2025年10月

シリーズ 「日本のサイバーセキュリティ政策史」第 10 回（連載全 2 回）

サイバーセキュリティはいつ、なぜ安全保障政策になったのか［前編］

～情報保全から安全保障へ～

サイバーセキュリティ政策分野に詳しい三角育生氏が日本の同政策史をひもとく本シリーズ。今年 5 月、いわゆる能動的サイバー防御導入に関する法律「サイバー対処能力強化法」及び同整備法が成立し、公布されました。そこで今回は、サイバーセキュリティと安全保障の問題を掘り下げます。サイバーセキュリティがどのように安全保障に関わる政策枠組みの中で重要度が高まっていったのか。2013年12月に国家安全保障会議（NSC）と閣議で決定された「国家安全保障戦略」策定作業において中心的役割を果たされた高見澤將林氏をお迎えし、安全保障政策の視点からの背景や理念を明かしていただきます。

【出席者】

高見澤 將林 氏
公益財団法人笹川平和財団上席フェロー／元内閣官房副長官補（事態対処・危機管理担当、国家安全保障局次長及び内閣サイバーセキュリティセンター長を兼務）／元軍縮会議日本政府代表部特命全権大使

聞き手：
三角 育生 氏
東海大学情報通信学部長・教授

日本における情報をめぐる「カルチャー」の課題

三角 今年 5 月、いわゆる能動的サイバー防御導入に関する法律「サイバー対処能力強化法」（重要電子計算機に対する不正な行為による被害の防止に関する法律）及び同整備法が成立し、公布されました（2 月 7 日閣議決定、5 月 16 日成立、同 23 日公布）。高見澤さんは、2013～2016 年に内閣官房副長官補の任にあり、日本初の国家安全保障に関する基本方針である「国家安全保障戦略」（2013 年 12 月 16 日閣議決定）の策定作業において中心的役割を果たされました。本日は、同戦略策定の背景や理念についておうかがいします。

日本のサイバーセキュリティ体制の歴史を遡ると、2000 年の IT 基本法（高度情報通信ネットワーク社会形成基本法）を起点に、さまざまな取り組みが進められてきました。同年、IT 戦略本部決

定「情報セキュリティ問題に取り組む政府の役割・機能の見直しに向けて」により、内閣官房に情報セキュリティ対策推進室が設置され、2005 年には内閣総理大臣の決定により、同推進室は内閣官房情報セキュリティセンターへと改組されます。その後、2014 年の「サイバーセキュリティ基本法」制定に伴い、内閣官房情報セキュリティセンターは内閣サイバーセキュリティセンター（NISC）へと改編され、2015 年には「サイバーセキュリティ戦略」も閣議決定されました。こうした流れの中で、サイバーセキュリティ政策の根本は IT 気質にありながら、安全保障の課題として強く取り上げられるようになってきています。

安全保障の枠組みの中で明確にサイバーセキュリティが記述されたのは、2013 年 12 月に発足した国家安全保障会議（NSC）の下で策定された「国家安全保障戦略」です（4 章 1 節 5 項「サイバーセキュリティの強化」）。また、本戦略を指針として「サイバーセキュリティ戦略」(2015)においても安全保障の節が設けられました（5 章 3 節「国際社会の平和・安定及び我が国の安全保障」）。まずおうかがいしたいのは、これらの戦略が策定された背後にどのような安全保障の考え方があり、その中でサイバーセキュリティがどのように位置づけられていったのかという点です。

高見澤　日本の安全保障・防衛戦略におけるサイバーセキュリティの位置づけを私なりに簡単に整理すると、当初は、サイバー攻撃への対処というよりも、機密情報が漏洩しないように守るという情報保全の観点で捉えられていました。その後、2000 年の IT 基本法の整備や Y2K 問題などを背景として、サイバー空間に接続されたシステムが、日本の安全保障・防衛においてきちんと機能する必要があるという問題意識が高まりました。この段階では指揮情報通信システムの機能の高度化に伴う課題の一つとしてサイバー攻撃への対応が意識されはじめたという段階にとどまっていたと思います。

三角さんから「サイバー対処能力強化法」のお話がありましたが、サイバーセキュリティと安全保障の関係については、日本では長らく安全保障問題をタブー視するところがあって、政府全体として、産官学の間で安全保障に対する問題意識が共有されてきませんでした。サイバーセキュリティについても、同様のことがいえるのではないかと思いますが、この分野では、特に情報をめぐる「カルチャー」の問題が影響しています。

