2023 年 5 月

シリーズ 「日本のサイバーセキュリティ政策史」第 4 回

情報セキュリティ政策の礎を固める
～無謬主義を乗り越えて～

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シリーズ。第 4 回は、内閣官房情報セキュリティセンター（NISC）総括担当内閣参事官などを歴任した関啓一郎氏をお迎えし、話をうかがいます。「リスク前提社会」やセキュリティ・バイ・デザインのコンセプト、サプライチェーンのリスク対応、政府全体のセキュリティ防御を図る GSOC、日・ASEAN 協力など、いまでは社会に定着した概念や取り組みが初めて政策メニューに上げられた時代。根底でどのような考えや議論があり、何を乗り越えたのか──。

【出席者】

関 啓一郎 氏
元内閣官房内閣参事官（内閣官房副長官補付）／内閣官房情報セキュリティセンター（NISC）内閣参事官（総括担当）、株式会社 NTT ファシリティーズ監査役

聞き手：
三角 育生 氏
東海大学情報通信学部長・教授

セキュリティ意識を醸成するところから

三角 最初に、関さんの NISC 在任中にとりまとめられた「第 2 次情報セキュリティ基本計画」（2009 年 2 月 3 日政策会議決定。以下、「第 2 次基本計画」という）についてうかがいます。

「第 1 次情報セキュリティ基本計画──『セキュア・ジャパン』の実現に向けて」（2006 年 2 月 2 日政策会議決定。以下、「第 1 次基本計画」という）では「限りなくリスクゼロを目指す」という表現が複数登場します。第 1 次基本計画を担当された内閣参事官によると、リスクがゼロにならないのは

わかっているけれど、目標を高く設定したということでした（本シリーズ第 3 回「日本の情報セキュリティ対策黎明期の政策立案～NISC 立ち上げに参画して～」）。第 2 次基本計画では「リスク前提」であるとはっきり書いています。これについて何か議論があったのでしょうか。

関 まず第 1 次基本計画策定時の考え方を振り返る必要があります。当時の日本社会においてはセキュリティ意識を醸成することが重要課題でした。サイバーセキュリティ対策の重要性が社会的に浸透していなかったのです。そこで、同計画では、セキュリティ意識の醸成と官民連携体制を強調したわけです。

サイバー攻撃にあった企業（組織）は被害者ではあるものの、セキュリティ体制が批判され企業イメージを損なうことがあります。そのため、被害企業には被害をなるべく公表したくないと考える傾向がありました。第 1 次基本計画は、官民が連携して互いに情報を出し合うことで、より「IT を安心して利用可能な環境」を構築することを強調したと考えています。また、IT の利活用ばかりを考えがちな傾向を改め、利活用とセキュリティを車の両輪で進めることに主眼が置かれました。

第 2 次基本計画の検討を重ねていた当時の状況として、愉快犯的なものが多かったサイバー攻撃が、徐々に経済的・計画的な攻撃に変わり、まだランサムウェアはありませんでしたが標的型攻撃も出てきた頃で、攻撃側の犯罪ビジネス化に対応する必要から、セキュリティ意識は高まりつつありました。

無謬主義が思考停止を招く──「事故前提社会」の発想を

三角 ちょうどその頃「Winny（ウィニー）」による情報漏えい事件が多発しました。

関 そうですね。企業や官公庁などで職員が自宅で作業するためにパソコンを持ち帰った際に情報が漏洩するなどの事件が相次ぎました。こうしたこともあってセキュリティへの意識が高まり、例えば官公庁をはじめさまざまな組織で情報を機密性の高いものとそうでもないものとに厳密に区分して、適切に取り扱えるようするなどの取り組みがなされるようになりました。ただ、事前対策としてセキュリティ部門あるいは総務部門を中心に厳しいルールを作るようになった結果、それが厳しすぎるがゆえに守れない事態が露呈しました。ユーザーの利便性を考慮しないセキュリティ重視の厳しいルールは形骸化します。担当部門はルールを作ったから守らない方が悪いと責任転嫁し、利用部門は ICT の利便性を過度に減殺するルールは守らないという結果となります。


