <http://www.ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle&_print>(2012 年 5 月 2 日アクセス)。

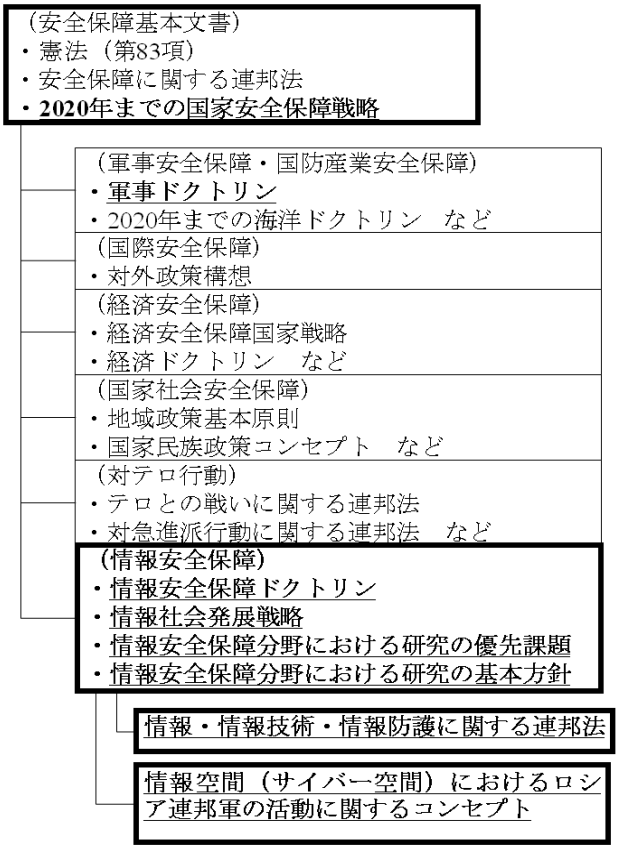
サイバー戦)に関する要人の発言についても考察し、今回公表されたサイバー戦コンセプトを分析することにより、ロシアが何を目標としているかを考察する。最後に、本サイバー戦コンセプトのもつ意義とその中核となる戦略を考えていきたい。

1　サイバー戦コンセプト制定の背景

(1) 情報安全保障に関する公文書体系(3)

ロシアの安全保障戦略を規定する最上位の公文書は「2020 年までの国家安全保障戦略 (4)」(2009 年)である。その細部を具体化する文書として、軍事安全保障については「軍事ドクトリン (5)」(2010 年)が、外交上の安全保障分野においては「対外政策構想」(2008 年) が定められている。同様に、情報安全保障に関しては「情報安全保障ドクトリン (6)」(2000 年) が制定されている。このほか、第 1 図に示す文書がある。

これらの中で、サイバー戦に関連する事項を規定する主要な文書は、「2020 年までの国家安全保障戦略」、「軍事ドクトリン」、「情報安全保障ドクトリン」である。さらに、その細部を規定するために、「情報社会発展戦略 (7)」(2008 年)、「情報・情報技術・情報防護に関する連邦法 (8)」(2006 年)、「情報安全保障分野における研究の優先課題 (9)」(2008 年) や「情報安全保障分野における研究の基本方針 (10)」(2008 年) などがある (第 1 図)。



出典：安全保障会議「ドキュメント：ロシア国家安全保障」『安全保障会議 HP』<http://www.scrf.gov.ru/documents/sections/3/>(2012 年 5 月 21 日アクセス)、注(2)資料及び注(8)資料から作成

第 1 図　情報安全保障に関する公文書体系

これらサイバー戦に関する公文書体系はピラミッド状に系統立っているものの、肝心の実施主体たる国防省 (軍) が具体的に実施する事項やサイバー情報活動に関する事項を規定するものは、今回の「ロ

(3) 拙稿「多面的なロシアのサイバー戦－組織・戦略・能力－」『ディフェンス』49 号 (隊友会、2011 年 10 月 17 日) 141 頁。
(4) 安全保障会議「2020 年までのロシア連邦国家安全保障戦略」『安全保障会議 HP』2009 年 5 月 12 日<http://www.scrf.gov.ru/documents/99.html>(2011 年 4 月 18 日アクセス)。
(5) 安全保障会議「ロシア連邦軍事ドクトリン」『安全保障会議 HP』2010 年 2 月 5 日<http://www.scrf.gov.ru/documents/33.html>(2011 年 4 月 18 日アクセス)。
(6) 安全保障会議「情報安全保障ドクトリン」『安全保障会議 HP』2000 年 9 月 9 日<http://www.scrf.gov.ru/documents/5.html>(2011 年 4 月 18 日アクセス)。
(7) 安全保障会議「情報社会発展戦略」『安全保障会議 HP』2008 年 2 月 7 日<http://www.scrf.gov.ru/documents/90.html>(2011 年 4 月 18 日アクセス)。
(8) 大統領府「情報・情報技術・情報防護に関する連邦法」『安全保障会議 HP』2006 年 7 月 8 日<http://www.internet-law.ru/law/inflaw/inf.htm>(2011 年 4 月 18 日アクセス)。
(9) 安全保障会議「情報安全保障分野における研究の優先課題」『安全保障会議 HP』2008 年 3 月 7 日<http://www.scrf.gov.ru/documents/5.html>(2011 年 4 月 18 日アクセス)。
(10) 安全保障会議「情報安全保障分野における研究の基本的方向性」『安全保障会議 HP』2008 年 3 月 7 日<http://www.scrf.gov.ru/documents/5.html>(2011 年 4 月 18 日アクセス)。