日本の情報文化には多くの課題があります。第一に、共有の文化の欠如です。情報を共有するという発想が希薄ですし、その結果共有のルールもありません。第二に、システム連携への抵抗です。情報をシステムでつなぐことに対して、そもそも危険だという認識や安全保障と関わることへの懸念が根強い。第三に、情報が「陰の仕事」というイメージです。諸外国では、情報は「安全保障のための最前線の仕事」という認識がありますが、わが国では必ずしもそう捉えられていません。第四に、情報を扱う人のインテリジェンス・リテラシーが十分でないことがあります。そして第五に、政策イニシアティブの不足です。政治的リーダシップの下で、新しい政策に取り組むことになれば、そのために必要される情報が明確になり、政策の遂行と結びついた継続的な情報活動がサイクルとして生まれます。機密情報についてもそこに光が当たり、さらに活用されていきます。こういうことをやりたいという積極的な意欲がなければ、せいぜい「知っている」というだけになり、宝の持ち腐れになってしまいます。

このような状況が何をもたらしているのか。各省庁や組織が保有するデータについて、具体的な内容に応じて分類づけをして一体的に管理するという発想が欠如しがちです。「持っている」という観点から文書管理は行うものの、どの情報のどの部分が機密性が高く、どの情報がどの施策に有効で、いかに関係者と共有し、活用すべきかを識別する文化が育っていません。

三角　たしかに政府組織の一部では一律に機密性を高く設定しているところがある一方で、機密性に敏感でない組織も多いですね。

高見澤　おっしゃるとおりです。少しでも機密性のある情報が含まれていると個別の内容に関係なく、十把一絡で「しまっておく」傾向が強かったと思います。

このような背景を理解した上で、日本の安全保障・防衛戦略においてサイバー攻撃への対処がどのように扱われてきたかを考えるべきです。

日本の防衛の戦略文書である「防衛計画の大綱」（以下、「大綱」）はこれまでに 6 回策定されています。最初が 1976 年（昭和 51 年）の「昭和 52 年度以降に係る防衛計画の大綱について」（51 大綱）です。その後 19 年を経て 1995 年（平成 7 年）に新たな大綱（07 大綱）が策定されます。これらの大綱では、時代背景もあり、サイバーセキュリティのコンセプトは確立していませんでした。また、大綱だけでなく、1978 年に初めて策定され、1997 年に改定された「日米防衛協力のための指針（ガイドライン）」でも、どちらかというと情報保全の観点から論じられています。

2004 年（平成 16 年）に策定された大綱では、初めて「サイバー攻撃にも対処し得る高度な指揮通信システムや情報通信ネットワークを構築する」ことが謳われました。もっとも、防衛省は IT 戦略あるいは IT 基本法の策定には深く関与していませんでしたので、安全保障とはいわば切り離された形で流れができていた中で、サイバー攻撃も意識されてきたということではないかと思います。

2010 年（平成 22 年）の大綱（22 大綱）では、サイバーセキュリティについて、時代の変化を反映して一定のコンセプトが示されました。具体的には、海洋や宇宙と並ぶ国際公共財という観点から「サイバー空間の安定的利用に対するリスク」について安全保障上の新たな課題と認識し、「サイバー攻撃への対処態勢及び対応能力を総合的に強化する」ことや「地域的及びグローバルな協力を推進する」ことが謳われました。しかし、サイバー攻撃への対応に対する包括的な指針は示されておらず、「自衛隊の情報システムを防護するために必要な機能を統合的に運用して対処するとともに、サイバー攻撃に関する高度な知識・技能を集積し、政府全体として行う対応に寄与する」

対談風景。左が高見澤氏

ということで一歩引いたような方針でした。それまでの大綱は、防衛政策や防衛力整備に関する課題を検討し、対応方針を示すというものであったため、ある種閉鎖的というかスコープも狭く、他省庁の関心も低かったというのが実態です。

国家安全保障戦略とサイバーセキュリティ

三角　サイバーセキュリティは当初、防衛戦略においては情報保全という感覚で捉えられていたところ、2010 年頃からサイバー攻撃の問題が顕在化し、米国の影響もあって日本でも徐々に問題意識が高まりはじめたわけですね。

髙見澤　こうした中で登場したのが第二次安倍政権（2012 年 12 月発足）です。国際情勢が厳しさを増す中で、国家安全保障戦略的なものを作成しなければ、日本として総合的な安全保障は実現できないという認識が高まりました。それが NSC の設置、特定秘密保護法の整備、国家安全保障戦略の策定、そしてそれに続くサイバーセキュリティ基本法、平和安全法制の策定へとつながる流れであったと理解しています。国家安全保障戦略を作成しようという時点では、サイバーについて総合的な取り組みをする必要があるという問題意識は防衛省の中にもありましたが、それを実現する手段がなかった。

