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[後編]

～国家像があって初めて安全保障のあり方が見えてくる～

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。今回は、髙見澤將林氏をお迎えし、サイバーセキュリティと安全保障の問題を深掘りします。2 回連載の「後編」では、ご自身の経験を踏まえつつ、省庁間協力の実現策、サイバー対処能力強化法の施行における重い課題、そして日本のサイバーセキュリティ政策のあるべき姿について論じていただきます。

【出席者】

髙見澤 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

共通課題に一緒に向かう仲間だという感覚を持てるかどうか

三角 2013 年に国家安全保障会議設置法に改正され、国家安全保障局（NSS）が設置されることで、従来の安全保障会議から議論の進め方などが画期的に変わったわけですね。

髙見澤 機微情報を「官邸には報告しても他省庁には出すな」だったのが「NSS に出せば情報が増える、得をする」という感覚になったのは大きな進歩です。

とはいえ、変わったのは安全保障会議に密接な関係を持つ中央省庁だけで、サイバー関係について「みんなでやりましょう」とはなりませんでした。例えば、事態室（内閣官房副長官補[事態対処・危機管理担当]付）と内閣サイバーセキュリティセンター（NISC）の情報共有について機微情報も含めて拡大する体制が構築されたわけではなく、外部に機微な情報を出すことには抵抗感があったことは課題として残りました。というのも、例えば平和安全法制関連では情報漏洩を非常に警戒していました。政治指導者、四大臣会合を中心とするところでの情報共有は格段に高まって、ほとんど何も隠し事がない状態ができた一方、そこに情報を集約して少数で議論しているからいいけれど、逆に、大勢で共有するとやはり漏れるという認識になっていたのかもしれません。

私自身は、事態室も NSS も NISC も大事にしていましたし、一体的に運用しなければならないと思っていました。ところが、相互に難しい感情があったわけです。NSS からすれば、事態室は国際的なことがわかっていない内向きの対処組織に見えていたようです。一方、事態室からすれば、

高見澤氏

NSS は対処の現場を知らない政策組織だと見えていたようです。NISC は、スタッフが多様で IT 分野を中心に人材が集まっているため事態対処などについて理解が進まないような感じがあったと思います。一方で、事態室からは、なぜ NISC には当直しない職員がいるのかという声が聞こえたりする。互いに文化が違っていました。

NISC が致命的だったのは、情報の機微な扱いを非常に気にしている人たちからすれば、民間から出向してきた人が多数所属していることです。日本にインテリジェンス共有の文化がないことを先ほど指摘しました。やっと特定秘密保護法（2014 年施行）ができましたが、その対象は狭かったという事情もあります。今年（2025 年 5 月）になって機微な情報を民間も含めてより幅広く共用するためのセキュリティ・クリアランス制度が全面施行されるようになりましたが、当時は機微な情報の扱いを理解している人とそうでない人たちの間に意識やスキルの点で大きな違いがあったと思います。インテリジェンス・リテラシーを高めて、データのガバナンスを行い、しっかり分類・サニタイゼーションをして、必要な情報を関係者間で極力共有する文化に変えていかないといけないのですが、なかなかできなかったというのが実態です。

サイバー分野に特徴的な難しい要素として、技術そのものの理解や技術的課題に対する取り組みにくさがみなさんにあったのではないかと思います。私自身、求められる知識が多くて「大変だな」と感じていました。もともと日本ではサイバー分野はかなり民間が主導しており、強制ではなく自主的なやり方や協力関係で成り立っている部分があったり、また独自の高度技術が絡んでいたりと、官民協力の最も難しい部分の特性をたくさん持っていたと思います。

三角　私は経済産業省（通商産業省）で安全保障輸出管理を担当し、外国の情報の機微な取扱いを経験していたので、関係者の情報の取扱いに対する姿勢のギャップを感じました。2005 年に情報セキュリティの業務についたとき、サイバー関係者が「情報共有しないとセキュリティを確保できない」というマインドであることに接して、従来の自分の意識とのギャップを感じました。実際、私が NISC に在籍していた当時、「NISC には民間人がいるから情報を提供できない」というような言い方をされたときには「困ったな」という感じはありました。