シア軍サイバー戦コンセプト」が初めてである。

（2）米国におけるサイバーコマンドの創設とサイバー戦略の制定

2010 年 9 月、米国のウィリアム・リン（William J. Lynn III）国防副長官（当時）は「新たな領域の防衛―国防総省のサイバー戦略―」と題する論文を発表した。その中で、2008 年に中東における米国防総省の秘匿コンピューターが USB メモリーによりウイルス感染されたのを発端として、秘匿ネットワーク全体が深刻な危機に晒されたことを明らかにした(11)。これを教訓として、米国は国防総省の軍事ネットワークの重層的かつ強固な防御策を構築し、各々の軍種が個別に防護していた体制を見直し、サイバー戦を統括する組織としてのサイバーコマンドを創設した。そして、サイバー空間というものを、陸、海、空、宇宙に次ぐ第 5 の戦闘領域として認識し、それに伴って、戦略、組織も新たに構築しなければならないとした。

さらにこれを受け、翌 2011 年 5 月には、ホワイトハウスが「サイバー空間のための国際戦略」を、同年 7 月には、国防総省が「サイバー空間での作戦に関する国防総省戦略」を公表した。

このような、米国のサイバーコマンドの創設やサイバー戦略制定の動きに対応し、かつそれを詳細に分析し、ロシア軍に取り入れようとする動きがみられる。

（3）イランにおける原発へのサイバー攻撃事例

2010 年 9 月 28 日、イラン鉱工業省の情報技術部門幹部の話として、イランが海外からの大規模なサイバー攻撃を受けており、産業用パソコン約 3 万台に感染が見つかったとの報道があった(12)。また同年 11 月 16 日、IAEA（国際原子力機関）により、イラン中部のナタンツ地区のウラン濃縮施設で約 8,400 台の遠心分離機がすべて停止していることが確認された(13)。さらに 11 月 29 日、イランのマフムード・アフマディネジャド（Mahmoud Ahmadi Nejad）大統領は、同国のウラン濃縮施設の遠心分離機がコンピューターウイルスに感染していたことを明らかにした(14)。

これについては後になって、セキュリティベンダーのシマンテック社が「スタックスネット」というウイルスによって引き起こされた事例であるという分析レポートを発表している(15)。

スタックスネットそのものは、2010 年の 7 月中旬に出現し、Windows の脆弱性を悪用して主として USB メモリーにより感染を引き起こし、感染後はネットワーク上で自己増殖するウイルスである。スタックスネットが注目されるのは、ドイツのシーメンス社製電力制御系ソフトウエアを攻撃対象にしていたことにある。このため、同社製の電力制御ソフトウエアを使用していたイランの核濃縮施設の遠心分離機が停止してしまったのである。このスタックスネットの事例は、サイバー戦の世界では 9.11 テロと同等の衝撃を我々に与え、それまで信じられていた安全神話を崩壊させた。スタックスネット出現以前の「インターネットとは繋がっていない特殊な制御システムや管制システムはサイバー攻撃とは無縁だ」という神話を崩壊させてしまったのである。

すなわち、クローズなシステムへのサイバー攻撃というものが可能であり、敵のあらゆる制御システムや管制システムを無力化するのに最も有効な手段

(11) W.J.リン「新たな領域の防衛－国防総省のサイバー戦略－」『フォーリン・アフェアーズ』第 89 巻第 5 号（2010 年 9/10 月号）97-108 頁。

(12) トレンドマイクロ「イランで産業用パソコン 3 万台からウイルス感染」『トレンドマイクロ HP』2010 年 9 月 28 日<http://is702.jp/news/804/partner/80>(2012 年 5 月 2 日アクセス)。

(13) AFPBB News「ウラン濃縮一時停止の謎、サイバー攻撃か設備の更新か」『AFPBB HP』 2010 年 12 月 1 日<http://www.afpbb.com/article/politics/2777480/6535286>(2012 年 5 月 2 日アクセス)。

(14) ロイター通信「イラン大統領が核施設サイバー攻撃認める、6 カ国協議再開も表明」『ロイターHP』2010 年 11 月 30 日<http://jp.reuters.com/article/topNews/idJPJAPAN-18395820101130>(2012 年 5 月 2 日アクセス)。

(15) シマンテック「Stuxnet:画期的な解明」『シマンテック HP』2010 年 11 月 30 日<http://www.symantec.com/connect/blogs/stuxnet-6>(2012 年 5 月 2 日アクセス)。本分析レポートによれば、攻撃技法については明らかになったが、攻撃源や攻撃主体については明らかになっていない。

であることが証明されたのである。

（4）エストニアにおけるサイバー攻撃事例[16]

2007 年 4 月、エストニア政府が同国を解放した旧ソ連軍兵士の像を首都タリン市郊外に移設しようとしたことをきっかけとして、エストニアのコンピューター・ネットワーク及び重要インフラに対し、サイバー攻撃が行われた。

このサイバー攻撃には、分散型サービス拒否攻撃（DDoS 攻撃: Distributed Denial of Service 攻撃[17]）及びウェブ改ざん攻撃[18]といった手法が用いられた。その結果、攻撃対象であった政府機関、通信事業者、メディアや銀行は一時麻痺状態に陥ってしまった[19]。

