資料９－２

# これまでの論点整理（案）

令和６年６月

# これまでのICTサイバーセキュリティ政策分科会の検討状況



これまでのICTサイバーセキュリティ政策分科会（以下「分科会」という。）において、

- 重要インフラ分野におけるサイバーセキュリティ対策強化の在り方
- サイバーセキュリティの基盤となる人材育成及び研究開発の在り方
- サイバーセキュリティの確保に向けた国際連携及び普及啓発の在り方

等、総務省が中長期的に取り組むべきサイバーセキュリティ施策の方向性についてご議論いただいたところ。

| 回　次 | 議　事　内　容 |
|---|---|
| 第１回<br>（R6.2.9） | ✓ サイバーセキュリティの最近の状況及びICTサイバーセキュリティ政策分科会について<br>✓ 我が国を取り巻くサイバーセキュリティの情勢（JSSEC、トレンドマイクロ）<br>✓ 通信分野におけるサイバーセキュリティ対策の取組について（NTTコミュニケーションズ、ICT-ISAC） |
| 第２回<br>（R6.2.27） | ✓ 放送分野におけるサイバーセキュリティ対策の取組について<br>（情報流通行政局、栗原構成員、日本ケーブルラボ） |
| 第３回<br>（R6.3.13） | ✓ 国際連携に係る取組状況について（NTTセキュリティホールディングス、JPCERT/CC）<br>✓ 海外における人材育成に係る取組状況について（JICA、世界銀行） |
| 第４回<br>（R6.3.27） | ✓ 地域における人材育成に係る取組状況（NICT、群馬県中之条町）<br>✓ 地域の事業者等に向けた普及啓発に係る取組状況（近畿総合通信局、日本シーサート協議会） |
| 第５回<br>（R6.4.5） | ✓ スマートフォンのセキュリティ確保に向けた取組状況（KDDI、OWASP）<br>✓ 情報通信ネットワークの安定性・信頼性の確保に向けた取組状況（KDDI、三菱総合研究所） |
| 第６回<br>（R6.4.26） | ✓ 自治体におけるサイバーセキュリティ対策の取組について<br>（自治行政局、KUコンサルティング、J-LIS、APPLIC） |
| 第７回<br>（R6.5.10） | ✓ 通信分野におけるサイバーセキュリティ対策の取組について（吉岡構成員、NICT、NTTコミュニケーションズ） |
| 第８回<br>（R6.5.27） | ✓ 量子計算機の進展に応じた耐量子計算機暗号の研究開発（NICT、KDDI総合研究所、横浜国立大学）<br>✓ AIの進展に応じたサイバーセキュリティ対策（新井構成員、三井物産セキュアディレクション、KDDI） |
| 第９回<br>（R6.6.14） | ✓ CYNEX・CYXROSS等について（NICT） |

# 分科会報告書の骨子案



➢ 総務省が取り組むべきサイバーセキュリティ政策について、当面の取組も盛り込みつつ2030年頃※も見据えた中長期的な方向性について、「ICTサイバーセキュリティ政策の中期重点方針」として取りまとめる。

※ 「2030年頃を見据えた情報通信政策の在り方」最終答申（2023年6月）によれば、2030年頃には、AIと人間の協働、サイバーとフィジカルの高度な融合、新たな生活・経済活動の場（メタバース）の実現等が期待されている。

- **サイバー攻撃の最近の動向**（サイバー攻撃関連の各種データ、最近の主なサイバー攻撃事案等）
- **サイバーセキュリティを巡る主な課題**（厳しさを増す国際情勢とサイバー攻撃リスクの高まり、多様化・複雑化するサプライチェーン等、セキュリティ人材の確保、生成AI等の新たな技術への対応等）
- **政府の主な動き**

**1．重要インフラ分野等におけるサイバーセキュリティの確保**

（1）通信（総合的なIoTボットネット対策、安全・安心な通信サービスの利用に向けたセキュリティ対策、サプライチェーン対策等）
（2）放送
（3）自治体
（4）データ流通基盤（クラウドセキュリティ、トラストサービス）

**2．サイバー攻撃対処能力の向上と新技術への対応**

（1）我が国のサイバー攻撃対処能力の向上（CYNEX・CYXROSS、人材育成等）
（2）新技術への対応（AIとセキュリティ、暗号技術）

**3．地域をはじめとするサイバーセキュリティの底上げに向けた取組**

（1）地域SECUNITY
（2）ガイドラインその他普及啓発に向けた取組

**4．国際連携の更なる推進**

（1）国際連携全般
（2）人材育成支援（AJCCBC、大洋州島しょ国その他地域への展開）

## （１）通信（総合的なIoTボットネット対策）

### ①新NOTICE（端末側の対策）

**【現状】**

- 2018年にNICT法を改正し、５年間の時限措置（不正アクセス禁止法の例外）として、NICTが、ID・パスワードに脆弱性のあるIoT機器を調査してISPに通知を行い、ISPが個別の利用者への注意喚起を行う取組（NOTICE）を2019年２月に開始。
- NOTICEの取組により、IoT機器の脆弱性解消に一定の成果はあったものの、依然としてID・パスワードに脆弱性のあるIoT機器を標的としたサイバー攻撃が発生している他、最近ではファームウェアの脆弱性を狙ったサイバー攻撃も増加。
- これを踏まえ、2023年にNICT法を改正し、NICTが行うIoT機器の調査について継続して実施可能とするとともに対象を拡充。
- 上記の法改正等を踏まえて、 2024年度より、 NOTICEをルータ等のIoT機器のセキュリティ向上を推進し、IoT機器を悪用したサイバー攻撃の発生等を防ぐためのプロジェクトとして再定義。
- 2024年４月から、ファームウェア脆弱性の調査と対処要請を開始。また、IoT機器の適正な管理に関する周知啓発活動を強化するとともに、IoT機器メーカやSIerとの連携により、利用者への注意喚起のみに依らない多様な関係者による対処を推進。

**【今後の取組の方向性】**

- 以下の取組を継続して実施することにより、ルーター等の乗っ取りの予防対策及び乗っ取られたルーター等のセキュリティ対策の見直しを推進してIoTボットネットの活動を抑制し、これに起因するサイバー攻撃の発生と被害の軽減を目指す。
  - ✓ ルーター等の管理者向けに、ルーター等の乗っ取りリスクと基本的な安全対策の周知啓発の実施
  - ✓ ルーター等を悪用したサイバー攻撃や、高リスク脆弱性を有するルーター等の調査
  - ✓ 高リスク脆弱性を有するルーター等については、関係者の連携による対処を推進
- NOTICEで得られたNICTの知見・ノウハウを活用し、高度な分析情報の提供や重要インフラを対象としたアタックサーフェス調査に取り組む。
- 適切なIoT機器のセキュリティ基準のあり方についても、NOTICEの取組や経済産業省で検討を進めているIoT製品に対するセキュリティ適合性評価制度の動向等を踏まえつつ不断に検討。

