2024 年 2 月

シリーズ 「日本のサイバーセキュリティ政策史」第 6 回

サイバーセキュリティ対策黎明期の重要インフラ防護

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 6 回は、内閣官房情報セキュリティセンター(NISC)発足時に重要インフラ防護担当参事官を務めた立石譲二氏をお迎えし、話をうかがいます。「日本社会は『恥の文化』で、自社の恥は他者に共有しません。そして日本人は何かが起こらない限り、残念ながら、行動が起こせないということにも注意が必要です」──大規模サイバー障害事案とは無縁、セキュリティ意識の醸成される前の時代の日本の経済社会において政策立案・実施に奔走する中で痛感した日本の課題とは。

【出席者】

立石 譲二 氏
一般財団法人海外産業人材育成協会（AOTS）専務理事／
元内閣官房副長官補(安全保障・危機管理)付内閣参事官
内閣官房情報セキュリティセンター（NISC）重要インフラ防護担当

聞き手：
三角 育生 氏
東海大学情報通信学部長・教授

サイバーテロ対策から情報セキュリティ対策へ

三角 立石さんは、内閣官房情報セキュリティセンター（NISC: 2005 年4月設立。2015 年に「内閣官房内閣サイバーセキュリティセンター（NISC）」に改組）設立に参画し、重要インフラ防護、政府機関のセキュリティ対策促進等を主導されました。NISC の前身である内閣官房情報セキュリティ対策推進室の時代からいらっしゃったのですね。

立石 そうです。2004 年に内閣官房副長官補(安全保障・危機管理)付内閣参事官として情報セキュリティ対策推進室に着任しました。ちょうど山口英先生（奈良先端科学技術大学院大学教授、故人）が情報セキュリティ補佐官に着任（同年 4 月）されて、高度情報通信ネットワーク社会推進戦略本部情報セキュリティ専門調査会の下に「情報セキュリティ基本問題委員会」（委員長：金杉明

信氏［日本電気株式会社代表取締役社長、故人］、同年 7 月設立）が立ち上がろうとするころです。2005 年の NISC 設立をまたいで 2006 年までの3年間在任しました。

三角　本日、おうかがいしたいことの中心は、重要インフラ領域における情報セキュリティへの取り組みについてです。関連文書を振り返ると、まず、「重要インフラのサイバーテロ対策に係る特別行動計画」（2000 年 12 月 15 日、情報セキュリティ対策推進会議。以下「特別行動計画」という）があります。その後の課題を踏まえて「第 2 次提言　我が国の重要インフラにおける情報セキュリティ対策の強化に向けて」（2005 年 4 月、情報セキュリティ基本問題委員会。以下「第 2 次提言」という）の提言がなされ、NISC の「重要インフラの情報セキュリティ対策に係る行動計画」（2005 年 12 月、情報セキュリティ政策会議決定。以下「第１次行動計画」という）が決定されました。これら文書発出にいたる経緯や背景をおうかがいできればと思います。

最初に、特別行動計画から第 2 次提言で変わった点についてです。

特別行動計画では、同計画の目的を「いわゆるサイバーテロなど、情報通信ネットワークや情報システムを利用した、国民生活や社会経済活動に重大な影響を及ぼす可能性があるいかなる攻撃からも重要インフラを防護すること」とし、対象とする重要インフラ分野として、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）の 7 つを位置づけています。

一方、第 2 次提言では、重要インフラとは何かを定義し直し、対象事業については、従来の 7 分野に加えて、水道、医療を、また物流等を対象に含めるべく見直すとしています。さらに、セキュリティ対策を行う対象を、特別行動計画が示したサイバーテロのような意図的な攻撃だけでなく、人為的ミスや自然災害に起因する事象まで広げました。そのあたりの背景を教えてください。