2009 年の 3 月になって、ロシア政権を強力に支援する青年組織「ナーシ（ロシア語の『我々の』の意）」の幹部であるコンスタンチン・ゴロスココフ（Константин Голоскоков）が英フィナンシャル・タイムズ紙に、自分とその仲間が 2007 年のエストニアに対するサイバー攻撃を行ったことを話した。また、エストニア政府に対して、「彼らが違法なことを行えば、我々が相応の方法で仕返しを行うという教訓を教えてやった」とも付言した。さらに、この攻撃を「我々は、違法行為を行った訳ではなく、単にエストニアのいろいろなサイトを繰り返し訪問しているうちに、それらのサイトの活動が停止してしまった。彼らの能力の限界が引き起こしたものだ」と述べ、自己の行為を正当化するとともに、ロシア政権の関与については否定した[20]。

しかし、「ナーシ」は以前から、ロシア政権の強い影響を受け、政権に反対する勢力に対しデモ活動を行うなどの疑惑が持たれている青年組織である。本サイバー攻撃が生起した前後に、在モスクワのエストニア大使館前において、デモや騒音による嫌がらせを実施している。これまで述べてきた政権と同組織の関係を鑑みると、本サイバー攻撃についても、政権の何らかの関与があった可能性が高い。

本事例は、実施主体は明確ではないものの、重要インフラに対する大規模なサイバー攻撃は、国家機能を麻痺させることが可能となることを証明した世界初の事例であった。エストニアは、高度に IT 化された社会であったため、サイバー攻撃に対する影響は甚大であり、そのような社会は、サイバー攻撃に対し非常に脆弱なことを示した。

（5）グルジア紛争におけるサイバー攻撃事例[21]

2008 年 8 月、民間サイトの扇動により行われたとされるグルジアへのサイバー攻撃も、軍事行動と同時に実施されたタイミングなどを考慮すると、ロシア政権の関与が疑われている。

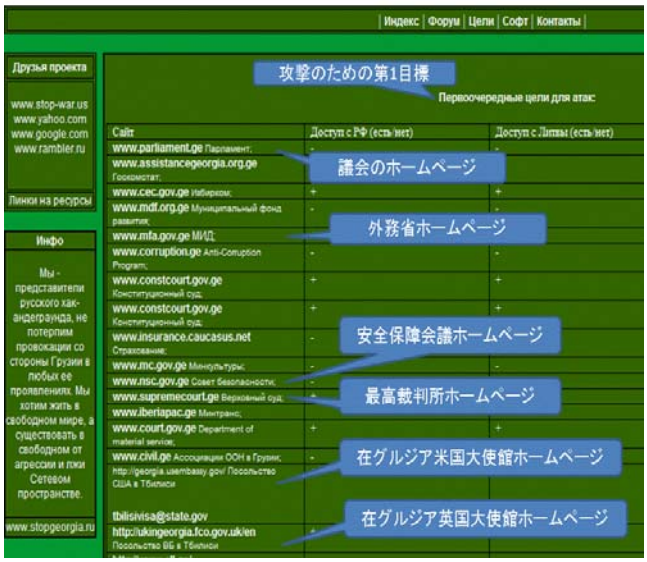
本事例を「グレー・グース」という米国の官民合同の情報セキュリティ専門のプロジェクトチームが詳細に分析を行った。それによれば、「StopGeorgia.ru」というロシアに所在する民間フォーラムが、標的となるグルジア政府のウェブサイトのリストを公開し、同ウェブサイトへのアクセスを不能とするための方法を伝授するという形式でサイバー攻撃を扇動していたことを突き止めた。また、「StopGeorgia.ru」のサイトは、グルジア紛争における地上戦が開始される数時間前に出現し、運営されていたことも明らかにした[22]。

---

(16) 拙稿「多面的なロシアのサイバー戦」138 頁。
(17) DDoS（Distributed Denial of Service）攻撃とは、分散された複数のコンピューターから、サーバーに大量のデータを送って多大な負担をかけ、機能停止に追い込むサイバー攻撃法。
(18) Web ページのデータや設定を書き換える不正行為。サイバー攻撃でも用いられる。
(19) オクスフォード・アナリティカ「ロシア: サイバー攻撃は広範な政治目的を反映している」『オクスフォード・アナリティカ HP』2010 年 3 月 2 日<http://www.oxan.com/display.aspx?StoryDate=20100302&ProductCode=CISDB&StoryNumber=1&StoryType=DB>(2012 年 4 月 11 日アクセス)。
(20) フィナンシャル・タイムズ「クレムリンが後援するグループがエストニアに対するサイバー攻撃の背後に存在」『フィナンシャル・タイムズ HP』2009 年 3 月 11 日<http://www.ft.com/cms/s/0/57536d5a-0ddc-8ea3-0000779fd2ac.html>(2012 年 4 月 11 日アクセス)。
(21) 拙稿「多面的なロシアのサイバー戦」139 頁。
(22) ワシントン・ポスト「ロシアのハッカーフォーラムがグルジアに対するサイバー攻撃を煽る」『ワシントン・ポスト HP』2008 年 10 月 16 日<http://voices.washingtonpost.com/securityfix/2008/10report_russian_hacker_forums_f.html>(2012 年 4 月 11 日アクセス)。

「StopGeorgia.ru」がなぜそのようなタイミングで運営を始め、結果としてロシアの多数の民間ハッカーを扇動し、グルジア政府のウェブサイトを攻撃することが可能であったのか。その鍵は、武力攻撃の時機に関する情報を事前に知っていたからではないかということである。