## （１）通信（総合的なIoTボットネット対策）

### ②C&Cサーバの検知・対処の推進（ネットワーク側の対策）

**【現状】**

- フロー情報の分析によるC&Cサーバである可能性が高い機器の検知について、正当業務行為として法的整理を実施した上で、2022～2023年度の2年間のプロジェクトとして、電気通信事業者におけるフロー情報の分析によるC&Cサーバ検知技術の有効性の検証や、事業者間の情報共有に当たっての課題整理のための実証事業を実施。
- 分析機能の強化や、能動的分析等の新たな手法の導入により、技術的に信頼度の極めて高いC&Cサーバリストの作成に成功。
- 分析結果として、C&Cサーバの挙動状況、国別やマルウェアファミリ等の属性も把握。
- オープン情報よりも早く検知されたC&Cサーバが数多く確認されており、フロー情報分析によって迅速な対処につながる可能性。
- フロー情報分析事業者の検出共通性は高くないことが判明しており、多くの事業者が分析に参画することで、より多くのC&Cサーバが検知できる可能性。

**【今後の取組の方向性】**

- C&Cサーバの生存期間が短いこと等も踏まえ、シード情報の拡充、AI技術の更なる活用、分析作業の自動化、能動的分析機能の拡充や外部プロジェクトとの連携等を進め、分析機能の強化や分析オペレーションの高度化を図り、より迅速かつ精緻なC&Cサーバリストの作成を目指す。
- 分析事業者の拡大に引き続き取り組み、C&Cサーバの検出網羅性の向上を図る。
- C&Cサーバリストに基づく対策については、まずは対策トライアルから始め、効果を検証しながら対策手法の改善を図っていくとともに、必要に応じて制度改正の検討を行う。
- 分析事業者が検知したC&Cサーバ情報の収集・精査・事業者への共有等、ハブ的な機能を担う統合分析対策センターについて、持続的な運用が可能となるように体制面等も含めて検討を進める。
- 上記について中長期的に取組を進めることにより、IoTボットネットの全体像を可視化した上で、各ボットネットの特性に応じた対処を実現することで、ボットネットの縮小を目指していく。

## （１）通信（その他の対策）

### ①安全・安心な通信サービスの利用に向けたセキュリティ対策

**【現状】**

- 利用者の意図しない利用者情報の取扱いが生じるスマートフォンアプリの類型として、透明性が不十分なアプリ、脆弱性があるアプリ及び不正なアプリに整理可能。
- これまで利用者が安心・安全にアプリを利用できるように、総務省がスマートフォン利用者情報取扱指針等を含む「スマートフォンプライバシーイニシアティブ（SPI）」を策定しているほか、民間団体もガイドライン等を策定しているが、アプリによる利用者情報の取扱いの実態を把握することは難しい。
- こうしたことを踏まえ、2023年度より人気アプリ等を対象に利用者の意図に反したスマートフォンアプリによる情報送信等について技術的な解析を実施することで、我が国のアプリ解析能力水準に係る課題等を整理。
- 我が国では導入が進んでいないRPKIや DNSSEC、DMARC等のネットワークセキュリティ認証技術について、昨年度までの実証結果を踏まえ、今年度に各認証技術を適切かつ円滑に導入・運用するためのガイドラインを新たに策定する予定。

**【今後の取組の方向性】**

- SPIについて、アプリケーション提供サイト運営事業者等による脆弱性があるアプリや不正なアプリへの対応等、セキュリティの観点を新たに盛り込んでいくとともに、スマートフォンアプリにおけるセキュリティ対策の実態把握等に取り組むことにより、我が国で広く普及するスマートフォンアプリにおいて、利用者情報が適切に保護される環境を目指す。
- ネットワークセキュリティ認証技術について、技術動向や企業の導入状況を踏まえつつ、各ガイドラインの周知啓発に取り組むとともに、企業の対策状況を可視化する枠組みの検討を進めることにより、各認証技術の導入を促進する。

## （１）通信（その他の対策）

### ②通信分野におけるサプライチェーン対策

**【現状】**

- 通信分野においては、オープンソースソフトウェア（OSS）の利用が急速に拡大していることを踏まえ、通信機器を対象としたSBOMを実際に作成することにより、我が国の通信分野におけるSBOMを導入する上での課題等を整理するとともに、諸外国におけるSBOMに係る動向を調査。
- 普及が進む5Gネットワークのセキュリティ確保を図るため、2022年に「5Gセキュリティガイドライン（第１版）」を公表し、本ガイドラインをベースにITUにおける勧告化に取り組んでいる。

**【今後の取組の方向性】**

- SBOMについては、経済産業省における取組とも連携しつつ、我が国の通信分野への導入に向けた留意事項等を取りまとめる等、SBOM導入の普及促進に取り組むことで、ソフトウェアの透明性を確保するとともに、OSS等のソフトウェア部品に含まれ得る脆弱性への対応の迅速化を目指していく。
- 5Gセキュリティについては国際標準化に関する議論の最新動向等も踏まえつつ、O-RANの海外展開にも貢献する観点から、継続してガイドラインのアップデートに取り組むとともに、Beyond5G/6Gについて標準化も含め我が国が先導的な役割を果たせるようセキュリティ分野においても貢献をしていく。

### ③最近の通信事業者における情報漏洩等の事案を踏まえた対応

**【現状】**

- 2022年３月～11月にかけて企業向けネットワークサービスを提供する事業者において、外部からの不正侵入による情報漏洩事案が発生したことを受け、2023年６月に再発防止のための行政指導を実施。また、2023年11月に、多くの国民が利用するメッセージサービスを提供する事業者において、不正アクセス等による情報漏洩事案が発生したことを受け、2024年3月及び４月に再発防止のための行政指導を実施。

**【今後の取組の方向性】**

- ICTの進展に伴い、サイバー攻撃による情報漏洩やサービス停止のリスク・社会的影響はますます増大しているところ、社会基盤を担う通信事業者において、企業全体としてのサイバーセキュリティ対策の向上が図られるよう、国として必要な支援及び指導を行っていく。