関氏

加えて、日本社会にありがちな「無謬主義」も改めなければならないと考えました。絶対に間違いはないという前提で対策を進める。そうすると、いざセキュリティ事故が発生したときに思考停止に陥ってしまう可能性があります。東京電力福島第 1 原発事故のときに「想定外」という言葉が使われましたが、事前対策にこだわると事故想定が甘くなるため、インシデント対応がおろそかになる恐れがあります。そこで、第 2 次基本計画では、事前の対策を進めつつ、いざというときには、慌てることなく合理的な対策をとることができる考え方に見直しました。このことについて、

第2次基本計画の本文では以下のように記述しています。

「第一次基本計画の下で追求された水準は、時として絶対的な無謬性の追求といっても過言ではない水準であった。情報セキュリティに係るリスクの状況にかんがみると、このような水準の事前対策を実現することは、現実には容易でない。実現可能性や、結果を追求するためのコストとのバランス、情報セキュリティの確保と引換え（トレードオフ）になり得る利便性とのバランスの観点を考慮する必要があるからである」。

利便性とのバランスについては理解されたのですが、実はこの文言に対して、策定前の検討段階で有識者の方々から「十分に対策をしない」といっているように読み取れる、という指摘を多々受けました。そこで、誤解を招かぬよう脚注で以下のように補足しました。

「『情報セキュリティ上の問題が生じない水準の事前対策』の実現が、『現実には容易ではない』としている趣旨は、『どれほど対策を実施したとしても、失敗や問題が生じることはあり得る（完璧であるという結果の実現は難しい）ということを認める、すなわち容認せざるを得ないリスクは存在し、これを acceptable risk として捉える』という意味であり、『必要な対策を行う体制や対策の内容などの改善を含め、対策を徹底的に行うことは容易ではない（ゆえに、適切な水準の対策であっても対策の徹底を行わなくても良い。）』という意味ではない。『適切な水準の対策については徹底するべき』ということについては、ここに改めて強調する」。すなわち、事前対策には一所懸命取り組みましょう。あわせて、問題が起きたときの対応についても思考停止をしないであらかじめ考えておきましょう、個々人も社会全体としても問題が起きたときこそ、きちんと対応できる体制を築きましょう、というメッセージです。

三角　いまでこそ、何かあったときにインシデントレスポンス（事故対応）が重要だと強調されるようになりましたが、当時はそういう状況ではなかったということなのですね。

守りのセキュリティから攻めのセキュリティへ

関　はい。それについては、第 2 次基本計画で以下のように記述しています。「『事故前提社会』では、脅威によってリスクが現実のものとなり得る事態を想定し、リスクを予見・予防するとともに、生じる損害や障害を極力小さくするべく、対処の手立てなどを検討するというリスク・マネジメント手法が重要となる」。つまり、守りのセキュリティから攻めのセキュリティへと転換しましょうということです。

三角　経済産業省が、情報セキュリティ対策に取り組む姿勢の情報を積極的に開示することで、ステークホルダーの信頼を得るようにしようと提案したのもその頃です。

関　そうですね。「なお、ここで『事故前提社会』とは、事故が有り得るから諦めて予防のための対策を行なわないということや、被害に遭うのは仕方がないことであると諦めるということを意味するものでは決してない」など、いまとなっては当たり前のことが記述されています。

三角　リスク前提のアプローチをとることについて、懸念を示す意見があったということですね。

関　はい。「手を抜く」と誤解されないようにと、むしろ心配してくださるがゆえの指摘と受け止めています。それだけ日本は、政府も民間も間違ってはいけない、という風潮があったといえるかもし

れません。日本がITで出遅れた原因の一つは、韓国のようにどんどん前に進めて、多少問題があってもあとで直せばいい、という社会文化とは異なり、日本は慎重で、想定される問題を1つずつ潰していって、潰し終わって進めようという社会文化、しかしその潰し終わった段階では、世の中はもう次の技術に移っていたというようなところがあります。当時、それも反省としてありました。

第2次基本計画の主眼は、がんばっても事故は起こりうる、がんばりすぎるとかえって守られなくなる、の2点です。そこは第1次基本計画から発想転換しました。

三角　仕事熱心な人ほど合理性に欠く窮屈なルールを守れなくなるというのは聞きます。もともとITを使って仕事を高度化、効率化しようとしているわけですから、情報セキュリティのみを考えた合理性に欠く厳しいルールを課してITを使いにくいものにしてしまっては、本末転倒、仕事をするなというのと等しいことになりかねないですね。

