サイバー強国中国と如何に向き合うか

原田　泉*

要　旨

スノーデン事件以降，中国は「サイバー強国」をめざし，米国を猛追している。その結果，サイバー空間は米国一極覇権の体制から米中覇権分有時代へと移行している。また近年の AI の進展によりサイバーセキュリティの世界も AI 対 AI の力勝負の局面を迎えようとしているが，ここでも先行する米国に中国が迫りつつある。このような状況下，日本はまずは自らの実力を高め，更に米英とのサイバー安全保障面での協力強化を進めなければならない。一方，中国との信頼醸成と友好関係の促進も同時に図らなければならない。

キーワード：サイバー攻撃，AI，機械学習，自律型致死性兵器，信頼醸成

1．はじめに

近年，サイバーセキュリティは，サイバー攻撃の可能性を懸念する段階から，社会機能の喪失につながる攻撃の予防と対処の段階と進化し，特に IoT（Internet of Things）によりあらゆる物がネットでつながる社会になると，これまで以上にサイバー攻撃の脅威が社会にとって飛躍的に拡大していくと思われる。このような状況にあって，我が国でもその対応が国家レベルの喫緊な課題として求められている。

特にスノーデン事件以降，米国によるインターネット管理が衰退する中，中国が「サイバー強国」をめざし飛躍的にその存在感を増しており，サイバー空間における勢力図が大きく変わろうとしている。

一方，最近最も注目されているのが AI（人工知能：artificial intelligence）の活用である。サイバーセキュリティ分野での AI 開発は国家の存亡にも大きくかかわる重要問題ともいわれているが，ここでも中国が先行する米国を猛追しているのである。

本稿ではこのようなサイバー空間での現状を述べるとともに，今後の我が国の対応を考えたい。

＊国際社会経済研究所　上席研究員

2．サイバー空間の現状認識

2-1　サイバー空間の国際関係

現在，サイバー攻撃は多種・多様，大規模，かつ高度化しており，国家機関や国際的な犯罪組織が主要な攻撃者となっている。

国家機関による攻撃は，重なる部分はあるものの，主に軍隊による軍事攻撃といわゆる諜報機関（インテリジェンス）による攻撃がある。

軍事攻撃には，スタクスネット[1]，DDos 攻撃などがあり，物的破壊も含む攻撃である。

これに対して諜報機関による攻撃は主に標的型メールに代表される情報窃取，またエシュロン[2]やプリズム[3]に代表される通信傍受（無線，有線）があり，また最近ではロシアの米国大統領選挙へのサイバー攻撃に見られるようなプロパガンダ・心理戦として，デマ情報の流布を行うフェイクニュース，偽メールなど世論操作や社会混乱を狙うものも目立ってきている。

また，国家安全保障のため，大国ではサイバーセキュリティ分野の研究機関に莫大な研究開発費を投入しており，レベルの違いはあるものの途上国も費用対効果の高い武器としてサイバー攻撃を認識しつつある。

一方，民間による攻撃は金銭目的のフィッシング，標的型メールで知的財産や電子マネーの詐取等であり，国家機関からの委託を受けるものもある。また，アルカイ

ダやIS等のテロ集団による軍事攻撃，プロパガンダも一部あり，アノミマスやウィキリークスなどのいわゆるハクティビスト[4]のプロパガンダやハッカー等の愉快犯も存在する。

このような状況下，サイバー空間での国際秩序作りは困難な局面を迎えている。国連も，サイバー空間の国際的な規範を作るべく取り組みを進めている。2010年，米国や中国，ロシアを含む15カ国からなる国連における政府専門家会合である国連サイバーGGE（Group of Governmental Experts）が設置され，米国主導で国際法を当てはめたサイバー空間の規範を作るべく議論を重ねている。しかし2017年6月に開催された最後の会合で，米国主導による国連のルール策定の取り組みは，中国やロシアが反発して事実上崩壊した[5]。

一方，インターネット自体はまだ米国の実質的支配下にあり米国国防総省傘下の情報機関である米国国家安全保障局（NSA）[6]による監視は続いている。周知のようにインターネットの電話帳といわれるDNS[7]のルートサーバレコードの管理権は米国商務省が握っている。また，インターネットの大動脈であるルートサーバーは，全世界に13台あるうち10台が米国政府の監督下で運営されている[8]。

その結果インターネットを流れる情報の8割以上が米国にある相互接続ポイントを経由することになる。そしてそれは，NSAの監視下となっている。したがって，米国の実効的な支配は継続しているといわざるを得ないのである。

しかし，一方では世界中のICT機器や部品，スマホの多くは中国製となっており，それらにセキュリティ上の脅威となるバックドアが仕組まれているとも言われている[9]。

もともとインターネットは米国の対ソ軍事戦略で開発され，その後冷戦構造崩壊とともに商用化する中で，サイバー空間は自由で国境のない空間という幻想が広まっていた。しかし，2013年のスノーデン事件以後は，サイバー空間は一面では米国の世界監視システムであり情報収集システムであって，安全保障面でもビジネス面でも米国の国益に叶うツール（特に9.11以降）であることが世界中に知れ渡ったのであった。しかしこれに不服があってもインターネットを使わないわけにはいかず，またテロ対策では先進国の多くがNSAや英国の政府通信本部（GCHQ）[10]を頼らざるを得ないという状況も存在するのである。