## 【第8回までの構成員等からいただいたご意見】

＜総合的なIoTボットネット対策＞

- マルウェアに感染させられる機器を観測していると、攻撃者同士の攻防があることが分かる。より適切な状況把握のためには、この状況を理解した上で観測を行うことが重要。【吉岡構成員】
- メーカーのセキュリティ対策においてはユーザへの適切な情報提供など改善の余地がある。【吉岡構成員】
- IoT機器のセキュリティ対策について、ユーザーだけでなくIoT機器メーカーやクラウドサービスプロバイダも含むISP/NW事業者の対応も重要ではないか。【盛合構成員、吉岡構成員、蔦構成員】
- ShodanやCensysは全世界向けのサービスで日本国内の機器に特化しておらず、シグネチャーの作りが弱いため、国内の機器を把握するには、信頼のおけるスキャナーを日本でも運用することは重要。【小山構成員、吉岡構成員】
- IoT機器で攻撃が行われているものの多くがルーターであることから、ISPの関わりが重要になると思う。例えばルーターのレンタル化を推進してISP側で管理するのが効果的ではないか。家庭用ルーターの脆弱性に係る責任を一般家庭に負わせることは無理があるため、ISPへ責任を課す方向もあるのではないか。【上原構成員】
- 新NOTICEがベンダーとISPを繋ぐ役割を担えるとよい。エンドオブライフを迎えた機器に対し、ベンダーが買い替えを促すためにNOTICEの枠組みで通知できるとよいのではないか。【上原構成員】
- 従来ISPを通した回線契約者への注意喚起だけではリーチできなかった対象について、ベンダーや設置業者との関係性を構築して対策を強化していくことが効果的である。【小山構成員】
- 通信インフラの健全性を維持するためにサイバー犯罪者のインフラを把握することは非常に重要。マスターC2、Tier2、3と、上位構造を含むボットネットの全容を把握して対策の効果判定を行えるとよい。【新井構成員】
- C&Cサーバの通信をブロックした場合の成果の測定をどのように行い、KPIを何に設定すべきなのかについては御意見をいただきながら考えていきたい。【小山構成員】

## 【第8回までの構成員等からいただいたご意見】

＜その他の対策＞

- スマートフォンアプリの動作に関する第三者検証は、利用者保護の観点からも必要な取り組みであり、我が国における解析能力の維持・向上は重要。解析事業者がスマートフォンアプリの解析を実施し、そのノウハウを共有する場を整えることが望ましい。【KDDI　本間氏】
- SPIの趣旨の周知徹底を図り、アプリストア運営者等の関係者においても、SPIを踏まえた適切な対応をとっていくことが重要。　【KDDI　本間氏】
- 現行のSPIにはプライバシーの観点から関係者が遵守すべき方向性を示しているが、脆弱性があるアプリや不正なアプリにおける利用者情報の取り扱い等に係るセキュリティの観点は明示的に含まれていないため、セキュリティの観点からの内容をSPIに盛り込むことが望ましい。なお 、その際 、日本スマートフォンセキュリティ協会 JSSECが策定した「スマートフォンアプリケーション開発者の実施規範 第一版2024年03月08日）」も参考にすることが望ましい 。【KDDI　本間氏】
- 技術水準の向上のためには教育が中心になると思うが、今後生成AIを用いたデコンパイルなど、解析ツールによる支援ができれば技術水準の向上や解析能力の属人性の低減に寄与できるのではないか。【新井構成員】
- 自社ネットワークセキュリティ対策技術の普及・促進を図るために作成した経営者・技術者に向けたガイドラインについて、中立性、継続性、専門性、妥当性・客観性、協調性、公平性の観点から、技術ごとにメンテナンスを視野に入れた運用体制の構築が必要。　【MRI　小川氏】
- ネットワークセキュリティの技術導入状況の外部公開や民間認定を進めるためには、運営体制や認定項目の設定等の軽重バランスをとった制度設計を行うことが重要。【MRI　小川氏】
- ２年程前から社内で開発している特定のシステムに対してSBOM出力を原則必須化している。様々なツールを活用することでSBOMは簡単に作成できるが、システムの変更や、新しい機能の追加により新しいソフトウェアの部品が必要になるとその度SBOMを作成し直すことになり、SBOMの維持管理に相当のコストを要する。【新井構成員】
- SBOMを作成しても最終更新が数年前というケースもあると聞く。更新・把握のしやすいツールは非常に重要。既存のツールの支援に当たって、一緒に開発に関わるなどするといいのではないか。【篠田構成員】
- SBOMの課題として管理のコストなどが挙げられていたが、サプライチェーンが広がることによる影響等、サプライチェーン上の課題も整理していく必要がある。【後藤主査】

## （２）放送

**【現状】**

- 放送は、国民生活にとって重要な情報伝達手段であり、極めて高い公共性を有する社会基盤であることから、重要インフラサービスの１つとして位置づけられている。
- ICTの進展に伴い、今後、放送分野においても、マスター設備（番組送出設備）を中心に放送設備のIP化・クラウド化・集約化が進むことが想定されることを踏まえ、サイバーセキュリティ対策をはじめとする地上テレビジョン放送等の安全・信頼性に関する技術的基準の検討を実施。
- 2023年11月に導入計画が具体化しているIP化について情報通信審議会から一部答申を受け、2024年４月に関連規定を整備。
- ICT-ISAC放送WGにおいても、放送設備サイバー攻撃対策ガイドラインの策定・普及、教育・訓練ツールの作成・配布等に取り組んでいる。
- ケーブルテレビについては、中小規模事業者によるセキュリティへの取組が不足していること等も踏まえ、業界団体が主導して、技術者向けのセキュリティに関する情報提供や人材育成支援等を実施。

**【今後の取組の方向性】**

- 放送設備のIP化を図る場合には放送事業者において安全・信頼性に関する新たな技術基準に基づくセキュリティ対策を着実に進めるとともに、放送分野におけるIP化・クラウド化・集約化の動向を引き続き注視しながら、必要に応じて基準の見直しに向けて検討を不断に行っていく。
- 放送分野のセキュリティ対策を支える人材育成・普及啓発については、民間や業界団体による取組とともに、CYDERや地域SECUNITY等の政府の支援策の効果的な活用も進めていく。