軍事行動を有利にするためにサイバー攻撃を実施する場合、攻撃目標、攻撃時機、実施要領等が軍事行動と密接にリンクされていなければその効果は限定的である。個人的なサイバー攻撃（ハッカー攻撃）では、国家からの情報や要請とは無関係で、自由にサイバー攻撃をするだけであるので、軍事行動と関係はない。他方、本事例においては、前述のような情報が「StopGeorgia.ru」フォーラムのサイトに公開されていた（第 2 図）。



出典：Coordinated Russia vs Georgia Cyber Attack in Progress, *ZDNet HP,* August 11, 2008　<http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670>(2012 年 5 月 2 日アクセス)より作成。

第 2 図「StopGeorgia.ru」フォーラムが示したグルジア政府関係機関の攻撃目標リスト

したがって、軍事行動とサイバー攻撃が同時に行われたこと、及びグルジア軍のインターネットを使った情報収集機能や連絡・調整機能を麻痺させ、ネットを使った政治的プロパガンダを封じてしまったという結果から考えると、ロシア政権と「StopGeorgia.ru」フォーラムが何らかの関係を有していたとするのが妥当である。

すなわち、本事例は、物理的な軍事攻撃と同時になされた史上初のサイバー攻撃事例であり、サイバー攻撃が単なる犯罪やテロの域を超えて戦争・紛争の一手段として用いられた最初の事例である。

2　情報安全保障（サイバー戦）に関するロシア要人の発言

（1）メドベージェフ大統領（当時）の米ミサイル防衛システムへの対抗措置発言

2011 年 11 月 23 日、ドミートリー・アナトリエヴィッチ・メドベージェフ（Дмитрий Анатольевич Медведев）大統領（当時）は、米国及び NATO のミサイル防衛計画が継続する場合には 5 つの対抗措置を採ると発言した(23)。その 1 つにおいて「私（メドベージェフ大統領）はロシア軍に対し、ミサイル防衛システムの情報交換機能及び情報管制機能を破壊する兵器の開発を命じた。それは非常に効果的で簡単に開発ができるとともに安価である」と述べた。ミサイル防衛システム等の情報管制機能を破壊するには、ピンポイントで攻撃できる高性能なミサイルなどの物理的な破壊兵器が効果的である。だが、そのような高性能な兵器の開発には莫大な予算と時間がかかる。それが簡単に開発でき安価であるとの条件を満たすもの、それはサイバー兵器に他ならない。既に述べたとおり、イランの原子力発電施設の遠心分離機の管制システムがサイバー攻撃によって被害を受けた「スタックスネット」の事例は記憶に新しい。ロシアがスタックスネットの事例を検証し、サイバー攻撃が最も効果的だと判断し、ミサイル防衛

(23) D.A メドベージェフ「メドベージェフ大統領は西側ミサイル防衛に対する対抗措置を強調」『RT　HP』2011 年 11 月 23 日<http://rt.com/politics/official-word/missile-defense-medvedev-offensive-051/print>(2011 年 11 月 24 日アクセス)。5 つの対抗手段のうち残りの 4 つは、「①カリニングラードの早期警戒レーダーを可動状態にする、②戦略核戦力部隊に導入される装備の防御能力を強化する、③導入される戦略弾道ミサイルに高度なミサイル防衛網を突破する能力及び最新の効果的な弾頭を付加する、④欧州のミサイル防衛システムに対する高度な攻撃兵器を配備する」である。

システムへの対抗措置の 1 つとして考えたのも理にかなっている。すなわち、ロシアはこの大統領の発言によって、西側のミサイル防衛システムが構築された暁にはサイバー攻撃をもってそれに対抗するということを明言したのである。

サイバー攻撃の実施について明言している国は、権利を留保するとした米国の他にはない状況である。そのような見地からメドベージェフ大統領（当時）による本発言は注目に値する。

（2）マカロフ参謀総長のサイバー戦への準備発言

翌 2012 年 1 月 28 日にニコライ・エゴーロヴィッチ・マカロフ（Николай Егорович Макаров）参謀総長は、軍事学アカデミーの会議において、ロシアは宇宙空間及びネットワーク空間での戦争の準備をしなければならないとの発言を行った[24]。また、「周知のとおり、戦争の中心（核心）は、陸上と海上での伝統的な戦争空間から、航空・宇宙空間及びサイバーセキュリティを含む情報分野に転換した。ネットワーク中心の戦争の概念は、大きな進歩を遂げている。我々は、このような課題を欧米先進国ではどのように解決しているかを承知している。また、現代の戦争は短時間で雌雄を決することになったので、戦争の初期段階がその経過と結末に決定的な影響力を持ち始めた。さらに、軍の活動をより高いレベルにするために、兵士の数を削減することを強いることになった」と述べた。

この発言の時期は、サイバー戦コンセプトをまとめあげ、後述のサイバーコマンドを創設すると決心した時期と合致しており、発言内容を裏付けるものである。

（3）ロゴジン副首相のサイバーコマンド創設に関する発言

同じく 2012 年 3 月 21 日、冒頭に述べたようにロゴジン副首相は、米国や NATO 諸国と同様にロシア軍の使用する軍事システム及びネットワークを防護するためにサイバーコマンドを創設することを表明した[25]。米国と同様にサイバーコマンドを国防省隷下に創設するとなると、サイバー戦に関する主管を国防省が担うことになる。また、このことは、サイバー戦の攻防一体の軍事組織を国防省隷下に新たに設けることを意味しており、サイバー戦における国防省の立場を明確にしている。