立石　まず、情報セキュリティ対策を行う対象、つまり「護るべきもの」の範囲を改めて定義した背景には山口補佐官の情報セキュリティに対する強い信念がありました。すなわち、サイバーテロ攻撃という（悪意ある）意図的要因に基づく切り口だけから入ってしまうと、もう一方の信頼性を損なっている主要な原因、すなわち人為的ミスや自然災害など非意図的要因による IT 障害が手つかずのままになってしまうという課題です。重要インフラのサービス維持と復旧が大切なのです。重要インフラの各事業において発生する障害（サービスの低下や機能不全等）のうち、IT の機能不全が引き起こす障害を指しますが、非意図的要因に起因する障害もサイバーテロ起因の障害同様、経済活動や国民生活には多大な支障をもたらすわけですから、同様の備えをしておかないと重要インフラの防護の対策としては完結しないということでした。その観点から、われわれが備えるべきは、サイバーテロ対策だけではなく、情報セキュリティ対策であったのです。情報セキュリティは「コンフィデンシャリティ（Confidentiality: 機密性）」、「インテグリティ（Integrity: 完全性）」、そして「アベイラビリティ（Availability: 可用性）」の3つの要素からなりますが、重要インフラ防護の一環として IT 障害に備えることは、3つの要素の維持・確保にかかっているという考え方でした。

重要インフラ分野を見直す

立石　重要インフラ分野については、既存の6つの業種および政府・行政サービスの7分野に限られないだろうという考え方は当初からありました。例えば、食料が届かないと困る、エネルギーや

立石氏

石油化学プラントも重要だ等の議論が当時ありました。

水道については、当時、日本では事件は起こっていませんでしたが、海外、例えば、豪州では既にサイバー攻撃によって未処理の汚水が下流河川に大量に放出されるなどの事案が実際に発生していました。飲み水の安全は、国民生活にとって重大であることから第 2 次提言で加わりました。

三角　もう一つ、第 2 次提言で加わったのは医療ですね。

立石　医療については重要インフラのサイバーテロ対策に係る特別行動計画（特別行動計画）のフォローアップで分野追加への検討が明記されていました。しかし、当初、医療関係者によると、自分たちのシステムはインターネットにつながっていない、あるいは使用している製品が汎用ではなく特注だから、脆弱性は共有されない、という意見が医療関係者や機器メーカーの多くにあったようです。

三角　物流については、第 2 次提言で含みがある表現となっています。この点はどうでしょうか。

立石　物流は最後まで議論がありました。一般に、重要インフラ事業者になると国からの指示やそれに基づくさまざまな負荷（負担やコスト）が増えることへの懸念が生じるのも事実です。コスト意識に敏感な物流業界においてもそのような捉えられ方があったかと思います。

三角　結果的には、物流も、第 2 次提言で重要インフラ分野として追加されました。

重要インフラに指定された分野の関係者は納得されていたのですか。

立石　当時、一部に疑問を感じていた方はいらっしゃったのではないかと思います。現実に顕著な情報セキュリティ事案が発生したことがあったのは、政府組織においてでしたから（※2000 年の省庁ウェブサイト改ざん事件のこと）。それにもかかわらず、国民生活に密接に関わる分野を重要インフラとして指定し、対策を講じるべき、訓練に参加すべきと指導されることは、すぐには納得しにくいものがあったと想像します。最終的には事業運営に関わるすべてのシステムではなく、事業継続に関わる「重要システム」に対象を限定するということで合意していただきました。

三角　第 2 次提言と第 1 次行動計画との関係についてですが、NISC 設置以前の 2004～2005 年で推進してきた政策の延長線上に、NISC における政策があると理解してよろしいでしょうか。

立石　はい、継続形です。

三角　そうすると、もともと水道、医療、物流を重要インフラ分野に指定することは視野にあったということですね。

立石　海外がそうでしたから、当然視野には入っていました。

三角　一方で、第2次提言には「石油プラント」の脆弱性に関する記述等がありましたが、第1次行動計画には石油等の分野は入らず、第 3 次行動計画（「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」2014 年 6 月、情報セキュリティ政策会議）まで待つことになりました。第 2 次提言策定時点では、プラント関連の業種では、意見が収まらなかったということでしょうか。