## 【第8回までの構成員等からいただいたご意見】

- 利用者の宅内端末が何らかの侵害で攻撃の起点になってしまうこともあり得るため、ケーブルテレビサービス全体のセキュリティを守るためにも利用者の宅内の端末のセキュリティを保っていくことも重要と考えている。【日本ケーブルラボ 取屋氏】
- 外部のネットワークに繋がずともファイル送付時のリスクはあるため安心とは言えない。放送事業者においても色々なシナリオを考えて対策・訓練を定期的に実施するのがよいのではないか。【盛合構成員】
- 放送設備側と番組制作側で意識に差はある。また、社員教育はできている一方、臨時スタッフ等も多く、またその入れ替わりも多い等の課題もある。【栗原構成員】
- 動作保証の観点からパッチが当てられないとの課題もあり、攻撃者が入らないようにネットワーク側で監視していくということが今後重要になってくる。【栗原構成員】
- IP化やクラウド化を前提に考えると、パッチを当てたくらいで異常な動作を起こすようなIT機器や放送設備ではあってはならない。システムの信頼性や安全性の面でも可用性の高いシステムをクラウド上に作り、その上でセキュリティパッチを迅速に当てられるような運用体制を構築していくことが必要ではないか。【小山構成員】
- ケーブルテレビは重要インフラとしてセキュリティには万全を期す必要があるものの、中小規模の事業者では情報収集やセキュリティ人材育成が難しいとの課題がある。【日本ケーブルラボ 取屋氏】
- ケーブルテレビ事業においても、ゼロトラストやSASE（Secure Access Service Edge）、SOC運用の高度化などが重要であり、セミナーを通して各種対策への理解・習得を図っている。また、業界内でのサイバーセキュリティ関係での情報共有にも力を入れている。 【日本ケーブルラボ 取屋氏】

## （3）自治体

**【現状】**

- 複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響を与えるリスクが想定されるため、それを担う情報システムにおいては、機密性はもとより、可用性や完全性の確保にも十分配慮した、情報システム全体の強靭性の向上が求められている。
- 地方公共団体の情報システム・ネットワークは、いわゆる「三層の対策」により強靭化の向上が図られてきたが、クラウドサービスの普及に伴い、インターネット接続系に業務端末・システムを配置したβ´モデルに対するニーズが高まっている。
- こうしたニーズ等を踏まえ、「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定に向けて検討が進められており、β´モデルへの移行やα´モデルの提示等、クラウドサービスの利用等に対応した必要なセキュリティ対策を新たに規定することとしている。
- システムの標準化については、2023年９月に閣議決定された「地方公共団体情報システム標準化基本方針」に基づき、原則として2025年度までに基幹業務システムを標準準拠システムに移行することとされている。
- 自治体分野における最も重要なセキュリティ対策の１つが、サイバー攻撃事案への対処及び情報セキュリティの統一的な窓口の役割を担うCSIRTの体制整備であり、さらにCSIRT機能を継続して維持していくことが必要。
- J-LISでは、自治体CSIRT協議会を運営する立場から、CSIRTの構築・運用支援、対応訓練や分野横断的演習等を実施している他、自治体職員向けにセキュリティも含むデジタル人材育成のための研修プログラムを提供。
- NICTが実施する実践的サイバー防御演習「CYDER」及び「プレCYDER」については、市町村の受講が進み、未受講自治体数も前年度比で約４割減少している。

**【今後の取組の方向性】**

- 今夏に改定予定の「地方公共団体における情報セキュリティポリシーに関するガイドライン」に基づくセキュリティ対策を着実に推進。
- クラウド化や標準化等、地方公共団体の情報システム・ネットワークを巡る今後の大きな環境変化に備えるためには、セキュリティ人材育成やCSIRTの体制強化が必要不可欠であることから 、J-LISや地域SECUNITYの取組の他、CYDERを通じて地方公共団体のCSIRTの能力・成熟度の強化に貢献していく。

# 1. 重要インフラ分野等におけるサイバーセキュリティの確保

## 【第8回までの構成員等からいただいたご意見】

＜自治体におけるサイバーセキュリティ対策の取組全般＞

- デジタル庁が提唱しているゼロトラストアーキテクチャをゴールに据え、全国ネットワークの構築によるセキュリティレベル・生産性の向上や、コストダウンが図れると思う。中長期的にゼロトラスト型に向けたビジョンを示すことが重要【小山構成員、後藤主査】
- 今後、三層分離からゼロトラストアーキテクチャの世界に移行する際、カスタマイズするほど、安全ではなくなるという大きなジレンマがある。解決策として、技術的な標準の在り方を示さなければならない。【上原構成員】
- 自治体行政の標準化・共通化・集約と、自治体の独自性のバランスをとることが重要。自治体の基幹システムを構築しているベンダ数は少なく、各自治体向けに地域のSIerがカスタマイズして提供している状況。自治体の疲弊は地域ビジネスの疲弊につながるため、地域のビジネスモデルについても考える必要がある。【APPLIC　吉本氏】

＜人材育成・体制整備関係＞

- CISO任命やCSIRT体制の整備は自治体規模による傾向は無い。また、大きな自治体では部署ごとのセキュリティ監査の頻度が少なく、セキュリティに関する意識の維持が難しい実態がある。【KUコンサルティング　高橋氏】
- 人口減少によって2040年に向けて自治体職員数が半減すると予測される中、現時点でも少ない情シス担当の更なる不足を見越して、自治体行政の標準化・共通化を進め、ガバメントクラウドに集約するといったスマート自治体への転換が必要となっている。人材育成のみならず外部人材の確保も重要。【APPLIC 吉本氏】
- 自治体のネットワークはLGWAN接続と三層分離だから安全という認識は誤りで、自治体のセキュリティにおいて完全防御は難しく、むしろインシデントが生じた際にいかに早く被害を見つけ、対応できるかが重要。そのためには、統一的な窓口としてのCSIRT体制の構築と、連絡管理体制の整備、訓練が重要。【KUコンサルティング　高橋氏】
- システムの不具合等問題が生じた際に的確な判断を行うため、組織の中において窓口としてのPoCは重要。【盛合構成員、KUコンサルティング　高橋氏】

## （４）データ流通基盤

### ①クラウドサービス

**【現状】**

- 昨今、官民問わずクラウドサービスの利用が急速に進み、それに伴うセキュリティ対策の重要性は引き続き高まっている状況。
- 2021年９月にクラウドサービス提供事業者向けの「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）」を公表。
- クラウドサービスの設定ミスに起因する情報漏えいや障害といった事故が多発していることを踏まえ、2022年10月に「クラウドサービス利用・提供における適切な設定のためのガイドライン」を公表した他、2024年４月には、利用者向けに本ガイドラインの内容をわかりやすく解説した「クラウドの設定ミス対策ガイドブック」を公表し、普及啓発を推進。