高見澤　そこは組織や文化もありますが、「人」による問題が大きいのではないかと感じています。組織や文化の違いを許容する、あるいは楽しむような雰囲気を持つか持たないか。サイバーならサイバーという共通の課題に一緒に向かっていく仲間だという感覚を持てるかどうかが鍵だと思います。確かに「省庁が違えば文化が違う」ため、話が通じていないということもありますね。例えば、職場で話していた内容を、そのままオープンな場で話す人がいたとすれば、特に情報管理を大事にする人からすれば、非常識で信頼できない人だという感覚になる。一方で、その本人からすれば、秘密でない話を一緒に仕事をしている人に話して何が悪いのか、そんなことを問題視する人は閉鎖的すぎるといった感覚を持つかもしれません。いずれも間違ってはいないのですが、それぞれの考え方の背景説明が必要です。そしてそこから共通的にやっていく。出向して他組織

の文化に触れると、割とみんな変わります。ですからそこは十分克服ができると思っています。結局、基本的な知識とやる気、そして振る舞い方についての相互理解。この 3 つが揃えば一緒にやっていける。当時の NISC でもそうだったと思います。

三角　そういう考え方をみなさんが持てるかがポイントですね。

髙見澤　お互いわかったつもりでいても、実はわかっていなかったり、全然わかっていないと思っていたけれど、実はお互い近いところで違う言い方していただけだったり、ということはよくあります。

ますます広がる安全保障領域とサイバーセキュリティ

三角　おっしゃるとおりで、同じようなことを違う言葉で言っていることが結構あります。例えば、「安全保障」という単語一つとっても範囲が広く、人によって概念が違います。どこまで安全保障の問題として捉えているのかを確認しないと、会話が成立しないことがあります。

髙見澤　それはよくあることですが、近年、経済と安保が融合化して一体となっているといわれます。さらに現在では、安全保障の経済化、すなわち経済がしっかりしないと安全保障が成り立たないというように、経済力が国力ないし安全保障力の主要な構成要素と認識されています。現行の国家安全保障戦略（2022 年 12 月 16 日閣議決定）はそのような考え方が大きな特徴です。

そのようなマインドに立てば、省庁間でより協力していかなければならないという認識になると思います。実際、経済産業省が主催する経済安全保障の会議に各省庁が出席し、有識者の前で経済産業省に対する意見を積極的に発言している様子から、これまでとはかなり変わってきていると痛感します。戦略ではサイバー安全保障という言葉がよく出てきますが、サイバーセキュリティもより統合的な方向に向かうべきでしょう。

サイバー対処能力強化法が画期的だと思うのは、国家を背景とする「高度に組織的かつ計画的な」サイバー攻撃に対しては、警察庁と防衛省・自衛隊が最初から省庁の枠を超えて連携して対処することが明記されていることです。これまでは、法執行機関として警察や海上保安庁がまず前面に出て、有事のときだけ自衛隊が出ていくというフェーズを分けた形での対応でした。もちろん有事以前でも自衛隊が出ていくことはありますが、基本的には法執行機関の力の及ばない段階になるまでは自衛隊はお呼びではないということでした。しかし今回この点が変わりました。

新しい法律についてはそれでも批判があります。権限をもっと広げるべきだとか、警察官職務執行法（警職法）の準用で十分なのか、最初から包括的な法制度の下で関係組織を一本化して対処すべきではないかといったものです。いずれももっともな部分もありますが、なかなかそう単純には行きません。警職法等の準用については、自衛隊・警察・海上保安庁の協力の深まり、運用実績の積み重ねが進んでいることを活用すべきです。今回の法律では、平素から関係機関が「一緒にやる」ことを想定し、物理的にも近いところで活動するわけですから、互いに協力しなければならないし、文化や情報の共有も進むでしょう。それが広がっていく形になればいいと思います。

一朝一夕にはできないでしょうが、内閣サイバー官が国家安全保障局の次長を兼ね、国家サイバー統括室が発足し、セキュリティ・クリアランスの制度が施行された新しい環境ができたわけです。サイバーに関する諸施策が政府横断的で官民連携が強化された一体のものとして運用でき