立石　海外では火を吹いた石油プラントがありますよ、という話をしても、関係省庁も事業者側も、日本では発生しないという立場でしたし、防災の観点からは石油コンビナート等災害防止法という

特別の法律が制定されていたという事情もあります。

三角氏

三角　例えば電力業界は、米国と日本とは業態がまったく違ったりします。そういった業態の違いがあるという認識からの意見ではないでしょうか。

立石　電力分野の関係者はそう言っていました。大半が民営化されマイクログリッド（小規模電力網）化が進んでいる国と、民間とはいえ地域独占が確立している国とは、状況は異なるといった意見です。また、プラント内の制御システムに海外では主流の SCADA のような汎用的ソフトウエアを利用していないという事情もあったのかもしれません。

三角　おそらく制御装置等の設計思想等は日本と海外では異なるものもあるし、物理的な防護を施しているから安全といった意識があったのでしょうね。

立石　重要インフラ事業者の意見には、制御系システムの大半はいわゆる一品モノ（特注品）を使用しており、基本的にインターネット上の汎用システムやそれらの脆弱性から独立しているから大丈夫だというものがありました。しかし、実際の現場を視察すると中央制御室の表示画面の中には Windows のロゴが表示されたパソコンなども使用されています。外部ネットワークとは接続されていない、と言う人もいましたが、遠隔でシステムのメンテナンスを受けていれば、メンテナンス業者がアクセスできるよう専用の外部ポートは開いているわけです。

当時、日本の代表的エアラインの発券カウンター窓口システムの電子証明書の有効期限情報がメイン業務システムのプロバイダーに共有されず、発券業務が全面停止する事案が発生しました。事案の発生自体は不幸なことですが、類似したことをときどき経験していれば、他の事業者でも、もう少しセキュリティ意識が高まったと思います。

また、2003 年 3 月には、飛行計画情報処理システムがプログラムミスによりダウンし、東京航空管制の機能が止まる事案がありました。国際民間航空機関（ICAO）のルールで、離発着時間や経路等の一連の航空輸送プランを共有しなければいけないのですが、そのプランの登録ができなくて離発着できず、航空ダイヤが全国的に混乱しました。一般的に、既存のシステムから新たに構築するシステムに切り替えるときには、新システムにトラブルがあったときには、すぐにスイッチを切り替えて旧システムに戻して稼働し続けられるよう、新旧並列、あるいは段階的な入れ替え体制をとります。しかし、その事案のときには、旧システムを完全に取り払った後に新システムに不具合が生じてしまったという事情があったのです。

三角　航空関連は、さまざまな関係者がいて複雑ですね。航空機の運行については航空分野の事業者で重要インフラの対象です。ご指摘のような航空管制に関するものは、国土交通省、すなわち政府機関の課題となりますね。

立石　今までお話したように、防護すべき重要インフラ分野を決めるときにはかなり苦労しました。とりわけ、人によって考えることが異なるため、重要インフラの定義をどこかでピン留めする必要があるだろうということになりました。そこで、第 2 次提言および第 1 次行動計画で明示しました。重要インフラとは、「他に代替することが著しく困難なサービスを提供する事業が形成する国民生

活及び社会経済活動の基盤であり、その機能が停止、低下又は利用不可能な状態に陥った場合に、我が国の国民生活又は社会経済活動に多大なる影響を及ぼすおそれが生じるものである」というものです。

三角　重要インフラの定義の議論はいつごろからされていたのですか。

立石　私が議論に参画したのは、第 2 次提言の検討段階からです。検討段階を経て、第 2 次提言をまとめるにあたり重要インフラの定義を固め、該当する事業の範囲をファインチューニングしました。