**【今後の取組の方向性】**

- 引き続き各種ガイドラインの普及啓発に取り組むとともに、必要に応じてガイドラインの見直し等を行うことにより、安心・安全なクラウドサービスの利用を促進する。
- クラウドボットネットを利用したサイバー攻撃の増加等、クラウドサービスを取り巻く国内外のセキュリティの最新動向の把握に継続して取り組む。

## （４）データ流通基盤

### ②トラストサービス

**【現状】**

- 我が国が推進する「信頼のあるデータ流通（DFFT）」の実現に向けて、トラストサービスは電子データを安心・安全に流通できる基盤として、重要な役割を担うことが期待されている。
- eシールについては、「eシールに係る検討会」を開催し、 2024年４月に、国によるeシールに係る認定制度の創設等を内容とする最終取りまとめを公表するとともに、技術・運用上の一定の基準を示した「eシールに係る指針（第２版）」を策定。
- タイムスタンプについては、時刻認証業務（電子データに係る情報にタイムスタンプを付与する役務を提供する業務）に対する認定制度を運用。

**【今後の取組の方向性】**

- 欧州のeIDAS2.0等の諸外国の動向を把握しながら、2024年度中のeシールの認定制度の創設やタイムスタンプに係る認定制度の的確な運用に取り組む。このような取組を通じ、各種トラストサービスを普及させることで、電子データを安心・安全に流通させることができる基盤を整え、DXを推進する。

## 【第8回までの構成員等からいただいたご意見】

＜トラストサービス＞

- eシールの対象は非常に広く、幅広いフォーマット、データを扱えるようにする必要がある。電子署名が普及するのに苦労したことを考えると、eシールについても制度を作るだけではなく、様々な仕掛けが必要だと思う。【上原構成員】

＜クラウドサービス＞

- 最近では、クラウドの中にもボットネットがあることがわかっている。クラウドからの攻撃は一台一台のリソースが大きく、かなり大きな攻撃ができると言われている。また、クラウドボットネットはIoT機器のみならず、クラウド上の他のホストを狙うこともあり、脅威がクロスオーバしている。【吉岡構成員】
- クラウド上のボットネットについて、クラウドサービスプロバイダの協力のもと対策を行うことができれば効果的だと思う。【蔦構成員、盛合構成員】

## （１）我が国のサイバー攻撃対処能力の向上

### ①CYNEX・CYXROSS

**【現状】**

- セキュリティ技術の過度な海外依存を脱却し、国内でのサイバーセキュリティ情報生成や人材育成を加速するエコシステムの構築を目指すCYNEXについて、NICTが開発したサイバー攻撃観測システムの供用等を通じて、産学官で連携してサイバー攻撃に係る情報収集・分析等を実施するとともに、その結果を活用して、国産サイバーセキュリティ製品の開発支援やセキュリティ人材育成支援を実施。2023年10月には、国内の産学官の組織が参画する「CYNEXアライアンス」が新規に発足。
- NICTが開発したセキュリティセンサーを政府端末に導入して端末情報を収集・分析するプロジェクトCYXROSSについては、センサー及びシステムの開発を完了し、2023年から一部府省庁の端末にセンサーを導入して端末情報の収集・分析を開始。

**【今後の取組の方向性】**

- CYNEX・CYXROSSの取組によって、国産のセキュリティ製品・技術による我が国のサイバー攻撃対処能力の向上を目指すとともに、安全保障の強化にも貢献していくため、主に以下の事項について取り組む。
  - ✓ CYNEXについては、産学官の連携により我が国におけるサイバーセキュリティ情報の収集・分析活動を抜本的に強化し、当該情報を利用する政府機関やセキュリティ関係団体、セキュリティベンダ、研究機関等のセキュリティ関係組織に対して必要な情報が提供される体制を構築する。
  - ✓ CYNEXで収集した情報やNICTが構築した演習基盤を供用することで、民間の演習実施事業者や教育機関等によるセキュリティ演習の実施を促進し、我が国で不足するセキュリティ人材を幅広く育成する。これらの取組をCYNEXアライアンスにおいて自立的に推進する。
  - ✓ CYXROSSについては、センサー導入府省庁を拡大し、端末情報をより広範に収集して、NICTのデータ及び技術も活用して独自に分析することで、我が国独自のサイバーセキュリティ脅威情報を生成し、政府システムのセキュリティ対策を強化するために当該情報をNISCやデジタル庁等の関係機関に提供する。加えて、CYXROSSをGSOCと連携させることで、エンドポイントを含む政府システムの一元的な監視体制の構築に貢献する。

## （１）我が国のサイバー攻撃対処能力の向上

### ②人材育成

**【現状】**

- 国の機関、地方公共団体及び重要インフラ事業者等の情報システム担当者等を対象として実践的サイバー防御演習「CYDER」を実施し、2023年度は3,742人が受講。
- 大阪・関西万博の安全な開催に資するよう、 2023年度から万博関連組織の情報システム担当者等を対象として万博向けサイバー防御講習「CIDLE（シードル）」を実施。
- 若手ICT人材を対象として、新たなセキュリティ対処技術を生み出しうる最先端のセキュリティ人材（セキュリティイノベーター）育成プログラム「SecHack365」を実施し、2023年度は38名が修了。

**【今後の取組の方向性】**

- NICTが収集・分析したサイバーセキュリティ情報及び構築した演習基盤を活用した実践的サイバー防御演習「CYDER」や、CSIRTの活動を支える「プレCYDER」を継続的に提供することで、未受講の政府機関・自治体ゼロを目指す等により、複雑化・巧妙化するサイバー攻撃に対する国の機関や地方公共団体等のCSIRTの基本的な対処能力を抜本的に強化する。
- 国の機関や地方公共団体等のCSIRT以外にも大きく拡大しているセキュリティ人材育成ニーズに対応できるように、CYDERで培った演習システムの産学官への展開・技術移転を推進する。
- 多くの優秀な修了生を輩出してきた我が国で唯一の長期ハッカソン形式による若手セキュリティ人材育成プログラム「SecHack365」を通じて、自ら課題を発見し新たな発想で解決策を生み出すことのできるセキュリティイノベーターの育成を継続するとともに、「SecHack365 Returns」等を通じて、修了生の社会での活躍を一層促進するために修了生によるコミュニティ活動を活性化させ、修了生が講師等としてプログラムに戻ってくるようなセキュリティ人材育成のエコシステム確立を目指す。