るように、さまざまな努力を積み重ね、サイバーコミュニティの形成につながっていくことを期待したいと思います。

主権に関わる部分をどう担保するか

三角　同感です。そのためにはどのようなアプローチが必要でしょうか。

高見澤　そこで重要なのが、瞬時に情報を共有できるシステム、すなわちリアルタイムで情報が更新され、すぐに参照できるようなシステムの構築です。サイバー対処能力強化法においては、サイバー攻撃の情報について国内はもとより諸外国やマイクロソフトなど外部組織からの協力を得る際、いかに情報をリアルタイムで共有するかが課題となります。それが「政府クラウド」上のシステムなのかどうかはわかりませんが、これからのサイバー安全保障においては、先ほどのマインドセットの問題や人的交流、情報保全のルール化、データのガバナンスなどに取り組む必要に迫られます。そして、それを実際に運用するためのネットワークを誰がどのように構築するのか。そこでは外国ファクターをどこまで排除するのか、主権に関わる部分をどう担保するのかという非常に重い問題もあります。

昨今「日米共同防衛における指揮・統制関係のあり方」が重要なテーマになっています。例えば、反撃能力を導入した場合の核抑止との関連、あるいはウクライナ危機のような緊張が高まったときの日米協議の進め方などです。これまでの日米協議は、非核三原則ではないですが、「枠組みはつくるけれども、事前協議ではノーとは言わない」と認識されてきました。「建前はよいが実質はゼロ」というのは言いすぎですが、日本はこうするから、ここは受け入れないけど、その他の点については米国にはこうしてくれ、日本も協力するというような形にできないかという気がします。できないことはできないので、建前は格好悪くとも実質を確保するという形を追求するようになってきているという印象を受けます。

これはサイバー領域でも課題になるかもしれません。サイバーは「スピード」「スケール」「インパクトの大きさ」が特徴で、GAFAM（グーグル、アップル、フェースブック、アマゾン、マイクロソフト）のような巨大 IT 企業や、その他民間の活動がサイバーセキュリティに大きな影響を与えています。サイバー関連のサプライチェーンや AI 開発において、日本は現状、米欧に大きく依存していると聞きます。この外部へのアウトソースが続く限り、「国内に基盤を置く」と言いつつも、実際には自律的なサイバーセキュリティの構築は困難です。


三角氏

サイバー対処能力強化法は、サイバーセキュリティにおけるわが国の課題の全体像を把握する「富士山の高さ」を知る一歩となります。エベレスト（最終的な理想形）には到達しないかもしれませんが、まずは何ができていないのかを明確にし、試行錯誤しながら取り組んでいくことが求められていると思います。

三角　同法が施行されると、いかにオペレーションするかに当面の間、意識、労力が注力されてしまうと考えられますが、今おっし

やった部分まで取り組む余力を持てるでしょうか。

髙見澤　「富士山の高さ」の現状把握は、オペレーションそのものの中から生まれます。

三角　おっしゃるとおりですが、例えば、先ほどの米国 IT 企業のクラウドと国産クラウドの置換について、国産クラウドの必要性は認識されても、米国の巨大企業との資本力、経験、力量の格差や、政策で主導しようとしても民間であるため収益を上げ続けねばならないという事実――こうした問題をどう解きほぐすかまで考える必要があります。そこまで頭が回らないのではないかと思うのです。

ただ、今お聞きしたサイバーの問題は、昔からそうですが、大部分を民間のインフラベースでつくっているので、民間の資本力と意識に大きく依存しています。経済原理で判断されてしまうため、今お聞きした話は世の中に認識されないままでいるのだと思います。その中で、政策的にどう進めるかを考えようとすると、しばしば立ち往生しがちです。

サイバー対処能力強化法の施行にあたっても、そのバックボーンとなる技術、ネットワーク、産業などを含めて全体をどうするのかというところまで戦略的に頭を働かそうとすると、相当、大変な取り組みになると思います。

