国家サイバーセキュリティ通信統合センターで、サイバー攻撃対策の強化を表明するオバマ米大統領（ロイター / アフロ）

特集

技術革新と安全保障

新たな主戦場としてサイバー空間が登場し、
高度な民生技術や、AIやドローンに象徴される
自動化・無人化技術が容易に安全保障と結びつく時代――。
安全保障における「軍事」形態の変化の実情を描き出し、
それが投げかける課題と向き合う。

対談

政府はサイバー空間を守れるか

世界中でサイバー空間における攻撃が続いている。この状況を受け、今年七月、外務省はサイバー安全保障政策室を設置した。新たな形の脅威に、日本はどのように立ち向かうか。

土屋大洋
慶應義塾大学教授
齋藤 敦
外務省サイバー安全保障政策室長

――今世紀に入り、サイバー空間での脅威が増しています。

土屋 サイバー犯罪そのものは、決して新しい現象ではありません。二〇一六年三月に発売されたフレッド・カプランの *Dark Territory* という本に、コンピュータ制御の戦争を描いたSF映画『ウォー・ゲーム』（一九八三）を観た当時のレーガン大統領のエピソードが紹介されています。大統領が軍の統合参謀本部議長に「こんなことは可能なのか」と尋ねると、「大統領、問題はお考えよりもいっそう深刻です」という答えが返ってきたというのです。九〇年代には、ビル・クリントン政権のCIA長官ジョン・ドイチが議会公聴会で「電子的パール・ハーバー」の可能性を警告していますし、九八年には米軍のコンピュータが攻撃された「ソーラー・サンライズ」事件など、国際的なサイバー攻撃の事例もありました。

そのような動きの中で大きな転機となったのは、二〇〇七年のエストニアに対するDDoS（分散型サービス拒否、Distributed Denial of Service）攻撃です。ここ

から局面が大きく変わりました。マルウェアの統計も急増を示しています。

大規模化・複雑化する脅威

――具体的にはどのような脅威があるのでしょうか。

土屋　近年のサイバー攻撃は大きく四つに整理できます。第一にDDoS。不特定のコンピュータをウイルスに感染させ、特定の日時に世界中からターゲットめがけてアクセスを殺到させるものです。第二に、APT（Advanced Persistent Threat）。「高度で執拗な脅威」という意味で、電子メールやその他の形で相手のPCに忍び込んで情報を盗むものです。第三に、「サプライ・チェーン」といわれる、初めからソフトウェアやハードウェアの中に仕込んでおくものがあります。

第四は、これが最も深刻で、私はCCC（Cyber-Conventional Combination）と呼んでいますが、サイバー攻撃と通常兵器攻撃の組み合わせです。高度な攻撃ができ、事例も増えています。たとえば、サイバーを使って陸海空軍に同時に打撃を与えるようなクロスドメイン攻撃。ロシアの場合は、偽情報――たとえばウクライナ情勢が悪化したときに、「核兵器を使用する準備がある」といった情報を意図的に流す――を使った情報戦を組み込んだ「ハイブリッド攻撃」など、総じて、高度化、複雑化し、深刻度が高まってきています。

齋藤　ご指摘のとおり、サイバー空間での悪意ある行為は、個人レベルから組織化されたものへと変化しています。CCCやハイブリッド型などは規模が大きくなっているのと同時に、目的がわからない攻撃も増えています。今年一〇月には、米国の有権者登録データベースなど選挙関連システムがサイバー攻撃を受けました。これは単なる経済的利得とは異なった意図があると考えられます。

土屋　目的はいろいろ考えられますね。個人の不満の発露、経済的利得、政治的情報の獲得、そして軍事目的です。難しいのは、目的を持つ人々とは別に、実行を請け負う人々がいて、ブラックマーケットを形成していることです。だから、実行者の特定（アトリビューション）はできても、その背後にいる真の計画者は誰なのかわからない。

齋藤　まさに、そこが脅威の源泉です。

土屋　ただ、キングス・カレッジ・ロンドンのトマス・リッドというサイバーセキュリティ研究者は、国家が資金と人材をつぎ込めば、かなりの事例は特定可能だと言っています。実際、米国では、昨年のソニーピクチャーズへの攻撃