## 【第8回までの構成員等からいただいたご意見】

＜人材育成＞

- CSIRT等の体制や人材育成への課題意識は高まっており、引き続き組織におけるCSIRT能力・成熟度の強化に資する取組を行っていくいことが必要。その中でも、インシデント対応をチームで学べる集合演習の継続的提供、自治体におけるガバメントクラウドへの移行等の現場の業務内容の変化に対応できるような内容のアップデート、オンラインを活用した受講機会の提供等を検討していく。【NICT　園田氏】
- 受講者だけではなく、その後の自組織での展開等についてもヒアリングし、事例紹介できるとより良い。オンライン対応に加えて、受講後の復習や自組織での展開に役立てられるコンテンツも効果的だと思う。【辻構成員】
- インシデント情報の共有・公開についても、共有の促進と底上げのカリキュラムがあればよい。その際、対応時のフローや公開時・報告時のテンプレートを用いて「サイバー攻撃被害に係る情報の共有・公表ガイダンス」に沿い、情報収集できるスキームが望まれる。【辻構成員】
- 毎回同じコンテンツであっても、演習も含めて実施すべき。異動のタイミングでパッケージとして、コンプライアンスやハラスメントなどのリスクマネジメント分野でまとめることも効果的だと思う。【小山構成員】
- 体制や予算が限られている企業では人材育成は難しい。国内でもサイバー攻撃の被害が非常に多く事案対応を行う人材育成や、シミュレーションの機会のニーズは多い。CYDERのますますの利活用に期待している。【新井構成員】
- プレCYDERのような機会を積み重ねることによって自治体のセキュリティリテラシーが上がるため、継続して取り組むことが重要。【群馬県中之条町　田村氏】
- 自治体それぞれに人事があり、特定の分野に人を固定させることができないので、セキュリティ担当に就いた職員がセキュリティ・ITの知識がほとんどない場合も多く、素早く知識をつけてもらうためにはこのような演習は役に立つと思う。CYDERのような演習を情勢の変化に合わせて継続して実施することが重要。【上原構成員】
- 全てベンダに任せきりで何をやっているのか、どういう機器があるか分からない事業者もいるので、意識の醸成の点でもよい取組である。【蔦構成員】

## （１）我が国のサイバー攻撃対処能力の向上

### ③研究開発を担うNICTの取組・体制強化

**【現状】**

- NICTサイバーセキュリティ研究所は、セキュリティ技術に係る様々な研究開発の他、同研究所の強みを活かして、各種サービス（例えば、ナショナルサイバートレーニングセンターにおける公的機関CSIRT等の能力強化、ナショナルサイバーオブザベーションセンターにおけるインターネットに接続された機器の脆弱性調査及び対処方法の助言等）を実施している。

**【今後の取組の方向性】**

- NICTサイバーセキュリティ研究所が実施する事業の中で提供される上記の各種サービスについて、同研究所の強みを活かしつつ、サービス利用者の実態とニーズを精緻に把握し、これらに一層寄り添った形でサービス提供を行えるよう、同研究所の事業推進体制を強化する。
- サイバーセキュリティにおける我が国の研究開発能力の強化に向け、 当該分野で豊富なデータと技術、人材を有するとともに標準化や成果発信等においても大きな影響力を有する米国との連携を深化するため、NICT内に政府機関や研究組織との間でのサイバーセキュリティ技術に関する結節点を形成し、共同研究や人材交流、情報の共有や発信を戦略的に活性化させる。
- 上記の取組も含め、今後策定されるNICTの第６期中長期計画（2026年度～2030年度）に基づき、AI、量子技術、Beyond5G/6G等の将来的な技術動向を十分踏まえながら、我が国唯一の情報通信分野を専門とする国立研究開発法人として、我が国の自律的なサイバー攻撃対処能力の向上に向けて一層重要な役割を果たしていく。

## （２）新技術への対応

### ①AIとセキュリティ

**【現状】**

- 生成AIをはじめとするAI技術の急速な普及にともない、サイバーセキュリティ分野においてもAIを起因とした新たなリスク（AIの脆弱性を狙ったサイバー攻撃、AIの不適切な利用によるセキュリティリスクやAIを悪用したサイバー攻撃等）が指摘されている。
- AIの脆弱性を狙ったサイバー攻撃に対しては既存のセキュリティ対策と組み合わせた多層防御の対策、AIの不適切な利用によるセキュリティリスクやAIを悪用したサイバー攻撃に対しては、利用者リテラシーの向上や悪意のあるAIの検知・削除等の対策が挙げられている。
- 一方で、AIは効果的なセキュリティ対策手段として活用が進んでおり、特に昨今、サイバー攻撃の大規模化・複雑化・巧妙化に伴い、SOC等のセキュリティ業務負荷の増加が課題となっている中、今後、生成AIの利活用が期待されている。

**【今後の取組の方向性】**

- 生成AI等のAI技術を巡る最新動向を把握しつつ、AIに起因するセキュリティリスクを可能な限り回避・低減するとともに、AIのセキュリティ対策への効果的な活用を目指していく。
- AIに起因するセキュリティリスクについては、調査検証を実施した上で、関係省庁・機関と連携しつつ、本年４月に公表した「AI事業者ガイドライン」に基づき、セキュリティリスクの回避・低減を目的とした「開発者」「提供者」「利用者」向けのガイドライン策定を目指すとともに、「AIセキュリティ情報発信ポータル」の更新等を通じて、AIセキュリティに関する情報の的確かつ分かりやすい発信に取り組む。
- AIのセキュリティ対策への効果的な活用については、迅速かつ的確なサイバー脅威情報の収集、通信等の重要インフラ分野におけるサイバー攻撃検知・対処オペレーション業務の高度化等、セキュリティ対策強化に向けた生成AIの活用を促進する。

## （２）新技術への対応

### ②耐量子計算機暗号等の暗号技術

**【現状】**

- サイバー空間の安全性・信頼性は、情報の秘匿や改ざんの防止、認証等のために用いられる暗号技術の基盤の上で成立しており、サイバー空間の拡大にあわせて、暗号技術の重要性も増大している。
- 現在広く利用されている現代暗号は、従来型コンピュータでは効率的な求解が困難な数学問題に基づき安全性を担保しているが、今後の量子コンピュータの大規模化による計算機能力の向上に伴い、多くの現代暗号において危殆化リスクの増大が見込まれている。特に、公開鍵暗号は、大規模量子コンピュータにより、鍵長を伸長したとしても現実的な時間での解読が可能となることから、大規模量子コンピュータでも解読困難な耐量子計算機暗号（PQC）への移行が必要となる。
- CRYPTRECでは各種現代暗号の安全性監視を実施しており、NICTもPQCを含む現代暗号の安全性評価に関する研究開発を実施している。2023年3月、CRYPTRECにおける検討を踏まえ、NICT及びIPAにおいて「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」を策定した。
- また、今後、無線サービスにおいてもPQC等への移行が必要となることを見据え、5G等でのユースケースに合わせたPQCへの機能付加技術等の研究開発を2021年度から2024年度まで実施している。