2-2　中国がサイバー強国へ

中国では近年，習近平国家主席により2014年4月に打ち出された「総合的国家安全保障観」[11]の下で，国家安全法（2015年7月1日施行）や反テロリズム法（2016年1月1日施行）等の国家安全に関する立法を進めてきているが，特に，スノーデン事件に大きなショックを受け，事件発覚以降サイバー強化へと大きく政策転換を図ってきている。

すなわち中国は「サイバー強国」をめざし，2014年以降国家を上げてサイバー面での強化を進めているのである。インターネットが正式に繋がって20周年という重要な節目に当たって，中国は2014年2月に中央ネットワーク安全・情報化指導小組を設立し，北京でその第一回会議を開催した[12]。

ここで習近平主席自らが組長に就任し，李克強氏，劉雲山氏が副組長を担当し，習近平主席がサイバー強国構築の戦略目標を提示したのである[13]。このことは中国が国家として如何にサイバーを重視するかを示したものと言えよう。

翌年の2015年9月25日に，米国で両首脳会談が行われた。そこでは，知的財産権に対する産業スパイなどのサイバー攻撃を双方の政府が容認しないことと，閣僚級の対話メカニズムを構築することで合意したのである。また両国はハイレベルでの共同対話メカニズム，すなわちサイバースペースにおける信頼醸成措置を構築していくことも明らかにした。その後12月2日，中国の郭声琨国務委員は米ワシントンでスーザン・ライス（Susan Rice）米大統領補佐官（安全保障担当）と会談し，サイバー犯罪を取り締まるうえでのガイドラインや，当局間のホットラインの設置などで合意したのである。

2016年10月には，習近平主席が，中国共産党中央政治局第36回集団学習会において，「サイバー空間の安全保障・防御能力の強化を加速し，IT技術を用いた社会ガバナンスの推進を加速し，我が国のサイバー空間における国際的発言権とルール設定権の向上を加速し，サイバー強国建設の目標に向けて努力を怠らない」ことを強調し[14]，さらに中央ネットワーク安全・情報化指導小組の承認を経て，国家インターネット情報弁公室は同年12月に「国家サイバー空間安全戦略」を発表した。これはサイバー空間の発展と安全に関する中国の立場と主張を明らかにし，戦略的方針と主要課題を明確にし，国のサイバーセキュリティの取り組みを指導する綱領的文書と位置付けられる[15]。

その後，中国外交部（外務省）と国家インターネット情報弁公室は 2017 年 3 月 1 日，「サイバー空間国際協力戦略」[16]を共同で発表した。これは，中国初のサイバー問題に関する国際戦略の公開となる。同戦略は平和発展，協力と相互利益をテーマに，サイバー空間における運命共同体の構築を目標として，サイバー空間における国際協力の推進について初めて全面的かつ系統的に中国の主張を打ち出したのである。また，世界のサイバー空間のガバナンスという難問の解決のために中国のプランを提起して，中国が主導するサイバー空間をめぐる国際交流・協力へ各国の参加を促そうとする戦略的文書でもある。またここでは，各国が「国際連合憲章」の主旨と原則を着実に遵守し，サイバー空間の平和と安全を確保することを提唱しており，主権の平等を堅持し，サイバーの覇権争いをせず，他国の内政に干渉しないことを提唱している。その上でサイバー空間における優位性による相互補完と共同発展を推進し，「デジタル・デバイド」（情報格差）を解消し，人々がインターネット発展の成果を享受できる状況を確保することを提唱しているのである。

他方，以上のようなサイバー戦略とともに，「サイバー安全法」[17]が 2016 年 11 月，全国人民代表会議において可決され，2017 年 6 月 1 日より施行された。

同法の初案が提出されたのは 2015 年 6 月のことであり，審議を経た第 3 案に至って施工されるまで丸 2 年を要した。また，この過程ではパブリックコメントの募集が 2 回も行われたほか，米国大使館や日米欧の在中商工会議所との意見交換も行われた。

同法の要点は以下 7 点にまとめられる。

① 個人情報の保護：中国国内での個人情報の収集，仕様，保護に関する要件が明確化された。
② 「ネットワーク運営者」：これにあたる事業者は，セキュリティにかかる責任を負うことが明確化された。
③ 「重要情報インフラ運営者」：これにあたる事業者は，その保護を名目に中国当局の強い統制を受けることが明確化された。
④ 機密情報の保存：中国国内で収集・生成された個人情報やデータは，中国国内で保管することが義務付けられた。
⑤ 国外へのデータ移転：原則的に禁止されることが明確化された。
⑥ セキュリティ製品の認証：重要なサイバー設備・セキュリティ製品については，中国当局のセキュリティ認証が義務付けられた。
⑦ 法的責任と罰則：サイバースペースにおける中国当局の強い権限が規定され，違反者には高額な罰金を含む罰則が与えられることが明確化された。

この内容については欧米諸国から懸念の声があがっている。たとえば英国の「フィナンシャル・タイムズ」は，同法の施行翌日の社説[18]において，「明らかに市民の言論と思想の統制を強化するだけでなく，グローバル企業が中国で操業する際の非関税障壁となる。その保護主義的な姿勢によって，ひいては中国企業の国際競争力も奪いかねない」と批判している。

その後 2017 年 10 月の中国共産党大会において習総書記は 21 世紀半ばまでに中国が「トップレベルの総合国力と国際的影響力を有する国となる」としたが，以上のような一連のサイバー強化策により既にサイバー空間では，米国一極覇権の体制から，二つのスーパーパワーの米中覇権分有時代へと移行していると言えるかもしれない。