髙見澤　そうですね。大変だからこそ国を挙げてやらなければなりません。

福島第一原子力発電所事故の廃炉作業の際にも感じたのですが、問題が生じると、普段関心の薄かった人も含めてみんなが「大変だ」と言って急速に情報共有が進み、協力体制が築かれる。しかし、新制度ができ、別の新たな案件が発生するとそちらに関心が移り、残された人々が「やっと静かになった」と言って黙々と取り組みを進めるのだけど、その取り組みは昔のようなセクター別の対応に回帰しがちで、総合的ではなくて、個々のセグメント対応になっていたりする傾向があるように思います。サイバーの領域でも、そういうことが起きているのではないでしょうか。

三角　同感です。AI やクラウドといった分野でも同様の懸念があります。これらの分野で奮闘している専門家は多くなく、さらに日本の優秀な人材が外資系企業に流出しがちである現状があります。彼らは外資系企業の文化の中で物事を考えるため、日本の「なかなかできない問題」の本質を理解できずに分断が発生しかねません。

髙見澤　国内に基盤を築くということは、外国企業や外国人に頼らないということでもないような気がするので、呼び寄せてやらないと最先端分野の競争にならないのではないかと思います。

三角　そこは悩ましいところです。すでに生じている技術力、資金力、資本力の圧倒的な差を考慮すると、きわめて大きな課題に思います。

髙見澤　そうですね。しかし、できるか、できないかではなく、やれる方法を考え抜いて、問題が生じるのであれば、それを解消していく施策を追求していくしかありません。国全体として危機感を持ち、みんなが競争的かつ野心的な目標に向かって学習できるような環境の整備、潤沢な研究資金の確保、国家による AI も活用したデータベースの構築と適切な利用体制の整備などを進めていくことが重要です。「諦めの高い壁」を破っていかなければなりません。

「何を成し遂げたいのか」を明確化して政策課題を設定する

三角　総合的な政策を出せるかが鍵ですね。サイバーだけでなく、安全保障に関しても、政策担当者みんなが共通の認識を持っているとはいえないでしょうし、必要なトレーニングを受けた人たちも十分ではないと思います。

髙見澤　今、日本の高校の教科書は変わってきています。社会科は「歴史総合」「地理総合」「公共」が必修で、「総合的な学習（探究）の時間」もあります。私は 2 年ほど前にこれらすべての教科書に目を通してみました。安全保障貿易管理やサイバーの記述はあまりありません。一方、核抑止、ウクライナ侵攻、冷戦史などは充実してきています。こういう状況があるのなら、高校生のうちから、安全保障やサイバー、インテリジェンスの知識を「当然知っているべきコモンナレッジ」として根付かせる必要性があると思います。「関ヶ原の戦いが何年に起きたかを知らないと日本人らしくない」と感じるのと同じような意識を醸成すべきだと思うのです。

三角　今いる政策担当者や政府、企業・組織から集まっている人たちについても、安全保障やサイバーに関する共通の概念や会話の基盤を持っていない人が多いのではないかと思います。

髙見澤　そう思います。サイバーは良い手段です。どこにでも関係しています。あらゆるところに広がっていて、横をつなぐ力を持っています。そして政策、技術、文化、人材などあらゆる課題が凝縮されています。

三角　サイバーはどこにでも関係しているのですが、逆に、どこでも使われているツール、サービスにすぎません。サイバー安全保障といわれて初めて利用者視点が入ってくると考えます。サイバーセキュリティ技術などを、ツール、サービスの消費者という視点から、安全保障政策を推進する立場として、どう考えるかが重要だと思います。そのような考え方をしっかり広めていかないと、サイバーと安全保障の課題について、理解は進まない気がします。

髙見澤　そうですね。日本としてこういうことをしたい、こういう国になるという国家像があって、安全保障のあり方やサイバー対策の具体的な位置づけが見えてくると感じます。