ISAC を超えた体制をつくれ

立石　NISC 設置後も、重要インフラについては、高度情報通信ネットワーク社会推進戦略本部情報セキュリティ政策会議に 2005 年 9 月に設置された重要インフラ専門委員会で引き続き議論され、私は同専門委員会の事務局担当の参事官として第 1 次行動計画案をまとめていきました。「CEPTOAR（Capability for Engineering of Protection, Technical Operation, Analysis and Response: セプター）」もその議論の過程で誕生したのです。

三角　第 2 次提言では、各重要インフラ内の情報共有機構「情報共有・分析センター（ISAC［Information Sharing and Analysis Center: アイザック］）」が必要と書いてあるのに、第 1 次行動計画では CEPTOAR に変わっていますが、その理由は何でしょうか。

立石　実は、当初、ISAC のようなセクター別のインシデント情報共有分析組織を念頭に制度設計を検討していました。しかし、山口補佐官が「私が目指しているのは ISAC ではない」とおっしゃったのがきっかけです。すなわち、情報共有（インフォメーションシェアリング）だけではなく、自身が所属する産業セクターに属するメンバー間で、セキュリティ強化策の実装（ディプロイ）までやらなければいけないという考え方です。補佐官から、インフォメーションシェアリングではない別の名称を考えてくれと何度もダメ出しがありました。そこでいろいろ考えている中で、職員の一人から「Capability for Engineering of Protection, Technical Operation, Analysis and Response と言い表すと、頭文字が『CEPTOAR（セプター）』になります」とのアイディアが出されました。それを山口補佐官に伝えると、「いいね、それ！それだよ！」とおっしゃって、それで決まったというのが裏話です。

三角　第 2 次提言では、重要インフラ横断的な情報共有を推進する組織の設立についても予告しています。

立石　第 1 次行動計画で「重要インフラ連絡協議会（CEPTOAR-Council: セプターカウンシル）」（仮称）を創設すると記載しました。当初、一般社団法人経済団体連合会に横割りの事務局を置くことを考えましたが、当時はサイバーセキュリティ事案への実感や関心が薄く、経営者が集まる組織にそれぞれの現場で起こりそうな情報を共有し、対策を実装する事務局を置くというのは現実的ではありませんでした。

三角　セプターカウンシルは 2009 年 2 月に創設されました。そうした経緯もあって、当面、NISC が事務局を務めることになったのですね。

サイバー攻撃だけを考えていたわけではない

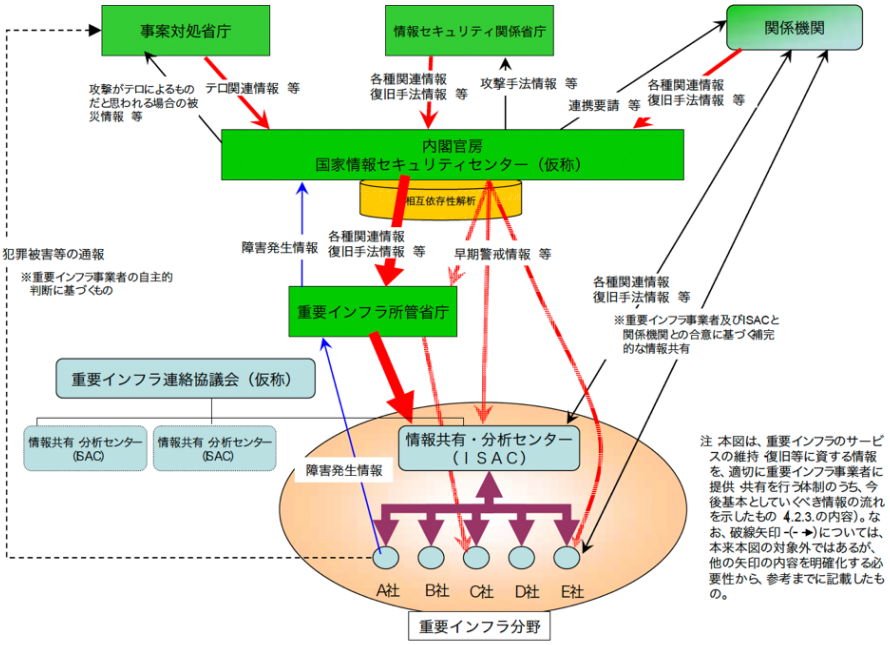
三角　第 2 次提言で重要インフラの対象拡大の方針を示し、第 1 次行動計画で医療、水道、物流が加わりましたが、重要インフラ分野の対象範囲を広げる作業が大変だったのですね。ほかにご苦労されたことはありますか。