もっとも、国家安全保障戦略の策定プロセスの中では、サイバーセキュリティは主要課題ではありませんでした。むしろ、その後の平和安全法制につながる「シームレスな対応」や対中戦略に重点が置かれていました。新しい防衛力のコンセプトをどのように構築するか、あるいはそれまでと同様に防衛関係費や自衛隊の規模は縮減する方向でよいのかといった問題や方向転換を図るためのさまざまな仕組みづくりが議論の中心だったと思います。

その背景には当時の国際情勢があります。米欧においてロシアへの不信感は芽生えはじめていましたが、ロシアによるクリミア侵攻（2014 年）以前で、ロシアが主要8カ国（G8）のメンバーだった時代です。スノーデン事件（2013 年）はありましたが、米国によるサイバー空間における活動について広く知られるようになったのはもう少し後だったような気がします。

サイバーに関する国際ルール設定の場、サイバーセキュリティに関する政府専門家会合（GGE）などでも、米ロや米中の対立は先鋭化していませんでした。2000 年代からの米国は 9.11 テロの影響で国際協力に焦点を移し、中国や G8 体制下での対テロ対策協力を重視していたわけです。

こうした状況の下では、国家安全保障戦略の策定過程においては、サイバー分野について当初から安全保障の観点から包括的に位置づけてきちんと検討するための作業には十分な時間が割けず、他の多くの重要案件に埋もれてしまった感がありました。私自身 NISC の代表でもあったわけですが、国家安全保障戦略の当初の草稿におけるサイバーに関する記述について「甘い」と困惑していたほどです。

三角　「甘い」とはどういうことでしょう。

髙見澤　その頃には、「サイバーセキュリティ戦略」がすでに情報セキュリティ政策会議においてとりまとめられていた（2013 年 6 月）わけですが、そもそも国家安全保障戦略の検討においてはサイバーに関する記述が少なく、具体的な施策に関する言及も少なかったのです。私自身はサイバ

一戦略の策定には直接関与していたわけではなかったので、谷脇（康彦）さん、三角さん、山内（智生）さんなど NISC の幹部らと議論を重ねる中で、安全保障の観点から「もう少し強い方針を打ち出すべきではないか」という感覚を得ました。そこで、一気にはいかないまでも、今後の政府全体としてのサイバーの取り組みにつながる内容を盛り込めないかと、国家安全保障戦略の議論の後段になって、「みんな知恵を出そう」と呼びかけをしたのが私の記憶です。これに対して、NISC 幹部組は、今まさに基本法のようなものが整備されるべき時期である、いいチャンスだという認識でした。結果として、将来のサイバーセキュリティ強化に向けた検討項目が国家安全保障戦略に盛り込まれることになったと記憶しています。

そうはいっても、依然としてサイバーセキュリティを安全保障上の最重要課題として積極的に推し進めるというよりは、「政府全体で協力しないとサイバーセキュリティは実現できませんよね」というような、やや中立的な書き方にとどまりました。さらに展開すべきという思いはありましたが、あまり踏み込んだ書き方にはできなかった。一方で、政策をさらに推進するための前提として、実態把握が重要だということで、ペネトレーションテストや最先端技術の活用など、次につながる要素は随所に散りばめることができました。

一体的な運用ができなかった要因

三角　次におうかがいしたいのは、サイバーセキュリティ対策における「連携」についてです。NSC が発足した翌月の 2014 年1月に国家安全保障局（NSS）が発足します。NSS には各省庁から行政官が出向または併任する形で所属しました。NISC の一部行政官も併任になりましたが、実際には「お客様」のような扱いで、内部に深く関わる機会はさほどありませんでした。本来、緊密な連携が必要であるにもかかわらず、「縦割り」が強かった印象です。これは何が原因だったと考えられるでしょうか。

高見澤さんは今年 3 月 28 日、サイバー対処能力強化法について衆議院内閣委員会に参考人として出席され、各方面との連携の重要性を指摘されました。そうしたお考えをお聞かせください。例えば、安全保障側の人々がサイバーセキュリティを単なる技術的な問題、あるいは技術者の話と捉えていたのでしょうか。それとも、NISC といったサイバーセキュリティ政策側の人間が、安全保障に対する理解が不足したまま、サイバーセキュリティ政策の話を進めていたことが原因でしょうか。あるいは、単に出身省庁の文化的な背景が影響していたのでしょうか。はたまた、安全保障は NSC が総指揮を執り、サイバーセキュリティはサイバーセキュリティ戦略本部長の官房長官の下で現場について現場の担当者に任せるという形を目指していたということでしょうか。今後、新しい体制を構築していく上で参考になると思うのです。