（4）プーチン首相（当時）の安全保障論文

同年 1 月から 2 月にかけて、ウラジーミル・ウラジーミロヴィッチ・プーチン（Владимир Владимирович Путин）首相（当時）は、3 月の大統領選挙における選挙公約とも言える 7 つの論文を公表した[26]。その 6 番目の論文は「強くあれ－ロシアの国家安全保障[27]」という安全保障に関する基本方針を述べたものであった。

その中でスマートな国防と言うことが重視されており、サイバー戦については「宇宙空間及び情報戦空間（一義的にはサイバー戦）における軍事的能力は軍事紛争の結末をつけるにあたって決定的ではないにしろ重要な意義をもつことになる。（中略）これらは全て核兵器とならんで政治・戦略的目的を達成するための質的に新しい手段となりうるものである。このような兵器システムは核兵器に匹敵する効果をもたらす一方で、政治・軍事的計画においてより受

(24) N.E.マカロフ「ロシアは宇宙・サイバー戦のための準備をしなければならない」『RIA ノーヴォスチ HP』2012 年 1 月 28 日<http://ria.ru/defense_safety/20120128/551041170-print.html>(2012 年 1 月 30 日アクセス)。

(25) D.O.ロゴジン「ロシアはサイバーコマンドを考えている」『RIA ノーヴォスチ HP』2012 年 3 月 21 日 < http://en.rian.ru/russia/20120321/172301330.html>(2012 年 3 月 22 日アクセス)。

(26) 7 つの論文は、①「ロシアは結集しつつある。我々が回答すべき条件」『イズベスチア』2012 年 1 月 16 日、②「民族問題」『独立新聞』1 月 23 日、③「我々の経済的課題について」『ヴェドモスチ』1 月 30 日、④「民主主義と国家の質」『コメルサント』2 月 6 日、⑤「公平さの構築：ロシアのための社会政策」『コムソモリスカヤ・プラウダ』2 月 13 日、⑥「強くあれ－ロシアの国家安全保障」『ロシア新聞』2 月 20 日、⑦「ロシアと変わりゆく世界」『モスクワ・ニュース』2 月 27 日である。

(27) V.V.プーチン「強くあれ－ロシアの国家安全保障」『ロシア新聞』2012 年 2 月 20 日<http://www.rg.ru/printable/2012/02/20/putin-armiya.html>(2012 年 5 月 23 日アクセス)。

け入れられやすい」と言及した。すなわち、サイバー戦が決定的ではないにしろ、ロシアが安全保障の拠り所にしている核兵器に匹敵する効果が得られるものであり、また、その使用のしきい値が低いと認識していることを示している。

3　「サイバー戦コンセプト[28]」の概要

(1) サイバー戦の定義と位置付け

サイバー戦コンセプトの冒頭(第 1 項)において、サイバー戦関連の用語について、次のように定義している。

① 情報空間（サイバー空間）での軍事紛争：情報兵器を使用した国内外の紛争を解決する形態
② 情報空間(サイバー空間)における軍事活動：防衛・安全保障の課題を解決するための軍事情報資源の活用
③ 情報セキュリティ部隊：情報戦（サイバー戦）の影響から、情報資源の安全確保を担う部隊
④ 情報戦（サイバー戦）：情報システム、情報プロセス及び情報資源、その他の重要インフラを破壊させるための、情報空間（サイバー空間）における 2 ないしそれ以上の国家間の争い
⑤ 情報インフラ：情報の収集、作成、処理、伝達、使用及び蓄積のための技術的手段（ツール）やシステムの総称
⑥ 情報兵器（サイバー兵器）：情報戦（サイバー戦）を行うために使用される情報技術、手段（ツール）及び手法
⑦ 情報空間（サイバー空間）：個人と社会、情報インフラと実際の情報に影響を与えるような情報の収集、作成、処理、伝達、使用及び蓄積に関連する活動の空間
⑧ 情報資源：実際の情報とその流れ
⑨ 危機の状態：紛争を解決するために軍事力を使用することによって特徴づけられる紛争のエスカレーションの段階

Введение（はじめに）
1　Основные термины и определения（基本的な用語と定義）
2　Принципы（原則）
2.1 Законность（法の秩序）
2.2 Приоритетность（優先度）
2.3 Комплексность（複雑性）
2.4 Взаимодействие（協同）
2.5 Сотрудничество（協力）
2.6 Инновационность（イノベーション）
3　Правила（規則）
3.1 Сдерживание и предотвращение конфликтов（抑止と紛争予防）
3.2 Разрешение конфликтов（紛争解決）
4　Меры доверия（信頼醸成措置）
Заключение（おわりに）

出典：国防省「情報空間（サイバー空間）におけるロシア軍の活動に関するコンセプト」『国防省 HP』2011 年 <http://www.ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle>(2012 年 5 月 4 日アクセス)より作成。

第 3 図　サイバー戦コンセプトの表紙と目次

(28) 国防省「情報空間（サイバー空間）におけるロシア軍の活動に関するコンセプト」。

⑩　国際的な情報安全保障：情報分野において、全世界的な安定を阻害し、国家及び世界の安全への脅威を排除できるような国際関係の状態
⑪　ロシアの情報安全保障システム：情報安全保障分野における国家政策を具現化するための国家安全保障の一部