立石　第 2 次提言に掲載した「情報提供・共有体制のイメージ図」に関するものがあります（下図参照）。この図は、重要インフラサービスの維持・復旧に資する情報を、適切に重要インフラ事業者に提供、共有を行う体制のうち、今後基本としていくべき情報の流れを示しています。この図において、事案対処省庁に対して伸びる矢印が破線であることについて理解を得るのが難しかったことです。なぜ障害発生時点で情報をシェアすることを示す実線ではないのかとの意見がありました。

三角　破線にした意図は何でしょうか。

立石　先日（2024 年 1 月 2 日）の羽田空港における日本航空機と海上保安庁機の衝突事故を思い浮かべてください。警察の捜査では、過失であっても刑法上の責任の有無を焦点とします。そして、捜査の結果立件されれば、その責任等はその後の裁判での争点となるのです。一方、再発防止策を検討するためには、何が起きたのか、科学的な知見が必要です。そのためには関係者に真実を証言してもらわねばならないのです。しかし犯罪立件のために情報が用いられるようであっては、その疑いをかけられた者の協力は得られにくくなります。現在も国内では賛否が分かれているのは承知していますが、海外では事故調査の際には真相究明のための関係者への聴取には刑事訴追の免責が設けられている国も多いのはそのためです。

図



「第 2 次提言　我が国の重要インフラにおける情報セキュリティ対策の強化に向けて」（2005 年 4 月、高度情報通信ネットワーク社会推進戦略本部 情報セキュリティ専門調査会 情報セキュリティ基本問題委員会）41 頁図 3「情報提供・共有体制のイメージ」

話を戻して、第 2 次提言では、情報セキュリティ対策を強化するため、事案発生検知から被害拡大防止、情報分析・検証と対抗策・再発防止策の検討および実施という一連の流れを示すことを目的とした同図では、事業所管省庁や関係団体との間で、何が起こったのかを分析して、その対応策を講じた上で、必要な情報が事案対処省庁に提供されるという流れを示しています。つまり犯罪捜査は別トラックとして並行して動いているという認識です。

三角　破線矢印について、「本来本図の対象外ではあるが、他の矢印の内容を明確化する必要性から、参考までに記載したもの」と付記されていますが、そういう背景があったのですね。実際、サイバー攻撃等の被害があれば被害届を提出すればそれが端緒となりますし、刑事責任を追及すべき事件であれば、親告罪でないかぎり、通報の有無にかかわらず捜査、起訴はできますね。

立石　いろいろな意見はありました。「重要インフラ事業者も、不正行為を発見すれば告発義務を負っているはずだ」という委員もおられました。しかし、IT 障害の原因には、システムエラーなどもありうるわけです。ポイントは、われわれは、当初から、システムエラーについても考慮していたのであって、サイバー攻撃だけ考えていたわけではないということです。そこまでを含めた情報共有の仕組みとする必要があったのです。

さらに、情報共有を進めるにあたっての課題として、日本の社会では、なかなか、都合の悪い情報を他人に話したがらないということがあります。いみじくも米国の文化人類学者ルース・ベネディクトが洞察したように、日本社会は「恥の文化」で、自社の恥は他者に共有しません。このことはしばしば問題となるものです。深く静かに潜航していて、ある日ある時気づいたら、何十年もその不正を続けていたというような話がいきなり出てくるわけです。

