2023 年 3 月

シリーズ 「日本のサイバーセキュリティ政策史」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～

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 3 回は、内閣官房情報セキュリティセンター（NISC）発足時に基本戦略等の参事官を歴任した小林正彦氏をお迎えし、話をうかがいます。2005 年、情報セキュリティへの理解が各国で高まる一方、日本では包括的な情報セキュリティ政策推進体制の整備が十分ではなかった時代に設立された NISC。情報セキュリティ確保を目指す新たな組織はどのように誕生し、どのような理念で戦略やルールを策定したのか――。

【出席者】

小林　正彦氏
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）客員上席研究員、元内閣官房情報セキュリティセンター(NISC)　内閣参事官

聞き手:
三角　育生氏
東海大学情報通信学部長・教授

NISC 設立への助走

三角　小林さんは内閣官房情報セキュリティセンター(NISC)の基本戦略等の内閣参事官を歴任され、ゼロからの組織の実務を切り盛りし、「政府機関の情報セキュリティのための統一基準」（政府統一基準）作りなどに奔走されました。政府統一基準等は NISC が立ち上がって間もない半年前後のタイミングで情報セキュリティ政策会議（議長：内閣官房長官。以下、「政策会議」という）決定となるなどしていますが、具体的に何に取り組み、何に苦心されたのか、当時の現場の状況をうかがいます。まず、NISC が設立された経緯を教えてください。

小林　実は、NISC 設立の前から助走は始まっていて、2003 年 7 月に策定された「e-Japan 戦略 II」（2003 年 7 月 IT 戦略本部決定）で、2005 年までに DoS 攻撃、コンピュータウイルス、不正アクセス等による被害を最小限にするための体制を確立することとなっていました。そして、「e-Japan 戦略 II 加速化パッケージ」（2004 年 2 月策定。以下、「加速化パッケージ」という）で、NISC を設立すること、および情報セキュリティ補佐官の設置、各府省庁の情報セキュリティ確保として各府省庁の情報セキュリティ対策の評価や情報システムとその運用に関する安全基準の策定等、地方公共団体の情報セキュリティの確保、重要インフラの情報セキュリティ確保、民間の情報セキュリティ強化、人材育成や普及啓発といった、設立された NISC が直ちに実施すべきメニューの項目立てが決まっていました。

三角　NISC 設立の前に、経済産業省の産業構造審議会（産構審）でも情報セキュリティ政策の推進について審議されていたのではないですか。

小林　産構審でも議論されていましたが、NISC の設立や情報セキュリティ補佐官の設置などをオーソライズしたのは e-Japan 戦略 II と加速化パッケージにおいてです。産構審は、それらに燃料補給をするような位置付けで動いていました。

三角　確かに加速化パッケージの 2 章で「セキュリティ（安全・安心）政策の強化」を掲げ、1 節で「2004 年までに内閣官房に情報セキュリティ対策についての助言・支援を行う情報セキュリティ補佐官（仮称）」を置くと書かれていますね。

小林　はい。補佐官に奈良先端技術大学院大学情報科学研究科教授の山口英（やまぐち すぐる）さんが着任されました。

三角　そして、同 2 節で「各府省庁の情報セキュリティ確保」が書かれています。当時、各府省庁のセキュリティ対策は足並みが揃っていなかったということでしょうか。

小林　政府機関に対するセキュリティ対策に関しては、2000 年 7 月に「情報セキュリティポリシーに関するガイドライン」（情報セキュリティ対策推進会議）が策定されていました。ただし、それはあくまでガイドラインに過ぎず、それに基づいて各府省庁が何を作るかについては、各府省庁の判断にゆだねられていました。それでは十分ではないということで、各府省庁、さらに地方公共団体、重要インフラ、民間のセキュリティ確保を図るうえでのメニューを加速化パッケージにおいて示したということです。

加速化パッケージがあったおかげで、NISC 設立後わずか 1 年で多くのメニューを一気に進めることができました。ただし、加速化パッケージでは、やるべき事項の項目がリストされてはいたものの、中身はほぼ白紙だったので、具体的な内容の作成にあたっては、集中的な作業が必要でした。急いで整備することについては、「日本の情報セキュリティ対策の遅れを取り戻すためにはブルドーザー的にドッグイヤーで進めるしかない」、という補佐官である山口さんの強い思いがありました。

三角　2005 年 6 月まで私は総合科学技術会議の事務局におりました。そこに山口さんがいらして、「情報セキュリティ対策に取り組む」と勢いよくお話しされていたのをよく記憶しています。