3．AI によるサイバーセキュリティ

3-1　AI によるサイバー防御

従来のサイバーセキュリティ技術では未知の脅威には対応できなかった。しかし最近未知のマルウエアを検知するために，機械学習[20]を使ってマルウエアの振る舞いや属性を深く分析する技術が生まれた。そこでは Dark Web[21]で取り引きされている情報を収集し，機械学習，自然言語処理といった技術で分析することで，今後生じる攻撃手法を事前に把握するのである。

現在，AI はサイバー空間における犯罪者側の動向を理解する技術として使用されており，深層学習[22]を使ってリアルタイムに大量の通信トラフィックを監視し，サイバー攻撃に共通するデータや送信元，接続数などの情報を AI が蓄積，解析し，その中で異常を検知して，新たな脅威の予測と迅速な対策を行っている。

深層学習を用いた AI による分析とは，データ内の注目すべき点となる特徴量[23]を数多く抽出し，その分析からマルウエアに対する知見を見出すものである。たとえば，マルウエアの解析で AI は，ファイルのサイズやファイルのヘッダ情報，文字列などから特徴量を確定し，約 5 億個にも上るマルウエアを AI に学習させることで，精度の高い検出を行うのである。また，シグネチャ[24]の作成中に生じるマルウエアと，有効な対策を作成する間のタイム

ラグを短縮化して，高い検出率を実現するのである。

今後 AI を利用したサイバー防御は，高度なサイバー攻撃を検知し，防御できる知的プラットフォームを形成して，膨大な量のオープンデータからサイバー攻撃に関連した情報を自動モニタリングするようになるであろう。また異常の検知，分類，予測，可視化を行う高精度な攻撃監視が進み，追加学習，オンライン特徴抽出，自動データ収集，自動ラベリングなどの自律学習機能も進展していくことで一層その防御力を増していくと考えられる。

機械学習の長所としては，大量かつ高次元の観測データから知識獲得できることや，観測データの追加学習による攻撃の変遷に合わせた異常の検出，分類，予測が可能なことがあげられる。もちろん AI は 24 時間，365 日働き続けることができるし，機械学習で判定可能なものは自動化し，管理者の負担を軽減することができる。

一方，短所としては，攻撃事例は少なく，攻撃に関連したデータの収集は容易でない点があげられる。また AI 自身の特性として騙されやすい（adversarial setting）点がある。悪意を持つ人々によって誤った学習データが使われたり，サイバー攻撃によって AI をだませる一定の入力パターンさえ調べれば，その判断や動作を歪ませることもできるのである。これら AI を誤作動させる内部・外部要因を取り除くのが AI の安全面での課題であるが，この関連研究はまだまだ進んでいないのが実情だと言われている[25]。

他方，サイバー攻撃面においては，AI や機械学習が進展することで，これまで人手でこなす必要のあった作業の自動化が進むと見られている。その結果，これまでよりも多くの攻撃の自動化が可能になると考えられる。たとえば，効果的なフィッシングメール[26]を作成し送付するができるようになるだろう。スピアフィッシング攻撃[27]では，標的を確定する際，どの企業，どのような組織が騙されやすいかなどの詳細情報を，攻撃者に与える必要があるが，AI システムは，大量のデータベースを収集，整理，処理して識別情報を結びつけ，詳細情報を攻撃者に与え，攻撃をより迅速かつ的確に実行させることができるのである。また，攻撃対象の絞込みと特定にも威力を発揮する。複数の情報源から，攻撃に対して特に脆弱な人物を特定することができる。

また，機械学習を使って企業内のスパムメールフィルタを混乱させることも可能となる。機械学習アルゴリズムを使ってネットワーク内でのユーザーの動作を模倣して異常動作の検出を回避するのである。未だ攻撃者が企業ネットワークにどのように侵入し，攻撃を仕掛けるかを把握する適切な方法がなく，そのため早期警告を行うための兆候を見つけるのが困難な状況である。

加えて，AI は，ID 盗難，DDoS 攻撃，パスワードクラッキングなどのサイバー攻撃の既存の試みを，より強力で効率的なものにし，複雑な攻撃を人間のハッカーよりも迅速かつ効果的にすることができ，人間のサイバー犯罪者が攻撃をカスタマイズするのを助けることができるのである。

3-2　AI を利用したサイバー攻撃の実現性

以上のように AI を利用することで，サイバー攻撃の効率は飛躍的に高まるのである。従来は特徴が僅かに異なる亜種のマルウエアを数多く作って検知を回避してきたが，今後は機械学習で開発の自動化を進めるなどして，新たなマルウエアがより大量に生み出されるようになると考えられる。

しかし，現在のところ犯罪者側から見ればまだまだ AI 利用のコストは高く，本格的な機械学習を用いての新たな攻撃の作成は散見されてはいない。攻撃者が金銭獲得などの目的を達成するために，AI 利用によるサイバー攻撃の費用対効果が良いと判断しなければならないが，まだそこまでには至っていないようである。とはいえ，AI サイバー攻撃は間違いなく起こると思われ，その要素技術であるデータサイエンスに取り組むハードルは低くなっている。手軽に機械学習アルゴリズムを利用可能にするためのシステムが，実際に提供されており，Google の「Cloud AutoML」や Amazon Web Services の「Amazon SageMaker」は，どちらもその例と言える。このように安価に機械学習アルゴリズムを利用可能にするためのシステムが提供されはじめ，学習データへのアクセスも楽になっており，こうしたトレンドは攻撃者にとってのハードルも下げるものとなる。