**【今後の取組の方向性】**

- NICTにおける暗号安全性評価に関する研究開発の取組を充実させるとともに、その成果も活用して、CRYPTRECにおける現代暗号に対する安全性監視能力を維持・強化し、我が国として、PQCを含む形で、現代暗号の安全性評価・監視を主体的に実施する。
- 現代暗号の安全性評価・監視は、従来型コンピュータの計算機能力向上に加えて、量子コンピュータの計算機能力向上を考慮に入れて実施する必要があることから、これらの技術の進展を的確に把握する。
- CRYPTRECにおける現代暗号の安全性評価・監視で得られる知見も踏まえ、「CRYPTREC 暗号技術ガイドライン（耐量子計算機暗号）」や「CRYPTREC 暗号リスト」の改定を含め、 PQC等への移行に向けて必要となる技術的検討及び情報発信を実施する。
- 量子コンピュータの計算機能力向上に伴う現代暗号の危殆化リスクに対しては、各分野において適切にリスクを把握した上で、暗号移行には一定の期間を要することも考慮に入れつつ、PQC等への移行に向けて必要な対応を進める。
- PQC等への円滑な移行に向け、PQCや鍵長を伸長した共通鍵暗号の性能向上技術やクリプト・アジリティ技術等の研究開発を推進する。

## 【第8回までの構成員等からいただいたご意見】

＜ＡＩとセキュリティ＞

- 自社CSIRTでも生成AIの活用を模索しているが、一歩進めて、セキュリティが専門ではない人にサイバー攻撃の状況を分かりやすく図示・映像化するなど生成AIに橋渡し人材の役割を担わせられたらと考えている。【小山構成員】
- AIについては、著作権、データ保護、ガバナンス等について議論されてきたが、セキュリティについても本格的な議論が必要になっている。セキュリティ関連の文書ではAIも脅威がある旨簡潔に書かれる印象があるが、本分科会ではもう少し具体的に様々な脅威等に触れてもよいのではないか。【蔦構成員】
- 攻撃者が制約のないAIを使用する一方で、研究者は制限のあるAIを使用するため、その差がAI vs AIの能力差となってしまうおそれがある。【蔦構成員、新井構成員】
- AIを攻撃に活用する動きが進むと守る側はどんどん不利になるため、 AI for SecurityとSecurity for AIについては、今はAI for Securityを強力に推し、Security for AIは最低限のリスクヘッジに留める場面なのではないか。【上原構成員】
- 内部不正に対するAIを用いた不正検知による未然防止、事後対応の重要性が高まっているが、従業員に対する監視や、AIによるプロファイリングに繋がるため、プライバシーとの関係性の整理が必要。【蔦構成員】
- 国益の観点ではLLMを使わないという選択肢はなく、LLMのセキュリティ自体を過度に気にすることで、利用促進を阻害するようなことは起きてはならない。LLMに係るリスクに濃淡をつけ、優先順位をつけて対策していくような実態に即したガイドラインの整備が重要。【三井物産セキュアディレクション　高江洲氏】

＜耐量子計算機暗号等の暗号技術＞

- 暗号化されたデータについて、量子コンピュータ等により将来解読が可能になるまで保存しておくという脅威に対しては、今のうちから鍵を２倍にしておくというのは一つの選択肢であるが、対策を行う分だけコストは発生するため、情報・資産の価値に鑑みての対策が必要となる。【KDDI総研　清本氏】
- PQCに関する研究は、未だ予断なく様々な面から検討を続けなければならないフェーズにあって、安全性評価に関する研究開発投資を怠ることはできないと感じた【上原構成員】
- 重要性が非常に高い基礎研究を行っている中、マネタイズできないとの話もあったが、予算不足で研究ができなくなるようなことがないよう、国においても引き続き進めていただきたい。【蔦構成員】

# 3. 地域をはじめとするサイバーセキュリティの底上げに向けた取組

## ①地域セキュニティ

**【現状】**

- 全国11か所の総合通信局等の管区においてセキュリティコミュニティの設立が完了し、各地域において、セミナーやインシデント演習を継続的に実施している他、セキュリティに関心のある層の裾野を拡大するため、若年層向けCTFを実施。

**【今後の取組の方向性】**

- 地域におけるセキュリティ対策の状況を継続的に調査し、各地域の実情を把握していくとともに、地域向けの普及啓発活動を行う機関と更に連携を拡大すること、特定の業界・参加者向けといったターゲットを明確にしたイベントの拡充を図っていくこと、普及啓発活動が持続的なものとなるよう、それを担う地域の人材・体制の整備に取り組むことより、より効果的な取組としていくことを目指す。

## ②ガイドラインその他普及啓発に向けた取組

**【現状】**

- 「サイバーセキュリティ対策情報開示の手引き」「スマートシティセキュリティガイドライン」「テレワークセキュティガイドライン」「Wi-Fiセキュリティガイドライン」を策定・公表しており、各ガイドラインの周知啓発に取り組むとともに必要に応じて改定を実施。
- 一般国民向けのセキュリティ対策に関する情報発信を目的とした「国民のためのサイバーセキュリティサイト」については、最新の技術動向や社会環境を踏まえて内容の更新を行うとともに、デザインの大幅な見直しを行い、2024年５月にリニューアル。

**【今後の取組の方向性】**

- 既存のガイドラインについては、引き続き周知啓発、必要に応じた改定を実施するとともに、セキュリティの最新動向を踏まえながら、ガイドライン等を通じたセキュリティ対策の促進に貢献していく。
- 「国民のためのサイバーセキュリティサイト」については、一般国民がサイバーセキュリティの基本知識や日々行うべき望ましいセキュリティ対策（サイバーハイジーン）を学ぶことができるサイトとして情報のアップデートを継続的に実施するとともに、政府が発信する信頼できる情報源として認知度の向上に努める。