この中で、特に第④項に注目したい。情報戦（サイバー戦）というものを単なるサイバー犯罪やサイバーテロと捉えているのではなく、情報空間（サイバー空間）における国家間の争い（紛争）と定義づけていることである。

（2）サイバー戦の原則

サイバー戦コンセプト第 2 項（原則）において、情報戦（サイバー戦）の根本原則を「情報空間（サイバー空間)におけるロシア軍の活動は､法の秩序、優先度、複雑性、協同、協力及び技術革新（イノベーション)という一連の原則に基づいて構築される」と位置づけている。この中で、法の秩序と（各省庁の）協同の言葉に注目したい。

法の秩序の項目（第 2.1 項）では､「2010 年の『軍事ドクトリン』におけるロシア軍の国外での使用条件をサイバー空間にまで拡大する必要性があること」を規定している。また、グローバルなサイバー空間での軍事活動の特殊性に関し､「ロシア軍は､国家主権の尊重、他国への内政不干渉、軍の使用及び軍の脅威、個別的または集団的自衛権の原則によって導かれる」とした。さらに、ロシア軍は､「国際人道法（情報兵器〔サイバー兵器〕の無差別使用の制限、人為的な危害及び危険な情報戦の手法の禁止などの原則）の規範に導かれている」とした。つまり、サイバー空間は特殊な戦闘領域ではあるものの従来からの国際法の原則を適用すべきであるとの姿勢を示している。

協同の項目（第 2.4 項）では、2000 年の「情報安全保障ドクトリン」の範囲内で省庁間の相互協力が実施されるとしている。その中で､「ロシア国防省が他の連邦執行機関と情報空間（サイバー空間）での行動を調整する」と国防省の優位も規定した。

（3）サイバー戦における抑止と紛争予防及び紛争解決

本コンセプト第 3 項（規則）には、サイバー戦における「抑止と紛争予防」及び「紛争解決」という物理的な戦争・紛争への対応をサイバー戦に適応させる方針を打ち出している。

ア　サイバー空間における抑止と紛争予防

まず、第 3.1 項（抑止と紛争予防）において、情報空間（サイバー空間）でのロシア軍の抑止と紛争予防活動は、次の原則により導かれるとしている。

①　情報空間（サイバー空間）における武力紛争を解決するためにロシア軍は情報セキュリティを確保するシステムを開発すること
②　情報空間（サイバー空間）における軍事・政治的性質への脅威を撃退するため、常続的な準備度（レディネス）において、セキュリティを高める手段の強度を維持すること
③　パートナー国との輪を広げ、共通的な利益に基づいて国家間連携を発展させるために　国連憲章や他の国際法の規範に従い、集団安全保障条約機構（CSTO)、独立国家共同体（CIS)、上海協力機構（SCO）と優先的に協力すること
④　情報空間（サイバー空間）で一般的に認められている規範と国際法の原則の適用を拡大するために、国際的な情報セキュリティを確保するための国連での条約の締結を追及すること
⑤　情報空間（サイバー空間）における潜在的な軍事衝突の可能性を早期に偵知するだけでなく、紛争の首謀者(国)､扇動者(国)及び共犯者(国)を明らかにすること
⑥　紛争の発生（とその拡大）の要因を識別し、緊急事態を回避するためにそれらをコントロールすること
⑦　大幅にコストの増加を要するような紛争の拡大とその転換に対応するための緊急措置を採ること
⑧　コストと労力が必要となるような、周辺国への紛争の拡大を回避する手順を遂行すること
⑨　建設的な協力の方向性において、紛争当事者

間に相互協力を行わせるために、紛争を引き起こした要因を解明し、中立化する措置を講じること
⑩　国際社会に説明するための公的、客観的かつ適時の手法を採ること

イ　サイバー空間における紛争解決

また、第 3.2 項（紛争解決）において、次の原則により、ロシア軍は情報空間（サイバー空間）における軍事紛争を解決すると規定している。

①　国連安全保障理事会、地域的機関及び条約、その他の平和的手段に対する交渉、調停、控訴によって、一義的に情報空間（サイバー空間）における軍事紛争を解決する。
②　緊張の場合には、国際情勢の不安定化や危機の出現を導くような特に極端な破壊的な戦争の形態を回避する。
③　情報空間（サイバー空間）での紛争のエスカレーション及びその危機の段階への転換に伴い、国際法の普遍的に認められた規範と原則に矛盾しない手段により、個別的及び集団的自衛権を行使する。
④　個別的及び集団的自衛権の課題を解決するため、国の民主的な手続きに基づいて対処の方法（大きさ）を決定する。その際、国際的な安全や安定の必要性と同様に他国の安全保障上の正当な国益をも考慮する。
⑤　個別的及び集団的自衛権上の国益に際しては、他国との交渉中に自主的に作用する合意や国際法に従って、他国の領土において安全を確保するための部隊とそのための手段を配置する。
⑥　紛争時には、拡大（エスカレーション）を減少し、紛争対立を解決する成果を確定するのに効果的に影響するような世論に基づいて形成される情勢について、国内外のメディアを継続的に把握する。

抑止と紛争予防及び紛争解決に関するいずれの規定についても従来の物理的な手法を情報空間（サイバー空間）に適用しているのが特徴的である。特に紛争の解決については、米国も公文書としては言及していないサイバー空間での集団的自衛権の行使にまで踏み込んでいることから、サイバー戦分野において米国よりも先んじたい、あるいはサイバー戦分野における国際規範はロシアが主導して作るのだ[29]という国家の強い意志を示している。