高見澤　難しい質問ですね。結論を先に言えば三角さんの指摘されたすべての要素が多かれ少なかれ絡み合っていると思います。特に一体的な運用ができなかったことは、先ほど述べた情報共有の文化や制度に関連しますので、少し長くなりますが、説明させてください。

国家安全保障会議設置法で画期的なのは「内閣官房長官は……議長の求めに応じて、会議に対し、国家安全保障に関する資料又は情報提供……を行わなければならない」（同法 6 条）という

表現が入っていることです。NSC の議長（総理大臣）が内閣情報調査室（内調）に対して「国家安全保障会議に情報を提供せよ」と言ったら、内調は情報を提供しなければいけないことが法的に担保されたということです。そして、NSC の事務を司る NSS ができて、しかもそれは内閣官房の総合調整機能を活かせる立場の「局」にしたわけです。すなわち、国家安全保障会議設置法により NSC の情報集約機能が実現した結果、NSC の事務局たる NSS にも関係省庁は情報提供しなければならなくなった。そこで、非常に機微な情報を含めて、NSC を中心にみんなで取り組むことになったわけです。

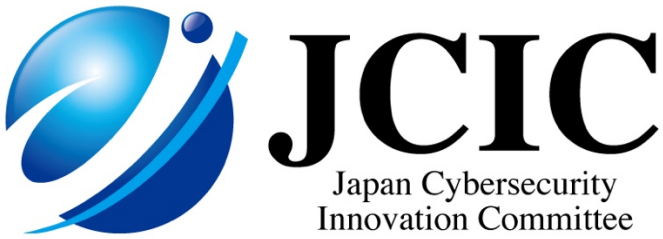
ちなみに、第一次安倍政権時代（2006～2007 年）の構想では、NSC の事務局である NSS は内閣官房ではなく、内閣に置く形でした。つまり、現在の NSS が持つような各省庁を横断した強力な総合調整機能は想定されておらず、他の省庁や組織と隔絶された役割を担う可能性があったわけで、そこが大きな違いです。

NSC（四大臣会合）に常時出席し、かつメインテーブルに座る事務方のメンバーは、私の知る限り 8 人でした。それは国家安全保障局長（当時は谷内正太郎さん）、国家安全保障局次長（[兼]内閣官房副長官補）の 2 人（当時は兼原信克さんと私）、内閣危機管理監、内閣情報官、防衛省の統合幕僚長と防衛政策局長、そして外務省の総合外交政策局長です。これ以外の人も出席しますが、この 8 人は常にメインテーブルに座っていました。この 8 人は会議に出席し、必要な情報や資料について報告し、閣僚からの御下問に答えながら議題を深掘りできる材料を提供するというスタイルがつくられました。

例えば安倍総理（当時）が「今日はこの議論をしよう」とおっしゃると、機微な情報についても説明して、「そうなるとこの方針でいいな」「いや、こういう情報もあります」「だったらこうした観点から分析したらどうなるのか」「その点については」という具合に閣僚はもちろん 8 人の誰かもその場でやり取りしたわけです。そのような雰囲気を安倍総理や麻生太郎副総理（当時）がつくっておられました。加えて谷内さんの特別な存在感もあって、みんなで活発に議論するわけです。そこでの情報活動は、安倍総理からの指示が「これについてはこうしたいから調べよ」という具合で、政策の方向性がはっきりしていました。そうすると、NSS では機微情報についてもみんなで集めるし、すべての関係省庁が集まってくる状況になります。この 8 人は NSC で何か説明したり発言したりしなければならないため、当然、その下のスタッフも役所の壁を越えて連携して作業に取り組みます。その結果、NSS の中で情報が一体化され、立体的なものとして扱う習慣ができました。

ちなみに昔の国防会議や安全保障会議では、すでにシナリオが決まっていることが多かったと思います。また事務方は少数を除いて後席に控えていて、発言する機会はほとんどなく、細かい話になって閣僚が後ろを向くときや資料説明を求められたときだけに発言が許されるという感じでした。

（「後編」につづく）



[本調査に関する照会先]

JCIC 事務局　info@j-cic.com