# 3. 地域をはじめとするサイバーセキュリティの底上げに向けた取組

## 【第8回までの構成員等からいただいたご意見】

＜地域におけるサイバーセキュリティの取組全般＞

- 我が国のサイバーセキュリティは啓発段階にあり、人材・予算ともに不足している。サプライチェーンに対する防護策として中堅以下の企業のサイバーセキュリティレベルの底上げ、基礎能力向上が重要。公助が発展途上で自助も困難であるため、シーサート同士の積極的なコミュニケーションによる共助が重要になる。【日本シーサート協議会 北村氏】
- 地域の企業はまず税理士に相談することから、普及啓発について、税理士にリーチしていくのは一つの選択肢としてあり得る。【蔦構成員】
- 加盟メンバーが自社内での活動において、協議会からの表彰を受けたことで理解を得られ活動がしやすくなったとの事例もあり、表彰制度等も効果的である。【日本シーサート協議会　北村氏】
- セキュリティの啓発は、地道にやっていくことも、目新しいもので足を運ぶ動機に繋げていくことも両方重要だと思う。様々な団体等との連携の中で取組の輪を広げるなど、多様なコンテンツで集客し啓発に繋げていくのも一つだと感じた。【新井構成員】
- 学生に向けての視野拡大とセキュリティ人口の増加のため、CTFは分かりやすくゲーム性もあって良いコンテンツだと思うが、CTFはセキュリティの仕事からは少し離れてしまっていると思うものもある。【辻構成員】
- 関西サイバーセキュリティネットワークが上手くいっている一番の理由は属人的な理由だと感じている。関心があり活動できる大学の研究者が複数揃っているという地の利があり、熱意をもって事務局を担う組織があることが非常に良く、継続して全体をみることができる人間が複数いることがかなり大きな要素である。【上原構成員、後藤主査】

＜その他普及啓発全般＞

- インシデント情報の共有・公開についても、共有の促進と底上げのカリキュラムがあればよい。その際、対応時のフローや公開時・報告時のテンプレートを用いて「サイバー攻撃被害に係る情報の共有・公表ガイダンス」に沿い、情報収集できるスキームが望まれる。【辻構成員（再掲）】

# 4. 国際連携の更なる推進

## ①国際連携全般

**【現状】**

- 国際情勢が緊迫化し、サイバー攻撃の脅威が高まっている中、サイバー空間の安全性確保のためには国際連携の更なる推進が必要不可欠な状況であり、関係省庁・機関と連携しつつ、二国間・多国間における各国政府・民間レベルでの情報共有やITUにおける国際標準化活動に積極的に関与。（主な実績：各国とのサイバー協議、クアッドサイバー会合、日ASEANサイバーセキュリティ政策会議、ITU-T SG17、ISAC連携ワークショップ等）

**【今後の取組の方向性】**

- 引き続き、関係省庁・機関と連携しつつ国際連携を推進し、サイバー空間の安全性確保に貢献するとともに、ICT分野における我が国のサイバーセキュリティ政策に関する取組の積極的な情報発信や国際機関等における標準化活動やその普及展開に取り組み、サイバーセキュリティ分野における我が国の国際的なプレゼンス向上を目指す。

## ②人材育成支援

**【現状】**

- ASEAN域内のサイバーセキュリティ能力の底上げに貢献するため、ASEAN等と連携し、2018年に日ASEANサイバーセキュリティ能力構築センター（AJCCBC）を開所。2023年３月以降はJICA技術協力により運営を支援。CYDER等の我が国発の演習コンテンツを提供している他、第三者連携のスキームを活用して有志国の研修プログラムも提供。2024年５月までの累計で、ASEAN域内の政府機関及び通信セクターの約1,700名が参加。
- 自由で開かれたインド太平洋（FOIP）の実現に向けた取組の一環として、 AJCCBCにおける知見・ノウハウを活用し、2024年２月に大洋州島しょ国を対象としたサイバーセキュリティ能力構築支援事業を試行的に実施。

**【今後の取組の方向性】**

- AJCCBCについては、JICAをはじめとする国内関係機関や有志国との連携の推進を通じて、我が国が提供するCYDER等の演習コンテンツの拡充に加え、第三者提供によるプログラムの拡大やICT以外の重要インフラセクターへの対象拡大を図ること等により、引き続きASAEN域内のサイバーセキュリティ能力の向上に貢献する。
- 大洋州島しょ国向け支援事業については、大洋州島しょ国のニーズを踏まえ、関係各国・機関と連携しつつ、実施体制や運用拠点等の検討を進め、2025年度以降の継続的かつ本格的な実施を目指す。
- AJCCBCや大洋州島しょ国向け支援事業で得られたノウハウ・知見を活用するとともに、有志国や世界銀行等の関係機関との連携を更に深めることにより、支援対象地域の拡大等、能力構築支援活動の更なる拡充に取り組む。

# 4. 国際連携の更なる推進

## 【第8回までの構成員等からいただいたご意見】

＜国際連携全般＞

- 日本のクリアランス法案により、日本のクリアランスシステムが米国のクリアランスシステムとインターオペラブルになれば、壁が無くなり、よりリッチな情報を使えるようになるのではないか。【NTTセキュリティホールディングス横浜氏】
- 日本の研究者が海外において研究開発を共同で行うといった場合に、半年を過ぎると現地の居住者となり、例えば米国の場合、米国で研究開発された技術を日本に帰国時に持ち帰り、日本の研究者と議論するといった場合には米国の輸出規制を考える必要生じる。最近は有志国以外との接触についても大変厳しいところがある。今後、研究開発や海外との情報交換・共同研究、日本の組織が海外に有する拠点と連携する場合にも同様の問題が生じるかと思う。【盛合構成員】
- サイバーセキュリティインシデントレスポンスという言葉について、特に海外のセキュリティコミュニティだと同じイメージを共有していないことが多くある。サイバーセキュリティフレームワークが理解を統一する手助けとなるため、このようなフレームワークに則った日本の製品やサービスを採用することで日本のサイバーセキュリティビジネスの支えになれば良いと考えている。【JPCERT　小宮山氏】

＜人材育成支援＞

- 途上国におけるサイバーセキュリティ分野では、ガバナンス等の脆弱性、重要インフラ防護の脆弱性、サイバー産業等の脆弱性の他、能力・スキルや国際連携の不足等の課題がある。【世界銀行　林氏】
- 演習などの効果はすぐには見えづらいものだと思うが、参加者のアンケートやコメントという観点以外での効果測定は、今後参加者を増やしていくために必要な情報だと思う。【辻構成員】
- 支援を進める段階で、サイバーセキュリティや情報プライバシー等の観点から制度面での対応が必要になる場合がある。特にこうした法的整備が円滑に進む国となかなか進みづらい国が非常に極端に分かれるという実態がある。【世界銀行　林氏】