で北朝鮮を、今年八月の民主党全国組織委員会攻撃の際にはロシアを名指ししています。また、二〇一四年にはＦＢＩの捜査により米国政府が中国人民解放軍のサイバー部隊である61398部隊を国内で起訴しました。

齋藤　それでもなお、「特定」という点で難しいのは、名指しされたほうが否定すると、それ以上話が進まないことになりやすい。中国61398部隊の事件は、米中ともサイバー攻撃の存在自体は認めていますが、中国政府は関与を否定しています。米ロ間については、米国民主党に対するサイバー攻撃に対して、ロシア政府は「自分たちも米国から攻撃を受けているがいちいち非難することはない」という内容のコメントを出しています。具体的な攻撃行為に対して、国や組織が最終的にどう関係しているのか、判断するのは非常に難しいのです。

土屋　名指しされた国が認めることはないでしょうが、アトリビューション自体は、主要国がそれなりのリソースをつぎ込み、さらに国際協力が進めば、かなりの程度可能であるというのがリッドの主張です。米、英、豪などと協力を進めることで、かなり能力を改善できるはずです。それにより、サイバー空間の状況も変わるのではないでしょうか。

齋藤　国際協力は重要で、日本もこれまで九ヵ国（米、豪、

サイバー空間は世界中でつながっている。法の支配、信頼醸成、能力構築を柱に、国際協力を進めたい。

さいとう　あつし　1970年生まれ。97年慶應義塾大学大学院修士課程修了、外務省入省。経済学修士。在インドネシア日本大使館参事官、総合外交政策局総務課外交政策調整官などを経て、本年７月より現職（宇宙室長を兼務）。

英、仏、ロ、印、イスラエル、エストニア、韓国）と二国間協議を進めているほか、中国とは日中韓の枠組みで意見交換を行うとともに、EUとも協議を行っています。

土屋　中ロについて、もう一つだけ。中国やロシアでは、政府内でも民間でも、脆弱性の残るシステムのパソコンをかなり使っていて、他国が簡単にサイバー攻撃をかけられます。そのようななかで、両国ともサイバー攻撃の現状を十分に開示していません。ただ、先ほどご紹介したリッドの論文によると、アトリビューションには、技術的なレベルとオペレーショナルなレベルがあり、その上にストラテジックなレベルがあって、どのように公開し、国民や他国にどう伝えるかはストラテジックな判断が必要です。ですので、中国もロシアも、下のレイヤーから上がってきた情報をそのまま公開してはいない、ということでしょう。政治的、外交的な判断が必要となるので、各国の政治的文化が表れてくる部分です。

サイバー外交の三つの柱

齋藤　日本のサイバーセキュリティ戦略を外交面から進めるために、「サイバー空間における法の支配の推進」「信頼醸成」「能力構築」の三つの柱を掲げています。

土屋　法の支配について、国際的には、二〇〇四年にサイバー犯罪条約が発効しています。しかし締約国数は四九ヵ国と少なく、中国やロシアは締約国ではありません。アジアでは日本とスリランカの二ヵ国だけです。

齋藤　サイバー犯罪では、国家によるものと、個人など国家以外の主体によるものとを分けて考えていて、サイバー犯罪条約が対象としているのは、国家以外の主体です。その点でこの条約の内容が時代に合っていないとか、実効性に乏しいといった批判があるのは事実です。他方で、新たな条約を一から作れるかといえば、それは相当難しい。少なくとも、国家以外の主体を対象とした犯罪行為に関しては、この条約の締約国を増やしていくことが重要だと考えます。

――中ロが未加盟なのはなぜですか。

齋藤　この条約は、一九九〇年代末から欧州評議会で議論を重ねるなかで生まれた条約なので、条約の意図や締約までのプロセスに不信感があるのかもしれません。

土屋　中ロとしては、自国が行っている国内の検閲や情報管理を国際的に認めてほしいということではないでしょうか。サイバー犯罪条約ではそこが確保されていない、と認識しているのでしょう。