もちろん国家の軍，情報機関等はこの限りではなく，既に後述のように AI によるサイバー攻撃の開発を進めているのである。したがってそう遠くない日にサイバー空間は，AI 対 AI の本格的な戦いの場になってしまうだろう。

4．中国における AI の開発と軍事利用

4-1　中国の AI 開発

AI は現在第 3 次ブームと言われている。この背景にはコンピュータ性能が飛躍的に伸びたこと，スマートフォ

ンの普及やIoTの登場で様々なセンサーから大量のデータが生み出され，これらのデータからAI自身が知識を獲得する機械学習が実用化されたためである。

米国のAI開発の優位性は，米国のGAFA（Google，Apple，Facebook，Amazon）のようなプラットフォーマーがデジタル市場で急成長を遂げており，その競争優位が固定され，支配的地位を占めることが懸念されるほど[28]，世界中のデジタルデータと情報を独占していることにある。

これに対し，中国には7億人以上のスマホ利用者が存在し，そこで独自に膨大で様々なデータが利用できるのである。そして中国のAIに関連する新興企業はベンチャーキャピタルから莫大な資金を呼び込んでいるのである。

一方，中国国民はプライバシーや個人情報保護に対しあまり頓着せず，このため比較的容易にデータを収集できる。これに加え，中国では，漢字を打ち込む手間が面倒なため，音声による支援サービスが欧米よりも普及しており，音声支援システムの改善も速くなる。特に音声認識分野では，百度に加えてi FLYTEK社（アイフライテック）という新興企業の成長が著しい。

中国の大手企業（百度，滴滴，騰訊）は，各社独自のAIリサーチラボを立ち上げている。とりわけ百度は，深層学習において世界レベルに達しており，シリコンバレーにAIラボを持ち，そこでは200人の開発者がライバルとなる米国企業に対抗すべく，自動運転車，物体認識のライブラリ，表情や自然言語の認識ソフトなど先駆的な開発を行っている。

騰訊も同様で，いくつかの中国トップレベルの科学技術大学に対して奨学金を提供し，学生らがWeChatの膨大なデータベースにアクセスできる一方で，騰訊側としても優れた研究成果や優秀な卒業生らを確保できるメリットを確保している。

また，華為技術も長期的事業拡大を狙いAI技術で世界のトップになるため莫大な投資をする計画を表明している[29]。

他方，技術革新による経済成長戦略を打ち出した中国は，米国のシリコンバレーのイノベーションリソースの活用を強化しているのである。その方法としては，シリコンバレーのインキュベーションシステムを中国国内に導入し，ベンチャー企業の中国国内での産業化，海外中国人を中心とする海外人材の中国国内への受け入れ，中国系VC（ベンチャー・キャピタル）やインキュベーターのシリコンバレーへの進出も加速化している。

調査会社Rhodium Groupによると，2016年6月までに不動産投資を除いて中国から60億ドルの資金がシリコンバレーに入っている[30]。半分以上は2015年初から16年央のあいだに投下され，中国資本は特に，AR/VR，AI，ビッグデータ，バイオなど中国が遅れている技術分野に関心を寄せている。中国系VCが主催するシリコンバレーでの投資説明会，人材誘致商談会，ベンチャー企業ロードショーなども数多く行われている。数年前までは，シリコンバレーで活躍する中国人技術者が注目されたが，この1，2年では中国系VCが注目されはじめ，シリコンバレーで中国VCの投資を欲しがるベンチャー企業が増えている。

一方，中国政府によるAI振興策も目覚ましいものがある。2017年7月，国務院がAI分野での世界的リーダーになることを目指し，2030年までに同国のAI産業を1500億ドル規模にまで成長させる以下のような「新世代AI開発計画」[31]を発表し，2030年を見据えた中国の新世代AI発展の指導思想，戦略目標，重点任務，保障措置を打ち出した。これは，中国のAI発展の先行優位性を創出し，革新型国家及び科学技術強国の構築を加速させることを目指している。

その戦略目標は，

① 2020年までに，AIの技術と利用が世界先端水準に達し，AI産業が経済成長の新しい原動力になり，AIの利用が民生改善の新しい手段になる。
② 2025年までに，AIの基礎理論は大きなブレークスルーを遂げ，一部の技術と利用は世界先端水準に達し，AIは中国の産業アップグレードと経済発展方式転換の主な原動力になり，知能社会の建設を進展させる。
③ 2030年までに，AIの理論，技術，利用は世界先端水準に達し，グローバルの主なAI革新センターになる。

その重点任務は，1.開放的かつ連携的なAI革新体系の構築，基礎理論，重要な共通技術，革新的プラットフォーム，高級人材等の関係の強化，2.高度で効率的な知能経済や，AIの新興産業を発展させ，産業の知能化を一層推進，3.安全かつ便利な知能社会を整備，効率的知能サービスを発展させ，社会ガバナンスの知能水準を引き上げ，社会の種々の関係において相互信頼を促進，4.AI分野における軍民融合の強化，軍民AI技術の相互転換を促進，5.ユビキタス，安全かつ効率的な