加えて、苦労したポイントとしては、海外のサイバーテロの事例を持ち出しても、聞いた人はみんな「所詮海外の話でしょう。日本で起こるわけがありませんよ」などと言う点でした。どこからそういう自信が湧き上がってくるのか、私にはまったくわからなかったのですが、「あなたは SF マニアですか？」とまで真顔で言われたりもしました。

現在にいたる課題も

三角　分野横断的演習検討に着手をしたのは立石さんの在任中ですか。

立石　私はそれをやり始めようとするときに離任しました。大規模演習をやろうとしたきっかけは、出張先の米国で知った米政府による演習「サイバーストーム」です。これは連邦政府・州政府・地方政府、重要インフラやシステム部門を含む民間、および関係国等が一堂に会し、サイバーセキュリティ事案への具体的な対応、関係省庁間の協調、官民連携や情報共有、回復のためのメカニズム等を検証・評価する国家的規模の演習です。

実際に米国を訪問し、この演習について取材した際に、関係者から異口同音に「会議室の中で、あらかじめ設定されたシナリオに沿って机上での訓練を繰り返しても意味はない。決められた手順どおりに実行できるかを確認・点検する訓練（ドリル）ではなく、想定しない事態の発生に対し事前の正解のない世界で関係者が着実に対応できるのかを確認し、うまくいかなかったところを反省して手順を改善していくための演習（エクササイズ）が必要なのだ。この演習（サイバーストーム）

の目的は重要インフラのサイバーセキュリティ演習（エクササイズ）であってサイバーセキュリティ訓練（ドリル）ではない」と言われました。

三角　どのような内容を考えていたのでしょうか。

立石　まず、実際に演習に参加するプレイヤーとは独立した統裁部を置きます。統裁部は演習に加わらず、各プレイヤーたちの行動を見て、期待する行動をとったかどうか記録に残していきます。振り返りの際の材料にするためです。プレイヤーには、政府、関係省庁、民間部門等のグループおよび役割を割り振ります。シナリオに基づいて、さまざまな状況がプレイヤーに付与されます。それらをグループ内で共有し、どのようなアクションをとるべきかを考えます。シナリオを事前に知っているのは統裁部だけです。例えば、海外からのサイバー攻撃を疑わせる証拠が確認された、と政府に報告が入る。政府内で議論するとともに、関連省庁に連絡し、確認する。官房長官役のプレイヤーは記者会見を開き状況を国民に説明する。メディアはそれを報道し、広く知られるようになると、自分たちは大丈夫だろうかと各組織で確認をする作業が走ったりする……というふうなことを思い描いていました。

三角　事案が発生したときに、どういう対応、行動をするかをディスカッションし、課題を洗い出していく机上演習（TTX）ですね。

立石　そうです。当時、自衛隊から出向されていた参事官補佐の方が、防衛における机上演習の知見を貸してくれました。それを重要インフラの演習でもぜひ取り入れたいと思っていたのですが、実行するところまでは私は NISC にいませんでした。

実は、NISC を卒業した後、独立行政法人情報処理推進機構(IPA)在職時代に FIRST（the Forum of Incident Response and Security Teams）とドイツ内務省 BSI（連邦情報セキュリティー庁）の共催でベルリンにおいて実施されたサイバー演習に参加する機会があって、まさしく思い描いていたような演習を実経験することができました。そのときの私の役は政府部門のチームの一員でした。会議室には被災国の大統領のコメントやさまざまな組織のプレスリリース、何時何分までに〇〇地区の通信を停止する、といったニュースが時々刻々とメール配信され、各会議室に飛び込んでくる。政府の立場で私は、さまざまな状況を踏まえて、事実に基づいてプレスリリースの文章を考えなければなりません。リスクコミュニケーションの鉄則は、最初に疑わしい被害の全容を言っておいて、事実が判明するほどに被害が小さくなっていく。「継続調査の結果、これまでの想定より被害は限定されることが判明しました」というのがベターです。最初に「大丈夫です」と言っておいて、「調べたら被害が確認されました」「もっと調べたらもっと被害がありました」というのがバッドコミュニケーションです。その鉄則を犯さないようにと私も他のメンバーも行動しました。