齋藤　一般論として、情報の自由な流通は、国内政治に対する批判的な見方を生む可能性があるので、規制したいと考える国もあるでしょう。そういう国は、条約ではなく自国の制度で管理したいのではないでしょうか。

土屋　先ほど、ロシアの「ハイブリッド攻撃」に言及しましたが、あるロシア人の研究者に言わせると、自分たちも米国から同じ攻撃を受けていると訴えます。やれ民主化が進んでいない、総選挙には不正があるなどと言い続けることこそハイブリッド攻撃ではないか、と言うのです。この話を聞いて、ロシアにとって、あるいは中国もそうかもしれませんが、コンテンツ自体もサイバーセキュリティの領域に入っているのではないか、と思いました。われわれがサイバーセキュリティを考える場合、マルウェアとかウイルスといったプログラムの話に収斂させがちです。その意味で、中ロとわれわれとの間にはコンセプトのずれがあるかもしれません。

齋藤　コンテンツの中身への介入は、政治的観点のみならず、宗教的・文化的観点からの介入もありえます。その意味では、認識のずれは中ロに限ったことではありません。いずれにせよ、それを克服していくためには、国際社会の主要国が議論を主導しつつ、さまざまな機会を通じて多くの国と信頼関係を醸成していくしかないと思います。

安全を高めるのためには、政府だけでなく、基幹インフラを担う民間企業の協力が不可欠だ。

つちや　もとひろ　1970年生まれ。99年慶應義塾大学大学院政策・メディア研究科後期博士課程修了。博士(政策・メディア)。国際大学グローバル・コミュニケーション・センター助教授、慶應義塾大学准教授などを経て、2011年より現職。著書に『サイバーセキュリティと国際政治』『暴露の世紀』など多数。

土屋　非国家主体によるサイバー犯罪については、国際刑事警察機構（インターポール）が、二〇一五年、シンガポールに、ＩＧＣＩ（インターポール・グローバル・コンプレックス・フォー・イノベーション）というサイバー犯罪に特化した組織を創設しました。日本の警察庁から中谷昇氏が総局長として赴任しています。中谷氏のお話では、ＩＧＣＩが対応できるのは非国家主体によるサイバー犯罪だけで、国家が絡むサイバー戦争には関与できないということでした。一方、サイバーセキュリティが問題になる場合のほとんどはサイバー犯罪であるとも述べています。ＩＧＣＩはインターポールの組織なので一九〇ヵ国が加盟していて、かなりの数のサイバー犯罪に対処可能です。ですから、非国家主体によるサイバー犯罪と、国家絡みのサイバー戦争やエスピオナージ（スパイ行為）とを切り分け、前者についてはＩＧＣＩ、後者については別の枠組みで対応していけばよいと思います。

国連の枠組みでの取組

齋藤　国家主体の行為を規律する重要な枠組みの一つが、国連の下にある政府専門家会合（ＧＧＥ）です。現状では、国家を主体としたサイバー空間への攻撃に特化した国際的なルールはありません。それでは、既存の国際法をどれだけ適用できるのかを検討するとともに、適用できない部分にはどう対応するか、法的な拘束力がない形であっても何らかの決まりを作るべきではないか、という機運が高まった結果、国連でＧＧＥが組織されました。

土屋　二〇〇四～〇五年に第一会期会合が開催され、現在は第五会期会合が今年八月から開催されています。ひとつ気になるのは、中ロ間の溝についてです。ある国際会議で中国人研究者は、「ロシアは、二〇一五年一二月のウクライナに対する電力網の攻撃などで、ＧＧＥが積み重ねてきた成果を台なしにした」と批判していました。一方で中国は、米国と一五年にサイバーに関して合意をしています。中ロの間に対応の差ができている気がするのですが……。

齋藤　国連ＧＧＥで議論していくことについての認識は共有されていると思います。ＧＧＥは、二〇一五年の第四会期会合で一致した事項について報告書を公表しています。その中で最も重要なポイントは、既存の国際法がサイバー空間にも基本的には適用されると合意したことです。国際社会での法的安定性がある程度確保できました。中ロもこれを前向きに評価しています。