小林氏

小林　山口さんが情報セキュリティ補佐官として任命される前にはJPCERT/コーディネーションセンター（Japan Computer Emergency Response Team Coordination Center)の代表理事に就いていらっしゃいましたが、その時点から、日本の情報セキュリティ対策を推進するべく事実上の指揮を取りはじめていましたね。

彼は、WIDE プロジェクトのボードメンバーであり JPCERT/コーディネーションセンターを立ち上げた方で、また、情報セキュリティ研究の草分け的存在です。彼が NISC にいたことで、センター長以下、審議官、参事官、担当官、民間出向者など全員が水を得たように動いて、高いパフォーマンスを発揮することができました。NISC の歴史を語るうえで欠かせない存在です。

山口さんと初めてお会いしたのは、私が独立行政法人情報処理推進機構（IPA）のセキュリティセンター長をしていた 2000 年前後のことです。あるとき JPCERT/CC 初代代表理事であった山口さんが IPA に来られ、情報セキュリティに対する世間の認識もようやく高まってきたところ、JPCERT/CC と IPA が協力している姿を世の中に示すことが必要だ、と力説され、象徴的な共同事業としてセミナーを開催しようということになりました。当時、IPA と JPCERT/CC は、ともにセキュリティ関係団体として活動しながら、協力する機会がなく、もしかしたら仲が悪いのではないかと噂されることもあったのですが、そのような世間の見方を打ち破る行事になり、日経 BP 関係の記事（注）にもしてもらいました。

最初の仕事

三角　2005 年 4 月 25 日に NISC が発足したとき、最初に何がなされましたか。

小林　NISC に補佐官を正式に置くことです。加速化パッケージに「2004 年 4 月までに補佐官を置く」とあり、当初、NISC の前身組織にあたる内閣官房情報セキュリティ対策推進室（2000 年 2 月発足）にポストが作られました。2005 年 4 月 25 日に NISC が正式に発足すると同時に、山口さんは NISC の補佐官としての発令となりました。私たち NISC の参事官なども同日付で発令されています。


三角氏

三角　2005 年 5 月に政策会議が設置されました。7 月に開催された第 1 回政策会議で、中長期の基本戦略「第 1 次情報セキュリティ基本計画（仮称）」を策定することと「早期に着手すべき統一的・横断的課題」が決定されています。

小林　第 1 回政策会議で先述した NISC でやることのメニュー項目をオーソライズしてもらいました。そこからスタートしたわけですが、最初の仕事は、政府機関への DoS 攻撃などが増加していたことから喫緊の課題である政府統一基準の策定でした。9 月に開催予定の第2回政策会議までに政府統一基準案を作成するべきとなったのです。各

府省庁間での協議等も必要となるため、本来であれば相当な時間を要します。そこで、第 2 回政策会議までに、緊急性の高いものや当然行うべきものに焦点をあてた「項目限定版」を作ることにしました。

三角　各府省庁のセキュリティ確保が急務だったから、第一に手をつけたということですね。当時、私は IPA にいましたが、山口さんから NIST（米国国立標準技術研究所）が発行した SP 800-53（連邦政府情報システムに推奨されるセキュリティ管理策［当時］）の翻訳はあるのかなど、いろいろ求められました。

小林　政府統一基準を作るうえで、ISMS（情報セキュリティマネジメントシステム）と SP 800-53 の 2 つを主たるバックボーンとしました。対策内容は ISMS をベースとして、構成は SP 800-53 を参考にしながら検討していきました。ISMS は完成度の高い対策集を PDCA の枠組みで構成したもので、対策集としてもマネジメントの教科書としても大変参考になったのですが、残念ながら政府という要素を特別視していません。すべての組織に適用できるよう汎用的な構成になっているので、その構成では政府の基本対策の型枠としては使いにくいものでした。特に、まず組織のリスクアセスメントをして、各種の管理策の必要性を検討し、その採否の判断をして、もし採用しないと判断するなら理由をきちんと考える、という ISMS の基本的な枠組みは、情報セキュリティ対策の経験が不足している多くの府省庁には高すぎるハードルでした。一方、SP 800-53 は、もともと NIST が米国政府機関向けに策定したものです。しかも、先行する様々な情報源を使って作ったとされていて、その中でも ISMS は相当参考にしているという印象を受けました。政府向けと限定されているので、管理策ごとに当然行うべき基本的な対策内容と、その対策の補強のしかたをそれぞれ区別して書くなど、各政府機関が実施しやすそうな構成となっていました。ただ、2つの文書はあくまでも参考として用い、文章は全部書き下ろしました。