知能化インフラ体系を整備，ネットワーク，ビッグデータ，HPC（ハイ・パフォーマンス・コンピューティング）等のインフラの整備を強化，6. 新世代 AI に特有の重要な基礎理論と重要な技術のボトルネックについて，統括を強化して，将来を見据えた重大科学技術プロジェクトのマトリックスを構築する――というものである。

以上の内容は，オバマ政権が 2016 年末に公表した AI の将来に関するいくつかの報告 と似通っている。しかし，中国がその計画を発表して以降，トランプ政権の動きは鈍く，AI 開発を促した前政権の方針を行動に移す気配を見せていない。かつては空想の産物だった AI だが，今ではアマゾンやグーグルをはじめとする米国企業の開発努力が実って現実のものとなり，国防分野にも影響を及ぼすほどの存在となっている。

しかし，トランプ政権が技術者の移民を制限しようとしていることもあり，米国に拠点を置いていた AI 開発事業は，トロントやロンドン，北京など外国に移りはじめており，これに伴い，中国がテクノロジーの次の大きな波を牽引するという可能性も高まりつつある。

中国が国家全体でどれだけの額を AI 事業に注ぎ込んでいるかは不明だが，北京市は市内の AI 開発パークに 20 億ドルを投資するとしている[33]。

これに加え，北京市経済・情報委員会が指導する北京市先端国際 AI 研究院が 2018 年 2 月 8 日に設立された。同研究院は複数のイノベーションセンター，科学研究プラットフォームから構成され，第 1 期として，北京 AI 基礎研究イノベーションセンター，北京智慧社会イノベーションセンター，北京 AI 特許イノベーションセンター，の 3 つのイノベーションセンターを設立した。同研究院の任務について李院長は，①北京市を中国だけではなく全世界からの AI 人材のセンターとし，特に産・学・研の連携を推進，② AI 技術の都市管理における実践及び関連産業における実用を推進，③より多くの AI 研究者の特許出願を奨励，特許取引から価値を創造し，特許プールを育成，知的財産権保護の仕組みを構築し，国際 AI 業界標準競争に参画，④中国科学研究院の指導の下，インフラプラットフォームを整備，中国最大の AI 共有コンピューティングプラットフォームとするなどと述べた[34]。

このような中国の AI の進展に対し米国では多くの懸念が出ている。下院監査委員会 IT 小委員会は，AI について予定している 3 回の公聴会の第 1 回目を開催した。証人として出席した専門家等からは，米国が AI 開発で他国に先駆けるには政府がさらに資金を投入して研究を支援すべきとの声が相次いだ。

民間企業や学術機関の専門家は，AI 分野は目覚ましい発展を見せているが，その可能性を完全に引き出すにはまだ程遠い段階にあると説明した。

有力な AI 企業である NVIDIA 社のイアン・バック(Ian Buck) 社長は,「AI は我々の世代における最大の経済的・技術的革命になるだろう」とし，2035 年には AI が米国経済に 8 兆ドルを貢献すると予測されていることを指摘し,「他国に先んじられるわけにはいかない」と述べた。

同氏は，中国をはじめとする他国は AI 研究への投資を積極的に拡大しているのに対して，米国政府の投資額はほぼ横ばいであることにも言及した。トランプ政権は，AI について「強くコミットしている」としているが，その一方で，トランプ政権が 2019 会計年度予算教書で非軍事研究開発予算を 19％以上削減していることに懸念が示されている[35]。

4-2　中国の AI のサイバー利用

このような中，元在日米軍司令部サイバーセキュリティ長のスコット・ジャーコフ（Scott Jarkoff）氏が産経新聞の取材で明らかにしたところによると，中国とロシアが AI を活用して自動的にサイバー攻撃を仕掛ける技術を取得したことが以下のようにわかった[36]。記事によると，
「AI を活用すれば，人材の省力化でハッキングの効率を高められる。AI が自ら攻撃手法を学んで技術を短期間で向上でき，大規模な攻撃を仕掛けることも容易になるという。北朝鮮も同様の技術を獲得した恐れがあり，AI を悪用した攻撃の脅威が世界に広がりそうだ。ジャーコフ氏は，欧州警察機関（ユーロポール）などと情報を共有し，2017 年中露の AI 技術取得の情報を入手したという。同氏によると，中露が獲得した AI 技術は自動的に膨大な数のパソコンやスマートフォンにウイルスを送れる機能を持つという。（中略）

ジャーコフ氏は，中露が AI の使用で攻撃を強化できる点について『睡眠を取る必要がないので攻撃の効率が大幅に上がる』と分析した。AI が大量のデータを基に自ら学習する深層学習を行うことで『攻撃の技術や手口が自動的に上がり，育成しなくても優秀なハッカーが誕生する』という。人間のハッカーであれば手法や攻撃を仕掛ける時間帯で犯行を特定されやすかったが AI では調査が難しく，攻撃側は追跡から逃れやすい』とした。

中国には，日本の官公庁の情報を盗むサイバー攻撃

を仕掛けるハッカー集団が存在し，ロシアでも，米大統領選で民主党全国委員会に攻撃した集団が確認されている。同氏は,『中露のハッカー集団がAIを使うことで,さらに重大な被害が起きる』と強調した。　また，日本の防衛省がネットワークを守るシステムにAIを導入する方針にも触れ『今後のサイバー戦争はAI同士の戦いになる』とした。」

