Internet Governance Forum 2019 参加報告書

2019 年 12 月 27 日

上田 格

1. はじめに

◆ Internet Governance Forum とは？

Internet Governance Forum とは、インターネットガバナンスの問題に関し、マルチステークホルダー（各界関係者）間で政策対話を行う、国際連合管轄下に設置されているフォーラムのことです。IP アドレスやドメイン名の管理に関する対話だけでなく、サイバーセキュリティやオンラインコンテンツの人権問題に至るまで幅広い対話を行っています。

今年（2019 年）は” One World. One Net. One Vision.”をテーマにドイツ・ベルリンにて 11 月 25 日～11 月 29 日まで開催されました。

◆ JPNIC 若手フェローシッププログラム(IGF 2019 参加支援プログラム)とは

JPNIC が日本の若い世代（18 歳～30 歳）を対象に、インターネットに関する国際会議に参加する機会(旅費等)を提供し、その経験を通じて、今後日本から関連分野の国際会議に積極的に参加する人々、インターネットを中心とするデジタル技術の国際的な動向に関心を持つ方々を増やすことを目的として旅費や会議情報等の支援をするプログラムです。

長期的には国際舞台における日本のプレゼンス向上に寄与することを目指しています。

◆私が本フェローシッププログラムに応募するにあたっての背景・動機

私がこのプログラムに応募した理由は、IGF で世界のインターネットガバナンスに関する議論のポイントや流れを捉え、少しでもサイバー空間が安全で信頼できるものになるよう貢献したいと思ったからです。

私は学生の頃からセキュリティの勉強をし、会社でもセキュリティの仕事をしていますが、インターネット空間の安全性・信頼性は必ずしも技術だけではなく、それを利用する人の問題でもあると感じています。

従って、政策的なガバナンスの議論も必要不可欠であると考え、その議論が最も多くされているのが IGF ではないかと考え参加を希望しました。

2. 参加したセッション

- Day0(11/25(月))
  - Youth IGF Summit
  - Strengthening the multi-stakeholder approach on international norms in cyberspace
  - Parliamentary perspective and opportunities for action

- IGF crash-course on emerging technologies

・ Day1(11/26(火))
  - IGF for Beginners Main Session
  - NRIs Collaborative Session on Cybersecurity: Discussing the National and Regional experiences in approaches and cooperation for cyber-security and cyber-safety and resilience for infrastructure providers and users
  - Tech Nationalism: 5G, Cybersecurity and Trade
  - Opening Ceremony

・ Day2(11/27(水))
  - Cybersecurity concerns everyone - Responsibility and education throughout the digital supply chain
  - Roadmap for Confidence Building Measures(CBM) in Cyberspace
  - Global Commission on the Stability of Cyberspace(GCSC)
  - BPF Cybersecurity: Putting agreements into action - operationalising cybersecurity norms

・ Day3(11/28(木))
  - Trust, Norms and Freedom in Cyberspace
  - Usual Suspects: Questioning the cybernorm-making
  - Issues on the Free Flow of Data, ICT Products and Services in a Digitally Connected World

・ Day4(11/29(金))
  - Information Sharing 2.0: Privacy and Cybersecurity
  - Security/Safety Concluding Session
  - Closing Ceremony

3. 2. のうち特に印象に残ったセッション

・ Parliamentary perspective and opportunities for action(day0)

このセッションは、主にドイツ・EU の議会議員を招いて、キーノートスピーチとワークショップ形式の 2 段階構成で、様々なステークホルダーからインターネットガバナンスに関して議会議員にインプット、議論をするものでした。ワークショップは「AI」「International Cooperation in secure open internet」「digital era democracy」「Peace and digitalization in a critical infrastructure area」の 4 つの小グループに分かれ、実施されました。

私は、「Peace and digitalization in a critical infrastructure area」のワークショップに参加しました。私はその中で下の 3 点が特に印象に残りました。

◆ 地位や出身母体に関係なく有名な政治家が参加者に気さくに話してくれた

私の参加した小グループにはエストニアの元外務大臣であり、GCSC の former chair であった Marina Kaljurand 氏が参加していました。議論の中で私の質問や他の参加者からの質問に対しても気さくに答えていたり、彼女の知識や考えを惜しみなく提供してくれました。例えば、「技術と政策のコミュニティのギャップをどのように埋めたらよいか？」という参加者の質問に対して、彼女は「技術の専門家には一般的な人が理解できる言葉で話してもらう訓練をしてもらうべき」というような回答をしていました。

