Cyber^3 Conference Okinawa 2015（議論の概要）

１．背景

- モノとモノとがインターネットでつながって自律的な情報のやり取りを実現する IoT（インターネット・オブ・シングス）により、広大で目に見えない**「サイバーコネクション」**網が世界中に拡大しており、様々なメリットをもたらす可能性。
- ただし、そのメリットの実現には、**「サイバーセキュリティ」**が必要不可欠。強靭なサイバーセキュリティがなければ、相互接続されたグローバル経済全体の安定・信頼性は確保できない。
- そのために、国際社会が一丸となって、ハイレベルな関係者が継続的に議論をすることが必要。もし対応ができなければ、既に急増している**「サイバークライム」**はますます増加し、大規模な被害を引き起こす可能性。

２．議論の概要

【サイバーコネクション】

- 行政、民間、ユーザー等、**IoT に関連する全ステークホルダーへの様々な教育が必要**。ユーザーが IoT のメリットを理解できるようになれば、IoT が受け入れられる比率も高まる（例：ウェブメールは、導入当初は安全と思われていなかったが、いまではほとんどの人が使っている）。
- IoT によってデータ量が増加すると、デバイスの脆弱性も必然的に増加するため、全ての脅威に対して完全に防御することは不可能。人体の免疫システムのように、外部からの無数の攻撃に耐えながらも、その影響を最小限に抑えて機能性を維持する、**耐性あるシステムの構築が必要。**
- IoT の規制にあたっては、全てのユーザーにメリットがもたらせるような、**バランスの取れた規制を構築することが必要。**

【サイバーセキュリティ】

- サイバー空間における諜報活動やサイバー攻撃に関しては、原発等の基幹インフラにはお互いに立ち入らないなど、**国家間で規範的な共通認識・ルールを構築し、合意点を見出していく取り組みが重要。**

・ 次のオリンピックでは、ハッカー、インサイダー、テロリスト等、あらゆるサイバー脅威に直面する可能性がある。**ロンドン五輪での経験を活かして綿密な計画を策定し、**全てのセキュリティ関係者が訓練を重ねる等、**十分な準備を行う必要。**

・ **サイバー規制は、**様々な利害・必要性を考慮しつつ、**適用国間での規範的価値や優先事項**（例：国境を越えた協力メカニズムの採用、インフラ保護、リスク管理など）**を具現化したものである必要。**国際免許証の仕組みは、各国の異なる道路規制においても機能しており、参考になる。

【サイバークライム】

・ **サイバー犯罪は国境を越えるものであり、国際的な法枠組みで対応する必要**があるが、現状の MLAT（刑事共助条約）では不充分で、新たな手法を開発する必要。

・ また、サイバー犯罪に関する技術は急速に進歩しているのに対して、法的な枠組みが十分に対応できていない。

・ 既存の情報共有モデル（例：インターポール、ユーロポール）はかなり進歩しており、これらを進化させつつ、**より強力な情報共有の実現のために、世界規模でのマルチステークホルダーによる協力が必要。**

・ 技術の進歩によって、セキュリティやプライバシーに関する課題も生じる。政府や企業は、優れたサイバー犯罪対策スタッフを育成し、経営幹部レベルを含めた準備・訓練を実施することで、脅威に対応する必要。

３．会議の意義・今後に向けて

・ 世界 30 か国から、政府関係者・企業経営者・大学教授等、異なる背景・視点を持つ 400 名超が一堂に会し、3 つのテーマについて情報共有・意見交換が行われた。このような**マルチステークホルダーによる対話プロセスは、複雑な問題の解決策にたどりつくために非常に重要な手法**であり、今後も継続してマルチステークホルダーによる議論が行われる必要。

・ 日本においては、2016 年の伊勢志摩サミットや、2020 年東京オリンピック・パラリンピック競技大会にむけて、セキュリティの強化が必要不可欠。**更なる官民連携、国際連携を推進し、世界各国と協力して、早急に取り組んでいく必要**。