三角　そうした演習のほか、課題としてどのようなことをお考えでしたか。

立石　日本に欠けているのはセキュリティ・クリアランス（適格性調査）です。

今まさに経済安全保障でホットなイシューになっていますけれど、情報共有しても心配のない相手かどうかの識別子が日本にはありません。NISC 在任中に英国の National Infrastructure Security Co-ordination Centre (NISCC: 現在の National Protective Security Authority[NPSA])に行く機会がありました。そこで「重要インフラ防護を考えるにあたって、セキュリティクリアランスはどうするつもりか？」と真顔で質問された経験があります。NISCC は重要インフラ防護のため関係する事業者間の機微な情報共有等を図る政府横断的な組織で、北アイルランドのテロ等、事案の発生が懸念される危険情報をシェアします。情報の受け手は、(Need to Know の原則に従って)知るべき立場にあるから情報を受け取り、それに応じた行動が求められます。ただし、その情報は決して認められた者以外にはシェアしてはいけないという規則があるのです。それを守れる人たちで構成されています。

さらに、繰り返しになりますが、日本は「恥の文化」の国です。そして日本人は何かが起こらない限り、残念ながら、行動が起こせないということにも注意が必要です。何かが起こらない限りはリアリティが湧かないのです。行政においてもきっかけとなる事実が必要であるというようなところがあります。

三角　いろいろ課題はあったものの、まず取り組むべき課題を第 1 次行動計画に記したということでしょうか。

立石　だるまの両目を入れられたかと言われると、片目しか入れられなかったところはあります。情報共有の仕組みとルート・組織、セキュリティ事案および重要インフラの定義、そして演習の必要性を含めて第 1 次行動計画にとりまとめるところまでをなんとかやったということです。大きな体系をつくって、あとはやり残したところを諦めずに着実に広げていく、というところまでやったところで、後任の参事官と交代し、私は NISC の政府機関の情報セキュリティ対策推進の担当参事官に移りました。

三角　立石さんが米国や英国に出張されて経験しているから気づけたことや、それに基づく思いが、組織的に引き継がれたのだとよいと思います。立石さんのお考えなどがきっかけとなった重要インフラ事業者等による横断的な演習はその後、継続されています。確かに、立石さんがおっしゃるように参加者が急増したのは、2015 年の日本年金機構の事案があった後、すなわち、きっかけとなる事象があったことによりますが。その後も、参加者は増え続け、2023 年の演習では、過去最多の 6,000 名規模となっています。セキュリティクリアランスに関しては、特定秘密保護法が 2014 年から施行され、適正評価等が行われましたし、現在、経済安全保障の議論の中で、より対象範囲の広いセキュリティクリアランスの検討が進められています。これらは NISC の外での制度ではありますが、着実に進んでいるわけですね。

本日は、NISC が設置されたころの重要インフラに係る政策立案・実施の背景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。

(2024 年 1 月 15 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】

立石 譲二（たていし じょうじ）氏

一般財団法人海外産業人材育成協会（AOTS）専務理事

1985 年東京工業大学大学院総合理工学研究科システム科学専攻修士課程修了。1998 年同大学院社会理工学研究科社会工学専攻博士課程修了。1985 年通商産業省(現経済産業省)入省、生活産業局繊維企画官、JETRO バンコクセンター次長等を経て、2004 年より内閣官房副長官補(安全保障・危機管理)付内閣参事官として、内閣官房情報セキュリティセンター重要インフラ防護担当、同センター政府機関総合対策促進担当等を務める（～2006 年）。その後、大臣官房参事官(調査統計グループ・総合調整担当)、独立行政法人情報処理推進機構(IPA)理事(技術本部長)等を歴任し、2017 年より現職。

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。

JCIC
Japan Cybersecurity
Innovation Committee

[本調査に関する照会先]

JCIC 事務局　info@j-cic.com