◆ EU における hackback(サイバー攻撃に対して行うサイバー攻撃による反撃)の議論

EU においては、国家からのサイバー攻撃(安全保障の議論)においては北大西洋条約の第 5 条をかなり強く意識しているようでした。また、(北大西洋条約で国連憲章が引用されていることもあり) 国連憲章 51 条に則った集団的自衛権の行使も併せて強く意識していました。つまり、個別的自衛権の行使を使うより、EU を一つの国のように考え、サイバー攻撃に対抗していくという意思が強いように感じました。

しかし、本当にその特定の国家主体がサイバー攻撃をしたかという attribution 問題においても、100%確信が持てない限りサイバー攻撃による反撃(つまり個別的自衛権の行使や集団的自衛権の行使)は絶対にできないという認識で一致しているようでした。

なお、非国家主体からのある国家に対する攻撃であれば、当該国家からの反撃は国際法上許されず、それは警察権の行使の議論に移るということが話されていました。

◆ EU のサプライチェーン・リスクに関する議論

日本だけでなく、EU でもサプライチェーン・リスクマネジメントに関する議論が盛んに行われている印象が強く感じられました。国力の問題等で EU 圏の国すべてがその国の重要なシステムを国産化できるわけではないため、サプライチェーン・リスクマネジメントはより難しくなると認識しているようです。また、ENISA (European Network and Information Security Agency) でも正規のシステム部品(悪意ある動作をしない部品)であるという認証・資格を作成することも可能ではあると思うが、具体的な案はまだ出ていないとのことでした。

・ NRIs Collaborative Session on Cybersecurity: Discussing the National and Regional experiences in approaches and cooperation for cyber-security and cyber-safety and resilience for infrastructure providers and users

サイバーセキュリティ分野において、日本、ブラジル、アメリカ等の NRI(National and Regional Initiatives)の間の成功事例の共有や意見交換を行うというセッションでした。私はその中で下の 3 点が特に印象に残りました。

◆ 脆弱性情報の共有やサイバー規範の強化

まず、技術的な脆弱性情報を共有するコミュニティはより多くの価値ある情報を持つ

軍や情報機関と連携を図るべきであるとのことでした。また、サイバー空間の規範を強化・実行するためや規範に対する助言をもらうために規範を作り上げるプロセスにも軍や情報機関に参画してもらうことが必要なのではないかという意見がありました。

◆ 規範の実装
テクノロジーコミュニティの方から、サイバー規範の実装（実行）はマルチラテラルな形で、特定の国家のみ実施するのではなく、マルチステークホルダーで全員が取り組む必要があり、テクノロジーコミュニティはその最初の一歩を踏み出すべきであるという発言がありました。

◆ CERT(Computer Emerging Response Team)コミュニティの効果
実際、とある CERT で特定の国にいるハッカーから攻撃を受けた際に、FIRST のような CERT コミュニティでその国の担当者（カウンターパート）とその情報を共有し、調査を依頼することは実際効果があるという現場の情報が興味深かったです。

・ Cybersecurity concerns everyone - Responsibility and education throughout the digital supply chain

ドイツのシーメンスや IBM など「Charter of trust」に署名をしている企業による当該枠組みの説明や重要性に関するパネルディスカッションでした。私が最も印象深かった点は、「Charter of trust」のようなセキュリティ施策は、同じ文脈で語られることの多い、Paris Call などのいわゆる cyber norm とどのようなところが異なるのか？と質問したときに頂いた回答でした。発表された方によると、「加盟企業に関しても、事務局がきちんと気を配ることができる企業数にしており、着実に成果を出して、『charter of trust』が課している要件を確実に満たせているか否かに関して着目をしている。」と話されており、加盟企業数はさほど重要ではないという点が興味深かったです。

4. 今回の経験を今後どう生かしていきたいか

今回 IGF に参加することがきっかけで、別な国際ワークショップにお誘いいただくこともありました。このような繋がりを大事にしながら、今回の IGF で得た知見を土台に、日本国内だけでなく、インターネットガバナンスに関する国際的な議論も含めて注意深くウォッチし、セキュリティの技術や知識の獲得はもちろんの事、制度や政策に関してもさらに理解を深めたいと考えています。

5. 参加支援プログラムに対する所感

今回の参加支援プログラムでは、IGF に参加させていただき世界的な議論を聞けたことはもちろん、単純に旅費を提供頂いただけでなく、IGF の会議前後まで含めて、長く IGF に

関わっていらっしゃる方やインターネットガバナンスの専門家の方々の見解を伺う機会や質問させていただく機会をいただき、非常に有意義でした。