　当時の政府統一基準のもう一つの特徴は、義務ではなく推奨としての位置付けであったということです。

三角　2014 年にサイバーセキュリティ基本法が制定され、サイバーセキュリティ戦略本部が決定した基準に各府省庁が準拠しているかの評価（監査）をすることになったことから、実質的に義務的になりましたが、それ以前は義務にするのは難しかったのでしょうね。

小林　はい。当時の政府統一基準は、義務ではなく、あくまでもテンプレート、つまりそれを参考にしながら府省庁で適切に定めてください、という位置付けだったわけです。しかし、義務ではなくとも、限りなく義務に近いものにするため、例えば政府統一基準の運用枠組みを説明する「政府機関の情報セキュリティ対策における政府機関統一基準の策定と運用等に関する指針」（2005 年 9 月 15 日政策会議決定）において、政府統一基準を「各府省庁が最低限行うべき情報セキュリティ対策を定めた政府の統一的な基準」であると述べて、「行うべき」対策と位置付けるなど、いろいろな工夫を施しました。

　当時、政府統一基準を作ることに対して、各府省庁からの反応は大きなものでした。概算要求後に決定されることになったので、予算措置の裏付けのないものをどのように実施するのかが一つ

の論点でした。「NISC が先頭に立って情報セキュリティ対策予算を確保し、府省庁に分配することはできないのか」という意見もありました。そのような状況の中、NISC としては、「政府統一基準は、義務的なものではなく、一定の期間を要したとしても、政府統一基準の定める水準にまで達するようにするためのもの」、「政府の中で対策が十分でない部局があれば、そこが狙われて国全体に被害が広がるので政府機関全体のために協力してほしい」という論理で説得したわけです。

三角　各府省庁の情報セキュリティ対策予算を増やしていくための追い風効果も期待して、府省庁における対策について毎年度評価することとしたと聞いた記憶があります。2005 年頃、総合科学技術会議は、科学技術関係予算について概算要求前にヒアリングをして評価（SABC）を行っていました。重複排除・連携強化、重要な政策分野への重点化を徹底するため、積極的に実施すべきもの（「S」）から、大幅に見直してから実施すべきもの（「C」）まで、メリハリの効いた科学技術関係資源の配分を実現しようというものです。私はその資源配分を担当していましたが、NISC の担当者の方が総合科学技術会議での取組みを参考にしたいと話を聞いてきたのを覚えています。

小林　予算を増やすにはどうしたらよいか、メンバー全員で検討し、工夫しました。府省庁の対策を評価して、必要な水準に達していないことを示して、それを根拠に予算の概算要求をしてもらい、政府予算案を決めてもらいたいという思いがありました。想定された反応ではありましたが、評価をすることについて相当強い抵抗を示した部局もありました。そうした反応に対して粘り強く説明して施策を実施していったわけです。

政府統一基準案の作成にあたっては、民間から有能な専門家の方々に集まってもらいました。当時、NISC のオフィスは内閣府の敷地の中庭に建てられた冷房がほとんど効かないようなプレハブ庁舎にありましたが、９月までに案を作成するため、日中は背中にあたる直射日光に辟易しながら、みんな徹夜に近い状態で「熱い夏」を越したわけです。

国の総合対策という意気込みで

三角　「第 1 次情報セキュリティ基本計画」（2006 年２月２日政策会議決定。以下、「第 1 次基本計画」という）で重視した事項、あるいは目的は何でしょうか。「限りなくゼロを目指す」という表現が散見されます。リスクゼロに近いものを目指していたのか、あるいは別の趣旨だったのでしょうか。

小林　「限りなくゼロを目指す」という文言は、2 カ所に書いてあります。最初にいっておきたいのは、「ゼロ」を実現することは無理な話ということです。情報セキュリティの世界ではリスク源は次々に出現します。しかし、最初の基本計画では目標を高く示すべきで、「目指す方向」の究極の目標値としてはゼロ以外に言葉がありません。究極の目標値はゼロであるが、必ずリスクが残るから漸近線のような意味で、リスクが存在することを前提にして対策を考えていく必要があるということを表現するために「限りなくゼロを目指す」となりました。

三角　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）では「リスク前提社会」といっています。そこで、第 1 次基本計画では「限りなくゼロを目指す」といっていたことを、第 2 次基本計画では「リスク前提社会」、すなわちリスクと共存する方針

に換わったと読まれる可能性はありますね。第 1 次基本計画策定時には、ゼロを目指すことを掲げなければいけない、といったような議論があったのではないかと思ってしまいます。