近年，AI開発面でも中国の進展は目覚ましく，今後サイバー安全保障の世界はAIの力勝負となることを認識して国家的な推進体制を作っているのである。

4-3　米国に続く中国のAI軍事利用

米国は，1990年代後半から当時登場した情報通信技術を活用した「軍事における革命」（RMA）[37]により世界をリードし，情報時代における不可欠な技術であるステルス，精密誘導兵器，ハイテクセンサー，指揮統制システム等においても圧倒的に優位であった[38]。そしてその延長線上に現在のAIの軍事利用がある。AIは戦争を情報化戦争から知能化戦争へシフトさせている。

AIは，戦場における指揮官を手助けし，その状況判断を正確かつ迅速にすることができ，ウォーゲーム，シミュレーション，サイバー戦や電子戦への適用，また仮想現実の技術と合体すると訓練・演習をより実戦的にすることもできるなど適用分野は軍事の大部分にわたっている。加えて，コンピュータによる画像認識と機械学習の技術を応用すると，目標認識が不可欠な各種兵器の能力を飛躍的に向上させることになる。このような結果，AIは軍事作戦スタイル，兵器体系などを刷新させ，指揮官の状況判断，幕僚活動，部隊運用，訓練なども大きく変えて戦争の様相を一変させるといわれている。

周知のように軍事バランスの変化は国際関係の変化に直結するものである。今後のAI開発優劣が国際関係をも左右すると考えられるのである。

米国は技術力で長年軍事的優位を保ってきたが，最近中国の人民解放軍は，米国が誇る最新技術，特にAIに注力し始めている。人民解放軍は，AIを軍事のあらゆる分野に取り込み，軍事分野における革命ともいえるAIの軍事利用を進めているのである。前述のように米国は現在AIで世界をリードしているが,中国は「新世代AI開発計画」を発表し，2030年までにAIで世界をリードするとの計画を明らかにした[39]。

既に中国はAI大国といえる。中国は米国に次ぎAI関連特許申請が多く，中国の学者はすでに米国の学者より多くのAI論文を発表しており，AI推進協会の2017年年次会議で，中国の研究者は初めて米国の研究者と同数の論文を提出した。また中国の官民は何十億ドルもの投資をし，有能な若者を育てる努力をしており，中国は米国を追い越しそうである。このような中国は，AIが戦争の性質を変えると考えており，AIが戦争で使われるようになるにつれ，戦闘のほとんどを人間のいないシステムで行うことが実現すると考えているのである。

米国のエルサ・カニア（Elsa B. Kania）氏は，人民解放軍のAIによる軍事革命に関する論文「戦場のシンギュラリティ」[40]を発表し，中国は，AIを将来の最重要技術と位置づけ，2030年までにAIで世界をリードするという目標を達成しようとしており，習近平主席が重視する「軍民融合」により,民間のAI技術を軍事転用して,AIによる軍事革命を実現しようとしていると指摘した。また，AIによる軍事革命の特徴の一つは，AIと無人機システム，たとえばロボット，無人飛行機，無人水上・水中船などの合体であり，この革命により戦争の様相は大きく変わると指摘している。

他方,AIの軍事利用によっては,小さな国や組織でも,我が国を含め他国を脅かしやすくなる。核兵器の開発は以前に比べより容易になっているかもしれないが，必要な資源や技術，専門知識はまだ入手しやすいとは言えないが，AI兵器ではコードやデジタルデータは安く手に入る場合が多く，広く拡散するものもあり，また，前述のようにAI利用によるサイバー攻撃のハードルが低くなりつつある。

機械学習やプログラムに基づき，攻撃目標を自律的に選択するAI兵器は，一般に「自律型兵器（AWS：autonomous weapon systems）」と呼ばれ，攻撃目標を人間がセットするタイプのミサイルや無人攻撃機とは異なる概念の兵器と言える。特に軍事拠点の破壊や人間の殺傷を目的にしたものを「自律型致死性兵器（LAWS: lethal autonomous weapon systems）」と呼ぶ。

米国防省は2012年，殺傷力の行使にかかわる決断は人が下さなければならないという暫定的な方針を定め[41]，2017年5月には,これを恒久的な方針に変更した[42]。

これまでLAWSの規制を巡り，日米ロ中など主要国の外交官が参加する政府専門家会合が2017年11月と2018年4月とに開催された。この会合は通常兵器の使用を規制する「国際特定通常兵器使用禁止制限条約（CCW：Convention on Certain Conventional

Weapons)」[43]の枠組によるもので，これまで焼夷弾，対人地雷，クラスター爆弾などの制限が検討され，後にCCWまたは個別の条約による使用規制につながった。

中国外交部軍縮局はここでのコンセンサスで枠組みを作り，制限することを希望しており，LAWSの研究開発と利用に反対しているとのことである[44]。

その後2018年8月末ジュネーブで開かれたAIを搭載した兵器の規制をめぐる国際会議で，日本政府は，LAWSを開発する意図はないとした上で，性急な規制は民生分野の技術発展を阻害するとして慎重な見方を示した[45]。AIの軍事利用は核兵器と同様に各国間の軍事バランス，ひいては国際関係すら大きく変えると言われているが，ここでも圧倒的な力を持つ米国に，中国やロシアが急追している現状がある。

5．むすび
我が国が今後執るべきサイバー・AI政策

以上述べてきたように中国のサイバー面，AI面での力は，極めて強大なものとなっている。このような状況に対し，我が国のサイバー面での対応施策に関しては，日本危機管理学会年報『危機管理研究』第25号の拙稿「IoT時代に向けてのサイバー危機管理の現状と我が国の課題」[46]で自分の国は自分で守るための以下の8項目の施策を提示した。