関　おっしゃるとおりです。情報セキュリティそれ自体を目的化してはいけないということです。

政府全体にセキュリティの傘をかける──GSOCの立ち上げ

三角　ほかに第2次基本計画を作るときにご苦労されたこと、特に注力されたことなどはありますか。

関　国、情報インフラ、企業、個人の4分野に分けることや、官民連携など大きな枠組みはほとんど変わっていません。具体的な対策についても、これはどちらかという各省の予算になるので、GSOC（Government Security Operation Coordination team)などNISCが直轄でやっていた部分を除けば、大きな変更はありません。

GSOCについては、2006年度に初期検討の予算が確保されていました。私は、2007年度に着任し、運用を開始するためにセンサーを構築して、それを各省に入れてもらうところを担当しました。

GSOCの名前はまだ登場していませんが、その設立の意図は「セキュア・ジャパン2006」（2006年6月15日情報セキュリティ政策会議決定）に記されています。「政府関係機関に対するサイバー攻撃等に関する横断的な問題解決機能の強化」、「情報収集、分析・解析機能の強化（内閣官房）」の項目で、「情報漏洩や情報システムの障害等の発生を防止し、発生した場合には迅速かつ的確に対応するための横断的な情報収集機能及び攻撃等の分析・解析機能を強化すべく、2006年度において、各政府機関のWebサーバ等の監視を試行的に開始するとともに、国内外の関係機関と連携した攻撃等の横断的分析・解析機能を構築する」。

概算要求基準の下では、新設のNISCにおいて大きな予算の確保は困難でしたが、2007年度にはGSOC構築予算を確保できました。「セキュア・ジャパン2007」（2007年6月14日情報セキュリティ政策会議決定）では、次のように具体的にGSOCの名称が登場しています。「政府横断的な対応体制の構築（GSOCの整備）（内閣官房及び全府省庁）」の項目で、「政府機関に対するサ

イバー攻撃、政府機関における情報漏洩や情報システムの障害等の発生をより確実に防止し、発生した場合にはより迅速かつ的確に対応するため、2008 年度における本格運用に向け、政府横断的な情報収集、攻撃等の分析・解析、各政府機関への助言、各政府機関の相互連携促進及び情報共有を行うための体制（Government Security Operation Coordination team ）（略称；GSOC）を整備する。

2007 年度においては、一部府省庁の情報システムに係るリアルタイム監視機能並びに内閣官房情報セキュリティセンターにおける横断的な監視情報の収集機能、攻撃等の分析・解析機能を整備するとともに、当該分析・解析の結果に基づく各政府機関への助言、各政府機関の相互連係促進及び情報共有を行うための体制を強化する。その際、様々な機関で研究が進められた最新技術の有効活用を図る」。

三角氏

要するに、GSOC センサーを手段として政府横断的に情報収集・監視をし、サイバー攻撃やその準備動作等の脅威を検知したり、情報を分析・解析して対策を考えたりして、各省庁にそれを提供するということです。有名な例として三角さんが担当されましたが、2015 年5月の不正アクセスによる日本年金機構からの情報流出事案の際には原因究明調査を行い、詳細な報告書を公表しています。

三角 内閣官房である NISC の役割は本来、各府省にまたがる施策の企画立案および総合調整を行うことです。当時、そういった実務を開始できたのは珍しいですね。

関 この時点はまだ理念的な段階でした。当初 NISC で予算をとるのは難しいのではないかと考えられていました。その中で GSOC が必要だと考える様々な方が動いて、内閣全体の中で 10 億円の予算が取れたのです。これをきっかけに、NISC が GSOC システムを構築し始めました。おそらく、企画立案・調整にあてはまらないということについては、どこの省庁もやっていないから、内閣官房が試行的にやって、本格化したら所掌を考えましょうという発想だったのではないかと思います。

財務省への説明では、GSOC を実現すれば、情報が集約されるため、情報セキュリティ対策の費用対効果が高まる、経費を節減できるということだったと思います。次の段階では各省のサーバ〓を集約することについても考えていました。守るべきところを少なくすることで、さらに経費を節減できるということです。サイバーセキュリティに関しては効率的な各省の予算編成ができる、と説明して理解を得ました。

国際情勢を見ると、2007 年 4 月にエストニア政府が首都にある第 2 次世界大戦のソ連軍勝利を記念した銅像の移設を決定したところ、それに対するロシア系住民の反発を契機に、エストニアに対する大規模なサイバー攻撃（DDoS 攻撃）が発生しました。政府機関、銀行、ISP 等に対する攻撃が3週間続き、オンライン銀行や政府ポータルサイトが利用不能になりました。また、当時、アノニマスのような集団などが攻撃をしかけてくることもありました。これらの事件をきっかけに、わが国において、大規模なサイバー攻撃について、強く認識されるようになりました。こうした情勢の中で GSOC システムが構築されたわけです。