小林　ありそうな誤解ですね。どこまでやってもリスクと共存せざるをえないことは、当時の関係者にとっても常識でしたから。

三角　2 つの基本計画を比較すると、新型コロナウイルスの例に近いのかなと思ってしまいました。新型コロナウイルス感染症が拡大しはじめた頃には「コロナを極力封じ込める」べく感染者の追跡を徹底していましたが、一定の対策が進むなどした今は、リスクを考えつつ経済活動と両立を考えるようになったのと、似ているのかなと。

ところで、第 1 次基本計画はすっきりしていて読みやすい文書です。施策の対象を政府、重要インフラにとどまらず民間まで含めているのは、e-Japan 戦略 II に民間が含まれていたからでしょうか。

小林　確かに e-Japan 戦略 II に書かれているから、ともいえますが、そもそも、わが国全体の総合的な対策をいかに進めるかという問題意識をもって基本計画を策定するわけですから、項目として民間に関するものを入れることは必然でした。ただ民間については何をどう書くかの苦労がありました。政府機関の総合対策は政府自らの課題ですし、重要インフラの大半は所管省庁があり業法によって一定の管理下にあるので、対策の推進についても書きやすいのですが、その他の一般的な民間企業等についての施策はどこまで書くのかという議論がありました。情報セキュリティの取組みを促すのにどのような手段があるのか、政策会議が発する戦略によって民間における取組みを実施してもらえるのかと。そんな葛藤はありましたが、結果として、問題意識はきちんと明示したうえで、手段としての施策は随時講じていこうということになりました。例えば、IPA が民間事業者に対する啓発をするなど、政府がとりうる手段で可能な限りの働きかけをしようということで、最後は NISC メンバーみんなで納得して民間に関する施策案を書きました。

三角　当時、経産省が企業に対して情報セキュリティガバナンスの考え方を提示し、「情報セキュリティ報告書」の作成・公表を促すなど民間に関する施策に取組んでいましたね。

普及啓発としての情報セキュリティの日

三角　やはり、民間における情報セキュリティの普及啓発は大事です。その一環として、当時、政策会議は 2 月 2 日を「情報セキュリティの日」としましたね。これは、第 1 次基本計画が決定された日ということからですね。

小林　情報セキュリティの日は 2 年目に定めました。2 月 2 日は第 1 次基本計画が決定された日ではありますが、「情報セキュリティの日」というより、関連行事を集中的に行う「情報セキュリティ月間」のようなものを新設し、これをぜひ 2 月にしたいという狙いがありました。先行するものとして６月頃には情報通信月間が、また 10 月頃には情報化月間がありました。こうしたイベントとは被らない時期として２月が一番よいのではないかという意識でした。第１次基本計画もスケジュール的に２月に決定できそうだという状況でしたので、２月２日に政策会議開催の段取りがついて、決定

されたわけです。

三角　情報セキュリティの普及啓発は、国民全体の課題として重要なことですからね。埋もれないようにすることは肝要だと思います。

重要インフラ 10 分野はどのように決まったか

三角　次に、2005 年 12 月 13 日に策定された「重要インフラの情報セキュリティ対策に係る行動計画」（政策会議決定。以下、「行動計画」）についてうかがいます。まず、第1回政策会議決定の「早期に着手すべき横断的課題」では、ISAC（Information Sharing and Analysis Center）と呼ぶ情報共有・分析機能の創設支援と記載されていました。一方、行動計画では CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response）と言い替えたのはなぜでしょうか。

小林　ISAC はテレコム・アイザックなど固有名詞に使われていることが多いので、それを一般的な名称にすることは避けた方がよいのではないかという議論がありました。また、新しい概念には新しい名前を付けるべきという問題意識もあって CEPTOAR という造語を作ったのです。CEPTOAR は日本語で「情報共有・分析機能」といわれますが、最後の「R」は「レスポンス」で、CEPTOAR はレスポンスも含んでいる新しい概念用語です。ISAC の語は「情報共有、分析」で「レスポンス」的な要素が名称には含まれていません。

三角　なるほど、対応も含める意識があったわけですね。

次に、重要インフラ分野はどのように定められたのでしょう。情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス(地方公共団体を含む)、医療、水道、物流の 10 分野があげられています。

小林　当時、重要インフラとは何かということについて、漠然とした理解はありました。情報通信、電力、ガス、水道は生活の基盤インフラゆえ重要インフラとして認識されましたし、航空管制でプログラムミスによるシステム障害の事案があったことから航空も重要インフラとして認識されました。なぜ 10 なのかについては、重要インフラとして認識されるものを列挙していったら 10 個になったということだったと思います。その後 14 分野に拡大しました。新たにあがったのは、空港、化学、クレジット、石油の4分野ですね。これらは当時、重要インフラだと認識されていませんでした。