1. サイバー戦における防衛力強化（反撃の研究開発）
2. サイバーインテリジェンスの強化，特に専門機関の創設
3. サイバーセキュリティの研究開発（AI，暗号等）と人材育成強化
4. 関連法令の整備，特に重要インフラ等に信頼性確認制度（セキュリティクリアランス），国民の個人情報等を安全に保有するためにデータベースは国内に設置，法執行機関による一部通信傍受に関する検討
5. 政府機関，重要インフラ関連企業等のICT機器にバックドアやスパイウエアが組み込まれていないかの安全検査の徹底
6. サイバーセキュリティの普及啓発とセキュリティバイデザインの推進
7. 海底ケーブルの陸揚げ地にサイバー国境所を設置し，海外からの不正アクセス等を制御する
8. 更なる米英とのサイバー安全保障面での協力強化

一方AI面では，以下のように考える。

AI関連技術の進歩は将来，経済面だけでなく国際的な力関係を揺るがす可能性があり，AIの軍事利用に関する規制をめぐる国際的な合意を図っていかねばなるまい。

EUは既に有識者会議によるAI倫理指針原案を策定しており，2018年末までには欧州委員会が最終案を作る予定である[47]。

我が国は，AIのルール作りに関しては，欧州との協力[48]を軸に更に広範な議論と大胆で大規模な国家的な取り組みが必要と思われる。

いずれにせよ，中国に対してはその実態の把握に努め，現実を直視して外交的友好関係の促進，信頼醸成を進める必要があるように思われる。

参考文献

ジョー・マクレイノルズ『中国の進化する軍事戦略』2017/5　原書房

チェン，ディーン『中国の情報化戦争―情報戦，政治戦から宇宙戦まで』2018/06　原書房

土屋大洋，持永大，村野正泰　『サイバー空間を支配する者 ――21世紀の国家，組織，個人の戦略』2018/8　日本経済新聞出版社

マーティン・ファン・クレフェルト『新時代「戦争論」』2018/05　原書房

兵頭二十八　『ＡＩ戦争論』　2018/04　飛鳥新社

伊東 寛　『サイバー戦争論―ナショナルセキュリティの現在』2016/08　原書房

『サイバー・インテリジェンス』　2015/09　祥伝社新書

渡辺悦和『中国人民解放軍の全貌』2018/05　扶桑新書

宮家邦彦　『AI時代の新・地政学』　2018/09 新潮新書

1）Stuxnet：2010年にイランを中心とする中東各地域で発見された，標的型攻撃を行うマルウェアの通称である。イランの原子力施設の制御システムをダウンさせたことで知られる。「IT用語辞典バイナリ」による

2）Echelon：米国を中心に，英国・カナダ・オーストラリア・ニュージーランドの5か国で共同運営する通信傍受システム。無線，電話，ファクシミリ，電子メール，各種データ通信を傍受し，米国のNSA（国家安全保障局）が一元的にその情報の収集と分析を行っているとされるが，米国政府は公式にはその存在を認めていない「デジタル大辞典」による。

3）PRISM：米国のNSA（国家保安省）が運営して通信監視プログラムである。正式名称はUS-984XN。メール，写真，音声，動画，文書，接続記録など，ネットでやりとりされるデジタルデータが主な対象。「Wikipedia」による。

4）hacktivist：社会的・政治的な主張を目的としたハッキング活動を行う者のこと。

5）外務省
https://www.mofa.go.jp/mofaj/press/release/press4_005330.html

6）National Security Agency：通信傍受・盗聴・暗号解読などの「信号情報」活動を担当する。

7）Domain Name System：インターネットの必要不可欠な基盤技術で，ドメイン名とIPアドレスの対応付けや，メールの宛先ホストを指示するためのシステム。

8）他のルートサーバー3台のうち2台は欧州，1台は日本にある。「Wikipedia」による。

9）Latest news on my Hardware Security Research　https://www.cl.cam.ac.uk/~sps32/sec_news.html#Assurance
WIRED　https://www.wired.com/2012/10/chinese-telecoms-suspicious/

10）Government Communications Headquarters：英国の情報共同体において，偵察衛星や電子機器を用いた国内外の情報収集・暗号解読などを担当する諜報機関

11）習近平「堅持総体国家安全観 走中国特色国家安全道路」『新華網』2014/4/15　http://news.xinhuanet.com/politics/2014-04/15/c_1110253910.htm

12）人民網　http://media.people.com.cn/BIG5/n/2014/0228/c40606-24488129.html

13）中央網絡安全和信息化領導小組　http://www.cac.gov.cn/

14）新華網「习近平：加快推进网络信息技术自主创新朝着建设网络强国目标不懈努力」http://www.xinhuanet.com/politics/2016-10/09/c_1119682204.htm

15）人民網日本語版　2016/12/29　この連略では，サイバー空間の主権を揺るぎなく守ること，国の安全を断固として守ること，重要な情報インフラを保護すること，サイバー文化建設を強化すること，サイバーテロと違法犯罪を取り締ること，サイバーガバナンスシステムを整備すること，サイバーセキュリティの基礎を固めること，サイバー空間の防護能力を高めること，サイバー空間の国際協力を強化することの9項目が挙げられている。

16）中国網日本語版　http://japanese.china.org.cn/politics/txt/2017-03/02/content_40390646.htm