（4）サイバー戦における信頼醸成措置

さらに、本コンセプト第 4 項（信頼醸成措置）には、ロシア軍は情報空間（サイバー空間）の軍事利用における信頼醸成措置を次の原則に従い実施することを定めている。

①　情報空間（サイバー空間）における国家安全保障構想（コンセプト）の交換
②　情報空間（サイバー空間）における危機的な事例や脅威、及びそれらの解決や安定化のために採られた措置に関する情報の迅速な交換
③　軍事的性質の紛争を解決する際の当事者間の懸念や協力を呼び起こすような、情報空間（サイバー空間）における活動についての協議

どの国も言及していない「情報空間（サイバー空間）における信頼醸成措置」の具体的な内容についても言及していることから、前項同様米国に対抗してサイバー戦分野において国際的なイニシアティブを採りたいとするロシアの強い姿勢が窺える。

（5）サイバー戦コンセプトの総括

本コンセプト最終項（おわりに）において、コンセプトの内容を次のとおり総括している。

①　現状では、ロシアの国防は情報空間（サイバー空間）における軍の有効性に依存している。それは、主としてサイバー空間で発生する紛争を抑止し、予防し、解決することのできる軍の能力よって達成される。

(29) ロシアは、中国とともにサイバー空間を米国が主張するような自由な空間としてではなく、規制すべき空間であるとの国際規範を作ろうとする動きをし始めている。

② ロシア軍は、情報空間（サイバー空間）において、信頼醸成措置はもちろんロシア軍の基本的な原則と規範に基づいて、直面する国防と安全保障の課題に対処するための計画を策定する。
③ 本コンセプトを実現し、世界全体に対し国際的な情報安全保障の枠組みの形成を追及するとともに、ロシア軍は、国家を防衛し、軍事紛争を抑止・予防し、軍事協力を強化するようなサイバー空間の活用を最大限に追求していく。

これらの総括から、国内的には、国防省（軍）が主導的にサイバー戦を実施していくという姿勢、対外的には、国際社会においてロシアがサイバー戦を主導していくのだという強い国家意志が表れている。

4 サイバー戦コンセプトの意義とその戦略

(1) サイバー攻撃に関する考察

本コンセプトにおける､定義そのものから言えば、ロシア軍が「サイバー攻撃」についてどのように考えているかは曖昧である。しかしながら、コンセプトの記述内容及びその行間からロシア軍がサイバー攻撃を明らかに考えていることが分かる。

その理由の第 1 は、本コンセプト第 3.2 項（紛争解決）の冒頭に「ロシア連邦軍は、次に導かれる規則によって情報空間（サイバー空間）における武力紛争を解決する」と記述していることである。軍が武力紛争を解決するといった場合、その中には当然敵に対する攻撃が含まれているのは言うまでもない。また、先に述べたとおり第 2.1 項（法の秩序）において､「ロシア連邦軍の国外における使用については、議会の関連規定に基づいて大統領が決定するものであり、その規定は、情報空間（サイバー空間）におけるロシア軍の使用にも拡張する必要がある」としていることである。この規定は、ロシア国外における連邦軍の使用について定めた「軍事ドクトリン」の規定をサイバー空間にも適用するものであり、物理的な軍事力の使用とサイバー空間での軍事力の使用を同等に扱うべきだとした規定である｡すなわち、ロシアの国益に適い関連法規の規定の下、大統領の決定があればロシア国外においてサイバー攻撃を実施すると明言したに等しい。

また、コンセプトに先立つ前述のメドベージェフ前大統領による NATO のミサイル防衛システムに対する対抗措置に関する発言も、本コンセプトの内容を裏付けている。

ロシアがこのようにサイバー攻撃に関するスタンスを明らかにする背景には、前述のように、サイバー戦分野における国際規範をロシアのイニシアティブによって作りたい、ロシアの国益に見合うように国際規範を定めたいとの強い意志があるものと考える。

(2) コンセプトを国防省が制定した意味

本コンセプトは、前述のとおりロシア国防省が初めて制定したサイバー戦に関する規定である。上位文書である｢2020 年までの国家安全保障戦略｣や｢軍事ドクトリン」及び「情報安全保障ドクトリン」については、安全保障会議が制定している。そこで、なぜ本コンセプトは国防省が制定することになったのかを考えてみたい。

先の 3 つの上位文書を読むと、当該事項に関する各省庁の役割が概ね読み取ることができる。すなわち、各省庁にまたがるような統制・調整事項が大きな問題である場合には安全保障会議が規定しているとみて間違いない。今回のサイバー戦コンセプトを国防省が制定したということは、サイバー戦を主導していく機関は国防省であり、国防省が他の省庁の上に立って調整する（場合によっては統制事項も含まれる）という決定がなされたと考えられる。その証左は、前述のとおり、本コンセプト第 2.4 項（協同）において､「ロシア国防省が、他の連邦執行機関と情報空間（サイバー空間）での行動を調整する」としており、他省庁との調整は国防省が主管するということを明確に定めている。

では、これまで情報戦・サイバー戦において重要な地位を占めているとみられた連邦保安庁はどのような任務と役割を保有するのかという疑問がでてくる。サイバー戦はそもそもコンピューター・ネットワーク防衛（Computer Network Defense: CND）、同攻撃（Computer Network Attack: CNA）及び同情報活動（Computer Network Exploitation: CNE）から成り立っている。今回のコンセプトによって、コンピュータ