土屋　ぜひ日本が影響力を行使して、イニシアティブを

とってほしいと思います。

アジアの能力開発に寄与する

齋藤　このあたりは「法の支配」と「信頼醸成」とが重なり合う部分でもありますね。

土屋　信頼醸成の大切さは言うまでもありませんが、現実には難しい問題です。

齋藤　信頼醸成は、「透明化」と「安定化」の二つの措置に大別されます。透明化とは、政策や意図を互いに説明し、相手をよく知ること。安定化とは、対立をエスカレーションさせないための措置を講じていくことです。定期的な対話はもちろん、問題発生時の速やかな連携、事例ごとの対応の共有などです。いずれも、眼前の問題だけでなく、中長期的な関係の構築・深化を重視しています。日本としては、G7各国のほか、日中韓三ヵ国の枠組みやロシアとも協議を実施しています。

土屋　エストニアやインド、東南アジア諸国連合（ASEAN）、北大西洋条約機構（NATO）とも始めていますね。

齋藤　サイバーの性質上、世界のあらゆる国々との対話が必要なので、適切なプライオリティを置きながら進めています。

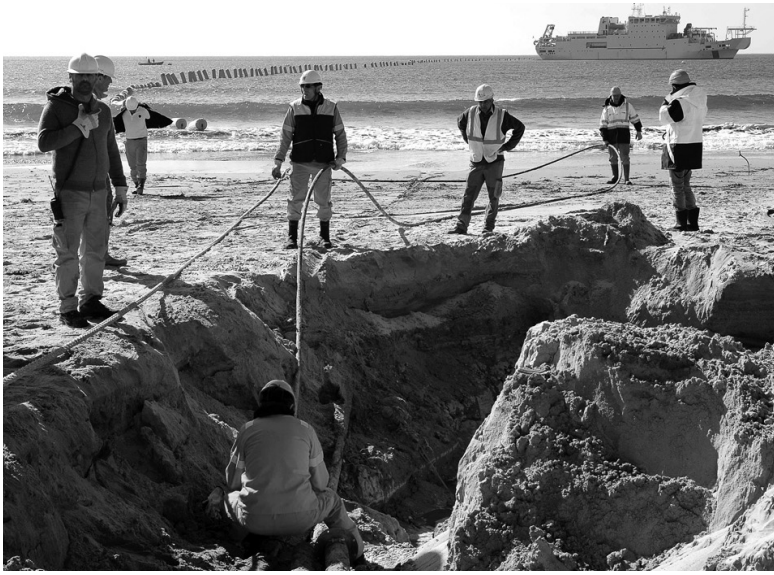
土屋　今年五月のG7伊勢志摩サミットでも議論されました。

齋藤　G7サミットとして五年ぶりにサイバーをテーマに議論し、G7首脳声明と付属文書を発表しました。情報の自由な流通を確保しながら、人権等の国際的な原則はしっかりと守ったうえで、サイバー空間における安全および安定を促進するとともに、経済発展を推進するようなサイバー空間をつくっていこう、という内容です。G7とはこのように認識を共有する部分が大きいです。

土屋　ASEANなどとの協力は、三本目の柱の「能力構築」にもつながります。

齋藤　能力構築支援については、関係省庁全体で基本方針を策定し、本年一〇月に行われたサイバーセキュリティ戦略本部で報告したところです。まず、ASEAN諸国を中心に、能力構築の取り組みを進めることにしています。インシデント（事案）に対する対応能力の向上、サイバー犯罪対策の支援、またサイバー空間に関する国際的ルール作りおよび信頼醸成措置に対する理解・認識を共有し、日本の経験や知見を活かして協力していきたいと思います。

土屋　能力構築において、知識やスキルはもちろん重要なのですが、そもそも多くの途上国においては、インフラが



フランスからシンガポールまで17ヵ国を結ぶデータ通信用海底ケーブルを敷設する作業員。2016年3月、仏南部のラセーヌシュルメールで（AFP =時事）

決定的に足りていません。特にサブサハラのアフリカと太平洋島嶼国は、デジタル・デバイドに苦しんでいると言われてきました。サブサハラ・アフリカのほうは、東海岸、西海岸それぞれに海底ケーブルがつながってきましたが、太平洋島嶼国には未開通の島国がたくさんあります。通信は商業性があるから政府開発援助（ＯＤＡ）を使えないというのが日本政府の従来の立場でしたが、たとえばパラオは人口二万人で、商業ベースにはのりません。教育ではインターネットはもはや必需品であり、環境構築を日本が支援することはとても重要な外交の一環になるはずです。ぜひそこまで含めたパッケージで、能力構築をやっていただきたいですね。