これまで日本では、「もの」を「つくる」ということに力を注いできましたが、これからは「こと」を「なす」ための方策をより総合的に追求していかなければなりません。国をより安全、強靭にし、国際的なネットワークを活性化するといった、より大きな目的を設定することです。このような「こと」を「なす」という視点に立つと、組織内でも、同業種でも、異業種でも、「もの」に焦点を絞りすぎるのではなく、「なすべきこと」を達成するために何が必要かといったより広範な問いを立てることが求められます。そのためには、サイバーセキュリティの関連でいえば、認知戦や情報戦、戦略的対話や人的交流といった多角的な要素を含めて検討する必要が出てきます。直接的・限定的な特定の答えを求めるだけでなく、「何を成し遂げたいのか」を明確にした政策課題の設定の仕方こそが求められると思います。

三角　国家の中枢においては、おっしゃったような広範な視点から全体戦略を統合していくことが重要です。一方、個別の政策や取り組みとなると、あまり幅広くては収束しないですし、認知戦、サイバーセキュリティそれぞれ別の取り組みとなるのではないかと思います。

髙見澤　大事な指摘です。それぞれについてメリハリをつけることは重要ですね。

三角　全体戦略目標を考えて、個別の専門分野においてはプロフェッショナルが力を強化してしっかりと取り組むことが不可欠だということですね。

本日は非常に興味深いお話を聞かせていただきました。どうもありがとうございました。

(2025 年 5 月 26 日収録。取材・構成：一般社団法人日本サイバーセキュリティ・イノベーション委員会[JCIC])

【出席者略歴】

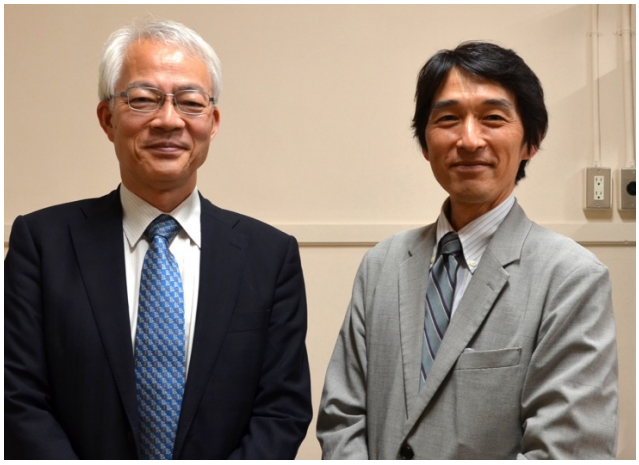
髙見澤 將林（たかみざわ のぶしげ）氏

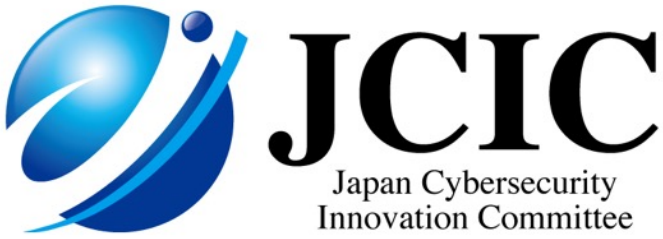
1978 年東京大学法学部卒業、防衛庁（現・防衛省）入庁。運用企画局長、防衛政策局長、防衛研究所長などを歴任。2013 年内閣官房副長官補。2014 年から新設の国家安全保障局次長、2015 年から内閣サイバーセキュリティセンター長を兼務。2016 年に退官後、2020 年 1 月までジュネーブ軍縮会議日本政府代表部大使を務める。2020 年 4 月より東京大学公共政策大学院客員教授。2024 年 4 月より公益財団法人笹川平和財団上席フェロー。

三角 育生（みすみ いくお）氏

東海大学情報通信学部長・教授

1987 年通商産業省(現経済産業省)入省。内閣サイバーセキュリティセンター(副センター長等)や経済産業省(サイバーセキュリティ・情報化審議官等)等において、サイバーセキュリティ、安全保障貿易管理といった行政に長く携わり、サイバーセキュリティ戦略の策定、サイバーセキュリティ基本法制定・改正、日本年金機構のインシデント対応等に従事。2020 年 7 月退官。2022 年 4 月より現職。博士(工学)、MA in Management。





[本調査に関する照会先]

JCIC 事務局　info@j-cic.com