ー・ネットワーク防衛と同攻撃については国防省（軍）の主管に、同情報活動については連邦保安庁の主管とする決定がなされたものとみられる。

その結果として、安全保障会議の下部組織として存在する「情報安全保障に関する省庁合同委員会[30]」（委員長：安全保障会議書記補佐官〔Помощник Секретаря〕）の役職や構成員にも変化があるかもしれない。例えば、現在、副委員長は連邦保安庁副長官であるが、今後このような重要なポストに国防省の高官が任命される可能性もでてくる。

（3）サイバーコマンド創設の意義

コンセプトの発表に前後して、前述のようにロゴジン副首相はロシア軍の軍事ネットワーク及びシステムを防護するために「サイバーコマンド」の創設を発表した[31]。この発表がコンセプト制定と時期を同じくしたのは、コンセプトの内容を具現化したに他ならない。すなわち、コンセプトで示されていた「ロシア国外でのロシア軍のサイバー空間での使用」及び「国防省が主管となり他省庁を調整する」ための実働部隊として「サイバーコマンド」を創設することにしたのである。前述のとおり、ロシア国外でサイバー戦を行うのは国防省である。今までもロシア軍にはサイバーに関連する組織として参謀本部情報総局や通信部隊があったが、攻防一体としてのサイバー戦を行うには不十分であった。サイバー戦コンセプトが制定され軍が主管機関となったので、具体的にサイバー戦を実行する実働部隊としてサイバーコマンドを創設するのである。

（4）サイバー演習場（サイバーレンジ）導入の動き

ロゴジン副首相は、サイバーコマンド創設発言を行った時、「政府は、高等軍事研究局（Advanced Military Research Agency）の設置のための予算を計画している」とも述べた[32]。この組織は、同副首相によると米国の国防高等研究計画局（DARPA: Defense Advanced Research Project Agency）と類似のものである。米国の DARPA には、国家サイバー演習場（National Cyber Range）があり、サイバー戦に関する総合演習・訓練、システムの脆弱性点検、ネットワーク・システム導入時の検査などに重要な役割を担っている。サイバーコマンド創設計画と同時にこの高等軍事研究局設置計画を発表したことから、両者は密接に関わり合っており、ロシアも総合的なサイバー演習場の設置を計画しているとみるのが妥当である。コンセプトで述べられたサイバー戦に関する諸活動を実施するには組織はもちろん実際の運用を効果あるものにするため、総合演習の実施、装備の点検、個々の教育訓練が必要であり、それを具現化するには、サイバー演習場は不可欠なものである。

（5）プーチン論文とサイバー戦コンセプト

前述のように、プーチン首相（当時）は大統領選に先立ち選挙公約とも言える安全保障論文を発表した[33]。その中で「特にサイバー空間における軍事能力が軍事的な戦争の性格を決定する上で大きな意義を有する」と明言した。これは次期大統領として、戦争・紛争の捉え方を新たにしたものであり、そのようなプーチン首相（当時）の意識改革が、今回の新たな軍のサイバー戦コンセプトの策定に深く関係していたものと考えられる。

サイバー戦コンセプトの策定やサイバーコマンドの創設並びに高等軍事研究局の設置などの最近のサイバー関連事象については、これまで見てきたように初めての事項が多々あり、プーチン現大統領のような実力者からのトップダウンの指示がなければ達成できないものである。

おわりに

ロシア国防省はサイバー戦に関するコンセプトをまとめあげ、サイバーに関する問題を単なる情報保証やサイバーテロ、サイバー犯罪と捉えるのではな

(30) 安全保障会議「情報安全保障に関する省庁合同委員会のメンバー」『安全保障会議 HP』2006 年 6 月 12 日<http://www.scrf.gov.ru/documents/46.html>(2011 年 4 月 18 日アクセス)。
(31) D.O.ロゴジン「ロシアはサイバーコマンドを考えている」。
(32) 同上。
(33) V.V.プーチン「強くあれ－ロシアの国家安全保障」。

く、広く戦争・紛争の一部であり、情報戦の一環としてのサイバー戦として捉えることを公表した。そして、その中核を担うのはこれまで主担当であった連邦保安庁ではなく、サイバー攻撃・サイバー防衛能力を併せもつ軍事組織サイバーコマンドを創設する国防省（軍）であるということを明確にした。さらに、コンセプトで明記はされていないものの、サイバー攻撃については、物理的な戦争・紛争の原則を適用し、ロシアの国益に否定的な影響を及ぼす場合には、大統領の決定により、ロシア領土外においてもサイバー攻撃を行うことを示している。

すなわち、米国の他には世界中のどの国もサイバー攻撃について明確に立場を表明しない中、ロシアは、軍のサイバー戦コンセプトを制定し、軍がサイバー戦における中核の機能を担うこと、サイバー戦を具体的に戦うサイバーコマンドを創設することを明確に示した。そして、大統領の決定があり、国益に否定的な影響がある場合には、国外においてサイバー攻撃を実施する権利を有することを表明した 2 番目の国家となった。その背景には、国際社会においてロシアがサイバー戦を主導していくのだという強い国家意志がある。

このコンセプトを基本として、今後どのようにロシアがサイバー戦を実施していくのかについて、要人の発言、事象（行動）、サイバー戦兵器やその開発状況などに注意を払っていくことが重要となってきている。

(Received:May 31,2012)
(Issued in internet Edition:July 1,2012)