17）中華人民共和国工業和信息部「中华人民共和国网络安全法」http://www.miit.gov.cn/n1146295/n1146557/n1146614/c5345009/content.html

18）Financial Times, 2017/6/2 “China’s cyber security law and its chilling effects”

19）新華網 2017年10月18日 中国共産党第19回全国代表大会
http://jp.xinhuanet.com/2017-10/18/c_136688582.htm

20）機械学習 machine learningとは，コンピュータがデータから反復的に学習し，そこに潜むパターンを見つけ出すこと。その学習した結果を新たなデータにあてはめることで，パターンにしたがって将来を予測することができる。

21）ダークウェブは，たとえURLを手に入れても，一般のブラウザーからは，アクセスできないサイト群である。しかも，そこへのアクセスは匿名化され，追跡が著しく困難になっている。世界中から犯罪者などが集まり，非合法コンテンツがやりとりされている。

22）深層学習 deep learningとは，人間が自然に行うタスクをコンピュータに学習させる機械学習の手法のひとつで，ニューラルネットと呼ばれる主に生物の神経系の挙動を模して学習できるようにデザインされたもの。

23）特徴量とは，機械学習を行う際に学習データにどのような特徴があるかを数値化したもの。この特徴量の抽出は人間が設計し作らなければならない。

24）異常なデータや普通とは異なる行動パターンを定義して，それを記録しておく。この記録されたものをシグネチャという。

25）AIを使ってセキュリティを向上させる，特に機械学習を使ってセキュリティ問題を解決しようという研究は比較的長い歴史を持っており，バイオ認証，侵入探知，DDOS探知，不正取引探知などの目的に応用されてきた。

26）インターネットのユーザーから経済的価値がある情報（例：ユーザー名，パスワード，クレジットカード情報）を奪うために行われる詐欺行為で，信頼されている主体に成りすましたEメールによって偽のWebサーバーに誘導することによって行われる。

27）偽の電子メールを使って不特定多数の人から個人情報などを盗み取るフィッシング詐欺（phishing）のこと。

28）経済産業省「第四次産業革命に向けた横断的制度研究会」報告書 http://www.meti.go.jp/press/2016/09/20160915001/20160915001-3.pdf
新産業構造ビジョン中間整理 30頁

29）South Morning Post 紙 https://www.scmp.com/tech/science-research/article/2167693/huawei-commits-huge-investment-top-ai-talent-eye-long-term

30）“Chinese Direct Investment in California 2017Update”
https://rhg.com/wp-content/uploads/2018/03/web_Chinese-Direct-Investment-in-California_2017-update.pdf

31）国務院，2017/07/20「国务院关于印发新一代人工智能发展规划的通知」

http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm

32）“Preparing for The Future of Artificial Intelligence” 2016/10
https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NS.C/preparing_for_the_future_of_ai.pdf
“The National Artificial Intelligence Research and Development Strategic Plan” 2016/10 https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf
“Artificial Intelligence, Automation, and the Economy” 2016.10
https://obamawhitehouse.archives.gov/blog/2016/12/20/artificial-intelligence-automation-and-economy

33） New York Times 紙, 2018/02/12
https://www.nytimes.com/2018/02/12/technology/china-trump-artificial-intelligence.html

34） 新京報他，2018/02/09
http://epaper.bjnews.com.cn/html/2018-02/09/node_31.htm

35）“More Money, Fewer Rules Could Help AI Grow, Experts Say”
http://www.nextgov.com/emerging-tech/2018/02/more-money-fewer-rules-could-help-ai-grow-experts-say/146004/

36） 産経新聞 2018/2/1 4

37） Revolution in Military Affairs：戦術・組織等といった，軍事に関する諸要素の革命的な変化のこと。

38） 原田泉『デジタル・デバイド』C & C 振興財団編　NTT 出版　2002/08（共著）第 8 章「軍事におけるデジタル・デバイド」

39）国务院关于印发新一代人工智能发展规划的通知
http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm

40） Elsa B. Kania,“Battlefield Singularity”, Center for a New American Security

41） WIRED“The next president will decide the fate of killer robots—and the future of war”
https://www.wired.com/2016/09/next-president-will-decide-fate-killer-robots-future-war/

42）Department of Defense DIRECTIVE NO. 3000.09 2012/11/21 Incorporating Change 1, May 8, 2017
http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf

43） 外務省 https://www.mofa.go.jp/mofaj/gaiko/arms/ccw/ccw.html

44） 2018 年 9 月 3 日　筆者の中国現代国際関係研究院でのヒアリングによる。

45） 産経新聞電子版 2018/9/3 https://www.sankei.com/politics/news/180903/plt1809030027-n1.html

46） 原田泉　危機管理研究第 25 号「IoT 時代に向けてのサイバー危機管理の現状と我が国の課題」2017/03

47）原案の骨子は，「AI の判断過程などについて企業に説明責任，AI が判断に誓ったデータのどの情報開示制度の創設，AI の透明度などを監視する機関の設置，AI の倫理性を認証する制度の創設，AI の欠陥による自己への賠償保険加入を企業に義務付け，AI を利用する企業の利益の一部を AI の透明化促進に還元」日本経済新聞　2018/11/6

48）「欧州委員会のカタイネン副委員長は 2018 年 10 月 23 日に「人工知能のルール作りで日本と協力できないか議論したい」と述べている。日本経済新聞　2018/10/23