齋藤　まさに国連の持続可能な開発目標（ＳＤＧｓ）につながる話だと思います。二〇一五年に合意した今後の開発目標（二〇三〇アジェンダ）の中にも、途上国に対してインターネット・アクセスの保障を高めるという指標があります。

セキュリティは異なる次元へ

土屋　先ほど、サイバー犯罪条約をめぐっては中ロ両国と根本的なところで認識の違いがあるのではないかという問題提起をしました。国際社会でサイバーセキュリティを確保するためのさまざまな取り組みの進展がある一方で、自由な情報の流通が危機に瀕しているのではないかという問題意識を持っています。

スノーデンが明らかにしたように、各国のインテリジェ

ンス機関は常に監視を行っていますが、通信のセキュリティを担保する今までの暗号レジームは、日米欧の技術者たちがアルゴリズムを公開し、お互いに対話しながら作ってきました。しかし、中国をはじめ何ヵ国かが独自のアルゴリズムを作り、しかも公開せず、いかに他国に読ませないかを考え始めています。そうなると、ある暗号が、中国のブラウザに組み込まれた鍵では認証できても、他のブラウザでは見られない、といったことも起こりえます。そもそもインターネットはあらゆる物理的障害を乗り越えて繋がることができるものだったのに、そうではなくなってしまうわけです。

齋藤　セキュリティの確保は重要で、そのための努力は各国とも必要です。ただそれが、他国との自由な情報の流通を妨げるものになってはいけないというご指摘は重要です。情報の自由な流通の確保を前提としたうえで、最低限どのような規制や取り組みが必要なのか、という観点で考えなくてはいけません。規制や防御が先行する逆転した議論もあり、懸念しています。

土屋　ＩｏＴ（Internet of Things）、人工知能（ＡＩ）、共有されないアルゴリズムといったものが次々と現れて、今後セキュリティは、外交や安全保障のレベルを超えた次元に行ってしまうのではないかと危惧します。

齋藤　ＡＩもＩｏＴも、生活を豊かにしていくものとして、どんどん促進する必要がありますが、同時に、その活用が、国民の安全や安心を脅かすことがないように、国際的な議論を重ね、制度を整える必要があります。技術の進歩にあわせて、不断に検討を続けなければなりません。

土屋　ソフトウェアによるサイバー攻撃は、今後必ず増えます。今後問題の焦点になってくるのは「ボット」と呼ばれる自動実行プログラムでしょう。人間が関与せず、自律的に相手の脆弱性を探し、二四時間三六五日攻撃し続ける。その相手方もボット。ボット対ボットの戦争もそう遠くないかもしれません。そうなれば、今までの戦争のルールでは対応できない。ハイブリッドで、クロスドメインな戦争が始まったとき、ドローンを飛ばす戦闘員はもう軍服など着ていないでしょう。ＧＧＥの次の段階として、新しい戦争のルールについての議論が現実問題として必要になってくるのではないでしょうか。

齋藤　伝統的な国際法は、国と国との関係を規律するものですが、サイバーの世界の出来事は国が把握できない要素も多い。そこでの対応には、二つのステップがあります。まず、既存の国際法の枠内で解決する。人道法的な部分で

あれば、「識別の原則」や「均衡性原則」ですね。次のステップとして、国家以外の主体にどう対応するか。まさに新しい課題です。テロリストや犯罪者によるサイバー空間の悪用が、国際社会全体の脅威となっているのは明らかですので、各国の協力が必要です。