三角　それらは私が NISC にいたときに追加されました。その理由の一つは、2011 年3月 11 日の東日本大震災です。震災を受けて石油供給の重要性が改めて一層認識されたことに始まります。その際に、同じようなプラント産業である化学も加わっています。クレジットについては、決裁の電子化が進む中、金融の延長線上で加わったと理解しています。空港は、航空分野が機能するには不可欠なものであるからです。

一方、豪雨など自然災害で下水道は重要ですが、現在のところは重要インフラとはなっていません。

小林　災害との関係の情報セキュリティとしては意識されるかもしれませんね。

私が最近執筆したコラム「サイバーセキュリティと情報セキュリティの狭間にて」（JCIC）で指摘したのですが、「サイバーセキュリティ基本法」（2014 年 11 月 6 日）ではサイバーセキュリティを「いわゆる電子的な情報、情報システム、情報通信ネットワークの安全性および信頼性が、対策を講じることで維持管理されていること」と定義しています。世の中ではあまり認識されていないようですが、「攻撃」という言葉でまとめていません。サイバー空間における攻撃以外にもリスクはあります。それが顕著に出るのが災害のときです。基本法的なサイバーセキュリティの対象の中にはいろいろなものが入りうるのですが、攻撃されるものという狭い意味でのサイバーセキュリティだけを考えると、下水道は恐らく入りません。

三角　重要インフラは「攻撃」されうるものを念頭に置いて考えていらしたということですね。重要インフラについては、現在、ますます深刻なサイバー攻撃などの脅威に晒されるようになってきていますが、NISC 発足当時からそうした危機感のもとメリハリをつけて対応していたということですね。

本日は、NISC 発足当時の経緯や取組みについてよくわかりました。どうもありがとうございました。

（注）2001 年 3 月 22 日開催の本行事の記事は以下のリンクで読むことが可能。

https://xtech.nikkei.com/it/free/ITPro/NEWS/20010322/1/

（2023 年1月 16 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]）

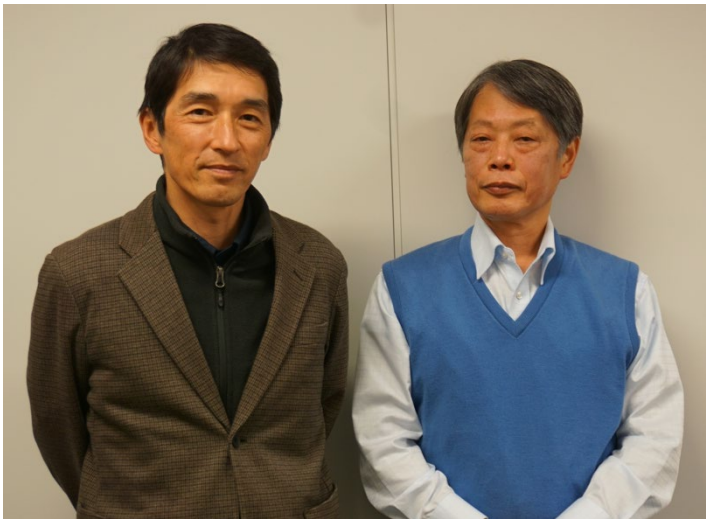
【出席者　略歴】

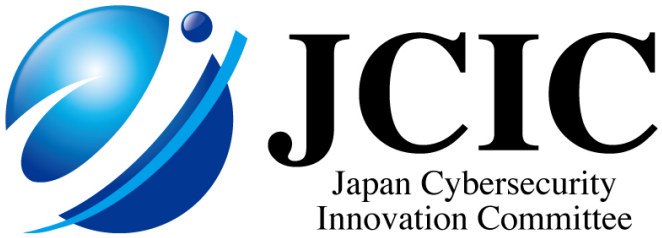
小林　正彦（こばやし　まさひこ）氏

1979 年に通商産業省入省。情報化政策、技術開発政策を中心に各部署を歴任。1999 年に独立行政法人情報処理推進機構（IPA）内に設立されたばかりのセキュリティセンターの所長を務め、2005 年に新設された内閣官房情報セキュリティセンター（SNISC)の初代内閣参事官を務めるなど、日本の情報セキュリティ政策の黎明期に顕著な足跡を残した。2007 年に退官。日本情報経済社会推進協会（JIPDEC）常務理事などを経て、2021 年より JCIC 客員上席研究員。

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