GSOC システムの構築に際しては、（私の着任前ですが）シンガポールの同様の機関を現地視

察しました。先方では、政治家を含む影響力を持つ人たちの理解を得られやすいように大きなモニターを含む見学用施設を設けたとのことでした。サイバー攻撃については、攻撃する側は発見されにくいように仕掛けてくるので、本来、見えにくいものです。それを可視化してわかりやすくするのも啓発の一環として必要であろうと理解しました。GSOC においても、NICTER（Network Incident analysis Center for Tactical Emergency Response：サイバー攻撃の大局的な動向を把握することを目的としたサイバー攻撃観測・分析システム）などを導入して、サイバー攻撃の現状を見にこられた方々にわかりやすく示せるよう工夫しました。

日・ASEAN 協力──セキュリティ水準の底上げを図る

三角　関さんの時代に開始されたものとして、東南アジア諸国連合（ASEAN）への取り組み、すなわちシニアレベルの政策対話がありますね。2009 年 2 月に第 1 回日・ASEAN 情報セキュリティ政策会議が開かれました。

関　林良造先生（当時、東京大学公共政策大学院教授。現、武蔵野大学国際総合研究所フェロー）に議長をしていただいて、特に山口英先生（初代情報セキュリティ補佐官、奈良先端科学技術大学院大学教授［故人］）が熱心に進めてくださいました。山口先生はすでに JPCERT/CC で各国と民間の連携を構築していたので、政府間連携も進めるべきだというお考えでした。日・ASEAN 情報セキュリティ政策会議には2つの発想がありました。一つはサプライチェーンリスクです。これは当時から意識されていました。

三角　リアルワールドのサプライチェーンですね。

関　そうです。日本の産業の主な供給地域は ASEAN でした。そこで情報セキュリティが脅かされれば日本にも影響します。そこでまずは ASEAN の情報セキュリティの水準を底上げしましょう、という発想がありました。もう一つは、日本流のルール作り等のメソドロジーを ASEAN に広めたいということ。そうすることで、現地の日本企業も活動しやすくなります。いずれも政府間の連携を強めることで実現させようということで始めました。

後に、2009 年頃から日本が ASEAN と政策対話を始めたことについて、アメリカの関係者などからも先見の明があると評価されました。

三角　当時、山口先生がおっしゃっていたのは、わが国の企業・産業のサプライチェーンの確保という目標があるため、情報通信系の政府機関だけではなくて、現地の産業を所管する政府機関からも参加してもらえ、ということです。

関　そうです。当時、IoT という言葉はまだなかったけれど、それに近いことをおしゃっていました。

三角　「ハードウエアセキュリティ」という言い方をされていましたね。

関　製造装置などに組み込む半導体やソフトウェアの情報セキュリティに気を付けなければいけないと話されていました。2008 年、中国製と見られるシスコ製品の偽物がアメリカの空軍、海兵隊、連邦航空局（FAA）、連邦捜査局（FBI）などの連邦政府機関向けに販売されて、ネットワーク障害などの事故が多数起こる事件もありました。山口先生はさらに、製造プラントの制御システムなども念頭に置かれていました。

三角　いわゆるセキュリティに係るサプライチェーンの問題や、組み込み系や制御系のシステムの情報セキュリティ確保が課題になりはじめた頃ですね。

関　こうしたことから、日・ASEAN については底上げということを特に意識しました。

三角　当時、私も NISC の職員とともに ASEAN 諸国に、政策会議を開始したいということについて説明するべく出張しました。ただし、現地の日本企業の方から、従業員が転職する際に紙の図面を持ち出す者がいて、そうした図面の管理も含めて大変だという声を聞きました。すなわち、IT セキュリティ以前の問題もあると痛感しました。

関　当時そうした背景はありましたね。

セキュリティ・バイ・デザインのコンセプト

三角　NISC がセキュリティ・バイ・デザインのコンセプトを打ち出したのも、関さんの時代ですね。2007 年頃から NISC で提唱し始めたように思います。

関　セキュリティ・バイ・デザインの思想の基本は、後からセキュリティを付け加えるのは高コストになるから、情報セキュリティを前提に企画・設計をすべきとの考え方です。同時に、サプライチェーン全体がセキュアであることを確保しましょうということも含まれています。当時、世界的にもそういう考え方があって、わが国でもそれを踏まえて NISC が提唱しました。