「戦争」におけるルールの変更

土屋　サイバー空間においては、「識別の原則」はもはや適用されていないと考えねばなりません。官民を問わず重要なインフラストラクチャーは攻撃対象として想定して準備が必要です。そして、「均衡性原則」に関していえば、原発に対するマルウェアなどによるサイバー攻撃が行われ、何らかの被害が出た場合を想定すると、物理的な爆発などであれば戦争行為として「均衡のとれた」反撃は想定できますが、より低レベルの攻撃、たとえば原発の停止や情報の消失などの場合、何が「均衡した」反撃と言えるのか。米国政府は「サイバー攻撃を認識したら核ミサイルを使う」と言っていましたが、いくらなんでも無理な話です。

齋藤　確かに難しい問題です。二〇一四年のNATOのウェールズサミット首脳宣言では、サイバー攻撃がNATOの集団安全保障につながりうるかどうかは「ケース・バイ・ケース」で決められるとされていました。つまりその基準は明確にしないということです。いったん基準を明確にしてしまうと、それに及ばないレベルの攻撃をかえって惹起する可能性が生じます。

土屋　おっしゃるとおり、メニューをはっきり作っておくと、逆に「そこまではやっていいんだ」ということになりかねません。ある程度曖昧にしておくことは、防衛の観点から重要です。

　そうすると、現実的に可能な対応は、米国が行ってきたことを見ても、経済制裁ということになります。確かに効果はある。昨年九月の米中合意は、中国が米国の経済制裁を怖れた結果でしょう。しかし、すでに制裁が行われている米ロ関係では、今さら制裁を追加してもあまり効果はない。北朝鮮も同様です。

　米国が経済制裁と並んで行っているのが、「ネイム・アンド・シェイム」、つまり名指しをして恥さらしにすることです。ほぼ黒だと特定したら――そこに政治的な判断が入るとは思うのですが――名前を公開する。これはかなり効果があると思います。日本は通信の秘密を重視していますからアトリビューションが難しいですが、他方でその能力を高めることは責任ある国家としてもはや必須の条件で

す。その結果を他国と共有することは、国際協力にもつながりますし。

齋藤　アトリビューション能力は抑止力にもなります。難しい問題の一つは、民間との情報共有です。民間も含めてインシデント情報を把握し、それを基にした対策を取る必要がありますが、現状では難しさがあります。日頃から連携を取り、ニーズを吸い上げる努力が必要です。

土屋　私は、民間企業であっても国家の基幹インフラを担うような場合は、従業員の通信の秘密がある程度制限されるのは当然だと思います。とはいっても、たとえば組織内の電子メールやインターネットの利用に、公私の区別をつける、といった程度の意識改革です。政府や会社のマシンを使用する際は、政府や会社のための通信に限り、プライベート目的の使用はやらないと決める。マシンは政府や会社の資産なのですから、その使用を把握したり限定したりすることは法的に可能です。そこでの通信は監視されて当然、という意識に改革する。

　さらに、重要な基幹インフラを持つ組織は、社内にセキュリティ対策部署を設置することはもはや必須で、それぞれの内部で監視した結果を業界他社と共有し、さらに管轄する官庁と密接に連絡を取っていくとよいと思います。

齋藤　まずは個々人でしっかりやっていただく。その上で、組織としてどこまで把握可能なのかは、議論する必要があると思います。日本政府の中では、内閣サイバーセキュリティセンター（ＮＩＳＣ）が、政府機関等においてインシデントが発生した場合はすぐに状況を把握できる態勢を整えています。

土屋　同時に人材の育成も進めなくてはなりません。人材のあり方はピラミッドです。頂上のトップガン的な人材を大量に育てる必要はなく、それを支える人材をもっとしっかり育てる必要があると思います。そのためには、早期の教育が必要ですし、専門職として確立させ、キャリアパスを作っておく必要がある。そうでないと、なかなか人材は育たないと思います。

齋藤　人材は国内、国際、両方の側面で重要になると思います。現在、日本政府も人材育成の強化を進めています。また、サイバー空間は国際的につながっていて他国の脅威は日本にも波及しますので、その人材育成への協力も必要です。サイバー空間をどう使うか、どういうセキュリティが必要なのか、といった基本的なレベルからの、幅広い人材育成が必要だと思います。●