三角　しかしその後、NISC が、セキュリティ・バイ・デザインについての手順をまとめた文書は、統一基準の規定内容を仕様書に落とし込むための仕様書作成マニュアルのようになってしまいました。本来は、全体を考えようというコンセプトの話ですね。

関　おっしゃるように、コンセプトあるいは哲学です。情報セキュリティを後付けするのではなくて、IT の企画・設計段階から組み込んでおく発想に切り替えろというムーブメントだと私は理解しています。当時、サプライチェーンリスクの議論の萌芽でもあるし、情報セキュリティを前提に設計するという意識があまりなかったため、声高に言って、意識改革、啓発をしたということです。

NISC が取りまとめたセキュリティ・バイ・デザインの文書は政府のシステム向けに作られたものなので、マニュアルみたいになっています。ただ、コンセプトとしては民間も含めて広まったと思います。

課題は言い続けること

三角　そうですね。本日お話をうかがってきた「リスク前提社会」や GSOC によるモニタリング、ASEAN などとの国際連携、サプライチェーンへの対応、セキュリティ・バイ・デザインなどはいまや当然のことになっています。こうしたメニューは関さんの在任中に出揃ったということですね。課題は、その後も繰り返しこれらの事項を言い続けなければならないことです。

関　別の要素から強く意識されるようになった今日、ということなのでしょうね。

三角　サイバーセキュリティの施策等への参入者が増えたということもあります。当時は、わが国の安全保障に関連してサイバーセキュリティを意識されていた方々の範囲が、今に比べて限られていたかと思います。異動による代替わりもありますし、新たな参入者があるたびに同じ考え方を

伝え続けねばならないということですね。

関　そうですね。今また変革の時代を迎えています。一段階フェーズが変わりました。ロシアによる選挙干渉に加えて、本格的な他国への攻撃が、前述したエストニアの例のみならず、ウクライナに対しても見られました。わが国も警戒が必要です。SF の世界の話ではなくて、現実に起こるという認識が高まりました。北朝鮮のサイバー部隊は強力だという分析もあると承知しています。核やミサイルのみではなく、総合的に警戒する必要があるということを一般の人でも意識せざるをえない状況です。

三角　本日お話をうかがってきた関さんの NISC 在任当時からだいぶ時代は変わりました。その中で、話題に上がったさまざまなコンセプトについて、繰り返し訴えていく必要があったということですね。本日はどうもありがとうございました。

（2023 年 2 月 27 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]））

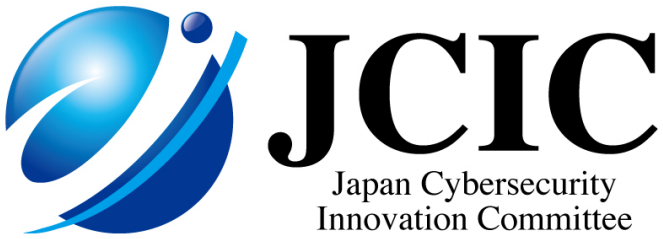
【出席者略歴】

関　啓一郎（せき　けいいちろう）氏

1983 年東京大学法学部卒業、郵政省（当時）入省。国際経済研究所ワシントン事務所長、マルチメディア振興室長、内閣官房内閣参事官（IT 戦略本部担当）などを経て、2007 年 7 月～2010 年 1 月内閣官房情報セキュリティセンター総括担当・内閣参事官（官房副長官補付）。その後、東京大学公共政策大学院教授、野村総合研究所主席研究員、総務省関東総合通信局長等を歴任。2021 年より現職。この間、愛媛大学客員教授、慶應大学非常勤講師を務める。主な著作に、「『インダストリー4.0』と『IoT』を理解するための基礎」、「ポイント解説平成 27 年改正個人情報保護法」、「サイバーセキュリティ基本法の成立とその影響」、「インターネットの法律問題」（共著）、「地上テレビ放送とビジネスモデルの将来」、「英国電気通信庁（OFTEL）の競争政策」など。

三角　育生（みすみ　いくお）氏

1987 年通商産業省入省。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～東海大学情報通信学部長・教授。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